MITIGATE

MITIGATE

Multidimensional, IntegraTed, rIsk assessment framework and dynamic, collaborative risk manaGement tools for critical information infrAstrucTrurEs

www.mitigateproject.eu

Grant Agreement No.653212
Topic: H2020-DS-2014-01
"**Risk Management and Assurance Models**"
Innovation Action

Deliverable D7.4

Repositories of Empirical Knowledge

Contractual Date of Delivery:	M30 / February 2018
Editor:	David Incertis, Rafael Company (VPF), Spyros Papstergiou, Eleni-Maria Kalogeraki (UPRC)
Work-package:	7
Distribution / Type:	PU
Version:	1.0
File:	D7.4_Repositories of Empirical Knowledge_final

Project co-funded by the European Union within the Horizon 2020 Programme

Abstract

This deliverable corresponds to the repositories of simulation scenarios, risk models, assurance models and more. The deliverable reflects the outcomes of task T7.4. “Repositories of threats, countermeasures and simulated scenarios”.

Executive Summary

Deliverable D7.4 populates, produces and provides databases/repositories of threat, countermeasures and simulated scenarios. These repositories are populated with specific threats, contingency plans and simulation models, which have been produced during the pilot operations of the project. These repositories provide reusable datasets, which could be used by interested parties as a basic set of evidence-based knowledge for risk management in the scope of dynamic supply chains in the maritime sector.

Version History

Version	Date	Comments, Changes, Status	Authors, contributors, reviewers
0.1	21/09/2017	Proposed TOC and contribution	David Incertis, Rafael Company
1.0	12/10/2017	Proposal of more concise TOC (sections 2-6 restructured/changed in new sections 2 and 3)	Spyros Papastergiou
1.1	19/10/2017	Addition of new section on scenarios of threats based on real events.	Spyros Papastergiou, David Incertis
1.2	23/10/2017	New TOC version previous to 6th SCM	Martin Stamer
2.0	07/11/2017	Working on sections 2, 3 and 4	David Incertis
2.1	15/12/2017	Distribution of contributions in section 3 with IMSSEA	David Incertis
2.2	19/12/2017	Redistribution of sub-sections in section 3	David Incertis
2.3	9/01/2018	New taxonomies added in section 2, proposition of cyber-attacks for section 3	Spyros Papastergiou
2.4	15/01/2018	Section 2 updated	David Incertis
2.5	25/01/2018	Contribution in section 3: cyber-attacks and statistics	Monica Canepa
2.6	5/02/2018	Attack Paths template for section 4	Eleni-Maria Kalogeraki
2.7	9/02/2018	Contribution on cyber-incidents (secton 3)	Monica Canepa
2.8	17/02/2018	Contribution in section 2	Spyros Papastergiou
2.9	26/02/2018	Contribution on statistics	Monica Canepa
3.0	26/02/2018	Final version of section 2	Spyros Papstergiou
3.1	27/02/2018	Final version of section 3 and conclusions	David Incertis
3.2			

Contributors

First Name	Last Name	Partner	Email
David	Incertis	VPF	mitigate@fundacion.valenciaport.com
Rafael	Company	VPF	rcompany@ fundacion.valenciaport.com
Spyros	Papastergiou	UPRC	spyrospapastergiou@gmail.com
Monica	Canepa	IMSSEA	m.canepa.unige@gmail.com
Eleni-Maria	Kalogeraki	UPRC	elmaklg1@gmail.com
Martin	Stamer	Fraunhofer	Martin.Stamer@cml.fraunhofer.de
Menia	Chatzikou	UPRC	mhatzikou@gmail.com
Apostolis	Karalis	UPRC	akaralis@hotmail.com
Christos	Douligeris	UPRC	cdoulig@unipi.gr
Dimitrios	Negkas	UPRC	akaralis@hotmail.com

Glossary

CERT	Computer Emergency Readiness/Response Team
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CSIRT	Computer Security Incident Response Team
ENISA	European Union Agency for Network and Information Security
ERP	Enterprise Resource Planning
NGIPS	Next Generation Intrusion Prevention Systems
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
RM	Risk Management
SC	Supply Chain
SCS	Supply Chain Service
SMB	Server Message Block
VLCC	Very Large Crude Carrier
WASC	Web Application Security Consortium

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Scope and objectives

This deliverable aims to populate, collect and provide a repository of threats, countermeasures and simulated scenarios. The repository is populated with specific threats, contingency plans and simulation models, which have been produced during the pilot operations of the project. This repository provides reusable datasets, which may be used by interested parties as a basic set of evidence-based knowledge for risk management in the scope of dynamic supply chains in the maritime sector. The deliverable also contains up to 27 different threat classification taxonomies, which are described in section 2. The taxonomies themselves can be found in the Annexes of the deliverable. Section 3 includes some statistics on cyber-attacks and the description of several real cyber attacks/incidents related to the logistic/maritime chain and other critical sectors such as energy.

1.2 Terminology

Asset: A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Attack: A well-defined set of actions that, if successful, would result in either damage to an asset, or undesirable operation.

Authentication: The process of verifying the identity or location of a user, service or application. Authentication is performed using at least one of three mechanisms: “something you have”, “something you know” or “something you are”. The authenticating application may provide different services based on the location, access method, time of day, etc.

Business partner: Ports/ port authorities, suppliers, contractors, suppliers, service contractors involved in the provision of a Supply Chain Service (SCS) or in any process/sub-process of the SCS.

Impact: Consequences for an organization or environment when an attack is realized, or weakness is present.

Phishing: is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

Supply Chain Service: Service provided by a supply chain, a linked set of resources and processes.

Threat: A potential violation of security (according to ISO 7498-2)

Vulnerability: A weakness or a flaw in an asset, raised either from implementation, design, or other processes, that can be exploited or triggered by a threat. Vulnerabilities could be induced through poor configuration, lack of security patching, etc.

Weakness: A type of mistake in software that, in proper conditions, could contribute to the introduction of vulnerabilities within that software. This term applies to mistakes regardless of whether they occur in implementation, design, or other phases of the SDLC.

Web Application: A software application, executed by a web server, which responds to dynamic web page requests over HTTP.

2 Threat Classification Taxonomies

Threat taxonomies respond to the necessity to offer a common language for conveying IT threats that could lead to cyber-attacks or cyber-incidents of any nature. Originally, threat taxonomies and catalogues were developed as an internal tool by different organizations related to ICT, used in the collection and consolidation of threat information. Regrettably, in the vast field of ICTs and computer science, there are many ways to classify cyber-threats, depending on many factors, so in general, existing incident taxonomies belong to either of the following groups[1]:

- Specific taxonomies developed by individual CERTs
- Universal, internationally recognized taxonomies

Several national CERTs have developed their way to classify cyber-threats, some just based on Internet security attacks (such as the one developed by the Latvian CERT NIC.LV, consisting of eleven types of cyber-attacks), based probably on the team's experiences; and other taxonomies are established according to who reported the incident, as in the case of the CERT-Hungary team, whose classification consists of just four categories (incidents reported by 1-National CIIP, 2-CIIP of partners with SLA, 3-International partners, 4-cooperating organizations). The value of these proprietary taxonomies is that they maximize the correlation with the team's needs and expectations, but they are not universally agreed or comparable with other taxonomies.

Following there is a description of different threat taxonomies and classifications, including some internationally agreed and others developed through European projects. The complete classification/taxonomies can be found in the Annex.

2.1 ENISA Threat Taxonomy

European Union Agency for Network and Security Information (ENISA) published its initial version (1.0) of threat taxonomy in January 2016. In this classification, cyber-threats should be understood as *threats applying to assets related to information and communication technology.* Such threats are materialized mostly in cyberspace, while some threats included are materialized in the physical world but affect information and cyber-assets. It would be worth noting that the taxonomy is mostly maintained only for cyber threats.

ENISA threat taxonomy has been built upon previous ENISA documents, whitebooks, other taxonomies and threat catalogues and even EU projects like Forward[2] or VITA[3]. It is considered to be a work in progress, which will be validated and enriched with additional information.

Threats taxonomy developed by ENISA consists of three fields:

- High level threats: The top-level threat category, used to distinguish different families of threats.
- Threats: The various threats within a family/category.

[1] ENISA: Existing taxonomies, published under Community Projects
[2] http://www.ict-forward.eu/
[3] https://www.researchgate.net/publication/220592994_Extensible_threat_taxonomy_for_critical_infrastructures

- Threats details: description of details of a specific threat, based on a specific attack type or method or targeting specific IT asset.

Next figure shows ENISA taxonomy as a mind map:

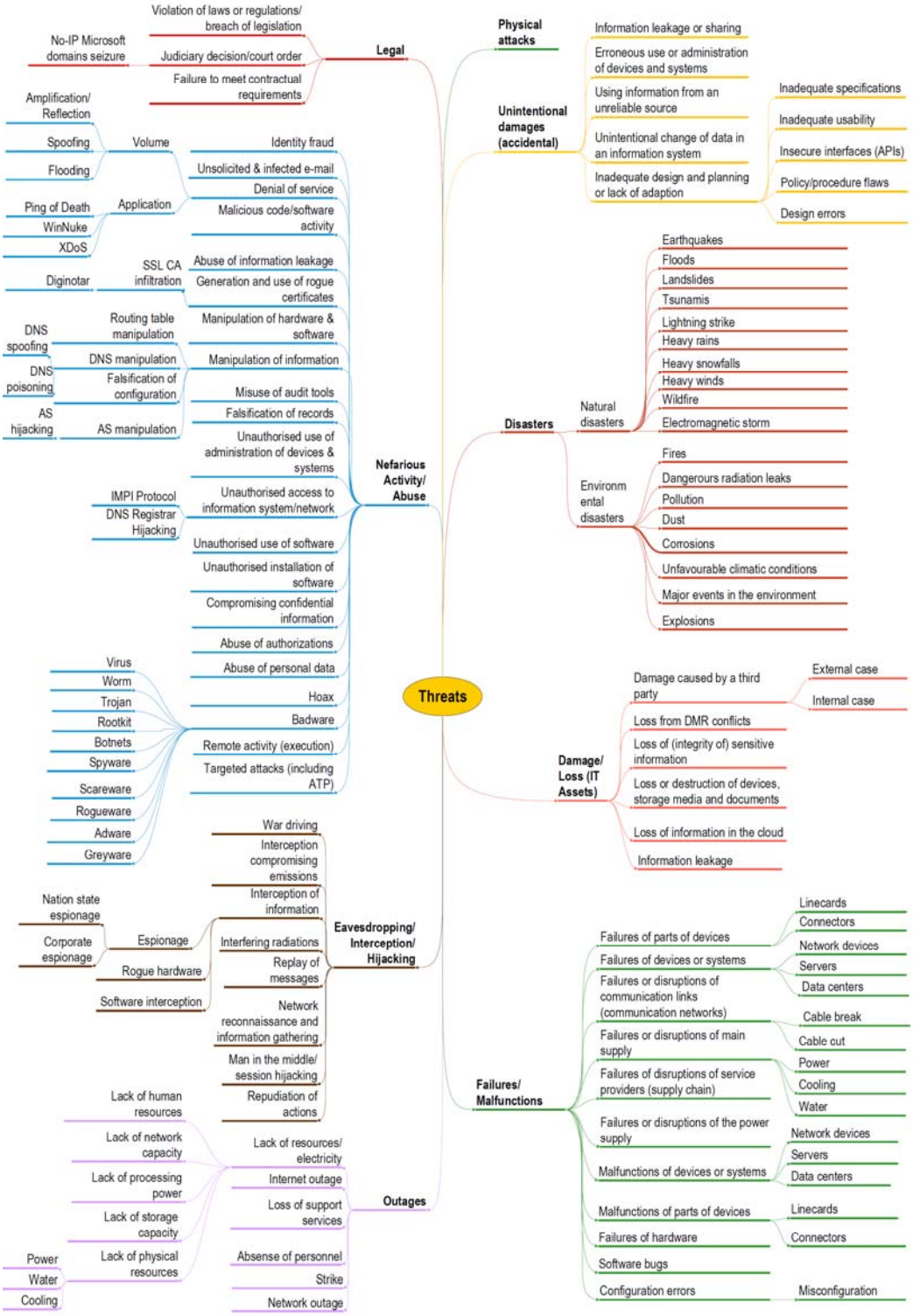

Figure 1 - ENISA Threat Taxonomy

Use-cases for threat taxonomy included: i) *Collection phase,* on which various findings are associated under a common threat ii) *Sorting/Consolidation phase* where threat and more information that is gathered is subjected to further grouping, analysis and prioritization and iii) *Asset exposure phase* where threats may be assigned to assets.

The complete ENISA Taxonomy can be found in Annex i.

2.2 WASC Threat Classification

The WASC Threat Classification [4] was created by the members of Web Application Consortium[4] in a cooperative effort to clarify and organise the threats to the security of a web site. This project aims to develop and promote industry standard terminology for describing these issues, so any professional related to IT security has the ability to access a consistent language and definition for web related security field. At present it is available version 2.0 of WASC Threat Classification although its last update is from January 2010. This classification outlines the attacks and weaknesses that can lead to the compromise of a website, its data or its users.

WASC provide two views, *Enumeration* and *Development Phase*. Enumeration view list the *Attacks* and *Weaknesses* that appear to endanger a web site. Attacks are defined as "a well-defined set of actions, that if successful, would result in either damage to an asset or undesirable operation". Weaknesses are "A type of mistake in software that in proper conditions could contribute to the introduction of vulnerabilities within that software".

Next there is a table that enumerates the attacks and weaknesses that can lead to the compromise of a website, its data, or its users. This serves as the base view for the WASC Threat Classification:

Attacks	Weaknesses
Abuse of Functionality	Application Misconfiguration
Brute Force	Directory Indexing
Buffer Overflow	Improper Filesystem Permissions
Content Spoofing	Improper Input Handling
Credential/Session Prediction	Improper Output Handling
Cross-Site Scripting	Information Leakage
Cross-Site Request Forgery	Insecure Indexing
Denial of Service	Insufficient Anti-automation
Fingerprinting	Insufficient Authentication
Format String	Insufficient Authorization
HTTP Response Smuggling	Insufficient Password Recovery
HTTP Response Splitting	Insufficient Process Validation
HTTP Request Smuggling	Insufficient Session Expiration
HTTP Request Splitting	Insufficient Transport Layer Protection

[4] An international group of experts

Attacks	Weaknesses
Integer Overflows	Server Misconfiguration
LDAP Injection	
Mail Command Injection	
Null Byte Injection	
OS Commanding	
Path Traversal	
Predictable Resource Location	
Remote File Inclusion (RFI)	
Routing Detour	
Session Fixation	
SOAP Array Abuse	
SSI Injection	
SQL Injection	
URL Redirector Abuse	
XPath Injection	
XML Attribute Blowup	
XML External Entities	
XML Entity Expansion	
XML Injection	
XQuery Injection	

Table 1 - Attacks and weaknesses of WASC Threat Classification

Development phase view focuses on where on the period of the development cycle is it possible that a vulnerability will appear.

The complete WASC Threat Classification can be found in Annex ii.

2.3 CAPEC - Common Attack Pattern Enumeration and Classification

CAPEC [5] provides publicly a very high level of detail catalog of common attack patterns classified into an intuitive manner together with a comprehensive schema for describing related attacks. Up to December 2017, CAPEC's list consisted of 508 attack patters and 4 levels of categorization.

CAPEC's taxonomy derives from Mitre's Common Weakness Enumeration (CWE[5]) and includes summaries, attack prerequisites and solutions for the most common attack patterns in every level of hierarchy, covering the entire attack life cycle [6]. Contains two views:

- By mechanisms of Attack: This is an effort to organize hierarchically attack patterns based on the mechanisms the employ. An example mechanism is:

[5] A dictionary of software security weaknesses and vulnerabilities

```
Collect and Analyse Information
    ▪ Excavation
        • Collect Data from Common Resource Locations
            o Detect Unpublicized web pages
            o (other…)
```

Other top-level mechanisms include:

- Inject Unexpected Items
- Engage in Deceptive Interactions
- Manipulate Timing and State
- Abuse Existing Functionality
- Employ Probabilistic Techniques
- Subvert Access Control
- Manipulate Data Structures
- Manipulate System Resources

- By domain of Attack: This view offers a two-leveled hierarchical categorization based on the domains of attack. An example is:

```
Software
    ▪ Brute Force
    ▪ (other…)
```

Other top-level domains are:

- Social Engineering
- Supply Chain
- Communication
- Physical Security
- Hardware

Full threat catalogue of CAPEC is presented in Annex iii.

2.4 ISO 28001:2007: Security management systems for the supply chain

According to the ISO 28001 standard on security management systems for the supply chain [10], a Supply Chain (SC) is the set of resources and processes which begins with the provision of raw materials and extends through the delivery of products or services to the customer through the different transport means. This standard provides specific guidance for implementation of a security management system for the supply chain. It is intended to assist organizations in establish reasonable levels of security and make better risk-based decisions for protection of the supply chain.

The ISO 28001:2007 uses a well-defined threat categorization that provides a systematic definition of threat categories so that: (a) Individual threat scenarios can be systematically identified and categorized for each Supply Chain Service (SCS), in a structured and repeatable manner, and (b) Threat

scenarios can be effectively mapped to the appropriate security controls and evaluated for their vulnerability in each business partner participating in the Supply Chain Service. In particular, all threat scenarios are divided into following categories:

a) **TC-1: Infrastructural Threats.** This category includes threats targeted to the infrastructure elements of a business partner (buildings, gates, warehouses, tracks, CCTV systems etc.).

b) **TC-2: Information & ICT Threats.** This category includes threats targeted to the information and ICT elements of a business partner (data, systems, software, hardware etc.).

c) **TC-3: Threats related with Personnel Security & Safety.** This category includes human centric threat scenarios.

d) **TC-4: Threats related with Goods and Conveyance Security.** By good we consider any item, exchanged or delivered via the SC Service, e.g. cargo, conveyance, and any related business procedures.

e) **TC-5: Other.** Under this category fall all other threats targeting the broader SC environment e.g. economical, security, commercial, and political instability.

- It should be noted that for each Threat Category, specific Threat Scenarios are defined, in order to assist the involved entities to examine the threat scenarios that are relevant to a Supply Chain Service under examination. Note that this categorization is not distinctive, and several threat scenarios may partially belong to more than one category. In Annex iv, threat scenarios for each threat category are defined.

2.5 Threats catalogue IT Grundschutz

IT Grundschutz[8] is a methodology created by the BSI (German initials for German Federal Office for Information Security). The aim of this methodology is to *achieve an appropriate security level for all types of information of an organization*.

On 2013 IT Grundschutz provided a non-technical catalogue of 46 elementary threats, both physical and cyber, including threat descriptions, example instances, causes and consequences of the threats. For example, for threat *Social Engineering* authors provide typical case attacks, like manipulating people by phone calls or developing a relationship with a targeted victim.

Many of the examples given by this catalogue and especially the more specific causes of the incidents can be narrowed down to more technical terms. *Loss of Integrity of Sensitive Information* threat is tagged by authors to be caused by: Transmission errors, malicious software incorrect input.

Full threat catalogue of IT Grundschutz is presented in Annex v.

2.6 CYSM Project Threats catalogue

CYSM (Collaborative Cyber/Physical Security Management System) is a project co-funded by the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme of the European Union developed between 2013 and 2015, that aimed at providing a targeted risk management methodology (CYSM-RM) for ports that relies on modelling and group decision making techniques using the collective knowledge of all users, estimating and rolling up risks (physical and cyber) across diverse target types, attack modes, and geographic levels. The CYSM-RM was implemented through a collaborative security management system (CYSM system) enabling ports' operators to: (a) model physical and cyber assets and interdependencies; (b) analyse and manage internal/external/interdependent physical and cyber threats/vulnerabilities; and (c) evaluate/manage physical and cyber risks against the requirements specified in the ISPS Code and ISO27001. During the project development, an activity for the identification of threats and vulnerabilities was carried out. The methodology for threats identification was based on various known threat categorization techniques (OCTAVE, CRAMM, NIST, etc). The result is a large number of threats grouped into the following categories:

- Physical Threats such as Earthquake, Flood, Hurricane, Lightning
- Technological Threats such as Hardware Malfunction
- Environmental Threats such as Pollution, Chemicals
- Human Threats such as Network Attacks, Virus Attack, Unauthorized Access
- Organized or Deliberate Attack such as Terrorist Attack - Explosive Mechanism, Sabotage, Arson
- Threats Lesion Data such as Malicious Data Corruption, Unauthorized Access to Data

Vulnerabilities were identified from previous audit controls, from universal lists relative to specific assets' vulnerabilities, from previous penetration tests and other available resources. The result was a list of vulnerabilities related to the specific threat of each asset. Assets identified were categorized as follows:

- ICT infrastructure
- Information and electronic data
- Physical infrastructure
- Software
- Hardware
- Site organization

Also, countermeasures (controls) were categorized according to the following classification:

- Generic
- Dissuasive and delay measures. Physical protection systems
- Detection of illegal actions and anti- intrusion. Electronic protection systems
- Video surveillance
- Identification systems

- Data protection measures
- Response systems
- Ship's operations and terminal's facilities

The whole catalogue can be found in Annex vi.

2.7 FORWARD Consortium Whitebook

FORWARD's project [2] motive on 2010 was to *identify relevant, future threats that have the potential to compromise the confidentiality, integrity, of Europe's Information and Communication Technology (ICT) infrastructures*.

28 threats in 8 categories were gathered with the aid of international experts, both from academia and industry and employing workshops and discussions about potential threats as well, focusing on those who require immediate attention. Three groups studied malware and fraud threats, emerging smart environments and critical systems. All research performed was around four axes: i) New Technologies, ii) New Applications iii) New business models and iv) New Social Dynamics.

The top-level threat categories by FORWARD were:

- Networking
- Hardware and Visualization
- Weak devices
- Complexity
- Data Visualization
- Data Manipulation
- Attack Infrastructures
- Human Factors
- Insufficient Security Requirements

Following the identification, the experts ranked the 28 threats based on the urgency for the need of their mitigation. This process was based on four factors: i) Threat Severity, ii) Possibility of spreading, iii) lack of awareness in the community and iv) Existing efforts for threat mitigation. Based on this analysis, the following five threats were considered the most urgent to attend:

1. Threats related to parallelism: The code written for parallel programming may be unsafe.
2. Threats related to scale: There is an increase to devices connected to a network and to the size of software packages.
3. Underground Economy support structures: Internet attacks motivated by underground economy have increases and their nature is not always easy to decipher.
4. Mobile device malware: There is a rapid increase on their number and the critical applications users download (e.g e-banking).
5. Threats related to Social Networks: There is an increase on the number of users and social network providers do not provide sufficient privacy protection.

Full threat catalogue FORWARD's project is presented in Annex vii.

2.8 *A Taxonomy of DDoS Attack and DDoS Defense Mechanisms, by* Jelena Mircovic

On 2004, Jelena Mircovic and Peter Reiher presented two taxonomies [9] for classifying attacks and defenses in the specialized area of Distributed Denial of Service (DDos) Attacks. The main criteria for the attack classification were common elements identified and important features in an attack. On the other hand, defenses mechanisms are classified based on their design decisions.

Attacks

As can be seen on following figure, authors used eight dimensions to classify DDos attacks, some of which also contain sub classes.

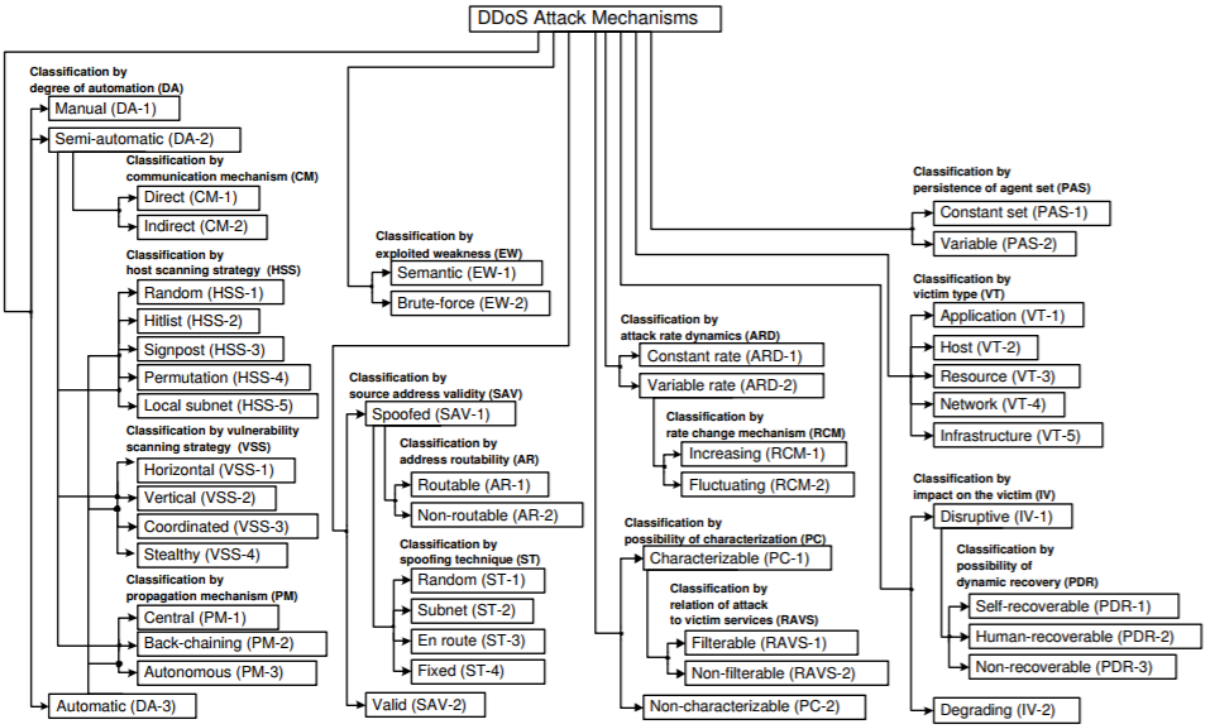

Figure 2 - A Taxonomy of DDoS Attack Mechanisms, by Jelena Mircovic

1. By Degree of Automation

First classification proposed is by the *degree of automation*, referring to whether the attack is performed manually or automatically. After, each attack is further characterised based on the communication mechanism between the agent and the handler. So, attacks can be *Manual*, *Semi-automatic* or *Automatic.*

In case of Semi-Automatic, attacks are also characterised by:

- *Communication Mechanism*, which is either *Direct* or *Indirect*
- *Host Scanning Strategy*: Refers to choosing vulnerable machines

- *Vulnerability Scanning Strategy.* Refers to targeting the vulnerabilities inside the vulnerable machines.
- *Propagation Mechanism*

2. *Semantic* or *Brute Force*
   - *Semantic*: exploiting a specific feature or weakness
   - *Brute Force:* delivering a very high amount of traffic volume to a targeted network
3. *By Source Address Validity*, having in mind the advantage an attacker maintains if he fakes his address. Spoofed Source Address is further categorized by Address Routability and by Spoofing Technique.
4. Next, attacks are characterised by their dynamics rate, being constant or variable. The latter then can be increasing or fluctuating.
5. Attacks can also be *characterizable or not.* This occurs at packets level and characterization may lead to better filtering.
6. Another classification is by *Persistence of Agent Set*, which refers to the commands that occur during the attack. So:
   - Constant Agent Set means that attacks are of the same type and happen in same rate.
   - Variable Agent Set means that attack is more complex and unpredictable resembling and army in which battalions attack at different times and places.
7. Moreover, authors characterize attacks by *Victim Type*, which include:
   - Application
   - Host
   - Resource Attacks
   - Network Attacks
   - Infrastructure
8. Final categorization on DDos attacks is by *Impact on Victim*. Disruptive impact is further divided according to possibility of dynamically recovering by itself, by Human, or non-recoverable.

Defences

DDos defence Mechanisms are characterised by:

1. *Activity level*

   This distinction focuses on preventive and reactive defense.

2. *Cooperation Degree*

   While employing defence, targeted entities can collaborate or not with other entities. Based on this distinction, authors enumerate *autonomous, cooperative* and *interdependent* mechanisms

3. *Deployment Location*

   This categorization refers to the defence service location. The cases are *Victim Network,* where historically most defence mechanisms were located, *Intermediate Network, in* which case victim contacts the infrastructure and request the service and finally *Source Network.* This last case means that source network applies mechanisms for preventing attacks happen from inside.

All three classifications contain subclasses that can be seen on next figure.

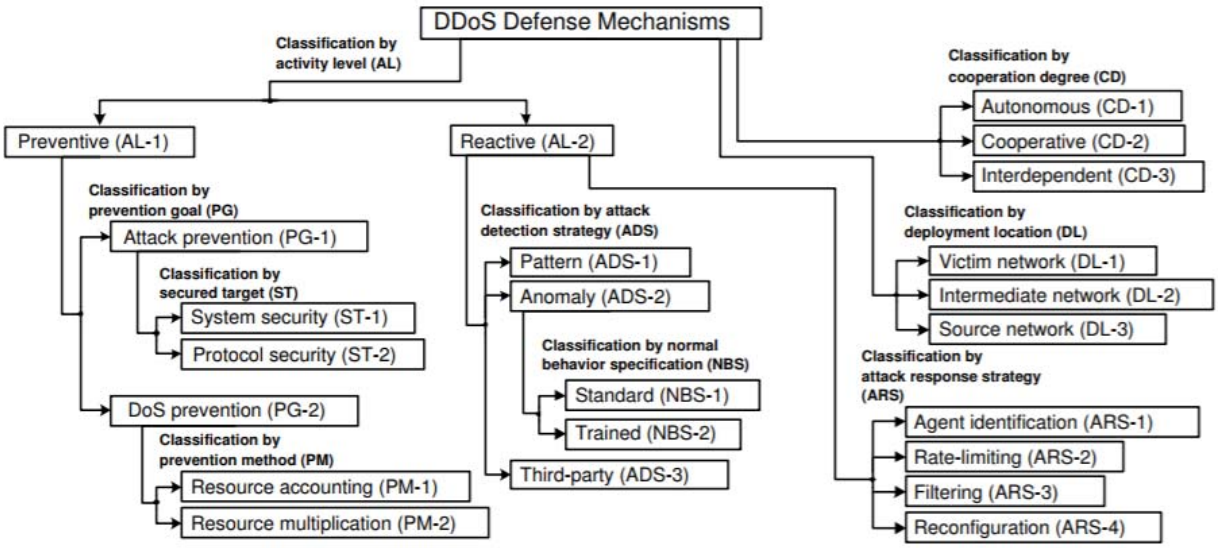

Figure 3 - A Taxonomy of DDoS Defence Mechanisms, by Jelena Mircovic

2.9 NIST Guide for conducting Risk Assessment

On 2012, National Institute of Standards and Technology (NIST) provided a special publication revision for conducting Risk Assessment [11]. On the use cases included on this paper, an exemplary taxonomy of threat sources and associated threat characteristics was used.

The main reason for the existence, the structure and the attributes of this taxonomy was to provide to an organization input for identifying assumptions for risk assessment.

The Taxonomy is structured by: *Threat Source Types, Descriptions* and *Characteristics.* Threat Source Types are organized hierarchically, and the top-level categories are:

1. *Adversarial*, which are threats types that try to exploit the organization's dependence on cyber resources.
2. *Accidental,* meaning threats that are caused by erroneous actions of people during their everyday work.
3. *Structural,* which refers to failure of equipment, environmental controls, aging software.
4. *Environmental.* This threat type focuses on natural disasters that affect critical infrastructures but are outside the control of an organization.

This hierarchy consists of three levels in most. Example instances include threats *Insider* and *Outsider* being members of class *Individual,* which is a member of class *Adversarial* while *User* and *Administrator* are members of class *Accidental* (two level hierarchy).

Full threat taxonomy is presented in Annex ix.

2.10 eCSIRT.net Incident Classification

The European CSIRT project (eCSIRT) was a consortium of established CSIRTs from the European CSIRT community that tried to raise the awareness and understanding of the work of Computer Security Incident Response Teams. On 2003 proposed an incident classification table [12] that would be used to categorize statistical threat data gathered by participating teams on the project, based on rules and validation.

The table employed by eCSIRT contains incident types which all belong to incident classes. Authors also provide detailed descriptions of the incident types (or just the classes). Examples of types are *Worm* and *Virus*, being part of the *Malicious Code* class.

Full Incident Classification table is presented in Annex x.

2.11 Proposed top level classification of incidents (by Andrew Cormack)

With the aim of helping exchanging data and statistics between incident response teams, Andrew Cormack proposed in 2000 a top-level incident classification [13]. This publication was part of Terena – Dante association (now GEANT) and their Task Force that initiates collaboration between European CSIRTs.

This table consisted only of high level threats (which referred to the impact of an attack) and their description.

Author intended to expand the catalogue with more threat types, analyzing the high level threats like for example “Denial Of Service” to “Crashed Service: malformed packet” and “multiple connections : resource starvation”.

Last, he allowed for other teams involved to include extension classifications for their own needs.

High level Threat	Threat details
Abusive communication	Any abusive or offensive message, whether sent by e-mail, web form, news, IRC etc. These include threats, offensive language, pornography etc.
Denial of Service	Actions that make excessive or unusual use of resources thus harming normal operation.

High level Threat	Threat details
Packet sniffing	Any unauthorised observation of the packet stream on a network. Usually aimed at obtaining passwords, commercial or personal information.
Other	Any incident that cannot be classified with one of the other classifications
Probe	Network traffic used to discover information about machines or services connected to a network.
Root compromise	A system is compromised to the "root" level, the attacker has total control over the system
Spam	Abuse of Internet message services (e-mail, news, IRC) usually involving the sending of large volumes of unsolicited mail. Often uses open systems at third party sites as relays to obscure the origin of the traffic, so reports of such relays are also placed in this classification.
Trojan	Any incident involving the use of a program which conceals its true function. This technique is often used to persuade users to install remote control (e.g. Back Orifice, Netbus) or attack programmes.
Unauthorised use	Any use of services without authority (e.g. "Borrowed" accounts, open web caches etc.)
Virus	Any incident involving viruses
Warez	Distribution of illegal software

Table 2 - Top level classification of incidents by Andrew Cormack

2.12 Incident Taxonomy by CESNET Archive

CESNET, an association of universities of Czech Republic and the Czech Academy of Sciences, employed on 2010 a simplistic, non-exhaustive enumeration of incidents [14]. This happened within an effort to help CSIRT teams use and create tools for incident categorization and evidently led procedures to be as automated as possible using machine learning algorithms.

This list has been created by examining up to date incident types based on their rapid increase of occurrence. Causing symptoms to a system was the rule for including a type to the list. As the authors note, some types are not mutually exclusive, for example spam is a part of Phishing.

CESNET's taxonomy was mostly a tool towards automation (or semi-automation) on incident handling, supporting other tools and not a detailed list. Nevertheless, it contained the most frequent incident types up to 2010, so it is not to be ignored.

High level Threat	Threat details
Spam	Usual unsolicited commercial email
Bounce	Mail backscatter (usually caused by spam)
Phishing	Spam is used as advertisement for a website which imitates some well-known institution in order to gain its clients' personal information (bank account credentials, credit card information).
Copyright	Copyright infringement, usually by means of peer-to-peer networks
Trojan	Malicious code on a server attempting to attack server clients and spread on (by defaced web page or active probing).
Malware	Malicious code on a client workstation, for example keylogger, rootkit or malware as a part of botnet. Trojan and Malware classes partially overlap, in many cases they can be in fact the same code. However, we are trying to distinguish the situation where primary function is to spread and attack another machines (Trojan), while Malware mainly collects user data, sends spam, etc.
Probe	Probing servers and networks. Portscan, portsweep, SSH (or other service) scan or unsuccessful attempts to crack service.
DOS	Simple or distributed. Again, it partially overlaps with a probe, but DOS's primary aim is denying the service, not a compromise.
Crack	Generally, any other compromise
Other	Anything we are not able to classify into previous categories. Meant as a fallback category, which should get reviewed regularly, and the results of which should get incorporated back into this taxonomy.
Unknown	It is not possible to clearly state the incident type from report (usually some additional clarification from the complainant is needed).

Table 3 - Incident Taxonomy by CESNET Archive

2.13 Incident Taxonomy by CERT NIC.LV

CERT.LV [39] is the Information Technology Security Incident Response Institution of the Republic of Latvia. Its mission is to promote cyber security nationally by obtaining and updating information on IT security threats.

CERT.LV defined an incident as "all kind of misuse of internet resources and violation of acceptable use, policies, including sending spam or viruses, phishing, port scanning, unauthorized access, system compromises, etc"

On 2011 its members proposed example threat taxonomy and since 2017 they use eCSIRT classification.

High level Threat	Threat details
Intrusion Attempts	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g. buffer overflow, backdoor, cross site scripting, etc.). Multiple login attempts (Guessing / cracking of passwords, brute force). An attempt using an unknown exploit.
Information Content Security	Besides a local abuse of data and systems the information security can be endangered by a successful account or application compromise. Furthermore, attacks are possible that intercept and access information during transmission (wiretapping, spoofing or hijacking). Human/configuration/software error can also be the cause.
Information Gathering	Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), port scanning.
Abusive Content	Spam or "Unsolicited Bulk Email", this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content. Child Pornography and other illegal content defined by the Law on Pornography Restrictions and Criminal law. Hate speech.
Vulnerable	Open for abuse: open resolvers, world readable printers, vulnerability apparent from Nessus etc scans, virus signatures not up-to-date, etc

High level Threat	Threat details
Intrusions	A successful compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by an unauthorized local access. Also includes being part of a botnet.
Fraud	Using resources for unauthorized purposes including profit-making ventures (E.g. the use of e-mail to participate in illegal profit chain letters or pyramid schemes). Type of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it or persuade the user to reveal a private credential.
Malicious Code	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
Availability	By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. DoS examples are ICMP and SYN floods, Teardrop attacks and mail-bombing. DDoS often is based on DoS attacks originating from botnets, but also other scenarios exist like DNS Amplification attacks. However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.) - or by Act of God, spontaneous failures or human error, without malice or gross neglect being involved.
Other	Consultations and all incidents which don't fit in one of the given categories.

Table 4 - Incident Taxonomy by CERT NIC.LV (adapted from eCSIRT)

2.14 A Taxonomy of Operational Cyber Security Risks (Software Engineering Institute)

On 2010 Carnegie Mellon Software Engineering Institute (SEI) presented a taxonomy [17] with the scope of helping organizations identify all potential cyber security risks. SEI defines this risk as operational threats to information and technology assets that affect confidentiality, availability and integrity of information or information systems.

SEI's taxonomy organised Operational Cyber Security Risks into four classes:

- Actions of People. These could be actions (or lack of action) taken by people accidentally or deliberately affecting cyber security.
- Systems and Technology Failures. This refers to failure of hardware, software and information systems.
- Failed Internal Processes. These are failures and problems in the internal business processes that result to inability for management, implementation and sustain of cyber security.
- External Events. These events are outside the control of an organization. Examples are disasters, service provider dependencies, business issues.

Then, each class is divided to subclasses, which are described by elements. These classes "draw upon the definition of the operational risk by the banking sector in the Basel II framework" focusing on the assets and the operations involved.

An example class of the taxonomy *Actions of People* has three subclasses, either of which contains elements:

1. Inadvertent
    a. Mistake
    b. Error
    c. Omission
2. Deliberate
    a. Fraud
    b. Sabotage
    c. Theft
    d. Vandalism
3. Inaction (Lack of)
    a. Skills
    b. Knowledge
    c. Guidance
    d. Availability

Full classes, subclasses and elements of the Taxonomy are presented in Annex xii.

Authors also compare this taxonomy with others in literature (Fisma, Octave, Nist, Cert) and try to map their classes and attributes.

2.15 ESCORTS Project

European network for the Security of Control and Real-Time Systems (ESCORTS) [18] was a project aiming at cyber security and specifically assisting European stakeholders in developing and maintaining control system security standards.

ESCORTS provided reports with Taxonomies of security vulnerabilities, threats and solutions. These reports focused on the problems that industrial control systems face and the solutions and countermeasures that could be taken. Authors did not include suggesting best practices on security solutions, but this might be part of their future work.

As far as *SCADA Vulnerabilities* are concerned, ESCORTS taxonomy classifies them into *Architectural, Security Policy, Software* and *Communication Protocol Vulnerabilities.* The last category contains three subcategories, *MORDBUS, DNP3* and *Summary of the vulnerabilities of protocol and relevant threats.*

Attack Scenarios are divided into *SCADA Protocol Oriented Attacks*, *Process Network Attacks* and *Exchange Network Attacks,* with each high-level category containing sub-categories. Some lists are not exhaustive but exemplary

Finally, project partners proposed four categories of SCADA security countermeasures having in mind the vulnerabilities mentioned earlier and not a complete list. These categories are: *Communication Protocol, Filtering and Monitoring, Architectural Good Practices* and *Organizational countermeasures* and each includes more specific sub-categories.

Full Vulnerabilities, Attack Scenarios and Securities countermeasures tables are presented in Annex xiii.

2.16 VERIS taxonomy

VERIS [33][36] stands for the Vocabulary of Event Recording and Incident Sharing and its community aims to provide quality information regarding cyber security (and physical) to industry organizations. To achieve this, VERIS assists then in collecting and sharing data with other organizations so a foundation that would help in learning from experience would be built.

The threat categorization VERIS provides contains general, both technical and non-technical descriptions of threat events. Also includes a large, complex but comprehensive and exchangeable vocabulary. The attributes it provides describe incidents by:

- *Incident Description:* Information about its discovery method, its confidence, its confirmation, the target victim and the cost to correct it.
- *Victim:* The number of victims.
- *Actor:* information about the attacker, for example his motive and the group he may belong inside or outside the organization.
- *Action:* The threats describe the *action* of malware or a hacking. VERIS defines action as what caused or contributed to an incident, and uses seven primal action categories: *Malware, Hacking, Social, Misuse, Physical, Error and Environmental.* Attributes of each category include: variety, vector, vulnerability, common name, notes. There is a distinction between malware and hacking in the action, and then each distinction is further categorized to variety and vector [35].
- *Asset:* Information about the assets involved in the incident.
- *Attribute:* Confidentiality and Integrity State.
- *Timeline:* The time of the incident.
- *Impact:* The overall loss caused by the incident, in numbers and descriptively.
- *Repeated:* Information about the Country and the Currency code.

VERIS taxonomy can be downloaded in JSON format through MISP framework's Github repository [37].

Tables of *Hacking Variety* and *Discovery Method* of the Taxonomy and examples of all attributes are presented in Annex viii.

2.17 OWASP Threat Categories and Application Threat Modelling (includes Stride Threat List)

OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security. They advocate approaching application security as a people, process, and technology problem because the most effective approaches to application security include improvements in all of these areas.

OWASP Application Threat Modelling is an approach for analyzing the security of an application. It is a structured approach that enables to identify, quantify, and address the security risks associated with an application. Threat modelling is not an approach to reviewing code, but it does complement the security code review process. The inclusion of threat modeling in the SDLC can help to ensure that applications are being developed with security built-in from the very beginning. This, combined with the documentation produced as part of the threat modeling process, can give the reviewer a greater understanding of the system [30].

STRIDE is a threat categorization used by OWASP. This categorization comes from the formulation of questions like [15]:

- How can an attacker change the authentication data?
- What is the impact if an attacker can read the user profile data?
- What happens if access is denied to the user profile database?

It is useful in the identification of threats by classifying attacker goals such as:

- **Spoofing identity**. An example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password.
- **Tampering with data**. Data tampering involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet.
- **Repudiation**. Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise—for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. **Nonrepudiation** refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package.
- **Information disclosure**. Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers.

- **Denial of service**. Denial of service (DoS) attacks deny service to valid users—for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability.
- **Elevation of privilege**. In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed.

The OWASP Top Ten Project is a document for web application security. It represents a broad consensus about the most critical security risks to web applications. Project members include a variety of security experts from around the world who have shared their expertise to produce this list. The most recent Top Ten Application Security Risks list is from 2017 [16]. It can be found in Annex xi.

Type	Example	Security Control
Spoofing	Threat action aimed to illegally access and use another user's credentials, such as username and password.	Authentication
Tampering	Threat action aimed to maliciously change/modify persistent data, such as persistent data in a database, and the alteration of data in transit between two computers over an open network, such as the Internet.	Integrity
Repudiation	Threat action aimed to perform illegal operations in a system that lacks the ability to trace the prohibited operations.	Non-Repudiation
Information disclosure	Threat action to read a file that one was not granted access to, or to read data in transit.	Confidentiality
Denial of service	Threat aimed to deny access to valid users, such as by making a web server temporarily unavailable or unusable.	Availability
Elevation of privilege	Threat aimed to gain privileged access to resources for gaining unauthorized access to information or to compromise a system.	Authorization

Table 5 - STRIDE Threat List

2.18 HP Tipping Point Event Taxonomy

Trend Micro Tipping Point's Intrusion Prevention System (IPS) deals with IT threat protection. Combining new application-level security practical with user awareness and inbound/outbound messaging inspection capabilities.

The scalable NGIPS protects the user's applications, network and data from new threats. The Tipping Point NGIPS protects the user's network from the sophisticated attacks.

Tipping Point now functions as a part of Trend Micro Security. Previously TippingPoint was a division of HP, part of their Enterprise Security Group. In September 2013, HP announced that it entered the next-generation firewall market with a new line of Tipping Point firewalls. The new line extends TippingPoint's existing intrusion prevention system (IPS) appliances with traditional stateful packet filtering and application control.

The HP TippingPoint Event Taxonomy is set for use with the SMS Web Services API version 1.1 and later [19].

Full event taxonomy table is presented in Annex xiv.

2.19 Threat Taxonomy for Cloud of Things

On 2016, University of Southampton published a study [21] on Cloud of Things (CoT) and referred to the need of properly analyzing security issues of this new technology. To achieve this, authors presented a threat model which could be used to construct a threat taxonomy specialized is this area of security.

Nist definition for Cloud computing: "a *model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*""

Authors describe the *Cloud of Things* as « a scalable IT paradigm for providing a pay per use on demand network access to self configurable mutual pool of identified interconnected sensing devices embedded with different technologies (e.g., Wireless Sensor and Actuator Networks (WSAN), Applications, Near Field Communications (NFC), Radio Frequency Identifier (RFID)), which can be distributed globally and promptly provisioned in order to perceive data from the real world environments and link it with the digital world»

Authors focused on simultaneous accesses to Internet of Things (IoT) devices and the constraints that should be implemented in order to avoid resource conflicts. The threat model proposed consisted of the following steps:

1. Outlining the adversary model: An assumption of the attacker's capabilities.
2. Listing assets of the system: IoT devices and other resources which may be subject to threat. List included *IoT devices, Cloud servers with storage capabilities* and *Client devices*
3. Identifying possible threats on those assets

4. Outlining mitigation strategies

Based on this threat model, a threat taxonomy was proposed. This taxonomy consisted of two high level threats, *Security* and *Privacy* which was also the motivation for potential threat identification. *Security* consisted of five threat categories*: Communication Threats, Physical Threats, Data Threats, Service Provisioning Threats* and *Other.* Each category then included several subcategories. *Privacy* threats were divided into seven sub categories: Unnoticed capture & Unaware identification*, IoT data inaccessibility, Lack of control and transparency, Loss of governance, Profiling and tracking, Unforeseen inference* and *Unauthorized disclosure.*

The full taxonomy is presented in Annex xv.

2.20 A Multi Dimension Taxonomy of Insider Threats in Cloud Computing

This taxonomy comes from a research to develop a framework for mitigating insider threats in cloud computing environments. The article in which the research is described [22] presents primarily a multidimensional taxonomy of insider threats in cloud computing and demonstrates its viability. The taxonomy provides a fundamental understanding for this complicated problem by identifying five dimensions; it also supports security engineers in identifying hidden paths, thus determining proper countermeasures, and presents a guidance that covers all bounders of insiders' threats issue in clouds; hence, it facilitates researchers' endeavours in tackling this problem. For instance, according to the hierarchical taxonomy, clearly many significant issues exist in public cloud, while conventional insider mitigation solutions can be used in private clouds. Finally, the taxonomy assists in identifying future research directions in this emerging area.

The full taxonomy table is presented in Annex xvi.

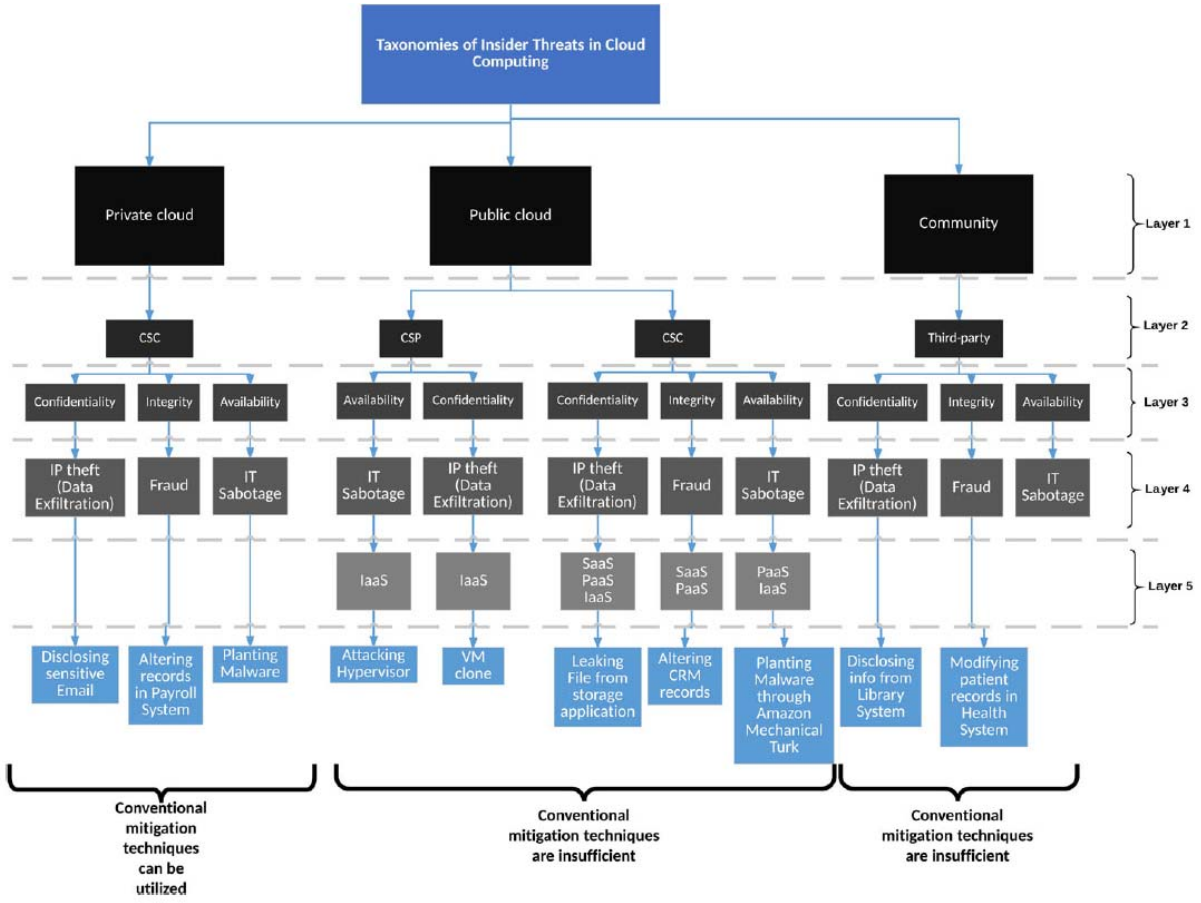

Figure 4 - Hierarchical Taxonomies of insider threats in Cloud Computing

2.21 A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks

Another specialized area of possible threats is Social Engineering. On 2015, Ryan Hartfield and George Loukas from University of Greenwitch published a study [23] on social engineering attacks taxonomies, also including a survey of defense mechanisms. Authors' aim was to help researchers and engineers develop defense approaches on present and future semantic attacks, focusing on special characteristics of those and not their particular implementation.

Semantic attacks are a type of social engineering attacks and in the context of social engineering have been defined as "the manipulation of user-computer interfacing with the purpose to breach a computer system's information security through user deception." On the table below, there can be seen examples of semantic attack exploits:

Table 6 - Examples of Semantic Attack Exploits

Attack Family	Exploits
Phishing	Email, Website, URL, IM, Forums, SMS, IRC
File Masquerading	Office Document File, Application File, System File
Application Masquerading	Scareware, Ransomware, Rogueware
Web Pop-Up	Media Plugin, Error Message, Bogus Questionnaire
Malvertisement	Infected Ad, One Click Fraud, Download Button
Social Networking	Friend Injection, Fake Video Links, Game Requests
Removable Media	USB, Flash/SD, CD/DVD
Wireless	Rogue AP, Rogue RFID

Authors in their implementation use three control stages proposed by CESG[6]: *Orchestration, Exploitation and Execution.*

Orchestration describes how the target victim is chosen, the level and method of the automation of the attack and the method used to reach the target victim. *Exploitation,* being the second stage focuses on two elements: What it was that actually deceived the user and how was the platform used manipulated. Finally, *Execution* stage describes the number of steps (one or multiple) of the attack and the attack persistence. The values of these attributes (shown in the table below) define the categories and subcategories of the taxonomy.

[6] https://www.gov.uk/government/organisations/cesg

Control Stage	Category	Category Details
Orchestration	**TD: Target Description**	TD1: Explicit Targeting
		TD2: Promiscuous Targeting
	MD: Method of Distribution	MD1: Software
		MD1-L: Local
		MD1-R: Remote
		MD2: Hardware without Software Interaction.
		MD3: Hardware with Software Interaction
	MA: Mode of Automation	MA1: Manual
		MA2: Automatic
Exploitation	**DV: Deception Vector**	DV1: Cosmetic
		DV2: Behaviour
		DV3: Hybrid.
	IM: Interface Manipulation	IM1: User Interface
		IM2: Programmatic Interface
Execution	**AP: Attack Persistence**	AP1: One-off
		AP2: Continual
	ES: Execution Steps	ES1: Single-Step Attack
		ES2: Multistep Attack

Table 7 - Taxonomy of semantic attack mechanisms

In Annex xvii a taxonomic Classification of Semantic Attacks can be found where typical attacks are mapped to values of the attributes. For example, *Bluetooth phishing* is mapped to the following values:

Control stage	Attribute	Value
Orchestration	**TD: Target Description**	TD2: Promiscuous Targeting
	MD: Method of Distribution	MD3: Hardware with Software Interaction
	MA: Mode of Automation	MA1: Manual
Exploitation	**DV: Deception Vector**	DV1: Cosmetic
	IM: Interface Manipulation	IM1: User Interface
Execution	**AP: Attack Persistence**	AP1: One-off
	ES: Execution Steps	ES1: Single-Step Attack

Table 8 - Taxonomic classification example for semantic attack "Bluetooth phishing"

2.22 VoIP Security and Privacy Threat Taxonomy

The VoIP Security and Privacy Threat Taxonomy, developed in 2005 by VOIPSA s the many potential security threats to VoIP deployments, services, and end users. The overall goal is to help drive VoIP security awareness with the press, industry and public. In particular this Taxonomy provides a detailed structure for technical vulnerabilities that informs the following constituencies:

- Press and public
- All vendors across the value chain including:
  - carriers,
  - service providers,
  - equipment vendors
  - software developers, and
  - system integrators
- The technical community of designers and experts
- Media and entertainment content developers and publishers
- The policy and regulatory community
- The law enforcement community

This Taxonomy also provides a clear definition of security to make security measurable, actionable and subject to economic and social trade-off analysis [24].

The full taxonomy table is presented in Annex xvii.

2.23 Circl -MISP Information Security Indicators Class

Computer Incident Response Center Luxembourg (CIRCL) [43] is a government driven initiative about the collection, analysis and reporting of computer security threats and incidents. CIRCL, along with Belgian Defence and NATO / NCIRC (Computer Incident Response Capability) have created Malware Information Sharing Platform (MISP)[42], an open source project that stores and shares information related to indicators of Compromise of targeted attacks, threat intelligence, financial fraud, vulnerability and counter terrorism. MISP maintains a database and a github repository [37] storing technical and general information about malware samples, incidents and other relevant information (also including relations between them. Data is stored in structured format and is update by trusted partners.

MISP database contains many threat taxonomies information in machine readable format. On table below CIRCL's own top-level incident classification [27] is presented.

Incident Classification	Description
Spam	Incident involving the reception or the sending of unsolicited emails or any other notification
System compromise	Incident involving the compromise of a computer-based element.
Scan	Incident including any act of network or system reconnaissance that could lead to a security incident. Legitimate security assessment will not be categorized as an incident.
Denial of Service	Incident involving a temporarily disruption of a computer-based element or network service.
Copyright issue	Reported incident including disclosure of information covered by a restrictive copyright. The classification is used for reports which are not classified and handled as a security incident.
Phishing	Incident including attacks posing as legitimate company, organization or people.
Malware	Incident including malicious software or software deliberately designed or abused by an attacker to pursue his goal(s).
XSS	Incident including Cross-Site Scripting vulnerabilities being or potentially being abused.
Vulnerability	A vulnerability reported or discovered that could lead to a security incident.
Fastflux	Incident involving techniques of hiding malicious activities by an ever-changing set of compromised systems.
SQL Injection	Incident involving techniques to directly abuse the backend database (not limited to SQL databases).
Information leak	Incident including disclosure of information where distribution should have been restricted.
Scam	Incident forcing a potential victim to act for the benefit of an attacker.

Table 9 - CIRCL Taxonomy - Schemes of Classification in Incident Response and Detection

MISP database contains complete taxonomies, general and technical and sometimes specialized in specific sectors, like MISP DDos attack taxonomy [25] presented on the table below, a full MISP Information Security Class that is presented in Annex xix , Ms-Caro malware classification[31] that is presented in Annex xii and Open Threat Taxonomy[32], shown in Annex xxiii.

DDos type	Description
Amplification-attack	Amplification attack
Reflected-spoofed-attack	Reflected and Spoofed attack
Slow-read-attack	Slow Read attack
Flooding-attack	Flooding attack
Post-attack	Large POST HTTP attack

Table 10 - MISP DDoS taxonomy

MISP Information Security Class is a 3-level taxonomy of large size and its top-level classes are:

- External malicious threat sources
- Incidents caused by malfunctions, breakdowns or human errors
- Internal deviant behaviours (including usurpation of rights of an identity)
- All categories if incidents
- Existence of abnormal behaviours that could lead to security incidents
- Existence of weaknesses in software that could be exploited and lead to security incidents
- Existence of weakness in the configuration of IT devices that could be exploited and lead to security incidents
- Existence of weaknesses in the IT and physical architecture that could be exploited and lead to security incidents
- Existence of weaknesses in the organization that could be exploited and lead to security incidents
- Impact measurement

Ms-Caro malware classification presents malware type classification, classification by script type and operating systems and a huge list of malware families.

Finally, Open Threat taxonomy is also a large one, containing high level categories, all causing threats to the confidentiality, integrity, or availability of information systems:

- Physical: information systems that are physical in nature
- Resource: incident is caused by lack of resources
- Personal: Failures caused by human personnel, deliberately or accidentally
- Technical: Technical in nature

Each low-level threat also comes with a severity rating.

2.24 CSSA taxonomies

CSSA was founded in November 2014 by seven major German companies as an alliance for jointly facing cyber security challenges in a proactive, fast and effective manner. Contrary to cyber attackers who obviously have an incentive to collaborate, commercial enterprises originally have had little interest in sharing information on attacks and damages with others. This information asymmetry needs to be overcome.

CSSA creates a secure space for a coordinated, efficient and confidential information exchange allowing organizations to benefit from the knowledge of their peers and mutually support and learn from each other. CSSA focuses on sharing and analyzing cyber threat intelligence in a collaborative approach. Objectives are to better detect and understand threats and enhance response actions.

CSSA is open for commercial enterprises with appropriate internal cyber security resources who are willing and capable to actively support CSSA and to share security-related incidents and information with peers. This demands a strong commitment of all members and a very high degree of confidentiality.

Founding members of the association are: Airbus Group, Allianz, BASF, Deutsche Bank, Deutsche Telekom, Henkel and Infineon. Currently, CSSA has 12-member companies. All members contribute the same membership fee and have the same rights.

CSSA taxonomy [26] is included in MISP taxonomies. This taxonomy can be found in Annex xx.

2.25 CSIRT Incident Classification

This classification provides the guidelines needed for Computer Security Incident Response Team (CSIRT) Incident Managers (IM) to classify the case category, criticality level, and sensitivity level for each CSIRT case. This information will be entered into the Incident Tracking System (ITS) when a case is created. Consistent case classification is required for the CSIRT to provide accurate reporting to management on a regular basis. In addition, the classifications will provide CSIRT IM's with proper case handling procedures and will form the basis of SLA's between the CSIRT and other Company departments. [28]

Incident Category	Description
DOS	Denial of service / Distributed Denial of service
forensics	Forensics work
compromised-information	Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property
compromised-asset	Compromised host (root account, Trojan, rootkit), network device, application, user account.
unlawful-activity	Theft / Fraud / Human Safety / Child Porn
internal-hacking	Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware
external-hacking	Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.
malware	A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan.
email	Spoofed email, SPAM, and other email security-related events.
consulting	Security consulting unrelated to any confirmed incident
policy-violation	Violation of various policies

Table 11 - CSIRT Incident Classification

Criticality Classification	Description
1	Incident affecting critical systems or information with potential to be revenue or customer impacting.
2	Incident affecting non-critical systems or information, not revenue or customer impacting. Employee investigations that are time sensitive should typically be classified at this level.
3	Possible incident, non-critical systems. Incident or employee investigations that are not time sensitive. Long-term investigations involving extensive research and/or detailed forensic work.

Table 12 - CSIRT Criticality Classification

Sensitivity Classification	Description
1	Extremely Sensitive
2	Sensitive
3	Not Sensitive

Table 13 - CSIRT Sensitivity Classification

2.26 Europol Incident Class

Europol released a document [41] that aims at describing the common taxonomy for the classification of incidents within the National Network of CSIRTs. In addition to the technical perspective, the document includes the introduction of what Europol refers to as “high level legal characterisation” to facilitate the ontological harmonization of incidents within the Portuguese Network, the international network of CERTs and foreign criminal investigation police forces (Law Enforcement Agencies - LEA) or other similar bodies, such as the INTERPOL and the Europol. The Europol-Incident taxonomy was designed to describe the type of incidents by class. According to Europol’s European Cybercrime Centre, the classification of incidents should be performed along two vectors – “Type of Incident” and “Type of Event”. Under the adopted model for classification of incidents it was further decided to make a division of the various specific Types of incidents by generic Classes, grouping sets of incidents with similar results or goals. Apart from the incident Classes and Types, a group of events linked to each Type of incident was identified. [29]

The Europol Event Taxonomy Table is presented in Annex xxi.

2.27 Sans Institute Malware Classification

Sans institute is an American non-profit organization specialized in cyber security training. On 2008, published a white paper [34] for handling procedures for dealing with different types of malware. On this work, authors emphasized on these types of malicious software and their propagation mechanisms. Moreover, a six step handling method is proposed: *Preparation, Identification, Containment, Eradication, Recovery, Lessons Learnt.*

On this publication authors also present a high level malware clasification seen in table below:

name	Property	examples
Virus	Copies itself to other files; Needs a host file to propagate and execute.	CIH, Virut, Redlof, Autorun.abt, Peacomm, NewHeur_PE
Worm	Exploits the vulnerabilities that are present and can spread over the network.	Code red, Netsky, Stration, Sasser, Bagle, Skipi, no_virus
Logic Bomb	Triggers a specific code on meeting conditions as per the logic written by its author.	Michelangelo
Backdoor	Listens on certain ports so that the attacker can gain access through them later.	Xhaker, sub7, Beast, Ginwui, Rexob, Hupigon
Trojan	Deceptive program that spoofs a harmless or useful program; but, actually stores other malware.	Limbo/NetHell, Pidief, ZeuS/PRG, Banker.bdn, PGPCoder, Torpig, Gozi
Spyware	Software used to spy on victim's activities and also used to steal sensitive information.	WhenUSave, PuritySCAN Virtumonde, SecurityToolbar
Rootkit	Set of programs that alter the OS functionality to hide themselves.	LRK, AFX, SInAR, Rustock, Mebroot
Bot / Botnet	Program that do the work on behalf of its master. A master may control millions of such bots and can use them for malicious purposes.	Agobot, Slackbot, Mytob, Rbot, SdBot, poebot, IRCBot, VanBot, Mpack, Storm

Table 14 – Sans Institute Malware Classification

Moreover, they categorize viruses based on different categories[35] to describe them:

- Memory based
  This classification describes the way viruses operate in memory. There are viruses that stay in memory as much as possible or temporarily, or not at all. Furthermore, they can be at user level process or process in the kernel.
- Target based
  This refers to how the virus spreads and the target it attacks. Main categories of this distinction are *Compiled*, *Interpreted* and *Multipartite.* Compiled viruses are tranformed to machine executable instructions, Interpreted ones's code is executed by an application. Last, Multipartite viruses implicate a variety of mechanisms to attack the host like infecting the boot sector or application documents and then spreading.
- Obfuscation tehnique based
  This classification is based on the technique viruses use to hide from detection and analysis. There are several sub categories, including *Encryption*, *Tunelling, No obfuscation, Oligomorphism, Metamorphisms, Stealth, Armoring, Retro.*
- Payload based
  This refers to the result of the infection. Some viruses may not carry anything more that its code, whereas other contain a message or graphic which does not extend the harm, others could destroy or corrupt files and partitions metadata. The paylod based sub category most virus belong to according to authors is *Droppers*, which help the attackers gain access to victims' personal data and therefore obtain financial gain or damage the functionality of an organization. Examples of the last sub category include: *Identity Theft, DDos, Phishing, Software Licence Theft* etc.

Full Sans Institute Categorization is presented on figure below and in Annex xxiv.

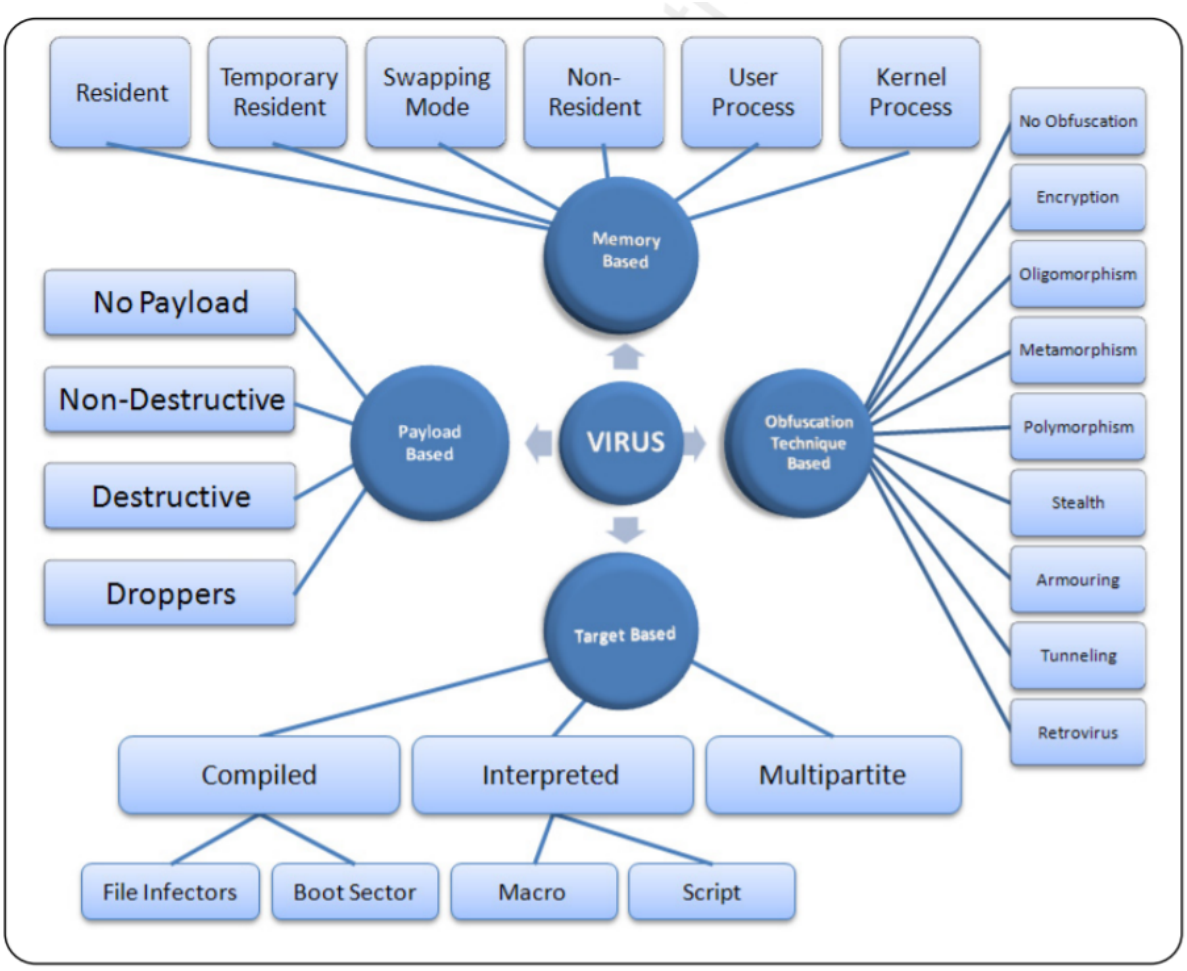

Figure 5 - Sans Institute Malware Classification

2.28 Taxonomies Comparison

As stated on the introduction, there are many ways to classify threats and many taxonomies and threat catalogues have been developed. Some of them are universally recognized, standardized and available to download, use or contribute and some are based on specific team's experiences in handling incidents and serve specific purposes. Moreover, a number of methodologies presented on previous sections may also include defense mechanisms or countermeasures mapped to the attack taxonomies.

The taxonomies analyzed vary on size, scope content, definition of a threat and their target entities. Some contain more than 500 threats, others just use a small set of classes that are employed in use cases. Some are suitable for security professionals while others are more valid for Academia. Moreover, some contain **technical** terms while the rest are more general and easier to be understood by non-security experts. For instance, *WASC, CAPEC, Ddos Taxonomy, ESCORTS, VERIS and* some others include at least some terms that may not be interpreted easily by common people or are technical abbreviations. Examples include: "Ext customer" (*VERIS*), "LDAP injection" (*WASC, CAPEC*).

On this section we are comparing the above taxonomies based on several attributes that have been presented on [6,17,35]. Some of the concepts, like simple top-level taxonomy, mutually exclusive categories, threat ranking, and others like ease of use are considered by ENISA and various CSIRTs [35] to be good practices. A taxonomy that is to be used in daily and correct basis and correctly should contain a large semantic vocabulary, at least all needed in operational requirements, which can be enriched by terms learned by national and international standards and other CSIRTs collaboration. Agreed practices may lead to simplicity, since it becomes easier then to export a taxonomy to others, because of the similarity of the general terms. The criteria are:

- *Ontology (multi dimensional):* An ontology is a tool for knowledge representation as a set of concepts. Compared to taxonomies, [35] ontologies are considered as 3-dimensional and, although not always being very clear, they cannot be represented as single table. A simple taxonomy is like a tree while an ontology resembles a forest. When a taxonomy is in form of ontology, this 3rd dimension is usually "the relationship between concepts". So, the difference between a taxonomy and an ontology can be described with this paradigm [35]: "a taxonomy will define the relation between a child and his parents where an ontology will also define the marriage relation between a child of a family and another child from a distinct family.". In our case, additional contextual dimensions [44] might be: a threat agent causing the threat and the threat leading to an attack on system assets.
- *Sector oriented:* Some taxonomies cover the best part of cyber threats whereas others focus on specific sectors of security or specific threat type. For example, Cloud services, Web sites. Furthermore, some taxonomies may focus on specific class of threats like Denial of Service Attacks or Viruses

- *Ranking threats – Performance Measurement in solving a problem*: This attribute refers to the existence of any kind of degree of threat severity in the taxonomy or the measuring the time an incident takes to close. The latter has been referenced by many CSIRT's and it is considered to be a good practice by ENISA [35]. Pre-estimated time for a threat improves the allocation of the security resources and keeping statistics.
- *Simple top-level taxonomy*: Simple top-level categorization is relevant to the complexity of the taxonomy but also implies that there might more than one level of categorization [35]. With a multi-level categorization system, the preferred level of complexity can easily be selected. If a non-technical report is required, a higher and more general categorization level can be used. If a technical report is required, then using the bottom level category enables that. Defining simple top-level categories helps selecting the preferred level of complexity for a taxonomy, so general and more technical reports can easily be deployed. Top level categories are easier to interpret whereas bottom ones may be more adequate for technical reports.
- *Hierarchical:* This distinction is closely connected to the precious one. This means that categories occur from other categories in the form of a tree. As stated in [35] "A taxonomy with at least 2-3 levels of categorization provides the most versatility and scalability, as it gives the choice of adding a branch to a tree or adding a leaf to the branch." [35].
- *Mutually exclusive categories:* An issue that has been reported by many CSIRTS is the mutual exclusivity of threat categories. It is considered good practice [35], especially if machine reading and classification is used, to define strict taxonomy terms and constraints in order to avoid categorizing an incident to two or more different classes by different analysts. Sometimes this cannot be avoided, and an incident may change categories during the handling cycle. This leads to ambiguous reports which cannot be interpreted and combined appropriately.
- *Machine Readable:* As an incident can be treated by both humans and machines [35], it is helpful for a taxonomy to be provided in both human readable and machine-readable format (json, xml etc). Using the contents of the MISP database or if stated in literature, we identify if a taxonomy comes in a machine-readable format.
- *Size (of semantic vocabulary):* Semantic vocabulary describes knowledge and information assets. In literature, some taxonomies that are considered popular may define the limits [35] and comparing to these one can consider if a taxonomy is large, medium or small.
- *Contains physical threats:* There is a distinction between taxonomies that contain at least some physical threat categories, compared to these that contain only cyber.

Methodology	Ontology (multi dimentional)	Sector oriented	Ranking threats-Performance Measurement in problem solving	Simple top level taxonomy	Machine readable	Mutually exclusive categories	Size (of semantic vocabulary)	Hierarchical	Contains physical threats
ENISA	No	No	*No*	Yes	Yes	Yes	Large	Yes	Yes
WASC	No	Yes – Web Sites	No	No	No	Yes	Medium	No	No
CAPEC	No	No	No	Yes	Yes	Yes	Large	Yes	No
ISO 28001:2007	Yes	Yes - Supply Chain	No	Yes	No	No	Medium	No	Yes
IT Grundsutz	No	No	No	Yes	No	No	Medium	No	Yes
CYSM	Yes	Yes – Port Security	No	Yes	No	Yes	Large	Yes	Yes
Forward whitebook	No	No	No	Yes	No	No	Medium	Yes	No
A Taxonomy of DDoS Attack and DDoS Defense Mechanisms Jelena Mircovic (*Ddos Taxonomy)*	Yes	Yes – Ddos attacks	*Yes*	No	No	No	Medium	No	No
Nist Guide for conducting Risk Assesment	No	No	*No*	Yes	No	No	Medium	No	Yes
eCSIRT.net Incident Classification	No	No	No	Yes	Yes	Yes	Medium	Yes	No
Proposed top level classification of incidents (by Andrew Cormack)	No	No	No	Yes	No	Yes	Small	No	No
Incident Taxonomy by Cesnet ARchive	*Yes- In MISP database*	No	No	Yes	No	Yes	Small	No	No

Methodology	Ontology (multi dimentional)	Sector oriented	Ranking threats- Performance Measurement in problem solving	Simple top level taxonomy	Machine readable	Mutually exclusive categories	Size (of semantic vocabulary)	Hierarchical	Contains physical threats
Incident Taxonomy by CERT NIC.LV	No	No	No	Yes	No	Yes	Small	No	No
A Taxonomy of Operational Cyber Security Risks (Software Engineering Institute)	No	No	No	Yes	No	Yes	Medium	Yes	Yes
Escorts Project	*No*	Yes – SCADA systems	No	Yes	No	Yes	Small	No	No
Veris taxonomy	*Yes*	No	No	Yes	Yes	Yes	Medium	No	No
OWASP - Threat Categories	*No*	No	No	Yes	No	Yes	Large	No	No
OWASP – Stride Threat Model	*No*	No	No	Yes	No	Yes	Small	No	No
HP Tipping Point Event Taxonomy V 2.2	*No*	Yes - SMS Web services	No	Yes	Yes	Yes	Medium	Yes	No
Threat Taxonomy for Cloud of Things	*No*	Yes- Cloud services	No	Yes	No	Yes	Medium	Yes	No
A Multidimension Taxonomy of Insider Threats in Cloud Computing	*Yes*	Yes- Cloud services	No	Yes	No	No	Small	Yes	No
A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks (Semantic Social Engineering)	Yes	Yes - Social Engineering	No	Yes	No	No	Medium	No	No
VoIP Security and Privacy Threat Taxonomy	*No*	Yes - VoIP	*No*	Yes	*No*	Yes	Medium	Yes	No

Methodology	Ontology (multi dimentional)	Sector oriented	Ranking threats- Performance Measurement in problem solving	Simple top level taxonomy	Machine readable	Mutually exclusive categories	Size (of semantic vocabulary)	Hierarchical	Contains physical threats
Circl taxonomies	*No*	No	No	Yes	*Yes*	Yes	Small	No	No
Circl - Misp - Information Security Indicators Class	*Yes- In MISP database*	No	No	Yes	Yes	Yes	Medium	Yes	No
Circl - Misp - MS-Caro Malware Classification	*Yes- In MISP database*	No	No	Yes	Yes	Yes	Medium	No	No
Circl - Misp - MS-Caro malware families	*Yes- In MISP database*	Yes	No	Yes	Yes	Yes	Large	No	No
Cssa taxonomies	*Yes- In MISP database*	No	No	Yes	Yes	Yes	Small	No	No
Csirt Incident Classification	*Yes*	No	*Yes*	Yes	Yes	Yes	Small	No	No
Europol - Incident Class	*Yes- In MISP database*	No	No	Yes	Yes	Yes	Medium	Yes	No
Sans Institute	*No*	Yes - Viruses	No	Yes	No	Yes	Medium	Yes	No

Table 15 - Taxonomies Comparison

On table above all the taxonomies are mapped to the previously mentioned attributes. Value of “Yes” indicates that the taxonomy in line fullfils the concept of the attribute. In some cases, there is an explanatory text or a scale indicator.

Several taxonomies are in form of **Ontology or contain multiple dimensions**. *ISO 28001 and CYSM* in a way form an ontologies such they relate assets to threats (and countermeasures) using the scenarios. Relationship between concepts also exists on *Taxonomy of DDoS Attack,* including defense mechanisms to the attack categories. On *Semantic Social Engineering* each typical attack is mapped to specific categories and attributes. *Veris* is multi dimensional providing several attributes that describe incidents and are connected to each other, like actor, victim and action. Multidimensional is also the taxonomy of *Insiders Threats in Cloud Computing,* applying different concepts like availability, confidentiality and integrity to cloud threat categories. MISP taconomies here

presented are in mostly in form of a table but their whole structure in MISP database are in form of ontology. For example, using an equal or similarily mapped namespace for representing a threat category that represents the same kind of threat in different taxonomies enhances the concept of an ontology.

Some of the taxonomies are aimed for **specific sectors**. *ISO 28001* focuses on security systems for the supply chain. *WASC* refers to the threats that web sites face whereas *Hp Tipping Event Point* taxonomy is concerned with SMS Web services. *Semantic Social Engineering* explains threats in Social Engineering and while *Threat Taxonomies for Cloud* and *A Multidimension Taxonomy of Insider Threats in Cloud Computing* present categorization of threats that are common in Cloud services. *VoIP Security and Privacy Threat Taxonomy* defines the potential threats to VoIP deployments. Last, *Escorts categorizes* threats based on dangers that SCADA systems face.

Moreover, taxonomies analyzed may focus on **specific class of threats**. For example, A Taxonomy *of DDoS Attack and DDoS Defense Mechanisms,* describes threats (and defense strategies) related to DDos attacks (which are also described in MISP taxonomies), whether *Sans Institute* mainly analyzes Virus categories and sub categories.

On the table below, we have collected all the taxonomies and indicated the number of their first level categories, the total threats that are mentioned and the maximum level of hierarchy that their models are built on. Moreover, since many of them categorize threats by different aspects, the figures are presented based on this specific assect. For example, *CAPEC taxonomy* is modeled “by mechanisms of attack” and “by domains of attack”. This distinction is not always clear, since a top-level category may sometimes be interpreted as a different categorization as in *WASC,* which provides only two high level categories, attacks and weaknesses with many threats belonging to those.
It would also be worth to take into account into a hierarchical taxconomy that if a category does not contain threats (while others of the same level may do), this category is also considered a threat in the context of total threats count.

Methodology	Different Categorization by	1st level categories	Total threats	Maximum level of hierarchy
ENISA		8	184	2
WASC		2	45	1
CAPEC	Mechanisms of Attack	9	~500	4
	Domains of Attack	6	38	1
ISO 28001:2007		5	32	2
IT Grundsutz		45	45	0
CYSM		6	~1300	2
Forward-whitebook		8	28	1
A Taxonomy of DDoS Attack and DDoS Defense Mechanisms Jelena Mircovic (Ddos Taxonomy)	Degree of automation	3	16	1
	Exploited weakness	2	2	0
	Source address validity	2	7	1
	Attack rate dynamics	2	3	1
	Possibility of characterization	2	3	1
	Persistense of agent set	2	2	0
	Victim type	5	5	0
	Impact on victim	2	4	1
Nist Guide for conducting Risk Assesment		4	34	2
eCSIRT.net Incident Classification		8	27	1
Proposed top level classification of incidents (by Andrew Cormack)		11	11	0

Methodology	Different Categorization by	1st level categories	Total threats	Maximum level of hierarchy
Incident Taxonomy by Cesnet ARchive		11	11	0
Incident Taxonomy by CERT NIC.LV		10	10	0
A Taxonomy of Operational Cyber Security Risks (Software Engineering Institute)		4	57	2
Escorts Project	Scada vulnerabilities	4	6	1
	Attack Scenarios	3	12	1
Veris taxonomy	Discovery method	29	29	0
	Hacking variety	47	47	0
OWASP - Threat Categories		10	116	1
OWASP - Stride Threat Model		6	6	0
HP Tipping Point Event Taxonomy V 2.2		8	40	1
Threat Taxonomy for Cloud of Things		2	33	2
A Multidimension Taxonomy of Insider Threats in Cloud Computing		3	12	5
A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks (Semantic Social Engineering)		30	30	0
VoIP Security and Privacy Threat Taxonomy		6	86	3
Circl taxonomies		13	13	0
Circl - Misp - Information Security Indicators Class		10	98	2
Circl - Misp - MS-Caro Malware Classification		35	35	0
Circl - Misp - MS-Caro malware families		457	457	0

Methodology	Different Categorization by	1st level categories	Total threats	Maximum level of hierarchy
Cssa taxonomies	Sharing Class	3	3	0
	Origin	7	7	0
Csirt Incident Classification		11	11	0
Europol Incident Class		46	46	0
Sans Institute	Malware type	8	8	1
	Virus type	4	32	3

Table 16 - Taxonomies' figures

ENISA, OWASP Threat Categories, CAPEC, Forward and MISP taxonomies include adequate size of a tested in real conditions semantic vocabulary but also seem to keep up with the national and international standards and other Csirts. Rest of the taxonomies listed here either use example threat categorizations or are focused on a specific sector.

Most taxonomies analyzed maintain a **simplicity in selecting high level categories,** which as mentioned before helps integration and comparison with other categorizations. For example, *ENISA and CAPEC (*categorizing both by have a few, clear, mutual exlusive, easy to interpret top level categories and multiple subcategories in two extra levels which suit both technical and non-technical reports. On the other hand, *WASC* only has two high level categories*,* attacks and weaknesses and mupltiple subcategories, making it harder to map to categories of other taxonomies, or create a report based on them.

Taxonomies with a small number of top level categories (e.g. *NIST, OCTAVE, EUROPOL*) also tend to weaken the **mutual exclusivity** of the categories. Furthermore, in cases where threat scenarios are included (e.g. *ISO 20081*) it is possible that a part of them will partially belong to more that one categories.

In general, most taxonomies that have been considered complete (with the addition of *eCSIRT*) maintain a **hierarchical schema** with levels of categorization varying from 1 to 5 (*A Multidimension Taxonomy of Insider Threats in Cloud Computing* is the taxonomy with 5 levels of categorization*)*. Although it would be rather subjective to consider **large or small** a taxonomy by its categories and other attributes presented, an effort has been made and presented on this comparison table. The characterization is based on the number of threats or the final level of each hierarchy: 1-20 is considered small, 21-100 medium and 101+ large. *ENISA, CYSM, CAPEC* and *MISP MS-Caro* taxonomies contain the largest size of semantic vocabulary.

A number of the taxonomies include a **degree of severity for threats**. *MISP Information Security Indicators Class* contains a high-level category with impact measurement on security incidents divided on monetary cost and website down time, *while Open Threat Taxonomy* includes a severity rating for each low-level threat. Furthermore, *CSIRT* contains a special categorization by criticality and sensitivity, which mostly refers to the system or information affected. ENISA includes whether its trend is increasing or decreasing or nothing. *CAPEC* does not include a degree of severity, although MITRE had published a "Common Weakness Scoring System[7]. Last, *Ddos Taxonomy* offers a classification based on the impact on the victim.

Apart from being understood by human experts, some of the taxonomies come with a **machine-readable format (**pdf, docx, jpg are not considered machine readable). *MISP* is a project that maintains a database and a Github repository where trusted partners can upload their taxonomies in machine readable format and download/export other taxonomies. On the comparison table we have indicated those taxonomies that are known to be available in machine readable format (e.g *CAPEC* can be downloaded in CSV or XML format) or are included on MISP database.

Last, most of the taxonomies analyzed in this paper cover **only cyber attacks**. The rest however include classes like "Fire", "physical attack" etc. *ENISA* contains a whole class with subclasses like Theft, Sabotage and Terrorist Attack. *ISO 28001,* focusing on the supply chain, describes threats related to infrastructures, goods and personnel. *IT Grundsutz* taxonomy contains a variety of physical threats including Fire, Unfavorable Climatic Conditions, Water and others. Environmental threats are also a class in *NIST* taxonomy, focusing though on the unavailability the cause to the systems. *Software Engineering Institute* proposes a threat category of External Events, which are divided to Hazards, Legal Issues, Business Issues and Service Dependencies. Last, *CYSM* also dedicates a top-level category to physical threats (Earthquake, flood, hurricane etc.)

[7] https://cwe.mitre.org/cwss/cwss_v1.0.1.html

3 Threat scenarios based on real cases

This Section describes some threat scenarios based on real cases in the maritime sector. Only few incidents were reported to the public, so the information available on this topic is scarce.

For several years now, the logistics sector has continuously been subject of several millions of IT based attacks (cyber-attacks) in many ways and with many purposes and targets. Traditionally, theft of goods, use of transport as a means of smuggling, or even theft of information (documents), has been made in physical form. Alarms were disconnected by physical manipulation of them, or data were stolen by using a floppy disc directly on the computer where the information was stored, for example. Today it is possible to manipulate physical systems (cameras, alarms, valves, CPUs, Operating Systems, etc.) without being present, and without having to physically access them. The interconnection of many of these systems, including databases and information repositories, to different networks, opens *an a priori* very vulnerable pathway for access, manipulation, destruction or subtraction of any tangible or non-tangible asset of the entity attacked.

Besides usual virus and malware that travel randomly in the Internet, ports, at nodes of the supply chain, are also subject to cyber attacks, usually initiated by different kind of groups, on an almost regular basis. These groups are mainly:

- Criminals
- Terrorists
- “Hacktivists”
- Corporate espionage

Criminals pursue to make money by performing different illegal actions using cyber attacks as a mean: drug/weapons/fake items smuggling, cargo theft, data ransom fee request, etc. They mainly use containers as the mean to perform their illegal actions, so they need access to certain information on the container’s contents, destination, location, etc. They also may bribe or cheat truck drivers to get access to these containers and even study their habits like regular routes and stops. The information that criminals get is used to identify the most vulnerable points in the supply chain and thus to increase the success of their physical attacks.

Terrorists objectives are usually like criminals’ ones when referring to making money, but their last objective is (geo)political or even religious. Terrorists may use cyber-attacks to smuggle weapons or even military uniforms, to encrypt sensitive data and ask for a ransom fee (using ransomware), etc.

Hacktivists usually perform their actions to demonstrate their abilities in finding and exploiting vulnerabilities, but they also can be motivated by personal, political or social convictions. They usually look for a “bombshell”, an action that could lead to major disturbances in the supply chain.

Corporate spies also use cyber-attacks to steal sensitive data/information. They are motivated by business competition. A typical case consists of stealing private data and financial information of a company’s customers.

3.1 Statistics on Cyber-attacks

Reliable and accurate statistics on cyber-attacks performed in the logistic chain are truly difficult to obtain due the high secrecy with regards these events in big companies. No one wants to force their hand and show their weaknesess. It is not good for the business. Anyway, this section tries to compile general statistics on different kind of cyber-attacks (including data breaches) performed in different sectors (including logistics and transportation) and to show the trends on cyber-attacks for the near future. The main sources of information have been the Symatec's Internet Security Threat Report [46] and the Lloyd's report "Facing the cyber-risk challenge" [47], both referring 2016 andprevious years (the most recent reports found available).

3.1.1 General figures

According to the surveys performed by Lloyd's, which involved 350 large European companies with interviews addressed to top management, the 92% of the companies considered have suffered a data breach in the past 5 years. With regards internal and external threats, hacking for financial gain has been the most frequent in Europe, and specifically in UK, France, Germany, Italy amd Norway, while in The Netherlands it was hacking for political motivations, in Spain Physical loss of paper or non-electronic devices or Malware in Sweden:

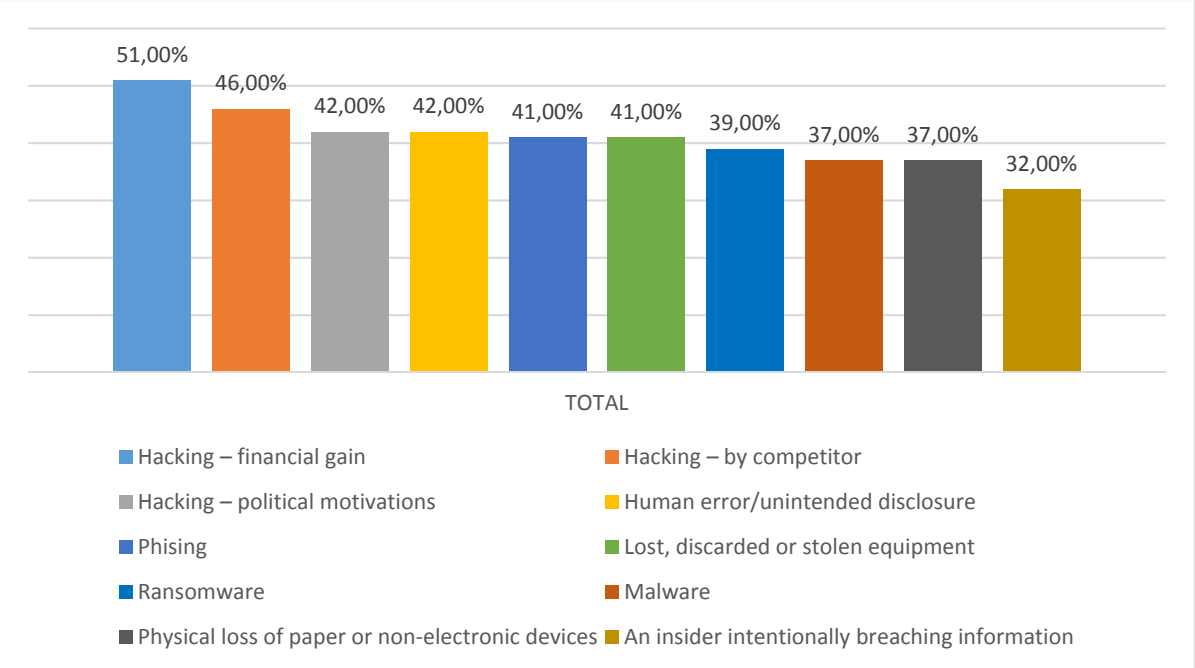

Figure 6 – Internal and external threats in Europe 2016. Source: Lloyd's cyber-risk report

According to Symantec report, other general figures with regards cyber-attacks in the last years are:

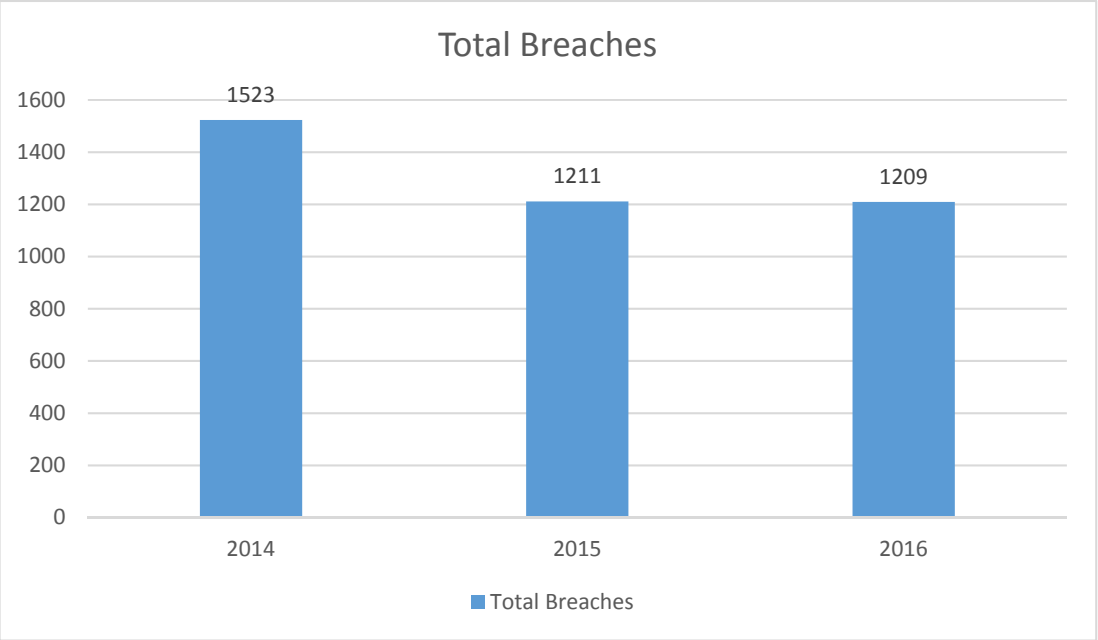

Figure 7 – Total data breaches in the world. Source: Symantec ISTR 2016

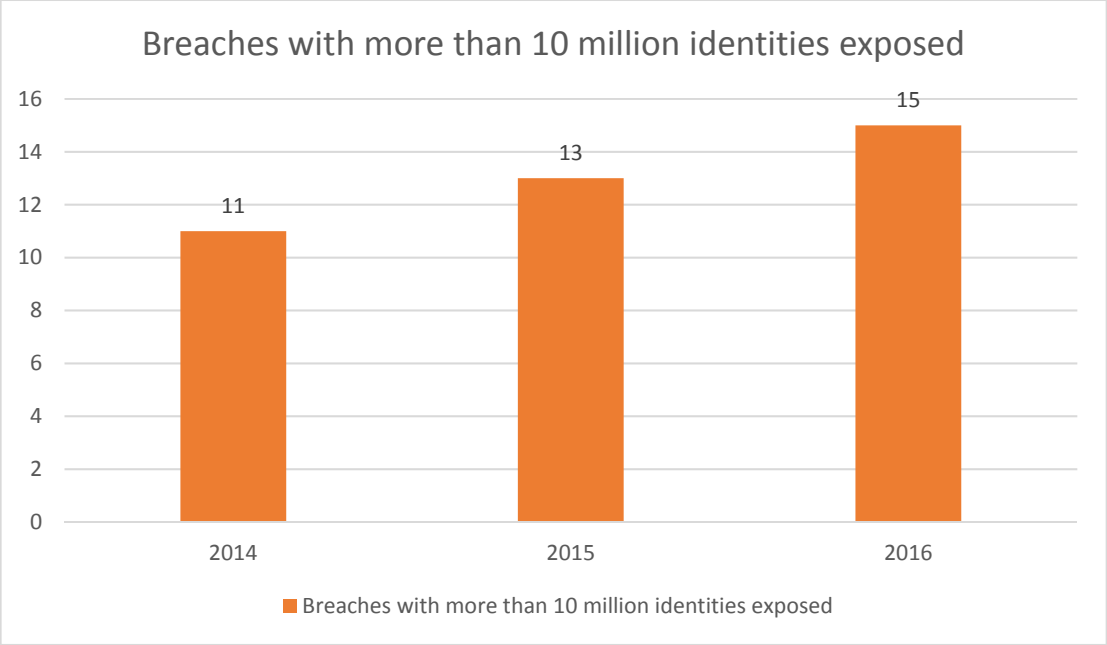

Figure 8 – Data breaches with more than 10 M identities exposed. Source: Symantec ISTR 2016

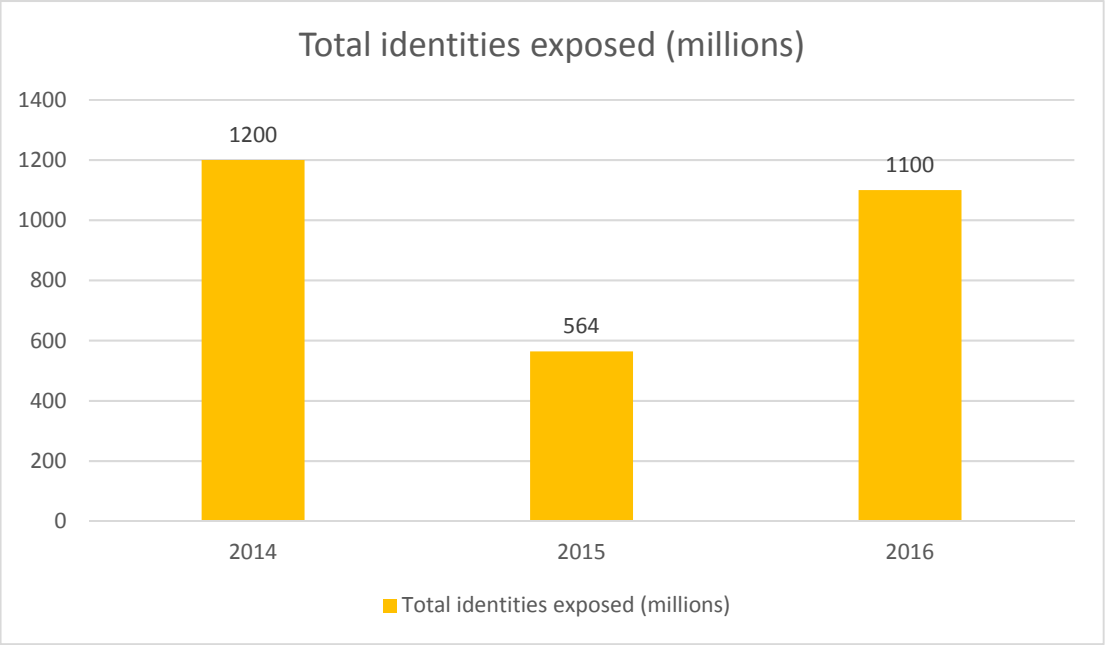

Figure 9 – Total identities exposed in the world. Source: Symantec ISTR 2016

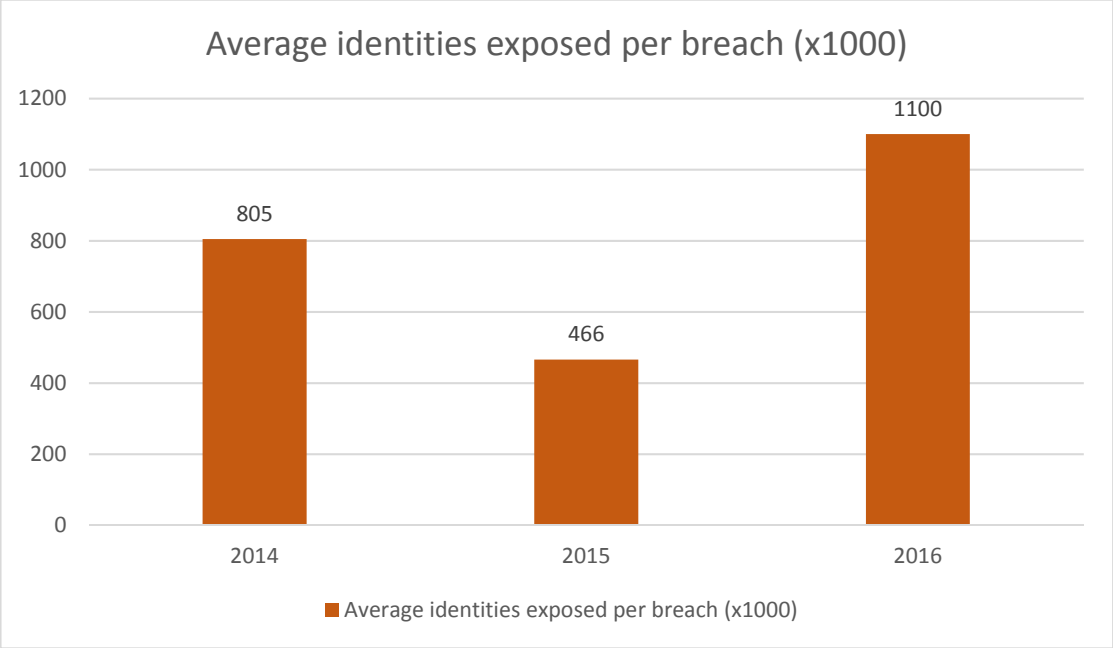

Figure 10 – Average identities exposed per breach in the world. Source: Symantec ISTR 2016

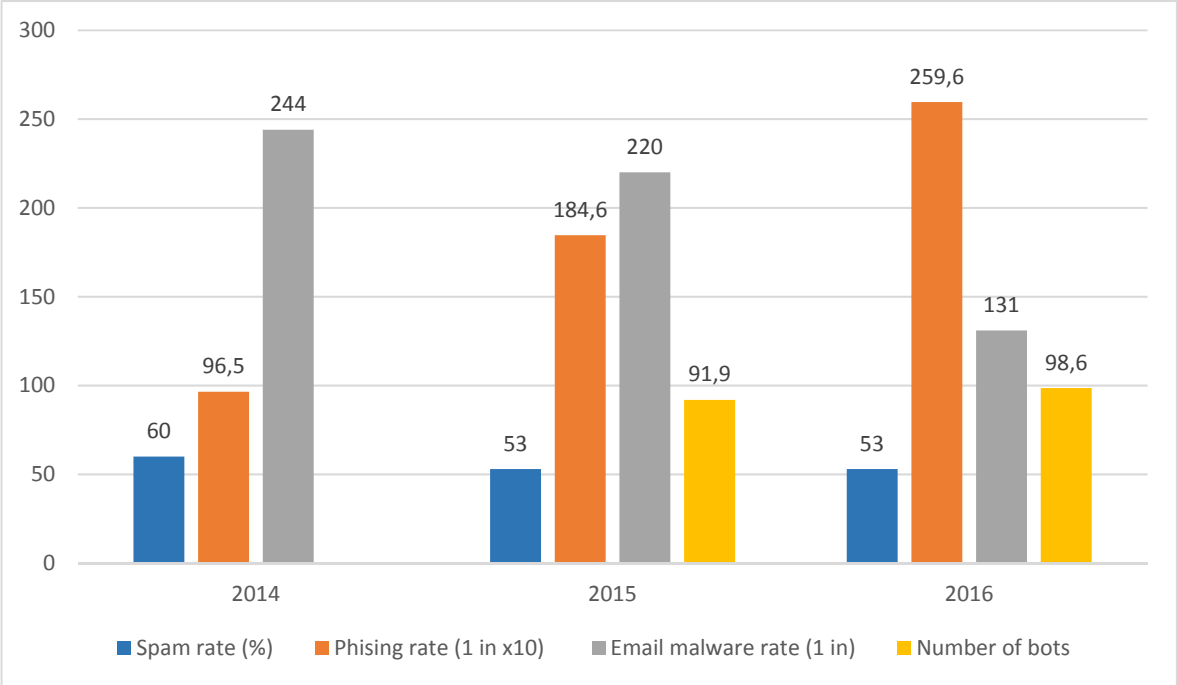

Figure 11 – Email threats, malware and bots. Source: Symantec ISTR 2016

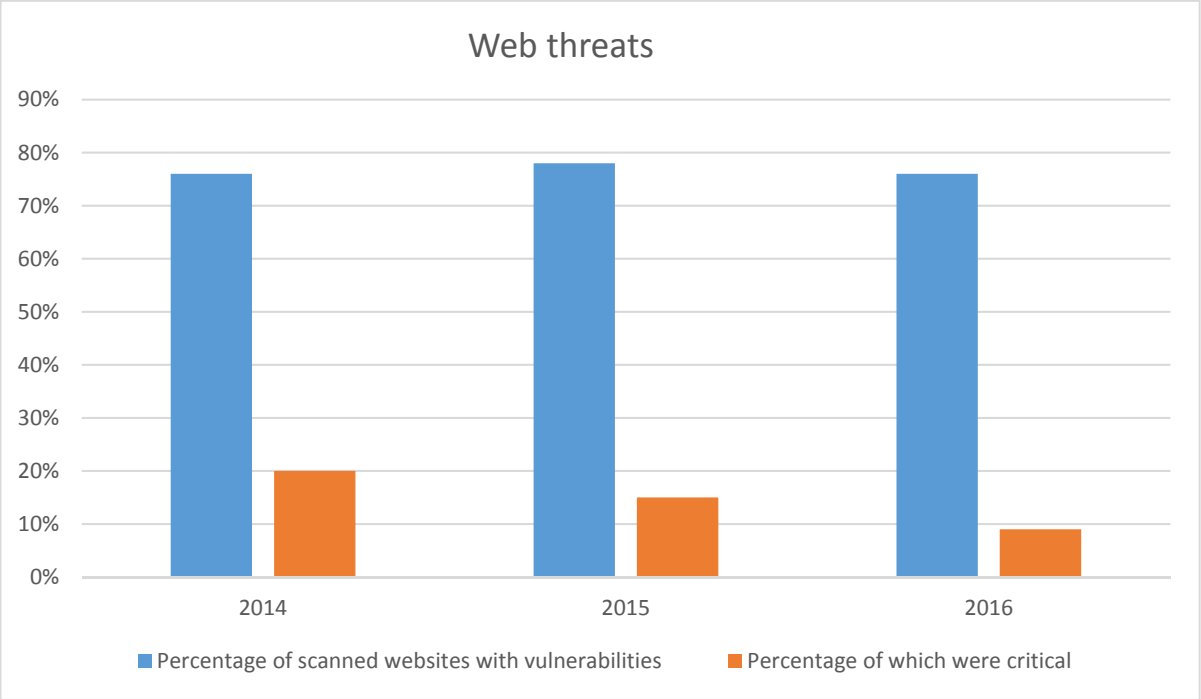

Figure 12 – Vulnerable websites scanned by Symantec. Source: Symantec ISTR 2016

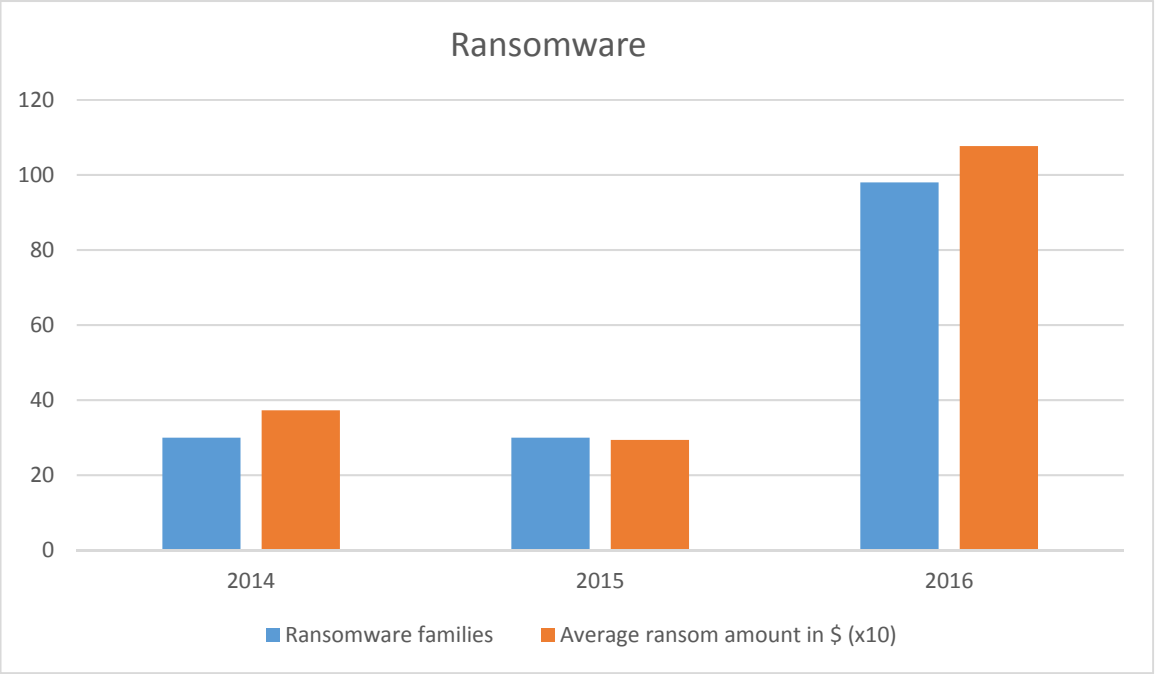

Figure 13 – Ransomware threats. Source: Symantec ISTR 2016

Next sections show general figures on cyber-attacks taken from the 2016 Symantec report.

3.1.2 E-mail attacks

This kind of attacks consists mainly of malware attached to e-mails (53% of the e-mails are spam, many of them containing malware, according to Symantec). Other kind of attack is phishing. It is noticeable that by sector, transportation and public utilities is the sector suffering the higher phising rate:

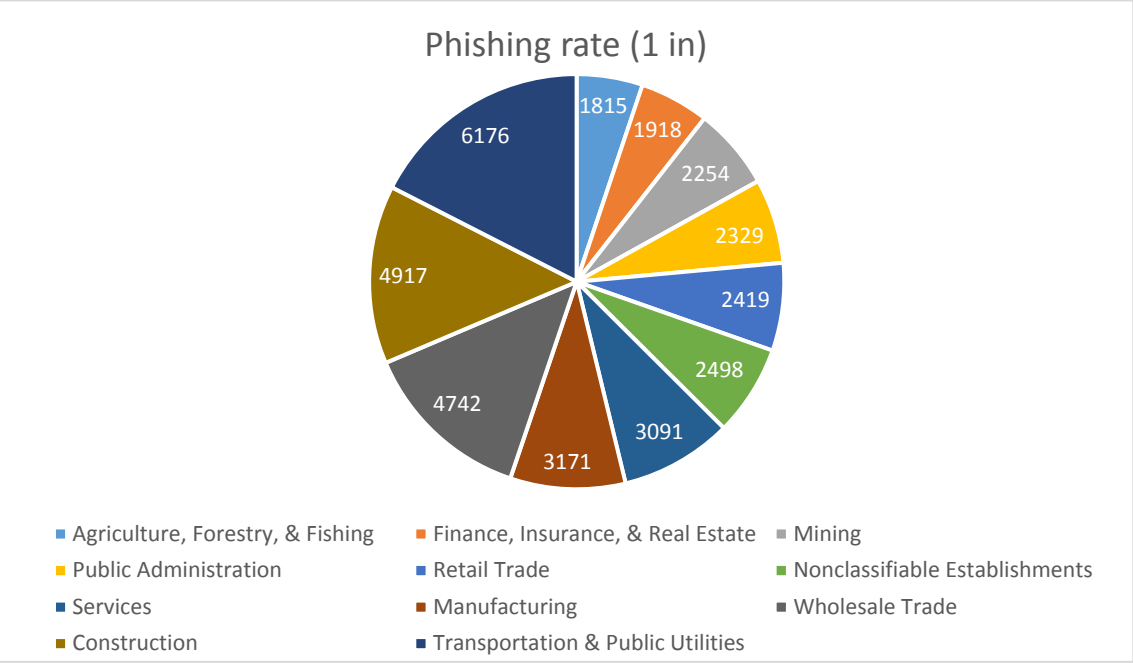

Figure 14 – Phishing rate. Source: Symantec ISTR 2016

Among the most used ways of phising there is the BEC attacks (Business Email Coprimise), also known as CEO fraud. BEC scams are a form of low-tech financial fraud where spoofed emails are sent to financial staff by scammers pretending to be the CEO or senior management. Symantec research in the first half of 2016 found that more than 400 businesses are targeted by BEC scams every day, with small- and medium-sized businesses the most targeted.

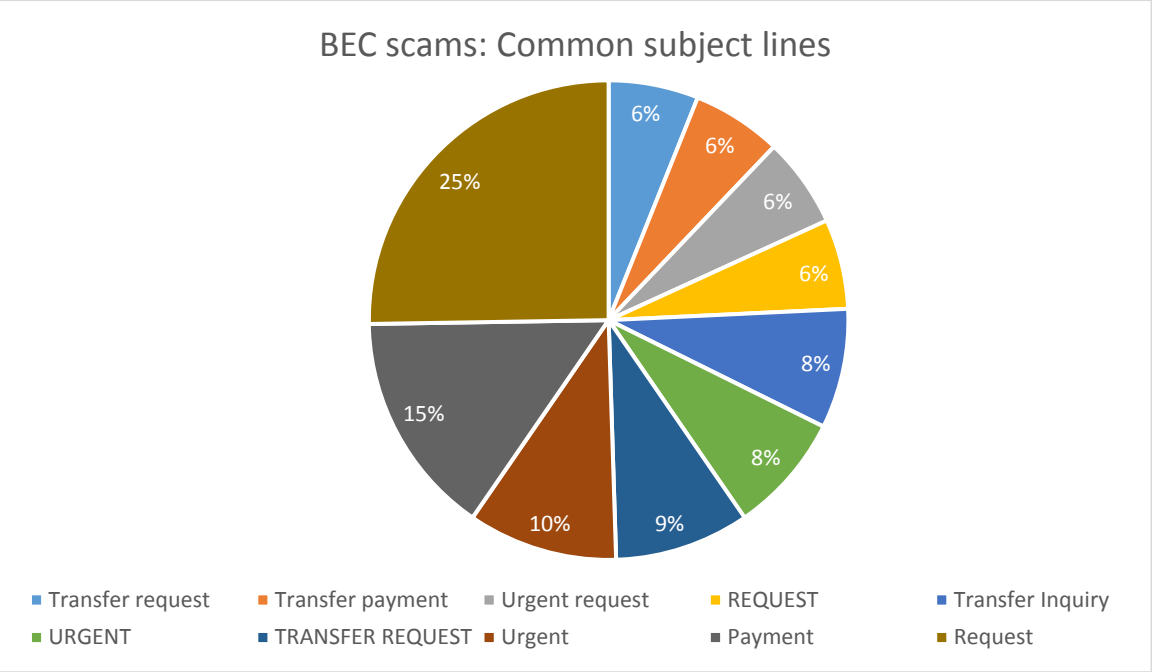

Figure 15 – BEC scams. Source: Symantec ISTR 2016

“Request” was the most popular keyword used in subject lines for BEC scam emails. It was followd by Payment (15%) and Urgent (10%).

As per spam e-mails rate by industry, the most hit one is construction, being transportation in eighth position, together with Finance, Insurance and Real Estate:

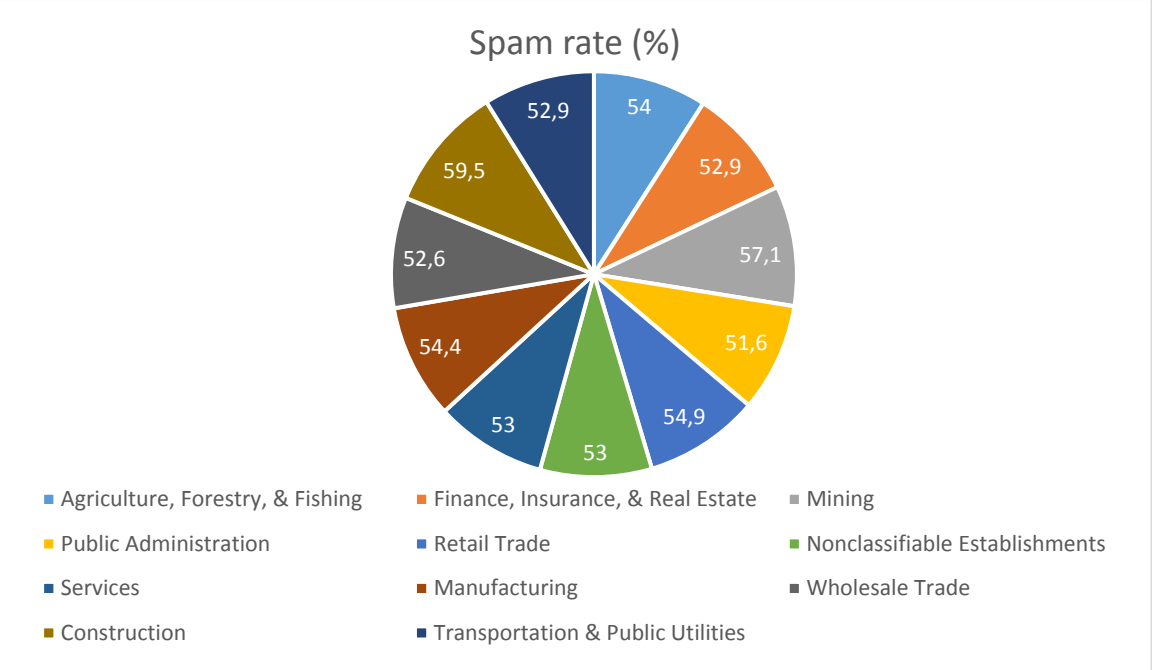

Figure 16 – Spam rate. Source: Symantec ISTR 2016

Other interesting figures with regards spam e-mails are the top ten subject line keywords seen in major malware campaigns in 2016. Invoice was the most used word, followed by Document (13%) and Scan (12%).

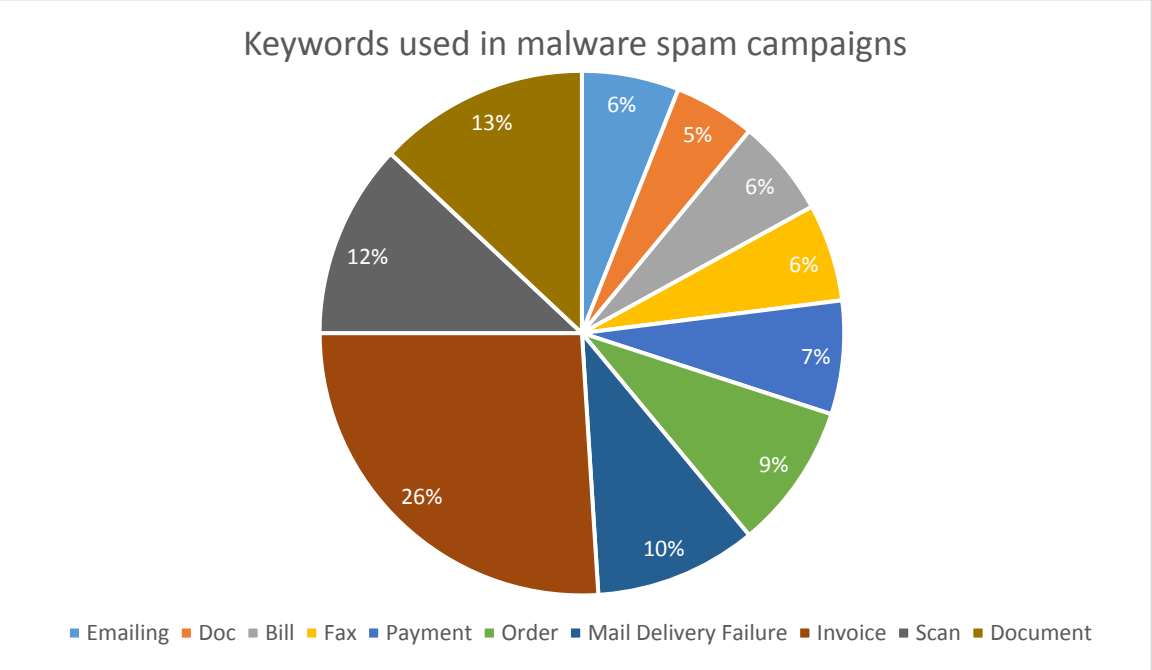

Figure 17 – Keywords in malware campaigns. Source: Symantec ISTR 2016

Finally, English is the preferred language used in spam campaigns (89% of the total), in the subject line.

3.1.3 Web attacks

Despite web-attacks by means kit explots have dropped by a third year-on-year, this kind of attacks are still a big problem, with an average of more than 229.000 being detected per day (according to Symantec) in 2016. More than 76% of the analysed websites contained vulnerabilities, 9% of which were deemed critical. Despite the percentage of vulnerabilities in websites have remained almost constant during the last years, the percentage of critical vulnerabilities fell steadily in the last three years (from 2014) from 20% up to the present 9%.

With regards the top 10 exploit kits, the Angler explot kit was the most common one during 2016 (22% of the total exploit kits). However, this exploit was almost inexistent at the end of 2016, being replaced by th RIG exploit kit, responsible of almost the 35% of attacks in december 2016.

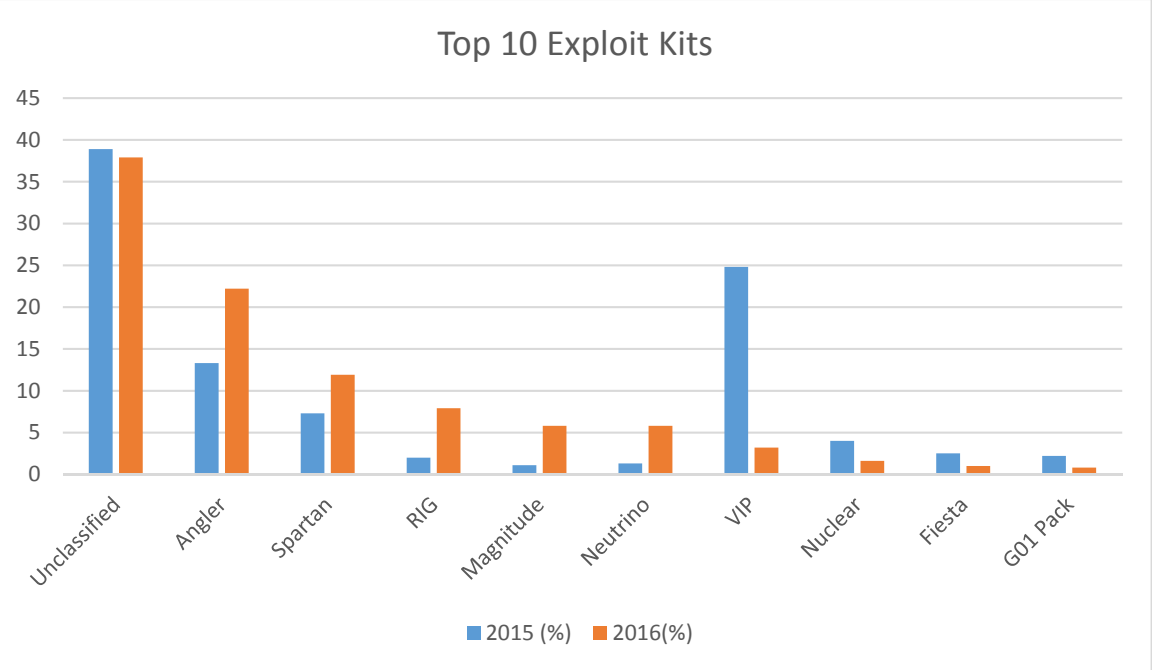

Figure 18 – Top 10 exploit kits. Source: Symantec ISTR 2016

Overall, web attacks dropped more than 30% between 2015 and 2016. This is explained by attackers moving to email as the primary infection vector. Despite the general drop in web threat activity, it remains a major threat with Symantec blocking an average of 229.000 unique web attacks on end point computers daily (as stated before) in 2016.

The most frequently exploited websites according to their classification is shown in the next chart:

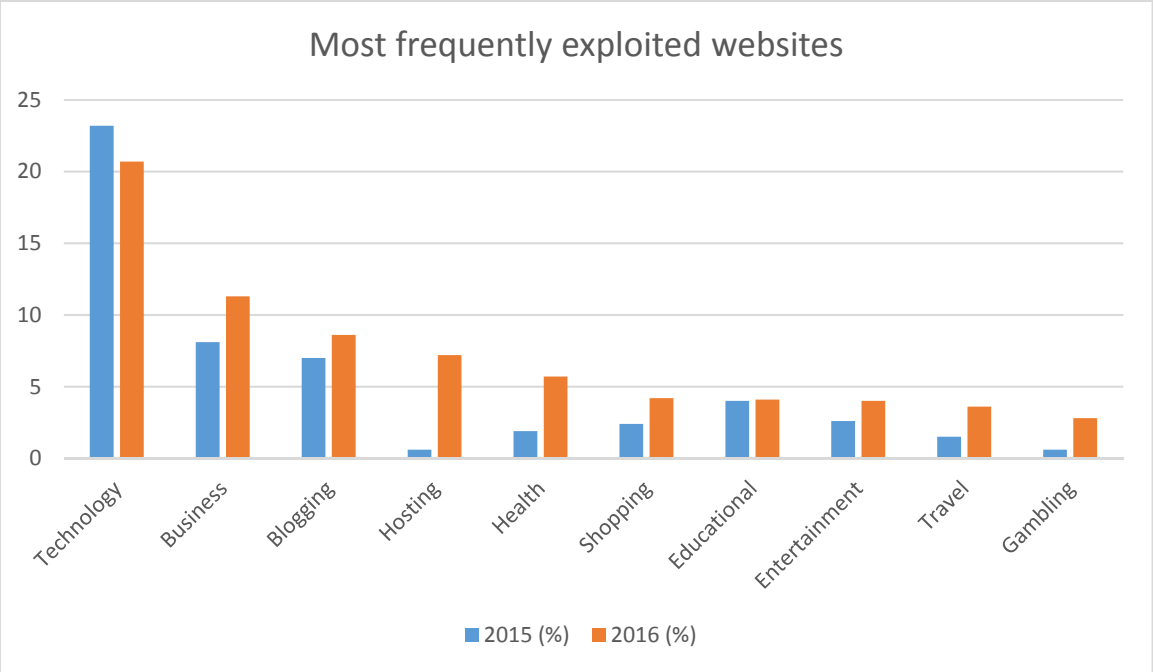

Figure 19 – Most frequently exploited websites. Source: Symantec ISTR 2016

Technology- and business-related websites were the most frequently exploited website categories in 2016. Technology websites were exploited nearly twice as much as business-related websites. Search, which was the third-most frequently exploited category in 2015, dropped out of the top 10 in 2016.

3.1.4 Cyber-crime

In 2016 two distinct sides of cyber crime emerged:

- Large-scale email campaigns to distribute "commodity" malware such as ransomware and online banking threats, performed by traditional mass-market cyber crime groups.
- Sophisticated financial heists carried out by organized criminal groups or even nation-state actors.

With regards malware, it continues to be a blight on the threat landscape with more than 357 million new variants observed in 2016. However, for the first time, the rate of new malware seen on the endpoint has remained largely stagnant in 2016 – increasing by half a percent.

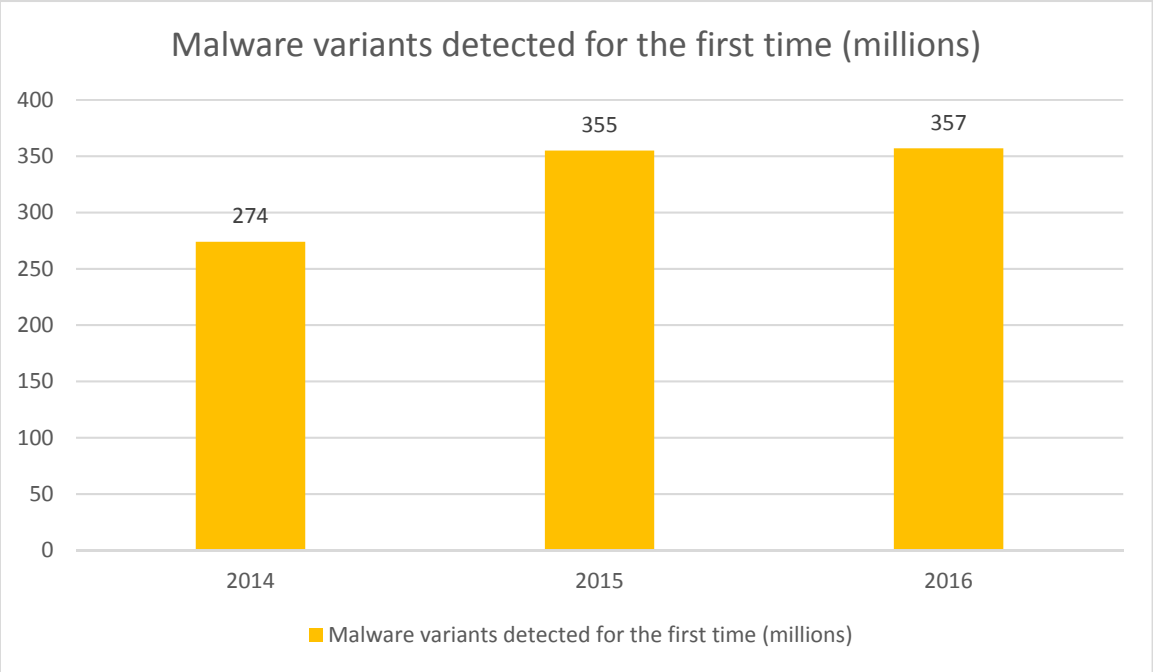

Figure 20 – Malware variants detected for the first time. Source: Symantec ISTR 2016

As per financial trojans, the next chart shows the top 10 of this kind of malware. Financial malware, specifically threats targeting online banking, has historically been a large driver of cyber crime. However, a number of arrests and takedowns, coupled with the continued success of ransomware, means that it has become less dominant.

Infection data shows that this area is dominated by five families (Ramnit, Bebloh, Zbot, Snifula, Cridex), while activity outside of this top five is negligible.

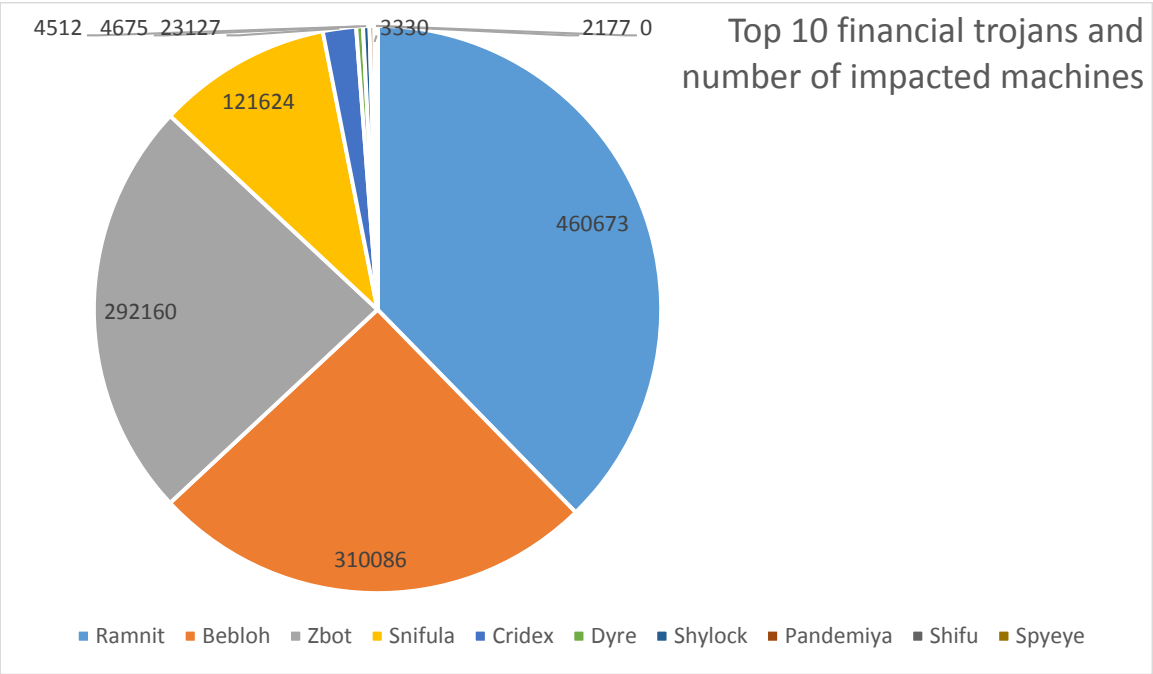

Figure 21 – Top 10 financial trojans and number of impacted machines. Source: Symantec ISTR 2016

With regards data breaches, the top 10 causes of data breaches in 2016, compared to 2015 (percentage) were:

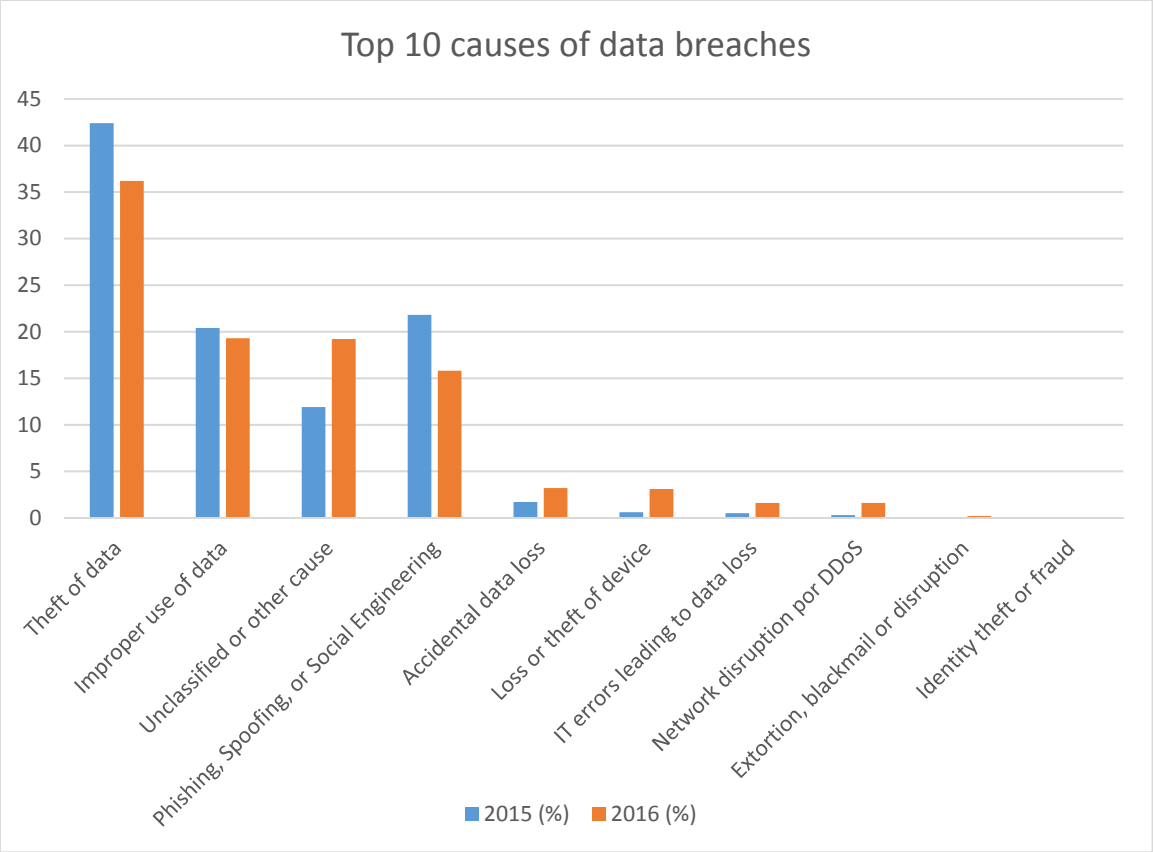

Figure 22 – Top 10 causes of data breaches. Source: Symantec ISTR 2016

While Theft of Data is the cause of just over a third of data breaches when looking at number of breaches, when measuring by the number of identities stolen, more than 91 percent of breaches fall into this category.

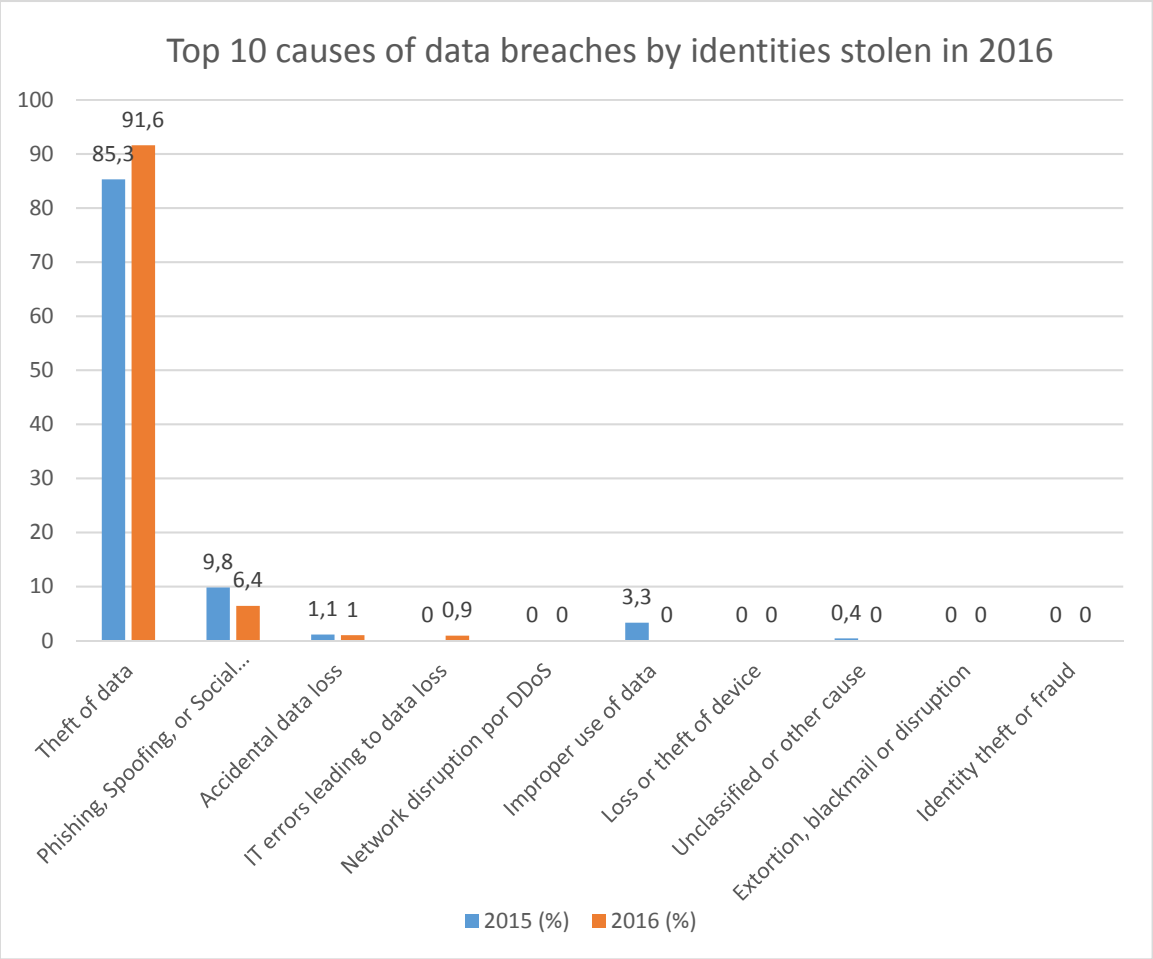

Figure 23 – Top 10 causes of data breaches by identities stolen. Source: Symantec ISTR 2016

Transportation and public utilities was the fifth sector more breached by number of incidents. Services; Finance, insurance & real estate and manufacturing are the sectors more affected by data breaches in 2016:

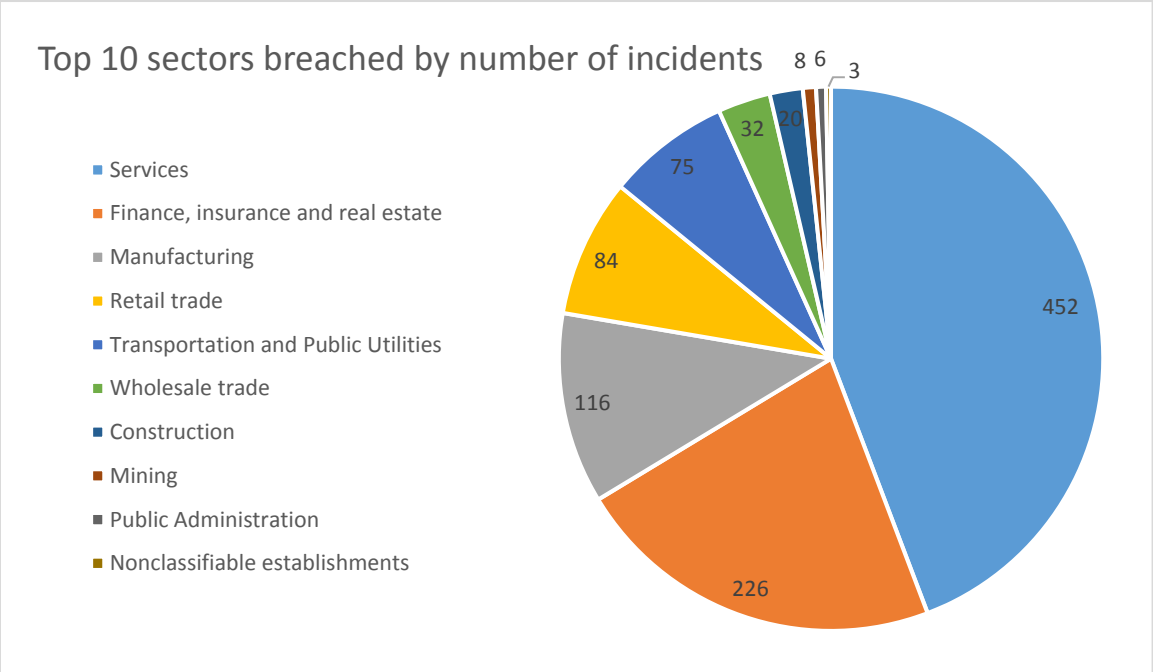

Figure 24 – Top 10 sectors breached by number of incidents. Source: Symantec ISTR 2016

As per countries, in the top 10 countries by number of data breaches, the United States leads the way:

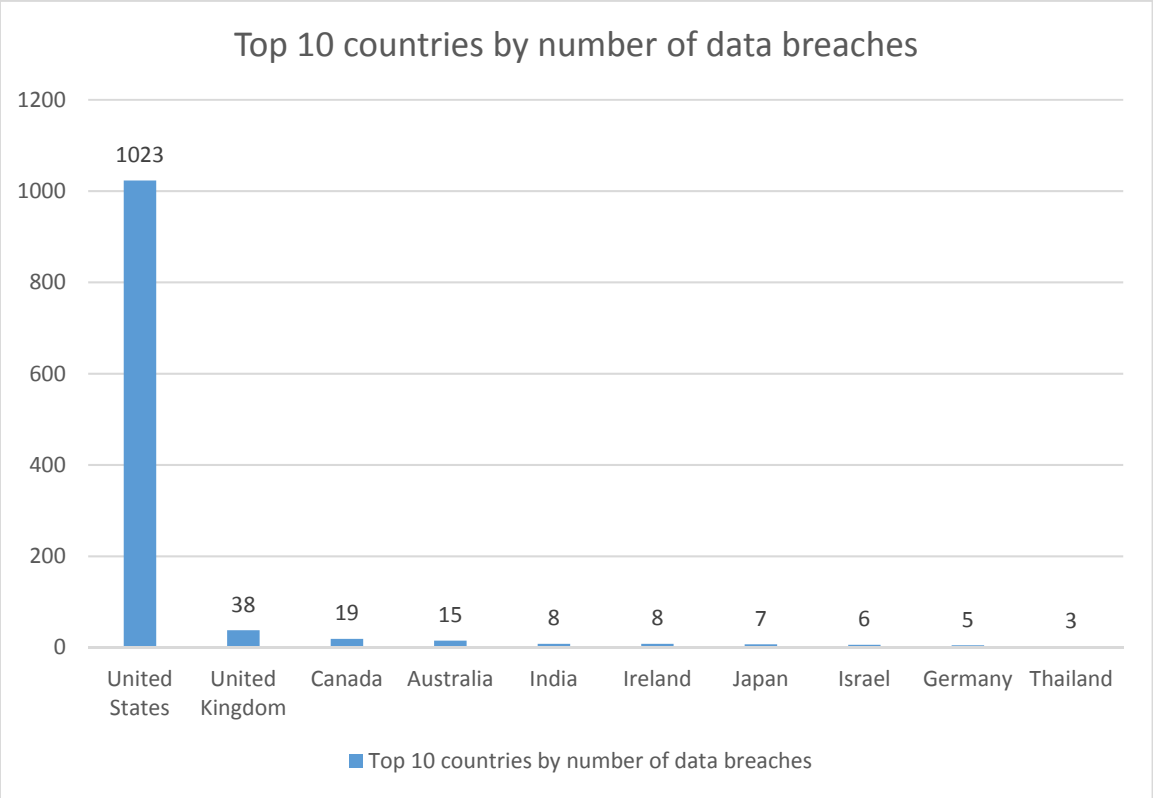

Figure 25 – Top 10 countries by number of data breaches. Source: Symantec ISTR 2016

3.1.5 Ransomware

During 2016, ransomware was one of the most significant threats facing both individuals and organizations. Attackers have honed and perfected the ransomware business model, using strongencryption, anonymous Bitcoin payments, and vast spam campaigns to create dangerous and wideranging malware. Ransomware is spread in a number of different ways and, generally speaking, the infection process involves a number of different stages at which the attack can be blocked. For example, in the case of ransomware distributed via email, most attacks (hundreds of thousands per day) are blocked by anti-spam defenses. In the case of web attacks, a significant number of ransomware attacks are performed using exploit kits, malicious web pages designed to exploit vulnerabilities on the victim's computer to install malware. A large number of ransomware attacks are blocked at exploit kit stage, before the ransomware can be installed on the victim's computer.

The number of new ransomware families discovered more than tripled to 98 in 2016, suggesting more and more attackers are now jumping on the ransomware bandwagon.

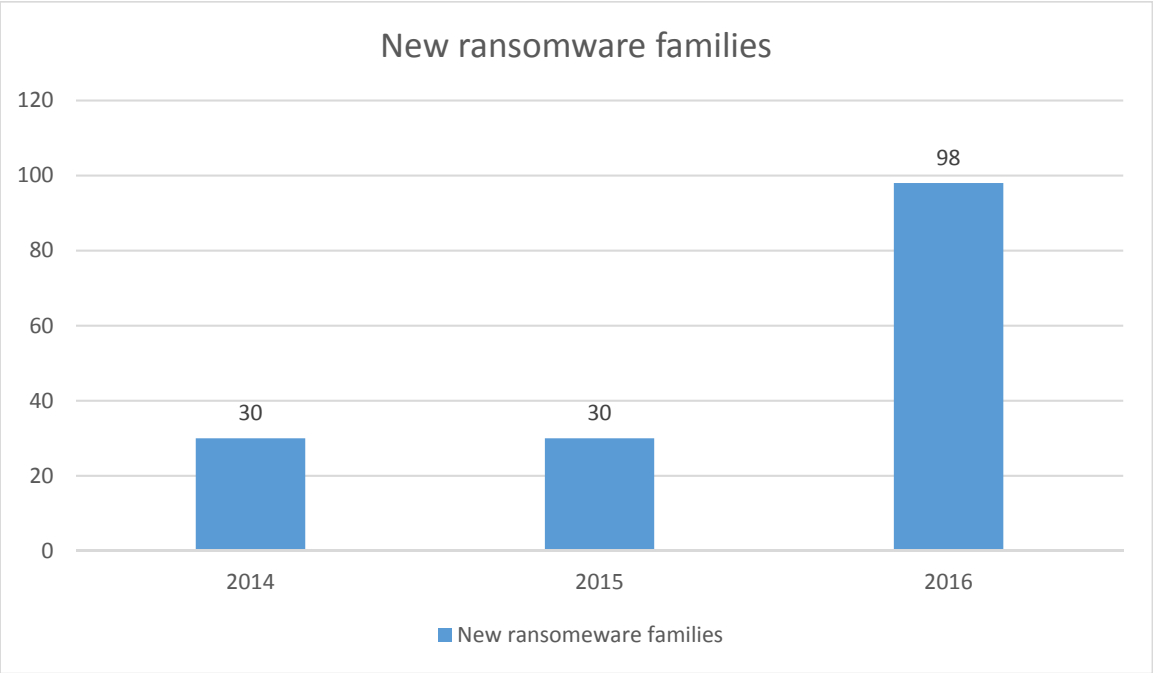

Figure 26 – New ransomware families detected. Source: Symantec ISTR 2016

3.1.6 Cyber-attack trends

Cyber-attackers have revealed new levels of ambition during the last years. 2016 was remarkable in terms of new cyber-attacks, including multi-milliion dollar virtual bank hesists, overt attempts to disrupt the US electoral process by state-sponsored groups, and some of the biggest distributed denial of service attacks on record powered by a botnet of Internet of Things devices. It seems that cyber espionage is experiencing a notable shift towards more overt activity, designed to destabilize and disrupt targeted organizations and countries. Until recently, cyber criminals mainly focused on bank customers, raiding accounts or stealing credit cards. However, a new breed of attacker has bigger ambitions and is targeting the banks themselves, sometimes attempting to steal millions of dollars in

a single attack. Gangs such as Carbanak have led the way, demonstrating the potential of this approach by pulling off a string of attacks against US banks.

Attackers ranging from cyber criminals to state-sponsored groups have begun to change their tactics, making more use of operating system features, off-the-shelf tools, and cloud services to compromise their victims. The most high-profile case of a living off the land attack took place during the US elections. A simple spear-phishing email provided access to Hillary Clinton's campaign chairman John Podesta's Gmail account without the use of any malware or vulnerabilities.

Malicious email has been also the weapon of choice for a wide range of attacks during the last years, and the trend is that this will continue at least in the near future. One in 131 emails sent in 2016 were malicious. It is a proven attack channel since it does not rely on vulnerabilities, but instead uses simple deception to lure victims into opening attachements, following links, or disclosing their credentials. Malicious emails disguised as routine correspondence, such as invoices or delivery notifications, were meanwhile the favoured means of spreading ransomware.

On the other hand, while ransomware and financial fraud groups continue to pose the biggest threat to end users, other threats are beginning to emerge. Attacks on Internet of Things devices and the "Cloud" are expected to gain their momentum. At present routers and security cameras (as IoT devices) have been subject of cyber-attacks, and even connected cars can be hacked for a new kind of terrorism.

3.2 Some real cyber-attacks

Next there is a description of some cyber-attacks performed in the supply chain and some other critical sectors, some of them involving port operations:

3.2.1 Smuggling drugs in the Por of Antwerp

In 2013, police disarmed a criminal gang that for two years had been smuggling drugs in containers that carried timber and bananas in a Belgian Port. Criminals hired the services of hackers to gain access to the Terminal Operating System (TOS) of two container terminals and thus controlling the movement and position of certain containers used to drugs and weapons trafficking. Methods used were:

- **Social engineering:** Hackers used techniques like spear phishing against employees of the terminals so they unwarily downloaded and installed trojans (remote access) to get log-in names, passwords and other data.
- **Physical manipulation of PCs:** When trojans were discovered thanks to the use of firewalls, hackers managed to access physically the terminal and installed keyloggers to keep tabs of the staff, especially the 9-digit pins that controlled access to the shipping containers. Using this PIN they were able to digitally mark the containers with cocaine as having been customs cleared.
- **Forged documentation:** By means of false papers and the hacked pin codes, the drivers of the organization could pick up the container on a location and time of their choice.

With regards the gear used to "own" the terminal system, it consisted of USB drives installed directly in the PC USB ports and small Linux computers running powerful hacking software called Metasploit. The devices were tucked inside a 15-by-5 inches casing of European power strips. The devices

("pwnies" in hackers' slang) sent out data via mobile networks, so they could be accessed from anywhere [1]. The investigation discovered that the intrusion mails containing malware (trojans) were sent from a Dutch IP address. The stolen data were forwarded to a server owned by the criminal group [2].

3.2.2 Crime syndicate in the Australian Customs System

In March 2012, a crime syndicate took advantage of the flaws of the Australian Customs and Border Protection Service's Integrated Cargo System to check if their shipping containers had been moved to a Customs Examination Facility or treated in a manner that suggested police attention. State and federal policing agencies discovered several instances where criminal syndicates abandoned contraband-filled containers as a result of being tipped off via the computer system that their cargo was to be examined. The vulnerability of the Customs computer program has been apparent since at least 2008, when a police operation found a suspected drug importing syndicate tapping into the system to find out if their containers were being screened. Also, criminal syndicates were using false identities or shelf companies to import goods into Australia and avoid detection [48].

3.2.3 Data hack in a US retailer

At the end of 2013, Target, a US retailer, was hit by one of the largest data breaches in the history of the retail industry. Between November 27 and December 15, 2013, Target's American brick-and-mortars stores experienced a data hack. Around 40 million customers credit and debit cards became susceptible to fraud after malware was introduced into the Point of Sale (POS) system in over 1800 stores. A 17-year-old Russian teen was suspected to be the author of the POS malware program, "BlackPOS", which was used by others to attack unpatched Windows computers used at Target.

The data breach of Target's customer information saw a direct impact on the company's profit, which fell 46 percent in the fourth quarter of 2013. Six months prior the company began installing a $1.6 million cyber security system. Target had a team of security specialists to monitor its computers constantly. Nonetheless, the supply chain attack circumvented these security measures.

It is believed that cyber criminals infiltrated a third-party supplier to gain access to Target's main data network. Although not officially confirmed, investigation officials suspected that the hackers first broke into Target's network on November 15, 2013 using passcode credentials stolen from a provider of HVAC systems. [49]

3.2.4 UK shipping firm Clarkson reports cyber attack

Clarkson is one of the world's main shipbrokers, sourcing vessels for the world's largest producers and traders of natural resources. It also has a research operation which collects and analyses data on merchant shipping and offshore markets. The company braced in July 2016 for a tranche of private data to be released, after refusing to pay a ransom to a hacker who staged a "criminal attack" on its computer systems. The company added: "The data at issue is confidential and lawyers are on standby wherever needed to take all necessary steps to preserve the confidentiality in the information." News of the cyber attack caused Clarkson shares to slip almost 6pc and they ended the day off 3.4pc at £28.14. Security consultants claimed to have found weaknesses that allowed them to manipulate

manifests of cargo, potentially allowing them smuggle goods. Altering manifests could also affect the way cargo is loaded on to ships to make sure weight is evenly distributed. If this is wrong, it could potentially mean vessels are unbalanced and more liable to capsize. [50]

3.2.5 US port cyber-attack thwarted

In December 2015, the US Coast Guard was alerted to a business e-mail compromise (BEC) attempt against a port facility in the US. A member of the company received an email from an unknown individual posing as the company's CEO, who claimed the company had an invoice due for payment. The email instructed the recipient to transfer US$15,000 and provided specific payment details, such as an account number and routing information for the transfer of funds. It rose questions as to whether the email was legitimate, and the company CEO was contacted to verify the request. The CEO instructed that they had not sent the email or authorised any transfer of funds. Upon further investigation it was revealed that the CEO's email had been spoofed. [51]

3.2.6 Petya-NotPetya attacks AP Møller-Maersk

On 27 June 2017 a malware never seen before, **named NotPetya** attacked the Danish giant AP Møller-Maersk, manager of the largest container fleet in the world. The attack led to a halt to global operations along the supply chain, causing a loss of approximately $300 million. At the same time, the same malware hit Russian and Ukrainian companies, among which the Russian oil company Rosnet [52]. The largest terminal at the Port of Los Angeles remained closed as Maersk continued to grapple with effects of a cyberattack that rippled across numerous countries on June 2017. Maersk said that 17 of its shipping container terminals worldwide were hacked and that, in response, the company deliberately shut down a number of its IT systems. [53]

Petya is a family of encrypting ransomware that was first discovered in 2016. The malware targets Microsoft Windows-based systems, infecting the master boot record to execute a payload that encrypts a hard drive's file system table and prevents Windows from booting. It subsequently demands that the user make a payment in Bitcoin in order to regain access to the system. Variants of Petya were first seen in March 2016, which propagated via infected e-mail attachments. In June 2017, a new variant of Petya was used for a global cyberattack, primarily targeting Ukraine. The new variant propagates via the EternalBlue exploit, which is generally believed to have been developed by the U.S. National Security Agency (NSA), and was used earlier in the year by the WannaCry ransomware. Kaspersky Lab referred to this new version as NotPetya to disambiguate it from the 2016 variants, due to these differences in operation. In addition, although it purports to be ransomware, this variant was modified so that it is unable to actually revert its own changes [54]

3.2.7 Ukraine's power grid hacked

The 2016 attack on the Ukrainian power grid, which deprived part of its capital, Kiev, of power for an hour, was caused by a cyber attack. The malware, detected as Win32 / Industroyer, is a powerful threat that can take direct control of the substation switches and circuit breakers. Industroyer is a modular malware.

A backdoor as the primary component used by attackers to manage the attack: install and control the other components and connect to a remote server to receive commands and report to attackers.

In 2015, an attack on electrical power distribution networks with BlackEnergy malware occurred, along with KillDisk and other malicious components, and therefore circumvented legitimate remote access software to control operator workstations and shut down power. [55]

3.2.8 Dripion: A backdoor trojan

In August 2015, Symantec identified a backdoor trojan (Backdoor.Dripion) that was previously unknown, infecting organizations located overseas in Taiwan, Brazil, and the United States. The purpose of Dripion is to steal information and has been used sparingly in a limited number of targeted attacks. The perpetrators of this attack tried to mask their activities including the use of domain names masquerading as corporate antivirus (AV) websites for their command and control (C & C) servers.

Once Dripion is installed, the attacker accesses the user's computer. Dripion has the functionality of a backdoor trojan: the aggessori are able to load, download and steal predetermined information from the victim and execute remote commands. Sensitive information such as the victim's computer name and the IP address are automatically transmitted to the C & C server at the time of infection development. [56]

3.2.9 Mumbai container terminal hit by ransomware attack

The largest Indian container port Jawaharlal Nehru Port Trust (JNPT), has been hit in June 2017 by a relapse of the global ransomware attack that led to the paralysis of some central banks and large European companies. Such attack arrives a few weeks after the attack of Wannacry ransomware, which has infected the systems of many companies. The Indian port tried to clear containers manually, but operational capacity dropped to a third at the terminal. Containers had to be piled outside the port due to delay in loading and unloading at Gateway Terminals India. [57]

3.2.10 Tanker group faces cyber-attack

BW Group, a company that owns fleets of tankers including VLCCs, product tankers and others was hit by a cyber security breach that allowed hackers to gain access to the company’s computer systems. The attack happened in July 2017, making it the first shipping-related cyber security breach reported since the NotPetya virus took down the operations of container shipping giant Maersk in June. The attack consisted of an unauthorised access, but internal and external communications to customers and stakeholders were not impacted. The company had to work around planned system downtimes as their IT department reinforced the cyber-security infrastructure. [58]

3.2.11 San Francisco Municipal Transport Agency suffers cyber-attack

In November 2016 the San Francisco public transfer suffered a ramsomware attack by hackers who locked up computers and data with 100 bitcoin demand. Hackers managed to infect and take over more than 2,000 computers used to operate San Francisco’s public transport system, forcing the Municipal Transportation Agency (MTA) to open the gates and allow passengers to ride for nothing. The attackers used a variant of the HDDCryptor malware to infect 2,112 computers, encrypting their

data and preventing them from operating normally – holding them to ransom for 100 bitcoin. Every computer was left displaying a black screen with a ransom note written across it stating: “You Hacked, ALL Data Encrypted”. The MTA’s operational and worker machines were affected, disrupting email, payment services, but not core operations, which allowed trains to continue running without payment.

In 2013 the Cryptolocker ransomware infected an estimated 234,000 computers, including at least 50,000 in the UK, and required a global police operation to neutralise it. [59]

3.2.12 Chinese manufacturer implanted malware to steal supply chain intelligence

In 2014, a Chinese manufacturer that sells devices for scanning items shipped or transported apparently has been implanting a malware in its products, as well as via the Windows XP embedded version of the software on the scanner maker's support website to steal information from logistics and shipping firms as well as manufacturing companies around the globe in an attack campaign dubbed "ZombieZero" by the researchers who discovered it. Researchers said scanners with another variant of the same malware were also sold to a large robotics firm and seven other companies. Once the scanner is connected to the victim's wireless network, it attacks the corporate network via the server message block (SMB) protocol, and the scanned information, including origin, destination, contents, value, and shipper and recipient information, is sent to a botnet that terminates at the Lanxiang Vocational School purportedly located in the Shangdong province in China. The school has been linked to the infamous Operation Aurora cyber espionage campaign that hit Google, Adobe, Intel, and many other major US firms more than four years ago and is located one block from the inventory scanner manufacturer in question. The botnet then sends the scanner a second piece of malware that targets the victim's corporate financial, customer, shipping, and manifest information, which allows the attacker to make a package “disappear” or “reappear”, for instance.

One ZombieZero victim company running 48 inventory scanners from the unnamed Chinese manufacturer found that 16 of the devices were infected with the malware. A firewall sits between the inventory scanner wireless network and the corporate network at one of its sites, and the firewall blocked the initial attack attempt. But then came a second attack via the RADMIN protocol, or port 4899, that bypassed the firewall. Nine corporate servers were infected with the cyberspying malware. Its second site was defenseless - no firewall - so the attack went through SMB and infiltrated the corporate network and ERP servers. [60]

3.2.13 Hacker Disabled Offshore Oil Platforms' Leak-Detection System

An aggrieved ex-employee of Pacific Energy Resources purposely disabled a computer system aimed at detecting pipeline leaks for three oil derricks off the Southern California coast in 2009. This hacker was an information technology consultant who used his multiple user accounts to impair the leak-detection system while logged in from his home. [61]

3.2.14 The Stuxnet computer worm

Stuxnet is a malicious computer worm, first uncovered in 2010 by Kaspersky Lab. Thought to have been in development since at least 2005, Stuxnet targets SCADA systems and was responsible for causing substantial damage to Iran's nuclear program. Although neither country has openly admitted responsibility, the worm is believed to be a jointly built American/Israeli cyberweapon.

Stuxnet specifically targets programmable logic controllers (PLCs), which allow the automation of electromechanical processes such as those used to control machinery on factory assembly lines, amusement rides, or centrifuges for separating nuclear material. Exploiting four zero-day flaws,] Stuxnet functions by targeting machines using the Microsoft Windows operating system and networks, then seeking out Siemens Step7 software. Stuxnet reportedly compromised Iranian PLCs, collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart. Stuxnet's design and architecture are not domain-specific and it could be tailored as a platform for attacking modern supervisory control and data acquisition (SCADA) and PLC systems (e.g., in factory assembly lines or power plants), the majority of which reside in Europe, Japan and the US. Stuxnet reportedly ruined almost one fifth of Iran's nuclear centrifuges. Targeting industrial control systems, the worm infected over 200,000 computers and caused 1,000 machines to physically degrade. [62]

3.2.15 Chrome extensions compromised

During 2017, Google's Chorme web browser Extensions have been under attack with a series of developers being hacked. In all these cases, some unknown attackers first gained access to the developers' Google web accounts by sending out phising emails with malicious links to steal account credentials. Once the attackers gained access to the accounts, either they hijacked their respective extensions and then modified them to perform malicious tasks, or they add malicious Javascript code to them in an attempt to hijack traffic and expose users to fake ads and password theft in order to generate revenue. In the case of the *Copyfish* extension, the attackers even moved the whole extension to one of its developers' accounts, preventing the software company from removing the infected extension from the Chrome store, even after being spotted compromised behaviour of the extension. [63]

3.2.16 ShadowPad backdoor

ShadowPad is one of the largest known supply-chain attacks, discovered in 2017 by Kaspersky Lab experts. It consists of a backdoor planted in a server management software product used by hundreds of large businesses around the world. When activated, the backdoor allows attackers to download further malicious modules or steal data. Kaspersky Lab experts were worried about suspicious DNS requests originating on a system involved in the processing of financial transactions. Further investigation showed that the source of these requests was server management software produced by a legitimate company and used by hundreds of customers in industries like financial services, education, telecoms, manufacturing, energy, and transportation. The most worrying finding was the fact that the vendor did not mean for the software to make these requests.

Further Kaspersky Lab analysis showed that the suspicious requests were actually the result of the activity of a malicious module hidden inside a recent version of the legitimate software. Following the installation of an infected software update, the malicious module would start sending DNS-queries to specific domains (its command and control server) at a frequency of once every eight hours. The request would contain basic information about the victim system (user name, domain name, host name). If the attackers considered the system to be "interesting", the command server would reply and activate a fully-fledged backdoor platform that would silently deploy itself inside the attacked computer. After that, on command from the attackers, the backdoor platform would be able to download and execute further malicious code. Once warned, the company reacted fast and released an updated version of the software without the malicious code. [64]

3.3 Cyber-incidents

Sometimes the problem are not criminals, hacktivists or malicious actors performing on purpose cyber-attacks on a company but errors or weaknesess in networks, software and computer systems, and even poor handling and unknonlewdge of brand-new systems operation. Sometimes the incident is also caused by a significant exposure to a known threat. Next there are some examples of these incidents related to the supply chain:

3.3.1 New computer system in Maher terminal

In 2013, Maher Terminals, which handles a third of the port of New York and New Jersey's volume, experienced significant difficulties after switching to a new computer system at one of its terminals. The impacts at the terminal, which lasted for several weeks, included the closing of the terminal for hours at a time and truck backups lasting 4–6 hours. The problems at the terminal caused significant delays in some supply chains in the Northeast. In addition, the problems at the terminal had a considerable impact on the operations of other terminals at the port [65].

3.3.2 Denial-of-Service in the Port of Vancouver

In March 2017, the Port of Vancouver's computer network was subject to a denial-of- service attack. A port spokesman said that during a meeting of Vancouver Energy held at the port, an attendee of the standing-room-only crowd unknowingly had a virus on their computer, and once the computer connected to the port's Wi-Fi, the virus started attacking the port's network, so it was not a purposeful attack. [66]

3.3.3 Ship's crew member affects ship's program

According to the Coastguard Field Intelligence report (2015) and a investigation of Robert M. Clark and Simon Hakim [67], a crew member of a ship plugged his smart phone into a ship's electronic chart system to charge the phone's battery. Malware on the phone migrated to the system and deleted or corrupted all of the charts, causing a two-day delay in the ship's schedule while technicians restored the system. U. S. Coast Guard also has noted with concern several instances in which malware impacted the dynamic positioning systems used for precise navigation control in the offshore oil industry. These operations, which involve large ships maneuvering alongside oil rigs in an offshore environment, are potentially dangerous. In one instance, investigators linked a sudden, unexpected power loss to viruses

found on the software controlling the system. Thankfully there were no injuries, damage, or pollution but the potential for such consequences is clear.

3.3.4 Failure in software design causes accident in a vessel

In 2008, an incident was reported in which the failure of a J-lay pipe-handling system caused two pipes to be dropped, one of which caused injuries to eight people, four of whom died as a result. [68]

The primary causes of the incident were found to be:

- Sudden release of the two quadruple joints was caused by a failure in conceptual design of the control system software. The program relevant to the JLT initialising instruction was pre-loaded in the erasable programmable read-only memory (EPROM) of the programmable logic controller (PLC) with the instruction to open all clamps. Members are recommended to investigate the possibility that this could happen to the PLC-based control systems on equipment on their vessels.
- The unnecessary presence and uncontrolled access of working personnel on to the access platform destroyed by the falling pipe exposed personnel to suspended load/dropped object hazard.

3.3.5 Ships collision after installing new positioning system

On February 26, 2011, the platform supply vessel *SBS Typhoon* made contact with the *Vos Scout*and the *PSV Ocean Searcher* while conducting tests of a newly installed Kongsberg DP system in Aberdeen Harbor. The authorities in charge of the investigation, UK's Marine Accident Investigation Bureau, released the final report on the incident, citing an incorrect pitch command signal generated by the newly installed DP system as the culprit. Ahead pitch was applied to the controllable pitch propellers because an incorrect pitch command signal was generated by the DP system signal modules. The error was not identified during factory tests or during the pre-trial checks although the system documentation specified the correct signal values. Actions taken on board to limit damage were hampered by a defective engine emergency stop and because a mode selector switch on the DP system was not moved to the correct position. [69]

4 Attacks on Pilot Scenarios

In the current section, cyber-threat scenarios, performed in the MITIGATE platform, are presented. The attack-based scenarios concern two Critical Services of the Maritime Industry: the Container Cargo Management (SCS 1) and the Vehicles Transport Service (SCS 2).

4.1 SCS 1. "Container Cargo Management"

4.1.1 Business Description

The containerized freight represents almost the third part of total trade exchanges measured in monetary value. The percentage of maritime transport in relation to total transport modes is even higher when kilometres or tonne-kilometres are measured. So these references are pointing to the important role of container terminals in the international carriage of goods. Any flow of goods materializes in a series of sections of transport between the nodes of the logistics infrastructure. In each of these sections a form of transportation is used which could be or not the same to the previous section. As nodes it is possible to quote production centres, logistics platforms and consumption centres. The container transport is a part of this global flow and the port terminal is a node of the infrastructure where converge besides of land and maritime nodes, the activity of several agents related with the transport.

Figure 27: Container Cargo Management Service

So, the Port Community is a set of stakeholders which take part in the supply chain that crosses the port and become part of a heterogeneous community, with several interests, but all of them dedicated directly or indirectly to the maritime shipping business. Within this group, the main role of the container terminals is just to carry on the land-sea connection. And this is the way as a port terminal becomes in an essential element of the port-logistics supply chains making possible the intermodality. Essentially, the container transport chain starts at the manufacturer/exporter's location, usually known as shipper. Usually, the container is packed and delivered from there via land carrier (mainly by truck), and depending on the distance and necessities, it also travels by train (through intermodal nodes) up to the port terminal. The management of this delivery is usually done by customs agents, shipping agencies and consignees. At port, other business partners play their role: customs office, port authority, container terminals, stevedores, service providers, shipping companies, etc. When the container is loaded on the containership it travels up to its destination, usually far away from its origin.

There, similar business partners are involved before the container reaches the receiver, also known as importer, and always after customs inspection and/or release. All this chain is subject to many documents and information exchange, both in paper or digital formats, being a complex and heterogeneous system subject to peculiarities and regulations of each country.

4.1.2 Cyber Threat Scenario

Next there is an example of Attack Path based in a scenario for Container Cargo Management, performed in the MITIGATE platform:

Attack Path Features			
Supply Chain Service (SCS)			
Container Cargo Management			
Process Name Port's Services Requested			
Order of Transportation			
Business Partner(s) involved			
Valencia Port Authority			
Assets' infrastructure involved			
PCS hosting server, PCS router, PCS server operating system, PCS antivirus, PCS database, PCS FTP Server, PCS VMware, PCS web server			
Attack Path Query (Q1)			
Asset Entry point	**Asset Target point**	**Attacker's Location** (Local/Adjacent/Network)	**Propagation Length** (n⊆ Z n≥1, n≤10)
PCS server operating system	PCS hosting server	Network	7
Attacker's Capability (Low (L)/Medium (M)/High (H)) **:**			**(H)**
Attack Path Query Results			

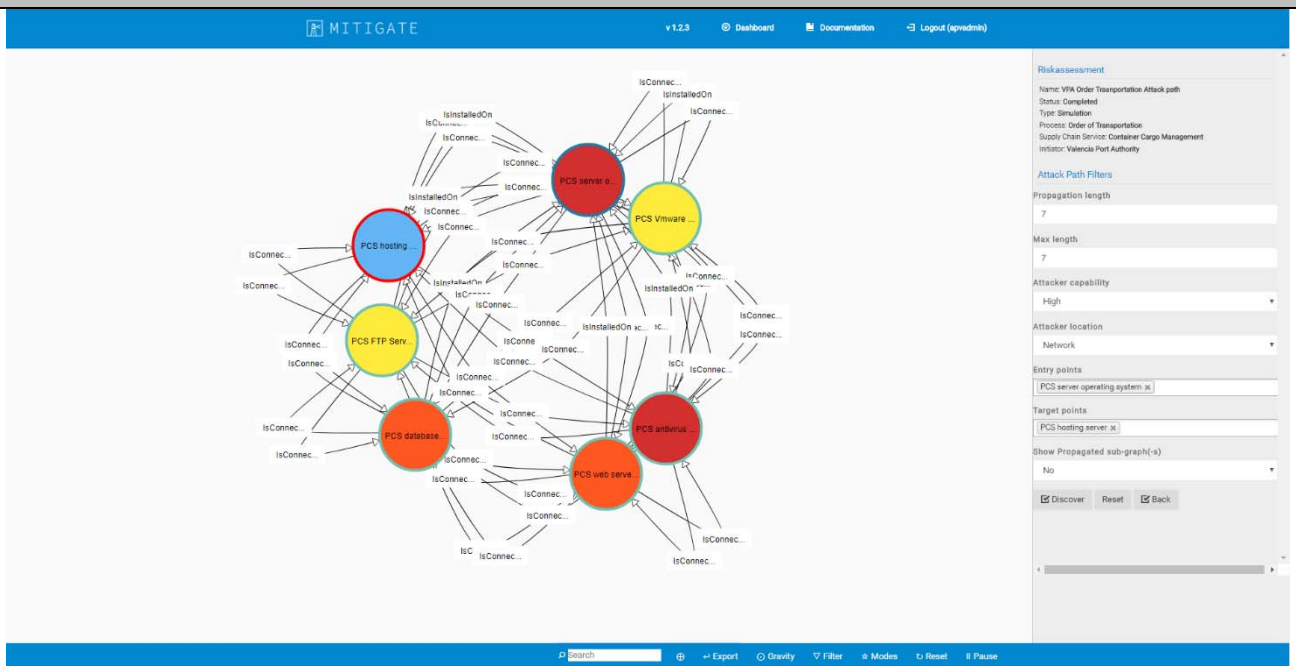

Table 17 : Attack Paths visualization for Q1

No	Asset Chain ($A1 \rightarrow A2 \rightarrow A3 \rightarrow A_X$)	Vulnerability Chain ($V1 \rightarrow V2 \rightarrow V_X$)	Assets' Chain Name	Assets' Chain Product Version	Assets' Chain Vendor	Assets' Chain Vulnerabilities
1	PCS server operating system → PCS hosting server → PCS antivirus	CVE-2016-7217 → CVE-2007-3012 → CVE-2010-0108	PCS server operating system	Windows server 2016	Microsoft	CVE-2016-7217
			PCS hosting server	Primergy bx300	Fujitsu	CVE-2007-3012
			PCS antivirus	Antivirus 10.0.9	Symantec	CVE-2010-0108
2	PCS server operating system → PCS hosting server → PCS database	CVE-2016-7217 → CVE-2007-3012 → CVE-2016-7250	PCS server operating system	Windows server 2016	Microsoft	CVE-2016-7217
			PCS hosting server	Primergy bx300	Fujitsu	CVE-2007-3012
			PCS database	Sql server 2016	Microsoft	CVE-2016-7250
3	PCS server operating system → PCS hosting server →PCS FTP Server	CVE-2016-7217 → CVE-2007-3012 → CVE-2009-0884	PCS server operating system	Windows server 2016	Microsoft	CVE-2016-7217
			PCS hosting server	Primergy bx300	Fujitsu	CVE-2007-3012
			PCS FTP Server	Filezilla server 0.9.0	Filezilla	CVE-2009-0884
4	PCS server operating system → PCS hosting server →PCS VMware	CVE-2016-7217 → CVE-2007-3012 → CVE-2009-3731	PCS server operating system	Windows server 2016	Microsoft	CVE-2016-7217
			PCS hosting server	Primergy bx300	Fujitsu	CVE-2007-3012
			PCS VMware	Esx server 4.0	Microsoft	CVE-2009-3731
5	PCS server operating system → PCS hosting server →PCS web server	CVE-2016-7217 → CVE-2007-3012 → CVE-2014-4078	PCS server operating system	Windows server 2016	Microsoft	CVE-2016-7217
			PCS hosting server	Primergy bx300	Fujitsu	CVE-2007-3012
			PCS web server	Internet information services 8.5	Vmware	CVE-2014-4078

Attack scenario Description

The adversary can execute arbitrary code by inducing the users into crafted websites (phishing attacks). The attack is based in an improper handling of objects in memory (CVE-2016-7217), that allows the attacker to get into the PCS OS. Once in the OS, the attacker can reach the PCS hosting by canceling an authentication dialog and obtain sensitive information of it through the CVE-2007-3012 vulnerability. Once the hosting is breached, other vulnerabilities (CVE-2010-0108, CVE-2016-7250, CVE-2009-0884, CVE-2009-3731, CVE-2009-3731, CVE-2014-4078) are leveraged to threat other assets in the scenario.

4.2 SCS 2. "Vehicles Transport Service"

4.2.1 Business Description

The "Vehicles Transport Service" is a massively complex system with numerous players, including shippers, transport operators of domestic and international transportation, warehouse management, order and inventory control, materials handling, import/export facilitation, and information technology. It involves the shipment and receipt of various types of vehicles and equipment, such as trucks, vans, truck trailers, forklifts, gantry cranes etc.

Figure 28: The Vehicles Transport Service

The "Vehicles Transport Service" breaks down into a number of processes, that involve several physical (docking of the ship, stevedoring, logistics procedures, transportation, inspection, etc) and cyber (vessel's pre-arrival and arrival arrangements, customs clearance documentation management, ISPS declaration, etc) asset operations. In this vein, the vehicles transport affects many sectors along the supply chain interconnecting multimodal transport infrastructure and heterogeneous ICT networks (SCADA, AIS, Port Information System network, etc.)

The emerging role of these multiple and sophisticated technologies attracts the attention of adversaries, engenders limitations in the Industry security awareness that fosters the exploitation of physical and cyber-threats growing up the rate of cyber-attacks committed within the supply chain. The CIIs operating within the Vehicles Transport Service have cyber multi-interdependencies, which adversaries may exploit to generate attack-paths, in order to compromise a series of interconnected cyber-assets of the Vehicles Transport Service.

4.2.2 Cyber Threat Scenario

This section, presents the cyber-threat scenarios performed in the MITIGATE platform regarding the Vehciles Transport Service. The attack-based scenarios are generated according to cyber-assets operations of three perminent processes of the Vehicles Transport Service; the Ship Formalities Arrangements process, the Port's Services Requested process and the Vehicle Unloading process.

Attack Path Features			
Supply Chain Service (SCS)			
Vehicles Transport Service			
Process Name Port's Services Requested			
Ship Formalities Arrangement			
Business Partner(s) involved			
Piraeus Port Authority (PPA)			
Assets' infrastructure involved			
Adobe Flash Player , Workstation1, Admin Operating System, Wireless Router			
Attack Path Query (Q2)			
Asset Entry point	**Asset Target point**	**Attacker's Location** (Local/Adjacent/Network)	**Propagation Length** (n⊆ Z n≥1, n≤10)
Adobe Flash Player	Admin Operating System	Network	7
Attacker's Capability (Low (L)/Medium (M)/High (H)) **:**			**(H)**
Attack Path Query Results			

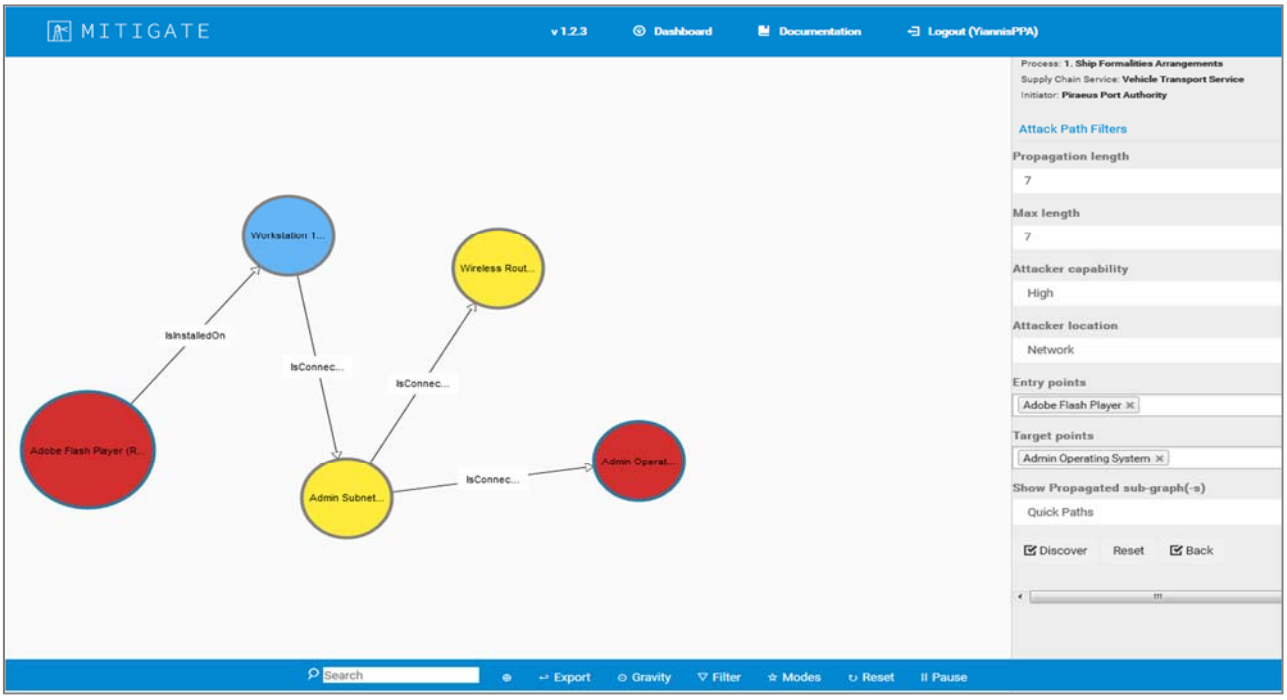

Table 18 : Attack Paths visualization for Q2

No	Asset Chain ($A1 \rightarrow A2 \rightarrow A3 \rightarrow A_X$)	Vulnerability Chain ($V1 \rightarrow V2 \rightarrow V_X$)	Assets' Chain Name	Assets' Chain Product Version	Assets' Chain Vendor	Assets' Chain Vulnerabilities
	Admin Adobe Flash→ Workstation 1→ Admin Operating System	CVE-2017-2925 → CVE-2017-8633→ CVE-2015-6112	Adobe Flash Player	Adobe Flash Player 24.0.0.186	Adobe	CVE-2017-2925 / Execute Code Overflow Memory corruption
			Workstation 1	Microsoft Windows 8.1 Pro Enterprise	Microsoft	CVE-2017-8633/ elevation of privileges
			Admin Operating System	Microsoft windows 7, sp1	Microsoft	CVE-2015-6112/ Obtain Information
2	Admin Adobe Flash→ Workstation 1→ Wireless Router→	CVE-2017-2925 → CVE-2017-8633 → CVE-2012-1338	Adobe Flash Player	Adobe Flash Player 24.0.0.186	Adobe	CVE-2017-2925 / Execute Code Overflow Memory corruption
			Workstation 1	Microsoft Windows 8.1 Pro Enterprise	Microsoft	CVE-2017-8633/ elevation of privileges
			Wireless Router	Cisco Catalyst 3560 router	Cisco	CVE-2012-1338/ Denial Of Service

Attack scenario Description

The adversary sends phishing emails to corporate staff asking them to click on a link that will take the user to a fraudulent website that appears legitimate. This fraudulent website contains malicious code, a specially crafted Flash content that exploits the vulnerability CVE-2017-2925 "Execute Code Overflow Memory corruption" on the "Internet Explorer 10" port operator's user web browser. In this way, the attacker can download and execute arbitrary code on the victims' system "Workstation 1" (Microsoft Windows 8.1), in order to gain access to it. Afterward, he exploits the CVE-2017-8633 vulnerability on the "Workstation 1" (Microsoft Windows 8.1) to gain elevated privileges on the "Admin Operating System" (Microsoft Windows 7). Then, the remote attacker can compromise either the (i) Administrator's Operating System (Microsoft Windows 7) or (ii) the wireless router, which is interconnected via the Admin subnet:

i) Further, the adversary can exploit the CVE-2015-6112 vulnerability on the "Admin Operating System" to obtain sensitive Port Authority information.

ii) The PPA "Wireless router" (Cisco Catalyst 3560) is configured with an IP address via an enabled interface on the "Workstation 1" (Windows 8.1 operating system) of the port operator user, which it can be switched remotely. Once the adversary has gained access to the "Workstation 1" operating system, he realizes that the adjacent PPA "Wireless router" (Cisco Catalyst 3560) device allows a web-consoled access using the default sisco account (user name: sisco, password: sisco). Therefore, he gets authenticated and exploits the CVE-2012-1338 vulnerability causing a denial of service (device reload) to the PPA Cisco router.

Attack Path Features			
Supply Chain Service (SCS)			
Vehicles Transport Service			
Process Name Port's Services Requested			
Port's Services Requested			
Business Partner(s) involved			
Piraeus Port Authority (PPA), Ship Agent			
Assets' infrastructure involved			
PPA Web Application (Tasklist module), Port Community System, PPA Database Server, PPA Database OS, DB Admin Web Browser, DB Admin Workstation, PSR VMware server			
Attack Path Query (Q3)			
Asset Entry point	**Asset Target point**	**Attacker's Location** (Local/Adjacent/Network)	**Propagation Length** (n⊆ Z n≥1, n≤10)
PPA Web Application (Tasklist module)	PPA Database Server	Network	7
Attacker's Capability (Low (L)/Medium (M)/High (H)) **:**			**(M)**
Attack Path Query Results			

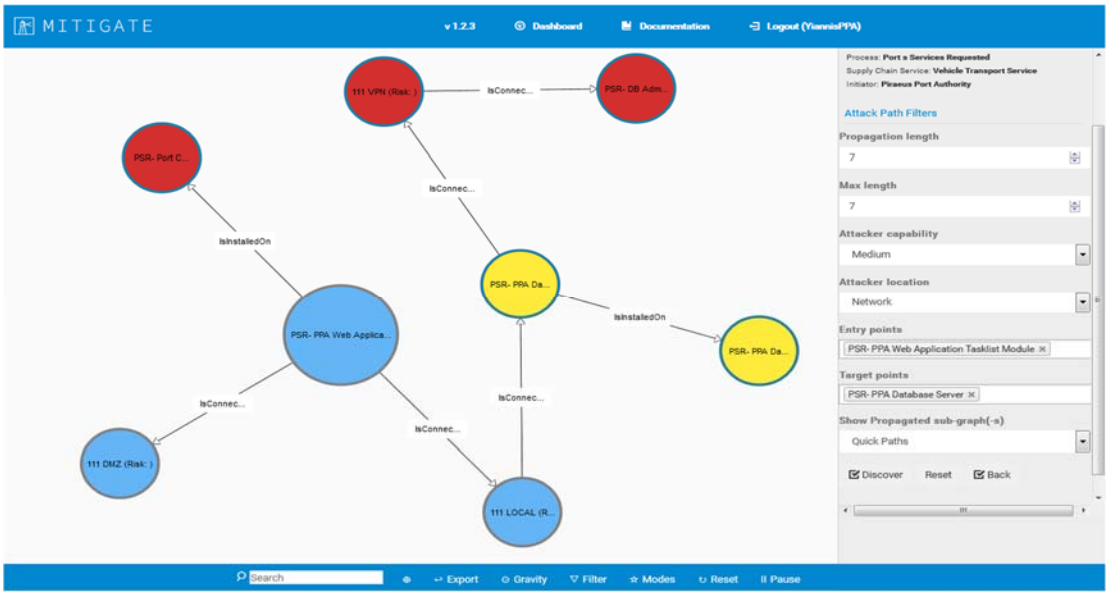

Table 19 : Attack Paths visualization for Q3

No	Asset Chain (A1 → A2 → A3→ A_X)	Vulnerability Chain (V1 → V2 → V_X)	Assets' Chain Name	Assets' Chain Product Version	Assets' Chain Vendor	Assets' Chain Vulnerabilities
1	PPA Web Application→ Port Community System→ PCD Database Server→ PCS Database OS	CVE-2009-1034 → CVE-2015-1763→	PPA Web Application (Tasklist module)	Drupal Tasklist Module v.5.1	Drupal	CVE-2009-1034 / Execute Code Sql Injection
			Port Community System	Microsoft Windows Server 2008, sp2	Microsoft	
			PPA Database Server	Microsoft SQL Server 2012, sp1	Microsoft	CVE-2015-1763/ Execute Code
			PPA Database OS	Microsoft Windows Server 2008, sp2, x64	Microsoft	
2	PPA Web Application→ Port Community System→ PCS Database Server→ DB Admin Web Browser→ DB Admin Workstation→ PSR VMware Server	CVE-2009-1034 → CVE-2015-1763 → CVE-2008-4197 → CVE-2009-3733	PPA Web Application (Tasklist module)	Drupal Tasklist Module 5.1	Drupal	CVE-2009-1034 / Execute Code Sql Injection
			Port Community System	Microsoft Windows Server 2008	Microsoft	
			PPA Database Server	Microsoft SQL Server	Microsoft	CVE-2015-1763/ Execute Code
			DB Admin Web Browser	Opera_browser,v.9.51	Opera	CVE-2008-4197/ Execute Code
			DB Admin Workstation	linux:linux	Suse Linux	
			PSR VMware Server	VMware server v.2.0.1	VMware	CVE-2009-3733/ Directory traversal

Attack scenario Description

The adversary (located within the premises of the Ship Agent collaborating business partner) performs a port scan against the web application of the Piraeus Port Authority, available through cyber dependency "Accessing".

The port scan reveals a Drupal-based "PPA web application", which includes Tasklist module 5.1. The latter, is vulnerable to CVE-2009-1034, which allows arbitrary SQL command execution using crafted URIs. Furthermore, the Drupal application runs with local administrator credentials, permitting the adversary to get a reverse shell and root-compromise the "Port Community System" (Microsoft Windows Server 2008).

The attacker explores the file system to identify additional targets and discovers a configuration file that lists, in plain text, the details of a database account (the database that serves the Drupal web application). Being now able to authenticate against the "PPA Database Server" (Microsoft SQL Server 2012), the attacker exploits the CVE-2015-1763 vulnerability, which allows authenticated users to execute arbitrary code and root-compromise the underlying operating system (Microsoft Windows Server 2008 for Database).

The VPN link, which is available through the server hosting the SQL database, provides network access to a Linux Workstation, belonging to the database administrator. The Linux Workstation is compromised using the CVE-2008-4197 vulnerability, which takes advantage of the installed "DB Admin Web Browser" (Opera Browser). Finally, the attacker

exploits the CVE-2009-3733 vulnerability, which affects an outdated installation of “PSR VMware Server” and results in authorized disclosure of information.

Attack Path Features			
Supply Chain Service (SCS)			
Vehicles Transport Service			
Process Name Port's Services Requested			
Vehicles Unloading			
Business Partner(s) involved			
Piraeus Port Authority (PPA)			
Assets' infrastructure involved			
SCADA Security System for Admin Wincc SCADA, Admin Wincc SCADA OS, SCADA HMI Software (User Group)			
Attack Path Query (Q4)			
Asset Entry point	**Asset Target point**	**Attacker's Location** (Local/Adjacent/Network)	**Propagation Length** (n⊆ Z n≥1, n≤10)
SCADA Security System for Admin Wincc SCADA	SCADA HMI Software (User Group)	Network	7
Attacker's Capability (Low (L)/Medium (M)/High (H)) **:**			**(H)**
Attack Path Query Results			

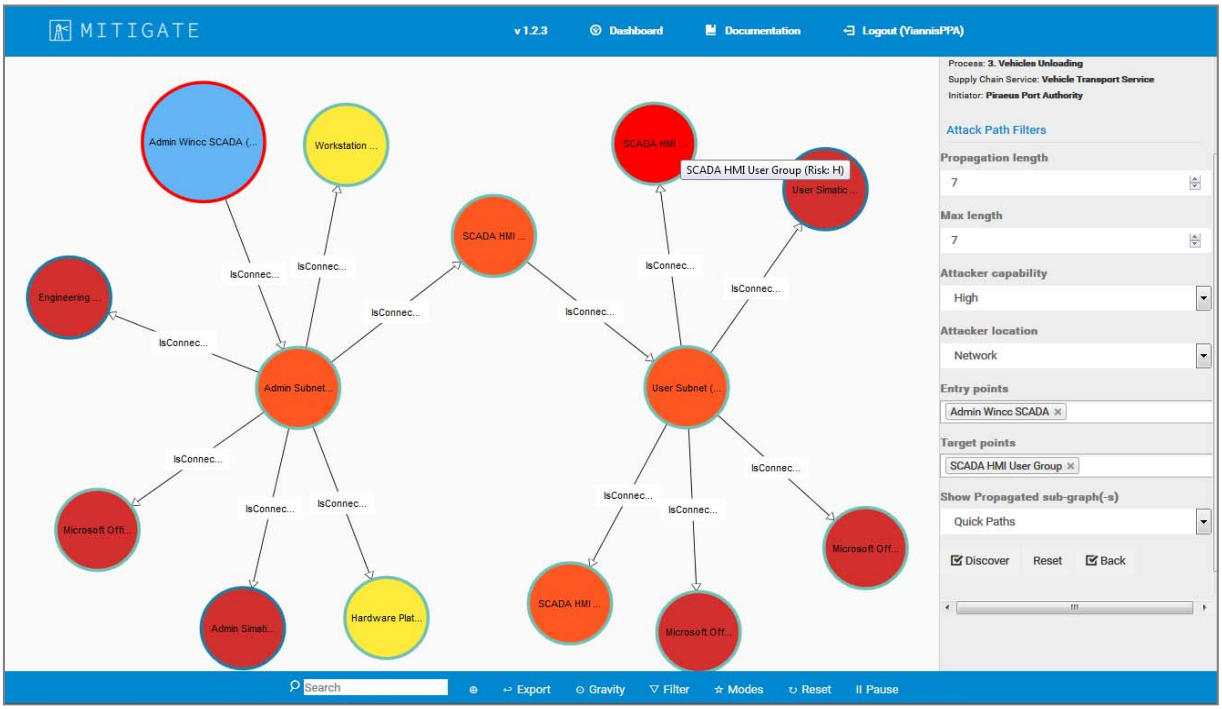

Table 20 : Attack Paths visualization for Q4

No	Asset Chain ($A1 \rightarrow A2 \rightarrow A3 \rightarrow A_X$)	Vulnerability Chain ($V1 \rightarrow V2 \rightarrow V_X$)	Assets' Chain Name	Assets' Chain Product Version	Assets' Chain Vendor	Assets' Chain Vulnerabilities
1	SCADA Security System for Admin Wincc SCADA → Admin Wincc SCADA OS → SCADA HMI Software (User Group)	CVE-2017-4053 → CVE-2016-5744→	SCADA Security System for Admin Wincc SCADA	Macafee Advanced Threat Defence 3.8	Macafee	CVE-2017-4053/ Execute Code
			Admin Wincc SCADA OS	Microsoft Windows 7, sp1	Microsoft	
			SCADA HMI Software (User Group)	simatic_wincc v.7.2	Siemens	CVE-2016-5744 / Obtain Information

Attack scenario Description

The "Human Machine Interface" (HMI), is considered an input-output SCADA device with a panel view for presenting graphically the process data to human operators and allows them to control and monitor the vehicles unloading from the vessels via communication between RTUs or PLCs. An insider disgruntled port employee exploits CVE-2017-4053 vulnerability on the Macafee security antivirus system installed on the "admin Wincc SCADA" (Microsoft Windows 7) that allows the attacker to gain access and the corresponding privileges (McAfee Advanced Threat Defence runs with the privileges of a admin). In this way, he becomes admin gaining access to the Admin Wincc SCADA OS all the vulnerabilities Siemens SIMATIC WinCC v. 7.2, is the HMI software that communicates with http servers via SSL certificate, installed on the "admin Wincc SCADA". SCHANNEL is the standard SSL library that ships with Windows 7, in which the CVE-2014-6321 vulnerability is detected. To this context, the insider is sending to port personnel crafted email notifications regarding the vehicles unloading arrangement and thus he manages to convince them to open and read the crafted contents allowing him to execute arbitrary code remotely compromising the admin Wincc SCADA OS.

Then, the malicious user is able to access the "Human Machine Interface" (SCADA HMI Software (User Group)) and reach and exploit the CVE-2016-5744 vulnerability of the HMI software User group allowing him to read arbitrary WinCC station files and obtain critical information of the vessel's terminal storage geolocation to organize his fraudulent activities.

5 Conclusions

This document contains a large number of categorizations and taxonomies of cyber-threats, some of them with a higher level of standardization and use. Be that as it may, this broad way of categorizing and classifying cyber-risks demonstrates the high complexity of the topic. On the other hand, the statistics shown and the predictable tendencies about cyber-attacks show that the ways of attacking systems with different purposes are increasingly sophisticated. Also, the emergence of new concepts such as the Internet of Things, the Cloud, or mobile applications that have been appearing over the past few years make it foreseeable that "cyber-attackers" adapt to new ways of living and using the technology. There have also been real cases of both malicious cyber-attacks and cyber-incidents in the logistics sector and other critical sectors such as energy. These cases show the great casuistry and diversity associated with cyber-attacks, with different purposes: data theft, political purposes, sabotage, financial gain, industrial espionage, etc. With the current and foreseeable scenario, it is necessary to provide the critical sectors with tools so that they can evaluate the risks, identify threats and establish mitigation measures in their IT systems and networks.

6 References

[1] ENISA: Existing taxonomies, published under Community Projects

[2] http://www.ict-forward.eu/

[3] https://www.researchgate.net/publication/220592994_Extensible_threat_taxonomy_for_critical_infrastructures

[4] http://projects.webappsec.org/f/WASC-TC-v2_0.pdf

[5] https://capec.mitre.org/[2017]

[6] Cyber Threat Intelligence Model: An evaluation of Taxonomies, Sharing Standards and Ontologies within Cyber Threat Intelligence [2017]

[7] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats_catalogue.pdf?__blob=publicationFile&v=1 [2013]

[8] https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html

[9] Mircovic J, Reiher P, A Taxonomy of DDoS Attack and DDoS Defense Mechanisms [2004] available at https://www.eecis.udel.edu/~sunshine/publications/ccr.pdf

[10]ISO, "ISO 28001: Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance", Geneva, Switzerland, 2007.

[11] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf [2012]

[12] http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html#HEAD6 [2003]

[13] https://www.terena.org/activities/tf-csirt/pre-meeting3/charter-incident-taxonomy.pdf

[14] http://archiv.cesnet.cz/doc/techzpravy/2010/otrs-csirt-workflow [2010]

[15] https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[16] https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf [2017]

[17] https://www.sei.cmu.edu/reports/10tn028.pdf [2010]

[18] http://cordis.europa.eu/result/rcn/55021_en.html [2009]

[19] https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c03964615 [2013]

[20] http://www85.homepage.villanova.edu/timothy.ay/MIS2040/OCTAVEthreatProfiles%5B1%5D.pdf [1999]

[21] https://www.researchgate.net/publication/310350401_Threat_Taxonomy_for_Cloud_of_Things [2016]

[22] https://academic.oup.com/comjnl/article/59/11/1612/2433249 [2016]

[23] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.696.3210&rep=rep1&type=pdf [2015]

[24] http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf [2005]

[25] https://www.misp-project.org/taxonomies.html#_information_security_indicators

[26] https://www.misp-project.org/taxonomies.html#_cssa

[27] https://www.misp-project.org/taxonomies.html#_circl

[28] https://www.misp-project.org/taxonomies.html#_csirt_case_classification

[29] https://www.misp-project.org/taxonomies.html#_europol_incident

[30] https://www.misp-project.org/taxonomies.html#_kill_chain

[31] https://www.misp-project.org/taxonomies.html#_ms_caro_malware

[32] https://www.misp-project.org/taxonomies.html#_open_threat

[33] http://veriscommunity.net/

[34] https://www.sans.org/reading-room/whitepapers/incident/malware-101-viruses-32848

[35] https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection/at_download/fullReport

[36] https://www.misp-project.org/taxonomies.html#_veris

[37] https://github.com/MISP/MISP

[38] https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/ENISA_Report%20on%20information%20sharing%20and%20common%20taxonomies%20between%20CERTs%20and%20Law%20Enforcement.pdf

[39] https://www.cert.lv/en/2011/01/incidents

[40] http://www.cert-hungary.hu/en

[41] https://www.europol.europa.eu/sites/default/files/documents/common_taxonomy_for_the_national_network_of_csirts.pdf

[42] http://www.misp-project.org/

[43] https://www.circl.lu

[44] https://www.enisa.europa.eu/publications/ontology_taxonomies

[45] https://www.owasp.org/index.php/Application_Threat_Modeling

[46] Internet Security Threat Report, Volume 22, April 2017, Symantec Corporation.

[47] Facing the cyber-risk challenge, A report by Lloyd's, 20 September 2016. Lloyd's.

[48] https://www.smh.com.au/technology/crime-syndicates-can-track-container-searches-20120328-1vyth.html

[49] https://en.wikipedia.org/wiki/History_of_Target_Corporation

[50] https://www.reuters.com/article/us-clarkson-cyber/uk-shipping-firm-clarkson-reports-cyber-attack-idUSKBN1DT1KO

[51] http://www.portstrategy.com/news101/world/americas/us-port-cyber-attack-thwarted

[52] https://safety4sea.com/countdown-the-top-shipping-stories-of-2017/

[53] http://www.latimes.com/business/technology/la-fi-maersk-cyber-attack-20170629-story.html

[54] https://en.wikipedia.org/wiki/Petya_(malware)

[55] https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

[56] https://www.symantec.com/connect/blogs/taiwan-targeted-new-cyberespionage-back-door-trojan

[57] https://thewire.in/152089/jnpt-indias-largest-container-port-hit-by-global-cyber-attack/

[58] http://www.marinemec.com/news/view,tanker-group-says-it-faced-cyber-attack-in-july_49564.htm

[59] https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware

[60] https://www.darkreading.com/attacks-breaches/chinese-hackers-target-logistics-and-shipping-firms-with-poisoned-inventory-scanners/d/d-id/1297182?

[61] https://www.wired.com/2009/03/feds-hacker-dis/

[62] https://en.wikipedia.org/wiki/Stuxnet

[63] https://thehackernews.com/2017/08/chrome-extension-hacking.html

[64] https://www.kaspersky.com/about/press-releases/2017_shadowpad-how-attackers-hide-backdoor-in-software-used-by-hundreds-of-large-companies-around-the-world

[65] https://www.joc.com/port-news/terminal-operators/maher-terminals/maher-terminals-hits-rough-patch-ny-nj_20130625.html

[66] http://www.columbian.com/news/2017/mar/10/port-of-vancouver-meeting-hindered-by-cyberattack/

[67] https://www.fox.temple.edu/cms/wp-content/uploads/2016/08/Cyber-Physical-Security-PDF.pdf

[68] https://www.imca-int.com/alert/447/failure-of-pipe-handling-system-causes-injuries-and-fatalities/

[69] http://gcaptain.com/report-glitch-caused-collision/

Annex: Repository of threats, countermeasures and simulated scenarios

Contents

i. ENISA Threat Taxonomy

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
1	**Physical attack (deliberate/ intentional)**								12	Physical Theft/Loss /Damage (ENISA Threat Landscape Published 2012)	6	Physical Damage/ Theft/Loss (ENISA Threat Landscape 2013)	10	Physical damage/theft /loss (ENISA Threat Landscape 2014)	Yes		Yes		Threats of intentional hostage human actions
2		***Fraud***													Yes		No		Fraud made by human
3			Fraud by employees												No		No		Fraud made by employees or others who are in relation with entities, that have access to knowledge about entities' information and IT Assets
4		***Sabotage***													Yes		No		Intentional actions (non-fulfillment or defective fulfillment of personal duties) aimed to cause disruption or damage of IT Assets
5		***Vandalism***													Yes		No		Act of physically damage of IT Assets
6		***Theft (devices, storage media and***			Stable (?)	"As was the case with our previous reports, people are people; so, why should it be that	Verizon data breach investigation report 2015								Yes		No		Stealing of information or IT Assets. Robbery

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
		documents)				we expect perfection when it comes to the physical security of their corporate devices? Also (predictably), folks still steal things" (page 45)										
7			Theft of mobile devices (smartphones/ tablets)									Difference	Devices	No		Taking of another person's property in the form of mobile devices for example smartphones, tablets.
8			Theft of fixed hardware		Decreasing (?)	Graph on page 79 showing decrease in number of incidents of data breach due to Theft or loss of computer or drive. From 27 to 21 %	Symantec internet security threat report 20					Difference	Cables	No		Taking of another person's hardware property (except mobile devices), which often contain business-sensitive data.
9			Theft of documents									Yes		No		Stealing documents of private/company archives, often for the purpose of re-sale or to achieve personal benefits.
10			Theft of backups									No		No		Stealing media device, on which copies of essential information are kept.

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
11		***Information leakage/ sharing***									13	Information Leakage (ENISA Threat Landscape 2013)	12	Information leakage (ENISA Threat Landscape 2014)	Yes		No		Sharing information with unauthorised entities. Loss of information confidentiality due to intentional human actions.
12		***Unauthorized physical access / Unauthorised entry to premises***													Yes		No		Unapproved access to facility.
13		***Coercion, extortion or corruption***													Yes		No		Actions caused by coercion, extortion or corruption
14		***Damage from the warfare***													No		No		Threats of direct impact of warfare activities
15		***Terrorists attack***													Yes	Bomb attacks/threats	No		Threats of bombing or other actions that counts as "terrorists attacks"
16	**Unintentional damage / loss of information or IT assets**														Yes		Yes		Threats of unintentional human actions or errors
17		***Information leakage/ sharing due to***			decreasing	Page 11 showing that 25% all data breaches incidents was cause by	Gemalto Breach Level Index 2014												

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference	Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference	Threat description
		human error				accident loss. In 2013, accidental loss accounted for 27% of the breaches.								
					Increasing (in UK)	75% of large organisations and 31% of small businesses suffered staff related security breaches in the last year.Large: Up from 58% a year ago. Small: Up from 22% a year ago. Page 4	HM Government 2015 Information Security Breaches Survey							
18					Increasing	number 3 (with score 17.1%) in top 10, Fig.39, page 49	Verizon data breach investigation report 2015							
			Accidental leaks/sharing of data by employees		Decreasing	Graph on page 79 showing decrease in number of incidents of data breach due to accidentally made data public	Symantec internet security threat report 20					No	No	Unintentional distribution of private or sensitive data to an unauthorized entity by staff member.
19			Leaks of data via mobile applications		Increasing (?)	"The biggest problem identified in this year's research is the negligent or careless employee with multiple mobile devices using commercial cloud apps and working outside the office"	Ponemon: 2015 State of the Endpoint Report: User-Centric Risk	W40						

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
20					Increasing	"Traditional threats increased 6 percentage points between 2013 and 2014, while threats that steal information from the device or track users declined in 2014." page 22	Symantec internet security threat report 20	W39							No		No		Threat of leakage private information using applications for mobile devices.
21			Leaks of data via Web applications	Insecure interfaces (APIs)	decreasing	Unintentional "publishing errors" as fiig. 26 on page 33	Verizon data breach investigation report 2015						3	Web application attacks /Injection attacks (ENISA Threat Landscape 2014)	No		No		Threat of leakage important information using web applications.
22			Leaks of information transferred by network												No		No		Threat of leakage important information by unsecure network traffic.
23		***Erroneous use or administration of devices and systems***		systems and technology failures --> Compatibility systems and technology failures --> Configuration manage											Yes		Yes		Information leakage / sharing / damage caused by users IT Assets misuse (lack of awareness of application features) or wrong / improperly IT Assets configuration or management

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference	Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference	Threat description
				ment Unpatched software (delayed patching processes)										
24			Loss of information due to maintenance errs / operators errors	Technological obsolescence								No	No	Threat of loss of information by incorrectly performed conservation of devices or systems
25			Loss of information due to configuration/ installation error	Inadequate management in complex solution (scale) Routing infrastructure								No	No	Threat of loss of information by errors in installation or system configuration
26			Increasing recover time									No	No	Threat of loss of availability of information by errors in use od backup media and increasing information recovery time
27			Loss of information due to user errors											
28		***Using information from an unreliable source***										Yes	Yes	Bad decision based on unreliable sources of information or

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
																			unchecked information.
29		***Unintentional change of data in an information system***													Yes		Yes		Loss of information integrity due to human error (information system user mistake)

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
30		***Inadequate design and planning or improperly adaptation***		systems and technology failures --> Process design or execution: - Process flow - Process documentation - Roles and responsibilities - Notifications and alerts - Information flow - Escalation of issues - Service level agreements - Task hand-off - Process controls - Status monitoring - Metrics - Periodic review - Process ownership											Difference	Inadequate designs and planning or lack of adaptions	Yes		Threats caused by improperly IT Assets or business processes design (inadequate specifications of IT products, inadequate usability, insecure interfaces, policy/procedure flows, design errors)

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference	Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference	Threat description
				- Supporting processes - Staffing - Funding - Training and development - Procurement systems and technology failures --> Business issues systems and technology failures: - Market conditions - Economic conditions Design errors Inadequate specifications Inadequate usability Outdated procedures Outdated										

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
				risk assessments Outdates Policies															
31		***Damage caused by a third party***													Yes		Yes		Threats of damage of IT Assets caused by third party

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
32			Security failure by third party	systems and technology failures --> Security settings								No		No		Threats of damage of IT Assets caused by breach security regulation by third party
33		***Damages resulting from penetration testing***		systems and technology failures --> Testing								Yes		No		Threats to information systems caused by improperly / inprepare conducting of IT penetration testing
34		***Loss of information in the cloud***										Difference	Loss of information	Yes		Threats of loosing information or data stored in the cloud
35		***Loss of (integrity of) sensitive information***										Yes		Yes		Threats of loosing information or data (or changing) information classified as sensitive
36			Loss of integrity of certificates									No		No		Threat of lossing integrity of certificates used for authorisation services
37		***Loss of devices, storage media and documents***				IBM X-Force 2Q2015 considers this as 7th of Top 8 with score 35%						Difference	Loss	Difference	Loss or destruction of devices, storage media and documents	Threats of the lack of availability (loosing) of IT Assets and documents
38			Loss of devices/ mobile devices									Yes	Devices	No		Threat of loosing mobile devices.

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
39			Loss of storage media												Yes		No		Threat of loosing data-storage medium.
40			Loss of documentation of IT Infrastructure												Yes	Documents	No		Threat of loosing important documentation.
41		***Destruction of records***													Yes	Destruction of records, devices or storage media	Difference	Loss or destruction of devices, storage media and documents	Threats of the lack of availability (destruction) of data and records (information) stored in devices and storage media
42			Infection of removable media												No		No		Threat of loss of important data due to infection of removable media.
43			Abuse of storage												No		No		Threat of loss of records by improperly/unauthorised use of storage devices
44	**Disaster (natural, environmental)**														Yes		Yes		Threats of damage of information assets caused by natural or environmental elements

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
45		***Disaster (natural earthquakes, floods, landslides, tsunamis, heavy rains, heavy snowfalls, heavy winds)***										Difference	Natural disasters --> Earthquake, Floods etc.	Difference	Natural disasters --> Earthquake, Floods etc.	Large scale and large effects natural disasters
46		***Fire***										Difference	Environmental disasters --> Fires	Difference	Environmental disasters --> Fires	Threat of fire
47		***Pollution, dust, corrosion***										Difference	Environmental disasters --> Pollutions, Dust, Corrosions	Difference	Environmental disasters --> Pollutions, Dust, Corrosions	Threat of disruption of work of IT systems (hardware) dur to pollution, dust or corrosion (arising from the air)
48		***Thunder stroke***										Difference	Natural disasters --> Lightning strike	Difference	Natural disasters --> Lightning strike	Threat of damage of IT hardware caused by the thunder strike (the electrical overvoltage)
49		***Water***										No		No		Threat of damage of IT hardware caused by the water
50		***Explosion***										Difference	Environmental disasters --> Explosions	Difference	Environmental disasters --> Explosions	
51		***Dangerous***										Difference	Environmental disasters --> Dangerous	Difference	Environmental disasters -->	

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
		radiation leak											radiation leaks		Dangerous radiation leaks	
52		***Unfavorable climatic conditions***										Difference	Environmental disasters --> Unfavorable climatic conditions	Difference	Environmental disasters --> Unfavorable climatic conditions	Threat of disruption of work of IT systems due to climatic conditions that have the negative effect on hardware
53			Lost of data or accessibility of IT infrastructure in result of extensive humidity									No		No		
54			Lost of data or accessibility of IT infrastructure in result of extensive temperature									No		No		
55		***Major events in the environment***										Difference	Environmental disasters --> Major events in the environment	Difference	Environmental disasters --> Major events in the environment	
56		***Threats from space / Electromagnetic storm***										Difference	Natural disasters --> Electromagnetic storm	Difference	Natural disasters --> Electromagnetic storm	Threats of the negative impact of solar radiation (harmful rays) to a satellites and radio wave communication systems -

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
																			Electromagnetic storm
57		***Wildlife***																	
58	**Failures/ Malfunction**														Yes		Yes		
59		***Failure of devices or systems***		- False sensor data - Privacy and ubiquitous sensors - Sensors and RFID - System maintainability and verifiability systems and technology failures --> Hardware systems and technology failures --> Systems: - Design - Specifications											Yes		Yes		Threat of failure of IT hardware and/or software assets or its parts

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
				- Integration - Complexity Coding practices												
60			Failure of defective data media									Difference	Data centers	Difference	Data centers	
61			Hardware failure									Difference	Servers	Difference	Servers	
62			Failure of applications and services	systems and technology failures --> Software								No		No		
63			Failure of parts of devices (connectors, plug in)									Difference	Network devices	Difference	Network devices	
64		***Failure or disruption of communication links (commun***		- Next generation networks - IPV6 and direct								Yes		Yes		Threat of failure or malfunction of communications links

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
		ication networks)		reachability of hos															
65			Failure of cable networks												Difference	Cable breaks	Difference	Cable breaks	
66			Failure of wireless networks												No		No		
67			Failure of mobile networks												No		No		
68															Additional	Cable cuts	Additional	Cable cuts	
69		***Failure or disruption of main supply***		systems and technology failures --> Supplier failure											Yes		Yes		Threat of failure or disruption of supply required for information systems
70			Failure or disruption of the power supply												Yes		Yes		
71			Failure of cooling infrastructure																
72		***Failure or disruption of service providers (supply chain)***		systems and technology failures: - Emergency services - Service											Yes		Yes		Threat of failure or disruption of thire party services required for proper operation of information systems

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
				dependencies												
73		***Malfunction of equipment (devices or systems)***		systems and technology failures --> Change control								Difference	Malfunctions of parts of devices	Difference	Malfunctions of parts of devices	Threat of malfunction of IT hardware and/or software assets or its parts
74	**Outages**			actions of people --> Outages actions of people: - Inaction - Skills - Knowledge - Guidance								Yes				
75		***Loss of resources***		systems and technology failures: - Capacity - Performance systems and technology failures: - Fuel - Transportation - Utilities								Difference	Lack of resources	Difference	Lack of resources/electricity	Unavailability of resources (supply) required for proper operation of information system

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
76			Loss of electricity												Difference	Lack of physical resources --> Power	Difference	Lack of physical resources --> Power	
77			Cooling outages																
78		***Absence of personnel***													Yes		Yes		Unavailability of key personnel and their competences
79		***Strike***													Yes		Yes		Unavailability of staff due strike (large scale absence of personnel)
80		***Loss of support services***													Yes		Yes		Unavailability of support services required for proper operation of information system
81		***Internet outage***													No		Yes		Unavailability of the Internet connection
82		***Network outage***													Yes	Network outages	Yes		Unavailability of communication links
83			Outage of cable networks												No		No		
84			Outage of wireless networks												No		No		
85			Outages of mobile networks												No		No		
86	**Eavesdropping/ Intercept**														Yes		Yes		Threats that relay on alters of

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
	ion/ Hijacking																		communication between two parties
87		***War driving***													No		Yes		Threat of locating and possible exploite connection to the wireless network
88		***Intercepting compromising emissions***													Yes		Yes		Threat of disclosure transmitted information using interception and analysis of compromising emission
89		***Interception of information***			Increasing	Number 3 in top 9 (with score 18%), fig. 25 on page 32	Verizon data breach investigation report 2015						14	Cyber espionage (ENISA Threat Landscape 2014)	Yes		Yes		Threat of interception of information improperly secured in transmission or improperly actions of staff
90			Corporate Espionage												Yes	Espionage	Yes	Espionage	
91			Nation state espionage		Increasing	"state-sponsored attackers, who carried out 56 of the breaches, or 4%, in 2014. (..) these sources increased from less than 1% in 2013. This is likely to be a continuing trend, as countries launch	Gemalto Breach Level Index 2014												

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
						hacks against each other for political, economic, retaliatory or other reasons" page 12													
					Increasing	"More state-sponsored cyberespionage came to light in 2014." page 61	Symantec internet security threat report 20	W39											
					Increasing	"One of the more popular events of 2014 was a report by FireEye concerning a group called APT28. According to this report, this group may have been supported by the Russian government and was aiming at providing information valuable to that government" page 18	CERT Polska report 2014												
92			Information leakage due to unsecured Wi-Fi, rogue access points												No		No		
93		***Interfering radiation***													Yes		Yes		Threat of failure of IT hardware or transmission

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
																			connection due to electromagnetic induction or electromagnetic radiation emitted from an another source
94		***Replay of messages***													Yes		Yes		Threat in which valid data transmission is maliciously or fraudulently repeated or delayed
95		***Network Reconnaissance, Network traffic manipulation and Information gathering***													No		Yes		Threat of identifying information about network to find security weaknesses
96		***Man in the middle/ Session hijacking***													Yes		Yes		Threats that relay on alters of communication between two parties
97	**Nefarious Activity/ Abuse**				Increasing	Number 5 in top 10 (with score 8,3%), fig. 35, page 41	Verizon data breach investigation report 2015								Yes		Yes		
98		***Identity theft (Identity Fraud/ Account)***		User interface	increasing (dramatically)	"The most common type of attack was identity theft. " "these attacks, which accounted for more than half of the total	Gemalto Breach Level Index 2014		13	Identity Theft (ENISA Threat Landscape Published 2012)	7	Identity Theft/Fraud (ENISA Threat Landscape 2013)	13	Identity theft/fraud (ENISA Threat Landscape 2014)	Yes		Yes	Identity fraud	Threat of identity theft action

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference	Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference	Threat description
						(54%). That's up dramatically from just 20% in 2013" page 12								
99			Credentials stealing trojans	inadequate AAA mechanisms	Increasing	"Over 95% of these incidents involve harvesting credentials from customer devices, then logging into web applications with them" page 42	Verizon data breach investigation report 2015					No	No	
100		***Receive of unsolicited E-mail***										Yes	Difference: Unsolicited & infected e-mail	Threat of receive of unsolicited E-mail that affect for information security and efficienty of work
101			SPAM		Decrease (but number of SPAM urls increased dramatically)	Graph on page 38 shows decreasing trend, however: "New spam URLs and their domains leaped by 380% in Q2. Most of this increase is due to hundreds of thousands of autogenerated or sequential domains dedicated to spam campaigns we discovered after we improved our collection of Realtime	McAfee Labs Threats Report August 2015							

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference	Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference	Threat description
						Blackhole Lists." page 38								
					Stable	"Yet the volume of worldwide spam has remained relatively consistent"	Cisco 2015 Midyear Security Report	W41						
					Increasing (partial)	"Spam volume is increasing in the United States, China, and the Russian Federation, but remained relatively stable in other regions in the first five months of 2015." page 3	Cisco 2015 Midyear Security Report	W41						
					Increasing (snowshoe spam)	"Snowshoe spam, which involves sending low volumes of spam from a large set of IP addresses to avoid detection, is an emerging threat"(..) "Worldwide spam volumes are on the rise, indicating that spam is still a lucrative vector for online criminals" on pages 18 and 19	Cisco Annual Security Report 2015	W41						

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
					Decreasing	Graph on page 12 showing "Overall Email Spam Rate". Drop from 66 to 60%	Symantec internet security threat report 20	W39											
					Stable	Recent IBM X-Force Advanced Research analysis indicates that the threat for spam is growing. However, the graph on page 6 of 2Q2015 shows stable/decreasing. In the same report (page 9) it says that "although the overall spam volume has not changed over the last two years..".	IBM X-Force 2Q2015		10	Spam (ENISA Threat Landscape Published 2012)	10	Spam (ENISA Threat Landscape 2013)	6	Spam (ENISA Threat Landscape 2014)	No		No		
102			Unsolicited infected e-mails		Increasing	The percentage of spam transporting malicious attachments increases	IBM X-Force 2Q2015												
					Increasing	"The most popular method of infection of users in Polish networks are malicious email attachments" page 6	CERT Polska report 2014								No		No		
103		***Denial of service***							6	Denial of Service (ENISA	8	Denial of service (ENISA	5	Denial of service (ENISA Threat	Difference	Denial of service	Yes		Threat of Deny of service type attacks at

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference	Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference	Threat description
									Threat Landscape Published 2012)	Threat Landscape 2013)	Landscape 2014)	attacks (DoS/DDoS)		information systems/services
104			Distributed Denial of network service (DDoS) (network layer attack i.e. Protocol exploitation / Malformed packets / Flooding / Spoofing)		Increasing	Increase in bandwidth volume of 253 Gbps Increase in attack duration 20% over five days. 55% are UDP flood, second SYNC. Single vector (56%) vs. multiple vector attacks.	IMPERVA Global DDoS Threat Landscape Q2 2015					Yes	No	
					Increasing	"6.04% increase in infrastructure layer (Layer 3 & 4) DDoS attack" page 6	Akamai's state of the internet security Q2 2015 report							
					Increasing	"SYN DDoS and TCP DDoS and were the most common scenarios of DDoS attacks."	Kaspersky DDoS Intelligence Report Q2 2015							
105			Distributed Denial of application service (DDoS) (application layer attack i.e. Ping of Death / XDoS /		Increasing	"17.65% increase in application layer (Layer 7) DDoS attacks" page 6	Akamai's state of the internet security Q2 2015 report							
					Increasing (?)	179 K RPS as largest attack (within customers. Need to check other reports).	IMPERVA Global DDoS Threat Landscape Q2 2015							

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
			WinNuke / HTTP Floods)			14% of application level attacks from China.										
					Decreasing	"HTTP DDoS was displaced to the third position" *Also look at* ***https://securelist.com/files/2015/08/ddos_report_q2_en_5.png*** *graph showing large decrease form 30,2 % to 13,8%*	Kaspersky DDoS Intelligence Report Q2 2015									
			Distributed DoS (DDoS) to both network and application services (amplification/reflection methods i.e. NTP/ DNS /…/ BitTorrent)		Increasing	"SSDP amplification – a relatively recent method but gaining in popularity;"	Kaspersky DDoS Intelligence Report Q2 2015									
106					Increasing	"nd quarter of 2015 set a record for the number of distributed denial of service (DDoS) attacks recorded on Akamai's Prolexic Routed network — more than double what was reported in q2 2014" page 5	Akamai's state of the internet security Q2 2015 report									
					Increasing	"Distributed denial-of-service (DDoS) attacks got worse again this year with our reporting partners logging	Verizon data breach investigation report 2015					Difference	Denial of service attacks (DoS/DDoS) --> CDoS	Difference	Application --> XDoS	

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
						double the number of incidents from last year" page 43													
					Stable	"Cybercriminals still use the misconfigured network services like DNS or NTP to launch DDoS attacks" page 5	CERT Polska report 2014												
107		***Malicious code/ software / activity***		Online games	Increasing	IBM X-Force 2Q2015 considers this as 4th of Top 8			2	Worms/Trojans (ENISA Threat Landscape Published 2012)	2	Worms/Trojans (ENISA Threat Landscape 2013)	1	Malicious code: Worms/Trojans (ENISA Threat Landscape 2014)	No		Yes		Threat of malicious code or software execution
					Decreasing	"Meanwhile, venerable old keylogger malware has been in decline, having only been observed in about 5% of the breaches recorded in this year's sample" page 5	Verizon data breach investigation report 2015												
			Abuse of resources			Malware using Bitcoin miners which are abusing CPU/memory resources.	https://blog.fortinet.com/2016/06/14/obfuscated-bitcoin-miner-propagates-through-ftp-using-password-dictionary https://www.cryptocoinsnews.com/new-malware-mines-bitcoin/												

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
108			Search Engine Poisoning						15	Search Engine Poisoning (ENISA Threat Landscape Published 2012)					Difference	DNS manipulations DNS spoofing DNS poisoning	Difference	Manipulation of information --> DNS manipulation --> DNS poisoning	
109			Exploitation of fake trust of social media		Decreasing (number of URLs in social media)	Graph on page 12 showing "Average Number of Phishing URLs on Social Media" in 2013 and 2014	Symantec internet security threat report 20	W39							No		No		
					Increasing	First, the increased use of social media has provided a quintessential goldmine of personal data for perpetrators	FBI 2014 Internet Crime Report	W40											
					Increasing (fake trust)	"This means that more and more users are clicking links embedded in emails,"	TrendMicro Report: A Rising Tide: New Hacks Threaten Public Technologies	W40											
					Increasing (fake trust)	Graph on page 12 shows great increase in number of Manually Shared Social Media Scams	Symantec internet security threat report 20	W39											
110			Worms/ Trojans		Increasing	IBM X-Force 1Q2015 foresees malware as "one of the most common attack types". Page 9	IBM x-Force 2Q2015 and IBM x-Force 1Q2015												

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
					Increasing	"In 2014, we observed the rise of Tinba, VMZeuS, Kronos and IFSB families" page 5	CERT Polska report 2014					Difference	Malware and viruses: - Trojans - Worms	Difference	Badware: - Trojans - Worms	
111			Rootkits									Difference	Malware and viruses--> Rootkits	Difference	Badware --> Rootkit	
112			Mobile malware		Increasing	"The total number of mobile malware samples grew 17% in Q2" and graphs on page 31	McAfee Labs Threats Report August 2015									
					Increasing	" In fact, 75 percent of respondents (an increase from 68 percent in last year's study) believe their mobile endpoints have been the target of malware over the past 12 months."	Ponemon: 2015 State of the Endpoint Report: User-Centric Risk	W40								
113					Increasing	Various info-graphics on page 10 showing i.e. Increase of cumulative android malware from 231 to 277 malware families.	Symantec internet security threat report 20	W39								
114					Decreasing	Figure 14 on page 18 shows drop from over 60k infections in September 2014 to below 10k in January of 2015	Verizon data breach investigation report 2015					No		No		

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference	Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference	Threat description
115			Infected trusted mobile apps									No	No	
116			Elevation of privileges									No	No	
117			Web application attacks / injection attacks (Code injection: SQL, XSS)		Increasing	Numbers 3 (19%) and 7 (6,3%) in top 10, figure 35, page 41	Verizon data breach investigation report 2015							
					Increasing	"Web threats got bigger and much more aggressive in 2014 (..) The web presented an incredibly threatening landscape in 2014, a trend set to continue in 2015" on page 32	Symantec internet security threat report 20	W39						
					Increasing	"Including events based on Shellshock nearly doubled the number of attack events we analyzed this quarter," page 26	Akamai's state of the internet security Q2 2015 report							
					Decreasing (Local File Inclusion only)	"In contrast, lfi attacks dropped significantly this quarter. In the last week of q1, we saw nearly 75 million lfi alerts due to an attack on a pair of large retail customers, while	Akamai's state of the internet security Q2 2015 report							

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
						in all of q2 we only saw 63 million alerts."													
					Increasing	"in all of these attacks: ATS (Automatic Transfer Script) used to host the webinjects and provide an easy platform for attackers to manage the money transfers." page 13	CERT Polska report 2014		3	Code Injection (ENISA Threat Landscape Published 2012)	3	Code Injection (ENISA Threat Landscape 2013)			Difference	Exploitation of software bugs --> Validation --> Input--> SQL injections	No		
118			Spyware or deceptive adware		Increasing	"Adware is an increasingly popular option for app publishers, growing from almost 300,000 apps in 2013 to more than 410,000 in the first three quarters of 2014 alone" page 19	Verizon data breach investigation report 2015								Difference	Malware and viruses: - Spyware Potentially unwanted software: - Adware	Difference	Badware: - Spyware - Adware	
119			Viruses																
120			Rogue security software/ Rogueware/ Scareware						9	Rogueware/Scareware (ENISA Threat Landscape Published 2012)	11	Rogueware/ Ransomware/ Scareware (ENISA Threat Landscape 2013)	15	Ransomware/ Rogueware/Scareware (ENISA Threat Landscape 2014)	Difference	Malware and viruses: - Scareware; - Roguware	Difference	Badware: - Scareware - Rogueware	
121					Increasing	"crypto-ransomware continues to grow, setting	Symantec intelligence report August 2015	W39											

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
						another monthly high for the year." on page 3													
					Increasing	"Ransomware attacks grew 113 percent in 2014, driven by more than a 4,000 percent increase in crypto-ransomware attacks" page 7	Symantec internet security threat report 20	W39											
					Decreasing (slowly)	"Ransomware attacks grew 113 percent in 2014, driven by more than a 4,000 percent increase in crypto-ransomware attacks" page 7	TrendMicro Report: A Rising Tide: New Hacks Threaten Public Technologies												
					Increasing	"After many years of evolution, ransomware has emerged as one of the most troublesome malware categories of our time." at first paragraph	Symantec Official Blog: The dawn of ransomwear: How ransomware could move to wearable devices	W40											
					Increasing	"Ransomware continues to grow very rapidly—with the number of new ransomware samples rising 58% in Q2" page 35	McAfee Labs Threats Report August 2015												

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference	Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference	Threat description
122			Exploits/ Exploit Kits		Increasing	" Infected machines can be utilized to perform new attacks (..) or to provide direct financial benefit to the attacker (such is the case with ransomware, data extraction, social engineering attacks on online banking users).(..). Both of these malware attack scenarios are serious threats" page 11	CERT Polska report 2014					No	No	
					Increasing	"We saw a 67% growth in the overall exploit-kit-related detection numbers quarter over quarter." on page 26	TrendMicro Report: A Rising Tide: New Hacks Threaten Public Technologies							
					Increasing (Office macros)	"Adversaries are once again using Microsoft Office macros to deliver malware. It's an old tactic that fell out of favor, but it's being taken up again as malicious actors seek new ways to thwart security	Cisco 2015 Midyear Security Report	W41						

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
						protections." page 3													
					Increasing (Flash)	"Exploits of Adobe Flash vulnerabilities are increasing. They are regularly integrated into widely used exploit kits such as Angler and Nuclear" page 3	Cisco 2015 Midyear Security Report	W41											
					Decreasing (Java only)	"Continuing a trend covered in the Cisco 2015 Annual Security Report, exploits involving Java have been on the decline in the first half of 2015". page 3	Cisco 2015 Midyear Security Report	W41											
					Stable (?)	Graph on page 10 showing that exploit kits are notable malware (no numbers were presented).	McAfee Labs Threats Report August 2015		4	Exploit Kits (ENISA Threat Landscape Published 2012)	4	Exploit Kits (ENISA Threat Landscape 2013)	8	Exploit kits (ENISA Threat Landscape 2014)	No		No		
123		***Social Engineering***			Increasing	IBM X-Force 2Q2015 considers this as 2nd of Top 8													
124			Phishing attacks			CozyDukes is using social engineering to get initial foothold in targeted organizations. They include	Kaspersky DDoS Intelligence Report Q2 2015		7	Phishing (ENISA Threat Landscape Published 2012)	9	Phishing (ENISA Threat Landscape 2013)	7	Phishing (ENISA Threat Landscape 2014)	Yes		No		

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference	Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference	Threat description
						high profile legitimate sites that host a ZIP archive.								
					Same level	Graph on page 7 shows that within last year there were months where phishing rate was 1:647 and months with rate 1:2666, but generally it is at about 1:2000 rate.	Symantec intelligence report August 2015							
					Increasing	"has made phishing a favorite tactic of state-sponsored threat actors and criminal organizations, all with the intent to gain an initial foothold into a network." page 12	Verizon data breach investigation report 2015							
					Increasing	"Phishing has also been on the rise since 2011, although the rate of growth has slowed in the last year" page 5	Verizon data breach investigation report 2015							
125			Spear phishing attacks		Increasing	"In 2014, attackers continued to breach networks with highly targeted spear-phishing attacks, which increased	Symantec internet security threat report 20	W39						

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
						eight percent overall." page 6													
					Decreasing (Spear phishing emails only)	Graph on page 13 showing Spear Phishing Emails per Day from 83 to 73	Symantec internet security threat report 20	W39											
					Increasing	"The biggest increase is in zero day attacks, APTs and spear phishing."	Ponemon: 2015 State of the Endpoint Report: User-Centric Risk	W40											
					Increasing	APT CozyDuke from Duke family, including anti-detection techniques and encryption. It is remarkable that this malware users social engineering techniques with some of the spear-fishing containing links to hacked websites. Naikon APT: this apt targets south-east Asia. It is based on a spear-phishing mails.	Kaspersky threat evolution q2 216											
126		***Abuse of Information Leakage***							14	Abuse of Information Leakage (ENISA Threat Landscape Published 2012)					Yes		Yes		? What is difference between others Physical attack (deliberate/ intentional)?

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference	Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference	Threat description
127			Leakage affecting mobile privacy and mobile applications		decreasing	"data breaches involving mobile devices should not be in any top-whatever list" page 20	Verizon data breach investigation report 2015					No	No	
128			Leakage affecting web privacy and web applications									No	No	
129			Leakage affecting network traffic									No	No	
130			Leakage affecting cloud computing									No	No	
131		***Generation and use of rogue certificates***										Yes	Yes	Threat of use of rogue certificates
132			Loss of (integrity of) sensitive information									No	No	
133			Man in the middle/ Session hijacking									No	No	

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference	Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference	Threat description
134			Social Engineering / signed malware (e.g. install fake trust OS updates – signed malware)									No	No	
135			Fake SSL certificates											
136		***Manipulation of hardware and software***			Increasing	IBM X-Force 2Q2015 considers this as 3rd of Top 8						Yes	Yes	Threat of unauthorized manipulation of hardware and software
137			Anonymous proxies									No	No	
138			Abuse of computing power of cloud to launch attacks (cybercrime as a service)			IBM X-Force 2Q2015 considers this as 8th of Top 8						No	No	
			Abuse of vulnerabilities, 0-day vulnerabilities		Increasing	"The biggest increase is in zero day attacks, APTs and spear phishing."	Ponemon: 2015 State of the Endpoint Report: User-Centric Risk	W40						
					Decreasing (Java only)	" We sa a significiant decrese in the exploitation of Java vulnerabilities in	2015 Trustwave Global Security Report	W41						

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference	Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference	Threat description
						2014, making up just 14.5 percent of exploits encountered by trustwave compared to 78 percent the previous year."								
139					Increasing	"August was a big month for zero-day vulnerabilities, in which a total of 11 were reported. This is by far the largest number disclosed in a given month to-date." page 3	Symantec intelligence report August 2015	W39				No	No	
140			Access of web sites through chains of HTTP Proxies (**Obfuscation**)									No	No	
141			Access to device software									No	No	
142			Alternation of software									No	No	unauthorized modifications to code or data, attacking its integrity
143			Rogue hardware											

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
144		***Manipulation of information***										Yes		Yes		Threat of intentional data manipulation to mislead information systems or somebody or to cover other nefarious activities (loss of integrity of information)
145			Repudiation of actions									Difference	Eavesdropping/Interception/Hijacking --> Repudiation of actions	Difference	Eavesdropping/Interception/Hijacking --> Repudiation of actions	
146			Address Space hijacking (IP prefixes) Routing table manipulation													
147			DNS poisoning / DNS spoofing / DNS Manipulations		Increasing	"We saw an increase in the number of DNS changer detections, particularly in Brazil."	TrendMicro Report: A Rising Tide: New Hacks Threaten Public Technologies	W40								
148			Falsification of record									Yes		Difference	Nefarious Activity/Abuse --> Falsification of records	
149			AS hijacking													
150			AS manipulation													

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
151			Falsification of configurations																
152		***Misuse of audit tools***													No		Yes		Threat of nefarious actions with use of audit tools (discovery security weaknesses in information systems)
153		***Misuse of information/ information systems (including mobile apps)***			Increasing	1) Number 4 in top 9 (with 18%), fig. 25 on page 32 2) "This year, we saw more incidents involving the end user than ever before" page 46	Verizon data breach investigation report 2015								Yes		No		Threat of nefarious action due to misuse of information / information systems
154		***Unauthorized activities***																	
155			Unauthorized use or administration of devices and systems		Increasing	IBM X-Force 2Q2015 calls this threat as 1st of top 8 security threats													
156			Unauthorized use of software																
157			Unauthorized access to the informati																

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
			on systems / networks (IMPI Protocol / DNS Register Hijacking)																
158			Network Intrusion																
159			Unauthorized changes of records																
160		***Unauthorized installation of software***																	Threat of unauthorized installation of software
161			Web based attacks (Drive-by download / malicious URLs / Browser based attacks)		Increasing	"Web-based attacks are growing increasingly sophisticated. " on page 61	Symantec internet security threat report 20	W39	1	Drive-by exploits (ENISA Threat Landscape Published 2012)	1	Drive-by Downloads (ENISA Threat Landscape 2013)	2	Web-based attacks (ENISA Threat Landscape 2014)	Difference	Unauthorized activities --> Unauthorized installation of software	Yes		
					Stable (excluding Drive-by-Download) ?	Graph on page 10 showing this is notable malware (no numbers were present)	McAfee Labs Threats Report August 2015	W39											
162		***Compromising confidential information (data breaches)***			Increasing	"The number of breaches increased 23 percent in 2014. Attackers were responsible for the majority of these breaches" page 16	Symantec internet security threat report 20	W39											
					Increasing	"Clearly, the numbers were up in 2014. Data breaches totaled	Gemalto Breach Level Index 2014		8	Compromising Confidential	12	Data Breaches (ENISA Threat	9	Data breaches (ENISA Threat Landscape 2014)	Yes		Yes		Threat of data breach

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
						1,540, up 46% from the 1,056 in 2013" page 3				Information (ENISA Threat Landscape Published 2012)		Landscape 2013)							
					Increasing	"Data breaches are still a significant issue, since the number of breaches increased 23 percent and attackers were responsible for the majority of these breaches" page 5	Symantec internet security threat report 20	W39											
						IBM X-Force 2Q2015 defines Insider Threat as being deliberate, accidental, from both insiders, ex-insiders and quasi-insiders. This is in fact a very "inclusive" definitions. It argues that 55% of all attacks emanate from persons with insider access to organizations.	IBM X-Force 2Q2015					11	Insider threat (ENISA Threat Landscape 2014)					
163		***Hoax***													Difference	Social engineering --> Pretexting/hoax	Yes		Threat of disruption of work due to False rumor and/or a fake warning
164			False rumor and/or a																

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference	Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference	Threat description
			fake warning											
165		***Remote activity (execution)***										Yes	Yes	Threat of remote activity over controled IT Assets
166			Remote Command Execution									No	No	
167			Remote Access Tool (RAT)			Naikon APT is using a RAT wotj 48 commands.	Kaspersky threat evolution q2 216							
168			Botnets / Remote activity		Same percentage of primitive DDoS bots (I need to analyze this further) as in previous years.	There is a shift from search engine impersonator due to existing defences (ASN verification) Higher overall deversity in DDoS bots user-agent variants, with top 10 covering 43% of attacks.	IMPERVA Global DDoS Threat Landscape Q2 2015							
					Decreasing	"The number of bots declined by 18 percent in 2014." on page 88	Symantec internet security threat report 20							
					Decrease (?)	"That said, DDoS attack scripts on the application side have been shifting more towards the use of non-botnet based resources, such as attack scripts that	Akamai's state of the internet security Q2 2015 report							

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
						leverage open proxies on the Internet" page 15													
					Stable	"C&C statistics are almost the same as last year's." page 7	CERT Polska report 2014												
						"(..)this is evidence that the botnet has been arranged by the cybercriminals to launch large-scale DDoS attacks."	Kaspersky DDoS Intelligence Report Q2 2015		5	Botnets (ENISA Threat Landscape Published 2012)	5	Botnets (ENISA Threat Landscape 2013)	4	Botnets (ENISA Threat Landscape 2014)	Difference	Malware and viruses --> Botnets	Difference	Badware --> Botnets	
						IBM X-Force 2Q2015 considers this as 5th of Top 8 (with score of 36%)													
169		***Targeted attacks (APTs etc.)***			Increasing	"Advanced persistent/targeted attacks increased dramatically"	Ponemon: 2015 State of the Endpoint Report: User-Centric Risk	W40											
					Increasing	"last year we also observed an increase in APT attacks," page 5	CERT Polska report 2014		11	Targeted Attacks (ENISA Threat Landscape Published 2012)	14	Targeted Attacks (ENISA Threat Landscape 2013)			Difference	Timescales --> Targeted attacks/advanced persistent threats	Yes		Threat of sophisticated targetes attack with combination of many attack techniques
170			Mobile malware												No		No		
171			Spear phishing attacks												No		No		
172			Installation of sophisticated and			"Fast forward to today, and RAM scraping has grown up in a big way." page 5	Verizon data breach investigation report 2015												

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference	Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference	Threat description
			targeted malware		Increasing	"The McAfee Labs malware zoo grew 12% in the most recent quarter. It now contains more than 433 million samples." page 33	McAfee Labs Threats Report August 2015	W39						
					Increasing	"The rate of malware has steadily increased"	Ponemon: 2015 State of the Endpoint Report: User-Centric Risk	W40						
					Increasing - POS	Graph on page 9 showing number of PoS malware detections (1Q 2014–2Q 2015). Nearly doubled this year.	TrendMicro Report: A Rising Tide: New Hacks Threaten Public Technologies	W40						
					Decreasing (Education sector)	"Malware related events in the education sector dropped from 42% to 35%"	2015 NTT Group Global Threat Intelligence Report	W41						
					Increasing	"Non-targeted attacks still make up the majority of malware, which increased by 26 percent in 2014." page 7	Symantec internet security threat report 20	W39						
					Increasing	"An interesting new category of malware threats made their debut: malware that changed the bank account number either in the Windows clipboard	CERT Polska report 2014					No	No	

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012		ENISA 2013		ENISA 2014		Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
						(VBKlip) or in the browser's memory (Banatrix). " page 5													
173			Watering Hole attacks		Increasing (?)	"Attackers also perfected watering hole attacks, making each attack more selective by infecting legitimate websites, monitoring site visitors and targeting only the companies they wanted to attack." page 6	Symantec internet security threat report 20	W39			15	Watering Hole (ENISA Threat Landscape 2013)			No		No		
174		***Failed of bussines process***													No				
175		***Brute force***																	
176		***Abuse of authorizations***																	
177	**Legal**														Yes		Yes		
178		***Violation of laws or regulations / Breach of legislation***													Yes		Yes		Threat of finacial or legal penatly or lost of trust of customers and collaborators due to violation of law or regulations
179		***Failure to meet contractual requirements***													Yes		Yes		Threat of finacial penatly or lost of trust of customers and collaborators

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference		Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference		Threat description
																due to failure to meet contractual requirements
180			Failure to meet contractual requirements by third party									No		No		
181		***Unauthorized use of IPR protected resources***										No		No		Threat of finacial or legal penatly or lost of trust of customers and collaborators due to improper/illegal use of copyrights material
182			Illegal usage of File Sharing services									No		No		
183		***Abuse of personal data***										Difference	Nefarious Activity/Abuse --> Abuse of personal data	Difference	Nefarious Activity/Abuse --> Abuse of personal data	Threat of illegal use personal data
184		***Judiciary decisions /court orders***		Value imbalance exploitations - Re-entries - Reputation lag exploitations -												

Nº	High Level Threats	Threats	Threat details	Exploit	Trends	Comments	References	Work Week	ENISA 2012	ENISA 2013	ENISA 2014	Threat Landscape and Good Practice Guide for Internet Infrastructure Yes/No/Additional/Difference	Threat Landscape and Good Practice Guide for Smart Home and Converged Me… Yes/No/Additional/Difference	Threat description
				Proliferation - Collusions - Discriminations - Playbooks - Unfair ratings - Sybil attacks										

ii. WASC Threat Classification

Threat Type	Threat	Threat details
Attack	Abuse of Functionality	Abuse of Functionality is an attack technique that uses a web site's own features and functionality to attack itself or others.
Attack	Brute Force	A brute force attack is a method to determine an unknown value by using an automated process to try a large number of possible values.
Attack	Buffer Overflow	A Buffer Overflow is a flaw that occurs when more data is written to a block of memory, or buffer, than the buffer is allocated to hold
Attack	Content Spoofing	Content Spoofing is an attack technique that allows an attacker to inject a malicious payload that is later misrepresented as legitimate content of a web application.
Attack	Credential/Session Prediction	Credential/Session Prediction is a method of hijacking or impersonating a web site user.
Attack	Cross-Site Scripting	Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance.
Attack	Cross-Site Request Forgery	A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim
Attack	Denial of Service	Denial of Service (DoS) is an attack technique with the intent of preventing a web site from serving normal user activity.
Attack	Fingerprinting	The most common methodology for attackers is to first footprint the target's web presence and

Threat Type	Threat	Threat details
		enumerate as much information as possible.
Attack	Format String	Format String Attacks alter the flow of an application by using string formatting library features to access other memory space.
Attack	HTTP Response Smuggling	HTTP response smuggling is a technique to "smuggle" 2 HTTP responses from a server to a client, through an intermediary HTTP device that expects (or allows) a single response from the server.
Attack	HTTP Response Splitting	In the HTTP Response Splitting attack, there are always 3 parties (at least) involved: • Web server, which has a security hole enabling HTTP Response Splitting • Target - an entity that interacts with the web server perhaps on behalf of the attacker. Typically this is a cache server forward/reverse proxy), or a browser (possibly with a browser cache). • Attacker - initiates the attack
Attack	HTTP Request Smuggling	HTTP Request Smuggling is an attack technique that abuses the discrepancy in parsing of non RFC compliant HTTP requests between two HTTP devices (typically a front-end proxy or HTTP-enabled firewall and a back-end web server) to smuggle a request to the second device "through" the first device.
Attack	HTTP Request Splitting	HTTP Request Splitting is an attack that enables forcing the browser to send arbitrary HTTP requests,

Threat Type	Threat	Threat details
		inflicting XSS and poisoning the browser's cache.
Attack	Integer Overflows	An Integer Overflow is the condition that occurs when the result of an arithmetic operation, such as multiplication or addition, exceeds the maximum size of the integer type used to store it. When an integer overflow occurs, the interpreted value will appear to have “wrapped around” the maximum value and started again at the minimum value, similar to a clock that represents 13:00 by pointing at 1:00.
Attack	LDAP Injection	LDAP Injection is an attack technique used to exploit web sites that construct LDAP statements from user-supplied input.
Attack	Mail Command Injection	Mail Command Injection is an attack technique used to exploit mail servers and webmail applications that construct IMAP/SMTP statements from user-supplied input that is not properly sanitized
Attack	Null Byte Injection	Null Byte Injection is an active exploitation technique used to bypass sanity checking filters in web infrastructure by adding URL-encoded null byte characters (i.e. %00, or 0x00 in hex) to the user-supplied data. This injection process can alter the intended logic of the application and allow malicious adversary to get unauthorized access to the system files.
Attack	OS Commanding	OS Commanding is an attack technique used for unauthorized execution of operating system commands.

Threat Type	Threat	Threat details
Attack	Path Traversal	The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory.
Attack	Predictable Resource Location	Predictable Resource Location is an attack technique used to uncover hidden web site content and functionality. By making educated guesses via brute forcing an attacker can guess file and directory names not intended for public viewing.
Attack	Remote File Inclusion (RFI)	Remote File Include (RFI) is an attack technique used to exploit "dynamic file include" mechanisms in web applications.
Attack	Routing Detour	The WS-Routing Protocol (WS-Routing) is a protocol for exchanging SOAP messages from an initial message sender to an ultimate receiver, typically via a set of intermediaries.
Attack	Session Fixation	Session Fixation is an attack technique that forces a user's session ID to an explicit value. Depending on the functionality of the target web site, a number of techniques can be utilized to "fix" the session ID value.
Attack	SOAP Array Abuse	XML SOAP arrays are a common target for malicious abuse.
Attack	SSI Injection	SSI Injection (Server-side Include) is a server-side exploit technique that allows an attacker to send code into a web application, which will later be executed locally by the web server.
Attack	SQL Injection	SQL Injection is an attack technique used to exploit applications that

Threat Type	Threat	Threat details
		construct SQL statements from user-supplied input. When successful, the attacker is able to change the logic of SQL statements executed against the database.
Attack	URL Redirector Abuse	URL redirectors represent common functionality employed by web sites to forward an incoming request to an alternate resource
Attack	XPath Injection	XPath Injection is an attack technique used to exploit applications that construct XPath (XML Path Language) queries from user-supplied input to query or navigate XML documents.
Attack	XML Attribute Blowup	XML Attribute Blowup is a denial of service attack against XML parsers. The attacker provides a malicious XML document, which vulnerable XML parsers process in a very inefficient manner, leading to excessive CPU load.
Attack	XML External Entities	This technique takes advantage of a feature of XML to build documents dynamically at the time of processing.
Attack	XML Entity Expansion	The XML Entity expansion attack, exploits a capability in XML DTDs that allows the creation of custom macros, called entities, that can be used throughout a document.
Attack	XML Injection	XML Injection is an attack technique used to manipulate or compromise the logic of an XML application or service
Attack	XQuery Injection	XQuery Injection is a variant of the classic SQL injection attack against the XML XQuery Language.
Weakness	Insufficient Authentication	Insufficient Authentication occurs when a web site permits an

Threat Type	Threat	Threat details
		attacker to access sensitive content or functionality without having to properly authenticate.
Weakness	Insufficient Authorization	insufficient Authorization results when an application does not perform adequate authorization checks to ensure that the user is performing a function or accessing data in a manner consistent with the security policy
Weakness	Insufficient Transport Layer Protection	Insufficient transport layer protection allows communication to be exposed to untrusted third-parties, providing an attack vector to compromise a web application and/or steal sensitive information
Weakness	Information Leakage	Information Leakage is an application weakness where an application reveals sensitive data, such as technical details of the web application, environment, or user-specific data.
Weakness	Improper Filesystem Permissions	Improper filesystem permissions are a threat to the confidentiality, integrity and availability of a web application.
Weakness	Improper Input Handling	Improper input handling is one of the most common weaknesses identified across applications today. Poorly handled input is a leading cause behind critical vulnerabilities that exist in systems and applications.
Weakness	Improper Output Handling	Output handling refers to how an application generates outgoing data. If an application has improper output handling, the output data may be consumed leading to vulnerabilities and actions never intended by the application developer.

Threat Type	Threat	Threat details
Weakness	Insufficient Session Expiration	Insufficient Session Expiration occurs when a Web application permits an attacker to reuse old session credentials or session IDs for authorization
Weakness	Insecure Indexing	Insecure Indexing is a threat to the data confidentiality of the web-site. Indexing web-site contents via a process that has access to files which are not supposed to be publicly accessible has the potential of leaking information about the existence of such files, and about their content.
Weakness	Insufficient Password Recovery	Insufficient Password Recovery is when a web site permits an attacker to illegally obtain, change or recover another user's password. Conventional web site authentication methods require users to select and remember a password or passphrase.

Table 21 – WASC threat classification

iii. CAPEC - Common Attack Pattern Enumeration and Classification

Attack mechanism	Meta Attack Pattern	Standard Attack Pattern	Detailed Attack Pattern
Collect and Analyze Information	**Excavation**	Collect Data from Common Resource Locations	Detect Unpublicized Web Pages
			Detect Unpublicized Web Services
			Screen Temporary Files for Sensitive Information
			Accessing/Intercepting/Modifying HTTP Cookies
		Dumpster Diving	
		Query System for Information	Directory Indexing
			Fuzzing for garnering J2EE/.NET-based stack traces, for application mapping
			Fuzzing and observing application log data/errors for application mapping
			Fuzzing for garnering other adjacent user/sensitive data
			Cross-Domain Search Timing
			WSDL Scanning
		Pull Data from System Resources	Probe iOS Screenshots -
			Probe Application Memory
		Obtain Data via Utilities	Dump Password Hashes
		Collect Data as Provided by Users	Capture Credentials via Keylogger
	Interception	Sniffing Attacks	Sniffing Network Traffic
			Accessing/Intercepting/Modifying HTTP Cookies
			Cellular Traffic Intercept
			Sniff Application Code
			Harvesting Usernames or UserIDs via Application API Event Monitoring

Attack mechanism	Meta Attack Pattern	Standard Attack Pattern	Detailed Attack Pattern
		Intent Intercept	Activity Hijack
	Footprinting		Explore for Predictable Temporary File Names
		Host Discovery	ICMP Echo Request Ping
			ICMP Address Mask Request
			ICMP Timestamp Request
			ICMP Information Request
			TCP ACK Ping
			UDP Ping
			TCP SYN Ping
			iFi MAC Address Tracking
			WiFi SSID Tracking
			Cellular Broadcast Message Request
			Signal Strength Tracking
		Port Scanning	TCP SYN Scan
			TCP Connect Scan
			TCP FIN scan
			TCP Xmas Scan
			TCP Null Scan
			TCP ACK Scan
			TCP Window Scan
			TCP RPC Scan
			UDP Scan
		Network Topology Mapping	Enumerate Mail Exchange (MX) Records
			DNS Zone Transfers
			Traceroute Route Enumeration

Attack mechanism	Meta Attack Pattern	Standard Attack Pattern	Detailed Attack Pattern
		Malware-Directed Internal Reconnaissance	
			Process Footprinting
			Services Footprinting
			Account Footprinting
			Group Permission Footprinting
			Owner Footprinting
		Owner Footprinting	Security Software Footprinting
	Reverse Engineering	White Box Reverse Engineering	Reverse Engineer an Executable to Expose Assumed Hidden Functionality or Content
			Read Sensitive Strings Within an Executable
			Lifting Sensitive Data Embedded in Cache
			Retrieve Embedded Sensitive Data
			Smudge Attack
		Black Box Reverse Engineering	Analysis of Packet Timing and Sizes -
			Electromagnetic Side-Channel Attack
			Compromising Emanations Attack
	Protocol Analysis	Cryptanalysis	Padding Oracle Crypto Attack
			Cryptanalysis of Cellular Encryption
	Fingerprinting	Active OS Fingerprinting	IP ID Sequencing Probe
			IP 'ID' Echoed Byte-Order Probe
			IP (DF) 'Don't Fragment Bit' Echoing Probe
			TCP Timestamp Probe
			TCP Sequence Number Probe
			TCP (ISN) Greatest Common Divisor Probe

Attack mechanism	Meta Attack Pattern	Standard Attack Pattern	Detailed Attack Pattern
			TCP (ISN) Counter Rate Probe
			TCP (ISN) Sequence Predictability Probe
			TCP Congestion Control Flag (ECN) Probe
			TCP Initial Window Size Probe
			TCP Options Probe
			TCP 'RST' Flag Checksum Probe
			ICMP Error Message Quoting Probe
			ICMP Error Message Echoing Integrity Probe
			ICMP IP Total Length Field Probe
			ICMP IP 'ID' Field Error Message Probe
		Passive OS Fingerprinting	
		Application Fingerprinting	Web Application Fingerprinting
			Scanning for Vulnerable Software
			Browser Fingerprinting
			AJAX Fingerprinting
	Information Elicitation	Pretexting	Pretexting via Customer Service
			Pretexting via Tech Support
			Pretexting via Delivery Person
			Pretexting via Phone
Inject Unexpected Items	Parameter Injection	Email Injection	Using Meta-characters in E-mail Headers to Inject Malicious Payloads
		Format String Injection	
		Reflection Injection	
		Command Delimiters	HTTP Parameter Pollution (HPP)

Attack mechanism	Meta Attack Pattern	Standard Attack Pattern	Detailed Attack Pattern	
			Flash Parameter Injection	
		Flash Injection	Cross-Site Flashing	
		Argument Injection		
	Code Inclusion	Local Code Inclusion	PHP Local File Inclusion	
		Remote Code Inclusion	Server Side Include (SSI) Injection	
			PHP Remote File Inclusion	
			WebView Injection	
	Resource Injection		Cellular Data Injection	
	Code Injection	Embedding Scripts within Scripts		
		File Content Injection	Overflow Binary Resource File	
			Using Meta-characters in E-mail Headers to Inject Malicious Payloads	
		Generic Cross-Browser Cross-Domain Theft		
		Cross-Site Scripting (XSS)	DOM-Based XSS	XSS Targeting Non-Script Elements
				XSS Targeting Error Pages
				XSS Using Alternate Syntax
				XSS Targeting HTML Attributes
				XSS Targeting URI Placeholders
				XSS Using Doubled Characters
				XSS Using Invalid Characters
				XSS Through HTTP Query Strings
				XSS Through HTTP Headers

Attack mechanism	Meta Attack Pattern	Standard Attack Pattern	Detailed Attack Pattern	
			Reflected XSS	XSS Targeting Non-Script Elements
				XSS Targeting Error Pages
				XSS Using Alternate Syntax
				XSS Targeting HTML Attributes
				XSS Targeting URI Placeholders
				XSS Using Doubled Characters
				XSS Using Invalid Characters
				XSS Through HTTP Query Strings
				XSS Through HTTP Headers
			Stored XSS	XSS Targeting Non-Script Elements -
				XSS Targeting Error Pages
				XSS Using Alternate Syntax
				XSS Using MIME Type Mismatch
				XSS Targeting HTML Attributes
				XSS Targeting URI Placeholders
				XSS Using Doubled Characters
				XSS Using Invalid Characters
	Command Injection	LDAP Injection		
		IMAP/SMTP Command Injection		
		Linux Terminal Injection	Manipulating Writeable Terminal Devices	
		XML Injection	DTD Injection	
			XPath Injection	
			XQuery Injection	
		SQL Injection	Command Line Execution through SQL Injection	

Attack mechanism	Meta Attack Pattern	Standard Attack Pattern	Detailed Attack Pattern		
			Object Relational Mapping Injection		
			SQL Injection through SOAP Parameter Tampering		
			Expanding Control over the Operating System from the Database		
			Blind SQL Injection		
		OS Command Injection			
	Local Execution of Code	Targeted Malware	Install New Service		
			Modify Existing Service		
			Install Rootkit		
			Replace File Extension Handlers		
			Schedule Software To Run		
			Replace Trusted Executable		
			Run Software at Logon		
			Replace Winlogon Helper DLL		
	Object Injection				
	Traffic Injection	Connection Reset	TCP RST Injection		
	Fault Injection		Mobile Device Fault Injection		
Engage in Deceptive Interactions	Content Spoofing		Checksum Spoofing		
			Spoofing of UDDI/ebXML Messages		
		Intent Spoof			
			Signature-Based Avoidance		
			Artificially Inflate File Sizes		
		Counterfeit GPS Signals	Carry-Off GPS Attack		
				Phishing	Spear Phishing

Attack mechanism	Meta Attack Pattern	Standard Attack Pattern	Detailed Attack Pattern
	Identity Spoofing	Fake the Source of Data	Counterfeit Websites / Mobile Phishing
			Counterfeit Organizations
			DNS Spoofing
		Principal Spoof	Cross Frame Scripting (XFS) (Standard Attack Pattern)
			Terrestrial Jamming
		Signature Spoof	Creating a Rogue Certification Authority Certificate
			Signature Spoofing by Key Theft
			Signature Spoofing by Improper Validation
			Signature Spoofing by Misrepresentation
			Signature Spoofing by Mixing Signed and Unsigned Content
			Signature Spoofing by Key Recreation
		Pharming	
		Phishing	Spear Phishing
			Mobile Phishing
	Resource Location Spoofing	Redirect Access to Libraries	Symlink Attack
			Leveraging/Manipulating Configuration File Search Paths
			DLL Search Order Hijacking
		Establish Rogue Location	BitSquatting
			Evil Twin Wi-Fi Attack
			Cellular Rogue Base Station
			TypoSquatting
			SoundSquatting
			Homograph Attack via Homoglyphs
	Action Spoofing	Clickjacking	Flash File Overlay
			iFrame Overlay

Attack mechanism	Meta Attack Pattern	Standard Attack Pattern	Detailed Attack Pattern		
			Activity Hijack		
			Task Impersonation		
			Scheme Squatting		
		Tapjacking			
	Manipulate Human Behavior	Pretexting	Pretexting via Customer Service		
			Pretexting via Tech Support		
			Pretexting via Delivery Person		
			Pretexting via Phone		
		Influence Perception	Influence Perception of Reciprocation		
			Influence Perception of Scarcity		
			Influence Perception of Authority		
			Influence Perception of Commitment and Consistency		
			Influence Perception of Liking		
			Influence Perception of Consensus or Social Proof		
		Target Influence via Framing			
		Influence via Incentives			
		Influence via Psychological Principles	Influence via Modes of Thinking		
			Target Influence via Eye Cues (Meta Attack Pattern)		
			Target Influence via Micro-Expressions	Target Influence via Neuro-Linguistic Programming (NLP) (Meta Attack Pattern)	Target Influence via Voice in NLP (Meta Attack Pattern)
			Target Influence via Eye Cues (Meta Attack Pattern)		

Attack mechanism	Meta Attack Pattern	Standard Attack Pattern	Detailed Attack Pattern
			Target Influence via The Human Buffer Overflow (Meta Attack Pattern)
			Target Influence via Interview and Interrogation(Meta Attack Pattern)
			Target Influence via Instant Rapport (Meta Attack Pattern)
Manipulate Timing and State	Forced Deadlock		
	Leveraging Race Conditions		Leveraging Race Conditions via Symbolic Links
			Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions
	Manipulating User State	Bypassing of Intermediate Forms in Multiple-Form Sets	
Abuse Existing Functionality	API Manipulation	Exploit Test APIs	
		Try All Common Switches	
		Exploit Script-Based APIs	
		Using Unpublished APIs	
	Flooding	TCP Flood	
		UDP Flood	
		ICMP Flood	
		HTTP Flood	
		SSL Flood	
		Amplification	
		XML Flood	XML Ping of the Death
			XML Entity Expansion

Attack mechanism	Meta Attack Pattern	Standard Attack Pattern	Detailed Attack Pattern
	Excessive Allocation	XML Nested Payloads	XML Quadratic Expansion
		XML Oversized Payloads	XML Entity Blowup
			XML Attribute Blowup
		Regular Expression Exponential Blowup	
		SOAP Array Blowup	
		TCP Fragmentation	
		UDP Fragmentation	
		ICMP Fragmentation	
	Resource Leak Exposure		
	Functionality Misuse		JSON Hijacking (aka JavaScript Hijacking)
		Inducing Account Lockout	
			Passing Local Filenames to Functions That Expect a URL
		Password Recovery Exploitation	
		Drop Encryption Level	Weakening of Cellular Encryption
	Communication Channel Manipulation -	Choosing Message Identifier	
		Exploiting Incorrectly Configured SSL	
	Sustained Client Engagement	HTTP DoS	

Attack mechanism	Meta Attack Pattern	Standard Attack Pattern	Detailed Attack Pattern	
	Protocol Manipulation	Windows ::DATA Alternate Data Stream		
		Client-Server Protocol Manipulation	HTTP Request Splitting (Standard Attack Pattern)	
			HTTP Response Smuggling	
			HTTP Verb Tampering	
			HTTP Request Smuggling	
			HTTP Response Splitting	
			Blue Boxing	
			Reflection Attack in Authentication Protocol (Standard Attack Pattern)	
		DNS Rebinding		
		Inter-component Protocol Manipulation		
		Data Interchange Protocol Manipulation		
		Web Services Protocol Manipulation (Meta Attack Pattern)	XML External Entities (Standard Attack Pattern)	XML Entity Blowup
			Soap Manipulation (Standard Attack Pattern)	SOAP Parameter Tampering
	Functionality Bypass	Calling Micro-Services Directly		
		Evercookie		
			Transparent Proxy Abuse	
Employ Probabilistic Techniques	Brute Force	Encryption Brute Forcing		
		Password Brute Forcing	Dictionary-based Password Attack	
			Rainbow Table Password Cracking (Standard Attack Pattern)	
			Try Common or Default Usernames and Passwords	
	Fuzzing			
			Unauthorized Use of Device Resources	

Attack mechanism	Meta Attack Pattern	Standard Attack Pattern	Detailed Attack Pattern	
Subvert Access Control	Authentication Abuse	Reflection Attack in Authentication Protocol		
	Authentication Bypass	Calling Signed Code From Another Language Within A Sandbox Allow This		
		Web Services API Signature Forgery Leveraging Hash Function Extension Weakness		
		Forceful Browsing		
	Privilege Abuse	Accessing Functionality Not Properly Constrained by ACLs	Accessing, Modifying or Executing Executable Files(Standard Attack Pattern)	Modify Shared File
				Add Malicious File to Shared Webroot
				Restful Privilege Elevation
		Exploiting Incorrectly Configured Access Control Security Levels		
		XML External Entities	XML Entity Blowup	
		WebView Exposure		
	Exploitation of Trusted Credentials	Session Credential Falsification through Forging	Session Credential Falsification through Manipulation	
			Session Credential Falsification through Prediction	
		SaaS User Request Forgery		
		Use of Known Domain Credentials	Remote Services with Stolen Credentials -	
			Windows Admin Shares with Stolen Credentials	
		Session Hijacking	Session Sidejacking	
			Cross Site Tracing	
			Reusing Session IDs (aka Session Replay)	
			Session Fixation	
		Cross Site Request Forgery	Cross Site Identification	

Attack mechanism	Meta Attack Pattern	Standard Attack Pattern	Detailed Attack Pattern		
	Exploiting Trust in Client	Create Malicious Client			
		Removing Important Client Functionality	Removal of filters: Input filters, output filters, data masking		
			Removing/short-circuiting 'Purse' logic: removing/mutating 'cash' decrements		
			Subversion of authorization checks: cache filtering, programmatic security, etc.		
		Manipulating Opaque Client-based Data Tokens	Accessing/Intercepting/Modifying HTTP Cookies		
		Manipulating User-Controlled Variables	Subverting Environment Variable Values -		
			Manipulating Hidden Fields		
		Man in the Middle Attack	XML Routing Detour Attacks (Standard Attack Pattern)		
			Application API Message Manipulation via Man-in-the-Middle (Meta Attack Pattern)	Transaction or Event Tampering via Application API Manipulation (Standard Attack Pattern)	Application API Navigation Remapping (Standard Attack Pattern) Also including: 1) Navigation Remapping To Propagate Malicious Content 2) Application API Button Hijacking
			Leveraging Active Man in the Middle Attacks to Bypass Same Origin Policy (Meta Attack Pattern)		
			Utilizing REST's Trust in the System Resource to Register Man in the Middle		
	Privilege Escalation	Cross Zone Scripting			
		Accessing, Modifying or Executing Executable Files	Modify Shared File		
			Add Malicious File to Shared Webroot		
		Hijacking a privileged process			
			Implementing a callback to system routine (old AWT Queue)		

Attack mechanism	Meta Attack Pattern	Standard Attack Pattern	Detailed Attack Pattern	
		Hijacking a Privileged Thread of Execution	Catching exception throw/signal from privileged block	
			Restful Privilege Elevation	
		Subvert Code-signing Facilities	Lifting signing key and signing malicious code from a production environment (Standard Attack Pattern)	
			Calling Signed Code From Another Language Within A Sandbox Allow This (Standard Attack Pattern)	
			Using URL/codebase / G.A.C. (code source) to convince sandbox of privilege	
		Target Programs with Elevated Privileges		
	Bypassing Physical Security	Bypassing Physical Locks (Meta Attack Pattern)	Lock Bumping (Meta Attack Pattern)	
			Lock Picking (Standard Attack Pattern)	
			Using a Snap Gun Lock to Force a Lock (Standard Attack Pattern)	
		Bypassing Electronic Locks and Access Controls	Bypassing Card or Badge-Based Systems (Standard Attack Pattern)	Cloning Magnetic Strip Cards (Standard Attack Pattern)
				Magnetic Strip Card Brute Force Attacks (Standard Attack Pattern)
				Cloning RFID Cards or Chips (Standard Attack Pattern)
				RFID Chip Deactivation or Destruction (Standard Attack Pattern)
	Physical Theft			
Manipulate Data Structures	Buffer Manipulation	Overflow Buffers	Buffer Overflow via Environment Variables	
			Client-side Injection-induced Buffer Overflow	
			Filter Failure through Buffer Overflow	
			SOAP Array Overflow	
			MIME Conversion	
			Overflow Binary Resource File	
			Buffer Overflow via Symbolic Links	
			Overflow Variables and Tags	
			Buffer Overflow via Parameter Expansion	

Attack mechanism	Meta Attack Pattern	Standard Attack Pattern	Detailed Attack Pattern
			String Format Overflow in syslog()
			Buffer Overflow in an API Call
			Buffer Overflow in Local Command-Line Utilities
		Overread Buffers	
	Shared Data Manipulation		
	Pointer Manipulation		
	Input Data Manipulation	Path Traversal	Relative Path Traversal
			Absolute Path Traversal
			Manipulating Web Input to File System Calls
		Integer Attacks	Forced Integer Overflow
		Leverage Alternate Encoding	Double Encoding
			Using Leading 'Ghost' Character Sequences to Bypass Input Filters
			Using Alternative IP Address Encodings
			Exploiting Multiple Input Interpretation Layers
			Embedding NULL Bytes
			Postfix, Null Terminate, and Backslash
			Using Slashes and URL Encoding Combined to Bypass Validation Logic
			Using Unicode Encoding to Bypass Validation Logic
			URL Encoding
			Using Escaped Slashes in Alternate Encoding
			Using Slashes in Alternate Encoding
			Using UTF-8 Encoding to Bypass Validation Logic
Manipulate System Resources	Infrastructure Manipulation	Cache Poisoning	DNS Cache Poisoning
			Force the System to Reset Values
		Audit Log Manipulation	Web Logs Tampering
			Log Injection-Tampering-Forging
		Block Logging to Central Repository	

Attack mechanism	Meta Attack Pattern	Standard Attack Pattern	Detailed Attack Pattern
	File Manipulation	Cause Web Server Misclassification	
		Accessing, Modifying or Executing Executable Files	Modify Shared File
			Add Malicious File to Shared Webroot
		Create files with the same name as files protected with a higher classification	
		Force Use of Corrupted Files	
		Leverage Executable Code in Non-Executable Files -	User-Controlled Filename
	Configuration / Environment Manipulation	Manipulate Application Registry Values	Modification of Registry Run Keys
			Poison Web Service Registry
		Schema Poisoning	XML Schema Poisoning
			Data Injected During Configuration
		Disable Security Software	
		Manipulating Writeable Configuration Files	
	Software Integrity Attack	Malicious Software Download	
		Malicious Software Update	Malicious Automated Software Update
			Malicious Manual Software Update
			Rooting SIM Cards
	Modification During Manufacture	Development Alteration	Malicious Logic Inserted Into Product Software by Authorized Developer
			Malicious Logic Insertion into Product Software via Configuration Management Manipulation
			Malicious Logic Insertion into Product Software via Inclusion of 3rd Party Component Dependency
			Infiltration of Software Development Environment
			Hardware Component Substitution During Baselining

Attack mechanism	Meta Attack Pattern	Standard Attack Pattern	Detailed Attack Pattern	
			Counterfeit Hardware Component Inserted During Product Assembly	
			Infiltration of Hardware Development Environment	
			ASIC With Malicious Functionality	
		Design Alteration	Documentation Alteration to Circumvent Dial-down	
			Documentation Alteration to Produce Under-performing Systems	
			Documentation Alteration to Cause Errors in System Design	
			Hardware Design Specifications Are Altered	
	Manipulation During Distribution	Malicious Hardware Component Replacement		
		Malicious Software Implanted		
		Rogue Integration Procedures		
	Hardware Integrity Attack	Hacking Hardware	Bypassing ATA Password Security	
		Malicious Hardware Update	Hardware Component Substitution	Provide Counterfeit Component
				Malicious Gray Market Hardware
	Malicious Logic Insertion	Malicious Logic Inserted Into To Product Software	Malware Infection into Product Software	
			Altered Installed BIOS	
			Open Source Libraries Altered	
		Malicious Logic Insertion into Product Hardware		
		Malicious Logic Insertion into Product Memory	USB Memory Attacks	
			Flash Memory Attacks	
	Contaminate Resource			
	Obstruction	Physical Destruction of Device or Component		
		Route Disabling	Disabling Network Hardware	
			BGP Route Disabling	

Attack mechanism	Meta Attack Pattern	Standard Attack Pattern	Detailed Attack Pattern
			DNS Domain Seizure
		Jamming	Orbital Jamming
			Wi-Fi Jamming
			Cellular Jamming
		Blockage	DNS Blocking
			IP Address Blocking
			Block Access to Libraries

Table 22 – Capec's classification by Mechanisms of Attack

Category	Meta Attack Pattern
Social Engineering	Information Elicitation
	Manipulate Human Behavior
Supply Chain	Modification During Manufacture
	Manipulation During Distribution
Communications	Interception
	Protocol Manipulation
	Traffic Injection
	Obstruction
Software	Brute Force
	Authentication Abuse
	Authentication Bypass
	Excavation
	Buffer Manipulation
	Flooding
	Pointer Manipulation
	Excessive Allocation

Category	Meta Attack Pattern
	Resource Leak Exposure
	Parameter Injection
	Content Spoofing
	Identity Spoofing
	Input Data Manipulation
	Resource Location Spoofing
	Footprinting
	Action Spoofing
	Code Inclusion
	Software Integrity Attack
	Reverse Engineering
	Functionality Misuse
	Fingerprinting
	Sustained Client Engagement
	Code Injection
	Command Injection
Physical Security	Bypassing Physical Security
	Physical Theft
	Physical Destruction of Device or Component (standard Attack Pattern)
Hardware	Footprinting
	Hardware Integrity Attack
	Malicious Logic Insertion

iv. ISO 28001:2007: Security management systems for the supply chain

Threat Category	Defined Threat Scenarios	
	Threat Scenario	*Application*
TC-1. Infrastructural Threats.	**$TS_{1.1}$:** Destroy a major / critical SC Infrastructure	– Warehouses of the stored cargo have been bombed – Fences/exterior walls of the warehouses have been destroyed or bypassed. – Buildings hosting a data center used in the SC-Service has been destroyed due to a deliberate action or a physical threat
	$TS_{1.2}$: Suspected or confirmed unauthorized access to SC infrastructures	– Unauthorized access to storage buildings etc – CCTV/DVS cameras do not operate well (due to a physical attack or lack of maintenance.
TC-2. Information & ICT Threats	**$TS_{2.1}$:** Information tampering (** as defined is ISO* 28001)	– Locally or remotely gaining access the supply chain's information/documentation systems for the purpose of disrupting operations or facilitating illegal activities
	$TS_{2.2}$: Information loss	– cargo/shipping/ billing/documentation/ information is destroyed due to a deliberate attack (e.g. sabotage) or physical attack (e.g. fire)
	$TS_{2.3}$: Communication interruption or loss	– optical fibers have been smuggled, – network connection has been disrupted
	$TS_{2.4}$: Software/system abuse	– A critical software for the SC has been hacked – Backdoors identified in a SC critical system
TC-3. Threats related with Personnel Security & Safety	**$TS_{3.1}$:** People under attack	– SC key personnel have been taken hostages – Threat against the life of people, (business partner's personnel, people using the SC, etc) – Take hostages/kill people.
	$TS_{3.2}$: Misuse / abuse of SC procedures	– The employees are not trained in the SC procedures, – An employee misuses his/her security credentials – Absence of key personnel of a business partners (e.g. due to a strike)

Threat Category	Defined Threat Scenarios	
	Threat Scenario	***Application***
TC-4. Threats related with Goods and Conveyance Security	**$TS_{4.1}$**: Intrude and/or take control of an asset (including conveyances) within the supply chain. (** as defined is ISO* 28001)	– Damage/destroy an asset (including conveyances). – Damage/destroy outside target using the asset or goods. – Cause civil or economic disturbance.
	$TS_{4.2}$: Use the supply chain as a means of smuggling. (** as defined is ISO* 28001)	– Illegal weapons into or out of the country/economy – Terrorist into or out of the country/economy
	$TS_{4.3}$: Cargo Integrity (** as defined is ISO* 28001)	– Tampering, sabotage and/or theft for the purpose of terrorism
	$TS_{4.4}$: Unauthorized use (** as defined is ISO* 28001)	– Conducting operations in the international supply chain to facilitate a terrorist incident including using the mode of transportation as a weapon.
	$TS_{4.5}$: Goods and Conveyance misuse	– The cargo received or delivered by/to a wrong person due to the luck of appropriate authentication procedures – The cargo transport related procedures have been alternated, and the activities have been misused – Closed cargo has been unsealed illegally, – Closed cargo contains wrong material – an employee or business partner in the SC is stealing SC-goods – unauthorized access to all cargo and conveyance storage areas
TC-5. Other		

v. Threats catalogue IT Grundschutz

High level Threats	Threat details - examples
Fire	
Unfavourable Climatic Conditions	
Water	
Pollution, Dust, Corrosion	
Natural Disasters	
Environmental Disasters	
Major Events in the Environment	
Failure or Disruption of the Power Supply	
Failure or Disruption of Communication Networks	
Failure or Disruption of Mains Supply	
Failure or Disruption of Service Providers	
Interfering Radiation	
Intercepting Compromising Emissions	
Interception of Information / Espionage	Many IT systems are protected against unauthorised access by identification and authentication mechanisms, e. g. in the form of user name and password verification. If the password is transmitted over the wire in an unencrypted form, it is under certain circumstances possible for an attacker to retrieve it.
	To be able to withdraw money out of an automatic teller machine, the correct PIN for the used electronic cash card or credit card must be entered. Unfortunately, the visual protection available for this equipment is frequently insufficient, so that an attacker can look over the shoulder of a customer entering the pin without much effort. If the attacker steals the card afterwards, he can plunder the account this way.
	To receive access rights to a PC or to otherwise manipulate it, an attacker can send the user a Trojan Horse which he has enclosed within an email as a supposedly useful programme.

High level Threats	Threat details - examples
	In many offices, workplaces are not sufficiently protected in terms of acoustics. As a consequence, colleagues and also visitors could possibly listen to conversations and come to know information which is not meant for them or is even confidential.
Eavesdropping	In the case of telephone calls, it is not only eavesdropping on conversations that can be of interest to an attacker. The information which is transmitted in signalling can be misused by an attacker as well e. g. due to an incorrect setting in the terminal resulting in the password being transmitted in plain text at the time of login.
	An attacker can easily eavesdrop on the entire communication if wireless transmission is unprotected or insufficiently protected (e. g. if a WLAN is protected only with WEP).
	Emails can be read throughout their entire journey through the network if they are not encrypted. Unencrypted emails should therefore not be compared with conventional letters but with postcards.
Theft of Devices, Storage Media and Documents	A notebook computer disappeared from the U.S. Department of State in the spring of 2000. In an official statement, it was not ruled out that the device could contain confidential information. Nor was there information given as to whether the device was protected by cryptographic or other measures against unauthorised access.
	A German Federal Office was repeatedly broken into through the same unsecured windows. Mobile IT systems disappeared along with other valuables. It could not be ruled out without a doubt that files were copied or manipulated.
	There were a number of data leaks in Great Britain, in which confidential documents were disclosed because data storage media were stolen. In one case, several computer hard disks were stolen from the British Air

High level Threats	Threat details - examples
	Force which contained personal information, collected by employees for security screening purposes.
	An employee of a call centre prepared copies of a large set of confidential customer data shortly before he had to leave the company. After leaving the company, he then sold this data to competitors. Since details about the incident were then published by the press, the call centre lost many important customers
Loss of Devices, Storage Media and Documents	An employee uses the journey in the tramway to her workplace to read over some documents. When getting off the tram in a hurry at her destination stop, she leaves the documents inadvertently on her neighbouring place. Although the documents are not confidential, several signatures of high-profile executives must nevertheless be collected once again as a consequence.
	At a major event, while searching through his briefcase, an employee inadvertently drops a memory card with confidential calculations on the ground without noticing. The finder views its contents on his laptop and sells the information to the competition.
	A manufacturer sends CDs with software updates for bug fixing by post to his customers. Some of these CDs are lost in the post. Neither the sender nor the recipients are informed about it. As a consequence, the effected customers experience malfunctions in the software.
Bad Planning or Lack of Adaption	
Disclosure of Sensitive Information	
Information or Products from an Unreliable Source	
Manipulation of Hardware or Software	In a Swiss financial company, an employee had manipulated the software used for certain financial services. This made it possible for him to illegally gain large amounts of money.
	By manipulating ATMs, attackers succeeded several times to illegally read the data stored on payment cards. In conjunction with PINs spied out, this data was then misused to withdraw money at the expense of the cardholder.

High level Threats	Threat details - examples
Manipulation of Information	An employee was so annoyed at the promotion of her roommate in the accounting department that during the short absence of her colleague, she illegally gained access to her computer. Here she has caused, by changing some figures in the monthly balance sheet, enormous negative impact on the published financial results of the company.
Unauthorised Access to IT Systems	If a user ID and password have been spied out, any unauthorised use of the applications or IT systems protected by them is well possible.
	Using inadequately safeguarded remote maintenance access, hackers could gain unauthorised access to IT systems.
	When interfaces of active network components are inadequately safeguarded, it is possible that an attacker gains unauthorised access to the network component. If they also manage to overcome the local security mechanisms, e. g. obtain administrative privileges, they could perform all administrative activities.
	Many IT systems have interfaces for the use of interchangeable data storage, such as extra memory cards or USB storage media. In an unattended IT system with the corresponding hardware and software, there is a risk that large amounts of data can be retrieved, or malicious software can be introduced this way.
Destruction of Devices or Storage Media	In a company an internal perpetrator used his knowledge about an important server being sensitive to too high operating temperatures and blocked the ventilation slits for the power supply fan using an object hidden behind the server. Two days later, the hard drive in the server suffered a temperature-caused defect, and the server was down for several days
	Humidity ingressing into an IT system, due to knocked-over coffee cups or watering the flowers can cause short circuits.

High level Threats	Threat details - examples
Failure of Devices or Systems	Firmware has been installed on an IT system which is not designed for this type of system. The IT system will then no longer start without errors and must be made operational by the manufacturer.
	A power failure in a memory system at the site of an Internet Service Provider (ISP) resulted in having to switch it off. Although the actual error could be corrected quickly, the affected IT systems could not start again due to inconsistencies in the file system. As a result, several Web servers operated by the ISP were not available for days.
Malfunction of Devices or Systems	
Lack of Resources	
Software Vulnerabilities or Errors	The most frequent warnings of the Computer Emergency Response Teams (CERTs) in recent years were related to security-relevant programming errors. These are errors made during programming of software which allow attackers to misuse it. A large proportion of these errors are caused by buffer overflows.
	Internet browsers are nowadays an important software component on clients. Browsers frequently do not only access the Internet but are also used for internal web applications in companies and public bodies. This is why software vulnerabilities or errors in browsers can impair information security overall particularly strongly.
Violation of Laws or Regulations	
Unauthorised Use or Administration of Devices and Systems	When examining log files, a network administrator came across inexplicable events occurring on different days but often early in the morning and in the afternoon. After a closer examination, it turned out that a wireless router was not configured properly. People waiting at the bus stop outside the office building have used this access to surf with their mobile devices on the Internet while waiting for the bus.
Incorrect Use or Administration of Devices and Systems	
Abuse of Authorisations	

High level Threats	Threat details - examples
Absence of Personnel	
Attack	In the 1980s, a bomb attack was perpetrated on the data centre of a large federal agency in Cologne. Due to the large penetrating power of the explosive device, not only windows and walls, but also many information systems in the data centre were destroyed.
	In the attack on the World Trade Center in New York on the 11th of September 2001, not only were many people killed but also were a number of IT facilities destroyed. As a result, several companies had considerable difficulty in continuing their business activities.
Coercion, Extortion or Corruption	
Identity Theft	To register with various email providers or auction platforms on the Internet, it sufficed to invent a fictitious name and to provide a suitable address from the phone book with it. At first, attackers could register using recognisable fictitious names, for example, derived from cartoon characters. As stronger plausibility checks were later introduced for this purpose, names, addresses and account numbers of real people have been used. Those affected have only learned about a fraud, when the first claims for payment arrived.
	The sender address of emails can be easily spoofed. It happens again and again that users are this way fooled into believing that an email comes from a trusted communication partner. Similar attacks are possible by manipulation of caller ID for voice calls or by manipulating the sender identity for fax connections.
	An attacker may use a masquerade to try to enter into an already existing connection without having to authenticate himself, since this step has already been performed by the original communication participants.
Reputation of Actions	An urgently needed spare part has been ordered electronically. After a week it is claimed still to be missing, in the meantime high losses due to production outage are incurred. The supplier denies having ever received an order.

High level Threats	Threat details - examples
Abuse of Personal Data	Personal data may be processed only for the purpose for which it was collected or stored for the first time. It is therefore inadmissible to use log files for attendance and monitoring conduct, if they were designed to store information on users' logging on to an IT system and logging off merely for access control.
	Persons who have access to personal data could disclose them in an unauthorised manner. For example, an employee at the front desk of a hotel could sell the guests' registration information to advertising companies.
Malicious Software	In the past, the malicious software W32/Bugbear was spread in two ways: it searched in local area networks for computers with shares, where write access was possible, and made copies of itself on each share found. Moreover, it sent itself as an HTML-email to recipients in the email address books of infected computers. Due to an error in the HTML routines of certain email programs, the malicious software was executed upon opening the message without further action by the recipient.
	The malicious software W32/Klez spread in different variants. Infected computers sent the virus to all recipients in the email address book of the computer. After this virus had infected a computer, by continuous manipulation of the operating system it prevented the installation of anti-virus programs from most popular manufacturers and made it significantly more difficult to perform disinfection of the infected computers.
Denial of Service	In spring 2007 in Estonia strong DoS attacks on numerous Internet sites over a prolonged period of time took place. This led to significant impairments in the use of information services and Internet services in Estonia.
Sabotage	In a mainframe computer centre, a manipulation of the uninterrupted power supply led to a temporary total failure. The perpetrator had repeatedly manually switched the uninterrupted power supply to bypass mode and then manipulated the main power supply of the building. Altogether there were four failures within three years. Even hardware was partially

High level Threats	Threat details - examples
	damaged. The disruption took between 40 and 130 minutes.
	Sanitary facilities were also located within a data centre. Due to blockage of the drains and the simultaneous opening of the water supply, water penetrated into central technology components. Damage caused this way resulted in interruptions of operation in the production system.
	Electronic archives present a particular risk of sabotage, since there, many sensitive documents are kept on a small floor space. Because of this aspect, by targeted unsophisticated manipulation a great deal of damage can be incurred under certain circumstances.
Replaying Messages	Replay attack: In a "replay attack" (replay of messages) attackers record valid messages and play this information at a later time almost unchanged.Also only part of a message may suffice, such as a password, to enter into an IT system without authorisation.
	Man-in-the-middle: In a "man-in-the-middle attack" the attacker assumes unnoticed a mediating position in the communication among various participants. In general, the attacker pretends here to be the sender of a message to the intended recipient, and he pretends to the recipient that he is the actual sender. If successful, the attacker can receive messages, which are not intended for him, evaluate them and purposefully manipulate them before they are forwarded to the intended recipient.
Unauthorised Entry to Premises	
Data Loss	
Loss of Integrity of Sensitive Information	

Table 23 – IT Grundsutz Threats Catalogue

vi. CYSM Project Threats catalogue

List of threats and vulnerabilities

TYPE OF ASSET	THREATS	
ICT Infrastructure	Contamination	Back-up files and systems not available
		Lack of maintenance of equipment and facilities
		Location is in an area susceptible to environmental conditions such as contamination, electronic interference extreme temperature and humidity vermin
		No business continuity plans or procedures for recovery of information and information assets
	Cyber-Vermin	Adware threats
		Back-up files and systems not available
		Malware threats
		No business continuity plans or procedures for recovery of information and information assets
		Phishing threats
		Pop-Ups threats
		Spyware threats
		Trojan threats
		Virus threats
		Worm threats
	Earthquake	Back-up files and systems not available
		Location is in an area susceptible to natural disasters
		No business continuity plans or procedures for recovery of information and information assets
	Electronic Interference	Back-up files and systems not available
		No business continuity plans or procedures for recovery of information and information assets
		Electromagnetic radiation
		Electrostatic charges
	Equipment Failure	Inadequate change control settings
		Incomplete / incorrect maintenance
		Non periodic replacement
		Susceptibility to electromagnetic radiation
		Susceptibility to moisture, dust, dirt
		Susceptibility to temperature fluctuations

		Susceptibility to voltage fluctuations
	Extremes of Temperature and Humidity	Back-up files and systems not available
		Improper or inappropriate maintenance of technical facilities
		Inadequate backup policy
		Inadequate change management procedure for infrastructure components
		Inadequate data backup procedure for both software and data
		Inadequate monitoring of environmental conditions
		Inadequate Physical and Environmental Security Policy and Procedures
		Inadequate Recovery Procedure
		Lack of a uniform physical security policy enforcement
		Lack of back-up facilities or processes
		Lack of environmental protection
		Location is in an area susceptible to environmental\ conditions such as extreme temperature and humidity
		Location is in an area susceptible to environmental conditions such as contamination, electronic interference extreme temperature and humidity vermin
		No business continuity plans or procedures for recovery of information and information assets
		No concrete assignment of Continuity/Disaster-related roles and responsibilities
		No formal or informal disaster/recovery plans
	Failure of outsourced operations	Back-up files and systems not available
		No business continuity plans or procedures for recovery of information and information assets
	Fire	Backup files and systems not available
		Improper or inappropriate maintenance of technical facilities
		Inadequate backup policy
		Inadequate change management procedure for infrastructure components
		Inadequate monitoring of environmental conditions
		Inadequate Physical and Environmental Security Policy and Procedures
		Inadequate Recovery Procedure
		Lack of a uniform physical security policy enforcement
		Lack of automatic fire suppression system
		Lack of back-up facilities or processes
		Lack of environmental protection
		Lack of fire detection devices
		No concrete assignment of Continuity/Disaster-related roles and responsibilities

		No formal or informal disaster/recovery plans
		No Business Continuity Plans for recovery of information and information assets
	Flood	Back-up files and systems not available
		Location is in an area susceptible to natural disasters
		No business continuity plans or procedures for recovery of information and information assets
		Susceptibility to water
	Hurricane	Back-up files and systems not available
		Location is in an area susceptible to natural disasters
		No business continuity plans or procedures for recovery of information and information assets
	Industrial Action	Inadequate incident handling
		Incorrect Access rights
		Lack of an industrial agreement
		Lack of audit logs to detect unauthorized use of application
		No concrete assignment of security incidents roles and responsibilities
		No formal incident review and handling process
		No formally documented procedures for identifying, reporting, and responding to suspected security incidents and violations
		No incident response and reporting procedures and policies
	Malicious destruction of data and facilities	Lack of Physical Security
	Malpractice	Unauthorized use of equipment
	Operational Staff or User Errors	Inadequate documentation
		Lack of a comprehensive security awareness and training program
		Lack of means to assess the employee awareness level
		Lack of user awareness
		Unskilled staff
	Power Fluctuations	Back-up files and systems not available
		Improper or inappropriate maintenance of technical facilities
		Inadequate change management procedure for infrastructure components
		Inadequate monitoring of environmental conditions
		Inadequate Physical and Environmental Security Policy and Procedures
		Lack of a uniform physical security policy enforcement
		Lack of environmental protection

		Location is in an area susceptible to power fluctuations
		No business continuity plans or procedures for recovery of information and information assets
		No power conditioning equipment
		No Uninterruptible Power Supply equipment
	Procedural Failures	Lack of safety requirements in contracts with customers and suppliers
		Application of the "Empty Office" & "Blank Screen" policies
		Inadequate response procedure for maintenance / repair
		Incomplete control for material exiting the facility
		Lack / Poor assigning of information security responsibilities
		Lack of administrative controls
		Lack of defined disciplinary process for handling security incidents
		Lack of formal approval process of published material
		Lack of formal installation process for corporate software
		Lack of formal process to enable/disable user passwords
		Lack of log files
		Lack of maintenance contracts and SLAs
		Lack of mechanisms for monitoring security breaches
		Lack of monitoring of sites where information is being processing
		Lack of problems / errors log files
		Lack of procedures to deal with classified information
		Lack of process for controlling copyrights
		Lack of reporting processes for safety risks
		Lack of risk assessment procedures
		Lack of security conditions in staff contracts
		Lack of security requirements in the job responsibilities of staff
		Lack of usage policies
		Lack of usage policy for corporate e-mails
		Minimum or no regular checks and site inspections
		Uncontrolled copy of data
		Uncontrolled copy of software
	Reduced budgets	Inadequate investment in appropriate security controls
	Sabotage	Lack of Physical Security
	Staff Risks	No staff

		Inadequate recruitment
		Inadequate safety training
		Incorrect use of software and hardware
		Insufficient awareness of security risks
		Lack of media use policy
		Lack of monitoring mechanisms
		Unsupervised work of external staff
	Storm	Back-up files and systems not available
		Location is in an area susceptible to natural disasters
		No business continuity plans or procedures for recovery of information and information assets
	Strike	Backup files and systems not available
		Inadequate Physical Security
	Technical failures	A/C Failure
		Aging storage media
		Dusty equipment
		Failures in the change management process
		Improper or inappropriate maintenance of technical facilities
		Lack of environmental protection
		Lack of network capacity through improper planning or maintenance
		Lack of user awareness
		Wear and Tear of equipment
	Terrorist attacks	Bombing of equipment, Molotov cocktails
		Industrial espionage
	Theft and Fraud	Back-up files and systems not available
		Inadequate audit logs to detect unauthorized access of the premises
		Inadequate change management procedure for infrastructure components
		Inadequate maintenance of the records regarding the repairs and modifications of the organization facilities physical components
		Inadequate monitoring of the organization premises
		Inadequate Physical and Environmental Security Policy and Procedures
		Inadequate Physical Security
		Insufficient security training
		Lack of a comprehensive security awareness and training program

		Lack of a formal entitlement review process regarding the access rights of the employees in the organization's premises
		Lack of a uniform policy and procedure for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media enforcement
		Lack of Logical Access security
		Lack of Physical Security
		No concrete assignment of security roles and responsibilities
		No documented and tested security plans for safeguarding the systems and networks
		No documented policies and procedures for physical control of hardware and software
		Uncontrolled copy of data
		Uncontrolled copy of software
	Tidal Surge/Wave	Back-up files and systems not available
		Location is in an area susceptible to natural disasters
		No business continuity plans or procedures for recovery of information and information assets
	Transmission errors	Back-up files and systems not available
		Lack Careful planning and laying of cables
		Lack of cryptographic means to protect integrity of data
		Lack of properly operation of network equipment
		No business continuity plans or procedures for recovery of information and information assets
	Unauthorised Data Access	Lack of logical access control and audit
		Lack of Physical Security
	Unauthorised Software Changes	Back-up files and systems not available

Information and electronic data	Communications Failure	Communication lines without protection
		Incomplete network management
		Insecure network architecture
		Lack of identification sender / receiver
		Lack shipment confirmation / reception
		Lines dial-up access
		Poor communication connection lines
		Transfer passwords unencrypted

		Transfer of passwords in clear
		Transfer sensitive information unencrypted
		Unprotected connection to the external network
	Contamination	Back-up files and systems not available
		Lack of maintenance of equipment and facilities
		Location is in an area susceptible to environmental conditions such as contamination, electronic interference extreme temperature and humidity vermin
	Cyber-Vermin	Back-up files and systems not available
	Data Corruption	Applying application programs to the wrong data in terms of time
		Incorrect dates
		Incorrect parameter set up
		Lack of identification and authentication mechanisms like user authentication
		Poor password management
		Unnecessary services enabled
		Unprotected password tables
		Widely-distributed software
	Denial of Service	Inadequate network management (resilience of routing)
		Incorrectly configured or maintained security safeguards
		Inefficient configuration of Anti Virus software
		Lack of a Firewall
		Lack of regular update of Anti virus software
		No Anti-Virus software
		Not keeping up to date with Security advisories will lead to a known weakness not being corrected in a timely manner
	Earthquake	Back-up files and systems not available
		Location is in an area susceptible to natural disasters
	Eavesdropping	Inadequate security controls for the protection of sensitive information being either in storage or during transmission (e.g., data encryption, public key infrastructure, virtual private network technology)
		Lack of encryption mechanisms
		Lack of physical security over data communications closets or hubs
		Unencrypted communications
		Unprotected communication lines
		Unprotected sensitive traffic

		Use of Shared Ethernet means that all traffic is broadcast to any machine on a local segment
	Electronic Interference	Back-up files and systems not available
	Equipment Failure	Inadequate change control settings
		Incomplete / incorrect maintenance
		Non periodic replacement
		Susceptibility to electromagnetic radiation
		Susceptibility to moisture, dust, dirt
		Susceptibility to temperature fluctuations
		Susceptibility to voltage fluctuations
	Extremes of Temperature and Humidity	Back-up files and systems not available
		Improper or inappropriate maintenance of technical facilities
		Inadequate backup policy
		Inadequate change management procedure for infrastructure components
		Inadequate data backup procedure for both software and data
		Inadequate monitoring of environmental conditions
		Inadequate Physical and Environmental Security Policy and Procedures
		Inadequate Recovery Procedure
		Lack of a uniform physical security policy enforcement
		Lack of back-up facilities or processes
		Lack of environmental protection
		Location is in an area susceptible to environmental\ conditions such as extreme temperature and humidity
		Location is in an area susceptible to environmental conditions such as contamination, electronic interference extreme temperature and humidity vermin
		No concrete assignment of Continuity/Disaster-related roles and responsibilities
		No formal or informal disaster/recovery plans
	Failure of outsourced operations	Back-up files and systems not available
		Unclear obligations in outsourcing agreements
	Files incidents	Reject without attention
		Unprotected storage
		Uncontrolled copies of files
		Uncontrolled copies of sensitive files
	Fire	Backup files and systems not available
		Improper or inappropriate maintenance of technical facilities

		Inadequate backup policy
		Inadequate change management procedure for infrastructure components
		Inadequate monitoring of environmental conditions
		Inadequate Physical and Environmental Security Policy and Procedures
		Inadequate Recovery Procedure
		Lack of a uniform physical security policy enforcement
		Lack of automatic fire suppression system
		Lack of back-up facilities or processes
		Lack of environmental protection
		Lack of fire detection devices
		No concrete assignment of Continuity/Disaster-related roles and responsibilities
		No formal or informal disaster/recovery plans
		No Business Continuity Plans for recovery of information and information assets
	Flood	Back-up files and systems not available
		Location is in an area susceptible to natural disasters
	Industrial Action	Inadequate audit logs to detect malicious use of information systems/applications
		Inadequate audit logs to detect unauthorized access
		Inadequate Network Administration Tools
		Incorrect Access rights
		Lack of an industrial agreement
		Lack of audit logs to detect unauthorized use of application
		Lack of data leak systems
		Lack of Event Management and Correlation System
		Lack of intrusion and Prevention Systems detection software
	Malicious Code	Inadequate education of staff on Software viruses
		Lack of checks for unauthorised software
		Lack of control of instant messaging
		Lack of policy for opening email attachments
		Lack of policy on using portable storage devices and media before scanning by Anti virus software
		Lack of regular update of Anti virus software
		Legacy systems
		No Anti Virus software
	Malicious destruction of data	Inadequate Firewall Policies

		Inadequate investment in appropriate security controls
		Inadequate operating policies for handling, processing or storing sensitive information
		Incorrectly configured or maintained application security features
		Incorrectly configured or maintained operating system
		Incorrectly configured or maintained security safeguards
		Lack of a Firewall
		Lack of intrusion detection software
		Lack of Physical Security
		Unsecured wireless ports
	Malpractice	Unauthorized use of equipment
	Masquerade	Inadequate identity and password policy
		Inadequate user training
		Insufficient security training
		Lack of a comprehensive security awareness and training program
		Lack of identification and authentication Mechanisms
		Lack of identification of sender and receiver
		Lack of means to assess the employee awareness level
		Unprotected password tables
	Misrouting or re-routing messages	Inadequate user training
		Lack of proof of receiving a message
		Transmission of unencrypted confidential data
	Network Intrusion	Inadequate Network implementation standards
		Inadequate Network Policies
		Incorrectly configured or maintained network operating system
		Lack of intrusion detection software
		Lack of update of Operating System security patches
		Poor joint cabling
		Single point of failure
	Operational Staff or User Errors	Complicated user interface
		Inadequate documentation
		Lack of a comprehensive security awareness and training program
		Lack of means to assess the employee awareness level
		Lack of user awareness

		Unskilled staff
	Personnel Incidents	Absence of personnel
		Inadequate recruitment procedures
		Incorrect use of software and hardware
		Insufficient security training
		Lack of monitoring mechanisms
		Lack of policies for the correct use of telecommunications media and messaging
		Lack of security awareness
		Unsupervised work by outside or cleaning staff
	Power Fluctuations	Back-up files and systems not available
		Improper or inappropriate maintenance of technical facilities
		Inadequate change management procedure for infrastructure components
		Inadequate monitoring of environmental conditions
		Inadequate Physical and Environmental Security Policy and Procedures
		Lack of a uniform physical security policy enforcement
		Lack of environmental protection
		Location is in an area susceptible to power fluctuations
		No power conditioning equipment
		No Uninterruptible Power Supply equipment
	Procedural Failures	Lack of safety requirements in contracts with customers and suppliers
		Application of the "Empty Office" & "Blank Screen" policies
		Inadequate response procedure for maintenance / repair
		Incomplete control for material exiting the facility
		Lack / Poor assigning of information security responsibilities
		Lack of administrative controls
		Lack of defined disciplinary process for handling security incidents
		Lack of formal approval process of published material
		Lack of formal installation process for corporate software
		Lack of formal process to enable/disable user passwords
		Lack of log files
		Lack of maintenance contracts and SLAs
		Lack of mechanisms for monitoring security breaches
		Lack of monitoring of sites where information is being processing
D	sitories of Empirical Knowledge	

		Lack of problems / errors log files
		Lack of procedures to deal with classified information
		Lack of process for controlling copyrights
		Lack of reporting processes for safety risks
		Lack of risk assessment procedures
		Lack of security conditions in staff contracts
		Lack of security requirements in the job responsibilities of staff
		Lack of usage policies
		Lack of usage policy for corporate e-mails
		Minimum or no regular checks and site inspections
		Uncontrolled copy of data
		Uncontrolled copy of software
	Reduced budgets	Inadequate investment in appropriate security controls
	Repudiation	Lack of proof of sending or receiving a message
		Lack of use of Digital signatures
	Sabotage	Incorrect Access rights
		Lack of Configuration Management controls
		Lack of Logical Access security
		Lack of Physical Security
	Social Engineering	Lack of awareness of the social engineering threat
		Lack of policy requiring enquires for information to be withheld until the identity of the requestor can be verified
		Lack of policy restricting the provision of information by staff over the phone
	Software Failure	Failure to produce management reports
		Immature or new software
		Lack of back-up copies
		Lack of effective change control
		Lack of physical protection of the building, doors and windows
		Unclear or incomplete specifications for developers
		Uncontrolled downloading and use of software
	Software or Programming Errors	Inadequate system development life cycle procedures
		Unclear or incomplete specifications
		Unskilled staff

	Staff Risks	No staff
		Inadequate recruitment
		Inadequate safety training
		Incorrect use of software and hardware
		Insufficient awareness of security risks
		Lack of media use policy
		Lack of monitoring mechanisms
		Unsupervised work of external staff
	Storm	Back-up files and systems not available
		Location is in an area susceptible to natural disasters
	Technical advances such as quantum computing	Inneficient encryption algorithms
	Terrorist attacks	Industrial espionage
	Theft and Fraud	Inadequate change management procedure for infrastructure components
		Inadequate Firewall Policies
		Inadequate monitoring of the organization premises
		Inadequate operating policies for handling, processing or storing sensitive information
		Incorrectly configured or maintained application security features
		Incorrectly configured or maintained operating system
		Incorrectly configured or maintained security safeguards
		Insufficient security training
		Lack of a comprehensive security awareness and training program
		Lack of a Firewall
		Lack of a formal entitlement review process regarding the access rights of the employees in the organization's premises
		Lack of a uniform policy and procedure for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media enforcement
		Lack of application safeguards leading to fraudulent payments being made
		Lack of appropriate control of outbound traffic
		Lack of checks for unauthorised software
		Lack of effective Software Change management leading to unauthorised software modifications that could be used to perpetrate a fraud
		Lack of Logical Access security

		Lack of Physical Security
		Lack of procedural safeguards leading to fraudulent payments being made
		Lack of safeguards leading to false credentials being created or accepted
		No concrete assignment of security roles and responsibilities
		Revealing too much information about systems to people without a “need to know”
		Uncontrolled copy of data
		Uncontrolled copy of software
		Uncontrolled copying of data and or software
		Unsecured wireless ports
	Tidal Surge/Wave	Back-up files and systems not available
		Location is in an area susceptible to natural disasters
	Transmission errors	Back-up files and systems not available
		Improper or inappropriate cabling
		Inadequate incident handling
	Unauthorised Data Access	Inability to authenticate requests for information
		Inadequate Firewall Policies
		Inadequate identity and password policy
		Inadequate investment in appropriate security controls
		Inadequate operating policies for handling, processing or storing sensitive information
		Inadequate review of the users access rights
		Incorrect Access rights
		Incorrectly configured or maintained application security features
		Incorrectly configured or maintained operating system
		Incorrectly configured or maintained security safeguards
		Lack of a Firewall
		Lack of identification and authentication Mechanisms
		Lack of intrusion detection software
		Lack of physical security over data communications cabinets
		No formal policy for the establishment and termination of the access right to information assets
		Portable devices storing unencrypted data and information
		Transmission of unencrypted sensitive data or information
		Unprotected password tables
		Unsecured wireless ports

	Unauthorised Dial-in Access	Dial-in banner leading to information which can expose the organisation to unauthorised dial in access
		Lack of an inventory of dial-up lines leading to inability to monitor dial up access
		Lack of audit logs to detect unauthorised access
		Lack of dial back authentication
		Lack of firewall
		Lack of intrusion detection software
		Lack of physical security over telecommunications equipment cabinets
		Lack of policies in respect of dial up access, modem use, and software use
		Lack of time restrictions on user access
		Lack of user authentication
	Unauthorised Software Changes	Back-up files and systems not available
		Easily accessible SCADA devices
		Inadequate engineering and quality processes for design and code review
		Inadequate reporting and handling of software malfunctions
		Inadequate Segregation of Duties between software developers and operations staff
		Inadequate supervision of programming staff
		Incorrectly configured or maintained operating system
		Incorrectly configured or maintained security safeguards
		Lack of a Firewall
		Lack of backups
		Lack of Configuration Management Software to enforce Configuration Management
		Lack of intrusion detection software
		Lack of Software Configuration Management policies and procedures
	Web Site Intrusion	Inadequate Firewall Policies
		Inadequate Software Development standards
		Incorrectly configured or maintained operating system
		Lack of intrusion detection software
		Lack of update of Operating System security patches

Physical Infrastructure	Access from the sea for vessels docking in the facility incidents	The port facility doesn't have a communications procedure for when ships are performing any "hot work" (e.g. welding) on deck

		The port facility doesn't have a ready-to-use stock of protective clothing / equipment for responding to emergencies at the ship / shore interface
		The port facility doesn't have a communications procedure for when ships are performing any "hot work" (e.g. welding) on deck
		The port facility staffis not trained to respond to all types of emergency at the vessel/shore/sea interface (fire, explosion, near drowning, ship hitting a dock, C494another ship, earthquake, etc.)
		The response time for fire incidents and/or explosion at or near the port, is unacceptable
		There are no policy procedures for bilge and waste removal of the vessels
		There are no policy procedures for fueling and watering of the vessels
		There are no policy procedures for removal of used oil of the vessels
		There are no policy procedures for unloading and loading of goods of the vessels
		There are sea-lanes that pass near the ship (200 meters or less)
		There are situations in which services are given to vessels from the seaward side, but without security monitoring
		There is a manoeuvring and docking area for vessels with hazardous material and fuel near a crowd concentration (passenger terminal, large hall, etc…)
		There is not a system for classifying / vetting employees providing port services on the seaward side
	Analysis of maneuvering, docking and storage areas failures	Itis not possible to immediately tow a vessel away using a tugboat
		The areas in the facility are not categorized per type of good (Container quay, Fuel, Hazardous materials, etc.)
		The not properly divided into areas
		The facility's rear area has unmonitored storage facilities for goods in transit
		The port facility doesn't disseminate written procedures to the ship before handling freight, coal/fuel tanks and/or ballast
		The port facility doesn't disseminate written procedures to the ship regarding emergency shutdown of all activities, before handling freight, coal/fuel tanks and/or ballast
		The port facility doesn't have a policy for cargo barges to maneuver alongside the quay to work with the goods
		The port facility doesn't provide docking and mooring services according to policy procedures
		The port facility has open / roofed / thermoregulated storage areas / shelters but are not properly identified

		The port facility supplies/serves only ships with their own derricks
		The type of building the port facility has is not classified (Solid wharfs, Foundation walls, etc)
	Analysis of vessel traffic systems at the facility and navigation aids failures	Regular sea shuttle services are not reported and monitored
		The duties policy for supply of water and/or food is not clear
		The duties policy for fueling and oils is not clear
		The duties policy for pilotage is not clear
		The duties policy for repair service is not clear
		The duties policy for towing services is not clear
		The duties policy for waste and bilge disposal is not clear
		The facility doesn't have a pilot boat service policy
		The facility operates sea services (towing, waste disposal, water supply, fuel supply, etc.) Outside policy and/or procedures.
		There is no clear policy per type of vessels reporting requirements
	Areas containing hazardous materials and goods failures	The area is dominated by other points outside the facility
		The area is ineffectively guarded
		The areais not properly defined and marked
		The physical measures for restricting access to the area are inefficient
		The site can't be easily identified
		There are ineffective procedures that cover the approach to the area
		There are no detection and tracking devices in the area
		There is an inadequate process of access control to the area
		There is inadequate control over the entry and exit of freight to and from the area
		There is no backup communication channel
		There is no backup electricity
		There is no efficient process of approach control to the area
		There is no emergency response process
		There is no suspicious movements detection process
	Areas holding sensitive security-oriented information failures	The area is dominated by other points outside the facility
		The area is ineffectively guarded
		The area is not properly defined and marked
		The physical measures for restricting access to the area are inefficient
		The site can't be easily identified

		There are ineffective procedures that cover the approach to the area
		There are no detection and tracking devices in the area
		There is an inadequate process of access control to the area
		There is inadequate control over the entry and exit of freight to and from the area
		There is no efficient process of approach control to the area
		There is no emergency response process
		There is no suspicious movements detection process
	Areas where security and tracking equipment is stored or located failures	The area doesn't have adequate physical security
		The area is dominated by other points outside the facility
		The area is ineffectively guarded
		The area is not properly defined and marked
		The facility doesn't have backup electricity
		The physical measures for restricting access to the area are inefficient
		The site can't be easily identified
		There are ineffective procedures that cover the approach to the area
		There are no detection and tracking devices in the area
		There is an inadequate process of access control to the area
		There is inadequate control over the entry and exit of freight to and from the area
		There is no efficient process of approach control to the area
		There is no emergency response process
		There is no suspicious movements detection process
	Berthing area failures	Appropriate controls based on the number of vessels being serviced are in place
		Control over the entry and exit of freight to and from the area is poorly executed
		Port Facility and berthing of vessels are influenced by tidal variations/conditions
		The area is dominated by other points outside the facility
		The area is not defined nor properly marked
		The area is not properly patrolled
		The area is poorly guarded
		The personel dosent have the equipment to guard the area
		The personnel is not properly trained to guard the area
		The personnel is not properly trained to patrol the area
		The site identification and mapping is poor

		The vessels docking alongside the port facility don't always do so with a Pilot on board / respecting the Port Facility procedures.
		There are no or insufficient detection and tracking devices in the area
		There are no physical measures for restricting access to the area
		There are no procedures that cover the approach to the area
		There are no procedures to search waterfront areas for explosives or other dangerous devices prior to a ship arrival at PF or aterfronts that have been unmanned or unmonitored
		There is no assignment of responsibilities for access control
		There is no process of approach control to the area
		There is no proper process of access control to the area
		There is no training for access control personnel
	Cargo facilities and equipment, and storage areas for general freight failures	Containers that are accepted without a departure date are not adequately monitored
		The access control to the storage areas is not properly monitored
		The freight storage areas are not properly fenced off
		The storage areas are not properly guarded
		The tracking or handling of containers that have not left the port despite passing their expiration date is not properly executed
		There is no adequate process for facility that are designated as restricted area
		There is no procedure for guarding the storage facilities
		There is not process for tracking or handling of containers that have not left the port despite passing their expiration date
	CCTV Failure	Camera equipment, doors, drawers and removable panels are not secured with key locks or screws and are not equipped with tamper proof switches
		Is there an alternate or independent power source available for use on the system in the event of power failure
		Maintenance records are not retained or are retained for short periods
		Personnel are not trained for operating the CCTV System
		The CCTV system doesn't view the perimeter fence/wall
		The existing lighting along the fenceis not suitable for the specific camera types
		The information is not saved effectively or for the long term
		The system doesn't have recording capabilities
		The system doesn't technically meet the operational needs
		The system effectively doesn't cover its viewing sector
		The system is deployed in accordance with the nature of the terrain

		The systemis not advanced or high-quality
		The systemis not monitored 24 hours by security personnel in a Security Control Room
		The systemis not utilized
		The systemis not well or at all maintained
		The system's current utilization is close to the maximum
		There are not any procedures for operating the system
	Command and control rooms at the facility failures	The command rooms are not protected as restricted areas
		The control rooms are not efficiently connected to electrical backup systems
		The control rooms are not properly manned throughout the day
		The control rooms are not properly manned throughout the night
		The control rooms are not protected with alarm systems
		The control rooms don't have fire detection systems
		The control rooms don't have fire extinguishing systems
		The entrances to the control rooms are not guarded
		There is no or inadequate access control system for the control rooms
	Contamination	Back-up files and systems not available
		Lack of maintenance of equipment and facilities
		Location is in an area susceptible to environmental conditions such as contamination, electronic interference extreme temperature and humidity vermin
		No business continuity plans or procedures for recovery of information and information assets
	Control rooms for vessel management systems, activity control and security control at the facility failures	The communications equipmentis not properly maintained
		Each Port Facility security force doesn't have their own communications system with direct communications between a security control/communications center and each security unit
		The area is dominated by other points outside the facility
		The area is ineffectively guarded
		The areais not properly defined and marked
		The communication system is not capable of transmitting instructions to all security forces simultaneously in a rapid or timely manner in emergency situations
		The communication system is not capable of transmitting instructions to all security forces simultaneously in a rapid or timely manner in normal situations
		The physical measures for restricting access to the area are inefficient
		The security communications center doesn't have adequate physical security

		The site can't be easily identified
		There are ineffective procedures that cover the approach to the area
		There are no detection and tracking devices in the area
		There is an inadequate process of access control to the area
		There is inadequate control over the entry and exit of freight to and from the area
		There is no alternate means of communication available to the security force
		There is no alternate or independent power source for security and communications systems
		There is no efficient process of approach control to the area
		There is no emergency response process
		There is no suspicious movements detection process
	Control systems at gates Failure	There are not any access control policy procedures
		Thereis not any access control policy training
		If logging is done by electronic means, is there a paper back up system
		No X-ray machines in the entrances
		The access control systemis not properly monitored from a C4I
		The CCTV systemis not monitored by appropriate / designated personnel
		The entrances don't have a CCTV system
		The entrances don't have a PA system
		The entrances don't have a pit for inspecting vehicle undersides
		The entrances don't have adequate access control systems
		The entrances don't have walkthrough metal detectors
		The logging of personal datais not approved by a Data Protection authority
		The movements of those entering and exiting the facility are not logged at the entrances
		The person entrances don't X-ray machines
		There are not adequate alarm systems at the entrance point
		There are not any designated areas where persons can be searched in privacy
		There is no process for logging of persons, vehicles
		Thereis not any access control policy
	Crowd concentration areas failures	Crowd concentrations are formed at the public points and no monitoring procedures exist
		People are not inspected before entering the crowd concentration
		The concentrations that are long long-lasting are not observed nor monitored for suspicious movements

		The concentrations that are occasional are not observed nor monitored for suspicious movements
		The crowd concentration points are not protected nor guarded
		The crowd concentrations are not visible from dominant points
		The crowd concentrations characteristics are not observed
		The exits/entrances don't enable rapid crowd evacuation in cases of emergency
		There are no PA systems in the crowd concentration points
		There areas for storing sensitive / hazardous materials near crowd concentration points
		There is no backup communication channel
		There is no backup electricity
		Thereis not any security procedure for crowd concentration at the port facility
	Denial of Service	Inadequate network management (resilience of routing)
	Earthquake	Back-up files and systems not available
		Location is in an area susceptible to natural disasters
		No business continuity plans or procedures for recovery of information and information assets
	Electricity, communication and telecommunication systems, and computer and network systems failure	The Access control system at the facility doesn't have electrical backup
		The alarm systems are not connected to a manned control center
		The backup copies are not saved where the policy instructs
		The communication system nodes are not adequately protected
		The computer rooms don't have effective access control system
		The computer rooms don't have effective automatic fire extinguishing systems
		The computer rooms don't have effective break-in detection system
		The computer rooms don't have effective fire detection systems
		The computer rooms don't have effective room locking
		The computer rooms don't power supply backup system have effective
		The Computer system at the facility doesn't have electrical backup
		The computers are not backed up per the policies
		The electrical substations are not equipped with
		The electrical substations are not equipped with Automatic fire extinguishing systems
		The electrical substations are not equipped with break-in detection system
		The electrical substations are not equipped with fire detection systems
		The electrical substations are not locked rooms

		The electricity plans are not available
		The facility doesn't have a substation
		The facility doesn't have more than one computer center for backup purposes
		The facility is not powered by more than one electricity sources
		The facility main electrical panel is not easily approached
		The general power supply backup for the facility through autonomous electricity generator is not enough
		The general power supply backup for the facility through UPS is not enough
		The Generator at the facility doesn't have electrical backup
		The network doesn't have built-in survivability and redundancy (Alternative communication channels and equipment with recovery ability in case of a fault)
		The security force at the facility doesn't have direct wireless communications with outside security agencies (Police, Coast Guard, Army, Fire brigade, Medical, etc)
		The Server system at the facility doesn't have electrical backup
		The servers are not located in the computer room
		The Shipping traffic management system at the facility doesn't have electrical backup
		The Unloading control system at the facility doesn't have electrical backup
		The UPS at the facility doesn't have electrical backup
		The utility system sites at the site are not safely guarded
		The various electrical panels at the facility are not equipped with Access ControlSystems
		The various electrical panels at the facility are not equipped with Automatic fire extinguishing systems
		The various electrical panels at the facility are not equipped with Break-in detection systems
		The various electrical panels at the facility are not equipped with fire detection systems
		The various electrical panels at the facility are not securely protected
		The wireless communication systems don't have a backup for when there are faults / power cuts
		There are inadequate / no procedures for guarding the utility sites at the facility
		There are no anti-virus devices installed on the servers
		There are no electronic hacking detection programs
		There are no electronic hacking prevention programs (Firewall)
		There are no organized and defined data backup procedures for the computer system

		There is (are) no secondary power supply line(s) which are separated from the primary power line(s) that are able to provide hot-plug switch
		There is no available capacity through autonomous electricity generator systems for the whole facility
		There is no disaster recovery mechanism in the system
		There is no effective backup for the computer centers
		There is no effective backup policy for the computer centers
		There is no efficient central communication network in the facility
	Electronic Interference	Back-up files and systems not available
		Electromagnetic radiation
		Electrostatic charges
		No business continuity plans or procedures for recovery of information and information assets
	Equipment Failure	Inadequate change control settings
		Incomplete / incorrect maintenance
		Non periodic replacement
		Susceptibility to electromagnetic radiation
		Susceptibility to moisture, dust, dirt
		Susceptibility to temperature fluctuations
		Susceptibility to voltage fluctuations
	Extremes of Temperature and Humidity	Back-up files and systems not available
		Improper or inappropriate maintenance of technical facilities
		Inadequate backup policy
		Inadequate change management procedure for infrastructure components
		Inadequate data backup procedure for both software and data
		Inadequate monitoring of environmental conditions
		Inadequate Physical and Environmental Security Policy and Procedures
		Inadequate Recovery Procedure
		Lack of a uniform physical security policy enforcement
		Lack of back-up facilities or processes
		Lack of environmental protection
		Location is in an area susceptible to environmental\ conditions such as extreme temperature and humidity

		Location is in an area susceptible to environmental conditions such as contamination, electronic interference extreme temperature and humidity vermin
		No business continuity plans or procedures for recovery of information and information assets
		No concrete assignment of Continuity/Disaster-related roles and responsibilities
		No formal or informal disaster/recovery plans
	Facility entrance gates failures	All perimeter gates guarded or secured are properly locked when not in use
		Crowds are concentrated in adequate distance from the gates
		The electrically opened gates can't be opened manually
		The gate can be broken into by driving through it, to penetrate the facility
		The gates and/or other entrances in perimeter barriers are not kept to the minimum number required for safe and efficient operations
		The gates can't be anchored to the ground
		The gates don't provide protection equivalent to that provided by the barrier of which they are part
		The guard post at the entrance is properly illuminated
		The keys are kept in a specific place
		The keys' cabinets are secure and only authorized personnel can access them
		The lighting fixtures are efficient and effective per type of entry / exit
		The number of combined vehicle & pedestrian gatesis not recognized nor maintained
		The number of gates for emergencies or special incidents onlyis not recognized nor maintained
		The number of pedestrian-only gatesis not recognized nor maintained
		The number of railway gatesis not recognized nor maintained
		The number of staff-only gatesis not recognized nor maintained
		The number of vehicle-only gates at the facilityis not recognized nor maintained
		The public waiting areas are properly monitored
		The vehicle gates can't prevent a vehicle from breaking through into the facility
		The vehicle gates don't prevent the entry of an unauthorized vehicle to the facility
		The waiting areas are not near sensitive locations
		There are lighting fixtures in the entrance area
		There are security processes for crowd concentrations at the entrances
		There are not adequate means to ensure that vehicles slow down near the gate
		There gates for administration only and are accordingly inspected

		Thereis not any entry / exit policy for each gate
		Thereis not any entry / exit policy for each type of gate
		There special gates and entrances for freight that are accordingly inspected
	Facility inlets and entry processes failures	Customs personnel boards on ships before the ships enter the port but without proper information sharing and communications
		Every vessel entering the facility is required to report over a non-trusted network
		Security personnel boards on ships before the ships enter the port but without proper information sharing and communications
		The facility's entrance doesn't have a manned observation post for visually identifying the vessels at the facility's inlet
		The facility's entrance doesn't have an anti-diver protection system
		The facility's inlet can't effectively identify divers
		The information consumers are not properly identified
		The inlet allows more than one vessel to pass through at once
		The PFSO / policy doesn't cover all inlets the facility has
		The ships that enter the facility only by towing don't have effective communications
		There are areas that are restricted (for entry/maneuvering) at the facility's inlet which are not monitored
		There is no binding procedure of written security reporting
		There is no binding security screening process that takes place outside the port
		There is no procedure / written guidelines for operating a maritime patrol launch
		There is no procedure for summoning a maritime patrol launch
		There is no procedure or policy for hull inspections by divers
		There is no risk profiling systems
		Vessels entering the facility are assisted by external electronic navigation aids belonging to port or national infrastructure over untrusted networks
		Vessels entering the facility require an entry pass but the user rights assignment process is not secure
		Vessels entering the facility require external electronic navigation aids belonging to port or national infrastructure over untrusted networks
	Failure of outsourced operations	Back-up files and systems not available
		No business continuity plans or procedures for recovery of information and information assets
		The communications equipmentis not properly maintained

	Failures at other sites at the port facility requiring restricted access	Each Port Facility security force doesn't have their own communications system with direct communications between a security control/communications center and each security unit
		The area is dominated by other points outside the facility
		The area is ineffectively guarded
		The areais not properly defined and marked
		The communication system is not capable of transmitting instructions to all security forces simultaneously in a rapid or timely manner in emergency situations
		The communication system is not capable of transmitting instructions to all security forces simultaneously in a rapid or timely manner in normal situations
		The physical measures for restricting access to the area are inefficient
		The security communications center doesn't have adequate physical security
		There are ineffective procedures that cover the approach to the area
		There are no detection and tracking devices in the area
		There is an inadequate process of access control to the area
		There is inadequate control over the entry and exit of freight to and from the area
		There is no alternate means of communication available to the security force
		There is no alternate or independent power source for security and communications systems
		There is no efficient process of approach control to the area
		There is no emergency response process
		There is no suspicious movements detection process
	Failures in the utilities and systems such as power stations, freight conveyance and water supply pipelines	Access to the main water shut-off valveis not controlled nor supervised
		Adequate measures are not taken to prevent poisoning of the facility's central water system
		Damage to the conveyance systems immediately stops works at the facility
		Pipes carrying hazardous materials enter the facility
		Regular water quality tests are not conducted at the facility
		The access to the conveyance systemsis not restricted nor controlled
		The conveyance systems are not adequately connected to electricity supply backup systems
		The conveyance systems are not effectively guarded
		The facility doesn't have a power station inside it
		The facility doesn't have adequate mobile water tanks
		The facility doesn't have adequate stationary water tanks

		The facility hasn't identified the water sources
		The facility's main water shut-off valveis not inside the facility boundaries
		The fire-fighting systems depend on water arriving from outside sources
		The hazardous material pipes are not underground throughout the facility and the nearby area
		The power station areais not effectively guarded
		The water at the facility is also used for cooling sensitive systems
		The water systemis not connected to a backup for continued functioning, such as a generator
		There are no procedures covering the various utility systems at the facility
		There are no effective inspections at the entrance to the power station
		There is no water supply control system
	Fire	Availability of flammable materials such as paper or boxes
		Back-up files and systems not available
		Lack of fire detection devices
		Lack of Physical Security
		Location is in an area susceptible to natural disasters
		No business continuity plans or procedures for recovery of information and information assets
	Flood	Back-up files and systems not available
		Location is in an area susceptible to natural disasters
		No business continuity plans or procedures for recovery of information and information assets
	Ground patrols on the perimeter failures	Assignment of patrols to agenciesis not clear (Coast Guard, Police, Security guards working at the facility (regular employees), Employees of a private security company)
		How many patrols are held simultaneously at the facility?
		Patrols are not held adequately on weekends
		Security force personnel doesn't record or report their presence at key points in PF by means of portable watch clocks, general watch clock stations, or telephones
		The frequency patrolis not enough
		The patrol personnelis not equipped with individual protective gear
		The patrol personnelis not trained (initial training)
		The patrol personnelis not trained (routine exercises)
		The patrol personnelis not trained (unexpected exercises)

		The patrol personnelis not trained (update training)
		The patrol's response time to an incident or identificationis not reasonable
		The patrols are held only on the inside of the facility
		The patrols are only held outside the fence, in the peripheral zone
		The patrols are routine and operate at specific times without changing the routine
		The patrols are not equipped with firearms or the reasonable means for stopping an attacker/infiltrator
		The patrols are not equipped with suitable communication and lighting equipment
		The patrols' type (mobile, on foot, inside the facility, outside, etc) is not in accordance with the facility type
		The security force doesn't have sufficient, adequately equipped vehicles to maintain patrols, respond to alarms and emergencies and maintain supervision
		The security force vehicles are not equipped with signs conspicuously identifying vehicle as a security police vehicle, emergency exterior overhead lights, and an electronic siren
		There are not any procedures for operating patrols
		There are not any security patrols along the fence
		There is no alternative plan for patrols and guarding for sensitive areas in the case of employee strikes
	Hazardous/sensitive material storage facilities failures	Patrols and inspections are not effectively held in hazardous material storage areas
		The access control system for areas storing sensitive / hazardous materials is ineffective
		The entrances to Hazardous/sensitive material storage facilities are not properly guarded
		The facilities containing hazardous materials are not marked in a manner that indicates their content
		The guidelines on the storage or placement of materials intended to prevent contact between types of materials that can cause an explosion or blaze are not respected
		The hazardous area doesn't have an emergency evacuation plan
		The hazardous area doesn't have an emergency plan
		The location of the sensitive storage facilities don't provide a reasonable response to terrorist attacks from outside the facility
		The monitoring devices in the sensitive areas are ineffective
		The monitoring devices in the sensitive areas are not serviced as indicated
		The monitoring devices in the sensitive areas don't work
		The PA / warning systems in the sensitive areas is ineffective
		The personnel doesn't perform drills as planned

		The personnel is not adequately trained for the Hazardous area
		The personnel is not aware of the entire area
		The separation / fence / barrier systems that prevent free access to sensitive / hazardous material storage facilities are ineffective
		The traffic and storage of hazardous material is not properly logged
		There is no policy or restrictions to accepting goods that do not have a departure date
		There are ineffective / out of scope hazardous material warehouse security regulations
		There are no separate storage facilities for hazardous materials
		There are no separate storage facilities for inflammable materials
		There is no 24x7 continuous guard at the hazardous materials storage sites
		There is no assignment of responsibility / authority of safety in the sensitive areas
		There is no backup communication channel
		There is no backup electricity
		There is no emergency response process
		There is no policy or restrictions to accepting goods at the facility
		There is no suspicious movements detection process
	Hurricane	Back-up files and systems not available
		Location is in an area susceptible to natural disasters
		No business continuity plans or procedures for recovery of information and information assets
	Incidents that have occurred at the port facility	Warnings and signs at the port facility are not observed and communicated properly
	Industrial Action	Lack of an industrial agreement
	Inspections at the gates – searches failures	There is no port search policy on searches of persons in place
		Goods are not properly inspected at the entrance
		Goods are not properly inspected at the exit
		Incoming passengers are not properly inspected at the entrance
		Is there a team of security personnel specialized in searching vehicles
		No adequate number of vehicles is inspected at the gates or elsewhere in the facility
		Ship crew members are not properly inspected at the entrance
		Ship crew members are not properly inspected at the exit
		Staff members are not properly inspected at the gate
		The gates can be bypassed, no adequate prevention systems in place
		The Port Search Policyis not prominently displayed

		The Port Vhicle Search Policyis not prominently displayed so that the drivers can see it
		The records of the searches are not adequately retained
		The records of the vehicles searches are not adequately retained
		There is no adequate communication channels for when searching persons
		There is no adequate communication channels for when searching vehicles
		There is no adequate personnel for goods to be properly inspected at the entrance
		There is no adequate personnel for goods to be properly inspected at the exit
		There is no adequate personnel for ship crew members to be properly inspected
		There is no adequate personnel for ship crew members to be properly inspected at the exit
		There is no adequate personnel for vehicles to be properly inspected at the entrance / exit
		There is no adequate port search policy on searches of vehicles entering and leaving the port in place
		There is no adequate procedure for goods to be properly inspected at the entrance
		There is no adequate procedure for goods to be properly inspected at the exit
		There is no adequate procedure for ship crew members to be properly inspected
		There is no adequate procedure for ship crew members to be properly inspected at the exit
		There is no adequate procedure for vehicles to be properly inspected at the entrance / exit
		There is no adequate training for goods to be properly inspected at the entrance
		There is no adequate training for goods to be properly inspected at the exit
		There is no adequate training for ship crew members to be properly inspected
		There is no adequate training for ship crew members to be properly inspected at the exit
		There is no adequate training for vehicles to be properly inspected at the entrance / exit
		There is no equipment for inspecting passengers
		There is no port search policy training for port personnel in place
		There is no process for inspecting passengers
		There is no team of legal personnel specialized in searching persons
		There is no team of legal personnel specialized in searching vehicles
		There is no team of security personnel specialized in searching persons
		There is no team of security personnel specialized in searching vehicles
		Vehicles are not properly inspected at the entrance/exit
		Security teams on ships don’t identify the facility’s security team

	Interface between security forces at the facility and security forces on vessels failures	The Declaration of Security procedures don't include the circumstances in which a DoS is required
		The Declaration of Security procedures don't include the responsibilities between the port facility and the ship
		The Declaration of Security procedures don't include the security activities to be implemented
		The emergency plan doesn't cover properly evacuating passengers from a docked ship
		The passengers are not inspected both when boarding and leaving the ship
		The responsibility of the security team on a ship start when it ascends the ship's gangway or an alternative entrance
		The security team hasn't been drilled in shooting in the vicinity of vessels
		The ship's security crew doesn't monitor the security inspections whenaccommodating goods, food and maintenance supplies
		The ship's security officer doesn't have a ship security activity plan covering emergencies at the facility
		The ship's security officer doesn't keep (on deck) a ship security activity plan covering emergencies at the facility
		The team doesn't use technological tools for screening items brought on board
		There is no effective supervision to prevent stowing away on the ship
		There is no process for security teams to be recognized / identified
		There is no process for when stowaways are found (e.g. does the port security team have responsibility for guarding him/her?)
		Thereis not a validated process for transferring information on suspicious passengers within the contact between the port facility and ship facility
		Thereis not any effective emergency communication channel between the ship and the security forces at the facility
		Thereis not any proper procedure for reporting a change in the alert level of the facility for ports docking inside it
		Thereis not proper division of sectors between the facility's security force and the ship's security team
	Lighting Failure	All areas with a lighting system are illuminated throughout the hours of darkness (sunset to sunrise) and periods of low visibility
		Docks, piers, wharfs and other working areas are not illuminated in a manner not to interfere with navigation with continuous lighting when there is any activity in these areas as a safety precaution

		Open yards are not illuminated with continuous or standby lighting
		Parking lots are not illuminated
		Parking lots are not illuminated in a manner to prevent shadows and areas of poor illumination between vehicles, and the illuminationis not even throughout the lot
		Pedestrian entrances are not illuminated with continuous lighting for open pedestrian entrances and standby lighting for pedestrian entrances that are locked or otherwise not accessible until security personnel authorize entry
		Repairs to lighting systems and replacement of inoperative are lamps effected immediately or in a reasonable time
		The facility doesn't have a lighting system
		The facility has an emergency backup power source for its protective lighting system
		The lighting aimed inward and outward
		The lighting doesn't operate regularly
		The lighting is activated throughout the hours of darkness (sunset to sunrise) and periods of low visibility
		The lighting system doesn't effectively illuminate the perimeter area so as to give effective detection capabilities
		The lighting systemis not deployed along most of the facility's perimeter
		The lighting systemis not deployed along the facility's entire perimeter
		The lighting systemis not well maintained
		The perimeter of all restricted areasis not illuminated with continuous or standby lighting
		The perimeter protective lightingis not arranged so that security force patrol personnel remain in comparative darkness
		The system doesn't have a good combination of flood lighting and regular lighting
		There are provisions for standby or emergency protective lighting
		There is no lighting flood lighting
		Thereis not an effective lighting system inside the facility
		Thereis not any strong lighting on the fence near sensitive areas
		Vehicle entrances are not illuminated
		Water approaches to dock, pier, or wharfs are not illuminated
	Malicious destruction of data and facilities	Lack of Physical Security
	Malpractice	Malicious Employees
		Unauthorized use of equipment
	Maneuvering and anchorage areas failures	The area is dominated by other points outside the facility

		The area is not defined nor marked
		The area is not properly guarded
		The site can't be easily identified
		There are no processes of access control to the area
		There are inadequate detection and tracking devices in the area
		There are no physical measures for restricting access to the area
		There are no processes of approach control to the area
		There are unclear procedures that cover the approach to the area
		There is limited or no control over the entry and exit of freight to and from the area
	Network Intrusion	Incorrectly configured or maintained security safeguards
	Operational security orders failures	Are all security posts, fixed and mobile, provided with security force orders
		Security posts, fixed and mobile are not provided with clear security force orders
		The division of forces and missionsis not suitable
		The facility doesn't operate according to the existing operation order
		The security force at the facility doesn't have operational orders
		The security force at the facility don't have a clear policy
		The security forces orders are not regularly reviewed by the PFSO
		The security order is outdated
		The security orders are mismatched to the operational need and actual application
	Other failures (including orders and plans, command and control, intelligence)	Measures taken for protecting information on computers (passwords, entry code, compartmentalization) are weak
		No communications channels have been established with Port Security Committees and local authorities
		No liaison has been established with Port Security Committees and local police whereby early warning of threat situation will be provided
		Sensitive and classified documents are not kept in a safe
		The dissemination of intelligence is executed over untrusted networks
		The existing security forces are not designed to provide effective responses to routine and emergency incidents
		The facility doesn't designate a person in charge of gathering, sorting and analyzing and evaluating intelligence material
		The facility doesn't have a clear information security procedure
		The facility doesn't have an intelligence unit

		The PF or the local community don't effectively maintain an organized, equipped and appropriate Crisis Response Force
		The PF or the local community don't effectively maintain an organized, equipped and appropriate Emergency Response Units
		The responsibilities are not defined for all facility workers with security oriented functions
		The security force doesn't have work plans (annual, monthly and weekly)
		The sources the intelligence system uses are not appropriate or validated
		The terrain file doesn't effectively cover the following thematic areas: police, fire brigade, army, other emergency forces
		The terrain file doesn't fulfill the operational needs
		The terrain fileis not available for review by security personnel
		There are contradicting objectives between the security guidelines and the regular operation of the facility
		There are no procedures for additional security forces to be brought in during emergency or crisis situations
		There are not clear and robust role assignments in the security forces with established routine and emergency authorities
		There is no clear distribution of responsibility between the security forces at the facility and outside forces
		There is no fault plan in the file
		There is no plan for disseminating intelligence (who consumes what)
		Thereis not a clear command and control plan from the individual to the department level
		Thereis not a clear definition of security objectives and priorities
		Thereis not a clearly defined command and control system
		Thereis not a valid emergency plan in the terrain file
		Thereis not any /an updated a terrain file for the facility
		Thereis not any clear procedure for changing deployment, reinforcement or making procedures more stringent following intelligence information
		Thereis not any systems for providing intelligence to various consumers
		Thereis not regular providing of intelligence material
		There port missions that are not covered by security objectives
	Other sites at the port facility requiring restricted access	The site can't be easily identified
	Passenger and crew member screening and waiting areas	The area is dominated by other points outside the facility
		The area is not defined nor marked

		The area is not properly guarded
		The crowd concentrated in the bus embarkation and disembarkation stop is not properly monitored or controlled
		The crowd concentrated in the facility staff dining rooms is not properly monitored or controlled
		The crowd concentrated in the incoming passenger terminal is not properly monitored or controlled
		The crowd concentrated in the metro station near the facility is not properly monitored or controlled
		The crowd concentrated in the outgoing passenger terminal is not properly monitored or controlled
		The crowd concentrated in the passenger entrance gate is not properly monitored or controlled
		The crowd concentrated in the passenger vehicle parking lot is not properly monitored or controlled
		The crowd concentrated in the passenger vessels waiting areas in not properly monitored or controlled
		The crowd concentrated in the staff entrance gate is not properly monitored or controlled
		The crowd concentrated in the vessel loading and unloading point is not properly monitored or controlled
		The crowd concentration can’t be easily observed from outside the facility
		The crowd is concentrated in designated areas
		The exit gateis not separated from the entrance gate
		The procedures that cover the approach to the area are inefficient
		The public enters the terminal using multiple entrances
		The site can’t be easily identified
		The terminal is near the entrance gate
		The terminal is near the perimeter fence (50 meters)
		The terminal is not an enclosed building
		There are no processes of access control to the area
		There are hazardous material storage areas near the crowd concentrations in the facility
		There are hazardous material transport routes that pass adjacent to the crowd concentrations in the facility
		There are inadequate detection and tracking devices in the area

		There are inadequate procedures for securing and guarding the passenger terminals at the facility
		There are no physical measures for restricting access to the area
		There are no processes of approach control to the area
		There are not any separate terminals for international and domestic shipping
		There are not proper security inspections at the terminal entrance
		There is a crowd concentration by day/night
		There is no control over the entry and exit of passengers / crew to and from the area
	Perimeter Incidents	Are all sensor equipment, doors, drawers and removable panels secured with key locks or screws and equipped with tamper proof switches?
		Are maintenance records retained and for how long?
		Are records of these inspections and/or test maintained and easily accessible?
		Are there concealed areas or disruptions along the fence that interfere with the system's functioning?
		Are there security procedures relating to the systems?
		Can the system be easily damaged or disrupted?
		If building walls, floors and roofs form a part of the barrier, are they complemented by another means of intrusion detection such as CCTV or motion detection sensors?
		Implementation of a detection system along the fence/wall
		Implementation of an detection/identification system advanced from the perimeter
		Implementation of an identification system along the fence/wall
		Is the system inspected and/or tested at least monthly?
		Is the system monitored 24 hours by security personnel in the Security Control Room?
		Is the system suitable for the climatic conditions characteristic to the facility?
		Is the system suitable for the topographic and environmental conditions?
		Is the viewing system well maintained?
		Is there an alternate or independent power source available for use on the system in the event of power failure?
		Technical resources on the fence
		Warning and alarm systems working well
	Personnel (general / security force) – frameworks, units and personnel in the security forces failures	Functions are not manned at a reasonable level
		No background check is performed prior to hire and regularly thereafter for every employee who has a role in PFSP or who has access to restricted areas
		Reserve and alert forces are not kept at the facility in routine

		The security force can't be reinforced immediately in emergencies
		The security force size changes in the night shift
		The security force size changes in the weekend
		The security officeris not involved in the processes of locating, sorting and hiring workers for the facility
		The security workers are not facility employees
		The security workers don't undergo regular / periodical security checks
		The security workers don't undergo security / criminal background checks
		The training doesn't fulfill the defined needs
		There are security personnel who work in shifts exceeding 10 hours
		There are not any armed security guards at the facility
		There are not appropriate criteria for hiring general workers at the facility
		There are not appropriate criteria for hiring security workers at the facility
		There are not basic criteria for hiring general workers at the facility
		There are not basic criteria for hiring security workers at the facility
		There are not clear standards for assessing the performance of all workers at the facility
		There are not clear standards for assessing the performance of the security staff at the facility
		There are not differing levels of security checks for workers in sensitive areas
		Thereis not any procedure for immediate security force reinforcements in emergencies
		Thereis not appropriate theoretical training for security workers
		Thereis not appropriate theoretical training process for security workers
		Thereis not practical training for security workers
	Personnel and procedures at the gates failures	The entrance area doesn't enable effective functioning in stormy weather
		The guard at the entrance can't cover the gate area nor effectively observe and identify opponents / incidents
		The guards at the gates are adequately trained
		The guards at the gates are adequately trained and drilled by the facility's security officer
		There are not any changes at the gates during hours of darkness or on weekends
		There are not clear instructions for cases and responses at the entrance gates
		There are not clearly communicated and trained emergency procedures
		There are not clearly communicated and trained instructions for cases and responses at the entrance gates

		There are not clearly communicated and trained instructions regarding acceptable civilian activities at the gates
		There are not clearly communicated and trained instructions regarding security activities at the gates
		There are not clearly communicated and trained procedures regarding regular acceptable activities at the gates
		There are not clearly written emergency procedures
		There are not clearly written instructions regarding security activities at the gates
		There are not clearly written procedures regarding regular acceptable activities at the gates
		There are not many guards at each gate
		There are not many guards on each shift
		There is no proper assignment of responsibilities for supervising and controlling the guards at the gates
	Personnel Incidents	Absence of personnel
		Inadequate recruitment procedures
		Incorrect use of software and hardware
		Insufficient security training
		Lack of monitoring mechanisms
		Lack of policies for the correct use of telecommunications media and messaging
		Lack of security awareness
		Unsupervised work by outside or cleaning staff
	Port facilities structural integrity incidents (quays, facilities and infrastructures)	The buildings in the facility are not properly recognized / categorized / risk profiled
		The buildings in which hazardous materials are stored don't fulfill safetyrequirements
		The sensitive buildings are located adjacent to the perimeter fence
		There are no clear procedures for inspecting the structural integrity of thebuildings
		There is no designated personnel to examine the condition of the buildings at the facility
	Port Facility Incidents	Analysis of access routes per types of cargo
		Analysis of access routes per types of facility
		Analysis of access routes per types of vehicles
		Analysis of environment and population characteristics that can affect the facility
		Classification of unregulated entry / exit routes that enable uncontrolled entry/exit into/out of the facility
		Designation of authorized approach routes for employees

		Designation of authorized approach routes for employees in case of emergency
		Designation of authorized approach routes for people
		Designation of authorized approach routes for people in case of emergency
		Designation of authorized approach routes for vehicles
		Designation of authorized approach routes for vehicles in case of emergency
		Designation of authorized exit routes for employees
		Designation of authorized exit routes for employees in case of emergency
		Designation of authorized exit routes for people
		Designation of authorized exit routes for people in case of emergency
		Designation of authorized exit routes for vehicles
		Designation of authorized exit routes for vehicles in case of emergency
		Designation of Crowd concentration areas
		Removal of obstacles
		Topography of the facility awareness (maps, communications)
		Analysis of connection to major external utility systems
		Analysis of past fence/wall penetrations and security upgrades
		Communications processes for security awareness with other PF
		Conditions of the perimeter fence/wall
		Designation of responsibilities for perimeter inspection
		Designation of responsibilities for perimeter maintenance
		Development of a delaying fence before the fence/wall
		Distance of the fence /wall from sensitive areas to enable an adequate responsetime by the security forces
		Effectiveness of the delaying fence
		Maintenance of inspections' records
		Other facilities in the periphery of the port facility that can affect it or be affected by it
		Port boundaries are not explicitely set
		Security, rescue and medical forces categorization and identification
		The perimeter and the clear zone is not inspected regularly and their condition assessed (wear and tear, erosion etc)
		The port's surroundings are not clearly communicated to personnel
		The port's surroundings are not clearly communicated to stakeholders
	Power Fluctuations	Back-up files and systems not available

		Improper or inappropriate maintenance of technical facilities
		Inadequate change management procedure for infrastructure components
		Inadequate monitoring of environmental conditions
		Inadequate Physical and Environmental Security Policy and Procedures
		Lack of a uniform physical security policy enforcement
		Lack of environmental protection
		Location is in an area susceptible to power fluctuations
		No business continuity plans or procedures for recovery of information and information assets
		No Uninterruptible Power Supply equipment
	Private security companies failures	The guards stay for long at the facility
		The private company guards are not armed
		The private company guards are not considered as Port Facility employees
		The private company guards are not trained
		The private company guards don't have authority
		The private company guards have different / loose employment standards
		The security guards don't undergo security vetting and sorting
		The security officer can't intervene in the employment times of guards
		The security officer can't veto the employment of a problematic guard
		The security officeris not involved in the selection and training of the guards
		The security officeris not involved in the selection of the guards
		Thereis not any limitation to the areas where company guards can be employed
	Procedural Failures	Lack of safety requirements in contracts with customers and suppliers
		Application of the "Empty Office" & "Blank Screen" policies
		Inadequate response procedure for maintenance / repair
		Incomplete control for material exiting the facility
		Lack / Poor assigning of information security responsibilities
		Lack of administrative controls
		Lack of defined disciplinary process for handling security incidents
		Lack of formal approval process of published material
		Lack of formal installation process for corporate software
		Lack of formal process to enable/disable user passwords
		Lack of log files

		Lack of maintenance contracts and SLAs
		Lack of mechanisms for monitoring security breaches
		Lack of monitoring of sites where information is being processing
		Lack of problems / errors log files
		Lack of procedures to deal with classified information
		Lack of process for controlling copyrights
		Lack of reporting processes for safety risks
		Lack of risk assessment procedures
		Lack of security conditions in staff contracts
		Lack of security requirements in the job responsibilities of staff
		Lack of usage policies
		Lack of usage policy for corporate e-mails
		Minimum or no regular checks and site inspections
		There are not clearly written instructions regarding acceptable civilian activities at the gates
		Risk elevation from Level 1 to Level 2 fails
		Risk elevation from Level 2 to Level 3 fails
		The coordination procedures for receiving assistance from outside agencies (army, police, fire brigade, medical) are not appropriate
		The coordination procedures for receiving assistance from outside agencies (army, police, fire brigade, medical) are not clear
		The drills / exercises on emergency procedures for terrorist attacks are not appropriate
		The drills / exercises on entry control procedures are not appropriate
		The drills / exercises on hostage situation handling procedures are not appropriate
		The drills / exercises on on the procedures for communication between security forces inside the facility are not appropriate
		The drills / exercises on procedure for handling disembarking seamen and their families are not appropriate
		The drills / exercises on rules of engagement and opening fire are not appropriate
		The drills / exercises on security man and guard force procedures are not appropriate
		The drills / exercises on site opening and closing procedures are not appropriate
		The drills / exercises on the coordination procedures for receiving assistance from outside agencies (army, police, fire brigade, medical) are not appropriate

		The drills / exercises on The drills / exercises on the procedures for handling dignitaries (including arrangement with visitor bodyguards) are not appropriate
		The drills / exercises on The drills / exercises on the procedures for inspecting and handling vessel cargo are not appropriate
		The drills / exercises on The drills / exercises on the procedures for maintaining and updating hazardous goods and hazardous material records are not appropriate
		The drills / exercises on The drills / exercises on the procedures for screeners at gates and scanners are not appropriate
		The drills / exercises on The drills / exercises on the procedures for the all employees at the facility for receiving threat messages (anonymous / identified) by telephone, fax, letter, note at gate, etc are not appropriate
		The drills / exercises on The drills / exercises on the procedures for the security force for receiving threat messages (anonymous / identified) by telephone, fax, letter, note at gate, etc are not appropriate
		The drills / exercises on the procedure for defining array structure and chain of command are not appropriate
		The drills / exercises on the procedure for delivering goods to vessels are not appropriate
		The drills / exercises on the procedure for deploying ready squad / rapid intervention force are not appropriate
		The drills / exercises on the procedure for employing private security companies and defining missions and responsibilities are not appropriate
		The drills / exercises on the procedure for handling suspects (pedestrians, vehicles and suspicious objects) are not appropriate
		The drills / exercises on the procedure for inspecting mail and parcels, including by courier are not appropriate
		The drills / exercises on the procedure for locating faults in security measures and equipment and further full functioning of the security system are not appropriate
		The drills / exercises on the procedure for locating hazardous materials inside the facility are not appropriate
		The drills / exercises on the procedure for maritime patrol and observation force are not appropriate
		The drills / exercises on the procedure for protecting hazardous material storage areas are not appropriate
		The drills / exercises on the procedure for summoning / operating maritime patrols are not appropriate

		The drills / exercises on the procedures for communication between the security force in the facility and outside forces (vessels, national authorities, local authorities, outside security agencies) are not appropriate
		The drills / exercises on the procedures for cooperation with the security officers of vessels for identifying embarking / disembarking persons are not appropriate
		The drills / exercises on the procedures for ensuring continuous contact even during a fault or incapacitation of utility systems at the facility are not appropriate
		The drills / exercises on the procedures for evacuating the facility of workers in the case of a fire, earthquake, leak of hazardous materials, etc are not appropriate
		The drills / exercises on the procedures for general personnel at the facility are not appropriate
		The drills / exercises on the procedures for guard mounting / changing of watches are not appropriate
		The drills / exercises on the procedures for handling crowd concentrations are not appropriate
		The drills / exercises on the procedures for hiring personnel for the security force are not appropriate
		The drills / exercises on the procedures for operating the control room are not appropriate
		The drills / exercises on the procedures for reporting security activity or possible compromises to security are not appropriate
		The drills / exercises on the procedures for securing sensitive security information stored on paper or electronic media are not appropriate
		The drills / exercises on visitor, subcontractor and maintenance and logistic, cleaning and other team entry procedures for the facility are not appropriate
		The drills / exercises on visitor, subcontractor and maintenance and logistic, cleaning and other team entry procedures for vessels are not appropriate
		The emergency procedures for terrorist attacks are not appropriate
		The emergency procedures for terrorist attacks are not clear
		The entry control procedures are not appropriate
		The entry control procedures are not clear
		The facilities don’t undergo regular audits and inspections
		The facilities don’t undergo unannounced audits and inspections
		The hostage situation handling procedures are not appropriate
		The hostage situation handling procedures are not clear

		The periodic update training on emergency procedures for terrorist attacksis not appropriate
		The periodic update training on entry control proceduresis not appropriate
		The periodic update training on hostage situation handling proceduresis not appropriate
		The periodic update training on on the procedures for communication between security forces inside the facilityis not appropriate
		The periodic update training on procedure for handling disembarking seamen and their familiesis not appropriate
		The periodic update training on rules of engagement and opening fire isn' tappropriate
		The periodic update training on security man and guard force proceduresis not appropriate
		The periodic update training on site opening and closing proceduresis not appropriate
		The periodic update training on the coordination procedures for receiving assistance from outside agencies (army, police, fire brigade, medical)is not appropriate
		The periodic update training on The periodic update training on the procedures for handling dignitaries (including arrangement with visitor bodyguards)is not appropriate
		The periodic update training on The periodic update training on the procedures for inspecting and handling vessel cargois not appropriate
		The periodic update training on The periodic update training on the procedures for maintaining and updating hazardous goods and hazardous material recordsis not appropriate
		The periodic update training on The periodic update training on the procedures for screeners at gates and scannersis not appropriate
		The periodic update training on The periodic update training on the procedures for the all employees at the facility for receiving threat messages (anonymous / identified) by telephone, fax, letter, note at gate, etcis not appropriate
		The periodic update training on The periodic update training on the procedures for the security force for receiving threat messages (anonymous / identified) by telephone, fax, letter, note at gate, etcis not appropriate
		The periodic update training on the procedure for defining array structure and chain of commandis not appropriate
		The periodic update training on the procedure for delivering goods to vesselsis not appropriate
		The periodic update training on the procedure for deploying ready squad / rapid intervention forceis not appropriate

		The periodic update training on the procedure for employing private security companies and defining missions and responsibilitiesis not appropriate
		The periodic update training on the procedure for handling suspects (pedestrians, vehicles and suspicious objects)is not appropriate
		The periodic update training on the procedure for inspecting mail and parcels, including by courieris not appropriate
		The periodic update training on the procedure for locating faults in security measures and equipment and further full functioning of the security system is not appropriate
		The periodic update training on the procedure for locating hazardous materials inside the facilityis not appropriate
		The periodic update training on the procedure for maritime patrol and observation forceis not appropriate
		The periodic update training on the procedure for protecting hazardous material storage areasis not appropriate
		The periodic update training on the procedure for summoning / operating maritime patrolsis not appropriate
		The periodic update training on the procedures for communication between the security force in the facility and outside forces (vessels, national authorities, local authorities, outside security agencies)is not appropriate
		The periodic update training on the procedures for cooperation with the security officers of vessels for identifying embarking / disembarking personsis not appropriate
		The periodic update training on the procedures for ensuring continuous contact even during a fault or incapacitation of utility systems at the facilityis not appropriate
		The periodic update training on the procedures for evacuating the facility of workers in the case of a fire, earthquake, leak of hazardous materials, etcis not appropriate
		The periodic update training on the procedures for general personnel at the facilityis not appropriate
		The periodic update training on the procedures for guard mounting / changing of watchesis not appropriate
		The periodic update training on the procedures for handling crowd concentrationsis not appropriate
		The periodic update training on the procedures for hiring personnel for the security forceis not appropriate
		The periodic update training on the procedures for operating the control roomis not appropriate

		The periodic update training on the procedures for reporting security activity or possible compromises to securityis not appropriate
		The periodic update training on the procedures for securing sensitive security information stored on paper or electronic mediais not appropriate
		The periodic update training on visitor, subcontractor and maintenance and logistic, cleaning and other team entry procedures for the facilityis not appropriate
		The periodic update training on visitor, subcontractor and maintenance and logistic, cleaning and other team entry procedures for vesselsis not appropriate
		The personnel is not aware of the procedures
		The procedure for defining array structure and chain of command are not appropriate
		The procedure for defining array structure and chain of command are not clear
		The procedure for delivering goods to vessels are not appropriate
		The procedure for delivering goods to vessels are not clear
		The procedure for deploying ready squad / rapid intervention force are not appropriate
		The procedure for deploying ready squad / rapid intervention force are not clear
		The procedure for employing private security companies and defining missions and responsibilities are not appropriate
		The procedure for employing private security companies and defining missions and responsibilities are not clear
		The procedure for handling disembarking seamen and their families are not appropriate
		The procedure for handling disembarking seamen and their families are not clear
		The procedure for handling suspects (pedestrians, vehicles and suspicious objects) are not appropriate
		The procedure for handling suspects (pedestrians, vehicles and suspicious objects) are not clear
		The procedure for inspecting mail and parcels, including by courier are not appropriate
		The procedure for inspecting mail and parcels, including by courier are not clear
		The procedure for locating faults in security measures and equipment and further full functioning of the security system are not appropriate
		The procedure for locating faults in security measures and equipment and further full functioning of the security system are not clear
		The procedure for locating hazardous materials inside the facility are not appropriate
		The procedure for locating hazardous materials inside the facility are not clear

		The procedure for maritime patrol and observation force are not appropriate
		The procedure for maritime patrol and observation force are not clear
		The procedure for protecting hazardous material storage areas are not appropriate
		The procedure for protecting hazardous material storage areas are not clear
		The procedure for summoning / operating maritime patrols are not clear
		The procedures are not reviewed or validated by the facility management
		The procedures are not reviewed or validated by the institutional security agencies
		The procedures are not reviewed or validated by the security guards
		The procedures are not reviewed or validated by the Security Officer
		The procedures are not reviewed or validated by the shift managers
		The procedures don't cover all reasonable scenarios
		The procedures don't cover all routine and emergency situations
		The procedures for communication between security forces inside the facility are not appropriate
		The procedures for communication between security forces inside the facility are not clear
		The procedures for communication between the security force in the facility and outside forces (vessels, national authorities, local authorities, outside security agencies) are not appropriate
		The procedures for communication between the security force in the facility and outside forces (vessels, national authorities, local authorities, outside security agencies) are not clear
		The procedures for cooperation with the security officers of vessels for identifying embarking / disembarking persons are not appropriate
		The procedures for cooperation with the security officers of vessels for identifying embarking / disembarking persons are not clear
		The procedures for ensuring continuous contact even during a fault or incapacitation of utility systems at the facility are not appropriate
		The procedures for ensuring continuous contact even during a fault or incapacitation of utility systems at the facility are not clear
		The procedures for evacuating the facility of workers in the case of a fire, earthquake, leak of hazardous materials, etc are not appropriate
		The procedures for evacuating the facility of workers in the case of a fire, earthquake, leak of hazardous materials, etc are not clear
		The procedures for guard mounting / changing of watches are not appropriate

		The procedures for guard mounting / changing of watches are not clear
		The procedures for handling crowd concentrations are not appropriate
		The procedures for handling crowd concentrations are not clear
		The procedures for handling dignitaries (including arrangement with visitor bodyguards) are not appropriate
		The procedures for handling dignitaries (including arrangement with visitor bodyguards) are not clear
		The procedures for hiring personnel for the security force are not appropriate
		The procedures for hiring personnel for the security force are not clear
		The procedures for inspecting and handling vessel cargo are not appropriate
		The procedures for inspecting and handling vessel cargo are not clear
		The procedures for maintaining and updating hazardous goods and hazardous material records are not appropriate
		The procedures for maintaining and updating hazardous goods and hazardous material records are not clear
		The procedures for operating the control room are not appropriate
		The procedures for operating the control room are not clear
		The procedures for reporting security activity or possible compromises to security are not appropriate
		The procedures for reporting security activity or possible compromises to security are not clear
		The procedures for screeners at gates and scanners are not appropriate
		The procedures for screeners at gates and scanners are not clear
		The procedures for securing sensitive security information stored on paper or electronic media are not appropriate
		The procedures for securing sensitive security information stored on paper or electronic media are not clear
		The procedures for summoning / operating maritime patrols are not appropriate
		The procedures for the all employees at the facility for receiving threat messages (anonymous / identified) by telephone, fax, letter, note at gate, etc are not appropriate
		The procedures for the all employees at the facility for receiving threat messages (anonymous / identified) by telephone, fax, letter, note at gate, etc are not clear
		The procedures for the security force for receiving threat messages (anonymous / identified) by telephone, fax, letter, note at gate, etc are not appropriate

		The procedures for the security force for receiving threat messages (anonymous / identified) by telephone, fax, letter, note at gate, etc are not clear
		The rules of engagement and opening fire are not appropriate
		The rules of engagement and opening fire are not clear
		The security man and guard force procedures are not appropriate
		The security man and guard force procedures are not clear
		The security procedures for general personnel at the facility are not appropriate
		The security procedures for general personnel at the facility are not clear
		The site opening and closing procedures are not appropriate
		The site opening and closing procedures are not clear
		The training on emergency procedures for terrorist attacksis not appropriate
		The training on entry control proceduresis not appropriate
		The training on hostage situation handling proceduresis not appropriate
		The training on on the procedures for communication between security forces inside the facilityis not appropriate
		The training on procedure for handling disembarking seamen and their families isn't appropriate
		The training on rules of engagement and opening fireis not appropriate
		The training on security man and guard force proceduresis not appropriate
		The training on site opening and closing proceduresis not appropriate
		The training on the coordination procedures for receiving assistance from outside agencies (army, police, fire brigade, medical)is not appropriate
		The training on the procedure for defining array structure and chain of command isn't appropriate
		The training on the procedure for delivering goods to vesselsis not appropriate
		The training on the procedure for deploying ready squad / rapid intervention forceis not appropriate
		The training on the procedure for employing private security companies and defining missions and responsibilitiesis not appropriate
		The training on the procedure for handling suspects (pedestrians, vehicles and suspicious objects)is not appropriate
		The training on the procedure for inspecting mail and parcels, including by courieris not appropriate

		The training on the procedure for locating faults in security measures and equipment and further full functioning of the security system is not appropriate
		The training on the procedure for locating hazardous materials inside the facility isn't appropriate
		The training on the procedure for maritime patrol and observation forceis not appropriate
		The training on the procedure for protecting hazardous material storage areas isn't appropriate
		The training on the procedure for summoning / operating maritime patrolsis not appropriate
		The training on the procedures for communication between the security force in the facility and outside forces (vessels, national authorities, local authorities, outside security agencies)is not appropriate
		The training on the procedures for cooperation with the security officers of vessels for identifying embarking / disembarking personsis not appropriate
		The training on the procedures for ensuring continuous contact even during a fault or incapacitation of utility systems at the facilityis not appropriate
		The training on the procedures for evacuating the facility of workers in the case of a fire, earthquake, leak of hazardous materials, etcis not appropriate
		The training on the procedures for general personnel at the facilityis not appropriate
		The training on the procedures for guard mounting / changing of watchesis not appropriate
		The training on the procedures for handling crowd concentrationsis not appropriate
		The training on the procedures for hiring personnel for the security forceis not appropriate
		The training on the procedures for operating the control roomis not appropriate
		The training on the procedures for reporting security activity or possible compromises to securityis not appropriate
		The training on the procedures for securing sensitive security information stored on paper or electronic mediais not appropriate
		The training on The training on the procedures for handling dignitaries (including arrangement with visitor bodyguards)is not appropriate
		The training on The training on the procedures for inspecting and handling vessel cargois not appropriate
		The training on The training on the procedures for maintaining and updating hazardous goods and hazardous material recordsis not appropriate

		The training on The training on the procedures for screeners at gates and scannersis not appropriate
		The training on The training on the procedures for the all employees at the facility for receiving threat messages (anonymous / identified) by telephone, fax, letter, note at gate, etcis not appropriate
		The training on The training on the procedures for the security force for receiving threat messages (anonymous / identified) by telephone, fax, letter, note at gate, etcis not appropriate
		The training on visitor, subcontractor and maintenance and logistic, cleaning and other team entry procedures for the facilityis not appropriate
		The training on visitor, subcontractor and maintenance and logistic, cleaning and other team entry procedures for vesselsis not appropriate
		The visitor, subcontractor and maintenance and logistic, cleaning and other team entry procedures for the facility are not appropriate
		The visitor, subcontractor and maintenance and logistic, cleaning and other team entry procedures for the facility are not clear
		The visitor, subcontractor and maintenance and logistic, cleaning and other team entry procedures for vessels are not appropriate
		The visitor, subcontractor and maintenance and logistic, cleaning and other team entry procedures for vessels are not clear
		There are no additional procedures for cargo inspections when in Risk Level 2
		There are no additional procedures for cargo inspections when in Risk Level 3
		There are no additional procedures for crew inspections when in Risk Level 2
		There are no additional procedures for crew inspections when in Risk Level 3
		There are no additional procedures for passenger inspections when in Risk Level 2
		There are no additional procedures for passenger inspections when in Risk Level 3
		There are no additional procedures for personnel inspections when in Risk Level 2
		There are no additional procedures for personnel inspections when in Risk Level 3
		There are no additional procedures for ship supplies inspections when in Risk Level 2
		There are no additional procedures for ship supplies inspections when in Risk Level 3
		There are no additional procedures for vehicles inspections when in Risk Level 2
		There are no additional procedures for vehicles inspections when in Risk Level 3
		There are no assessment procedures

		There are no procedures for issuance of temporary badges for individuals who forgotten their permanent badges and those who have lost their badges
		There are no procedures in existence to ensure the return of identification badges upon termination of employment or assignment
		There are no routines for constraints of movements when Risk Level 3 is announced
		There is no additional personnel assigned in case elevation of Risk to Level 2
		There is no additional personnel assigned in case elevation of Risk to Level 3
		There is no additional personnel assigned in case of emergency
		There is no emergency response fallback plan (how the facility operates in cases of emergency)
		There is no risk profiling per event or threat scenario
		There procedures are not clear nor user-friendly
	Processes and organizational activities for the security handling of passengers failures (processes, procedures, personnel, equipment and means)	Hazardous materials are not completely covered in the inspection
		Incriminating findings are not forwarded to the ship's security officer
		Not all passengers undergo the same security process
		Only a small sample of outgoing passengers are inspected
		Team managers don't regularly perform audits on their workers
		The X-ray machines are not regularly calibrated
		The communications channels are not secure.
		The facility's management doesn't have a clear procedure for security handling of passengers and their luggage
		The members of the screening unit are not aware of the procedure instructions
		The outgoing passenger handling procedure regarding weapon identification is incomplete
		The outgoing passenger luggage is not or is partially inspected
		The outgoing passengers are not inspected or are inspected within the facility
		The passengeris not questioned during the inspection
		The procedure doesn't cover the detection of explosive devices
		The procedureis not complete (doesn't cover incriminating findings)
		The procedures are not regularly updated per the ISPS Code instructions
		The procedure's principles are not verified by a state agency
		The screening staff doesn't operate in accordance with the procedures
		The screening systems can be bypassed
		The screening team doesn't take part in wide-scale port exercises

		The security screener doesn't always perform a body search exercise after metal detector warnings
		The security screener doesn't handle the passenger's ticket and passport
		The security screener doesn't know how to identify suspicious signs in Behavior, Ticket and passport, Luggage or Passenger's body.
		The security screener doesn't receive concentrated training days
		The security screener doesn't receive relevant "intelligence" on passengers (e.g. State shipping suspect list, International terrorist list, List of countries defined as suspicious, etc)
		The security screener doesn't undergo a directed X-ray screening exercise regularly
		The security staff doesn't use the proper equipment for its chain of inspections (X-ray machine, Sniffer, Walkthrough metal detector, Hand-held metal detector, Manual frisking, Explosive detection dogs, Chemical detection kit, etc)
		The security staffis not properly trained for their job
		The security team doesn't analyze incidents and learn the respective lessons
		There are no clear guidelines for handling unaccompanied passenger luggage
		There are no special inspection cubicles for body searches
		There are passengers (Diplomats, Government officials, Seamen, VIPs, Disabled passengers, Infants, etc) that undergo less stringent screening
		There are not clear instructions for handling passengers when weapons are found
		There is no "suspicious passenger" clear definition in the procedure
		There is no attention to sweeps in the screening area
		There is no clear communication process for reporting findings to the relevant stakeholders
		There is no definition of security stakeholders
		There is no formal procedure for passengers to prove their identity by boarding passes and/or passports before being allowed in areas where search will take place.
		There is no policy for additional inspections that a suspicious passenger undergoes (eg inspection of objects using other technological tools, Thorough body search, denial of voyage to passenger, Transfer to security forces, etc)
		There is no policy for principles used for inspecting passengers (All passengers vs Sampling vsProfiling vs Questioning)
		There is no training for the procedure for passengers to prove their identity by boarding passes and/or passports before being allowed in areas where search will take place.

		There is partial inspection (either through Ticket inspection or Document inspection or Walkthrough metal detector or Hand-held metal detectors)
		Thereis not complete separation between screened and unscreened passengers
	Restricted areas inside the port facility failures	Security is not adequately provided at access points of restricted areas
		At Security Level 2 facilities there are inadequate measures to monitor access to restricted areas by CCTV with recording facilities
		For Security Level 1 facilities, measures don't include restriction on parking adjacent to Restricted Areas
		Personnel other than those whose duties require access to information or equipment are also allowed within restricted areas
		Persons whose duties do not require access are not required to remain under constant escort while in restricted areas
		Procedures for personnel dedicated to guard or patrol restricted areas are not properly implemented at Sec Level II
		Procedures for personnel dedicated to guard or patrol restricted areas are not properly implemented at Sec Level III
		Procedures to continuously guarded restricted areas at SEC Level III are poorly implemented or non-existent
		Procedures to limit access of restricted areas to other than security and essential personnel are poorly or not implemented at Sec Level II
		Procedures to limit access of restricted areas to other than security and essential personnel are poorly or not implemented at Sec Level III
		Restricted areas don't have a personnel identification and control processes
		Security personnel don't properly perform routine patrols of restricted areas
		The personnel is not trained to perform personnel identification and control
		The restricted areas don't have a clearly marked perimeter barrier
		The restricted areas don't have a personnel identification and control system with all entrances/exits guarded, controlled, or secured with alarms
	Sabotage	Lack of Physical Security
	Security failures	Has the security force structure been defined
		No constraints and stipulations have been defined in the concept
		The facility doesn't have a defined security concept
		The facility doesn't have a proper security concept
		The facility doesn't have a validated security concept

		The facilityis not properly geared to cope with the threat scenarios defined
		The goals defined in the concept are not clear
		The goals defined in the concept are not valid
		The primary and secondary objectives been defined in the concept are not clear
		The primary and secondary objectives been defined in the concept are not valid
		The priorities been defined in the concept are not clear
		The priorities been defined in the concept are not valid
		The threats and scenarios don't correspond with the current situation of the facility
		There is no clear distinction among, the authorities, the facility's management and the security officer
		Thereis not a security plan
		Thereis not any responsible party to define the main threats and scenarios
	Security handling of crewmen on vessels failures	Crews' passes are not properly confirmed with the ship
		Service engineers are not vetted and searched before being allowed on board ship
		Service engineers work orders are not confirmed with the ship before they are allowed on board
		The communications are done over untrusted networks
		The facility doesn't have a procedure for security handling of crewmen and their luggage
		The procedural principles haven't been validated by a state agency
		The procedure hasn't been updated after receiving ISPS code instructions
		The screening system can be bypassed
		The security team doesn't have proper equipment for inspecting crewmen
		The ship doesn't give notice of the crew and passenger list
		There are not any special cubicles for body searches at checkpoints
		There is no clear principle for inspecting crewmen (All crewmen are inspected vs Sample vs Profiling vs Questioning)
		There is no clear procedure for incoming crewmen inspections (Ticket inspections vs Document inspection vs Metal detector gate vs Wand search vs Questioning)
		There is no clear procedure for incoming crewmen's luggage inspections
		There is no clear procedure for outgoing crewmen inspections (Ticket inspections vs Document inspection vs Metal detector gate vs Wand search vs Questioning)
		There is no clear procedure for outgoing crewmen's luggage inspections
		There is no clear verification procedure
		There is no complete separation between screened and unscreened crewmen

		There is no pass issuance process for ship's crew when in port
		There is no procedure for incoming crewmen inspected
		There is no procedure for incoming crewmen inspections
		There is no procedure for outgoing crewmen inspections
		There is no procedure for outgoing crewmen to be inspected
		Thereis not any difference in the inspection of crewmen disembarking for shore leave and crewmen who are being replaced
		Thereis not different handling of visitors boarding ships (relatives, welfare workers, employee committees, etc.)
	Security handling of delivery of ship stores failures	Drivers entering the facility are not required to show identification and obtain gate passes to control and identify those authorized to deliver ship's stores
		Inspections of delivery vehicles are not performed prior to entry into the facility
		Ship's stores are not coordinated between PFSO and the vessel
		Ship's stores are not scheduled in advance of delivery
		Ship's stores are not screened using scanning/detection equipment, mechanical devices, or canines
		There are not any escorts provided for delivery vehicles within the facility
		There are not any restricted areas designated to perform inspections of ship's stores
		There are not procedures in place to prevent tampering with ship's stores
		There are not procedures in place to visually and/or physically inspect ship's stores
		There are not proper procedures in place to visually and/or physically inspect ship's stores
		Unscheduled deliveries of ship's stores are not prevented from being accepted
	Security handling of freight failures	Accesses to areas where documentation is processedis not limited solely to authorized personnel
		All commercial goods conveyed by sea are not given security coverage
		Bulk goods are not inspected
		Cargo documentationis not properly guarded to piece counts indicated/ avoid fraud
		Cargo is moved directly from railcars or vessels to storage facilities, and directly from storage facilities to railcars and vessels without proper security inspections in place
		Cargo is released to entities other than the carrier specified in the delivery order without release authorizing delivery to another carrier
		Cargo stored in open areas, and palletized or stacked cargo in warehouse facilities,is not properly stacked and placed within, away from, and parallel to non-perimeter fences and walls, to ensure unimpeded views for security personnel

		Databases are not secure
		Delivery and receiving operations are not segregated
		Delivery documents are not closely scrutinized
		Does the team have a machine for screening containers
		Electronic Data Interface (EDI) information and delivery orders for cargo and containers are not checked for accuracy and verified before acceptance
		Excess size consignments are not inspected
		Incidents of weapon smuggling using commercial goods are not properly forwarded to competent authorities
		Incriminating findings are forwarded to the facility's security officer over untrusted networks
		Incriminating findings are not properly forwarded to the facility's security officer
		Information sharing is done over untrusted networks
		Members of the screening unit don't know the procedure instructions
		Personnel processing delivery orders don't properly verify the identity of the trucker and trucking company before releasing the shipment
		Seal numbers on containers are not verified against documents, and seals are not checked for integrity before arrival, departure, or transfer
		Security personnel are not properly kept aware of the location of certain dangerous cargoes
		Security personnel don't take measures to implement a higher standard of security for sensitive / dangerous cargoes
		Shipments are not classified in accordance with the threat level
		Teams are not properly trained for explosives
		The facility doesn't have a written procedure for security handling of commercial freight
		The loading/unloading connections of pipelines, loading arms, or transfer hoses are not securely capped or blank-flanged when not in service or in standby service
		The master flow and drain valves, and other valves that would permit direct outward flow of a bulk liquid storage tanks contents to the surface are not securely locked in the closed position when in a non-operating or non-standby status
		The PF operator doesn't physically or electronically maintain, and continuously update, an accurate list of all cargoes, and a location chart, of all cargo/containers on the facility
		The procedures don't cover hazardous materials
		The procedures don't cover the detection of weapons

		The procedures don't cover the handling of explosive devices
		The procedures haven't been updated after receiving ISPS Code instructions
		The procedures' principles are not validated established by a state agency
		The screener teamis not properly trained for its job
		The screening grounds are not sterile
		The screening team doesn't work according to the procedures
		The security agreements are not manifested or properly documented
		The security handling of freight transferred at seais not different from that of freight transferred on the wharf
		The security screener team members are not physically drilled after the initial training
		The security team doesn't abide to reporting requirements.
		The security team doesn't have a technological inspection technique
		The security team doesn't know how to analyze the meaning of shipments from foreign countries / based on the risk profiling
		The security team doesn't use a computerized customer database
		The security teamis not capable / trained to analyze the meaning of "commercial paperwork"
		The security team make telephone inquiries on commercial shipments without proper identification / security procedures
		The starter controls on all bulk liquid transfer pumps are not locked in the "off" position, or located at a site accessible only to authorized personnel
		The team doesn't get explosive detection dogs for random shipment inspection or for suspicious shipment inspection
		The team doesn't have a technological sniffer
		The team doesn't have an organic compound detection machine
		The team doesn't have an X-ray machine
		The team managers don't conduct operational supervision of workers
		The workers don't participate in a wide-scale exercise
		There are no policies and/or measures in place to prevent the theft of cargo documentation
		There are no procedures in place to prevent tampering with cargo
		There are not any security agreements with customs agents
		There are not any security agreements with dispatchers
		There are not any security agreements with freight forwarders

		There are not any security agreements with logistics service providers
		There are not any security agreements with transport operators
		There are not clear procedures for the screening of vehicle and its cargo entering the facility
		There are not proper procedures in place for inventory control
		There are not proper procedures in place for the movement and storage of cargo
		There are not separate procedures and security measures in effect to protect arms, ammunition and dangerous cargos
		There are not separate procedures for hazardous material cargo
		There is no clear policy of what inspections are performed on freight (Inspection of documents, Checking of companies / dispatchers, External inspection of freight, Opening and inspection of content, Explosive detection dogs, Sniffer, X-ray, etc)
		There is no clear policy of where is the cargo inspected (on designated secure restricted areas for the inspection of cargo, on the quay / wharf, on the storage warehouses, at the manufacturing plant, elsewhere)
		There is no policy for drivers entering the facility to show identification and obtain gate passes to control and identify those authorized to pick up or deliver cargo
		There is no procedure for certain dangerous cargoes to be adequately described on the documentation, and the weights and piece counts as well as information sharing of the relevant stakeholders
		There is no screening policy (e.g. Full effective supervision, Partial supervision, No supervision)
		There is no separate procedure for incoming and outgoing freight
		Thereis not no definition and handling procedures for shipments coming from a country defined as suspicious
	Security handling of outgoing passengers' private vehicles failures	Explosive detection dogs are not used
		Incidents of weapon smuggling using vehicles are not properly forwarded to the relevant stakeholders
		It is possible for a vehicle to sail while its driver is left in the facility
		The security team hasn't been properly drilled in the smuggling of weapons using vehicles
		The team hasn't been trained to handle vehicles or other means of transport (motor boat), surfboards, motorcycles, etc
		The vehicle screening system can be bypassed
		There is no policy for outgoing vehicles to be inspected

		There is no procedure for private vehicles boarding ships inspected (Ticket inspection, Document inspection, Visual inspection of trunk / hold, Exterior inspection of vehicle, Metal-detector screening of driver and passengers, Sniffer, Explosive detection dogs, etc)
		There is no procedure to inspect if a vehicle contains (additional) luggage
		There is no procedure to match vehicles to their drivers
	Security, lifesaving and medical units inside the facility failures	The emergency procedures are not adequately shared by the security units in the facility and by outside security/safety agencies
		The port facility doesn't have a clinic inside it
		The port facility doesn't have a coast guard station inside it
		The port facility doesn't have a fire station inside it
		The port facility doesn't have a police station inside it
		The port facility doesn't have an environmental station inside it
		The port facility doesn't have proper emergency procedures
		The port facility emergency procedures shared by the security units and the support units at the facility
		The port facility equipment location doesn't enable proper evacuation, rescue and support activity in emergencies
		The port facility's security plans are not suitable for or adapted to the security plans of the other security agencies (Coast Guard, police, fire brigade, etc.)
		The support and rescue forces are not properly equipped (Means of transport (sea/land), lifeboats, Ambulances, Helicopters, Tugboats, Cranes, Suits for handling hazardous material leaks, Other as appropriate)
		There is no proper training or drills with the relevant Emergency Response Units
	Staff Risks	No staff
		Inadequate recruitment
		Inadequate safety training
		Incorrect use of software and hardware
		Insufficient awareness of security risks
		Lack of media use policy
		Lack of monitoring mechanisms
		Unsupervised work of external staff
	Storage areas near the quay failures	Faults and problems in the warehouses affect other sensitive areas
		The warehouses near the quay are not adequately guarded

		The warehouses near the quay are not adequately monitored
		The warehouses near the quay are not adequately secured/guarded
		There are not adequate alarm and alert devices in the warehouses
		There are not clear procedures for guarding the warehouses / storage areas
		Thereis not proper access control to the storage areas
	Storing freight and goods areas failures	The area is dominated by other points outside the facility
		The area is ineffectively guarded
		The areais not properly defined and marked
		The physical measures for restricting access to the area are inefficient
		The site can't be easily identified
		There are ineffective procedures that cover the approach to the area
		There are no detection and tracking devices in the area
		There is an inadequate process of access control to the area
		There is inadequate control over the entry and exit of freight to and from the area
		There is no backup communication channel
		There is no backup electricity
		There is no efficient process of approach control to the area
		There is no emergency response process
		There is no suspicious movements detection process
	Storm	Back-up files and systems not available
		Location is in an area susceptible to natural disasters
		No business continuity plans or procedures for recovery of information and information assets
	Strike	Backup files and systems not available
		Inadequate Physical Security
	Systems, equipment and measures failures	All security force vehicles are not equipped with a spotlight
		Duties other than those related to security are also performed by security personnel
		Guard assignments, times and patrol routes do not vary at frequent intervals tom avoid establishing routines
		Guards go home with their firearms at the end of their shifts
		Security force personnel, who are required to carry firearms, do not receive proper training
		Security force vehicles are not equipped with signs conspicuously identifying vehicle as a security police vehicle, emergency exterior overhead lights, and an electronic siren

		Security personnelis not required to wear uniforms that are complete, distinct, and authoritative
		The allowance to carry firearms or other security meansis not clear
		The equipmentis not appropriate for its missions
		The equipmentis not properly positioned
		The equipment roster doesn't meet the operational needs
		The facility doesn't have communication measures
		The facility doesn't have day and night observation measures – binoculars, infrared equipment, image intensifiers and thermal viewers
		The facility doesn't have dedicated equipment for coping with unconventional events
		The facility doesn't have dedicated equipment for unique forces and units (such as bomb disposal units, etc.)
		The facility doesn't have non-lethal weaponry (tear gas, shockers, anti-riot equipment, etc.)
		The facility doesn't secure communication measures
		The facility's non-lethal weaponry is outdated or near end of life
		The firearm storage room at the facilityis not secure
		The patrol launches are not equipped with GPS systems
		The patrol vehicles are not equipped with GPS systems
		The security force doesn't have sufficient, adequately equipped vehicles to maintain patrols, respond to alarms and emergencies and maintain supervision
		The security forceis not equipped with individual and unit level protective measures (from individual vests, protective vehicles, to explosion containment kits).
		There are no lighting measures on watchtowers
		There are no lighting measures for guards
		There are no lighting measures on patrol launches
		There are no lighting measures on vehicles
		There is no equipment roster for the security force per guard
		There is no equipment roster for the security force per guard post
		There is no equipment roster for the security force per maritime patrol
		There is no equipment roster for the security force per mobile patrol
		There is no equipment roster for the security force per unit level equipment
		Thereis not any firearm storage room at the facility
	Technical Failure	Perimeter fails

		Aging storage media
		Dusty equipement
		Interruption or failure of water supply
		Lack of back-up facilities or processes
		Maintenance Error
		Operational capacity overload
		Wear and Tear of equipment
	Territorial waters & sea approach routes to the port failures	Entering in the port access laneis not authorized
		Entering in the port access laneis not reported
		The areas dominating the lanes don't have good accessibility and concealment
		The blocking of the port access lane prevents the port facilities' further functioning
		The facility itself is used as a navigation lane for another port without proper policies and procedures
		The lane doesn't have predefined pilot obligations for navigational purposes
		The lane doesn't have predefined vessel characteristics (passenger, freight, fishing, etc.)
		The lane doesn't have predefined vessel size acceptance policies
		The maritime patrol activity near the port doesn't provide a sufficient answer to security of the lanes
		The maritime patrols are not equipped with equipment suitable for coping with different security and safety situations and scenarios
		The navigation lane pass near utility facilities that are essential to the country (electricity, energy stores, defense bases, quarries, etc.) and no proper policies are defined
		The navigation lane passes near other port facilities and no proper policies are defined
		The navigation lane to the facility passes near the territory of a foreign country and no proper policies are defined
		The port access lane doesn't enable emergency docking
		The port doesn't have set access lanes
		The sea patrols are not performed at the same frequency on weekends and holidays as on working days
		The security forces at the port don't have an involvement policy for managing these systems
		The security forces at the port don't report unusual incidents arising in these systems
		The traffic to the port is through multiple lanes or unrecognized lanes
		There are areas that dominate the lanes

		There been cases of smuggling on or near the route and no proper security measures are defined or implemented
		There have been cases of piracy (taking of goods from a ship while it is sailing/docked) on or near the lane and no proper security measures are defined or implemented
		There have been other criminal acts and no proper security measures are defined or implemented
		There is no a system for commanding and controlling the territorial waters of the port
		There is no agency (Coast Guard, Navy, Local police, Facility security staff, Private agency, other) that guides the sea patrols in the facility area
		There is no agency (Coast Guard, Navy, Local police, Facility security staff, Private agency, other) that is in charge of conducting sea patrols
		There is no procedure at the port for checking the possibility that a vessel in the lane is under terrorist threat
		There is no regular Coast Guard activity in the access lanes
		There is no shipping lane command and control system
		There is no vessel identification system
	Terrorist attacks	Backup files and systems not available
		Falsification of Identity
		Improper or inappropriate maintenance of technical facilities
		Inadequate audit logs to detect unauthorized access of the premises
		Inadequate backup policy
		Inadequate data backup procedure for both software and data
		Inadequate maintenance of the records regarding the repairs and modifications of the organization facilities physical components
		Inadequate monitoring of the organization premises
		Inadequate Physical and Environmental Security Policy and Procedures
		Inadequate Physical Security
		Inadequate Recovery Procedure
		Industrial espionage
		Lack of a formal entitlement review process regarding the access rights of the employees in the organization's premises
		Lack of a uniform physical security policy enforcement
		Lack of a uniform policy and procedure for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media enforcement

		Lack of back-up facilities or processes
		Lack of environmental protection
		Lack of Logical Access security
		No concrete assignment of Continuity/Disaster-related roles and responsibilities
		No formal or informal disaster/recovery plans
		Telecommunications interception
		unsafe protection against bombing, molotov cocktails
		Use of weapons
		No Business Continuity Plans for recovery of information and information assets
	Theft and Fraud	Inadequate audit logs to detect unauthorized access of the premises
		Inadequate change management procedure for infrastructure components
		Inadequate maintenance of the records regarding the repairs and modifications of the organization facilities physical components
		Inadequate monitoring of the organization premises
		Inadequate Physical and Environmental Security Policy and Procedures
		Inadequate Physical Security
		Insufficient security training
		Lack of a comprehensive security awareness and training program
		Lack of a formal entitlement review process regarding the access rights of the employees in the organization's premises
		Lack of a uniform policy and procedure for controlling physical access to work areas and hardware (computers, communication devices, etc.) and software media enforcement
		Lack of Logical Access security
		Lack of Physical Security
		No concrete assignment of security roles and responsibilities
		No documented and tested security plans for safeguarding the systems and networks
		No documented policies and procedures for physical control of hardware and software
	Tidal Surge/Wave	Back-up files and systems not available
		Location is in an area susceptible to natural disasters
		No business continuity plans or procedures for recovery of information and information assets
	Training, control and supervision failures	Corrections recommended in lesson learning processes are not tracked
		The exercises don't encompass all fields of security

		The exercises don't test all security levels and echelons
		The facility's security manager doesn't use exercises for testing workers and the method of work
		The quality of materials, lesson sets and examinations are not relevant nor current
		The security manager doesn't have a regular exercise plan
		There are no regular audits of the security force
		There are no security reviews at the facility
		There is no lessons learned process in the facility
		There is no periodical shooting training held
		There is no physical, unarmed combat and combat training for security personnel
		There is no process of adapting procedures and guidelines to lessons that have been learned
		There is no regular instruction for security staff for updating and refreshing purposes (security plan, procedures, guidelines, etc.)
		There is no structured process of disseminating lessons to workers
		There is no training on body searching
		There is no training on cargo inspection
		There is no training on handling of weapons
		There is no training on locating of weapons (standard / improvised)
		There is no training on luggage inspection
		There is no training on questioning
		There is no training on sweeps for locating suspicious objects
		There is no training on vehicle inspection
		There is no training on weapon identification
		There is no training unit for the security force at the facility
	Transmission errors	Back-up files and systems not available
		Lack Careful planning and laying of cables
		Lack of cryptographic means to protect integrity of data
		Lack of properly operation of network equipment
		No business continuity plans or procedures for recovery of information and information assets
	Unauthorised Data Access	Lack of a Firewall
		Lack of Physical Security
	Unauthorised Dial-in Access	Lack of a Firewall

	Unauthorised Software Changes	Back-up files and systems not available
	Unloading and loading vessels areas failures	The area is dominated by other points outside the facility
		The area is ineffectively guarded
		The areais not properly defined and marked
		The physical measures for restricting access to the area are inefficient
		The site can't be easily identified
		There are ineffective procedures that cover the approach to the area
		There are no detection and tracking devices in the area
		There is an inadequate process of access control to the area
		There is inadequate control over the entry and exit of freight to and from the area
		There is no backup communication channel
		There is no backup electricity
		There is no efficient process of approach control to the area
		There is no emergency response process
		There is no suspicious movements detection process
	Vermin (Adware, Malware, Phishing, Pop-Ups, Spyware, Viruses, Trojans, and Worms)	Back-up files and systems not available
		No business continuity plans or procedures for recovery of information and information assets
	Vessel embarkation and disembarkation areas failures	Access points are not entirely secured or monitored
		Embarkation areas are not monitored or controlled
		No physical security measures are in place to prevent unauthorized personnel gaining access to the ship whilst at berth
		The area is dominated by other points outside the facility
		The area is not defined nor marked
		The area is not properly guarded
		The gangways and ropes are not manned with security personnel at all times when the ship is berthed
		The gangways are not always locked and barred at night
		The restricted areas don't have adequate physical barriers
		The ship's lighting systems degrade the existing security lighting
		The ship's lighting systems are not properly used to supplement the port lighting at night
		The site can't be easily identified
		There are no processes of access control to the area

		There are inadequate detection and tracking devices in the area
		There are no physical measures for restricting access to the area
		There are no processes of approach control to the area
		There are unclear procedures that cover the approach to the area
		There is limited or no control over the entry and exit of freight to and from the area
	Vessel Incidents	Awareness of vessel traffic per cargo type (maps, schedules, notices)
		Awareness of vessel traffic per terminal facility (maps, schedules, notices)
		Awareness of vessel traffic per vessel type(maps, schedules, notices)
	Vessel traffic management system (VTMS) failures	Access control system in the VTMS control room is not effective
		Automatic fire extinguishing systems in the VTMS control room are not effective
		Break-in detection system in the VTMS control room is not effective
		Effective room locking in the VTMS control room is not adequate
		Fire detection systems in the VTMS control room are not effective
		Power supply backup system in the VTMS control room is not effective
		Standalone air conditioning system in the VTMS control room is not effective
		The CCTV cameras are not reasonably protected from malicious damage
		The computer system doesn't have a disaster recovery mechanism
		The computer system doesn't have electronic hacking detection software
		The computer system doesn't have electronic hacking prevention software (Firewall)
		The equipment used by the VTMS is not appropriate
		The radar system doesn't cover the entire facilities' entrance areas
		The radar systems don't have adequate access denial fence
		The radar systems don't have adequate break-in detection system
		The radar systems don't have adequate cctv security
		The radar systems don't have adequate communication backup systems
		The radar systems don't have adequate physical security
		The radar systems don't have adequate power supply backup systems
		The radio and communication transmissions are not regularly recorded
		The response the CCTV array givesis not adequate
		The safeguards in the VTMS control room are not effective
		The security responsibilities are not properly assigned
		The system doesn't provide a response to all vessel types and has identified restrictions
		The VTMS control room doesn't operate 24x7

		The VTMS control roomis not located in a separate secure installation
		The VTMS control roomis not observed by ground based guards outside the facility
		The VTMS doesn't use remote radar stations
		There are dead spots that the system does not cover
		There are no effective or adequate emergency procedures
		There are no written guidelines about cases and responses for the VTMS
		There are no written procedures covering regular activity at the gates
		There is no adequate backup to the communication channels between the radar stations and the control room
		There is no procedure for reporting a vessel under terrorist threat in the facility
		There is no procedure for reporting the change of an alert status in the port to the port facilities
		There is no training for the procedures for reporting the change of an alert status in the port to the port facilities
		There is no training no procedures covering regular activity at the gates
		There is no training on emergency procedures
		There is no training on the guidelines about cases and responses for the VTMS
		There is no training on the procedures for reporting a vessel under terrorist threat in the facility
		Voice communication systems are ineffectively connected to the competent agencies
		VTMS computers that are connected to outside systems are not properly identified
		VTMS control computer systems are not properly protected against viruses
	Watchtowers Failures	Observation devices are not placed in the towers
		Searchlights are not placed in the watchtowers
		The activities in the positions are not covered by procedures
		The activities procedures are not clearly explained to the personnel
		The existing towers don't cover the terrain with an effective and sufficient line of sight
		The existing watchtowers haven't been correctly located in accordance with the terrain and surroundings
		The guards at the watchtower don't direct other forces from their position during an incident
		The guards don't have the means to quickly contact the control room or another force in the facility during an incident
		The guards in the tower are exposed to threats from outside the facility

		The number of watchtowers the facility has are limited
		The towers don't enable convenient and effective observation so that the guards stationed on them can effectively fulfill their assignments
		There are not any watchtowers along the perimeter fence/wall
		There are not enough watchtowers deployed along the perimeter fence
		Towers are not manned
		Towers are not manned both day and night
		Towers are not manned to the same extent during weekends, holidays, etc
	Waters near the facility failures	Suspicious vessels are not effectively monitored or stopped in the area of the water near the facility
		The breakwater serves as a commercial area without proper safety measures
		The breakwater serves as a tourist area without proper safety measures
		The CCTV is based on WiFi networks without the proper security features
		The communications to the utilities facilities are not secure
		The facility doesn't have stern docking at the breakwater
		The facility services are located nearby (tugboats, pilots, oilers, waste disposal) but not monitored
		The nearby waters are not viewable by CCTV system
		The port doesn't have an independent system for vessel management and maneuvering assistance
		The tourist boats are located nearby (cruising in the area of the facility only) but not monitored
		The utility facilities in the waters near the facility are not monitored
		The waters near the facility have an unrecognized / uncategorized diving area
		There are facilities for loading and unloading fuel, gas or other substances in the waters near the facility
		There are fish hatcheries in the waters near the facility
		There are fishing areas in the waters near the facility without proper monitoring
		There are hazardous material facilities in the waters near the facility
		There are places for fishing on the breakwater without proper safety measures
		There are places in the water near the facility that are radar dead zones
		There are tropical islands/vessels in the waters near the facility that are not properly monitored
		There is a Coast Guard base near the facility

		There is a marina in the waters near the facility
		There is a naval base near the facility
		There is holiday and sailing area in the waters near the facility without proper monitoring
		There is no safe access for communications to the ships to/from the port facility
		There is no security entries / exits in the facility
		What is the (closest) ships' docking distance from the breakwater
	Web Site Intrusion	Incorrectly configured or maintained security safeguards

Software	Abuse of rights	Disposal or reuse of storage media without proper erasure
		Lack of audit trail
		No 'logout' when leaving the workstation
		No or insufficient software testing
		Well-known flaws in the software
		Wrong allocation of access rights
	Contamination	Back-up files and systems not available
		Lack of maintenance of equipment and facilities
		Location is in an area susceptible to environmental conditions such as contamination, electronic interference extreme temperature and humidity vermin
	Cyber-Vermin	Back-up files and systems not available
	Data Corruption	Applying application programs to the wrong data in terms of time
		Incorrect dates
		Incorrect parameter set up
		Lack of identification and authentication mechanisms like user authentication
		Poor password management
		Unnecessary services enabled
		Unprotected password tables
		Widely-distributed software
	Denial of Service	Incorrectly configured or maintained
		Inefficient configuration of Anti Virus software
		Lack of a Firewall
		Lack of regular update of Anti virus software
		No Anti-Virus software

	Earthquake	Back-up files and systems not available
	Electronic Interference	Back-up files and systems not available
		Inadequate monitoring of environmental conditions
		Inadequate Physical and Environmental Security Policy and Procedures
		Inadequate Recovery Procedure
		Lack of a uniform physical security policy enforcement
		Lack of environmental protection
		Location is in an area susceptible to environmental conditions such as contamination, electronic interference extreme temperature and humidity vermin
	Equipment Failure	Inadequate change control settings
		Incomplete / incorrect maintenance
		Non periodic replacement
		Susceptibility to electromagnetic radiation
		Susceptibility to moisture, dust, dirt
		Susceptibility to temperature fluctuations
		Susceptibility to voltage fluctuations
	Extremes of Temperature and Humidity	Back-up files and systems not available
		Improper or inappropriate maintenance of technical facilities
		Inadequate backup policy
		Inadequate change management procedure for infrastructure components
		Inadequate data backup procedure for both software and data
		Lack of back-up facilities or processes
		Location is in an area susceptible to environmental\ conditions such as extreme temperature and humidity
		No concrete assignment of Continuity/Disaster-related roles and responsibilities
		No formal or informal disaster/recovery plans
	Failure of outsourced operations	Back-up files and systems not available
		Unclear obligations in outsourcing agreements
	Fire	Backup files and systems not available
		Back-up files and systems not available
		Improper or inappropriate maintenance of technical facilities
		Inadequate backup policy
		Inadequate change management procedure for infrastructure components
		Inadequate monitoring of environmental conditions

		Inadequate Physical and Environmental Security Policy and Procedures
		Inadequate Recovery Procedure
		Lack of a uniform physical security policy enforcement
		Lack of automatic fire suppression system
		Lack of back-up facilities or processes
		Lack of environmental protection
		Lack of fire detection devices
		No concrete assignment of Continuity/Disaster-related roles and responsibilities
		No formal or informal disaster/recovery plans
		No Business Continuity Plans for recovery of information and information assets
	Flood	Back-up files and systems not available
		Inadequate data backup procedure for both software and data
		Location is in an area susceptible to natural disasters
	Malicious Code	Inadequate education of staff on Software viruses
		Inadequate information security policy
		Lack of checks for unauthorised software
		Lack of control of instant messaging
		Lack of policy for opening email attachments
		Lack of policy on using portable storage devices and media before scanning by Anti virus software
		Lack of regular update of Anti virus software
		Legacy systems
		No Anti Virus software
	Malicious destruction of data	Inadequate investment in appropriate security controls
		Incorrectly configured or maintained operating system
		Incorrectly configured or maintained security safeguards
		Lack of a Firewall
		Lack of checks for unauthorised software
		Lack of communication between HR and IT groups in respect of terminated employees leading to such employees still having access to system
		Lack of intrusion detection software
	Malpractice	Unauthorized use of equipment
	Network Intrusion	Inadequate Firewall Policies
		Inadequate network Development standards

		Inadequate Software Development standards
		Incorrectly configured or maintained operating system
		Incorrectly configured or maintained security safeguards
		Lack of a Firewall
		Lack of intrusion detection software
		Lack of update of Operating System security patches
	Operational Staff or User Errors	Complicated user interface
		Inadequate documentation
		Lack of a comprehensive security awareness and training program
		Lack of means to assess the employee awareness level
		Lack of user awareness
		Incorrect parameter set up
		Incorrect dates
		Unskilled staff
	Personnel Incidents	Absence of personnel
		Inadequate recruitment procedures
		Incorrect use of software and hardware
		Insufficient security training
		Lack of monitoring mechanisms
		Lack of policies for the correct use of telecommunications media and messaging
		Lack of security awareness
		Unsupervised work by outside or cleaning staff
	Power Fluctuations	Back-up files and systems not available
		Improper or inappropriate maintenance of technical facilities
		Inadequate change management procedure for infrastructure components
		Inadequate monitoring of environmental conditions
		Inadequate Physical and Environmental Security Policy and Procedures
		Lack of a uniform physical security policy enforcement
		Lack of environmental protection
		Location is in an area susceptible to power fluctuations
		No power conditioning equipment
		No Uninterruptible Power Supply equipment
	Procedural Failures	Uncontrolled copy of data

		Uncontrolled copy of software
	Reduced budgets	Inadequate investment in appropriate security controls
	Sabotage	Incorrect Access rights
		Lack of Configuration Management controls
		Lack of Logical Access security
		Lack of Physical Security
	Social Engineering	Lack of awareness of the social engineering threat
		Lack of policy requiring enquires for information to be withheld until the identity of the requestor can be verified
		Lack of policy restricting the provision of information by staff over the phone
	Software Failure	Disposal or reuse of storage media without complete remission
		Improper rights of use allocation
		Incomplete control software
		Known software errors
		Lack file and change control
		Lack of backup files
		Lack of documentation
		Lack of file processes
		Lack of mechanisms for user identification
		Mishandling passwords
		Non-locking the computer when the removal of the user
		Unclear or incomplete specifications for developers
		Uncontrolled installation and use software
		Unencrypted Passwords
		Unfriendly user interface
		Failure to produce management reports
		Immature or new software
		Lack of back-up copies
		Lack of effective change control
		Lack of physical protection of the building, doors and windows
		Unclear or incomplete specifications for developers
		Uncontrolled downloading and use of software
	Software or Programming Errors	Inadequate Engineering Code Security Guidelines for Developing Web Based Applications
		Inadequate reporting and handling of software – malfunctions

		Inadequate security testing of the applications
		Inadequate Segregation of Duties between software developers and operations staff
		Inadequate Software Development standards
		Inadequate supervision of programming staff
		Inadequate system development life cycle procedures
		Lack of efficient and effective configuration change control
		Lack of software auditing
		No check for security flaws, covert channels and back doors as part of the applied software change control procedures
		Unclear or incomplete specifications
		Unskilled staff
	Storm	Back-up files and systems not available
		Location is in an area susceptible to natural disasters
	Technical failures	Lack of user awareness
	Terrorist attacks	Industrial espionage
	Theft and Fraud	Incorrectly configured or maintained operating system
		Incorrectly configured or maintained security safeguards
		Insufficient security training
		Lack of a comprehensive security awareness and training program
		Lack of a Firewall
		Lack of checks for unauthorised software
		No concrete assignment of security roles and responsibilities
		Uncontrolled copy of data
		Uncontrolled copy of software
		Uncontrolled copying of data and or software
	Tidal Surge/Wave	Back-up files and systems not available
		Location is in an area susceptible to natural disasters
	Transmission errors	Back-up files and systems not available
		Improper or inappropriate cabling
		Inadequate incident handling
	Unauthorised Access	Dial-in banner leading to information which can expose the organisation to unauthorised dial in access
		Lack of an inventory of dial-up lines leading to inability to monitor dial up access
		Lack of audit logs to detect unauthorised access
		Lack of dial back authentication

		Lack of firewall
		Lack of intrusion detection software
		Lack of physical security over telecommunications equipment cabinets
		Lack of policies in respect of dial up access, modem use, and software use
		Lack of time restrictions on user access
		Lack of user authentication
	Unauthorised Data Access	Inability to authenticate requests for information
		Inadequate Firewall Policies
		Inadequate identity and password policy
		Inadequate investment in appropriate security controls
		Inadequate operating policies for handling, processing or storing sensitive information
		Inadequate review of the users access rights
		Incorrect Access rights
		Incorrectly configured or maintained application security features
		Incorrectly configured or maintained operating system
		Incorrectly configured or maintained security safeguards
		Lack of a Firewall
		Lack of identification and authentication Mechanisms
		Lack of intrusion detection software
		Lack of physical security over data communications cabinets
		No formal policy for the establishment and termination of the access right to information assets
		Portable devices storing unencrypted data and information
		Transmission of unencrypted sensitive data or information
		Unprotected password tables
		Unsecured wireless ports
	Unauthorised Software Changes	Back-up files and systems not available
		Easily accessible SCADA devices
		Inadequate engineering and quality processes for design and code review
		Inadequate reporting and handling of software malfunctions
		Inadequate Segregation of Duties between software developers and operations staff
		Inadequate supervision of programming staff
		Incorrectly configured or maintained operating system
		Incorrectly configured or maintained security safeguards

		Lack of a Firewall
		Lack of backups
		Lack of Configuration Management Software to enforce Configuration Management
		Lack of intrusion detection software
		Lack of Software Configuration Lack of Software Configuration
		Lack of Software Configuration Management policies and procedures
		Management policies and procedures
	Use of Pirated Software	Inadequate control of software distribution
		Lack of policies in respect of software use
		Lack of policy restricting staff to use of licensed software
		Lack of software auditing
		Uncontrolled copying of data and/or software
		Unrestricted copying of software
	Web Site Intrusion	Inadequate Firewall Policies
		Inadequate Software Development standards
		Incorrectly configured or maintained operating system
		Incorrectly configured or maintained security safeguards
		Lack of a Firewall
		Lack of intrusion detection software
		Lack of update of Operating System security patches

Hardware	Breach of information system maintainability	Insufficient maintenance/faulty installation of storage media
	Destruction of equipment or media	Lack of periodic replacement schemes
	Loss of power supply	Susceptibility to voltage variations
	Theft of media or documents	Lack of care at disposal
	Theft of media or documents	Uncontrolled copying
	Interception of compromising interference signals	Lack of care at disposal
	Retrieval of recycled or discarded media	Lack of care at disposal

Site organization	Abuse of rights	Lack of formal procedure for user registration and de-registration

		Lack of formal process for access right review (supervision)
		Lack or insufficient provisions (concerning security) in contracts with customers and/or third parties
		Lack of procedure of monitoring of information processing facilities
		Lack of regular audits (supervision)
		Lack of procedures of risk identification and assessment
		Lack of fault reports recorded in administrator and operator logs
	Breach of information system maintainability	Inadequate service maintenance response
		Lack or insufficient Service Level Agreement
		Lack of change control procedure
	Corruption of data	Lack of formal procedure for ISMS documentation control
		Lack of formal procedure for ISMS record supervision
	Data from untrustworthy sources	Lack of formal process for authorization of public available information
	Denial of actions	Lack of proper allocation of information security responsibilities
	Destruction of equipment or media	Inadequate or careless use of physical access control to buildings and rooms
	Equipment failure	Lack of continuity plans
	Error in use	Lack of e-mail usage policy
		Lack of procedures for introducing software into operational systems
		Lack of records in administrator and operator logs
		Lack of procedures for classified information handling
		Lack of information security responsibilities in job descriptions
	Illegal processing of data	Lack or insufficient provisions (concerning information security) in contracts with employees
	Loss of power supply	Unstable power grid
	Theft of equipment	Lack of physical protection of the building, doors and windows
		Lack of defined disciplinary process in case of information security incident
		Lack of formal policy on mobile computer usage
		Lack of control of off-premise assets
	Theft of media or documents	Lack or insufficient 'clear desk and clear screen' policy
		Lack of information processing facilities authorization
		Lack of established monitoring mechanisms for security breaches
	Unauthorized use of equipment	Lack of regular management reviews

List of countermeasures

TYPE OF COUNTERMEASURE	GENERAL MEASURE	DETAILED MEASURE
GENERIC	Port Facility Security Plan (PFSP) in force	
	Designation of a Port Facility Security Officer (PFSO)	
	PFSP adapted to PF particularities: Procedures	Security procedures for general personnel at the facility.
		Procedures for hiring personnel for the security force.
		Standards for assessing the performance of the security staff at the facility
		Standards for assessing the performance of all workers at the facility
		Site opening and closing procedures.
		Entry and access control procedures
		Visitor, subcontractor and maintenance and logistic, cleaning and other team entry procedures for the facility.
		Visitor, subcontractor and maintenance and logistic, cleaning and other team entry procedures for vessels.
		Procedure for handling disembarking seamen and their families.
		Procedures for handling dignitaries (including arrangement with visitor bodyguards).
		Procedures for inspecting and handling vessel cargo.
		Procedure for delivering goods to vessels
		Procedure for inspecting mail and parcels, including by courier.
		Procedures for maintaining and updating hazardous goods and hazardous material records.
		Procedure for locating hazardous materials inside the facility.
		Procedure for protecting hazardous material storage areas.
		Procedures for the security force for receiving threat messages (anonymous / identified) by telephone, fax, letter, note at gate, etc.
		Procedures for the all employees at the facility for receiving threat messages (anonymous / identified) by telephone, fax, letter, note at gate, etc.

		Procedure for defining array structure and chain of command.
		Procedure for maritime patrol and observation force.
		Security man and guard force procedures.
		Procedures for screeners at gates and scanners.
		Procedures for guard mounting / changing of watches.
		Procedures for operating the control room.
		Procedure for handling suspects. (pedestrians, vehicles and suspicious objects)
		Procedure for deploying ready squad / rapid intervention force.
		Procedures for handling crowd concentrations
		Procedure for employing private security companies and defining missions and responsibilities.
		Rules of engagement and opening fire.
		Procedures for communication between security forces inside the facility.
		Procedures for communication between the security force in the facility and outside forces. (vessels, national authorities, local authorities, outside security agencies).
		Procedures for cooperation with the security officers of vessels for identifying embarking / disembarking persons.
		Procedures for ensuring continuous contact even during a fault or incapacitation of utility systems at the facility.
		Procedures for reporting security activity or possible compromises to security.
		Procedures for securing sensitive security information stored on paper or electronic media.
		Procedure for locating faults in security measures and equipment and further full functioning of the security system.
		Coordination procedures for receiving assistance from outside agencies (army, police, fire brigade, medical).
		Procedures for evacuating the facility of workers in the case of a fire, earthquake, leak of hazardous materials, etc.
		Emergency procedures
		SCADA Procedures
		Hostage situation handling procedures.

		Procedure for summoning / operating maritime patrols
		Procedures for inspecting the structural integrity of the buildings
		procedures to search waterfront areas for explosives or other dangerous devices prior to a ship arrival at PF or waterfronts that have been unmanned or unmonitored
		Procedures that cover the approach to the area
		data backup procedures
		disaster recovery procedure
		procedure for reporting the change of an alert status in the port to the port facilities
		Perocedures for docking and mooring
		Procedures for inventory control
		Procedures to visually and/or physically inspect ship's stores
		Procedures to prevent tampering with ship's stores
	Security assessment with a sufficiently wide casuistry	
	Inclusion in the PFSP of a scheme of the facilities indicating sensitive points (points of access, work areas, storage areas, etc., to make easier the control of the PF and the implementation of corrective measures).	
	Establish links to the security organization with the relevant authorities and the forces of state security.	State shipping suspect list
		International terrorist list
		List of countries defined as suspicious
	Inclusion of threat assessments that are made from government bodies.	
	PFSP audits	
	Procedures for promptly pass a certain level of protection to the next higher (or lower)	
	Maintain a register of incidents and security threats	
	Incorporation of interim measures of protection through to implementation of definitive ones	
	Control of possession and use of firearms in general, and particularly in places with storage of dangerous goods.	
	Duplication of networks, services and supplies.	

	Access control	
	Inspections of cargo, passenger and luggage supplies	
	Inspections of water network	Water quality tests conducted at the facility (every 3 months)
		Water supply control system
		The water system is connected to a backup for continued functioning, such as a generator
	Defence of necessary equipment for the operation of the PF	
	Protection of vehicles (ships and wheeled) to prevent them could be used for illegal purposes	
	Defence against sabotage whether from inside or outside	
	Annotation and correction of deficiencies in the various corrective measures as may be of procedural or materials nature	
	Protection of communication systems network	Secure terrestrial wireless communications systems
		Secure terrestrial wired communications systems
		Secure terrestrial satellite communications systems
	Lighting	Flood lighting system
		Regular lighting system
		Lighting system has a good combination of flood lighting and regular lighting
		Lighting system is deployed along the perimeter
		Emergency backup power source for the lighting system
		The existing lighting is suitable for the camera type
		Illumination of the perimeter area
		Illumination of most of the perimeter area
		Strong lighting on the fence near sensitive areas
		Effective lighting system inside the facility
		Illumination of restricted areas
		Illumination of vehicle entrances
		Illumination of pedestrian entrances
		Illumination of docks, piers, wharfs and other working areas in a manner not to interfere with navigation
		Illumination of water approaches to dock, pier, or wharfs
		Illumination of parking lots

		Illumination of parking lots in a manner to prevent shadows and areas of poor illumination between vehicles
		Illumination of perimeter so that security force patrol personnel remain in comparative darkness
		Standby or emergency protective lighting
		The lighting is aimed inward or outward
		Activation of lighting throughout the hours of darkness (sunset to sunrise) and periods of low visibility
		All areas with a lighting system are illuminated throughout the hours of darkness (sunset to sunrise) and periods of low visibility
	Maintenance Plan	
	Training, control and supervision	Training and drilling program
		Training on handling of weapons
		Training on questioning
		Training on body searching
		Training on luggage inspection
		Training on vehicle inspection
		Training on cargo inspection
		Training on sweeps for locating suspicious objects
		Training on lifesaving and medical treatment
		Training program to respond to all types of emergency at the vessel/shore/sea interface (fire, explosion, near drowning, ship hitting a dock, another ship, earthquake, etc.)
		Analysis of the incidents and learn lessons
	Port Police (annual drills)	
	Biweekly drills for avoid mechanical failures	
	Traditional detection systems	Trained dogs
		Manual frisking

Dissuasive and delay measures. Physical protection systems	Fence/wall	Fence not scalable
		A regular mesh wire fence
		A welded mesh wire fence
		A palisade fence

		A masonry/brick fence
		The fence is at least 2,5 meters high
		The fence/wall surrounds the entire facility
		The fence/wall surround most of the facility
		The height of the fence/wall is uniform along its entire length
		Segments of fence are less than 2,5 meters high
		The fence is anchored to the ground
		There is a concrete belt at the bottom of the fence
		The fence/wall has an upper slope
		The top of the fence/wall has a barbed wire coil
		The fence/wall is vaulted over controls
		All perimeter fences and walls have an unobstructed zone of at least 5 meters on each side
		There are drainage ditches or water conduits along the fence/wall
		The perimeter and the clear zone are inspected regularly (at least every 3 months) and their condition assessed (wear and tear, erosion etc)
		Records of the fence/wall's inspections are maintained (at least one year) and are easily accessible
		The fence /wall's distance from sensitive areas enables an adequate response time by the security forces
		There is a delaying fence before the fence/wall
		There are other obstacles (natural or artificial) before the fence/wall
		Port boundaries are marked
	Ribbon cutting obstacles	
	Barriers, lifting barriers, tourniquet, drums, turnstile …	
	Perimeter protection by tension cable	
	Bollards (fixed or retractable)	
	Speed reducers	
	Intimidator signals	
	High security locks	
	Security shells for elements of the protection system	
	Uniforms (refers to uniformed staff)	Security guards covering a 24/7 rota
		Dedicating additional security guards on each shift

		Security guards (Security guards working at the facility (regular employees))
		Security guards (Employees of a private security company)
		Security guards equipped with firearms
		Security guards equipped with Handcuffs, plasticuffs (band-type restraints for wrists and ankles)
		Security guards equipped with Batons
		Security guards equipped with individual Security Equipment
		Security guards equipped with suitable communication (Hand-held radio)
		Security guards equipped with suitable lighting equipment (Flashlight (torch))
		Security guards equipped with individual protective gear
		Security guards equipped with whistle
		Security guards equipped with pepper spray
		Security guards equipped with notebook
		Security guards equipped with bull horn
	Construction type of hyperstatic or redundant character	
	Surveillance	Watchtowers along the perimeter fence/wall
		Watchtowers are correctly located in accordance with the terrain and surroundings
		Watchtowers cover the terrain with an effective and sufficient line of sight
		Watchtowers enable convenient and effective observation so that the guards stationed on them can effectively fulfill their assignments
		Observation devices in the towers
		Searchlights in the watchtowers
		Means and mechanisms that assists guards means to quickly contact the control room or another force in the facility during an incident
		Manned Watchtowers
		Manned Watchtowers both day and night
		Manned Watchtowers (24/7)
		Observation measures (binoculars), image intensifiers and thermal viewers
		Observation measures (image intensifiers)
		Observation measures (thermal viewers)

Detection of illegal actions and anti-intrusion. Electronic protection systems	Infrared barriers	
	Perimeter protection by microphonic cable	
	Perimeter protection cable in electrical compression	
	Invisible perimeter protection	
	X-ray scanners fixed	People X-Ray inspection systems
		Baggage X-ray
	Portable scanners	
	Operation scanner in motion	
	Fixed metal detectors	
	Portable metal detectors	
	Portable explosive detectors	
	Anti-bomb containers	
	Explosive ordnances disposal	
	Detection of radioactive material pass	
	Drug detectors	
	Spectrum monitoring systems	
	License Plate Recognition and undercarriage inspection systems	
	RF jamming systems	
	Mobile telephony interception systems	
	Pit for inspecting vehicle undersides	
	Designated areas where persons can be searched in privacy	
	Access control systems (entrance, gates, buildings)	
	Access control system is monitored from a C4I	
	The movements of those entering and exiting the facility are logged	
	Persons/vehicles movement logging system	
	Persons/vehicles paper-based logging system	
	Logging of personal data is approved by a Data Protection authority	

Video surveillance	CCTV	CCTV system (Analog)
		CCTV system (Digital)
		CCTV system (Analog) with recording capabilities
		CCTV system (Digital) with recording capabilities
		The camera equipment, doors, drawers and removable panels are secured with key locks or screws and equipped with tamper proof switches
		Alternate or independent power source is available for use on the system
		The system is monitored 24 hours by security personnel
		The CCTV recording information are saved effectively (at least one year)
		The CCTV system is deployed in accordance with the nature of the terrain
		The CCTV system covers its viewing sector
		Records of the CCTV system are retained (at least one year)
		CCTV systems (e.g. based on WiFi networks) have the proper security features
	Fiber optic telemonitoring systems	
	IP telemonitoring systems	
	Via radio telemonitoring systems	
	ATM telemonitoring systems (asynchronous transfer mode)	
	Digital recording and video transmission	
	Thermal cameras with night vision	

Identification systems	Presence control systems	Detection system (North Finder)
		Detection system (Laser Range Finder)
		Detection system (Thermal Imaging)
		Detection system (Video motion detector)
		Detection system (Acoustic Detection System)
		Detection system (Tremor Detection System)
		The detection systems are inspected and/or tested at least monthly
		Records of the detection systems' inspections are maintained (at least one year) and are easily accessible
		The sensor equipment, doors, drawers and removable panels are secured with key locks or screws and equipped with tamper proof switches

		Alternate or independent power source is available for use on the system
		The system is monitored 24 hours by security personnel
		Concealed areas are monitored by appropriate intrusion detection systems
		Perimeter intrusion detection systems
		The detection systems are suitable for the climatic conditions characteristic to the facility
		The detection systems are suitable for the topographic and environmental conditions
		Warning and alarm systems
		Alarm systems connected to a manned control center
	Access control systems	Gates (vehicle, pedestrian, railway, combined vehicle & pedestrian, staffy and emergencies or special incidents) numbered and marked on a plan
		Electrically opened gates
		Manually opened gates
		Gates anchored to the ground
		Means and mechanisms to prevent the entry of an unauthorized vehicle to the facility
		Means and mechanisms to prevent the entry of an unauthorized staff/personnel to the facility
		Means and mechanisms to ensure that vehicles slow down near the gate
		Special gates and entrances for freight
		Gates for administration only
		Gates guarded or secured
		Perimeter gates guarded or secured
		Perimeter gates locked when not in use
		Lighting fixtures in the entrance area
		Illumination of the guard post at the entrance
		Gates' keys are secure and only authorized personnel can access them
		Waiting areas are not near sensitive locations
		Crowds are concentrated in adequate distance from the gates
	Readers / writers cards	
	Cards printers	
	Security labeling systems	
	Biometric identification systems (fingerprints, eyes, hand, etc.)	

	Accounting and affiliation systems of individuals (as complement of previous systems)	
	Contactless identification systems	Transponders
		Digital control systems of mechanical
		Fire detection systems
		Fire fighting systems
		Vehicle automatic identification systems
		Speed control systems
		Intercom systems
		Public address systems
		Positioning systems
		Moisture detection systems
		Electrical fault detection systems
		Rounds control systems
		Incident management systems
		Warehouse or inventory control systems
		Computer protection systems

Data protection measures	Procedures should be implemented for the management of removable media	
	in accordance with the classification scheme adopted by the organization	
	Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access	
	Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities	
	Media should be securely disposed of, using formal procedures	
	Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage	

	Tests of the security functionality should be carried out during development	
	All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use	
	Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes	
	Operating procedures should be documented and made available to all users who need them	
	Rules for the development of software and systems should be established and applied to developments within the organization	
	A formal user registration and de-registration procedure should be implemented for granting and revoking access for all user types to all systems and services	
	Passwords management systems should be interactive and should ensure quality passwords	
	Principles for engineering secure systems should be established, documented, maintained and applied to any information system development efforts	
	The implementation of changes should be controlled by the use of formal change control procedures	
	Backup copies of information, software and system images should be taken and tested regularly in accordance with the agreed backup policy	
	Media containing information should be protected against unauthorized access, misuse or corruption during transportation	
	Networks should be managed and controlled to protect information in systems and applications	

	Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification	
	Information involved in application service transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay	
	Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access	
	Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed	
	The organization should determine its requirements for information security and continuity of information security management in adverse situations, eg during a crisis or disaster	
	Information should be classified in terms of its value, legal requirements, sensitivity or criticality to the organization	
	Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents	
	All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement	
	Security should be applied to off-site assets taking into account the different risks of working outside the organization's premises	
	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted	

	Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products	
	External datacenter replication	

Response systems	Port Police or Coast Guard	Police station inside port facility
		Coast guard station inside port facility
		Security patrols along the fence
		Security patrols (conducted by Coast Guard)
		Security patrols (conducted by Police)
		Security patrols (conducted by Security guards working at the facility (regular employees))
		Security patrols (conducted by Employees of a private security company)
		Mobile security patrols
		Foot security patrols
		Combined (mobile and on foot) security patrols
		Security patrols inside the facility
		Security patrols outside the fence, in the peripheral zone
		Security patrols (24/7)
		Security force vehicles equipped with signs conspicuously identifying vehicle as a security police vehicle, emergency exterior overhead lights, and an electronic siren
		Guard assignments, times and patrol routes are varied at frequent intervals to avoid establishing routines
		Non-lethal weaponry (tear gas, shockers, anti-riot equipment, etc.)
		Patrols personnel equipped with firearms
		Patrols personnel equipped with Handcuffs, plasticuffs (band-type restraints for wrists and ankles)
		Patrols personnel equipped with Batons
		Patrols personnel equipped with individual Security Equipment
		Patrols personnel equipped with suitable communication (Hand-held radio)

		Patrols personnel equipped with suitable lighting equipment (Flashlight (torch))
		Patrol personnel equipped with individual protective gear
		Patrol personnel equipped with whistle
		Patrols personnel equipped with pepper spray
		Patrols personnel equipped with notebook
		Patrols personnel equipped with bull horn
		Alternative plan for patrols and guarding for sensitive areas in the case of employee strikes
		Security force personnel record or report their presence at key points in facility
		by means of portable watch clocks, general watch clock stations, or telephones
		Patrol vehicles equipped with GPS systems
		Patrol launches equipped with GPS systems
	Clinic inside port facility	
	Civil Defence	Environmental station inside port facility
		The location of equipment in the port facility enable proper evacuation, rescue and support activity in emergencies
		Support and rescue forces equipped with means of transport (sea/land)
		Support and rescue forces equipped with lifeboats
		Support and rescue forces equipped with ambulances
		Support and rescue forces equipped with helicopters
		Support and rescue forces equipped with tugboats
		Support and rescue forces equipped with cranes
		Support and rescue forces equipped with suits for handling hazardous material leaks
	Fire	Fire station inside port facility
		Fire hydrants
		Automatic fire extinguishing systems
		The facility has stationary water tanks
		The facility has mobile water tanks
		The facility has more than one water source
		The facility's main water shut-off valve is inside the facility boundaries
		The fire-fighting systems does not depend only on water arriving from outside sources
	Squad Against Biological And Chemical Threats	
	National Police	Security force vehicles equipped with a spotlight
		Security force equipped with individual vests

		Security force equipped with protective vehicles
		Security force equipped with explosion containment kits
	Army	
Ship's operations and terminal's facilities	The vessels docking alongside the port facility are always with a Pilot on board	
	Port Facilities and berthing of vessels are not influenced by tidal variations/conditions	
	Physical barrier and measures for restricting access to the area	
	Gangways and ropes are manned with security personnel at all times when the ship is berthed	
	Gangways are locked and barred at night	
	Ship's lighting is on to supplement the port lighting at night	
	Ship's lighting does not degrade the existing security lighting	
	Separate terminals for international and domestic shipping	
	Terminal is an enclosed building	
	Area can't be easily observed from outside the facility	
	Exit gate separated from the entrance gate	
	There are not hazardous material transport routes that pass adjacent to the area (e.g. crowd concentrations area) in the facility	
	There are not hazardous material storage areas near the area (e.g. crowd concentrations area) in the facility	
	Vessel traffic management system (VTMS)	Vessel traffic management system (VTMS) (Long range systems (Radar)-based)
		Vessel traffic management system (VTMS) (IFF (Identify Friend/Foe) device-based)
		Vessel traffic management system (VTMS) (CCTV system-based)
		Vessel traffic management system (VTMS) (IFF (Identify Friend/Foe) device-based)

		Vessel traffic management system (VTMS) (Computer system-based)
		Vessel traffic management system (VTMS) (Radar-based) covers the entire facility's entrance area
		Vessel traffic management system (VTMS) (Radar-based) covers most of the facility's entrance area
		VTMS control room is located in a separate secure installation
		VTMS control room can't be easily observed by ground outside the facility
		VTMS control room operates throughout the day
	Conveyance systems are connected to electricity supply backup systems	
	Equipment at the facility for loading/unloading ships (cranes, moving gantry cranes, pneumatic or mechanical – grasps, scoops, conveyors, "endless bolts", grain elevators, etc.)	
	Alternative loading/unloading equipment	
	The facility have a power station inside it	
	The hazardous material pipes are underground throughout the facility and the nearby area	
	Multiple access lanes have been set	
	The lanes include various vessel characteristics (passenger, freight, fishing, etc.)	
	Emergency docking does not block the port access lane	
	Lighthouses and Beacons	
	Buoys	
	Breakwater	
	Stern docking at the breakwater does not exist	
	Fishing areas in the waters near the facility are marked	
	Holiday and sailing areas in the waters near the facility are marked	
	Places for fishing on the breakwater are marked	
	Tourist areas on the breakwater are marked	
	Commercial areas on the breakwater are marked	

	Promontories that projects into the waters near the facility are marked	
	Hazardous material facilities in the waters near the facility are marked	
	Tropical islands/vessels in the waters near the facility are marked	
	Utility facilities (e.g. marina, naval base) in the waters near the facility are marked	
	Fish hatcheries in the waters near the facility are marked	
	Facilities for loading and unloading fuel, gas or other substances in the waters near the facility are marked	
	Facility services are located nearby (tugboats, pilots, oilers, waste disposal) are marked	
	Tourist boats located nearby (cruising in the area of the facility only) are marked and monitored	
	The inlet allows more than one vessel to pass through at once	
	Protection of underwater access	Anti-diver protection system (at facility's entrance)
		Facility's inlet is physically blocked to divers
		Facility's inlet is physically blocked against suspicious vessels
	Ship's stores are scheduled in advance of delivery	
	Cargo inspections	Cargo inspections (on the vessel)
		Cargo inspections (on the quay / wharf)
		Cargo inspections (in the storage warehouses)
		Cargo inspections (at the manufacturing plant)

vii. FORWARD consortium Whitebook threat categorization

Threat Category	Threat	comments
Networking		Threats that are related to the introduction and deployment of new (often wireless) network technologies, but it also covers emerging threats against infrastructure services (routing, DNS) on the current Internet.
	Routing infrastructure	
	IPv6 and direct reachability of hosts	
	Naming (DNS) and registrars	
	Wireless communication	
	Denial of service	
Hardware and virtualization		Threats due to new hardware and software developments that allow computation to be moved to virtual computers, and ultimately, the cloud. It also covers malicious hardware.
	Malicious hardware	
	Virtualization and cloud computing	
Weak devices		Threats that are introduced with new computing devices that are limited, both computationally and because of power constraints. The problem is that security is "expensive," and weak devices might not be able to afford to implement and run adequate protection mechanisms.
	Sensors and RFID	
	Mobile device malware	
Complexity		Threats that emerge due to the fact that some future systems will contain billions of components. Another source of complexity are large monolithic systems that offer more and more functionality. The increased complexity leads to

Threat Category	Threat	comments
		unexpected and unintended dependencies, interactions, and security consequences.
	Unforeseen cascading effects	
	Threats due to scale	
	System maintainability and verifiability	
	Hidden functionality	
	Threats due to parallelism	
Data Manipulation		Threats that stem from the fact that people (and systems) store more data online, and this data is becoming increasingly valuable and sensitive.
	Privacy and ubiquitous sensors	
	False sensor data	
	Threats related to social networks	
	Online games	
Attack infrastructures		Threats that are related to the fact that adversaries actively develop and deploy offensive platforms (such as botnets). That is, 7adversaries no longer perform hit-and-run attacks, but they establish operational bases on the Internet used to carry out malicious campaigns.
	Underground economy support structures	
	Advanced malware	
Human factors		Human factors always played a role in security. This category covers threats that are due to increasing concerns over insider attacks, especially in the context of outsourcing. The category also covers threats that are related to new social engineering attacks.
	User interface	

Threat Category	Threat	comments
	The insider threat	
	Safety takes priority over security	
	New vectors to reach victims	
	Targeted attacks, spear phishing	
Insufficient security requirements		This category covers problems and threats related to legacy and commercial-off-the-shelf systems that have not been built with sufficient protection and are now used and deployed in scenarios for which their protection mechanisms are inadequate.
	Retrofitting security to legacy systems	
	Use of COTS components	
	Next generation networks	
Threats related to parallelism		Single processors have hit the CPU speed wall. However, Moore's law continues to hold, and processor manufacturers are now shipping machines with many CPU cores. These multi-cores need to be programmed, and the paradigm shift from sequential to parallel programming will likely bring a wide range of new vulnerability classes that we need to mitigate. Thus, we require new techniques to help developers write correct code and to detect bugs in parallel programs
Threats related to scale		The effects of scale can be felt everywhere on the Internet. This ranges from the sheer number of devices connected to the network to the size and complexity of individual software packages. We need ways to manage the complexity, scale, and security of such systems
Underground economy support structures		Many attacks on the Internet are driven and fueled by a thriving underground economy. This is the result of a paradigm shift from "hacking for fun" to "hacking

Threat Category	Threat	comments
		for profit." Unfortunately, the mechanics of the underground economy and its support structures are poorly understood. However, it is necessary to study and actively combat the root cause that drives such diverse threats as botnets, phishing, and spam.
Mobile device malware		Malware is already a significant problem on today's Internet. Consider that the number of mobile devices is growing rapidly, users get more comfortable downloading and installing applications (e.g., via Apple's AppStore), and phones are increasingly used for critical applications (e.g., for online banking). Thus, it is just a matter of time before mobile device malware will become mainstream. Unfortunately, mobile devices are constrained, both computationally and because of power limitations, making it hard to deploy costly, traditional anti-malware techniques. As a result, better malware defenses are crucially required for mobile devices.
Threats related to social networks		Social networks are regularly used by hundreds of millions of users who provide a wealth of private information online that could be abused. In addition, social network providers have been notoriously unwilling to provide sufficient privacy protection for their users, and they are looking for ways to monetize their audience and the data they upload. This is a dangerous combination that provides attackers with new ways to reach (and scam) victims, and it can lead to severe, large-scale data theft.

Table 24 - FORWARD Consortium threat categorization

viii. VERIS Taxonomy

Discovery method	Description
Ext - audit	External - security audit or scan
Ext - incident response	External - Notified while investigating another incident
Ext - unknown	External - unknown
Other	Other
Int - NIDS	Internal - network IDS or IPS alert
Ext - emergency response team	External - Emergency response team
Ext - fraud detection	External - fraud detection (e.g., CPP)
Int - incident response	Internal - discovered while responding to another (separate) incident
Ext - customer	External - reported by customer or partner affected by the incident
Prt - audit	Partner - Audit performed by a partner organization
Int - IT review	Internal - Informal IT review
Int - log review	Internal - log review process or SIEM
Int - unknown	Internal – unknown

Discovery method	Description
Ext - suspicious traffic	External - Report of suspicious traffic
Int - HIDS	Internal - host IDS or file integrity monitoring
Prt - Other	Partner – Other
Ext - monitoring service	External - managed security event monitoring service
Prt - antivirus	Partner - Notified by antivirus company but not through AV product
Prt - Unknown	Partner -Unknown
Int - security alarm	Internal - physical security system alarm
Ext - law enforcement	Internal - notified by law enforcement or government agency
Int - antivirus	Internal - antivirus alert
Int - infrastructure monitoring	Internal - Infrastructure monitoring
Prt - incident response	Partner - notified while investigating another incident
Int - data loss prevention	Internal - Data loss prevention software
Int - fraud detection	Internal - fraud detection mechanism

Discovery method	Description
Prt - monitoring service	Partner - Reported by a monitoring service
Int - reported by employee	Internal - reported by employee who saw something odd
Ext - actor disclosure	External - disclosed by threat agent (e.g., public brag, private blackmail)

Table 25 – VERIS Discovery Method

Hacking Variety	Description
XSS	Cross-site scripting
HTTP Response Splitting	HTTP Response Splitting
Unknown	Unknown
Buffer overflow	Buffer overflow
Format string attack	Format string attack
LDAP injection	LDAP injection
SSI injection	SSI injection
MitM	Man-in-the-middle attack
Path traversal	Path traversal

Hacking Variety	Description
URL redirector abuse	URL redirector abuse
Use of backdoor or C2	Use of Backdoor or C2 channel
Mail command injection	Mail command injection
Virtual machine escape	Virtual machine escape
OS commanding	OS commanding
Soap array abuse	Soap array abuse
Footprinting	Footprinting and fingerprinting
Cryptanalysis	Cryptanalysis
SQLi	SQL injection
XML external entities	XML external entities
Abuse of functionality	Abuse of functionality
XML injection	XML injection
Routing detour	Routing detour
HTTP response smuggling	HTTP response smuggling

Hacking Variety	Description
Forced browsing	Forced browsing or predictable resource location
Cache poisoning	Cache poisoning
Null byte injection	Null byte injection
Reverse engineering	Reverse engineering
Brute force	Brute force or password guessing attacks
Fuzz testing	Fuzz testing
Offline cracking	Offline password or key cracking (e.g., rainbow tables, Hashcat, JtR)
CSRF	Cross-site request forgery
XML entity expansion	XML entity expansion
RFI	Remote file inclusion
Session fixation	Session fixation
Integer overflows	Integer overflows
XQuery injection	XQuery injection

Hacking Variety	Description
Pass-the-hash	Pass-the-hash
XML attribute blowup	XML attribute blowup
Session prediction	Credential or session prediction
Use of stolen creds	Use of stolen authentication credentials
HTTP request smuggling	HTTP request smuggling
XPath injection	XPath injection
Other	Other
DoS	Denial of service
Special element injection	Special element injection
HTTP request splitting	HTTP request splitting
Session replay	Session replay

Table 26 – VERIS Hacking Variety

Attribute	Example Value
ISO Currency Code	DZD - Algerian Dinar
Confidence	High confidence

Attribute	Example Value
Targeted	Targeted: victim chosen as target then actor determined what weaknesses could be exploited
Discovery Method	Internal - financial audit and reconciliation process
Cost Corrective Action	Simple and cheap
Security Incident	Suspected
Country	Bangladesh
Impact:Overall_rating	Insignificant: Impact absorbed by normal activitie
Actor:motive	Grudge or personal offense
Asset:management	Internally managed
Asset:variety	Media - Flash drive or card
Asset:Governance	Hosted by 3rd party
Asset:Hosting	Externally hosted in a shared envirnoment
Asset:Ownership	Customer owned
Asset:Cloud	Misconfiguration or error by hosting provider
Victim:Employcount	Over 100,0001 employees
Timeline:Unit	Months
Impact:loss:rating	Major
Impact:loss:variety	Legal and regulatory costs
Attribute:integrity:variety	Created new user account
Attribute:availability:variety	Acceleration
Attribute:confidentiality:data_victim	Customer
Attribute:confidentiality:state	Transmitted encrypted
Attribute:confidentiality:data_disclosure	Yes (confirmed)

Attribute	Example Value
Actor:internal:job_change	Lateral move
Actor:internal:variety	End-user or regular employee
Actor:external:variety	Customer (B2C)
Action:malware:vector	Remotely injected by agent (i.e. via SQLi)
Action:malware:variety	Send spam
Action:social:vector	In-person
Action:social:target	Customer (B2C)
Action:social:variety	Online scam or hoax (e.g., scareware, 419 scam, auction fraud)
Action:environmental:variety	Hazardous material
Action:error:vector	Carelessness
Action:error:variety	Loss or misplacement
Action:misuse:vector	Physical access within corporate facility
Action:misuse:variety	Use of unapproved software or services
Action:hacking:vector	Remote shell
Action:hacking:variety	Cross-site scripting
Action:psysical:vector	Given temporary visitor access
Action:psysical:variety	Snooping (sneak about to gain info or access)
Attribute:confidentiality:data:variety	Personal or identifying information (e.g., addr, ID#, credit score)

Table 27 - VERIS Attributes examples

ix. NIST Guide for Conducting Risk Assessment

Threat Source Type (high level) and description	Threat Source Type	Threat	Characteristics
Adversarial: Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	**Individual**	Outsider	Capability, Intent, Targeting
		Insider	
		Trusted Insider	
		Privileged Insider	
	Group	Ad hoc	
		Established	
	Organization	Competitor	
		Supplier	
		Partner	
		Customer	
	Nation-State		
Accidental: Erroneous actions taken by individuals in the course of executing their everyday responsibilities.	**User**		Range of effects
	Privileged User/Administrator		
Structural: Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.	**Information Technology (IT) Equipment**	Storage	Range of effects
		Processing	
		Communications	
		Display	
		Sensor	
		Controller	
	Environmental Controls	Temperature/Humidity Controls	
		Power Supply	
	Software	Operating System	

Threat Source Type (high level) and description	Threat Source Type	Threat	Characteristics
		Networking	
		General-Purpose Application	
		Mission-Specific Application	
Environmental : Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization. Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks)	**Natural or man-made disaster**	Fire	Range of effects
		Flood/Tsunami	
		Windstorm/Tornado	
		Hurricane	
		Earthquake	
		Bombing	
		Overrun	
	Unusual Natural Event (e.g., sunspots)		
	Infrastructure Failure/Outage	Telecommunications	
		Electrical Power	

Table 28 - NIST Guide threat sources categorization

x. eCSIRT Incident Classification

Incident Class	Incident Type	Description / Examples
Abusive Content	**Abusive Content**	or "Unsolicited Bulk Email", this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having an identical content.
	Harassment	Discreditation or discrimination of somebody (i.e. Cyberstalking)
	Child/Sexual/Violence/...	Child Pornography, glorification of violence, ...
Malicious Code	**Virus**	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialer	
Information Gathering	**Scanning**	Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, …).
	Sniffing	Observing and recording of network traffic (wiretapping).
	Social Engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats)

Incident Class	Incident Type	Description / Examples
Intrusion Attempts	**Exploiting of known Vulnerabilities**	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g. buffer overflow, backdoors, cross side scripting, etc.).
	Login attempts	Multiple login attempts (Guessing / cracking of passwords, brute force).
	new attack signature	An attempt using an unknown exploit.
Intrusions	**Privileged Account Compromise**	A successful compromise of a system or application (service). This can have been caused remote by a known or new vulnerability, but also by an unauthorized local access.
	Unprivileged Account Compromise	
	Application Compromise	
Availability	**DoS**	By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. Examples of a remote DoS are SYS- a. PING-flooding or E-mail bombing (DDoS: TFN, Trinity, etc.). However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.).
	DDoS	
	Sabotage	
Information Security	**Unauthorised access to information**	Besides a local abuse of data and systems the information security can be endangered by a successful account or application compromise. Furthermore, attacks are possible that intercepts and access information during transmission (wiretapping, spoofing or hijacking).
	Unauthorised modification of information	

Incident Class	Incident Type	Description / Examples
	Unauthorized use of resources	Using resources for unauthorized purposes including profit-making ventures (E.g. the use of e-mail to participate in illegal profit chain letters or pyramid schemes).
	Copyright	Selling or Installing copies of unlicensed commercial software or other copyright protected materials (Warez).
	Masquerade	Type of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it.
Other	**All incidents which don't fit in one of the given categories should be put into this class.**	If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.

Table 29 - ECSIRT.net Incident Classification

xi. OWASP Threat Categories

OWASP Security risks	Threat agents / attack vectors
A1- INJECTION	Almost any source of data can be an injection vector, environment variables, parameters, external and internal web services, and all types of users. Injection flaws occur when an attacker can send hostile data to an interpreter.
A2- BROKEN ACCESS CONTROL	Attackers have access to hundreds of millions of valid username and password combinations for credential stuffing, default administrative account lists, automated brute force, and dictionary attack tools. Session management attacks are well understood, particularly in relation to unexpired session tokens.
A3- SENSITIVE DATA EXPOSURE	Rather than directly attacking crypto, attackers steal keys, execute man-in-the-middle attacks, or steal clear text data off the server, while in transit, or from the user's client, e.g. browser. A manual attack is generally required. Previously retrieved password databases could be brute forced by Graphics Processing Units (GPUs).
A4- XML EXTERNAL ENTITIES (XXE)	Attackers can exploit vulnerable XML processors if they can upload XML or include hostile content in an XML document, exploiting vulnerable code, dependencies or integrations.
A5-BROKEN ACCESS CONTROL	Exploitation of access control is a core skill of attackers. SAST and DAST tools can detect the absence of access control but cannot verify if it is functional when it is present. Access control is detectable using manual means, or possibly through automation for the absence of access controls in certain frameworks.
A6- SECURITY MISCONFIGURATION	Attackers will often attempt to exploit unpatched flaws or access default accounts, unused pages, unprotected files and directories, etc to gain unauthorized access or knowledge of the system.

OWASP Security risks	Threat agents / attack vectors
A7- CROSS SITE SCRIPTING (XSS)	Automated tools can detect and exploit all three forms of XSS, and there are freely available exploitation frameworks.
A8- INSECURE DESERIALIZATION	Exploitation of deserialization is somewhat difficult, as off the shelf exploits rarely work without changes or tweaks to the underlying exploit code.
A9- USING COMPONENTS WITH KNOWN VULNERABILITIES	While it is easy to find already-written exploits for many known vulnerabilities, other vulnerabilities require concentrated effort to develop a custom exploit.
A10- INSUFFICIENT LOGGING & MONITORING	Exploitation of insufficient logging and monitoring is the bedrock of nearly every major incident. Attackers rely on the lack of monitoring and timely response to achieve their goals without being detected.

Table 30 - OWASP TOP 10 - 2017 Threat Categories

xii. A Taxonomy of Operational Cyber Security Risks (Software Engineering Institute)

Class	Subclass	Risk
Actions of People	**Inadvertent**	Mistakes
		Errors
		Omissions
	Deliberate	Fraud
		Sabotage
		Theft
		Vandalism
	Inaction	Skills
		Knowledge
		Guidance
		Availability
Systems and Technology Failures	**Hardware**	Capacity
		Performance
		Maintenance
		Obsolescence
	Software	Compatibility
		Configuration Management
		Change Control
		Security Settings
		Coding Practices
		Testing
	Systems	Design
		Specifications
		Integration

Class	Subclass	Risk
		Complexity
Failed Internal Processes	**Process Design and/or Execution**	Process Flow
		Process Documentation
		Roles and Responsibilities
		Notifications and Alerts
		Information Flow
		Escalation of Issues
		Service Level Agreements
		Task Hand-Off
	Process Controls	Status Monitoring
		Metrics
		Periodic Review
		Process Ownership
	Supporting Processes	Staffing
		Funding
		Training and Development
		Procurement
External Events	**Hazards**	Weather Event
		Fire
		Flood
		Earthquake
		Unrest
		Pandemic
	Legal Issues	Regulatory compliance
		Legislation
		Litigation

Class	Subclass	Risk
	Business Issues	Supplier Failure
		Market Conditions
		Economic Conditions
	Service Dependencies	Utilities
		Emergency services
		Fuel
		Transportation

Table 31 - Taxonomy of Operational Cyber Security Risks by Software Engineering Institute

xiii. ESCORTS Project

High Level Vulnerabilities	Vulnerabilities
Architectural vulnerabilities	
Security policy vulnerabilities	
Software vulnerabilities	
Communication protocol vulnerabilities	MODBUS vulnerabilities
	DNP3 vulnerabilities
	Summary of the vulnerabilities of protocol and relevant threats.

Table 32 - SCADA vulnerabilities by ESCORTS Project

High Level Attack Scenario	Attack Scenario
SCADA protocol-oriented attacks	SCADA malware DOS scenario
	SCADA unauthorised command execution scenario
	SCADA system data poisoning
Process network attacks	OPC DOS
	OPC corruption poisoning
	OPC protocol corruption
	SCADA server DOS
	SCADA server corruption
	SCADA server data flow corruption
	HMI corruption
Exchange network attacks	Real-time databases attacks
	Diagnostic server attacks

Table 33 - Attack scenarios Classification by ESCORTS Project

High Level Security Countermeasures	Security Countermeasures
Communication protocol	TCP/IP

High Level Security Countermeasures	Security Countermeasures
	SCADA protocol (Modbus, DNP3 etc.)
Filtering and monitoring countermeasures	multi-homed PC
	multi-homed server with software firewall
	layer 3 switch network filtering

High Level Security Countermeasures	Security Countermeasures
	two port firewall
	dual filtering (router firewall)
	multi-port firewall with demilitarised zone
	paired firewall and multiple DMZ
	firewall / VLAN architecture
	firewall / VLAN / VPN architecture
	Monitoring
	limits of intrusion detection in SCADA systems
Architectural	firewall and network segregation
	hyper text transfer protocol (HTTP)
	FTP and trivial file transfer protocol (TFTP)
	telnet
	simple mail transfer protocol (SMTP)
	simple network management protocol (SNMP)
	distributed component object model (DCOM)
	SCADA and industrial protocols
	antivirus and malware detection
	backup, restore and disaster recovery
	remote access and data transfer services
	system hardening
	wireless connectivity
	account management
	software management and update
Organisational	

Table 34 – Organizational Countermeasures Classification by ESCORTS project

xiv. HP Tipping Point Event Taxonomy

Major Category	Category Description	Minor Categories
Vulnerability	This category includes events triggered by an attempt to exploit vulnerability in any application, operating system, or networked hardware device.	Buffer/Heap Overflow
		Denial of Service (Crash/Reboot)
		Configuration Error
		Race Condition
		Invalid Input (Command Injection, Cross-Site Scripting, SQL Injection, etc.)
		Access Validation
		Other
Malicious Code	This includes events triggered by viruses, worms, Trojans, backdoors, and all manner of blended malware threats.	Worm
		Virus
		Trojan/Backdoor
		IRC Botnet/Blended Threat
		Phishing
		Other
Distributed Denial of Service (DDoS)	This category includes events triggered by traffic thresholds that indicate an attempt to make a resource unavailable	SYN Flood Attack
		Other Flood Attack (e.g., ACK, CPS, etc.)
		Iterative Application Attack (Hammer)
		Other
Security Policy	This category includes events that indicate an attempt to violate an organization's security policy. It covers P2P, IM, email attachments, IRC, and other network communication types.	P2P
		Chat and Instant Messaging
		Streaming Media
		Email Attachments
		Forbidden Application Access or Service Request (Telnet, SMB Null Session, etc.)

Major Category	Category Description	Minor Categories
		Authentication Failure (Telnet login failed, brute force, etc.)
		Spyware
		Other
Reconnaissance or Suspicious Access	This category includes events that indicate network activity usually associated with common information gathering techniques used by attackers to launch more sophisticated attacks.	Port Scan
		Suspicious Application Access
		Suspicious Service Request
		Host Scan
		Other
Application or Protocol Anomaly	This category includes events that indicate a violation of a protocol or application's RFC.	Protocol Anomaly
		Evasion Technique
		Application Anomaly
		Other Anomaly
Traffic Thresholds	This category includes events triggered by predefined thresholds for specific applications or ports.	Traffic Threshold
		Application Threshold
		Other
IP Filters	This category includes events triggered by predefined IP access control lists.	Deny
		Accept
		Other

Table 35 - HP Tipping Point Event Taxonomy

xv. Threat Taxonomy for Cloud of Things

Threat Type	High Level Threat	Threat
Security Threats	**Communication threats**	Availability
		Eavesdropping
		Spoofing
		Man-in-the-middle (MITM) attack
		Replay attack
	Physical threats	Device capture
		Node damaging
		Side channel attack
	Data threats	Data retrieval from devices
		Data Integrity & Confidentiality
		Device authenticity
		Key compromisation
		False data injection
		Weak cryptographic protocols
		Data loss and leakage
		Data breaches
		Data sensitivity
	Service provisioning threats	Unidentified and unauthorized access
		Escalation of privileges
		Identity theft
		Service hijacking
		Insecure interfaces and API
		Compromising management interface
	Other threats	Malicious insiders

Threat Type	High Level Threat	Threat
		Shared technology issues
		Abusing cloud computing
Privacy Threats		Unnoticed capture & unware identitification
		IoT data inaccessibility
		Lack of control and transparency
		Loss of governance
		Profiling and tracking
		Unforeseen inference
		Unauthorised disclosure

Table 36 - Taxonomy of threats for Cloud of Things

xvi. A multi dimension Taxonomy of Insider Threats in Cloud Computing

Layer 1	Layer 2	Layer 3	Layer 4	Layer 5	Example
Private Cloud	CSC	Confidentiality	IP Theft (Data exfiltration)		Disclosing sensitive Email
		Integrity	Fraud		Altering Records in Payroll System
		Availability	IT Sabotage		Printing Malware
Public Cloud	CSP	Availability	IT Sabotage	IaaS	Attacking Hypervisor
		Confidentiality	IP Theft (Data exfiltration)	IaaS	VM clone
	CSC	Confidentiality	IP Theft (Data exfiltration)	SaaS Paas IaaS	Leaking file from storage application
		Integrity	Fraud	SaaS Paas	Altering CRM records
		Availability	IT Sabotage	Paas IaaS	Planting Malware through Amazon Mechanical Turk
Community	Third Party	Confidentiality	IP Theft (Data exfiltration)		Disclosing info from library system
		Integrity	Fraud		Modifying patient records in

Layer 1	Layer 2	Layer 3	Layer 4	Layer 5	Example
					health system
		Availability	IT Sabotage		

Table 37 - Hierarchical Taxonomies of insider threats in Cloud Computing

xvii. A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks

Attack	Classification		
	Orchestration	Exploitation	Execution
Bluetooth Phishing (Snarfing Attack)	MA1, TD2, MD3	DV1, IM1	AP1, ES1
Cryptovirus/Cryptotrojan/Cryptoworm	MA2, TD2, MD1-L	DV1, IM2	AP2, ES1
Drive-By Download	MA2, TD2, MD1-R	DV3, IM2	AP1, ES1
Fake Mobile App	MA2, TD2, MD1-R	DV2, IM2	AP2, ES2
Forum Phishing—Manual	MA1, TD2, MD1-R	DV2, IM1	AP1, ES1
HTTPS Man-in-the-Middle Adware	MA2, TD2, MD1-L	DV3, IM2	AP2, ES1
Instant Message Phishing—Automated	MA2, TD2, MD1-R	DV2, IM1	AP1, ES1
Malicious Web Pop-Up	MA2, TD2, MD1-R	DV1, IM2	AP1, ES1
Malvertisement	MA2, TD2, MD1-R	DV1, IM1	AP2, ES1
Multimedia Masquerading	MA2, TD2, MD1-R	DV1, IM2	AP1, ES1

Attack	Classification		
	Orchestration	Exploitation	Execution
NFC Phishing	MA2, TD2, MD3	DV3, IM2	AP1, ES2
P2P Malware	MA2, TD2, MD1-R	DV1, IM1	AP1, ES1
PDF File Masquerading	MA2, TD2, MD1-L	DV3, IM2	AP1, ES1
Peripheral Masquerading—USB	MA1, TD1, MD3	DV3, IM2	AP2, ES2
Peripheral Masquerading—Firewire	MA1, TD1, MD2	DV3, IM2	AP2, ES1
Phishing Website	MA2, TD2, MD1-R	DV3, IM2	AP1, ES1
Ransomware	MA2, TD2, MD1-L	DV1, IM2	AP2, ES2
Rogueware	MA2, TD2, MD1-L	DV3, IM2	AP2, ES2
Rogue Access Point	MA1, TD2, MD3	DV2, IM1	AP2, ES1
Scareware	MA2, TD2, MD1-L	DV3, IM2	AP2, ES2
Search Engine Poisoning (Spamdexing)	MA2, TD2, MD1-R	DV2, IM1	AP1, ES1
SMS Worm (Selfmite)	MA2, TD2, MD1-L	DV1, IM2	AP1, ES2
Spam Phishing Email (Botnet-generated)	MA2, TD2, MD1-R	DV1, IM1	AP1, ES1

Attack	Classification		
	Orchestration	Exploitation	Execution
Spear-Phishing Email	MA1, TD1, MD1-R	DV1, IM1	AP1, ES1
Spear-Phishing Email—APT	MA1, TD1, MD1-R	DV3, IM1	AP1, ES2
Tabnabbing	MA2, TD2, MD1-R	DV1, IM2	AP1, ES1
Typosquatting (also known as Cybersquatting)	MA2, TD2, MD1-R	DV1, IM1	AP1, ES2
Visual SSL Spoofing	MA2, TD2, MD1-R	DV1, IM1	AP1, ES1
Watering Hole	MA2, TD1, MD1-R	DV3, IM2	AP1, ES1
WiFi Evil Twin	MA1, TD2, MD3	DV3, IM2	AP2, ES2

Table 38 - Taxonomic Classification of Semantic Attacks

xviii. VoIP Security and Privacy Threat Taxonomy

High level Threat	Threat Category	Threat	Examples
Social Threats	***Misrepresentation***	Misrepresenting Identity	Presentation of a false caller ID name or number with the intent to mislead
			Presentation of a false voice, name, or organization in a voice/video mail with the intent to mislead
			Presentation of a false email with the intent to mislead
			Presentation of false presence information with the intent to mislead
		Misrepresenting Authority	Presentation of a password, key or certificate of another with the intent to mislead
			Circumvention of conditional access with the intent to mislead
			False claim of government authority bypassing ordinary authentication
		Misrepresenting Rights	Presentation of a password, key or certificate with the intent to gain rights not granted
			Circumvention of conditional access with the intent to gain rights not granted
			Modification of access control lists with the intent to gain rights not grated
		Misrepresenting Content	False impersonation of the voice of a caller with the intent to mislead
			False impersonation of the words of a caller with the intent to mislead
			Misleading printed words, still images or moving images in video
			Mmodifications of spoken, written or visual content with the intent to mislead
	Theft of Services		Unauthorized deletion or altering of billing records
			Unauthorized bypass of lawful billing systems

			Unauthorized billing
			Taking of service provider property
	Unwanted Contact	Harassment	
		Extortion	
		Unwanted Lawful Content	Including VoIP SPAM and Other Subjectively Offensive Content
Eavesdropping	**Call Pattern Tracking**		
	Traffic Capture		
	Number Harvesting		
	Conversation Reconstruction		
	Voicemail Reconstruction		
	Fax Reconstruction		
	Video Reconstruction		
	Text Reconstruction		
Interception and Modification	***Call Black Holing***		
	Call Rerouting		
	Fax Alteration		
	Conversation Alteration		
	Conversation Degrading		
	Conversation Impersonation and Hijacking		
	False Caller Identification		

Service Abuse	***Call Conference Abuse***			
	Premium Rate Service (PRS) Fraud			
	Improper Bypass or Adjustment to Billing			
	Other Improper Access To Services		Various forms of call bypass connection via conferencing, signaling and transferring means to add unauthorized parties, possibly dropping connections to conceal the fraud.	
			Various forms of identity theft where legitimate credentials obtained without consent are used for access without permission of their rightful owner.	
			Various forms of internal fraud exploiting internal access access into authentication systems (e.g. RADIUS, LDAP, Active Directory, VOIP gateway and signaling switches)	
			Registration attacks in which an attacker exploits vulnerabilities in registration injecting themselves into a signal path.	
			Misconfiguration of end-points	
			Various methods of concealing fraud by spreading access across multiple accounts to avoid detection by fraud analytical analysis and reporting software.	
Intentional Interruption of Service	***Denial of Service***	VoIP Specific DoS	Request Flooding	User Call Flooding
				User Call Flooding Overflowing to Other Devices
				Endpoint Request Flooding
				Endpoint Request Flooding after Call Setup
				Call Controller Flooding
				Request Looping
				Directory Service Flooding
				Disabling Endpoints with Invalid Requests

			Malformed Requests and Messages	*Injecting Invalid Media into Call Processor*
				Malformed Protocol Messages
			QoS Abuse	
			Spoofed Messages	Faked Call Teardown Message
				Faked Response
			Call Hijacking	Registration Hijacking
				Media Session Hijacking
				Server Masquerading
		Network Services DoS		
		Underlying Operating System/Firmware DoS		
		Distributed Denial of Service		
	Physical Intrusion		Physical access to facilities containing networking equipment	Location where the facility which may be at a sensitive site
				Entry Points including windows, doors, wiring closets, maintenance and roof entrances, floors, emergency exits, and shipping and receiving areas.
			Physical access to the cable and wire system in such facilities	Access to electrical signals conducted over copper wires through an antenna or inductive coil
				Fiber optics systems that are physically wiretapped
				Wireless systems - antennas in proximity to the target system and RF signals that are interfered with or intercepted
			Physical access to systems and equipment	
			Vulnerability to social engineering attacks	Classic social engineering of enterprise personnel via phone, direct contact or email
				Impersonation

				False ID
				Surreptitious Entry
				Unmonitored/uncontrolled access, entry
Other Interruptions of Service	***Loss of Power***			
	Resource Exhaustion		Deficiencies in software or hardware that causes depletion of memory resource (e.g. buffers) in a network element.	
			Deficiencies in software or hardware that consumes most of CPU resource in a network element.	
			Hardware or software errors that limit available bandwidth of a communication link.	
			Software or hardware deficiencies that generate unnecessary messages reducing bandwidth resources	
			Errors in operations by network management system or by craft personnel resulting in limited or unavailable memory, CPU or bandwidth resources.	
			Attacks in this security threat category may target Endpoints, Servers, or both:	
	Performance Latency			

Table 39 - VoIP Security and Privacy Threat Taxonomy

xix. MISP Information Security Indicators Class

Information Security Indicators - Class	Category	Indicator	Description
IEX (external malicious threat sources.)	**Forgery**	Forged domain or brand names impersonating or imitating legitimate and genuine names	Forged domains are addresses very close to the domain names legitimately filed with registration companies or organizations (forged domains are harmful only when actively used to entice customers to the website for fraudulent purposes). It also includes domain names that imitate another domain name or a brand.
		Wholly or partly forged websites (excluding parking pages) spoiling company's image or business	Forged websites correspond to two main threats (forgery of sites in order to steal personal data such as account identifiers and passwords, forgery of services in order to capitalize on a brand and to generate turnover that creates unfair competition). In this case, reference is often made to phishing (1st usage) or pharming.
	Spam	Not requested received bulk messages (spam) targeting organization's registered users	Spam are messages received in company's or organization's messaging systems in the framework of mass and not individualized campaigns, luring into clicking dangerous URLs (possibly Trojan laden) or enticing to carry out harmful to concerned individual actions.
	Phishing	Phishing targeting company's customers' workstations spoiling	Phishing involves a growing number of business sectors (financial organizations, e-commerce sites, online games, social sites etc.). It

		company's image or business	includes attacks via e-mail with messages that contain either malicious URL links (to forged websites) or malicious URL links (to malware laden genuine websites).
		Spear phishing or whaling carried out using social engineering and targeting organization's specific registered users	Spear phishing are "spoofed" and customized messages looking like a usual professional relationship or an authority and asking to click on or open dangerous URL links or dangerous attachments (malware laden).
	Intrusion	Intrusion attempts on externally accessible servers	Attempts are here systematic scans (excluding network reconnaissance) and abnormal and suspicious requests on externally accessible servers, detected by an IDS/IPS or not.
		Intrusion on externally accessible servers	Intrusion on externally accessible servers
		Intrusions on internal servers	This kind of incident typically comes after a PC malware installation or an intrusion on an externally accessible server often followed by a lateral movement. This indicator does not include the figures from the Misappropriation indicator which may however start with an intrusion on an internal server. This indicator includes the so-called APTs (Advanced Persistent Threats), which constitute however only a small part of this indicator. APTs are long lasting and stealthy incidents with large compromises of data through outbound links, which is not the case of most

			incidents of the IEX_INT.3 type. This type of incident is often the result of targeted attacks.
	Defacements	Obvious and visible websites defacements	Obvious defacements measure the defacement of homepages and of the most consulted pages of sites.
	Misappropriation	Servers resources misappropriation by external attackers	This indicator measures the amount of resources of servers misappropriated by an external attacker after a successful intrusion (on an externally accessible or an internal server).
	Denial of service	Denial of service attacks on websites	This indicator measures denial-of-service attacks against websites, carried out either by sending of harmful requests (DoS), by sending a massive flow coming from multiple distributed sites (DDoS) or via other techniques. Due to the current state of the art of attack detection, the indicator is limited to DDoS attacks.
	Malware	Attempts to install malware on workstations	Malware installation attempts are detected by current conventional means (Antivirus and base IPS) and blocked by the same means. This indicator (which includes desktop and laptop PC based workstations but does not include the different types of other workstations and mobile smart devices) provides an approximate insight into the malicious external pressure suffered in this regard. This indicator should be associated with indicator on successful

			malware installation in order to assess the actual effectiveness of conventional detection and blockage means in the fight against malware.
		Attempts to install malware on servers	Malware installation attempts are detected by current conventional means (antivirus and base IPS) and blocked by the same means. This indicator gives an approximate insight into the malicious external pressure suffered in this regard. This indicator should be associated with indicator on successful malware installation in order to assess the actual effectiveness of conventional detection and blockage means in the fight against malware.
		Malware installed on workstations	Malware could be not detected by conventional means (lack of activation or appropriate update), or noninventoried and/or specific very stealthy incidents, most of the time not detectable by conventional means (AV and standard IPS), consequently requiring other supplementary detection means (network or WS load, outbound links, advanced network devices as DPI tools, users themselves reporting to help desks). This indicator (which includes desktop and laptop Windows-based workstations but does not include the different types of other workstations and mobile smart devices) therefore applies to both

			classical viruses and worms, as well as all new malware such as Trojan horses (which are defined as malware meant to data theft or malicious transactions) or bots (which are defined here as vectors for spam or DDoS attacks).
		Malware installed on internal servers	Malware could be not detected by conventional means (lack of activation or of appropriate update), or noninventoried and/or specific very stealthy incidents, most of the time not detectable by conventional means (AV and standard IPS), consequently requiring other supplementary detection means (network or server load, outbound links, advanced network devices as DPI tools, administrators themselves). This indicator therefore applies to both classical viruses and worms, as well as all new malware such as Trojan horses (which are defined as malware meant to data theft or malicious transactions)
	Human intrusion	Human intrusion into the organization's perimeter	This indicator measures illicit entrance of individuals into security perimeter.
IMF (Incidents caused by malfunctions, breakdowns or human errors.)	**Breakdowns**	Workstations accidental breakdowns or malfunctions	Breakdowns or malfunctions apply to both hardware and software, caused by system errors (components failure or bugs).
		Servers accidental breakdowns or malfunctions	Breakdowns or malfunctions apply to both hardware and software, caused by system

			errors (components failure or bugs).
		Mainframes accidental breakdowns or malfunctions	Breakdowns or malfunctions apply to both hardware and software, caused by system errors (components failure or bugs).
		Networks accidental breakdowns or malfunctions	Breakdowns or malfunctions apply to both hardware and software, caused by system errors (components failure or bugs).
	Mail Delivery	Delivery of email to wrong recipient	This indicator measures errors from the sender when selecting or typing email addresses leading to misdelivery incidents. Consequences may be very serious when confidentiality is critical.
	Loss (or theft) of mobile devices	Loss (or theft) of mobile devices belonging to the organization	This indicator measures the loss of all types of systems containing sensitive or not information belonging to the organization, whether encrypted or not (laptop computers, USB tokens, CD-ROMs, diskettes, magnetic tapes, smartphones, tablets, etc.). In some cases, it could be difficult to differentiate losses from thefts.
	Log production	Downtime or malfunction of the log production function with possible legal impact	This type of event could have two main causes: an accidental system malfunction or a system manipulation error by an administrator. Logs taken into account here are systems logs and applications logs of all servers.
		Absence of possible tracking of the person involved in a security	Concerns unique data related to a given and known to organization user (identifier

		event with possible legal impact	tied to application software or directory). This indicator is a sub-set of indicator IMF_LOG.1.
		Downtime or malfunction of the log production function for recordings with evidential value for access to or handling of information that, at this level, is subject to law or regulatory requirements	This indicator primarily relates to Personal Identifiable Information (PII) protected by privacy laws, to information falling under the PCI-DSS regulation, to information falling under European regulation in the area of breach notification (Telcos and ISPs to begin with), and to information about electronic exchanges between employees and the exterior (electronic messaging and Internet connection). This indicator does not include possible difficulties pertaining to proof forwarding from field operations to governance (state-of-the-art unavailable). This indicator is a sub-set of indicator IMF_LOG.1 but can be identical to this one in advanced organizations.
IDB (internal deviant behaviours (including especially usurpation of rights or of identity)._	**User impersonation**	User impersonation	A person within the organization impersonates a registered user (employee, partner, contractor, external service provider) using identifier, passwords or authentication devices that had previously been obtained in an illicit manner (using a social engineering technique or not). This measures cases of usurpation for malicious purposes, and not ones that relate to user-friendly usage. Moreover, assumption is made that ID/Password is the main way of authentication

	Abuse of privileges	Privilege escalation by exploitation of software or configuration vulnerability on an externally accessible server	Exploited vulnerabilities are typically tied to the underlying OS that supports the Web application, exploited notably through injection of additional characters in URL links. This behaviour specifically involves external service providers and company's business partners that wish to access additional information or to launch unlawful actions (for example, service providers seeking information about their competitors). This type of behaviour is less frequent amongst employees, since it is often easier to get the same results by means of social engineering methods.
		Privilege escalation on a server or central application by social engineering	It is often easier to get the same results by means of social engineering methods than with technical means. Help desk teams are often involved in this kind of behaviour.
		Use on a server or central application of administrator rights illicitly granted by an administrator	Illicitly granting administrator privileges generally comes from simple errors or more worrisome negligence on the part of the administrators (malicious action is rarer). The case of forgotten temporary rights (see next indicator), is not included in this indicator.
		Use on a server or central application of time-limited granted rights after the planned period	This indicator measures situations where time-limited user accounts (created for training, problem resolution, emergency access, test, etc.)

			are still in use after the initial planned period.
		Abuse of privileges by an administrator on a server or central application	The motivation of rights usurpation by an administrator is often the desire to breach the confidentiality of sensitive data (for example, human resources data). This indicator is similar to the indicator IDB_RGH.6 (but with consequences that may be however often potentially more serious).
		Abuse of privileges by an operator or a plain user on a server or central application	This indicator applies for example to authorized users having access to personal identifiable information aboutcelebrities with no real need for their job (thereby violating the "right to know").
		Illicit use on a server or central application of rights not removed after departure or position change within the organization	This indicator also takes into account the problem of generic accounts (whose password might have been changed each time a user knowing this password is leaving organization).
	Misappropriation	Server resources misappropriation by an internal source	This indicator measures misappropriation of on-line IT resources for one's own use (personal, association etc.).
	Access to hacking Website	Access to hacking Website	This indicator measures unauthorized access to a hacking Website from an internal workstation
	Deactivating of logs recording	Deactivating of logs recording by an administrator	This event is generally decided and deployed by an administrator in order to improve performance of the system under his/her responsibility (illicit voluntary stoppage). This indicator is a

			reduced subset of indicator IUS_RGH.5
IWH (all categories of incidents)	**Exploitation of a software vulnerability**	Exploitation of a software vulnerability without available patch	This indicator measures security incidents that are the result of an exploitation of a disclosed software vulnerability that has no available patch (with or without an applied workaround measure). It is used to assess the intensity of the exploitation of recently disclosed software vulnerabilities (zero day or not). Patching here applies only to standard software (excluding bespoke software), and the scope is limited to workstations (OS, browsers and various add-ons and plug-ins, office automation standard software).
		Exploitation of a non-patched software vulnerability	This indicator measures security incidents that are the result of the exploitation of a non-patched software vulnerability though a patch exists. It is used to assess effectiveness or application of patching-related organization and processes and tools (patching not launched). It is linked with indicator VOR_VNP.2 that is intended to assess problems of exceeding the "time limit for the window of exposure to risks". It has the same limitations as IWH_VNP.1 regarding scope.
		Exploitation of a poorly-patched software vulnerability	This indicator measures security incidents that are the result of the exploitation of a poorly patched software vulnerability. It is used to

			assess effectiveness of patching-related organization and processes and tools (process launched but patch not operational - Cf. no reboot, etc.). It is linked with indicator VOR_VNP.1, IWH_VNP.1 and IWH_VNP.2. It has the same limitations as IWH_VNP.1 regarding scope.
	Exploitation of a configuration flaw	Exploitation of a configuration flaw	This indicator measures security incidents that are the result of the exploitation of a configuration flaw on servers or workstations. A configuration flaw should be considered as a nonconformity against state-of-the-art security policy.
	Unknown	Not categorized security incidents	This indicator measures all types of incidents that are new and/or a complex combination of more basic incidents and cannot be fully qualified and therefore precisely categorized.
	Non-inventoried	Security incidents on non-inventoried and/or not managed assets	This indicator measures security incidents tied to assets (on servers) non-inventoried and not managed by appointed teams. It is a key indicator insofar as a high percentage of incidents corresponds with this indicator on average in the profession (according to some public surveys).
VBH (Existence of abnormal behaviours that could lead to security incidents.)		Server accessed by an administrator with unsecure protocols	This indicator measures the use of insecure protocols set up by an administrator to get access to organization based externally accessible servers making an external intrusion possible. Insecure protocol means unencrypted, without

			time-out, with poor authentication means etc. (for example Telnet).
		P2P client in a workstation	This indicator measures the installation of P2P clients set up by a user on its professional workstation with the risk of partial or full sharing of the workstation content. It applies to workstations that are either connected to the organization's network from within the organization or directly connected to the public network from outside (notably home). There is a high risk of accidental sharing (in one quarter of all cases) of files that may host confidential company data. It is most often carried out through HTTP channel (proposed on all of these services).
		VoIP clients in a workstation	This indicator measures VoIP clients installed by a user on his/her own workstation in order to use a peer-to-peer service. It applies to workstations connected to an organization's network from within the organization or directly connected to the public network from outside (notably home). The associated risk is to exchange dangerous Office documents. It is most often carried out through HTTP channel (proposed on all of these services).
		Outbound connection dangerously set up	This indicator measures outbound connection dangerously set up to get remote access to the

			company's internal network without using an inbound VPN link and a focal access point with possible exploitation by an external intruder. The outbound connection method consists for example in using a GoToMyPC™ software or a LogMeIn® software or a computer to computer connection in tunnel mode.
		Not compliant laptop computer used to establish a connection	This indicator measures remote or local connection to the organization's internal network from a roaming laptop computer that is organization-owned and is configured with weak parameters. In this situation and in case of the existence of a software to check compliance of roaming computers, another related software blocks the connection in principle and prevents its continuation.
		Other unsecure protocols used	This indicator measures other unsecure or dangerous protocols set up with similar behaviours. The other cases are the other than the 5 previous ones (VBH_PRC.1 to VBH_PRC.5). It relates to dangerous or abusive usages, i.e. situations where usages are not required and where other more secure solutions exist.
	Internet Access Control	Outbound controls bypassed to access Internet	This indicator measures the detection of Internet access from the internal network by means that bypass the outbound security devices. It primarily relates to Internet accesses from a perimeter

			area or to tunnelling (SSL port 443) or to straight accesses (via an ADSL link or public Wi-Fi access points and the telephone network) or to accesses via Smartphones connected to the workstation. The main underlying motivation is to prevent user tracking.
		Anonymization site used to access Internet	This indicator measures the detection of anonymous Internet access from an internal workstation through an anonymization site. The goal is to maintain free access and to avoid organization's filtering of accesses to forbidden websites.
	File Transfer	Files recklessly downloaded	This indicator measures the download of files from an external website that is not known (no reputation) within the profession to an internal workstation. "No reputation" can be assessed by information provided by URL outbound filtering devices.
		Personal public instant messaging account used for business file exchanges	This indicator measures the use of personal public instant messaging accounts for business exchanges with outside. This file exchange method has to be avoided due to network AV software bypassing and to identify lesser effectiveness of AV software.
		Personal public messaging account used for business file exchanges	This indicator measures the use of personal public messaging accounts for business file exchanges with the exterior. The risk is to

			expose information to external attackers.
	WTI	Workstations accessed in administrator mode	This indicator measures access to workstations in administrator mode without authorization.
		Personal storage devices used	This indicator measures the use personal storage devices on a professional workstation to input or output information or software. Mobile or removable personal storage devices include USB tokens, smartphones, tablets, etc. It is not applicable to personal devices authorized by security policy (Cf. VBH_WTI.3 and BYOD).
		Personal devices used without compartmentalization (BYOD)	This indicator measures the lack of or the removal of basic security measures meant to compartmentalize professional activities on personal devices. Personal devices (BYOD) include PCs, tablets, smartphones, etc.
		Not encrypted sensitive files exported	This indicator measures the lack of encryption of sensitive files uploaded from a professional workstation to professional mobile or removable storage devices.
		Personal software used	This indicator measures the presence of personal software on a professional workstation that does not comply with the corporate security policy. It corresponds with all types of local unauthorized software (with a user licence or not), such as common personal software (games, office automation

			etc.) or more dangerous ones (hacking etc.). It should be added that VBH_PRC.2 and VBH_PRC.3 are a share of this indicator, and that this indicator is a subset of VBH_WTI.1.
		Mailbox or Internet access with admin mode	This indicator applies to users using their admin account on a workstation.to access their own mailbox or Internet. This behaviour is particularly dangerous since malware (through attached pieces on email or drive-by download on Web browser) are far easier to install on the workstation in this case.
	Passwords	Weak passwords used	The required strength of passwords depends on the organization's security policy, but usable general recommendations in ISO/IEC 27002
		Passwords not changed	This indicators measures password not changed in due periodic time (case of changes not periodically imposed). Situations in which changes are not periodically imposed by accessed systems themselves remain fairly frequent within organizations (apart from Active Directory), the figure being around 25 % of the cases on average.
		Administrator passwords not changed	This indicator measures password not changed in due periodic time by an administrator in charge of an account used by automated applications and processes (case of changes not periodically imposed). Situations in which changes

			are not periodically imposed by accessed systems themselves remain fairly frequent within organizations (apart from Active Directory), the figure being around 25 % of the cases on average.
	Rights	Not compliant user rights granted illicitly by an administrator	This indicator measures the granting of not compliant user rights by an administrator outside any official procedure. This vulnerability may originate with an error, negligence or malice.
	Human weakness	Human weakness exploited by a spear phishing message meant to entice or appeal to do something possibly harmful to the organization	This vulnerability typically includes clicking on an Internet link or opening an attached document
		Human weakness exploited by exchanges meant to entice or appeal to tell some secrets to be used later	This vulnerability applies to discussions through on-line media leading to leakage of personal identifiable information (PII) or various business details to be used later (notably for identity usurpation)
VSW (existence of weaknesses in software that could be exploited and lead to security incidents.)	**Web applications software vulnerabilities**	Web applications software vulnerabilities	This indicator measures software vulnerabilities detected in Web applications running on externally accessible servers.
	OS software vulnerabilities regarding servers	OS software vulnerabilities regarding servers	These indicators measure software vulnerabilities detected in OS running on externally accessible servers.
	Web browsers software vulnerabilities	Web browsers software vulnerabilities	This indicator measures software vulnerabilities detected in Web browsers running on workstations.

VCF (existence of weaknesses in the configuration of IT devices that could be exploited and lead to security incidents.)	**Dangerous or illicit services**	Dangerous or illicit services on externally accessible servers	This indicator measures the presence of illicit and dangerous system services running on an externally accessible server.
	Logs	Insufficient size of the space allocated for logs	Such event could cause an overflow in case of quick series of unusual actions.
	Firewall	Weak firewall filtering rules	This indicator measures the gaps between the active firewall filtering rules and the security policy.
	Workstations	Workstation wrongly configured	This indicator measures the use of workstation with a disabled or lacking update AV and/or FW. The lack of update includes signature file older than x days (generally at least 6 days).
		Autorun feature enabled on workstations	This indicator measures the presence of Autorun feature enabled on workstations.
	User accounts	Access rights configuration not compliant with the security policy	This indicator measures access rights configuration that are not compliant with corporate security policy. This indicator is more reliable in case of existence of a central repository of user rights within organization (and of an IAM achievement)
		Not compliant access rights on logs	This indicator measures non-compliant access rights on logs in servers which are sensitive and/or subject to regulations. This situation representing a key weakness since the necessary high confidence in the produced logs has been reduced to nothing.

		Generic and shared administrator accounts	This indicator measures generic and shared administration accounts that are unnecessary or accounts that are necessary but without patronage. It concerns operating systems, databases and applications.
		Accounts without owners	This indicator measures accounts without owners that have not been erased. These are accounts that have no more assigned users (for example after internal transfer or departure of the users from organization).
		Inactive accounts	This indicator measures accounts inactive for at least 2 months that have not been disabled. These accounts are not used by their users due to prolonged but not definitive absence (long term illness, maternity, etc.), with the exclusion of messaging accounts (which should remain accessible to users from their home).
VTC(existence of weaknesses in the IT and physical architecture that could be exploited and lead to security incidents.)	**BKP**	Malfunction of server-hosted sensitive data safeguards	On servers hosting sensitive data with respect to availability, it concerns malfunctions of safeguards due to lack of periodic testing. This kind of event may be very serious since usually put trust is betrayed in a critical function.
	IDS	Full unavailability of IDS/IPS	Many causes are possible, including deliberate disconnection by a network administrator (to streamline operations or since IDS/IPS output is deemed too difficult to use), unwitting disconnection (error by a

			network administrator), breakdown, software malfunction, etc.
	Wi-Fi	Wi-Fi devices installed on the network without any official authorization	Many causes are possible, including for example local decisions for easier access of mobile users, rogue user behaviours or workstations configured as access points.
	Remote access points	Remote access points used to gain unauthorized access	This indicator is interesting to assess whether such accesses are localized (local areas, countries, etc.) or involve the whole organization or are increasing and spreading to whole organization.
	NRG	Devices or servers connected to the organization's network without being registered and managed	According to some convergent studies, this event may be at the origin of some 70 % of all security incidents associated to malice.
	Physical access control	Not operational physical access control means	This indicator includes access to protected internal areas. The 1st cause is the lack of effective control of users at software level. The 2nd cause is hardware breakdown of a component in the chain.
VOR(existence of weaknesses in the organization that could be exploited and lead to security incidents.)	**Discovery of attacks**	Discovery of attacks	This indicator measures stealthy security incidents difficult to detect. As most studies show, the time to discovery is often several months, time frame especially used to steal sensitive data. Incidents taken into account here are IEX_INT.3, IEX_MLW.3 and IEX_MLW.4. This indicator gives landmarks regarding what may be deemed

			excessive, i.e. with an assumption which is above one week.
	VNP	Excessive time of window of risk exposure	This indicator measures situations in which the time of the window of risk exposure exceeds the time limit expressed in security policy. The window of risks exposure is the period of time between the public disclosure of a software vulnerability and the actual and checked application of a patch that corresponds with the vulnerability's remediation (independently of the time needed for the vendor to provide the patch). This indicator only applies to workstations (OS, application software and browsers), and to critical vulnerabilities (as publicly determined via the CVSS scale) that require an action as quickly as possible.
		Rate of not patched systems	This indicator measures the rate of not patched systems for detected critical software vulnerabilities (see VOR_VNP.1 for criticality definition). Not patched systems to be taken into account are the ones which are not patched beyond the time limit defined in security policy. This indicator only applies to workstations (OS, application software and browsers).
		Rate of not reconfigured systems	This indicator measures the rate of not reconfigured systems for detected critical configuration vulnerabilities. Configuration vulnerabilities

			are either non-conformities relative to a level 3 security policy, or discrepancies relative to a state-of-the-art available within the profession (and that can correspond with a configuration master produced by a vendor and applied within the organization). This indicator only applies to workstations (OS, application software and browsers). Not reconfigured systems to be taken into account are the ones which are not reconfigured beyond the time limit defined in security policy.
	Reaction plans	Reaction plans launched without experience feedback	This indicator applies to plans for responding to incidents formalized in security policy launched without experience feedback.
		Reaction plans unsuccessfully launched	This indicator measures failure in the performance of plans, leading to non-recovery of incidents and to subsequent possible launch of an escalation procedure.
	Projects	Launch of new IT projects without information classification	This indicator measures the launch of new IT projects without information classification. Availability of a classification model and scheme within the organization would make easier this task.
		Launch of new specific IT projects without risk analysis	This indicator measures the launch of new specific IT projects without performing a full risk analysis.

		Launch of new IT projects of a standard type without identification of vulnerabilities and threats	This indicator measures the launch of new IT projects of a standard type without identification of vulnerabilities and threats and of related security measures. For these IT projects, potential implementation of a simplified risk analysis method or of pre-defined security profiles can be applied.
IMP(impact measurement)	**Cost**	Average cost to tackle a critical security incident	The average cost taken into account includes the following kinds of overhead: disruption to business operations (increased operating costs, etc.), fraud (money, etc.) and incident recovery costs (technical individual time, asset replacement, etc.). It does not include possible (generally very heavy) breach notification costs to customers and enforcement bodies (according to US and recently EU laws or regulations).
	Time	Average time of Websites downtime due to whole security incidents	Applies to all 4 classes, but main security incidents concerned are malfunctions or breakdowns (software or hardware), DoS or DDoS attacks and Website defacements.
		Average time of Websites downtime due to successful malicious attacks	This indicator is a subset of the previous one (IMP_TIM.1) focusing on 3 possible classes (IEX, IUS, IMD).

		Average time of Websites downtime due to malfunctions or unintentional security incidents	This indicator is a subset of IMP_TIM.1 focusing on one class (IMF).

Table 40 – MISP Information Security Indicators Class

xx. CSSA Taxonomies

sharing-class	Description
High_profile	Generated within the company during incident/case related investigations or forensic analysis or via malware reversing, validated by humans and highly contextualized.
Vetted	Generated within the company, validated by a human prior to sharing, data points have been contextualized (to a degree) e.g. IPs are related to C2 or drop site.
Unvetted	Generated within the company by automated means without human interaction e.g., by malware sandbox, honeypots, IDS, etc.

Table 41 - CSSA Sharing Class

origin	Description
Manual_investigation	Information gathered by an analyst/incident responder/forensic expert/etc.
Honeypot	Information coming out of honeypots.
Sandbox	Information coming out of sandboxes
Email	Information coming out of email infrastructure
3rd-party	Information from outside the company

origin	Description
Other	If none of the other origins applies.
Unknown	Origin of the data unknown

Table 42 - CSSA Origin Taxonomy

xxi. Europol Event Taxonomy

Europol-event	Description
infected-by-known-malware	System(s) infected by known malwareThe presence of any of the types of malware was detected in a system.
dissemination-malware-email	Dissemination of malware by email Malware attached to a message or email message containing link to malicious URL.
hosting-malware-webpage	Hosting of malware on web page
c&c-server-hosting	Hosting of malware on web page. Web page disseminating one or various types of malware.
worm-spreading	Replication and spreading of a worm. System infected by a worm trying to infect other systems.
connection-malware-port	Connection to (a) suspicious port(s) linked to specific malware. System attempting to gain access to a port normally linked to a specific type of malware.
connection-malware-system	Connection to (a) suspicious system(s) linked to specific malware. System attempting to gain access to an IP address or URL normally linked to a specific type of malware, e.g. C&C or a distribution page for components linked to a specific botnet.
flood	Flood of requests. Mass mailing of requests (network packets, emails, etc…) from one single source to a specific service, aimed at affecting its normal functioning.
exploit-tool-exhausting-resources	Exploit or tool aimed at exhausting resources (network, processing capacity, sessions, etc…) One single source

Europol-event	Description
	using specially designed software to affect the normal functioning of a specific service, by exploiting a vulnerability.
packet-flood	Packet flooding. Mass mailing of requests (network packets, emails, etc…) from various sources to a specific service, aimed at affecting its normal functioning.
exploit-framework-exhausting-resources	Exploit or tool distribution aimed at exhausting resources. Various sources using specially designed software to affect the normal functioning of a specific service, by exploiting a vulnerability.
vandalism	Logical and physical activities which – although they are not aimed at causing damage to information or at preventing its transmission among systems – have this effect.
disruption-data-transmission	Intentional disruption of data transmission and processing mechanisms. Logical and physical activities aimed at causing damage to information or at preventing its transmission among systems.
system-probe	Single system scan searching for open ports or services using these ports for responding.
network-scanning	Scanning a network aimed at identifying systems which are active in the same network.
dns-zone-transfer	Transfer of a specific DNS zone.
wiretapping	Logical or physical interception of communications.
dissemination-phishing-emails	Mass emailing aimed at collecting data for phishing purposes with regard to the victims.

Europol-event	Description
hosting-phishing-sites	Hosting web sites for phishing purposes.
aggregation-information-phishing-schemes	Collecting data obtained through phishing attacks on web pages, email accounts, etc…
exploit-attempt	Unsuccessful use of a tool exploiting a specific vulnerability of the system.
sql-injection-attempt	Unsuccessful attempt to manipulate or read the information of a database by using the SQL injection technique.
xss-attempt	Unsuccessful attempts to perform attacks by using cross-site scripting techniques.
file-inclusion-attempt	Unsuccessful attempt to include files in the system under attack by using file inclusion techniques.
brute-force-attempt	Unsuccessful login attempts by using sequential credentials for gaining access to the system.
password-cracking-attempt	Attempt to acquire access credentials by breaking the protective cryptographic keys.
dictionary-attack-attempt	Unsuccessful login attempts by using system access credentials previously loaded into a dictionary.
exploit	Use of a local or remote exploit. Successful use of a tool exploiting a specific vulnerability of the system.
sql-injection	Manipulation or reading of information contained in a database by using the SQL injection technique.
XSS	Attacks performed with the use of cross-site scripting techniques.
file-inclusion	Inclusion of files into a system under attack with the use of file inclusion techniques.

Europol-event	Description
control-system-bypass	Unauthorised access to a system or component by bypassing an access control system in place.
theft-access-credentials	Theft of access credentials. Unauthorised access to a system or component by using stolen access credentials.
unauthorized-access-system	Unauthorised access to a system or component.
unauthorized-access-information	Unauthorised access to a set of information.
data-exfiltration	Unauthorised access to and sharing of a specific set of information.
modification-information	Unauthorised changes to a specific set of information.
deletion-information	Unauthorised deleting of a specific set of information.
illegitimate-use-resources	Misuse or unauthorised use of resources. Use of institutional resources for purposes other than those intended.
illegitimate-use-name	Illegitimate use of the name of an institution or third party. Using the name of an institution without permission to do so.
email-flooding	Sending an unusually large quantity of email messages.
spam	Sending an unsolicited message. Sending an email message that was unsolicited or unwanted by the recipient.

Europol-event	Description
copyrighted-content	Distribution or sharing of copyright protected content. Distribution or sharing of content protected by copyright and related rights.
content-forbidden-by-law	Dissemination of content forbidden by law (publicly prosecuted offences). Distribution or sharing of illegal content such as child pornography, racism, xenophobia, etc…
unspecified	Other unspecified event. Other unlisted events.
undetermined	Field aimed at the classification of unprocessed events, which have remained undetermined from the beginning.

Table 43 - Europol Event Taxonomy

xxii. MS-Caro malware classification

Malware Type	description
Adware	Adware - Software that shows you extra promotions that you cannot control as you use your PC
Backdoor	A type of trojan that gives a malicious hacker access to and control of your PC
Behavior	A type of detection based on file actions that are often associated with malicious activity
BroswerModifier	A program than makes changes to your Internet browser without your permission
Constructor	A program that can be used to automatically create malware files
DDoS	When a number of PCs are made to access a website, network or server repeatedly within a given time period. The aim of the attack is to overload the target so that it crashes and can't respond
Dialer	A program that makes unauthorized telephone calls. These calls may be charged at a premium rate and cost you a lot of money
DoS	When a target PC or server is deliberately overloaded so that it doesn't work for any visitors anymore
Exploit	A piece of code that uses software vulnerabilities to access information on your PC or install malware
HackTool	A type of tool that can be used to allow and maintain unauthorized access to your PC
Joke	A program that pretends to do something malicious but actually doesn't actually do anything harmful. For example, some joke programs pretend to delete files or format disks
Misleading	The program that makes misleading or fraudulent claims about files, registry entries or other items on your PC
MonitoringTool	A commercial program that monitors what you do on your PC. This can include monitoring what keys you press; your email or instant messages; your voice or video conversations; and your

Malware Type	description
	banking details and passwords. It can also take screenshots as you use your PC
Program	Software that you may or may not want installed on your PC
Potentially Unwanted Applications	Characteristics of unwanted software can include depriving users of adequate choice or control over what the software does to the computer, preventing users from removing the software, or displaying advertisements without clearly identifying their source.
PWS	A type of malware that is used steal your personal information, such as user names and passwords. It often works along with a keylogger that collects and sends information about what keys you press and websites you visit to a malicious hacker
Ransom	A detection for malicious programs that seize control of the computer on which they are installed. This trojan usually locks the screen and prevents the user from using the computer. It usually displays an alert message.
RemoteAccess	A program that gives someone access to your PC from a remote location. This type of program is often installed by the computer owner
Rogue	Software that pretends to be an antivirus program but doesn't actually provide any security. This type of software usually gives you a lot of alerts about threats on your PC that don't exist. It also tries to convince you to pay for its services
SettingsModifier	A program that changes your PC settings
SoftwareBundler	A program that installs unwanted software on your PC at the same time as the software you are trying to install, without adequate consent
Spammer	A trojan that sends large numbers of spam emails. It may also describe the person or business responsible for sending spam
Spoofer	A type of trojan that makes fake emails that look like they are from a legitimate source
Spyware	A program that collects your personal information, such as your browsing history, and uses it without adequate consent
Tool	A type of software that may have a legitimate purpose, but which may also be abused by malware authors

Malware Type	description
Trojan	A trojan is a program that tries to look innocent, but is actually a malicious application. Unlike a virus or a worm , a trojan doesn't spread by itself. Instead they try to look innocent to convince you to download and install them. Once installed, a trojan can steal your personal information, download more malware, or give a malicious hacker access to your PC
TrojanClicker	A type of trojan that can use your PC to click on websites or applications. They are usually used to make money for a malicious hacker by clicking on online advertisements and making it look like the website gets more traffic than it does. They can also be used to skew online polls, install programs on your PC, or make unwanted software appear more popular than it is
TrojanDownloader	A type of trojan that installs other malicious files, including malware, onto your PC. It can download the files from a remote PC or install them directly from a copy that is included in its file.
TrojanDropper	A type of trojan that installs other malicious files, including malware, onto your PC. It can download the files from a remote PC or install them directly from a copy that is included in its file.
TrojanNotifier	A type of trojan that sends information about your PC to a malicious hacker. It is similar to a password stealer
TrojanProxy	A type of trojan that installs a proxy server on your PC. The server can be configured so that when you use the Internet, any requests you make are sent through a server controlled by a malicious hacker
TrojanSpy	A program that collects your personal information, such as your browsing history, and uses it without adequate consent.
VirTool	A detection that is used mostly for malware components, or tools used for malware-related actions, such as rootkits.
Virus	A type of malware. Viruses spread on their own by attaching their code to other programs or copying themselves across systems and networks.
Worm	A type of malware that spreads to other PCs. Worms may spread using one or more of the following methods: Email programs, Instant messaging programs, File-sharing programs, Social networking sites, Network shares, Removable drives with Autorun enabled, Software vulnerabilities

Table 44 - MS Caro – Classification by malware type

Platform	description
AndroidOS	Android operating system
DOS	MS-DOS platform
EPOC	Psion devices
FreeBSD	FreeBSD platform
iPhoneOS	iPhone operating system
Linux	Linux platform
MacOS	MAC 9.x platform or earlier
MacOS_X	MacOS X or later
OS2	OS2 platform
Palm	Palm operating system
Solaris	System V-based Unix platforms
SunOS	Unix platforms 4.1.3 or earlier
SymbOS	Symbian operatings system
Unix	General Unix platforms

Platform	description
Win16	Win16 (3.1) platform
Win2K	Windows 2000 platform
Win32	Windows 32-bit platform
Win64	Windows 64-bit platform
Win95	Windows 95, 98 and ME platforms
Win98	Windows 98 platform only
WinCE	Windows CE platform
WinNT	WinNT
ABAP	Advanced Business Application Programming scripts
ALisp	ALisp scripts
AmiPro	AmiPro script
ANSI	American National Standards Institute scripts
AppleScript	compiled Apple scripts

Platform	description
ASP	Active Server Pages scripts
AutoIt	AutoIT scripts
BAS	Basic scripts
BAT	Basic scripts
CorelScript	Corelscript scripts
HTA	HTML Application scripts
HTML	HTML Application scripts
INF	Install scripts
IRC	mIRC/pIRC scripts
Java	Java binaries (classes)
JS	Javascript scripts
LOGO	LOGO scripts
MPB	MapBasic scripts
MSH	Monad shell scripts

Platform	description
MSIL	
Perl	Perl scripts
PHP	Hypertext Preprocessor scripts
Python	Python scripts
SAP	SAP platform scripts
SH	Shell scripts
VBA	Visual Basic for Applications scripts
VBS	Visual Basic scripts
WinBAT	Winbatch scripts
WinHlp	Windows Help scripts
WinREG	Windows registry scripts
A97M	Access 97, 2000, XP, 2003, 2007, and 2010 macros
HE	macro scripting

Platform	description
O97M	Office 97, 2000, XP, 2003, 2007, and 2010 macros - those that affect Word, Excel, and Powerpoint
PP97M	PowerPoint 97, 2000, XP, 2003, 2007, and 2010 macros
V5M	Visio5 macros
W1M	Word1Macro
W2M	Word2Macro
W97M	Word 97, 2000, XP, 2003, 2007, and 2010 macros
WM	Word 95 macros
X97M	Excel 97, 2000, XP, 2003, 2007, and 2010 macros
XF	Excel formulas
XM	Excel 95 macros
ASX	XML metafile of Windows Media .asf files
HC	HyperCard Apple scripts
MIME	MIME packets
Netware	Novell Netware files

Platform	description
QT	Quicktime files
SB	StarBasic (Staroffice XML) files
SWF	Shockwave Flash files
TSQL	MS SQL server files
XML	XML files

Table 45 - MS Caro (platform types)

Malware Family	Description
Zlob	2008 - A family of trojans that often pose as downloadable media codecs. When installed, Win32/Zlob displays frequent pop-up advertisements for rogue security software
Vundo	2008 - A multiplecomponent family of programs that deliver pop-up advertisements and may download and execute arbitrary files. Vundo is often installed as a browser helper object (BHO) without a user's consent
Virtumonde	2008 - multi-component malware family that displays pop-up advertisements for rogue security software
Bancos	2008 - A data-stealing trojan that captures online banking credentials and relays them to the attacker. Most variants target customers of Brazilian banks.
Cutwail	2008 - A trojan that downloads and executes arbitrary files, usually to send spam. Win32/Cutwail has also been observed to transmit Win32/Newacc
Oderoor	2008 - a backdoor trojan that allows an attacker access and control of the compromised computer. This trojan may connect with remote web sites and SMTP servers.

Malware Family	Description
Newacc	2008 - An attacker tool that automatically registers new e-mail accounts on Hotmail, AOL, Gmail, Lycos and other account service providers, using a Web service to decode CAPTCHA protection.
Captiya	2008 - A trojan that transmits CAPTCHA images to a botnet, in what is believed to be an effort to improve the botnet's ability to detect characters and break CAPTCHAs more successfully
Taterf	2008 - A family of worms that spread through mapped drives in order to steal login and account details for popular online games.
Frethog	2008 - A large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games
Tilcun	2008 - A family of trojans that steals online game passwords and sends this captured data to remote sites.
Ceekat	2008 - A collection of trojans that steal information such as passwords for online games, usually by reading information directly from running processes in memory. Different variants target different processes.
Corripio	2008 - a loosely-related family of trojans that attempt to steal passwords for popular online games. Detections containing the name Win32/Corripio are generic, and hence may be reported for a large number of different malicious password-stealing trojans that are otherwise behaviorally dissimilar.
Zuten	2008 - A family of malware that steals information from online games.
Lolyda	2008 - A family of trojans that sends account information from popular online games to a remote server. They may also download and execute arbitrary files.
Storark	2008 - A family of trojans that steals online game passwords and sends this captured data to remote sites.
Renos	2008 - A family of trojan downloaders that installs rogue security software.
ZangoSearchAssistant	2008 - Adware that monitors the user's Web-browsing activity and displays pop-up advertisements related to the Internet sites the user is viewing.
ZangoShoppingReports	2008 - Adware that displays targeted advertising to affected users while they browse the Internet, based on search terms entered into search engines.
FakeXPA	2008 - A rogue security software family that claims to scan for malware and then demands that the user pay to remove nonexistent threats. Some variants unlawfully use Microsoft logos and trademarks.

Malware Family	Description
FakeSecSen	2008 - A rogue security software family that claims to scan for malware and then demands that the user pay to remove non-existent threats. It appears to be based on Win32/SpySheriff
Hotbar	2008 - Adware that displays a dynamic toolbar and targeted pop-up ads based on its monitoring of Web-browsing activity.
Agent	2008 - A generic detection for a number of trojans that may perform different malicious functions. The behaviors exhibited by this family are highly variable
Wimad	2008 - A detection for malicious Windows Media files that can be used to encourage users to download and execute arbitrary files on an affected machine.
BaiduSobar	2008 - A Chinese language Web browser toolbar that delivers pop-up and contextual advertisements, blocks certain other advertisements, and changes the Internet Explorer search page
VB	2008 - A detection for various threats written in the Visual Basic programming language.
Antivirus2008	2008 - A program that displays misleading security alerts in order to convince users to purchase rogue security software. It may be installed by Win32/Renos or manually by a computer user.
Playmp3z	2008 - An adware family that may display advertisements in connection with the use of a 'free music player' from the site 'PlayMP3z.biz.'
Tibs	2008 - a family of Trojans that may download and run other malicious software or may steal user data and send it to the attacker via HTTP POST or email. The Win32/Tibs family frequently downloads Trojans belonging to the Win32/Harnig and Win32/Passalert families, both of which are families of Trojan downloaders which may in turn download and run other malicious software
SeekmoSearchAssistant	2008 - Adware that displays targeted search results and pop-up advertisements based on terms that the user enters for Web searches. The pop-up advertisements may include adult content.
RJump	2008 - a worm that attempts to spread by copying itself to newly attached media (such as USB memory devices or network drives). It also contains backdoor functionality that allows an attacker unauthorized access to an affected computer
SpywareSecure	2008 - A program that displays misleading warning messages in order to convince users to purchase a product that removes spyware

Malware Family	Description
Winfixer	2008 - A program that locates various registry entries, Windows prefetch content, and other types of data, identifies them as privacy violations, and urges the user to purchase the product to fix them.
C2Lop	2008 - a trojan that modifies Web browser settings, adds Web browser bookmarks to advertisements, updates itself and delivers pop-up and contextual advertisements.
Matcash	2008 - a multicomponent family of trojans that downloads and executes arbitrary files. Some variants of this family may install a toolbar. observed to use the Win32/Slenfbot worm as a means of distribution.
Horst	2008 - CAPTCHA Breaker typically delivered through an executable application that masquerades as an illegal software crack or key generator
Slenfbot	2008 - A family of worms that can spread via instant messaging programs and may spread via removable drives. They also contain backdoor functionality that allows unauthorized access to an affected machine. This worm does not spread automatically upon installation but must be ordered to spread by a remote attacker.
Rustock	2008 - A multicomponent family of rootkitenabled backdoor trojans, developed to aid in the distribution of spam. Recent variants appear to be associated with the incidence of rogue security programs.
Gimmiv	2008 - a family of trojans that are sometimes installed by exploits of a vulnerability documented in Microsoft Security Bulletin MS08-067.
Yektel	2008 - A family of trojans that display fake warnings of spyware or malware in an attempt to lure the user into installing or paying money to register rogue security products such as Win32/FakeXPA.
Roron	2008 - This virus spreads by attaching its code to other files on your PC or network. Some of the infected programs might no longer run correctly. Attempts to send personal information to a remote address. It may spread via e-mail, network shares, or peer-to-peer file sharing.
Swif	2008 - A trojan that exploits a vulnerability in Adobe Flash Player to download malicious files. Adobe has published security bulletin APSB08-11 addressing the vulnerability.
Mult	2008 - A group of threats, written in JavaScript, that attempt to exploit multiple vulnerabilities on affected computers in order to download, execute or otherwise run arbitrary code. The malicious JavaScript may be hosted on compromised or malicious websites, embedded in specially crafted PDF files, or could be called by other malicious scripts.
Wukill	2008 - a family of mass-mailing e-mail and network worms. The Win32/Wukill worm spreads to root directories on certain local and mapped drives. The

Malware Family	Description
	worm also spreads by sending a copy of itself as an attachment to e-mail addresses found on the infected computer.
Objsnapt	2008 - A detection for a Javascript file that exploits a known vulnerability in the Microsoft Access Snapshot Viewer ActiveX Control.
Redirector	2008 - The threat is a piece of JavaScript code that is inserted on bad or hacked websites. It can direct your browser to a website you don't want to go to. You might see the detection for this threat if you visit a bad or hacked website, or if you open an email message.
Xilos	2008 - a detection for a proof-of-concept JavaScript obfuscation technique, which was originally published in 2002 in the sixth issue of 29A, an early online magazine for virus creators
Decdec	2008 - A detection for certain malicious JavaScript code injected in HTML pages. The virus will execute on user computers that visit compromised websites.
BearShare	2008 - A P2P file-sharing client that uses the decentralized Gnutella network. Free versions of BearShare have come bundled with advertising supported and other potentially unwanted software.
BitAccelerator	2008 - A program that redirects Web search results to other Web sites and may display various advertisements to users while browsing Web sites.
Blubtool	2008 - An Internet browser search toolbar that may be installed by other third-party software, such as a peer-to-peer file sharing application. It may modify Internet explorer search settings and display unwanted advertisements.
RServer	2008 - Commercial remote administration software that can be used to control a computer. These programs are typically installed by the computer owner or administrator and should only be removed if unexpected
UltraVNC	2008 - A remote access program that can be used to control a computer. This program is typically installed by the computer owner or administrator and should only be removed if unexpected.
GhostRadmin	2008 - A remote administration tool that can be used to control a computer. These programs are typically installed by the computer owner or administrator and should only be removed if unexpected
TightVNC	2008 - A remote control program that allows full control of the computer. These programs are typically installed by the computer owner or administrator and should only be removed if unexpected
DameWareMiniRemoteControl	2008 - A detection for the DameWare Mini Remote-Control tools. This program was detected by definitions prior to 1.147.1889.0 as it violated the

Malware Family	Description
	guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors. Microsoft has released definition 1.147.1889.0 which no longer detects this program.
SeekmoSearchAssistant_Repack	2008 - A detection that is triggered by modified (that is, edited and re-packed) remote control programs based on DameWare Mini Remote Control, a commercial software product
Nbar	2008 - A program that may display advertisements and redirect user searches to a certain website. It may also download malicious or unwanted content into the system without user consent.
Chir	2008 - A family with a worm component and a virus component. The worm component spreads by email and by exploiting a vulnerability addressed by Microsoft Security Bulletin MS01-020. The virus component may infect .exe, .scr, and HTML files.
Sality	2008 - A family of polymorphic file infectors that target executable files with the extensions .scr or .exe. They may execute a damaging payload that deletes files with certain extensions and terminates security-related processes and services.
Obfuscator	2008 - A detection for programs that use a combination of obfuscation techniques to hinder analysis or detection by antivirus scanners
ByteVerify	2008 - a detection of malicious code that attempts to exploit a vulnerability in the Microsoft Virtual Machine (VM). This flaw enables attackers to execute arbitrary code on a user's machine such as writing, downloading and executing additional malware. This vulnerability is addressed by update MS03-011, released in 2003.
Autorun	2008 - A family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.
Hamweq	2008 - A worm that spreads through removable drives, such as USB memory sticks. It may contain an IRC-based backdoor enabling the computer to be controlled remotely by an attacker
Brontok	2008 - a family of mass-mailing e-mail worms. The worm spreads by sending a copy of itself as an e-mail attachment to e-mail addresses that it gathers from files on the infected computer. It can also copy itself to USB and pen drives. Win32/Brontok can disable antivirus and security software, immediately terminate certain applications, and cause Windows to restart immediately when certain applications run. The worm may also conduct denial of service (DoS) attacks against certain Web sites

Malware Family	Description
SpywareProtect	2008 - A rogue security software family that may falsely claim that the user's computer is infected and encourages the user to buy a product for cleaning the alleged malware from the computer
Cbeplay	2008 - A trojan that may upload computer operating system details to a remote Web site, download additional malware, and terminate debugging utilities
InternetAntivirus	2008 - A program that displays false and misleading malware alerts to convince users to purchase rogue security software. This program also displays a fake Windows Security Center message
Nuwar	2008 - A family of trojan droppers that install a distributed P2P downloader trojan. This downloader trojan in turn downloads an e-mail worm component.
Rbot	2008 - A family of backdoor trojans that allows attackers to control the computer through an IRC channel
IRCbot	2008 - A large family of backdoor trojans that drops malicious software and connects to IRC servers via a backdoor to receive commands from attackers.
SkeemoSearchAssistant	2008 - A program that displays targeted search results and pop-up advertisements based on terms that the user enters for Web searches. The pop-up advertisements may include adult content
RealVNC	2008 - A management tool that allows a computer to be controlled remotely. It can be installed for legitimate purposes but can also be installed from a remote location by an attacker.
MoneyTree	2008 - A family of software that provides the ability to search for adult content on local disk. It may also install other potentially unwanted software, such as programs that display pop-up ads.
Tracur	2008 - A trojan that downloads and executes arbitrary files. It is sometimes distributed by ASX/Wimad.
Meredrop	2008 - This is a generic detection for trojans that install and run malware on your PC. These trojans have been deliberately created in a complex way to hide their purpose and make them difficult to analyze.
Banker	2008 - A family of data-stealing trojans that captures banking credentials such as account numbers and passwords from computer users and relays them to the attacker. Most variants target customers of Brazilian banks; some variants target customers of other banks.
Ldpinch	2008 - A family of data-stealing trojans that captures banking credentials such as account numbers and passwords from computer users and relays them to the attacker. Most variants target customers of Brazilian banks; some variants target customers of other banks.

Malware Family	Description
Advantage	2008 - a family of adware that displays pop-up advertisements and contacts a remote server to download updates
Parite	2008 - a family of polymorphic file infectors that targets computers running Microsoft Windows. The virus infects .exe and .scr executable files on the local file system and on writeable network shares. In turn, the infected executable files perform operations that cause other .exe and .scr files to become infected.
PossibleHostsFileHijack	2008 - an indicator that the computer's HOSTS file may have been modified by malicious or potentially unwanted software
Alureon	2008 - A data-stealing trojan that gathers confidential information such as user names, passwords, and credit card data from incoming and outgoing Internet traffic. It may also download malicious data and modify DNS settings.
PowerRegScheduler	2008 - This program was detected by definitions prior to 1.159.567.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors. Microsoft has released definition 1.159.567.0 which no longer detects this program.
APSB08-11	2008 - A trojan that attempts to exploit a vulnerability in Adobe Flash Player. In the wild, this trojan has been used to download and execute arbitrary files, including other malware.
ConHook	2008 - A family of Trojans that installs themselves as Browser Helper Objects (BHOs) and connects to the Internet without user consent. They also terminate specific security services and download additional malware to the computer.
Starware	2008 - This program was detected by definitions prior to 1.159.567.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors. Microsoft has released definition 1.159.567.0 which no longer detects this program.
WinSpywareProtect	2008 - A program that may falsely claim that the user's system is infected and encourages the user to buy a promoted product for cleaning the alleged malware from the computer.
MessengerSkinner	2008 - A program, that may be distributed in the form of a freeware application, that displays advertisements, downloads additional files, and uses stealth to hide its presence
Skintrim	2008 - A trojan that downloads and executes arbitrary files. It may be distributed by as a Microsoft Office Outlook addon used to display emoticons or other animated icons within e-mail messages.

Malware Family	Description
AdRotator	2008 - delivers advertisements, and as the name suggests, rotates advertisements among sponsors. AdRotator contacts remote Web sites in order to deliver updated content. This application also displays fake error messages that encourage users to download and install additional applications.
Wintrim	2008 - A family of trojans that display pop-up advertisements depending on the user's keywords and browsing history. Its variants can monitor the user's activities, download applications, and send system information back to a remote server.
Busky	2008 - A family of Trojans that monitor and redirect Internet traffic, gather system information and download unwanted software such as Win32/Renos and Win32/SpySheriff. Win32/Busky may be installed by a Web browser exploit or other vulnerability when visiting a malicious Web site.
WhenU	2008 - This program was detected by definitions prior to 1.173.303.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.
Mobis	2008 - This program was detected by definitions prior to 1.175.2037.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.
Sogou	2008 - Detected by definitions prior to 1.155.995.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors. Microsoft has released definition 1.155.995.0 which no longer detects this program.
Sdbot	2008 - A family of backdoor trojans that allows attackers to control infected computers. After a computer is infected, the trojan connects to an internet relay chat (IRC) server and joins a channel to receive commands from attackers.
DelfInject	2008 - This threat can download and run files on your PC.
Vapsup	2008 - This threat can perform a number of actions of a malicious hacker's choice on your PC.
BrowsingEnhancer	2008 - This program was detected by definitions prior to 1.175.1834.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.
Jeefo	2008 - virus infects executable files, such as files with a .exe extension. When an infected file runs, the virus tries to run the original content of the file while

Malware Family	Description
	it infects other executable files on your PC. This threat might have got on your PC if you inserted a removable disk or accessed a network connection that was infected.
Sezon	2008 - An adware that redirects web browsing to advertising or search sites.
RuPass	2008 - a DLL component which may be utilized by adware or malicious programs in order to monitor an affected user's Internet usage and to capture sensitive information. Win32/RuPass has been distributed as a 420,352-byte DLL file, with the file name 'ConnectionServices.dll'.
OneStepSearch	2008 - Modifies the user's browser to deliver targeted advertisements when the user enters search keywords. It may also replace or override web browser error pages that would otherwise be displayed when unresolvable web addresses are entered into the browser's address bar.
GameVance	2008 - Software that displays advertisements and tracks anonymous usage information in exchange for a free online gaming experience at the Web address 'gamevance.com.'
E404	2008 - is a browser helper object (BHO) that takes advantage of invalid or mistyped URLs entered in the address bar by redirecting the browser to Web sites containing adware
Mirar	2008 - This program was detected by definitions prior to 1.175.2037.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.
Fotomoto	2008 - A Trojan that lowers security settings, delivers advertisements, and sends system and network configuration details to a remote Web site.
Ardamax	2008 - The tool can capture your activity on your PC (such as the keys you press when typing in passwords) and might send this information to a hacker.
Hupigon	2008 - A family of trojans that uses a dropper to install one or more backdoor files and sometimes installs a password stealer or other malicious programs.
CNNIC	2008 - enables Chinese keyword searching in Internet Explorer and adds support for other applications to use Chinese domain names that registered with CNNIC. Also contains a kernel driver that protects its files and registry settings from being modified or deleted
MotePro	2008 - May display advertisement pop-ups and download programs from predefined Web sites. When installed, Win32/MotePro runs as a Web Browser Helper Object (BHO).
CnsMin	2008 - Installs a browser helper object (BHO) that redirects Internet Explorer searches to a Chinese search portal. CnsMin may be installed without

Malware Family	Description
	adequate user consent. It may prevent its files from being removed or restore files that have been previously removed.
BaiduIebar	2008 - A detection for an address line search tool. This program was detected by definitions prior to 1.153.956.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors. Microsoft has released definition 1.153.956.0 which no longer detects this program.
Ejik	2008 - This program was detected by definitions prior to 1.175.1915.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.
AlibabaIEToolBar	2008 - This program was detected by definitions prior to 1.175.1834.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.
BDPlugin	2008 - a DLL file which is usually introduced to an affected system as a component of BrowserModifier:Win32/BaiduSobar. It may display unwanted pop-ups and advertisements on the affected system.
Adialer	2008 - A trojan dialer program that connects to a premium number or attempts to connect to adult websites via particular phone numbers without your permission, connects to remote hosts without user consent.
EGroupSexDial	2008 - A dialer program that may attempt to dial a premium number, thus possibly resulting in international phone charges for the user.
Zonebac	2008 - A family of backdoor Trojans that allows a remote attacker to download and run arbitrary programs, and which may upload computer configuration information and other potentially sensitive data to remote Web sites.
Antinny	2008 - A family of worms that targets certain versions of Microsoft Windows. The worm spreads using a Japanese peer-to-peer file-sharing application named Winny. The worm creates a copy of itself with a deceptive file name in the Winny upload folder so that it can be downloaded by other Winny users.
RewardNetwork	2008 - A program that monitors an affected user's Internet usage and reports this usage to a remote server. Win32/RewardNetwork may be visible as an Internet Explorer toolbar.
Virut	2008 - A family of file infecting viruses that target and infect .exe and .scr files accessed on infected systems. Win32/Virut also opens a backdoor by connecting to an IRC server

Malware Family	Description
Allaple	2008 - A multi-threaded, polymorphic network worm capable of spreading to other computers connected to a local area network (LAN) and performing denial-of-service (DoS) attacks against targeted remote Web sites.
VKit_DA	2008 - This virus spreads by attaching its code to other files on your PC or network. Some of the infected programs might no longer run correctly.
Small	2008 - A generic detection for a variety of threats.
Netsky	2008 - A mass-mailing worm that spreads by e-mailing itself to addresses found on an infected computer. Some variants contain a backdoor component and perform DoS attacks.
Luder	2008 - A virus that spreads by infecting executable files, by inserting itself into .RAR archive files, and by sending a copy of itself as an attachment to e-mail addresses found on the infected computer. This virus has a date-activated, file damaging payload, and may connect to a remote server and accept commands from an attacker.
IframeRef	2008 - A generic detection for specially formed IFrame tags that point to remote websites that contain malicious content.
Lovelorn	2008 - This threat is classified as a mass-mailing worm. A mass mailing email worm is self-contained malicious code that propagates by sending itself through e-mail. Typically, a mass mailing email worm uses its own SMTP engine to send itself, thus copies of the sent worm will not appear in the infected user's outgoing or sent email folders. Technical details are currently not available.
Cekar	2008 - This threat downloads and installs other programs, including other malware, onto your PC without your consent.
Dialsnif	2008 - This threat can perform a number of actions of a malicious hacker's choice on your PC.
Conficker	2008 - A worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products and downloads arbitrary files.
LoveLetter	2009 - A family of mass-mailing worms that targets computers running certain versions of Windows. It can spread as an e-mail attachment and through an Internet Relay Chat (IRC) channel. The worm can download, overwrite, delete, infect, and run files on the infected computer.
VBSWGbased	2009 - A generic detection for VBScript code that is known to be automatically generated by a particular malware tool.

Malware Family	Description
Slammer	2009 - A memory resident worm that spreads through a vulnerability present in computers running either MSDE 2000 or SQL Server that have not applied Microsoft Security Bulletin MS02-039.
Msblast	2009 - A family of network worms that exploit a vulnerability addressed by security bulletin MS03-039. The worm may attempt Denial of Service (DoS) attacks on some server sites or create a backdoor on the infected system
Sasser	2009 - A family of network worms that exploit a vulnerability fixed by security bulletin MS04-011. The worm spreads by randomly scanning IP addresses for vulnerable machines and infecting any that are found
Nimda	2009 - A family of worms that spread by exploiting a vulnerability addressed by Microsoft Security Bulletin MS01-020. The worm compromises security by sharing the C drive and creating a Guest account with administrator permissions.
Mydoom	2009 - A family of massmailing worms that spread through e-mail. Some variants also spread through P2P networks. It acts as a backdoor trojan and can sometimes be used to launch DoS attacks against specific Web sites
Bagle	2009 - A worm that spreads by e-mailing itself to addresses found on an infected computer. Some variants also spread through peer-to-peer (P2P) networks. Bagle acts as a backdoor trojan and can be used to distribute other malicious software.
Winwebsec	2009 - A family of rogue security software programs that have been distributed with several different names. The user interface varies to reflect each variant's individual branding
Koobface	2009 - A multicomponent family of malware used to compromise computers and use them to perform various malicious tasks. It spreads through the internal messaging systems of popular social networking sites
Pdfjsc	2009 - a family of specially crafted PDF files that exploits vulnerabilities in Adobe Acrobat and Adobe Reader. The files contain malicious JavaScript that executes when opened with a vulnerable program.
Pointfree	2009 - a browser modifier that redirects users when invalid Web site addresses or search terms are entered in the Windows Internet Explorer address bar
Chadem	2009 - A trojan that steals password details from an infected computer by monitoring network traffic associated with FTP connections.
FakeIA	2009 - A rogue security software family that impersonates the Windows Security Center. It may display product names or logos in an apparently unlawful attempt to impersonate Microsoft products

Malware Family	Description
Waledac	2009 - A trojan that is used to send spam. It also has the ability to download and execute arbitrary files, harvest e-mail addresses from the local machine, perform denial-of-service attacks, proxy network traffic, and sniff passwords
Provis	2009 - This threat can perform a number of actions of a malicious hacker's choice on your PC.
Prolaco	2009 - A family of worms that spreads via email, removable drives, Peer-to-Peer (P2P) and network shares. This worm may also drop and execute other malware.
Mywife	2009 - A mass-mailing network worm that targets certain versions of Microsoft Windows. The worm spreads through e-mail attachments and writeable network shares. It is designed to corrupt the content of specific files on the third day of every month.
Melissa	2009 - A macro worm that spreads via e-mail and by infecting Word documents and templates. It is designed to work in Word 97 and Word 2000, and it uses Outlook to reach new targets through e-mail
Rochap	2009 - A family of multicomponent trojans that download and execute additional malicious files. While downloading, some variants display a video from the Web site 'youtube.com' presumably to distract the user
Gamania	2009 - A family of trojans that steals online game passwords and sends them to remote sites.
Mabezat	2009 - a polymorphic virus that infects Windows executable files. Apart from spreading through file infection, it also attempts to spread through e-mail attachments, network shares, removable drives and by CD-burning. It also contains a date-based payload that encrypts files with particular extensions.
Helpud	2009 - A family of trojans that steals login information for popular online games. The gathered information is then sent to remote websites.
PrivacyCenter	2009 - a family of programs that claims to scan for malware and displays fake warnings of 'malicious programs and viruses'. They then inform the user that they need to pay money to register the software in order to remove these non-existent threats.
FakeRean	2009 - This family of rogue security programs pretend to scan your PC for malware, and often report lots of infections. The program will say you have to pay for it before it can fully clean your PC. However, the program hasn't really detected any malware at all and isn't really an antivirus or antimalware scanner. It just looks like one, so you'll send money to the people who made the program. Some of these programs use product names or logos that unlawfully impersonate Microsoft products.

Malware Family	Description
Bredolab	2009 - A downloader that can access and execute arbitrary files from a remote host. Bredolab has been observed to download several other malware families to infected computers
Rugzip	2009 - A trojan that downloads other malware from predefined Web sites. Rugzip may itself be installed by other malware. Once it has performed its malicious routines, it deletes itself to avoid detection.
Fakespypro	2009 - A rogue security family that falsely claims that the affected computer is infected with malware and encourages the user to buy a promoted product it claims will clean the computer.
Buzuz	2009 - A trojan that downloads malware known as 'SpywareIsolator' a rogue security software program.
PoisonIvy	2009 - A family of backdoor trojans that allow unauthorized access to and control of an affected machine. Poisonivy attempts to hide by injecting itself into other processes
AgentBypass	2009 - A detection for files that attempt to inject possibly malicious code into the explorer.exe process.
Enfal	2009 - This threat can perform a number of actions of a malicious hacker's choice on your PC.
SystemHijack	2009 - A generic detection that uses advanced heuristics in the Microsoft Antivirus engine to detect malware that displays particular types of malicious behavior.
ProcInject	2009 - This threat can perform a number of actions of a malicious hacker's choice on your PC.
Malres	2009 - A trojan that drops another malware, detected as Virtool:WinNT/Malres.A, into the system.
Kirpich	2009 - a trojan that drops malicious code into the system. It also infects two system files; the infected files are detected as Virus:Win32/Kirpich.A, in the system. This does not constitute virus behavior for the trojan as it does not infect any other files and therefore does not have any conventional replication routines. TrojanDropper:Win32/Kirpich.A also disables Data Execution Protection and steals specific system information.
Malagent	2009 - A generic detection for a variety of threats.
Bumat	2009 - A generic detection for a variety of threats.
Bifrose	2009 - A backdoor trojan that allows a remote attacker to access the compromised computer and injects its processes into the Windows shell and Internet Explorer.

Malware Family	Description
Ripinip	2009 - This threat can give a hacker unauthorized access and control of your PC.
Riler	2009 - This threat can perform a number of actions of a malicious hacker's choice on your PC.
Farfli	2009 - A trojan that drops various files detected as malware into a system. It also has backdoor capabilities that allow it to contact a remote attacker and wait for instructions.
PcClient	2009 - A backdoor trojan family with several components including a key logger, backdoor, and a rootkit.
Veden	2009 - A name used for backdoor trojan detections that have been added to Microsoft signatures after advanced automated analysis.
Banload	2009 - A family of trojans that download other malware. Banload usually downloads Win32/Banker, which steals banking credentials and other sensitive data and sends it back to a remote attacker.
Microjoin	2009 - a tool that is used to deploy malware without being detected. It is used to bundle multiple files, consisting of a clean file and malware files, into a single executable.
Killav	2009 - a trojan that terminates a large number of security-related processes, including those for antivirus, monitoring, or debugging tools, and may install certain exploits for the vulnerability addressed by Microsoft Security Bulletin MS08-067
Cinmus	2009 - This threat can perform a number of actions of a malicious hacker's choice on your PC.
MessengerPlus	2009 - A non-Microsoft add-on for Microsoft's Windows Live Messenger, called Messenger Plus!. It comes with an optional sponsor program installation, detected as Spyware:Win32/C2Lop.
Haxdoor	2009 - a backdoor trojan that allows remote control of the machine over the Internet. The trojan is rootkit-enabled, allowing it to hide processes and files related to the threat. Haxdoor lowers security settings on the computer and gathers user and system information to send to a third party
Nieguide	2009 - a detection for a DLL file that connects to a Web site and may display advertisements or download other programs
Ithink	2009 - displays pop-up advertisements; it is usually bundled with other applications
Pointad	2009 - This program was detected by definitions prior to 1.175.2145.0 as it violated the guidelines by which Microsoft identified unwanted software.

Malware Family	Description
	Based on analysis using current guidelines, the program does not have unwanted behaviors.
Webdir	2009 - A Web Browser Helper Object (BHO) used to collect user information and display targeted advertisings using Internet Explorer browser. Webdir attempts to modify certain visited urls to include affiliate IDs.
Microbillsys	2009 - a program that processes payments made to a billing Web site. It is considered potentially unwanted software because it cannot be removed from the Add/Remove Programs list in Control Panel; rather, a user requires an 'uninstall code' before the program can be removed.
Kerlofost	2009 - a browser helper object (BHO) that may modify browsing behavior; redirect searches; report user statistics, behavior, and searches back to a remote server; and display pop-up advertisements.
Zwangi	2009 - A program that runs as a service in the background and modifies Web browser settings to visit a particular Web site
DoubleD	2009 - an adware program that displays pop-up advertising, runs at each system start and is installed as an Internet Explorer toolbar.
ShopAtHome	2009 - A browser redirector that monitors Web-browsing behavior and online purchases. It claims to track points for ShopAtHome rebates when the user buys products directly from affiliated merchant Web sites.
FakeVimes	2009 - a downloading component of Win32/FakeVimes - a family of programs that claims to scan for malware and displays fake warnings of 'malicious programs and viruses'. They then inform the user that they need to pay money to register the software in order to remove these non-existent threats.
FakeCog	2009 - This threat claims to scan your PC for malware and then shows you fake warnings. They try to convince you to pay to register the software to remove the non-existent threats.
FakeAdPro	2009 - a program that may display false and misleading alerts regarding errors and malware to entice users to purchase it.
FakeSmoke	2009 - a family of trojans consisting of a fake Security Center interface and a fake antivirus program.
FakeBye	2009 - A rogue security software family that uses a Korean-language user interface.
Hiloti	2009 - a generic detection for a trojan that interferes with an affected user's browsing habits and downloads and executes arbitrary files.
Tikayb	2009 - A trojan that attempts to establish a secure network connection to various Web sites without the user's consent.

Malware Family	Description
Ursnif	2009 - A family of trojans that steals sensitive information from an affected computer
Rimecud	2009 - A family of worms with multiple components that spreads via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system
Lethic	2009 - A trojan that connects to remote servers, which may lead to unauthorized access to an affected system.
CeeInject	2009 - This threat has been 'obfuscated', which means it has tried to hide its purpose so your security software doesn't detect it. The malware that lies underneath this obfuscation can have almost any purpose.
Cmdow	2009 - a detection for a command-line tool and violated the guidelines by which Microsoft identified unwanted software.
Yabector	2009 - This trojan can use your PC to click on online advertisements without your permission or knowledge. This can earn money for a malicious hacker by making a website or application appear more popular than it is.
Renocide	2009 - a family of worms that spread via local, removable, and network drives and also using file sharing applications. They have IRC-based backdoor functionality, which may allow a remote attacker to execute commands on the affected computer.
Liften	2009 - a trojan that is used to stop affected users from downloading security updates. It is downloaded by Trojan:Win32/FakeXPA.
ShellCode	2009 - A generic detection for JavaScript-enabled objects that contain exploit code and may exhibit suspicious behavior. Malicious websites and malformed PDF documents may contain JavaScript that attempts to execute code without the affected user's consent.
FlyAgent	2009 - A backdoor trojan program that is capable of performing several actions depending on the commands of a remote attacker.
Psyme	2009 - This threat downloads and installs other programs, including other malware, onto your PC without your consent.
Orsam	2009 - A generic detection for a variety of threats. A name used for trojans that have been added to MS signatures after advanced automated analysis.
AgentOff	2009 - This threat can perform a number of actions of a malicious hacker's choice on your PC.
Nuj	2009 - a worm that copies itself to fixed, removable or network drives. Some variants of this worm may also terminate antivirus-related processes.

Malware Family	Description
Sohanad	2009 - Worms automatically spread to other PCs. They can do this in a number of ways, including by copying themselves to removable drives, network folders, or spreading through email.
I2ISolutions	2009 - This program was detected by definitions prior to 1.175.2037.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.
Dpoint	2009 - This program was detected by definitions prior to 1.175.1915.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.
Silly_P2P	2009 - Worms automatically spread to other PCs. They can do this in a number of ways, including by copying themselves to removable drives, network folders, or spreading through email.
Vobfus	2009 - This family of worms can download other malware onto your PC, including: Win32/Beebone, Win32/Fareit, Win32/Zbot. Vobfus worms can be downloaded by other malware or spread via removable drives, such as USB flash drives.
Daurso	2009 - a family of trojans that attempts to steal sensitive information, including passwords and FTP authentication details from affected computers. This family targets particular FTP applications and also attempts to steal data from Protected Storage.
MyDealAssistant	2009 - This program was detected by definitions prior to 1.175.2037.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.
Adsubscribe	2009 - This program was detected by definitions prior to 1.175.1834.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.
MyCentria	2009 - This program was detected by definitions prior to 1.175.2037.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.
Fierads	2009 - This program was detected by definitions prior to 1.175.2037.0 as it violated the guidelines by which Microsoft identified unwanted software. Based on analysis using current guidelines, the program does not have unwanted behaviors.

Malware Family	Description
VBInject	2009 - This is a generic detection for malicious files that are obfuscated using particular techniques to prevent their detection or analysis.
PerfectKeylogger	2009 - a commercial monitoring program that monitors user activity, such as keystrokes typed. MonitoringTool:Win32/PerfectKeylogger is available for purchase at the company's website. It may also have been installed without user consent by a Trojan or other malware.
AgoBot	2010 VOL09 - A backdoor that communicates with a central server using IRC.
Bubnix	2010 VOL09 - A generic detection for a kernel-mode driver installed by other malware that hides its presence on an affected computer by blocking registry and file access to itself. The trojan may report its installation to a remote server and download and distribute spam email messages and could download and execute arbitrary files.
Citeary	2010 VOL09 - A kernel mode driver installed by Win32/Citeary, a worm that spreads to all available drives including the local drive, installs device drivers and attempts to download other malware from a predefined website.
Fakeinit	2010 VOL09 - A rogue security software family distributed under the names Internet Security 2010, Security Essentials 2010, and others.
Oficla	2010 VOL09 - A family of trojans that attempt to inject code into running processes in order to download and execute arbitrary files. It may download rogue security programs.
Pasur	2010 VOL09 - a name used for backdoor trojan detections that have been added to Microsoft signatures after advanced automated analysis.
PrettyPark	2010 VOL09 - A worm that spreads via email attachments. It allows backdoor access and control of an infected computer.
Prorat	2010 VOL09 - A trojan that opens random ports that allow remote access from an attacker to the affected computer. This backdoor may download and execute other malware from predefined websites and may terminate several security applications or services.
Pushbot	2010 VOL09 - A detection for a family of malware that spreads via MSN Messenger, Yahoo! Messenger, and AIM when commanded by a remote attacker. It contains backdoor functionality that allows unauthorized access and control of an affected machine.
Randex	2010 VOL09 - A worm that scans randomly generated IP addresses to attempt to spread to network shares with weak passwords. After the worm infects a computer, it connects to an IRC server to receive commands from the attacker.

Malware Family	Description
SDBot	2010 VOL09 - A family of backdoor trojans that allows attackers to control infected computers over an IRC channel.
Trenk	2010 VOL09 - a name used for backdoor trojan detections that have been added to Microsoft signatures after advanced automated analysis.
Tofsee	2010 VOL09 - A multi-component family of backdoor trojans that act as a spam and traffic relay.
Ursap	2010 VOL09 - a name used for backdoor trojan detections that have been added to Microsoft signatures after advanced automated analysis.
Zbot	2010 VOL09 - A family of password stealing trojans that also contains backdoor functionality allowing unauthorized access and control of an affected machine.
Ciucio	2010 VOL10 - A family of trojans that connect to certain websites in order to download arbitrary files.
ClickPotato	2010 VOL10 - A program that displays popup and notification-style advertisements based on the user's browsing habits.
CVE-2010-0806	2010 VOL10 - A detection for malicious JavaScript that attempts to exploit the vulnerability addressed by Microsoft Security Bulletin MS10-018.
Delf	2010 VOL10 - A detection for various threats written in the Delphi programming language. The behaviors displayed by this malware family are highly variable.
FakePAV	2010 VOL10 - A rogue security software family that masquerades as Microsoft Security Essentials.
Keygen	2010 VOL10 - A generic detection for tools that generate product keys for illegally obtained versions of various software products.
Onescan	2010 VOL10 - A Korean-language rogue security software family distributed under the names One Scan, Siren114, EnPrivacy, PC Trouble, My Vaccine, and others.
Pornpop	2010 VOL10 - A generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.
Startpage	2010 VOL10 - A detection for various threats that change the configured start page of the affected user's web browser, and may also perform other malicious actions.
Begseabug	2011 VOL11 - A trojan that downloads and executes arbitrary files on an affected computer.

Malware Family	Description
CVE-2010-0840	2011 VOL11 - A detection for a malicious and obfuscated Java class that exploits a vulnerability described in CVE-2010-0840. Oracle Corporation addressed the vulnerability with a security update in March 2010.
Cycbot	2011 VOL11 - A backdoor trojan that allows attackers unauthorized access and control of an affected computer. After a computer is infected, the trojan connects to a specific remote server to receive commands from attackers.
DroidDream	2011 VOL11 - A malicious program that affects mobile devices running the Android operating system. It may be bundled with clean applications, and is capable of allowing a remote attacker to gain access to the mobile device.
FakeMacdef	2011 VOL11 - A rogue security software family that affects Apple Mac OS X. It has been distributed under the names MacDefender, MacSecurity, MacProtector, and possibly others.
GameHack	2011 VOL11 - Malware that is often bundled with game applications. It commonly displays unwanted pop-up advertisements and may be installed as a web browser helper object.
Loic	2011 VOL11 - An open-source network attack tool designed to perform denial-ofservice (DoS) attacks.
Lotoor	2011 VOL11 - A detection for specially crafted Android programs that attempt to exploit vulnerabilities in the Android operating system to gain root privilege.
Nuqel	2011 VOL11 - A worm that spreads via mapped drives and certain instant messaging applications. It may modify system settings, connect to certain websites, download arbitrary files, or take other malicious actions.
OfferBox	2011 VOL11 - A program that displays offers based on the user's web browsing habits. Some versions may display advertisements in a pop-under window. Win32/OfferBox may be installed without adequate user consent by malware.
OpenCandy	2011 VOL11 - An adware program that may be bundled with certain thirdparty software installation programs. Some versions may send user-specific information, including a unique machine code, operating system information, locale, and certain other information to a remote server without obtaining adequate user consent.
Pameseg	2011 VOL11 - A fake program installer that requires the user to send SMS messages to a premium number to successfully install certain programs.
Pramro	2011 VOL11 - A trojan that creates a proxy on the infected computer for email and HTTP traffic, and is used to send spam email.
Ramnit	2011 VOL11 - A family of multi-component malware that infects executable files, Microsoft Office files, and HTML files. Win32/Ramnit spreads to

Malware Family	Description
	removable drives and steals sensitive information such as saved FTP credentials and browser cookies. It may also open a backdoor to await instructions from a remote attacker.
Rlsloup	2011 VOL11 - A family of trojans that are used to send spam email. Rlsloup consists of several components, including an installation trojan component and a spamming payload component.
ShopperReports	2011 VOL11 - Adware that displays targeted advertising to affected users while browsing the Internet, based on search terms entered into search engines.
Sinowal	2011 VOL11 - A family of password-stealing and backdoor trojans. It may try to install a fraudulent SSL certificate on the computer. Sinowal may also capture user data such as banking credentials from various user accounts and send the data to Web sites specified by the attacker.
Stuxnet	2011 VOL11 - A multi-component family that spreads via removable volumes by exploiting the vulnerability addressed by Microsoft Security Bulletin MS10-046.
Swimnag	2011 VOL11 - A worm that spreads via removable drives and drops a randomly-named DLL in the Windows system folder.
Tedroo	2011 VOL11 - A trojan that sends spam email messages. Some variants may disable certain Windows services or allow backdoor access by a remote attacker.
Yimfoca	2011 VOL11 - A worm family that spreads via common instant messaging applications and social networking sites. It is capable of connecting to a remote HTTP or IRC server to receive updated configuration data. It also modifies certain system and security settings.
Bamital	2011 VOL12 - A family of malware that intercepts web browser traffic and prevents access to specific security-related websites by modifying the Hosts file. Bamital variants may also modify specific legitimate Windows files in order to execute their payload.
Blacole	2011 VOL12 - An exploit pack, also known as Blackhole, that is installed on a compromised web server by an attacker and includes a number of exploits that target browser software. If a vulnerable computer browses a compromised website containing the exploit pack, various malware may be downloaded and run.
Bulilit	2011 VOL12 - A trojan that silently downloads and installs other programs without consent. Infection could involve the installation of additional malware or malware components to an affected computer.

Malware Family	Description
Dorkbot	2011 VOL12 - A worm that spreads via instant messaging and removable drives. It also contains backdoor functionality that allows unauthorized access and control of the affected computer. Win32/Dorkbot may be distributed from compromised or malicious websites using PDF or browser exploits.
EyeStye	2011 VOL12 - A trojan that attempts to steal sensitive data using a method known as form grabbing, and sends it to a remote attacker. It may also download and execute arbitary files and use a rootkit component to hide its activities.
FakeSysdef	2011 VOL12 - A rogue security software family that claims to discover nonexistent hardware defects related to system memory, hard drives, and overall system performance, and charges a fee to fix the supposed problems.
Helompy	2011 VOL12 - A worm that spreads via removable drives and attempts to capture and steal authentication details for a number of different websites or online services, including Facebook and Gmail.
Malf	2011 VOL12 - A generic detection for malware that drops additional malicious files.
Rugo	2011 VOL12 - A program that installs silently on the user's computer and displays advertisements.
Sirefef	2011 VOL12 - A rogue security software family distributed under the name Antivirus 2010 and others.
Sisproc	2011 VOL12 - A generic detection for a group of trojans that have been observed to perform a number of various and common malware behaviors.
Swisyn	2011 VOL12 - A trojan that drops and executes arbitrary files on an infected computer. The dropped files may be potentially unwanted or malicious programs.
BlacoleRef	2012 VOL13 - An obfuscated script, often found inserted into compromised websites, that uses a hidden inline frame to redirect the browser to a Blacole exploit server.
CVE-2012-0507	2012 VOL13 - A detection for a malicious Java applet that exploits the Java Runtime Environment (JRE) vulnerability described in CVE-2012-0507, addressed by an Oracle security update in February 2012.
Flashback	2012 VOL13 - A trojan that targets Java JRE vulnerability CVE-2012-0507 on Mac OS X to enroll the infected computer in a botnet.
Gendows	2012 VOL13 - A tool that attempts to activate Windows 7 and Windows Vista operating system installations.

Malware Family	Description
GingerBreak	2012 VOL13 - A program that affects mobile devices running the Android operating system. It drops and executes an exploit that, if run successfully, gains administrator privileges on the device.
GingerMaster	2012 VOL13 - A malicious program that affects mobile devices running the Android operating system. It may be bundled with clean applications, and is capable of allowing a remote attacker to gain access to the mobile device.
Mult_JS	2012 VOL13 - A generic detection for various exploits written in the JavaScript language.
Patch	2012 VOL13 - A family of tools intended to modify, or 'patch' programs that may be evaluation copies, or unregistered versions with limited features for the purpose of removing the limitations.
Phoex	2012 VOL13 - A malicious script that exploits the Java Runtime Environment (JRE) vulnerability discussed in CVE-2010-4452. If run in a computer running a vulnerable version of Java, it downloads and executes arbitrary files.
Pluzoks	2012 VOL13 - A trojan that silently downloads and installs other programs without consent. This could include the installation of additional malware or malware components.
Popupper	2012 VOL13 - A detection for a particular JavaScript script that attempts to display pop-under advertisements.
Wizpop	2012 VOL13 - Adware that may track user search habits and download executable programs without user consent.
Wpakill	2012 VOL13 - A family of tools that attempt to disable or bypass WPA (Windows Product Activation), WGA (Windows Genuine Advantage) checks, or WAT (Windows Activation Technologies), by altering Windows operating system files, terminating processes, or stopping services.
Yeltminky	2012 VOL13 - A family of worms that spreads by making copies of itself on all available drives and creating an autorun.inf file to execute that copy.
Aimesu	2013 VOL15 - A threat that exploits vulnerabilities in unpatched versions of Java, Adobe Reader, or Flash Player. It then installs other malare on the computer, including components of the Blackhole and Cool exploit kits.
Bdaejec	2013 VOL15 - A trojan that allows unauthorized access and control of an affected computer, and that may download and install other programs without consent.
Bursted	2013 VOL15 - A virus written in the AutoLISP scripting language used by the AutoCAD computer-aided design program. It infects other AutoLISP files with the extension .lsp.

Malware Family	Description
Colkit	2013 VOL15 - A detection for obfuscated, malicious JavaScript code that redirects to or loads files that may exploit a vulnerable version of Java, Adobe Reader, or Adobe Flash, possibly in an attempt to load malware onto the computer.
Coolex	2013 VOL15 - A detection for scripts from an exploit pack known as the Cool Exploit Kit. These scripts are often used in ransomware schemes in which an attacker locks a victim's computer or encrypts the user's data and demands money to make it available again.
CplLnk	2013 VOL15 - A generic detection for specially crafted malicious shortcut files that attempt to exploit the vulnerability addressed by Microsoft Security Bulletin MS10-046, CVE-2010-2568.
CVE-2011-1823	2013 VOL15 - A detection for specially crafted Android programs that attempt to exploit a vulnerability in the Android operating system to gain root privilege.
CVE-2012-1723	2013 VOL15 - A family of malicious Java applets that attempt to exploit vulnerability CVE-2012-1723 in the Java Runtime Environment (JRE) to download and install files of an attacker's choice onto the computer.
DealPly	2013 VOL15 - Adware that displays offers related to the user's web browsing habits. It may be bundled with certain third-party software installation programs.
Fareit	2013 VOL15 - A malware family that has multiple components: a password stealing component that steals sensitive information and sends it to an attacker, and a DDoS component that could be used against other computers.
FastSaveApp	2013 VOL15 - An adware program that displays offers related to the user's web browsing habits. It may use the name 'SaveAs' or 'SaveByClick'.
FindLyrics	2013 VOL15 - An adware program that displays ads related to the user's web browsing habits.
Gamarue	2013 VOL15 - A worm that is commonly distributed via exploit kits and social engineering. Variants have been observed stealing information from the local computer and communicating with command-and-control (C&C) servers managed by attackers.
Gisav	2013 VOL15 - An adware program that displays offers related to the user's web browsing habits. It can be downloaded from the program's website, and can be bundled with some third-party software installation programs.
InfoAtoms	2013 VOL15 - An adware program that displays advertisements related to the user's web browsing habits and inserts advertisements into websites.

Malware Family	Description
Perl/IRCbot.E	2013 VOL15 - A backdoor trojan that drops other malicious software and connects to IRC servers to receive commands from attackers.
Javrobat	2013 VOL15 - An exploit that tries to check whether certain versions of Adobe Acrobat or Adobe Reader are installed on the computer. If so, it tries to install malware.
Kraddare	2013 VOL15 - Adware that displays Korean-language advertisements.
PriceGong	2013 VOL15 - An adware program that shows certain deals related to the search terms entered on any web page.
Protlerdob	2013 VOL15 - A software installer with a Portuguese language user interface. It presents itself as a free movie download but bundles with it a number of programs that may charge for services.
Qhost	2013 VOL15 - A generic detection for trojans that modify the HOSTS file on the computer to redirect or limit Internet traffic to certain sites.
Reveton	2013 VOL15 - A ransomware family that targets users from certain countries or regions. It locks the computer and displays a location-specific webpage that covers the desktop and demands that the user pay a fine for the supposed possession of illicit material.
Rongvhin	2013 VOL15 - A family of malware that perpetrates click fraud. It might be delivered to the computer via hack tools for the game CrossFire.
Seedabutor	2013 VOL15 - A JavaScript trojan that attempts to redirect the browser to another website.
SMSer	2013 VOL15 - A ransomware trojan that locks an affected user's computer and requests that the user send a text message to a premium-charge number to unlock it.
Tobfy	2013 VOL15 - A family of ransomware trojans that targets users from certain countries. It locks the computer and displays a localized message demanding the payment of a fine for the supposed possession of illicit material. Some variants may also take webcam screenshots, play audio messages, or affect certain processes or drivers.
Truado	2013 VOL15 - A trojan that poses as an update for certain Adobe software.
Urausy	2013 VOL15 - A family of ransomware trojans that locks the computer and displays a localized message, supposedly from police authorities, demanding the payment of a fine for alleged criminal activity.
Wecykler	2013 VOL15 - A family of worms that spread via removable drives, such as USB drives, that may stop security processes and other processes on the computer, and log keystrokes that are later sent to a remote attacker.

Malware Family	Description
Weelsof	2013 VOL15 - A family of ransomware trojans that targets users from certain countries. It locks the computer and displays a localized message demanding the payment of a fine for the alleged possession of illicit material. Some variants may take steps that make it difficult to run or update virus protection.
Yakdowpe	2013 VOL15 - A family of trojans that connect to certain websites to silently download and install other programs without consent.
Anogre	2013 VOL16 - A threat that exploits a vulnerability addressed by Microsoft Security Bulletin MS11-087. This vulnerability can allow a hacker to install programs, view, change, or delete data or create new accounts with full administrative privileges.
Brantall	2013 VOL16 - A family of trojans that download and install other programs, including Win32/Sefnit and Win32/Rotbrow. Brantall often pretends to be an installer for other, legitimate programs.
Comame	2013 VOL16 - A generic detection for a variety of threats.
Crilock	2013 VOL16 - A ransomware family that encrypts the computer's files and displays a webpage that demands a fee to unlock them.
CVE-2011-3874	2013 VOL16 - A threat that attempts to exploit a vulnerability in the Android operating system to gain access to and control of the device Java/CVE-2012-1723. A family of malicious Java applets that attempt to exploit vulnerability CVE-2012-1723 in the Java Runtime Environment (JRE) in order to download and install files of an attacker’s choice onto the computer.
Deminnix	2013 VOL16 - A trojan that uses the computer for Bitcoin mining and changes the home page of the web browser. It can accidentally be downloaded along with other files from torrent sites.
Detplock	2013 VOL16 - A generic detection for a variety of threats.
Dircrypt	2013 VOL16 - Ransomware that encrypts the user's files and demands payment to release them. It is distributed through spam email messages and can be downloaded by other malware.
DonxRef	2013 VOL16 - A generic detection for malicious JavaScript objects that construct shellcode. The scripts may try to exploit vulnerabilities in Java, Adobe Flash Player, and Windows.
Faceliker	2013 VOL16 - A malicious script that likes content on Facebook without the user's knowledge or consent.
FakeAlert	2013 VOL16 - A malicious script that falsely claims that the computer is infected with viruses and that additional software is needed to disinfect it.

Malware Family	Description
Jenxcus	2013 VOL16 - A worm that gives an attacker control of the computer. It is spread by infected removable drives, like USB flash drives. It can also be downloaded within a torrent file.
Loktrom	2013 VOL16 - Ransomware that locks the computer and displays a full-screen message pretending to be from a national police force, demanding payment to unlock the computer.
Miposa	2013 VOL16 - A trojan that downloads and runs malicious Windows Scripting Host (.wsh) files.
Nitol	2013 VOL16 - A family of trojans that perform DDoS (distributed denial of service) attacks, allow backdoor access and control, download and run files, and perform a number of other malicious activities on the computer.
Oceanmug	2013 VOL16 - A trojan that silently downloads and installs other programs without consent.
Proslikefan	2013 VOL16 - A worm that spreads through removable drives, network shares, and P2P programs. It can lower the computer's security settings and disable antivirus products.
Rotbrow	2013 VOL16 - A trojan that installs browser add-ons that claim to offer protection from other add-ons. Rotbrow can change the browser's home page, and can install the trojan Win32/Sefnit. It is commonly installed by Win32/Brantall.
Sefnit	2013 VOL16 - A family of trojans that can allow backdoor access, download files, and use the computer and Internet connection for click fraud. Some variants can monitor web browsers and hijack search results.
Urntone	2013 VOL16 - A webpage component of the Neutrino exploit kit. It checks the version numbers of popular applications installed on the computer, and attempts to install malware that targets vulnerabilities in the software.
Wysotot	2013 VOL16 - A threat that can change the start page of the user's web browser, and may download and install other files to the computer. It is installed by software bundlers that advertise free software or games.
AddLyrics	2014 VOL17 - A browser add-on that displays lyrics for songs on YouTube, and displays advertisements in the browser window.
Adpeak	2014 VOL17 - Adware that displays extra ads as the user browses the Internet, without revealing where the ads are coming from. It may be bundled with some third-party software installation programs.
Axpergle	2014 VOL17 - A detection for the Angler exploit kit, which exploits vulnerabilities in recent versions of Internet Explorer, Silverlight, Adobe Flash Player, and Java to install malware.

Malware Family	Description
Bepush	2014 VOL17 - A family of trojans that download and install add-ons for the Firefox and Chrome browsers that post malicious links to social networking sites, track browser usage, and redirect the browser to specific websites.
BetterSurf	2014 VOL17 - Adware that displays unwanted ads on search engine results pages and other websites. It may be included with software bundles that offer free applications or games.
Bladabindi	2014 VOL17 - A family of backdoors created by a malicious hacker tool called NJ Rat. They can steal sensitive information, download other malware, and allow backdoor access to an infected computer.
Caphaw	2014 VOL17 - A family of backdoors that spread via Facebook, YouTube, Skype, removable drives, and drive-by download. They can make Facebook posts via the user's account, and may steal online banking details.
Clikug	2014 VOL17 - A threat that uses a computer for click fraud. It has been observed using as much as a gigabyte of bandwidth per hour.
CVE-2014-0322	This threat uses a vulnerability MS14-012, CVE-2014-0322 in Internet Explorer 9 and 10 to download and run files on your PC, including other malware.
CVE-2013-0422	2014 VOL17 - A detection for a malicious Java applet that exploits the Java Runtime Environment (JRE) vulnerability described in CVE-2013-0422, addressed by an Oracle security update in January 2013.
Dowque	2014 VOL17 - A generic detection for malicious files that are capable of installing other malware.
Fashack	2014 VOL17 - A detection for the Safehack exploit kit, also known as Flashpack. It uses vulnerabilities in Adobe Flash Player, Java, and Silverlight to install malware on a computer.
Feven	2014 VOL17 - A browser add-on for Internet Explorer, Firefox, or Chrome that displays ads on search engine results pages and other websites, and redirects the browser to specific websites.
Fiexp	2014 VOL17 - A detection for the Fiesta exploit kit, which attempts to exploit Java, Adobe Flash Player, Adobe Reader, Silverlight, and Internet Explorer to install malware.
Filcout	2014 VOL17 - An application that offers to locate and download programs to run unknown files. It has been observed installing variants in the Win32/Sefnit family.
Genasom	2014 VOL17 - A ransomware family that locks a computer and demands money to unlock it. It usually targets Russian-language users, and may open pornographic websites.

Malware Family	Description
Kegotip	2014 VOL17 - A password-stealing trojan that can steal email addresses, personal information, or user account information for certain programs.
Krypterade	2014 VOL17 - Ransomware that fraudulently claims a computer has been used for unlawful activity, locks it, and demands that the user pay to unlock it.
Lecpetex	2014 VOL17 - A family of trojans that steal sensitive information, such as user names and passwords. It can also use a computer for Litecoin mining, install other malware, and post malicious content via the user's Facebook account.
Lollipop	2014 VOL17 - Adware that may be installed by third-party software bundlers. It displays ads based on search engine searches, which can differ by geographic location and may be pornographic.
Meadgive	2014 VOL17 - A detection for the Redkit exploit kit, also known as Infinity and Goon. It attempts to exploit vulnerabilities in programs such as Java and Silverlight to install other malware.
Neclu	2014 VOL17 - A detection for the Nuclear exploit kit, which attempts to exploit vulnerabilities in programs such as Java and Adobe Reader to install other malware.
Ogimant	2014 VOL17 - A threat that claims to help download items from the Internet, but actually downloads and runs files that are specified by a remote attacker.
OptimizerElite	2014 VOL17 - A misleading program that uses legitimate files in the Prefetch folder to claim that the computer is damaged and offers to fix the damage for a price.
Pangimop	2014 VOL17 - A detection for the Magnitude exploit kit, also known as Popads. It attempts to exploit vulnerabilities in programs such as Java and Adobe Flash Player to install other malware.
Phish	2014 VOL17 - A password-stealing malicious webpage, known as a phishing page, that disguises itself as a page from a legitimate website.
Prast	2014 VOL17 - A generic detection for various password stealing trojans.
Slugin	2014 VOL17 - A file infector that infects .exe and .dll files. It may also perform backdoor actions.
Spacekito	2014 VOL17 - A threat that steals information about the computer and installs browser add-ons that display ads.
Tranikpik	This threat is a backdoor that can give a hacker unauthorized access and control of your PC

Malware Family	Description
Wordinvop	2014 VOL17 - A detection for a specially-crafted Microsoft Word file that attempts to exploit the vulnerability CVE-2006-6456, addressed by Microsoft Security Bulletin MS07-014.
Zegost	2014 VOL17 - A backdoor that allows an attacker to remotely access and control a computer.
Archost	2014 VOL18 - A downloader that installs other programs on the computer without the user's consent, including other malware.
Balamid	2014 VOL18 - A trojan that can use the computer to click on online advertisements without the user's permission or knowledge. This can earn money for a malicious hacker by making a website or application appear more popular than it is.
BeeVry	2014 VOL18 - A trojan that modifies a number of settings to prevent the computer from accessing security-related websites, and lower the computer's security.
Bondat	2014 VOL18 - A family of threats that collects information about the computer, infects removable drives, and tries to stop the user from accessing files. It spreads by infecting removable drives, such as USB thumb drives and flash drives.
Bregent	2014 VOL18 - A downloader that injects malicious code into legitimate processes such as explorer.exe and svchost.exe, and downloads other malware onto the computer.
Brolo	2014 VOL18 - A ransomware family that locks the web browser and displays a message, often pretending to be from a law enforcement agency, demanding money to unlock the browser.
CostMin	2014 VOL18 - An adware family that installs itself as a browser extension for Internet Explorer, Mozilla Firefox, and Google Chrome, and displays advertisements as the user browses the Internet.
CouponRuc	2014 VOL18 - A browser modifier that changes browser settings and may also modify some computer and Internet settings.
Crastic	2014 VOL18 - A trojan that sends sensitive information to a remote attacker, such as user names, passwords and information about the computer. It can also delete System Restore points, making it harder to recover the computer to a pre-infected state.
Crowti	2014 VOL18 - A ransomware family that encrypts files on the computer and demands that the user pay a fee to decrypt them, using Bitcoins.

Malware Family	Description
CVE-2013-1488	2014 VOL18 - A detection for threats that use a Java vulnerability to download and run files on your PC, including other malware. Oracle addressed the vulnerability with a security update in April 2013.
DefaultTab	2014 VOL18 - A browser modifier that redirects web browser searches and prevents the user from changing browser settings.
Ippedo	2014 VOL18 - A worm that can send sensitive information to a malicious hacker. It spreads through infected removable drives, such as USB flash drives.
Kilim	2014 VOL18 - A trojan that hijacks the user's Facebook, Twitter, or YouTube account to promote pages. It may post hyperlinks or like pages on Facebook, post comments on YouTube videos, or follow profiles and send direct messages on Twitter without permission.
Mofin	2014 VOL18 - A worm that can steal files from your PC and send them to a malicious hacker. It spreads via infected removable drives, such as USB flash drives.
MpTamperSrp	2014 VOL18 - A generic detection for an attempt to add software restriction policies to restrict Microsoft antimalware products, such as Microsoft Security Essentials and Windows Defender, from functioning properly.
Mujormel	2014 VOL18 - A password stealer that can steal personal information, such as user names and passwords, and send the stolen information to a malicious hacker.
PennyBee	2014 VOL18 - Adware that shows ads as the user browses the web. It can be installed from the program's website or bundled with some third-party software installation programs.
Phdet	2014 VOL18 - A family of backdoor trojans that is used to perform distributed denial-of service (DDoS) attacks against specified targets.
Rimod	2014 VOL18 - A generic detection for files that change various security settings in the computer Win32/Rotbrow. A trojan that installs browser add-ons that claim to offer protection from other add-ons. Rotbrow can change the browser's home page, and can install the trojan Win32/Sefnit. It is commonly installed by Win32/Brantall.
Sigru	2014 VOL18 - A virus that can stop some files from working correctly in Windows XP and earlier operating systems. It spreads by infecting the master boot record (MBR) on connected hard disks and floppy disks.
SimpleShell	2014 VOL18 - A backdoor that can give a malicious hacker unauthorized access to and control of the computer.

Malware Family	Description
Softpulse	2014 VOL18 - A software bundler that no longer meets Microsoft detection criteria for unwanted software following a program update in September of 2014.
SquareNet	2014 VOL18 - A software bundler that installs other unwanted software, including adware and click-fraud malware.
Tugspay	2014 VOL18 - A downloader that spreads by posing as an installer for legitimate software, such as a Java update, or through other malware. When installed, it downloads unwanted software to the computer.
Tupym	2014 VOL18 - A worm that copies itself to the system folder of the affected computer, and attempts to contact remote hosts.
Vercuser	2014 VOL18 - A worm that typically spreads via drive-by download. It also receives commands from a remote server, and has been observed dropping other malware on the infected computer.
Adnel	2015 VOL19 - A family of macro malware that can download other threats to the computer, including TrojanDownloader:Win32/Drixed.
Adodb	2015 VOL19 - A generic detection for script trojans that exploit a vulnerability in Microsoft Data Access Components (MDAC) that allows remote code execution. Microsoft released Security Bulletin MS06-014 in April 2006 to address the vulnerability.
AlterbookSP	2015 VOL19 - A browser add-on that formerly displayed behaviors of unwanted software. Recent versions of the add-on no longer meet Microsoft detection criteria, and are no longer considered unwanted software.
BrobanDel	2015 VOL19 - A family of trojans that can modify boletos bancários, a common payment method in Brazil. They can be installed on the computer when a user opens a malicious spam email attachment.
CompromisedCert	2015 VOL19 - A detection for the Superfish VisualDiscovery advertising program that was preinstalled on some Lenovo laptops sold in 2014 and 2015. It installs a compromised trusted root certificate on the computer, which can be used to conduct man-in-the-middle attacks on the computer.
CouponRuc_new	2015 VOL19 - A browser modifier that changes browser settings and may also modify some computer and Internet settings.
CVE-2014-6332	2015 VOL19 - This threat uses a Microsoft vulnerability MS14-064 to download and run files on your PC, including other malware.
Dyzap	2015 VOL19 - A threat that steals login credentials for a long list of banking websites using man-in-the-browser (MITB) attacks. It is usually installed on the infected computer by TrojanDownloader:Win32/Upatre.

Malware Family	Description
EoRezo	2015 VOL19 - Adware that displays targeted advertising to affected users while browsing the Internet, based on downloaded pre-configured information.
FakeCall	2015 VOL19 - This threat is a webpage that claims your PC is infected with malware. It asks you to phone a number to receive technical support to help remove the malware.
Foosace	2015 VOL19 - A threat that creates files on the compromised computer and contacts a remote host. Observed in the STRONTIUM APT.
IeEnablerCby	2015 VOL19 - A browser modifier that installs additional browser addons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
InstalleRex	2015 VOL19 - A software bundler that installs unwanted software, including Win32/CouponRuc and Win32/SaverExtension. It alters its own 'Installed On' date in Programs and Features to make it more difficult for a user to locate it and remove it.
JackTheRipper	2015 VOL19 - A virus that can stop some files from working correctly in Windows XP and earlier operating systems. It spreads by infecting the master boot record (MBR) on connected hard disks and floppy disks.
Kenilfe	2015 VOL19 - A worm written in AutoCAD Lisp that only runs if AutoCAD is installed on the computer or network. It renames and deletes certain AutoCAD files, and may download and execute arbitrary files from a remote host.
KipodToolsCby	2015 VOL19 - A browser modifier that installs additional browser addons without the user's consent. It bypasses the normal prompts or dialogs that ask for consent to install add-ons.
Macoute	2015 VOL19 - A worm that can spread itself to removable USB drives, and may communicate with a remote host.
NeutrinoEK	2015 VOL19 - This threat is a webpage that spreads the exploit kit known as Neutrino.
Peaac	2015 VOL19 - A generic detection for various threats that display trojan characteristics.
Peals	2015 VOL19 - A generic detection for various threats that display trojan characteristics.
Radonskra	2015 VOL19 - A family of threats that perform a variety of malicious acts, including stealing information about the computer, showing extra advertisements as the user browses the web, performing click fraud, and downloading other programs without consent.

Malware Family	Description
SaverExtension	2015 VOL19 - A browser add-on that shows ads in the browser without revealing their source, and prevents itself from being removed normally.
Sdbby	2015 VOL19 - A threat that exploits a bypass to gain administrative privileges on a machine without going through a User Access Control prompt.
Simda	2015 VOL19 - A threat that can give an attacker backdoor access and control of an infected computer. It can then steal passwords and gather information about the computer to send to the attacker.
Skeeyah	2015 VOL19 - A generic detection for various threats that display trojan characteristics.
Wordjmp	2015 VOL19 - An exploit that targets a vulnerability in Word 2002 and 2003 that could allow an attacker to remotely execute arbitrary code. Microsoft released Security Bulletin MS06-027 in June 2006 to address the vulnerability.
Bayads	2015 VOL20 - A program that displays ads as the user browses the web. It can be bundled with other software. It may call itself bdraw, delta, dlclient, Pay-ByAds, or pricehorse in Programs and Features.
CandyOpen	2015 VOL20 - This application can also affect the quality of your computing experience. We have seen this leading to the following potentially unwanted behaviors on PCs: Adds files that run at startup, Modifies boot configuration data, Modifies file associations, Injects into other processes on your system, Changes browser settings, Adds a local proxy, Modifies your system DNS settings, Stops Windows Update, Disables User Access Control (UAC), These applications are most commonly software bundlers or installers for applications such as toolbars, adware, or system optimizers. We have observed this application installing software that you might not have intended on your PC.
Colisi	2015 VOL20 - Behavioral detection of certain files acting in a malicious way.
Creprote	2015 VOL20 - These programs are most commonly software bundlers or installers for software such as toolbars, adware, or system optimizers. The software might modify your homepage, your search provider, or perform other actions that you might not have intended.
Diplugem	2015 VOL20 - A browser modifier that installs browser add-ons without obtaining the user's consent. The add-ons show extra advertisements as the user browses the web, and can inject additional ads into web search results pages.
Dipsind	2015 VOL20 - A threat that is often used in targeted attacks. It can give an attacker access to the computer to download and run files, steal domain credentials, and perform other malicious actions.

Malware Family	Description
Donoff	2015 VOL20 - A threat that uses an infected Microsoft Office file to download other malware onto the computer. It can arrive as a spam email attachment, usually as a Word file (.doc).
Dorv	2015 VOL20 - A trojan is a type of malware that can't spread on its own. It relies on you to run them on your PC by mistake, or visit a hacked or malicious webpage. They can steal your personal information, download more malware, or give a malicious hacker access to your PC.
Dowadmin	2015 VOL20 - A software bundler that does not provide the user with the option to decline installation of unwanted software.
Fourthrem	2015 VOL20 - A program that installs unwanted software without adequate consent on the computer at the same time as the software the user is trying to install.
Hao123	2015 VOL20 - This threat is a modified Internet Explorer shortcut that changes your Internet Explorer homepage. It might arrive on your PC through bundlers that offer free software. The threat will run a separate threat-related file that changes the Internet Explorer.
Mizenota	2015 VOL20 - This program is a software bundler that installs unwanted software on your PC at the same time as the software you are trying to install. It may install one of the following: BrowserModifier:Win32/SupTab, BrowserModifier:Win32/Sasquor, BrowserModifier:Win32/Smudplu, SoftwareBundler:Win32/Pokavampo, BrowserModifier:Win32/Shopperz, Adware:Win32/EoRezo
Mytonel	2015 VOL20 - A program that downloads and installs other programs onto the computer without the user's consent, including other malware.
OutBrowse	2015 VOL20 - A software bundler that installs additional unwanted programs alongside software that the user wishes to install. It can remove or hide the installer's close button, leaving no way to decline the additional applications.
Peapoon	2015 VOL20 - An adware program that shows users ads that they cannot control as they browse the web. It may identify itself as Coupon in Programs and Features.
Pokki	2015 VOL20 - A browser add-on that formerly displayed behaviors of unwanted software. Recent versions of the add-on no longer meet Microsoft detection criteria, and are no longer considered unwanted software.
Putalol	2015 VOL20 - An adware program that shows users ads that they cannot control as they browse the web. It may identify itself as Lolliscan in Programs and Features.
SpigotSearch	2015 VOL20 - This application can affect the quality of your computing experience. For example, some potentially unwanted applications can: Install

Malware Family	Description
	additional bundled software, Modify your homepage, Modify your search provider. These applications are most commonly software bundlers or installers for applications such as toolbars, adware, or system optimizers. We have observed this application installing software that you might not have intended on your PC.
Spursint	2015 VOL20 - This threat has been detected as one of the executable malware that are distributed through URLs.
Sulunch	2015 VOL20 - A generic detection for a group of trojans that perform a number of common malware behaviors.
SupTab	2015 VOL20 - A browser modifier that installs itself and changes the browser's default search provider, without obtaining the user's consent for either action.
Sventore	2015 VOL20 - This trojan can install other malware or unwanted software onto your PC.
Tillail	2015 VOL20 - A software bundler that installs unwanted software alongside the software the user is trying to install. It has been observed to install the browser modifier Win32/SupTab.
VOPackage	2015 VOL20 - This application can also affect the quality of your computing experience. We have seen this leading to the following potentially unwanted behaviors on PCs: Adds files that run at startup, Installs a driver, Injects into other processes on your system, Injects into browsers, Changes browser settings, Changes browser shortcuts, Installs browser extensions, Adds a local proxy, Tampers with root certificate trust, Modifies the system hosts file, Modifies your system DNS settings, Disables anti-virus products, Tampers with system Group Policy settings, These applications are most commonly software bundlers or installers for applications such as toolbars, adware, or system optimizers. We have observed this application installing software that you might not have intended on your PC.
Xiazai	2015 VOL20 - A program that installs unwanted software on the computer at the same time as the software the user is trying to install, without adequate consent.
Zlob	2008 - A family of trojans that often pose as downloadable media codecs. When installed, Win32/Zlob displays frequent pop-up advertisements for rogue security software
Vundo	2008 - A multiplecomponent family of programs that deliver pop-up advertisements and may download and execute arbitrary files. Vundo is often installed as a browser helper object (BHO) without a user's consent

Malware Family	Description
Virtumonde	2008 - multi-component malware family that displays pop-up advertisements for rogue security software
Bancos	2008 - A data-stealing trojan that captures online banking credentials and relays them to the attacker. Most variants target customers of Brazilian banks.
Cutwail	2008 - A trojan that downloads and executes arbitrary files, usually to send spam. Win32/Cutwail has also been observed to transmit Win32/Newacc
Oderoor	2008 - a backdoor trojan that allows an attacker access and control of the compromised computer. This trojan may connect with remote web sites and SMTP servers.
Newacc	2008 - An attacker tool that automatically registers new e-mail accounts on Hotmail, AOL, Gmail, Lycos and other account service providers, using a Web service to decode CAPTCHA protection.
Captiya	2008 - A trojan that transmits CAPTCHA images to a botnet, in what is believed to be an effort to improve the botnet's ability to detect characters and break CAPTCHAs more successfully
Taterf	2008 - A family of worms that spread through mapped drives in order to steal login and account details for popular online games.
Frethog	2008 - A large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games
Tilcun	2008 - A family of trojans that steals online game passwords and sends this captured data to remote sites.
Ceekat	2008 - A collection of trojans that steal information such as passwords for online games, usually by reading information directly from running processes in memory. Different variants target different processes.

Table 46 - MS Caro Malware Families

xxiii. Open Threat Taxonomy

Threat Category	Category Description	Threat
Physical	Threats to the confidentiality, integrity, or availability of information systems that are physical in nature. These threats generally describe actions that could lead to the theft, harm, or destruction of information systems.	Loss of Property - Rating: 5.0
		Theft of Property - Rating: 5.0
		Accidental Destruction of Property - Rating: 3.0
		Natural Destruction of Property - Rating: 3.0
		Intentional Destruction of Property - Rating: 2.0
		Intentional Sabotage of Property - Rating: 2.0
		Intentional Vandalism of Property - Rating: 2.0
		Electrical System Failure - Rating: 4.0
		Heating, Ventilation, Air Conditioning (HVAC) Failure - Rating: 3.0
		Structural Facility Failure - Rating: 2.0
		Water Distribution System Failure - Rating: 2.0
		Sanitation System Failure - Rating: 1.0
		Natural Gas Distribution Failure - Rating: 1.0
		Electronic Media Failure - Rating: 3.0
Resource	Threats to the confidentiality, integrity, or availability of	Disruption of Water Resources - Rating: 2.0

Threat Category	Category Description	Threat
	information systems that are the result of a lack of resources required by the information system. These threats often cause failures of information systems through a disruption of resources required for operations.	Disruption of Water Resources - Rating: 2.0
		Disruption of Fuel Resources - Rating: 2.0
		Disruption of Materials Resources - Rating: 2.0
		Disruption of Electrical Resources - Rating: 4.0
		Disruption of Transportation Services - Rating: 1.0
		Disruption of Communications Services - Rating: 4.0
		Disruption of Emergency Services - Rating: 1.0
		Disruption of Governmental Services - Rating: 1.0
		Supplier Viability - Rating: 2.0
		Supplier Supply Chain Failure - Rating: 2.0
		Logistics Provider Failures - Rating: 1.0
		Logistics Route Disruptions - Rating: 1.0
		Technology Services Manipulation - Rating: 3.0
Personal	Threats to the confidentiality, integrity, or availability of information systems that are the result of failures or actions performed by an organization's personnel. These threats can be the result of deliberate or accidental actions that cause harm to information systems.	Personnel Labor / Skills Shortage - Rating: 5.0
		Loss of Personnel Resources - Rating: 3.0
		Disruption of Personnel Resources - Rating: 3.0
		Social Engineering of Personnel Resources - Rating: 4.0

Threat Category	Category Description	Threat
		Negligent Personnel Resources - Rating: 4.0
		Personnel Mistakes / Errors - Rating: 4.0
		Personnel Inaction - Rating: 3.0
Technical	Threats to the confidentiality, integrity, or availability of information systems that are technical in nature. These threats are most often considered when identifying threats and constitute the technical actions performed by a threat actor that can cause harm to an information system.	Organizational Fingerprinting via Open Sources - Rating:
		System Fingerprinting via Open Sources - Rating: 2.0
		System Fingerprinting via Scanning - Rating: 2.0
		System Fingerprinting via Sniffing - Rating: 2.0
		Credential Discovery via Open Sources - Rating: 4.0
		Credential Discovery via Scanning - Rating: 3.0
		Credential Discovery via Sniffing - Rating: 4.0
		Credential Discovery via Brute Force - Rating: 4.0
		Credential Discovery via Cracking - Rating: 4.0
		Credential Discovery via Guessing - Rating: 2.0
		Credential Discovery via Pre-Computational Attacks - Rating: 3.0
		Misuse of System Credentials - Rating: 3.0
		Escalation of Privilege - Rating: 5.0
		Abuse of System Privileges - Rating: 4.0
		Memory Manipulation - Rating: 4.0

Threat Category	Category Description	Threat
		Cache Poisoning - Rating: 3.0
		Physical Manipulation of Technical Device - Rating: 2.0
		Manipulation of Trusted System - Rating: 4.0
		Cryptanalysis - Rating: 1.0
		Data Leakage / Theft - Rating: 3.0
		Denial of Service - Rating: 2.0
		Maintaining System Persistence - Rating: 5.0
		Manipulation of Data in Transit / Use - Rating: 2.0
		Capture of Data in Transit / Use via Sniffing - Rating: 3.0
		Capture of Data in Transit / Use via Debugging - Rating: 2.0
		Capture of Data in Transit / Use via Keystroke Logging - Rating: 3.0
		Replay of Data in Transit / Use - Rating: 2.0
		Misdelivery of Data - Rating: 2.0
		Capture of Stored Data - Rating: 3.0
		Manipulation of Stored Data - Rating: 3.0
		Application Exploitation via Input Manipulation - Rating: 5.0
		Application Exploitation via Parameter Injection - Rating: 4.0
		Application Exploitation via Code Injection - Rating: 4.0
		Application Exploitation via Command Injection - Rating: 4.0

Threat Category	Category Description	Threat
		Application Exploitation via Path Traversal - Rating: 3.0
		Application Exploitation via API Abuse - Rating: 3.0
		Application Exploitation via Fuzzing - Rating: 3.0
		Application Exploitation via Reverse Engineering - Rating: 3.0
		Application Exploitation via Resource Location Guessing - Rating: 2.0
		Application Exploitation via Source Code Manipulation - Rating: 3.0
		Application Exploitation via Authentication Bypass - Rating: 2.0

Table 47 - Open Threat Categorization

xxiv. Sans Institute Threat Categorization

Classification Type	Category	Sub Category	
Memory Based	**Resident**		
	Temporary Resident		
	Swapping Mode		
	Non resident		
	User Process		
	Kernel Process		
Target Based	**Compiled Viruses**	File Infector	Appending virus
			Prepending virus
			Overwriting virus
			Cavity virus
			Compressing virus
			Amoeba virus
			Entry point obfuscation virus
			Companion virus
			Code Virus
		Boot Sectors	
	Interpreted Viruses	Macro virus	
		Script virus	
	Multipartite Viruses		
Obfuscation Technique Based	**No obfuscation**		
	Encryption		
	Oligomorphism		
	Polymorphism		
	Metamorphism		
	Stealth		
	Armoring		

Classification Type	Category	Sub Category	
	Tunelling		
	Retro virus		
Payload Based	**Non payload**		
	Non destructive payload		
	Desctructive		
	Droppers		

Table 48 – Sans Institute Virus Classification