



THE EU CYBERSECURITY AGENCY

BUILDING A COMMON LANGUAGE TO FACE FUTURE INCIDENTS

REFERENCE SECURITY INCIDENT TAXONOMY

WORKING GROUP – RSIT WG

Rossella Mattioli
Expert in Network and Information Security
CSIRT Relations team
ENISA - European Union Agency for Network and Information Security

CSIRTS SITUATION IN EUROPE TODAY

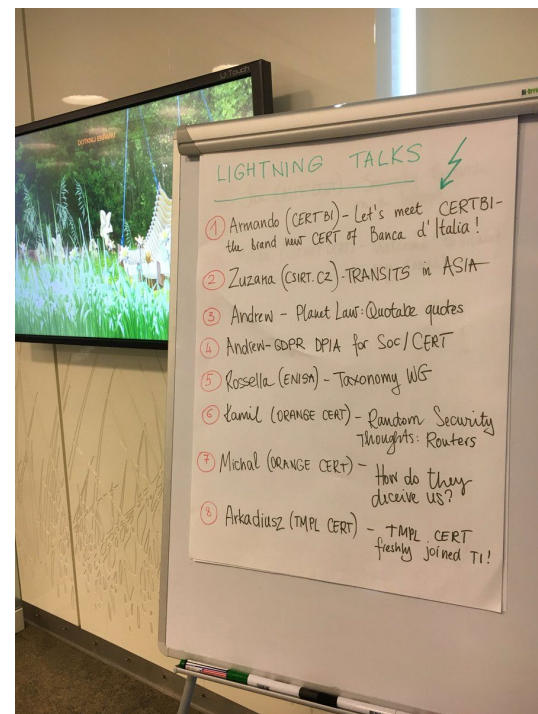
- 387 ENISA Inventory listed teams:
 - teams in CSIRTs Network: 40
 - Trusted Introducer listed: 173 out of 174
 - Trusted Introducer accredited: 152 out of 158
 - 23 out of 40 CSIRTs Network members are accredited
 - Trusted Introducer certified: 25 out of 25*
 - 7 out of 40 CSIRTs Network members are certified
 - FIRST members: 177 out of 450
 - 30 out of 40 CSIRTs Network members are FIRST Members



<http://enisa.europa.eu/csirts-map>

COMMUNITY COMES TOGETHER: REFERENCE SECURITY INCIDENT TAXONOMY WORKING GROUP – RSIT WG

- ENISA introduces this idea in 2017 to the TF-CSIRT
- 52 participants from 17 MS and European Institutions within European CSIRT community
- Building a common language to face future incidents



<https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force>



REFERENCE INCIDENT TAXONOMY WORKING GROUP – RSIT WG

- Approved as official TF-CSIRT working group by the TF-CSIRT Steering Committee on 26 September 2018.
- Taxonomy available in human and machine readable format



TF-CSIRT Hague
May 2017

TF-CSIRT
Stockholm
September 2017

ENISA publishes
status report
Q4 2017



RSIT WG GitHub
with working
version and
documentation

TF-CSIRT Vilnius
September 2018

TF-CSIRT meeting
& FIRST Regional
Symposium
Europe
January 2019

TF-CSIRT
Luxembourg May
2019

<https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force>



As the need for information exchange, incident reporting and use of automation in incident response increases, it is becoming evident that developing a set of standardised guidelines is crucial. This common ground would help incident handlers in dealing with technical incidents on a daily basis.

RSIT WG SCOPE

<https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/Documentation/ToR.md>



AIM AND OBJECTIVES

- Develop Reference Document (Classifications, incident types or examples, and definition) using eCSIRT.net as a starting point.
- Define and develop an Update and Versioning Mechanism
- Host reference document
- Organise regular physical meetings with the stakeholders
- In the 2nd phase broader working group with non-European teams (FIRST) to achieve global consensus on incident reference taxonomy



USE CASES

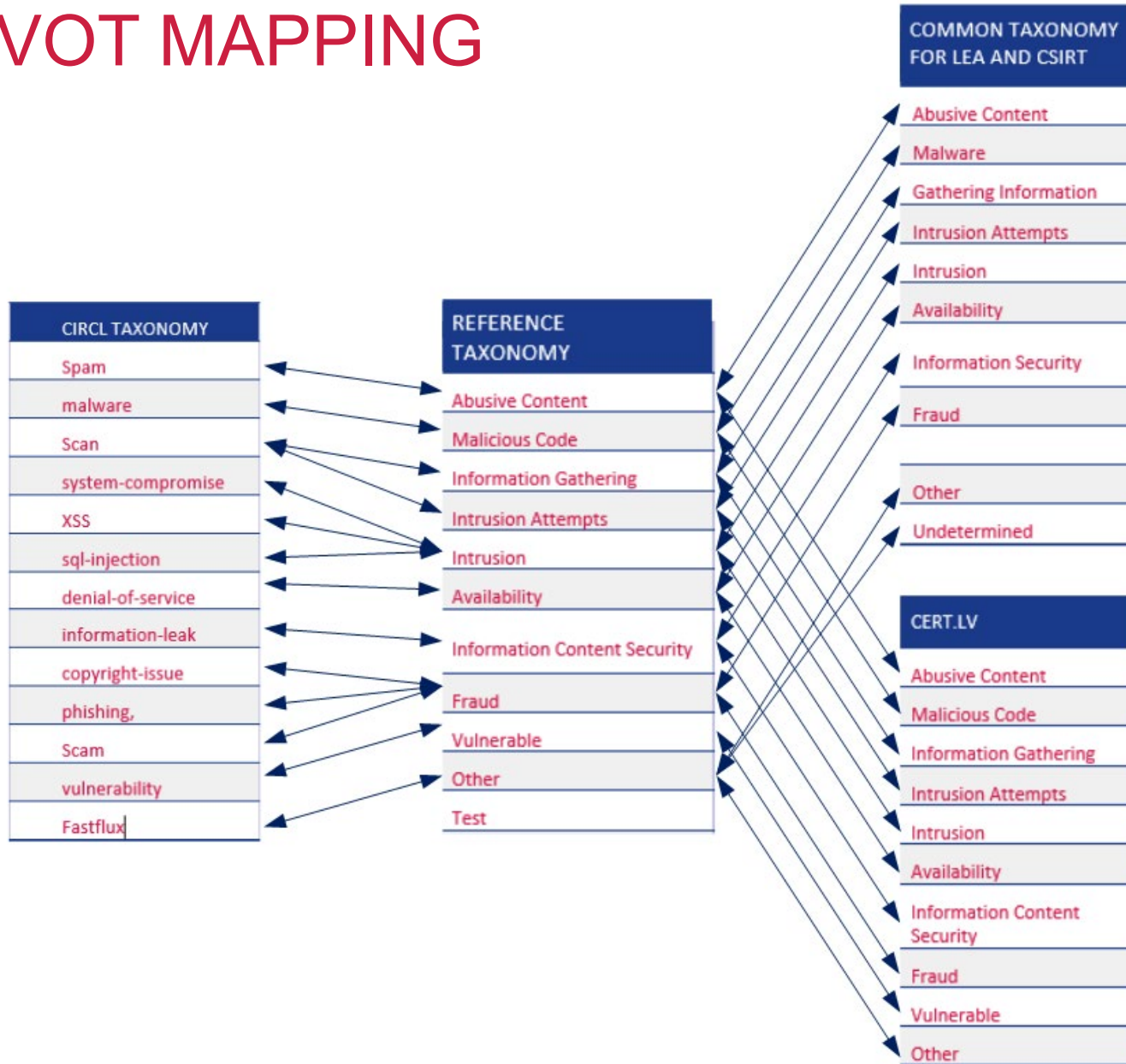
- Incident handling
- Incident reporting
- Media outreach
- Policy discussion
- Cross border incidents
- Pivot mapping with existing initiatives

Statistics

- Performance and internal KPIs
- Comparison with other entities
- Trends
- Global / annual overview
- Explanation of external report

<https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/Documentation/Use%20Cases.md>

PIVOT MAPPING



HOW RSIT WG WORKS

Taxonomy text as a working copy on GitHub in MISP machine tag schema.

Use GitHub 's "pull request" feature to transparently document change requests via a JSON file .

Anyone can add or change text and he/she is allowed to propose these changes on GitHub via pull requests.

STARTING POINT ECSIRT.NET

Incident Classification	Incident Examples	Description / Explanation
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 <i>functionally comparable</i> content.
	<i>Harmful Speech</i> ¹	Discreditation or discrimination of somebody (e.g. cyber stalking, <i>racism and threats against one or more individuals</i>)
	Child/Sexual/ Violence/...	Child Pornography, glorification of violence, ...
Malicious Code ²	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	
	<i>Rootkit</i>	
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, ...), <i>port scanning</i> .
	Sniffing	Observing and recording of network traffic (<i>wiretapping</i>).
	Social Engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).

¹ Was "harassment" – legally the term "harmful speech" is more correct, as it includes harassment, discrimination and defamation

² "Malicious code" refers to malicious software inserted into a system. The vector that caused the insertion is not apparent here. The vector can be an "intrusion" from the outside, but also a USB stick, or other internal vector.



ADDITIONAL NEW FIELDS, UPDATE AND VERSIONING MECHANISM

After discussion, the WG decided to implement as of Version 1 of the taxonomy the following principles:

- The first column should be considered as being fixed in nature – maximum one change/year.
- The second column is considered as being more adaptable – two to three times/year.
- There must be a clearly defined update process for both columns.
- This process should include the history and version number of the changes (CHANGELOG file, etc.).



ADDITIONAL NEW FIELDS, UPDATE AND VERSIONING MECHANISM

- Every new version **MUST** have a new version number and this version number **SHOULD** be added as meta-data.
- Old versions **MUST** remain online.
- For changes and the addition of new fields, the process is the following:
- Members propose change(s) and/or additional field(s) together with their motivation and use case(s) to the mailing list/GitHub at least 30 working days before the next meeting of the working group.
- The WG will discuss the proposal(s) during the next physical meeting and vote.

Please note that:

- The first column is of the “**MUST**” (mandatory) type, the second column is of the “**SHOULD**” (recommended but not mandatory) type.

VERSION 1.1

CLASSIFICATION (1ST COLUMN)	INCIDENT EXAMPLES (2ND COLUMN)	Description / Examples
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.
Abusive Content	Harmful Speech	Discreditation or discrimination of somebody, e.g. cyber stalking, racism or threats against one or more individuals.
Abusive Content	(Child) Sexual Exploitation/Sexual /Violent Content	Child Sexual Exploitation (CSE), Sexual content, glorification of violence, etc.
Malicious Code	Infected System	System infected with malware, e.g. PC, smartphone or server infected with a rootkit.
Malicious Code	C2 Server	Command-and-control server contacted by malware on infected systems.
Malicious Code	Malware Distribution	URI used for malware distribution, e.g. a download URL included in fake invoice malware spam.
Malicious Code	Malware Configuration	URI hosting a malware configuration file, e.g. webinjects for a banking trojan.
Information Gathering	Scanning	Attacks that send requests to a system to discover weaknesses. This also includes testing processes to gather information on hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), port scanning.
Information Gathering	Sniffing	Observing and recording of network traffic (wiretapping).
Information Gathering	Social Engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).
Intrusion Attempts	Exploitation 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, backdoor, cross site scripting, etc.)

https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/working_copy/humanv1.md

FROM ECSIRT.NET TO RSIT V1.1

Incident Classification	Incident Examples	Description / Examples
Abusive Content	Spam	or "Unsolicited Bulk Email" without the recipient's permission for the collection of messages.
	Harmful Speech ¹	Discreditation or discrimination of somebody, e.g. cyber stalking, racism or threats against one or more individuals.
	Child/Sexual/Violence/...	Child Pornography
Malicious Code ²	Virus	Software that is inserted into a system without the user's consent. Interaction is not intended by the user.
	Worm	
	Trojan	
	Spyware	
	Dialer	
Rootkit		
Information Gathering	Scanning	Attacks that send requests to a system to discover weaknesses. This also includes testing processes to gather information on hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), port scanning.
	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).

¹ Was "harassment" – legally the term "harmful speech" is more appropriate.
² "Malicious code" refers to malicious software inserted into a system without the user's consent. Interaction is not intended by the user. It can be an "intrusion" from the outside, but also a USB stick, or a malware already present on the system.

CLASSIFICATION (1ST COLUMN)	INCIDENT EXAMPLES (2ND COLUMN)	Description / Examples
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.
Abusive Content	Harmful Speech	Discreditation or discrimination of somebody, e.g. cyber stalking, racism or threats against one or more individuals.
Abusive Content	(Child) Sexual Exploitation/Sexual /Violent Content	Child Sexual Exploitation (CSE), Sexual content, glorification of violence, etc.
Malicious Code	Infected System	System infected with malware, e.g. PC, smartphone or server infected with a rootkit.
Malicious Code	C2 Server	Command-and-control server contacted by malware on infected systems.
Malicious Code	Malware Distribution	URI used for malware distribution, e.g. a download URL included in fake invoice malware spam.
Malicious Code	Malware Configuration	URI hosting a malware configuration file, e.g. webinjects for a banking trojan.
Information Gathering	Scanning	Attacks that send requests to a system to discover weaknesses. This also includes testing processes to gather information on hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), port scanning.
Information Gathering	Sniffing	Observing and recording of network traffic (wiretapping).
Information Gathering	Social Engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).

FROM ECSIRT.NET TO RSIT V1.1

Intrusion Attempts ³	Exploiting of known Vulnerabilities	An attempt to compromise a system or to disrupt any service with a standardised identifier such as (scripting, etc.).	Intrusion Attempts	Exploitation 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, backdoor, cross site scripting, etc.)	
	Login attempts	Multiple login attempts (Guessing / cracking of passwords, brute force).		Intrusion Attempts	Login attempts	Multiple login attempts (Guessing / cracking of passwords, brute force).
	New attack signature	An attempt using an unknown exploit.		Intrusion Attempts	New attack signature	An attack using an unknown exploit.
Intrusions ⁴	Privileged Account Compromise	A successful compromise of a system or remotely by a known or new vulnerability includes being part of a botnet.	Intrusions	Privileged Account Compromise	Compromise of a system where the attacker gained administrative privileges.	
	Unprivileged Account Compromise			Compromise of a system using an unprivileged (user/service) account.		
	Application Compromise			Compromise of an application by exploiting (un)known software vulnerabilities, e.g. SQL injection.		
	Bot			Physical intrusion, e.g. into corporate building or data center.		
Availability	DoS	By this kind of an attack a system is blocked, delayed or the system crashes. DoS examples exist like mail-bombing, DDoS often is based on flood scenarios exist like DNS Amplification attack. However, the availability also can be affected by power supply, etc.) – or by Act of God, or gross neglect being involved.	Intrusions	Application Compromise	Compromise of an application by exploiting (un)known software vulnerabilities, e.g. SQL injection.	
	DDoS			Burglary	Physical intrusion, e.g. into corporate building or data center.	
	Sabotage			Denial of Service	Denial of Service attack, e.g. sending specially crafted requests to a web application which causes the application to crash or slow down.	
Information Content Security	Outage (no malice)	Outage caused e.g. by air condition failure or natural disaster.	Availability	Distributed Denial of Service	Distributed Denial of Service attack, e.g. SYN-Flood or UDP-based reflection/amplification attacks.	
	Unauthorised access to information			Misconfiguration	Software misconfiguration resulting in service availability issues, e.g. DNS server with outdated DNSSEC Root Zone KSK.	
Information Content Security	Unauthorised modification of information	Unauthorised modification of information, e.g. by an attacker abusing stolen login credentials for a system or application or a ransomware encrypting data.	Availability	Sabotage	Physical sabotage, e.g. cutting wires or malicious arson.	
				Outage	Outage caused e.g. by air condition failure or natural disaster.	
			Information Content Security	Unauthorised access to information	Unauthorized access to information, e.g. by abusing stolen login credentials for a system or application, intercepting traffic or gaining access to physical documents.	
				Information Content Security	Unauthorised modification of information	Unauthorised modification of information, e.g. by an attacker abusing stolen login credentials for a system or application or a ransomware encrypting data.
			Information Content Security	Data Loss	Loss of data, e.g. caused by harddisk failure or physical theft.	

³ An "attempt" refers to the mechanism used to try and create an intrusion. The intru

⁴ An "intrusion" will as rule of thumb be the result of a successful intrusion attempt

FROM ECSIRT.NET TO RSIT V1.1

Fraud	Unauthorized use of resources	Us
	Copyright	Of
	Masquerade	Typ
	Phishing	Me
Vulnerable	Open for abuse	Op
Other	All incidents which don't fit in one of the given categories should be put into this class.	If
Test	Meant for testing	Me

Fraud	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.
Fraud	Copyright	Offering or Installing copies of unlicensed commercial software or other copyright protected materials (Warez).
Fraud	Masquerade	Type of attack in which one entity illegitimately impersonates the identity of another in order to benefit from it.
Fraud	Phishing	Masquerading as another entity in order to persuade the user to reveal private credentials.
Vulnerable	Weak crypto	Publicly accessible services offering weak crypto, e.g. web servers susceptible to POODLE/FREAK attacks.
Vulnerable	DDoS amplifier	Publicly accessible services that can be abused for conducting DDoS reflection/amplification attacks, e.g. DNS open-resolvers or NTP servers with monlist enabled.
Vulnerable	Potentially unwanted accessible services	Potentially unwanted publicly accessible services, e.g. Telnet, RDP or VNC.
Vulnerable	Information disclosure	Publicly accessible services potentially disclosing sensitive information, e.g. SNMP or Redis.
Vulnerable	Vulnerable system	A system which is vulnerable to certain attacks. Example: misconfigured client proxy settings (example: WPAD), outdated operating system version, etc.
Other	Other unclassified	All incidents which don't fit in one of the given categories should be put into this class or the incident is not classified.
Other	Undetermined	The classification of the incident is unknown/undetermined.
Test	Test	Meant for testing.

© S-CURE bv, PRESECURE GmbH and SURFnet
 Arvidsson and Don Stikvoort are acknowledged
 author at don@elsinore.nl for the sake of future

MACHINE READABLE

```
312 lines (309 sloc) | 12.2 KB
Raw Blame History
1 {
2   "values": [
3     {
4       "entry": [
5         {
6           "description": "Or 'Unsolicited Bulk Email', this means that the recipient has not granted verifiable permission for the",
7           "expanded": "Spam",
8           "value": "spam"
9         },
10        {
11          "description": "Discreditation or discrimination of somebody, e.g. cyber stalking, racism or threats against one or more",
12          "expanded": "Harmful Speech",
13          "value": "harmful-speech"
14        },
15        {
16          "description": "Child Sexual Exploitation (CSE), Sexual content, glorification of violence, etc.",
17          "expanded": "(Child) Sexual Exploitation/Sexual/Violent Content",
18          "value": "violence"
19        }
20      ],
21      "predicate": "abusive-content"
22    },
23    {
24      "entry": [
25        {
26          "description": "System infected with malware, e.g. PC, smartphone or server infected with a rootkit.",
27          "expanded": "Infected System",
28          "value": "infected-system"
29        },
30        {
31          "description": "Command-and-control server contacted by malware on infected systems.",
32          "expanded": "C2 Server",
33          "value": "c2-server"
34        },
35        {
36          "description": "URI used for malware distribution, e.g. a download URL included in fake invoice malware spam.",
37          "expanded": "Malware Distribution",
38          "value": "malware-distribution"
39        }
40      ]
41    }
42  ]
43 }
```

DEPENDENCIES AND TOOL MAPPING

Incident Handling Automation



Threat Intelligence Platform



Security tools



Taxonomy users



Statistics based on the RSIT WG taxonomy





NEXT STEPS

Join us and help us developing the taxonomy and build a common language to better share future incidents

Via email

csirt-relations@enisa.europa.eu

IRL after this talk or stop by the ENISA booth

**BOF Reference Security Incident Taxonomy Working Group (RSIT WG):
Today Lowther Suite
17:00 – 18:00**

THANK YOU FOR YOUR ATTENTION

 +30 28 14 40 9711

 csirt-relations@enisa.europa.eu

 www.enisa.europa.eu

