EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ASPECTS OF COOPERATION BETWEEN CSIRTS AND LE

Toolset, Document for trainees

JANUARY 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, visit www.enisa.europa.eu.

CONTACT

For contacting the authors please use CSIRT-LE-cooperation@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

AUTHORS (IN ALPHABETICAL ORDER BY SURNAME)

Philip Anderson, Sandra Blanco Bouza, Smaragda Karkala (ENISA), Gregoire Kourtis, Alexandra Michota (ENISA), Catalin Patrascu, Silvia Portesi (ENISA), Václav Stupka, Koen Van Impe.

ACKNOWLEDGEMENTS

ENISA would like to thank the following people and organisations:

- The following subject matter experts, selected from the List of Network and Information Security (NIS) Experts compiled following the ENISA Call for Expressions of Interest (CEI) (ref. ENISA M-CEI-17-C01):
  - Philip Anderson, Sandra Blanco Bouza, Catalin Patrascu, Václav Stupka and Koen Van Impe, who, together with the ENISA project team, drafted the toolset;
  - François Beauvois and Yonas Leguesse who contributed as reviewers.
- Gregoire Kourtis, who provided input to the drafting of the toolset, in particular the graphical representations.
- Europol's European Cybercrime Centre (EC3) for the peer-review of the handbook from which this toolset is derived.
- The ENISA colleagues who provided input and reviewed the handbook from which this toolset is derived, in particular Jo De Muynck and Christian Van Heurck.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-463-3, DOI: 10.2824/2038

TABLE OF CONTENTS

1. INTRODUCTION

1.1 THEMATIC AREA

This training material has been developed based particularly on the *ENISA 2020 Report on CSIRT-LE Cooperation - A study of the roles and synergies among selected EU MS/EFTA countries*[1]. Some of the 2020 report's conclusions are that, in terms of incident response and cybercrime, the position and role of the computer security incident response teams (CSIRTs) and law enforcement (LE) in the national institutional framework varies from country to country. Similarly, the structure and the organisation of the judiciary also depends on the country.

In addition, between the three communities - CSIRTs, LE and judiciary - different approaches and different levels of cooperation exist. While the operational cooperation, especially in the daily interactions and informal communication, seems to be well-established, sometimes it seems that more structured cooperation could be achieved to have less fragmented information flow between the three communities. Also, there is a more significant gap in the interaction between CSIRTs and the judiciary, compared to the cooperation established between LE and the judiciary. CSIRTs would rather often interact with the judiciary in case they are called as an expert witness in court.

Moreover, LE is not solely involved in the detection and investigation of cybercrimes. A key component of their role is the preventive aspects of cybercrime, and it is in this role that cooperation with other communities, particularly the CSIRT community, becomes apparent to support preventive strategies. Preventive aspects of incidents/cybercrimes can also be seen as the initial ground for establishing cooperation between the CSIRTs and the LE communities, which can then extend to other phases of the incident/crime investigation. On the other hand, CSIRTs play an important role in informing (potential) victims of cybercrime and providing them with information on how to report a crime to the police.

CSIRT and LE communities also need to closely cooperate to mitigate the risks of having evidence compromised or destroyed.

Regarding the incident handling and cybercrime investigation, several competences are required. While each community has developed its own set of skills and knowledge, they can all benefit from the competences of the other communities.

Finally, the 2020 report on CSIRT and LE cooperation also concluded that despite the initiatives that are already in place to facilitate training within each community, or joint trainings engaging two communities (e.g. CSIRTs and LE, or LE and the judiciary), it seems that there is a need for more training and exercises addressing the three communities together.

The 2020 report on CSIRT and LE, the handbook and this toolset are a set of deliverables complementing each other as follows:

- The report analyses roles, duties, competences, synergies and potential interferences across the three communities (CSIRTs, LE and judiciary).
- The handbook helps the trainer explain these concepts through scenarios.
- The toolset contains exercises for trainees based on these scenarios.

[1] ENISA, 2020 Report on CSIRT-LE Cooperation - A study of the roles and synergies among selected EU Member States/EFTA countries, https://www.enisa.europa.eu/publications/2020-report-on-csirt-le-cooperation (26 January 2021)

1.2 LEARNING OUTCOMES

As a result of attending this training, the trainee should be able to:

- demonstrate knowledge of interactions across the three communities (CSIRTs, LE and judiciary); synergies, interferences and challenges
- use the SoD matrix to collect the data to identify the key responsibilities for their communities (CSIRTs, LE, and judiciary) and link them with the skills required to fulfil these duties
- better understand the legal and organisational framework defining the competences of CSIRTs, LE, and the judiciary, in their activities related to fighting cybercrime
- understand different decision-making processes among the communities
- capture potential synergies and possible overlaps
- overcome possible interferences of cooperation between CSIRTs and LE and their interaction with the judiciary
- ensure structured integration of liaison officers for coordination between the different communities
- perform uniform and effective communication between CSIRTs, LE and the judiciary toward victim and relevant stakeholders
- coordinate basic first responder actions at victim site (collecting evidence without tampering it, informing partners of which evidence is gathered)
- explain technical terms to non-technical participants, e.g. to the judiciary
- better translate legal constraints to CSIRTs
- identify appropriate approaches and tools to help support effective collaboration
- identify and develop a common plan to enhance cooperation

1.3 COURSE DURATION AND TRAINING OUTLINE

2-3 hours

1.4 COURSE CONTENTS

The training includes three scenarios where trainees learn when and how CSIRT members cooperate with LE when dealing with cyber security incidents. The three scenarios cover:

- Theft of confidential data
- Ransomware
- DDoS and malware blended attack

2. CASE STUDIES

2.1 CASE STUDY 1: THEFT OF CONFIDENTIAL DATA

Figure 1: Overview of case study 1

Overview of the case study 1	
Targeted Audience	This exercise is useful for incident responders and members of law enforcement of all experience levels. It is particularly helpful for national CSIRT members and law enforcement officers involved in cybercrime investigations
Total Duration	45 minutes
Scenario	This is a group exercise. Each trainee is a member of CSIRT, LE or the judiciary who is involved in the prevention, mitigation and investigation of the cybersecurity incident/crime. Their goals are to address key ramifications resulting from the theft of confidential data, identify synergies that could be exploited by cooperating with the other communities, and potential interferences in case of lack of cooperation/coordination
Task 1	Identify and describe the organisational profile
Task 2	Describe measures that CSIRT and/or LE can take to prevent the incident/crime
Task 3	Use the SoD Matrix to analyse possible duties (tasks), synergies and potential interferences between CSIRT, LE and the judiciary
Task 4	List possible measures that CSIRT and/or LE can take during the incident response/crime investigation while performing different duties
Task 5	Group discussion on balancing the incident mitigation (asset protection) and criminal investigation (evidence collection and preservation)

2.1.1 Objectives

In this exercise, the trainees will learn when and how CSIRT, LE, and judiciary representatives can cooperate. In particular, the objectives of the exercise are to:

- Understand and appreciate the specifics of CSIRT/LE activities
- Analyse roles of different actors and how they can cooperate
- Identify synergies that can be exploited
- Grasp the complexity of cooperation

2.1.2 Scenario

2.1.2.1 Setting the stage

This scenario describes an incident where carefully selected individuals working for different Member States (MS A, MS B, and MS C) subscribe to a fake event. The event website mimics an event organized by an EU Commissioner and contains malicious documents. Once installed on the victim's computer, the malware included in the document exfiltrates domain and VPN access login credentials and selected documents with sensitive information. The credentials and the sensitive information is then monetized by the attacker via a semi-public website.

The internal security team of the Ministry of Education of MS A, to which one of the victims belongs, detects the incident. The internal security team of the Ministry of Education of MS A notifies the MS A national CSIRT, which in turn contacts law enforcement (of MS A).

The location where the exfiltration of data took place is in European MS D - whereas the website making the exfiltrated data available is located in Country Z, a non-EU/EFTA country.

In this case study, we use the concept of lanes to describe two distinct events that are part of the same security incident. The concept of lanes is used to demonstrate to the students that different security events which at first seem unrelated, can in fact be related to the same security incident. It is an opportunity for students to understand that separate investigations, started from different security events, will eventually merge because they deal with the same security incident. Students should cover both lanes to grasp the full details of the security incident.

Figure 2: Graphical representation of scenario 1 - Attack

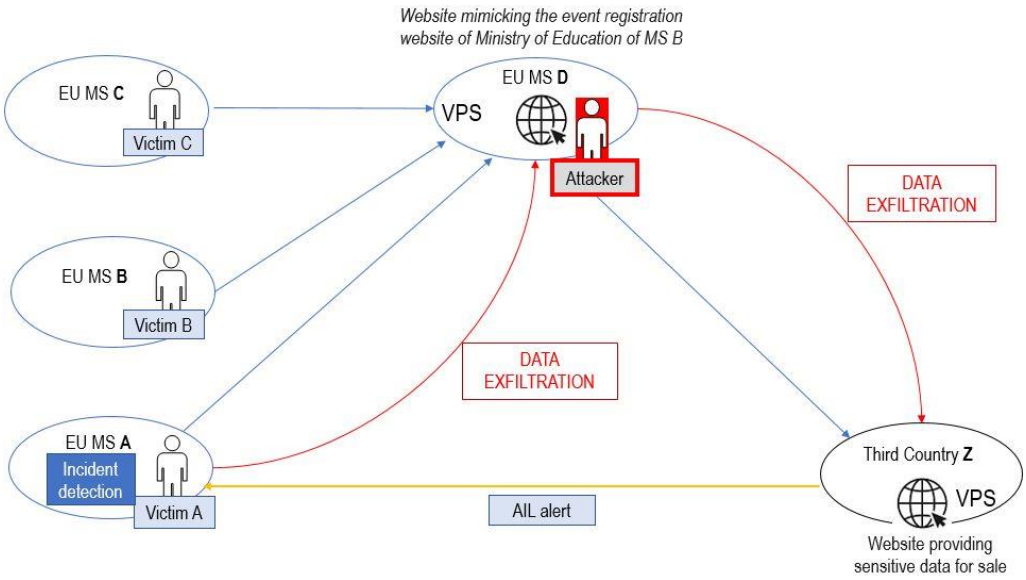
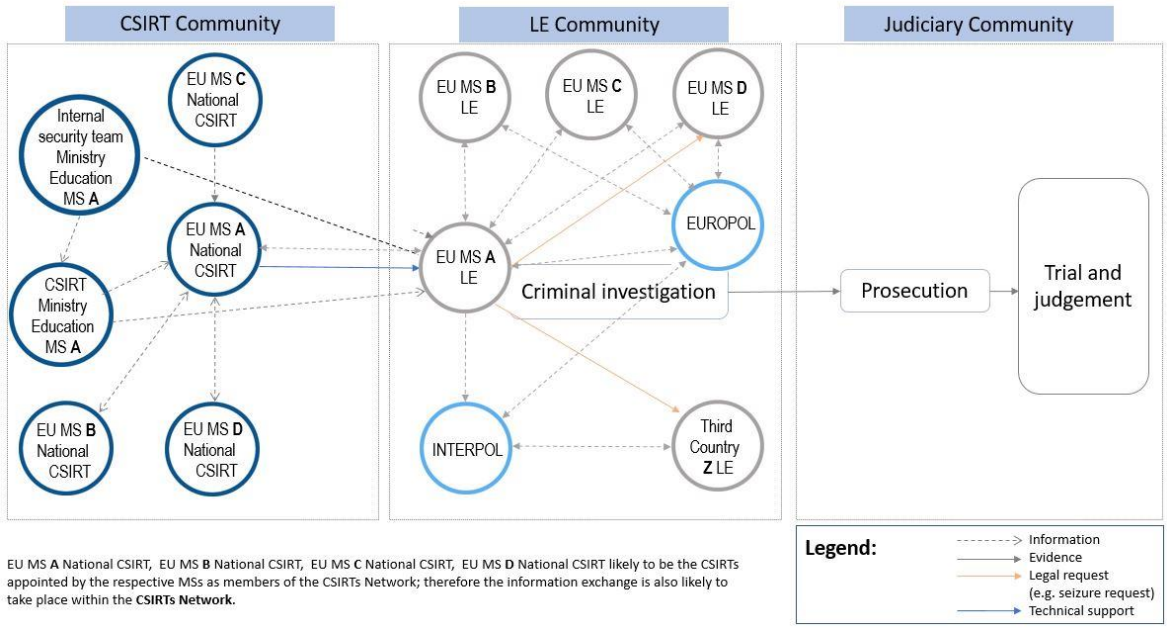


Figure 3: Graphical representation of scenario 1 – Overview of interactions



2.1.2.2 Before the breach

Reconnaissance

The attackers in this scenario spent a considerable amount of time on the reconnaissance of their potential new victim. They used online research of the Ministry of Education of MS A to find individuals of interest. They mapped out with whom these individuals typically collaborate, in particular with individuals at other ministries in MS A but also at Ministries of Education in other countries and with the European Commission. The attackers supplemented this information with the publicly available calendar information from the Commissioner.

The attackers used the following tactics and techniques:

Tactic TA0017 - Organizational Information Gathering[2]	"Organizational information gathering consists of the process of identifying critical organizational elements of intelligence an adversary will need about a target in order to best attack. Similar to competitive intelligence, organizational intelligence-gathering focuses on understanding the operational tempo of an organization and gathering a deep understanding of the organization and how it operates, in order to best develop a strategy to target it."[3]
Tactic TA0016 - People Information Gathering[4]	"People Information Gathering consists of the process of identifying critical personnel elements of intelligence an adversary will need about a target in order to best attack. People intelligence-gathering focuses on identifying key personnel or individuals with critical accesses in order to best approach a target for attack. It may involve aspects of social engineering, elicitation, mining social media sources, or be thought of as understanding the personnel element of competitive intelligence."[5]

[2] MITRE Corporation, *Organizational Information Gathering*, https://attack.mitre.org/tactics/TA0017/ (retrieved on 13 October 2020)
[3] MITRE Corporation, *Organizational Information Gathering*, https://attack.mitre.org/tactics/TA0017/ (retrieved on 13 October 2020)
[4] MITRE Corporation, *People Information Gathering*, https://attack.mitre.org/tactics/TA0016/ (retrieved on 13 October 2020)
[5] MITRE Corporation, *People Information Gathering*, https://attack.mitre.org/tactics/TA0016/ (retrieved on 13 October 2020)

Technique T1301 - Analyze business processes[6]	"Business processes, such as who typically communicates with who, or what the supply chain is for a particular part, provide opportunities for social engineering or other".[7]

The attackers then used one of the appointments in the Commissioner's calendar to set up a fake round table event to collect future views on a specific topic, hosted by the Ministry of Education of MS B. The attackers identified which individuals in the Ministry of Education of MS A would be the most interested in this topic. Then, the attackers set up fake personas to impersonate representatives of the Ministry of Education of MS B, and they created a website mimicking the event registration website of the Ministry of Education of MS B.

Technique T1295 - Analyze social and business relationships, interests, and affiliations[8]	"Social media provides insight into the target's affiliations with groups and organizations. Certification information can explain their technical associations and professional associations. Personal information can provide data for exploitation or even blackmail."[9]

Tactic TA0023 - Persona Development[10]	"Persona development consists of the development of public information, presence, history and appropriate affiliations. This development could be applied to social media, website, or other publicly available information that could be referenced and scrutinized for legitimacy over the course of an operation using that persona or identity." [11]

Initial access

Armed with a list of targets selected during reconnaissance, the attackers used the personas impersonating staff working for the Ministry of Education of MS B to send out invitations for the fake event. The event website requested that visitors enter personal information, and it contained documents, such as a call for proposals or Q&A, which were prepared by the attackers to include malicious code.

Technique T1566 - Phishing: Spear phishing Link[12]	"Adversaries may send spearphishing emails with a malicious link in an attempt to elicit sensitive information and/or gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments." [13]

[6] MITRE Corporation, *Analyze business processes*, https://attack.mitre.org/techniques/T1301/ (retrieved on 13 October 2020)
[7] MITRE Corporation, *Analyze business processes*, https://attack.mitre.org/techniques/T1301/ (retrieved on 13 October 2020) (See also the reference of *Gregory Scasny. (2015, September 14) "Understanding Open Source Intelligence (OSINT) and its relationship to Identity Theft"*, retrieved March 1, 2017)
[8] MITRE Corporation, *Analyze social and business relationships, interests, and affiliations*, https://attack.mitre.org/techniques/T1295/ (retrieved on 13 October 2020)
[9] MITRE Corporation, *Analyze social and business relationships, interests, and affiliations*, https://attack.mitre.org/techniques/T1295 / (retrieved on 13 October 2020) (See also the reference of *Gregory Scasny. (2015, September 14) "Understanding Open Source Intelligence (OSINT) and its relationship to Identity Theft"* as retrieved March 1, 2017.)
[10] MITRE Corporation, *Persona Development*, https://attack.mitre.org/tactics/TA0023/ (retrieved on 13 October 2020)
[11] MITRE Corporation, *Persona Development*, https://attack.mitre.org/tactics/TA0023/ (retrieved on 13 October 2020)
[12] MITRE Corporation, *Phishing:Spearphishing Link*, https://attack.mitre.org/techniques/T1566/002/ (retrieved on 13 October 2020)
[13] MITRE Corporation, *Phishing: Spearphishing,* https://attack.mitre.org/techniques/T1566/002/ (retrieved on 13 October 2020).

Execution

The event website included text to lure the visitors into opening the documents because they contained "essential" information on the event. The malicious documents were Office documents, with a blurred image and a text stating that to see the content, the user needed to "Enable Decryption via Enable Content", which enabled Word macros. Once the macro was enabled, it downloaded and ran the malicious executable file.

Technique T1204 - User Execution[14]	"An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behaviour from forms of Phishing."[15]

Credential access and Collection

The malicious executable was, in fact, a variant of a well-known keylogger specifically designed to collect credentials entered by a user when starting a VPN client. The captured credentials were regularly sent out to an external website. Apart from a keylogger, the malware was also able to collect files on the local system of the victim. It searched for specific types of files with particular names which were sent out to an external website.

MITRE Technique T1056 – Input Capture[16]	"Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. Credential API Hooking) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. Web Portal Capture)." [17]
Technique T1567 – Exfiltration Over Web Service[18]	"Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Popular Web services acting as an exfiltration mechanism may give a significant amount of coverage due to the likelihood that hosts within a network are already communicating with them prior to the compromise. Firewall rules may also already exist to permit traffic to these services. Web service providers also commonly use SSL/TLS encryption, giving adversaries an added level of protection." [19]
Technique T1029 – Scheduled Transfer[20]	"Adversaries may schedule data exfiltration to be performed only at certain times of the day or at certain intervals. This could be done to blend traffic patterns with normal activity or availability."[21]
Technique T1560 – Archive Collected Data[22]	"An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender."[23]
Technique T1005 – Data from local system[24]	"Adversaries may search local system sources, such as file systems or local databases, to find files of interest and sensitive data prior to Exfiltration."[25]

[14] MITRE Corporation, *User Execution*, https://attack.mitre.org/techniques/T1204/ (retrieved on 13 October 2020).
[15] MITRE Corporation, *User Execution*, https://attack.mitre.org/techniques/T1204/ (retrieved on 13 October 2020).
[16] MITRE Corporation, *Input Capture*, https://attack.mitre.org/techniques/T1056/ (retrieved on 13 October 2020).
[17] MITRE Corporation, *Input Capture*, https://attack.mitre.org/techniques/T1056/ (retrieved on 13 October 2020).
[18] MITRE Corporation, *Exfiltration Over Web Service*, https://attack.mitre.org/techniques/T1567/ (retrieved on 13 October 2020).
[19] MITRE Corporation, *Exfiltration Over Web Service*, https://attack.mitre.org/techniques/T1567/ (retrieved on 13 October 2020).
[20] MITRE Corporation, *Scheduled Transfer*, https://attack.mitre.org/techniques/T1029/ (retrieved on 13 October 2020).
[21] MITRE Corporation, *Scheduled Transfer*, https://attack.mitre.org/techniques/T1029/ (retrieved on 13 October 2020).
[22] MITRE Corporation, *Archive Collected Data*, https://attack.mitre.org/techniques/T1560/ (retrieved on 13 October 2020).
[23] MITRE Corporation, *Archive Collected Data*, https://attack.mitre.org/techniques/T1560/ (retrieved on 13 October 2020).
[24] MITRE Corporation, *Data from Local System*, https://attack.mitre.org/techniques/T1005/ (retrieved on 13 October 2020).
[25] MITRE Corporation, *Data from Local System*, https://attack.mitre.org/techniques/T1005/ (retrieved on 13 October 2020).

2.1.2.3 Initial response

Breach notification

Lane 1
During a weekly review of network activity, the security operations team of the Ministry of Education of MS A noticed that there was a substantial amount of outbound traffic to an external website located in MS D. Their initial investigation showed that the internal source of the traffic was on a network segment used by individuals working on sensitive material.

The security team of the Ministry of Education of MS A alerted its internal CSIRT and started collecting information on the affected assets.

Lane 2
At the same time, the CSIRT team of the Ministry of Education of MS A got an alert from one of their public crawlers. The team received an internal notification from the AIL framework[26] showing that there was a hit on the name of the Ministry of Education of MS A for a website located on a VPS in Country Z. The website was protected with a password and required payment to access it. It provided some screenshots and extracts of texts to show what type of information was available for potential "customers".

Upon inspection of the screenshot of the alert, they immediately spotted that the document contained sensitive information which shouldn't be publicly accessible.

The response of the CSIRT
The CSIRT handler on duty for the Ministry of Education of MS A classified the incidents according to the ENISA RSIT[27] as "Information Content Security", "Leak of confidential information".

The CSIRT requested the security operations team to safeguard the logs of the affected assets in their SIEM and use EDR tooling to capture live system memory and collect important system artefacts. Unfortunately, the EDR had not been deployed to all assets. In the meantime, the security operations team was able to isolate the system process responsible for the exfiltration of the data. Additionally, they still saw active network activity to the external website. This activity meant that the exfiltration was ongoing.

The CSIRT notified the CISO and the Secretary-General of the Ministry of Education of MS A of the possible security incident. A crisis team was formed, including the Press Officer, the legal department, the HR department and a representative of the General Secretariat of the Ministry of Education of MS A.

At this stage, it was unknown which type of data was exfiltrated. Still, because of the volume of data already exfiltrated and the type of assets (workstations and individuals involved), the CSIRT of the Ministry of Education of MS A suggested filtering traffic to the IP in MS D until further investigation. Additionally, according to the representative of the Ministry of Education of MS A, the screenshot in the AIL alert was of a document which had not been published and which was processed on one of the affected assets.

[26] GitHub, *CIRCL / AIL-framework*, https://github.com/CIRCL/AIL-framework (retrieved on 13 October 2020)
[27] GitHub, *enisaeu / Reference-Security-Incident-Taxonomy-Task-Force*, https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force (retrieved on 13 October 2020).

The CSIRT of the Ministry of Education of MS A immediately instructed the network team to filter all traffic to and from the IP in MS D.

The CISO of the Ministry of Education of MS A, together with the head of CSIRT of the Ministry of Education of MS A, contacted the national CSIRT of MS A to report the incident and LE of MS A to file a complaint.

Criminal investigation in MS A

LE officials of MS A were informed of the case details, including the fact that this concerned sensitive information and that there was a very high suspicion that data had been exfiltrated to a server in MS D.

LE conducted an investigation and went on-site to the Ministry of Education of MS A to review the available log material.

The CSIRT of the Ministry of Education of MS A provided LE with their collected reports on network traffic, together with the screenshots and information of the leaked documents on the server in Country Z, a non-EU/EFTA country.

The CSIRT of the Ministry of Education of MS A informed LE that the activity was still ongoing and that they implemented a network filter.

Investigation analysis

Because of the network filter, the malware was unable to contact the server in MS D. This triggered a failsafe mechanism, and it started encrypting all the files on the workstation.

The CSIRT of the Ministry of Education of MS A informed LE that the evidence on the workstation was most likely no longer usable. The logs in the SIEM were still available.

Lane 1

LE analysed the network traffic with support from the MS A national CSIRT. The logs clearly showed the volume of traffic to the server in MS D.

LE of MS A reached out to their contacts in MS D (with the support of Europol) requesting to seize the server and collect the evidence. Unfortunately, the hosting company, a bulletproof hoster, did not respond to the request. LE then attempted to get a warrant for the server.

Together with the information from the MS A national CSIRT, the LE created a timeline of events.

Lane 2

Based on the alert data of the CSIRT of the Ministry of Education of MS A, LE identified the hosting company where the website was offering the sensitive information. LE contacted their peers in Country Z (with the support of INTERPOL) to formally request the server be seized and investigated. They used the evidence received from the agency to support their case.

Criminal investigation in MS D

Lane 1

LE in MS D was able to identify the individuals that registered and set up the website and VPS. An investigation of the activity on the server showed that it was accessed multiple times via IP addresses belonging to VPN nodes, but also included one residential IP address from MS D. This most likely occurred after a glitch of the VPN killswitch exposed the IP of the user behind

the VPN. The activity on the server corresponded with the victim's VPN login attempts of stolen credentials.

Most of the logs included VPN node accesses, but also had one residential IP address from MS D, most likely after a glitch of the VPN service which exposed the IP of the user behind the VPN. The activity on the server corresponded with VPN login attempts of stolen credentials.

The server also had temporary copies of some of the sensitive documents, sorted according to the collection date.

The server in MS D, however, did not show any activity related to the server in the Country Z.

Lane 2
LE was unable to collect the server in Country Z because, by the time the hosting company received the request, the owners of the server had destroyed their VPS server.

However, LE was able to identify the individuals that purchased the VPS at the hosting company.

LE investigation did take different screenshots of the website before the server's destruction. These screenshots showed the nature of the site's documents, along with the methods used to request money to access the website.

LE / Prosecutor requested a warrant and seizure of the electronic devices of this individual.

LE investigation of the computers of the individuals in MS D showed that their devices contained traces of the sensitive documents. An examination of the SSH history, browser and e-mail activity also revealed frequent access to the server in Country Z.

The investigation also showed frequent open-source IM (instant messaging) conversations with another individual in MS D, not linked to the website in MS D but seemingly with a form of control on the server in Country Z.

The forensic investigation of these electronic devices showed that this individual had configured and set up the server in Country Z. The e-mail conversation stored on the devices showed an exchange of the content of the documents and methods of payment.

2.1.3 Tasks

2.1.3.1 Task 1: Identify and describe the organisational profile

Identify and describe the organisational profile; specifically, the main subjects (actors) involved in the scenario, in particular, CSIRT/LE and judiciary actors using the table below.

Figure 4: Subjects/Roles template

Subjects	Community (CSIRT, LE, Judiciary, other)	Specific role related to the scenario	Comments

2.1.3.2 Task 2: Describe measures that CSIRT and/or LE can take to prevent the incident/crime

Although the actual preventive measures for the prevention of the incident, such as implementing proper security controls and network segmentation, were already in place there are a couple of additional activities where CSIRT and/or LE can play an active role. Taking into account the SoD matrix in Annex B and especially the phase “prior to incident/crime”, which activities can you identify?

Use the template below to list the duties related to “prior to the incident/crime” phase (column 1) and the suggested measures (column 2). The last column (column 3) can be used to note additional comments.

Figure 5: Duty/Suggested measure template

Duty (task)	Suggested measure	Comments

2.1.3.3 Task 3: Use the SoD Matrix to analyse possible duties (tasks), synergies and potential interferences between CSIRT, LE and judiciary

Select some duties from column 1 of the SoD in Annex B and in relation to some of these duties, briefly describe the measures that could be taken by each community in the scenario.

The template below can be used by listing the duties (tasks) in column 1 (duties to be taken from column 1 of the SoD matrix in Annex B) and the synergies and potential interferences in column 2. Column 3 can be used to add comments.

Figure 6: Duties, synergies and potential interferences - Template

Duty (task)	Synergies and potential interferences	Comments

2.1.3.4 Task 4: List possible measures that CSIRT and/or LE can take during the incident response/crime investigation while performing the different duties

List possible measures that CSIRT and/or LE can take during the incident response/crime investigation while performing the different duties.

Column 1 should be used to list the duties (tasks) taken from the SoD matrix in Annex B, in particular duties during the incident/crime (duties 7 to 22 of the SoD matrix in Annex B). Column 2 should be used for the suggested measures related to each duty with specific reference to the scenario. Column 3 can be used for comments.

Figure 7: Duty/suggested measure template

Duty (task)	Suggested measure	Comments

2.1.3.5 Task 5: Discussion on lessons learned from this scenario

Discuss the issue of balancing the incident mitigation (asset protection) and the criminal investigation (evidence collection and preservation) with reference to the scenario.

One of the responses of the CSIRT of the Ministry of Education of MS A involves filtering outgoing network activity to the attackers, effectively preventing the further exfiltration of sensitive information. This filtering is an understandable activity, certainly as a short-term containment measure. The side-effect of this measure, however, triggers the malware and results in encrypted workstations, and as such a loss of evidence.

Discuss the pros and cons of short-term containment actions to protect the victim, but which might alert the attacker that they have been detected. In general, this depends on the type of incident and the victim.

As a reference, the courses of action matrix from Lockheed Martin[28] can be use. This action matrix includes two significant categories of actions:

- passive (Discover and Detect)
- active (Deny, Disrupt, Degrade, Deceive and Destroy)

Note that this discussion is not about the chain of custody as such, but rather which options to choose for either taking an active or passive approach in containing an incident.

2.1.4 Lessons Learned

Theft of confidential data is rather complex and demands different skills, including technical and legal.

Although for training purposes the scenario is presented as less complicated than real cases might be, it still allows each party to understand the complexities in terms of actors involved, roles played, duties (tasks) performed, synergies to exploit, and risks of interference.

[28] Eric M. Hutchins E. M., Clopperty M. J., Amin R. M., *Lockheed Martin Corporation Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf (retrieved on 20 October 2020)

2.2 CASE STUDY 2: RANSOMWARE

Figure 8: Overview of case study 2

Overview of case study 2	
Targeted Audience	This exercise is useful for incident responders and members of law enforcement of all experience levels. It is particularly helpful for national CSIRT members and law enforcement officers involved in cybercrime investigations.
Total Duration	45 minutes
Scenario	This is a group exercise. Each trainee is a member of either a CSIRT team and/or law enforcement that is involved in the prevention, mitigation and investigation of cybersecurity incidents. Their goal is to address the key ramification of a ransomware attack against the municipal hospital.
Task 1	Notification of the incident
Task 2	Setting up the task force, division of duties
Task 3	Possible duties (tasks), synergies and potential interferences between CSIRT, LE and the judiciary
Task 4	Incident handling, evidence collection, cooperation
Task 5	International cooperation and information sharing
Task 6	Post-incident preventive measures

2.2.1 Objectives

In this exercise, the trainees will learn when and how CSIRT members cooperate with LE. In particular, the objectives of the exercise are to:

- Explain CSIRT and LE cooperation in a health sector-related ransomware scenario
- Raise the trainees' awareness regarding the differences between the legal systems of various countries and the consequences of these differences
- Understand and appreciate the specifics of CSIRT/LE activities
- Practice setting up and coordinating a task force for dealing with large scale attacks
- Provide information on how to cooperate and share information
- Practice how to identify and propose post-incident reactive and preventive measures

2.2.2 Scenario

2.2.2.1 Setting the stage

A ransomware attack has been discovered in a large municipal hospital on the hospital patient records servers. All computers are locked and display a message indicating that the files have been encrypted; the hacker is demanding 11 bitcoins (approx. €100,000) to provide the decryption key. The image on the computer screens also states that if the payment is not received within five days, the price will increase. Within ten days, the patient data will be erased on the servers and leaked to a public website, and a notification will be sent to the national data privacy agency.

You are a member of a task force established to help the hospital's network and information security team to deal with the incident. You have been assembled; it is now 05:45. It appears that all significant servers are affected. An initial assessment shows that the hospital email system and patient record systems are inaccessible, and the hospital intranet sites are also unavailable.

Figure 9: Graphical representation of scenario 2 – Attack

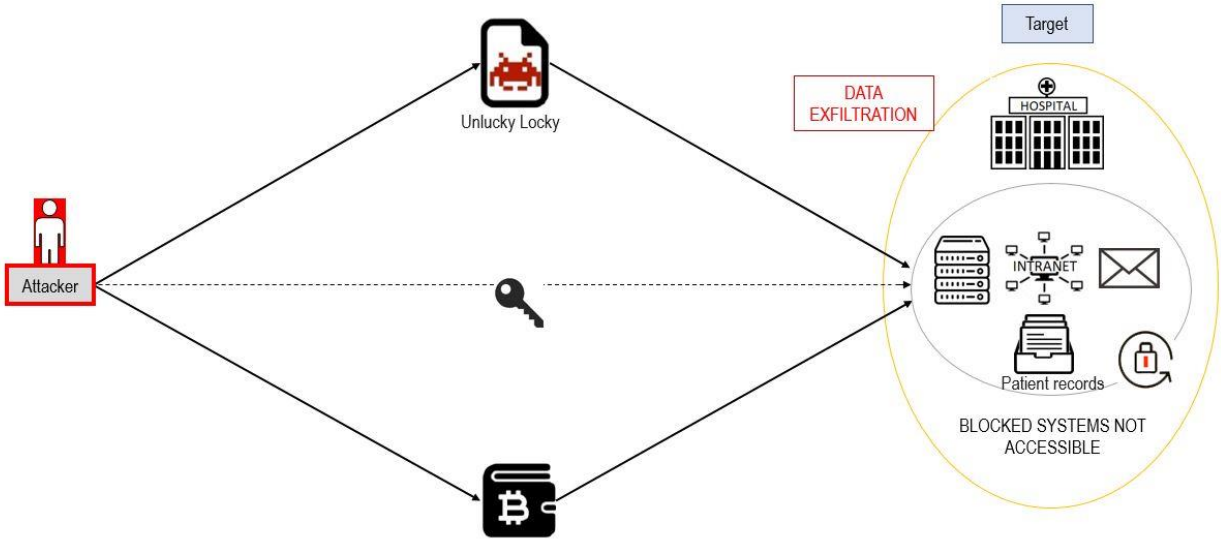
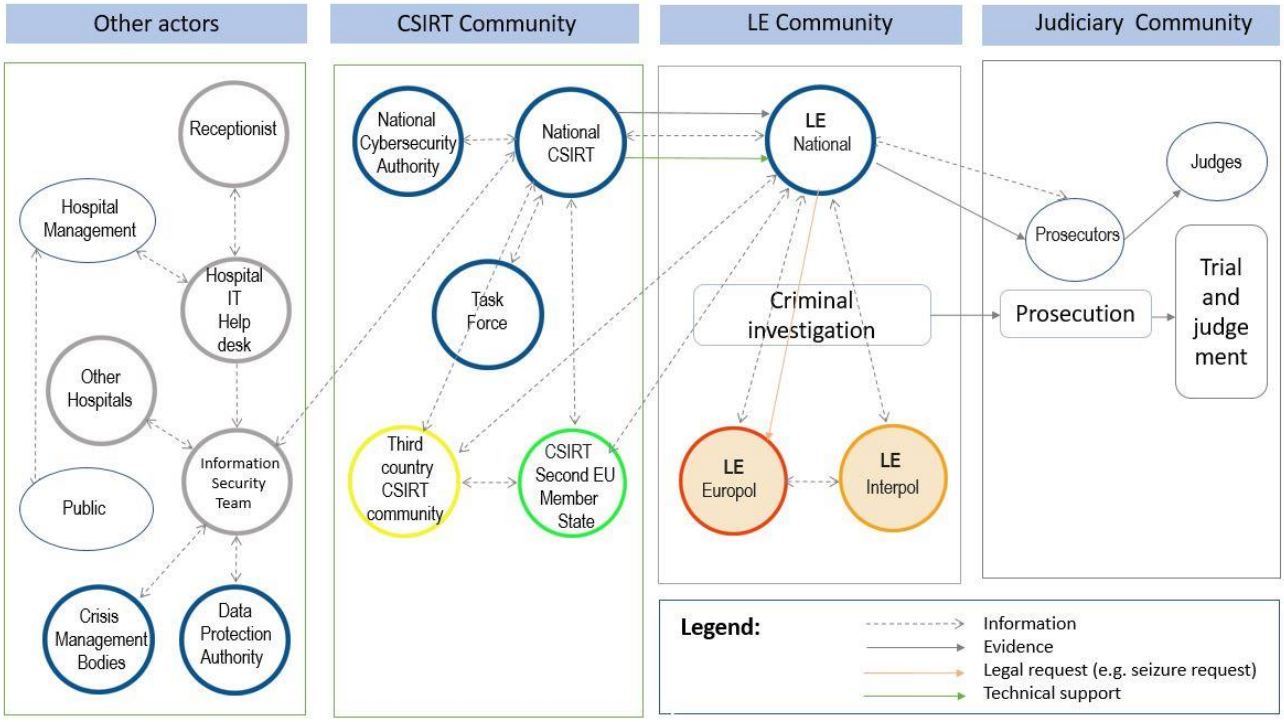


Figure 10: Graphical representation of scenario 2 – Overview of interactions



2.2.2.2 Organisational profile

The hospital is the largest municipal hospital in your area. Last year the hospital took care of almost 1 million patients and had about 5,000 employees. As such, the hospital relies on a network with up to 10,000 connected devices, which includes workstations, diagnostic tools and servers storing patients' data. Outside exposure is important through several hundreds of public IP addresses. In recent years, hospital management was somewhat reluctant to invest in cybersecurity, and even though most computers are relatively well taken care of, some, especially those operating specialised equipment, are running legacy systems like Windows XP, due to compatibility issues. The network is not segmented, and critical systems are in the same network as specialised equipment, as well as all workstations. The hospital has no clear rules on data management and backup. Patient data that are stored in the hospital's information systems are backed up and protected from ransomware. Still, a lot of relevant data about currently hospitalised and treated patients are not stored in the information systems, but on the doctors' workstations, which are not being backed up.

2.2.2.3 Before the breach

The COVID-19 pandemic is still very much going on, which leads to heavy pressure on your country's hospital system. Some cybercriminals decided to take advantage of this situation and started targeting medical facilities with their ransomware campaigns. The hospital's security team issued and distributed a directive that explained this threat to the employees and informed them how to be cautious and prevent their devices from getting infected with malware.

2.2.2.4 Initial response

Breach notification

When a receptionist in the X-ray department tried to log in at the start of her shift, she could not open the files and a message indicating that the files have been encrypted appeared on her screen. She notified a supervisor who then called the hospital's IT helpdesk to report what happened, who in turn notified the hospital's network and information security team.

The response of the CSIRT team

The hospital's network and information security team handler received the alert from the hospital staff and identified it as a high priority threat. The handler classified it according to the ENISA RSIT[29] as an incident of "Information Content Security", "Unauthorised modification of information", caused by the ransomware.

From an initial analysis, it appeared that the ransomware was called UnluckyLocky, a new type of ransomware with limited online information. Therefore, it was assumed that there was no known decryption key. The handler uncovered a news report online that described another hospital that seemed to have been infected by a similar attack with ransomware named Gotcha. The news article suggested that the response to the incident was slow and that almost all the computers and servers were infected. Additionally, the public was made aware of the incident as it had a significant impact on the hospital not being able to offer essential services. The incident went on for six days during which time even the hospital's most basic functionality was forced to stop.

The handler then attempted to identify the source of the ransomware with the limited publicly available information on UnluckyLocky published by the respected security company.They were able to find out that the source was a malicious website that informed about the Covid-19 pandemic and offered for download a tool for analysis of the decease symptoms. The executable, however, contained malicious code that was executed by the user who downloaded it from the website.

Technique T1204 - User Execution[30]	"An adversary may rely upon specific actions by a user to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behaviour from forms of Phishing." [31]

Upon execution, the malware first enumerated and exfiltrated the data, then encrypted the data within the target computer system and any connected storages. This rendered most of the data unavailable to the user while still allowing the user to operate the essential functions of the computer system. The malware also regularly prompted a window warning the user that the system was encrypted and decryption keys would be provided upon payment of the ransom.

Technique T1486 - Data Encrypted for Impact[32]	"Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted. In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted. In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR." [33]

The malware also regularly launched a task that attempted to spread the malicious code via email messages sent to stored addresses.

[29] GitHub, *enisaeu / Reference-Security-Incident-Taxonomy-Task-Force*, https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force (retrieved on 13 October 2020.
[30] MITRE Corporation, *User Execution,* https://attack.mitre.org/techniques/T1204/ (retrieved on 13 October 2020).
[31] MITRE Corporation, *User Execution,* https://attack.mitre.org/techniques/T1204/ (retrieved on 13 October 2020).
[32] MITRE Corporation, *Data Encrypted for Impact*, https://attack.mitre.org/techniques/T1486/ (retrieved on 13 October 2020).
[33] MITRE Corporation, *Data Encrypted for Impact*, https://attack.mitre.org/techniques/T1486/ (retrieved on 13 October 2020).

Technique T1053 - Scheduled Task/Job[34]	"Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically requires being a member of an admin or otherwise privileged group on the remote system." [35]

The handler proceeded to analyse the extent of the issue by randomly checking workstations within the hospital for signs of the malware. He found out that the malware managed to spread across the whole hospital, rendering some of the critical data and equipment unavailable.

The hospital's network and information security team was overwhelmed by the attack, so they reached out to the national CSIRT.

Note: In this scenario, you are a member of the national CSIRT that is helping the hospital with this security breach.

Criminal investigation

The national cybersecurity authority reported this incident to law enforcement. The police cyber unit started the investigation. They immediately contacted the national CSIRT, which provided general information, a sample of the ransomware and a link to the source website. A sample was sent to Europol through the EMAS sandbox for crossmatching.

The police found out that the website was hosted by a web hosting provider based in one of the EU MSs. They ordered the provider, via European investigation order, to provide stored subscriber and traffic data related to the relevant account.

Provided data revealed that the malicious content was uploaded from a country outside the EU. Even though the police immediately requested legal assistance and also asked Europol for assistance, based on past experiences with this particular country, it was virtually impossible to get any cooperation in such cases from the official authorities.

Information sharing

Even though it was unlikely that LE would get assistance through official channels, in the third country there is a well-functioning CSIRT community which is regularly and openly sharing information. The national CSIRT involved in dealing with the incident offered LE to request traffic data if they are given identifiers provided by the web hosting provider.

2.2.3 Tasks

2.2.3.1 Task 1: Notification of the incident

As stated above, the hospital's network and information security team notified the national cybersecurity authority of the incident. Who else should be notified within and outside of the hospital? Are there any legal obligations for the hospital to report such incidents to public institutions?

Use the template below to list individuals, authorities and other parties that should be informed about the incident. Column 1 should be used to list the parties to be notified and column 2 to identify whether the notification is required or recommended. Column 3 can be used for comments.

[34] MITRE Corporation, *Scheduled Task/Job*, https://attack.mitre.org/techniques/T1053/ (retrieved on 13 October 2020).
[35] MITRE Corporation, *Scheduled Task/Job*, https://attack.mitre.org/techniques/T1053/ (retrieved on 13 October 2020).

Figure 11: Notification list – Template

Who to notify	Required / recommended	Comments
Within the organisation		
Outside the organisation		

2.2.3.2 Task 2: Setting up the task force, division of duties

The national cybersecurity authority decided that a task force should be established to deal with the crisis. Who should be involved in this task force (e.g. which organisations or [inter]national authorities, the expertise level of members of the task force)? Are there any rules on this in your country?

Use the template below to list individuals/organisations that should be involved in the task force. Column 1 should be used to list the parties to be involved, column 2 to identify what kind of expertise can they contribute and column 3 to identify which tasks they can be involved in and what role should they play. Column 4 can be used for comments. Afterwards, discuss whether there are any relevant rules or best practices on this in your country.

Figure 12: Task force members list - template

Organisation	Expertise	Tasks/role	Comments

The university that cooperates with the hospital offered their volunteer ICT experts (students and employees) who can help to deal with the crisis. Can they be involved? In which activities (e.g. reinstallation of hospitals computers, incident handling, attempting to break the encryption, track the source of the attack, etc.)?

Explain which activities related to the incident handling can volunteers be involved and how. Column 1 should be used to name the activity and column 2 to describe the involvement.

Figure 13: Involvement of volunteers - Template

Activity	Description

Figure 14: Duties, synergies and potential interferences – Template

Duty (task)	Synergies and potential interferences	Comments

2.2.3.3 Task 3: Possible duties (tasks), synergies and potential interferences between CSIRT, LE and the judiciary

Select some of the duties from column 1 of the SoD in Annex B and with some of these duties, briefly describe the measures to that could be taken by each community in the scenario.

The template below can be used by listing the duties (tasks) in column 1 (to be taken from column 1 of the SoD matrix in Annex B) and the synergies and potential interferences in column 2. The last column, column 3, can be used to add comments.

Figure 15: Duties, synergies and potential interferences – Template

Duty (task)	Synergies and potential interferences	Comments

2.2.3.4 Task 4: Incident handling, evidence collection, coordination

Experts in the task force found out by using sandbox analysis that the ransomware is not only encrypting data from the information systems but is also exfiltrating patient data outside the organisation. CSIRT members immediately proposed to block communication to the C&C server to prevent further disclosure of sensitive information. LE, however, suggested to wait with this measure and try to track the data in an attempt to locate the attacker, since they're suspecting that the attacker is based in the EU even though he used servers located in third countries to disseminate the malware.

Explain, how you would deal with this issue, what should have priority – protection of sensitive data or locating the attacker, and whether there are any official rules on this in your country?

The template below can be used by listing the duties (tasks) in column 1 (to be taken from column 1 of the SoD matrix in Annex B) and the measures to be taken to deal with the issue in column 2. The last column of the template below, column 3, can be used to add comments.

Figure 16: List of suggested measures to deal with mutual interferences – Template

Duty (task)	Suggested measure	Comments

2.2.3.5 Task 5: International cooperation and information sharing

As stated above, the CSIRT offered LE, they can ask the third country network operators to unofficially provide traffic data that could help to identify the attacker.

Explain whether LE would be able to provide the CSIRT with necessary identifiers and traffic data acquired from the web hosting provider for this purpose. Also, whether the unofficial data collected by the third country network operator that leads to identifying the attacker would be usable as evidence in court by LE.

Figure 17: Information sharing and use – Template

Information sharing and use
Sharing information with the CSIRT
Use of the data unofficially obtained by the CSIRT

2.2.3.6 Task 6: Post incident preventive measures

Explain based on information you have about the incident and hospitals systems, what kinds of post incident preventive measures would you recommend to the Network and Information Security Team to implement.

The template below can be used to categorise proposed measures in column 1 (whether these measures are organisational, technical or legal by nature), and list and describe the proposed measures in column 2 and 3. The last column of the template below, column 4, can be used to identify who should implement these suggested measures.

Figure 18: List of preventive post-incident security measures – Template

Category (e.g. organisational, technical, legal)	Measure	Description	To be implemented by

2.2.4 Lessons Learned

Ransomware cases are rather complex and demand many different skills, including technical and legal, as well as the ability for other communities to share information and cooperate.

Although for training purposes the scenario is presented as less complicated than real cases might be, it still allows each party to understand the complexities in terms of actors involved, roles played, duties (tasks) performed, synergies to exploit, and risks of interference.

2.3 CASE STUDY 3: DDOS AND MALWARE BLENDED ATTACK

Figure 19: Overview of case study 3

Overview of case study 3	
Targeted Audience	This exercise is useful for incident responders and members of the law enforcement of all experience levels. It is particularly helpful for national CSIRT members and law enforcement officers involved in cybercrime investigations
Total Duration	30 minutes
Scenario	This is a group exercise. Each trainee is a member of either the CSIRT team and/or law enforcement who is involved in the prevention, mitigation and investigation of cybersecurity incidents. Their goal is to address the key ramification of a DDoS and malware blended attack against a large size airport in a European capital city
Task 1	Notification of the incident
Task 2	Setting up task force, division of duties
Task 3	Possible duties (tasks), synergies and potential interferences between CSIRT, LE and the judiciary
Task 4	International cooperation and information sharing
Task 5	Post incident preventive measures

This case study should be conducted in groups so that different results and approaches of each group can be compared. Then, the advantages and disadvantages of individual solutions should be discussed.

2.3.1 Objectives

The current exercise scenario aims to familiarize the trainees with technical, procedural and legal aspects of incident management. In particular, the objectives are to:

- Raise awareness about what types of cyber incidents might affect an airport and what can be the impact of such incidents
- Learn about the role of the CSIRT, Law Enforcement, and National Cybersecurity Authority
- Understand the importance of efficient coordination between main stakeholders during a large scale/high impact incident
- Practice setting up and coordinating task force for dealing with large scale attack
- Understand the importance of information sharing during cybersecurity attacks
- Practice how to identify and propose post-incident reactive and preventive measures
- Learn about preventive measures against such type of incidents

2.3.2 Scenario

2.3.2.1 Setting the stage

A large size airport in a European capital city is under massive DDoS attack, combined with a malware attack, causing key systems outages and malfunctioning (i.e. systems assuring functions like flight scheduling, passengers' check-in, baggage routing, etc.).

Already the situation has had significant adverse effects on the airport's operations and safety. Undetected attacks resulted in the change of the flight plans provoking delays and influencing the aircrafts cleaning and fuelling process, as well as the time required to load the luggage, affecting the world-wide traffic.

You are a member of a task force established to help the airport company to deal with the incident. An initial assessment shows that the IT team has yet to come up with a course of action for stopping the attack and restoring the services. The pressure from the media, authorities, and passengers is rapidly growing.

Figure 20 Graphical representation of scenario 3 – Attack

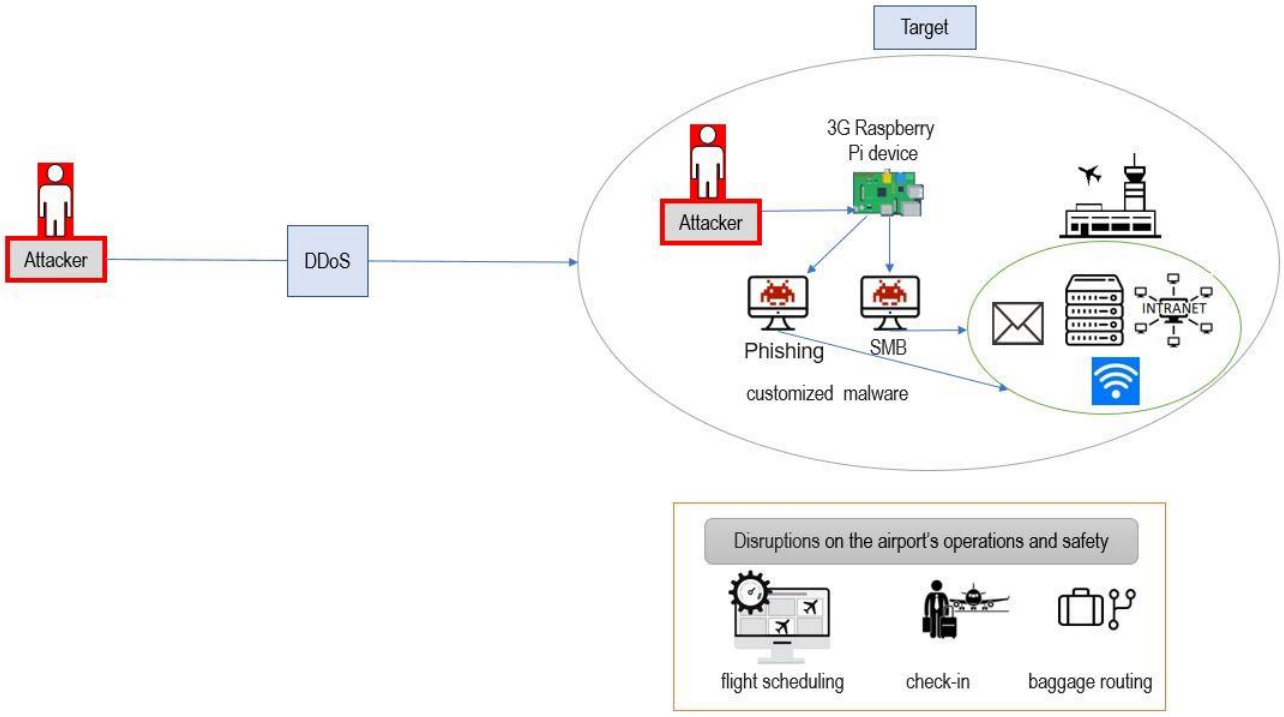
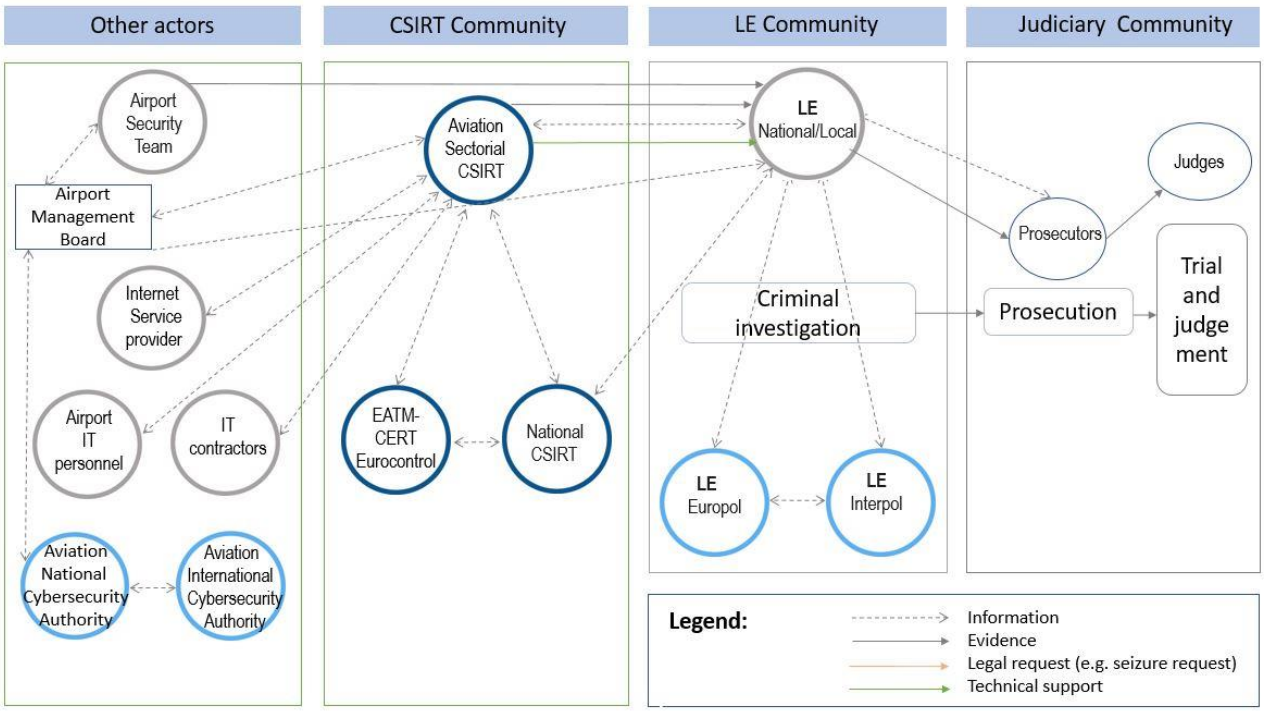


Figure 21: Graphical representation of scenario 3 – Overview of interactions



2.3.2.2 Organisational profile

The affected airport is one of the biggest air traffic hubs in Europe, with an average of more than 100,000 passengers passing through per day.

The management of the airport invested only in perimetral security in recent years (firewalls, gateways, etc.). At the same time, internal network suffers from lack of proper segmentation, and some of the critical systems are running old operating systems due to legacy and compatibility constraints.

The airport is running its own on-prem data centre doubled by a disaster recovery site, but the BCP plan wasn't tested in the last two years.

2.3.2.3 Before the breach

The attackers gathered information online about the airport company and identified useful data: the IP addresses space, systems and applications, management and key personnel names and contact details, etc.

Reconnaissance was also done at the physical perimeter of the airport by attackers disguised as passengers.

Attackers managed to plant a rogue 3G Raspberry Pi device in the airport network. The device is used to sniff the network traffic for systems discovery and credentials extraction (plain-text credentials sent over the network or easy-to-crack hashes).

While the attacker created a diversion with the DDoS attack, some of the internal systems of the airport were infected with a customized malware delivered using two different infection vectors: spear-phishing emails sent from the rogue device to avoid email gateway filtering, and Windows SMB exploits launched from the same device.

Technique TA0015 – Technical information gathering[36]	"Technical information gathering consists of the process of identifying critical technical elements of intelligence an adversary will need about a target in order to best attack. Technical intelligence gathering includes, but is not limited to, understanding the target's network architecture, IP space, network services, email format, and security procedures". [37]
Technique TA0016 – People information gathering[38]	"People Information Gathering consists of the process of identifying critical personnel elements of intelligence an adversary will need about a target in order to best attack. People intelligence gathering focuses on identifying key personnel or individuals with critical accesses in order to best approach a target for attack. It may involve aspects of social engineering, elicitation, mining social media sources, or be thought of as understanding the personnel element of competitive intelligence". [39]
Technique T1465 – Rogue Wi-Fi access points[40]	"An adversary could set up unauthorized Wi-Fi access points or compromise existing access points and, if the device connects to them, carry out network-based attacks such as eavesdropping on or modifying network communication". [41]
Technique T1566.001 – Spearphishing attachment[42]	"Adversaries may send spearphihing emails with a malicious attachment in an attempt to elicit sensitive information and/or gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution". [43]
Technique T1210 - Exploitation of Remote Services[44]	"Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. The exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system."[45]

2.3.2.4 Initial response

Breach notification

A lot of people are reporting at the check-in desks that their flights seem to have disappeared from the schedule display systems or they have long delays. At the same time, people can't obtain information from other online sources because the internet is inaccessible from the airport Wi-Fi network and even if they use their 3G/4G/5G connection the airport website and other related platforms are unavailable.

It becomes clear that the IT infrastructure and applications are affected by an incident, and a cyber-attack is suspected. The network team starts to investigate, and they report that a huge DDoS attack is conducted against the airport's internet-facing systems.

The security team is also reporting that a high number of database operations were executed in a short interval of time using credentials of a user that is claiming to know nothing about the situation.

[36] MITRE Corporation, *Technical information gathering,* https://attack.mitre.org/techniques/TA0015/ (retrieved on 13 October 2020).
[37] MITRE Corporation, *Technical information gathering,* https://attack.mitre.org/techniques/TA0015/ (retrieved on 13 October 2020).
[38] MITRE Corporation, *People information gathering,* https://attack.mitre.org/techniques/TA0016 (retrieved on 13 October 2020).
[39] MITRE Corporation, *People information gathering,* https://attack.mitre.org/techniques/TA0016 (retrieved on 13 October 2020).
[40] MITRE Corporation, *Rogue Wi-Fi access points,* https://attack.mitre.org/techniques/T1465 (retrieved on 13 October 2020).
[41] MITRE Corporation, *Rogue Wi-Fi access points,* https://attack.mitre.org/techniques/T1465 (retrieved on 13 October 2020).
[42] MITRE Corporation, *Spearphishing attachment,* https://attack.mitre.org/techniques/T1566.001 (retrieved on 13 October 2020).
[43] MITRE Corporation, *Spearphishing attachment,* https://attack.mitre.org/techniques/T1566.001 (retrieved on 13 October 2020).
[44] MITRE Corporation, Exploitation of remote services, https://attack.mitre.org/techniques/T1210/ (retrieved on 13 October 2020)
[45] MITRE Corporation, Exploitation of remote services, https://attack.mitre.org/techniques/T1210/ (retrieved on 13 October 2020)

The airport management board decides to notify the aviation sectorial CSIRT and to file a complaint to the police.

Technique T1498 – Network Denial of Service[46]	"Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth services rely on. Example resources include specific websites, email services, DNS, and web-based applications. Adversaries have been observed conducting network DoS attacks for political purposes[1] and to support other malicious activities, including distraction[2], hacktivism, and extortion".[47]
Technique TA0006 – Credential Access[48]	"Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals" [49]

Response of the CSIRT team

The CSIRT Team uses lessons learned from recent similar attacks against airports and starts the Incident Response process with actions meant to contain the incident as much as possible.

The user account responsible for altering the airport databases is disabled, and the user workstation is isolated from the network and sent to the digital forensics laboratory. All recent activity of the user is tracked because there's plausible suspicion that the user was the victim of a spear-phishing attack which resulted in his workstation being infected with malware.

Additionally, the CSIRT team is working with the airport IT personnel, the ISP, airport IT vendors, and international partners to try to come up with a mitigation plan for the DDoS attack. Multiple scenarios are studied, but for the moment it is decided to ask the ISP to filter the traffic coming from outside of the country the airport is located in.

Next, the technical investigation of the incident is started:

- Analyse logs from perimeter security solutions (firewall, web and email gateway, proxy, etc.)
- Analyse the recent activity of the user causing database malicious actions and conduct a forensically sound investigation of his workstation
- Try to identify rogue devices in the network

Criminal investigation

The national cybersecurity authority reported this incident to LE. The local police cyber unit started the investigation by:

- Analysing security video cameras from the airport in the last month to try to identify attackers planting rogue devices
- LE/Prosecutor requesting a warrant and seizure of the electronic devices of possible suspects

Information sharing

The CSIRT is conducting an information exchange about the incident with other CSIRTs (especially the ones in the aviation sector/sectorial CSIRTs), trying to find out if similar attacks

[46] MITRE Corporation, *Network Denial of Service,* https://attack.mitre.org/techniques/T1498 (retrieved on 13 October 2020).
[47] MITRE Corporation, *Network Denial of Service,* https://attack.mitre.org/techniques/T1498 (retrieved on 13 October 2020).
[48] MITRE Corporation, *Credential Access,* https://attack.mitre.org/techniques/TA0006 (retrieved on 13 October 2020).
[49] MITRE Corporation, *Credential Access,* https://attack.mitre.org/techniques/TA0006 (retrieved on 13 October 2020).

were conducted recently and gather information about investigation results and mitigation measures.

In cooperation with the airport management, CSIRT will share the gathered information with the national LE authorities and will offer their further support to continue the investigations and facilitate information exchange nationally and internationally.

2.3.3 Tasks

2.3.3.1 Task 1: Notification of the incident

The airport security team needs to quickly do an initial assessment of the situation and notify the incident according to existing procedures and legal framework.

As previously mentioned, The National Competent Cybersecurity Authority or the National CSIRT is notified.

To whom else and when should the incident be reported?

Figure 22: Notification list – Template

Who to notify	Required / recommended	Comments
Within the organisation		
Outside the organisation		

2.3.3.2 Task 2: Setting up the task force, division of duties

While in the context of a criminal investigation the prosecutor/judge is in charge of assigning roles for dealing with the investigation of the cybercrime, the national CSIRT may establish a task force to respond to the incident and deal with the crisis generated by the incident.

The National CSIRT is in charge of establishing a task force to deal with the crisis generated by the incident.

Analyse the legal and organisational framework by defining the competences of CSIRTs, LE, and the judiciary in their activities related to fighting cybercrime, and capture potential synergies and possible overlaps. Analyse the possible interferences in the cooperation between CSIRTs and LE and their interaction with the judiciary. To collect data and roles and duties, use the SoD matrix in ANNEX B.

The role of the IT contractors of the airport should be decided: will they be part of the task force?

Figure 23: Task force template

Organisation	Expertise	Tasks/role	Comments

2.3.3.3 Task 3: Possible duties (tasks), synergies and potential interferences between CSIRT, LE and judiciary

Select some of the duties from column 1 of the SoD in Annex B and with some of these duties, briefly describe the measures to that could be taken by each community in the scenario.

The template below can be used by listing the phase (e.g. during the incident/crime) in column 1, the duties (tasks) in column 2 (to be taken from column 1 of the SoD matrix in Annex B), and the synergies and potential interferences in column 3. The last column of the template below, column 4, can be used to add comments.

Figure 24: Duties, synergies and potential interferences – Template

Phase	Duty (task)	Synergies and potential interferences	Comments

2.3.3.4 Task 4: International cooperation and information sharing

Briefly explain how Interpol, Europol and Eurocontrol can collaborate with CSIRTs/LE/Judiciary during the international criminal investigation.

The template below can be used to list the name of the organisation in column 1, the name of the organisation it collaborates with in column 2 and the kind of collaboration they have in column 3.

Figure 25: Information sharing and use – Template

Name of the organisation	Names of the organisation it collaborates with	Kind of collaboration

2.3.3.5 Task 5: Post-incident preventive measures

Explain based on information you have about the incident, what kinds of post-incident preventive measures you would recommend to the airport information security team to implement and how you would formulate the outcome as a gap analysis and a remediation roadmap.

The template below can be used by listing the duties (tasks) in column 1 (to be taken from column 1 of the SoD matrix in Annex B), and the proposed preventive security measures in column 2.

Figure 26: Suggestion on preventive security measures – Template

Duty (Task)	Proposed preventive security measures

2.3.4 Lessons Learned

DDoS and malware blended attack cases are rather complex and sophisticated. They demand many skills as it's not easy to identify what is the primary attack vector or what is the ultimate target of the attacker. The scenario allows each party to understand its role under the legal framework of each member state.

Although for training purposes the scenario is presented as less complicated than real cases might be, it still allows each party to understand the complexities in terms of actors involved, roles played, duties (tasks) performed, synergies to exploit, and risks of interference.

3. BIBLIOGRAPHY

ENISA (2018), *Review of Behavioural Sciences Research in the Field of Cybersecurity*, https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity (retrieved on 13 October 2020)

ENISA Training Resources page: https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material (retrieved on 14 October 2020)

CSIRTs by Country –Interactive Map, https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map (retrieved on 13 October 2020)

ENISA, 2020 Report on CSIRT-LE Cooperation - A study of the roles and synergies among selected EU Member States/EFTA countries, https://www.enisa.europa.eu/publications/2020-report-on-csirt-le-cooperation (26 January 2021)

ENISA, *An overview on enhancing technical cooperation between CSIRTs and LE* (2019), https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-tools-for-enhancing-cooperation-between-csirts-and-le (retrieved on 13 October 2020)

ENISA, *Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime - A first collection of practices* (2012), https://www.enisa.europa.eu/publications/cooperation-between-certs-and-law-enforcement-agencies-in-the-fight-against-cybercrime-a-first-collection-of-practices (retrieved on 15 October 2020)

ENISA, *Cooperation between CSIRTs and Law Enforcement: interaction with the Judiciary* (2018), https://www.enisa.europa.eu/publications/csirts-le-cooperation (retrieved on 13 October 2020)

ENISA, *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity* (2018), https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity (retrieved on 13 October 2020)

ENISA, *Electronic evidence - a basic guide for First Responders* (2014), https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders (retrieved on 15 October 2020)

ENISA, *Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime (2012)*, https://www.enisa.europa.eu/publications/good-practice-guide-for-addressing-network-and-information-security-aspects-of-cybercrime (retrieved on 15 October 2020)

ENISA, *Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects* (2017), www.enisa.europa.eu/publications/improving-cooperation-between-csirts-and-law-enforcement (retrieved on 13 October 2020)

ENISA, *Information sharing and common taxonomies between CSIRTs and Law Enforcement* (2015), https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement (retrieved on 15 October 2020)

ENISA, *Reference Incident Classification Taxonomy,* https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy (retrieved on 13 October 2020)

ENISA, Reference Security Incident Taxonomy Working Group, https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force (retrieved on 13 October 2020)

ENISA, *Roadmap on the cooperation between CSIRTs and LE* (2019), https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-roadmap-on-csirt-le-cooperation (retrieved on 13 October 2020)

ENISA, *ENISA Threat Landscape – 2020*, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends (retrieved on 10 November 2020)

ENISA, *Tools and Methodologies to Support Cooperation between CSIRTs and Law Enforcement* (2017), www.enisa.europa.eu/publications/tools-and-methodologies-to-support-cooperation-between-csirts-and-law-enforcement (retrieved on 13 October 2020)

ENISA, *Training material on CSIRT-LE cooperation area* (2019), https://www.enisa.europa.eu/news/enisa-news/training-material-to-enhance-cooperation-across-csirts-and-law-enforcement (retrieved on 13 October 2020)

ENISA, *Trainings for Cybersecurity Specialists*, (handbooks and toolsets) https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material (retrieved on 13 October 2020)

Reference Security Incident Classification Taxonomy (RSIT taxonomy), https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/working_copy/humanv1.md (retrieved on 13 October 2020)

ANNEX A: MAIN ABBREVIATIONS

Abbreviation	Description
AIL	Analysis of Information Leaks
BCP	Business Continuity Plan
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
C&C	Command and Control
DDoS	Distributed Denial of Service
DPA	Data Protection Authority
EATM-CERT	European Air Traffic Management Computer Emergency Response Team
EDR	Endpoint Detection and Response
EFTA	European Free Trade Association
EMAS	Europol Malware Analysis Solution
ICT	Information and Communication Technology
IOC	Indicators Of Compromise
IP	Internet Protocol
ISP	Internet Service Provider
LE	Law Enforcement
LEA	Law Enforcement Agency
MS	Member State
n/g	National/governmental
Q&A	Question and answer
RSIT	Reference Security Incident Taxonomy
SIEM	Security Information and Event Management
SOC	Security Operation Centre
SoD	Segregation (or separation) of Duties
SSH	Secure SHell

TTP	Tactics, Techniques and Procedures
VPN	Virtual Private Network
VPS	Virtual Private Server

ANNEX B: SEGREGATION OF DUTIES (SOD) MATRIX

Version 1.6 of 5 June 2020

- **Responsible (R)**: Who is responsible for performing this duty? Who is the decision maker?
- **Supporting (S)**: Who is providing support when performing this duty? (if applicable)
- **Consulted (C)**: Who is consulted during the performance of this duty? (if applicable)
- **Informed (I)**: Who is informed when performing this duty? (For instance, if CSIRT should report a crime to LEA; this means that LEA is informed) (if applicable)

Duties related to (supporting) cybercrime fighting activities	CSIRTs	LE	Prosecutors	Judges	Training topics (e.g. technical skills etc.	ADDITIONAL COMMENTS (including information on possible synergies and potential interferences)
Prior to incident/crime						
1. Delivering training						
2. Participating in training						
3. Collecting cyber threat intelligence						
4. Analysing vulnerabilities and threats						
5. Issuing recommendations for new vulnerabilities and threats						
6. Advising potential victims on preventive measures against cybercrime						
During the incident/crime						
7. Discovering of the cyber-security incident/crime						
8. Identifying and classifying the cyber-security incident/crime						
9. Identifying the type and severity of the compromise						
10. Collecting data that may be evidence/evidence						
11. Providing technical expertise						
12. Preserving the evidence that may be crucial for the detection of a crime in a criminal trial						
13. Advising the victim to report / obligation to report a cybercrime to law enforcement (LE)						
14. Informing the victim of a cybercrime						
15. Informing other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.)						
16. Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling						

17. Mitigating a cybersecurity incident						
18. Conducting the criminal investigation						
19. Leading the criminal investigation						
20. In the case of disagreement, having the final say for a criminal investigation						
21. Authorizing the investigation carried out by the LE						
22. Ensuring that fundamental rights are respected during the investigation and prosecution						
Post incident/crime						
23. Advising on systems recovery						
24. Protecting the constituency						
25. Preventing and containing cyber-security incidents from a technical point of view						
26. Analysing and interpreting collected evidence						
27. Requesting testimonies from CSIRTs and LE						
28. Admitting and assessing the evidence						
29. Judging who committed a crime						
30. Assessing cyber security incident damage and cost						
31. Reviewing the response and updating policies and procedures						

Some explanations regarding the SoD matrix:

- At the top of the SoD Matrix all the four **possible roles** that each actor (CSIRT, LE, Prosecutors, and Judges) may play are listed and briefly explained: Responsible (R), Supporting (S) (if applicable), Consulted (C) (if applicable), and informed (I) (if applicable).
- In the rows, the **duties** are listed and numbered for convenience (e.g. 10. Collecting data that may be evidence/Evidence collection). It must be noted that “duties” is used here as a synonymous of “tasks”
- Column 2, Column, 3, Column 4, Column 5, refer to the **actors**, respectively CSIRT, LE, Prosecutors, and Judges.
- The interviewees are asked to indicate which role(s) each actor (CSIRTs, LE, prosecutors, judges) has in the performance of duties during a cybercrime (supporting) fighting activity. In other words, the interviewees are asked to identify whether the CSIRTs, the LE, the prosecutors or the judge are for a particular duty responsible (R) for that duty, and, if applicable, which other actor is Supporting (S) the performance of that duty, is Consulted (C) or is Informed (I) during the performance of that duty.
- Column 6 (optional) is used to capture information on **training topics**, which is closely connected to the competencies that are required for the performance of the specific duties.
- Column 7 is used for any **additional information** that the interviewee might provide and to record possible synergies and potential interferences, especially for those cases where a task is performed by more than one community.

An example of completed information related to one duty in the SoD Matrix in the table below.

Table 1. Example of completed information related to one duty in the SoD Matrix

- **Responsible (R): Who is responsible for performing this duty? Who is the decision maker?**
- **Supporting (S): Who is providing support when performing this duty? (if applicable)**
- **Consulted (C): Who is consulted during the performance of this duty? (if applicable)**
- **Informed (I): Who is informed when performing this duty? (For instance, if CSIRT should report a crime to LEA; this means that LEA is informed) (if applicable)**

Duties related to (supporting) cybercrime fighting activities	CSIRTs	LE	Prosecutors	Judges	Training topics (e.g. technical skills etc.)	ADDITIONAL COMMENTS (including information on possible synergies and potential interferences)
Prior to incident/crime						
10. Collecting data that may be evidence/Evidence collection	S	R	I C		Digital forensics	Prosecutor depending on the specific case may be informed or consulted, in other words requested to provide guidance.

TP-02-20-982-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, visit www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-463-3
DOI: 10.2824/2038