EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TECHNICAL ASPECTS OF COOPERATION BETWEEN CSIRTS AND LE

Toolset, Document for trainees

DECEMBER 2019

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found 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

Alexandra Michota (ENISA), Andreas Mitrakas (ENISA), Constantinos Patsakis, Václav Stupka

LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 2019/881.
This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

ISBN: 978-92-9204-341-4, DOI: 10.2824/46779

TABLE OF CONTENTS

1. WHAT YOU WILL LEARN

1.1 THEMATIC AREA

In 2017, ENISA presented tools and methodologies to support the cooperation between Computer Security Incident Response Teams (CSIRTs) -in particular national and governmental CSIRTs, and Law Enforcement (LE) and provide some recommendations to help them to cooperate closer aiming to successfully fight against cybercrime.

ENISA confirmed that CSIRTs and LE exchange information regularly, during incident handling and criminal investigations, both formally and informally and that trust is the key success factor to their cooperation. CSIRTs and LE have different objectives and ways to collect and process information. However, between the two communities there is an increased reciprocal understanding of needs. According to the data collected, CSIRTs are more inclined to use open source tools, e.g. the Malware Information Sharing Platform (MISP). Information sharing between CSIRTs and LE occurs in a rather unsystematic manner. A common taxonomy for CSIRTs and LE has been developed and there are ongoing efforts towards a broader adoption and use of it.

- **Learning outcomes**

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

  - Demonstrate knowledge of tools and methodologies, forms and procedures used for the cooperation between CSIRTs and LE
  - Demonstrate knowledge of the common taxonomy developed for CSIRTs and LE
  - Demonstrate knowledge of MISP capabilities
  - Define use cases for Threat Intelligence Platform (TIP) and real-time information sharing

2. CASE STUDIES

2.1 CASE STUDY 1

The objective of this case study is to explain CSIRT and LE roles in a ransomware infection scenario.

Figure 1.1: Main objective of the case study

Main Objective	
Targeted Audience	CSIRTs and LE
Total Duration	30 minutes
Scenario	Trainees are observers of a ransomware attack.
Task 1	Determine who accessed the system and when
Task 2	Determine if it was a malware infection or human actions
Task 3	Identify the methods of recovering the encrypted data
Task 4	Identify the obstacles that could occur during the investigation
Task 5	Identify expected activities of relevant stakeholders by filling in the ‘Segregation of Duties’ (SoD) matrix

2.1.1 Objectives

Identify the steps that have to be taken in order to solve a case of ransomware infection and bring it to Court. The goal is for the attendants to determine who does what, what their role is, the order of events, and what possible drawbacks might appear during the investigation. The participants must see what is missing from each side in terms of skills, clearance and determine the course of action in one national and one cross-jurisdiction twist of the same scenario.

2.1.2 Scenario

Company ‘C’ has contacted Law Enforcement Agency (LEA) ‘L’ to report that after trying to log in to their database server (MongoDB), their data were encrypted and there was a ransomware notice in the configuration file to pay an amount of a cryptocurrency to a specific address.

The questions that have to be answered are the following:

1. Who performed the encryption?
2. Can the data be recovered?

The scenario is illustrated in the following figure:

Figure 1.2: Ransomware infection scenario

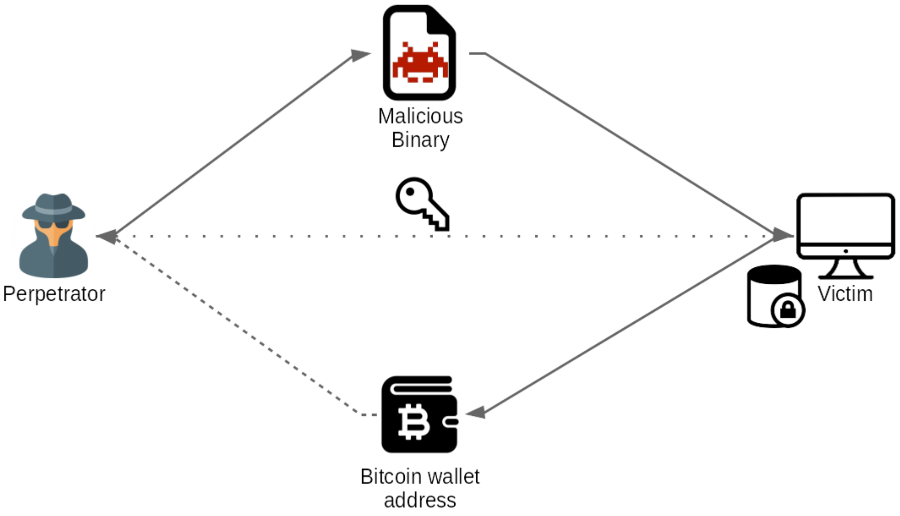

Figure 1.3: Timeline of the events

Date/time	Incident description
1/3/2019 09:42	The perpetrator sends an email with a malicious attachment to the victim through a vulnerable SMTP server as part of a campaign.
1/3/2019 09:43	The victim receives the email and opens the attachment.
1/3/2019 09:49	The compromised host performs a network scan.
1/3/2019 09:54	The compromised host connects to the MongoDB server.
1/3/2019 09:55	The encryption of all records has started.
2/3/2019 01:51	The encryption has finished and the ransomware notice has been placed.
4/3/2019 09:01	The victim company realises a disruption in their services.
4/3/2019 09:08	The victim company realises that their database server has been encrypted.
4/3/2019 10:57	The victim company informs the CSIRT.

2.1.3 Tasks

2.1.3.1 Investigation analysis

Based on the system logs, one tries to determine who accessed the system and when. The last database transaction can be used to determine which user performed the data encryption. Was this a result of a malware infection or human actions, e.g. can we identify the presence of a malicious binary in the file system or was it a malicious user interaction from the terminal logs? Did the user authenticate to the device locally or remotely? In the case of the latter, which are the previous “hops” (IP addresses). If no direct user interaction seems to have been performed, then one needs to check open services and their security status. Could someone take over the control through an existing service, e.g. exploit a vulnerability.

The investigation of network traffic may record:

1. Remote login attempts
2. Remote usage of local services
3. Attempts to connect to a Command and Control (C&C) server (NX requests)
4. Attempts to connect to other local devices from the penetrated machine

From the above and inspection of the collected binary (dynamic and reverse engineering) possible IPs of the perpetrator can be found. Note that these IPs may be “hops” that the attacker uses and not the actual IPs.

The ransomware notice points to a crypto wallet, therefore, the address of the wallet needs to be monitored for previous and new transactions as it can be used as a link to the perpetrator. Note that the use of cryptocurrencies like Monero and ZCash can make things even worse as the transactions are by default more private than others while there are many laundry services for cryptocurrencies .

The obvious answer for recovering the encrypted data is the backups. However, if this is not possible, then the keys should be searched in the memory dump. The reverse engineering of the binary or cache files from the file system may provide some relevant data, e.g. hard-coded keys, poor handling of cryptographic primitives, lack of enough entropy to produce the keys or even use of file system to store parts of the keys. The above may be exploited to at least partially recover the decryption key.

Possible obstacles during the investigation

- Size of data that have to be collected from the victim.
- Use of file-less malware
- Good use of cryptographic primitives
- Exploitation of TPM/TEE features.
- Since the device has been penetrated, logs may have been tampered with/removed.
- Not enough privileges to perform memory dump
- Use of obfuscation, anti-VM, and anti-debug to make the analysis of the sample even harder.
- Network connections and logs indicate use of proxies.

2.1.3.2 Segregation of Duties

Please use the SoD matrix (Figure 1.4) to identify, what activities can be performed or facilitated by the relevant stakeholders throughout the cybercrime investigation lifecycle. The aim of this matrix is to highlight conflicting or overlapping duties performed by one community or more.

2.1.3.3 Outcomes

The scenario illustrates the roles, measures, and possible obstacles during the investigation of a ransomware scenario.

2.1.4 Lessons learned

Ransomware cases are rather complex and demand many skills without being sure that the perpetrators can be determined. The scenario allows each party to understand its role under the legal framework of each member state.

Figure 1.4: ‘Segregation of Duties’ matrix

Cybercrime fighting activities	CSIRTs	LE	Judges	Prosecutors	Training topics (e.g. technical skills etc.)
Prior to incident/crime					
Delivering/participating in training					Problem-solving and critical thinking skills
Collecting cyber threat intelligence					Knowledge of cyber threat intelligence landscape
Analysis of vulnerabilities and threats					Development and distribution of tools for preventive and reactive mitigation
Issuing recommendations for new vulnerabilities and threats					Dealing with specific types of threats and vulnerabilities
Advising potential victims on preventive measures against cybercrime					Raising awareness on preventive measures against cybercrime
During the incident/crime					
Discovery of the cybersecurity incident/crime					Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis
Identification and classification of the cybersecurity incident/crime					Incident and crime classification and identification
Identify the type and severity of the compromise					Knowledge of cyber threats and incident response procedures
Evidence collection					Knowledge of what kind of data to collect; organisation skills
Providing technical expertise					Technical skills
Preserving the evidence that may be crucial for the detection of a crime in a criminal trial					Digital investigations; forensics tools;
Advising the victim to report / obligation to report a cybercrime to law enforcement (LE)					Obligations and restriction on information sharing; communication channels
Duty to inform the victim of a cybercrime					Obligations and restrictions to the information sharing
Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.)					Obligations and rules for information sharing among communities.
Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling					Communication skills; communication channels
Mitigation of an incident					Well-prepared & well-organised to react promptly in an incident
Conducting the criminal investigation					Knowledge of the legal framework; decision-making skills
Leading the criminal investigation					Knowledge of the incident response plan; leadership skills
In the case of disagreement, the final say for an investigation					Knowledge of the legal framework; decision-making skills
Authorizing the investigation carried out by the LE					Decision-making in the criminal procedure
Ensuring that fundamental rights are respected during the investigation and prosecution					Fundamental rights in criminal investigations and prosecutions
Post incident/crime					
Systems recovery					Technical skills
Protecting the constituency					Drafting and establishing procedures; technical knowledge
Preventing and containing IT incidents from a technical point of view					Technical skills pertaining to system administration, network administration, technical support or intrusion detection
Analysis and interpretation of collected evidence					Criminalistics, digital forensics, admissible evidence
Requesting testimonies from CSIRTs and LE					Testimonies in a criminal trial
Admitting and assessing the evidence					Evidence in a criminal trial
Judging who committed a crime					Technical knowledge and knowledge of the legal framework
Assessing incident damage and cost					Evaluation skills
Reviewing the response and update policies and procedures					Knowledge how to draft an incident response and procedures

2.2 CASE STUDY 2

The objective of this case study is to explain CSIRT and LE roles in a data exfiltration scenario.

Figure 2.1: Main objective of the case study

Main Objective	
Targeted Audience	CSIRTs and LE
Total Duration	30 minutes
Scenario	Trainees are observers of a data exfiltration attack
Task 1	Determine who accessed the system and when
Task 2	Determine the process of investigating the IP address
Task 3	Identify means of further investigation
Task 4	Identify the obstacles that could occur during the investigation
Task 5	Identify expected activities of relevant stakeholders by filling in the SoD matrix

2.2.1 Objectives

Identify the steps that have to be taken in order to solve a case of data exfiltration and bring it to court. The goal is for the attendants to determine who does what, what their role is, the order of events, and what possible drawbacks might appear during the investigation. The participants must see what is missing from each side in terms of skills, clearance and determine the course of action in one national and one cross-jurisdiction twist of the same scenario.

2.2.2 Scenario

Company ‘C’ has contacted LEA ‘L’ to report that after citizen report user data are being sold to a dark web forum. ‘C’ wants to bring the people who have leaked the data to justice. The questions that have to be answered are the following:

1. Have the claimed data been exfiltrated?
2. The leakage is internal or external?
3. Who generated the data leak?

The scenario is illustrated in the following figure:

Figure 2.2: Data exfiltration scenario

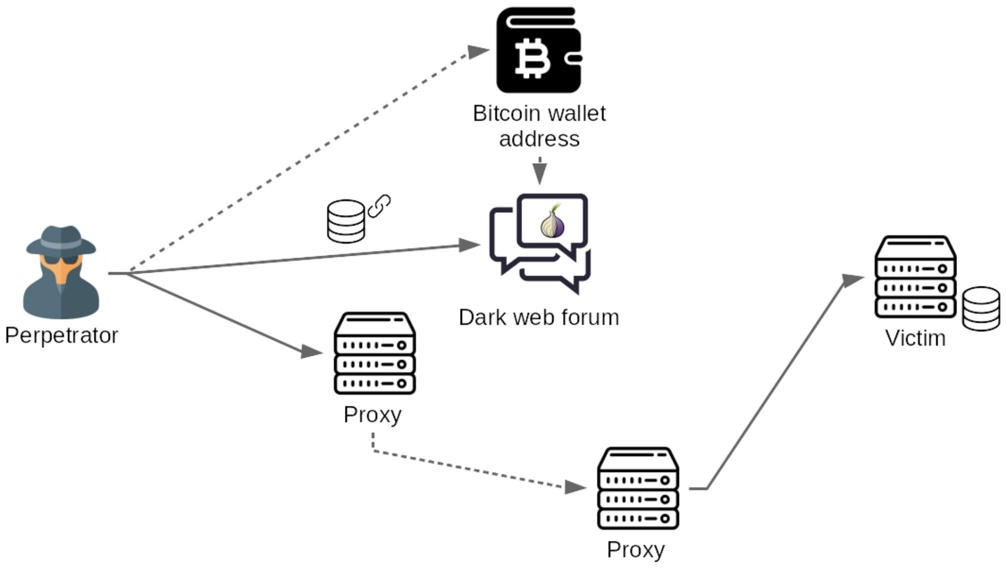

Figure 2.3: Timeline of the events

Date/time	Incident description
4/3/2019 22:37	The perpetrator uses a set of proxies and manages to connect to the Database (DB) server of the victim.
4/3/2019 22:48	The perpetrator starts the data extraction from the DB server, record by record
19/4/2019 05:38	All data have been exported.
27/4/2019 02:19	The perpetrator creates a new topic on a dark web forum advertising the dataset and requesting payments in bitcoin.
29/4/2019 03:55	An employee of the company sends an email to the company informing them of the data leakage.
31/4/2019 10:43	The victim company informs the CSIRT.

2.2.3 Tasks

2.2.3.1 Investigation analysis

Based on the system logs, one tries to determine who accessed the system and when. The excerpts of the data that are used on the forum may give a rough estimation of the oldest possible date that the database was leaked. Since the database consists of several MBs, the database logs may indicate queries and actions that have been performed which may dump the contents of the database or at least indicate when the action was performed. Database dumps may have been performed either through a backup command or through sequential calls of specific queries. In the former case, a backup file is created which is then siphoned through SSH/FTP or a local backdoor mechanism. Since the backup file may have been left on the server or its creation can be determined from the filesystem, it is essential to look for such traces in the terminal logs and the filesystem. This could potentially lead IPs that the attacker used to exfiltrate the data. Note that the use of local IPs does not mean that the perpetrator is an insider, as an attacker may have used an internal node as a pivot to perform the attack.

Network log files may indicate continuous GET requests from specific IPs that were used to exfiltrate the data sequentially. In this case, it might be a coordinated attack, so that multiple hosts are used, possibly also compromised, to decrease the amount of time needed to collect the data.

Since the post has been posted to a dark web forum, the authorities need to check the background of the user and correlate the information with other intelligence. Obviously, these forums do not cooperate with LEAs, therefore, the posts of the corresponding user have to be collected in order to determine whether they may contain self-identifying information. Payment means, e.g. a bitcoin address could also be used to collect further information for the perpetrator.

Possible obstacles during the investigation:

- The lack of support from forum administrators to collect further evidence.
- Size of data that have to be collected from the victim.
- It might be impossible to determine that the disclosed dataset belongs to ‘C’.
- Impossible to determine when the attack was performed.
- The exfiltrated data are old enough that the victim does not enough logs.
- Use of file-less malware
- Since the device has been penetrated, logs may have been tampered with/removed.
- Not enough privileges to perform memory dump
- Use of obfuscation, anti-VM, and anti-debug to make the analysis of the sample even harder.
- Use of cryptocurrencies for the payment. Some cryptocurrencies like Monero and ZCash offer more privacy guarantees.

2.2.3.2 Segregation of Duties

Please use the SoD matrix (Figure 2.4) to identify, what activities can be performed or facilitated by the relevant stakeholders throughout the cybercrime investigation lifecycle. The aim of this matrix is to highlight conflicting or overlapping duties performed by one community or more.

2.2.3.3 Outcomes

The scenario illustrates the roles, measures, and possible obstacles during the investigation of a data exfiltration scenario.

2.2.4 Lessons Learned

Data exfiltration cases are rather complex and demand many skills to determine how the data were syphoned. The scenario allows each party to understand its role under the legal framework of each member state.

Figure 2.4: ‘Segregation of Duties’ matrix

Cybercrime fighting activities	CSIRTs	LE	Judges	Prosecutors	Training topics (e.g. technical skills etc.)
Prior to incident/crime					
Delivering/participating in training					Problem-solving and critical thinking skills
Collecting cyber threat intelligence					Knowledge of cyber threat intelligence landscape
Analysis of vulnerabilities and threats					Development and distribution of tools for preventive and reactive mitigation
Issuing recommendations for new vulnerabilities and threats					Dealing with specific types of threats and vulnerabilities
Advising potential victims on preventive measures against cybercrime					Raising awareness on preventive measures against cybercrime
During the incident/crime					
Discovery of the cybersecurity incident/crime					Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis
Identification and classification of the cybersecurity incident/crime					Incident and crime classification and identification
Identify the type and severity of the compromise					Knowledge of cyber threats and incident response procedures
Evidence collection					Knowledge of what kind of data to collect; organisation skills
Providing technical expertise					Technical skills
Preserving the evidence that may be crucial for the detection of a crime in a criminal trial					Digital investigations; forensics tools;
Advising the victim to report / obligation to report a cybercrime to law enforcement (LE)					Obligations and restriction on information sharing; communication channels
Duty to inform the victim of a cybercrime					Obligations and restrictions to the information sharing
Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.)					Obligations and rules for information sharing among communities.
Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling					Communication skills; communication channels
Mitigation of an incident					Well-prepared & well-organised to react promptly in an incident
Conducting the criminal investigation					Knowledge of the legal framework; decision-making skills
Leading the criminal investigation					Knowledge of the incident response plan; leadership skills
In the case of disagreement, the final say for an investigation					Knowledge of the legal framework; decision-making skills
Authorizing the investigation carried out by the LE					Decision-making in the criminal procedure
Ensuring that fundamental rights are respected during the investigation and prosecution					Fundamental rights in criminal investigations and prosecutions
Post incident/crime					
Systems recovery					Technical skills
Protecting the constituency					Drafting and establishing procedures; technical knowledge
Preventing and containing IT incidents from a technical point of view					Technical skills pertaining to system administration, network administration, technical support or intrusion detection
Analysis and interpretation of collected evidence					Criminalistics, digital forensics, admissible evidence
Requesting testimonies from CSIRTs and LE					Testimonies in a criminal trial
Admitting and assessing the evidence					Evidence in a criminal trial
Judging who committed a crime					Technical knowledge and knowledge of the legal framework
Assessing incident damage and cost					Evaluation skills
Reviewing the response and update policies and procedures					Knowledge how to draft an incident response and procedures

2.3 CASE STUDY 3

The objective of this case study is to explain CSIRT and LE roles in a child pornography sharing scenario.

Figure 3.1: Main objective of the case study

Main Objective	
Targeted Audience	CSIRTs and LE
Total Duration	30 minutes
Scenario	Trainees are observers of child pornography sharing
Task 1	Identify the steps of investigating a user's profile
Task 2	Determine the process of locating the user and blocking the dissemination of the material
Task 3	Determine possible means to identify the victims
Task 4	Identify possible obstacles during the investigation
Task 5	Identify expected activities of relevant stakeholders by filling in the SoD matrix

2.3.1 Objectives

Identify the steps that have to be taken in order to solve a case where child pornography sharing is reported and bring it to Court. The goal is for the attendants to determine who does what, what their role is, the order of events, and what possible drawbacks might appear during the investigation. The participants must see what is missing from each side in terms of skills, clearance and determine the course of action in one national and one cross-jurisdiction twist of the same scenario.

2.3.2 Scenario

During an investigation, the authorities discovered in a topic posted to a closed forum where users share child pornography content and a user sharing a link with relevant video streaming.

The questions that have to be answered are the following:

1. Can the perpetrators be identified?
2. How can the victims portrayed in the shared content be identified?

The scenario is illustrated in the following figure:

Figure 3.2: Timeline of the events

Date/time	Incident description
31/4/2019 05:36	The perpetrator posts several paedophile content on a dark web forum
2/5/2019 13:42	A LEA becomes aware of the content.
2/5/2019 17:44	The perpetrator posts a link to paedophile live streaming content

2.3.3 Tasks

2.3.3.1 Investigation analysis

The LEAs must login to the forum with the corresponding credentials and download all the necessary web pages. Moreover, the profile of each user must be investigated to determine whether additional data or metadata have been posted on the forum that may link the individual with his/her real identity. Note that all shared images from the perpetrators on the paedophile topic and others as well may contain EXIF information pointing to information ranging from GPS location to camera characteristics, and from user/profiles names to software processing library.

Having collected the images, the next step is to determine the source of the video stream. The video stream may originate directly from the perpetrator's device so there is a direct link with his/her IP or through a streaming service. In the latter case, LE must contact the corresponding service provider to a) block the link b) request further data for the perpetrator.

To identify the victims portrayed in the shared content, LE may use services provided by Europol and Microsoft to determine whether the content has already been shared and/or link it to existing cases.

Possible obstacles during the investigation:

- Lack of cooperation from the administrators of the forum.
- Lack of identifying information/metadata.
- Poor cooperation/delayed response from the streaming service provider.
- Victim not already known.
- The content does not guarantee that the portrayed victims are beyond doubt underage.

2.3.3.2 Segregation of Duties

Please use the SoD matrix (Figure 3.3) to identify, what activities can be performed or facilitated by the relevant stakeholders throughout the cybercrime investigation lifecycle. The aim of this matrix is to highlight conflicting or overlapping duties performed by one community or more.

2.3.3.3 Outcomes

The scenario illustrates the roles, measures, and possible obstacles during the investigation of a child pornography sharing.

2.3.4 Lessons Learned

Child pornography cases are very sensitive and demand many skills to determine not only who is sharing the content, but also who the victims that are portrayed are. The scenario allows each party to understand its role under the legal framework of each member state.

Figure 3.3: ‘Segregation of Duties’ matrix

Cybercrime fighting activities	CSIRTs	LE	Judges	Prosecutors	Training topics (e.g. technical skills etc.)
Prior to incident/crime					
Delivering/participating in training					Problem-solving and critical thinking skills
Collecting cyber threat intelligence					Knowledge of cyber threat intelligence landscape
Analysis of vulnerabilities and threats					Development and distribution of tools for preventive and reactive mitigation
Issuing recommendations for new vulnerabilities and threats					Dealing with specific types of threats and vulnerabilities
Advising potential victims on preventive measures against cybercrime					Raising awareness on preventive measures against cybercrime
During the incident/crime					
Discovery of the cybersecurity incident/crime					Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis
Identification and classification of the cybersecurity incident/crime					Incident and crime classification and identification
Identify the type and severity of the compromise					Knowledge of cyber threats and incident response procedures
Evidence collection					Knowledge of what kind of data to collect; organisation skills
Providing technical expertise					Technical skills
Preserving the evidence that may be crucial for the detection of a crime in a criminal trial					Digital investigations; forensics tools;
Advising the victim to report / obligation to report a cybercrime to law enforcement (LE)					Obligations and restriction on information sharing; communication channels
Duty to inform the victim of a cybercrime					Obligations and restrictions to the information sharing
Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.)					Obligations and rules for information sharing among communities.
Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling					Communication skills; communication channels
Mitigation of an incident					Well-prepared & well-organised to react promptly in an incident
Conducting the criminal investigation					Knowledge of the legal framework; decision-making skills
Leading the criminal investigation					Knowledge of the incident response plan; leadership skills
In the case of disagreement, the final say for an investigation					Knowledge of the legal framework; decision-making skills
Authorizing the investigation carried out by the LE					Decision-making in the criminal procedure
Ensuring that fundamental rights are respected during the investigation and prosecution					Fundamental rights in criminal investigations and prosecutions
Post incident/crime					
Systems recovery					Technical skills
Protecting the constituency					Drafting and establishing procedures; technical knowledge
Preventing and containing IT incidents from a technical point of view					Technical skills pertaining to system administration, network administration, technical support or intrusion detection
Analysis and interpretation of collected evidence					Criminalistics, digital forensics, admissible evidence
Requesting testimonies from CSIRTs and LE					Testimonies in a criminal trial
Admitting and assessing the evidence					Evidence in a criminal trial
Judging who committed a crime					Technical knowledge and knowledge of the legal framework
Assessing incident damage and cost					Evaluation skills
Reviewing the response and update policies and procedures					Knowledge how to draft an incident response and procedures

2.4 CASE STUDY 4

The objective of this case study is to explain CSIRT and LE roles in a Denial of Service (DoS) attack scenario.

Figure 4.1: Main objective of the case study

Main Objective	
Targeted Audience	CSIRTs and LE
Total Duration	30 minutes
Scenario	Trainees are observers of a DoS attack
Task 1	Determine why the server was brought down
Task 2	Determine who is the owner of the IP performing the attack
Task 3	Identify further investigation steps
Task 4	Identify the obstacles that could occur during the investigation
Task 5	Identify expected activities of relevant stakeholders by filling in the SoD matrix

2.4.1 Objectives

Identify the steps that have to be taken in order to solve a DoS attack and bring it to court. The goal is for the attendants to determine who does what, what their role is, the order of events, and what possible drawbacks might appear during the investigation. The participants must see what is missing from each side in terms of skills, clearance and determine the course of action in one national and one cross-jurisdiction twist of the same scenario.

2.4.2 Scenario

Company ‘C’ has contacted LEA ‘L’ to report that their servers are down due to a DoS attack leading to huge monetary losses and wants to track down the perpetrators and bring them to justice.

The question that has to be answered is who orchestrated the attack.

The different possible scenarios are illustrated in the following figure:

Figure 4.2: Dos attack

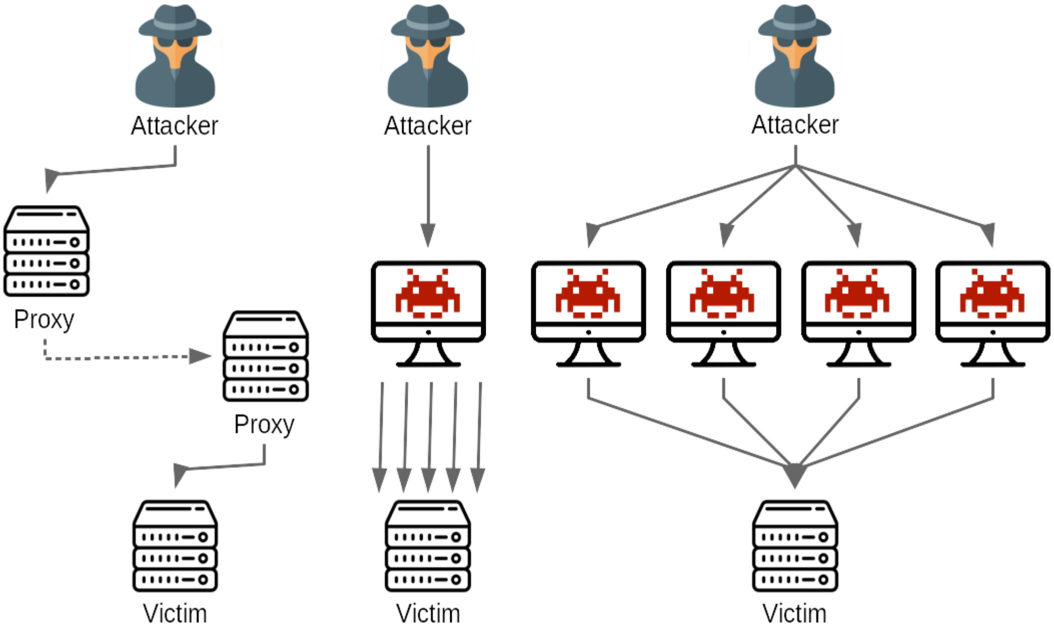

Figure 4.3: Timeline of events

Date/time	Incident description
31/4/2019 11:39	The perpetrator starts a malicious campaign to create her army of bots
17/5/2019 10:41	The perpetrator sends her bots a command to start a DNS amplification attack towards the victim.
17/5/2019 10:42	The victim's servers are taken down due to unprecedented bandwidth usage.
17/5/2019 15:23	The victim company informs the CSIRT.

2.4.3 Tasks

2.4.3.1 Investigation analysis

The network logs have to be investigated in order to determine why the server was brought down, if it has been a single attacker using a tool or known exploit, or a distributed denial of service (DDoS). In the former case, there might be a chance that the IP performing the attack belongs to the perpetrator; therefore, the logged IP has to be investigated. In the latter case though, we are probably having a botnet attacking the organisation, therefore, the logged IPs actually belong to bots, that is compromised machines from the perpetrator that are ordered to perform the attack. In this case, the logs have to be studied by the CSIRT to determine patterns with previous attacks and if possible collect sample binaries from the infected hosts to allow further investigation through reverse engineering. Finally, the case of DNS amplification attacks also involves botnets, however, cooperation from the corresponding DNS servers is needed. In both botnet cases further intelligence and cross-border cooperation is needed to find the perpetrators.

Possible obstacles during the investigation

- Identification of perpetrator if they are using a botnet.
- Use of proxy when performing the attack.
- Need of “side” information (e.g. post in forums from the attacking team) when performing the analysis.
- Usage of amplification methods e.g. DNS amplification

2.4.3.2 Segregation of Duties

Please use the SoD matrix (Figure 4.4) to identify, what activities can be performed or facilitated by the relevant stakeholders throughout the cybercrime investigation lifecycle. The aim of this matrix is to highlight conflicting or overlapping duties performed by one community or more.

2.4.3.3 Outcomes

The scenario illustrates the roles, measures, and possible obstacles during the investigation of DoS attacks.

2.4.4 Lessons Learned

Modern DoS attacks are rather complex and transnational involving thousands or even millions of compromised machines. The scenario allows each party to understand its role under the legal framework of each member state.

Figure 4.4: ‘Segregation of Duties’ matrix

Cybercrime fighting activities	CSIRTs	LE	Judges	Prosecutors	Training topics (e.g. technical skills etc.)
Prior to incident/crime					
Delivering/participating in training					Problem-solving and critical thinking skills
Collecting cyber threat intelligence					Knowledge of cyber threat intelligence landscape
Analysis of vulnerabilities and threats					Development and distribution of tools for preventive and reactive mitigation
Issuing recommendations for new vulnerabilities and threats					Dealing with specific types of threats and vulnerabilities
Advising potential victims on preventive measures against cybercrime					Raising awareness on preventive measures against cybercrime
During the incident/crime					
Discovery of the cybersecurity incident/crime					Digital investigations; forensics tools; penetration testing; vulnerability scanning; flow analysis
Identification and classification of the cybersecurity incident/crime					Incident and crime classification and identification
Identify the type and severity of the compromise					Knowledge of cyber threats and incident response procedures
Evidence collection					Knowledge of what kind of data to collect; organisation skills
Providing technical expertise					Technical skills
Preserving the evidence that may be crucial for the detection of a crime in a criminal trial					Digital investigations; forensics tools;
Advising the victim to report / obligation to report a cybercrime to law enforcement (LE)					Obligations and restriction on information sharing; communication channels
Duty to inform the victim of a cybercrime					Obligations and restrictions to the information sharing
Duty to inform other stakeholders/authorities (operators of vulnerable systems, data protection authorities, telecommunications authorities, etc.)					Obligations and rules for information sharing among communities.
Acting as a single point of contact (PoC) for any communication with other EU Member States for the incident handling					Communication skills; communication channels
Mitigation of an incident					Well-prepared & well-organised to react promptly in an incident
Conducting the criminal investigation					Knowledge of the legal framework; decision-making skills
Leading the criminal investigation					Knowledge of the incident response plan; leadership skills
In the case of disagreement, the final say for an investigation					Knowledge of the legal framework; decision-making skills
Authorizing the investigation carried out by the LE					Decision-making in the criminal procedure
Ensuring that fundamental rights are respected during the investigation and prosecution					Fundamental rights in criminal investigations and prosecutions
Post incident/crime					
Systems recovery					Technical skills
Protecting the constituency					Drafting and establishing procedures; technical knowledge
Preventing and containing IT incidents from a technical point of view					Technical skills pertaining to system administration, network administration, technical support or intrusion detection
Analysis and interpretation of collected evidence					Criminalistics, digital forensics, admissible evidence
Requesting testimonies from CSIRTs and LE					Testimonies in a criminal trial
Admitting and assessing the evidence					Evidence in a criminal trial
Judging who committed a crime					Technical knowledge and knowledge of the legal framework
Assessing incident damage and cost					Evaluation skills
Reviewing the response and update policies and procedures					Knowledge how to draft an incident response and procedures

3. REFERENCES

ENISA. (2017). *Tools and Methodologies to Support Cooperation between CSIRTs and Law Enforcement.* Retrieved from https://www.enisa.europa.eu/publications/tools-and-methodologies-to-support-cooperation-between-csirts-and-law-enforcement

A ANNEX: ABBREVIATIONS

Abbreviation	Description
C&C	Command and Control
CSIRT	Computer Security Incident Response Team
DoS	Denial-of-Service (attack)
DDoS	Distributed Denial-of-Service (attack)
GDPR	General Data Protection Regulation
IOC	Indicators Of Compromise
IP	Internet Protocol
LE	Law Enforcement
LEA	Law Enforcement Agency
MISP	Malware Information Sharing Platform
SoD	Segregation (or separation) of Duties
TIP	Threat Intelligence Platform

TP-03-20-177-EN-N

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found 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: 978-92-9204-341-4
DOI: 10.2824/46779