{elysiumsecurity}
cyber protection & response

```
1 1 1 0 0 1 0 1 0 0 0 0 1 1 0 1 1 0 0 0 0 1 1 1 1                                 0
0 1 0 1 1 1 0 1 0 1 1 0 1 1 1 0 1                                                 0
1 1 0 0 1 0                                                                       1
1 0 0 1 0                                                                         1
1 0 1 1 1                                                                         1
0 1 0 1                                                                         0 1
0 0 1 0                                                                         1 0
1 1 0 1                                                                         0 1
0 1 1 1                                                                         1 1
1 0 0                                                                           1 0
0 1 0                                                                         1 0 0
1 1 1                                                                         0 0 0
1 0 1                                                                         0 1 0
0 1 1                                                                         1 1 1
1 1                                                                         0 1 1 0
1 0                                                                         1 1 1 1
1 1                                                                       1 0 1 0 0
0                                                                     1 1 0 0 1 1 1
0                                                             0 1 1 0 0 1 0 1 1 0 1
1                                                     1 0 0 0 1 0 1 0 1 1 0 1 0 1 1
1                                             1 0 1 0 1 1 1 0 0 1 0 1 0 0 1 1 1 0 1 0
```

ELYSIUMSECURITY LTD

INCIDENT RESPONSE METHODOLOGIES

CYBER INCIDENT PLAYBOOKS

TECHNICAL GUIDE

VERSION:	1.2.0
DATE:	06/11/2020
AUTHOR:	SYLVAIN MARTINEZ
REFERENCE:	ES-TG-IRM
REPORT ENGINE:	2.1.0
CLASSIFICATION:	PUBLIC

DISCLAIMER

This document was created by ELYSIUMSECURITY LTD. and is based on the work done by the CERT Société Générale (SG CERT) which is available for free, under the Creative Commons Attribution 3.0 Unported License, on the following GitHub repository:

https://github.com/certsocietegenerale/IRM

You are free to use the content of this document as per the aforementioned license and with referencing the author(s).

CHANGE HISTORY

VERSION	DATE	COMMENTS
1.0.0	27/08/2020	First version including the same content as the SG CERT version but with a different layout
1.0.1	01/08/2020	Updated content of the IRM – some content was removed, updated and added
1.0.2	05/08/2020	Initial internal release
1.1.0	11/08/2020	Updated the IRM layout first page, removed any company logos and added IRM definition, added a link to the SG CERT github repository on each IRM page. Added a section on the overall IRM structure.

OVERVIEW

This document provides a number of Incident Response Methodologies (IRM) aimed at helping a company with the handling of different types of cyber incidents.

It has been laid out so each IRM can be printed as a dual sided standalone page.

Compare to the great work done by the SG CERT this version provides:

- A definition for each type of IRM documented;
- New order to the IRM references;
- Cosmetic changes;
- Opportunity to include your incident response team contact details;
- A more visual IRM cycle;
- Updates to the content of the IRMs;
- Standardisation of the each phase objectives definition;
- Standardisation of the Lessons Learnt phase actions.

Although this document can be used AS-IS, we recommend you do the following:

- Review each IRM to ensure the actions listed are aligned with your Incident Response processes;
- Include your incident contact details in each of the IRM abstract section.

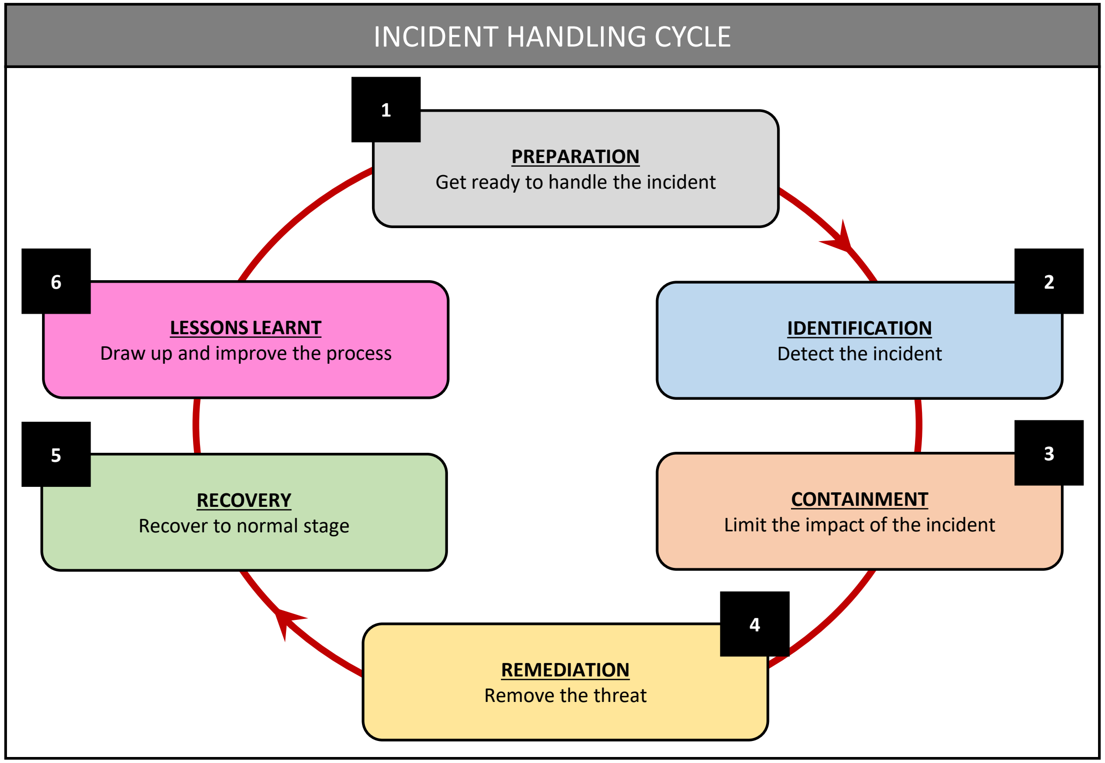
INCIDENT RESPONSE METHODOLOGIES LIST & MAPPING

ELYSIUMSECURITY REFERENCE	SCOPE	ES VERSION	SG CERT REFERENCE	SG CERT VERSION
IRM #1	PHISHING	V1.2	IRM #13	V1.1
IRM #2	SCAM	V1.1	IRM #14	V1.1
IRM #3	SOCIAL ENGINEERING	V1.1	IRM #10	V1.2
IRM #4	INFORMATION LEAKAGE	V1.1	IRM #11	V1.2
IRM #5	INSIDER ABUSE	V1.1	IRM #12	V1.1
IRM #6	MOBILE MALWARE	V1.1	IRM #9	V1.2
IRM #7	WINDOWS MALWARE	V1.1	IRM #7	V1.3
IRM #8	WINDOWS INTRUSION	V1.1	IRM #2	V1.2
IRM #9	UNIX INTRUSION	V1.1	IRM #3	V1.4
IRM #10	RANSOMWARE	V1.2	IRM #17	V1.0
IRM #11	DDOS	V1.1	IRM #4	V1.4
IRM #12	NETWORK ATTACK	V1.1	IRM #5	V1.4
IRM #13	WEBSITE DEFACEMENT	V1.1	IRM #6	V1.3
IRM #14	WORM INFECTION	V1.1	IRM #1	V1.3
IRM #15	BLACKMAIL	V1.1	IRM #8	V1.3
IRM #16	TRADEMARK INFRINGEMENT	V1.1	IRM #15	V1.1

OVERALL STRUCTURE

Each IRM is based on the following standard incident handling cycle which contains 6x phases. Each phase in that cycle has a dedicated and documented section with the same colour coding header used in the diagram below.

Each IRM starts with a definition of its scope and each section in those IRMs starts with a set of objectives.



INCIDENT HANDLING CYCLE

1 **PREPARATION** Get ready to handle the incident

2 **IDENTIFICATION** Detect the incident

3 **CONTAINMENT** Limit the impact of the incident

4 **REMEDIATION** Remove the threat

5 **RECOVERY** Recover to normal stage

6 **LESSONS LEARNT** Draw up and improve the process

IRM #1

PHISHING

Guidelines to handle phishing incidents
Version 1.2

PHISHING DEFINITION

“The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers”
(OXFORD LANGUAGES)

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue. It is aimed at:

- Administrators
- Security Teams and Operation Centre
- CISOs and deputies

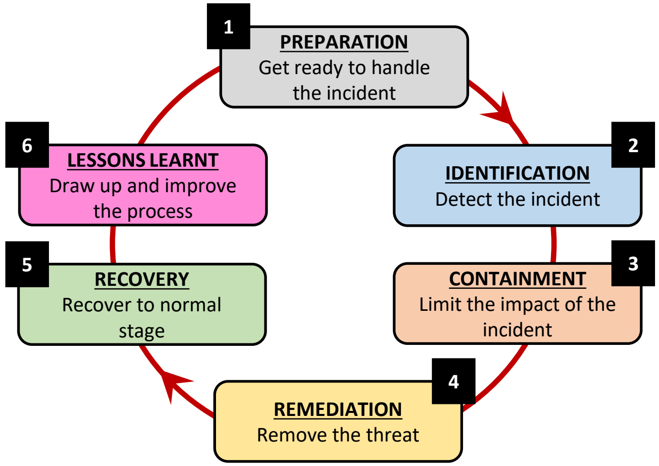
Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line’s Incident.

Incident Response Team contact:

____

____

INCIDENT HANDLING CYCLE



1 **PREPARATION** Get ready to handle the incident

2 **IDENTIFICATION** Detect the incident

3 **CONTAINMENT** Limit the impact of the incident

4 **REMEDIATION** Remove the threat

5 **RECOVERY** Recover to normal stage

6 **LESSONS LEARNT** Draw up and improve the process

1 PREPARATION

Objective: Establish contacts, define procedures, gather information to save time during an attack.

- Create a list of all legitimate domains belonging to your company. This will help analysing the situation, and prevent you from starting a takedown procedure on a forgotten legitimate website.
- Prepare one web page hosted on your infrastructure, ready to be published anytime, to warn your customers about an ongoing phishing attack. Prepare and test a clear deployment procedure as well.
- Prepare takedown e-mail forms. You will use them for every phishing case, if possible in several languages. This will speed up things when trying to reach the hosting company etc. during the takedown process.
- Implement active anti-phishing solutions, like Mimecast, Proofpoint, TrendMicro, MS ATP, etc.
- Implement a staff phishing reporting process.

Internal contacts

- Maintain a list of all people involved in domain names registration in the company.
- Maintain a list of all people accredited to take decisions on cybercrime and eventual actions regarding phishing. If possible, have a contract mentioning you can take decisions.

External contacts

- Have several ways to be reached in a timely manner (24/7 if possible):
  - E-Mail address, easy to remember for everyone
  - Web forms on your company’s website (max 2 clicks away from the main page)
  - Visible Twitter account
- Establish and maintain a list of takedown contacts in:
  - Hosting companies
  - Registry companies
  - E-Mail providers
- Establish and maintain contacts in CERTs worldwide, they will probably always be able to help if needed.

1 PREPARATION

Raise customer awareness

Don’t wait for phishing incidents to communicate with your customers. Raise awareness about phishing fraud, explain what phishing is and make sure your customers know you won’t ever ask them for credentials or banking information by e-mail or on the phone.

Raise business line awareness

People in business lines must be aware of phishing problems and consider security as a priority. Therefore, they should apply good practices such as avoid sending links (URL) to customers, and use a signature stating that the company will never ask them for credential or banking information online.

2 IDENTIFICATION

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

Phishing Detection

- Monitor all your points of contact closely (e-mail, web forms, etc.)
- Deploy phishing traps and try to gather phishing from partners/third-parties
- Review your Anti-phishing report regularly
- Investigate staffs’ report of suspicious email
- Monitor your web logs. Check there is no suspicious referrer bringing people to your website. This is often the case when the phishing websites brings the user to the legitimate website after he’s been cheated.

Document created by ELYSUMSECURITY LTD – https://www.elysiumsecurity.com – Based on the Société Générale IRM 13 freely available on github

2 IDENTIFICATION

Involve appropriate parties

As soon as a phishing website is detected, contact the people in your company who are accredited to take a decision, if not you. The decision to act on the fraudulent website/e-mail address must be taken as soon as possible, within minutes.

Collect evidence

Make a time-stamped copy of the phishing web pages. Use an efficient tool to do that, like HTTrack for example. Don't forget to take every page of the phishing scheme, not just the first one if there are several. If needed, take screenshots of the pages.

3 CONTAINMENT

Objective: Mitigate the attack's effects on the targeted environment.

- In case of a phishing website, block the URL of the attack everywhere (web proxy, firewall, AV, etc) in case of a phishing website.
- Report the fraudulent e-mail content on spam-reporting websites/partners.
- Communicate with your customers if required.
- If the attack is public, deploy the alert/warning page with information about the current phishing attack.
- In case you are impacted several times a week, don't always deploy an alert/warning message but rather a very informative phishing page to raise awareness.
- Check the source-code of the phishing website and see where the data is exported: either to another web content you cannot access (a PHP script usually),   or sent by e-mail to the fraudster.
- Watch how the phishing-page is built. Do the graphics come from one of your legitimate website, or are they stored locally? in case the graphics are taken from one of your own websites, you could change the graphics to display a "PHISHING WEBSITE" logo on the fraudster's page.

4 REMEDIATION

Objective: Objective: Take actions to remove the threat and avoid future incidents.

- In case the fraudulent phishing pages are hosted on a compromised website, try to contact the owner of the website. Explain clearly the fraud to the owner, so that he takes appropriate actions: remove the fraudulent content, and most of all upgrade the security on it, so that the fraudster cannot come back using the same vulnerability.
- In any case, also contact the hosting company of the website. Send e-mails to the contact addresses of the hosting company (generally there is an abuse@hostingcompany) then try to get someone on the phone, to speed things up.
- Contact the e-mail hosting company to shut down the fraudulent accounts which receive the stolen credentials or credit card information (Either on an "e-mail only" phishing case or on a usual one, if you managed to get the destination e-mail address).
- In case there is a redirection (the link contained in the e-mail often goes to a redirecting URL) also take down the redirection by contacting the company responsible for the service.

In case you get no answer, or no action is taken, don't hesitate to call back and send e-mails on a regular basis, every two hours for example.

- If the takedown is too slow, contact a local CERT in the involved country, which could help taking down the fraud.

5 RECOVERY

Objective: Restore the system to normal operations.

Assess the end of the phishing case

- Ensure that the fraudulent pages and/or e-mail address are down.
- Keep monitoring the fraudulent URL. Sometimes a phishing website can reappear some hours later. In case a redirection is used and not taken down, monitor it very closely.
- At the end of a phishing campaign, remove the associated warning page from your website.

6 LESSONS LEARNT

Objective: Document the incident's details, discuss lessons learned, and adjust plans and defences.

Inform your hierarchy and subsidiaries about the incident, this could help to avoid similar attacks later.

Report

An incident report should be written and made available to all of the stakeholders.
The following themes should be described:

- Initial detection.
- Actions and timelines.
- What went right.
- What went wrong.
- Incident cost.

Capitalize

Actions to improve impersonation and credential harvesting protection should be defined to capitalize on this experience.

IRM #2
SCAM

Guidelines to handle fraudulent scam incidents
Version 1.1

SCAM DEFINITION

"A fraudulent or deceptive act, especially armed at defrauding someone or group of their money or other valuables."
(IGI GLOBAL)

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue. It is aimed at:

- Administrators
- Security Teams and Operation Centre
- CISOs and deputies

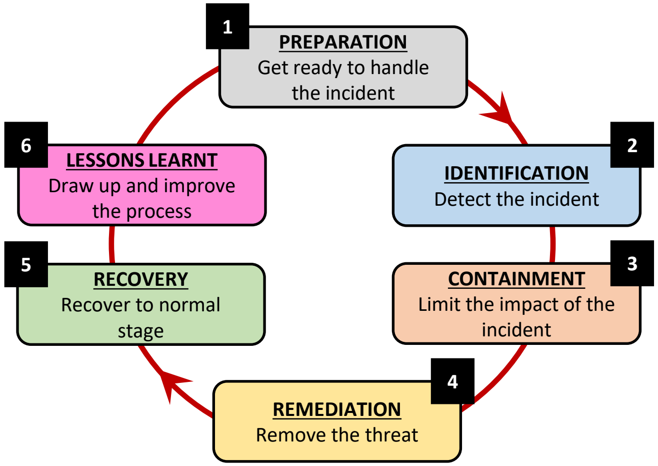
Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident.

Incident Response Team contact:

____

____

INCIDENT HANDLING CYCLE



1 **PREPARATION** Get ready to handle the incident

2 **IDENTIFICATION** Detect the incident

3 **CONTAINMENT** Limit the impact of the incident

4 **REMEDIATION** Remove the threat

5 **RECOVERY** Recover to normal stage

6 **LESSONS LEARNT** Draw up and improve the process

1 PREPARATION

Objective: Establish contacts, define procedures, gather information to save time during an attack.

Create a list of all legitimate domains belonging to your company and prevent you from starting a takedown procedure on a "forgotten" legitimate website.

- Prepare one web page hosted on your infrastructure, ready to be published anytime, to warn your customers about a large ongoing fraudulent scam attack. Prepare and test a clear deployment procedure as well.
- Prepare takedown e-mail forms. You will use them for every fraudulent scam case, if possible in several languages. This will speed up things when trying to reach Internet operating companies during the takedown process.
- Have several ways to be reached in a timely manner (24/7 if possible):
  - E-Mail address, easy to remember for everyone
  - Web forms on your company's website (max 2 clicks away from the main page)
  - Visible Twitter account

Contacts

- Maintain a list of all people accredited to take decisions on cybercrime and eventual actions regarding the topic. If possible, establish a contract with clear processes.
- Establish and maintain a list of takedown contacts in:
  - Hosting companies
  - Registrars
  - Registry companies
  - E-Mail providers
- Establish and maintain contacts in CERTs worldwide, they will probably always be able to help if involved.

Raise customer awareness

Don't wait for scam incidents to communicate with your customers. Raise awareness on several kinds of scamming fraud (lottery scam, 419 scam etc.), explain what it is and make sure your customers know you won't ever contact them for such matters by e-mail.

2 IDENTIFICATION

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

Fraudulent scam detection

- Monitor all your points of contact closely (e-mail, web forms, etc.)
- Deploy spam traps and try to gather spam from partners/third-parties.
- Deploy active monitoring of scam repositories, like 419scam or Millersmiles for example.
- Monitor any specialised mailing-list you can have access to, or any RSS/Twitter feed, which could be reporting scam letters.
- Use automated monitoring systems on all of these sources, so that every detection triggers an alarm for instant reaction.

Involve appropriate parties

As soon as a scam campaign is detected, contact the people in your company who are accredited to take a decision, if not you.
The decision to act on the fraudulent e-mail address must be taken as soon as possible, within minutes.

Collect evidence

Get samples of the fraudulent e-mails sent by the fraudsters. Be careful to collect the e-mail headers in addition to the e-mail content. Collect several e-mails if possible, to check for the real sender's IP address. This will help the investigation, analysing if the campaign is sent from one machine or from a botnet.

If you feel unsure about collecting e-mail headers, please check http://spamcop.net/fom-serve/cache/19.html

3 CONTAINMENT

Objective: Mitigate the attack's effects on the targeted environment.

- Report the fraudulent e-mail content on spam/fraud reporting websites/partners/tools.
- Communicate with your customers.
- Deploy the alert/warning page with information about the current scam attack if the brand is impacted.
- In case you are impacted several times a week, don't always deploy an alert/warning message but rather a very informative page about scam, to raise awareness.

4 REMEDIATION

Objective: Take actions to remove the threat and avoid future incidents.

- In case there is a fraudulent web page related to the fraud, hosted on a compromised website, try to contact the owner of the website. Explain clearly the fraud to the owner, so that he takes appropriate actions: remove the fraudulent content, and most of all upgrade the security on it, so that the fraudster cannot come back using the same vulnerability.
- In any case, also contact the hosting company of the website. Send e-mails to the contact addresses of the hosting company (generally there is an abuse@hostingcompany) then try to get someone on the phone, to speed things up.
- Contact the e-mail hosting company to shut down the fraudulent account of the fraudster. Don't forget to send them a copy of the fraudulent e-mail.
- In case you get no answer, or no action is taken, call back and send e-mails on a regular basis.
- If the takedown is too slow, contact a local CERT in the involved country, which could help taking down the fraud, and explain them the difficulties you face.

5 RECOVERY

Objective: Restore the system to normal operations.

Assess the end of the case

- Ensure that the fraudulent e-mail address has been shut down.
- If there is any fraudulent website associated to the fraud, keep monitoring it.
- At the end of a fraudulent scam campaign, remove the associated warning page from your website.

6 LESSONS LEARNT

Objective: Document the incident's details, discuss lessons learned, and adjust plans and defences.

Inform your hierarchy and subsidiaries about the incident, this could help to avoid similar attacks later.

Report

An incident report should be written and made available to all of the stakeholders.

The following themes should be described:

- Initial detection.
- Actions and timelines.
- What went right.
- What went wrong.
- Incident cost.

Capitalize

Actions to improve fraud detection and protection should be defined to capitalize on this experience.

IRM #3

SOCIAL ENGINEERING

Guidelines to handle a social engineering incident (phone or email)
Version 1.1

SOCIAL ENGINEERING DEFINITION

“the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes”
(OXFORD LANGUAGES)

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue. It is aimed at:

- Administrators
- Security Teams and Operation Centre
- CISOs and deputies

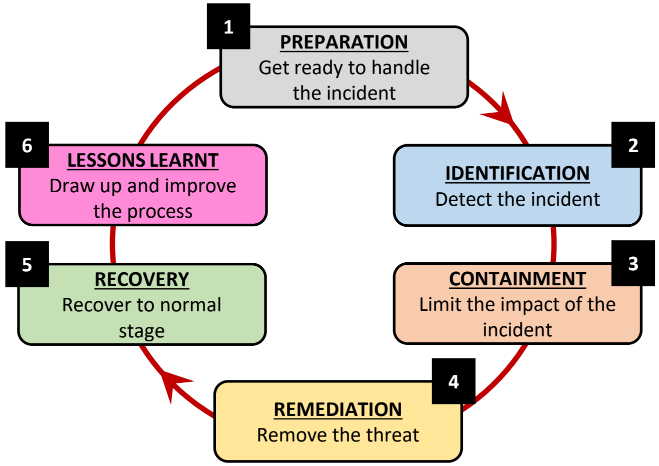
Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line’s Incident.

Incident Response Team contact:

____

____

INCIDENT HANDLING CYCLE



1 **PREPARATION** Get ready to handle the incident

2 **IDENTIFICATION** Detect the incident

3 **CONTAINMENT** Limit the impact of the incident

4 **REMEDIATION** Remove the threat

5 **RECOVERY** Recover to normal stage

6 **LESSONS LEARNT** Draw up and improve the process

1 PREPARATION

Objective: Establish contacts, define procedures, gather information to save time during an attack.

- Raise user awareness and security policies
- Never give any personal or corporate information to an unidentified person. This could include user IDs, passwords, account information, name, e-mail address, phone (mobile or landline) numbers, address, social security number, job titles, information on clients, organization or IT systems.
- The goal of the social engineer is to steal human resources, corporate secrets or customer/user data.
- **Report any suspicious event to your manager, who will forward it to the CISO in order to have a centralized reporting.**
- Have a defined process to redirect any “weird” request to a “red” phone, if needed. Red phone number must be clearly tagged as “Social Engineering”. **The phone number has to be easy to identify in the global phone directory of your company but requests on reverse number should not be displayed.**
- Red phone line should always be recorded for evidence collecting purposes.
- Prepare to handle conversation with social engineers to identify which information could help tracking the attacker and his goals.
- Check your legal department to see which actions are allowed and which reactions they can handle.

2 IDENTIFICATION

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

WARNING: This part has to be mostly done by the user

Phone call

- Someone you don't know calls you/your service, asking for detailed information.
- If the contact works out of the company and requests for information that could be valuable for a competitor, deny his requests and go to part 3.
- If the contact pretends to be an employee of your company but the phone number is hidden or not internal, propose that you call back to the declared number in the directory. If the supposedly attacker agrees, call back to check. If he rejects this option, go to part 3.
- The attacker might use several techniques to entice his victim to speak (fear, curiosity, empathy ...). Do not disclose information in any case.
- Listen carefully to his requests and at the end ask for a phone number to call back or an email address to reply.
- Take notes and stay calm, even if the attacker is shouting or threatening, remember he tries to use human weaknesses.
- If you can go further, the following information will be precious: the name of the correspondent, requested information / people, accent, language skills, industry language and organizational knowledge, background noises, time and duration of the call

2 IDENTIFICATION

E-mail

Someone you don't know requests detailed information.

- If the contact has an “out of the company” e-mail address and requests information that could be valuable for a competitor, go to part 3.
- If the contact uses an internal e-mail address but is asking for weird information, ask him some explanations and use the company directory to get his manager's name that you'll place as a copy.
- Eventually notify top management to inform them that an incident has been encountered relating to a social engineering attack. They might understand the goals depending on the context.

3 CONTAINMENT

Objective: Mitigate the attack’s effects on the targeted environment.

WARNING: This part has to be mostly done by the user

At this step, you should be pretty sure that you're dealing with a social engineering attack.

Actions for all employees:

Phone call

- If the attacker urges you to give a phone number, follow these steps:
  - Use the “red phone line” from your CERT/CSIRT, if existing.
  - Give him the number with an invented name.
  - Immediately call your CERT/CSIRT team explaining what happened and the chosen invented name.
- If the attacker stresses you too much and does not let you time to find the Red Phone number, ask him to call you back later, pretending a meeting.

3 CONTAINMENT

- If the attacker wants to reach someone, follow these points :
  - Place on hold the attacker and call CERT/CSIRT team and explain what happened
  - Transfer the conversation of the attacker to CERT/CSIRT team (do not give him the number)

E-mail

Forward to your security team all email including headers (send as attached documents) for investigation purposes. It might help to track the attacker.

Actions for CERT or incident response team:

Phone call

- Resume the conversation with the attacker and use one of these techniques:
  - Impersonate the identity of the people whom the attacker is willing to speak
  - Slow down and make last the conversation and entice the attacker to make mistake.
  - Explain him that social engineering attack is forbidden by law, punished by sanctions and that lawyer team will handle the issue if it continues
- If the trap phone number has been used, prepare to “burn it”, create another one and display it in the directory.

E-mail

- Collect as much information as possible on the email address:
  - Analyze the email headers and try to locate the source
  - Search the e-mail address with Internet tools
  - Geolocalize the user behind the email address

Aggregate all social engineering attacks to visualize the scheme.

4 REMEDIATION

Objective: Take actions to remove the threat and avoid future incidents.

Some possible remediation actions can be tried:

- Alert the law enforcement and/or file a complaint,
- Discuss the problem in circles of trust to know if the company is facing this issue alone,
- Threaten the attacker with legal actions if he can be identified

5 RECOVERY

Objective: Restore the system to normal operations.

Notify the top management of the actions and the decisions taken on the social engineering case.

6 LESSONS LEARNT

Objective: Document the incident’s details, discuss lessons learned, and adjust plans and defences.

Inform your hierarchy and subsidiaries about the incident, this could help to avoid similar attacks later.

Report

An incident report should be written and made available to all of the stakeholders.

The following themes should be described:

- Initial detection.
- Actions and timelines.
- What went right.
- What went wrong.
- Incident cost.

Capitalize

Actions to improve the social engineering handling processes should be defined to capitalize on this experience.

IRM #4

INFORMATION LEAKAGE

Guidelines to handle and respond to information disclosed intentionally
Version 1.1

INFORMATION LEAKAGE DEFINITION

“unintended loss of information from an organization. This usually occurs as a result of employees passing information to others sometimes unwittingly sometimes wittingly.”
(IGI GLOBAL)

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue. It is aimed at:

- Administrators
- Security Teams and Operation Centre
- CISOs and deputies

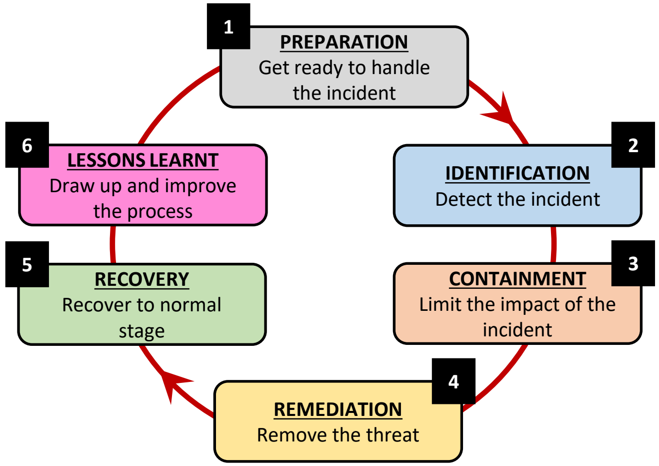
Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line’s Incident.

Incident Response Team contact:

____

____

INCIDENT HANDLING CYCLE



1 **PREPARATION** Get ready to handle the incident

2 **IDENTIFICATION** Detect the incident

3 **CONTAINMENT** Limit the impact of the incident

4 **REMEDIATION** Remove the threat

5 **RECOVERY** Recover to normal stage

6 **LESSONS LEARNT** Draw up and improve the process

1 PREPARATION

Objective: Establish contacts, define procedures, gather information to save time during an attack.

Contacts

- Identify internal technical contacts (security team, incident response team …)
- Make sure to have contact points in your public relation team, human resources team and legal department
- Identify external contacts who might be needed, mainly for investigation purposes (like Law Enforcement for example).

Security policy

- Make sure that the corporate information value is explained in the rules of the procedure, the IT chart, awareness and training session
- Make sure all valuable assets are identified as it should be
- Make sure that security incident escalation process is defined and the actors are clearly defined and identified.

2 IDENTIFICATION

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

Data leak can occur from anywhere. Remember that the cause of the leakage can be an individual employee willingly or unwillingly bypassing security issues, or a compromised computer.

Step 1: DETECT THE ISSUE

- **Incident notification process:** Internal information can be a good source of detection: employee confidence, security team identifying a problem, etc.

- **Public monitoring tool:** A watch on Internet search engines and public database can be very valuable to detect information leakage.

2 IDENTIFICATION

- **DLP (Data Loss Prevention) tool:** If there is a DLP tool in the company, it can provide valuable information to incident handlers working on information leakage.

Step 2: CONFIRM THE ISSUE

Don’t do anything, without a written request from the concerned CISO/person in charge. Based on your legal team advisory, a written permission from the concerned user might also be handy.

- **E-Mail:**

The disclosure source could have sent data using his corporate e-mail address.
On the messaging system, look for e-mails sent to or received from a suspect account or with a special subject.
On the e-mail client on the desktop of the suspect (if available), use a tool which allows you to search by filtering out the “PRIVATE” flagged e-mails. If you really need to do so, ask the user for a written agreement or ask him to be with you. When applicable, look through related log files.

Use forensic tools to check for deleted browsing history.
Also check all the offline content left from all browsing.

- **Browsing:**

Data might have been sent on webmail/forums/dedicated websites.
On the proxy server, check the logs relating to the suspect account connections on the suspected URL used to disclose data.
On the desktop (if available), check the history of the installed browsers. Remember some people might have different browsers on the same desktop computer; be sure to check every browser history. If the moment of the data leak can be time-stamped, some log files can provide useful information.

2 DETECTION

- **External storage devices:**

A various number of devices can be used to store data: USB keys, CD-ROM, DVD, external hard disks, smartphones, memory cards…
Little information will be found concerning data transfer using these devices. The USB key used to transfer data can be referenced by the operating system. A forensic analysis can confirm the use of hardware but not the data transmitted.

- **Local files:**

If nothing has been found yet, there are still chances to find traces in the local file system of the suspect. Just like for e-mail researches, use a parsing tool which forbids any access to the PRIVATE zone of the user. If you really need to do so, act accordingly to local employment law.

- **Network transfer:**

Multiple ways might be used to transfer data out of the company: FTP, instant messenger, etc. Try to dig into log files showing such activity.
Data might also have been sent using a VPN tunnel or on an SSH server. In this case, one can prove the connection by watching log files but can't see the content transmitted.

- **Printer:**

Data can be sent to printers connected to the network. In this case, check for traces on the spooler or directly on the printer, since some constructors directly store printed documents on a local hard drive.

- **Malware:**

If nothing has been found, think of a possible malware compromise and act accordingly with the "Malware Detection" IRM.

Note: Even when enough evidence has been found, always look for more. It is not because you proved that data got fraudulently from A to B with one method that it wasn't also sent to C with another method. Also don't forget that someone else could have accessed the computer. Was the suspected employee actually in front of his computer when the leak occurred?

3 CONTAINMENT

Objective: Mitigate the attack's effects on the targeted environment.

Notify the management, legal and PR team to make sure they are prepared to deal with a massive or targeted disclosure.

Depending on the leakage vector, block the access to the disclosure URI, the disclosure server, the disclosure source or the disclosure recipients. This action must be done on all infrastructure points.

Suspend the logical and physical credentials of the insider if the leakage has been confirmed. Involve HR and legal team before any action.

Isolate the computing system (desktop, printer) used to disclose data in order to perform a forensic analysis later. This manipulation should be done the hard way: remove the electric plug (and the battery in case of a laptop).

4 REMEDIATION

Objective: Take actions to remove the threat and avoid future incidents.

If data has been sent to public servers, ask the owner (or webmaster) to remove the disclosed data. Be sure to adjust your request to the recipients (hacktivism webmaster won't behave as a press webmaster)

If it's not possible to remove the disclosed data, provide a complete analysis to the PR team and the management. Monitor leaked documents spread on websites and social networks (FB, Twitter, etc) and Internet user's comments or reactions.

Provide the elements to HR team to eventually file a complaint against the insider.

5 RECOVERY

Objective: Come back to the previous functional state.

If a system has been compromised, restore it completely.
Eventually warn your employees or some local teams about the issue to raise awareness and increase security rules.
When situation comes back to normal, eventually remove the official communication.

6 LESSONS LEARNT

Objective: Document the incident's details, discuss lessons learned, and adjust plans and defences.

Inform your hierarchy and subsidiaries about the incident, this could help to avoid similar attacks later.

Report
An incident report should be written and made available to all of the stakeholders.
The following themes should be described:

- Initial detection.
- Actions and timelines.
- What went right.
- What went wrong.
- Incident cost.

Capitalize
Actions to improve information leakage handling processes should be defined to capitalize on this experience.

IRM #5

INSIDER ABUSE

Guidelines to handle internal abuse of systems and processes
Version 1.1

INSIDER ABUSE DEFINITION

"deliberate abuse of the organization's systems by an authorized user."
(CIMCOR)

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue. It is aimed at:

- Administrators
- Security Teams and Operation Centre
- CISOs and deputies

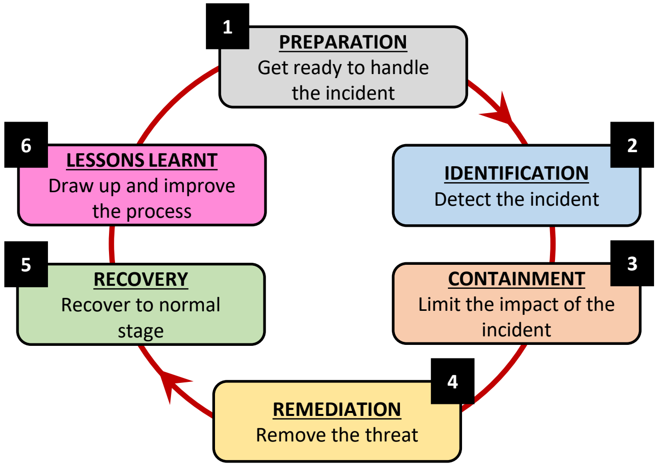
Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident.

Incident Response Team contact:

____

____

INCIDENT HANDLING CYCLE



1 PREPARATION

Objective: Establish contacts, define procedures, gather information to save time during an attack.

Contacts

- Make sure to also have contact points in your public relation team, human resources team and legal department
- Have a centralized logging facility
- Be sure to have a global authorization and clearance process. This process must specially take care of the removal of privileges on former jobs
- Provide strong authentication accordingly to the risk of the business application

2 IDENTIFICATION

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

Insider abuses are hard to detect and there is no 100% success tips.

Technical identification

- **Alerts from a SIEM or correlation tools**

Malicious behaviour can have been detected with the correlation of several abnormal events

- **Alerts from an IDS/IPS detecting an intrusion**

In case the insider tried to hack the system, an Intrusion Detection System (or Intrusion Prevention System) can be able to trigger an alert.

Human identification

- **Management:**

The manager of the insider might be the first to notice the suspected behaviour.

- **Control, risk, compliance:**

These teams have their own systems to detect operational anomalies and they can also trigger alerts if something abnormal is detected.

- **Colleagues:**

Insider's colleagues are maybe the most valuable notification channel because they know perfectly the tasks, the process and the impacts on their duty jobs. They can guess easily what is happening.

- **External parties:**

External partners or structure can also have their own detection capabilities. If operations have been falsified internally, these external entities can bring a real enlightenment.

3 CONTAINMENT

Objective: Mitigate the attack's effects on the targeted environment.

Don't do anything, without a written request from the concerned CISO/person in charge. Based on your legal team advisory, a written permission from the concerned user might also be handy.

- **Involve people:**

Different people should be informed about the abuse so that they can help to assist on it. This includes HR management, legal management, PR management and business management of the suspected insider.

- **Meeting:**

An HR manager should meet the suspected insider to explain him/her what has been found and what will happen. Support can be required from legal, technical and management people.

- **Privileges lowering:**

If the suspected insider is allowed to stay at work until the end of the investigation, provide him/her a computer with minimum authorizations.

- **Authorization freeze:**

Suspend access and authorizations of the suspected insider. This must include application clearance. This can also include system account, keys, building facility badge.

- **Remote access:**

Suspend remote access capabilities, i.e.: smartphones, VPN accounts, tokens...

- **Seizure:**

Seize all the professional computing device of the suspected insider.

3 CONTAINMENT

Case 1: abnormal activity

If nothing malicious or fraudulent is confirmed yet, two investigations should start right now:
- forensics investigation on the computing devices of the suspected insider.
- log investigation on different audit trails components

Case 2: malicious / fraudulent activity

If malicious or fraudulent behaviour is already confirmed, think about file a complaint against the suspected insider.

In this case, do not take any further technical actions. Provide the legal team or law enforcement officer all requested evidences and be ready to assist on demand.

If collateral damages can result from the abuse, be sure to contain the incident impacts before making it public. Be sure to inform authorities if required.

4 REMEDIATION

Objective: Take actions to remove the threat and avoid future incidents.

The remediation part is pretty limited in case of an insider abuse. Following actions can be considered depending on the case:

■ Take disciplinary action against the malicious employee (or terminate the contract) and remove all his/her credentials.

■ Delete all fictitious or fraudulent operations made by the insider

■ Review all programs or scripts made by the insider and remove all unnecessary codes

5 RECOVERY

Objective: Restore the system to normal operations.

If the incident has not been made public yet, be sure to warn all the impacted stakeholders (customers, concerned partners …) and required authorities. This communication must be made by top management in case of huge impacts.

Eventually warn your employees or some local teams about the issue to raise awareness and increase security rules.

6 LESSONS LEARNT

Objective: Document the incident's details, discuss lessons learned, and adjust plans and defences.

Inform your hierarchy and subsidiaries about the incident, this could help to avoid similar attacks later.

Report

An incident report should be written and made available to all of the stakeholders.
The following themes should be described:

- Initial detection.
- Actions and timelines.
- What went right.
- What went wrong.
- Incident cost.

Capitalize

Actions to improve the social engineering handling processes should be defined to capitalize on this experience. For example:

- Authorization process improvements
- Controls improvements in the organisation
- Awareness on fraud and malicious activity

IRM #6
MOBILE MALWARE

Guidelines to handle suspicious mobile phone and app
Version 1.1

MOBILE MALWARE DEFINITION

"malicious software that specifically targets the operating systems on mobile phones."
(FORCEPOINT)

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue. It is aimed at:

- Administrators
- Security Teams and Operation Centre
- CISOs and deputies

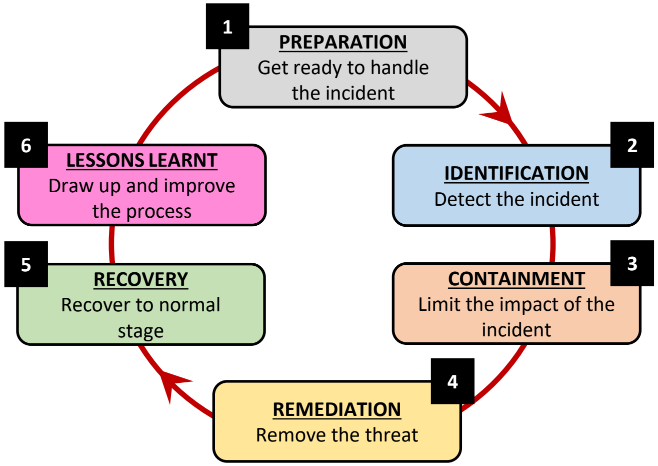
Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident.

Incident Response Team contact:

____

____

INCIDENT HANDLING CYCLE



1 **PREPARATION** Get ready to handle the incident

2 **IDENTIFICATION** Detect the incident

3 **CONTAINMENT** Limit the impact of the incident

4 **REMEDIATION** Remove the threat

5 **RECOVERY** Recover to normal stage

6 **LESSONS LEARNT** Draw up and improve the process

1 PREPARATION

Objective: Establish contacts, define procedures, gather information to save time during an attack.

- Mobile helpdesk must have a defined process in case of a suspected malware infection: replace the smartphone of the user with a new one and isolate the suspicious device for analysis by the forensic investigator.

- A good knowledge of the usual activity of the smartphone is appreciated (default and extra tools running on it). A smartphone support expert can be helpful to assist the forensic investigator.

- A monitoring should be done to check unusual user bill or network activity.

2 IDENTIFICATION

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

Main points of notification for suspicious smartphone:

- Antivirus raises alerts;
- Unusual system activity, unusually slow system;
- Unusual network activity, very slow Internet connection;
- The system reboots or shutdowns without reason;
- Some applications crash unexpectedly;
- User receive one or multiple messages, some could have unusual characters (SMS, MMS, Bluetooth messages, etc.);
- Huge increase in phone bill or web activity.
- Unusual calls to unusual phone numbers or at unusual hours/days.

Evidence such as website URLs need to be gathered.
Ask the user about his/her usual activity on the smartphone: which websites are browsed, which external applications are installed. This information can optionally be cross-checked with the company's policy.

3 CONTAINMENT

Objective: Mitigate the attack's effects on the targeted environment.

- Ensure user is given a temporary or new permanent device to avoid any time constraint on the investigation;
- Back up the smartphone data;
- Remove battery to block all activity (wifi, Bluetooth, etc);
- Launch an antivirus check on the computers that are/have been synchronized or linked with the smartphone;
- Send the suspicious smartphone and appropriate components (SIM, battery, power cable, memory cards) to your security incident response team. This team will help to isolate the malicious content and send it to antivirus companies;

4 REMEDIATION

Objective: Take actions to remove the threat and avoid future incidents.

If some encryption or password accesses are set, find out a way to get access to the stored data. If this is not possible, the investigation will suffer high limitations.

Specific tools should be used by your incident response team to lead forensic investigation on the smartphone.

There are three areas you should focus:

1. **The network traffic:** intercepting and analysing the network traffic from the phone/app using a proxy such as BURP Suite;
2. **The phone settings:** looking at privacy and app settings for anything suspicious, this includes trusted certificates;
3. **The mobile apps:** If possible, identify and decompile any suspicious app for analysis;

Actions:

- Remove SIM from the smartphone and disable data network (i.e.: WIFI and mobile data) if not already done;
- Recover phone history, web history and all available logs;
- Recover server connections log if available;
- Identify and remove the threat on the smartphone;
- if the threat is related to an installed application, identify its location on Internet and remove it.

5 RECOVERY

Objective: Restore the system to normal operations.

If user needs to recover from the infected support, define a quarantine period and appropriate anti-virus check, if possible, to ensure nothing could harm user or the company's systems.

Restore the data saved previously from a trusted source on the destination device.

Once the investigations are over, wipe the infected smartphone (if possible) and reset it to factory settings with a pristine firmware and file system, in order to be used again.

6 LESSONS LEARNT

Objective: Document the incident's details, discuss lessons learned, and adjust plans and defences.

Inform your hierarchy and subsidiaries about the incident, this could help to avoid similar attacks later.

Report

An incident report should be written and made available to all of the stakeholders.
The following themes should be described:

- Initial detection.
- Actions and timelines.
- What went right.
- What went wrong.
- Incident cost.

Capitalize

Actions to improve mobile phone usage policy and related processes should be defined to capitalize on this experience.

IRM #7

WINDOWS MALWARE

Guidelines to handle suspicious activities from a Windows machine
Version 1.1

WINDOWS MALWARE DEFINITION

"malicious software that specifically targets the operating systems of electronic devices running on windows."
(ELYSIUMSECURITY & FORCEPOINT)

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue. It is aimed at:

- Administrators
- Security Teams and Operation Centre
- CISOs and deputies

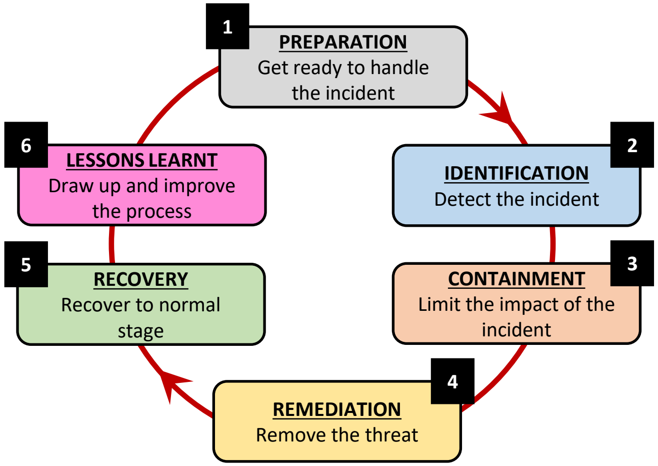
Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident.

Incident Response Team contact:

____

____

INCIDENT HANDLING CYCLE



1 PREPARATION

Objective: Establish contacts, define procedures, gather information to save time during an attack.

- A physical access to the suspicious system should be offered to the forensic investigator.
- A good knowledge of the usual network and local activities of the computer is appreciated. You should have a file describing the usual port activity, to have a comparison base with current state.
- A good knowledge of the common used services and installed applications is needed. Don't hesitate to ask a Windows Expert for their assistance, when applicable.

2 IDENTIFICATION

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

General signs of malware presence on the desktop

Several leads might hint that the system could be compromised by malware:

- Antivirus software raising an alert, unable to update its signatures, shutting down or unable to run manual scans;
- Unusual hard-disk activity: the hard drive makes huge operations at unexpected times;
- Unusually slow computer: sudden, unexplained slowdowns not related to system usage;
- Unusual network activity: Slow internet connection / poor network share performance at irregular intervals;
- The computer reboots without reason;
- Applications crashing unexpectedly
- Pop-up windows appearing while browsing the web; (sometimes even without browsing)
- Your IP address (if static) is blacklisted on one or more Internet Black Lists;
- People are complaining about you e-mailing them/reaching them by IM etc. while you did not;

2 IDENTIFICATION

Actions below uses default Windows tools. Authorized users can use the **SysInternals** Troubleshooting Utilities to perform these tasks.

Volatile data

Before carrying out any other actions, make sure to make a volatile memory capture by downloading and run the DumpIt utility from a USB key

Volatile data provides valuable forensic information and is straightforward to acquire.

Unusual Accounts

Look for unusual and unknown accounts created, especially in the Administrators group:

C:\> lusrmgr.msc

Unusual Files

- Look for unusual big files on the storage support, bigger than 10MB seems to be reasonable.
- Look for unusual files added recently in system folders, especially *%SystemRoot%\system32*.
- Look for files using the "hidden" attribute:

C:\> dir /S /A:H

Unusual Registry Entries

Look for unusual programs launched at boot time in the Windows registry, especially:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run*

Check for the same entries in HKCU

Unusual Processes and Services

- Check all running processes for unusual/unknown entries, especially processes with username "SYSTEM" and "ADMINISTRATOR" :

C:\> taskmgr.exe

(or tlisk, tasklist depending on Windows release)

- Look for unusual/unexpected network services installed and started:

C:\> services.msc

C:\> net start

Document created by ELYSUMSECURITY LTD – https://www.elysiumsecurity.com – Based on the Société Générale IRM 7 freely available on github

2 IDENTIFICATION

Unusual Network Activity

- Check for file shares :

```
C:\> net view \\127.0.0.1
```

- List opened sessions on the machine:

```
C:\> net session
```

- Check for opened shares on other systems:

```
C:\> net use
```

- Check for suspicious Netbios connexions:

```
C:\> nbtstat –S
```

- Look for any suspicious network connections

```
C:\> netstat –na 5
```

- Use a sniffer (Wireshark, tcpdump etc.) and see if there are unusual attempts of connections to or from remote systems. Try browsing sensitive websites (banking website for example) and check if unusual network activity is triggered but do not authenticate.

Unusual Automated Tasks

- Look at the list of scheduled tasks for any unusual entry:

```
C:\> at
```

- Also check user's autostart directories:

```
C:\Documents and Settings\user\Start Menu\Programs\Startup
C:\WinNT\Profiles\user\Start Menu\Programs\Startup
```

Unusual Log Entries

- Check log files for unusual entries:

```
C:\> eventvwr.msc
```

- Check firewall log files for suspect activity. You can also use an up-to-date antivirus to identify malware on the system, but be aware that it could destroy evidence.

If nothing suspicious has been found, it doesn't necessarily mean that the system is not infected (a rootkit could have been installed). The system may be investigated further by making a bit-by-bit copy of the incriminated hard-drive and analysing the copy with tools such as X-Ways, FTK or Encase.

3 CONTAINMENT

Objective: Mitigate the attack's effects on the targeted environment.

Pull the network plug off physically, to prevent more infection on the network and to stop any actions being done from your computer (e.g. the malware could be sending spam, taking part in a DDoS attack or storing illegal files on the system).

Send the suspect binaries to your CERT, or request CERT's help if you are unsure about the malware's nature. The CERT should be able to isolate the malicious content and can send it to all AV companies, including your corporate contractors. (The best way is to create a zipped, password-encrypted file of the suspicious binary.)

4 REMEDIATION

Objective: Take actions to remove the threat and avoid future incidents.

Reboot from a live CD/USB or trusted network installation and backup all important data on an external storage support. If unsure, bring your hard-drive to your IT helpdesk and ask them to make a copy of the important content.

Remove the binaries and the related registry entries.

- Find the best practices to remove the malware. They can usually be found on AntiVirus companies' websites.
- Run an online antivirus scan.
- Launch a based live CD/USB containing disinfection tools (can be downloaded from AV websites), or a dedicated anti-virus live CD/USB.

5 RECOVERY

Objective: Restore the system to normal operations.

If possible reinstall the OS and applications and restore user's data from clean, trusted backups. If deemed necessary, you may ask your local IT helpdesk to reimage the disk.

In case the computer has not been reinstalled completely:

Restore files which could have been corrupted by the malware, especially system files.

Reboot the machine after all the suspicious files have been removed, and confirm that the workstation is not exhibiting any unusual behaviour. A full, up-to-date AV scan of the hard-drive and memory are recommended.

6 LESSONS LEARNT

Objective: Document the incident's details, discuss lessons learned, and adjust plans and defences.

Inform your hierarchy and subsidiaries about the incident, this could help to avoid similar attacks later.

Report
An incident report should be written and made available to all of the stakeholders.
The following themes should be described:

- Initial detection.
- Actions and timelines.
- What went right.
- What went wrong.
- Incident cost.

Capitalize
Actions to improve windows malware detection and eradication processes should be defined to capitalize on this experience.

Document created by ELYSUMSECURITY LTD – https://www.elysiumsecurity.com – Based on the Société Générale IRM 7 freely available on github

IRM #8

WINDOWS INTRUSION

Guidelines to handle unauthorised access to a Windows machine
Version 1.1

WINDOWS INTRUSION DEFINITION

"unauthorised access to the operating and/or file systems of electronic devices running on windows."
(ELYSIUMSECURITY & FORCEPOINT)

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue. It is aimed at:

- Administrators
- Security Teams and Operation Centre
- CISOs and deputies

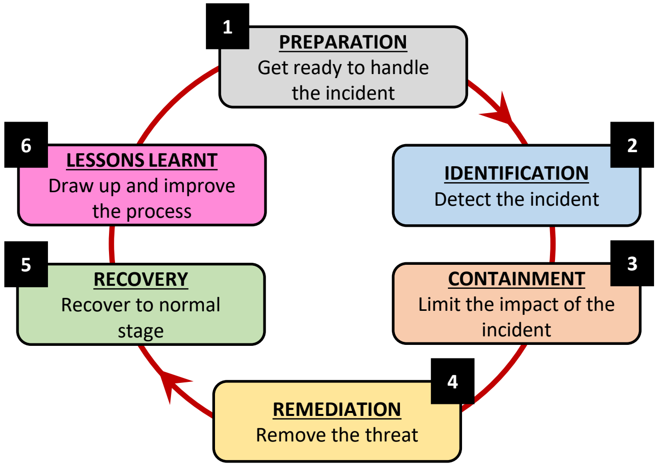
Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident.

Incident Response Team contact:

____

____

INCIDENT HANDLING CYCLE



1 PREPARATION

Objective: Establish contacts, define procedures, gather information to save time during an attack.

- A physical access to the suspicious system should be given to the forensic investigator. Physical access is preferred to remote access, since the hacker could detect the investigations done on the system (by using a network sniffer for example).
- A physical copy of the hard-disk might be necessary for forensic and evidence purposes. Finally, if needed, a physical access could be needed to disconnect the suspected machine from any network.
- A good knowledge of the usual network activity of the machine/server is needed. You should have a file on a secure place describing the usual port activity, to compare efficiently to the current state.
- A good knowledge of the usual services running on the machine can be very helpful. Don't hesitate to ask a Windows Expert for his assistance, when applicable. A good idea is also to have a map of all services/running process of the machine.

It can be a real advantage to work in a huge corporate environment, where all user machines are the same, installed from a master CD/USB/Image. Have a map of all processes/services/applications. On such environment where users are not allowed to install software, consider any additional process/service/application as suspicious.

The more you know the machine in its clean state, the more chances you have to detect any fraudulent activity running from it.

2 IDENTIFICATION

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

Please note that the **Sysinternals** Troubleshooting Utilities can be used to perform most of these tasks.

2 IDENTIFICATION

- **Unusual Accounts**

Look for unusual accounts created, especially in the Administrators group:
C:\> lusrmgr.msc
or
C:\> net localgroup administrators or *net localgroup administrateurs*

- **Unusual Files**

Look for unusually big files on the storage support, bigger than 5MB. (can be an indication of a system compromised for illegal content storage)
Look for unusual files added recently in system folders, especially C:\WINDOWS\system32.
Look for files using the "hidden" attribute:
C:\> dir /S /A:H

- **Unusual Registry Entries**

Look for unusual programs launched at boot time in the Windows registry, especially:
*HKLM\Software\Microsoft\Windows\CurrentVersion\Run**
Use "*HiJackThis*" if possible. (Also have a look in your Startup folder)

- **Unusual Processes and Services**

Check all running processes for unusual/unknown entries, especially processes with username "SYSTEM" and "ADMINISTRATOR":
C:\> taskmgr.exe
(or *tlisk*, *tasklist* depending on Windows release)

- **Check user's autostart folders**

C:\Documents and Settings\user\Start Menu\Programs\Startup
C:\WinNT\Profiles\user\Start Menu\Programs\Startup

- **Look for unusual/unexpected network services installed and started**

C:\> services.msc
C:\> net start

- **Unusual Network Activity**

Check for file shares and verify each one is linked to a normal activity:
C:\> net view \\127.0.0.1

Document created by ELYSUMSECURITY LTD – https://www.elysiumsecurity.com – Based on the Société Générale IRM 2 freely available on github

2 IDENTIFICATION

Look at the opened sessions on the machine:

```
C:\> net session
```

Have a look at the sessions the machine has opened with other systems:

```
C:\> net use
```

Check for any suspicious Netbios connexion:

```
C:\> nbtstat –S
```

Look for any suspicious activity on the system's ports :

```
C:\> netstat –na 5
```

- **Unusual Automated Tasks**

Look at the list of scheduled tasks for any unusual entry:

```
C:\> at
```

- **Unusual Log Entries**

Watch your log files for unusual entries:

```
C:\> eventvwr.msc
```

If possible, use "*Event Log Viewer*" or such tool

Search for events affecting the firewall, the antivirus, the file protection, or any suspicious new service.

Look for a huge amount of failed login attempts or locked out accounts.

Watch your firewall (if any) log files for suspect activity.

- **Rootkit check**

Run "*Rootkit Revealer*", "*Rootkit Hooker*", "*Ice Sword*", "*Rk Detector*", "*SysInspector*", "*Rootkit Buster*".

- **Malware check**

Run at least one anti-virus product on the whole disk. If possible use several anti-virus. The anti-virus must absolutely be up-to-date.

3 CONTAINMENT

Objective: Mitigate the attack's effects on the targeted environment.

If the machine is considered critical for your company's business activity and can't be disconnected, backup all important data in case the hacker notices you're investigating and starts deleting files. Also make a copy of the system's memory for further analysis. (use tools such as Memoryze,win32dd etc.)

3 CONTAINMENT

If the machine is not considered critical for your company and can be disconnected, shut the machine down the hard way, removing its power plug. If it is a laptop with a battery on, just push the "off" button for some seconds until the computer switches off.

Offline investigations should be started right away if the live analysis didn't give any result, but the system should still be considered compromised.

Make a physical copy (bit by bit) of the whole hard disk on an external storage support using forensic tools

Try to find evidences of every action of the hacker:

- **Find all files used by the attacker**, including deleted files (use your forensic tools) and see what has been done with it or at least their functionality, in order to evaluate the threat.
- **Check all files accessed recently.**
- **Check log files**
- Inspect network shares to see if the malware has spread through it.
- More generally, try to **find how the attacker got into the system**. All leads should be considered. If no computer proof of the intrusion is found, never forget it could come from a physical access or a complicity / stealing of information from an employee/insider.
- Apply fixes when applicable (operating system and applications), in case the attacker used a known fixed vulnerability.

4 REMEDIATION

Objective: Take actions to remove the threat and avoid future incidents.

In case the system has been compromised:

- Temporary remove all accesses to the accounts involved in the incident;
- Remove all malicious files installed by the attacker;

5 RECOVERY

Objective: Restore the system to normal operations.

No matter how far the hacker has gone into the system and the knowledge you might have about the compromise, as long as the system has been penetrated, the best practice is **to reinstall the system fully from original media and apply all fixes to the newly installed system.**

In case this solution can't be applied, you should:

- **Change all the system's accounts passwords**, and make your users do so in a secure way: they should use passwords with upper/lower case, special characters, numbers, and at least be 8 characters long.
- **Restore all files** that could have been changed (Example: *svchost.exe*) by the attacker.

6 LESSONS LEARNT

Objective: Document the incident's details, discuss lessons learned, and adjust plans and defences.

Inform your hierarchy and subsidiaries about the incident, this could help to avoid similar attacks later.

Report

An incident report should be written and made available to all of the stakeholders.

The following themes should be described:

- Initial detection.
- Actions and timelines.
- What went right.
- What went wrong.
- Incident cost.

Capitalize

Actions to improve windows intrusion detection management processes should be defined to capitalize on this experience.

IRM #9
UNIX INTRUSION

Guidelines to handle unauthorised access to a Unix based machine
Version 1.1

UNIX INTRUSION DEFINITION

“unauthorised access to the operating and/or file systems of electronic devices running on a Unix based system.”
(ELYSIUMSECURITY & FORCEPOINT)

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue. It is aimed at:

- Administrators
- Security Teams and Operation Centre
- CISOs and deputies

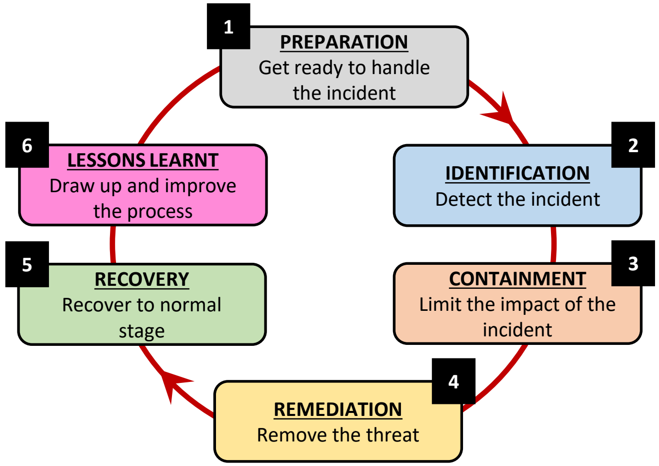
Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line’s Incident.

Incident Response Team contact:

____

____

INCIDENT HANDLING CYCLE



1 **PREPARATION**
Get ready to handle the incident

2 **IDENTIFICATION**
Detect the incident

3 **CONTAINMENT**
Limit the impact of the incident

4 **REMEDIATION**
Remove the threat

5 **RECOVERY**
Recover to normal stage

6 **LESSONS LEARNT**
Draw up and improve the process

1 PREPARATION

Objective: Establish contacts, define procedures, gather information to save time during an attack.

- A physical access to the suspicious system should be offered to the forensic investigator.
- A physical copy of the hard-disk might be necessary for forensic and evidence purposes. If needed, a physical access could be necessary to disconnect the suspected machine from any network.
- A good knowledge of the usual network activity of the machine/server is needed. You should have a file on a secure place describing the usual port activity, to compare efficiently to the current state.
- A good knowledge of the usual services is needed. Don’t hesitate to ask a Unix/Linux Expert for his assistance, when applicable.
- You should have a regularly updated list of all critical files, (especially SUID and GUID files) stored in a secure place out of the network or even on paper. With this list, you can easily separate usual SUID files and detect unusual ones.
- Have a map of your usual port activity/traffic rules.

2 IDENTIFICATION

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

Unusual Accounts

Look for any suspicious entry in /etc/passwd, especially with UID 0. Also check /etc/group and /etc/shadow.
Look for orphaned files, which could have been left by a deleted account used in the attack:

```
# find / \( -nouser –o –nogroup \) -print
```

Unusual Files

- Look for all SUID and GUID files:

```
# find / -uid 0 \( –perm -4000 –o –perm 2000 \) –print
```

- Look for weird file names, starting with “. “, “.. “, “ “

```
# find / -name “ *“ –print
# find / -name “. *“ –print
# find / -name “.. *“ –print
```

2 IDENTIFICATION

- Look for large files (here: larger than 10MB)

```
# find / -size +10MB –print
```

- Look for processes running from or to files which have been unlinked :

```
 # lsof +L1
```

- Look for unusual files in /proc and /tmp. This last directory is a place of choice for hackers to store data or malicious binaries.

Unusual Services

- Run chkconfig to check for all enabled services:

```
# chkconfig --list
```

- Look at the running processes (remember: a rootkit might change your results).

```
# ps -aux
```

- Use *lsof –p [pid]* on unknown processes

You should know your usual running processes to figure out which processes could have been added by a hacker. Especially check processes running under UID 0.

Unusual Network Activity

Try to detect sniffers on the network: Look at your kernel log files for interfaces entering promiscuous mode such as :“*kernel: device eth0 entered promiscuous mode*”
Use # *ip link* to detect the “PROMISC” flag.

- Look for unusual port activity: # *netstat –nap* and # *lsof –i* to get more information about processes listening to ports.
- Look for unusual MAC entries in your LAN:

```
# arp -a
```

- Look for any unexpected IP address on the network.

Unusual Automated Tasks

- Look for unusual jobs scheduled by users mentioned in /etc/cron.allow. Pay a special attention to the cron jobs scheduled by UID 0 accounts (root):

```
# crontab –u root -l
```

- Look for unusual system-wide cron jobs:

# cat /etc/crontab and # *ls –la /etc/cron.**

2 IDENTIFICATION

Unusual Log Entries
Look through the log files on the system for suspicious events, including the following:

- Huge number of authentication/login failures from local or remote access tools (sshd,ftpd,etc.);
- Remote Procedure Call (RPC) programs with a log entry including large number of strange characters;
- A huge number of Apache logs mentioning “error”;
- Reboots (Hardware reboot);
- Restart of applications (Software reboot);
- Almost all log files are located under /var/log directory;

Unusual Kernel log Entries

- Look through the kernel log files on the system for suspicious events. Use : # dmesg
- List all important kernel and system information with # lsmod or # lspci
- Look for known rootkit (use rkhunter and such tools)

File hashes
Verify all MD5 hashes of your binaries in /bin, /sbin, /usr/bin, /usr/sbin or any other related binary storing place. (use AIDE or such tool)

WARNING: this operation may change all file timestamps. This should only be done after all other investigations are done and you feel like you can alter these data.

3 CONTAINMENT

Objective: Mitigate the attack’s effects on the targeted environment.

If the machine is considered critical for your company’s business activity and can’t be disconnected, backup all important data in case the hacker notices you’re investigating and starts deleting files. Also make a copy of the system’s memory for further analysis. (use tools such as Memoryze,win32dd etc.)

3 CONTAINMENT

If the machine is not considered critical for your company and can be disconnected, shut the machine down the hard way, removing its power plug. If it is a laptop with a battery on, just push the “off” button for some seconds until the computer switches off.

Offline investigations should be started right away if the live analysis didn’t give any result, but the system should still be considered compromised.

Make a physical copy (bit by bit) of the whole hard disk on an external storage support using forensic tools

Try to find evidences of every action of the hacker:

- **Find all files used by the attacker**, including deleted files (use your forensic tools) and see what has been done with it or at least their functionality, in order to evaluate the threat.
- **Check all files accessed recently.**
- **Check log files**
- Inspect network shares to see if the malware has spread through it.
- More generally, try to **find how the attacker got into the system**. All leads should be considered. If no computer proof of the intrusion is found, never forget it could come from a physical access or a complicity / stealing of information from an employee/insider.
- Apply fixes when applicable (operating system and applications), in case the attacker used a known fixed vulnerability.

4 REMEDIATION

Objective: Take actions to remove the threat and avoid future incidents.

In case the system has been compromised:

- Temporary remove all accesses to the accounts involved in the incident;
- Remove all malicious files installed by the attacker;

5 RECOVERY

Objective: Restore the system to normal operations.

No matter how far the hacker has gone into the system and the knowledge you might have about the compromise, as long as the system has been penetrated, the best practice is **to reinstall the system completely and apply all security fixes**.

In case this solution can’t be applied, you should:

- Change all the system’s accounts passwords, and make your users do so in a secure way: they should use passwords with upper/lower case, special characters, numbers, and at least be 7 characters long.
- Check the integrity of the whole data stored on the system, using MD5 hashes.
- Restore all binaries which could have been changed (Example: /bin/su)

6 LESSONS LEARNT

Objective: Document the incident’s details, discuss lessons learned, and adjust plans and defences.

Inform your hierarchy and subsidiaries about the incident, this could help to avoid similar attacks later.

Report
An incident report should be written and made available to all of the stakeholders.
The following themes should be described:

- Initial detection.
- Actions and timelines.
- What went right.
- What went wrong.
- Incident cost.

Capitalize
Actions to improve Unix/Linux intrusion detection management processes should be defined to capitalize on this experience.

IRM #10

RANSOMWARE

Guidelines to handle and respond to ransomware infection
Version 1.2

RANSOMWARE DEFINITION

"a type of malicious software designed to block access to a computer system until a sum of money is paid."
(OXFORD LANGUAGES)

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue. It is aimed at:

- Administrators
- Security Teams and Operation Centre
- CISOs and deputies

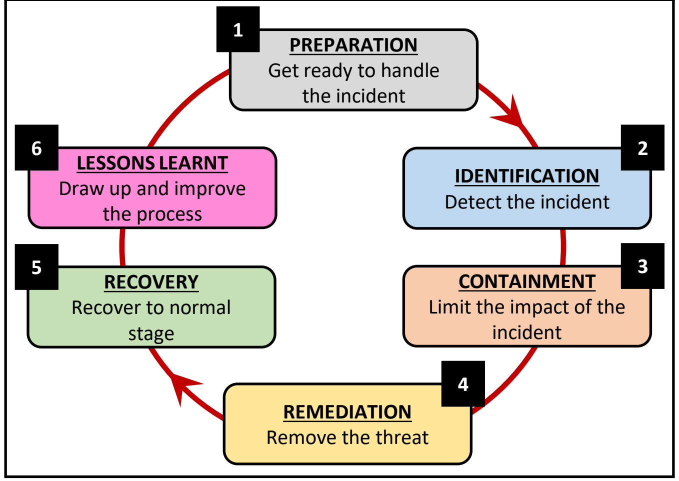
Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident.

Incident Response Team contact:

____

____

INCIDENT HANDLING CYCLE



1 **PREPARATION** Get ready to handle the incident

2 **IDENTIFICATION** Detect the incident

3 **CONTAINMENT** Limit the impact of the incident

4 **REMEDIATION** Remove the threat

5 **RECOVERY** Recover to normal stage

6 **LESSONS LEARNT** Draw up and improve the process

1 PREPARATION

Objective: Establish contacts, define procedures, gather information to save time during an attack.

- A good knowledge of the usual operating systems security policies is needed.
- A good knowledge of the usual users' profile policies is needed.
- Ensure that the endpoint and perimetric (email gateway, proxy caches) security products are up to date and their logs are enabled
- Since this threat is often detected by end-users, raise your IT support awareness regarding the ransomware threat
- **Make sure to have exhaustive, recent and reliable backups of local and network users' data;**

2 IDENTIFICATION

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

General signs of ransomware presence

Several leads might hint that the system could be compromised by ransomware:

- Odd professional emails (often masquerading as invoices) containing attachments are being received
- A ransom message explaining that the documents have been encrypted and asking for money is displayed on user's desktop
- People are complaining about their files not being available or corrupted on their computers or their network shares with unusual extensions (.abc, .xyz, .aaa, etc..)
- Numerous files are being modified in a very short period of time on the network shares
- Systems and/or applications become unavailable

2 IDENTIFICATION

Host based identification

- Look for the aforementioned extensions or ransom notes;
- Capture a memory image of the computer (if possible)
- Look for unusual executable binaries in users' profiles (%ALLUSERSPROFILE% or %APPDATA%) and %SystemDrive%
- Look for unusual program in the registry that automatically starts
- Look for unusual services running and that are set to start automatically
- Look for unusual processes
- Look for unusual email attachment patterns
- Look for unusual network or web browsing activities; especially connections to Tor or I2P IP, Tor gateways (tor2web, etc) or Bitcoin payment websites

Network based identification

- Look for unusual VPN activities (odd hours, infrequent countries of origin, etc)
- Look for unusual network or web browsing activities especially connections to Tor or I2P IP, Tor gateways (tor2web, etc) or Bitcoin payment websites
- Look for connection patterns to Exploit Kits
- Look for connection patterns to ransomware C&C
- Look for unusual email attachment patterns

3 CONTAINMENT

Objective: Mitigate the attack's effects on the targeted environment.

- Disconnect all computers that have been detected as compromised from the network
- If you cannot isolate the computer, disconnect/cancel the shared drives (NET USE x: \\unc\path\ /DELETE)
- Block traffic to identified ransomware's C&C
- Send the undetected samples to your endpoint security provider and if within your company policy to Virustotal (this may expose sensitive data)
- Send the uncategorized malicious URL, domain names and IP to your perimetric security provider and research them online (but do not go on those URLs)
- **Do not reboot an infected system unless you have no choice;**
- **Do not switch off an infected system unless you have no choice;**

4 REMEDIATION

Objective: Take actions to remove the threat and avoid future incidents.

- Remove the binaries and the related registry entries (if any) from compromised profiles (%ALLUSERSPROFILE% or %APPDATA%) and %SystemDrive%
- Remove the services related to the ransomware
- If your current anti virus did not detect the malware/ransomware, try running a different one from a USB stick (i.e.: EMISOFT Emergency kit – portable version)
- If the above step is not possible reimage the computer with a clean install

5 RECOVERY

Objective: Come back to the previous functional state.

1. Update antivirus signatures for identified malicious binaries to be blocked
2. Ensure that no malicious binaries are present on the systems before reconnecting them
3. Ensure that the network traffic is back to normal
4. Restore user's documents from backups
5. Ensure the backups used are from before the incident first happened

All of these steps shall be made in a step-by-step manner and with technical monitoring.

6 LESSONS LEARNT

Objective: Document the incident's details, discuss lessons learned, and adjust plans and defences.

Inform your hierarchy and subsidiaries about the incident, this could help to avoid similar attacks later.

Report
An incident report should be written and made available to all of the stakeholders.
The following themes should be described:

- Initial detection.
- Actions and timelines.
- What went right.
- What went wrong.
- Incident cost.

Capitalize
Actions to improve malware and network intrusion detection processes should be defined to capitalize on this experience.

IRM #11
DDOS

Guidelines to handle Distributed Denial of Service incidents
Version 1.1

DDOS DEFINITION

"A Distributed Denial Of Service that makes the targeted services unavailable for its legitimate users by flooding the network with illegitimate traffic."
(IGI GLOBAL)

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue. It is aimed at:

- Administrators
- Security Teams and Operation Centre
- CISOs and deputies

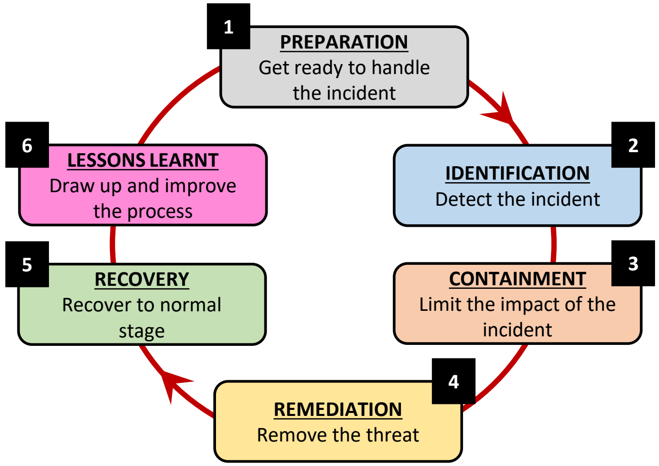
Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident.

Incident Response Team contact:

____

____

INCIDENT HANDLING CYCLE



1 **PREPARATION** Get ready to handle the incident

2 **IDENTIFICATION** Detect the incident

3 **CONTAINMENT** Limit the impact of the incident

4 **REMEDIATION** Remove the threat

5 **RECOVERY** Recover to normal stage

6 **LESSONS LEARNT** Draw up and improve the process

1 PREPARATION

Objective: Establish contacts, define procedures, gather information to save time during an attack.

Internet Service Provider support

- Contact your ISP to understand the DDoS mitigation services it offers (free and paid) and what process you should follow.
- If possible, subscribe to a redundant Internet connection.
- If possible, subscribe to an Anti-DDoS service provider.
- Establish contacts with your ISP and law enforcement entities. Make sure that you have the possibility to use an out-of-band communication channel (e.g.: phone).

Inventory

- Create a whitelist of the IP addresses and protocols you must allow if prioritizing traffic during an attack. Don't forget to include your critical customers, key partners, etc.
- Document your IT infrastructure details, including business owners, IP addresses and circuit IDs, routing settings (AS, etc); prepare a network topology diagram and an asset inventory.

Network infrastructure

- Design a good network infrastructure without Single Point of Failure or bottleneck.
- Distribute your DNS servers and other critical services (SMTP, etc) through different AS.
- Harden the configuration of network, OS, and application components that may be targeted by DDoS.
- Baseline your current infrastructure's performance, so you can identify the attack faster and more accurately.
- If your business is Internet dependent, consider purchasing specialized DDoS mitigation products or services.

1 PREPARATION

- Confirm DNS time-to-live (TTL) settings for the systems that might be attacked. Lower the TTLs, if necessary, to facilitate DNS redirection if the original IP addresses get attacked. 600 is a good TTL value.
- Depending of the criticality of your services, consider setting-up a backup that you can switch on in case of issue.

Internal contacts

- Establish contacts for your IDS, firewall, systems, and network teams.
- Collaborate with the business lines to understand business implications (e.g., money loss) of likely DDoS attack scenarios.
- Involve your BCP/DR planning team on DDoS incidents.

The "preparation" phase is the most important element of a successful DDoS incident response.

2 IDENTIFICATION

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

Analyse the attack

- Understand the logical flow of the DDoS attack and identify the infrastructure components affected by it.
- Understand if you are the target of the attack or a collateral victim
- Review the load and log files of servers, routers, firewalls, applications, and other affected infrastructure.
- Identify what aspects of the DDoS traffic differentiate it from benign traffic
    - ○ Source IP addresses, AS, etc
    - ○ Destination ports
    - ○ URLs
    - ○ Protocols flags

Network analysis tools can be used to review the traffic: **Tcpdump**, **Tshark**, **Snort**, **Argus**, **Ntop**, **Aguri**, **MRTG, etc.**

2 IDENTIFICATION

- If possible, create a NIDS signature to focus to differentiate between benign and malicious traffic.

Involve internal and external actors

- Contact your internal teams to learn about their visibility into the attack.
- Contact your ISP to ask for help. Be specific about the traffic you'd like to control:
  - Network blocks involved
  - Source IP addresses
  - Protocols
- Notify your company's executive and legal teams.

Check the background

- Find out whether the company received an extortion demand as a precursor to the attack.
- Search if anyone would have any interest into threatening your company:
  - Competitors
  - Ideologically-motivated groups (hacktivists)
  - Former employees

3 CONTAINMENT

Objective: Mitigate the attack's effects on the targeted environment.

- If the bottleneck is a particular feature of an application, temporarily disable that feature.
- Attempt to throttle or block DDoS traffic as close to the network's "cloud" as possible via a router, firewall, load balancer, specialized device, etc.
- Terminate unwanted connections or processes on servers and routers and tune their TCP/IP settings.
- If possible, switch to alternate sites or networks using DNS or another mechanism. Blackhole DDoS traffic targeting the original IP addresses.

3 CONTAINMENT

- Set up an alternate communication channel between you and your users/customers (e.g.: web server, mail server, voice server, etc.)
- If possible, route traffic through a traffic-scrubbing service or product via DNS or routing changes (e.g.: sinkhole routing)
- Configure egress filters to block the traffic your systems may send in response to DDoS traffic (e.g.: backsquatter traffic), to avoid adding unnecessary packets to the network.
- In case of an extortion attempt, try to buy time with the fraudster. For example, explain that you need more time in order to get management approval.

If the bottleneck is at the ISP's side, only the ISP can take efficient actions. In that case, work closely with your ISP and make sure you share information efficiently.

4 REMEDIATION

Objective: Take actions to remove the threat and avoid future incidents.

- Contact your ISP and make sure that it enforces remediation measures. For information, here are some of the possible measures:
  - Filtering (if possible at level Tier1 or 2)
  - Traffic-scrubbing/Sinkhole/Clean-pipe
  - Blackhole Routing
- If the DDoS sponsors have been identified, consider involving law enforcement. *This should be performed upon the direction of your company's executive and legal teams.*

Technical remediation actions can mostly be enforced by your ISP.

5 RECOVERY

Objective: Restore the system to normal operations.

Assess the end of the DDoS condition

- Ensure that the impacted services are reachable again.
- Ensure that your infrastructure performance is back to your baseline performance.

Rollback the mitigation measures

- Switch back traffic to your original network.
- Restart stopped services.

Ensure that the recovery-related actions are decided in accordance with the network teams. Bringing up services could have unexpected side effects.

6 LESSONS LEARNT

Objective: Document the incident's details, discuss lessons learned, and adjust plans and defences.

Inform your hierarchy and subsidiaries about the incident, this could help to avoid similar attacks later.

Report

An incident report should be written and made available to all of the stakeholders.

The following themes should be described:

- Initial detection.
- Actions and timelines.
- What went right.
- What went wrong.
- Incident cost.

Capitalize

Actions to improve DDOS handling processes should be defined to capitalize on this experience.

IRM #12
NETWORK ATTACK

Guidelines to handle suspicious network activity
Version 1.1

NETWORK ATTACK DEFINITION

"an attempt to gain unauthorized access to an organization's network, with the objective of stealing data or perform other malicious activity."
(CYNET)

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue. It is aimed at:

- Administrators
- Security Teams and Operation Centre
- CISOs and deputies

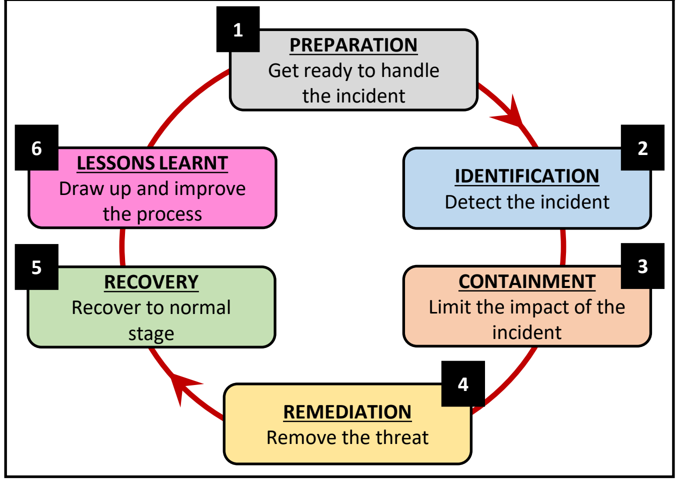
Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident.

Incident Response Team contact:

____

____

INCIDENT HANDLING CYCLE



1 PREPARATION

Objective: Establish contacts, define procedures, gather information to save time during an attack.

Intrusion Detection Systems

- Ensure that the monitoring tools are up to date;
- Establish contacts with your network and security operation teams;
- Make sure that an alert notification process is defined and well-known from everyone.

Network

- Make sure that an inventory of the network access points is available and up-to-date;
- Make sure that network teams have up to date network maps and configurations;
- Look for potential unwanted network access points (xDSL, Wifi, Modem, …) regularly and close them;
- Ensure that traffic management tools and processes are operational.

Baseline traffic

- Identify the baseline traffic and flows;
- Identify the business-critical flows.

2 IDENTIFICATION

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

Sources of detection:

- Notification by user/helpdesk;
- IDS alert;
- Detection by network staff;
- Complain from an external source.

Record suspect network activity

Network frames can be stored into a file and transmitted to your incident response team for further analysis.
Use network capture tools (tshark, windump, tcpdump…) to dump malicious traffic. Use a hub or port mirroring on an affected LAN to collect valuable data.

Network forensic requires skills and knowledge . Ask your incident response team for assistance or advices.
Analyse the attack

- Analyze alerts generated by your IDS;
- Review statistics and logs of network devices;
- Try to understand the goal of the malicious traffic and identify the infrastructure components affected by it;
- Identify the technical characteristics of the traffic:

Source IP address(es)

  - Ports used, TTL, Packet ID, …
  - Protocols used
  - Targeted machines/services
  - Exploit(s)
  - Remote accounts logged in

At the end of this step, the impacted machines and the modus operandi of the attack should have been identified. Ideally, the source of the attack should have been identified as well. This is where you should do your forensic investigations, if needed.

If a compromised computer has been identified, check IRM cheat sheets dedicated to intrusion.

Document created by ELYSUMSECURITY LTD – https://www.elysiumsecurity.com – Based on the Société Générale IRM 5 freely available on github

3 CONTAINMENT

Objective: Mitigate the attack's effects on the targeted environment.

If the issue is considered as strategic (sensitive resources access), a specific crisis management cell should be activated.

Depending on the criticality of the impacted resources, the following steps can be performed and monitored:

- Disconnect the compromised area from the network
- Isolate the source of the attack. Disconnect the affected computer(s) in order to perform further investigation;
- Find acceptable mitigation measures for the business-critical traffic in agreement with the business line managers;
- Terminate unwanted connections or processes on affected machines;
- Use firewall/IPS rules to block the attack;
- Use IDS rules to match with this malicious behaviour and inform technical staff on new events;
- Apply ad hoc actions in case of strategic issue:
    - Block exfiltration destination or remote location on Internet filters ;
    - Restrict strategic file servers to reject connections from the compromised computer;
    - Select what kind of files can be lost / stolen and restrict the access for confidential files;
    - Create fake documents with watermarking that could be use as a proof of theft;
    - Notify targeted business users about what must be done and what is forbidden;
    - Configure logging capabilities in verbose mode on targeted environment and store them in a remote secure server.

4 REMEDIATION

Objective: Take actions to remove the threat and avoid future incidents.

Block the source

- Using analysis from previous steps identification and containment, find out all communication channels used by the attacker and block them on all your network boundaries;
- If the source has been identified as an insider, take appropriate actions and involve your management and/or HR team and/or legal team;
- If the source has been identified as an external offender, consider involving abuse teams and law enforcement services if required;

Technical remediation

- Define a remediation process. If necessary, this process can be validated by another structure, like your incident response team for example;
- Remediation steps from intrusion IRM can also be useful;

Test and enforce

- Test the remediation process and make sure that it properly works without damaging any service;
- Enforce the remediation process once tests have been approved by both IT and business;

5 RECOVERY

Objective: Restore the system to normal operations.

1. Ensure that the network traffic is back to normal
2. Re-allow the network traffic that was used as a propagation method by the attacker
3. Reconnect sub-areas together if necessary
4. Reconnect the area to your local network if necessary
5. Reconnect the area to the Internet if necessary

All of these steps shall be made in a step-by-step manner and with a technical monitoring.

6 LESSONS LEARNT

Objective: Document the incident's details, discuss lessons learned, and adjust plans and defences.

Inform your hierarchy and subsidiaries about the incident, this could help to avoid similar attacks later.

Report

An incident report should be written and made available to all of the stakeholders.
The following themes should be described:

- Initial detection.
- Actions and timelines.
- What went right.
- What went wrong.
- Incident cost.

Capitalize

Actions to improve the network intrusion management processes should be defined to capitalize on this experience.

IRM #13
WEBSITE DEFACEMENT

Guidelines to handle a compromised webserver
Version 1.1

WEBSITE DEFACEMENT DEFINITION

"an unauthorised change to the visual appearance of a website or a web page."
(ELYSIUMSECURITY)

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue. It is aimed at:

- Administrators
- Security Teams and Operation Centre
- CISOs and deputies

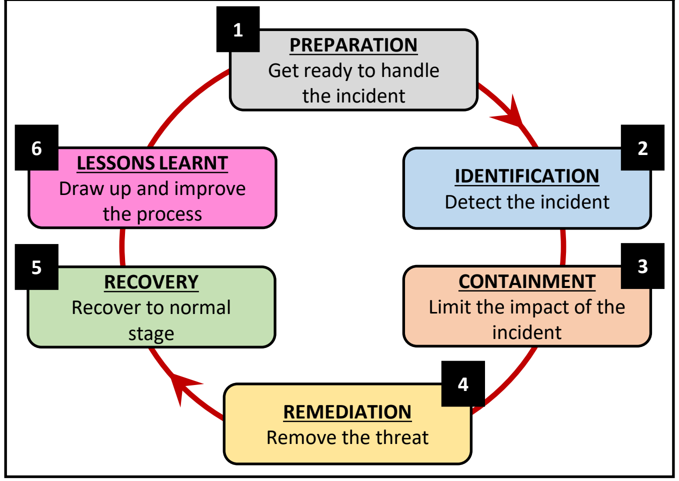
Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident.

Incident Response Team contact:

____

____

INCIDENT HANDLING CYCLE



1 **PREPARATION** Get ready to handle the incident

2 **IDENTIFICATION** Detect the incident

3 **CONTAINMENT** Limit the impact of the incident

4 **REMEDIATION** Remove the threat

5 **RECOVERY** Recover to normal stage

6 **LESSONS LEARNT** Draw up and improve the process

1 PREPARATION

Objective: Establish contacts, define procedures, gather information to save time during an attack.

- Have up-to-date schemes describing your applicative components related to the web server;
- Build a backup website up and ready, on which you can publish content;
- Define a procedure to redirect every visitor to this backup website;
- Deploy monitoring tools to quickly detect any abnormal behaviour on your critical websites;
- Export the web server's log files to an external server. Make sure clocks are synchronized between each server;
- Reference external contents (static or dynamic) and create a list for each of them. Don't forget third parties for advertisement;
- Reference contact points of your hosting provider;
- Be sure your hosting provider enforces policies to log all events;
- Make sure you have an up-to-date network map.

2 IDENTIFICATION

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

Usual channels of detection are:

- **Webpage monitoring:** The content of a web page has been altered. The new content is either very discreet (an "iframe" injection for example) or obvious (*"You have been 0wn3d by xxx"*);
- **User:** users call or notification from employees about problems they noticed while browsing the website;
- Security checks with tools such as Google SafeBrowsing;

Verify the defacement and detect its origin:

- Check files with static content (in particular, check the modification dates, hash signature);
- Check webpage's data content providers (mashup);
- Check link presents in the web page (src, meta, css, script, etc.);
- Check log files;
- Scan the databases for malicious content;

The source code of the suspicious page must be analysed carefully to identify the problem clearly. In particular, **be sure the problem is on a web server belonging to the company** and not on a web content located outside your infrastructure, like commercial banners from a third party.

Document created by ELYSUMSECURITY LTD – https://www.elysiumsecurity.com – Based on the Société Générale IRM 6 freely available on github

3 CONTAINMENT

Objective: Mitigate the attack's effects on the targeted environment.

- **Backup all data** stored on the web server for forensic purposes and evidence collecting. If possible: make a complete bit-by-bit copy of the hard-disk containing the web server. This will help recover deleted files;
- **Check your network architecture map. Verify that the vulnerability exploited by the attacker is not located somewhere else :**
  - Check the system on which the web server is running;
  - Check other services running on that machine;
  - Check the connections to other systems, which might be compromised;

If the source of the attack is another system on the network, disconnect it if possible physically and investigate on it.

Try to find evidences of every action of the attacker:

- **Find out how the attacker got into the system in the first place and fix it :**
  - Web component vulnerability allowing write access: fix the vulnerability by applying editor's fix;
  - Open public folder: fix the bug;
  - SQL weakness allowing injection: correct the code;
  - Mashup components: cut mashup feed;
  - Administrative modification by physical access: modify the access rights;
- **If required, deploy a temporary web server**, up to date with its applications. It should offer the same content than the compromised web server or at least show another legitimate content such as "Temporary unavailable". The best is to display a temporary static content, containing only HTML code. This prevents another infection in case the attacker has used vulnerability in the legitimate PHP/ASP/CGI/PL/etc. code.

4 REMEDIATION

Objective: Take actions to remove the threat and avoid future incidents.

Remove all altered content and replace it with the legitimate content, restored from earlier backup. Make sure this content is free from vulnerabilities.

5 RECOVERY

Objective: Restore the system to normal operations.

- **Change all user passwords**, if the web server provides user-authentication, and you have evidence/reasons to think the passwords may have been compromised. This can require a large user communication;

- **If backup server has been used, restore the primary web server component as nominal;**

6 LESSONS LEARNT

Objective: Document the incident's details, discuss lessons learned, and adjust plans and defences.

Inform your hierarchy and subsidiaries about the incident, this could help to avoid similar attacks later.

Communication

If the defacement has been visible for part of your users, plan to explain the incident publicly.

Report

An incident report should be written and made available to all of the stakeholders.

The following themes should be described:

- Initial detection.
- Actions and timelines.
- What went right.
- What went wrong.
- Incident cost.

In case of vulnerability discovery, **report any undocumented vulnerability** lying on a product running on the web server (like a PHP forum) to its editor, so that the code can be upgraded in order to release a fix.

Capitalize

Actions to improve the web defacement processes should be defined to capitalize on this experience.

IRM #14
WORM INFECTION

Guidelines to handle a system's work infection
Version 1.1

WORM INFECTION DEFINITION

"a standalone malware computer program that replicates itself in order to spread to other computers."
(WIKIPEDIA)

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue. It is aimed at:

- Administrators
- Security Teams and Operation Centre
- CISOs and deputies

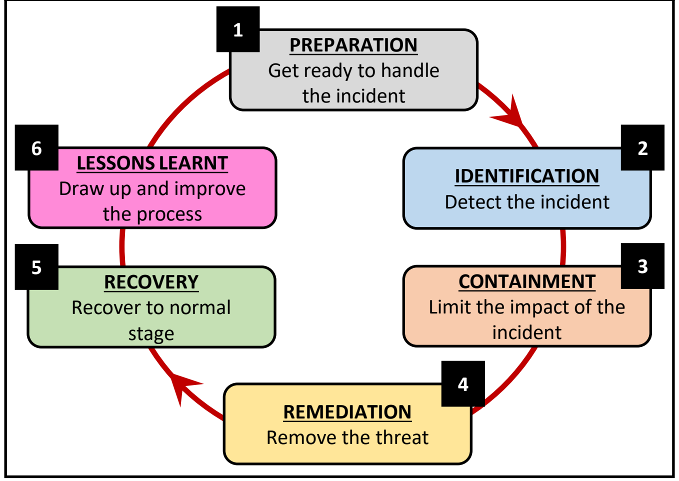
Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident.

Incident Response Team contact:

____

____

INCIDENT HANDLING CYCLE



1 PREPARATION

Objective: Establish contacts, define procedures, gather information to save time during an attack.

- Define actors, for each entity, who will be involved into the crisis cell. These actors should be documented in a contact list kept permanently up to date;
- Make sure that analysis tools are up, functional (Antivirus, IDS, logs analysers), not compromised, and up to date;
- Make sure to have architecture map of your networks;
- Make sure that an up to date inventory of the assets is available;
- Perform a continuous security watch and inform the people in charge of security about the threat trends;

2 IDENTIFICATION

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

Detect the infection

Information coming from several sources should be gathered and analysed:

- Antivirus logs;
- Intrusion Detection Systems;
- Suspicious connection attempts on servers;
- High amount of accounts locked;
- Suspicious network traffic;
- Suspicious connection attempts in firewalls;
- High increase of support calls;
- High load or system freeze;
- High volumes of e-mail sent;

If one or several of these symptoms have been spotted, the actors defined in the "preparation" step will get in touch and if necessary, create a crisis cell.

Identify the infection

Analyse the symptoms to identify the worm, its propagation vectors and countermeasures.
Leads can be found from :

- CERT's bulletins;
- External support contacts (antivirus companies, etc.);
- Security websites (Secunia, SecurityFocus etc.);

Notify Chief Information Security Officer.
Contact your CERT if required.

Assess the perimeter of the infection

Define the boundaries of the infection (i.e.: global infection, bounded to a subsidiary, etc.).
If possible, identify the business impact of the infection.

3 CONTAINMENT

Objective: Mitigate the attack's effects on the targeted environment.

The following actions should be performed and monitored by the crisis management cell:

1. Disconnect the infected area from the Internet;

2. Isolate the infected area. Disconnect it from any network;

3. If business-critical traffic cannot be disconnected, allow it after ensuring that it cannot be an infection vector or find validated circumventions techniques;

4. Neutralize the propagation vectors. A propagation vector can be anything from network traffic to software flaw. Relevant countermeasures have to be applied (patch, traffic blocking, disable devices, etc.) For example, the following techniques can be used:
   - Patch deployment tools (WSUS);
   - Windows GPO;
   - Firewall rules;
   - Operational procedures;

5. Repeat steps 2 to 4 on each sub-area of the infected area until the worm stops spreading. If possible, monitor the infection using analysis tools (antivirus console, server logs, support calls);

The spreading of the worm must be monitored.

Mobile devices

Make sure that no laptop, tablet, phone or mobile storage can be used as a propagation vector by the worm.
If possible, block all their connections.
Ask end-users to follow directives precisely.
At the end of this step, the infection should be contained.

4 REMEDIATION

Objective: Take actions to remove the threat and avoid future incidents.

Identify
Identify tools and remediation methods.
The following resources should be considered:
- Vendor fixes (Microsoft, Oracle, etc.);
- Antivirus signature database;
- External support contacts;
- Security websites;

Define a disinfection process. The process has to be validated by an external structure, like your CERT for example.

Test
Test the disinfection process and make sure that it properly works without damaging any service.

Deploy
Deploy the disinfection tools. Several options can be used:
- Windows WSUS;
- GPO;
- Antivirus signature deployment;
- Manual disinfection;

Warning: some worms can block some of the remediation deployment methods. If so, a workaround has to be found.

Remediation progress should be monitored by the crisis cell.

5 RECOVERY

Objective: Restore the system to normal operations.

Verify all previous steps have been done correctly and get a management approval before following next steps.

1. Reopen the network traffic that was used as a propagation method by the worm;
2. Reconnect sub-areas together;
3. Reconnect the mobile laptops to the area;
4. Reconnect the area to your local network;
5. Reconnect the area to the Internet;

All of these steps shall be made in a step-by-step manner and a technical monitoring shall be enforced by the crisis team.

6 LESSONS LEARNT

Objective: Document the incident's details, discuss lessons learned, and adjust plans and defences.

Inform your hierarchy and subsidiaries about the incident, this could help to avoid similar attacks later.

Report
An incident report should be written and made available to all of the stakeholders.
The following themes should be described:
- Initial detection.
- Actions and timelines.
- What went right.
- What went wrong.
- Incident cost.

Capitalize
Actions to improve the worm infection management processes should be defined to capitalize on this experience.

IRM #15

CYBER BLACKMAIL

Guidelines to handle a cyber blackmail attempt
Version 1.1

CYBER BLACKMAIL DEFINITION

"also referenced as CYBEREXTORTION - an act of coercion using the threat of revealing or publicizing either substantially true or false information about a person or people unless certain demands are met."
(WIKIPEDIA)

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue. It is aimed at:

- Administrators
- Security Teams and Operation Centre
- CISOs and deputies

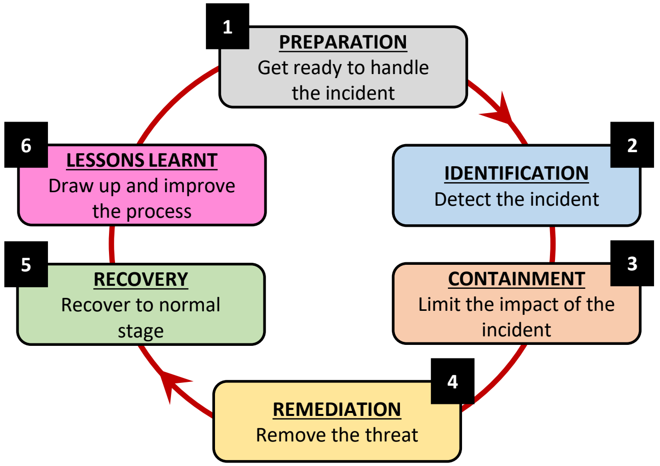
Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident.

Incident Response Team contact:

____

____

INCIDENT HANDLING CYCLE



1 **PREPARATION** Get ready to handle the incident

2 **IDENTIFICATION** Detect the incident

3 **CONTAINMENT** Limit the impact of the incident

4 **REMEDIATION** Remove the threat

5 **RECOVERY** Recover to normal stage

6 **LESSONS LEARNT** Draw up and improve the process

1 PREPARATION

Objective: Establish contacts, define procedures, gather information to save time during an attack.

Contacts

- Identify internal contacts (security team, incident response team, legal department etc.);
- Identify external contacts who might be needed, mainly for investigation purposes like Law Enforcement;
- Make sure that security incident escalation process is defined and the actors are clearly defined;
- Be sure to have intelligence gathering capabilities (communities, contact, etc.) that might be involved in such incidents;

Awareness

- Make sure that all the relevant employees are aware of blackmail issues. This can be part of the security awareness program.

Verify backup and incident response process is in place and up to date.

2 IDENTIFICATION

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

- Alert relevant people;
- Keep traces of any communications related to the incident (don't send emails to trash; write down any phone contact with phone number and timestamp if available, fax, etc.);
- Try to get as much details as you can about the author (name, fax, postal address, etc.);
- Examine possible courses of actions with your incident response team and legal team;
- If internal data is concerned, check you have a safe backup of it and try to find out how it was gathered;
- Include top management to inform them that blackmail is happening and is being handled according to a defined process;

Document created by ELYSUMSECURITY LTD – https://www.elysiumsecurity.com – Based on the Société Générale IRM 6 freely available on github

3 CONTAINMENT

Objective: Mitigate the attack's effects on the targeted environment.

Determine how you can answer to the blackmail and the consequences and costs of ignoring, answering yes or no.

Most common threats tied with blackmail are:

- Denial of service;
- Reveal sensitive data on Internet (credit card or other personal data from customers or internal worker/director, confidential company data, etc.);
- Reveal sensitive private information about employees/VIPs;
- Block your data access (wiped or encrypted through ransomware for example);
- Mass-mailing using the brand (spam, child pornography, bad rumours, etc.);

Check the background

- Check if similar blackmailing attempts have taken place in the past. Check if other companies have been threatened as well;
- All related technical data should be checked carefully and collected for investigation purposes;
- Search if anyone would have any interest into threatening your company:
  - Competitors
  - Ideologically-motivated groups
  - Former or current employees
- Try to identify the attacker with the available pieces of information;
- More generally, try to **find how the attacker got into the system or got the object of the blackmail;**

Contact local law enforcement to inform them.

Try to gain time and details from fraudster. Ask:

- **Proof of what he said: example data, intrusion proof, etc;**
- **Time to get what fraudster wants (money, etc.) ;**

4 REMEDIATION

Objective: Take actions to remove the threat and avoid future incidents.

If a flaw has been identified on a technical asset or a process allowing the attacker to get access to the object of the blackmail, ask for IMMEDIATE fix in order to prevent another case.

- After getting as much information as possible, ignore the blackmail and ensure appropriate watch is in place to detect and react accordingly on any new follow-ups;

- Don't take any remediation decision alone if strategic assets or human people are targeted. Involve appropriate departments;

Remember that a positive answer to the fraudster is an open door for further blackmails.

5 RECOVERY

Objective: Restore the system to normal operations.

Notify the top management of the actions and the decision taken on the blackmail issue.

6 LESSONS LEARNT

Objective: Document the incident's details, discuss lessons learned, and adjust plans and defences.

Inform your hierarchy and subsidiaries about the incident, this could help to avoid similar attacks later.

If you don't want to file a complaint, at least notify Law Enforcement as other organizations could be affected. At the same time, inform hierarchy and subsidiaries to have a unique position in case the fraudster tries to blackmail another internal department.

Report

An incident report should be written and made available to all of the stakeholders.

The following themes should be described:

- Initial detection.
- Actions and timelines.
- What went right.
- What went wrong.
- Incident cost.

Capitalize

Actions to improve the blackmail handling processes should be defined to capitalize on this experience.

IRM #16

TRADEMARK INFRINGEMENT

Guidelines to handle trademark infringement incidents

Version 1.1

TRADEMARK INFRINGEMENT DEFINITION

“a violation of the exclusive rights attached to a trademark without the authorization of the trademark owner or any licensees.”
(WIKIPEDIA)

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue. It is aimed at:

- Administrators
- Security Teams and Operation Centre
- CISOs and deputies

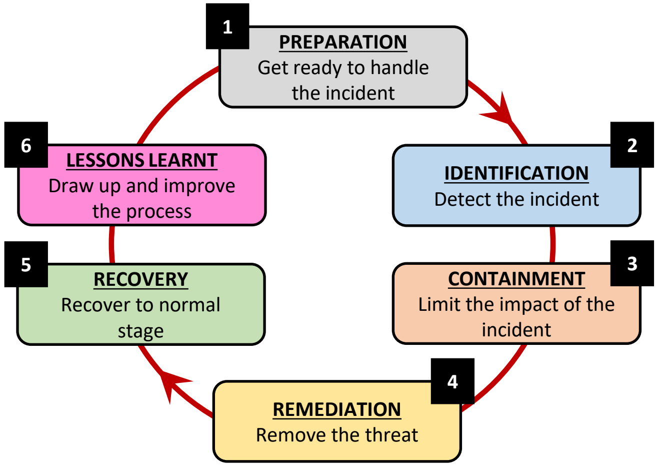
Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line’s Incident.

Incident Response Team contact:

____

____

INCIDENT HANDLING CYCLE



1 **PREPARATION** Get ready to handle the incident

2 **IDENTIFICATION** Detect the incident

3 **CONTAINMENT** Limit the impact of the incident

4 **REMEDIATION** Remove the threat

5 **RECOVERY** Recover to normal stage

6 **LESSONS LEARNT** Draw up and improve the process

1 PREPARATION

Objective: Establish contacts, define procedures, gather information to save time during an attack.

- Maintain a list of all legitimate trademarks belonging to your company and its subsidiaries. This will help in assessing the situation at hand and prevent you from starting an infringement procedure on an outdated trademark, an unrelated legitimate website or social network account;

- Establish a thorough, evidence-based information list related to your trademarks to support your legal rights:
    - ○ Name(s), legitimate domain names and social media accounts used by your company and its subsidiaries;
    - ○ Your trademarked words, symbols, taglines, graphics, etc.;
    - ○ Trademark registration numbers if applicable;
    - ○ International and federal/local trademark registration offices (USPTO, INPI, etc.) where registered trademarks have been labelled as such if applicable;
    - ○ Any other document establishing clearly that a trademark belongs to your company;

- Prepare trademark infringement e-mail forms. You will use them for every trademark infringement case, if possible in several languages. This will help speed up things when trying to reach out the registrar, service provider and any other relevant party during the procedure;

- Promote a central domain management system using normalized WHOIS fields;

- Promote an ethical online advertisement to avoid appearing in parked domain names;

1 PREPARATION

Internal contacts

- Maintain a list of all people involved in trademark registration in the company especially those part of the legal and PR departments.

- Maintain a list of all people accredited to take decisions on trademarks and eventual actions regarding trademark infringement. If possible, obtain a written agreement that gives you the ability to take this kind of decisions.

External contacts

- Establish and maintain a list of external contacts within registrars and service providers involved in trademark issues.

2 IDENTIFICATION

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

Trademark infringement Detection

- Deploy active monitoring of domain names registration through registries’ zones updates whenever possible or brand alert services such as DomainTools;

- Set up feeds to monitor usernames, pages and groups on social networks;

- Analyse HTTP referrers in website logs to identify fraudulent content downloads and fraudulent mirroring of your websites;

- Set up brand name monitoring with specialized search engines;

Leverage automation whenever possible to trigger alarms and improve reaction times.

Document created by ELYSUMSECURITY LTD – https://www.elysiumsecurity.com – Based on the Société Générale IRM 15 freely available on github

2 IDENTIFICATION

Involve appropriate parties
As soon as an infringement is detected, contact the people in your company who are accredited to take a decision if you haven’t been empowered to do so on your own.

The decision to act on the fraudulent domain name, group or user account must be taken as soon as possible.

Collect evidence

- Collect evidence of infringing domain names, websites, specific URLs (e.g. Facebook vanity URL), pages, groups or account details;
- Make a time-stamped copy of the infringing material (page, group, blog, forum, micro-blogging timeline, etc) and take screenshots if possible;

3 CONTAINMENT

Objective: Mitigate the attack’s effects on the targeted environment.

- Evaluate the impact of the trademark infringement:
  - Can it be used for traffic redirection (cybersquatting, typosquatting, SEO)?
  - Can it be used for spoofing, counterfeiting or scamming (cybersquatting with redirect to the corporate website)?
  - Can it be used to slander the brand?

- Evaluate the visibility of the infringing component:
  - Website visibility (ranking).
  - Number of fans or followers on social medias.

- Monitor the dormant, infringing domain for signs of fraudulent activities:
  - See IRM-1-Phishing and IRM-2-Scam for more information.

4 REMEDIATION

Objective: Take actions to remove the threat and avoid future incidents.

In most trademark issues, monitoring is usually sufficient. Remediation must be started only if there’s an impact on your company or its subsidiaries.

Domain name

- Contact the domain name owner and hosting service provider to notify them of the trademark infringement and ask them to remove the fraudulent content;

- Contact the domain name registrar to notify them of the trademark infringement and ask them to deactivate the associated domain name or to transfer it to you;

- Ask the domain name owner or registrar to redirect all DNS requests to your name servers if possible;

- If neither the domain name owner nor the registrar comply with your requests, initiate an Uniform Domain-Name Dispute-Resolution Policy (UDRP) procedure if you are empowered to do so or ask the internal contacts to conduct it.

Social network account

- Contact the service provider of the infringing page, group or account to notify them of any violation of their Trademark Policies or Terms of Service and ask them to deactivate the infringing account;

- Ask the service provider to transfer the trademarked account to an existing company account if possible.

In both cases, send e-mails to the contact addresses of the registrar or service provider. There’s generally an e-mail address to report abuse, legal or copyright issues.

Fill out a trademark or abuse complain form if available.

5 RECOVERY

Objective: Restore the system to normal operations.

Assess the end of the infringement case

- Ensure that the infringing domain name, page, group or account are down or redirected to your company;
- Keep monitoring the infringing domain name, page, group or account. Sometimes a website can reappear later;
- Acquire the infringing domain name when it is available on the market;

6 LESSONS LEARNT

Objective: Document the incident’s details, discuss lessons learned, and adjust plans and defences.

Inform your hierarchy and subsidiaries about the incident, this could help to avoid similar attacks later.

Report
An incident report should be written and made available to all of the stakeholders.
The following themes should be described:

- Initial detection.
- Actions and timelines.
- What went right.
- What went wrong.
- Incident cost.

Capitalize
Actions to improve the trademark infringement management processes should be defined to capitalize on this experience.

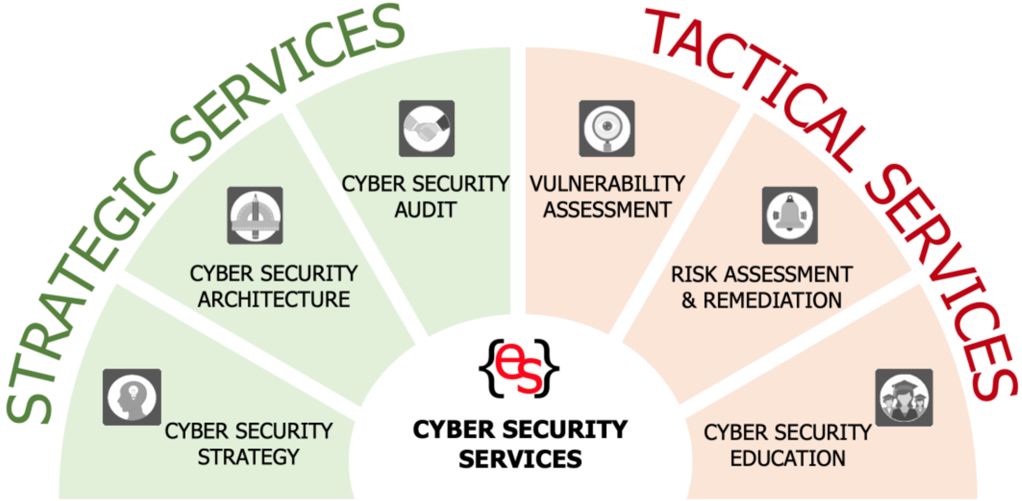
ABOUT ELYSIUMSECURITY LTD.

ELYSIUMSECURITY PROVIDES A PORTFOLIO OF **STRATEGIC** AND **TACTICAL SERVICES** TO HELP COMPANIES **PROTECT** AND **RESPOND** AGAINST **CYBER SECURITY THREATS**. WE DIFFERENTIATE OURSELVES BY OFFERING **DISCREET**, **TAILORED** AND **SPECIALIZED** ENGAGEMENTS.

ELYSIUMSECURITY OPERATES IN **MAURITIUS** AND IN **EUROPE**, A ***BOUTIQUE STYLE*** APPROACH MEANS WE CAN **EASILY ADAPT** TO YOUR BUSINESS OPERATIONAL MODEL AND REQUIREMENTS TO PROVIDE A **PERSONALIZED SERVICE** THAT FITS YOUR WORKING ENVIRONMENT.

ELYSIUMSECURITY PROVIDES **HIGH LEVEL EXPERTISE** GATHERED THROUGH YEARS OF **BEST PRACTICES EXPERIENCE** IN LARGE INTERNATIONAL COMPANIES ALLOWING US TO PROVIDE ADVICE BEST SUITED TO YOUR **BUSINESS OPERATIONAL MODEL** AND **PRIORITIES**.

ELYSIUMSECURITY PROVIDES **PRACTICAL EXPERTISE** TO **IDENTIFY VULNERABILITIES**, ASSESS THEIR **RISKS** AND **IMPACT**, **REMEDIATE** THOSE RISKS, **PREPARE** AND **RESPOND** TO INCIDENTS AS WELL AS RAISE **SECURITY AWARENESS** THROUGH AN ORGANIZATION.



HTTPS://WWW.ELYSIUMSECURITY.COM
CONSULTING@ELYSIUMSECURITY.COM