INCIDENT RESPONSE METHODOLOGIES

-

CYBER INCIDENT PLAYBOOKS

Table of Contents

INTRODUCTION

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

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 each phase objectives definition
- Standardisation of the lessons learnt phase actions.

Each IRM is based on the following standard incident handling cycle which contains 6 phases.

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

MALWARE INFECTION RESPONSE

Guidelines to handle information system Worm infection

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

- 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 (EDR, Antivirus, IDS, logs analyzers), 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.

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 analyzed:

- Antivirus logs
- IDS/IPS
- EDR
- Suspicious connection attempts on servers
- High number of locked accounts
- 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

Analyze symptoms to identify the malware, its propagation vectors and countermeasures.

Leads can be found from:

- CERT's bulletins
- External support contacts (antivirus companies, etc.)
- Security websites
- Threat intelligence capabilities and providers

Notify Chief Information Security Officer.
Contact your national CERT and regulators 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.

CONTAINMENT
OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

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

Disconnect the infected area from the Internet.

1. Isolate the infected area. Disconnect it from any network.
2. If business-critical traffic cannot be disconnected, allow it after ensuring that it cannot be an infection vector or find validated circumventions techniques.
3. Neutralize the propagation vectors. A propagation vector can be anything from network traffic to software flaw. Relevant countermeasures must be applied (patch, traffic blocking, disable devices, etc.).

For example, the following tools/techniques can be used:

- EDR
- Patch deployment tools (WSUS)
- Windows GPO
- Firewall rules
- Operational procedures

4. 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 malware must be monitored.

Mobile devices

- Make sure that no laptop, Smartphone or mobile storage can be used as a propagation vector by the malware. If possible, block all their connections.
- Ask end-users to follow directives precisely.

At the end of this step, the infection should be contained.

REMEDIATION
OBJECTIVE: TAKE ACTIONS TO REMOVE THE THREAT AND AVOID FUTURE INCIDENTS.

Identify
Identify tools and remediation methods.
The following resources should be considered:

- Antivirus signature database
- External support contacts
- Security websites
- Yara scan, Loki, DFIR-ORC, ThorLite
- EDR search

Define a disinfection process. The process has to be validated by an external structure, i.e. CERT, SOC, Incident Response team.

The most straight-forward way to get rid of the worm is to remaster the machine.

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:

- EDR
- Windows WSUS and GPO
- Antivirus signature deployment
- Manual disinfection
- Vulnerability patching

Warning: some worm can block some of the remediation deployment methods. If so, a workaround must be found.

Remediation progress should be monitored by the crisis cell.

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

LESSON LEARN

OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

Report

A crisis report should be written and made available to all of the actors of the crisis management cell.

The following themes should be described:

- Initial cause of the infection
- Actions and timelines of every important event
- What went right
- What went wrong
- Incident cost
- Indicators of compromise

Capitalize

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

WINDOWS INTRUSION DETECTION

Live Analysis on a suspicious Windows system

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

- Deploy an EDR solution on endpoints and servers
  - This tool became one of the cornerstones of the incident response in case of ransomware or in large scale compromise, facilitating identification, containment, and remediation phases.
  - Launch EDR Search and AV scan with IOC explicit rules and get first indicators for remediation progress following.
  - Set your EDR policies in prevent mode.
- In absence of EDR, 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.
- Acquisition profiles for EDR or tools like FastIR, DFIR Orc, KAPE must be prepared.
- 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.

Be prepared to notify abuse teams and law enforcement services and regulators if required during an incident (cell crisis management).

It can be a real advantage to work in a huge corporate environment, where all user machines are the same, installed from a master. 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.

ENDPOINTS

- 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
- Make sure all equipment get setting on same NTP

- Select what kind of files can be lost / stolen and restrict the access for confidential files
- Make sure that analysis tools are up, functional (Antivirus, EDR, IDS, logs analyzers), not compromised, and up to date
- Install from the same original master

IDENTIFICATION

OBJECTIVE: DETECT THE INCIDENT, DETERMINE ITS SCOPE, AND INVOLVE THE APPROPRIATE PARTIES.

1 – Evidence acquisition

WARNING (VOLATILE DATA):
BEFORE CARRYING OUT ANY OTHER ACTIONS, MAKE SURE TO MAKE A VOLATILE MEMORY CAPTURE BY DOWNLOADING AND RUNNING FTK IMAGER, WINPMEM OR ANOTHER UTILITY FROM AN EXTERNAL DRIVE.
VOLATILE DATA PROVIDES VALUABLE FORENSIC INFORMATION AND IS STRAIGHTFORWARD TO ACQUIRE.

Volatile data
Volatile data is useful to perform analysis on command line history, network connections, etc. Use "Volatility" if possible.

Take a triage image

- Use tools like EDR, FastIR, DFIR Orc, KAPE with preconfigured profiles.

Or full disk copy image

- With tools like dd, FTKImager, etc.

Warning: you may need admin privileges on the machine or a write-blocker (physical or logical) depending on the use case.

2 – Memory analysis:

- Look for rogue processes
- Review process DLLs and handles
- Check network artifacts
- Look for code injection
- Check the presence of rootkits
- Dump suspicious processes for further analysis

If the issue is considered as strategic (sensitive resources access), a specific crisis management cell should be activated. i.e., Large Scale Compromise IRM

IDENTIFICATION

3 – Identify persistence mechanisms:

Persistence can be allowed through different techniques including:

- Scheduled tasks
- Service replacement
- Service creation
- Auto-start registry keys and startup folder
- Dll search order hijacking
- Trojaned legitimate system libraries
- Local Group Policy
- MS office add-in
- Pre-boot persistence (BIOS/UEFI/MBR alteration)

*You may consider using Microsoft autoruns for a quick win

4 – Check Event Logs

- Scheduled tasks log (creation and execution)
- Account Logon Events (check for out-of-office connections)
- Suspicious local account
- Malicious Services
- Clearing Event Logs
- RDP/TSE Logs
- Powershell Logs
- SMB Logs

5 – Super-Timeline

- Process evidence and generate a super-timeline with tools like Log2timeline
- Analyze the generated timeline with TimelineExplorer or glogg for example

6 – To go further

- Hash lookups
- MFT anomalies and timestamping
- Anti-virus/Yara analysis/Sigma:

    Mount the evidence in a read-only mode. Run Anti-virus scan or multiple Yara files for a quick-win detection.
    Please note that unknown malware may be not detected.

If the issue is considered as strategic (sensitive resources access), a specific crisis management cell should be activated. i.e., Large Scale Compromise IRM

CONTAINMENT
OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

Make sure that all footholds of the attackers have been identified before taking containment measure
Be discrete if necessary and possible

Memory and selective volatile artifacts' acquisition must be achieved before the following steps:
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.

If possible, isolate the machine via EDR

Or

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:

- Inspect network shares or any publicly accessible folders shared with other users 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.
- Apply fixes when applicable (operating system and applications) in case the attacker used a known vulnerability.

REMEDIATION
OBJECTIVE: TAKE ACTIONS TO REMOVE THE THREAT AND AVOID FUTURE INCIDENTS.

WARNING:
ONLY START REMEDIATING ONCE YOU ARE 100% SURE THAT YOU HAVE WELL SCOPED UP AND CONTAINED THE PERIMETER - TO PREVENT THE ATTACKER FROM LAUNCHING RETALIATION ACTIONS.

In case the system has been compromised:

- The most straight-forward way to get rid of the malware is to remaster the machine.
- Temporarily remove all accesses to the accounts involved in the incident.
- Remove all malicious files installed and persistence mechanisms put in place by the attacker.
- Apply the EDR prevention mode for all identified IOCs.

RECOVERY
OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.

No matter how far the hacker has advanced into the system and the knowledge you might have obtain about the compromise, if the system has been breached, the best practice is to reinstall the system fully from original media and apply all security updates 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.
- Restore all files that could have been altered (Example: svchost.exe) by the attacker.

LESSON LEARNED

OBJECTIVE: DOCUMENT THE INCIDENT’S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

Report

An incident report should be written and made available to all applicable actors.

The following topics should be covered:

- Initial detection
- Actions and timelines of every important events
- What went right
- What went wrong
- Impact from the incident
- Indicators of compromise

Lessons learned

Actions to improve the Windows intrusion detection management processes should be defined to capitalize on this experience.
Profiles of acquisition tools can be tweaked to better match artifacts detected during the investigation.

UNIX/LINUX INTRUSION DETECTION

Live Analysis on a suspected system

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

Deploy an EDR solution on endpoints and servers

- This tool became one of the cornerstones of the incident response in case of ransomware or in large scale compromise, facilitating identification, containment, and remediation phases.
- Launch EDR Search and AV scan with IOC explicit rules and get first indicators for remediation progress following.
- Set your EDR policies in prevent mode.

In absence of EDR, 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 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.

- Use Auditd and Linux Logs like system, message, and applications logs (Apache, NGINX, …)
- Use AppArmor for example

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.

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 ". "or ".. "or " " :

```
# find / --name " *" –print

# find / --name ". *" –print

# find / --name ".. *" --print
```

- 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.

IDENTIFICATION

Unusual Services

Run chkconfig (if installed) to check for all enabled services:

```
# chkconfig --list
```

Look at the running processes (remember: a rootkit might change your results for everything in this paper, especially here!).

```
# ps –aux
```

Use lsof -p [pid] on unknown processes

You should know your usual running processes and be able to figure out which processes could have been added by a hacker. Pay special attention to the processes running under UID 0.

Unusual Network Activity

- Try to detect sniffers on the network using several ways:
  - 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

- Look for unusual MAC entries in your LAN:

  # arp -a

- Look for unexpected or new IP addresses on the network:

  # netstat -ntaupe

  # netstat -ant

  # watch ss -tt

IDENTIFICATION

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

  # ls –la /etc/cron.*

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 that includes a 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 in most Linux distributions. Here are the main ones (paths may vary according to distributions):

- /var/log/message: General message and system related stuff
- /var/log/auth.log: Authentication logs
- /var/log/kern.log: Kernel logs

- /var/log/cron.log: Crond logs (cron job)
- /var/log/maillog: Mail server logs
- /var/log/httpd/: Apache access and error logs directory
- /var/log/boot.log: System boot log
- /var/log/mysqld.log: MySQL database server log file
- /var/log/secure: Authentication log
- /var/log/utmp or /var/log/wtmp: Login records file
- /var/log/syslog: cron, samba activity and more
- /root/.*history: Root user command history
- /home/*/.*history: Users' command history

To look through the log files, tools like cat and grep may be useful:

```
# cat /var/log/httpd/access.log | grep "GET /signup.jsp"
```

IDENTIFICATION

Unusual Kernel log Entries

- Look through the kernel log files on the system for suspicious events:

```
# dmesg
```

List all important kernel and system information:

```
# lsmod

# 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 will probably change all file timestamps. This should only be done after all other investigations are done and you feel like you can alter these data.

- On systems with RPM installed, use:

```
# rpm –Va | sort
```

- On some Linux, a script named check-packages can be used.
- On Solaris:

```
# pkg_chk –vn
```

- On Debian:

```
# debsums –ac
```

- On Openbsd (not really this but a way):

    # pkg_delete -vnx

CONTAINMENT
OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

- Securely backup important data from the compromised machine, if possible, using a bit-by-bit physical copy of the whole hard disk on an external support. Also make a copy of the memory (RAM) of the system, which will be investigated if necessary.
- Isolate with the EDR and inspect other computers and networks.

Or

- Isolate with the firewall or switches.

If the machine is not considered critical for the 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 identification step didn't give any result, but the system is still suspected of being compromised.

Try to find evidence of every action of the attacker: (using forensic tools like Sleuth Kit/Autopsy for example)

- Find all files used by the attacker, including deleted files and see what has been done with them or at least their functionality to evaluate the threat.
- Check all files accessed recently.
- Check log files.
- 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 an insider.
- Apply fixes when applicable, to prevent the same kind of intrusion, in case the attacker used a known fixed vulnerability.

REMEDIATION
OBJECTIVE: TAKE ACTIONS TO REMOVE THE THREAT AND AVOID FUTURE INCIDENTS.

WARNING: ONLY START REMEDIATING ONCE YOU ARE 100% SURE THAT YOU HAVE WELL SCOPED UP AND CONTAINED THE PERIMETER - SO AS TO PREVENT THE ATTACKER FROM LAUNCHING RETALIATION ACTIONS.

Temporarily remove all accesses for the involved accounts in the incident and remove malicious files.

RECOVERY
OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.

No matter how far the attacker has gone into the system and the knowledge you might have about the compromise, as long as the system has been compromised, 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
- Check the integrity of the whole data stored on the system, using file hashes (i.e., SHA256)
- Restore all binaries which could have been changed (Example: /bin/su)
- Replace all compromised packages with safe ones

LESSONS LEARNED

OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

Report

A crisis report should be written and made available to all the actors of the crisis management cell. The following themes should be described:

- Initial detection
- Actions and timelines
- What went right
- What went wrong
- Incident cost
- Indicators of compromise

Capitalize

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

Lessons learned

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

DDOS INCIDENT RESPONSE

Guidelines to handle Distributed Denial of Service incidents

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

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 and to an Anti-DDoS services 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).
- Make sure your ISP and DDoS mitigation service have a 24/7 phone support.

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.
- Deploy a Web Application Firewall to protect against application-layer DDoS.
- 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.
- 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 on 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.

IDENTIFICATION

Communication

- Prepare an internal and an external communication template about DDoS incidents.
- Identify channel where this communication will be posted.
- The “preparation” phase is to be considered as the most important element of a successful DDoS incident response.

Analyze the attack

- Keep in mind the DDoS attack could be a smokescreen hiding a more sophisticated and targeted attack.
- Check your anti-DDoS service analysis and your scrubbing centre reports:
  - 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, Netflow, Ntop, MRTG, Cacti, Nagios

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.

IDENTIFICATION

OBJECTIVE: DETECT THE INCIDENT, DETERMINE ITS SCOPE, AND INVOLVE THE APPROPRIATE PARTIES.

Check the background

- Find out whether the company received an extortion demand as a precursor to the attack:
  - Check for emails in your security email gateway based on a keyword list.
  - Some threat actors send extortion demands directly to the email addresses in the Whois records of the targeted website.
- Look for revendications of the attack on Social Medias.
- Search if anyone would have any interest into threatening your company:
  - Competitors
  - Ideologically motivated groups (hacktivists)
  - Former employees

CONTAINMENT
OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

- If the bottleneck is a particular feature of an application, temporarily disable the 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.
- 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 to get management approval.

If the bottleneck is at the ISP's or anti-DDoS service's side, only they can take efficient actions. In that case, work closely with your ISP and/or anti-DDoS provider and make sure you share information efficiently.

REMEDIATION
OBJECTIVE: TAKE ACTIONS TO STOP THE DENIAL-OF- SERVICE CONDITION.

- Contact your ISP and/or anti-DDoS provider and make sure that they enforce remediation measures. For information, here are some of the possible measures:
  - Filtering (if possible, at level Tier 1 or 2)
  - Traffic-scrubbing/Sinkhole/Clean-pipe
  - IP public balancing/splitting/switching
  - Blackhole Routing

Technical remediation actions can mostly be enforced by your ISP and/or anti-DDoS provider.

IF THE ATTACK HAD A MAJOR IMPACT, YOU MAY HAVE TO MAKE AN INCIDENT REPORTING TO REGULATORS.
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.

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.

LESSONS LEARNED
OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

Report
An incident report should be written and made available to all applicable actors.

The following topics should be covered:

- Initial detection
- Actions and timelines of every important events
- What went right
- What went wrong
- Impact from the incident
- Indicators of compromise

Lessons learned
Actions to improve the DDoS management processes should be defined to capitalize on this experience. Consider what relationships inside and outside your organizations could help you with future incidents.

MALICIOUS NETWORK BEHAVIOUR

Guidelines to handle a suspicious network activity

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

- Intrusion Detection Systems (EDR, NIPS, IPS)
- 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.
- Verify access to the device and its ability to watch concerned perimeters.
- Ensure that you can isolate endpoints, area (with EDR for example or Firewall).

Network

- Make sure that an inventory of the network access points is available, accessible and up to date, if possible, with versioning.
- Make sure that network teams have up to date network maps and configurations with concerned zones and operational teams.
- Look for potential unwanted network access points regularly and close them.
- Look for VPN access and Cloud access from rare locations.
- Deploy and monitor traffic management tools.

Baseline traffic

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

Make sure people are comfortable with the tools and know how to use them. Keep logs operational even when they have been archived.
Having a good log retention policy is essential (more than 6 months).

IDENTIFICATION

OBJECTIVE: DETECT THE INCIDENT, DETERMINE ITS SCOPE, AND INVOLVE THE APPROPRIATE PARTIES.

Sources of detection:

- Notification by user/helpdesk.
- IDS/IPS/NIDS/EDR logs, alerts and reports.
- Detection by network staff.
- Firewall and proxy logs.
- Complaint from an external source.
- Honeypots or any other deceptive solution.

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 advice.
- Know how to restore and consult logs even when they have been archived.

Analyze 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.
- Map with business risks to properly prioritize the analysis or containment.
- Identify traffic's technical characteristics:
    - 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.

CONTAINMENT

OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

If the issue is considered as strategic (sensitive resource 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) to perform further investigation.
- Adopt acceptable mitigation controls (MFA, geo-filtering) for the business-critical flux in agreement with the business line managers.
- Terminate unwanted connections or processes on affected machines.
- Use firewall/IPS/EDR rules to block the attack.

- Use IDS rules to match with this malicious behavior and inform technical staff on new events.
- Apply ad hoc actions in case of strategic issue:
  - Deny egress destinations in EDR, proxies and/or firewalls.
  - Configure security controls policy management to contain or reject connections from compromised machines.
  - Limit access to critical/confidential data.
  - Create booby-trapped documents with watermarking that could be used 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.

REMEDIATION
OBJECTIVE: TAKE ACTIONS TO STOP THE MALICIOUS BEHAVIOR.

Block the source

- Using analysis from previous steps identification and containment, find out all communication channels used by attacker and block them on all your network boundaries.
- If the source has been identified as an insider, take appropriate action 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 the Intrusion IRMs (2-Windows and 3-Linux) 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.

RECOVERY
OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.

1. Ensure that the network traffic is back to normal.
2. Re-allow connections to previously contained network segments.

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

LESSON LEARNED

OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

Report

A report should be written and made available to all the actors. The following themes should be described:

- Initial cause of the issue
- Actions and timelines
- What went right
- What went wrong
- Incident cost
- Indicators of compromise

Capitalize

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

WEBSITE DEFACEMENT

Live reaction on a compromised web server

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

- Have up-to-date schemes describing your applicative components related to the web server.
- Make sure you have an up-to-date network map.
- Build a backup website up-and-ready, on which you can publish content.
- Define a procedure to redirect every visitor to this backup website (a static maintenance page for example).
- Deploy monitoring and intrusion prevention tools (WAF, fail2ban and the likes) to detect and prevent any abnormal activities targeting your critical webservers.
- Export the web server's log files to an external server. Make sure clocks are synchronized between each server.
- Deploy attack and vulnerability exploitation detection rules based on the server's logs and monitor them.
- Audit your websites before the release and on regular basis (monthly if possible).
- Reference all sources of external static or dynamic contents.
- Have operational contacts of your hosting provider readily available.
- Make sure your hosting provider enforces policies to log all events and verify your contractual compliance.
- Prepare communication templates in case the incident is visible for users and needs to be explained.

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 explicit ("You have been hacked by xxx").
- Users: you receive calls from users or notifications from employees about problems they notice while
- browsing the website.
- Security checks with tools such as Google SafeBrowsing.

Verify the defacement incident and detect its origin:

- Check files' metadata (in particular, check modification dates, hash signatures).
- Check mashup content providers.

- Check links present in the source code (src, meta, css, scripts, …).
- Check log files and alerts generated by the detection rules.
- Scan databases for malicious content.

The source code of the suspicious page must be analyzed carefully to identify and scope up the problem.

Be sure the problem originates from a web server belonging to the company and not from the web content located outside your infrastructure, such as in ad banners from a third party.

CONTAINMENT
OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

- Back up all the data stored on the web server for forensic purposes and evidence collection. The best practice here, if applicable, is to create a complete bit-to-bit copy of the hard-disk used by the web server. This may notably be helpful to recover deleted content.
- Check your network architecture map. Verify that the vulnerability exploited by the attacker is not located elsewhere:
  - Check the system on which the web server is running
  - Check other services running on that machine
  - Check incoming and outgoing connections made from the server

If the source of the attack stems from another system, investigate the culprit machine.

- Try to find evidence behind every action perpetrated by the attacker:
- Find out how the attacker got into the system in the first place and fix the root cases:
  - A web component vulnerability allowing write access: fix the vulnerability by applying applicable remediations
  - CMS plugin vulnerabilities are often exploited by attackers and need to be identified and patched.
  - Open public folder: make it private
  - SQL weakness allowing injection: correct the code
  - Mashup components: cut off implicated mashup feeds
  - An administrative modification by physical access: modify the access rights

If required (complex issue on an important web server), deploy a temporary up-to-date web server. The server should offer the same content than that one of the compromised machines or at least display legitimate content such as a static maintenance page. The best is to display temporary static content, containing only HTML code. This prevents another infection in case the attacker is still able to leverage the same vulnerability.

REMEDIATION
OBJECTIVE: TAKE ACTIONS TO REMOVE THE THREAT AND AVOID FUTURE DEFACEMENTS.

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

RECOVERY
OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.

- Change all user passwords if the web server provides user-authentication and you have evidence or reasons to believe the passwords may have been compromised. This may require a user communication campaign.
- If a backup server has been used, restore the primary web server components to the nominal state.
- Monitor logs and alerts closely to detect new attacks.

LESSON LEARNED
OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

Communication
If the defacement has become public, consider preparing and sending out a dedicated communication message explaining the incident.

Report
A crisis report should be written and made available to all the involved parties.

The following topics should be detailed:

- Initial detection
- Actions and timelines
- What went right
- What went wrong
- Incident's cost
- Indicators of compromise

Should a vulnerability be identified, report any undocumented flaw impacting to the application's editor, so that the code can be reviewed and receive an official fix.

Capitalize
Actions to improve the handling of defacement incidents should be defined to capitalize on this experience.

WINDOWS MALWARE DETECTION

Live Analysis on a suspicious computer

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

- Deploy an EDR solution on endpoints and servers
  - This tool became one of the cornerstones of incident response in case of ransomware or in large scale compromise, facilitating identification, containment, and remediation phases.
  - Launch EDR Search and AV scan with IOC explicit rules and get first indicators for remediation progress following.
  - Set your EDR policies in prevent mode to prevent unnecessary business disruption.
- In absence of EDR, a physical access to the suspicious system should be given to the forensic investigator. Physical access is preferred to remote access, as 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.
- Acquisition profiles for EDR or tools like FastIR, DFIR Orc, KAPE, DumpIt, FTK Imager, WinPmem must be prepared and tested.
- 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.

Endpoints

- Ensure that the monitoring tools are up to date.
- Deploy Sysmon, SmartScreen and apply recommendation baselines from ANSSI and CIS.
- Establish contacts with your network and security operation teams.
- Make sure that an alert notification process is defined and well-known from everyone.
- Make sure all equipment are synchronized with the same NTP.
- Select what kind of files can be lost / stolen and restrict the access for confidential files.
- Make sure that analysis tools are up, functional (Antivirus, EDR, IDS, logs analyzers), not compromised, and up to date.
- Install from the same original master.

IDENTIFICATION

OBJECTIVE: DETECT THE INCIDENT, DETERMINE ITS SCOPE, AND INVOLVE THE APPROPRIATE PARTIES.

The family of malware identified will impact the next steps of the incident response. Investigation will be faster for a Potentially Unwanted Software or a Miner. Stealer, Dropper or Ransomware family will imply a deeper analysis and may lead to another kind of incident (please refer to large scale malware compromise, Ransomware, Windows Intrusion Detection or Worm Infection if needed).

General signs of malware presence on the desktop

- Several leads might hint that the system could be compromised by malware:
- EDR, HIDS, 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 present on one or more Internet Blocklists.
- People are complaining about you e-mailing them/reaching them by IM etc. while you did not.

If the issue is considered as strategic (sensitive resources access), a specific crisis management cell should be activated. i.e., Large Scale Compromise IRM-18

IDENTIFICATION

1 – Evidence acquisition

WARNING (VOLATILE DATA):

BEFORE CARRYING OUT ANY OTHER ACTIONS, MAKE SURE TO MAKE A VOLATILE MEMORY CAPTURE BY DOWNLOADING AND RUNNING FTK IMAGER, WINPMEM OR ANOTHER UTILITY FROM AN EXTERNAL DRIVE.

VOLATILE DATA PROVIDES VALUABLE FORENSIC INFORMATION AND IS STRAIGHTFORWARD TO ACQUIRE.

- Volatile data:

Volatile data is useful to perform analysis on command line history, network connections, etc. Use “Volatility” if possible.

- Take a triage image:

Use tools like EDR, FastIR, DFIR Orc, KAPE with preconfigured profiles.

Or

- Full disk copy image:

  With tools like dd, FTKImager, etc.

Warning: you may need admin privileges on the machine or a write-blocker (physical or logical) depending on the use case.

2 – Memory analysis:

- Look for rogue processes
- Review process DLLs and handles
- Check network artifacts
- Look for code injection
- Check the presence of rootkits
- Dump suspicious processes for further analysis

If the issue is considered as strategic (sensitive resources access), a specific crisis management cell should be activated. i.e., Large Scale Compromise IRM-18

IDENTIFICATION

3 – Identify persistence mechanisms:

Persistence can be allowed through different techniques including:

- Scheduled tasks
- Service replacement
- Service creation
- Auto-start registry keys and startup folder
- Dll search order hijacking
- Trojaned legitimate system libraries
- Local Group Policy
- MS office add-in
- Pre-boot persistence (BIOS/UEFI/MBR alteration)

You may consider using Microsoft autoruns for a quick win.

4 – Check Event Logs

- Scheduled tasks log (creation and execution)
- Account Logon Events (check for out-of-office connections)
- Suspicious local account
- Malicious Services
- Clearing Event Logs
- RDP/TSE Logs

- Powershell Logs
- SMB Logs

5 – Super-Timeline

- Process evidence and generate a super-timeline with tools like Log2timeline.
- Analyze the generated timeline with TimelineExplorer or glogg for example.

6 – To go further

- Hash lookups
- MFT anomalies and timestamping
- **Anti-virus/Yara analysis/Sigma**
  - Mount the evidence in a read-only mode. Run Anti-virus scan or multiple Yara files for a quick- win detection.
  - Please note that unknown malware may be not detected.

If the issue is considered as strategic (sensitive resources access), a specific crisis management cell should be activated. i.e., Large Scale Compromise IRM

CONTAINMENT
OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

WARNING (VOLATILE DATA):

MEMORY AND SELECTIVE VOLATILE ARTIFACTS' ACQUISITION MUST BE CARRIED OUT BEFORE THE FOLLOWING STEPS HAVE TAKEN PLACE.

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.

- If possible, isolate the machine via EDR.

OR

- 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 a few seconds until the computer switches off.

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.)

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

- Inspect network shares or any publicly accessible folders shared with other users 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.
- Apply fixes when applicable (operating system and applications) in case the attacker used a known vulnerability.

REMEDIATION
OBJECTIVE: TAKE ACTIONS TO REMOVE THE THREAT AND AVOID FUTURE INCIDENTS.

WARNING: ONLY START REMEDIATING ONCE YOU ARE 100% SURE THAT YOU HAVE WELL SCOPED UP AND CONTAINED THE PERIMETER - AS TO PREVENT THE ATTACKER FROM LAUNCHING RETALIATION ACTIONS.

The most straight-forward way to get rid of the malware is to remaster the machine.

- 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.
- Remove all malicious files installed and persistence mechanisms put in place by the attacker.
- Apply the EDR prevention mode for all identified IOCs.

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.
- Change all the system's accounts passwords and make your users do so in a secure way.
- Reboot the machine after all the suspicious files have been removed and confirm that the workstation is not exhibiting any unusual behavior. A full, up-to-date AV and EDR scan of the hard-drive and memory are recommended.

If a user is at the origin of the compromise, you should reinforce security awareness campaigns.

LESSON LEARNED
OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

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
- Indicators of compromise

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

Profiles of acquisition tools can be tweaked to better match artifacts detected during the investigation.

BLACKMAIL

Guidelines to handle blackmail attempt

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

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.

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.
- Investigate email to get all the information about the incident (username, MX servers, etc.).
- 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.

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 [1])
- Mass-mailing using the brand (spam, sextortion, child pornography [2], bad rumors, 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.)

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.

RECOVERY
OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.

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

LESSON LEARNED

OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

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 actors of the incident.

Following themes should be described:

- Initial detection
- Actions and timelines
- What went right
- What went wrong
- Incident cost
- Indicators of compromise

Capitalize

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

MALWARE ON SMARTPHONE

How to handle a suspicious smartphone

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

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.

It is recommended to:

- Enable logging (MDM, applications list or else)
- Install Antivirus/Security apps over smartphone
- Configure a VPN to analyze network activity

For Forensic:

- For Android:
  - Activate Developer options with USB Debugging (be careful it could be a risk, public USB charging facilities for example) or have a process to activate it
  - Unlock OEM options if possible
- Test your extraction routines in advance to make sure they are compatible with your evidence

IDENTIFICATION

OBJECTIVE: DETECT THE INCIDENT, DETERMINE ITS SCOPE, AND INVOLVE THE APPROPRIATE PARTIES.

Main points of notification for suspicious smartphone:

- Antivirus/Security apps raise alerts
- Check for anomalous rights granted to applications
- Anomalous system activity, unusually slow functioning
- Anomalous network activity, slow Internet connection
- The system reboots or shutdowns without reason
- Applications crash unexpectedly
- User receives one or multiple messages, containing unusual characters (SMS, MMS, Bluetooth messages, etc.)
- Increase in phone bill or web activity
- Calls to unknown phone numbers or at unusual hours/days
- A monitoring should be done to check unusual user bill or network activity

Ask the user about his/her usual activity on the smartphone: which websites usually visited, which external applications are installed.

CONTAINMENT
OBJECTIVE: MITIGATE THE ATTACK'S IMPACTS ON THE TARGETED ENVIRONMENT.

Ask the user to provide his/her credentials to access the smartphone including:

- SIM card PIN code
- Smartphone password
- iCloud login/password
- Google Play credentials,
- backup password…
- Ensure the user is provided with a replacement device to use during the investigation.
- Back up the smartphone data by creating a physical filesystem, logical backup or manual acquisition.
- Put the phone in a faraday bag if available.

After acquisition, remove the battery (if feasible) or put the phone in the airplane mode to block all activity (WiFi, Bluetooth, etc).

Additional actions:

- Remove the SIM to perform additional analysis outside the smartphone.
- Perform an antivirus or security scan of the backup or acquired files on a dedicated forensic station.
- Perform applicable forensic routine base on your use case.

Specific tools should be used by your incident response team to lead forensic investigation on the smartphone.
Use a dedicated forensic solution to analyze the captured data or the smartphone (Cellebrite, XRY, Oxygen, Axiom, Andriller, etc.)

REMEDIATION
OBJECTIVE: TAKE ACTIONS TO REMOVE THE THREAT AND AVOID FUTURE INCIDENTS.

- Remove the identified threat from the smartphone.

Or

- Wipe the infected smartphone and Hard/Soft reset it to factory settings with a pristine firmware.
- Reinsert the SIM card back into the smartphone.

Signal all identified malicious applications still available through marketplaces for removal.

RECOVERY

OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.

- Selectively reinstall saved data and apps from the backup.

You may consider retaining the device for an additional quarantine period to perform appropriate security checks.

LESSON LEARNED

OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

Report

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

Following themes should be described:

- Initial detection
- Actions and timelines
- What went right
- What went wrong
- Incident cost
- Indicators of compromise

Capitalize

Actions to improve the smartphone policy should be defined to capitalize on this experience.
Debrief the incident with user to improve his/her awareness.

SOCIAL ENGINEERING INCIDENT

How to handle a social engineering incident (phone or e-mail)

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, AND GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

- 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.
- 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.

RED PHONE:

Red phone number must be clearly tagged as “Social Engineering”.

The phone number must 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.

INDENTIFICATION

OBJECTIVE: DETECT THE INCIDENT, DETERMINE ITS SCOPE, AND INVOLVE THE APPROPRIATE PARTIES.

- 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
- 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.

CONTAINMENT
OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

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.

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.

CONTAINMENT

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.

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
- Report email addresses used by the attacker to the provider abuse teams

RECOVERY

OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.

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

LESSON LEARNED

OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

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 the actors of the incident.

The following themes should be described:

- Initial cause of the infection
- Actions and timelines of every important event
- What went right
- What went wrong
- Incident cost (direct and indirect losses)
- Indicators of compromise

Capitalize

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

INFORMATION LEAKAGE

Deal with internal information disclosed intentionally

IDENTIFICATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

Contacts

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

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.

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 (i.e., large scale/ransomware).

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.
- Monitor ransomware shaming list websites to detect potential data leakage including third-parties.

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.

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.

IDENTIFICATION

Browsing:

- Data might have been sent on webmail/forums/dedicated websites.
- On the proxy server or SIEM, 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.

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.

IDENTIFICATION

Malware/Ransomware:

A malware/ransomware compromise can be at the source of an information leakage and must be treated accordingly with the "Malware Detection" IRM 7 or "Ransomware" IRM 17.

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. Analyze concerned data if available

- Sometime, leaked data can be downloaded and analyzed by security team. Ransomware shaming list website often publish leaked information.
- Using data analysis tools like Aleph can help legal teams to decide what actions need to be taken.

At the end of this phase, you may consider involving law enforcement services and regulators if required.

CONTAINMENT
OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

- Notify the management, legal and public relation/communication 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).

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.

RECOVERY
OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.

- 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.

LESSON LEARNED
OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

Inform hierarchy, subsidiaries and partners to share the best practices applied on this incident to enforce similar rules on other locations.

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

The following themes should be described:

- Initial cause of the infection
- Actions and timelines of every important event
- What went right
- What went wrong
- Incident impact
- Indicators of compromise

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

INSIDER ABUSE

Guidelines to handle and respond to internal information disclosed intentionally

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

Contacts

- Make sure to have contact points in your public relation team, human resources team and legal department
- Centralize logging for access controls
- Make 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
- Prepare internal and external communication strategy
- Prepare a Data Loss Prevention (DLP) process with GDPR and risk team

Be prepared to notify implicated providers and law enforcement services and regulators if required during an incident (cell crisis management).

IDENTIFICATION

OBJECTIVE: DETECT THE INCIDENT, DETERMINE ITS SCOPE, AND INVOLVE THE APPROPRIATE PARTIES.

Technical identification*

- Alerts from a SIEM or correlation tools:
  - Malicious behavior 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.
- Alerts from DLP controls and services:
  - Tools and processes to detect and prevent data breaches and data exfiltration.
- Alerts from physical access controls

Human identification

- Management:
  - The manager of the insider might be the first to notice the suspected behavior.
- 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.

CONTAINMENT

OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

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

1. **Involve people**

Experts should be informed about the incident so that they can help to assist on it. This includes HR management, legal management, DLP team, PR management and business management of the suspected insider.

2. **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.

3. **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.

4. **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.

5. **Remote access**

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

6. **Seizure**

Seize all the professional computing device of the suspected insider.

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

Use the IRM 02 or 03 depending on the operating system.

Case 2: malicious / fraudulent activity

If malicious or fraudulent behavior 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 evidence 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.

Prepare a communication plan with the communication team (customers, partners …)

REMEDIATION

OBJECTIVE: TAKE ACTIONS TO REMOVE THE THREAT AND AVOID FUTURE INCIDENTS.

- The remediation part is 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
- Review all programs or scripts made by the insider and remove all unnecessary codes
- Review administration tasks (IT Team)

Involve implicated providers and law enforcement services and regulators if required.

RECOVERY

OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.

If the incident has not yet been made public, make sure to notify 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 local teams about the issue to raise awareness and harden security controls.

Roll back on the fraudulent operations committed by the insider.

LESSONS LEARNED

OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

Report

An incident report should be written and made available to all applicable actors. The following themes should be described:

- Initial cause of the infection
- Actions and timelines of every important event
- What went right
- What went wrong
- Incident cost
- Indicators of compromise

Capitalize

Some improvement might be especially valuable considering insider abuse:

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

CUSTOMER PHISHING INCIDENT RESPONSE

Guidelines to handle customer phishing incidents

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

- Create a list of all legitimate domains belonging to your company. This will help analyzing 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.
- Deploy DKIM, DMARC and SPF to all mail chain.
- Monitor cybersquatted domains and content posted on them. Gather contact and abuse information to be prepared in the case you need to use them.

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 (ex: security@yourcompany)
  - Web forms on your company's website (location of the form is important, no more than 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.

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/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/banking information online.

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 spam traps and try to gather spam from partners/third-parties.
- Deploy active monitoring of phishing repositories, like PhishTank and Google Safe Browsing for example.
- Monitor any specialized mailing-list you can have access to, or any RSS/Twitter feed, which could be reporting phishing cases.
- Use automated monitoring systems on all of these sources, so that every detection triggers an alarm for instant reaction.
- 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.

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.

Check the source-code of the phishing website:

- See where the data is exported: either to another web content you cannot access (a PHP script usually), sent by e-mail to the fraudster or using an application API (like Telegram for example).
- Gather information about the phishing-actor which may be available in URI, source code and credential dropping system (email addresses, Telegram bots, etc).
- Do the graphics come from one of your legitimate websites, or are they stored locally?

If possible, 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.

CONTAINMENT
OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

Spread the URL of the attack in case of a phishing website:
Use every way you have to spread the fraudulent URL on every web browser: use the options of Internet Explorer, Chrome, Safari, Firefox, Netcraft toolbar, Phishing-Initiative, etc. This will prevent the users from accessing the website while you work on the remediation phase.

Spread the fraudulent e-mail content on spam-reporting websites/partners. Communicate with your customers:
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.

REMEDIATION
OBJECTIVE: TAKE ACTIONS TO STOP THE PHISHING CAMPAIGN.

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

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.

LESSON LEARNED

OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

Report

A crisis report should be written and made available to all of the actors of the crisis management cell.

The following themes should be described:

- Initial cause of the infection
- Actions and timelines of every important event
- What went right
- What went wrong
- Incident cost

Capitalize

Consider what preparation steps you could have taken to respond to the incident faster or more efficiently.

Update your contacts-lists and add notes as to what is the most effective way to contact each involved party.

Consider what relationships inside and outside your organization could help you with future incidents.

Collaborate with legal teams if a legal action is required.

SCAM INCIDENT RESPONSE

Guidelines to handle fraudulent scam incidents

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

- Create a list of all legitimate domains belonging to your company. This will help analyzing 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 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 (ex: security@yourcompany)
  - Web forms on your company's website (location of the form is important, no more than 2 clicks away from the main page)
  - Visible Twitter account
- Deploy DKIM, DMARC and SPF to all mail chain.

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.

IDENTIFICATION

OBJECTIVE: DETECT THE INCIDENT, DETERMINE ITS SCOPE, AND INVOLVE APPROPRIATE PARTIES.

Warning: Have a dedicated corporate equipment to identify or exchange with the scammer, do not use your personal equipment.

Fraudulent scam detection

- Monitor all your points of contact closely (e-mail, web forms, etc.).
- Monitor cybersquatted domains and content posted on them. Gather contact and abuse formation to be prepared in the case you need to use them.
- Monitor social media accounts usurping your top management or your trademark.
- Deploy spam traps and try to gather spam from partners/third-parties.
- Deploy active monitoring of scam repositories, like 419scam for example.
- Monitor any specialized mailing-list you can have access to, or any RSS/Twitter feed, which could be reporting scam letters.

Use automated monitoring systems on all 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, analyzing if the campaign is sent from one machine or from a botnet.

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

CONTAINMENT

OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

- Spread the fraudulent e-mail content on spam/fraud reporting websites/partners/tools.
- Communicate with your customers.
- Add the URLs in your Blackhole DNS, proxies and firewall's blocklist.

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.

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, and specifically if the scam page is hosted on a cybersquatted domain, 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.
- Contact social media abuse team to takedown fraudulent accounts.
- Block email exchange with this company or person.

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.

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.

LESSON LEARNED
OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

Report
A crisis report should be written and made available to all of the actors of the crisis management cell.

The following themes should be described:

- Initial cause of the infection
- Actions and timelines of every important event
- What went right
- What went wrong
- Incident cost
- Indicators of compromise

Capitalize
Consider what preparation steps you could have taken to respond to the incident faster or more efficiently.

- Update your contacts-lists and add notes as to what is the most effective way to contact each involved party.
- Consider what relationships inside and outside your organization could help you with future incidents.
- Improve DKIM, SPF and DMARC filters.
- Collaborate with legal teams if a legal action is required.

TRADEMARK INFRINGEMENT INCIDENT RESPONSE

Guidelines to handle and respond to trademark infringement incidents

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

- 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.
- Prepare takedown processes and templates with the legal team.
- Have process, experts, and technologies in place to manage the brand portfolio.
- Have a centralize process or repository to manage applicable brand names, IPs, domains, PII's, keywords, etc.

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.

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.
- Set up feeds to monitor usernames, pages and groups on social networks.
- Analyze 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.
- Collect and analyze alerts from trusted partners.

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.

CONTAINMENT

OBJECTIVE: MITIGATE THE INFRINGEMENT 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.

REMEDIATION

OBJECTIVE: TAKE ACTIONS TO STOP THE TRADEMARK INFRINGEMENT.

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 complies with your requests, initiate a 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.

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.
- Consider acquiring the infringing domain name if available.

LESSON LEARNED
OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

Report

A crisis report should be written and made available to all of the actors of the crisis management cell.

The following themes should be described:

- Initial cause of the infection
- Actions and timelines of every important event
- What went right
- What went wrong
- Incident cost
- Indicators of compromise

Capitalize

- Consider what preparation steps you could have taken to respond to the incident faster or more efficiently.
- Update your contacts-lists and add notes as to what is the most effective way to contact each involved party.
- Consider what relationships inside and outside your organization could help you with future incidents.
- Collaborate with legal teams if a legal action is required.

PHISHING

Guidelines to handle and respond to phishing targeting collaborators

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

- Prepare a communication, ready to be published anytime, to warn your collaborators about an ongoing phishing attack. Prepare and test a clear deployment procedure as well.
- Deploy DKIM, DMARC and SPF to all mail chain.
- Implement multi-factor authentication mechanisms.
- Monitor cybersquatted domains and content posted on them. Gather contact and abuse information to be prepared in the case you need to use them.

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 (ex: security@yourcompany)
  - Web forms on your company's website (location of the form is important, no more than 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.

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

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/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/banking information online.

- Run periodic awareness phishing campaigns.
- Deploy a technical solution allowing collaborators to easily report email to security teams.
- Establish specific procedures for attachment and URL analysis.

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 spam traps and try to gather spam from partners/third parties.
- Deploy active monitoring of phishing repositories, like PhishTank and Google Safe Browsing for example.
- Monitor any specialized mailing-list you can have access to, or any RSS/Twitter feed, which could be reporting phishing cases.
- Use automated monitoring systems on all these sources, so that every detection triggers an alarm for instant reaction.
- 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.

Phishing attack scoping

- Determine the number of targeted users.
- Search for exploited compromised accounts and identify related malicious activities.

Analyze the phishing

- Remember to follow established analysis procedures

Determine:

  - If it is a credential harvesting campaign or a malware spreading campaign
  - If it is a targeted campaign or not
- Inspect message subject and body.
- Use sandbox environment to analyse malicious attachments and extract IOCs.
- Analyse links, domain and hostnames with threat intelligence services.
- Check the source-code of the phishing website.

- Investigate email headers for interesting artifacts: originated server and sender information for example.

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.

CONTAINMENT

OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

- Block network IOCs discovered via the attachment / URL analysis on DNS, firewalls, or proxies.
- Block the phishing campaign based on senders, subjects, or other email artifacts via email gateway.
- Try to delete phishing emails from inbox.
- Apply DNS Sinkhole on the suspicious URL (optional depending on DNS architecture).
- Communicate with your collaborators.
- Deploy the alert/warning page with information about the current phishing attack.

REMEDIATION

OBJECTIVE: TAKE ACTIONS TO STOP THE PHISHING CAMPAIGN.

- Change and/or block temporarily login credentials of compromised accounts.

If the phishing campaign was targeted, consider contacting law enforcement and regulators.

You may consider contacting your local CERT.

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.

LESSON LEARNED

OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

Report

A crisis report should be written and made available to all of the actors of the crisis management cell.

The following themes should be described:

- Initial cause of the infection
- Actions and timelines of every important event
- What went right
- What went wrong
- Incident cost
- Indicators of compromise

Capitalize

Consider what preparation steps you could have taken to respond to the incident faster or more efficiently.

- Update your contacts-lists and add notes as to what is the most effective way to contact each involved party.
- Consider what relationships inside and outside your organization could help you with future incidents.
- Collaborate with legal teams if a legal action is required.

RANSOMWARE

Guidelines to handle and respond to ransomware infection

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

A good knowledge of:

- The usual operating systems security policies is needed.
- The usual users' profile policies is needed.
- Architecture, VLAN segmentation and interconnexions:
  - Have the capability to isolate entities, regions, partners or Internet.

Ensure that the endpoint and perimetric (email gateway, proxy caches) security products are up to date.

Deploy an EDR solution on endpoints and servers:

- This tool became one of the cornerstones of the incident response in case of ransomware or in large scale compromise, facilitating identification, containment and remediation phases.
- Launch EDR Search and AV scan with IOC explicit rules and get first indicators for remediation progress following.
- Set your EDR policies in prevent mode.

Since this threat is often detected by end-users, raise your IT support awareness regarding the ransomware threat.

Block IOCs linked to ransomware activities gathered by Threat Intelligence.

Deploy and operate security solutions enabling detection and facilitating response:

- Log gathering in a SIEM
- Have the capacity to run tools like YARA or DFIR-ORC (ANSSI)

Have a good log retention and verbosity

Define a strict posture versus the attacker

Prepare internal and external communication strategy

If a machine is identified with ransomware, unplug it from network and keep it turned on for memory forensics investigation

BACKUPS PREPARATION: Make sure to have exhaustive, recent and reliable backups of local and network users' data.

You can follow the 3-2-1 backup rules: each of these rules is meant to make sure that your data is stored in multiple ways.

So, if you're backing something up, you would have:

- At least three copies: three different copies mean three different copies in different places. By keeping them on different places, it reduces risk of a single event destroying multiple copies.
- In two different formats: this means that you must use at least two different methods to store your data. For example, DVD, Hard drive, Cloud services are different formats. But if you store two copies into two hard drive, here you will just use one format.
- With one of those copies off- site: Keeping one copy off-site ensures that even whatever happen where your data is (fire, break-in, natural disaster...) at least one copy is safe somewhere else. In this rule, cloud services make sense.

Try to use one backup format stored out of your network: even lateral movement happens from the threat that harm your network with encryption one copy will be out of reach.

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:

- Monitoring of ransomware IOCs by a SOC.
- Supervision of EDR alerts.
- 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.
- Publication of information on the ransomware operator websites or forums.
- Lateral movement is usually done, check all connection to the AD and ShareFile server with privileged accounts at abnormal day time.
- Look for unusual network or web browsing activities; especially connections to Tor I2P IP, Tor gateways (tor2web, etc.) or Bitcoin payment websites.
- Look for rare connections.

Scoping of the incident:

- EDR or large-scale hunting tools like YARA or DFIR-ORC allows to make the scoping of the ransomware infected machines.
- The identification of the initial access and the pivot used by the attackers is the priority, as in Large scale malware compromise. This allows to establish the following phases actions.

The identification of the Threat Actor at the origin of the ransomware attack could help the following phases based on known TTPs.

Ransomware network compromise identification have many similarities with Large scale malware compromise. Most of the time, reaction decision must be taken faster in ransomware cases. For more details about Large scale malware compromise, please refer to IRM-18.

CONTAINMENT
OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

- Make a public statement as soon as possible based on the communication template elaborated in the preparation phase.
- Follow the posture defined in the preparation phase.
- Send the undetected samples to your endpoint security provider and/or private sandboxes.
- Send the uncategorized malicious URL, domain names and IP to your perimetric security provider.
- Block traffic to C2s.
- Block any IP detected as used by attackers.
- Isolate compromised VLAN, interconnexion, entities, regions, partners or Internet.
- Disable accounts compromised/created by attackers.
- Disconnect all computers that have been detected as compromised from the network.
  - You could isolate with our EDR and shut down internet just keeping your EDR connections up.
- If you cannot isolate computers, disconnect/cancel the shared drives.
  - (NET USE x: \\unc\path\ /DELETE)

Monitor ransomware threat actor websites and Internet to find if there is any dataleak publication related to the ransomware compromise.

REMEDIATION
OBJECTIVE: TAKE ACTIONS TO REMOVE THE THREAT AND AVOID FUTURE INCIDENTS.

- Remove the initial access used by the attacker.
- Remove binaries used by the attacker to lateralize on the network.
- Remove any accounts created by attackers.
- Go back configuration changes.
- Operate a systems and network configuration hardening.

RECOVERY
OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS

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.

Prioritize your recovery plan based on your DRP (disaster recovery plan).
All of these steps shall be made in a step-by-step manner and with technical monitoring.

- Verify that backups are not compromised: only restore from a backup if you are very confident that the backup and the device you are connecting it to are clean.

OR

- Reimage the computer with a clean install.
- Reset credentials including passwords (especially for administrator and other system accounts).

Monitor network traffic to identify if any infection remains.

If possible, apply geo-filtering on firewalls to block illegitimate foreign country traffic.

Maintain the monitoring ransomware threat actor websites and Internet to find if there is any data leak publication related to the ransomware compromise.

LESSONS LEARNED

OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES

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

The following themes should be described:

- Initial cause of the infection
- Actions and timelines of every important event
- What went right
- What went wrong
- Incident cost
- Indicators of compromise

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

LARGE SCALE COMPROMISE

Guidelines to handle and respond to large scale compromise

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

- Deploy an EDR solution on endpoints and servers:
  - This tool became one of the cornerstones of the incident response in case of ransomware or in large scale compromise, facilitating identification, containment, and remediation phases
  - Launch EDR Search and AV scan with IOC explicit rules and get first indicators for remediation progress following
  - Set your EDR policies in prevent mode
- Block IOCs linked to malware activities gathered by Threat Intelligence.
- Deploy and operate security solutions enabling detection and facilitating response:
  - Log gathering in a SIEM
  - Have the capacity to run tools like YARA or DFIR-ORC (ANSSI) (https://github.com/dfir-orc)
- Have a good log retention and verbosity.
- Define a strict posture versus the attacker.
- Prepare internal and external communication strategy.
- Have a process to define a posture as soon as the compromise is detected: discreet or fast reaction.

Be prepared to notify abuse teams and law enforcement services and regulators if required during an incident (cell crisis management).

Endpoint

- 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 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.
- Make sure all equipment get setting on same NTP.
- Select what kind of files can be lost / stolen and restrict the access for confidential files.
- Make sure that analysis tools are up, functional (Antivirus, EDR, IDS, logs analyzers), not compromised, and up to date.

PREPARATION

Network

A good knowledge of architecture, VLAN segmentation and interconnexions:

- Have the capability to isolate entities, regions, partners, or Internet.
  - 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, Wi-Fi, Modem, …) regularly and close them.
- Ensure that traffic management tools and processes are operational.
- 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.

Baseline traffic

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

IDENTIFICATION

OBJECTIVE: DETECT THE INCIDENT, DETERMINE ITS SCOPE, AND INVOLVE THE APPROPRIATE PARTIES.

You may need to notify abuse teams and law enforcement services and regulators at the beginning of this step if required.

Detection

- Monitoring of IOCs "from Threat intelligence" by SOC.
- Supervision of Antivirus, EDR, SIEM, IDS alerts and logs.
- Odd professional emails (often masquerading as invoices) containing attachments are being received.
- Lateral movement is usually done, check all connection to the AD and ShareFile server with privileged accounts at abnormal day time.
- High number of accounts locked.
- Look for unusual network or web browsing activities; especially connections to Tor I2P IP, Tor gateways (tor2web, etc) or Bitcoin payment websites.
- Look for rare connections.

If a machine is identified with a malware, unplug it from network and keep it turned on for memory forensics investigation .

Scoping of the incident

- Use EDR, endpoint logs, system logs, tools allowing at scale IOC search.
- Identify pivoting techniques on the network.
- Review statistics and logs of network devices.
- Identify malicious usage of compromised accounts.
- Identify Command and control servers in firewall logs, proxy logs, IDS logs, system logs, EDR, DNS logs, NetFlow and router logs.

IDENTIFICATION

Find initial vector of compromise

- Investigate exposed assets (especially those who are not up to date).
- Verify the presence of binaries in user profiles, %ALLUSERSPROFILE% or %APPDATA% and %SystemDrive%.

The identification of the Threat Actor at the origin of the attack could help the following phases based on known TTPs

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. Keep your backup safe and disconnected from compromised scope.

CONTAINMENT

OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

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

- Make sure that all footholds of the attackers have been identified before taking containment measure
- Be discrete if necessary and possible

2. If applicable to the attack:

- Isolate compromised VLAN, interconnexion, entities, regions, partners, or Internet
- Disconnect all computers that have been detected as compromised from the network

You could isolate with your EDR and shut down internet just keeping your EDR connections up.

- Block traffic to C2s
- Block any IP detected as used by attackers
- Disable accounts compromised/created by attackers
- Send the undetected samples to your endpoint security provider and/or private sandboxes
- Send the uncategorized malicious URL, domain names and IP to your perimetric security provider

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
- DNS sinkhole
- Stop Sharefile services
- Terminate unwanted connections or processes on affected machines

CONTAINMENT

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/EDR console, server logs, support calls):

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
- 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

REMEDIATION

OBJECTIVE: TAKE ACTIONS TO REMOVE THE THREAT AND AVOID FUTURE INCIDENTS.

Endpoint

- Reinitialize all accesses to the accounts involved in the incident
- Remove any accounts created by attackers
- Remove the initial access used by the attacker
- Remove binaries used by the attacker to lateralize on the network
- Remove persistence
- Change password of compromised accounts
- Go back configuration changes
- Operate a system hardening

Network

- 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
- Check if security configuration is untouched: GPO, AV, EDR, Patch…
- Operate network configuration hardening

If the source has been identified as an external offender, consider involving abuse teams and law enforcement services and regulators if required.

RECOVERY

OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.
Prioritize your recovery plan based on your DRP (disaster recovery plan).
All the following steps shall be made in a step-by-step manner and with technical monitoring.

Endpoint
Ensure that no malicious binaries are present on the systems before reconnecting them

- Best practice is to reinstall compromised system fully from original media
- Apply all fixes to the newly installed system
- If this solution is not applicable:
  - Restore any altered files
  - Change all passwords (with a strong password policy)

Network

1. Ensure that the network traffic is back to normal (secured)
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

Monitor network traffic to identify if any infection remains.

If possible, apply geo-filtering on firewalls to block illegitimate foreign country traffic.

LESSONS LEARNED

OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

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

The following themes should be described:

- Initial cause of the infection
- Actions and timelines of every important event
- What went right
- What went wrong
- Incident cost
- Indicators of compromise

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