INCIDENT RESPONSE METHODOLOGY

IRM #18
LARGE SCALE COMPROMISE

Guidelines to handle and respond to large scale compromise

IRM Author: CERT SG
Contributor: CERT aDvens
IRM version: 2.0
E-Mail: cert.sg@socgen.com
Web: https://cert.societegenerale.com
Twitter: @CertSG

C'EST VOUS L'AVENIR

SOCIETE GENERALE

ABSTRACT

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

WHO SHOULD USE IRM SHEETS?

- Administrators
- Security Operation Center
- CISOs and deputies
- CERTs (Computer Emergency Response Team)

Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident Response team or CERT immediately if needed.

→ IRM CERT SG: https://github.com/certsocietegenerale/IRM

→ IRM CERT aDvens (French version): https://github.com/cert-advens/IRM

INCIDENT HANDLING STEPS

6 STEPS ARE DEFINED TO HANDLE SECURITY INCIDENTS

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 a normal stage
6. Lessons learned: draw up and improve the process

IRM provides detailed information for each step of the incident response process. The steps come from NIST Computer Security Incident Handling Guide.

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.

Remediation steps from IRM-2 and IRM-3 can also be useful.

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.