INCIDENT RESPONSE METHODOLOGY

IRM #5 MALICIOUS NETWORK BEHAVIOUR

Guidelines to handle a suspicious network activity

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

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.

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.

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

→ IRM CERT aDvens (French version): https://github.com/certadvens/IRM

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) in order 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.

For more details on authentication and infrastructure recovery, check the Large-scale malware compromise IRMXXX

LESSONS 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.