INCIDENT RESPONSE METHODOLOGY

IRM #2
WINDOWS
INTRUSION
DETECTION

Live Analysis on a suspicious
Windows system

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.

References:

→ **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.

▪ 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 usecase.

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

Most of the above guidance is inspired by SANS Institute posters: https://www.sans.org/posters
It's always better to run several of these tools than only one.

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

Most of the above guidance is inspired by SANS Institute posters: https://www.sans.org/posters
It's always better to run several of these tools than only one.

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, as long as 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.

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

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.