INCIDENT RESPONSE PLAYBOOK

IRP #7 MALWARE DETECTION

Guidelines to Handle Malware Incident.

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 malicious actor 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 purposes. In some circumstances 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. Metadata describing the typical network activity should be kept to enable efficient comparison with 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 SME for assistance, when applicable. A good idea is also to have a map of standard services and/or running processes of the asset.

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 System Support teams.
- Make sure that an alert notification process is defined and well-know.
- Make sure all equipment is synchronized with the same NTP server.
- Make sure that analysis tools are up and 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.

Detect the infection.

Information coming from several sources should be gathered and analysed:

- 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.

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.

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

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

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.

During this phase, the objective is to minimize the blast radius of the attack within an organization's network. Usually this takes place at the endpoint level, leveraging an EDR.

If the machine is considered critical for your company's business activity and can't be disconnected, backup all important data in case the malicious actor notices you're investigating and starts deleting files.

Below are some examples of actions that can be taken in response to malware-related detections such as "Suspicious File Downloaded" and "Malware Executed" (or equivalent ones):

Suspicious File Downloaded:

- **Initiate host scan**: initiates an on-demand scan of the specified host
- **Quarantine file**: moves the suspicious file into quarantine on the affected host.

Malware Executed:

- **Isolate host via EDR**: isolate the affected device from the network to prevent further communication with malicious actors.
- **Stop process and ban hash**: Adds the specified hash to global ban list(s) to stop current processes and prevent further execution on the network.
- **Reset User Credentials**: Reset credentials of the affected user to prevent further access to the Environment.

- 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.

Once the machine is isolated and the initial threat has been contained, the investigative phase seeks to understand the full scope of the potential incident.

Query to Automate	Insight	Typical Data Source
What are the indicators of compromise (IOCs) associated with this malware incident?	IOCs, such as file name and file hash, are run against threat intel to identify malicious activity.	Endpoint detection and response (EDR), threat intelligence
What are the Indicators of Attack (IOAs) associated with this malware incident?	IOAs look for common tactics and techniques such as execution, persistence, and lateral movement. Particularly useful in detecting file-less malware.	User activity monitoring, EDR, security information and event management (SIEM)
What is the behaviour and purpose of the malware?	Using a sandbox environment for dynamic analysis helps to uncover the true purpose of the suspicious file.	Sandbox
Where did the malware originate from?	Identifying the source of the malware reveals the attack timeline and potential scope.	Network perimeter (e.g., firewall, proxy, etc.), email gateway, SIEM

Where else may the malware have spread?	It's critical to identify whether this is a widespread threat or a targeted attack on a single machine.	SIEM, EDR

For more details, check the **Windows and Linux intrusion IRP-2 and IRP-3**

ERADICATION

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.

If not feasible then proceed with the following steps:

- 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.
- Terminate user session and force password reset for the affected user account(s).
- 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.

For more details on authentication and infrastructure recovery, check the Large-scale malware compromise IRP-18

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 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.