INCIDENT RESPONSE PLAYBOOK

IRP #17 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.

ERADICATION

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.

For more details, check the Large-scale malware compromise IRP-18

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.