LetsDefend

Malware Playbook

letsdefend.io

START

Verify

Alarms escalated from Tier1 to Tier2 should be caused by a truly harmful event, but escalated alarms by Tier1 analysts are not always True Positive due to technical inadequacy, faulty/incomplete analysis, and authorization problems.

Before initiating Incident Response processes, please verify that the alarm from the Tier1 analyst was caused by malicious activity.

Connect to the Machine

Find the device in the alarm details on the 'Endpoint Security' page and access the device with the help of the 'Connect' button if it is necessary.

Analyze Malware

Analyze malware in third party tools and find C2 address.

You can use the free products/services below.
- AnyRun
- VirusTotal
- HybridAnalysis

Is the file malicious?

Malicious

Malware Type

What is the malware type?
- Trojan
- Spyware
- Adware
- Rootkit
- Ransomware
- Worm
- Keylogger

What is the Initial Access Method Used in the Attack?

It is very important to determine the technique used by the attacker in the "Initial Access" tactic in order to determine the root cause, make the systems more secure and not repeat the same incident again. Please choose the correct initial access method that used in the attack.

-External remote services, -Phishing, -Supply Chain Compromise, -Valid Accounts, -Drive-by Compromise

Define Scope

Have you seen IOCs on more than one machine?

NO

YES

Malware Spread

How did the malware spread?

-Internal/external phishing
-Malicious websites
-Shared networks
-Other

Check if the Malware is Quarantined/ Cleaned

Log management
endpoint security
Malware quarantined/cleaned?

Has the Malware Been Executed on the Device?

Please examine the alert details and the logs on the device to determine whether the malware is successfully executed on the system.

Choose "Yes" if malware was successfully executed on the system.

NO

YES

Which Technique(s) Was Used As An Execution Tactic?

-Command and Scripting Interpreter
-Exploitation for Client Execution
-Scheduled Task/Job
-Serverless Execution
-User Execution
-Windows Management Instrumentation

Check If Someone Requested the C2

Please go to the "Log Management" page and check if the C2 address accessed. You can check if the malicious file is run by searching the C2 addresses of the malicious file. Please click "Accessed" if someone access the malicious address.

Does the device need the be isolated?

Containment

Systems exposed to cyber attack should be isolated and the effect of cyber attack should be reduced.

Backup Evidences

Before starting the eradication process, the evidence on the system must be transferred to a secure environment. Please move the evidence on the system to a secure environment.

Eradication

Go to Endpoint Security and connect to the machine. Then, destroy any malicious file, user or other suspicious artifact that needs to be destroyed.

Recovery

Recovery phase is restoring all affected systems and devices to allow for normal operations to continue. Playbook's 'Recovery' task has been created to teach the stages of incident response. Recovery will not be performed.

Lesson Learned

- How did the cyber attack happen?
- How well did staff and management perform in dealing with the incident?
- What would the staff and management do differently the next time a similar incident occurs?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?

Artifacts

Take notes about finded artifacts during the investigation

Analyst Note

Please enter your analysis comments.

END

LetsDefend