Attack Lifecycle Detection of an Operational Technology Breach

paraflare.com/attack-lifecycle-detection-of-an-operational-technology-breach/

Melanie Ninovic

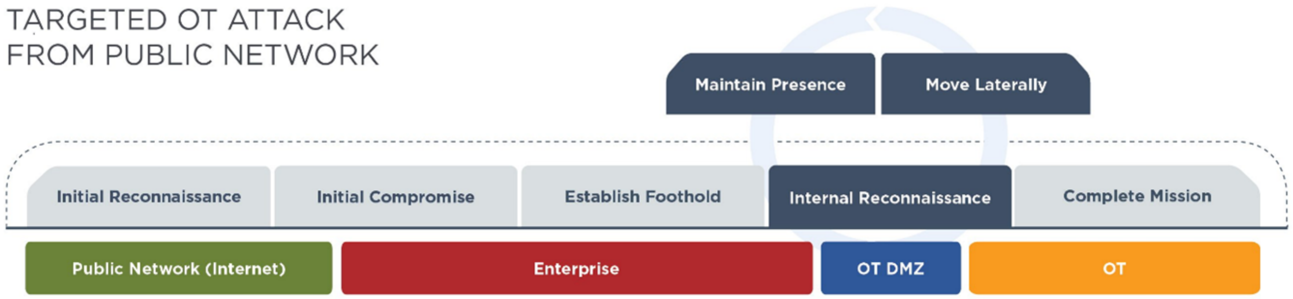
Melanie Ninovic
Digital Forensics & Incident Response Consultant at ParaFlare
Dec 6, 2021
5 min read.

FireEye Mandiant released a red teaming case study in April 2021 that explores the tactics, techniques, and procedures (TTPs) used to penetrate an information technology (IT) network and ultimately gain access to the operational technology (OT) network. ParaFlare is expanding on this research to provide useful detection and response methods to those responsible for securing a technology-enabled environment.

Regardless of whether your organisation deals with OT or not, the detections explored within this article relate to commonly found tools or techniques used against an IT environment, such as phishing emails, Remote Desktop Protocol (RDP), mimikatz, and Cobalt Strike. Threat actors with clear motives will live off the land and use already existing tools, or those that are publicly available, to further compromise a network whether it be in the IT or OT space.

Attack Lifecycle

In FireEye Mandiant's case study, the following graphic was provided to demonstrate what phases of the attack lifecycle are conducted in which part of an organisation's network. There is a clear path to the OT environment, but this requires a series of successfully executed activities before completing their mission; all of which is detectable within your IT environment.



Credit: https://www.fireeye.com/blog/threat-research/2021/04/hacking-operational-technology-for-defense-lessons-learned.html

Detections

ParaFlare's operations team has dissected the case study's lifecycle into useful detections that we are using to protect our customers, and provide a head start for organisations who are susceptible to similar breaches. This will mostly look at endpoint and network signatures that we can detect from the IT side of the environment, as these will not, due to their nature, generally be available in OT infrastructure.

1. Initial compromise

In this case study, one set of emails contained an embedded link to a malicious file hosted on the internet, and the other had a malicious file attached to the email. Detection strategies include:

- Endpoint Detection and Response (EDR) and Anti-Virus signature and behavioural alerts for downloading a malicious document, clicking a malicious link, and the activity that followed.
- Network Detection. If your organisation is capturing network traffic via Zeek, files.log will be able to detect any files being downloaded with common phishing extensions like .docx, .pdf etc. The Zeek http.log will also capture important data on files traversing the network, such as 'resp_filenames' and 'resp_mime_types'.

Proxy logs will be able to show:

- HTTP GET request to the malicious link that was embedded in the email.
- HTTP GET request to the malicious document downloaded to the victim's machine.
- MIME or content types can be filtered to those commonly used for phishing campaigns like 'application/zip', 'application/pdf', 'application/msword', and 'application/vnd.openxmlformats/%'.

2. Establish foothold

The red team used Cobalt Strike's Command and Control (C2) protocol to establish their foothold. We can detect this by:

- monitoring 'ESTABLISHED' connections to remote IP addresses to detect C2 beaconing.
- monitoring HTTP POST requests to remote IP addresses with encrypted binary blobs; this generally includes information about the compromised host such as its hostname.
- looking for base64 encoded code within HTTP GET and POST requests, in the 'data' field.

3. Internal reconnaissance

ldapsearch was used to enumerate information in the enterprise domain. This is a Linux based tool that would be difficult to detect unless you are monitoring processes or bash history.

Monitoring Linux processes can be done via top, ps -aux, lsof, and netstat.

Active and passive port scanning was conducted to further understand the enterprise network and determine any communication paths to the OT environment.

- Monitoring or detecting port scans are often difficult as they usually rely on the ICMP protocol. However, a network IDS like Snort has inbuilt signatures to detect this type of activity, especially if the threat actor is using publicly accessible tools such as nmap.
- For initial reconnaissance from the external network, nmap would show up in HTTP logs with ‘nmap’ in the user agent string.

Keystroke logging via Cobalt Strike’s C2 was also used to gather information relating to hostnames, IP addresses, usernames, and passwords to internal systems within the organisation. This type of reconnaissance later enabled a remote desktop session to the OT network.

- Keyloggers can be found by monitoring the running processes on the host.
- Established and listening network connections should also be monitored as the logs would be sent to a remote IP address controlled by the threat actor.

4. Persistence
Mimikatz was used to extract credentials for local user accounts and those of the domain administrators. As threat actors know mimikatz.exe will create P1 alerts, they often change the name of the binary. Therefore, ParaFlare recommends using command line parameters to detect mimikatz execution:

- mimikatz.exe “log log.txt” “privilege::debug” “sekurlsa::logonpasswords” “exit”
- The parameter ‘sekurlsa’ is more difficult to change, so having a rule for this string would be more effective to detect this activity
- If you are capturing System.evtx, you will be able to detect the new service that Mimikatz will create by monitoring EID 7045, and EID 7040 will log the start and stop of that service.

PowerSploit, based off PowerShell was used in this case study to exploit common security misconfigurations. It has many other features, but they all mostly rely on PowerShell’s script block.

- Script Block Logging is logged under EID 4104 in the ‘Windows PowerShell’ event log. It will also be captured in the Security event log under EID 4688 (new process creation).
- In the case of DLL injections, one of the PowerSploit modules, you can detect this by alerting on processes that spawn rundll32.exe. This is made easier if you have Process Tracking audit events enabled to log each new process creation.

5. Lateral movement
WMImplant was used to move laterally from one system to another in the internal IT network.

- Enable event log Microsoft-Windows-WMI-Activity/Operational.
- Monitor and alert on EID 5861 (WMI) and EID 4104 (Script Block Logging).
- Monitor for WMIPrvSe.exe process creation as this is required for WMI-based tools to execute.

SMB was utilised to move from the patch management server in the DMZ to the Windows-based intermediary systems in the OT network.

> Set up alerting for ‘ESTABLISHED’ network connections from one internal IP address to another. This can be done through Sysmon, Zeek, or other network monitoring tools.

Response

ParaFlare’s DFIR team has written some queries (based off OSQuery) to assist organisations in their own threat hunting capabilities. Additionally, we explore some event logs and other forensic artifacts requiring analysis to identify malicious activity relating to this case study.

1. Initial compromise
Event logs can be examined to identify any Microsoft Office files that contained embedded macros from a phishing attempt:

> C:\Windows\System32\winevt\Logs\OAlerts.evtx will display informational alerts from Microsoft Office files. These are the pop ups that are displayed whilst using Microsoft Office files, like ‘Save As’, ‘this workbook contains links to one or more external sources’, and ‘Start application CMD.EXE’. Search within this event log for keywords such as cmd, powershell, or the term ‘macro’.

Web browser history, looking for a malicious document download or accessing a malicious link:

- Chrome: C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\History
- Firefox: C:\Users\<username>\Appplication Data\Mozilla\Firefox\Profiles\places.sqlite
- Internet Explorer: C:\Users\<username>\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

For executed programs and opened files per user, analyse C:\Users\<username>\NTUSER.DAT:

- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

2. Establish foothold
To detect Cobalt Strike, we can look at network connections and sockets via OSQuery:

- ```SELECT processes.name, processes.path, processes.cmdline, listening_ports.address, llistening_ports.pid, listening_ports.port, listening_ports.protocol FROM listening_ports JOIN processes ON listening_ports.pid = processes.pid WHERE listening_ports.address = “0.0.0.0”;```
- ```SELECT sockets.pid, processes.name, sockets.path, sockets.remote_address, sockets.remote_port, sockets.state FROM process_open_sockets sockets JOIN processes ON sockets.pid = processes.pid WHERE sockets.remote_port NOT LIKE ‘0’ ORDER BY sockets.remote_port ASC;```

3. Persistence
For mimikatz to run successfully, the threat actor will need to enable WDigest. We can determine this via OSQuery, since we know it is enabled if the data field is set to 1:

> ```SELECT * FROM registry WHERE path = ‘HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential’ AND data = 1;```

Mimikatz will also have to install a service. Using OSQuery, list all automatically executing services:

> ```SELECT name, display_name, status, path, user_account FROM services WHERE start_type = “AUTO_START” AND path NOT LIKE “%System32\svchost.exe%”;```

4. Lateral movement
SMB activity can be detected via OSQuery by looking at processes and open pipes:

> ```SELECT proc.path as processPath, proc.pid, proc.parent as ppid, proc.cwd as currentWorkingDirectory, pipe.pid as pipePid, pipe.name AS pipename FROM processes proc JOIN pipes pipe ON proc.pid=pipe.pid;```

WMImplant activity can be identified via OSQuery’s multiple WMI based tables:

- ```SELECT name, query, relative_path FROM wmi_event_filters WHERE name NOT LIKE 'SCM%';```
- ```SELECT * FROM wmi_filter_consumer_binding WHERE consumer NOT LIKE '%SCM%';```
- ```SELECT name, scripting_engine, script_file_name, class, relative_path FROM wmi_script_event_consumers;```

Other recommendations

ParaFlare recognises that simple lapses in security may have dire consequences later down the track. Here are some instances of this from FireEye Mandiant's report:

- Operational manuals with plaintext usernames and passwords provide easy access for any threat actor looking for this information. We recommend at minimum to encrypt this material, but further to the point, not displaying plaintext credentials in any document.
- Disable macros within the Microsoft Office suite for files that have been received from the Internet.
- Sensitive documents including OT system and network designs should only be accessible to those who require access. This is known as the principle of least privilege. More to this, these types of documents should be password protected. Ensure logging is enabled and monitored. This should include:
  - PowerShell's v5 Script Block Logging to allow for alerting on new commands being executed within the environment. This can be done through the Group Policy by going to Administrative Templates -> Windows Components -> Windows PowerShell -> Turn on PowerShell Script Block Logging. EID 4103 and 4104 to inspect script blocks.
  - Security event log captures new process creation, which analysts can use to detect malicious scripts and command line arguments by examining EID 4688. To enable this in Group Policy: Security Settings -> Audit Policy -> Audit Process Tracking.
  - Microsoft-Windows-WMI-Activity/Operational: EID 5857 shows wmiprvse execution and path to provider DLL's.

References

For more information on this case study, please visit the following link:
FireEye Mandiant Research: https://www.fireeye.com/blog/threat-research/2021/04/hacking-operational-technology-for-defense-lessons-learned.html

ParaFlare is here to support our customers, new or existing, with the content within this article and any other queries you may have. Please reach out to us if you have any questions.

Have a comment? Join the conversation on LinkedIn