

Real time Soc Simulation lab 2

The Scenario

A sales employee, straying from their role, falls victim to a malvertising trap while searching for a printer driver. This misstep downloads malware disguised as a legitimate driver, triggering a network-wide compromise through privilege escalation and lateral movement. Can you trace the attack chain and secure the network before it is too late?

Scenario objectives

- Monitor and analyze alerts generated by the malware activity, including suspicious network connections and process executions.
- Trace the attack chain from the initial malvertising compromise to the malware's lateral movement across the network.
- Identify key indicators of compromise (IOCs), such as malicious file downloads and C2 communications.

Alert 1

Description:	A network connection to a domain resembling a legitimate one (potential typo-squatting) was detected. Further investigation is recommended to determine the legitimacy of the activity.
datasource:	firewall
timestamp:	24/01/2025 20:50:29.288
Action:	blocked
SourceIP:	10.1.3.129
SourcePort:	37453
DestinationIP:	
DestinationPort:	80
URL:	http://www.googl.com
Application:	web-browsing
Protocol:	TCP
Rule:	Block-Phishing-Sites

typosquatting is a form of cyberattack and cybersquatting where malicious actors register domain names that are like legitimate ones, often with slight typographical errors. The goal is to exploit common typing mistakes made by users when entering URLs or

searching for websites and is often used for phishing, malware distribution, or ad fraud.

1. *Who*

- Source: User on internal host with IP `10.1.3.129`
- Destination: External host at IP `178.92.53.38`
- User/Process: User manually typed the URL.

2. *When*

- Timestamp of First Alert: 24 January 2025, 21:50
- Timestamp of Second Alert: 24 January 2025, 21:52

3. *What*

- Incident Description:
- The first alert was triggered by a mistyped URL (`googl.com`), which was flagged by the system as a potential typosquatting attack. As a result, the connection was blocked.
- The user corrected the URL two minutes later, typing the valid address `google.com`. This connection attempt was not flagged.

4. *Where*

- Source IP: `10.1.3.129` (Internal Network)
- Destination IP: `178.92.53.38` (External Host)
- Application: Web-browsing (via TCP)
- Rule Applied: Allow-Internet (For successful web connection to google.com)

5. *Why*

- **Why did the alert trigger?** — The first alert was caused by a mistyped URL (`googl.com`), which our system flagged as a possible ****typosquatting attack**** due to the similarity to a well-known domain (google.com).
- **Why was the action taken?** — The system blocked the action to protect against potential malicious typosquatting, which involves creating look-alike domains to deceive users into visiting fake websites for phishing or malware distribution.
- **Why was the second connection allowed?** — The user correctly typed `google.com`, which is a legitimate URL, and the connection was allowed by the firewall rule `Allow-Internet`.
- **Why was this a false positive?** — The misinterpretation occurred because of a harmless typo, which led to the system flagging the connection. After the correction, no suspicious activity was detected.

Next Steps

Recommendation — No further action is needed for this case as it was a false positive. However, it's recommended to fine-tune the typosquatting detection system to minimize future misflags.

Preventive Measures — Review and possibly adjust URL filtering thresholds to reduce the likelihood of false positives while maintaining security.

Alert 2

3410	Suspicious Network Connection to Known Malicious IP	Medium	Network	Jan 24th 2025 at 21:55	Closed
Description:	A network connection to a suspicious IP address was detected. Further investigation is recommended to determine the legitimacy and intent of this connection.				
datasource:	firewall				
timestamp:	24/01/2025 20:55:23.288				
Action:	allowed				
SourceIP:	10.1.3.129				
SourcePort:	79733				
DestinationIP:	178.92.53.38				
DestinationPort:	80				
URL:	https://www.beanie-print-driver.thm				
Application:	web-browsing				
Protocol:	TCP				
Rule:	Allow-Internet				

The source IP 10.1.3.129 associated with the user liam.espinosa searched for a beanie driver using the Google Engine which search then ended with the user visiting <https://beanie-print-driver.thm> with IP address of 178.92.53.38, which is a known malicious IP address. Looking from the logs, we only find one log connected to this IP destination address at the time of 24/01/2025 20:55:23.288.

Alert 3

3411	Suspicious Network Connection to Known Malicious IP	Medium	Network	Jan 24th 2025 at 22:03	
Description:	A network connection to a suspicious IP address was detected. Further investigation is recommended to determine the legitimacy and intent of this connection.				
datasource:	firewall				
timestamp:	24/01/2025 21:03:29.288				
Action:	allowed				
SourceIP:	10.1.3.129				
SourcePort:	50432				
DestinationIP:	178.92.220.140				
DestinationPort:	8090				
URL:					
Application:	unknown-tcp				
Protocol:	TCP				
Rule:	Allow-Internet				

The third alert arrives at 24/01/2025 21:03:29.288. Taking the timestamp when this occurred, let's search for events that happened immediately after in SIEM.

Immediately after there is a beanie-printerdriver.exe file downloaded to the user liam.espinoza Downloads folder. This is the exact location C:\Users\LiamEspinoza\Downloads\Beanie-PrintDriver.exe. In Splunk we are conducting an additional search now to understand the actions that are taking place on the machine under this username — `*| spath User | search User="TRYHATME\\liam.espinoza"`.

```
> 1/24/25 9:03:29.000 PM [ [-]
Computer: win-3454
EventID: 11
Hashes: SHA256-9dd4bd43f696022d10977d7198ca4bde98bcc0b3d47159d8223ef158c0e8acb5
Image: C:\Program Files\Google\Chrome\Application\chrome.exe
ProcessGuid: {d4e62d57-0c12-489b-b3e6-d5ad82e982b9}
ProcessId: 4523
TargetFilename: C:\Users\LiamEspinoza\Downloads\Beanie-PrintDriver.exe
User: TRYHATME\liam.espinoza
datasource: sysmon
timestamp: 01/24/2025 21:03:30.158
}
Show as raw text
User = TRYHATME\liam.espinoza host = 10.10.247.166:8989 source = eventcollector sourcetype = _json
```

Waiting a few minutes and reviewing the logs from the machine we can see that at 1/24/25 9:14:21.000 PM, there was a command executed from liam.espinoza's machine, which tries to elevate privileges.

CommandLine: SharpUp.exe -AlwaysInstallElevated. This indicates attempts for privilege escalation.

These commands were registered:

CommandLine: SharpUp.exe -AlwaysInstallElevated

CommandLine: SharpUp.exe -CachedGPPPassword

CommandLine: SharpUp.exe -DomainGPPPassword

CommandLine: SharpUp.exe -ModifiableScheduledTask

CommandLine: SharpUp.exe -ModifiableServices

CurrentDirectory: C:\Users\LiamEspinoza\AppData\Local\Temp\ — the directory from which the commands are executed.

```
> 1/24/25 8:22:09.000 PM [-]
CommandLine: SharpUp.exe -DomainGPPPassword
Computer: win-3454
CurrentDirectory: C:\Users\LiamEspinoza\AppData\Local\Temp\
EventID: 1
Hashes: SHA256~47ef43fa9b502199ef9af0bc545681ddc1ef1a468d3498d858ee8e3cc57f67
Image: C:\Users\LiamEspinoza\AppData\Local\Temp\SharpUp.exe
ParentImage: C:\Users\LiamEspinoza\Downloads\Beanie-PrintDriver.exe
ParentProcessGuid: {eab81932-2848-4f77-a8ba-7e50d13420f5}
ParentProcessId: 5634
ProcessGuid: {6d5c1983-176a-af31-a5e1-96c889a86c47}
ProcessId: 6016
User: TRYHATME\Liam.espinoza
datasource: system
timestamp: 01/24/2025 20:22:10.147
}
Show as raw text
User = TRYHATME\Liam.espinoza host = 10.10.181.115:8989 source = eventcollector sourcetype = _json

> 1/24/25 8:21:49.000 PM [-]
CommandLine: SharpUp.exe -AlwaysInstallElevated
Computer: win-3454
CurrentDirectory: C:\Users\LiamEspinoza\AppData\Local\Temp\
EventID: 1
Hashes: SHA256~47ef43fa9b502199ef9af0bc545681ddc1ef1a468d3498d858ee8e3cc57f67
Image: C:\Users\LiamEspinoza\AppData\Local\Temp\SharpUp.exe
ParentImage: C:\Users\LiamEspinoza\Downloads\Beanie-PrintDriver.exe
ParentProcessGuid: {eab81932-2848-4f77-a8ba-7e50d13420f5}
ParentProcessId: 5634
ProcessGuid: {f83c4976-984a-8d63-a95e-68c77c04e56}
ProcessId: 6010
User: TRYHATME\Liam.espinoza
datasource: system
timestamp: 01/24/2025 20:21:50.083
}
Show as raw text
User = TRYHATME\Liam.espinoza host = 10.10.181.115:8989 source = eventcollector sourcetype = _json
```

Alert 4

We can see here that a Powershell command was executed.

Searching through the logs in Splunk this is what we see:

ParentCommandLine: powershell.exe -ExecutionPolicy Bypass -File “C:\Users\LiamEspinoza\Documents\InstallUpdates.ps1” — this temporarily allows the script to execute regardless of system policies.

This is the command executed — if (Test-Path ‘ITServe\Installers\CapItAll-Sales-Installer.exe’) { Start-Process ‘ITServe\Installers\CapItAll-Sales-Installer.exe’ } — it checks if a file exists at a given path and if yes, it executes it. The assumption is that this file is downloaded to the host when the malicious driver was installed on the targeted host and it allows for lateral movement.

```
1/24/25 9:21:33.000 PM { [-]
  CommandLine: \\ITServe\Installers\CapItAll-Sales-Installer.exe
  Computer: win-3454
  EventID: 1
  Hashes: SHA256*d3f2c60d36e1477d7a15f96bf1b5d209d93b52bfa2bd47268a6cf8c891def56b
  Image: \\ITServe\Installers\CapItAll-Sales-Installer.exe
  ParentCommandLine: powershell.exe -ExecutionPolicy Bypass -File "C:\Users\MiamEspinoza\Documents\InstallUpdates.ps1"
  ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
  ParentProcessGuid: {d8f7b214-7a4d-4b4c-b215-8f33b6e217a7}
  ParentProcessId: 6435
  ProcessGuid: {b3af9374-273c-48a5-bef9-c9b3728e5f12}
  ProcessId: 6521
  User: TRYHATME\miam.espinoza
  datasource: sysmon
  timestamp: 01/24/2025 21:21:34.055
}
Show as raw text
User = TRYHATME\miam.espinoza host = 10.10.247.166:8989 source = eventcollector sourcetype = _json
```

Several alerts appear afterwards:

The timeframe for the alerts is from Jan 24th 2025 at 22:28 to Jan 24th 2025 at 22:37. However now several users are infected, since now that same CapitAll-Sales-Installer.exe is being executed on several different hosts.

Hosts infected:

TRYHATME\kyra.flores

TRYHATME\miguel.odonnell

TRYHATME\cain.omoore

External tools to use in this scenario are encouraged and the way to do it is through the Analyst VM which is part of the Simulator where you can several analyst tools like Wireshark or TryDetectThis which is their tools= for file analysis and URL/IP security check.

If you successfully manage to resolve and find all the true positives, you eventually arrive at this point below.

