Home SOC Project

Summary

I built a basic log collection setup on my Windows laptop using Sysmon + Splunk, then created simple reports to review process activity, DNS lookups, and registry changes.

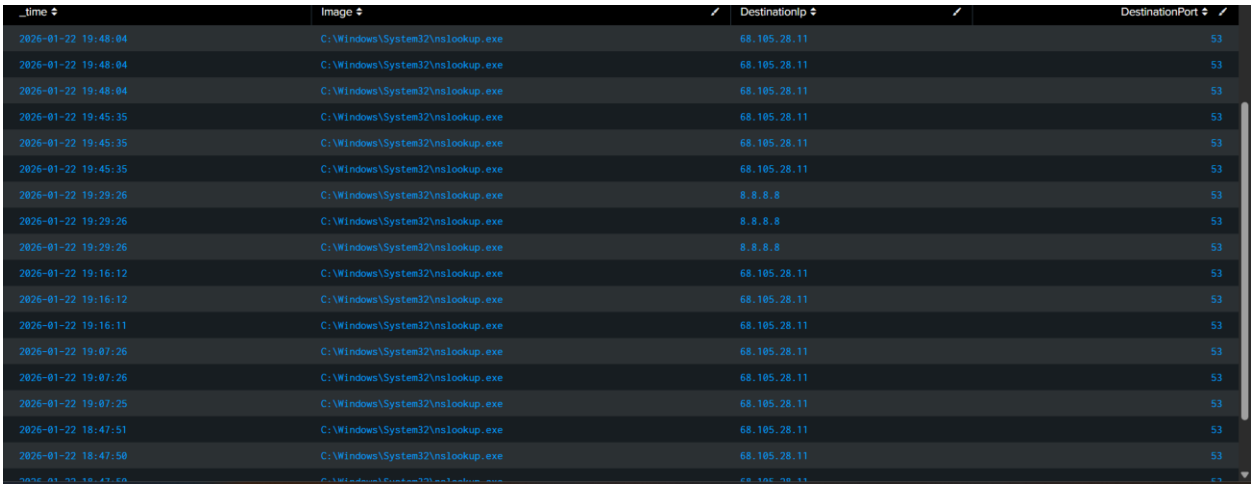
Goal

Get hands-on practice collecting logs and using Splunk to answer basic investigation questions like:

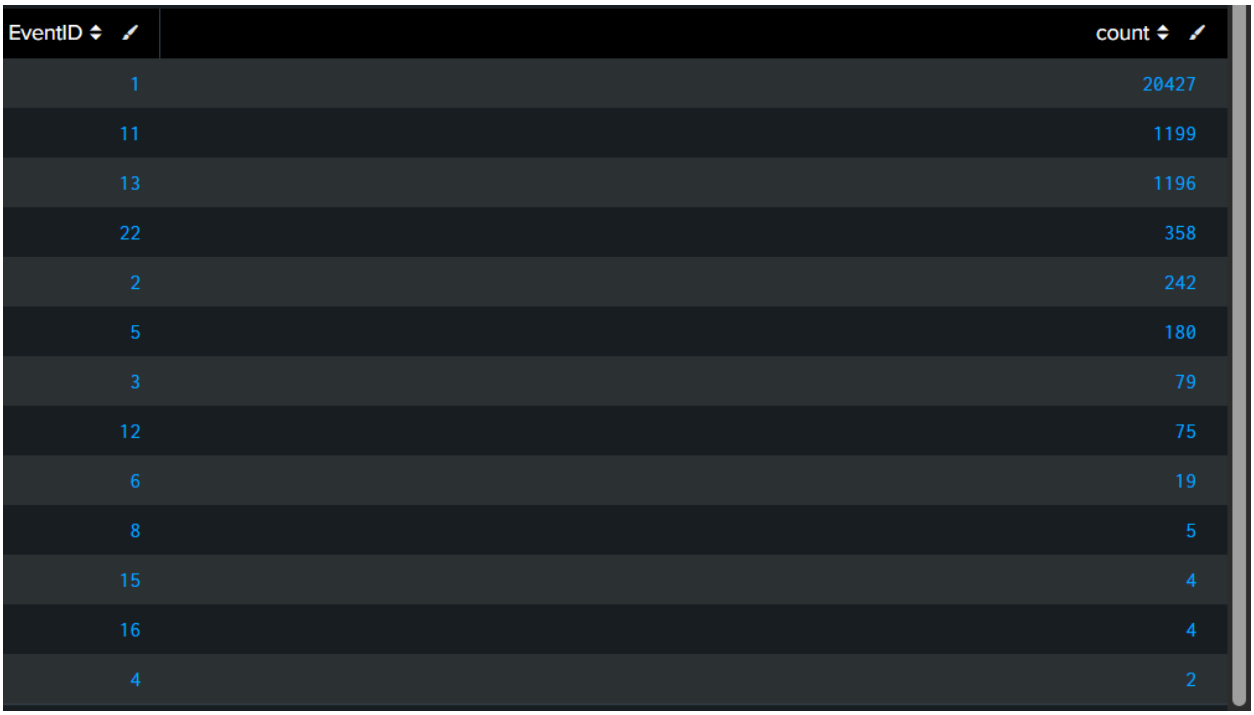
- What ran on the system?
- What domains were looked up?
- What registry settings were changed?

Tools used

- Windows 11
- Sysmon (Sysinternals)
- Splunk Enterprise (local install)



_time	Image	DestinationIp	DestinationPort
2026-01-22 19:48:04	C:\Windows\System32\nslookup.exe	68.105.28.11	53
2026-01-22 19:48:04	C:\Windows\System32\nslookup.exe	68.105.28.11	53
2026-01-22 19:48:04	C:\Windows\System32\nslookup.exe	68.105.28.11	53
2026-01-22 19:45:35	C:\Windows\System32\nslookup.exe	68.105.28.11	53
2026-01-22 19:45:35	C:\Windows\System32\nslookup.exe	68.105.28.11	53
2026-01-22 19:45:35	C:\Windows\System32\nslookup.exe	68.105.28.11	53
2026-01-22 19:29:26	C:\Windows\System32\nslookup.exe	8.8.8.8	53
2026-01-22 19:29:26	C:\Windows\System32\nslookup.exe	8.8.8.8	53
2026-01-22 19:29:26	C:\Windows\System32\nslookup.exe	8.8.8.8	53
2026-01-22 19:16:12	C:\Windows\System32\nslookup.exe	68.105.28.11	53
2026-01-22 19:16:12	C:\Windows\System32\nslookup.exe	68.105.28.11	53
2026-01-22 19:16:11	C:\Windows\System32\nslookup.exe	68.105.28.11	53
2026-01-22 19:07:26	C:\Windows\System32\nslookup.exe	68.105.28.11	53
2026-01-22 19:07:26	C:\Windows\System32\nslookup.exe	68.105.28.11	53
2026-01-22 19:07:25	C:\Windows\System32\nslookup.exe	68.105.28.11	53
2026-01-22 18:47:51	C:\Windows\System32\nslookup.exe	68.105.28.11	53
2026-01-22 18:47:50	C:\Windows\System32\nslookup.exe	68.105.28.11	53



EventID	count
1	20427
11	1199
13	1196
22	358
2	242
5	180
3	79
12	75
6	19
8	5
15	4
16	4
4	2

What I set up

- Installed Sysmon to generate detailed Windows activity logs
- Configured Splunk to ingest Sysmon logs (Sysmon/Operational)
- Verified data was coming in and created reports to review the activity

Evidence (what I observed)

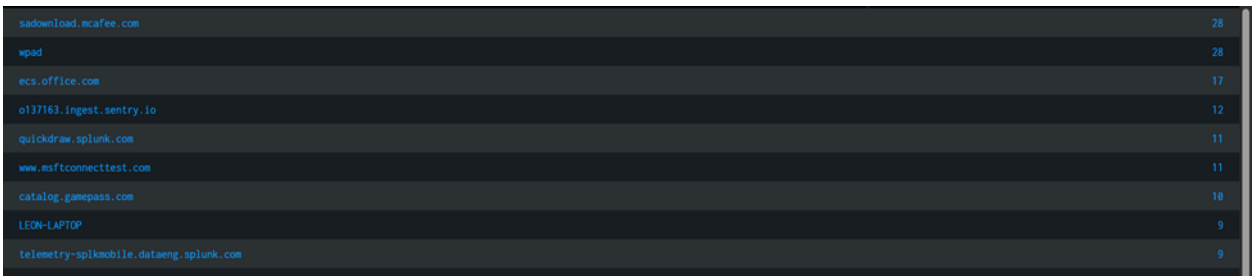
- nslookup.exe generated outbound connections to DNS resolvers over port **53**.
- Destination IPs observed included **68.105.28.11** and **8.8.8.8.**

Why this matters (SOC relevance)

This demonstrates process-to-network attribution, which is used in investigations to determine what program initiated what network traffic, a common first step in identifying suspicious outbound activity.

DNS Reports (Event ID 22)

C:\Program Files (x86)\Microsoft\EdgeWebView\Application\144.0.3719.82\msedgewebview2.exe	wpad	10
C:\Program Files\WindowsApps\Microsoft.GamingServices_33.108.12001.0_x64__8wekyb3d8bbwe\gamingservices.exe	catalog.gamepass.com	9
C:\Windows\System32\spoolsv.exe	LEON-LAPTOP	9
C:\Windows\System32\svchost.exe	www.msftconnecttest.com	9
C:\Program Files\Common Files\McAfee\ModuleCore\ModuleCoreService.exe	sadownload.mcafee.com	7
C:\Program Files\Google\Chrome\Application\chrome.exe	wpad	7
C:\Program Files (x86)\ExpressVPN\services\ExpressVPN.AppService.exe	clientstream.launchdarkly.com	6
C:\Program Files (x86)\ExpressVPN\services\ExpressVPN.AppService.exe	o137163.ingest.sentry.io	6
C:\Program Files\Google\Chrome\Application\chrome.exe	kape.dataplane.rudderstack.com	6
C:\Program Files\McAfee\WebAdvisor\servicehost.exe	sadownload.mcafee.com	6



sadownload.mcafee.com	28
wpad	28
ecs.office.com	17
o137163.ingest.sentry.io	12
quickdraw.splunk.com	11
www.msftconnecttest.com	11
catalog.gamepass.com	10
LEON-LAPTOP	9
telemetry-splkmobile.dataeng.splunk.com	9

Summary

Used Sysmon DNS logs in Splunk to see what domains my computer was looking up and which apps were responsible.

What I did

- Collected Sysmon DNS events (EventID 22) into Splunk.
- Built a “Top Domains” report to quickly see the most common lookups.
- Built a “DNS by App” report to connect domains back to the program that requested them.

Why it matters

If something suspicious happens, this helps answer two basic questions fast:

1. “What domain did the computer try to reach?”
2. “What program tried to reach it?”

What I learned

Seeing domain activity is helpful, but seeing the process behind it is what really makes it useful for investigations.

Basic Process Hunting (Sysmon EventID 1)

2026-01-23 13:56:08	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe	C:\WINDOWS\system32\cmd.exe /c "ver"
2026-01-23 13:55:08	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe	C:\WINDOWS\system32\cmd.exe /c "ver"
2026-01-23 13:54:08	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe	C:\WINDOWS\system32\cmd.exe /c "ver"
2026-01-23 13:53:08	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe	C:\WINDOWS\system32\cmd.exe /c "ver"
2026-01-23 13:52:08	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe	C:\WINDOWS\system32\cmd.exe /c "ver"

C:\Program Files\Splunk\bin\splunk-optimize.exe	14825
C:\Program Files\Splunk\bin\splunkd.exe	1791
C:\Program Files\Splunk\bin\btool.exe	1043
C:\Program Files\Splunk\bin\splunk.exe	989
C:\Program Files\Splunk\bin\python3.9.exe	611
C:\Program Files\Splunk\bin\splunk-powershell.exe	588
C:\Windows\System32\cmd.exe	452
C:\Program Files\Splunk\bin\splunk-MonitorNoHandle.exe	294
C:\Program Files\Splunk\bin\splunk-admon.exe	294
C:\Program Files\Splunk\bin\splunk-netmon.exe	294

Summary

Used Sysmon process logs in Splunk to spot command-line activity and build a simple baseline of what runs most on my PC.

What I did

- Built a report focused on command-line tools (PowerShell/cmd/etc.) so I could quickly review what commands were being run.
- Built a “top processes” baseline to understand normal activity.

Why it matters

Command-line activity is often where investigations start, and having a baseline makes it easier to notice something that looks out of place.

Registry Monitoring (Sysmon EventID 13)

2026-01-23 14:06:06	C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE	HKU\S-1-5-21-2401923302-3386338003-748317986-1001\Software\Microsoft\Office\16.0\Word\Security\Trusted Documents\TrustRecords\https://d.docs.live.net/a368856d7dc65003/Documents/Home%20SOC%20(Windows)%20-%20Splunk%20%5eM%20Sysmon%20Telemetry.docx
2026-01-23 14:06:06	C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE	HKU\S-1-5-21-2401923302-3386338003-748317986-1001\Software\Microsoft\Office\16.0\Word\Security\Trusted Documents\TrustRecords\https://d.docs.live.net/a368856d7dc65003/Documents/Home%20SOC%20(Windows)%20-%20Splunk%20%5eM%20Sysmon%20Telemetry.docx
2026-01-23 14:05:18	C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE	HKU\S-1-5-21-2401923302-3386338003-748317986-1001\Software\Microsoft\Office\16.0\Word\Security\Trusted Documents\TrustRecords\https://d.docs.live.net/a368856d7dc65003/Documents/Home%20SOC%20(Windows)%20-%20Splunk%20%5eM%20Sysmon%20Telemetry.docx

C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	HKU\S-1-5-21-2401923302-3386338003-748317986-1001\Software\Microsoft\Windows\CurrentVersion\Run\MicrosoftEdgeAutoLaunch_67D916BCFC7B97776DE93EA2279A3899	"C:\Program Files (x86)\Microsoft\Edge\Applicati --no-startup-window --win-sess
C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	HKU\S-1-5-21-2401923302-3386338003-748317986-1001\Software\Microsoft\Windows\CurrentVersion\Run\MicrosoftEdgeAutoLaunch_67D916BCFC7B97776DE93EA2279A3899	"C:\Program Files (x86)\Microsoft\Edge\Applicati --no-startup-window --win-sess
C:\Program Files (x86)\ExpressVPN\expressvpn-ui\ExpressVPN.exe	HKU\S-1-5-21-2401923302-3386338003-748317986-1001\Software\Microsoft\Windows\CurrentVersion\Run\ExpressVPN	C:\Program Files (x86)\ExpressVPN\expressvpn-ui\ExpressVPN.exe
C:\WINDOWS\servicing\TrustedInstaller.exe	HKLM\System\CurrentControlSet\Control\Winlogon\Notifications\Components\TrustedInstaller\Events	(Empty)
C:\WINDOWS\servicing\TrustedInstaller.exe	HKLM\System\CurrentControlSet\Control\Winlogon\Notifications\Components\TrustedInstaller\Events	CreateSession
C:\WINDOWS\servicing\TrustedInstaller.exe	HKLM\System\CurrentControlSet\Control\Winlogon\Notifications\Components\TrustedInstaller\Events	(Empty)

summary

Used Sysmon registry change logs in Splunk to see what registry values were modified and which programs made the changes.

What I did

- Built a report showing recent registry value updates (EventID 13).

Why it matters

Registry changes can be normal, but they can also be a sign of something trying to set itself to run automatically. This report helps narrow down what changed and where to look first.

What I learned:

Even normal apps can change startup-related registry settings, so it’s important to check what changed, where, and which program did it before assuming it’s malicious.