Threat Hunting with Splunk

Hunter Juhan

```
┌──(hjuhan@batcave)-[~]
└─$ whoami
```

Hunter Juhan

Threat Hunter at Global Payments
Four Years Experience in Cybersecurity
Education

- Columbus State University - Computer Science, Cybersecurity, 2019

Certifications

- Network+, Security+, CySA+, eJPT, Splunk Core User, AWS CCP, BTL1

Hobbies

- Full-time Husband and Father, Hiking, and Bourbon Enthusiast

Agenda

1 Brief Overview of Threat Hunting

2 Setting up Splunk

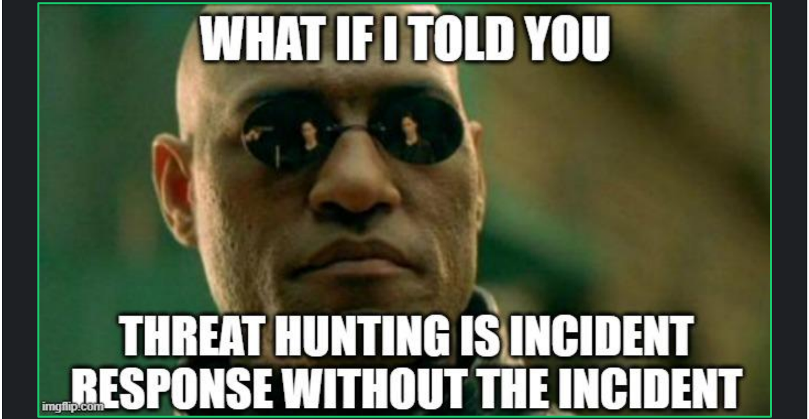
3 Threat Hunting Example

4 Hands On with Splunk

Threat Hunting

“The proactive effort of searching for signs of malicious activity in the IT infrastructure, both current and historical, that have evaded existing security defenses”

- *the Targeted Hunting integrating Threat Intelligence (TaHiTI) methodology*



What is Threat Hunting?

❏ Proactive vs. Reactive Approach

❏ Assumed Breach Mentality

It is NOT

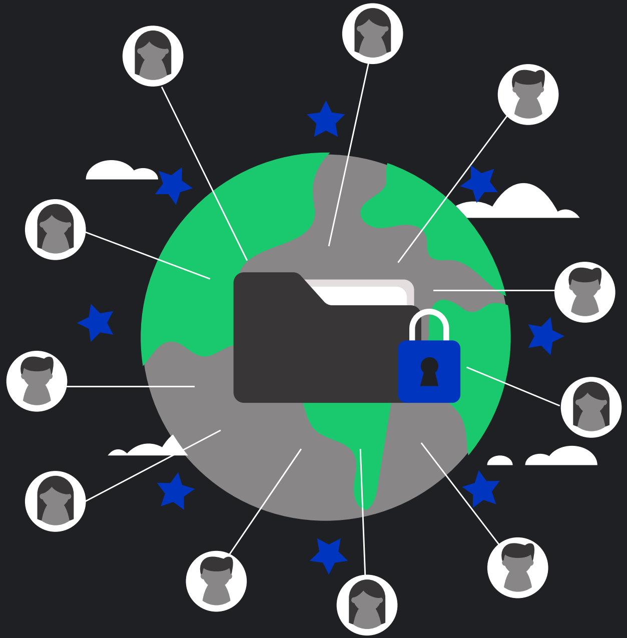
❏ Pentesting, Purple, Red Teaming

❏ Searching for IOCs

❏ Security Monitoring

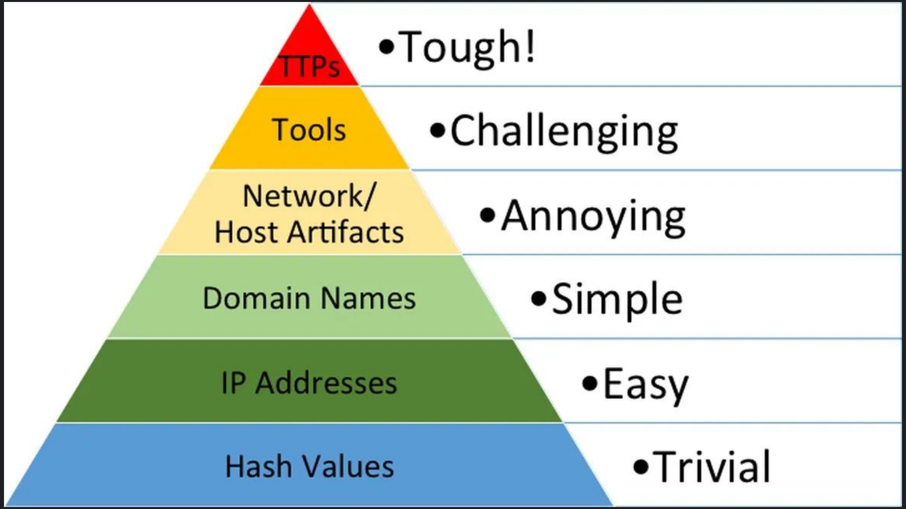
❏ Incident Response

❏ Guaranteed Results

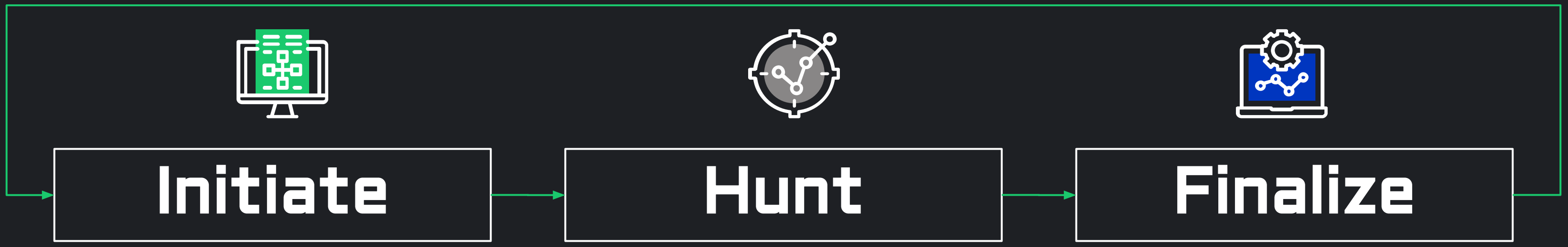


Hunt at the Top of the Pyramid

- ❏ Addresses how difficult it is for attackers to change characteristics of their attack
- ❏ Hunting focuses on the top 3 layers
- ❏ Hunting on the lower layers is not considered to be threat hunting



Threat Hunting Process



Initiate

- Threat Intelligence
- Security Monitoring
- Incident Response
- MITRE ATT&CK

Hunt

- Determine Hypothesis
- Data Collection
- Execute the Hunt
  - Retrieve Data
  - Analyze Data

Finalize

- Document Findings
- Handover
  - IR
  - Gaps
  - Detections
  - Vuln Mgmt

Tips

01 Start Broadly, then Narrow Down

02 Have an Adversarial Mindset

03 Compare Known-Good to Known-Bad

04 Avoid Bias

05 Speak to developers, sys admins, app owners

Let’s Hunt Some Threats!

Splunk Access

VirtualBox Instructions:

- ❑ Unzip the VM (password: cyberdefenders.org)
- ❑ Start the VM
- ❑ Log into the VM (user:vagrant, password:vagrant)
- ❑ Access Splunk from the Host Machine via http://127.0.0.1:8000

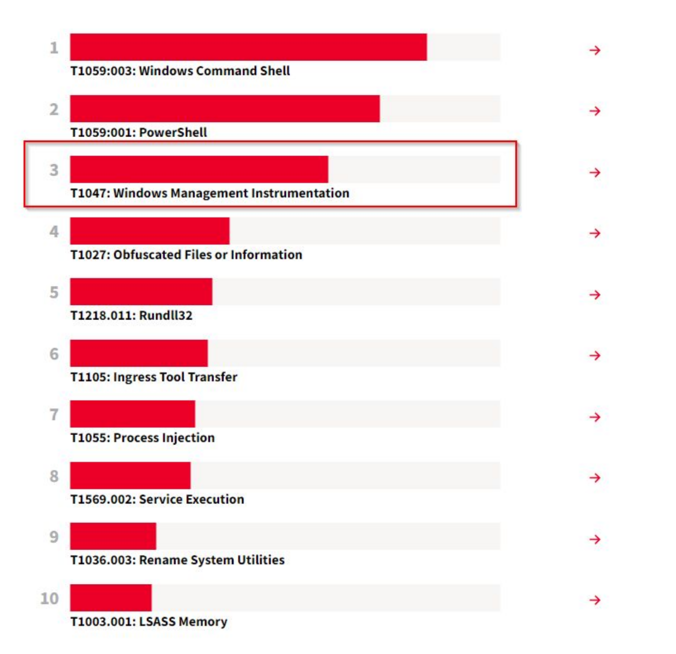
Lateral Movement - WMI

Description

Windows Management Instrumentation (WMI) is a Windows administration feature that provides a uniform environment for local and remote access to Windows system components.

Hypothesis

Adversaries will look to move laterally to other systems using Windows Management Instrumentation (WMI).



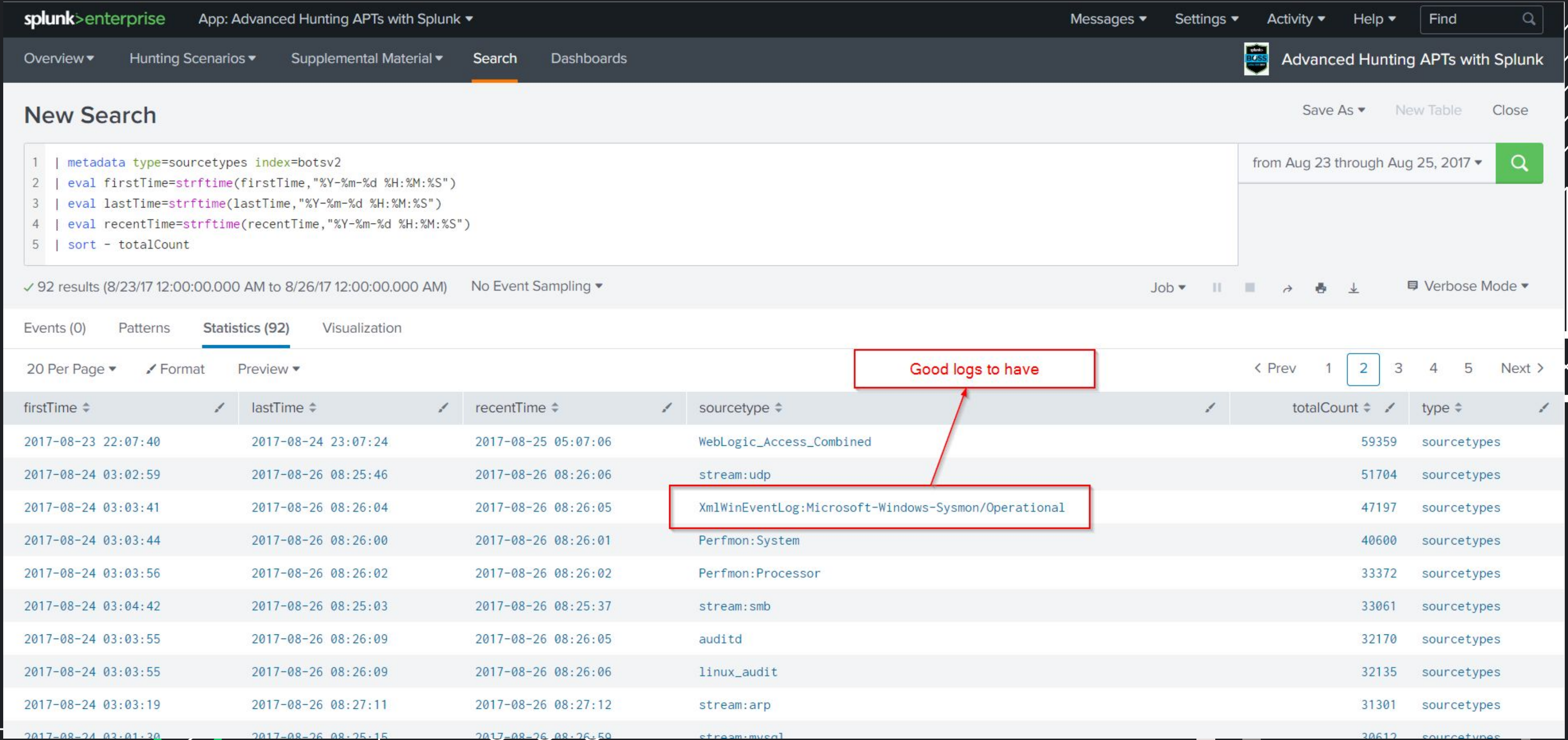
Questions to Ask

1. What data sets provide us a way to view lateral movement and communication between Windows hosts?
2. Can we see network communication between Windows hosts?
3. Are there actions taken on hosts that might indicate similar activities occurring on others?
4. What systems are communicating with one another?
5. What users are associated with those systems?

What data do we have?

```
| metadata type=sourcetypes index=botsv2
| eval firstTime=strftime(firstTime,"%Y-%m-%d %H:%M:%S")
| eval lastTime=strftime(lastTime,"%Y-%m-%d %H:%M:%S")
| eval recentTime=strftime(recentTime,"%Y-%m-%d %H:%M:%S")
| sort - totalCount
```

What data do we have?



New Search

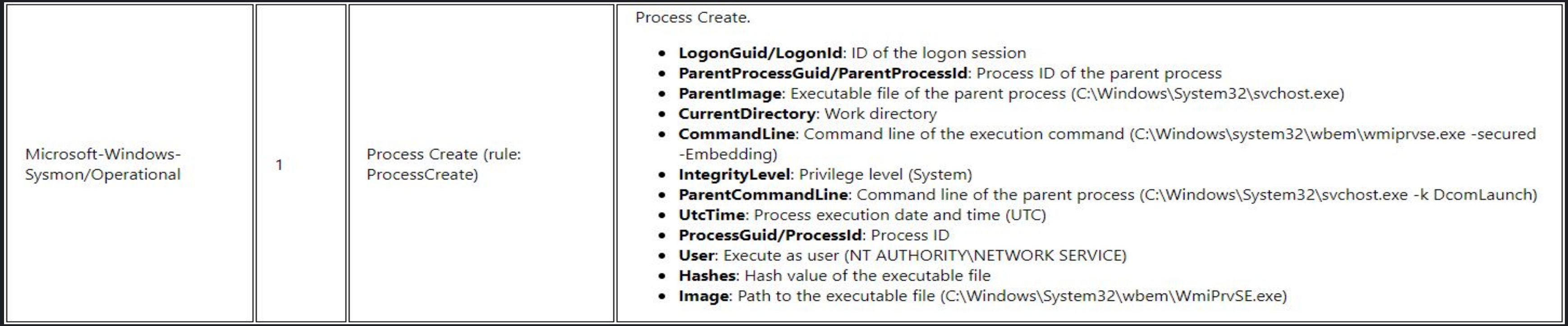
```
| metadata type=sourcetypes index=botsv2
| eval firstTime=strftime(firstTime,"%Y-%m-%d %H:%M:%S")
| eval lastTime=strftime(lastTime,"%Y-%m-%d %H:%M:%S")
| eval recentTime=strftime(recentTime,"%Y-%m-%d %H:%M:%S")
| sort - totalCount
```

✓ 92 results (8/23/17 12:00:00.000 AM to 8/26/17 12:00:00.000 AM)

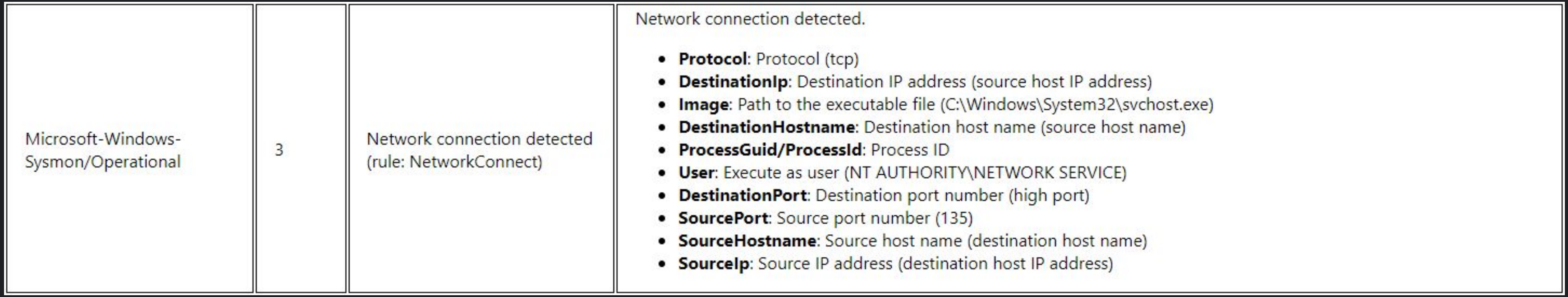
Good logs to have

firstTime	lastTime	recentTime	sourcetype	totalCount	type
2017-08-23 22:07:40	2017-08-24 23:07:24	2017-08-25 05:07:06	WebLogic_Access_Combined	59359	sourcetypes
2017-08-24 03:02:59	2017-08-26 08:25:46	2017-08-26 08:26:06	stream:udp	51704	sourcetypes
2017-08-24 03:03:41	2017-08-26 08:26:04	2017-08-26 08:26:05	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	47197	sourcetypes
2017-08-24 03:03:44	2017-08-26 08:26:00	2017-08-26 08:26:01	Perfmon:System	40600	sourcetypes
2017-08-24 03:03:56	2017-08-26 08:26:02	2017-08-26 08:26:02	Perfmon:Processor	33372	sourcetypes
2017-08-24 03:04:42	2017-08-26 08:25:03	2017-08-26 08:25:37	stream:smb	33061	sourcetypes
2017-08-24 03:03:55	2017-08-26 08:26:09	2017-08-26 08:26:05	auditd	32170	sourcetypes
2017-08-24 03:03:55	2017-08-26 08:26:09	2017-08-26 08:26:06	linux_audit	32135	sourcetypes
2017-08-24 03:03:19	2017-08-26 08:27:11	2017-08-26 08:27:12	stream:arp	31301	sourcetypes
2017-08-24 03:01:30	2017-08-26 08:25:15	2017-08-26 08:26:59	stream:mysql	30612	sourcetypes

WMI Execution - Event Logs

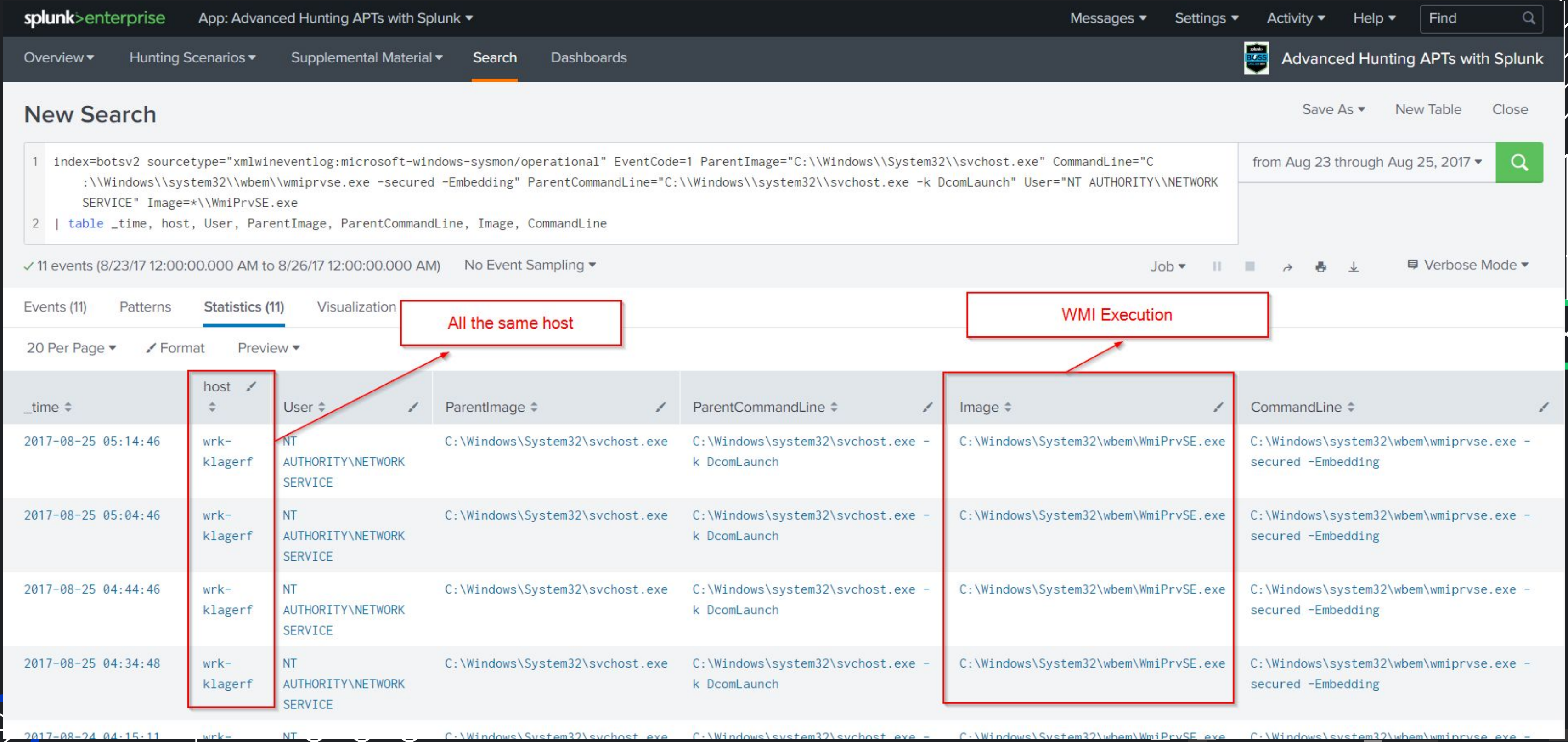


Microsoft-Windows-Sysmon/Operational	1	Process Create (rule: ProcessCreate)	Process Create. - **LogonGuid/LogonId**: ID of the logon session - **ParentProcessGuid/ParentProcessId**: Process ID of the parent process - **ParentImage**: Executable file of the parent process (C:\Windows\System32\svchost.exe) - **CurrentDirectory**: Work directory - **CommandLine**: Command line of the execution command (C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding) - **IntegrityLevel**: Privilege level (System) - **ParentCommandLine**: Command line of the parent process (C:\Windows\System32\svchost.exe -k DcomLaunch) - **UtcTime**: Process execution date and time (UTC) - **ProcessGuid/ProcessId**: Process ID - **User**: Execute as user (NT AUTHORITY\NETWORK SERVICE) - **Hashes**: Hash value of the executable file - **Image**: Path to the executable file (C:\Windows\System32\wbem\WmiPrvSE.exe)



Microsoft-Windows-Sysmon/Operational	3	Network connection detected (rule: NetworkConnect)	Network connection detected. - **Protocol**: Protocol (tcp) - **DestinationIp**: Destination IP address (source host IP address) - **Image**: Path to the executable file (C:\Windows\System32\svchost.exe) - **DestinationHostname**: Destination host name (source host name) - **ProcessGuid/ProcessId**: Process ID - **User**: Execute as user (NT AUTHORITY\NETWORK SERVICE) - **DestinationPort**: Destination port number (high port) - **SourcePort**: Source port number (135) - **SourceHostname**: Source host name (destination host name) - **SourceIp**: Source IP address (destination host IP address)

WMI Execution in Splunk



New Search

```
index=botsv2 sourcetype="xmlwineventlog:microsoft-windows-sysmon/operational" EventCode=1 ParentImage="C:\\Windows\\System32\\svchost.exe" CommandLine="C
    :\\Windows\\system32\\wbem\\wmiprvse.exe -secured -Embedding" ParentCommandLine="C:\\Windows\\system32\\svchost.exe -k DcomLaunch" User="NT AUTHORITY\\NETWORK
    SERVICE" Image=*\\WmiPrvSE.exe
| table _time, host, User, ParentImage, ParentCommandLine, Image, CommandLine
```

from Aug 23 through Aug 25, 2017 ▾

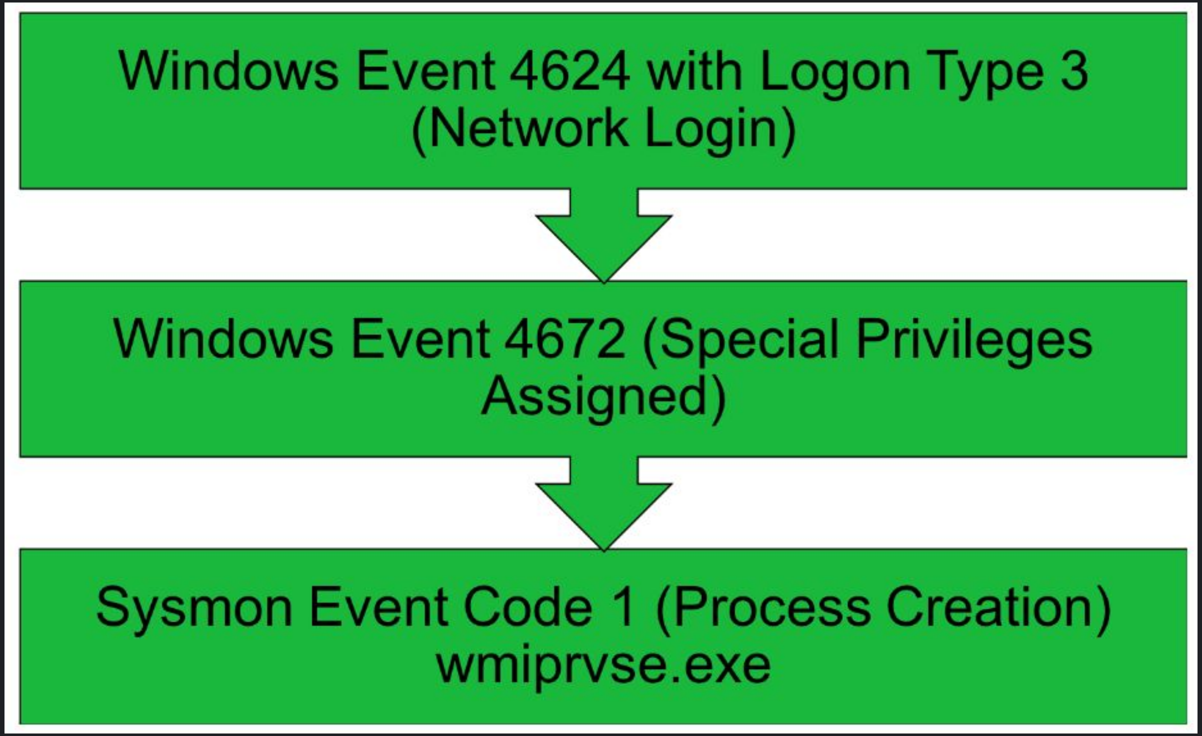
✓ 11 events (8/23/17 12:00:00.000 AM to 8/26/17 12:00:00.000 AM) No Event Sampling ▾

All the same host

WMI Execution

_time	host	User	ParentImage	ParentCommandLine	Image	CommandLine
2017-08-25 05:14:46	wrk-klagerf	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch	C:\Windows\System32\wbem\WmiPrvSE.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
2017-08-25 05:04:46	wrk-klagerf	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch	C:\Windows\System32\wbem\WmiPrvSE.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
2017-08-25 04:44:46	wrk-klagerf	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch	C:\Windows\System32\wbem\WmiPrvSE.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
2017-08-25 04:34:48	wrk-klagerf	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch	C:\Windows\System32\wbem\WmiPrvSE.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
2017-08-24 04:15:11	wrk-	NT	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -	C:\Windows\System32\wbem\WmiPrvSE.exe	C:\Windows\system32\wbem\wmiprvse.exe -

Remote Execution via WMI

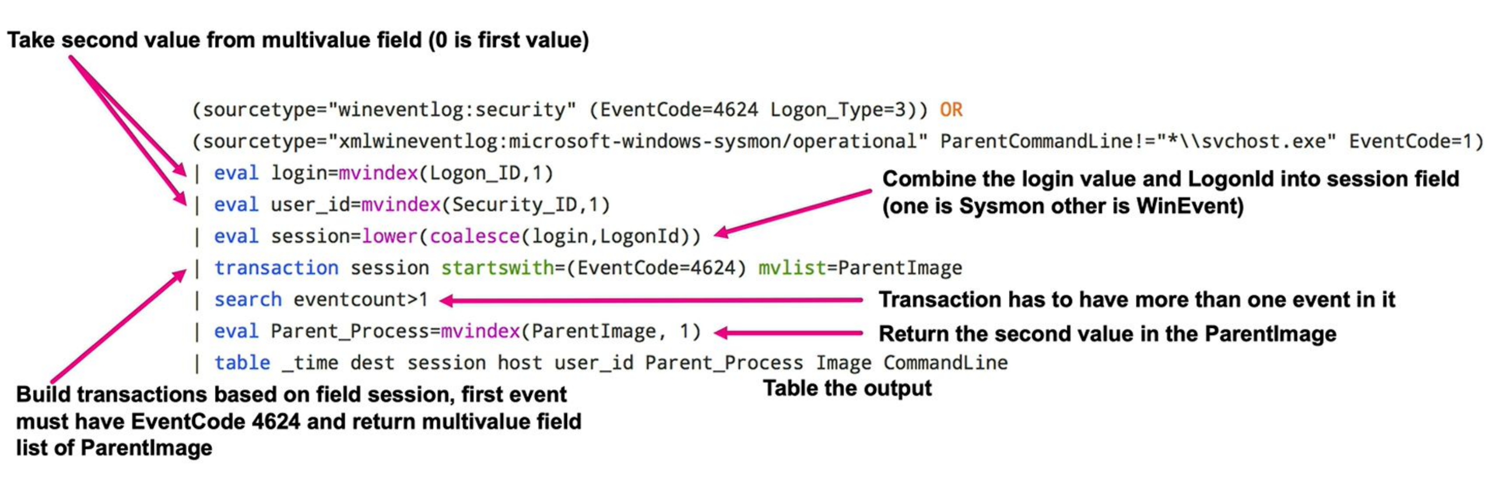


Windows Event 4624 with Logon Type 3 (Network Login)

Windows Event 4672 (Special Privileges Assigned)

Sysmon Event Code 1 (Process Creation) wmiprvse.exe

Remote Execution via WMI



Take second value from multivalue field (0 is first value)

```
(sourcetype="wineventlog:security" (EventCode=4624 Logon_Type=3)) OR
(sourcetype="xmlwineventlog:microsoft-windows-sysmon/operational" ParentCommandLine!="*\\svchost.exe" EventCode=1)
| eval login=mvindex(Logon_ID,1)
| eval user_id=mvindex(Security_ID,1)
| eval session=lower(coalesce(login,LogonId))
| transaction session startswith=(EventCode=4624) mvlist=ParentImage
| search eventcount>1
| eval Parent_Process=mvindex(ParentImage, 1)
| table _time dest session host user_id Parent_Process Image CommandLine
```

Combine the login value and LogonId into session field (one is Sysmon other is WinEvent)

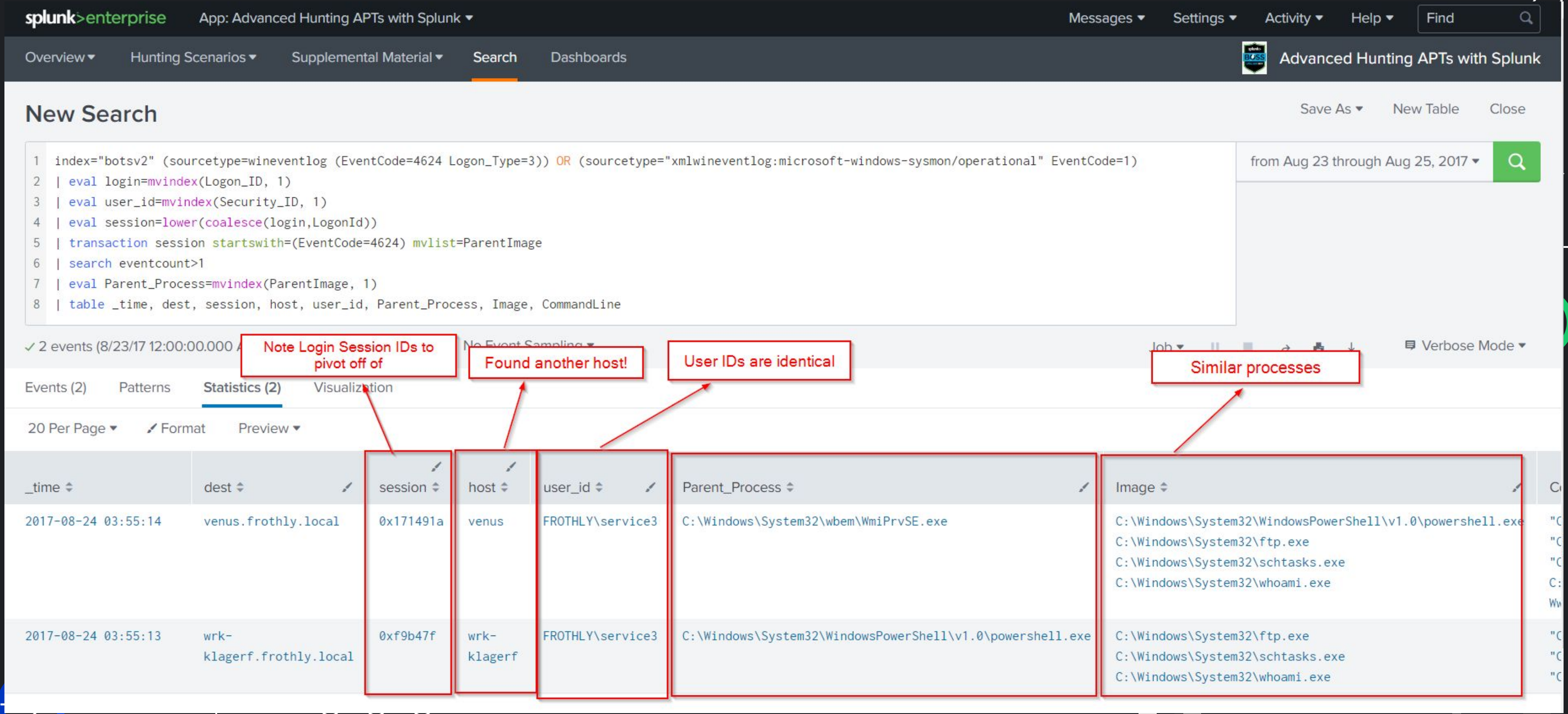
Transaction has to have more than one event in it

Return the second value in the ParentImage

Table the output

Build transactions based on field session, first event must have EventCode 4624 and return multivalue field list of ParentImage

Remote Execution via WMI in Splunk



New Search

```
index="botsv2" (sourcetype=wineventlog (EventCode=4624 Logon_Type=3)) OR (sourcetype="xmlwineventlog:microsoft-windows-sysmon/operational" EventCode=1)
| eval login=mvindex(Logon_ID, 1)
| eval user_id=mvindex(Security_ID, 1)
| eval session=lower(coalesce(login,LogonId))
| transaction session startswith=(EventCode=4624) mvlist=ParentImage
| search eventcount>1
| eval Parent_Process=mvindex(ParentImage, 1)
| table _time, dest, session, host, user_id, Parent_Process, Image, CommandLine
```

✓ 2 events (8/23/17 12:00:00.000 A

Note Login Session IDs to pivot off of

Found another host!

User IDs are identical

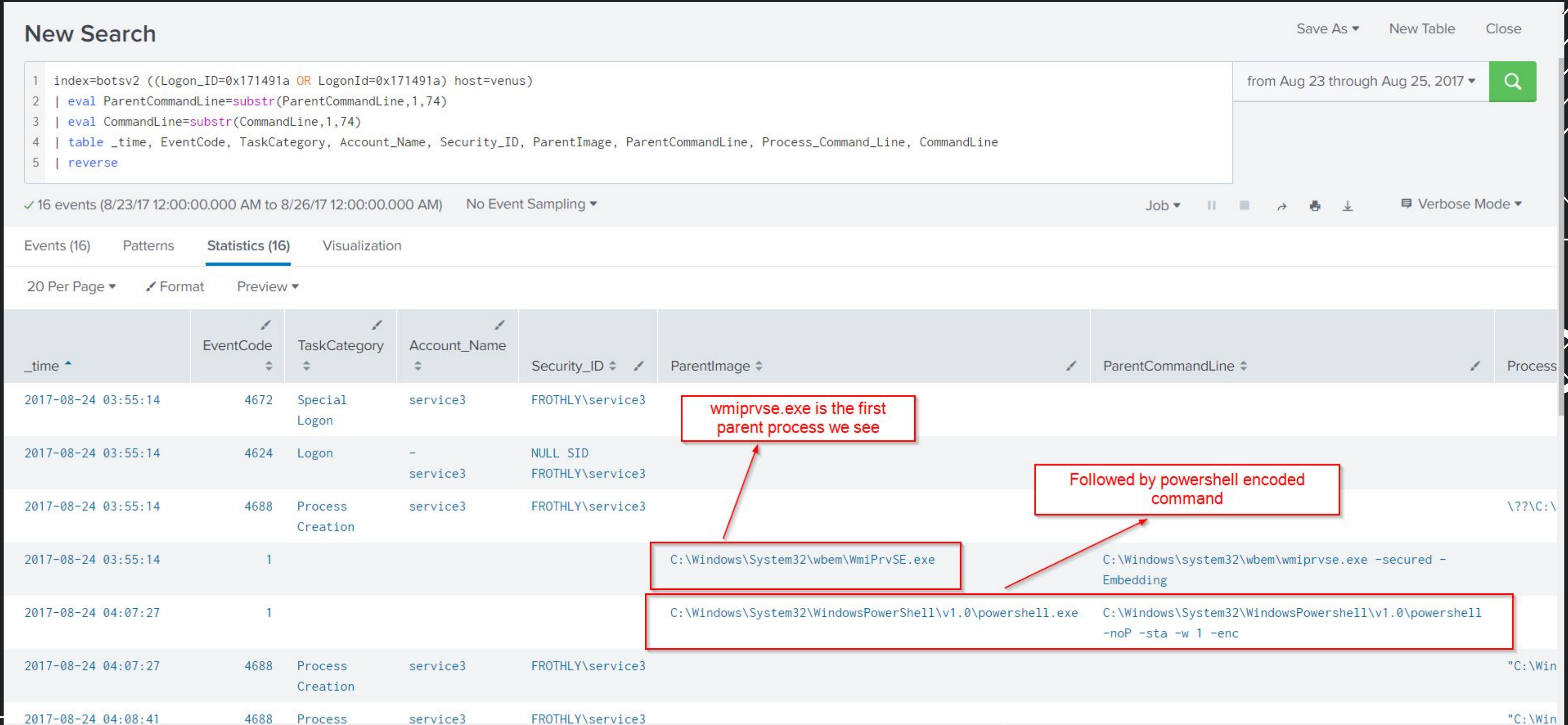
Similar processes

_time	dest	session	host	user_id	Parent_Process	Image	C
2017-08-24 03:55:14	venus.frothly.local	0x171491a	venus	FROTHLY\service3	C:\Windows\System32\wbem\WmiPrvSE.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe C:\Windows\System32\ftp.exe C:\Windows\System32\schtasks.exe C:\Windows\System32\whoami.exe	"C "C "C C: Ww
2017-08-24 03:55:13	wrk-klagerf.frothly.local	0xf9b47f	wrk-klagerf	FROTHLY\service3	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\ftp.exe C:\Windows\System32\schtasks.exe C:\Windows\System32\whoami.exe	"C "C "C

Login Sessions - Time to Pivot

- ❑ What other processes are associated with these hosts and login sessions?
- ❑ Do we see wmiprvse.exe (Windows Management Instrumentation Provider Service) elsewhere?
- ❑ Check and validate external network connections to the source in question

Login Sessions - venus



```
index=botsv2 ((Logon_ID=0x171491a OR LogonId=0x171491a) host=venus)
| eval ParentCommandLine=substr(ParentCommandLine,1,74)
| eval CommandLine=substr(CommandLine,1,74)
| table _time, EventCode, TaskCategory, Account_Name, Security_ID, ParentImage, ParentCommandLine, Process_Command_Line, CommandLine
| reverse
```

from Aug 23 through Aug 25, 2017 ▾

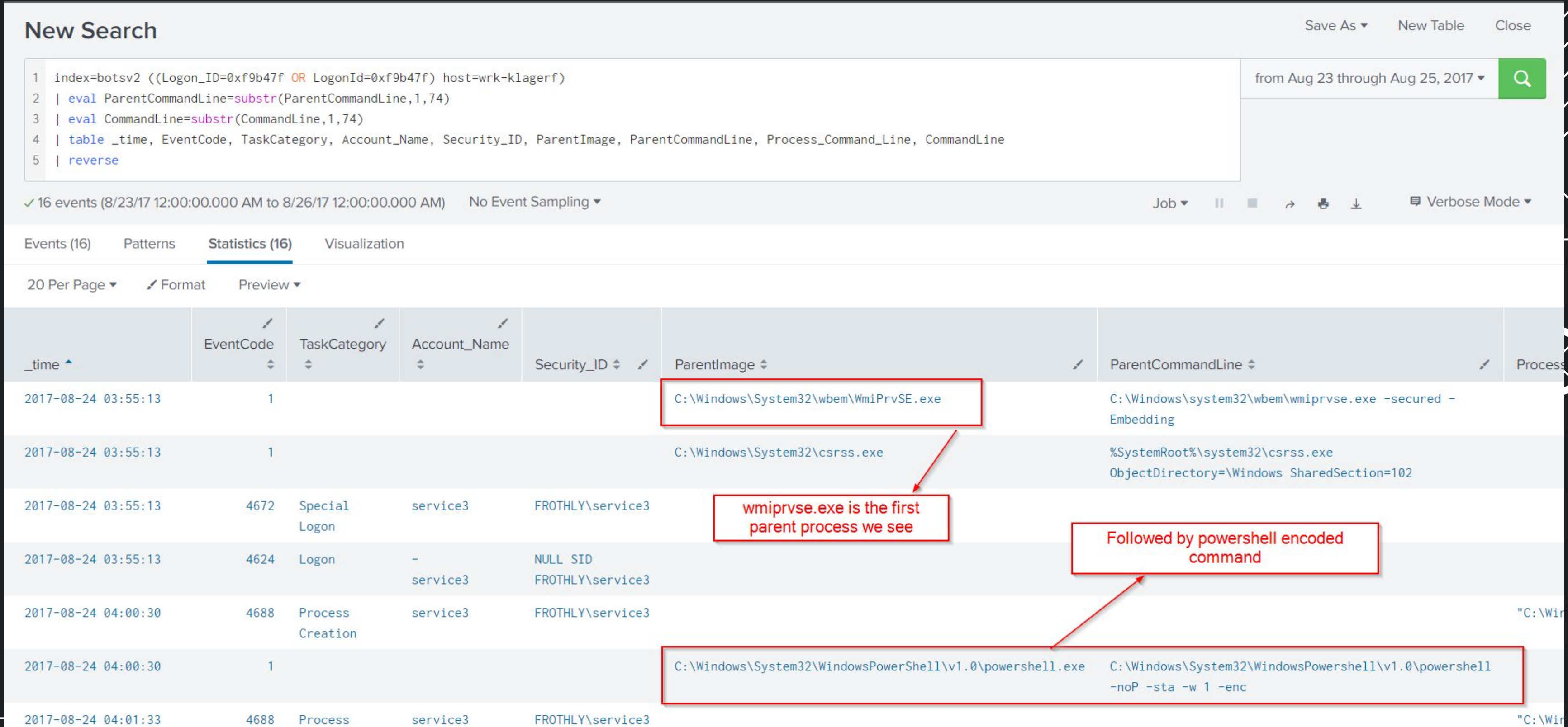
✓ 16 events (8/23/17 12:00:00.000 AM to 8/26/17 12:00:00.000 AM) No Event Sampling ▾

_time	EventCode	TaskCategory	Account_Name	Security_ID	ParentImage	ParentCommandLine	Process
2017-08-24 03:55:14	4672	Special Logon	service3	FROTHLY\service3			
2017-08-24 03:55:14	4624	Logon	- service3	NULL SID FROTHLY\service3			
2017-08-24 03:55:14	4688	Process Creation	service3	FROTHLY\service3			\??\C:\
2017-08-24 03:55:14	1				C:\Windows\System32\wbem\WmiPrvSE.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	
2017-08-24 04:07:27	1				C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\WindowsPowershell\v1.0\powershell -noP -sta -w 1 -enc	
2017-08-24 04:07:27	4688	Process Creation	service3	FROTHLY\service3			"C:\Win
2017-08-24 04:08:41	4688	Process	service3	FROTHLY\service3			"C:\Win

wmiprvse.exe is the first parent process we see

Followed by powershell encoded command

Login Sessions - wrk-klagerf



```
index=botsv2 ((Logon_ID=0xf9b47f OR LogonId=0xf9b47f) host=wrk-klagerf)
| eval ParentCommandLine=substr(ParentCommandLine,1,74)
| eval CommandLine=substr(CommandLine,1,74)
| table _time, EventCode, TaskCategory, Account_Name, Security_ID, ParentImage, ParentCommandLine, Process_Command_Line, CommandLine
| reverse
```

from Aug 23 through Aug 25, 2017 ▾

✓ 16 events (8/23/17 12:00:00.000 AM to 8/26/17 12:00:00.000 AM) No Event Sampling ▾

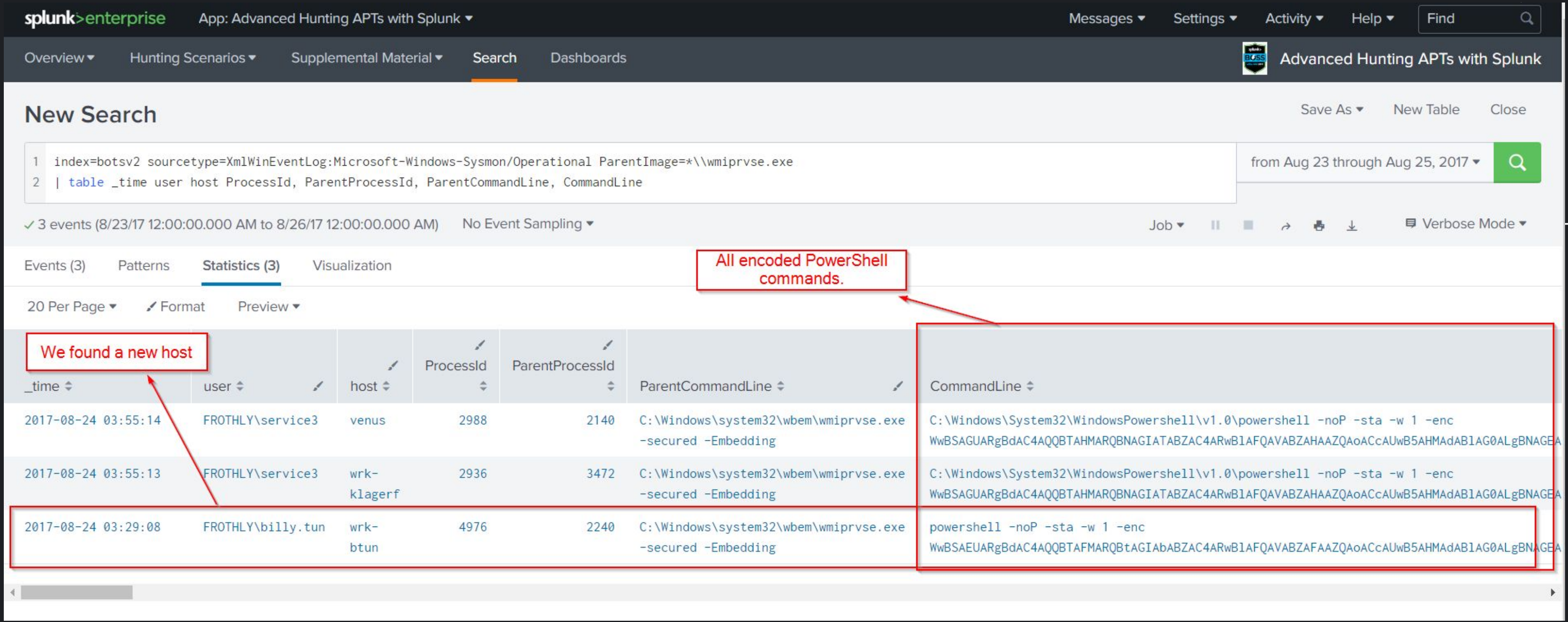
Events (16) Patterns **Statistics (16)** Visualization

_time	EventCode	TaskCategory	Account_Name	Security_ID	ParentImage	ParentCommandLine	Process
2017-08-24 03:55:13	1				C:\Windows\System32\wbem\WmiPrvSE.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	
2017-08-24 03:55:13	1				C:\Windows\System32\csrss.exe	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=102	
2017-08-24 03:55:13	4672	Special Logon	service3	FROTHLY\service3			
2017-08-24 03:55:13	4624	Logon	- service3	NULL SID FROTHLY\service3			
2017-08-24 04:00:30	4688	Process Creation	service3	FROTHLY\service3			"C:\Wi
2017-08-24 04:00:30	1				C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\WindowsPowershell\v1.0\powershell -noP -sta -w 1 -enc	
2017-08-24 04:01:33	4688	Process	service3	FROTHLY\service3			"C:\Wi

wmiprvse.exe is the first parent process we see

Followed by powershell encoded command

Wmiprvse.exe



New Search

```
index=botsv2 sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational ParentImage=*\\wmiprvse.exe
| table _time user host ProcessId, ParentProcessId, ParentCommandLine, CommandLine
```

from Aug 23 through Aug 25, 2017 ▾

✓ 3 events (8/23/17 12:00:00.000 AM to 8/26/17 12:00:00.000 AM) No Event Sampling ▾

All encoded PowerShell commands.

We found a new host

_time	user	host	ProcessId	ParentProcessId	ParentCommandLine	CommandLine
2017-08-24 03:55:14	FROTHLY\service3	venus	2988	2140	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	C:\Windows\System32\WindowsPowershell\v1.0\powershell -noP -sta -w 1 -enc WwBSAGUARgBdAC4AQQBTAHMARQBNAGIATABZAC4ARwBlAFQAVABZAHAAZQAoACcAUwB5AHMAdABlAG0ALgBNAGEA
2017-08-24 03:55:13	FROTHLY\service3	wrk-klagerf	2936	3472	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	C:\Windows\System32\WindowsPowershell\v1.0\powershell -noP -sta -w 1 -enc WwBSAGUARgBdAC4AQQBTAHMARQBNAGIATABZAC4ARwBlAFQAVABZAHAAZQAoACcAUwB5AHMAdABlAG0ALgBNAGEA
2017-08-24 03:29:08	FROTHLY\billy.tun	wrk-btun	4976	2240	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	powershell -noP -sta -w 1 -enc WwBSAEUARgBdAC4AQQBTAFMARQBtAGIAbABZAC4ARwBlAFQAVABZAFAAZQAoACcAUwB5AHMAdABlAG0ALgBNAGEA

Lateral Movement - Findings

Were We Able To Confirm Our Hypothesis?

- ❑ Yes, WMI was used for lateral movement

What We Learned

- ❑ Internal hosts venus and wrk-klagerf were both infected via lateral movement from wrk-btun
- ❑ PowerShell was used to facilitate the lateral movement
- ❑ Processes are all running encoded PowerShell
- ❑ Wrk-btun also sees encoded PowerShell with a different launcher, but same commands

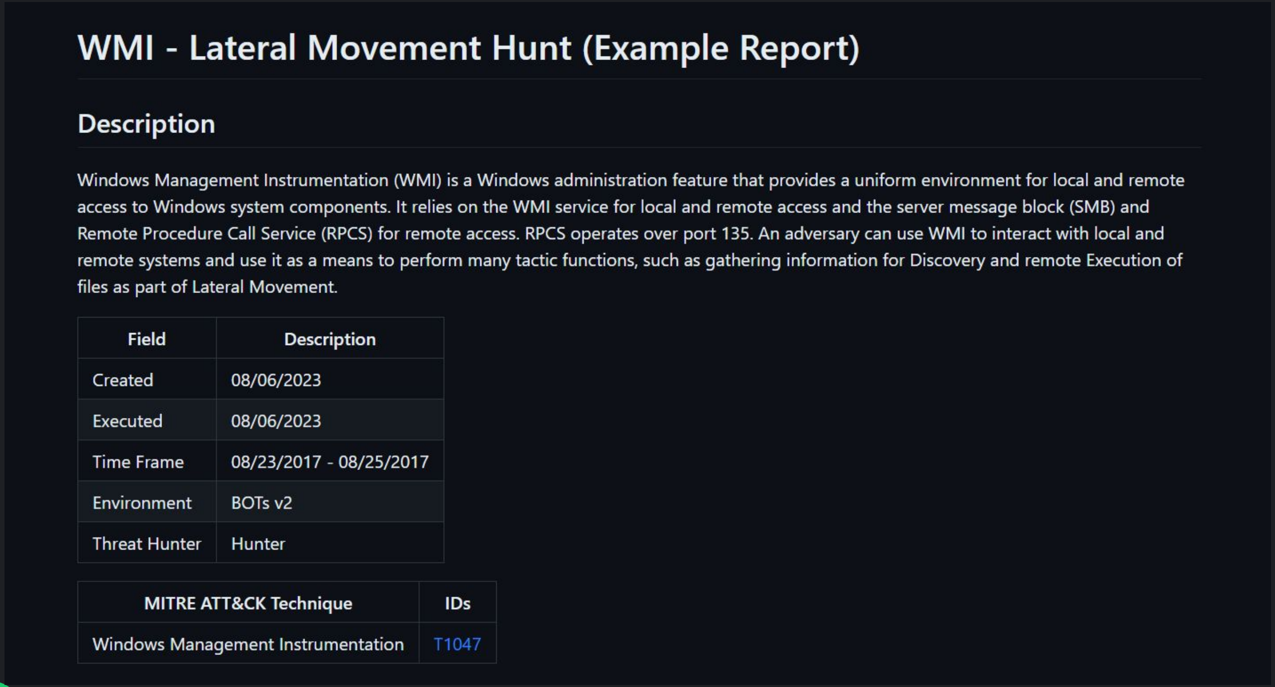
Lateral Movement - Outputs

Handover

- ❑ Document Findings
- ❑ Incident Response
- ❑ Alert on encoded PowerShell
- ❑ Windows Remote Management Tools – Understand which ones are needed and which ones are not
- ❑ Alert for specific orders of action that might indicate lateral movement
- ❑ Understand data flows in environment

Threat Hunt Report

https://github.com/threatHNTR/hunt-resources/blob/main/example-hunt-report.md



WMI - Lateral Movement Hunt (Example Report)

Description

Windows Management Instrumentation (WMI) is a Windows administration feature that provides a uniform environment for local and remote access to Windows system components. It relies on the WMI service for local and remote access and the server message block (SMB) and Remote Procedure Call Service (RPCS) for remote access. RPCS operates over port 135. An adversary can use WMI to interact with local and remote systems and use it as a means to perform many tactic functions, such as gathering information for Discovery and remote Execution of files as part of Lateral Movement.

Field	Description
Created	08/06/2023
Executed	08/06/2023
Time Frame	08/23/2017 - 08/25/2017
Environment	BOTs v2
Threat Hunter	Hunter

MITRE ATT&CK Technique	IDs
Windows Management Instrumentation	T1047

Resources

- https://bots.splunk.com/ - Hunting Lateral Movement
- https://www.betaalvereniging.nl/wp-content/uploads/DEF-TaHiTI-Threat-Hunting-Methodology.pdf
- https://attack.mitre.org/techniques/T1047/
- https://www.slideshare.net/votadlos/hunting-lateral-movement-in-windows-infrastructure
- https://redcanary.com/threat-detection-report/techniques/
- https://github.com/threatHNTR/hunt-resources/blob/main/example-hunt-report.md

Hands On Activity

1. Register for a Splunk account
2. Go to https://bots.splunk.com/
3. Play Boss of the SOC Version 1

OR

1. Log into the Splunk VM
2. Go to the "Advanced Hunting APTs with Splunk" App
3. Run through some of the Hunting Scenarios

THANK YOU!