



# Creating Detection Research Opportunities

Leveraging ATT&CK Evaluations

# Roberto Rodriguez

## @Cyb3rWard0g

- Microsoft Threat Intelligence Center (MSTIC) R&D
- I ❤️ Open Source
- Projects:
  - @HunterPlaybook 🏹
  - @THE\_HELK
  - ATTACK-Python-Client
  - @OSSEM\_Project
  - @Mordor\_Project + Mordor Labs 😈
  - Blacksmith & More
- Non-tech:
  - Blacksmithing!
  - Cooking Recipes: <https://infosecwelldone.com/>



# Agenda

- ATT&CK Evaluations
- APT29 Eval (Round 2)
  - Network Design
  - Emulation Plans
- Detection Research Opportunities
  - Mordor Labs
  - Mordor Datasets
  - Detection Hackathons
  - Threat Hunter Playbook 😊

# ATT&CK Evaluations

MITRE evaluates cybersecurity products using an open methodology based on the ATT&CK® knowledge base.

- Empowering end-users with objective insights into how to use specific commercial security products to address known adversary behaviors
- Providing transparency around the true capabilities of security products to address known adversary behaviors
- Driving the security vendor community to enhance its capability to address known adversary behaviors



# APT29 Eval (Round 2)

A threat group that reportedly compromised the Democratic National Committee starting in the summer of 2015.

## Scenario 1 / Day 1

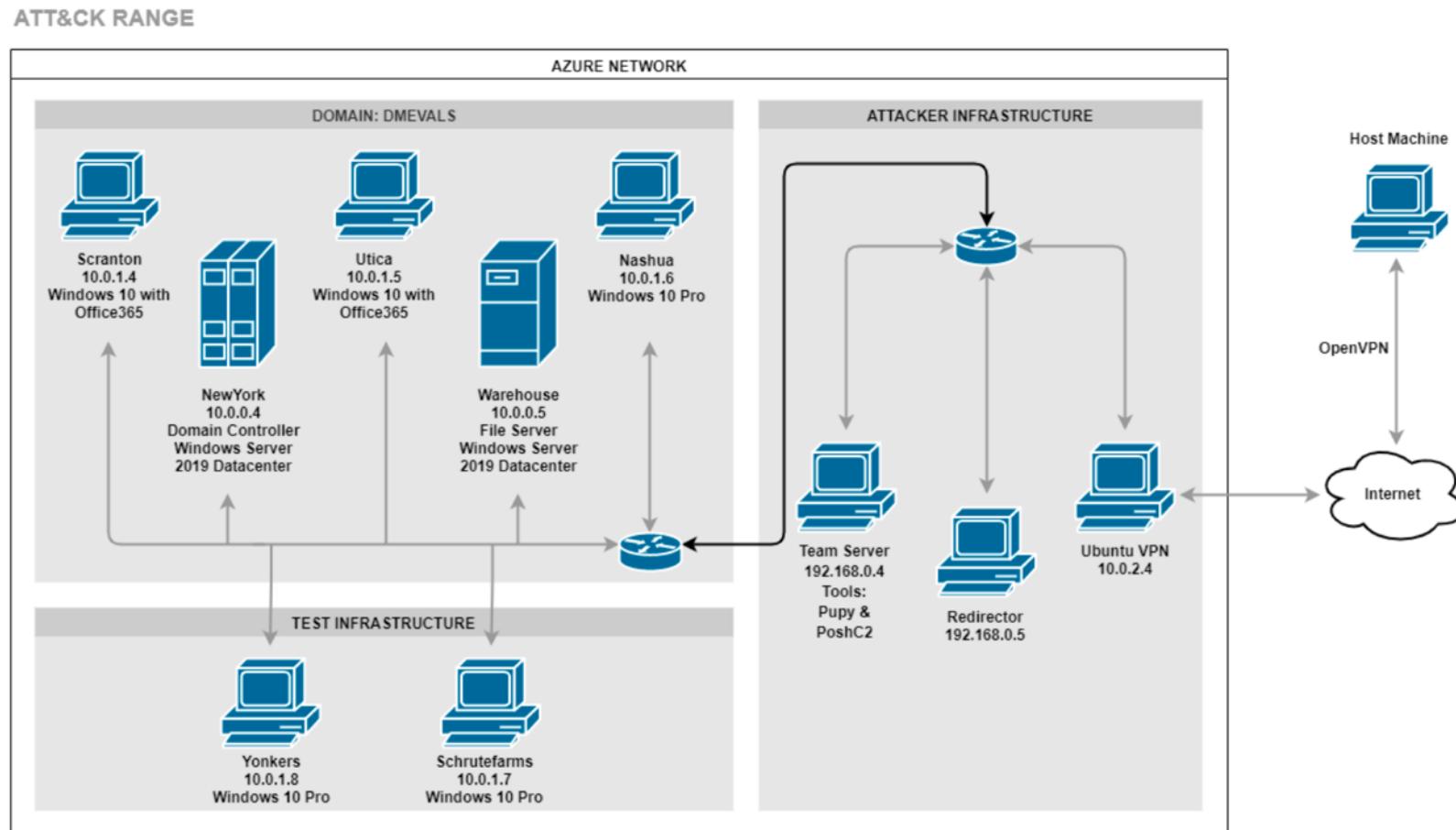
- The first scenario (executed with Pupy, Meterpreter, and custom tooling) begins with the execution of a payload delivered by a widespread "spray and pray" spearphishing campaign.

## Scenario 2 / Day 2

- The second scenario (executed with PoshC2 and custom tooling) focuses on a very targeted and methodical breach, beginning with the execution of a specially crafted payload designed to scrutinize the target environment before executing

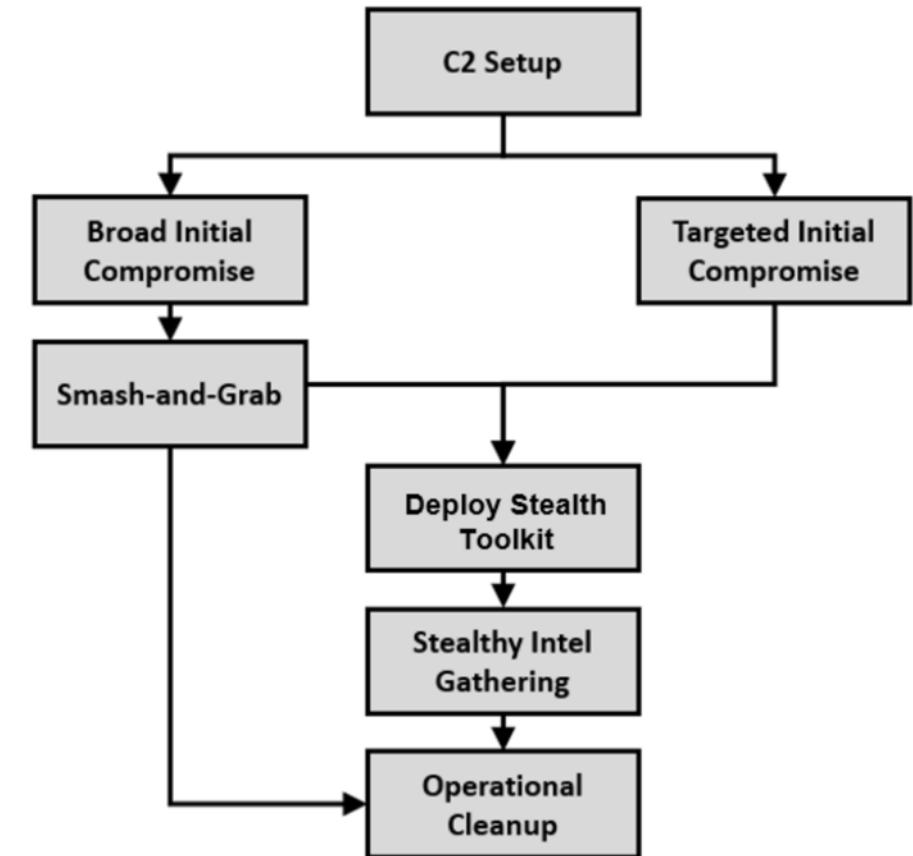


# APT29 Eval – Network Design



# APT29 Eval – Emulation Plans

- In their broader campaigns, APT29 has conducted smash-and-grab espionage with rapid collection and exfiltration.
- In their smaller more targeted campaigns, APT29 has utilized a different toolset incrementally modified to attempt to evade published intelligence about their operations.



# APT29 Eval – Emulation Plans – Day 1

mitre-attack / attack-arsenal

Watch ▾ 8 Star 39 Fork 12

Code Issues 1 Pull requests 1 Actions Projects 0 Wiki Security 0 Insights

Branch: master ▾ Create new file Upload files Find file History

attack-arsenal / adversary\_emulation / APT29 / Emulation\_Plan / Day 1 / payloads /

connormagee	Initial Release of ATT&CK Arsenal	Latest commit 66650ce 27 days ago
..		
Seaduke	Initial Release of ATT&CK Arsenal	27 days ago
SysinternalsSuite	Initial Release of ATT&CK Arsenal	27 days ago
cod.3aka3.scr	Initial Release of ATT&CK Arsenal	27 days ago
hostui.cpp	Initial Release of ATT&CK Arsenal	27 days ago
monkey.png	Initial Release of ATT&CK Arsenal	27 days ago
shockwave.local.pfx	Initial Release of ATT&CK Arsenal	27 days ago

[https://github.com/mitre-attack/attack-arsenal/tree/master/adversary\\_emulation/APT29/Emulation\\_Plan/Day%201/payloads](https://github.com/mitre-attack/attack-arsenal/tree/master/adversary_emulation/APT29/Emulation_Plan/Day%201/payloads)

# APT29 Eval – Emulation Plans – Day 2

mitre-attack / attack-arsenal

Watch 8 Star 39 Fork 12

Code Issues 1 Pull requests 1 Actions Projects 0 Wiki Security 0 Insights

Branch: master Create new file Upload files Find file History

attack-arsenal / adversary\_emulation / APT29 / Emulation\_Plan / Day 2 / payloads /

connormagee Initial Release of ATT&CK Arsenal	Latest commit 66650ce 27 days ago
..	
2016_United_States_presidential_election_-_Wikipedi... Initial Release of ATT&CK Arsenal	27 days ago
Invoke-Mimikatz.ps1 Initial Release of ATT&CK Arsenal	27 days ago
Invoke-WinRMSession.ps1 Initial Release of ATT&CK Arsenal	27 days ago
MITRE-ATTACK-EVALS.HTML Initial Release of ATT&CK Arsenal	27 days ago
m Initial Release of ATT&CK Arsenal	27 days ago
make_lnk.ps1 Initial Release of ATT&CK Arsenal	27 days ago
powerview.ps1 Initial Release of ATT&CK Arsenal	27 days ago
schemas.ps1 Initial Release of ATT&CK Arsenal	27 days ago

[https://github.com/mitre-attack/attack-arsenal/tree/master/adversary\\_emulation/APT29/Emulation\\_Plan/Day%202/payloads](https://github.com/mitre-attack/attack-arsenal/tree/master/adversary_emulation/APT29/Emulation_Plan/Day%202/payloads)

# APT29 Eval – DIY Plugin

Home Campaigns

Plugins Advanced Docs Logout

evals gameboard training compass sandcat stockpile manx

# ATT&CK | Eval - APT 29

## About

This CALDERA plugin is meant to emulate the techniques used by the MITRE ATT&CK team in ATT&CK evaluations. Multiple CALDERA adversary profiles have been developed for both APT3 and APT29. Consult the evals' plugin README.md for environment setup guidance. For general CALDERA questions, consult the CALDERA wiki .

[https://github.com/mitre-attack/attack-arsenal/tree/master/adversary\\_emulation/APT29/CALDERA\\_DIY/evals](https://github.com/mitre-attack/attack-arsenal/tree/master/adversary_emulation/APT29/CALDERA_DIY/evals)

# APT29 Eval – DIY Plugin

The screenshot shows a web-based interface for creating an ATT&CK profile. On the left, there's a sidebar titled "Profiles" with a "VIEW" button. Below it, a description explains that profiles are collections of ATT&CK TTPs designed to create specific effects on a host or network. It includes a dropdown menu set to "ATT&CK Eval APT29 - Day 1.A", a "Save" button, and a "Delete profile" button.

The main area displays a kill chain visualization with four phases:

- Phase 1:** Contains one step: **1.A - RTLO Start Sandcat (T1036)**. It is labeled as EXECUTION | RTLO OVERRIDE and includes a Windows icon and a trash bin icon.
- Phase 2:** Contains two steps: **1.B - PowerShell (1086)** and **2.A - Automated Collection (T1119)**. Both are labeled as EXECUTION | POWERSHELL and COLLECTION | AUTOMATED COLLECTION respectively, each with a Windows icon and a trash bin icon.
- Phase 3:** Contains one step: **2.B.1 - Data from staged file (T1074) and Exfiltration over C2 Channel (T1041)**. It is labeled as EXFILTRATION | EXFILTRATION OVER COMMAND AND CONTROL CHANNEL and includes a Windows icon, a lock icon, a trash bin icon, and a file icon.
- Phase 4:** Contains no visible steps.

At the top right, there are links for "Plugins", "Advanced", "Docs", and "Logout".

[https://github.com/mitre-attack/attack-arsenal/tree/master/adversary\\_emulation/APT29/CALDERA\\_DIY/evals](https://github.com/mitre-attack/attack-arsenal/tree/master/adversary_emulation/APT29/CALDERA_DIY/evals)

What If I can replicate all that, collect  
the data generated and share it with  
the InfoSec community 🤔 ?

---

Mordor Style!

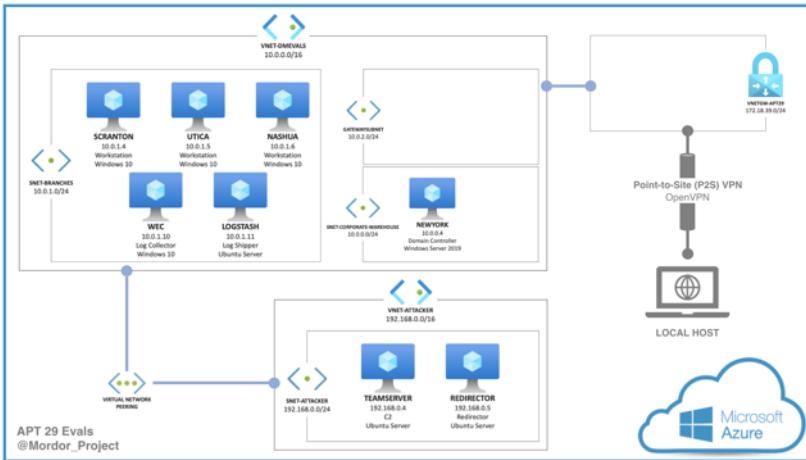
---

MORDOR

# Creating Research Opportunities



## Mordor Datasets



## Mordor Labs

### APT29 Evals Detection Hackathon May 2nd, 2020

[launch](#) [binder](#)

Place for resources used during the Mordor Detection hackathon event featuring APT29 ATT&CK evals datasets.

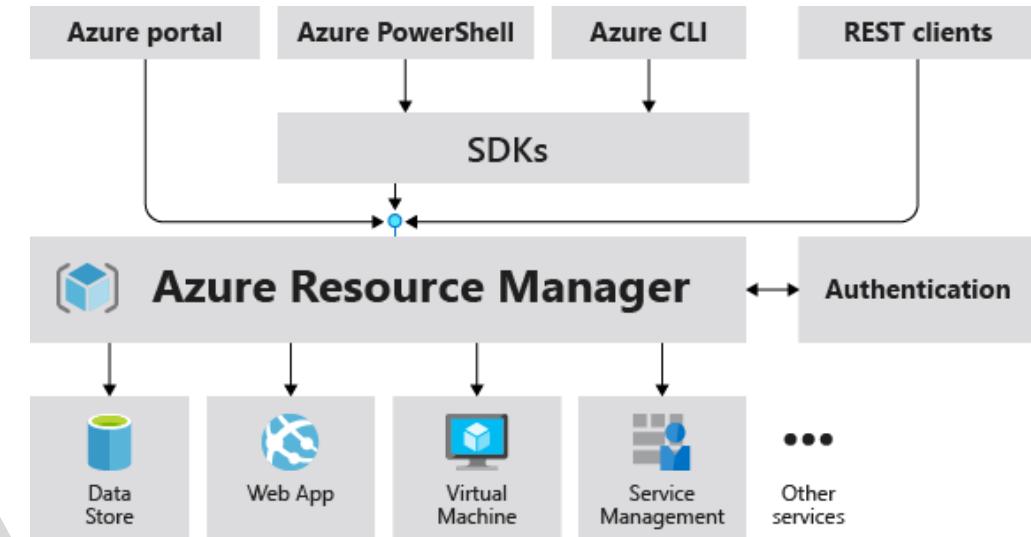
### Agenda

Time	Topic	Session	Type
10:00 - 10:10	Greet the community	General	Live Team Event
10:10 - 10:20	Getting started and Guidelines	General	Live Team Event
10:20 - 10:40	APT29 Environment & Datasets Overview	General	Live Team Event
10:40 - 11:30	Open infrastructure for open research!	General	Live Team Event
11:30 - 12:00	Break	Break	Break

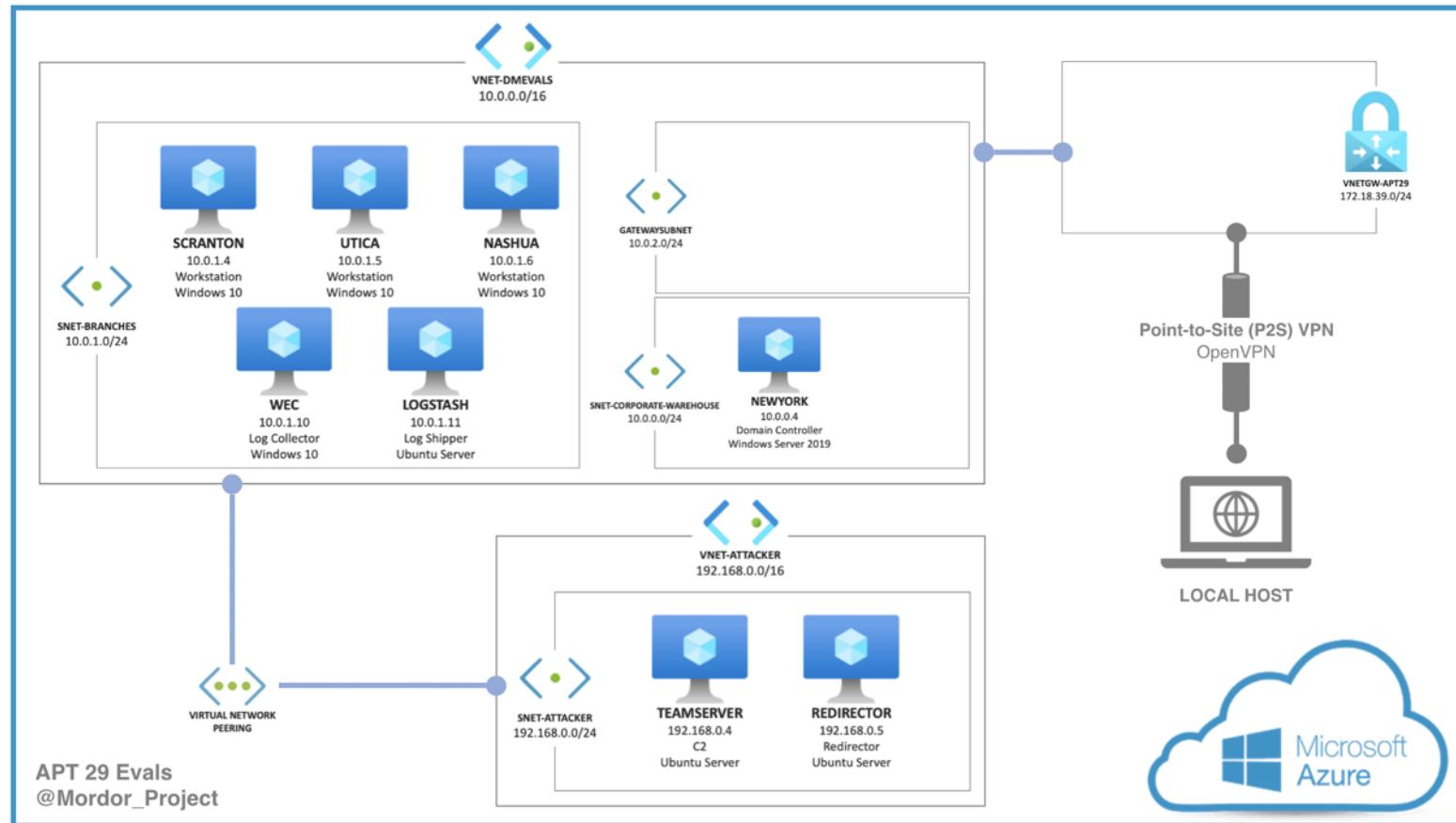
# Mordor Labs 🔥

Cloud Templates and scripts to deploy network environments **exclusively** to generate datasets for the Mordor project.

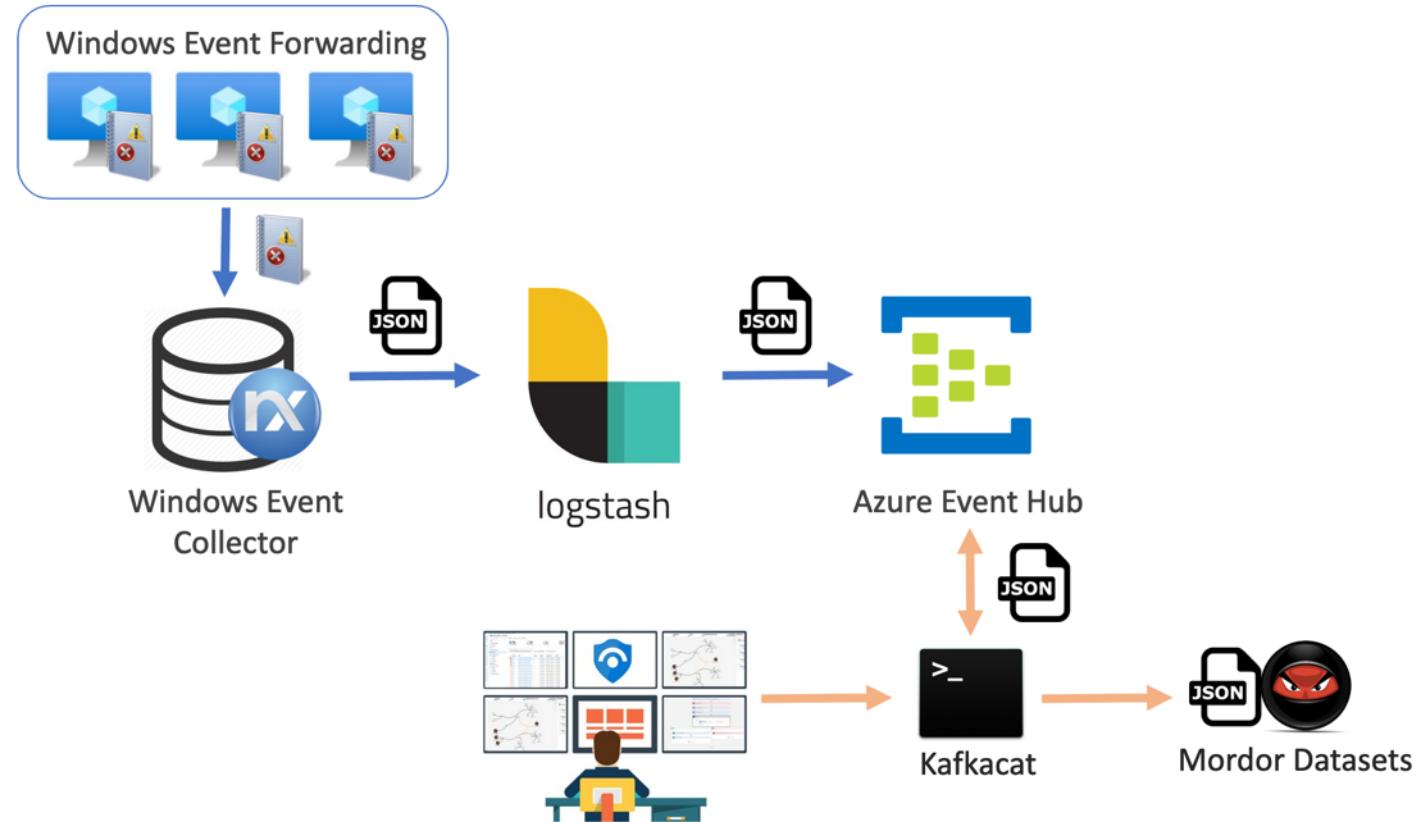
- Azure Resource Manager (ARM) Templates
- AWS Cloud Formation Templates
- Blacksmith Initiative:
  - <https://github.com/hunters-forge/Blacksmith>
- Building all future ATT&CK Evals environments 🍺 (would you like to help?)



# Mordor Labs – APT 29 Network

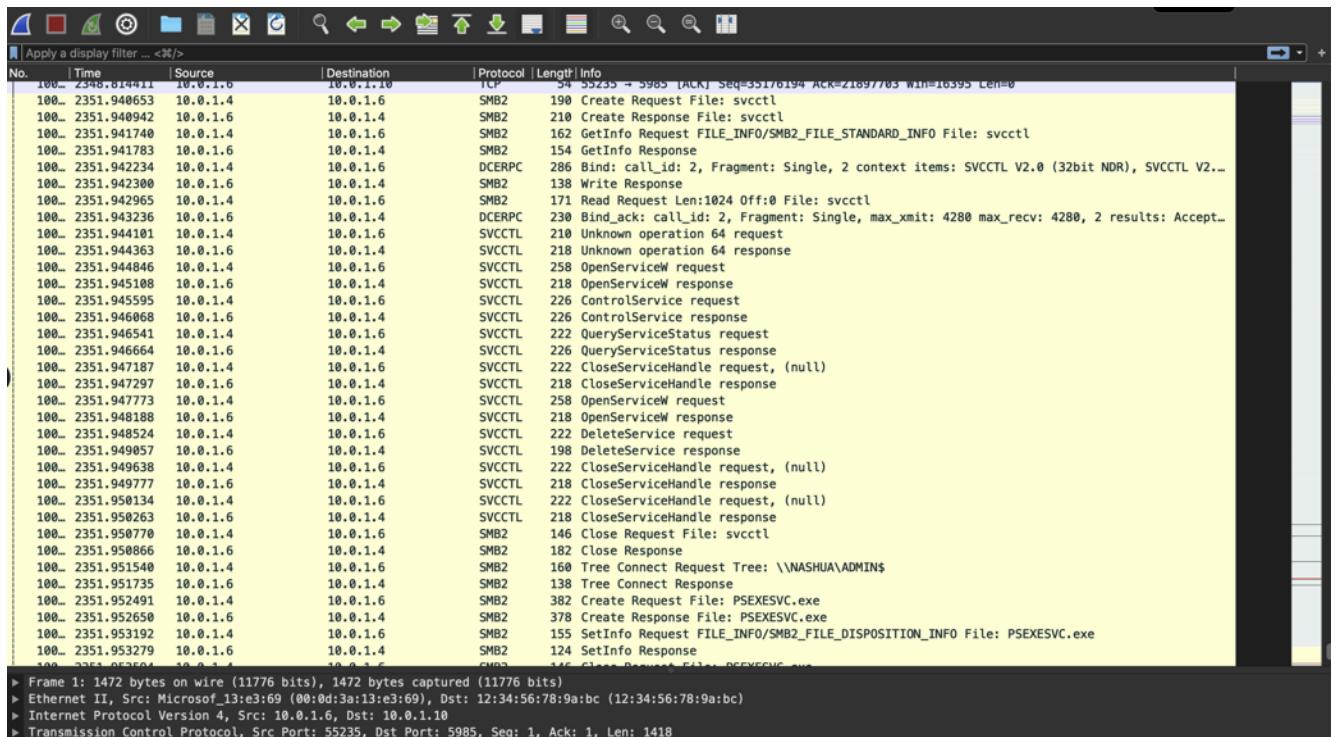


# Mordor Labs – Host Telemetry



# Mordor Labs – Network Telemetry

- netsh trace start capture=yes  
traceFile=\$FILE fileMode=single  
persistent=yes maxSize=0  
overwrite=yes
- pktmon start --etw -p 0 -l real-time (Windows 10 2004)
- Azure Network Watcher Agent extension for Windows



The screenshot shows a NetworkMiner capture window displaying a list of network packets. The columns include No., Time, Source, Destination, Protocol, Length, and Info. The traffic is primarily SMB2 requests between two hosts, with some DCERPC and SVCCTL requests. The 'Info' column provides detailed descriptions of each packet's purpose, such as 'Create Request File: svcctrl' or 'GetInfo Request FILE\_INFO/SMB2\_FILE\_STANDARD\_INFO File: svcctrl'. The bottom status bar indicates the first frame details: Frame 1: 1472 bytes on wire (11776 bits), 1472 bytes captured (11776 bits), Ethernet II, Src: Microsoft\_13:e3:69 (00:0d:3a:13:e3:69), Dst: 12:34:56:78:9a:bc (12:34:56:78:9a:bc), Internet Protocol Version 4, Src: 10.0.1.6, Dst: 10.0.1.10, Transmission Control Protocol, Src Port: 55235, Dst Port: 5985, Seq: 1, Ack: 1, Len: 1418.

No.	Time	Source	Destination	Protocol	Length	Info
100...	2351.9404411	10.0.1.6	10.0.1.10	TCP	54	35235 → 5985 [ACK] Seq=35176194 ACK=21897703 Win=16395 Len=0
100...	2351.940653	10.0.1.4	10.0.1.6	SMB2	190	Create Request File: svcctrl
100...	2351.940942	10.0.1.6	10.0.1.4	SMB2	210	Create Response File: svcctrl
100...	2351.941740	10.0.1.4	10.0.1.6	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_STANDARD_INFO File: svcctrl
100...	2351.941783	10.0.1.6	10.0.1.4	SMB2	154	GetInfo Response
100...	2351.942234	10.0.1.4	10.0.1.6	DCERPC	286	Bind: call_id: 2, Fragment: Single, 2 context items: SVCCTL V2.0 (32bit NDR), SVCCTL V2...
100...	2351.942308	10.0.1.6	10.0.1.4	SMB2	138	Write Response
100...	2351.942965	10.0.1.4	10.0.1.6	SMB2	171	Read Request Len:1024 Off:0 File: svcctrl
100...	2351.943236	10.0.1.6	10.0.1.4	DCERPC	230	Bind_ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280, 2 results: Accept...
100...	2351.944181	10.0.1.4	10.0.1.6	SVCCTL	218	Unknown operation 64 request
100...	2351.944363	10.0.1.6	10.0.1.4	SVCCTL	218	Unknown operation 64 response
100...	2351.944846	10.0.1.4	10.0.1.6	SVCCTL	258	OpenServiceW request
100...	2351.945108	10.0.1.6	10.0.1.4	SVCCTL	218	OpenServiceW response
100...	2351.945595	10.0.1.4	10.0.1.6	SVCCTL	226	ControlService request
100...	2351.946066	10.0.1.6	10.0.1.4	SVCCTL	226	ControlService response
100...	2351.946561	10.0.1.4	10.0.1.6	SVCCTL	222	QueryServiceStatus request
100...	2351.946661	10.0.1.6	10.0.1.4	SVCCTL	226	QueryServiceStatus response
100...	2351.947187	10.0.1.4	10.0.1.6	SVCCTL	222	CloseServiceHandle request, (null)
100...	2351.947297	10.0.1.6	10.0.1.4	SVCCTL	218	CloseServiceHandle response
100...	2351.947773	10.0.1.4	10.0.1.6	SVCCTL	258	OpenServiceW request
100...	2351.948184	10.0.1.6	10.0.1.4	SVCCTL	218	OpenServiceW response
100...	2351.948524	10.0.1.4	10.0.1.6	SVCCTL	222	DeleteService request
100...	2351.949857	10.0.1.6	10.0.1.4	SVCCTL	198	DeleteService response
100...	2351.949638	10.0.1.4	10.0.1.6	SVCCTL	222	CloseServiceHandle request, (null)
100...	2351.949777	10.0.1.6	10.0.1.4	SVCCTL	218	CloseServiceHandle response
100...	2351.950134	10.0.1.4	10.0.1.6	SVCCTL	222	CloseServiceHandle request, (null)
100...	2351.950263	10.0.1.6	10.0.1.4	SVCCTL	218	CloseServiceHandle response
100...	2351.950770	10.0.1.4	10.0.1.6	SMB2	146	Close Request File: svcctrl
100...	2351.950866	10.0.1.6	10.0.1.4	SMB2	182	Close Response
100...	2351.951540	10.0.1.4	10.0.1.6	SMB2	160	Tree Connect Request Tree: \\NASHUA\ADMIN\$
100...	2351.951735	10.0.1.6	10.0.1.4	SMB2	138	Tree Connect Response
100...	2351.952491	10.0.1.4	10.0.1.6	SMB2	382	Create Request File: PSEXEVSC.exe
100...	2351.952656	10.0.1.6	10.0.1.4	SMB2	378	Create Response File: PSEXEVSC.exe
100...	2351.953192	10.0.1.4	10.0.1.6	SMB2	155	SetInfo Request FILE_INFO/SMB2_FILE_DISPOSITION_INFO File: PSEXEVSC.exe
100...	2351.953279	10.0.1.6	10.0.1.4	SMB2	124	SetInfo Response
100...	2351.953504	10.0.1.4	10.0.1.6	SMB2	145	Close Request File: PSEXEVSC.exe

# Mordor Labs – Network Telemetry

- [https://github.com/OTRF/mordor\\_labs/blob/master/environments/attack-evals/apt29/scripts/Start-Packet-Capture.sh](https://github.com/OTRF/mordor_labs/blob/master/environments/attack-evals/apt29/scripts/Start-Packet-Capture.sh)
- [https://github.com/OTRF/mordor\\_labs/blob/master/environments/attack-evals/apt29/scripts/Stop-Packet-Capture.sh](https://github.com/OTRF/mordor_labs/blob/master/environments/attack-evals/apt29/scripts/Stop-Packet-Capture.sh)

The screenshot shows the Microsoft Azure Network Watcher | Packet capture interface. On the left, there's a sidebar with icons for Overview, Monitoring, Topology, Connection monitor, and Connection monitor (Preview). The main area displays two packet capture jobs:

Name	Target	Storage	Status	Bytes per packet
NASHUA_PCAP	NASHUA	h7eop5gsqelqk	Running	Entire packet (default)
SCRANTON_PCAP	SCRANTON	h7eop5gsqelqk	Running	Entire packet (default)

Below the table, there's a blob storage details panel for a blob named "packetcapture\_00\_05\_38\_79...". The details are as follows:

CREATION TIME	4/29/2020, 8:47:03 PM
TYPE	Append blob
SIZE	348.36 MiB
ACCESS TIER	N/A
ACCESS TIER LAST MODIFIED	N/A
SERVER ENCRYPTED	true
ETAG	0x8D7ECA00553A48C
CONTENT-TYPE	application/octet-stream
CONTENT-MD5	-

# Mordor Labs – Emulation Plans & Videos

	A	B	C	D	E	F	G	H
1	Stage	Technique	Step	Description	hands-on	User	Source	Target
5	Initial Breach	User Execution, Masquerading, Uncommonly Used Port	1.A	The scenario begins with an initial breach, where a legitimate user clicks (T1204) an executable payload (screensaver executable) masquerading as a benign word document (T1036). Once executed, the payload creates a C2 connection over port 1234 (T1065) using the RC4 cryptographic cipher .	Double click `3aka3.doc` on C:\programdata\victim\	pbeesly	SCRANTON	PUPY
6	Initial Breach	Command-Line Interface, PowerShell	1.B	pupy terminal -> CMD -> PowerShell  The attacker then uses the active C2 connection to spawn interactive cmd.exe (T1059) and powershell.exe (T1086) shells.	[pupy] > shell  [pupy (CMD)] > powershell	admin	TEAM SERVER	SCRANTON
7	Rapid Collection and Exfiltration	File and Directory Discovery, Automated Collection, Data from Local System, Data Compressed, Data Staged	2.A	The attacker runs a one-liner command to search for filesystem for document and media files (T1083, T1119), collecting (T1005) and compressing (T1002) content into a single file (T1074).	Paste the following PowerShell 1-liner into the Pupy terminal:  [pupy (PowerShell)] >  \$env:APPDATA;\$files=ChildItem -Path \$env:USERPROFILE\ -Include *.doc,*.xps,*.xls,*.ppt,*.pps,*.wps,*.wpd,*.ods,*.odt,*.lwp,*.jtd,*.pdf,*.zip,*.rai,*.docx,*.url,*.xlsx,*.pptx,*.ppsx,*.pst,*.ost,*.psw,*.pass,*.login,*.admin,*.sifir,*.sifer,*.vpn,*.jpg,*.txt,*.lnk -Recurse -ErrorAction SilentlyContinue   Select -ExpandProperty FullName; Compress-Archive -LiteralPath \$files -CompressionLevel Optimal -DestinationPath \$env:APPDATA\Draft.Zip -Force	admin	TEAM SERVER	SCRANTON

# Mordor Labs – Emulation Plans & Videos

```
Extracted: Guest:aad3b435b514b4eaaad3b435b514b4ee:31abcfef8d16ae931b73c59d7e8c889e8
Extracted: wardog:aad3b435b514b4eaaad3b435b514b4ee:42dd29d36be8f1c975fc869d3bce33e
Extracted: NT AUTHORITY\SYSTEM:aad3b435b514b4eaaad3b435b514b4ee:448e38b42764e6192ede33382a7a98aa
[+] Collecting tokens...
DNEVAL\pbeesly
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\SYSTEM
Window Manager\DWIM-1
Window Manager\DWIM-2
Font Driver Host\UMFD-0
Font Driver Host\UMFD-1
Font Driver Host\UMFD-2
NT AUTHORITY\NETWORK SERVICE
metasploit > execute -f powershell.exe -i -h
Process 3852 created.
Channel 3 created,
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\windows\system32> cd "C:\Program Files\SysinternalsSuite"
cd "C:\Program Files\SysinternalsSuite"          0
PS C:\Program Files\SysinternalsSuite> Move-Item .\psversion.txt psversion.ps1
Move-Item .\psversion.txt psversion.ps1
PS C:\Program Files\SysinternalsSuite> .\psversion.ps1
.\psversion.ps1
PS C:\Program Files\SysinternalsSuite> Invoke-ScreenCapture;Start-Sleep -Seconds 3;View-Job -JobName "Screenshot"
Invoke-ScreenCapture;Start-Sleep -Seconds 3;View-Job -JobName "Screenshot"



| <u>ID</u> | <u>Name</u> | <u>PSJobTypeName</u> | <u>State</u> | <u>HasMoreData</u> | <u>Location</u> | <u>Command</u> |
|-----------|-------------|----------------------|--------------|--------------------|-----------------|----------------|
| 1         | Screenshot  | BackgroundJob        | Running      | True               | localhost       | ...            |


```

<https://medium.com/threat-hunters-forge/mordor-labs-part-2-executing-att-ck-apt29-evals-emulation-plan-day1-17fae7a81229>

# @Mordor\_Project 😈

- The Mordor project provides pre-recorded security events generated by simulated adversarial techniques in the form of JavaScript Object Notation (JSON) files for easy consumption.
- The pre-recorded data is categorized by platforms, adversary groups, tactics and techniques defined by the MITRE ATT&CK Framework.
- The pre-recorded data represents not only specific known malicious events but additional context/events that occur around it.
- I hope it becomes the official Data Repository for the InfoSec Community 🤘
- Website: <https://mordordatasets.com/introduction>



# Mordor Datasets – APT29 Eval (Host)

## Datasets

Type	Scenario	Dataset	Size	Timestamp
Host	Day 1	<a href="#">apt29_evals_day1_manual.zip</a>	367M	2020-05-01225525
Host	Day 2	<a href="#">apt29_evals_day2_manual.zip</a>	1.6GB	2020-05-02035409

# Mordor Datasets – APT29 Eval (Host)

## Host Day 1 Summary

Channel	count	%
Microsoft-Windows-Sysmon/Operational	143884	73.4
Security	28627	14.6
security	12375	6.3
Microsoft-Windows-PowerShell/Operational	5694	2.9
Windows PowerShell	5285	2.7
System	91	0.0
Microsoft-Windows-WMI-Activity/Operational	90	0.0
Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational	15	0.0
Microsoft-Windows-Firewall With Advanced Security/Firewall	10	0.0
Microsoft-Windows-TerminalServices-LocalSessionManager/Operational	9	0.0
Microsoft-Windows-Bits-Client/Operational	1	0.0

# Mordor Datasets – APT29 Eval (Host)

## Host Day 2 Summary

Channel	count	%
Microsoft-Windows-Sysmon/Operational	407265	69.3
Windows PowerShell	69084	11.8
Microsoft-Windows-PowerShell/Operational	60372	10.3
Security	27207	4.6
security	22854	3.9
Microsoft-Windows-Windows Firewall With Advanced Security/Firewall	292	0.0
System	105	0.0
Microsoft-Windows-WMI-Activity/Operational	81	0.0
Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational	14	0.0
Microsoft-Windows-TerminalServices-LocalSessionManager/Operational	10	0.0
Microsoft-Windows-Bits-Client/Operational	2	0.0

# Mordor Datasets – APT29 Eval (Network)

hunters-forge / mordor

Code Issues 5 Pull requests 1 Actions Projects 0 Wiki Security 0 Insights Settings

Branch: master ➔ mordor / datasets / large / apt29 / day1 / zeek / individual\_zeek\_logs / Create new file Upload files Find file History

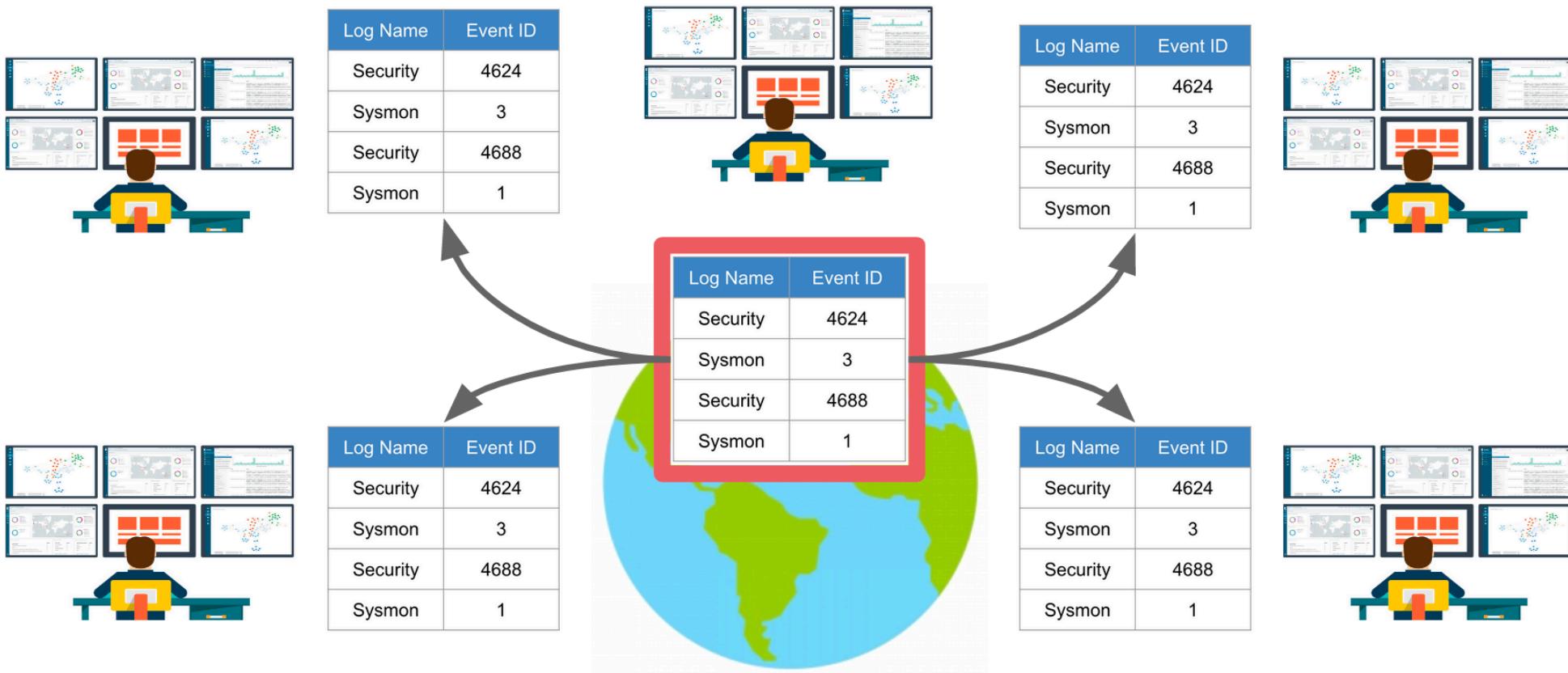
Cyb3rWard0g apt29 ✓ Latest commit 1cf0701 12 days ago

..

<a href="#">NASHUA_conn.log</a>	apt29	12 days ago	
<a href="#">NASHUA_dce_rpc.log</a>	apt29	12 days ago	
<a href="#">NASHUA_dns.log</a>	apt29	12 days ago	
<a href="#">NASHUA_dpd.log</a>	apt29	12 days ago	
<a href="#">NASHUA_files.log</a>	apt29	12 days ago	
<a href="#">NASHUA_kerberos.log</a>	apt29	12 days ago	
<a href="#">NASHUA_notice.log</a>	apt29	12 days ago	
<a href="#">NASHUA_smb_files.log</a>	apt29	12 days ago	
<a href="#">NASHUA_smb_mapping.log</a>	apt29	12 days ago	

<https://github.com/hunters-forge/mordor/tree/master/datasets/large/apt29>

# Mordor Datasets- Empowering Researchers



# Detection Hackathon ✨

- A virtual event to get together and learn about adversary techniques through data!
- Main goals
  - Collaborate and learn some basic data analysis techniques together 🌎
  - Explore different analytics platforms and share feedback (what works and what doesn't)
  - Contribute to other open source projects!
- Not only # of contributions, but how many people we help and meet 🍻
- Making the difference by providing data and leveraging the amazing ATT&CK resources 💥!

Roberto Rodriguez  
@Cyb3rWard0g

APT29 Evals Detection Hackathon! 🏠 Join me on May 2nd to learn about adversarial techniques through free telemetry (e.g Sysmon) and help develop detection rules (e.g  $\#sigma$ ) A @Mordor\_Project Event! 😈🍻

Info: [mordordatasets.com/hackathons/apt...](https://mordordatasets.com/hackathons/apt...)

Registration: [bit.ly/APT29Detection...](https://bit.ly/APT29Detection...)

ATT&CK @MITREattack · Apr 21

The ATT&CK Evaluations Team just released the APT29 Evaluation results, DIY Eval profile, and a Joystick update on attackevals.mitre.org. Check out [medium.com/mitre-attack/a...](https://medium.com/mitre-attack/a...) to learn more about the evaluation process.

[Show this thread](#)

5:46 PM · Apr 21, 2020 · Twitter Web App

# Detection Hackathon – APT29 Evals

OTRF / [detection-hackathon-apt29](#)

Unwatch 6 Star 44 Fork 13

Code Issues 48 Pull requests 1 Actions Projects 2 Wiki Security 0 Insights Settings

Place for resources used during the Mordor Detection hackathon event featuring APT29 ATT&CK evals datasets Edit

Manage topics

25 commits 1 branch 0 packages 0 releases 3 contributors GPL-3.0

Branch: master New pull request Create new file Upload files Find file Clone or download

File / Commit	Description	Date
Cyb3rWard0g Merge pull request #51 from neu5ron/master ...	Latest commit 133e973 13 days ago	
SIEMs/HELK	Updated docs	15 days ago
datasets	rename	14 days ago
emulation-plans	Updated Emulation plan, host event logs and README	16 days ago
notebooks	Update notebooks	16 days ago
rules/windows/sysmon	initial rule	15 days ago
.gitattributes	unlfs	17 days ago
.gitignore	Uploaded Emulation Plan Day 1	18 days ago
Dockerfile	Notebooks and Docker	16 days ago
LICENSE	Initial commit	19 days ago
README.md	Update README.md	16 days ago

<https://github.com/OTRF/detection-hackathon-apt29>

# Detection Hackathon – APT29 Evals

2 Open ✓ 0 Closed		Sort ▾
<b>APT29 - Day 2</b> <small>🕒 Updated 16 days ago</small>	The second scenario (executed with PoshC2 and custom tooling) focuses on a very targeted and methodical breach, beginning with the execution of a specially crafted payload designed to scrutinize the target environment before executing. The scenario continues through a low and slow takeover of the initial target and eventually the entire domain. Both scenarios include executing previously established persistence mechanisms after a simulated time lapse to further the scope of the breach.	...
<b>APT29 - Day1</b> <small>🕒 Updated 16 days ago</small>	The first scenario (executed with Pupy, Meterpreter, and custom tooling) begins with the execution of a payload delivered by a widespread "spray and pray" spearphishing campaign, followed by a rapid "smash and grab" collection and exfiltration of specific file types. After completing the initial data theft, the value of the target is realized, and the adversary drops a secondary, stealthier toolkit used to further explore and compromise the target network.	...

# Detection Hackathon – APT29 Eval

The screenshot shows a GitHub project board titled "APT29 - Day1" with a progress bar indicating it was updated 16 days ago. The board has four columns: "Initial Breach", "Collection and Exfiltration", "Deploy Stealth Toolkit", and "Defense Evasion and Discovery". Each column contains several cards representing specific detection techniques, each with a title, description, and a note indicating it was opened by "Cyb3rWard0g".

Initial Breach	Collection and Exfiltration	Deploy Stealth Toolkit	Defense Evasion and Discovery
1.A) User Execution, Masquerading, Uncommonly Used Port #1 opened by Cyb3rWard0g	2.A) File and Directory Discovery, Automated Collection, Data from Local System, Data Compressed, Data Staged #3 opened by Cyb3rWard0g	3.A) Remote File Copy, Obfuscated Files or Information #5 opened by Cyb3rWard0g	4.A) PowerShell, Deobfuscate/Decode Files or Information #8 opened by Cyb3rWard0g
1.B) Command-Line Interface, PowerShell #2 opened by Cyb3rWard0g	2.B) Exfiltration Over Command and Control Channel #4 opened by Cyb3rWard0g	3.B) Component Object Model Hijacking, Bypass User Account Control, Commonly Used Port, Standard Application Layer Protocol, Standard Cryptographic Protocol #6 opened by Cyb3rWard0g	4.B) Process Discovery, File Deletion #9 opened by Cyb3rWard0g
	7.A) Screen Capture, Clipboard Data, Input Capture #16 opened by Cyb3rWard0g	3.C) Modify Registry #7 opened by Cyb3rWard0g	4.C) File and Directory Discovery, System Owner/User Discovery, System Information Discovery, System Network Configuration Discovery, Process Discovery, Security Software Discovery, Permission Groups Discovery, Execution through API #10 opened by Cyb3rWard0g
	7.B) Data from Local System, Data Compressed, Data Encrypted, Exfiltration Over Alternative Protocol #17 opened by Cyb3rWard0g		

<https://github.com/OTRF/detection-hackathon-apt29/projects/1>

# Detection Hackathon – APT29 Eval ❤



Cyb3rWard0g commented 7 days ago • edited

Author Member

## 3.B.1 Component Object Model Hijacking

Procedure: Modified the Registry to enable COM hijacking of sdclt.exe using PowerShell

Criteria: Addition of the DelegateExecute subkey in HKCU\Software\Classes\Folder\shell\open\ command

Sysmon Logs

```
SELECT Message
FROM apt29Host
WHERE Channel = "Microsoft-Windows-Sysmon/Operational"
    AND EventID = 13
    AND LOWER(TargetObject) RLIKE '.*\\\\\\\\\\folder\\\\\\\\\\shell\\\\\\\\\\open\\\\\\\\\\com
```

Results

```
|Registry value set:
RuleName: -
EventType: SetValue
UtcTime: 2020-05-02 02:58:30.649
ProcessGuid: {47ab858c-e18b-5eac-b103-000000000400}
ProcessId: 6868
Image: C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetObject: HKU\S-1-5-21-1830255721-3727074217-2423397540-1107_Classes\Folder\shell\o
Details: (Empty)|
```



Cyb3rWard0g commented 7 days ago

Member Author

## 3.B.2 Bypass User Account Control

### Detection Category (Telemetry)

Procedure: Executed elevated PowerShell payload

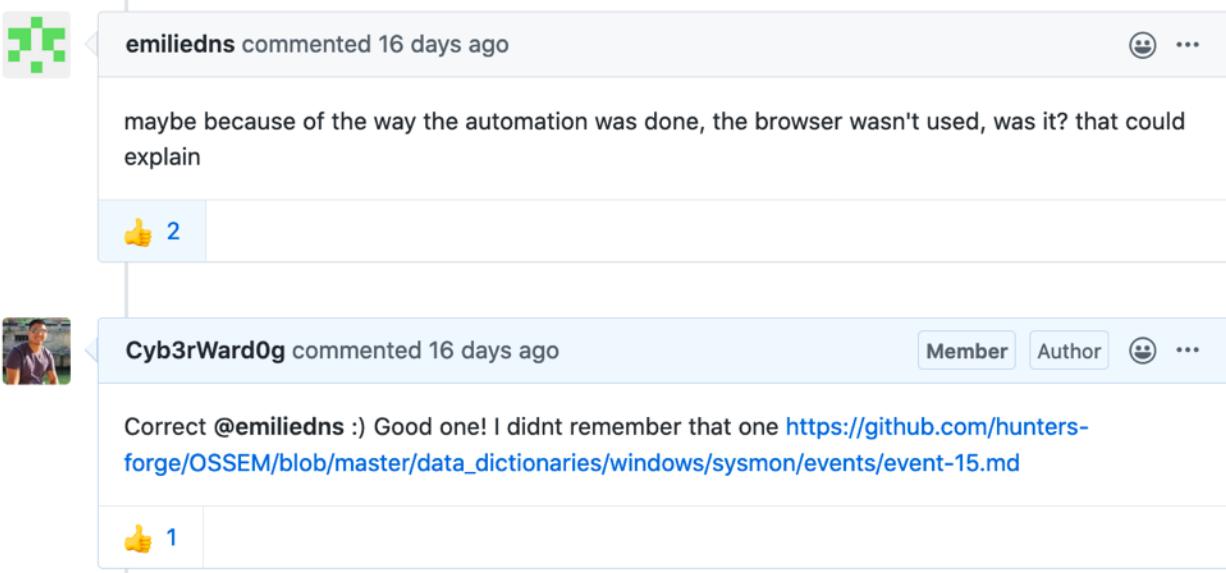
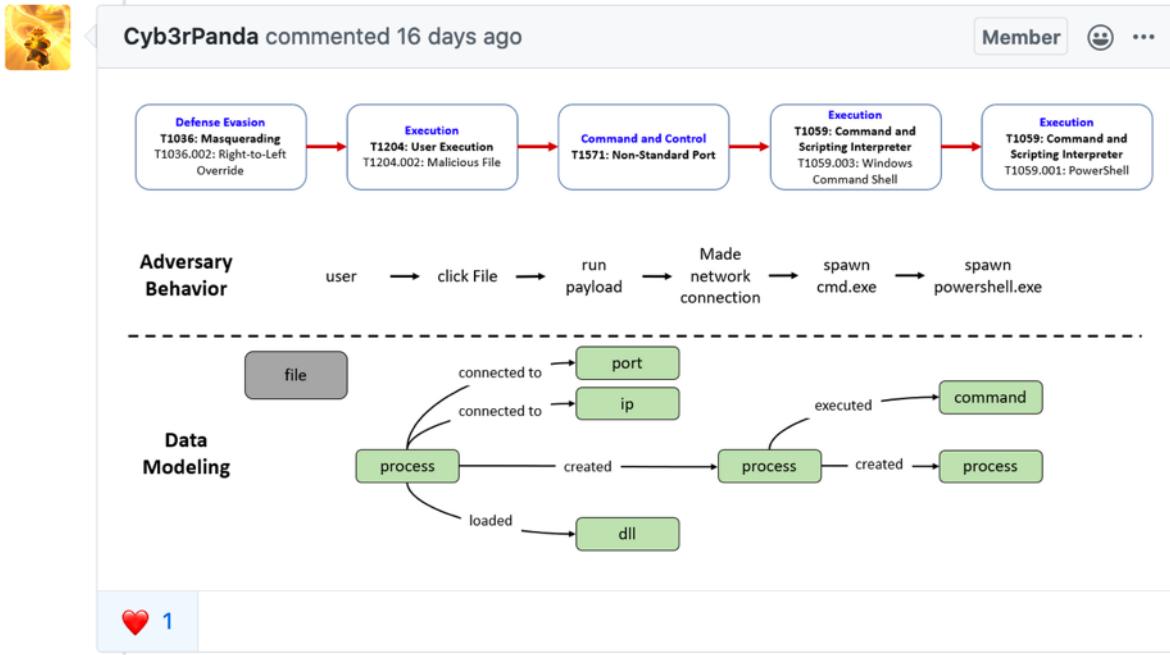
Criteria: High integrity powershell.exe spawning from control.exe (spawned from sdclt.exe)

```
bypassUAC = spark.sql(
    """
    SELECT a.Image, a.CommandLine
    FROM apt29Table a
    INNER JOIN (
        SELECT ProcessGuid
        FROM apt29Table
        WHERE Channel = "Microsoft-Windows-Sysmon/Operational"
            AND EventID = 1
            AND LOWER(Image) LIKE "%control.exe"
            AND LOWER(ParentImage) LIKE "%sdclt.exe"
    ) b
    ON a.ParentProcessGuid = b.ProcessGuid
    WHERE a.Channel = "Microsoft-Windows-Sysmon/Operational"
        AND a.EventID = 1
        AND a.IntegrityLevel = "High"
    """
)
bypassUAC.show(truncate = False, vertical = True)
```

Results

```
Image | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
CommandLine | "PowerShell.exe" -noni -noexit -ep bypass -window hidden -c "sal a New-0
```

# Detection Hackathon – APT29 Eval ❤



# Detection Hackathon – APT29 Evals ❤



neu5ron commented 14 days ago

Member



...

alright here start of my rule, will keep working this with more operations:

```
title: Domain Enumeration Network Reconnaissance Activity
status: experimental
description: Domain enumeration via network reconnaissance. Seen in APT 29 and other co
references:
  - "https://github.com/OTRF/detection-hackathon-apt29/issues/37"
author: '@neu5ron (Nate Guagenti)'
date: 2020/05/03
modified: 2020/05/03
tags:
  - attack.discovery
  - attack.t1087
  - attack.t1082
logsource:
  product: zeek
  service: dce_rpc
detection:
  selection:
    operation:
      - SamrLookupIdsInDomain
      - SamrGetGroupsForUser
    timeframe: 30s
    condition: selection | count(operation) by src_ip > 4
falsepositives:
  - False positives depend on scripts and administrative tools used in the monitored
level: medium
```



DarthRaki commented 12 days ago • edited

...

Okay my First ever sigma rule! this was fun

```
title: Data from Local System, Data Compressed, Data Encrypted, Exfiltration Over Alter
author: Greg Howell
date: 2020/04/05
references:
  - https://github.com/OTRF/detection-hackathon-apt29/issues/17
tags:
  - attack.data_exfiltration
  - attack.t1002
  - attack.t1005
  - attack.t1022
logsource:
  product: zeek
  service: files
  service: http
detection:
  selection1:
    uri:
      - '*.7z'
      - '*.zip'
      - '*.rar'
  selection2:
    mime_types: '*compressed'
  selection3:
    filetype: '*compressed'
  selection4:
    http.bodyMagic: '*compressed'
    condition: selection1 and selection2 or selection3 or selection4
falsepositives:
  - nothing observed so far
level: high
```



# Detection Hackathon – APT29 Eval ❤



neu5ron commented 14 days ago

alright here start of my rule, will keep w

```
title: Domain Enumeration Network
status: experimental
description: Domain enumeration v
references:
  - "https://github.com/OTRF/de
author: '@neu5ron (Nate Guagenti)
date: 2020/05/03
modified: 2020/05/03
tags:
  - attack.discovery
  - attack.t1087
  - attack.t1082
logsource:
  product: zeek
  service: dce_rpc
detection:
  selection:
    operation:
      - SamrLookupIdsInDoma
      - SamrGetGroupsForUse
  timeframe: 30s
  condition: selection | count(
falsepositives:
  - False positives depend on s
level: medium
```

1

neu5ron commented 14 days ago

Member



...

@Cyb3rWard0g I can't find the executable download anywhere if I should move this somewhere else let me know, but here is a sigma rule for that:

```
title: Executable from Webdav
status: experimental
date: 2020/05/01
description: Detects executable access via webdav6
author: 'Adam Swan'
references:
  - http://carnal0wnage.attackresearch.com/2012/06/webdav-server-to-download-custom.h
  - https://github.com/OTRF/detection-hackathon-apt29
tags:
  - attack.command_and_control
  - attack.T1043
logsource:
  category: proxy
detection:
  selection_webdav:
    - c-useragent: '*WebDAV*'
    - c-uri: '*webdav*'
  selection_executable:
    - resp_mime_types: '*dosexec*'
    - c-uri: '*.exe'
  condition: selection_webdav AND selection_executable
falsepositives:
  - unknown
level: medium
```

1

What can we do with the results?  
(Still a work in progress..)

---

# @HunterPlaybook

- A community-based open source project developed to share threat hunting concepts and aid the development of techniques and hypothesis for hunting campaigns by leveraging security event logs from diverse operating systems.
- Sharing research via open infrastructure (@mybinderteam) with the InfoSec Community 
- Website: <https://threathunterplaybook.com/introduction.html>

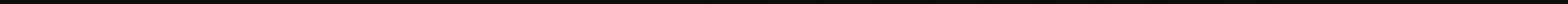


# Threat Hunter Playbook: Documenting..

```
vendor: OTR Community
step: 3.B.2
procedure: Executed elevated PowerShell payload
criteria: High integrity powershell.exe spawning from control.exe (spawned from sdclt.exe)
technique:
  name: Bypass User Account Control
  id: T1088
issue: https://github.com/OTRF/detection-hackathon-apt29/issues/6
detections:
  - main_type: Telemetry
    modifier_type:
    description: Telemetry showed control.exe creating a high integrity powershell.exe.
    reference:
    queries:
      - id: 6C8780E9-E6AF-4210-8EA0-72E9017CEE7D
        data_sources:
          - Microsoft-Windows-Sysmon/Operational
        rule_contribution:
        logic: |
          SELECT Message
          FROM apt29Host a
          INNER JOIN (
            SELECT ProcessGuid
            FROM apt29Host
            WHERE Channel = "Microsoft-Windows-Sysmon/Operational"
              AND EventID = 1
              AND LOWER(Image) LIKE "%control.exe"
              AND LOWER(ParentImage) LIKE "%sdclt.exe"
          ) b
          ON a.ParentProcessGuid = b.ProcessGuid
          WHERE a.Channel = "Microsoft-Windows-Sysmon/Operational"
            AND a.EventID = 1
            AND a.IntegrityLevel = "High"
```

[https://github.com/hunters-forge/ThreatHunter-Playbook/blob/master/docs/evals/apt29/steps/3.B.2\\_bypass\\_user\\_account\\_control.yaml](https://github.com/hunters-forge/ThreatHunter-Playbook/blob/master/docs/evals/apt29/steps/3.B.2_bypass_user_account_control.yaml)

Releasing something today



# Threat Hunter Playbook: Creating a Report..



## All Results - Report

Step	Procedure	Criteria	Technique	Detections						
1.A.1	User Pam executed payload rcs.3aka3.doc	The rcs.3aka3.doc process spawning from explorer.exe	User Execution	<table><thead><tr><th>Type</th><th>Notes</th></tr></thead><tbody><tr><td>Telemetry</td><td>Telemetry showed explorer.exe executing rcs.3aka3.doc [1] [2]</td></tr><tr><td>General</td><td>A General detection can be created to show new applications executed on the endpoint by leveraging registry modifications to \Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\CompatibilityAssistant\Store [1]</td></tr></tbody></table>	Type	Notes	Telemetry	Telemetry showed explorer.exe executing rcs.3aka3.doc [1] [2]	General	A General detection can be created to show new applications executed on the endpoint by leveraging registry modifications to \Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\CompatibilityAssistant\Store [1]
Type	Notes									
Telemetry	Telemetry showed explorer.exe executing rcs.3aka3.doc [1] [2]									
General	A General detection can be created to show new applications executed on the endpoint by leveraging registry modifications to \Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\CompatibilityAssistant\Store [1]									

Threat Hunter Playbook

Search this book...

Pre-Hunt Activities

Data Management

Campaign Notebooks

ATT&CK Evaluations

APT 29

All Results - Report

Free Telemetry Notebook

# Threat Hunter Playbook: Creating a Report..

The screenshot shows a web-based Threat Hunter Playbook interface. On the left is a sidebar with a logo of a dog wearing a cap and the text "Threat Hunter Playbook". Below the logo are search and navigation links for "Pre-Hunt Activities", "Campaign Notebooks", and "Targeted Notebooks", along with specific items like "Data Management" and "ATT&CK Evaluations". At the bottom of the sidebar, it says "Powered by Jupyter Book". The main content area has a header "DFD6A782-9BDB-4550-AB6B-525E825B095E". It includes sections for "Data Sources" (listing "Microsoft-Windows-Sysmon/Operational"), "Logic" (containing a SQL query), and "Output" (containing a registry value set). The logic section contains the following SQL query:

```
SELECT Message  
FROM apt29Host  
WHERE Channel = "Microsoft-Windows-Sysmon/Operational"  
AND EventID = 13  
AND TargetObject RLIKE '.*\\\\\\\\\\\\\\\\AppCompatFlags\\\\\\\\\\\\\\\\Compatibility Assistant\\\\\\\\\\\\\\\\Store\\\\\\\\\\\\\\\\'
```

The output section contains the following registry value set:

```
Registry value set:  
RuleName: -  
EventType: SetValue  
UtcTime: 2020-05-02 03:01:29.278  
ProcessGuid: {47ab858c-cc06-5eac-9402-000000000400}  
ProcessId: 1144  
Image: C:\windows\system32\svchost.exe  
TargetObject: HKU\S-1-5-21-1830255721-3727074217-2423397540-1107\Software\Microsoft\Windows NT\Current Version\Compatibility Assistant\Store  
Details: Binary Data
```

[https://threathunterplaybook.com/evals/apt29/detections/1.A.1\\_DFD6A782-9BDB-4550-AB6B-525E825B095E.html](https://threathunterplaybook.com/evals/apt29/detections/1.A.1_DFD6A782-9BDB-4550-AB6B-525E825B095E.html)

# Threat Hunter Playbook: Creating a Notebook..



Threat Hunter Playbook

Search this book...

Pre-Hunt Activities

Data Management

Campaign Notebooks

ATT&CK Evaluations

APT 29

All Results - Report

Free Telemetry Notebook

Targeted Notebooks

Windows

Linux

Mac

Group APT29

Description APT29 is a threat group that has been attributed to the Russian government and has operated since at least 2008. This group reportedly compromised the Democratic National Committee starting in the summer of 2015

Author Open Threat Research - APT29 Detection Hackathon

## Import Libraries

```
from pyspark.sql import SparkSession
```

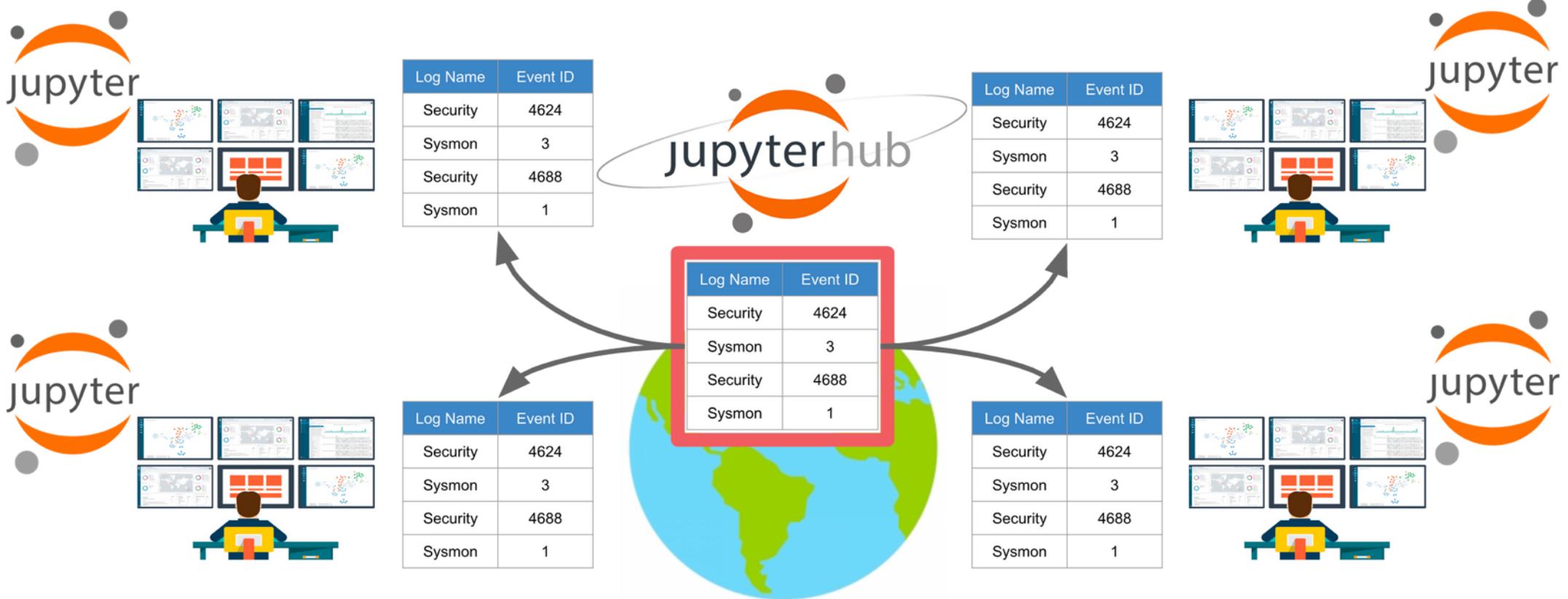
## Start Spark Session

```
spark = SparkSession.builder.getOrCreate()
spark.conf.set("spark.sql.caseSensitive", "true")
```

On this page

- Import Libraries
- Start Spark Session
- Decompress Dataset
- Import Datasets
- Create Temporary SQL View
- Adversary - Detection Steps
- 1.A.1. User Execution
- 1.A.2. Masquerading
- 1.A.3. Uncommonly Used Port
- 1.A.4. Standard Cryptographic Protocol
- 1.B.1. Command-Line Interface
- 1.B.2. PowerShell
- 2.A.1. File and Directory Discovery
- 2.A.2. Automated Collection
- 2.A.3. Data from Local System
- 2.A.4. Data Compressed
- 2.A.5. Data Staged
- 2.B.1. Exfiltration Over Command and Control Channel
- 3.A.1. Remote File Copy
- 3.A.2. Obfuscated Files or Information
- 3.B.1. Component Object Model Hijacking
- 3.B.2. Bypass User Account Control
- 3.B.3. Commonly Used Port

# Threat Hunter Playbook: Empowering others



# Threat Hunter Playbook: Notebook Demo



## Free Telemetry Notebook

Group APT29

Description APT29 is a threat group that has been attributed to the Russian government and has operated since at least 2008. This group reportedly compromised the Democratic National Committee starting in the summer of 2015

Author [Open Threat Research - APT29 Detection Hackathon](#)

[Binder](#) [ThebeLab](#)

Threat Hunter Playbook

Search this book...

Pre-Hunt Activities

Data Management

# Threat Hunter Playbook: Notebook Demo

 binder



Starting repository: hunters-forge/ThreatHunter-Playbook  
/master

You can learn more about building your own Binder repositories in the [Binder community documentation](#).

Build logs hide

```
Found built image, launching...
Launching server...
```

<https://threathunterplaybook.com/notebooks/campaigns/apt29Evals.html>

# Threat Hunter Playbook: Notebook Demo

The screenshot shows a Jupyter Notebook interface with the title "Free Telemetry Notebook". The notebook header includes the Jupyter logo, the name "apt29Evals", and a note "(unsaved changes)". It features a standard toolbar with File, Edit, View, Insert, Cell, Kernel, Help, and various cell type and execution buttons. The top right corner shows "Not Trusted" and "PySpark\_Python3".

The main content area displays the following information:

- Group:** APT29
- Description:** APT29 is a threat group that has been attributed to the Russian government and has operated since at least 2008. This group reportedly compromised the Democratic National Committee starting in the summer of 2015.
- Author:** [Open Threat Research - APT29 Detection Hackathon](#)

**Import Libraries** ¶

```
In [ ]: from pyspark.sql import SparkSession
```

**Start Spark Session**

```
In [ ]: spark = SparkSession.builder.getOrCreate()
spark.conf.set("spark.sql.caseSensitive", "true")
```

<https://threathunterplaybook.com/notebooks/campaigns/apt29Evals.html>

# Open Threat Research

(A community movement)

Coming soon ..



---

# Thank You!

---

@Cyb3rWard0g

@Mordor\_Project

@HunterPlaybook

<https://launchpass.com/threathunting>