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

https://attackevals.mitre.org/

APT29 Eval (Round 2)

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

Scenario 1 / Day 1

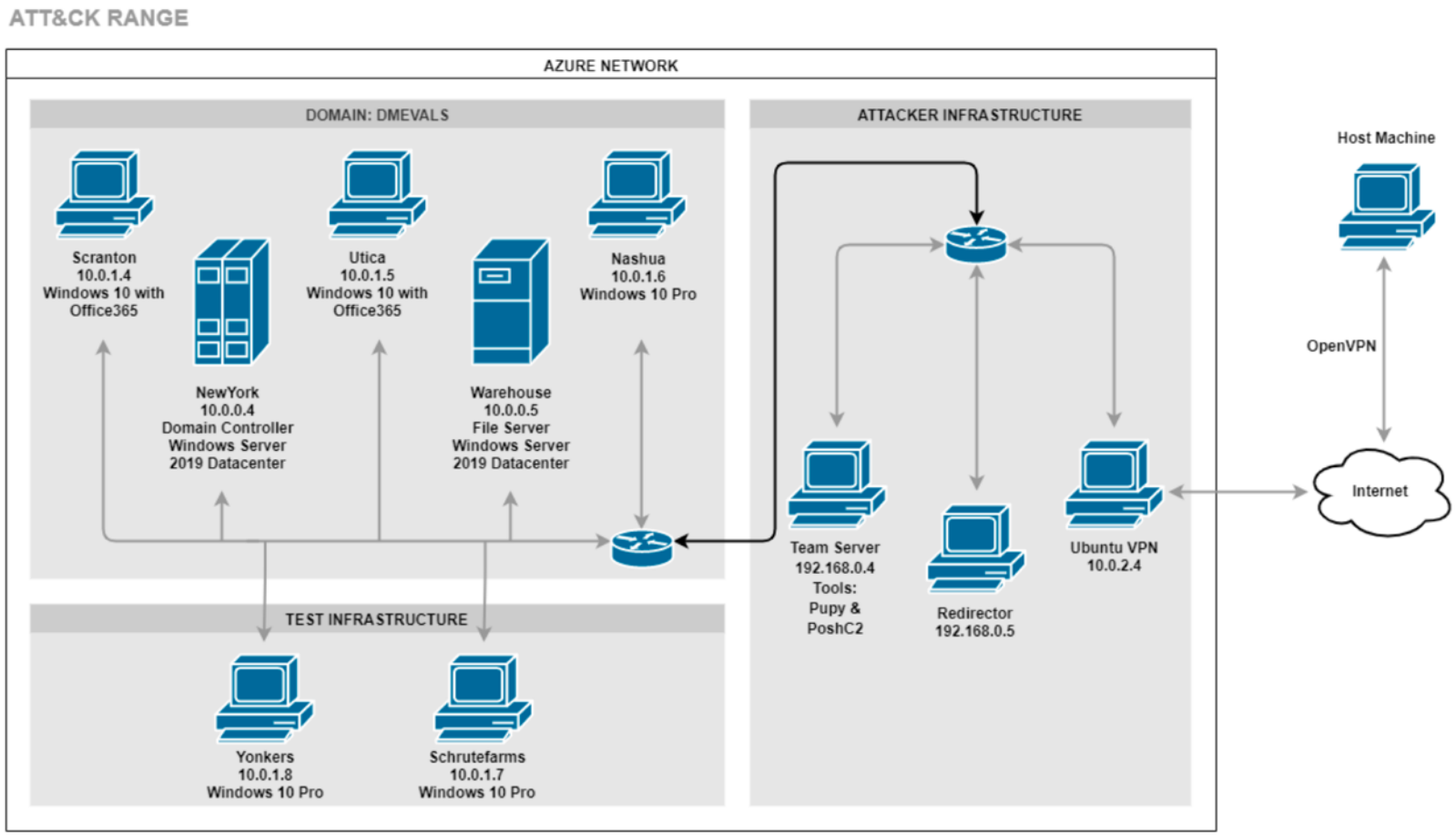
- The first scenario (executed with Pupy, Meterpreter, and custom tooling) begins with the execution of a payload delivered by a widespread "spray and pray" spearphishing campaign.

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

https://attackevals.mitre.org/APT29/

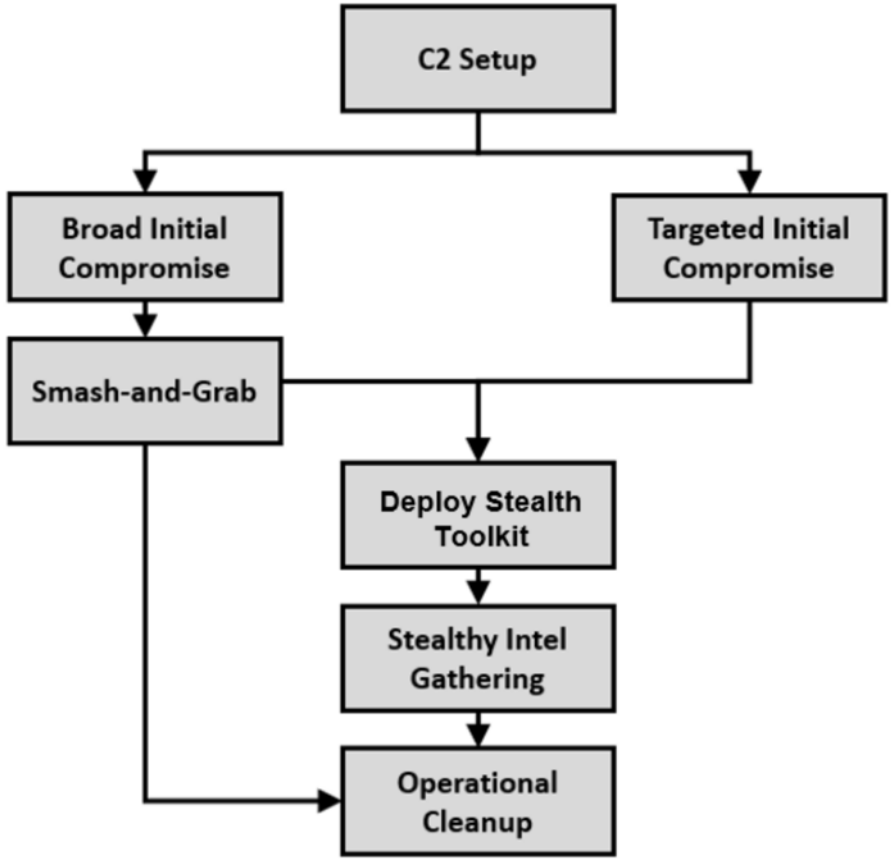
APT29 Eval – Network Design



https://attackevals.mitre.org/APT29/environment.html

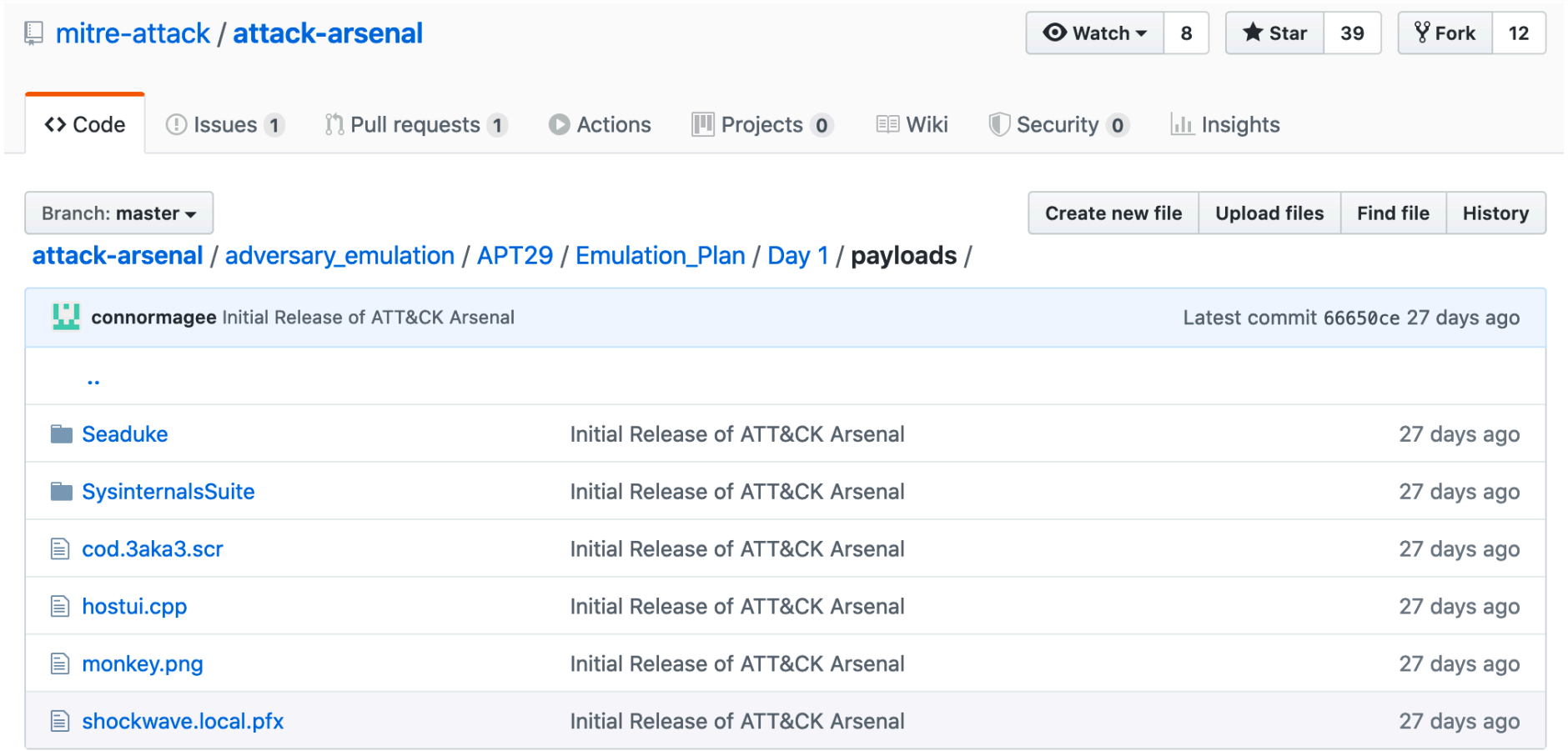
APT29 Evals – Emulation Plans

- 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.



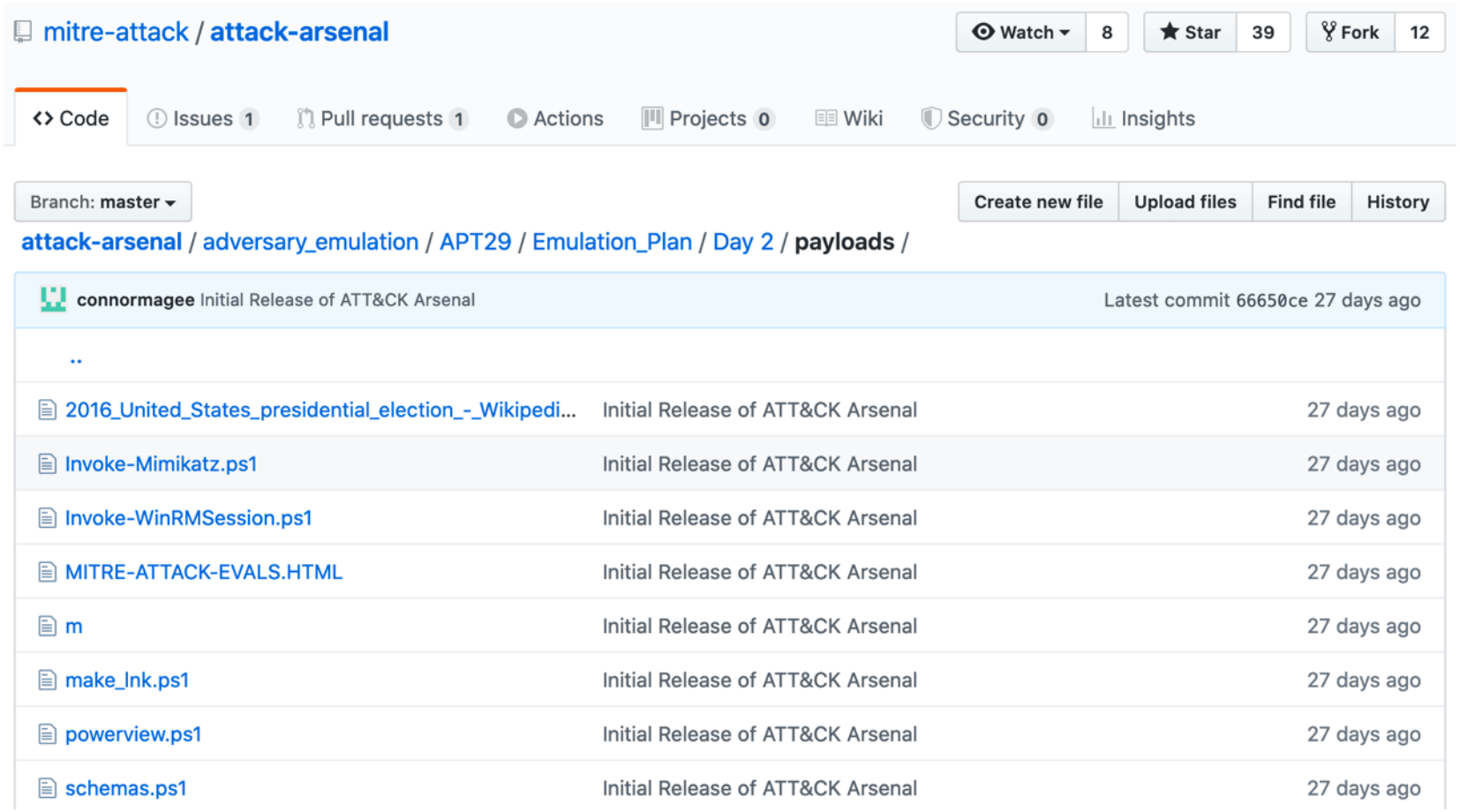
https://github.com/mitre-attack/attack-arsenal/tree/master/adversary_emulation/APT29/Emulation_Plan

APT29 Evals – Emulation Plans – Day 1



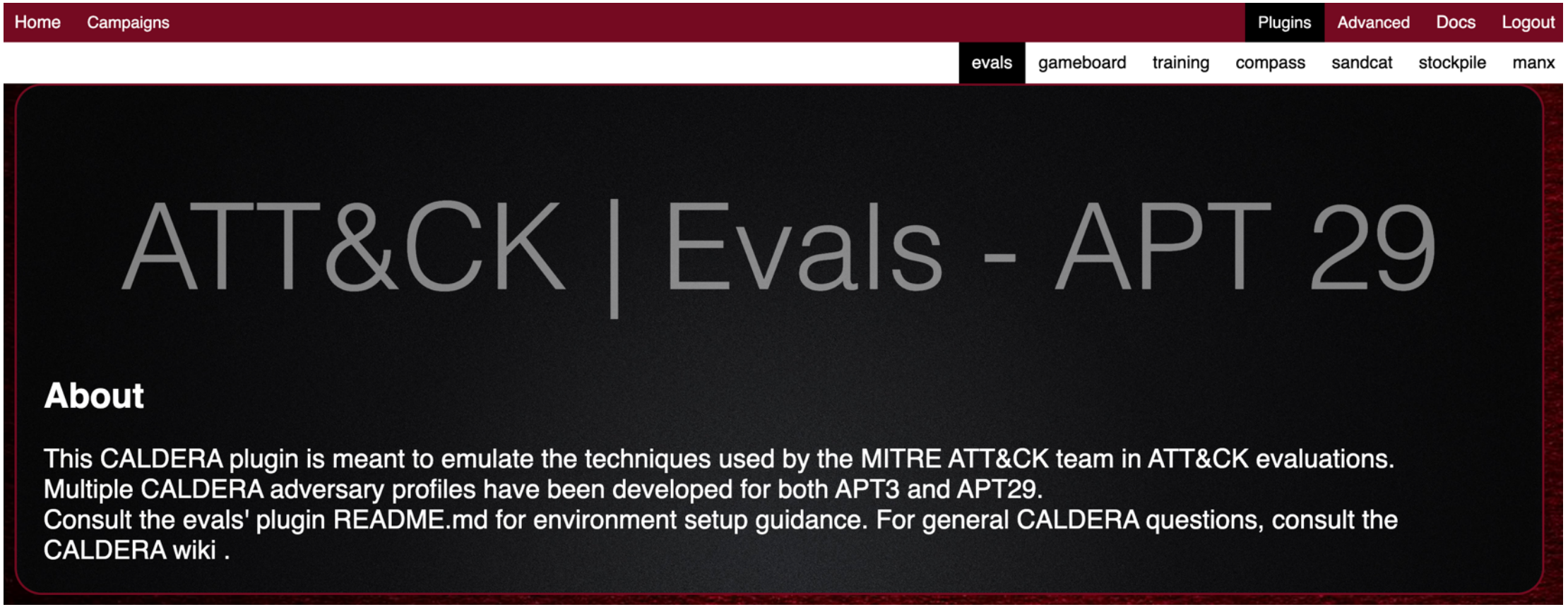
https://github.com/mitre-attack/attack-arsenal/tree/master/adversary_emulation/APT29/Emulation_Plan/Day%201/payloads

APT29 Evals – Emulation Plans – Day 2



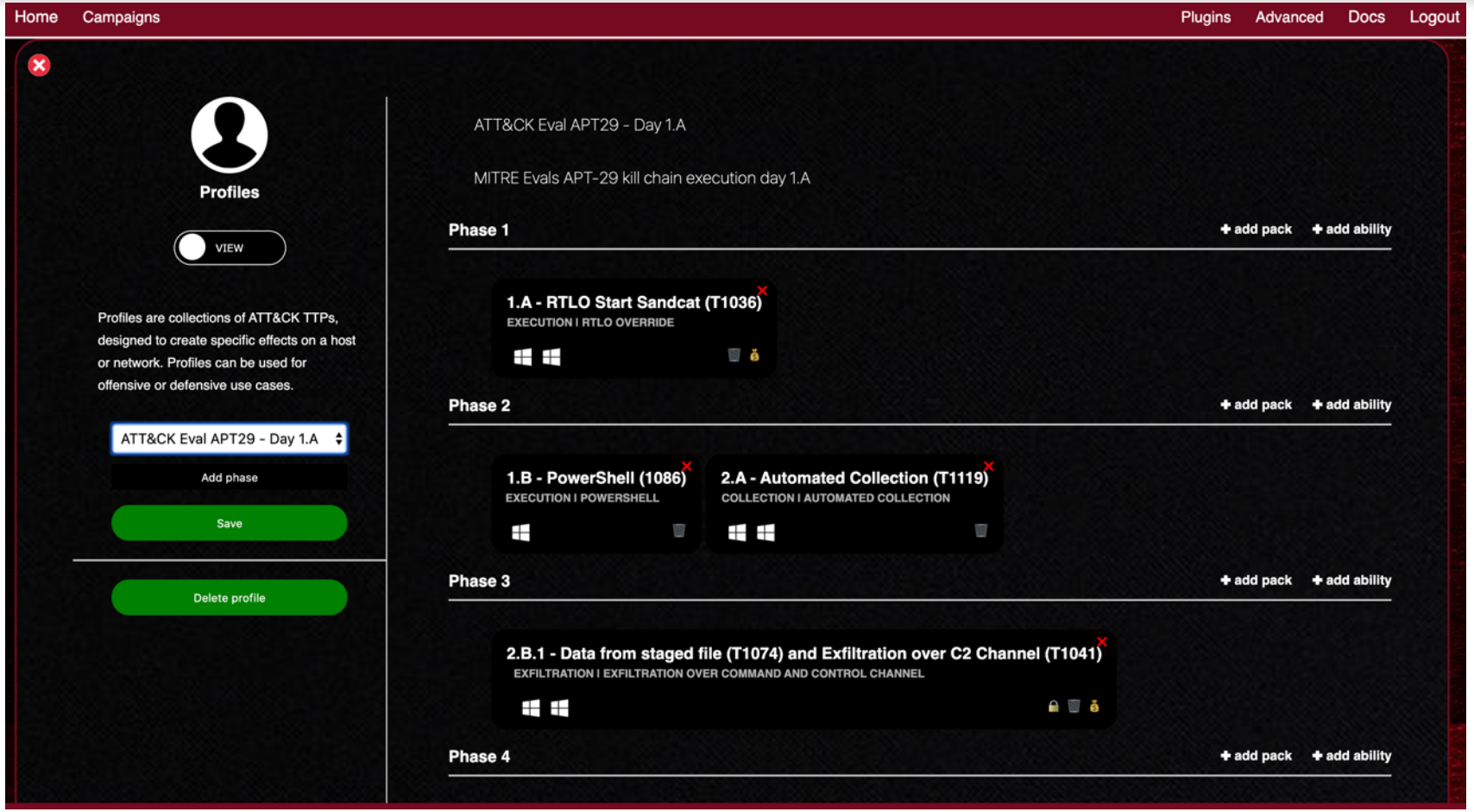
https://github.com/mitre-attack/attack-arsenal/tree/master/adversary_emulation/APT29/Emulation_Plan/Day%202/payloads

APT29 Evals – DIY Plugin



https://github.com/mitre-attack/attack-arsenal/tree/master/adversary_emulation/APT29/CALDERA_DIY/evals

APT29 Evals – DIY Plugin



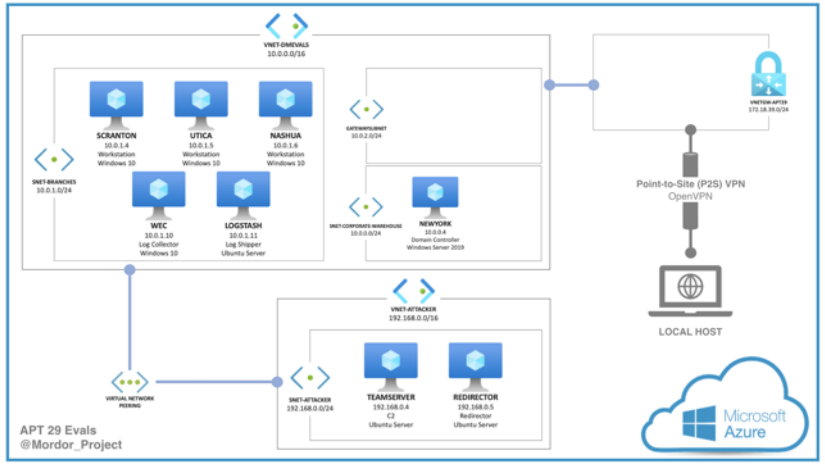
https://github.com/mitre-attack/attack-arsenal/tree/master/adversary_emulation/APT29/CALDERA_DIY/evals

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

Mordor Style!

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.

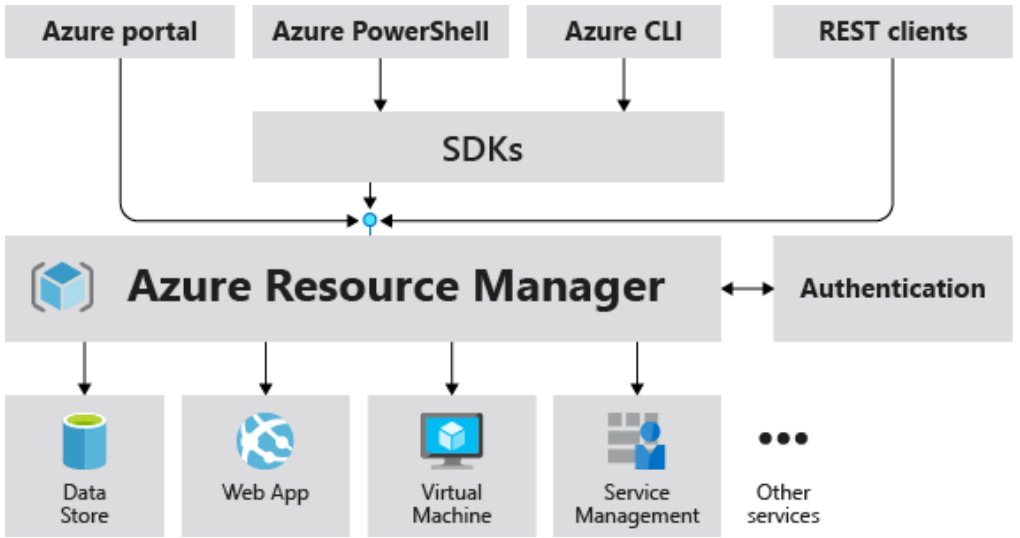
Agenda

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 🔥

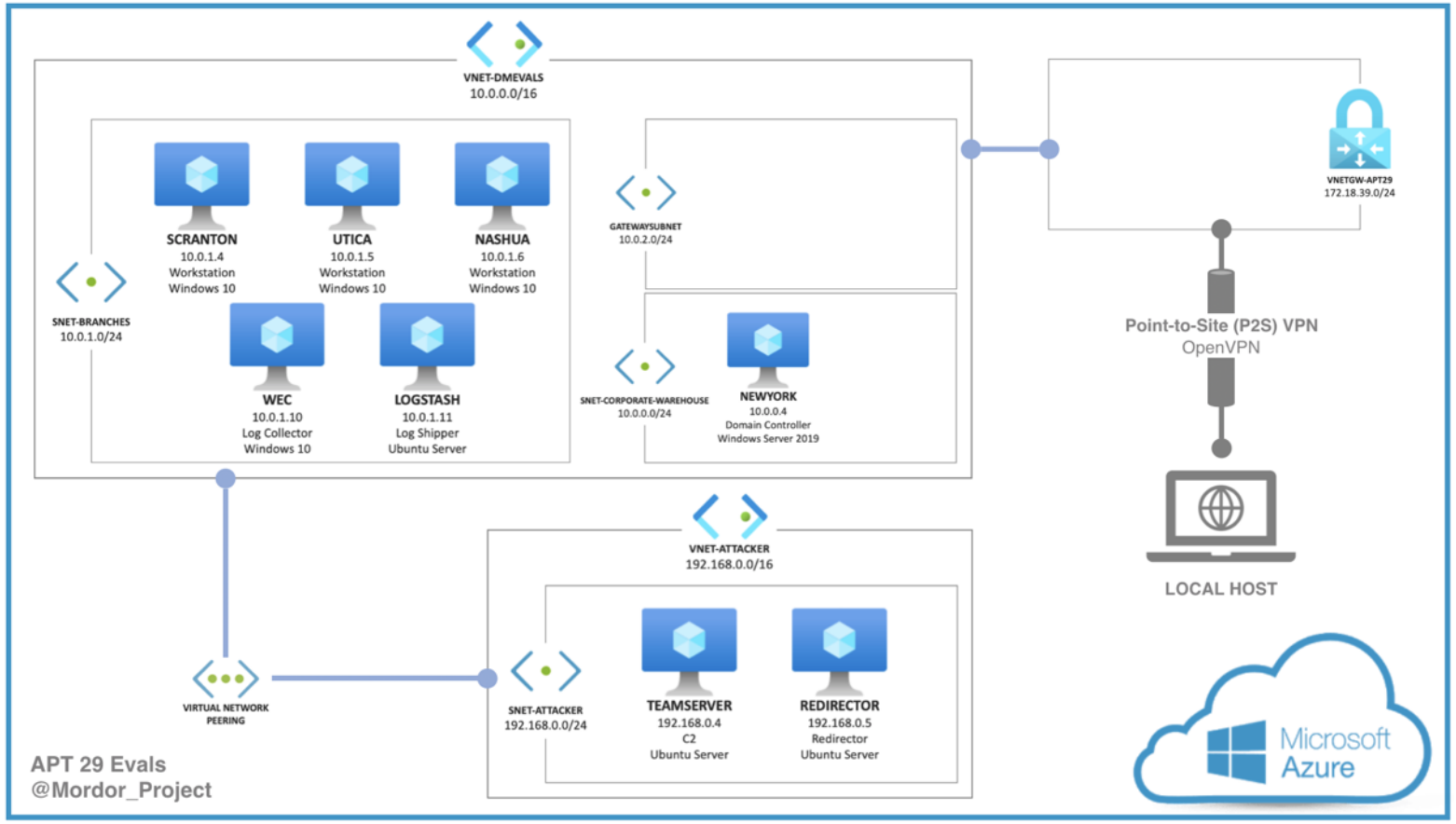
Cloud Templates and scripts to deploy network environments **exclusively** to generate datasets for the Mordor project.

- 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?)



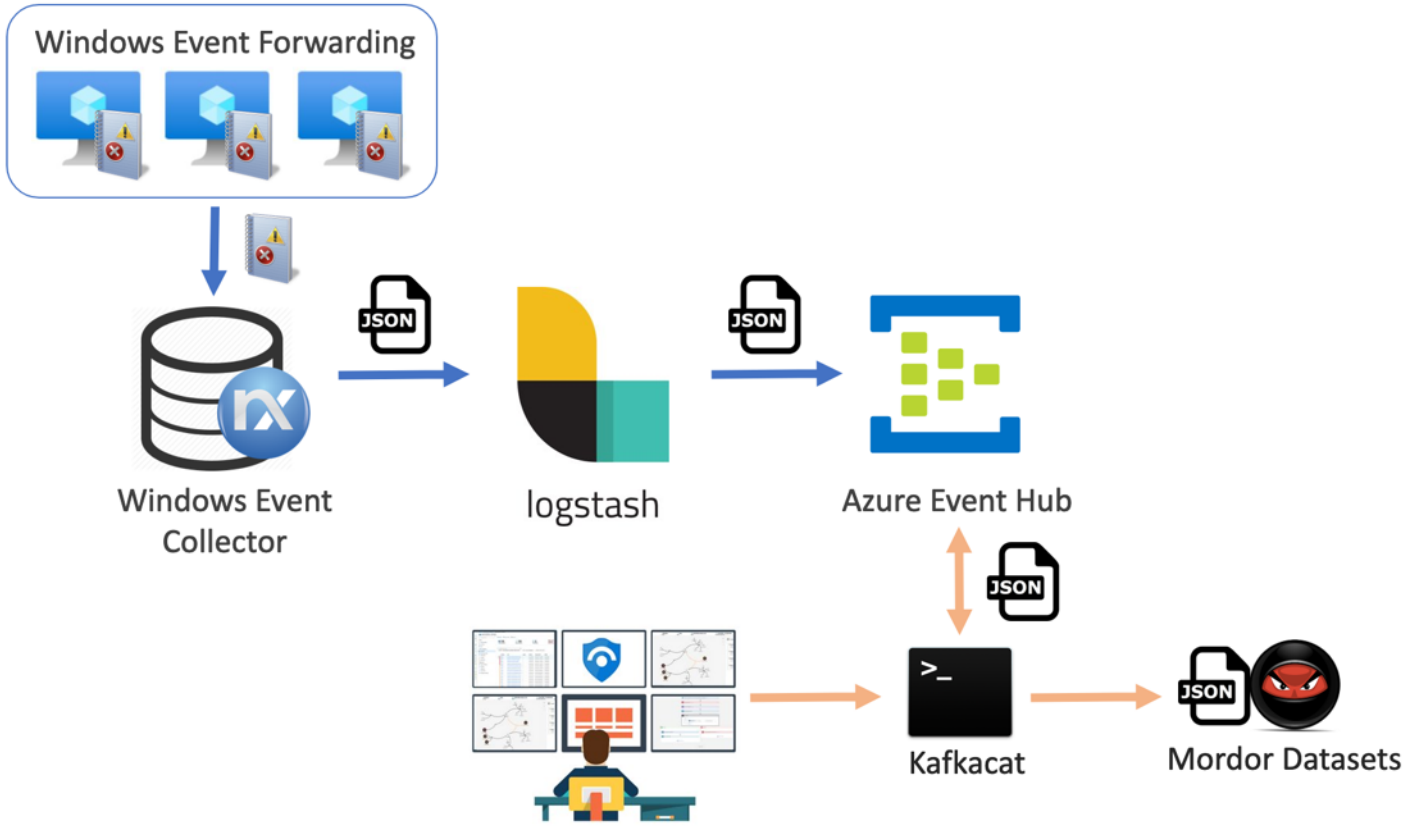
https://github.com/OTRF/mordor-labs

Mordor Labs – APT 29 Network



https://medium.com/threat-hunters-forge/mordor-labs-part-1-deploying-att-ck-apt29-evals-environments-via-arm-templates-to-create-1c6c4bc32c9a

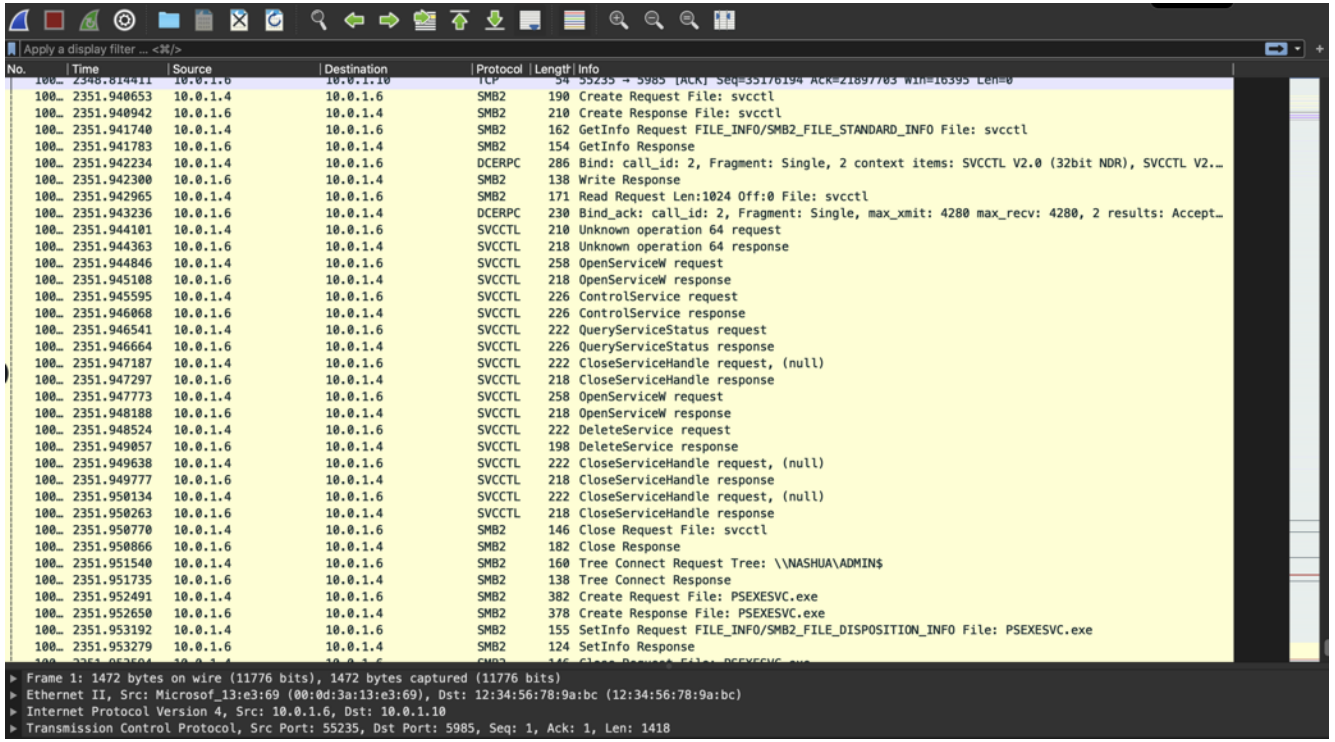
Mordor Labs – Host Telemetry



https://medium.com/threat-hunters-forge/mordor-labs-part-1-deploying-att-ck-apt29-evals-environments-via-arm-templates-to-create-1c6c4bc32c9a

Mordor Labs – Network Telemetry

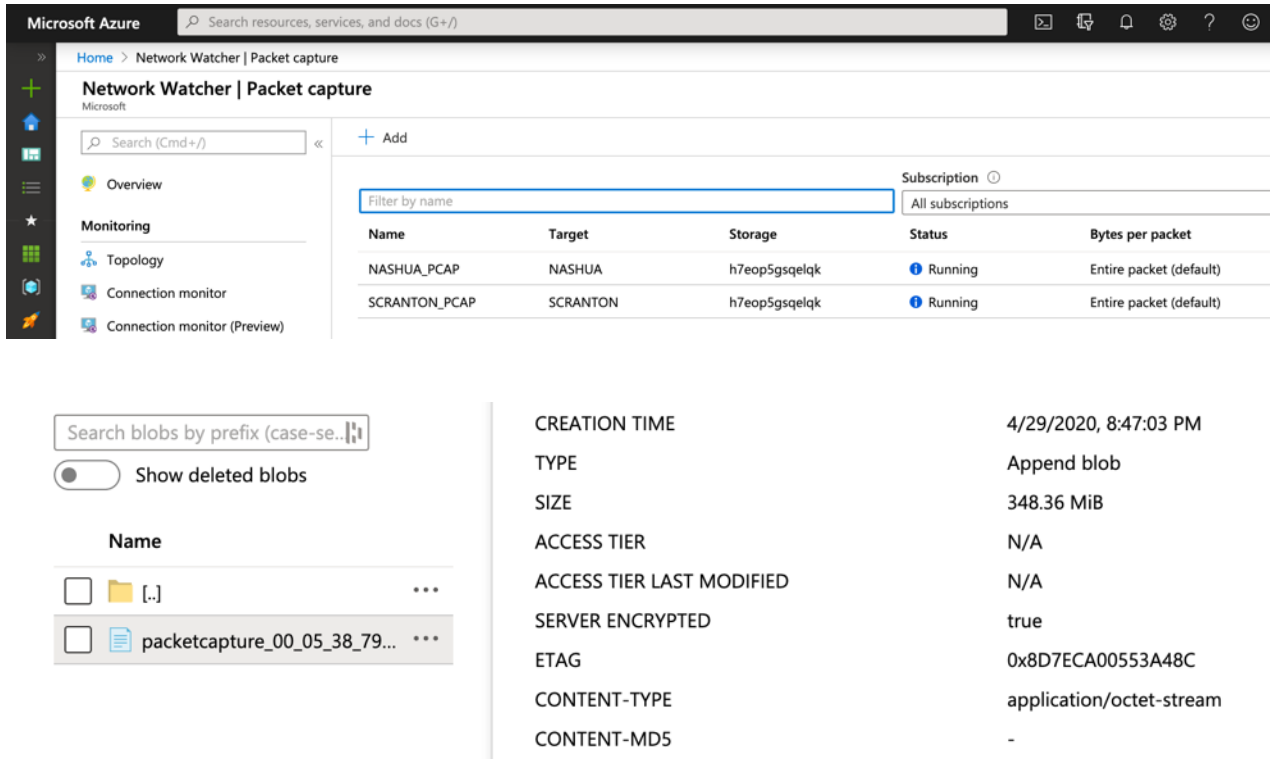
- netsh trace start capture=yes traceFile=$FILE fileMode=single persistent=yes maxSize=0 overwrite=yes
- pktmon start --etw -p 0 -l real-time (Windows 10 2004)
- Azure Network Watcher Agent extension for Windows



https://medium.com/threat-hunters-forge/mordor-labs-part-1-deploying-att-ck-apt29-evals-environments-via-arm-templates-to-create-1c6c4bc32c9a

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/Stop-Packet-Capture.sh



https://medium.com/threat-hunters-forge/mordor-labs-part-1-deploying-att-ck-apt29-evals-environments-via-arm-templates-to-create-1c6c4bc32c9a

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, *.rar,*.docx,*.url,*.xlsx,*.pptx,*.ppsx,*.pst,*.ost,*psw*,*pass*,*login*,*admin*,*sifr*,*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

https://github.com/OTRF/detection-hackathon-apt29/tree/master/emulation-plans

Mordor Labs – Emulation Plans & Videos

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

https://github.com/hunters-forge/mordor

Mordor Datasets – APT29 Evals (Host)

Datasets

Type	Scenario	Dataset	Size	Timestamp
Host	Day 1	apt29_evals_day1_manual.zip	367M	2020-05-01225525
Host	Day 2	apt29_evals_day2_manual.zip	1.6GB	2020-05-02035409

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

Mordor Datasets – APT29 Evals (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-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

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

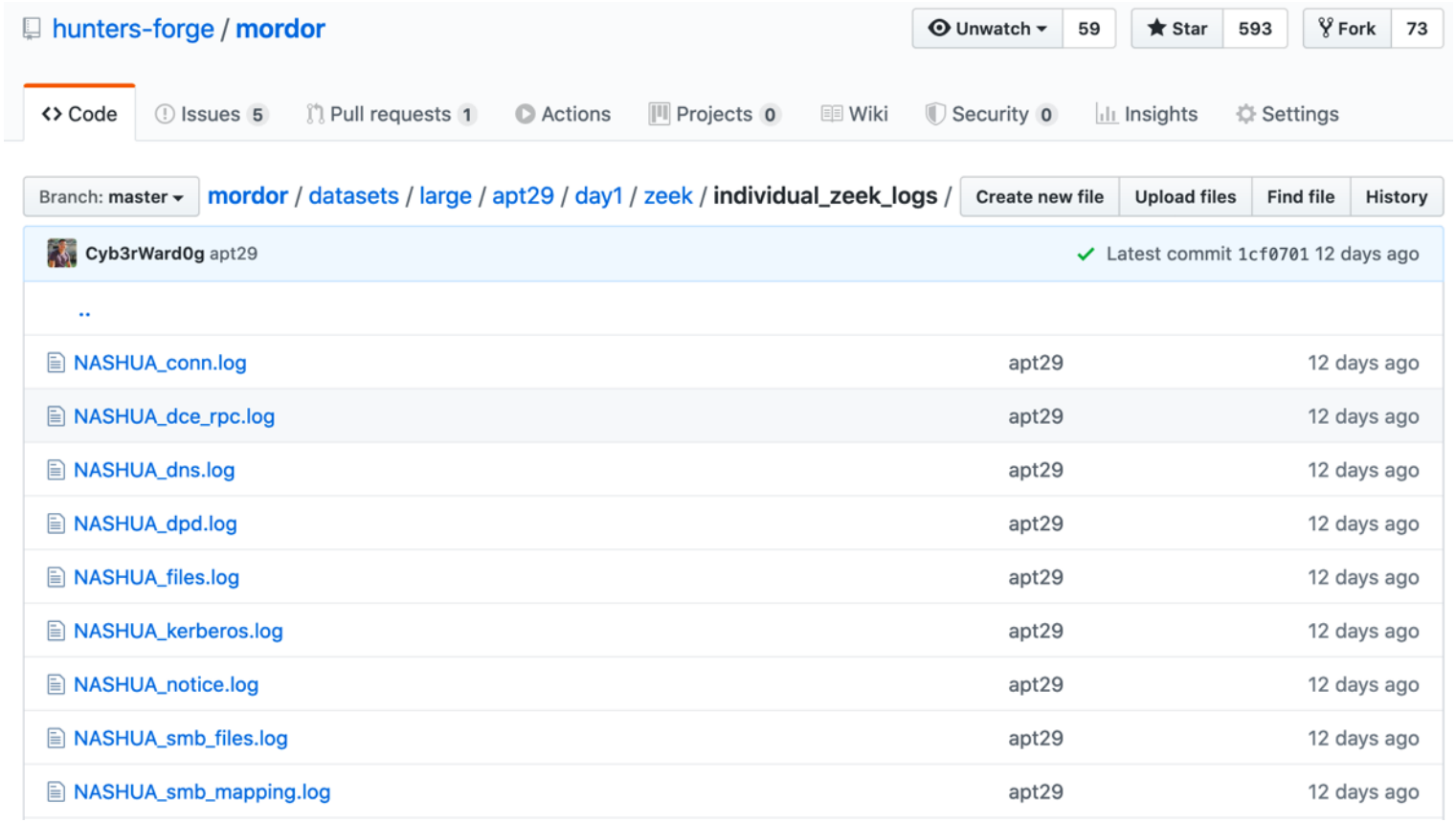
Mordor Datasets – APT29 Evals (Host)

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

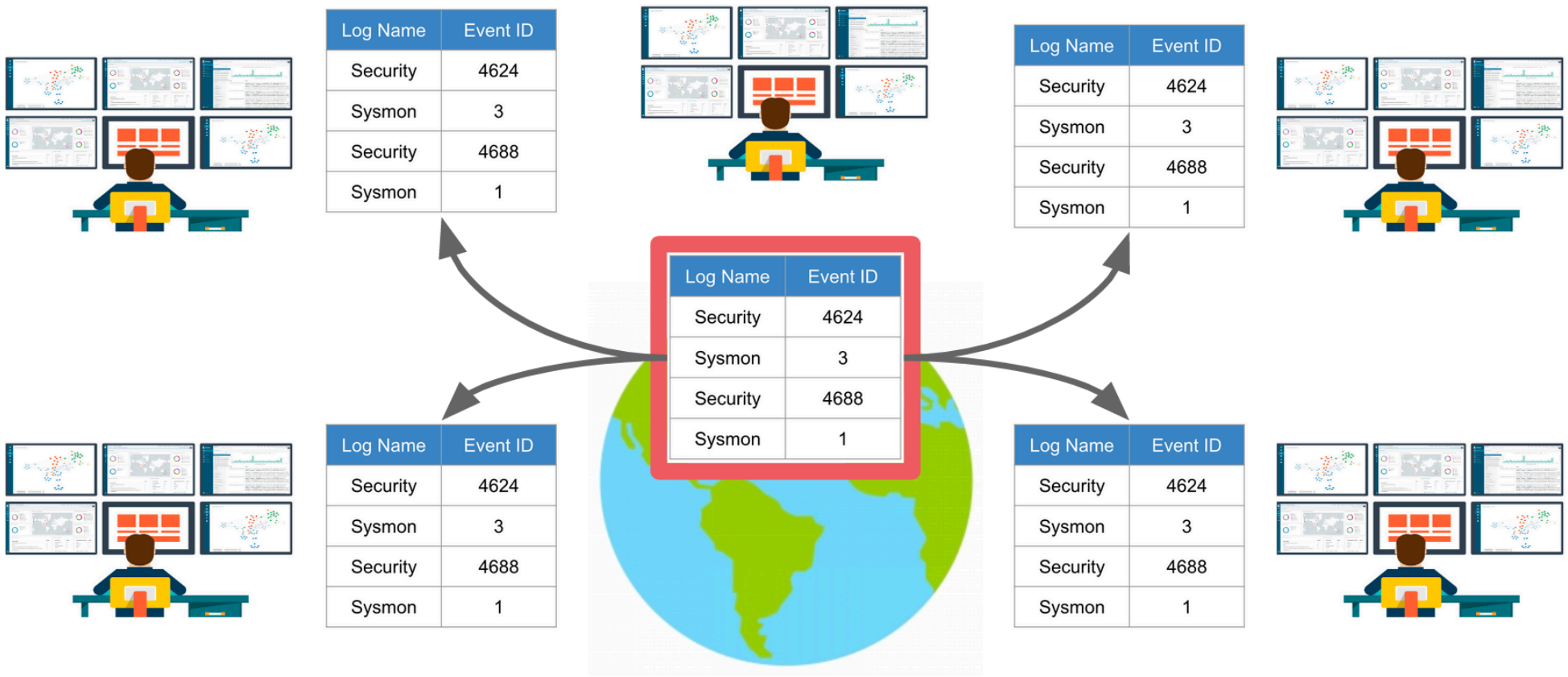
https://github.com/hunters-forge/mordor/tree/master/datasets/large/apt29

Mordor Datasets – APT29 Evals (Network)



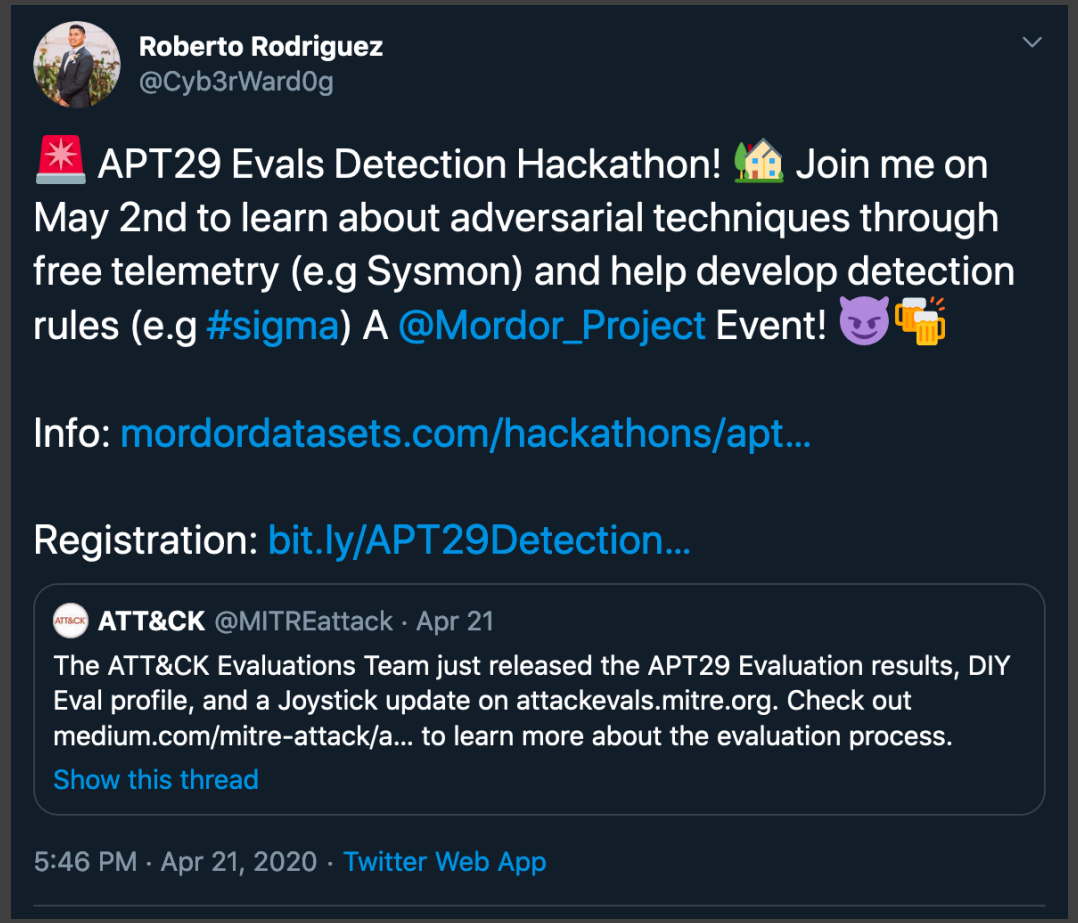
https://github.com/hunters-forge/mordor/tree/master/datasets/large/apt29

Mordor Datasets- Empowering Researchers



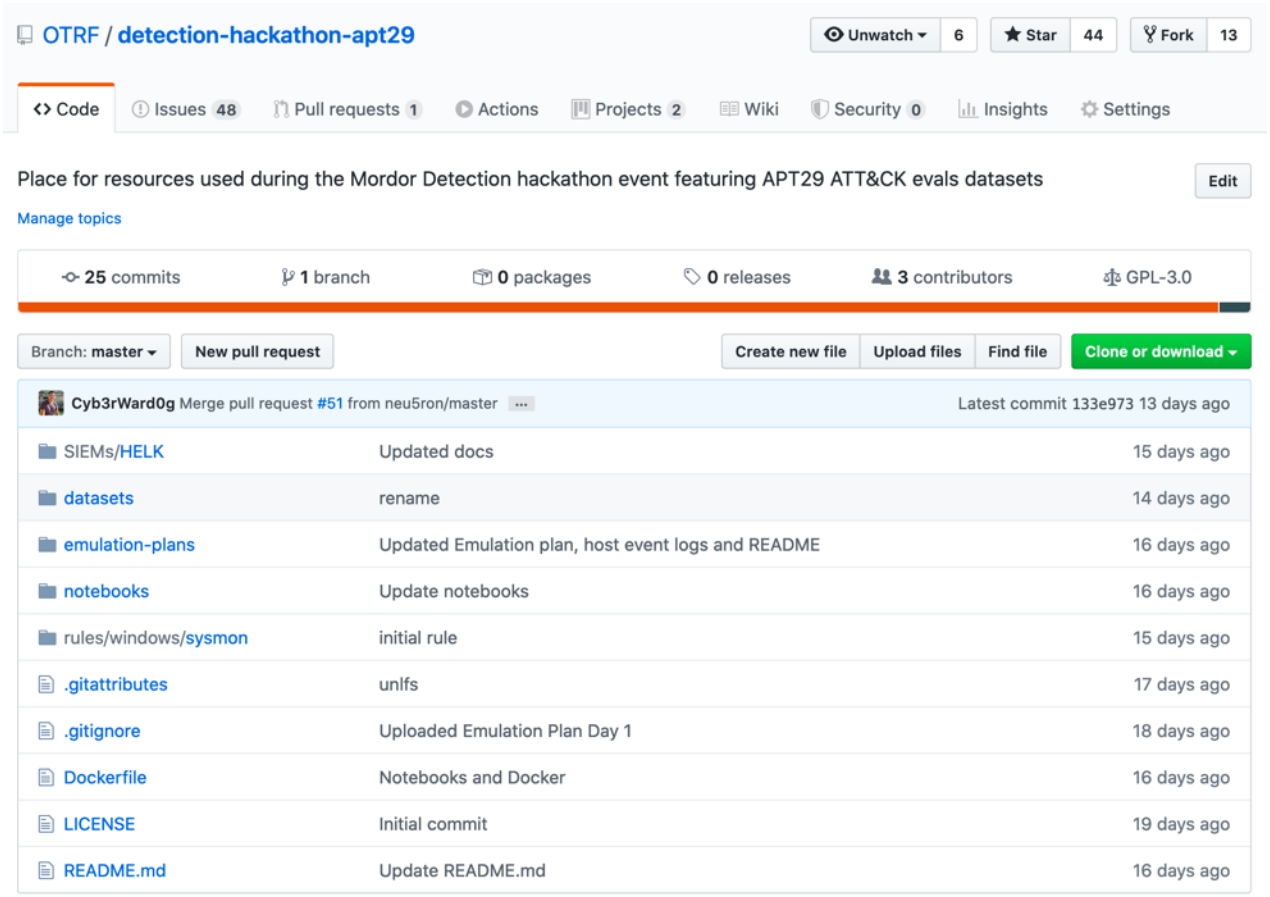
Detection Hackathon ⚔️

- 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 💥!



https://twitter.com/Cyb3rWard0g/status/1252715463773126662

Detection Hackathon – APT29 Evals



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

Detection Hackathon – APT29 Evals

2 Open ✓ 0 Closed Sort

APT29 - Day 2

Updated 16 days ago

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.

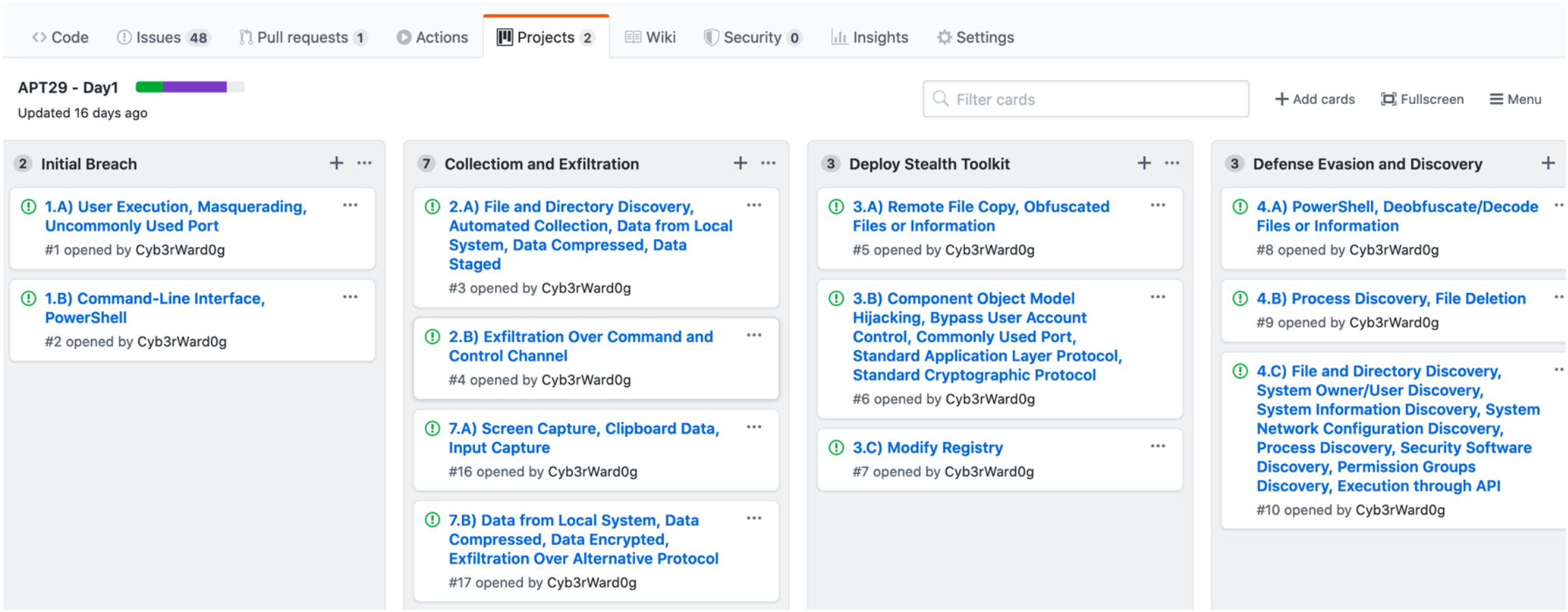
APT29 - Day1

Updated 16 days ago

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.

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

Detection Hackathon – APT29 Evals



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

Detection Hackathon – APT29 Evals ❤️

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)

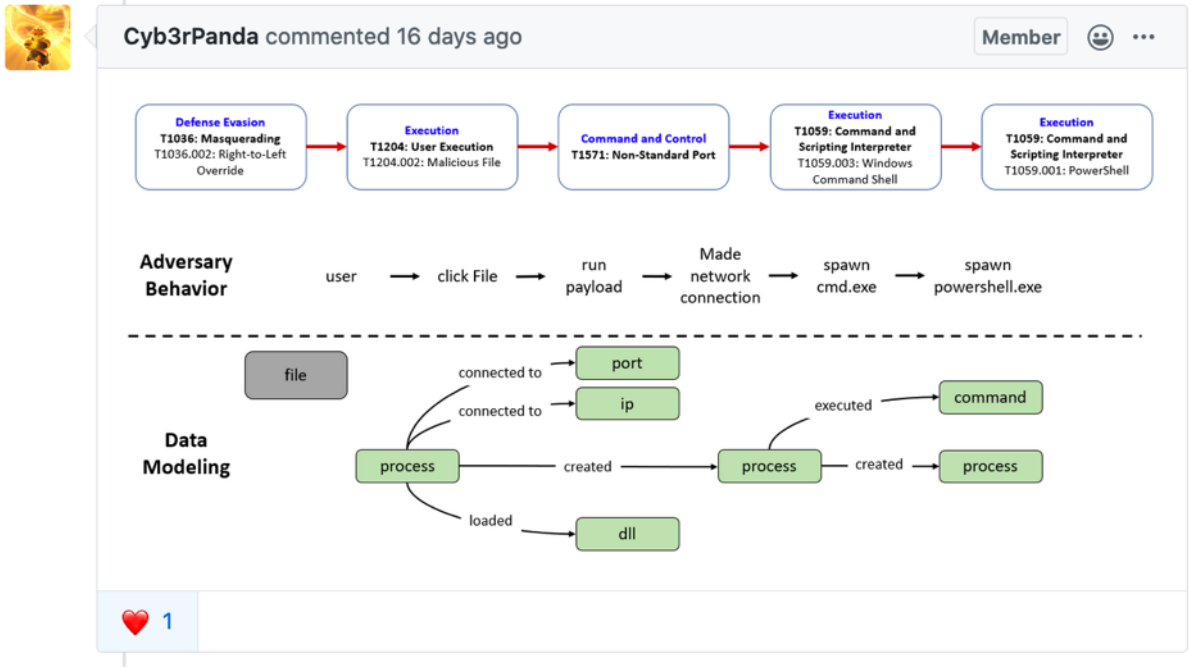
```
bypassUAC = spark.sql(
    '''
SELECT a.Image, a.CommandLine
FROM apt29Table a
INNER JOIN (
    SELECT ProcessGuid
    FROM apt29Table
    WHERE Channel = "Microsoft-Windows-Sysmon/Operational"
        AND EventID = 1
        AND LOWER(Image) LIKE "%control.exe"
        AND LOWER(ParentImage) LIKE "%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)
```

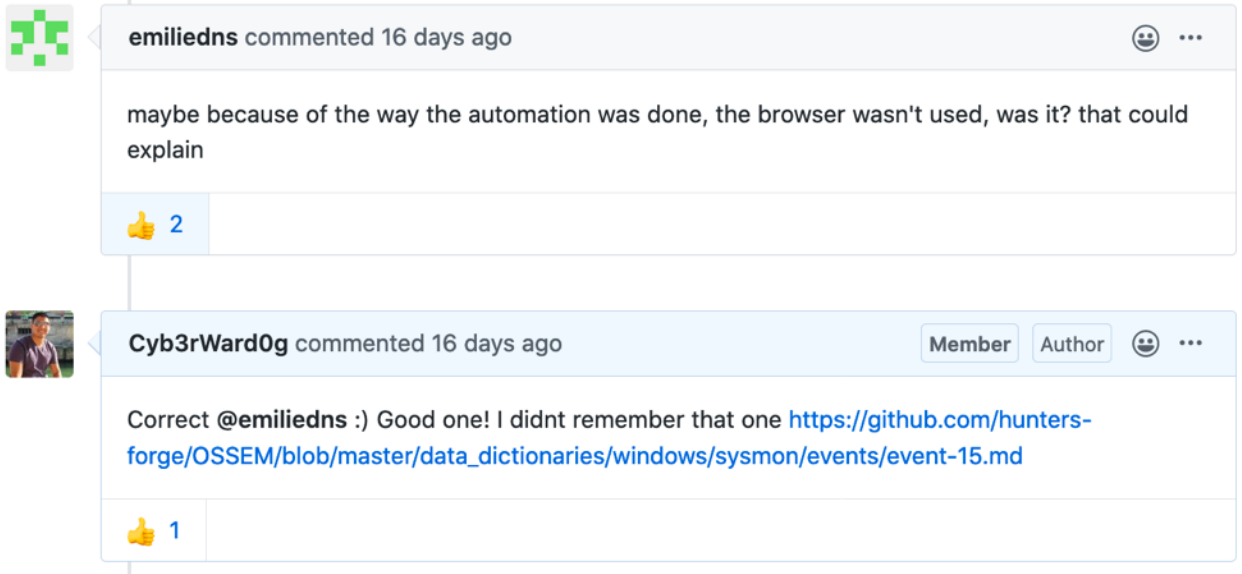
Results

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

https://github.com/OTRF/detection-hackathon-apt29/issues/6

Detection Hackathon – APT29 Evals ❤️





https://github.com/OTRF/detection-hackathon-apt29/issues/1

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
```

❤️ 1

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
```

🎉 1 ❤️ 1 🚀 1 👀 1

https://github.com/OTRF/detection-hackathon-apt29/issues/6 & 17

Detection Hackathon – APT29 Evals ❤️

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

```
mpressed, Data Encrypted, Exfiltration Over Alter

n-hackathon-apt29/issues/17

n2 or selection3 or selection4
```

https://github.com/OTRF/detection-hackathon-apt29/issues/6 & 17 & 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

https://github.com/hunters-forge/mordor

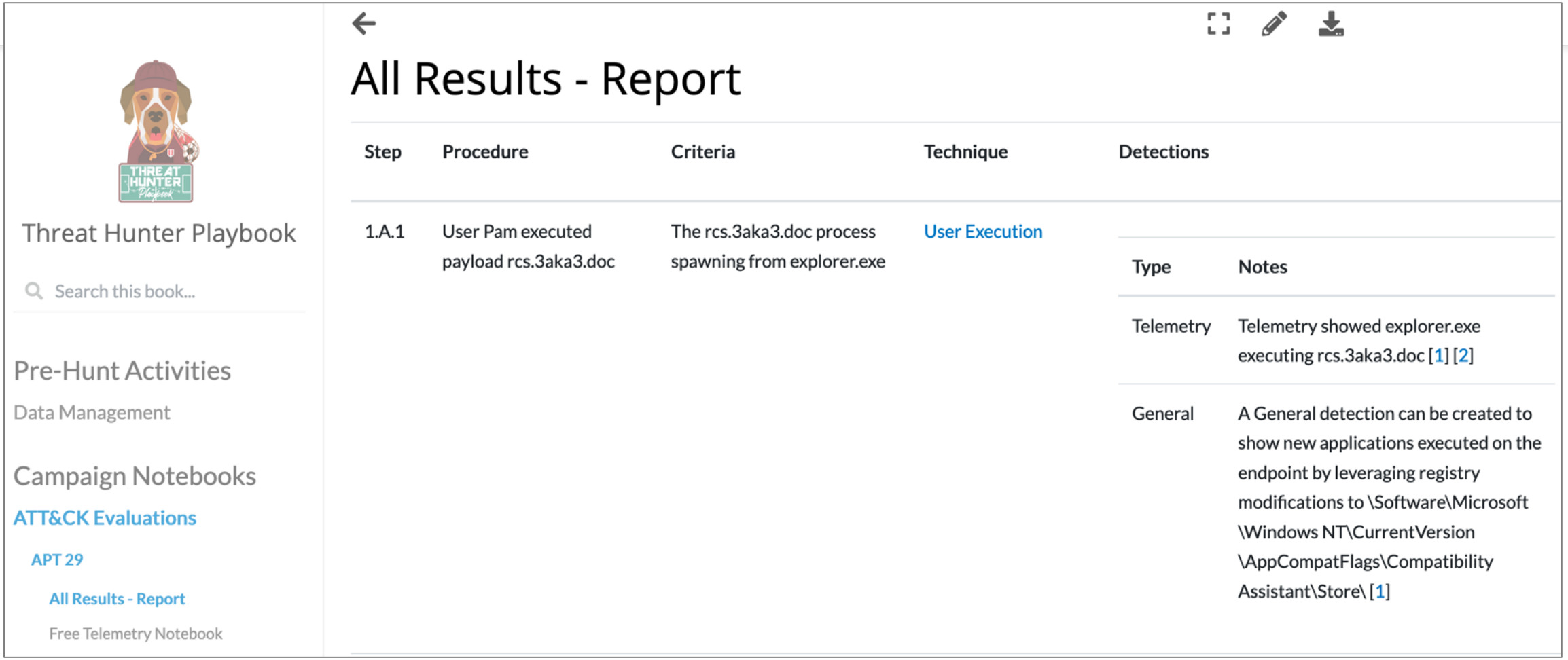
Threat Hunter Playbook: Documenting..

```yaml
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

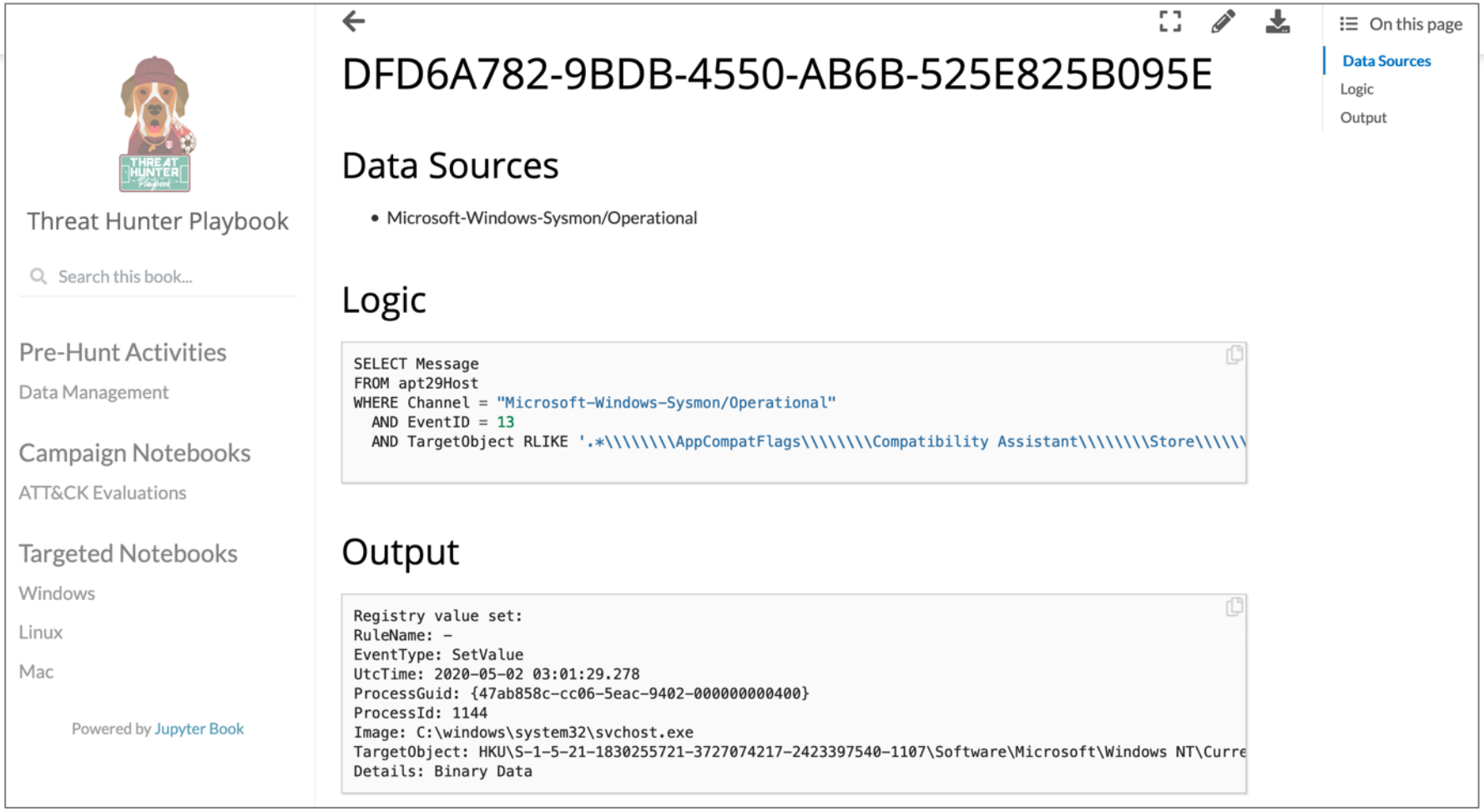
Releasing something today 

Threat Hunter Playbook: Creating a Report..



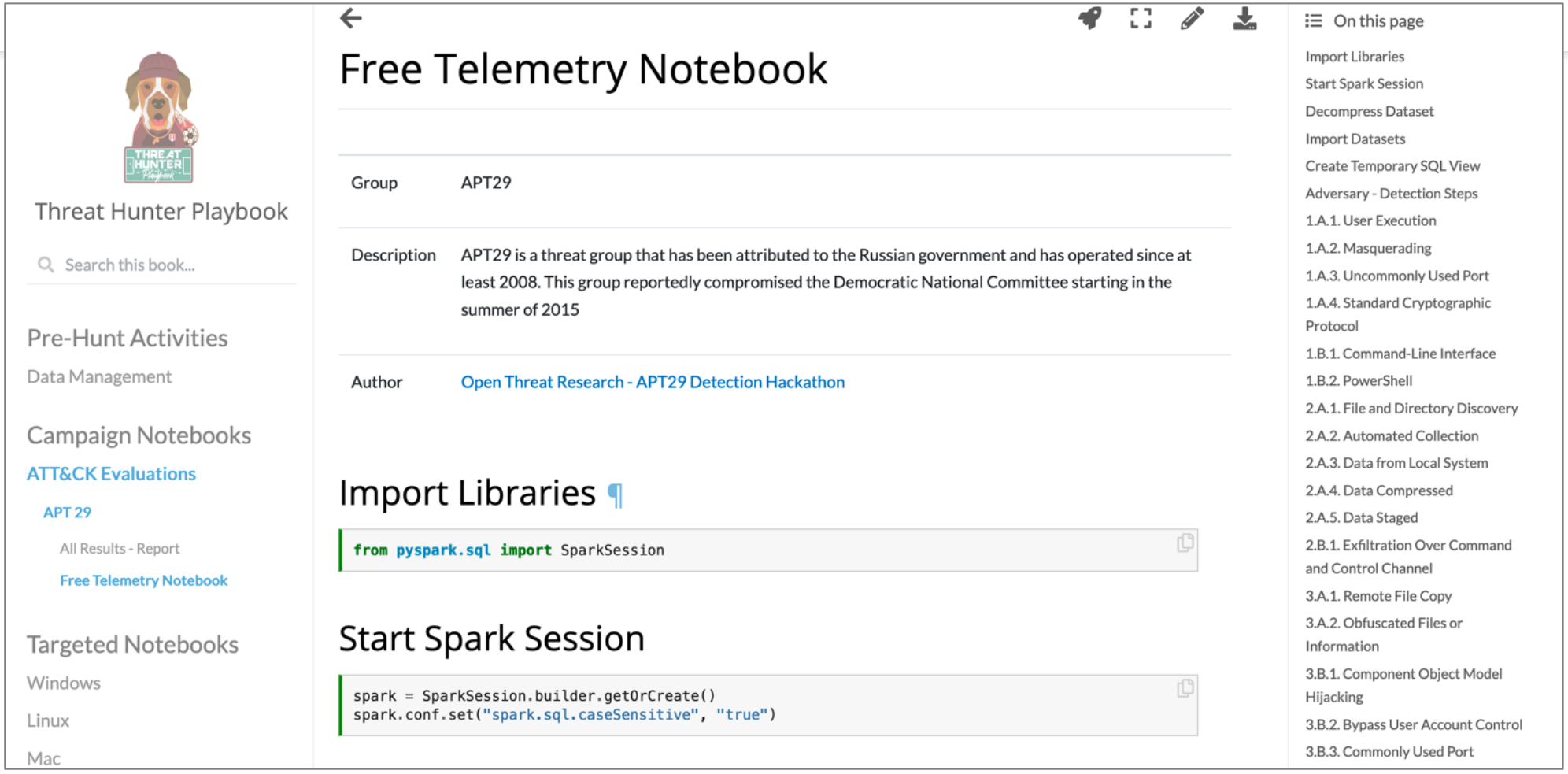
https://threathunterplaybook.com/evals/apt29/report.html

Threat Hunter Playbook: Creating a Report..



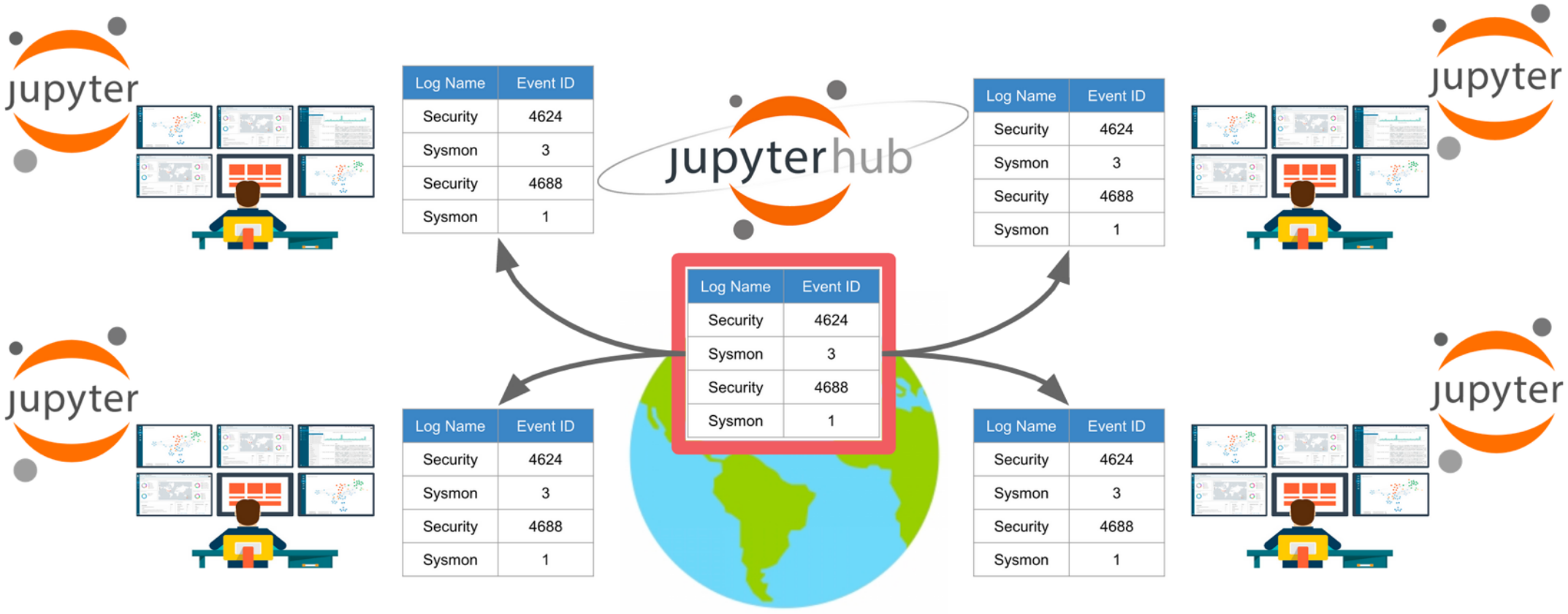
https://threathunterplaybook.com/evals/apt29/detections/1.A.1_DFD6A782-9BDB-4550-AB6B-525E825B095E.html

Threat Hunter Playbook: Creating a Notebook..

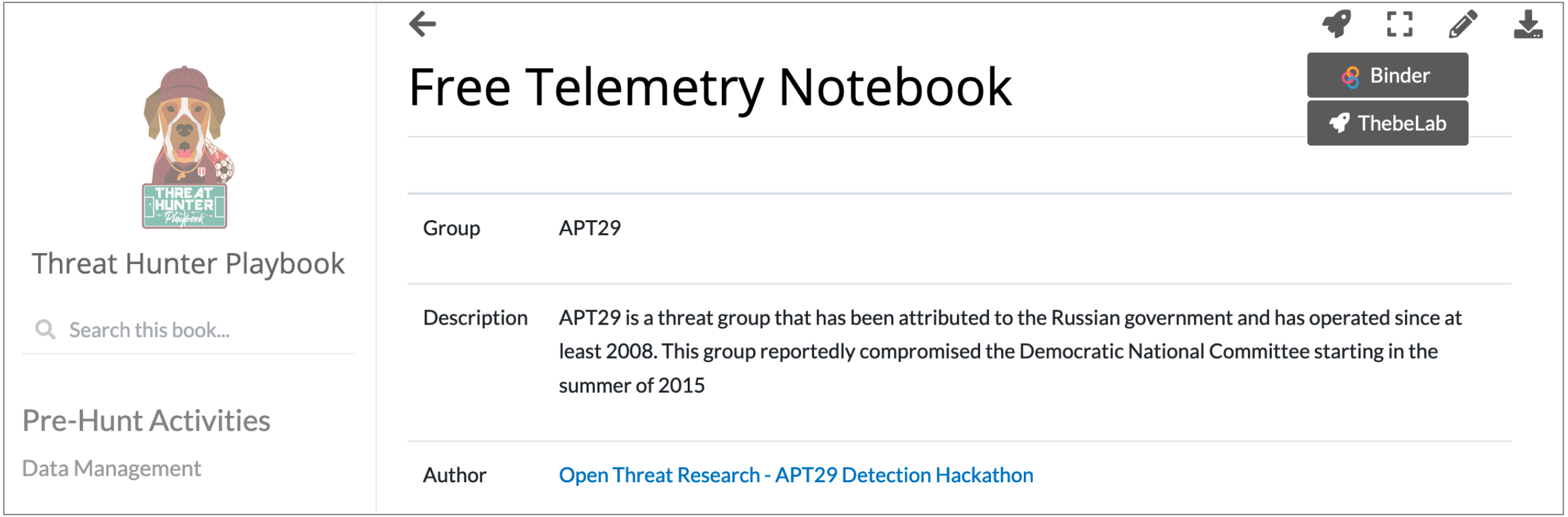


https://threathunterplaybook.com/notebooks/campaigns/apt29Evals.html

Threat Hunter Playbook: Empowering others

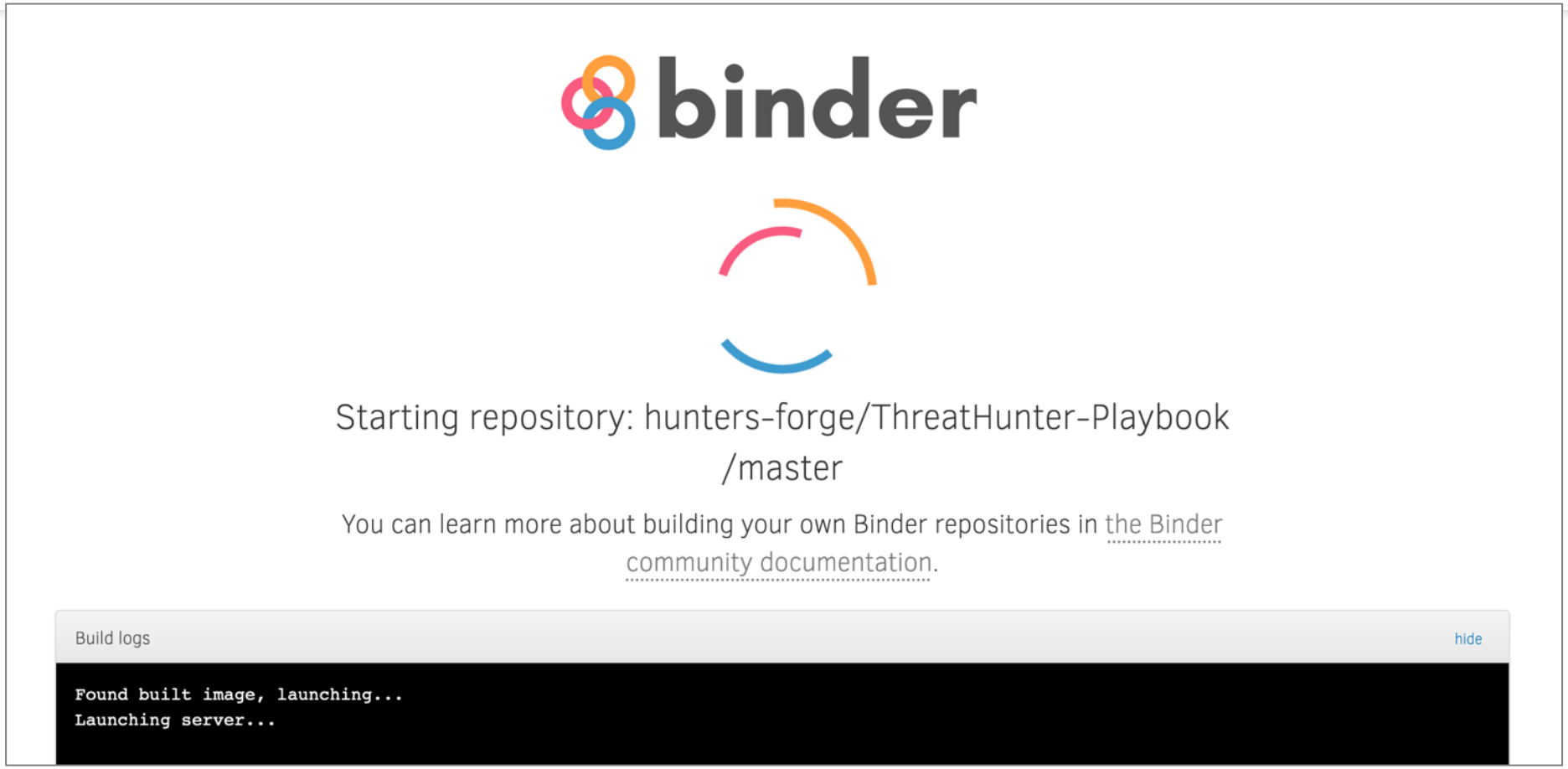


Threat Hunter Playbook: Notebook Demo



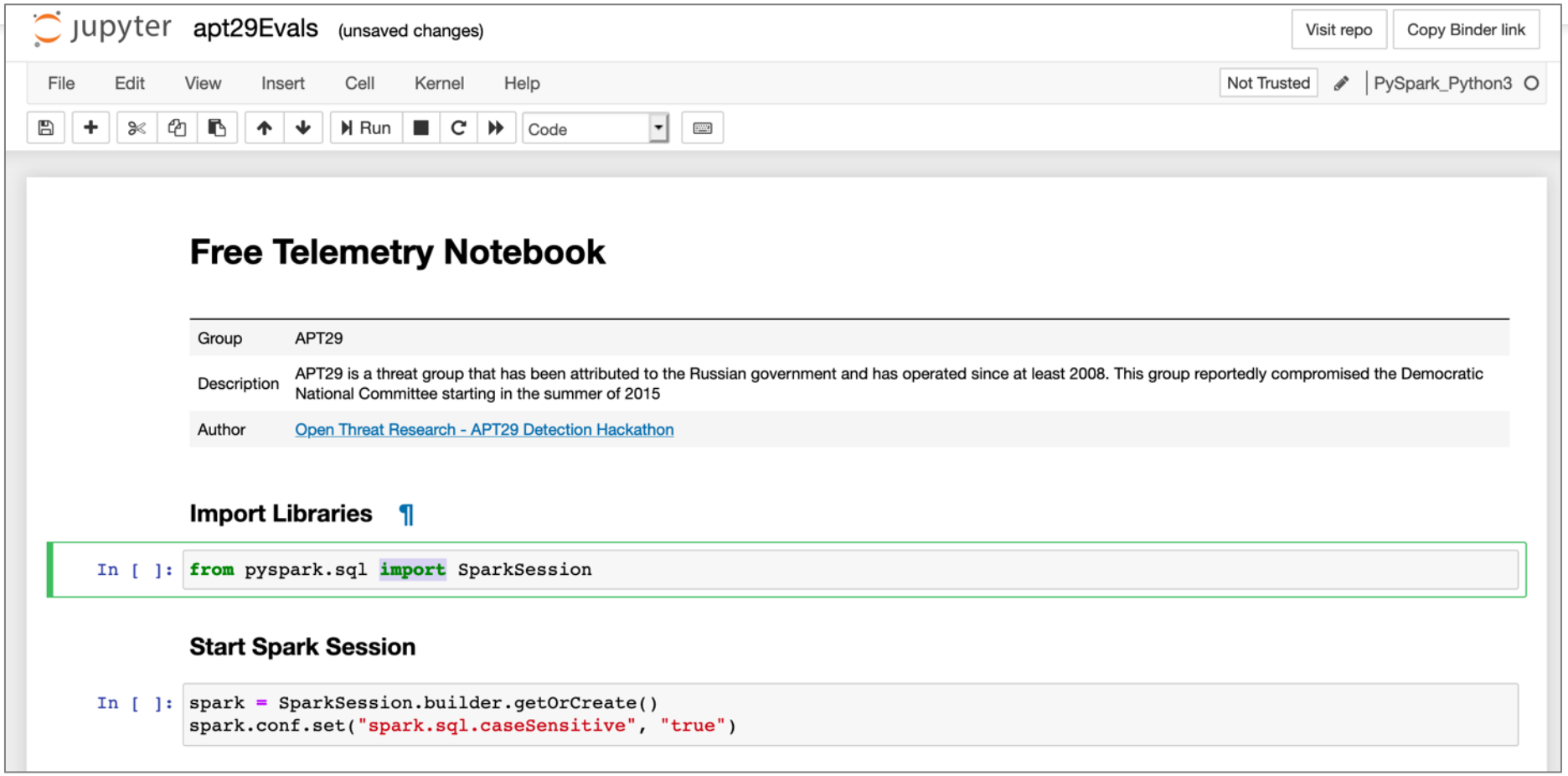
https://threathunterplaybook.com/notebooks/campaigns/apt29Evals.html

Threat Hunter Playbook: Notebook Demo



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

Threat Hunter Playbook: Notebook Demo



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