MITRE ATT&CK: The Play at Home Edition

- Katie Nickels @ MITRE
- Ryan Kovar @ Splunk

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

System Owner/User Discovery (T1033)

Katie Nickels (@LiketheCoins)

- ATT&CK Threat Intelligence **Lead** at MITRE (@MITREattack)
- SANS **Instructor** for FOR578: Cyber Threat Intelligence
- 10+ years of experience in threat intel and network defense
- Program Manager for **Cyberjutsu Girls Academy**
- Baker of chocolate things
- CrossFitter
- Oxford comma believer

System Owner/User Discovery (T1033)

Ryan Kovar (@meansec)

- Principal Security Strategist at **Splunk**
- MSc(Dist) Information Security
- Minister of OODAlooping at Splunk
- US/UK DoD/PubSec **Nation State Hunting** Roles
- Enough white in beard to speak authoritatively
- Co-Creator of Boss of the SOC CTF
- Hates printers and trilobites


We use Splunk
But you don’t have to!

Agenda

- ♟ Let’s tell a story
- ♟ Oops, now I see where we went wrong
- ♟ Pass go, collect 200 TTPs


So you've heard of this ATT&CK thing...
but how do you actually ~~play~~ *use* it?


We want to tell you a story...
Premium


Premium
FROTHLY
Quality

“I don’t really know how we are **defended** and it makes me **uncomfortable.**”

- Grace Hoppy

CEO

“If it’s not an **IP**,
how do I **use** it?
- Mallory Kraeusen
Threat Intel

“I’m **drowning** in meaningless **alerts** and my data isn’t **helping** me!”

- Alice Bluebird
Network Defender

“I’m **not sure** how I can **help**.”

- Kevin Lagerfield

Red Team


LIVE
breakyourownnews.com
SS Hops and Ale
BREAKING NEWS
BEER TANKER THREATENED
19:25
HOPS PRICES PLUMET AS CONSUMERS CONSIDER "FROSE ALL DAY" OPTIONS

Iranians in my HOPS!

GH

Grace Hoppy
Today, 8:47 PM
Mallory Kraeusen

Reply all

Inbox

What the heck is going on over there! I turned on HOPSNN and found out there is cyberwarfare? Hops prices are affected!! I have a board meeting this week and I KNOW this is going to come up. I need to you find out how this going to impact us and if they are going to come after us next and how/if we are defended.

Regards,
Grace Hoppy
CEO
"Have a nice day!"

Iranians in my HOPS!

GH

Grace Hoppy

Today, 8:47 PM

Reply all

Inbox

What the heck is going on over there? I turned on HOPSNN and heard out there is cyberwarfare? Hops prices are affected!! I have a board meeting this week and I KNOW this is going to come up and I need to know if this is going to impact us and if they are going to come after us next and how/if we are defended.

Regards,

Grace Hoppy

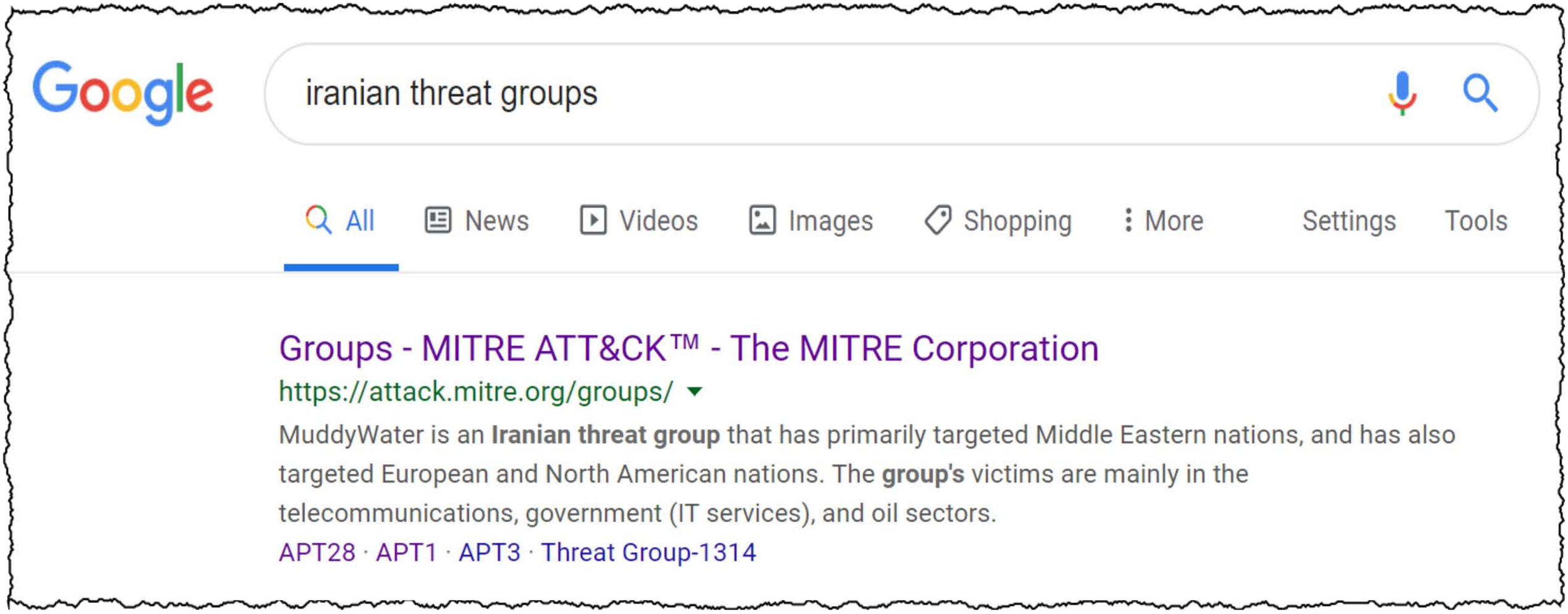
CEO

"Have a nice day!"

“I need to you to find out how this will impact us…. are we defended?”

How does Mallory find info on Iranian groups…

…and can ATT&CK help?


Google
iranian threat groups
All
News
Videos
Images
Shopping
More
Settings
Tools
Groups - MITRE ATT&CK™ - The MITRE Corporation
https://attack.mitre.org/groups/
MuddyWater is an Iranian threat group that has primarily targeted Middle Eastern nations, and has also targeted European and North American nations. The group's victims are mainly in the telecommunications, government (IT services), and oil sectors.
APT28 · APT1 · APT3 · Threat Group-1314

Groups

NEODYMIUM		NEODYMIUM is an activity group that conducted a campaign in May 2016 and has heavily targeted Turkish victims. The group has demonstrated similarity to another activity group called PROMETHIUM due to overlapping victim and campaign characteristics. NEODYMIUM is reportedly associated closely with BlackOasis operations, but evidence that the group names are aliases has not been identified.
Night Dragon		Night Dragon is a campaign name for activity involving a threat group that has conducted activity originating primarily in China.
OilRig	IRN2, HELIX KITTEN, APT34	OilRig is a suspected Iranian threat group that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its operations within the Middle East. It appears the group carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets. FireEye assesses that the group works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests. This group was previously tracked under two distinct groups, APT34 and OilRig, but was combined due to additional reporting giving higher confidence about the overlap of the activity.
Orangeworm		Orangeworm is a group that has targeted organizations in the healthcare sector in the United States, Europe, and Asia since at least 2015, likely for the purpose of corporate espionage.
Patchwork	Dropping Elephant, Chinastrats, MONSOON, Operation Hangover	Patchwork is a cyberespionage group that was first observed in December 2015. While the group has not been definitively attributed, circumstantial evidence suggests the group may be a pro-Indian or Indian entity. Patchwork has been seen targeting industries related to diplomatic and government agencies. Much of the code used by this group was copied and pasted from online forums. Patchwork was also seen operating spearphishing campaigns targeting U.S. think tank groups in March and April of 2018.
PittyTiger		PittyTiger is a threat group believed to operate out of China that uses multiple different types of malware to maintain command and control.
PLATINUM		PLATINUM is an activity group that has targeted victims since at least 2009. The group has focused on targets associated with governments and related organizations in South and Southeast Asia.
Poseidon Group		Poseidon Group is a Portuguese-speaking threat group that has been active since at least 2005. The group has a history of using information exfiltrated from victims to blackmail victim companies into contracting the Poseidon Group as a security firm.

Groups

NEODYMIUM		NEODYMIUM is an activity group that conducted a campaign in May 2016 and has heavily targeted Turkish victims. The group has demonstrated similarity to another activity group called PROMETHIUM due to overlapping victim and campaign characteristics. NEODYMIUM is reportedly associated closely with BlackOasis operations, but evidence that the group names are aliases has not been identified.
Night Dragon		Night Dragon is a campaign name for activity involving a threat group that has conducted activity originating primarily in China.
OilRig	IRN2, HELIX KITTEN, APT34	OilRig is a suspected Iranian threat group that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its operations within the Middle East. It appears the group carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets. FireEye assesses that the group works on behalf of the Iranian government based on infrastructure details that contain racked under two he activity.
		least 2015, likely
Patchwork	Dropping Elephant, Chinastrats, MONSOON, Operation Hangover	Patchwork is a cyberespionage group that was first observed in December 2015. While the group has not been definitively attributed, circumstantial evidence suggests the group may be a pro-Indian or Indian entity. Patchwork has been seen targeting industries related to diplomatic and government agencies. Much of the code used by this group was copied and pasted from online forums. Patchwork was also seen operating spearphishing campaigns targeting U.S. think tank groups in March and April of 2018.
PittyTiger		PittyTiger is a threat group believed to operate out of China that uses multiple different types of malware to maintain command and control.
PLATINUM		PLATINUM is an activity group that has targeted victims since at least 2009. The group has focused on targets associated with governments and related organizations in South and Southeast Asia.
Poseidon Group		Poseidon Group is a Portuguese-speaking threat group that has been active since at least 2005. The group has a history of using information exfiltrated from victims to blackmail victim companies into contracting the Poseidon Group as a security firm.

OilRig is a suspected Iranian threat group

OilRig?

GROUPS

Overview
admin@338
APT1
APT12
APT16
APT17
APT18
APT19
APT28
APT29
APT3
APT30
APT32
APT33
APT37
APT38
APT39
Axiom
BlackOasis
BRONZE BUTLER
Carbanak
Charming Kitten
Cleaver
Cobalt Group

Home > Groups > OilRig

OilRig

OilRig is a suspected Iranian threat group that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its operations within the Middle East. It appears the group carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets. FireEye assesses that the group works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests. [1] [2] [3] [4] [5] [6][7] This group was previously tracked under two distinct groups, APT34 and OilRig, but was combined due to additional reporting giving higher confidence about the overlap of the activity.

ID: G0049
Associated Groups: IRN2, HELIX KITTEN, APT34
Contributors: Robert Falcone, Bryan Lee
Version: 1.1

Associated Group Descriptions

Name	Description
IRN2	[14]
HELIX KITTEN	[7][14]
APT34	This group was previously tracked under two distinct groups, APT34 and OilRig, but was combined due to additional reporting giving higher confidence about the overlap of the activity. [7] [6]

Techniques Used

Domain	ID	Name	Use
Enterprise	T1087	Account Discovery	OilRig has run `net user`, `net user /domain`, `net group "domain admins" /domain`, and `net group "Exchange Trusted Subsystem" /domain` to get account listings on a victim.[3]
Enterprise	T1119	Automated Collection	OilRig has used automated collection.[5]
Enterprise	T1110	Brute Force	OilRig has used brute force techniques to obtain credentials.[8]
Enterprise	T1059	Command-Line Interface	OilRig has used the command-line interface for execution.[6][9][5][8]

GROUPS
Overview
admin@338
APT1
APT12
APT16
APT17
APT18
APT19
APT28
APT29
APT3
APT30
APT32
APT33
APT37
APT38
APT39
Axiom
BlackOasis
BRONZE BUTLER
Carbanak
Charming Kitten
Cleaver
Cobalt Group

Home > Groups > OilRig

OilRig

OilRig is a suspected Iranian threat group that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its operations within the Middle East. It appears the group carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets. FireEye assesses that the group works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests. [1] [2] [3] [4] [5] [6][7] This group was previously tracked under two distinct groups, APT34 and OilRig, but was combined due to additional reporting giving higher confidence about the overlap of the activity.

ID: G0049
Associated Groups: IRN2, HELIX KITTEN, APT34
Contributors: Robert Falcone, Bryan Lee
Version: 1.1

Techniques Used

Ass

Name	
IRN2	
HELIX KITTEN	[7][14]
APT34	This group was previously tracked under two distinct groups, APT34 and OilRig, but was combined due to additional reporting giving higher confidence about the overlap of the activity. [7] [6]

Techniques Used

Domain	ID	Name	Use
Enterprise	T1087	Account Discovery	OilRig has run `net user`, `net user /domain`, `net group "domain admins" /domain`, and `net group "Exchange Trusted Subsystem" /domain` to get account listings on a victim.[3]
Enterprise	T1119	Automated Collection	OilRig has used automated collection.[5]
Enterprise	T1110	Brute Force	OilRig has used brute force techniques to obtain credentials.[8]
Enterprise	T1059	Command-Line Interface	OilRig has used the command-line interface for execution.[6][9][5][8]

			Discovery
S0075	Reg	[3] [6]	Credentials in Registry, Modify Registry, Query Registry
S0258	RGDoor	[16]	Command-Line Interface, Data Encrypted, Deobfuscate/Decode Files or Information, Remote File Copy, Standard Application Layer Protocol, System Owner/User Discovery
S0185	SEASHARPEE	[8]	Command-Line Interface, Remote File Copy, Timestomp, Web Shell
S0096	Systeminfo	[6]	System Information Discovery
S0057	Tasklist	[3] [6]	Process Discovery, Security Software Discovery, System Service Discovery

References

1. Falcone, R.. (2017, April 27). OilRig Actors Provide a Glimpse into Development and Testing Efforts. Retrieved May 3, 2017.
2. ClearSky Cybersecurity. (2017, January 5). Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford. Retrieved May 3, 2017.
3. Falcone, R. and Lee, B.. (2016, May 26). The OilRig Campaign: Attacks on Saudi Arabian Organizations Deliver Helminth Backdoor. Retrieved May 3, 2017.
4. Grunzweig, J. and Falcone, R.. (2016, October 4). OilRig Malware Campaign Updates Toolset and Expands Targets. Retrieved May 3, 2017.
5. Unit 42. (2017, December 15). Unit 42 Playbook Viewer. Retrieved December 20, 2017.
6. Sardiwal, M, et al. (2017, December 7). New Targeted Attack in the Middle East by APT34, a Suspected Iranian Threat Group, Using CVE-2017-11882 Exploit. Retrieved December 20, 2017.
7. Lee, B., Falcone, R. (2018, July 25). OilRig Targets Technology Service Provider and Government Agency with QUADAGENT. Retrieved August 9, 2018.
8. Davis, S. and Caban, D. (2017, December 19). APT34 - New Targeted Attack in the Middle East. Retrieved December 20, 2017.
9. Lee, B., Falcone, R. (2018, February 23). OopsIE! OilRig Uses ThreeDollars to Deliver New Trojan. Retrieved July 16, 2018.
10. Mandiant. (2018). Mandiant M-Trends 2018. Retrieved July 9, 2018.
11. Falcone, R. and Lee, B. (2017, October 9). OilRig Group Steps Up Attacks with New Delivery Documents and New Injector Trojan. Retrieved January 8, 2018.
12. Falcone, R. and Lee, B. (2017, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to Greenbug Threat Group. Retrieved January 8, 2018.
13. Falcone, R., Wilhoit, K.. (2018, November 16). Analyzing OilRig's Ops Tempo from Testing to Weaponization to Delivery. Retrieved April 23, 2019.
14. Meyers, A. (2018, November 27). Meet CrowdStrike's Adversary of the Month for November: HELIX KITTEN. Retrieved December 18, 2018.
15. Singh, S., Yin, H. (2016, May 22). https://www.fireeye.com/blog/threat-research/2016/05/targeted_attacksaga.html. Retrieved April 5, 2018.
16. Falcone, R. (2018, January 25). OilRig uses RGDoor IIS Backdoor on Targets in the Middle East. Retrieved July 6, 2018.
17. Wilhoit, K. and Falcone, R. (2018, September 12). OilRig Uses Updated BONDUPDATER to Target Middle Eastern Government. Retrieved February 18, 2019.

			Discovery
S0075	Reg	[3] [6]	Credentials in Registry, Modify Registry, Query Registry
S0258	RGDoor	[16]	Command-Line Interface, Data Encrypted, Deobfuscate/Decode Files or Information, Remote File Copy, Standard Application Layer Protocol, System Owner/User Discovery
S0185	SEASHARPEE	[8]	Command-Line Interface, Remote File Copy, Timestomp, Web Shell
S0096	Systeminfo	[6]	System Information Discovery
S0057	Tasklist	[3] [6]	Process Discovery, Security Software Discovery, System Service Discovery

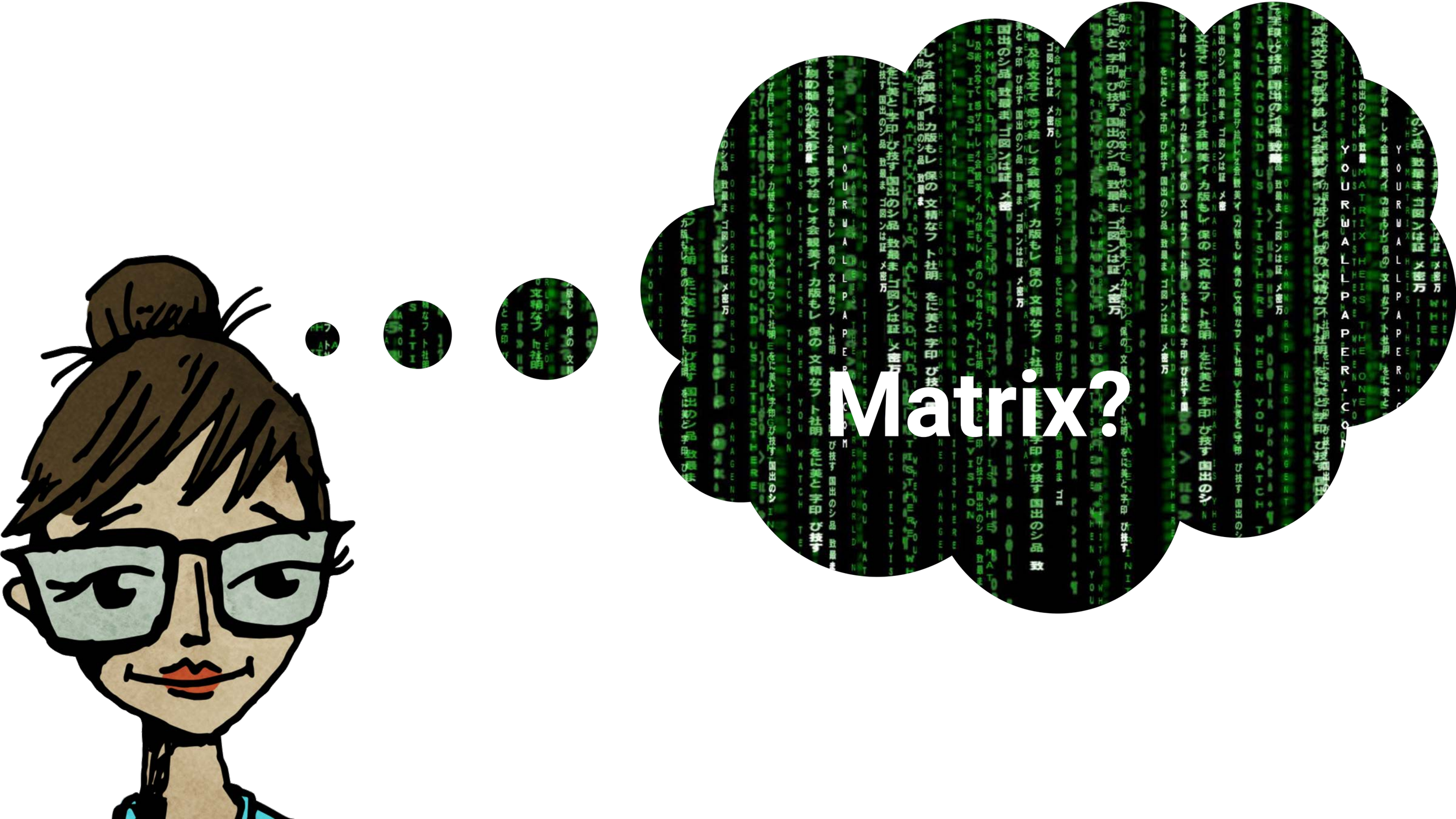
References

References

1. Falcone, R.. (2017 nt M-Trends 2018. Retrieved July 9, 2018.
Testing Efforts. R 17, October 9). OilRig Group Steps Up Attacks with New
2. ClearSky Cyberse lew Injector Trojan. Retrieved January 8, 2018.
Signed Malware, 17, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to
3. Falcone, R. and L etrieved January 8, 2018.
Organizations De 18, November 16). Analyzing OilRig's Ops Tempo from Testing
4. Grunzweig, J. and ery. Retrieved April 23, 2019.
Toolset and Expa er 27). Meet CrowdStrike's Adversary of the Month for
5. Unit 42. (2017, December 15). Unit 42 Playbook Viewer. Retrieved December 20, 2017. November: HELIX KITTEN. Retrieved December 18, 2018.
6. Sardiwal, M, et al. (2017, December 7). New Targeted Attack in the Middle East by APT34, a Suspected Iranian Threat Group, Using CVE-2017-11882 Exploit. Retrieved December 20, 2017.
7. Lee, B., Falcone, R. (2018, July 25). OilRig Targets Technology Service Provider and Government Agency with QUADAGENT. Retrieved August 9, 2018.
8. Davis, S. and Caban, D. (2017, December 19). APT34 - New Targeted Attack in the Middle East. Retrieved December 20, 2017.
9. Lee, B., Falcone, R. (2018, February 23). OopsIE! OilRig Uses ThreeDollars to Deliver New Trojan. Retrieved July 16, 2018.
15. Singh, S., Yin, H. (2016, May 22). https://www.fireeye.com/blog/threat-research/2016/05/targeted_attacksaga.html. Retrieved April 5, 2018.
16. Falcone, R. (2018, January 25). OilRig uses RGDoor IIS Backdoor on Targets in the Middle East. Retrieved July 6, 2018.
17. Wilhoit, K. and Falcone, R. (2018, September 12). OilRig Uses Updated BONDUPDATER to Target Middle Eastern Government. Retrieved February 18, 2019.

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service


Matrix?

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service

Re: Iranians in my HOPS!

MK

Mallory Kraeusen
Wed 7/24/2019 6:39 PM
Grace Hoppy

Grace,

Did some research using this nifty free thing called ATT&CK. Found out the following:

OilRig - Suspected Iranian group

- Has targeted financial, government, energy, chemical, and telecom industries
- Supposed leaks in March 2019
- Phishing campaign in June 2019 (APT34)
- Does appear to be a threat to Frothly due to targeting aligning with Iranian interests
- Tracking 200 indicators used by group

Mallory

From: Grace Hoppy <ghoppy@froth.ly>
Sent: Wednesday, July 24, 2019 8:47 PM

Re: Iranians in my HOPS!

MK

Mallory Kraeusen

Wed 7/24/2019 6:39 PM

Grace Hoppy

Grace,

Did some research using this nifty free thing called ATT&CK. Found out the following:

OilRig - Suspected Iranian group

- Has targeted financial, government, energy, chemical, telecom industries
- Supposed leaks in March 2019
- Phishing campaign in June 2019 (APT34)
- Does appear to be attempt to [illegible] aligning with Iranian interests
- Tracking 200 indicators used by group

Mallory

From: Grace Hoppy <ghoppy@froth.ly>
Sent: Wednesday, July 24, 2019 8:47 PM

“OilRig/Iranians… they’re a threat”

OilRig Indicators

MK

Mallory Kraeusen

Today, 9:54 PM

Alice Bluebird

Reply all

Sent Items

Alice,
  Long story but basically I need you to block/action a bunch of OilRig/APT34 references at the bottom of this page that have indicators. Please do 30-day searches and also proactively block. Thanks in advance!

https://attack.mitre.org/groups/G0049/

Regards,
  Mallory

OilRig Indicators

MK

Mallory Kraeusen

Today, 9:54 PM

Alice Bluebird

Reply all

Sent Item

Alice,

Long story but basically I need you to block/whitelist a bunch of OilRig/APT34 references at the bottom of this page that have indicators. Please do 30-day searches and also proactively block. Thanks in advance!

https://attack.mitre.org/groups/G0049/

Regards,

Mallory

“Plz block OilRig indicators. (TTPs wha?)”

From: Alice Bluebird <Abluebird@froth.ly>
Sent: Wednesday, July 24, 2019 10:34 PM
To: Mallory Kraeusen <mkraeusen@froth.ly>
Subject: Re: OilRig Indicators

Mallory,
Okay, we didn't have any hits and the indicators are all blocked. But what do we now? That doesn't seem like it will be good enough for Grace. There are technique thingamabobs on that page too. Maybe we can do something with those?

Alice
Network Defender Extraordinaire

From: Alice Bluebird <Abluebird@froth.ly>
Sent: Wednesday, July 24, 2019 10:34 PM
To: Mallory Kraeusen <mkraeusen@froth.ly>

"No hits…but what do we do now? What are these techniques?"

Mallory,

Alice
Network Defender Extraordinaire

How does Alice stop hoarding indicators and start detecting techniques?

T1057	Process Discovery	OilRig has run `tasklist` on a victim's machine.[3]
T1016	System Network Configuration Discovery	OilRig has run `ipconfig /all` on a victim.[3][4]
T1049	System Network Connections Discovery	OilRig has used `netstat -an` on a victim to get a listing of network connections.[3]
T1033	System Owner/User Discovery	OilRig has run `whoami` on a victim.[3][4]
T1007	System Service Discovery	OilRig has used `sc query` on a victim to gather information about services.[3]

Process Discovery

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software running on systems within the network.

Windows

An example command that would obtain details on processes is "tasklist" using the Tasklist utility.

Mac and Linux

In Mac and Linux, this is accomplished with the `ps` command.

ID: T1057

Tactic: Discovery

Platform: Linux, macOS, Windows

System Requirements: Administrator, SYSTEM may provide better process ownership details

Permissions Required: User, Administrator, SYSTEM

Data Sources: Process monitoring, Process command-line parameters

CAPEC ID: CAPEC-573

Version: 1.0

Process Discovery

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software running on systems within the network.

Windows

An example command that would obtain

Tasklist utility.

Mac and Linux

In Mac and Linux, this is accomplished w

Data Sources: Process monitoring, Process command-line parameters

ID: T1057

Tactic: Discovery

Platform: Linux, macOS, Windows

System Requirements: Administrator, SYSTEM may provide better process ownership details

Permissions Required: User, Administrator, SYSTEM

Data Sources: Process monitoring, Process command-line parameters

CAPEC ID: CAPEC-573

Version: 1.0

Correlation Search

Search Name *: Threat Activity Detected

App *: Enterprise Security

UI Dispatch Context *: Enterprise Security

Set an app to use for links such as the drill-down search in a notable event or links in an email adaptive response action. If None, uses the Application Context.

Description: Creating detection from ATT&CK for T1057 of tasklist.exe

Describes what kind of issues this search is intended to detect.

Mode: Guided | Manual

Search *:

```
index=*
(source="*WinEventLog:Security"  OR
EventCode=4688) Tasklist.exe
```


Correlation Search
Search Name *
Threat Activity Detected
App *
Enterprise Security
UI D
Description
Creating detection from ATT&CK for T1057 of tasklist.exe
Describes what kind of issues this search is intended to detect.
Mode
Guided
Manual
Search *
index=*
(source="*WinEventLog:Security" OR EventCode=4688) Tasklist.exe

```
>>> Signature = 0
>>> OilRigTechniques = 41
>>> while Signature < OilRigTechniques:
...     print("Write or find more signatures")
...     Signature += 1
...
```

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulati	Access Token Manipulati	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternativ Protocol	Disk Structure Wipe
Spearphishing Attachmen	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Comman and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Servic	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromis	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discove	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communicatior		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisonin and Relay	Remote System Discover	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass							
	Source	Launch Daemon	Sudo	Group Policy Modification							
	Space after Filename	Launchctl	Sudo Caching	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Additior	Valid Accounts	Hidden Users							
	Trap	Local Job Scheduling	Web Shell	Hidden Window							
	Trusted Developer Utilities	Login Item		HISTCONTROL							
	User Execution	Logon Scripts		Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver		Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchctl							
		Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		Rc.common		Modify Registry							
		Re-opened Applications		Mshta							
		Redundant Access		Network Share Connection Removal							
		Registry Run Keys / Startup Folder		NTFS File Attributes							
		Scheduled Task		Obfuscated Files or Information							
		Screensaver		Plist Modification							
		Security Support Provider		Port Knocking							
		Service Registry Permissions Weakness		Process Doppelgänging							
		Setuid and Setgid		Process Hollowing							
		Shortcut Modification		Process Injection							
		SIP and Trust Provider Hijacking		Redundant Access							
		Startup Items		Regsvcs/Regasm							
		System Firmware		Regsvr32							
		Systemd Service		Rootkit							
		Time Providers		Rundll32							
		Trap		Scripting							
		Valid Accounts		Signed Binary Proxy Execution							
		Web Shell		Signed Script Proxy Execution							
		Windows Management Instrumentation Event Subscription		SIP and Trust Provider Hijacking							
		Winlogon Helper DLL		Software Packing							
				Space after Filename							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

We’re good to go against OilRig, our #1 threat!

h/t to Kyle Rainey and Red Canary

How does Kevin test existing detections?

ATOMIC RED TEAM

T1057 - Process Discovery

Description from ATT&CK

> Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software running on systems within the network.
>
> ### Windows
>
> An example command that would obtain details on processes is "tasklist" using the Tasklist utility.
>
> ### Mac and Linux
>
> In Mac and Linux, this is accomplished with the `ps` command.

Atomic Tests

- Atomic Test #1 - Process Discovery - ps

Atomic Test #1 - Process Discovery - ps

Utilize ps to identify processes

Supported Platforms: macOS, CentOS, Ubuntu, Linux

Inputs

Name	Description	Type	Default Value
output_file	path of output file	path	/tmp/loot.txt

Run it with `sh` !

```
ps >> #{output_file}
ps aux >> #{output_file}
```

```
C:\>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0      6,700 K
smss.exe                       464 Services                   0        108 K
csrss.exe                      688 Services                   0      1,708 K
wininit.exe                    868 Services                   0         16 K
csrss.exe                      880 Console                    1      4,536 K
services.exe                   972 Services                   0      9,900 K
lsass.exe                      992 Services                   0     20,000 K
svchost.exe                    720 Services                   0        860 K
fontdrvhost.exe                728 Services                   0        672 K
svchost.exe                   1052 Services                   0     22,856 K
winlogon.exe                  1108 Console                    1      6,344 K
WUDFHost.exe                  1124 Services                   0      4,320 K
fontdrvhost.exe               1212 Console                    1      8,700 K
WUDFHost.exe                  1284 Services                   0      1,248 K
svchost.exe                   1348 Services                   0     15,492 K
svchost.exe                   1404 Services                   0      4,932 K
dwm.exe                       1552 Console                    1     65,448 K
svchost.exe                   1620 Services                   0      4,588 K
svchost.exe                   1628 Services                   0      5,436 K
```

Time	Urgency	Security Domain	Title	Status	Risk Score	Action
8/4/19 10:22:52.000 PM	Critical	Endpoint	Threat Activity Detected (Tasklist.exe)	New	0	
8/4/19 10:22:43.000 PM	Critical	Endpoint	Threat Activity Detected (Tasklist.exe)	New	0	
8/4/19 10:22:32.000 PM	Critical	Endpoint	Threat Activity Detected (ps)	New	0	
8/4/19 10:22:16.000 PM	Critical	Endpoint	Threat Activity Detected (Tasklist.exe)	New	0	
8/4/19 10:22:05.000 PM	Critical	Endpoint	Threat Activity Detected (Tasklist.exe)	New	0	
8/4/19 10:21:07.000 PM	Critical	Endpoint	Threat Activity Detected (Tasklist.exe)	New	0	
8/4/19 10:22:43.000 PM	Critical	Endpoint	Threat Activity Detected (Tasklist.exe)	New	0	
8/4/19 10:22:32.000 PM	Critical	Endpoint	Threat Activity Detected (ps)	New	0	
8/4/19 10:22:16.000 PM	Critical	Endpoint	Threat Activity Detected (Tasklist.exe)	New	0	
8/4/19 10:22:05.000 PM	Critical	Endpoint	Threat Activity Detected (Tasklist.exe)	New	0	
8/4/19	Critical	Endpoint	Threat Activity Detected	New	0	

Time	Urgency	Security Domain	Title	Status	Risk Score	Action
8/4/19 10:22:52.000 PM	Critical	Endpoint	Threat Activity Detected (Tasklist.exe)	New	0	
8/4/19 10:22:43.000 PM	Critical	Endpoint	Threat Activity Detected (Tasklist.exe)	New	0	
8/4/19 10:22:32.000 PM	Critical	Endpoint	Threat Activity Detected (ps)	New	0	
8/4/19 10:22:16.000 PM	Critical	Endpoint	Threat Activity Detected (Tasklist.exe)	New	0	
8/4/19 10:22:05.000 PM	Critical	Endpoint	Threat Activity Detected (Tasklist.exe)	New	0	
8/4/19 10:21:07.000 PM	Critical	Endpoint	Threat Activity Detected (Tasklist.exe)	New	0	
8/4/19 10:22:43.000 PM	Critical	Endpoint	Threat Activity Detected (Tasklist.exe)	New	0	
8/4/19 10:22:32.000 PM	Critical	Endpoint	Threat Activity Detected (ps)	New	0	
8/4/19 10:22:16.000 PM	Critical	Endpoint	Threat Activity Detected (Tasklist.exe)	New	0	
8/4/19 10:22:05.000 PM	Critical	Endpoint	Threat Activity Detected (Tasklist.exe)	New	0	
8/4/19	Critical	Endpoint	Threat Activity Detected			

Attacks detected!


We did all the things. This is fine. Everything is fine.


And then...


FBI
FBI
FBI
“Sorry, you’re pwned.”

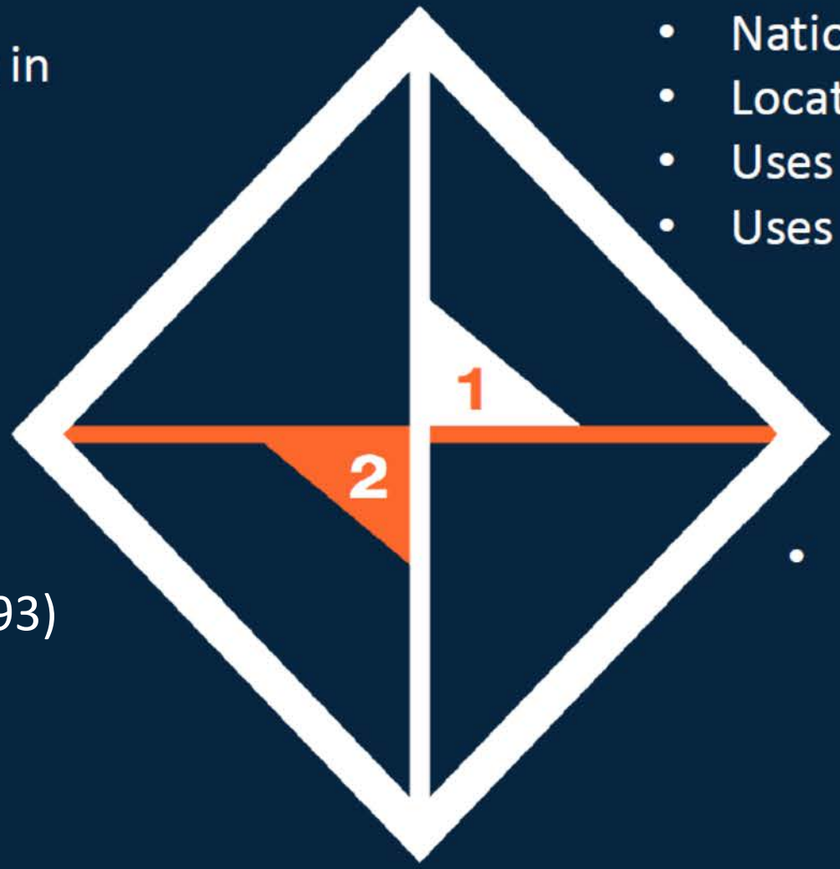

LIVE
BREAKING NEWS
FROTHLY HACKED BY TAEDONGGANG
1:12
DATA STOLEN! INSIDER THREAT? WILL THIS AFFECT THEIR IPO? WAS BOTS FOR NAUGH

1 SOCIO-POLITICAL AXIS

- Seeking to obtain high end Western Beers for production in their breweries

ADVERSARY

- Nation state sponsored adversary
- Located (+8.0 time zone)
- Uses Korean encoded language
- Uses Hancom Thinkfree Office



CAPABILITIES

- PowerShell (T1086)
- Spearphishing Attachment (T1193)
- Service Execution (T1035)

INFRASTRUCTURE

- European VPS servers

2 TECHNICAL AXIS

- Documents with .hwp suffix
- PS exec lateral movement
- YMLP
- Self signed SSL/TLS certificates
- +8.0 hour time zone
- Korean fonts for English
- Korean text google translated to English
- Naenara user agent string

VICTIMS

- Western innovative Brewers and Home Brewing companies

A special thanks to THREATCONNECT


WHY DID WE EVER USE ATT&CK?

So you've "implemented" ATT&CK and you're unhappy…now what?

What went wrong?

CxO

Had a false sense of security

Couldn’t follow up and action new threats

CTI

Defender

Had gaps in defenses but drowning in alerts

Didn’t test in depth or work with Blue Team

Red Team

Let’s get Frothly back on track

How can a CxO have a better understanding of their risk by using ATT&CK?

Communicate confidence level

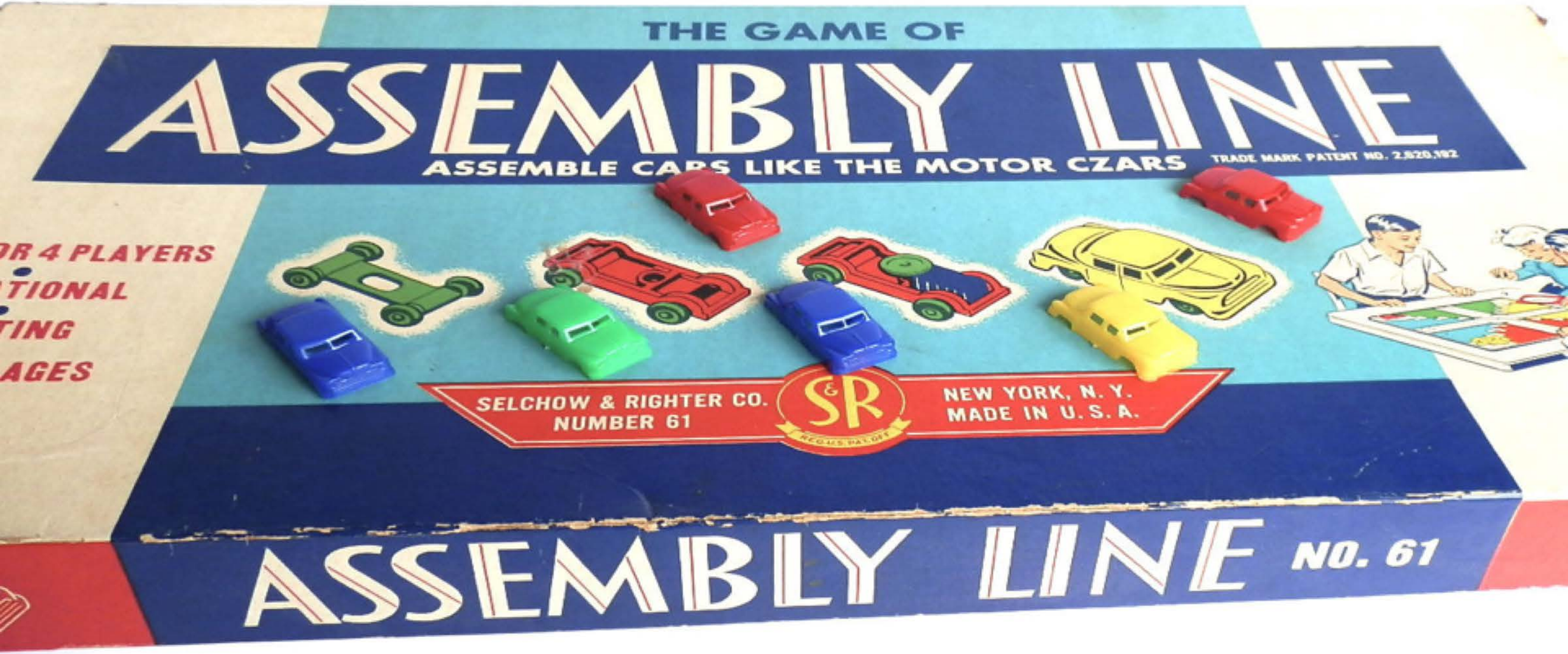
Initial Access 11 items	Execution 33 items	Persistence 59 items	Privilege Escalation 28 items	Defense Evasion 67 items	Credential Access 19 items	Discovery 22 items	Lateral Movement 17 items	Collection 13 items	Command And Control 16 items	Exfiltration 9 items	Impact 14 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass							
	Source	Launch Daemon	Sudo	Group Policy Modification							
	Space after Filename	Launchctl	Sudo Caching	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Users							
	Trap	Local Job Scheduling	Web Shell	Hidden Window							
	Trusted Developer Utilities	Login Item		HISTCONTROL							
	User Execution	Logon Scripts		Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver		Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchctl							
		Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		Rc.common		Modify Registry							
		Re-opened Applications		Mshta							
		Redundant Access		Network Share Connection Removal							
		Registry Run Keys / Startup Folder		NTFS File Attributes							
		Scheduled Task		Obfuscated Files or Information							
		Screensaver		Plist Modification							
		Security Support Provider		Port Knocking							
		Service Registry Permissions Weakness		Process Doppelgänging							
		Setuid and Setgid		Process Hollowing							
		Shortcut Modification		Process Injection							
		SIP and Trust Provider Hijacking		Redundant Access							
		Startup Items		Regsvcs/Regasm							
		System Firmware		Regsvr32							
		Systemd Service		Rootkit							
		Time Providers		Rundll32							
		Trap		Scripting							
		Valid Accounts		Signed Binary Proxy Execution							
		Web Shell		Signed Script Proxy Execution							
		Windows Management Instrumentation Event Subscription		SIP and Trust Provider Hijacking							
		Winlogon Helper DLL		Software Packing							
				Space after Filename							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

Color gradient by confidence in detections

0 5

h/t to Olaf Hartong

Integrate your teams



Red Team

Threats

Capabilities

Gaps

Detections

ATT&CK

What's my Risk?

Risk to org

CxO

CTI

Threats in theory

Real detections

Defender

Crawl

Walk

Run

MITRE ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credentials in Files	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Registry	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Supply Chain Compromise	Exploitation for Client	Bootkit	Exploitation for Privilege	Compiled HTML File	Hooking	Password Policy	Remote File	Email Collection	Scheduled Transfer	Domain Generation

Active: 1
Available: 15
Needs data: 1
Total: 17
Selected: 0
Threat Groups:
OilRig

MITRE ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drag-by Compromise	AppleScript	.bash_profile and .bashrc	Access Manipulation	Binary Padding	Bash History	Application Window Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Clear Command History	Credentials in Files	Network Service Scanning	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Registry	Network Share Discovery	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Compile After Delivery	Forced Authentication	Password Policy Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Hooking	Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Input Capture	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Domain Generation Algorithms

Command-Line Interface

Account Manipulation

Dynamic Data Exchange

Application Shimming

Active: 1
Available: 19
Needs data: 0
Total: 20
Selected: 0
Threat Groups:
OilRig

How can a threat intel analyst action new threats?

Build your own threat library

Karkoff

TLP: WHITE

Confidence Level	Medium
Other Known Names	

Description

Karkoff is a lightweight backdoor used by the DNSpionage group. According to SecureList researchers,its developers didn't obfuscate or include any defense measures to avoid the malware to be disassembled. The malware will persist as a service with the name "MSExchangeClient", mimicking a Microsoft legitimate tool.

Campaign	Techniques	Tactics	Description
DNSpionage Upgraded Their Tool into Karkoff	DTTT0008 - Environment Awareness*	Defense Evasion	Karkoff uses the information collected from the local system in order to fingerpint the victims and avoid researchers or sandboxes.
DNSpionage Upgraded Their Tool into Karkoff	DTTT0024 - File Management	Collection	Karkoff logs the executed command in a log file.
DNSpionage Upgraded Their Tool into Karkoff	T1001 - Data Obfuscation	Command and Control	Karkoff uses base64 encoding to initially obfuscate C2 communications.
DNSpionage Upgraded Their Tool into Karkoff	T1005 - Data from Local System	Collection	Karkoff collects data from the local system.

Most Used Techniques (2019 sample)

#	Technique Name
1	T1071 - Standard App Layer Protocol
2	T1082 - System Information Discovery
3	T1059 - Command-Line Interface
4	T1105 - Remote File Copy
5	T1083 - File and Directory Discovery
6	T1060 - Registry Run Keys / Start Folder
7	T1057 - Process Discovery

8	T1056 - Input Capture
9	T1113 - Screen Capture
10	T1107 - File Deletion
11	T1041 - Exfiltration Over C2 Channel
12	T1086 - PowerShell
13	T1193 - Spearphishing Attachment
14	T1016 - System Network Config Discovery

Courtesy of the Threat Library Team – Deloitte

Build on the framework

Karkoff

TLP: WHITE

Confidence Level

Other Known Names

Description

Karkoff is a lightweight backdoor used by the DNSpionag esearchers,its developers didn't obfuscate or include any defense measures to avoid the malware to be disass s a service with the name "MSExchangeClient", mimicking a Microsoft legitimate tool.

DTTT0008 - Environment Awareness*

Campaign	Techniques	Tactics	Description
DNSpionage Upgraded Their Tool into Karkoff	DTTT0008 - Environment Awareness*	D B	formation collected from the local system in order to ms and avoid researchers or sandboxes.
DNSpionage Upgraded Their Tool into Karkoff	DTTT0024 - File Management	C	ecuted command in a log file.
DNSpionage Upgraded Their Tool into Karkoff	T1001 - Data Obfuscation	Command and Control	Karkoff uses base64 encoding to initially obfuscate C2 communications.
DNSpionage Upgraded Their Tool into Karkoff	T1005 - Data from Local System	Collection	Karkoff collects data from the local system.

T1001 - Data Obfuscation

Courtesy of the Threat Library Team – Deloitte

About Techniques Naming Convention

Naming convention	Use	Example
TXXXX	For Mitre's ATT&CK framework techniques	T1208 - Kerberoasting
DTTTXXXX	For Deloitte techniques unavailable in Mitre's ATT&CK framework	DTTT0001 - Bashware

Courtesy of the Threat Library Team – Deloitte

DTT0006 - DNS Tunneling

TLP: WHITE

Confidence Level	High

Description

DNS Tunneling is a technique used for Command and Control and Data Exfiltration. Also known as **VPN over DNS**, it's based on using the Domain Name Server protocol (DNS) as a covert communication channel, bypassing the organization's firewall. The Cyber Actors can tunnel other protocol such as SSH or HTTP within DNS, and covertly exfiltrate the information stolen or tunnel IP traffic. There are multiple instances on where DNS was used as a tunnel as a bidirectional and full remote control channel for compromised hosts in the internal network. This technique can allow Cyber Actors to transfer files, download additional malware modules, etc. DNS tunnels can also be used to bypass captive portals, to avoid paying for WiFi service and bypass other restrictions.

> ⓘ Please note that DNS Tunneling is considered a sub-technique for T1094 - Custom Command and Control Protocol, although is being conserved for clarification purposes

DTTT0006 - DNS Tunneling

TLP: WHITE

DTTT0006 - DNS Tunneling

Confide

Description

DNS Tunneling is a technique used for Command and Control and Data Exfiltration. Also known as **VPN over DNS**, it's based on using the Doma tors can tunnel oth multiple instances rnal network. o be used to bypass captive portals, to avoid paying for WiFi service and bypass other restrictions.

DNS Tunneling is considered a sub-technique for

T1094 - Custom Command and Control Protocol

Please note that DNS Tunneling is considered a sub-technique for T1094 - Custom Command and Control Protocol, although is being conserved for clarification purposes

Courtesy of the Threat Library Team – Deloitte

DTTT0021 - Timing-based evasion*

TLP: WHITE

Confidence Level	High

Description

Timing-based evasion is a technique used by malware to run at specific times of the day or after certain user's actions, such as opening a specific program, click on a specific part of a document, executing only after a system reboot, or before or after specific dates.

Deprecated

This technique is deprecated and shouldn't be used. This technique has been replaced by ATT&CK Framework technique T1497 - Virtualization/Sandbox Evasion. This technique will be maintained for compatibility with past items.

Courtesy of the Threat Library Team – Deloitte

DTTT0021 - Timing-based evasion*

TLP: WHITE

Deprecated

replaced by ATT&CK Framework technique T1497 - Virtualization/Sandbox Evasion.

Courtesy of the Threat Library Team – Deloitte

How can a blue teamer know what to detect and if she has the right data?

Map data to TTPs

Process Discovery

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software running on systems within the network.

Windows

An example command that would obtain

Tasklist utility.

Mac and Linux

In Mac and Linux, this is accomplished w

Data Sources: Process monitoring, Process command-line parameters

ID: T1057

Tactic: Discovery

Platform: Linux, macOS, Windows

System Requirements: Administrator, SYSTEM may provide better process ownership details

Permissions Required: User, Administrator, SYSTEM

Data Sources: Process monitoring, Process command-line parameters

CAPEC ID: CAPEC-573

Version: 1.0

scripts

This folder contains one-off scripts for working with ATT&CK content. These scripts are included either because they provide useful functionality or as demonstrations of how to fetch, parse or visualize ATT&CK content.

script	description
techniques_from_data_source.py	Fetches the current ATT&CK STIX 2.0 objects from the ATT&CK TAXII server, prints all of the data sources listed in Enterprise ATT&CK, and then lists all the Enterprise techniques containing a given data source. Run `python3 techniques_from_data_source.py -h` for usage instructions.
techniques_data_sources_vis.py	Generate the csv data used to create the "Techniques Mapped to Data Sources" visualization in the ATT&CK roadmap. Run `python3 techniques_data_sources_vis.py -h` for usage instructions.

https://github.com/mitre-attack/attack-scripts/tree/master/scripts

Assess your data potential with ATTACK Datamap

Olaf Hartong Follow

Apr 7 · 4 min read

https://medium.com/@olafhartong/assess-your-data-potential-with-att-ck-datamap-f44884cfed11

The Unfetter Project

Discover and analyze gaps in your security posture.

https://nsacyber.github.io/unfetter/

DeTT&CT

Detect Tactics, Techniques & Combat Threats

https://github.com/rabobank-cdc/DeTTECT

Atomic Threat Coverage

Automatically generated actionable analytics designed to combat threats based on MITRE's ATT&CK.

https://github.com/krakow2600/atomic-threat-coverage

Content selection

Status: Any

Originating app: Any

MITRE Tactic: Any

MITRE Technique: Process Discovery

MITRE Threat Group: Any

Data Source: Any

Data Source Category: Any

Bookmark Status: Any

Featured: Any

Search Filter:

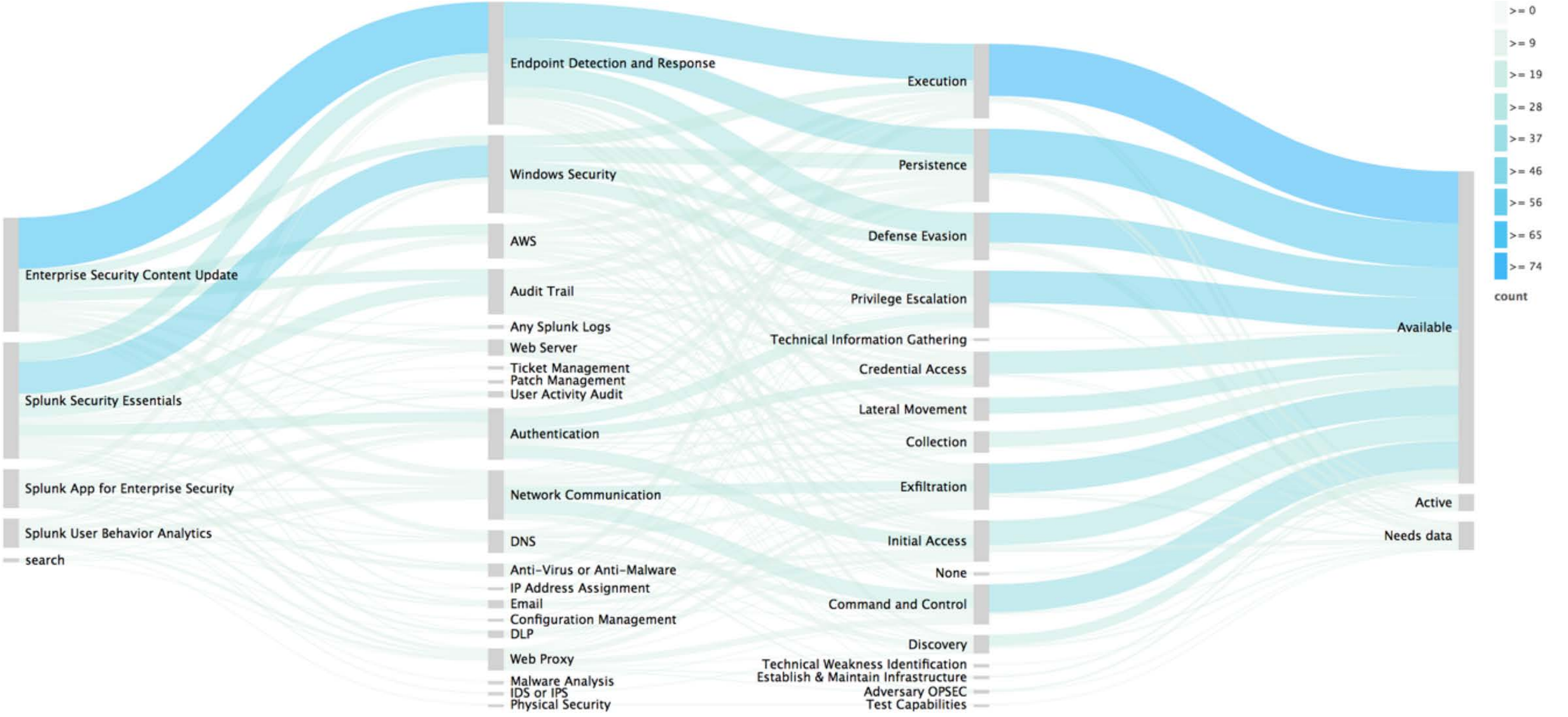
2. Selected Content

Use the drop downs or tables to further filter your selection.

Selection | Content list | Selection by Data Source | **Selection by Data Source Category** | Selection by MITRE Tactic | Selection by MITRE Technique | Selection by MITRE Threat Group

Click to filter

	Data Source Category	Total	Active	Available	Needs data	Selected	eventtypeId	Data Availability	Data Coverage
1	Process Launch	4	0	4	0	0	DS009EndPointIntel-ET01ProcessLaunch	Good	failure
2	Process Launch	2	0	2	0	0	VendorSpecific-winsec	Good	complete
3	Windows Security Logs	2	0	2	0	0	DS009EndPointIntel-ET01ProcessLaunch	Good	failure
4	Windows Security Logs	2	0	2	0	0	VendorSpecific-winsec	Good	complete


Enterprise Security Content Update
Splunk Security Essentials
Splunk App for Enterprise Security
Splunk User Behavior Analytics
search
Endpoint Detection and Response
Windows Security
AWS
Audit Trail
Any Splunk Logs
Web Server
Ticket Management
Patch Management
User Activity Audit
Authentication
Network Communication
DNS
Anti-Virus or Anti-Malware
IP Address Assignment
Email
Configuration Management
DLP
Web Proxy
Malware Analysis
IDS or IPS
Physical Security
Execution
Persistence
Defense Evasion
Privilege Escalation
Technical Information Gathering
Credential Access
Lateral Movement
Collection
Exfiltration
Initial Access
None
Command and Control
Discovery
Technical Weakness Identification
Establish & Maintain Infrastructure
Adversary OPSEC
Test Capabilities
Available
Active
Needs data
>= 0
>= 9
>= 19
>= 28
>= 37
>= 46
>= 56
>= 65
>= 74
count

One Sig!=Complete TTP Coverage

MITRE Cyber Analytics Repository

Analytics Data Model Sensors

Fork me on GitHub

Welcome to the Cyber Analytics Repository

The MITRE Cyber Analytics Repository (CAR) is a knowledge base of analytics developed by MITRE based on the MITRE ATT&CK adversary model.

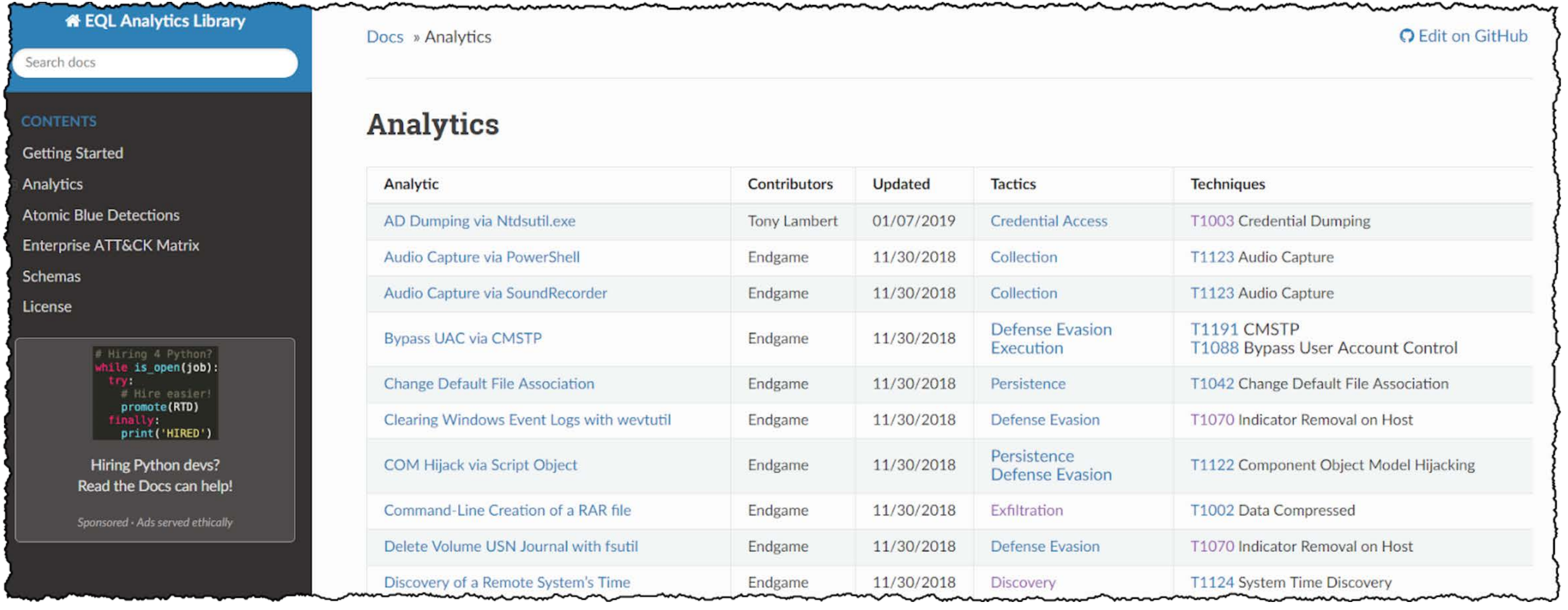
If you want to start exploring, try viewing the Full Analytic List or use the CAR Exploration Tool (CARET). Also, check out the new ATT&CK Navigator Layer that captures the current set of ATT&CK tactics and techniques covered by CAR.

Analytics stored in CAR contain the following information:

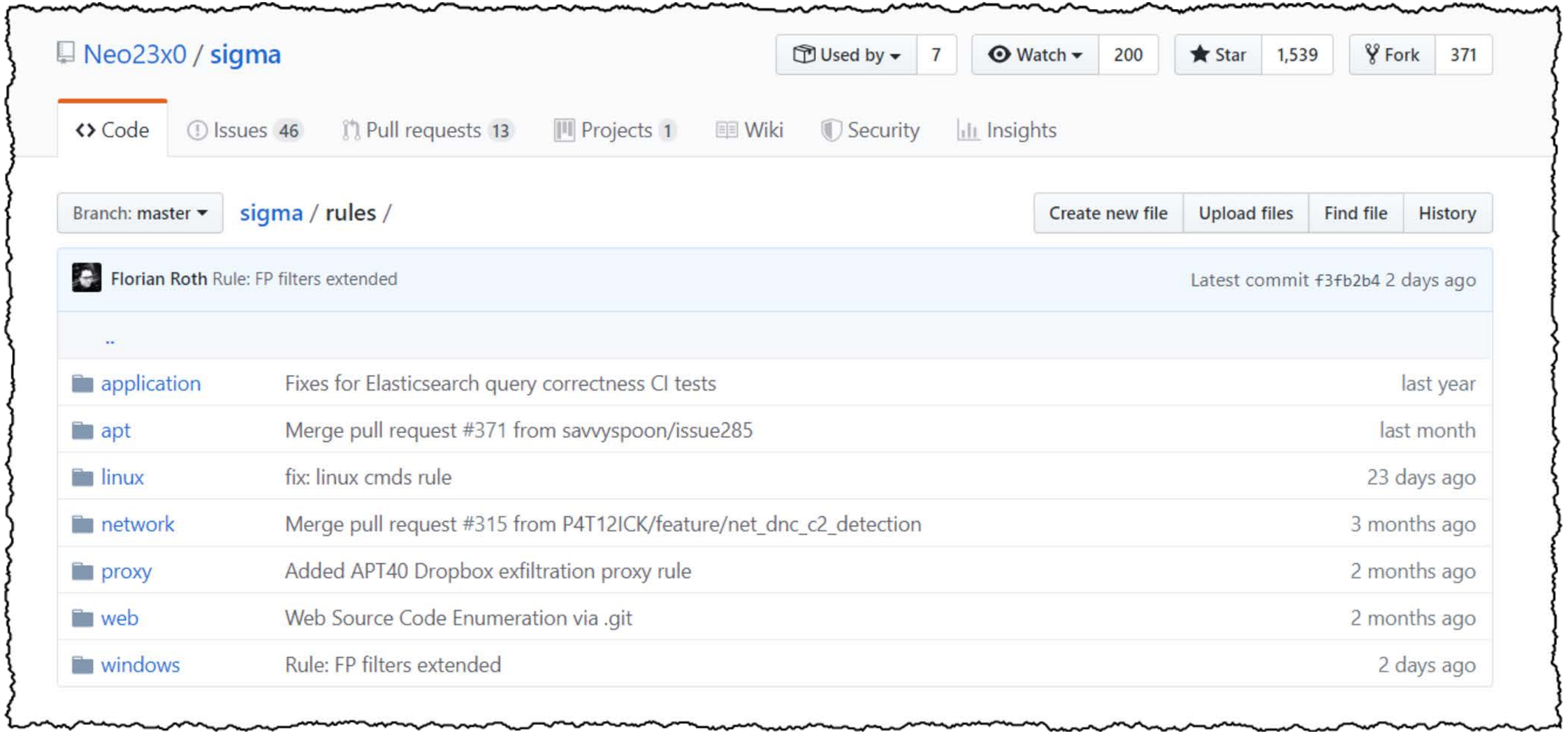
- a *hypothesis* which explains the idea behind the analytic
- the *information domain* or the primary domain the analytic is designed to operate within (e.g. host, network, process, external)
- references to ATT&CK Techniques and Tactics that the analytic detects
- the Glossary
- a pseudocode description of how the analytic might be implemented
- a unit test which can be run to trigger the analytic

In addition to the analytics, CAR also contains a data model for observable data used to run the analytics and sensors that are used to collect that data.

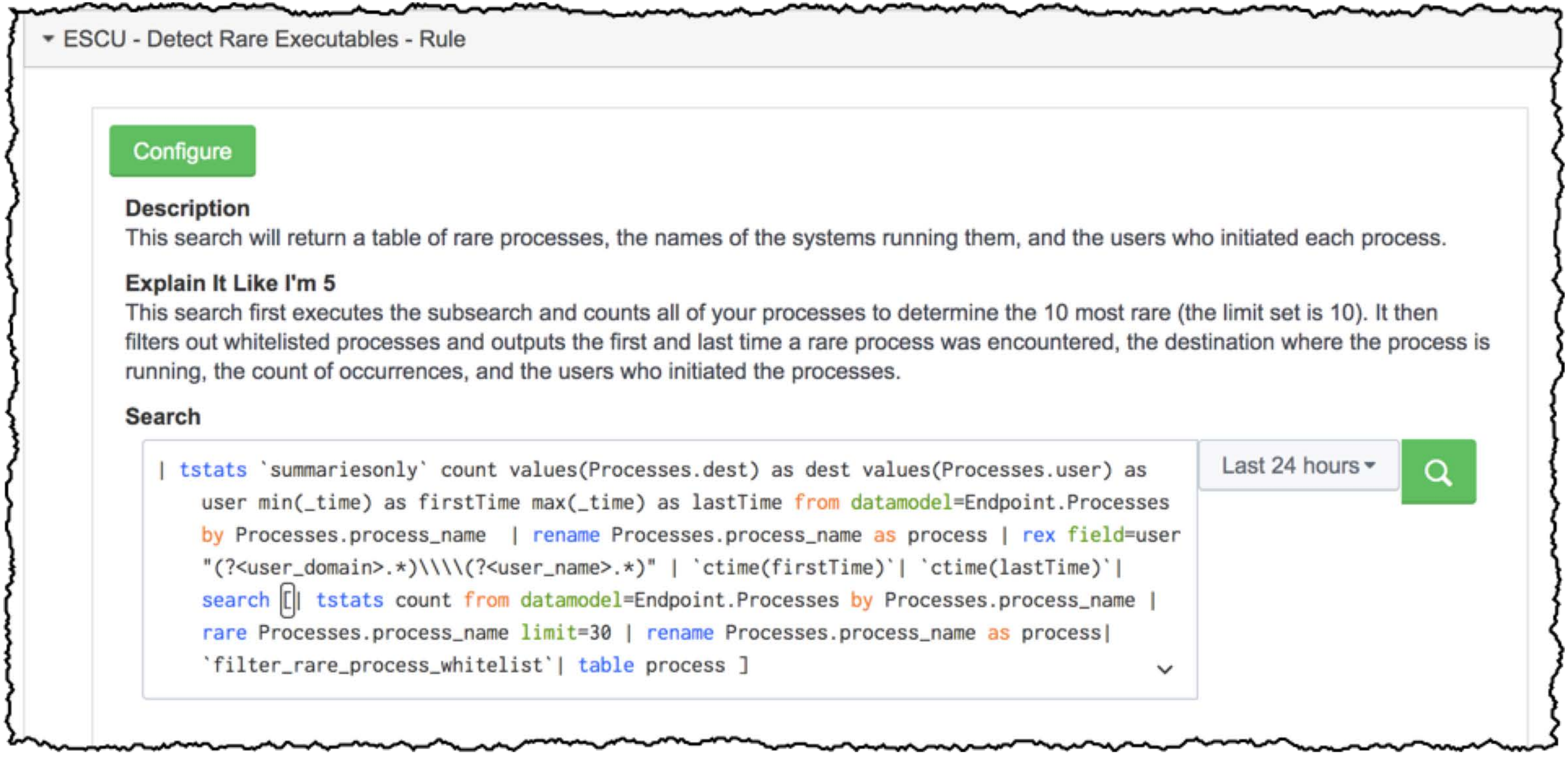
https://car.mitre.org/



https://eqllib.readthedocs.io/en/latest/analytics.html



https://github.com/Neo23x0/sigma/tree/master/rules


ESCU - Detect Rare Executables - Rule
Configure
Description
This search will return a table of rare processes, the names of the systems running them, and the users who initiated each process.
Explain It Like I'm 5
This search first executes the subsearch and counts all of your processes to determine the 10 most rare (the limit set is 10). It then filters out whitelisted processes and outputs the first and last time a rare process was encountered, the destination where the process is running, the count of occurrences, and the users who initiated the processes.
Search
| tstats `summariesonly` count values(Processes.dest) as dest values(Processes.user) as user min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes by Processes.process_name | rename Processes.process_name as process | rex field=user "(?<user_domain>.*)\\\\(?<user_name>.*)" | `ctime(firstTime)`| `ctime(lastTime)`| search [| tstats count from datamodel=Endpoint.Processes by Processes.process_name | rare Processes.process_name limit=30 | rename Processes.process_name as process| `filter_rare_process_whitelist`| table process]
Last 24 hours

		Time	Security Domain	Title	Urgency	Statu
⌄	☐	8/4/19 8:05:47.000 AM	Access	Brute Force Access Behavior Detected From 10.255.3.2	⚠ Medium	New

Description:

The system 10.255.3.2 has failed authentication 40 times and successfully authenticated 4 times in the last hour

Additional Fields	Value	Action
Application	sshd	
Category	Lateral MovementIIAM Analytics	
Kill Chain Phase	None	
MITRE ATT&CK Tactic ID	TA0006	
MITRE ATT&CK Tactic	TA0006 - Credential Access	
MITRE ATT&CK Technique ID	T1110	
MITRE ATT&CK Technique	T1110 - Brute Force	
MITRE ATT&CK Technique Description	Adversaries may use brute force techniques to attempt access to accounts when passwords are unknown or when password hashes are obtained. [Credential Dumping] (https://attack.mitre.org/techniques/T1003) is used to obtain password hashes, this may only get an	

Related Investigations:

Currently not investigated.

Correlation Search:

Access - Brute Force Access Behavior Detected - Rule

History:

View all review activity for this Notable Event

Contributing Events:

View all login attempts by system 10.255.3.2

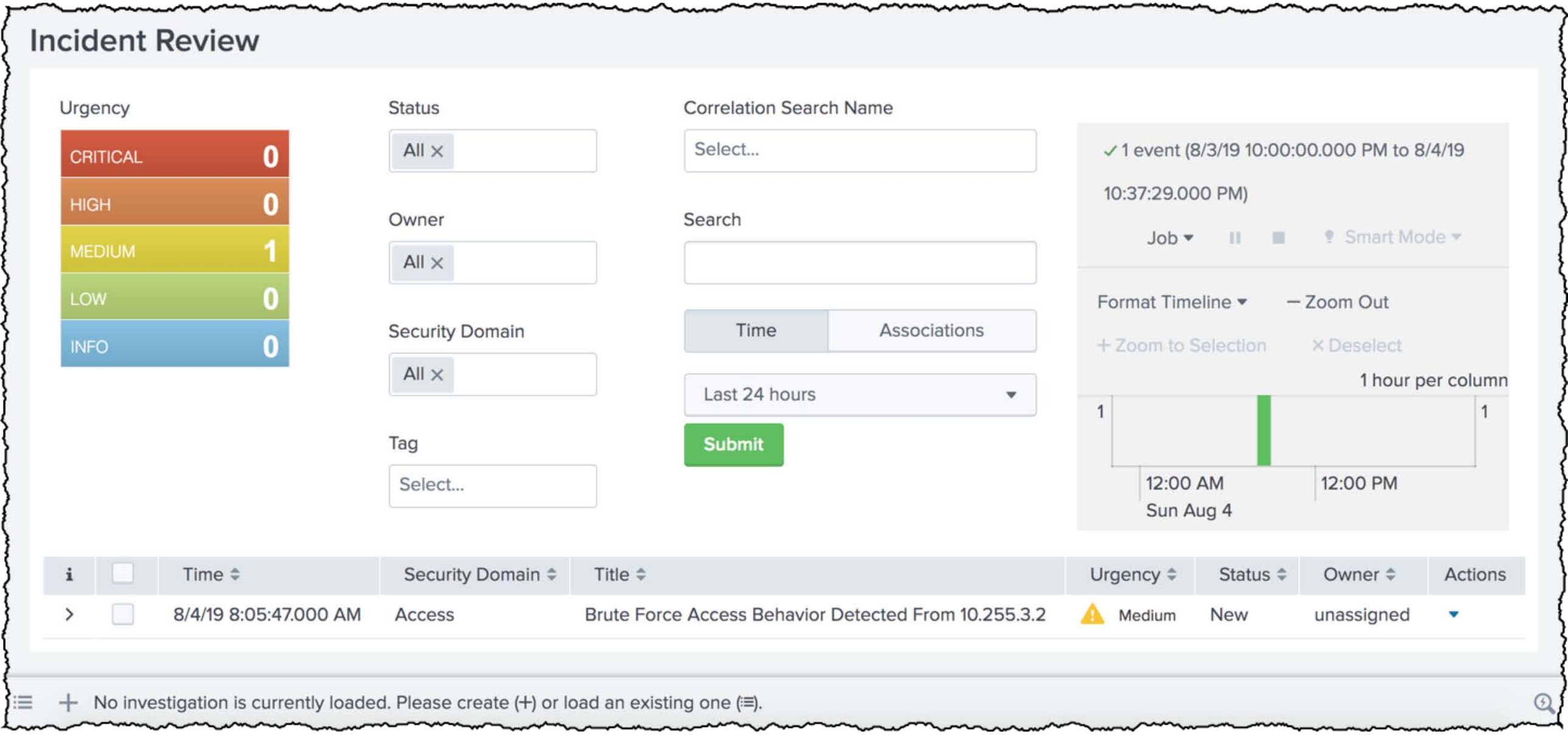
Adaptive Responses: ⟳

Response	Mode	Time
Notable	saved	2019-08-04T08:05:47+0000
Risk Analysis	saved	2019-08-04T08:05:47+0000

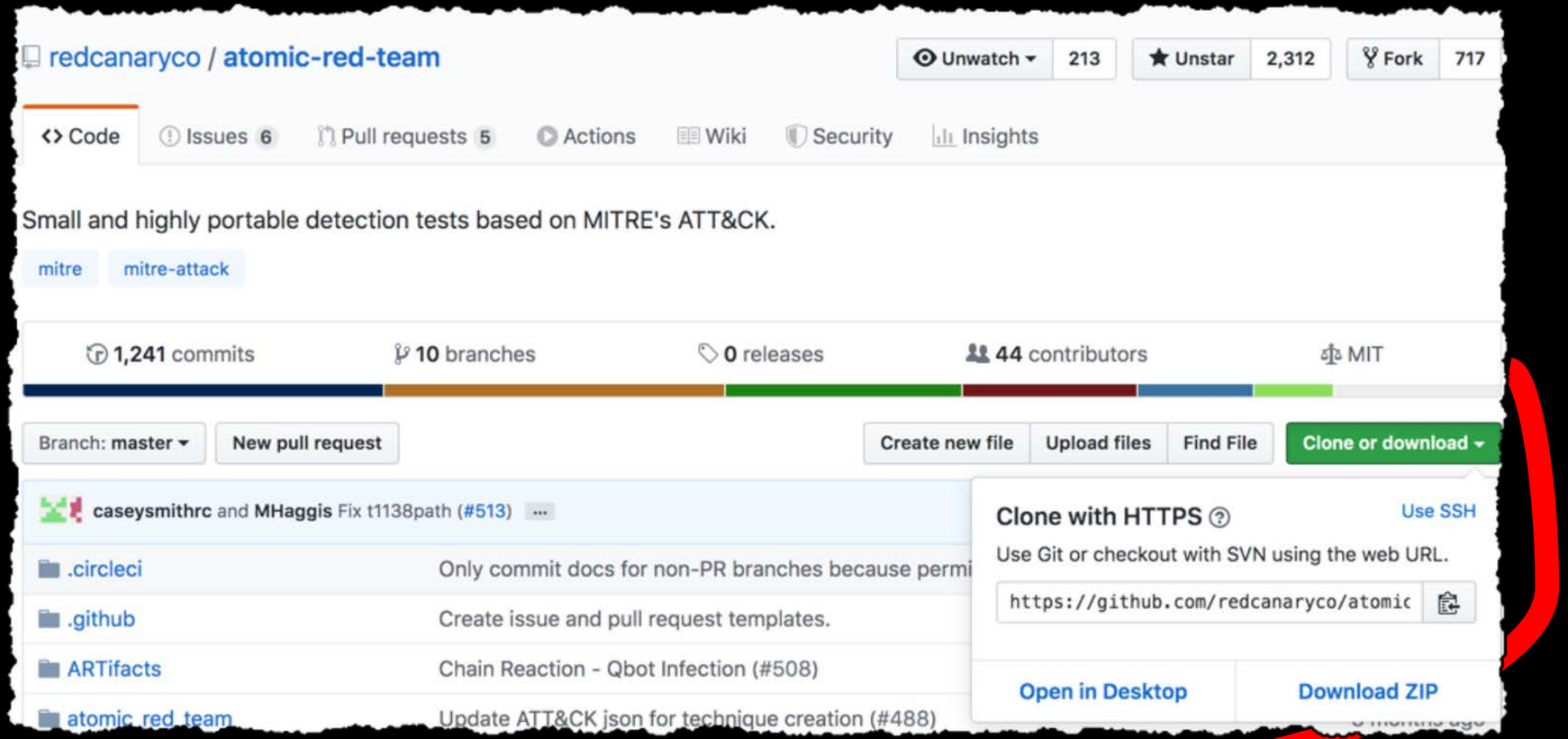
View Adaptive Response Invocations

Additional Fields	Value	Action
Application	sshd	
Category	Lateral Movement|IAM Analytics	
Kill Chain Phase	None	
MITRE ATT&CK Tactic ID	TA0006	
MITRE ATT&CK Tactic	TA0006 - Credential Access	
MITRE ATT&CK Technique ID	T1110	
MITRE ATT&CK Technique	T1110 - Brute Force	
MITRE ATT&CK Technique Description	Adversaries may use brute force techniques to attempt access to accounts when	

Reduced Alerts



How can a red teamer help improve defenses?




```
/Users/jacob /Documents/Frothly_Atomics/atomics/T1057
notyobox:T1057  jacob $ ls
T1057-F.md      T1057.md        T1057.yaml
```

```
// Get a handle to the process.

hProcess = OpenProcess( PROCESS_QUERY_INFORMATION |
                        PROCESS_VM_READ,
                        FALSE, processID );
if (NULL == hProcess)
    return 1;

// Get a list of all the modules in this process.

if( EnumProcessModules(hProcess, hMods, sizeof(hMods), &cbNee
{
    for ( i = 0; i < (cbNeeded / sizeof(HMODULE)); i++ )
    {
        TCHAR szModName[MAX_PATH];
```

https://docs.microsoft.com/en-us/windows/win32/psapi/enumerating-all-modules-for-a-process

Go Purple

What blue detected

What red did that blue missed


Combine your powers for hunting parties


13 DEAD END DRIVE
How do you (and Frothly) “Play at Home”
with ATT&CK?

“How are we defended?”

“I can **communicate** about our defenses and make better **decisions**.”

“If it’s not an IP,
how do I use it?”

“I’m tracking **multiple** threats
and I’m a
Pyramid of Pain **master**.”

“I’m drowning in alerts and missing data!”

“I can **prioritize** alerts and **use** the data I have.”

“I don’t know how to help!”

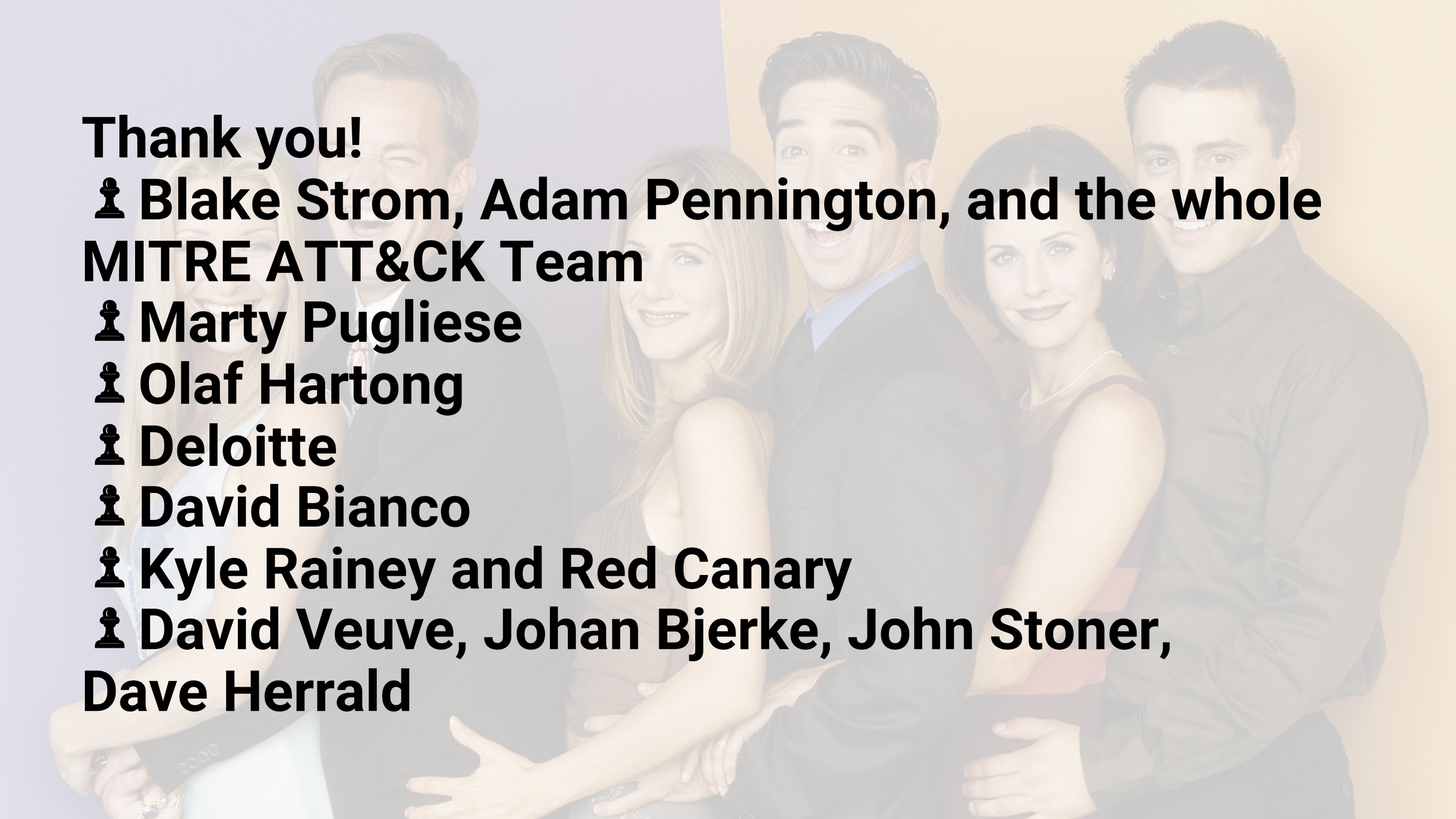
“I know how to **help** defense get better.”

Takeaways

- ♟ ATT&CK is for everyone
- ♟ Start small and be realistic
- ♟ Collaborate and cooperate

Thank you!

- Adriana and Deveeshree
- Black Hat
- Splunk, Haiyan Song, Cara Cavaggion



Thank you!

- Blake Strom, Adam Pennington, and the whole MITRE ATT&CK Team
- Marty Pugliese
- Olaf Hartong
- Deloitte
- David Bianco
- Kyle Rainey and Red Canary
- David Veuve, Johan Bjerke, John Stoner, Dave Herrald

References

https://github.com/mitre-attack/attack-navigator
https://github.com/redcanaryco/atomic-red-team
https://redcanary.com/blog/avoiding-common-attack-pitfalls/
https://splunkbase.splunk.com/app/3435
https://github.com/mitre-attack/attack-scripts/tree/master/scripts
https://medium.com/@olafhartong/assess-your-data-potential-with-attck-datamap-f44884cfed11
https://nsacyber.github.io/unfetter/
https://github.com/rabobank-cdc/DeTTECT
https://github.com/krakow2600/atomic-threat-coverage
https://car.mitre.org/
https://eqllib.readthedocs.io/en/latest/analytics.html
https://github.com/Neo23x0/sigma/tree/master/rules
https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Questions?
-->Join us in Coral B

Katie Nickels
(@LiketheCoins)
attack@mitre.org

Ryan Kovar
(@meansec)