

AMERICA'S ALL TIME
FAVORITE MODEL

ATT&CK™

MITRE ATT&CK: The Play at Home Edition v2.0

IT'S A HIT

T1100

ATT&CK

- Katie Nickels @ MITRE
- Ryan Kovar @ Splunk

for
2
players

OBJECT
Sink all of your
opponent's ships.

average playtime 20 minutes

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.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

© 2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 19-01159-11.



We use Splunk

But you don't have to!

Agenda

 **Let's tell a story**

 **Oops, now I see where we went wrong**

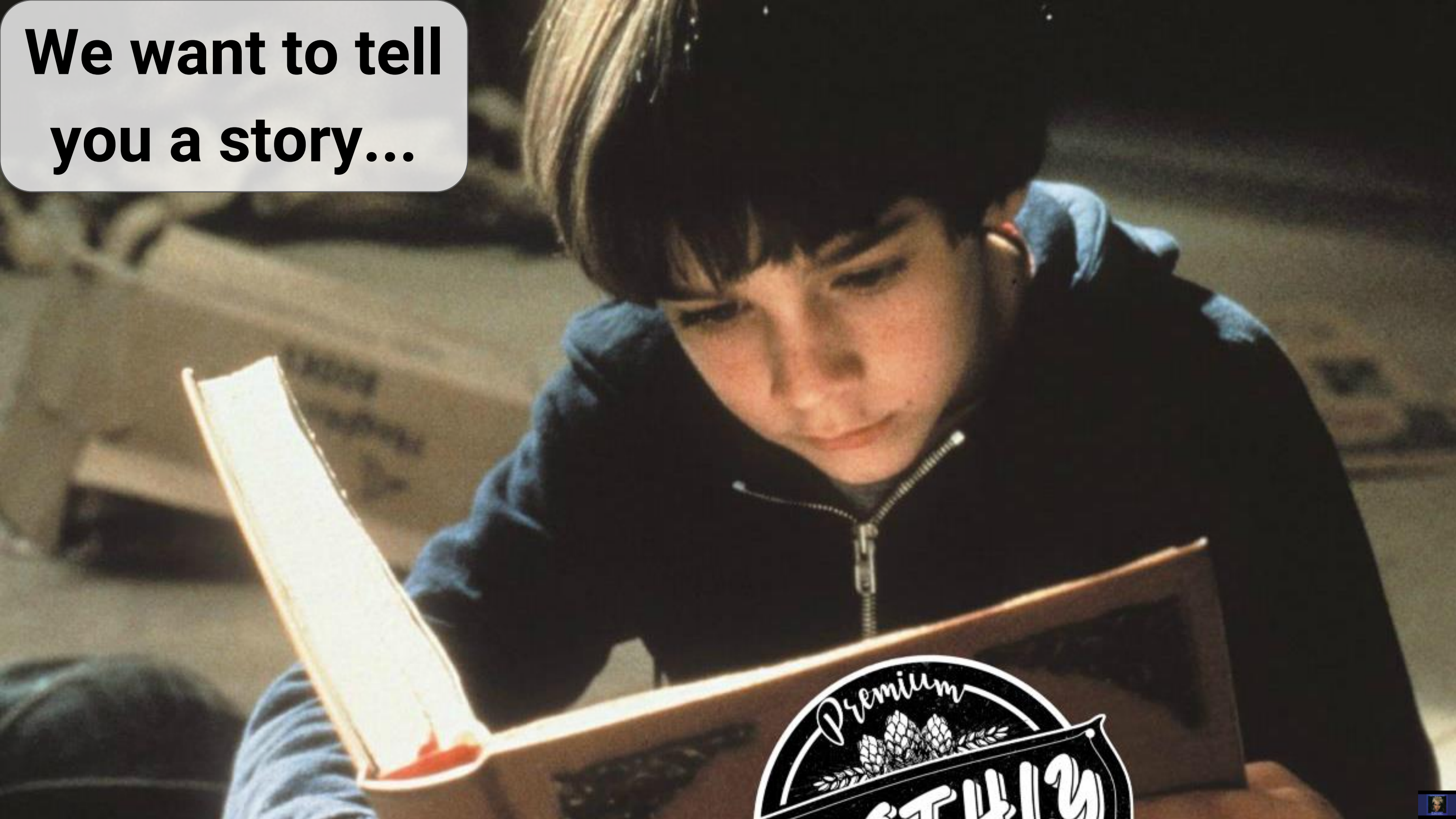
 **Pass go, collect 200 TTPs**

**So you've heard of
this ATT&CK thing...**

**but how do you
actually play *use* it?**



**We want to tell
you a story...**







“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!



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!



Grace Hoppy

Today, 8:47 PM

Reply all | v

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

Inbox

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

Regards,

Grace Hoppy

CEO

"Have a nice day!"



**How does Mallory find info on Iranian groups...
...and can **ATT&CK** help?**



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.
PROMETHIUM		PROMETHIUM 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 NEODYMIUM due to overlapping victim and campaign characteristics. PROMETHIUM is reportedly associated closely with BlackOasis operations, but evidence that the group names are aliases has not been identified.

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

OilRig is a suspected Iranian threat group

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

- 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 <code>net user</code> , <code>net user /domain</code> , <code>net group "domain admins" /domain</code> , and <code>net group "Exchange Trusted Subsystem" /domain</code> 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

Associated Groups



Name	Associated Groups
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 <code>net user</code> , <code>net user /domain</code> , <code>net group "domain admins" /domain</code> , and <code>net group "Exchange Trusted Subsystem" /domain</code> 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, Timestamp, 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, Timestamp, Web Shell
S0096	Systeminfo	[6]	System Information Discovery
S0057	Tasklist	[3] [6]	Process Discovery, Security Software Discovery, System Service Discovery

References

- Falcone, R. (2017, October 9). OilRig Group Steps Up Attacks with New New Injector Trojan. Retrieved January 8, 2018.
- ClearSky Cybersec (2017, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to ... Retrieved January 8, 2018.
- Falcone, R. and Lee, B. (2018, November 16). Analyzing OilRig's Ops Tempo from Testing ... Retrieved April 23, 2019.
- Grunzweig, J. and ... (2017, December 15). Unit 42 Playbook Viewer. Retrieved December 20, 2017.
- Unit 42. (2017, December 15). Unit 42 Playbook Viewer. Retrieved December 20, 2017.
- 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.
- Lee, B., Falcone, R. (2018, January 25). OilRig uses RGDoor IIS Backdoor on Targets in the Middle East. Retrieved July 6, 2018.
- Davis, S. and Caban, D. (2017, December 19). APT34 - New Targeted Attack in the Middle East. Retrieved December 20, 2017.
- Lee, B., Falcone, R. (2018, February 23). Oops! OilRig Uses ThreeDollars to Deliver New Trojan. Retrieved July 16, 2018.
- November: HELIX KITTEN. Retrieved December 18, 2018.
- Singh, S., Yin, H. (2016, May 22). https://www.fireeye.com/blog/threat-research/2016/05/targeted_attacksaga.html. Retrieved April 5, 2018.
- Falcone, R. (2018, September 12). OilRig Uses Updated BONDUPDATER to Target Middle Eastern Government. Retrieved February 18, 2019.

References

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	Applnit 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	Applnit 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

OilRig Indicators



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



Mallory Kraeusen

Today, 9:54 PM

Alice Bluebird ▾

↻ Reply all ▾

Sent item

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

Alice,

Long story but basically I need you to block/delete 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

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>

Subject: Re: O Big indicators

**“No hits...but what do we do now?
What are these techniques?”**

Mallory,
Okay, we didn't have any hits and the indicators are all blocked. But what do we do now? That doesn't seem like it will be any more effective. We can do something with the...
Alice
Network Defender Extraordinaire



How does Alice stop hoarding indicators and start detecting techniques?

T1057	Process Discovery	OilRig has run <code>tasklist</code> on a victim's machine. ^[3]
T1016	System Network Configuration Discovery	OilRig has run <code>ipconfig /all</code> on a victim. ^{[3][4]}
T1049	System Network Connections Discovery	OilRig has used <code>netstat -an</code> on a victim to get a listing of network connections. ^[3]
T1033	System Owner/User Discovery	OilRig has run <code>whoami</code> on a victim. ^{[3][4]}
T1007	System Service Discovery	OilRig has used <code>sc query</code> 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 with

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 ▾

UID

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	Defensive 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	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 Alternate 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	Hooking	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	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 File or Information	LLMNR/NB1-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		Obscured Files or Information							
		Screensaver		Plist Modification							
		Security Support Provider		Port Knocking							
		Service Registry Permissions Weakness		Process Doppelganging							
		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		SIP and Trust Provider Hijacking							
		Winlogon Helper DLL		Software Packing							
				Space after Filename							
				Template Injection							
				Timestamp							
				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?





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}
```

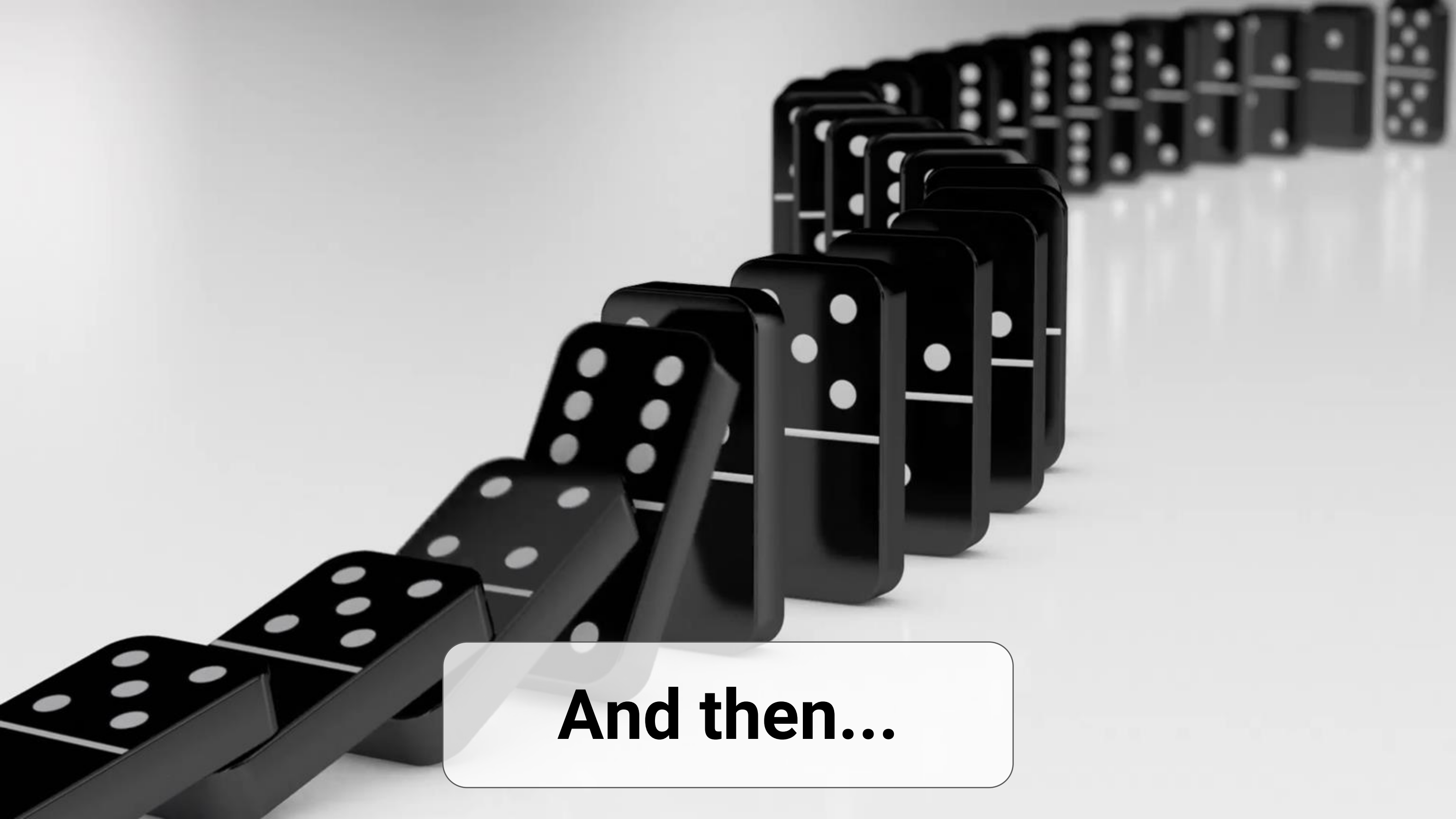
Time ↕	Urgency ↕	Security Domain ↕	Title ↕	Status ↕	Risk Score ↕	Action
8/4/19 10:22:52.000 PM	 Critical	Endpoint	Threat Activity Detected (Tasklist.exe)	New	0	▼
8/4/19 10:22:43.000 PM	 Critical	Endpoint	Threat Activity Detected (Tasklist.exe)	New	0	▼
8/4/19 10:22:32.000 PM	 Critical	Endpoint	Threat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

Attacks detected!

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





And then...



“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

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 Frothy back on track



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



Communicate confidence level

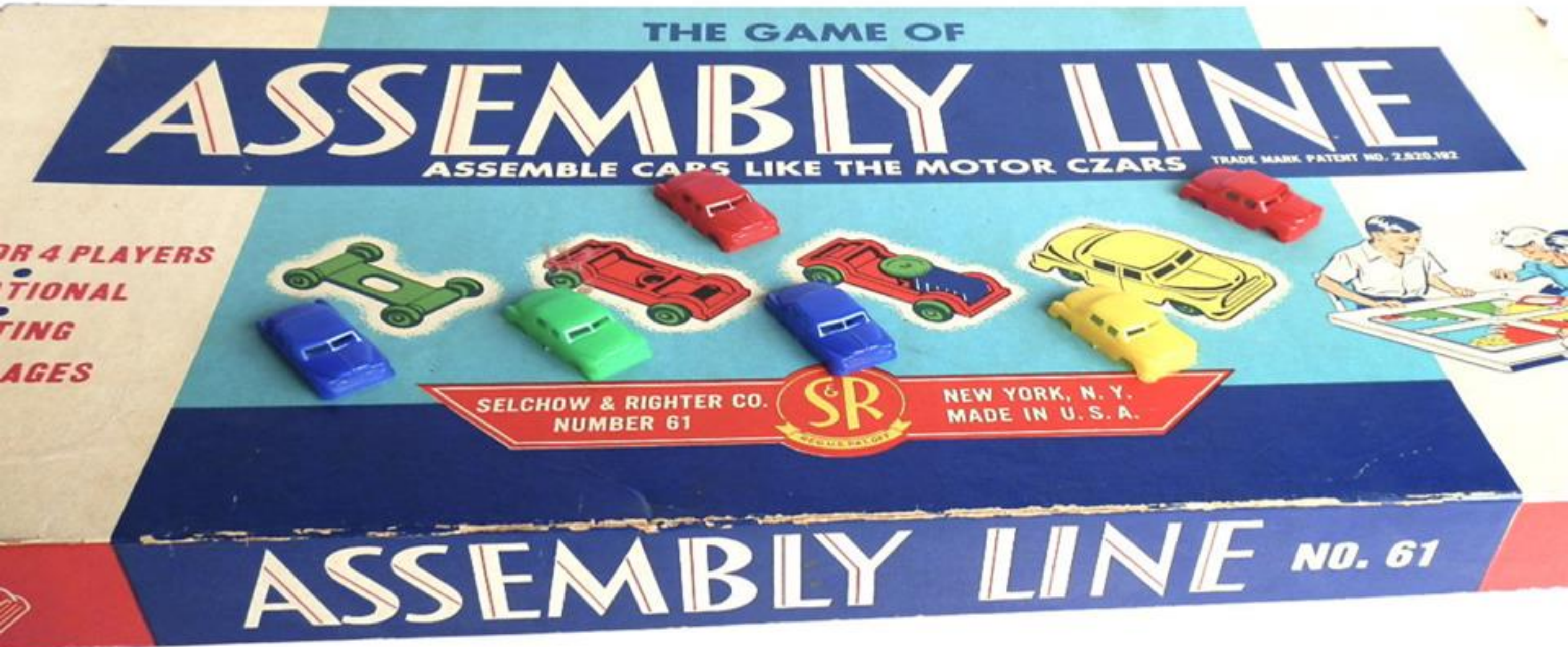
Initial Access 11 items	Execution 33 items	Persistence 59 items	Privilege Escalation 28 items	Defense Evasion 67 items	Credential Access 19 items	Discovery 22 items	Lateral Movement 17 items	Collection 13 items	Command And Control 23 items	Exfiltration 9 items	Impact 14 items
Drive-by Compromise	AppleScript	bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Export 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	Appnlt 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	Appnlt 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 Network Medium	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 Compromis	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/NB1-NS Poisoning 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 Evasion	Securityd Memory Interception	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 Layer 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		Obscured Files or Information							
		Screensaver		Plist Modification							
		Security Support Provider		Port Knocking							
		Service Registry Permissions Weakness		Process Doppelganging							
		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 Firewall Filter Hijacking		SIP and Trust Provider Hijacking							
		Winlogon Helper DLL		Software Packing							
				Space after Filename							
				Template Injection							
				Timestamp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

Color gradient by confidence in detections



h/t to Olaf Hartong

Integrate your teams





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 Registry	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 File and Directory Discovery	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 Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Domain Generation

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

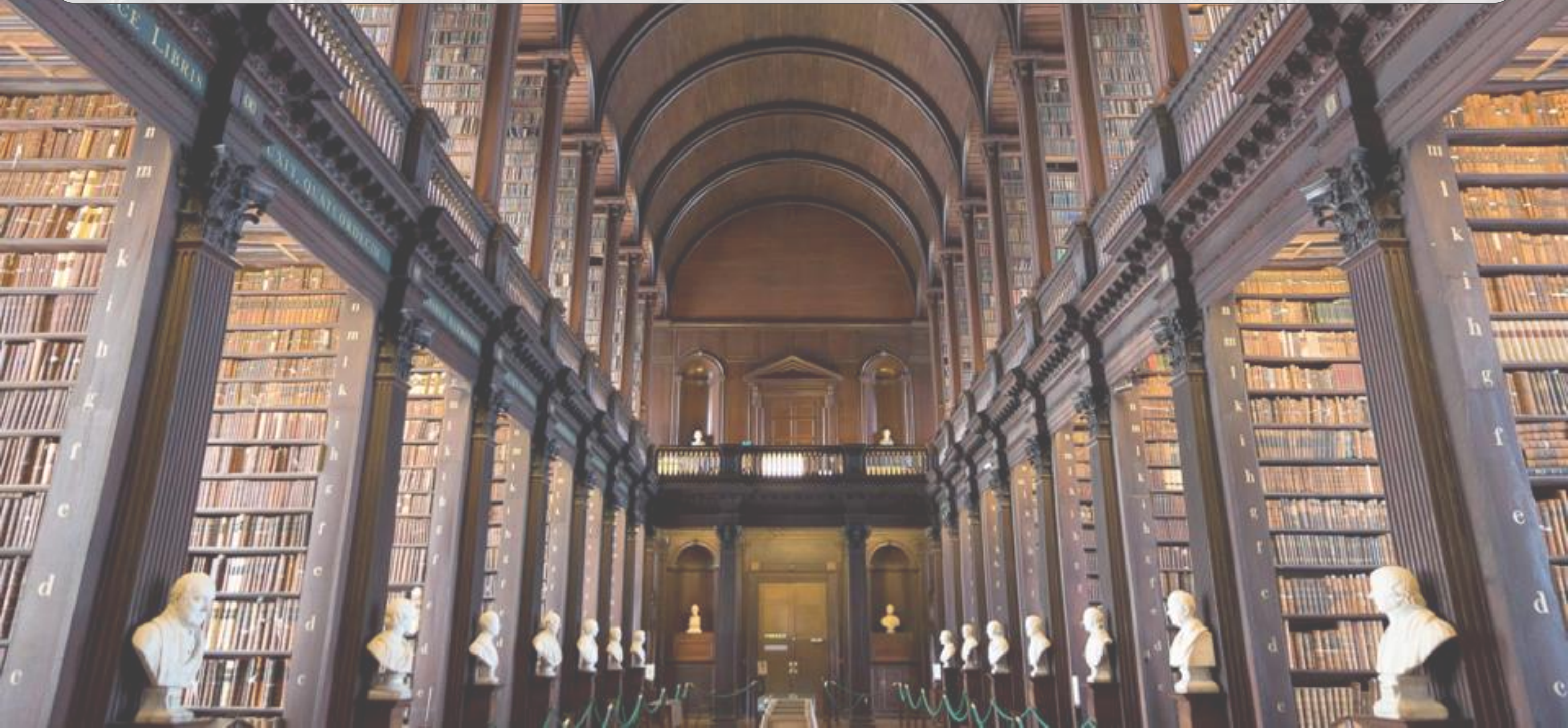
MITRE ATT&CK Matrix

Initial Access	Execution	Persistence	Privileged Actions	Escalation	Command-Line Interface	Account Manipulation	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Manipulation	Access Features	Command-Line Interface	Account Manipulation	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	AppCertificate	AppInit DLLs	Command-Line Interface	Account Manipulation	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
External Remote Services	Command-Line Interface	Account Manipulation	AppInit DLLs	AppInit DLLs	Command-Line Interface	Account Manipulation	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	AppInit DLLs	Command-Line Interface	Account Manipulation	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	AppInit DLLs	Command-Line Interface	Account Manipulation	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Application Shimming	Command-Line Interface	Account Manipulation	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing Link	Execution through API	Authentication Package	Authentication Package	Authentication Package	Command-Line Interface	Account Manipulation	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Spearphishing via Service	Execution through Module Load	BITS Jobs	BITS Jobs	BITS Jobs	Command-Line Interface	Account Manipulation	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Supply Chain Compromise	Exploitation for Client	Bootkit	Exploitation for Client	Exploitation for Client	Command-Line Interface	Account Manipulation	Remote File Copy	Email Collection	Scheduled Transfer	Domain Generation

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	<p>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.</p>

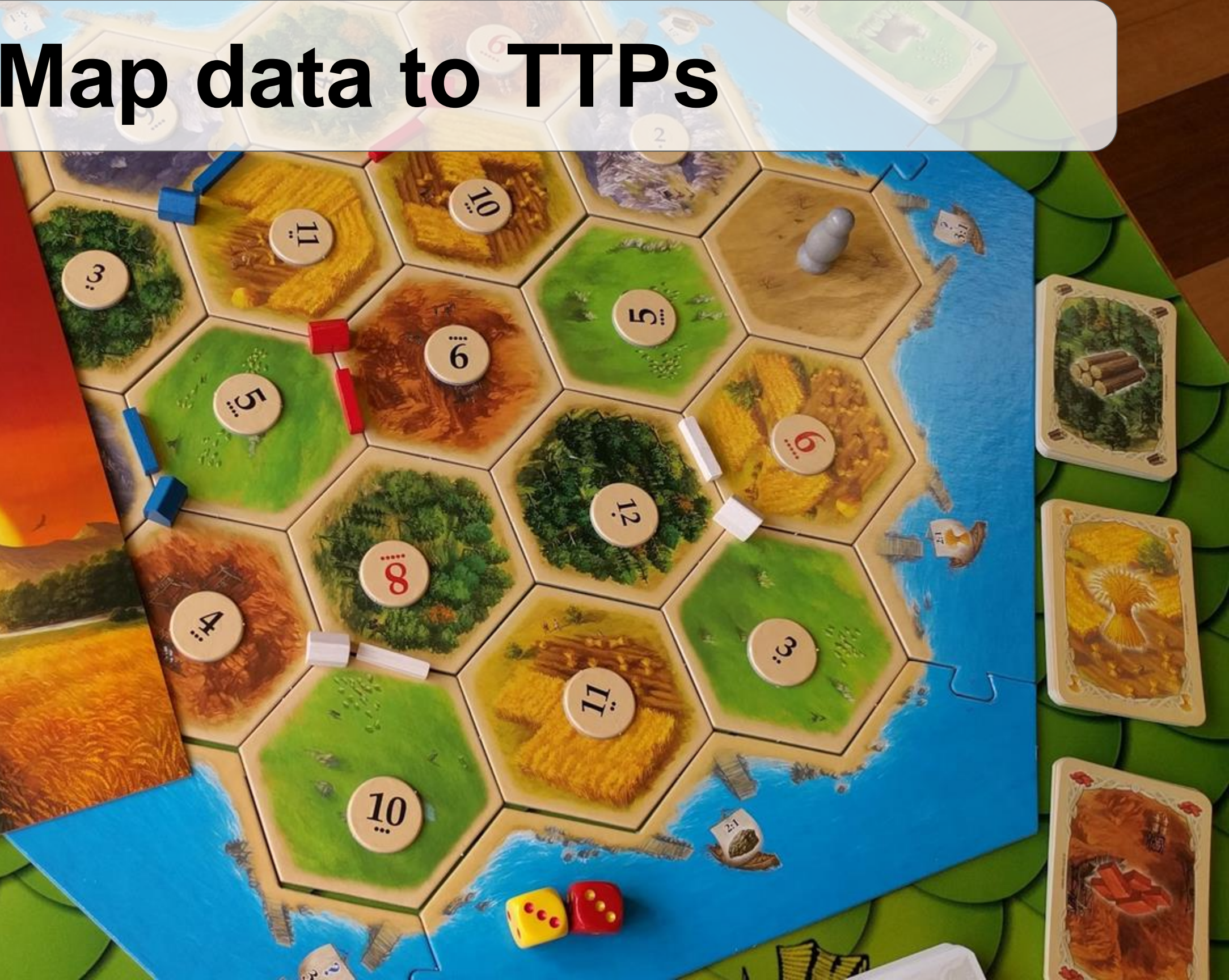
Campaign	Techniques	Tactics	Description
DNSpionage Upgraded Their Tool into Karkoff	DTTT0008 - Environment Awareness*	Defense Evasion	Karkoff uses the information collected from the local system in order to fingerprint the victims and avoid researchers or sandboxes.
DNSpionage Upgraded Their Tool into 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

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 with

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

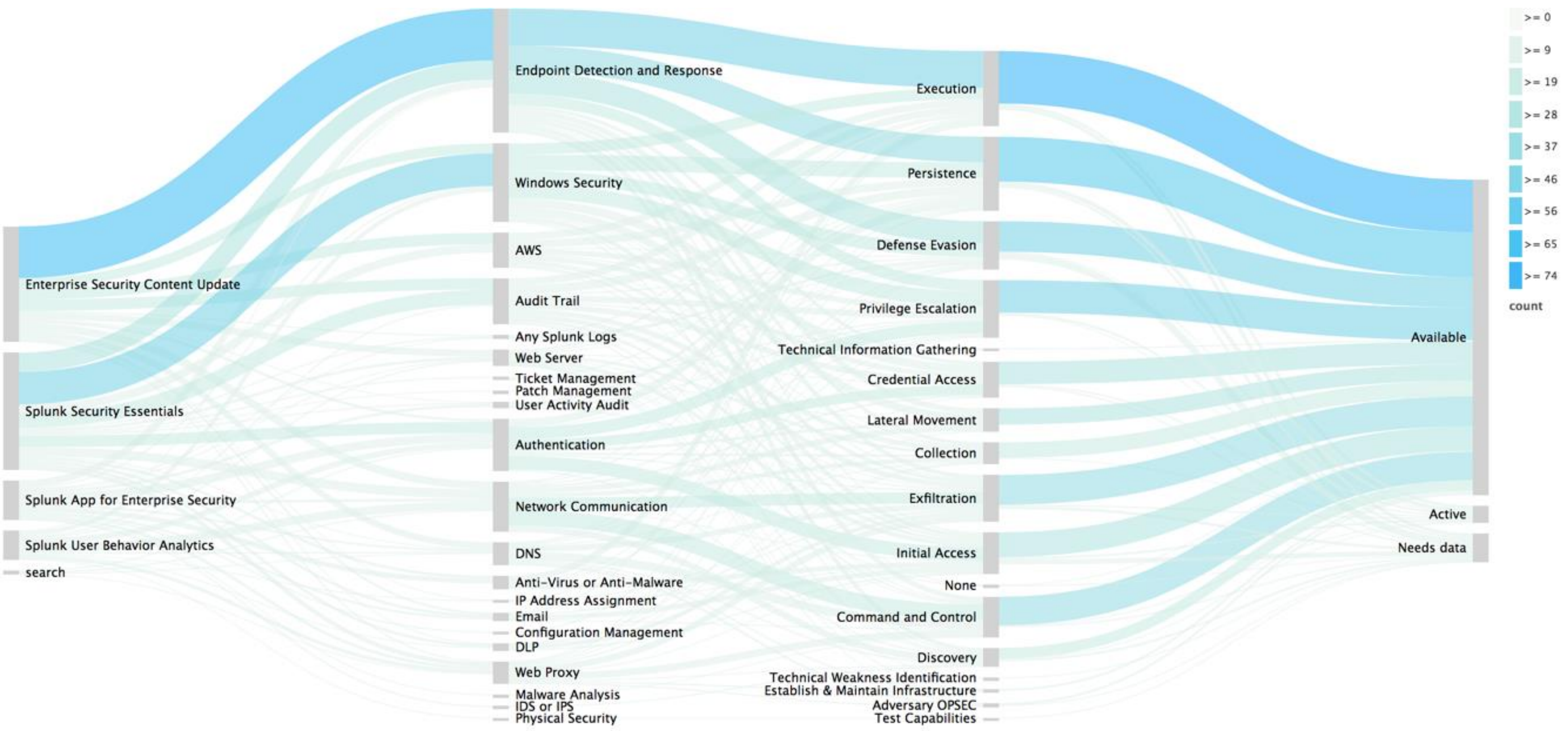
Version: 1.0

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 <code>python3 techniques_from_data_source.py -h</code> 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 <code>python3 techniques_data_sources_vis.py -h</code> for usage instructions.

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



One Sig!=Complete TTP Coverage



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.

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>.*)\\" | `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 ▼



Reduced Alerts

Incident Review

Urgency

CRITICAL	0
HIGH	0
MEDIUM	1
LOW	0
INFO	0

Status

All ×

Owner

All ×

Security Domain

All ×

Tag

Select...

Correlation Search Name

Select...

Search

Time Associations

Last 24 hours

Submit

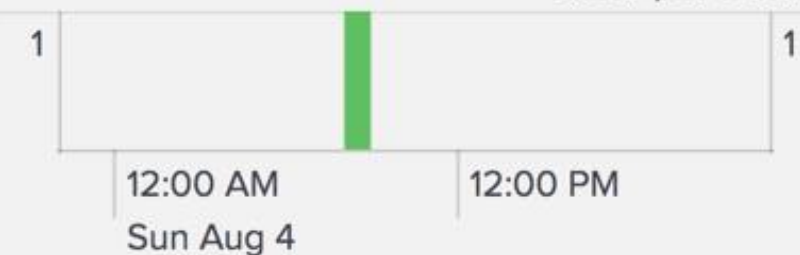
✓ 1 event (8/3/19 10:00:00.000 PM to 8/4/19 10:37:29.000 PM)

Job ▾ || ■ Smart Mode ▾

Format Timeline ▾ – Zoom Out

+ Zoom to Selection × Deselect

1 hour per column



i	<input type="checkbox"/>	Time ⇅	Security Domain ⇅	Title ⇅	Urgency ⇅	Status ⇅	Owner ⇅	Actions
>	<input type="checkbox"/>	8/4/19 8:05:47.000 AM	Access	Brute Force Access Behavior Detected From 10.255.3.2	⚠ Medium	New	unassigned	▾

**How can a red
teamer help improve
defenses?**

Small and highly portable detection tests based on MITRE's ATT&CK.

mitre mitre-attack

1,241 commits 10 branches 0 releases 44 contributors MIT

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

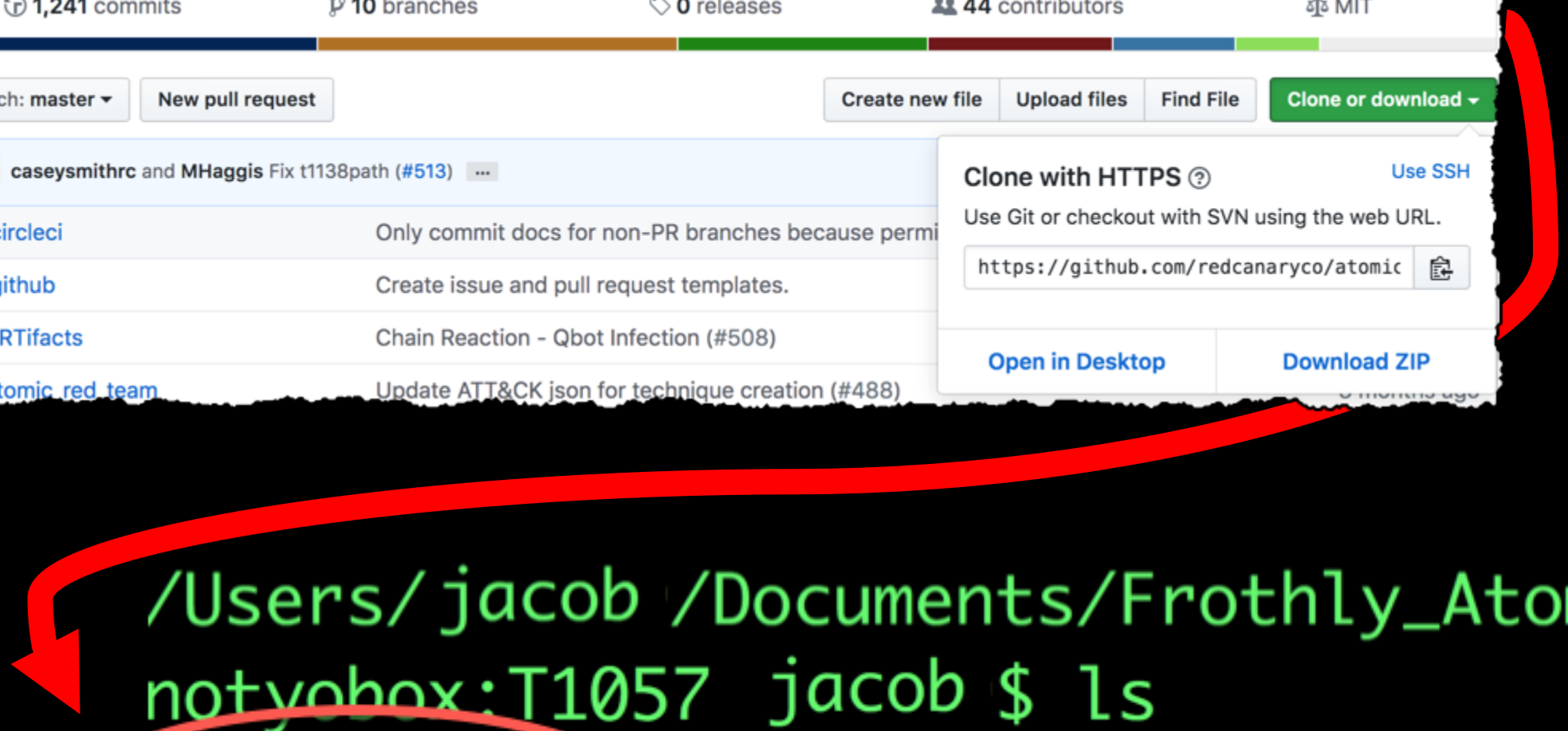
- caseysmithrc and MHaggis Fix t1138path (#513)
- .circleci Only commit docs for non-PR branches because perm...
- .github Create issue and pull request templates.
- ARTifacts Chain Reaction - Qbot Infection (#508)
- atomic_red_team Update ATT&CK json for technique creation (#488)

Clone with HTTPS Use SSH

Use Git or checkout with SVN using the web URL.

https://github.com/redcanaryco/atomic

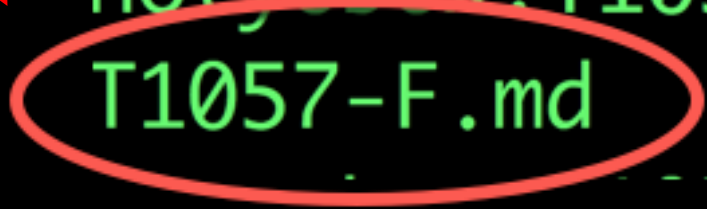
Open in Desktop Download ZIP



```

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

```

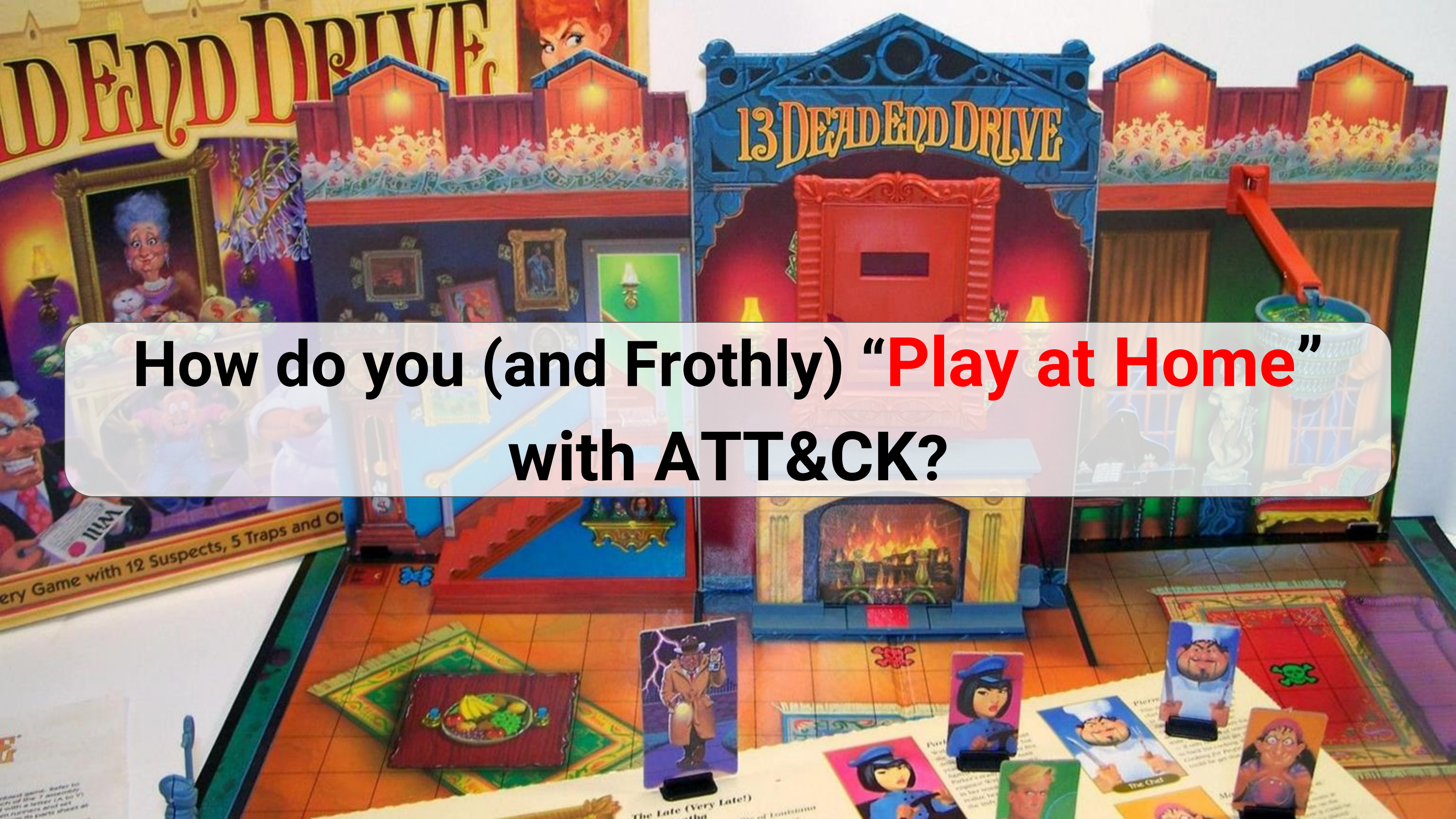


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Command And	Exfiltration	Impact	
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	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	Damage 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	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/NB1-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 Execution							
		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 Doppelganging							
		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		SIP and Trust Provider Hijacking							
		Winlogon Helper DLL		Software Packing							
				Space after Filename							
				Template Injection							
				Timestamp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

Go purple!

What blue detected

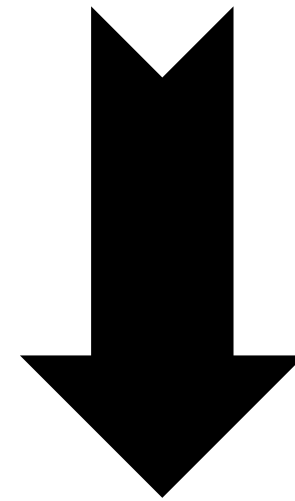
What red did that blue missed



How do you (and Frothly) **“Play at Home”**
with ATT&CK?



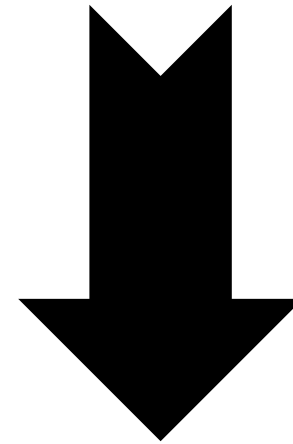
“How are we defended?”



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



“If it’s not an IP,
how do I use it?”

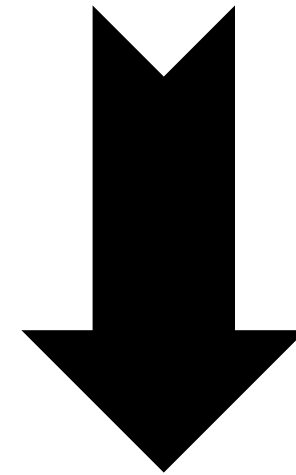


“I’m tracking **multiple** threats
and I’m a
Pyramid of Pain master.”



Defense

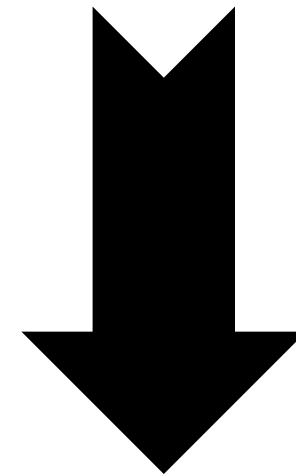
“I’m drowning in alerts
and missing data!”



“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!

**♟ 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**

♟ Women's Society of Cyberjutsu

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-attack-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>

Thank you!

Katie Nickels

MITRE

 @LiketheCoins

Ryan Kovar

Splunk

 @meansec