

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.

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.

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



A painting depicting a factory or industrial setting. In the foreground, several workers are engaged in manual labor; one uses a long pole to move a large, dark, cylindrical object, while others assist. The background features tall, red cylindrical tanks, pipes, and a complex network of scaffolding and ladders. The lighting is dramatic, with strong highlights and deep shadows, creating a sense of industrial power and movement.

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 | ▾

Inbox

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

What the heck is going on over there? I turned on HOPSNIV 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. I am not sure if we are prepared. I am not sure what 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.
PRONTO		PRONTO is a threat group that has been active since at least 2010. The group has been involved in several high-profile incidents, including the 2014 hack of the U.S. Office of Personnel Management.

Groups

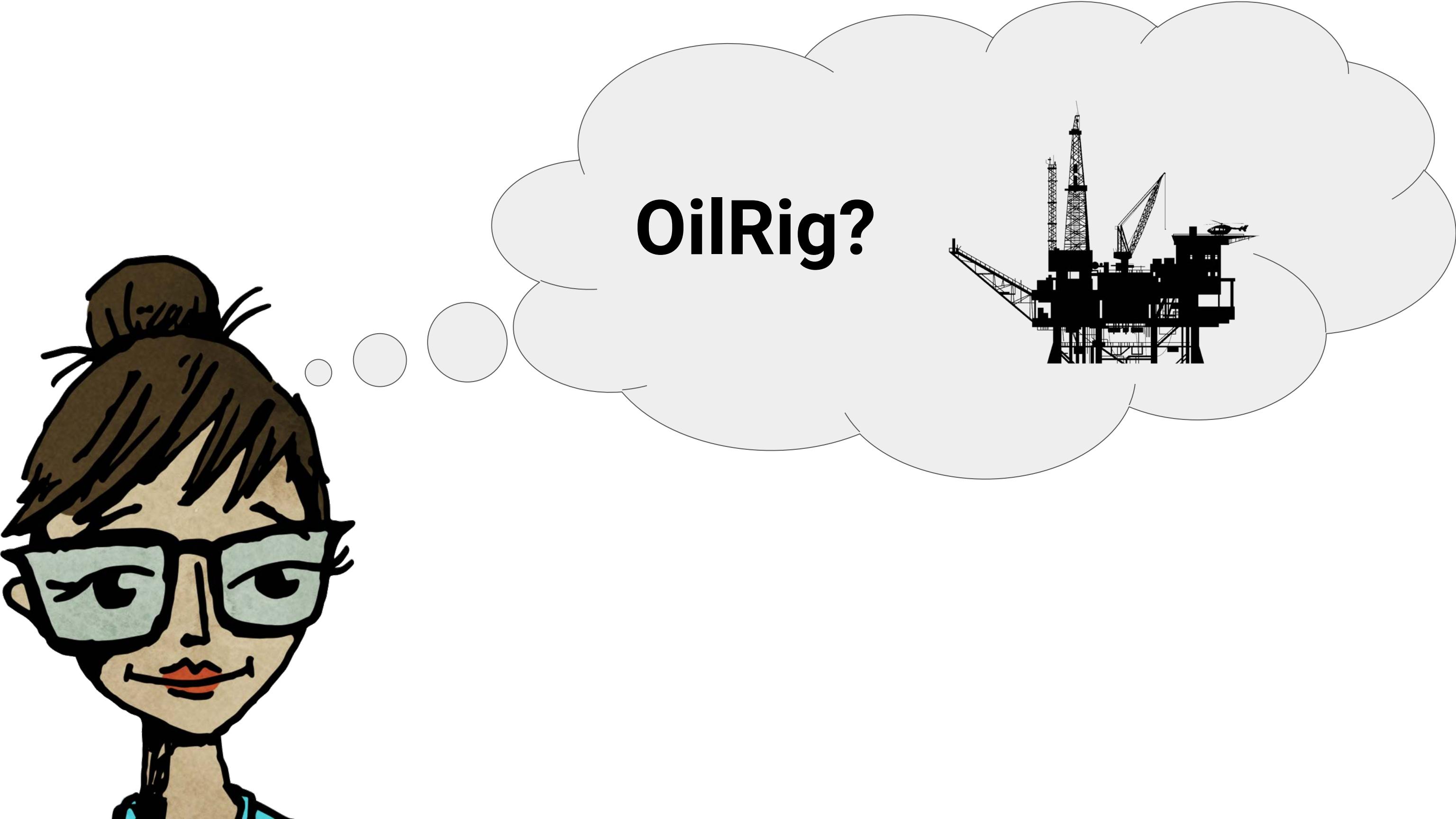
NEODYMIUM		NEODYMIUM is an activity group that conducted a campaign in May 2016 and has heavily targeted Turkish victims. The group has demonstrated similarity to another activity group called PROMETHIUM due to overlapping victim and campaign characteristics. NEODYMIUM is reportedly associated closely 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
the activity.

OilRig is a suspected [Iranian](#) threat group

at 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.



A cartoon illustration of a person with brown hair and glasses, looking thoughtful with a slight smile. A thought bubble originates from their head, containing the text "OilRig?". From the end of the thought bubble, a line extends to a detailed black silhouette of an offshore oil rig. The oil rig features a helipad with a helicopter, multiple levels of platforms, and a tall derrick tower. The background consists of several light gray, rounded shapes resembling clouds or thought bubbles.

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

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

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

Ass

Techniques Used

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, 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

1. Falcone, R.. (2017, December 20). OilRig Targets Technology Service Providers and Government Agencies. Retrieved December 20, 2017.
2. ClearSky Cybersecurity. (2017, October 9). OilRig Group Steps Up Attacks with New Variant M-Trends 2018. Retrieved July 9, 2018.
3. 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.
4. Lee, B., Falcone, R. (2018, July 25). OilRig Targets Technology Service Provider and Government Agency with QUADAGENT. Retrieved August 9, 2018.
5. Davis, S. and Caban, D. (2017, December 19). APT34 - New Targeted Attack in the Middle East. Retrieved December 20, 2017.
6. Falcone, R. (2018, January 25). OilRig uses RGDoor IIS Backdoor on Targets in the Middle East. Retrieved July 6, 2018.
7. Wilhoit, K. and Falcone, R. (2018, September 12). OilRig Uses Updated BONDUPDATER to Target Middle Eastern Government. Retrieved February 18, 2019.
8. Falcone, R. (2017, November 16). Analyzing OilRig's Ops Tempo from Testing Efforts. Retrieved November 16, 2017.
9. Falcone, R. (2018, February 23). OopsIE! OilRig Uses ThreeDollars to Deliver New Trojan. Retrieved July 16, 2018.
10. Falcone, R. (2018, April 27). Meet CrowdStrike's Adversary of the Month for April 2018. Retrieved April 27, 2018.
11. Falcone, R. (2018, May 22). OilRig Targets Middle Eastern Government. Retrieved May 22, 2018.
12. Falcone, R. (2018, June 12). OilRig Targets Middle Eastern Government. Retrieved June 12, 2018.
13. Falcone, R. (2018, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to New Injector Trojan. Retrieved January 8, 2018.
14. Falcone, R. (2018, November 16). Analyzing OilRig's Ops Tempo from Testing Efforts. Retrieved November 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. Falcone, R. (2018, February 23). OopsIE! OilRig Uses ThreeDollars to Deliver New Trojan. Retrieved February 23, 2018.
18. Falcone, R. (2018, March 27). Meet CrowdStrike's Adversary of the Month for March 2018. Retrieved March 27, 2018.
19. Falcone, R. (2018, April 27). Meet CrowdStrike's Adversary of the Month for April 2018. Retrieved April 27, 2018.
20. Falcone, R. (2018, May 22). OilRig Targets Middle Eastern Government. Retrieved May 22, 2018.
21. Falcone, R. (2018, June 12). OilRig Targets Middle Eastern Government. Retrieved June 12, 2018.
22. Falcone, R. (2018, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to New Injector Trojan. Retrieved January 8, 2018.
23. Falcone, R. (2018, November 16). Analyzing OilRig's Ops Tempo from Testing Efforts. Retrieved November 16, 2018.
24. Falcone, R. (2018, December 12). OilRig Targets Middle Eastern Government. Retrieved December 12, 2018.
25. Falcone, R. (2019, January 25). OilRig Targets Middle Eastern Government. Retrieved January 25, 2019.
26. Falcone, R. (2019, February 23). OilRig Targets Middle Eastern Government. Retrieved February 23, 2019.
27. Falcone, R. (2019, March 27). Meet CrowdStrike's Adversary of the Month for March 2019. Retrieved March 27, 2019.
28. Falcone, R. (2019, April 27). Meet CrowdStrike's Adversary of the Month for April 2019. Retrieved April 27, 2019.
29. Falcone, R. (2019, May 22). OilRig Targets Middle Eastern Government. Retrieved May 22, 2019.
30. Falcone, R. (2019, June 12). OilRig Targets Middle Eastern Government. Retrieved June 12, 2019.
31. Falcone, R. (2019, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to New Injector Trojan. Retrieved January 8, 2019.
32. Falcone, R. (2019, November 16). Analyzing OilRig's Ops Tempo from Testing Efforts. Retrieved November 16, 2019.
33. Falcone, R. (2019, December 12). OilRig Targets Middle Eastern Government. Retrieved December 12, 2019.
34. Falcone, R. (2020, January 25). OilRig Targets Middle Eastern Government. Retrieved January 25, 2020.
35. Falcone, R. (2020, February 23). OilRig Targets Middle Eastern Government. Retrieved February 23, 2020.
36. Falcone, R. (2020, March 27). Meet CrowdStrike's Adversary of the Month for March 2020. Retrieved March 27, 2020.
37. Falcone, R. (2020, April 27). Meet CrowdStrike's Adversary of the Month for April 2020. Retrieved April 27, 2020.
38. Falcone, R. (2020, May 22). OilRig Targets Middle Eastern Government. Retrieved May 22, 2020.
39. Falcone, R. (2020, June 12). OilRig Targets Middle Eastern Government. Retrieved June 12, 2020.
40. Falcone, R. (2020, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to New Injector Trojan. Retrieved January 8, 2020.
41. Falcone, R. (2020, November 16). Analyzing OilRig's Ops Tempo from Testing Efforts. Retrieved November 16, 2020.
42. Falcone, R. (2020, December 12). OilRig Targets Middle Eastern Government. Retrieved December 12, 2020.
43. Falcone, R. (2021, January 25). OilRig Targets Middle Eastern Government. Retrieved January 25, 2021.
44. Falcone, R. (2021, February 23). OilRig Targets Middle Eastern Government. Retrieved February 23, 2021.
45. Falcone, R. (2021, March 27). Meet CrowdStrike's Adversary of the Month for March 2021. Retrieved March 27, 2021.
46. Falcone, R. (2021, April 27). Meet CrowdStrike's Adversary of the Month for April 2021. Retrieved April 27, 2021.
47. Falcone, R. (2021, May 22). OilRig Targets Middle Eastern Government. Retrieved May 22, 2021.
48. Falcone, R. (2021, June 12). OilRig Targets Middle Eastern Government. Retrieved June 12, 2021.
49. Falcone, R. (2021, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to New Injector Trojan. Retrieved January 8, 2021.
50. Falcone, R. (2021, November 16). Analyzing OilRig's Ops Tempo from Testing Efforts. Retrieved November 16, 2021.
51. Falcone, R. (2021, December 12). OilRig Targets Middle Eastern Government. Retrieved December 12, 2021.
52. Falcone, R. (2022, January 25). OilRig Targets Middle Eastern Government. Retrieved January 25, 2022.
53. Falcone, R. (2022, February 23). OilRig Targets Middle Eastern Government. Retrieved February 23, 2022.
54. Falcone, R. (2022, March 27). Meet CrowdStrike's Adversary of the Month for March 2022. Retrieved March 27, 2022.
55. Falcone, R. (2022, April 27). Meet CrowdStrike's Adversary of the Month for April 2022. Retrieved April 27, 2022.
56. Falcone, R. (2022, May 22). OilRig Targets Middle Eastern Government. Retrieved May 22, 2022.
57. Falcone, R. (2022, June 12). OilRig Targets Middle Eastern Government. Retrieved June 12, 2022.
58. Falcone, R. (2022, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to New Injector Trojan. Retrieved January 8, 2022.
59. Falcone, R. (2022, November 16). Analyzing OilRig's Ops Tempo from Testing Efforts. Retrieved November 16, 2022.
60. Falcone, R. (2022, December 12). OilRig Targets Middle Eastern Government. Retrieved December 12, 2022.
61. Falcone, R. (2023, January 25). OilRig Targets Middle Eastern Government. Retrieved January 25, 2023.
62. Falcone, R. (2023, February 23). OilRig Targets Middle Eastern Government. Retrieved February 23, 2023.
63. Falcone, R. (2023, March 27). Meet CrowdStrike's Adversary of the Month for March 2023. Retrieved March 27, 2023.
64. Falcone, R. (2023, April 27). Meet CrowdStrike's Adversary of the Month for April 2023. Retrieved April 27, 2023.
65. Falcone, R. (2023, May 22). OilRig Targets Middle Eastern Government. Retrieved May 22, 2023.
66. Falcone, R. (2023, June 12). OilRig Targets Middle Eastern Government. Retrieved June 12, 2023.
67. Falcone, R. (2023, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to New Injector Trojan. Retrieved January 8, 2023.
68. Falcone, R. (2023, November 16). Analyzing OilRig's Ops Tempo from Testing Efforts. Retrieved November 16, 2023.
69. Falcone, R. (2023, December 12). OilRig Targets Middle Eastern Government. Retrieved December 12, 2023.
70. Falcone, R. (2024, January 25). OilRig Targets Middle Eastern Government. Retrieved January 25, 2024.
71. Falcone, R. (2024, February 23). OilRig Targets Middle Eastern Government. Retrieved February 23, 2024.
72. Falcone, R. (2024, March 27). Meet CrowdStrike's Adversary of the Month for March 2024. Retrieved March 27, 2024.
73. Falcone, R. (2024, April 27). Meet CrowdStrike's Adversary of the Month for April 2024. Retrieved April 27, 2024.
74. Falcone, R. (2024, May 22). OilRig Targets Middle Eastern Government. Retrieved May 22, 2024.
75. Falcone, R. (2024, June 12). OilRig Targets Middle Eastern Government. Retrieved June 12, 2024.
76. Falcone, R. (2024, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to New Injector Trojan. Retrieved January 8, 2024.
77. Falcone, R. (2024, November 16). Analyzing OilRig's Ops Tempo from Testing Efforts. Retrieved November 16, 2024.
78. Falcone, R. (2024, December 12). OilRig Targets Middle Eastern Government. Retrieved December 12, 2024.
79. Falcone, R. (2025, January 25). OilRig Targets Middle Eastern Government. Retrieved January 25, 2025.
80. Falcone, R. (2025, February 23). OilRig Targets Middle Eastern Government. Retrieved February 23, 2025.
81. Falcone, R. (2025, March 27). Meet CrowdStrike's Adversary of the Month for March 2025. Retrieved March 27, 2025.
82. Falcone, R. (2025, April 27). Meet CrowdStrike's Adversary of the Month for April 2025. Retrieved April 27, 2025.
83. Falcone, R. (2025, May 22). OilRig Targets Middle Eastern Government. Retrieved May 22, 2025.
84. Falcone, R. (2025, June 12). OilRig Targets Middle Eastern Government. Retrieved June 12, 2025.
85. Falcone, R. (2025, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to New Injector Trojan. Retrieved January 8, 2025.
86. Falcone, R. (2025, November 16). Analyzing OilRig's Ops Tempo from Testing Efforts. Retrieved November 16, 2025.
87. Falcone, R. (2025, December 12). OilRig Targets Middle Eastern Government. Retrieved December 12, 2025.
88. Falcone, R. (2026, January 25). OilRig Targets Middle Eastern Government. Retrieved January 25, 2026.
89. Falcone, R. (2026, February 23). OilRig Targets Middle Eastern Government. Retrieved February 23, 2026.
90. Falcone, R. (2026, March 27). Meet CrowdStrike's Adversary of the Month for March 2026. Retrieved March 27, 2026.
91. Falcone, R. (2026, April 27). Meet CrowdStrike's Adversary of the Month for April 2026. Retrieved April 27, 2026.
92. Falcone, R. (2026, May 22). OilRig Targets Middle Eastern Government. Retrieved May 22, 2026.
93. Falcone, R. (2026, June 12). OilRig Targets Middle Eastern Government. Retrieved June 12, 2026.
94. Falcone, R. (2026, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to New Injector Trojan. Retrieved January 8, 2026.
95. Falcone, R. (2026, November 16). Analyzing OilRig's Ops Tempo from Testing Efforts. Retrieved November 16, 2026.
96. Falcone, R. (2026, December 12). OilRig Targets Middle Eastern Government. Retrieved December 12, 2026.
97. Falcone, R. (2027, January 25). OilRig Targets Middle Eastern Government. Retrieved January 25, 2027.
98. Falcone, R. (2027, February 23). OilRig Targets Middle Eastern Government. Retrieved February 23, 2027.
99. Falcone, R. (2027, March 27). Meet CrowdStrike's Adversary of the Month for March 2027. Retrieved March 27, 2027.
100. Falcone, R. (2027, April 27). Meet CrowdStrike's Adversary of the Month for April 2027. Retrieved April 27, 2027.
101. Falcone, R. (2027, May 22). OilRig Targets Middle Eastern Government. Retrieved May 22, 2027.
102. Falcone, R. (2027, June 12). OilRig Targets Middle Eastern Government. Retrieved June 12, 2027.
103. Falcone, R. (2027, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to New Injector Trojan. Retrieved January 8, 2027.
104. Falcone, R. (2027, November 16). Analyzing OilRig's Ops Tempo from Testing Efforts. Retrieved November 16, 2027.
105. Falcone, R. (2027, December 12). OilRig Targets Middle Eastern Government. Retrieved December 12, 2027.
106. Falcone, R. (2028, January 25). OilRig Targets Middle Eastern Government. Retrieved January 25, 2028.
107. Falcone, R. (2028, February 23). OilRig Targets Middle Eastern Government. Retrieved February 23, 2028.
108. Falcone, R. (2028, March 27). Meet CrowdStrike's Adversary of the Month for March 2028. Retrieved March 27, 2028.
109. Falcone, R. (2028, April 27). Meet CrowdStrike's Adversary of the Month for April 2028. Retrieved April 27, 2028.
110. Falcone, R. (2028, May 22). OilRig Targets Middle Eastern Government. Retrieved May 22, 2028.
111. Falcone, R. (2028, June 12). OilRig Targets Middle Eastern Government. Retrieved June 12, 2028.
112. Falcone, R. (2028, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to New Injector Trojan. Retrieved January 8, 2028.
113. Falcone, R. (2028, November 16). Analyzing OilRig's Ops Tempo from Testing Efforts. Retrieved November 16, 2028.
114. Falcone, R. (2028, December 12). OilRig Targets Middle Eastern Government. Retrieved December 12, 2028.
115. Falcone, R. (2029, January 25). OilRig Targets Middle Eastern Government. Retrieved January 25, 2029.
116. Falcone, R. (2029, February 23). OilRig Targets Middle Eastern Government. Retrieved February 23, 2029.
117. Falcone, R. (2029, March 27). Meet CrowdStrike's Adversary of the Month for March 2029. Retrieved March 27, 2029.
118. Falcone, R. (2029, April 27). Meet CrowdStrike's Adversary of the Month for April 2029. Retrieved April 27, 2029.
119. Falcone, R. (2029, May 22). OilRig Targets Middle Eastern Government. Retrieved May 22, 2029.
120. Falcone, R. (2029, June 12). OilRig Targets Middle Eastern Government. Retrieved June 12, 2029.
121. Falcone, R. (2029, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to New Injector Trojan. Retrieved January 8, 2029.
122. Falcone, R. (2029, November 16). Analyzing OilRig's Ops Tempo from Testing Efforts. Retrieved November 16, 2029.
123. Falcone, R. (2029, December 12). OilRig Targets Middle Eastern Government. Retrieved December 12, 2029.
124. Falcone, R. (2030, January 25). OilRig Targets Middle Eastern Government. Retrieved January 25, 2030.
125. Falcone, R. (2030, February 23). OilRig Targets Middle Eastern Government. Retrieved February 23, 2030.
126. Falcone, R. (2030, March 27). Meet CrowdStrike's Adversary of the Month for March 2030. Retrieved March 27, 2030.
127. Falcone, R. (2030, April 27). Meet CrowdStrike's Adversary of the Month for April 2030. Retrieved April 27, 2030.
128. Falcone, R. (2030, May 22). OilRig Targets Middle Eastern Government. Retrieved May 22, 2030.
129. Falcone, R. (2030, June 12). OilRig Targets Middle Eastern Government. Retrieved June 12, 2030.
130. Falcone, R. (2030, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to New Injector Trojan. Retrieved January 8, 2030.
131. Falcone, R. (2030, November 16). Analyzing OilRig's Ops Tempo from Testing Efforts. Retrieved November 16, 2030.
132. Falcone, R. (2030, December 12). OilRig Targets Middle Eastern Government. Retrieved December 12, 2030.
133. Falcone, R. (2031, January 25). OilRig Targets Middle Eastern Government. Retrieved January 25, 2031.
134. Falcone, R. (2031, February 23). OilRig Targets Middle Eastern Government. Retrieved February 23, 2031.
135. Falcone, R. (2031, March 27). Meet CrowdStrike's Adversary of the Month for March 2031. Retrieved March 27, 2031.
136. Falcone, R. (2031, April 27). Meet CrowdStrike's Adversary of the Month for April 2031. Retrieved April 27, 2031.
137. Falcone, R. (2031, May 22). OilRig Targets Middle Eastern Government. Retrieved May 22, 2031.
138. Falcone, R. (2031, June 12). OilRig Targets Middle Eastern Government. Retrieved June 12, 2031.
139. Falcone, R. (2031, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to New Injector Trojan. Retrieved January 8, 2031.
140. Falcone, R. (2031, November 16). Analyzing OilRig's Ops Tempo from Testing Efforts. Retrieved November 16, 2031.
141. Falcone, R. (2031, December 12). OilRig Targets Middle Eastern Government. Retrieved December 12, 2031.
142. Falcone, R. (2032, January 25). OilRig Targets Middle Eastern Government. Retrieved January 25, 2032.
143. Falcone, R. (2032, February 23). OilRig Targets Middle Eastern Government. Retrieved February 23, 2032.
144. Falcone, R. (2032, March 27). Meet CrowdStrike's Adversary of the Month for March 2032. Retrieved March 27, 2032.
145. Falcone, R. (2032, April 27). Meet CrowdStrike's Adversary of the Month for April 2032. Retrieved April 27, 2032.
146. Falcone, R. (2032, May 22). OilRig Targets Middle Eastern Government. Retrieved May 22, 2032.
147. Falcone, R. (2032, June 12). OilRig Targets Middle Eastern Government. Retrieved June 12, 2032.
148. Falcone, R. (2032, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to New Injector Trojan. Retrieved January 8, 2032.
149. Falcone, R. (2032, November 16). Analyzing OilRig's Ops Tempo from Testing Efforts. Retrieved November 16, 2032.
150. Falcone, R. (2032, December 12). OilRig Targets Middle Eastern Government. Retrieved December 12, 2032.
151. Falcone, R. (2033, January 25). OilRig Targets Middle Eastern Government. Retrieved January 25, 2033.
152. Falcone, R. (2033, February 23). OilRig Targets Middle Eastern Government. Retrieved February 23, 2033.
153. Falcone, R. (2033, March 27). Meet CrowdStrike's Adversary of the Month for March 2033. Retrieved March 27, 2033.
154. Falcone, R. (2033, April 27). Meet CrowdStrike's Adversary of the Month for April 2033. Retrieved April 27, 2033.
155. Falcone, R. (2033, May 22). OilRig Targets Middle Eastern Government. Retrieved May 22, 2033.
156. Falcone, R. (2033, June 12). OilRig Targets Middle Eastern Government. Retrieved June 12, 2033.
157. Falcone, R. (2033, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to New Injector Trojan. Retrieved January 8, 2033.
158. Falcone, R. (2033, November 16). Analyzing OilRig's Ops Tempo from Testing Efforts. Retrieved November 16, 2033.
159. Falcone, R. (2033, December 12). OilRig Targets Middle Eastern Government. Retrieved December 12, 2033.
160. Falcone, R. (2034, January 25). OilRig Targets Middle Eastern Government. Retrieved January 25, 2034.
161. Falcone, R. (2034, February 23). OilRig Targets Middle Eastern Government. Retrieved February 23, 2034.
162. Falcone, R. (2034, March 27). Meet CrowdStrike's Adversary of the Month for March 2034. Retrieved March 27, 2034.
163. Falcone, R. (2034, April 27). Meet CrowdStrike's Adversary of the Month for April 2034. Retrieved April 27, 2034.
164. Falcone, R. (2034, May 22). OilRig Targets Middle Eastern Government. Retrieved May 22, 2034.
165. Falcone, R. (2034, June 12). OilRig Targets Middle Eastern Government. Retrieved June 12, 2034.
166. Falcone, R. (2034, July 27). OilRig Uses ISMDoor Variant; Possibly Linked to New Injector Trojan. Retrieved January 8, 2034.
167. Falcone, R. (2034, November 16). Analyzing OilRig's Ops Tempo from Testing Efforts. Retrieved November 16, 2034.
168. Falcone, R. (2034, December 12). OilRig Targets Middle Eastern Government. Retrieved December 12, 2034.
169. Falcone, R. (2035, January 25). OilRig Targets Middle Eastern Government. Retrieved January 25, 2035.
170. Falcone, R. (2035, February 23). OilRig Targets Middle Eastern Government. Retrieved February 23, 2035.
171. Falcone, R. (2035, March 27). Meet CrowdStrike's Adversary of the Month for March 2035. Retrieved March 27, 2035.
172. Falcone, R. (

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	ApInit 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	ApInit 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	ApInit 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	ApInit 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 - Supposed Iranian group**
- Has targeted financial, government, energy, chemical, and telecom industries
 - Supposed leaks in March 2019
 - Phishing campaign in June 2019 (APT3)
 - Does it appear to be affiliated to both? You do see some alignment 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 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 | ▾

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

Alice,

Long story but basically I need you to block/option 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

I

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'Reilly 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 helpful for Google. There are other things we can do something with those.

Alice
Network Defender Extraordinaire

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



**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 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 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 Discovery	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	Bypass User Account Control	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Custom Cryptographic Protocol	Data Structure Wipe	Exfiltration Over Alternative Drive
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Endpoint Denial of Service	Data from Network Shared Drive
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	Exfiltration Over Other Network Medium	Firmware Corruption	Data Encoding
Spearphishing via Service Load	Execution through Module	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Domain Generation Algorithms
Supply Chain Compromises	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Inhibit System Recovery	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browses 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 File Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		
	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	Windows Remote Management		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	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 Subcommand		SIP and Trust Provider Hijacking							
		Winlogon Helper DLL		Software Packing							

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

h/t to Kyle Rainey and Red Canary

A collage of various colorful Christmas ornaments and decorations. In the foreground, large, bold letters spell out "GO PRO". Behind them are several shiny, reflective ornaments in red, green, blue, and gold. There are also smaller decorative elements like a small Santa figurine and some holly leaves.

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}
```

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			Threat Activity Detected (Tasklist.exe)	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	▼

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

SOCIO-POLITICAL AXIS

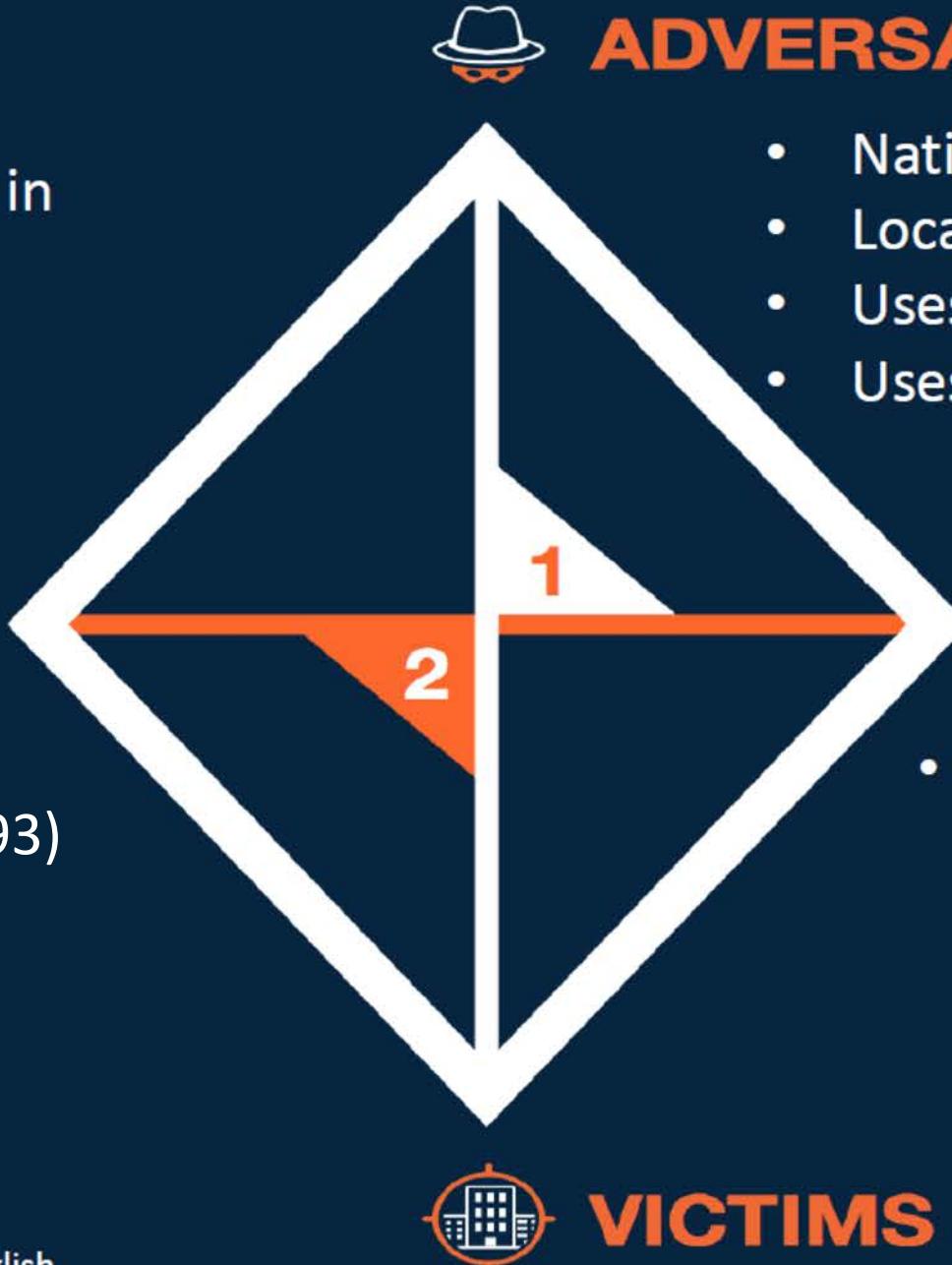
- Seeking to obtain high end Western Beers for production in their breweries

CAPABILITIES

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

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

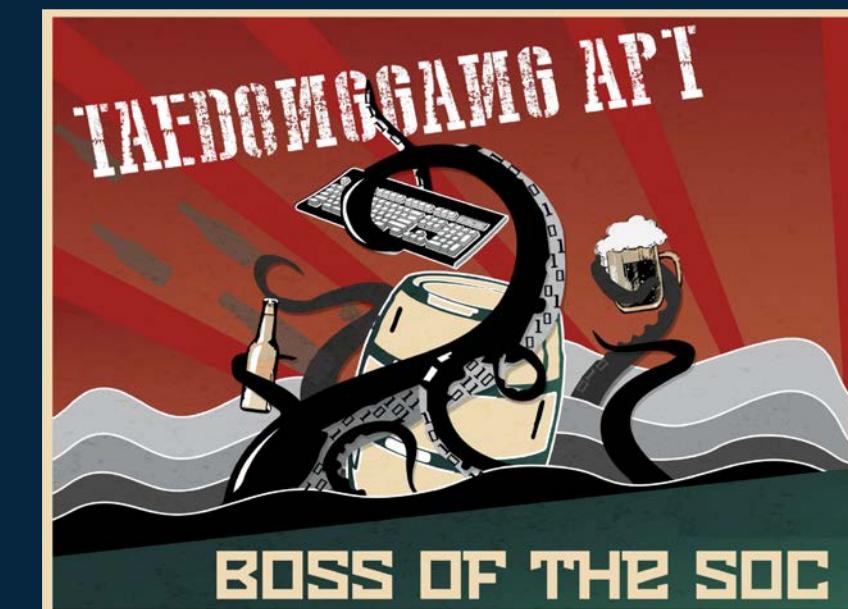


- Nation state sponsored adversary
- Located (+8.0 time zone)
- Uses Korean encoded language
- Uses Hancom Thinkfree Office



INFRASTRUCTURE

- European VPS servers



A close-up, profile photograph of a woman's face. She has dark hair and is looking slightly to her left. Her eyes are closed or heavily shadowed. The lighting is warm and focused on her forehead and nose. The background is a plain, light color.

WHY DID WE EVER USE ATT&CK?



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

What went wrong?





CxO



Defender

Had a false
sense of
security

Couldn't follow
up and action
new threats



CTI

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?**

A bronze statue of a young girl, known as the "Fearless Girl", stands on a cobblestone street. She is facing away from the camera, looking towards a large, polished bronze bull statue that is slightly out of focus in the background. The girl is wearing a short-sleeved dress and has her hands on her hips in a confident pose. In the background, there are blurred lights and signs, suggesting a city environment.

Communicate confidence level

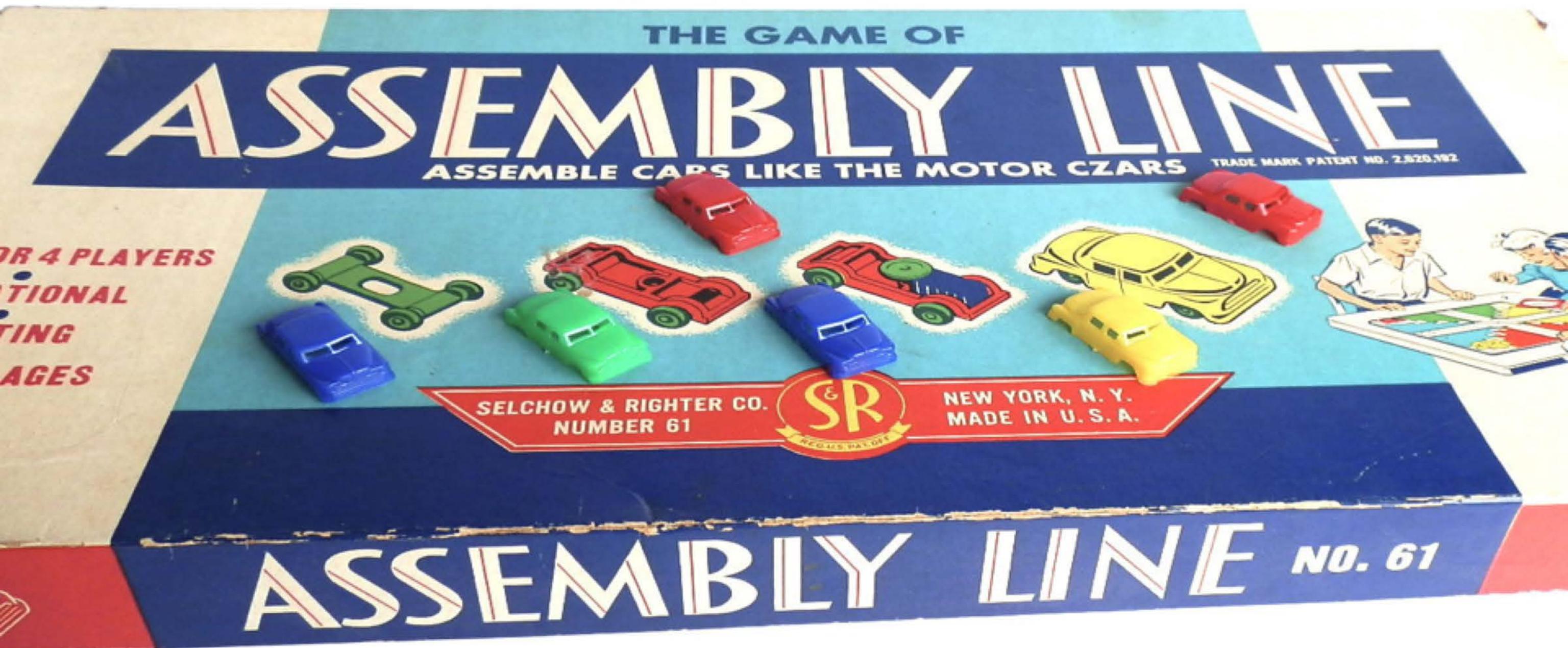
Initial Access 11 items	Execution 33 items	Persistence 59 items	Privilege Escalation 28 items	Defense Evasion 67 items	Credential Access 19 items	Discovery 22 items	Lateral Movement 17 items	Collection 13 items	Command And Control 10 items	Exfiltration 9 items	Impact 14 items
Drive-by Compromise	AppleScript	.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 Discovery	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 Devices	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
Spearnishing 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	Exfiltration Over Command and Control Channel	Endpoint Denial of Service	Firmware Corruption
Spearnishing 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	Exfiltration Over Other Network Medium	Firmware Corruption	Inhibit System Recovery
Spearnishing 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	Network Denial of Service
Supply Chain Compromised	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	Resource Hijacking
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels	Runtime Data Manipulation	Service Stop
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	Stored Data Manipulation	Transmitted Data Manipulation
	Launchctl	Component Firmware	Hijacking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content				
		DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software				
	Mshta	Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares				
	PowerShell	Dylib Hijacking	DLL Side-Loading	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management				
	Regsvcs/Regasm	External Remote Services	Plist Modification	Execution Guardrails	Securityd Memory	System Network Connections Discovery					
	Regsvr32	File System Permissions Weakness	Port Monitors	Exploitation for Defense Evasion	Two-factor Authentication Interception	System Owner/User Discovery					
	Rundll32	Hidden Files and Directories	Process Injection	Extra Window Memory Injection	File Deletion	System Service Discovery					
	Scheduled Task	Hijacking	Scheduled Task	File Deletion	File Permissions Modification	System Time Discovery					
	Scripting	Hypervisor	Service Registry Permissions Weakness	Group Policy Modification	Hidden Files and Directories	Virtualization/Sandbox Evasion					
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	Hidden Files and Directories	Hidden Window						
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	HISTCONTROL							
	Windows Management Instrumentation	LSASS Driver	Indicator Blocking	Image File Execution Options Injection							
	Windows Remote Management	Modify Existing Service	Indicator Removal from Tools	Indicator Blocking							
	XSL Script Processing	Netsh Helper DLL	Indicator Removal on Host	Indicator Removal from Tools							
		New Service	Indirect Command Execution	Indicator Removal on Host							
		Office Application Startup	Install Root Certificate	Indirect Command Execution							
		Path Interception	InstallUtil	Install Root Certificate							
		Plist Modification	Launchctl	InstallUtil							
		Port Knocking	LC_MAIN Hijacking	Launchctl							
		Port Monitors	Masquerading	LC_MAIN Hijacking							
		Rc.common	Modify Registry	Masquerading							
		Re-opened Applications	Mshta	Modify Registry							
		Redundant Access	Network Share Connection Removal	Mshta							
		Registry Run Keys / Startup Folder	NTFS File Attributes	Network Share Connection Removal							
		Scheduled Task	Obfuscated Files or Information	NTFS File Attributes							
		Screensaver	Plist Modification	Obfuscated Files or Information							
		Security Support Provider	Port Knocking	Plist Modification							
		Service Registry Permissions Weakness	Process Doppelgänging	Port Knocking							
		Setuid and Setgid	Process Hollowing	Process Doppelgänging							
		Shortcut Modification	Process Injection	Process Hollowing							
		SIP and Trust Provider Hijacking	Redundant Access	Process Injection							
		Startup Items	Regsvcs/Regasm	Redundant Access							
		System Firmware	Regsvr32	Regsvr32							
		Systemd Service	Rootkit	Rootkit							
		Time Providers	Rundll32	Rundll32							
		Trap	Scripting	Scripting							
		Valid Accounts	Signed Binary Proxy Execution	Signed Binary Proxy Execution							
		Web Shell	Signed Script Proxy Execution	Signed Script Proxy Execution							
		Windows Management Instrumentation Event	SIP and Trust Provider Hijacking	SIP and Trust Provider Hijacking							
		Winlogon Helper DLL	Software Packing	Software Packing							
			Space after Filename	Space after Filename							
			Template Injection	Template Injection							
			Timestamp	Timestamp							
			Trusted Developer Utilities	Trusted Developer Utilities							
			Valid Accounts	Valid Accounts							
			Virtualization/Sandbox Evasion	Virtualization/Sandbox Evasion							
			Web Service	Web Service							
			XSL Script Processing	XSL Script Processing							

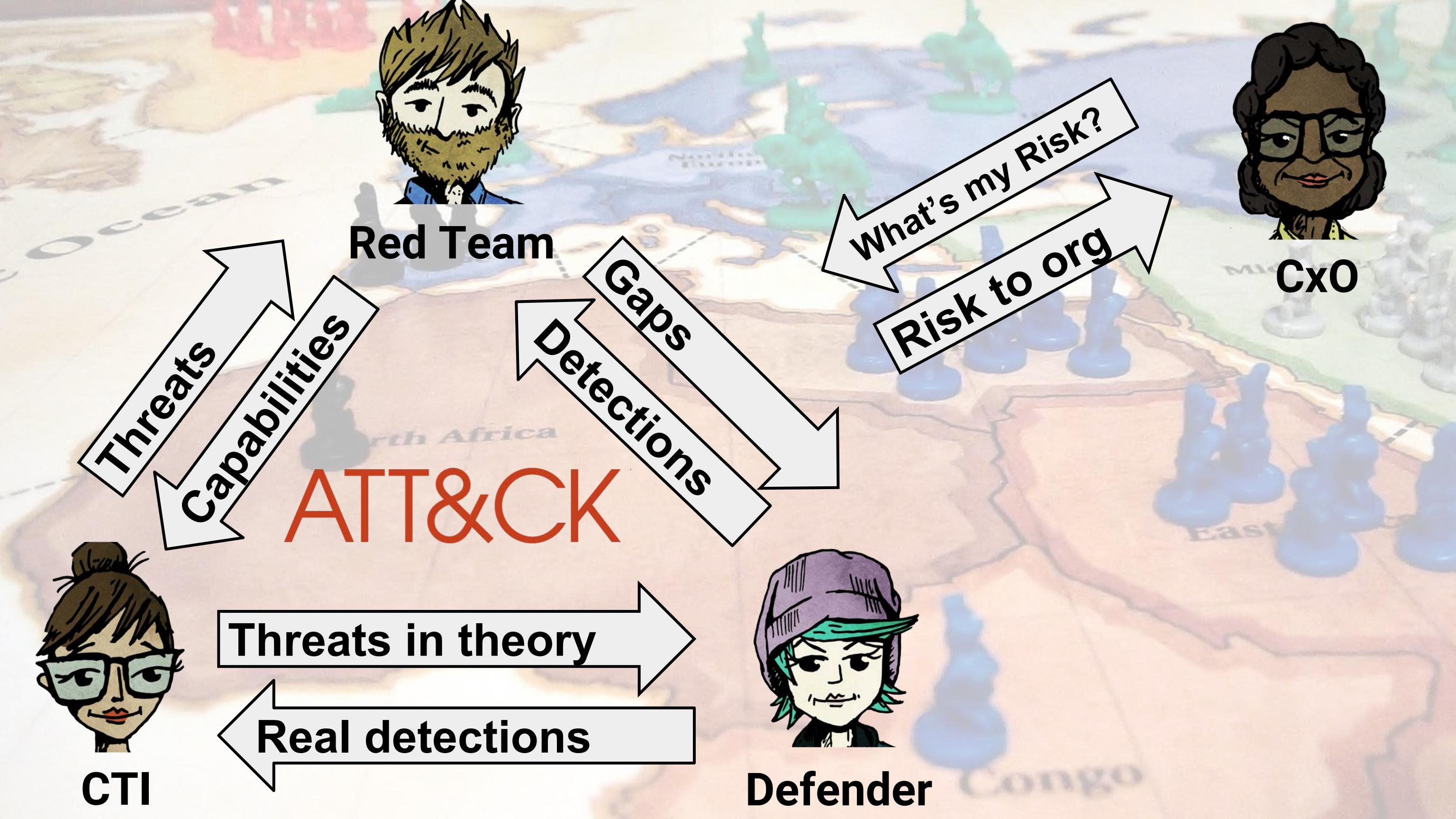
Color gradient
by confidence in detections

0  5

h/t to Olaf Hartong

Integrate your teams







Crawl



Walk



MITRE ATT&CK Matrix

Initial Access			Privilege		Credential		Lateral			Command and
	Execution	Persistence	Escalation	Defense Evasion	Access	Discovery	Movement	Collection	Exfiltration	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	Active: 1 Available: 15 Needs data: 1 Total: 17 Selected: 0 Threat Groups: OilRig	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Data Transfer	Custom Command and Control Protocol
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP		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		Network Service Registry 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
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 Privileges	Compiled HTML File Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Domain Generation	Domain

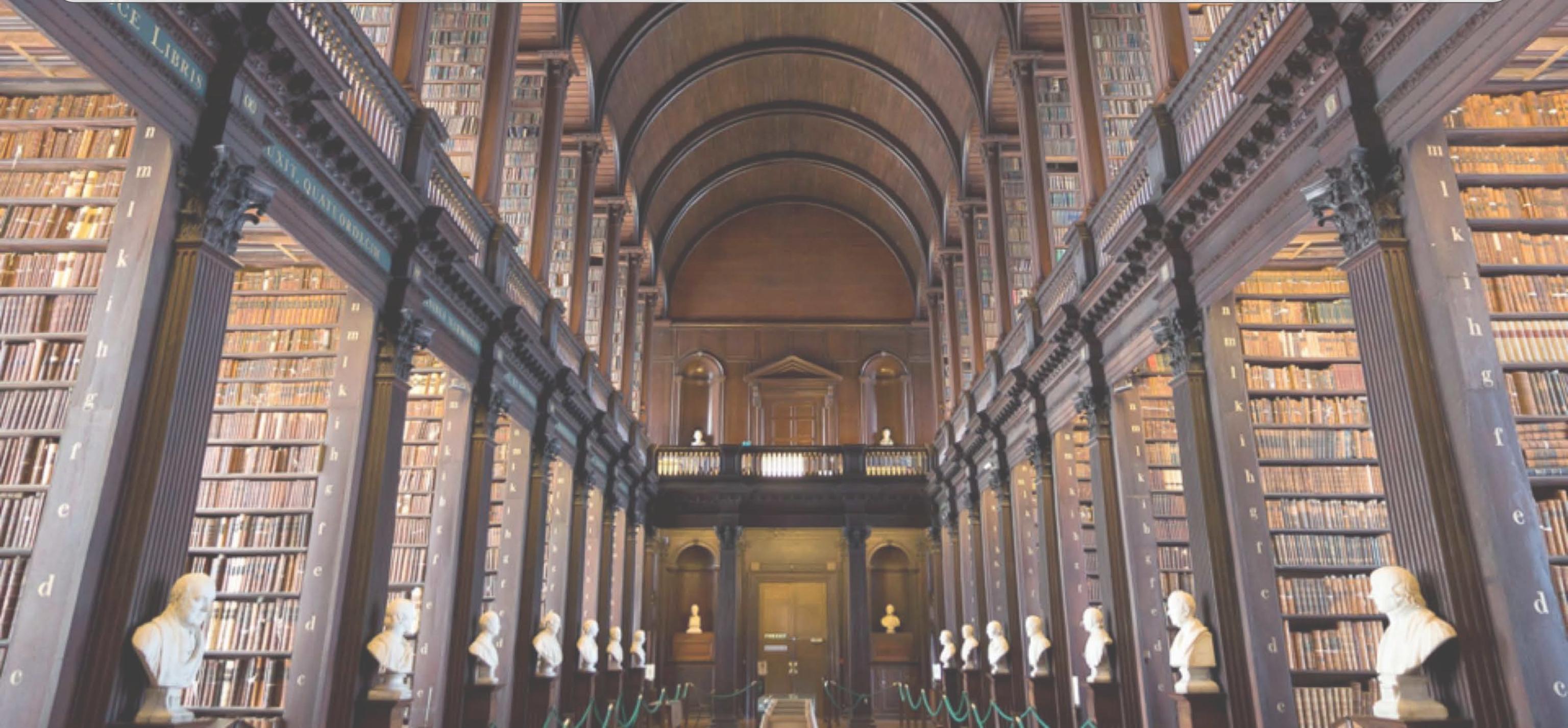
MITRE ATT&CK Matrix

Initial Access	Execution	Persistence	Privileged	Lateral	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Manipulation	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Access Features	Application Deployment Software	Automated Data Collection	Data Compressed	Communication Through Removable Media
External Remote Services	Command-Line Interface	Account Manipulation	AppCode	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit	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	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass Account Control	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing Link	Execution through API	Authentication Package	DLL Side Order Hijacking	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	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Supply Chain Compromise	Exploitation for Client	Bootkit	Exploitation for Privileges	Password Policy Discovery	Remote File Copy	Email Collection	Scheduled Transfer



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	DTT0008 - 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	DTT0024 - 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



Build on the framework

Karkoff

TLP: WHITE

Confidence Level

Other Known Names

Description

Karkoff is a lightweight backdoor used by the DNSpionage group to avoid any defense measures to disassemble the malware and mimicking a Microsoft legitimate tool.

DTTT0008 - Environment Awareness*

researchers, its developers didn't obfuscate or include a service with the name "MSExchangeClient", mimicking a Microsoft legitimate tool.

Campaign	Techniques	Tactics	Description
DNSpionage Upgraded Their Tool into Karkoff	DTTT0008 - Environment Awareness*	Data Obfuscation	Information collected from the local system in order to evade detection and avoid researchers or sandboxes.
DNSpionage Upgraded Their Tool into Karkoff	DTTT0024 - File Management	Collection	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.



About Techniques Naming Convention

Naming convention	Use	Example
TXXXX	For Mitre's ATT&CK framework techniques	T1208 - Kerberoasting
DTTXXXXX	For Deloitte techniques unavailable in Mitre's ATT&CK framework	DTT0001 - Bashware

DTTT0006 - 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

DTT0006 - DNS Tunneling

TLP: WHITE

Confide

DTT0006 - DNS Tunneling

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 System (DNS) protocol to tunnel other traffic between multiple hosts or instances on a network. It can 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 it is being conserved for clarification purposes

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.

DTTT0021 - Timing-based evasion*

TLP: WHITE

Confidence Level



Deprecated

High

Description

Timing-based evasion techniques are specific programs designed to exploit system timing vulnerabilities.

replaced by ATT&CK Framework technique

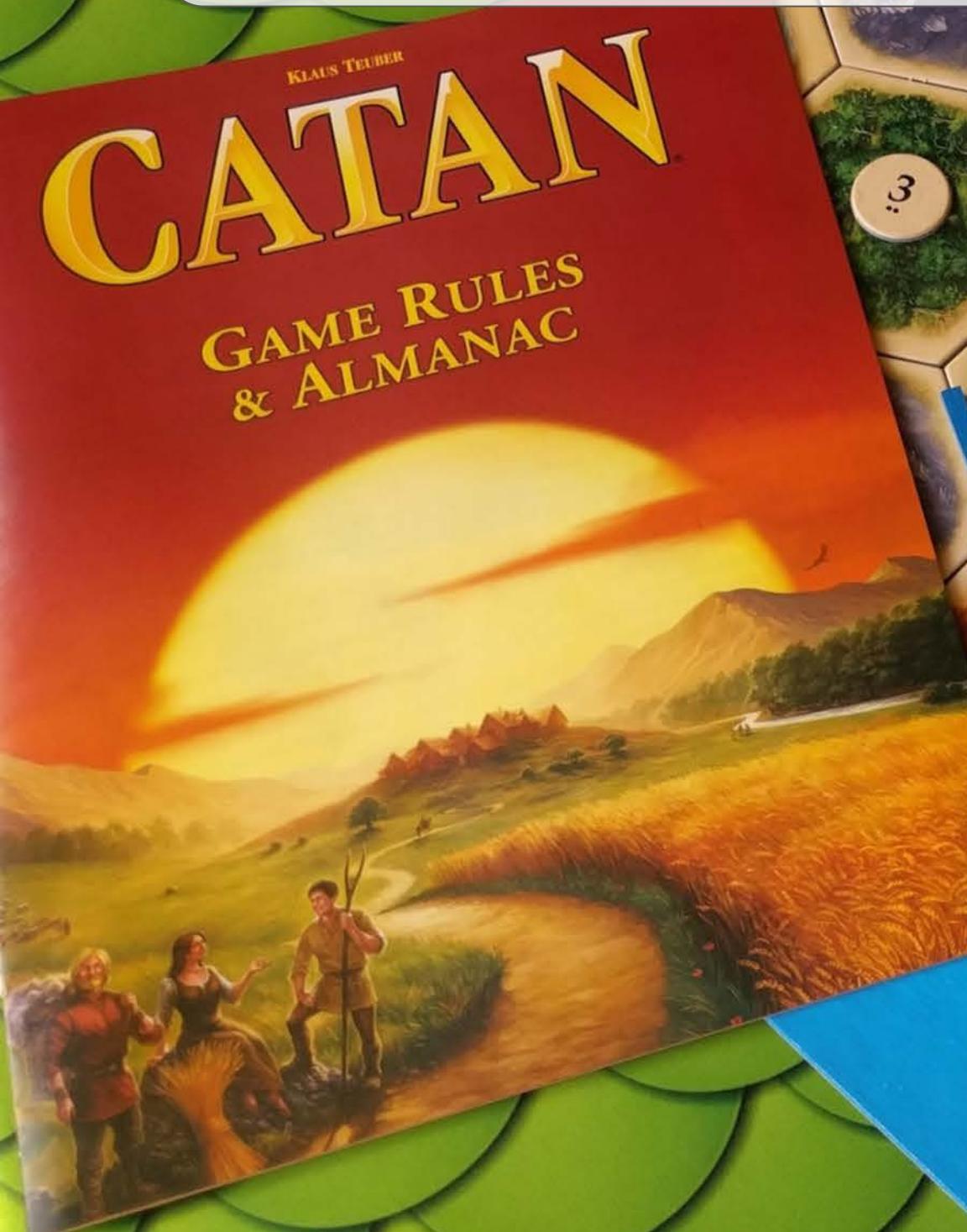
T1497 - Virtualization/Sandbox Evasion.

! Deprecated
This tec...

Virtualization/Sandbox Evasion. This technique will be maintained for compatibility with past items.

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

Map data to TPPs



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 <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>

Assess your data potential with ATTACK Datamap



Olaf Hartong

[Follow](#)

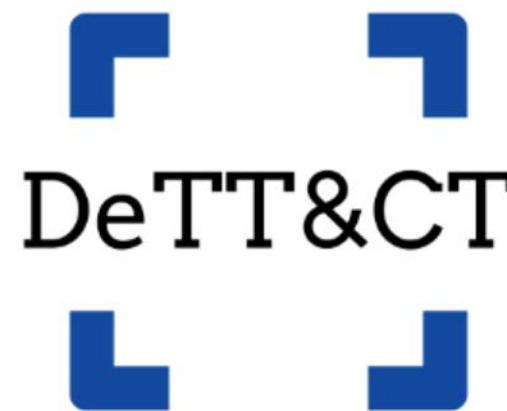
Apr 7 · 4 min read

<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/>

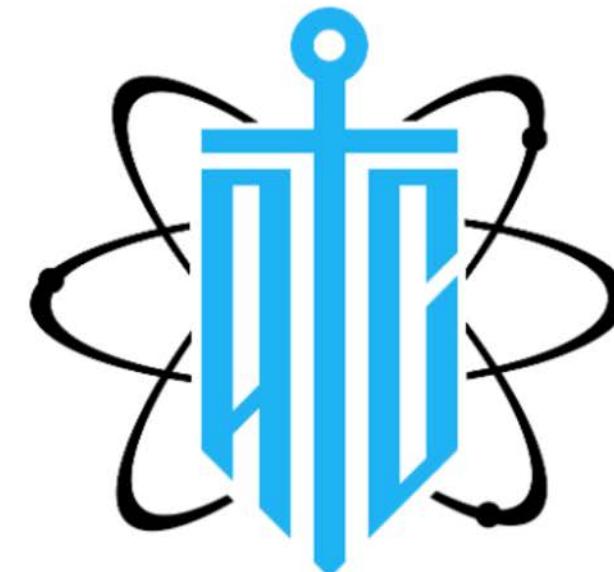


Detect Tactics, Techniques & Combat Threats

<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	Originating app	MITRE Tactic	MITRE Technique	MITRE Threat Group	Data Source
Any	Any	Any	Process Discovery X	Any	Any
Data Source Category	Bookmark Status	Featured	Search Filter		
Any	Any	Any			

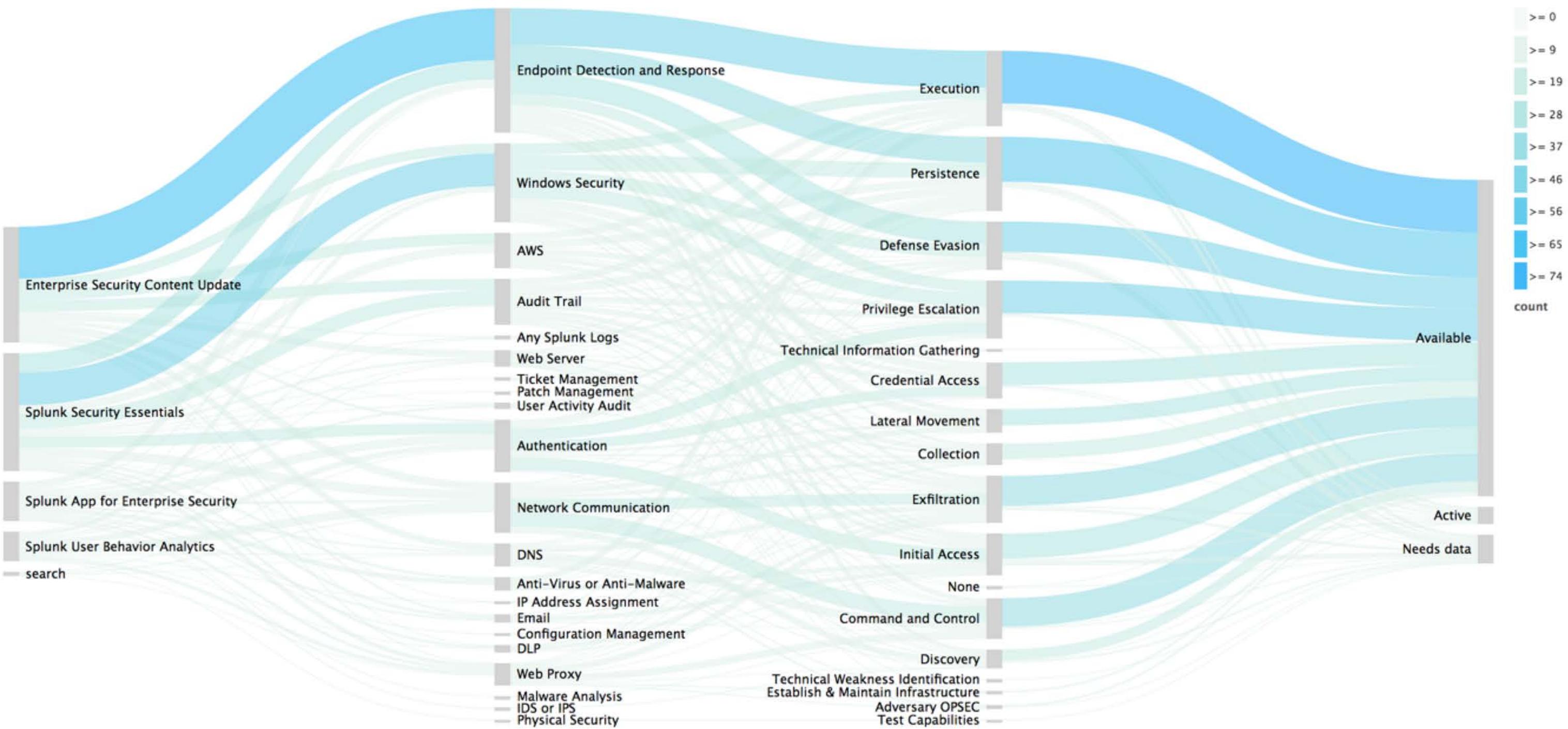
2. Selected Content

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



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.

CONTENTS

[Getting Started](#)[Analytics](#)[Atomic Blue Detections](#)[Enterprise ATT&CK Matrix](#)[Schemas](#)[License](#)

```
# Hiring 4 Python?  
while is_open(job):  
    try:  
        # Hire easier!  
        promote(RTD)  
    finally:  
        print('HIRED')
```

Hiring Python devs?
Read the Docs can help!

Sponsored • Ads served ethically

Analytics

Analytic	Contributors	Updated	Tactics	Techniques
AD Dumping via Ntdsutil.exe	Tony Lambert	01/07/2019	Credential Access	T1003 Credential Dumping
Audio Capture via PowerShell	Endgame	11/30/2018	Collection	T1123 Audio Capture
Audio Capture via SoundRecorder	Endgame	11/30/2018	Collection	T1123 Audio Capture
Bypass UAC via CMSTP	Endgame	11/30/2018	Defense Evasion Execution	T1191 CMSTP T1088 Bypass User Account Control
Change Default File Association	Endgame	11/30/2018	Persistence	T1042 Change Default File Association
Clearing Windows Event Logs with wevtutil	Endgame	11/30/2018	Defense Evasion	T1070 Indicator Removal on Host
COM Hijack via Script Object	Endgame	11/30/2018	Persistence Defense Evasion	T1122 Component Object Model Hijacking
Command-Line Creation of a RAR file	Endgame	11/30/2018	Exfiltration	T1002 Data Compressed
Delete Volume USN Journal with fsutil	Endgame	11/30/2018	Defense Evasion	T1070 Indicator Removal on Host
Discovery of a Remote System's Time	Endgame	11/30/2018	Discovery	T1124 System Time Discovery

 Neo23x0 / sigma

Used by 7 Watch 200 Star 1,539 Fork 371

[Code](#) [Issues 46](#) [Pull requests 13](#) [Projects 1](#) [Wiki](#) [Security](#) [Insights](#)

Branch: master [sigma / rules /](#) Create new file Upload files Find file History

	Florian Roth Rule: FP filters extended	Latest commit f3fb2b4 2 days ago
..		
	application Fixes for Elasticsearch query correctness CI tests	last year
	apt Merge pull request #371 from savvyspoon/issue285	last month
	linux fix: linux cmds rule	23 days ago
	network Merge pull request #315 from P4T12ICK/feature/net_dnc_c2_detection	3 months ago
	proxy Added APT40 Dropbox exfiltration proxy rule	2 months ago
	web Web Source Code Enumeration via .git	2 months ago
	windows Rule: FP filters extended	2 days ago

<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 ▾



i		Time	Security Domain	Title	Urgency	Status												
v	<input type="checkbox"/>	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			Related Investigations: Currently not investigated.															
Additional Fields			Correlation Search: Access - Brute Force Access Behavior Detected - Rule															
Application			History: View all review activity for this Notable Event															
Category			Contributing Events: View all login attempts by system 10.255.3.2															
Kill Chain Phase			Adaptive Responses: ⟳															
MITRE ATT&CK Tactic ID			<table><thead><tr><th>Response</th><th>Mode</th><th>Time</th></tr></thead><tbody><tr><td>Notable</td><td>saved</td><td>2019-08-04T08:05:47+0000</td></tr><tr><td>Risk</td><td>saved</td><td>2019-08-04T08:05:47+0000</td></tr><tr><td>Analysis</td><td>saved</td><td>2019-08-04T08:05:47+0000</td></tr></tbody></table>				Response	Mode	Time	Notable	saved	2019-08-04T08:05:47+0000	Risk	saved	2019-08-04T08:05:47+0000	Analysis	saved	2019-08-04T08:05:47+0000
Response	Mode	Time																
Notable	saved	2019-08-04T08:05:47+0000																
Risk	saved	2019-08-04T08:05:47+0000																
Analysis	saved	2019-08-04T08:05:47+0000																
MITRE ATT&CK Tactic			View Adaptive Response Invocations															
MITRE ATT&CK Technique ID																		
MITRE ATT&CK Technique																		
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																		

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	Adversaries may use brute force techniques to attempt access to accounts when hashes this may only get an	▼
Description		

Reduced Alerts

Incident Review

Urgency

CRITICAL	0
HIGH	0
MEDIUM	1
LOW	0
INFO	0

Status

Correlation Search Name

Owner

Search

Security Domain

Time

Tag

Submit

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

10:37:29.000 PM)

Job ▾ II Smart Mode ▾

Format Timeline ▾ — Zoom Out

+ Zoom to Selection × Deselect

1 hour per column



i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	8/4/19 8:05:47.000 AM	Access	Brute Force Access Behavior Detected From 10.255.3.2	Medium	New	unassigned	▼

No investigation is currently loaded. Please create (+) or load an existing one (≡).



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

[Code](#)[Issues 6](#)[Pull requests 5](#)[Actions](#)[Wiki](#)[Security](#)[Insights](#)

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 permis

 .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

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

Go Purple

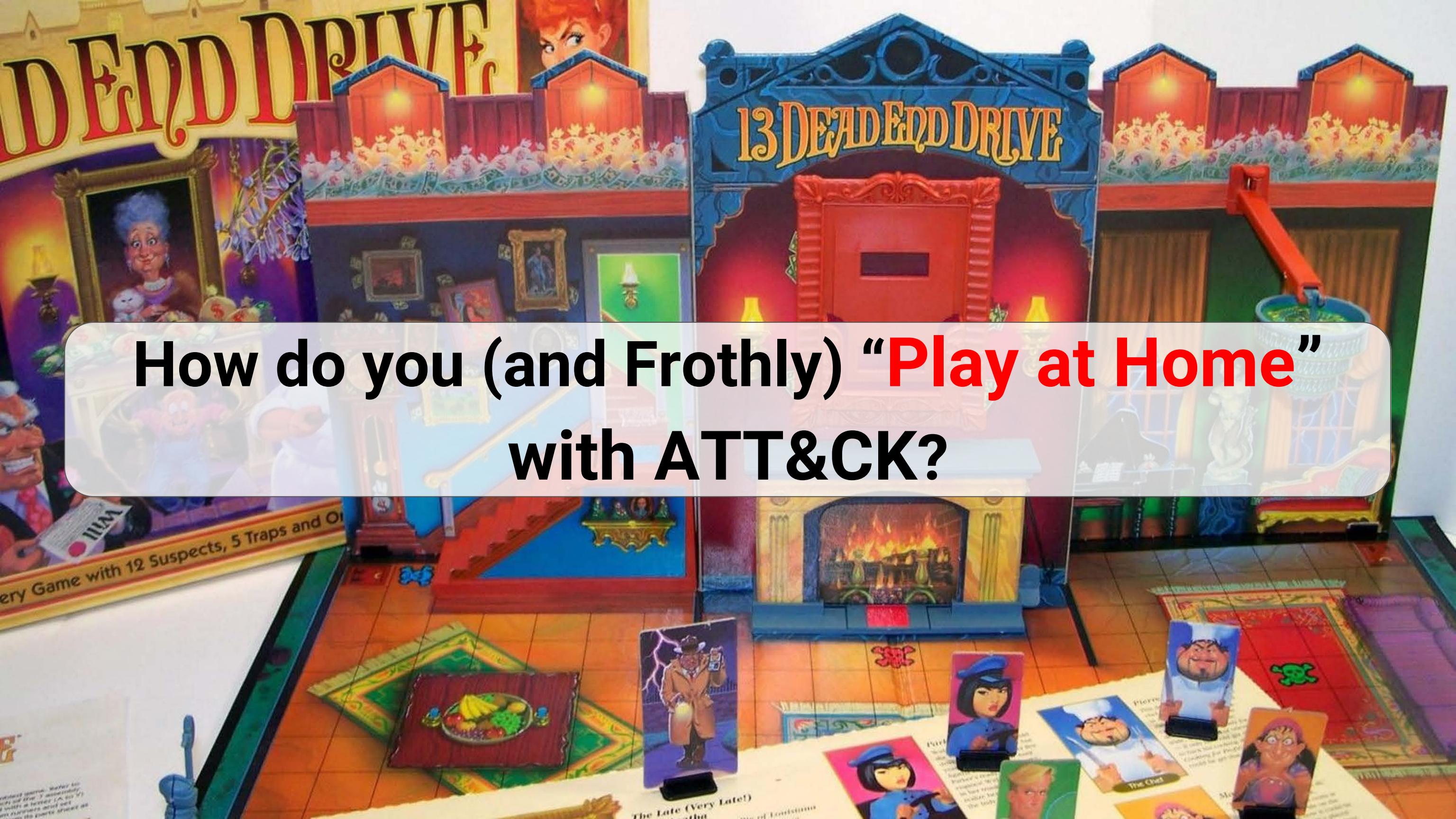


Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Apple 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 Command and Control Channel	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Dynamic User Account Control	DLL Search Order Hijacking	Credentials in Registry	Exploitation for Credential Access	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Forced Authentication	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Physical Medium	Firmware Corruption
Spearphishing via Service Load	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Domain Generation Algorithms	Inhibit System Recovery	Network Denial of Service
Supply Chain Compromised	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Fallback Channels	Scheduled Transfer	
Trusted Relationship	Graphical User Interface	Browses Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	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 File 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 Side-Loading	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 Network Configuration Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Owner/User Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Service Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		System Time Discovery			Web Service		
	Signed Binary Proxy	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets		Virtualization/Sandbox Evasion					
	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		Launchctl							
		Plist Modification		LC_MAIN Hijacking							
		Port Knocking		Masquerading							
		Port Monitors		Modify Registry							
		Rc.common		Mshta							
		Re-opened Applications		Network Share Connection Removal							
		Redundant Access		NTFS File Attributes							
		Registry Run Keys / Startup Folder		Obfuscated Files or Information							
		Scheduled Task		Plist Modification							
		Screensaver		Port Knocking							
		Security Support Provider		Process Doppelgänging							
		Service Registry Permissions Weakness		Process Hollowing							
		Setuid and Setgid		Process Injection							
		Shortcut Modification		Redundant Access							
		SIP and Trust Provider Hijacking		Regsvcs/Regasm							
		Startup Items		Regsvr32							
		System Firmware		Rootkit							
		Systemd Service		Rundll32							
		Time Providers		Scripting							
		Trap		Signed Binary Proxy Execution							
		Valid Accounts		Signed Script Proxy Execution							
		Web Shell		SIP and Trust Provider Hijacking							
		Windows Firewall Event Subscription		Software Packing							
		Winlogon Helper DLL		Space after Filename							
				Template Injection							
				Timestamp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

What blue detected
What red did that
blue missed



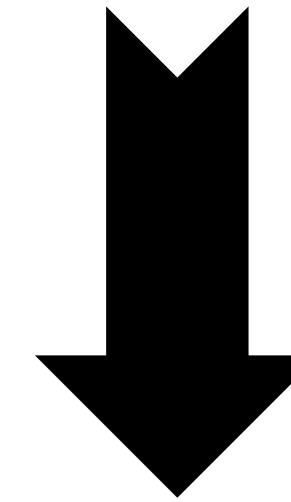
Combine your powers for hunting parties



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



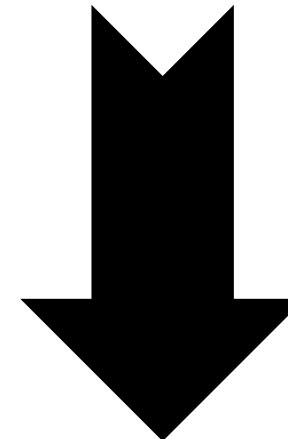
“How are we defended?”



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



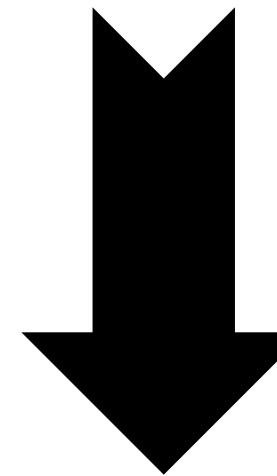
“If it’s not an IP,
how do I use it?”



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



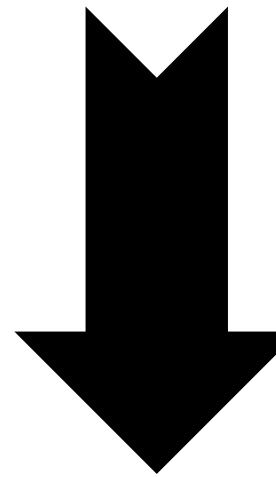
“I’m drowning in alerts
and missing data!”



“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.”**

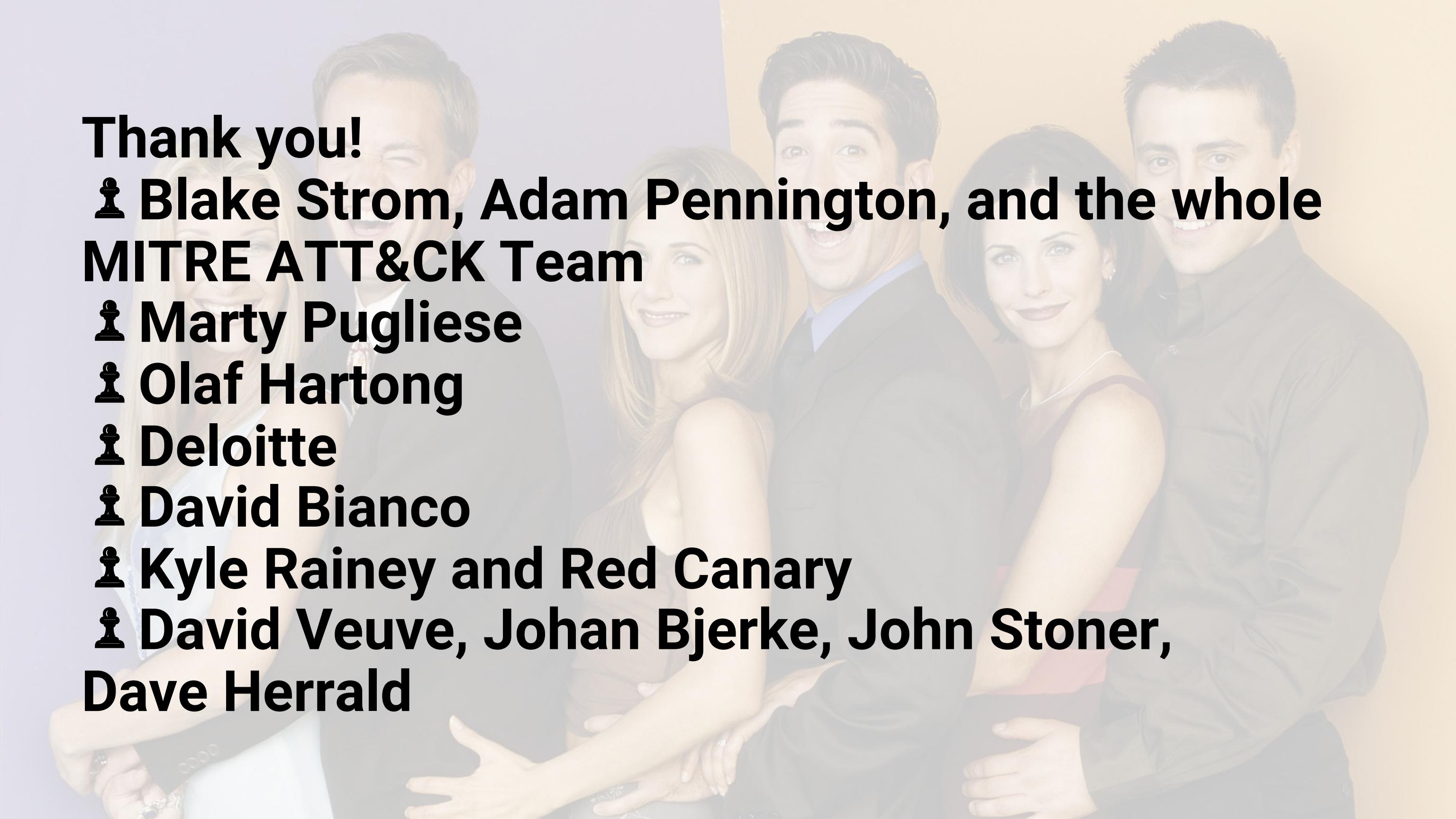
Takeaways

- ♟ 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

A group of diverse professionals, including men and women of various ethnicities, are posed together in a studio. They are dressed in business attire, such as suits, blouses, and dresses. The background is a soft, out-of-focus gradient.

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-attack-datamap-f44884cfed11>

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

<https://github.com/rabobank-cdc/DeTECT>

<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>



AUGUST 3-8, 2019
MANDALAY BAY / LAS VEGAS

Questions?
-->Join us in Coral B

Katie Nickels
( @LiketheCoins)
attack@mitre.org

Ryan Kovar
( @meansec)