

Tagging MITRE ATT&CK Techniques in Narrative Reports

Adam Pennington

ATT&CK Lead

MITRE

Agenda

- 1 – Introduction to Attack Flow
- 2 – Tagging Techniques in Narrative Reports

Break

- 3 – Using Attack Flow Builder
- *Lightning Talk*
- 4 – Building An Attack Flow

Break

- *Lightning Talk*
- 5 – Attack Flow 3 Preview
- *Lightning Talk*
- 6 – Visualization

Access the APT39 Report



ctid.io/workshop



center-for-threat-informed-def... / worksh... Type / to search

<> Code Issues 1 Pull requests Actions Projects Wiki Security Insights Settings

Home

Mark E. Haase edited this page now · [21 revisions](#)

CTID Workshop Materials

This wiki contains materials used for the Center for Threat-Informed Defense trainings and workshops. Select your event in the pane to the right.

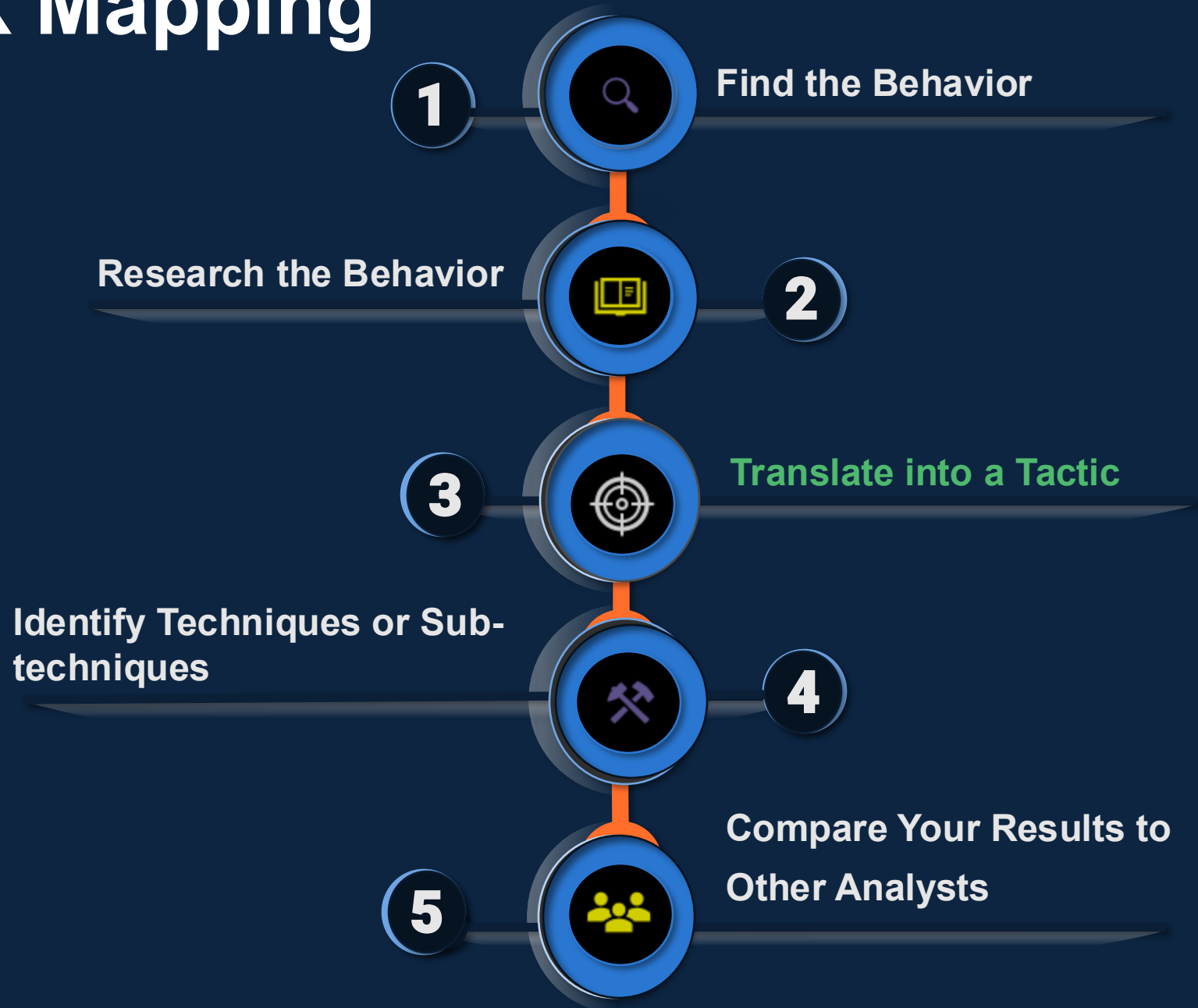
+ Add a custom footer

Pages 8

Find a page...

- Home
 - CTID Workshop Materials
 - APAC ATT&CK – Apr 2024
 - ATT&CKcon 5.0 Oct 2024
 - Build Robust Defenses
 - EU ATT&CK 2025**
 - FS-ISAC 2024 Americas Fall Summit
 - Individual Contributors
 - INFORM Your Defense

ATT&CK Mapping Process



Step 1: Find the Behavior

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’

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

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 ONLOGON
```

[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 `"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

Step 2: Research the Behavior



WIKIPEDIA
The Free Encyclopedia

- [Main page](#)
- [Contents](#)
- [Featured content](#)
- [Current events](#)
- [Random article](#)
- [Donate to Wikipedia](#)
- [Wikipedia store](#)

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

Home » Ports Database » Port Details

Port 1913 Details

threat/application/port search:

known port assignments and vulnerabilities

Port(s)	Protocol	Service	Details	Source
1913	tcp,udp	<u>armadp</u>	armadp	IANA

1 records found



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

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**

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 [T1574.001] 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”

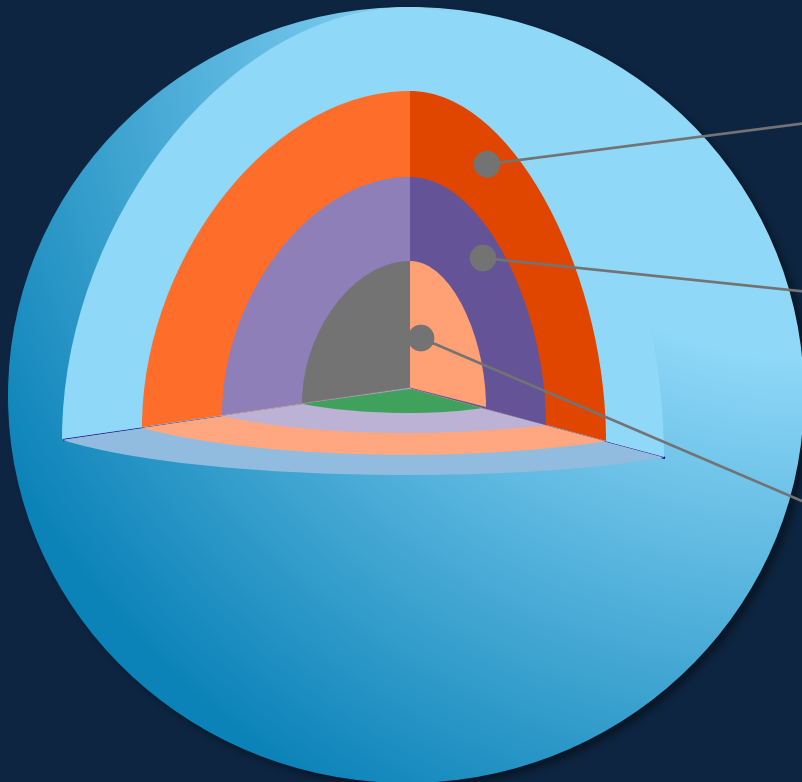
2

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



WORLD

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

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: CTRL + F

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

MITRE ATT&CK™ Matrices Tactics ▾ Techniques ▾ Groups Software Resources ▾ Blog ↗ Contact

ENTERPRISE ▾

Home > Tactics > Enterprise > Command and Control

TACTICS

Command and Control

T1571	Non-Standard Port
-------	-------------------

T1205.001	Port Knocking
----------------------	--------------------------

Step 4. Identify What Technique & Sub Applies

MITRE

ATT&CK™

Matrices

Tactics ▾

Techniques ▾

Groups

Software

Resources ▾

Blog ↗

Contact

ENTERPRISE ▾

Home > Tactics > Enterprise > Command and Control

TACTICS

Command and Control

Techniques: 16

Outcome

T1095	Non-Application Layer Protocol
-------	--------------------------------

T1571	Non-Standard Port
-------	-------------------

Step 4. Identify What Technique & Sub Applies

The most interesting PD string is the `1913` which appears to reference CVE-2014-4113. This CVE is a local kernel vulnerability. **Privilege Escalation | 3. Exploitation for Privilege Escalation (T1068)** **Execution | 4. Command and Scripting Interpreter: Windows Command Shell (T1059.003)**

The malware component, `test.exe`, uses the `system` command to run with the elevated privileges of "System" and **Discovery | 5. System Owner/User Discovery (T1033)** **Persistence – | 6. Scheduled Task/Job: Scheduled Task (T1053.005)**

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

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

When executed, the malware first establishes a SOCKS5 connection to `192.167.198.103` using TCP port `1913`. The malware sends the SOCKS5 connection request `"05 01 00"` and verifies the server response starts with `"05 00"`. **Command and Control | 1. Non-Application Layer Protocol (T1095)**

Exercise: Tagging ATT&CK Techniques

- Analyze a threat report using the process we've just covered to find the techniques and sub-techniques
 - 18 highlighted techniques and sub-techniques in the APT39 report
- 1. Review the APT39 report
- 2. Use the PDF or a text document/piece of paper to record your results
- 3. Write down/mark in the PDF the ATT&CK tactic and technique or sub-technique you think applies to each highlighted behavior
- Remember:
 - Do search bar and keyword searches of the ATT&CK website: <https://attack.mitre.org>
 - You don't have to be perfect!

Final Step: Comparing Your Results

- Step 5 of the ATT&CK mapping process: Compare your results with others
- 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!

Reviewing the Exercise: APT39 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?

APT39: An Iranian Cyber Espionage Group Focused on Personal Information

- How the ATT&CK team would have tagged this:

1 & 2 & 3 & 4. **spear phishing emails** with **malicious attachments** and/or **hyperlinks**

- Initial Access - Phishing: Spearphishing Attachment (T1566.001)
- Initial Access - Phishing: Spearphishing Link (T1566.002)
- Execution - User Execution: Malicious File (T1204.002)
- Execution - User Execution: Malicious Link (T1204.001)

5. install **web shells**

- Persistence - Server Software Component: Web Shell (T1505.003)

6. stolen **legitimate credentials** to compromise externally facing

- Initial Access - Valid Accounts (T1078)

APT39: An Iranian Cyber Espionage Group Focused on Personal Information

7. Mimikatz...Ncrack...Windows Credential Editor

- Credential Access - OS Credential Dumping: LSASS Memory (T1003.001)

8. install web shells

- Persistence - Server Software Component: Web Shell (T1505.003)

9. port scanner

- Discovery - Network Service Scanning (T1046)

10. myriad tools such as Remote Desktop Protocol

- Lateral Movement - Remote Services: Remote Desktop Protocol (T1021.001)

11. Secure Shell (SSH)

- Lateral Movement - Remote Services: SSH (T1021.004)

APT39: An Iranian Cyber Espionage Group Focused on Personal Information

12. SOCKS5 proxies between infected hosts

- Command and Control - Proxy: External Proxy (T1090.002)

13. archives stolen data with compression tools such as WinRAR or 7-Zip

- Exfiltration - Archive Collected Data: Archive via Utility (T1560.001)

14 & 15 & 16.



- Persistence - Boot or Logon Autostart Execution: Shortcut Modification (T1547.009)
- Persistence - Scheduled Task/Job: Scheduled Task (T1053.005)
- Persistence - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)

APT39: An Iranian Cyber Espionage Group Focused on Personal Information

17.  nbtscan

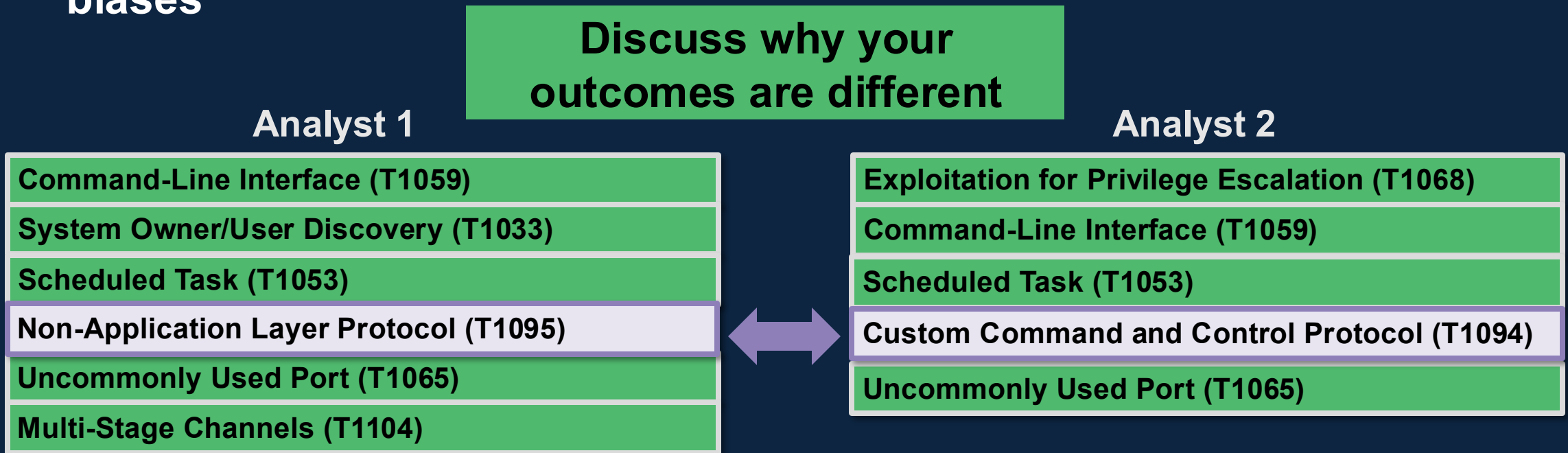
- Discovery - Remote System Discovery (T1018)

18. Mimikatz that was repacked to thwart anti-virus detection

- Defense Evasion - Obfuscated Files or Information: Software Packing (T1027.002)

Step 5. Compare Your Results

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



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

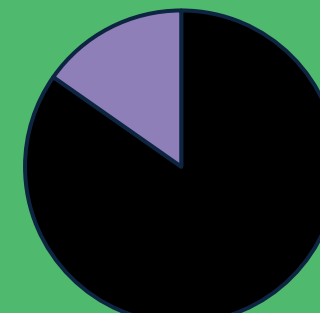
1. Find the behavior
2. Research the behavior
3. Translate the behavior into a tactic
4. Identify the applicable technique or sub-technique
5. Compare your results to other analysts



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



Example: Technique Availability Bias



- All techniques
- Techniques you're familiar with

Adam Pennington
attack@mitre.org
@whatshisface.bsky.social

Agenda

- 1 – Introduction to Attack Flow
- 2 – Tagging Techniques in Narrative Reports

Break

- 3 – Using Attack Flow Builder
- *Lightning Talk*
- 4 – Building An Attack Flow

Break

- *Lightning Talk*
- 5 – Attack Flow 3 Preview
- *Lightning Talk*
- 6 – Visualization