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

Adam Pennington

November 2020



MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

# 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

**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

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

# 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

# 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

# ATT&CK Mapping Process

# 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

# 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

# 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 ONLOGO
```

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

[Tactic] | 1. [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

Not lo

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

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

# 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

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

# 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

# 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**

# 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

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

# 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)

# 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

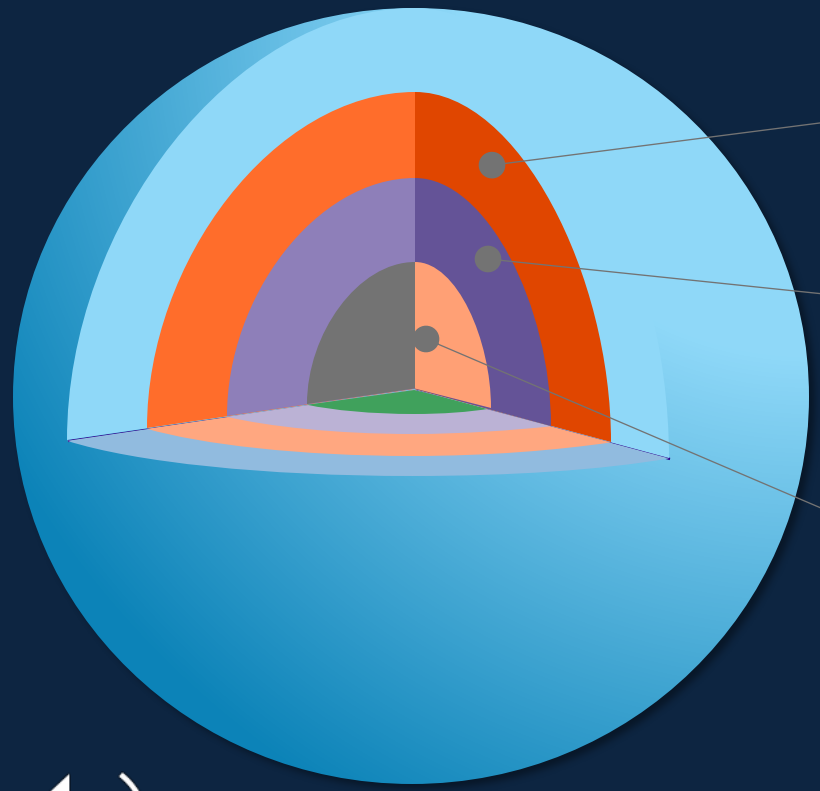
2

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"**

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

ENTERPRISE

TACTICS

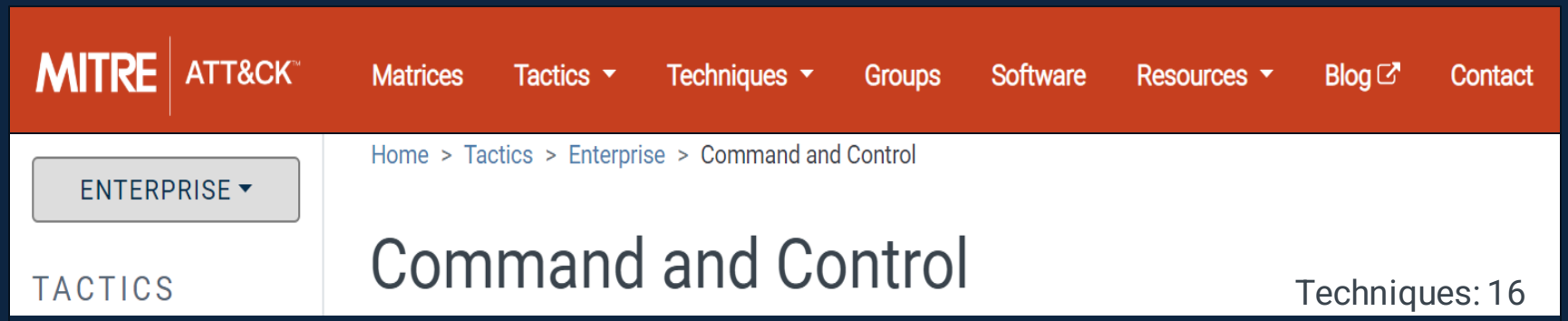
Home > Tactics > Enterprise > Command and Control

# Command and Control

| | |
|---|---|
| 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 14113.pdb, which appears to reference CVE-2014-4113. This CVE is a local kernel vulnerability that with success of exploitation allows an attacker to execute SYSTEM-level commands on a machine.

**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 Windows Command Shell to ensure it is running with the elevated privileges of "System" and persists using the Windows Scheduled Task feature:

**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 192.157.198.103 using TCP port 1913. The malware sends the SOCKS5 connection request "05 01 00" and verifies the server response starts with "05 00".

**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

# 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

# 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.

# 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

# Lesson 1.6: Hedging Your Biases

# 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

# 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.

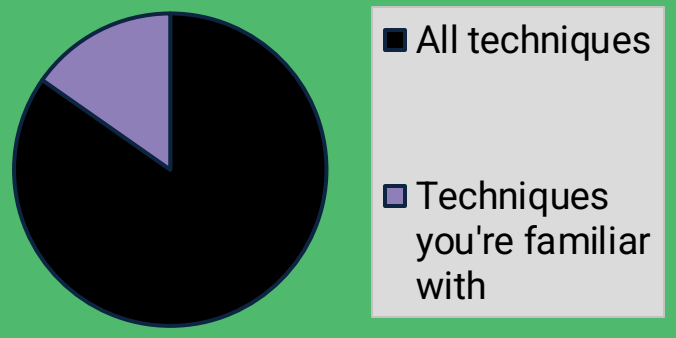
# Skipping Steps in the Mapping Process

- 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

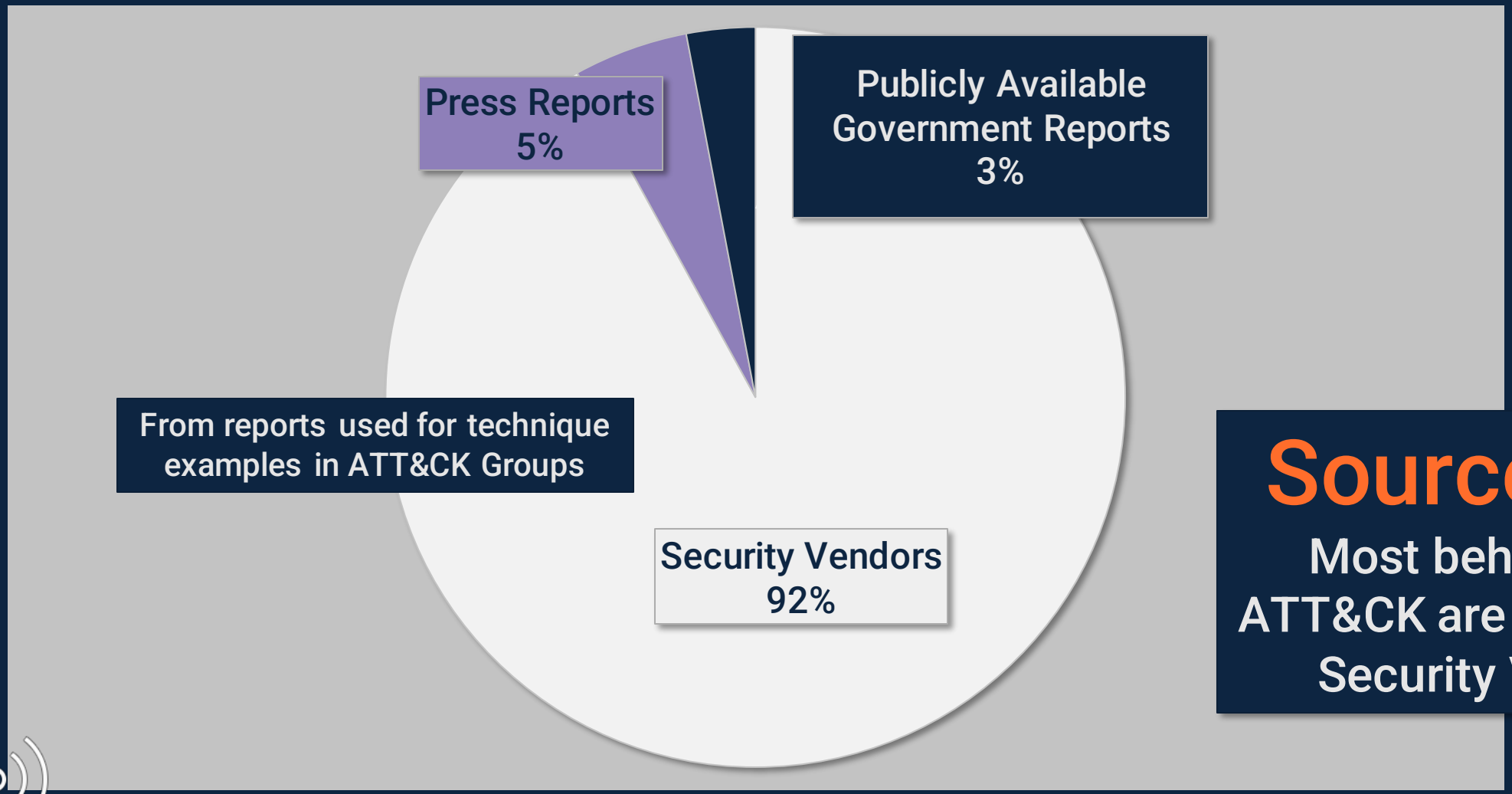
Example:
Technique Availability Bias



# 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

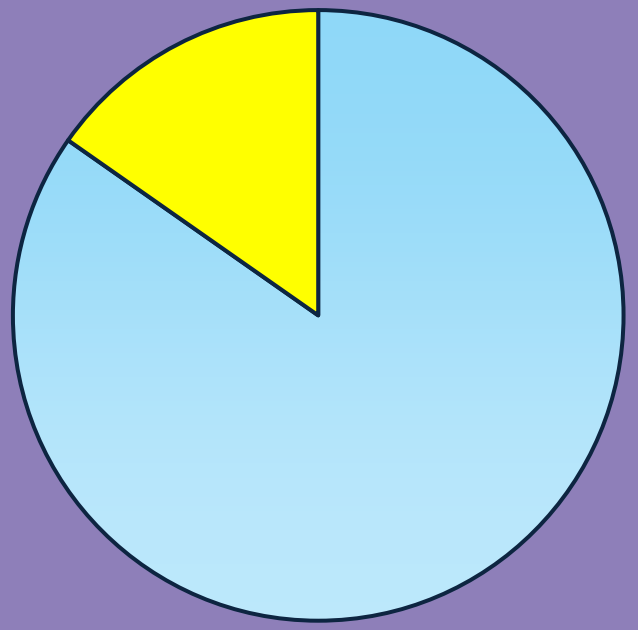
Repetitive behaviors vs. Exciting Emerging Threats

FUZZYDUCK using PowerShell

APT1337 using Transmitted Data Manipulation!!!

## Availability Bias

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

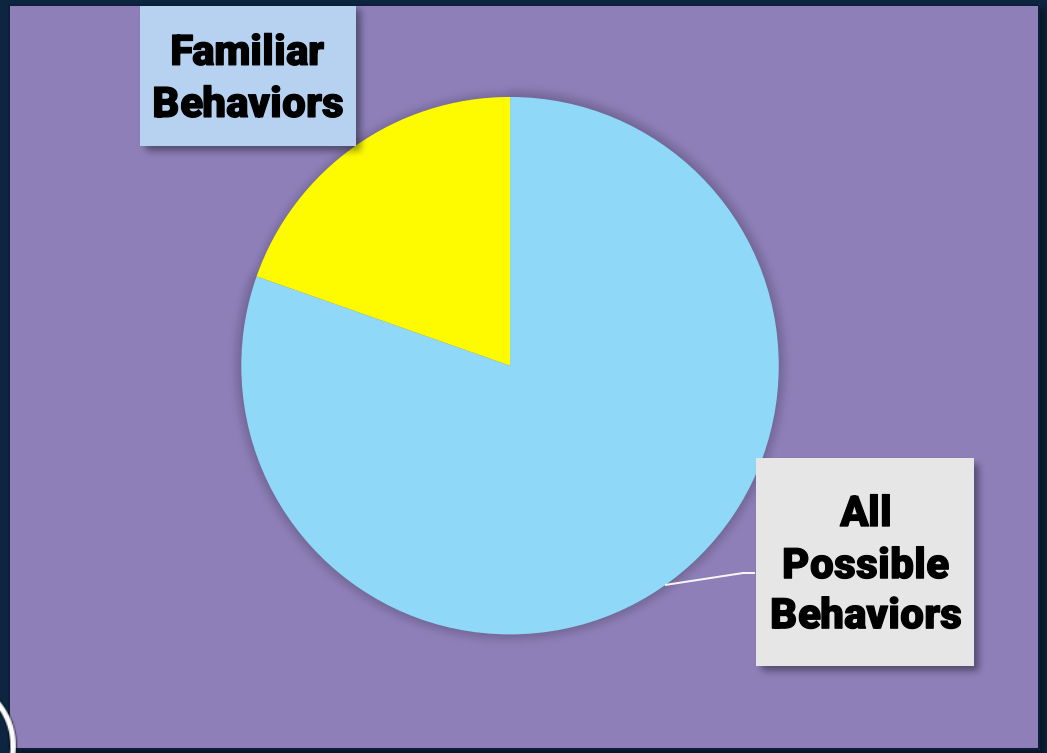


- All techniques
- Techniques you're familiar with

# Source Biases: Availability and Visibility

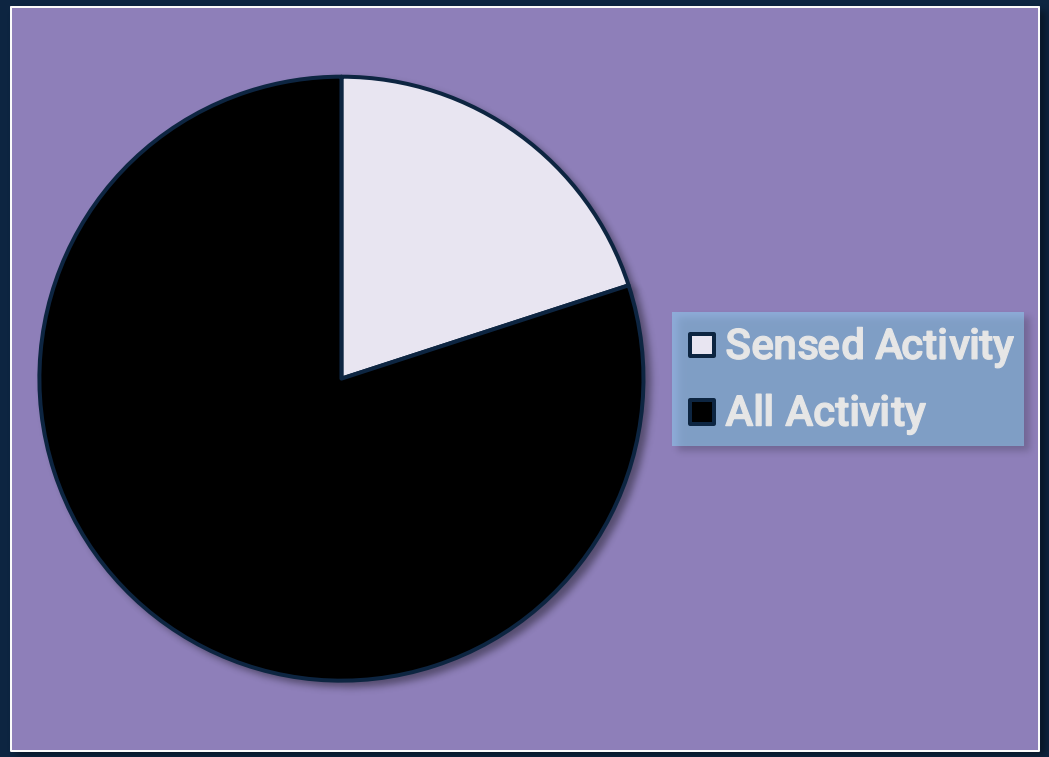
## Availability Bias

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




## Visibility Bias

Data aligned with sensors vs all activity



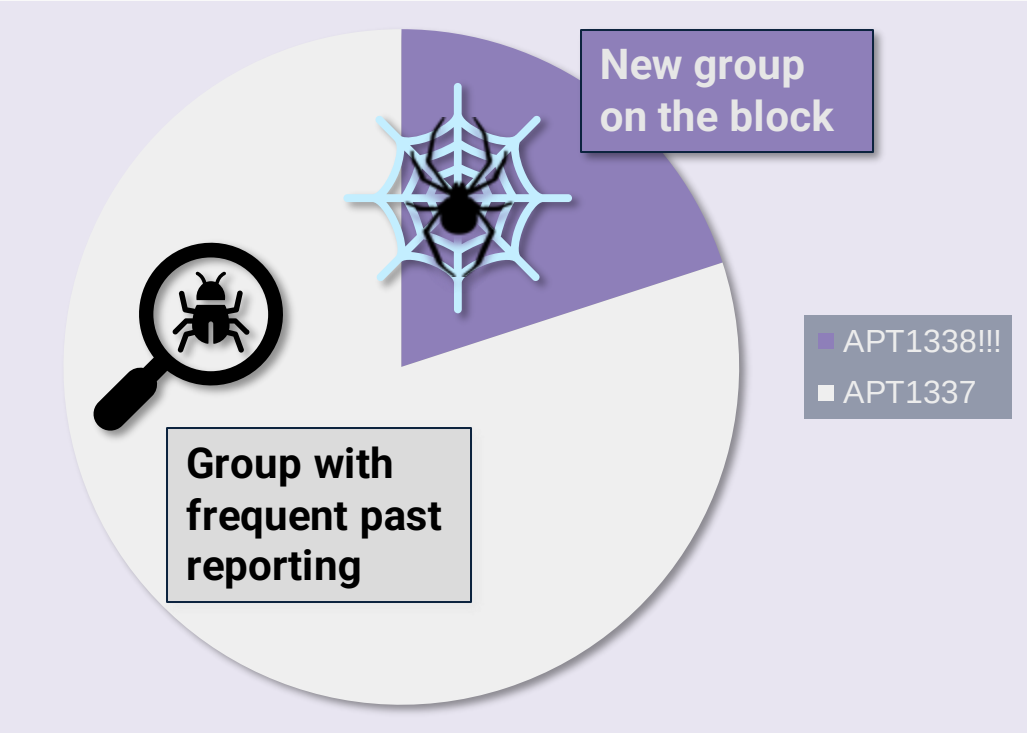
# Source Biases: Victim and Novelty

## 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

Collaborate and identify ways to mitigate biases

- Diversity of thought makes for stronger teams

02: Adjust & Calibrate

Adjust and calibrate your data sources

03: Diverse Sources

Add different data sources (including your own)

04: Prioritize the Known

Prioritize the *known* over the *unknown*

- As opposed to absolute comparison

# 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

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**