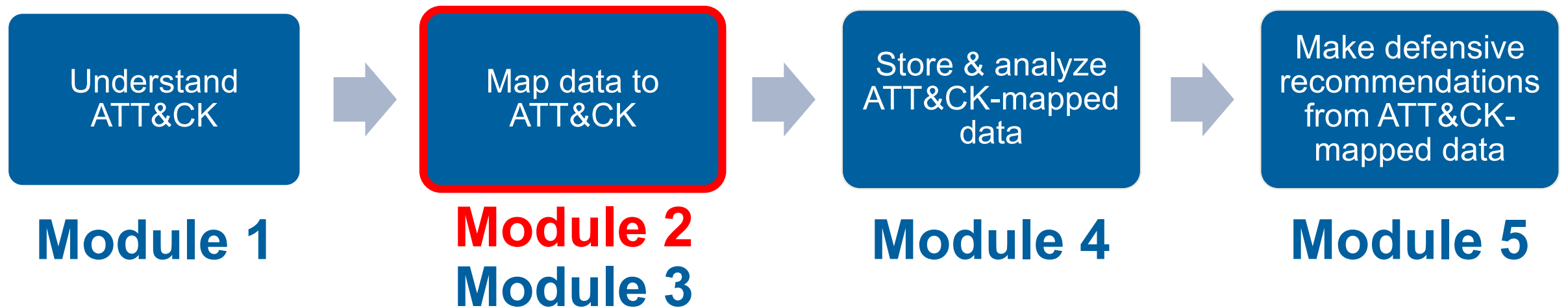

Module 2: Mapping to ATT&CK from a Finished Report

Process of Applying ATT&CK to CTI



Why is it Difficult to Map CTI to ATT&CK?

- **Requires a shift in analyst thinking**
 - Indicators → behaviors
- **Volume of ATT&CK techniques**
- **“Technical” detail of some ATT&CK techniques**

But it's worthwhile because this process...

- **Forces analysts to shift to thinking about behaviors**
- **Allows them to learn about new adversary techniques**
- **Pushes them to learn the “technical” side**

Process of Mapping to ATT&CK

0. Understand ATT&CK

1. Find the behavior

2. Research the behavior

3. Translate the behavior into a tactic

4. Figure out what technique applies to the behavior

5. Compare your results to other analysts

Two key sources for where you get information:

1. Finished reporting

2. Raw data

0. Understand ATT&CK

- **You need to know what to look for before you can do this**
- **To get analysts started:**
 - Watch an ATT&CK presentation like Sp4rkcon
 - Read the Philosophy Paper and items from our Getting Started page
 - Read the Tactic descriptions
 - *Skim* the Technique list
- **Encourage ongoing learning and discussion**
 - Have analysts present a technique a week in your team training

1. Find the Behavior

- **Different mindset from looking for indicators**
- **Look for what the adversary or software does**
- **Focus on initial compromise and post-compromise details**
 - Info that may not be useful for ATT&CK mapping:
 - Static malware analysis
 - Infrastructure registration information
 - Industry/victim targeting information

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 /ru "System" /rl "System" /dp
```

[Tactic] | 1. [Technique] [Tactic] | 2. [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

2. Research the Behavior

- **CTI analysts may not be familiar with adversary/software behavior**
- **Encourage them to do additional research:**
 - Of your own team or organization (defenders/red teamers)
 - Of external resources
- **Time-consuming, but builds better analysts**
- **Understanding of core behavior helps with next steps**

2. Research the Behavior



WIKIPEDIA
The Free Encyclopedia

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

Not logged in

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]}

<https://en.wikipedia.org/wiki/SOCKS>

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>

3. Translate the Behavior into a Tactic

- **What is the adversary trying to accomplish?**
- **Often requires domain expertise**
 - Finished intel can give you context
- **Only 12 options:**
 - Initial Access
 - Execution
 - Persistence
 - Privilege Escalation
 - Defense Evasion
 - Credential Access
 - Discovery
 - Lateral Movement
 - Collection
 - Command and Control
 - Exfiltration
 - Impact

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**

4. Figure Out What Technique Applies

- Often the toughest part
- *Not every behavior is necessarily a technique*
- Key strategies:
 1. Look at the list of Techniques for the identified Tactic
 2. Search attack.mitre.org
 - Try key words
 - Try “procedure”-level detail
 - Try specific command strings

4. Figure Out What Technique Applies

MITRE | ATT&CK™

Matrices Tactics ▾ Techniques ▾ Groups Software Resources ▾ Blog ↗ Contact

Home > Tactics > Enterprise > Command and Control

ENTERPRISE ▾

TACTICS

Command and Control

Techniques: 21

T1094	Custom Command and Control Protocol
-------	-------------------------------------

**Protocol vs.
Port**

→ 2 techniques?

T1043	Commonly Used Port
-------	--------------------

4. Figure Out What Technique Applies

“the malware first establishes a **SOCKS5 connection**”

socks|

Techniques

Term found on page
Standard Non-Application Layer
Protocol (ID: T1095)
Connection Proxy (ID: T1090)

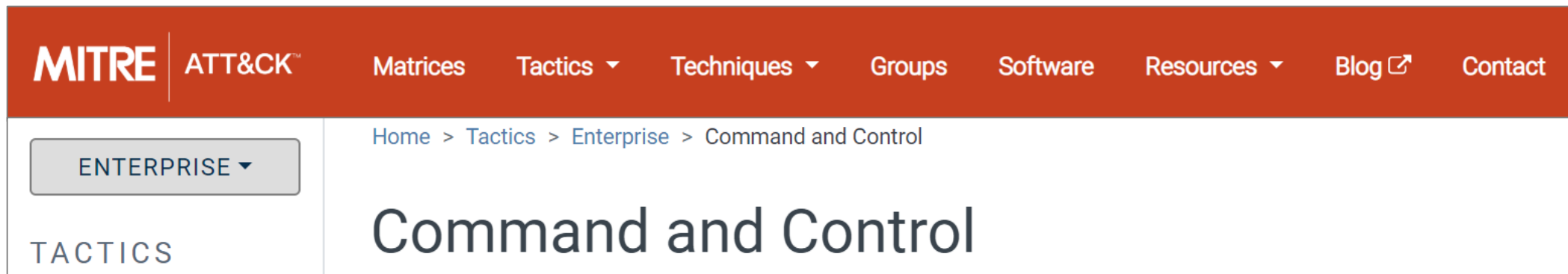
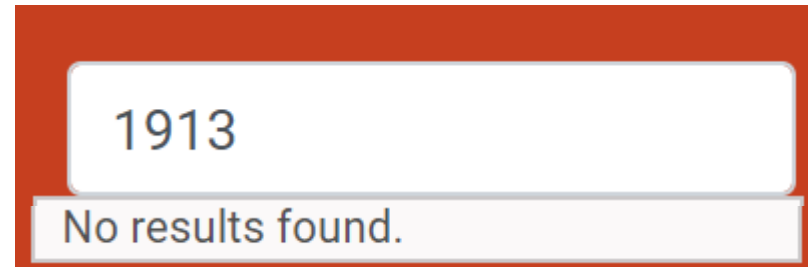
Standard Non-Application Layer Protocol

Use of a standard 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).

BUBBLEWRAP can communicate using SOCKS.^[4]

4. Figure Out What Technique Applies

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



A screenshot of the MITRE ATT&CK website. The top navigation bar includes 'MITRE ATT&CK™' and links for 'Matrices', 'Tactics', 'Techniques', 'Groups', 'Software', 'Resources', 'Blog', and 'Contact'. Below the navigation bar, a breadcrumb trail reads 'Home > Tactics > Enterprise > Command and Control'. A 'TACTICS' sidebar is visible on the left, and the main heading is 'Command and Control'.

T1043	Commonly Used Port
-------	---------------------------

T1065	Uncommonly Used Port
-------	-----------------------------

“CTRL+ F” FTW

T1205	Port Knocking
-------	----------------------

Rinse and Repeat

The most interesting PDB string is **Privilege Escalation | 3. Exploitation for Privilege Escalation (T1068)**. It is a local kernel vulnerability that, **Execution | 4. Command-Line Interface (T1059)** with successful exploitation.

The malware component, `test.exe`, uses the Windows **Discovery | 5. System Owner/User Discovery (T1033)** to verify it is running with the elevated privileges of "System" and **Persistence – | 6. Scheduled Task (T1053)** creates persistence by creating the following scheduled task:

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

Command and Control | 2. Uncommonly Used Port (T1065)

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

Exercise 2: Cybereason Cobalt Kitty Report

- **Analyze a threat report to find the Enterprise ATT&CK techniques**
 - 22 highlighted techniques in the Cybereason Cobalt Kitty report
- **Choose a PDF from attack.mitre.org/training/cti under Exercise 2**
 - Choose your own adventure: start with “highlights only” or “tactic hints”
- **Use the PDF or a text document/piece of paper to record your results**
- **Write down the ATT&CK tactic and technique you think applies to each highlight**
- **Tips:**
 - Do keyword searches of our website: <https://attack.mitre.org>
 - Remember that you don’t have to be perfect
 - Use this as a chance to dive into ATT&CK
- ***Please pause. We suggest giving yourself 30 minutes for this exercise.***

Exercise 2 Optional Bonus Step: Compare your results to other analysts

- Step 5 of the process: Compare your results to other analysts
- Helps hedge against analyst biases
 - More likely to identify techniques you've previously identified

Analyst 1

Command-Line Interface (T1059)
System Owner/User Discovery (T1033)
Scheduled Task (T1053)
Standard Non-Application Layer Protocol (T1095)
Uncommonly Used Port (T1065)
Multi-Stage Channels (T1104)

Analyst 2

Exploitation for Privilege Escalation (T1068)
Command-Line Interface (T1059)
Scheduled Task (T1053)
Custom Command and Control Protocol (T1094)
Uncommonly Used Port (T1065)



Discuss why it's different

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

Finishing Exercise 2 (Optional Bonus Step)

- **Now, compare your answers to another analyst's answers**
- **Compare what you each had for each technique answer**
 - Discuss where there are differences – why did you have different answers?
 - 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.***

Going Over the Exercise – Cybereason Report

- **Think about:**

- What were the *easiest & hardest* techniques to identify?
- How did you identify each technique?
- 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 emails** ... **link to a malicious site****

 - Initial Access - Spearphishing Link (T1192)

- 2. Two types of payloads were found in the **spear-phishing emails** ... **Word documents****

 - Initial Access - Spearphishing Attachment (T1193)

- 3. Two types of payloads were found in the **spear-phishing emails** ... **Word documents with malicious macros****

 - Defense Evasion/Execution – Scripting (T1064)

- 4. Two types of payloads were found in the **spear-phishing emails****

 - Execution – User Execution (T1204)

<https://cybr.ly/cobaltkitty>

Cybereason Cobalt Kitty Report

5. cmd.exe Parent process

- Execution - Command-Line Interface (T1059)

6. The two **scheduled tasks** are created on infected Windows

- Execution/Persistence - Scheduled Task (T1053)

7. *schtasks /create /sc MINUTE /tn "Windows Error Reporting" /tr "mshta.exe about:'<script language=\\\"vbscript\\\"...*



- Execution/Defense Evasion - Mshta (T1170)

8. That **downloads** and executes an **additional payload** from the same server

- Command and Control - Remote File Copy (T1105)

<https://cybr.ly/cobaltkitty>

Cybereason Cobalt Kitty Report

9.  powershell.exe  
Parent process

- Execution - PowerShell (T1086)

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 - Registry Run Keys / Startup Folder (T1060)

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 – New Service (T1050)
- Persistence – Modify Existing Service (T1031)

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 - Standard Application Layer Protocol (T1071)

<https://cybr.ly/cobaltkitty>

Cybereason Cobalt Kitty Report

18. :80 (*in traffic from compromised machine to C&C server*)

- Command and Control - Commonly Used Port (T1043)

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

- Command and Control - Remote File Copy (T1105)
- Execution - Regsvr32 (T1117)

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

- Defense Evasion - Masquerading (T1036)

22. 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 finished reporting to ATT&CK, work through the FireEye APT39 report in the same manner. The PDF is available at attack.mitre.org/training/cti under Exercise 2. (No tactic hints option this time!)
- Answers are provided in a separate PDF.

Skipping Steps in the Process

Once you're experienced, you maybe able to skip steps
...but this increases your bias
...and it won't work every time

0. Understand ATT&CK

1. Find the behavior

2. Research the behavior

3. Translate the behavior into a tactic

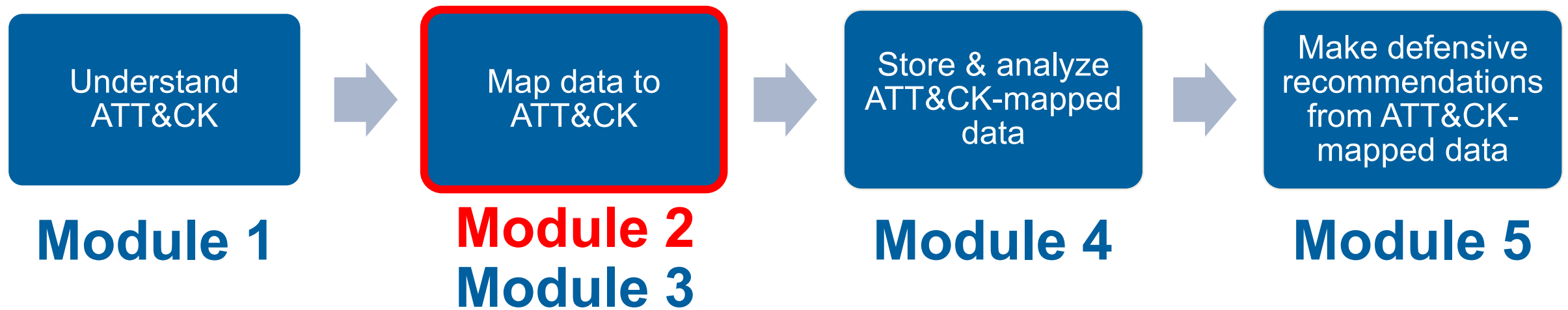
4. Figure out what technique applies to the behavior

5. Compare your results to other analysts

**Sometimes
we jump
directly here**



Process of Applying ATT&CK to CTI



End of Module 2
