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

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

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]

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

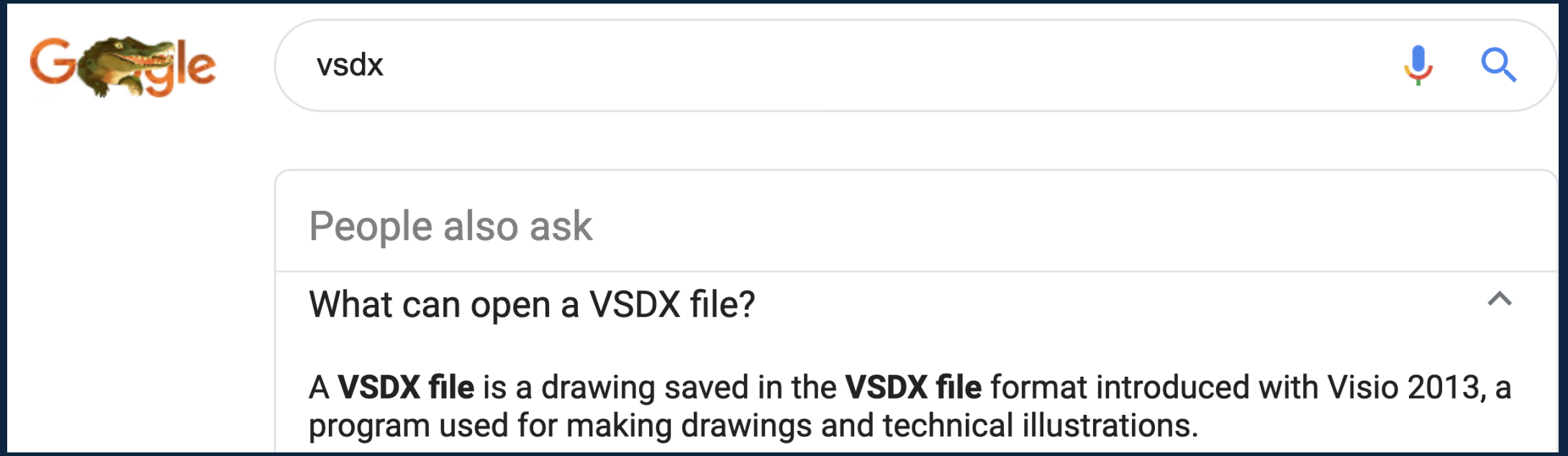
Shareware version
Type RAR -? for help

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

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

CYBRARY

3. Translate the Behavior into a Tactic

```
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

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

5. Compare Your Results to Other Analysts

- 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

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 =

Defense Evasion - Masquerading (T1036)

C2 I over https

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

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

req

UPLOAD file (upload a file server->client)

Command and Control - Ingress Tool Transfer(T1105)

DOWNLOAD

Execution - Command and Scripting Interpreter (T1059)

SHELL command (runs a command via cmd.exe)

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

PSHELL

Execution-Native API (T1106)

EXEC path given via CreateProcess)

Defense Evasion - Masquerading (T1036)

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

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

HKEY_CURRENT_USER\Soft

"C:\Windows\System32\w

Raw Data to Narrative Reporting

- 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

Completed Reporting Examples

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

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