


CS668

Module 3.3:

Mapping to ATT&CK from Raw Data



Mapping to ATT&CK from Raw Data

- So far, working from intel where activity has already been analyzed
- Analysis of techniques/behaviors directly from source data
 - Likely more information available at the procedure level
 - Not reinterpreting another analyst's prose
 - Greater knowledge/expertise required to interpret intent/tactic
- Broad set of possible data can contain behaviors
 - Shell commands, malware, forensic disk images, packets

Process of Mapping to ATT&CK



1. Understand ATT&CK
2. Find the behavior
3. Research the behavior
4. Translate the behavior into a tactic
5. Figure out what technique applies to the behavior
6. Compare your results to other analysts



1. Find the Behavior

ipconfig /all

sc.exe \\ln334656-pc create

.\recycler.exe a -hpfGzq5yKw C:\\$Recycle.Bin\old
C:\\$Recycle.Bin\Shockwave network.vsd

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

ipconfig /all



Command Prompt

```
C:\Users\Sandeep K. Shukla>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : Sandeep
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
```

Ethernet adapter vEthernet (Default Switch):

```
Connection-specific DNS Suffix . :
Description . . . . . : Hyper-V Virtual Ethernet Adapter #2
Physical Address. . . . . : 00-15-5D-78-8E-40
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::e8c0:71b3:d85c:e00f%32(Preferred)
IPv4 Address. . . . . : 172.29.96.1(Preferred)
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 536876381
DHCPv6 Client DUID. . . . . : 00-01-00-01-29-02-06-5B-0C-37-96-33-D9-CF
NetBIOS over Tcpip. . . . . : Enabled
```

Ethernet adapter vEthernet (Wi-Fi):

```
Connection-specific DNS Suffix . :
Description . . . . . : Hyper-V Virtual Ethernet Adapter #6
```

Command sc query



```
Command Prompt

this case. If the query command is followed by nothing or one of
the options listed below, the services are enumerated.
type=   Type of services to enumerate (driver, service, userservice, all)
        (default = service)
state=  State of services to enumerate (inactive, all)
        (default = active)
bufsize= The size (in bytes) of the enumeration buffer
         (default = 4096)
ri=     The resume index number at which to begin the enumeration
        (default = 0)
group=  Service group to enumerate
        (default = all groups)

SYNTAX EXAMPLES
sc query           - Enumerates status for active services & drivers
sc query eventlog  - Displays status for the eventlog service
sc queryex eventlog - Displays extended status for the eventlog service
sc query type= driver - Enumerates only active drivers
sc query type= service - Enumerates only Win32 services
sc query state= all - Enumerates all services & drivers
sc query bufsize= 50 - Enumerates with a 50 byte buffer
sc query ri= 14 - Enumerates with resume index = 14
sc queryex group= "" - Enumerates active services not in a group
sc query type= interact - Enumerates all interactive services
sc query type= driver group= NDIS - Enumerates all NDIS drivers

C:\Users\Sandeep K. Shukla>
```

Command `sc <server> create`



Command Prompt

```
Link-local IPv6 Address . . . . . : fe80::45c7:c497:df6:8f71%61
IPv4 Address. . . . . : 172.20.64.1
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . :
```

```
C:\Users\Sandeep K. Shukla>sc \\SANDEEP create
```

DESCRIPTION:

Creates a service entry in the registry and Service Database.

USAGE:

```
sc <server> create [service name] [binPath= ] <option1> <option2>...
```

OPTIONS:

NOTE: The option name includes the equal sign.

A space is required between the equal sign and the value.

```
type= <own|share|interact|kernel|filesys|rec|userown|usershare>
      (default = own)
```

```
start= <boot|system|auto|demand|disabled|delayed-auto>
      (default = demand)
```

```
error= <normal|severe|critical|ignore>
      (default = normal)
```

```
binPath= <BinaryPathName to the .exe file>
```

```
group= <LoadOrderGroup>
```

```
tag= <yes|no>
```

```
depend= <Dependencies(separated by / (forward slash))>
```

```
obj= <AccountName|ObjectName>
     (default = LocalSystem)
```

```
DisplayName= <display name>
```

```
password= <password>
```

```
C:\Users\Sandeep K. Shukla>
```

2. Research the Behavior



- **Can be similar to analysis of finished reporting for raw data**
- **May require expertise in the specific data type**
 - Network, forensics, malware, Windows cmd line, etc
- **May require multiple data sources, more context**
 - 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: <code>ipconfig /all >> %temp%\download</code> ^[1]

2. Research the Behavior

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

- Can make some educated guesses, but not enough context

File analysis:

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

```
C:\recycler.exe
```

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

```
Roshal Shareware versionType RAR -? for
```

```
help
```

- Aha! 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
```



vsd^x



People also ask


What can open a VSDX file?

A **VSDX file** is a drawing saved in the **VSDX file** format introduced with Visio 2013, a program used for making drawings and technical illustrations.

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

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.vsd
```

- 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 Applies

- Similar to working with finished reporting we may jump straight here

- Procedure may map directly to Technique/Tactic
- May have enough experience to compress steps

`ipconfig /all`

- Specific procedure in **System Network Configuration Discovery (T1016)**
- Also **Command-Line Interface (T1059)**

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

- We figured out researching this that “a -hp” compresses/encrypts
- Appears to be **Data Compressed (T1002)** and **Data Encrypted (T1022)**
- Also **Command-Line Interface (T1059)**

4. Concurrent Techniques



- Don't just think of what's happening – think of *how* it's happening
- Certain tactics commonly have concurrent techniques:
 - Execution
 - Defense Evasion
 - Collection
- Examples:
 - Data Compressed + Data Encrypted (2x Exfiltration)
 - Spearphishing Attachment + User Execution (Initial Access + Execution)
 - Data from Local System + Email Collection (2x Collection)
 - Process Discovery + Command-Line Interface (Discovery + Execution)



4. Different Types of Techniques

- **Not all techniques are created equal!**
 - Credit to Red Canary: <https://www.redcanary.com/blog/avoiding-common-attack-pitfalls/>
- **Some are specific**
 - Rundll32
 - Netsh Helper DLL
- **Some are broad**
 - Scripting
 - Obfuscated Files or Information
- **Some capture “how” the behavior occurs**
 - Masquerading
 - Data Transfer Size Limits
 - Automated Collection



5. Compare Your Results to Other Analysts

- Same caveats about hedging biases
- May need a broader set of skills/experience to work with types of data

Analyst 1

- Packets
- Malware/Reversing
- Windows command line

Analyst 2

- Windows Events
- Disk forensics
- macOS/Linux

Pros/cons of Mapping from the Two Different Sources

Step	Raw	Finished
Find the behavior	Nearly everything may be a behavior (not all ATT&CK)	May be buried amongst prose, IOCs, etc
Research the behavior	May need to look at multiple sources, data types. May also be a known procedure	May have more info/context, may also have lost detail in writing
Translate the behavior into a tactic	Have to map to adversary intent, need domain knowledge/expertise	Often intent has been postulated by report author
Figure out what technique applies to the behavior	May have a procedure that maps straight to technique, or may require deep understanding to understand how accomplished	May be as simple as a text match to description/procedure, or may be too vague to tell
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

Exercise 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
- Both tickets are at <https://attack.mitre.org/training/cti> under Exercise 3
- 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 Questions



- What questions would you have asked of your incident responders?
- What was easier/harder than working with finished 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 the Exercise (Ticket 473822)



`ipconfig /all` System Network Configuration Discovery (T1016)
`arp -a` System Network Configuration Discovery (T1016)
`echo %USERDOMAIN%\%USERNAME%` System Owner / User Discovery (T1033)
`tasklist /v` Process Discovery (T1057)
`sc query` System Service Discovery (T1007)
`systeminfo` System Information Discovery (T1082)
`net group "Domain Admins" /domain` Permission Groups Discovery (T1069)
`net user /domain` Account Discovery (T1087)
`net group "Domain Controllers" /domain` Remote System Discovery (T1018)
`netsh advfirewall show all` System Network Configuration Discovery (T1016)
`netstat -ano` System Network Connections Discovery (T1049)

Discovery

Going Over Exercise 3 (Ticket 473845)

Command and Control - Data Encoding (T1132)

C2 protocol is base64

30 seconds requesting a command

Command and Control - Standard Application Layer Protocol (T1071)

UPLOAD file (upload a file server->client)

DOWNLOAD file (download a

Command and Control - Remote File Copy (T1105)

SHELL command (runs a command

Execution - Command-Line Interface (T1059)

PSHELL command (runs a command via powershell

Execution - Powershell (T1086)

EXEC path (executes a PE at the

Execution - Execution through API (T1106)

SLEEP n (skips n beacons)

10.1.1.1:24123 -> 129.83.44.12:443

129.83.44.12:443 -> 10.1.1.1:24123

Command and Control - Commonly Used Port (T1043)

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

Defense Evasion - Masquerading (T1036)

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\winpool

REG_SZ "C:\Windows\System32\winpool.exe"

Persistence - Registry Run Keys (T1060)

From Raw Data to Finished Reporting with ATT&CK



- We've talked about augmenting reports with ATT&CK and analyzing data with ATT&CK, possibly in parallel with analysis for 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
 - Allows much easier capture of how a technique was done

Finished Reporting Examples

During operation Tangerine Yellow, the actors used Pineapple RAT to execute 'ipconfig /all¹' via the Windows command shell².

1. Discovery – System Network Configuration Discovery (T1016)

2. Execution – Command-Line Interface (T1059)

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

instead of

Appendix C – ATT&CK Techniques

- System Network Configuration Discovery
- Command-Line Interface
- Hardware Additions

End of Module 3.3

