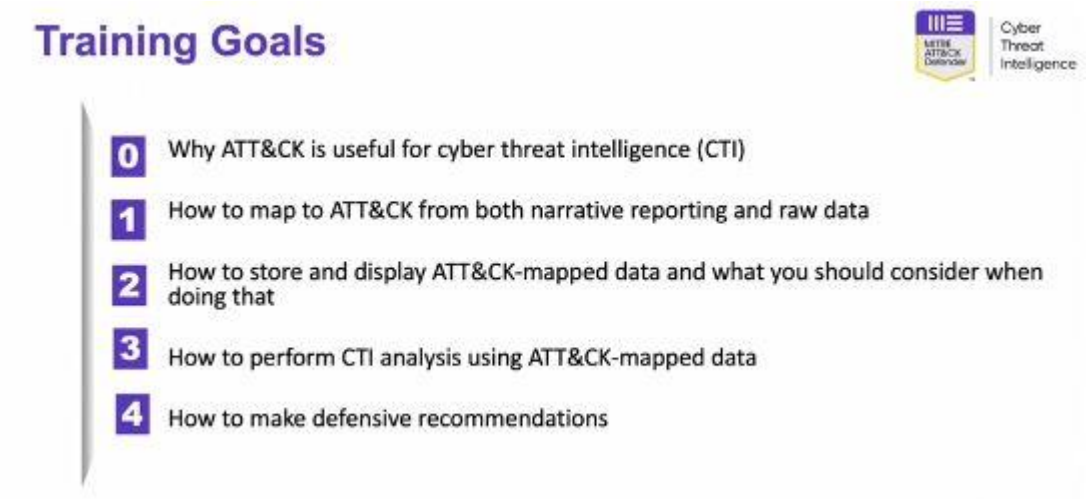
MITRE ATT&CK Defender: Introduction to ATT&CK for CTI

LESSON 1 Introduction to ATT&CK for Cyber Threat Intelligence:

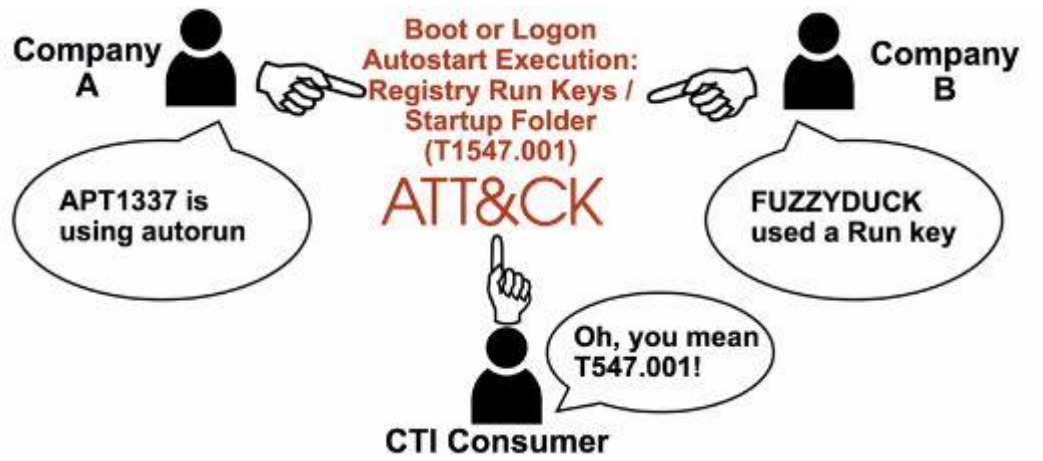
Objectives:



Important References for Analysis of ATTACKS:

- **MITRE ATT&CK -** https://attack.mitre.org/matrices/enterprise/
- **MITRE Engage -** https://engage.mitre.org/matrix/
- **MITRE Cyber Analytics Repository -** https://car.mitre.org/analytics/
- **MITRE Engenuity -** https://mitre-engenuity.org/attackevaluations/
- **CTID MITRE Engenuity -** https://ctid.mitre-engenuity.org/
- **Adversary Emulation Plans -** https://attack.mitre.org/resources/adversary-emulation-plans/
- **MITRE ATT&CK Data Sources -** https://github.com/mitre-attack/attack-datasources
- **MITRE CTI -** https://github.com/mitre/cti
- **ATT&CK Navigator-** https://mitre-attack.github.io/attack-navigator/

Example of how threat mapping is done using ATT&CK-



LESSON 2 Map Narrative & Raw Data to ATT&CK:

Example1-

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] | 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 "05 00".

- "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**

Behaviour Analysis using ATT&CK -

"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~~

The most interesting PD[Privilege Escalation | 3. Exploitation for Privilege Escalation (T1068)]3. 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 witl 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"
```

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".

The most interesting PDB string is the "4113.pdb," which appears to reference CVE-2014-4113. This CVE is a local kernel vul[Execution | 4. Command and Scripting Interpreter: Windows Command Shell (T1059.003)]achine.

The malware component, test.exe, uses t[Discovery | 5. System Owner/User Discovery (T1033)]y 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"
```

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".

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 Persistence – | 6. Scheduled Task/Job: Scheduled Task (T1053.005)

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

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".

Excersise 1-

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)
5. cmd.exe
   Parent process
   - 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)

https://cybr.ly/cobaltkitty
CYBRARY

9. powershell.exe
   Parent process
   - 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)

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)

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)

Example 2-

```
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

Behaviour Analysis using ATT&CK-

```
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

```
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)

Excersise 2-

(A)

```
ipconfig /all
arp -a
echo %USERDOMAIN%\%USERNAME%
tasklist /v
sc query
systeminfo
net group "Domain Admins" /domain
net user /domain
net group "Domain Controllers" /domain
netsh advfirewall show allprofiles
netstat -ano
```

ATT&CK mapped data-

```
ipconfig /al   System Network Configuration Discovery (T1016)
arp -a         System Network Configuration Discovery (T1016)
echo %USERDOMAIN System Owner / User Discovery (T1033)
tasklist /v    Process Discovery (T1057)
sc query       System Service Discovery (T1007)
systeminf      System Information Discovery (T1082)
net group "    Permission Groups Discovery: Domain Groups (T1069.002)
net user /domai Account Discovery: Domain Account (T1087.002)
net group "Domain Controllers" / Remote System Discovery (T1018)
netsh advfirewall show         System Network Configuration Discovery (T1016)
netstat -an    System Network Connections Discovery (T1049)
```

(B)

```
Filename = winspool.exe
C2 protocol is base64 encoded commands over https. The RAT beacons every 30 seconds
requesting a command.
    UPLOAD file (upload a file server->client)
        DOWNLOAD file (download a file client->server)
        SHELL command (runs a command via cmd.exe)
        PSHELL command (runs a command via powershell.exe)
        EXEC path (executes a PE at the path given via CreateProcess)

Copy C:\winspool.exe -> C:\Windows\System32\winspool.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\winspool REG_SZ
"C:\Windows\System32\winspool.exe"
```

ATT&CK mapped data -

```
Filename = winspool
C2 p
req
    UPLOAD file (upload a file server->client)
        DOWNLOAD fi
        SHELL co
        PSHELL
        EXEC path
Copy C:\winspool.exe
HKEY_CURRENT_USER\Sof
"C:\Windows\System32\w
```

Defense Evasion - Masquerading (T1036)

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

over https

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

Command and Control Command and Control - Ingress Tool Transfer(T1105)

Execution - Command and Scripting Interpreter (T1059)

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

Execution-Native API (T1106)

given via CreateProcess)

Defense Evasion - Masquerading (T1036)

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

LESSON 3 Store & Analyze ATT&CK-mapped data:

Expressing and Storing ATT&CK-Mapped Data

Cyber Threat Intelligence

Event Triggered Execution: Component Object Model Hijacking	APT28 has used COM hijacking for persistence by replacing the legitimate `MMDeviceEnumerator` object with a payload.[23][11]

https://attack.mitre.org/groups/G0007/

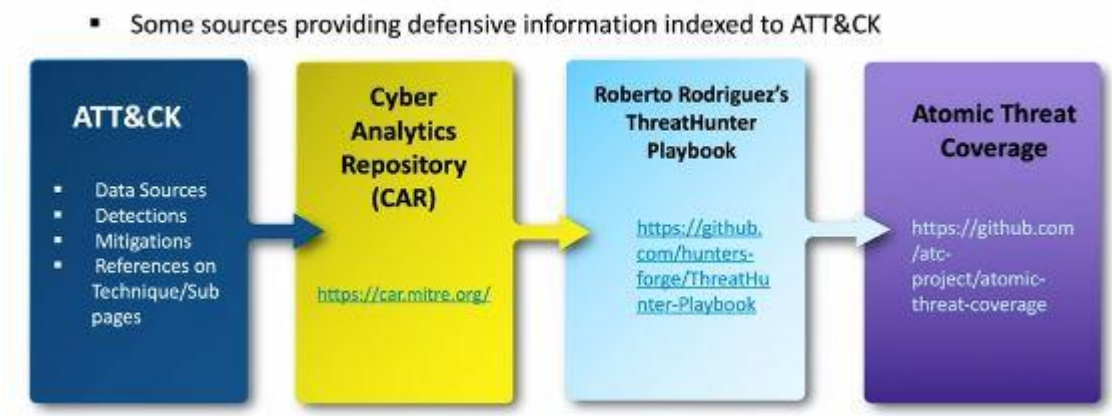
Full-Text Report

APT15 was also observed using Mimikatz to dump credentials and generate Kerberos golden tickets. This allowed the group to persist in the victim's network in the event of

ATT&CK Technique

OS Credential Dumping (T1003)

LESSON 4 Make Defensive Recommendations from ATT&CK-mapped data:



In short MITRE ATT&CK helps us analyse questions such as what risks are most critical to address?, what risks can be tolerated?, as well as help us understand importance of informed decisions, assessments using threats will lead us towards necessary enhancements.

I hope this is helpful in getting Introduction to MITRE ATT&CK for CTI perspective.

-By Shefali Kumari