Module 1: Introducing the Training and Understanding ATT&CK
Using MITRE ATT&CK™ for Cyber Threat Intelligence Training

Katie Nickels and Adam Pennington
Training Overview

- Five modules consisting of YouTube videos and exercises are available at attack.mitre.org/training/cti
- Module 1: Introducing training and understanding ATT&CK
  A. Topic introduction (Video)
- Module 2: Mapping to ATT&CK from finished reporting
  A. Topic introduction (Video)
  B. Exercise 2: Mapping to ATT&CK from finished reporting (Do it yourself with materials on attack.mitre.org/training/cti)
  C. Going over Exercise 2 (Video)
- Module 3: Mapping to ATT&CK from raw data
  A. Topic introduction (Video)
  B. Exercise 3: Mapping to ATT&CK from raw data (Do it yourself with materials on attack.mitre.org/training/cti)
  C. Going over Exercise 3 (Video)
Training Overview

- **Module 4: Storing and analyzing ATT&CK-mapped intel**
  A. Topic introduction (Video)
  B. Exercise 4: Comparing layers in ATT&CK Navigator
     (Do it yourself with materials on attack.mitre.org/training/cti)
  C. Going over Exercise 4 (Video)

- **Module 5: Making ATT&CK-mapped data actionable with defensive recommendations**
  A. Topic introduction (Video)
  B. Exercise 5: Making defensive recommendations
     (Do it yourself with materials on attack.mitre.org/training/cti)
  C. Going over Exercise 5 and wrap-up (Video)
Process of Applying ATT&CK to CTI

Module 1: Understand ATT&CK
Module 2: Map data to ATT&CK
Module 3: Map data to ATT&CK
Module 4: Store & analyze ATT&CK-mapped data
Module 5: Make defensive recommendations from ATT&CK-mapped data
Introduction to ATT&CK and Applying it to CTI
Tough Questions for Defenders

- How effective are my defenses?
- Do I have a chance at detecting APT29?
- Is the data I’m collecting useful?
- Do I have overlapping tool coverage?
- Will this new product help my organization’s defenses?
What is ATT&CK?

A knowledge base of adversary behavior

➢ Based on real-world observations
➢ Free, open, and globally accessible
➢ A common language
➢ Community-driven
The Difficult Task of Detecting TTPs

David Bianco’s Pyramid of Pain

Breaking Down ATT&CK

Tactics: the adversary’s technical goals

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Command and Control</th>
<th>Exfiltration</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive-by Compromise</td>
<td>Scheduled Task</td>
<td>Binary Padding</td>
<td>Network Sniffing</td>
<td>Application</td>
<td>Application</td>
<td>Attack</td>
<td>Data Exfiltration</td>
<td>Attack</td>
<td>Automated Exfiltration</td>
<td>Data Destruction</td>
<td></td>
</tr>
</tbody>
</table>

**Procedures: Specific technique implementation**

**Spearphishing Attachment Procedure Examples**

**Name** | **Description**
--- | ---
**APT12** | APT12 has sent emails with malicious Microsoft Office documents and PDFs attached. [88][89]
**APT19** | APT19 has sent spearphishing emails with malicious attachments in RTF and XLSM formats to deliver initial exploits. [92]

**Techniques:** how the goals are achieved

Technique: Spearphishing Attachment

Spearphishing Attachment

Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution.

There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary’s payload exploits a vulnerability or directly executes on the user’s system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.
Technique: Spearphishing Attachment

ID: T1193

Tactic: Initial Access

Platform: Windows, macOS, Linux

Data Sources: File monitoring, Packet capture, Network intrusion detection system, Detonation chamber, Email gateway, Mail server

CAPEC ID: CAPEC-163

Version: 1.0
Technique: Spearphishing Attachment

Mitigations

<table>
<thead>
<tr>
<th>Mitigation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus/Antimalware</td>
<td>Anti-virus can also automatically quarantine suspicious files.</td>
</tr>
<tr>
<td>Network Intrusion Prevention</td>
<td>Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity.</td>
</tr>
<tr>
<td>Restrict Web-Based Content</td>
<td>Block unknown or unused attachments by default that should not be transmitted over email as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some email scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious attachments in Obfuscated Files or Information.</td>
</tr>
<tr>
<td>User Training</td>
<td>Users can be trained to identify social engineering techniques and spearphishing emails.</td>
</tr>
</tbody>
</table>

Detection

Network intrusion detection systems and email gateways can be used to detect spearphishing with malicious attachments in transit. Detonation chambers may also be used to identify malicious attachments. Solutions can be signature and behavior based, but adversaries may construct attachments in a way to avoid these systems.
**Technique: Spearphishing Attachment**

**Procedure Examples**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APT12</td>
<td>APT12 has sent emails with malicious Microsoft Office documents and PDFs attached. [88][89]</td>
</tr>
<tr>
<td>APT19</td>
<td>APT19 sent spearphishing emails with malicious attachments in RTF and XLSM formats to deliver initial exploits. [62]</td>
</tr>
<tr>
<td>APT28</td>
<td>APT28 sent spearphishing emails containing malicious Microsoft Office attachments. [22][23][24][25][26][27]</td>
</tr>
</tbody>
</table>

**References**


Group: APT29

APT29 is a threat group that has been attributed to the Russian government and has operated since at least 2008. [1] [2] This group reportedly compromised the Democratic National Committee starting in the summer of 2015. [3]

ID: G0016

Associated Groups: YTTRIUM, The Dukes, Cozy Bear, CozyDuke

Version: 1.2
## Group: APT29

### Associated Group Descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>YTTRIUM</td>
<td>[10]</td>
</tr>
<tr>
<td>The Dukes</td>
<td>[1]</td>
</tr>
</tbody>
</table>

### Techniques Used

<table>
<thead>
<tr>
<th>Domain</th>
<th>ID</th>
<th>Name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>T1015</td>
<td>Accessibility Features</td>
<td>APT29 used sticky-keys to obtain unauthenticated, privileged console access. [4] [6]</td>
</tr>
<tr>
<td>Enterprise</td>
<td>T1088</td>
<td>Bypass User Account Control</td>
<td>APT29 has bypassed UAC. [4]</td>
</tr>
</tbody>
</table>
Group: APT29

Software

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>References</th>
<th>Techniques</th>
</tr>
</thead>
</table>

References

ATT&CK Use Cases

Detection

processes = search Process:Create
reg = filter processes where (exe == "reg.exe" and parent_exe == "cmd.exe")
cmd = filter processes where (exe == "cmd.exe" and parent_exe != "explorer.exe")
reg_and_cmd = join (reg, cmd) where (reg.ppid == cmd.pid and reg.hostname == cmd.hostname)
output reg_and_cmd

Assessment and Engineering

Adversary Emulation

Finding Gaps in Defense

Comparing APT28 to APT29

Legend

- APT28
- APT29
- Both

ATT&CK and CTI
Threat Intelligence – How ATT&CK Can Help

▪ Use knowledge of adversary behaviors to inform defenders

▪ Structuring threat intelligence with ATT&CK allows us to…
  – Com\textit{pare} behaviors
    ▪ Groups to each other
    ▪ Groups over time
    ▪ Groups to defenses
  – Comm\textit{unicate} in a common language
Communicate to Defenders

THIS is what the adversary is doing!
The Run key is AdobeUpdater.

Registry Run Keys / Startup Folder (T1060)

Oh, we have Registry data, we can detect that!

ATT&CK

CTI Analyst

Defender
Communicate Across the Community

Company A

APT1337 is using autorun

Company B

FUZZYDUCK used a Run key

CTI Consumer

Oh, you mean T1060!

Registry Run Keys / Startup Folder (T1060)
Process of Applying ATT&CK to CTI

Module 1
Understand ATT&CK

Module 2
Map data to ATT&CK

Module 3
Store & analyze ATT&CK-mapped data

Module 4
Make defensive recommendations from ATT&CK-mapped data

Module 5

End of Module 1