ADVERSARY TRADECRAFT & PUBLIC SAFETY

Making Threat Intelligence More Effective With MITRE ATT&CK

TRAVIS RANDALL
THREAT INTELLIGENCE ANALYST
MOTOROLA SOLUTIONS, INC.
FIRST Responders & CRITICAL INFRASTRUCTURE

- Police
- Fire
- Emergency Medical
- National Security
- Critical Infrastructure

~75%

ENTERPRISES, LOCAL BUSINESSES, & MORE

- Utilities
- Mining, Oil & Gas
- Education
- Manufacturing
- Hospitality & Retail
- Transportation & Logistics

~25%

WHO WE SERVE
WHO WE SERVE (CONT.)
OUR MISSION

Investigate and report how public safety is being targeted

Identify critical vulnerabilities to emergency service systems and technologies

Guide secure design decisions in public safety products and services MSI provides
EXTERNAL PRODUCTS

2021 CYBER THREATS TO PUBLIC SAFETY
CRIMINAL OPERATIONS FOCUS

Insights from the Motorola Solutions Threat Intelligence Team - Second in a Series

HOW AND WHY CRIMINAL FORUMS “BANNED” RANSOMWARE

We are agnostic, we do not participate in geopolitics, do not need to tie us with a defined government and look for other sources.
Our goal is to make money, and not create.
From today we introduce moderation and our partners want to encrypt to avoid social control.

Figure F: Bandits attract victims based on their online reputation.

EXTORTION GROUPS REBRAND, IN MORE WAYS THAN ONE

The Extortion Forum and following attacks have resulted in rapid multiplication of criminal forums operating across the globe. In 2021, we have seen many examples of criminal forums that include the “Extortion Forum”.

Figure G: Extortion Forum.

In addition to rebranding, the Extortion Forum has been actively promoting its capabilities to attract new members.

Figure H: Extortion Forum.

Although there have been increased efforts to shutdown the forum, the Extortion Forum has continued to operate with limited success.

Figure I: Extortion Forum.

The forum has continued to attract new members, albeit with reduced success compared to its peak activity in 2021.

Figure J: Extortion Forum.

In conclusion, the Extortion Forum continues to operate, albeit with reduced success compared to its peak activity in 2021. The forum has continued to attract new members, albeit with reduced success compared to its peak activity in 2021.

Figure K: Extortion Forum.

In conclusion, the Extortion Forum continues to operate, albeit with reduced success compared to its peak activity in 2021. The forum has continued to attract new members, albeit with reduced success compared to its peak activity in 2021.

Figure L: Extortion Forum.

In conclusion, the Extortion Forum continues to operate, albeit with reduced success compared to its peak activity in 2021. The forum has continued to attract new members, albeit with reduced success compared to its peak activity in 2021.

Figure M: Extortion Forum.

In conclusion, the Extortion Forum continues to operate, albeit with reduced success compared to its peak activity in 2021. The forum has continued to attract new members, albeit with reduced success compared to its peak activity in 2021.

Figure N: Extortion Forum.
WHERE DOES TRADECRAFT COME IN?
WHY IS KNOWING TRADECRAFT IMPORTANT?

- Allows for pre-determined plans
  - Playbooks
- Identifies attack bottlenecks
  - Product-level defenses
- Teaches us what to look for
  - Alert prioritization
- Validates defenses
  - Purple-teaming
WHO IS THE MITRE CORPORATION?

- Non-profit
- Federally-funded
- Researches threats
WHAT IS ATT&CK?

Reconnaissance
- Active Scanning
- Gutter Victim Host Information
- Gutter Victim Identity Information
- Gutter Victim Network Information
- Gutter Victim Org Information
- Whisking for Information
- Search Closed Sources
- Search Open Technical Databases
- Search Open Websites/Command
- Search Victim-Owned Websites

Resource Development
- Execute Infrastructure
- Compromise Account
- Compromise Compromise
- Compromise Network
- Develop Capabilities
- Establish Account
- Obtain Capabilities
- Use Capabilities

Initial Access
- Drive-by Compromise
- Exploit Public-Facing Application
- Internally Facing Services
- Hardware Additions
- Intrusion
- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution
- Command and Scripting Interpreter
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication
- Native API
- Scheduled Tasks

Deliver
- Exploiting the Victim
- Delivering a customized bundle to the victim via email, web, USB, etc.

Exploitation
- Exploiting a vulnerability to execute code on victim’s system

Installation
- Installing malware on the asset

WEAPORIZATION
- Coupling exploits with backdoor into deliverable payload

EXTRICATION
- Command and Control
- Command Channel
- Transfer Data to Cloud Account

Commands
- Application Layer Protocol
- Data Transfer Size Limit
- Exfiltration Over Alternate Transport Protocols
- Exfiltration Over C2 Channel
- Task Scheduler
- Exfiltration Over Other Network Medium
- Exfiltration Of Physical Media
- Exfiltration Over Other Media
- Exfiltration Of C2

Impact
- Account Access Removal
- Data Deletion
- Data Encrypted
- Data Manipulation
- Data Gathering
- Data Manipulation
- Data Exfiltration
- Data Impersonation
- Data Destruction
- Data Exfiltration
- Data Exfiltration

Actions On Objectives
- With “hands on keyboard” access, intruders accomplish their original goals

1. Reconnaissance
   - Harvesting email addresses, conference information, etc.
2. Weaponization
   - Coupling exploits with backdoor into deliverable payload
3. Delivery
   - Delivering a customized bundle to the victim via email, web, USB, etc.
4. Exploitation
   - Exploiting a vulnerability to execute code on victim’s system
5. Installation
   - Installing malware on the asset
6. Command & Control (C2)
   - Command channel for remote manipulation of victim

Motorola Solutions
### WHAT IS ATT&CK? (CONT.)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>10 techniques</td>
<td>7 techniques</td>
<td>9 techniques</td>
<td>12 techniques</td>
<td>10 techniques</td>
<td>18 techniques</td>
<td>9 techniques</td>
<td>19 techniques</td>
<td>40 techniques</td>
<td>29 techniques</td>
<td>9 techniques</td>
<td>17 techniques</td>
<td>9 techniques</td>
<td>13 techniques</td>
</tr>
<tr>
<td>Active Scanning (&lt;sup&gt;23&lt;/sup&gt;)</td>
<td>Gather Victim Host Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Gather Victim Identity Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Gather Victim Network Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Whisking for Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Closed Sources (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Open Technical Databases (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Open Network/Domain (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Victim-Owned Websites (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Reconnaissance (&lt;sup&gt;10&lt;/sup&gt;)</td>
<td>Resource Development (&lt;sup&gt;7&lt;/sup&gt;)</td>
<td>Initial Access (&lt;sup&gt;9&lt;/sup&gt;)</td>
<td>Execution (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Persistence (&lt;sup&gt;10&lt;/sup&gt;)</td>
</tr>
<tr>
<td>Active Scanning (&lt;sup&gt;23&lt;/sup&gt;)</td>
<td>Gather Victim Host Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Gather Victim Identity Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Gather Victim Network Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Whisking for Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Closed Sources (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Open Technical Databases (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Open Network/Domain (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Victim-Owned Websites (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Reconnaissance (&lt;sup&gt;10&lt;/sup&gt;)</td>
<td>Resource Development (&lt;sup&gt;7&lt;/sup&gt;)</td>
<td>Initial Access (&lt;sup&gt;9&lt;/sup&gt;)</td>
<td>Execution (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Persistence (&lt;sup&gt;10&lt;/sup&gt;)</td>
</tr>
<tr>
<td>Active Scanning (&lt;sup&gt;23&lt;/sup&gt;)</td>
<td>Gather Victim Host Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Gather Victim Identity Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Gather Victim Network Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Whisking for Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Closed Sources (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Open Technical Databases (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Open Network/Domain (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Victim-Owned Websites (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Reconnaissance (&lt;sup&gt;10&lt;/sup&gt;)</td>
<td>Resource Development (&lt;sup&gt;7&lt;/sup&gt;)</td>
<td>Initial Access (&lt;sup&gt;9&lt;/sup&gt;)</td>
<td>Execution (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Persistence (&lt;sup&gt;10&lt;/sup&gt;)</td>
</tr>
<tr>
<td>Active Scanning (&lt;sup&gt;23&lt;/sup&gt;)</td>
<td>Gather Victim Host Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Gather Victim Identity Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Gather Victim Network Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Whisking for Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Closed Sources (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Open Technical Databases (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Open Network/Domain (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Victim-Owned Websites (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Reconnaissance (&lt;sup&gt;10&lt;/sup&gt;)</td>
<td>Resource Development (&lt;sup&gt;7&lt;/sup&gt;)</td>
<td>Initial Access (&lt;sup&gt;9&lt;/sup&gt;)</td>
<td>Execution (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Persistence (&lt;sup&gt;10&lt;/sup&gt;)</td>
</tr>
<tr>
<td>Active Scanning (&lt;sup&gt;23&lt;/sup&gt;)</td>
<td>Gather Victim Host Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Gather Victim Identity Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Gather Victim Network Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Whisking for Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Closed Sources (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Open Technical Databases (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Open Network/Domain (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Victim-Owned Websites (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Reconnaissance (&lt;sup&gt;10&lt;/sup&gt;)</td>
<td>Resource Development (&lt;sup&gt;7&lt;/sup&gt;)</td>
<td>Initial Access (&lt;sup&gt;9&lt;/sup&gt;)</td>
<td>Execution (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Persistence (&lt;sup&gt;10&lt;/sup&gt;)</td>
</tr>
<tr>
<td>Active Scanning (&lt;sup&gt;23&lt;/sup&gt;)</td>
<td>Gather Victim Host Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Gather Victim Identity Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Gather Victim Network Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Whisking for Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Closed Sources (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Open Technical Databases (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Open Network/Domain (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Victim-Owned Websites (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Reconnaissance (&lt;sup&gt;10&lt;/sup&gt;)</td>
<td>Resource Development (&lt;sup&gt;7&lt;/sup&gt;)</td>
<td>Initial Access (&lt;sup&gt;9&lt;/sup&gt;)</td>
<td>Execution (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Persistence (&lt;sup&gt;10&lt;/sup&gt;)</td>
</tr>
<tr>
<td>Active Scanning (&lt;sup&gt;23&lt;/sup&gt;)</td>
<td>Gather Victim Host Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Gather Victim Identity Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Gather Victim Network Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Whisking for Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Closed Sources (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Open Technical Databases (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Open Network/Domain (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Victim-Owned Websites (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Reconnaissance (&lt;sup&gt;10&lt;/sup&gt;)</td>
<td>Resource Development (&lt;sup&gt;7&lt;/sup&gt;)</td>
<td>Initial Access (&lt;sup&gt;9&lt;/sup&gt;)</td>
<td>Execution (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Persistence (&lt;sup&gt;10&lt;/sup&gt;)</td>
</tr>
<tr>
<td>Active Scanning (&lt;sup&gt;23&lt;/sup&gt;)</td>
<td>Gather Victim Host Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Gather Victim Identity Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Gather Victim Network Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Whisking for Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Closed Sources (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Open Technical Databases (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Open Network/Domain (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Victim-Owned Websites (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Reconnaissance (&lt;sup&gt;10&lt;/sup&gt;)</td>
<td>Resource Development (&lt;sup&gt;7&lt;/sup&gt;)</td>
<td>Initial Access (&lt;sup&gt;9&lt;/sup&gt;)</td>
<td>Execution (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Persistence (&lt;sup&gt;10&lt;/sup&gt;)</td>
</tr>
<tr>
<td>Active Scanning (&lt;sup&gt;23&lt;/sup&gt;)</td>
<td>Gather Victim Host Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Gather Victim Identity Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Gather Victim Network Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Whisking for Information (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Closed Sources (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Open Technical Databases (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Open Network/Domain (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Search Victim-Owned Websites (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Reconnaissance (&lt;sup&gt;10&lt;/sup&gt;)</td>
<td>Resource Development (&lt;sup&gt;7&lt;/sup&gt;)</td>
<td>Initial Access (&lt;sup&gt;9&lt;/sup&gt;)</td>
<td>Execution (&lt;sup&gt;12&lt;/sup&gt;)</td>
<td>Persistence (&lt;sup&gt;10&lt;/sup&gt;)</td>
</tr>
</tbody>
</table>
HOW DO YOU AND OTHERS SELECT THE RIGHT TTPs?

- **If you DON’T know your threats**
  - Set aside 1 week+ to do research
  - Identify your **most common** actors or attacker types; **what is their tradecraft?**
    - Sophos, Mandiant, ESET, Dragos, etc. can help here

- **If you ALREADY know your threats**
  - Identify the most likely attackers via your threat model
  - Validate that you have an up-to-date list of their operational tradecraft

*Most security research and government alerting already maps to MITRE ATT&CK*
WHEN THE TECHNIQUE ISN’T ON ATT&CK:

- Ensure it *isn’t* available
- Get Creative
  - Broadcast-denial-of-service (BDoS)
  - Telephony-denial-of-service (TDoS)
- Be Consistent
- Establish Clear Definition
WHEN THE TECHNIQUE ISN’T ON ATT&CK (CONT.):

GLOSSARY OF TERMS

TACTICS, TECHNIQUES AND PROCEDURES NOT ON THE MITRE ATT&CK FRAMEWORK:

- **9-1-1 Direct**: Threat actors may directly call emergency lines (such as 9-1-1 in the United States) to target local PSAPs in TDoS attacks.

- **Admin Line Discovery**: Threat actors may use the internet to research administrative lines belonging to PSAPs (such as 1-800 numbers) to conduct TDoS attacks.

- **Botnet Creation**: Threat actors may exploit victim devices via techniques like Drive-By Compromise to create botnets before conducting denial of service attacks. Created botnets are frequently used in TDoS attacks against PSAPs.

- **Botnet Purchase**: Threat actors may rent or purchase botnets via criminal marketplaces to amass the necessary machines to conduct denial of service attacks. This is often implemented in TDoS attacks against PSAPs.

- **Broadcast Denial of Service**: Threat actors may disrupt LMR communications for political, ideological or financial motivations by jamming frequencies or remotely interfering with LMR devices.

- **Execution Via Botnet**: Threat actors may use botnets to produce high amounts of traffic or simulated phone calls in TDoS attacks.

- **Hardware or Key Theft**: A common way for threat actors to gain access to LMR transmissions. Threat actors may use stolen radios or hardware encryption keys to surveil encrypted communications between first responders and federal officers. Threat actors may also use stolen radios or hardware encryption keys to conduct Broadcast Denial of Service attacks.

- **Data Extort/Publish**: Threat actors may steal data for the purpose of extorting victims for its release. In these instances, threat actors may publish portions of the data on custom, data-sharing sites. This behavior is often observed in association with extortion groups.

- **9-1-1 Direct**: Threat actors may position attacks during times in which defenders are unable to proactively respond due to high call volume or low staffing, like holidays or statewide events (such as the 2020 protests in the United States).
Contribute

You can help contribute to ATT&CK.

ATT&CK is in a constant state of development. We are always on the lookout for new information to help refine and extend what is covered. If you have additional techniques, know about variations on one already covered, have examples of techniques in use, or have other relevant information, then we would like to hear from you.

We are looking for contributions in the following areas in particular, but if you have other information you think may be useful, please reach us at attack@mitre.org.

All contributions and feedback to ATT&CK are appreciated. Due to the high volume of contributions, it may take us about a week to get back to you. We may ask you follow-up questions to help us understand your contribution and gather additional information. We recommend you read our philosophy paper to understand our approach to maintaining ATT&CK so that we get the right details up front. If we find the contribution fills a gap, then we will make edits and send you a draft version of the technique or Group/Software page for your review prior to it being published, listing you as a contributor if desired. Content updates happen roughly every 6 months.
### CUSTOM TELEPHONY-DENIAL-OF-SERVICE MAPPING

<table>
<thead>
<tr>
<th>VICTIM DISCOVERY</th>
<th>PHONE/COMPUTER ACCESS</th>
<th>CALL EXECUTION</th>
<th>PERSISTENCE</th>
<th>IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Line Discovery</td>
<td>Botnet Purchase</td>
<td>Execution Via Botnet</td>
<td>Call Spoofing</td>
<td>Telephony Denial of Service</td>
</tr>
<tr>
<td>9-1-1 Direct</td>
<td>Botnet Creation</td>
<td>Scheduled Task/Job</td>
<td>Critical Timing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Drive-by Compromise</td>
<td>Exploitation for Client Execution</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Phishing</td>
<td>Malicious Link</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Malicious File</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Heatmap: Color-coded TTPs, in descending order of likelihood
- Even with custom maps, follow MITRE’s methodology
FIRST USE CASE
SECURE PRODUCT DEVELOPMENT

- Makes intelligence actionable
  - ATT&CK TTPs → product changes
- ATT&CK can highlight unknown threats
- Make recommendations product-specific
  - Where necessary
- Work directly with product owners to make it relevant

**EXAMPLE:**

Enabling or enforcing **multi-factor authentication** for two-way radio management networks in response to observed adversary tradecraft
SECOND USE CASE
NETWORK MONITORING

- Alert recommendations for network monitoring
- Focus on the most relevant threats
  - A SOC can’t alert on everything
- Tailor recommended alerts. We focus on products & customer verticals
- Understand limitations of alerting sensors and software

EXAMPLE:

When targeting police, extortion gangs often scan for exposed Remote Desktop Protocol or VPN services. They then brute-force or exploit these services for initial access.

This knowledge can be turned into alert categories.
THIRD USE CASE
INCIDENT RESPONSE

- Create threat actor PLAYBOOKS centered on MITRE ATT&CK
  - Update regularly
  - Save for most relevant threats
  - Include IOCs — but focus on tradecraft
- Using ATT&CK keeps everyone on the same page
- ATT&CK's mitigations are designed for this

EXAMPLE:

The format of playbooks can differ, but documents should include these basic categories.
ADDITIONAL RESOURCES:

- Getting started with MITRE ATT&CK
  - Go to [Attack.MITRE.org/Resources/Getting-Started](https://www.Attack.MITRE.org/Resources/Getting-Started) for more information about the framework

- How to use MITRE ATT&CK in Purple-Teaming exercises
  - Medium.com article 'Getting Started with ATT&CK'

- How CISA says MITRE ATT&CK should be used
  - CISA.gov link titled 'Best Practices for MITRE ATT&CK Mapping'
QUESTIONS?