Leveraging MITRE ATT&CK® for Cyber Operations and Risk Management

© 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation. More information available at https://attack.mitre.org.
Introductions

• Casey Kahsen
  • Section chief of network forensics for CISA hunt and incident response team
  • Previously served as incident response engagement lead and technical lead for host forensics
  • Extensive work in operationalizing ATT&CK for hunt and incident response operations

• Adam Isles
  • Principal, Chertoff Group, Cyber Defense, Risk Management
  • Led build-out of cyber defense model utilizing ATT&CK for organizations in financial services, retail and manufacturing sectors
  • Prior roles at DHS, DOJ
What is the Security Objective(s)?

• Considerations:
  • Business model
  • Adversary interest
  • How could an adversary compromise me?
  • Security approach and security investments

• Measuring effectiveness:
  • Do our countermeasures actually work?
  • In the event of compromise, are we prepared to respond?
Enter...ATT&CK

“Periodic Table” of Tactics & Techniques
(prerequisite for mapping to defensive countermeasures)

Library of Threat Actor Groups
(ensables mapping to business)

Additional Data Elements
(ensables mapping to defensive countermeasures)

- Data sources
- Mitigations
- Filters (Windows, Linux, cloud, ICS, etc.)

Source: MITRE Corporation

https://attack.mitre.org/
Pyramid of Pain

• ATT&CK Reflects tactics and techniques observed in the real world

• Why is this important?
  • Industry historically focused on methodology that is low on the pyramid
  • Forces adversary to change tools and behavior to avoid detection
    • Lowers their ROI

• For the Defender:
  • Behavior focused detection > artifact focused detection
  • ATT&CK based hunting

What to search? David Bianco’s pyramid of pain

http://detect.respond.blogspot.mx/2013/03/the-pyramid-of-pain.html

TTP-based detection: Special behavior detectors above collected events, manual search

Tool-based detection: AV detects, Yara rules, tools-specific detectors above collected events

IOC-based detection: Automatic matching of indicators from collected events using different threat intelligence feeds
Evolution of ATT&CK at CISA

• 2017
  • Large scale campaign tracked via behavioral markers

• 2018
  • Early adoptions of the Operations Management System (OMS)

• 2019
  • Began working with MITRE to:
    • Research playbooks
    • Common techniques hunted for across IR industry
    • Data sources required to perform ATT&CK based hunting (tooling to accommodate)

• 2020
  • Evolution of the OMS to leverage ATT&CK
  • ATT&CK integration into custom Splunk App
  • ATT&CK integration into engagement report (customer deliverable)
Operations Management System (OMS)

• Centralized command center location for our deployment teams:
  • Team management and tasking (Planner)
  • Collaboration and document sharing (Teams)
  • Engagement notes and documentation (OneNote)
  • Engagement document management (SharePoint)

• Goals:
  • Significant reduction of time to effective analysis (automation & templates)
  • Compounded effect results in reduction of
    • Time to effective detection
    • Time to effective defense
    • Time to effective reporting
OMS cont.

- Pre-built templates
  - Standardized tasks (end)
- All teams function
- Allows our leads (end)
- Designate tasks
- Track progress of tasks
OMS cont.

• Analytical tasks organized and use ATT&CK methodology
  • Characterizes phases of threat actor activity
  • Industry standard lexicon/terminology

• Baseline data for understanding the analytical task
  • Junior analysts

• Adversary tactics based hunting
  • Drives our teams to look for relevant data that is high on the pyramid

• OMS 2.0
  • Leverage decision trees based on identified techniques (if X is detected, then search for Y)
ATT&CK in CISA

CISA uses ATT&CK based incident response processes to:

- Find
- Identify
- Describe

Teach a man to fish mentality:

- What was found
- What data was required
- Associated Mitigations

Adversary behaviors associated with risk observations (“this is what could happen”)

(1) Institute Multi-Factor Authentication for Access to M365

ACME currently utilizes username and password for authentication to M365, syncing cloud credentials to Active Directory. As seen in this incident, simple username and password authentication is easily compromised by an adversary, with the adversary gaining complete access to the compromised account’s email, which contain vital information.

CISA recommends that ACME leverage the security of multi-factor authentication (MFA) supplied within M365. MFA utilizes two or more factors to authenticate to systems. This can be a combination of username and password and a token, either soft or physical. With this extra step, an adversary would be prevented from gaining access to ACME’s M365 environment if they were able to compromise username and password credentials again.

Summary: MFA ([M1032]) helps mitigate the following threat actor techniques that were observed in use in this incident:

Table 3: Observed ATT&CK techniques that align with this mitigation

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Persistence</th>
<th>Collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid Accounts [T1078]</td>
<td>Account Manipulation [T1098]</td>
<td>Email Collection [T1114]</td>
</tr>
</tbody>
</table>
ATT&CK: Tying Mission/Business Model to Threat and Tying Threat Actors to TTPs

1. ID key business attributes
   - Core manufacturing processes
   - Sensitive IP
   - Personal data
   - Volume of financial transactions

2. Research to identify threat actors targeting those business attributes
   - Research and analysis of Open-Source, Commercial Threat Intelligence
     - MITRE ATT&CK, etc.
   - Alerts from CISA, other public sector sources
   - Engage w/ defenders to confirm relevance

3. Map threat actors to TTPs
   - TTPs are risk-rated and sorted based on priority
   - Supplement with ubiquitous TTPs
     - TTPs used by all groups regardless of sightings
ATT&CK: Prioritizing Investments
ATT&CK: Measuring Performance

Run Testing; Obtain Pass/Fail test results

Apply TTP-specific Risk Rating

Generate Performance Rating

Risk Diagnostic Example

TTP-Specific Risk Rating

- Difficulty of attack
- Ease of defense
- Additional factors

Trending/benchmarking context
**ATT&CK & Risk: Summary**

**INHERENT RISK**
- Isolate a core set of risk-informing factors and generate inherent risk profiles across business units.

**THREAT MODEL**
- Identify likely threat actors based on client's industry sector; generate set of TTPs likely to be applied against organization.

**THREAT RATING**
- Risk-rate TTPs based on factors such as ease of attack, difficulty of defense, impact, frequency.

**MAPPING**
- Map organization's defensive countermeasures to likely TTPs.

**SAMPLE SET**
- Identify sample set of assets for initial diagnostic.

**MEASURE**
- Measure overall effectiveness in defending against sample TTP set.

**BUSINESS CASE**
- Develop business case justification for investments based on risk reduction potential.

**ATT&CK TTP ID numbering in CISA alerts helps identify repeat TTPs (and thereby prioritize countermeasures).**

**ATT&CK Mitigation ID numbering in CISA alerts help map TTPs to mitigations.**

**When CISA alerts identify targeted asset types, this helps identify sample sets for testing.**

**CISA alerts help map threat actors and TTPs to industry sectors.**
How’d I do?

• Survey Monkey Link

• Mobile Link
  • Text Survey to XXX-XXX