Automation: The Wonderful Wizard of CTI (or is it?)
Who We Are

Sarah Yoder (@sarah__yoder)
• Cyber Security Engineer
• Cyber threat intelligence + red teaming
• Disneyland enthusiast, Triathlete, Chai Tea Fanatic

Jackie Lasky
• Cyber Security Engineer
• Cyber threat intelligence + threat hunting
• Photographer, Traveler, Dog-lover
The Plan

1. How We Use CTI for ATT&CK
2. Our Automation Tool - TRAM
3. How This Can Help You
4. Challenges with Automation
5. The Future of TRAM


Warner Bros.
What does Cyber Threat Intelligence mean for ATT&CK?

- CTI forms the basis of ATT&CK
- We help to organize CTI by keeping ATT&CK up-to-date
- We develop ways to share or organize CTI
- We show and provide ways to use CTI
Before We Got A “Brain”

Backlog of reports

Analyst gets assigned report to read and review

Data is entered into ATT&CK

http://www.loc.gov/exhibits/oz/images/uc55.jpg
The Yellow Brick Road: Reporting ⇒ ATT&CK

1. Find open source threat reporting
   • APT groups, software

2. Find behaviors in the report
   • Think ATT&CK structure

https://www.hiclipart.com/search?clipart=goodbye+Yellow+Brick+Road
Finding Behaviors in Finished Reporting

- The Trojan **obfuscates its executable code** prior to compilation, rather than packing it like most other ransomware, making it harder for researchers to reverse engineer.
- It also obscures the links to the necessary API function, and stores hashes to strings rather than the actual strings.
- Upon installation, the Trojan reviews the directory in which it was launched. If it is launched from an ‘incorrect’ directory — such as a potential automated sandbox — it will not execute.
- The trojan can also write without exception if the victim PC has a keyboard set to Cyrillic script.

- Before encrypting files on a victim device, **SynAck** checks the hashes of all running processes and services against its own hash table to ascertain that the victim device is not interacting with virtual machines, office applications, script interpreters, database applications, backup systems, or other possibly to make it easier to seize valuable files which might otherwise be tied up into the running processes.

**Impact** | **Data Encrypted for Impact (T1486)**
--- | ---
**Defense Evasion** | **Obfuscated Files or Information (T1027)**
--- | ---
**Defense Evasion** | **Virtualization/Sandbox Evasion (T1497)**
--- | ---
**Discovery** | **File and Directory Discovery (T1083)**
--- | ---
**Defense Evasion** | **Process Discovery (T1057)**
--- | ---
**System Service Discovery (T1007)**
Remembering ATT&CK (there’s a lot!)

**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>Exploit</td>
<td>Scheduled Tasks</td>
<td>Unpatched Software</td>
<td>Binary Padding</td>
<td>Network Sniffing</td>
<td>Account Hijacking</td>
<td>Application Discovery</td>
<td>Audio Capture</td>
<td>Command and Control</td>
<td>Automated Exfiltration</td>
<td>Data Destruction</td>
</tr>
<tr>
<td>Drive-by Exploiting Application</td>
<td>Local Access</td>
<td>Account Hijacking</td>
<td>Account Hijacking</td>
<td>Brute Force</td>
<td>Application Window Discovery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>External Remote Services</td>
<td>Malicious Document</td>
<td>Click for Action</td>
<td>Command and Control</td>
<td>Credential Stuffing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware Actions</td>
<td>PowerShell</td>
<td>Extra Privilege Hijacking</td>
<td>Exploitation of Components</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploitation Using Removable Media</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Spearing Attachment**

**Procedures Examples**

**Procedures: Specific technique implementation**

**APT12**
- APT12 has sent emails with malicious Microsoft Office documents and PDFs attached. [88][89]

**APT19**
- APT19 sent spear phishing emails with malicious attachments in RTF and XLSM formats to deliver initial exploits. [82]
Trapped in a Time-Consuming Process

- Too many reports, not enough people!
- Human error
- Training new team members

https://www.pinterest.com/pin/16578883002744446/
Off to the Emerald Automation City

The “Magic” behind TRAM?

- **Get Data**
  - ATT&CK procedure examples
  - STIX/TAXII data from ATT&CK

- **Clean & Prepare Data**
  - Normalization
  - Natural language processing

- **Build & Train Models**
  - Python Logistic regression and supervised learning
  - Count Vectorizer, feature extraction, cross validation, etc.
The “Magic” behind TRAM? (Continued)

- **Test Data**
  - Submit a report via URL
  - Models generate predictions on *unseen* data

- **Review Model Decision**
  - Accept or Reject the predictions
  - Add in missing techniques

- **Feedback Loop**
  - Annotations are recorded and sent back to the database to build new models
  - Reports can be exported
Threat Report ATT&CK Mapper (TRAM) Demo

Enter New Report

Insert URL
Enter URL

Insert Title
Enter the article title

Submit

NEEDS REVIEW
Example Report
Source Analyze

ANALYST REVIEWING

COMPLETE
Why Does This Matter?

- Easier to get started with ATT&CK
- Streamline the workflow
- Find techniques we forget about (or have never heard of)
- Use reporting that is important to you
Overcoming Challenges

- Prediction Accuracy
- How do we look for techniques not in ATT&CK yet?
- Building automations can take away time from other work

https://www.ranker.com/list/wicked-witch-margaret-hamilton-career
Is the Wizard of Automation real?

- Why is automating CTI hard to do?
- Augmenting CTI work to blend human analysis with AI

https://media.giphy.com/media/AEMyf9O6MpSB/giphy.gif
Future of TRAM

- Despite full automation not being the answer to all our problems, development on TRAM is still on track
- Finding the balance as we transition the workflow
- We encourage and appreciate contributions from the community!