MITRE ATT&CK: The Play at Home Edition

Nicholas Hayden
Global Head of Intelligence Operations
Anomali
<table>
<thead>
<tr>
<th>Layer</th>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MITRE ATT&amp;CK</td>
<td>Tells a Story</td>
<td></td>
</tr>
</tbody>
</table>

<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>Exfiltration</th>
<th>Command And Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive-by Compromise</td>
<td>AppleScript</td>
<td>Custom Administrative Access</td>
<td>Access Token Manipulation</td>
<td>Account Discovery</td>
<td>Application Discovery</td>
<td>Audio Capture</td>
<td>Automated Exfiltration</td>
<td>Commonly Used Port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploit Public-Facing Application</td>
<td>CMSTP</td>
<td>Accessibility Features</td>
<td>Binary Padding</td>
<td>Bash History</td>
<td>Application Discovery</td>
<td>Browser Bookmark Discovery</td>
<td>Data Compressed</td>
<td>Communication Through Removable Media</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command-Line Interface</td>
<td>AppCert Dlls</td>
<td>AppCert DLLs</td>
<td>HTTPS</td>
<td>Brute Force</td>
<td>Document Discovery</td>
<td>URL</td>
<td>Data Encrypted</td>
<td>Connection Proxy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware Additions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Custom Command and Control Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Custom Cryptographic Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Data Encoding</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Data Obfuscation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Data Staging</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Data Exfiltration Other Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Data Exfiltration Other Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Multi-hop Proxy</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Multi-stage Channels</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Multi-band Communication</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Multi-layer Encryption</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Port Knocking</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Remote Access Tools</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Remote File Copy</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Standard Application Layer Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Standard Cryptographic Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Standard Non-Application Layer Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Uncommonly Used Port</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Web Service</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend:
- MITM: Man-in-the-Middle
- ST: Stealing Tapes
- SST: Stealing Software
- SP: Stealing Programs
- SH: Stealing Hardware
- SS: Stealing Scripts
- SR: Stealing Records
- SM: Stealing Money
- S: Staging
- C: Compromise
- E: Exploit
- D: Defense
- A: Access
- P: Privilege
- S: Subscription
- L: Lateral
- M: Movement
- C: Command
- A: Action
Since this is MITRE ATT&CK: The Play at Home Edition
What better way to tell a story then…
Disney + Story = ?
ONCE UPON A TIME

IN A KINGDOM FAR FAR AWAY
Or…
Disney + Star Wars = ?
A long time ago in a galaxy far, far away....
<table>
<thead>
<tr>
<th>Layer</th>
<th>Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Elevation</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></td>
<td>APT 32</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>

**Initial Access**
- Java and Oracle JRE
- Adobe Flash
- Acrobat

**Execution**
- Java
- Adobe Flash
- Acrobat

**Persistence**
- Java
- Adobe Flash
- Acrobat

**Privilege Elevation**
- Java
- Adobe Flash
- Acrobat

**Defense Evasion**
- Java
- Adobe Flash
- Acrobat

**Credential Access**
- Java
- Adobe Flash
- Acrobat

**Discovery**
- Java
- Adobe Flash
- Acrobat

**Lateral Movement**
- Java
- Adobe Flash
- Acrobat

**Collection**
- Java
- Adobe Flash
- Acrobat

**Command And Control**
- Java
- Adobe Flash
- Acrobat

**Exfiltration**
- Java
- Adobe Flash
- Acrobat

**Impact**
- Java
- Adobe Flash
- Acrobat

**APT 32**
APT 33
Do the Groups Matter?
Key Takeaways

• Statistical based historical knowledge (Cyber Threat Data) of advisory’s tactics will tell a story

• Everyone in the community needs help contribute to the story by associating tactics and techniques to current events

• We need to start using threat intel data to actually produce intelligence
Once We Understand the Story

We can start to predict the storm!
How Does a Good Disney Story End?
Questions?