Cyber Security

presented by
Ascent Solutions
Ascent Solutions

• Serious IT Transformation
• Cloud first, security everywhere
Outline

• Introduction
• Cyber Actors
• Cyber Kill Chain
• Diamonds vs Paperclips
• Cloud
• Q/A
<table>
<thead>
<tr>
<th>Adversary</th>
<th>Motives</th>
<th>Impacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>⚔ Nation States, Intelligence Services</td>
<td>• Economic, political, and/or military advantage</td>
<td>• Loss of competitive advantage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Loss of command &amp; control capability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Prolonged foothold in one's network for future attacks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Disruption of business activities / asset loss</td>
</tr>
<tr>
<td>🎁 Organized Crime</td>
<td>• Financial gain</td>
<td>• Regulatory inquiry/penalty</td>
</tr>
<tr>
<td></td>
<td>• Collect information for future financial gain</td>
<td>• Consumer and shareholder lawsuits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Brand and reputational damage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Consumer confidence loss</td>
</tr>
<tr>
<td>🔊 Hacktivists</td>
<td>• Political or social change</td>
<td>• Disruption of business activities and loss of assets</td>
</tr>
<tr>
<td></td>
<td>• Pressure business to change their practices</td>
<td>• Brand and reputational damage</td>
</tr>
<tr>
<td></td>
<td>• Create fear and uncertainty</td>
<td>• Consumer confidence loss</td>
</tr>
<tr>
<td>🔐 Insiders, Former Insiders</td>
<td>• Personal advantage, monetary gain</td>
<td>• Disclosure of trade secrets</td>
</tr>
<tr>
<td></td>
<td>• Sabotage for personal grievances</td>
<td>• Disruption of business activities and loss of assets</td>
</tr>
<tr>
<td></td>
<td>• Bribery or coercion</td>
<td>• Brand and reputational damage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Consumer confidence loss</td>
</tr>
</tbody>
</table>
The Kill Chain*

1. RECONNAISSANCE
   - Open-source research, social network research, port scan, IP sweep, Google research

2. WEAPONIZATION
   - Combine the exploit tool with the method

3. DISTRIBUTION & STRATEGY
   - Phishing email, website drive-by, SQL inject script

4. EXPLOITATION
   - Infected Word doc or PDF opened; Java script exploited in browser; command line SQL inject

5. PERSIST/LATERAL MOVEMENT
   - Registry key changed; privilege escalation; look for open connections

6. COMMAND & CONTROL
   - Malware or compromised system reaches out for instructions

7. ACTION ON TARGET
   - Search the target; Destroy or disrupt; Package and prepare data for exfiltration

*Slide from Armor Defense, Inc.
Diamonds and Paperclips

• You wouldn’t protect diamonds the same way you would protect paperclips
• Identify key infrastructure
• Put your resources in the right place
• Requires you understand which one is which
Cloud

• What is the cloud?
  • IaaS
  • PaaS
  • SaaS
• Whatever it is, we can’t do it
• Unsecure
• Too hard
Considerations for IoT

• There are many ways to do IoT securely
  • A solution isn’t secure if it doesn’t fit your needs

• There are also wrong ways
  • Find the right resources

• Identity Driven Security
  • New control vector

• MFA for data access
  • Canalize the enemy

• Visualization / Alerts
  • Patrol your ecosystem
Questions?