Network Attacks Against Physical Access Controls

Chris Carlis
Mike Kelly
September 24, 2018
Introductions – Chris Carlis

• Co-founder / Principal Consultant
• 8 Years Experience Penetration Testing
• Red Teaming / Network / Physical / Wireless / Social Engineering
Introductions – Mike Kelly

• Principal Consultant at Secureworks
• 8 Years Experience
• Penetration Testing / Red Teaming / Hardware Security
• Security Researcher
Introductions - Continued

• Hacker Mindset
• Known Knowns
• Known Unknowns
• Unknown Unknowns
• We’re here to help*
Outline

• Definitions
• Attacker Point Of View
• Traditional and Contemporary Tactics
• Targeting Devices, Systems and Personnel
• Wrap Up
Definitions

• Penetration Test (Pentest)
  • A test designed to enumerate paths of entry/compromise

• Red Team Engagement
  • Broader scope, stealth focused, testing detection & response capabilities

• Physical Access Control Software (PACS)

• Door Controller
The Attacker’s Point Of View

• Motivations
  • Network Access
  • Theft of Physical Property
  • Business Disruption
  • Employee Harm
Traditional Entry Tactics

- Tailgating / Piggy Backing
- Lockpicking
- Locking mechanism bypass
- Physical theft of credentials
- Non-standard entry points
Contemporary Entry Tactics

- RFID Badge Cloning
- RFID Reader Compromise
- Social Engineering
Limitations

- Risk
- Reliability
- Persistence
- Depth of Access
A Different Approach

- Targeting Devices
- Targeting Infrastructure Systems
- Targeting Security Personnel
Targeting Devices
Targeting Devices

Data Center, Metro Denver

Completed in two phases, this data center utilizes an AMAG Symmetry Enterprise system with over 100 HID iClass readers, with the EN-1DBC IP door controllers, biometric readers, over 150 IP cameras and video analytics.

PROJECT TYPE: DATA CENTER, SECURITY SYSTEMS
INDUSTRY: CORPORATE
### Targeting Devices

<table>
<thead>
<tr>
<th>0000</th>
<th>0010</th>
<th>0020</th>
<th>0030</th>
<th>0040</th>
<th>0050</th>
<th>0060</th>
</tr>
</thead>
<tbody>
<tr>
<td>6c 40 08 b9 67 2e 00 15</td>
<td>bd 00 1f 72 08 00 45 00</td>
<td>l@..g... ...r..E.</td>
<td>00 48 0c 1f 00 00 80 06</td>
<td>e3 c5 c0 a8 64 7c c0 a8</td>
<td>.H....... .....d</td>
<td>..</td>
</tr>
<tr>
<td>0020</td>
<td>0030</td>
<td>0040</td>
<td>0050</td>
<td>0060</td>
<td>0070</td>
<td>0080</td>
</tr>
<tr>
<td>64 fe 0b b9 04 73 c8 74</td>
<td>08 c4 5a aa e7 b6 50 18</td>
<td>d.....s.t ..Z...P.</td>
<td>31 14 23 20 23 4a 43 56</td>
<td>10 10 10 1c 32 10 10 38</td>
<td>1.# #JCV ....2..8</td>
<td>00 7710 000,2,1, 0051</td>
</tr>
</tbody>
</table>
Targeting Devices

DEMO
Targeting Devices

• Publicly available information
• Misconfigured devices
• Lack of network segmentation
Targeting Devices

- CVE-2017-16241 – AMAG EN Series
- ZDI-16-223 – HID EVO / discoveryd
- CVE-2017-17704 - Software House iStar Ultra
- ACV-128401 – AXIS Network Cameras (390 models)
Targeting Infrastructure Systems
Targeting Infrastructure Systems

Starting Symmetry

To start Symmetry:
1. Log into Windows. Use the account that you specified during the client software installation.
2. Start Symmetry from the Programs menu or using the Symmetry System Management icon.
3. If prompted, enter the activation code or choose to activate your license via the Internet. If you click Register Later, you have up to 21 days to enter the activation code in the "Maintenance/Licensing/System Licenses" screen. Please refer to page 26 for details of how to obtain the activation code.

Default Login User Names and Passwords

The following default login names and passwords are provided. The engineer name and password are fixed, but for all others, you should ensure that they are changed as soon as possible.

<table>
<thead>
<tr>
<th>Name</th>
<th>Password</th>
<th>Permissions Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUARD</td>
<td>GUARD</td>
<td>Guard Permissions</td>
</tr>
<tr>
<td>ADMINISTRATOR</td>
<td>ADMINISTRATOR</td>
<td>Administrator Permissions</td>
</tr>
<tr>
<td>MANAGER</td>
<td>MANAGER</td>
<td>System Manager Permissions</td>
</tr>
<tr>
<td>INSTALLER</td>
<td>INSTALL</td>
<td>Installer Permissions</td>
</tr>
<tr>
<td>ENGINEER</td>
<td>INCOM</td>
<td>Engineer Permissions</td>
</tr>
</tbody>
</table>
Targeting Infrastructure Systems
Targeting Infrastructure Systems

<table>
<thead>
<tr>
<th>Access Rights</th>
<th>Personal</th>
<th>Locator</th>
<th>Biometrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN Code: 9999</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDS Code:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card Issue Level: 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facility/Customer Code: 0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Chris Carlis

Contractor
Targeting Infrastructure Systems

- Principal of Least Access
- Multi-factor Authentication
- Default / Hardcoded Credentials
- New User Review
Targeting Security Personnel
Targeting Security Personnel
Targeting Security Personnel

- User Education
- Data Hygiene
Summary

• Your network perimeter is your physical perimeter is your network perimeter
• Secure on Install
• Researchers are you friends
Q&A
Thank you!

exfil.co
dolosgroup.io