How to Think Like A Criminal
An attack perspective of your AMI solution
Goal of our presentation

• Talk through some real world attacks, including those aimed at AMI
• Demonstrate a live attack
• Talk about mitigations and how to prevent and detect attacks
Attack Tree to Disable Take Out Point

- Common AMI Mitigations:
  - System integrity validation checks
  - Encrypt flash storage and contain an integrity check protecting configuration data from modification and snooping
  - Signed Firmware that is verified by prior to installation and execution
  - Local Firewall usage minimizing attack surface
  - Removing unnecessary services and control remote access for take out
Fired Employee Hacks and Shuts Down Smart Water Readers in Five US Cities

Flanagan disabled water reader base stations

Things turned sour when Flanagan's employer fired him on November 16, 2013, for undisclosed reasons. This didn't sit well with Flanagan, who used his knowledge of the TGB stations he installed to access these devices and disable their ability to communicate with their respective water utility providers' upstream equipment. The former employee also changed passwords to offensive words on some TGBs.

According to court documents, the FBI tracked down Flanagan's actions to six incidents in five cities across the US East Coast: Aliquippa (Pennsylvania), Egg Harbor (New Jersey), Kennebec (Maine), New Kensington (Pennsylvania), and Spotswood (New Jersey).

<table>
<thead>
<tr>
<th>COUNT</th>
<th>DATE</th>
<th>COMPUTER</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>March 1, 2014</td>
<td>TGB in the Kennebec Water District</td>
</tr>
<tr>
<td>2.</td>
<td>April 22, 2014</td>
<td>TGB in the Aliquippa Water Authority</td>
</tr>
<tr>
<td>3.</td>
<td>April 30, 2014</td>
<td>TGB in the Kennebec Water District</td>
</tr>
<tr>
<td>5.</td>
<td>May 9, 2014</td>
<td>TGB in Egg Harbor City, NJ</td>
</tr>
<tr>
<td>6.</td>
<td>May 19, 2014</td>
<td>TGB in New Kensington, PA</td>
</tr>
</tbody>
</table>

source: Waterworld, Former Water Utility Employee Gets Prison Time for Hacking Into Metering systems, June 20, 2017
Mitigations for Disabling Collector

- Development
- Code Signing
- Utility Operations
- Security
- Intrusion Detection, Prevention
- Key Management
- Provisioning PKI
- Traffic Inspection
- Secured Messaging
- Endpoints
- System Root of Trust
- Key Management
- Utility Engineering
- Firewalls
- Maintenance
- Certificate
- Software
- OTP

Secure Tool Access
Message Integrity Check
Disable test ports
Flash Encryption
Firmware Authenticity
Interrupting Electricity Flow

**Common AMI Mitigations**

- All commands sent from HES to meter are digitally signed using utility root of trust and verified by device prior to executing command
- Optical ports on meters can be disabled once in field preventing access to device
- Head End System (HES) supports RBAC to limit who can issue connects/disconnect commands
- HES supports velocity checks and blocked periods for connect/disconnect commands
- Field Tools are secured against unauthorized use
Look up Smart Meter Hack on Youtube
Mitigations for Interrupting Electricity Flow

- Velocity Check
- Signed Messages
- Privileged Usage
- Verify Signatures
- Message Integrity Check
- Broadcast Restriction
- Disable test ports
- Flash Encryption
Compromise Head End System

- Common AMI Mitigations
  - User credentials are protecting using a salted hash
  - HES authentication systems supports user lockout preventing brute force attacks on credentials
  - HES is regularly tested using variety of security testing tools
  - Secure deployment and lockdown of servers HES runs on
Spear Phishing Campaign

• Emails with Word Document Attachment
• Email would request file using open SMB (Server message block - ~file sharing protocol)
  • The request authenticates the client; using users credentials
  • Hash of user’s password is provided; even if file is not downloaded
• Password cracking tools used on user’s credential hash
• With Valid credentials, threat actors can masquerade as valid users
Malware Initial Findings Report (MIFR) - 10128830
2017-10-13

Notification

This report is provided “as is” for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/lp/

Summary

Description

US-CERT received an artifact for analysis, a résumé-themed phishing email with an attached malicious Microsoft Word Document. Analysis of the artifact indicates the use of a “Redirect to SMB” attack to steal the victim’s credentials.

Additional analysis on related activity is also referenced in MIFR-10126327 and MIFR-10126336.

Emails

| Processed | 1 |

Files

<table>
<thead>
<tr>
<th>Processed</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>722154e30d2ba10a0a8020a8ad750a7a (CV Controls Engineer.docx)</td>
<td></td>
</tr>
</tbody>
</table>
Email Resume From Jon Patrick

Hello, [Victim]

Over 10 years Controls/Software Experience

  Software development for PLC based control systems:
  SIEMENS S5, S7-200, S7-300, S7-400 series,
  Rockwell 5000, 500 series.
  SCADA, HMI configuration.

  Various Conveyor system experiences
  Networking with PLC's: Ethernet, PROFIBUS-DP, PROFINET, MPI, ASi, DeviceNet, DH+
  EPLAN

Multi-skilled controls engineer with experience in hands-on project based work. Experience ranges from budget estimate and managing electric engineering projects to developing and commissioning software for PLC - SCADA control systems.

I Look forward to hearing back.

Best Regards,
Synopsis of recommendations

- Keep antivirus up to date
- Restrict users from installing applications
- Strong password policy
- Patch operating systems
- Personal firewalls
- Disable unnecessary services
- Scan and remove suspicious attachments
- Monitor and restrict browsing activity
- Scan all downloaded software before executing
Additional Spear Phishing Campaign

• Emails with generic theme (contract/legal) and attached document (.pdf)
• Nothing malicious embedded in the .pdf
• Email contained a link
• Link was an external web page that would request the user’s login and password
American Nuclear Society
Eastern Washington Section

Together with other Technical Societies, invites you to a

Holiday Party!

Saturday, December 10, 2016
Tri-City Country Club
314 N Underwood St, Kennewick, WA

5:30 p.m. Salsa Dancing Instruction (optional)
6:30 p.m. Buffet Dinner
6:30 p.m. Manhattan Bar Opens
8:00 p.m. Door Prizes and Announcements
8:30 p.m. Open Dance with Vickie and the VelveTones

Special Commemoration to Albert Einstein Professor Extraordinaire

Tickets $25  RSVP by December 1, 2016

Reserve your spot today! http://www.anseasternwashington.org/holiday-party-2016.html

Occupancy limited to first 100 reservations
Watering Hole Domains

• Infrastructure of trusted organizations was compromised
• - about half were trade publications and informational websites related to process control, ICS or critical infrastructure
• Websites were altered to contain or reference malicious content
• Websites were altered with legitimate credentials
Open Source and Network Reconnaissance

• The attackers utilized some of the following open source tools:
  • Hydra – Brute force, online password cracking tool
  • SecretsDump – Dumps secrets (including credentials) from the registry
  • CrackMapExe – Windows/Active Directory attack tool
  • Phishery – Opensource phishing toolkit on GitHub
ICS and SCADA targets

• Attack targeted workstations and servers that had data output from energy generation systems

• Attackers copied profile and configuration for these systems (SCADA WIRING DIAGRAM / SCADA LAYOUT)
DHS and FBI provided detection and response recommendations

• The DHS recommended provided IPs, domain names, file hashes and network signatures that can be used to determine whether an attack occurred or is occurring

YARA rules were provided and system owners were encouraged to run the YARA tool on any system suspected to have been a target.

The Alert includes network signature host based rules useful for detecting malicious activity.
Hacking Demonstration of Keylogging

- Step 1: Install keylogger on target
- Step 2: Wait for user to enter credentials
- Step 3: Record keystrokes while user enters credentials
- Step 4: Own the user
Layered Security Approach

- Application Security
- Network Security
- Device Security

Diagram showing layers of security:
- Layer 1: Network Security
- Layer 2: Device Security
- Layer 3: Application Security
Layered Security Considerations

**Device Layer**
- Chip security
- Secure booting
- Physical security protection
- Firmware Authenticity Check

**Network Layer**
- Backhaul Security
- Firewalls and intrusion prevention systems
- Identification, Authentication and Encryption

**Application Layer**
- Role-based access
- Activity monitoring
- Identification, Authentication and Encryption
- Key Vault
Takeaways

- Understanding the attack vectors is helping us defend our systems

- Utility security teams continually improve the security of their environments. Landis+Gyr is providing AMI mitigations designed to complement our customer’s systems.

- Landis+Gyr is helping utilities maintain trust, keeping the lights on and protecting utility customer’s data

For Reference:

- AMI Attack Methodology, Version 1.0, Jan 2009, InGuardians white paper
- Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology, February 12, 2014
Thank You – Be Careful Out There

Steve Chasko
Security Architect
stephen.chasko@landisgyr.com

Damien Hugoo
Product Manager - Security
damien.hugoo@landisgyr.com