Attachment #11.5 Return to Agenda

# **Cyber Security Overview**

**Doug Chapman** VP & CIO

#### **NYSRC Executive Committee Meeting**

March 9, 2018



©COPYRIGHT NYISO 2018. ALL RIGHTS RESERVED

## Agenda

- Cyber threats overview for the electric industry
- Sources for cyber security intelligence
- NERC Supply Chain Security Standard



### **Cybersecurity Threat Overview for Utilities**

- The threat landscape for utilities has many overlaps with other sectors
- Common threats include:
  - Phishing attacks to install malware and / or harvest credentials
  - Ransomware attack
  - Crypto currency mining
  - Watering hole attack
  - Internet-based scanning for vulnerabilities in a corporate perimeter
  - Distributed Denial of Service (DDoS) attacks



## **Phishing Attack**

- Very popular form of attack that has been around since the mid-1990's
- Typically a fraudulent email appearing to come from a legitimate source
- Emails include a link to a fraudulent website or an attachment containing malware
- Objective of the attacker is to either install malware on the host computer, or get the victim to divulge private information
- Emails can be sent to a wide audience very quickly
- Can be hard to recognize
- Employee training is very important!



### **Ransomware Attack**

- A form of malware that finds data that a user has access to and encrypts the files
- For a price (or Ransom), the victim is then told how to recover the files
- Often spreads through phishing, although not exclusively
- User access to many active data stores adds risk to this type of attack



## **Crypto Mining Attack**

- Digital currencies have gained popularity and value
- Mining for digital currencies has become a more popular way for cyber criminals to generate illegal revenues
- Crypto mining is a complex process where computer resources are used for blockchain transaction verification
- Crypto mining is a highly resource intensive activity
- Cyber criminals are hijacking computers in larger numbers to support mining activities
- Business systems slow down or stop functioning due to a lack of resources that is being consumed by the mining malware

## Watering Hole Attack

- Attacker guesses or observes what website a targeted business or group often uses
- Attacker looks for vulnerabilities in the website
- Attacker then compromises the website with malware or redirection code
- A victim from the targeted group visits the compromised website and is infected with the malware



## **The Classic Cyber Attack Lifecycle**

1	Reconnaissance	<ul> <li>Identify potential targets</li> <li>Assess vulnerabilities</li> </ul>
2	Initial Compromise	• Bypass perimeter defenses through a compromised system or account
3	Command & Control	Adversary installs malware to establish persistent remote access to your environment
4	Lateral Movement	<ul> <li>Once the connection is established, attacker moves laterally to compromise additional systems</li> </ul>
5	Target Attainment	• At this stage, attacker has a good understanding of your IT environment and has obtained persistent access to the target system
6	Action Objectives	Attacker is then in a position to execute their objectives at a time of their choosing



## **Unique Risks for Utilities**

- Utilities typically implement a logically (or physically) separate network for their critical operations systems
  - Often referred to as the "OT" or Operational Technology environment
- Cyber attackers can use common attack vectors to gain access to a corporate network, then pivot to the OT environment
- Utilities also use a wide variety of "connected" equipment in the field that can provide additional attack vectors to an adversary if not adequately protected
- NERC's CIP standards are intended to protect the OT environment
- Avoid the trap of targeting only CIP compliance within the security program
- Need to be secure and compliant!

## **Significant Cyber Events / Threats**

#### Ukraine Cyber Incident

- December, 2015
- Malware introduced in to corporate network
- Gained credentials
- Pivoted to OT network
- Used valid credentials to gain access to OT systems
- Used OT systems to cut off power to over 230,000 customers

#### Dyn Cyber Attack

- October 2016
- Dyn provides domain name services on the Internet
- Attacker used a Botnet of 10M+ IoT devices to flood DYN with domain name lookup requests
- Impacted Internet access to many popular services such as Amazon

#### Industroyer Malware

- Modular malware that is customizable
- Tailored to target Industrial Control Systems
- Can target substation switches and breakers
- Thought to have been used in the 2016 attack on the Ukraine power grid

#### WannaCry Malware

- May 2017
- Worldwide cyber attack affecting over 150 countries
- Self propagating malware using Windows vulnerability
- Patch was already available from Microsoft
- Encrypted data and demanded ransom payment



### **Managing Cyber Security Risks**

Key Elements of a Strong Security Program

Accurate Inventory	<ul> <li>Inventory of assets that need to be managed and maintained</li> </ul>
Network Controls and Remote Access	Network segmentation with limited and controlled access between segments     Secure remote access with multi-factor authentication
Monitoring and Incident Response	<ul> <li>System monitoring capabilities to detect malicious activity</li> <li>Security incident response procedures with escalations defined</li> </ul>
Access Management Controls	Strong access management processes     Application of "Least Privilege" principles
Password Management	Strong passwords     Change default passwords
Vulnerability Management	<ul> <li>Monitor and test vulnerabilities of systems</li> <li>Address vulnerabilities consistently and quickly</li> </ul>
Security Governance & Risk Management	<ul> <li>Strong security policies that includes controls to enforce them</li> <li>Risk management framework that informs improvement programs</li> </ul>
Employee Training	<ul> <li>Security awareness programs for employees</li> <li>Phishing exercises</li> </ul>



## **Sources for Cybersecurity Intelligence**

- **MS-ISAC:** Multistate Information Sharing & Analysis Center
- E-ISAC: Electricity Information Sharing & Analysis Center
- CRISP: Cybersecurity Risk Information Sharing Program
- ICS-CERT: Industrial Control Systems Cyber Emergency Response Team



#### **NERC CIP Supply Chain Security Requirements**

- New set of requirements to address supply chain security concerns
- NERC submitted draft language to FERC in September, 2017
- FERC has largely accepted the language, but is contemplating some changes
- FERC issued a NOPR in January 2018, with comments due back in March



#### **NERC CIP Supply Chain Security Requirements**

#### Proposed requirements cover 4 primary areas:

- **1.** Implement processes to assess cyber risks from vendor product and services
- 2. Updates to vendor contracts to meet new compliance requirements
  - Vendor coordination / notification of incidents, vendor remote access, software integrity, etc.
- 3. Implement processes to manage vendors remote access to critical systems
- 4. Verification of software integrity and authenticity

#### **Other key points:**

- NERC proposed an 18 month implementation, FERC is leaning towards 12 months
- FERC is interested in being more inclusive regarding the types of devices that are in scope



# **Questions?**

