
AMERICAN
PUBLIC
POWER™
ASSOCIATION
Powering Strong Communities

American Public Power Association's Cybersecurity Services Program

APPA Western Regional Cyber Summit

August 22, 2019

Anaheim, CA

Cyber & Physical Preparedness

- Help members develop “all-hazards” approach to disaster preparation and response
- Show federal policymakers public power’s commitment to security and mutual aid
- Strengthen government/industry partnerships
- Minimize new federal regulation

DOE Cooperative Agreement Overview

Goal:
Develop a culture of cyber security within public power utilities.

Objective:
Engage with public power distribution utilities to understand their cyber security awareness, capabilities and risks. Move each utility from its existing state to a public power target profile.

Tasks:
1. Cybersecurity risk assessments (Cybersecurity Scorecard)
2. Onsite cyber vulnerability assessments
3. Pilot existing and emerging security technologies
4. Information sharing between utilities and APPA, E-ISAC, MS-ISAC, other partners

Acknowledgment: *These activities are based upon work supported by the Department of Energy under Award Number DE-OE0000811.*

DOE Cooperative Agreement Overview

- In 2016 APPA partnered with the Department of Energy
- 3-year, $7.5M Cooperative Agreement;

- 2016-17 – Analysis and Data Collection
- 2017-18 – Deployment and Resource Development
- 2018-19 – Sustainability

Acknowledgment: *These activities are based upon work supported by the Department of Energy under Award Number DE-OE0000811.*

Sodinokibi Ransomware Actors Target Management Service Providers' Clients

Summary

- In June 2019, the FBI received notification of ransomware variant Sodinokibi, also known as "REvil" and "Sodin," compromising managed service providers (MSPs) by leveraging victim-installed remote monitoring and managing (RMM) software. Actors behind the Sodinokibi ransomware infection likely leveraged compromised network credentials to gain access to the system. Upon gaining access, Sodinokibi actors use PowerShell scripts to drop an executable containing Sodinokibi into the MSP's network infrastructure, infecting its customers' systems.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

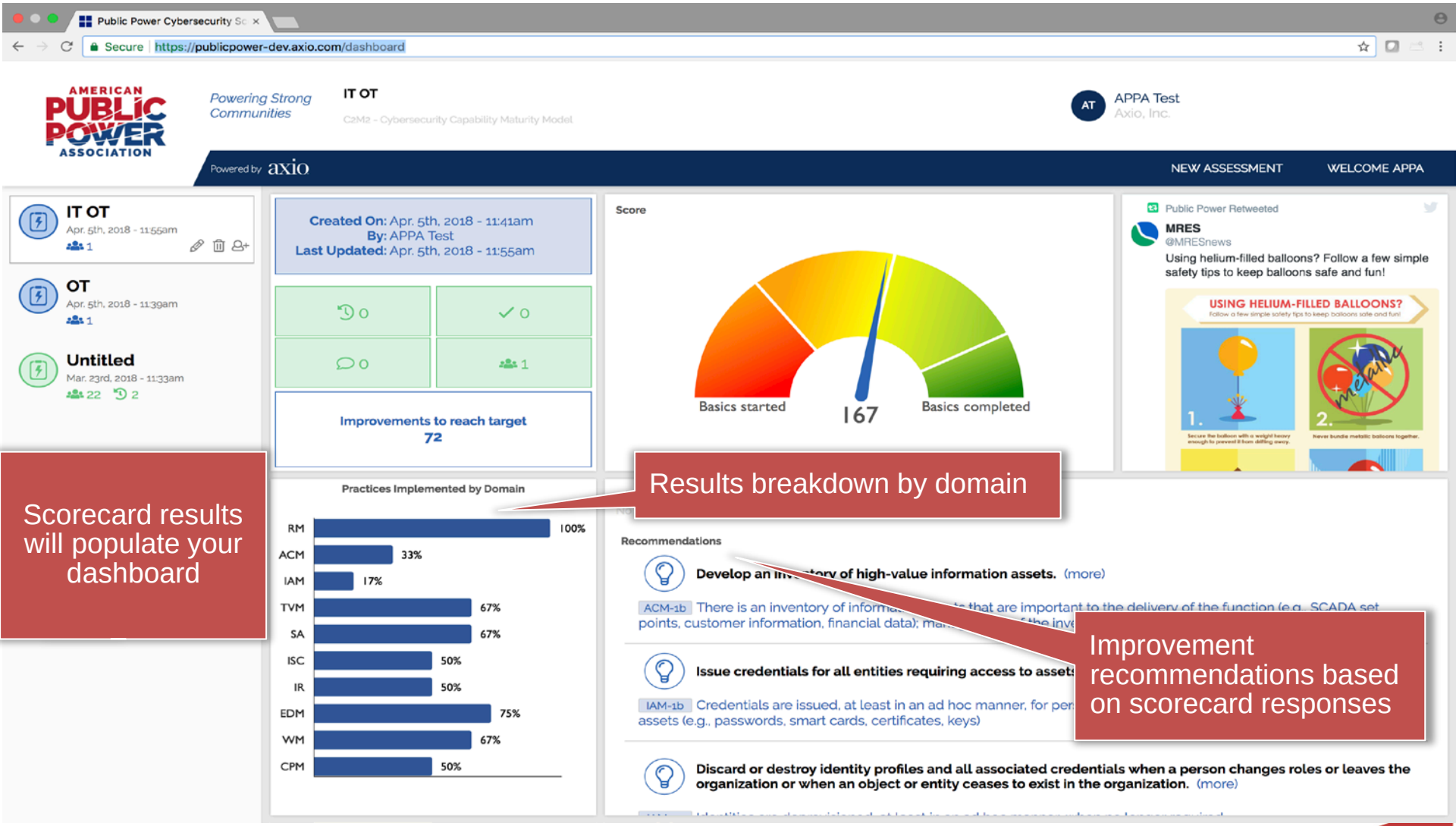
Threat

- FBI investigative activity identified several Sodinokibi ransomware actors compromising MSPs as a means to spread ransomware throughout the MSPs' client networks. This tactic resulted in multiple US companies suffering infection and encryption of file systems as the result of only one cyber intrusion. Once executed, Sodinokibi encrypts the victim files and produces a .txt file displaying the ransom note. The .txt file provides instructions on how to download and configure a TOR browser. Through the TOR browser, the victim accesses a unique uniform resource locator (URL) containing a chatroom, monitored by the actors responsible for Sodinokibi, for payment and decryption instructions.

- Sodinokibi actors likely leveraged CVE-2018-8453 to conduct privilege escalation. Upon identification of the vulnerability, Microsoft released a patch for this CVE in October 2018.

Recommendations

- Regularly back up data and verify its integrity.
- Secure your backups.
- Patch the operating system, software, and firmware on devices.
- Monitor remote connections and software,
- Apply two-factor authentication to user login credentials



Scorecard results will populate your dashboard

Results breakdown by domain

Improvement recommendations based on scorecard responses

Scorecard Activity

- 272 public power utilities participating
  - (2019 Goal is to reach 400 utilities)
- 520 foundational cybersecurity self assessments at the 272 utilities
  - (14 Questions – 45 minutes)

- All public power utilities have **FREE** access to the Scorecard portal

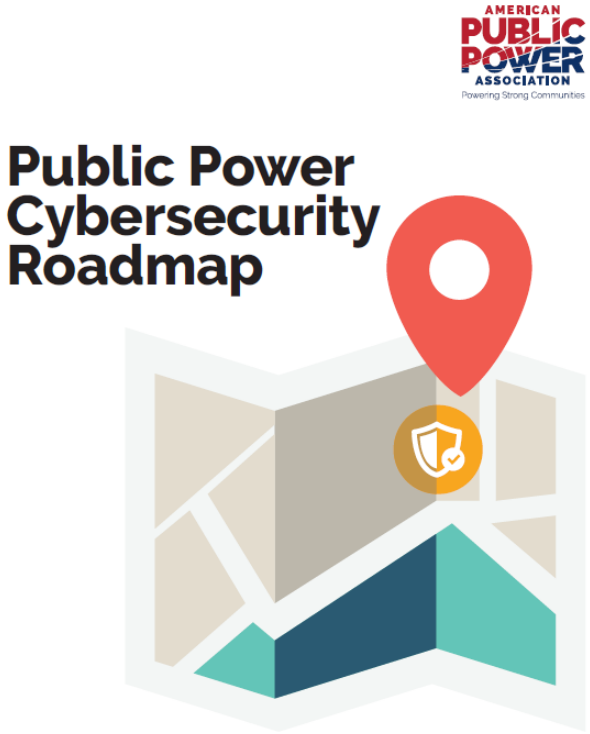
- Utilities who have taken the assessment have reported that the Scorecard is helping to **“take the guesswork out of what they should be striving to achieve”**

Cybersecurity Roadmap

Cybersecurity Roadmap

- Using the Scorecard output, provide public power utilities with clear actions to improve their cybersecurity program

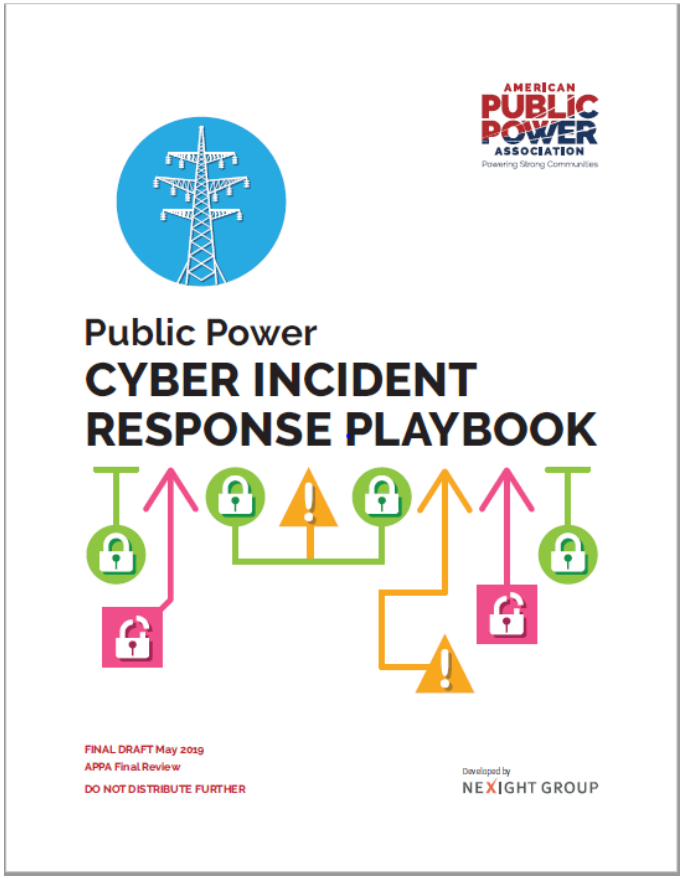
- Provide information that creates a compelling business case for security investments.



Incident Response Playbook

Cyber Incident Response Playbook

- Modeled after mutual aid response network
- Cyber Mutual Assistance (CMA) being developed nationally
- Utilities sharing cyber resources and expertise in a crisis
- Exercising the playbook to be prepared (GridEx V – November 13-14, 2019)



Acknowledgment: *These activities are based upon work supported by the Department of Energy under Award Number DE-OE0000811.*

Cybersecurity Training

- Signing up JAAs to be host sites for training
  - Cybersecurity@publicpower.org
- Deliver low cost **cybersecurity training and exercises** that align with the Scorecard
- Conduct Regional facilitated
  - Orlando July 10-11 (103 attendees)
  - Kearney Nebraska July 24-25 (73 attendees)
  - Los Angeles California August 22 (75 registrations)
- Hosting a year end public power **cybersecurity summit (November 18-20, 2019 Nashville TN)**

Technology Deployment

- After completing the Scorecard, utilities may be ready to reduce risk by investing in cybersecurity technologies from managed security service providers or other vendors.
- The Association's new Cybersecurity Technology Assistance Program (CTAP) can support that investment first by connecting public power utilities to cybersecurity technology solution providers. Then we can offer an 80% cost share for deploying a monitoring system at qualified utilities.
- Developing a **Cyber Asset Tracking** technology to provide public power utilities with an online tool for:
  - Cyber Asset Inventory
  - Geolocation of Cyber Assets
  - Matching of publicly know vulnerabilities with cyber assets

Acknowledgment: *These activities are based upon work supported by the Department of Energy under Award Number DE-OE0000811.*

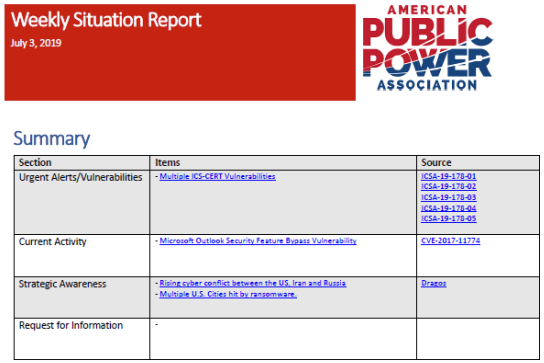
Secure Information Sharing

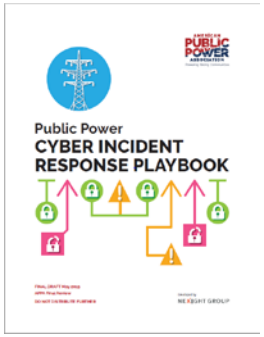
- Sign up for the E-ISAC at www.eisac.com
- Sign up for the MS-ISAC at www.cisecurity.org
- We continue to recommend the E-ISAC as the trusted source of public power utility's ICS threat information.
- Developing a program for **Shared Cybersecurity Services**
  - Joint Action Agency model as a framework to possibly provide a shared cyber analyst
  - Mature organizations mentoring others
  - Concise threat feed in our Secure Trusted Community (STC) network

Acknowledgment: *These activities are based upon work supported by the Department of Energy under Award Number DE-OE0000811.*

Additional Cybersecurity Resources

- **Cybersecurity Scorecard**
  - 261 public power utilities
- **Cybersecurity Roadmap**
  - Helps you develop an action plan
- **Incident Response Playbook**
  - Cyber Mutual Aid
  - Shared cyber resources
- **Cybersecurity Training**
  - We bring training to you
- **Secure Information Sharing**
  - Weekly Situation Report (new)





Resources page:
www.publicpower.org/gridsecurity

Nathan Mitchell
Sr. Director of Cyber and Physical Security Services
American Public Power Association
2451 Crystal Dr., Suite 1000,
Arlington, VA 22202

Direct: 202.467.2925
NMitchell@PublicPower.org

cybersecurity@publicpower.org