Cybersecurity Essentials and Management (Energy Sector)

CSP001

Topic 3/10: Energy Sector Threats and Vulnerabilities

PRESENTATION BY: STYLIANOS KARAGIANNIS (PDMFC, PORTUGAL)

Cyberattacks on Energy

Cyberattacks on Energy

Introduction to Cybersecurity in the Energy Sector

- The energy sector, including electricity generation, transmission, and distribution, is considered critical infrastructure.
- As the sector increasingly adopts digital technologies for monitoring, control, and automation, it becomes more susceptible to cyber threats.
- A successful cyberattack on energy infrastructure could lead to power outages, disruption of essential services, and even physical damage to equipment.

Common Cybersecurity Threats

Common Threats

- **Malware:** Examples include Stuxnet, a sophisticated malware that targeted SCADA systems, and NotPetya, a destructive ransomware that caused widespread damage to energy companies.
- **Ransomware:** In 2019, the city of New Orleans declared a state of emergency after a ransomware attack disrupted its computer systems, including those used for managing its energy infrastructure.
- **Phishing:** Attackers may send emails impersonating legitimate organizations or personnel to trick employees into revealing sensitive information or clicking on malicious links.
- **Social Engineering:** An attacker posing as a technician may gain physical access to critical infrastructure by convincing personnel of their legitimacy through manipulation tactics.

Cyberattacks on Energy

Energy Sector Specific Threats

Energy Sector Threats

- **Attacks on SCADA Systems:** The Dragonfly (aka Energetic Bear) and Havex (aka Ekans) cyber espionage campaigns targeted SCADA systems used in energy infrastructure for espionage and potential sabotage purposes.
- **Attacks on Smart Grids:** In 2020, the US Cybersecurity and Infrastructure Security Agency (CISA) issued an advisory warning of ongoing cyber threats targeting organizations in the energy sector, including those involved in smart grid technologies.
- Black Energy is a sophisticated malware toolkit associated with cyberattacks targeting the energy sector, particularly in Ukraine. Black Energy establishes communication channels with remote servers controlled by attackers, allowing for remote command execution and data exfiltration.

Black Energy

Details on the Techniques

- Step 1: Initial Intrusion: Exploits a backward-compatibility setting in Windows 7 and later to bypass default User Access Control (UAC) settings.
- Step 2: Communication with C2 Server: Communicates with its Command and Control (C2) server over HTTP, using web protocols for data exchange.
- Step 3: Autostart Execution: Drops its main DLL component and creates a .lnk shortcut to that file in the startup folder, ensuring automatic execution upon system boot.
- Step 4: Exploitation and Persistence: Creates a new service using either a hard-coded or randomly generated name, ensuring persistence by modifying system processes.
- Step 5: Reconnaissance and Data Gathering: Gathers credentials from web browsers like Firefox, Google Chrome, and Internet Explorer, extracting sensitive information for further exploitation.

Black Energy

Details on the Techniques

Technique ID	Descripion
T1548.002	BlackEnergy attempts to bypass default User Access Control (UAC) settings by exploiting a backward-compatibility setting found in Windows 7 and later.
T1071.001	BlackEnergy communicates with its C2 server over HTTP.
T1547.001	The BlackEnergy 3 variant drops its main DLL component and then creates a .lnk shortcut to that file in the startup folder.
T1547.009	The BlackEnergy 3 variant drops its main DLL component and then creates a .lnk shortcut to that file in the startup folder.
T1543.003	One variant of BlackEnergy creates a new service using either a hard-coded or randomly generated name.
T1555.003	BlackEnergy has used a plug-in to gather credentials from web browsers including FireFox, Google Chrome, and Internet Explorer.

Sandworm Team

Overview

- **Background:** Sandworm Team is a highly sophisticated cyber threat group attributed to Russia's GRU Unit 74455. Active since at least 2009, Sandworm Team is known for its destructive cyber operations targeting various sectors globally.
- **Notable Attacks:** 2015 and 2016 attacks against Ukrainian electrical companies and government organizations, resulting in power outages and disruptions.
- Some operations conducted by Sandworm Team involved collaboration with APT28 (also known as Fancy Bear or Strontium), another Russian threat group affiliated with GRU Unit 26165.

Thank you

Presenter: Stylianos Karagiannis (PDMFC, Portugal)

Please send all questions to:
stylianos.karagiannis@pdmfc.com