Western Interconnection Cyber Security and Mission Assurance

Part I: Western Interconnection Cyber Threat Landscape

Jayden Lyons

CYBR370

Norwich University

03/07/2020

Executive Summary

Ensuring the safety and security of the Western Interconnection power grid is a foremost priority due to a disturbing trend in cyberattacks targeting vital industrial infrastructure and a rapidly evolving cyber threat landscape. Attacks aimed at disrupting or destroying the Western Interconnection power supply may occur as a direct physical attack against the grid or a cyberattack exploiting the digital systems controlling the Western Interconnection. Nearly 20% of the entire North American population rely on electricity generation and transmission from the Western Interconnection. Significant cyberattacks on industrial systems around the world in recent years have raised the stakes for industrial control system cybersecurity. In addition, Western Interconnection cyber security concerns include new vulnerabilities created by the integration of evolving technologies in industrial power systems such as IT-integrated operational technology, insecure IoT devices, poorly configured vendor and supply chain technology, and a significant expansion of Internet connections.

This report summarizes the current cyber threat and cyber security environment for industrial control systems and provides guidance and recommendations for an effective security architecture to protect the Western Interconnection power system. The single greatest threat to U.S. critical infrastructure is a sophisticated cyberattack capable of corrupting safety controls, remotely controlling system processes, damaging, disrupting or disabling vital infrastructure in the energy sector. However, a strong cyber security posture that optimizes the role of people, technology, and operations is the best defense against evolving cyber threats and will ensure the safety and reliability of industrial systems in the United States.

The Western Interconnection power grid is one of three main interconnections that supply electricity to the continental United States. The Western Interconnection operates independently and facilitates the distribution of electric power to 14 states on the west coast serving a U.S. population of over 80 million. The Western Interconnection is a complex physical grid consisting of 136,000 miles of transmission lines, operated and controlled by 34 balancing authorities and 500 companies in the U.S., providing all of the electric, natural gas, hydroelectric, nuclear, wind, and solar power for the Western region. Industrial Control System (ICS) networks manage the production and distribution of electricity through a network of power plants, distribution substations, and electronic devices and controls (Congressional Research Service, 2018). Though the Western Interconnection is historically very reliable, the network is vulnerable to significant failures due to natural, operational, man-made events and evolving cyber threats (Congressional Research Service, 2018). A sophisticated cyberattack via malware disseminated in an ICS network may result in catastrophic loss of life, damage and destruction of the public utilities system, and remote control of critical system operations by foreign adversaries.

Internet of Things (IoT) devices connected to an ICS network represent an evolving ICS security vulnerability as well. Attackers are increasingly targeting IoT devices to gain access to an ICS network, launch denial of service attacks and other malicious payloads. The introduction of digital smart grid technology developed to modernize grid operations also represents a potential ICS security vulnerability. Along with the proposed benefits of advanced operational technology (OT) and improved grid

efficiency comes the potential risks associated with increasing the number of information technology (IT) controls connecting industrial processes to the Internet.

Adversarial threats to an ICS network can arise from a variety of sources including terrorist groups to disgruntled employees to foreign state-sponsored hackers. The Western Interconnection power grid represents a large-scale and ambitious target, most likely requiring an attacker to have nation-state level technical skills, an in-depth understanding of ICS engineering and processes, and considerable confidence to even attempt. The Western Interconnection would not be an attractive target for attackers seeking to steal data, spy on communications, or leverage monetary payment. Without an obvious financial or espionage angle, the attacker’s intent is most likely to disrupt an ICS process thereby compromising the grid’s operation. The targeting of critical infrastructure to disrupt, degrade, or destroy systems is consistent with numerous attacks engaged in by Russian, North Korean, and Iranian nation state actors, and intrusions of this nature may be with immediate intent or in preparation for a contingency (Johnson et al, 2017). Considering the level of expertise and resources required to carry out an attack of this nature, an advanced persistent threat (APT) group with unlimited financial resources and full support of a foreign nation-state represents the highest priority adversary.

APT groups are highly skilled in deploying both traditional and advanced malware, social engineering attacks, and strategic web compromise. APT groups are the most dangerous type of adversary because they are prepared to invest an unlimited amount of time and resources to develop the necessary sophisticated attack tools and to achieve the objective mandated by their government (Chapple & Seidl, 2015). APT groups also have very little risk aversion because they are essentially carrying out the orders of their government with the expectation they will be protected by their nation-state and thus are confident in their ability to avoid detection and prosecution.

A state-sponsored APT group is certainly capable of carrying out an attack on the Western Interconnection power grid by deploying, for example, Industroyer, a devastating new strain of ICS malware specifically designed to target power grids. Cybersecurity experts suspect Industroyer code was utilized in a 2016 cyberattack on an electrical substation in Ukraine (Paganini, 2017). Analysis of Industroyer code revealed an advanced malware featuring multiple backdoors enabling remote control and execution, at least 4 payloads enabling circuit breaker control, a denial of service (DOS) attack against protection relays, and a wiping tool to cover their tracks and make it difficult to restore systems (Paganini, 2017). The creators of Industroyer are more advanced and went to great lengths to create malware capable of directly controlling ICS switches and circuit breakers (Paganini, 2017). Industroyer malware can be installed in a network covertly via human error, phishing or social engineering lure, malicious insider threat, security gap, or remote access trojan among other methods. Upon accessing the network, a launcher is installed through a backdoor, which initiates the malicious payloads and wiper while the command and control server is hidden in the Tor network on the dark web.

The new class of ICS malware including Industroyer is designed to cause maximum mayhem and destruction of industrial systems such as Western Interconnection power grid. Most industrial networks lack even basic security such as access control, network monitoring, threat detection, security logging and auditing, and this is the larger problem facing ICS networks (Perelman, 2018). The figure below applies the cyber kill chain to the Industroyer attack and summarizes the steps an APT group would likely take to intrude on an ICS network to achieve their objectives.

A screenshot of a cell phone

Description automatically generated

Figure 1.1 Industroyer Cyber Kill Chain

In order to combat the cyber kill chain and thwart cyberattacks as early in the process as possible, industrial networks need the harden ICS security and develop an incident response plan for early detection, restoration of compromised systems, and to mitigate any disruption of the Western Interconnection. The diagram below illustrates the steps taken to eradicate Industroyer malware.

A close up of text on a white background

Description automatically generated

Figure 1.2 ICS Malware Containment and Removal Process