Risk Mitigation Consulting Inc.

Intelligence and Analysis Division

WHITE PAPER SERIES

The Increasing Threat to National Energy Grids from Cyberattack

INTENT

This white paper is designed to provide analysis of relevant, publicly available information on threat and hazard events/trends and their potential impacts to the interests of the United States, both at home and abroad. This product is not intended to be an all-encompassing assessment of the subject.

The Increasing Threat to National Energy Grids from Cyberattack

Introduction

Over the past two years the cyber sector has increasingly become a target for cyberattacks. Globally, cyberattack-induced blackouts have occurred only twice. Hackers have successfully penetrated several nations' energy grids on multiple occasions, and cyberthreats occur on a daily basis. Critical infrastructure cyberattacks are "one of the most serious national security challenges we must confront," according the Department of Homeland Security (DHS). |DHS warns that a large cyberattack could threaten "U.S. lifeline networks, critical defense infrastructure, and much of the economy; it could also endanger the health and safety of millions of citizens." [3]

Between 2011 and 2014, electric utilities reported 362 physical and cyberattacks that caused outages or other power disturbances to the U.S. Department of Energy. Of those, 14 were cyberattacks and the rest were physical in nature. While the Department of Energy received only 14 reports of cyberattacks from utilities over the past four years, other reporting systems show rising cyberthreats. The branch of DHS that monitors cyberthreats received reports of 151 "cyber incidents" related to the energy industry in 2013 — up from 111 in 2012 and 31 in 2011. It is uncertain whether the increase is due to more incidents or an increase in reporting.[3]

Potential Attack Effects

Because the nation's electrical grid operates as an interdependent network, the failure of any one element requires energy to be drawn from other areas. If multiple parts fail at the same time, there is the potential for a cascading effect. Should hackers successfully target just a few key power plants across the country, the national electric grid may be disrupted for days, weeks, or longer. In August 2003, a sudden blackout wiped out power across seven Northeastern states and Ontario. A software glitch, human error, and a tree branch caused a chain reaction of power outages. A 2013 study of the outage estimated that it caused 90 excess deaths in New York City alone because of air pollution and sweltering summer heat. Even though there was no significant damage to infrastructure connected to the 2003 blackout, it took at least six hours and as much as two days to return electric service to the affected areas.[4]

Cyberattacks Methods

Attempted and successful cyberattacks have used a variety of methods to gain access to critical industrial control systems. Hackers have created highly targeted email messages containing fake résumés laced with malicious code for control engineering jobs and sent them to the senior industrial control engineers who maintain broad access to critical industrial control systems. Once the recipients clicked on those documents, attackers could steal their credentials and proceed to other machines on a network. In some cases, the hackers also compromised legitimate websites that they knew their victims frequented — something security specialists call a watering hole attack. And in others, they deployed what are known as man-in-the-middle attacks in which they redirected their victims' internet traffic through their own machines. Documented attack methods include: Open Source Reconnaissance, Spear-phishing Emails, Watering-hole Domains, Host-based Exploitation, Industrial Control System Infrastructure Targeting, and Ongoing Credential Gathering.[6]

Case Studies

Several nations' energy grids have been targeted and breached by cyberattacks. This is not an all-inclusive list.

Ukraine: December 2015

A successful attack on the Ukrainian National Power Grid was the first major assault on a nation's power grid and the first confirmed hack to take down a power grid. Several reports have indicated that the hack was planned for several months, as the hackers studied the network and gained access to operator credentials. A telephone flood and custom-built malware attacked several power companies in the Ukraine and caused blackouts in the Ivano-Frankivsk, Horodenka, Kalush, Dolyna, Kosiv, Tysmenytsia, Nadvirna, and Yaremche regions. To help it pass through security shields and maximize its damage, the malware attack was also timed with a telephone flood that targeted support departments of the electricity companies keeping most of their staff busy. The power wasn't out long in Ukraine: just one to six hours for all the areas hit. But more than two months after the attack, the control centers were still not fully operational.[2]

Ukraine: December 2016

Hackers used malicious malware to target employees, sending e-mails that allowed them to steal login credentials and shut down substations. This attack, unlike the first, was fully automated. The attack resulted in 75 minutes of darkness in parts of the city of Kiev, taking out 200 megawatts of capacity—about 20 percent of the city's nighttime energy consumption. Power was restored 45 minutes after personnel switched equipment from automatic to manual mode, and 75 minutes after the blackout started. This was the second ever attack to take out a nation's power grid.[1]

Ireland: April 2017

EirGrid, the company that manages Ireland's electric grid, was targeted by "state-sponsored" hackers, leaving its network exposed to attack. The original breach took place on April 20 and lasted just short of seven hours. The hackers used a virtual wiretap to access unencrypted communications sent to and from EirGrid in the UK, Wales, and Northern Ireland. The breach was discovered 3 months later, in July, but it is unknown if any malicious software was installed onto EirGrid's control systems. A breach of the system could result in power outages across Ireland.[8]

United States: 2017 DHS, FBI Report

The Department of Homeland Security and Federal Bureau of Investigation warned in a report that the nuclear, energy, aviation, water and critical manufacturing industries have been targeted along with government entities in attacks dating back to at least May. According to the report, hackers had succeeded in compromising some targeted networks. The objective of the attackers is to compromise organizational networks with malicious emails and tainted websites to obtain credentials for accessing computer networks of their targets.[9]

United States: 2018 DHS, FBI Report

"Since at least March 2016, Russian government cyber actors ... targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors," according to the report. Since May, hackers have been penetrating the computer networks of companies that operate nuclear power stations and other energy facilities, as well as manufacturing plants in the United States and other countries. According to the report, the attacks most often targeted specific people — industrial control engineers who have direct access to systems that, if damaged, could lead to an explosion, fire or a spill of dangerous material.[6]

2017 Symantec Report

According to Symantec, the hacking group dubbed Dragonfly started targeting western energy-sector companies, including in the U.S., Turkey and Switzerland in 2011. They describe Dragonfly as interested in both learning how energy facilities operate and also gaining access to operational systems themselves, to the extent that the group now potentially has the ability to sabotage or gain control of these systems should it decide to do so. Symantec has strong indications of attacker activity in organizations in the U.S., Turkey, and Switzerland, with traces of activity in organizations outside of these countries. The U.S. and Turkey were also among the countries targeted by Dragonfly in its earlier campaign, though the focus on organizations in Turkey does appear to have increased dramatically in this more recent campaign.[7]

Mitigation

As nations and hacker groups seek to penetrate energy grids, it is vital that the United States push to prevent such an attack, strengthen the cyber security of critical infrastructure, and prepare to respond to a successful cyberattack. According to a report released by the Congressional Research Service (CRS) in March 2018, since 2014, "security risks to the power grid have become an even greater concern in the electric utility industry." The CRS assess that the power industry "has not necessarily reached the level of physical security needed based on the sector's own assessments of risk." The report also shows that in the three years since federal overseers implicated a series of new standards for physical security of grid locations, the industry has worked to improve its defenses but has struggled to implement all of the government's recommendations. For example, manual backup functionality isn't present at many power grid control systems in the U.S. Ukraine was able to circumvent the malware that left many of their substations unresponsive to remote commands by utilizing manual methods to issue commands. Should an automated station without manual backup be affected by a cyberattack, it may be much harder to restore power.[5]

The DoD is working on an automated system to speed up recovery time to a week or less — what it calls the Rapid Attack Detection, Isolation, and Characterization (RADICS) program. The RADICS program is intended to detect early warning signs and distinguish between attacks and normal outages, pinpoint the access point of the attack and determine what malicious software was used, and include an emergency system that can rapidly connect various power-supply centers, without any human coordination.[10]

Source List

1. MIT Technology Review. *Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks*. 22 December 2016.
   Wired. *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*. 3 March 2016.
2. USA Today. *Bracing for a Big Power Grid Attack*. 24 March 2015.
3. USA Today. *Power Grid Security Fears Surge Since 2003 Blackout*. 24 March 2015
4. Congressional Research Service. *NERC Standards for Bulk Power Physical Security: Is the Grid More Secure?* March 2018.
5. New York Times. *Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say*. 6 July 2017.
6. Symantec. *Dragonfly: Western Energy Sector Targeted by Sophisticated Attack Group*. 20 October 2017
7. Irish Independent. *'State-Sponsored' Hackers Targeted Eirgrid Electricity Network in 'Devious Attack.'* 30 March 2018.
8. Reuters. *U.S. Warns Public About Attacks on Energy, Industrial Firms*. 21 October 2017.
9. Vocativ. *Military Is Ramping Up Preparation for Major U.S. Power Grid Hack*. 18 April 2017.