PEPPERDINE UNIVERSITY

Pepperdine Policy Review

Volume 16 Article 1

4-23-2024

A Case Study of Russian Cyber-Attacks on the Ukrainian Power Grid: Implications and Best Practices for the United States

Miles Pollard
Pepperdine University, miles.pollard@yahoo.com

A Case Study of Russian Cyber-Attacks on the Ukrainian Power Grid: Implications and Best Practices for the United States

Miles Pollard

School of Public Policy, Pepperdine University

Abstract

This paper examines the rise of cyber warfare affecting power grid security, focusing on the vulnerabilities exploited in the Ukrainian power grid infrastructure by programs like BlackEnergy and CRASHOVERRIDE. It extends this analysis to similar vulnerabilities that may be in critical command and control systems of the United States' power grids. The Sandworm and Electrum cyber-attacks on Ukraine's grid are dissected, revealing the escalating threat to industrial control systems.

Detailed exploits of the Radmin command-and-control software such using the plugin tool Mimikatz with NTLM and Kerberos for static and dynamic analysis, the CVE-2008-3431 DSEFix exploit, and the Win32/SSHBearDoor trojan are analyzed, alongside the unique nature of the Russian TDoS attacks and the use of KillDisk software. In the context of the United States cyber-energy policy, the paper highlights key initiatives like NERC's bi-annual GridEx preparedness exercise, the CRISP public-private information sharing program, the American Public Power Association’s cybersecurity scorecard, and the NIST Cybersecurity framework. Emphasis is placed on the importance of application whitelisting, multi-factor authentication, proactive use of the Yara forensic tool, and SIP server rate limiting as defensive measures.

The paper concludes by underscoring the evolving capabilities of foreign adversaries, the ambiguity in interpreting the scope and intent of cyber-attacks, and the necessity of a robust combination of intelligence, governmental, and civilian cyber capabilities to defend power grids against threats from nation-states and cybercriminals.

Keywords: Sandworm, Electrum, BlackEnergy, CRASHOVERRIDE, Cyber Policy, Energy Policy

A Case Study of Russian Cyber-Attacks on the Ukrainian Power Grid: Implications and Best Practices for the United States

The United States has entered a new Cold War. This Cold War, unlike its previous iteration of kinetic proxy conflicts, is happening every day in the cybersphere as the internet becomes a ubiquitous part of everyday life. As utilities use remote access tools like Shodan over the internet, nonstate actors and antagonistic nation states exploit such weakness for political and material advantages. While Russia has launched kinetic attacks into the sovereign nation of Ukraine in a bid to reclaim their previous provinces under the guise of protecting the ethnic Russians in the region, Russia has also engaged in invisible attacks, but no less deadly, have been conducted against Ukraine. In fact, Ukraine suffered from multiple attacks after the annexation of Crimea in 2014 but before the ongoing war in 2023.

On December 23, 2015, and December 17, 2016, online agents called Sandworm, which is associated with Russia, targeted the Ukrainian power grid by disabling the substations responsible for providing electricity to localities. While Ukraine is a special case given their use of old Soviet equipment, these cyber-attacks conducted against Ukraine exemplify the nascent domain of cyber warfare and the need for states to harden their power grids. Furthermore, earlier attacks like Stuxnet laid the groundwork for hacks targeting industrial processes and utility providers. Specifically, Stuxnet infiltrated the Siemens command and control software that Iran's nuclear enrichment program used and destroyed their enrichment centrifuges in 2011. (Lee et al., 2017)

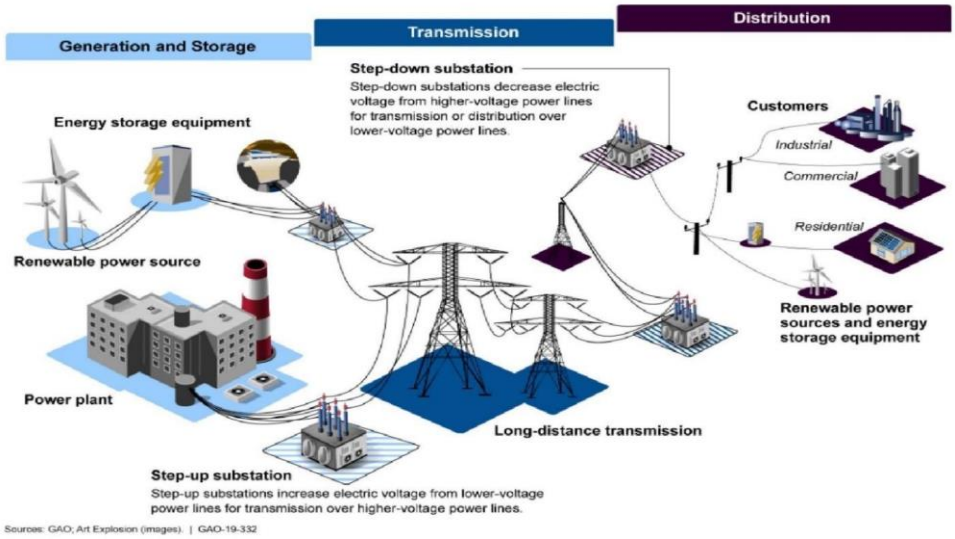
Risk Assessment

Since the Stuxnet attack, a myriad of groups have analyzed the possibility of attacking critical command and control systems used in operating power grids in the intervening years. Three broad areas of the power grid can be targeted: Generation, transmission, and distribution.

Bulk power generation can be targeted by infiltrating power plants and disabling or destroying electrical production equipment like generators. In fact, the United States performed such an attack as a part of the Aurora experiment to bring attention to the vulnerabilities of an unprotected system (Greenburg, 2020).

Figure 1

Critical Infrastructure Protection



Source: U.S. Government Accountability Office, 2019.

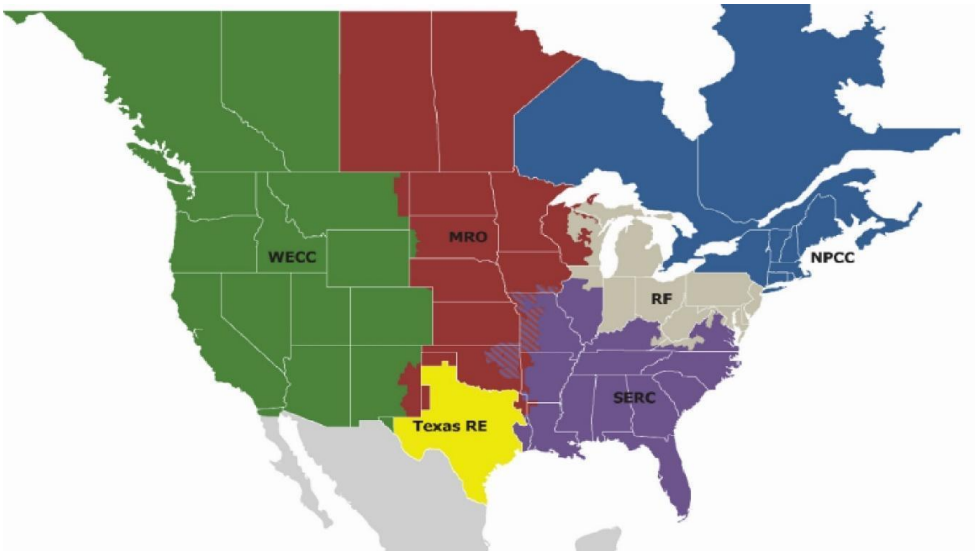
Other areas include transmission and distribution vulnerabilities. Often, command and control centers for one or all of these areas will be targeted. If the goal is destruction, generation is often chosen as transmission and distribution systems have automatic trips that will shut down if too much voltage is running through them. However, interfering with the signals sent between the three systems can cause power generators to send large amounts of electricity down the power lines which can overload breakers in a synchronized attack.

The United States has created its power grid not with security in mind but with practicality. While all power grids fall under the Federal Energy Regulatory Commission, they

are further broken down into six regions that have limited levels of interconnection (Gramlich, 2021). These regions have negotiating power to arrange pricing and serve a geographically similar consumer base. Below this regional organization are entities called “balancing authorities” who coordinate the day-to-day operations of most plants and maintain a constant supply of power to the populace. Additionally, electrical disturbances have been tracked by the Department of Energy to ascertain the causes of power outages.

Figure 2

Federal Energy Regulatory Commission Regions

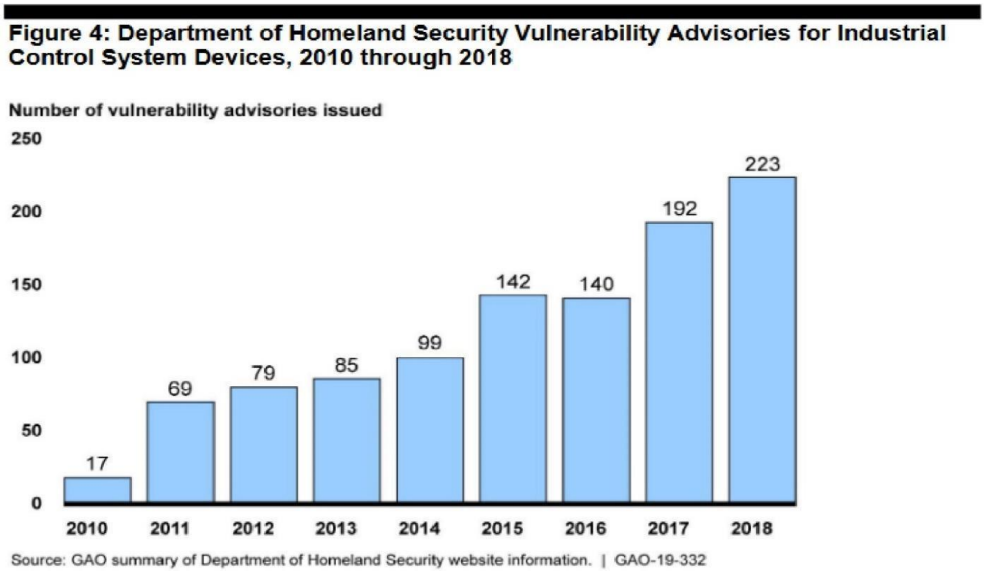


Source: North American Electric Reliability Corporation, 2022.

There have been 38 documented accounts of cyber-electrical disturbance events in the United States since 2002 with most not causing any outages (Office of Cybersecurity, Energy Security, and Emergency Response, 2022). These events may be conducted to conduct harm or simply to engage in espionage. The Department of Homeland Security has been issuing an increasing number of security vulnerability advisories each year, with 223 such advisories being issued in 2018.

Figure 3

Vulnerability Advisories for Industrial Control System Devices



Source: U.S. Government Accountability Office, 2019.

Therefore, it behooves the United States and policy analysts to learn from previous attacks on power grids. The most prominent examples come from Ukraine as it has been engaged in both kinetic and cyber conflict with Russia since the seizure of Crimea in 2014. These attacks, orchestrated by hacking groups Sandworm and Electrum, have been the most prominent examples of how power grids can be disrupted, and while the results may have been temporary, they may foretell how a full-fledged cyber-attack on power grids may occur in the future.

2015 Sandworm Attack on Ukraine

According to analysts at ESET, a software security firm located in Slovakia, the Sandworm attack started with a spear-fishing campaign on the corporate employees of power companies encouraging them to open emails with a Word, Excel, or PowerPoint attachment (Cherepanov & Lipovsky, 2016a). Though they tried a variety of attacks, Sandworm's most prominent tactic was pretending to be the Minister of Industrial Policy of Ukraine. In this attack,

they encouraged workers to update their passwords if they contained words inside the attached Word document (Cherepanov & Lipovsky, 2016). Inside this attachment was a macro that served as a vector to install a computer toolkit called BlackEnergy 3. This toolkit, unlike its previous iterations, has a specific functionality that is designed to infiltrate normal worker computer systems and spy without being detected.

Using these subtle tools, BlackEnergy 3 allowed Sandworm to discern the habits of the individuals who work on the computer by analyzing the logs of bootups and shutdowns. These plug-ins access file system operations and information, passwords, network scanning, windows accounts, system hardware, BIOS, and Windows info as well as creating a parasitic infector, taking screenshots, installing a remote desktop, updating the malware, and destroying the system (Samani, 2018). It also used the powerful capabilities of Black Energy 2 which was first discovered back in 2010 (Cherepanov & Lipovsky, 2014). Perhaps the most important plugin tool utilized is Mimikatz which is often used by legitimate administrators to obtain passwords and hashes from Windows stored memory.

Mimikatz can do this via three methods. The first way is to break the encryption for the Windows Credential Manager which has passwords and other credentials within the manager. Mimikatz can access these credentials by exploiting a vulnerability in the Credential Manager's encryption process by gaining administrative privileges. However, a later analysis by ESET yielded no evidence of escalation, meaning that Sandworm either used another vulnerability or had some ability to cover the trail of admin escalation (Cherepanov & Lipovsky, 2016).

The second method involves Mimikatz using the command "sekurlsa::logonpasswords" to extract the encryption key. To do this, it performs both a static and a dynamic analysis. In static analysis, it uses predefined parameters to hunt for information encrypted using either New

Technology Local Area Network Manager (NTML) or Kerberos. Despite its name, NTML was invented in the early 1990s and is not particularly well suited to encryption in the modern era. NTML uses hashing which is a type of challenge-response protocol where a client must present a hashed response that corresponds to the password on the file.

Notable weaknesses to hashing include brute force attacks which send multiple hashes until it finds the correct answer and man-in-the-middle attacks that involve a 3rd party pretending to be the server or client to receive the correct password. Additionally, Mimikatz can use the "sekurlsa::wdigest" command to bypass these protocols altogether if the machine uses Windows 7 or older. Once authenticated, a hacker can “pass-the-hash” to gain admin privileges. In the case of Mimikatz rewriting the hash to one that only Mimikatz generated and has access to, the process is called “overpass-the-hash”.

While Kerberos is a more updated encryption system that is harder to break, Mimikatz uses a command called "sekurlsa::tickets" to extract the tickets, and other authentication information, from Kerberos. While static analysis sends pre-defined data structures into the memory to root out information, dynamic analysis utilizes other tools. Under dynamic analysis, Mimikatz intercepts the authentication information, or tickets, from Kerberos by injecting a Dynamic Link Library (DLL) into the Local Security Authority Subsystem Service (LSASS) process. DLL is a highly desirable program to modify because it is a component highly shared among many subsystems and gets regular updates that can be spoofed. The downside is that the regular updates can disrupt any existing exploits. When successfully hacked, this exploit is called “pass-the-ticket” which is comparable to NTML’s “pass-the-hash” exploit.

Lastly, Mimikatz can intercept network traffic interception to extract password credentials. This is typically done by infiltrating the Server Message Block (SMB) which is used

to share information over a network which is comprised of computers, printers, or other such hardware. Mimikatz uses a DLL such as when infiltrating Kerberos to run one of two actions. Either it modifies the list of DLLs that are normally used by the hardware to only use the Mimikatz DLL or to use a function called CreateRemoteThread API which adds the Mimikatz to the list of DLL code. Utilizing at least one of these abilities, Sandworm was able to recreate the administrative privileges if an admin had ever logged into the device.

To bypass Windows 64-bit security on the compromised Windows server, Sandworm used the BlackEnergy 2 toolkit's kernel-mode driver. However, gaining entry to the system required a valid signature and a reboot. To overcome these obstacles, Sandworm modified DSEFix, a program that leverages an exploit called CVE-2008-3431 to override the security signature requirement and disables the need for a reboot (Cherepanov & Lipovsky, 2016). Once inside the system, Sandworm would sometimes remain inactive, waiting for the right moment to act. Moving around large amounts of data or accessing other servers would increase the risk of discovery. To avoid detection, Sandworm created a unique command and control server on each computer within the compromised network, enabling them to remain on the undetected servers even if one of them is found. In the case of discovery, Sandworm created a backdoor using the Win32/SSHBearDoor trojan (Cherepanov & Lipovsky, 2016).

However, this tactic was merely the first step for Sandworm because they had only infiltrated the corporate side of the company. Sandworm wanted to gain credentials to access the system that controlled the actual electrical grid. Rather than using a brute force attack that would be more noticeable, they quietly observed their targets and used their control of servers to impersonate the administrative personnel that had access to the supervisory control and data acquisition (SCADA) system (Buchanan, 2022). Their main goal was to find out which users had

remote access to the actual electrical side of the company and forge their credentials. Once they had access to the Windows Domain controllers for the whole command and control center, Sandworm could finally start targeting the electrical grid (Zetter, 2016b).

Sandworm likely exploited the Russian Famatech software called Radmin that the command-and-control centers were using to remotely access all of their substations (Cherepanov & Lipovsky, 2016) Once they had full access to the Radmin software, Sandworm carefully planned and executed their five-pronged attack. They likely chose the late afternoon on December 23 specifically as this would be the time when day workers would be transitioning out while the night shift for Christmas Eve would be coming in.

First, Sandworm used its remote access privileges to open all the power breakers to overload the grid. Workers, tired from a full day of work and looking forward to a night with their families during the holidays, watched helplessly as the cursors moved from breaker to breaker. The workers frantically tried to regain control before being logged out. However, neither day nor night workers could even log in because all their passwords had been changed. Opening all the breakers, which are supposed to impede and regulate electrical flow, would cause a surge of electricity to be sent down the power lines and damage the power grid's infrastructure by overloading and taxing the generators and burning out the transmission network.

Second, Sandworm used the remote management interface to target the uninterruptible power supply (UPS) that was supposed to provide backup power in case of emergencies (CISA, 2021a). This not only caused damage to the power grid infrastructure but also had a psychological impact as the UPS was used to provide power to the actual power grid command-and-control center (Buchanan, 2022). The attack affected two out of the three command-and-

control centers, leaving confused technicians fumbling around in the dark with phones and flashlights, trying to understand what was going on.

Third, Sandworm disabled the serial-to-ethernet converters at over 30 substations. In effect, this firmware attack effectively bricked the converters requiring permanent replacement (Buchanan, 2022). Additionally, because these converters were in substations in remote areas, it was difficult for workers to access and replace them so that the command centers could remotely control the electrical flow to these far-off regions. Since Sandworm had already opened all the breakers, they had no use for the substations and wanted them open as long as possible to short out or trip them offline. In order just to understand what was going on and eventually restore power, the befuddled workers were required to manually go to the physically remote substations to check readouts and communicate back to the command-and-control center to restore power (Zetter, 2016b). However, Sandworm anticipated this reaction.

Fourth, Sandworm began a telephone denial-of-service (TDoS) attack on the command-and-control centers (Assante, 2016). This TDoS attack involved phone calls ranging from a variety of localities providing misleading information as to the extent of the power outages. Sandworm accomplished this by flooding a session initiation protocol (SIP) server that is used to establish and manage communications sessions over the internet. It drowned out the real phone calls coming from consumers who were reporting factual information. Some have argued that the source of these attacks was from Moscow (Zetter, 2016b). Others at ESET, however, claim that for $50 individuals operating on some dark websites will conduct the calls themselves (Cherepanov & Lipovsky, 2016). Another confounding factor is that the calls can come from abroad and be spoofed to appear that they are coming from specific localities via the use of virtual private networks (VPNs) (Zetter, 2016a).

Lastly, Sandworm devised a method of further slowing down the manual restart of the power grid. To do this, they utilized a program called KillDisk (Buchanan, 2022). Approximately 90 minutes after the attack when Sandworm knew that the administrators, technicians, and engineers would be scrambling to restore power manually, they set off a time bomb with the KillDisk program. The program has several methods of disrupting the computer network that it is on. It can wipe a whole disk of important system files by randomizing the data, making recovery impossible (Cherepanov, 2016b). Additionally, it can partition a disk and override the master boot record which prevents the operating system from initializing the computer (Zetter, 2016b).

Similar attacks that wiped computers have been used by North Korea and Iran in their sabotage operations (Buchanan, 2022). One unique facet of Sandworm's attack, however, was that in at least one case in a remote terminal unit, a human-machine interface (HMI) was overwritten for some unknown reason or perhaps by accident (CISA, 2021a). However, a later report in 2021 by the Cybersecurity and Infrastructure Security Agency (CISA) found BlackEnergy software attacking HMIs like "GE's Cimplicity, Advantech/Broadwin's WebAccess, and Siemens' WinCC" lending credence to the theory of intentional infiltration (CISA, 2021b).

With this five-pronged assault, the energy grids were reduced to manual operations, and workers were forced to replace the equipment damaged in the attack. However, this synchronized attack on multiple power centers only brought down the power grid for one to six hours, depending on location, despite having the capacity to do far worse (Assante, 2016). This suggests that it "may have been meant to signal Russia's capability to attack Ukraine's physical infrastructure, but without doing irreparable damage" (Connell & Vogler, 2017). For example,

there may have been more command-and-control centers that were targeted. According to Nikolay Koval, who was the head of Ukraine's Computer Emergency Response Team during the attack and who currently serves as CEO of Ukrainian cyber security firm Cys Centrum, six other companies serving six other regions could have been attacked as well but managed to mitigate the damage before it caused outages for consumers (Zetter, 2016a).

Implications

This attack may have been in response to an attack in the Crimea region perpetrated by pro-Ukrainian separatists (Luhn, 2015). The separatists are alleged to have knocked out power for two million Crimean residents as well as the key naval base at Sevastopol; however, this explanation does not account for the fact that the power stations and command-and-control centers were beginning to be hacked in March of 2015 (Zetter, 2016b). However, they may have merely been prepping the attack waiting for a politically expedient event to occur. It is also worth noting that the attack could have been much larger in scope which may suggest a rushed attack, although this is unlikely given the level of preparation and patience already undergone; additionally, it could have been a warning to Ukraine that Sandworm has the sophistication to do much more and has operated within key utilities for months without getting caught (Buchanan, 2022).

With regards to the United States, the same serial-to-Ethernet converters that Ukraine utilized are being utilized within the US grid (Zetter, 2016b). Additionally, the United States has relied on its ability to automate much of its electrical grid to maximize efficiency. In some cases, the United States is unable to restore power manually as the analog controls have been replaced with solely digital ones (Zetter, 2016a). Admiral Rodgers who oversaw Cyber Command in 2016 feared what cyber tools sophisticated actors like Russia could use to infiltrate the US (Rogers,

2016). In fact, Ukrainian media organizations talking about the recent elections in the Donbas region were attacked with similar attacks using KillDisk software during this time (Cherepanov, 2016a). This means that similar media organizations in the US could be struck in order to influence election outcomes or punish certain types of reporting.

2016 Electrum Hack on Ukraine

On December 17, 2016, Electrum, which likely has some human operators pulled from the Sandworm team, is suspected of using a new program to knock out the Ukrainian Ukrennegro power station called CRASHOVERRIDE which attacked the plant's highly automated control systems (Buchana, 2022). The program seemed to be based on the Havex code, which was used to spy on industrial sites using open platform communications (OPC). Unlike previous versions, this code did not require tailoring the program to a single vendor allowing access to various components even if they were sourced from different companies (DRAGOS, 2023). However, unlike the Dragonfly campaign that focused on espionage with this software, Electrum would use it solely for offense. As in the 2015 Sandworm hack, Electrum used BlackEnergy, which has already been explored in detail in the previous section, in a far more refined and targeted way to achieve the desired results (Buchanan, 2022).

As mentioned above, in the 2015 hack the exploitation of HMIs allowed for rapid analysis of industrial control systems to plan the attack and did not necessitate months of data collection. DRAGOS, an information technology company that often works with ESET, confirmed that the hackers used a TOR VPN by backtracking the nodes that were active during the attack (DRAGOS, 2023). First, CRASHOVERRIDE infiltrates the industrial control system, creates a backdoor using a hard-coded proxy address, and then leaves a time bomb with a data wiper module similar to KillDisk that will detonate after one or two hours. To wipe the data, the

wiper zeros all the registry keys, which initializes the systems, and then masquerades as the control system (DRAGOS, 2023).

Similar to Sandworm's five-pronged attack, Electrum would conduct a three-pronged attack. After taking over the control system, CRASHOVERRIDE would open and close breakers to disrupt electricity flow and follow that up with the second attack with the wiper component that used the timed detonation to erase Windows files that were critical to remotely reset the breakers. However, the third phase of the attack did not occur as planned as it failed to disable the protective relays that would prevent an overload in the grid which severely limited the scope of the attack (Buchanan, 2022). Interestingly, while Electrum managed to disrupt the reporting status of the protective Siemens SIPROTEC relays, it did not turn them off suggesting they either made a careless mistake or intended to do so for some type of signaling purposes (DRAGOS, 2023).

Implications

The 2016 Electrum hack has left some analysts perplexed. While it is true that the attack was far more refined and quickly carried out, it did not have the same impact as the 2015 hack with power being restored to the single station rather quickly. Perhaps it was a proof of concept to train a new team, a quick demonstration by Russia to frustrate Ukraine near the holidays when the last attack happened, or maybe it was a signal to the rest of the world that Russia had a tool that targeted OPC and could quickly and easily attack control systems using any type of vendor components (Buchanan, 2022). One thing is certain; cyber-attacks that are limited in scope are often difficult to interpret, perhaps by design.

Analysis of Best Practices

Officially, the Department of Energy was given responsibility for "collaborating with critical infrastructure owners and operators in the energy sector, identifying vulnerabilities, and helping to mitigate incidents" via Presidential Policy Directive 21 (GAO, 2021). Additionally, they are to work with the Department of Homeland Security (DHS) to implement remedial measures and help harden the energy grid. DHS contains the Cybersecurity and Infrastructure Security Agency (CISA) which provides a variety of recommendations to utilities and other professionals of which offensive elements to keep track of. This helps patch their defenses to protect critical systems. As evidenced by the evolution of Sandworm's BlackEnergy into the adaptable CRASHOVERRIDE software, offensive cyber capabilities are rapidly advancing and, in some cases, outpacing defenses.

While the variety of offensive cyber capabilities is quickly mounting, there are solutions to counter these threats. As described in the 2015 Sandworm attack, hackers likely breached the defenses on the company side by using embedded macros in Word, Excel, PowerPoint, and other applications that can access personal data (Constantin, 2015). Therefore, both those working on the corporate side and those who are working in sensitive control areas should be mandated to follow strict hygiene practices of only enabling documents that they are expecting and can validate by email signature and a quick personal message.

The DoE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) has created a cybersecurity risk information sharing program called CRISP as a pilot program (Office of Cybersecurity, Energy Security, and Emergency Response, 2023). This public-private partnership is designed to provide the government with the necessary information to determine what types of attacks are being used against power generation organizations. Organizations receive a catalog of the data as well as actionable alerts on what practices might best be used to

mitigate future attacks. National Laboratories use this information to construct hypothetical scenarios and track likely avenues of assault to better prepare the collective power grid apparatus from organizations like Sandworm and Electrum. In 2022, CRISP expanded its membership by 14% to almost 1,600 members and provided 90 intelligence briefings and 230 analytical products to its members (NERC, 2023).

Enrolling in such a program may be beneficial as around 54% of those surveyed by Siemens in 2019 expected some type of cyberattack to befall their critical infrastructure within the next year (Arampatzis, 2021). It may be necessary to expand such a program to include the distribution and transmission organizations because they are particularly vulnerable because of their regular use of remote access features and their connections to business networks (GAO, 2022).

One key practice recommended by CISA is using application whitelisting, especially for static systems like database servers and HMI computers (CISA, 2021a). Whitelisting, as opposed to blacklisting, which is only useful for blocking known threats, only allows certain programs that are pre-approved to run on that machine. This forestalls many exploits and requires attackers to both know the applications that are whitelisted and somehow trick these computers into thinking that the hackers are using them. This can raise the bar against easy exploits if proper updates are maintained. Additionally, CISA recommends locking down any ports and devices that are not in use. Using multi-factor authorization should also be required whenever using remote access programs.

According to the GAO, each state should create a commission staffed with dedicated personnel that creates security standards for operators (GAO, 2021). The commission should regularly meet with stakeholders and conduct tabletop exercises of cyber intrusions with a

variety of experts and practitioners. The commission would also work with universities to develop cybersecurity courses for these utility professionals. For better standard practices, the commission could enforce the usage of the DoE's Cybersecurity Capability Maturity Model, the American Public Power Association's cybersecurity scorecard self-assessment, and the NIST Cybersecurity framework to assess readiness in the case of an attack. Furthermore, mandating participation in the bi-annual GridEx preparedness exercise with the North American Reliability Organization (NERC) and the Department of Energy should prepare the utility operators and pre-condition them for a real attack. Any resulting suggestions or lessons learned need to also apply to both bulk power producers and distribution command and control systems.

In one particular case, the GAO is particularly concerned. As the United States adopts more microgeneration capabilities with residential solar power being sold back into the grid, this trend magnifies the issues regarding securely regulating the power grid. Distribution systems for these solar generators could be hacked as, "for instance, an attacker may instruct compromised solar inverters to inject power into the grid to cause voltage and stability issues, potentially resulting in a power outage" (GAO, 2021). Firmware updates sent out from solar companies to their distribution system are also a vector for potential adversaries to exploit. Additionally, many distribution systems utilize GPS which can be jammed or spoofed, which can disrupt both time and electrical synchronization) (GAO, 2021).

To protect from TDoS attacks like those in the 2015 Sandworm hack, organizations can use filtering and rate-limiting traffic to an always updated SIP server (Brooks, 2023). Rate limiting traffic sets a maximum limit on the amount of SIP calls that can be sent from an IP address which limits automated TDoS attacks. Additionally, having backups of critical systems, regularly patching vulnerabilities, limiting their remote connections, closely monitoring those

remote connections that are necessary, aggregating login information, and scanning networks regularly against baselines utilizing the YARA forensic tool can protect the power grid (Lee, Assante, & Conway 2018). Lastly, the Council on Foreign Relations recommends that FEMA create a formalized response plan in the case of such an attack, that NERC mandate the retention of manual operations to restore the power grid in the case of emergency, and that a tax credit should be extended to utilities to spend on cybersecurity (Knake, 2017).

Conclusion

The power grid attacks on Ukraine have provided ample evidence of the mounting cyber threat to industrial control systems. Whether it is the generation, transmission, or distribution of power, the loss of electricity in the modern economy has devastating consequences for both production and security. During outages, not only do factories and offices lose operations causing losses in worker productivity but also water treatment facilities and hospitals become unable to provide for citizens, which can cause massive health outbreaks. Given the rising number of cyber intrusions and the complicated nature of the power grid, the United States has tasked many agencies to analyze these current threats and the fallout from such attacks. Foreign adversaries such as Russia may utilize such attacks in the event of kinetic conflict rendering the subject particularly critical to American foreign policy.

Starting with the base of the Stuxnet virus and continuing with BlackEnergy and CRASHOVERRIDE, Russia has proven that they have the capabilities to rapidly improve their cyber exploits to cause lasting damage to an enemy’s power grid. However, cyber-attacks are not as easily interpreted as conventional strikes due to the nature of how the automated programs operate. Was an attack limited by the hackers’ ability to adequately model and design around a

control system, or was it deliberately limited to show a calibrated attack that hints at the further capability if used in a serious confrontation?

The United States can take prudent measures to mitigate the chances of a cyber intrusion and respond rapidly to such an event. Using digital hygiene practices like avoiding enabling macros and using two-factor authentication represent low hanging fruit for a utility company to implement. Whitelisting only necessary programs and restricting network traffic can protect the power grid from easy exploits and TDoS attacks. Additionally, enrolling in the CRISP or similar programs to report information to federal agencies as well as regularly engaging in tabletop exercises can prepare a company for when a cyber intrusion does happen.

Though the nature of decentralized power grids may provide challenges to the industry, securing the generation, transmission, and distribution of power is of critical national importance. No longer can the United States rely on its two oceans to protect it in this new cyber domain. The threats range from nation-states to cyber criminals alike; however, the United States can fend off these threats through the use of its intelligence apparatus and the diligent exercise of its government and civilian cyber capabilities.

References

Arampatzis, A. (2019). “Is the Electric Grid Ready to Respond to Increased Cyber Threats?” Tripwire, October 23, 2019. https://www.tripwire.com/state-of-security/electric-grid-ready-increased-cyber-threats.

Assante, M. (2016). “Confirmation of a Coordinated Attack on the Ukrainian Power Grid.” SANS Industrial Control Systems Security Blog | Confirmation of a Coordinated Attack on the Ukrainian Power Grid | SANS Institute, January 6, 2016. https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid/.

Brooks, C. (2023). “3 Alarming Threats to the U.S. Energy Grid – Cyber, Physical, and Existential Events.” Forbes. Forbes Magazine, February 17, 2023. https://www.forbes.com/sites/chuckbrooks/2023/02/15/3-alarming-threats-to-the-us-energy-grid--cyber-physical-and-existential-events/?sh=7c8e267101a1.

Cherepanov, A. & Lipovsky, R. (2016). “BlackEnergy - What we really know about the notorious cyber attacks.” Virus Bulletin. ESET, October 2016. https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Cherepanov-Lipovsky.pdf.

Cherepanov, A. & Lipovsky, R. (2014). “Last-Minute Paper: Back in Blackenergy: 2014 Targeted Attacks in the Ukraine and Poland.” Virus Bulletin :: Last-minute paper: Back in BlackEnergy: 2014 targeted attacks in the Ukraine and Poland, September 25, 2014. https://www.virusbulletin.com/conference/vb2014/abstracts/back-blackenergy-2014-targeted-attacks-ukraine-and-poland.

Cherepanov, A. (2016a). "Blackenergy by the SSHBEARDOOR: Attacks against Ukrainian News Media and Electric Industry." WeLiveSecurity, January 3, 2016. https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric-industry/.

Cherepanov, A. (2016b). "The Rise of Telebots: Analyzing Disruptive KillDisk Attacks." WeLiveSecurity, December 13, 2016. https://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/.

Constantin, L. (2015). "Macro-Based Malware Is Making a Comeback, Researchers Warn." Computerworld. IDG News Service, January 7, 2015. https://www.computerworld.com/article/2866055/macro-based-malware-is-making-a-comeback-researchers-warn.html.

CISA. (2021a). Cybersecurity and Infrastructure Security Agency. "Cyber-Attack against Ukrainian Critical Infrastructure: CISA." Cybersecurity and Infrastructure Security Agency CISA, March 4, 2021. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.

CISA. (2021b). Cybersecurity and Infrastructure Security Agency. "Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)," March 4, 2021. https://www.cisa.gov/news-events/ics-alerts/ics-alert-14-281-01e.

DRAGOS. (2023). "CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations." DRAGOS. Accessed April 13, 2023. https://www.key4biz.it/wp-content/uploads/2017/06/CrashOverride-01.pdf.

"Electric Disturbance Events (OE-417) Annual Summaries"(2023). Office of Cybersecurity, Energy Security, & Emergency Response. oe.netl.doe.gov. Accessed April 13, 2023. https://www.oe.netl.doe.gov/OE417_annual_summary.aspx.

Greenberg, A. (2020). “How 30 Lines of Code Blew up a 27-Ton Generator.” Wired, October 23, 2020. https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/.

Knake, R. K. (2017). “A Cyberattack on the U.S. Power Grid.” Contingency Planning Memorandum 31. Council on Foreign Relations, April 2017. https://cdn.cfr.org/sites/default/files/pdf/2017/03/ContingencyPlanningMemo31_Knake.pdf.

Lee, R. M, Assante, m. J., & Conway, T. (2018). “Analysis of the Cyber Attack on the Ukrainian Power Grid,” *Electricity Information Sharing and Analysis Center*, March 18, 2018, pp. 1-29, 24-25.

Luhn, A. (2015). “Crimea Declares State of Emergency after Power Lines Attacked.” The Guardian. Guardian News and Media, November 22, 2015. https://www.theguardian.com/world/2015/nov/22/crimea-state-of-emergency-power-lines-attacked.

NREC. (2023). North American Electric Reliability Corporation. “Annual Report 2022.” NERC, February 2023. https://www.nerc.com/news/Pages/NERC-Publishes-2022-Annual-Report-.aspx.

Office of Cybersecurity, Energy Security, and Emergency Response. (2023). “Cybersecurity Risk Information Sharing Program (CRISP).” Department of Energy . Accessed April 13, 2023. https://www.energy.gov/sites/default/files/2021-12/CRISP%20Fact%20Sheet_508.pdf.

Rogers, M. (2016). “Statement of Admiral Michael S. Rogers Commander United States Cyber Command Before the Senate Armed Forces Committee.” Senate Armed Forces Committee,

April 5, 2016. https://www.armed-services.senate.gov/imo/media/doc/Rogers_04-05-16.pdf.

Samani, R. (2018). "Updated Blackenergy Trojan Grows More Powerful." McAfee Blog, March 21, 2018. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/updated-blackenergy-trojan-grows-more-powerful/.

GAO. (2019). U.S. Government Accountability Office. "CRITICAL INFRASTRUCTURE PROTECTION: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid." GAO, August 2019. https://www.gao.gov/assets/710/701114.pdf.

GAO. (2021). U.S. Government Accountability Office. "ELECTRICITY GRID CYBERSECURITY: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems," March 2021. https://www.gao.gov/assets/720/713257.pdf.

GAO. (2022). U.S. Government Accountability Office. "Securing the U.S. Electricity Grid from Cyberattacks," April 14, 2022. https://www.gao.gov/blog/securing-u.s.-electricity-grid-cyberattacks.

Zetter, K. (2016a). "Everything We Know about Ukraine's Power Plant Hack." Wired, January 20, 2016. https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/.

Zetter, K. (2016b). "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." Wired, March 3, 2016. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.