DRAGOS

North American Electric Cyber Threat Perspective

January 2020

Summary

The electric utility industry is a valuable target for adversaries seeking to exploit industrial control systems (ICS) and operations technology (OT) for a variety of purposes. A power disruption event from a cyberattack can occur from multiple components of an electric system including disruptions of the operational systems used for situational awareness and energy trading, targeting enterprise environments to achieve an enabling attack through interconnected and interdependent IT systems, or through a direct compromise of cyber digital assets used within OT environments. Attacks on electric systems – like attacks on other critical infrastructure sectors – can further an adversary's criminal, political, economic, or geopolitical goals. As adversaries and their sponsors invest more effort and money into obtaining effects-focused capabilities, the risk of a disruptive or destructive attack on the electric sector significantly increases.

The number of publicly known attacks impacting ICS environments around the world continues to increase, and correspondingly the potential risk due to a disruptive cyber event impacting the North American electric sector is currently assessed as high. This report highlights multiple threats and adversaries focusing on critical infrastructure and their capabilities. Dragos anticipates the threat landscape associated with the sector will remain high as the detected intrusions continue to rise.

Of the activity groups that Dragos is actively tracking, nearly two-thirds of the groups performing ICS specific targeting and disruption activities are focused on the North American electric sector. Additionally, existing threats to ICS are expanding and establishing new interest in electric utility operations in North America. For example, the Dragos tracked activity group XENOTIME – the most dangerous and capable activity group – initially focused its targeting efforts on oil and gas operations before expanding to include North American electric utilities. Dragos also identified the MAGNALLIUM activity group expanding targeting to include electric utilities in the US. This activity group expansion and shift to the electric sector coincided with increasing political and military tensions in Gulf Coast Countries (GCC).

Dragos research of the CRASHOVERRIDE attack indicates ELECTRUM targeted recovery operations. Such activity, if successful, could prolong outages following a cyberattack and cause physical damage to equipment or harm to operators. These findings suggest the group had greater ambitions than what it achieved during its 2016 attack, and represent worrying possibilities for safety and protection-focused attacks in the future.

Historically, adversaries have demonstrated the capabilities to significantly disrupt electric operations in large-scale cyber events through specialized malware and deep knowledge of targets' operations environments. Although North America has not experienced similar attacks, ICS-targeting adversaries exhibit the interest and ability to target such networks with activities that could facilitate such attacks.

The electric sector, as a whole, has been working for over a decade to address cyber threats through board level decisions,[1] preparedness exercises like GridEx, the NERC CIP standards, and direct investment in ICS-specific security technologies. However, adversaries will continue to evolve and the industry must be ready to adapt.

This report provides a snapshot of the threat landscape as of January 2020 and is expected to change in the future as adversaries and their behaviors evolve.

Key Findings

- The threat landscape focusing on electric utilities in North America is expansive and increasing, led by numerous intrusions into ICS networks for reconnaissance and research purposes and ICS activity groups demonstrating new interest the electric sector.
- Attacks on electric utilities can have significant geopolitical, humanitarian, and economic impact. Thus, state-associated actors will increasingly target power and related industries like natural gas to further their goals.
- One significant threat includes active supply chain compromises by activity groups targeting original equipment manufacturers, third-party vendors, and telecommunications providers.
- Research into the 2016 CRASHOVERRIDE attack demonstrates the adversary's intent and ability to target protection and safety operations to cause prolonged outages, equipment destruction, and human health and safety concerns.
- Utilities are slowly improving visibility in electric operational environments, and current regulatory standards in North America ensure the electric power sector maintains a minimum level of cybersecurity for all of the in-scope facilities. Further recommendations are included in this report for asset owners and operators to address cyber risk in their operations environment.
- The complete "energy infrastructure sector" (electric, oil and gas, etc) of all countries are at risk as companies and utilities are facing multiple global adversaries. Cyberattacks are an increasing means to project dominance using cyberattacks in the energy domain.

Activity Groups

Dragos tracks seven activity groups[2] targeting electric utilities in North America, and 11 total groups. Dragos does not perform state or actor attribution of activity groups and none should be implied.

---

[1] https://dragos.com/wp-content/uploads/yir-execs-2018.pdf

[2] Dragos categorizes ICS-targeting activity into activity groups based on observable elements that include an adversary's methods of operation, infrastructure used to execute actions, and the targets they focus on. The goal, as defined by the Diamond Model of Intrusion Analysis, is to delineate an adversary by their observed actions, capabilities, and demonstrated impact– not implied or assumed intentions. These attributes combine to create a construct around which defensive plans can be built. At this time, two activity groups possess ICS-specific capabilities and tools to cause disruptive events: XENOTIME and ELECTRUM.

PARISITE targets utilities, aerospace, and oil and gas entities. Its geographic targeting includes North America, Europe, and the Middle East. PARISITE uses open source tools to compromise infrastructure and leverages known virtual private network (VPN) vulnerabilities for initial access. The scope of this group's targeting also includes government and non-governmental organizations. This group has operated since at least 2017 based on infrastructure Dragos identified. Dragos intelligence indicates PARISITE serves as the initial access group and enables further operations for MAGNALLIUM.

Links[3]: MAGNALLIUM

XENOTIME is known for its TRISIS attack which caused the disruption at an oil and gas facility in the Kingdom of Saudi Arabia in August 2017. It was specially tailored to interact with Triconex safety controllers and represented an escalation of ICS attacks due to its potential catastrophic capabilities and consequences. In 2018 XENOTIME activity expanded to include electric utilities in North America and the APAC region; oil and gas companies in Europe, the US, Australia, and the Middle East; as well as devices beyond the Triconex controllers. This group also compromised several ICS vendors and manufacturers, providing a potential supply chain threat.[4]

Links: Temp.Veles[5]

[3] Links means that there are technical overlaps or assessments made from other entities that provide some connection to the groups; however this is not to imply that there is a one to one relationship to these groups and they should not be considered aliases.
[4] https://dragos.com/resource/xenotime/
[5] https://attack.mitre.org/groups/G0088/

MAGNALLIUM has targeted energy and aerospace entities since at least 2013. The activity group initially targeted an aircraft holding company and oil and gas firms based in Saudi Arabia, but expanded their targeting to include entities in Europe and North America. In the fall of 2019, following increasing tensions in the Middle East, Dragos identified MAGNALLIUM expanding its targeting to include electric utilities in the US. MAGNALLIUM appears to still lack an ICS-specific capability, and the group remains focused on initial IT intrusions.[6]

Links: APT 33, Elfin[7], PARISITE

DYMALLOY is a highly aggressive and capable activity group that has the ability to achieve long-term and persistent access to IT and operational environments for intelligence collection and possible future disruption events. The group's victims include electric utilities, oil and gas, and advanced industry entities in Turkey, Europe, and North America.[8] In recent months, Dragos has identified this actor expanding its targeting to include the APAC region based on newly identified malware samples.

Links: Dragonfly 2.0, Berserk Bear[9]

ELECTRUM currently focuses on electric utilities and mostly targets entities in Ukraine. It is responsible for the disruptive CRASHOVERRIDE event in 2016.[10] This group is capable of developing malware that can modify electric equipment processes, leveraging ICS protocols and communications.

Links: SANDWORM[11]

---

[6] https://dragos.com/resource/magnallium/
[7] https://attack.mitre.org/groups/G0064/
[8] https://dragos.com/resource/dymalloy/
[9] https://attack.mitre.org/groups/G0074/
[10] https://dragos.com/resource/anatomy-of-an-attack-detecting-and-defeating-crashoverride/
[11] https://attack.mitre.org/groups/G0034

RASPITE targets electric utilities in the US and government entities located in the Middle East. Dragos also identified additional victims in Saudi Arabia, Japan, and Western Europe, but has not identified new RASPITE activity since mid-2018.[12]

Links: Leafminer[13]

ALLANITE targets business and ICS networks in the US and UK electric utility sectors. The group maintains performs reconnaisance in operational environments to potentially stage disruptive events. There is no indication ALLANITE has a disruptive or damaging capability or intent at this time.[14]

Links: PALMETTO FUSION,[15] Dragonfly 2.0, Berserk Bear

COVELLITE compromised networks associated with electric energy, primarily in Europe, East Asia, and North America. The group has not shown an ICS-specific capability at this time. While technical activity linked to COVELLITE behaviors exist in the wild, there has been no evidence or indications this group remains active from an electric-targeting perspective.[16]

Links: Lazarus Group,[17] WASSONITE

CHRYSENE developed from an espionage campaign that first gained attention after the destructive Shamoon cyberattack in 2012 that impacted Saudi Aramco. The activity group targets petrochemical, oil and gas, and electric generation sectors. Targeting has shifted beyond the group's initial focus on the Gulf Region and the group remains active and evolving in more than one area.[18]

Links: APT 34, GREENBUG, OilRig[19]

---

[12] https://dragos.com/resource/raspite/
[13] https://attack.mitre.org/groups/G0077/
[14] https://dragos.com/resource/allanite/
[15] https://www.us-cert.gov/ncas/alerts/TA17-293A
[16] https://dragos.com/resource/covellite/
[17] https://attack.mitre.org/groups/G0032
[18] https://dragos.com/resource/chrysene/
[19] https://attack.mitre.org/groups/G0049/

HEXANE targets oil and gas and telecommunications in Africa, the Middle East, and Southwest Asia. Dragos identified the group in May 2019. HEXANE operations rely on malicious document files to drop malware on victim machines, from which HEXANE can then proceed to further goals in the target network.[20]

Links: CHRYSENE, OilRig

WASSONITE targets electric generation, nuclear energy, manufacturing, and research entities in India, and likely South Korea and Japan. The group's operations rely on DTrack malware, credential capture tools, and system tools for lateral movement. WASSONITE has operated since at least 2018.

Links: Lazarus Group, COVELLITE

Threats to Energy Infrastructure

As evidenced by the expansion of oil and gas targeting adversaries XENOTIME and MAGNALLIUM into the electric sector, there is a growing trend of threat proliferation across critical infrastructure sectors. That is, threats to one ICS entity are potential threats to other industrial verticals. Adversaries are increasingly targeting multiple verticals with purposes including espionage, information gathering, and potentially disruptive events.[21]

This trend is driven by multiple variables including an increasing investment to develop offensive capabilities specifically for ICS-targeting operations. Attackers are obtaining the skills necessary for a cyber-physical event as greater attention is paid to ICS in general and as open-source information on industrial networks, protocols, and devices becomes more widely available. Additionally, the spread of commodity IT hardware and software into OT networks increases the attack surface, providing ingress opportunities via techniques familiar to the adversary.

Therefore, all energy-related entities should be familiar with malicious activity across critical infrastructure sectors.

Overview of the North American Electric System

The phrase “electric grid” as a single entity is a bit of a misnomer. The way power is generated, transmitted, and distributed across North America is best described as an electric *system*: the Bulk Electric System. The

[20] https://dragos.com/resource/hexane/
[21] https://dragos.com/blog/industry-news/threat-proliferation-in-ics-cybersecurity-xenotime-now-targeting-electric-sector-in-addition-to-oil-and-gas/

system is complex, resilient, and segmented. The North American Bulk Electric System is broken down into four Interconnections, the Eastern, Western, Texas, and Quebec Interconnections.[22]

Certain electric power entities in the United States must adhere to mandatory cybersecurity standards under authority from the Federal Energy Regulatory Commission (FERC) and established by the North American Electric Reliability Corporation (NERC). These Critical Infrastructure Protection (CIP) Reliability Standards have several requirements for in-scope facilities and systems across Bulk Electric System (BES). These regulations are also used outside of the United States across North America. Each Canadian province adopts the standards for their utilities and the Mexican regulator, Comisión Reguladora de Energia (CRE),works with NERC on reliability efforts and defines cybersecurity rules for their country.[23] The NERC CIP Reliability Standards are seperated into several topic areas, outlined below:

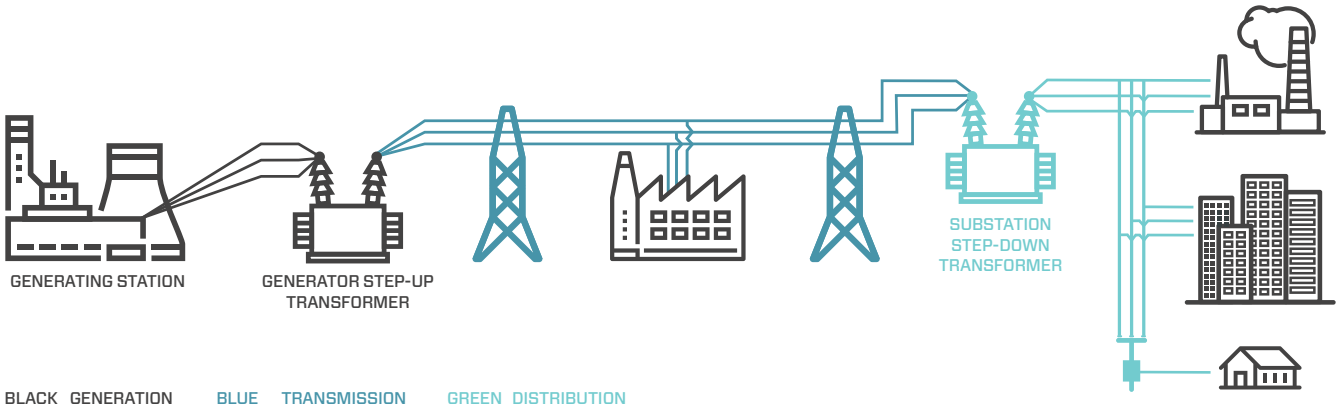
CIP-002-5.1	Bulk Electric System (BES) **Cyber System Categorization**
CIP-003-6	Security Management Controls
CIP-004-6	Personnel & Training
CIP-005-5	Electronic Security Perimeter(s)
CIP-006-6	Physical Security of BES Cyber Systems
CIP-007-6	System Security Management
CIP-008-5	Incident Reporting and Response Planning
CIP-009-6	Recovery Plans for BES Cyber Systems
CIP-010-2	Configuration Change Management and Vulnerability Assessments
CIP-011-2	Information Protection
CIP-014-2	Physical Security

A new standard, CIP-013 on supply chain cyber risk management, will be mandatory in July 2020. There are periodically updates to the NERC CIP Reliability Standards based on FERC rulemakings or industry efforts to address new topic areas or requirements.

Adhering to cybersecurity regulations makes North American electric utilities unique in the ICS industry by ensuring a minimum level of cybersecurity best practices are maintained.

[22] https://www.eia.gov/todayinenergy/detail.php?id=27152
[23] https://www.ferc.gov/CalendarFiles/20180731083631-Madrigal,%20CRE.pdf

Electric Power Operational Segments Threat Perspective



Electricity goes through multiple stages in the creation, transportation, and delivery of power to a customer. Electric power is generated from energy sources like fossil fuels, nuclear power, or renewables at power generation facilities commonly referred to as power plants. The transmission system then carries electricity across long distances from the generation power plants to distribution substations. From there it is distributed to customers. The transmission and distribution systems include substations to transform voltage levels, serve as switching stations, and provide electric power to consumers.

Generation

Threat Landscape

At this time, Dragos assesses at least three activity groups demonstrate the intent or capability to infiltrate or disrupt electric power generation operational networks. XENOTIME has demonstrated the capability to access, operate, and conduct attacks in an industrial environment. Dragos assesses this group would be capable of refocusing its disruptive efforts on electric utilities since it has already affected safety instrumented systems, in the Triconex, which are a mainstay in power generation. Additionally, DYMALLOY targeted generation facilities and demonstrated the ability to obtain screenshots of sensitive ICS data including screenshots of human machine interfaces (HMIs). ALLANITE poses a threat to generation as it shares some similarities in targeting and capabilities with DYMALLOY along with proven reconnaissance and exfil of sensitive data from operational environments. Neither group has demonstrated ICS-disruptive or destructive capabilities, as they focused on operational environment reconnaissance.

Assessment

At this time, ICS-targeting adversaries have not successfully disrupted electric generation operations in North America, however, we do note a communications disruption that was reported to NERC earlier this year. The

observed threat activities targeting this segment, including obtaining documentation on sensitive operations networks, could be used for espionage purposes or to facilitate a disruptive attack.

Transmission

Threat Landscape

ELECTRUM is a well-resourced activity group with demonstrated capabilities to disrupt power transmission. Dragos has identified connections between ELECTRUM and SANDWORM but note they are uniquely different.

SANDWORM served as the likely initial access vector to enable another, ICS-specific entity, ELECTRUM, to conduct a sequenced, ICS-specific attack aimed at physical process destruction in the CRASHOVERRIDE malware[24] attack on 17 December 2016 in Kiev, Ukraine. It impacted 200MW of load at a transmission substation. The malware was highly tailored to deenergize a transmission-level substation by opening and closing circuit breakers and switchgear, devices responsible for balancing power across the electric system, and ensuring operator, power line, and equipment safety. The attack demonstrated a deep understanding of the transmission environment and industrial protocols in use, enabling the adversary to customize malware for the specific target.

A recent Dragos report published in August describes ELECTRUM's attempts to disrupt protective relays to create an unsafe, unstable condition for reconnected transmission lines at the moment of physical restoration.[25] This suggests the attack could have caused much more significant – and dangerous – consequences including equipment destruction, extended outages, and operator injury. Although the protection-focused piece of the attack failed, it could act as a blueprint for future electric-targeting adversaries attempting to disrupt operations and cause the greatest possible damage.

Assessment

While this attack occured in Europe, the CRASHOVERRIDE framework would be trivial to modify in order to attack North American electric infrastructure. The intent to modify the framework has not been observed to date. Additionally, Dragos' research suggests concerning ambitions for ELECTRUM: causing a physically-destructive event during restoration operations, a consequence not seen in previous attacks. North American electric utilities should consider ELECTRUM to be a serious threat and be prepared to identify similar behaviors, including abuse of native functionality to and from ICS equipment.

Distribution

Threat Landscape

In the current threat landscape, one adversary group has disrupted electric distribution operations. The first-ever blackout caused by a cyberattack took place in Ukraine on 23 December 2015. The attackers leveraged malware to gain remote access to three electric power distribution companies, control distribution

[24] ESET originally identified CRASHOVERRIDE and named it Industroyer https://www.eset.com/int/industroyer/
[25] https://dragos.com/resource/crashoverride-reassessing-the-2016-ukraine-electric-power-event-as-a-protection-focused-attack/

management systems, and disrupt electricity to around 230,000 people.[26] Power was fully restored after several hours.

Robert M. Lee, CEO of Dragos and one of the leads on the investigation of the 2015 cyberattack on Ukraine's distribution electric system, attributed this attack to SANDWORM which was later confirmed by iSight.[27]

ASSESSMENT

Although adversaries have not disrupted electric distribution operations in North America, the behaviors and tool use exhibited by activity groups including SANDWORM and ELECTRUM could be deployed in electric distribution facilities within North America. The adversary in the 2015 Ukraine electric sector attacks did not use ICS-specific malware, rather controlled operations remotely via existing tools in the operations environment.

Disrupting electric power through cyber means at any point throughout generation, transmission, and distribution requires an adversary to have a fundamental understanding of the enterprise and operations environments, equipment used, and how to operate specialized equipment. Because an adversary must spend a long time within the target environment learning the required skills to successfully disrupt electric power, defenders have multiple points of opportunity along the potential attack chain to detect and eliminate adversary access.

Regional Assessment[28]

North America

Seven of 11 tracked activity groups target North American electric entities: PARISITE, XENOTIME, DYMALLOY, ALLANITE, MAGNALLIUM, RASPITE, and COVELLITE.

Dragos identified a recent increase in activity targeting North American electric entities, led by the identification of PARISITE activity targeting known VPN vulnerabilities, and MAGNALLIUM password spraying campaigns[29] focusing on oil and gas that expanded to include the electric sector. MAGNALLIUM's increased activity coincides with rising escalations between the US and allies, and Iran in the Middle East.[30] Dragos expects this activity to continue.

Additionally, XENOTIME activity enabling potential supply chain compromise could affect entities in North America. Compromising ICS hardware and software vendors poses a threat to all ICS entities regardless of region due to global production and distribution.

---

[26] https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
[27] https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
[28] Dragos does not perform attribution on threats. However, when other third-parties perform attribution, especially government entities, we document this for others if it is of interest. It is our position that this style of attribution is not valuable from a network defense perspective and thus Dragos does not spend resources on performing this action internally.
[29] https://www.wired.com/story/iran-apt33-industrial-control-systems/
[30] https://dragos.com/blog/industry-news/rising-cyber-escalation-between-us-iran-and-russia-ics-threats-and-response/

In June 2019, public reporting described US cyber efforts and capabilities focused on Russia's electric system.[31] Following a report in the New York Times, Russian officials said US meddling in the country's power system could lead to "cyberwar."[32] Given the increasing tensions and divisive rhetoric around cyber capabilities targeting electric systems, North American asset owners and operators should be aware of the potential increased risk to electric operations.

It is unknown what, if any, impact the 2020 US federal elections may have on cyber threats to the North American electric system. But, major elections continue to play a significant role in cyber operations and this upcoming event cannot be ignored by any critical infrastructure sector.

Dragos continues to track phishing campaigns targeting North American electric utilities, with all activity generally focused on initial access operations. Since April 2019, over a dozen US-based electric utilities received spearphishing emails spoofing licensing and certification bodies with the intent to deliver LookBack malware. The security firm Proofpoint first publicly reported this campaign.[33] Asset owners and operators should ensure employees are trained to identify phishing attempts and report to security personnel when observed.

6 Concerning and Possible Attack Scenarios for North American Electric

1. Destructive Event Causing Power Outage

As evidenced by the disruptive attacks on electric power in Ukraine, it is possible for adversaries to infiltrate operations environments and leverage a deep understanding of a target's network to facilitate a potentially disruptive or destructive attack. Dragos assesses adversaries interested in ICS are likely investing time and resources into developing ICS-specific capabilities.

ELECTRUM's activities targeting transmission operations indicate an intent to cause physical destruction during power restoration by attempting to disable protective relays.[34] If executed correctly, such an event would cause a prolonged power outage, severely hamper restoration, and potentially cause physical harm to operators and equipment.

A disruptive electric sector cyber event has not been observed in North America, however Dragos tracks groups capable of establishing a foothold in operations environments which could lay the groundwork for follow-on disruptive operations.

[31] https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html
[32] https://www.nytimes.com/2019/06/17/world/europe/russia-us-cyberwar-grid.html
[33] https://www.proofpoint.com/us/threat-insight/post/lookback-forges-ahead-continued-targeting-united-states-utilities-sector-reveals
[34] https://dragos.com/resource/crashoverride-reassessing-the-2016-ukraine-electric-power-event-as-a-protection-focused-attack/

2. Third-Party and Original Equipment Manufacturer (OEM) Compromises

Vendors and third-party contractors are essential to enterprise and ICS operations. The numerous vendor or contractor touchpoints within generation, transmission, and distribution can provide an ingress into electric utility environments via compromised or poorly-secured network connections.

Adversaries are increasingly utilizing third-party compromise as a method for affecting intended targets. This attack vector enables an adversary to utilize the implicit trust between companies, suppliers or supporting entities. Dragos has observed multiple adversaries including XENOTIME, DYMALLOY, and ALLANITE leveraging trusted relationships to infiltrate target networks. This includes compromising vendor networks as well as strategic web compromises. VPN appliances are used for remote connections to operations networks, and PARISITE, among other groups, is targeting these connections.

Another attack vector exploited by adversaries is through a managed service provider (MSP). MSPs will typically be embedded within and maintain extensive remote access to client IT and OT networks. Thus, a breach at an MSP can lead to direct access to multiple victim networks. The most extensive operation publicly disclosed was the series of intrusions into MSPs conducted by state-sponsored adversaries, linked in other resources to APT10, announced by the US-CERT in 2018.[35]

Asset owners and operators in North America will need to address these supply chain risks with the mandatory implementation of CIP-013. Using threat information for CIP-013 implementation may benefit asset owners and operators in addressing impactful sector-specific concerns.

3. Systematic Attack on Electricity Generation

Due to the electric sector's reliance on various energy resources, an attacker intent on disrupting electric power operations may target an entity along the supply chain required for producing electricity. For instance, disrupting natural gas pipelines can affect electric generation and downstream natural gas distribution, which has an amplifying effect to the response plans—especially considering the time of year or regional reliance on natural gas.

These can be referred to as a "systematic" attack on the inputs required for energy production along the electric power supply chain. At this time, Dragos has not observed adversary activity relating to systematic attacks or the associated risk.

4. OT Communications Gateways

As evidenced by a recent cyber event disrupting an electric utility's OT communications, attackers can exploit vulnerabilities in the firewalls separating IT systems from OT to impact operations.

A solar generation utility in the US experienced communications outages in March 2019 when an attacker exploited known firewall vulnerabilities to cause unexpected device reboots.[36] The incident caused

[35] https://www.us-cert.gov/ncas/alerts/TA18-276B
[36] https://www.eenews.net/stories/1061421301

communications outages of less than five minutes between field devices at sites and between sites and the control center, according to a NERC report.[37] Dragos intelligence indicates the attacker targeted a known vulnerability in Cisco firewalls.

While the impact was minimal, the activity did affect generation network connectivity for the utility. A longer lasting disruption, or more successful exploitation, could have lead to more severe consequences for the individual utility if the adversary gained a foothold or cut communications completely.

5. Adversary Access Through Cellular or Satellite Connections

As demonstrated by HEXANE activity, telecommunications networks are valuable targets for ICS-targeting attackers. Gaining access to a mobile or satellite network could allow an adversary to interact with power generation facilities that utilize cellular devices or satellite connections, including GPS, for communication, monitoring, time-syncs, and management. Geographically dispersed and remote operations – such as remote substations – often depend on cellular or satellite communication networks. Cellular and satellite network bridges into OT environments need to be closely monitored.

6. Power Outages Provide Adversary Disruption Opportunities

Planned electric outages and maintenance windows can give adversaries insight into a utility's operations and recovery procedures; timing of large-scale outages;[38] and knowledge that anomalous behavior may have a higher likelihood of going undetected during such events.

During initial equipment installation or maintenance windows it is normal for utilities to allow additional external entities into operational environments with USB keys, configuration files, laptops for engineers and vendors, etc. This is a prime opportunity to exploit and infect an OT network purposefully or incidentally. In 2018 Schneider Electric alerted customers that USB sticks, shipped with two Conext products, may have been infected with unidentified malware during manufacturing by a supplier.[39] Although no customers publicly reported incidents of infection in this case, it demonstrates the possibility for attackers to leverage third-party compromise to surreptitiously implant USB malware targeting electric entities. Such an event previously occurred: in 2012, an electric utility experienced a malware infection on its control systems network during planned upgrades, which was distributed accidentally via USB. This caused unexpected downtime and delayed the plant restart for three weeks.[40] This type of attack would also bypass a companies security stack by being placed directly in the operations network.

As extreme weather events increasingly cause electric power companies to schedule mass power outages,[41] more opportunities arise for adversaries to infiltrate networks during times of scheduled blackouts. During planned outages, unusual activity may naturally occur on operations networks allowing

---

[37] https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/20190901_Risks_Posed_by_Firewall_Firmware_Vulnerabilities.pdf
[38] https://www.kron4.com/powershutoffs/pge-power-shutoffs-where-when-next-outages-are-scheduled/
[39] https://www.se.com/ww/en/download/document/SESN-2018-236-01/
[40] https://www.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2012.pdf
[41] https://www.npr.org/2019/10/18/771486828/california-can-expect-blackouts-for-a-decade-says-pg-e-ceo

an adversary to blend-in with other abnormal network traffic. An adversary could also use scheduled blackouts as an opportunity to launch denial of service attacks against a utility's phone system, such as observed in the 2015 Ukraine attacks, to prevent operators from responding to customer issues and undermining public confidence in the utility.

Additionally, natural events are well-known to cause disruptions for physical equipment in the field. Utilities are aware of physical impacts storms have, but fail to add cyber intrusions to any impact analysis, continuity of operations, or disaster recovery methodology. Taking down field devices in the middle of a hurricane is unlikely to cause much alarm and unlikely to be investigated past the usual physical causes. This area is ripe for attackers to go unnoticed and cause lengthy downtimes without arousing suspicions.

Defensive Recommendations

Electric sector asset owners and operators can implement the following host and network based recommendations to improve the defensibility of their OT environments.

- CONSEQUENCE-DRIVEN Identify and prioritize critical assets (crown jewels) and connections, and process consequences of cyberattacks.[42] Perform threat assessments to scope the most impactful risk of disruptive or destructive attacks and use such data to shape threat hunting and defensive postures. While CIP-002 impacts over 1,500 utilities in North America and forces an impact-based discussion of cybersecurity and reliability, that is only from the Bulk Electric System perspective. It is recommended that utilities perform their own consequence-driven analysis for improved security on assets and systems that may impact their operations—and leverage a risk-based security approach outside of NERC CIP programs. Smaller utilities may not have in-scope facilities, yet could have impacts to their local communities (including distribution assets, where there are no NERC CIP requirements).
- THIRD-PARTIES Ensure that third-party connections and ICS interactions are monitored and logged, from a "Trust, but Verify" mindset. Where possible, isolate or create DMZs for such access to ensure that third-party access does not result in complete, unfettered, or unmonitored access to the entire ICS network. Implement features such as jump hosts, bastion hosts, and secure remote authentication schema wherever possible. In-scope systems for the upcoming CIP-013 implementation should leverage an enterprise-wide supply chain risk management program, where appropriate. Dragos recommends using threat information and consequence-driven analysis to address supply chain cyber risk.
- RESPONSE PLANS Develop, review, and practice cyberattack response plans and integrate cyber investigations into root-cause analysis for all events. Especially consider intelligent adversaries which may also attack plans during remediation and response to increase disruption scale and downtime. Where required, consider leveraging CIP-008 and CIP-009 exercises to review the controls and across the entire utility security program to provide additional resilience to utility operations.
- ACCOUNT MANAGEMENT Expanding on the requirements from CIP-007, which applies system security management controls for in-scope BES Cyber Systems, ensure all devices and services do not use

[42] https://dragos.com/resource/dependency-modeling-for-identifying-cybersecurity-crown-jewels-in-an-ics-environment/

default credentials. If possible, do not use hardcoded credentials. Monitor for any hardcoded methods that cannot be removed or disabled. Restrict access to devices to only necessary personnel. Implement the principle of least privilege across all applications, services, and devices to ensure individuals are only able to access the resources needed to perform their duties. This includes ensuring application-layer services including file shares and cloud storage services are properly segmented. Following the Purdue Model, network connections should be terminated before continuing to different levels.

- ACCESS RESTRICTIONS Restrict administrative access within a domain, limit the number of domain administrators, and separate networking, server, workstation, and database administrators into separate organizational units (OUs). Identity is key in defense.
- SEGMENTATION Where possible, segment and isolate networks to limit lateral movement. This can be done most easily with a firewall or access control list (ACL) for companies to virtually segment networks and reduce attack surface while limiting adversary mobility. While CIP-005 provides requirements on creating an Electronic Security Perimeter for in-scope BES Cyber Systems, a similar approach may be useful for smaller utilities and other facilities. Additional guidance from NERC on leveraging firewalls has been released that can be applied regardless of NERC CIP requirements.[43]
- VISIBILITY A comprehensive approach for visibility into ICS/OT environments should be taken to ensure that there is no gap in monitoring. Asset owners and operators and security personnel should work together to gather network and host-based logs starting from the most critical infrastructure, also known as "crown jewels." The ability to identify and correlate suspicious network, host, and process events can greatly assist in either identifying intrusions as they occur, or facilitate root-cause analysis after a disruptive event. Ensure network monitoring of the operations network through ICS-focused technologies.
- ACCESSIBILITY Identify and categorize ingress and egress routes into control system networks. This includes engineer and administrator remote access portals, but also covers items such as business intelligence and licensing server links that need to access IT resources or the wider internet. Limit these types of connections, via firewall rules or other methods, to ensure a minimized attack surface. This approach compliments the requirements of CIP-005, and Dragos recommends considering where to place similar controls outside of NERC CIP compliance programs.
- PUBLIC DATA Assess asset owner hosted, publicly posted information and data that could allow sensitive information to be utilized by an adversary. Work with vendors, contractors, and other to minimize or prevent identification of specific sites, capabilities, or equipment in marketing and related materials. Some data, like regulatory filings, may require working with legal counsel to manage—or at least monitor.
- CONFIGURATION Identify and store "known good" configuration information for ICS devices in non-network accessible locations to provide baselines for comparison as well as restore points in the event of disruption. Update these items frequently to ensure such storage mirrors production environments. This action not only assists recovery in the event of IT malware propagating into ICS networks, but also

[43] *See* NERC Control Systems Security Working Group guideline titled "Control System Electronic Connectivity." This guideline provides a number of examples with variants on the four-legged firewall model. This guideline is not intended to be specific to CIP compliance; rather it is focused on good security practices.

facilitates analysis by providing baselines to compare potentially manipulated configurations against. CIP-010 provides additional context for this approach for in-scope BES Cyber Systems.

- THREAT INTELLIGENCE Use and operationalize ICS-specific threat intelligence. Threat intelligence can enable identification of known threat behaviors. Electric power entities should understand the behaviors and capabilities of activity groups targeting other industrial verticals, such as oil and gas, as these adversaries actively shift and expand targeting to include additional energy sectors. The Dragos Platform incorporates intelligence-driven threat behavior analytics,[44] automating identification of known attacker behaviors. Dragos WorldView Threat Intelligence provides up-to-date intelligence feeds, reports, analysis, and defensive recommendations for new and ongoing threats to oil and gas. The NERC CIP Reliability Standards do not address threat management, which is a mature—but necessary—practice for any security program.
- DEFENSE-IN-DEPTH Design and implement defense-in-depth surrounding ICS networks where security controls and enhanced visibility are applied to hosts capable of handling such tasks. Examples include requiring remote access to flow through a jump-host featuring enhanced Windows and network logging to ensure adequate monitoring of remote access to the control system network. OT cybersecurity requires a strategy specific to the vertical and cannot be a simple extension of the enterprise implementation.
- NETWORK INFRASTRUCTURE ALLANITE and DYMALLOY regularly target routers and switches during compromises, changing configurations to allow for persistent access or delivery of additional malware. Implement router, switch, and firewall configuration baselines and a configuration management program to ensure adversaries do not tamper with configurations and exploit security gaps.

Conclusion

The North American electric sector cyber threat landscape is diverse and active. Activity groups have demonstrated capabilities that could impact operations and network connectivity across operational environments. Electric utilities remain at risk for a disruptive – and potentially destructive – cyberattack due to the political and economic impact such an event may cause.

Although North America has not experienced a disruptive cyberattack to electric system operations and reliability, ICS-targeting adversaries previously demonstrated the capability to disrupt electricity in Europe. With additional resources and retooling, such disruptive methods could potentially be applicable to the North American electric system.

At this time, Dragos has observed adversary activity targeting utility enterprise networks which may enable intial intrusion and reconnaissance at those entity sites. The data gathered and access achieved could facilitate preliminary steps for a potentially disruptive event within the OT environment. Dragos has also observed adversary reconnaissance inside ICS networks.

---

[44] https://dragos.com/blog/industry-news/threat-analytics-and-activity-groups/

The increasing threat of supply chain and third-party attacks is concerning. They provide opportunities for adversaries to compromise operations environments and bypass a utility's security stack over trusted connections. The aforementioned weaponized USB, software updates and maintenance work will also clear most security barriers as the OEMs, maintenance engineers and MSPs are seen as trustworthy and non-hostile. NERC Registered Entities with in-scope systems can take advantage of the recent focus around CIP-013 to create robust supply chain risk management programs focused on both security and compliance objectives across operations.

A disruptive attack would require significant effort to achieve in North America, and as an adversary must spend significant time within compromised networks to learn operations (i.e. dwell time) this provides defenders with numerous opportunities to identify and remove malicious activity prior to disruption. Defenders still maintain the advantage at this time.