Report

GLOBAL ELECTRIC CYBER THREAT PERSPECTIVE

September 2021

DRAGOS, INC.

info@dragos.com

@DragosInc

TABLE OF CONTENTS

SUMMARY

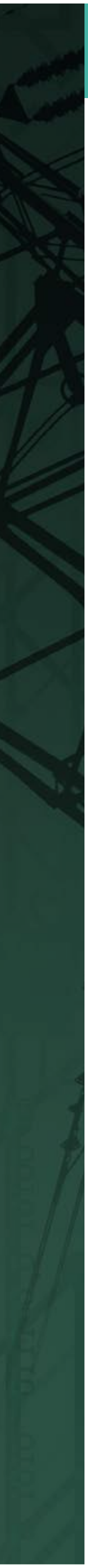
The number of cyber intrusions and attacks targeting the electric sector is increasing from Activity Groups (AG), or threat groups, and from ransomware operations. In 2020, Dragos identified three new AGs targeting the electric sector: TALONITE, KAMACITE, and STIBNITE. Additionally, supply chain risks and ransomware attacks continue to enable intrusions and disruptive impacts on electric utility operations. Of the AGs that Dragos is actively tracking, two-thirds of the groups performing Industrial Control Systems (ICS)-specific targeting activities are focused on the electric sector.

Historically, adversaries have demonstrated the capabilities to significantly disrupt electric operations in large-scale cyber events through misuse of control systems, leveraging specialized malware and deep knowledge of targets' operations environments. ICS-targeting adversaries continue to exhibit the interest and ability to target electric utility networks with activities that could provide prerequisites for facilitating future attacks. However, similar disruptive attacks have not been publicly observed in the Electric Utility industry since 2016.

A power disruption event from a cyberattack can occur at various points in electric system operations such as control centers, dispatch centers, or within the generation, transmission, or distribution environments throughout an organization's service territory. Attacks on the electric power system – like attacks on other critical infrastructure sectors – can further an adversary's political, economic, and national security goals. As adversaries and their sponsors invest more effort and money into obtaining disruptive capabilities, the risk of a disruptive or destructive attack on the electric utility industry significantly increases.

In many parts of the world the electric sector leads other industrial sectors in security investments. While the security investments have historically been focused on enterprise information technology (IT) networks there is significant advancement in operational technology (OT) security underway. As an example, in North America the electric sector has been working for over a decade to address cyber threats through board level decisions, preparedness exercises like GridEx, the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards, and recently a 100-day action plan at the direction of the White House in partnership with the Department of Energy[1]. This 100-day action plan was focused on increasing OT visibility, detection, and response in ICS networks and culminated with President Biden signing a National Security Memorandum[2] focused on ICS technology adoption across other areas. Dragos's Neighborhood Keeper technology was selected[3] as part of this effort by electric sector participants and visibility across OT networks in the United States (U.S.) increased from sub-5% to over 70% of the electric system.

As the industry starts to get more visibility than ever before it must be prepared for what it finds. This report provides a snapshot of the threat landscape through June 2021.



KEY FINDINGS

- **THE ICS SECURITY RISK TO ELECTRIC UTILITIES IS HIGH** and increasing, led by numerous intrusions for reconnaissance and information gathering purposes, and ICS threats from specific Activity Groups demonstrating new interest in the electric sector. In fact, three out of the four new AGs Dragos discovered in 2020, and eleven out of fifteen in total, have been observed targeting the electric utility industry.

- **WHILE THE NUMBER OF INTRUSIONS IN THE ELECTRIC** sector has increased, we have not observed new groups demonstrating ICS-disruptive or -destructive capabilities. New interest in the electric sector demonstrated by XENOTIME, who has already targeted Safety Instrumented Systems in the past, is a sign that the industry should maintain a high level of attention.

- **SUPPLY CHAIN THREATS ARE INCREASING IN SCALE AND** sophistication, as evidenced by the attacks on SolarWinds revealed in December 2020. Software updates and routine patching are not the only potential entry vector that could be abused in a supply chain type of intrusion. Original Equipment Manufacturer (OEM), vendors and third-party contractors could provide an ingress into electric utility environments via compromised or poorly-secured direct network connections and remote access connections.

- **RANSOMWARE REMAINS A THREAT TO ELECTRIC** operations, and could potentially disrupt critical operational systems or operational support systems.

ACTIVITY GROUPS (AGs)

Dragos tracks 11 AGs[4] targeting electric systems out of a total of 15 groups that we track. Dragos only tracks a threat group if they are explicitly targeting ICS or attempting to gain access to them. As an example, simply sending phishing emails to utilities would not qualify. However, a focus of the adversary to breach ICS networks or success in doing so would rise to the level of activity worth tracking. Two of those eleven, ELECTRUM and XENOTIME, possess ICS-specific capabilities and tools to cause disruptive events. Dragos does not speculate on the identity of these AGs and none should be implied. The 11 AGs targeting electric systems that Dragos tracks are listed below, along with the names of other threat groups (in "Links") that have shown some overlap in capabilities, targets, or infrastructure.

ALLANITE

targets business and ICS networks in the U.S. and U.K. electric utility sectors. The group maintains access to victims to understand the operational environment and stage for potential disruptive events. ALLANITE is currently showing no indication of disruptive or damaging capability or intent [5]

Links: PALMETTO FUSION[6], Dragonfly 2.0, Berserk Bear

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, ranging across the Middle East, North Africa, United States and Europe.[7]

Links: APT34, GREENBUG, OilRig[8]

DYMALLOY

is a highly capable AG that has the ability to achieve long-term and persistent access to IT and operational environments for intelligence collection and possible future disruptive events. The group's victims include electric utilities, oil and gas, and advanced industry entities in Turkey, Europe, and North America[9] Dragos identified this group expanding its targeting to include the Asia-Pacific (APAC) region, based on analysis of malware samples. DYMALLOY is currently showing no indication of disruptive or damaging capability or intent.

Links: Dragonfly 2.0, Berserk Bear[10]

ELECTRUM

currently focuses on electric utilities and mostly targets entities in Ukraine. It is responsible for the disruptive CRASHOVERRIDE event in 2016[11] This group is capable of developing malware that can impact electric operations, leveraging known ICS protocols and communications.[12]

Links: KAMACITE, Sandworm

KAMACITE

participated in multiple critical infrastructure intrusion events, including operations enabling the 2015 and 2016 Ukraine power events, as well as the persistent campaign targeting U.S. Energy companies from late 2019 to mid 2020[13] Dragos assesses KAMACITE to be the Activity Group associated with developing access for other groups like ELECTRUM, which then follows through with the ICS-focused attack as observed in 2016. KAMACITE should not be seen itself as having ICS-specific capabilities but instead enabling the access for the teams that do, making it an especially concerning threat.[14]

Links: ELECTRUM, Sandworm[15]

MAGNALLIUM

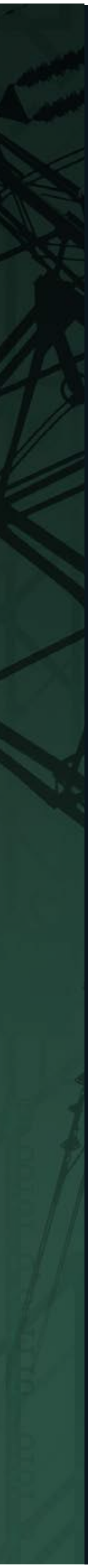
targeted petrochemical and aerospace manufacturers since at least 2013. The AG initially targeted an aircraft holding company and energy companies based in Saudi Arabia, but expanded their targeting to include entities in Europe and North America. In the fall of 2019, following increasing tensions in the Middle East, Dragos identified MAGNALLIUM expanding its targeting to include electric utilities in the U.S. MAGNALLIUM appears to lack an ICS-specific capability, and the group remains focused on initial IT intrusions.[16]

Links: APT 33, Elfin[17]

PARISITE

has been operating since 2017, targets electric utilities, aerospace, oil and gas entities, and government and non-governmental organizations. Its geographic targeting includes North America, Europe, and the Middle East. PARISITE uses open source tools to compromise infrastructure and leverage known virtual private network (VPN) vulnerabilities for initial access.[18]

Links: MAGNALLIUM



STIBNITE

targets wind power plants and government entities in Azerbaijan. It launched multiple intrusion operations against targets from late 2019 through 2020. STIBNITE leverages spearphishing to drop a custom malware known as PoetRAT. This malware is part of a complete Stage 1 operation as defined by the ICS Cyber Kill Chain.[19] STIBNITE is currently showing no indication of disruptive or damaging capability or intent.

TALONITE

targets the electric utility sector in the U.S.. Its activities focus on initial access operations using spearphishing techniques with malicious documents or embedded executables. Dragos began tracking TALONITE in 2020. TALONITE activity consists of information gathering operations.[20] TALONITE is currently showing no indication of disruptive or damaging capability or intent.

Links: TA410[21]

WASSONITE

is an ICS-focused activity group Dragos identified based on a malware intrusion at the Kudankulam Nuclear Power Plant (KKNPP) facility in India. Dragos observed WASSONITE tools and behavior targeting multiple ICS entities including electric generation, nuclear energy, manufacturing, and organizations involved in space-centric research. Geographic targeting focuses on Asian entities mostly in India, as well as possibly Japan and South Korea. WASSONITE has been active since at least 2018.[22] WASSONITE is currently showing no indication of disruptive or damaging capability or intent.

Links: Lazarus

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. In 2018, XENOTIME activity expanded to include electric utilities in North America and the APAC region; oil and gas companies in Europe, the U.S., Australia, and the Middle East; and devices beyond the Triconex controllers. This group also compromised several ICS vendors and manufacturers, executing potential supply chain compromise.[23]

Links: Temp.Veles[24]

OVERVIEW OF THE ELECTRIC SECTOR

The phrase "electric grid" as a single entity is a misnomer. The way power is generated and distributed is best described as an electric system. The electric system is complex, resilient, and interconnected. In North America, for example, the electric system is comprised of four interconnections: Eastern, Western, Electric Reliability Council of Texas (ERCOT), and Quebec.[25] In Europe, the transmission system network is operated by the European Network of Transmission System Operators (ENTSO-E).[26] In Australia, the transmission network system is operated by the Australian Energy Market Operator (AEMO),[27] who operates the Wholesale Electricity Market (WEM) in Western Australia, and the National Energy Market (NEM), covering the rest of the country. Those systems are in turn formed by the interconnection of many local electric grids.

This interconnection model enables the safe and reliable flow of power within an interconnection and allows for some flow between interconnections through Direct Connection (DC) tie lines. This design allows for power flows to occur through multiple paths within an interconnection and contains frequency disturbances within an interconnection. The Engineered approach provides redundancy, protections from complete collapse, and provides numerous benefits during emergency operations. However, while the system has been fairly resilient, the complexity has been increasing significantly and as a result such interconnections and dependencies may actually reduce its resilience, which still remains largely untested in the face of a determined cyber threat.

Electric utilities have processes in place to provide mutual aid to other entities if one experiences an event such as a storm, fire, or cyberattack that affects their service territories. Regional mutual assistance groups and industry partnerships can share resources and enable stabilization and reliability following disruptive or destructive events. Responding to real-time events, electric utilities have well defined emergency operations procedures to control and position the electric system during degrading operational conditions that may include public appeals for reducing load, service interruptions, load shedding, and power system restoration actions.

Electric entities registered to perform specific reliability tasks in the U.S. and Canada, and parts of Mexico, must adhere to cybersecurity regulations established by the NERC-CIP standards. Mexico's electric grid system is regulated by Comisión Reguladora de Energía (CRE). The commission works with NERC on reliability efforts and defines cybersecurity rules for power entities in Mexico. Globally, cybersecurity regulations or guidance vary, but many countries rely on standards developed by the International Electrotechnical Commission (IEC) and International Organization for Standardization (ISO). The ISO and IEC Joint Technical Committee (JTC1) creates cybersecurity standards for Operational Technology (OT) equipment including nuclear power and electric power utilities. Europe and Australia have also developed similar frameworks, the Directive on Security of Network and Information Systems (NIS-D) and the Australian Energy Sector Cyber Security Framework (AESCSF) respectively, although they are not enforced regulations yet and are more high level for critical infrastructure rather than completely electric-specific. Adhering to cybersecurity regulations and best practices makes electric utilities unique in the ICS industry by ensuring a minimum level of cybersecurity is maintained.

ELECTRIC POWER OPERATIONAL SEGMENTS THREAT PERSPECTIVE

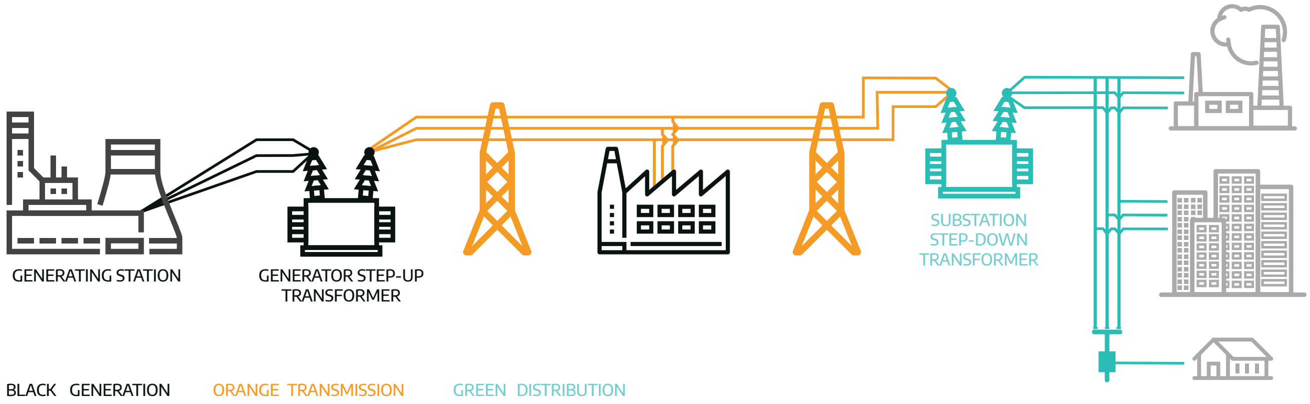


Figure 1: Electricity Distribution

Before electricity reaches customers, it goes through multiple steps including generation, transmission, and distribution. 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 carries electricity across long distances from the plants to distribution substations. From there, it is distributed to customers. The transmission and distribution systems include substations where transformers are used to step up or step down voltage levels, in order to provide appropriate service delivery to industrial, commercial, and residential customers.

GENERATION

THREAT LANDSCAPE

Dragos assesses that at least five AGs demonstrate the intent or capability to infiltrate or disrupt electric power generation. XENOTIME has demonstrated the capability to access, operate, and conduct attacks in an industrial environment. Dragos assesses this group would be capable of retooling and refocusing its disruptive efforts on electric utilities because it has already targeted Safety Instrumented Systems, like Triconex, which is a mainstay in power generation. DYMALLOY demonstrated the ability to access OT networks in generation facilities and obtain screenshots of sensitive ICS data, including screenshots of Human Machine Interfaces (HMIs). ALLANITE is also a threat to generation because it shares some similarities in targeting and capabilities with

DYMALLOY. Neither group has demonstrated ICS-disruptive or -destructive capabilities as of now, and they focus on general reconnaissance.

WASSONITE actively targeted critical infrastructure in Asia including nuclear power generation, and successfully deployed malware in the administration systems of at least one nuclear power plant. This is concerning, though no evidence suggests it successfully penetrated operations networks. While the AG is yet to display any ICS-specific capability or disruptive intent, actions to date indicate a sustained and continuing interest in these resources. Finally, STIBNITE has been observed specifically targeting wind turbine companies that generate electric power in Azerbaijan. Based on current collection efforts, the activity appears confined exclusively to Azerbaijan. STIBNITE uses PoetRAT remote access malware in its intrusion operations to gather information, take screenshots, transfer files, and execute commands on victim systems. Also in this case, the activity mirrors observations in many of Dragos's AGs, where ICS intentions exist even if ICS-specific capabilities have not yet manifested.

ASSESSMENT

ICS-targeting adversaries have not successfully disrupted electric power generation. The observed activities targeting this segment, including obtaining documentation on sensitive operations networks, could be used for espionage purposes or to facilitate a disruptive attack.

TRANSMISSION

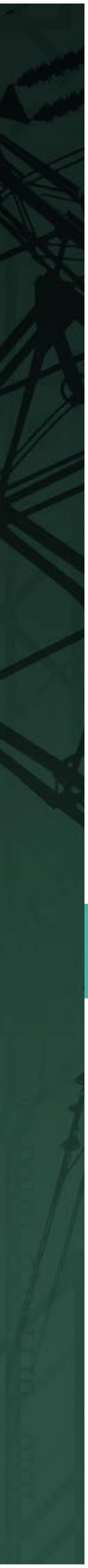
THREAT LANDSCAPE

At least two AGs are a threat to transmission operations. ELECTRUM is a well-resourced AG with the capability to disrupt power transmission. Dragos assesses KAMACITE serves as an initial access and facilitation group for ELECTRUM.

ELECTRUM was responsible for the CRASHOVERRIDE malware attack in December 2016 in Kiev, Ukraine.[28] The adversaries tailored malware to de-energize a transmission-level substation by opening and closing numerous circuit breakers used in the delivery of power in 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.

ASSESSMENT

While this attack took place in Europe, it may be possible for a similar cyberattack to occur in other parts of the world, with modifications for different industrial protocols, devices, and network topology found in a target environment. For example, the attack targeted breaker operations controlled by ABB devices adhering to the IEC 61850[29] standard and communicating using the Manufacturing Message Specification (MMS) protocol. However, Dragos assesses with moderate confidence the attack can be leveraged to other equipment that adheres to these standards.



DISTRIBUTION

THREAT LANDSCAPE

In the current threat landscape, one adversary group has disrupted electric distribution operations. KAMACITE operations enabled the first widespread outage caused by a cyberattack, which took place in Ukraine on 23 December 2015. The adversaries leveraged malware to gain remote access to three electric power distribution companies, performed system operations using the target environments' distribution management systems, and disrupt electricity to approximately 230,000 people.[30] Power was fully restored after a few hours through manual operations.

ASSESSMENT

Contrary to ELECTRUM, KAMACITE did not use ICS-specific malware in the 2015 Ukraine incident. It controlled operations remotely via existing tools in the operations environment. The behaviors and tools use exhibited by AGs, including KAMACITE and ELECTRUM, could be deployed in distribution operations globally depending on the adversary sponsor's focus.

Disrupting electric power 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. Adversaries must spend an extended period of dwell time within the target environment learning the control system specifics to successfully deliver an attack that disrupts electric service, whereas defenders have multiple points of opportunity along the potential attack chain to detect and eliminate adversary access.

THREAT LANDSCAPE

RANSOMWARE

Dragos observed a significant rise in the number of non-public and public ransomware events that have affected ICS environments and operations. Between 2018 and 2020, ten percent of ransomware attacks that occurred on industrial and related entities targeted electric utilities, according to data tracked by Dragos and IBM Security X-Force.[31] It was the second most targeted industry after manufacturing. Although most ransomware strains impacting ICS and related entities are IT-focused, ransomware can have disruptive impacts on operations if it is able to bridge the IT/OT gap due to improper security hygiene. Dragos identified multiple ransomware strains adopting ICS-aware functionality, including the ability to kill industrial-focused computer processes if identified in the environment, with activity dating to 2019. EKANS, MEGACORTEX, and CLOP are just a few ransomware strains that contain this type of code. EKANS and other ICS-aware ransomware represent a unique and specific risk to industrial operations not previously observed in ransomware operations.

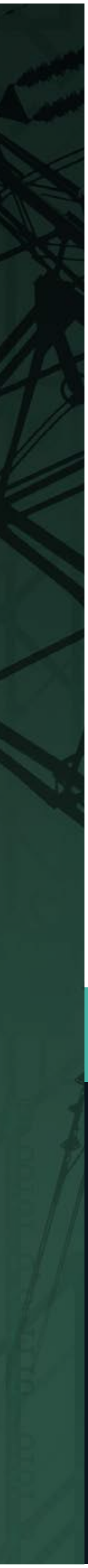
CASE STUDY

Multinational energy company Enel Group experienced two ransomware attacks in 2020. In June, it experienced an EKANS ransomware attack impacting its IT operations,[32] followed by a NetWalker ransomware attack in October.[33] The ransomware attacks did not impact the delivery of electric service, however NetWalker adversaries subsequently leaked data allegedly belonging to Enel when the company did not pay the multi-million dollar ransom.

Ransomware operators are increasingly incorporating data theft techniques into their campaigns to further ransom demands. An adversary may steal data from a target company before encrypting infected machines and threaten to publish the data online, either on adversary-run websites or hacking forums if a ransom demand is not paid. This method could encourage companies to pay ransoms demanded by adversaries, which further encourages cyber criminals to conduct ransomware campaigns. Data stolen or leaked by adversaries could contain sensitive information on the targeted company and information about its customers. Although a ransomware adversary may only be interested in leveraging data for financial purposes, adversaries interested in specifically targeting the electric industry could use leaked data to aid in attack development. For example, an adversary could use customer data to identify potential opportunities for third-party or supply chain compromise, or data like schematics, network diagrams, or other internal documentation to identify targets for operational gain.

CASE STUDY

In 2021 Dragos responded to several ransomware incidents. In one specific case, at a U.S. power company, the adversary stayed undetected inside the network for over a month, during which they performed credential harvesting, lateral movement, mapped network topology, and performed data exfiltration before completing the operation. The ransomware attack itself took less than 1 hour until it was detected, at which point it was too late as the amount of compromised systems was enough to halt the company's operations. In this case, like many others, what made it easier for the adversary to maximize the damage was a flat, non-segmented network and the lack of multi-factor authentication (MFA) on externally exposed resources and services, which would have prevented such incident.



Ransomware is not just for financially motivated operators. State-sponsored adversaries may also leverage ransomware in cyber operations. In May 2020, the Republic of China (Taiwan) government attributed ransomware events targeting oil and gas and semiconductor companies to the Winnti Group.[34]

One of the potential risks of destructive malware in an ICS environment is represented by the historian technology, since historian deployment is often architected in a manner that bridges communications from a read-only historian in an IT network segment and a plant historian within the OT network. Moreover, sensor data is short-lived unless recorded in a historian and a destructive attack on its data could result in unrecoverable losses if not well defended. To help assess such risk and model defenses for hazards at the transition from enterprise to ICS environment, Dragos has applied the Bow Tie risk analysis approach to the specific case of ICS Historians[35/36], which helps in identifying relevant threats, defenses, impacts, and methods to reduce those associated impacts from creating an adverse event related to the hazard.

INTERNET-EXPOSED ASSETS

Industrial and networking assets exposed to the internet are a significant cyber risk for electric utilities. Various tracked ICS-targeting AGs – PARISITE, MAGNALLIUM, ALLANITE, and XENOTIME – have previously targeted or currently attempt to exploit remote access technology or logon infrastructure.

According to the 2020 Dragos Year in Review Report detailing lessons learned from the incident response and services team, 100 percent of incident response cases involved adversaries directly accessing the ICS network from the internet. There were 33 percent of organizations that had routable network connections into their operational environments.

CASE STUDY

In March 2019, a "cyber event" disrupted electrical system operations at an electric facility in North America. The event related to a Denial-of-Service (DoS) incident that briefly disrupted communications between the control center and remote generation sites. The event targeted Cisco Adaptive Security Appliances (ASA) software affected by Common Vulnerabilities and Exposures (CVE), CVE-2018-0296, a combination path traversal vulnerability and remote crash vulnerability reported in June 2018. This vulnerability could allow an adversary to view sensitive information without authentication and crash the device.

In July 2020, the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) published an alert encouraging asset owners and operators to take immediate actions restricting exposure of OT assets to the internet. According to the alert, behaviors observed recently before publication include:

- Spearphishing to gain initial access to Information Technology (IT) before pivoting to OT;
- Deploying commodity ransomware to impact IT and OT environments;
- Connecting to internet-accessible Programmable Logic Controllers (PLCs) that require no authentication;
- Using common ports and standard application layer protocols to communicate with controllers and download modified control logic;
- Using vendor engineering software and program downloads; and
- Modifying control logic and parameters on PLCs.

Adversaries are quick to weaponize and exploit vulnerabilities in internet-facing services including Remote Desktop Protocol (RDP) and VPN services. New vulnerabilities revealed in the summer of 2020 impacting critical network infrastructure services including F5, Palo Alto Networks, Fortinet, Citrix, and Juniper network devices will likely be exploited by ICS-targeting adversaries, if they are not already.[38] These vulnerabilities can enable adversaries to gain initial access to enterprise operations and potentially pivot into industrial operations.

SUPPLY CHAIN COMPROMISES

Adversaries can abuse existing trust relationships and interconnectivity to gain access to sensitive resources – including systems in some cases – with little likelihood of detection.

In December 2020, FireEye revealed the first details of a massive supply chain compromise campaign that impacted companies and governments around the globe, including electric utilities.[39] Adversaries compromised IT management software known as SolarWinds to gain access to thousands of organizations that used the software.[40] Concerningly, many integrators and original equipment manufacturers (OEMs) use SolarWinds in OT networks and across maintenance links. Dragos responded to numerous incident response cases where compromised versions of SolarWinds were present in the ICS networks of companies. Dragos also identified that at least two global OEMs were using the compromised SolarWinds software across maintenance links directly into ICS networks to include turbine control software. Adversaries could have easily leveraged this access to cause significant disruption.

The activity was one of the largest supply chain compromise events ever publicly identified and underscored the potential risks introduced to the environment via software, firmware, or third-party integrations within operations environments.[41]

But software updates are not the only potential entry vector that could be abused in a supply chain type of intrusion. In April 2021, Dragos discovered the compromise of a South Asian ICS provider with significant links to Electric industry customers in Europe. Original equipment manufacturers (OEM), vendors, and third-party contractors are essential to enterprise and ICS operations. The numerous vendor or contractor touchpoints within generation, transmission, and distribution could provide an ingress into electric utility environments via compromised or poorly-secured direct network connections.

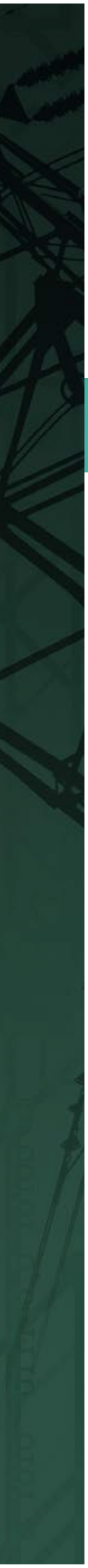
DYMALLOY, ALLANITE, and XENOTIME have used supply chain compromise methods to gain access to victim networks. DYMALLOY and ALLANITE compromised vendors and contractors for subsequent phishing campaigns targeting the electric sector.[42] XENOTIME compromised several ICS vendors and manufacturers in 2018, providing potential supply chain threat opportunities and vendor-enabled access to target ICS networks.[43]

SYSTEMIC THREATS

The electric utility industry supports all critical infrastructure verticals in one form or another, and a disruption to power could have cascading and disruptive effects on other sectors like manufacturing, mining operations, or water desalination.

Moreover, big manufacturing companies are becoming renewable power providers too, and those power plants supply electricity to all their manufacturing plants. A disruption to one of these facilities could cause disruption to manufacturing operations across the company.

Many countries globally – especially in the Middle East – rely on desalination operations for parts of their water supply. Facilities can turn salt water into potable water through an energy-intensive process. Membrane-based



desalinization requires significant electricity and is the most common desalinization technology worldwide, according to the International Energy Agency.[44] A disruption to electric operations supporting desalination efforts could limit the production of potable water.

Mining operations use massive amounts of energy. In the U.S., approximately 32 percent of the mining industry energy sources are electric.[45] In Australia, the electric system supplies 21 percent of the energy for the country's mining sector. Electric energy supports drilling and materials handling operations, which could be disrupted in the event of a cyberattack on generation, transmission, or distribution, especially at on-site power generation facilities supporting mining operations.

DEFENSIVE RECOMMENDATIONS

Asset owners and operators can implement the following host and network-based recommendations to improve detection and defense against ICS-targeting groups.

- ACCESS RESTRICTIONS and ACCOUNT MANAGEMENT:
  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.

  Ensure all devices and services do not use default credentials. If possible, do not use hard-coded credentials. Monitor for any hard-coded 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, like file shares and cloud storage services, are properly segmented. Following the Purdue Model, network connections should be terminated before continuing to different levels.

- 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.

- 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 response plan essential elements during remediation and response to increase disruption scale and downtime.

- 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.

- 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 demilitarized zones (DMZs) for such access to ensure that third-parties cannot gain 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. Dragos recommends using threat information and consequence-driven analysis to address supply chain cyber risk.

- VISIBILITY:
  Take a comprehensive approach for visibility into ICS/OT environments to ensure that there is no gap in monitoring. Asset owners, 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 identifying intrusions as they occur or facilitating root-cause analysis after a disruptive event. Ensure network monitoring of the operations network through ICS-focused technologies.

CONCLUSION

Electric utilities remain at risk for a disruptive – or potentially destructive – cyberattack due to the political and economic impact such an event may cause. Due to the interconnectivity of electric systems that enable robust resilience and redundancy during disruptive events such as storms or earthquakes, the system in most developed areas would likely recover very quickly from a disruptive cyber event. Regulations implemented by governing bodies help ensure a minimum level of security in this sector, which generally does not apply to other ICS verticals.

A disruptive attack requires significant effort to achieve, as evidenced by CRASHOVERRIDE. An adversary’s requisite dwell time within a target environment provides defenders with numerous opportunities to identify and remove malicious activity. The enterprise-targeting activity observed by Dragos enables initial intrusion and data gathering, and lays the groundwork for an adversary to pivot to potentially disruptive events. The growing threat of supply chain attacks and vendor compromises allows new avenues for AGs to compromise IT and OT environments alike.

REFERENCES

1 Department of Energy

2 National Security Memorandum

3 Dragos's Neighborhood Keeper

4 Dragos categorizes ICS-targeting activity into AGs 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 AGs possess ICS-specific capabilities and tools to cause disruptive events: XENOTIME and ELECTRUM.

5 ALLANITE

6 PALMETTO FUSION

7 CHRYSENE

8 OilRig

9 DYMALLOY

10 Berserk Bear

11 CRASHOVERRIDE

12 ELECTRUM

13 KAMACITE

14 KAMACITE

15 Sandworm

16 MAGNALLIUM

17 Elfin

18 PARISITE

19 STIBNITE

20 TALONITE

21 TA410

22 WASSONITE

23 XENOTIME

24 Temp.Veles

25 Eastern, Western, Electric Reliability Council of Texas (ERCOT), and Quebec

26 European Network of Transmission System Operators (ENTSO-E)

27 Australian Energy Market Operator (AEMO)

28 CRASHOVERRIDE malware attack in December 2016 in Kiev, Ukraine

29 IEC 61850

30 Unprecedented Hack Ukraines Power Grid

31 Ransomware In ICS Environments

32 EKANS Ransomware Misconceptions And Misunderstandings

33 Netwalker Ransomware Attack

34 Taiwan Ministry of Justice Investigation Bureau

35 ICS Historians 1

REFERENCES

36 ICS Historians 2

37 Denial-of-Service (DoS) incident

38 New vulnerabilities

39 Evasive Attacker Leverages Solarwinds Supply Chain Compromises With Sunburst Backdoor

40 SolarWinds

41 Third-Party Integrations

ABOUT DRAGOS, INC.

Dragos has a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The practitioners who founded Dragos were drawn to this mission through decades of government and private sector experience.

Dragos codifies the knowledge of our cybersecurity experts into an integrated software platform that provides customers critical visibility into ICS and OT networks so that threats and vulnerabilities are identified and can be addressed before they become significant events. Our solutions protect organizations across a range of industries, including power and water utilities, energy, and manufacturing, and are optimized for emerging applications like the Industrial Internet of Things (IIoT).

Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

TO LEARN MORE ABOUT DRAGOS AND OUR TECHNOLOGY, SERVICES, AND THREAT INTELLIGENCE FOR THE INDUSTRIAL COMMUNITY, PLEASE VISIT

www.dragos.com.

THANK YOU