DRAGOS

INTELLIGENCE BRIEF

ELECTRUM: Cyber Attack on Poland's Electric System 2025

Executive Summary

On December 29, 2025, a coordinated cyberattack targeted multiple sites across the Polish power grid, specifically those connected to distributed energy generation. The attack affected communication and control systems at combined heat and power (CHP) facilities and systems managing the dispatch of renewable energy systems from wind and solar sites. While the attack did not result in power outages, adversaries gained access to operational technology systems critical to grid operations and disabled key equipment beyond repair at the site. Due to the lack of electric outages, asset operators and the broader community may be mistaken to think this is not overly concerning. However, what was demonstrated, especially for other countries who currently or will depend more on DERs, should be very alarming

This is the first major cyber attack targeting distributed energy resources (DERs), the smaller wind, solar, and CHP facilities being added to grids worldwide. Unlike the centralized systems impacted in electric grid attacks in 2015 and 2016 in Ukraine, these distributed systems are more numerous, require extensive remote connectivity, and often receive less cybersecurity investment. This attack demonstrates they are now a valid target for sophisticated adversaries.

This report provides technical analysis of the attack, context on Poland's energy system transformation, and defensive recommendations for power system operators managing similar infrastructure.

Why We're Publishing This Report

Dragos is involved in an incident response at one of the numerous incidents across the Polish system that are part of this attack. None of the details of this report contain sensitive incident response or client information. However, through these efforts, Dragos confirms the seriousness of the attack and assesses with moderate confidence that the threat group ELECTRUM is responsible.

Dragos is publishing this to amplify CERT Polska's efforts by adding operational technology (OT)-specific context and defensive recommendations for the electric sector. Dragos wants to thank CERT Polska for their tireless effort across their community in the face of an irresponsible attack.

We are releasing this analysis for three primary reasons:

- To provide the electric system operator community with technical insights into the first major coordinated attack on distributed energy resources, including specific defensive recommendations.
- To educate the broader community on how distributed generation infrastructure differs from traditional systems and why this attack represents a strategic shift in adversary targeting.
- To support CERT Polska's ongoing work by validating the cyber attack from an independent OT security perspective.

Poland Incident Overview

On January 14, 2026, Poland's Prime Minister Donald Tusk briefed government leaders on a cyber attack that occurred on December 29, 2025. The briefing, along with subsequent ones, detailed how the attack had been carried out, that it had been thwarted, and that the system had never been at risk. Tusk acknowledged the need for great protection for IT and OT, with operational technology specifically highlighted, especially considering the implementation of a new act to improve national resilience, a direct consequence of European directives on this matter.

This represents the first major coordinated attack targeting distributed energy resources at scale. While Dragos has responded to cybersecurity incidents at individual renewable and distributed generation facilities in the past, those incidents involved single sites or opportunistic compromises. The Poland attack is significant because of the coordinated nature of the attacks across numerous sites simultaneously and the demonstrated intent of a sophisticated adversary to systematically target this infrastructure. Through our incident response work, Dragos can confirm the seriousness of the attack and assess with moderate confidence that the threat group ELECTRUM is responsible.

Dragos knows from public statements that the attack targeted systems that facilitate communication and control between grid operators and DER assets – specifically, combined heat and power (CHP) facilities and systems that manage dispatch of renewable energy from wind and solar sites. This doesn't mean the communications links were taken down; rather, the assets that facilitate that telemetry and the devices that enable network connectivity were targeted.

Through a combination of exposed network devices and exploited vulnerabilities, adversaries compromised Remote Terminal Units (RTUs) and communication infrastructure at the affected sites. This equipment sits behind defenses that inevitably contain vulnerabilities, whether through misconfigurations, unpatched systems, or exploitable services. Once past those defenses, adversaries encountered RTUs and communications infrastructure that were not designed to withstand sophisticated cyber threats.

Taking over these devices requires capabilities beyond simply understanding their technical flaws. It requires knowledge of their specific implementation. The adversaries demonstrated this by successfully compromising RTUs at multiple sites, suggesting they had mapped common configurations and operational patterns to exploit systematically.

The Polish government's response appropriately emphasized that the transmission systems, the backbone of the electric grid, were not compromised. However, the adversaries did gain access to operational technology systems with direct connections to generation assets. While these systems are not transmission infrastructure, they are important operational systems that could enable a significant impact.

In electricity systems, the loss of communications typically does not cause immediate equipment shutdown. When a device loses connectivity, it generally continues operating. It simply cannot be monitored or controlled remotely. This is why the power remained on, which is the primary measure of operational impact for electric grids.

What remains unclear is whether ELECTRUM attempted to issue operational commands to this equipment or focused solely on disabling communications. Due to limited logging of network communications and OT commands at the affected sites, Dragos cannot definitively determine

the full scope of the adversary's actions. We can confirm that they successfully disabled communications equipment, including some OT devices.

For power system operators managing similar distributed energy infrastructure, this incident demonstrates that adversaries with OT-specific capabilities are actively targeting systems that monitor and control distributed generation. This attack did not result in power loss but the access achieved represents the type of foothold that could enable operational impacts, particularly when similar access is achieved across larger numbers of sites simultaneously or if adversaries develop deeper knowledge of specific site configurations. The disabling of certain OT or industrial control system (ICS) equipment beyond repair at the site moved what could have been seen as a pre-positioning attempt by the adversary into an attack.

Background

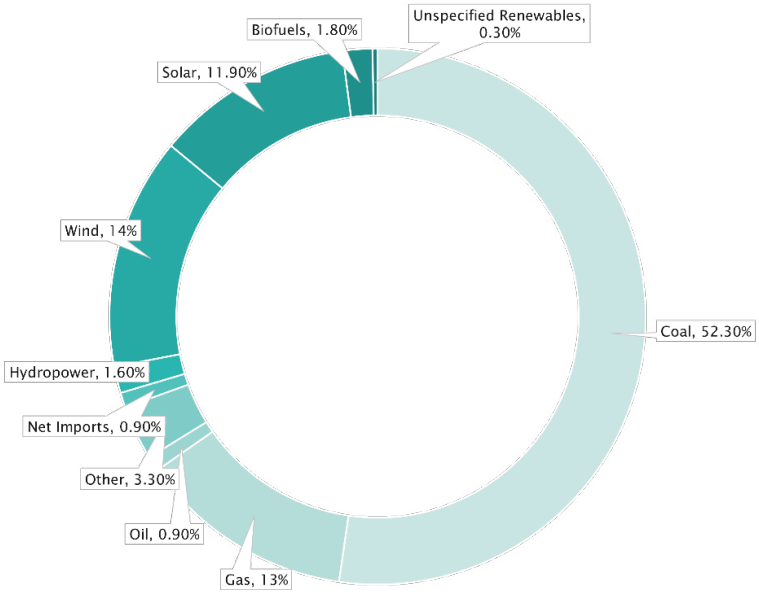
Poland's Energy Systems

Previous attacks on electrical infrastructure targeted centralized systems or individual substations. The 2015 Ukraine attacks focused on distribution control centers that manage energy flow across regions. The 2016 attack targeted a transmission substation using CRASHOVERRIDE malware. In both cases, adversaries sought to disrupt large, centralized control points that manage significant portions of the grid.

Poland, like much of the world, is transforming its energy system from large, carbon-intensive generation to a mix of smaller renewable facilities embedded throughout the grid. This transition brings well-documented operational challenges. The 2025 collapse of the Iberian power grid demonstrated how quickly grid stability can be affected. Not just by the loss of large generation facilities, but by frequency fluctuations from distributed sources.

Figure 1

Electricity Consumption in Poland in 2025[1]



Grid vulnerability to disruptions depends heavily on the generation mix and system inertia. Poland generates over 50 percent of its energy from coal or lignite-fired power plants, providing significant inertia that helps stabilize grid frequency. Wind and solar make up approximately 25 percent of capacity. Grids with higher renewable penetration and less inertia, common in regions aggressively pursuing decarbonization, may be more susceptible to the cascading effects of coordinated DER disruption. Defenders in these regions should consider Poland a warning: as your DER portfolio grows, so does the attack surface.

Traditional large generation facilities are built with substantial physical security: fenced perimeters, on-site staff, and centralized operations. Cybersecurity investments can be integrated into these facilities as a small component of overall construction and operating costs. DERs operate under different constraints:

- Hundreds of small sites instead of dozens of large facilities
- Built with tight financial margins where every cost matters
- Often developed by companies building to sell rather than operate long-term
- Fixed-scope agreements that may not prioritize security features

These facilities require extensive remote connectivity for multiple purposes: operations, energy trading, maintenance, and vendor support. Service level agreements often mandate vendor access. Meeting these connectivity requirements with low-cost commodity solutions across numerous sites creates a larger, less manageable attack surface than traditional infrastructure.

Beyond remote access, many operators have limited visibility into what occurs within the networks themselves, meaning the east-west traffic between devices and systems. This makes detecting adversary lateral movement or malicious commands significantly more difficult than monitoring traffic entering and leaving the network.

Historical Context

10 Years of Practice

An attack on a power grid at any time is irresponsible, but to carry it out in the depths of winter is potentially lethal to the civilian population dependent on it. It is unfortunate that those who attack these systems appear to deliberately choose timing that maximizes impact on civilian populations.

2015 Attack: Regional Distribution Substations

On December 23, 2015, a coordinated attack on three distribution network operators in Ukraine marked the first publicly confirmed cyber attack to cause power outages. Adversaries defeated multiple layers of IT defenses to create broad impact across more than 60 substations serving hundreds of thousands of customers. While their techniques were not particularly advanced, their planning and understanding of how the system would respond allowed them to layer their effects by blinding network operators, preventing remote restoration of communications, and removing customers' ability to contact utilities to report outages.

2016 Attack: Transmission Substations

On December 17, 2016, the same adversary returned with a more sophisticated approach. This time they targeted a transmission substation using CRASHOVERRIDE[2]/Industroyer, purpose-built malware designed to communicate directly with OT/ICS protocols. CRASHOVERRIDE used 4 ICS specific protocols, IEC 104 - a protocol for power system monitoring and control over TCP/IP networks, IEC-101 (IEC-104's serial equivalent), IEC 61850 (standard for communication in electrical substations), and OLE for Process Control Data Access (OPC DA), a set of standards and specifications for industrial automation data exchange. It also deployed a wiper module to impede recovery, deleting configuration and related files to hamper restoration on infected SCADA systems. While the attack affected a single substation, it still impacted hundreds of thousands of customers on a day when energy is life-critical. The deployment of OT protocol-specific malware represented a significant escalation, moving from manual operator interaction to automated execution.

Threat Group: ELECTRUM

Dragos worked extensively on these investigations and attributed the 2015 and 2016 attacks to ELECTRUM with high confidence. ELECTRUM is tracked elsewhere in the industry as synonymous with the threat actor Sandworm, though Dragos notes that not all Sandworm activity is ELECTRUM or vice versa. This group has demonstrated a deep understanding of electrical grid equipment and operations, proficiency with industrial protocols used in power systems, and the ability to develop custom malware and wiper tools for both IT and OT environments. ELECTRUM's operations demonstrate a working knowledge of control workflows, substation operations, and the operational dependencies within electrical systems. This knowledge enables them to achieve real-world physical effects. Since 2016, ELECTRUM has continued to develop capabilities targeting electrical infrastructure.

Post-2016 ELECTRUM Operations

After 2016, ELECTRUM and its enabling counterpart, KAMACITE, conducted reconnaissance across European infrastructure, expanding their understanding of potential targets. From 2016 through 2022, they were observed enumerating systems and mapping networks across Europe, demonstrating sustained interest in critical infrastructure beyond Ukraine,

When Russia's invasion of Ukraine began in February 2022, ELECTRUM's capabilities were immediately evident. Within hours of the invasion, they deployed destructive malware against the KA-SAT satellite network (operated by Viasat), disrupting communications for tens of thousands of terminals across Europe. This attack affected not only Ukrainian military communications but also civilian infrastructure, including wind turbines in Germany that relied on the satellite network for remote monitoring and control.

Throughout 2022 and beyond, ELECTRUM developed and deployed numerous custom capabilities:

- CaddyWiper – Deployed against Ukrainian organizations in March 2022, designed to render systems inoperable by irreversibly destroying data
- Industroyer2 – A refined version of their 2016 CRASHOVERRIDE malware, discovered in April 2022 before it could be used to disrupt electrical operations in Ukraine
- Living-off-the-land scripts – Custom PowerShell and batch scripts targeting automation systems, designed to avoid detection while achieving operational effects

These operations demonstrated ELECTRUM's ability to sustain multiple lines of effort: developing ICS-specific capabilities, creating destructive malware to complicate recovery, and adapting their tactics based on the operational environment.

More recently, their operations have begun to widen beyond Ukraine, acting directly and through hacktivist personas, affecting exposed infrastructure across multiple sectors. The systems have not always been as large as the previous operations, but they have demonstrated a pattern of exploiting vulnerable environments to maintain operational tempo and generate psychological effects.

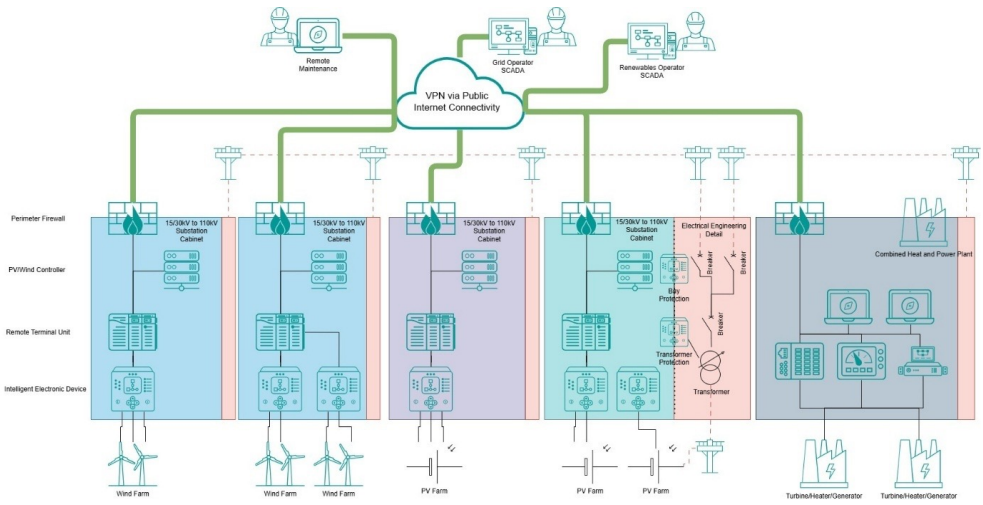
For a comprehensive analysis of ELECTRUM's decade-long campaign targeting critical infrastructure, including detailed technical analysis of the 2015 and 2016 Ukraine power grid attacks and the development of purpose-built ICS malware such as CRASHOVERRIDE and Industroyer2, read Dragos's full ELECTRUM threat intelligence report: ELECTRUM and KAMACITE: Ten Years of Adversary Tradecraft in ICS Operations.[3]

Targeted Systems

Electrical networks were not originally designed for distributed renewable energy systems. These new energy sources have been overlayed onto existing infrastructure. Network operators work to facilitate new connections, but demand exceeds the rate at which sites can be added. This creates pressure to implement solutions quickly, sometimes with compromises that can be managed through visibility and control.

Figure 2

Typical Renewable Energy Infrastructure



RTUs standardize how distributed sites interface with control centers, enabling operators to manage large numbers of remote facilities from a single SCADA system. Within these installations are systems often specified by manufacturers or chosen by system integrators, leading to significant variations in implementation. The technology may be similar across sites, but configurations and applications differ.

This combination of standardization and variation likely explains both what adversaries achieved and what they failed to accomplish.

If the RTUs are common and interface similarly with external networks, compromising them becomes repeatable. Even with a variety of vendors, a handful of methods could have a

widespread impact. Similarly, if sites share common connectivity infrastructure – the same firewalls with identical vulnerabilities or configurations – adversaries can systematically identify and attack RTUs.

However, operational control is a different matter. While many of these RTUs have control capabilities, tools like CRASHOVERRIDE or Industroyer2 cannot simply be deployed. CRASHOVERRIDE manipulated four different protocols to achieve the basic function of opening a circuit breaker. Industroyer2 replicated standardized commands between SCADA systems and substation RTUs. The RTUs in distributed energy systems lack this standardization, and each requires unique commands tailored to its specific configuration.

Comparing the 2025 Attack to Previous Operations

The December 2025 attack on Poland's distributed energy infrastructure represents both continuity and evolution. The attack shares technical similarities with previous ELECTRUM operations, including the use of wipers and targeting of communication infrastructure. However, it demonstrates a shift in targeting strategy.

Previous attacks focused on centralized control systems managing large portions of the grid – distribution control centers in 2015, a transmission substation in 2016. The Poland attack instead targeted the distributed edge of the grid: the RTUs and communication systems managing dozens of smaller generation sites. This shift reflects the changing nature of electric grids, as countries like Poland add more distributed renewable generation.

When compared with the 2015 attack in Ukraine, it shows similar technical tactics, techniques, and procedures, such as wiping Windows devices and damaging exposed serial terminal servers, but lacks the coordinated sequencing that maximized impact in that operation.

The Poland attack also resembles the 2016 deployment of CRASHOVERRIDE, which contained software flaws, or bugs, suggesting rushed deployment without adequate testing. The adversaries demonstrated an understanding of the equipment but achieved limited impact. Dragos assesses with low confidence that this was due to incomplete preparation rather than a lack of capability.

ELECTRUM possesses the skills to develop these site-specific commands, but doing so requires time, testing, and detailed knowledge of each location's configuration. The attack timeline, from identifying vulnerable infrastructure through planning to execution, may not have allowed for this level of preparation.

Dragos assesses with moderate confidence that opportunism was a key factor in the attack. Rather than executing a precisely planned operation with specific outcomes, ELECTRUM exploited whatever opportunities their access provided: wiping Windows-based devices, resetting configurations, or attempting to permanently damage (or brick) equipment. Each location required different manual actions rather than a single automated tool. The attack is more opportunistic than the 2015 or 2016 operations. It appears the operation was rushed, but Dragos cannot make an assessment as to why.

A majority of the equipment targeted in the attack sat outside the direct DER control process – systems related to grid safety and stability monitoring rather than active generation control but have the potential to despatch or curtail outputs. These systems were likely exposed on the

same networks that adversaries had accessed. These are not classified as "protection systems" that maintain safe equipment operation, but they provide monitoring functions that support grid stability. The probability of these systems being needed during the brief attack window was low, suggesting that the attacks were intended to disrupt whatever was accessible rather than achieve specific operational outcomes.

Potential Implications for OT/ICS

From the direct evidence we have seen and public statements we know that at least 12 sites were affected and it is likely at least double this. A scenario where adversaries achieved full operational control could have looked significantly different.

A typical onshore wind farm or CHP facility produces 50-100Mw of energy. Assuming all of these were operating at capacity, they would have been producing around 1.2 GW of energy at the time of the attack. On January 17, 2026, Poland set a consumption record, reaching 30 GW. While 1.2 GW represents only 5 percent of the total supply, the sudden simultaneous loss of this amount of generation would have had a noticeable impact on the system frequency. Such frequency deviations have caused cascading failures in other electrical systems, including the 2025 Iberian grid collapse.

In all major blackouts of the last decade, frequency has been a critical factor. System operators use a stable frequency to measure the balance between supply and demand. Protection systems automatically shed less critical loads from the system as frequency drops, matching reduced generation with decreased consumption. Other systems monitor the rate of change of frequency (ROCOF) to isolate network sections exhibiting sudden instability. This balance has proven particularly difficult in low-inertia systems with high renewable penetration.

This attack was unlikely to cause a nationwide blackout in Poland under current conditions. Strong AC interconnection with neighboring countries and spinning thermal generation would have allowed the system to absorb the disruption, though localized outages could have occurred. However, as Poland and other countries reduce spinning reserves during the energy transition, this style of attack could cause more severe consequences. In regions where high renewable penetration and limited thermal backup are already the reality, a coordinated attack disabling 1.2 GW of distributed generation could trigger cascading failures leading to widespread outages.

Smaller DER assets are rarely subject to legislation mandating cybersecurity protections. Under the first iteration of the European NIS directive, the UK set the threshold for inclusion at 2 GW. In the United States, a generation facility must typically exceed 1500Mw to be classified "medium" as part of the Bulk Electric System (BES). Every site affected in the Poland attack falls significantly below these thresholds, yet their coordinated compromise demonstrates the systemic risk that distributed assets can pose when attacked at scale.

Five Critical Controls for OT/ICS Cybersecurity

Electric system asset owners and operators can defend their systems by applying the SANS ICS 5 Critical Controls.[4] Each control addresses specific aspects of OT cybersecurity readiness and resilience and is directly applicable to defending against the access enablement, OT positioning, and execution techniques observed in ELECTRUM operations described in this report.

01. OT/ICS Incident Response

ELECTRUM compromised distributed generation sites and deployed wiper malware to impede recovery. This creates a fundamentally different incident response challenge than traditional attacks on centralized infrastructure. When communications to multiple remote sites are lost simultaneously, operators must be prepared to dispatch personnel for manual restoration while assuming that remote access infrastructure and backup systems may be compromised.

Incident response plans for DER environments must address how to prioritize restoration when dozens of sites lose connectivity at once, how to perform forensics when wipers have destroyed evidence on Windows systems and potentially corrupted RTU configurations, and how to detect whether adversaries achieved operational control or only communications disruption when logging may be incomplete. Organizations should prepare incident response procedures and consolidate information about remote sites in case network-based distribution fails during an attack. Additionally, in a table top exercise (TTX) of the incident response plan it should be determined what questions are going to need to be answered and what data needs to be collected ahead of the attack to make sure the data is available in the incident. Unlike IT incident response much of the data critical to OT incident response and root cause analysis is transient network data and OT commands. This type of data is covered in Critical Control 3. In this incident, data was not collected and thus unavailable.

02. Defensible Architecture

Adversaries succeeded by exploiting common configurations across multiple sites. Once they understood how to compromise edge devices at one location, they could repeat the attack at scale. This demonstrates why treating each DER site as an independent security zone is critical. If a wind farm's firewall is compromised, that breach should not provide access to solar sites, CHP facilities, or the broader DER portfolio of assets.

ELECTRUM specifically targeted edge systems, such as firewalls, at generation sites. These devices require hardening, monitoring, and the elimination of default credentials. Because DER sites are built rapidly with cost constraints, standardized configurations are common. This becomes a force multiplier for adversaries. Introduce variation in security controls across sites, segment individual sites from each other, and ensure that vendor remote access to one site cannot be leveraged to reach others.

03. OT/ICS Network Visibility & Monitoring

RTUs and communications infrastructure were compromised without triggering detection at many sites. For distributed generation operators, this means adversaries were moving through networks, accessing devices, and potentially issuing commands without visibility systems recording their actions. When the operation was discovered, limited logging meant incident responders would have difficulty determining whether operational commands were attempted or only communications were disrupted.

Distributed energy networks require continuous, OT-native visibility. Organizations should maintain a comprehensive view of all OT assets, such as RTUs, control systems, engineering workstations, historians, and IT/OT boundary devices, along with the protocols and paths they use. Network monitoring must interpret ICS protocols such as IEC-104, DNP3, and Modbus to detect anomalous control commands, unexpected sources of protocol traffic, and deviations from normal operational behavior. It is also critical to understand the known tactics, techniques, and procedures (TTPs) of adversaries such as ELECTRUM to be able to distinguish those quickly and add critical context for defenders.

Critical detection capabilities for DER operators include monitoring communications between control centers and every remote RTU, identifying patterns indicating multiple sites being access in sequence, tracking configuration changes on RTUs and edge devices, and alerting when multiple sites lose communications simultaneously. Without logged network traffic and OT commands prior to an attack, post-incident analysis cannot determine attack scope, techniques used, or whether equipment was manipulated.

Alerts should provide clear context: who initiated an action, which asset was affected, and what control function was invoked. This level of visibility is essential for detecting adversaries who misuse legitimate OT functionality rather than deploying obvious malware.

04. Secure Remote Access

Distributed energy facilities require extensive connectivity for operations, energy trading, maintenance, and vendor support, creating a substantial attack surface that was likely exploited in this case. Unlike centralized power generation, where on-site staff can perform many functions, DER models depend on remote operations. Service level agreements often mandate vendor access to meet availability commitments. This creates numerous access paths across dozens of sites, often using commodity VPN solutions to keep costs down.

Every remote access path to a DER site is a potential entry point. The systematic compromise demonstrates that adversaries can exploit these paths to move across a distributed portfolio. Organizations must enforce multi-factor authentication across all remote access, maintain comprehensive inventories of who has access to which sites, implement time-bound sessions that expire after specific maintenance windows, and monitor for access patterns like a single credential accessing multiple sites in rapid succession. Treating remote access as an operational convenience rather than critical infrastructure is no longer viable for DER operators.

05. Risk-based Vulnerability Management

This operation succeeded in gaining repeatable access. When the same firewall model with the same vulnerability or misconfiguration is deployed at multiple generation sites, a single exploit becomes a system-wide compromise. This is the central vulnerability management challenge for distributed generation: standardization that enables operational efficiency also enables adversary scalability.

Pay attention to edge systems at generation sites, such as firewalls and virtual private network (VPN) appliances, as these sit at the boundary between the internet and OT networks. A compromised firewall at a wind farm provides direct access to the RTUs that manage turbines. Organizations should maintain an inventory of devices across sites and treat those vulnerabilities as critical. Where rapid patching across dozens of remote sites is operationally challenging, implement compensating controls: enhanced monitoring to detect exploitation attempts, network segmentation to limit what compromised devices can reach, and access restrictions that reduce the attack surface.

References

[1] LowCarbonPower - https://lowcarbonpower.org/region/Poland

[2] CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations - https://hub.dragos.com/hubfs/116-Whitepapers/CrashOverride-whitepaper.pdf

[3] ELECTRUM and KAMACITE: Ten Years of Adversary Tradecraft in ICS Operations - https://hub.dragos.com/report/electrum-kamacite-ten-years-of-adversary-tradecraft-in-ics-operations

[4] The Five ICS Cybersecurity Critical Controls - https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls

About Dragos

Dragos is the world's leading OT cybersecurity firm headquartered in Washington DC, USA area with offices around the world. It provides the most effective OT cybersecurity technology for industrial and critical infrastructure to deliver on our global mission: safeguarding civilization. The Dragos Platform provides visibility and monitoring of OT environments for asset identification, vulnerability management, and threat detection with continuous insights generated by the industry's most experienced OT threat intelligence and services team. Dragos protects customers across the range of operational sectors, including electric, oil & gas, data centers, manufacturing, water, transportation, mining, and government.

Learn more: dragos.com