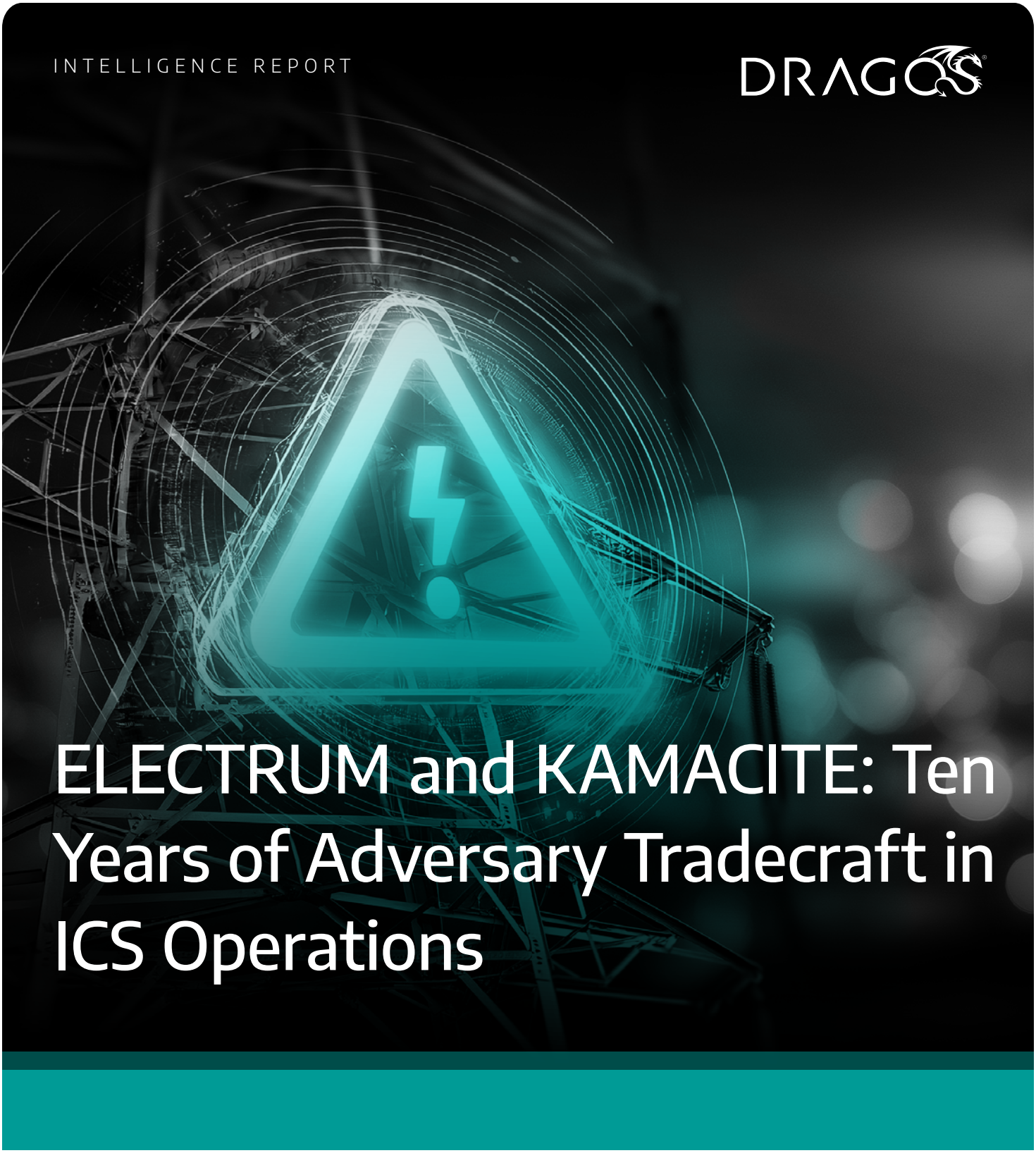
INTELLIGENCE REPORT

DRAGOS



ELECTRUM and KAMACITE: Ten Years of Adversary Tradecraft in ICS Operations

CO-AUTHORS:

KYLE O'MEARA, DIRECTOR, ADVERSARY HUNTING

BRYCE LIVINGSTON, ASSOCIATE PRINCIPAL ADVERSARY HUNTER

DRAGOS, INC

JANUARY 2026

Executive Summary

Since December 2015, a limited number of cyber operations have fundamentally altered how defenders assess risk to industrial control environments. Stuxnet demonstrated that adversaries could engineer cyber capabilities to manipulate industrial processes and cause physical impacts. Subsequent campaigns attributed to ELECTRUM and KAMACITE, beginning in 2015, demonstrated how these techniques could be operationalized at scale against civilian critical infrastructure, extending cyber-physical risk from exceptional cases into sustained threat activity.

Beginning with the first publicly confirmed cyber-induced power outages in 2015 and 2016, these operations demonstrated how access to enterprise networks could translate into deliberate disruptions of industrial control systems under real-world conditions. Over time, ELECTRUM's activity has shown that OT disruption does not require a constant escalation in technical complexity. Instead, the group has demonstrated the ability to apply different approaches - manual interaction, protocol-native tools, and destructive follow-on activity - depending on access conditions, objectives, and operational risk.

Importantly, the impact of these operations extends beyond the individual incidents themselves. The sustained use of OT-focused tradecraft over multiple years reflects the development of an experienced operational capability, repeatedly exercised under real-world conditions. This experience, once gained, does not dissipate. As a result, the risk posed by disruption of industrial processes is shaped not only by specific tools and campaigns but by the persistence of adversary knowledge, operational confidence, and tested execution models that remain relevant well beyond any single conflict or region.

This report examines ELECTRUM and KAMACITE's ICS-impacting operations to explain how OT disruptions became operationalized, sustained, and globally relevant to defenders confronting industrial cyber risk today.

ELECTRUM & KAMACITE Overview

ELECTRUM and KAMACITE are closely linked threat groups whose operations reflect a coordinated approach to achieving operational technology (OT) impact. While both KAMACITE and ELECTRUM have technical overlaps with activity tracked in open-source intelligence as Sandworm (also Seashell Blizzard, APT44), Dragos tracks ELECTRUM and KAMACITE as distinct threat groups based on their roles, tradecraft, and operational focus within intrusion campaigns targeting industrial environments.

KAMACITE operates primarily as an access and enablement threat group. Its activity focuses on establishing and maintaining initial access to targeted organizations, typically through techniques such as spearphishing, credential compromise, exploitation of exposed services, and lateral movement within enterprise environments. Beyond initial access, KAMACITE conducts reconnaissance and persistence activities intended to position operations closer to OT environments. In multiple campaigns, this positioning activity occurred over extended periods, indicating deliberate preparation rather than opportunistic intrusion.

ELECTRUM is responsible for executing actions on objectives that result in direct interaction with industrial control systems. Following access enablement, ELECTRUM conducts operations that bridge IT and OT environments, deploying tooling within operational networks, and performs ICS-specific actions that manipulate control systems or

disrupt physical processes. These actions have included both manual interactions with operator interfaces and the deployment of purpose-built ICS malware, depending on the operational requirements and objectives. ELECTRUM's activity demonstrates a working understanding of industrial architectures, control workflows, and protocol behavior sufficient to achieve real-world operational effects.

Taken together, ELECTRUM and KAMACITE represent a coordinated operational model in which access, positioning, and OT execution are treated as distinct but interdependent functions. This separation of roles has enabled sustained OT-focused activity across multiple incidents and operational contexts. Understanding how these threat groups interact and how their capabilities differ is essential for interpreting OT impact events later in this report and for assessing how similar intrusion paths may unfold in industrial environments today.

Evolution of ICS Capability

ELECTRUM's ability to affect industrial control systems did not emerge fully formed, nor did it follow a simple trajectory toward increasingly complex or automated attacks. Instead, the group's OT-focused capability evolved through a series of cyber attacks that clarified what was feasible, how disruption could be reliably executed, and how tradecraft could be sustained over time. These developments were shaped by deliberate adversary choices tied to their objectives rather than a single, continuous escalation in technical sophistication.

From Feasibility to Operational Reality

Early ICS-impacting operations attributed to ELECTRUM demonstrated that access to enterprise environments could be translated into direct manipulation of industrial control systems under real-world conditions. The December 2015 Ukraine power grid disruption marked the first publicly confirmed instance of a cyber operation directly manipulating ICS to interrupt civilian electric service. In that operation, adversaries used hands-on interaction with operator environments followed by enterprise compromise, leveraging legitimate interfaces and workflows to open breakers and disrupt power delivery.

While technically straightforward, this attack was operationally significant. It demonstrated that OT impact was not confined to bespoke, highly engineered attacks such as Stuxnet, but could be achieved against live civilian infrastructure using adversary tradecraft. At this stage, the primary constraint was not the ability to interact with control systems, but the reliability, timing, and discretion of execution. Achieving impact required sustained access and detailed operational knowledge, often gained through extended periods of undetected presence.

Operationalization Through Purpose-Built Tooling

Subsequent operations reflected efforts to reduce execution constraints by introducing tooling that directly interacts with industrial control system protocols. The December 2016 Ukraine power grid attack, which involved the deployment of CRASHOVERRIDE (also known as Industroyer), represented a clear shift toward operationalization. Rather than relying on manual interaction with operator interfaces, the malware could issue automated control commands via native ICS protocols.

This approach abstracted earlier manual actions into software, enabling faster execution and greater coordination under certain conditions. However, it also introduced dependencies on protocol compatibility, environmental

assumptions, and precise targeting. As a result, purpose-built ICS malware did not replace earlier techniques so much as expand the set of operational options available to ELECTRUM. Manual interaction and malware-enabled execution coexist; each is applied where most appropriate.

Sustained Capability, Stealth, and Tradecraft Flexibility

Later operations demonstrated ELECTRUM's ability to sustain OT-focused activity by selectively applying different techniques depending on access conditions, objectives, and tolerance for detection. The attempted deployment of Inudstroyer2 in 2022 illustrates this flexibility. While again leveraging purpose-built ICS malware, the operation was tightly scoped, time-bound, and closely aligned with broader operational objectives, reflecting a mature understanding of both opportunity and risk.

Through multiple campaigns, ELECTRUM has consistently emphasized stealth before OT execution. Extended dwell time, restrained activity within IT environments, and deliberate timing of OT actions suggest that avoiding premature detection was likely prioritized over speed and scale. In some cases, this included deep positioning within OT environments, such as access to supervisory control platforms like MicroSCADA, providing operational awareness that supported both manual and malware-enabled execution. In select cases, destructive components such as wiper malware were deployed after OT actions were completed, primarily to delay recovery or complicate response rather than serve as the primary mechanism of disruption.

Taken together, these operations illustrate a transition from initial feasibility demonstrations (2015) to operationalization through purpose-built tooling (2016) to a sustained capability characterized by flexibility in execution and careful management of detection risk. This evolution provides essential context for the ICS cyber kill chain described later in the next section and for the ICS impact events examined later in the report.

The ICS Cyber Kill Chain

OT-focused intrusions conducted by ELECTRUM and KAMACITE consistently follow a structured lifecycle that reflects the division of labor between the two threat groups and the operational requirements of targeting industrial environments. While individual operations vary in tooling, timing, and objectives, the underlying phases of activity remain largely consistent and provide a valuable framework for understanding how OT impact is achieved.

This lifecycle is characterized by KAMACITE's role in enabling access and positioning and ELECTRUM's role in executing OT-focused actions, including disruption and destruction. The phases below describe this progression and establish a structure for the ICS event deep dives that follow later in this report.

Initial Access and Foothold Establishment (KAMACITE)

Operations typically begin with KAMACITE establishing initial access to targeted organizations, most often within IT environments. This access is commonly achieved through spearphishing campaigns, exploitation of public-facing services, and the use of stolen credentials. At this stage, activity is generally indistinguishable from conventional IT intrusions and is focused on gaining a reliable foothold rather than immediate impact.

Once access is established, KAMACITE prioritizes persistence and operational security. This includes deploying both commodity and bespoke malware, maintaining redundant access paths, and avoiding actions that could trigger early

detection. The objective at this stage is not disruption, but durability, ensuring continued access long enough to support downstream operations.

Reconnaissance and Credential Expansion (KAMACITE)

Following initial access, KAMACITE conducts reconnaissance to understand the victim environment and identify pathways toward higher-value systems. This includes mapping network architecture, identifying domain relationships, harvesting credentials, and assessing boundaries between IT and OT networks.

During this phase, KAMACITE often focuses on identifying dual-homed systems, jump hosts, and administrative accounts that could facilitate lateral movement. Reconnaissance activity is typically deliberate and paced, emphasizing stealth and long-term positioning rather than rapid progression.

IT-to-OT Positioning and Preparation (KAMACITE & ELECTRUM)

Once sufficient access and environmental understanding are achieved, operations transition toward positioning within or adjacent to OT environments. This phase may involve accessing supervisory control systems, engineering workstations, or other systems that bridge IT and OT domains.

At this point, control of the operations shifts from KAMACITE to ELECTRUM. KAMACITE's role in maintaining access and supporting lateral movement continues, but ELECTRUM assumes responsibility for executing OT-focused actions. Preparation during this phase often includes validating access paths, assessing operational constraints, and determining appropriate execution methods based on objectives and risk tolerance.

OT Execution and Manipulation (ELECTRUM)

ELECTRUM conducts actions in OT environments and represents the point at which operations transition from access and preparation to direct interaction with industrial processes. Execution methods vary and may include manual interaction with control interfaces, automated actions using purpose-built ICS malware, or a combination of both.

Decisions made during this phase reflect a balance between operational impact and detection risk. Actions are often tightly scoped and time-bound, with execution aligned to broader objectives rather than opportunistic disruption.

Post-Execution Activity and Impact Management (ELECTRUM)

Following operations in OT environments, ELECTRUM may conduct additional action to manage operational outcomes. This can include deploying destructive components, such as wiper malware, primarily to delay recovery, complicate response efforts, or obscure forensic visibility. These actions are typically sequenced after manipulation of the OT environment rather than used as the primary mechanism for OT impact.

In other cases, post-execution activity may involve withdrawal from the environment, maintaining dormant access for future use, or transitioning to alternative objectives. The specific approach depends on mission goals and the assessed value of continued access.

ICS Cyber Kill Chain Summary

The ICS cyber kill chain described above highlights the complementary roles of KAMACITE and ELECTRUM and underscores that OT-focused attacks are the culmination of extended, multi-phase operations rather than isolated actions. By separating access enablement from OT execution, these threat groups demonstrate an operational model designed for flexibility, stealth, and sustained capability.

This lifecycle framework provides the foundation for the ICS event deep dives that follow, where individual operations are examined in detail using these phases as a consistent analytical lens.

ICS Impact Event Deep Dives

This section examines select ICS-impacting operations attributed to ELECTRUM and KAMACITE using the lifecycle described in the previous section. Each deep dive focuses specifically on OT-relevant activity and impact, rather than providing a comprehensive recounting of enterprise compromise or geopolitical context.

Events are analyzed using a consistent structure to highlight adversary tradecraft, execution choices, and operational constraints. This approach enables comparison across campaigns and supports identification of enduring patterns in OT-focused adversary behavior.

It is important to note that the events examined here do not represent an exhaustive accounting of all OT-impacting activity attributable to these groups. The ongoing Ukraine-Russia conflict, along with limitations in visibility, attribution confidence, and reporting, means that some operations may not be observable or cannot be conclusively assessed. Rather than speculate on unconfirmed activity, this analysis focuses on well-documented incidents where OT impact can be reliably evaluated. Taken together, these events provide sufficient insight into how OT disruption is enabled, executed, and sustained under real-world conditions.

2015 Ukraine Electric Grid Attack

The electric power grid is generally organized into three primary functional domains: generation, transmission, and distribution. Electricity is generated at power plants, transmitted over long distances via high-voltage transmission lines, and subsequently stepped down to lower voltages for delivery to end customers through distribution networks. Along both transmission and distribution systems, substations serve critical roles, including voltage transformation, switching, and feeder management, as well as fault detection and protection.

Substations control the routing and flow of electrical power across transmission and distribution lines through the coordinated operation of switching equipment, most notably circuit breakers. These devices manage the energization and de-energization of electrical paths within the grid. Opening a breaker interrupts the electrical circuit, removing the flow of power along that line segment and de-energizing the associated downstream infrastructure.

This operational reality was exploited during the 23 December 2015 cyber attack on the Ukrainian electric distribution sector, in which three oblenergos (regional control centers for distribution) were deliberately disrupted through unauthorized access to operator control environments. ELECTRUM leveraged compromised remote access to distribution control systems to issue legitimate control commands through supervisory interfaces, remotely opening

circuit breakers, and interrupting the flow of electricity. Rather than exploiting physical equipment failures or protocol-level vulnerabilities, the attackers misused standard ICS functionality to achieve operational impact.

The coordinated opening of breakers at three oblernegos caused widespread outages, impacting over 60 substations serving hundreds of thousands of customers. The incident underscored the systemic risk posed by ELECTRUM's access to grid control systems and highlighted the operational and societal consequences of malicious manipulation of electric distribution infrastructure.

2016 Ukraine Electric Grid Attack with CRASHOVERRIDE

By 2016, ELECTRUM had shifted from opportunistic disruption to attempting a repeatable, weaponized capability: CRASHOVERRIDE. Rather than simply reusing the tactics observed during the 2015 operation, ELECTRUM pursued a fundamentally different approach aimed at embedding disruptive functionality directly within the power system environment.

Instead of relying primarily on remote operators interacting with human-machine interfaces (HMIs), the 2016 activity focused on introducing malicious logic into systems integral to grid operations, enabling disruption to be executed programmatically rather than manually.

The intrusion once again originated within enterprise IT environments; however, the critical inflection point occurred during lateral movement. Attackers gained access to a dual-homed system that bridged both IT and ICS/OT networks, serving as a conduit into the control center environment. This pivot highlighted the operational risk posed by systems that span trust boundaries between corporate and operational networks.

From this position, ELECTRUM targeted data historian infrastructure, which occupies a central role at the intersection of operational control and system visibility. By compromising multiple database servers and harvesting credentials, the adversary obtained privileged access deep within the control environment. That access was then abused in a manner particularly relevant to defenders: legitimate database functionality, specifically Microsoft SQL Server features such as `xp_cmdshell`, was leveraged to execute operating system–level commands, effectively transforming trusted infrastructure into an execution and staging platform.

With this foothold established, ELECTRUM deployed CRASHOVERRIDE, the first publicly documented malware framework designed to natively communicate using electric power system protocols. CRASHOVERRIDE used 4 ICS specific protocols, IEC 104 - a protocol for 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. This marked a departure from IT-centric malware repurposed for ICS/OT environments, representing purpose-built tooling for grid disruption.

The operational intent was explicit. Rather than depending on human operators to issue control commands, CRASHOVERRIDE sought to automate disruption by directly interacting with protective relays and ABB-controlled switchgear through protocol-level communications.

In execution, the operation failed to achieve the scale and duration of impact observed in 2015. Design limitations, deployment errors, and mismatches between the malware's assumptions and the target environment constrained the resulting outage. However, the reduced operational impact should not be interpreted as a strategic failure.

Measured correctly, the 2016 activity represents a clear escalation: a transition from manual, operator-driven disruption to system-native, protocol-aware automation capable of enabling repeatable effects against electric grid infrastructure.

2022 Industroyer2 Event

In March 2022, multiple malicious capabilities were identified within a Ukrainian electric distribution utility, prior to the execution of a planned disruptive operation. This pre-positioning provided early visibility into an adversary campaign that again demonstrated ELECTRUM's continued focus on electric grid operations.

The primary disruptive capability identified was Industroyer2, a new variant of the previously observed CRASHOVERRIDE malware framework. Industroyer2 is an industrial control system (ICS)–capable malware designed to communicate directly with electric grid equipment using the IEC 60870-5-104 (IEC-104) protocol. Through native protocol interactions, the malware is capable of issuing commands to manipulate breaker states—opening or closing circuits—thereby enabling direct physical effects on power distribution operations.

Industroyer2 exhibits numerous technical overlaps with the original CRASHOVERRIDE IEC-104 module, including similarities in protocol implementation, shared code structures, and overlapping string artifacts. Notably, the malware contained highly specific configuration data, including explicitly defined target substations and associated information object addresses (IOAs). This level of detail suggests that ELECTRUM possessed a deep understanding of the victim's environment, including control logic, device addressing, and grid topology.

In parallel with Industroyer2, the adversary deployed a coordinated set of destructive malware capabilities, consisting of multiple wipers and a propagation mechanism, intended to degrade recovery efforts and amplify operational impact.

Destructive and Supporting Malware Observed

- CaddyWiper was deployed as part of the March 2022 operation and was designed to destroy data on compromised systems irreversibly, rendering affected hosts inoperable. Its presence aligns with prior ELECTRUM operations in which wipers were used to impede restoration and incident response activities.
- SoloShred was identified during the same incident and specifically targeted Solaris-based systems. The malware leverages native system utilities to overwrite disk contents, resulting in permanent data loss and system failure.
- AwfulShred was also deployed during the Industroyer2 incident and had previously been observed during the compromise of Ukrinform. In addition to destroying disk contents using tools such as shred or dd, AwfulShred disables HTTP and SSH services, further limiting remote management, forensic access, and recovery operations.
- While not a wiper itself, OrcShred functioned as a propagation and tasking mechanism within the environment. The worm scheduled execution of either AwfulShred or SoloShred depending on the operating system present on the infected host, enabling automated and adaptive deployment of destructive payloads across mixed environments.

Taken together, the combination of Industroyer2 and coordinated wiper deployment reflects a deliberate strategy to pair grid-disruptive capabilities with systemic destruction of IT and OT-adjacent infrastructure, increasing both the immediacy of operational impact and the complexity of recovery.

This incident further reinforces ELECTRUM's evolution toward tightly integrated campaigns that blend protocol-aware ICS malware with destructive payloads, designed not only to disrupt power delivery but also to degrade an operator's ability to respond, investigate, and restore service.

2022 MicroSCADA EOL Compromise

In October 2022, ELECTRUM conducted a disruptive operation targeting a Ukrainian electric substation, continuing the group's sustained focus on electric grid infrastructure. Earlier, in June 2022, ELECTRUM had gained access to a hypervisor hosting an end-of-life (EOL) instance of MicroSCADA within the substation's operational technology (OT) environment. The extended dwell time between initial access and operational activity suggests deliberate reconnaissance and preparation rather than opportunistic exploitation.

Following this access, ELECTRUM attempted to execute a set of custom living-off-the-land (LOTL) scripts designed to degrade the availability and control of the targeted substation. These scripts leveraged native system tools and legitimate administrative functionality rather than introducing bespoke malware into the OT environment. This approach mirrors earlier ELECTRUM operations that favored misuse of trusted infrastructure to blend malicious activity with normal operational behavior.

In parallel, ELECTRUM deployed a new variant of CaddyWiper to systems within the associated IT environment. The wiper activity appears intended to remove operational artifacts, complicate forensic analysis, and hinder incident response, consistent with destructive actions observed during ELECTRUM operations in 2015 and early 2022. The reintroduction of wiper malware reinforces a recurring pattern in which grid-focused disruption is paired with data destruction to limit recovery and attribution.

From an operational lifecycle perspective, these actions satisfy Stage 1 (Initial Access and Reconnaissance) and Stage 2 (Execution and Control) of the ICS Cyber Kill Chain, demonstrating ELECTRUM's ability to position itself for potential physical effects even when final impact cannot be confirmed.

At present, Dragos assesses that ELECTRUM's period of dormancy following initial access most likely reflects continued system reconnaissance, environment mapping, and collection of operational data, rather than disengagement. However, Dragos cannot confirm whether the October 2022 operation successfully interrupted substation operations or resulted in power outages.

The initial compromise vector associated with the June–October 2022 activity remains unidentified, and the absence of definitive outage confirmation highlights the challenges inherent in assessing cyber effects within complex OT environments.

Adversary Patterns Across OT Impact Events

Analysis of ICS impact events attributed to ELECTRUM and KAMACITE reveals recurring patterns that persist across campaigns, tools, and time periods. While individual operations differ in execution and scope, the consistency of these patterns underscores how OT-focused attacks are structured, enabled, and carried out in practice.

This section synthesizes observations drawn from multiple OT impact events to highlight enduring characteristics of ELECTRUM and KAMACITE's tradecraft.

Division of Labor Between Access and Execution

Across OT impact events, a clear separation of responsibilities is observed between KAMACITE and ELECTRUM. KAMACITE consistently operates upstream of OT execution, establishing and maintaining access, conducting reconnaissance, and positioning operations closer to OT environments. ELECTRUM assumes responsibility once conditions are suitable for OT-focused activity, including execution and impact management. This separation enables flexibility in execution timing and methods while reducing the operational risk associated with premature OT interaction.

Emphasis on Stealth and Prolonged Positioning

OT impact events are typically preceded by extended periods of low-profile activity. KAMACITE's access operations emphasize persistence and discretion, while ELECTRUM's OT-focused actions are often tightly scoped and deliberately timed. Across events, avoiding premature detection appears to take precedence over speed and scale. This pattern suggests that OT impact is treated as a deliberate outcome of sustained access rather than opportunistic escalation.

Flexible Execution Methods

ELECTRUM demonstrates flexibility in how cyber-physical operations are performed. Both manual interaction with control systems and automated execution using protocol-native malware are observed, with the chosen method reflecting access conditions, operational objectives, and operational risk. The coexistence of these approaches indicates that custom tooling is not a prerequisite for OT impact, nor does its presence eliminate the relevance of manual execution.

Depth of OT Knowledge Before Execution

Cyber-physical events impacting OT consistently reflect a level of operational awareness that extends beyond surface-level access. Visibility into control workflows, system state, and operational dependencies informs execution decisions and timing. This awareness reduces the likelihood of unintended consequences and supports precise manipulation of industrial processes rather than indiscriminate disruption.

Expansion of Targeting Beyond Traditional Geographies

More recent activity attributed to KAMACITE indicates continued access-oriented operations extending beyond previously observed regional focus. Through at least July 2025, KAMACITE has been observed conducting scanning activity against industrial devices located in the United States. This activity did not immediately culminate in publicly reported OT disruption, but it is notable for its geographic scope and target selection.

The observed scanning activity suggests an effort to identify exposed or weakly protected assets outside of Ukraine, where both KAMACITE and ELECTRUM have focused much of their effort for the past 3 years. While scanning alone does not indicate imminent OT impact, its occurrence within U.S.-based industrial environments highlights the

broadening of targeting considerations and reinforces that KAMACITE's access operations are not confined to a single region or operational context.

Within the lifecycle described in this report, such activity aligns with early-stage access identification and positioning. Its relevance lies not in immediate effect, but in what it reveals about how potential future OT-focused operations may be scoped and prepared.

Implications for OT Defenders

Taken together, these patterns illustrate that OT-focused attacks are not defined by a single technique or tool, but by a structured approach that combines access enablement, positioning, deliberate execution, and impact management. Defenders should therefore prioritize detection and response capabilities that address progression toward OT impact rather than focusing solely on individual malware families or execution techniques.

Recent access-oriented activity attributed to KAMACITE, including scanning of industrial devices in the United States, reinforces the relevance of this lifecycle-based perspective. While such activity does not indicate imminent OT disruption, it highlights how early-stage operations may occur well outside historically affected regions and long before any visible OT impact. For defenders, this underscores the importance of monitoring for precursor activity, such as asset exposure, anomalous access attempts, and unauthorized interaction with OT-adjacent systems, before execution phases are reached.

Understanding how KAMACITE and ELECTRUM operate across phases, and how their roles intersect, provides a more reliable basis for identifying OT risk than treating each event as an isolated incident. Defenders that can identify and disrupt activity earlier in this progression are better positioned to prevent OT impact altogether, rather than responding only after physical processes are affected.

Strategic Assessment & Outlook

The activity examined in this report demonstrates that OT-focused cyber operations attributed to ELECTRUM and KAMACITE are best understood as the result of sustained operational capability rather than isolated or exceptional incidents. Once the feasibility of cyber-enabled OT disruption was established, subsequent operations clarified how such activity could be operationalized, retained, and selectively applied under different conditions and objectives. This transition from demonstration to durable capability represents a lasting shift in how OT cyber risk must be assessed.

A defining characteristic of this capability is the separation of roles between access enablement and OT execution. KAMACITE's access-oriented operations create the conditions under which OT impact becomes possible, while ELECTRUM applies execution tradecraft when timing, access, and risk tolerance align. This division of labor enables flexibility in execution and allows OT impact to remain an option, even when it is not immediately exercised. This extends risk beyond discrete incidents and into prolonged periods of latent exposure.

Notably, the observed evolution of this capability does not indicate a requirement for increasingly complex or novel techniques. Instead, ELECTRUM's operations reflect deliberate selection among established approaches, manual interaction, protocol-native malware, and selective destructive follow-on activity, based on operational context. This

reinforces that the barrier to OT impact is less about technical innovation and more about access, positioning, and operational awareness.

More recent access-stage activity attributed to KAMACITE, including scanning of industrial devices outside of Ukraine through 2025, reinforces that this operational model is not geographically constrained. While such activity does not imply imminent OT disruption, it highlights that the preparatory phases of OT-focused intrusions may occur broadly and well in advance of any observable impact, underscoring the persistence and portability of this capability.

For defenders, the strategic implication is clear: OT risk is shaped by progression, not by singular moments of execution. Organizations that focus solely on detecting OT malware signatures or disruptive actions may miss earlier indications that access and positioning are underway. Conversely, defenders who understand and monitor the full lifecycle of OT threats, from initial access to OT positioning to ICS impact, are better equipped to disrupt malicious operations before physical processes are affected. As demonstrated throughout this report, sustained visibility, intelligence, and OT-native detection across the ICS cyber kill chain are essential to addressing a risk that persists not because it is new, but because it remains operationally viable.

Taken together, ELECTRUM and KAMACITE activity illustrates how OT-focused cyber operations persist not through constant escalation, but through sustained access, selective execution, and careful management of detection risk. As industrial environments continue to evolve, this operational model remains relevant. Not because it is new, but because it remains viable.

Apply the 5 Critical Controls for World-Class OT Cybersecurity

Apply the 5 Critical Controls for World-Class Cybersecurity, as recommended by SANS. 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 and KAMACITE operations described in this report.

1. ICS INCIDENT RESPONSE

Prepare and routinely exercise an OT-specific incident response plan that accounts for adversary behavior observed across ELECTRUM and KAMACITE campaigns. These operations demonstrate that OT impact is typically preceded by extended dwell time, quiet access enablement in IT environments, and deliberate positioning near or within OT networks. Incident response planning should therefore emphasize early containment before an OT attack, as well as a coordinated response when OT manipulation is attempted.

Start by identifying which OT systems, supervisory platforms (such as SCADA and engineering workstations), and IT/OT boundary assets would require immediate isolation during an incident. Plans should explicitly address scenarios involving both manual control manipulation through operator interfaces and protocol-native attacks using ICS protocols such as IEC-104 or IEC-61850. Because multiple ELECTRUM operations paired OT execution with destructive malware to delay recovery, response playbooks should include procedures for loss of visibility, corrupted systems, and degraded recovery tooling.

When indicators of compromise or suspicious OT-adjacent activity are detected, containment actions should be executed promptly in accordance with predefined authority and escalation paths. If an incident is declared or

assistance is required, Dragos Incident Response is available to support OT-specific containment, investigation, and recovery.

2. DEFENSIBLE ARCHITECTURE

Design and maintain a defensible OT architecture that limits an adversary's ability to move from IT access into OT execution. ELECTRUM and KAMACITE repeatedly exploited trusted relationships, dual-homed systems, and permissive architectures rather than novel vulnerabilities. OT environments should therefore be treated as high-consequence systems requiring deliberate segmentation and access control.

Restrict administrative and engineering access to OT systems through dedicated management networks and hardened jump hosts. Eliminate unnecessary dual-homed systems and ensure that historians, virtualization platforms, and supervisory servers that bridge IT and OT are tightly controlled and monitored. Disable unused services and administrative functions on OT-adjacent infrastructure and enforce change control for configuration updates that affect operational access or control paths.

Where legacy or end-of-life OT platforms are in use, apply compensating architectural controls such as segmentation, access restriction, and enhanced monitoring to reduce the likelihood that these systems can be abused for OT positioning or execution.

3. ICS NETWORK VISIBILITY & MONITORING

Maintain continuous, OT-native visibility into assets, communications, and control activity across the environment. ELECTRUM operations relied heavily on stealth and the misuse of legitimate ICS functionality, making traditional IT-focused monitoring insufficient for detecting malicious activity.

Organizations should maintain a single, trusted view of OT assets, including control systems, engineering workstations, historians, and IT/OT boundary devices, along with the protocols and control paths they use. Network monitoring should be capable of interpreting ICS protocols and detecting anomalous control commands, unexpected sources of protocol traffic, and changes in normal operational behavior.

These requirements are increasingly reflected across global regulatory and standards frameworks governing critical infrastructure and industrial cybersecurity. While implementation approaches vary by region, there is broad alignment on the need for OT-native visibility that can detect malicious activity that blends into normal industrial operations. This includes expectations articulated through frameworks such as NERC CIP and INSM in North America, NIS2 and related national guidance in Europe, UK CAF guidance, and comparable regulatory and policy initiatives across the Middle East, Australia, and Asia.

Alerts should provide clear context around who initiated an action, which asset was affected, and what control function was invoked. The Dragos Platform centralizes this OT-native visibility and applies Dragos threat intelligence to help analysts identify adversary behavior earlier in the kill chain. OT Watch services further support proactive threat hunting and investigation to identify precursor activity before OT execution occurs.

4. SECURE REMOTE ACCESS

Secure all remote access paths into OT environments, as credentialed access and trusted remote connections were foundational to every observed ELECTRUM and KAMACITE operation. Remote access should be treated as a primary risk factor rather than a convenience capability.

Enforce strong authentication, including multi-factor authentication, for all remote access into OT-adjacent systems such as jump hosts, engineering workstations, and supervisory platforms. Apply least-privilege access models and regularly audit user accounts to ensure access remains aligned with operational need. All remote sessions should be logged, monitored, and time-bound, with the ability to disable access quickly if suspicious behavior is observed.

Pay particular attention to credential reuse between IT and OT environments, as adversaries repeatedly leverage enterprise credentials to pivot into OT environments.

5. RISK-BASED VULNERABILITY MANAGEMENT

Apply risk-based vulnerability management focused on reducing adversary access and positioning opportunities rather than patching in isolation. ELECTRUM and KAMACITE demonstrated that exploitation of known weaknesses, legacy platforms, and legitimate system functionality can be sufficient to achieve OT impact.

Prioritize remediation based on operational risk, exposure to IT or remote access paths, and the role of the asset in enabling lateral movement toward OT systems. OT assets that sit at trust boundaries, host supervisory functions, or provide administrative access should receive the highest priority.

Where patching is not feasible, particularly for legacy or end-of-life OT systems, implement compensating controls such as stricter access restrictions, segmentation, and enhanced monitoring. The Dragos Platform supports this approach by maintaining accurate OT asset inventory and aligning remediation decisions with Dragos Now / Next / Never vulnerability prioritization methodology.

ABOUT DRAGOS, INC.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. 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.

Request a Demo