9TH ANNUAL | 2026

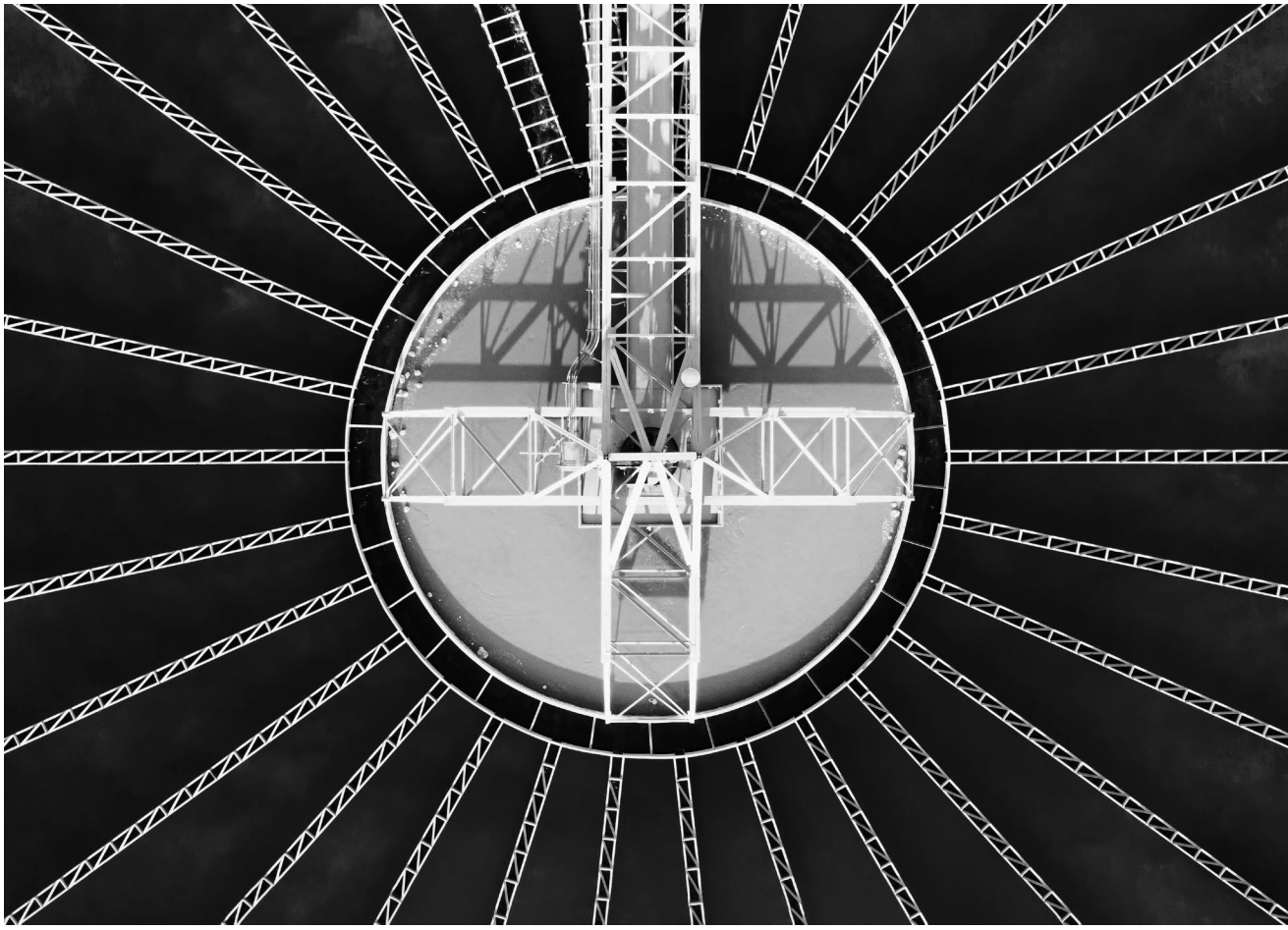
YEAR IN REVIEW

OT/ICS CYBERSECURITY REPORT

Table of Contents

Table of Contents (cont.)

Table of Contents (cont.)



A Message From Our Founder

Ten years ago, Jon Lavender, Justin Cavinee, and I founded Dragos with a focused passion on protecting OT from those who meant it, and the communities that depend on it, harm. When I started my career in this field there was no compendium of knowledge of the threats, vulnerabilities, and what insights could be shared from engagements like incident response. There were anecdotal insights and hushed rumors with lots of claims of classified insights hidden away somewhere. It is hard to build a professional community and have an understanding of what the right security efforts are on anecdotal insights. With that in mind, I started the Year in Review 9 years ago as a freely available report capturing the Dragos team's knowledge on the threat landscape. Our goal was simple, keep the product pitching out of it and share whatever we are legally and ethically allowed to share that helps empower defenders. OT cybersecurity is obvious to people as necessary now, but ten years ago it was not. I remember telling the team early on that if Dragos failed it would at least be the Year in Review report we could leave behind; that every year we were contributing something useful to the community that could outlast us. Ten years later I'm proud that we are not at risk of going away and we are still sharing with this community we all love so much.

I hope you enjoy the report, take insights from it to drive your security efforts, and are able to share the knowledge contained here to help others understand that OT is the critical part of critical infrastructure. It is worthy of protection and can be protected. It is not easy to be in this field, you as the reader know that first hand. But OT cybersecurity isn't a market, it isn't a category, it's a mission - focused on protecting people against some of the worst adversaries imaginable. Adversaries that target civilian infrastructure, go after our communities, and willfully accept risk up to and including the loss of human life of our loved ones, families, of our children. Armed with knowledge you can go from being the victim to being the hunter against these adversaries. In this report my team professionally calls them Threat Groups. Internally to Dragos we just call them what they are, assholes.

Happy Hunting,

Robert M. Lee, CEO

Introduction

In 2025, adversaries targeting operational technology (OT) crossed a line that had previously been limited to a small number of well-known attacks impacting industrial control systems (ICS). They are no longer simply gaining access and waiting. Multiple threat groups, independently and across different geopolitical alignments, moved into actively mapping control loops: identifying engineering workstations, exfiltrating configuration files and alarm data, and learning how physical processes operate well enough to disrupt them. This is the removal of the last practical barrier between having access and being able to cause physical consequences. It indicates that the teams behind these operations are being told to prepare to act, not just to maintain options.

Adversaries Are Mapping Control Loops to Cause Physical Impact

This year's report introduces three new threat groups - AZURITE, PYROXENE, and SYLVANITE - and documents significant evolution in established groups like VOLTZITE, KAMACITE, ELECTRUM, and BAUXITE. Several of these groups now operate in paired models where one team develops initial access and hands it off to a second team with ICS-specific capability. That division of labor compresses the timeline from compromise to operational readiness, in some cases from weeks to days, and lowers the barrier for the groups that ultimately cause impact.

ELECTRUM, the group responsible for the Ukrainian power outages in 2015 and 2016 and the most operationally experienced infrastructure-attack group Dragos is aware of, expanded its targeting beyond Ukraine into Poland in late December 2025. That attack, which targeted decentralized energy resources including combined heat and power facilities and renewable energy management systems, was the first major coordinated cyberattack against DERs anywhere in the world.

Meanwhile, KAMACITE, the access development team that feeds ELECTRUM, expanded from Ukrainian targets into the European OT supply chain and conducted sustained reconnaissance of internet-exposed industrial devices across the United States between March and July 2025. The scanning was not opportunistic. It targeted specific components in a sequence that suggests intent to understand entire control loops, not isolated devices. The pattern is consistent with what you would expect from a team being told to prepare for operations, not just collect.

Exploits Are Weaponized in 24 Days But Mitigation Takes Longer

Adversaries also moved faster on vulnerabilities in 2025. Median time from disclosure to public exploit: 24 days. Four percent of ICS vulnerabilities were actively exploited at disclosure and in multiple incident response cases, Dragos reported exploited vulnerabilities to vendors and waited 90+ days for public advisories while attacks continued elsewhere. Meanwhile, 26 percent of advisories offered no patch, and 25 percent contained incorrect CVSS scores, leaving defenders with incomplete or wrong guidance while adversaries operationalized exploits.

Ransomware Shutdowns Are Operational Incidents Being Mislabeled as IT

Ransomware continued to hit industrial organizations hard. Dragos tracked 119 ransomware groups impacting over 3,300 industrial organizations in 2025, compared to 1693 attacks in 2024. But the numbers understate the problem. There is a persistent and significant mischaracterization of ransomware incidents as IT-only, driven by responders who see a Windows operating system and classify the incident without recognizing that the system was hosting SCADA software or functioning as an engineering workstation.

Gap Between Adversary Capability and Defender Visibility Is Widening

The most concerning finding in this report may be the simplest one. Thirty percent of Dragos incident response cases in 2025 started not with a detected intrusion or a ransom note, but with someone saying: something seems wrong. In the majority of those cases, the data needed to answer whether cyber was involved had never been collected. OT network telemetry is transient. If you are not recording it when it happens, it is gone. You cannot investigate what you cannot see, and in a growing number of cases, asset owners are making public statements that incidents had nothing to do with cyber not because they determined that to be the case, but because they lacked the data to determine anything at all.

Dragos estimates that fewer than 10 percent of OT networks worldwide have network visibility and monitoring in place. Everything in this report is drawn from that fraction. The threats documented here are also operating in the environments that are not looking. The 26 threat groups Dragos tracks, the 3,300+ ransomware incidents, the vulnerability findings, and the lessons from the field all represent the minimum view, not the maximum.

OT Security Fundamentals Remain the Most Effective Defense

The fundamentals of OT security - knowing what is in your environment, monitoring what is happening, controlling access, and being prepared to respond - remain the most effective defense against every threat in this report. Ninety percent of the asset owners Dragos works with still cannot detect the style of attack that ELECTRUM used a decade ago. As the threats get more aggressive and infrastructure gets more complex, the gap between what adversaries can do and what defenders can see is widening. The operational tempo of adversaries now outpaces the detection capabilities of most defenders. Closing that gap is not a technology problem. It is a prioritization and investment problem, and the window to address it is getting smaller.

Methodology and Sourcing

Dragos focuses on Operational Technology (OT) environments only; therefore, this report covers only that scope. To identify OT specific threat groups, Dragos aligns with the SANS ICS Cyber Kill Chain paper and the Diamond Model paper.[1,2] If a threat has targeted organizations with OT networks, that alone is not enough to be a Stage 1 adversary. The organization's targeting must be due to its OT networks, which support the assessment that it is a Stage 1 adversary. If the adversary gains access to OT networks and the activity appears intentional, the assessment is that they are a Stage 2 adversary. Furthermore, Dragos tracks Temporary Activity Threads (TATs) to gather and disseminate information about unidentified or emerging cyber threat groups or activity. TATs serve as a provisional classification for clusters of cyber threat activities that have not yet reached a level of analytical rigor to be designated as an enduring Threat Group. It is important to note that the level of insight and data collection in OT networks worldwide remains minimal, despite their criticality, and they remain an emerging area. Dragos estimates that fewer than 10 percent of OT networks worldwide have visibility and monitoring. However, the nature of threats and vulnerabilities yields insights that can be applied more broadly and are representative of the community as a whole. With enhanced visibility and monitoring, new threats would be discovered, but not at a linear scale with the visibility gained. Despite this, Dragos maintains the largest source of such insights into OT networks globally.

The Dragos Intelligence Fabric is the primary source for the Year in Review report. It is composed of numerous sources, including first-party data sets tied to the Dragos Platform technology, which is deployed at thousands of sites globally. Insights from the Dragos Platform are available when customers use the OT Watch and OT Watch Complete 24/7 monitoring services, optionally opt in to Neighborhood Keeper, or take advantage of the Dragos Incident Response services. The Dragos intelligence team leverages these sources, trusted second parties and partners, and third-party datasets, both commercially available and those available only through unique collaborations. As part of intelligence reporting, Dragos's Vulnerability Analysts utilize the Now, Next, Never methodology.[3] Now, Next, and Never are the priorities we set for vulnerabilities in the Dragos Platform. These factors are considered in vulnerability assessments, and the determination is included in the database advisory as "Now" vulnerabilities. Dragos investigates each vulnerability and provides an assessment that typically includes mitigation advice if a patch cannot be applied immediately or if the vendor doesn't provide a patch or alternative mitigation. The evaluation considers the vulnerable component and how that impacts the rest of the process. The "Next" vulnerabilities can be mitigated through proper network segmentation, returning us to the defensible architecture critical control. Often, network segmentation can be implemented without disrupting the industrial process, whereas patching these devices may cause an outage. After the network is segmented, adversaries must follow paths and chokepoints to penetrate deeply into the industrial network, where asset owners have the best visibility to monitor for exploitation. The "Never" vulnerabilities are items that will not reduce the device's inherent risk to your process, even if you fully remediate. These vulnerabilities are generally overhyped, challenging to exploit, and can be mitigated by the available features.[4]

1 **The Diamond Model of Intrusion Analysis – US Department of Defense**
https://apps.dtic.mil/sti/pdfs/ADA586960.pdf

2 **The Industrial Control System Cyber Kill Chain – SANS**
https://www.sans.org/white-papers/36297

3 **Towards Improving CVSS – Carnegie Mellon University**
https://www.sei.cmu.edu/documents/574/2018_019_001_538372.pdf

4 **Risk-Based Vulnerability Management for Operational Technology – Dragos**
https://hub.dragos.com/hubfs/116-Datasheets/Dragos_Risk-Based_Vulnerability_Management_OT_Cybersecurity.pdf?hsLang=en

These sources make the Dragos Intelligence Fabric the world's largest dataset on OT security insights, covering threats and vulnerabilities. However, it is not a complete view, and no government, vendor, or other entity can have one. Therefore, it is important for readers to take the assessments as the minimum, not the maximum, view. For example, if a threat group is known to target a specific industry or country, that will be stated, but it should not be taken to mean that no other industry or country is targeted. It is common for some industries and countries to invest very little in OT network visibility and monitoring or in OT-specific services, leaving them with few insights. Throughout the report, where further sourcing is available, it will be noted whether the insight comes from OT Watch, Neighborhood Keeper, the intelligence team's hunting, or Dragos Services, such as incident response or assessments.

01.

Dragos Identifies Three New Threat Groups in 2025

Dragos now tracks 26 threat groups that target OT environments specifically because of their industrial operations. Eleven of those were active last year. In 2025, Dragos identified three new groups demonstrating a critical shift: adversaries moving from prepositioning for future attacks to actively mapping control loops and understanding how to manipulate physical processes.

AZURITE and PYROXENE operate inside OT environments, exfiltrating alarm data, configuration files, and operational intelligence from engineering workstations. SYLVANITE operates as an initial access provider, rapidly weaponizing edge device vulnerabilities and handing off compromised environments to Stage 2 adversaries like VOLTZITE within days. This division of labor compresses the timeline from initial breach to operational impact.

SINCE 2021

Az

New Threat Group:

AZURITE

ICS IMPACT: Loss of confidentiality, and theft of operational information, long-term access and offensive operations enablement.

Infrastructure

- Use of compromised SOHO networking equipment for communications
- Multi-tiered management of controller nodes, proxy/relay notes, and infector nodes
- Usage of other multiuse ORBs associated with several threat groups

Adversary

- Overlap with Flax Typhoon, Ethereal Panda, UNC5923, Raptor Train, Red Dev 54, TAT-2023-35, TAT-2023-46, TAT-2025-16
- Likely has the same adversary customer as VOLTZITE

Victimology

- Targets Taiwan, United States, Europe, Japan, South Korea, Australia
- Targets Manufacturing, Defense, Automotive, Electric, Government, Oil and Gas

Capabilities

- Strong operational security practices
- Heavily uses living off the land binaries and techniques
- Exploits a wide array of vulnerabilities using public POCs
- Initial reconnaissance of a target is conducted in a slow and steady fashion to evade detection, especially internally
- Use of open-source offensive security tooling, e.g. Mimikatz, Metasploit, JuicyPotato
- Use of multiple web shells - Chopper, AntSword, SuperShell, devilszshell, and Godzilla
- Exploitation of internet-facing Ivanti, Fortinet, Cisco, and F5 assets

About AZURITE

This year, Dragos introduced a new threat group, AZURITE, an ICS Kill Chain Stage 2 adversary targeting OT engineering workstations and exfiltrating OT operational data. While Dragos assesses with moderate confidence that AZURITE does not possess a Stage 2 tool or malware capability in its arsenal designed specifically to target OT processes, hardware, protocols, or software, they have demonstrated the capability to operate in OT environments using reconnaissance, lateral movement, and actions on objective. AZURITE's interest in targeting and exfiltrating of OT operational data, project files, alarm data, process information, employee operator information, etc., versus typical intellectual property (IP) theft, is demonstrative of AZURITE's intent and motivation to collect OT information that almost certainly assist in developing OT specific tooling or malware capabilities for either the AZURITE operators or AZURITE's adversary customer. AZURITE conducts interactive operations with engineering workstation hosts to identify information of interest and stages the data outside of the OT network for exfiltration. AZURITE demonstrates knowledge of OT-centric software for operating or monitoring OT processes. AZURITE has not been observed manipulating, stopping, or modifying OT-specific software; it has only identified and exfiltrated information already on target assets. This activity is highly likely to support capability development, target designation, and environment awareness for the preparation of offensive operations in case of geopolitical conflict.

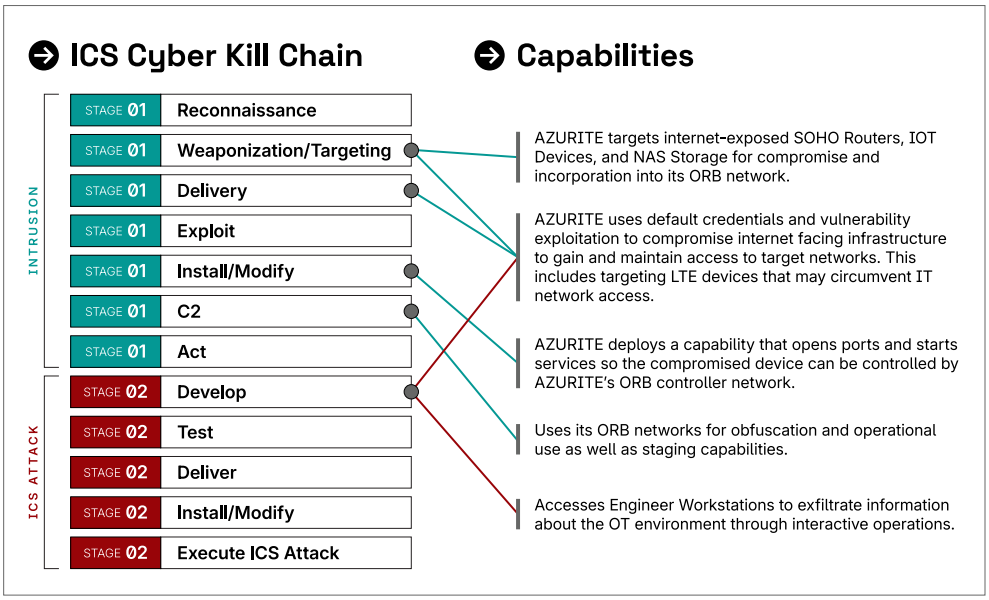
AZURITE targets manufacturing, automotive, electric, oil and gas, pharmaceutical, defense industrial base, and government organizations. From a regional perspective, AZURITE targets the United States, Australia, Europe, Japan, South Korea, and Taiwan. AZURITE activity shares technical overlaps with Flax Typhoon. Assets targeted by AZURITE for initial access include remote access, edge devices, Small Office/Home Office (SOHO) routers, and web application firewalls (WAFs). AZURITE's likely intent is to gain and maintain access to victim networks as a source of intelligence and persistent access to support socio-political or geopolitical taskings. Dragos assesses with moderate confidence that AZURITE is not deterred from its operations by public exposure, law enforcement infrastructure takedowns, or government sanctions based on AZURITE continuing its operations even after indictments and sanctions were leveled against the adversary operators.

AZURITE uses a combination of purpose-built VPS Infrastructure and compromised SOHO devices incorporated into adversary-controlled botnets for adversary operators to conduct automated and interactive reconnaissance, capability staging, exploitation, command and control, actions on the objective, and exfiltration.

AZURITE focuses on exploiting vulnerabilities in public-facing infrastructure and administrative portals, which are often exposed to the internet and serve as entry points for attackers, eliminating the need for phishing or user interaction. These include SSL-VPNs, firewalls, ADC/WAF appliances, NAS devices, and web applications with management interfaces. High-profile examples include Citrix NetScaler (CVE-2023-3519), Fortinet FortiOS SSL-VPN flaws (CVE-2024-21762, CVE-2023-27997), F5 BIG-IP TMUI/iControl (CVE-2023-46747, CVE-2022-1388), Cisco ASA/FTD web services (CVE-2020-3452), and Zyxel firewalls/NAS (CVE-2023-28771, CVE-2024-29973). Many of these vulnerabilities allow pre-authentication remote code execution (RCE) or authentication bypass via a single HTTP(S) request, enabling mass scanning and rapid exploitation. Common attack classes include command injection, deserialization of RCE, template injection, buffer overflows in VPN daemons, and path traversal flaws.

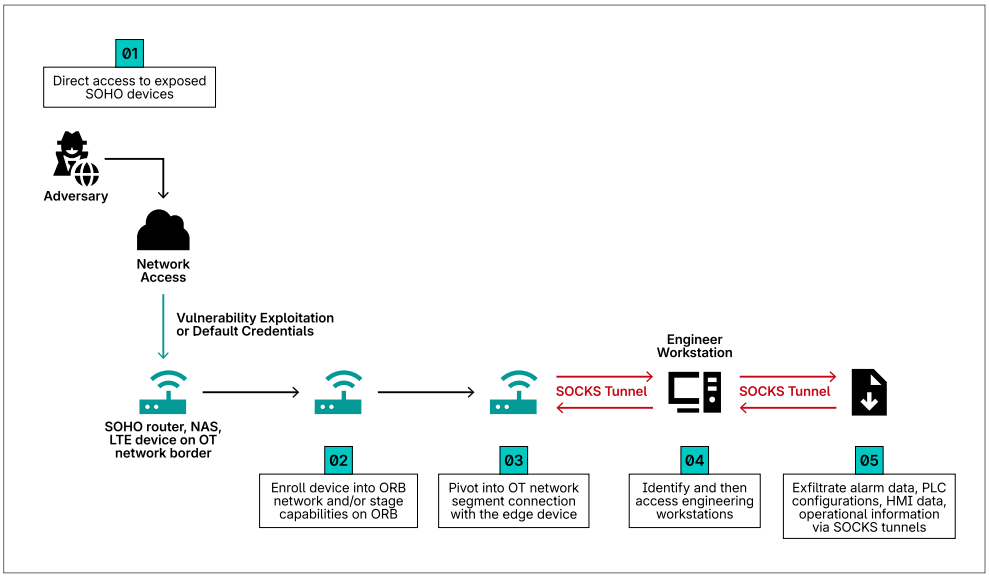
ICS CYBER KILL CHAIN

AZURITE: Stage 1 & Stage 2 Attacks



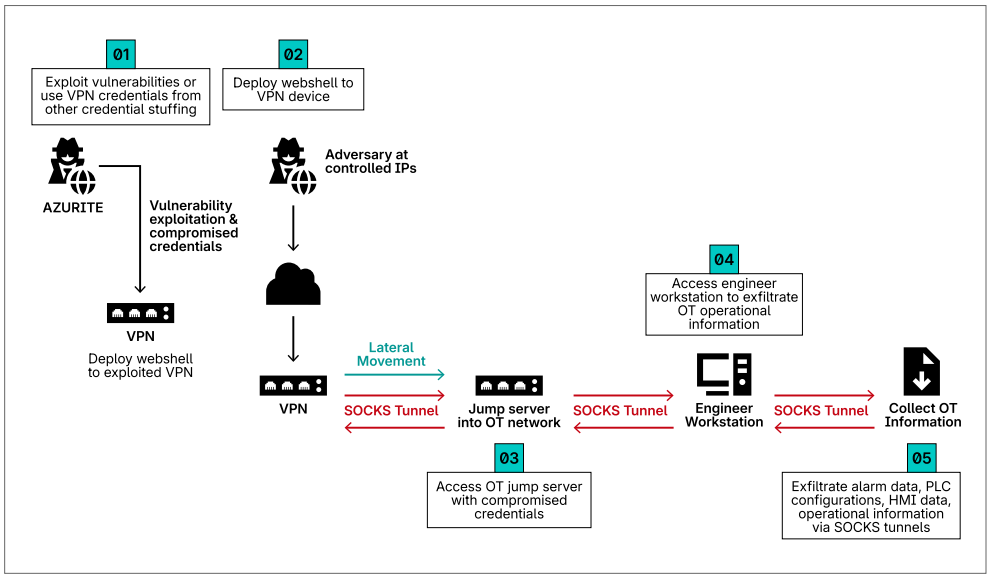
ATTACK PATH

AZURITE Attack Path 1: SOHO Device Compromise to Achieve OT Access



ATTACK PATH

AZURITE Attack Paths: VPN Access to OT Environment and Engineer Workstation



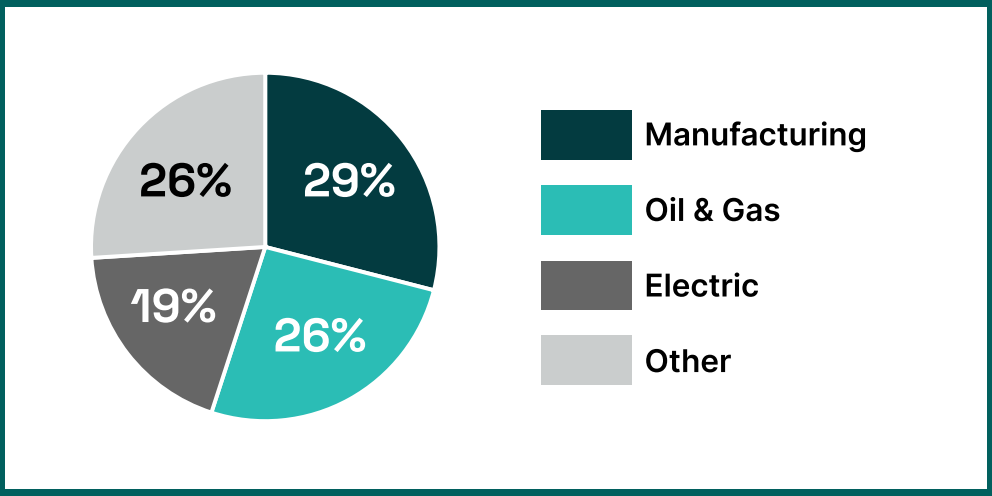
Insights From Dragos Intelligence Fabric

53 percent of Dragos Services assessments conducted included findings associated with Internet connectivity or externally facing issues. Severity rankings distributed: Critical – 20 percent, High – 31 percent, Medium – 34 percent, Low – 15 percent.

The industry breakdown of Internet or External facing issues: manufacturing is the leading contributing vertical at 29 percent, oil and gas 26 percent, electric at 19 percent, Other – 26 percent.

DRAGOS INTELLIGENCE DATA

Internet Connectivity or External Facing Issues



Defensive Recommendations and Mitigations

Critical Control 01: ICS Incident Response Plan

- AZURITE exploits internet-facing devices to access engineering workstations and exfiltrate OT operational data. ICS incident response plans should address scenarios where adversaries establish persistence through memory-resident web shells and conduct data staging from OT-adjacent assets.
- Response procedures should include validation of engineering workstation integrity, investigation of anomalous outbound data transfers, and credential rotation following suspected remote access compromise.

Critical Control 02: Defensible Architecture

- Implement segmentation between IT and OT networks. AZURITE has demonstrated the capability to operate from compromised edge devices, pivot deeper into victim networks, and exfiltrate data from compromised assets.
- If available, regularly use manufacturer-provided system integrity checking tools to identify any non-standard or unplanned changes to the operating system.

Critical Control 03: ICS Network Visibility and Monitoring

- AZURITE uses Remote Desktop Protocol (RDP) to access Engineering Workstations using compromised credentials.
- AZURITE uses NPS, Cobalt Strike, Sliver, and other offensive security capabilities to conduct command and control with non-application layer protocols, especially SOCKS/SOCKS5 protocol. Conduct regular threat hunts and monitor for anomalous SOCKS/SOCKS5 protocol usage within both IT and OT environments, especially if network assets do not use this protocol during normal operations or function.

Critical Control 04: Secure Remote Access

- AZURITE targets remote access devices like Citrix, Cisco, Ivanti, Palo Alto Networks Global Protect, and Fortinet for exploitation to gain and maintain access to victim OT networks.
- MFA - Ensure credential access for internet-facing devices is protected by MFA methods. AZURITE utilizes compromised, reused, or adversary-created credentials to access and persist in the network using valid accounts.
- Log Checks - Regularly check logs on internet-facing devices for new user accounts, especially ones that have elevated privileges. Also, examine the source IP of user accounts with elevated privileges that have successfully authenticated to identify potential adversary credential reuse or compromise.
- Restart internet-facing network devices – Some web shells deployed by AZURITE are memory resident but do not persist through device reboots.

Critical Control 05: Risk-Based Vulnerability Management

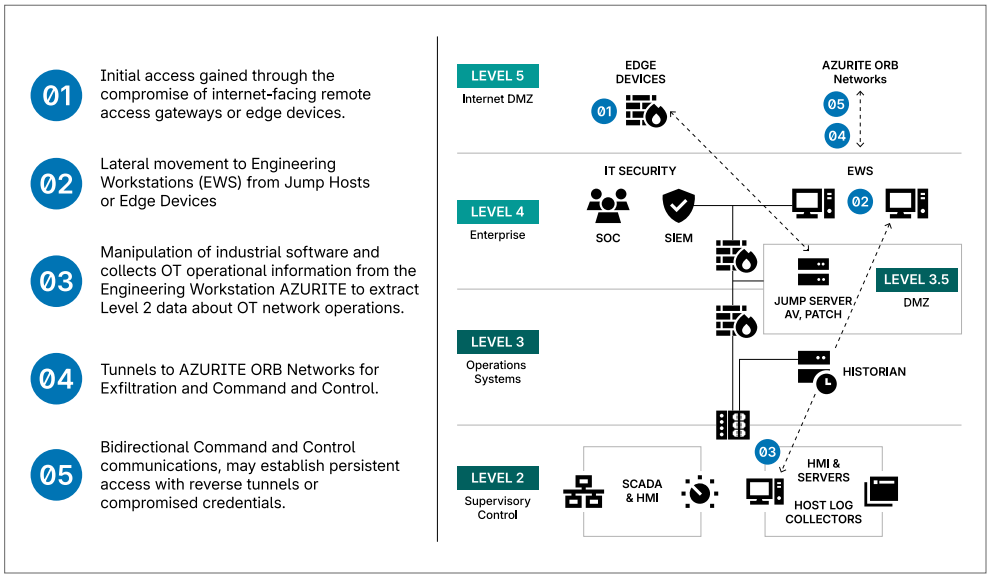
- Internet Facing Devices - ensure internet-facing devices, especially those that serve as VPN gateways or firewalls, are adequately patched for the latest security vulnerabilities as soon as possible.
- Monitor threat intelligence - for adversary campaigns targeting the organization's internet-facing network devices, especially VPNs, firewalls, and web applications. AZURITE quickly implements publicly available proof of concept (POC) code into its operations, taking advantage of the lag time between POC availability and when most organizations have installed patches for the related vulnerability.

Tips for Hunting:

As part of threat hunting exercises, audit connections of valid sessions into the network via internet-facing network devices such as VPN gateways and compare with baselines of normal usage. Investigate outliers in the number of sessions, IP addresses, user locations, bytes transferred per session, access times, and any other properties of remote access sessions that can be analyzed.

INFOGRAPHIC

Hunting for AZURITE



SINCE 2017

Py

New Threat Group:

PYROXENE

ICS IMPACT: Compromise of IT-to-OT pathways enabling lateral movement into industrial environments. Establishes footholds that support future operational disruption or targeted ICS manipulation.

Infrastructure

- Spoofed domains of legitimate entities
- Azure and Cloudflare for C2
- Compromised websites and email accounts
- LIS for malware hosting
- Bulletproof hosting providers
- Controls privately owned VPSs and VPNs

Adversary

- Overlaps with APT35 cluster, associated with entities and operators sanctioned by US Government
- Disruptive operations align with geopolitical tensions
- Focus on strategic supply chain compromises
- Employs misattribution tactics

Victim

- Confirmed critical infrastructure victims in United States, Europe, and Middle East
- Focus on transportation and logistics, defense, government, technology, aerospace, and aviation

Capabilities

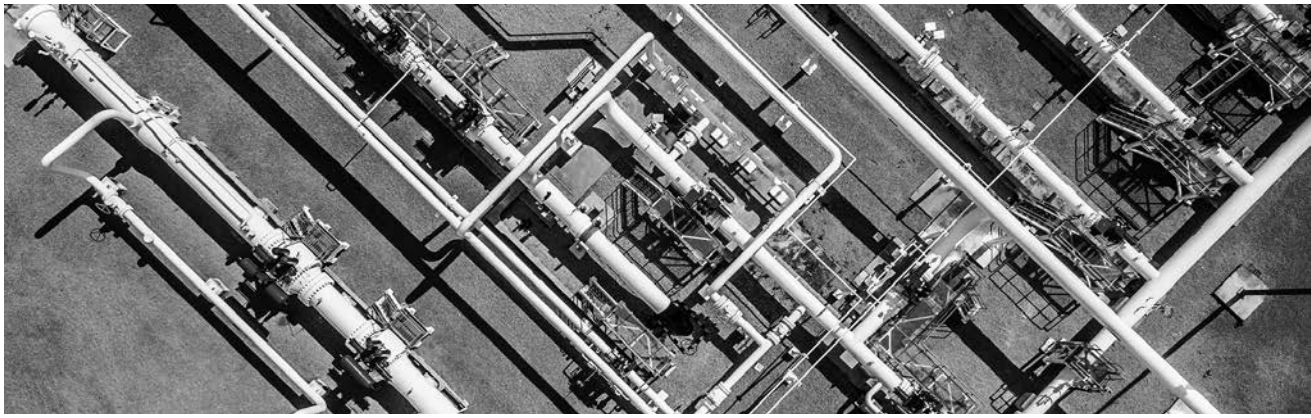
- Custom-developed malware and tooling
- Obfuscates C2 using email, LIS, and Cloud hosting
- Engages in long-term social engineering campaigns
- Manages multiple campaigns concurrently
- Strategic Website Compromises (SWC)
- Creates destructive Wiper Malware

About PYROXENE

Dragos designated PYROXENE as an active threat group in 2025 after observing a sustained focus on supply chain-leveraged attacks targeting defense, critical infrastructure, and industrial sectors, with operations expanding from the Middle East into North America and Western Europe since 2023. Dragos observed PYROXENE activity aligning with Stage 2 Develop of the ICS Cyber Kill Chain, including reconnaissance and assessment of pathways into OT environments. Between 2024 and 2025, Dragos observed PYROXENE conducting multiple campaigns targeting aviation, aerospace, defense, and maritime sectors across the United States, Western Europe, Israel, and the United Arab Emirates. In early 2025, Dragos identified an intrusion collaboration between PYROXENE and PARISITE. Dragos assessed with high confidence that PARISITE functions as an initial access provider, handing off compromised access within critical infrastructure networks to PYROXENE in early 2024. This access enabled PYROXENE to conduct internal network reconnaissance and establish pathways toward an OT environment. Dragos assesses with low confidence PYROXENE intentionally pursued access to and surveyed an OT network for prepositioning and support of future effects operations, satisfying Stage 2 Develop of the ICS Cyber Kill Chain. Collaboration with PARISITE, an initial access provider with a demonstrated history of compromising critical infrastructure and conducting destructive operations, materially increases the likelihood that existing IT or OT-adjacent access could be rapidly operationalized to cause loss of view, loss of control, or loss of availability in ICS environments. PYROXENE exhibits substantial technical overlap with activity tracked by the broader threat activity commonly referred to as UNC1549. This activity is assessed by the U.S. Government to conduct espionage-driven operations aligned with the Islamic Revolutionary Guard Corps Cyber Electronic Command (IRGC-CEC) and has been subject to U.S. sanctions for targeting U.S. critical infrastructure since at least 2017.

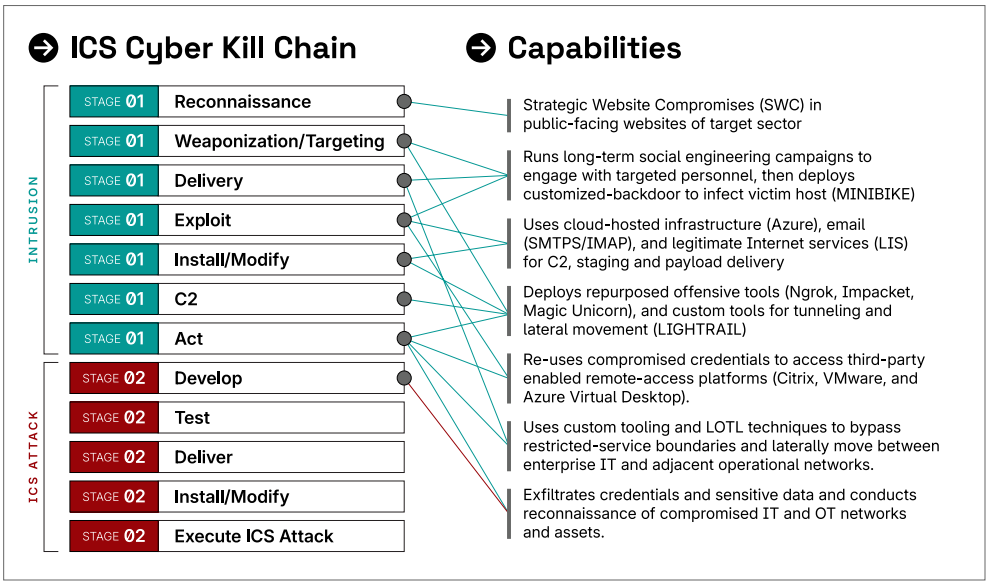
Dragos observed PYROXENE activity that leveraged recruitment-themed social engineering against targeted individuals. PYROXENE used extended interactions via fake social media profiles prior to delivering tailored malware to establish stealth backdoors which leveraged a unique, victim-specific, Microsoft Azure-based command and control infrastructure.

PYROXENE conducts extensive reconnaissance of trusted suppliers, contractors, and business relationships to enumerate externally exposed systems, shared infrastructure, and human access pathways, leveraged as indirect entry points into higher-value targets. Rather than consistently targeting primary victims directly, the group focuses on weaknesses across the broader ecosystem supporting critical operations, deliberately engaging lower-barrier entities as access-enabling footholds.



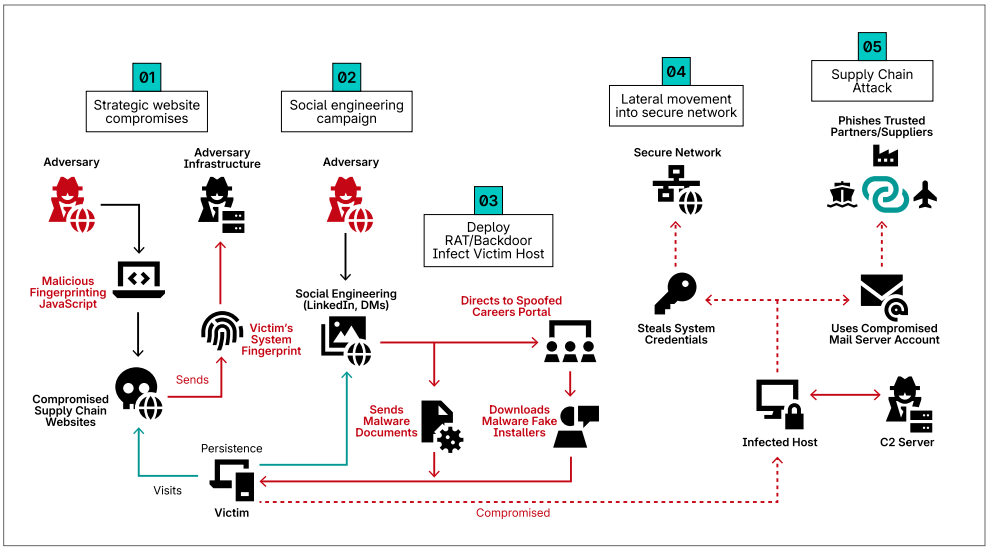
ICS CYBER KILL CHAIN

PYROXENE: Stage 1 & Stage 2 Attacks



ATTACK PATH

PYROXENE Attack Path



Haifa Bay Port Water-Hole Attacks

Since at least 2023, PYROXENE has compromised multiple public-facing websites of companies supporting industrial-sector operations, including Utilities, Telecommunications, Technology, Manufacturing, and Logistics, and has staged malicious fingerprinting JavaScript for visitor tracking. In October 2024, PYROXENE conducted watering-hole attacks against a local water utility company that manages the local water supply for the Haifa Bay Port on the coast of Israel. Haifa Bay Port hosts several organizations of high strategic importance to Israel's maritime, industrial, and defense sectors, including Rafael Advanced Defense Systems, Haifa Chemicals, Elbit Systems, the Haifa Naval Base, Bazan Group, and ZIM Shipping. These entities represent high-value targets for Iranian military and intelligence interests. Dragos has also observed targeting of these organizations by TAT25-93, which has technical overlaps with Charming Kitten, and TAT25-12, as well as additional technical overlaps with Emennet Pasargad. Strategically positioned watering-hole activity targeting entities based in the Haifa Bay area are likely to support the identification and profiling of personnel associated with organizations operating in the region for potential subsequent targeting.

Credential-Harvesting Campaigns

Since 2024, PYROXENE has conducted credential-harvesting campaigns targeting industrial-sector organizations, using spoofed enterprise IT and remote-access login portals to capture credentials and authentication tokens. PYROXENE has staged a credential-harvesting infrastructure targeting European and defense and aerospace organizations. Stolen credentials enable initial access and lateral movement, increasing the likelihood that PYROXENE will progress from IT compromise to OT networks via exposed pathways.

Early Signs of Future OT Capability Positioning

In June 2025, Dragos identified PYROXENE deploying wiper malware against multiple undisclosed organizations in Israel, occurring in immediate temporal proximity to the 12-day conflict between Iran and Israel. Dragos assesses with high confidence that this activity represented a geopolitically motivated effort to cause a severe impact on Israeli critical infrastructure in direct response to the conflict, leveraging existing adversarial capabilities to deliver destructive effects. Wiper malware targeting IT systems can have a severe downstream impact on ICS operations. Destructive wiping of IT systems can render systems unbootable and disrupt operational dependencies, resulting in loss of availability. Even without direct PLC targeting, the loss of supporting IT services can halt operations, delay recovery, and increase safety risk across industrial environments. Dragos assesses with moderate confidence PYROXENE is actively positioning for future ICS-impacting operations by exploiting supply chains, trusted relationships, and IT–OT dependencies, creating a credible risk of disruption or destruction even when OT networks are not directly targeted.

Defensive Recommendations and Mitigations

Control 01: ICS Incident Response Plan

- PYROXENE conducts supply chain compromises to preposition attacks toward higher-value targets. ICS incident response plans should account for social engineering campaigns characterized by prolonged engagement driven by impersonation tactics, and for access pathways between IT and OT through trusted third-party account compromise.

Control 02: Defensible Architecture

- Strict IT/OT segmentation, tightly governed contractor, vendor, and supplier access, and continuous monitoring of trusted access paths are critical to preventing PYROXENE from leveraging prepositioned footholds from within IT environments to enable downstream intrusions toward OT.

Control 03: ICS Network Visibility and Monitoring

- PYROXENE leverages native system utilities and living-off-the-land (LOTL) techniques to enumerate OT assets, services, and configurations following access through IT. Resulting operational data may be staged for exfiltration, underscoring the need to monitor OT and IT environments for anomalous use of legitimate administrative tools, unexpected data staging, and abnormal outbound transfers that deviate from established operational baselines.

Control 04: Secure Remote Access

- PYROXENE operations have been facilitated by prior initial access gained by PARISITE, which routinely exploits exposed and unpatched remote access infrastructure, particularly VPN appliances. Enforcing strong remote access controls, including timely patching of internet-facing services, MFA across all remote access pathways, and strict governance of VPN and third-party access, is critical to disrupting PARISITE-enabled intrusions that support PYROXENE's follow-on operations.

Control 05: Risk-Based Vulnerability Management

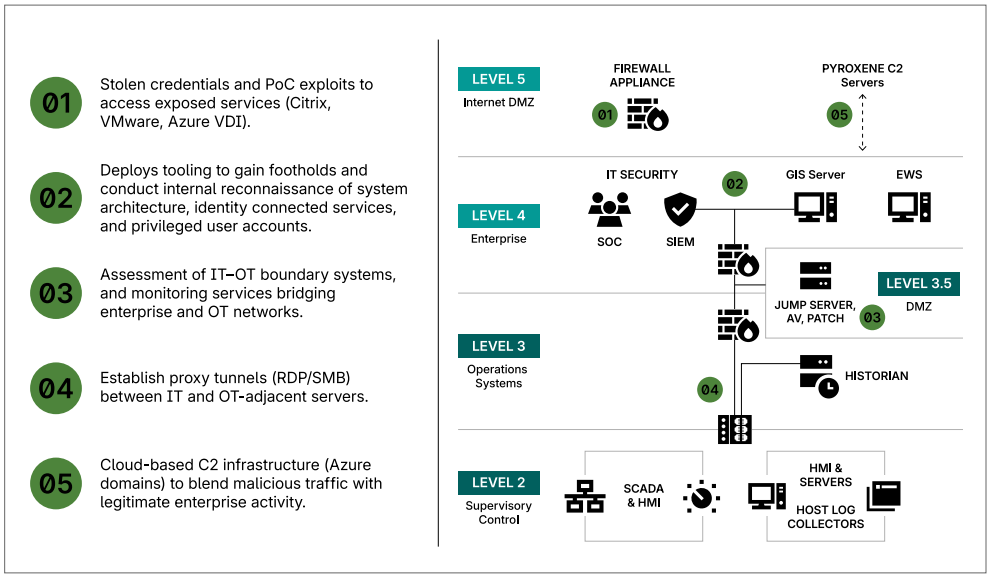
- PYROXENE conducts reconnaissance and data acquisition within OT environments to enumerate assets and network architecture, enabling identification of potentially vulnerable systems and access pathways. A risk-based vulnerability management program should prioritize remediation of OT assets and pathways identified as high risk to reduce the likelihood that observed weaknesses are assessed, prepositioned against, or leveraged in future operations.

Tips for Hunting:

As part of threat hunting exercises, audit third-party and contractor access patterns, particularly those with privileged access to IT-OT boundary systems such as jump servers and historian databases. Monitor for stolen credentials and proof-of-concept exploits used to access exposed services including Citrix, VMware, and Azure VDI environments. Investigate the deployment of reconnaissance tooling in Level 4 and Level 5 DMZ environments, focusing on internal enumeration of system architecture, identity-connected services (SOC, SIEM), and privileged user accounts. Establish baselines for normal IT-OT boundary traffic and investigate anomalous proxy tunnels using RDP or SMB protocols between IT and OT-adjacent servers. Review cloud-based command and control infrastructure, particularly Azure domains, for signs of malicious traffic being blended with legitimate enterprise activity to evade detection.

INFOGRAPHIC

Hunting for PYROXENE



New Threat Group:

SYLVANITE

SINCE 2023

Sy

ICS IMPACT: Large-scale initial access operations targeting industrial organizations. Enables credential theft, VPN exploitation, and sustained access that can be leveraged for follow-on ICS-focused campaigns.

Infrastructure

- Virtual Private Servers (VPS)
- Small Office Home Office (SOHO) routers
- Favors Vultr, Linode, Kaopu Cloud, Forewin Telecom Group, and BGP Network Ltd providers

Adversary

- Multiple entities working under the same overarching direction
- Assessed intent is initial access and credential theft that is passed to other threat groups, including VOLTZITE
- Overlaps with UNC5221, UNC5174, UNC5291, UNC3236, HOUKEN, Red Dev 61, CL-STA-0048, and UTA0178

Victim

- Electric Power Generation, Transmission & Distribution (2211), Water, Sewage and Other Systems (2213), Oil and Gas (2111), Manufacturing (31-33), Public Administration (92)
- North America, United Kingdom, Europe, France, Japan, South Korea, Guam, Philippines, Saudi Arabia

Capabilities

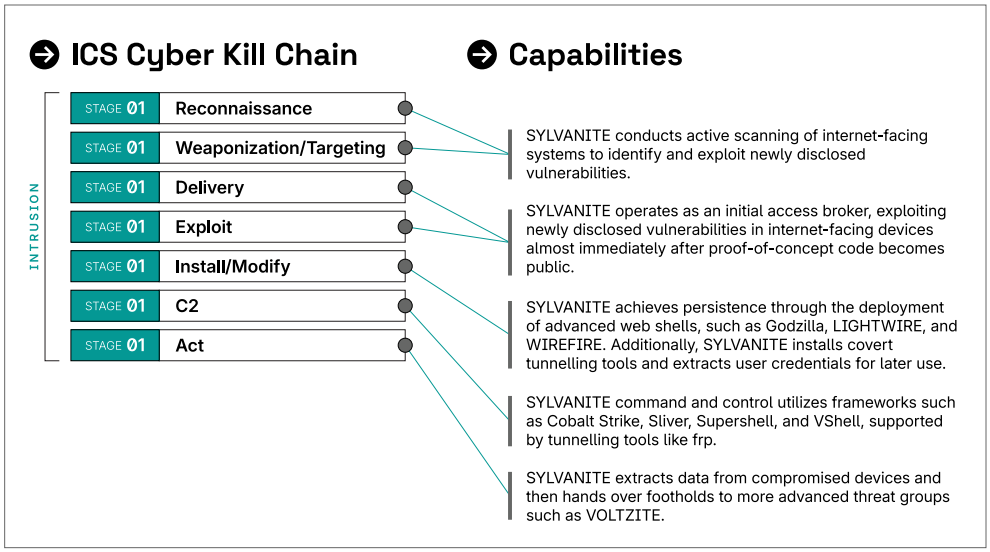
- N-day exploitation of internet0facing products from F5, Ivanti, SAP, ConnectWise
- Cobalt Strike C2, Silver C2, Supershell C2, Fast Reverse Proxy (frp), Fscan, Vshell backdoor
- Godzilla, LIGHTWIRE, THINSPOOL, WIREFIRE
- WARPWIRE, ZIPLINE, SNOWLIGHT, GOREVERSE, GOHEAVY

About SYLVANITE

SYLVANITE is an ICS Kill Chain Stage 1, initial access threat group that operates at scale, overlapping with multiple widespread campaigns designed to compromise internet-facing systems. Dragos has previously observed SYLVANITE handing off initial access directly to VOLTZITE during intrusions. Because VOLTZITE has a history of stealing OT data and manipulating OT systems, Dragos classifies it as a Stage 2 threat group. As a result, SYLVANITE's initial access operations align with Stage 1 of the ICS Cyber Kill Chain. SYLVANITE activity has been observed across multiple regions, including North America, Europe, the United Kingdom, France, Japan, South Korea, Guam, the Philippines, and Saudi Arabia. Targeted sectors include Electric Power Generation, Transmission, and Distribution; Water and Wastewater; Oil and Gas; Manufacturing; and Public Administration. According to the ICS Cyber Kill Chain, SYLVANITE has not yet shown evidence of moving into OT networks, their focus remains on OT network information and operating procedures. This enables SYLVANITE to significantly enhance the ability of ICS-focused adversaries, such as VOLTZITE, to whom SYLVANITE has previously provided ICS victim footholds, to develop highly targeted and sophisticated ICS-capable malware. SYLVANITE's observed use of Stage 1 capabilities lead Dragos to assess SYLVANITE as a Stage 1 threat group. SYLVANITE shares technical overlaps with UNC5221, UNC5174, UNC5291, UNC3236, HOUKEN, Red Dev 61, CL-STA-0048 and UTA0178. In 2025, Dragos directly observed SYLVANITE activity within the United States electric and water utility sector during an incident response.

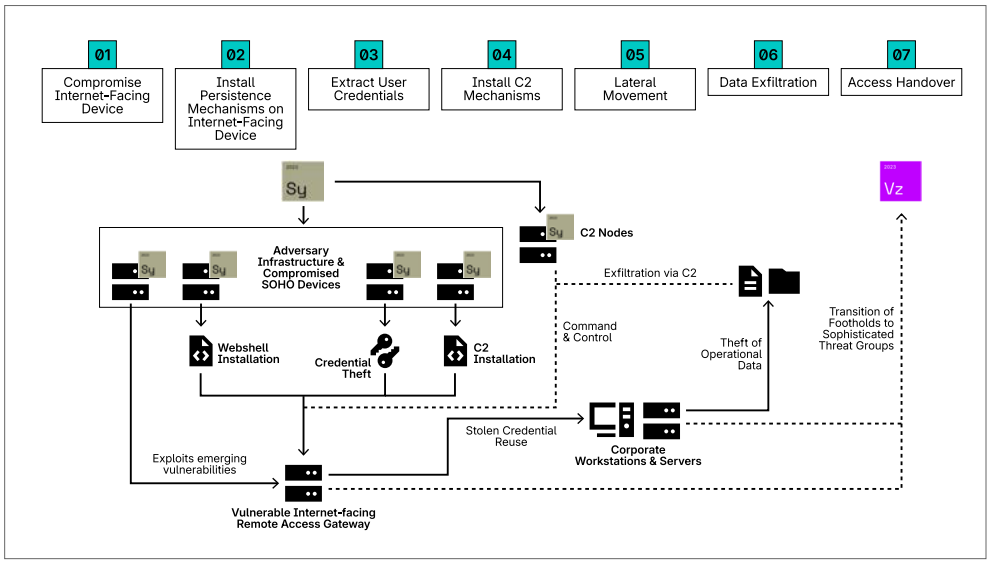
ICS CYBER KILL CHAIN

SYLVANITE: Stage 1 Attacks



ATTACK PATH

SYLVANITE Attack Path



Ivanti Endpoint Manager Mobile (EPMM) Compromise

SYLVANITE closely monitors exploit research and rapidly weaponizes it. If an active, public POC exists and vulnerable assets are exposed on the internet, adversaries like SYLVANITE will take advantage of them. In May 2025, Dragos responded to an incident in which an adversary compromised an Ivanti Endpoint Manager Mobile (EPMM) instance of a United States utility by exploiting CVE-2025-4427 and CVE-2025-4428. Dragos designated the set of activities perpetrated by this adversary as TAT25-43, and additional analysis later confirmed that TAT25-43 was attributed to SYLVANITE. The Ivanti EPMM instance was located in the utility's DMZ, and incident response procedures were initiated to determine whether the adversary had pivoted into the organization's adjacent OT networks from the compromised Ivanti EPMM server. Dragos observed the adversary efficiently using Stage 1 capabilities within the DMZ; however, due to the lack of telemetry in adjacent networks, Dragos could not use network monitoring and visibility that would have supported the detection of any Stage 2 activity. TAT25-43 rapidly enumerates and compromises Ivanti EPMM servers using an exploitation proof of concept shared on the Internet before Ivanti issued a patch to remediate the vulnerability. Exploitation of Ivanti EPMM devices allows adversaries to establish a foothold in victim networks, steal personally identifiable information (PII) and authentication tokens for connected LDAP users, and remotely manage mobile devices. During the Ivanti EPMM campaign conducted by TAT25-43, SYLVANITE accessed the backend MySQL database using hardcoded credentials stored in /mi/files/system/.mifpp. They then executed mysqldump to extract tables such as mi_user, mifs_ldap_users, and mifs_ldap_server_config, which contained LDAP user details and Office 365 tokens. These credentials were replayed across other internal systems, enabling lateral movement without triggering alerts associated with account creation or password spraying.

Once inside, SYLVANITE utilizes tunnelling and proxy tools to maintain connectivity and pivot deeper into the network. Tools like Fast Reverse Proxy (FRP) and GoHeavy establish covert channels, while GoReverse provides SSH-based reverse shells for remote access. These methods enable SYLVANITE to bypass traditional egress points and move laterally without relying solely on standard remote administration protocols. SYLVANITE also deploys reconnaissance utilities such as fscan to map internal network services and identify exploitable systems. This scanning phase enables the identification of targets for credential reuse and

subsequent exploitation. In Windows environments, SYLVANITE leverages built-in remote execution mechanisms, including PsExec, WMIExec, and SMBExec, as well as WinRM (TCP ports 5985/5986), to execute commands remotely and propagate laterally. These techniques align with MITRE ATT&CK tactics for lateral movement and are often combined with LOTL approaches to minimize detection.

Once inside a victim network, SYLVANITE establishes multiple command-and-control and persistence mechanisms within exploited devices and passes control to other threat groups, including VOLTZITE. This approach positions SYLVANITE as a significant risk to OT environments, where exploitation can have severe safety and operational impacts. Dragos assesses with moderate confidence that SYLVANITE consists of multiple entities contracted by various upstream threat groups under a common alignment, including those with ICS-disruptive capabilities, to exploit emerging, novel initial access techniques and steal credentials, enabling long-term persistence in victim networks. SYLVANITE utilizes adversary-controlled or rented infrastructure, such as VPS and compromised SOHO routers. SYLVANITE favors ISPs and cloud services such as Vultr, Linode, Kaopu Cloud, Forewin Telecom Group, and BGP Network Ltd.

Dragos assesses with moderate confidence that SYLVANITE is primarily an initial access group focused on espionage and data harvesting to inform and provide access to more ICS-capable adversaries, as evidenced by SYLVANITE previously handing over access points to VOLTZITE.

A Series of Exploitation Campaigns

In December 2023, SYLVANITE exploited Ivanti Connect Secure VPN vulnerabilities (CVE-2023-46805, CVE-2024-21887), deploying web shells such as GLASSTOKEN, disabling logging, and modifying appliance components to evade integrity checks. They also altered JavaScript files to capture credentials and embedded backdoors for persistent command-and-control communication. Later campaigns included F5 BIG-IP (CVE-2023-46747) and ConnectWise ScreenConnect (CVE-2024-1709), where custom tooling and the Supershell C2 framework were used to establish access.

In April 2025, SYLVANITE exploited a SAP NetWeaver zero-day vulnerability (CVE-2025-31324), deploying the KrustyLoader malware loader to deliver Sliver C2 and the SNOWLIGHT malware downloader, followed by the VSHELL Remote Access Trojan (RAT) for remote access. Most recently, Ivanti EPMM vulnerabilities (CVE-2025-4427, CVE-2025-4428) were exploited using Java Reflection payloads embedded in HTTP GET requests, resulting in the creation of interactive shells linked to SYLVANITE-controlled infrastructure. SYLVANITE achieves persistence through the deployment of advanced web shells, such as Godzilla, LIGHTWIRE, and WIREFIRE, which are often memory-resident and deeply integrated into application frameworks like Apache Tomcat, thereby more likely to evade detection. Credential harvesting is a core tactic employed by SYLVANITE. SYLVANITE extracts data from backend databases on compromised devices, including Lightweight Directory Access Protocol (LDAP) information and Office 365 tokens, enabling lateral movement.

Positioning for Future Disruptive Attacks

SYLVANITE's established initial access points could be leveraged for future disruptive operations that may directly or indirectly affect OT networks. In environments where IT and OT networks lack proper segmentation, compromising the IT network could allow adversaries to pivot into OT systems with minimal difficulty. These intrusions could disrupt critical processes in OT environments if access is handed over to Stage 2 threat groups, as SYLVANITE has previously demonstrated. SYLVANITE's initial access activities involve port scanning across IT and OT networks. Port scanning can unintentionally impact OT networks by reducing asset availability. Many OT devices are not designed to handle sudden surges in network traffic and may become unresponsive or enter a degraded state. This can lead to an unintended denial-of-service condition, potentially triggering cascading failures that disrupt operational continuity. SYLVANITE exfiltrates sensitive operating data and user credentials. Data exfiltrated from victim networks, especially OT network information or operating procedures, significantly enhances the ability of an upstream ICS-focused adversary, such as VOLTZITE, which SYLVANITE has demonstrated working collaboratively with in previous intrusions, to develop highly targeted and sophisticated ICS-capable malware.

In short, SYLVANITE lowers the barrier for ICS-focused adversaries to achieve their objectives, making timely patching, segmentation, and monitoring of internet-facing assets essential for ICS asset owners. Asset owners should harden and monitor internet-facing devices, because SYLVANITE's entire tradecraft revolves around exploiting these systems before patches are widely applied.

Insights From Dragos Intelligence Fabric

- 73 percent of Dragos IR cases (all time) included active exploitation or valid credential reuse of VPN/jumphosts.
- 56 percent of Dragos Network Penetration Tests conducted included findings associated with abusing LOTL tools, such as WinRM. WinRM is routinely leveraged by Dragos Red Team in ICS DMZs to enable Domain Controller access and lateral movement.
- 10 percent of Dragos Network Penetration Tests conducted included findings associated with the abuse of Insecure Protocols, such as LDAP, further escalation of privileges and lateral movement.
- 58 percent of Dragos Architecture Reviews conducted included findings associated with the use of Insecure Protocols, such as LDAP.

Defensive Recommendations and Mitigations

Control 01: ICS Incident Response Plan

- SYLVANITE exploits network edge devices to move deeper into victim networks and then hand over access to ICS-capable threat groups. ICS incident response plans should address scenarios in which an adversary exploits an emerging vulnerability in internet-facing network devices and then establishes multiple long-term persistence mechanisms.

Control 02: Defensible Architecture

- Strict IT/OT segmentation and monitoring of network edge devices, and continuous monitoring of trusted access paths are critical to preventing SYLVANITE from leveraging footholds from within IT environments to enable downstream intrusions toward OT. The use of jump hosts between IT and OT networks, as well as strong MFA implementation, is vital for mitigating SYLVANITE intrusions.

Control 03: ICS Network Visibility and Monitoring

- SYLVANITE leverages native system utilities and LOTL techniques to enumerate assets, services, and configurations across IT networks. Resulting data may be staged for exfiltration, underscoring the need to monitor OT and IT environments for anomalous use of legitimate administrative tools, unexpected data staging, and abnormal outbound transfers that deviate from established operational baselines.

Control 04: Secure Remote Access

- SYLVANITE operations routinely exploit exposed and unpatched remote access infrastructure, particularly VPN appliances. Enforcing strong remote access controls, including timely patching of internet-facing services, MFA across all remote access pathways, and strict governance of VPN and third-party access, is critical to disrupting SYLVANITE-enabled intrusions that may support VOLTZITE's follow-on operations.

Control 05: Risk-Based Vulnerability Management

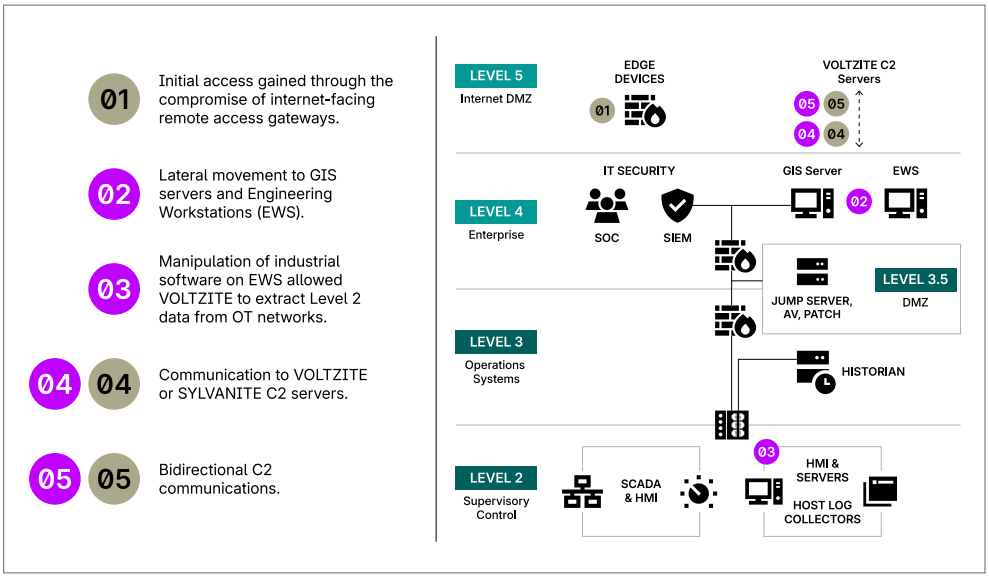
- SYLVANITE conducts exploitation efforts against internet-facing remote gateways. A risk-based vulnerability management program should prioritize remediation of assets and pathways identified as high risk to reduce the likelihood that observed weaknesses are assessed, prepositioned against, or leveraged in future operations.

Tips for Hunting:

As part of threat hunting exercises, audit connections of valid sessions into the network via internet-facing network devices such as VPN gateways and edge devices, and compare with baselines of normal usage. Investigate outliers in the number of sessions, IP addresses, user locations, bytes transferred per session, access times, and any other properties of remote access sessions that can be analyzed. Monitor for lateral movement from compromised edge devices to GIS servers, Engineering Workstations (EWS), and historian databases within Level 3 and Level 4 environments. Establish baselines for normal industrial software behavior on EWS and investigate anomalous manipulation attempts that could enable VOLTZITE to extract Level 2 data from OT networks, including SCADA systems, HMI interfaces, and host log collectors. Review bidirectional command and control communications to VOLTZITE or SYLVANITE C2 servers, particularly focusing on traffic patterns between Level 3.5 DMZ jump servers and external infrastructure that may indicate handoff activities between the two threat groups.

INFOGRAPHIC

Hunting for SYLVANITE & VOLTZITE



02.

Advancing Toward OT: Active Threat Group Operations

While new groups emerged in 2025, established adversaries demonstrated that operational experience matters—and that years of access-building in one region can rapidly translate to disruptive capability in another.

KAMACITE and ELECTRUM, responsible for Ukraine's 2015 and 2016 power outages, are the most experienced infrastructure-disrupting adversaries in the world.

After years focused exclusively on Ukrainian targets, they expanded operations back into Europe and the United States in 2025. VOLTZITE achieved Stage 2 capability by moving beyond data exfiltration to direct manipulation of engineering workstations. BAUXITE escalated from hacktivist defacements to deploying custom wiper malware during regional conflicts.

Threat Group Update:

KAMACITE & ELECTRUM

SINCE 2014

Ka

SINCE 2016

El

Insights From Dragos Intelligence Fabric

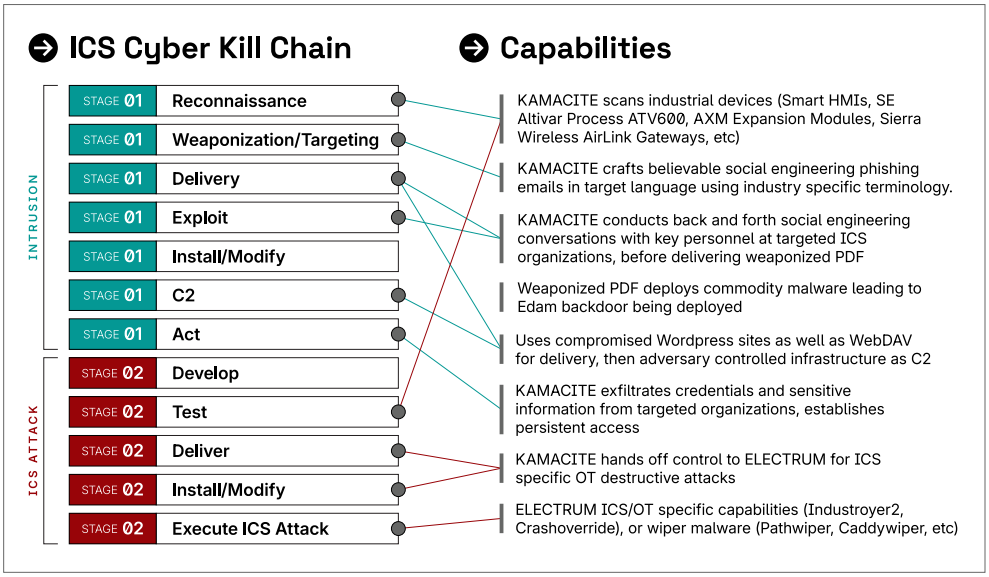
- In late December 2025, a coordinated cyberattack against Polish energy infrastructure occurred, which included combined heat and power (CHP) facilities and systems supporting renewable energy generation management. Public statements from Polish authorities indicated the activity was assessed as originating from actors linked to Russian state services and that defensive measures prevented any disruption to national power delivery or grid stability.
- While no customer-facing outages were reported, the targeting demonstrates continued adversary focus on operational environments that directly support power generation, grid coordination, and regional energy stability.
- Dragos has been tracking this activity through a combination of incident response, internal analysis, and sensitive source reporting, though specific technical details cannot be disclosed at this time due to source handling constraints. Available information indicates that the activity included deliberate attempts to directly impact operational assets rather than remaining confined to enterprise reconnaissance or access operations.
- Dragos assesses with moderate confidence that the activity reflects tradecraft and operational objectives consistent with the ELECTRUM threat group. This assessment remains preliminary and subject to refinement as additional information becomes available. Dragos is also aware that national cybersecurity authorities have been proactively engaging with energy-sector organizations to provide restricted technical information related to this activity.
- CHP facilities and renewable energy aggregation platforms represent operationally meaningful leverage points within modern energy systems. CHP plants provide localized thermal and electrical stability for municipal or industrial customers, while renewable management systems increasingly coordinate dispatch, curtailment, telemetry, and grid balancing functions across geographically distributed assets. Disruption or manipulation of these systems, even if localized, can introduce cascading operational complexity, operator workload stress, and recovery challenges, particularly during seasonal demand peaks.

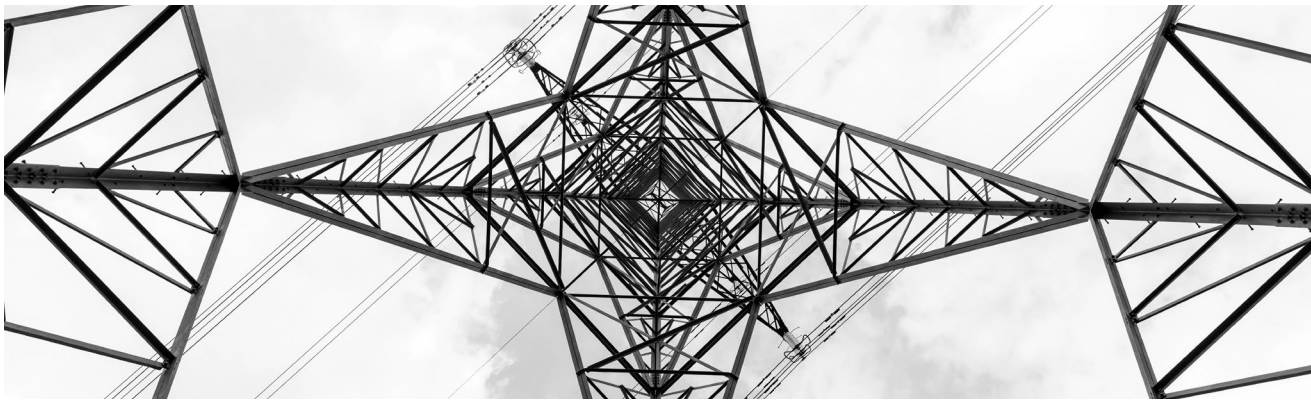
Notable Timing of Activity

The attacks occurred approximately six days after the 10th anniversary of the December 2015 cyber-induced power outage in Ukraine, widely regarded as the first publicly confirmed cyber operation to successfully disrupt electric power operations, endangering civilian infrastructure and life in the middle of Eastern European winter. That activity was subsequently attributed by multiple governments to the same Russian threat ecosystem now associated with ELECTRUM, which has technical overlaps with Sandworm, which the U.S. government has attributed to the Russian General Staff Main Intelligence Directorate's Russian (GRU's) Main Centre for Special Technologies (GTsST). While anniversaries alone should not be over-weighted as causal indicators, Russian cyber operations have historically demonstrated sensitivity to symbolic timing, messaging value, and operational signaling during periods of geopolitical tension. The proximity of this activity to a milestone in the evolution of cyber-enabled infrastructure disruption reinforces the strategic context for assessing it. Over the past year, both KAMACITE and ELECTRUM have executed destructive attacks against ISPs in Ukraine and widespread, persistent scanning of exposed industrial devices in the United States, signaling a significant and potentially alarming shift in targeting from recent years.

ICS CYBER KILL CHAIN

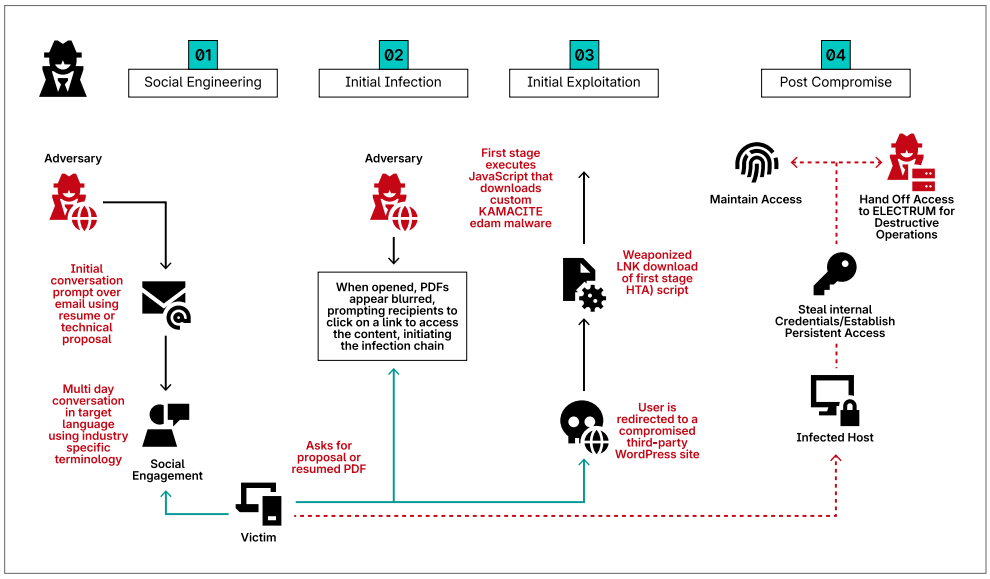
ELECTRUM: Stage 1 & Stage 2 Attacks





ATTACK PATH

KAMACITE Attack Path



Expansion of KAMACITE Targeting Across the ICS Supply Chain

Beginning in late 2024 and extending into early 2025, Dragos observed a significant escalation in KAMACITE activity targeting organizations across the European OT/ICS supply chain, a departure from prior years, when the group largely focused on Ukrainian critical infrastructure and government entities. This shift became clearer following a February 2025 CERT-UA report on threat activity designated UAC-0212, which detailed a multi-stage campaign impacting energy, water, and heating organizations across ten Ukrainian regions and more than 20 firms supporting industrial operations. Dragos had previously observed portions of this campaign in the Dragos Intelligence Fabric, where KAMACITE had specifically targeted attendees of the Gas Infrastructure Europe (GIE) conference hosted in Munich, Germany. CERT-UA also identified attempts to compromise at least 25 Ukrainian companies involved in developing or supplying industrial process control technologies widely deployed across Ukraine. Dragos assesses, with moderate confidence, that UAC-0212 represents the same activity tracked as KAMACITE, supported by extensive 1:1 technical overlap across infrastructure, malware, and targeting patterns. Dragos observed KAMACITE execute in late 2024. CERT-UA's findings confirmed that KAMACITE's spear-phishing activity against attendees of the 2024 GIE conference, which Dragos initially assessed as a standalone campaign, was likely part of a broader and more ambitious effort to exploit trusted relationships across the European industrial ecosystem. Dragos' analysis indicates the campaign continued at least through March 2025, after which KAMACITE likely abandoned the infrastructure dedicated to the campaign.

Consistent Tactics, But Expanded Operational Scale

Starting in late 2024 and extending through early 2025, the scope and ambition of KAMACITE's access-building efforts changed. Rather than focusing only on direct critical-infrastructure operators, the group expanded upstream, attempting to compromise suppliers, integrators, and vendors whose technologies shape Ukraine's industrial environment. This represents a meaningful evolution, not in techniques, but in operational design and campaign intent. Dragos's analysis indicates that the campaign did not introduce radically new tactics. Instead, it showcased KAMACITE's ability to apply its well-established playbook at a much larger scale and across a wider range of victims than previously observed.

Key elements included:

- Highly tailored spear-phishing to compromise engineering, operations, and vendor personnel.
- Long-term, multi-day conversations with key personnel at targeted organizations in native language using industry-specific terms.
- Infrastructure use patterns consistent with historic campaigns.

Why This Campaign Matters

KAMACITE's upstream supply chain focus represents a meaningful risk to industrial defenders. By compromising vendors and integrators rather than only operators, the group increases:

- Its potential reach across entire sectors,
- Its ability to pre-position access deep in trusted relationships, and
- The potential future workload of ELECTRUM, should destructive or ICS-specific operations be initiated.

Dragos assesses with high confidence that KAMACITE's core mission remains unchanged: to provide ELECTRUM with persistent access to high-value industrial targets. The supply chain 2024–2025 campaign demonstrates that the group can conduct long-duration, multi-vector access operations against entire industrial ecosystems, not just single organizations.

U.S. Reconnaissance Campaign (March–July 2025): Expansion into Direct ICS Target Mapping in the U.S.

Shortly after concluding its 2024–2025 supply-chain campaign in Europe, KAMACITE shifted to a new phase of activity: sustained, infrastructure-linked reconnaissance against internet-exposed industrial devices located exclusively within the United States. Dragos analysis of internet telemetry indicated this activity began as early as March 2025 and continued through late July 2025. While Dragos found no evidence of successful exploitation during this period, the scope and precision of the scanning reveal a meaningful evolution in KAMACITE's operational posture. While the European campaign was designed to infiltrate trusted vendors and upstream service providers, this activity directly probed U.S.-based edge-exposed ICS assets, including Schneider Electric Altivar variable-frequency drives, Smart HMIs, Accuenergy AXM modules, and Sierra Wireless Airlink gateways. These technologies underpin routine industrial operations across a variety of industrial sectors, including Water and Wastewater, Manufacturing, Energy, and Building Automation, making them attractive as pivot points, disruption targets, or sources of process intelligence.

From Access-Building to Control-Loop Mapping

The key development is not the act of scanning itself; multiple adversaries routinely search for exposed ICS equipment, but the specific selection of components and the sequencing of the reconnaissance.

Across the four-month period, KAMACITE appeared to:

- Enumerate operator interfaces (Smart HMIs)
- Identify actuators capable of directly influencing physical processes (Altivar variable frequency drives (VFDs))
- Map metering and process-visibility points (Accuenergy AXM modules)
- Target remote-access gateways that bridge ICS assets back to corporate or vendor networks (Sierra Wireless Airlink)

Taken together, the scanning pattern suggests an intent to understand entire control loops rather than isolated devices. By correlating HMIs, VFDs, meters, and gateways, an adversary can build a detailed operational view of exposed industrial environments, including where commands originate, how they propagate, and where physical effects could be induced. This marks a subtle but significant shift from prior KAMACITE activity. Rather than building access through trusted corporate chains (as in the European campaign), KAMACITE appears to have spent several months in mid-2025 constructing targeted intelligence at the edge of U.S. operational environments, where security practices remain uneven, and internet exposure is common.

The campaign introduced several concerning signals:

- A rapid pivot to U.S. ICS exposure immediately after retiring European campaign infrastructure. The timing suggests reconnaissance was not opportunistic. It followed directly on the heels of KAMACITE's access-building efforts in Europe, indicating a potential new phase of targeting rather than a one-off exploratory effort.
- A focus on components with known security debt and broad deployment. Schneider Electric Altivar VFDs were included a CISA advisory (CVE-2025-7746) in September 2025.
- While Dragos cannot confirm the scanning was vulnerability-driven, the prevalence of Altivar devices in U.S. critical manufacturing underscores why they may attract adversary attention.
- Targeting industrial cellular gateways mirrors past disruptive incidents. Sierra Wireless AirLink devices have previously been compromised to enable lateral movement into ICS environments, including by Dragos-tracked threat group VOLTZITE in 2025. Their presence in this scanning sequence is notable: these gateways often sit at unmonitored OT edges and provide direct ingress into isolated field assets.

The scanning mirrored known real-world disruptions caused by other adversaries abusing exposed devices. The tactic aligns with historical campaigns such as the targeting of exposed of Unitronics PLCs (BAUXITE) and poorly secured HMIs (TAT24-22; shares technical overlaps with CyberArmyofRussia_Reborn), both of which led to tangible operational consequences in some cases, including water-system outages and unauthorized parameter changes at U.S. water facilities. While KAMACITE's campaigns across Europe and the U.S. dominated much of the first half of 2025, Dragos continued to observe ELECTRUM conducting destructive cyber operations in Ukraine, reinforcing that KAMACITE's access-building is not an abstract concern but a prerequisite for real-world impact. Every ELECTRUM operation observed in 2025 required a foothold inside targeted networks, and Dragos assesses with moderate confidence that KAMACITE facilitated at least part of the initial access used in these incidents.

What Defenders Should Infer

The scanning activity demonstrates that KAMACITE is now willing to:

- Conduct broad-spectrum reconnaissance across the U.S. industrial footprint,
- Integrate infrastructure knowledge into the development of initial access methods to support ELECTRUM's operations, and
- Explore direct OT-edge entry points, rather than focusing on enterprise or supply-chain compromise.

This expansion increases the likelihood that future destructive or disruptive campaigns could draw on previously identified exposed U.S. operational environments, control-loop layouts, device capabilities, and exposed ingress routes. These insights reinforce the view that internet-exposed ICS devices are not merely "low-hanging fruit" but continue to be strategically meaningful reconnaissance targets.

ELECTRUM Activity in 2025: Destructive Operations Underscore Why KAMACITE's Access Matters

In late May 2025, ELECTRUM conducted a coordinated destructive operation targeting eight Ukrainian ISPs. As in previous incidents, ELECTRUM obfuscated its involvement by operating through the hacktivist persona Solntsepek (tracked by Dragos as TAT25-41), a pro-Russian hacktivist persona typically associated with doxing but repeatedly co-opted as a deniable front for ELECTRUM campaigns. On 26 May 2025, Solntsepek claimed responsibility for disruptions at Interlink, ActiveNet, Svit-Net LLC, Palvi Telecom, NPO Orikhiv, ISP Aries, Corbina, and D-Lan. Dragos independently verified outages affecting several of these ISPs, including a four-hour disruption to Corbina's autonomous system, as shownin historical internet telemetry. This represents the third observed instance of ELECTRUM pairing destructive operations with the Solntsepek persona to mask attribution. The targeting focus, ISPs supporting Ukrainian call centers and communications infrastructure, aligns with ELECTRUM's long-standing pattern of degrading civilian and military coordination capacity during periods of elevated conflict intensity.

June 2025: Identification of New Destructive Malware (PathWiper)

In parallel with the ISP attacks, Cisco Talos identified PathWiper, which Dragos has previously linked to ELECTRUM with moderate confidence. PathWiper appeared in the wild beginning March 2025 and submitted independently by several Ukrainian entities to online malware repositories over the following week, suggesting multiple victim environments.

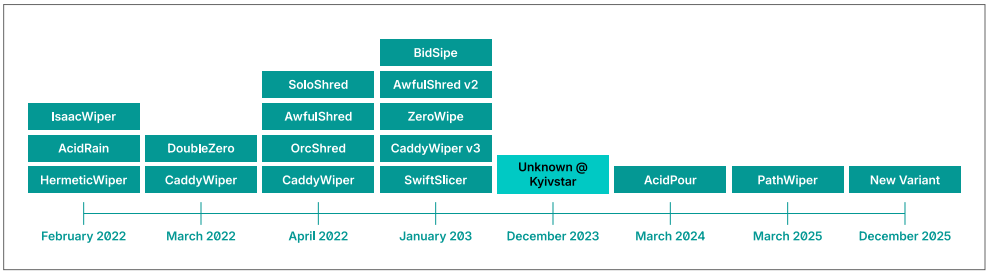
Technical analysis indicates PathWiper:

- Overwrites critical filesystem structures (MBR, NTFS metadata)
- Enumerates mounted volumes systematically
- Targets all accessible storage media to inflict irreversible data loss
- Reflects a more deliberate, volume-aware methodology than HermeticWiper.

While still under active assessment, the malware's destructive purpose, code lineage indicators, and timing relative to the ISP incident align with known ELECTRUM tradecraft. Dragos assesses with low confidence PathWiper may have been deployed as part of a broader, still-unmapped campaign across Ukrainian critical infrastructure. Dragos also identified another destructive wiper variant in December 2025, reinforcing that ELECTRUM continues to iterate, refine, and expand its destructive toolkit. The discovery confirms that ELECTRUM's development pipeline remains active, and its destructive capability set continues to evolve.

INFOGRAPHIC

Timeline of ELECTRUM Wiper Capabilities



The ISP attacks, the emergence of PathWiper, and the December 2025 destructive malware discovery collectively demonstrate that ELECTRUM remains one of the most aggressive and capable OT/ICS-adjacent threat actors in the world. Even when targeting IT infrastructure, ELECTRUM's destructive malware often affects organizations that provide critical operational services, telecommunications, logistics, and infrastructure support, blurring the traditional boundary between IT and OT. KAMACITE's continuous reconnaissance and access-development directly enable ELECTRUM's destructive operations. These activities are neither theoretical nor preparatory, they are part of active campaigns culminating in real-world outages, data destruction, and coordinated destabilization campaigns.

Defensive Recommendations and Mitigations

Control 01: ICS Incident Response Plan

- ELECTRUM's activity targeting Polish energy infrastructure again demonstrated adversary willingness to directly engage operational environments supporting power generation, grid coordination, and energy aggregation. ELECTRUM made deliberate attempts to affect operational assets rather than remaining confined to reconnaissance or access validation, reinforcing that future incidents may involve loss of view, degraded device integrity, unexpected control behavior, or loss of confidence in operational telemetry rather than clean system outages alone.
- ICS incident response plans should explicitly address how organizations will operate when the integrity of field devices, control logic, or command pathways cannot be assumed. Plans should define decision authority and escalation thresholds for transitioning from automated or remote control to local or manual operations, isolating affected control segments, validating sensor accuracy, and maintaining safe operating states while investigations are underway.
- Tabletop exercises (TTXs) should be used to identify the specific operational and cybersecurity questions that must be answered during a suspected OT-impacting incident, such as whether unauthorized control commands were issued, where those commands originated, which assets were affected, and whether current telemetry can be trusted, and ensure the data required to answer those questions is collected and retained ahead of time. This includes defining requirements for OT command logging, network traffic visibility across IT–OT boundaries, remote access audit trails, and telemetry that can support rapid reconstruction of events during response.
- Response playbooks should integrate engineering, operations, safety, and cybersecurity functions to ensure coordinated actions prioritize physical safety, process stability, and controlled recovery over rapid restoration of connectivity. Procedures should include validation of controller and protection logic state prior to re-energization, staged restoration of automation, and clear criteria for returning systems to normal operation following suspected manipulation. Organizations supporting generation, dispatch, or aggregation functions should regularly exercise these scenarios to ensure personnel are prepared to manage operational disruption, not solely IT service degradation.

Control 02: Defensible Architecture

- KAMACITE's expansion into upstream supply-chain compromise and its subsequent reconnaissance of exposed OT edge assets highlight the need for defensible architectures that eliminate implicit trust and constrain adversary movement toward operational systems. ELECTRUM's demonstrated interest in operational leverage points, including CHP facilities and renewable management platforms, further elevates the importance of strong architectural separation between enterprise environments, vendor access zones, and control networks.
- Strict IT/OT segmentation, tightly governed vendor access, and explicit allow-listing of communication pathways are critical to preventing prepositioned access from propagating into environments where operational disruption could be attempted. Field devices, gateways, HMIs, and telemetry infrastructure should not be directly exposed to the internet. Where remote connectivity is operationally necessary, access should terminate in monitored DMZs with controlled routing and inspection before reaching control systems.
- Architectural reviews should explicitly evaluate whether remote access pathways, cellular gateways, or vendor-maintained systems bypass segmentation controls

or introduce unintended trust relationships that could enable rapid escalation from reconnaissance to operational impact.

Control 03: ICS Network Visibility and Monitoring

- Observed KAMACITE scanning activity between March and July 2025 indicates deliberate attempts at mapping of control loops, device roles, and ingress pathways rather than indiscriminate discovery. This type of reconnaissance enables adversaries to understand where commands originate, how they propagate, and where physical effects could be induced, a prerequisite for operational manipulation observed in recent ELECTRUM activity.
- Visibility programs should prioritize detection of reconnaissance behaviors against OT assets, including abnormal enumeration of HMIs, drives, controllers, meters, and industrial gateways, as well as unexpected inbound traffic originating from external networks or vendor access points. Monitoring should extend across IT–OT boundaries to correlate external scanning, vendor authentication events, configuration changes, and deviations from established OT traffic baselines.
- Telemetry capable of identifying abnormal protocol usage, repeated connection attempts, unauthorized service exposure, and unusual data flows is critical for detecting early-stage adversary positioning before access transitions into attempted disruption of operational workflows or control systems. Visibility capabilities should be designed not only to detect anomalous activity, but to preserve the forensic and operational data required to answer time-critical incident response questions identified through ICS tabletop exercises, including command provenance, asset interaction sequencing, and changes to operational state.

Control 04: Secure Remote Access

- Both KAMACITE and ELECTRUM's operations through 2025 demonstrate that both trusted relationships and internet-exposed OT edge assets are viable access pathways. ELECTRUM's recent activity confirms that once access is established, adversaries may attempt to directly affect operational assets rather than remaining confined to reconnaissance or staging.
- All remote access pathways, including vendor connections, VPN infrastructure, cellular gateways, and remote management services, should enforce strong authentication, multi-factor controls, and least-privilege access policies. Internet-facing services should be minimized wherever feasible and continuously assessed for unauthorized exposure or misconfiguration.
- Organizations should ensure remote access infrastructure is monitored, patched, and included in vulnerability management programs, recognizing that compromise of gateways or VPN appliances can provide direct ingress into OT environments that support power generation, dispatch, or grid coordination functions. Vendor access should be tightly governed, time-bound, logged, and routinely reviewed to prevent persistent footholds from being leveraged for operational activity.

Control 05: Risk-Based Vulnerability Management

- The targeted selection by KAMACITE of widely deployed industrial components and devices, some with known security debt, demonstrates how adversaries prioritize vulnerabilities that provide scale, operational leverage, and access into control

environments. Recent attempts by ELECTRUM to affect operational assets reinforce that exposure of vulnerable devices is no longer a theoretical risk but a potential enabler of real-world operational disruption.

- Risk-based vulnerability management programs should prioritize remediation of externally reachable field devices, remote access infrastructure, and systems that directly influence physical processes or bridge enterprise and OT networks. Asset inventories should explicitly track internet-exposed devices, cellular gateways, remote management interfaces, and vendor-managed systems.
- Vulnerability prioritization should incorporate exploitability, exposure, operational consequence, and observed adversary targeting patterns rather than relying solely on severity scoring. Remediation planning should focus on eliminating externally reachable attack surfaces and reducing the feasibility of control-loop mapping, unauthorized access, and downstream operational manipulation.

Threat Group Update:

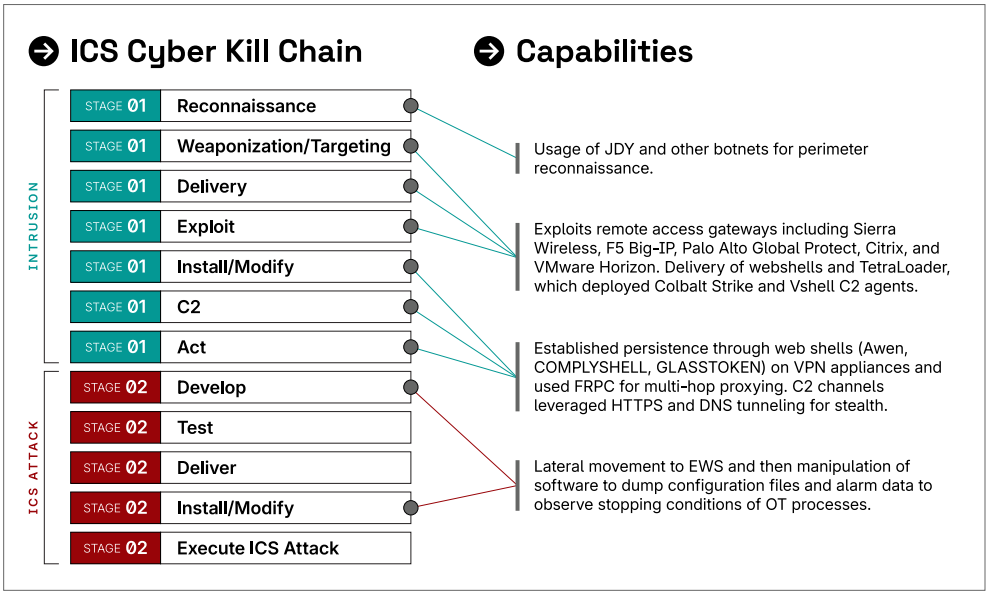
VOLTZITE

About VOLTZITE

As seen in last year's coverage of VOLTZITE, it maintains a dedicated focus on OT data, with a history of OT network intrusions and heavy usage of LOTL techniques. VOLTZITE maintains a dedicated focus on OT data, with a history of OT network intrusions, and leverages proxy networks to steal Geographic Information System (GIS) data, OT network diagrams, and OT operating instructions from its victims. Aided by this ICS-focused data, VOLTZITE could craft a malicious OT-specific tool capable of operational disruption. VOLTZITE has previously exfiltrated GIS data containing critical information about the layout and architecture of energy systems.

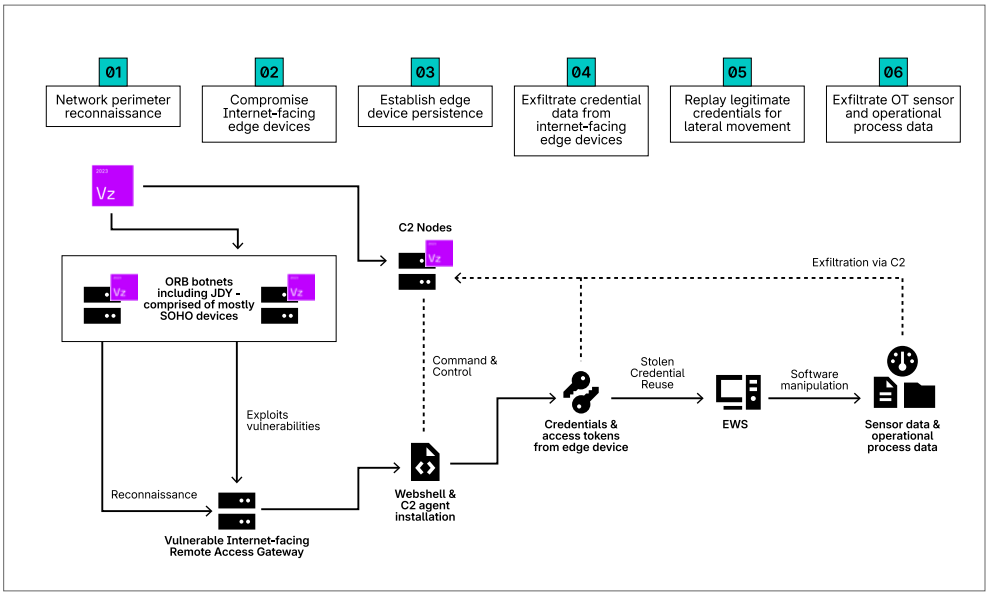
ICS CYBER KILL CHAIN

VOLTZITE: Stage 1 & Stage 2 Attacks



ATTACK PATH

VOLTZITE Attack Path



Sierra Wireless Airlink Targeting

In 2025, VOLTZITE continued its operations against critical infrastructure targets. The most impactful campaign involved compromising Sierra Wireless Airlink RV50 and RV55 cellular gateways using their web interfaces (TCP/9191, TCP/9443) across Electric and Oil and Gas organizations. Sierra Wireless Airlink devices are industrial-grade cellular routers and gateways designed to provide reliable wireless connectivity for mission-critical applications. These cellular routers enable remote monitoring, configuration, and management of connected equipment and networks. They also connect industrial IoT devices, vehicles, and critical infrastructure to cellular networks. Not all cellular gateways are created equal when it comes to interacting with industrial environments. The major risks with these cellular gateways are the following:

- Bypassing Network Perimeter: Cellular connections can create unauthorized pathways into OT networks, bypassing traditional security controls
- Visibility Gaps: IT security teams may not even know cellular devices exist in OT environments
- Legacy Integration: When connected to older OT equipment without security features, the router becomes a critical attack vector
- Physical Security: Devices in remote locations may be physically accessible to attackers

The activity analyzed against Sierra Wireless Airlink devices primarily targeted U.S. midstream pipeline operations but also extended to upstream and downstream environments. Techniques observed included exploitation of remote services, multi-hop proxying for command-and-control, and exfiltration of operational and sensor data, with potential implications for follow-on disruptive actions. The Sierra Wireless devices served as entry points for lateral movement into operational technology networks, allowing potential manipulation of control systems. VOLTZITE pivoted to engineering workstations, where they manipulated the software to dump configuration files and alarm data to investigate what would trigger operational processes to stop. This highlights an increase in VOLTZITE's ICS-specific capability, leading Dragos to designate VOLTZITE as a Stage 2 threat group.

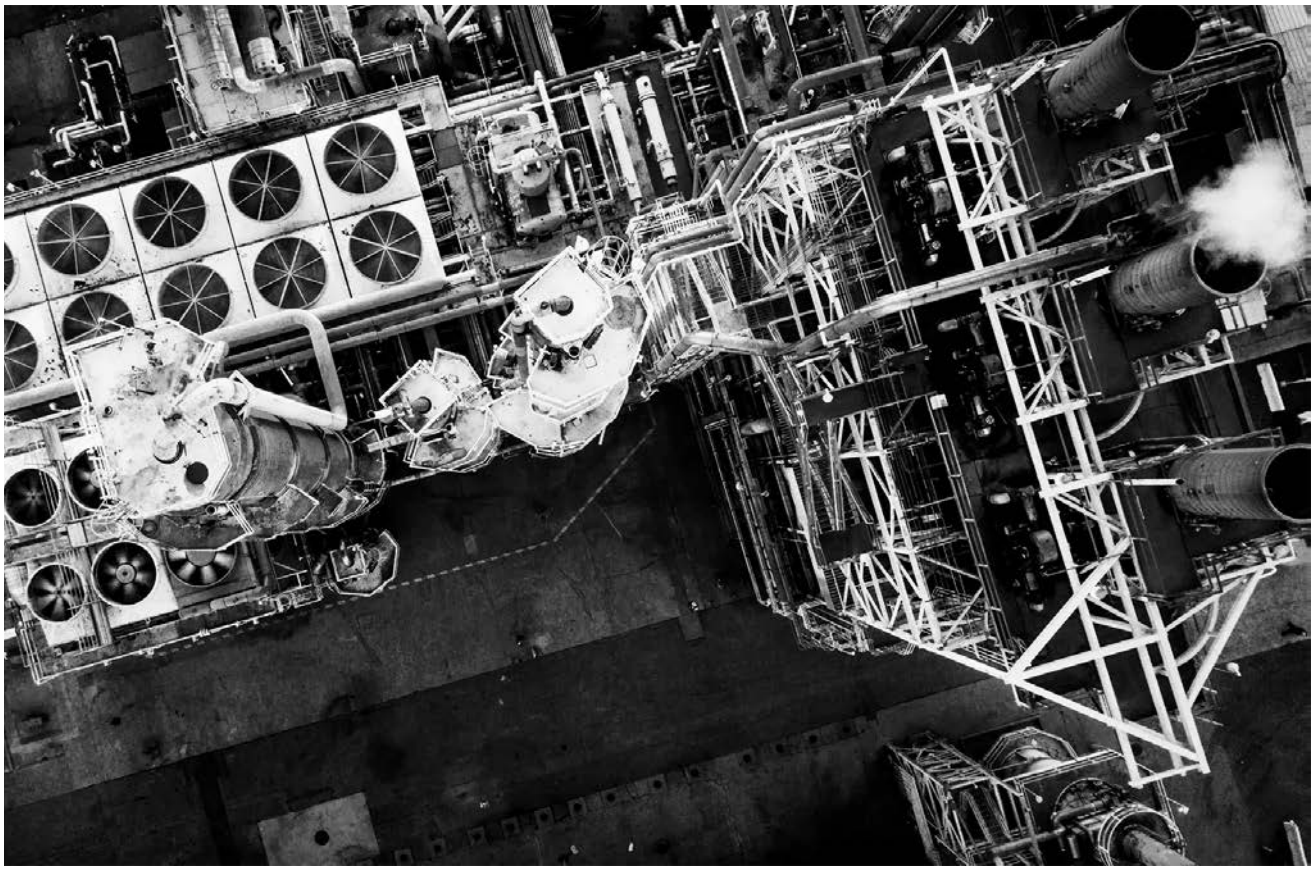
JDY Botnet Activity

Additionally, Dragos observed VOLTZITE-linked activity leveraging the JDY botnet to conduct systematic reconnaissance of public-facing Internet Protocol (IP) address ranges and remote access gateways across the Energy, Oil and Gas, and Defense sectors. This scanning focused on VPN appliances, including F5 Big-IP, Palo Alto GlobalProtect, and Citrix. While no exploitation was confirmed during this phase, Dragos assesses with moderate confidence that the intent appeared to be pre-staging for future intrusions and exfiltration of operational data.

Exploited Trimble Cityworks GIS Software

In early 2025, TAT25-09 exploited a RCE vulnerability (CVE-2025-0994) in Trimble Cityworks (Cityworks) GIS asset management software via Microsoft Internet Information Services (IIS) servers. Dragos identified low confidence operational overlap between VOLTZITE and this operation. The vulnerability stems from unsafe deserialization in IIS when handling Cityworks application data, allowing the adversary to craft malicious serialized objects that execute arbitrary code without authentication. Attackers deployed JoJoLoader, an open-source Rust-based loader, to deliver payloads such as Cobalt Strike and VShell, enabling command execution and data exfiltration. GIS systems map physical assets and operational relationships. Stolen GIS data can enable adversaries to plan precise, disruptive attacks on Electric and Water utilities. US based utilities and municipalities often rely on GIS data for infrastructure operations, but this information can be weaponized by adversaries for future ICS intrusions. Asset owners should remove unnecessary internet exposure for GIS servers, prepare for adversaries to use stolen GIS data in future ICS attacks, and assess other GIS vendors for similar vulnerabilities.

Overall, VOLTZITE's 2025 operations reflect a shift toward not only collecting and exfiltrating data from IT networks but also directly interacting with OT network-connected devices and stealing sensor and operational data. Every VOLTZITE campaign in 2025 hinged on exploiting or enumerating the following devices: Sierra Wireless AirLink RV50/RV55 for direct ICS access and manipulation, and VPN gateways (F5 Big-IP, Palo Alto GlobalProtect, Citrix, VMware Horizon). If these assets are hardened, patched, and monitored for anomalous behavior, VOLTZITE loses its easiest and most reliable path into OT environments.



Insights From Dragos Intelligence Fabric

- 32 percent of Dragos Network Penetration Tests included successful password spraying over SSH or SMB, techniques favored by VOLTZITE.
- Less than 5 percent of Dragos Services engagements revealed PowerShell Execution Logging enabled, which is an essential piece of detecting VOLTZITE.
- 95 percent of Services customers employed MFA for remote access. VOLTZITE commonly leverages insecure remote access to gain initial access to OT environments.

Defensive Recommendations and Mitigations

Control 01: ICS Incident Response Plan

- VOLTZITE gains initial access via the exploitation of network edge devices or footholds established by SYLVANITE in a similar fashion. As it moves deeper into IT and OT networks, VOLTZITE exfiltrates Geographic Information System (GIS) data, OT network diagrams, and OT operating instructions from its victims. ICS incident response plans should address scenarios in which an adversary exploits an emerging vulnerability in internet-facing network devices and then establishes multiple long-term persistence mechanisms, ultimately leading to the exfiltration of sensitive OT data.

Control 02: Defensible Architecture

- Asset owners should apply best-practice general and device-specific security hardening techniques on network edge devices, and continuously monitor remote access, such as cellular gateways and VPN appliances, as they are VOLTZITE's primary beachhead into ICS networks.

Control 03: ICS Network Visibility and Monitoring

- With VOLTZITE's tradecraft reliant on exploiting blind spots in edge devices and OT-adjacent systems, Dragos recommends visibility beyond standard perimeter monitoring. Specifically, continuous telemetry from cellular and remote access gateways is crucial for detecting anomalous web interface access, SSH/HTTP/TLS sessions, and unexpected admin account activity. Internal network monitoring for east-west traffic is crucial for detecting lateral movement.

Control 04: Secure Remote Access

- VOLTZITE operations routinely exploit exposed, unpatched remote-access infrastructure, particularly VPN appliances. Enforcing strong remote access controls, including timely patching of internet-facing services, MFA across all remote access pathways, and strict governance of VPN and third-party access, is critical to disrupting VOLTZITE-enabled intrusions that may lead to follow-on Stage 2 activity.

Control 05: Risk-Based Vulnerability Management

- Either directly or through SYLVANITE operations as a proxy, VOLTZITE conducts exploitation efforts against internet-facing remote gateways. A risk-based vulnerability management program should prioritize remediation of assets and pathways identified as high risk to reduce the likelihood that observed weaknesses are assessed, prepositioned against, or leveraged in future operations.

INFOGRAPHIC

Hunting for VOLTZITE

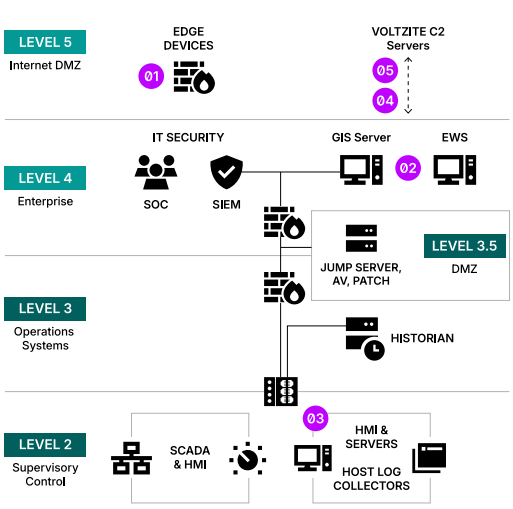
01 Initial access gained through the compromise of internet-facing remote access gateways.

02 Lateral movement to GIS servers and Engineering Workstations (EWS).

03 Manipulation of industrial software on EWS allowed VOLTZITE to extract Level 2 data from OT networks.

04 Communication to VOLTZITE C2 servers.

05 Bidirectional C2 communications.



Threat Group Update:

BAUXITE

SINCE 2023

Bx

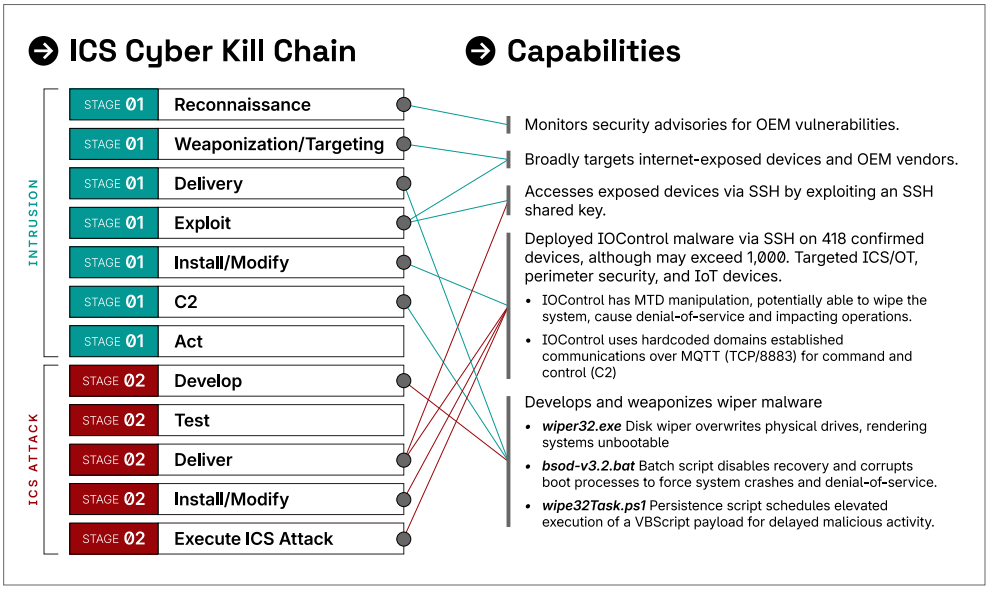
About BAUXITE

Dragos has tracked BAUXITE campaigns targeting OT entities and devices globally since late 2023. BAUXITE shares significant technical overlap with the CyberAv3ngers hacktivist persona, which first emerged in 2020, and demonstrates a direct operational focus on causing severe impact on ICS. BAUXITE represents a credible operational risk to ICS asset owners as it has demonstrated a convergence of hacktivist signaling, destructive malware deployment, and direct ICS-focused targeting. BAUXITE has repeatedly carried out activities consistent with Stage-2 ICS Kill Chain behaviors, including prior manipulation of Unitronics PLCs (November 2023-January 2024), Sophos Firewall Attacks (April 2024-May 2024) and IOControl Campaign (2023-2024) compromising over 400 global OT devices and firewalls. In 2025, BAUXITE escalated its operations by deploying custom wiper malware against targets in Israel amid a regional conflict. This marked a shift from prior access and disruption to destructive intent, with the malware designed to degrade system availability by wiping disks. Although these wipers were not ICS-specific, their use in campaigns that targeted industrial entities reflects a willingness to impose operational downtime and aligns with BAUXITE's broader geopolitical objectives.

BAUXITE also maintained an active hacktivist posture throughout 2025, sending threatening emails to ICS vendors, security researchers, and operational technology stakeholders. This psychological operation is notable because it increases operational and reputational pressure on industrial operators, particularly during periods of heightened geopolitical tension.

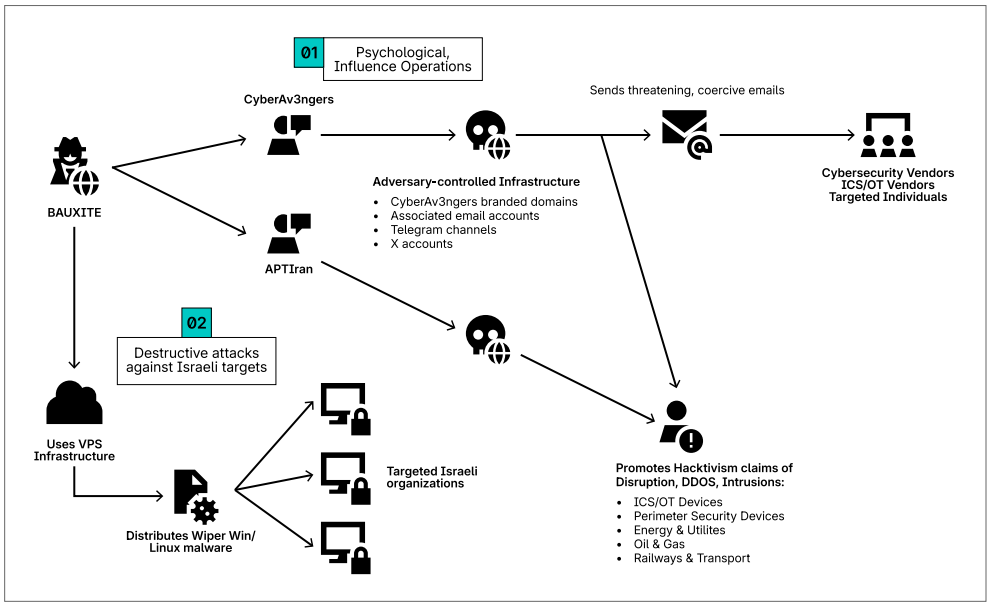
ICS CYBER KILL CHAIN

BAUXITE: Stage 1 & Stage 2 Attacks



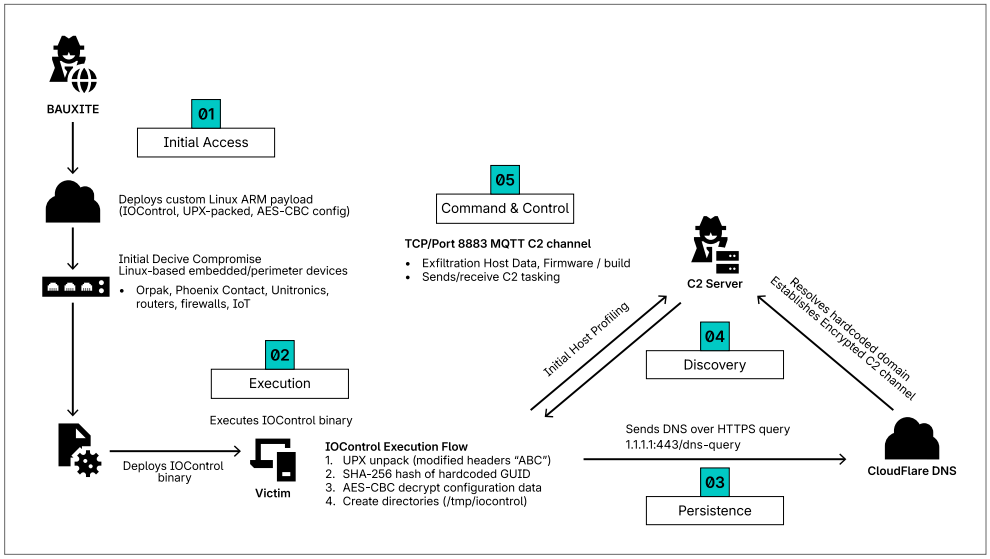
ATTACK PATH

BAUXITE Attack Path 2025 Activity



ATTACK PATH

BAUXITE Attack Path IOControl

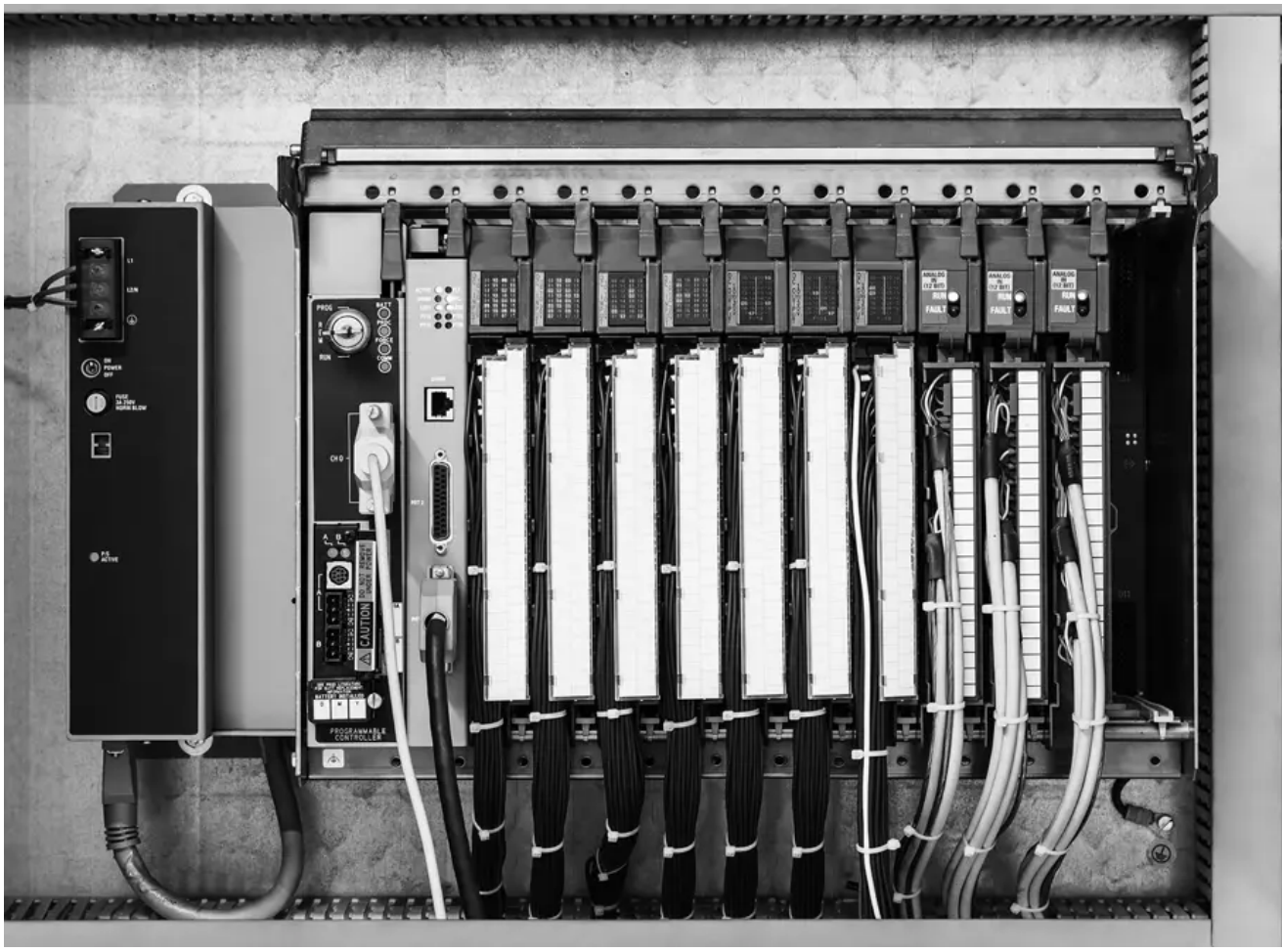


Threatening Email Campaign

In May 2025, the CyberAv3ngers hacktivist persona distributed politically charged threatening emails from an email address associated with a prior CyberAv3ngers Telegram contact profile. Dragos assesses with high confidence that BAUXITE primarily distributed these emails to public email accounts of cybersecurity and ICS vendors, to media organizations, and directly to individuals who have publicly engaged in intelligence research or reporting on CyberAv3ngers' activity. In some cases, an individual's corporate and personal email addresses were targeted. Dragos' review of the email activity found that the distribution was broad and lacked any specific threat or stated intent to attack, and that BAUXITE had likely sought to attract public attention through intimidation and to amplify their perceived notoriety within the cybersecurity community.

Wiper Malware

In June 2025, Dragos conducted a technical analysis of wiper malware and, with high confidence, assessed that BAUXITE had deployed two wiper variants against unspecified targets in Israel in destructive cyber operations. Dragos further assesses with high confidence that BAUXITE's shift toward broader operational disruption activity was likely an adversarial collective response to the conflict between Israel and Iran in June 2025.



Insights From Dragos Intelligence Fabric

- Service accounts with SSH access often rely on shared keys, a condition frequently observed by Dragos Red Team, while Bauxite has independently leveraged shared SSH keys to access exposed devices.
- Restricting service accounts from interactive logon and monitoring for interactive SSH use can significantly reduce this risk.

16%

In 16 percent of service engagements, significant backup deficiencies were identified, a critical concern for restoring systems following wiper malware attacks.

10%

10 percent of Architecture Reviews and Network Penetration Tests identified Service Account and SSH Security issues such as excessive privileges, interactive access, and weak credentials that increase compromise potential.

Defensive Recommendations and Mitigations

Control 01: ICS Incident Response Plan

- BAUXITE activity affecting OT has included unauthorized modification of controller logic, interaction with engineering workstations, and destructive activity against IT systems, which can impact operations. An OT-specific incident response plan should therefore be structured around consequence-based scenarios such as loss of view, loss of control, or loss of availability, and support rapid identification of the intrusion root cause. Response procedures should include validating controller logic and device state, clearly defined decision points for isolating affected OT segments, and coordinated IT–OT response actions when disruption to IT systems affects operational continuity.

Control 02: Defensible Architecture

- BAUXITE access patterns demonstrate the risk posed by weakly defended pathways into OT environments. Defensible architecture should minimize permitted ingress and egress by enforcing segmentation boundaries, industrial DMZs, and tightly controlled communication paths. Asset owners should, where possible, eliminate direct internet exposure for controllers and OT management interfaces and restrict unnecessary services and ports.

Control 03: ICS Network Visibility and Monitoring

- BAUXITE operations involve direct interaction with OT, and while specific techniques may change over time, the effects remain consistent and observable at the network and process level. OT monitoring should prioritize detecting behaviors indicative of operational impact, including unauthorized changes to OT assets, atypical external communications originating from OT environments, and abnormal data movement. Detection should be based on deviations from established OT baselines rather than dependence on previously observed tools or protocols, enabling resilience as BAUXITE TTPs adapt.

Control 04: Secure Remote Access

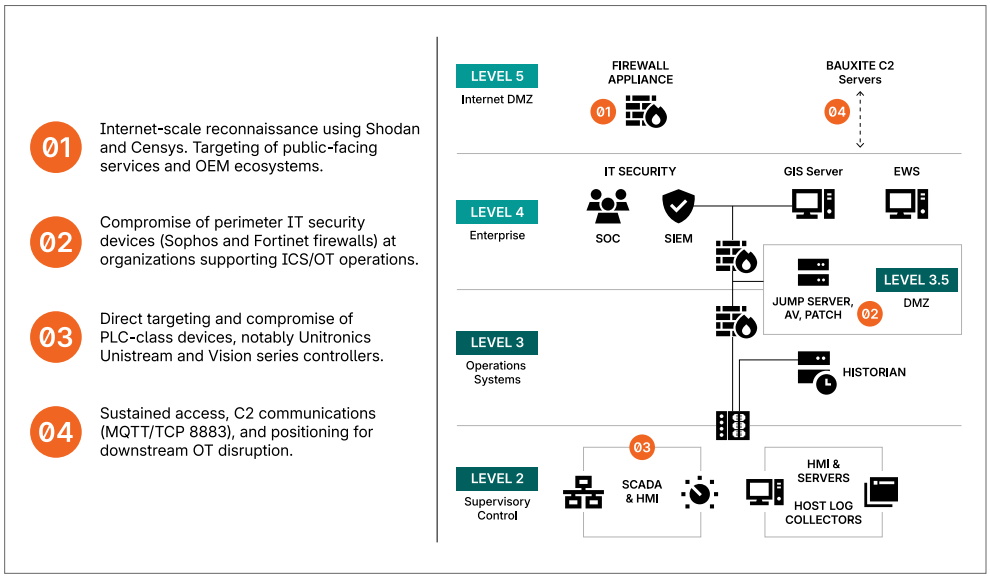
- BAUXITE relies on poorly governed remote access into OT environments. Asset owners should maintain an accurate inventory of remote access paths, route remote and vendor access through monitored jump hosts, and enforce strong authentication and conditional access on externally reachable services. Unmanaged administrative access should be removed by eliminating default or shared credentials, rotating keys where required, and disabling remote management interfaces when not operationally necessary.

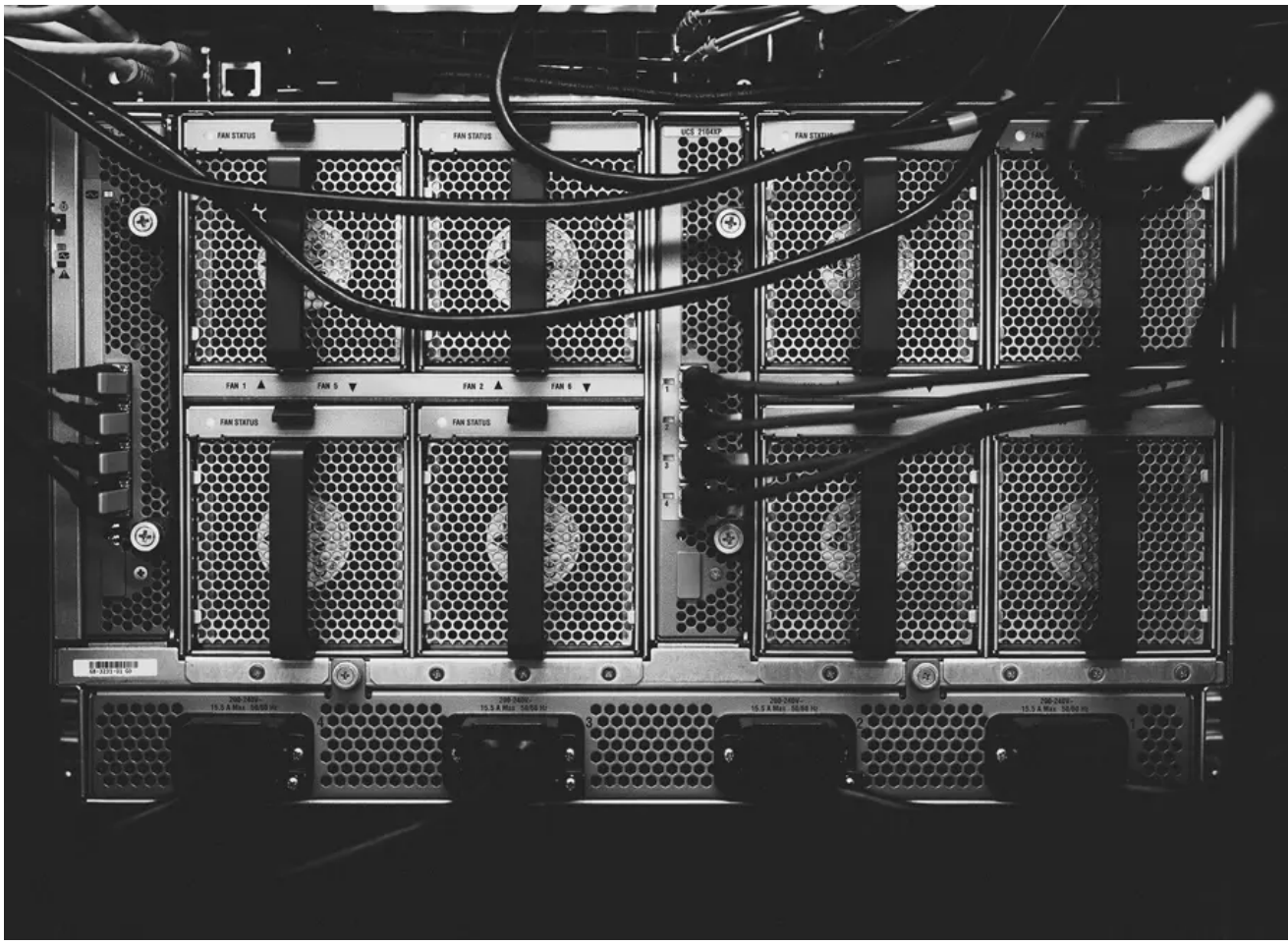
Control 05: Risk-Based Vulnerability Management

- A risk-based vulnerability management program should prioritize remediation of weaknesses that enable manipulation of OT assets, including exposed services, unauthenticated access paths, and firmware or configuration flaws. When remediation is not feasible, these conditions should be tracked and mitigated, as BAUXITE has demonstrated the ability to exploit such weaknesses.

INFOGRAPHIC

Hunting for BAUXITE





03.

ICS-Adjacent Capabilities Research & Trends

The threat groups covered in this report represent the adversaries Dragos tracks with enough analytical confidence to name and characterize. But the broader ecosystem of ICS-relevant capability development extends well beyond those groups. Throughout 2025, Dragos identified new tools, scripts, and operational activity that demonstrate a widening pool of actors acquiring the ability to interact with and disrupt industrial control systems.

What connects these discoveries is a common theme: the tools are not sophisticated. ICS protocols were designed for reliability in environments that were never expected to be connected to outside networks, and they carried that design forward today. They lack authentication, they are well documented, and their protocol libraries are publicly available. Building a tool that can send a command to a PLC or write to a Modbus register does not require the resources of a state program. It requires documentation and a reason to try. The discoveries in this section show that more actors have both.

PLC_Controller.exe

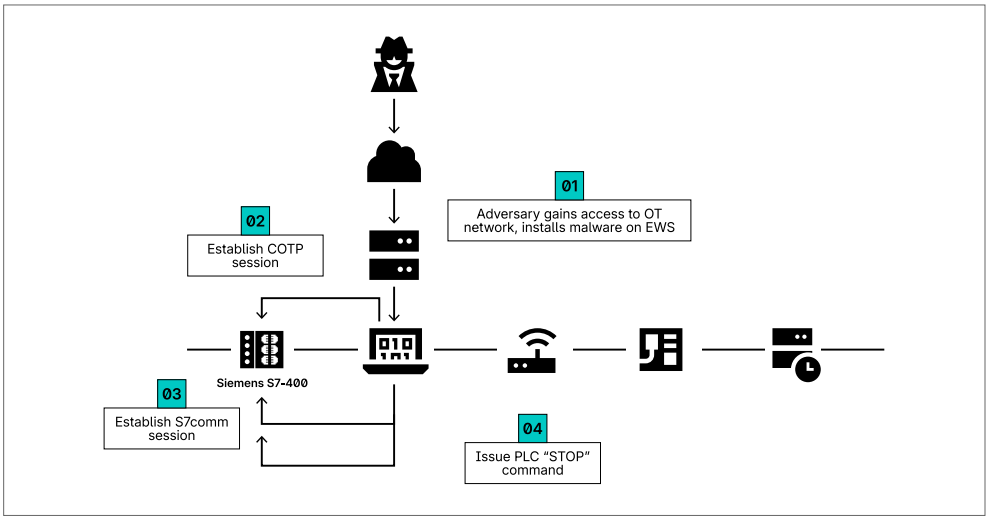
In July 2025, Dragos discovered an attack tool named PLC_Controller.exe, a compiled Python-based tool that can issue S7comm and Connection-Oriented Transport Protocol (COTP) requests to force older Siemens S7 PLC models into "STOP" mode. The availability and functionality of this tool pose tangible risks to ICS asset owners, as a motivated adversary could immediately operationalize the capabilities. If deployed with malicious intent against operational environments, PLC_Controller could cause a loss of control and operational disruption. Dragos found that this capability is limited to older S7-300 and S7-400 models, mirroring the functionality of the Simatic S7 Metasploit modules. However, PLC_Controller.exe is a fully functional tool that could be leveraged to disrupt or degrade operations in an environment running vulnerable Siemens PLCs. Dragos identified 45 percent of S7 PLC devices as older S7-300 and S7-400 models through the Dragos Intelligence Fabric. Dragos assesses, with moderate confidence, that PLC_Controller.exe was used in a national red team exercise coordinated by China's Ministry of Public Security. The availability and functionality of such a capability pose a credible risk to ICS, as a motivated adversary could easily operationalize it. If deployed with malicious intent against operational environments, PLC_Controller could cause a Loss of Control and operational disruption, underscoring the importance of ensuring legacy PLCs are adequately secured and monitored.

Main of PLC_Controller - Strings and Comments Translated from Simplified Chinese

```python
def main():
    """Main function: parse command line arguments and send command in a loop"""
    parser = argparse.ArgumentParser(description='S7 PLC attack tool - sends attack command every 2 minutes')
    parser.add_argument('ip', help='PLC IP address')
    args = parser.parse_args()
    command = 'stop'
    print(f'An attack command will be sent to {args.ip} every 2 minutes')
    print('Press Ctrl+C to terminate the program')
    try:
        iteration = 1
        while True:
            print(f'\n==== Sending command iteration {iteration} ====')
            start_time = time.time()
            result = plc_control(args.ip)
            status = 'Success' if result else 'Failure'
            print(f'Command execution result: {status}')
            elapsed_time = time.time() - start_time
            wait_time = max(0, 120 - elapsed_time)
            time.sleep(wait_time)
            iteration += 1
```

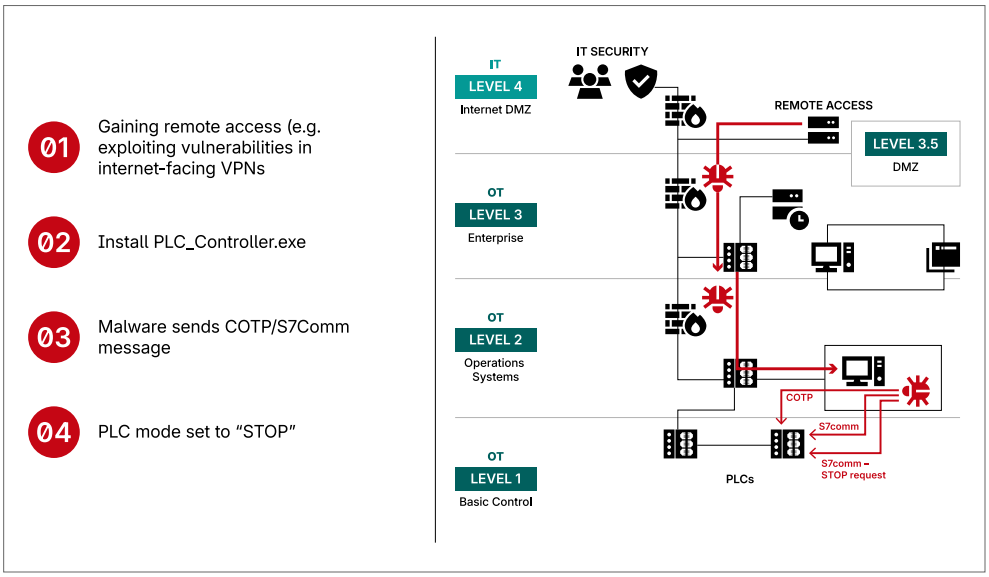
ATTACK PATH

PLC_Controller.exe Attack Path



ATTACK PATH

PLC_Controller.exe Attack Path



Suspicious PowerShell Modbus Tool

In November 2025, Dragos discovered and analyzed a PowerShell script named exploit.ps1 that scans for Modbus servers on a given subnet, identifies holding registers with values greater than 400, and repeatedly writes 1,000 to the holding register. The script was discovered alongside a customized version of a publicly accessible Slowloris HTTP DoS tool. The developers added botnet functionality to Slowloris for coordinated DDoS attacks. Dragos assesses with high confidenceexploit.ps1 is designed to be used as an offensive tool but remains a low-risk threat to OT environments, as it was seemingly developed for a specific environment. Dragos cannot determine whether exploit.ps1 is a legitimate offensive capability or a red-teaming tool used for defensive testing. While exploit.ps1 appears tailored to a specific environment, it could easily be modified to a more generic Modbus capability.

Infinitely Writing to Holding Register via Modbus

```
270     # STEP 5: CONTINUOUS WRITE
271     Write-Host "`n[5/5] Writing $WriteValue to D$targetAddr continuously..." -ForegroundColor Cyan
272     Write-Host "Press Ctrl+C to stop`n" -ForegroundColor Gray
273
274     $writeRegs = ConvertTo-ModbusRegs $WriteValue
275
276     while ($true) {
277         $ok = Write-ModbusRegisters -Addr $plcIP -Prt $Port -Slv $Slave -Ref $targetAddr -Payload $writeRe
278
279         if ($ok) {
280             Write-Host "." -NoNewline -ForegroundColor Green
281         } else {
282             Write-Host "X" -NoNewline -ForegroundColor Red
283         }
284
285         Start-Sleep -Milliseconds $DelayMs
```

Adversaries Stealing ICS Data

Several TATs in 2025 have been observed stealing ICS data, which is useful for mapping OT threats relevant to Stage 2 capabilities. TAT25-74 compromised an India-based metals manufacturer, stealing HMI data from at least two steel and ferroalloy manufacturing plants. The data, in Microsoft SQL Server backup files, included thousands of industrial process control tags and dozens of user credentials for the affected HMIs. After analyzing some of the control tags, Dragos assesses with high confidence information was obtained from a graphite-based arc furnace process.

TAT25-95 compromised a Pakistani state-owned power transmission company responsible for operating and maintaining high-voltage power transmission networks. TAT25-95 used Metasploit and Impacket to abuse the Active Directory environment for privilege escalation and lateral movement, then subsequently exfiltrated user credentials, NTLM hashes, Kerberos tickets, private keys, and other sensitive data. TAT25-95 was observed searching for "SCADA" related exploits in Metasploit, then scanning for open ports on TCP/502. Further, TAT25-95 gained access to the victim's OwnCloud file storage and syncing server and enumerated the file system, searching for files with "SCADA" in the name or path. TAT25-95 used Meterpreter to exfiltrate discovered files, including approximately 100 PowerPoint files. The information obtained provided details of the victim's operational processes and could be used to develop and deploy an ICS capability designed to disrupt, degrade, or deny access to OT environments.

Searching for SCADA-related Metasploit Modules

```
msf6 auxiliary(scanner/smb/smb_login) > search type:auxiliary scada

Matching Modules
================

   #   Name                                                  Disclosure Date
   -   ----                                                  ---------------
   0   auxiliary/dos/scada/igss9_dataserver                  2011-12-20
   1   auxiliary/admin/scada/advantech_webaccess_dbvisitor_sqli  2014-04-08
   2   auxiliary/admin/scada/multi_cip_command               2012-01-19
   3   auxiliary/scanner/scada/bacnet_l3                     .
   4   auxiliary/dos/scada/beckhoff_twincat                  2011-09-13
   5   auxiliary/scanner/scada/digi_addp_version             .
   6   auxiliary/scanner/scada/digi_addp_reboot              .
   7   auxiliary/scanner/scada/digi_realport_serialport_scan .
   8   auxiliary/scanner/scada/digi_realport_version         .
```

Scanning the Modbus Servers

```
msf6 auxiliary(scanner/portscan/tcp) > set rhosts 172.[redacted].0/24
rhosts => 172.[redacted].0/24
msf6 auxiliary(scanner/portscan/tcp) > set ports 502
ports => 502
msf6 auxiliary(scanner/portscan/tcp) > run
```

Hacktivists and Proven Claims

In 2025, Dragos observed hacktivism continue to evolve from symbolic website defacements and surface-level DDoS attacks into a more sophisticated, geopolitically influenced threat ecosystem. Hacktivist groups increasingly blend ideological messaging with state-aligned interests, adopting tactics traditionally associated with financially motivated or nation-state threat actors. Campaigns incorporate large-scale data leaks, synchronized information operations, and attempts to disrupt physical processes. Platforms like Telegram and X serve as command-and-amplification hubs, while accessible AI-driven reconnaissance tools and DDoS-for-hire marketplaces significantly expand operational reach. These groups increasingly publish intrusion walkthroughs, configuration files, or control-system screenshots to maximize psychological and/or geopolitical impact.

As expected, Dragos observed that the most abused exposure points include internet-facing HMIs; however, misconfigured engineering workstations, weak remote-access services (especially VNC, RDP, and SSH with default or reused credentials), and open field protocols such as Modbus/TCP, DNP3, and MQTT exploited in hacktivist operations were also observed. Several campaigns exploited OPC UA endpoints that lacked authentication and Internet-exposed BACnet devices. Groups such as Z-Pentest and Dark Engine leveraged broad scanning platforms, often built on open-source tools, to identify vulnerabilities in HMIs, PLC gateways, and historian servers.

Once inside a victim's network, hacktivist groups frequently demonstrated basic but effective lateral movement, including pivoting from a compromised Windows "jump host" to a domain controller via SMB or RDP before accessing file servers or engineering project repositories. In environments with flat or poorly segmented IT/OT networks, attackers have accessed PLC management interfaces or brokered communications servers (e.g., MQTT brokers, OPC UA gateways) by simply following broadcast traffic or conducting lightweight scans.

In 2025, hacktivist groups also started adopting toolsets previously associated with advanced adversaries. For initial access, some campaigns referenced the use of Cobalt Strike beacons or open-source equivalents (Brute Ratel-like frameworks, Sliver C2). For reconnaissance, operators frequently relied on Advanced IP Scanner, Angry IP Scanner, various 'netscan' utilities, or built-in capabilities such as Windows net commands, WMI queries, and PowerShell, which are considered LOTL techniques. Across Linux-based OT gateways, hacktivists have been observed abusing Dropbear SSH, BusyBox utilities, and default system binaries to maintain persistence or perform enumeration. While still opportunistic, the blending of C2 frameworks with LOTL approaches reflects a maturation of capability.

Targeting specific hardware and firmware has also been publicly claimed. Examples include exploitation of outdated cellular gateways such as Sierra Wireless AirLink RV50/RV50X devices running older ALEOS firmware; attacks against exposed Moxa EDR and NPort units; and opportunistic targeting of industrial VPN appliances. In several cases, hacktivists exploited known vulnerabilities in Fortinet FortiOS, taking advantage of organizations that had not yet updated. Other incidents involved outdated HMI/SCADA web servers running legacy versions of Indusoft Web Studio, Ignition instances with unsecured MQTT brokers, and Siemens SIMATIC panels deployed with default credentials. While some claims cannot be fully validated, they align with the well-documented presence of thousands of outdated OT devices online.

The single most crucial defensive action remains the elimination or hardening of external exposure. Minimizing internet-facing interfaces, enforcing strict network segmentation, enabling MFA for all remote access, and keeping OT gateways, HMIs, and VPN appliances fully patched fundamentally reduces the attack surface. Environments that layer segmentation with strong authentication, continuous monitoring, and disciplined patch management are far less likely to experience the opportunistic but increasingly capable campaigns that define hacktivism in 2025.

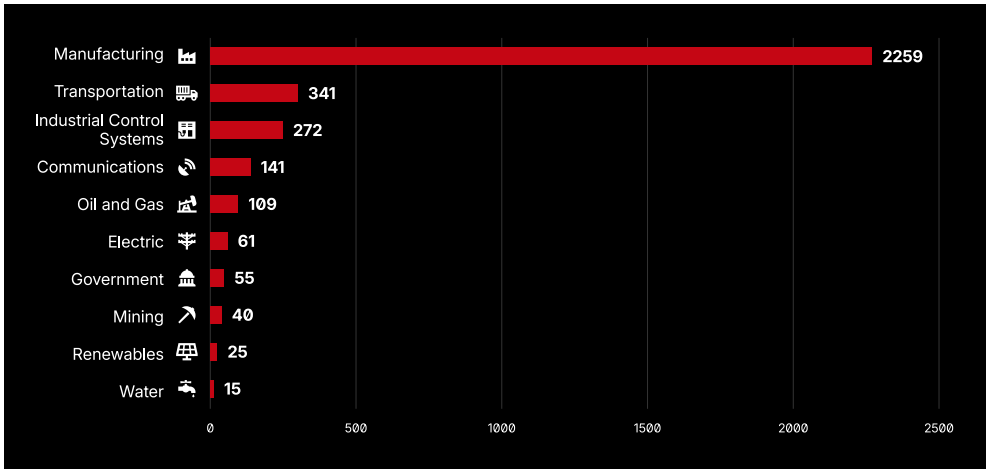
04.

Ransomware-as-a-Service (RaaS) Threats to Industrial Organizations

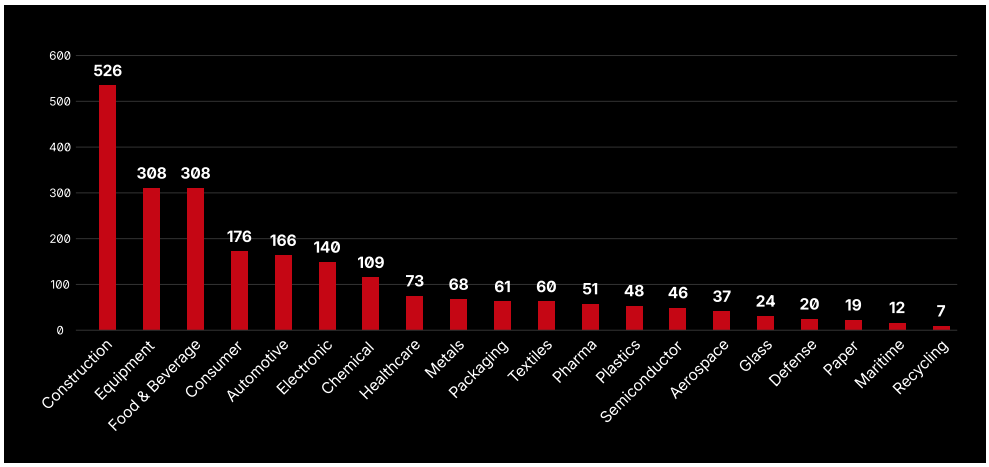
Overview

The persistent mischaracterization of ransomware as solely an IT problem obscures growing risks to OT environments. While adversaries increasingly target industrial organizations—with attacks becoming more frequent and disruptive—they rely on basic tactics that exploit weak security practices rather than sophisticated techniques. Additionally, Dragos has observed numerous instances in which a ransomware case was classified as IT only because the victim company or its security firm misclassified OT devices, such as engineering workstations and HMIs, as IT devices because they ran on Windows Operating Systems. While exact numbers are difficult to obtain, there are a considerable number of OT-specific ransomware incidents that are mischaracterized. Dragos tracked 119 ransomware groups targeting industrial organizations in 2025, a ~49 percent increase from 80 in 2024. These groups collectively impacted 3,300 industrial organizations, reflecting affiliate-driven volume and persistent targeting of industrial sectors. The actual number is likely higher, as many incidents go unreported or undetected. Strong OT detection maturity, underpinned by comprehensive visibility, remains foundational to detecting ransomware in OT networks. This capability directly correlates with response success: organizations with solid OT detection contain faster, remediate more effectively, and minimize damage to critical operations. Manufacturing accounted for more than two-thirds of all observed victims, underscoring how deeply the sector depends on highly integrated IT–OT systems and how quickly ransomware-related outages can propagate into production and operational workflows.

Ransomware by Sector



Ransomware Impact by Manufacturing Subsectors



Ransomware by Region

Ransomware Targeting Virtualization and OT Boundary Systems

Ransomware groups and affiliates in 2025 continued to rely on remote-access and virtualization abuse. Dragos consistently observed affiliates using valid credentials, commodity infostealers, or initial access broker (IAB)-provided access to authenticate into VPN portals, firewall interfaces, or vendor tunnels before pivoting into OT boundary networks. Once inside, they leveraged RDP, SMB/PsExec, WinRM, WMI, and SSH to move laterally toward VMware ESXi hypervisors and OT-support servers hosting SCADA, HMI, historian, and engineering workloads. The operational impact stemmed not from ICS-specific malware, but from the encryption or corruption of the virtualization infrastructure on which OT depends. These activities routinely resulted in Denial of View, Denial of Control, and multi-day Loss of Productivity and Revenue, even without any interaction with industrial protocols, i.e., a Fog affiliate that used compromised VPN access to reach an OT-adjacent ESXi hypervisor and deploy ransomware on SCADA-supporting virtual machines. Although no PLCs or field devices were touched, the loss of the virtualization layer immediately removed operator visibility and control, resulting in operational delays until the systems were rebuilt.

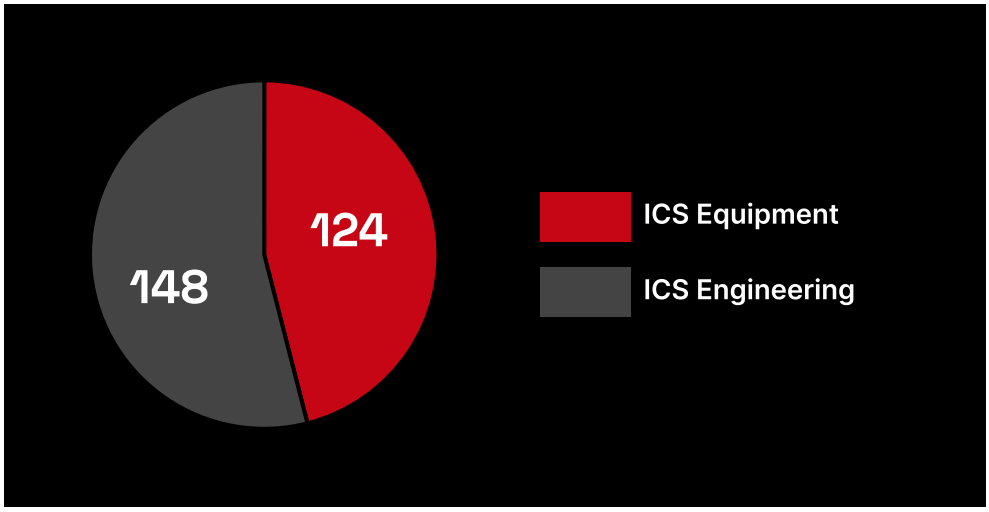
Expansion and Fragmentation of the RaaS Ecosystem

Dragos observed a more fragmented ecosystem in which affiliates frequently moved between RaaS programs and used the same intrusion playbooks regardless of RaaS group association. This fragmentation, combined with increased availability of stolen credentials and ready-made access from IABs, lowered the barrier for affiliates to launch opportunistic campaigns against industrial organizations. Fragmentation was also evident in the lineage of several ransomware programs active in 2025. Devman, Akira, BlackSuit, and INC Ransom reflect the continued dispersion of operators and affiliates from the broader Conti ecosystem, re-emerging under new brands while maintaining similar tradecraft and targeting patterns. In parallel, Dragos identified TAT24-87 operating as a highly active IAB whose access was subsequently leveraged by multiple ransomware operations, including BlackBasta, BlackSuit, 3AM, and EncryptHub. These overlaps in access, infrastructure, and operator behavior indicate that many of the "new" groups observed in 2025 were drawing from the same underlying affiliate pool and IAB-provided footholds rather than representing truly distinct adversaries.

Increased Targeting of OT-Adjacent and Supply-Chain Entities

Throughout 2025, ransomware affiliates continued to compromise engineering firms (148 compromises), OT managed-service providers, ICS equipment vendors (124 compromises), and system integrators. These are all organizations whose environments often contain engineering documentation, configuration backups, remote access credentials, and privileged pathways to multiple industrial sites. This reflects a broader cybercrime strategy in which adversaries seek maximum operational leverage by targeting entities whose compromise can exert pressure across an entire industrial ecosystem rather than on a single operator. Cl0p's exploitation of Cleo MFT, CrushFTP, and later Oracle E-Business Suite (EBS) demonstrated how a single vulnerability in widely used file-transfer or ERP software can expose operational documents, engineering data, and vendor-customer integrations across hundreds of industrial organizations, even when no OT networks are directly accessed.

ICS Subsectors Impact by Ransomware



False ICS Claims and Narrative-Driven Extortion

A growing trend in 2025 was the use of false ICS claims in ransomware extortion. Dragos observed multiple ransomware operators and hybrid hacktivist personas attempting to inflate their perceived capabilities by misrepresenting access to industrial systems. In one example, Devman published screenshots of hypervisor consoles and environmental monitoring dashboards, falsely claiming to have developed "ICS-aware ransomware." Dragos analysis found no evidence supporting these assertions and no indication Devman accessed or could interact with ICS equipment. Despite being technically inaccurate, such claims created uncertainty for victims, introduced friction into executive decision-making, and attracted media amplification. These narratives allowed adversaries to artificially increase extortion pressure.

Identity-Centric Intrusions Enabling IT-to-OT Operational Impacts

During 2025, affiliates increasingly relied on credential logs sourced from infostealers, password reuse across OT and IT systems, cloud-synchronized identities, and compromised vendor accounts sold through IAB marketplaces. This approach allowed adversaries to bypass perimeter detections entirely by authenticating legitimately into VPN portals, remote desktop infrastructure, and cloud identity providers used across IT–OT boundaries. Identity abuse allowed adversaries to move rapidly and quietly through enterprise environments. These campaigns required no specialized exploits and often avoided detection entirely until critical enterprise systems underpinning OT continuity such as ERP, virtualization, cloud SaaS platforms, or backup infrastructure, were degraded or unavailable.

TAT25-84 (Scattered Lapsus$ Hunters) provided the clearest illustration of this identity-centric threat model. Building on TAT24-02's tradecraft, the group systematically exploited help-desk workflows, self-service password reset mechanisms, and MFA enrollment to gain privileged access. This enabled compromise of SAP, Azure AD, ERP, and virtualization platforms that indirectly support industrial operations. Resulting impacts included production line shutdowns due to ERP outages, logistics delays that disrupted maintenance scheduling, and loss of visibility into vendor-supplied industrial components. Although TAT25-84 did not access ICS assets or execute Stage 2 activity, their identity-driven intrusions demonstrated how compromises of enterprise identity systems can cascade into measurable OT impacts, particularly in highly integrated industrial environments where IT availability is essential to operational continuity.

Overall, the ransomware threat landscape impacting industrial organizations in 2025 remained highly active and operationally disruptive, shaped less by the emergence of ICS-tailored malware and more by the expanding, fragmented ecosystem of affiliates and IABs exploiting weaknesses in remote access, identity, supply-chain relationships, and OT-support virtualization. As these trends show no sign of slowing, OT/ICS asset owners must, above all, implement ICS network visibility and monitoring, as well as proper segmentation. ICS-grade rigor should be applied to all OT access pathways and OT-support virtualization, treating VPNs, vendor tunnels, identity providers, and ESXi/vCenter environments that touch OT as critical ICS assets, so that even when ransomware compromises enterprise systems, it cannot easily escalate into industrial outages.

Insights From Dragos Intelligence Fabric

- Dragos incident response teams observed an increase in cases involving compromised credentials and unauthorized access to VMware ESXi during ransomware events.
- Exploitation of trusted third-party relationships is frequently observed in incidents involving leaked credentials from external partners.
- 5 days is the average dwell time for Dragos OT Ransomware Cases in 2025, all time is 42 days for Ransomware.
- Dragos Incident Response observed significant operational disruption in all OT ransomware cases in 2025.
- 54 percent of Dragos Services Architecture Reviews conducted revealed appropriate levels of ICS network monitoring deployed.
- 88 percent of Dragos TTXs reported degraded detection capabilities.
- 3 percent of Network Penetration Tests reported lack of monitoring - customer's do not often request a Network Penetration Tests if they lack monitoring. They are almost certainly past the initial implementation stages of monitoring and are now progressing towards operationalizing or optimizing their visibility.
- 56 percent of Dragos Network Penetration Tests included findings related to LOTL activity.
- 3 percent of services engagements identified use of default credentials.
- 53 percent of services reports identified public or internet facing assets.
- 49 percent of services engagements revealed remote access weaknesses.

OT Ransomware Stats

54%

of Dragos Services Architecture Reviews conducted revealed appropriate levels of ICS network monitoring deployed

88%

of Dragos TTXs reported degraded detection capabilities

23%

of IR cases were OT ransomware

42 days

Average dwell time of OT ransomware across all services data

05.

Vulnerabilities

The threat groups documented earlier in this report are getting into OT environments through a relatively consistent set of paths: exposed VPNs, unpatched edge devices, remote access infrastructure, and credential reuse. These are not exotic attack surfaces. They are known weaknesses in known products, and in many cases the vulnerabilities being exploited have public proof-of-concept code available. The gap is not awareness that these vulnerabilities exist. The gap is that the OT vulnerability ecosystem does not always give defenders what they need to act on them.

Industrial vulnerability management is fundamentally different from its IT counterpart. Advisories are frequently published with no patch, no workaround, and sometimes inaccurate severity scores. Equipment runs on decades-long life cycles where patching may be impractical, risky, or irrelevant to the actual threat. And the conventional wisdom of prioritizing by CVSS score breaks down in environments where a medium-severity flaw on an internet-exposed gateway poses far more real-world risk than a critical-rated vulnerability buried deep in an air-gapped process network.

This section examines the vulnerability landscape as it actually affects OT defenders: where the advisory ecosystem falls short, how adversaries are exploiting what is available, where emerging technologies like battery energy storage systems are introducing risk faster than security practices can account for, and what the data says about where to focus limited resources.

Battery Energy Storage System and Demand Energy Response Research

Following a DOE whitepaper on battery energy storage systems (BESS)[1], Dragos investigated the security of battery management system (BMS) products. This led to an internal research project to evaluate the security of Nuvation BMS and Multi-Stack Controllers (MSCs), which are manufactured in the United States and Canada and distributed globally.

Product-Specific Vulnerabilities

The Nuvation BMS is a typical field device with no meaningful security. Direct network access to the BMS allows disconnecting batteries, changing battery chemistry, capacity, reserve capacity, shunt, and relay settings. These, in turn, can result in a loss of control, a loss of view, manipulation of control, and manipulation of view in a BESS. For example, manipulating battery capacity or shunt configuration can change an asset owner's view of the battery's charge status, and changes to the minimum reserve capacity and relay settings can affect battery availability by causing the BMS to disconnect the battery. For these reasons, the Nuvation BMS is not intended to be exposed to higher-level networks. A list of Nuvation-related vulnerabilities may be found on the Dragos website[2]. Additionally, Dragos evaluated the MSC, which is intended for exposure to higher level networks. The MSC also provides cloud access, allowing Nuvation to remotely monitor and reconfigure the battery systems. During this evaluation, Dragos identified authentication bypass and OS command injection vulnerabilities in the MSC (since fixed by the vendor). Furthermore, Dragos assessed the cloud service used to remotely manage the systems, which allowed any user with credentials to manipulate other user's BMS. This access could be obtained by reverse-engineering equipment to obtain cloud credentials. This issue has also been fixed as of December 2025.

The full details of these vulnerabilities are published in VA-2025-06. Dragos advises end users to restrict access to both the BMS (especially TCP/80 and TCP/502) and the MSC (especially TCP/80, TCP/443, TCP/502, and TCP/3003). Security-conscious users may wish to prevent the MSC from making outbound UDP/1194 network connections.

Wider Industry Issues

One item Dragos evaluated with Nuvation products was the support for an industry-standard communications overlay called SunSpec. This is a data model which can be implemented on Modbus or DNP3 network protocols that provides a self-describing map of data and control points.[3] This allows vendor-agnostic tools to automatically discover the meaning of IO points defined in a device which implements SunSpec.

While useful for asset owners, this functionality may enable attackers to use tools that also discover the IO and control points on a device. Due to the standard, there are basic controls which devices 'MUST' implement. For example, BMSs feature a control word to disconnect or

1 **Battery Energy Storage Systems Report – U.S. Department of Energy** https://www.energy.gov/sites/default/files/2025-01/BESSIE_supply-chain-battery-report_111124_OPENRELEASE_SJ_1.pdf

2 **Nuvation Battery Storage Systems Vulnerabilities: CVE-2025-64119 – Dragos** https://www.dragos.com/community/advisories/CVE-2025-64119

3 **SunSpec Model Definitions – Github** https://github.com/sunspec/models

reconnect their battery stacks, which can cause a loss of control for owners of battery systems. The full range of settings on the BMS is not available via SunSpec; however, several attacks are possible with an understanding of the data model, which are publicly available.

SunSpec Modbus also features tables for many other product types, including inverter-specific profiles, generic profiles for AC-producing equipment, and generic profiles for DC power systems. Dragos scanned the Internet for devices that implement Modbus-SunSpec and found just over 100, including 1MW power inverters designed to supply grid power to electric utilities. These inverters contain remote control capability including the ability to disconnect the inverter. These inverters were likely in production, with readable output of 500-900kW during daylight hours.

Since SunSpec Modbus is a traditional control systems protocol, it allows manipulation without authentication. Therefore, protection is largely device dependent. For example, some devices may prevent sensitive direct operations, such as changing battery capacity or other settings, while the device is in use. However, it appears that many SunSpec devices will follow the specification requirements, which require that certain control commands be implemented in specific registers. These registers are discoverable without referring to a device-specific datasheet, instead they are described in SunSpec device profiles. This makes them easier to discover and makes attack tool development far simpler and more re-usable.

It is worth noting that the SunSpec Alliance published several security specifications, including firmware upgrade and authentication requirements. Dragos has not yet identified any device implementing this security profile. Upon review of the specifications, Dragos also remains skeptical that the security requirements will offer adequate protection against modern threat groups. A device could implement the requirements of current security specifications and still allow unauthorized access to systems, the loading of malicious firmware, and changes to sensitive settings without a meaningful barrier to entry.

End users should require that distributed energy resources (DER) implement the SunSpec security standards, but should not rely on these standards to provide full protection on their own. For these reasons, every BESS should be protected from direct network access. Furthermore, any cloud or VPN management service for a BESS should be evaluated for basic security controls, such as whether clients can access BESS resources owned by another client (as in the Nuvation evaluation). Subcontracting seems to be a common theme in internet-exposed BESS and other SunSpec systems. Management of the systems is often outsourced to firms which specialize in battery or other DER systems, but these firms often lack cybersecurity knowledge.

Exploitation of Vulnerabilities in ICS

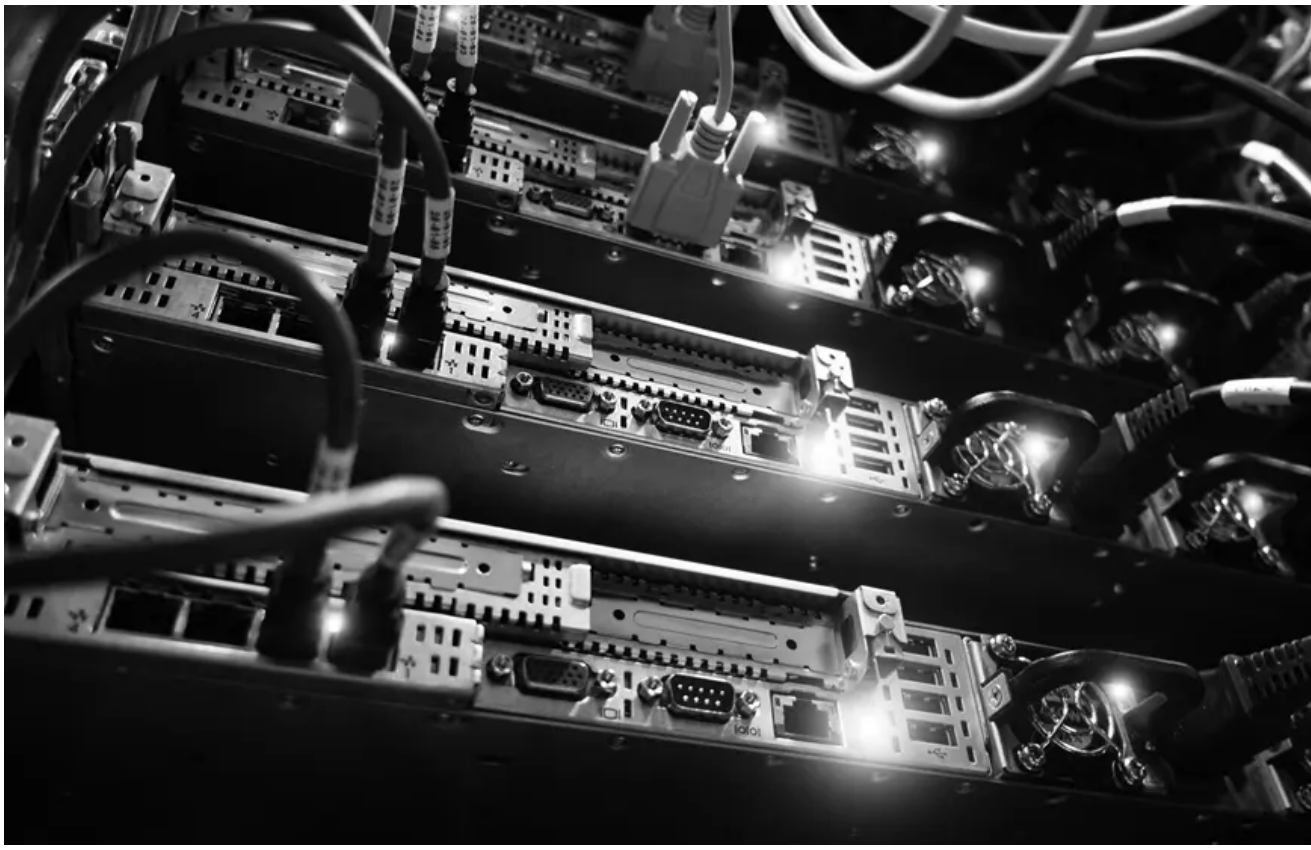
In 2025, Dragos determined that most ICS-specific vulnerabilities exploited were used to gain initial access or facilitate reconnaissance in OT. Only ~4 percent of ICS-relevant vulnerabilities are exploited in the wild, and half of those (2 percent) are only relevant to ICS because they provide unauthorized access to ICS networks. Most of the exploitation identified in 2025, targeted applications and devices vulnerable to unauthenticated remote code execution, many of which have public Proof of Concepts (POC) available online. It's important for asset owners to understand exposure, track vulnerabilities with public POCs, and monitor feeds, such as Known Exploited Vulnerabilities (KEV), to stay informed about active exploitation.

Ransomware Groups Continue to Target Exposed FTP Servers

In 2025, Dragos observed widespread exploitation of vulnerabilities in file transfer solutions, including Cleo MFT, CrushFTP, and Wing FTP. These flaws allow adversaries to gain administrator-level access or execute arbitrary code remotely, often without authentication. Once compromised, adversaries can steal sensitive files, deploy backdoors, and potentially pivot deeper into connected networks. File transfer tools often handle operational documents, engineering files, and credentials, making them attractive targets for ransomware groups and IABs seeking financial gain through extortion or resale of access.

Beginning in late 2024, the Cl0p ransomware group exploited Cleo MFT vulnerabilities (CVE-2024-50623 and CVE-2024-55956) and claimed to have targeted more than 300 victims across the Transportation, Manufacturing, and Food sectors. CrushFTP faced two major campaigns in 2025: CVE-2025-31161 in March and CVE-2025-54309 in July, enabling attackers to bypass authentication and gain full control of servers. Wing FTP was also targeted via CVE-2025-47812, which allowed unauthenticated remote code execution through Lua injection, granting root or SYSTEM-level privileges. Post-compromise activities included installing remote access tools such as AnyDesk and ScreenConnect, creating new accounts, and setting up persistence mechanisms.

Opportunistic adversaries continue to scan for exposed, unpatched systems, with thousands of vulnerable instances still online. These campaigns mirror previous attacks on MOVEit, GoAnywhere, and Accellion, highlighting a persistent trend of exploiting widely used file transfer platforms for initial access and extortion.



Adversaries Exploiting Exposed Perimeter Devices

Throughout 2024 and 2025, adversaries actively exploited multiple vulnerabilities in perimeter-facing technologies. These include flaws in Ivanti Connect Secure VPN, Palo Alto Networks PAN-OS and Expedition, Fortinet FortiOS/FortiProxy, F5 BIG-IP, and Cisco ASA/FTD appliances. Most of these vulnerabilities allow unauthenticated, adversaries to bypass authentication, escalate privileges, or execute arbitrary code, often through exposed web interfaces or VPN services. Public Proof of Concept exploits and widespread deployment of these devices across industries make them high-value targets for ransomware groups and opportunistic adversaries.

Key examples of threats compromising exposed perimeter devices include Ivanti Connect Secure vulnerabilities (CVE-2025-0282, CVE-2025-0283), which enable remote code execution and privilege escalation, and Palo Alto PAN-OS flaws (CVE-2024-0012, CVE-2024-9474, CVE-2025-0108) that allow authentication bypass and script execution. Fortinet devices were compromised by exploitations of SSL VPN and web interface vulnerabilities (CVE-2024-21762, CVE-2024-55591), while F5 BIG-IP suffered from unauthenticated RCE (CVE-2023-46747). Cisco ASA and FTD appliances faced repeated issues, including brute-force VPN attacks (CVE-2023-20269), web services DoS (CVE-2024-20353), and information disclosure (CVE-2020-3259). Many of these flaws are actively exploited in the wild, requiring minimal skill and no user interaction.

Dragos noted a recurring trend: Java-based ecosystems (e.g., Confluence, ActiveMQ, Log4j) continue to attract adversary investment due to their widespread use and dependency chains. Vendors with complex edge appliances—such as Fortinet, F5, Zyxel, and Cisco—show repeated exposure, often requiring urgent multi-version upgrades and guidance to avoid internet-facing management interfaces. Misconfigurations and default credentials also amplify risk, as seen with Apache Superset (CVE-2023-27524) and SOHO devices such as GL.iNet routers and PCMan FTP. Exploitation windows are extremely short, with weaponization occurring within hours of disclosure, underscoring the need for same-day patching, hardening defaults, and prioritizing pre-auth RCE vulnerabilities.

Defenders should stay abreast of advisories and reports related to the exploitation of known vulnerabilities and patch systems, when feasible. These vulnerabilities highlight a persistent trend: adversaries increasingly targeting perimeter devices as initial access points for ransomware, data theft, and lateral movement into enterprise and OT networks. It is especially important to triage any compromise, identify any follow-on activity, and share lessons learned with trusted communities.

2025 Vulnerability Trends

Industrial control systems (ICS) underpin critical infrastructure, yet vulnerability management remains fragmented and unreliable. Dragos analyzes ICS-relevant vulnerabilities and uncovers systemic issues in advisories, scoring, and mitigations. Discrepancies between CISA, vendor advisories, and the National Vulnerability Database (NVD) are still common, creating delays and confusion for asset owners.

NVD analysis alone can take up to two years, leaving organizations without timely guidance and exposing them to unnecessary risk. One of the most significant findings was inconsistency in CVSS scoring. Dragos determined 15 percent of CISA and NVD CVEs had incorrect CVSS scores in 2025. Of these corrections, 64 percent were higher than originally reported, likely caused by vendors understating severity. 31 percent were lower than initially published, and the remaining 4 percent had incorrect attributes that did not affect the numeric score. These inaccuracies can lead to poor prioritization and misunderstanding of risk.

Moreover, CVSS scores often fail to reflect ICS-specific realities. For example, a system with a 'critical' vulnerability may still allow exploitation even after patching, thanks to insecure-by-design features. This is why Dragos applies its own risk-based prioritization model called 'Now, Next, Never.' Only 3 percent of analyzed vulnerabilities fell into the Now category, representing those actively exploited, remotely accessible, and often accompanied by a public POC. These pose immediate and severe risks to critical systems. Next vulnerabilities accounted for 71 percent and were typically remotely exploitable but can be mitigated through strong network hygiene practices such as segmentation and enforcing least privilege. Finally, Never vulnerabilities accounted for 27 percent of all CVEs, offering minimal risk reduction even when addressed. These "Never" vulnerabilities often come with high prerequisites to exploit, along with the attacker gaining very little 'new' access in an industrial environment. Often these "Never" vulnerabilities are only exploitable with some existing access to the ICS, which means that an attacker is not likely to need the vulnerability to achieve an industrial impact.

Dragos also identified significant gaps in remediation options, 25 percent of advisories contained no patch or mitigation advice, leaving asset owners without a clear path to reduce risk. To address this, Dragos analysts assessed vulnerable components and provided tailored mitigations for 52 percent of advisories which were initially missing the data, helping organizations maintain resilience despite vendor limitations.

Weaponization trends further complicates the threat landscape. In 2025, 4 percent of ICS-relevant vulnerabilities had a public POC and were actively exploited. The majority of these advisories earn a "Now" remediation rating, with exceptions made for exploitation in 3rd party libraries or other product types that provide neither immediate access to, nor immediate impact to, industrial operations.

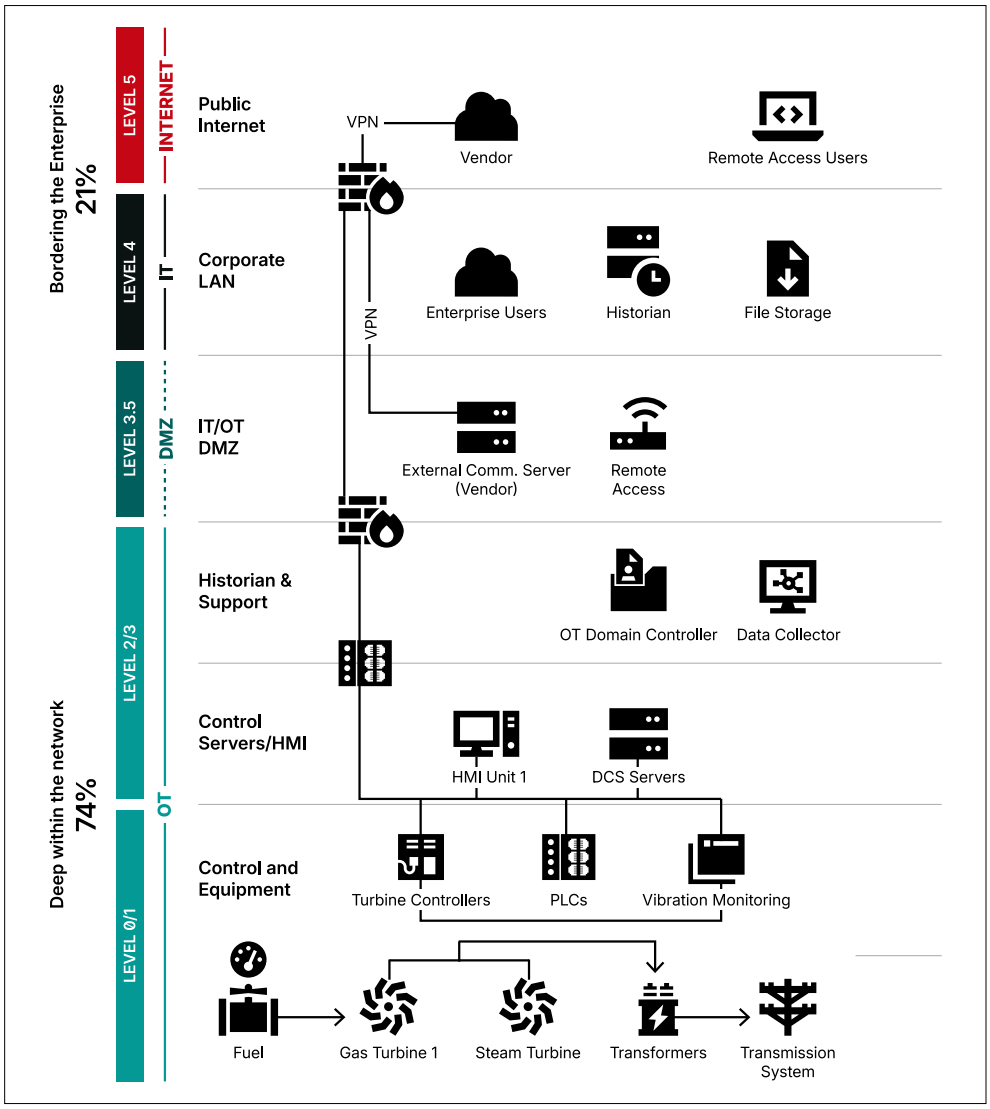
Dragos also examined asset placement within networks and found that 73 percent of advisories applied to assets that are located deep within ICS environments, close to critical processes. Only 22 percent of vulnerable assets were positioned at the enterprise boundary, where exploitation often provides adversaries with initial access to ICS networks.

Finally, Dragos assessed the operations impact of vulnerabilities on critical processes. Only 1 percent of advisories, if exploited, would affect the operator's view of the process without impacting control, and none impacted control alone. However, 27 percent affected both view and control, making them prime targets for sophisticated attacks. Fortunately, 72 percent would cause no immediate process impact, though multiple vulnerabilities could be chained to achieve disruptive outcomes.

ICS vulnerability management cannot rely solely on CVSS scores or delayed NVD analysis. Dragos addresses these gaps by applying a risk-based prioritization model, providing mitigations when patches are unavailable, and monitoring weaponization trends and asset placement risks. Asset owners should focus on vulnerabilities that truly matter to operational resilience rather than those with the highest CVSS score.

INFOGRAPHIC

Purdue Model



Vulnerability Statistics

In 2025, 15 percent of CISA and NVD CVEs had incorrect CVSS scores, which can prevent accurate prioritization for patch management and mitigation.

Of those corrections:

64%

of CVEs were **MORE SEVERE** than the public advisory

31%

were **LESS SEVERE** than reported

4%

had **incorrect attributes** that did not affect the score

These inaccuracies are often caused by vendors understating severity.

Some advisories alerted asset owners to a problem without a solution.

Of those:

25%

of public advisories contained **no patch or mitigation advice**

Dragos provided tailored mitigation advice for 52 percent of advisories that were initially missing this data, helping organizations maintain resilience despite vendor limitations.

Chart 1: CVEs with Proof of Concept

4%

of ICS-relevant vulnerabilities had a public POC and were **actively exploited** in 2025

CVSS Score Corrections (of the 15% with errors)

64%

scored **higher** after Dragos research

31%

scored **lower**

4%

had **incorrect attributes** that did not affect the score

NOW/NEXT/NEVER:

Managing vulnerabilities in OT requires risk-based prioritization.

In 2025, Dragos reported:

3%

of vulnerabilities required immediate action **("Now")** — actively exploited, remotely accessible, often with a public POC

71%

can be addressed with compensating controls or at next maintenance cycle **("Next")** — typically remotely exploitable but mitigable through network hygiene like segmentation and least privilege

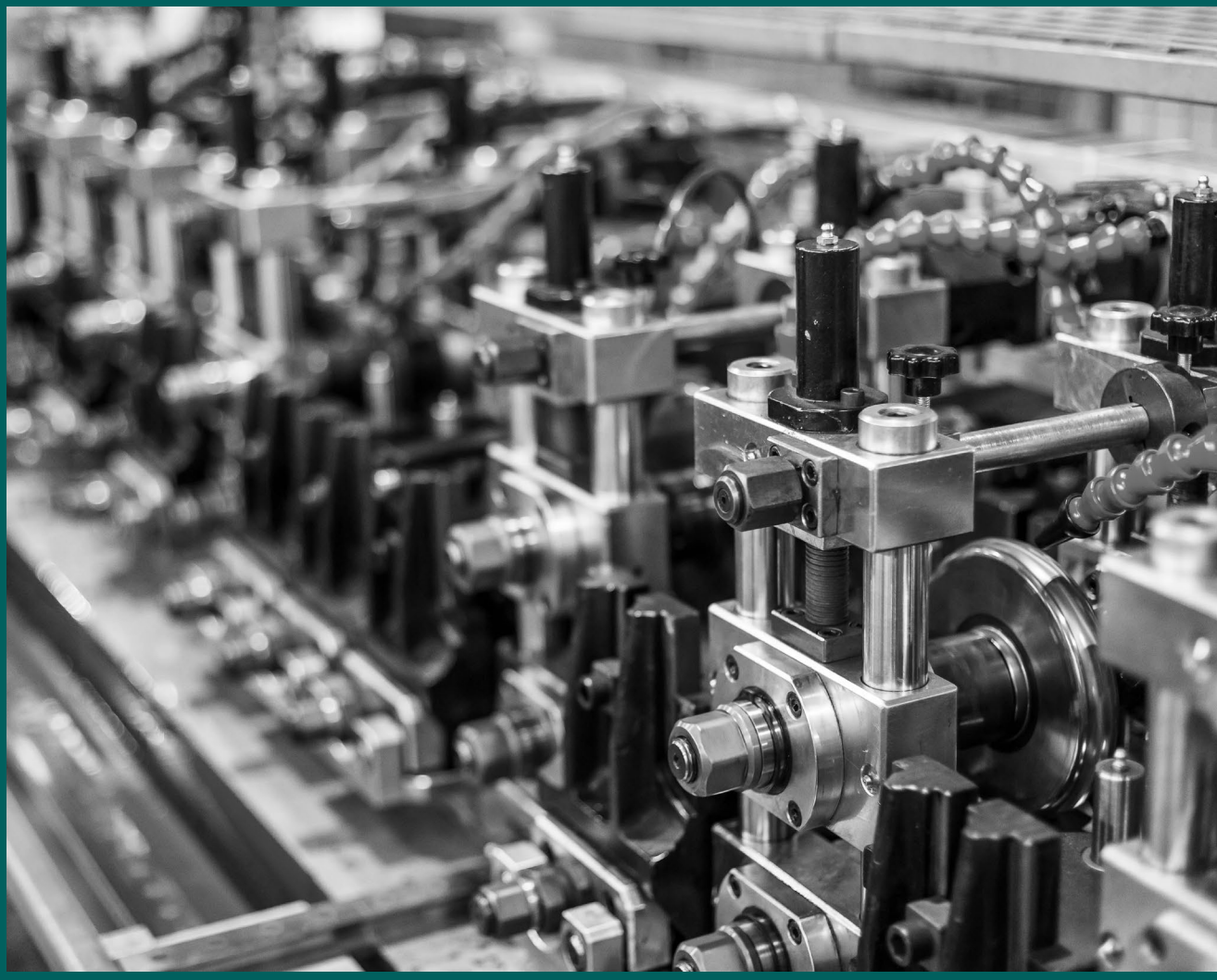
27%

don't warrant remediation efforts **("Never")** — high prerequisites to exploit with minimal risk reduction even when addressed

Insights From Dragos Intelligence Fabric

80 percent of service engagements included findings related to OT vulnerability management

Only 5 percent of reports identified EOL or unsupported assets, underscoring that EOL assets are rarely the core issue - limited visibility hinders the application of risk-based mitigations beyond patching, which is often impractical or delayed.



06.

Findings from the Field: 2025 Lessons Learned

Overview

Throughout 2025, incident response cases were consistently initiated after the identification of malware (23 percent) and ransomware (23 percent). However, unexplained operational issues (30 percent) were commonly considered cyber-related for diligence purposes. These cases were characterized by irregular events (e.g., premature value and hardware failures) that asset owners were unable to determine the root cause of, due to a lack of data collection and monitoring before the incident. The numbers are rounded out by a mixture of malicious network traffic and false positives, at 15 percent and 7 percent, respectively. While most incidents resulted in at least a one-week outage, the longest Dragos recovery effort in 2025 lasted approximately three weeks. Adversaries targeted hypervisors hosting critical OT systems, demonstrating operational efficiency by compromising shared infrastructure rather than individual assets. These attacks primarily exploited weak credentials associated with privileged accounts.

Call to Action

The activity observed throughout the last few years reinforces a clear and urgent reality: Adversaries continue to gain access to OT/ICS networks through exposed public-facing systems, rapid exploitation of newly disclosed vulnerabilities, and insecure default configurations. Persistent visibility gaps prevent organizations from detecting this activity once access is established, particularly after adversaries pivot to OT/ICS networks. Incomplete asset inventory, limited telemetry, and a lack of ICS-aware monitoring allow adversaries to conduct reconnaissance, establish persistence, and abuse native protocols without detection, with awareness frequently occurring only after operational or business impact.

In 2026, defenders should anticipate continued exploitation of high-value, internet-exposed technologies and ICS-adjacent platforms. While reducing external attack surfaces and hardening management interfaces remain necessary, these measures alone do not address the core challenge of safeguarding critical infrastructure. Organizations must prioritize gaining visibility into OT/ICS environments by establishing accurate asset inventories, collecting relevant telemetry, and deploying ICS-aware detection capabilities. Continuous monitoring and evaluation of the effectiveness of deployed security controls, including isolation and boundary devices, coupled with timely intelligence sharing within trusted communities, remains critical to exposing adversary behavior before operational or business impact occurs.

The following insights and statistics are grouped by relevance to the SANS ICS 5 Critical Controls and industry breakouts have been provided where analysts have assessed with medium to high confidence, and industry breakouts are provided where analysts have assessed with medium to high confidence that the sample size is representative of the industry.

Critical Control 01: OT/ICS Incident Response

IR Cases

A common theme among confirmed OT incidents with a cyber dimension was the presence of weaknesses in remote access, monitoring, human behaviour, and the overall security posture. The incidents observed by Dragos this year revealed a trend toward operational disruption, forced environment rebuilds due to ransomware, and persistent gaps in OT security practices. Malware and ransomware led the charge, comprising the majority of incidents responded to by Dragos. The average dwell time between incidents was 5.4 days across these incidents. In addition to malware (23 percent) and ransomware (23 percent), the third most common incident responded to involved operational issues. Examples included unexplained incidents, treated as cyber-related for diligence purposes, such as irregular values and hardware failure (30 percent). The numbers are rounded out by a mixture of malicious network traffic and false positives, at 15 percent and 7 percent, respectively.

Incident Response Plans

Asset owners and operators must develop and maintain an OT/ICS-specific Incident Response Plan (IRP) addressing the unique requirements and risks of their OT/ICS environments. This plan should consider how these industrial systems operate and how best to respond to likely OT/ICS events. In 2025, 10 percent of Dragos services reports included a finding related to deficiencies in organizational IRPs and 6 percent cited the complete absence of an OT/ICS IRP. This figure rises sharply to 24 percent within the Manufacturing sector, indicating a higher prevalence of foundational IRP gaps in that industry.

For asset owners that have established OT/ICS-specific incident response procedures, Dragos recommends customers operationalize and exercise those plans and technical provisions. Tabletop exercises (TTXs) are one of the most effective methods for validating incident response plans, as they allow organizations to assess roles, decision-making, communication, and procedural gaps in a low-risk, controlled environment. Exercises provide incident responders with a low-stress educational opportunity to identify gaps and improvements in core IR capabilities. TTXs also provide a means of socializing content and raising awareness of OT/ICS cybersecurity among plant personnel.

- DETECT: The process of identifying and categorizing anomalous activity or events in a timely manner and understanding their potential impact.
- COMMUNICATE: Distributing information to and corresponding with people and organizations during a disruptive event.
- ACTIVATE: The process of activating an information system-focused Incident Response Plan (IRP) that may assemble the [CSIRT, SIRT, IRT, IMT], depending on the extent of an event.
- RESPOND: The process of executing response processes, technical capabilities, and procedures upon notification of a qualifying event.
- CONTAIN: The activities performed to prevent the expansion of an event and mitigate its effects.
- DOCUMENT: The process of documenting and cataloguing event information, decisions, and evidence.
- RECOVER: The process of restoring systems to a normal operational state following a cybersecurity incident or event.

The Dragos engagement team scores these capabilities based upon the following ratings:

- COULD PERFORM WITHOUT CHALLENGE (P): The target associated with the core capability could be completed in a manner according to the published IRP and did not negatively impact the performance of other activities. The performance of this activity did not increase the risk associated with the incident.
- COULD PERFORM WITH SOME CHALLENGES (S): The target associated with the core capability could be completed in a manner according to the published IRP and did not negatively impact the performance of other activities. The performance of this activity did not increase the risks associated with the incident. However, opportunities to enhance effectiveness and/or efficiency were identified.
- COULD PERFORM WITH MAJOR CHALLENGES (M): The target associated with the core capability was completed in a manner that achieved the objective(s), but some or all of the following were observed: demonstrated actions in accordance with the published IRP had a negative impact on the performance of other activities and contributed to additional risks associated with the incident.
- LIKELY UNABLE TO PERFORM (U): The target associated with the core capability could not or would not be performed according to the published IRP.

2025 TTX Scores – Industry Breakdown

Core Capability	Average All Industries	Average Oil & Gas	Average Manufacturing	Average Electric
Activate	Some Challenges	Some Challenges	Some Challenges	No Challenges
Detect	Some Challenges	Some Challenges	Major Challenges	Major Challenges
Respond	Some Challenges	Some Challenges	Some Challenges	Some Challenges
Communicate	Some Challenges	Major Challenges	Major Challenges	Some Challenges
Recover	Some Challenges	Some Challenges	Some Challenges	No Challenges
Contain	Some Challenges	Major Challenges	Major Challenges	Some Challenges
Document	Some Challenges	Major Challenges	Major Challenges	Some Challenges

The table above highlights several notable challenges identified through tabletop exercises. A significant majority of organizations reported difficulties with detection (88 percent), containment (94 percent), and incident response plan (IRP) activation (82 percent), underscoring persistent gaps in operational readiness. Dragos consistently observed that 82 percent of asset owners lacked clear criteria for determining when operational anomalies should trigger cybersecurity investigations. TTXs for OT environments differ from IT-focused exercises, as initial indicators are often observed within industrial processes and operations, where they may be misinterpreted as routine operational anomalies rather than cybersecurity events. In some cases, OT/ICS personnel lacked the foundational skills needed to conduct basic cybersecurity investigations, such as log review and network traffic analysis, which support early identification of cybersecurity issues. Integrating these activities into existing troubleshooting processes enables more efficient triage before engaging cybersecurity specialists.

Critical Control 02: Defensible Architecture

Dragos considers an architecture defensible when it is purpose-built to reduce OT/ICS risks through system design and implementation. In 2025, 42 percent included at least one major finding related to Control #2, Defensible Architecture, with the highest prevalence in manufacturing at 27 percent, followed by oil and gas at 20 percent and electric at 19 percent.

Network Segmentation

Poor IT and OT segmentation remains the most common architectural weakness, appearing in 81 percent of reports, with representation across all sectors, including 29 percent in oil and gas, 24 percent in manufacturing, and 22 percent in electric.

Common misconfigurations or lack of best practices include:

- Lack of egress control - a network enforces inbound access control but no outbound access control
- Insecure remote access - direct connectivity is permitted from untrusted to trusted network zones
- Overly-permissive rules - a rule permits a large number of source IP, and/or destination IP, and/or services
- Insecure service - a rule permits legacy services that are known for being insecure (e.g., Telnet)
- Rule shadowing - One rule has the same (or larger) scope than a second rule with a same or different action
- Rule correlation - two rules with same or different actions have an overlapping scope but not entirely
- Rule redundancy - two rules with the same action have any amount of overlap
- Rule irrelevance - a rule that affects packets that cannot possibly reach that firewall
- Rule generalization - a rule with a scope that is entirely covered by a second rule with a same or different action

Dragos observed significant third-party and downstream risk in OT/ICS environments from service providers and managed security partners that introduced ingress points into victim networks. The risk was further compounded through weak security practices such as poor password hygiene, storing critical credentials in human-readable formats, and unnecessarily exposing remote access. In these cases, flat network architectures allowed malware and ransomware to move laterally with minimal resistance. These incidents proved disruptive because of longstanding architectural weaknesses that left few effective barriers once adversaries gained access.

Findings related to shared IT and OT domains were identified in 12 percent of reports overall, but were most heavily concentrated in manufacturing at 46 percent, compared to 14 percent in oil and gas and 12 percent in electric.

Shared IT/OT domains create unnecessary pathways between enterprise IT networks and operational technology (OT) environments. This weakens the security posture of OT environments because a compromise in the IT network can more easily propagate into OT systems, potentially disrupting critical industrial processes and bypassing traditional network segmentation controls designed to protect safety and reliability.

Default or Weak Credentials

The use of default or vendor-supplied credentials was once prevalent in OT/ICS environments. These credentials are widely known and easily exploited, giving attackers a low-effort path to unauthorized access and potential control of critical systems. By 2025, default credentials appeared in only 3 percent of reports overall, but they remained more common in certain sectors, particularly electric at 35 percent and oil and gas at 26 percent, highlighting persistent gaps in basic security hygiene.

In 2025, Adversaries capitalized on these weaknesses by deploying ransomware variants such as Fog and Greenlux, which leveraged weak credentials and limited network segmentation to gain a foothold in OT environments. In several incidents, attackers compromised hypervisors supporting critical OT systems and encrypted servers and virtual disks. The widespread adoption of virtualization increased attacker efficiency by enabling lateral movement, stealthy persistence, and scalable ransomware operations.

Endpoint Protection

Traditional antivirus (AV) and endpoint detection and response (EDR) solutions are less common in OT environments due to concerns about system stability and compatibility with legacy equipment. When present, they are often outdated and configured with extensive whitelisting of directories and network shares to avoid disrupting critical operations, a condition that is commonly exploited by both red teams and adversaries to store malicious files without detection.

These limitations are reflected in 2025 services data, where 19 percent of all reports cited gaps in endpoint security or malware protection within OT/ICS network segments, most frequently in oil and gas at 37 percent, followed by electric at 25 percent and manufacturing at 11 percent.

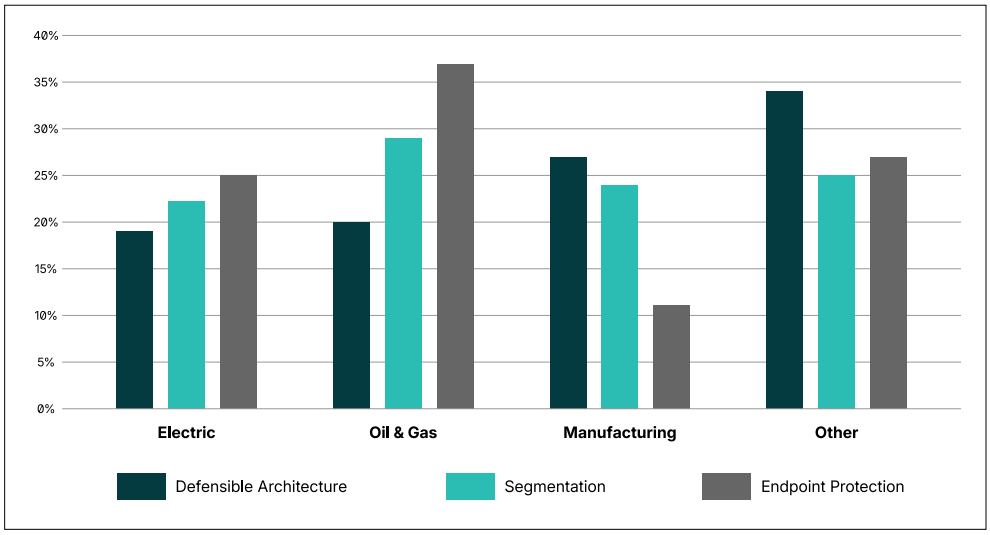
In practice, AV and EDR tools deployed in OT/ICS environments rely primarily on signature-based detection, with little contextual awareness of OT systems or ICS-specific malware. As a result, they provide limited visibility and are most effective at detecting commodity, IT-centric malware rather than stage 2 adversary activities targeting industrial operations.

This gap is further illustrated in incident response data, where 13 percent of 2025 Dragos IR cases involved headless malware that operates without a user interface or visible processes, allowing it to execute silently and evade traditional signature-based detection mechanisms that rely on visible artifacts or user interaction.

An effective approach combines careful AV/EDR deployment with network monitoring and asset visibility to detect threats without disrupting critical operations. When deployed, they provide visibility into malicious activity and help detect known threats, but they often struggle to identify novel or targeted attacks specific to industrial systems. Dragos recommends deploying up-to-date EDR/AV on jump servers and systems within the OT DMZ to protect critical access points without impacting operational systems and leveraging an ICS-aware networking monitoring solution for detecting stage 2 attacks.

Defensible Architecture Findings by Industry Sector and Category

Distribution of defensible architecture, network segmentation, and endpoint protection findings across Electric, Oil & Gas, Manufacturing, and other sectors from 2025 Dragos Services engagements.



Critical Control 03: ICS Network Visibility & Monitoring

Across incident response, penetration testing, and consulting engagements, persistent visibility gaps were observed, with environments routinely lacking the telemetry needed to conduct root-cause analysis or detect malicious activity. Visibility forms the foundation of robust cybersecurity programs and enables the development of metrics that drive maturity and resilience. Achieving meaningful visibility requires centralized collection and correlation of network and device logs, network traffic analysis, and accurate asset inventories across IT and OT network segments.

In practice, visibility is often limited to narrow monitoring scopes, such as observing only the IT to OT boundary or failing to inspect ICS-specific protocols. These constraints prevent defenders from developing an accurate understanding of critical network activity and adversary behavior once access is established.

Despite its importance, 2025 assessments continue to reveal persistent visibility gaps, with Architecture Reviews identifying substantial deficiencies in OT and ICS visibility and monitoring across 46 percent of assessments, particularly in oil and gas, electric, and manufacturing environments. Dragos Network Penetration Tests revealed similar detection gaps, with 56 percent demonstrating an inability to identify adversary activity that leveraged native administrative tools. In these cases, red teamers abused legitimate system utilities such as PowerShell, cmd.exe, WMI, RDP, and SSH to operate without triggering alerts.

This lack of detection capability is reinforced by control implementation data, as fewer than 5 percent of tested environments had PowerShell execution logging enabled, despite its role as a foundational control for exposing this class of stealthy activity.

In OT/ICS environments, the abuse of ICS-native protocols is functionally equivalent to IT-centric living-off-the-land techniques. This activity typically requires no custom malware, appears operationally legitimate, blends into normal control communications, and frequently evades traditional security tools that lack ICS protocol awareness and context. As a result, the use of insecure protocols without compensating controls consistently ranks among the top findings in Dragos Services engagements. The impact of this protocol abuse extends beyond data exposure to include the misoperation of industrial equipment, as demonstrated in multiple historic OT cyber incidents.

These visibility gaps were also observed in 88 percent of tabletop exercises. Deficient detection capabilities in emulated incident response scenarios indicate that meaningful operational or business impact would likely occur before detection in real-world incidents, leading to longer and more costly response efforts. Collectively, these results reinforce the critical need for comprehensive visibility, advanced detection capabilities, and continuous evaluation to strengthen OT cybersecurity posture.

Critical Control 04: Secure Remote Access

Secure remote access, in this context, refers to a controlled and monitored method for connecting OT networks to business IT networks or external locations. Dragos recommends implementing multi-factor authentication (MFA), jump hosts, VPNs, and other verification mechanisms to minimize the risk of unauthorized access by effectively limiting, managing, and monitoring interactive connections to OT/ICS networks. These practices help ensure both business continuity and operational flexibility.

In 2025, service data continued to underscore MFA as the single most effective control for remote access, with fewer than 5 percent of reports identifying environments without any MFA implementation, even if not consistently enforced across all access paths. However, MFA represents only one component of a comprehensive remote access strategy.

Broader weaknesses in remote access controls remain prevalent, as 49 percent of services reports included elevated findings related to Control #4, Secure Remote Access. These issues most frequently affected manufacturing at 28 percent, followed by oil and gas at 25 percent and the electric sector at 17 percent.

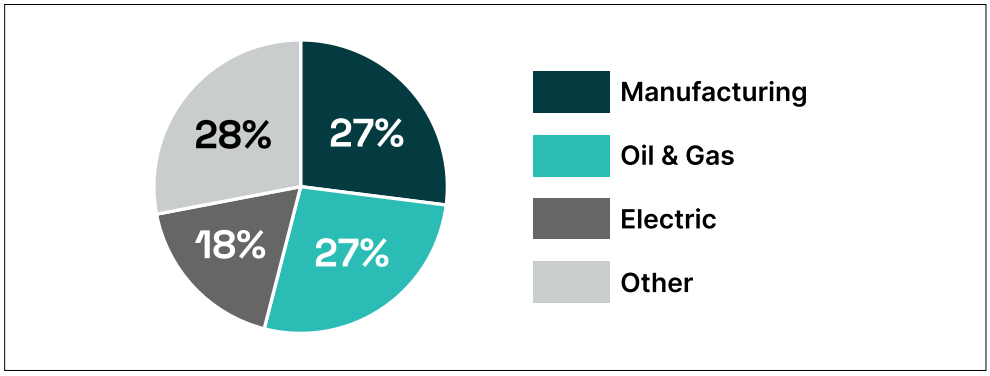
Findings in this category commonly involved insecure configurations of RDP, VNC, and remote administration utilities. In this context, remote access refers to lateral or internal network access and does not necessarily imply direct internet exposure.

Nevertheless, exposure to public networks remains a significant risk. Over half of all services reports, 53 percent, identified public or internet-facing systems associated with the same control, impacting 27 percent of oil and gas, 27 percent of manufacturing, and 18 percent of electric environments. These conditions continue to present exploitable pathways, as demonstrated by hacktivist groups such as CyberAv3ngers, which have successfully compromised devices in this category.

Two primary categories of incidents dominated this year: ransomware and commodity malware. Although their root causes differed, the outcomes were similar, namely process disruption and costly OT/ICS environment rebuilds. These attacks exploited well-known weaknesses, including shared credentials, lack of MFA, poor credential storage, and exposed management interfaces. Each of these gaps directly relates to deficiencies in secure remote access and network segmentation; two controls that, when neglected, enable adversaries to gain and maintain access.

Secure Remote Access Findings by Industry Sector

Industry breakdown of elevated secure remote access findings from 2025 Dragos Services engagements, with Manufacturing and Oil & Gas each accounting for the largest share.

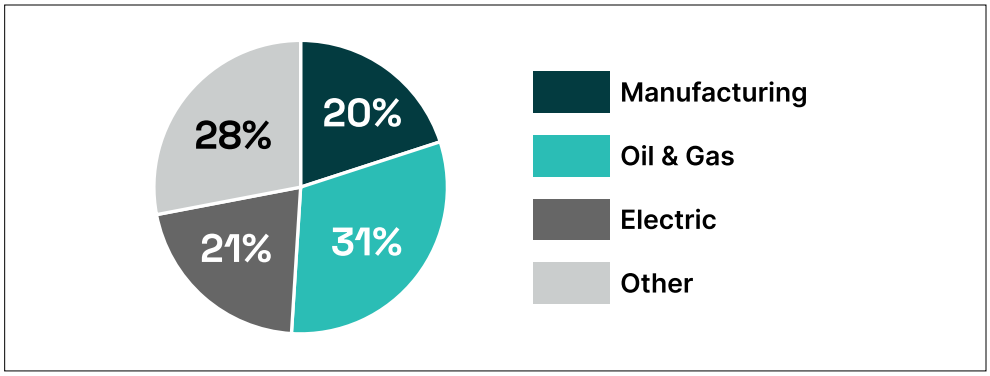


Critical Control 05: Risk-based Vulnerability Management

OT/ICS environments face unique challenges for vulnerability management. Legacy and unsupported systems make patching difficult without risking operational disruptions or safety incidents. Limited visibility, proprietary protocols, and strict change management further complicate the identification and remediation of vulnerabilities. High availability requirements, evolving threats, and regulatory pressures force organizations to balance security improvements with continuous operation. In 2025, 80 percent of reports included a finding related to control #5, Vulnerability Management, affecting 31 percent of oil and gas, 20 percent of manufacturing, and 21 percent of electric environments. Interestingly, findings related to end-of-life or unsupported operating systems and applications were highlighted in less than 5 percent of reports. These numbers reflect a common misconception that OT/ICS systems cannot be updated. While patching serves as the primary vulnerability mitigation mechanism in IT environments, OT systems operate under fundamentally different constraints. System interdependencies, safety requirements, and vendor qualification processes often make patching infrequent or impractical, making alternative mitigations the norm. As a result, organizations struggle less with unsupported systems and more with accurately identifying vulnerabilities and implementing effective compensating controls across OT environments, driven by persistent visibility gaps, including incomplete asset inventories and limited insight into system communications. Applying a risk-based approach enables timely patching and mitigation without disrupting operations. For more details on specific OT/ICS vulnerabilities and trends, refer to the Vulnerabilities section of this report.

Vulnerability Management Findings by Industry Sector

Industry breakdown of vulnerability management findings from 2025 Dragos Services engagements, with Oil & Gas representing the largest share at 31 percent.



07.

Call to Action

The activity observed throughout 2025 reinforces an urgent reality: adversaries are already targeting infrastructure as it evolves. ELECTRUM's focus on distributed energy resources in Poland and the security gaps identified in battery energy storage systems demonstrate that new infrastructure is being deployed faster than security can keep pace. Looking ahead, organizations face compounding complexity as AI technologies move into operational environments. Organizations that cannot monitor today's OT networks will find that AI adoption creates exponentially greater blind spots, making root cause analysis and incident response increasingly difficult. Establishing comprehensive OT visibility now, before AI and renewable energy adoption further accelerate, is critical for maintaining operational resilience.

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