8TH ANNUAL
YEAR IN REVIEW
2025

OT/ICS CYBERSECURITY REPORT

CONTENTS

Introduction

Throughout the year, Dragos identifies threats to operational technology (OT) and industrial control systems (ICS) infrastructure, conducts services to help defenders mature their program, and prioritizes mitigations for resilient operations. Enhanced by Dragos telemetry, we approach our eighth annual Year in Review report with field-tested guidance. It serves to provide several detailed examples of key attack paths Dragos observed as well as some of the context and motivation behind these attacks.

If this is the beginning of your OT/ICS cybersecurity journey, welcome and don't be alarmed. Start your year off by systematically identifying your organization's exposure and work to reduce that exposure as much as possible. Read more about threats to exposed assets such as BAUXITE on page 22 and KurtLar SCADA on page 35.

If you already know your exposure, or have a plan to reduce it, consider the attack scenarios mentioned throughout this report and decide whether you'd be susceptible to these same attacks. Use these scenarios to inform visibility and monitoring strategies, create your incident response plans, and plan segmentation efforts.

If you have a good threat prevention strategy, it's time to test it. Consider the attack scenarios mentioned throughout this report and identify visibility gaps. Would you notice if an adversary downgraded your firmware? Read more on FrostyGoop malware and associated attack chain on page 29.

If vulnerability management seems overwhelming, read how OT vulnerability management is different than IT in the Vulnerability Trends section on page 55. Learn how to prioritize mitigation and remediation of vulnerabilities with the "Now, Next, Never" framework on page 54.

Buckle in and get ready to hunt. Hacktivists tell you who they are, but we continually observe adversaries hiding amongst the noise. Read more about ELECTRUM's AcidPour on page 13 and VOLTZITE on page 14.

No matter your cybersecurity maturity, read on. From ICS threat groups and hacktivists to ICS malware attacks and criminal ransomware, you will learn about the latest real-world attacks, and what you can do about them. Combined with insights from our incident responders and guidance from our vulnerability team, this report provides a comprehensive look at the most important cyber threats affecting OT environments and organizations.

KEY HIGHLIGHTS: BY THE NUMBERS

Dragos tracks 23 THREAT GROUPS, 9 of which were active in 2024.

ICS Cyber Kill Chain Stage 2 Capability

Key Vulnerabilities Findings

70%

of vulnerabilities **reside deep within the network.**

22%

of advisories were **network exploitable and perimeter facing** in 2024.

39%

of the advisories that Dragos analyzed **could cause both a loss of view and loss of control,** down from 53 percent in the previous year.

22%

of advisories **had incorrect data** in 2024.

47%

Dragos provided mitigations for 47 percent of the advisories that had none.

Key Ransomware Findings

87%

Ransomware attacks against industrial organizations **increased 87 percent** over the previous year.

60%

Dragos tracked **60 percent more ransomware groups** impacting OT/ICS in 2024.

69%

of all ransomware attacks targeted **1,171 manufacturing entities** in **26 unique manufacturing subsectors**.

OT Protocols Used

Modbus | FINS | Meter-bus
CIP | OPS/UA | S7comm
CODESYS

IT Protocols Used

SSH | RDP | VNC
HTTP | HTTPS | PPTP
IMAP | WebDAV (over HTTPS)

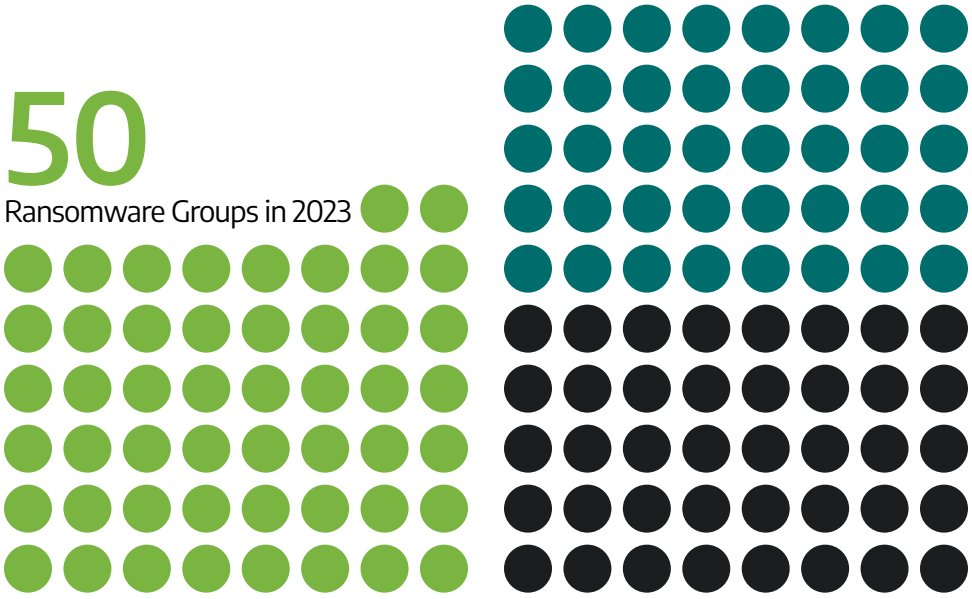
Industries Targeted

- Electric
- Oil & Gas
- Defense Industrial Base
- Manufacturing
- Telecommunications
- Maritime
- Water & Wastewater
- Food & Beverage
- Chemical Manufacturing
- Mining
- Transportation & Logistics

Ransomware Groups

80
Ransomware Groups in 2024

50
Ransomware Groups in 2023



50%
target
Manufacturing

Defender's Guide to the Current Threat Landscape

The cybersecurity threat landscape in 2024 was shaped by escalating geopolitical tensions and their intersection with industrial operations globally. From persistent campaigns by mature threat groups to opportunistic attacks by hacktivists or ransomware operators, adversaries demonstrated a growing awareness of OT/ICS environments as potential attack vectors to achieve their goals. This year highlighted the increasingly complex threat landscape and the corresponding escalating pressure on defenders to enhance visibility into and resilience of OT/ICS networks.

Adversaries Targeting OT: Awareness Over Sophistication

A striking trend in 2024 was the continued lowering of the barrier to entry for adversaries targeting OT/ICS. Adversaries that would have once been unaware of or ignored OT/ICS entirely now view it as an effective attack vector to achieve disruption and attention. For example, Blackjack's Fuxnet malware, revealed in April 2024, though rudimentary compared to more sophisticated ICS-capable malware like PIPEDREAM, signaled a growing awareness of the impact that disruptive attacks on OT networks can have. Similarly, the hacktivist persona CyberArmyofRussia_Reborn's (CARR) campaigns targeting internet-exposed OT devices through much of 2024 demonstrated that even basic techniques, such as manipulating internet-exposed human-machine interface (HMI) settings remotely, could result in tangible disruptions.[1]

This shift is not indicative of a deeper technical understanding of OT but reflects a more widespread recognition of its utility in achieving adversary goals. For ransomware operators, this has meant targeting manufacturing environments where downtime directly pressures victims to pay ransom. For hacktivists, targeting OT offers a fast and disruptive way to amplify their messages. These attacks reinforce a crucial reality: sophistication is not always necessary to achieve impactful outcomes, and the proliferation of adversaries amplifies the overall risk.

This focus on simplicity highlights a critical point for defenders: effective implementation of the SANS ICS 5 Critical Controls[2] remains the best defense against OT-targeting adversaries. Organizations with strong incident response capabilities, defensible architectures, secure remote access protocols, and robust network monitoring are far better positioned to reduce the risk of a successful attack on the enterprise OT even in this increasingly complex environment.

Defender Progress: Incremental But Uneven

Defenders have made progress in understanding the importance of securing OT environments, but this progress remains uneven across sectors and regions. Regulated industries, such as electric power in North America, demonstrate higher maturity levels than less regulated sectors, such as water utilities or manufacturing. Initiatives like the Dragos Community Defense Program (CDP) contribute to increased awareness, but visibility into OT environments lags behind adversary tactics in many cases.[3]

Highlighting uneven progress, many organizations implement secure remote access but lack the internal

[1]Hackers Linked to Russia's Military Claim Credit for Sabotaging U.S. Water Utilities - Wired; [2]5 Critical Controls for World-Class OT Cybersecurity; [3] Dragos Community Defense Program – Dragos, Inc.

network monitoring and visibility to find third-party and legacy connections that leave their networks open to compromise. In one case, the Dragos team identified a legacy vendor connection inside an organization's OT network weeks before a ransomware group compromised the vendor. Removing the legacy connection prevented the organization from harmful exposure to the vendor's compromised network. Whether it is OT virtual private networks (VPN) with direct access to the internet or demilitarized zones (DMZs) with insecure configurations, Dragos Services engagements routinely observe organizations that lack visibility and monitoring to identify ad hoc additions to their environment.

While a lack of visibility prevents organizations from understanding attack vectors inside their network, it is the root of why organizations fail to understand their external attack surface, leaving them vulnerable to opportunistic adversaries relying on tools like Shodan and Censys to discover exposed devices. Internet-exposed ICS devices were among the most exploited vectors for OT-targeting attacks in 2024. The harmful assumption that "we won't be targeted" remains a significant hurdle for defenders, particularly in organizations with limited resources or competing priorities.

2024 demonstrated that OT is no longer a niche target. The proliferation of adversaries—enabled by greater awareness and understanding of OT and the effectiveness of basic attack techniques — has made defending critical infrastructure more challenging than ever. Skilled adversaries remain hidden within critical infrastructure while hacktivists exploit exposed weak infrastructure. Both are enabled by an environment where a majority of the community is not yet aware of the specific threat to OT differentiated from IT, or worse, is informed but knowingly chooses to ignore or downplay its veracity. Doing the basics continues to be the prime directive for most of the community. Now more than ever, defenders who can uncover and illuminate hidden threats are stepping up to hunt.

SERVICES DATA ANALYSIS: Dragos conducts on-site visits at various industrial sites to assess security gaps and provide actionable recommendations through architecture reviews, penetration tests, tabletop exercises, and more. In 2022, Dragos revamped the collection and analysis of data from these on-site engagements to better present the state of industrial cybersecurity with more accurate MITRE ATT&CK for ICS tagging, industry delineation, and deeper analysis of security findings. These firsthand field observations are used to communicate trends in industrial cybersecurity, provide industry specific insights, and share key issues to address in efforts to enhance security.

OT-Centric Cyber Operations Increase as Geopolitical Tension and Conflicts Continue

A cyber attack on a municipal energy company disrupted heat to hundreds of apartment buildings in Ukraine.[4] A purported attack by Ukraine-aligned Blackjack group damaged critical infrastructure monitoring devices in Russia.[5] The pro-Iranian CyberAv3ngers attacked fuel management systems in Israel.[6] In 2024, Dragos witnessed continued offensive cyber activities linked to ongoing geopolitical conflicts. Threat groups, including hacktivists, shifted to more overt cyber operations aligned to the goals of their respective side, and the more mature groups sought to cause disruptive effects.

The Ukraine-Russian Conflict Fuels Activity for Established Dragos Threat Groups

KAMACITE and **ELECTRUM** continue to collaborate in support of Russian military objectives by targeting critical infrastructure in Ukraine. KAMACITE establishes a foothold into victim IT networks and hands control to ELECTRUM for OT operations, such as the 2016 CRASHOVERRIDE attack, which temporarily cut power to part of Kyiv.[7]

In 2024, KAMACITE used the Kapeka backdoor targeting Ukrainian critical infrastructure entities supplying heat, water, and electricity. Meanwhile, ELECTRUM collaborated with hacktivist groups to obscure its cyber attack against Kyivstar, a Ukrainian telecommunications company.

This new KAMACITE and ELECTRUM activity illustrates the accelerating effects of the Ukraine-Russia conflict on the development of OT-related cyber attack techniques.

[4] Impact of FrostyGoop ICS Malware on Connected OT Systems - Dragos Inc.; [5] Strategic Overview of the Fuxnet Malware - Dragos Inc.; [6] Iran-linked crew used custom 'cyberweapon' in U.S. critical infrastructure attacks – The Register; [7] CRASHOVERRIDE: Analyzing the Malware that Attacks Power Grids – Dragos, Inc.

KAMACITE Technical Update

Tracking KAMACITE is important because they hand off their access to OT disruption teams, like ELECTRUM, which has technical overlaps with Sandworm, tracked by other organizations.[8]

Since 2015, KAMACITE conducted at least three disruptive campaigns targeting electric infrastructure in Ukraine, deploying GreyEnergy and BlackEnergy, as well as developing and using VPNFilter and CyclopsBlink botnets. In 2024, KAMACITE introduced new, custom Windows-based malware strains and expanded its focus to European oil and natural gas (ONG) entities.

KAMACITE targets organizations in Ukraine, Eastern and Central Europe in the following verticals:

- **Oil & Natural Gas**
- **Electric**
- **Defense Industrial Base**
- **Manufacturing**

Given KAMACITE's role as an initial access provider and their consistent use of phishing, Dragos urges organizations to conduct regular user education to identify phishing attempts. Additionally, proper segmentation between enterprise IT and OT/ICS is critical in preventing a KAMACITE compromise from escalating to a disruptive event. Finally, visibility into north-south traffic in ICS environments is important. Defenders should monitor for suspicious activity, such as terminated connections between control centers or abnormal polling of substations to toggle breaker statuses.

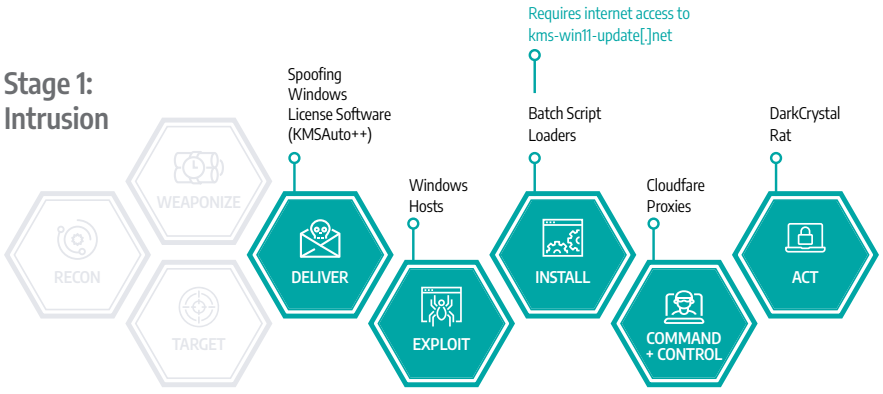
KAMACITE Campaigns

Kapeka Campaign (2022-2023)

Discovered in 2024, KAMACITE used Kapeka in a campaign targeting multiple Ukrainian critical infrastructure operators beginning in March 2023.[9, 10] Kapeka has technical overlaps with GreyEnergy, and analysis reflects ongoing development efforts within KAMACITE's toolset. The number of discovered Kapeka samples is low, suggesting this malware has been used in low-volume, likely targeted attacks since at least mid-2022.

DarkCrystal RAT (2022-2024)

KAMACITE continues to use criminally sourced, commodity malware in spear-phishing campaigns targeting Ukrainian entities. DarkCrystal RAT (DCRat) was used for surveillance and information theft.

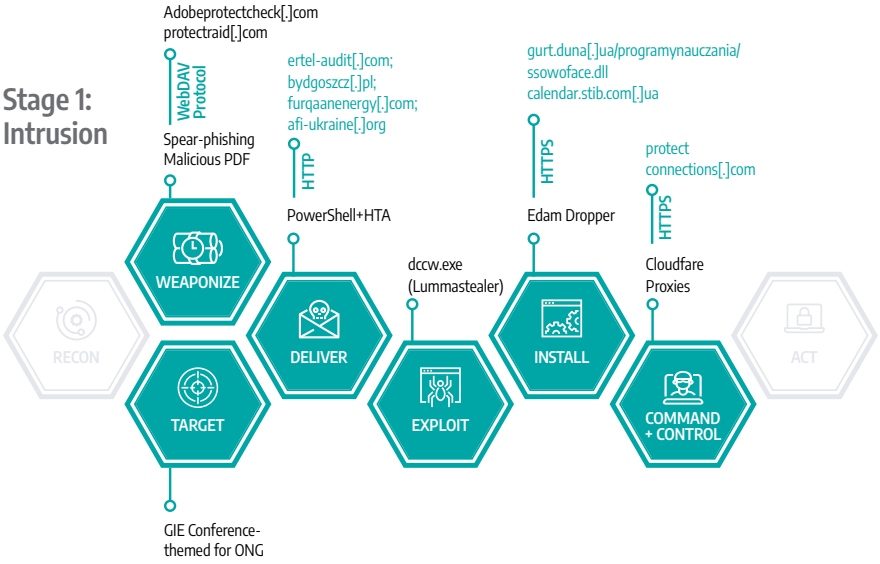


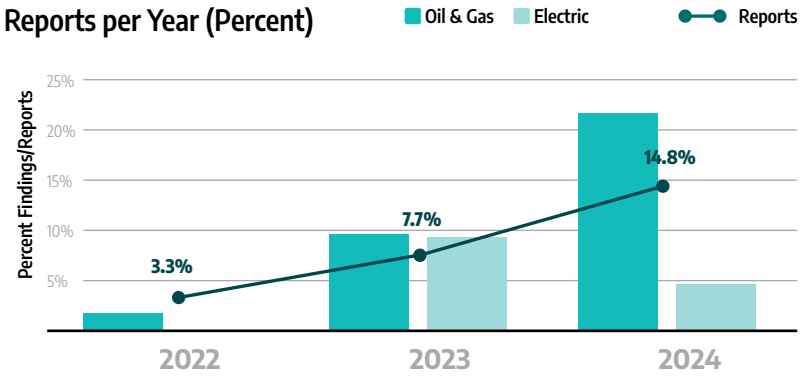
[8]Sandworm Team - MITRE; [9]WithSecure uncovers Kapeka, a new malware with links to Russian nation-state threat group Sandworm - WithSecure; [10]UAC-0133 (Sandworm) plans for cyber sabotage on nearly 20 critical infrastructure facilities in Ukraine – CERT-UA (Machine Translated)

LummaStealer and GIE Conference Campaign (2024)

KAMACITE used LummaStealer and employed a commodity loader service, now tracked by Dragos as TAT24-97.[11, 12] These capabilities are primarily delivered via spear phishing, using domains that resemble prominent technology provider names.

KAMACITE targeted European ONG organizations, using the 2024 Gas Infrastructure Europe (GIE) conference hosted in Germany as a spear-phishing theme. The campaign relied on a relatively complex infection chain, leading to the deployment of another custom-developed Windows backdoor named "Edam." This was a notable shift from an exclusive focus on Ukraine to broader European targets. This coincided with the expiration of an agreement allowing Russian state-owned company Gazprom to supply gas to Eastern and Central Europe.





Percent of service engagements, by vertical, that had insecure PowerShell configurations similar to ones exploited in KAMACITE's Edam attack.

As more PowerShell related tactics, techniques, and procedures (TTPs) are attributed to tracked threat groups like KAMACITE, Dragos is increasingly critical of related security configurations. Enabling PowerShell logging to support incident response, and enabling AMSI to block malicious scripts are the most common PowerShell related recommendations from Dragos security assessments.

Hunt for WebDAV Communication to the Internet

WebDAV is a protocol that runs on top of HTTP and may be observed for syncing files across a network; if you see this communication between unexpected assets, such as to the internet, dig in.

[11]PEAKLIGHT: Decoding the Stealthy Memory-Only Malware - Google; [12]WebDAV-as-a-Service: Uncovering the Infrastructure behind Emmenhtal loader distribution - Sekoia

ELECTRUM Technical Update

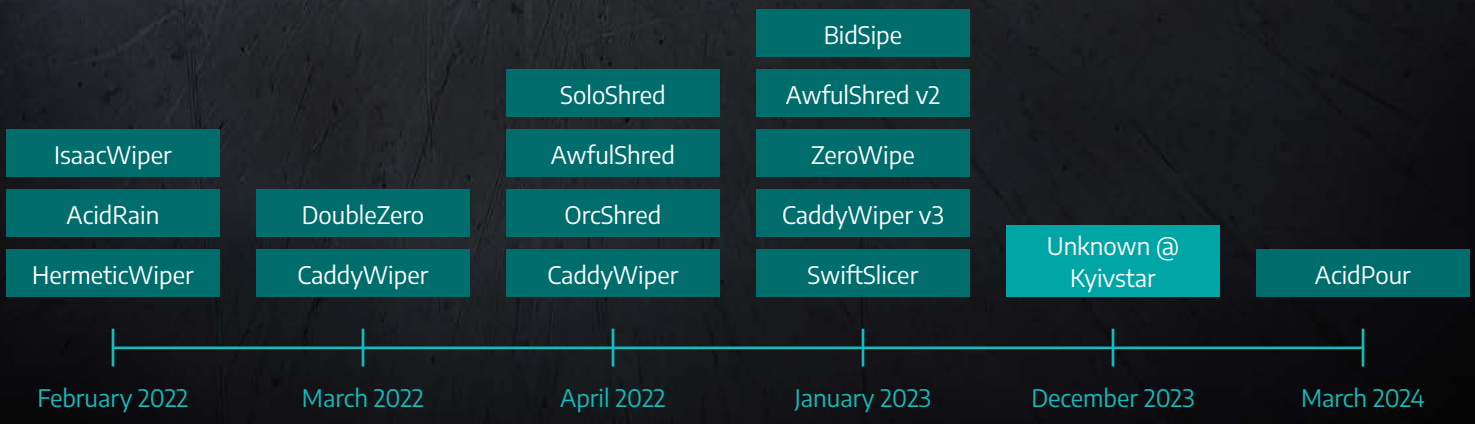
One of Dragos's oldest threat groups, ELECTRUM is responsible for multiple ICS attacks, including the CRASHOVERRIDE event in 2016, which blacked out a portion of Kyiv for about an hour, and the failed Industroyer2 attempt in 2022. ELECTRUM has technical overlaps with the Sandworm APT.[13] While they were not as active as KAMACITE in 2024, ELECTRUM used hacktivist personas to conceal their other operations and developed a new wiper capability, AcidPour.

ELECTRUM targets Ukraine, though Dragos also observed the targeting of energy companies in Germany.

Electric

ELECTRUM demonstrated their ability to reach Stage 2 - Execute ICS Attack of the ICS Cyber Kill Chain.

Given ELECTRUM's history of wiper malware usage, asset owners should implement basic security measures to prevent or at least monitor binary execution within control system environments or monitor when such files transfer into the ICS network. End users should disallow new service installs, disable service changes, and implement application whitelisting so only authorized applications can execute on devices if possible. Asset owners and operators must be prepared to not merely prevent such actions but also ensure quick recovery in these circumstances. Robust backups of engineering files such as project logic, IED configuration files, and ICS application installers should be offline and tested.



Timeline of ELECTRUM Wiper Capabilities

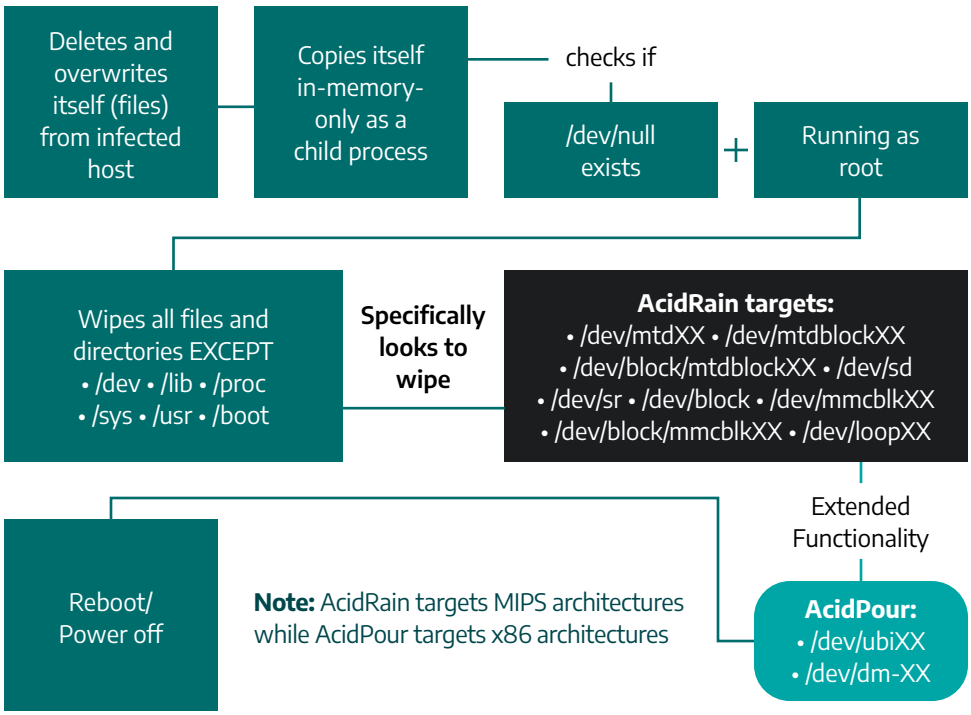
[13]Sandworm Team - MITRE

ELECTRUM Campaigns

KyivStar Attack and Hacktivists Cover (December 2023)

Ukraine's primary telecommunications provider, Kyivstar, experienced a cyber attack, resulting in significant service disruptions nationwide. Following the incident, two pro-Russian hacktivist online personas, KillNet and Solnetspek, claimed responsibility through nearly identical messages posted on their Telegram channels. In early 2024, Dragos analyzed the Kyivstar incident and determined that ELECTRUM used the resources and reputation of the hacktivist persona Solnetspek to obfuscate its operational activities.

AcidPour Wiper Capabilities



AcidPour Wiper (March 2024)

Dragos analyzed ELECTRUM's new capability, AcidPour. AcidPour is a binary compiled for Linux operating systems that can search and wipe Unsorted Block Images (UBI) directories in embedded devices, including devices in OT environments.

AcidPour extended the functionality of AcidRain, a previously used wiper, in February 2022. AcidRain impacted ViaSat modems and caused a partial interruption of KA-SAT's consumer-oriented satellite broadband service. The attack also impacted wind turbines in Germany.[14]

The discovery and implications of AcidPour underscore the persistent threat posed by ELECTRUM's arsenal of wiper malware, particularly considering their potential to inflict substantial operational disruptions and damage in OT environments.

[14] AcidRain | A Modem Wiper Rains Down on Europe - SentinelOne

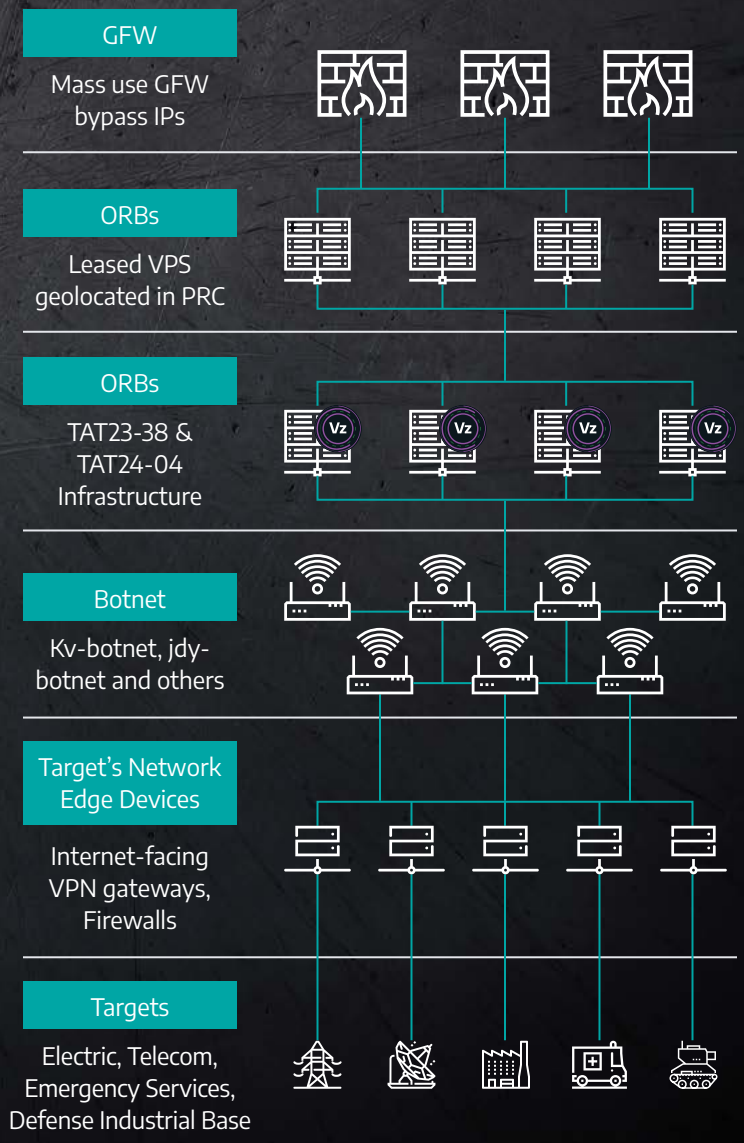
Geopolitical Tensions in Asia Facilitate Further VOLTZITE Activity

Throughout the year, the threat group VOLTZITE continued its activities, compromising small office and home office (SOHO) routers and interacting with geographic information systems (GIS). Analysis reveals that VOLTZITE and its affiliates are using infrastructure from compromised organizations as relay points for use in a botnet. These actions facilitate adversary-controlled peer-to-peer (P2P) relay networks that enumerate internet-exposed critical infrastructure, impacting sectors such as electric, oil and gas, water and wastewater, and government entities.

VOLTZITE Technical Update

VOLTZITE is arguably the most crucial threat group to track in critical infrastructure. Due to their dedicated focus on OT data, they are a capable threat to ICS asset owners and operators. This group shares extensive technical overlaps with the Volt Typhoon threat group tracked by other organizations.[15] VOLTZITE has a history of OT network intrusions, and like in previous years, Dragos observed VOLTZITE continuing to use different proxy networks and steal GIS data, OT network diagrams, and OT operating instructions from their victims. Aided by this ICS-focused data, VOLTZITE could craft a malicious OT-specific tool capable of operational disruption. Instead, this threat group uses tools already available on the systems known as living-off-the-land (LOTL) techniques. With careful monitoring and investigation of "odd" network communication, defenders can identify and defend against VOLTZITE.

VOLTZITE disguises its operations by setting up complex chains of network infrastructure. Dragos tracked their continuing provision of operational relay box (ORB) networks and compromised SOHO routers operated by electric utilities that provide telecommunications infrastructure and energy services to a specific region. Since these routers' IP addresses would look neutral to network defenders, VOLTZITE likely intended to use these compromised routers to exploit other critical infrastructure targets.



Historical VOLTZITE Infrastructure Usage

[15] Volt Typhoon – MITRE

VOLTZITE conducts slow and steady reconnaissance efforts from multi-layered network infrastructure and shares infrastructure with other groups attributed to the Chinese state by others. Dragos observed this network reconnaissance against critical infrastructure network edge devices, such as VPN gateways and firewalls from known VOLTZITE co-opted botnets, such as the JDY botnet.

VOLTZITE continues to focus on exfiltrating OT-related data from its victims' networks. In many cases, Dragos observed VOLTZITE exfiltrating GIS data containing critical information about the spatial layout of energy systems.

VOLTZITE usually exploits vulnerabilities in internet-facing VPN appliances or firewalls for initial access. Dragos encourages asset owners and operators to implement adequate patch management and system integrity plans on those types of assets in their network. Dragos expects VOLTZITE operations against critical infrastructure of the United States and Western-aligned nations to continue into 2025. Defenders must monitor activity at every level of the Purdue model, from internet-facing VPN appliances to the business network through DMZs and within OT networks to identify VOLTZITE. The best way to identify VOLTZITE is by monitoring its behaviors; it purposely blends in with trusted networks and uses tools already available. Compare any unusual lateral movement with expected traffic within your network and validate suspicious user activity that originates from regular employee accounts.

Confirmed victims of **VOLTZITE** were found in North America, Guam, Europe, Asia, New Zealand, and Africa. Its campaigns have affected industrial sectors, including:

- **Electric Power Generation, Transmission, and Distribution**
- **Emergency Management**
- **Telecommunication**
- **Satellite Services**
- **Defense Industrial Base**

65%

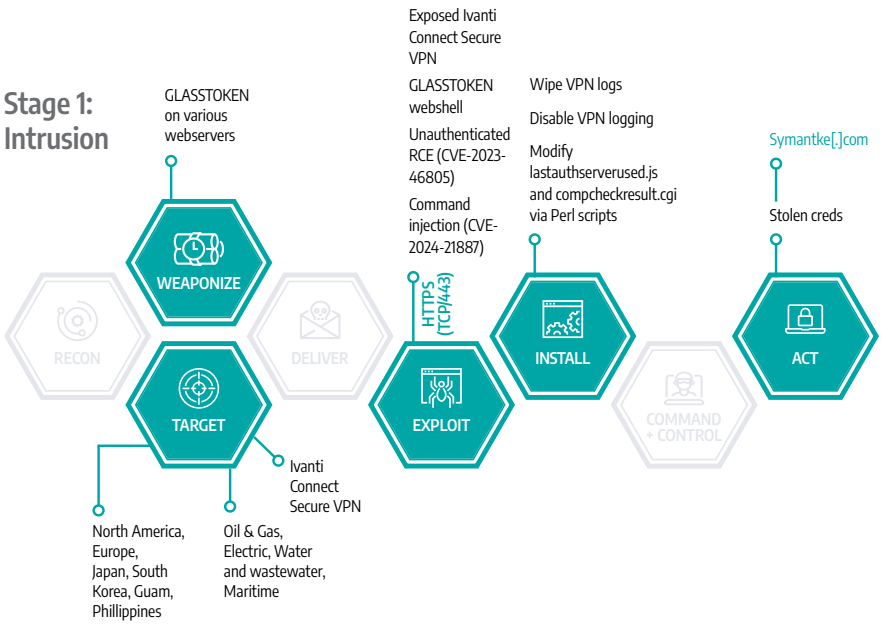
of sites Dragos assessed had insecure remote conditions. This includes insecure configurations, unpatched systems, and poor network architecture related to remote access appliances and applications.

VOLTZITE Campaigns

Ivanti VPN Zero-Day Campaign (December 2023)

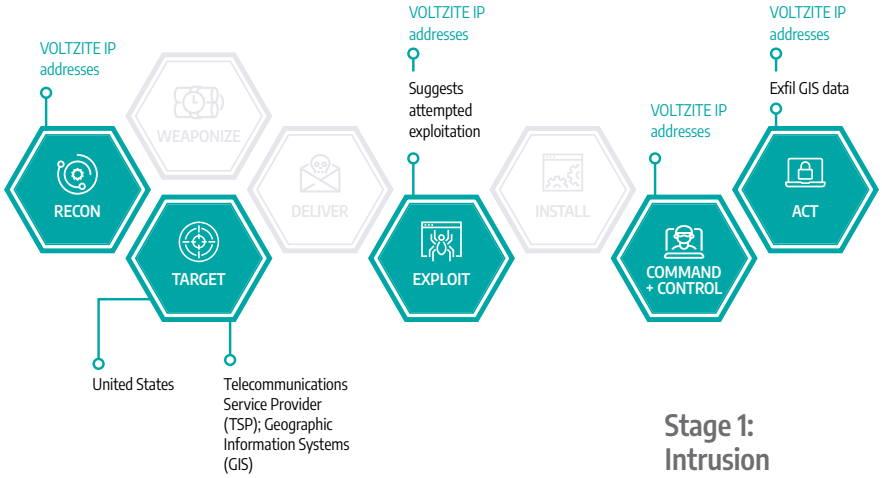
By combining the exploits, VOLTZITE can execute remote code, enabling theft of configuration data, reverse tunneling from the ICS VPN appliance, and other malicious behaviors.[16]

Monitor SYS32039 and SYS32040 for new files being created.



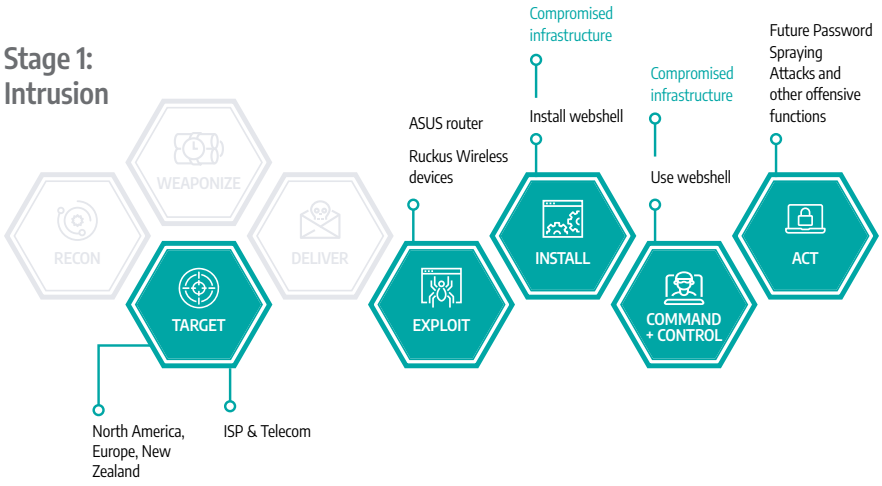
Telecom and EMS Campaign (January 2024)

VOLTZITE conducted reconnaissance of U.S. telecommunications and command-and-control (C2) activity with U.S. Emergency Services GIS endpoints.[17]



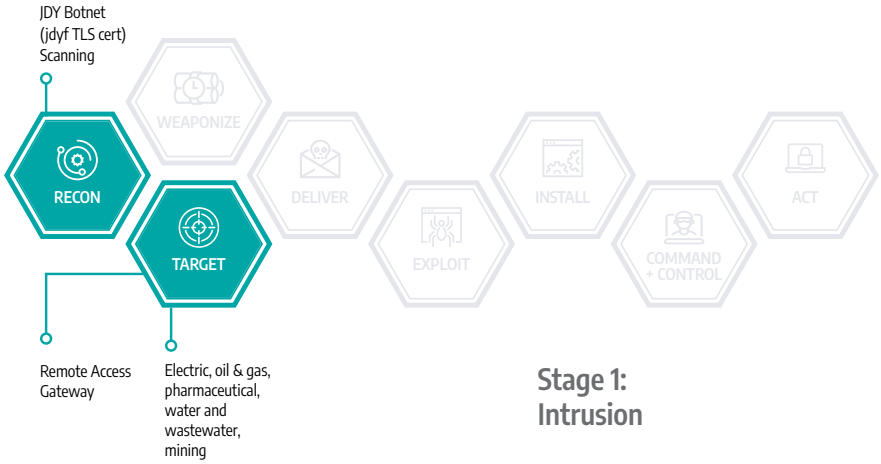
ISP and Telecommunications Campaign (August 2024)

VOLTZITE compromised SOHO devices in electric, utility, and telecommunications cooperative infrastructure for use in operational relay networks to support future operations.



[16]Active Exploitation of Two Zero-Day Vulnerabilities in Ivanti Connect Secure VPN - Volexity; [17]VOLTZITE Espionage Operations Targeting U.S. Critical Systems - Dragos Inc.

JDY Botnet (Late 2024)
VOLTZITE scanned targets with JDY botnet certificates. Target organizations were in the electric, oil and natural gas, manufacturing, and defense industrial base sectors.



Tips for Hunting

Do I have an adversary in my network collecting and exfiltrating GIS data? To help answer this question, you may need to evaluate your visibility, please refer to the Collection Management Framework.

Dragos Identifies Two New Threat Groups in 2024

Shifting away from the existing Dragos-designated groups, two newly coined Dragos threat groups were also very active during this period, conducting a series of conflict-adjacent campaigns.

GRAPHITE targets entities in the energy, oil and gas, logistics, and government sectors associated with the conflict in Ukraine, spanning across Eastern Europe and the Middle East.

Moving to the conflict in the Middle East, **BAUXITE** targets entities in oil and gas, electric, water and wastewater, and chemical manufacturing in the United States, Europe, Australia, and the Middle East. BAUXITE demonstrates technical alignment with the pro-Iranian group CyberAv3ngers. BAUXITE is likely to enhance its capabilities and continue disruptive activities against OT/ICS entities globally, especially those party to the Israel-Hamas conflict.

Introducing GRAPHITE

Dragos designated GRAPHITE as a new threat group after discovering a campaign targeting hydroelectric generation facilities to steal credentials. Since then, Dragos observed GRAPHITE targeting industrial and energy organizations in Eastern Europe and Asia. The group has strong technical overlaps with the cluster identified as APT28 and other names.[18] GRAPHITE focuses on organizations with relevance to the military situation in Ukraine, observable since Russia's invasion of Ukraine in February 2022.

In early 2023, Dragos identified GRAPHITE conducting a spear-phishing campaign targeting hydroelectric generation facilities, and other ICS organizations throughout Eastern Europe and the Middle East. The campaign exploited a no-click flaw in Microsoft Outlook allowing GRAPHITE to steal Windows authentication data.[19] Concurrently, GRAPHITE conducted near-constant phishing operations using custom script-based malware. While these two campaigns used different tools and techniques, they targeted organizations in critical industries across a similar geography.

GRAPHITE used a network of compromised Ubiquiti Edge Routers to distribute malware and maintain C2 channels. GRAPHITE used this network as early as 2022 and their network remained active until February 2024, when the U.S. Justice Department announced a court-approved disruption of the botnet.[20] Since 2024, Dragos observed GRAPHITE relying more on legitimate internet services (LIS), such as API endpoint testing services or GitHub, for staging payloads and C2 activities.

GRAPHITE is a relevant threat for OT/ICS organizations as its targeting profile may shift in response to geopolitical developments in Eastern Europe but has not yet demonstrated Stage 2 capabilities. Dragos encourages defenders of industrial organizations, especially those involved in any way with Ukraine, to familiarize themselves with this adversary.

Since at least March 2022, GRAPHITE conducted numerous campaigns achieving Stage 1 ICS Cyber Kill Chain impacts. Confirmed victims of GRAPHITE were found throughout Eastern Europe and the Middle East. Its campaigns have affected multiple critical infrastructure sectors, including:

- **Electric**
- **Oil & Natural Gas**
- **Rail/Freight Logistics**
- **Aviation Logistics**
- **Defense Industrial Base**

Dragos penetration testers also use internet infrastructure to test for C2 channels. 17 percent of penetration tests in 2024 resulted in findings related to C2 communication, with DNS channels being the primary contributor. If you can resolve internet addresses (e.g., www.dragos.com), adversaries can use this to remotely access those networks.

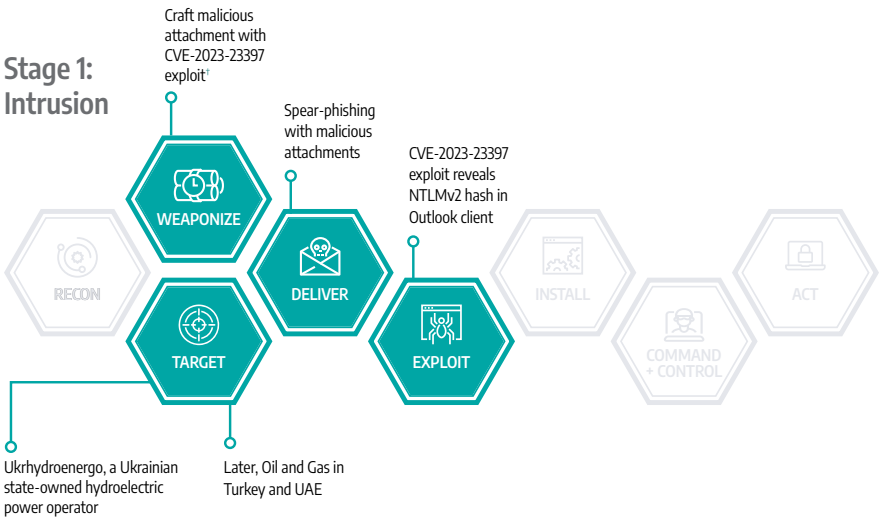
Tips for Hunting

Would we see an adversary spearphishing through legitimate internet services? Note: focus on spearphishing hooks and behaviours instead of their hosting source.

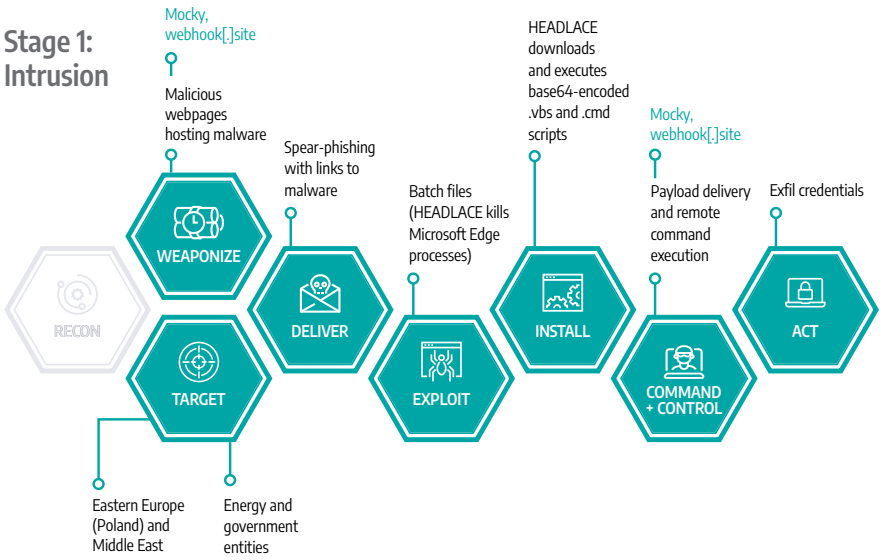
[18]APT28 - MITRE; [19]Microsoft Outlook Elevation of Privilege Vulnerability - Microsoft; [20]Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate of the General Staff (GRU) – U.S. Justice Department

GRAPHITE Campaigns

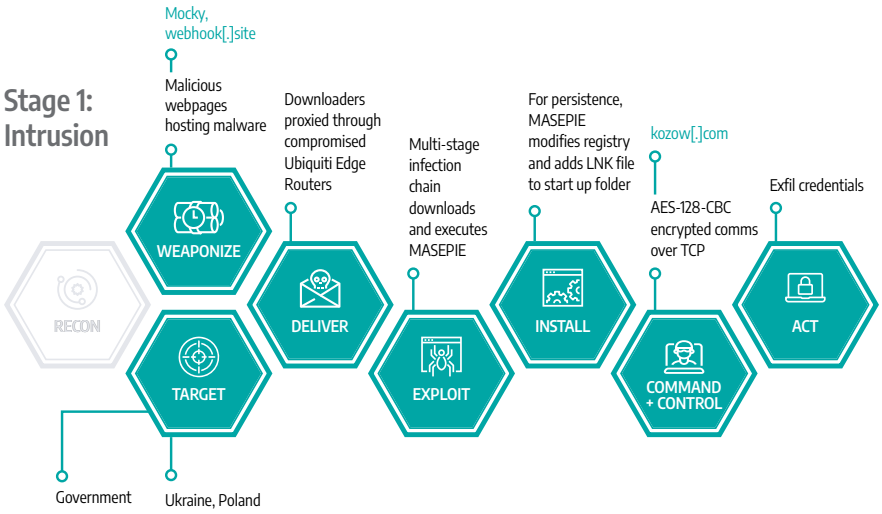
From March 2022 to October 2023, a spear-phishing campaign targeted natural gas pipeline operators and hydroelectric generation facilities in Eastern Europe and West Asia. A vulnerability in Microsoft Outlook allowed for malicious attachments to capture credentials.[21, 22]



Throughout 2023, spear-phishing campaigns targeted energy and government entities in Poland and the Middle East. Malicious websites delivered a Windows batch script backdoor dubbed HEADLACE, which allowed remote command execution.[23]

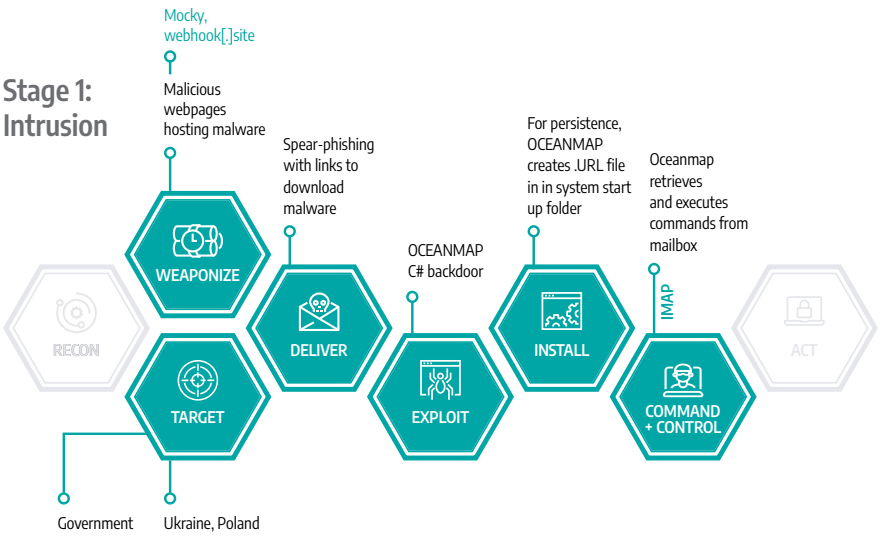


From 2023 to February 2024, a spear-phishing campaign targeted government entities in Poland and Ukraine. Compromised Ubiquiti Edge Routers were used to deliver MASEPIE malware. This Python backdoor allowed for encrypted reverse proxy connections to C2 infrastructure.[24, 25]

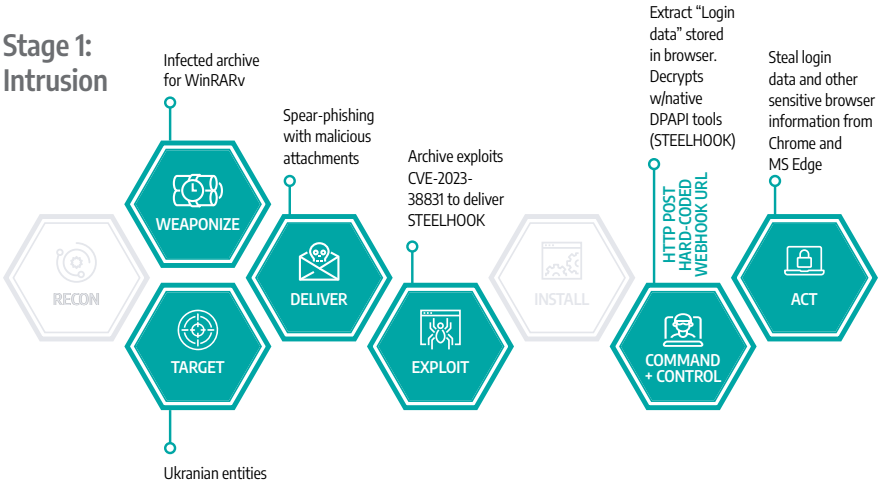


[21]Fighting Ursa Aka APT28: Illuminating a Covert Campaign – Palo Alto; [22]APT28 Cyber attacks Using the CVE-2023-23397 Vulnerability - National Security and Defense Council of Ukraine; [23]APT28 cyber attack: msedge as a bootloader, TOR and mockbin.org/website.hook services as a control center (CERT-UA#7469) - CERT-UA; [24]APT28 campaign targeting Polish government institutions – CERT.PL; [25]APT28: From initial attack to creating threats to a domain controller in an hour (CERT-UA#8399) - CERT-UA; †Guidance for investigating attacks using CVE-2023-23397

From 2023 to present, a spear-phishing campaign targeted government entities in Ukraine and Poland. Malicious websites are used to deliver OCEANMAP malware. This C# backdoor allowed remote commands on victim devices over IMAP.[26]



In early 2024, a spear-phishing campaign targeted Ukrainian entities. A vulnerability in the WinRAR archiver tool infects emails and sends malicious attachments that deploy a PowerShell stealer dubbed STEELHOOK. This malware allows the adversary to extract login data from Google Chrome and Microsoft Edge browsers.[27, 28]



Simultaneous campaigns in 2024 saw GRAPHITE maintaining malicious websites designed to appear as legitimate web login portals of popular service providers such as Outlook on the Web (OWA) and ukr.net (a popular Ukrainian online service). Using a credential-phishing toolkit, likely custom to GRAPHITE, adversaries could successfully bypass two-factor authentication and Captcha solving to profile a victim's browser and location.[29]

OT Watch Identified **14 percent of customers** communicating to external addresses via IMAP protocol.
*A minor portion of these environments are untuned.

Hunt for yourself in the Dragos Platform.
To identify IMAP communicating to non RFC-1918 addresses:

```
type:Communications AND NOT ip_dst_network_id:* AND
protocol:IMAP AND dst_port_o2r: *
```

[26]APT28: From initial attack to creating threats to a domain controller in an hour (CERT-UA#8399) - CERT-UA; [27]APT28 cyber attack: msedge as a bootloader, TOR and mockbin.org/website.hook services as a control center (CERT-UA#7469) - CERT-UA; [28]Government-backed actors exploiting WinRAR vulnerability - Google; [29]APT28 leverages multiple phishing techniques to target Ukrainian civil society - Sekoia

Introducing BAUXITE

Dragos-designated threat group BAUXITE was implicated in multiple global campaigns targeting OT/ICS entities and specific devices. This group shares substantial technical overlaps, based on capabilities and network infrastructure, with the pro-Iranian hacktivist persona CyberAv3ngers, which has explicit affiliations with the Iranian Revolutionary Guard Corps—Cyber and Electronic Command (IRGC-CEC), as reported by the U.S. Government.[30] The U.S. Government sanctioned multiple members of the CyberAv3ngers, including their leader.[31]

BAUXITE is on OT/ICS-focused forums, where they ask questions about OT/ICS original equipment manufacturer (OEM) hardware. They extensively monitor security advisories from OEMs and ICS protocols, likely documenting and cataloging known vulnerabilities to target in future campaigns.

Given BAUXITE's technical alignment with CyberAv3ngers and its reported ties to the IRGC-CEC, its targeting strategies and operational focus evolved under state-sponsored directives or geopolitical pressures. Throughout 2025, BAUXITE is expected to enhance its capabilities and attempt to conduct disruptive operations against OT/ICS entities globally.

Dragos recommends identifying assets with SSH exposed to the internet and concealing access behind VPN. Double check that accounts with SSH access do not have default or easily guessed passwords. Audit SSH keys; remove unnecessary keys; and rekey existing keys from exposed devices. **Refer to the Dragos OT-CERT Getting Started Guide: Default Passwords and Internet-Exposed Devices.**

Since late 2023, Dragos observed four BAUXITE campaigns, including those with Stage 2 ICS Cyber Kill Chain impacts via trivial compromises of exposed devices. Confirmed victims of BAUXITE are in the United States, Europe, Australia, and West Asia. Its campaigns affected multiple critical infrastructure sectors, including:

- **Electric**
- **Oil & Natural Gas**
- **Water/Wastewater**
- **Food & Beverage**
- **Chemical**
- **Manufacturing**

45%

of OT Watch customers have SSH communicating to publicly routable addresses. Dragos penetration testers leverage existing SSH paths for general purpose encrypted communication including demonstrating C2 tunnels and proxies.

*A minor portion of these environments are untuned.

Hunt for yourself in the Dragos Platform. To identify SSH communicating to non RFC-1918 addresses:

```
type: Communications AND ip_dst_asset_id: * AND
NOT ip_dst_network_id: * AND protocol:SSH AND
src_port_r2o: *
```

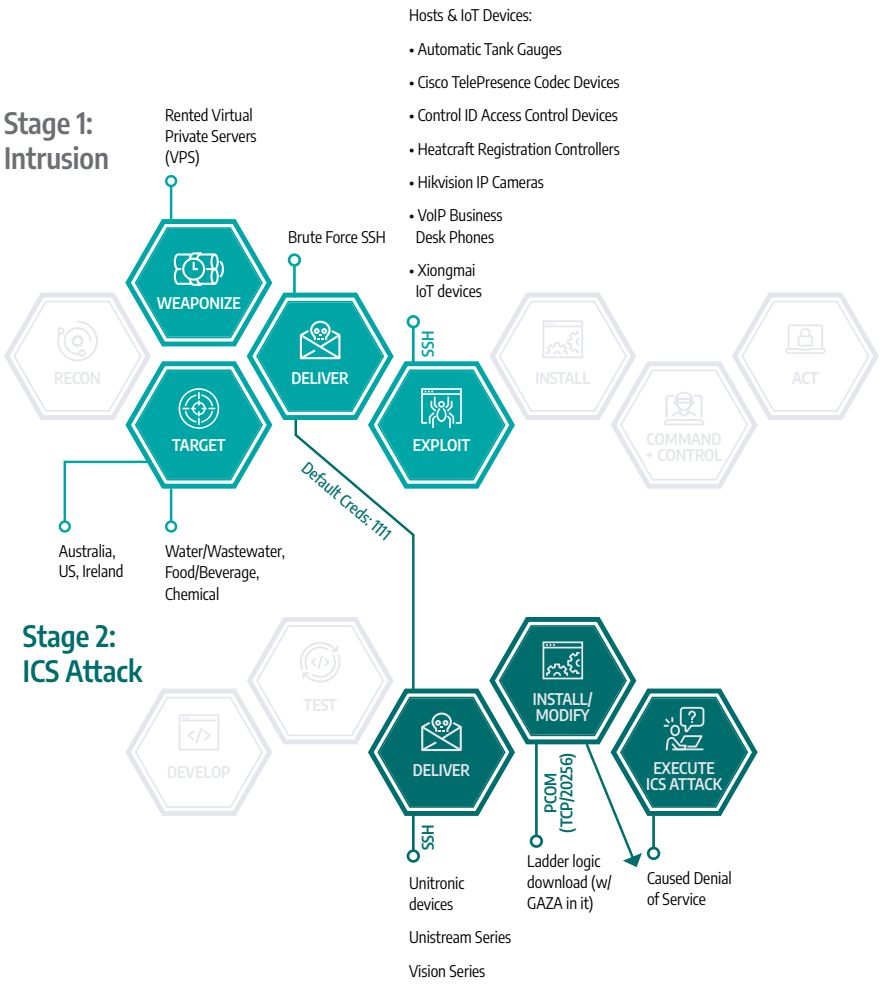
[30]CyberAv3ngers - MITRE; [31]Treasury Sanctions Actors Responsible for Malicious Cyber Activities on Critical Infrastructure – U.S. Dept. of the Treasury

BAUXITE Campaigns

Unitronics Campaign (November 2023-January 2024)

This campaign affected nearly 100 OT/ICS organizations globally, reaching ICS Cyber Kill Chain Stage 2 by compromising Unitronics Unistream and Vision series programmable logic controllers (PLCs) exposed on the internet. The adversary is capable of downloading logic to these controllers, causing a denial of service (DoS) equivalent to execute an ICS attack.

In late 2023, Dragos's investigation uncovered widespread exploitation tactics, including SSH brute-force attacks targeting a diverse set of vulnerable hosts and internet of things (IoT) devices, such as Hikvision IP cameras, automatic tank gauges, VoIP business desk phones, Control ID access control systems, Xiongmai IoT devices, Heatcraft refrigeration controllers, and Cisco TelePresence codec devices.[32]



[32]Cyber Av3ngers Hacktivist Group Targeting Israel-Made OT Devices - Dragos Inc.

Sophos Firewall Attack (April 2024-May 2024)

BAUXITE targeted vulnerable Sophos firewalls, resulting in enterprise impact on chemical, food and beverage, and water and wastewater industries. Dragos Services conducted an incident response to a U.S. oil and natural gas (ONG) organization where BAUXITE compromised Sophos firewalls at oil rig sites.

According to Dragos telemetry, Sophos devices are found in North America in oil and natural gas and electric utilities.

5%

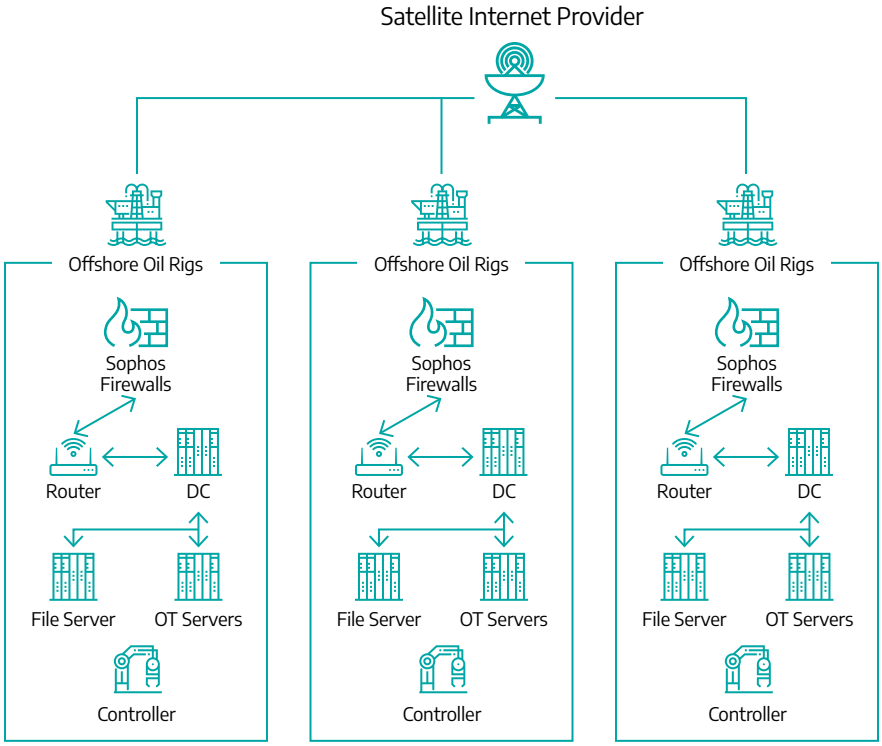
OT Watch identified **5 percent of customers** communicating to external addresses via PPTP protocol.

*A minor portion of these environments are untuned.

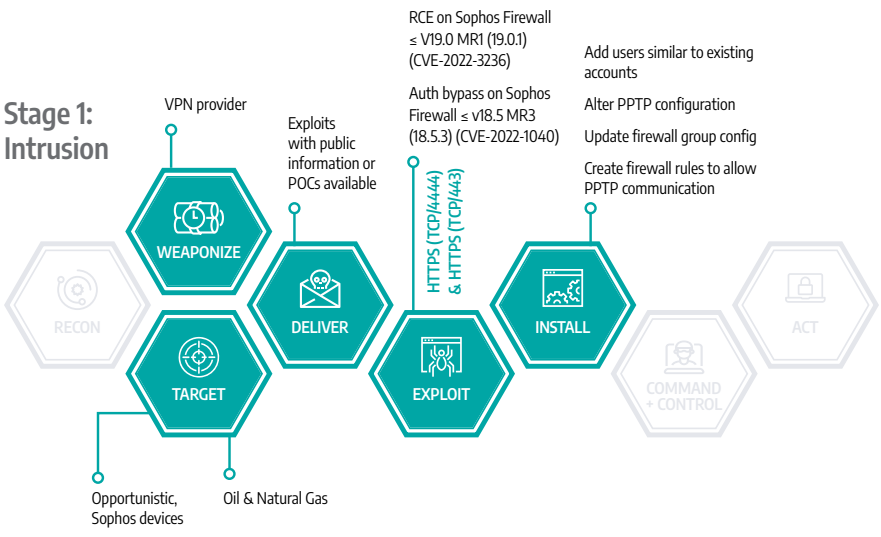
Hunt for yourself in the Dragos Platform. To identify PPTP communicating to non RFC-1918 addresses:

```
type:Communications AND
NOT ip_dst_network_id:* AND
protocol:PPTP AND dst_port_
o2r: *
```

If you use a satellite internet provider, such as Starlink or Viasat, you may be inadvertently exposing your equipment to the internet. Consider these scenarios when assessing your organization's exposure.



Example of Compromised Infrastructure



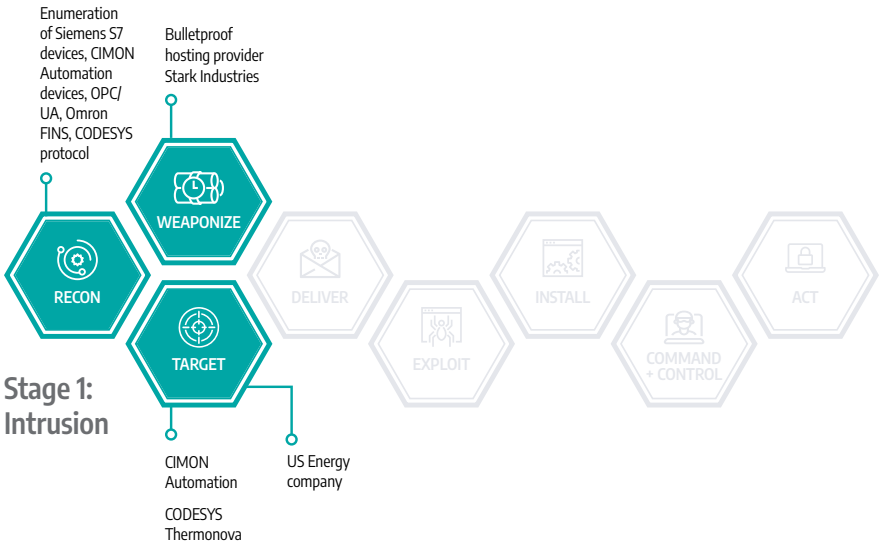
Reconnaissance Scanning Campaign (June 2024-July 2024)

BAUXITE accessed multiple OT/ICS OEMs and utility web pages. This activity was likely conducted to gather intelligence on products, services, and other critical information that could support future operational objectives.

BAUXITE conducted port scanning of multiple internet-exposed OT/ICS devices, likely to identify potential targets for future operations. The following internet-exposed devices were targeted:

- **Siemens S7 devices** via s7comm (TCP/102).
- **CIMON Automation devices** via CIP (TCP/44818).
- **Devices running OPC Unified Architecture (OPC/UA) Server** via UDP/4840.
- **Omron Factory Interface Network Service (FINS)** TCP/9600.
- **Devices running CODESYS** (TCP/11740, TCP/1217, and UDP/1740-1743).

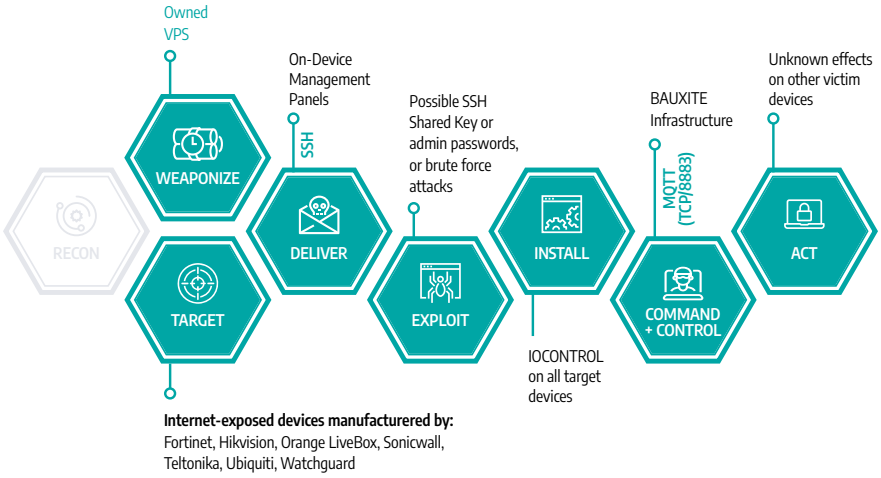
These protocols overlap with CHERNOVITE-developed PIPEDREAM.



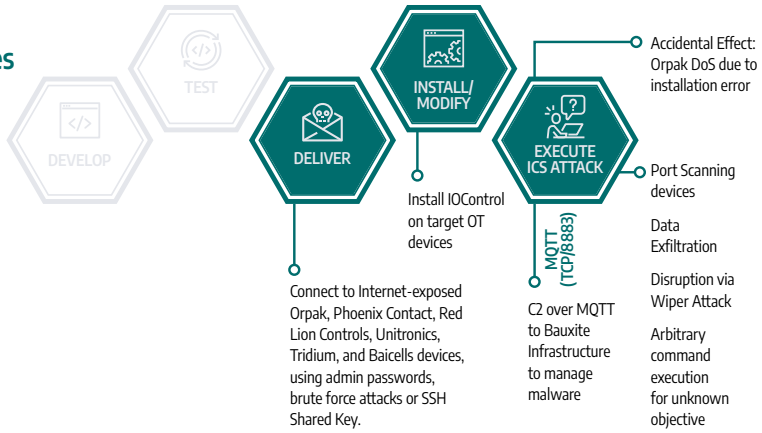
IOControl Campaign (Late 2023-2024)

BAUXITE compromised over 400 global OT/ICS devices and firewalls by installing a custom-embedded Linux backdoor called IOControl. IOControl is a remote access trojan and communicates to the C2 server using Message Queuing Telemetry Transport (MQTT) on TCP/8883. This communication is established to a hardcoded domain hosted on Cloudflare via DNS over HTTPS (DoH). As of publication, this domain is sinkholed, mitigating risk to defenders. Each IOControl sample is unique to the targeted device, with newer samples that can wipe the system via memory technology device (MTD) manipulation.

Stage 1: Widespread intrusion against non-OT devices



Stage 2: Attack on OT Devices



According to Neighborhood Keeper, Orpak devices are used in electric generation in Australia and New Zealand.

Electric

Phoenix Contact devices are used in North America, Asia, and Europe, in the following industries:

- **Transportation & Logistics**
- **Manufacturing**
- **Chemical**
- **Mining**

ICS-Focused Malware Increasingly Used as a Tool in Conflict-Driven Campaigns

Two new variants of ICS malware were observed in April 2024, both of which occurred in association with the Ukraine-Russia conflict. While the use of ICS malware as a toolset in geopolitical conflicts is not a new concept, the alleged deployment by both parties to the Ukraine-Russia war indicates a tit-for-tat escalation with implications for the larger OT/ICS community.

BlackJack Claims Disruption of Industrial Sensors in Moscow

In April 2024, the self-named hacktivist group BlackJack claimed to breach Moskollektor, a municipal organization that maintains Moscow's communication system for a gas, water, and sewage network. BlackJack asserts that it compromised communications to thousands of sensors responsible for maintaining operations in the Moscow region.

Stolen data released by BlackJack on a public website indicates they accessed routers and sensor gateway devices, likely through default credentials. These gateways are connected to industrial sensors through a serial connection which monitors Moskollektor's underground tunnel infrastructure and collects and transmits physical data.

Teams are often unaware of default credentials. Dragos flags default credentials in only 6 percent of architecture reviews, but approximately 1 in every 4 penetration tests find default credentials in industrial environments. Active inspections are the best way to identify this issue.

Using the Fuxnet malware, BlackJack claimed to disable thousands of sensors and destroy sensor gateway devices, rendering them unable to transmit information. Additionally, BlackJack asserted they exfiltrated organizational data, defaced social media accounts, accessed the emergency service number 112, and factory reset devices and workstations. They also released screenshots of the Fuxnet source code; however, they did not provide a sample of the Fuxnet binary, and it has not appeared in any public malware repositories or Dragos telemetry.

After analyzing all the data released by BlackJack, it is likely that disruption to the industrial sensors and sensor gateways did occur. However, the extent of the disruption was not as significant as BlackJack claimed. The released screenshots indicate that Fuxnet likely would lead to the disruption or destruction of the sensor gateways if deployed. It is unclear if Fuxnet caused a permanent or temporary DoS condition on the sensors themselves.

The Fuxnet Malware

Pending evidence of its compiled form, Fuxnet is the eighth known ICS-specific malware due to its ability to disrupt Meter-bus communication to the industrial sensors.[33] According to the source code screenshots released by BlackJack, Fuxnet contains two major components:

Sensor Gateway Destructor

The sensor gateways provide internet access to sensor-collected industrial data.

1

THE DESTRUCTOR CONSISTS OF THREE PARTS

File System
Stops and removes critical services; deletes critical files.

UBI Volume
Destroys UBI volume; leaves UBI Volume Update IOCTL operation hanging by writing a less-than-promised amount of data, effectively bricking the device.

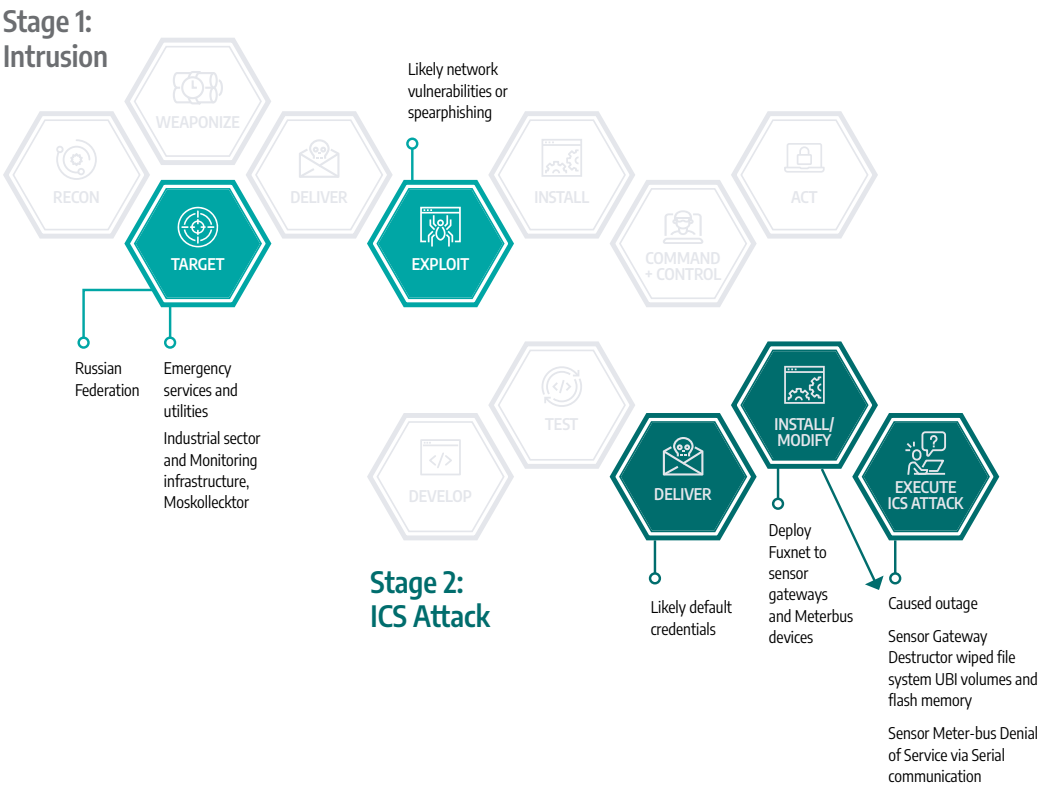
Flash Memory
Destroys MTD flash memory via erase-then-write technique to wear out NAND memory.

Sensor Meter-Bus DoS

2

Overwhelms sensors by sending many Meter-Bus requests over a serial connection. These requests are randomly generated packets of data that loosely conform to the Meter-Bus standard, thus fuzzing the device to cause a potential DoS condition.

The Sensor Gateway Destructor component is a more generic Linux wiper malware, whereas the Meter-Bus DoS component provides unique ICS-specific capability. Meter-bus is a European standard protocol for reading specific sensor data from water, gas, and electricity meters. By overwhelming the device with randomly generated requests, it is possible Fuxnet triggered unknown zero-day vulnerabilities in the industrial sensor's Meter-bus protocol stack, thus rendering them inoperable. The sensor



[33]Strategic Overview of the Fuxnet Malware - Dragos

gateways were likely physically damaged and required device replacement to resume normal operations.

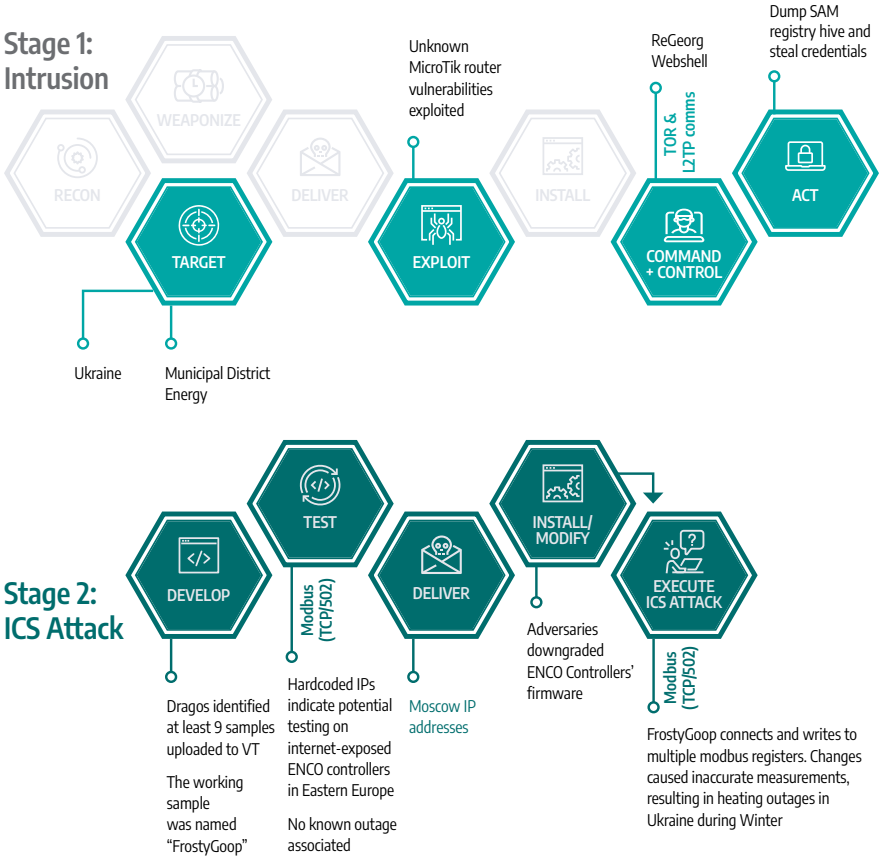
Lessons from Fuxnet

The attack on Moskollektor underscores the normalization of attacks on industrial devices by groups driven by geopolitical conflicts. Fuxnet was highly tailored to Moskollektor and is unlikely to be used against another industrial environment without significant changes to the codebase. Poor practices such as default credentials greatly help adversaries and can be commonplace in operational facilities. Dragos telemetry indicates that default credentials are still commonly used in environments.

However, the SANS ICS 5 Critical Controls[34] can strengthen an organization's security posture and better defend against threats like the Fuxnet malware. Asset owners should be sure to identify and mitigate ICS components with default credentials as part of a risk-based vulnerability management program and implement thorough asset hardening and strict access controls to strengthen their defensible architecture.

FrostyGoop Malware Impacts Heating in Ukraine

In April 2024, Dragos discovered FrostyGoop, the ninth known ICS malware.[35] FrostyGoop modified instrument measurements of ENCO controllers resulting in heating outages for over 600 apartment buildings in Ukraine during the winter. FrostyGoop interacts with ICS devices over Modbus TCP/502, a standard ICS protocol used worldwide, combining generic, publicly available Modbus libraries with logging capabilities to adaptively send commands to read and write registers on ICS devices. Dragos tracks this activity as TAT24-24.



The January 2024 cyber attack against a municipal district energy company in Ukraine involving FrostyGoop was likely a part of hybrid warfare in support of the Ukraine-Russia conflict. The Cyber Security Situation Center (CSSC), a part of the Security Service of Ukraine (Служба безпеки України),

[34]The Five ICS Cybersecurity Critical Controls - SANS; [35]Impact of FrostyGoop Modbus Malware on Connected OT Systems - Dragos

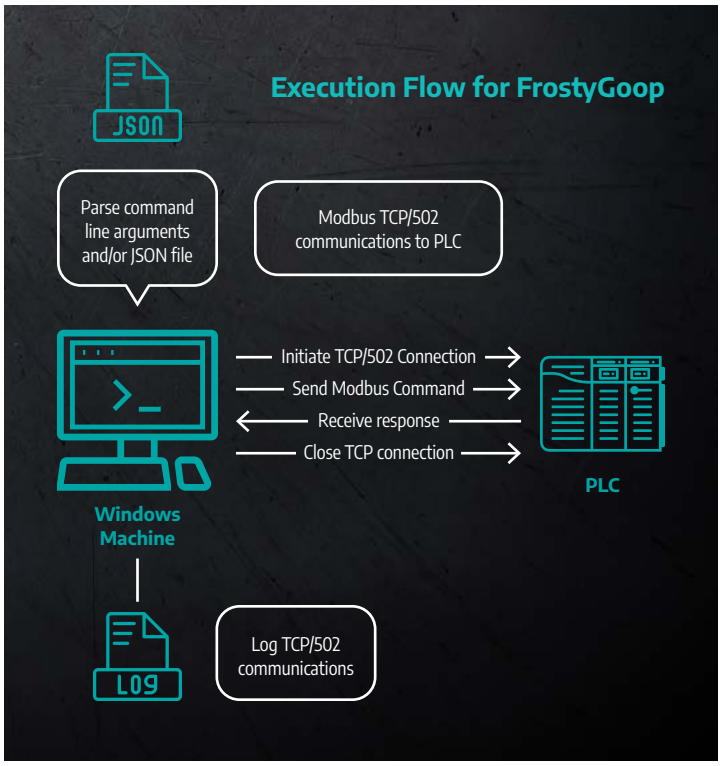
shared details with Dragos about the incident. Analysis suggests that FrostyGoop was also used to target ENCO controllers with TCP/502 open to the public-facing internet. ENCO controllers are found throughout Eastern Europe and Dragos's investigation of FrostyGoop revealed that there were over 46,000 internet-exposed ICS devices communicating over Modbus worldwide. While FrostyGoop was used to target ENCO devices, its functionality is not specific to these devices, allowing it to interact with numerous other commonly used ICS devices such as PLCs, DCS, sensors, actuators, and field devices.

Most concerning was the inability of common antivirus software to detect FrostyGoop due to its blending of malicious activity with normal operations. Exploitation of well-known ICS protocols is becoming more frequent within ICS malware development, underscoring the need for more sophisticated OT-aware detection and response methods. TAT24-24 downgraded the controller firmware before the attack.

The attack's involvement of internet-exposed controllers and insufficient network segmentation highlights the risks of not implementing basic cybersecurity controls and the importance of doing so.

The FrostyGoop Malware

Dragos identified FrostyGoop and eight other similar samples on an opensource repository, VirusTotal. It was written in Go and accepts a json file with a list of target IP addresses. It is capable of reading and writing to Modbus registers over TCP/502 and has a hardcoded UnitID of 254.



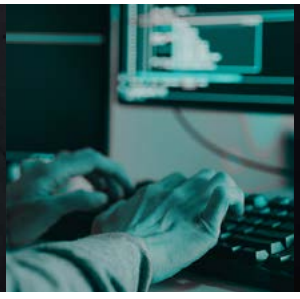
Many Modbus devices have a default UnitID of 254, so FrostyGoop has the potential to impact several other Modbus-speaking devices not specific to ENCO Control devices.

Lessons from FrostyGoop

Natively, FrostyGoop can impact any Modbus device with a UnitID of 254. Dragos recommends looking for vulnerable devices in your own network and continuously monitoring them, including monitoring devices for new Modbus connections on TCP/502. Dragos also recommends restricting access to Modbus TCP/502 and ensuring Modbus devices are not accessible from the public-facing internet.

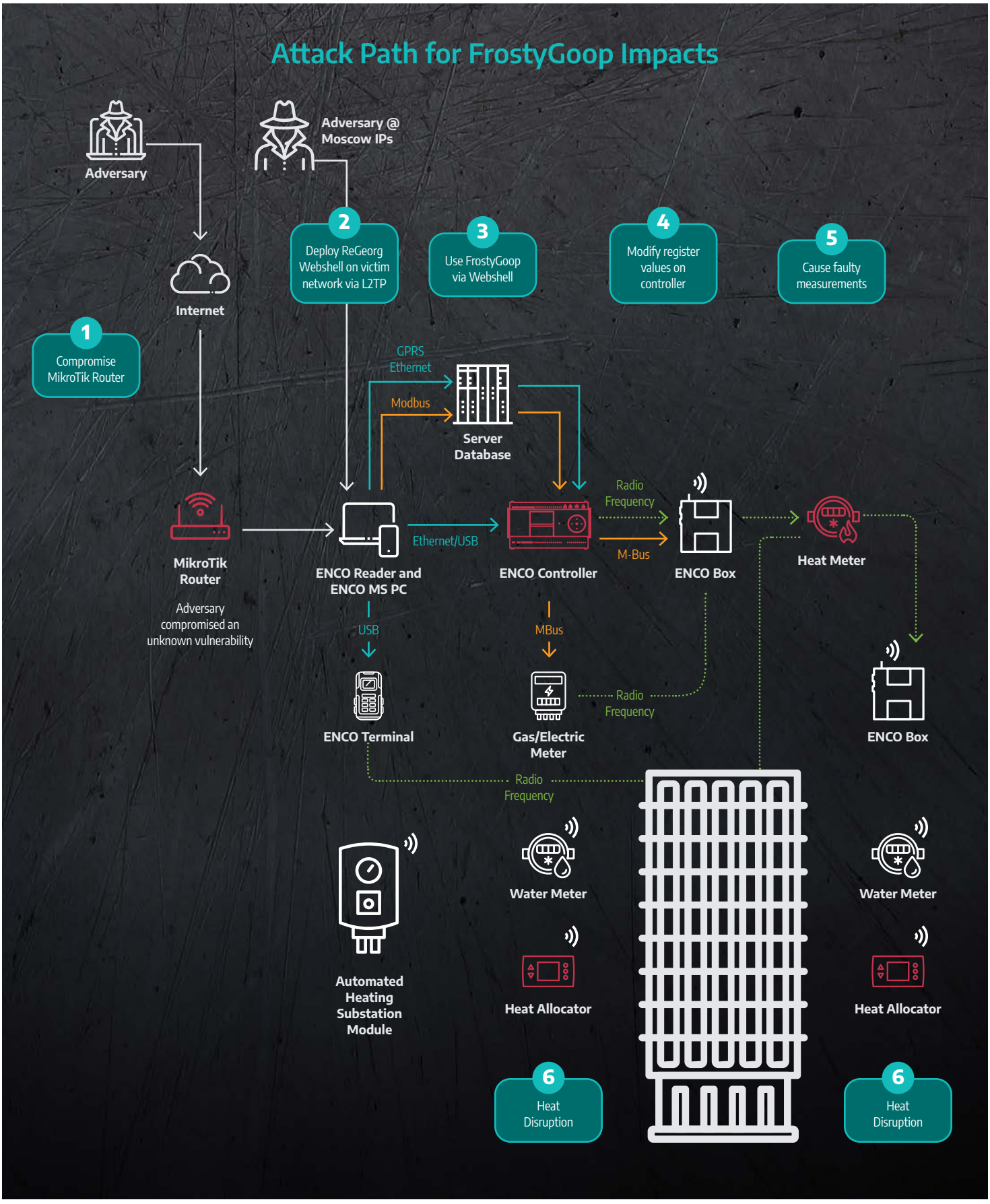
Tips for Hunting

OT Watch hunts for downgraded firmware. Would you notice if an adversary downgraded your controllers?



Here's the Dragos Platform query to search for Modbus devices with a unitID of 254 in your own environment:

```
type:"modbus" AND modbus_unit_id:"254" AND
modbus_function_code: (3 OR 6 OR 16)
```


Attack Path for FrostyGoop Impacts
Adversary
Adversary @ Moscow IPs
Internet
1
Compromise MikroTik Router
2
Deploy ReGeorg Webshell on victim network via L2TP
3
Use FrostyGoop via Webshell
4
Modify register values on controller
5
Cause faulty measurements
GPRS Ethernet
Modbus
Server Database
MikroTik Router
Adversary compromised an unknown vulnerability
ENCO Reader and ENCO MS PC
Ethernet/USB
ENCO Controller
Radio Frequency
M-Bus
ENCO Box
Heat Meter
USB
MBus
ENCO Terminal
Gas/Electric Meter
Radio Frequency
ENCO Box
Radio Frequency
Water Meter
Water Meter
Automated Heating Substation Module
Heat Allocator
Heat Allocator
6
Heat Disruption
6
Heat Disruption

An ICS Malware Definition

In 2024, Dragos created a definition of ICS malware based on historical data and our own experiences. For defenders, this provides assurance that ICS malware is a credible, real-world threat worth considering in scenario-based defensive applications such as incident response planning, tabletop exercises, and threat baselines.

ICS Malware Definition

At Dragos, ICS malware is defined as follows:

> ***ICS-capable software intentionally designed for adverse effects on operational technology (OT) environments.***

The definition requires that ICS Malware contain three properties:

- The software must be ICS-capable.
- The software must be designed with malicious intent.
- The software must have the ability for adverse effects on OT environments.

Identifying a sample as ICS malware is an evidence-based intelligence assessment. If sufficient evidence for all three properties is found, the ICS malware designator is applied to the sample.

Three Properties of ICS Malware

ICS-Capable

ICS-Capable, according to SANS, means the software contains OT/ICS functions for navigating, altering, or retrieving information from OT networks, devices, or software. In other words, its code allows for speaking ICS protocols or interacting with PLCs and other OT devices.

Here are a few examples of ICS-capable software:

- Software that speaks ICS protocols like IEC104, OPCUA, and HART
- Software that can upload or download ladder logic programs
- Software that runs on the PLC interacting with ladder logic runtime or other operating system internals
- Software that runs on the engineering workstation that interacts with or modifies the engineering software (e.g., modifies project files).

The ICS-Capable property distinguishes the subset of ICS software from other types of software like standard Windows or Linux tools. Tools like Process Hacker, day-to-day Windows and Linux malware implants, and various ransomware variants are not considered ICS malware because they are not ICS-capable.

Designed with Malicious Intent

Malicious Intent is important for distinguishing malware from defender tools and other tools designed for a benign purpose. In the IT world, PSExec can be used by adversaries for lateral movement. Dragos does not call PSExec malware because it was designed for system administrators.[36] In the same way, something that looks like ICS malware but does not have malicious intent could be ICS research, an ICS red team tool, or a sub-component of a vendor's engineering software abused for malicious purposes.

To determine if the software was designed with malicious intent, Dragos uses evidence like code capabilities and behavior, binary similarity, developer information, threat group association, incident response data, and victim/deployment information.

[36] PsExec – Microsoft Learn

The Ability for Adverse Effects on OT Environments

This property introduces a burden of proof on the analyst to show that the software can achieve an adverse outcome and specifies the category of actions considered detrimental for OT. Identifying this property answers the question: *What adverse consequences can the ICS-capable software cause?*

Adverse Effects are like those described as Stage 2 effects in the ICS Cyber Kill Chain and vary by site and industry.[37] Here are a few examples of Adverse Effects:

- Collecting sensitive process information
- Enabling unauthorized access to OT devices
- Downloading arbitrary ladder logic or executable code to PLCs
- Bypassing OT firewalls or other security controls
- Manipulation of set points, variables, or other PLC settings

What if the malware does not work? If a tool is ICS-capable and designed with malicious intent but has no ability for adverse effects, it is likely broken malware or malware in development. Depending on how close it is to functioning, it may be called "potential ICS Malware."

[37] The Industrial Control System Kill Chain - SANS

What Does the ICS Malware Definition Mean for Asset Owners?

If your organization is implementing the SANS ICS 5 Critical Controls, then our list of ICS malware is a concrete guidepost for prioritizing defenses.[38]

For example, if your organization relies on Modbus/TCP, it might be at risk for a FrostyGoop-style attack. Using information about the malware, you can vet various aspects of your organization's implementation of the 5 Critical Controls by asking questions about each control.

In the same way, asset owners can refer to any ICS malware family that has been reported and design a similar exercise when considering their defensive posture. A version using FrostyGoop as the example is presented in the figure below.

Targeted disablement of operations via ICS malware is a common concern of our customers and one of many threat event categories reviewed as part of Dragos's new Threat Baseline service. With Threat Baselines, Dragos has helped organizations identify the potential repercussions of a FrostyGoop Modbus TCP attack against devices in their networks and helped them identify a mitigation path and recover against such an attack. Completing Threat Baselines in 2024 highlighted that industrial environments are uniquely configured, and reviewing threats from different perspectives helped identify common and uncommon insecurities.

ICS Incident Response Plan (Scenario Planning)

- What would an adversary need to do to attack our Modbus/TCP components?
- Are there online and offline backups of program and configuration files for Modbus/TCP components in my environment?

Defensible Architecture (Asset ID/Crown Jewels)

- Which processes are controlled by Modbus/TCP devices?
- How many Modbus/TCP devices are in my environment?

Network Visibility & Monitoring

- Are devices in my network emitting Modbus/TCP unnecessarily?
- Can we identify new and potentially unwanted communications to Modbus/TCP devices?

Secure Remote Access

- Are Modbus/TCP devices exposed to the internet?

Risk-Based Vulnerability Management

- Investigation of the FrostyGoop attack suggests that the adversaries may have gained access to the victim network via a vulnerability in an externally facing router. What vulnerabilities exist for my internal routers? Are they mitigated adequately?

[38] The Five ICS Cybersecurity Critical Controls – SANS

Hacktivists Continue to Wave Their Flags in Support of Certain Geopolitical Conflicts

Recent geopolitical conflicts, such as the Israel-Hamas and Ukraine-Russia conflicts, have intensified the relationship between hacktivism and state objectives. The hacktivist group CyberArmyofRussia_Reborn (CARR) continues to target critical sectors in the U.S., specifically water and wastewater and oil and natural gas, with confirmed incidents in California, Florida, and Pennsylvania.

The pro-Russia hacktivist group CyberVolk threatened Pakistan's critical infrastructure and announced the development of a new CyberVolk ransomware. This alarming trend suggests that hacktivists could leverage destructive malware to extend the impact of their operations.

In July 2024, the Holy League formed as a coalition of pro-Russian hacktivists including CARR, CyberVolk, and over 50 other active personas. This alliance represents a substantial threat, targeting NATO, European nations, Ukraine, and Israel. Their coordinated capabilities heighten risks for industrial organizations globally.

Hacktivists Claim Impacts to Critical Infrastructure

Hacktivism is a contemporary form of digital activism. It employs tactics like launching distributed denial of service (DDoS) attacks, defacing websites, and accessing internet-exposed devices to draw attention to political or social causes amplified through social media. These hacktivist personas may appear as formal groups or individuals, but, in practice, their names and branding are self-proclaimed monikers rather than established organizational entities.

Since 2022, hacktivists increasingly use freely and commercially available tools, such as Shodan, Censys, or Kali Linux, to discover and exploit vulnerable or misconfigured targets, including OT/ICS OEM products.

OT-CERT Notifies TAT24-76 Victims of HMI Compromise

Dragos OT-CERT is the Operational Technology – Cyber Emergency Readiness Team dedicated to addressing the OT resource gap that exists in industrial infrastructure. Designed to support asset owners and operators of industrial infrastructure, Dragos OT-CERT provides free cybersecurity resources for the OT/ICS community.

In September 2024, Dragos discovered a Python-based malware named kurtlar.exe/kurtlar_scada.exe. The malware connects to internet-exposed VNC servers and captures a screenshot of the access. Using evidence from the malware, Dragos identified a Telegram channel where TAT24-76 claimed to have used kurtlar.exe to compromise several internet-exposed VNC servers hosting HMIs.

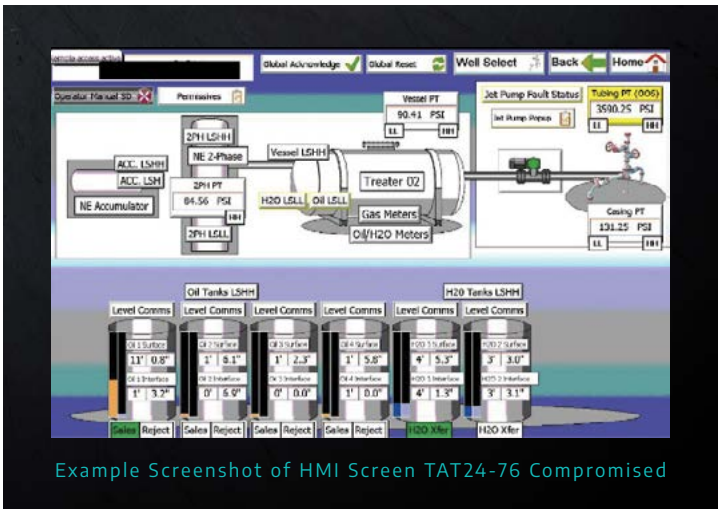
Dragos uses Temporary Activity Threads (TATs) for tracking and disseminating information about unidentified or developing cyber threat groups or activity. TATs serve as a provisional classification for clusters of cyber threat activities that have not yet reached a level of analytical rigor to be designated as a threat group.

TAT24-76 developed kurtlar.exe/kurtlar_scada.exe and advertised a variety of offerings in their channel, including:

- Initial access into organizations, public and private, via web shells

- VNC access to HMI and SCADA devices
- Exploits (primarily focused on WordPress)
- Database dumps
- DDoS tools
- A VIP channel containing private hacking courses (including how to identify Internet-exposed devices, additional exploits, and malware)

TAT24-76 uses their Telegram channel to sell their malware by showing evidence of successful compromises. This evidence included screenshots of compromised HMIs, as seen in the graphic at right.

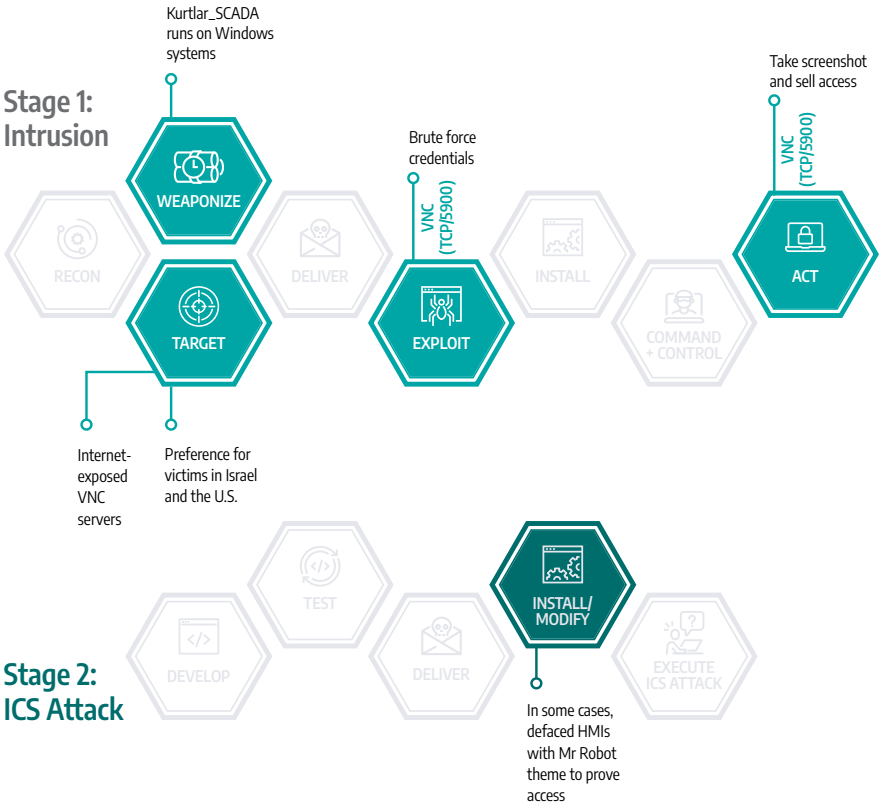


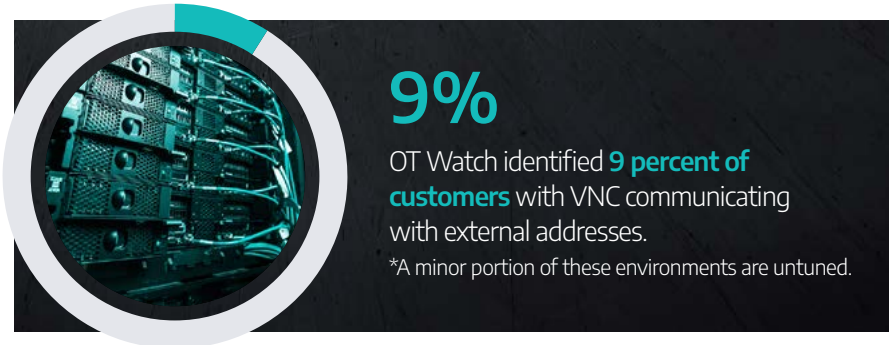
Example Screenshot of HMI Screen TAT24-76 Compromised

After investigating the screenshots, Dragos determined that a subset of the victims were compromised and notified them through Dragos's OT-CERT victim notification service. OT-CERT successfully notified compromised victims, restricting access to TAT24-76 and further manipulation from buyers.

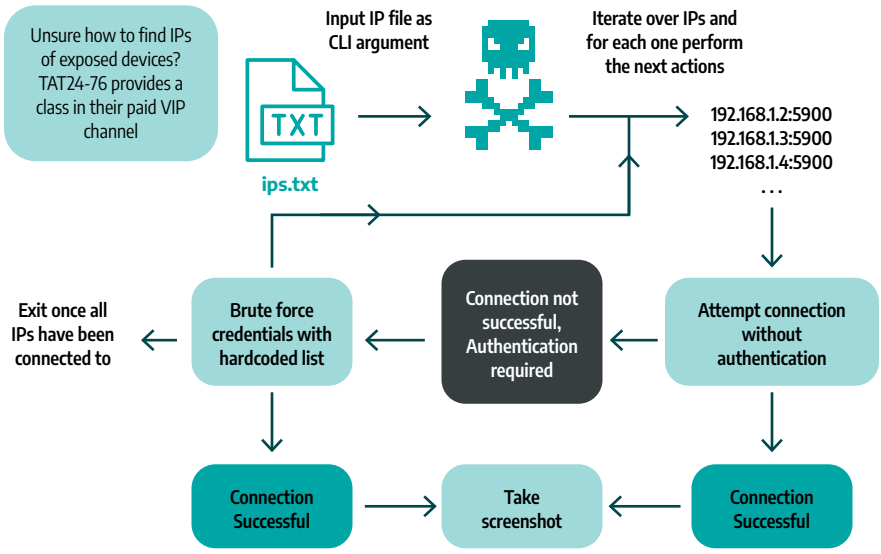
Despite their simplicity, kurtlar.exe and kurtlar_scada.exe are still effective against internet-exposed and poorly secured industrial devices running VNC servers. Strategies to mitigate this threat include:

- Restricting access to any VNC server, especially on ports TCP/5800, TCP/5900, and TCP/5901. If remote access is required, use a VPN.
- Ensuring default and weak credentials are changed.





Execution Flow of kurtlar.exe and kurtlar_scada.exe



The kurtlar.exe / kurtlar_scada.exe VNC Malware

kurtlar.exe iterates through a list of target IP addresses.

kurtlar_scada.exe attempts to connect over VNC on TCP ports 5800, 5900, and 5901, trying a hardcoded list of credentials. If successful, it captures a screenshot, with the IP address and credentials used.

CyberArmyofRussia_Reborn and Z-Pentest

The CyberArmyofRussia (CARR), tracked by Dragos as TAT24-22, is a self-proclaimed pro-Russia hacktivist group. TAT24-22 targets NATO and Eastern European countries to gain clout and likely formal support from the Russian government.

TAT24-22 uses DDOS attacks and accesses internet-exposed OT/ICS devices. However, it is debatable whether they understand the interfaces of OT/ICS devices they gain access to or the impacts caused by their manipulations. In numerous incidents, after accessing an OT device, they miscategorized the device's location and industry facility type. While their skillset is debatable, there are confirmed attacks on U.S. water and wastewater and energy facilities, causing various levels of disruption. There are probable attacks targeting organizations in:

- Water & Wastewater in Romania, Poland, and France
- Food & Beverage in Spain,
- Energy in United States and Germany

Based on their confirmed attacks and operations targeting OT/ICS organizations, the U.S. Department of Treasury sanctioned the members of CARR in July 2024.[39]

In September 2024, Z-Pentest, tracked by Dragos as TAT24-56, emerged on the scene and took on most operations targeting internet-exposed OT/ICS devices.

Hunt3r Kill3rs

The hacktivist persona Hunt3r Kill3rs, tracked by Dragos as TAT24-45, escalated its activities by targeting internet-exposed OT/ICS devices in Europe, Israel, and the United States, and focusing on weak or default authentication settings.

Despite possessing limited technical capabilities, Hunt3r Kill3rs achieved Stage 2 of the ICS Cyber Kill Chain for the third time, manipulating device data fields and resetting passwords on exposed controllers. Although Dragos could not verify operational impacts from the victims, these compromises could cause loss of control, loss of view, and operational disruptions.

[39]Treasury Sanctions Leader and Primary Member of the Cyber Army of Russia Reborn – U.S. Dept. of the Treasury

Hunt3r Kill3rs' opportunistic targeting and visibility on Telegram underscore a growing threat to industrial environments, particularly where even trivial compromises can cause operational disruptions. Dragos has observed Hunt3r Kill3rs leveraging internet-exposed devices to garner notoriety. This behavior aligns with broader trends among self-proclaimed hacktivists.

Convergence of Adversaries and Hacktivists

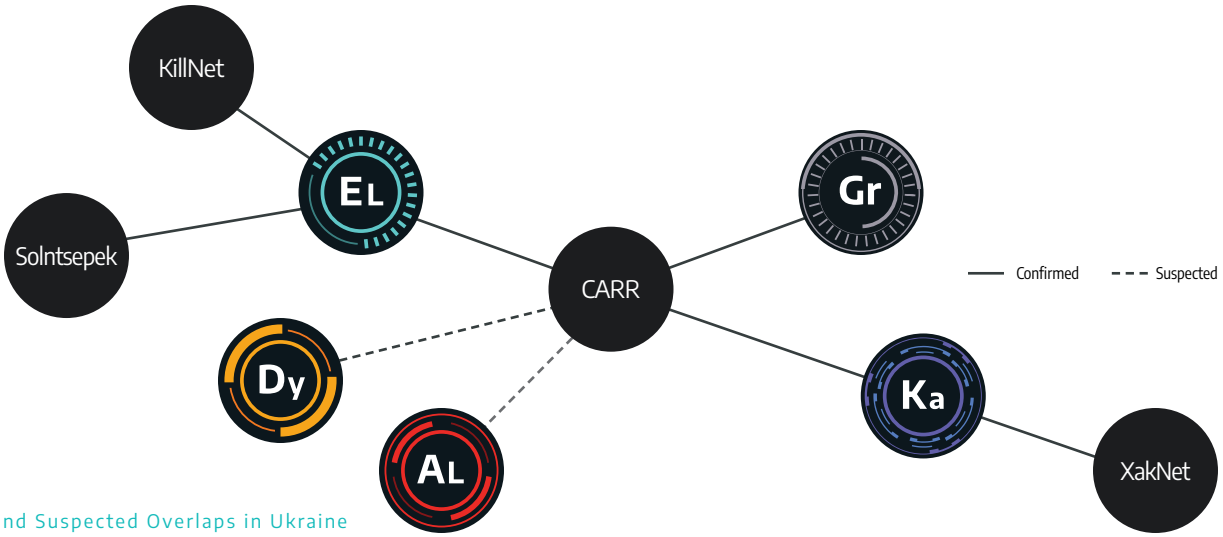
There is a growing convergence of interests between sophisticated adversaries and hacktivist personas. Dragos has seen them both use shared infrastructure and intelligence to attack OT/ICS targets. Since at least 2022, Dragos has confirmed convergence between:

- GRAPHITE and CARR
- KAMACITE and CARR
- ELECTRUM and CARR
- ELECTRUM and KillNet
- ELECTRUM and Solntsepek
- KAMACITE and XakNet

There is also suspected convergence between:

- DYMALLOY and CARR
- ALLANITE and CARR

The strategic implications for ICS defenders are significant, as adversaries may transition between espionage-focused campaigns and destructive operations based on broader objectives while leveraging hacktivist personas to conduct lower-sophistication attacks. The role of hacktivist personas, whether as a deliberate distraction from the primary attack or for other purposes, remains a subject of ongoing analysis and debate.



Confirmed and Suspected Overlaps in Ukraine

The Ransomware Landscape

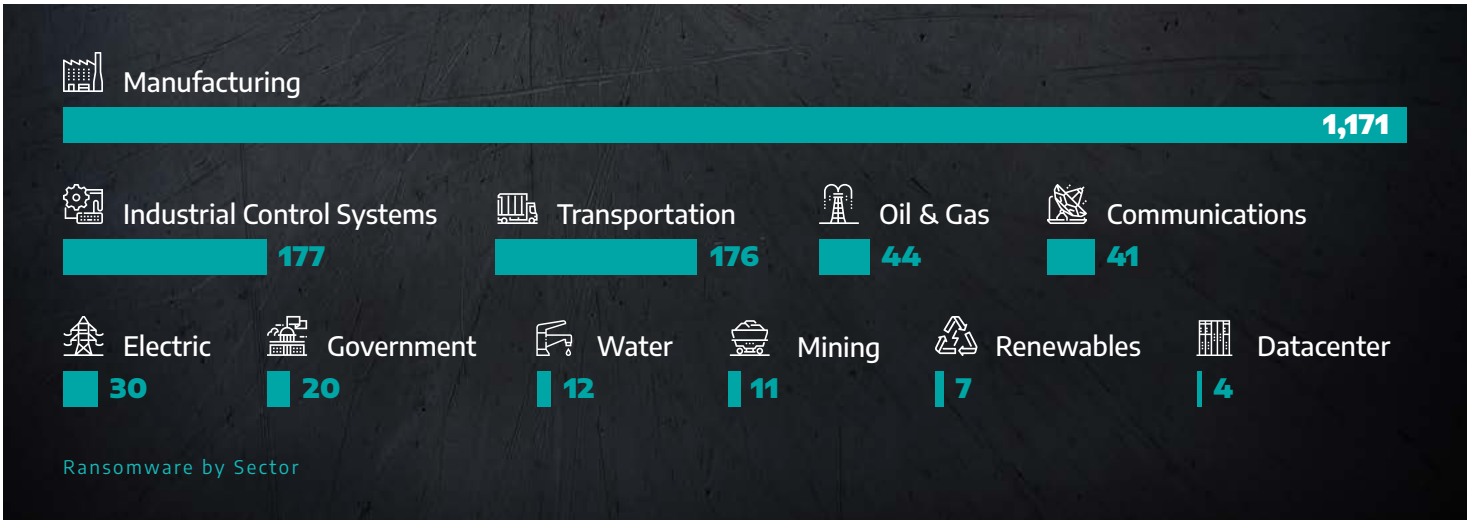
Ransomware is viewed as a legitimate threat for multiple industries because of the disruptive nature of a successful attack. Dragos first observed an uptick in ransomware attacks against industrial organizations in 2022, and since then, the number of attacks has doubled year over year.

In 2024, Dragos observed 1,693 industrial organizations with sensitive data and information posted onto various ransomware groups' dedicated leak sites (DLS). Although a DLS posting is not indicative of a successful ransomware attack on its own, the sheer volume and clear upward trend of industrial organizations getting attacked by numerous ransomware groups clearly highlight that all OT/ICS asset owners and operators and industrial organizations must be mindful of the current ransomware threat landscape and how it pertains to their respective security posture and operations.

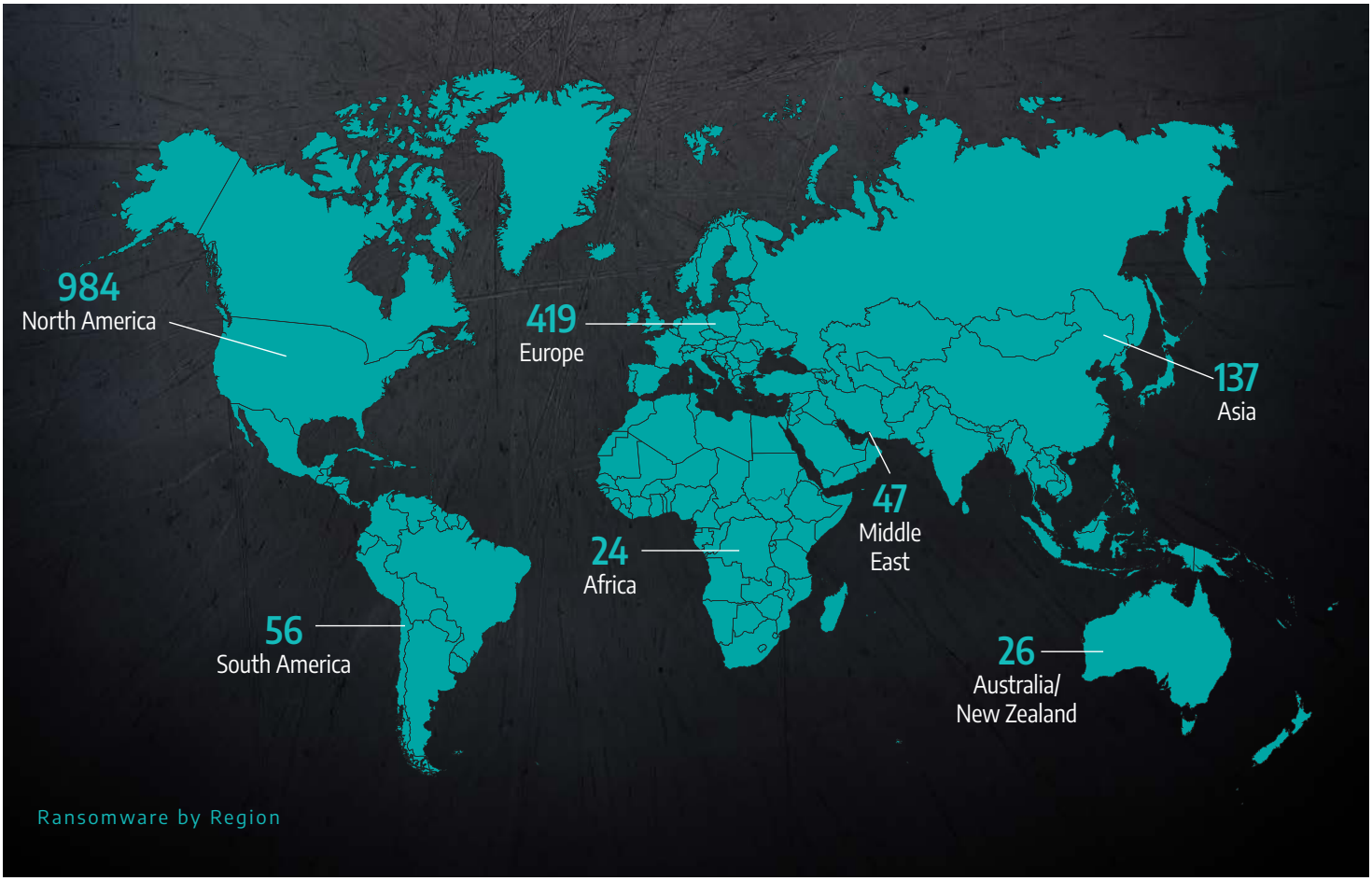
There was more than double the number of attacks in the second half of 2024 over the previous two quarters. It is unclear what factors might have driven an increase in ransomware activity. Possible contributors could include law enforcement actions taken against prominent ransomware groups earlier in the year, an increasing number of intrusion vectors as the year went on, and/or the emergence of new ransomware adversaries later in the year.

> Although Dragos did not observe any specific ICS-tailored ransomware variants in 2024, ransomware adversaries halted production lines, impaired supply chains, and exfiltrated sensitive data that could easily be used in follow-on malicious activity. It is very likely ransomware operators in 2024 implemented some level of victim selection with a preference towards organizations with a low tolerance for downtime.

Manufacturing remains the top target for ransomware attacks against industrial organizations; more than 50 percent of all observed ransomware victims were in the manufacturing sector, representing 1,171 attacks. Ransomware groups know that even brief disruptions can cause significant financial and logistical fallout, putting safety at risk and making manufacturers more likely to pay. Other industrial sectors, including energy, transportation, and industrial control system vendors, also remain high on the list as ransomware groups refine their tactics to



Ransomware by Sector



maximize pressure and impact. With these threats showing no sign of slowing, organizations must prioritize resilience, proactive defenses, and incident response readiness.

Ransomware attacks against industrial organizations are not evenly distributed, and certain regions bear the brunt due to geopolitical tensions, economic incentives, and adversary focus. North America accounted for 984 attacks – 58 percent of all cases. Europe followed with 419 attacks, making up 25 percent of the total. Understanding these regional patterns is key to strengthening defenses, anticipating future threats, and ensuring security strategies align with real-world risks.

Dragos tracked nearly 80 ransomware groups in 2024, a 60 percent increase from the 50 groups observed in 2023. Collectively, these groups attacked an average of 34 industrial organizations per week during the first half of 2024. That number more than doubled during the second half of the year (see chart next page).

The most active ransomware groups against industrial organizations were RansomHub, Fog, and LockBit3.0. Notably, RansomHub quickly escalated activities starting in February 2024 by attracting ransomware affiliates from Cyclops and Knight. They claimed more than 300 victims across multiple critical infrastructure sectors in 2024. Fog similarly expanded their operations into industrial sectors as 2024 went on and they were also one of the primary ransomware groups observed targeting vulnerable remote services and appliances. LockBit3.0 operations were disrupted by the international law enforcement effort "Operation Cronos" in February 2024, but they were persistent and remained a viable threat to industrial organizations throughout the year.[40, 41]

[40]The NCA Announces the disruption of LockBit with Operation Cronos - NCA; [41]Unveiling the Fallout: Operation Cronos' Impact on LockBit Following Landmark Disruption - TrendMicro

DRAGOS
SAFEGUARDING CIVILIZATION

Ransomware by Group/Strain

Ransomware Trends in 2024

Dragos observed two noteworthy trends within the 2024 ransomware threat landscape:

- Ransomware adversaries using remote tools and services.
- Convergence of geo-politics, hacktivism, and ransomware.

Ransomware Adversaries Using Remote Tools and Services

Starting in 2023, Dragos noted a general trend of adversaries targeting remote services and taking advantage of the lack of basic network security defense principles. That trend continued in 2024 as ransomware adversaries largely used these resources – particularly VPN appliances – to gain initial intrusion into victim networks and move laterally through compromised systems, thereby achieving Stage 1 of the ICS Cyber Kill Chain. Ransomware adversaries were also observed leveraging credential-based tactics, including pass-the-hash, brute force, and credential-stuffing techniques to bypass multi-factor authentication (MFA). Two examples of this are as follows:

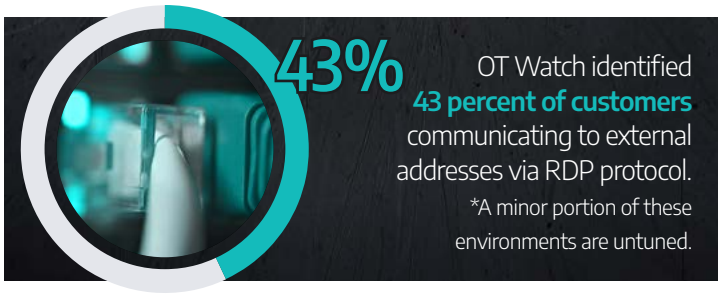
- Eldorado and Play ransomware groups attacked VMware ESXi environments to encrypt or disable virtual machines.[42, 43]
- Akira ransomware group consistently exploited vulnerable VPN appliances to gain initial access throughout 2024.

In addition to taking advantage of vulnerable remote services, ransomware groups also continued using LOTL strategies by using native administrative tools (e.g., PowerShell, certutil.exe, PsExec) to conceal malicious activities and remain undetected for extended periods of time.

Of the ransomware incidents Dragos responded to in 2024, victim organizations that enforced strict network segmentation between IT and OT systems and conducted offline backup testing significantly shortened the recovery times and avoided paying the ransom. Conversely, organizations that did not employ network segmentation and had poorly secured remote access pathways led to more lengthy recovery times, more involved incident response efforts, more severe production downtime, and increased remediation costs.

Dragos's incident response efforts for ransomware victims mirrored much of the observed "targeting remote services" trend. In fact, more than 50 percent of the ransomware incidents Dragos responded to in 2024 involved some element of a remote service, such as a VPN appliance or remote desktop protocol (RDP) server being leveraged by adversaries. Further, 25 percent of the ransomware incidents resulted in a full OT/ICS shutdown, and the other 75 percent of the incidents resulted in partial disruptions.

Dragos's observations from incident response engagements were reflected within the ransomware ecosystem where initial access brokers (IABs) commonly exploited unpatched vulnerabilities in hypervisors, VPN appliances, and remote access solutions, often within hours of public disclosure, granting ransomware affiliates



[42]New Eldorado Ransomware Targets Windows, VMware ESXi VMs – Bleeping Computer; [43]Play Ransomware Group's New Linux Variant Targets ESXi, Shows Ties with Prolific Puma – Trend Micro

a low-barrier-of-entry method for attacking industrial organizations and establishing a critical foothold within victim's environments.

These findings strongly indicate that numerous ransomware groups are leveraging low-barrier-of-entry intrusion tactics against industrial organizations and capitalizing on a lack of basic network and security hygiene practices. Until these elements are properly addressed and secured, ransomware groups will continue exploiting them.

Convergence of Geo-Politics, Hacktivism, and Ransomware

In 2023 and into early 2024, Dragos observed a trend of hacktivist groups, or self-proclaimed hacktivist groups, actively targeting and achieving Stage 2 of the ICS Cyber Kill Chain against industrial organizations and critical infrastructure and services worldwide. A new concerning evolution in the hacktivism threat landscape emerged in 2024, with hacktivist and self-proclaimed hacktivist groups employing ransomware as part of their operations against a variety of targets.

Three notable hacktivist groups were actively using ransomware within their operations in 2024: Handala, Kill Security, and CyberVolk.

CyberVolk is the most unique example due to their launching a ransomware-as-a-service (RaaS) in June 2024 and then announcing they were developing a proprietary "CyberVolk" ransomware in July 2024.[44] CyberVolk is a self-proclaimed member of the hacktivist alliance called Holy League, whose membership includes hacktivist personas such as CyberArmyofRussia_Reborn (CARR), and they primarily target NATO-aligned countries using DoS attacks and ransomware. Based on their activities and claims on social media, CyberVolk appears to support Russian state interests.

There's a realistic probability that this fusion of economic, political, and ideological interests has the potential to shape the ransomware threat landscape in 2025 and beyond, particularly in sectors critical to public safety and economic stability that are viewed as strategic targets of interest by hacktivist and self-proclaimed hacktivist groups. Consequently, OT/ICS asset owners must become more geopolitically aware if their organizations operate within certain high-tension regions or are in sectors that supply critical services and utilities to the public.

[44]Ransomware Groups Demystified: CyberVolk Ransomware - RAPID7

Insights from Dragos Incident Response

Throughout 2024, Dragos Incident Response mainly observed three kinds of incidents: ransomware compromise, operational errors, and legacy malware infection. Incidents involving ransomware or operational errors led to either partial or full disruption to OT operations. Legacy malware continues to be a problem in OT environments and leads to a weaker security posture.

Ransomware Incidents

Ransomware compromises accounted for the majority of cases that Dragos responded to, with 25 percent resulting in a complete shutdown of an OT site, and 75 percent resulting in at least some disruption to operations. Twenty percent of all incidents involved an exploitation of remote access, including VPN exploits, remote access applications, and RDP from corporate.

While data exfiltration is common in IT-related ransomware incidents, Dragos did not find signs of an adversary exfiltrating data from OT environments. Even though the adversaries explicitly threatened organizations with data exfiltration and disclosure as part of their ransom demands, they failed to act on those threats. No ransoms were paid, and organizations possessed adequate capacity to restore operations without engaging adversaries. Despite this capacity to recover, Dragos noted that backups were not always readily accessible and that sites were often materially impacted as part of incidents reported this year.

Operational Errors Causing Incidents

Aside from ransomware, the next highest type of incident was operational errors due to hardware misconfiguration, hardware failure, or human error. Each incident involved a disruption to operations to some degree. Although each of these incidents was initially reported to Dragos as potentially related to adversary activity, an investigation by incident responders concluded that they were not OT-related cybersecurity incidents. Dragos recommends that organizations activate their incident response retainer even if it is unclear if they are dealing with an event caused by an adversary. With their abilities to analyze network and host data, incident responders provide a capability that process engineers and operators often lack. This alone can significantly reduce the time needed to complete root cause analysis, thereby decreasing mean time to recovery.

Legacy Malware

Dragos Incident Response also encountered incidents due to legacy malware. Though similar to ransomware, Dragos tracks this separately due to strains such as WannaCry and other malware historically present within OT systems. This malware lingers within legacy environments and uses exploits successfully due to inadequate patching, architectural deficiencies, and other factors introduced by out-of-date operating systems. Often, the malware discovered is found "headless" in that the malware will continue to spread but will not be accessible by any recent adversaries. While the presence of headless malware is not an indicator of an active intrusion, it degrades general cybersecurity readiness and leads to time-consuming remediation efforts. Further, the security monitoring alerts generated by headless malware can be symptomatic of wider issues such as additional policy violations and poor patching practices.

The Importance of Network Security Monitoring

ICS protocol aware network visibility is key in quickly scoping the extent of a potential compromise and identifying systems to further analyze the root cause of a compromise. In one case, due to the Dragos Platform having been deployed at the affected site before an incident, and the Dragos OT Watch team actively monitoring the Platform, root cause analysis, remediation, and mitigation was performed in about 15 hours.

In other cases, even when monitoring was deployed post-incident, it still played a key role in significantly shortening the time needed to make an informed decision about reconnecting an isolated OT network, thereby minimizing downtime. If network-based security monitoring was not feasible for whatever reason, the analysis for scoping and root cause depended entirely on host-based forensics and log review. This not only demanded considerable effort to collect forensic data from OT systems in the field, but also significantly extended the time required for analysis.

If process logs did not record setpoint changes or read operations, it would be impossible to verify access and potential process manipulation. Deploying ICS protocol aware networking monitoring pre-incident would have detected read/write communication to controllers, making it easier to verify potential process manipulation. Even if the root cause is human error or hardware failure, monitoring helps identify the issue more quickly, reducing both analysis time and overall downtime.

The Basics Matter

It bears repeating that an organization that is implementing the SANS ICS 5 Critical Controls will be able to significantly reduce the impact to OT in case of a breach, likely have enough time to react to a breach before it turns into a full compromise, will be aware of key processes and systems to protect and collect data from if analysis is needed, and have incident response playbooks that focus on the most likely scenarios, allowing responders to streamline their efforts. Investing in the efforts of doing the basics right, will result in less impact and lower downtime.

Vulnerabilities

Industrial systems weren't built with cybersecurity in mind, yet today's adversaries are actively hunting for weaknesses in OT devices and protocols. From unpatchable flaws to design limitations, these vulnerabilities create openings for adversaries to disrupt operations or gain initial access. As threats evolve, so must our approach - focusing not just on patching, but on understanding and mitigating risks before they can be exploited.

Fieldbus: Servo Drives Drive New Research Areas

Dragos continued fieldbus protocol research in 2024.[45] This year, research focused on the CANopen protocol implemented in servo drives. A major finding from this research was highlighting the risk that layered protocols like CANopen pose to organizations and the lack of detection mechanisms for those attacks. These layered protocols are called 'Turducken' protocols and have been identified as a new area to explore. In the short-term, Dragos now has signature-based detections for a variety of attacks using CANopen over a common PLC network protocol. Longer-term, Dragos plans to implement tooling to address Turducken protocols in fieldbus equipment. his tooling will provide greater visibility for detecting attacks and identifying potential misconfigurations.

Turducken protocols are application layer protocols which are layered atop one another. In the case of Dragos's 2024 research, the protocol layers were Modbus-RTU, layered atop CANopen, which was layered inside of the proprietary CODESYS protocol. During documentation review, Dragos also identified products which layer Modbus-RTU atop CANopen atop Modbus/TCP.

Previously, Dragos researched a number of Turducken protocols related to LOGIIC Project 12, where the HART protocol was often layered on top of both proprietary protocols and common industrial protocols.[46] In a different

[45]Fieldbus - Wikipedia; [46]Excerpt: LOGIIC's Project 12 Safety Instrumentation Report – Global Cybersecurity Alliance

effort, Dragos researched Omron devices which showed EtherCAT layered over a proprietary NXBus protocol, itself placed inside of HTTP requests.[47]

Dragos considers most fieldbus equipment as insecure-by-design. This means that engineering issues exposed by the bottom-level protocol are not necessarily worthy of CVEs. Still, detections should determine if attacks, or even erroneous changes, are made against this equipment.

These protocols are often composable (as with Modbus-RTU/CANopen/X, where X may be CIP or CODESYS or Modbus/TCP), and each layer of the composable protocol has its own quirks, such as fields with variable lengths, request pipelining, and even undocumented functionality, making it difficult to write network-based analytics for them.

As interest increases in identifying attacks against low-level equipment, the natural engineering response should be composable dissectors: the ability to easily extract an inner payload and pass it to a choice of inner dissectors, ad infinitum, until the entire Turducken is unraveled. Looking through Dragos Neighborhood Keeper datasets, "several models of PLCs with Turducken protocol support were identified. Dragos Neighborhood Keeper is an opt-in collective defense and community-wide visibility solution that enables a more informed industrial defense by sharing threat intelligence across industries and geographic regions. Several PLC models with Turducken protocol support include:

- Rockwell Automation ControlLogix systems with HART-aware IO modules. These modules allow direct access to instrumentation, including attacks outlined in LOGIIC Project 12.
- Schneider Electric controllers using CODESYS runtime and CANopen support. These devices provide direct SDO access to CANopen devices including the ability to reconfigure and remotely operate these components, out of band with the process control logic.

Fortunately, end user security recommendations for both types of exposure can be performed using control systems logic itself.[48] Sensitive settings can be monitored by the controller logic, with safe shutdown logic executed if device settings are changed out-of-band.

To protect fieldbus equipment, ICS community awareness must change. A common assumption is that field devices, and especially instruments and actuators, are insecure-by-design. What is not well-considered by owners is the accessibility of this equipment.
If you use a device type manager (DTM) to manage fieldbus equipment over an Ethernet network, the underlying protocol for access may not be secure. While the protocol may be nested and appear complex or even nonsensical at first glance, the apparent complexity of the protocol may be overcome by researchers and threat groups.

If you do not use DTMs to manage your fieldbus equipment, the devices may still be exposed, so restrict access to engineering ports on, for example, PLCs which have fieldbus communications features and to fieldbus couplers and protocol translators. These devices may translate fieldbus protocols into more common Modbus/TCP, Ethernet/IP, DNP3, or other process bus protocols.
It is important to consider not just how you use and manage your devices, but also how they could be used and managed – potentially by someone other than you.

IoT Equipment in ICS Environments

Several vulnerabilities in IoT devices were exploited as recently as November 2024 to propagate the Mirai botnet, which maintained upwards of 15,000 active IP addresses used to conduct DDoS attacks.[49] This long-running botnet executes fully automated infection of IoT and OT devices allowing it to hide malicious processes, scan for vulnerable devices, proliferate, and update itself. This botnet is successful because most IoT equipment runs inadequately hardened, open source GNU/Linux under the hood.

[47]Exploiting Omron's NEX PLC Runtime and Protocol – S4, Logan Carpenter; [48]Safety Instruments Testing: Spotting and Stopping Process Attacks - Dragos; [49]Mirai Botnet Variant Exploits Four-Faith Router Vulnerability for DDoS Attacks – The Hacker News

With easy to exploit exposures such as TELNET or SSH enabled by default and trivial infection mechanisms like unauthenticated command injection, many of these devices have 'low-hanging fruit' type vulnerabilities that can give low-level access to tamper with the device firmware. The shared operating systems and CPU architectures of these devices make them vulnerable to existing tools. Thus, building management systems like HVAC, lighting, physical access control, and physical security systems are easy targets for adversaries. While these systems may not directly maintain production, an outage of any one of them can stop production. For example, if a lighting control system falls offline, workers may not be able to work. Similarly, in regulated environments such as pharmaceuticals and food manufacturing, loss of HVAC and climate control systems will often require production to halt. As such, it is best to view IoT hardware used in an industrial setting as a 'part of the process' from a plant perspective.

In 2023, Dragos analyzed a tool called IoT Exploit, an "IoT device vulnerability scanning, verification, and exploitation toolkit" that bundles more than a thousand publicly available exploits targeting IP cameras, NVRs, DVRs, routers, and industrial devices. It contains capabilities to capture Real-Time Streaming Protocol (RTSP) streams, perform brute forcing of authentication over multiple protocols, conduct DoS attacks, and more. IoT Exploit contains roughly 175 exploits targeting OT devices with the ability to speak numerous industrial protocols, as well as hundreds of additional exploits for generic IoT devices. While this toolkit appears to be a red teaming tool developed for vulnerability scanning purposes, its public existence will no doubt filter into automated tools. Dragos has no evidence of malicious use of the IoT Exploit toolkit in our telemetry. "Dual-use tools" – those created for research or defensive purposes with the ability to be used maliciously – are commonly used amongst adversaries. As such, there is a strong likelihood that IoT Exploit or some component of it will eventually be used maliciously.

One of the best ways to protect IoT systems is simple: identify and change default passwords. This is especially important in internet-exposed systems.[50] Additionally, restrict access to device management interfaces and monitor for exploitation of these devices. And, most importantly, have a plan in place should these systems stop functioning correctly. For example, the ability to manually turn off magnetic door latches should be a part of every plant's safety plan.

[50]OT Cybersecurity Best Practices for SMBs: Managing Default Passwords and Identifying OT/ICS Devices Exposed to the Internet - Dragos

Supply Chain and Third-Party Components: Acknowledging Hidden Risks

Third-party components expand or support the capabilities of OT equipment and systems. These components, often unknown to the end-users, can have vulnerabilities that compromise the security of the component and, consequently, the entire product into which it is built. Fortunately, these risks can be mitigated through vulnerability management, software bill of materials (SBOM) implementation, and other proactive strategies.

Third-party components are software or hardware modules created by an external entity other than the developer of the underlying core software. Often, these third-party components are designed by a company, developers, or research organizations to integrate products from different vendors and add functionality to products. For example, OEMs of industrial products may incorporate software modules from another vendor into their applications and equipment to add functionality, simplify integration, and improve compatibility with other systems.

Products often rely on third-party components, so any vulnerabilities in those components can directly impact the security and functionality of the dependent products. While a vendor-manufactured product, such as a PLC, may be up to date with its own security patches for issues under the vendor's control, it could still include a third-party add-on component with an unaddressed vulnerability. In such cases, the vendor might implement temporary mitigations to reduce the risk, but addressing the root cause of the issue would largely depend on the third-party creator to provide a proper fix.

In April 2024, the Bianlian ransomware group attempted to use the Palo Alto Networks PAN-OS vulnerability, CVE-2024-3400, against organizations in the water and wastewater, manufacturing, and mining sectors in multiple regions. Notably, the Siemens RUGGEDCOM APE1808 product integrates Palo Alto Networks PAN-OS as a third-party component. Since CVE-2024-3400 exists in PAN-OS, the Siemens product is susceptible to the same vulnerability. While there is no evidence of Siemens products being actively targeted due to CVE-2024-3400, this example highlights the risk of third-party components. The Siemens product's reliance on PAN-OS provides a potential avenue for exploitation to adversaries and, as a result, exposes the owning organizations to intrusion.

Practical Solutions for Managing Third-Party Risks

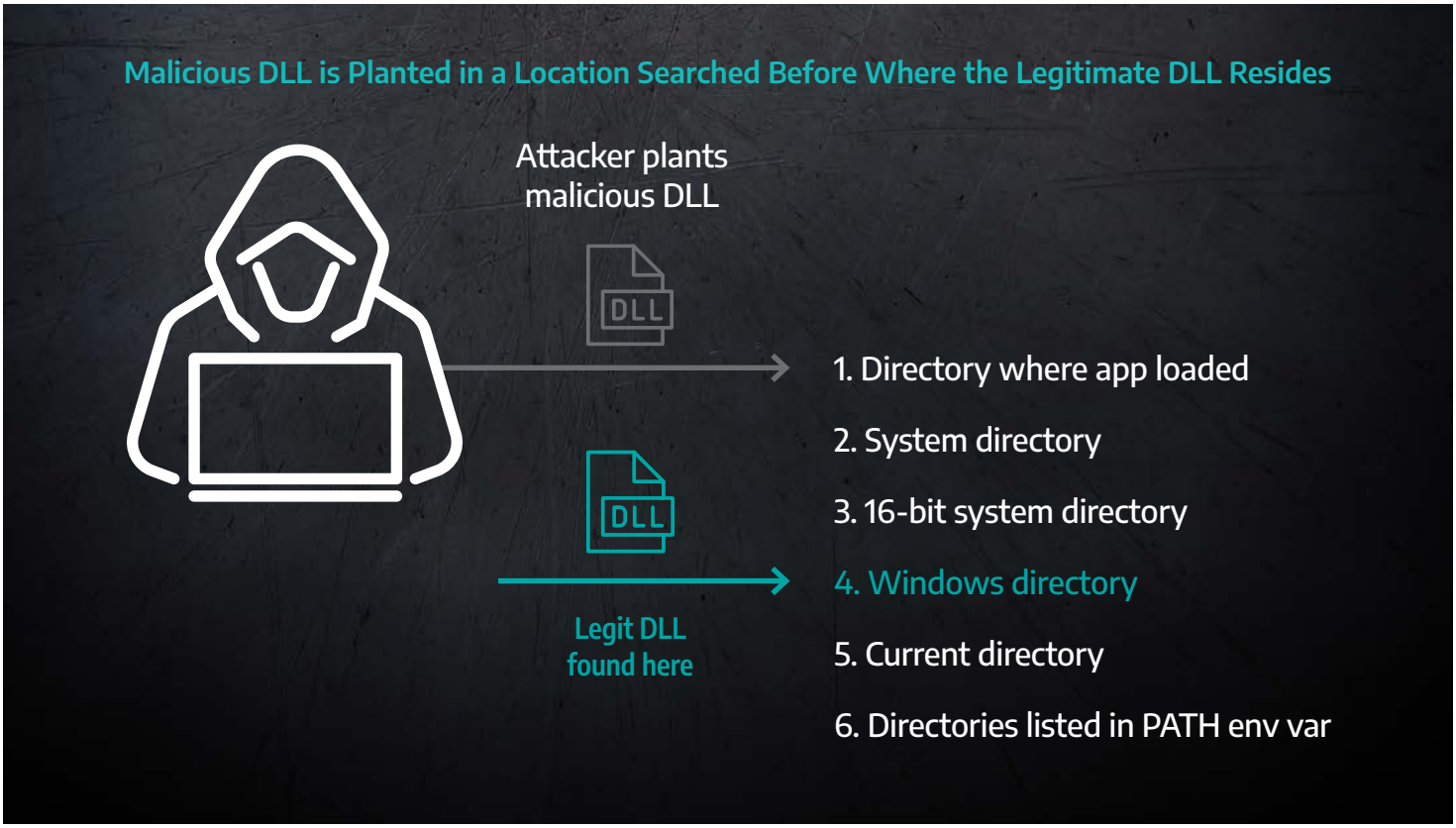
Asset operators and owners should focus on vulnerability management by identifying and addressing the most critical vulnerabilities in their environment. This approach helps reduce the likelihood of exploitation, protects critical operations, and keeps systems running smoothly by addressing risks before an adversary can take advantage of a vulnerability. The Dragos Platform, which supports risk-based vulnerability management and prioritization, can simplify this process. Additionally, following the SANS ICS 5 Critical Controls framework, which emphasizes actions like secure configurations and continuous vulnerability monitoring, can provide a structured and effective approach to managing these risks.[51]

For vendors, implementing an SBOM is essential.[52] This document should list all software versions and add-on components within a product. By providing clear visibility into a product's components, an SBOM enables faster and more efficient responses to critical vulnerabilities. This transparency fosters operational resilience and supports proactive risk management specific to third-party integrations.

DLL Hijacking: An Ongoing Problem for OT

Dragos currently tracks 104 dynamic-link library (DLL) hijacking vulnerabilities impacting industrial software. Dragos vulnerability researchers view these vulnerabilities as low-hanging fruit; they are usually easy to discover and exploit. These exploits are highly versatile and can allow an adversary to gain initial access, escalate privileges, evade detection, or gain persistence on a Windows host system.[53]

DLL hijacking is a type of vulnerability that abuses a DLL search order algorithm in the Microsoft Windows operating system to trick a vulnerable application into loading adversary-created code.



[51]The Five ICS Cybersecurity Critical Controls – SANS; [52]SBOM - CISA; [53]Suggested Practices to Defend Against DLL Hijacking - Dragos Inc.

Historically, DLL hijacking has been leveraged against industrial organizations several times.

Stuxnet exploited CVE-2012-3015 to trick Siemens SIMATIC manager software into executing a malicious DLL masquerading as S7hkimdb.dll, which then decrypts and loads the main Stuxnet payload with administrator privileges.[54] Stuxnet was deployed to slow Iran's development of enriched uranium.

APT10 used DLL hijacking to deploy credential theft tools in Operation Cloud Hopper, a cyber espionage campaign targeting multiple sectors, including industrial manufacturing, energy, mining, and more.[55]

MuddyWater leveraged DLL side-loading in the POWGOOP malware, a remote access trojan that targeted government, oil and gas, telecommunications, and more.[56] While remote access trojans (RATs) can allow adversaries to gain full administrative privileges and remote control of a target computer, public reporting indicates that this activity was primarily espionage-focused.

Cotx/CotSam/DNSep malware targeted military industrial organizations in Eastern Europe and Afghanistan and used DLL hijacking in security software to decrypt backdoors.[57] These backdoors provided arbitrary command execution and collected host information. Kaspersky states that analysis of threat activity indicates these malware families were deployed for cyberespionage purposes.

The Meatball and FourteenHi malware families targeted Eastern European industrial organizations and the Russian government. They used DLL hijacking to install a remote access trojan.[58]

MuddyWater used DLL hijacking to escalate privileges in a campaign against Israeli airlines and airports in September and October 2023.[59]

A variant of the HEADLACE malware family, a Batch-based backdoor used by GRAPHITE, contained a DLL side-loading component. CERT-UA reported that HEADLACE was used against a Ukrainian critical infrastructure entity.[60]

APT41 used DLL hijacking to execute the DUSTTRAP malware, a remote access trojan used against the automotive sector and shipping and logistics organizations.[61]

Dragos encourages ICS asset owners to hunt for DLL hijacking vulnerabilities in their systems and implement mitigations, such as:

- Enabling the CWDIllegalInDllSearch registry key on an application-specific basis.
- Following the principle of least privilege when running applications.
- Audit application directories to ensure *Everyone* and *Standard Users* groups do not have write access.

Dragos encourages OT vendors to review the Microsoft Dynamic-Link Library Security webpage for best programming practices to reduce the occurrence of the vulnerability in their software products.

[54]Stuxnet 0.5: The Missing Link – Symantec (via gwu.edu); [55]Operation Cloud Hopper - PwC, BAE; [56]MAR-10369127, MuddyWater – CISA; [57]Targeted attack on industrial enterprises and public institutions – Kaspersky; [58]Common TTPs of attacks against industrial organizations – Kaspersky; [59]Iranian Nation-State APT Groups 'Black Box' Leak - ClearSky; [60]APT28 Cyber attack – CERT-UA; [61]APT41 Has Arisen From the DUST – Mandiant

"Now, Next, Never" Vulnerability Framework

The Common Vulnerability Scoring System (CVSS) is inadequate for prioritizing vulnerabilities in ICS.[62] CVSS relies on numerical scoring to evaluate vulnerabilities based on technical attributes, but it was not originally designed with industrial systems in mind. As a result, CVSS lacks the contextual information necessary for conducting risk assessments specific to ICS. For example, CVSS fails to account for whether a vulnerability impacts the ICS process, or if mitigating a vulnerability will render a device inoperable for the owner. To address these situations, Dragos developed a framework for sorting vulnerabilities into three categories: Now, Next, and Never. This framework helps asset owners identify and prioritize the vulnerabilities with the highest risk to their operational process.

Dragos monitors emerging threats, their techniques, and the vulnerabilities they exploit. The "Now, Next, Never" model helps accurately capture the true impact of these vulnerabilities, empowering organizations with the guidance needed to respond effectively to emerging threats.

The high-level vulnerability attributes covered by this process include:

- Impacts to Operations
- Active Exploitation or Public Proof-of-Concepts
- Network Exploitability
- Insecure-by-Design Features and Mitigation Availability
- Authentication and User Interaction Requirements
- Broader ICS Network Access Capabilities

Now vulnerabilities are:

- Remotely exploitable
- Require no authentication or authentication is easily bypassed
- Impact ICS processes or allow new access to ICS
- Actively exploited by advisories or have a public proof of concept

Now vulnerabilities have a patch or alternative mitigation, such as restricting access to vulnerable ports, or proper engineering process design. **These account for 6 percent of vulnerabilities in ICS.**

Next vulnerabilities are:

- Remotely exploitable
- Not actively targeted by adversaries
- Could impact operations
- Require adversaries to do prep work such as credential stealing

Next vulnerabilities are mostly mitigated through good network hygiene or measures like network segmentation included as part of the Defensible Architecture control in the SANS ICS 5 Critical Controls. **These account for 63 percent of vulnerabilities in ICS.**

Never vulnerabilities are:

- Difficult to execute
- The same risk that exists inherently in ICS (insecure-by-design).

Never vulnerabilities **account for 31 percent of vulnerabilities in ICS**, and are not worth the effort to remediate.

[62] Common Vulnerability Scoring System SIG - FIRST

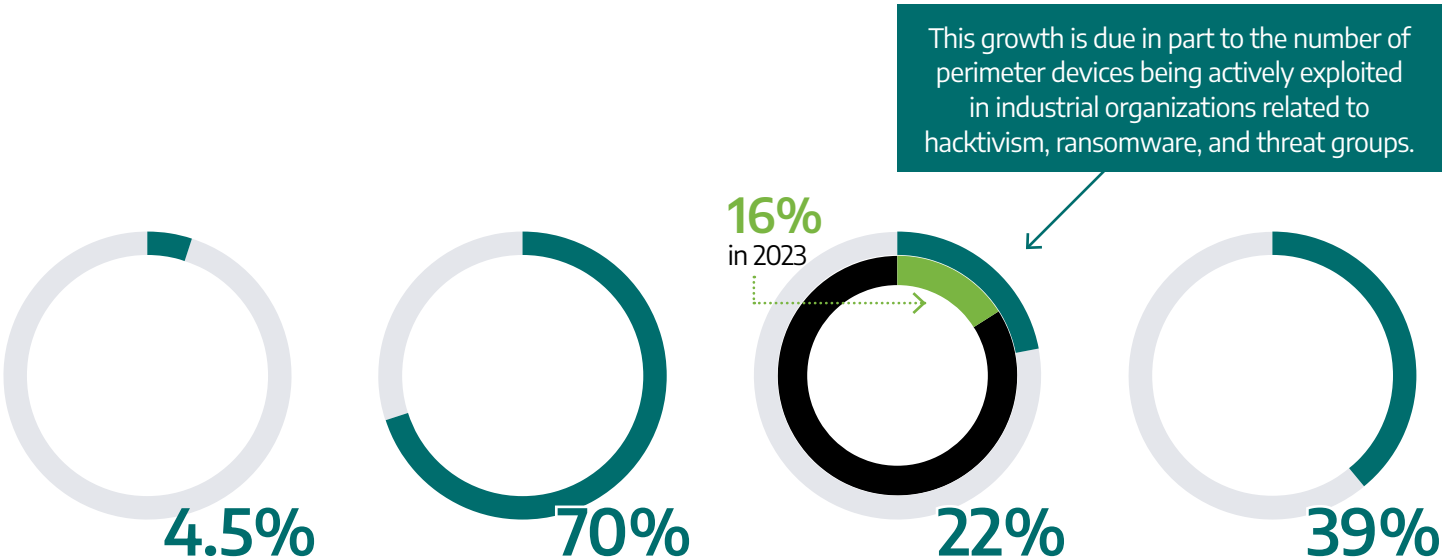
Vulnerability Trends

Because OT environments are subject to different regulations and must remain operational for safety and production, asset owners cannot mitigate system vulnerabilities in the same timeframe as in IT environments. While IT can be more flexible in allowing updates to mitigate vulnerabilities, OT's emphasis on maintaining day-to-day operations without interruption complicates vulnerability management and needs a strategic plan. Dragos focuses on vulnerability management with OT challenges at the forefront, focusing on protecting critical systems and mitigating risks while maintaining operational needs with little to no disruption.

Dragos prioritizes vulnerabilities that, if exploited, can cause a deep impact on industrial processes. Key considerations include:

- Are the vulnerabilities actively exploited?
- Do the vulnerabilities provide direct access to OT/ICS networks?
- Can the vulnerabilities cause a loss of view or loss of control to the process?

As our research has shown, CVSS scores alone often do not reflect the risk in operational environments. Dragos digs deeper to find true severity levels and mitigation options, score and accuracy corrections, and provide context to help defenders. In 2024, Dragos found that:



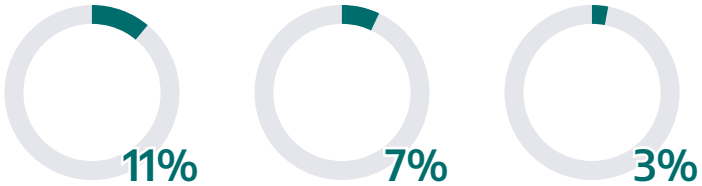
4.5%
of vulnerabilities had a Proof-of-Concept (POC) and were actively exploited

70%
of vulnerabilities were deep within the ICS network. This means that devices associated with the vulnerabilities were Purdue Level 3.5 and below, closer to the process.

22%
of advisories were network-exploitable and perimeter-facing

39%
of vulnerabilities could cause both a loss of view and a loss of control.

In 2024, 22 percent of advisories contained incorrect data, which can prevent accurate prioritization for patch management and mitigation.



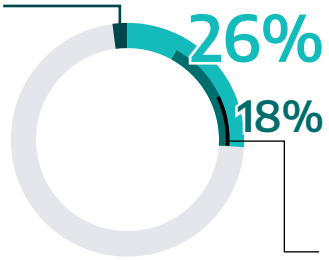
11% of CVEs **HAD ERRORS** in them, which makes it more difficult to prioritize correctly

7% were **MORE SEVERE** than the public advisory

3% were **LESS SEVERE** than reported

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

Only **2%** provided alternate mitigations to a provided patch or primary mitigation advice.

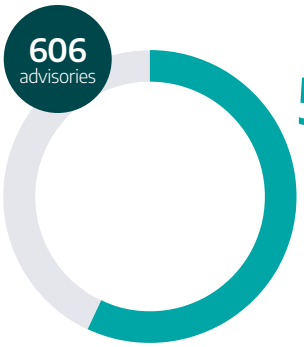


26% of public advisories offered **no patch**.

18% of public advisories had **no patch** and **no mitigation.**

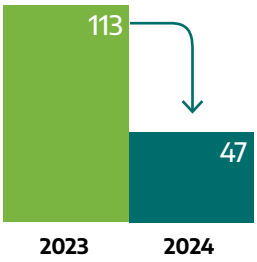
47% **Dragos provided alternate mitigation** advice for 47 percent of advisories that were missing both patches and mitigations.

Out of 606 public advisories that Dragos assessed in 2024:



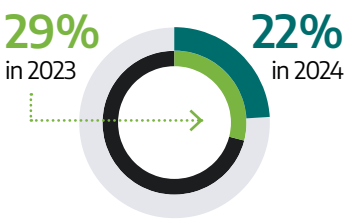
57% had a patch but no mitigations, a **3 percent increase from 2023**

The number of ICS-specific protocol network-exploitable vulnerability advisories that provided alternate mitigation **decreased by more than half:** from 113 in 2023 to 47 in 2024.



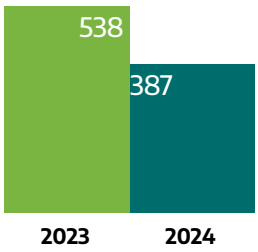
Overall, there was a marked decline in the number of errors seen in assessed CVEs from 2023 to 2024.

CVE errors



CVE errors fell from 29 percent in 2023 to 22 percent in 2024, indicating that **vendors and researchers are scoring vulnerabilities more accurately upon release.**

CVEs with Proof of Concepts



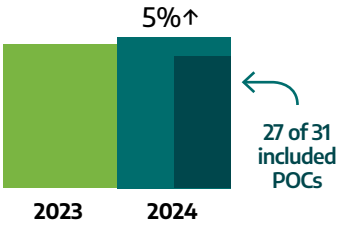
Dragos researchers also observed a drastic decrease in the total number of **CVEs with POCs**. In 2023, there were 538 CVEs with POCs and only 387 in 2024.

After more research...

151 (7 percent) of CVEs **scored higher** after further research

55 (27 percent) **scored lower**

Advisories with actively exploited CVE errors



In exploit analysis, 2024 saw an **increase by 5 percent** in the total number of advisories with CVEs that were actively exploited.

Call to Action

Industrial operations are now firmly in the crosshairs of state-sponsored threat groups, cyber criminals, and hacktivists, all seeking to exploit ICS vulnerabilities for espionage, disruption, and destruction. The 2025 OT/ICS Cybersecurity Report makes one fact abundantly clear: adversaries are evolving faster than defenders.

Adversaries are not just testing OT networks—they are actively embedding themselves within critical infrastructure, positioning for long-term access, operational disruption, and potential large-scale consequences. The use of living-off-the-land techniques, ICS malware, and targeted reconnaissance proves that these groups understand industrial systems better than ever before.

Organizations can no longer afford passive defense strategies or outdated security postures. The time for reactive security is over. Defenders must move toward continuous monitoring, proactive threat hunting, and incident response capabilities tailored for OT environments. Foundational practices like the SANS ICS 5 Critical Controls still provide OT/ICS asset owners with the best means to prepare for potential cyber events stemming from geopolitical conflict.

#1 Incident Response Plan:

Update OT Incident Response Plans – or ensure that you have one. Adversaries are becoming more OT/ICS aware, and their tactics, techniques, and procedures (TTPs) are targeting deeper into industrial environments. Ensure your plans have ways to respond to and recover, for example whether SCADA servers have been encrypted by ransomware or BAUXITE-modified PLC logic.

#2 Defensible Architecture

Fully understand your attack surface. Proactively conduct annual attack surface analysis and prioritize network gateways and perimeter resources such as VPN, RDP, and SSH devices targeted by BAUXITE. One easy way to accomplish this would be to leverage tools such as Shodan and Censys to perform external analysis of assets that may be "exposed" to the public-facing internet. Once inside the network, audit firewall rules and validate the attack surface within the network to prevent lateral movement from adversaries like VOLTZITE with NP-View.

#3 Visibility and Monitoring

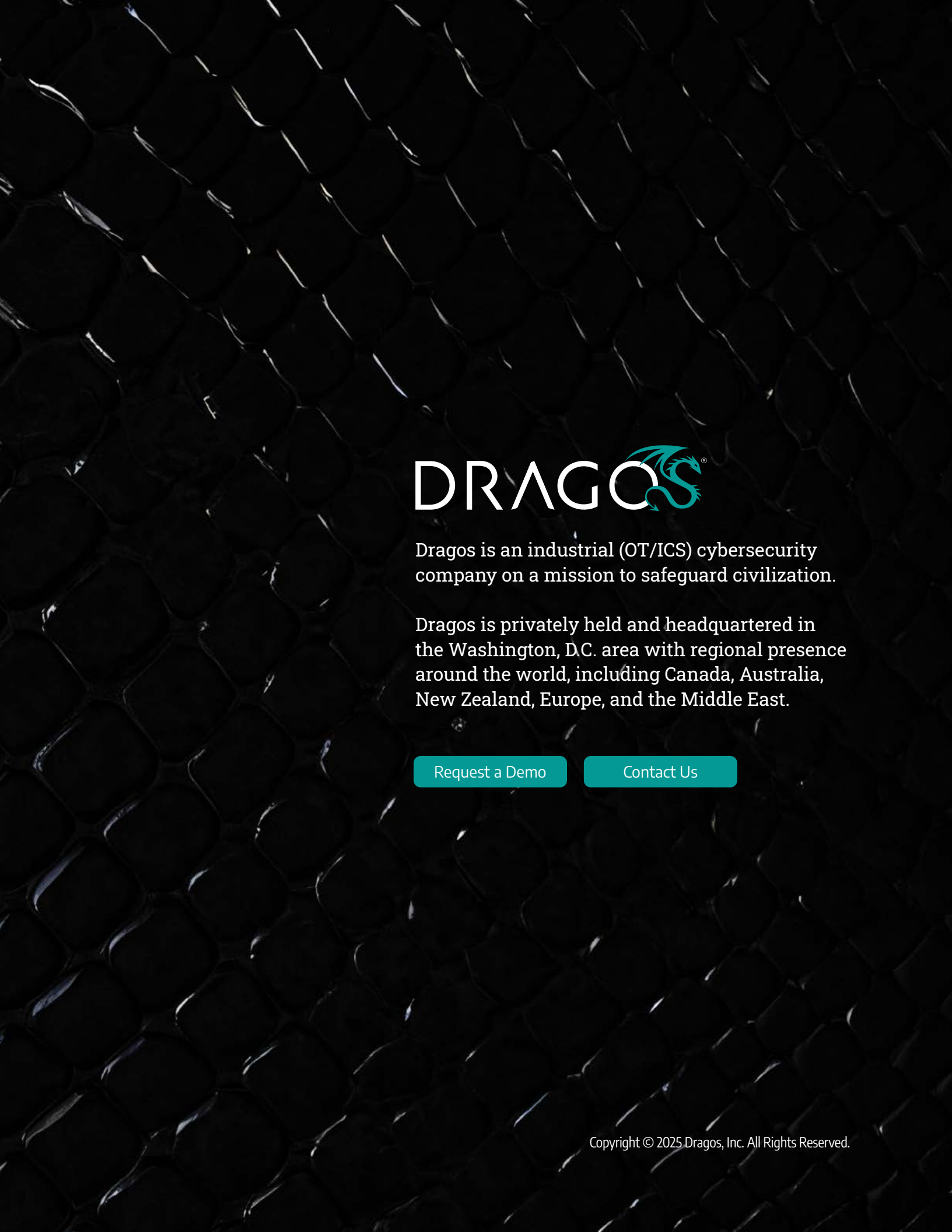
Increase visibility and monitoring. OT-aware monitoring solutions, like the Dragos Platform, can detect adversaries' subtle movements before they strike, steal information, or take other actions. The Dragos Platform also alerts on configuration and command code changes, helping teams decipher between security events and engineering mishaps.

#4 Secure Remote Access

Focus on remote access. Vendor remote access continues to be an attack vector seen in Dragos Incident Response cases. Ad hoc access points should undergo the same scrutiny as main firewalls and corporate VPN connections with increased access logging, alerting, and multifactor authentication.

#5 Risk-Based Vulnerability Management

Ensure your approach to vulnerability mitigation is strategic and focused on real-world threats that apply to your industry. Enrich your understanding of CVEs to verify they are accurate, focusing on those that will cause a loss of view or control of the process. Then, make a plan and execute the plan, even if it is a multi-year plan.



Dragos is an industrial (OT/ICS) cybersecurity company on a mission to safeguard civilization.

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

Request a Demo

Contact Us