DRAGOS

EXECUTIVE SUMMARY

FOCUS ON EUROPE

OT CYBERSECURITY

THE 2023 YEAR IN REVIEW

MAY 2024

TABLE OF CONTENTS

Executive Summary

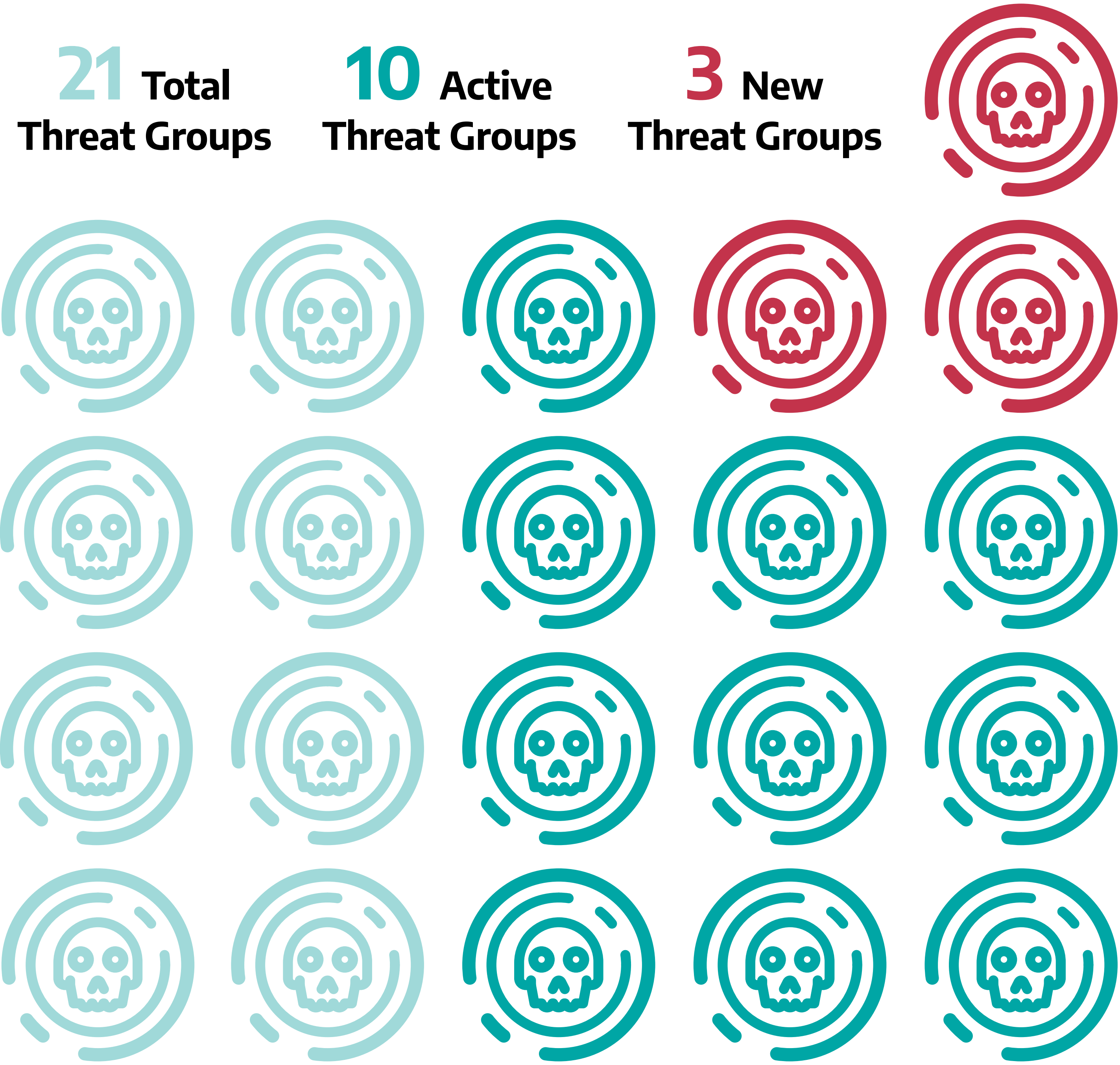
Several forces drove a surge of activity from adversaries targeting operational technology (OT) infrastructure in 2023, marking a pivotal shift in the OT cyber threat landscape for industrial sectors based in European markets. Motivated by mounting geopolitical tensions, sophisticated threat groups and hacktivists demonstrated the capacity to breach the networks of critical infrastructure and, in some cases, disrupt OT systems. With each passing year, the number of ransomware incidents globally climbs even higher, leading to cascading impacts for virtually every industrial sector, particularly manufacturing. Meanwhile, the number of vulnerabilities present in industrial control systems (ICS) continue to grow exponentially, along with the adversaries' appetite to exploit them.

Based on customer engagements across various industries within the past year, we saw that electric, oil and gas, water, and manufacturing sectors made moderate improvements in their OT cybersecurity posture on average, but industrial organisations still struggle with passwords and still more are unable to detect threats to their OT environment. It is time to take bigger strides. Addressing this challenge requires coordinated efforts from partners across the European cybersecurity community and, when necessary, emergency measures to mitigate adverse effects on critical business operations and the communities they serve.

Read on to get a summary view of the significant OT cybersecurity trends impacting European industrial infrastructure organisations in 2023. We offer up-to-date data on current threat groups, new and old, actively targeting industrial organisations. We highlight our ransomware and vulnerability findings, noting the industries and devices at increasing risk. And we provide frontline insights with actionable guidance to help you effectively defend against and respond to industrial cyber threats. We conclude with an overview of the five critical controls for OT cybersecurity to help you understand how to jumpstart your cybersecurity journey.

KEY HIGHLIGHTS: BY THE NUMBERS

Threat Group Highlights – 2023



21 Total Threat Groups

10 Active Threat Groups

3 New Threat Groups

Key Vulnerabilities Findings

80%

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

16%

of advisories were **network exploitable and perimeter facing** in 2023.

53%

of the advisories that Dragos analysed **could cause both a loss of view and loss of control,** up from 51% last year.

31%

of advisories **contained errors** in 2023.

49%

Dragos provided mitigations for 49% of the advisories that had none.

Key Ransomware Findings

↑ **50%**

Ransomware attacks against industrial organisations **increased 50 percent** over last year.

28%

Dragos tracked **28% more ransomware groups** impacting ICS/OT in 2023.

70%

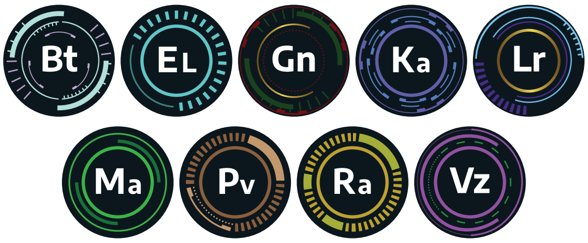
of all ransomware attacks targeted **638 manufacturing entities** in **33 unique manufacturing subsectors**.

2023 Dragos Threat Groups Summary

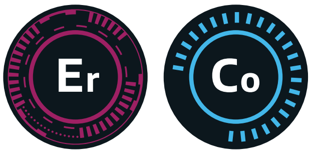
Three new threat groups: **GANANITE, LAURIONITE** and **VOLTZITE**

10 active threat groups: **BENTONITE, ELECTRUM, GANANITE, KAMACITE, LAURIONITE, MAGNALLIUM, PETROVITE, RASPITE, TALONITE** and **VOLTZITE**

ELECTRUM demonstrates Stage 1 & 2 aspects of the ICS Cyber Kill Chain

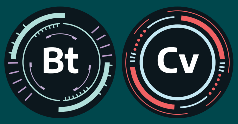


9 threat groups demonstrate at least Stage 1 of the ICS Cyber Kill Chain: **BENTONITE, ELECTRUM, GANANITE, KAMACITE, LAURIONITE, MAGNALLIUM, PETROVITE, RASPITE,** and **VOLTZITE**



2 threat groups, **ERYTHRITE** and **COVELLITE**, were retired in 2023. **11 threat groups** were dormant

Threat Group Statistics from 2022 Year in Review:



2 new threat groups: **BENTONITE** and **CHERNOVITE**

8 active threat groups: **BENTONITE, CHERNOVITE, ELECTRUM, ERYTHRITE, KAMACITE, KOSTOVITE, WASSONITE** and **XENOTIME**

Notable OT Cybersecurity Trends in 2023

Reaching a Tipping Point for OT Facilities

More than ever, factories, power plants, and pipelines share common devices, software packages, network protocols, and facility designs, as industrial facilities have moved towards a more homogenous infrastructure and have connected OT environments to other internal networks and the internet. These developments bring advantages to Europe's owners and operators of operational technology, but it means cyber adversaries can exploit systems remotely and their attack capabilities can be repurposed. This past year, we learned of vulnerabilities present in a subset of Rockwell Automation ControlLogix communication modules. These devices, used across various industrial sectors, might have been compromised if not for the advance collaboration between government agencies, Rockwell Automation, and security vendors (including Dragos) to search for evidence of exploitation and develop threat detections. This example helps illustrate the significant challenges facing the OT community and how we can work together to enable a unified, risk-based response.

Geopolitical Agendas Motivated OT Threat Groups

Executing cyber attacks on critical infrastructure has long been the domain of sophisticated and skilled adversaries, and 2023 was no different. The Ukraine-Russia war continued to serve as the backdrop for significant targeting of OT assets across government, energy, electric, telecommunications, transport, and manufacturing sectors by adversaries on either side of the conflict. This includes disruptive attacks indirectly involved in the conflict, as well as visible destructive attacks, such as those involving the known threat group ELECTRUM, which can directly help achieve military objectives while indirectly benefitting political and economic goals. Mounting tensions between China and Taiwan also led to targeted cyber espionage across several industrial organisations in the Asia-Pacific region and North America. As global adversaries expand their reach and improve their attack capabilities, industrial organisations will want to maintain situational awareness to understand the potential risks to their business.

Determined Hacktivists Disrupted Peace of Mind, Then OT Systems

Less sophisticated hacktivists, motivated by the same geopolitical events, conducted widespread operations in 2023. Hacktivist groups spread false or exaggerated claims of successful cyber attacks on critical OT infrastructure throughout the year, leading to fears and uncertainty about the resilience of regional critical services. After consistent promotion of misleading claims targeting companies in the Middle East, one such hacktivist group, the self-styled CyberAv3ngers, broadened their operations and stepped up their objectives late in the year with attacks on programmable logic controllers (PLCs) used by water utilities across North America, Europe, and Australia with an anti-Israel message. These events represented the first time a hacktivist group was able to achieve Stage 2 of the ICS Cyber Kill Chain, which refers to the development and testing of a capability to meaningfully execute an attack on operational technology. This led to material impacts on at least one community in Erris, Ireland, where 180 residents were left without water services for several days. These attacks demonstrates that it is possible to disrupt physical processes using unsophisticated methods in environments with internet-accessible critical assets and otherwise weak security controls.

European OT Assets Exposed

Exposed OT assets, devices that can be identified and accessed across the public internet, present risks to operators when those assets are improperly secured and configured or where an operator is unaware that the device is even exposed. Groups like CyberAv3ngers and other threats may conduct their own scans to identify publicly available assets, but publicly available scan data also offers broad coverage with continually improving detail. Through publicly available resources, Dragos identified at least 4,700 internet-facing OT devices within Europe that are accessible via the public internet. This number is not exhaustive but nonetheless represents a potential risk to operators where devices can be detected, and software versions or patch levels are identified, leaving no questions on which ones may be vulnerable. Industrial organisations are advised to assess their external infrastructure that is discoverable from the internet and block the exposure of critical assets connected to physical processes.

Too Many Vulnerabilities, Not Enough Guidance for OT

Of the 531 advisories impacting industrial environments disclosed last year, Dragos provided updated mitigation for 49 percent of the advisories that had missing mitigation advice. The inadequacies of the Common Vulnerability Scoring System (CVSS) and the lack of mitigations tailored to operational technology environments accompanying vulnerabilities complicates an already burdensome undertaking. Patching is not always possible, or even necessary in OT environments. Time wasted patching vulnerabilities that only require monitoring might mean a more critical vulnerability gets overlooked. One positive sign is the increase in the number of vulnerabilities that require user authentication to exploit. This is a good thing for defenders, but having a password is not enough to label a device secure. There are many ways for adversaries to obtain credentials as well as escalate their privileges. Industrial environments need vulnerability prioritisation metrics tailored to OT, and vulnerabilities should be addressed in context of operational factors and the specific configurations in place.

European Industrial Organisations Impacted by Ransomware

Ransomware groups do not explicitly target OT networks, but risks to these environments are introduced by precautionary operations shutdowns to limit the impact of an attack, flattened industrial networks, and the integration of OT kill processes into ransomware strains. Ransomware attacks on industrial organisations increased by nearly 50 percent in 2023, affecting virtually all sectors. Of the 905 global ransomware incidents impacting industrial organisations in 2023, only 285 incidents involved European organisations, up from 182 in the previous year.

Attacks outside of Europe can also impact European OT operators when supply chain dynamics enter the equation. Dragos identified at least 115 industrial control system-related suppliers worldwide that were impacted by a ransomware attack in the second half of 2023. In May 2023, the ransomware group Black Basta compromised the large Switzerland-based industrial conglomerate ABB. ABB provides industrial automation and process control equipment and services across various industries worldwide, including energy (electric, nuclear, renewable, oil, and natural gas) utilities, marine, rail, automotive, transport, and manufacturing. The ransomware group attempted lateral movement to other entities that shared a trusted connection with ABB, with one industrial partner possibly compromised.

Key Steps to Secure European Critical Infrastructure

The NIS2 Directive is a landmark piece of European cybersecurity legislation with expanded sectors, stricter regulations, and new obligations. Entered into force on 16 January, 2023, the deadline for Member States to transpose the NIS2 Directive into applicable national law is 17 October, 2024. This is a crucial deadline for businesses. Failure to comply with the NIS2 Directive in European Union Member States can result in severe consequences, including financial penalties and damage to reputation. It is therefore essential that companies are fully prepared and compliant before the deadline date. Unlike the previous directive, where member states could decide which organisations were to meet the requirements, the NIS2 Directive identifies Operators of Essential Services (OES) based on their size, which means it covers significantly more organisations and sectors than the previous version.

In Germany specifically, IT-Sicherheitsgesetz 2.0, or IT-SIG 2.0, was put into practice as of May 2023. The regulation is being updated further to include additional mandatory security controls on critical infrastructure organisations and their ability to detect cyber attacks. As a result, this puts heightened pressure on organisations in Germany, which are now forced to meet strict new cybersecurity requirements from two key pieces of security legislation. The threat level is higher than ever. These new regulations represent an opportunity for businesses to put their OT cybersecurity controls to the test and see what work still needs to be done.

2023 Global OT Threat Landscape

The OT cyber threat landscape continued to evolve in 2023, with an increase in tracked threat groups, ransomware events, and other cyber operations driven by global conflict. The adversaries involved in these activities varied widely in terms of their level of sophistication, deployed capabilities, and intended targets. On one end of the spectrum, some threat groups used advanced techniques, such as leveraging native functionality, including living off the land (LOTL) techniques, to conduct reconnaissance and intelligence operations. Conversely, some adversaries focused on soft targets such as internet-accessible devices that lacked proper hardening, thus making them easy to damage and cause operational disruptions.

In 2023, Dragos tracked 21 threat groups focused on OT targets following the addition of three newly defined groups – VOLTZITE, GANANITE, LAURIONITE – and the retirement of two threat groups, ERYTHRITE and COVELLITE.

The number of known threat groups targeting ICS/OT has grown significantly since the first publication of the OT Cybersecurity Year in Review in 2017. Even as some groups retire and go dormant, new groups step in to fill those ranks. Dragos Intelligence tracks threat groups that attempt to gain access to OT systems and those with the potential to facilitate such attacks in the future. Cyber adversaries often do extensive research and development to build their programs and campaigns over time, and several Dragos-tracked threat groups show signs of evolving their disruptive and destructive capabilities.

New Dragos Threat Groups

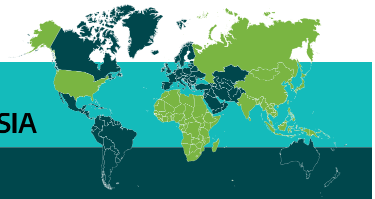
VOLTZITE

VOLTZITE, which overlaps with Volt Typhoon (Microsoft), was first observed performing reconnaissance and enumeration of multiple electric companies based in the United States. Since then, **VOLTZITE** has been observed targeting cybersecurity research, technology, defence industrial bases, banking, satellite services, telecommunications, and educational organisations. They have traditionally targeted US-based facilities, but have since expanded their targeting to include organisations in Africa and Southeast Asia. This group heavily uses living off the land (LOTL) techniques, which can make detection and response efforts more difficult. This strategy, paired with slow and steady reconnaissance, enables **VOLTZITE** to avoid detection from security teams.

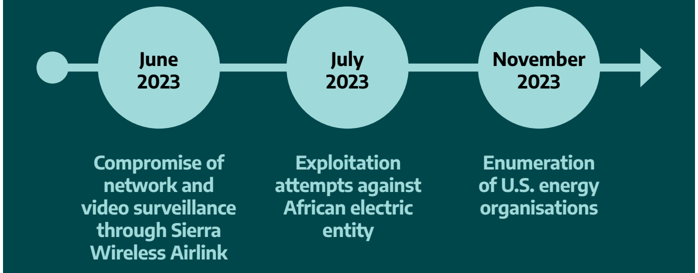
The threat group's behaviour in 2023 suggests their current goal is espionage, information gathering, and persistent access. **VOLTZITE's** proximity to the utility's OT network in observed cases and subsequent SMB traversal manoeuvres demonstrated attempts to penetrate the OT network, aiming to access OT data with a focus on SCADA-related information. It is important to note that data stolen from operational technology networks may result in unintended disruption to critical industrial processes or provide the adversary with crucial intelligence to aid in follow-up offensive tool development or attacks against OT.

Vz

TARGETS: AFRICA, UNITED STATES, ASIA



NOTABLE ACTIVITY

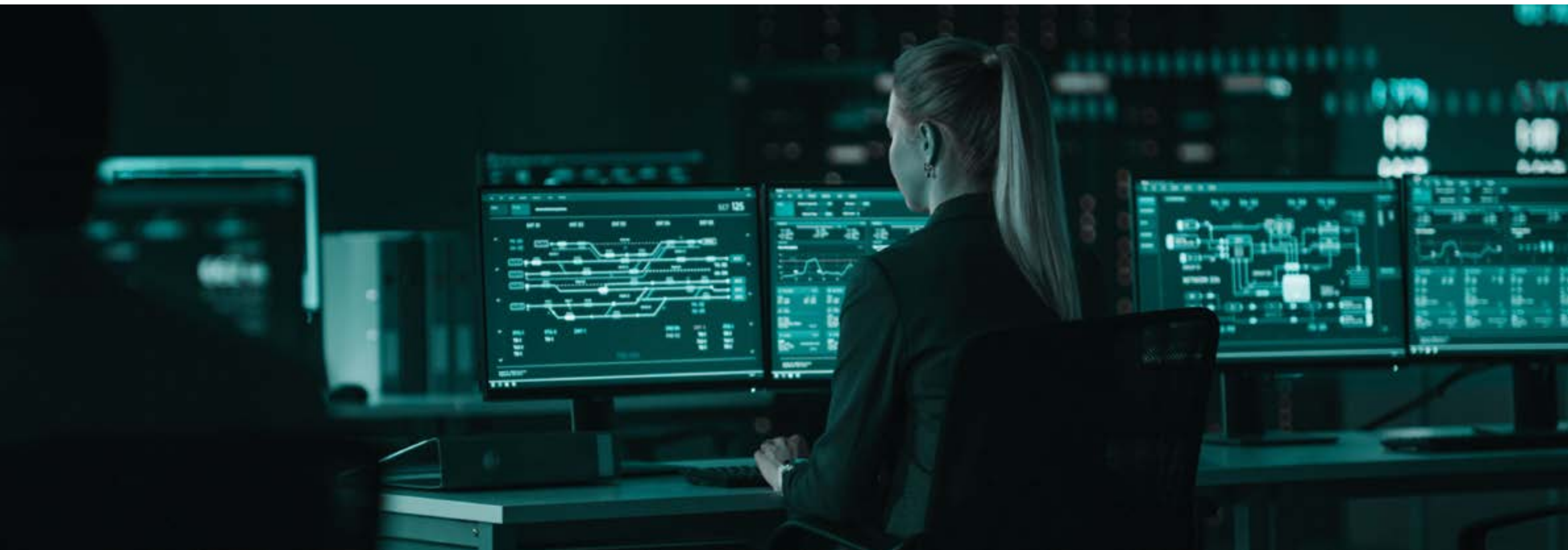


June 2023 — Compromise of network and video surveillance through Sierra Wireless Airlink

July 2023 — Exploitation attempts against African electric entity

November 2023 — Enumeration of U.S. energy organisations

- VOLTZITE exploited public internet-facing Sierra Wireless Airlink devices of a U.S. emergency management and traffic monitoring entity in a June 2023 campaign.
- Possible exploitation attempts in July 2023 against an African electric transmission, distribution, and retailer entity.
- VOLTZITE conducted extensive reconnaissance of U.S. energy organisations in November 2023.



This case study breaks down a VOLTZITE persistent threat hunt executed by Dragos OT Watch utilising the Platform, Threat Intelligence and Neighbourhood Keeper at a U.S. based electric utility.

OT Watch Threat Hunting Uncovers VOLTZITE

- The Dragos Intelligence team started tracking **VOLTZITE's** activities at the beginning of 2023.
- A new utility customer deployed the Dragos Platform in response to a pre-existing network compromise with a potential ICS/OT impact. The platform was positioned to monitor the IT-OT interface (Level 3-4) and OT-OT communications (Level 2).
- Following deployment, Dragos OT Watch utilised the Dragos Platform to identify malicious activity within the environment working with Dragos Intelligence using tactics, techniques, and procedures (TTPs) and threat hunt analytics.
- The threat hunt confirmed adversary evidence adjacent to the OT network; and incident response analysis found evidence of adversary discovery actions with a focus on SCADA related information. This was seen in the Dragos Platform as server message block (SMB) traversal with the group pivoting within the environment, and likely, looking for information about the environment as a further means of persistence.
- Consistent with OT Watch operations, findings were promptly escalated to the customer with a full summary of all threat hunt findings after the full investigation. The recommendations further empowered the customer's incident response efforts in cleaning up the incident to eliminate the adversary from the environment. The environment continues to be monitored via the Dragos Platform and OT Watch.
- Taking the success of the threat hunt and the detailed understanding on the tactics of this threat group provided by the Dragos Intelligence team, OT Watch extended the hunt across all relevant OT Watch customers.
- The Dragos Intelligence team enhanced the effort by analysing Neighborhood Keeper data for indications of **VOLTZITE** behaviours and then notifying impacted parties anonymously. With these findings, Dragos threat detections engineers developed high-fidelity detections back into the Platform deployed via Dragos Knowledge Packs for continuous monitoring.

The overall response to the **VOLTZITE** threat highlights the importance of coordinated efforts and the advantage of ICS/OT capabilities unique to Dragos. This engagement not only addressed a complex threat but also strengthened the protective measures across critical infrastructure customers.

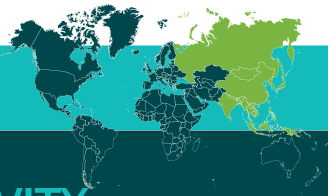
GANANITE

GANANITE targets critical infrastructure and government entities in the Commonwealth of Independent States and Central Asian nations. **GANANITE** focuses on espionage and data theft, with the possibility of handing off initial access to other threat groups. This group is focused on its target sets by employing many known tools and techniques to infiltrate its victims. **GANANITE** has been observed conducting multiple attacks against key personnel related to ICS operations management in a prominent European oil and gas company, rail organisations in Turkey and Azerbaijan, multiple transportation and logistics companies, an automotive machinery company, and at least one European government entity overseeing public water utilities.

Although **GANANITE** has not yet shown evidence of moving into OT networks or an elevated capability resembling Stage 2 actions of the ICS Cyber Kill Chain, their assessed capabilities show efficient use of multiple phases across Stage 1 of the ICS Cyber Kill Chain.

Gn

GANANITE TARGETS: ASIA



NOTABLE ACTIVITY

January 2023 — Recon and infiltration of EU critical infrastructure orgs

May 2023 — CIS targeting with espionage and data theft

- On 13 January 2023, GANANITE conducted reconnaissance against and infiltrated various European critical infrastructure organisations. Along with credential capture via masqueraded domain phishing pages, the adversary utilises an open-source Python RAT named Stink.
- In May of 2023, GANANITE continued targeting government and industrial organisations in the Commonwealth of Independent States with a focus on espionage and data theft, with the potential to hand off initial access to other threat groups.

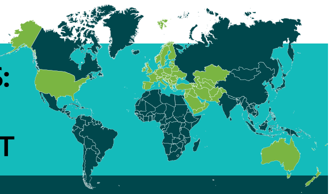
LAURIONITE

LAURIONITE was first discovered actively targeting and exploiting Oracle E-Business Suite iSupplier web services and assets across several industries, including aviation, automotive, manufacturing, and government. Oracle E-Business Suite is one of the most widely used enterprise solutions for integrated business processes, including numerous industrial organisations such as United States Steel and Unifi textile manufacturing. This group utilises a combination of open-source offensive security tooling and public proof of concepts to aid in their exploitation of common vulnerabilities.

By utilising compromised infrastructure, **LAURIONITE** can remain undetected or overlooked due to its origin being from trusted or known organisations. Targeting companies that use Oracle's E-Suite iSupplier technology may not inherently impact OT assets but could allow adversaries like **LAURIONITE** to gain visibility into third-party vendor relationships, which can lead to follow-on intrusion operations. **LAURIONITE** has demonstrated the ability to conduct the complete attack cycle of offensive cyber operations that achieve Stage 1 of the ICS Cyber Kill Chain.

Lr

LAURIONITE TARGETS: U.S., AUSTRALIA, EUROPE, MIDDLE EAST



NOTABLE ACTIVITY

March 2023 — Targeting and exploitation of Oracle iSupplier

- **As early as 5 March 2023, LAURIONITE was observed targeting and exploiting Oracle E-Business Suite iSupplier web services.**

Other Active Threat Group Updates

KAMACITE – Active Since 2014

January: KAMACITE continued targeting Ukrainian telecommunications entities using the DarkCrystal remote access trojan (RAT) and then using native tools that exist within a victim's own networks. This activity continues a multi-year trend from KAMACITE conducting initial intrusion operations against Ukraine entities to reconnaissance operations against global industrial entities likely in pursuit of enabling follow-on intrusion operations from threat groups like ELECTRUM.

ELECTRUM – Active Since 2016

January: A variant of CADDYWIPER, used as part of the INDUSTROYER2 event, was identified in the wild. Dubbed SwiftSlicer, the destructive malware used Active Directory Group Policy to delete shadow copies and overwrites files before rebooting the computer.

MAGNALLIUM – Active Since 2013

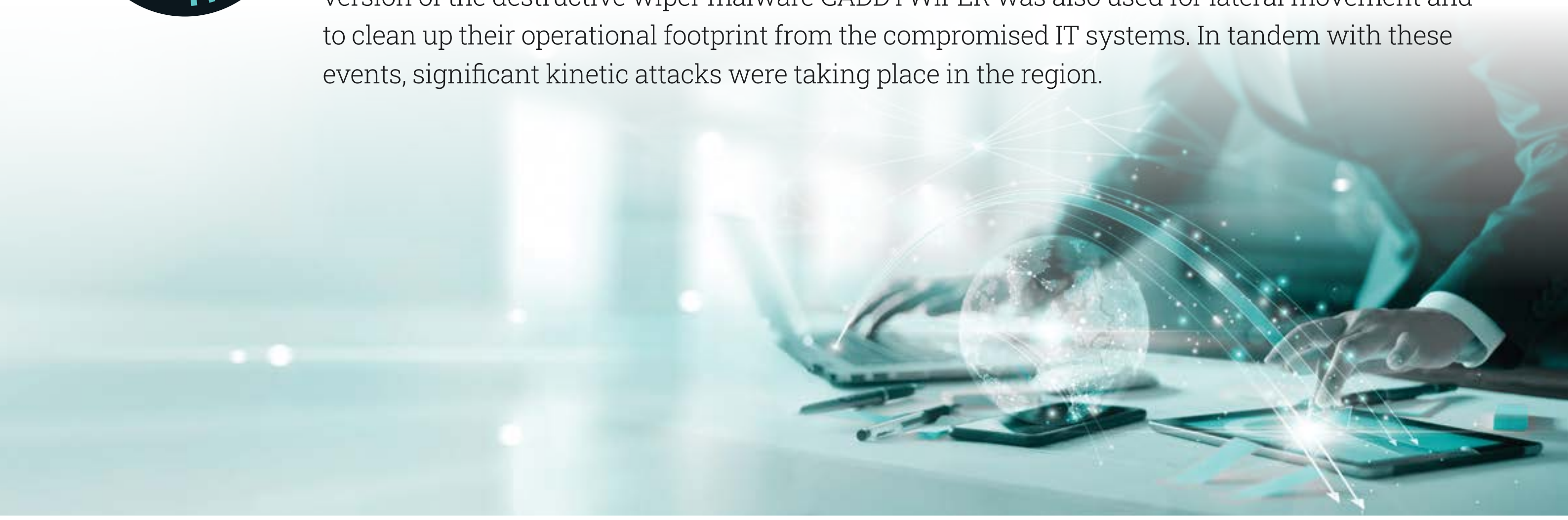
July: MAGNALLIUM had seemingly disappeared for nearly a year until they began password-spraying operations against multiple defence and mining organisations. Prior MAGNALLIUM cyber operations have included initial access and reconnaissance actions before deploying destructive wiper malware on the victim's IT networks.

RASPITE – Active Since 2017

September: RASPITE conducted widespread campaigns scanning for vulnerable server message block (SMB) devices and using password-spraying techniques against various industry sectors, including defence and mining.

ELECTRUM – Active Since 2016

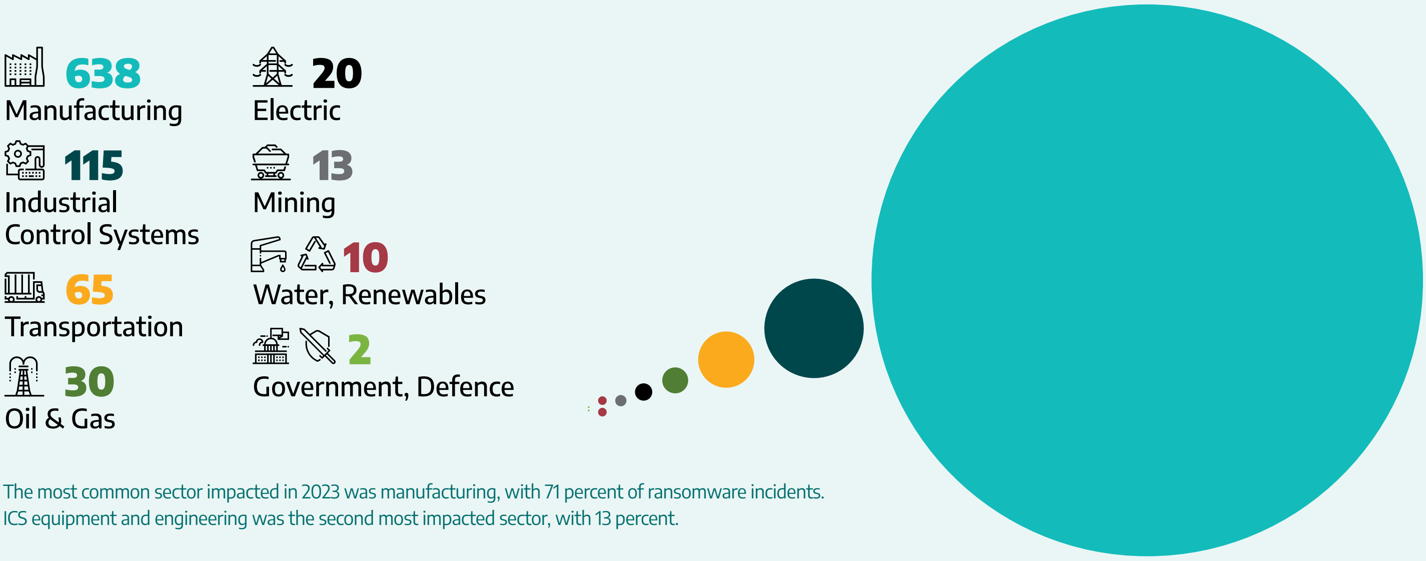
November: New information on the cyber attack in October 2022 revealed ELECTRUM leveraged a vulnerable device, running end-of-life (EOL) MicroSCADA software in the OT environment. ELECTRUM then attempted to impact the availability and control of a substation in Ukraine. A version of the destructive wiper malware CADDYWIPER was also used for lateral movement and to clean up their operational footprint from the compromised IT systems. In tandem with these events, significant kinetic attacks were taking place in the region.



2023 Ransomware Trends

Fifty ransomware groups were responsible for 905 reported ransomware incidents impacting industrial organisations this past year. This represents a 49.5 percent increase from 2022. Industrial organisations have much to lose because operational disruptions can carry significant financial and reputational costs. Further, there can be numerous cascading impacts on downstream businesses and outputs. The most common sector impacted in 2023 was manufacturing, with 71 percent of ransomware incidents. ICS equipment and engineering was the second most impacted sector, with 13 percent.

Ransomware operators' primary methods to gain initial access to victims' networks have remained steady in 2023, including collaborating with initial access brokers, phishing, and exploiting publicly accessible network assets, such as VPNs and RDP servers. Dragos also observed ransomware campaigns exploiting public-facing services and capitalising on disclosed vulnerabilities.



The most common sector impacted in 2023 was manufacturing, with 71 percent of ransomware incidents. ICS equipment and engineering was the second most impacted sector, with 13 percent.

Figure 1: Ransomware Incidents by Sector • 2023

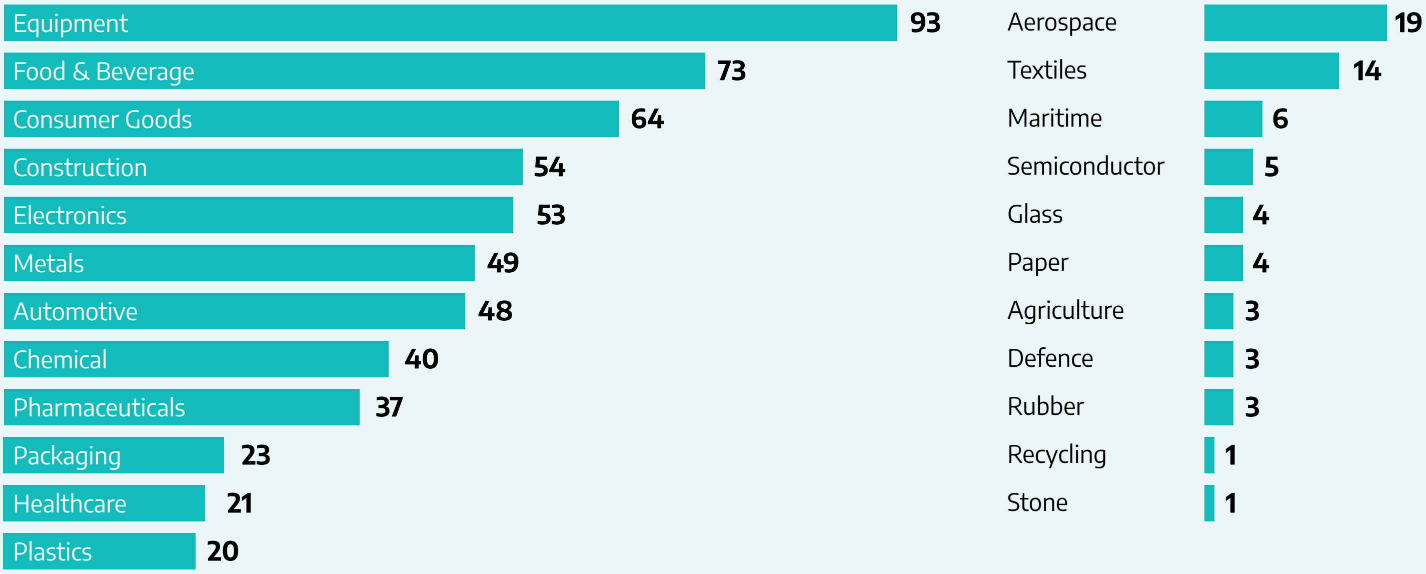


Figure 2: Ransomware by Manufacturing Subsector • 2023

2023 OT Vulnerability Trends

Many factors set OT apart from IT. Consider the type of devices, systems, and protocols used within these environments; the network architecture of typical OT networks; and the impact vulnerabilities can have on normal operations and the physical world. This is why OT vulnerabilities need to be mitigated and addressed according to strict operational requirements, where uptime is paramount, and considering the specific configuration and implementation of an asset. This is a challenge because many vulnerability advisories contain errors and lack actionable mitigations tailored to OT.

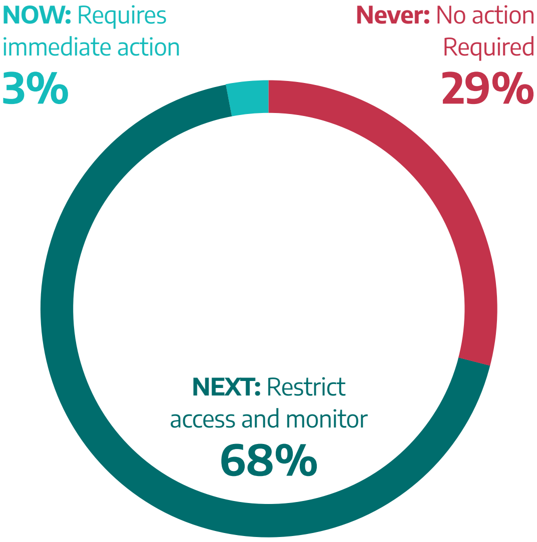
The Common Vulnerability Scoring System (CVSS) misapplication is the most common form of error encountered in vulnerability advisories. Dragos corrects CVSS scores and often directly contacts the vendors and researchers for clarification on how an adversary might exploit a given vulnerability in an OT environment.

Prioritising vulnerabilities into actionable categories saves asset owners and operators from wasting time and resources on vulnerabilities with little or no impact on their operations. To prioritise the 2010 vulnerabilities to the signal of the ones you should care about, Dragos follows the Computer Emergency Response Coordination Center's (CERT/CC) **Now, Next, Never** methodology.

Vulnerabilities that fall into the **Now** category require immediate action and accounted for 3 percent of the vulnerabilities assessed in 2023. These vulnerabilities are generally network exploitable, have public proof of concept, and affect the loss of view or loss of control of operational technology processes. The **Now** category also include vulnerabilities under active exploitation by adversaries. Asset owners and operators should address these vulnerabilities as soon as practicable.

Neighborhood Keeper allows the community to gain anonymised visibility across various industrial environments. As a collective defense and community-wide visibility solution, Neighborhood Keeper enables a more informed industrial defense by sharing threat intelligence across industries and geographic regions. Dragos uses this data to help the community identify risk areas and how best to address them. Of the vulnerabilities reported through Neighborhood Keeper, 13 percent fall within the **Now** category, which requires immediate action.

Of the 2010 vulnerabilities in 2023, Dragos found that 3 percent required immediate action. A full 68 percent can be addressed by network monitoring, network segmentation, or MFA. And 29 percent require no immediate action but should be monitored for signs of possible exploitation.



From the OT Cybersecurity Frontlines

In 2023, we saw major regulatory shifts for critical infrastructure asset owners, resulting in organisations devoting more time and resources to preparing for a cybersecurity event. This included updates for U.S. pipeline operators in North America with TSA Pipeline-2021-02D (SD-02D). In Europe, it was the Network and Information Systems Directive (NIS2); in Australia, the Security of Critical Infrastructure SOCI Act; and the Essential Cybersecurity Controls (ECC) ECC in the Kingdom of Saudi Arabia.

Dragos worked with organisations growing their cybersecurity capabilities, defining or refining processes, and exercising plans. Organisations leading in this area are shifting from a reactive mindset that leverages break-glass retainers to a holistic approach for incident response that includes multiple levels within organisations supported by detection capabilities, training, and external experts.

In 2023, the quantity, type, and scope of tabletop exercises that Dragos facilitates changed. The number of exercises increased by 217 percent from 2022. The types and scope of the exercises shifted in 2023. Notably, this includes an increase of 350 percent in executive and board-level exercises.

Tabletop exercise findings and associated recommendations are organised by core capabilities for OT cybersecurity readiness and incident response. These are detect, communicate, activate, respond, contain, document, and recover. Core capabilities map to standard incident response processes regardless of whether the organisation favours the four-step U.S. National Institute of Standards and Technology (NIST) process, SANS Preparation - Identification - Containment – Eradication - Recovery - Lessons Learned (PICERL), or some variation. Regardless of how the incident response plan is structured, these capabilities are needed to handle a cybersecurity event successfully.

Core Capability	2022 Score	2023 Score	Change	Metrics are as follows
Detect	73%	65%	-8	🟩 Performed without Challenges **80-100** 🟧 Performed with Some Challenges **66–79** 🟥 Performed with Major Challenges **50–65** ⬛ Unable to Perform **0–49**
Activate/Elevate	81%	67%	-14	
Respond	76%	62%	-14	
Contain	81%	64%	-17	
Communicate	76%	57%	-19	
Document	73%	65%	-8	
Remediate/Recover	81%	61%	-20	

Figure 4: Average Tabletop Exercise Scores (All OT)

Implementing 5 Critical Controls

As ICS/OT cybersecurity becomes a top priority, from boardrooms to the manufacturing floor, leaders and their teams must work together to implement programs and critical safeguards. A first step in implementing critical cybersecurity controls is achieving alignment on the key priorities. The SANS Institute identified five critical controls for ICS/OT cybersecurity.[1] We offer additional insight on how to implement these controls in your OT environments.

1 ICS incident response plan

OT's incident response plan (IRP) should be distinct from IT's. OT involves different device types, communication protocols, different types of tactics, techniques, and procedures (TTPs) specific to the industrial threat groups. Investigation requires a different set of tools and languages. Create a dedicated plan that includes the right points of contact, such as which employees have which skills inside which plant, and well thought-out next steps for specific scenarios at specific locations. An integral component of an IRP is establishing the collection criteria needed to respond to an incident prior to an incident. Consider table top simulation exercises to test and improve response plans.

2 A defensible architecture

OT security strategies often start with hardening the environment—removing extraneous OT network access points, maintaining strong policy control at IT/OT interface points, and mitigating high risk vulnerabilities. However, a defensible architecture is not simply a "hardened" one. It is one that supports the people and processes behind it. More specifically, it must support the collection requirements that were established in the IRP and implemented for improved OT visibility and monitoring.

3 Visibility and monitoring

A successful OT security posture maintains an inventory of assets, maps vulnerabilities against those assets (and mitigation plans), and actively monitors traffic for potential threats. Visibility gained from monitoring your industrial assets validates the security controls implemented in a defensible architecture. Threat detection from monitoring allows for scaling and automation for large and complex networks. Defenders should concentrate on the threat behaviours (or TTPs) identified in the IRP to avoid excess noise and focus on the risks they care about the most.

4 Secure remote access

Secure remote access is critical to OT environments. A key method, multi-factor authentication (MFA) is a rare case of a classic IT control that can be appropriately applied to OT. Implement MFA across your systems of systems to add an extra layer of security for a relatively small investment. Where MFA is not possible, consider alternate controls such as jumphosts with focused monitoring. The focus should be placed on connections in and out of the OT network and not on connections inside the network.

5 Risk-based vulnerability management

Knowing your vulnerabilities – and having a plan to manage them – is a critical component to a defensible architecture. Of the OT-specific vulnerabilities released last year, the majority of them had incomplete or erroneous information. An effective OT vulnerability management program requires timely awareness of key vulnerabilities, the small percentage that need immediate attention and apply to the environment, with correct information and risk ratings, as well as alternative mitigation strategies to minimise exposure while continuing to operate.

[1] https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

Download the 2023 OT Cybersecurity Year in Review Report

To get the complete analysis and review the full set of data from last year, download a copy of the Dragos 2023 OT Cybersecurity Year in Review Report. We offer a complete breakdown of our OT cyber threat intelligence findings, with frontline insights and actionable guidance that aligns to each finding.

Get your copy at dragos.com/year-in-review.

DRAGOS

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

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.

Dragos.com