OT CYBERSECURITY
THE 2023 YEAR IN REVIEW

FEBRUARY 2024

DRAGOS

TABLE OF CONTENTS

INTRODUCTION

In 2023, a surge in global tension resulted in an increase in cyber threat activity and disruptions in critical infrastructure worldwide. Escalating conflicts, including those between Ukraine and Russia, Israel and Hamas, and countries in the South China Sea, emboldened adversaries and hacktivists to develop new capabilities and reuse old techniques. Simultaneously, ransomware attacks affected more industrial organizations, with a nearly 50 percent increase in reported incidents. Asset owners must take necessary precautions to address these threats or fall victim to them.

Among the threats that organizations must consider are the capabilities developed in conflict areas. A year after Russia's invasion of Ukraine, cyber threat activity in the region continues to escalate. Dragos and the community became aware of new destructive malware capabilities as **ELECTRUM** conducted targeted cyber operations against Ukrainian critical infrastructure. The mixture of traditional kinetic warfare with cyber-focused capabilities has created a new testbed for increased threat capabilities worldwide.

Similarly, the conflict that erupted in the Middle East included cyber attacks on critical infrastructure. Pro-Israeli hacktivists claimed responsibility for the attacks that claimed to disrupt over 70 percent of the gas stations in Iran, while pro-Hamas hacktivists targeted Israeli-manufactured operational technology (OT) hardware and software. The impact of these attacks on industrial equipment spread beyond the conflict zone and affected various sectors, such as water and manufacturing, around the globe.

Throughout the year, Dragos continued to track threat groups as they developed capabilities and gained access. Mounting tensions between China and Taiwan contributed to the environment where Dragos observed **VOLTZITE** target several industrial organizations in the Asia-Pacific region, Africa, and North America — including entities in electric, satellite communications, telecommunications, emergency management, and defense industrial base sectors — with cyber attack campaigns assessed to be aimed at long-term espionage objectives. **VOLTZITE's** actions towards U.S. electric entities, telecommunications, and GIS systems signify clear objectives to identify vulnerabilities within the country's critical infrastructure that can be exploited in the future with destructive or disruptive cyber attacks. Dragos tracked 21 threat groups targeting industrial organizations including three new threat groups.

Although threat groups and hacktivists posed significant risks in 2023, ransomware was the primary concern for many organizations globally. This concern is well founded, considering the rise in ransomware attacks and the industrial impact observed by Dragos during incidents this year. These trends, along with new reporting requirements, saw an increased focus on response from many organizations. Regulatory changes in the United States, Europe, Australia, Asia, and the Middle East required organizations to develop capabilities to meet reporting obligations. To this end, Dragos conducted more exercises with a wider range of participants and industries in 2023.

Another major focus area for organizations this year was understanding what risks vulnerabilities posed and how best to respond to them. 2023 saw a 14 percent increase in vulnerabilities advisories, with 31 percent of advisories that Dragos analyzed having incorrect data. The year also saw the discovery of a major vulnerability impacting Rockwell Automation's ControlLogix communication modules, reminiscent of the zero-day that **XENOTIME** exploited in the TRISIS attack. However, this event exemplified how vendors, governments, and our community leverage communication and visibility to enable a unified, risk-based response.

Dragos started the Year in Review to highlight significant trends in the OT cybersecurity community. This year's report aims to go further by offering practitioners and leaders the most up-to-date data, along with perspectives from the field, to help them better defend critical infrastructure around the world. These perspectives are focused on providing actionable insights that have been tried and tested to help organizations effectively defend against and respond to industrial cyber threats.

THE RISING TIDE OF INDUSTRIAL CYBER THREAT ACTIVITY

The Dragos Platform provides visibility and insight through OT Watch and Neighborhood Keeper data. The Dragos threat intelligence teams assess and research vulnerabilities and actively track adversaries impacting operational technology. Dragos consultants and responders provide frontline perspectives from various engagements, including assessments, exercises, and incident response. Since Dragos first started gathering data for Year in Review in 2017, many trends have remained consistent with notable milestones along the way. The data and perspectives presented in this report are focused on the global industries that Dragos serves.

2016 – CRASHOVERRIDE Not identified until months later, CRASHOVERRIDE malware was used in 2016 as the first malicious code to attack electric substations – the facilities and equipment that are designed to protect bulk electric systems were manipulated to have the opposite effect. The CRASHOVERIDE legacy lives on with a series of attacks utilizing INDUSTROYER2 malware observed as recently as October 2022.

2017 – TRISIS The threat group XENOTIME deployed the TRISIS malware against a Safety Instrumentation System (SIS) at a petrochemical plant in Saudi Arabia. TRISIS represents the expansion of malware targets and methods of execution, and the first time system safety features have been targeted and compromised directly.

2018 – EXPANDED THREAT GROUPS In 2018, Dragos expanded the number of Threat Groups tracked from 3 to 8. This trend continued over time — to date there are 21 Dragos-designated Threat Groups with the intent to gain access to OT environments and potentially disrupt them.

2019 – INCREASED RANSOMWARE IN OT In 2019, Dragos tracked a 50 percent uptick in ransomware within OT. The first ransomware case Dragos responded to occurred within the electric sector also in 2019.

2020 – EKANS RANSOMWARE Dragos analyzed EKANS malware variants with capabilities to stop ICS-related Windows processes before initiating encryption. This functionality represents a natural but troubling consequence of target expansion. Ransomware groups increase the odds of victims paying a ransom when business is disrupted.

2021 - RANSOMWARE ATTACK IMPACTS OT In 2021, Colonial Pipeline was impacted by ransomware, causing a precautionary shutdown of OT operations. Again, ransomware instances continued to balloon in 2023 with 905 instances, an increase of nearly 50 percent over the last year.

2022 – ENTER CHERNOVITE In 2022 Dragos discovered the CHERNOVITE Threat Group, developer of the PIPEDREAM malware, a highly motivated and well-funded entity, that is skilled in software development methods and well versed in industrial control systems (ICS) intrusion techniques.

2023 – EVOLVING THREAT LANDSCAPE Rising tensions and financial opportunity continued to spur a wide variety of actors to target industrial environments - including hactivists, criminal gangs, and three new Dragos-designated Threat Groups.

KEY HIGHLIGHTS: INSPIRING ACTION

☞ **If you haven't assessed your external infrastructure for critical systems yet, 2024 is the time.** This includes identifying your organization's internet routable netblocks and IP space, including what contractors or vendors may have set up for you. Network scan your public spaces and compare it against Shodan, Whois, and your documentation. Ensure critical assets or assets connected to your process environment are not discoverable from the internet. Learn more about why this guidance is important from the 2023 attack on Unitronics PLC devices by the CyberAv3ngers on page 11.

☞ **If you haven't segmented your network yet, the best time for that was in the 2000s; the second best time is now.** This network segmentation includes separating devices with network and host-based firewalls by function, not just systems from the internet, but systems from each other and critical processes. Do not merely focus on IPv4 when your systems also use IPv6. When operators traverse network zones to log in using a virtual private network (VPN), remote desktop protocol (RDP), or other remote access tools, they should leverage separate authentication. In 2023, increased ransomware impacts on OT environments highlight the necessity of this old but still useful guidance. Read more on Ransomware on page 21.

☞ **Restricting and monitoring outbound communication is also important in addition to segmentation.** This includes evaluating default routes, gateways, and firewall rules to external networks and proxy configurations. In 2023, several adversaries, such as VOLTZITE, GANANITE, and ransomware groups, leveraged communication to external networks for command and control (C2) communication, allowing exfiltration of data and remote control of network assets. For more on this see the OT Cyber Threat Landscape section of this report on page 9.

☞ **If your organization already regularly assesses standard guidance, such as auditing segmentation rules and configuration, you still have work to do.** As defensible architecture continues to mature, adversary techniques shift with it. Learn which techniques our penetration testers leverage in OT assessments in the Frontline Perspective section on page 20, as well as which techniques still work for ransomware groups on page 21 and threat groups on page 9. Understanding the attack surface is vital for prioritizing a response or identifying adversaries within your network. Hunting for evidence of these techniques in use within your monitoring system is the best way to identify unwanted operators hiding in your OT environment.

☞ **Lastly, reduce the risk of vulnerable equipment used in OT processes, but do it in a systematic way.** In 2023, Dragos prioritized and wrote mitigation guidance for 531 OT-related advisories, 2010 vulnerabilities. Read more on key insights, trends, and mitigations from vulnerabilities on page 27.

LEARNING FROM ADVERSARY-OWNED ROCKWELL AUTOMATION VULNERABILITIES

In 2023, the U.S. Government informed Rockwell Automation of two APT-owned vulnerabilities impacting a subset of ControlLogix communication modules. These communication modules are part of a significant Rockwell Automation product line and assist in controlling processes in many industrial verticals. In coordination with their government partners, Rockwell Automation organized a defensive working group comprised of various vendors, including Dragos. The working group's goal: develop detections for these vulnerabilities and search for evidence of exploitation.

As part of the working group, Dragos analysts studied the vulnerabilities and the impacted communications modules. With Rockwell Automation and other community members, they developed detection signatures that would alert on artifacts specific to varying methods of potential exploitation. Dragos vulnerability analysts deployed these signatures to Neighborhood Keeper and OT Watch to find signs of malicious activity. They triaged any alerts, paying attention to false positives and tuning signatures accordingly.

Dragos analysts passed the detection results back to the working group so that the rest of the community could tune their signatures for their respective platforms. In this way, Neighborhood Keeper helped the community to avoid unnecessary alerting once the detections and vulnerabilities were made public. Aside from signature tuning, Neighborhood Keeper provided visibility into the number of vulnerable devices and how widespread their use is in different industries and regions. Dragos passed this information back to the working group so that they could assess the vulnerabilities' risk and potential impact.

The collaboration between the U.S. Government and Rockwell Automation, along with the formation of a working group of security vendors to ensure a defensive front before public release, and the coordinated publishing of vulnerability information, represents a significant accomplishment for the industrial control systems (ICS) community. Product owners and OEMs can look to Rockwell Automation as an excellent example of community and defense-forward practice and consider following this path for vulnerability disclosure. This new approach of blending U.S. Government intelligence with security industry expertise and OEM knowledge is undoubtedly the way forward in combating future cyber adversary threats to critical infrastructure.

Dragos Frontline Perspective

THE VULNERABILITIES

Rockwell Automation and the U.S. Government released two vulnerabilities:

CVE-2023-3595 This vulnerability in 1756 EN2* and 1756 EN3* products allows a malicious user to perform remote code execution with persistence on the target system through maliciously crafted CIP messages.

CVE-2023-3596 In the 1756-EN4* products, this vulnerability allows a malicious user to cause a denial of service through maliciously crafted CIP messages.

THE EXPLOIT

An unreleased exploit capability leveraging these vulnerabilities is associated with an unnamed advanced persistent threat (APT) group.

Dragos Frontline Perspective

Dragos OT Watch customers and Neighborhood Keeper participants were protected by monitoring for this threat before it was publicly announced. If a situation like this were to happen again, Dragos Community Defense Program members would benefit via the program's emerging threat monitoring.

13%

of Rockwell Automation assets were ControlLogix communication modules, across manufacturing, paper and pulp, automotive, mining, chemical, food and beverage, electric, oil and gas, etc.

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 analyzed **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.

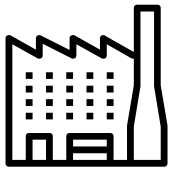
Key Ransomware Findings

50%

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

28%

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



70%

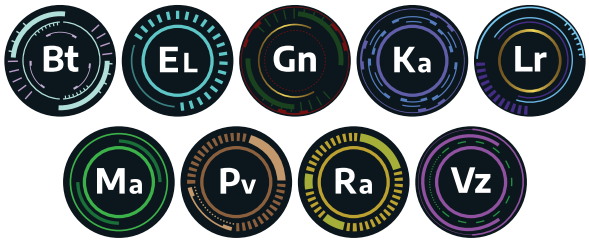
of all ransomware attacks targeted **638 manufacturing entities** in **33 unique manufacturing subsectors**.

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**

OT CYBER THREAT LANDSCAPE

The OT cyber threat landscape continued to evolve in 2023, with an increase in tracked threat groups, ransomware events, and other threat activities 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 targeted low-hanging fruit such as internet-accessible devices that lacked proper hardening, thus making them easy to damage and cause operational disruptions.

Threat groups continued to use publicly disclosed vulnerabilities and discover and develop their own capabilities. Most of the observed threat activity targeted IT-centric devices that are commonly used in OT, such as Sierra Wireless modems or Citrix. In 2023, Dragos worked with one of our strategic partners, Rockwell Automation, on a community response to a set of adversary-developed vulnerabilities targeting OT devices. The identified vulnerabilities have the potential to result in loss/denial of view (T0829, T0815), denial/manipulation of control (T0813, T0831), theft of operational information (T0882), and loss of productivity and revenue (T0828).

CONFLICT-DRIVEN THREAT ACTIVITY

The overlaps of OT cybersecurity threats with regional and global kinetic events have never been more evident than in 2023. Cyber adversaries with a range of capabilities have used the Ukraine-Russia and Israel-Hamas wars to conduct targeted operations against critical infrastructure, and less sophisticated hacktivists have used the same conflicts to cause panic and negatively impact public perception of the resilience of critical services. Geopolitical tensions worldwide, including in Asia and Africa, have also driven intelligence gathering and capability staging activity.

The Ukraine-Russia conflict drove the activity of more mature threat groups, such as **ELECTRUM**, which conducted targeted cyber operations against Ukrainian critical infrastructure entities. A new destructive wiper malware attributed to **ELECTRUM** was observed in the wild in June 2023. Later, in September 2023, Dragos reported on a spear-phishing campaign that targeted Ukrainian critical infrastructure organizations linked with **ELECTRUM** and **KAMACITE**. Lastly, in November 2023, a cybersecurity vendor published a report providing evidence of destructive malware activity targeting Ukrainian electric substations in October 2022. Dragos assessed with moderate confidence that **ELECTRUM** conducted the October 2022 destructive malware activity.

According to multiple sources, the mounting tension between China and Taiwan also contributed to increased targeted cyber espionage attacks against multiple industrial organizations in the Asia-Pacific region and the United States.[1] One threat group in particular, **VOLTZITE**, has targeted numerous critical infrastructure entities in Guam, the United States, and other countries since at least 2021. **VOLTZITE** overlaps with Volt Typhoon, a group that the U.S. Government has publicly linked to the People's Republic of China. **VOLTZITE** heavily uses living off the land (LOTL) techniques and, in some cases, has been observed conducting "hands-on keyboard" post-compromise actions within a victim's networks.

Dragos Frontline Perspective

Living off the land (LOTL) describes the use of typically pre-existing, legitimate capabilities present on a victim host and network for malicious purposes. In the information technology (IT) world, this means using native system capabilities such as PowerShell or server message block (SMB) as part of an attack. In the OT world, this can mean using the native functionality of a PLC or control system to issue a control command.

VOLTZITE has shown continued interest in the electric and telecommunications sectors in the United States, evidenced by the long-term reconnaissance of multiple electric entities. If **VOLTZITE** establishes an initial foothold on the network perimeter of a target, it may then be able to pivot further into a victim's information technology (IT) network and then move laterally onto the victim's OT network. Dragos has only observed **VOLTZITE** operations achieving Stage 1 of the ICS Cyber Kill Chain. They have not displayed actions or capabilities designed to disrupt, degrade, or destroy ICS/OT assets or operations.

Dragos Frontline Perspective

Dragos has observed multiple operational overlaps between the Volt Typhoon and Dragos-tracked threat group VOLTZITE. In a collaborative effort with the Electric Information Sharing and Analysis Center (E-ISAC), Our analysis revealed likely active and ongoing VOLTZITE initiated scanning activities against electric sector organizations in North America between November and December 2023. VOLTZITE's persistent interest and activities within critical infrastructure sectors warrant monitoring and preparedness by ICS/OT organizations.

Dragos leverages its intelligence to drive hunting with our customer environment and the community. This was used to track and analyze indicators of compromise and behavioral tactics, techniques, and procedures relevant to the **VOLTZITE** threat group. A significant outcome of this is finding a high confidence indicator within a Dragos Platform customer's environment, allowing OT Watch to better assist the client during their incident response efforts and providing Dragos Intelligence with real-world behavioral elements surrounding the **VOLTZITE** indicator, including activity suggesting remote desktop protocol (RDP) usage and server message block (SMB) directory traversal. Another interesting finding was **VOLTZITE** overlaps with infrastructure associated with the Mirai Botnet and another activity cluster that differs from **VOLTZITE** but may be operationally connected.

Dragos's analysis of **VOLTZITE** operations underscores the need for ongoing vigilance among organizations operating in the global electric sector, as the observed activity suggests continued and specific interest in these networks. Further, **VOLTZITE's** actions involving prolonged surveillance and data gathering align with Volt Typhoon's assessed objectives of reconnaissance and gaining geopolitical advantage in the Asia-Pacific region.

[1] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a; https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

Throughout 2023, hacktivists and other unsophisticated, opportunistic threat groups have conducted widespread distributed denial of service (DDoS) attacks against various industrial organizations and critical infrastructure. Pro-Russia groups like *CyberArmyofRussia_Reborn* attacked industrial organizations in Europe in May 2023. *NoName057(16)* attacked European and North Atlantic Treaty Organization (NATO) aligned countries and their manufacturing and transportation organizations. Additionally, *Anonymous Sudan* was also observed attacking the United States and other NATO-aligned entities. Similar activity has been observed with pro-Hamas hacktivist groups such as the *CyberAv3ngers* and *Team Insane Pakistan* claiming disruptive attacks against Israeli Railways, an Israeli town's power grid system, and an Israeli hydroelectric plant. In late December 2023, the hacktivist group *Predatory Sparrow* allegedly disrupted Iranian gas stations with an unspecified cyber attack.

Dragos Frontline Perspective

The hacktivists' DDoS attacks had minimal impacts and primarily disrupted the organization's websites. In many cases, Dragos found that claims of disruptive attacks against critical infrastructure were wildly exaggerated or completely fabricated. However, most hacktivist groups aim to gain notoriety, spread misinformation, cause fear, uncertainty, and doubt (FUD), and draw international media attention to geopolitical and social causes.

These operations also included the successful compromise of public-facing OT devices, as was observed in late November with the attack on Unitronics devices. The *CyberAv3ngers* successfully compromised numerous U.S., European, and Australian industrial companies using internet-accessible Unitronics PLC devices. Dragos assesses with moderate confidence that the adversaries scanned the open internet to identify publicly accessible Unitronics devices and then attempted to log into the devices using the Unitronics default password. This adversary appears not to possess OT capabilities; however, this attack still led to a Loss of View and Control (T0829, T0827) for some of those impacted.

Dragos Frontline Perspective

Dragos identified over 1800 internet-exposed Unitronics devices, but only 0.0001 percent of Neighborhood Keeper monitored assets are Unitronics. Dragos assesses with moderate confidence that Unitronics devices are more common in environments with limited visibility, such as remote locations or smaller organizations. This type of device is often deployed without proper visibility or hardening. Basic hygiene and device management are critical to stopping this activity, including understanding what is publicly accessible.

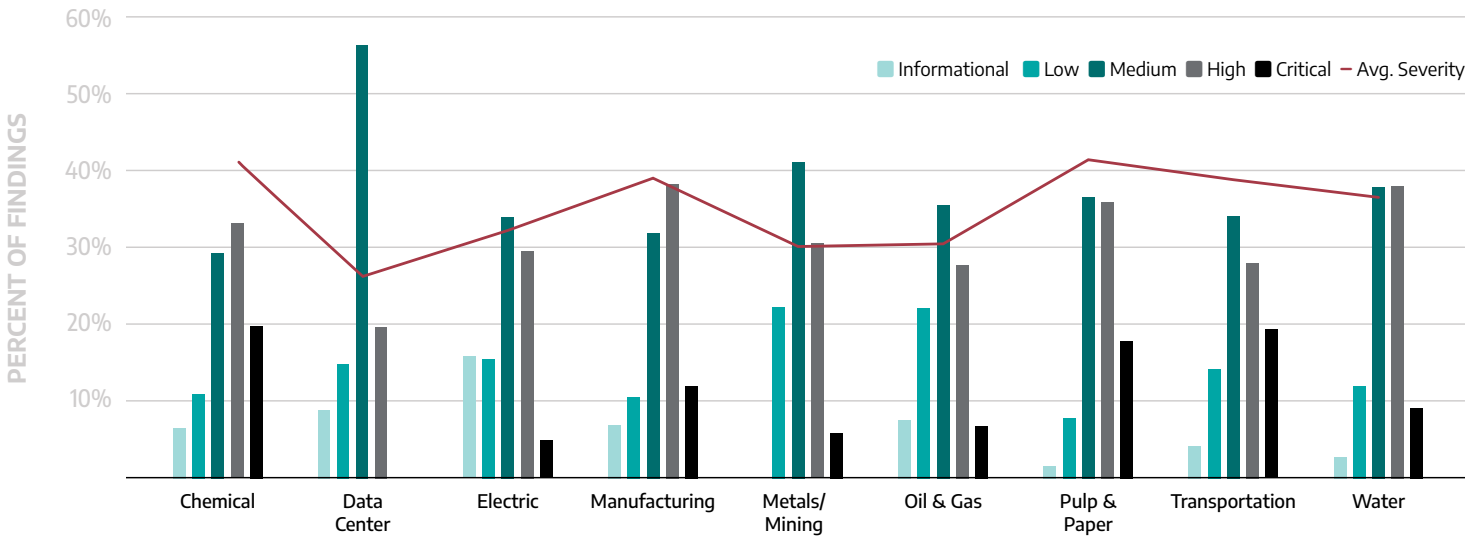


Figure 1: Findings Severity per Vertical

NEW THREAT GROUP ACTIVITY

Dragos observed 10 active Threat Groups during 2023, including three new Dragos-identified Threat Groups: **GANANITE, VOLTZITE,** and **LAURIONITE**. These new threat groups conduct primarily long-term reconnaissance and intellectual property theft operations. Of the three, **VOLTZITE** has been most active in targeting critical infrastructure organizations. Dragos has not identified **VOLTZITE, GANANITE,** or **LAURIONITE** utilizing any ICS-specific capabilities; however, their persistent interest and activities within critical infrastructure sectors warrant monitoring and preparedness by ICS/OT organizations.

Dragos observed all three threat groups conducting diverse operations against various organizations, including cybersecurity research firms, government and military defense entities, rail, manufacturing, automotive, and utilities. **GANANITE** and **LAURIONITE** have exhibited an opportunistic approach to their initial access operations; however, **VOLTZITE's** operations strongly indicate espionage and reconnaissance objectives in the Asia-Pacific region and the United States – particularly the electric sector.

All three newly identified threat groups possess capabilities that target and exploit public-facing infrastructure used or owned by victim organizations. Types of infrastructure included but were not limited to targeting public internet-facing Sierra Wireless Airlink devices, Fortinet FortiGuard, VPN infrastructure, and Oracle eBusiness Suite iSupplier Web Services.

Dragos Frontline Perspective

Dragos observed threat groups, including **GANANITE** and **LAURIONITE**, targeting some of these sectors with the least mature environments (transport, manufacturing, water utilities). Dragos assesses a sector's level of maturity based on the number and severity of findings observed by Dragos during its assessment in those respective environments. Organizations in these sectors should understand the elevated risk this presents. Threat groups have been observed using certain MITRE ATT&CK techniques. Dragos uses these TTPs to correlate threat actor behavior with field observations.

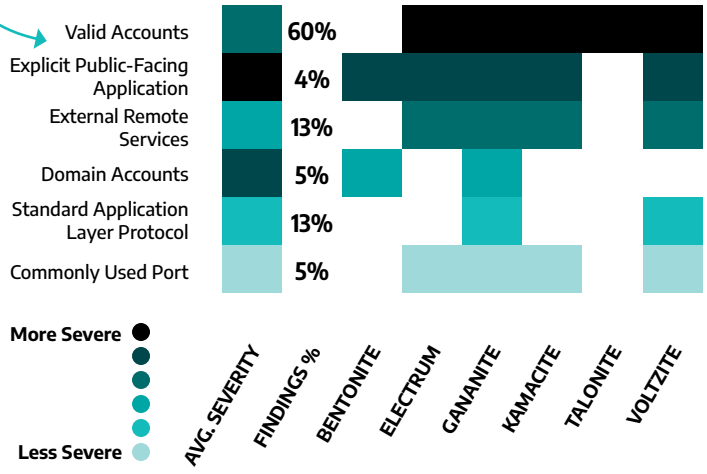


Figure 2: Findings and MITRE TTPs by Threat Groups Using Public Exploits

Dragos Frontline Perspective

Exploiting public-facing devices and external services is a common technique that Dragos observed four Threat Groups utilizing in 2023. A defensible architecture to protect against this technique includes multiple layers of defense, secure remote access setup with MFA, and monitoring.

20%

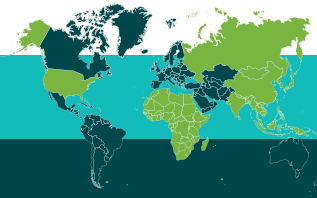
Dragos issued findings related to externally facing networks such as the internet in 20 percent of engagement reports.

28%

Dragos found inadequately configured firewalls protecting OT environments in 28 percent of engagements in 2023.

DRAGOS
SAFEGUARDING CIVILIZATION

VOLTZITE



TARGETS: UNITED STATES, ASIA, AFRICA

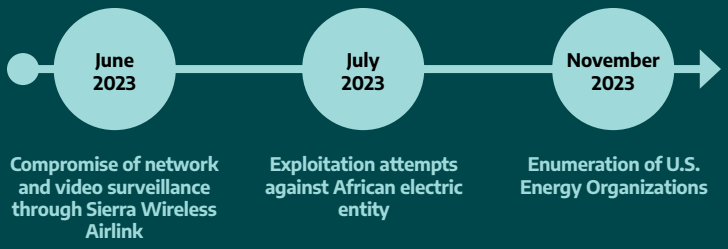
VOLTZITE, a Dragos-tracked threat group that has operational overlaps with Volt Typhoon (first reported on by the U.S. Cybersecurity and Infrastructure Security Agency and Microsoft in May 2023), was performing reconnaissance and enumeration of multiple US-based electric companies, and since then has been observed targeting electric power transmission and distribution, emergency services, telecommunications, defense industrial bases, and satellite services. **VOLTZITE's** actions towards US electric entities, telecommunications, and GIS systems signify clear objectives to identify vulnerability within the country's critical infrastructure that can be exploited in the future with destructive or disruptive cyber attacks. While **VOLTZITE** has traditionally targeted US facilities, we also are aware of the group targeting organizations 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.

KEY HIGHLIGHTS

- **Heavily utilized living off the land techniques to inhibit the potential identification of malicious activity.**
- **Conducts offensive operations with a significant focus on detection evasion and sophisticated operational security tradecraft.**
- **Conducts slow and steady reconnaissance against a target focusing on credential theft, lateral movement, and long-term espionage.**
- **Exploits internet accessible SOHO routers, using them as intermediary hops back to adversary controlled infrastructure.**

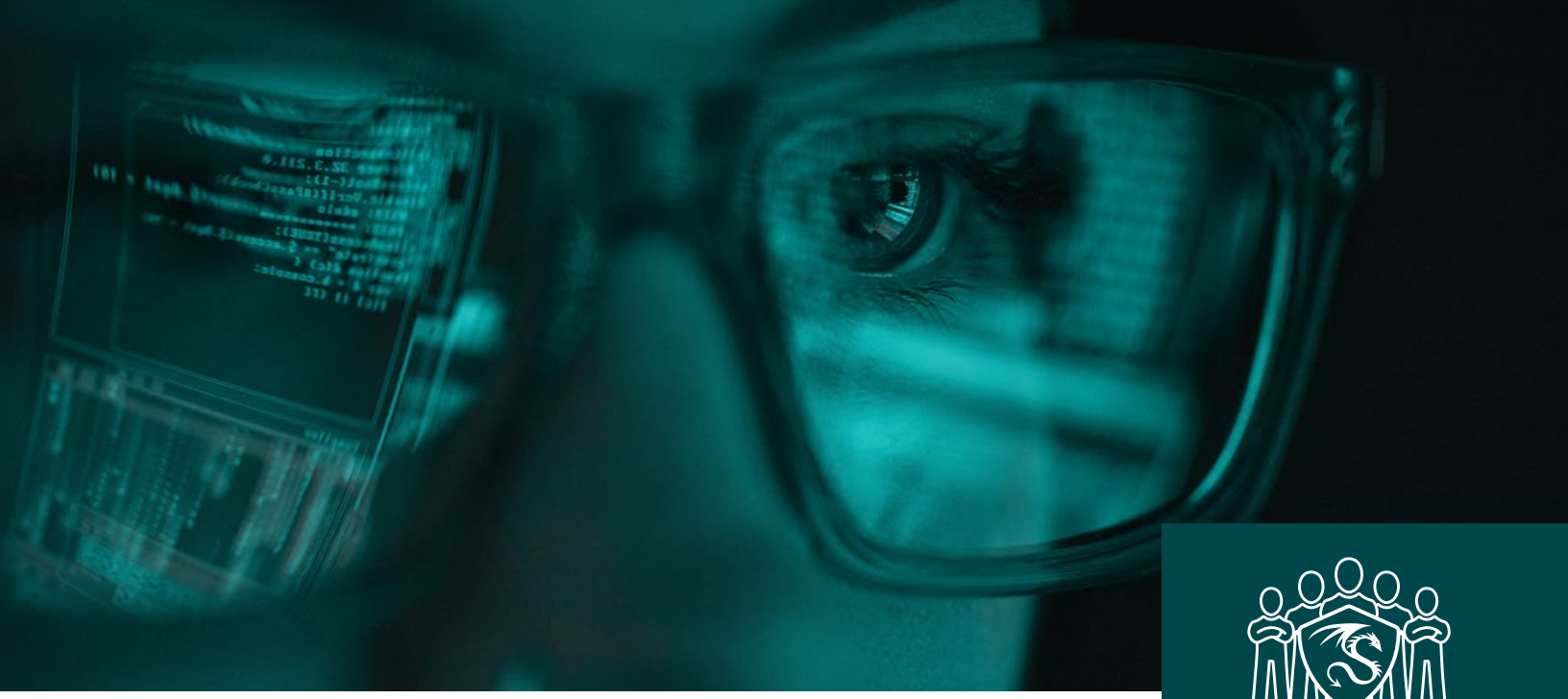
NOTABLE ACTIVITY



- **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 organizations in November 2023.**

Impact and Implications

VOLTZITE conducts enumeration against victims' internet-facing assets in a slow and sustained fashion, likely to lessen the chance of being detected. Once they have exploited a victim's internet-facing asset, they exhibit consistent use of living off the land techniques, making detection more difficult for defenders. **VOLTZITE's** 2023 behavior suggested operational objectives of espionage and information gathering. Data stolen from operational technology (OT) 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 ICS networks.



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

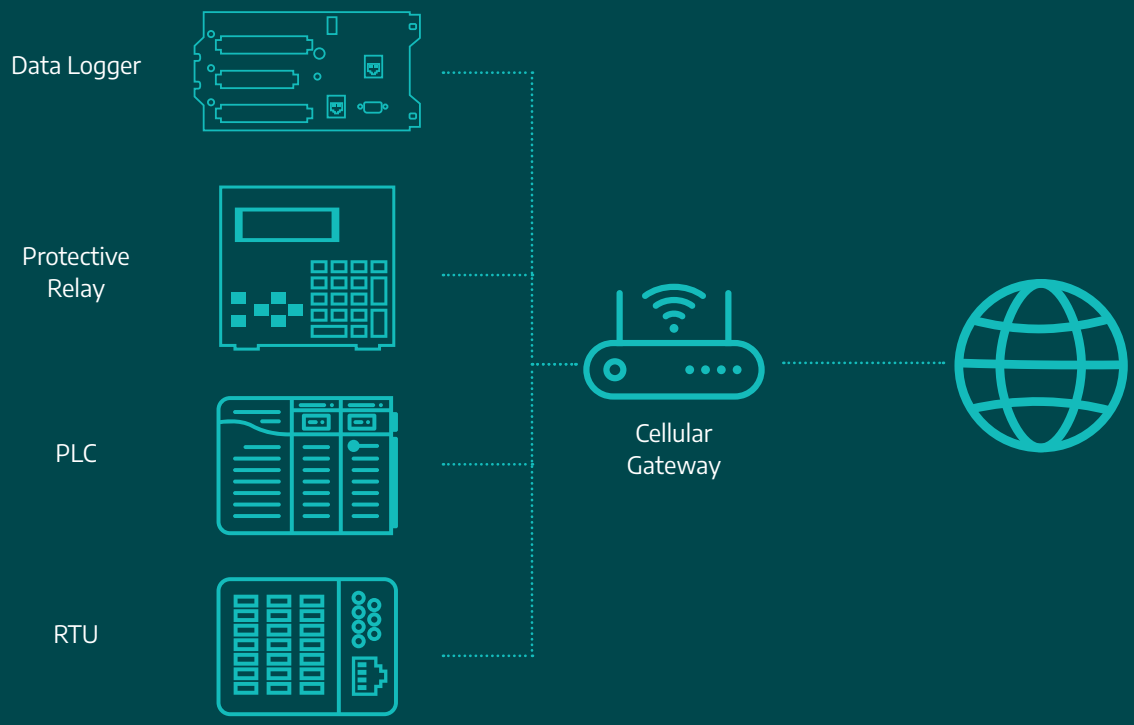
OT Watch Threat Hunting Uncovers VOLTZITE

- 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 utilized 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 analyzing Neighborhood Keeper data for indications of **VOLTZITE** behaviors 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.

Dragos Frontline Perspective

Asset owners often deploy cellular gateways such as the Sierra Wireless devices in remote locations where wired connections are not practical or economical. These gateways are usually connected directly to OT devices, exposing those devices to misconfiguration or vulnerabilities of the gateway. Given the limited visibility and reliance on a single layer of protection when a gateway and connected device are compromised, long adversary dwell times are possible.



Dragos has seen these devices used by utilities for pole-top deployments connected to CAP banks and reclosers and at remote pump stations, storage tanks, and lift stations. Further, Dragos has seen their use in MET towers, small hydro, distributed solar, and storage in generation environments. The most concerning instances are when Dragos has found cellular gateways connected to larger control systems such as a DCS or PLC Process Control Network (PCN) as a remote access mechanism that bypasses standard security controls. Organizations must have an accurate asset inventory and visibility to protect against the risk that these types of devices introduce to an industrial environment.

DRAGOS
SAFEGUARDING CIVILIZATION

GANANITE

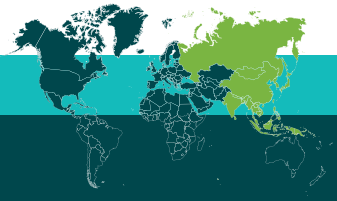
GANANITE is a Dragos-designated Threat Group that targets critical infrastructure and government entities in the Commonwealth of Independent States and Central Asian nations. **GANANITE** focuses on espionage and data theft, with the possibility of handing off initial access to other threat groups. **GANANITE** focuses persistently on its target sets by employing many known tools to infiltrate its victims. Building on the use of StinkRAT and publicly available proof of concept exploits for internet-exposed endpoints, **GANANITE** also exhibits use of tooling such as TELEMIRIS and JLORAT, which has been attributed by Kasperky as being exclusively used by a threat group under the direction of or working with TURLA.

Impact and Implications

GANANITE has been observed conducting multiple attacks against key personnel related to ICS operations management in a prominent European oil and gas company, rail organizations 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, their assessed capabilities show efficient use of multiple phases across Stage 1 of the ICS Cyber Kill Chain.

Gn

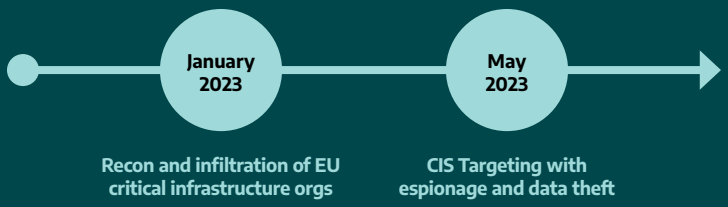
TARGETS: ASIA



KEY HIGHLIGHTS

- **Leveraged publicly available proof of concept (POC) exploits for internet-exposed endpoints, along with many remote access trojans (RAT), such as Stink Rat, LodaRAT, WarzoneRAT, and JLORAT.**
- **Use of energy -focused phishing lures.**
- **Exfiltrated web browser information from victim machines using Telegram in addition to traditional C2 methods over HTTP and HTTPS.**
- **Conducted in-depth reconnaissance of target organizations through Shodan and FOFA to build a profile of the target and potential vulnerabilities of the exposed asset.**

NOTABLE ACTIVITY



- **On January 13, 2023, TR-2023-01 documented reconnaissance against and infiltrated various European critical infrastructure organizations. Along with credential capture via masqueraded domain phishing pages, the adversary utilizes an open-source Python RAT named Stink.**
- **In May of 2023, GANANITE continued targeting government and industrial organizations 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.**

Dragos Frontline Perspective

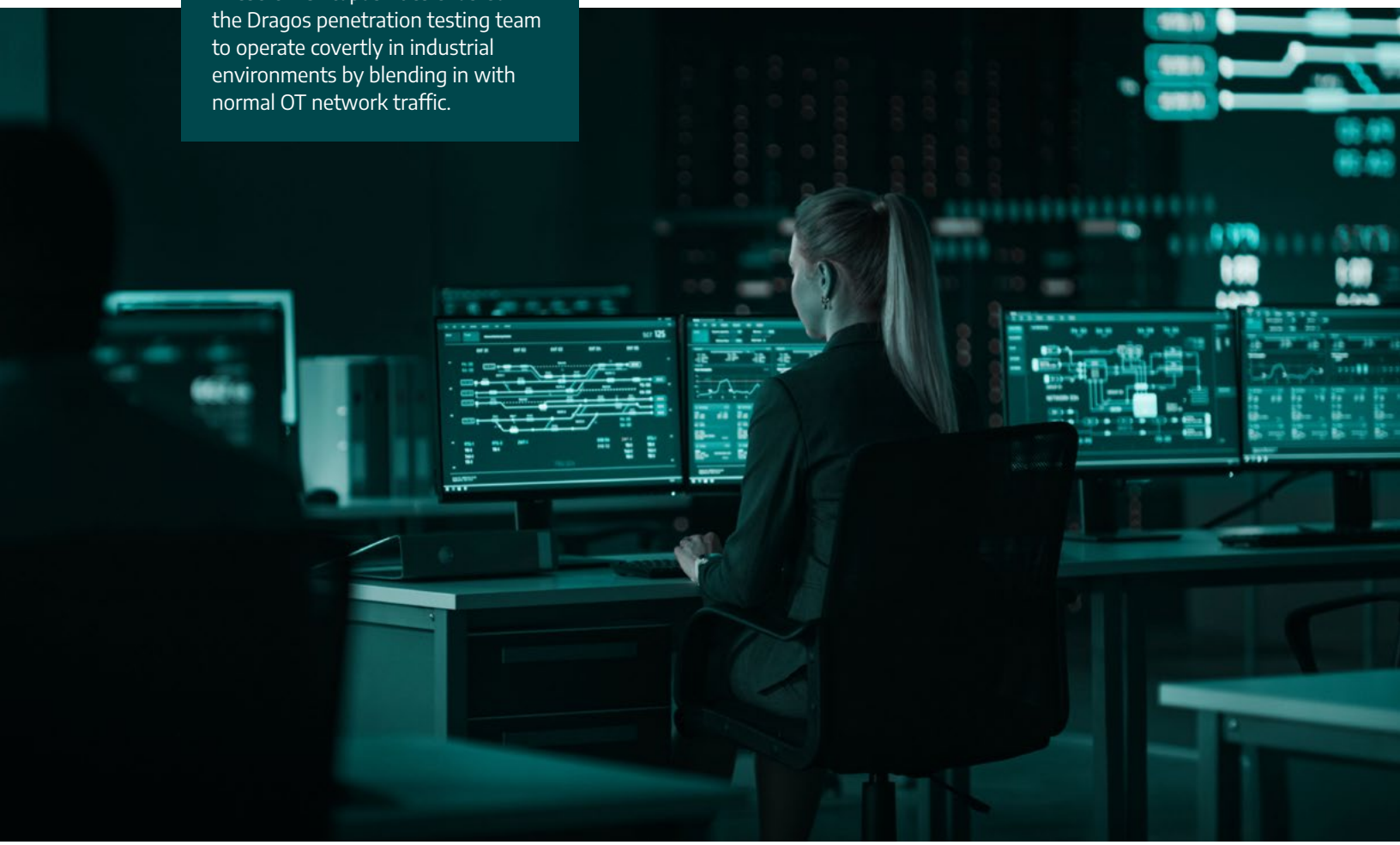
ICS attacks comprise of two parts: a penetration of the enterprise IT environment (Stage 1) which allows for a crossing into the ICS network, culminating in final reconnaissance and penetration of control system resources (Stage 2). It's worth noting that Stage 1 does not always take place in a victim's IT environment, but the compromise may be in a vendor's environment that has access to the enterprise's OT environment.

Dragos Frontline Perspective

Adversaries use command and control (C2) to communicate with and control compromised systems by leveraging standard protocols like HTTP, HTTPS, or DNS for communication channels. C2 capabilities have progressed to the point where some frameworks can integrate third-party applications or non-traditional network protocols to facilitate or hide C2 traffic. Dragos researches how threat groups use common OT protocols for C2 operations and develop capabilities as part of a proof of concept.

Dragos focused on open platform communication unified architecture (OPC UA) and DNP3, given its widespread utilization across a range of critical industrial environments and the availability of robust open-source libraries for each protocol. These OT C2 capabilities enabled the Dragos penetration testing team to operate covertly in industrial environments by blending in with normal OT network traffic.

Further, **GANANITE's** operations have displayed extensive research and use of known exploits against the external perimeter of its targets. **GANANITE** uses tools such as Shodan and FOFA search engines that contain data about internet-facing assets to build a profile of its target. After identifying the IP netblocks of its target, they then utilize data from Shodan and FOFA to identify any presence of devices exhibiting known exploitable vulnerabilities. **GANANITE** then moves on to exploit those vulnerabilities with publicly available exploits. For those reasons, industrial organizations in Europe and Central Asia face a significant risk from **GANANITE** due to their initial intrusion capabilities, post-compromise espionage TTPs, and intellectual property theft, all of which can be used in follow-on attacks against the victim organizations.



DRAGOS
SAFEGUARDING CIVILIZATION

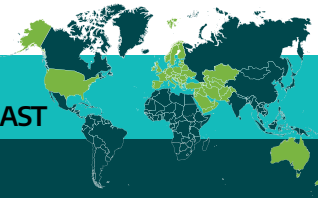
LAURIONITE

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. This group utilizes a combination of open-source offensive security tooling and public proof of concepts to aid in their exploitation of common vulnerabilities.

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 from Reconnaissance to Actions on the Objective. The adversary operators show expertise in various offensive cyber operation skills in navigating target systems, exploiting vulnerabilities, maintaining persistence, conducting lateral movement, internal reconnaissance, defense evasion, and exfiltration.

Oracle E-Business Suite is one of the most widely used enterprise solutions for integrated business processes, including numerous industrial organizations such as United States Steel and Unifi textile manufacturing.

By utilizing compromised infrastructure, **LAURIONITE** can remain undetected or overlooked due to its origin being from trusted or known organizations.



TARGETS: UNITED STATES, AUSTRALIA, EUROPE, MIDDLE EAST

KEY HIGHLIGHTS

- **Leveraged CVE-2022-21587 and CVE-2022-21589 to exploit Oracle iSupplier instances.**
- **Utilized LOLBins or LOTL Binaries to maintain a stealthier profile. Uses these tools to exploit system vulnerabilities, establish persistence, conduct lateral movement, perform internal reconnaissance, and exfiltrate victim data.**
- **Utilized Behinder and Godzilla webshells and open-source security tools such as netcat, proxychains, Neo-reGeorg, and Pwncat-cs.**
- **Performed offensive operations against other targets from compromised victim infrastructure.**

NOTABLE ACTIVITY

March 2023

Targeting and exploitation of Oracle iSupplier

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

Impact and Implications

While current observations and visibility of **LAURIONITE** operations do not indicate the adversary seeks to advance to OT networks, Dragos cannot discount this as a possible course of action the adversary may select in the future. **LAURIONITE** actively seeks out iSupplier instances with a significant presence across many industry verticals and sectors, including industrial organizations such as manufacturing.

Targeting companies that use Oracle's E-Suite iSupplier technology may not inherently impact OT assets; however, the nature of enterprise resource planning software such as iSupplier could allow adversaries like **LAURIONITE** to gain visibility into third-party vendor relationships, which can lead to follow-on intrusion operations.

Dragos Frontline Perspective

Dragos often finds that during tabletop exercises, organizations don't fully understand how OT processes depend on business systems. A compromise of a critical business system can impact operations unless the asset owner understands these dependencies and puts sufficient mitigations in place. This risk was highlighted in the 2021 ransomware attack against Colonial Pipeline, in which cyber attacks against enterprise business applications resulted in significant downstream impacts on industrial operations.

UPDATES ON SOME OF THE MOST ACTIVE THREAT GROUPS

ELECTRUM

ELECTRUM, a Dragos-tracked threat group that overlaps with Sandworm, was highly active throughout 2023 and their operations were largely influenced by the Ukraine-Russia conflict. For example, a new wiper malware was identified in June 2023 with characteristics similar to RoarBat and was used to target Windows operating systems. ELECTRUM has used wiper malware previously, such as AcidRain and CaddyWiper, which was previously part of the INDUSTROYER2 event. Another noteworthy ELECTRUM observation involving wiper malware came in November 2023 when Mandiant published a report about disruptive cyber attacks against a Ukrainian electric substation in October 2022. In that attack, ELECTRUM exploited a vulnerable hypervisor running end-of-life MicroSCADA software in the OT environment and used a (then) new version of CaddyWiper malware.

RASPITE & MAGNALLIUM

Dragos also observed that threat groups such as **RASPITE** and **MAGNALLIUM** conducted widespread campaigns scanning for vulnerable SMB devices and using password-spraying techniques against various industry sectors, including defense and mining. Interestingly, **MAGNALLIUM** is a Dragos-tracked threat group that had seemingly disappeared for nearly a year until they began their password-spraying operations again in July 2023 against multiple defense and mining organizations. Prior **MAGNALLIUM** cyber operations have included initial access and reconnaissance actions before deploying destructive wiper malware on the victim's IT networks.

Dragos Frontline Perspective

Dragos's tracked threat groups are based on clusters of activity relevant to assessed capabilities, intent, victimology, and infrastructure. From our perspective, it is common for Dragos-tracked threat groups to go into periods of dormancy. This dormancy can be because their operational objectives have shifted, they are conducting more IT-oriented cyber attacks against a broader range of entities that do not fall within the industrial organization category, or they are developing new tools and standing up new infrastructure to stay ahead of security researchers and law enforcement.

KAMACITE

In addition to the **ELECTRUM** activity, **KAMACITE** continued targeting Ukrainian telecommunications entities through early 2023 using spearphishing and the DarkCrystal remote access trojan and then leveraging LOTL techniques within victim networks. This activity continues a multi-year trend of **KAMACITE** conducting initial intrusion operations against Ukraine entities and, more broadly, reconnaissance operations against global industrial entities likely in pursuit of enabling follow-on intrusion operations from threat groups like **ELECTRUM**.

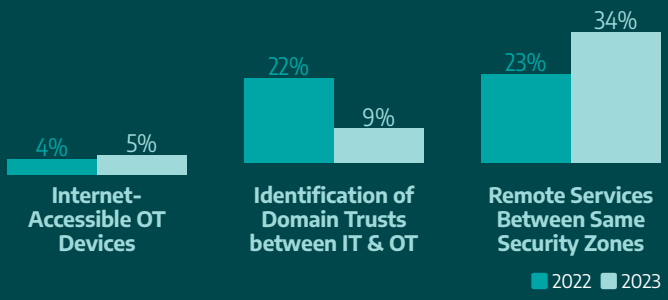
Dragos Frontline Perspective

The DarkCrystal remote access trojan (a.k.a. DCRat) is a widely available remote access trojan first observed in 2018 and has been used by numerous adversaries with varying levels of sophistication and capabilities. DarkCrystal RAT is often available through Darknet criminal forums and marketplaces and can be used to remotely access compromised networks, steal information such as user credentials from victim networks, and collect network information.

Dragos Frontline Perspective

Dragos leveraged its visibility of adversary activity to mirror commonly used and emerging tactics, techniques, and procedures (TTPs) when conducting penetration testing. This includes using public-facing reconnaissance and open-source intelligence (OSINT) to understand exploitation paths into an environment. Once initial access was established, the focus shifted to establishing persistence, expanding access, and compromising the OT objectives.

Throughout 2023, Dragos leveraged common MITRE ATT&CK information-gathering tactics, including Reconnaissance (TA0043), Discovery (TA0102), and Initial Access (TA0108) to identify potential accounts and assets that could be exploited. This included finding internet-accessible OT assets (5 percent in 2023, up slightly from the 4 percent observed in 2022), identifying domain trusts between IT and OT (9 percent in 2023, down 13 percent from 22 percent in 2022), and remote services between the same security zones (34 percent in 2023, a slight increase from 23 percent observed in 2022).



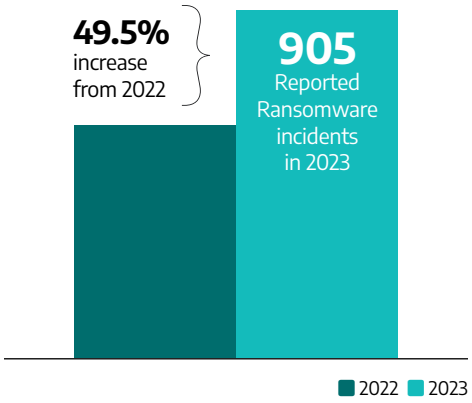
Once the Dragos team gained initial access, the priority became gaining Persistence (TA0110) where applicable and Laterally Move (TA0109) throughout the target environment, inching closer to OT Crown Jewels. The Dragos team identified many lateral movement techniques in 2023 but often leveraged common avenues to illustrate security gaps between IT and OT environments.

In 2023, on almost 5 percent of network penetration tests, the Dragos team moved laterally throughout an OT environment using Default Credentials (T0812). They also found that Hardcoded Credentials (T0891) can lead to the same result or even increased access. Dragos identified custom Python and PowerShell scripts that perform automated functions across domains, networks, and assets in multiple assessments. These cleartext and default credentials were collected and tested across the in-scope assets to identify credential reuse or misuse.

2023 INDUSTRIAL RANSOMWARE ANALYSIS

INCREASE IN RANSOMWARE ACTIVITY

Dragos observed 50 active ransomware groups impacting industrial organizations in 2023 out of 77 groups that have historically attacked industrial organizations and infrastructure. This represents a 28 percent increase over last year. Dragos tracked 905 reported ransomware incidents impacting industrial organizations in 2023, a 49.5 percent increase from 2022. Industrial organizations 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. This leads to high-leverage situations.



Ransomware adversaries and their activity vary widely in techniques employed and sophistication demonstrated – and they have impacted a broad range of industrial targets in 2023. Hundreds of ransomware variants exist in the wild, such as LockBit, ALPHV, Hunters International, Rhysida, and NoEscape. Although there are more ransomware groups in the wild than were active in 2023, it is important to remember that a widespread practice within the criminal ecosystem is for groups to rebrand and create offshoot ransomware variants.

Dragos Frontline Perspective

ALPHV, BlackCat, and Darkside (the perpetrators of the Colonial Pipeline attack) are evidence of this type of ransomware rebranding and codesharing. All three groups share commonalities in code, infrastructure, and TTPs, and some aspects can be traced back to an older group, REvil.

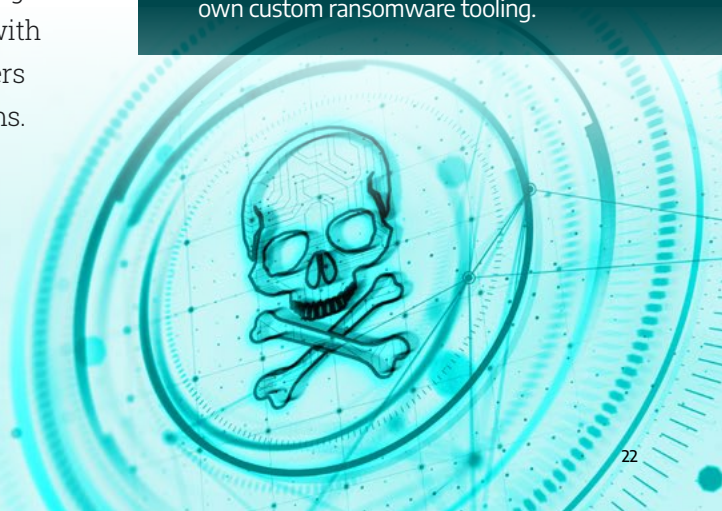
INDUSTRIAL RANSOMWARE ATTACKS

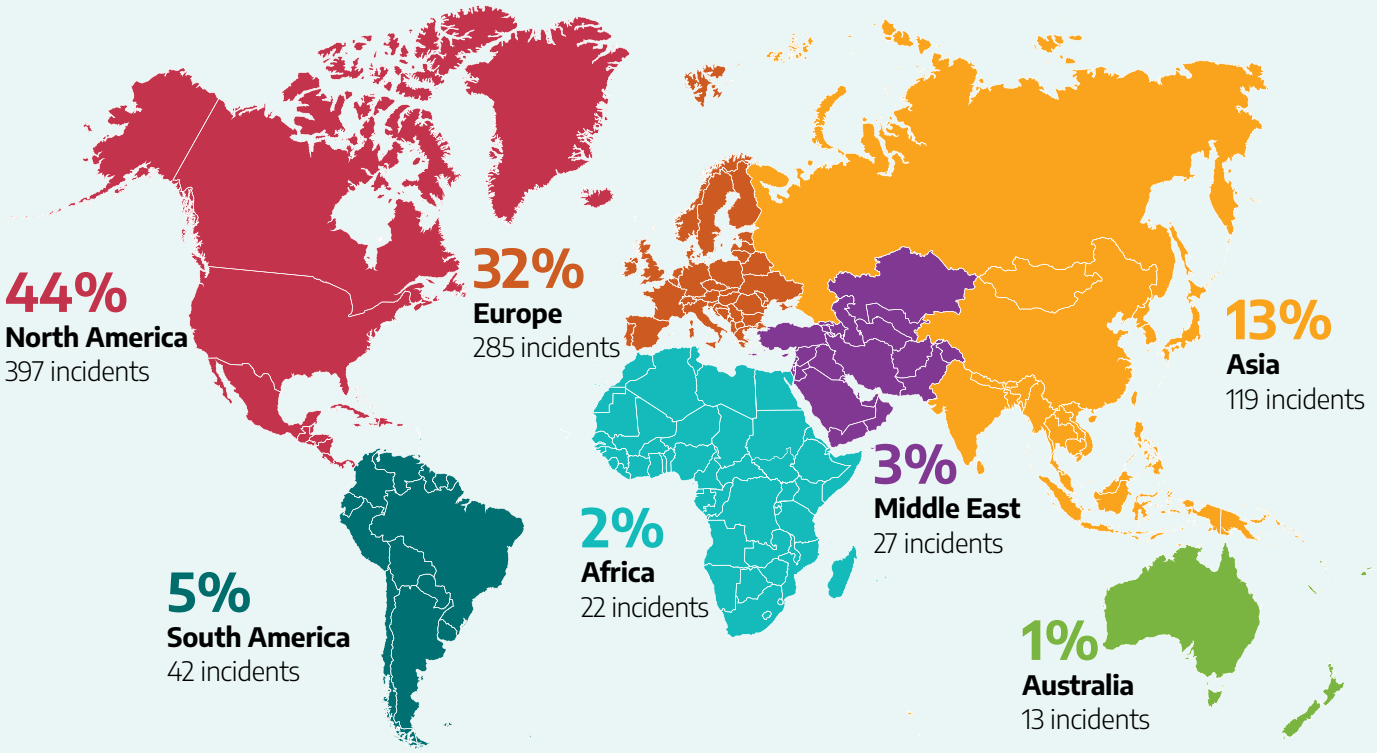
LockBit ransomware was the most-used ransomware variant against industrial organizations throughout 2023. Specifically, LockBit operations accounted for 25 percent of the total ransomware incidents against industrial organizations in 2023, with ALPHV and BlackBasta accounting for 9 percent each. LockBit, like many ransomware groups, operates as a Ransomware-as-a-Service (RaaS) provider.

LockBit operators capitalize on extortion tactics to increase the probability of the victim paying the ransom. One such tactic is stealing sensitive data, including industrial data from victim organizations, with StealBit, an information stealing tool created by the LockBit developers and typically deployed before LockBit encrypts compromised systems. If the victim doesn't pay the ransom, the stolen data is posted to the LockBit dark web resources, which other adversaries can leverage.

Dragos Frontline Perspective

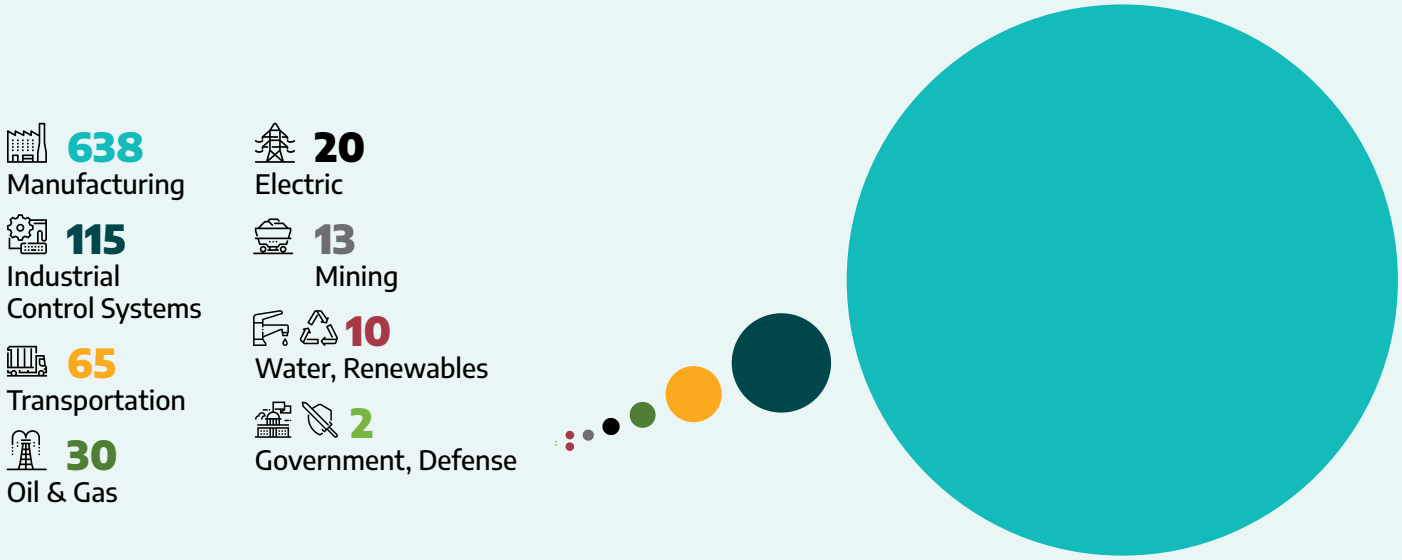
Ransomware-as-a-Service is a model where ransomware purveyors "rent" access to their proprietary ransomware infrastructure, which creates a low-barrier-of-entry option for lesser-skilled adversaries wishing to profit from ransomware operations. The ransomware purveyors' profit from affiliates renting their infrastructure, and they also get a percentage of any successful ransomware operations. Affiliates that rent access to the ransomware purveyor's infrastructure benefit from not having to develop their own custom ransomware tooling.





Ransomware is a global threat; however, the majority of ransomware attacks impacted organizations in North America with 44 percent of incidents, with Europe being the second most common target with 32 percent.

Figure 4: Ransomware Incidents by Continent • 2023



The most common sector impacted in 2023 was manufacturing, with 71 percent of ransomware incidents.
The industrial control systems sector, which is made up of companies that develop OT equipment and applications, was the second most impacted sector with 13 percent.

Figure 5: Ransomware Incidents by Sector • 2023

INDUSTRIAL RANSOMWARE TRENDS

EXPLOITING KNOWN VULNERABILITIES

Ransomware operators' primary methods to gain initial access to victims' networks have remained steady in 2023, including collaborating with initial access brokers,[2] phishing, and exploiting publicly accessible network assets, such as VPNs and RDP servers. Dragos also observed ransomware campaigns exploiting public-facing services such as Citrix using the Citrix Bleed vulnerabilities. These ransomware groups include Lockbit, BlackBasta, and ALPHV. Ransomware operators are highly adept at capitalizing on recently disclosed vulnerabilities like Citrix Bleed. They often quickly develop or use available exploitation capabilities against those vulnerable technologies and integrate that exploitation code into their ransomware operational framework. The timeline for the rapid spread of Citrix Bleed activity, which impacted numerous industrial organizations is shown below.

Dragos Frontline Perspective

Dragos Incident Responders observed this exploit impacting industrial customers during their work this year. In one case, the Dragos responders identified that Citrix Bleed vulnerability was the initial attack vector after a reconnaissance phase where the victims' external infrastructure was scanned.

Date	Event
10 October	Citrix discloses CVE-2023-4966 and CVE-2023-4967
17 October	Mandiant reports in-the-wild zero-day exploitation since at least late August 2023
23 October	Proof-of-Concept (PoC) code to exploit the vulnerability published to GitHub
24 October	GreyNoise starts detecting in-the-wild exploitation exploits
27 October	Mass exploitation of vulneratility underway. Suspected exploitation by Ransomware group. Boeing added to LockBit 3.0 leak site.
10 November	LockBit 3.0 ransomware attack against the Industrial and Commercial Bank of China (ICBC) and DP World
11 November	Evidence of Lockbit 3.0 victim running vulnerable Citrix appliances
16 November	Medusa ransomware attack against Toyota Financial Services — suspected access via German office running a vulnerable Citrux appliance
21 November	Joint Cybersecurity Advisory released

Another example of this type of activity is from May 2023, following the public disclosure of a MOVEit zero-day vulnerability. The *Cl0p* ransomware group leveraged this vulnerability to gain initial access and claimed numerous victims. Some of these victims include critical infrastructure organizations, government entities related to critical infrastructure, and organizations that support essential infrastructure operations. The impact of vendors and service providers can be especially problematic, given their role in supporting control systems.

Dragos Frontline Perspective

Investigation and analysis by Dragos have yielded some important insights into *Cl0p's* activities. Notably, Dragos was able to recover targeted process names associated with specific hash values embedded in a *Cl0p* sample. While most of these are IT-related processes, *Cl0p* ransomware does contain targeting of OT-related processes found on Windows operating systems. However, it does not use or target OT-specific protocols. *Cl0p* has the ability to stop many running computer programs associated with OT vendors such as Honeywell, IBM, Mitsubishi Electric, Rockwell, Schneider Electric, Siemens, and more.

[2]Initial Access Brokers (IABs) are cyber adversaries that opportunistically attack organizations to gain access into their networks usually through exploiting weak credentials, phishing, and watering hole techniques, and then sell that access to other cyber threats on Darknet marketplaces and forums.

LACK OF SUFFICIENT SECURITY CONTROLS

Regardless of the methods used to gain access to a victim's environment, the ransomware groups' ability to impact industrial environments depends largely on the types of security controls network defenders have in place. For most of the environments that Dragos works within, assets are not directly connected to a public-facing network but are instead behind at least a single layer of defense, such as a firewall or a proxy. The effectiveness of these security controls varies greatly, and organizations should not assume that a single layer is sufficient protection.

Dragos issued findings on segmentation issues or improperly configured firewalls in 28 percent of our engagements in 2023. Like many observations, this varies significantly across industries. Dragos continues to observe network segmentation issues in transportation and manufacturing more frequently than other industries for instance.

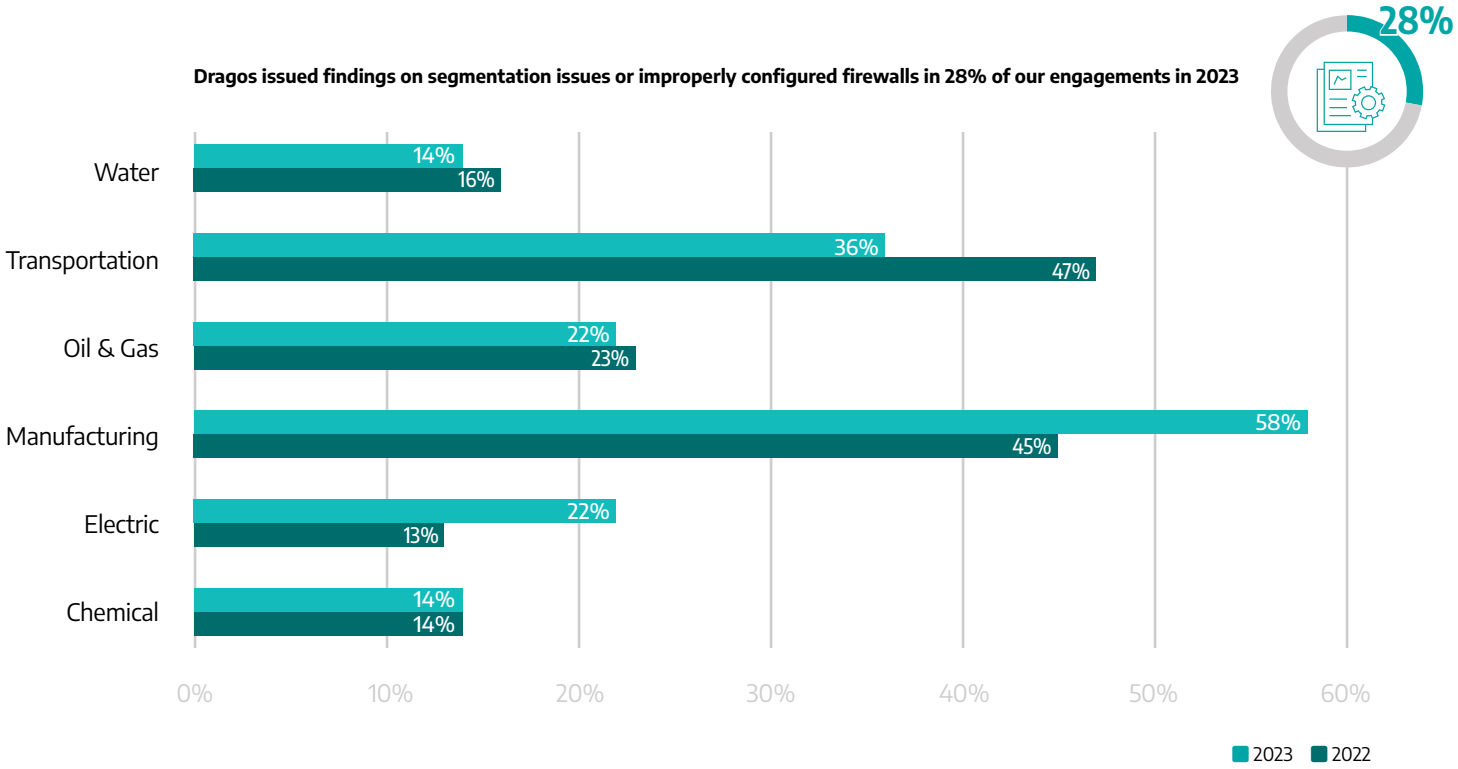


Figure 6: Reports Containing Segmentation Findings

Dragos Frontline Perspective

In 2023, Dragos observed that approximately 70 percent of OT-related incidents originated from within the IT environment. Network segmentation and separate domains are key architectural changes recommended as mitigations for these incidents.

LEVERAGING LIVING OFF THE LAND TECHNIQUES TO FURTHER ACCESS

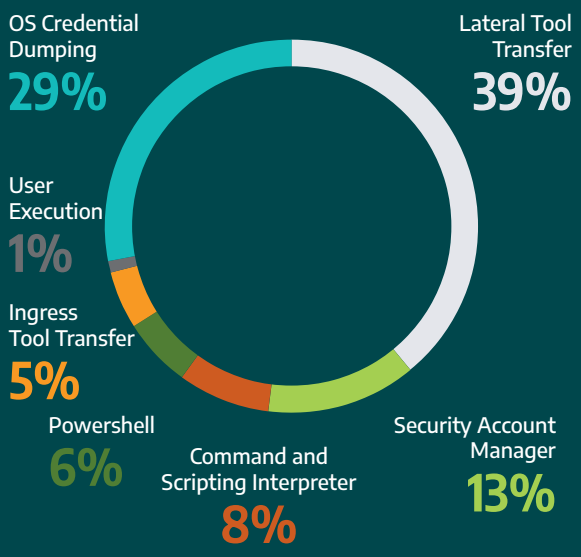
Post-compromise TTPs will vary slightly between ransomware groups and their affiliates, but most leverage LOTL techniques. This includes using native tools like PsExec and PowerShell to move laterally through the victim's network and discover highly desirable targets. After establishing remote access to one of these targets, threat groups continue to leverage LOTL tools to escalate privileges (Task Manager, BitsAdmin, and WMIC), gain persistence (Scheduled Tasks), and establish command-and-control (SSH and Rundll32) channels.

The figure at right shows the LOTL TTPs used by the different pen test teams. In addition to using LOTL, adversaries will also use non-native tools. Over the year, Dragos OT Watch threat hunters found unexpected remote access tools running in over 10 percent of customer OT environments. Ransomware groups use these tools and associated TTPs to move throughout an environment and compromise systems. Microsoft Active Directory often becomes a primary target. Ransomware groups have been observed using tools as well as LOTL techniques to compromise Active Directory to gain access to valid accounts.

Dragos Frontline Perspective

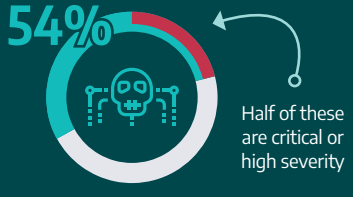
Dragos utilized these same LOTL techniques effectively in 63 percent of its penetration testing engagements across both Stage 1 and Stage 2 of the ICS Cyber Kill Chain. Of the LOTL techniques used by Dragos for penetration testing, Lateral Tool Transfer (T0867) accounted for 39 percent, followed by OS Credential Dumping (T1003) at 29 percent and Security Account Manager (T1047) at 13 percent. Four other LOTL TTPs account for the remaining 19 percent: Command and Scripting Interpreter (T1059), PowerShell (T1086), Ingress Tool Transfer (T1105), and User Execution (T1204).

LOTL TTPs Used by PenTest Team



Dragos Frontline Perspective

To combat this, common TTP of Valid Account (T1078) compromise defenders must implement preventative security controls, including Privileged Account Management (M0926 and M1026), user account management, multi-factor authentication, and password policies. However, most importantly, IT and OT environments should not share an authentication domain.



Dragos found remote access security issues in 54 percent of penetration tests.

Dragos found that 1 in 10 industrial environments have a shared domain architecture.

OT VULNERABILITIES

VULNERABILITY ASSESSMENT OVERVIEW

Vulnerability advisories provide information on common hardware and software vulnerabilities and exposures (CVEs). Dragos analyzes vulnerability advisories associated with ICS/OT environments and prioritizes them so that asset owners of industrial organizations do not have to.

The difference between IT and OT environments is pronounced when assessing vulnerabilities. The type of devices, systems, and protocols used within OT environments, the network architecture of typical OT networks, and the impact vulnerabilities can have on normal operations and the physical world drive these differences. OT Vulnerabilities should be mitigated and addressed differently than IT vulnerabilities based on the strict operational requirements of OT systems (e.g., system uptime and vendor qualification processes).

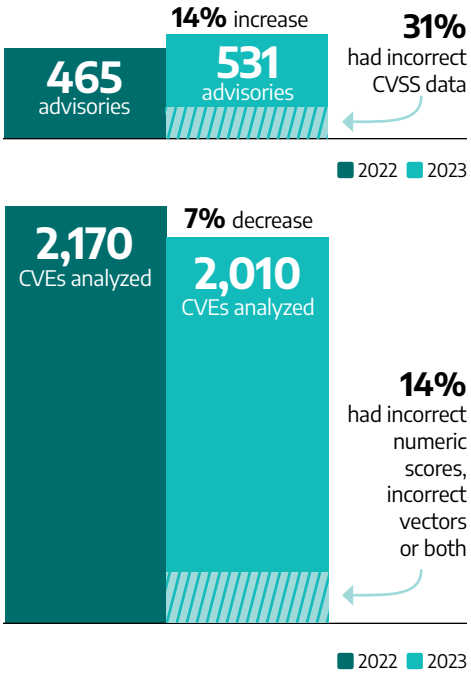
Many vulnerability management programs focus their remediation on 'Critical' vulnerabilities with a CVSS of 9.0 or higher. That is, programs specify that these vulnerabilities should be mitigated with urgency. There are three problems with this approach.

- **First:** Researchers often have no input to the final copy of a public advisory and Common Vulnerability Scoring System (CVSS) scores may be inaccurate. The reliance on industrial OEMs, which differ in maturity levels, makes it difficult for the industrial community to have consistent scoring and severity guidance. Because of this, the vulnerability advisories issued by the vendors and other CVE Numbering Authorities (CNA) are often incorrect and vague.
- **Second:** CVSS does not account for typical OT network architecture. Network-exploitable vulnerabilities are often given a critical score even when the service is not immediately exploitable in a well-architected network.
- **Third:** Advisories often lack practical steps besides 'apply the patch.' Patching OT software, especially firmware, may be difficult or impossible for many organizations. Occasionally, advisories are even released with no patch and no other mitigation advice, making them useless documents for defenders.

Instead, an approach that considers OT environments and requirements yields a better result. This is born out in an analysis of the data at the end of each year.

Dragos Frontline Perspective

Dragos predicts the number of vulnerability advisories relevant to industrial operations will double in the next five years. This rapid growth in vulnerabilities is attributed to vendors and researchers being more focused on OT and because Dragos is tracking an increasing number of sources.



In 2023, Dragos analyzed 2010 CVEs contained in 531 advisories. This is a 14 percent increase in advisories and a 7 percent decrease in CVEs from 2022. As a reminder, Dragos tracked 465 advisories and 2170 CVEs in 2022.

VULNERABILITY ACCURACY

16% of advisories were network exploitable and perimeter facing

Dragos identifies and makes recommendations on vulnerabilities in **23% of its engagements.**

Advisories with no patch when announced

28%

Advisories that had a patch

72%

Advisories that had no mitigation at all

74%

Advisories with no vendor mitigation

73%

Advisories with no alternate mitigation

99%

Advisories with a patch and no mitigation

54%

Advisories with no patch and no mitigation

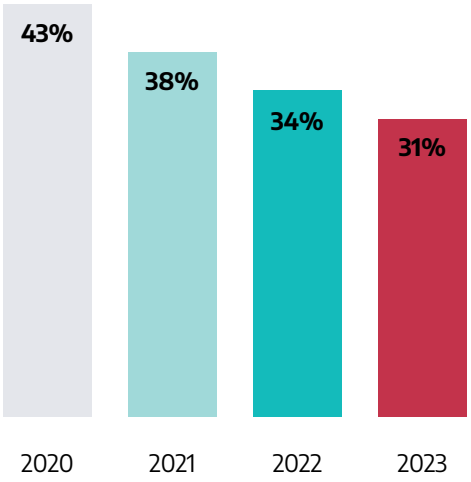
19%

Advisories for which Dragos provided missing mitigation advice

49%

Figure 7: Advisories with Errors and Lacking in Actionable Guidance

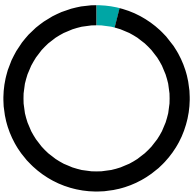
Errors could cause asset owners and operators to waste resources on low-risk vulnerabilities over more severe ones



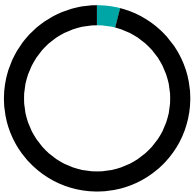
Dragos analyzed 531 advisories
31% had incorrect data

14% of the 2010 CVEs analyzed by Dragos had errors associated with the advisories with incorrect data. Dragos assessed these CVEs to correct the CVSS scores with the below results.

9%
Dragos found to be **MORE SEVERE** than the CVSS score



4%
Dragos found to be **LESS SEVERE**



1%
were the same

Figure 8: The State of ICS/OT Vulnerabilities

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.

Dragos found 9 percent of CVEs in security advisories were more severe according to the CVSS calculator[3] than reported originally. Note that a rise in score should not alarm asset owners as CVSS was not built with industrial control systems in mind. Proper urgency is better defined with **"Now, Next, Never"** prioritization, which is defined more in depth later. After correction, only 1 percent of the advisories had the exact same score.

Dragos Frontline Perspective

Dragos predicts the number of vulnerability advisories relevant to industrial operations will double in the next five years. This rapid growth in vulnerabilities is attributed to vendors and researchers being more focused on OT and because Dragos is tracking an increasing number of sources.

[3] https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

VULNERABILITY RISK MITIGATION

Patching every vulnerability is difficult in OT environments and may not improve OT network security. In fact, patching unnecessarily may bring its own risk – unsuccessful patch application may cause unwanted downtime. In addition, many OT devices and software have "foreverday" vulnerabilities and are insecure by design. This means patching a system to close a vulnerability may do nothing to improve the security of affected components, as underlying design flaws are still present. A far better approach is to focus remediation and mitigation on items that positively impact the overall hygiene of the industrial process.

Addressing vulnerabilities generally means deploying updates or applying security controls that do not already exist. Patching within an OT environment must be done in a way that ensures that normal, safe operations are maintained. Often, this results in patches being delayed until a maintenance window. For this reason, it is important to have alternate methods to mitigate vulnerabilities in an advisory.

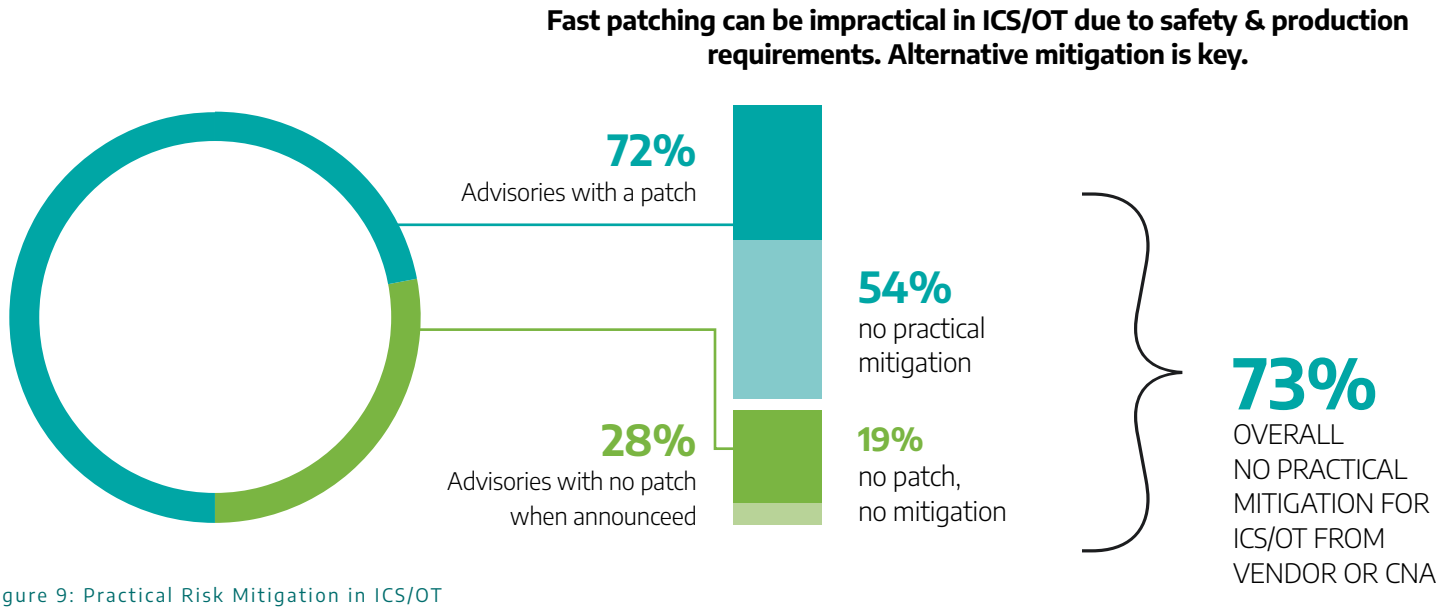


Figure 9: Practical Risk Mitigation in ICS/OT

In 2023, 72 percent of the advisories Dragos analyzed came with a patch, but 54 percent of those advisories with a patch contained no mitigation advice. This is a +1 percent change from last year for patches and +1 percent change for mitigation advice. Dragos provided mitigations for the 49 percent of the advisories that had no mitigations from any other source. Advisories with no patch when announced, accounted for 28 percent of all advisories in 2023, and roughly 19 percent of those without a patch had no mitigation at all. This leaves OT network defenders without many options when often some of the simplest changes in behavior and tooling can have the most significant impact.

NOW, NEXT, NEVER PRIORITIZATION

Prioritizing 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 prioritize and get from the noise of 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.

This methodology prioritizes the vulnerabilities that defenders should mitigate immediately and places them in the **Now** category. Vulnerabilities in the **Next** category can be mitigated through firewall rules and good network hygiene. This second group could be patched on the next maintenance cycle but should be monitored for abnormal network activity or exploitation. Lastly, vulnerabilities that do not increase the inherent risk of the device fall into the **Never** category.

This prioritization considers if the vulnerability is perimeter-facing and easily exploitable, like a VPN bypass, a data historian that may be used as a pivot point, or other weaknesses in a remote access service. These issues could enable an adversary to obtain access to the network. Prioritization also focuses on the vulnerabilities being actively exploited by threat groups today. Dragos looks for advisories with a public POC, making the barrier to entry lower to exploit.

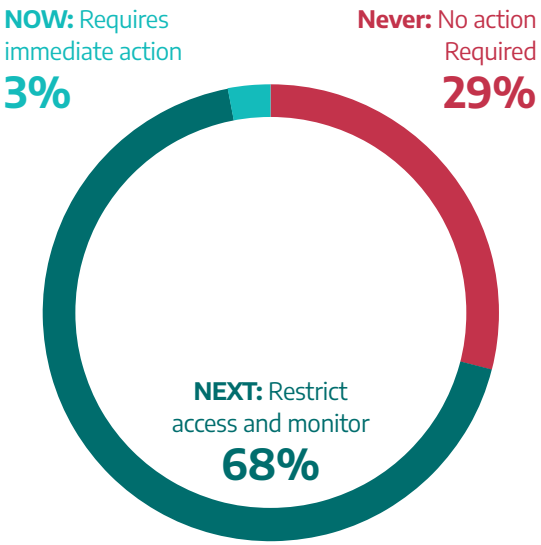
Another priority must be life-safety systems. If a vulnerability introduces the capability to modify the logic on a safety system, that would belong in the **Now** category.

Using the above as the main criteria for 'now' vulnerabilities, Dragos found that only 3 percent of vulnerabilities analyzed in 2023 fell into the **Now** category. Of the 3 percent, 17 percent are given this rating because it's on the network edge and 83 percent because of the vulnerability's capabilities.

In 2022, Dragos became a CNA (CVE Number Authority). A benefit of Dragos being a CNA is that it allows Dragos to work closely with vendors and OEMs to arrive at accurate CVSS scoring, proper mitigations, and prioritization without giving vulnerabilities a brand name. CNAs can also ensure that timely information is released to end users, especially for design flaws where a vendor may require years to redesign the system and close the flaw. Being a CNA gives the researcher freedom to publish mitigation information in these cases.

In 2023, 35 of Dragos-discovered CVEs were publicly disclosed. Eighteen of these CVEs were managed by Dragos as a CNA. These included primarily network-facing vulnerabilities that should not normally be exposed to corporate or internet networks, as well as several file format vulnerabilities that are likely to disclose credentials or overwrite files. None were considered Now-level vulnerabilities, despite several having 'Critical' CVSS scores.

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.



VULNERABILITY SEVERITY

Loss of control and loss of view of the industrial process are among the worst scenarios in an ICS environment. The ability of operations to safely and reliably operate a system depends on an accurate view and control of the industrial process. Dragos investigates the possible impact of vulnerabilities to help organizations focus on the most impactful ones.

In 2023, 53 percent of the advisories Dragos analyzed vulnerabilities that could cause both a loss of view and control of the process through a vulnerable OT system. This was a shift of +3 percent from 2022. A full 46 percent of all the vulnerabilities have no ability to impact the control or visibility of the industrial process. Of these vulnerabilities, 1 percent could only cause loss of view without impacting loss of control.

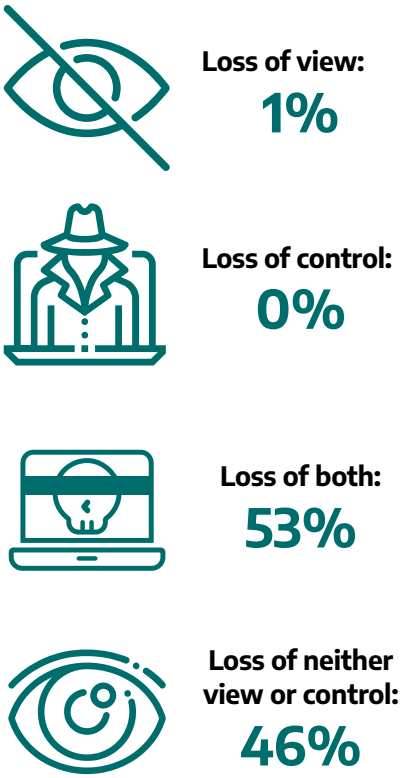


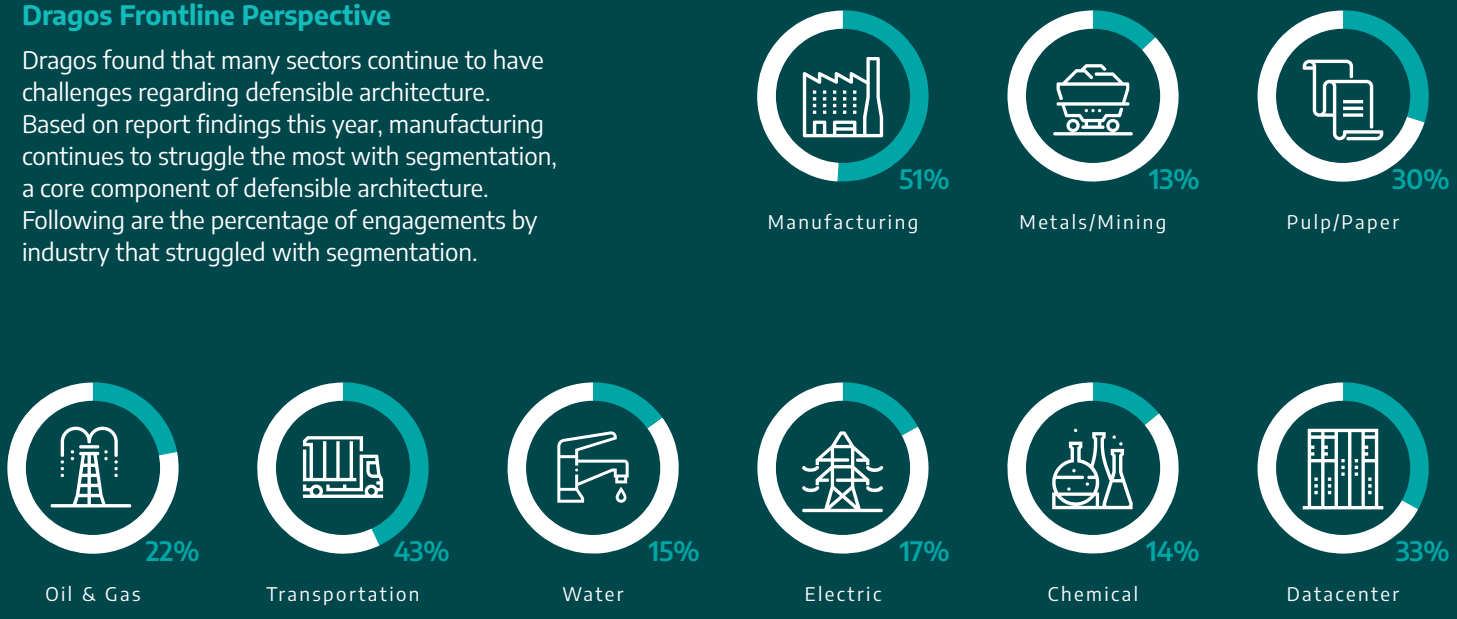
FIgure 10: Loss of view, loss of control, or both

WHERE THE VULNERABILITIES RESIDE IN THE NETWORK

There are different threat profiles for vulnerable assets deep within the ICS network than those at the enterprise's border. A PLC protected by a firewall is less at risk than one directly on the internet. When prioritizing vulnerability mitigation, organizations should consider the network landscape and where vulnerable systems reside in their architecture.

Dragos Frontline Perspective

Dragos found that many sectors continue to have challenges regarding defensible architecture. Based on report findings this year, manufacturing continues to struggle the most with segmentation, a core component of defensible architecture. Following are the percentage of engagements by industry that struggled with segmentation.



Dragos provides expected Purdue levels per advisory assessment based on common placement in a well-designed environment. In a well-designed network, adversaries must compromise multiple layers before impacting industrial processes. This attack path includes gaining initial access to enterprise networks before pivoting to OT networks to compromise systems deep within the ICS network. This makes the opportunity to exploit vulnerabilities deep within the network more challenging.

In 2023, 19 percent of these vulnerabilities were remote access vulnerabilities bordering the enterprise, while 80 percent resided deep within the ICS network. 62 percent pertains to vulnerabilities found at levels 0 to 3 of the Purdue Model, which should have restricted access, among other hardening configurations. This includes restricting access to engineering workstations, PLCs, and sensors, which can impact the industrial process.

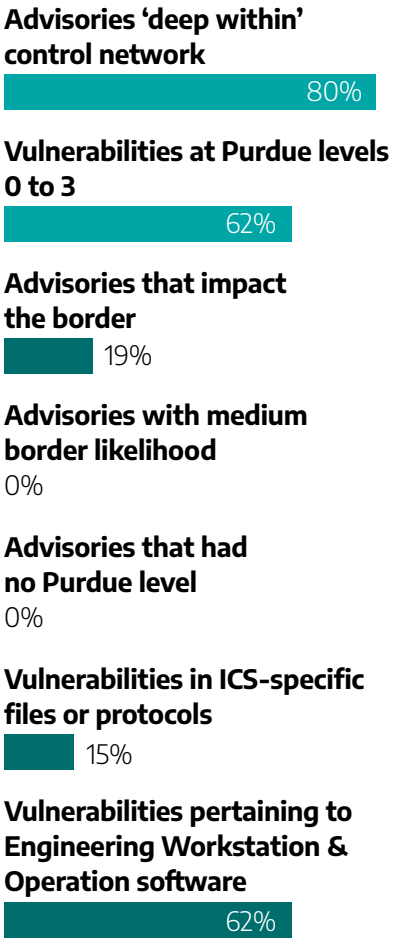


Figure 11: Where do vulnerabilities reside?

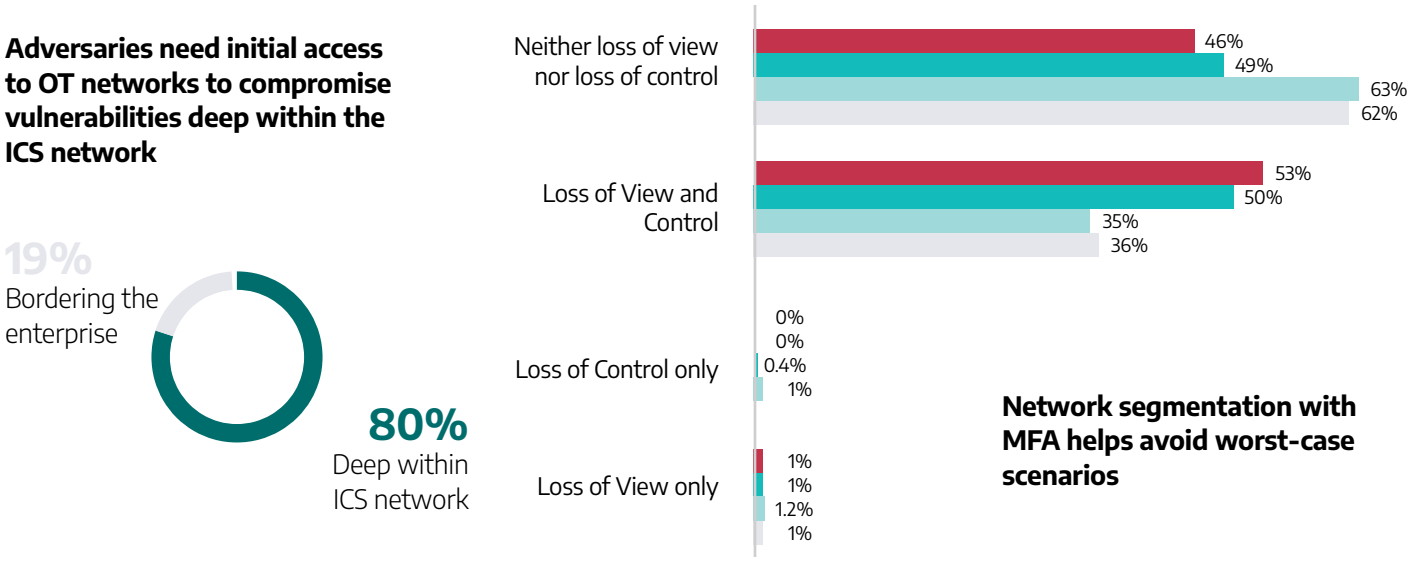


Figure 12: Where the Vulnerabilities Reside

VULNERABILITY EXPLOITABILITY

Dragos continually looks for evidence of exploitation in the wild. Asset owners with vulnerable assets actively being exploited in the wild by adversaries or proven through a penetration test have an increased urgency to mitigate. Because of this, exploitation is factored into the **Now, Next, Never** prioritization.

In 2023, 5 percent of advisories included vulnerabilities being actively exploited. Recall that only 3 percent of all advisories are given **Now** priority for remediation – active campaigns make up the bulk of the highest priority remediations.

Public proof of concepts (PoCs) are examples of exploitation code available for public use. Example code may be specific to a product's implementation and configuration, but it is meant to prove the presence of a vulnerability. PoCs can be weaponized as a stand-alone exploit or incorporated into an exploitation framework. The existence of a PoC lowers the barrier of entry for adversaries to exploit vulnerabilities. Twenty-three percent of advisories Dragos assessed in 2023 had public PoCs available at the time of disclosure.

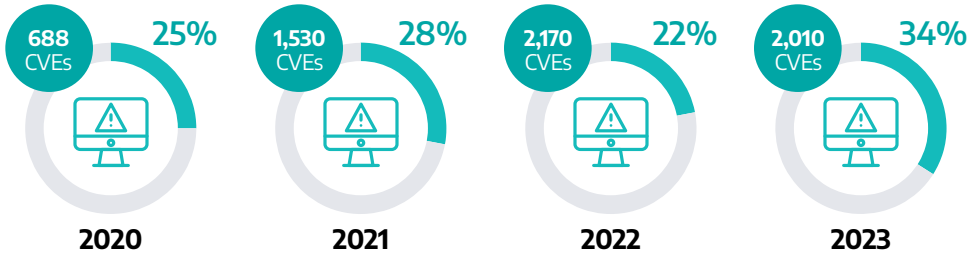
VULNERABILITY TRENDS

Dragos observed several vulnerability trends in 2023.

THE RISE OF AUTHENTICATION-REQUIRED VULNERABILITIES

2023 saw a significant increase in the number of vulnerabilities that require authentication to exploit. Dragos first noticed a trend of high-profile vulnerabilities, which garnered a large amount of press. These vulnerabilities all had the curious aspect of requiring existing, often administrative access, to the victim's device in order for an adversary to achieve any effect.

Based on the 2023 data and prior years, a definite surge in vulnerabilities is reported, requiring some authentication. This represents a significant increase both in number and percentages.



While the exact cause of such a surge is difficult to pinpoint, there are several factors:

- More devices and protocols under research are incorporating authentication. This is a positive sign.
- There is an uptick in authentication-required rootkit exploitation, for example, against Cisco and other remote availability services.
- Low-hanging fruit vulnerabilities and everyday vulnerabilities in legacy protocols have already been uncovered and assigned CVEs (sometimes multiple times), forcing researchers to look elsewhere.

Dragos Frontline Perspective

Dragos expects this trend to continue. CISA advisories advocating for secure-by-design development processes[4] should put pressure on vendors to provide authentication by default. It is important that end users cite such reports during the requirements building and procurement phases of new installations.

[4]Secure By Design – CISA.gov

It is worth noting that while a privilege requirement in a vulnerability is a good thing for defenders, it is not an excuse to label a device secure just because it has a password set. Adversaries can often find ways to obtain credentials, either via brute force attacks, social engineering, or simply knowing default credentials for a product. For some systems, authentication may be disabled entirely by the end user, and such a decision will not be reflected in the CVSS score.

TREND ANALYSIS BY VULNERABILITY TYPE

Common Weakness Enumeration (CWE) identifiers play a crucial role in classifying vulnerabilities, allowing the community to relay vulnerabilities in a shared language. They are assigned to CVEs to describe the underlying cause of the vulnerability. In 2023, Dragos assessed each vulnerability impacting ICS and found several noteworthy CWEs based on their use in the wild.

OUT-OF-BOUND READ/WRITE - CWE-787/CWE-125

Out-of-bounds read and write vulnerabilities consistently rank among the most exploited and disclosed CWEs year after year. This trend can be attributed to the complexity of developing intricate systems with tens of thousands of data structures and hundreds of third-party dependencies.

Such vulnerabilities exploit the way data structures are implemented and accessed. Developers commonly use data structures to organize and store information systematically. The most basic example of this is an array, a numbered list where you can store and manage multiple pieces of information, making it easy to access each piece by its specific position. Issues arise when code can read or write beyond the predefined bounds of these structures.

Consider a scenario where a vendor employs a proprietary industrial control system (ICS) protocol, enabling engineering workstation (EWS) software to assign a name to a PLC. Internally, the PLC may store this data in an array within its memory, with reserved regions explicitly designated for this purpose. Should the protocol code fail to impose character restrictions within the array's size, adversaries can exploit this vulnerability to write information beyond the array's intended memory space. An adversary, for instance, could send a request with a name surpassing the array's supported size, potentially resulting in loss of view and control. Ensuring secure bounds checking for all data accesses, adopting secure programming practices, and comprehensive code security reviews are crucial for preventing buffer overflows. The prevalent use of third-party libraries in modern software introduces an additional potential vulnerability avenue that may go unnoticed by developers. Therefore, it is essential for vendors to track all software dependencies. This can be accomplished through manual tracking or utilizing a software bill of materials

STATISTICS

CWE-787 and CWE-125 consistently rank at the top with the most CVEs, the most public proof of concepts, and the most actively exploited vulnerabilities reported year over year. In 2023 alone, advisories reported twelve CVEs related to CWE-787 that have been exploited. This figure surpasses the CWE-787 and CWE-125 CVEs reported over the preceding three years of ten.

Advisories containing CVEs with CWE-787/CWE-125 (combined)

2022	2023	% of advisories
54	**67**	**12.6%**

Number of CVEs with CWE-787/CWE-125

Year	CWE-787	CWE-125	Combined
2022	180	94	274
2023	187	134	321
16% OF ALL CVEs			

Number of CVEs with CWE-787/CWE-125 and a public proof of concept (+ exploits)

Year	CWE-787	CWE-125	Combined
2022	40 of 180	27 of 94	67 of 274
2023	60 of 187	51 of 134	111 of 321

Notable impacted products in 2023

- CODESYS Runtime
- PHOENIX CONTACT PLCnext Firmware
- Hitachi Energy's SDM600
- Rockwell Automation 1756-EN2T

(SBOM) service, ensuring a proactive approach to identifying and managing potential security risks associated with third-party components.

EXPLOITATION

Out-of-bounds read and write commands are commonly exploited by threat groups. A notable case is the TRISIS malware, utilizing an out-of-bounds write to compromise a Triconex Safety Instrumented System. Also, this year, it was discovered that a threat group had developed capabilities around CVE-2023-3595. This particular CVE affected the Rockwell Automation 1756 Ethernet modules and was categorized as an out-of-bounds write vulnerability.

OS COMMAND INJECTION - CWE-78

Improper Neutralization of Special Elements used in a Command, also known as Command Injection, is a security vulnerability that occurs when an application does not properly handle user-supplied data within a command it executes. In its simplest form, this vulnerability allows an adversary to manipulate the input in such a way that the application unwittingly executes unintended commands on the system. Adversaries do this by using special characters to break out of the original command and execute additional commands.

Issues like these are common in networking devices, particularly those equipped with network troubleshooting tools like ping. Typically, these tools take a user-provided IP address and insert it into a ping command in the underlying operating system. If the device fails to properly check or validate this input, a user with malicious intent could input something like 8.8.8.8;cat /etc/passwd. Without proper validation, the ping tool might execute the command ping 8.8.8.8;cat /etc/passwd on the operating system, inadvertently exposing sensitive information like the password file to the user.

To prevent Command Injection vulnerabilities, vendors must employ secure coding practices, including robust input validation and sanitization, using parameterized queries, and avoiding the direct construction of system commands from user input.

EXPLOITATION

Palo Alto Networks reported that CVE-2022-29303 was used to spread a variety of the Mirai botnet. This particular CVE impacted the CONTEC SolarView Compact power monitoring system. This device has a web server that included an emailing service which did not properly validate the email address provided by the user. Threat groups were able to craft a malicious command injection request that downloaded a variant of Mirai[5] on to the device.

STATISTICS

In 2023, OS Command Injection emerged as the second most actively exploited CWE, maintaining its consistent presence among the top three most exploited vulnerabilities over the past four years. This persistent prevalence can be attributed to a significant factor: one-third of its CVEs over the last four years have had public proof of concept. The availability of these public proofs of concept lowers the bar for exploitation, making OS Command Injection an attractive target for adversaries. The accessibility of such readily available methods reduces the effort required for exploitation. For this reason and others, Dragos prohibits the public disclosure of any POCs developed by Dragos and encourages other security vendors to do the same.

Number of advisories containing CVEs with CWE-78

2023	2022	2021	2020
17	9	10	4

Number of CVEs with CWE-78

2023	2022
47	23

Number of CVEs with CWE-78 and a public proof of concept (+ exploits)

2023	2022
13 of 47	3 of 23

Notable impacted products in 2023

- Siemens RUGGEDCOM ROX
- Delta Electronics DVW-W02W2-E2
- PHOENIX CONTACT WP
- Multiple WAGO controllers and HMI

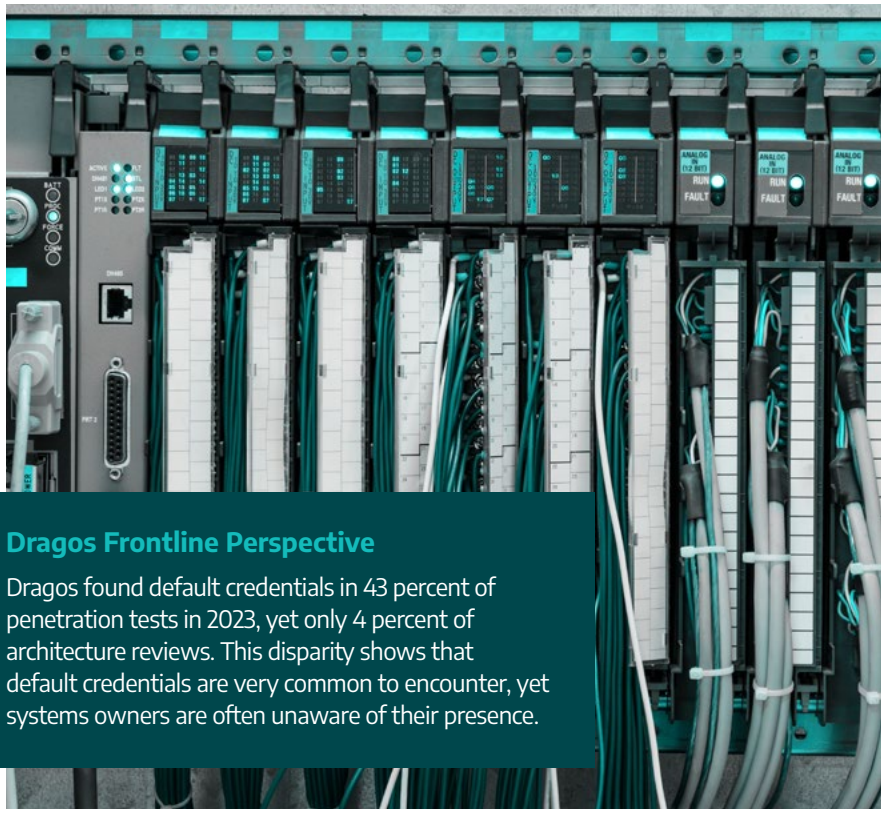
[5]Mirai - https://unit42.paloaltonetworks.com/mirai-variant-targets-iot-exploits

USE OF HARD-CODED CREDENTIALS – CWE-798

Vendors frequently embed credentials directly into the source code or include static access accounts within the shipped file systems of their products. These accounts typically remain unchangeable, leaving product owners with no means to modify them. Attackers discover or crack these passwords and use them to gain privileged access. In ICS/OT, this is a common issue since many vendors ship products with maintenance interfaces that are not mentioned to asset owners.

EXPLOITATION

BADOMEN, a PIPEDREAM[6] malware module designed to target Omron PLCs, exploited CVE-2022-34151. This CVE is associated with hardcoded credentials and encryption keys statically programmed into the Sysmac Studio EWS software for communicating with Omron NX/NJ PLCs. Likely by reverse engineering Sysmac Studio, the threat group CHERNOVITE uncovered these credentials and utilized them to develop BADOMEN. Later, the same credentials were publicly disclosed when a project called ICS Forensics Tools[7] was uploaded to Git Hub and presented at Black Hat Europe by Microsoft's Cyberx research team. Thankfully, shortly after the project was uploaded, the module containing CVE-2022-34151 was removed.



Dragos Frontline Perspective

Dragos found default credentials in 43 percent of penetration tests in 2023, yet only 4 percent of architecture reviews. This disparity shows that default credentials are very common to encounter, yet systems owners are often unaware of their presence.

STATISTICS

Since 2019, the incidence of Hard-Coded Credentials CVEs has demonstrated an average annual increase of 133 percent. However, a significant shift occurred in 2023, marking the first year new Hard-Coded Credentials CVEs have declined. This year, Dragos identified 23 CVEs related to hard-coded credentials, the lowest count since 2020 and a substantial decrease from the previous year's 40 CVEs. This reduction is possibly attributable to heightened security awareness surrounding these vulnerabilities. In addition, many popular systems with hard-coded credentials have already been uncovered and disclosed. While relatively easy to prevent, the impact of hard-coded credentials vulnerabilities is substantial, often leading to highly privileged access.

Number of advisories containing CVEs with Hard-Coded Credentials

2023	2022
17	23

CVEs with Hard-Coded Credentials

2023	2022
23	40

Number of CVEs with Hard-Coded Credentials and a public proof of concept that had exploits

2023	2022
3 of 23	1 of 40

Notable impacted products in 2023

- Moxa NPort IAW5000A-I/O Series
- Siemens SICAM A8000
- Schweitzer Engineering Laboratories SEL-5037 SEL Grid Configurator
- PHOENIX CONTACT WP 6xxx

[6]PIPDREAM – https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/
[7]ICS Forensics Tools – https://github.com/microsoft/ics-forensics-tools

PATH TRAVERSAL – CWE-22

Path traversal vulnerabilities were among the most prevalent types of vulnerabilities analyzed by Dragos in 2023. Typically, these vulnerabilities affect web servers and other applications that interact with the local file system of a device, host, or server. They also frequently impact engineering software, where project files contain file paths as a part of the archive.

Exploiting such vulnerabilities often results in adversaries gaining unauthorized access to restricted or unintended areas within the file system. These issues typically arise when user input is not properly validated or sanitized when constructing file paths or accessing files on the file system.

For example, consider a web server that serves images at the universal resource locator (URL): https://x.y.z/images/johndoe.jpeg. An adversary could craft a malicious URL using escape characters to access sensitive files. It's important to note that URL paths are not the only vectors for these types of attacks. Any process that relies on user input to access files could potentially be vulnerable to path traversal attacks. In addition to this, various techniques, including zipslips[9] and universal naming convention (UNC) path injection, can also be used to exploit path traversal vulnerabilities.

EXPLOITATION

CVE-2018-13379 is a path traversal vulnerability that impacts FortiOS, the operating system used by Fortinet's FortiGate Firewall. Dragos has observed adversaries conducting exploitation against CVE-2018-13379 against industrial or ICS entities using Fortinet devices, including PARISITE and VANADINITE.

CVE-2022-33971 is a blank CVE covering a number of individual issues in Omron PLCs, including a path traversal flaw in the embedded web application. The BADOMEN tool allows for file listings, retrieval, and overwrite on the PLC firmware using the file APIs.

STATISTICS

Path traversal remains consistently among the most common vulnerabilities year after year, averaging 54 CVEs annually over the past three years, placing it among the top 5 most prevalent vulnerabilities. What's particularly concerning is that this CWE-22 has become the second most actively exploited in 2023, following the use of this technique in PIPEDREAM in 2022 and against FortiOS by PARISITE in 2019 and VANADINITE in 2020, and has consistently ranked in the top 5 most exploited CWEs since 2020. Despite this, path traversal vulnerabilities are relatively straightforward to prevent. By implementing proper user input validation, these issues can be entirely avoided. In the coming years, efforts to address and mitigate this vulnerability type will hopefully lead to a positive trend in the opposite direction.

Number of advisories containing CVEs with Path Traversal

2023	2022
23	**26**
4% OF ALL ADVISORIES	

Number of CVEs with Path Traversal

2023	2022
55	**53**
3% OF ALL CVEs	

Number of CVEs with Path Traversal and a public proof of concept that had exploits

2023	2022
10 of 55	**10 of 53**

Notable impacted products in 2023

- Omron Sysmac Studio and NX-IO Configurator (EWS Software)
- Schweitzer Engineering Laboratories SEL-5033 and SEL-5036 (EWS Software)
- Fortinet FortiOS (networking devices)
- Siemens SICAM A8000 Devices (Remote Terminal Unit)

[9]Zip Slip - https://security.snyk.io/research/zip-slip-vulnerability

NEIGHBORHOOD KEEPER VULNERABILITY DATA

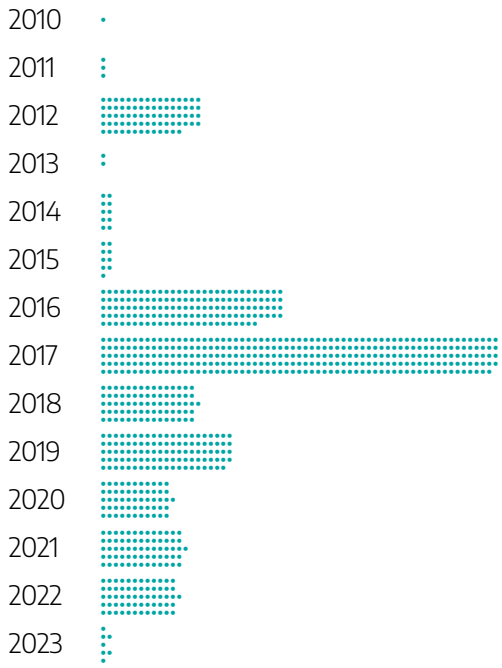
In 2023, Dragos added vulnerability tagging to its Neighborhood Keeper program. This presents both Neighborhood Keeper users and Dragos analysts with data regarding vulnerabilities on Neighborhood Keeper participants' networks.

This data provides an interesting glimpse at what products are most often left unpatched on industrial networks.

Perhaps unsurprisingly: PLCs, industrial computers marketed for use as HMIs, industrial network switches, and remote IO devices, make up the bulk of vulnerable components.

What is surprising about the vulnerable components is how long equipment is often left unpatched. It is not possible to gather complete numbers for vulnerable components due to the anonymous nature of Neighborhood Keeper participation at present, however the data can be broken down by CVE year. When counted simply for number of occurrences of a particular CVE on a network, by year, the following data is shown at right.

# of CVEs present on Neighborhood Keeper participant networks by CVE year



Again, it can be misleading to read too much into Neighborhood Keeper data. Visibility biases are present in the data, both in terms of where Neighborhood Keeper sensors are deployed an in terms of what vulnerabilities can be identified by Neighborhood Keeper sensors. For an example of the latter: vulnerabilities in engineering software with file format issues, are almost certainly not observable by Neighborhood Keeper…unless the software also broadcasts a very obvious network to identify itself, these vulnerabilities could only be discovered with a more thorough assessment that includes inspecting individual host filesystems.

The data does, however, show some interesting characteristics. Specifically: many control systems networks go unpatched for long periods of time. Fully half of the identified vulnerability years are CVEs dating 2016-2017, meaning that vulnerabilities patched 6-7 years prior were extremely prevalent on networks in 2023.

A key takeaway from this analysis is that advisories absolutely must come with alternate mitigation advice: many end users may fail to apply patches for years after they become available. Indeed, many end users may NEVER apply patches, even when those patches are deemed of critical importance. Thankfully, these end users take other steps to defend the vulnerable components.

Looking at Neighborhood Keeper data from different angles: of the vulnerabilities which occurred most frequently in the Neighborhood Keeper dataset, none were labeled of immediate importance. Of the 493 CVEs that Dragos tracks as **Now**, meaning that immediate action should be taken by owners to remediate the vulnerability, only 86 are observed on Neighborhood Keeper participant networks. Some of these 86 vulnerabilities are widespread across Neighborhood Keeper participants.

The prevalence of a vulnerability within the community is part of the analysis that Dragos uses to prioritize exploitation detection development. That is, some vulnerabilities are likely to go years or decades without patching. When these vulnerabilities are deemed critical – because known threat groups target the component, or because public PoC exploits are readily available – and the observation is made that most users do not apply patches for the vulnerability, then a detection for exploitation becomes much more important.

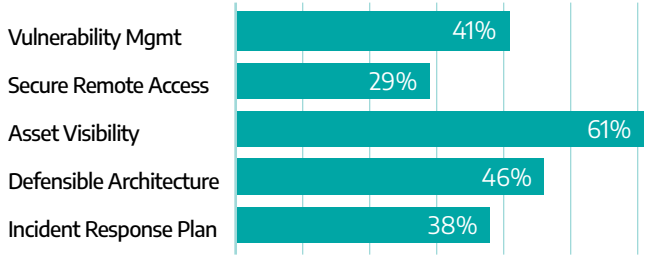
ASSESSING CYBER READINESS

In 2023, we saw major regulatory shifts for critical infrastructure asset owners, resulting in organizations 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. One of the most significant changes was not targeted at critical infrastructure but at firms publicly traded in the U.S.: the new Securities and Exchange Commission (SEC) Cybersecurity Risk Management Rules. These rules apply to many OT asset owners, including investor-owned utilities and manufacturing firms.

Dragos observed organizations growing their cybersecurity capabilities, defining or refining processes, and exercising plans. Organizations 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 organizations supported by detection capabilities, training, and external experts.

Developing resiliency is a focal aspect of the 5 Critical Controls for OT Cybersecurity.[10] Of all Dragos services engagements in 2023, 94 percent had a finding relating to one of these controls. Improving ICS network visibility tops the list appearing in more than half of our reports. Limited logging and monitoring, weak segmentation, and lack of asset inventories were some of the other top recurring findings Dragos issued that were relevant to the five critical controls.

2023 Service Engagements with 5CC Findings



Dragos has observed this shift through findings identified while working on tabletop exercises with customers. In 2023, the quantity, type, and scope of the exercises that Dragos facilitated changed. The number of 2023 tabletop exercises doubled from 2022, and executive and board-level tabletop exercises tripled. This highlights organizations' increased focus, rooted in executive management, on being prepared for a cybersecurity event.

Dragos Frontline Perspective

Dragos executed its largest exercise in 2023 in partnership with a longtime customer. The exercise included over 350 participants across multiple levels parts of the business. The exercise allowed responders, operators, adjacent business units, partners, and leadership to practice responding to a large-scale cybersecurity event using incident response, business continuity, and crisis management plans. The exercise was modeled on threat group activity and capabilities observed in 2023.

[10] https://hub.dragos.com/guide/5-critical-controls

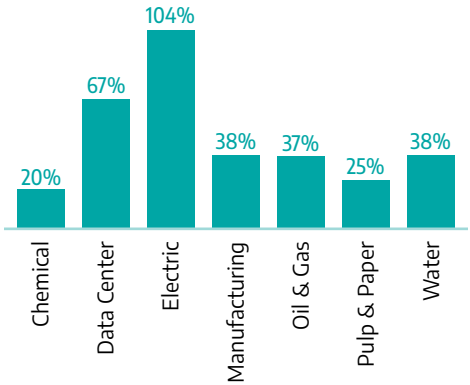
This shift was not perceived equally across industry verticals, but nearly all verticals increased focus on tabletop exercises. The most significant increase was seen in the electric sector, where the tabletop exercises' share of reports in that sector increased 104 percent year over year. Throughout the industrial space, teams are shifting focus toward tabletop exercises.

Even when regulations don't require organizations to perform exercises, many willingly conduct them to increase awareness and preparedness. This is the case with one of the most significant changes in regulation this year: the SEC Cybersecurity Risk Management Rules. The SEC ruling requires registrants to disclose an event within four business days after a registrant determines that a cybersecurity incident is material. It also requires that organizations describe how they will assess, identify, and manage material risks from cybersecurity threats and how their boards will provide oversight.

Tabletop exercises' findings and associated recommendations are organized by core capabilities for ICS/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 organization favors the four-step 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.

The core capabilities tested with the lowest aggregate score was Communicate, although scores across all capabilities fell in 2023, with the Contain capability falling by 19 percent year over year. The Contain core capability requires organizations to understand the scope and impact of an event before taking appropriate action.

2023 Tabletop Exercise Share Growth per Industry (2022–23)



Dragos Frontline Perspective

SEC 8K regulatory requirements have become a major theme during most exercises involving public companies that operate in the United States. Executive leadership and boards have taken a more active role in managing and governing cybersecurity risks.

Core Capability	2022 Score	2023 Score	Change
Detect	73%	65%	-8
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

Metrics are as follows

- Performed without Challenges **80-100**
- Performed with Some Challenges **66–79**
- Performed with Major Challenges **50–65**
- Unable to Perform **0–49**

Figure 13: Average Tabletop Exercise Scores (All OT)

Dragos Frontline Perspective

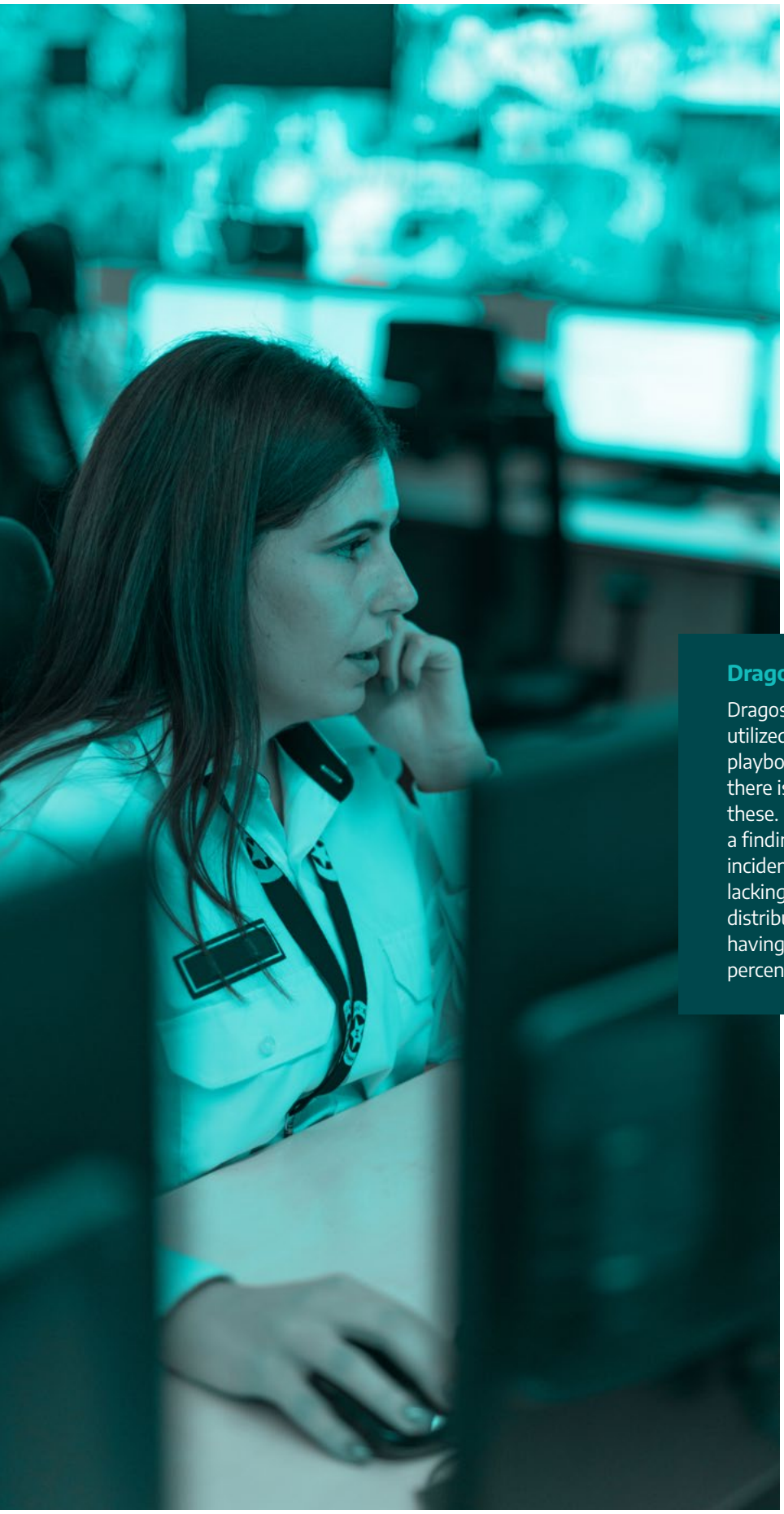
Dragos tabletop exercise facilitators observed that even mature organizations with well-developed detection capabilities and processes often overlook the expertise that system operators and engineers can provide. Integrating cybersecurity awareness into daily practices, especially troubleshooting, can result in valuable human detection capabilities.

Not every sector performs the same. During 2023, the electric sector scored the lowest, with an aggregated score of 59 percent across all core capabilities.

Core Capability	Electric	Oil & Gas	Manufacturing	Pharma
Detect	61%	68%	63%	69%
Activate/Elevate	63%	65%	69%	69%
Respond	60%	70%	60%	56%
Contain	61%	65%	60%	69%
Communicate	51%	68%	52%	56%
Document	58%	63%	69%	69%
Remediate/Recover	61%	70%	63%	50%

- Performed without Challenges **80-100**
- Performed with Some Challenges **66–79**
- Performed with Major Challenges **50–65**
- Unable to Perform **0-49**

Figure 14: Average Tabletop Exercise Scores by Industry



Ransomware remains the most common scenario in 2023, accounting for 50 percent of scenarios. The scores against ransomware were lower in every capability than the average scores that included all scenarios.

Core Capability	Score
Detect	**61%**
Activate/Elevate	**72%**
Respond	**67%**
Contain	**59%**
Communicate	**60%**
Document	**66%**
Remediate/Recover	**67%**

Dragos Frontline Perspective

Dragos found that organizations that have developed and utilized OT-specific incident response plans and ransomware playbooks during exercise perform better. Unfortunately, there is still a significant gap in organizations implementing these. Dragos found that 27 percent of engagements included a finding indicative of a weakness in the organization's incident response plan, and 12 percent that were completely lacking an OT incident response plan. This is not evenly distributed across verticals, with manufacturing and chemical having the most incident response plan findings as a percentage of sector engagements.

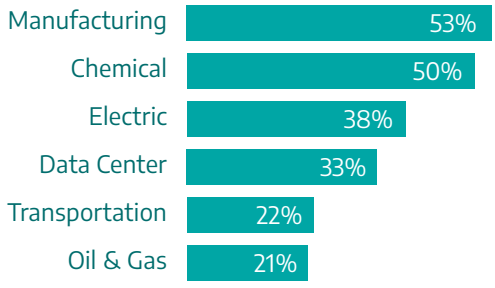


Figure 15: Incident response planning findings by industry

Dragos is an industrial (ICS/OT) 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.

Dragos.com