DRAGOS

ICS/OT CYBERSECURITY

YEAR IN REVIEW 2022 • FOCUS ON EUROPE

2022 Year in Review Focus on Europe

Looking back at 2022, several factors and trends effectively reshaped the cyber threat landscape for industrial control systems (ICS) and operational technology (OT) in Europe. The escalated conflict between Russia and Ukraine raised alarm bells and prompted ICS/OT asset owners in Europe and around the globe to shore up their defenses against the possibility of destructive or disruptive cyber attacks. Of particular concern are geographically dispersed industrial operations such as renewable electric generation, electric transmission, upstream and midstream oil and gas, and water and wastewater management. Set against this complex geopolitical context, the frequency and sophistication in the number of targeted cyber threats that focus on infiltrating and disrupting industrial control systems continues to grow in 2023.

Fortunately, many industrial organisations have grown more cognisant of the threats and vulnerabilities they face. Analysis from Dragos Professional Services engagements in 2022 showed hopeful improvements in the percentage of organisations that have tackled the way they handle security perimeters and external connections. However, statistics from these field observations also demonstrate that the industrial community still has a lot of work to do to improve OT network visibility, segmentation, and controlling connections and credentials over ICS/OT assets.

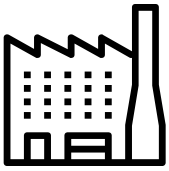
Key Statistical Findings

↑ 87%

Ransomware attacks against industrial organisations **increased 87 percent** over last year.

+35%

Dragos tracked **35% more ransomware groups** impacting ICS/OT in 2022.



72%

of all ransomware attacks targeted **437 manufacturing entities** in **104 unique manufacturing subsectors**.

20

Dragos tracked **20 ICS/OT Threat Groups** in 2022, with **two new groups** entering the scene

2,170

Dragos investigated **2170 vulnerabilities** in 2022, compared to just 703 in 2020

46%

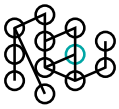
The **number of CVEs investigated** has grown at an average annual rate of 46% over the last four years

34%

One-third of vulnerability advisories **contained errors** in 2022.

53%

Dragos provided mitigations for 53% of the advisories that had none.



83%

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

13%

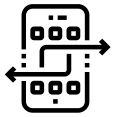
of advisories were **extremely critical** in 2022

51%

of the advisories that Dragos analysed **could cause both a loss of view and loss of control,** up from 35% last year.

80%

of Dragos services customers had **limited to no visibility** into their ICS environment

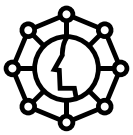


50%

of Dragos services engagements **involved issues with network segmentation**

53%

External connections to OT dropped significantly from 70% to 53%.



54%

of Dragos services engagements included findings related to **shared credentials**

DRAGOS
SAFEGUARDING CIVILIZATION

European ICS/OT Cybersecurity Trends 2022-2023

Geopolitical Conflict Changes the Calculus

The Russian invasion of Ukraine in 2022 illustrated the impact of geopolitical conflict and physical warfare on cybersecurity, particularly in industrial infrastructure sectors. Industrial sectors in Ukraine were hard hit with a high number of operations targeting electric and oil and gas sectors in concert with kinetic military action, as well as hacktivist activity that have held steady.

On February 25, 2022, the day after Russia invaded Ukraine, the ransomware group Conti declared that if a cyber attack or warfare were directed against Russia, Conti would use "all possible resources to strike back at the critical infrastructure of an enemy."[1] On February 27, an adversary uploaded a video to Twitter demonstrating how to alter a Russian Fornovogas Human Machine Interface (HMI) used with a gas compressor. The video features an unknown operator clicking through menus on the HMI, altering the off-delay time, exiting the HMI software, deleting the profile configuration, and browsing to the host operating system root user configuration directory. The action and capabilities, though not impactful, were consistent with trending popularisation of ICS/OT hacktivism immediately following Russian invasion in Ukraine.

More concerning were the actions of well-funded threat groups with the motivation and capabilities to execute cyber attacks on ICS/OT operations, presumably with the intent to influence geopolitical events and gain an advantage on the ground. If successful, these types of attacks can have untold impact on the lives of ordinary citizens and are difficult to recover from. On April 12, the Computer and ESET released advisories describing multiple malware capabilities discovered at a Ukrainian energy provider. The malware, referred to as INDUSTROYER2, a later variant of CRASHOVERRIDE, was deployed with a set of malware wipers and other capabilities. The attack was fortunately prevented but confirmed that adversaries that have historically targeted Ukraine entities would maintain operations and be a factor in the conflict. Dragos associates INDUSTROYER2 with ELECTRUM, a known threat group that has consistently targeted the energy sector and has successfully executed ICS/OT attacks in Ukraine. Another known threat group that continues to be a threat is KAMACITE – Dragos has observed consistent activity throughout 2022-2023, including targeting the same oblenergo previously hit by a cyber attack in 2015, and it is generally expected that these activities and campaigns will continue.

As Western countries placed sanctions on Russia and indicted key members of Russian cyber operations, governments across Europe and the United States prepared for potential retaliation with measures that included actions to safeguard ICS operations and OT networks. Dragos observed fewer cyber-focused attacks on ICS/OT on energy sectors not directly associated with the conflict than predicted at the beginning of the war between Russia and Ukraine, with most analysed threats suggesting that adversaries focused on reconnaissance. Nonetheless, the obvious conclusion is that physical wars must factor for ICS/OT and demonstrate the interest of nation-state actors to use cyber operations to amplify psychological effects and target critical infrastructure, including energy utilities, oil and gas pipelines , water utilities, and transportation systems. Defenders should be aware of these capabilities and priorities to protect critical infrastructure and services.

New ICS Malware Strains

On April 13, 2022, Dragos and third-party partners disclosed the discovery of the PIPEDREAM malware, the seventh known ICS-specific malware known to date and the most sophisticated example so far. Analysed by Dragos and third parties before it was employed, it has the potential for disruptive and

1 Russian ransomware gang threatens countries that punish Moscow for Ukraine invasion - Politico

and destructive cyber attacks.[2] In present form, adversaries could leverage PIPEDREAM to target specific equipment used in the electric industry. However, PIPEDREAM targets three ubiquitous software components CODESYS, Modbus, and OPC UA. CODESYS is used by over 500 suppliers, Modbus by over 600, and OPC UA by over 4200 suppliers. These suppliers produce equipment used by electric, oil and gas, manufacturing, food and beverage, and other industries.

PIPEDREAM is the most sophisticated ICS-specific malware known to date. While CRASHOVERRIDE was only going to work in on transmission sites in the electric industry, and TRISIS worked only in petrochemical with a specific safety system, PIPEDREAM can be used across industries. With PIPEDREAM, adversaries are capable of scalable and repeatable ICS/OT cyber operations.

While PIPEDREAM is itself new, its emergence is also indicative of the trend toward more technically capable and adaptable adversaries targeting ICS/OT. In addition to implementing common ICS-specific protocols in PIPEDREAM, CHERNOVITE improved the techniques from prior ICS malware. CRASHOVERRIDE, and the associated threat group, ELECTRUM, exploited the OPC Data Access (OPC DA) protocol to manipulate breakers and electrical switchgear. CHERNOVITE, on the other hand, uses the newer but comparable OPC UA protocol.

Around the same time, security researchers investigated the deployment of INDUSTROYER2, the sixth known ICS-specific malware. The April 2022 incident marked the first time the ICS-specific malware had been reconfigured and then redeployed in an electric utility environment, which was also impacted by CRASHOVERRIDE in 2016.

INDUSTROYER2 utilises the International Electrotechnical Commission (IEC) IEC-104 protocol to control and communicate with industrial equipment. INDUSTROYER2 is a new variant of CRASHOVERRIDE with fewer capabilities. The 2016 CRASHOVERRIDE malware had a modular framework and multiple

2 PIPEDREAM: CHERNOVITE's Emerging Malware Targeting Industrial Control Systems - Dragos

components, including a 104 module that utilised the IEC 104 protocol for communicating with industrial equipment. This module is designed to leverage the IEC 104 protocol to change the state of Information Object Addresses (IOA) to switch physical breaker statuses from open to closed or vice versa, causing disruptive effects. The targeted substations and IOA information contained within the configuration information indicate that ELECTRUM had a detailed understanding of the victim's environment before deploying INDUSTROYER2.

Ransomware Groups Targeting Manufacturing

Germany, Austria, Switzerland, and Italy make up a significant portion of manufacturing in Europe; together, Germany and Italy account for 47 percent of sold production in Europe, according to Eurostat.[3] In 2022, Dragos observed 194 ransomware incidents targeting industrial infrastructure in Europe, accounting for 32 percent of incidents globally, most of which were in the manufacturing sector. These are

3 Industrial Production Statistics - Eurostat

primarily motivated by profit, while other motivations are extremely difficult to prove. Ransomware attacks on European industrial infrastructure, particularly in manufacturing, is expected to continue to expand as adversaries develop more scalable operations and malware strains.

Risks to North Sea Oil & Natural Gas Assets

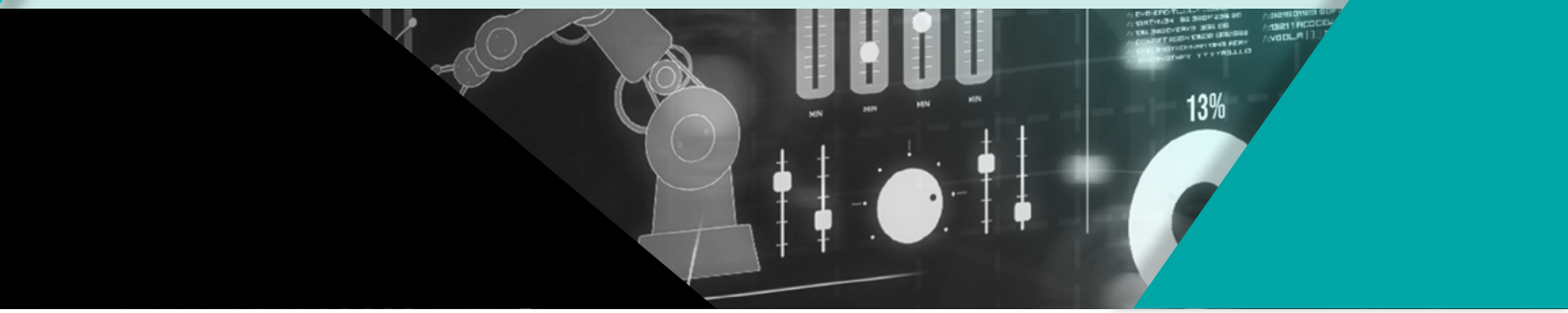
Increased targeting of the European oil and gas sector is likely, specifically by known threats groups such as XENOTIME and DYMALLOY. Gasification and processing terminals in key areas including the Isle of Grain and Rotterdam demonstrate key dependencies that could have a significant impact on European liquid natural gas operations if successfully disrupted by adversary groups. If these facilities are deemed too impenetrable for adversaries to dedicate time and resources to target, third-party suppliers of critical equipment, including the hydrogen used in the regasification process, may become attractive targets for adversaries due to lower barriers of entry caused by less mature security controls. As European oil and gas operations expand and markets become more competitive, the economic interests of states that rely on the oil and gas market - for instance, state-owned oil companies - will likely generate more intrusions by groups like XENOTIME and DYMALLOY. All third-party connections should be thoroughly analysed to ensure a cyber attack on a third-party can be cordoned off from key dependencies.

United Kingdom Electric Sector Threats

The unique layout of the United Kingdom (UK) energy sector naturally leads to a distinctive threat landscape due to the limited number of controlling parties. The UK electric sector is at risk of disruption by adversaries capable of carrying out coordinated attacks against multiple power stations. A cyber attack against energy transmission assets would be the most disruptive because these organisations must leverage a strong defense in depth at every level of the Purdue model to remain well guarded against adversaries. However, smaller distribution companies are less likely to have dedicated security staff and budgets. The Dragos 2022 Year in Review report indicates that 50 percent of ICS/OT assets haveporous IT/OT boundaries, with the likelihood that these distribution companies have OT devices connected directly to the internet or IT devices connecting into OT systems. This reality poses a significant potential for disruption if just one or two power stations or distribution centers experience an outage. For example, on August 9, 2019, a simultaneous fire and lightning strike at small power stations on opposite sides of the United Kingdom led to one million customers losing access to electricity. While this event was not cyber-related in nature, it highlights the potential for adversaries with knowledge of OT environments to cause significant disruption through a small and coordinated cyber attack. Additionally, this event had a significant downstream impact on other key industrial infrastructure, including transportation and water.

Dragos assesses with moderate confidence, that threat groups that have previously targeted electricity operations in Europe, including XENOTIME and VANADINITE, are likely to continue to demonstrate an interest in the United Kingdom energy infrastructure; however, a direct cyber attack is unlikely, barring significantly heightened political tensions. Dragos assesses with low confidence adversaries, whether state-affiliated or cyber-criminals, may target small energy distributors and power stations to cause disruption or demand ransom payments.

ICS/OT Threat Landscape



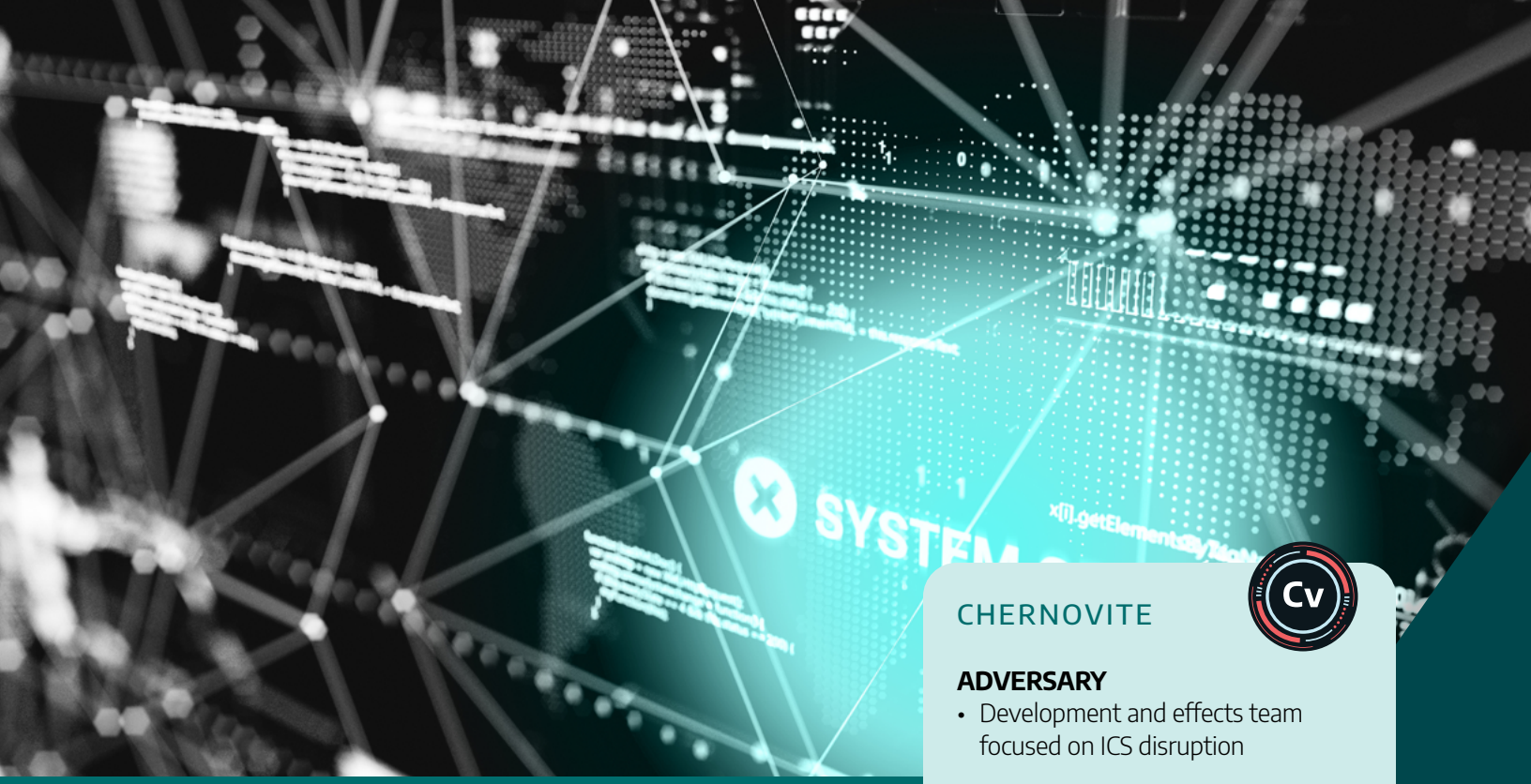
The ICS/OT threat landscape consists of a range of attackers, many of them opportunistic in seeking OT targets. These include increasingly prolific ransomware groups that will attack any industry and frequently find many OT networks low-hanging fruit, ripe for picking. More disconcerting are the highly sophisticated, well-organised threat groups that are focused on industrial infrastructure. These are the ICS/OT Threat Groups that Dragos has tracked for its annual Year in Review reports for the last six years running.

2022 Threat Group Update

During 2022, Dragos tracked 20 threat groups focused on ICS targets, including two newly defined ICS/OT Threat Groups — CHERNOVITE and BENTONITE. From a statistical perspective, the year-over-year activity across these threat groups remains relatively steady overall. The groups under observation stayed the same, and the total number of active groups increased by two.

While 12 groups were dormant during 2022, the most capable and potentially most dangerous threat groups Dragos tracks remain active. These are groups that check off many of the boxes for tactics, techniques, and procedures (TTPs) outlined in MITRE's ICS Cyber Kill Chain. Additionally, Dragos analysts find that the newer groups are growing increasingly more sophisticated.

DRAGOS
SAFEGUARDING CIVILIZATION



2022 New Threat Groups

CHERNOVITE

CHERNOVITE is the developer of PIPEDREAM, a modular ICS attack framework that illustrates the growing maturity of technically capable and adaptable adversaries targeting ICS/OT. CHERNOVITE possesses a greater breadth of ICS-specific knowledge than previously discovered threat groups. The ICS/OT expertise demonstrated in the PIPEDREAM malware includes capabilities to disrupt, degrade, and potentially destroy physical processes in industrial environments. PIPEDREAM is the first cross-industry and repeatable disruptive ICS attack framework known to date.

To date, PIPEDREAM has not been used in any known operations. However, Dragos assesses with high confidence that a state actor developed PIPEDREAM intending to leverage it in future operations for disruptive or destructive purposes.

CHERNOVITE

ADVERSARY
- Development and effects team focused on ICS disruption

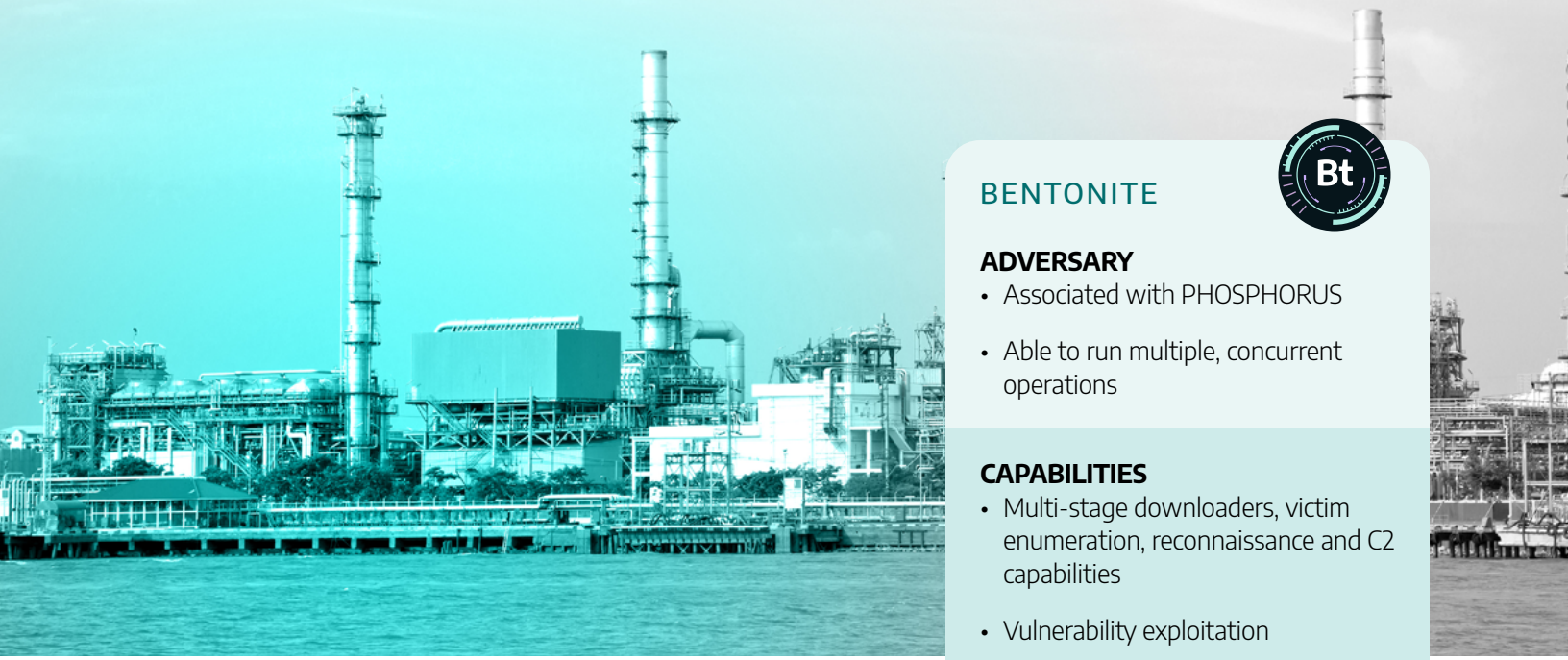
CAPABILITIES
- Unique tool development
- Uses ICS-specific protocols for reconnaissance, manipulation, and disabling of PLCs
- PLC Credential Capture. Password brute forcing and denial of service

VICTIMS
- Could impact all industries, initially targeting electric, ONG, and manufacturing
- Companies with Schneider Electric, Omron, and CODESYS PLCs, as well as any OPC UA

INFRASTRUCTURE
- Unknown

ICS IMPACT
- Loss of View, Availability, Safety, and Control
- ICS Kill Chain Stage 2 – Install/ Modify, Execute ICS

DRAGOS
SAFEGUARDING CIVILIZATION



BENTONITE

BENTONITE is a new ICS Threat Group increasingly and opportunistically targeting maritime oil and natural gas (ONG), governments, and the manufacturing sectors since 2021. While BENTONITE does not exhibit the breakthrough capabilities of CHERNOVITE, the group was found last year to be actively attacking industrial organisations. BENTONITE's operations have impacted North American ONG maritime support organisations and state, local, tribal, and territorial (SLTT) governments. BENTONITE compromised these organisations by exploiting vulnerabilities on internet-facing assets through Log4j and VMWare Horizons vulnerabilities.

Once BENTONITE gains access to a victim's environment, BENTONITE is very tenacious in its persistence to retain its access by performing lateral movement to other hosts, collecting credentials, and establishing long-term persistence to re-enable access to the adversary operator through scheduled tasks in combination with malware implants.

BENTONITE has overlapping activity clusters with Microsoft's activity group PHOSPHORUS (DEV-0270) and CrowdStrike's activity group NEMESIS KITTEN.

BENTONITE

ADVERSARY
- Associated with PHOSPHORUS
- Able to run multiple, concurrent operations

CAPABILITIES
- Multi-stage downloaders, victim enumeration, reconnaissance and C2 capabilities
- Vulnerability exploitation
- Heavy use of Powershell to facilitate compromise
- Disruptive capabilities

VICTIM
- Highly opportunistic
- U.S. oil and gas, manufacturing
- State, local, tribal and territorial organisations

INFRASTRUCTURE
- Credential harvesting
- Separate domains for phishing and C2
- Utilises Github for delivery, SSH and HTTP for C2

ICS IMPACT
- Espionage, data exfiltrations, and IT compromise
- Disruptive effects possible

Other Active Threat Group Updates

KOSTOVITE • Active Since 2021

2022 Activity Highlights:

December: KOSTOVITE-linked adversary, APT5, reported by U.S. government to have exploited zero-day vulnerability in perimeter-facing Citrix Application Delivery Controllers (ADCs) and Citrix Gateways, targeting National Security Systems, Department of Defense, and Defense Industrial Base information systems.

The attack was not against an ICS/OT target, but parallels KOSTOVITE's 2021 tactics and zero-day exploitation against targets that include an energy firm.

KAMACITE • Active Since 2014

2022 Activity Highlights

February: Intelligence released in the UK jointly with U.S. agencies detailed a new malware capability called CYCLOPS BLINK targeting small office/home office (SOHO) routers and network attached storage (NAS). Dragos assesses with high confidence this activity is associated with KAMACITE.

May: Dragos analysed CYCLOPS BLINK command and control (C2) infrastructure and identified communication with host domains for organisations in the rail, aerospace, food and beverage, and automotive sectors, indicating scanning activity.

June: Dragos identified KAMACITE network infrastructure communicating with a regional power distribution entity in Ukraine, one of the same entities impacted in a 2015 cyber attack.

XENOTIME • Active Since 2014

2022 Activity Highlights

Throughout 2022: Dragos observed XENOTIME reconnaissance and research activity focused on oil and natural gas (ONG) and liquefied natural gas (LNG) entities in the U.S., including component manufacturers that support ONG operations.

XENOTIME is the only threat group that has demonstrated the ability to compromise and disrupt industrial safety instrumented systems (SIS), which can lead to environmental damage, loss of containment, loss of control, and loss of life.

ELECTRUM • Active Since 2016

2022 Activity Highlights

April: Dragos assesses with a high degree of confidence that ELECTRUM was behind the deployment of INDUSTROYER2, the sixth known sample of ICS-specific malware, which was uncovered by ESET researchers at a Ukrainian utility provider.

ERYTHRITE • Active Since 2020

2022 Activity Highlights

ERYTHRITE continued to compromise industrial organisations across multiple sectors in the U.S. and Canada with its adaptable search engine optimisation (SEO) poisoning and custom, rapidly redeveloped malware.

Dragos has observed ERYTHRITE compromise the OT environment of a Fortune 500 manufacturer, the IT environments of two large electrical utilities, large food and beverage companies, auto manufacturers, IT service providers, and multiple oil and natural gas (ONG) service firms.

WASSONITE • Active Since 2018

2022 Activity Highlights

October: Dragos analysed WASSONITE's use of nuclear energy-themed spear phishing lures written in Hangul to deliver a multi-component backdoor that can take screenshots, log keystrokes, and collect removable media information and specific victim files. It can also upload, download, and execute follow-on commands from a command and control (C2) server.

Focus on 2022 OT Ransomware

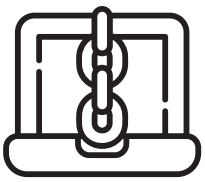
Ransomware attacks disrupted the operations of multiple industrial organisations, suppliers, and subsidiaries in 2022. There has been a surge of ransomware-related initial access campaigns, demonstrating that specific ransomware groups were more active in 2022 than in 2021. For example, remote desktop protocol (RDP) enables adversaries' initial access and is used in typical Lockbit ransomware-as-a-service (RaaS) attacks.

This year witnessed the demise of Conti and the introduction of a new version of Lockbit, Lockbit 3.0. Several other ransomware groups introduced this year, such as Black Basta, targeted industrial organisations.

The RaaS trend, which Dragos called out in the 2021 Year in Review report as a growing attack vector, became even more prevalent in 2022 with an even greater impact on ICS and OT.

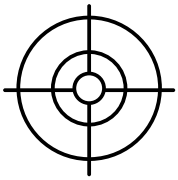
With over 70 percent of all ransomware attacks focused on manufacturing, ransomware actors continue to broadly target many manufacturing industries. As ransomware activity increases, it results in more risk for OT networks, particularly networks with poor segmentation.

2022 INDUSTRIAL RANSOMWARE ACTIVITY BY THE NUMBERS



57

Dragos monitors **57 different ransomware groups** that target industrial organisations and infrastructure



39

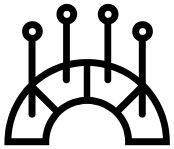
39 ransomware groups actively targeted industrial organisations

30%

30% increase in ransomware groups targeting industrial sectors

605

In 2022, Dragos tracked **605 ransomware attacks** against industrial organisations



87%

Attack volume increased 87% over 2021

DRAGOS
SAFEGUARDING CIVILIZATION

FIGURE 2: RANSOMWARE INCIDENTS BY SECTOR • 2022

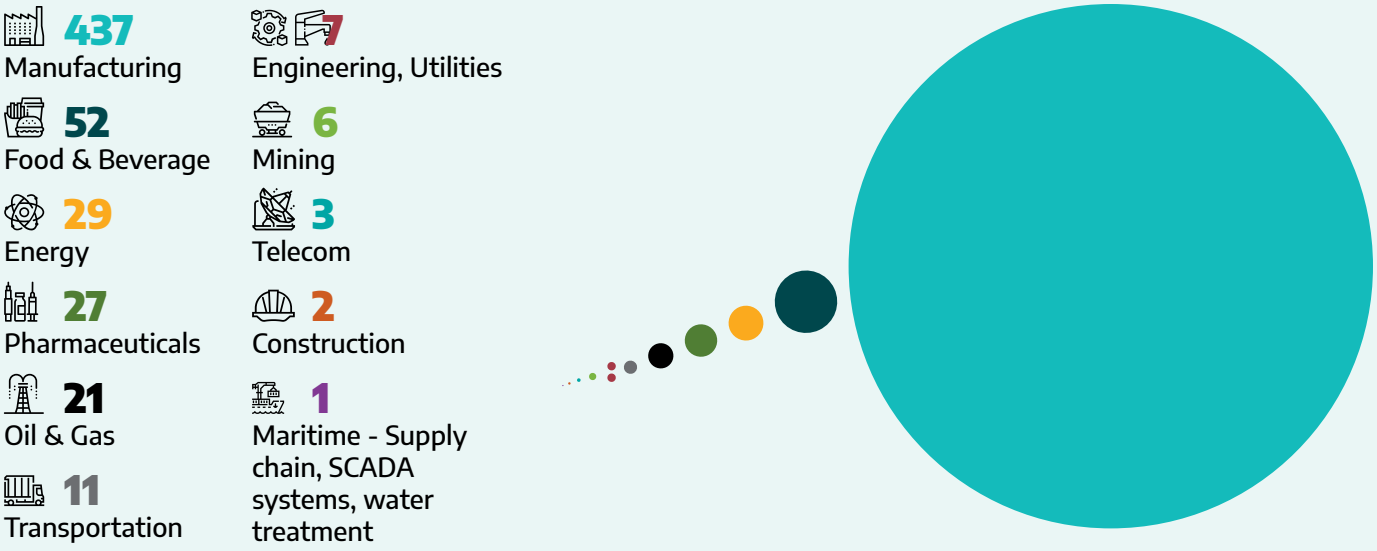
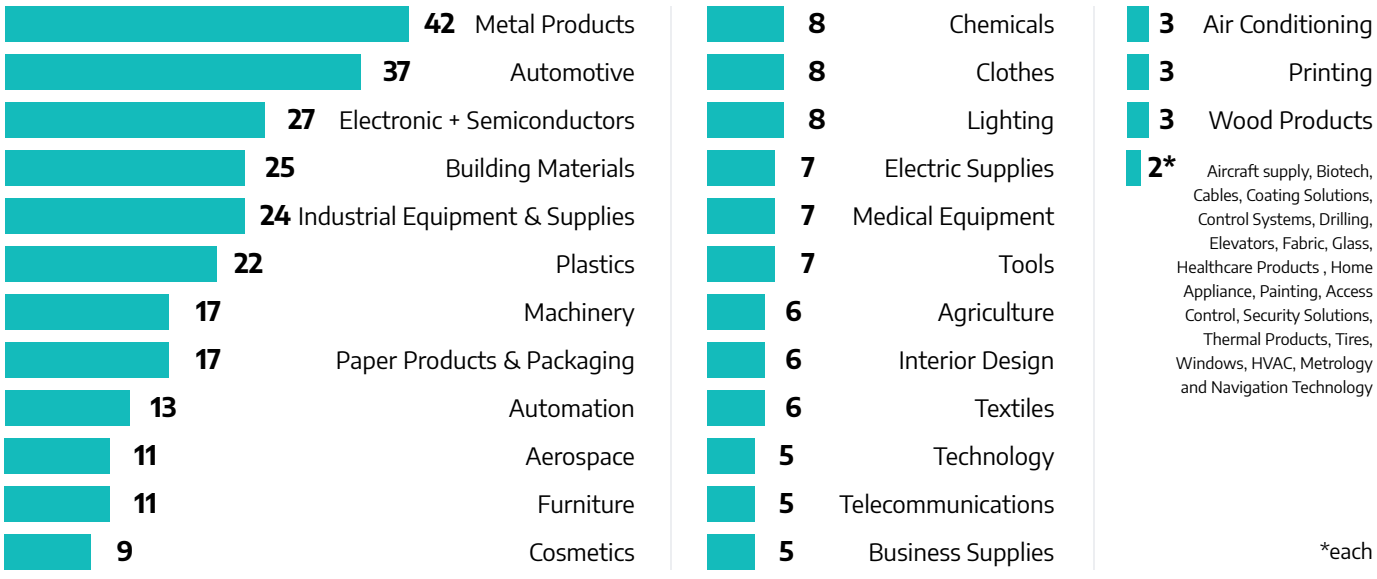


Figure 4 shows that 72 percent of all 2022 ransomware attacks Dragos tracked targeted 437 manufacturing entities in 104 unique manufacturing subsectors. Figure 4 also shows that nine percent of attacks targeted food and beverage; five percent targeted the energy sector; four percent targeted the pharmaceuticals; three percent targeted the oil and natural gas sector. Ten percent of victims were in metal products manufacturing, nine percent were in automotive, six percent were in electronic and semiconductor, 5.7 percent were in building materials, 5.5 percent were in industrial equipment and supplies manufacturing, and 5 percent were in plastics. See Figure 5.

FIGURE 3: RANSOMWARE BY MANUFACTURING SUBSECTOR

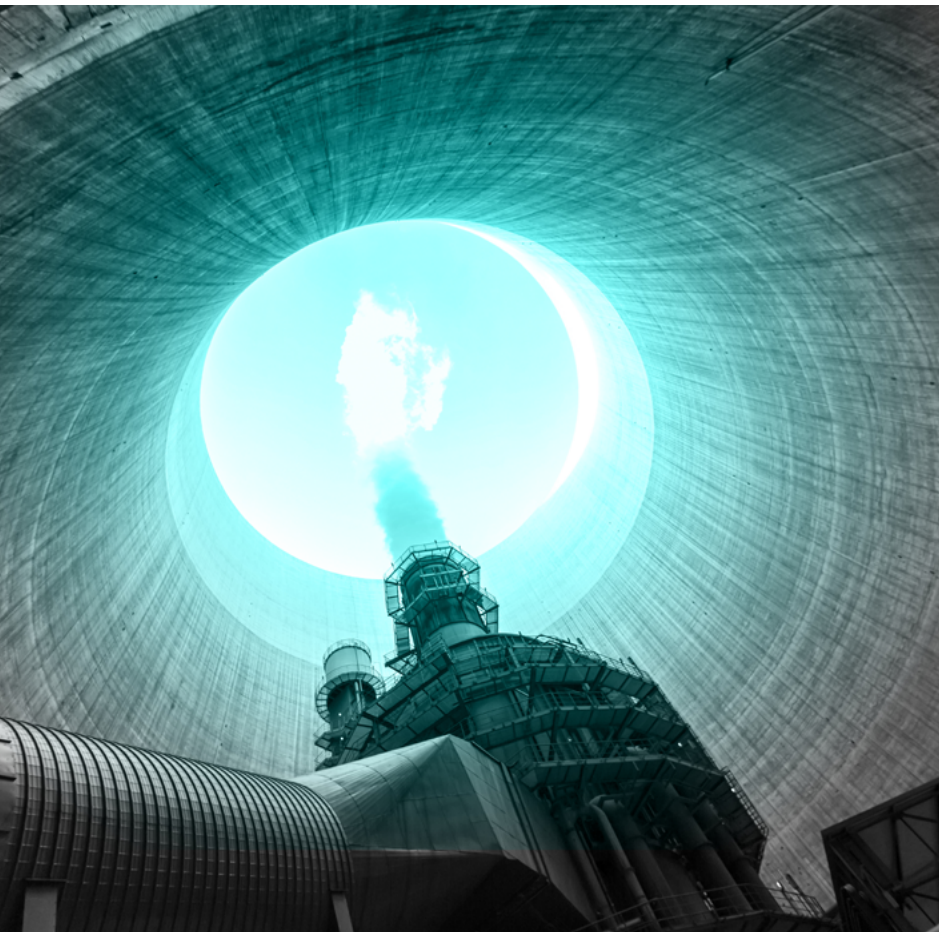


DRAGOS
SAFEGUARDING CIVILIZATION

OT Vulnerability Trends

In 2022, the rapid growth in vulnerabilities continued to challenge cybersecurity professionals. Dragos collects and reviews ICS/OT vulnerabilities dating back over a decade and has found that as companies and researchers gain better visibility into industrial components and networks, more vulnerabilities with specific OT impacts are identified.

One explanation for the continued rapid growth in advisories and CVEs is the ever-expanding number of researchers constantly looking for new vulnerabilities. Another reason is the growing awareness of the risks to our civilisation associated with ICS/OT vulnerabilities. The ongoing convergence of information technology (IT) and operational technology (OT) has led to an ever-expanding host of vulnerabilities that will continue to threaten industrial operations.



2022 OVERALL ICS/ OT VULNERABILITY STATISTICS AT A GLANCE

465

advisories analysed

2,170

CVEs analysed (+27% over 2021)

46%

average annual growth rate over last four years in ICS/OT CVEs

50%

of ICS/OT vulnerabilities **could result in both Loss of View and Loss of Control**

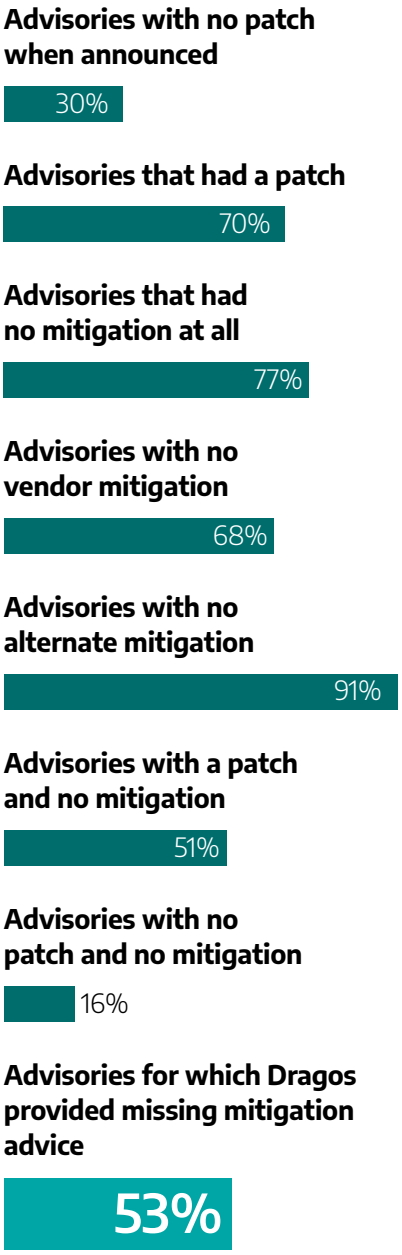
Why ICS/OT Vulnerability Prioritisation Remains Tricky

Vulnerability reporting in the industrial space is improving; however, there are still significant gaps in mitigations and reporting. These include incorrectly rating the severity of vulnerabilities and limited investment and resources focused on identifying vulnerabilities with ICS-specific protocols and services. Consequently, many industrial organisations struggle to find actionable guidance on how to prioritise remediation and mitigation efforts based on risk.

With respect to ICS/OT vulnerabilities, it is important to focus and prioritise threats accurately and have precise, actionable mitigations that reduce the amount of downtime while still protecting people and processes.

Published vendor and public CERT advisories often do not provide enough details to mitigate the inherent risks and bridge the gaps until it is time to apply a patch.

FIGURE 7:
ADVISORIES WITH ERRORS AND LACKING IN ACTIONABLE GUIDANCE



In prioritising vulnerabilities, Dragos uses a **Now**, **Next**, **Never** framework developed by CERT/Coordination Center (CERT/CC) to help asset owners and operators identify vulnerabilities and prioritise patching. The framework is not a one-size-fits-all solution for patch management. However, when combined with consequence-driven threat modeling, it can help OT security practitioners determine when and if to fix flaws in industrial control equipment.

Vulnerabilities that fall into the **Now** category require immediate action. In 2022, two percent of vulnerabilities fell into the **Now** category, down two percent from last year. These vulnerabilities are generally network exploitable, have a public proof of concept, and affect the loss of view or loss of control of OT processes. There are exceptions, however, where adversaries have targeted these vulnerabilities for initial access with the intent to disrupt operations. Asset owners and operators should address these vulnerabilities as soon as practicable.

Frontline Insights from OT Cybersecurity Consulting Engagements

Year after year, the Dragos Professional Services team offers insightful observation of the on-the-ground realities faced by industrial defenders for our Year in Review. 2022 engagements showed that while progress is being made on many fronts, most organisations still struggle with the four major areas of ICS/OT environmental hardening: network visibility, building and maintaining security perimeters, managing external connections to OT environments, and limiting the use of shared credentials.

DRAGOS
SAFEGUARDING CIVILIZATION

2022 Frontline Findings

Finding	Details	% Change over 2021	Historical Trend	Observations/Analysis
Limited to No IT Network Visibility	80% of services customers had limited to no visibility into their OT environments	-6	2019 **81%** 2020 **90%** 2021 **86%** 2022 **80%**	The good news is that visibility of OT networks is definitively getting better every year. This number is dropping. Additionally, this combined statistic doesn't reflect that the services team observes that the number of organisations with no visibility at all is significantly declining.
Poor Security Perimeters	50% of Dragos services engagements involved issues with network segmentation	-27	2019 **71%** 2020 **88%** 2021 **77%** 2022 **50%**	Dragos analysts speculate the significant improvements here are a result of increased awareness that proper segmentation is an essential aspect of a defensible architecture, one of the five critical controls for ICS/OT cybersecurity, stemming from both government regulation like the TSA Security Directives for oil and gas organisations, as well as increased attention paid to high-profile incidents in 2021 and 2022.
External Connections to OT Environments	53% of services engagements found evidence of undocumented or uncontrolled external connections to OT environments	-17	2019 **100%** 2020 **33%** 2021 **70%** 2022 **53%**	This year marks a trend reversal. In the wake of COVID-19, 2021 saw a huge spike in demand for remote access that wiped out a lot of progress being made in controlling external connections during that year. The improvement here shows that many organisations are regaining control. However, 53 percent is still a concerningly high number.

2022 Frontline Findings (continued)

Finding	Details	% Change over 2021	Historical Trend	Observations/Analysis
Lacked Separate IT & OT User Management	54% of Dragos services engagements included findings related to shared credentials	+10	2019 **54%** 2020 **54%** 2021 **44%** 2022 **54%**	While there was a 10-point increase in this category over 2021, this prevalence of this finding has remained stubbornly stable over the last four years. Shared credentials remain remarkably common and open industrial organisations to attacks that easily pivot to OT networks from IT networks using valid accounts.

Implementing 5 Critical Controls

The SANS Institute identified five critical controls for ICS/OT cybersecurity[4] . We offer additional insight on how to implement these controls in your OT environments.

1. ICS incident response plan

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

2. A defensible architecture

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

3. Visibility and monitoring

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

4. Secure remote access

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

5. Risk-based vulnerability management

Knowing your vulnerabilities – and having a plan to manage them – is a critical component to a defensible architecture. Over 2100 OT-specific vulnerabilities were released last year, the majority of them with incomplete or erroneous information. An effective OT vulnerability management program requires timely awareness of key vulnerabilities, the less than 2 percent that need immediate attention and apply to the environment, with correct information and risk ratings, as well as alternative mitigation strategies to minimize exposure while continuing to operate.

4 https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

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

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

Dragos.com