DRAGOS

ICS/OT CYBERSECURITY

YEAR IN REVIEW 2022 • EXECUTIVE SUMMARY

2022 Year in Review Executive Summary

The cybersecurity risks for industrial organizations continued to grow in 2022. Attacks increased on industrial infrastructure sectors, particularly accelerating in the electric and manufacturing verticals. The attack volume comes both from criminal threat actors that target industrial control systems (ICS) and operational technology (OT) infrastructure opportunistically, as well as organized threat groups that specifically focus on industrial environments. The tooling these threat groups use grows more sophisticated and in 2022 Dragos observed two new strains of ICS/OT-focused malware. Meanwhile, the number of vulnerabilities found in OT environments continues to grow, with many advisories containing errors and still offering limited advice for mitigation.

Fortunately, many industrial organizations have grown more cognizant of the threats and vulnerabilities they face. Analysis from Dragos professional services engagements in 2022 showed hopeful improvements in the percentage of organizations 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 assets.

1 https://www.politico.com/news/2022/02/25/russian-ransomware-gang-threatens-countries-ukraine-00011896

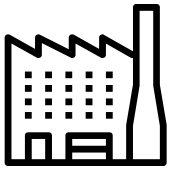
Key Statistical Findings

↑ 87%

Ransomware attacks against industrial organizations **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%

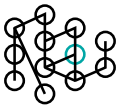
The **number of CVEs investigated** has grown at an average annual rate of 46% over the last four years

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%

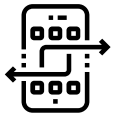
of advisories were **extremely critical** in 2022

51%

of the advisories that Dragos analyzed **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

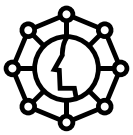


50%

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

Influential ICS/OT Security Trends of 2022

Ransomware

Ransomware attacks on industrial infrastructure organizations nearly doubled in 2022. 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.

Geopolitical Conflict

The Russian invasion of Ukraine in 2022 illustrated the impact of geopolitical conflict and physical warfare on the cybersecurity risks to industrial infrastructure sectors. Ukraine saw increased threat group activity targeting its energy and critical industrial infrastructure sectors. As Western countries placed sanctions on Russia and indicted key members of Russian cyber operations, the U.S. government prepared for potential retaliation with measures that included actions to safeguard ICS and OT environments. Dragos observed fewer cyber-focused attacks on OT in U.S. energy sectors than predicted at the beginning of the war between Russia and Ukraine, with most analyzed threats showing adversaries focused on reconnaissance.

New ICS Malware Strains

In 2022 industrial organizations faced two new malware strains focused directly at ICS environments, bringing the total observed ICS-specific malware up to seven.

FIGURE 1: SIGNIFICANT ICS RANSOMWARE EVENTS IN 2022

- JAN — **JAN 8** Ransomware Group Impacts Subex and Sectrio
- JAN — **JAN 27** Ransomware-as-a-Service Impacts Multiple Industries
- FEB — **FEB** Ransomware Attack on Kojima Industries
- FEB — **FEB** Third wiper malware targets Ukrainian entities
- MAY — **MAY 9** Ransomware Attack on AGCO
- MAY — **LATE MAY** Foxconn Ransomware Attack
- AUG — **AUG 15** South Staffordshire Water Ransomware Incident
- AUG — **AUG 24** Greek Natural Gas company, DESFA, Ransomware Incident
- SEP — **SEPT** Modular Mining Possibly Impacted by BianLian Ransomware
- OCT — **OCT** Ransomware Attacks Obtain CEII from Electrical Industry
- OCT — **OCT/NOV** Mining and Metals and Food & Beverage
- DEC — **DEC 27** Ransomware Attack on Copper Mountain Mining Company

INDUSTROYER2 is a new variant of CRASHOVERRIDE with fewer capabilities, but reconfigured and redeployed in a Ukrainian electric utility. INDUSTROYER2 utilizes the International Electrotechnical Commission (IEC) IEC-104 protocol to control and communicate with industrial equipment.

PIPEDREAM is a new modular ICS/OT malware that represents an advanced threat across all industrial sectors. PIPEDREAM represents a new evolution in malware development. It is the first known cross-industry scalable ICS/OT malware with disruptive capabilities. Given the right operational conditions, it could be used for destructive effects.

Some ICS/OT Products Are Insecure By Design

In 2022, a group of 56 vulnerabilities were disclosed across the products of 13 vendors. Dubbed OT:ICEFALL, these unrelated vulnerabilities impact a range of ICS/OT devices. They include weaknesses to exploits that could perform remote, unauthenticated control systems changes against vibration/shaft monitoring systems, distributed control systems controllers, PLCs, and networking equipment. Many of the issues are known to the vendors and are design flaws that are difficult, if not impossible, to patch. These vulnerabilities highlight the need to protect industrial control systems from outside access. They also highlight the need for vendors to assign CVEs for vulnerabilities and to disclose issues to customers, even when there is no plan to patch the issue.

Software Supply Chain Concerns Grow

Discoveries like INDUSTROYER2, PIPEDREAM, and OT:ICEFALL highlight broader concerns over software supply chain security risks that could impact industrial environments in the coming years. Just like IT equipment, OT equipment contains software libraries and other components that if targeted could pose accelerated risks to a wider range of assets. For example, PIPEDREAM targets underlying components and protocols that greatly increases the scalability of

ICS/OT attacks. Last year's fallout from the December 2021 discovery of the Apache Log4j vulnerability adds another proof point to these concerns. Dragos observed threat actors exploiting Log4j in OT networks, now declared an endemic vulnerability, during 2022.

TSA Security Directives

In 2022, the U.S. Transportation Security Administration (TSA) incorporated feedback from pipeline owners and operators, industry groups, and other federal partners, to develop the new version of the directive known as Pipeline-2021-02C for improvement of cybersecurity resilience of pipeline organizations. The shift from a prescriptive, compliance-based standard to a functional, performance-based standard was a major improvement from Pipeline-2021-02B. Through last year, Dragos observed noticeable improvements in the cyber readiness of oil and gas industry because of these changes. This sector led others in improvements to visibility, security perimeters, control over external connections, and shared password usage within ICS/OT environments.

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-organized 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. For example, the PIPEDREAM capability demonstrates that CHERNOVITE has the knowledge

and resources to develop capabilities for targeting, manipulating, and disrupting ICS devices.

Threat Group Trends Over Time

The number of known threat groups targeting ICS/OT has grown significantly since the inception of the Dragos Year in Review. Even as some groups retire or go dormant, new groups step in to fill those ranks. Over the course of the last six years, the number of known threat groups has increased by 300 percent.

Dragos tracks threat groups that attempt to gain access to ICS/OT networks and that could cause a potential threat to them in the future.

A number of the ICS/OT Threat Groups that Dragos tracks may evolve their disruptive and destructive capabilities in the future because ICS/OT adversaries often do extensive research and development (R&D) and build their programs and campaigns over time. Dragos maintains a list of dormant threat groups to analyze new activity, looking for any overlaps or similarities in the threat group tactics, techniques, and procedures (TTP) or target sets, with potential revival of dormant groups some months down the line.

Because of this, threat group reporting was slightly modified for the 2022 Year in Review to cover activity back to the beginning of 2020. The modification now defines active, dormant, and retired groups as follows:

- If a threat group has been active during the last 24 months, it is considered active.
- If there is no threat group activity during the last 24-48 months, it is considered dormant.
- If there is no activity in 48 months, the threat group is considered retired.

For context, these are the Dragos-designated active threat groups from the 2021 Year in Review:

- Three new ICS Threat Groups: **KOSTOVITE**, **ERYTHRITE**, and **PETROVITE**
- Three active ICS Threat Groups: **STIBNITE**, **WASSONITE**, and **KAMACITE**

20 ICS-Focused Threat Groups Tracked

Two new and active threat groups: **CHERNOVITE** and **BENTONITE**

Six existing and active threat groups: **ELECTRUM, ERYTHRITE, KAMACITE, KOSTOVITE, WASSONITE** and **XENOTIME**.

Twelve threat groups were dormant.
Zero threat groups were retired in 2022.

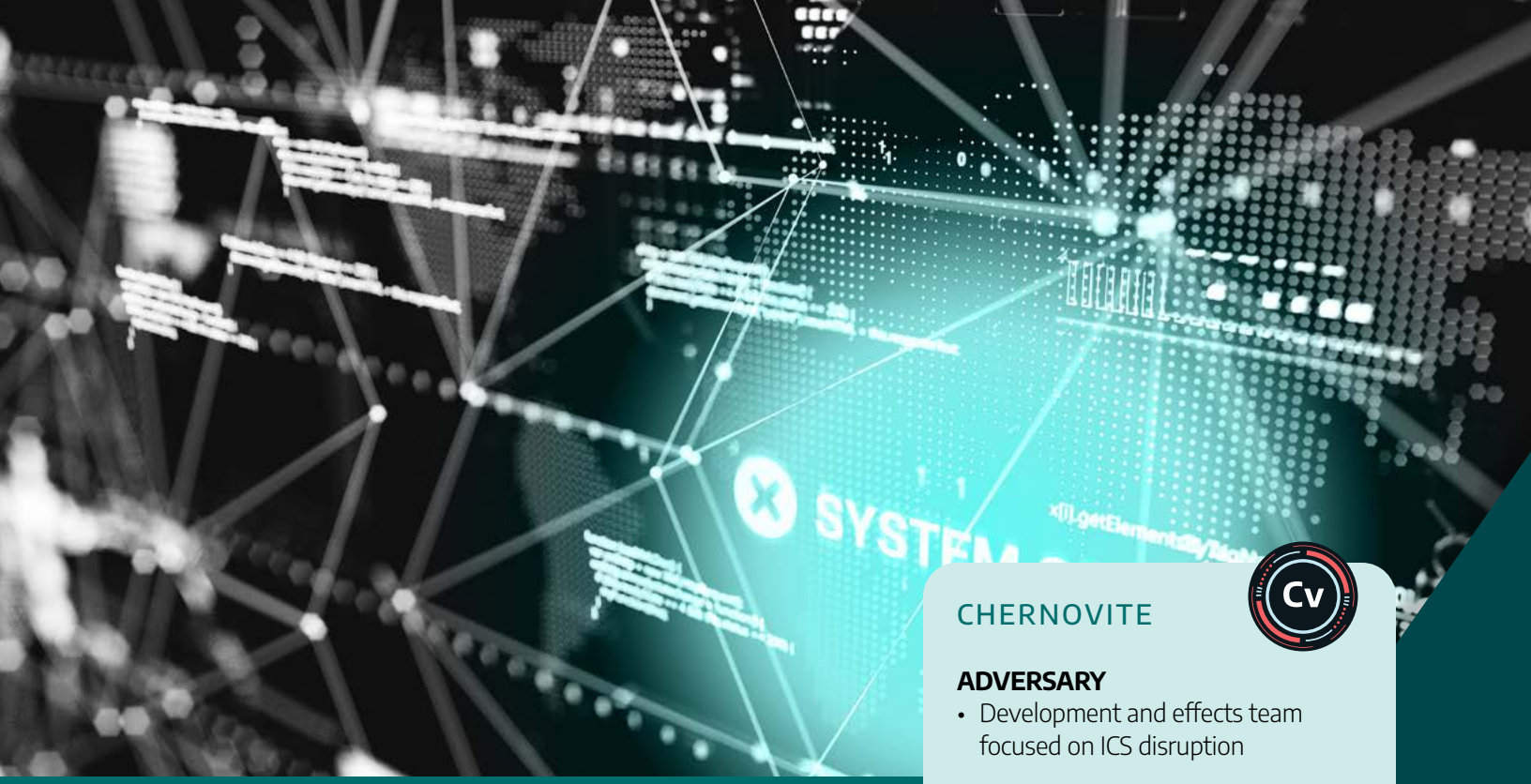
Two active threat groups exhibit only Stage 1 aspects of the ICS Cyber Kill Chain: **BENTONITE** and **WASSONITE** .

ERYTHRITE exhibits only Stage 2 aspects of the ICS Cyber Kill Chain

Four active threat groups exhibit all aspects of ICS Cyber Kill Chain Stage 1 and several of Stage 2 (Develop and Install/Modify): **ELECTRUM, KAMACITE, KOSTOVITE** and **XENOTIME** .

CHERNOVITE exhibits all aspects of ICS Cyber Kill Chain Stage 1 and Stage 2

Year	Observable ICS/OT Threat Groups
2017	5
2018	8
2019	11
2020	15
2021	18
2022	20



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

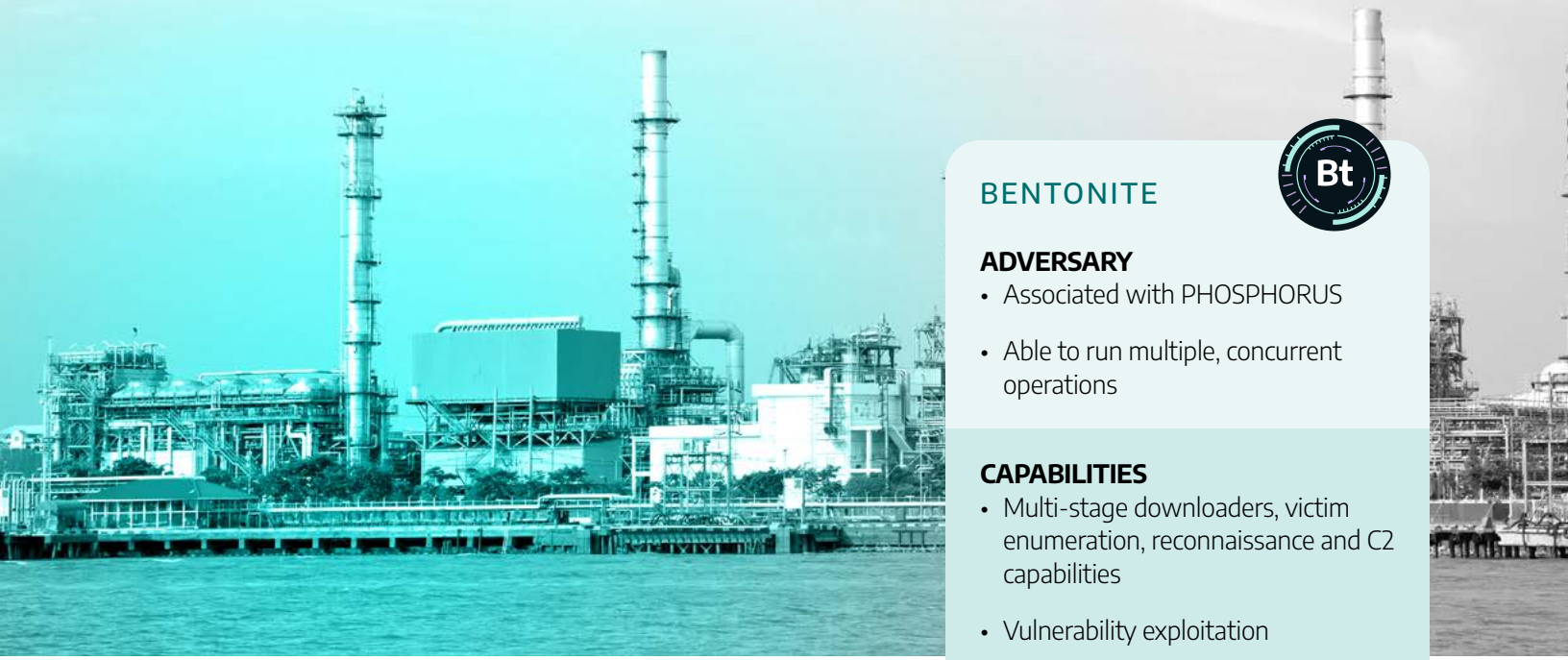
CAPABILITIES
- Unique tool development
- Uses ICS-specific protocols for reconnaissance, manipulation, and disabling of PLCs
- PLC Credential Capture. Password brute forcing and denial of service

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 organizations. BENTONITE's operations have impacted North American ONG maritime support organizations and state, local, tribal, and territorial (SLTT) governments. BENTONITE compromised these organizations 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 organizations

INFRASTRUCTURE
- Credential harvesting
- Separate domains for phishing and C2
- Utilizes 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 analyzed CYCLOPS BLINK command and control (C2) infrastructure and identified communication with host domains for organizations 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 organizations across multiple sectors in the U.S. and Canada with its adaptable search engine optimization (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 analyzed 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

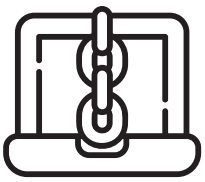
Ransomware attacks disrupted the operations of multiple industrial organizations, suppliers, and subsidiaries in 2022. There has been a surge of ransomware-related initial access campaigns, demonstrating that specific ransomware groups were more active in 2022 than in 2021. For example, remote desktop 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 organizations.

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.

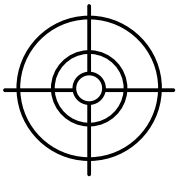
With over 70 percent of all ransomware attacks focused on manufacturing, ransomware actors continue to broadly target many manufacturing industries. As ransomware activity increases, it results in more risk for OT networks, particularly networks with poor segmentation.

2022 INDUSTRIAL RANSOMWARE ACTIVITY BY THE NUMBERS



57

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



39

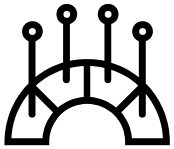
39 ransomware groups actively targeted industrial organizations

30%

30% increase in ransomware groups targeting industrial sectors

605

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



87%

Attack volume increased 87% over 2021

DRAGOS
SAFEGUARDING CIVILIZATION

FIGURE 2: RANSOMWARE INCIDENTS BY SECTOR • 2022

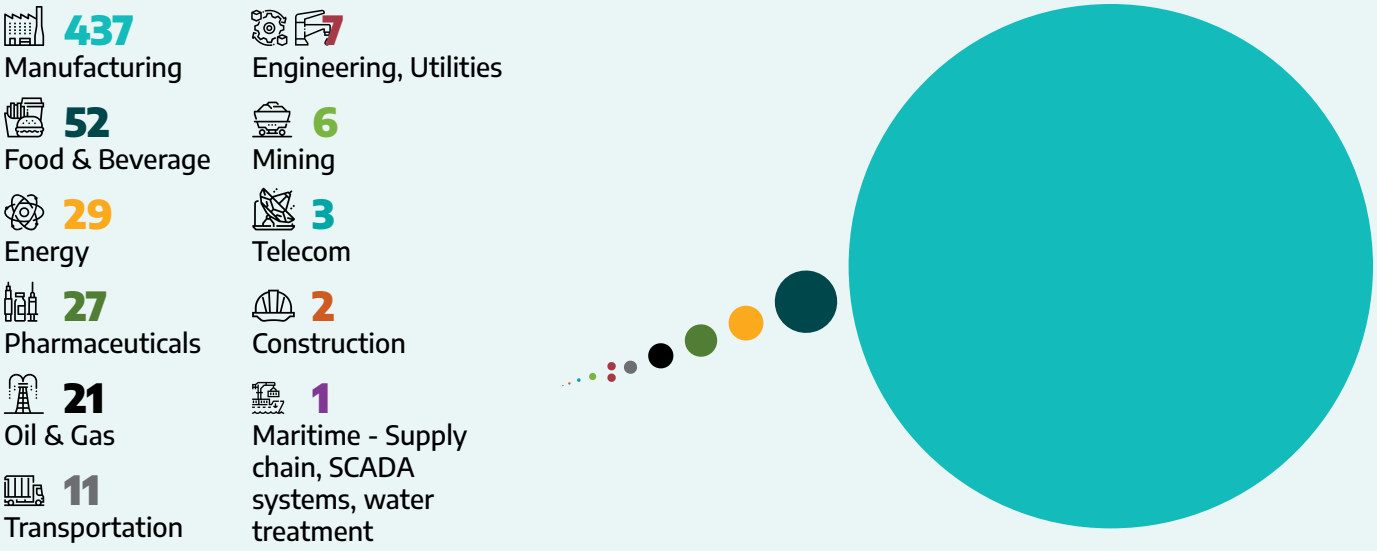
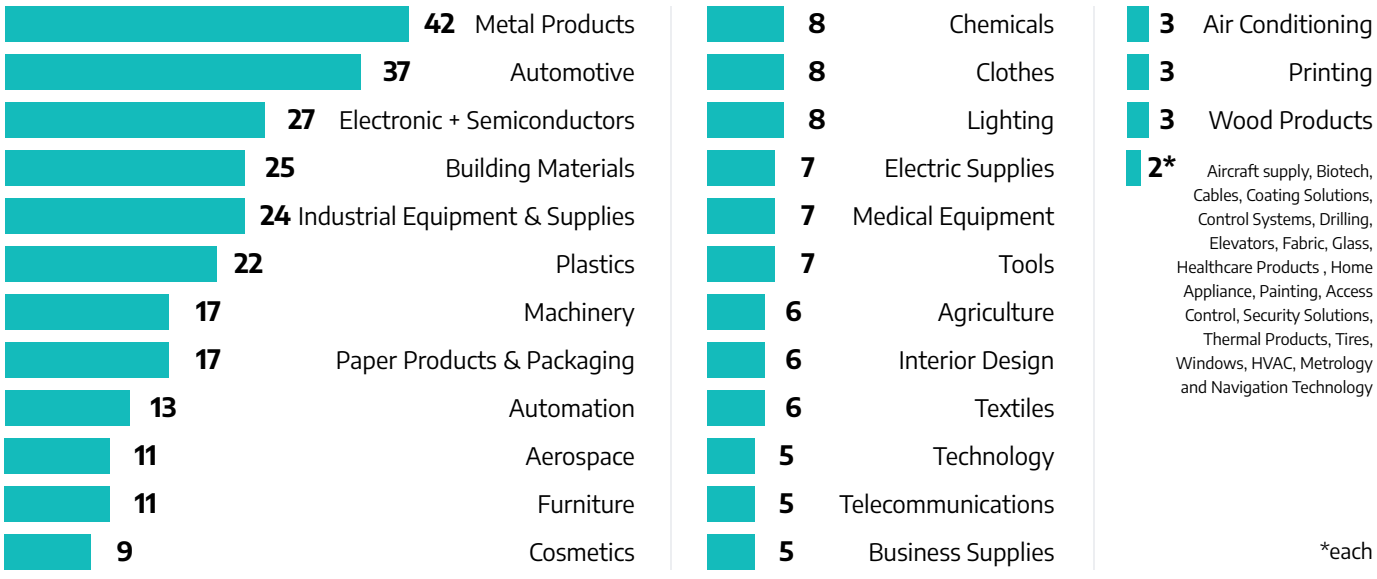


Figure 4 shows that 72 percent of all 2022 ransomware attacks Dragos tracked targeted 437 manufacturing entities in 104 unique manufacturing subsectors. Figure 4 also shows that nine percent of attacks targeted food and beverage; five percent targeted the energy sector; four percent targeted the pharmaceuticals; 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.

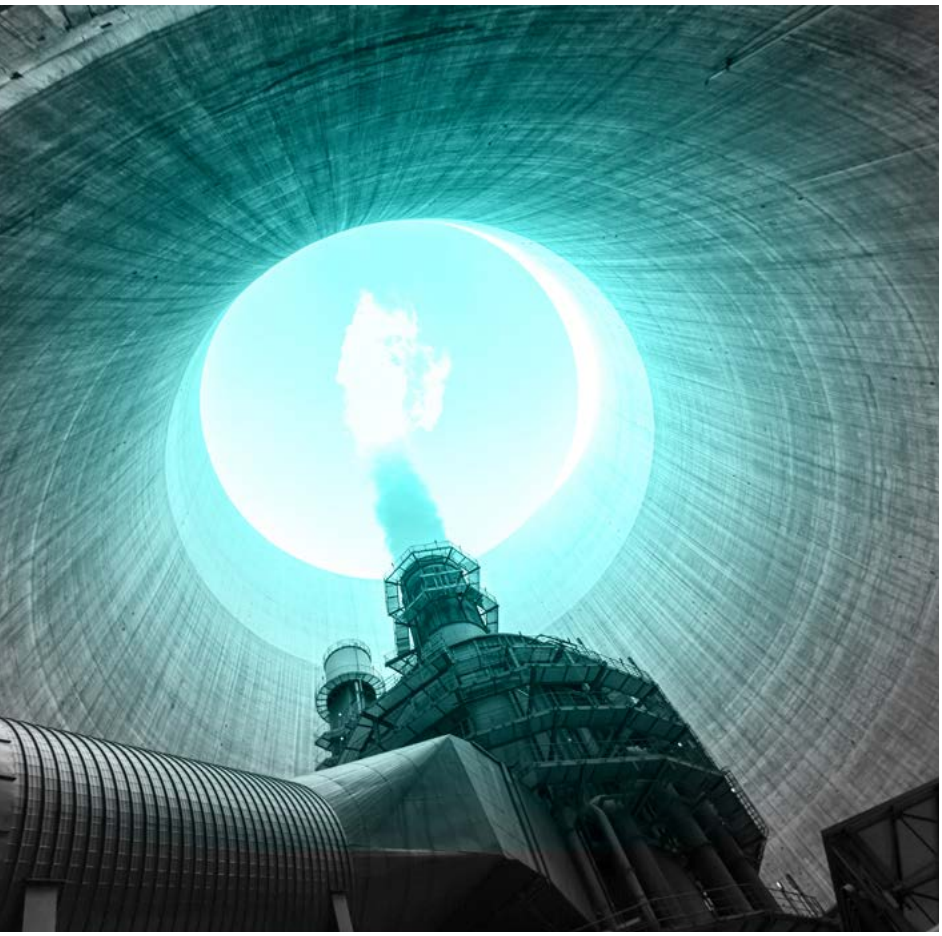
FIGURE 3: RANSOMWARE BY MANUFACTURING SUBSECTOR



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 civilization 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 analyzed

2,170

CVEs analyzed (+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 Prioritization 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 organizations struggle to find actionable guidance on how to prioritize remediation and mitigation efforts based on risk.

With respect to ICS/OT vulnerabilities, it is important to focus and prioritize 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.

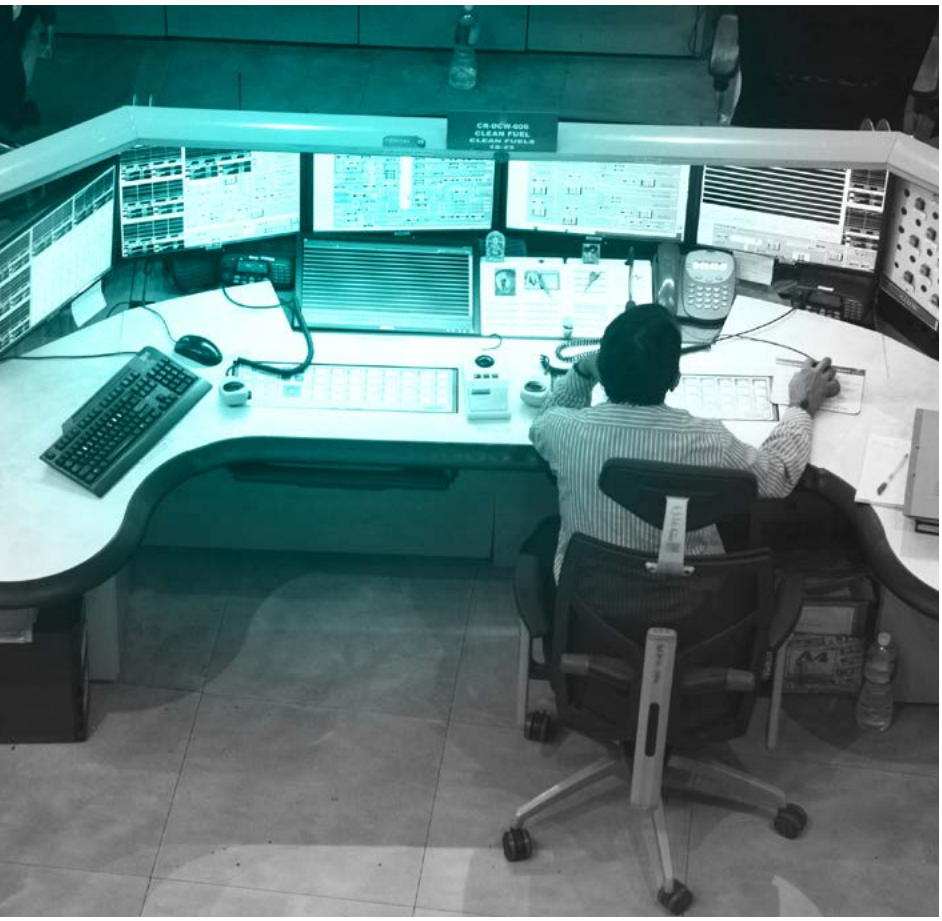
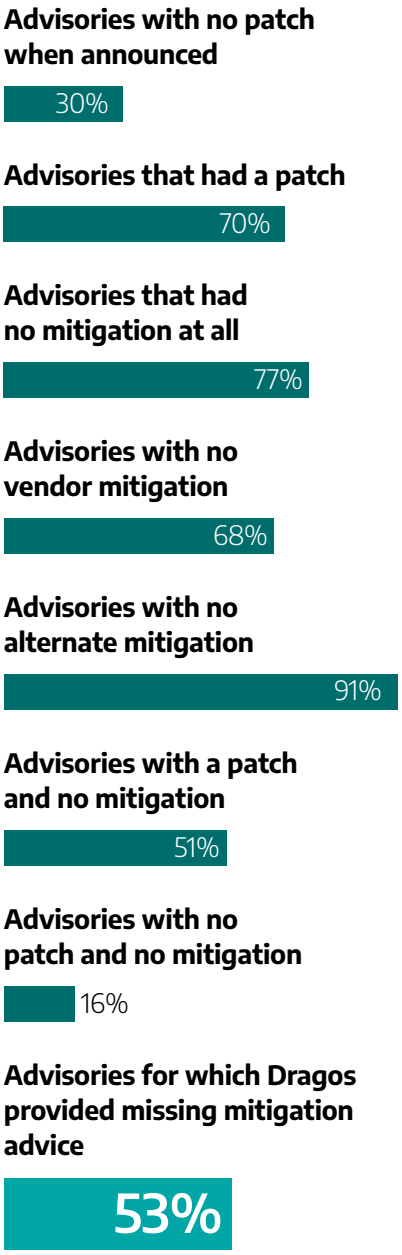


FIGURE 7:
ADVISORIES WITH ERRORS AND LACKING IN ACTIONABLE GUIDANCE



In prioritizing vulnerabilities, Dragos uses a **Now**, **Next**, **Never** framework developed by CERT/Coordination Center (CERT/CC) to help asset owners and operators identify vulnerabilities and prioritize 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 organizations 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 organizations 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 organizations, 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 organizations 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 organizations 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[2]. 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.

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

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