



DRAGO



ICS/OT CYBERSECURITY
YEAR IN REVIEW 2022

Contents

- 2022 Key Findings Overview 4**
- Key Highlights: By the Numbers 6**
- 2022 Threat Activity 8**
 - 2022 New Threat Groups 11**
 - CHERNOVITE 11
 - BENTONITE 13
 - Updates on Active Threat Groups 14**
 - KOSTOVITE 15
 - KAMACITE 17
 - XENOTIME 18
 - ELECTRUM 19
 - ERYTHRITE 20
 - WASSONITE 21
 - CHERNOVITE'S PIPEDREAM 22**
 - Implications and Outlook 22
 - 2022 Industrial Ransomware Analysis 26**
 - Increase in Ransomware Activity 26
 - Industrial Ransomware Attacks 27
 - Ransomware Timeline 28
 - Industrial Ransomware Trends: Moves and Changes 29
 - What's Next? 34
 - Ransomware Kill Chain 34
- ICS/OT Vulnerabilities 36**
 - Root Cause Analysis of Password "Cracking" Vulnerabilities 37**
 - Root-Cause #1: Protocols Lacking Authentication on Critical Functions 39
 - Root-Cause #2: Undocumented Protocol Commands 39
 - Conclusion 39
 - OT:ICEFALL and the Importance of Public Reporting 40**
 - Mitigations for OT:ICEFALL 41

- Key ICS Vulnerability Trends.....42**
 - Overview of Key Findings 42
 - Many Advisories Contained Errors and Lacked Patches and Actionable Guidance..... 43
 - ICS Impact: Loss of View, Loss of Control, or Both 44
 - Where Do Vulnerabilities Reside? 45
 - Errors in Vulnerability Severity Scores 46
- Prioritization and Recommended Actions for Remediations.....47**
 - Now, Next, Never 47
 - Mitigating Vulnerabilities in 2022 48
- Dragos Frontline Perspective 50**
 - Key Findings Overview 51**
 - Methodology..... 51
 - Dataset 51
 - 2022 Key Findings 53**
 - Limited or No OT Network Visibility 53
 - Poor Security Perimeters 55
 - External Connections to OT Environments 57
 - Lacked Separate IT and OT User Management 59
 - Impact of Oil & Gas Pipeline Regulations 61**
 - Assessing Cyber Readiness 63**
 - What is a Tabletop Exercise (TTX)? 64
 - Scoring TTXs 64
 - Key Takeaways for OT Overall 65
 - Key Takeaways for Industry Breakdown 66
 - Key Takeaways for Ransomware Scenarios..... 67
 - 5 Critical Controls for ICS/OT Cybersecurity 68**

2022 Key Findings Overview

2022 saw a breakthrough escalation in capabilities by a new modular industrial control systems (ICS) malware, PIPEDREAM, developed by the threat group, CHERNOVITE. CHERNOVITE'S PIPEDREAM toolkit has the capabilities to impact devices that control critical infrastructure – devices that manage the electrical grid, oil and gas pipelines, water systems, and manufacturing plants. For industrial operators this can be viewed as a supply chain risk, as the methods target key vendor systems.

PIPEDREAM is the first reusable cross-industry capability that impacts native functionality in industrial protocols and a wide variety of devices. Dragos and our third-party partners discovered and analyzed its capabilities before it was employed. Malware development is shifting towards improving on the known and successful techniques used in earlier ICS cyber attacks. This accumulated knowledge may have informed PIPEDREAM's malware framework, which is more robust and modular and most likely will inform CHERNOVITE and other adversaries' malware development in the future.

The threats and ransomware attacks tracked by Dragos in 2022 show a continued increase. Highlights of these attacks by vertical industry include:

- The first attacks against the mining and metals industries in Australia and New Zealand (ANZ) region.
- Continued targeting of renewable energy companies in the U.S. and the European Union (EU).
- Increased attacks on energy, food and beverage, pharmaceuticals, chemicals, water and wastewater
- Accelerated attacks in electrical, manufacturing, oil and natural gas, and liquefied natural gas

Russia's Invasion of Ukraine

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

During 2022, Ukraine saw increased threat group activity targeting its energy and critical industrial infrastructure sectors. Russia's 2022 invasion of Ukraine provided opportunities for Russia-aligned actors to use their cyber offensive capabilities preemptively and in parallel to its kinetic attacks. As Western countries placed sanctions on Russia and indicted key members of Russian cyber operations, the U.S. government's Cybersecurity and Infrastructure Security Agency (CISA) prepared for potential retaliation by issuing a call for "Shields Up," which included actions to safeguard ICS and OT environments.

According to an analysis of the threats against U.S. energy entities, adversaries are primarily focused on reconnaissance. Dragos has observed fewer cyber-focused attacks on OT in U.S. energy sectors than predicted at the beginning of the war between Russia and Ukraine. Dragos has not observed any ICS Cyber Kill Chain Stage 2 follow-on attacks against U.S. energy entities.

While Dragos observed less than the predicted activity, there was still at least one significant attack. The Dragos-designated threat group ELECTRUM deployed a new variant of CRASHOVERRIDE/INDUSTROYER at a Ukrainian power company; however, this new variant did not have the full capabilities of CRASHOVERRIDE.

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

Impacts of Ransomware on Manufacturing

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 sectors and subsectors. As ransomware activity increases, it results in more risk for OT networks, particularly networks with poor segmentation.

Trends in ICS/OT Vulnerabilities

Vulnerabilities saw an increase of 27 percent in 2022. This was a material increase, but a slowdown in the growth rate. Improvements in the rate of mistakes and risk ratings were a very positive signal. The standard information technology (IT) approach to vulnerability mitigation is a patch. To patch in the OT world often requires system and plant shut-downs. ICS/OT relies on alternative mitigation to both reduce risk and maintain production. The 77 percent of vulnerabilities that lack that mitigation makes maintaining operations very challenging.

Markers for a Strong ICS/OT Cyber Defense – 5 Critical Controls

On the defense side, Dragos recommends using the SANS “Five ICS Cybersecurity Critical Controls” for industrial cybersecurity as the frame to evaluate progress. The statistics shown are only “indicators” of the five critical controls, though derived from in-depth engagements with industrial clients.

Trends in **ICS-Specific Incident Response**, the first of SANS Five Critical Controls, were mixed, with improvements in detection, elevation, and plan activation; scores declined in the ability to communicate, document, and recover. Electric utilities showed the best preparedness, followed by oil and gas.

Manufacturing represented the worst results among verticals.

For **Defensible Architecture**, the second critical control, there were marked improvements to use of network segmentation in engagements. Environments with significant network segmentation issues were down 2700 basis points; but with 50 percent of environments still having issues, there is plenty of room for improvement. Similarly, uncontrolled external connections into OT were found in 53 percent of engagements in 2022; still high, but much better than 2021’s 70 percent.

ICS Network Visibility, the third critical control, continued to be a challenge. A full 80 percent of environments had little or no visibility into traffic and devices in ICS/OT environments. Though an improvement of 600 basis points from 2021, the large number indicates that a vast majority of environments will find it challenging to detect and investigate issues, much less maintain accurate asset inventory.

Secure Remote Access is the fourth critical control, and showed negative trending, with users in 54 percent of environments using same credentials for IT systems as OT systems. Remote access is the most common way for threat groups to penetrate OT systems; sharing the same credentials make it much easier for threats to cross from IT to OT systems.

Finally, for **Risk-Based Vulnerability Management**, the reduction in outright mistakes is encouraging. Only fifteen percent of CVEs included errors in 2022, down 4 percent from 2021. But with 77 percent of vulnerabilities lacking mitigation steps, it demonstrates the challenge of employing a risk-management approach that can both mitigate the risk of exploit AND reduce production downtime from patches.

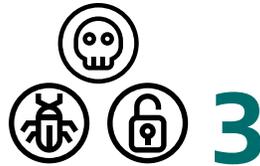
Of course, that is a summary of only some of the findings. Much more detail from Dragos’s intelligence research, platform measurements, and consulting engagements follow.

Key Highlights: By the Numbers

PIPEDREAM summary



The seventh ICS-impacting Malware



ICS-specific malware components inside PIPEDREAM



ICS protocols abused:
FINS, MODBUS, CODESYS, OPC UA, Schneider Electric NetManage



of devices potentially impacted



of suppliers impacted

Threat Group Summary

Two New Threat Groups Identified



CHERNOVITE



BENTONITE

Key Ransomware Findings



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



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



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

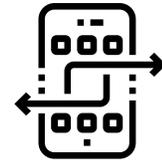
Key Service Engagement Findings

80% 

of services customers had **limited OT visibility** into their ICS environment

-6%
FROM
2021

50%



of services engagements **identified issues with network segmentation**

-27%
FROM
2021

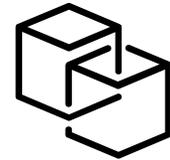
53%



of services engagements discovered **undisclosed or uncontrolled external connections** to the OT environment

-17%
FROM
2021

54%



of services customers **lacked separate IT and OT user management**

+10%
FROM
2021

Key Vulnerabilities Findings

↑
27%



increase in the **number of vulnerabilities that Dragos investigated** in 2022 over 2021

34%



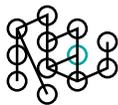
of advisories **contained errors** in 2022.

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

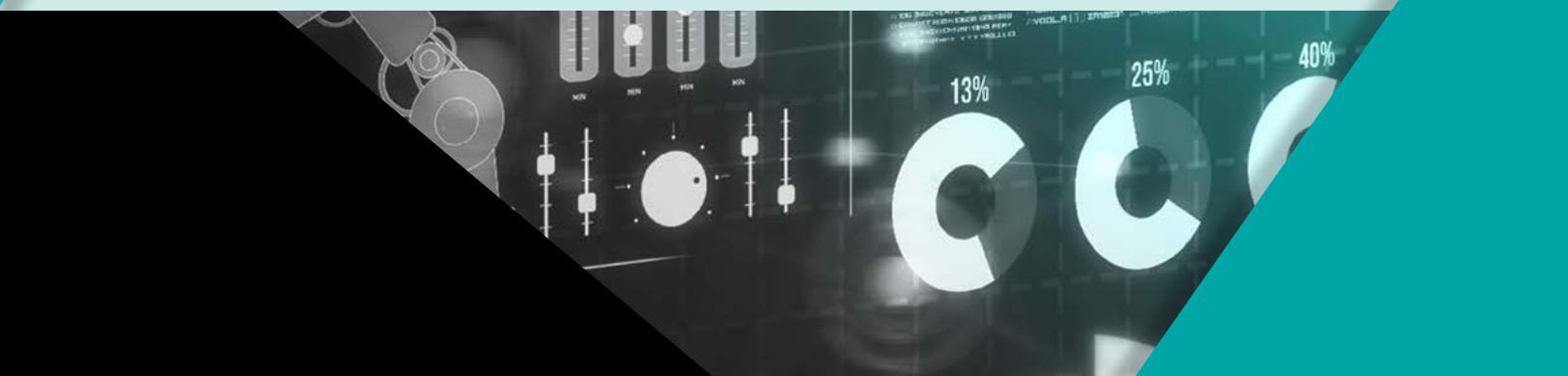
51%



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



2022 Threat Activity



Threat Activity Overview

After analyzing year-over-year activity, Dragos assesses with low confidence that the increase in threat group activity and the focus on energy sectors (electric, renewables, and ONG) could be the result of geopolitical tensions between the Russian Federation and the European Union (EU) over energy resources

and the ongoing war in Ukraine. Threat group activity is relatively steady, and some of the increase in activity is unrelated to geopolitical tensions. Some threats Dragos tracks such as CHERNOVITE may proliferate into disruptive and destructive capabilities in the future.

Summary of Dragos-designated threat group intelligence for 2022:



There are two new threat groups: **CHERNOVITE** and **BENTONITE**

There were eight active threat groups: **BENTONITE, CHERNOVITE, ELECTRUM, ERYTHRITE, KAMACITE, KOSTOVITE, WASSONITE** and **XENOTIME**.



KOSTOVITE, KAMACITE, XENOTIME and **ELECTRUM** exhibit all aspects of the ICS Kill Chain Stage 1, and several of Stage 2 (Develop, and Install/Modify).

BENTONITE and **WASSONITE** demonstrate only Stage 1 aspects of the ICS Cyber Kill Chain



ERYTHRITE demonstrates only Stage 2 aspects of the ICS Cyber Kill Chain.

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

For context, here are the Dragos-designated threat group statistics from the 2021 Year in review:

Three new threat groups: **KOSTOVITE, ERYTHRITE** and **PETROVITE**

Three active threat groups: **STIBNITE, WASSONITE** and **KAMACITE**

During 2022, Dragos tracked 20 threat groups and discovered two new threat groups – **CHERNOVITE** and **BENTONITE**.



CHERNOVITE is the threat group that developed PIPEDREAM. PIPEDREAM is the seventh and most recent ICS-targeted malware discovered in 2022.

CHERNOVITE represents the most dangerous threat group to date as it exhibits all aspects of the ICS Kill Chain Stage 1 and Stage 2.



BENTONITE targets the ONG and LNG industrial verticals in the U.S.

How Dragos Tracks Threat Activity

To be prepared for future threats to industrial infrastructure, Dragos emphasizes the importance of understanding how adversaries steal information, and gain access to a company's ICS/OT network and systems.

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 threats that Dragos tracks may evolve their disruptive and destructive capabilities in the future because adversaries often do extensive research and development (R&D) and build their programs and campaigns over time. This R&D informs their future campaigns and ultimately increases their disruptive capabilities. For instance, most of PIPEDREAM's modules are examples of capabilities that were designed to target OT and ICS infrastructure. Even when an adversary accidentally stumbles onto an OT environment, there is still a risk to that environment. Adversarial intent is not necessarily positively correlated with attacks on ICS/OT environments – they may be “targets of opportunity” discovered during enterprise IT reconnaissance.



For the 2022 Year in Review, Dragos has broadened its criteria for threat group reporting. Dragos now covers threat group activity from 2020 to 2022.

This methodology is based on the following parameters:

- **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.**
- **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.**

This new approach allows Dragos to focus and provide intelligence on the cyber threats that occurred during the last two years. In cases where the evolution of an attack pattern is recognized, even when threat groups are retired, Dragos will report on this activity. Threat groups could go dormant for various reasons, such as the threat group stopping its activity or repurposing its operations. Or, potentially, we lost visibility of its actions.



2022 New Threat Groups

CHERNOVITE & BENTONITE

CHERNOVITE – Developer of PIPEDREAM

CHERNOVITE is the developer of PIPEDREAM, a modular ICS attack framework and the seventh known ICS-specific malware, following STUXNET, HAVEX, BLACKENERGY2, CRASHOVERRIDE, TRISIS, and Industroyer2. CHERNOVITE's PIPEDREAM is the first ever cross-industry disruptive/destructive ICS/OT capability. It represents a substantial escalation in adversarial capabilities.

CHERNOVITE possesses a breadth of ICS-specific knowledge beyond what has been demonstrated by previously discovered threat groups. The ICS expertise demonstrated in the PIPEDREAM malware includes capabilities to disrupt, degrade, and potentially destroy physical processes in industrial environments.

PIPEDREAM is the first scalable, cross-industry ICS attack framework known to date.

While PIPEDREAM itself is a new ICS capability, its emergence is also indicative of the trend toward more technically capable and adaptable adversaries targeting ICS/OT. In addition to implementing common ICS/OT-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.

Dragos assesses with high confidence that a state

actor developed PIPEDREAM intending to leverage it in future operations for disruptive or destructive purposes. Dragos assesses with moderate confidence that CHERNOVITE represents an “effects/impact team” instead of an “access team” – meaning, that PIPEDREAM was designed to be leveraged for impact after the initial access into the target environment has been obtained by another threat group.

Most likely, CHERNOVITE developed PIPEDREAM’s capabilities for a malicious operator with the intent and motivation to access, manipulate, and disrupt OT environments and processes. PIPEDREAM’s capabilities can provide an adversary with a range of options for learning about a target’s OT network architecture and identifying its assets and processes. This information can set the stage for disruptive and destructive effects, but it also increases an adversary’s knowledge to develop even more capabilities to disrupt or destroy on a much broader scale.

In its present form, the PIPEDREAM attack framework could be leveraged to target equipment in multiple sectors and industries. Given PIPEDREAM’s modular nature, CHERNOVITE could easily adapt it to compromise and disrupt a broader set of targets.

Therefore, it is necessary for defenders to harden their environment against CHERNOVITE’s known set of capabilities and focus on the tactics, techniques, and procedures (TTP), abuse of environment-native protocols and functionality, and exploitation of a lack of OT asset visibility and network monitoring.

Dragos assesses with low confidence that no adversary has employed or leveraged components of PIPEDREAM against industrial networks for disruptive or destructive effects. Dragos’s discovery of CHERNOVITE constitutes a rare case of accessing and analyzing malicious capabilities developed by an adversary before its employment, giving defenders a unique opportunity to prepare in advance.



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

BENTONITE

BENTONITE is a new threat group increasingly and opportunistically targeting maritime oil and gas (ONG), governments, and the manufacturing sectors since 2021. BENTONITE conducts offensive operations for both espionage and disruptive purposes.

BENTONITE seeks to exploit vulnerable remote access assets or internet-exposed assets that can facilitate access.

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 achieves initial access, the adversary delivers a downloader-type malware implant to retrieve additional malware implants from adversary-created GitHub accounts. These malware implants conduct command and control to adversary-owned infrastructure, reconnoiter the compromised host, conduct network reconnaissance, and establish a connection through SSH, enabling the adversary operator to perform interactive operations.

BENTONITE's activities are highly opportunistic when it comes to the victims they target. Additionally, once BENTONITE gains access to a victim's environment, this adversary 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 utilizes legitimate infrastructure, such as GitHub, and adversary-owned infrastructure for command and control and capability delivery. BENTONITE is capable of and has in past compromised disrupted operations through wipers; however, this was not observed in the compromises of the ONG or SLTT organizations.

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

VICTIMS

- 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



Updates on Active Threat Groups

KOSTOVITE, KAMACITE, XENOTIME,
ELECTRUM, ERYTHRITE, WASSONITE

KOSTOVITE

In June 2021, Dragos began tracking the threat group KOSTOVITE. KOSTOVITE's operational technology (OT)-related operations have focused on the compromise of an energy firm and the firm's managed global power generation facilities.

KOSTOVITE has achieved Industrial Control System (ICS) Cyber Kill Chain Stage 1 and subsequent ICS Kill Chain Stage 2, Develop events.

While KOSTOVITE's demonstrated capabilities do not extend to industrial control system (ICS)-disruption-specific tools or resources, KOSTOVITE has demonstrated skilled lateral movement and initial access operations into ICS/OT environments and on SCADA assets.

KOSTOVITE focuses on compromising and subverting internet-exposed remote access devices as a jump-off point into OT targets while establishing persistence across the upgrades of the remote access devices.

KOSTOVITE maliciously enlists third-party internet of things (IoT) devices to relay and obfuscate the origin of their activities. KOSTOVITE shows unusual discipline by dedicating a set of compromised IoT devices to a single target and then performing a clean-up operation at the end of its activities.

Based on non-public reporting on Manganese adversary activity and activity described by an early 2022 Kaspersky ICS CERT report², multiple adversaries with different objectives may share a common infrastructure with KOSTOVITE.

While the infrastructure enumerated by Microsoft and Kaspersky shows a tentative link to the KOSTOVITE activity that Dragos observed in 2021, Dragos cannot definitively tie all these activities to one adversary.

Recent public reporting shows KOSTOVITE may be linked to the APT5 adversary group. The U.S. government reported in December 2022 that APT5 was actively exploiting a zero-day vulnerability in Citrix perimeter access devices, which parallels KOSTOVITE's zero-day exploitation against an energy O&M firm in 2021, and previous APT5 campaigns targeting perimeter devices in 2019. Both KOSTOVITE and APT5 have leveraged vulnerabilities in perimeter-facing remote access appliances, achieving persistent access to targets over several months undetected. There is a likelihood that KOSTOVITE's tooling may



KOSTOVITE

ADVERSARY

- High level of operational discipline and network device knowledge
- Lives off land with stolen sys/net-admin creds

CAPABILITIES

- Zero-day exploits
- Undetected intrusion via internet remote access device compromise and subversion

VICTIMS

- Global energy company based in U.S.
- North America, Australia

INFRASTRUCTURE

- Dedicated per target
- Compromised home and small business IoT devices exposed to Internet
- Compromised enterprise perimeter devices

ICS IMPACT

- Stage 2 of ICS Kill Chain
- Intrusion into OT networks and devices

² Targeted attack on industrial enterprises and public institutions - Kaspersky ICS CERT

³ <https://media.defense.gov/2022/Dec/13/2003131586/-1/-1/0/CSA-APT5-CITRIXADC-V1.PDF>

expand to include the remote access device zero-days exploited by APT5.

If KOSTOVITE once again takes aim at ICS and OT, asset owners and operators should be ready with

robust detection, defense, and mitigation regimes for the ICS and OT enclaves that are inside the enterprise perimeter and potentially vulnerable to KOSTOVITE exploitation.



KAMACITE

KAMACITE is a threat group targeting industrial infrastructure verticals since at least 2014. KAMACITE is linked to multiple industrial infrastructure intrusion events, including operations enabling the 2015 and 2016 Ukraine power events. KAMACITE possesses industrial control system (ICS)-specific capabilities but has also facilitated ICS disruptive events executed by other threat groups such as ELECTRUM.

Most recently, in June of 2022, Dragos identified KAMACITE network infrastructure communicating with an oblenergo (a regional power distribution entity) in Ukraine. The oblenergo KAMACITE targeted in this incident was one of the same oblenergos impacted in a 2015 cyber attack, which triggered a large-scale power outage across western Ukraine.

In February 2022, the National Cyber Security Centre (NCSC) in the UK released a joint report with CISA, NSA, and FBI detailing the new malware capability called CYCLOPS BLINK, stating that it targets “primarily small office/home office (SOHO) routers and network-attached storage (NAS) devices.”⁴ The CYCLOPS BLINK malware family targets routers and firewall devices from WatchGuard and ASUS and adds them to a botnet for command and control (C2).

Dragos assesses with high confidence that this activity is associated with KAMACITE. At the time of the February 2022 report, Dragos identified victims in the electric, natural gas, and food and agriculture (including manufacturing, processing, and storage) industries communicating with KAMACITE’s C2 infrastructure.

In March of 2022, Dragos analyzed new CYCLOPS BLINK samples that appeared in the wild.⁵ Based on this analysis, Dragos discovered new C2 infrastructure associated with KAMACITE’s CYCLOPS BLINK operations. Dragos identified a set of hosting provider-owned IP addresses, which host domains for organizations in the rail, aerospace, food & beverage, and automotive sectors, along with three U.S. Government IP addresses communicating with this new CYCLOPS BLINK C2 infrastructure.

Dragos assesses with moderate confidence that this was scanning activity to identify vulnerable target devices.

In April of 2022, the U.S. Department of Justice (DOJ) released a public notice that stated that through March of 2022, the U.S. DOJ had been copying and removing malware from vulnerable

⁴ <https://www.ncsc.gov.uk/news/joint-advisory-shows-new-sandworm-malware-cyclops-blink-replaces-vpnfilter>

⁵ <https://www.mandiant.com/resources/blog/ukraine-and-sandworm-team>

⁶ <https://portal.dragos.com/#/products/AA-2022-15>



KAMACITE

ADVERSARY

- Overlaps with SANDWORM activity⁵

CAPABILITIES

- Phishing & credential replay for initial access
- Custom malware development & deployment; also known to modify third party criminal malware

VICTIMS

- Europe, including Ukraine, and U.S.

INFRASTRUCTURE

- Primary focus on compromised infrastructure in Europe
- Spoofs legitimate technology & social media services

ICS IMPACT

- Operations linked to five ICS targeting events
- Proven operations leading to disruption
- Facilitated the 2015 and 2016 Ukraine power events

firewall devices, which were being used for C2 CYCLOPS BLINK operations.

In May of 2022, KAMACITE targeted routers and IP cameras for initial network access to environments as early as March 2022. These devices were different from devices targeted in the CYCLOPS BLINK campaign. Dragos discovered victims throughout Ukraine and worldwide, including a victim in the food and beverage sector.

Based on past activities and renewed activities in 2022, Dragos assesses with moderate confidence that KAMACITE will continue to conduct reconnaissance and C2 operations.

XENOTIME

The Dragos-tracked threat group XENOTIME is one of the four (including CHERNOVITE, ELECTRUM, and KAMACITE) publicly known threat groups that has the intent, motivation, and capability to target and disrupt or destroy critical infrastructure, particularly in the ONG sector.

During 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.

Dragos is aware of extensive XENOTIME research activity focused on LNG compressor train processes, LNG terminal ports, offshore production sites, and emergency response organizations for ONG, as well as onshore production sites around shale gas and midstream organizations.

Dragos has not observed any indication that XENOTIME is currently conducting active exploitation or compromise operations against ONG or LNG organizations. However, XENOTIME's ongoing activities represent a significant increase in future risk to the LNG and ONG sectors.

Dragos assesses with low confidence XENOTIME's ultimate goal is causing a loss of containment for environmental impact, which would delay operations or potentially shut down an LNG export terminal. Currently, XENOTIME is in the development



XENOTIME

ADVERSARY

- Unique tool development

CAPABILITIES

- TRISIS
- Custom credential harvesting
- Off-the-shelf tools

VICTIMS

- Oil and gas, electric utilities
- Middle East, North America

INFRASTRUCTURE

- Virtual Private Server and compromised, legitimate infrastructure
- European web hosting providers
- Asian shipping company

ICS IMPACT

- Demonstrated capability to execute disruptive ICS attack, such as the 2017 TRISIS incident

phase of offensive cyber operations, most likely focusing on capability and infrastructure development.

ELECTRUM

ELECTRUM is still active in 2022 and continues to develop and modify capabilities against electric grid operations.

In April 2022, Dragos learned of a series of recent public security announcements from the Slovakian security firm ESET, which identified multiple malware capabilities uncovered at a Ukrainian utility provider. Dragos assesses with moderate confidence that the threat group behind this 2022 attack was ELECTRUM, marking the third time ELECTRUM had attacked a Ukrainian utility provider. While the execution of a successful industrial control systems (ICS) attack was prevented, years earlier ELECTRUM's malware was also used to attack a Ukrainian ICS electric grid in 2016.⁷

In the April 2022 incident, ELECTRUM deployed INDUSTROYER2 malware along with a set of wiper malware. The wiper malware deployed with INDUSTROYER2 was used to cover ELECTRUM's tracks.

Dragos assesses with high confidence that ELECTRUM will continue to target electric utilities in Ukraine. ELECTRUM also has the capability to target electric entities outside of Ukraine because of the similar equipment and protocols in other electric environments.



ELECTRUM

ADVERSARY

- Overlaps with SANDWORM activity⁸

CAPABILITIES

- Unique RAT & malicious wiper modules

VICTIMS

- Electric sector
- Europe, including Ukraine

INFRASTRUCTURE

- Leveraged servers hosting many additional services such as Tor

ICS IMPACT

- Executed control system portion of 2016 Ukraine power event, deployed CRASHOVERRIDE designed to manipulate electric transmission equipment

INDUSTROYER2

INDUSTROYER2 is the sixth known ICS-specific malware; however, the April 2022 incident marked the first time ICS-specific malware had been reconfigured and then redeployed in an electric utility environment, which was also impacted by CRASHOVERRIDE in 2016.

INDUSTROYER2 utilizes 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

components, including a 104 module that utilized 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.

⁷ <https://www.dragos.com/threat/electrum/>

⁸ <https://www.mandiant.com/resources/blog/ukraine-and-sandworm-team>

ELECTRUM's 2016 Attack

Looking back at ELECTRUM's history, the second attack on the Ukrainian power grid occurred in December of 2016, causing a power grid outage in Kyiv that turned off the lights for a quarter million Ukrainians. It was a significant incident that blacked out a portion of the city's electricity for about an hour. Dragos's assessment of the events determined that at least two threat groups – KAMACITE and ELECTRUM – combined their efforts to execute this ICS attack.

In the 2016 attack, ELECTRUM used malware designed to attack industrial control systems (ICS) called CRASHOVERRIDE. However, unlike CRASHOVERRIDE, which had multiple components, INDUSTROYER2, used in April 2022, only utilizes the International Electrotechnical Commission (IEC) IEC-104 protocol to communicate with its industrial equipment targets.

ERYTHRITE

During 2022, ERYTHRITE continued to compromise industrial organizations across multiple sectors in North America with its adaptable search engine optimization (SEO) poisoning and custom, rapidly redeveloped malware. ERYTHRITE has a consistent ability to develop and deploy malware and infrastructure at scale.

While ERYTHRITE has not demonstrated any ICS-specific capabilities, ERYTHRITE poses a persistent and active threat to industrial organizations when you consider the volume of its activity, its focus on data and credential theft during its post-compromise activities, and its affiliation with the cybercriminal ecosystem. ERYTHRITE is a particular threat to organizations where poor ICS/OT network segmentation and network visibility have created a vulnerable environment.

Since 2021, 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.

**ERYTHRITE****ADVERSARY**

- Overlap with group known as Solarmaker

CAPABILITIES

- Search Engine Optimization (SEO) poisoning; bespoke, rapidly refashioned low detection credential stealing and remote access malware

VICTIMS

- U.S., Canada
- ~20% of Fortune 500 companies
- Large Electric Utility
- Electronic agreement and document signature company

INFRASTRUCTURE

- C2 and management in Russia, reverse proxies in North America and Europe, hundreds of thousands of vulnerable but otherwise legitimate websites abused for SEO poisoning

ICS IMPACT

- Credentials, sensitive information, and remote access to OT environments potentially sold to illicit third parties

WASSONITE

Since 2018, the Dragos-tracked threat group WASSONITE has targeted industrial control systems (ICS) entities in the nuclear energy, electric, oil and gas, advanced manufacturing, pharmaceutical, and aerospace industries predominately in South and East Asia, with some additional targets in North America. WASSONITE's operations have demonstrated a repeated ability to achieve initial Stage 1 activity defined by the ICS Cyber Kill Chain.

In October 2022, Dragos analyzed WASSONITE's use of nuclear energy-themed spear phishing lures written in Hanguk to deliver the AppleSeed backdoor. The Appleseed backdoor is 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.

WASSONITE's use of spear phishing lures with content and titles highly targeted toward nuclear energy in East Asia is consistent with WASSONITE's enduring, long-term interest in targeting organizations in this industry. Dragos's analysis of the malicious files and the adversary's infrastructure led to the identification of additional samples and domains associated with this campaign.

WASSONITE's continued deployment of customized variants of the AppleSeed backdoor throughout 2021 and 2022 represented a shift in capabilities away from the previous use of customized variants of DTrack malware.

The WASSONITE activity group leverages spear phishing lures, often customized for specific industries and organizations, as their initial infection vector. WASSONITE malware variants also display highly targeted modifications for individual environments, including hard-coded credentials, non-public internet protocol (IP) addresses, and uncommon ports for specific applications.

Dragos assesses with moderate confidence that WASSONITE will continue to target ICS entities in nuclear energy, electric, oil and gas, advanced manufacturing, pharmaceutical, and aerospace industries in East Asia, South Asia, and North America.



WASSONITE

ADVERSARY

- Limited technical overlaps to COVELLITE⁹ and the cluster of activities tracked by other organizations as Kimsuky

CAPABILITIES

- Customized variants of the DTrack and Appleseed RATs
- Mimikatz and system tools for lateral movement and file transfers

VICTIMS

- Nuclear energy, electric, oil and gas, advanced manufacturing, pharmaceutical, and aerospace industries
- South/East Asia and North America

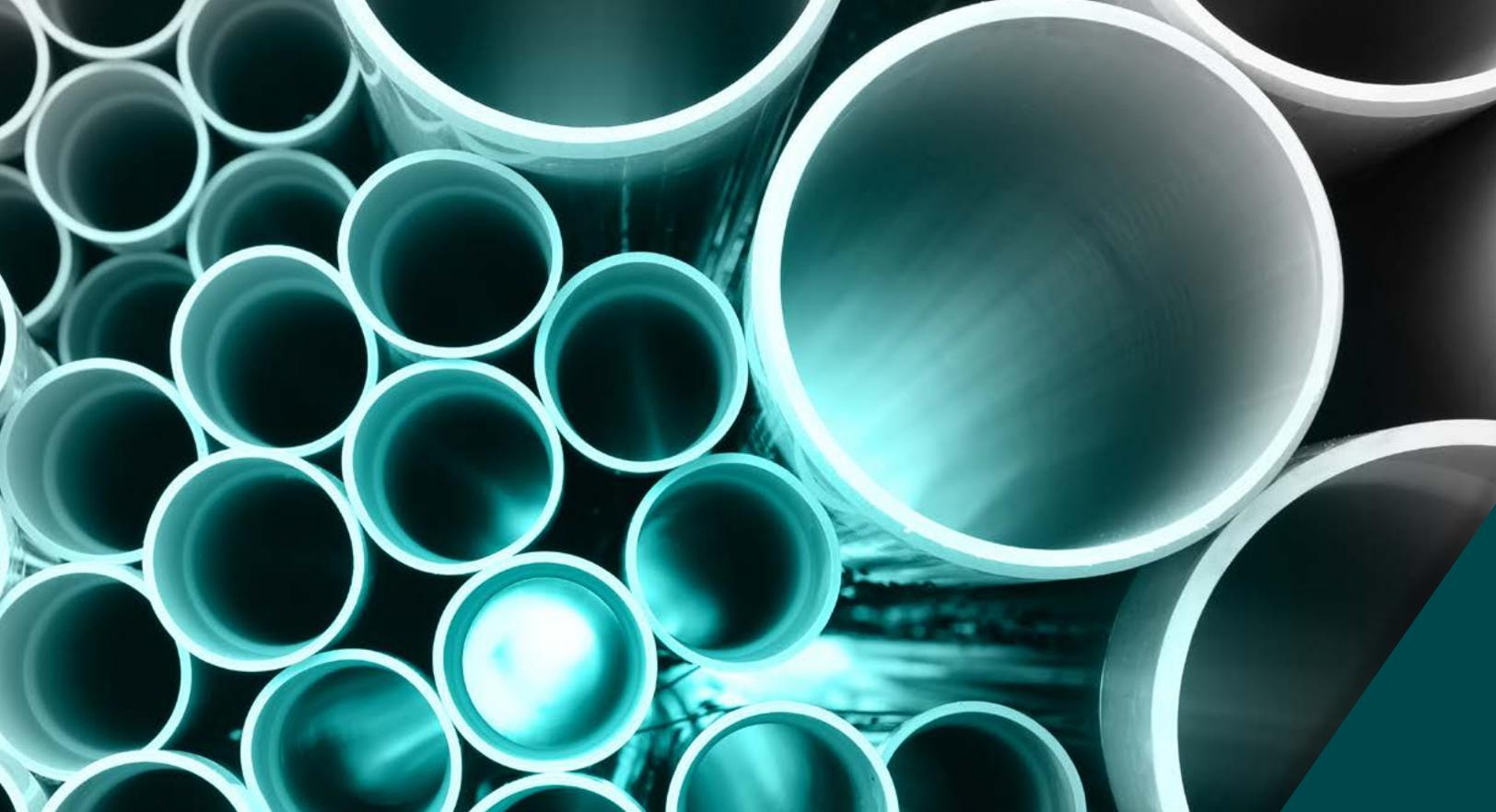
INFRASTRUCTURE

- Adversary-registered and controlled domains & infrastructure for C2
- Use of compromised, legitimate services in some instances

ICS IMPACT

- Focus on targeting ICS-related organizations
- Focus on network actions consistent with information gathering, including from protected network segments

9 <https://www.dragos.com/threat/covellite/>



CHERNOVITE'S PIPEDREAM

IMPLICATIONS AND OUTLOOK

In April of 2022, Dragos and a partner announced the discovery of PIPEDREAM – a cross-industry industrial control system (ICS) attack framework developed by the threat group CHERNOVITE explicitly to attack industrial infrastructure. PIPEDREAM is the seventh-known ICS-specific malware, and the fifth malware specifically developed to disrupt industrial processes.

PIPEDREAM represents a new evolution in malware development. It is the first cross-industry scalable ICS malware with disruptive capabilities. Given the right operational conditions, PIPEDREAM could be used for destructive effects.

Dragos identified and analyzed PIPEDREAM's capabilities through our daily business and collaboration with various partners in early 2022.

The discovery of PIPEDREAM before its employment gives industrial operators, security vendors, and industrial control system vendors a unique opportunity to take this proactive intelligence and turn it into concrete action to prevent, detect, and mitigate attacks like PIPEDREAM – and future attacks that leverage TTPs similar to PIPEDREAM.

The Role of Industrial Operators

Industrial operators are at the ground level of critical infrastructure, and when it comes to delivering critical services, they are the closest to the customer. To secure against attacks, Dragos recommends that industrial operators implement the five critical controls highlighted in the SANS white paper, "The Five Critical Controls for ICS/OT," by Tim Conway and Robert M. Lee.¹⁰

¹⁰ <https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/>

Role of ICS Vendors

ICS vendor partnerships are essential in securing OT networks against PIPEDREAM or similar-styled malware. Partnerships can assist in primarily two important ways:

First, ICS vendors can provide value to vulnerability and risk management programs by being more transparent about their underlying products' software stack. PIPEDREAM's use of CODESYS means that potentially thousands of products are at risk across industries.

Also, vendors should include more information, such as the inclusion of CODESYS and other third-party components, with product installers and purchases and provide information to customers on their website.

In addition, vendor support teams should have that information readily available if a site needs to evaluate whether products from a particular vendor are a concern. To that end, current SBOM standards help deliver the information in a machine-ingestible way. Vendor development teams should consider producing a software bill of materials (SBOM) as part of their development cycle. Microsoft has open-sourced a tool and includes guidance on how to integrate it into current continuous integration/continuous delivery (CI/CD) pipelines.¹¹

No individual industrial operator, security vendor, or ICS vendor can independently solve or mitigate attacks like PIPEDREAM. All three communities should collaborate transparently with support from projects like MITRE ATT&CK and relevant industry-sharing groups so sites can be more secure from PIPEDREAM and any other future attempts to disrupt critical infrastructure.

PIPEDREAM as a Potential Supply Chain Threat

Havex, CRASHOVERRIDE, Industroyer2, and PIPEDREAM all leverage the standardized ICS protocols that are built into a variety of products. Before PIPEDREAM, CRASHOVERRIDE and Industroyer2 were focused primarily on the electric power industry for disruption (IEC104, IEC101, IEC61850/MMS, OPC-

PIPEDREAM consists of five components:



EVILSCHOLAR: A capability designed to discover, access, manipulate, and disable CODESYSv3 devices, with an initial targeting of Schneider Electric motion controllers.



BADOMEN: A capability designed to scan, identify, and interact with Omron PLCs.



MOUSEHOLE: A tool for interacting with OPC UA servers. This includes reading and writing node attribute data, enumerating the Server Namespace and associated node IDs, and brute forcing credentials.



DUSTTUNNEL: A custom remote operational implant capability to perform host reconnaissance and command and control (C2).



LAZYCARGO: A user-mode Windows executable that drops and exploits a vulnerable ASRock driver to load an unsigned driver.

¹¹ <https://github.com/microsoft/sbom-tool/>

DA). Havex was the industry’s first glimpse into the potential cross-industry impact an adversary could have by taking advantage of a standard protocol. Havex’s campaign goal was espionage, and by using OPC DA, the adversary gathered data on networks from companies in the energy, aviation, and pharmaceutical sectors, to name a few.

While we can never know whether CHERNOVITE looked at Havex when designing PIPEDREAM, we do know that PIPEDREAM takes that cross-industry ability to the next level with the EVILSCHOLAR and MOUSEHOLE malware. Combined, they target CODESYS, MODBUS, and OPC UA and give the toolkit the ability to target thousands of devices across critical industries. See Table 1.

TABLE 1: OVERVIEW OF CODESYS, MODBUS, AND OPC UA

Main components and description	Malware	Architecture	Ubiquity	Vendors/Suppliers
CODESYS – Leading manufacturer of independent IEC 61131-3 automation suite.	 EVILSCHOLAR	Several million CODESYS-compatible devices.	1,000 different device types.	Over 500 manufacturers. Examples: Advantech, Berghof Automation, Bosch Rexroth, Eaton, Hitachi, Schneider Electric, Omron
Industrial reach categories				
<ul style="list-style-type: none"> • Building automation • Energy generation, transportation, and storage • Manufacturing automation (assembly, textile, and packaging); 		<ul style="list-style-type: none"> • Transportation (Construction and agriculture vehicles, ships, yachts, and commercial transportation) • Chemical, water treatment, recycling • Other embedded applications like intelligent weighing systems 		
Source: www.codesys.com				

Main components and description	Malware	Architecture	Ubiquity	Vendors/Suppliers
MODBUS – De facto standard data communication protocol connecting industrial electronic devices originally published by Modicon (now Schneider Electric) in 1979 for use with its programmable logic controllers (PLC).	 EVILSCHOLAR	Commonly seen on TCP port 502.	600+ suppliers, 200+ controllers, 60+ software packages, and 100s of other device types such as IO modules, network gateways, modems, and RTUs.	A wide variety of industries and companies. Examples: Grundfos, Hitachi Industrial Products, Phoenix Contact, Schneider Electric, ABB, Emerson, Honeywell, IBM, Rockwell Automation, and Schweitzer engineering.
Source: www.modbus.org				

TABLE 1: OVERVIEW OF CODESYS, MODBUS, AND OPC UA (CONTINUED)

Main components and description	Malware	Architecture	Ubiquity	Vendors/Suppliers
<p>OPC UNIFIED ARCHITECTURE (OPC UA) – Multi-platform standard industrial protocol used for monitoring and control to simplify communications with devices that traditionally spoke different protocols.</p>	 MOUSEHOLE	The goal of the OPC UA protocol is to simplify communications with devices that traditionally spoke different protocols like a translator.	More than 4,200 suppliers have created more than 35,000 different OPC products used in more than 17 million applications.	4,200 suppliers who have created more than 35,000 different OPC products used in more than 17 million applications.

Source: opcfoundation.org/about/opc-technologies/opc-ua/

Is PIPEDREAM a Supply Chain Risk?

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 malware is new and different compared to CRASHOVERRIDE, which focused on electric substation-specific protocols, or TRISIS, which impacted one particular safety controller (Triconex). Most likely, the adversary will continue to improve this

toolkit—not just to improve support for the CODESYS protocol, but possibly even to expand it to support other protocols. The OPC UA and Modbus components in PIPEDREAM are open-source projects that are widely available. A quick internet search shows there are many other open-source projects for supporting other protocols in the industrial/OT space, such as CIP, BACNet, EthernetIP, Profinet, EtherCAT, and more. The adversary could leverage any one of these to expand their potential target space and give PIPEDREAM even more cross-industry flexibility.





2022 Industrial Ransomware Analysis

Ransomware continued to pose financial and operational risks to industrial organizations worldwide in 2022. Of all the industrial sectors in 2022, ransomware groups targeted the manufacturing industry more than any other –nearly twice as much as the other industrial groups combined.

This year witnessed the demise of Conti and the introduction of a new version of Lockbit, Lockbit 3.0. Black Basta and several other ransomware groups targeting industrial control systems and operational technologies were introduced this year.

Increase in Ransomware Activity

Dragos monitors and analyzes the activities of 57 different ransomware groups that target industrial organizations and infrastructures. Through publicly disclosed incidents, network telemetry, and dark web resources, Dragos observed that out of these

57 groups, only 39 were active in 2022 – showing a 30 percent increase year over year. Dragos tracked 605 ransomware attacks against industrial organizations in 2022, an increase of 87 percent over last year.

There were multiple reasons for the increase in ransomware activity impacting industrial organizations, including political tensions, the introduction of Lockbit Builder, and the continued growth of ransomware-as-a-service (RaaS). Dragos observed ransomware trends tied to political and economic events, such as the conflict between Russia and Ukraine and Iranian and Albanian political tensions.

Russia's invasion of Ukraine on February 24, 2022 increased the likelihood of impactful cyber activity against the industrial infrastructure of both combatants. Other indications of political partisanship (which may have impacted industrial organizations) include Conti's declared alignment with the Russian Federation before it disbanded in May of 2022.

RaaS continued to grow as an attack vector in 2022 with an even greater impact on ICS and OT.

Typically, the RaaS developers provide their offerings, complete with data exfiltration tools, to other criminal actors who use them to opportunistically attack organizations. The adversaries who stage the attacks and the RaaS developers divide the profits. LockBit is a good example. RaaS makes it even more difficult to identify the ransomware groups behind these incidents because they are not directly launching attacks but instead through a modular platform-as-a-service offering. The RaaS model, with its cloud-based, point-and-click interface, lowers the barrier to entry into this type of criminal activity.

As with any ransomware attack, there is always a threat of adversaries achieving Stage 1 and cascading impacts onto operational processes and systems. In addition, attacks against IT infrastructure can impact OT networks.

Industrial Ransomware Attacks

Ransomware attacks disrupted the operations of multiple 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 attacks.

Dragos identified multiple potential victims of Conti ransomware in the automotive manufacturing sector. In 2022, Dragos analyzed multiple variants of Lockbit ransomware, affecting many industries, including electric, manufacturing, construction, transportation, technology, consumer services, retail, and logistics – with many enabled by remote desktop software. Dragos discovered multiple ransomware variants/affiliates impacting food and beverage entities with ransomware variants executing ICS Cyber Kill Chain Stage 1 – Install/Modify, Act attacks. However, Dragos assesses with moderate confidence that the ransomware groups are not explicitly targeting this sector but going after “low-hanging fruit.”

FIGURE 1: SIGNIFICANT ICS RANSOMWARE EVENTS IN 2022



JAN 8 Ransomware Group Impacts Subex and Sectrio



JAN 27 Ransomware-as-a-Service Impacts Multiple Industries



FEB Ransomware Attack on Kojima Industries



FEB Third wiper malware targets Ukrainian entities



MAY 9 Ransomware Attack on AGCO



LATE MAY Foxconn Ransomware Attack



AUG 15 South Staffordshire Water Ransomware Incident



AUG 24 Greek Natural Gas company, DESFA, Ransomware Incident



SEPT Modular Mining Possibly Impacted by BianLian Ransomware



OCT Ransomware Attacks Obtain CEII from Electrical Industry



OCT/NOV Mining and Metals and Food & Beverage



DEC 27 Ransomware Attack on Copper Mountain Mining Company

Ransomware Timeline

The ransomware timeline (see previous page) lists the most impactful industrial ransomware attacks that Dragos reported on during 2022. The attacks spanned many industries, including energy, automotive, agriculture, water, mining, and metals.

Subex and Sectrio

On January 8, 2022, the ransomware Group Ragnar Locker listed telecom analytics firm, Subex and its Sectrio subsidiary on their dedicated leak site (DLS) along with over 500 GB of data. Because Subex and Sectrio provide solutions to many industrial organizations, Dragos assesses with low confidence that this release of sensitive data could impact ICS/OT organizations and may enable Stage 1 of the ICS Kill Chain.

Ransomware-as-a-Service Impacts Multiple Industries

In January 2022, Dragos analyzed multiple variants of Lockbit Ransomware-as-a-Service, impacting many industries, including electric, manufacturing, construction, wholesale, finance, professional services, legal, transportation, technology, consumer services, retail, and logistics. Remote desktop protocols could enable initial access in a typical Lockbit attack. Exfiltration tool, Stealbit, steals data before executing the Lockbit ransomware. A Lockbit attack could disable Microsoft Windows assets, potentially impacting remote access to OT networks through lateral movement across networks.

Kojima Industries Corp

This Conti-related ransomware attack in February of 2022 targeted Kojima, a supplier of Toyota's plastic parts and electronic components. The incident suspended Toyota plant operations for several days. Concurrently, Dragos observed internet telemetry of a common Conti-controlled Emotet Tier 2 node in Command and Control (C2) with networks of several other global automakers. Dragos observed numerous automotive organizations across North America and Japan frequently communicating with the Emotet C2 servers. Emotet is a malware strain and cybercrime operation that has precipitated ransomware events.

OT-SPECIFIC RANSOMWARE RISKS

After Dragos assessments, we typically ask the team some specific **qualitative** questions to help understand the state of defensive architectures related to ransomware:

- Did the asset owner have an existing IRP/playbook designed for OT ransomware events?
- Yes, no, or out of scope (unknown)?
- Did the asset owner have strong Level 3/Level 4 protections to prevent opportunistic ransomware delivery?

More quantitative:

- OTW Fleet – Native MSFT protocols (RDP, NetBIOS, ntlm, smb, etc.) between Level 3 and Level 4 (or lower trust) networks. High volume, limited, none.

Multiple Ukrainian Entities

In February 2022, a ransomware variant called "HermeticRansom" was discovered with destructive capabilities targeting multiple Ukrainian entities. Dragos assesses with moderate confidence that adversaries will use HermeticRansom to target other entities.

AGCO

In May 2022, AGCO, a U.S.-based manufacturer and distributor of agricultural equipment, disclosed that they suffered a ransomware attack affecting multiple production facilities. Black Basta was responsible for this incident. Dragos assesses with low confidence that this precautionary shutdown of their IT networks also impacted AGCO's ICS networks and operations.

Foxconn

Foxconn confirmed that a late-May 2022 ransomware attack impacted operations at one of the company's manufacturing locations in Tijuana, Mexico. Foxconn is a Taiwanese multinational electronics contract manufacturer headquartered in Tucheng, New Taipei City, Taiwan. The Ransomware as a Service (RaaS) group Lockbit 2.0 claimed responsibility for the attack.

South Staffordshire Water (SSW)

In mid-August 2022, the UK water company, SSW, disclosed that it had been the victim of a “criminal cyber-attack” that disrupted its IT network but did not impact its ability to supply clean water to the public. ClOp claimed responsibility for this ICS Cyber Kill Chain Stage attack, which could manipulate process chemicals. This may have been an attempt to exaggerate the attack, cause reputational damage, and encourage them to pay.

DESFA

In August 2022, DESFA, a Greek natural gas company, released an official statement that a cyber attack impacted the availability of certain systems with the possible leakage of several files and data after the ransomware group, Ragnar Locker posted information to their dark web resources. DESFA also stated that their natural gas system operations were not impacted. However, Dragos analyzed network telemetry, examined alleged stolen information, and found occurrences of documents and manuals related to SCADA and PLCs from this ICS Cyber Kill Chain Stage: Stage 1 breach.

Modular Mining

In September 2022, Modular Mining, a large-scale mining technology solutions provider, was possibly impacted by BianLian Ransomware. Consequently, the victim shut down its impacted servers to contain the incident. This compromise could facilitate a supply chain attack and enable an adversary to leverage existing third-party connections into customer environments. Because customer data is on the list of impacted data, the unauthorized acquisition of this data by a third party could facilitate Stage 1 of the ICS Kill Chain through the disclosure of this sensitive technical customer data.

Electrical Infrastructure Ransomware Event

In October 2022, E-ISAC published a bulletin stating that compromised data, including topology information, could “allow a capable adversary to model electricity systems dynamically.” No known outages have been reported from this data extraction; the extent of data compromise and energy sector exposure remains unknown. E-ISAC has confirmed,

however, that the compromised data includes topology information that could “allow a capable adversary to dynamically model electricity systems.”

Mining and Metals and Food & Beverage

In December 2022, Dragos discovered Trickbot infrastructure, and subsequently identified three victims – two mining and metals companies and one food and beverage company – communicating with this threat group infrastructure. Two of these three companies have publicly noted that some aspects of their OT operations were impacted in October and November 2022. Dragos assesses with moderate confidence that cybercrime groups will use Trickbot and similar bots to drop ransomware and impact the operations of mining and metals companies.

Copper Mountain Mining Company (CMMC)

On December 27, 2022, CMMC reported that adversaries targeted their corporate offices with an enterprise IT systems-based ransomware attack. The attack forced CMMC to preventatively shut down the mill at their open pit mine near Princeton, British Columbia, Canada. Dragos has not identified the ransomware group claiming responsibility for the attack but continues to monitor for additional information.

Industrial Ransomware Trends: Moves and Changes

While Conti led in ransomware activity through most of the first two quarters, it shut down its operations in mid-May 2022, two weeks after the U.S. State Department announced a reward for any information about Conti leadership and its affiliates. Conti accounted for 9.6 percent of ransomware incidents targeting industrial organizations and infrastructures in 2022.

A significant new ransomware group called Black Basta was responsible for 9 percent of ransomware incidents, including some of the most major ransomware incidents, such as the May 2022 incident that halted AGCO's operations for weeks.

Several new ransomware groups formed in Q3, including SPARTA BLOG, BIANLIAN, Donuts, ONYX, and YANLUOWANG. To date, Dragos cannot confirm whether these groups have reformed from other dissolved ransomware groups such as Conti.

The Lockbit ransomware group accounted for the largest number of ransomware incidents that targeted industrial organizations and infrastructures in the last year, at 28 percent. Lockbit offers an exfiltration tool along with Lockbit 2.0, Stealbit, which it uses to steal data before executing Lockbit 2.0 ransomware. The adversaries added Lockbit Builder capabilities into their new Lockbit 3.0 strain. Anti-detection mechanisms, anti-debugging, and the ability to disable Windows Defender software are among the features that make Lockbit 3.0 one of the fastest-growing ransomware strains.

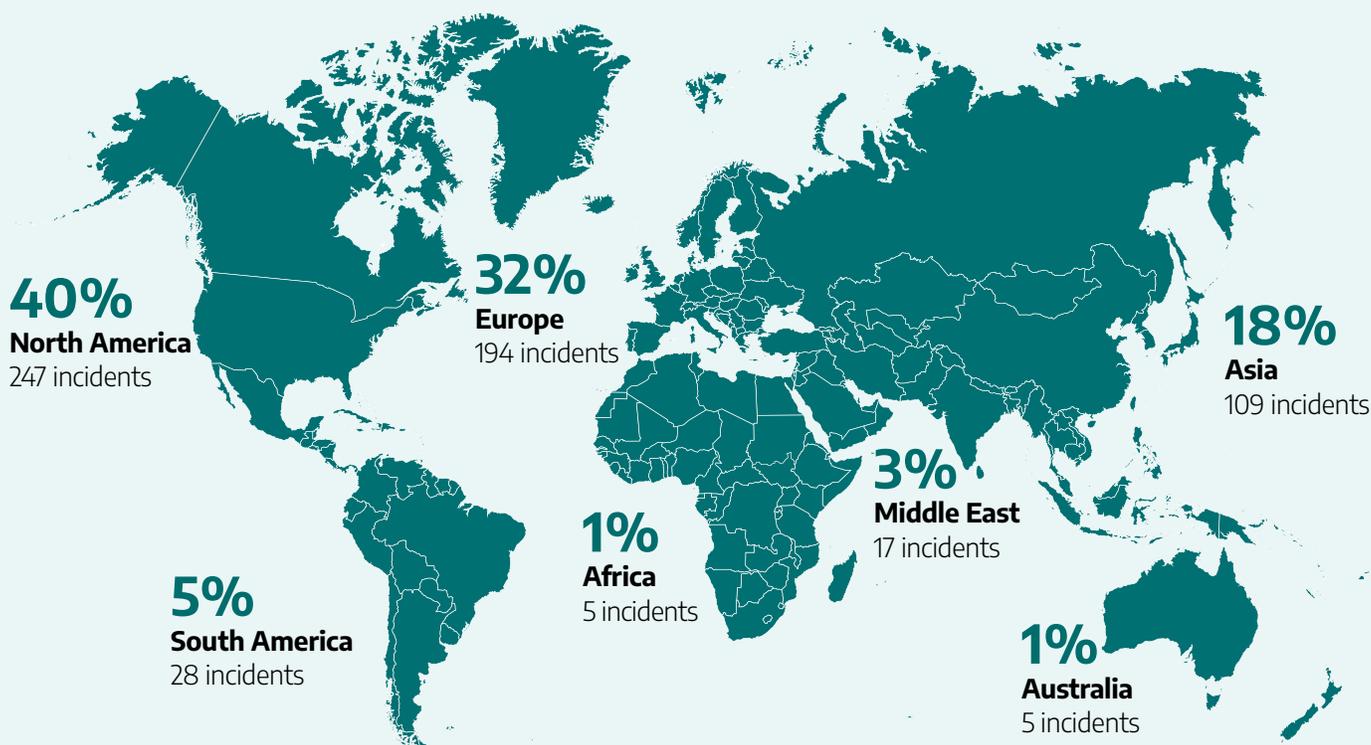
In the third quarter, an unknown adversary claimed they had hacked Lockbit servers and leaked Lockbit 3.0 builder, allowing anyone access to their ransomware creation feature.

Dragos assesses with moderate confidence that Lockbit 3.0 will continue to target industrial organizations and will pose a threat to industrial operations into 2023, whether through the Lockbit gang itself, or others creating their own version of Lockbit ransomware. Lockbit led with the most ransomware activity of all ransomware groups in 2022.

Industrial Ransomware by the Numbers

The breakdowns of ransomware activities for 2022 follow.

FIGURE 3: RANSOMWARE INCIDENTS BY CONTINENT • 2022



Globally, 40 percent of the ransomware attacks targeted industrial organizations and infrastructures in North America, for a total of 247 incidents; Europe is second with 32 percent or 194 incidents; Asia with 18 percent or 109 incidents; South America with 5 percent; the Middle East with 3 percent; Australia and Africa each had 1 percent. North America remains one of the most highly targeted regions by ransomware.

FIGURE 4: RANSOMWARE INCIDENTS BY SECTOR • 2022

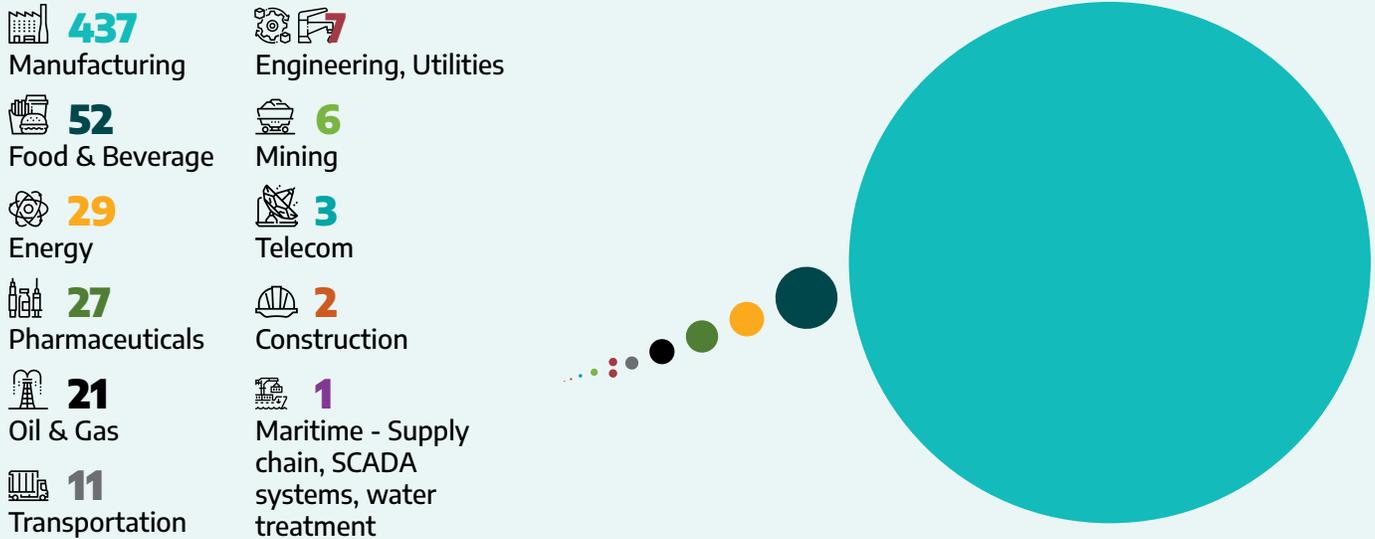
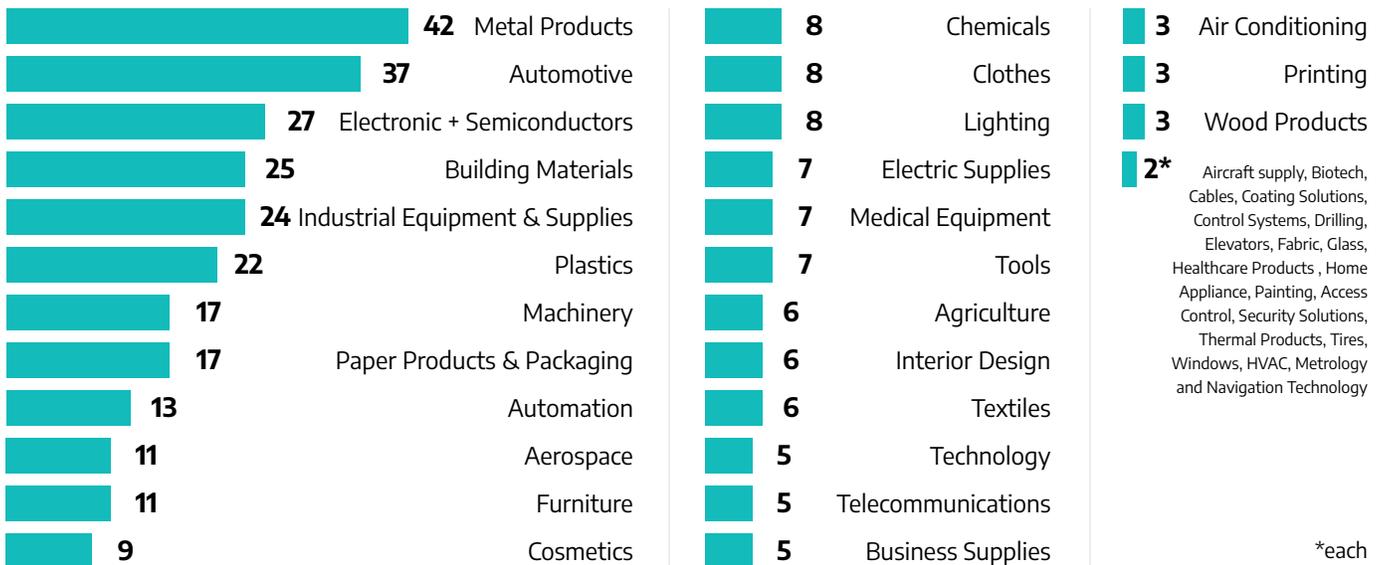


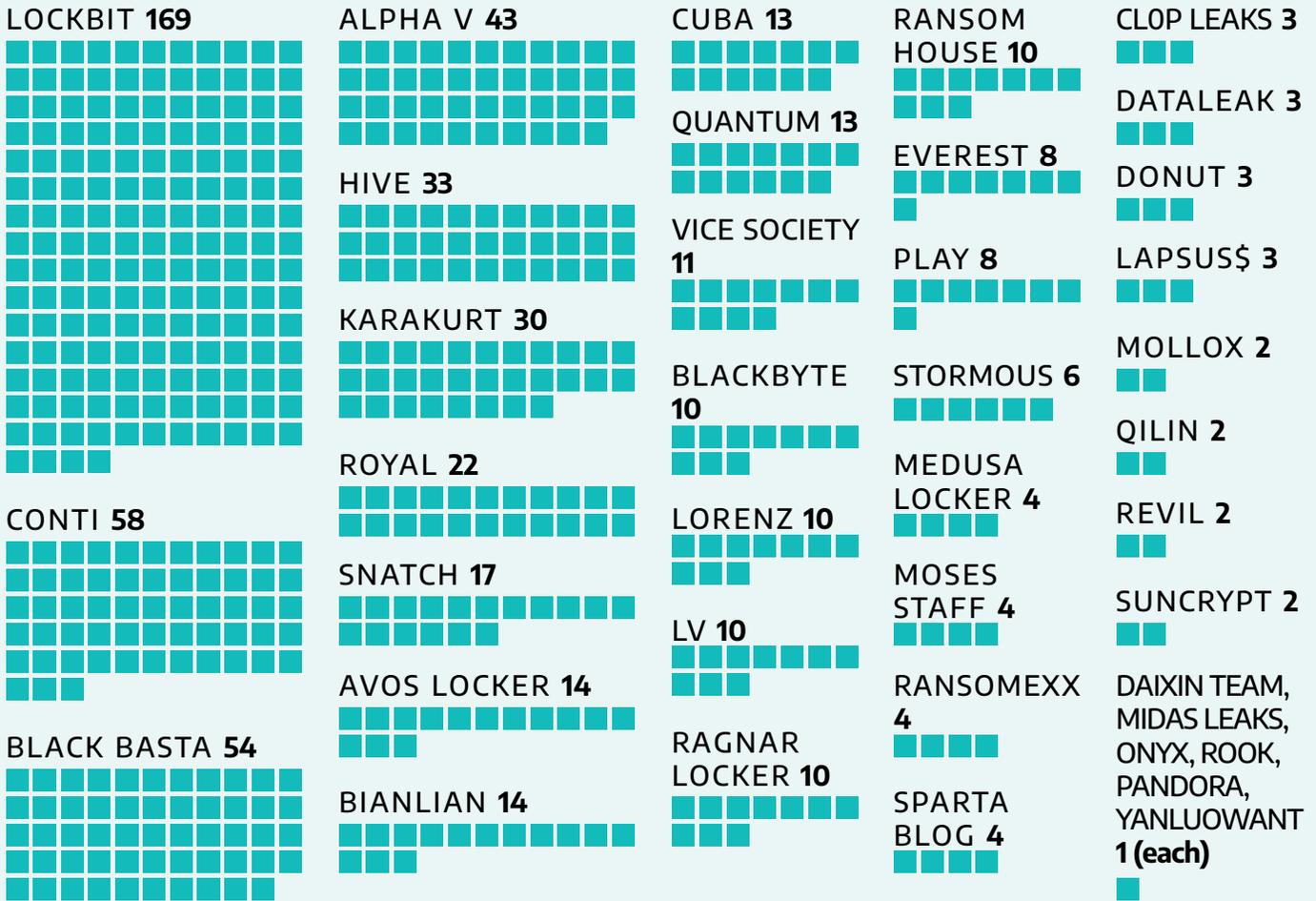
Figure 4 shows that 72 percent of all 2022 ransomware attacks Dragos tracked targeted 437 manufacturing entities in 104 unique manufacturing subsectors. Figure 4 also shows that nine percent of attacks targeted food and beverage; five percent targeted the energy sector; four percent targeted the pharmaceuticals; 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 5: RANSOMWARE BY MANUFACTURING SUBSECTOR



*each

FIGURE 6: RANSOMWARE INCIDENTS BY SECTOR RANSOMWARE GROUP • 2022



Analysis of ransomware data shows that Lockbit 2.0 and Lockbit 3.0 made 28 percent of the total ransomware attacks in 2022; Conti made 10 percent; Black Basta made 9 percent; AlphaV made seven percent; and Hive and Karakurt made five percent of ransomware attacks each. Ransomware attacks against manufacturing entities often impact other sectors that depend on manufacturers in their operations or supply chain, such as aerospace, food and beverage, and automotive organizations.

Ransomware Victimology Trends

Table 2 summarizes the victim sectors and regions that ransomware groups targeted in 2022.

TABLE 2: RANSOMWARE GROUPS AND SECTORS/REGIONS TARGETED

Ransomware Group	Sectors/Regions Targeted
Black Basta	North America and Europe
Cuba	Manufacturing, Energy
DAIXIN TEAM	Asia / Manufacturing
DATALEAK	Manufacturing, Food & Beverage
LAPSUS\$	Telecommunications
LV	Manufacturing, Food & Beverage
Medusalocker	North America and Europe / Manufacturing, Food & Beverage
Midas Leaks	Asia / Manufacturing
Mollox	Manufacturing
Moses Staff	Middle East / Manufacturing
ONYX	North America / Manufacturing
Pandora	Asia / Manufacturing
PLAY	Manufacturing, Food & Beverage
Quantum	Manufacturing, Energy
Ragnar Locker	Manufacturing, Oil & Natural Gas
RANSOMEXX	North America and Europe
Revil	Asia / Manufacturing
Rook	Middle East / Pharmaceuticals
Royal	North America and Europe
Snatch	Manufacturing, Oil & Natural Gas
SPARTA BLOG	Europe / Manufacturing, Energy
Suncrypt	Europe / Manufacturing, Food & Beverage
Vice Society	Manufacturing
YANLUOWANG	North America / Manufacturing

What's Next?

Dragos assesses with high confidence that ransomware will continue to disrupt industrial operations in 2023, whether through the integration of OT kill processes into ransomware strains, flattened networks enabling ransomware to spread into OT environments, or through operators' precautionary shutdowns of OT environments to prevent ransomware from spreading to the OT systems.

Because of the changes in ransomware groups and the leaking of the Lockbit 3.0 Builder, Dragos assesses with moderate confidence that during 2023 more new ransomware groups will appear as either new groups or reformed ones.

Dragos assesses with moderate confidence that ransomware groups will continue to target higher-value, industrial entities. In 2023, cybercriminals will continue to show more interest in vendors and suppliers because of the interconnectivity with their

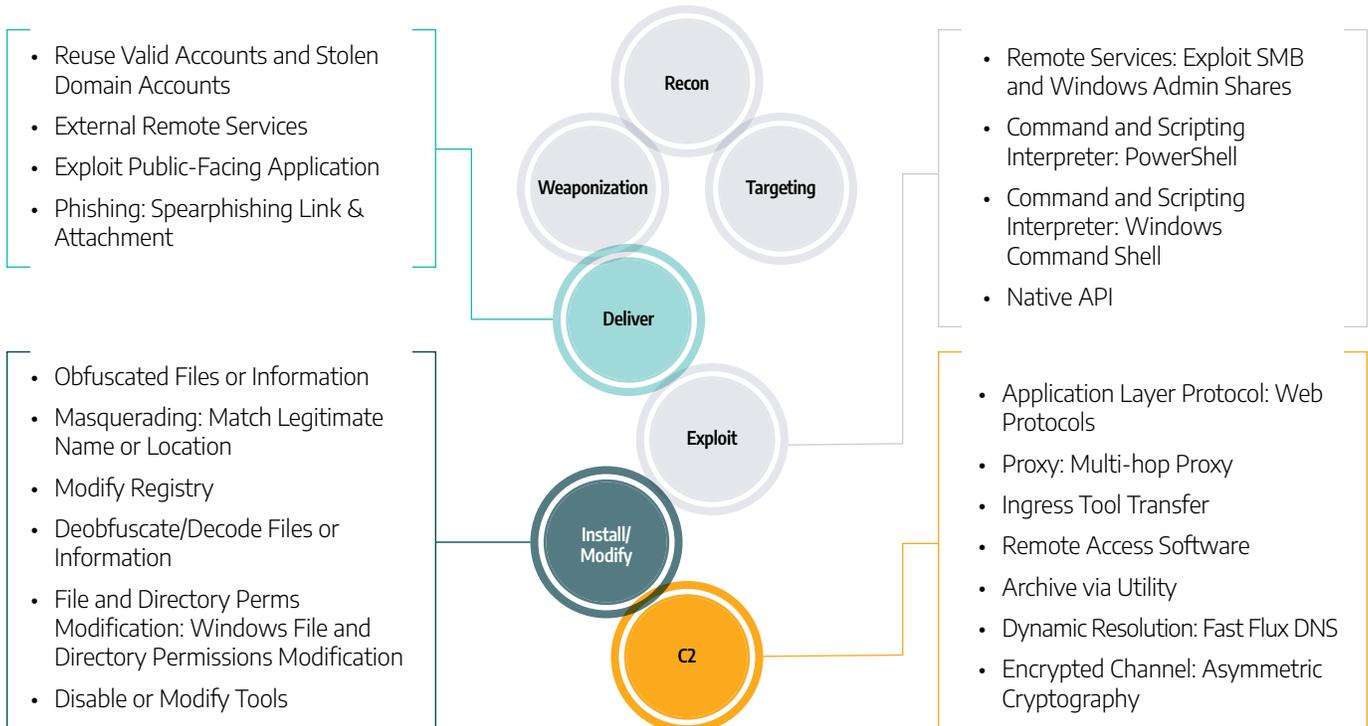
customers downstream. This is largely due to the criticality of operations and their reach into numerous OT environments, which often results in higher or more frequent ransom payouts.

Ransomware Kill Chain

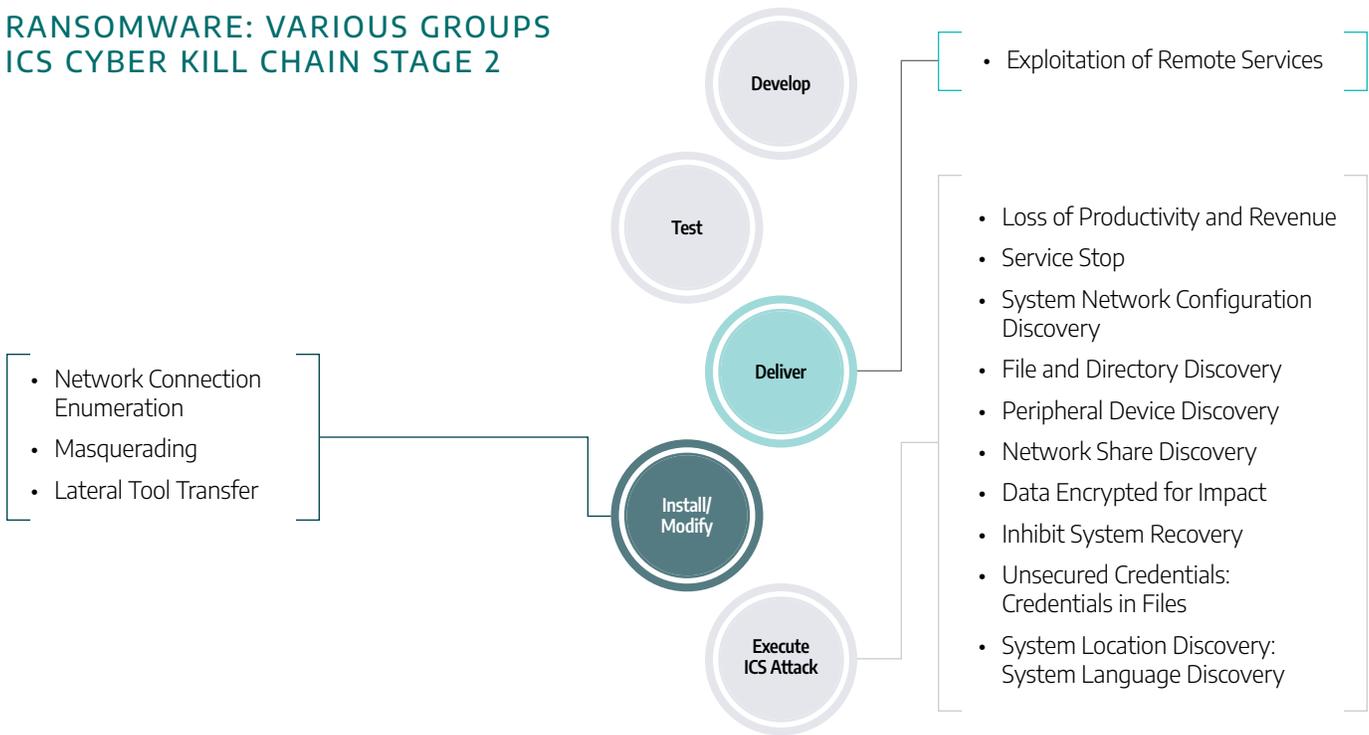
Ransomware has numerous variants, but in most cases, it relies on similar threat behaviors. Dragos has analyzed the most common strains of ransomware utilized by the ransomware groups in Table 2 above and plotted the most recurring TTPs to the ICS Cyber Kill Chain.

Defenders should utilize kill chains as the input for data collection requirements in a collection management framework. Identify the sources of data that can be used to detect the TTPs of an identified threat scenario. The earlier in the kill chain that an attack is detected, the more opportunities and options defenders have to respond and recover before the attack leads to consequences in the industrial process.

RANSOMWARE: VARIOUS GROUPS • ICS CYBER KILL CHAIN STAGE 1



**RANSOMWARE: VARIOUS GROUPS
ICS CYBER KILL CHAIN STAGE 2**



THE RANSOMWARE KILL CHAIN

The Ransomware Kill Chain illustrated above shows a jump from Stage 1 to Stage 2, but is this practical? We looked to our OT Watch fleet to provide insight into the likelihood of this second stage progression and the prevalence of cross-zone communications between enterprise and OT environments. Looking at interesting protocols like RDP and SMB, which are commonly leveraged by ransomware groups for lateral movement and ransomware propagation, the team focused on unique pairs of cross-zone hosts communicating over this gap.

From a broad perspective, looking at this data over a 90-day period, the team identified an average of, per customer, 482 source/destination host pairs communicating using RDP and 1,712 unique source/destination host pairs communicating over SMB.

Digging deeper, the team also identified cross-boundary connections using the same protocols. The team discovered 6.6 percent of these unique RDP host pair connections traversed directly from enterprise to OT zones and 3.6 percent of SMB host pair connections from enterprise to OT. Following the pathway of further ransomware propagation, 40 percent of RDP cross-zone connections existed between OT zones and 21.8 percent for SMB.

In short, what we identified was the potential for an enterprise-side ransomware attack to propagate directly from enterprise into OT networks, and from there, a significant propagation path within the OT network itself. Even if an OT environment is not the intended target, ransomware can often have an opportunistic impact to OT due to these existing cross-zone network communication pathways.



ICS/OT Vulnerabilities

In 2022, the rapid growth in vulnerabilities continued to challenge ICS and OT 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 ICS impacts are identified.

In this section, we discuss some of the most concerning ICS vulnerabilities that Dragos discovered or assessed this year and provide an update on the trends in ICS impacts from Common Vulnerabilities and Exposures (CVE). These vulnerabilities highlight the complex nature of connected and networked components in OT/ICS environments and underscore the fast-growing universe of persistent threats across all Purdue Model layers.



Root Cause Analysis of Password “Cracking” Vulnerabilities

In 2022, Dragos shed light on a slightly different avenue of attacks in ICS—gaining access to the industrial equipment by cracking operator passwords. See the Dragos password “cracking” ecosystem research described in the blog post, “The Story of Troy and the

Password ‘Cracking’ Trojan Horse” and other reports and presentations.^{12,13} Dragos continues to identify other samples and discovered one that embeds approximately 40 exploits targeting a variety of systems and vendors. See Table 3.

TABLE 3: LIST OF TARGETED SYSTEMS AND VENDORS

Vendor	Product Name	System Type
Mitsubishi Electric	GOT 1020	HMI
	GOT1055	HMI
	F920	HMI
	F930, F940	HMI
Weintek	Weintek HMI Project File	Project File
IDECC	HG2F-SS	HMI
Hitech	Project File	Project File

12 The Story of Troy and the Password “Cracking” Trojan Horse – Dragos.com

13 Analysis of PLC Password Cracking Malware - Dragos

TABLE 3: LIST OF TARGETED SYSTEMS AND VENDORS (CONTINUED)

Vendor	Product Name	System Type
OMRON	C200H, HX	PLC
	CPM1A	PLC
	CPM2A*	PLC
	CQM1, CQM1H	PLC
	CJ1M, CS1G	PLC
	CP1E	PLC
	CP1J, CP1L, CP2M	PLC
	Zen	PLC
Mitsubishi	FX0, FX1, FX2, FX2C	PLC
	FX2N, FX2 EPPROM	PLC
	Q02	PLC
Delta Automation	DVP ES, EX, SS, EC	PLC
	DVP SS2, SV, ES2, EH (ID)	PLC
	DVP Project File	Project File
LG	K80S	PLC
	K120S	PLC
Siemens	S7-200 REL 02.00, 02.01	PLC
	S7-200 Project File	Project File
	LOGO 0BA6	PLC
Fatek Automation	FBs	PLC
	FBe	PLC
	FBe-FBs Project File	Project File
Panasonic	NAIS FP0	PLC
	NAIS FPG	PLC
Allen Bradley	ML1000	PLC
Vigor	VB Series	PLC
Fuji Electric	NB Series	PLC
Pro-Face	GP Series	HMI
	GP Project File	Project File
Fuji-Hakko	UG Series	HMI
	V7, V8	HMI
	Fuji-Hakko Project File	Project File

Dragos performed root cause analysis on three password retrieval and modification vulnerabilities to understand how the exploits worked and what mechanisms were being abused. Root cause analysis highlights shared security issues between vendors, specifically, the lack of secure password protection mechanisms. Dragos modified the serial exploits to demonstrate they could be leveraged over the network, increasing the severity of the vulnerabilities and then responsibly disclosed them to the vendors.

Let's examine the two primary root causes that lead to these vulnerabilities.

Root-Cause #1: Protocols Lacking Authentication on Critical Functions

Each vulnerability could be mitigated with proper access controls in place. For example, an adversary could directly read two of the three vulnerabilities stored in the password in a PLC memory region without any authentication. The third vulnerability correctly disallowed unauthenticated read requests, but allowed unauthenticated write requests, so an adversary could simply overwrite the password with arbitrary values. Further, since there was no filtering of the values to be overwritten, an adversary could overwrite the password with non-ASCII values, which are values that do not map to keyboard characters, and which could prevent an engineer from connecting to the programmable logic controller (PLC). This would not impact the PLCs ability to run but would block an engineer from connecting to and retrieving data from the PLC, creating a Loss of Control condition.

Root-Cause #2: Undocumented Protocol Commands

Two of the three exploits contained special privilege commands that were not documented in the protocol specification. Analysis indicates that they allow an unauthenticated user to obtain critical information, including retrieving the password, from the PLC.



For example, Dragos researchers reverse engineered binaries bundled with the PLCs programming software and discovered hundreds of undocumented commands in Mitsubishi Electric's SLMP protocol. Dragos suspects many industrial protocols contain undocumented commands that an adversary could leverage to impact operations if discovered.

Conclusion

The vulnerabilities embedded in the password "cracking" sample are simple and can be easily discovered. The protocols leveraged by the exploits lack basic access controls and could be considered insecure by design. Further, just because some protocol commands are undocumented does not mean an adversary cannot find them.

These issues are shared across multiple vendors and product lines. Identifying and drawing attention to them helps push the industry in the right direction. Baking authentication into the protocol and removing unnecessary and overly privileged commands from the protocol will mitigate these issues. Vendors should be aware of this and should prioritize mitigations to help reduce vulnerability exposure.



OT:ICEFALL and the Importance of Public Reporting

OT:ICEFALL is a group of 56 vulnerabilities across 13 product lines' hardware and software, which were disclosed in 2022 in the OT:ICEFALL report.¹⁴ Vulnerabilities ranged from specific products and protocols to generic third-party products that may themselves be used in industrial devices from many vendors.

The commonality between the disclosures is really just 'security and design flaws in many products related to process automation.' Many of these flaws, being design flaws, are not issues that can be 'patched' by the vendor. Fixing the underlying problem requires simultaneously changing both product firmware and configuration/programming software. This is because the insecurity of the system requires changes to both ends of the communication. These updates themselves introduce risk to end users, who must ensure that all systems are updated simultaneously, or

else some subset of workstations and devices will be left unable to communicate with one another.

Dragos researchers privately reported some issues from the ICEFALL dataset to affected vendors years prior to their public disclosure in the ICEFALL report. As such, the Dragos Platform and vulnerability management system already had detections for vulnerable ICEFALL systems, along with practical mitigation steps for protecting vulnerable devices.

In addition to augmenting the OT:ICEFALL vulnerability set in the Dragos vulnerability data, Dragos also publicly disclosed its own set of vulnerabilities in 2022. Although Dragos does not market its vulnerabilities with names and logos, it does publish information about its own research at dragos.com/advisories. Advisories in 2022 bear many similarities to the OT:ICEFALL dataset, including

issues in PLCs, VPN appliances, serial converters, cellular gateways, engineering workstation software packages, and industrial radios.

The best possible output from any public vulnerability disclosure is information on contextual severity and remediation information. Most of these vulnerabilities will not end up exposed to attackers in a well secured industrial plant. Nor will many security patches be immediately applied. As such, advisories from Dragos are more often given lower risk ratings except in unusual circumstances. Those circumstances include software packages or appliances specifically aimed at sharing information across trust boundaries or in safety critical systems or other operations controls where public proof of concept code exists. In addition, Dragos' customer vulnerability database provides remediation actions beyond patching – such as listing specific port numbers to block, as well as Platform detections and rules used to identify the use of these vulnerabilities on your network.

Mitigations for OT:ICEFALL

The best advice for defenders is to treat all embedded industrial products as insecure – in other words,

assume that a malicious actor with network access to the device may permanently alter the behavior of the device. Pay particular attention to embedded industrial products associated with the “crown jewels” in your plant and limit the network connectivity to those devices appropriately.

Typically, only a few servers and workstations need to communicate with embedded controllers – usually a Human-Machine Interface (HMI) or open platform communications (OPC) server and an engineering workstation (EWS). Monitor the traffic to and from these controllers for new network protocols, and new commands being used, and identify when changes to program logic or other control settings are changed.

Dragos Platform customers may also monitor their network for “Phoenix Contact PLC Program Write Detection,” particularly if the detection is triggered by new workstations, non-engineering workstations, or outside of normal work hours. This detection has been a part of the Dragos Platform since 2020. Dragos continues to incorporate detection analytics for other vulnerabilities in the OT:ICEFALL report, as well as other public reporting.



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 OT vulnerabilities that will continue to threaten industrial organizations for years to come.

Many Advisories Contained Errors and Lacked Patches and Actionable Guidance

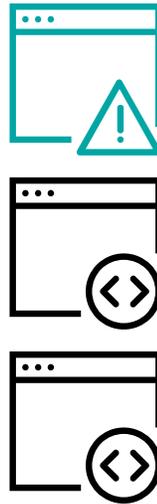
A full 34 percent of the advisories that Dragos analyzed in 2022 contained errors, and 14.9 percent of their CVEs had errors in the Common Vulnerability Scoring System (CVSS) scores associated with them.

As shown in Figure 7, 30 percent of the advisories that Dragos analyzed during 2022 had no patch, and 77 percent contained no mitigation from a vendor or other CNA. Vendors often do not provide mitigations for asset owners and operators if they cannot patch the identified vulnerability.

In 2022, 68 percent of all the advisories that Dragos analyzed were published without vendor mitigations, down from 91 percent in 2021. This means there was no practical advice for industrial cyber security professionals from vendors on how to mitigate the risks associated with these advisories.

This advice is critical for network defenders if they are unable to apply any available patches or if no patch was provided. Thirty percent of all advisories analyzed had no patch when announced. Dragos provided mitigations for the 53 percent of advisories that contained no mitigation from either vendors or ICS-CERT.

During this period, we found that nine percent of the advisories we analyzed had no alternative mitigation, up from seven percent last year. ICS-CERT within CISA provides alternate mitigations in some advisories where it can in an attempt to mitigate situations where no patch is available from a vendor or where industrial organizations find that patching is not feasible or is too expensive from an operational standpoint.



One Third of Advisories Contained Errors in 2022

FIGURE 7: ADVISORIES WITH ERRORS AND LACKING IN ACTIONABLE GUIDANCE

Advisories with no patch when announced

30%

Advisories that had a patch

70%

Advisories that had no mitigation at all

77%

Advisories with no vendor mitigation

68%

Advisories with no alternate mitigation

91%

Advisories with a patch and no mitigation

51%

Advisories with no patch and no mitigation

16%

Advisories for which Dragos provided missing mitigation advice

53%

Fifty-one percent of the advisories with a patch in 2022 had no other mitigation, down from 64 percent last year. With no other mitigation provided, defenders have no choice but to use the patch that is released or to leave their networks wholly unprotected.

Sixteen percent of the advisories without a patch had no mitigation, down from 19 percent last year. This shows a three percent improvement, trending in the right direction. If industrial organizations do not have a patch or mitigations that they can apply, they have little to no protection against the exploitation of these vulnerabilities.

Over the years, the growth in mitigations shows that vendors and ICS-CERTs are getting better at generating mitigations. This shows significant improvement over where we started ten years ago. Vendors are getting better at including ports and file extensions, and although they are not fully mitigating themselves, they are on the right path.

ICS Impact: Loss of View, Loss of Control, or Both

There is no worse operations scenario for industrial asset owners and operators than a possible loss of control or loss of view in an ICS environment. Under these conditions, data continues to flow, and the systems continue to operate, but they are no longer operating as designed, and the operator is typically unaware of the issue.

In 2022, 50 percent of the advisories Dragos analyzed could cause both a loss of view and loss of control in an OT system, up from 35 percent last year. This percentage is much smaller when looking at the loss of one or the other as shown in Figure 8. The uptick in this advisory category stems partly from researchers who are increasingly targeting hardware that is impacted in this way.

FIGURE 8: LOSS OF VIEW, LOSS OF CONTROL, OR BOTH



Where Do Vulnerabilities Reside?

Of the vulnerabilities that Dragos analyzed in 2022, 83 percent resided deep within the ICS network, an increase of four percent. Deep within the network applies to equipment on Levels 0 to 3 of the Purdue Model and includes engineering workstations, PLCs, sensors, and industrial controllers.

The lower the level of exploit in the Purdue Model, the more likely that adversaries will need access to an OT network to exploit it, making it more challenging. Exploitation requires that adversaries have an initial access strategy in place, which can take time and effort to develop or it requires collaboration with an initial access broker.

Implementing proper network segmentation can help mitigate these vulnerabilities, especially when combined with multi-factor authentication (MFA) for remote sessions.

All of the advisories we examined had a Purdue Model level associated with them, while nine percent were in ICS-specific files or protocols, showing a six percent increase over last year. Sixty-three percent were in engineering workstations and operations software, a seven percent increase over last year.

Sixty-three percent of the vulnerabilities Dragos analyzed were at Purdue levels 3 and 2, a seven percent increase over last year, which shows an increased research interest in systems as those levels.

Fifteen percent of the advisories that Dragos analyzed applied to products within the enterprise bordering the internet at Purdue Level 3.5, 4, or 5, a decrease of four percent over last year. This can include networking communication equipment, VPNs, data historians, remote desktop software, or firewalls commonly deployed in the demilitarized zone or enterprise networks.

FIGURE 9: WHERE DO VULNERABILITIES RESIDE?

Advisories ‘deep within’ control network

83%

Advisories at Purdue levels 3 and 2 control network

63%

Advisories that impact the border

15%

Advisories with medium border likelihood: 0 percent

0%

Advisories that had no Purdue level

0%

Vulnerabilities in ICS-specific files or protocols

9%

Vulnerabilities pertaining to Engineering Workstation & Operation software

63%

Errors in Vulnerability Severity Scores

In addition to the lack of actionable information in most ICS-related vulnerability advisories, many advisories and individual vulnerabilities contained errors that could inadvertently mislead practitioners who use CVSS scores to triage for mitigation or patching. These errors could cause asset owners and operators to dedicate more resources to fixing the vulnerabilities that represent a lower level of risk in their ICS environment over those that might represent a higher level of risk.

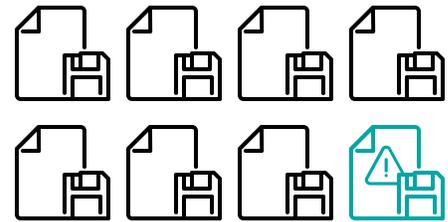
CVEs are scored using the Common Vulnerability Scoring System (CVSS), an open industry standard for assessing the severity of computer system security vulnerabilities developed by the National Infrastructure Advisory Council (NIAC). CVSS scores are calculated for each CVE based on a formula that depends on several metrics that approximate the ease of exploit and the impact of exploit. Scores range from 0 to 10, with 10 the most severe. The CVSS was designed for enterprise IT systems but can also apply to ICS/OT environments.

Dragos defines the most critical vulnerabilities as vulnerabilities that are network-exploitable, perimeter-facing, and capable of having a severe ICS impact. In 2022, Dragos found that 13 percent of advisories were extremely critical, an increase of .5 percent over last year.

Dragos provides corrected CVSS scores based on how an adversary could leverage a vulnerability in an ICS environment. The corrected information allows practitioners to prioritize the CVEs that carry the most risk for their environments so they can focus their resources on the most severe issues first.

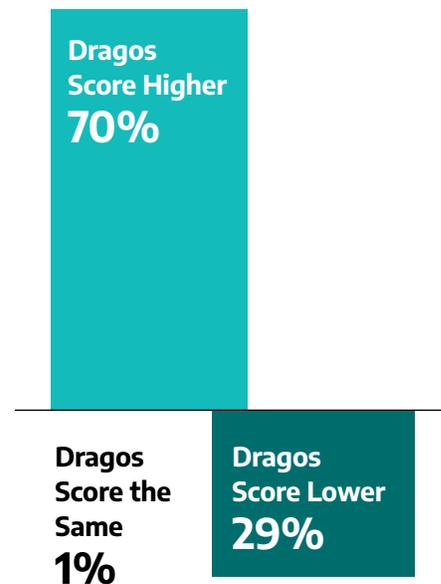
However, CVSS scores can be misleading and often do not accurately capture all the risks of a particular vulnerability. ICS security professionals should not use them as the sole factor in prioritizing vulnerabilities.

Of all the CVEs that Dragos analyzed in 2022, Dragos gave a higher severity score to 70 percent of CVEs than they had received at publication. Dragos gave a lower severity score to 29 percent of CVEs. Only 1 percent of scores remained the same.



1 in 8 advisories (13%) were extremely critical in 2022

FIGURE 10: CVE SECURITY SCORES THAT DRAGOS CORRECTED



and if they were implemented to play a key role in their process. These vulnerabilities typically do not directly impact OT operations, but they have the potential to do so based on their implementation in the customer environment.

Next vulnerabilities pose a greater threat for asset owners and operators who do not have proper network segmentation or who have networks that are accessible from the internet. Asset owners and operators can mitigate these vulnerabilities simply by updating firewall rules. It is important that defenders conduct a firewall rule audit regularly and justify every allow rule.

Vulnerabilities in the **Never** category pose a possible threat but rarely require action or prioritization. In 2022, 30 percent of priorities fell into this category, an 11 percent decrease over 2021. These vulnerabilities typically are not associated with any impact to OT processes, are difficult to leverage, and often do not increase the inherent vulnerability of the product.

It is more beneficial for an organization to monitor its environment for signs of exploitation rather than taking devices and services offline to patch or taking appropriate mitigation measures. Although considered **Never** vulnerabilities, Dragos does not recommend ignoring them entirely if time and resources permit. Patching ICS technologies can be more complex than patching most enterprise IT network technologies, and the value presented from patching this group of vulnerabilities can be minimal. Asset owners and operators should conduct risk assessments to determine if it is safe to continue operations without addressing the identified vulnerabilities.

The Dragos platform provides visibility into these **Now, Next, Never** categories and recommends actions that align with each of these categories.

Mitigating Vulnerabilities in 2022

With security concerns growing and controls mandated in some industries, the benefits from the level of effort spent on one security control over another are not always clear. 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.

While it is a positive action when a firmware or software patch is released with an advisory, end users in industrial environments may still hesitate to apply it. Patches are often synonymous with downtime, and there are many documented cases where patching has caused issues or plant failures.

NOW: Requires immediate action

2%

NOW

NEXT:
Limited threat vulnerabilities

68%

NEVER: Possible threat (monitor)

30%

In a best-case scenario, applying a patch requires restarting the software. This can be challenging for a plant that operates 24/7. Even if a plant or manufacturing facility runs a regular business workday, patching at any time introduces the risk of failure. If the application of a new patch fails, the system may need to be re-installed or even restored from a backup. This takes time, and production may come to a halt.

Other alternate, less disruptive mitigations can be as simple as restricting the port numbers for network-exposed vulnerable services. For example, a firewall can restrict access to the affected service, reducing risk until a patch can be applied. Other mitigations include

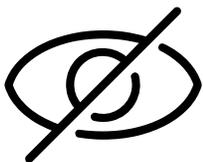
implementing configuration changes that disable a vulnerable feature. For example, file extensions make it possible to monitor inbound email attachments, web proxy servers, and file change permissions without affecting the program functionality, or network monitoring for exploitation of the vulnerabilities.

Vulnerability reporting in the ICS 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.

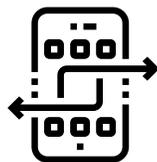


Dragos Frontline Perspective

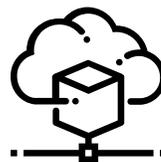
For the last six years, Dragos has leveraged our Professional Services team to develop an on-the-ground understanding of the realities facing the industrial community and to bring back insights and lessons learned from the field. In 2019, Dragos identified four key findings that we continue to track year over year:



Limited or No OT
Network Visibility



Poor Security Perimeters



External Connections to
OT Environments



Lack of Separate IT and
OT User Management



Key Findings Overview

Methodology

Dragos considers limited visibility to be only monitoring the IT to OT boundary, and not the activity inside the OT network. Full visibility is achieved when network and device logs are centralized and can correlate various segments with network traffic analysis and asset inventories. Dragos considers findings to be related to poor security perimeters if they involve issues such as porous firewall rules, network boundary bypasses, or flat networks. Poor security perimeters also include instances where the only segmentation is the initial firewall between the IT-OT boundary and when there are unnecessary communication pathways to critical assets within the network. An external connection is defined as any internet protocol (IP) and/or asset that communicates beyond a pre-defined security perimeter. This definition also extends to communication that originates from a location that is remote and outside of the company's

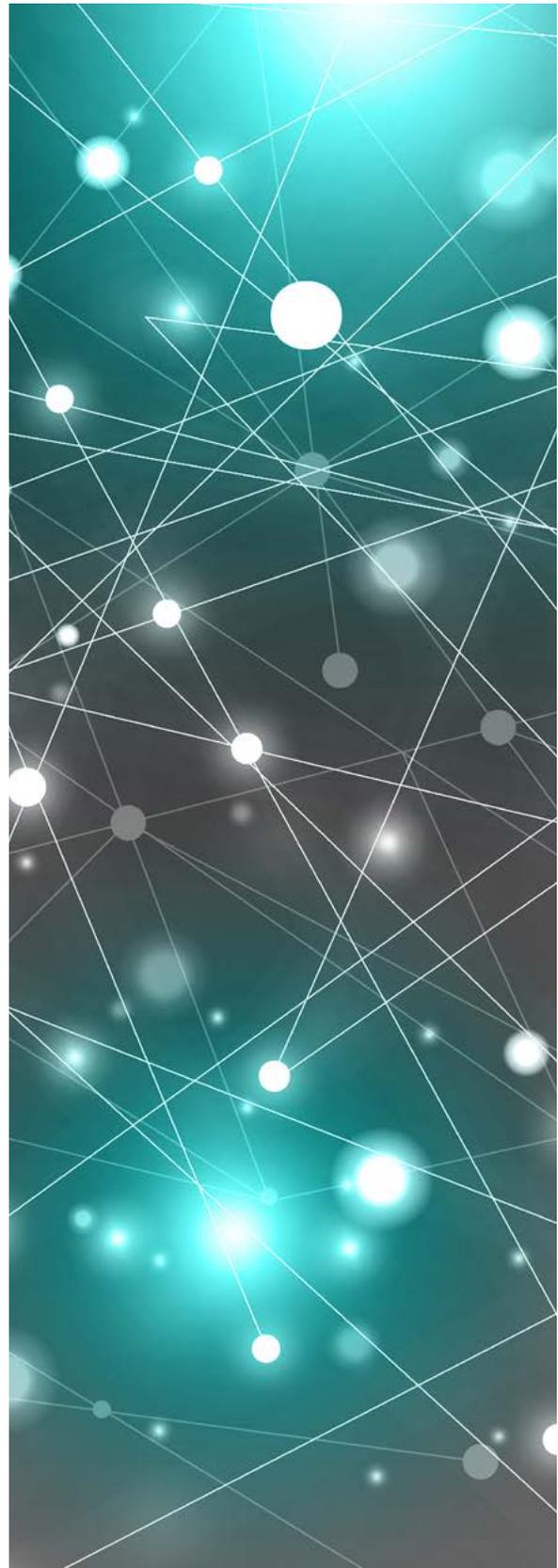
boundaries – such as in the case of third-party connections (3PC). Lack of separate IT and OT User Management refers to when accounts are shared or utilized in both the IT and OT networks; this includes default accounts and vendor accounts.

Dataset

The dataset includes the following service engagement types: architecture reviews, compromise assessments, device penetration tests, incident response, maturity assessments, network penetration tests, network vulnerability assessments, tabletop exercises, and threat hunts. These engagements were conducted in the following OT industry verticals: chemical, datacenters, food and beverage, electric, metals and mining, nuclear, oil and gas, pharmaceutical, renewables, transportation, water and wastewater, and manufacturing.

Each entry in the dataset is one engagement, but that engagement can and often does include multiple sites. Some categories are subsets of others, but all are only counted once per industry breakout and in the overall percentage. For example, food and beverage and pharmaceutical are included in the manufacturing category with other types of manufacturing that are not called out specifically. The dataset for electric consists of engagements in transmission, distribution, and generation (including nuclear and renewables). The oil and gas dataset includes upstream, midstream, downstream, pipelines, liquified natural gas, and offshore facilities. The transportation dataset includes rail, shipping, and airlines and airports. For each key finding:

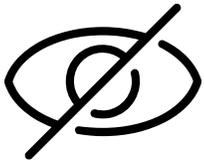
- We have provided breakouts by OT industry where we assess with medium to high confidence that the sample size is representative of the industry as a whole.
- The other category combines assessments where we have significant data, but if broken down by industry may misrepresent that industry
- Other includes food and beverage, pharmaceutical, datacenters, transportation, nuclear, mining and metals, and renewables.



2022 Key Findings

KEY FINDING #1

Limited or No OT Network Visibility



Visibility is the starting point for robust cybersecurity programs, which evolves into metrics to develop more mature and secure environments. Visibility comes

in various forms from asset visibility to data flow inspection, but it can be summarized as anything that increases the defender's knowledge of their own environment. It often starts with asset inventory but must also include network monitoring and device logs. Dragos considers only monitoring the IT to OT boundary, and not the activity inside the OT network, to be limited visibility. Similarly, monitoring OT communication flows without proper OT protocol dissection leaves defenders blind to the context needed to analyze critical network traffic. Full visibility is achieved when network and device logs are centralized and can correlate various segments with network traffic analysis and asset inventories.

FIGURE 11: DURING 2022, DRAGOS UNCOVERED THAT 80% OF ITS SERVICES CUSTOMERS HAD LIMITED TO NO VISIBILITY INTO THEIR ICS ENVIRONMENT.



Visibility is critical for network security and facilitates the prioritization of future improvements. In 2022, 80 percent of Dragos services engagements included a finding associated with limited or no OT visibility. This represents a six percent drop from 2021 and a 10 percent drop from 2020. In 2022, at least 60 percent of customers in all verticals had findings related to OT network visibility and as a result increasing OT network visibility remains the most common recommendation from Dragos. However, the overall visibility of OT networks is definitively getting better every year. The split of engagements with no OT network visibility findings versus just limited visibility is now heavily skewed towards limited. Dragos expects this trend to continue as the industry continues to take large steps forward in the cybersecurity maturity journey. It should be noted that engagements without a visibility finding infrequently occur, but when they do, they are always directly correlated to clients further along in the OT cybersecurity maturity journey.

Table 4 shows this key finding further broken down by OT vertical. It is a comparison with the prior year.

The first column is the industry vertical, and the second column shows the percentage of service engagements that included a finding of limited or no OT visibility in 2021. The third column is the same metric for 2022 engagements and the last column is the delta between 2021 and 2022. For this table, the higher the percentage, the more prevalent the limited OT visibility finding was for that OT industry vertical. In 2022, the chemical industry made noteworthy progress in this area as shown with its 38 percent decrease. Most verticals remained consistent since this metric tracks both limited and no OT visibility.

Visibility is related to three of the five critical controls for ICS cybersecurity identified by the SANS Institute, specifically: a defensible architecture, ICS network visibility and monitoring, and risk-based vulnerability management.

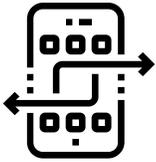
The correlation between ICS network visibility and monitoring is obvious, but visibility also provides an increased understanding of the network and network components, which is a crucial aspect of a defensible architecture and vulnerability management.

TABLE 4: PERCENTAGE OF NETWORK VISIBILITY ISSUES BY OT VERTICAL

Industry	2021 Average	2022 Average	% Change
Chemical	100%	62%	-38
Electric	85%	86%	+1
Manufacturing	90%	89%	-1
Oil & Gas	83%	76%	-7
Water & Wastewater	100%	100%	0
Other	91%	82%	-9
All	86%	80%	-6

KEY FINDING #2

Poor Security Perimeters

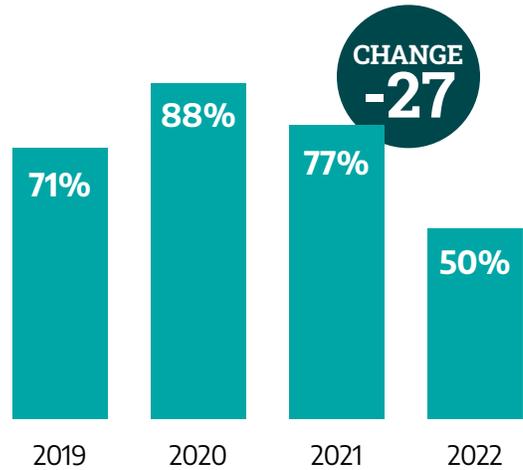


Network security boundaries are perhaps the most common technical security control across any industry and have been for decades. As such, nearly every service engagement that Dragos

executes involves evaluating the effectiveness of network segmentation. Dragos considered findings to be related to poor security perimeters if they involve issues such as porous firewall rules, network boundary bypasses, or flat networks. This includes instances where the only segmentation is the initial firewall between the IT-OT boundary and when there are unnecessary communication pathways to critical assets within the network.

A flat network is problematic for several reasons. Flat networks often combine assets that should be separated into their own networks such as VoIP phones and IP cameras. These readily accessible

FIGURE 12: IN 2022, 50% OF DRAGOS SERVICES ENGAGEMENTS IDENTIFIED ISSUES WITH NETWORK SEGMENTATION.



assets may use vulnerable protocols, which are easily compromised. Additionally, once an adversary gets initial access, a flat network allows access to the entire network and any connected assets. This is especially true of ICS/OT networks as the assets they connect may lack the traditional security controls found on a corporate/IT network. While 50 percent may seem like an alarming number of engagements with network architecture issues, this is a significant decrease from 2021 for a continued downward trend over the last two years.

Table 5 shows this key finding further broken down by OT vertical as well as its comparison with 2021. The first column is the industry vertical, and the second column shows the percentage of service engagements that included a finding related to network segmentation issues in 2021. The third column is the same metric for 2022 engagements, and the last column is the delta between 2021 and 2022. For this table, the higher the percentage, the more prevalent the issues with network segmentation were for that OT industry vertical. The 39 percent fluctuation in

the oil and gas vertical is likely correlated to the implementation of the TSA Security Directives released in response to the ransomware attack on Colonial Pipeline. Identifying IT/OT interdependencies and applying strong network segmentation were major aspects of the security directives. Conversely, the 75 percent shift in the water industry is not from a new regulator but is a combination of improvements made in the wake of the Oldsmar attack.

Poor security perimeters are directly related to proper segmentation, a requirement for a defensible architecture, one of the five critical controls for ICS cybersecurity identified by the SANS Institute. Additionally, the ability to perform risk-based vulnerability management, the fifth ICS cybersecurity critical control, is diminished when defenders cannot rely on a defensible architecture. Isolation limits vulnerable assets from direct external attacks and allows defenders more opportunities to contain attacks before they reach the crown jewels.

TABLE 5: POOR SECURITY PERIMETERS BY OT INDUSTRY

Industry	2021 Average	2022 Average	% Change
Chemical	100%	33%	-67
Electric	55%	48%	-7
Manufacturing	90%	82%	-8
Oil & Gas	75%	36%	-39
Water & Wastewater	100%	25%	-75
Other	86%	66%	-20
All	77%	51%	-26

KEY FINDING #3

External Connections to OT Environments



An external connection is defined as any internet protocol (IP) and/or asset that communicates beyond a pre-defined security perimeter. The ICS environment security parameters consist of implemented levels or

zones for network architecture and segmentation that typically follow the Purdue Model. External access can be described as any user communicating from outside the security perimeter of a zone. This definition can also extend to communication that originates from a location that is remote and outside of the company’s boundaries – such as in the case of third-party connections (3PC). In many cases, external connectivity is required to facilitate remote work by employees, integrators, original equipment manufacturers, and other vendors and partners. However, the use of out-of-band devices (modems, LTE, 5G, landlines, etc.) to facilitate remote access bypasses the normal network flow enforcement mechanisms within the defensive architecture. This results in many of these external connections not being controlled or monitored appropriately.

Similarly, many OT environments are believed to be fully segmented and even appear so on their network diagrams. However, in most cases, when analyzed with the Dragos Platform, external connections are identified. In 2022, findings related to undocumented or uncontrolled external connections to OT environments dropped significantly from 70 percent to 53 percent. The year of 2022 marks a trend reversal, because in 2021, external connections doubled from 2020 due to the high demand for remote access in the wake of the COVID-19 Pandemic. While a 17 percent improvement, 53 percent is still a concerningly high number of uncontrolled external connections to OT environments.

Table 6 shows this key finding broken out by OT vertical as well as a comparison from 2021. The first column is the industry vertical, and the second column shows the percentage of service engagements that identified

FIGURE 13: IN 2022, EXTERNAL CONNECTIONS TO OT DROPPED SIGNIFICANTLY FROM 70% TO 53%.

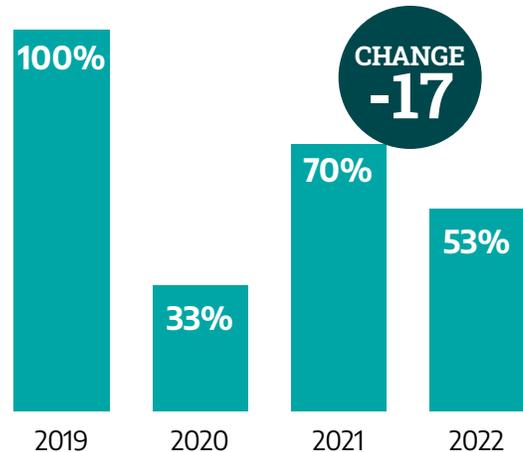


FIGURE 14: WHY MFA?



The most effective security control for reducing the cyber risks associated with remote access remains multi-factor authentication (MFA). It is not feasible to implement MFA everywhere for every situation. The top three Dragos recommendations for secure remote access are:

- Limit the number of different remote access vendors, products, solutions in an environment (a recent hunt found most had nine different solutions).
- Avoid always active remote connections; instead implement them as available upon request and then utilize monitoring to ensure they are only used when authorized.
- Ensure the ability to rapidly disconnect external connections; this is essential for effective incident response.

TABLE 6: EXTERNAL CONNECTIVITY BY OT INDUSTRY

Industry	2021 Average	2022 Average	% Change
Chemical	80%	33%	-47
Electric	60%	38%	-22
Manufacturing	80%	82%	+2
Oil & Gas	77%	31%	-46
Water & Wastewater	75%	83%	+8
Other	86%	66%	-20
All	70%	53%	-17

undocumented or uncontrolled external connections to OT environments in 2021. The third column is the same metric for 2022 engagements and the last column is the delta between 2021 and 2022. For this table, the higher the percentage, the more prevalent the undocumented or uncontrolled external connections were for that OT industry vertical.

Note the 46 percent change in the oil and gas vertical is again likely correlated to the implementation of the TSA Security Directives. This is a momentous shift and should be considered a validation of the hard work the oil and gas industry has performed since the release of the security directives. In many Cybersecurity Architecture Design Reviews (CADRs), the operators had OT visibility at the control center but little to none at the terminals or pump stations. Obtaining network packet captures in these low visibility areas was challenging as they were often in remote areas and geographically dispersed. However, 30 percent

of the time, it led to the identification of unknown or uncontrolled external connections to these critical systems.

The electric industry also saw a substantial positive change, with a drop of 22 percent, related to uncontrolled external connections. However, there is a compelling disparity within the electric industry between traditional electric and renewables. In general, renewables have a much lower cybersecurity maturity than traditional electric generation, transmission, and distribution. Evidence of this is in our finding that 75 percent of renewables have uncontrolled external connections to OT, which is the case for only 38 percent of electric as a whole. This sizable difference between renewables, a subset of electric and electric as a whole, is not surprising due to the differences in how they are staffed. Renewables rely more on remote connections as they are typically unstaffed, minimally staffed, or even operated by a third-party.

KEY FINDING #4

Lacked Separate IT and OT User Management

Dragos considers shared credentials to be accounts that are utilized in both the IT and OT networks, including default accounts and vendor accounts. Leveraging valid accounts for lateral movement is a technique used by nearly all adversaries, even those not focused on OT and ICS. ICS adversaries seek to discover and compromise these shared accounts because they are frequently used to access critical industrial systems and can enable them to pivot from corporate IT networks to ICS/OT environments. When identifying any control system devices, workstations, servers, or applications, an adversary would likely attempt to leverage a manufacturer or supplier set of default credentials. These credentials are easily found in vendor documentation and online repositories available on the Internet. While the intention of creating these credentials is for the initial configuration and deployment of the devices, the default accounts commonly have administrative permissions. These types of permissions, if leveraged by an adversary, would allow them to make unauthorized changes to the devices or applications, causing an event that will likely vary in terms of consequences depending on the environment or vertical the change is being made in.

In 2022, 54 percent of Dragos services engagements included findings related to shared credentials. This is a 10 percent increase from last year, but zero percent change when compared to the last four years. From that longer

FIGURE 15: IN 2022, 54% OF DRAGOS SERVICES ENGAGEMENTS INCLUDED FINDINGS RELATED TO SHARED CREDENTIALS.

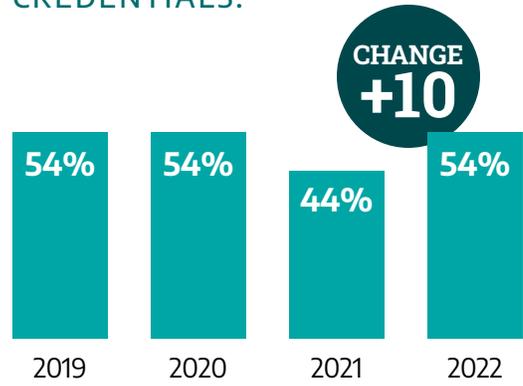


TABLE 7: 3 LACK OF SEPARATE IT & OT USER MANAGEMENT BY OT INDUSTRY

Industry	2021 Average	2022 Average	% Change
Chemical	20%	66%	+46
Electric	30%	40%	+10
Manufacturing	60%	73%	+13
Oil & Gas	50%	46%	-4
Water & Wastewater	100%	29%	-71
Other	86%	63%	-23
All	44%	54%	+10



timeframe perspective, it continues to hover around 50 percent, making shared credentials the key finding that has been the most consistent over the last four years.

Table 7 shows this key finding further broken down by OT vertical as well as its comparison from the 2021. The first column is the industry vertical, and the second column shows the percentage of service engagements that included a finding related to shared credential usage in 2021. The third column is the same metric for 2022 engagements and the last column is the delta between 2021 and 2022. For this table the higher the percentage the more prevalent the use of shared credentials was for that OT industry vertical.

In 2022, the water industry reduced their use of shared credentials by 71 percent. This positive shift in the water industry is presumably related to the cyber hygiene improvements implemented in the wake of the Oldsmar attack. The drastic change in the chemical vertical is likely due to the different types of chemical facilities and equipment in scope of the 2022 engagements compared to those in 2021. This past year's dataset included a diverse set of facilities such as petrochemical, plastics manufacturing, etc.

This key finding relates to three of the five critical controls for ICS cybersecurity: a defensible architecture, secure remote access, and risk-based vulnerability management. Leveraging shared credentials, like default accounts, vendor accounts, and those from IT trusts, adversaries can negate the layers of protections provided by network zones and levels. Shared credentials, especially those from domain trusts from IT networks, can also negatively impact the security of remote access. It can enable an adversary to pivot to OT networks from IT networks using valid accounts and then laterally move across the OT network with relative ease. As previously stated, risk-based vulnerability management assumes defenders can rely on a defensible architecture and secure remote access. Shared credentials degrade defensible architectures and secure remote access, therefore, also degrading a defender's ability to leverage risk-based vulnerability management.



Impact of Oil & Gas Pipeline Regulations

Over the last year, the U.S. Transportation Security Administration (TSA) worked with pipeline owners and operators to understand how they could revise Pipeline-2021-02B to better meet the goal of improving the overall cybersecurity resilience of pipeline organizations. The TSA considered feedback from industry groups and other federal partners, along with the input gained from the pipeline owners' and operators' submissions against Pipeline-2021-02B. The agency then incorporated this feedback into the new version of the directive known as Pipeline-2021-02C. The shift from a prescriptive, compliance-based standard to a functional, performance-based standard is a major improvement in Pipeline-2021-02C.

Pipeline-2021-02C contains many of the same requirements as Pipeline-2021-02B, including the need for a cybersecurity assessment program. This program incorporates assessment and auditing measures

during an architecture design review, which is required to be performed, at a minimum, every two years. In Pipeline-2021-02B, these architecture reviews were identified as Validated Architecture Design Reviews (VADR) and in Pipeline-2021-02C, the name was changed to Cybersecurity Architecture Design Review (CADR). While the name has become more generic, the elements of the program have not. C/VADRs continue to be performed, focusing on evaluating the owner's and operator's existing OT cybersecurity program.

The Dragos method of conducting a C/VADR focuses on identifying a list of IT/OT interdependencies, all external connections to OT, and zone boundaries based on the criticality of consequence and necessity. As a part of this process, Dragos conducts a network topology review and reviews organization policies and procedures. Pipeline owners and operators will meet the directive requirements of Pipeline-2021-02C

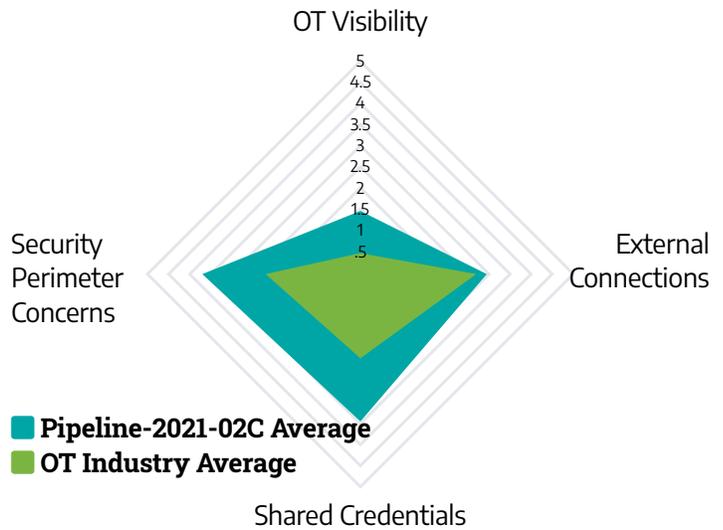
by incorporating these elements into their cybersecurity assessment program, but more importantly, it will ensure they are implementing measures that best protect their critical systems.

In 2022, Dragos performed V/CADRs for at least 20 percent of the pipeline operators in scope of Pipeline-2021-02C. At the same time, Dragos doubled its 2021 architecture reviews in the other OT verticals. This allows Dragos to compare common findings and trends of those within scope of the rule and the OT industry overall.

The radar chart in Figure 16 shows the cybersecurity strength and weaknesses of those in scope of the Pipeline-2021-02C by calculating the key findings and tracking along the central axis of the chart. The chart also includes these data points for the OT industry overall for comparison. The key finding percentages were converted to a 5-point scale. A score of 5 is the best possible score for that finding, meaning it was rarely found; 0 means the finding was prevalent in the vast majority of the engagements.

The oil and gas industry, at least those in scope of the Pipeline-2021-02C, score higher in three of the four key findings than the OT industry overall. For external connections, the oil and gas industry is on par with the OT industry overall. However, with the implementation of the Pipeline-2021-02C and its focus on identifying, limiting, and controlling external connections, Dragos expects this to improve in 2023.

FIGURE 16: KEY FINDINGS IN CADRS FOR PIPELINE-2021-02C VS ARS IN OT OVERALL



- Visibility is still a challenge for pipeline owners and operators, but trends higher than the OT industry average.
- Network security perimeters are significantly higher than the average OT industry.
- Shared credentials are less prevalent than the average OT industry.
- External connections are on par with the average OT industry.



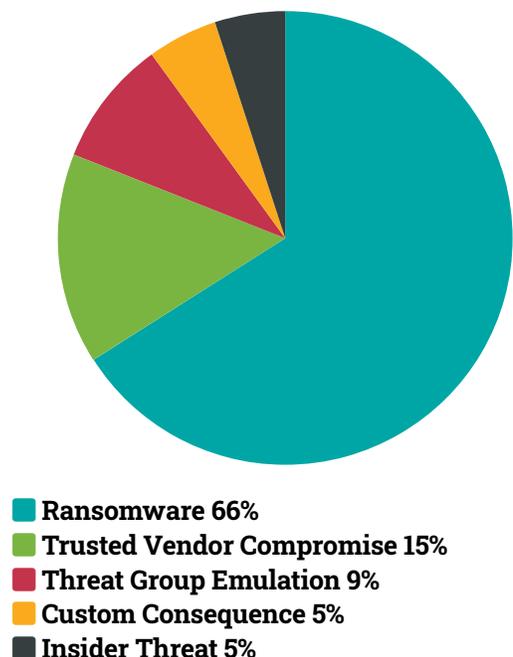


Assessing Cyber Readiness

OT-specific incident response plans are essential for industrial asset owners to account for the complexities and operational necessities of their environments. In fact, it is the first control, prioritized above the other four, in the five critical controls for ICS cybersecurity identified by the SANS Institute. SANS details three steps to the incident response planning process:

1. Scenario selection based on real-world examples.
2. Consider consequence-based scenarios.
3. Performing tabletop exercises (TTX) of those scenarios.

FIGURE 17: TTX SCENARIOS



What is a Tabletop Exercise (TTX)?

A TTX is a step-by-step method that demonstrates how a realistic attack may occur within your industrial environment. TTXs give participants and organizations the ability to practice how they would respond. This allows teams to understand their strengths and weaknesses. The most successful exercises include a range of staff across multiple disciplines and teams, including operators, plant managers, industrial control systems (ICS) support staff, and operational technology (OT) support staff, and IT. Dragos recommends including anyone who would play a role in an actual incident. TTXs are designed to evaluate the effectiveness of cybersecurity incident response plans, the coordination of the plans with partners, capability and resource employment, communication flow, and the actions with plan activation.

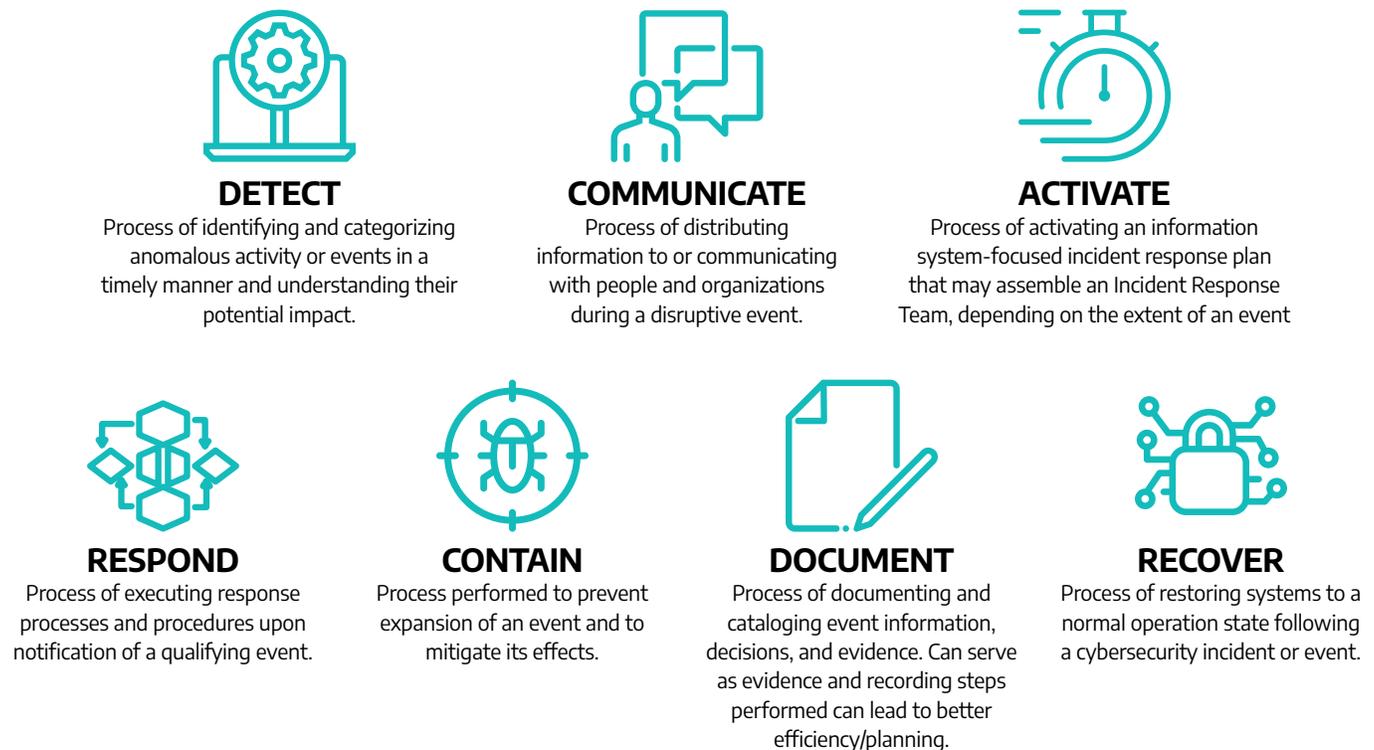
In 2022, Dragos executed over three times the number of TTXs for the OT industry than in 2021. Many factors contributed to this increase, most notably an increased

focus on OT cybersecurity from executives and regulatory commitments. The most common scenario chosen was ransomware at 66 percent. Ransomware being the top scenario choice was expected as it poses some of the most threatening financial and operational risks to industrial organizations.

Scoring TTXs

TTX findings and associated recommendations are listed in relation to the achievement of objectives through the employment of core capabilities for ICS/OT cybersecurity readiness and IR, identified as: detect, communicate, activate, respond, contain, document, and recover. Think of the core capabilities as a process that maps to common incident response processes regardless of if it is a four-step National Institute of Standards and Technology (NIST) process or the SANS Preparation - Identification - Containment - Eradication - Recovery - Lessons Learned (PICERL) process or some variation. Regardless of how the incident response plan (IRP) is structured, these capabilities are needed to successfully handle a cybersecurity event.

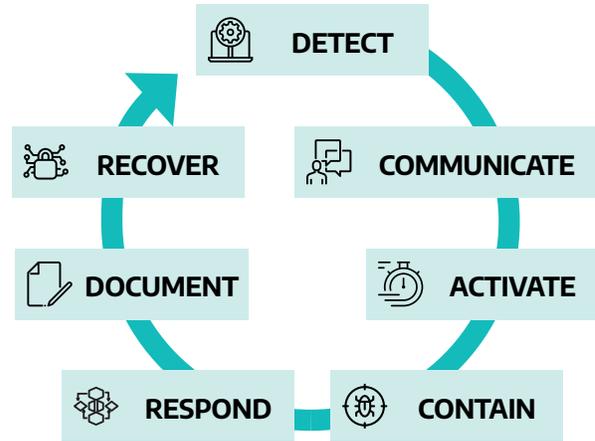
FIGURE 18: CORE CAPABILITIES



Viewing the core capabilities as a process allows originations and incident responders to view the capabilities as they feed into each other. For example, before a response action can be undertaken, the incident response process must be activated. Each core capability feeds into the next one in the process.

The two core capabilities that are more universal are the communication and document capabilities. In the flow, they are placed where those functions are most important. Once something is detected, there needs to be good communication in place to properly achieve activation. Similarly, documentation of the incident needs to be in place before recovery can be achieved successfully.

FIGURE 19: CORE CAPABILITIES AS A PROCESS



Key Takeaways for OT Overall

The core capabilities tested with the lowest aggregate score were **Detect** and **Document**. Despite increasing by 8 percent from 2021, **Detect** remains the most challenging core capability for asset owners. **Activate/Elevate** increased 12 percent leveling up from

being performed with some challenges to without challenges. A key takeaway from 2021 was that even when detection was performed with major challenges, many clients were able to compensate with a strong communication capability to remediate and recover without challenges. The data does not suggest that this has changed.

FIGURE 20: AVERAGE TTX SCORES (ALL OT)

Core Capability	2021 Score	2022 Score	Change	Metrics are as follows
Detect	65%	73%	+8	<ul style="list-style-type: none"> ■ Performed without Challenges 80-100 ■ Performed with Some Challenges 66-79 ■ Performed with Major Challenges 50-65 ■ Unable to Perform 0-49
Activate/Elevate	69%	81%	+12	
Respond	71%	76%	+5	
Contain	79%	81%	+2	
Communicate	85%	76%	-9	
Document	69%	73%	-4	
Remediate/Recover	85%	81%	-4	

Key Takeaways for Industry Breakdown

The 2022, TTX overall score was composed from many tabletop exercises encompassing several verticals including electric, oil and gas, manufacturing, metals and mining, data centers, and pharmaceuticals. TTXs in the electric, oil and gas, and manufacturing verticals, made up over 75 percent of the TTXs executed in 2022.

Customers in the electric industry scored the highest overall in comparison with other OT industries. Most likely, this is due to electric being the most mature vertical in terms of OT cybersecurity. Dragos expects the oil and gas industry scores will increase in 2023 as they continue to implement the TSA security directives.

FIGURE 21: VERTICALS

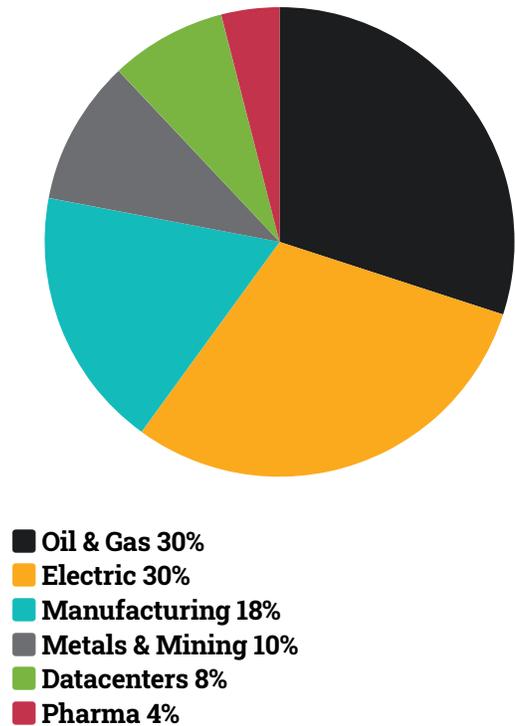


FIGURE 22: AVERAGE TTX SCORES BY INDUSTRY

Core Capability	Electric	Oil & Gas	Manufacturing	Metals/Mining	Datacenters	Pharma
Detect	81%	72%	65%	67%	75%	75%
Activate/Elevate	91%	78%	65%	83%	88%	75%
Respond	78%	78%	70%	75%	88%	50%
Contain	84%	88%	80%	67%	75%	75%
Communicate	84%	72%	65%	67%	63%	75%
Document	78%	69%	70%	75%	63%	50%
Remediate/Recover	88%	75%	70%	83%	88%	50%

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

Key Takeaways for Ransomware Scenarios

The value an asset owner receives from executing a TTX is directly correlated to the scenario and how applicable it is to their industry and cybersecurity goals. For that reason, scenarios should be selected based on real-world examples the asset owner is likely to face. In 2022, ransomware was the most common scenario chosen and made up 66 percent of all TTX scenarios Dragos conducted. The scores against ransomware were lower in every capability than the average scores that included all scenarios. This is surprising as one would expect ransomware would appear to be the most straightforward scenario. However, the results show that the OT industry continues to be threatened and challenged by ransomware and its potential impacts.

FIGURE 23: AVERAGE TTX SCORES FOR RANSOMWARE SCENARIO

Core Capability	Ransomware
Detect	67%
Activate/Elevate	75%
Respond	76%
Contain	79%
Communicate	75%
Document	71%
Remediate/Recover	79%

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**





5 Critical Controls for ICS/OT Cybersecurity

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

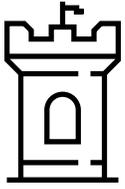


1. ICS incident response plan

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. Managing the potential impact of an incident is different for

pipelines, electrical grids, and manufacturing plants.

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. These criteria are used to establish the minimum requirements for OT visibility and monitoring. Dragos published a white paper on Collection Management Frameworks, available at: dragos.com/resource/collection-management-frameworks-beyond-asset-inventories-for-preparing-for-and-responding-to-cyber-threats. 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. Lastly, many aspects of risk-based vulnerability management are only possible when the defenders can leverage a defensible architecture.



3. Visibility and monitoring

You can't protect what you can't see. 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 incident response plan to avoid excess noise and focus on the risks they care about the most. Additionally, monitoring can also identify vulnerabilities easily for action.



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. While patching an IT system like a worker's laptop is relatively easy, shutting down a plant has huge costs.

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.



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](https://dragos.com)

