DRAGOS

EXECUTIVE SUMMARY

ICS/OT CYBERSECURITY YEAR IN REVIEW 2021

Executive Summary

In 2021, the industrial community attracted high-profile attention. Major cybersecurity incidents struck industrial organizations in a range of sectors, with international headlines detailing everything from a compromise of a water treatment facility with intent to poison its community to a ransomware attack against a pipeline operator that disrupted gas supplies to the southeastern United States. These reports underscored the potential devastating outcomes a security breach of critical infrastructure could have on communities and a country's economy. They also elevated the discussion the ICS/OT* community has been having for years on cyber readiness and brought them to the proverbial kitchen table—and the policymakers' and regulators' office desks, too.

With the 2021 Dragos Year in Review, Dragos experts hope to continue to help industrial organizations more fully understand the cyber risks surrounding their most important assets—their ICS/OT environments. The report provides data-driven insights that add context to the sensational stories and evidence from the field of how industrial organizations are progressing in their cybersecurity readiness and where they need to continue their work to provide safe and reliable operations into 2022 and beyond.

*The terms "ICS" and "OT" will be used interchangeably for the purpose of this report. These terms are used differently in different communities.

IN THE HEADLINES

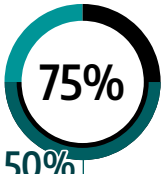
The last year has seen a number of dramatic stories develop that involved cyber attacks against high-profile ICS and OT targets. Alongside important industry-wide statistics about the threat landscape, the risk posture across ICS organizations, and the OT vulnerabilities observed in 2021, Dragos offered insight and context in the 2021 Year in Review about the most important headlines. Among the highlights were the following crucial stories.

Oldsmar Demonstrates the Risk to Water Systems

The City of Oldsmar announced in February 2021 that there was an unlawful intrusion into the City's water treatment system and that an adversary attempted to poison the water supply. Officials found that the adversary accessed and attempted to change the level of the corrosive chemical sodium hydroxide in the water. Fortunately, the operator of the machine immediately detected the remotely controlled mouse movements before the water plant released contaminated water into the water supply. While security controls such as automated pH testing would have also prevented the distribution of toxic water, Oldsmar highlights just how vulnerable critical infrastructure—such as water utilities—are to cyber attacks

DRAGOS
FRONTLINE PERSPECTIVE

75% of water utilities had external connections to the OT.



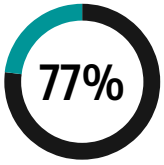
75% of potential process impacts for water utilities led to a loss of control.

50% led to a loss of safety.

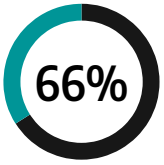
DarkSide Ransomware Disrupts Colonial Pipeline

As the largest fuel pipeline in the U.S., Colonial Pipeline delivers approximately 45 percent of the gasoline consumed on the U.S. East Coast. In May 2021, Colonial Pipeline's billing system was compromised by a ransomware attack which was reportedly the result of a single compromised password leveraged for remote access. To contain the attack and limit damage to only its IT network, Colonial Pipeline halted its pipeline operations. The resulting shutdown was no trivial matter— gas shortages and panic-buying ensued. The attack illustrates the importance of the interconnections and interdependencies between IT and OT systems.

DRAGOS
FRONTLINE PERSPECTIVE



77% of Oil & Gas architectures had external connections to OT segments.



66% of Oil & Gas potential process impacts involved a loss of availability (through ransomware or other means).

REvil Ransomware Attack Strikes JBS Foods

Also in May 2021, the notorious Russian hacker group REvil attacked the computer networks of JBS Foods—one of the largest beef suppliers in the world, with meatpacking facilities in the U.S., U.K., Australia, Canada, Mexico, and Brazil. This costly but containable ransomware attack spurred the firm to shut down many of its operations and to pay $11 million in Bitcoin ransom. While JBS Foods could maintain much of its system operations without REvil's assistance, it chose to pay the ransom.

Dragos uncovered and enumerated the networks associated with more than a dozen JBS facilities worldwide. Dragos found what appeared to be the exfiltration of gigabytes of data on the popular file storage service Mega from a network associated with the JBS's office in Brisbane, Australia.

DRAGOS
FRONTLINE PERSPECTIVE

100% of Food & Beverage architectures had external connections to OT.

2021 Threat Activity

Looking broadly at threat activity groups targeting ICS and OT with a range of attacks, Dragos discovered three new activity groups with the assessed motivation of targeting ICS/OT.

KOSTOVITE
In March 2021 when KOSTOVITE compromised the perimeter of an energy operation and maintenance provider network, it exploited a zero-day vulnerability in the popular remote access solution, Ivanti Connect Secure. KOSTIVITE used dedicated operational relay infrastructure against this target to obfuscate the origin of its activities, then stole and used legitimate account credentials for its intrusion.

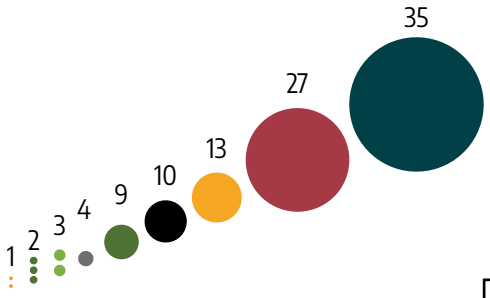
PETROVITE
PETROVITE targets mining and energy operations in Kazakhstan. One targeted group has 16 business units that focus on mining and power generation throughout Kazakhstan. Dragos is aware of targeted operations that started during the third quarter of 2019 and have intermittently continued throughout 2021.

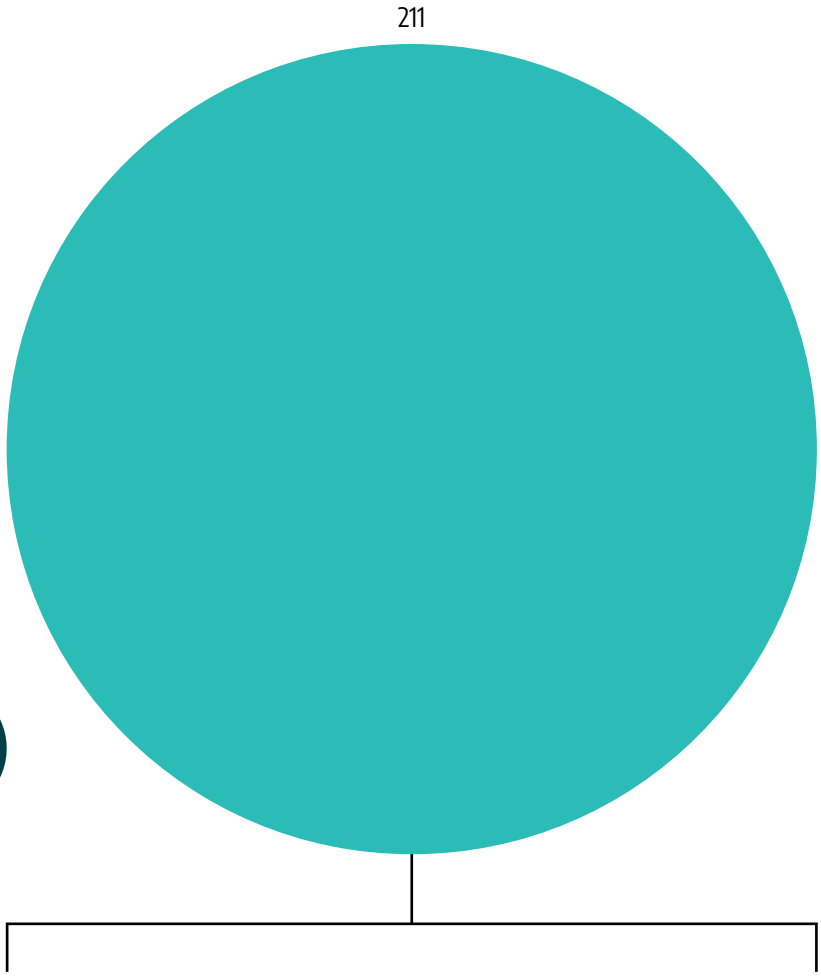
ERYTHRITE
ERYTHRITE is an activity group that broadly targets organizations in the U.S. and Canada with ongoing, iterative malware campaigns. Dragos has observed ERYTHRITE compromising the OT environments of a Fortune 500 company and the IT networks of a large electrical utility, food and beverage companies, auto manufacturers, IT service providers, and multiple oil and natural gas (ONG) service firms.

2021 was a ruthless year for ransomware gangs and their affiliates, with attacks reaching epic proportions, making ransomware the number one attack vector in the industrial sector. Dragos researchers observed that ransomware groups targeted the manufacturing industry more than any other ICS/OT sector in 2021– nearly twice as much as the other industrial groups combined.

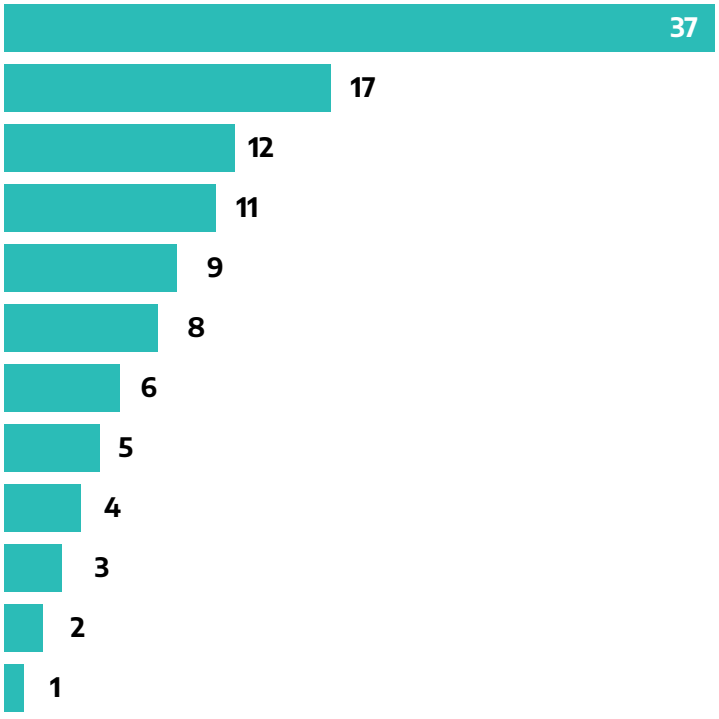
Ransomware by ICS Sector

211 Manufacturing
35 Food & Beverage
27 Transportation
13 Energy
10 Oil & Gas
9 Pharmaceuticals
4 Chemical
3 Mining, Logistics
2 Aerospace, Agriculture, ICS Equipment Distributor
1 Construction, Water

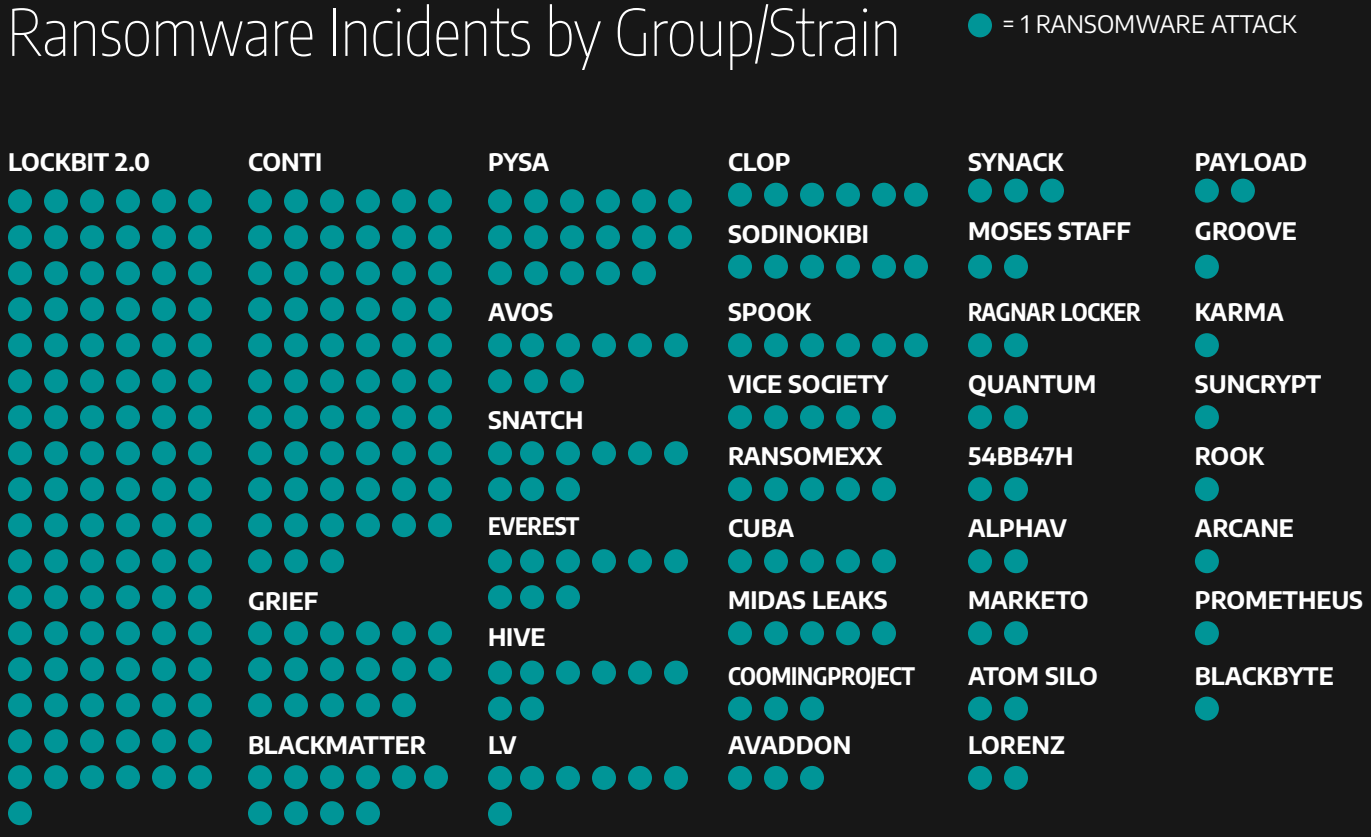




Ransomware by Manufacturing Subsector



Ransomware Incidents by Group/Strain



The marked spike in ransomware attacks can be attributed in large part to the emerging ransomware-as-a-service (RaaS) phenomena. Ransomware gangs like Conti and Lockbit 2.0 have mobilized into an underground marketplace where their developers outsource operations to affiliates who execute the attacks.

Conti and Lockbit 2.0 caused 51 percent of the total ransomware ICS/OT Dark Web postings, with 70 percent of their malicious activity targeting manufacturing.

Dragos Frontline Perspective

Lessons Learned from Incident Response

OT defenders require visibility, credible threat intelligence, and extensive process knowledge to mitigate the physical consequences of OT cyber attacks. Data analyzed across Dragos professional service engagements in 2021 shows many organizations grappled with these challenges last year. Dragos works with a broad range of industrial infrastructure sectors, including electric, oil and gas, food and agriculture, manufacturing, chemical, transportation, nuclear, water and wastewater, technology (data center building automation equipment), and mining sectors. The findings described below come from a range of service types, including architectural reviews, compromise assessments, vulnerability assessments, penetration tests, tabletop exercises, and incident response:

Limited or No OT Network Visibility

During 2021, Dragos uncovered that 86% of its services customers had limited to no visibility into their ICS environment.

2021 **86%**
2020 **90%**
2019 **81%**

Poor Security Perimeters

In 2021, 77% of Dragos services engagements involved issues with network segmentation (which is a slight decrease from 2020).

2021 **77%**
2020 **88%**
2019 **71%**

External Connections to the ICS Environment

In 2021, external connections to OT spiked upwards, more than doubling to 70%.

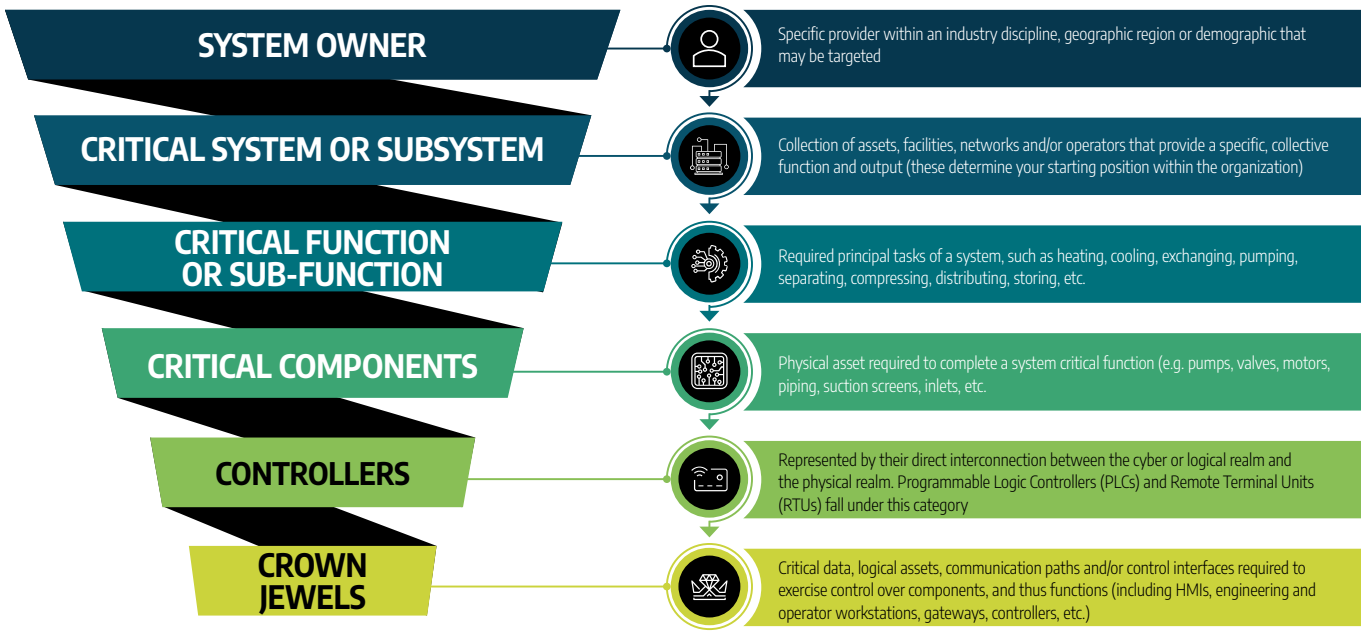
2021 **70%**
2020 **33%**
2019 **100%**

Lacked Separate IT & OT User Management

Forty-four percent of service engagements have shared credentials between IT and OT networks – an improvement from 54% last year.

2021 **44%**
2020 **54%**
2019 **54%**

Dragos uses a consequence-driven approach, the Crown Jewel Analysis (CJA) Model, when scoping and conducting ICS/OT cybersecurity assessments. The CJA Model is a repeatable scoping approach that helps visualize how an attacker assesses a system to achieve a specific consequence.



Using CJA and credible threat intelligence, Dragos creates plausible attack scenarios to educate asset owners and operators on its potential exposure to adversaries and activity groups and to better prioritize the findings and recommendations in our reports.

55%

of our crown jewel analyses (CJAs) had a potential impact involving the denial, loss, or manipulation of process control.

20%

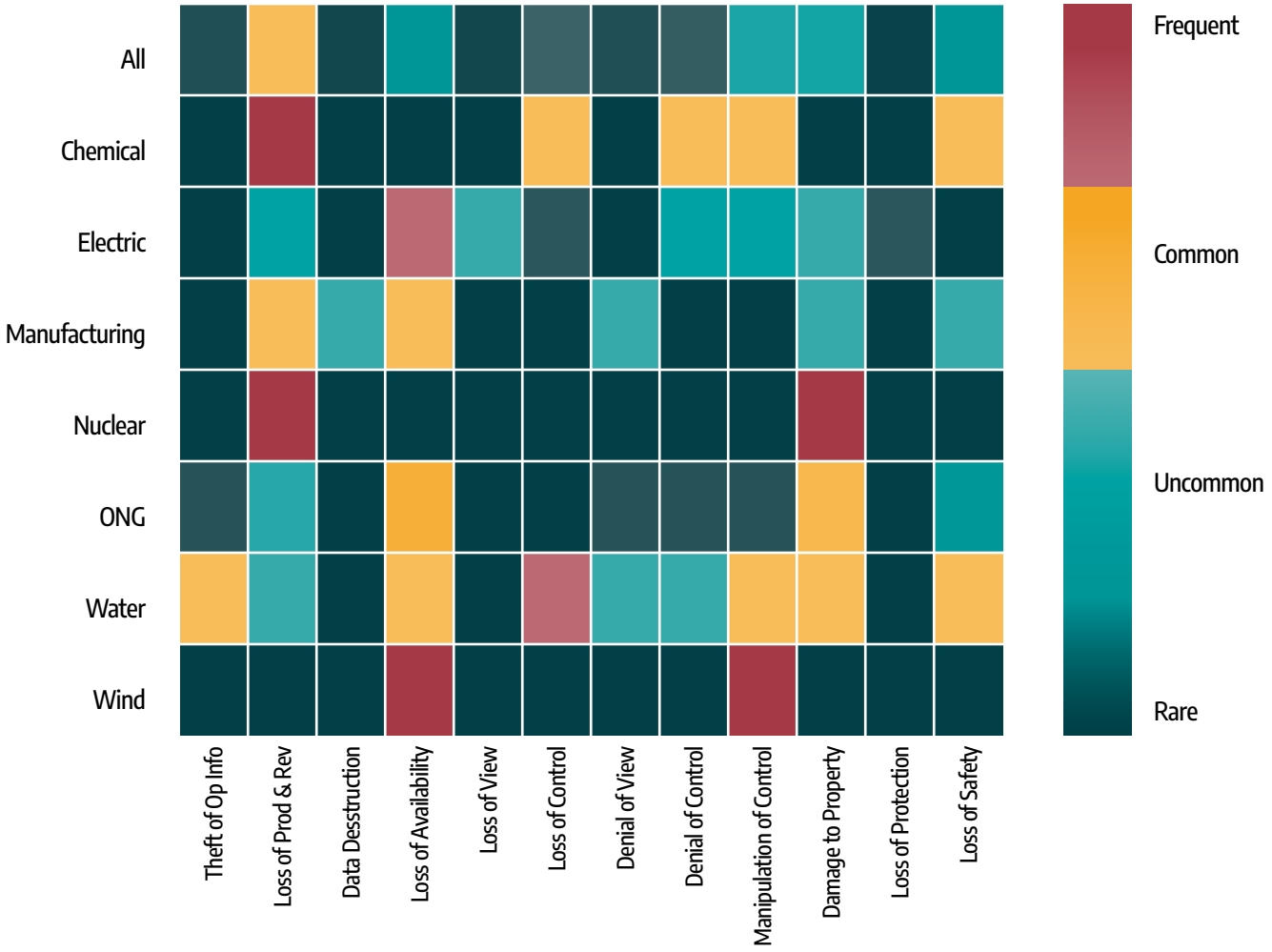
included a loss of safety impact.

The most common impacts for the Energy sector CJAs were **LOSS OF AVAILABILITY** and **MANIPULATION OF CONTROL.**

The manufacturing CJAs were evenly distributed, with the most common CJA impact involving a **LOSS OF PRODUCTIVITY AND REVENUE.**

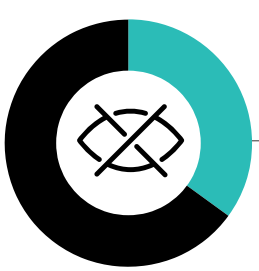
The following heatmap shows the ICS/OT impacts identified across each OT industry vertical from CJA engagements in 2021. Each row depicts a specific industry and each column is an operational impact identified during the CJA.

CJA Impact by Sector Heat Map



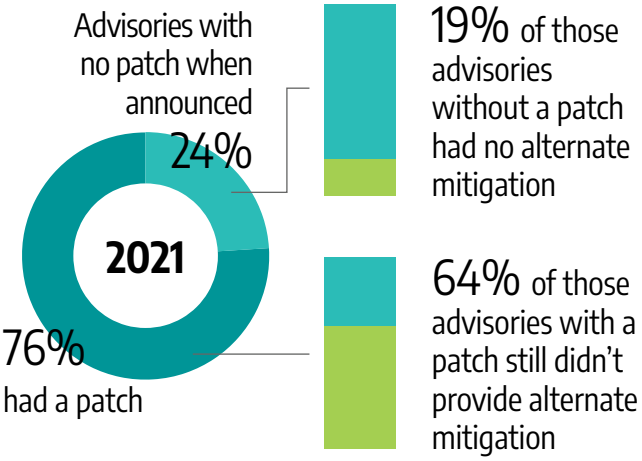
Vulnerabilities

2021 was a challenging year for ICS and OT vulnerabilities. The numbers bear this out with a near doubling of published ICS and OT vulnerabilities in 2021 than that which was published in 2020. Some of the flaws that arose included the likes of Log4j, the Windows zero-day vulnerability nicknamed PrintNightmare, and industrial hardware rootkit-level vulnerabilities that can enable an attacker to compromise exposed devices. These examples underscore the fast-growing universe of persistent vulnerabilities that exist throughout all layers of the Purdue Model. These vulnerabilities are also evidence of the complex nature of connected and networked components in OT environments and ICS.



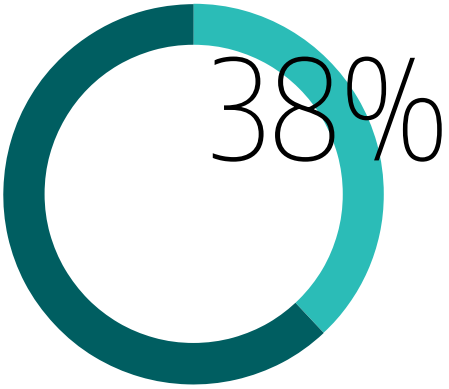
35% of ICS and OT vulnerability advisories in 2021 could cause both a loss of view and loss of control in an OT system

Dragos researchers analyzed 1703 ICS/OT common vulnerabilities and exposures (CVE) during 2021, which is more than twice as many as last year.



Dragos provides customers with insight into managing risks on disclosed ICS vulnerabilities beyond what is included in vendor advisories. In 2021, we provided additional mitigation advice for 69 percent of advisories that did not include this information.

For each CVE, Dragos independently assesses, confirms, and often corrects the advisories and describes any flaws in firmware or software. In addition to the lack of actionable information from most ICS-related vulnerability advisories in 2021, many advisories and individual vulnerabilities contained errors that could inadvertently mislead practitioners who use CVSS scores to triage for mitigation or patching. This could cause asset owners and operators to dedicate more resources to fixing the vulnerabilities that represent a lower level of risk and severity over those that might represent a higher level of risk for their own ICS/OT environments.



of OT vulnerabilities contained errors in the Common Vulnerability Scoring System (CVSS) score associated with the CVE.

Asset owners should take this into account when making patching and mitigation decisions for their networks. CVSS scores can be misleading and often do not accurately capture all of the risk of a particular vulnerability. ICS/OT security professionals should not use them as the sole factor to prioritize vulnerabilities.

Remediate, Mitigate, Monitor, & Ignore Breakdown

In the past year, we found that the Dragos platform could provide additional recommended actions on top of the Now, Next, Never categories used in previous years. We wanted to highlight the specific actions our customers should take based off of the threat level of the assessed vulnerabilities. So, instead of discussing our "Now, Next, Never" prioritization, we are now providing the recommended actions: Remediate, Mitigate, Monitor, Ignore.

Possible risks are often local threats which can coincide with adversaries living off the land. Dragos recommends that that ICS security professionals monitor these vulnerabilities for malicious activity. In 2021, 87 percent of the vulnerabilities that Dragos analyzed were "Mitigate" or "Monitor." Vulnerabilities in the "Ignore" category do not increase the level of risk to the process at all. The effort it takes to mitigate these vulnerabilities is generally not a good use of the ICS security professional's time because adversaries are not as likely to exploit them.

Only 8.8% of the vulnerabilities that Dragos reviewed were in the "Ignore" category.

Recommendations

1 BUILD A MORE DEFENSIBLE ARCHITECTURE (External Connections, Poor Perimeters)

70% OF SERVICE ENGAGEMENTS included a finding of external connections from OEMs, IT networks, or the Internet to the OT network and **77% OF SERVICE ENGAGEMENTS** included a finding about improper network segmentation. Network architects can leverage traditional tools and concepts such as strong segmentation, firewalls, or software defined networks to reduce cyber risk. This can take a variety of forms such IEC62443 zones and conduits, DMZs, jumphosts, etc.

2 BOLSTER OT MONITORING CAPABILITIES

86% OF SERVICE ENGAGEMENTS included a finding around lack of visibility across OT networks, making detections, triage, and response incredibly difficult at scale. 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. Additionally, monitoring can also identify vulnerabilities easily for action.

3 STRENGTHEN REMOTE ACCESS AUTHENTICATION

44% OF SERVICE ENGAGEMENTS included a finding about shared credentials in OT systems, the most common method of lateral movement & privilege escalation. The most effective control for remote access authentication is multi-factor authentication (MFA). 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.

4 BETTER PRIORITIZE OT VULNERABILITY MANAGEMENT

The number of ICS/OT vulnerabilities discovered doubled in 2021, but **ONLY 4% OF FLAWS REQUIRE IMMEDIATE ACTION** because they are being actively exploited in the wild or for which a public exploit is available. Dragos recommends defenders prioritize those that bridge IT and OT over those residing deep within the ICS/OT network or those that fall into the "Remediate" category in Dragos's vulnerability analysis.

5 CONTINUALLY IMPROVE THE ICS/OT INCIDENT RESPONSE PLAN (IRP)

Tabletop exercise (TTX) testing of existing ICS/OT incident response (IR) plans in 2021 showed that **MOST ORGANIZATIONS FACED AT LEAST SOME CHALLENGES IN FIVE OUT OF SEVEN CORE IR CAPABILITIES.** Dragos recommends that industrial organizations have a dedicated IR plan for their ICS/OT environments that they regularly exercise against real threat scenarios with cross-disciplinary teams (IT, OT, Executives, etc.).

For more details, read the full 2021 Dragos Year in Review report HERE.

Dragos is an industrial (OT/ICS/IIoT) 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