



DRAGO 

ICS/OT CYBERSECURITY  
**YEAR IN REVIEW 2021**

# Contents

<b>Introduction</b> .....	<b>4</b>
<b>Key Highlights</b> .....	<b>5</b>
Activity Groups.....	5
Ransomware Findings.....	5
Service Engagement Findings.....	5
Vulnerability Advisory Findings.....	6
<b>In the Headlines</b> .....	<b>7</b>
When OT Cyber Disruption Leads to Panic and Economic Shutdown .....	7
When Ransomware Attacks Endanger the Nation’s Food Supply .....	8
Oldsmar Demonstrates the Risk to Water Systems .....	10
When the U.S. Food Supply Chain Became a Target .....	11
<b>2021 Threat Activity</b> .....	<b>12</b>
Key Updates on Activity Groups.....	13
Updates on Previously Known Activity Groups .....	14
STIBNITE.....	14
WASSONITE .....	15
KAMACITE.....	16
<b>New Activity Groups</b> .....	<b>17</b>
KOSTOVITE .....	18
PETROVITE .....	20
ERYTHRITE .....	21
<b>Ransomware and Industrial Infrastructure</b> .....	<b>23</b>
The Unintended and Intended Ransomware Threats to OT .....	23
Industrial Security Ransomware Trends .....	24
Ransomware Incidents By Group: Conti and Lockbit 2.0 .....	25
Why Were Ransomware Gangs So Successful in 2021? .....	26
The Growing Maturity of Ransomware as a Business.....	26
Looking Ahead Into 2022 .....	26
<b>Dragos Frontline Perspective</b> .....	<b>27</b>
<b>Lessons Learned from Incident Response</b> .....	<b>28</b>
<b>Lessons Learned from the SolarWinds Compromise</b> .....	<b>29</b>
<b>The Value of Root Cause Analysis</b> .....	<b>30</b>
<b>Who Changed the Setpoints?</b> .....	<b>30</b>
Need for Monitoring and Incident Response Plans .....	31

The Ghost in the Power Generator.....	32
Never Let an Incident Response Team’s First ICS Be Your ICS! .....	33
An MSP Case Study – An ICS/OT Service Provider is Compromised .....	34
Key Takeaways .....	35
The Complexity of Remote Access in OT Environments.....	36
<b>Data-Driven Insights from the Field.....</b>	<b>39</b>
<b>Top 4 Key Findings .....</b>	<b>40</b>
Limited or No OT Network Visibility .....	40
Poor Security Perimeters .....	41
External Connections to the ICS Environment .....	42
Lacked Separate IT & OT User Management .....	43
<b>Findings Across Industry Verticals.....</b>	<b>44</b>
<b>Cybersecurity Assessments Findings.....</b>	<b>45</b>
The Crown Jewel Analysis (CJA) Model .....	45
<b>Cyber Readiness Findings.....</b>	<b>47</b>
Average TTX Scores.....	47
<b>Vulnerabilities.....</b>	<b>48</b>
<b>Introduction .....</b>	<b>49</b>
<b>Apache Log4j Vulnerability .....</b>	<b>50</b>
Why Are Industrial Networks Vulnerable to Log4j?.....	50
Next Steps to Mitigate Log4j.....	51
<b>Windows Zero-Day Vulnerability: PrintNightmare .....</b>	<b>51</b>
How Adversaries Gain Access to OT Networks with PrintNightmare .....	51
<b>PLC and Industrial Hardware Rootkit-Level Vulnerabilities.....</b>	<b>53</b>
The Long-Term Risks of Persistent Rootkits .....	53
What Are the Impacts of Rootkits?.....	54
Mitigating the Risks of Rootkit Vulnerabilities.....	55
<b>Key ICS Vulnerability Trends: By the Numbers.....</b>	<b>56</b>
Where Do the Vulnerabilities Reside? .....	57
Loss of View, Loss of Control, or Both.....	58
Many Advisories Lack Actionable Guidance .....	59
Correcting Vulnerability Severity Ratings.....	60
Vulnerability Recommended Actions: Remediate, Mitigate, Monitor, Ignore.....	61
<b>Mitigating Vulnerabilities in 2022.....</b>	<b>62</b>
<b>5 Security Controls for a World-Class OT Cybersecurity Program .....</b>	<b>63</b>



## INTRODUCTION

---

Dragos is excited to present the fifth year of the annual Dragos Year In Review report on Industrial Control System (ICS)/Operational Technology (OT) cyber threats, vulnerabilities, assessments, and incident response observations. The ICS/OT\* community has long suffered from more anecdotes on security than insights driven from data and real-world cases given the sensitivity of the subject. A lack of insights into the ICS/OT threat landscape and state of security prevent the community from having meaningful discussions on how to address today's challenges. The Dragos Year in Review report was launched with the intent to add ground-truth reality into the discussion as an attempt to move the conversation and security efforts forward.

In 2021, the industrial community attracted high-profile attention. Headlines range from the 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 potentially devastating outcomes a security breach of infrastructure could have on communities and a country's economy. Beyond these public examples, there are numerous other matters that were never made public. Industrial organizations are becoming aware that they no longer fully understand the security risks surrounding their most important assets – their ICS/OT environments.

This report captures how a portion of the industrial community is performing and progressing, and highlights the areas that need improvement to provide safe, 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.



# KEY HIGHLIGHTS

## ACTIVITY GROUPS



KOSTOVITE



PETROVITE



ERYTHRITE

Dragos discovered **three new activity groups** with the assessed motivation of targeting ICS/OT.

**Two of the groups have achieved Stage 2 of the ICS Cyber Kill Chain** showing their ability to get access directly to ICS/OT networks.\*\*

## RANSOMWARE FINDINGS



65%

**Manufacturing** accounted for 65% of all ransomware attacks.

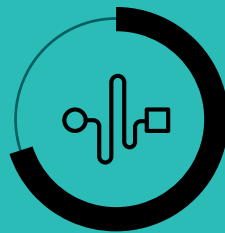
51%

**Two ransomware groups** caused 51 percent of attacks (Lockbit 2.0 and Conti).

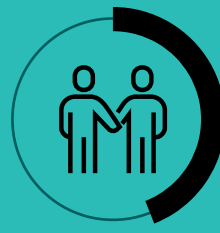
## SERVICE ENGAGEMENT FINDINGS



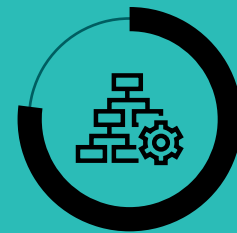
**86% of service engagements** have a lack of visibility across OT networks — making detections, triage, and response incredibly difficult at scale.



**70% of service engagements** included a finding of external connections from OEMs, IT networks, or the internet to the OT network.



**44% of service engagements** included a finding about shared credentials in OT systems, the most common method of lateral movement and privilege escalation.



**77% of service engagements** included a finding about improper network segmentation.

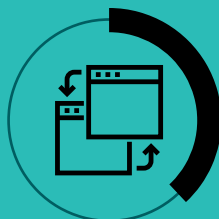
\*\*The ICS Cyber Kill Chain breaks intrusions into Stage 1 and Stage 2 operations. Stage 1 are IT network compromises where the adversary appears to have a goal of getting into the ICS/OT networks of the company but has not achieved this yet. Stage 2 operations are those where the adversary has gained access to ICS/OT networks. At the completion of the ICS Cyber Kill Chain an adversary conducts disruptive or destructive operations. The paper can be found [here](#).

# KEY HIGHLIGHTS

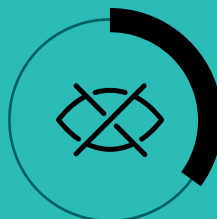
## VULNERABILITY ADVISORY FINDINGS



**More than twice as many** common vulnerabilities and exposures (CVE) were published in 2021 than in 2020.



**38% of ICS vulnerability advisories** contained errors that would make it difficult to prioritize mitigations.



**35% of the advisories** could cause both a loss of view and loss of control in OT systems.



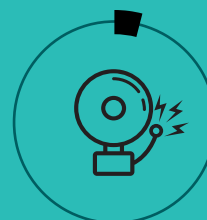
**19% of advisories** without a patch had no alternate mitigation.



Dragos provided mitigation advice that was missing for **69% of advisories**.



**64% of advisories** with a patch had no alternate mitigation advice.



**Only 4% of advisories** that Dragos analyzed required immediate remediation.

# IN THE HEADLINES

## When OT Cyber Disruption Leads to Panic and Economic Shutdown

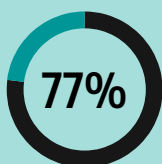
**The DarkSide ransomware attack on Colonial Pipeline highlighted the impact of an attack on pipelines to the broader public. Colonial Pipeline is the largest fuel pipeline in the U.S. and delivers approximately 45 percent of the gasoline consumed on the U.S. East Coast. Colonial Pipeline halted its pipeline operations to contain the ransomware attack to its IT operations and ensure the safety of the public. The resulting shutdown caused gas shortages and panic-buying by the public, and the Transportation Security Agency (TSA) introduced new regulations for the pipeline community.**

With Colonial Pipeline's billing system compromised, the decision to shut down the entire pipeline was made to isolate and contain the attack and help ensure the adversary did not spread to the Operational Technology (OT) network controlling pipeline operations. This was an appropriate and safety-focused decision. Greater visibility into the OT networks would have better armed Colonial Pipeline in their decision-making process, but their actions ensured that no one was hurt.

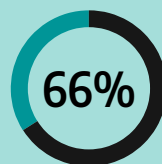
Colonial Pipeline engaged the FBI and Mandiant for the IT efforts and Dragos for the OT security work to ensure Colonial would be in a good place in the future. Lessons learned for organizations include: Ensure that key incident response questions and answers are identified before a security incident to determine if the organization will be comfortable continuing operations. Questions and answers on OT security efforts, incident response planning, and data collection strategies will drive preparedness.

For governments, lessons learned from the regulation should be that the wholesale adoption of IT security controls into OT environments can be ill-suited at best and disruptive at worst. The TSA regulations included some requirements that would not reduce the risk of cyber threats to pipeline infrastructure and, if followed completely, would likely result in outages. Governments and regulators should work closely with the asset owner and operator community, as well as industry subject matter experts to ensure that the security controls put forward are tailored to the risks and appropriate for industrial automation environments.

### DRAGOS FRONTLINE PERSPECTIVE



of oil & gas architectures had external connections to OT segments.



of oil & gas potential process impacts involved a loss of availability (through ransomware or other means).

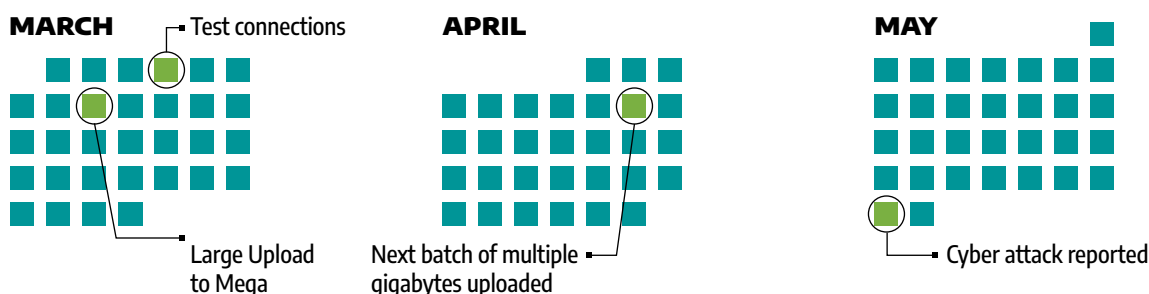
# IN THE HEADLINES

## When Ransomware Attacks Endanger the Nation's Food Supply

**In May 2021, the ransomware group REvil breached 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, and Mexico. According to reports, the ransomware was detected in JBS's Sao Paulo operation, targeting critical infrastructure within the organization. In recent years, REvil has attacked multiple organizations by encrypting their files and demanding Bitcoin payments in exchange for decryptors and the assurance they will not leak stolen information.**

After the attack, JBS Foods shut down many of its operations and then paid \$11 million in Bitcoin ransom. Externally, 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 uncovered that this exfiltration tactic is consistent with previous reports of ransomware operators that use the open-source transfer tool Rclone, combined with Mega, to stage its stolen data. Dragos observed test connections to Mega on March 4 and 5, 2021, with a large upload on March 7. The next batch of multiple gigabytes took place on April 9. The final batch was uploaded on May 30, the same day that JBS reported the cyber attack. The crucial ability to detect an adversary's exfiltration activities can disrupt the encryption phase of such ransomware attacks.



*Continued next page>>>*



When you consider that JBS supplies almost a quarter of the U.S. with its meat products, there are important lessons to learn from this cyber attack:

- In-depth knowledge of how IT and OT infrastructure overlaps and is connected will enable teams to quickly identify and isolate infected systems.
- Identifying the strain of the malware and how it is impacting systems will help prevent further spread.
- Identifying the data that was compromised during an attack is critical for determining its value to the organization, as well as the dependencies to the data that may impact operations.
- A robust backup plan is key for disaster recovery efforts. With JBS, they shut down operations to contain the attack and decrease the overall damage.

## DRAGOS FRONTLINE PERSPECTIVE



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

# IN THE HEADLINES

## Oldsmar Demonstrates the Risk to Water Systems

**The cyber attack on the Oldsmar water system in Florida on February 5, 2021, demonstrated the potential risks to municipal water systems throughout the world. During a press conference, the City of Oldsmar announced there was an unlawful intrusion into the City's water treatment system and that an adversary attempted to poison the water supply.**

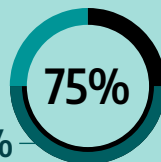
According to the sheriff of Oldsmar, the adversary accessed the Human Machine Interface (HMI) installed on a workstation, which was used to control the water treatment process through a remote access tool called TeamViewer. TeamViewer is a popular tool technicians and administrative support use to gain remote access to a computer. The attackers changed the level of sodium hydroxide (NaOH), also known as lye or caustic soda, to 11,100 parts per million (ppm), which is a significant increase from the normal amount of 100 ppm. The operator saw the remotely controlled mouse movements on the HMI and acted quickly.

**Sodium hydroxide (NaOH)** is a corrosive chemical used in low concentrations to regulate the pH level of drinking water to protect water pipes. At higher levels, it is toxic and can damage human tissues. Fortunately, Oldsmar municipal water plant engineers immediately observed the attack and restored the NaOH levels to normal operating parameters before the water plant released the contaminated water into the Oldsmar water supply.

**DRAGOS**  
FRONTLINE PERSPECTIVE



of water utilities had external connections to OT.



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

50% led to a loss of safety.

The actions of the operators and personnel at Oldsmar were commendable and prevented any risk to the public. However, organizations will not always be lucky enough to observe overt actions by adversaries. Historically, many industrial organizations have invested heavily in prevention. They must also invest heavily in the ability to detect, respond, and recover with technology and personnel. Unfortunately, for many smaller utilities, such as some municipal water systems, economics can prevent such investments. It is not uncommon for smaller utilities to share their IT staff or have contractors versus a full-time cybersecurity staff.

Until the economic conditions change, such as government financial support, the cybersecurity maturity of the smaller utilities is unlikely to change.

# IN THE HEADLINES

## When the U.S. Food Supply Chain Became a Target

**In mid-September 2021, the ransomware group BlackMatter attacked New Cooperative, an association of Iowa corn and soybean farmers, and demanded a \$5.9 million ransom payment for a decryptor. The attack was more evidence that infrastructure and the U.S. food supply chain had become targets. New Cooperative claimed that the breached software governed the feeding schedules of 11 million farm animals and 40 percent of their grain production. Blackmatter, the ransomware group previously known as Darkside, had claimed that they would “avoid targeting critical infrastructure,” yet their actions did not reflect their public statements.**

New Cooperative, its 60+ locations, and other U.S. farming and grain co-ops found themselves the target of ransomware groups. Dark web forums suggested that adversaries had exfiltrated 1000 GB of New Cooperative’s data; however, Dragos could not identify that exfiltration of data from New Cooperative’s network had occurred as the adversary claimed. On September 23, the Minnesota-based Crystal Valley Cooperative announced it was also hit with ransomware, which forced the company offline and disrupted its business operations.

Later in October, the ransomware group BlackByte allegedly attacked a second Iowa cooperative called Farmer’s Cooperative Elevator Co. The threat group threatened to release 100 gigabytes of data that included financial, sales, and accounting information if the ransom was not paid.

Historically, it is unusual for adversaries to target farmer co-ops. This series of attacks illustrates that industrial targets like farmer co-ops, once thought of as unlikely victims, can become prime targets without notice. U.S. Agriculture Secretary Tom Vilsack has urged cooperatives to strengthen their defenses against cyber attacks to avoid disruptions to the nation’s harvest.

SECTION ONE

---

# 2021 Threat Activity

## Key Updates on Activity Groups

During 2021, cyber risk to industrial sectors grew and accelerated, largely led by ransomware. Dragos emphasizes the importance of understanding how adversaries gain access and steal information to better prepare for threats in the future. Adversaries tend to build their operations and capabilities methodically over time; their previous efforts often determine their future success.

Dragos tracks threats, also identified as activity groups, which show the intent, opportunity, or capability of impacting industrial operations. Some of these threats have shown the intent and capability to disrupt operations and even cause destructive effects. These threats may be in the early stages of their journey, and have only shown the intent to target industrial organizations by attempting to gain access to ICS/OT networks or collecting organizational information.

Dragos tracks a number of groups that have targeted industrial networks, but do not show the intention of disrupting them—this is much more common in reality than is publicly reported. Adversaries may do this for intellectual property theft, capability development for future attacks, or simply gaining and maintaining access for future undetermined needs. In some cases, adversaries gain access to the IT networks of an organization or its supply chain to get information about the ICS of the target. As an example, engineering drawings are useful in both intellectual property theft and disruptive capability development but would not usually be stored in the ICS networks of the company. These drawings would more likely be stored in the IT networks of that company's integrator. Although not every compromise will relate to an impact today, many can inform the attacks of the future.

Currently, Dragos tracks 18 worldwide threat groups, with three of the newest groups discovered during 2021. Two of the new Activity Groups, KOSTOVITE and ERYTHRITE, demonstrate Stage 2 ICS Cyber Kill Chain<sup>1</sup> intrusions with a focus on access operations and data theft over disruption. This shows that adversaries are willing to spend time, effort, and resources targeting, compromising, and harvesting information from ICS/OT environments for future purposes.

<sup>1</sup>SANS ICS Cyber Kill Chain

# Updates on Previously Known Activity Groups

**Throughout 2020, the Activity Groups identified prior to 2021 remained active against industrial organizations. While already covered in previous Year in Review reports, the following key activities occurred in 2021 that are worth noting:**

## STIBNITE

From late 2019 through early 2020, the Activity Group STIBNITE emerged with its first phase of Stage 1 industrial infrastructure intrusions. STIBNITE initially focused on IT intrusion and information gathering on wind turbine companies that generate electric power in Azerbaijan. Azerbaijan is near the Caucasus region, an area that is a significant source of energy for Europe.

In February 2021, STIBNITE targeted Azerbaijani environmental science, technology, and industrial engineering experts, researchers, and practitioners interested in technical conferences. STIBNITE sent victims spear-phishing emails about such events as a first lure and attempt at installing a new version of PoetRAT written in .NET. A month later, STIBNITE used a State Oil Company of the Azerbaijan Republic (SOCAR) spear-phishing lure targeting the Azerbaijan Ministry of Ecology and Natural Resources. The STIBNITE spear-phishing emails all contained a downloadable document with a macro that when executed would drop a new version of PoetRAT written in Python.

STIBNITE continues to target entities in Azerbaijan and uses infrastructure overlapping with its previous intrusions to make updates to PoetRAT. There does not appear to be motivation or active operations that should be of concern to global ICS owners outside of Azerbaijan, although global operators can learn from the tactics, techniques, and procedures (TTPs) of STIBNITE to enhance their defenses against adversaries leveraging similar tactics. However, STIBNITE has demonstrated an explicit and calculated interest in targeting Azerbaijani wind generation capabilities while it is still in its infancy. In addition, STIBNITE has shown a repeated interest in targeting entities related to Azerbaijani renewable energy projects. It is likely STIBNITE will gain initial access to these projects as they reach operational maturation by masquerading as related and trusted entities, which STIBNITE has demonstrated in the past.



**Dragos assesses with moderate confidence that Azerbaijani asset owners and operators related to renewable energy interests should anticipate activities from STIBNITE as more renewable asset projects reach commercial operation in the future.**



## STIBNITE

**Target Geography**  
Azerbaijan

**Victimology**  
Electricity, Wind,  
Renewable Energy

**Malware**  
PoetRAT

## WASSONITE

In late October 2019, Dragos identified the adversary WASSONITE targeting the Kudankulam Nuclear Power Plant (KKNPP) nuclear facility in India. Subsequent intelligence research combined with public announcements from KKNPP confirmed that adversaries had breached its IT network. In addition, Dragos identified a pattern of activity associated with the same tactics, tools, and techniques spanning multiple ICS entities that included electric generation, nuclear energy, manufacturing, and space-centric research sectors.

Dragos has determined that WASSONITE has operated since at least 2018 with limited technical overlaps to the cluster of activity tracked as Kimsuky.<sup>2,3</sup> The WASSONITE activity group leverages spear phishing as their initial infection vector. WASSONITE uses malware with customization for specific internal networks in their targeting of ICS verticals. WASSONITE's geographic targeting has focused on Asian entities, including India and possibly Japan and South Korea. WASSONITE operations represent Stage 1 of the ICS Cyber Kill Chain intrusions. Intrusion activity consisted of known malware leveraged in enterprise systems used for data theft and reconnaissance, known credential harvesting tools, and use of Windows system tools for file transfer and lateral movement.

On April 17, 2020, Dragos identified a variant of DTrack malware with technical overlaps to previously observed samples associated with WASSONITE. This DTrack variant included specific hardcoded ports and internal IP addresses targeting the Fujitsu Systemwalker distributed computing and data center management software.

In July 2021, Dragos discovered multiple victims in the oil & gas, electric, and component manufacturing industries communicating with a WASSONITE command and control server (C2) server associated with 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 the C2 server.<sup>4,5</sup>

While it is unknown if the Appleseed backdoor was deployed within an OT environment, the screenshot functionality is valuable for use against the victim's system operator or Human Machine Interface (HMI) as a form of recon or data exfiltration to further understand the industrial process.



**Dragos assesses that WASSONITE will continue to target ICS entities in the electric generation, nuclear energy, manufacturing, and space-centric research sectors with their demonstrated intent and capabilities, with subsequent access sufficient in many cases to execute follow-on attacks.**



### WASSONITE

#### Target Geography

India, Japan, Korea

#### Victimology

Electricity, Nuclear, Manufacturing, Space research

#### Malware

DTrack variant

<sup>2</sup>The Lazarus Constellation – Lexfo; <sup>3</sup>Kimsuky, King of Spearphishing – Virus Bulletin; <sup>4</sup>Operation MUZABI – KISA; <sup>5</sup>Kimsuky's Appleseed Backdoor – Malwarebytes Labs



## KAMACITE

Since 2014, the activity group KAMACITE has had a long-running and consistent pattern of targeting critical infrastructure and industrial verticals. KAMACITE has repeatedly targeted U.S. electric utilities, oil and gas, and other industrial firms since as early as 2017 and has had additional operations throughout Europe and North America. KAMACITE also has extensive activity targeting the Ukraine electricity sector.

KAMACITE has technical overlaps with the group identified as Sandworm, which multiple government and third-party entities have linked to the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation, abbreviated as G.R.U. and commonly known as GRU.<sup>6</sup>

Many aspects of KAMACITE's operations and tradecraft have remained remarkably similar during the past six years. Dragos assesses that KAMACITE serves as ELECTRUM's access team, focusing on gaining footholds in target networks. Although KAMACITE has not directly caused an ICS disruptive event according to Dragos analysis, the group is responsible for enabling other adversaries, such as ELECTRUM, to deliver ICS-specific disruption with access operations.

Dragos has determined that KAMACITE has facilitated ICS-specific operations leveraging its BLACKENERGY2 malware. BLACKENERGY malware first emerged in 2007 and subsequently inspired or provided the foundation for three malware families: BLACKENERGY2, BLACKENERGY3, and GREYENERGY. Of these, BLACKENERGY2 is one of a few malware samples to be publicly identified with built-in ICS capability. Though BLACKENERGY2 had ICS capabilities it was BLACKENERGY3 which served as the access tool to the IT networks that allowed the adversary to pivot to OT networks and orchestrate the 2015 cyber attack on Ukraine's electric system.

In 2021, Dragos uncovered two new GREYENERGY dropper variants in the wild: one in March of 2021, and another in August 2021.



**Dragos's continual discovery of new GREYENERGY files in the wild demonstrates that KAMACITE continues its development of GREYENERGY to further its operations.**

**KAMACITE may be using all GREYENERGY components in conjunction with other actions and tools to facilitate more disruptive ICS attacks. ICS asset owners and defenders should view all components of GREYENERGY as possible mechanisms with the ability to enable an ICS-focused attack.**



### KAMACITE

#### Target Geography

United States, Ukraine, and other parts of Europe

#### Victimology

Electricity, Oil & Gas, Industrial

#### Malware

BLACKENERGY 2/3, GREYENERGY

<sup>6</sup> AG-2021-01: KAMACITE



# 2021's New Activity Groups



KOSTOVITE



PETROVITE



ERYTHRITE



## KOSTOVITE

A major renewable energy operation and maintenance (O&M) firm was compromised and engaged the Dragos incident response team. Dragos deployed a team of investigators to analyze the intrusion and determined that the O&M company was not an opportunistic target. This narrative is the background behind the investigation into the purposefully executed intrusion by the activity group Dragos now tracks as **KOSTOVITE**.

The Dragos incident response investigation for KOSTOVITE's O&M provider target showed that KOSTOVITE reached Stage 2 of ICS Kill Chain capabilities with confirmed access into the O&M firm's OT networks and devices. In March 2021, when KOSTOVITE compromised the perimeter of this renewable energy O&M network, it exploited a zero-day vulnerability in the popular remote access solution Ivanti Connect Secure, formerly known as Pulse Secure. KOSTOVITE is an adversary with significant tactics, techniques, and procedures (TTP) and technical overlaps with the threat group known as UNC2630.<sup>7</sup> UNC2630 is a group with a history of access operations and data theft and is associated with the use of 12 malware families deployed exclusively on Ivanti VPN appliances.

KOSTOVITE used dedicated operational relay infrastructure against this target to obfuscate the origin of its activities and then stole and used legitimate account credentials for its intrusion. KOSTOVITE then used the stolen account information to move laterally and gain access to the OT environments of multiple energy generation facilities in North America and Australia from the one single ingress location. Once past the perimeter ingress, KOSTOVITE used only what is referred to as the target's organic infrastructure, meaning no tools or code from outside the target's network, to move laterally across target infrastructure. This adversary then accessed servers the renewable energy provider used for monitoring and control. In the course of the investigation, the Dragos analysts determined the adversary had been undetected and active in the OT networks for at least a month.

<sup>7</sup>Re-Checking Your Pulse: Updates on Chinese APT Actors Compromising Pulse Secure VPN Devices – Mandiant

### Target Geography



#### Industries

Renewable Energy

#### Malware type

Highly customized webshells

#### ICS Cyber Kill Chain

Stage 2, Develop

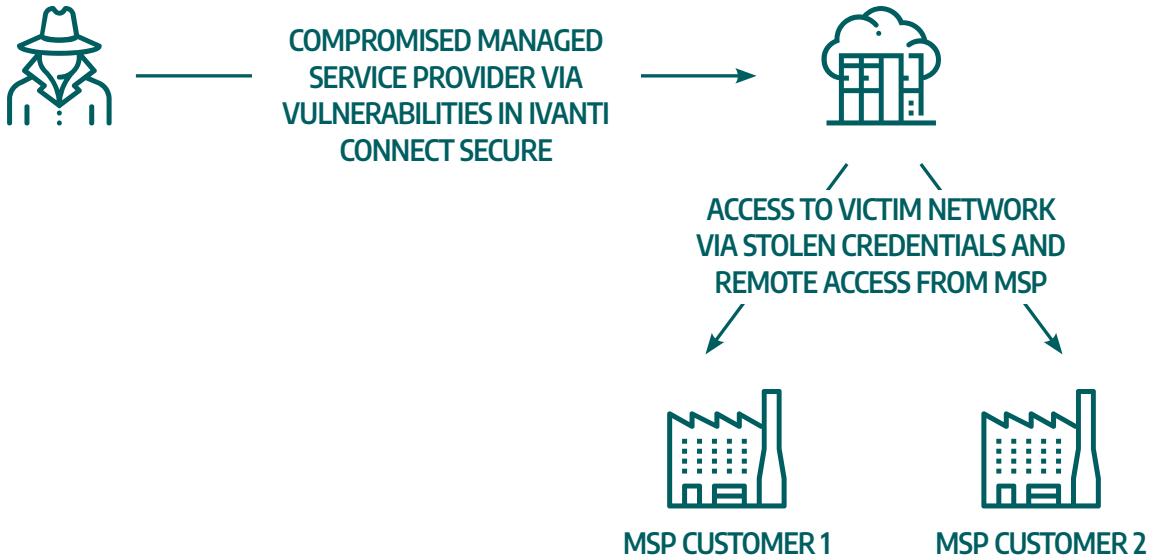
Organic target network Living Off the Land

## MITRE ATT&CK for Enterprise and ICS

<b>T0884</b>	Connection Proxy
<b>T0819</b>	Exploit Public-Facing Application
<b>T1505</b>	<b>.003</b> Server Software Component: Web Shell
<b>T0859</b>	Valid Accounts
<b>TA0006</b>	Credential Access
<b>T0817</b>	Drive By Compromise
<b>T1555</b>	Credentials from Password Stores
<b>T0822</b>	External Remote Services
<b>T1078</b>	Valid Accounts
<b>T1078</b>	<b>.003</b> Valid Accounts: Local Accounts
<b>T1078</b>	<b>.002</b> Valid Accounts: Domain Accounts
<b>T0806</b>	Brute Force I/O
<b>T0858</b>	Change Operating Mode
<b>T0840</b>	Network Connection Enumeration
<b>T0888</b>	Remote System Information Discovery
<b>T1614</b>	System Location Discovery
<b>T1602</b>	Data from Configuration Repository
<b>T0807</b>	Command-Line Interface
<b>T1021</b>	<b>.001</b> Remote Services: Remote Desktop Protocol
<b>T1021</b>	<b>.004</b> Remote Services: SSH



# KOSTOVITE



The **KOSTOVITE** intrusion highlights the risks of many single-point-of-failure perimeter defenses, particularly remote access devices exposed to the internet. It also shows what a skilled and operationally disciplined adversary can achieve in poorly segmented OT and ICS environments when there is minimal monitoring for adversarial lateral movement, masquerading of accounts, and living-off-the-land (LoL) intrusion techniques.



# PETROVITE

Dragos is currently tracking a Stage 1 ICS Cyber Kill Chain adversary identified as **PETROVITE**. PETROVITE demonstrates Stage 1 of the ICS Kill Chain capabilities and targets mining and energy operations in Kazakhstan. The overlaps with other activity groups and consistent capability development could lead to more targeted ICS incidents beyond general system reconnaissance and collection. While Dragos cannot connect PETROVITE to any known, disruptive event, the group remains active and continues to display an interest in collection on ICS/OT systems and networks.

 **Dragos is aware of targeted operations that started during the third quarter of 2019 and have intermittently continued throughout 2021.** Intrusions during 2019 used compromised legitimate infrastructure in Kazakhstan, whereas intrusions during 2021 focused on compromising legitimate infrastructure in other parts of the world.

## Target Geography



### Sectors

Critical Manufacturing, Energy

### Malware

ZEBROCY/  
ZEKAPAB

### Industries

Mining, Electric - Generation

### Infrastructure

Legitimate, compromised third-party infrastructure

### ICS Cyber Kill Chain

Stage 1, Actions on Objectives

## MITRE ATT&CK for Enterprise and ICS

<b>T1589</b>	.002	Gather Victim Identity Info: Email Addresses
<b>T1591</b>	.100	Gather Victim Org Info: Determine Physical Locations
<b>T1584</b>		Compromise Infrastructure
<b>T1566</b>	.100	Phishing: Spearphishing Attachment
<b>T1059</b>	.003	Command & Scripting Interpreter: Windows Command Shell
<b>T1053</b>	.005	Scheduled Task
<b>T1547</b>	.100	Boot or Logon Autostart Execution: Keys / Startup Folder
<b>T1140</b>		Deobfuscate/Decode Files or Information
<b>T1480</b>		Execution Guardrails
<b>T1036</b>		Masquerading
<b>T1056</b>	.100	Input Capture: Keylogging
<b>T1083</b>		File and Directory Discovery
<b>T1082</b>		System Information Discovery
<b>T1033</b>		System Owner/User Discovery
<b>T1113</b>		Screen Capture
<b>T1074</b>	.100	Data Staged: Local Data Staging
<b>T1071</b>	.100	Application Layer Protocol: Web Protocols
<b>T1573</b>	.002	Encrypted Channel: Asymmetric Cryptography
<b>T1132</b>	.100	Data Encoding: Standard Encoding
<b>T1041</b>		Exfiltration Over C2 Channels



# ERYTHRITE

The new **ERYTHRITE** Activity Group demonstrated Stage 2 of the ICS Cyber Kill Chain in one of its compromises. ERYTHRITE targets organizations in the U.S. and Canada. 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. ERYTHRITE has been active since at least May of 2020.

ERYTHRITE performs highly effective search engine poisoning and deployment of credential stealing malware. Their malware is released as part of a rapid development cycle designed to be evasive to endpoint detection. ERYTHRITE has technical overlaps to another group multiple IT security organizations have labeled as Solarmarker.<sup>8</sup>

Dragos's findings are generally in agreement with a 2021 third-party security research report<sup>9</sup> which posits that during 2021 Solarmarker malware compromised approximately 20 percent of Fortune 500 companies. ERYTHRITE's wholesale exfiltration of credentials poses a particular risk to victims that use common authentication systems or credentials in their IT and ICS/OT environments, an exposure Dragos investigators found all too often in multiple ICS incident response investigations.

In ERYTHRITE's most recent Search Engine Optimization (SEO) poisoning campaign they used a two-pronged approach that began with uploading specially crafted Portable Document Format (PDF) documents to otherwise legitimate websites which in turn linked to malware delivery sites. ERYTHRITE leveraged the popular WordPress plugin Formidable Forms to upload hundreds of malicious PDFs loaded with thousands of keywords. These keywords were optimized for search engine crawling so that the SEO poisoned PDFs hosted on the otherwise legitimate but subverted websites appeared at the top of a search. When Dragos reached out to the owner of one subverted website, the owner confirmed that the adversary abused an unprotected Formidable Forms-based contact form, enabling arbitrary file uploads. Dragos assesses with

<sup>8</sup>Threat Spotlight: Solarmarker – Talos Intelligence; <sup>9</sup> Solarmarker In-depth Analysis – Prodaft

## Target Geography



### Industries & Sectors

All  
ICS Cyber Kill Chain  
Stage 2, Develop

### Malware

Malware and SEO poisoning,  
possible affiliate-based  
operation model

### Infrastructure

Command and Control (C2) and  
affiliate/panel management  
hosts in St. Petersburg and  
Moscow, Russian Federation,  
and reverse proxies/load  
balancers in France, Germany,  
Switzerland, Denmark,  
Romania, Canada, and the U.S.

## MITRE ATT&CK for Enterprise and ICS

<b>T1016</b>	System Network Configuration Discovery
<b>T1033</b>	System Owner/User Discovery
<b>T1036</b>	Masquerading
<b>T1041</b>	Exfiltration Over C2 Channel
<b>T1049</b>	System Network Connections Discovery
<b>T1055</b>	Process Hollowing
<b>T1059</b>	PowerShell
<b>T1059</b>	Windows Command Shell
<b>T1071</b>	Command and Control (C2) Over Web Protocols
<b>T1082</b>	System Information Discovery
<b>T1127</b>	Trusted Developer Utilities Proxy Execution
<b>T1140</b>	Deobfuscate/Decode Files or Information
<b>T1189</b>	Drive-by-download
<b>T1217</b>	Browser Bookmark Discovery
<b>T1547</b>	Registry Run Keys / Startup Folder
<b>T1547</b>	Shortcut Modification
<b>T1555</b>	Credentials from Web Browsers
<b>T1560</b>	Archive via Utility
<b>T1564</b>	Hide Artifacts
<b>T1574</b>	Hijack Execution Flow



## ERYTHRITE

moderate confidence that ERYTHRITE has misused the unprotected Formidable Forms contact pages of multiple other websites.

These SEO tactics may use a variety of methods such as “cloaking” or “link farming” to increase the page rank of ERYTHRITE optimized search terms. Search engine algorithms rank the importance and trustworthiness of content based in part on the number of links to a web page. Unfortunately, in this case, it leads to a malicious PDF.



**Dragos assesses with moderate confidence that ERYTHRITE will continue to compromise and steal credentials and data from organizations leaving their OT environments vulnerable to further compromise by ERYTHRITE or others.**

# Ransomware and Industrial Infrastructure

2021 was a pivotal year for ransomware gangs and their affiliates, with ransomware becoming the number one cause for compromises in the industrial sector. Of all the industrial sectors in 2021, ransomware groups targeted the manufacturing industry more than any other, nearly twice as much as the other industrial groups combined.

## THE UNINTENDED AND INTENDED RANSOMWARE THREATS TO OT

In many industrial sector compromises, weak boundaries between OT and IT, and poorly understood interactions between these systems, coupled with the rise in remote access (as more organizations rely on their work-from-home staff), have increased the overall risk. While ransomware mainly targets enterprise IT systems, there are a number of instances when it does impact OT directly and in integrated IT and OT environments.

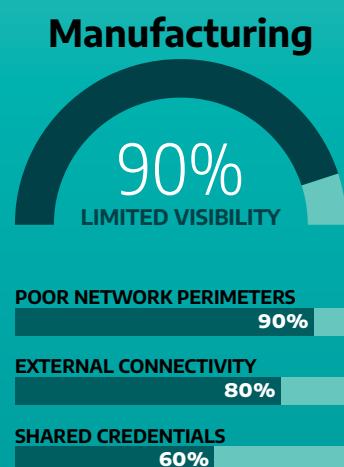
Some ransomware adversaries indirectly impact OT when attacking enterprise IT. Once adversaries achieve initial access, they can execute ransomware to gain a foothold in critical enterprise IT systems and potentially move laterally into OT systems. After compromising an organization, they demand ransoms that require victims to pay for the keys to decrypt their files. Often targets have little recourse to restore functionality to their systems.

Conversely, some ransomware groups specifically target OT systems. EKANS is a specific ICS-targeted ransomware that in 2020 targeted companies across electric, oil and gas, medical and pharmaceutical manufacturing, and automotive sectors. Dragos analyzed multiple variants of EKANS malware and discovered that the EKANS variant has the ability to stop ICS-related Windows processes before initiating encryption.

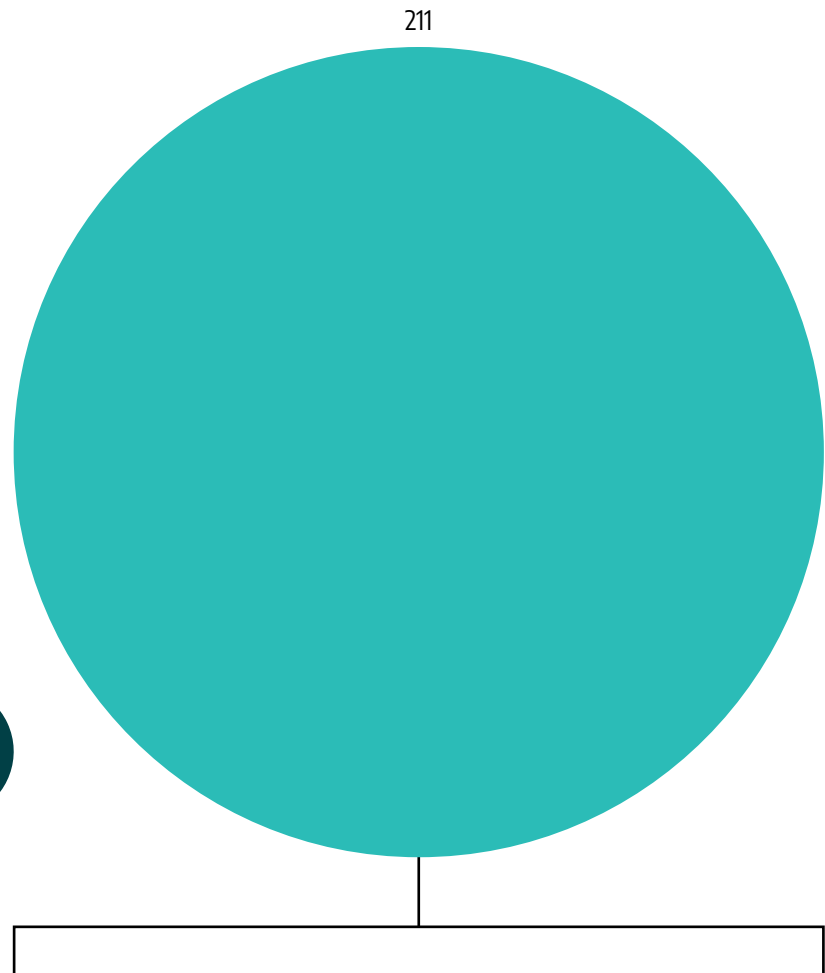
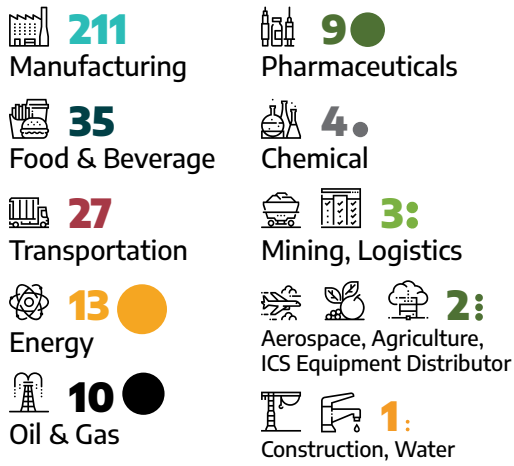
## INDUSTRIAL SECURITY RANSOMWARE TRENDS

Analyzing industrial security trends during 2021, Dragos compiled data on these ransomware sectors: Manufacturing accounted for 65%, with Food & Beverage coming in second (11%), and Transportation third (8%). When analyzing manufacturing subsectors, Dragos found that Metal Components (17%), Automotive (8%), and Technology (6%) were the most common.

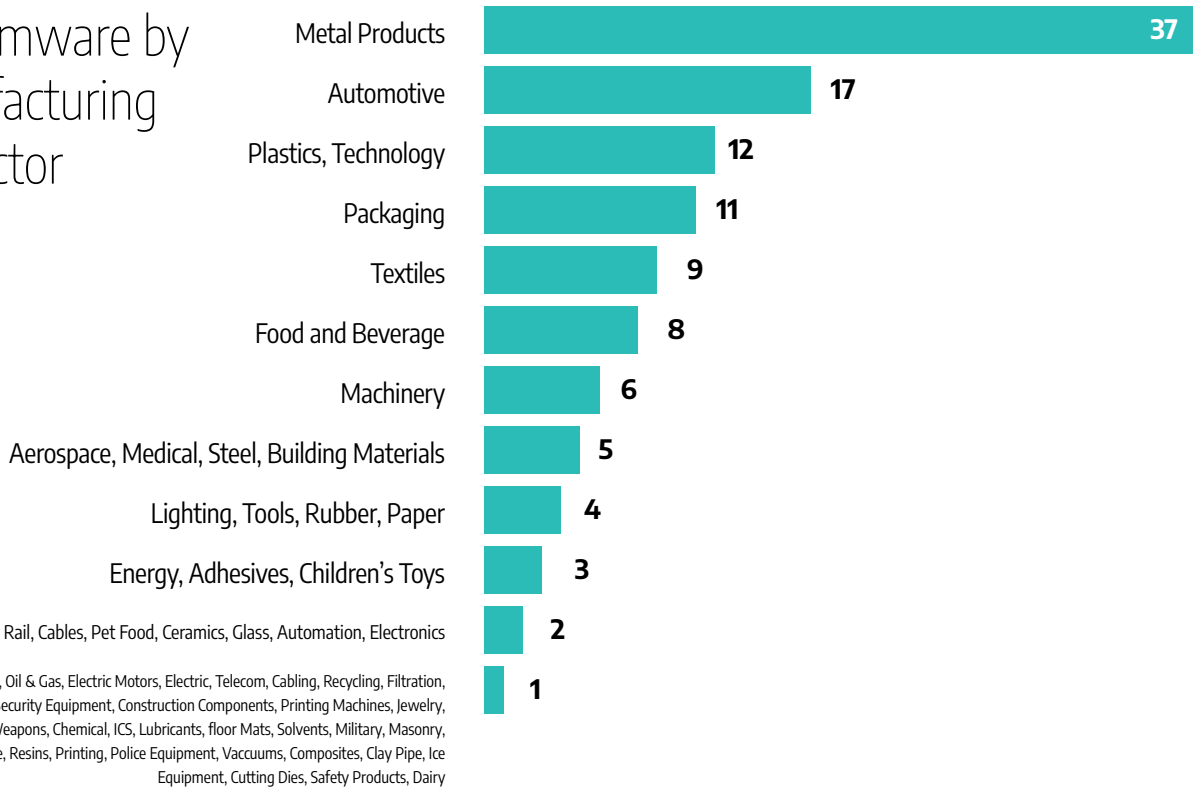
**These are troubling trends when paired with the Dragos services team finding that the manufacturing sector is often the least mature in their OT security defenses.**



# Ransomware by ICS Sector



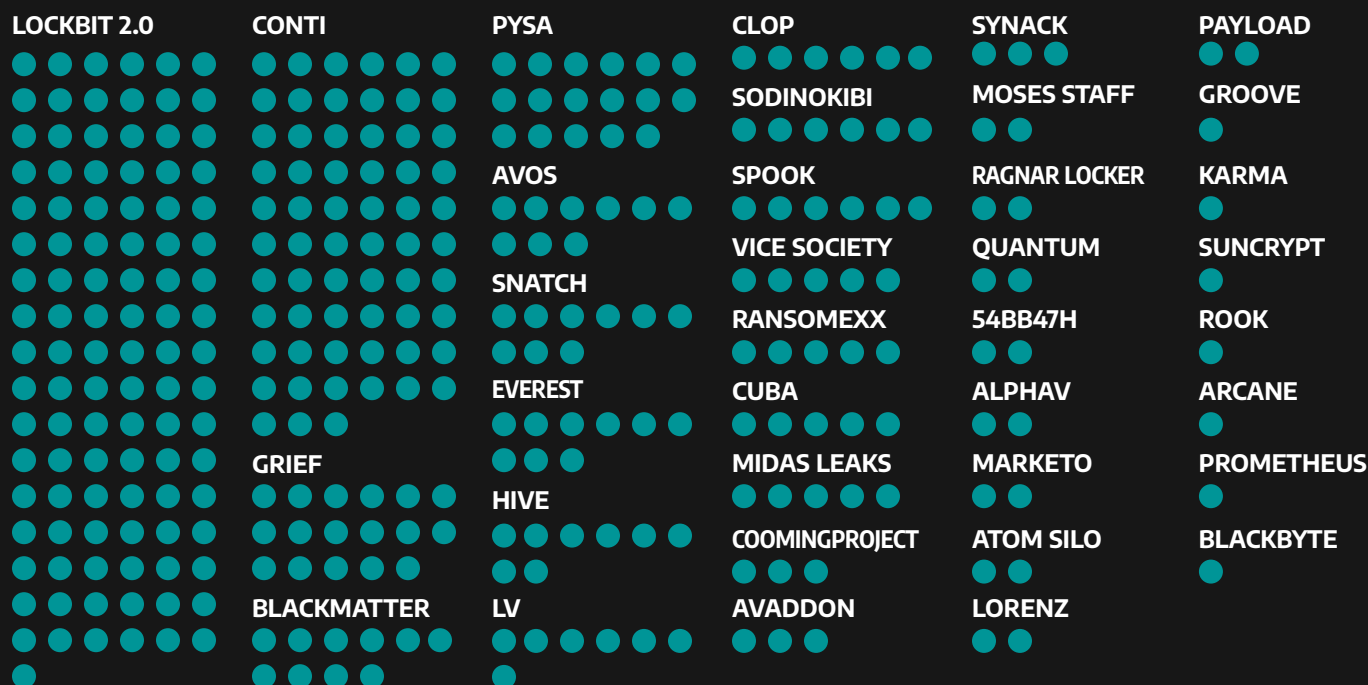
# Ransomware by Manufacturing Subsector





# Ransomware Incidents by Group/Strain

● = 1 RANSOMWARE ATTACK



## RANSOMWARE INCIDENTS BY GROUP: CONTI AND LOCKBIT 2.0

Two ransomware groups, Conti and Lockbit 2.0, caused 51 percent of the total ransomware attacks, with 70 percent of their malicious activity targeting manufacturing. Conti dates to 2020, with recent confirmed attacks targeting CS Energy and Shutterfly. In June of 2021, Lockbit 2.0 retooled and now focuses on stealing data and extorting victims for financial gain by threatening publication of exfiltrated data if victims do not pay the ransom. In 2021, Lockbit 2.0 claimed to possess the data of energy equipment supplier Schneider Electric, according to a post on Lockbit 2.0's dark web forum. The compromise was never confirmed, and the posted Schneider Electric data appears to have come from a previous attack on Vestas, a Danish wind turbine manufacturer.

## WHY WERE RANSOMWARE GANGS SO SUCCESSFUL IN 2021?

This spike in ransomware attacks can be attributed to the ransomware-as-a-service (RaaS) phenomena. However, another key factor is the digital transformation of the industrial sectors and the increased connectivity between IT and OT. Ransomware gangs like Conti and Lockbit 2.0 have mobilized an underground marketplace where their developers outsource operations to affiliates who execute the attacks. Affiliates do not require high-level technical expertise because the ransomware software has been developed and they can purchase access to systems and hackers for hire, which significantly lowers barriers to entry.

## THE GROWING MATURITY OF RANSOMWARE AS A BUSINESS

With ransomware actors having fewer barriers to entry the financial impacts are becoming higher for the industrial sectors. Typically, ransomware groups threaten to release exfiltrated corporate and personal information before encrypting the target filesystems, then dump the information on dark web leak sites. During the first half of 2021, the average remediation costs of ransomware attacks against ICS sectors continued to rise from downtime, staffing, disruption to device and network operations, lost business opportunities, and paid ransoms.

DarkSide (now rebranded as REvil) offered customer service with real-time chat support and brought in at least \$60 million before it announced it was closing its operations. Investing in their business, ransomware gangs are funding research and development, which is fueling their industry as their extortion methods become more extreme.

Ransomware trends are likely to continue shifting as groups reform, reprioritize, and law enforcement pursues them and takes them offline. As groups disband and reform, there is a blending of ransomware strains, and a greater likelihood that more strains with ICS/OT capabilities will be developed in 2022.

## LOOKING AHEAD INTO 2022



**Dragos assesses with high confidence that ransomware will continue to disrupt industrial operations and OT environments, whether through the integration of OT kill processes into ransomware strains, the existence of flattened networks to prevent ransomware from spreading into OT environments, or through operators shutting down OT environments as a precaution while they attempt to stop IT ransomware from spreading to OT systems.**

**Dragos assesses with low confidence that state-sponsored adversaries may leverage ransomware to mask their alternate operations, for theft of intellectual property (including key OT schematic details), for reconnaissance of target networks, and for other Stage 1 components of the ICS Cyber Kill Chain.**

**Finally, Dragos assesses that ransomware actors' extortion techniques will continue to grow in severity and intensity as adversaries deploy any means available to pursue their ransom payments.**

SECTION TWO

---

# **Dragos Frontline Perspective**

## Lessons Learned from Incident Response

A cybersecurity incident is a crisis for any organization. However, cyber attacks targeting industrial organizations, including ransomware, have the potential to disrupt operations and pose safety risks if not swiftly mitigated. Incident response is rarely an inexpensive endeavor in terms of money, people, operational disruption, or time.

The Dragos Incident Response team helps organizations prepare for, respond to, and recover from cyber incidents in industrial environments. Our team of experienced incident responders have consulted on numerous cases where significant time and resources could have been saved with preparation. As an example, many of the questions that organizations want answered are best answered through network traffic analysis that cannot be obtained after the attack if the environment was not configured to collect that data or tools used to provide those insights had not been deployed prior to the incident. A key point is that while preparation ahead of an incident is always core in IT or OT incident response it is much more important in OT incident response because of the unique nature of the environments and questions to be answered.

The following topics showcase some lessons learned from our field engagements in 2021 that may help organizations avoid some of the most common issues that increase the time, personnel, downtime, and expense of managing a cybersecurity incident.



# Lessons Learned from the SolarWinds Compromise

In December 2020, the SolarWinds Orion breach was reported. Initially, it was not clear how the SolarWinds breach affected ICS/OT environments. It is common knowledge that SolarWinds Orion is an IT infrastructure monitoring platform. It was not well understood, however, that several Managed Service Providers (MSPs) also use the tool to monitor their customer ICS/OT environments. Additionally, many industrial OEMs embed the software as part of their management offerings and some of the largest OEMs use the tool to monitor service and maintenance access. As a result, many ICS/OT environments were compromised directly with the software installed in their environments or indirectly through their third-party agreements despite not directly installing SolarWinds in their own environment.

Both detection and documentation are crucial to incident response. The sooner an incident is detected, the sooner you can stop an adversary from accomplishing their objectives—which often includes severe financial damage to the target organization. Documenting an incident improves incident response workflows as well as the effective remediation and lessons learned afterward. If organizations do not properly document incidents and findings, they cannot learn from these events and will continue to make the same mistakes.

**Beginning in January 2021, the Dragos incident response team responded to several SolarWinds compromise cases. Aggregated across these cases the lessons learned were consistent for organizations to protect themselves from this style of supply chain risk:**



Monitor and log internal (East/West) communications within the industrial environments.



Monitor and log perimeter (North/South) communications along all perimeters, including third party connections.

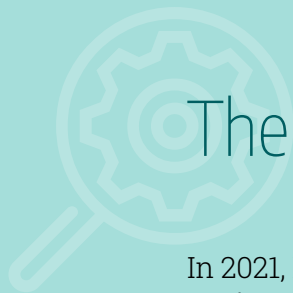


Customize and test your ICS/OT Incident Response Plan, don't rely on your IT Plan.



Know what data exists to support your detection, analysis, and hunting capabilities.<sup>10</sup>

<sup>10</sup> Learn more [here](#).



# The Value of Root Cause Analysis

In 2021, Dragos responded to a few incidents that resulted from malfunctioning equipment or software, rather than adversaries. In each case, the impacted organization made the right call by activating their incident response plans and identifying possible root causes that may have impacted plant processes. These engagements all proved the importance of analyzing the network traces caused by malicious activities with awareness of the OT protocols used and the industrial processes controlled by the systems investigated. The collaboration between internal security and operations teams, external responders, and in some instances ICS vendors is key to a successful root cause analysis (RCA).

## Who Changed the Setpoints?

In one case, Dragos responded after an electric power transmission site observed an unauthorized setpoint change that resulted in a limited impact on operations and was quickly remediated. The command resembled a global test command run annually, but there was no test at the time. Because the edge devices used at the site are radio-controlled, it was feared that the unauthorized command might have been sent via a Man-in-the-Middle attack. The organization did the right thing and launched an official investigation of the incident and retained Dragos to help with incident response and root cause analysis of the event.

The team of incident responders deployed the Dragos Platform to collect network telemetry to monitor for potential, ongoing malicious activities. The incident response team identified identical commands issued to the edge devices. As the Dragos Platform captured the traffic, responders were able to identify the host responsible for issuing the commands and proceeded to collect forensic data and perform analysis. The team discovered that the command was issued by the actual control software after the server rebooted. They contacted the OT vendor to help investigate the root cause and the vendor found a programming error caused by an edge-case configuration. Within two weeks from the point of contact, the vendor had a fix for the software issue and deployed it to the customer environment shortly thereafter.



While this event was not a security breach, it highlights the value of network security monitoring and root cause analysis beyond the cybersecurity use case. A complex issue was detected and the root cause was determined in a matter of days. However, if the monitoring had been in place at the affected site prior to the incident, the resolution would have come more quickly.

This case also demonstrates the value of strong relationships with your most important OEMs and third-party vendors. The positive relationship between the client, the OEM of the affected equipment, and Dragos enabled the joint team to quickly identify the root cause and identify and implement a solution.

### **NEED FOR MONITORING AND INCIDENT RESPONSE PLANS**

Had this been an actual cyber attack, the setpoint changes could have had more devastating effects. Because of a lack of monitoring network traffic, the point of origin from which the setpoints were changed would not have been identified and would have to have been tediously hunted for using host forensic analysis. In most cases, the collection of forensic artifacts from hosts in ICS environments is a manual process that requires you to weigh the potential impact of this process against the downtime of systems that control important physical processes.

Because the safety and reliability of ICS operations is the priority, forensic data collection often takes place over an extended period of time. As a result, some important data may be overwritten, which is another reason why continuous network monitoring is so important in ICS operations. Monitoring that is aware of the industrial protocols that are used in a specific environment allows defenders to make sense of interactions of the IT layer and with the physical layer of operations, such as the industrial process itself.



# The Ghost in the Power Generator

In another case, Dragos was called in for an incident that was also deemed to be operations related with no adversary involvement. One night, unexpectedly, the gas-powered turbines at a peak power generation site suddenly turned on and went into idle. The SCADA operations had not issued the command for the site to go online. The company appropriately activated its incident response retainer and Dragos personnel immediately went to the site. Because no ICS network monitoring was in place at the site, Dragos responders had to rely on logs and host data. Working with the local operations crew, our response team conducted a walkthrough inspection of the site.

The determination was made that the commands to activate the control loop to start the generator most likely came from the HMI housed in a small shed-like facility. There were no remote connections, so the team considered direct action. However, security cameras did not show anyone approaching the HMI or the shed. The Dragos incident response team did identify moisture on the HMI and noticed it was a touch screen that was also set to be abnormally bright.

Because of compliance and warranty concerns no non-native tools were allowed to be used on the HMI. Therefore, the Dragos incident response team improvised by deploying MS Paint on the system as it is a native and signed binary. The team left the system running overnight and in the morning was able to identify large brush-like movements on the HMI. The responders were able to use MS Paint to confirm that the moisture was causing “clicks” on the touchscreen HMI that resulted in kicking off the control loop while the generator was down for maintenance.

Had ICS network monitoring been in place at the site, malicious activity could have been ruled out as a root cause much faster by confirming or ruling out any remote access to the HMI, potentially enabling the local operations team to identify the actual cause without having to call in external responders. Further, the commands from the HMI would have been immediately observed by the operations staff leading to less lost time and quicker root cause analysis on an operations issue.

This case also shows the importance of being on site during ICS incident response to accurately assess the environment and understand the situation. This awareness, combined with experience and out-of-the-box thinking, can lead to the quick resolution of a case versus relying only on logs and forensic data.





# Never Let an Incident Response Team's First ICS Be Your ICS!

An electric operator contacted Dragos to conduct an incident analysis after they experienced a ransomware attack on a control center for renewable energy. Dragos was the second team retained to respond to the case, after the first analysis left many questions unanswered.

The adversary leveraged an internet-connected SCADA server listed on Shodan.io, harvested credentials on this system, and then moved laterally through the environment. Because of a weak security posture and no network segmentation, the adversary gained access to the domain controller and other key systems at the plant. After manually exploring the environment and manipulating some systems to facilitate data infiltration and exfiltration, the adversaries went silent. A week later, the adversary executed the ransomware attack where they deployed scripts and tools to weaken the company's defenses, such as Microsoft Defender, and deployed ransomware through the Group Policy, WinRM, and PSEXEC-as-a-service to most systems on the network. The adversary also performed some anti-forensics measures by clearing the Windows event logs and disabling further logging. While they took their time initially exploring and mapping out the environment, the actual attack of manipulating its defenses to deploying and executing the malware happened in about an hour.

The organization immediately realized something was wrong when applications failed and computer systems stopped responding. They quickly called in an incident response provider who did not have experience in ICS incident response. The provider ran antivirus programs on the affected systems, which deleted data that would have facilitated root cause analysis and did not result in recovering any data encrypted by the ransomware. They additionally spent time performing vulnerability scans across the environment which can be extremely risky in ICS/OT networks.

## In this and similar engagements, the key takeaways are:



Ensure you have separate Incident Response Plans (IRPs) in place for IT and ICS/OT.



Set up incident response retainers as part of your IRPs.

Engaging outside help during an incident could cause you to select inadequate support when you need it fast.



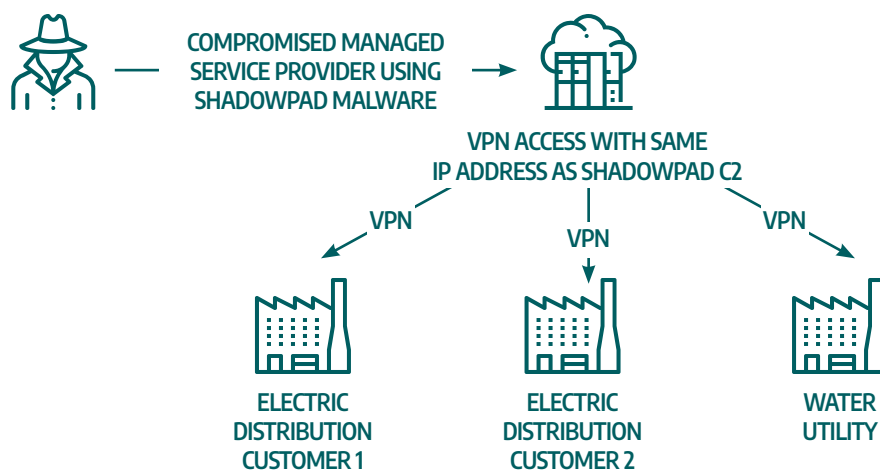
When interacting with an OT environment, comprehensive knowledge of industrial control systems is a must. For example, pausing or even fully stopping or removing computer systems from an OT environment could impact the safety and reliability of the operations.



Do not run antivirus programs on industrial control systems to "remove" a malware infection. The antivirus malware deletion attempts result in incomplete removal of the malware and files for essential OT operations could be deleted. Systems must be in a verifiable good state for safe, reliable operation of the ICS. Compromised computer systems in an ICS/OT environment should always be rebuilt from known good backups or golden images.

# AN MSP CASE STUDY

## AN ICS/OT SERVICE PROVIDER IS COMPROMISED



In April 2021, Dragos identified the compromise of an industrial Managed Service Provider (MSP) and OT software vendor based in South Asia with a worldwide customer base. The MSP was compromised by multiple persistent Shadowpad malware infections on multiple internet egress points used by the MSP. The Shadowpad malware C2 was associated with an adversary that had infrastructure overlaps with a threat group tracked by another company labeled as RedEcho.<sup>11</sup>

Dragos observed in internet telemetry that this MSP had ongoing VPN tunnels with multiple prominent electric and water utility customers in the United Kingdom. Dragos confirmed that the VPN connections were legitimate tunnels used by the South Asian MSP to provide contracted service for their utility customers. These VPN connections were temporally correlated with, and using the same network egress points, as the Shadowpad malware C2 traffic.

While Dragos could not confirm that the adversary had direct access to the MSP's UK-based electric and water utility customer networks through the VPN tunnels, the C2 malware activity on the same MSP networks as the VPN connections to the MSP utility customers clearly represented increased risk to UK critical infrastructure. Dragos notified the MSP and the affected MSP customers via the national CERTs. Initially the MSP downplayed the compromise, stating it was likely incidental malware that already had been removed.

After more discussion where the Dragos Intel team explained that the indicators and behaviors identified matched those of an ongoing threat group, the MSP contacted Dragos to share they hired an incident response provider to perform analysis and mitigation. During the conversation, Dragos learned that the incident response was limited to identifying the systems actively communicating with the adversary's C2 infrastructure and the remediation efforts focused on removing malware with antivirus software. Unsurprisingly, more Shadowpad C2 communication from the MSP reappeared just a few weeks later.

***Continued next page>>>***

<sup>11</sup>China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions – Recorded Future

In the third quarter of 2021, Dragos observed the MSP shut down three of its broadband network connections affected by the Shadowpad malware, representing some 762 static internet IP addresses directly allocated to the MSP. The MSP moved services including the website and one of three previous firewalls to a different network with only a few dynamic IP addresses. Dragos assesses with low confidence that the network abandonment and migration by the MSP is related to the MSP discovering or understanding the extent of compromise.

## Key Takeaways

When performing incident response, following a proper process is important. Whether you are relying on an external incident response provider or have an internal team, always ensure they:

- **Determine the root cause of the intrusion into the OT environment.**
- **Develop a recommended course of action for the OT operations team to contain, mitigate, and eradicate.**
- **During all steps, ensuring the OT environment remains in a safe and reliable state is imperative.** Running antivirus software on OT computer systems with the intent to remove malware neither helps to effectively analyze a threat nor reliably removes it.

At best, this approach will remove malware partially from a system and will delete valuable forensic data while inspiring a false sense of security. The impacted network must be swept for additional compromised systems and any affected system should be rebuilt from clean backups or a golden image.

As an MSP, it is important to monitor all ingress and egress points on the network and monitor internal network traffic for unusual lateral movement. By now it is an established fact that adversaries will target MSPs to leverage trusted access to the adversary's advantage. Monitoring for any unusual activities is an important security measure to keep customers safe. Any access that can be switched to multi-factor authentication (MFA) should be addressed. Considering the operational constraints of an MSP, MFA might be difficult to implement at best and impossible at worst. As it is one of the most effective defensive controls, implementing MFA at least on all MSP-owned systems should be considered.

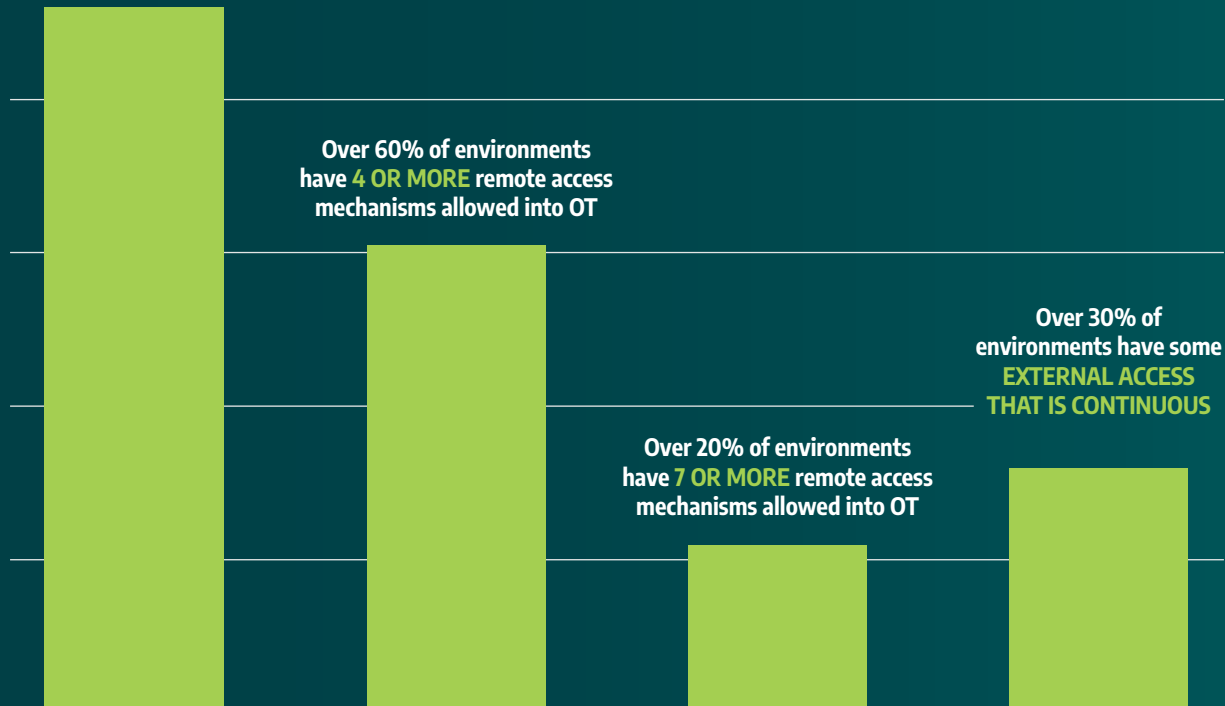
As an MSP customer, you should monitor all network segments and systems accessed by an MSP for any unusual activity such as administrative access outside of maintenance windows or access to systems that are not managed by the MSP. Dragos realizes this is easier said than done. At minimum, perform risk assessment when considering tasking to an MSP and establish that OT security monitoring is an effective method to minimize risk that needs to be factored into the business case.

# The Complexity of Remote Access in OT Environments

**OT Watch is an optional subscription to the Dragos Platform that enables our global hunt team to find unknown threats from our customers ICS/OT environments, gain additional visibility and insights, and provide guidance on vulnerability management.**

When the attack on the Oldsmar water treatment facility went public, the Dragos OT Watch team began a series of threat hunts looking for other unauthorized access from legitimate remote access solutions. Over the course of the threat hunt, the OT Watch team documented the following remote access solutions to shed light on what remote access looks like in OT and how that can cause a breach similar to Oldsmar and why remote access continues to be a security risk.

Over 90% of networks covered by OT Watch have **SOME FACET OF REMOTE ACCESS** in their industrial network segments.<sup>12</sup>



<sup>12</sup> As a point of clarification, OT Watch itself is an external connection out of the environment. We did not include OT Watch traffic in this analysis as it does not enable remote access to the monitored networks.

# We have classified remote access into the following two categories:

## OEM AND VENDOR

### REMOTE ACCESS SOLUTIONS:

Remote access solutions are a key component of modern OT equipment solutions, particularly during the pandemic when most organizations had to quickly shift to a remote workforce. Both standardized reference architectures and consistent remote access provide equipment to vendors and ensure the equipment functions as designed. Remote access solutions help provide timely resolution of problems system users may encounter and can increase the value of an asset owner's investment.

However, when implementing these types of solutions it is critical that the asset owners understand how each remote access method is used and consider the security posture of the asset that is being accessed.

**USE CASE:** First- and third-party connections are used for operations (dispatch, control, etc.), security services (monitoring, patching, antivirus, and other updates), and maintenance and diagnostics. These may be interactive access, are often persistent, and could be both.

**RISK:** The main risk is the potential for supply chain attacks that impact a considerable number of a vendor's customers where the service itself becomes the attack vector.

**STRATEGY:** Trust, but verify. Monitor and log all remote connections and have isolation playbooks as a component to your incident response plans.

## FACILITY DEPLOYED

### REMOTE ACCESS SOFTWARE

Another class of remote access solutions are one-off solutions such as Remote Desktop Protocol (RDP), TeamViewer, VNC (Virtual Network Computing), or PCAnywhere which are enabled or installed by the facilities—often with little to no oversight. Frequently this stems from groups of stakeholders working on different projects or acquiring new process assets through mergers, acquisitions, or other business consolidation events.

**USE CASE:** Allows both vendor and asset owner access while onsite or offsite. Often a remote access software solution like PCAnywhere is used as an onsite tool to remotely connect to systems in different buildings or rooms at the same location.

**RISK:** Misconfiguration can change an 'onsite' remote access tool to become a rogue remote access tool. Lack of oversight or documentation leads to end-of-life software, vulnerabilities, and unknown access methods.

**STRATEGY:** Monitor your east/west network traffic in addition to your north/south network traffic and be sure to enforce a remote access strategy, focused on chokepoints where possible, that enables staff to work safely.



**The critical take-away in our analysis of remote access solutions is to know what methods are in use and by whom, and to routinely audit and review your access logs for any irregularities. You should pay particular attention to remote access methods that do not have specific use cases or are overly broad. Often, remote access to the OT environments is persistent and there is no baseline understanding for what is and is not "normal vendor access."**

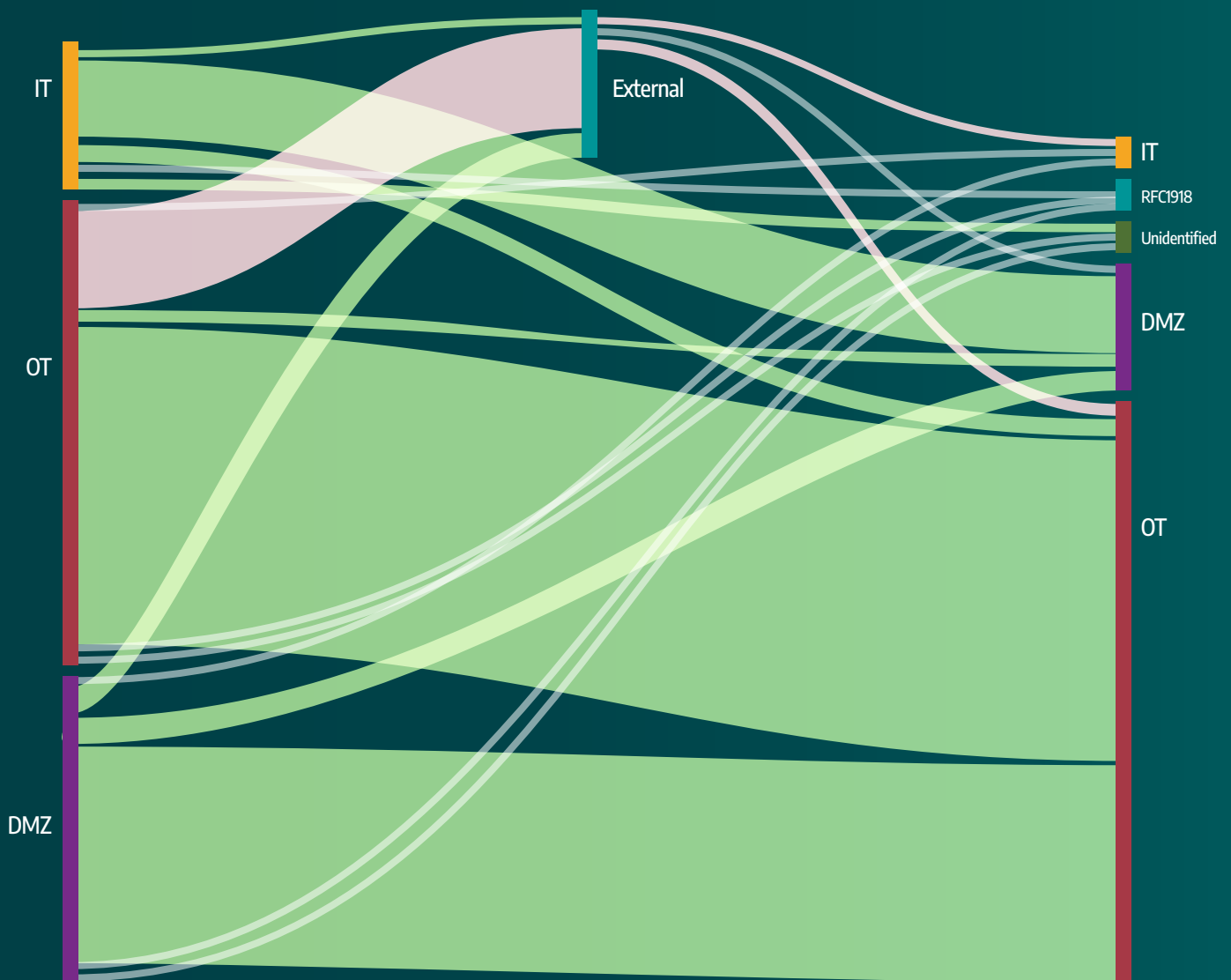
### REMOTE ACCESS INTO OT ENVIRONMENTS

Many customers believe their OT networks are accessible only from their enterprise IT environments, or they are completely separated. The data tells a different story.

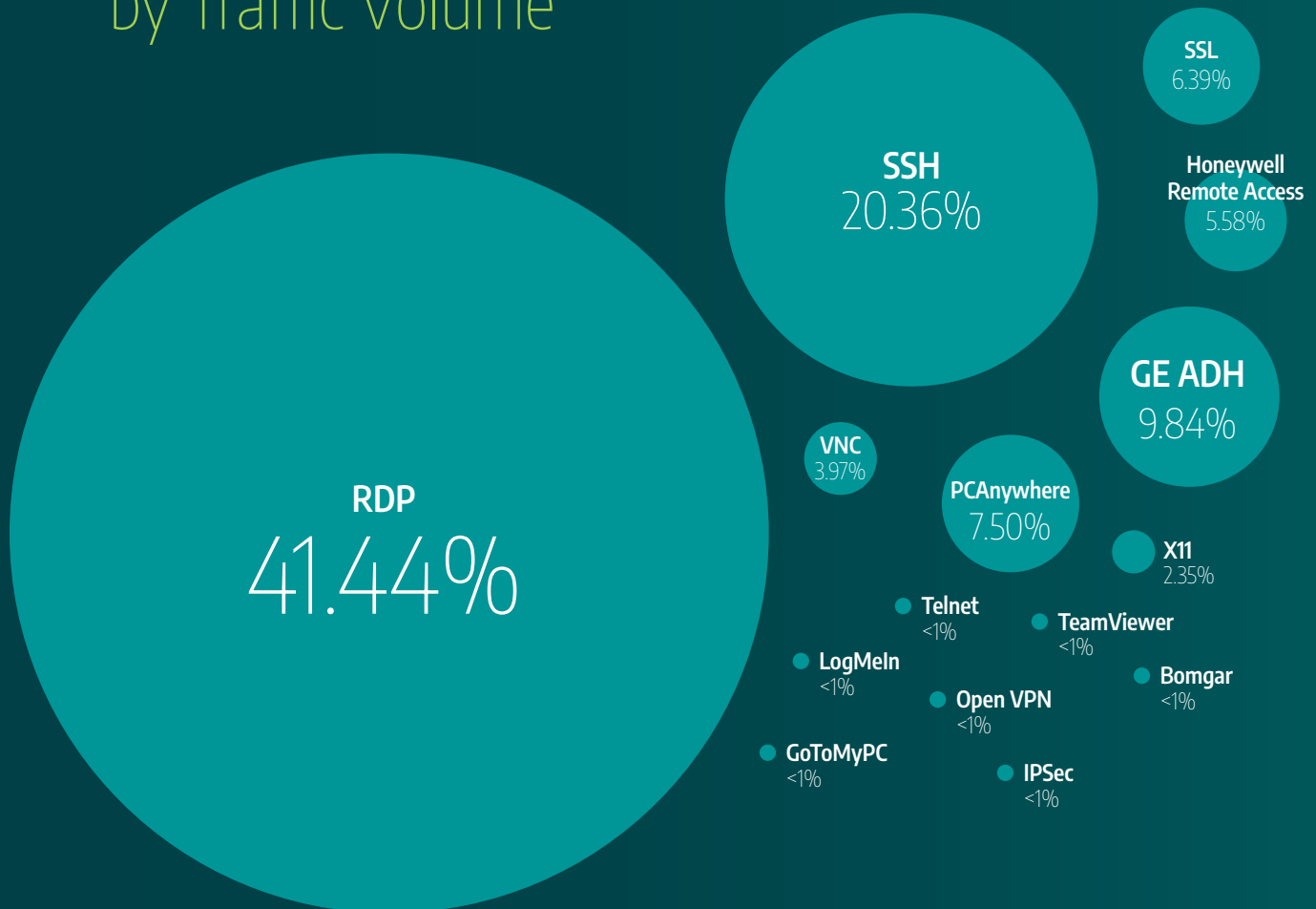
The following diagram shows a complicated architecture where multiple network segments have remote access to multiple network segments. Notably, the majority of remote access is not from the "Internet to OT" connection, but the connections between internal OT to OT systems. That said, a wide variety of sources and destinations exist between "IT to OT" and "OT to IT" connections.



The flows depicted in green are common and expected while the flows highlighted in pink are more interesting and need additional monitoring and auditing to ensure they are not being used improperly.



## Source to Destination Zone, by Traffic Volume



### DATA-DRIVEN INSIGHTS FROM THE FIELD

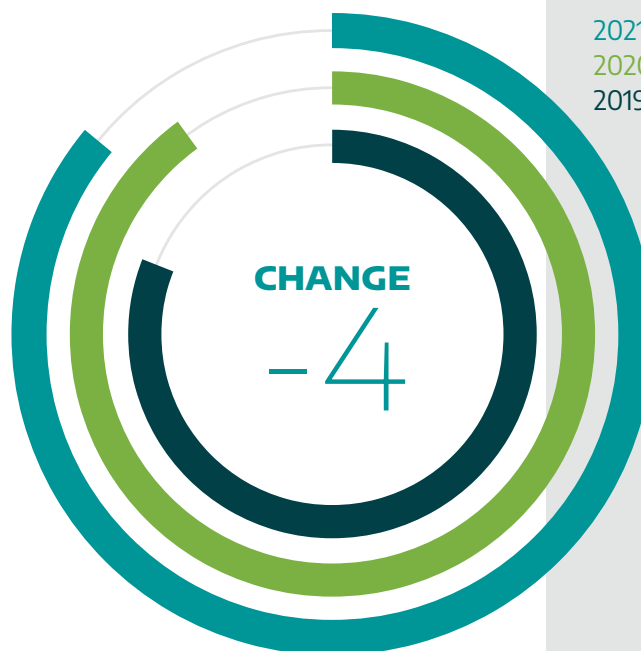
The physical consequences and impacts of a cyber attack on OT systems are exacerbated by the complex interdependencies between IT, OEM, and the cloud connections that are deeply entwined within operations environments. The Dragos team has been rank-stacking and comparing our findings year over year since 2017. Our key take-away: Dragos's new customers in 2021 had the same issues that our new customers had in 2020, who also had the same challenges as customers in the previous years. In some ways, this is good because it enforces that we understand what the top challenges are for the industrial community.



**TOP 4 KEY FINDINGS: ONE**

# 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.**



Visibility is more than asset inventory. When customers only monitor the IT to OT boundary without monitoring the activity inside the ICS network, Dragos considers this limited visibility. Frequently, defenders are blind to critical network traffic when they do not capture the OT communication flows, or they capture these flows but do not utilize ICS protocol dissection. Full visibility is achieved when network and device logs are centralized and can correlate various segments with network traffic analysis and asset inventories.

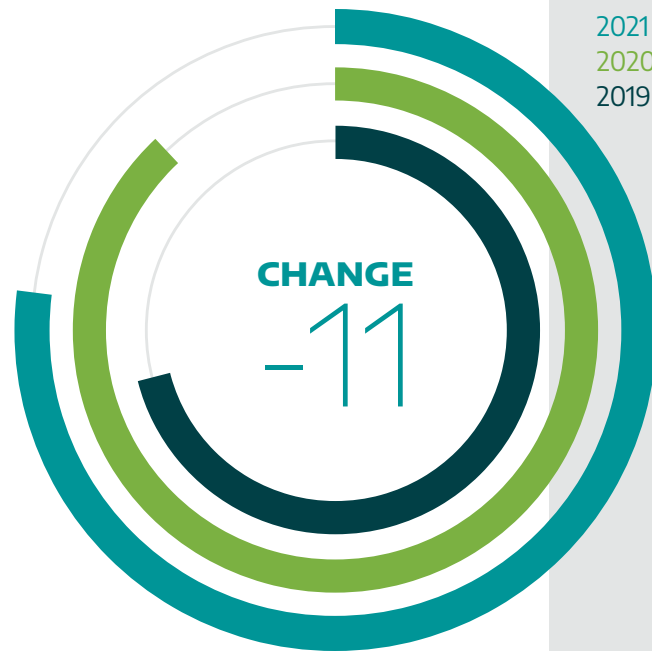
Defenders can see the full picture of what is occurring across their industrial assets and sites only with full visibility. Full visibility facilitates the identification of threats. Threat detection can come in many forms, but its major purpose is to emphasize behaviors that the human defender should be aware of such as ransomware, control manipulation, and safety manipulation. Threat intelligence provides the necessary context for threat detections so defenders can make the best defensive decisions. Early detections, with the appropriate context, enable defenders to rapidly execute response playbooks, which expedite response, containment, and remediation efforts.



**TOP 4 KEY FINDINGS: TWO**

## Poor Security Perimeters

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



For the last two decades, OT asset owners have concentrated their cybersecurity posture on prevention. Specifically, they rely on segmentation, firewalls, and DMZs to isolate their operational networks from the internet, corporate networks, and vendors. Yet, poor security perimeters continue to be a major problem for most OT asset owners.

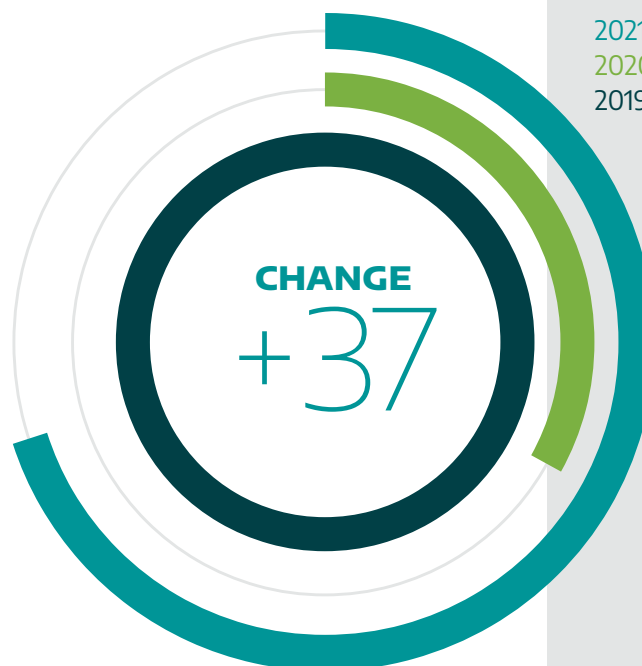
Dragos considered findings to be related to poor security perimeters if they involved issues such as porous firewall rules, network boundary bypasses, or flat networks. This includes instances where the only segmentation is the initial firewall between the IT-OT boundary and when there are unnecessary communication pathways to critical assets within the network. While it is unlikely that an adversary could cause an operational impact with access only to the corporate network, poor perimeters between IT and OT often allow adversaries to pivot from the corporate network to operational networks, where they can cause ICS impacts. However, an OT interdependency on an IT asset, such as a billing system that also performs scheduling or product tracking, is one example of how an adversary could impact operations from the corporate network.

Every OT asset owner needs a defensible architecture. A network with weak borders, especially when combined with a lack of visibility, is nearly impossible to defend from even a moderately motivated adversary.

**TOP 4 KEY FINDINGS: THREE**

## External Connections to the ICS/OT Environment

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



A major theme in the 2019 Year In Review report was the disconnect between expectations and reality on fully segmented and air-gapped systems. During 2020, there was a significant improvement in isolated ICS environments (with a two-thirds drop in external routable network connections). In 2021, external connections to OT spiked upwards, more than doubling to 70%. Dragos assesses that this increase is due to the high demand for remote access in the wake of the COVID-19 pandemic.

Many OT environments appear fully segmented on paper, yet when validated with the Dragos Platform analysis the Dragos team finds that the environments often have many connections and are not as segmented as originally believed. These environments may have been initially designed and implemented as segmented, but over time firewall exceptions and persistent vendor connections steadily bridged the gap between IT and OT.

The most effective security control for reducing the cyber risks associated with remote access is multi-factor authentication (MFA). However, MFA cannot be implemented everywhere or in every situation. Dragos recommends that vendor connections are enabled upon request and then monitored to ensure they are used only when authorized. And the ability to rapidly disconnect external connections is essential for effective incident response.

**TOP 4 KEY FINDINGS: FOUR**

## Lacked Separate IT & OT User Management

**In 2021, 44% of Dragos services engagements included findings related to shared credentials.**



For example, an organization may leverage the same credential management on the IT network as it does on the Demilitarized Zone (DMZ) and ICS network. This is yet another configuration that can lead to a weakening of perimeters and may enable an adversary to easily traverse to ICS assets using the credentials it obtained from IT accounts.

There is no question that reusing credentials may feel more efficient to the endpoint administrators maintaining your operating environments. However, frequently, this technique can allow an adversary to move laterally across your operating environment. And, it may not raise any alarms if the activity is not recognized as “new” in your operating environment and lead to a security incident going unnoticed.

# Findings Across Industry Verticals

The heatmap below illustrates a breakdown of our four key findings by OT industry verticals.



**AT LEAST 50% OF CUSTOMERS IN ALL VERTICALS** have significant issues with network perimeters and visibility.



All four common findings are **PREVALENT AND EXIST IN MORE THAN 70%** of the Water, Food & Beverage and Wind industries.



**USE OF SHARED CREDENTIALS BETWEEN IT AND OT VARIES SIGNIFICANTLY DEPENDING UPON THE VERTICAL.** It is exceptionally rare in Electric but frequently observed in Rail. Shared Credentials findings were some of the least consistent of our “top 4” across the verticals.



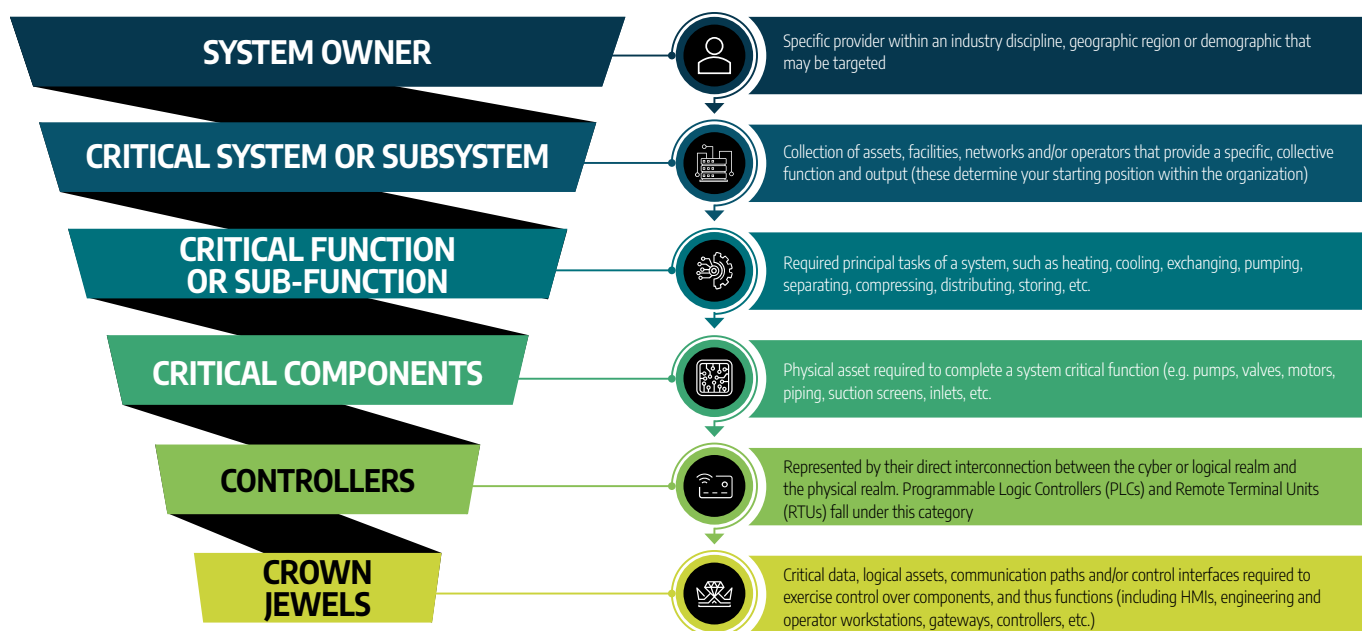
# Cybersecurity Assessments Findings

In 2021, Dragos performed ICS cybersecurity assessments across nearly every OT vertical. The data from these engagements enables Dragos to provide key insights on the OT industry as well as provide specific findings for individual sectors. Dragos uses a consequence-driven approach called the Crown Jewel Analysis (CJA) Model when scoping and conducting these assessments. This approach helps bind the scope of assessments while keeping the adversary mindset.

## THE CROWN JEWEL ANALYSIS (CJA) MODEL

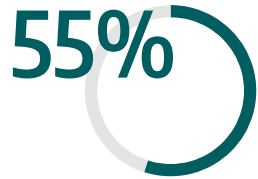
The Crown Jewel Analysis (CJA) Model is a repeatable scoping approach that helps visualize how an attacker assesses a system to achieve a specific consequence.

CJA is visualized using a reverse pyramid. For each layer, the elements contributing the most to functional output (primary purpose); functional dependencies (reliance on other systems to fulfill functional output); and level of exposure must be analyzed and understood before progressing to a lower layer. Adversaries and activity groups utilize a similar process when identifying Crown Jewels to further their attack chain.



Using CJA and credible threat intelligence, Dragos creates plausible attack scenarios to educate asset owners and operators on the potential exposure to adversaries and activity groups and to better prioritize the findings and recommendations in the reports. The scenarios illustrate realistic ways that an adversary could achieve a desired impact to the process or facility, specific to that facility's implementation and security posture.

The following heatmap shows the ICS impacts identified across each OT industry vertical. Each row represents a specific industry, and each column represents an operational impact identified during the crown jewel analysis.



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

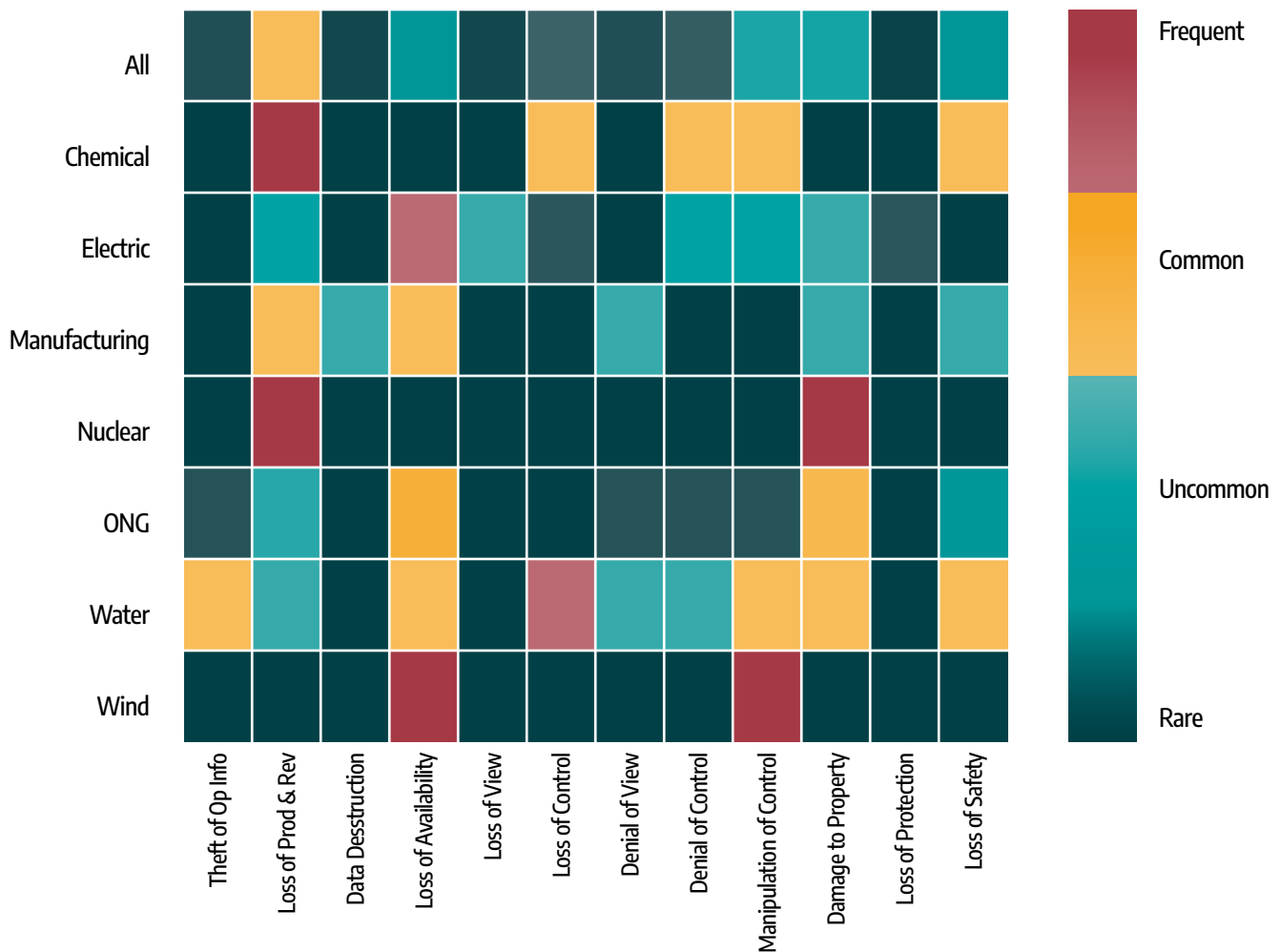


included a loss of safety impact.



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

## CJA Impact by Sector Heat Map



# Cyber Readiness Findings

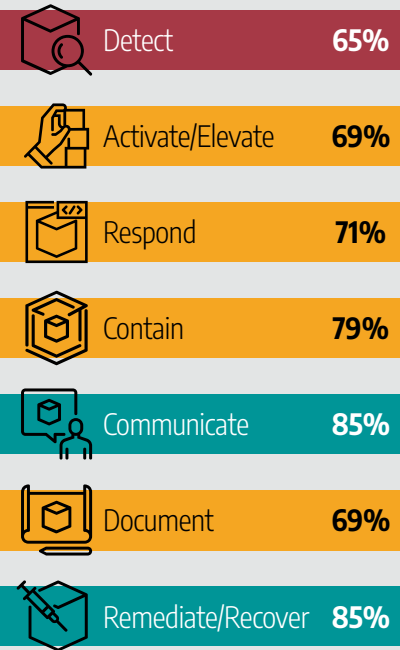
In 2021, Dragos executed numerous cybersecurity tabletop exercises (TTXs) across several OT industry verticals.

A TTX is a training and planning readiness event that uses a threat emulation scenario to challenge and evaluate a client's existing response plans, practices, and capabilities. They include collaboration between all stakeholders, including IT and OT security teams and operations leaders to strengthen internal communication strategies and develop relationships. TTXs are designed to evaluate the effectiveness of the client's cybersecurity incident response plans, the coordination of the plans with partners, capability and resource employment, communication flow, and the actions taken upon plan activation.





A Dragos TTX demonstrates how a realistic attack may occur within a unique ICS environment based on the organization's most concerning risks. Dragos passively researches and analyzes perceived cybersecurity risks within the outward-facing network infrastructure. Any risk that would allow the development of unauthorized access to key OT assets is added to the exercise scenario. Unique environmental information such as asset types, vendors, personnel, partnerships, network architecture, and models have been coupled with specific threat behavior, real-world historical events, and activity groups to generate a theoretical exercise scenario.

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, activate/elevate, respond, contain, communicate, and remediate/recover.

## AVERAGE TTXs FINDINGS



### Metrics are as follows:

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

## AVERAGE TTX SCORES

The 2021 TTX overall score was composed from many tabletop exercises encompassing several verticals with a strong representation by both ONG and Electric verticals. A key takeaway from these average scores is 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 core capability tested with the lowest aggregate score is Detect. This gives confidence in our above assessment findings demonstrating limited visibility within the OT environments.

SECTION THREE

---

# **ICS/OT Vulnerabilities**



## Vulnerabilities

2021 was a challenging year for ICS and OT vulnerabilities. There were nearly double the published ICS and OT vulnerabilities in 2021 than 2020. This year highlighted vulnerabilities range from the remote, persistent, and nearly ubiquitous risks like Log4j, the Windows zero-day vulnerability PrintNightmare, and industrial hardware rootkit-level vulnerabilities that allow attackers to compromise exposed devices. These vulnerabilities underscore the fast-growing universe of persistent threats that exist across all layers of the Purdue Model. These vulnerabilities also highlight the complex nature of connected and networked components in OT environments and in ICS.

There continues to be a trend where the guidance in vulnerabilities is lacking in context and details for operators to make risk-based decisions. Dragos added additional mitigation strategies for 69 percent of advisories that did not have sufficient mitigation advice in 2021.

# Apache Log4j Vulnerability



## WHAT IS IT?

Before the Alibaba Cloud Security team disclosed the Log4j vulnerability to Apache in November of 2021, few people anticipated that a Java logging library could have such negative far-reaching security impacts. The Log4j vulnerability (CVE-2021-44228) allows for remote code execution and access to servers and hardware that use Java and that the Log4j framework can be exploited to take complete control of a system.

Log4j is a frequently used logging solution that allows developers to monitor the execution of their Java applications for errors and exceptions. Utilizing Log4j was considered a best practice and is a commonly used design pattern within enterprise Java development.



## WHY ARE INDUSTRIAL NETWORKS VULNERABLE TO LOG4J?

The exploitation of Log4j involves sending a specially designed request to the target system. The request generates a log using Log4j and leverages the Java Naming and Directory Interface (JNDI) lookup feature to perform a request to an attacker-controlled server from where a malicious payload can be fetched and executed. Industrial networks are among the systems that are vulnerable to the Log4j Java logging library.

Dragos has observed both the attempted and successful exploitation of the Log4j vulnerability in the wild. Based on these observations, on December 8, 2021, Dragos coordinated a takedown of malicious domains used during the early exploitation attempts. Dragos has also observed other intelligence organizations reporting cyber criminals launching Log4j attacks to deliver Cobalt Strike beacons, malware, cryptocurrency miners, ransomware, DDoS attacks, and other malicious programs.

Because Log4j has been a ubiquitous logging solution for Enterprise Java development for decades, the vulnerability has the potential to persist within the software and hardware of Industrial Control Systems (ICS) environments for years to come. Log4j is found in open-source repositories used in numerous industrial applications, such as Object Linking and Embedding for Process Control (OPC) Foundation's Unified Architecture (UA) Java Legacy. Adversaries also can leverage Log4j in proprietary Supervisory Control and Data Acquisition (SCADA) and Energy Management Systems (EMS), which use Java in their codebase.

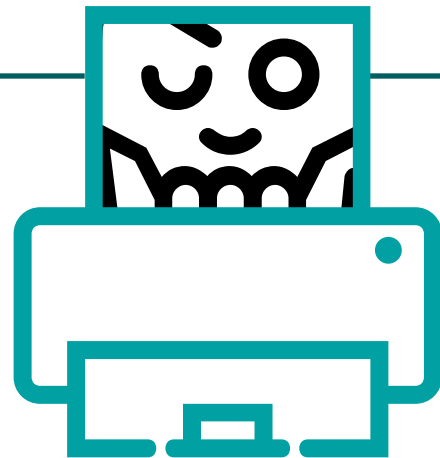


### NEXT STEPS TO MITIGATE LOG4J

Major OT vendors have been disclosing the vulnerability's impact on their software and equipment. Dragos assesses additional disclosures will continue as more vendors identify the use of Log4j across ICS product lines. Unfortunately, the nature of the Log4j vulnerability makes it challenging to identify. Because of this, Dragos assesses that Log4j will be a persistent vulnerability in ICS environments for years to come.

OT networks that incorporate robust segmentation in their environments reduce the risks from this vulnerability, but should be patched during the next turnaround or operational shutdown. For ICS environments that lack segmentation or allow direct internet access to ICS assets such as JAVA-based SCADA / HMI products / hardware devices, Dragos recommends that organizations patch immediately and strongly consider disabling internet access to all affected ICS/OT assets.

## Windows Zero-Day Vulnerability: PrintNightmare



### WHAT IS IT?

On June 29, 2021, security researchers at Sangfor Technologies accidentally disclosed a Windows zero-day vulnerability nicknamed PrintNightmare in a how-to-exploit guide published on a public GitHub repository. PrintNightmare is a critical security vulnerability affecting the Microsoft Windows operating system. The vulnerability occurs within the print spooler service and allows a remote-authenticated adversary to execute malicious code at SYSTEM-level privileges. This enables an adversary to create new users with full user rights, install malicious software, and modify or delete data.



### HOW ADVERSARIES GAIN ACCESS TO OT NETWORKS WITH PRINTNIGHTMARE

Adversaries can leverage PrintNightmare CVE-2021-34527, CVE-2021-34481, and CVE-2021-36958 vulnerabilities to gain access to OT networks from IT networks through OT DMZ remote access workstations or "jump boxes" if they are left unpatched. Also, these vulnerabilities make an OT network's unpatched Windows assets susceptible to lateral movement and privilege escalation.

The PrintNightmare vulnerability was first discovered in March 2021. Sangfor, a network security and cloud computing solutions company, planned to share its research at Black Hat that year. However, the proof-of-concept (POC) was released due to confusion over another Print Spooler vulnerability (CVE-2021-1675, released on June 8, 2021). The researchers assumed the remote code execution (RCE) proof-of-concept was the same method to exploit Windows Print Spooler CVE-2021-1675 and thus was the same vulnerability. Because CVE-2021-1675 had already been patched, they saw no harm in releasing details earlier than planned.

The exploitation of the PrintNightmare vulnerability can enable the compromise of a desktop or server running the Print Spooler service and allows an adversary to obtain SYSTEM-level privileges. On July 6, 2021, Microsoft began releasing unscheduled or out-of-band patches to address the vulnerability, which resulted in some printers no longer functioning – where after patching, only administrators could install printer drivers to a Windows print server.

A third vulnerability was discovered on July 15, 2021, impacting the Windows Print Spooler Service (CVE-2021-34481) that could also allow an adversary to perform remote code execution at SYSTEM-level privileges. Microsoft addressed this third vulnerability on August 10, 2021, with an out-of-band patch. A fourth vulnerability (CVE-2021-36958) was then discovered on August 11, 2021, affecting the Windows Print Spooler Service again with remote code execution (RCE) at SYSTEM-level privileges if exploited. This fourth vulnerability was patched on September 14, 2021, during the September 2021 Microsoft Patch Tuesday security updates.



### **WHAT IS THE RISK OF PRINTNIGHTMARE TO OT ENVIRONMENTS?**

Dragos has not observed any adversaries leveraging the PrintNightmare vulnerability in OT network compromises. However, Dragos penetration testers have successfully leveraged PrintNightmare to help clients enhance their detections for it. For example, detections and preventions were in place for blocking the binary and PowerShell script variants of the exploit in some environments. Dragos demonstrated capabilities by executing the PowerShell variant of PrintNightmare in memory and by leveraging PowerShell ISE to bypass the prevention and detection mechanisms.

The vulnerabilities in the Print Spooler Service enable escalation of privileges and freedom of movement within the OT network's Windows assets. Windows assets in an OT environment can serve many functions such as engineering and remote access workstations, HMIs, historians, and multiple types of servers providing basic networking and domain functions. Leaving these assets unpatched allows even low-sophistication adversaries to have more options and methods for compromising network assets.

# PLC and Industrial Hardware Rootkit-Level Vulnerabilities



## **THE LONG-TERM RISKS OF PERSISTENT ROOTKITS**

Existing vulnerabilities in industrial equipment often allow threat groups to install persistent rootkits when there are insufficient hardware protections in the equipment's original design. Most modern industrial hardware lacks the functionality needed to securely boot the device, and often both modern and legacy hardware remain in service for decades. This results in a class of vulnerabilities that do not disappear as long as the hardware remains in service.

Rootkit-style vulnerabilities in the industrial space are not new. Specific research examples go back more than a decade to 2009.<sup>13</sup> Due to a rush to fix long-standing insecurities in industrial products combined with existing industrial protocols, this class or chain of vulnerabilities is becoming increasingly difficult to detect. Frequently vendors add encryption features to the industrial protocols, while leaving the underlying insecurity exposed. On the surface this strategy looks good to end users because traffic is no longer in plain text, but this does not add much, if any, complexity to the path to compromise that the adversary must follow or the defenses he must surmount or circumvent.

As a result, it is more challenging to analyze traffic on the wire to determine if a device is being compromised. For example, an attacker may need to circumvent a trusted relationship between the engineering workstation and the PLC. Once that trusted relationship is exploited, the controller may be permanently infected. Worse, if the traffic is encrypted, it may be tough to determine that the infection took place.

There are many examples of firmware rootkits in the wild and many devices have a series of vulnerabilities that can be used together to install rootkits.

<sup>13</sup>Leveraging Ethernet Vulnerabilities in Field Devices – Digital Bond



## WHAT ARE THE IMPACTS OF ROOTKIT VULNERABILITIES?

In 2021, Iranian researchers reported<sup>14</sup> a rootkit they discovered in a server's integrated Lights Out peripheral (iLO) boards. The rootkit allowed the adversary to maintain access to the individual board on the server hardware. From this point, the adversary issued low-level commands to the computer hardware, including the ability to wipe the server remotely and potentially install new software along with or in place of the standard computer operating system.

In 2021, Siemens disclosed a vulnerability in its PLC, CVE-2020-15782,<sup>15</sup> which can allow an attacker to load malicious logic files into the PLC. This malicious logic can circumvent memory protections in the PLC and may overwrite core PLC functions with a rootkit. Dragos discovered similar problems with other PLC logic runtimes in prior years. In 2019, Dragos demonstrated use of a ladder logic payload for developing a rootkit in Phoenix Contact's logic runtime, which is used by dozens of PLC vendors.<sup>16</sup> Earlier research covered rootkits in another ladder logic runtime by 3S-Software.<sup>17</sup>

Triconex SIS was the victim of such an attack, which used CVE-2018-8872 and CVE-2018-7522<sup>18</sup> to install additional functionality in the firmware. Dragos continued to research the device and identified several other rootkit-style vulnerabilities<sup>19</sup> in the Triconex line, particularly in the network interface cards of the controller which could be used for a similar purpose as the HP iLO rootkit.

Dragos has researched a number of industrial embedded products including Emerson's WirelessHART Gateway products,<sup>20</sup> Tofino Xenon industrial hardware,<sup>21</sup> Lilee Systems train communications gateways<sup>22</sup> and GE MDS radio equipment.<sup>23</sup> Vendors have been responsive to the issues reported. However, the designs of these products mean that they can rarely be secured from the risk of rootkit installation. Instead, Dragos advisories highlight which services allow for the potential installation of a rootkit so that end users may restrict access to and monitor those services for suspicious activity.

<sup>14</sup> Implant.ARM.iLObleed.a – Amn Pardaz; <sup>15</sup> SSA-434534 – Siemens Product CERT; <sup>16</sup> Broken Rungs – CS3STHLM;

<sup>17</sup> Vulnerability Inheritance in Dutch Controllers – Black Hat Sessions; <sup>18</sup> ICSA-18-107-02 – ICS CERT; <sup>19</sup> VA-2018-02 – Dragos Triconex Vulnerability Report;

<sup>20</sup> VA-2021-06 – Dragos Emerson WirelessHART Gateway Vulnerability Report; <sup>21</sup> VA-2021-02 – Tofino Xenon Security Appliance Vulnerability Report;

<sup>22</sup> VA-2022-01 – Lilee Systems/Alstom Rail CMU-2110 Vulnerabilities; <sup>23</sup> VA-2022-03 – GE MDS Network and Serial Vulnerabilities



## MITIGATING THE RISKS OF ROOTKIT VULNERABILITIES

Developing a full-fledged rootkit is not a simple task. Finding and chaining the vulnerabilities together to allow firmware modification requires significant research. Once installed, a rootkit may allow for intentional or unintentional damage to the equipment. For example, a rootkit that does not properly sanitize or bounds-check future attacker inputs can cause misoperation.

Dragos assesses that this was the case with the TRISIS rootkit, where after installation the rootkit allowed for direct memory tampering. Dragos assesses that an error in the memory tampering caused the safety system to trip the plant, causing the discovery of the implant. This example highlights the need for the attacker to test their rootkit on numerous revisions of the target system under various configurations. Rootkits should not be considered the most likely problem. However, vulnerabilities that present persistent access to embedded systems can become a problem. The compromise of these devices can be challenging to detect and root out of a network.

The best steps to mitigate the risks associated with rootkits include:

- Ask the vendor to implement the NULL CIPHER when adding security to their protocols. This allows devices and users to mutually authenticate while leaving the network traffic visible to inspection.
- Monitor embedded devices for unusual network traffic. For example, a VPN appliance or PLC establishing or attempting to establish outbound network connections is a cause for concern.
- Check all downloads with the vendor code signature to ensure it is legitimate and unmodified software.
- Minimize network exposure of embedded products and monitor the network traffic to and from such products. Remember that embedded devices are complicated to analyze forensically because network traffic flows are often the only practical way to analyze these devices without sending them back to the factory.

Keeping these longstanding issues in mind when mitigating new device vulnerabilities is essential. It is crucial to be aware of rootkit vulnerabilities when exposing devices. Even if a device “has all the patches applied,” it could still be susceptible to vulnerability chaining or even abuse of features which could allow an attacker to install a rootkit and compromise your system.

**BY THE NUMBERS**

# Key ICS Vulnerability Trends

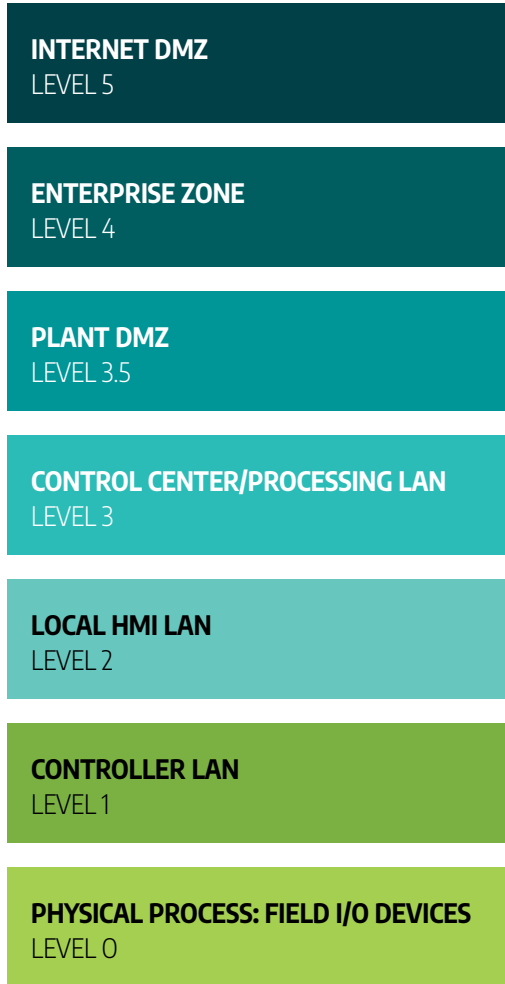
In 2021, the number of reported ICS vulnerabilities continued to increase, which coincided with an increase in vendors providing patches for disclosed flaws in advisories. Dragos researchers analyzed 1703 ICS/OT common vulnerabilities and exposures (CVE) during 2021, which is more than twice as last year. For each CVE, Dragos independently assesses, confirms, and often corrects the advisories and describes any flaws in firmware or software.

Of the advisories that Dragos individually reviewed in 2021, 38 percent 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.



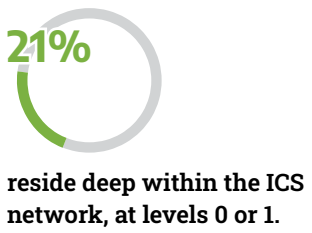
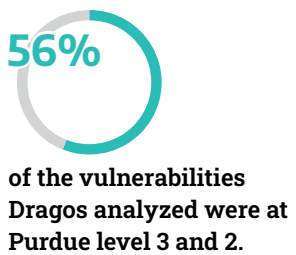
# Where Do the Vulnerabilities Reside?

Of the vulnerabilities that Dragos focused on in 2021, 77 percent resided deep within the ICS network, meaning they apply to equipment on Levels 0 to 3 of the Purdue Model. This includes engineering workstations, PLCs, sensors, and industrial controllers.



of the advisories Dragos analyzed applied to products within the enterprise bordering the internet at Purdue Level 3.5, 4, or 5.

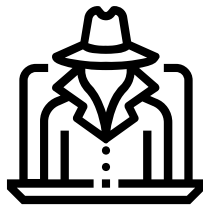
Often this includes networking communication equipment, VPNs, data historians, remote desktop software, or firewalls commonly deployed in the demilitarized zone or enterprise networks.



At the lower levels, adversaries would need access to a control system network to exploit these vulnerabilities, making them more difficult to exploit. Implementing proper network segmentation can help mitigate these vulnerabilities, especially when combined with Multi-Factor Authentication (MFA) for remote sessions.

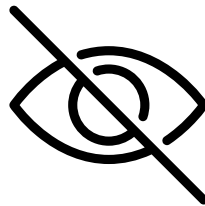
# Loss of View, Loss of Control, or Both

Loss of control and loss of view are among the worst operations scenarios in an ICS environment. In 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 2021, 35 percent of the advisories that Dragos analyzed could cause both a loss of view and loss of control in an OT system. The percentage is much smaller when looking at loss of one or the other, as shown below.



Loss of Control  
only (by Advisory)

**0.4%**



Loss of View  
only (by Advisory)

**1.2%**



Loss of both  
View & Control  
(by Advisory)

**35%**

DRAGOS  
FRONTLINE  
PERSPECTIVE

**30%**

of potential process  
impacts involved causing  
a loss of view or a loss of  
control

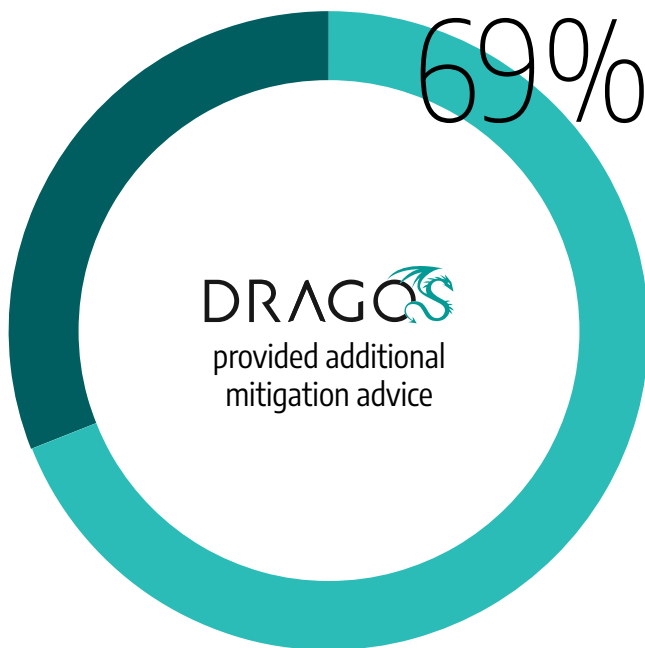
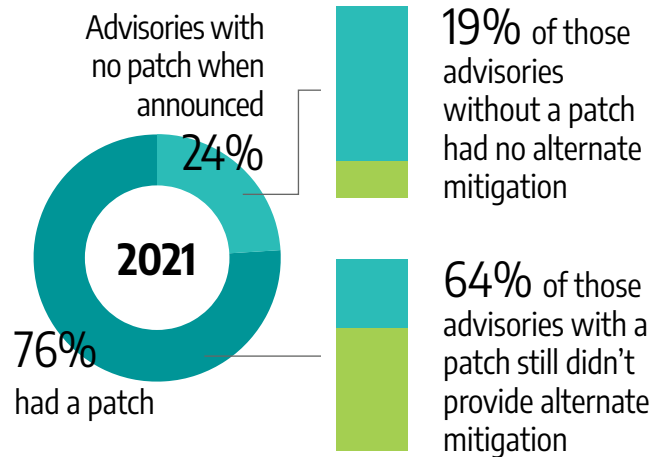
**50%**

of potential process  
impacts involved causing  
denial of, loss of, or  
manipulation of control

# Many Advisories Lack Actionable Guidance

In 2021, 24 percent of advisories had no patch when announced, while 76 percent had a patch. Frequently, vendors do not provide advice to asset owners and operators if they are unable to patch the identified vulnerability. Of the advisories that Dragos tracked in 2021 that did not initially have a patch, 19 percent had no mitigation. Sixty-four percent of those advisories that had a patch had no mitigation.

When a patch is unavailable from a vendor or industrial organizations find that patching isn't feasible or is too expensive from an operational standpoint, they look for alternative mitigation as a substitute. **In 2021, Dragos found that 96 percent of the patches that they analyzed had no alternate mitigation.**



**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.**

# Correcting Vulnerability Severity Ratings

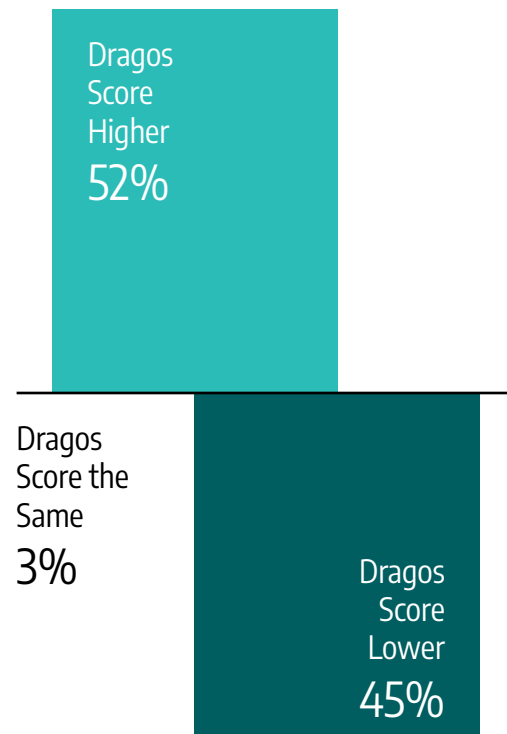
In addition to the lack of actionable information for most ICS-related vulnerability advisories, many advisories and individual vulnerabilities contained errors that could inadvertently mislead practitioners who use CVSS scores to triage for mitigation or patching. These errors could cause asset owners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

CVEs are scored using the InformaCVSS, which is a free and open industry standard for assessing the severity of computer system security vulnerabilities. The National Infrastructure Advisory Council (NIAC) launched the CVSS scoring system in February 2005, with the goal of providing “open and universally standard severity ratings of software vulnerabilities.” CVSS scores are calculated for each CVE based on a formula that depends on several metrics that approximate ease-of-exploit and the impact of exploit. Scores range from 0 to 10, with 10 being the most severe. CVSS was designed with IT systems in mind, but it can be somewhat helpful in ICS/OT environments as well.

Dragos provides corrected CVSS scores based on how an adversary could leverage a vulnerability in ICS environments in its WorldView threat intelligence reports. The corrected information allows practitioners to prioritize the CVEs that carry the most risk for their own environments and to focus their resources on the most severe issues first. However, CVSS scores can be misleading and often do not accurately capture all of the risk of a particular vulnerability. ICS security professionals should not use them as the sole factor in prioritizing vulnerabilities.

In 2021, Dragos gave a higher score to 52% of CVEs relating to ICS/OT networks than what these CVEs had received at publication. Forty-five percent of the severities that Dragos analyzed had a lower severity score than at publication, and three percent stayed the same.

## CVE SCORES THAT DRAGOS CORRECTED



# Vulnerability Recommended Actions: Remediate, Mitigate, Monitor, Ignore.

Dragos works with the community to help vendors provide more accurate, actionable, and easier-to-track advisories. In 2021, we significantly enhanced the vulnerability management features offered to customers through the Dragos Platform.

Dragos assesses vulnerabilities in our WorldView Intelligence reports and in the Dragos Platform and categorizes them by threat levels: "Immediate Action," "Limited Threat," "Possible Threat," "No Action," and "Hype." Dragos also recommends four different responses to those threats. Immediate action vulnerabilities require just that, consideration within the environment and a priority for remediation. These are network exploitable vulnerabilities that may have been actively exploited in the wild or for which a public exploit is available online. These flaws have a higher risk of impacting ICS networks and generally apply to devices that can affect the industrial control process. In 2021, four percent of vulnerabilities were in the "Remediate" category.

About half of the vulnerabilities fall into the "Limited Threat" category. Dragos recommends defenders resolve these vulnerabilities through proper network hygiene, segmentation, and network monitoring. A common recommendation is to limit the potential communication paths so that assets that need to communicate with each other are the only assets that can communicate with each other over routable protocols. This enables ICS security professionals to funnel ICS/OT risks into focal points that they can monitor for threats so they can get their teams back to intelligence-based decision making.

In the past year, Dragos found that the Dragos Platform could provide additional recommended actions on top of the Now, Next, Never categories used in previous years. The focus is to highlight the specific actions customers should take based on the risk level of the assessed vulnerabilities. So, instead of discussing "Now, Next, Never" prioritization, Dragos now provides the recommended actions: Remediate, Mitigate, Monitor, and Ignore.

Possible risks are often local threats which can coincide with adversaries living off the land. Dragos recommends that ICS security professionals monitor these vulnerabilities for malicious activity. In 2021, 87 percent of the vulnerabilities that Dragos analyzed were in the "Mitigate" and "Monitor" categories.

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 9% of the vulnerabilities that Dragos reviewed were in this category.



# 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. In the realm of ICS/OT vulnerabilities, it is important to focus and prioritize threats accurately and have clear actionable mitigations that reduce the amount of downtime, while still protecting people and processes.



**PUBLISHED VENDOR AND PUBLIC CERT ADVISORIES ALONE 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 the patch.



**PATCHES ARE OFTEN SYNONYMOUS WITH DOWNTIME AND THERE ARE MANY DOCUMENTED CASES WHERE THE ACT OF PATCHING HAS CAUSED ISSUES OR PLANT FAILURES.**

In a best-case scenario, applying a patch requires restarting 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 applying a 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.**

A firewall can be used to 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, file extensions that 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.

# 5 Security Controls for a World-Class OT Cybersecurity Program

Five years ago, the Dragos YIR was designed to drive insights into where the ICS/OT community defenses are and to better describe the threats and vulnerabilities that are unique to industrial environments.

This multi-year data set and the findings from this year's report point to clear security controls that can put organizations on a path to a more safe and reliable industrial process. Dragos recommends that organizations focus on key security controls that can be done well, as opposed to spreading the focus across too many possibilities. There are many IT security controls that have a significantly reduced value when applied to OT or can introduce risk to the OT environment. Taking this into consideration, here are the five security controls that when implemented have the best value in significantly enhancing ICS/OT networks against cyber threats.

## 1

### **A DEFENSIBLE ARCHITECTURE**

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 as IEC62443 zones and conduits, DMZs, jump hosts, etc.

A key component of a defensible architecture is the ability to add humans to make it a defended architecture. As an example, unmanaged switches and flat networks are an indefensible architecture in most cases due to the inability for defenders to get the data they need to act. Infrastructure preparation and data gathering is a core requirement to being able to defend a network.

## 2

### **ICS NETWORK MONITORING**

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.

To gain the values of ICS network monitoring ensure that the organization can monitor East/West traffic inside the ICS network and do so with an understanding of the ICS protocols and what is happening within them. The unique system-of-systems nature of ICS means there's a higher emphasis on network monitoring than on endpoint monitoring though both should be done when possible.

# 3

## REMOTE ACCESS AUTHENTICATION

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

## KEY VULNERABILITY MANAGEMENT

The majority of vulnerabilities do not need to be addressed if you have a defensible architecture. Dragos recommends defenders prioritize those that bridge IT and OT over those residing deep within the OT network or those that fall into the "Remediate" category in Dragos's vulnerability analysis. In short, roughly 4% of vulnerabilities this year met this qualification.

# 5

## ICS INCIDENT RESPONSE PLAN (IRP)

Lastly, Dragos recommends that industrial organizations have a dedicated incident response plan (IRP) for their ICS/OT environments, and that these organizations regularly exercise the plan with cross-disciplinary teams (IT, OT, Executives, etc.).

One very effective way of utilizing an incident response retainer with a provider like Dragos, or others, is to have a Tabletop Exercise against a real threat scenario the organization is concerned about and use that to drive alignment across the organization. The scenario and TTX should also be used to identify use-cases and key tactics, techniques, and procedures security operations personnel should be monitoring for instead of expecting them to identify and analyze every anomaly that occurs.





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](https://www.dragos.com)