Everything You Need to Know to Defend Against ICS/OT Cyber Threats in 2023

ICS/OT CYBERSECURITY YEAR IN REVIEW 2022

Keeping up on the latest cyber news is tough and distinguishing hype from reality is even more challenging. Dragos's 2022 ICS/OT Cybersecurity Year in Review is filled with insights into the top threats to industries, vulnerabilities facing industrial control systems (ICS), and guidance on responding to threats in operational technology (OT) environments. This comprehensive annual report covers everything you need to know to be cyber ready in 2023. Keep scrolling to view the top 6 key takeaways from this year's report.

1 CHERNOVITE's PIPEDREAM is the First Scalable, Cross-Industry ICS Attack Framework with the Potential for Disruptive and Destructive Cyber Attacks

7th ICS/OT TARGETING MALWARE
After STUXNET, HAVEX, BLACKENERGY, CRASHOVERRIDE, TRISIS, and Industroyer2

PIPEDREAM enables extensive and flexible adversary capabilities within victim environments and targets software components and communication protocols used across all industrial sectors.

OPC UA · Modbus · ASRock

All industries are potentially at risk from PIPEDREAM.

46% of MITRE ATT&CK for ICS techniques can be executed using this malware

1000s of devices potentially impacted

100s of suppliers impacted

LESSON LEARNED FROM THE FRONTLINES

SECURING ICS/OT ASSETS FROM PIPEDREAM

Maintain an accurate asset inventory and threat detections based on knowledge of real industrial adversary behaviors. An **ICS Network Visibility** program that uses ICS protocol aware technologies makes it possible to defend against disruptive and destructive threats like PIPEDREAM.

80% OF CUSTOMERS across Dragos Professional Services engagements in 2022 still lack visibility across OT networks

2 Two New Threat Groups Expertly and Aggressively Targeting Industrial Environments

CHERNOVITE
To develop PIPEDREAM, CHERNOVITE demonstrated a not seen before breadth of knowledge of ICS protocols and intrusion techniques available to disrupt OT environments. CHERNOVITE has developed the capabilities to achieve Stage 2 of the ICS Cyber Kill Chain and execute an ICS attack.

BENTONITE
BENTONITE is increasingly and opportunistically targeting maritime oil and gas (ONG), state, local, tribal, and territorial (SLTT) governments, and manufacturing sectors since 2021. BENTONITE conducts offensive operations for espionage and disruptive purposes, targeting vulnerabilities in internet-exposed assets to facilitate access.

LESSON LEARNED FROM THE FRONTLINES

SECURE REMOTE ACCESS IS CRITICAL

Threat groups like BENTONITE demonstrate the importance of **Secure Remote Access** in ICS/OT environments including multi-factor authentication (MFA). Where MFA is not possible, consider alternate controls such as jumphosts with focused monitoring on connections in and out of OT networks.

53% of Dragos Professional Services engagements in 2022 included findings of external connections to OT

3 Continued and Persistent Threat Group Activity Targeting Industries Around the Globe

Dragos adversary hunters observed the activity of six known Threat Groups targeting industrial organizations.

KOSTOVITE
Targets energy in North America and Australia

KAMACITE
Targets many industrial sectors in Europe, including Ukraine, and the U.S.

XENOTIME
Targets oil and gas, electric in the Middle East and North America

ELECTRUM
Targets electric in Europe, including Ukraine

ERYTHRITE
Targets multiple industrial sectors in the U.S. and Canada

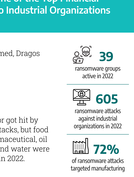
WASSONITE
Targets multiple industrial sectors in South/East Asia and North America

LESSON LEARNED FROM THE FRONTLINES

SHARED CREDENTIALS HELP ADVERSARIES

Leveraging valid accounts is the most common method of lateral movement and privilege escalation.

Shared accounts can be used to pivot from corporate IT networks to ICS/OT environments, where they are frequently used to access critical industrial systems.



54% of Dragos Professional Services engagements in 2022 included a finding about shared credentials in OT systems

4 Ransomware Cited as One of the Top Financial and Operational Risks to Industrial Organizations

↑87% increase in ransomware attacks against industrial organizations over last year

To keep customers informed, Dragos monitors:
- Public Incidents
- Network Telemetry
- Dark Web Resources

The manufacturing sector got hit by the most ransomware attacks, but food & beverage, energy, pharmaceutical, oil & gas, mining & metals, and water were among other top targets in 2022.

39 ransomware groups active in 2022

605 ransomware attacks against industrial organizations in 2022

72% of ransomware attacks targeted manufacturing

LESSON LEARNED FROM THE FRONTLINES

RANSOMWARE ATTACKS CAN START IN IT NETWORKS, PIVOT TO OT

Ransomware represents a top cyber risk to industrial organizations, particularly those without a **Defensible Architecture**. OT security strategies often start with hardening the environment—removing extraneous OT network access points and maintaining strong policy control at IT/OT interface points.

Improper network segmentation findings occurred in 50% of Dragos Professional Services engagements in 2022

5 ICS/OT Vulnerabilities Increase 27 Percent, with 77 Percent Providing No Mitigations

Dragos researchers analyze vulnerabilities to assess how easily and frequently they can be exploited by adversaries. A full 34 percent of advisories that Dragos analyzed in 2022 contained errors.

LESSON LEARNED FROM THE FRONTLINES

TAKE A PRACTICAL, RISK-BASED APPROACH

There will always be more vulnerabilities, and the next patch – it can turn into a catch-up game and there are only some cases where it makes sense. And not all of them need to be addressed. It's okay to ignore many.

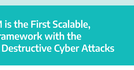
ONLY 2% of ICS/OT vulnerabilities need to be addressed **NOW**

68% of vulnerabilities are network exploitable with direct operational impact – these need to be addressed **NEXT**: Mitigate through network monitoring, segmentation, MFA

30% of vulnerabilities pose a possible threat but rarely require action – they likely **NEVER** need to be addressed: Monitor these

6 Where to Begin? Be Proactive About Cyber Readiness

Every OT-focused cybersecurity program should begin with having a well-thought-out **ICS Incident Response plan** (IRP) that is distinct from IT's. OT involves different devices, communication protocols, adversary behaviors, and vulnerability management practices. Cyber attacks can result in physical impacts and investigations require a different set of tools.



Want to Learn More?

The Dragos 2022 ICS/OT Cybersecurity Year in Review report will help you identify your critical industrial threats, prioritize vulnerabilities, and improve your ICS/OT cybersecurity posture with year-over-year data and insights. Read the full report at dragos.com/year-in-review.

Let Dragos help you get started on your ICS/OT cybersecurity journey. Connect with us at sales@dragos.com or learn more about our technology and solutions at dragos.com.

DRAGOS