Ransomware: The #1 Threat Targeting Manufacturers Worldwide

ICS/OT CYBERSECURITY YEAR IN REVIEW 2022

According to the 2022 ICS/OT Cybersecurity Year in Review, ransomware attacks on industrial infrastructure organizations nearly doubled in 2022. More than 70 percent of all ransomware attacks focused on manufacturing, and threat groups continue to broadly target many different manufacturing sectors. As ransomware activity increases, it results in more risk for OT networks, particularly networks with poor segmentation. **Here's a high-level view of the impact of ransomware around the globe.**

Key Ransomware Findings

↑ 87%

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

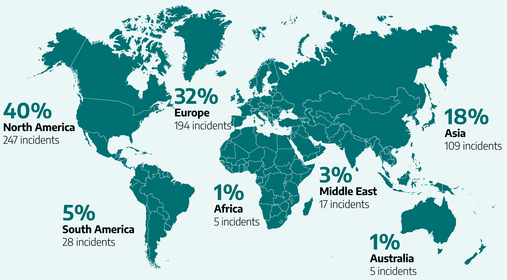
+35%

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

72%

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

Ransomware Incidents by Continent • 2022



Notable Ransomware Incidents Impacting Manufacturers

JAN

Ransomware-as-a-Service Impacts Multiple Industries

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

FEB

Ransomware Attack on Kojima Industries

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

MAY

Ransomware Attack on AGCO

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

MAY

Foxconn Ransomware Attack

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

DEC

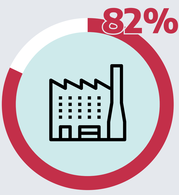
Trickbot Tied to Food and Beverage Ransomware Attack

In December 2022, Dragos discovered Trickbot infrastructure, and subsequently identified three victims – two mining and metals companies and one food and beverage company – communicating with this threat group infrastructure. Two of these three companies have publicly noted that some aspects of their OT operations were impacted in October and November 2022.

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 should start with hardening the environment—removing extraneous OT network access points and maintaining strong policy control at IT/OT interface points.



of manufacturers had poor security perimeters at the beginning of their engagements with Dragos in 2022

What's Next in 2023?

Dragos assesses that ransomware groups will continue to target high-value, industrial entities. In 2023, cybercriminals will continue to show more interest in vendors and suppliers because of the interconnectivity with their customers downstream. This is largely due to the criticality of operations and their reach into numerous OT environments, which often results in higher or more frequent ransom payouts.

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