2022 ICS/OT Threat Landscape Recap & What to Watch for This Year

By Dragos, Inc.

Published: 2023-04-14 · Archived: 2026-04-05 17:09:44 UTC

Our annual 2022 ICS/OT Threat Landscape webinar, moderated by Dr. Thomas Winston, Director of Intelligence Content, and delivered by Kent Backman, Principal Adversary Hunter, and Josh Hanrahan, Senior Adversary Hunter, covers the significant events and activity reported by the Dragos Threat Intelligence team in our 2022 ICS/OT Cybersecurity Year in Review report. This blog highlights the main topics and trends shared in our recent webinar, including new and active adversary threats targeting industrial infrastructure, malware and tools used in different attack stages, and vulnerabilities targeted for compromise.

Heightened ICS/OT Adversary Activity

Dragos Threat Intelligence tracks threat groups that attempt to gain access to ICS/OT environments or conduct activity that can be used to facilitate future threats to industrial infrastructure. Dragos adversary hunters are currently tracking 20 ICS/OT threat groups, up from five threat groups in 2017.

In 2022, the industrial community experienced a shift in the cyber threat landscape that was ushered in by increasingly homogenous operational technology (OT) infrastructures and knowledgeable adversaries targeting industrial control systems (ICS). Compounding on previous years, last year saw the discovery of new ICS-specific malware, new threat groups targeting industrial organizations, and adaptive adversary campaigns leveraging weaknesses in the industrial community's defenses. As a result, heightened attention is required to safeguard against disruptions in electric grids, oil pipelines, water systems, and manufacturing plants that can place human populations at risk.

ICS/OT Malware Development Capabilities Evolve

Dragos Threat Intelligence is focused on the threat groups exploiting OT networks and ICS devices, and the industries they are targeting for that purpose. A cyber attack in OT requires an understanding of the ICS/OT environment, adversaries need knowledge of devices and systems and how they communicate, and they need to be able to use that knowledge to manipulate physical processes and create an impact. Several threat groups developed new malware capabilities specifically designed for executing attacks on industrial and critical infrastructure.

PIPEDREAM Malware – First-Cross Industry Attack Framework

In April of 2022, Dragos and a partner announced the discovery of PIPEDREAM — a cross-industry industrial control system (ICS) attack framework developed by the threat group CHERNOVITE explicitly to attack industrial infrastructure. Dragos identified and analyzed PIPEDREAM's capabilities through our daily business and in collaboration with various partners in early 2022. PIPEDREAM is the seventh known ICS-specific

malware, and the fifth malware specifically developed to disrupt industrial processes. Given the right operational conditions, PIPEDREAM could be used for destructive effects, but it was found before it was employed.

Initially developed to compromise devices used in the electric industry, as well as oil and gas, PIPEDREAM represents a new evolution in malware development as the first cross-industry scalable ICS malware with disruptive capabilities and could easily be adapted for other industries.

Industrial Infrastructure Recon, Initial Access, C2 Activity in 2022

Executing an impact on industrial control systems can require extensive research and development. Adversaries often conduct reconnaissance to gain information and initial access to networks to execute a future attack on their ICS/OT targets. That takes time. Moreover, attacks on ICS/OT also do not require intent, so OT networks may be "targets of opportunity." Even when an adversary accidentally stumbles onto an OT environment, there is still a risk to that environment. In 2022, Dragos observed activity from multiple threat groups targeting industrial organizations globally for reconnaissance, initial access, and long-term persistence leveraging signature techniques, along with the development of new capabilities and attack patterns.

	**BENTONITE – NEW THREAT GROUP TARGETING OIL & GAS, MANUFACTURING IN THE U.S. SINCE 2021** BENTONITE is a highly opportunistic group conducting offensive operations for espionage. In 2022, BENTONITE was observed exploiting Log4j and VMWare Horizons vulnerabilities in remote access devices and internet-facing assets. Once initial access is achieved, BENTONITE installs a downloader-type malware, and the downloader implant retrieves additional malware from an adversary created Github account that allows BENTONITE to gain command and control, conduct reconnaissance, and perform interactive operations. BENTONITE has in the past caused disruptive effects from ransomware and wiper malware, but for different objectives.
	**KOSTOVITE – SINCE 2021** KOSTOVITE compromises internet-exposed remote access and is skilled lateral movement & initial access operations into ICS/OT. Dragos observed the activities of multiple adversaries in 2022 sharing common infrastructure KOSTOVITE. APT5, a KOSTOVITE-linked group, was observed actively exploiting a zero-day in Citrix perimeter access devices, and have bypassed Ivanti Pulse Secure, Palo Alto, Fortinet, Sophos, and Sonicwall edge devices, sometimes living off the land inside their target networks, undiscovered, for months.

	**XENOTIME – SINCE 2014** XENOTIME has demonstrated the capability of executing disruptive ICS attacks, such as the 2017 TRISIS incident. TRISIS, the 5th ICS-specific malware, was deployed in an industrial facility in the Middle East by a well-funded attack team. This malware targeted safety instrumented systems (SIS) and was the first malware to specifically target human life, but it ultimately failed to disrupt operations at that facility. In 2022, XENOTIME conducted reconnaissance focus on oil and natural gas, and liquefied natural gas industries. XENOTIME makes heavy use of off-the-shelf tools and open-source information sources. This threat group is currently in the development phase and continues to target downstream & midstream oil & gas/liquid natural gas, with a focus on pipeline, maritime, refining.
	**KAMACITE – SINCE 2014** KAMACITE facilitated the 2015 and 2016 Ukraine power events with ELECTRUM and can execute Stage 1 of the ICS Cyber Kill Chain and pivot to OT networks. In early 2022, KAMACITE targeted vulnerabilities in WatchGuard and ASUS firewall and router devices used in small/home office devices with CYCLOPS BLINK malware. In May, KAMACITE targeted another set of routers and IP cameras for initial access, independent of CYCLOPS BLINK operations. Then, in June 2022, KAMACITE was observed communication with the same oblenergo targeted in 2015 Ukraine cyber attack. Last year, despite a primary focus on the electric sector, KAMACITE's CYCLOPS BLINK infrastructure was observed communicating with victims in natural gas, rail, aerospace, food & beverage manufacturing, automotive, and the U.S.
	**ERYTHRITE – SINCE 2021** ERYTHRITE targets industrial infrastructure companies with search engine optimization (SEO) poisoning campaigns and credential stealing and remote access malware throughout 2022, opening the door for this threat group to supply credentials, sensitive information, and remote access to OT environments to third parties. ERYTHRITE has a high volume of activity and uses hundreds of thousands of vulnerable, otherwise legitimate websites as part of their adaptable SEO poisoning campaigns. From there, ERYTHRITE deploys custom, rapidly refreshed. This credential stealing and remote access malware could be deployed in an OT environment for many months before it is detected.

	**WASSONITE – SINCE 2018** WASSONITE has primarily focused their activity on a wide range of industrial sectors in South and East Asia, with an interest in nuclear energy, electric, oil & gas, advanced manufacturing, pharmaceutical, and aerospace industries. As recently as October 2022, Dragos analyzed WASSONITE's nuclear-energy themed spear phishing lures that are used for the deployment of customized variants of the AppleSeed backdoor remote access tool. These customized variants demonstrated significant knowledge of industrial operations, including hard-coded credentials and non-public IP addresses. Once deployed, the AppleSeed backdoor allows WASSONITE to take screenshots, log keystrokes, and collect information and files. It can also upload, download, and execute follow-on commands from a command and control (C2 server). WASSONITE has been observed using Mimikatz and other system tools for lateral movement and file transfers.

Ransomware Risk to Industrial Organizations

Ransomware continued to pose financial and operational risks to industrial organizations worldwide in 2022. Of all the industrial sectors in 2022, ransomware groups targeted the manufacturing industry more than any other, nearly twice as much as the other industrial groups combined, with **72 percent of attacks impacting manufacturers**.

Ransomware attacks impacted these sectors the most in 2022:

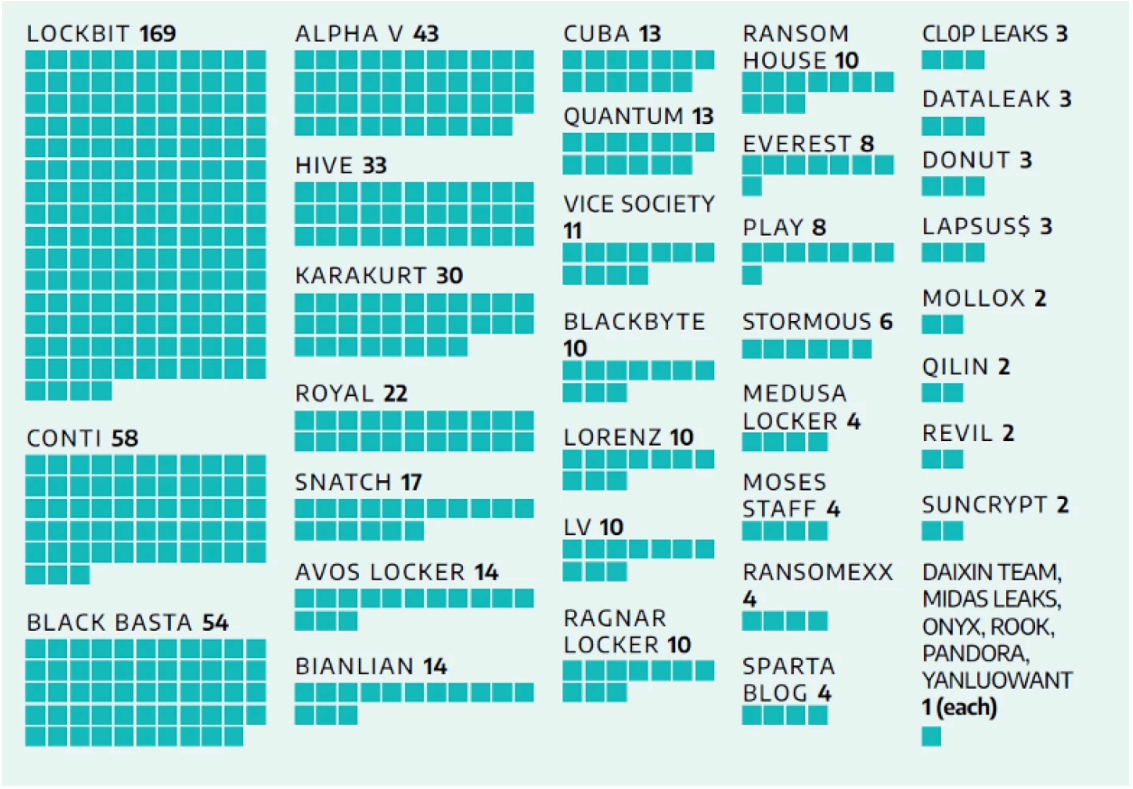
- Manufacturing – 72 percent of attacks (437 ransomware attacks)
- Food & Beverage – 9 percent (52 ransomware attacks)
- Energy – 5 percent (29 ransomware attacks)
- Pharmaceuticals – 4 percent (27 ransomware attacks)
- Oil & Gas – 3 percent (21 ransomware attacks)

Ransomware in the Manufacturing Sector

The manufacturing sector is not only the hardest hit by ransomware attacks, but manufacturers are also often the least mature in their OT security defenses. In fact, from Dragos services engagements in 2022, when we look across the manufacturing industry, 89 percent of manufacturers have limited visibility over their networks and assets and are not able to detect threats in their environment. A full 82 percent of the manufacturing industry has poor network segmentation making it easy for ransomware adversaries to pivot to OT. Finally, 82 percent do not have secure remote connections, and 73 percent are still sharing passwords. This is concerning when disruption of only a few days can have a significant impact on manufacturers and can affect their bottom line. Not only that, but it can also have an impact on the manufacturing supply chain. In February 2022, Kojima Industries Corp, a supplier of Toyota's plastic parts and electronic components, was the victim of a ransomware attack. When Kojima suspended operations, the just in time and Kanban of Toyota production systems resulted in the suspension of Toyota operations as well when they were unable to source the parts needed to continue.

Moves & Changes in the Ransomware Space

The demise of Conti and the introduction of a new version of Lockbit, Lockbit 3.0. Black Basta and several other ransomware groups targeting industrial control systems and operational technologies restructured "the ransomware industry" in 2022.



Despite leading strong with 58 attacks in the early part of 2022, Conti shutdown operations in May after declaring alignment with the Russian Federation. Lockbit quickly took up the mantle – their activity accounted for 169 incidents, or 28 percent of ransomware attacks in 2022. The launch of Lockbit 3.0 helped encourage growth in the ransomware space, reducing the barriers to entry for any adversary to participate in Lockbit 3.0 affiliate enterprises. Making matters worse, the builder used to develop Lockbit 3.0 was leaked online, making it easier for even unskilled adversaries to start up their own ransomware group. Dragos observed activity targeting industrial organizations from 39 different ransomware groups in 2022, and there is the potential for the field to get even more crowded in 2023.

ICS/OT Threat Landscape Takeaways

The webinar concluded with these final points of focus from Dragos ICS/OT adversary hunters:

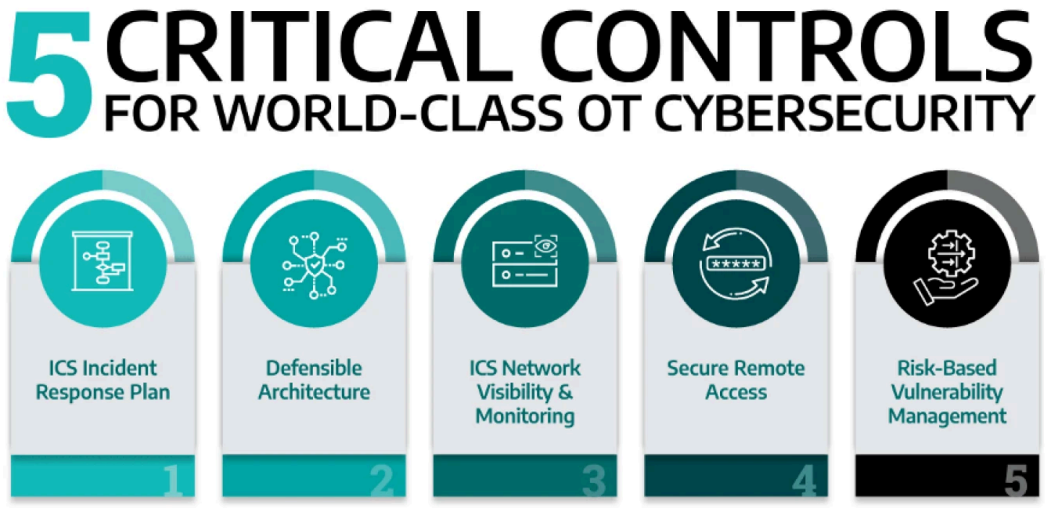
- PIPEDREAM brings forward a new extensible and modular OT focused malware framework that advances attack philosophies first showcased with CRASHOVERRIDE and TRISIS. CHERNOVITE presents a concerning threats to all ICS organizations.
- Dragos-tracked threat groups continue to target ICS/OT entities with both existing and new capabilities.
- BENTONITE has exhibited Stage 1 capability and has shown evidence of OT data exfiltration from oil & gas and manufacturing targets.

- Manufacturing is the standout sector bearing the burden of ransomware attacks by a large margin. All manufacturing organizations should factor in ransomware threats to their threat models.

Watch the 2022 ICS/OT Year in Review Threat Landscape webinar to learn more about these findings.

Recommendations

Dragos recommends five critical controls for OT cybersecurity identified by the SANS Institute for a baseline framework to help defend against adversary activity directed at ICS/OT environments. One way to achieve organizational alignment on implementing the critical controls is to tie the effort back to real-world scenarios involving newly discovered ICS-specific malware and known OT threat group behaviors. If you are just getting started on your ICS/OT cybersecurity journey, these tips will point you in the right direction but for more information.



Download our guide to SANS 5 Critical Controls to learn more.

Download Now

Source: https://www.dragos.com/blog/2022-ics-ot-threat-landscape-recap-what-to-watch-for-this-year/