2022 ICS Attacks: Fewer-Than-Expected on US Energy Sector, But Ransomware Surged

Industrial cybersecurity company Dragos on Tuesday published its ICS/OT Cybersecurity Year in Review report for 2022, sharing details on state-sponsored attacks and malware, as well as ransomware and vulnerabilities.

When it comes to malware designed specifically to target industrial control systems (ICS), the discovery of Pipedream/Incontroller is the most significant event. This ICS attack framework, linked to Russia and aimed at energy facilities, has the capabilities to impact tens of thousands of industrial systems that control critical infrastructure.

In addition, the existence of Industroyer2 came to light last year. The malware, used in an attack aimed at an energy provider in Ukraine, is designed to cause damage by manipulating ICS.

In total, seven pieces of ICS malware have been discovered to date, including Stuxnet, Havex, BlackEnergy2, CrashOverride, and Trisis.

In addition to new malware, 2022 saw two threat actors being added to the list of groups targeting industrial organizations: Chernovite, which is the developer of Pipedream, and Bentonite, an Iran-linked actor that opportunistically targeted maritime oil and gas, government and manufacturing organizations for espionage and disruption.

Dragos has been tracking 20 threat groups that have targeted industrial organizations, eight of which were active in 2022.

When Russia launched its invasion of Ukraine, Dragos predicted

that there would be an increase in attacks targeting operational technology (OT) systems at US organizations in the energy sector.

However, Dragos admitted in its report that it saw fewer-than-expected attacks against this sector, and it’s not aware of any successful ICS-focused attacks on US energy entities.

[Read: Cyber Insights 2023 | ICS and Operational Technology **]**

On the other hand, ransomware attacks surged last year. Dragos tracked more than 600 attacks against industrial organizations, which represents an 87% increase compared to the previous year.

The company has been tracking a total of 57 groups, including 39 that were active in 2022, 30% more than in 2021.

More than 70% of the attacks observed last year were aimed at organizations in the manufacturing sector (437 attacks), followed by the food and beverage industry (52 attacks), energy (29), pharmaceuticals (27), and oil and gas (21).

The most targeted manufacturing subsectors were metal products, automotive, electronics, building materials, industrial equipment and supplies, and plastics.

The LockBit group was responsible for 28% of all attacks recorded last year, followed at a significant distance by Conti, which shut down operations in May, and Black Basta.

Dragos has also analyzed the ICS vulnerabilities disclosed in 2022. The company has reviewed 2,170 CVEs, 27% more than in 2021. Of these, 83% reside deep within the ICS network, and half of the total could lead to loss of view and loss of control.

Dragos has been keeping track of security advisories containing incorrect data and found that 34% of the ones published in 2022 were in this category. Worryingly, 70% of the vulnerabilities described in these advisories were more severe in reality compared to what the advisory said.

The complete Dragos ICS/OT Cybersecurity Year in Review 2022 report is available in PDF format.

Related: New Dragos OT-CERT Provides Free Industrial Cybersecurity Resources

Related: Cybersecurity Experts Cast Doubt on Hackers' ICS Ransomware Claims

https://www.securityweek.com/2022-ics-attacks-fewer-than-expected-on-us-energy-sector-but-ransomware-surged/