waterfall

The Top 10 Cyber Attacks on OT in 2024

There were many cyber attacks on industrial control systems and critical infrastructure worldwide in 2024. Below are just some of the most novel and impactful.

OT/ICS Industries Targeted in 2024

- Building Automation
- Discrete Manufacturing
- Food & Beverage
- Government Infrastructures
- Metals & Mining
- Oil & Gas
- Pharmaceuticals
- Power Utilities
- Process Manufacturing
- Transportation
- Water Utilities

1 Volt Typhoon repeatedly caught “living off the land” in US Critical Infrastructure

When: Ongoing

Industry: Government Infrastructure, Power and Water Utilities, and others

What happened: Responsible for multiple CISA advisories, Chinese nation-state group Volt Typhoon was first active in 2021 but went undiscovered until May 2023. Declared eradicated from networks by the FBI in January, the attackers have repeatedly made efforts to maintain their foothold in infected networks by exploiting multiple zero-day vulnerabilities in SOHO routers, remote-access solutions, and by rebuilding their KV-botnet infrastructure.

Consequence: Loss of confidence in cyber defenses deployed at private utilities with service and supply agreements to the US Government’s global operations.

Significance: Volt Typhoon is determined to maintain stealthy access to critical infrastructure IT networks, with capability to pivot into OT networks at any time.

2 Novel FrostyGoop malware left residents of Lviv freezing in winter

When: January

Industry: Power & Energy Utilities

What happened: A new malware called FrostyGoop was found to be exploiting a zero-day vulnerability in internet-facing Mikrotik routers. The attacker was caught remotely sending Modbus commands to mis-operate an un-named heating utility in Ukraine. Andy Greenberg of Wired connected this to the January attack on Lvivteploenergo, noting the two incident’s similarities and them bearing the hallmarks of Russia’s Sandworm group.

Consequence: In the dead of winter, 600 homes in Lviv's Sykhiv neighborhood lost all heating for two days.

Significance: This may be the first example of nation-state malware punching a hole into OT networks to remotely manipulate critical infrastructure.

3 Moscollector’s IOT sensors disabled by novel Fuxnet malware

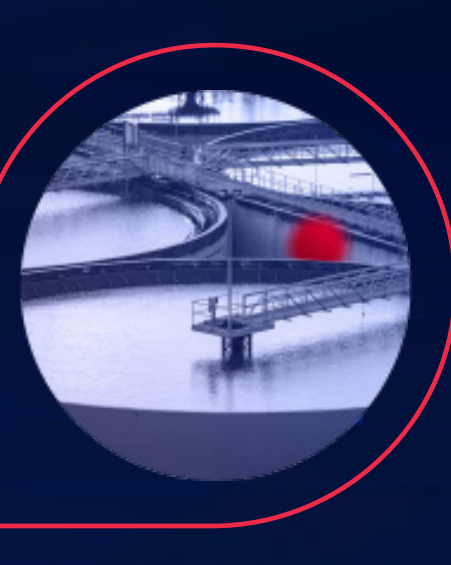
When: April

Industry: Water, Power & Energy Utilities

What happened: BlackJack, nation-state affiliates of Ukraine’s SBU, claimed to have significantly impacted Moscollector’s sensor network. Claroty analyzed a Fuxnet malware sample from the attack adding credibility to BlackJack’s claims. Fuxnet has the capability of sending spurious commands over RS-485/MBus protocols and bricking sensor gateways by destroying their flash memory chips.

Consequence: The attack destroyed or disabled thousands of IOT devices deployed throughout underground utility corridors.

Significance: A novel malware was deployed directly targeting weaknesses in IOT sensor gateways critical to power, wastewater, and heating services during wartime.



4 Muleshoe, Texas sees tanks overflow as Russia tests America’s defenses

When: January

Industry: Water

What happened: Mandiant published analysis showing Sandworm masqueraded as hacktivist group Cyber Army of Russia Reborn (CARR), after CARR bragged about their attack on Mulshoe's water treatment plant. In July, the US Treasury sanctioned Yuliya Pankratova and Denis Degtyarenko, holding them responsible for this attack and other "unsophisticated" attacks in the US and the EU.

Consequence: The attack impacted operations by mis-operating the control system and causing water tanks to overflow for over 30 minutes.

Significance: Pretending to be unsophisticated hacktivists, a nation-state group exposed embarrassing weaknesses in cyber defenses and was likely capable of much worse.

5 Barnett's Couriers suffers the ultimate shutdown: Bankruptcy and Closure

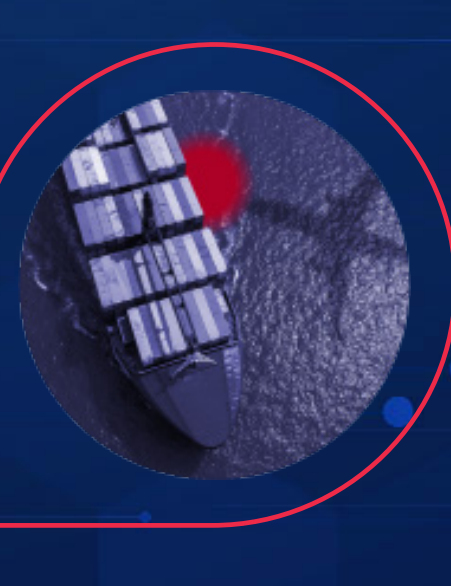
When: April

Industry: Transportation

What happened: A North Wollongong, Australia trucking company was hit by a cyber attack, likely ransomware. The company announced costs related to the attack were so significant that the company was forced to permanently close after operating for 40 years.

Consequence: Freight operations were shut down for three weeks, the company went bankrupt, and all contractors and employees were laid off.

Significance: In the last few years, ransomware-induced bankruptcies and business closures have become more commonplace.



6 BlackBasta halts manufacturing at Keytronic Corp. for two weeks

When: May

Industry: Discrete Manufacturing

What happened: A printed circuit board assembly (PCBA) manufacturer shut down operations as a precaution after detecting unusual activity on their IT network. Later, a BlackBasta ransomware affiliate claimed responsibility and leaked data.

Consequence: $17m in lost revenue and remediation expenses as production in the US and Mexico was shut down for two weeks.

Significance: Ransomware continues to disproportionately impact manufacturers, with many operations being forced to shut down in an abundance of caution, or due to dependencies on third parties and shared services.

7 Pandemonium as Omni Hotels loses all control for 11 Days

When: March

Industry: Building Automation

What happened: A hotel chain with 50 upscale hotels and resorts in North America responded to a cyber attack by shutting down systems to protect data. This decision impacted operations, which depended on the IT network. Omni scrambled to accommodate existing reservations, but new reservations could not be made keeping customers away.

Consequences: An estimated $40m of revenue was lost with operations down at 50 locations, including keycard access to rooms, for 11 days.

Significance: Like the attack on MGM Casinos and Resorts in 2023, malware proves costly when spread through fully integrated but poorly protected building control systems and enterprise networks.

8 Bologna’s RideMovi sees its eBikes totally trashed, electronically

When: July

Industry: Transportation

What happened: A pirate smartphone app called Ride’n Godi allowed users to unlock bikes for free, without needing to subscribe to the official RideMovi service. Illegal bike use became widespread, severely disrupting a large bike sharing service in Bologna. Bikes were reportedlyleft in unforeseen places, with empty batteries and physical damage, taking many weeks to replace or restore the bikes to service.

Consequences: Rendered 80% (~1,300 bikes) of RideMovi’s fleet was damaged, un-traceable, or temporarily unusable.

Significance: As ride sharing, self-driving cars, and other services become increasingly integrated into modern infrastructure, the consequences of such incidents are likely to escalate.

9 Welch Food’s North Eastern Plant Goes Down 3 Weeks

When: February

Industry: Food & Beverage

What happened: A spokesperson at Welch Foods stated a "criminal group" attempted to extort them by encrypting plant systems critical to their juice, jam and jelly production. Next, they brought in over 100 law enforcement personnel and experts to investigate and restore systems into operation.

Consequence: Production was shut down for three weeks and over 200 workers were sent home.

Significance: Food & beverage plants continue to see significant consequences from ransomware attacks.

10 HAL Allergy pharmaceuticals has a bad reaction to ransomware

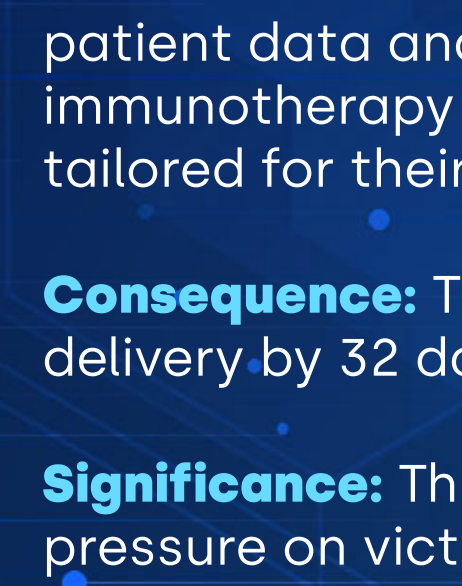
When: February

Industry: Pharmaceuticals

What happened: HAL Allergy fell pretty to a RansomHouse double-extortion ransomware attack in late February, compromising patient data and impacting operations. HAL is a leader in supplying immunotherapy serums and other allergy therapies that are uniquely tailored for their patients.

Consequence: The attack delayed order processing and product delivery by 32 days.

Significance: This attack was carefully timed to exert maximum pressure on victims just before the spring allergy season when therapies are at peak demand.



Pharmaceutical manufacturers must protect both physical operations and sensitive data – data critical to physical processes. This can include patented or trade-secret formulae, manufacturing recipes, patient data for producing tailored therapies, and health records used for prescribed treatments.

Waterfall offers a whole suite of solutions to physically protect critical environments and streamline your operations across OT/IT boundaries. For more info and to learn how Waterfall can help protect your site

Contact Us to Schedule a Free Consultation