waterfall

The Top 10 Attacks of 2023

In 2023, there were many cyber attacks on industrial control systems and critical infrastructure around the world. Here is a selection of the most notorious, impactful, or significant attacks to date.

What OT/ICS industries are in-scope?

Ransomware hits the Dole Food Company

Attack date: 2023-02-23

Industry: Food & Beverage

Cost: $10.5M

Consequence: Halts production and delays shipments in North America for 2 weeks

Summary: Dole chose to shut down production in an abundance of caution and initiate recovery, and stated they are unlikely to recover all costs through insurance.

SAF-Holland Group ransomed by BlackCat (ALPHV) affiliate

Attack date: 2023-03-25

Industry: Discrete Manufacturing

Cost: €40M lost sales and €1M response and recovery

Consequence: Halts production for 2 weeks and causes a 3-month production backlog

Summary: This heavy commercial vehicle builder said recovery took significantly more time than the initial outage, and in an EU filing stated the ransomware attack cost them heavily.

GhostSec hacktivists exploit vulnerabilities at Galil Sewage Corp.

Attack date: 2023-04-09

Industry: Water & Wastewater

Cost: (Unknown)

Consequence: Interrupted wastewater treatment for 1 day

Summary: Despite being warned a week prior by reliable government intelligence, Galil does not disconnect their Unitronics pump controllers from the internet, allowing GhostSec to remotely exploit known vulnerabilities and cause damage to those controllers.

A network intrusion at Badische Stahlwerke (BSW)

Attack date: 2023-04-20

Industry: Process Manufacturing

Cost: (Unknown)

Consequence: Shutdown production and furloughed 850 employees

Summary: The German steelmaker BSW pre-emptively shutdown all production systems in a controlled manner, immediately after discovering "unauthorized access to its network."

Americold ops iced by novel Cactus ransomware threat actor

Attack date: 2023-04-25

Industry: Building Automation

Cost: (Unknown)

Consequence: Shut down all its 250 cold-storage warehouses for 1 week

Summary: Adding to global supply chain challenges, virtually no inbound or outbound shipments are accepted at Americold while they shut down in an abundance of caution, initiate recovery, and file with the US SEC.

22 Danish Critical Energy Infrastructure sites narrowly avoid a suspected nation-state attack

Attack date: 2023-05-11 & 2023-5-22 (two waves)

Industry: Power, Oil & Gas

Cost: (Unknown)

Consequence: Near miss; Some utilities forced into island (stand-alone) mode

Summary: SektorCERT SOC discovered live attacks and compelling evidence that Russia's Sandworm group exploited multiple firewall vulnerabilities to breach critical networks, requiring aggressive defensive action and narrowly avoiding serious consequences.

LockBit ransomware infects Granules India

Attack date: 2023-05-20

Industry: Pharmaceutical

Cost: "Significant revenue loss" reported to India's National Stock Exchange

Consequence: Shutdown production 40+ days

Summary: To control the situation, Granules chose to isolate their network during recovery and restoration, which took extra time to meet strict re-certification, regulatory and quality standards.

Brunswick Corporation

Attack date: 2023-06-13

Industry: Discrete Manufacturing

Cost: up to $85M

Consequence: Lost 10 days production (unrecoverable)

Summary: The well-known manufacturer of Mercury Marine outboard motors suffers a cyber attack and is forced to shut down. Brunswick's CEO said the loss cannot be recovered this fiscal year due to a fully-booked production schedule.

Scattered Spider causes operational chaos for MGM Resorts

Attack date: 2023-09-08

Industry: Building Automation

Cost: $100M lost revenue and $10M in recovery and restoration

Consequence: Lost physical access and services at 19 properties in Las Vegas

Summary: After successfully spear-phishing an employee, the Scattered Spider ransomware gang was able to encrypt 100 VMware ESXi servers, shutting down building management systems, denying physical access through electronic key cards, and more.

Cyber attack freezes DP World's 4 Australian ports

Attack date: 2023-11-10

Industry: Transportation

Cost: Estimated damages in $ millions for time-sensitive perishable goods

Consequence: Shutdown 4 ports for 3 days; 10-day backlog of 30K containers to clear

Summary: After a major cyber attack, DP World pre-emptively shutdown port operations in Melbourne, Freemantle, Botany and Brisbane to investigate. These ports manage 40% of all goods in and out of Australia, and 10% of total container traffic worldwide.

Did you know that Waterfall's Unidirectional Security Gateways and solutions are ideally suited for preventing remote attacks and their serious consequences, like these? For more information or a free consultation, email us at **info@waterfall-security.com**.