Kaspersky ICS CERT

kaspersky

A brief overview of the main incidents in industrial cybersecurity Q2 2026

20.08.2026

Version 1.0

Contents

In Q2 2026, 163 incidents were publicly confirmed by victims. All of these incidents are included in the table at the end of the overview, with select incidents described in detail.

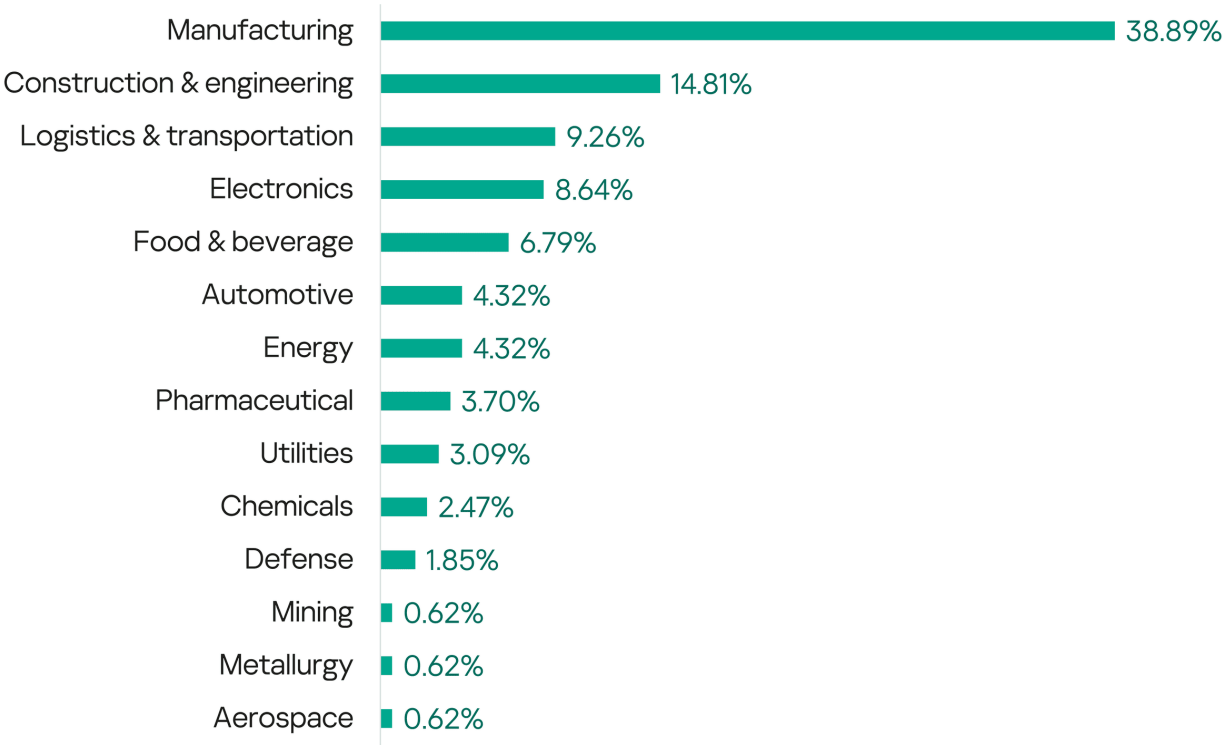
Report at a glance

In our review of publications by researchers investigating threats to industrial organizations, we noted a significant increase in stories describing attacks on control systems intended to cause physical damage. Unsurprisingly, the number of such incidents confirmed by the attacked parties has also increased. The organizations that suffered most were obviously the ones not paying sufficient attention to the security of their automation systems for a number of reasons, primarily economic ones.

We all remember how, in 2023, US utility companies, represented by a coalition of states and the AWWA and NRWA water associations, succeeded in getting a federal appeals court to block new Environmental Protection Agency (EPA) requirements that water utilities undergo mandatory cybersecurity audits. The logical result was a series of incidents at water utilities across the United States beginning in the first quarter and continuing into the third, as we will discuss in our next report. Insufficient security of public utilities, particularly water supply, is a global problem, not just a US-specific one. These utilities are typically small private enterprises with modest IT/OT budgets, making it difficult for them to invest significant resources in information security. We recall the recent cyberincident in Køge, Denmark, which resulted in a ruptured main pipeline. This quarter, we also learned more about the 2025 attacks on water supply facilities in five Polish cities.

For the same reasons as utility automation systems, automatic tank gauge (ATG) systems in petroleum storage facilities remain a popular target for hacktivists. In Q4 2025, the Canadian Cybersecurity Centre (CCCS) reported attacks on these systems; now they have hit facilities in the United States.

Hacktivist enthusiasts repeatedly remind us that many vital automation systems remain under the radar. Many of these systems are concentrated in transportation and logistics infrastructure, particularly rail transport. We all remember the story of the Polish schoolboy who derailed trams. This quarter, a similar incident was reported in Taiwan, resulting in a 48-minute delay to four trains.



April

- GEM Terminal Industry Co.
- Hasbro Inc.
- Hygrade Metal Moulding Manufacturing Corp.
- Labconco Corporation
- Aegis Energy Services
- Allstates WorldCargo
- The Los Angeles County Metropolitan Transportation Authority
- Chemical & Industrial Engineering Inc.
- Toyo Tire Holdings of Americas Inc
- Coral Bay Nickel Corporation / Sumitomo Metal Mining Co.
- Luxottica of America
- Saver NV
- Brownmed
- Kloeckner Metals Corporation
- Good Faith Energy
- David Evans Enterprises
- Pritchard Brown
- Itron Inc.
- Straumann Group
- Drummond Company
- Pediatric Products
- Swedish thermal power plant
- Cota Co.
- Clayco Electric Co.
- Hoshino USA
- Rev Up Brands / Revolution Dancewear
- Sagent Pharmaceuticals
- Innovative Scientific Solutions
- Plastics Extrusion Machinery
- Steel Warehouse Company
- Well Shin Technology Co.
- F&P Georgia Manufacturing
- Universal Pure
- Rich Products Corporation
- H2 Builders
- Medtronic
- API Industries / Aluf Plastics
- Curtis Steel Company
- Syntec Technology Co.
- Quality Carton & Converting
- Indoor Biotechnologies
- Murata Electronics North America
- Taiwan High Speed Rail Corporation
- Denso Corporation

May

- ACME Truck Line
- NCH Corporation
- Diamond Chemical Co.
- Empire Express
- Helix Energy Solutions Group
- AOTCO Metal Finishing
- Flow Systems
- West Pharmaceutical Services
- Cyber Power Systems
- Alliance Roofing
- Swavelle and Mill Creek Fabrics
- Skoda Auto
- New Congol / New Congoleum
- Blue Enterprises / Hogan Transports
- Pulpdent Corporation
- Champion Manufacturing
- Unoaerre
- Heberger
- Froch Enterprise Co.
- Gulfstream Services
- Lamb-Star Engineering
- Foxconn Technology Group
- Oriental Diamond
- Tokyo Hoso Kogyo Corporation
- EAC Consulting
- Obagi Cosmeceuticals
- Visual Creations
- Extant Aerospace
- Bishop Lifting
- Lantronix
- Delon Hampton & Associates
- Carlysle Engineering
- US gas stations
- pewag
- Fluke Corporation
- Kintetsu World Express
- Bomco
- Lusamerica Foods
- International Door
- Perrigo Company
- Beyond Measure Design & Construction
- Kent Industrial
- Rhomberg-Bau
- Sodick Co.
- Barnhart Crane & Rigging Company
- C.N. Wood Co.
- Koa Glass Co.
- Ampex Data Systems Corp.
- ERMI
- KDM Signs
- Fabbrica
- Nickey Kehoe
- Eversource Energy
- Carnival Corporation
- Perma-Chink Systems
- Eagle Oil & Gas
- Johnson-Peltier Electric
- Hallcon Corporation
- Mercury Systems
- Zachary Confections
- Steel Warehouse Company
- Texollini
- Gator Cases
- Takeda Pharmaceuticals USA

June

- Belimed
- Swift Transportation Co. of Arizona
- Lumax International Corp.
- Yorozu Automotive Tennessee
- Powell Electronics
- Asplundh Engineering Services
- Pride Solvent & Chemical Co., Pride Solvent & Chemical Co. of NY, and Pride Solvent and Chemical Co.
- Rockville Fuel & Feed Co.
- MasTec
- Othon
- Murata Power Solutions
- Project Consulting Services
- Distribution Services International
- Mackay Sugar
- Beusa Energy
- Novo Nordisk
- Galvion, Inc.
- Triumph Group
- Landstar System Holdings
- American Future Technology Corporation / iBUYPOWER
- Superior Drywall
- General Plastic Industrial Co. / Katun Corporation
- Kee Wah Bakery
- High Mowing Organic Seeds
- Kodak
- SunSource Borrower
- Stanley Pearlman Enterprises
- Fresenius Kabi USA
- Wright-Ryan Construction
- Circle Floors
- Louisiana Machinery Company
- Ludlum Measurements
- London Hydro
- Tata Electronics
- Cedro Têxtil
- Dongye Precision Machinery Co. / RiFu Precision Industry Co.
- Ludlum Measurements
- Boyd Bros. Transportation / WTI Transport
- Bajaj Auto Limited
- Nidec Chaun Choung Technology Corporation
- Ufagormolzavod
- Sapporo Holdings / Pokka Pte. and Sleeman Breweries
- Domus Design Centers
- Ukrposhta
- Faith Group Co.
- Nissan North America
- Challenge Manufacturing Company
- Yellow Corporation
- Gilman Brothers Company
- Bannari Amman Sugars Limited
- Northern Technologies International Corporation
- Gemeinschaftsstadtwerke Kamen
- Kubota North America Corporation
- Jenike & Johanson

2026

ICS-targeting attack

North Dakota water treatment plant

Utilities

Ransomware

Attacks targeting ICS

A water treatment plant serving the city of Minot, North Dakota, was hit with ransomware in March. City officials confirmed the incident and reported that the water treatment plant and all facilities related to the city's water system had remained operational and safe at all times. According to a letter provided by the city to the FBI and seen by the media, staff detected the ransomware on March 14, forcing operators to revert to manual processes for about 16 hours before a replacement server could be installed. Minot's communications and engagement manager stated that ransomware had been detected on the Minot Water Treatment Plant's SCADA system. According to the letter, a message from those who had installed the ransomware was found on the now-uninstalled SCADA server, but it did not contain a direct request for money and the city did not pay any amount. Minot's communications and engagement manager didn't know which ransomware family was responsible for the attack, but said that the city's technical recovery was nearly complete. The plant used an old server to support its gauge readings while staff prepared a new server.

Thermal power plant in Sweden

Energy

Attacks targeting ICS

According to a Swedish defense official, a group of hackers attempted to disrupt operations at a thermal power plant in Sweden in Spring 2025. Sweden's minister for civil defense said during a press conference in Stockholm on April 15 that the attack was directed at systems that control physical activities and that the attack was unsuccessful because of the facility's built-in security protection. The targeted plant wasn't named. Sweden's security service investigated the incident and identified alleged perpetrators that are believed to have links to Russia.

Taiwan high speed rail

Transportation, logistics

Denial of operations

Attacks targeting ICS

Cyber-physical consequences

A student in Taiwan was arrested for interfering with the TETRA (TErrestrial Trunked RAdio) communication system used by Taiwan High Speed Rail Corporation (THSRC). According to local media reports, the student halted four trains for 48 minutes on April 5 by using software-defined radio (SDR) communications and handheld radios to transmit a high-priority "General Alarm" signal, triggering emergency braking procedures. Before the attack, the student intercepted and decoded TETRA radio parameters using SDR equipment he had bought online and then programmed them into handheld radios to impersonate legitimate beacons. The police also found that an accomplice provided the

attacker with some critical THSRC parameters that enabled the attack. THSRC's radio system has reportedly been in service for 19 years and its parameters were apparently not rotated during that time, allowing the attacker to bypass seven verification layers. Following the incident, THSRC examined the logs and found that the signal had been sent from a radio beacon that hadn't been assigned for duty. Upon checking that the device was not missing, a plausible scenario was unauthorized cloning, and the police were alerted.

U.S. gas stations

Energy

Attacks targeting ICS

According to CNN, U.S. officials suspect that Iranian-linked hackers were behind a series of breaches involving automatic tank gauge (ATG) systems used to monitor fuel storage tanks. The systems were accessible online without password protection, allowing attackers to manipulate the display readings viewed by operators to output incorrect fuel levels. According to officials, the incidents did not result in physical damage. The sources briefed on the investigation said Iran's history of targeting gas tank systems is one reason the country is a top suspect. But, the sources cautioned, the U.S. government may not be able to definitively determine who was responsible because of a lack of forensic evidence left by the hackers.

In June, The U.S. Cybersecurity and Infrastructure Security Agency (CISA), FBI, NSA, Department of Energy, and other U.S. government partners published a joint notice warning that hackers are targeting internet-exposed automatic tank gauge (ATG) systems used to monitor fuel and liquid storage tanks across various critical infrastructure sectors.

Polish water supply

Utilities, water supply

Attacks targeting ICS

Poland's Agencja Bezpieczeństwa Wewnętrznego (ABW) disclosed in May that attackers had breached water treatment facilities in five Polish towns during 2025: Jabłonna Lacka, Szczytno, Małdyty, Tolkmicko and Sierakowo. By gaining access, in some cases, to industrial control systems, the attackers were able to alter the technical parameters of equipment, which posed a direct risk to the continuity of their operation and, consequently, the supply of water to the population. Earlier in 2025, Deputy Prime Minister of Poland and Minister of Digital Affairs Krzysztof Gawkowski confirmed to the Onet.pl news portal that an attack on an unnamed water and sewage infrastructure of a large Polish city had occurred on August 13, 2025.

Attacks leading to denial of operations

Foxconn

Electronics, manufacturing

Denial of IT systems and operations

Ransomware

Multinational electronics manufacturer Foxconn Technology Group, headquartered in Taiwan where the company is known as Hon Hai, confirmed on May 12 to news sources that the company's North American factories had experienced a cyberattack. According to Foxconn, the cybersecurity team immediately activated the response mechanism and implemented multiple operational measures to ensure the continuity of production and delivery. The affected factories were in the process of resuming normal production. An employee at one of Foxconn's Wisconsin factories told DysruptionHub on May 5 that they began dealing with Wi-Fi issues on May 1 and were sent home due to the network outages. Computers were not working and employees had to use paper and pen for several different tasks. Internal notices reviewed by DysruptionHub also cited ongoing network issues affecting operations. One notice said the company could not continue normal activities and that operations would remain closed for the rest of the day to ensure the safety, efficiency, and integrity of company processes. A separate notice said there would be no first-shift production on May 5 because of continued network issues. On May 12 the company reported the attack in the bulletin on the Taiwan Stock Exchange portal. The day before, Nitrogen ransomware group listed Foxconn on its data leak website. The group claimed to possess 8 terabytes of Foxconn data, comprising more than 11 million files, and posted sample images it described as proof of leakage.

West Pharmaceutical Service

Pharmaceutical, manufacturing

Denial of IT systems, services and operations, data leakage

Ransomware

U.S. manufacturer of injectable pharmaceutical packaging and delivery systems West Pharmaceutical Services Inc. disclosed that it had experienced a cyberattack in a Form 8-K filing with the U.S. Securities and Exchange Commission (SEC). West Pharmaceutical first detected the incident on May 4, and three days later determined that the incident was a material cybersecurity attack in which certain data was exfiltrated by an unauthorized party and certain systems were encrypted. The incident had temporarily disrupted the company's global business operations. West Pharmaceutical notified law enforcement agencies and brought in third-party cyber forensic experts. The company has restored its core enterprise systems. Critical processes for shipping, receiving, and manufacturing have restarted at some sites with restoration of the remaining sites in process, although the timeline for full recovery remains unknown. On May 13, an update on the company's website stated that based on

the findings of Palo Alto Networks Unit 42, the available evidence indicated that the identified unauthorized activity has been contained and the immediate risk to West's operational environment has been mitigated.

Unoaerre

Manufacturing

Denial of IT systems and operations

Ransomware

Italian jewelry manufacturing company Unoaerre was the victim of a cyberattack that paralyzed its operating system, leading the cybercriminals to demand a ransom of EUR 3.8 million in Bitcoin. According to the local news outlet, the attack happened on May 8. The plant was gradually emptied and employees were asked to leave the premises as a precaution, while IT specialists began operations to isolate the systems and contain the intrusion. Initial investigations suggested that the attack may have links to countries in the Middle East and Eastern Europe. Despite the interruption, initial checks indicated that the damage was not irreversible and that production could resume. Technical investigations remained to determine whether sensitive data, commercial information, or confidential projects were accessed.

Mackay Sugar

Food and beverage, manufacturing

Denial of services and operations

Ransomware

Australian sugar producer Mackay Sugar disclosed on June 10 that it had suffered a cyberattack affecting some of its operations. Advocacy group Canegrowers confirmed the incident had shut down sugar milling and cane haulage across the Farleigh and Racecourse mills just outside Mackay. Canegrowers Mackay chairman said many growers were issued with cease harvesting advice by Mackay Sugar early on June 10, adding that the cyberincident had affected multiple parts of the business. In an update on June 12, Mackay Sugar stated that the company had recommenced a limited manual crushing operation at the Farleigh Mill, processing cane that had been harvested prior to the incident. While some operations have resumed in a controlled manner, key cane supply and logistics systems remained subject to ongoing restoration and no additional cane was being accepted at the mills.

On June 17, Mackay Sugar said the investigation had identified evidence of unauthorized access by an external party to parts of the IT environment. The company's monitoring has identified that an external party has made a claim about the company on a dark web site. Mackay Sugar worked urgently to verify the claims, including the nature and extent of any information which may have been accessed. The company continued to progress the restoration of the systems that support cane supply, harvesting and mill operations.

On June 26, Mackay Sugar issued a report that all three Mackay Sugar mills were now operational. The Gentlemen ransomware group claimed responsibility for the attack on Mackay Sugar on June 15.

Kintetsu World Express

Transportation, logistics

Denial of IT systems and operations

Japanese logistics provider Kintetsu World Express (KWE), which offers air and sea cargo services globally, has issued a statement announcing an IT outage that occurred in the early hours of May 15, 2026, at KWE-Kintetsu World Express (S) Pte Ltd., a subsidiary of the group, following unauthorized access by a third party. After the intrusion, the affected systems were taken offline and isolated. This incident has affected some of Singapore's air export-related operations and domestic warehousing operations. No impact on operations outside of Singapore or on core business systems has been confirmed. On May 20, the company issued a statement providing an update and said that all affected operations had returned to normal. Immediately after this incident occurred, the group established an emergency response headquarters and, in cooperation with external security experts, took action based on its cybersecurity business continuity plan (BCP).

Katun Corporation

Manufacturing

Denial of IT systems and operations

Taiwanese manufacturer of compatible toner cartridges for copiers and printers General Plastic Industrial Co., Ltd. announced unauthorized access to the computer network of its subsidiary Katun Corporation in a bulletin published on the Taiwan Stock Exchange (TWSE) portal on June 16. Upon learning of the unauthorized access, the IT department immediately carried out system isolation procedures to prevent the impact from expanding and simultaneously activated defense measures. The company assessed the operational impact of this incident, including the temporary suspension of shipments. Shipment operations were in the process of being restored and have gradually resumed.

Cedro Têxtil

Manufacturing

Denial of IT systems and operations

Brazilian textile manufacturer Cedro Têxtil confirmed it has fallen victim to a cybersecurity incident that has affected its technological environments and impacted the operation of certain corporate systems. An employee told the media outlet Sete Dias that the core system supporting the company's entire network had gone offline, and that operations had been suspended since June 18 and were expected to resume after 10:00 PM on June 22. The company has mobilized experts to bring the situation under control and is working to safely

restore operations. The company has not yet identified the perpetrator of the attack.

Incidents at large organizations

Medtronic

Manufacturing

Data leakage

American-Irish medical device manufacturing company Medtronic disclosed a cyberattack in a Form 8-K filing with the U.S. Securities and Exchange Commission (SEC). The company announced on April 24 that an unauthorized third party had accessed data in some of the company's information technology systems. Based on its investigation, Medtronic has not identified any impact to its products, patient safety, connections to customers, manufacturing and distribution operations, financial reporting systems, or ability to meet patient needs. In addition, the company did not expect the incident to have a material impact on its business or financial results. On the same day, April 24, Medtronic reported a cyberattack on its website. According to Medtronic's website, the networks that support the company's corporate IT systems, products, and manufacturing and distribution operations are separate. Hospital customer networks remain separate from Medtronic IT networks and are secured and managed by customers' IT teams. The company has been working to identify any personal information that may have been accessed.

Skoda Auto

Automotive, manufacturing

Personal data leakage

Czech automobile manufacturer Skoda Auto discovered that unauthorized individuals had exploited a vulnerability in the software used to run its online shop during a recent technical security monitoring exercise. The company's online shop contained customers' personal information, including full names, postal addresses, email addresses, phone numbers, order history, and hashed passwords. No credit card numbers or other financial information were stored there, as this information is exclusively processed by payment service providers. As a precaution, Skoda's online shop was taken offline as soon as the incident was discovered. The vulnerability has since been eliminated, and the incident has been handed over to a specialized IT forensics department for technical analysis. The incident has also been reported to the relevant data protection authority. The company couldn't say for sure whether customers' personal details were ever copied or retrieved.

Denso

Automotive, manufacturing

Data leakage

Ransomware

Japanese automotive components manufacturer Denso Corporation confirmed on its website that its group companies' facilities located in Italy and Morocco have suffered unauthorized access to their networks by a third party. After learning about the unauthorized access on March 28, 2026, the company immediately established an internal emergency response headquarters. As a result of investigations, the company confirmed that it can't be ruled out that some information concerning external parties and the company may have been illegally extracted by a third party due to the unauthorized access. At the time of notification, no significant impact has been confirmed on production activities or product deliveries to customers as a result of this incident. The Qilin ransomware group claimed responsibility for the attack on Denso in April.

Novo Nordisk

Pharmaceutical, manufacturing

Personal data leakage

Extortion

Danish pharmaceutical company Novo Nordisk has disclosed a cyberattack involving unauthorized access to a limited number of internal IT systems. The company took several of its systems offline following the incident, notified authorities, and investigated with the assistance of external cybersecurity experts. The company's core business operations were not impacted and remained up and running. Novo Nordisk discovered that certain non-public data, including personal data, were copied externally without authorization. In a June 18 update, the company said that the incident affected a limited amount of information related to patients participating in certain clinical trials. According to Novo Nordisk's breach notice, this information is not directly linked to any patients by name or other direct identifiers. Healthcare providers affected by the incident were informed that compromised data may include company name, registration number, contact email address, phone number, office location, and WhatsApp details. The FulcrumSec extortion group claimed on June 16 to have stolen more than a terabyte of data from Novo Nordisk and said it was exploring selling parts of the data after unsuccessfully demanding $25 million from the company.

Tata Electronics

Electronics, manufacturing

Personal data leakage, supply chain

Ransomware

Indian electronics company Tata Electronics confirmed to Reuters in a statement on June 22 that it had identified a cybersecurity incident on some of its systems a few weeks ago, after researchers said The World Leaks groups posted purported component design and specification papers of Apple and Tesla, both customers of the Indian group. Response protocols were deployed immediately, and the incident has had no impact on the company's operations

across businesses, which remained unaffected. A source familiar with the matter said that Tata Electronics had received a ransom demand related to the incident. Reuters reported that Tata Electronics informed some employees at its iPhone assembly operations about the data breach, according to a second industry source familiar with the matter. The report also said Apple was investigating the incident.

The World Leaks ransomware group claimed responsibility for the attack on Tata Electronics on June 12. Among the leaked information, there are multiple directories and documents allegedly containing manufacturing data for Apple products, including internal component schematics, PCB designs, material specifications, and SDK files. The World Leaks dark web site said the Tata Electronics data consists of more than 200,000 files totaling over 630 gigabytes.

Ukrposhta

Logistics, transportation

Denial of IT systems and IT services

Hacktivist

Ukrainian national postal operator Ukrposhta reported temporary disruptions to its mobile app following a cyberattack on its IT systems. The attack, which occurred on the night of June 24 to 25, led to instability and outages of digital services. Ukrposhta confirmed the incident, saying that experts worked to quickly restore normal operation of the platform. Ukrposhta added that they will notify users after the application is fully restored. The IT Army of Russia hacktivist group claimed responsibility for the attack on June 25. The group alleged it had breached Ukrposhta's infrastructure several weeks earlier, gained access to one of the company's servers and exfiltrated a database containing user information, along with other internal data.

Appendix. Full list of confirmed incidents

Victim	Industry / Profile	Country	Impact features	Date of notification Date of incident (if known) Suspected attackers
GEM Terminal Industry Co.	Electronics, manufacturing / Manufacturer of electrical terminals	Taiwan	Denial of IT systems Ransomware	April 1, 2026 Gentlemen
Medtronic	Manufacturing / Medical device manufacturer	USA	Personal data leakage	April 24, 2026
Hasbro Inc.	Manufacturing / Toy manufacturer	USA	Denial of IT systems and services	April 1, 2026 March 28, 2026
Minot water treatment plant	Utilities	USA	Ransomware Attacks targeting ICS	April 1, 2025 March 14, 2025
Swedish thermal power plant	Energy	Sweden	Attacks targeting ICS	April 15, 2026
Cota Co.	Manufacturing / Manufacturer of hair care products	Japan	Denial of IT systems Ransomware	April 15, 2026 March 27, 2026
Itron Inc.	Utilities / Utility technology provider	USA	Not specified	April 13, 2026
Coral Bay Nickel Corporation / Sumitomo Metal Mining Co.	Metallurgy, manufacturing / Non-ferrous metals producer	Philippines	Denial of IT systems Ransomware	April 8, 2026 April 2, 2026
Saver NV	Utilities / Waste management and recycling company	Netherlands	Denial of IT systems and services, personal data leakage	April 9, 2026 DragonForce

			Ransomware	
Straumann Group	Manufacturing / Dental implant manufacturer	Switzerland	Personal data leakage Ransomware	April 13, 2026 0apt
Well Shin Technology Co.	Electronics, manufacturing / Consumer electronics manufacturer	Taiwan	Denial of IT systems	April 20, 2026
Syntec Technology Co.	Electronics, manufacturing / Manufacturer of PC-based CNC controllers and advanced motion control solutions	Taiwan	Denial of IT systems	April 29, 2026
Chemical & Industrial Engineering Inc.	Construction and engineering / Engineering services	USA	Personal data leakage Ransomware	April 5, 2026 August 2025 Cicada3301
Hygrade Metal Moulding Manufacturing Corp.	Manufacturing / Metal roll-form manufacturer	USA	Personal data leakage	April 1, 2026 July 25, 2025
Kloeckner Metals Corporation	Manufacturing / Metals manufacturing company	USA	Personal data leakage	April 10, 2026 February 23, 2026
Good Faith Energy	Construction and engineering / Solar panel installation	USA	Personal data leakage	April 10, 2026
David Evans Enterprises	Construction and engineering / Engineering services company	USA	Personal data leakage	April 10, 2026 February 26, 2026
Rev Up Brands / Revolution Dancewear	Manufacturing / Clothing manufacturer	USA	Personal data leakage	April 17, 2026 March 16, 2026
Drummond Company	Mining / Coal mining processor	USA	Personal data leakage	April 14, 2026 February 20, 2026

Sagent Pharmaceuticals	Pharmaceutical, manufacturing / Pharmaceutical manufacturing company	USA	Personal data leakage Ransomware	April 17, 2026 February 11, 2026 Worldleaks
Pediatric Products	Manufacturing / Medical products manufacturing company	USA	Personal data leakage	April 14, 2026 February 17, 2026
Universal Pure	Food and beverage, logistics / Cold chain logistics and food safety provider	USA	Personal data leakage	April 21, 2026 August 20, 2024
Labconco Corporation	Manufacturing / Laboratory equipment manufacturing company	USA	Personal data leakage	April 1, 2026 December 8, 2025
Aegis Energy Services	Manufacturing / Manufacturer of combined heat and power systems	USA	Personal data leakage	April 2, 2026 September 17, 2025
Allstates WorldCargo	Logistics and transportation / Transportation company	USA	Personal data leakage	April 2, 2026
Toyo Tire Holdings of Americas Inc	Manufacturing / Tire manufacturer	USA	Personal data leakage	April 6, 2026
Brownmed	Manufacturing / Medical device manufacturing company	USA	Personal data leakage	April 9, 2026
Pritchard Brown	Manufacturing / Manufacturer of non-wood building material	USA	Personal data leakage	April 10, 2026 September 16, 2025
Clayco Electric Co.	Construction and engineering / Electrical	USA	Personal data leakage Ransomware	April 15, 2026 Qilin

	contracting company			
Innovative Scientific Solutions	Defense, manufacturing / Measurement tools, pressure-sensitive paint systems, custom timing and control device manufacturer	USA	Personal data leakage	April 17, 2026
Plastics Extrusion Machinery	Manufacturing / Manufacturer of downstream equipment for the PVC pipe and custom profile industries	USA	Personal data leakage Ransomware	April 17, 2026 Akira
F&P Georgia Manufacturing	Automotive, manufacturing / Manufacturer of subframes, modular assemblies, lower arms, trailing arms, pedals, stampings	USA	Personal data leakage	April 20, 2026 Nitrogen
H2 Builders	Construction and engineering / Luxury home construction	USA	Personal data leakage	April 23, 2026
API Industries / Aluf Plastics	Manufacturing / Plastics and packaging manufacturing company	USA	Personal data leakage	April 24, 2026
Quality Carton & Converting	Manufacturing / Packaging and containers manufacturer	USA	Personal data leakage Ransomware	April 29, 2026 February 10, 2026 Akira
Indoor Biotechnologies	Manufacturing / Manufacturer of highly purified proteins, allergen products, immunoassays	USA	Personal data leakage	April 30, 2026 March 2, 2026

Steel Warehouse Company	Manufacturing / Producer of steel products	USA	Personal data leakage Ransomware	April 17, 2026 January 23, 2025 Cactus
Luxottica of America	Manufacturing / Manufacturer of ophthalmic lenses, frames, sunglasses	USA	Personal data leakage	April 8, 2026
Hoshino USA	Manufacturing / Manufacturer of guitars and drums	USA	Personal data leakage	April 15, 2026
Curtis Steel Company	Manufacturing / Steel processing services	USA	Personal data leakage	April 28, 2026 Akira
Rich Products Corporation	Food and beverage, manufacturing / Food and beverage manufacturing company	USA	Personal data leakage	April 22, 2026 November 13, 2025
Murata Electronics North America	Electronics, manufacturing / Electronics components manufacturer	USA	Personal data leakage	April 30, 2026 March 2025
Foxconn Technology Group	Electronics, manufacturing / Electronics manufacturer	Taiwan	Denial of IT systems and operations Ransomware	May 12, 2026 May 1, 2026 Nitrogen
West Pharmaceutical Services	Pharmaceutical, manufacturing / Manufacturer of injectable pharmaceutical packaging and delivery systems	USA	Denial of IT systems, services and operations, data leakage Ransomware	May 7, 2026 May 4, 2026
Cyber Power Systems	Electronics, manufacturing / Manufacturer of uninterruptible power supply (UPS) systems, power	Taiwan	Denial of IT systems	May 7, 2026

	distribution units (PDUs), rack enclosures and surge protectors			
Heberger	Construction and engineering / Construction company	Germany	Not specified	May 11, 2026 May 7, 2026
Unoaerre	Manufacturing / Jewelry manufacturer	Italy	Denial of IT systems and operations Ransomware	May 10, 2026 May 8,2026
Froch Enterprise Co.	Manufacturing / Manufacturer of metal pipes, tubes, bars, plates, sheets, and coils	Taiwan	Denial of IT systems	May 11, 2026
Oriental Diamond	Manufacturing / Fine diamond jewelry manufacturer	Japan	Denial of IT systems, personal data leakage Ransomware	May 12, 2026 May 4, 2026 Gentlemen
Kintetsu World Express	Logistics and transportation / Logistics provider	Japan	Denial of IT systems and operations	May 17, 2026 May 15, 2026
Rhomberg-Bau	Construction and engineering / Construction company	Austria	Denial of IT systems	May 21, 2026
Kent Industrial	Manufacturing / Industrial machinery and surface grinder manufacturer	Taiwan	Denial of IT systems	May 20, 2026
Skoda Auto	Automotive, manufacturing / Automobile manufacturer	Czechia	Personal data leakage	May 8, 2026
Taiwan High Speed Rail Corporation	Logistics and transportation	Taiwan	Denial of operations	April 30, 2026 April 5, 2026

			Attacks targeting ICS	
US gas stations	Energy	USA	Attacks targeting ICS	May 15, 2026
The Los Angeles County Metropolitan Transportation Authority	Logistics and transportation	USA	Denial of services Hacktivist	April 2, 2026 March 2026 Ababil of Minab
Tokyo Hoso Kogyo Corporation	Construction and engineering / Construction and civil engineering company	Japan	Denial of IT systems, personal data leakage Ransomware	May 12, 2026 April 2, 2026 Qilin
Sodick Co.	Manufacturing / Manufacturer of numerically controlled (NC) electric discharge machines	Japan	Denial of IT systems	May 21, 2026 May 15, 2026
Koa Glass Co.	Manufacturing / Manufacturer of silver glass antimicrobials	Japan	Denial of IT systems Ransomware	May 26, 2026 May 17,2026 Gentlemen
Denso Corporation	Automotive, manufacturing / Automotive components manufacturer	Japan	Denial of IT systems Ransomware	April 30, 2026 March 28, 2026 Qilin
Diamond Chemical Co.	Chemicals, manufacturing / Manufacturer of laundry, ware wash, housekeeping, sanitizing products	USA	Personal data leakage	May 5, 2026 July 26, 2025
Gulfstream Services	Energy / Oilfield rental tool and industrial services company	USA	Personal data leakage Ransomware	May 11, 2026 Play
Empire Express	Logistics and transportation /	USA	Personal data leakage	May 5, 2026

	Transportation company		Ransomware	June 27, 2025 Dragonforce
ACME Truck Line	Logistics and transportation / Transportation company	USA	Personal data leakage Ransomware	May 1, 2026 February 18, 2026 Medusa
NCH Corporation	Chemicals, manufacturing / Chemical manufacturing company	USA	Personal data leakage Ransomware	May 1, 2026 Embargo
Lamb-Star Engineering	Construction and engineering / Civil engineering firm	USA	Personal data leakage	May 11, 2026 January 20, 2026
New Congol / New Congoleum	Manufacturing / Flooring manufacturer	USA	Personal data leakage Ransomware	May 8, 2026 March 24, 2026 Dragonforce
Blue Enterprises / Hogan Transports	Logistics and transportation / Transportation company	USA	Personal data leakage	May 8, 2026 October 25, 2025 Qilin
pewag	Manufacturing / Chain manufacturer	USA	Personal data leakage	May 15, 2026 March 30, 2026
Carlysle Engineering	Construction and engineering / Fire protection safety provider	USA	Denial of IT systems, personal data leakage Ransomware	May 14, 2026 March 23, 2026
Extant Aerospace	Defense, manufacturing / Aerospace manufacturer	USA	Personal data leakage	May 13, 2026 August 23, 2025
Fluke Corporation	Manufacturing / Manufacturer of industrial test, measurement, and diagnostic equipment	USA	Personal data leakage Ransomware	May 15, 2026 August 10, 2025 Clop

Barnhart Crane & Rigging Company	Construction and engineering / Lifting, rigging, and transportation provider	USA	Personal data leakage Ransomware	May 21, 2026 April 23, 2025 Chaos
Eversource Energy	Utilities / Energy supplier	USA	Personal data leakage	May 27, 2026 April 2026
Bomco	Manufacturing / Precision metal component manufacturer	USA	Personal data leakage	May 18, 2026
Perrigo Company	Manufacturing / Health and wellness product manufacturer	USA	Personal data leakage	May 19, 2026 March 4, 2026
Carnival Corporation	Logistics and transportation / Marine transportation company	USA	Personal data leakage Ransomware	May 27, 2026 April 10, 2026 ShinyHunters
Helix Energy Solutions Group	Energy / Energy services company	USA	Personal data leakage Ransomware	May 5, 2026 Clop
EAC Consulting	Construction and engineering / Civil engineering, transportation engineering, construction management	USA	Personal data leakage Ransomware	May 12, 2026 Play
Bishop Lifting	Manufacturing / Manufacturer of custom lifting solutions	USA	Personal data leakage	May 13, 2026
Ampex Data Systems Corp.	Electronics, manufacturing / Manufacturer of rugged digital data storage systems, recorders	USA	Personal data leakage Ransomware	May 26, 2026 March 21, 2026 Play

Beyond Measure Design & Construction	Construction and engineering / Construction company	USA	Personal data leakage Ransomware	May 19, 2026 Pear
ERMI	Manufacturing / Manufacturer of specialized medical equipment	USA	Personal data leakage	May 26, 2026 February 15, 2025
Eagle Oil & Gas	Energy / Oil and gas exploration and production company	USA	Personal data leakage Ransomware	May 28, 2026 October 13, 2025 Akira
Texollini	Manufacturing / Textile manufacturer	USA	Personal data leakage	May 29, 2026 February 16, 2026
Johnson-Peltier Electric	Construction and engineering / Heavy industrial electrical construction	USA	Personal data leakage	May 28, 2026 March 10, 2026
Alliance Roofing	Construction and engineering / Roofing and waterproofing contractor	USA	Denial of IT systems, personal data leakage Ransomware	May 7, 2026 October 6, 2025 Akira
Lusamerica Foods	Food and beverage, manufacturing / Seafood processor	USA	Personal data leakage Ransomware	May 18, 2026 January 31, 2025 Play
C.N. Wood Co.	Construction and engineering / Construction company	USA	Personal data leakage	May 22, 2026 May 6, 2026
Hallcon Corporation	Logistics and transportation / Transportation company	USA	Personal data leakage	May 28, 2026 November 13, 2025
Perma-Chink Systems	Manufacturing / Manufacturer of log home restoration products	USA	Personal data leakage	May 27, 2026 May 7, 2026

Swavelle and Mill Creek Fabrics	Manufacturing / Textile manufacturer	USA	Personal data leakage	May 7, 2026 September 26, 2025
AOTCO Metal Finishing	Manufacturing / Electroplating services	USA	Personal data leakage Ransomware	May 6, 2026 March 27, 2026 DragonForce
Pulpdent Corporation	Manufacturing / Dental research and manufacturing company	USA	Personal data leakage	May 8, 2026 March 13, 2026
Champion Manufacturing	Manufacturing / Patient recliners manufacturer	USA	Personal data leakage	May 8, 2026 January 2026
Lantronix	Manufacturing / Manufacturer of industrial and enterprise IoT products	USA	Personal data leakage Ransomware	May 13, 2026 April 13, 2025 Hunters International
Mercury Systems	Electronics, manufacturing / Microelectronics, radio frequency and microwave component, secure memory, digital signal processor manufacturer	USA	Personal data leakage	May 28, 2026
Gator Cases	Manufacturing / Protective case manufacturer	USA	Denial of IT systems, personal data leakage Ransomware	May 29, 2026 April 28, 2026 Gentlemen
Zachary Confections	Food and beverage, manufacturing / Confectionery specialties manufacturer	USA	Denial of IT systems, personal data leakage Ransomware	May 28, 2026 April 20, 2026 Qilin

KDM Signs	Manufacturing / Signage manufacturing	USA	Denial of IT systems, personal data leakage	May 26, 2026 March 11, 2026
Obagi Cosmeceuticals	Pharmaceutical, manufacturing / Skin care systems manufacturer	USA	Personal data leakage	May 12, 2026 August 19, 2025
Visual Creations	Manufacturing / Manufacturer of POP displays and store fixtures	USA	Personal data leakage	May 12, 2026
Delon Hampton & Associates	Construction and engineering / Engineering company	USA	Personal data leakage Ransomware	May 13, 2026 DragonForce
International Door	Manufacturing / Door manufacturer	USA	Personal data leakage Ransomware	May 18, 2026 Nightspire
Fabbrica	Manufacturing / Building facades and curtain wall manufacturer	USA	Personal data leakage Ransomware	May 26, 2026 DragonForce
Takeda Pharmaceuticals USA	Pharmaceutical, manufacturing / Pharmaceutical manufacturing company	USA	Personal data leakage	May 29, 2026 February 23, 2026
Flow Systems	Manufacturing / Flow measurement component and integrated test system manufacturer	USA	Personal data leakage	May 6, 2026
Steel Warehouse Company	Manufacturing / Manufacturer and processor of steel products	USA	Personal data leakage	May 28, 2026

Mackay Sugar	Food and beverage, Manufacturing / sugar producer	Australia	Denial of services and operations Ransomware	June 10, 2026 Gentlemen
Belimed	Manufacturing / Manufacturer of advanced cleaning, disinfection, and sterilization systems	Switzerland	Data leakage Ransomware	June 1, 2026 INC Ransom
Lumax International Corp.	Electronics, engineering / Distribution of electronic and telecommunication components and materials, system integration engineering services	Taiwan	Denial of IT systems Ransomware	June 2, 2026 Lockbit 5.0
Novo Nordisk	Pharmaceutical, manufacturing / Pharmaceutical manufacturing company	Denmark	Personal data leakage Extortion	June 11, 2026 FulcrumSec
General Plastic Industrial Co. / Katun Corporation	Manufacturing / Manufacturer of compatible toner cartridges for copiers and printers	Taiwan	Denial of IT systems and operations	June 16, 2026 June 2, 2026
Kee Wah Bakery	Food and beverage, manufacturing / Bakery product manufacturer	China	Denial of IT systems	June 16, 2026 June 12, 2026
London Hydro	Utilities, energy / Power utility	Canada	Personal data leakage	June 20, 2026
Tata Electronics	Electronics, manufacturing / Electronics company	India	Personal data leakage, supply chain Ransomware	June 22, 2026 World Leaks
Kodak	Chemicals, manufacturing /	USA	Data leakage	June 17, 2026

	Commercial print, packaging, advanced materials, and chemicals		Extortion	ShinyHunters
Bajaj Auto Limited	Automotive, manufacturing / Manufacturer of cars, scooters, and motorcycles	India	Denial of IT systems Ransomware	June 23, 2026
Nidec Chaun Choung Technology Corporation	Electronics, manufacturing / Manufacturer of thermal management products	Taiwan	Denial of IT systems	June 24, 2026 June 22, 2026
Cedro Têxtil	Manufacturing / Textile manufacturer	Brazil	Denial of IT systems and operations	June 22, 2026
Ufagormolzavod	Food and beverage, Manufacturing / dairy producer	Russia	Denial of services	June 24, 2026
Dongye Precision Machinery Co. / RiFu Precision Industry Co.	Manufacturing / Industrial equipment manufacturer	Taiwan	Denial of IT systems	June 22, 2026
Faith Group Co.	Manufacturing / Cosmetics manufacturer	Japan	Denial of IT systems Ransomware	June 26, 2026
Ukrposhta	Logistics and transportation / National postal operator	Ukraine	Denial of IT systems and IT services Hacktivist	June 25, 2026 IT Army of Russia
Sapporo Holdings / Pokka Pte. and Sleeman Breweries	Food and beverage, manufacturing / Beverage manufacturer	Japan	Not specified	June 24, 2026
Bannari Amman Sugars Limited	Food and beverage, manufacturing / Food production company	India	Not specified	June 29, 2026 June 27, 2026

Gemeinschaftsstadt-werke Kamen	Utilities / Water supply, energy supply	Germany	Denial of services	June 29, 2026 June 28, 2026
Nickey Kehoe	Manufacturing / Furniture manufacturer	USA	Personal data leakage	May 26, 2026 March 29, 2026
Rockville Fuel & Feed Co.	Manufacturing / Concrete manufacturer	USA	Personal data leakage Ransomware	June 5, 2026 April 2, 2026 Akira
MasTec	Construction and engineering / Infrastructure engineering and construction company	USA	Personal data leakage Ransomware	June 5, 2026 August 9, 2025 Clop
Othon	Construction and engineering / Civil engineering firm	USA	Personal data leakage	June 5, 2026 March 12, 2026
Asplundh Engineering Services	Construction and engineering / Engineering firm for renewable energy, commercial and industrial, and utility projects	USA	Personal data leakage	June 4, 2026 January 11, 2026
Pride Solvent & Chemical Co., Pride Solvent & Chemical Co. of NY, and Pride Solvent and Chemical Co.	Chemicals, manufacturing / Chemical and solvent manufacturer	USA	Personal data leakage Ransomware	June 4, 2026 March 13, 2026 Dragonforce
Project Consulting Services	Energy, engineering / Engineering, design, and project management for the energy infrastructure industry	USA	Personal data leakage Ransomware	June 9, 2026 Play
Distribution Services International	Logistics and transportation /	USA	Personal data leakage	June 9, 2026

	Global logistics management and supply chain services			
Beusa Energy	Energy / Energy exploration company	USA	Personal data leakage	June 10, 2026
Ludlum Measurements	Manufacturing / Manufacturer of radiation detection instruments and technologies	USA	Personal data leakage Ransomware	June 22, 2026 Embargo
Fresenius Kabi USA	Pharmaceutical, manufacturing / Pharmaceutical manufacturing company	USA	Personal data leakage	June 17, 2026 January 6, 2026
American Future Technology Corporation / iBUYPOWER	Electronics, manufacturing / Hardware manufacturer	USA	Personal data leakage Ransomware	June 12, 2026 June 18, 2025 Lynx
SunSource Borrower	Manufacturing / Manufacturer of Industrial equipment and supplies	USA	Personal data leakage	June 17, 2026 March 31, 2026
Stanley Pearlman Enterprises	Food and beverage, manufacturing / Seafood processor	USA	Personal data leakage	June 17, 2026
Nissan North America	Automotive, manufacturing / Motor vehicle manufacturer	USA	Personal data leakage Ransomware	June 26, 2026 May 27, 2026 ShinyHunters
Yorozu Automotive Tennessee	Automotive, manufacturing / Automobile parts manufacturer	USA	Personal data leakage Ransomware	June 2, 2026 October 9, 2024 RansomHub
Murata Power Solutions	Electronics, manufacturing / Electronics components manufacturer	USA	Personal data leakage	June 8, 2026 March 2025

Galvion, Inc.	Defense, manufacturing / Tactical and protective equipment manufacturing company	USA	Personal data leakage	June 11, 2026
Triumph Group	Aerospace, manufacturing / Manufacturer of aviation and industrial components, accessories, subassemblies, systems, and aircraft structures	USA	Personal data leakage Extortion	June 11, 2026 Coinbase Cartel
Ludlum Measurements	Manufacturing / Radiation detection instrumentation manufacturing company	USA	Personal data leakage Ransomware	June 19, 2026 Embargo
Swift Transportation Co. of Arizona	Logistics and transportation / Transportation company	USA	Personal data leakage	June 1, 2026 March 9, 2026
Landstar System Holdings	Logistics and transportation / Transportation company	USA	Personal data leakage	June 11, 2026
Boyd Bros. Transportation / WTI Transport	Logistics and transportation / Transportation company	USA	Personal data leakage	June 22, 2026
Wright-Ryan Construction	Construction and engineering / Construction company	USA	Personal data leakage Ransomware	June 18, 2026 Inc ransom
Superior Drywall	Construction and engineering / Construction company	USA	Personal data leakage Ransomware	June 12, 2026 Safepay

Circle Floors	Construction and engineering / Flooring contractor	USA	Personal data leakage Ransomware	June 18, 2026 Play
Powell Electronics	Electronics, manufacturing / Electronic components manufacturer	USA	Personal data leakage Ransomware	June 3, 2026 Payouts King
High Mowing Organic Seeds	Food and beverage, manufacturing / Producer of food crop varieties	USA	Personal data leakage	June 16, 2026
Challenge Manufacturing Company	Automotive, manufacturing / Manufacturer of metal stamping and complex robotic welding assemblies	USA	Personal data leakage Ransomware	June 26, 2026 Chaos
Yellow Corporation	Logistics and transportation / Transportation company	USA	Personal data leakage	June 26, 2026
Gilman Brothers Company	Manufacturing / Foamboard products manufacturer	USA	Personal data leakage	June 26, 2026
Louisiana Machinery Company	Manufacturing / Construction equipment manufacturer	USA	Personal data leakage	June 18, 2026
Domus Design Centers	Manufacturing / Manufacturer of furniture items	USA	Personal data leakage Ransomware	June 25, 2026 Akira
Northern Technologies International Corporation	Manufacturing / Manufacturer of corrosion management solutions	USA	Personal data leakage Ransomware	June 26, 2026 February 13, 2026 Chaos

Kubota North America Corporation	Manufacturing / Agricultural machinery manufacturer	USA	Personal data leakage	June 30, 2026 March 16, 2026
Jenike & Johanson	Construction and engineering / Powder and bulk solids handling, processing, and storage technology	USA	Personal data leakage	June 30, 2026

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global Kaspersky project aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky ICS CERT ics-cert@kaspersky.com