Kaspersky ICS CERT

kaspersky

A brief overview of the main incidents in industrial cybersecurity Q4 2025

19.03.2026

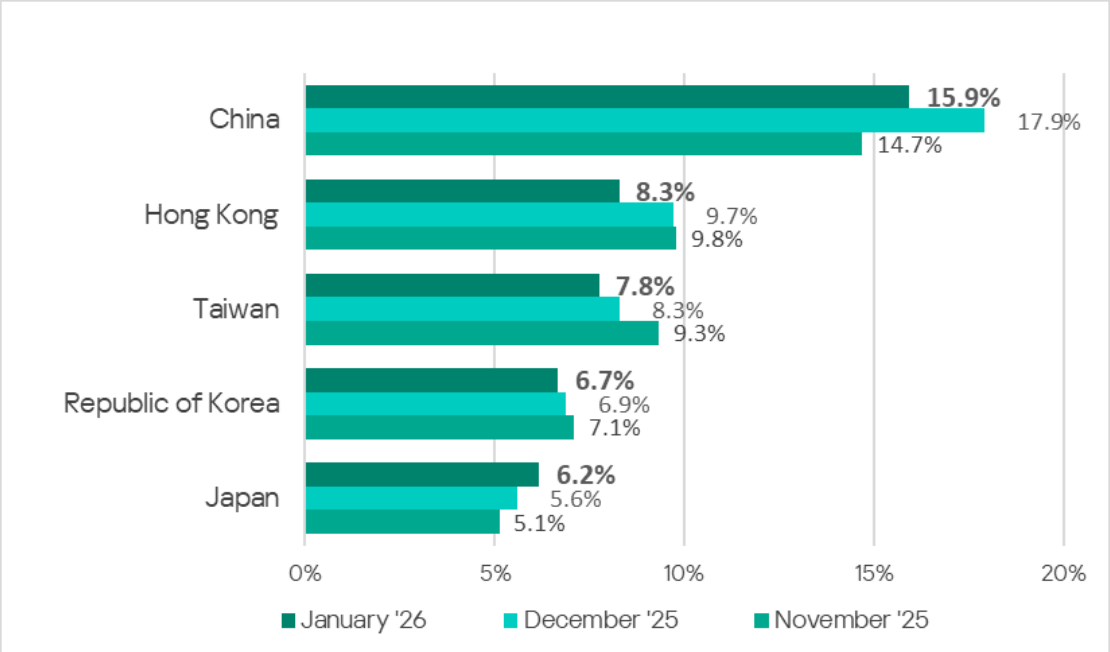
Version 1.0

Contents

In Q4 2025, 161 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

When evaluating the results of the quarter in terms of publicly confirmed cyberincidents at industrial enterprises, several observations can be made. First, attention is drawn to the disproportionately large number of incidents that have occurred in organizations from certain countries and territories, such as Japan and Taiwan. The number of incidents is particularly high when looking at estimates of the accessibility of computers related to industrial automation systems in these countries to cyberthreats.

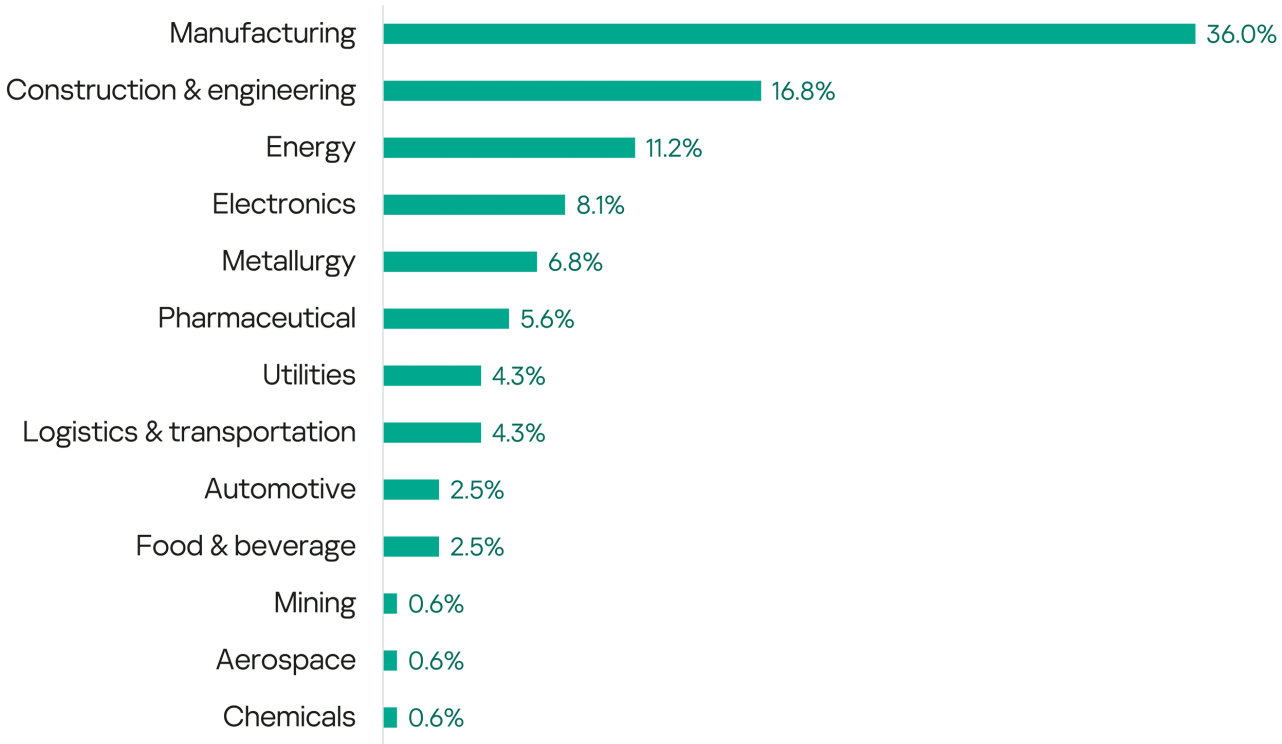


According to this indicator, we can see that both Japan and Taiwan could be ranked among the territories that are safe in terms of cybersecurity. However, cyberincident statistics suggest otherwise. Clearly, protection measures against the most common threats, whose quality can be indirectly assessed from the above diagram, may not be sufficient to protect against targeted attacks – the main cause of most cyberincidents. The situation regarding Taiwan probably reflects aspects of the geopolitical landscape – the territory is located in a geopolitical fault zone – and a large number of targeted attacks and incidents seems inevitable. In our opinion, one reason for the high number of cyberincidents in Japan is that Japanese enterprises rely too heavily on the 'conscientiousness' of their employees. They assume that employees will not engage in any behavior that could compromise cybersecurity, such as using

work computers for personal purposes, connecting flash drives unnecessarily, visiting suspicious websites or opening phishing emails. As a result, they only implement automated cybersecurity tools to a limited extent in enterprises.

Attacks on logistics infrastructure and transport companies remain a significant risk, with a consistently high number of cyberincidents in this sector. It is obvious that incidents in the field of transport and logistics affect many other sectors. Therefore, protecting transport and logistics companies from cyberattacks should be a priority.

The incident in the Danish city of Køge is a rare example of attacks with obvious cyber-physical consequences. After tampering with the control systems of a municipal water supplier, the attackers caused a local rupture of the pipeline. This incident reminds us of how fragile the information security of public utilities can be. In many countries, housing and communal services infrastructure is composed of many small, disparate enterprises that are simply unable to reliably protect their equipment from attacks. Fortunately, attacks on these enterprises are sporadic and unsystematic, and do not lead to large-scale consequences.



October — November — December — 2025

- AP Air
- SI-BONE
- Burt Process Equipment
- Rogers Mechanical Contractors
- Lowe Engineers
- Asahi
- Affärsverken
- Renault UK
- Brightstar Global Solutions Corporation
- Mino Kogyo Co., Ltd.
- BK Technologies Corporation
- Natare Corporation
- Avnet
- Compound Solutions
- Architectural Graphics
- Pure Haven
- Omrin
- SA Bendheim
- Ansell Limited
- MANGO
- Dairy Farmers of America
- Dulcich Inc./Pacific Seafood
- Tong Yang Industry Co.
- Jewett-Cameron Trading Co. Ltd.
- The Branch Group
- Ajinomoto Health & Nutrition
- Wytech Industries
- Weber GmbH
- Aussie Fluid Power
- Driver Driven Transportation / B.J. Transport
- Envoy Air
- AVer Information Inc.
- Askul Corp.
- Nickelhütte Aue GmbH
- Brox Industries
- Linemaster Switch Corporation
- Timberline Construction
- DALB
- Haven Manufacturing
- A.Y. McDonald Industries
- Aries Freight Systems
- Form Energy
- Fujifilm Biotechnologies
- Kurogane Kasei
- Goltens Worldwide Management Corp.
- Topco Scientific Co.
- The DiMarco Group
- Svenska Kraftnät
- VDyne
- Madeira USA
- RKA Consulting Group
- Central Boiler Companies
- Club Car
- Horner & Shifrin
- Superior Boiler
- Antaya Technologies Corp.
- Four G Construction
- Paris Ceramics USA / GKNYTWO
- TEIN, Inc
- Antigo Construction
- Fujian Fuzhen Metal Packaging Co.
- Hyundai AutoEver America
- Southern Graphics Inc.
- Mainetti USA
- Alpha Omega Winery
- Dealmed Medical Supplies
- GlobalLogic
- Integrated Silicon Solution
- Chase Affiliated Companies
- Mack Energy Corporation
- KLA Corporation
- GTC Control Solutions
- KLA Corporation dba KLA Instruments – Filmetrics
- Hampton Roads Sanitation District
- AllEarth Renewables
- Ruag LLC
- S&H Transport
- GL Veneer
- Hamilton Construction Company
- Roebbelen Contracting
- LaBella Associates
- Landfill Drilling & Piping
- Crocker Architectural & Sheet Metal Co.
- Optimum Design Associates
- Port Alliance group
- TerranearPMC
- Kier & Wright Civil Engineers and Surveyors Inc.
- Idemitsu Lubricants America Corporation
- Logitech International S.A
- woom GmbH
- Greer Commission of Public Works
- True World Foods
- Mencom Corporation
- Stadtwerke Detmold
- Francotyp-Postalia, Inc.
- LG Energy Solution
- WEL Companies
- Tung Ho Textile Co.
- FS Italiane Group / Almaviva
- Mechanical Systems & Services
- EnCon United Company
- Cool Wind Ventilation Corp.
- Buffalo Games
- Enverus Holdings
- Kern Oil & Refining Co. dba Kern Energy
- Iberia
- Win Win Precision Technology Co.
- Conway-Phillips Holding
- JASCO Applied Sciences
- Trailer Transit
- Bartek Ingredients
- Yac Garter Co.
- Takeuchi Manufacturing Incorporated
- Bär Cargolift (Gerd Bär GmbH)
- Aras Kargo
- Inotiv
- Barr & Barr
- Garden of Life
- ECM Consultants, Inc
- NCH Corporation
- MAG Aerospace
- Tris Pharma
- Thyssen Mining
- Golden Artist Colors, Inc
- Bleyl Interest Inc
- PES Energize
- Yem Chio Co., Ltd.
- Volume Transportation Inc.
- Hanson Professional Services
- Wood, Patel & Associates
- Ryan Biggs Clark Davis Engineering, (RBCD)
- Flexium Interconnect Inc.
- 21 Air
- Rain Bird Corporation
- Lydig Construction
- PDVSA (Petróleos de Venezuela, S.A)
- LKQ Corporation
- The Scharine Group
- CES Group Engineers, LLP
- Dainichi Color Vietnam Co.
- Pawling Corporation
- Tureby Alkestrup Waterworks
- American Holt, LLC
- HydroServe LLC dba Gustavo Preston Company
- McIntosh Laboratory
- Supreme Electronics Co.
- National Romanian Waters Administration (Administrația Națională Apele Române)
- Chiesi USA
- Cytek Biosciences Inc.
- Southeast Mechanical Contractors
- Pharmaceutics International
- La Poste
- Nanyang Industries Co., Ltd. (Nan Yang Industries Co., Ltd.) / Sanyang Motor Co., Ltd
- Fieldtex Products
- Evergreen Printing
- BTU International
- Oltenia Energy Complex (Complexul Energetic Oltenia)
- Korean Air
- Mercury Wire Products
- Pacific Railway Enterprises
- Cabinets 2000

Attacks leading to denial of operations

Asahi

Manufacturing, food and beverage

Denial of IT systems, operations and services, personal data leakage

Ransomware

The Japanese brewery Asahi Group Holdings disclosed that it experienced a system failure due to a cyberattack that affected operations in Japan. The company reported that it had suspended order and shipment operations at group companies in Japan, as well as call center operations, including customer service desks. The system failure was limited to operations within Japan. On October 3, Asahi Group Holdings confirmed that the disruption was caused by a ransomware attack on its systems and a subsequent investigation found evidence of data exfiltration. The company stated that it was unable to receive email communications from external sources. On October 8, the company announced that the incident had impacted technology assets in Japan. Asahi Breweries resumed production at all six of its domestic factories on October 2, and partial shipments of beer were resumed. On October 14, the company acknowledged the possibility that personal information may have been transferred without authorization. On October 7, the Qilin ransomware group claimed responsibility for the attack on Asahi Group Holdings by adding the company to the list of victims on its data leak site.

Jewett-Cameron Trading

Manufacturing

Denial of IT systems and operations, data leakage

Ransomware

Jewett-Cameron Trading Co., a US specialty wood and metal products manufacturer learned that a threat actor had gained unauthorized access to portions of the company's IT environment and claimed to have unlawfully accessed certain company information and data on October 15, according to a Form 8-K report filed with the Securities and Exchange Commission (SEC). Following an investigation, Jewett-Cameron Trading Co. concluded that the cybersecurity incident involved a third party gaining unauthorized access and deploying encryption and monitoring software to a portion of the company's internal corporate IT systems. The incident caused disruptions and limited access to portions of the company's business applications that support aspects of the company's operations and corporate functions. The company voluntarily took these applications offline as a precautionary measure. Based on the reviewed information, Jewett-Cameron Trading Co. believed the unauthorized activity had been contained.

Jewett-Cameron Trading Co. believes that threat actors unlawfully accessed specific computer systems and exfiltrated images of video meetings and computer screens that may have contained sensitive company information. The threat actors threatened to release this information publicly if the

company did not provide them with a monetary payment. In response to the incident, the company took additional cybersecurity measures, including closing off the point of unauthorized access and bolstering its cybersecurity capabilities. The company believed that the costs associated with these activities will be largely covered by its cybersecurity insurance policy. However, the company's operations may be materially impacted by the extended period offline. This could also affect the company's financial results for the first quarter of fiscal 2026.

Analysis indicated that the exfiltrated data was primarily IT- and finance-related information that the company had been gathering and analyzing in preparation for filing its Annual Report on Form 10-K with the Securities and Exchange Commission for the fiscal year ended August 31, 2025.

Askul

Logistics, transportation

Denial of services and operations, personal data leakage, supply chain

Ransomware

Japanese retailer Muji took its stores offline because of a logistics outage caused by a ransomware attack on its delivery partner, Askul Corp. On October 19, Muji stated that the issue had affected all retail services, including browsing or making purchases on online stores, viewing order histories via the Muji app, and displaying some web content. Askul Corp issued a statement on October 19, acknowledging that it was targeted by ransomware, causing operational disruptions. The company suspended orders and shipping operations. Askul's customer service desk was also unreachable via phone or the website. On October 22, Askul Corp confirmed that the outages primarily occurred in its warehouse management system (WMS). On October 31, the company confirmed that some of the information it stored had been leaked. The compromised data included information related to inquiries from customers of the B2B e-commerce websites Askul and Soloel Arena (company name, contact name, email address, registered phone number, inquiry content, etc.), information regarding inquiries from customers of consumer e-commerce website Lohaco (customer name, email address, phone number, inquiry content, etc.), and information registered in the product-related system by product suppliers (supplier company name, department name, name, email address, etc.). The company reported this matter to the relevant authorities, including the Personal Information Protection Commission. On October 30, RansomHouse claimed responsibility for the cyberattack on Askul Corp.

TEIN

Automotive, manufacturing

Denial of IT systems, operations

Ransomware

On October 31, Japanese high-performance automotive suspension manufacturer TEIN suffered a ransomware attack that affected the company's operations. The attack hit 'the main server', affecting all group companies. The Japan HQ factory halted production for one day. The subsidiary factory in China (TEIN Shock Absorber Manufacturing (Jiangsu)) was forced to shut down for one week from November 3. The company planned to make up for lost time by operating on weekends and expected the overall impact to be minimal. Its order and shipping system was run on a separate server and was not affected by the incident. The company has not confirmed a data leak. On November 6, the Warlock ransomware group claimed responsibility for the attack on TEIN.

Petróleos de Venezuela

Energy

Denial of IT systems, operations and services

Ransomware

Venezuela's national oil company (Petróleos de Venezuela, S.A., PDVSA) said in a statement on December 15 that it had been the target of a cyberattack. The company claimed the incident did not affect its operations in any way, adding that the breach was limited to some administrative systems. In its statement, PDVSA blamed the United States and 'domestic conspirators' for orchestrating the attack in an 'attempt to undermine national stability'. According to an internal memo seen by Bloomberg, PDVSA instructed operational and administrative staff to disconnect from the network and shut down their computers. Three sources familiar with the situation also told Bloomberg that systems on PDVSA's network that manage the country's main crude terminal were offline on December 15. This was confirmed by Reuters in a report citing an inside source who said there was no delivery of cargoes and that all systems were down. The sources said that oil output, refining and domestic distribution were not affected. According to a PDVSA source cited by Reuters, the company detected a ransomware attack. PDVSA resumed loading crude and fuel cargoes on December 17.

Gerd Bär GmbH

Manufacturing

Denial of IT systems, IT services and operations, data leakage

Ransomware

On November 28, German lifting and handling equipment manufacturer Bär Cargolift (Gerd Bär GmbH) was hit by a cyberattack. According to a statement on the company's website, the perpetrators succeeded in undermining the technical and organizational measures designed to protect the IT environment, encrypting parts of it in the process. During the incident, the web shop was taken offline, but customers could still order spare parts by email and telephone. By the first week of December, email security and production were reportedly operational again. After the company restored the web shop

functionality, orders for cargo lifts and spare parts could be placed. In December, the PayoutsKing ransomware group claimed responsibility for the attack on Gerd Bär GmbH.

Attempts to disrupt operations

Port Alliance group

Transportation, logistics

DDoS

On November 13, Russia's Port Alliance group, which operates a network of sea cargo terminals, reported on its Telegram channel that "foreign hackers" had targeted its systems over a period of three days in a distributed denial of service (DDoS) attack and an attempted hack. In a statement, the group said critical elements of its digital infrastructure had been targeted with "the aim of disrupting export shipments of coal and mineral fertilizers from its terminals in the Baltic, Black Sea, Far East and Arctic regions". Despite the attack's high intensity, complexity, and constantly changing attack vectors, it was successfully suppressed. The functionality of all key systems was maintained, and the operational business processes of the ports and terminals were unaffected. The attack was identified as multi-vector, combining DNS amplification, SYN, IP fragmentation, and UDP flooding, with a peak intensity of up to 16 Gbps. It utilized a botnet of over 15,000 unique IP addresses from around the world, including Russia, and employed constantly changing attack vectors to bypass core security systems.

Attack with cyber-physical effect

Danish water utility

Utility, water supply

Denial of operations

Attacks targeting ICS

Cyber-physical consequences

On December 18, the Danish Defense Intelligence Service (DDIS) issued a statement alleging that the Russian-speaking group Z-Pentest carried out a destructive cyberattack on a Danish water utility in 2024. At a press conference, Denmark's defense minister condemned the cyberattacks and labeled them as "unacceptable", citing an incident in December 2024 in Køge. Previous reports indicate that the attack on the water utility targeted a small treatment plant near the town of Køge, where hackers manipulated the pressure in the system, causing three pipes to burst.

Incidents at large organizations

Envoy Air

Transportation, logistics

Data leakage

Zero-day vulnerability

Extortion

US airline Envoy Air, owned by American Airlines, confirmed that data was compromised from its Oracle E-Business Suite application after the Clop extortion group listed American Airlines on its data leak site on October 16. In an email, a company spokesperson stated that the company was aware of the incident. Upon learning of the matter, Envoy Air immediately began an investigation and contacted law enforcement. The company conducted a thorough review of the affected data and confirmed no sensitive or customer data was compromised. According to the airline's statement, a limited amount of business information and commercial contact details may have been compromised. Oracle initially stated that the threat actors were exploiting vulnerabilities patched in July, but later disclosed that the extortion group exploited the zero-day vulnerability CVE-2025-61882 in the attacks. CrowdStrike and Mandiant revealed that Clop exploited these flaws in early August to breach systems and deploy malware.

RUAG

Manufacturing, aerospace, engineering

Denial of IT systems

Ransomware

RUAG LLC, the US subsidiary of RUAG MRO Holding, a Swiss arms manufacturer, fell victim to a ransomware attack. The incident was contained and did not affect other systems within the RUAG group. The compromised IT infrastructure could not be used to access systems or data in Switzerland or other companies belonging to RUAG MRO Holding. According to a company statement, no particularly sensitive data relating to employees in Switzerland was affected. On November 3, the Akira ransomware group claimed responsibility for the attack on RUAG LLC (Mecanex USA).

LG Energy Solution

Chemicals, manufacturing

Data leakage

Ransomware

A spokesperson for South Korea-based battery manufacturer LG Energy Solution confirmed to The Record on November 18 that the company had been affected by ransomware, following claims made by the Akira cybercriminal group. According to official comments, the attack targeted a specific overseas facility. The company confirmed that the headquarters and other facilities were not affected. After recovery measures were taken, the impacted facility resumed normal operations, and LG Energy Solution conducted security operations and investigations as a precautionary measure. The spokesperson did not respond to further questions about the nature of the incident. On November 17, the Akira ransomware group added the company to its leak site,

claiming to have stolen 1.7 terabytes of data, including corporate documents and employee information databases.

Iberia

Transportation, logistics

Personal data leakage, supply chain / trusted partner

Spanish airline Iberia notified customers of a data security incident stemming from a compromise at one of its suppliers. The disclosure came just days after a threat actor claimed to have access to 77 GB of data allegedly stolen from the airline. According to an email seen by threat intelligence platform Hackmanac, the compromised data could have included customers' names and surnames, email addresses, and loyalty card (Iberia Club) identification numbers. The airline said customers' Iberia account login credentials and passwords were not compromised and that no banking or payment card information was accessed. Iberia attributed the breach to a third-party vendor rather than to its own servers. In the forum post, the threat actor claimed the data was extracted directly from the airline's internal servers and contained A320/A321 technical data, AMP maintenance files, engine information, and other internal documents. The actor labeled the data ISO 27001 and ITAR-classified and marketed it for industrial espionage, resale to competitors, or potential use by foreign governments.

On January 6, researchers at Hudson Rock published a report about a threat actor named Zestix that had been auctioning data allegedly stolen from corporate file-sharing portals belonging to approximately 50 large companies, including Iberia. The hacker allegedly stole 77 GB of data that included technical materials for A320 and A321 aircraft, maintenance files, engine data, aircraft damage charts, and confidential fleet data. An Iberia spokesperson confirmed to Recorded Future News that Hudson Rock's research related to the November incident.

FS Italiane Group / Almaviva

Transportation, logistics

Data leakage, supply chain / trusted partner

Data belonging to Italy's national railway operator, FS Italiane Group, was exposed when a threat actor breached the organization's IT services provider, Almaviva. The hacker claimed to have stolen 2.3 terabytes of data and leaked it on a dark web forum. According to the threat actor, the leak included confidential documents and sensitive company information. Almaviva is a large Italian company that operates globally, providing services such as software design and development, system integration, IT consulting, and customer relationship management (CRM) products. In a public statement about the incident, Almaviva said it had identified and isolated the cyberattack, which resulted in the theft of some data. The functions and services of the affected systems remained active. The relevant authorities – the Public Prosecutor's

Office, the Postal Police, the National Agency for Cybersecurity, and the Data Protection Authority – were informed.

Logitech International

Electronics, manufacturing

Personal data leakage

Ransomware

Swiss multinational electronics and technology company Logitech International S.A. filed a Form 8-K with the US Securities and Exchange Commission and published a statement on its website confirming a data breach. According to BleepingComputer, the company suffered as a result of the aforementioned attack by the Clop ransomware group on Oracle E-Business Suite in July. The cybersecurity incident did not impact Logitech's products, business operations or manufacturing. The stolen data likely included limited employee and consumer information, as well as customer and supplier data. However, the company did not believe that the hackers gained access to sensitive information such as national ID numbers or credit card information because that data was not stored in the breached systems. At the time of the filing, Logitech International S.A. did not believe the incident would materially affect its financial condition or results of operations. The company maintains a comprehensive cybersecurity insurance policy that was expected to cover incident response and forensic investigation costs, as well as any business interruptions, legal actions or regulatory fines. Logitech International S.A. stated that the breach occurred through a third-party zero-day vulnerability that was patched as soon as a fix became available. On November 6, Logitech International S.A. was listed on the Clop data leak extortion site.

Appendix. Full list of confirmed incidents

Victim	Industry / Profile	Country	Impact features	Date of notification Date of incident (if known) Suspected attackers
Asahi	Food and beverage, manufacturing / Brewing company	Japan	Denial of IT systems, operations and services, personal data leakage	October 3, 2025 September 29, 2025 Qilin

			Ransomware	
BK Technologies Corporation	Manufacturing / Telecommunications manufacturing company	USA	Denial of IT systems, personal data leakage	October 6, 2025 September 20, 2025
Svenska Kraftnät	Utilities / Electricity transmission system operator	Sweden	Data leakage Ransomware	October 26, 2025 Everest
Envoy Air	Logistics and transportation / Airline	USA	Data leakage Ransomware	October 18, 2025 Clop
Affärsverken	Energy / Heat and power plant	Sweden	Unknown	October 3, 2025
Omrin	Utilities, transportation / Waste collection, treatment and recycling company	The Netherlands	Denial of services, personal data leakage Ransomware	October 13, 2025 Qilin
Tong Yang Industry Co.	Automotive, manufacturing / Manufacturer of auto repair parts	Taiwan	Ransomware	October 15, 2025 Qilin
Topco Scientific Co.	Electronics, manufacturing / Semiconductor and optoelectronic components manufacturer	Taiwan	Denial of IT systems, data leakage	October 25, 2025 October 23, 2025
AVer Information	Electronics, manufacturing / Manufacturer of technology solutions for education and professional business applications	Taiwan	Denial of IT systems	October 19, 2025 October 18, 2025

Jewett-Cameron Trading Co.	Manufacturing / Specialty wood and metal products manufacturer	USA	Denial of IT systems and operations, data leakage	October 15, 2025
Mino Kogyo Co.	Manufacturing / Manufacturer of die-cast aluminum products	Japan	Denial of IT systems, personal data leakage Ransomware	October 4, 2025 October 1, 2025 SafePay
Weber GmbH	Manufacturing / Automation machinery manufacturing company	Germany	Denial of IT systems Ransomware	October 16, 2025 RansomHouse
Aussie Fluid Power	Manufacturing / Hydraulic equipment manufacturer	Australia	Personal data leakage Ransomware	October 17, 2025 Anubis
Nickelhütte Aue GmbH	Metallurgy, manufacturing / Manufacturer of non-ferrous metal concentrates	Germany	Denial of IT systems Ransomware	October 20, 2025
Kurogane Kasei	Chemicals, manufacturing / Chemical manufacturer	Japan	Denial of IT systems, data leakage Ransomware	October 24, 2025 October 16, 2025 RansomHouse
Ansell Limited	Manufacturing / Manufacturer of personal protective equipment	Australia	Personal data leakage Ransomware	October 14, 2025 Clop
Avnet	Logistics and transportation, electronics, engineering / Electronic	USA	Data leakage Extortion	October 7, 2025

	components distributor			
MANGO	Logistics and transportation, manufacturing / Fashion retailer	Spain	Personal data leakage	October 14, 2025
Askul Corp.	Logistics and transportation, manufacturing / E-commerce and logistics services	Japan	Denial of services and operations, supply chain, personal data leakage Ransomware	October 19, 2025 RansomHouse
Renault UK	Automotive, manufacturing / Car manufacturer	France	Personal data leakage	October 3, 2025
Burt Process Equipment	Manufacturing / Manufacturer of equipment for fluid handling and treatment applications, including pH systems, pumps, power tools, chem feed machines, heaters and heat exchangers	USA	Personal data leakage Ransomware	October 2, 2025 Akira
DALB	Manufacturing / Printed signage and thermoformed plastic components manufacturer	USA	Personal data leakage Ransomware	October 21, 2025 May 20, 2025 Akira
Pure Haven	Manufacturing / Organic personal care products manufacturer	USA	Personal data leakage	October 10, 2025 September 2, 2025
The Branch Group	Construction and engineering /	USA	Personal data leakage	October 15, 2025 January 14, 2025

	Construction engineering company		Ransomware	Cactus
Dairy Farmers of America	Food and beverage, manufacturing / Dairy products and ingredients manufacturing	USA	Personal data leakage Ransomware	October 14, 2025 June 11, 2025 Play
Dulcich / Pacific Seafood	Food and beverage, manufacturing / Producer of meat and fish products	USA	Personal data leakage	October 14, 2025 June 24, 2025
Brox Industries	Construction and engineering, manufacturing / Manufacturer of asphalt products	USA	Personal data leakage	October 20, 2025 February 28, 2025
Madeira USA	Manufacturing / Apparel and fashion embroidery manufacturer	USA	Personal data leakage	October 27, 2025 October 8, 2025
Goltens Worldwide Management Corp.	Logistics and transportation, energy / Technical services provider for the maritime, offshore, energy sectors	USA	Personal data leakage	October 24, 2025 May 26, 2025
Form Energy	Energy, manufacturing / Manufacturer of multi-day energy storage systems and iron-air battery systems	USA	Personal data leakage Ransomware	October 22, 2025 September 16, 2025
RKA Consulting Group	Construction and engineering, manufacturing / Municipal engineering,	USA	Personal data leakage	October 27, 2025 January 8, 2025

	engineering design, and traffic engineering			
Central Boiler Companies	Manufacturing / Manufacturer of outdoor furnaces	USA	Denial of IT systems, personal data leakage	October 27, 2025 August 1, 2025
AP Air	Manufacturing / Motor vehicle parts manufacturer	USA	Personal data leakage Ransomware	October 1, 2025 July 13, 2025 Akira
SI-BONE	Manufacturing / Medical device manufacturer	USA	Personal data leakage	October 1, 2025
Rogers Mechanical Contractors	Construction and engineering / Industrial HVAC, plumbing, and control systems company	USA	Denial of IT systems, personal data leakage	October 2, 2025 January 31, 2025
Compound Solutions	Chemicals, manufacturing / Manufacturer of industrial inorganic chemicals	USA	Personal data leakage Ransomware	October 8, 2025 February 28, 2025 Play
Architectural Graphics	Manufacturing / Architectural branding and signage manufacturer	USA	Denial of IT systems, personal data leakage	October 9, 2025 February 22, 2025
Lowe Engineers	Construction and engineering / Civil engineering, highway and roadway design, utility systems analysis, hydrology/hydraulics, water and wastewater systems design, aerial	USA	Personal data leakage Ransomware	October 2, 2025 January 12, 2025 Lynx

	mapping, photogrammetry			
Natare Corporation	Manufacturing, construction and engineering / Manufacturer of stainless-steel pools, spas, pool equipment for competition, fitness, leisure, aquatic recreation	USA	Denial of IT systems, personal data leakage Ransomware	October 6, 2025 August 13, 2025 Akira
Ajinomoto Health & Nutrition	Food and beverage, manufacturing / Ingredient manufacturer	USA	Personal data leakage Ransomware	October 15, 2025 Qilin
Wytech Industries	Manufacturing / Medical equipment manufacturer	USA	Personal data leakage Ransomware	October 15, 2025 Akira
Linemaster Switch Corporation	Manufacturing / Manufacturer of foot switches and hand controls	USA	Personal data leakage	October 20, 2025
Haven Manufacturing	Manufacturing / Automation machine manufacturing company	USA	Personal data leakage	October 21, 2025
Driver Driven Transportation / B.J. Transport	Logistics and transportation, energy / Transportation and shipping logistics company	USA	Personal data leakage	October 17, 2025 August 12, 2025
A.Y. McDonald Industries	Manufacturing / Manufacturer of water works valves and fittings, natural gas valves, and residential and	USA	Denial of IT systems Personal data leakage Ransomware	October 21, 2025 January 12, 2025 RansomHub

	commercial water pumping systems			
Fujifilm Biotechnologies	Manufacturing / Biologics process development and biologics cGMP manufacturing	USA	Personal data leakage	October 23, 2025
The DiMarco Group	Construction and engineering / Commercial construction	USA	Personal data leakage Ransomware	October 25, 2025 Lynx
Club Car	Manufacturing / Motor vehicle manufacturing company	USA	Personal data leakage Ransomware	October 27, 2025 Qilin
Horner & Shifrin	Construction and engineering / Surveying, site development, and construction services	USA	Personal data leakage	October 28, 2025 July 17, 2025
Superior Boiler	Manufacturing / Industrial boiler manufacturer	USA	Personal data leakage	October 29, 2025
Antaya Technologies Corp.	Automotive, manufacturing / Manufacturer of on-glass connectors for the automotive industry	USA	Personal data leakage	October 29, 2025 August 7, 2025
Paris Ceramics USA / GKNYTWO	Manufacturing / Manufacturer of flooring products	USA	Personal data leakage	October 31, 2025
Timberline Construction	Construction and engineering / Construction company	USA	Personal data leakage	October 20, 2025 August 21, 2025

Brightstar Global Solutions Corporation	Manufacturing / Manufacturer of gaming equipment	USA	Personal data leakage	October 3, 2025 November 17, 2024
SA Bendheim	Manufacturing / Manufacturer of building products	USA	Personal data leakage	October 13, 2025
VDyne	Manufacturing / Manufacturer of medical devices	USA	Personal data leakage Ransomware	October 26, 2025 Qilin
Four G Construction	Construction and engineering / Construction services, pipeline construction	USA	Personal data leakage	October 29, 2025
Aries Freight Systems	Logistics and transportation, energy / Logistics provider	USA	Personal data leakage	October 21, 2025
RUAG LLC	Aerospace, defense, manufacturing, engineering / Arms manufacturer	USA	Denial of IT systems Ransomware	November 11, 2025 Akira
Fujian Fuzhen Metal Packaging Co.	Manufacturing / Metal packaging manufacturer	Taiwan	Denial of IT systems Ransomware	November 3, 2025 Radar/Dispossessor
TEIN	Automotive, manufacturing / High-performance automotive suspension manufacturer	Japan	Denial of IT systems and operations Ransomware	October 31, 2025 Warlock
Win Win Precision Technology Co.	Electronics, manufacturing / Manufacturer of solar photovoltaic modules and	Taiwan	Denial of IT systems	November 24, 2025

	semiconductor products			
Tung Ho Textile Co.	Manufacturing / Textile manufacturing	Taiwan	Denial of IT systems	November 19, 2025
Logitech International S.A.	Electronics, manufacturing / Electronics and technology company	Switzerland	Personal data leakage	November 14, 2025
woom GmbH	Manufacturing / Bicycle manufacturer	Austria	Denial of IT systems, personal data leakage	November 14, 2025 November 7, 2025 INC Ransom
Stadtwerke Detmold	Utilities / Energy distribution and water supply	Germany	Denial of IT systems and IT services	November 16, 2025
Yac Garter Co.	Electronics, manufacturing / Manufacturer of electronic chips, electric tapes and circuit boards	Japan	Denial of IT systems Ransomware	November 26, 2025 November 25, 2025
FS Italiane Group / Almaviva	Logistics and transportation, energy / National railway operator	Italy	Data leakage, supply chain	November 19, 2025 November 2025
LG Energy Solution	Chemicals, manufacturing / Battery manufacturer	South Korea	Data leakage Ransomware	November 18, 2025 Akira
Iberia	Logistics and transportation / Airline	Spain	Personal data leakage, supply chain / trusted partner	November 23, 2025
Port Alliance group	Logistics and transportation / Network of sea cargo terminals operator	Russia	DDoS	November 13, 2025

GlobalLogic	Construction and engineering / Digital engineering provider	USA	Personal data leakage	November 7, 2025 July 10, 2025 Clop
Alpha Omega Winery	Food and beverage, manufacturing / Producer of wines	USA	Personal data leakage Ransomware	November 6, 2025 December 27, 2023
Dealmed Medical Supplies	Manufacturing / Medical equipment manufacturing company	USA	Personal data leakage Ransomware	November 6, 2025 June 7, 2025 DragonForce
Integrated Silicon Solution	Electronics, manufacturing / Integrated circuits manufacturer	USA	Personal data leakage Ransomware	November 7, 2025 June 6, 2025 WorldLeaks
Greer Commission of Public Works	Utilities / Water, natural gas, electric and wastewater service	USA	Personal data leakage	November 14, 2025 June 19, 2025
S&H Transport	Logistics and transportation / Transportation provider	USA	Personal data leakage	November 12, 2025 June 8, 2025
Hampton Roads Sanitation District	Utilities / Wastewater treatment facility	USA	Personal data leakage Ransomware	November 10, 2025 October 6, 2025 Clop
GL Veneer	Manufacturing / Wood manufacturer	USA	Denial of IT systems, personal data leakage Ransomware	November 12, 2025 August 26, 2025 Play
Enverus Holdings	Energy / Energy industry software services provider	USA	Personal data leakage	November 21, 2025 August 12, 2025

Cool Wind Ventilation Corp.	Manufacturing / Metal ductwork manufacturer	USA	Personal data leakage Ransomware	November 20, 2025 August 26, 2025 Play
WEL Companies	Logistics and transportation / Transportation provider	USA	Personal data leakage Ransomware	November 18, 2025 January 30, 2025 RansomHub
JASCO Applied Sciences	Manufacturing / Manufacturer of specialized oceanographic and underwater acoustic equipment	USA	Personal data leakage Ransomware	November 25, 2025 July 21, 2025 Rhysida
Mainetti USA	Manufacturing / Manufacturer of industrial packaging solutions and clothes hooks	USA	Personal data leakage Ransomware	November 5, 2025 June 12, 2025
Hyundai AutoEver America	Automotive, manufacturing / Automotive information technology organization	USA	Denial of IT systems, personal data leakage	November 3, 2025 February 22, 2025
Chase Affiliated Companies	Energy / Services for oil and gas operations, including well completion, cementing solutions, drilling operations, oilfield construction, frac pond construction	USA	Personal data leakage	November 7, 2025
Mack Energy Corporation	Energy / Oil and gas exploration company	USA	Personal data leakage	November 7, 2025
KLA Corporation	Electronics, manufacturing /	USA	Personal data leakage	November 7, 2025 August 5, 2025

	Electronic components manufacturer		Ransomware	Meow
Antigo Construction	Construction and engineering / Concrete breaking services	USA	Personal data leakage Ransomware	October 31, 2025 June 1, 2025 Dragonforce
Hamilton Construction Company	Construction and engineering / Heavy civil contractor	USA	Personal data leakage	November 12, 2025 June 19, 2025
Roebbelen Contracting	Construction and engineering / Construction services for institutional, commercial, industrial, and public agency clients	USA	Personal data leakage	November 12, 2025 August 22, 2025
LaBella Associates	Construction and engineering / Engineering, and construction planning services	USA	Personal data leakage Ransomware	November 12, 2025 March 24, 2025 Rhysida
True World Foods	Food and beverage, manufacturing / Seafood products company	USA	Personal data leakage Ransomware	November 14, 2025 August 14, 2025 Lynx
GTC Control Solutions	Construction and engineering / Provider of turbine and industrial controls support services	USA	Personal data leakage	November 7, 2025 August 14, 2025
Mechanical Systems & Services	Construction and engineering / HVAC service, mechanical design and construction, security systems,	USA	Personal data leakage	November 19, 2025

	building automation and controls, energy management			
Kern Oil & Refining Co. dba Kern Energy	Energy / Oil and refining company	USA	Personal data leakage	November 21, 2025 August 2025
EnCon United Company	Manufacturing, construction and engineering / Concrete manufacturing and construction company	USA	Personal data leakage	November 19, 2025
Trailer Transit	Logistics and transportation / Trucking transportation company	USA	Personal data leakage Ransomware	November 25, 2025 September 9, 2025 Metaencryptor Team
Conway-Phillips Holding	Energy, construction and engineering / Storage tank construction services to petroleum, power, chemical, and renewable fuel industries	USA	Personal data leakage	November 24, 2025 September 26, 2025
TerranearPMC	Utilities, construction and engineering / Radiological waste management and construction management services	USA	Personal data leakage Ransomware	November 13, 2025 September 6, 2025 Play
Landfill Drilling & Piping	Energy, construction and engineering / Installation of landfill gas collection systems and	USA	Personal data leakage	November 12, 2025 September 8, 2025

	leachate collection systems			
Crocker Architectural & Sheet Metal Co.	Manufacturing, construction and engineering / Metal fabrication and construction services	USA	Personal data leakage	November 12, 2025
Kier & Wright Civil Engineers and Surveyors	Construction and engineering / Civil engineering	USA	Personal data leakage Ransomware	November 13, 2025 Qilin
Idemitsu Lubricants America Corporation	Manufacturing / Industrial lubricants manufacturer	USA	Personal data leakage	November 13, 2025
Optimum Design Associates	Electronics, manufacturing / Ed circuit board design and layout, engineering, turnkey manufacturing services	USA	Personal data leakage	November 12, 2025
Mencom Corporation	Manufacturing / Manufacturer of industrial power, control, signal, and networking connector solutions	USA	Personal data leakage	November 14, 2025 November 7, 2024
Francotyp-Postalia	Manufacturing / Manufacturer of mailing products	USA	Personal data leakage	November 17, 2025 October 3, 2025
Buffalo Games	Manufacturing / Manufacturer of consumer products	USA	Personal data leakage Ransomware	November 20, 2025 Akira

Takeuchi Manufacturing Incorporated	Manufacturing / Manufacturer of construction equipment (compact excavators, track loaders)	USA	Personal data leakage Ransomware	November 26, 2025 Play
AllEarth Renewables	Energy, manufacturing / Manufacturer of renewable energy sources, including solar panels and equipment	USA	Personal data leakage	November 10, 2025 October 7, 2025
KLA Corporation dba KLA Instruments – Filmetrics	Electronics, manufacturing / Manufacturer of high-precision equipment for the semiconductor and electronics industries	USA	Personal data leakage	November 7, 2025 August 5, 2025
Bartek Ingredients	Food and beverage, manufacturing / Industrial food/ingredient manufacturer	Canada	Personal data leakage Ransomware	November 25, 2025 August 31, 2025 INC Ransom
Southern Graphics	Manufacturing / Large-format graphics manufacturing and industrial printing	USA	Personal data leakage Ransomware	November 4, 2025 Daixin
Bär Cargolift (Gerd Bär GmbH)	Manufacturing / Lifting and handling equipment manufacturer	Germany	Denial of IT systems, IT services and operations, data leakage Ransomware	November 30, 2025 November 28, 2025 PayoutsKing
National Romanian Waters	Utilities / Water supply	Romania	Denial of IT systems and IT services	December 22, 2025 December 20, 2025

Administration (Administrația Națională Apele Române)			Ransomware	
Petróleos de Venezuela, S.A.	Energy / Oil company	Venezuela	Denial of IT systems, operations and services Ransomware	December 15, 2025
PES Energize	Utilities, energy / Electricity provider	USA	Denial of IT systems and services	December 6, 2025
Yem Chio Co.	Manufacturing / Manufacturer of packaging materials	Taiwan	Denial of IT systems Ransomware	December 8, 2025 December 6, 2025
Flexium Interconnect Inc.	Electronics, manufacturing / Manufacturer of flexible printed circuit boards	Taiwan	Unknown	December 11, 2025
Dainichi Color Vietnam Co.	Chemicals, manufacturing / Manufacturer of plastics, dyes and compounds for plastics	Vietnam	Denial of IT systems Ransomware	December 17, 2025 December 15, 2025
Tureby Alkestrup Waterworks	Utilities / Water supply	Denmark	Denial of operations	December 18, 2025 December 18, 2024 Z-Pentest
Korean Air	Logistics and transportation / Airline	South Korea	Personal data leakage Ransomware	December 29, 2025 Clop
Oltenia Energy Complex (Complexul	Energy / Energy producer	Romania	Denial of IT systems and services	December 27, 2025 December 26, 2025

Energetic Oltenia)			Ransomware	Gentlemen
Nanyang Industries Co. (Nan Yang Industries Co.) / Sanyang Motor Co.	Automotive, manufacturing / Manufacturer of Hyundai automobiles and mini-trucks	Taiwan	Denial of IT systems and services Ransomware	December 23, 2025 Dire Wolf
Supreme Electronics Co.	Electronics, manufacturing / Electronics manufacturing company	Taiwan	Denial of IT systems and services Ransomware	December 21, 2025 Qilin
NCH Corporation	Manufacturing / Manufacturer of industrial maintenance, water treatment and lubricants	USA	Personal data leakage Ransomware	December 5, 2025 August 9, 2025 Clop
MAG Aerospace	Manufacturing, construction and engineering, aerospace / Specialized aerospace parts and systems integration manufacturer	USA	Personal data leakage	December 5, 2025 August 30, 2025
Inotiv	Pharmaceutical, manufacturing / Manufacturer of research-related products like specialized lab diets and bedding	USA	Denial of IT systems and services, personal data leakage	December 2, 2025 August 5, 2025 Qilin
Ryan Biggs Clark Davis Engineering	Construction and engineering / Structural engineering	USA	Personal data leakage	December 10, 2025 September 24, 2025

21 Air	Logistics and transportation / Airline	USA	Personal data leakage	December 11, 2025 June 3, 2025
Barr & Barr	Construction and engineering / Construction management services	USA	Personal data leakage Ransomware	December 4, 2025 September 4, 2025 Akira
Garden of Life	Manufacturing / Manufacturer of dietary supplements and health products	USA	Personal data leakage Ransomware	December 4, 2025 August 9, 2025 Clop
LKQ Corporation	Automotive, logistics and transportation / Auto parts distributor	USA	Personal data leakage Ransomware	December 15, 2025 August 9, 2025 Clop
Rain Bird Corporation	Manufacturing / Irrigation and water management systems manufacturer	USA	Personal data leakage	December 11, 2025 February 11, 2025
HydroServe dba Gustavo Preston Company	Manufacturing / Manufacturer of fluid handling systems	USA	Personal data leakage	December 19, 2025 October 6, 2025
McIntosh Laboratory	Electronics, manufacturing / Audio sound system manufacturer	USA	Denial of IT systems, personal data leakage Ransomware	December 19, 2025 October 6, 2025 Safepay
BTU International	Electronics, manufacturing / Manufacturer of advanced thermal processing equipment	USA	Personal data leakage	December 26, 2025 August 11, 2025

Chiesi USA	Pharmaceutical, manufacturing / Pharmaceutical manufacturing company	USA	Personal data leakage	December 22, 2025 June 23, 2025
Cytek Biosciences	Manufacturing / Medical instrumentation manufacturer	USA	Personal data leakage Ransomware	December 22, 2025 November 1, 2025 Rhysida
Cabinets 2000	Manufacturing / Cabinet manufacturer	USA	Denial of IT systems, personal data leakage Ransomware	December 30, 2025 October 2, 2025 BlackShrantac
Volume Transportation	Logistics and transportation / Trucking transportation services	USA	Denial of IT systems, personal data leakage Ransomware	December 8, 2025 August 18, 2025 Qilin
The Scharine Group	Manufacturing / Agricultural equipment manufacturer	USA	Personal data leakage Ransomware	December 16, 2025 Play
American Holt	Manufacturing / Manufacturer of aftermarket replacement parts for machines	USA	Personal data leakage	December 18, 2025 October 22, 2025
Southeast Mechanical Contractors	Construction and engineering / HVAC, electrical, and plumbing services company	USA	Personal data leakage	December 22, 2025 October 17, 2025
Pharmaceutics International	Pharmaceutical, manufacturing / Pharmaceutical	USA	Personal data leakage Ransomware	December 22, 2025 October 17, 2025 RansomHub

	manufacturing company			
Fieldtex Products	Manufacturing / Manufacturer of soft-sided carrying cases	USA	Personal data leakage Ransomware	December 23, 2025 Akira
Mercury Wire Products	Manufacturing / Producer of wires and cables	USA	Personal data leakage Ransomware	December 29, 2025 Sinobi
Pacific Railway Enterprises	Construction and engineering / Rail system designs, railroad construction, communication and application programming services	USA	Personal data leakage Ransomware	December 29, 2025 Akira
Tris Pharma	Pharmaceutical, manufacturing / Pharmaceutical manufacturing company	USA	Personal data leakage	December 5, 2025 September 24, 2025
ECM Consultants	Construction and engineering / Engineering services	USA	Personal data leakage Ransomware	December 4, 2025 July 4, 2025 Sinobi
Wood, Patel & Associates	Construction and engineering / Engineering services	USA	Personal data leakage Ransomware	December 9, 2025 July 4, 2025 Play
CES Group Engineers	Construction and engineering / Engineering services	USA	Personal data leakage	December 16, 2025 August 20, 2025
Thyssen Mining	Mining / Mining and heavy industrial operations	USA	Personal data leakage	December 5, 2025 August 13, 2025

Hanson Professional Services	Construction and engineering / Engineering, infrastructure and industrial design services	USA	Personal data leakage Ransomware	December 8, 2025 Chaos
Golden Artist Colors	Manufacturing / Paint products manufacturer	USA	Personal data leakage Ransomware	December 5, 2025 November 7, 2025 Nitrogen
Pawling Corporation	Manufacturing / Industrial hardware and building products manufacturing	USA	Denial of IT systems, personal data leakage	December 17, 2025 August 20, 2025 Akira
Bleyl Interest	Construction and engineering / Engineering services	USA	Personal data leakage Ransomware	December 5, 2025 Akira
Lydig Construction	Construction and engineering / Construction company	USA	Personal data leakage	December 12, 2025 June 21, 2025 Play
Evergreen Printing	Manufacturing / Printing company	USA	Denial of IT systems and services Ransomware	December 23, 2025 December 19, 2025 Qilin
Aras Kargo	Logistics and transportation / Logistics company	Turkey	Denial of IT systems and services Ransomware	December 1, 2025 November 30, 2025
La Poste	Logistics and transportation / Logistics company	France	Denial of IT services DDoS	December 22, 2025 Noname057(16)

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