Kaspersky ICS CERT

kaspersky

A brief overview of the main incidents in industrial cybersecurity Q2 2025

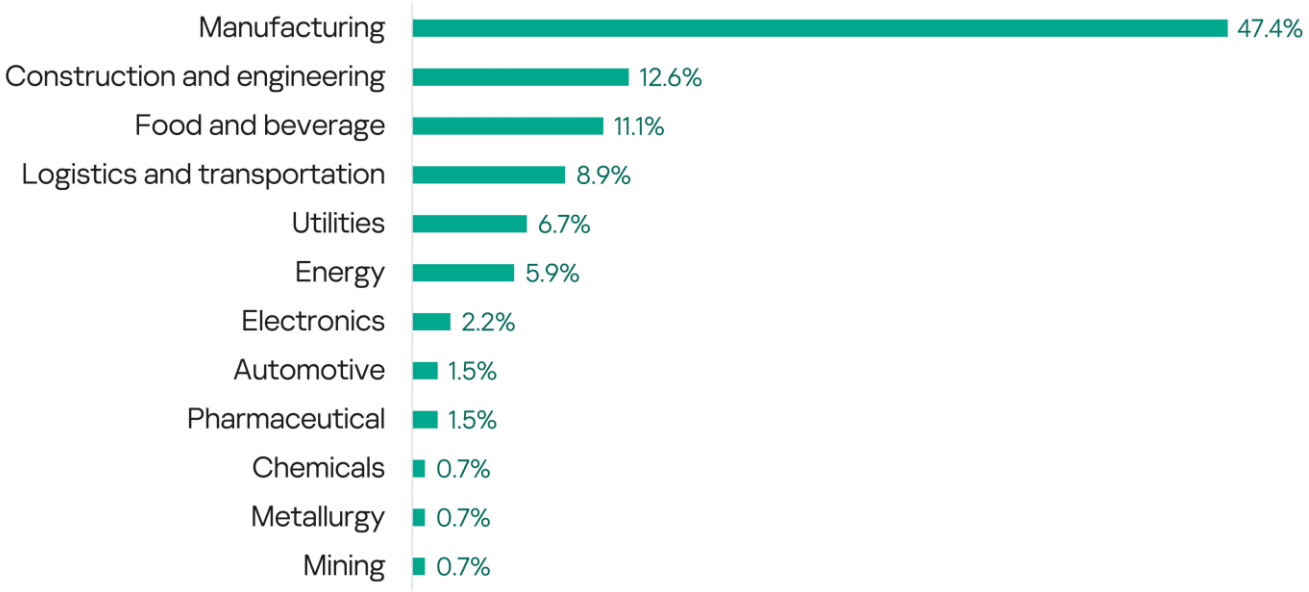
09.10.2025

Version 1.0

Contents

In Q2 2025, 135 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



April May June 2025

- Samsung
- JPW Industries
- Smiths Tubular Systems – Laconia (Titeflex)
- VF Outdoor
- Gemini Industries
- Nevro
- WK Kellogg Co
- Tempel Steel Company
- Sensata Technologies
- Ushio Europe
- Optimax Technology Corporation
- Eu-Rec
- Plasser American
- Mercury Corporation
- Harrison Poultry
- SRAM
- Sistema Intermunicipal de los Servicios de Agua Potable y Alcantarillado
- Technology Container
- Granby Heating Products
- Lee Valley Tools
- Athena Cosmetics
- KWS Manufacturing Company
- Bath Fitter Distributing
- ZTEX Construction
- Baskervill & Son, P.C.
- Harris Steel Company
- Treston IAC
- Empire Group of Reading PA
- Allied Telesis
- Maxxis International – USA
- KYB Americas Corporation
- Kintetsu World Express
- American Standard
- Aigües de Mataró
- Oettinger Getränke
- Genpro
- Crystal Geyser Water Company
- Swiss Post Cargo Germany
- J. Dahmen
- Silgan Containers
- Holz Ruser
- Lion Brothers
- M.J. Biopharm
- JLL Hut/Heads Up Technologies
- InterTest
- Huntsman Building Solutions
- Nova Scotia Power
- Tootsie Roll Industries
- Cusanos Italian Bakery

- Volkswagen Group of America
- Pittman Construction Company
- Heartland Recreational Vehicles
- Nixon
- TerraSource
- Riverside Energy Michigan
- PEZ Candy
- Philadelphia Macaroni Company
- Global Crossing Airlines
- Woods Hole Group
- South African Airways
- Masimo Corporation
- Starkville Utilities
- J. Ranck Electric
- Caltrol
- Breton
- Compumedics USA
- Kittrich
- Metromont
- Tomoku
- Mann Lake Acquisition
- Alex Apparel
- Reliable Glass & Door
- Dior
- Nucor
- Texas Fifth Wall Roofing System
- DJH Services
- Prismecs
- Arla Foods
- Motor Controls
- Kirk Corporation Companies
- Weber Packaging Solutions
- AXT
- Peter Green Chilled
- Uttar Haryana Bijli Vitran Nigam
- E.B. Archbald & Associates
- Kenai Drilling
- O'Neill Wetsuits
- Pactiv Evergreen
- Adidas
- Industrial Service Solutions
- MDG Design
- Amalgamated Sugar Company
- DC Safety Sales

- Cartier
- Wellteam
- City Public Service Energy
- FUJIPOLY Hong Kong Ltd.
- Western New York Energy
- Anchor Industries
- Excellence Optoelectronics
- Farm's Best Food Industries Sdn Bhd
- Rio Marine
- United Natural Foods
- General Digital Corporation
- Colorado West Construction
- Nova Scotia Power
- Optiline Enterprises
- Nash Brothers Construction
- Lake Risevatnet dam
- Delkin Devices
- Doyon
- Fasana
- Alpha Baking Company
- WestJet
- Controlled Air
- Krispy Kreme
- Infab Holdco
- Eastern Platinum (Eastplats)
- Birdair
- Ardurra
- Cowboy Clean Fuels
- Case Foods
- Bray International
- Electronics for Imaging
- Curium Pharma
- Bluegrass Ingredients
- Estes Forwarding Worldwide
- Siloking
- S.W. Cole Engineering
- Hawaiian Airlines
- Petoskey Plastics
- Automated Building Systems
- J-Kraft
- Johnson Controls
- Associated Truss Company (Associated Truss & Lumber)

Incidents at large organizations

Samsung Germany

Manufacturing, electronics

Personal data leakage

According to the cybercrime intelligence firm Hudson Rock, a threat actor, going by the pseudonym GHNA published approximately 270,000 customer records allegedly stolen from Samsung Germany's ticketing system. GHNA apparently gained access to Samsung's system using stolen credentials from a Spectos account used for monitoring and service quality improvements. The credentials were compromised in 2021, when an employee's computer was infected with the Raccoon Infostealer. Hudson Rock identified personally identifiable information such as names, addresses, email addresses, as well as transaction information, order numbers, tracking URLs, support interactions, and communication between customers and Samsung.

On April 1, Samsung provided Heise and CSO with a brief statement saying that an incident involving unauthorized access to customer data had occurred on an IT system belonging to one of Samsung's business partners in Germany. Samsung said it took the security of its customers' data very seriously and was investigating the extent of the incident.

On April 7, the Spectos service provider released a statement. According to the statement, a cloud server belonging to Spectos was compromised by a targeted cyberattack on March 29. The attackers exploited a vulnerability in a secondary server to gain unauthorized access to data storage within the cloud infrastructure. Personal data from two customers was collected and published on the dark web. Additional activity by the attacker was detected on April 2. This resulted in the immediate shutdown of the affected servers and the hiring of the external cybersecurity service provider G DATA to conduct a forensic investigation. Spectos informed all the relevant authorities in accordance with applicable legal regulations.

Attacks leading to insolvency

Eu-Rec

Utilities, waste management

Denial of operations, personal data leakage, insolvency

Ransomware

German disposal company Eu-Rec learned on April 7 that it had fallen victim to a cyberattack despite extensive security measures. It couldn't be ruled out that unauthorized third parties had gained access to personal data during the attack. The personal data of an estimated 200 private customers and business contacts was exposed. According to the Mercur news portal, the cyberattack forced Eu-Rec to file for insolvency with the Trier District Court. The report stated that the company was already in a strained financial situation due to rising energy prices and fluctuating orders. The cyberattack exacerbated the situation by causing significant disruption to operations. Despite the insolvency, Eu-Rec's business operations will continue in full. Employees' wages were secured through insolvency benefits. The Safepay ransomware group claimed responsibility for the attack.

Fasana

Manufacturing

Denial of operations, insolvency

Ransomware

In May, a cyberattack disrupted operations at German paper napkin manufacturer Fasana, leaving the company facing insolvency. According to a report in the Kölner Stadtanzeiger newspaper, on May 19, all systems, including PCs and laptops, were paralyzed, and all the printers began printing ransom notes. One employee stated that orders worth more than 250,000 euros could not be fulfilled on May 20, and no significant revenue was generated over the following two weeks. Employees did not receive their May salaries on time. The insolvency administrator noted that the company couldn't even print a delivery note and that business operations were completely paralyzed. Approximately 190 laptops and PCs were collected, scanned, and had all programs reinstalled. IT specialists were called in to enable communication and get production up and running as quickly as possible. Three weeks after the attack, the full range of programs was apparently still unavailable. For instance, it was reported that customer service was using only one computer.

According to a report by WDR, Fasana suffered a ransomware attack by a group known to the police. The malware spread rapidly, locking computers and encrypting files. No publicly tracked ransomware gang claimed responsibility for the attack.

Attack with cyber-physical effect

Lake Risevatnet dam

Utilities, water supply

Denial of operations

According to the Norwegian energy news agency Energiteknikk, unknown attackers hacked a Norwegian dam and remotely opened its water valve to full capacity in April. The incident affected the Lake Risevatnet dam in the municipality of Bremanger in Western Norway. The valve operated at full capacity for four hours before the unauthorized intervention was detected and contained. Fortunately, the attack resulted in minimal damage, as the volume of water only slightly exceeded the minimum water flow requirement. The water level exceeded the minimum norm by 497 liters per second, while local authorities said the riverbed could withstand up to 20,000 liters per second. An investigation found that the hack was possible due to a weak password for the valve's web control panel. This is considered a common problem for many industrial control systems. However, it was unclear whether the valve was intentionally turned on at full power.

On April 10, the dam operator notified the National Security Authority, which shared the information with the dam safety unit of the Norwegian Directorate of Water Resources and Energy. A document seen by journalists noted that the attack originated in Russia, though the Directorate did not confirm this.

Attacks leading to denial of operations

Sensata Technologies

Manufacturing

Denial of operations and services, data leakage

Ransomware

Sensata Technologies Holding, a US global industrial technology company that makes mission-critical sensors, electrical protection components, and sensor-rich solutions, experienced a ransomware incident on April 6 that encrypted certain devices in its network. According to a Form 8-K filed with the US Securities and Exchange Commission (SEC), the incident temporarily impacted Sensata Technologies' operations, including shipping, receiving, manufacturing, production and various other support functions. The company implemented interim measures to restore certain functions, but the timeline for a full recovery was not known. A preliminary investigation identified evidence that files were taken from the company's environment. Sensata Technologies worked to identify and review the files involved.

Upon discovery of the incident, Sensata Technologies immediately activated its response protocols and implemented containment measures, including

proactively taking its network offline. The company also launched an investigation with the assistance of third-party cybersecurity professionals. In coordination with legal counsel, Sensata Technologies notified law enforcement of the matter and supported its investigation. As of the date of the Form 8-K, Sensata Technologies did not expect the incident to materially impact the company's financial results and operations for the three months ending June 30, 2025. However, the full scope and impact of the incident was still unknown and it could be determined in the future that the incident was material to the company's financial statements and results of operations.

Kintetsu World Express

Transportation, logistics

Denial of operations and services

Ransomware

Kintetsu World Express, a Japanese logistics provider that offers air and sea cargo services globally, confirmed that it had fallen victim to a ransomware attack that disrupted some of its systems. Kintetsu World Express first reported service disruptions affecting certain customers on April 23, when the attack was first discovered. No additional details were provided at that time.

In a statement issued on April 28, the company announced that an investigation had determined the cause of the failure to be unauthorized access to the system by a third party through ransomware. Some operations continued to be affected. Kintetsu World Express established an Emergency Response Headquarters to conduct investigations, including a forensic investigation, to identify the scope of the incident's impact and its cause. The investigations were conducted in coordination with external professionals. The company also consulted with and reported to the Japanese police regarding the incident. In a statement issued on April 30, the company said it was in the process of restoring the affected systems. Most systems remained fully functional, enabling the company to support customers with minimal disruption.

Optimax Technology Corporation

Manufacturing

Denial of operations

Ransomware

According to a bulletin from the Taiwan Stock Exchange portal published on April 7, the information systems of Taiwanese polarizer manufacturer Optimax Technology Corporation were attacked by hackers. Once the cyberattack was detected, the company immediately activated relevant defense mechanisms to minimize the cybersecurity risks. There was no evidence of personal data or internal document leaks, and there was no significant impact on the company's operations. The company continued to enhance the security controls of its network and information infrastructure, while closely monitoring them to ensure information security. In April, the Qilin ransomware group and another actor named Devman claimed responsibility for the attack on Optimax Technology Corporation.

Excellence Optoelectronics

Manufacturing, electronics

Denial of IT systems and operations

Ransomware

According to a bulletin from the Taiwan Stock Exchange portal published on June 5, Taiwanese LED lamp and component manufacturer Excellence Optoelectronics suffered a cyberattack targeting its intranet and information systems. The company immediately activated relevant defense mechanisms to avoid any impact on information security and global operations. There was no significant impact on the company's operations. The company said it would continue to closely monitor and strengthen its information security measures.

Holz Ruser

Manufacturing

Denial of operations

German wood processing company Holz Ruser suffered a cyberattack on April 17, according to a local news outlet. The owner and managing director said at the time that the full extent of the damage could not be assessed until April 23 due to the holidays. The malware reportedly spread to the entire IT system and paralyzed business operations. No further information was available at the time of the announcement.

Masimo Corporation

Manufacturing

Denial of operations and services

According to a Form 8-K filing with the US Securities and Exchange Commission, US medical equipment manufacturer Masimo Corporation identified unauthorized activity on its on-premises network on April 27. Upon detection, the company activated its incident response protocols and implemented containment measures, including the proactive isolation of affected systems. Masimo Corporation promptly commenced an investigation with the help of third-party cybersecurity professionals to assess, mitigate, and remediate the incident. The company also notified and coordinated with law enforcement. As a result of the incident, some of the company's manufacturing facilities operated below normal levels, and the company's ability to process, fulfill, and ship customer orders in a timely manner was temporarily impacted. The company worked diligently to restore normal business operations, bring the affected portions of its network back online, and mitigate the impact of the incident. The full scope, nature, and impact of the incident were unknown. The company believed the incident did not affect its cloud-based systems and appeared to be unrelated to them.

Nucor

Manufacturing, metallurgy

Denial of IT systems and operations, data leakage

The US steel company Nucor Corporation identified a computer security breach involving unauthorized access to certain information technology systems. According to a Form 8-K filing with the US Securities and Exchange Commission on May 14, the company took steps to contain and respond to the incident. These steps included implementing its incident response plan and notifying federal law enforcement authorities. Production operations were temporarily suspended at some plants, but were later restarted. In a subsequent filing with the US Securities and Exchange Commission, Nucor Corporation confirmed that the attackers also stole data from compromised systems. The company said it had restored access to systems impacted by the breach, and believed the threat actor no longer had access to its IT systems. According to Nucor Corporation, the cybersecurity incident did not have a material impact, nor was it reasonably likely to have, a material impact on the company's business operations.

Breton

Manufacturing

Denial of IT systems and operations

On May 1, Breton, an Italian company that produces machines and plants for engineered stone and metalworking, suffered a cyberattack. According to a post on its website, the attack affected the IT infrastructure at the company's headquarters, temporarily compromising some operating systems. Thanks to its prepared and tested computer emergency response plan, the company environment was completely secured, and operations were quickly restored.

Arla Foods

Manufacturing, food and beverage

Denial of IT systems and operations

Arla Foods, a Danish dairy company with operations in Germany, was affected by a cybersecurity incident. The company identified suspicious activity at its Upahl dairy site that impacted the local IT network. Production was temporarily affected as a result of the safety measures initiated in response to the incident. Production and IT experts worked diligently to resume normal operations at the site, with the company systematically restarting systems to ensure a return to full functionality. Arla Foods informed affected customers of possible delivery delays and cancellations. BleepingComputer asked the company if the attack involved data theft or encryption, but Arla declined to share any additional information.

Wellteam

Manufacturing

Denial of operations and services

According to a local media report, German packaging manufacturer Wellteam fell victim to a cyberattack that impacted nearly every operational process, halting machinery and transportation. The attack rendered machines inoperable and prompted the company to send employees home. Wellteam reportedly became aware of the attack on May 23. Initially, internal communications were affected. Despite the implementation of extensive protective measures in accordance with internal emergency procedures, serious disruptions ultimately occurred. Production was severely disrupted. Wellteam declined to disclose further details about the attack. The company stated that because they reacted quickly, no data – neither employee nor customer – was leaked.

Siloking

Manufacturing

Denial of IT systems and operations

Ransomware

On June 15, German agricultural machinery manufacturer Siloking was hit by a cyberattack that caused operational disruptions. In response to a request, the company stated in a press release that ransomware had encrypted systems. Production continued in emergency mode. After the cyberattack was discovered, the authorities and the State Criminal Police Office were immediately notified. The network and all the company computers were reinstalled. In June, the Qilin ransomware group claimed responsibility for the attack on Siloking.

Estes Forwarding Worldwide

Transportation, logistics

Denial of operations

Ransomware

On June 25, US logistics company Estes Forwarding Worldwide told FreightWaves that it had been hit by a cyberattack on May 28. Estes Forwarding Worldwide said it had notified employees and customers of the attack. The company assured that there was no significant disruption to its business. Thanks to robust cybersecurity protocols, system redundancies, and the swift response of the IT team and third-party security experts, the company was fully operational within hours. Estes Forwarding Worldwide expressed gratitude for the support of its parent company, Estes Express Lines, throughout the incident. Neither Estes LTL nor Estes Logistics were impacted by the attack. EFW said it would enhance its security measures. In June, the Qilin ransomware group claimed responsibility for the attack on Estes Forwarding Worldwide.

United Natural Foods

Transportation, logistics

Denial of services and operations

US grocery supplier and distributor United Natural Foods filed a Form 8-K with the US Securities and Exchange Commission, disclosing that unauthorized access to their system was discovered on June 5. The company promptly activated its incident response plan, implementing containment measures that included proactively taking certain systems offline. These measures temporarily impacted the company's ability to fulfill and distribute customer orders. The incident caused disruptions to business operations that were expected to continue. With the help of third-party cybersecurity professionals, United Natural Foods worked actively to assess, mitigate, and remediate the incident and notified law enforcement. According to its business continuity plans, United Natural Foods implemented workarounds to continue servicing its customers where possible. The company continued working to restore its systems and bring them safely back online.

Appendix. Full list of confirmed incidents

Victim	Industry/Profile	Country	Impact features	Date of notification/ Date of incident (if known)/ Suspected attackers
JPW Industries	Manufacturing / Machine and industrial equipment manufacturer	USA	Personal data leakage Ransomware	April 1, 2025 February 3, 2025 RansomHub
Nevro	Manufacturing / Medical equipment manufacturer	USA	Personal data leakage	April 3, 2025 November 21, 2024
Gemini Industries	Chemicals, manufacturing / High-quality, innovative wood coatings manufacturer	USA	Personal data leakage Ransomware	April 2, 2025 October 15, 2024 RansomHub
Tempel Steel Company	Manufacturing / High-precision electrical steel	USA	Denial of IT systems,	April 4, 2025 February 6, 2025

	laminations manufacturer		personal data leakage Ransomware	Cactus
VF Outdoor	Manufacturing / Clothing manufacturer	USA	Personal data leakage	April 2025 March 13, 2025
Lee Valley Tools	Manufacturing / Woodworking and gardening tools manufacturer	Canada	Personal data leakage	April 15, 2025 October 8, 2024
Plasser American	Manufacturing / Railway track maintenance equipment and machinery manufacturer	USA	Personal data leakage Ransomware	April 9, 2025 February 2, 2025 Safepay
Harrison Poultry	Food and beverage, manufacturing / Poultry product producer	USA	Personal data leakage	April 10, 2025 November 14, 2024
Athena Cosmetics	Manufacturing / Cosmetics manufacturer	USA	Personal data leakage Ransomware	April 15, 2025 January 15, 2025 Cactus
KWS Manufacturing Company	Manufacturing / Industrial equipment manufacturer	USA	Personal data leakage Ransomware	April 15, 2025 January 24, 2025 Play
Allied Telesis	Manufacturing / Network communications solution manufacturer	Japan	Personal data leakage Ransomware	April 21, 2025 April 30, 2024 LockBit 3.0
Baskervill & Son, P.C.	Construction and engineering / Construction and engineering services	USA	Personal data leakage Ransomware	April 17, 2025 September 13, 2024 Play
Genpro	Logistics and transportation /	USA	Personal data leakage	April 24, 2025 September 21, 2024

	Logistics and transportation company			
Silgan Containers	Manufacturing / Packaging and container manufacturer	USA	Personal data leakage Ransomware	April 25, 2025 February 2, 2024 LockBit 3.0
SRAM	Manufacturing / Bicycle component manufacturer	USA	Personal data leakage	April 10, 2025 March 6, 2025
Mercury Corporation	Manufacturing / Metal and plastic products manufacturer	USA	Personal data leakage	April 9, 2025 February 18, 2025
ZTEX Construction	Construction and engineering / Earthwork, underground utilities, asphalt paving, concrete paving, concrete retaining walls, gas line installation, directional drilling	USA	Personal data leakage	April 16, 2025
Treston IAC	Manufacturing / Office and laboratory furniture manufacturer	USA	Personal data leakage Ransomware	April 18, 2025 November 10, 2024 Hunters International
Maxxis International – USA	Manufacturing / Tire manufacturer	USA	Personal data leakage Ransomware	April 21, 2025 October 17, 2024 Black Suit
Empire Group of Reading PA	Construction and engineering / Demolition and excavation services provider	USA	Personal data leakage Ransomware	April 17, 2025 January 16, 2025 Lynx
Harris Steel Company	Manufacturing / Steel slitting and processing manufacturer	USA	Personal data leakage Ransomware	April 16, 2025 DragonForce

CMC Design Build	Construction and engineering / Design-build construction corporation	USA	Personal data leakage	April 22, 2025
KYB Americas Corporation	Automotive, manufacturing / Manufacturer of hydraulic components for agriculture, construction, forestry, and material handling industries	USA	Denial of IT systems, personal data leakage Ransomware	April 22, 2025 February 11, 2025 Cactus
American Standard	Manufacturing / Plumbing and building product manufacturer	USA	Personal data leakage Ransomware	April 23, 2025 RansomHub
Lion Brothers	Manufacturing / Manufacturer of apparel decorations for sports, lifestyle and fashion brands	USA	Personal data leakage	April 25, 2025 October 5, 2024
JLL Hut/Heads Up Technologies	Manufacturing / Aviation and aerospace component manufacturer	USA	Personal data leakage	April 28, 2025
Tootsie Roll Industries	Food and beverage, manufacturing / Confectionary manufacturer	USA	Personal data leakage	April 29, 2025
Crystal Geyser Water Company	Food and beverage, manufacturing / Beverage manufacturer	USA	Personal data leakage	April 25, 2025
Smiths Tubular Systems – Laconia (Titeflex)	Manufacturing / Flexible metal hose and tubing manufacturer	USA	Personal data leakage	April 1, 2025 January 23, 2025
Technology Container	Manufacturing / Reusable corrugated plastic boxes, flat sign	USA	Personal data leakage	April 11, 2025

	board and corrugated paper box manufacturer			
Bath Fitter Distributing	Manufacturing / Bath and shower manufacturer	Canada	Personal data leakage Ransomware	April 15, 2025 December 4, 2024 BlackBasta
InterTest	Manufacturing / Industrial inspection equipment and remote viewing systems manufacturer	USA	Personal data leakage	April 28, 2025 February 12, 2025
Cusanos Italian Bakery	Food and beverage, manufacturing / Bread manufacturer	USA	Personal data leakage	April 29, 2025
Granby Heating Products	Manufacturing / Heating equipment manufacturer	Canada	Personal data leakage Ransomware	April 14, 2025 BlackBasta
Huntsman Building Solutions	Manufacturing / Polyurethane spray foam and coatings manufacturer	USA	Personal data leakage	April 28, 2025 February 11, 2025
WK Kellogg Co	Food and beverage, manufacturing / Food manufacturer	USA	Personal data leakage Ransomware	April 4, 2025 December 7, 2024 Clop
Aigües de Mataró	Utilities / Water utility	Spain	Denial of IT services, personal data leakage	April 23, 2025 April 21, 2025
Sistema Intermunicipal de los Servicios de Agua Potable y Alcantarillado	Utilities / Water utility, sewerage services	Mexico	Denial of IT services	April 10, 2025

Oettinger Getränke	Food and beverage, manufacturing / Beer and soft drink manufacturer	Germany	Unknown Ransomware	April 24, 2025 RansomHouse
Nova Scotia Power	Utilities / Power producer, transmission and distribution company	Canada	Denial of IT systems and services, personal data leakage Ransomware	April 28, 2025 March 19, 2025
Swiss Post Cargo Germany	Logistics and transportation / Transport, logistics, warehousing and customs clearance solutions	Germany	Denial of IT systems and services, data leakage	April 25, 2025
M.J. Biopharm	Pharmaceutical, manufacturing / Biopharmaceutical company	India	Denial of IT systems Ransomware	April 27, 2025
Ushio Europe	Manufacturing / Special lamps manufacturer	The Netherlands	Denial of IT systems and services Ransomware	April 7, 2025 Termite
J. Dahmen	Logistics and transportation / Transport, logistics, warehousing and customs clearance solutions	Germany	Denial of IT services Ransomware	April 25, 2025 April 23, 2025 Akira
Global Crossing Airlines	Logistics and transportation / Airline	USA	unknown	May 5, 2025 Anonymous
South African Airways	Logistics and transportation / Airline	South Africa	Denial of IT systems and IT services Ransomware	May 6, 2025 May 3, 2025 INC Ransom

Nixon	Manufacturing / Watch and accessory manufacturer	USA	Personal data leakage	May 2, 2025 December 18, 2024
E.B. Archbald & Associates	Energy / Energy production accounting services provider to oil and gas producers and operators	USA	Personal data leakage Ransomware	May 21, 2025 March 23, 2025 Qilin
TerraSource	Manufacturing / Industrial equipment manufacturer	USA	Personal data leakage	May 2, 2025
Starkville Utilities	Utilities / Electric and water utility	USA	Personal data leakage	May 6, 2025 October 23, 2024
Compumedics USA	Manufacturing / Medical device manufacturer	USA	Personal data leakage	May 8, 2025 March 13, 2025
Caltrol	Manufacturing / Provider of automation including process control solutions, valves, instrumentation	USA	Personal data leakage Ransomware	May 7, 2025 January 27, 2025 Cactus
Kittrich	Manufacturing / Consumer packaged goods manufacturer	USA	Personal data leakage	May 8, 2025 February 12, 2025
DJH Services	Energy / Oil and gas producer	USA	Denial of IT systems, personal data leakage	May 14, 2025 February 13, 2025
DC Safety Sales	Manufacturing / First aid and preparedness product manufacturer	USA	Personal data leakage	May 28, 2025 December 11, 2024
Kenai Drilling	Energy / Development of onshore and offshore oil, gas and geothermal wells	USA	Personal data leakage	May 22, 2025 May 17, 2025

PEZ Candy	Food and beverage, manufacturing / Candy manufacturer	USA	Personal data leakage	May 5, 2025 Abyss
Philadelphia Macaroni Company	Food and beverage, manufacturing / Pasta manufacturer	USA	Personal data leakage	May 5, 2025 FOG
Riverside Energy Michigan	Energy / Development and exploration of oil and gas assets	USA	Personal data leakage	May 5, 2025 February 4, 2025
J. Ranck Electric	Construction and engineering / Construction service provider	USA	Personal data leakage	May 7, 2025 February 23, 2025
Metromont	Manufacturing / Precast concrete manufacturer	USA	Personal data leakage	May 8, 2025
Alex Apparel	Manufacturing / Garment manufacturer	USA	Personal data leakage	May 12, 2025 March 10, 2025
Motor Controls	Manufacturing / Industrial machinery manufacturer	USA	Personal data leakage	May 16, 2025
Pittman Construction Company	Construction and engineering / Heavy highway construction services provider	USA	Personal data leakage Ransomware	May 2025 Lockbit3
Kirk Corporation Companies	Construction and engineering / Water and wastewater treatment plant construction	USA	Denial of IT systems, personal data leakage	May 19, 2025 August 7, 2024
Weber Packaging Solutions	Manufacturing / Manufacturer of pressure-sensitive labels, labeling systems, RFID labeling	USA	Personal data leakage Ransomware	May 19, 2025 October 7, 2024 BlackBasta

AXT	Electronics, manufacturing / Semiconductor manufacturer	USA	Personal data leakage Ransomware	May 20, 2025 April 8, 2025 DragonForce
Amalgamated Sugar Company	Food and beverage, manufacturing / Sugar production, processing, and manufacturing company	USA	Personal data leakage Ransomware	May 28, 2025 February 5, 2025 Cactus
Reliable Glass & Door	Manufacturing / Glass and door services provider	USA	Personal data leakage	May 12, 2025 November 7, 2024
O'Neill Wetsuits	Manufacturing / Wetsuits and water gear manufacturer	USA	Personal data leakage Ransomware	May 23, 2025 February 23, 2025 RansomHub
Woods Hole Group	Construction and engineering / Engineering solutions along the coast, in the ocean, and in wetland and terrestrial environments	USA	Personal data leakage	May 6, 2025 March 4, 2025
Mann Lake Acquisition	Manufacturing / Manufacturer of beekeeping supplies	USA	Personal data leakage	May 9, 2025 March 14, 2025
Heartland Recreational Vehicles	Manufacturing / Towable recreational vehicles manufacturer	USA	Personal data leakage Ransomware	May 1, 2025 RansomHub
Volkswagen Group of America	Automotive, manufacturing / Automotive manufacturer	USA	Personal data leakage Ransomware	May 2025 Stormous
Industrial Service Solutions	Manufacturing / Provider of equipment and applications, valves, actuation, motors,	USA	Personal data leakage	May 27, 2025

	generators, pumps, compressors, coolers, boilers, heat exchangers, mixers, electrical-equipment controls, peripheral equipment			
MDG Design	Construction and engineering / Construction of residential apartment buildings	USA	Personal data leakage Ransomware	May 28, 2025 April 25, 2025 Qilin
Texas Fifth Wall Roofing System	Construction and engineering / Commercial roofing to the construction and re-roof installations of single-ply, metal, and composite systems	USA	Personal data leakage Ransomware	May 14, 2025 Frag
Pactiv Evergreen	Manufacturing / Manufacturer of fresh food and beverage packaging	USA	Personal data leakage	May 23, 2025
Tomoku	Manufacturing / Paper and packaging manufacturer	Japan	Denial of IT services	May 8, 2025 May 3, 2025 Gunra
Uttar Haryana Bijli Vitran Nigam	Utilities / Energy distribution utility	India	Denial of services	May 20, 2025 May 7, 2025
Peter Green Chilled	Logistics and transportation / Logistics and transportation company	UK	Denial of services Ransomware	May 20, 2025 May 14, 2025
Prismecs	Energy / Power plant operator	USA	Email hijacking	May 15, 2025
Adidas	Manufacturing / Sporting goods manufacturer	Germany	Personal data leakage	May 23, 2025

Alpha Baking Company	Food and beverage, manufacturing / Food manufacturer	USA	Personal data leakage Ransomware	June 13, 2025 January 22, 2025 RansomHub
General Digital Corporation	Manufacturing / Manufacturer of industrial and military grade monitors	USA	Personal data leakage Ransomware	June 5, 2025 January 14, 2025 Space Bears
Bray International	Manufacturing / Flow control and automation product and accessory manufacturer	USA	Personal data leakage	June 20, 2025 April 17, 2024
Electronics for Imaging	Manufacturing / Printer manufacturer and digital front ends for digital printing solutions provider	USA	Personal data leakage Ransomware	June 20, 2025 September 17, 2024 Hellcat
Bluegrass Ingredients	Food and beverage, manufacturing / Food ingredient manufacturer	USA	Personal data leakage Ransomware	June 25, 2025 November 05, 2024 Akira
Curium Pharma	Pharmaceutical, manufacturing / Pharmaceutical manufacturer	France	Personal data leakage	June 20, 2025 October 15, 2024
Doyon	Energy / Oil field services, utility management, engineering management	USA	Personal data leakage Ransomware	June 12, 2025 April 1, 2024 Black Basta
Colorado West Construction	Construction and engineering / General building construction services	USA	Personal data leakage	June 6, 2025 May 29, 2025
Western New York Energy	Energy / Fuel ethanol producer	USA	Personal data leakage Ransomware	June 4, 2025 April 25, 2025 SafePay

Optiline Enterprises	Construction and engineering / Construction company	USA	Personal data leakage Ransomware	June 9, 2025 December 26, 2024 Cactus
Nash Brothers Construction	Construction and engineering / Underground utility construction	USA	Personal data leakage Ransomware	June 10, 2025 December 2024 Lynx BianLian
Delkin Devices	Manufacturing / Flash storage devices and accessories manufacturer	USA	Personal data leakage	June 11, 2025
Krispy Kreme	Food and beverage, manufacturing / Doughnut producer	USA	Personal data leakage Ransomware	June 16, 2025 November 29, 2024 Play
Controlled Air	Construction and engineering / Engineering, building automation, energy management, mechanical construction	USA	Personal data leakage Ransomware	June 15, 2025 RansomHub
Infab Holdco	Manufacturing / Medical equipment manufacturer	USA	Personal data leakage	June 16, 2025
Birdair	Construction and engineering / Specialty contractor for custom tensile membrane structures	USA	Denial of IT systems, personal data leakage Ransomware	June 20, 2025 October 27, 2024 Play
Ardurra	Construction and engineering / Civil engineering company	USA	Personal data leakage	June 20, 2025

Case Foods	Food and beverage, manufacturing / Poultry processing company	USA	Personal data leakage	June 20, 2025
J-Kraft	Manufacturing / Cabinet manufacturer	USA	Personal data leakage Ransomware	June 30, 2025 Worldleaks
Automated Building Systems	Construction and engineering / Commercial building automation and integration, energy conservation, lighting, building controls provider	USA	Personal data leakage	June 30, 2025 February 2025
Rio Marine	Logistics and transportation / Repairs and upgrades, refits and installations, vessel maintenance, hydraulic systems	USA	Personal data leakage Ransomware	June 5, 2025 July 30, 2024 Cactus Sarcoma
Petoskey Plastics	Manufacturing / Plastic manufacturer	USA	Personal data leakage	June 27, 2025
S.W. Cole Engineering	Construction and engineering / Geotechnical engineering services, construction materials testing provider	USA	Personal data leakage	June 26, 2025
Cowboy Clean Fuels	Energy / Renewable energy production	USA	Personal data leakage	June 20, 2025
Johnson Controls	Manufacturing / Manufacturer of HVAC equipment, security and automation systems for buildings	Ireland	Denial of IT systems, personal data leakage Ransomware	June 30, 2025 September 24, 2023 Dark Angels
City Public Service Energy	Utilities / Municipal electric utility	USA	Personal data leakage	June 2, 2025

Associated Truss Company (Associated Truss & Lumber)	Manufacturing / Wood building product manufacturer	USA	Personal data leakage	June 30, 2025
Anchor Industries	Manufacturing / Tent manufacturer	USA	Denial of IT services Ransomware	June 4, 2025 May 26, 2025 Play
FUJIPOLY Hong Kong Ltd.	Manufacturing / Thermal interface material manufacturer	Japan	Denial of IT systems Ransomware	June 3, 2025 SpaceBears
Eastern Platinum (Eastplats)	Mining, manufacturing / Mining company	Canada	Denial of IT systems, data leakage Ransomware	June 16, 2025 WorldLeaks
WestJet	Logistics and transportation / Airline	Canada	Denial of IT systems and IT services Ransomware	June 13, 2025 Scattered Spider
Hawaiian Airlines	Logistics and transportation / Airline	USA	Denial of IT systems Ransomware	June 26, 2025 Scattered Spider
Farm's Best Food Industries Sdn Bhd	Food and beverage, manufacturing / Food producer	Malaysia	Denial of IT services	June 5, 2025 June 3, 2025
Cartier	Manufacturing / Jewelry and watch manufacturer	France	Personal data leakage	June 2, 2025
Dior	Manufacturing / Luxury good manufacturer	France	Personal data leakage	May 13, 2025 May 7, 2025
Samsung	Electronics, manufacturing / Manufacturing conglomerate	Germany	Personal data leakage	April 1, 2025 March 29, 2025

Eu-Rec	Utilities / High-quality recycling technology manufacturer	Germany	Denial of operations, personal data leakage, insolvency Ransomware	April 7, 2025 Safepay
Fasana	Manufacturing / Paper napkin manufacturer	Germany	Denial of operations, insolvency Ransomware	June 12, 2025 May 19, 2025
Lake Risevatnet dam	Utilities / Water supply	Norway	Denial of operations	June 10, 2025 April 2025
Sensata Technologies	Manufacturing / Mission-critical sensors, electrical protection components and sensor-rich solutions	USA	Denial of operations and services, data leakage Ransomware	April 6, 2025
Kintetsu World Express	Logistics and transportation / Logistics provider	Japan	Denial of operations and services Ransomware	April 23, 2025
Optimax Technology Corporation	Manufacturing / Polarizer manufacturer	Taiwan	Denial of operations Ransomware	April 7, 2025 Qilin, Devman
Excellence Optoelectronics	Electronics, manufacturing / LED components, modules, and energy manufacturer	Taiwan	Denial of IT systems and operations Ransomware	June 5, 2025
Holz Ruser	Manufacturing / Wooden pallets, pallets, slotted corrugated cartons manufacturer	Germany	Denial of operations	April 25, 2025 April 17, 2025

Masimo Corporation	Manufacturing / Medical equipment manufacturer	USA	Denial of services and operations	May 6, 2025
Nucor	Metallurgy, manufacturing / Steel manufacturer and recycler	USA	Denial of IT systems and operations, data leakage Ransomware	May 13, 2025
Breton	Manufacturing / Producer of machines and plants for engineered stone and metalworking	Italy	Denial of IT systems and operations	May 7, 2025 May 1, 2025
Arla Foods	Food and beverage, manufacturing / Dairy company	Germany	Denial of IT systems and operations	May 16, 2025
Wellteam	Manufacturing / Packaging manufacturer	Germany	Denial of services and operations	June 2, 2025 May 23, 2025
Siloking	Manufacturing / Agricultural machinery manufacturer	Germany	Denial of IT systems and operations Ransomware	June 25, 2025 June 15, 2025 Qilin
Estes Forwarding Worldwide	Logistics and transportation / Logistics company	USA	Denial of operations	June 25, 2025 May 28, 2025 Qilin
United Natural Foods	Logistics and transportation / Grocery supplier and distributor	USA	Denial of services and operations	June 5, 2025

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