Kaspersky ICS CERT

kaspersky

A brief overview of the main incidents in industrial cybersecurity Q1 2025

26.06.2025

Version 1.0

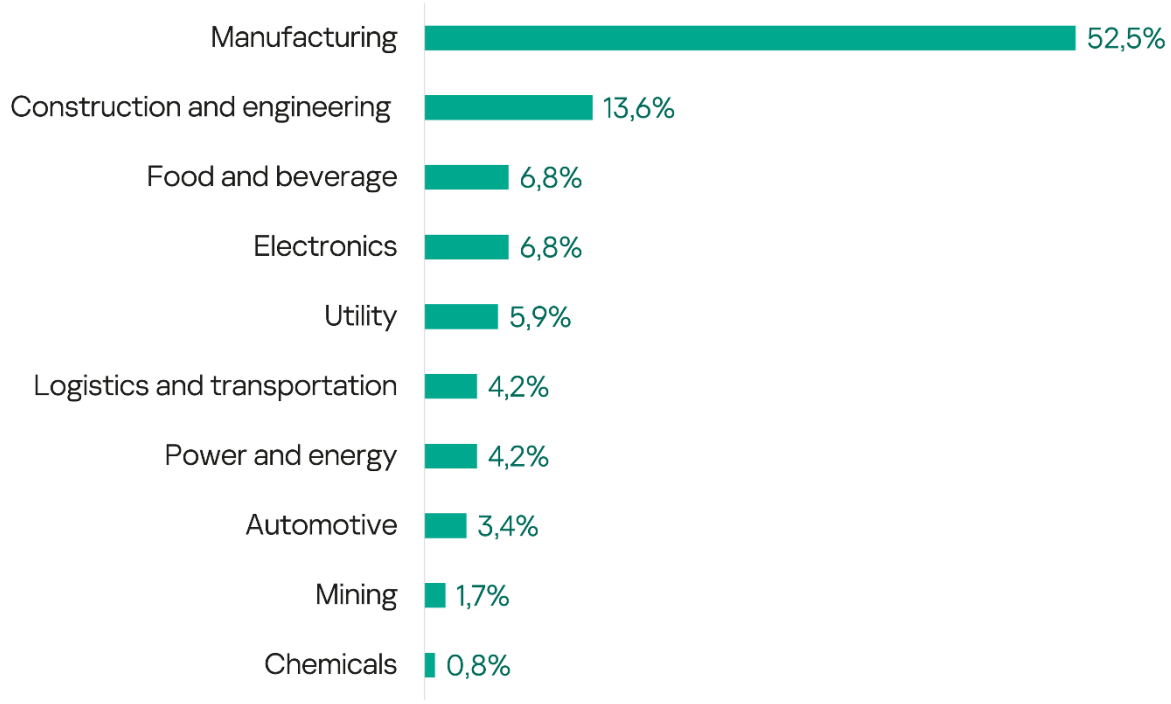
Contents

Report at a glance ... 3
Incidents at large organizations ... 5
Tata Technologies ... 5
Two separate attacks ... 5
Troxler Electronic Laboratories ... 5
Unsuccessful negotiations ... 6
National Presto Industries ... 6
Attacks leading to denial of operations ... 7
Marposs ... 7
Crystal D ... 7
Fabricaciones Militares ... 7
Ålands Centralandelslag ... 8
Imaflex ... 8
Kuala Lumpur International Airport ... 8
Unimicron Technology ... 9
Astral Foods ... 9
Ganong Bros. ... 10
The attack, which lasted almost a year ... 10
Littleton Electric Light and Water Departments ... 10
Appendix. Full list of confirmed incidents ... 11

In Q1 2025, 118 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

This quarter, organizations from multiple industrial sectors around the world reported serious incidents caused by cyberattacks. These attacks resulted in the loss of confidential data and the interruption of IT services and key operational processes, including the production and supply of products. The most high-profile story of the quarter was undoubtedly the attack on Kuala Lumpur airport, which knocked out many of its information systems, including departure and arrival boards, check-in terminals and baggage handling systems, for 10 hours.



January

- Prime Technological Services
- Stiiizy
- Avery Products
- Edw. C. Levy
- Garden of Life
- Flashforge
- Clutch Industries
- Prodinger
- Argenio Bros.
- All American Poly
- Mity, Inc.
- Marposs
- Smiths Group
- KMB Design Group
- GIGAFLIGHT Connectivity, Inc.
- Yazoo Valley Electric Power Association
- Mizuno USA
- James H. Maloy
- Unimicron Technology
- InterCon Construction
- Tata Technologies
- O'Connor Corporation

February

- Galliker's Dairy Company
- Fashion Box/Replay
- Mayer Steel Pipe Corporation
- Nan Ya Printed Circuit Board Corporation
- SMC Corporation of America
- Textiles Coated
- Big Green Egg
- American Plumbing & Heating Corporation
- Lighthouse Electric Company
- IMI
- Mark Dunning Industries
- JSP International Group
- Vorwerk
- Canyon State Electric
- Transcend Information
- Fortune Electric
- Port of Ostend
- Mid-State Industrial
- Natures Organics
- Oceanside Glasstile Company
- Finn Corporation
- McMillan Electric Company
- Commercial Specialty Truck Holdings
- Eckert & Ziegler SE
- Trinity Petroleum Management
- NioCorp Developments
- Trident Maritime Systems
- Fortis Solutions Group
- Raymond Limited
- Daedong-USA
- Hartson-Kennedy
- Standard Calibrations
- QualiTech
- Nuna Baby Essentials
- Title 9 Sports
- Imaflex
- Racal Acoustics
- Advanced Foam Recycling / Amalgamate Processing
- Biagi Bros.
- Suit-Kote Corporation
- Anellotech
- McLanahan Corporation
- Nijhuis Bouw BV

March

- Topy America
- National Presto Industries
- Bavaria Sausage
- Adval Tech Group
- Fabricaciones Militares Sociedad del Estado
- Pocket Nurse
- Power Test Industries
- Purecoat North / Purecoat International
- Unikorn Semiconductor Corporation
- Stadtwerke Schwerte
- Jonti-Craft
- Grede Holdings
- Boart Longyear Group
- Ålands Centralandelslag (Ålandsmejeriet and Ålandsbagarn)
- Engine Power Source
- Eckert & Ziegler Isotope Products
- TERREPOWER
- Numotion
- Crystal D
- Brucha
- F.tech R&D North America
- OBI
- Connecticut Container Corporation / Unicorr Packaging Group
- Lane Automotive
- Littleton Electric Light & Water Department
- Erickson Companies
- Edesur Dominicana
- Continental Aerospace Technologies
- IKAV Energy
- OEC Freight Companies
- Ganong Bros.
- Cardo Systems
- Keding Enterprises Co.
- Leisure Time Products / Backyard Discovery
- Mark Thomas
- Strauss Brands
- Geokon
- Mission Bell Mfg
- CSG Consultants
- Great Western Drilling Company
- Water and Sewerage Corporation
- AMA S.p.A. (Azienda Municipale Ambiente)
- Astral Foods
- Fireproof Contractors
- Kuala Lumpur International Airport
- Johnson Health Tech
- Plaisted Companies
- Smiths Interconnect and Smiths Interconnect Americas
- Sunnking Electronics Recycling
- Sheng Yu Steel
- Hofmann Fördertechnik
- Champion Home Builders

Incidents at large organizations

Tata Technologies

Construction, engineering

Denial of IT services

Ransomware

On January 31, Indian multinational engineering company Tata Technologies, which focuses on heavy machinery for the automotive, aerospace and industrial sectors, reported a cybersecurity incident to the National Stock Exchange of India. According to the company's report, a ransomware incident prompted the multinational company to temporarily suspend some of its IT services. Those services were subsequently restored. The company's client delivery services remained fully functional and unaffected throughout the attack. In a statement to Recorded Future, the company said it launched an investigation immediately after discovering the cyberattack. A company spokesperson confirmed that there was no disruption to operations, and Tata Technologies continued to seamlessly deliver services to its customers. In March, the Hunters International ransomware group claimed responsibility for the attack on Tata Technologies, stating they had stolen 1.4 TB of data, consisting of 730,000 files. However, the group did not post any samples of the stolen files or elaborate on the type of documents they hold.

Two separate attacks

Troxler Electronic Laboratories

Manufacturing, construction

Personal data leakage

Ransomware

Troxler Electronic Laboratories Inc., a US manufacturer of testing and quality control measurement equipment for the highway and construction industry as well as nuclear moisture/density gauges (for industrial radiography), suffered two separate cyberattacks in which hackers stole personal information. On November 10, 2024, Troxler detected suspicious activity in its network environment. Upon discovering this incident, Troxler promptly took steps to secure its network and engaged a specialized cybersecurity firm to investigate the nature and scope of the incident. As a result of the investigation, Troxler learned that an unauthorized actor accessed certain files and data stored within its network. Upon learning this, Troxler began a time-consuming and detailed reconstruction and review of the data stored on its servers at the time of the incident to determine whose information may have been affected. On December 4, 2024, Troxler identified individuals whose sensitive data may have been included in the impacted data. Around December 11, 2024, Troxler became aware of additional suspicious activity that could have resulted in access to or copying of information from the same systems that were previously impacted. Troxler

determined that the following information may have been copied without authorization as a result of the event: name, Social Security number, and driver's license number. The RansomHub ransomware group claimed responsibility for the attack on Troxler Electronic Laboratories in December 2024.

Unsuccessful negotiations

National Presto Industries

Manufacturing

Denial of operations, services and IT systems, data leakage

Ransomware

According to a regulatory filing with the Securities and Exchange Commission, National Presto Industries, a consumer products manufacturer and defense company based in the USA, reported a cyberattack that caused a system outage on March 1. Upon discovering the attack, the company activated its incident response team, comprised of internal personnel and external cybersecurity experts retained to assist with addressing the incident. The company conducted a forensic analysis to determine the nature, scope and impact of the incident. The incident temporarily impacted the company's operations, including shipping and receiving, some manufacturing processes, and various other back-office functions, much of which was quickly restored. National Presto Industries implemented temporary measures to maintain critical functions while systems were being restored. According to the filling, the incident could potentially have a material impact on the company's financial condition and operating results.

The InterLock ransomware group claimed responsibility for a cyberattack on National Defense Corporation, a subsidiary of National Presto Industries. On its dark web leak site, InterLock claimed to have hacked the company and exfiltrated 4,200 GB of data consisting of 2,900,205 files and 449,989 folders. The group provided some screenshots as proof. InterLock told DataBreaches that it had attempted to extort the company, but the negotiations were unsuccessful because National Defense Corporation did not consider the incident to be significant. The company allegedly told InterLock that the stolen information would have little value to others and that it would experience minimal financial impact from the data breach. National Defense Corporation also allegedly informed InterLock that all operations were back to normal. The ransomware group claimed to have encrypted the systems of at least three National Presto Industries entities, including AMTEC, which manufactures ammunition and explosives for the military and law enforcement.

Attacks leading to denial of operations

Marposs

Manufacturing

Denial of operations and services

Ransomware

On January 26, Marposs, an Italian producer of measurement and control systems for the manufacturing industry, suffered a ransomware cyberattack that encrypted some of its servers. The attack impacted business activities in various ways, with more serious consequences for logistics and less for production. Marposs notified the relevant authorities of the incident and began gradually restoring its systems to resume normal operations. The company responded quickly by setting up a team of cybersecurity experts to minimize the damage. Because of the cyberattack, the company requested the activation of the Ordinary Layoff Fund until February 7 to protect people and the company itself. This tool, designed for emergency situations like this one, was applied partially and flexibly to the most affected sectors and was intended to be reduced as activities gradually resumed.

Crystal D

Manufacturing

Denial of operations and services

Ransomware

On March 7, Crystal D, a US manufacturer of crystal awards and gifts, reported experiencing a cyberattack that disrupted its operations, including communication and deliveries. Orders scheduled to ship March 7 were rescheduled. According to the company's statement, there was no indication that the hackers accessed sensitive customer information. On March 12, the company said it was able to communicate with customers and process orders again. The executive vice president of marketing and sales explained that the cyberbreach compelled Crystal D to temporarily shut down parts of its network. The company was unable to access phones and email accounts, and communication with customers was down. At least some orders that were set to ship were delayed and required rescheduling. The LockBit ransomware group claimed responsibility for the cyberattack on Crystal D.

Fabricaciones Militares

Manufacturing

Denial of operations and services, data leakage

Ransomware

According to Cyber Press, the Argentinian state-owned military manufacturer Fabricaciones Militares Sociedad del Estado (Military Industries State Corporation) was hit by a cyberattack attributed to the MONTI ransomware group. The attack allegedly resulted in the theft of over 300 GB of sensitive data. Production was halted at the company's Domingo Matheu small arms facility in Buenos Aires, delaying deliveries under the FONDEF National Defense Fund-backed contracts. Argentina's Cybersecurity Agency (Unidad Fiscal Especializada en Ciberdelincuencia) confirmed that threat actors accessed

sensitive documents. On its dark web portal, the MONTI group mocked the management of Fabricaciones Militares for its insufficient cooperation, which, according to Cyber Press, suggests that negotiations were underway to recover the stolen information.

Ålands Centralandelslag

Food and beverage, manufacturing

Denial of operations

According to local press, two Finnish dairy and bakery production companies of the Åland Central Cooperative (Ålands Centralandelslag, ÅCA) – Ålandsmejeriet and Ålandsbagarn – were subjected to a cyberattack on March 5. After several hours of intensive work, all systems were operational again. Some operations were delayed because some processes were being carried out analogically for security reasons. ÅCA warned its customers to remain vigilant for any unusual communications from the company.

Imaflex

Manufacturing

Denial of operations, denial of IT systems, personal data leakage

On February 21, Imaflex, a Canadian manufacturer of solutions for the flexible packaging space, polyethylene (plastic) film and bags, announced that a cybersecurity incident had occurred, disrupting its systems and operations. Imaflex immediately took steps to contain and mitigate any potential impact on its data and operations. The company launched a comprehensive investigation to determine the source and extent of the incident, working closely with third-party cybersecurity experts in line with industry best practices. Although operations were impacted, Imaflex continued to manufacture, ship and perform back-office functions as required, albeit with some temporary workarounds. On March 27, the company announced that it had restored its systems and resumed normal operations. Imaflex reported to the Attorney General of the Commonwealth of Massachusetts that sensitive personally identifiable information in its care had been compromised.

Kuala Lumpur International Airport

Transportation, logistics

Denial of operations and services

Ransomware

According to a joint statement from Malaysia's National Cyber Security Agency and Malaysia Airports Holdings Berhad, the computer disruptions that affected Kuala Lumpur International Airport were the result of a cyberattack. The coordinated statement confirmed that the attack began on March 23, causing operational disruptions across critical airport systems. The Malaysian prime minister stated that he refused to pay the US$10 million ransom demanded by the hackers. No further technical details were disclosed. Despite the attack, Malaysia Airports officials confirmed that core operations at Kuala Lumpur International Airport were not significantly impacted. However, reports and

photographs circulating online indicated that several terminal systems, including flight information displays, check-in kiosks, and baggage handling, were rendered inoperable for over 10 hours. This forced airport staff to revert to manual operations, using whiteboards and markers to communicate departure times. A former Malaysian member of parliament drew attention to the prolonged outage.

The Qilin ransomware gang claimed responsibility for the attack. The attackers said they stole 2 TB of data during the attack.

Unimicron Technology

Manufacturing, electronics

Denial of operations

Ransomware

According to a bulletin published in the Taiwan Stock Exchange portal, a China-based subsidiary of Taiwanese manufacturer of printed circuit boards and integrated circuit carriers Unimicron Technology Corp. was hit by a ransomware attack. The statement said that the incident occurred on January 30 and affected Unimicron Technology (Shenzhen) Corp. The company stated that the impact on its operations was limited and that it had engaged an external cyber forensics team to analyze the incident and help implement defense measures. Unimicron did not confirm a data breach. The Sarcoma ransomware group claimed responsibility for an attack on Unimicron in February and published samples of files allegedly stolen from the company's systems during the attack. The threat actors claimed to be holding 377 GB of database files and documents exfiltrated from the company. BleepingComputer reached out to Unimicron for an updated statement addressing Sarcoma's allegations, but there was no immediate response.

Astral Foods

Manufacturing, food and beverage

Denial of operations and services, financial losses

On March 16, South African poultry producer Astral Foods confirmed that it had suffered a cybersecurity incident. The attack caused downtime in the poultry processing division, which impacted deliveries to customers and resulted in a production backlog. Although the company swiftly implemented disaster recovery protocols, the temporary halt in operations resulted in financial losses. The Poultry Division was negatively impacted by the downtime in processing and deliveries to customers. This resulted in a loss of revenue and additional costs to catch up on the production backlog. No confidential information or sensitive data of customers, suppliers or individual stakeholders was compromised as a result of the cyber-intrusion.

Ganong Bros.

Manufacturing, food and beverage

Denial of operations

Ransomware

According to local media, Canadian candy manufacturer Ganong Bros. was hit by a ransomware attack. The company discovered the incident on February 22, 2025. Operations at the facility in St. Stephen were temporarily disrupted. Upon discovering the attack, Ganong Bros. immediately took countermeasures to protect its network and data. These measures included retaining third-party cybersecurity experts and external legal counsel to assist with containment and remediation and to conduct a forensic investigation to determine the extent of the incident. In particular, Ganong's investigation aimed to determine the extent to which any data, including personal information, may have been compromised. Ganong declined to comment on whether a ransom was demanded or paid. In March, the PLAY ransomware group claimed responsibility for the attack on Ganong Bros.

The attack, which lasted almost a year

Littleton Electric Light and Water Departments

Water supply, energy, utility

Data leakage

APT

Dragos published a report describing its work assisting the Littleton Electric Light & Water Department (LELWD), a public power utility, in combating the advanced threat group VOLTZITE, which had persistent access to LELWD's network. Since the start of 2023, VOLTZITE, a threat group identified by Dragos that overlaps with Volt Typhoon, has been responsible for the widespread compromise of industrial organizations across critical infrastructure sectors. Dragos found evidence of lateral movement by the hackers and data exfiltration. However, an investigation revealed that the compromised information did not include any sensitive customer data. The utility was also able to change its network architecture to remove any advantages for the adversary.

Dragos told SecurityWeek that the LELWD breach was discovered in November 2023. An investigation revealed that the hackers had been in the organization's network since February 2023, for more than 300 days. In the case of the LELWD power utility, the hackers were seen collecting data on OT systems. Dragos believes Volt Typhoon is one of several active threat groups capable of developing and testing "specific and meaningful attacks on ICS". They have also been observed exfiltrating geographic information system (GIS) data containing critical information about the spatial layout of energy systems in many cases outside of the LELWD hack.

Appendix. Full list of confirmed incidents

Victim	Industry / Profile	Country	Impact features	Date of notification / Date of incident (if known) / Suspected attackers
Garden of Life	Manufacturing / Dietary supplement manufacturer	USA	Personal data leakage	January 17, 2025 December 18, 2024
Avery Products	Manufacturing / Label and sticker manufacturer	USA	Personal data leakage Ransomware	January 13, 2025 July 18, 2024
Prodinger	Manufacturing / Packaging solution manufacturer	Germany	Data leakage, denial of IT services and product delivery Ransomware	January 21, 2025 December 6, 2024
All American Poly	Manufacturing / Blown film extrusion manufacturer	USA	Personal data leakage Ransomware	January 27, 2025 August 26, 2024 RansomHub
Mizuno USA	Manufacturing / Sports equipment and sportswear manufacturer	USA Japan	Personal data leakage Ransomware	January 30, 2025 August 21, 2024 BianLian
Flashforge	Manufacturing / 3D printer and filament manufacturer	China	Data leakage	January 20, 2025
Mayer Steel Pipe Corporation	Manufacturing / Steel pipe manufacturer	Taiwan	Denial of IT services	February 2, 2025
Fashion Box/Replay	Manufacturing / Textile manufacturer	Italy	Data leakage, personal data leakage	February, 2025 January 29, 2025
Natures Organics	Manufacturing / Environmentally conscious cleaning and personal care product manufacturer	Australia	Data leakage Ransomware	February 12, 2025 January 30, 2025 Medusa
Raymond Limited	Manufacturing / Fabric manufacturing and real estate company	India	Denial of IT systems Ransomware	February 19, 2025 RansomHub

GIGAFLIGHT Connectivity, Inc.	Manufacturing / Aerospace wire manufacturer	USA	Personal data leakage	January 29, 2025 May 20, 2024
Textiles Coated	Manufacturing / Textile manufacturer	USA	Denial of IT systems, personal data leakage	February 4, 2025 November 1, 2024
Mid-State Industrial	Manufacturing / Provider of manufacturing, repairing, designing, disassembling and transporting expertly designed equipment and machinery	USA	Personal data leakage Ransomware	February 11, 2025 January 23, 2025 Play
SMC Corporation of America	Manufacturing / Pneumatic control device manufacturer	USA Japan	Personal data leakage Ransomware	February 3, 2025 December 3, 2024 Qilin
Nuna Baby Essentials	Manufacturing / Baby product manufacturer	USA Netherlands	Personal data leakage	February 21, 2025 September 8, 2024
Daedong-USA	Manufacturing / Agricultural machinery manufacturer	USA	Personal data leakage	February 20, 2025 January 12, 2024
Racal Acoustics	Manufacturing / Headset manufacturer	UK	Denial of IT systems, personal data leakage Ransomware	February 24, 2025 May 2, 2024 RansomHub
Hartson-Kennedy	Manufacturing / Countertop manufacturer	USA	Personal data leakage Ransomware	February 20, 2025 June 24, 2024 Clop
Stiiizy	Manufacturing / Cannabis producing company	USA	Personal data leakage	January 8, 2025 October 10, 2024 Everest
McMillan Electric Company	Manufacturing / Electric motor maker	USA	Personal data leakage Ransomware	February 13, 2025 October 29, 2024 Medusa
McLanahan Corporation	Manufacturing / Engineering and manufacturing equipment provider	USA	Personal data leakage	February 28, 2025 February 23, 2024

Mity, Inc.	Manufacturing / Furniture manufacturer	USA	Personal data leakage Ransomware	January 27, 2025 March 6, 2024
JSP International Group	Manufacturing / Synthetic resin and plastic material manufacturer	USA Japan	Personal data leakage Ransomware	February 7, 2025 RansomHub
Commercial Specialty Truck Holdings	Manufacturing / Truck body and aftermarket part producer	USA	Personal data leakage	February 13, 2025
Big Green Egg	Manufacturing / Grill and cooking system manufacturer	USA	Personal data leakage Ransomware	February 4, 2025 July 26, 2024 RansomHub
Oceanside Glasstile Company	Manufacturing / Glass and tile manufacturer	USA	Personal data leakage Ransomware	February 12, 2025 August 15, 2024 RansomHub
Finn Corporation	Manufacturing / Landscaping equipment manufacturer	USA	Denial of IT systems, personal data leakage Ransomware	February 12, 2025 November 12, 2024 DragonForce
Fortis Solutions Group	Manufacturing / Packaging solutions	USA	Personal data leakage	February 18, 2025 January 5, 2024
Title 9 Sports	Manufacturing / Athletic clothing manufacturer	USA	Personal data leakage	February 21, 2025 November 2, 2024
Standard Calibrations	Manufacturing / Measurement products and services company	USA	Personal data leakage Ransomware	February 20, 2025 November 30, 2024 Play
QualiTech	Food & beverage, manufacturing / Plant nutrition, animal nutrition, and food ingredient product manufacturer	USA	Personal data leakage Ransomware	February 21, 2025 November 19, 2024 Lynx
Ålands Central-andelslag (Ålandsmejeriet and Ålandsbagarn)	Food and beverage, manufacturing / Dairy and bakery production	Finland	Denial of operations	March 6, 2025 March 5, 2025

Advanced Foam Recycling / Amalgamate Processing	Manufacturing / Foam supply company	USA	Personal data leakage	February 24, 2025 June 25, 2024
Suit-Kote Corporation	Manufacturing / Asphalt product manufacturer	USA	Denial of IT systems, personal data leakage Ransomware	February 26, 2025 October 16, 2024 Black Basta
Mark Dunning Industries	Utilities / Waste management	USA	Personal data leakage	February 7, 2025 November 7, 2023
Adval Tech Group	Manufacturing / Innovative plastic and metal component manufacturer	Switzerland	Denial of IT systems Ransomware	March 3, 2025 March 2, 2025 Lynx
Numotion	Manufacturing / Medical equipment manufacturer	USA	Personal data leakage	March 7, 2025 September 2, 2024
Keding Enterprises Co.	Manufacturing / Wood product manufacturing company	Taiwan	Denial of IT systems	March 17, 2025
Johnson Health Tech	Manufacturing / Fitness and wellness product manufacturer	Taiwan	Ransomware	March 25, 2025 CrazyHunter
Sheng Yu Steel	Manufacturing / Steel product manufacturer	Taiwan	Denial of IT systems Ransomware	March 30, 2025 Underground
Brucha	Manufacturing / Insulated panel manufacturer	Austria	Denial of IT systems Ransomware	March 7, 2025 March 3, 2025
Troxler Electronic Laboratories	Manufacturing / Testing/quality control measurement equipment manufacturer	USA	Personal data leakage Ransomware	December 30, 2024 October 29, 2024 RansomHub
National Presto Industries	Manufacturing / Consumer product manufacturer and defense company	USA	Denial of operations, services and IT systems, data leakage Ransomware	March 1, 2025 InterLock

Marposs	Manufacturing / Producer of measurement and control systems for the manufacturing industry	Italy	Denial of operations and services Ransomware	January 28, 2025 January 26, 2025
Crystal D	Manufacturing / Manufacturer of crystal awards and gifts	USA	Denial of operations and services Ransomware	March 7, 2025 LockBit
Fabricaciones Militares Sociedad del Estado	Manufacturing / Military manufacturer	Argentina	Denial of operations and services, data leakage Ransomware	March 3, 2025 Monti
Imaflex	Manufacturing / Manufacturer of solutions for the flexible packaging space, polyethylene (plastic) film and bags	Canada	Denial of operations, denial of IT systems, personal data leakage	February 21, 2025 February 17, 2025
Prime Technological Services	Electronics, manufacturing / Electronics manufacturing service provider	USA	Personal data leakage	January 2025
Nan Ya Printed Circuit Board Corporation	Electronics, manufacturing / Circuit board manufacturer	Taiwan	Denial of IT systems	February 2, 2025
Unimicron Technology	Electronics, manufacturing / Circuit board manufacturer	Taiwan	Ransomware	January 30, 2025 Sarcoma
Transcend Information	Electronics, manufacturing / Storage, multimedia and industrial product manufacturer	Taiwan	Denial of IT systems Ransomware	February 7, 2025 RansomHub
Fortune Electric	Energy, manufacturing / Power transformer and	Taiwan	Denial of IT systems Ransomware	February 8, 2025 Lynx

	switchgear manufacturer			
Unikorn Semiconductor Corporation	Electronics, manufacturing / Semiconductor foundry	Taiwan	Unknown	March 4, 2025
Smiths Group	Construction and engineering / General industrial, safety and security, energy, and aerospace market contactor	UK	Denial of IT systems	January 28, 2025
Tata Technologies	Construction and engineering / Automotive, aerospace, industrial heavy machinery	India	Denial of IT services Ransomware	January 31, 2025
Edw. C. Levy	Construction and engineering / Concrete and asphalt manufacturer	USA	Denial of IT systems, personal data leakage Ransomware	January 16, 2025 October 29, 2023
InterCon Construction	Energy, construction / Oil and gas pipelines, facility management, horizontal directional drilling, overhead and electric services, telecommunications, utility design work	USA	Personal data leakage Ransomware	January 30, 2025 November 9, 2024 Hunters International
Argenio Bros.	Construction and engineering / Highway and street construction	USA	Personal data leakage	January 23, 2025 October 28, 2024
KMB Design Group	Construction and engineering / Telecommunications engineering, traditional civil,	USA	Personal data leakage Ransomware	January 28, 2025 December 30, 2024 BlackBasta

	mechanical, electrical, environmental, structural, solar, energy engineering services, fielding and construction management services			
O'Connor Corporation	Construction and engineering / Industrial, mechanical, and safety construction services	USA	Denial of IT systems, personal data leakage	January 31, 2025 November 23, 2024
James H. Maloy	Construction and engineering / Heavy highway and site development contractor	USA	Denial of IT systems, personal data leakage Ransomware	January 30, 2025 November 5, 2024 Akira
IMI	Construction and engineering / Precision fluid engineering	UK	Unknown	February 6, 2025
Lighthouse Electric Company	Construction and engineering / Electrical construction and maintenance service contractor	USA	Personal data leakage Ransomware	February 4, 2025 October 21, 2024 RansomHub
Canyon State Electric	Construction and engineering / Provider of commercial electric contracting services	USA	Personal data leakage	February 7, 2025 January 8, 2025
Nijhuis Bouw BV	Construction and engineering / Housing complex, industrial building, shopping mall, apartment, and	Netherlands	Personal data leakage Ransomware	February 28, 2025

	warehouse developer			
Trident Maritime Systems	Construction and engineering / Engineering solutions in marine interiors, distributed ship systems, electro-mechanical solutions, and automation and control	USA	Personal data leakage	February 17, 2025 February 1, 2023
American Plumbing & Heating Corporation	Manufacturing / Plumbing manufacturer	USA	Denial of IT systems, personal data leakage Ransomware	February 4, 2025 December 17, 2024 RansomHub
Yazoo Valley Electric Power Association	Utility / Electrical power and maintenance services provider	USA	Personal data leakage Ransomware	January 30, 2025 August 23, 2024 Akira
Stadtwerke Schwerte	Utility / Gas, water and electricity provider	Germany	Denial of IT systems, denial of IT services	March 5, 2025
Edesur Dominicana	Utility / Electricity provider	Dominican Republic	Ransomware	March 13, 2025 March 11, 2025 Hunters International
Water and Sewerage Corporation	Utility / Sanitation and water treatment company	Bahamas	Ransomware	March 21, 2025
AMA S.p.A. (Azienda Municipale Ambiente)	Utility / Environment management solution provider	Italy	Denial of IT services	March 24, 2025
Littleton Electric Light & Water Department	Utility / Water and electricity provider	USA	Data leakage	March 12, 2025
Clutch Industries	Automotive, manufacturing / Automotive clutch system manufacturer	Australia	Data leakage Ransomware	January 21, 2025 Lynx
Port of Ostend	Logistics and transportation	Belgium	Denial of IT systems and services	February 11, 2025 February 10, 2025

Biagi Bros.	Logistics and transportation / 3PL, warehousing, and trucking solution provider	USA	Personal data leakage Ransomware	February 25, 2025 December 31, 2024 Cactus
Anellotech	Chemicals, manufacturing / Sustainable chemical manufacturer	USA	Personal data leakage Ransomware	February 26, 2025 December 24, 2024
NioCorp Developments	Mining, manufacturing / Critical mineral development	USA	Misdirected vendor payments	February 14, 2025
Galliker's Dairy Company	Food and beverage, manufacturing / Dairy product producer	USA	Personal data leakage	February 2025 June 23, 2024
Boart Longyear Group	Mining, manufacturing / Provider of drilling services, drilling equipment, and performance tooling for mining and drilling companies	USA	Personal data leakage Ransomware	March 6, 2025 June 29, 2024 Dark Angels
Bavaria Sausage	Food and beverage, manufacturing / Sausage and meat product manufacturer	USA	Personal data leakage	March 3, 2025 April 6, 2024
Purecoat North / Purecoat International	Manufacturing / Provider of application coating services utilized by the aerospace, electronics, transportation and microwave industries	USA	Personal data leakage	March 4, 2025 November 19, 2024
Pocket Nurse	Manufacturing / Manufacturer	USA	Personal data leakage	March 3, 2025

	and distributor of medical supplies and equipment for simulation and healthcare education			
Jonti-Craft	Manufacturing / Furniture manufacturer	USA	Personal data leakage Ransomware	March 5, 2025 October 18, 2024 BlackBasta
Engine Power Source	Manufacturing / Industrial engine distributor	USA	Personal data leakage Ransomware	March 6, 2025 January 1, 2025 Lynx
TERREPOWER	Automotive, manufacturing / Auto part manufacturer	USA	Personal data leakage	March 7,2025 December 12, 2024
Erickson Companies	Manufacturing, construction / Framing system manufacturer	USA	Personal data leakage	March 12, 2025 November 16, 2024
Trinity Petroleum Management	Energy, construction / Oil and gas service provider	USA	Personal data leakage Ransomware	February 13, 2025 October 10, 2024 BianLian
IKAV Energy	Energy / Exploration and production energy company	USA	Personal data leakage Ransomware	March 13, 2025 DragonForce
OBI	Food and beverage, manufacturing / Fresh, frozen and canned wild Alaska seafood producer	USA	Personal data leakage	March 11, 2025 August 12, 2024
F.tech R&D North America	Manufacturing / Chassis system manufacturer for the automotive industry	USA	Personal data leakage Ransomware	March 7, 2025 Qilin
Connecticut Container Corporation / Unicorr Packaging Group	Manufacturing / Manufacturer of custom corrugated products and protective packaging	USA	Personal data leakage Ransomware	March 11, 2025 January 26, 2025 Akira

Grede Holdings	Manufacturing / Manufacturer of high-quality ductile, gray, and specialty iron castings for the mobility industry	USA	Denial of IT systems, personal data leakage Ransomware	March 5, 2025 January 27, 2025 Cactus
Topy America	Automotive, manufacturing / Steel wheel manufacturer for a variety of automotive manufacturers	USA	Personal data leakage	March, 2025 December 8, 2024
Mark Thomas	Construction and engineering / Planning, design and construction management of municipal infrastructure	USA	Personal data leakage	March 17, 2025 October 11, 2024
Leisure Time Products / Backyard Discovery	Manufacturing / Wooden outdoor playset manufacturer	USA	Personal data leakage Ransomware	March 17, 2025 October 31, 2024 Clop/ EMBARGO
Geokon	Manufacturing / Geotechnical and structural instrumentation manufacturer	USA	Personal data leakage Ransomware	March 19, 2025 January 30, 2025 Lynx
Great Western Drilling Company	Energy / Production and acquisition of oil and gas	USA	Personal data leakage	March 20, 2025
Fireproof Contractors	Construction and engineering / Fireproofing, thermal and acoustical insulation, waterproofing, and firestop service	USA	Personal data leakage Ransomware	March 24, 2025 Nitrogen
Strauss Brands	Food and beverage, manufacturing / Grass-fed beef manufacturer	USA	Personal data leakage Ransomware	March 19, 2025 Medusa

Astral Foods	Food and beverage, manufacturing / Poultry producer	South Africa	Denial of operations and services, financial losses	March 24, 2025 March 16, 2025
Ganong Bros.	Food and beverage, manufacturing / Candy manufacturer	Canada	Denial of operations Ransomware	March 14, 2025 February 22, 2025 Play
CSG Consultants	Construction and engineering / Building, engineering and construction management service provider	USA	Personal data leakage Ransomware	March 20, 2025 August 2024 Akira
Sunnking Electronics Recycling	Electronics / Free and convenient electronics recycling	USA	Personal data leakage	March 28, 2025 February 5, 2025
Plaisted Companies	Manufacturing, construction / Construction and landscaping material manufacturer	USA	Denial of IT systems, personal data leakage Ransomware	March 26, 2025 September 2024 Play
Smiths Interconnect and Smiths Interconnect Americas	Electronics, manufacturing / Manufacturer of electronic components, microwave, optical and radio frequency products and sub-systems	USA UK	Personal data leakage	March 27, 2025 January 23, 2025
Mission Bell Mfg	Manufacturing, construction / Custom architectural millwork and casework manufacturer	USA	Personal data leakage	March 20, 2025 January 31, 2025
Power Test Industries	Manufacturing / Dynamometers and heavy equipment	USA	Denial of IT systems, personal data leakage Ransomware	March 3, 2025 April 29, 2024 LockBit

	testing system manufacturer			
Continental Aerospace Technologies	Manufacturing / Aircraft engine manufacturer	USA	Denial of IT systems, personal data leakage	March 13, 2025 February 12, 2024
Champion Home Builders	Construction and engineering / Modular homebuilder	USA	Personal data leakage Ransomware	March 31, 2025 January 16, 2025 Clop
Cardo Systems	Electronics, manufacturing / Manufacturer of communication devices for groups in motion	Israel	Personal data leakage	March 14, 2025 January 28, 2025
Lane Automotive	Automotive, manufacturing / Steel wheel manufacturer for a variety of automotive manufacturers	USA	Personal data leakage	March 12, 2025 March 23, 2023
Eckert & Ziegler Isotope Products	Manufacturing / Supplier of radioactive isotopes and related products for medical and industrial applications	USA	Personal data leakage	March 6, 2025 February 2, 2025
Eckert & Ziegler SE	Manufacturing / Supplier of radioactive isotopes and related products for medical and industrial applications	Germany	Denial of IT systems	February 13, 2025
OEC Freight Companies	Logistics and transportation / Freight forwarding and logistics services	USA	Personal data leakage	March 14, 2025 May 13, 2024
Vorwerk	Manufacturing / Kitchen appliance manufacturer	Germany	Personal data leakage	February 7, 2025

Hofmann Fördertechnik	Logistics and transportation / Intralogistics service provider	Germany	Denial of IT systems and services	March 31, 2025 Hunters International
Kuala Lumpur International Airport	Logistics and transportation	Malaysia	Denial of operations and services Ransomware	March 25, 2025 March 23, 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