Kaspersky ICS CERT

kaspersky

A brief overview of the main incidents in industrial cybersecurity Q3 2025

18.12.2025

Version 1.0

Contents

In Q3 2025, 129 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

The third quarter of 2025 was marked by several major incidents, some of which rank among the largest and most significant of the past couple of years. Perhaps most notably, all of them occurred in just one sector – transportation and logistics.

A ransomware attack on Jaguar Land Rover resulted in a five-week production shutdown, causing direct losses estimated at tens of millions of dollars and forcing the company to take out additional loans totaling $4.69 billion from the government and commercial banks. Several JLR suppliers were forced to file for bankruptcy as a result of the incident. According to estimates by the UK's Cyber Monitoring Centre (CMC), the attack impacted approximately 5,000 UK organizations, resulting in losses to the UK economy of $2.5 billion. The damage to the global automotive sector and the overall impact on the global economy still need to be assessed.

A ransomware attack on Collins Aerospace's ARINC cMUSE online check-in platform disrupted operations at several major European airports, further demonstrating the air transportation sector's vulnerability to supply chain attacks.

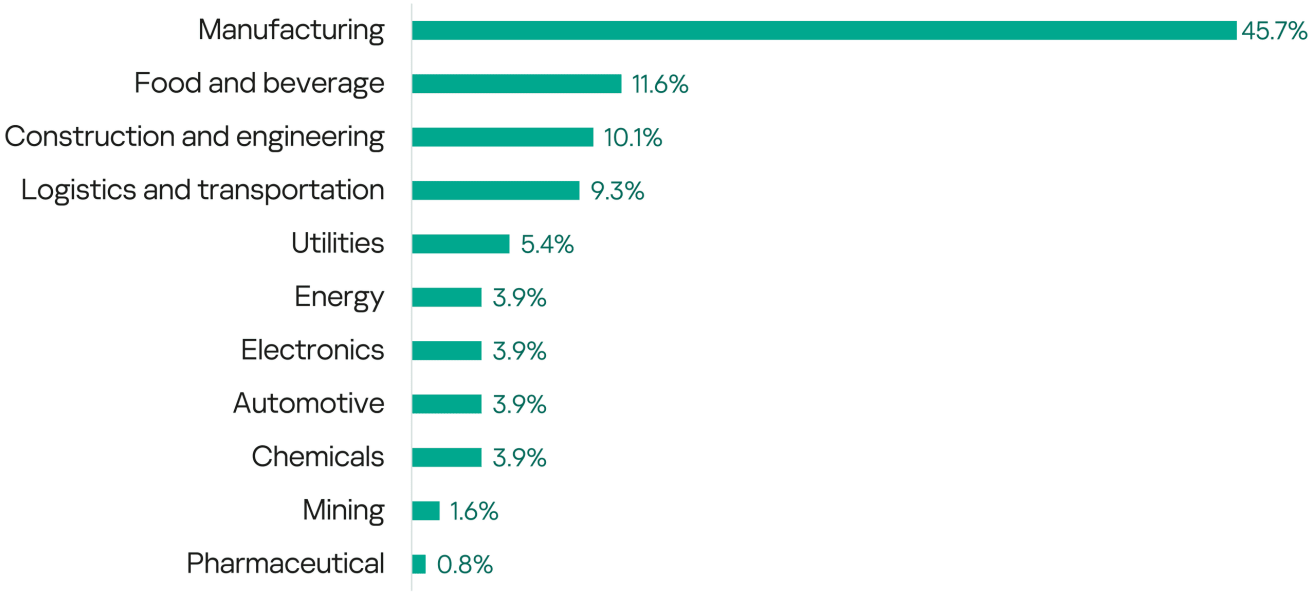
Aeroflot, Russia's largest airline, also fell victim to hackers. Numerous flights were cancelled following a hacktivist attack on the airline's systems.

Four more air transportation companies – Air France, KLM, Air Serbia, and Qantas – as well as Rhode Island Airport, reported cyberattacks resulting in the theft of confidential data.

The list of casualties in the transportation sector doesn't end there. Two automotive giants, Stellantis and Bridgestone, as well as several smaller organizations, also reported incidents.

Pakistan Petroleum Limited suffered a ransomware attack that impacted the continuity of its financial operations. Similar incidents should be expected in Asia in the near future.

And according to Poland's deputy prime minister, the country may have experienced a cybersecurity incident where the threat of a "major city" being left without water was allegedly prevented. We hope further details of the incident, including the technical aspects, will soon be made publicly available.



July — August — September — 2025

- Rhode Island Airport Corporation
- JCI Jones Chemicals
- Qantas
- Hero España
- Farmer's Rice Cooperative
- Louis Vuitton
- Surmodics
- HEXPOL Compounding Americas
- HEIM & HAUS
- Control Module
- EIZO Rugged Solutions
- SEMCO Technologies
- AzureWave Technologies
- Artivion
- NPK Construction Equipment
- Wibaie
- American Welding
- Tri State Electric
- GMK Associates
- FLOE International
- Dosatron International
- Vero Foods
- Mesa Natural Gas Solutions
- Ergonomic Products
- Berridge Manufacturing Company
- American Cord & Webbing
- Versa Designed Surfaces
- Novabev Group
- Delfingen
- Air Serbia
- BARTEC
- Birdsong Peanuts
- Safe Fleet Holdings
- Top Hydraulic
- Keystone Shipping
- Massachusetts Municipal Wholesale Electric Company
- King Industries
- Sauers Lopez Construction
- Tower Manufacturing Corporation
- Serviço Autônomo de Água e Esgoto de Barretos
- Distinctive Surfaces of Florida
- Certis USA LLC (Certis Biologicals)
- Lithium Nevada / Lithium Americas Corp.
- Lollytogs (LT Apparel Group)
- Exel Composites
- Baillie Lumber
- Aeroflot
- Vest Tube
- TIMEC Oil & Gas
- Kibernetik AG

- Vaquero Underground Services
- Chanel
- PAC Strapping Products
- Pandora
- Episciences (Epionce)
- Air France and KLM
- Pakistan Petroleum Limited
- Old Dutch Foods
- Shinn Fu Company of America
- LBX Company
- Cate Equipment Company
- ENGIE Power & Gas
- Rohtstein Corporation
- Polish water supply
- Lumitex
- Brookshire Grocery Company
- City of Wichita Falls Cypress Water Treatment Facility
- Peter Pauper Press
- The Seydel Companies
- BB Diversified Services
- Data I/O Corporation
- KNH Enterprise
- The Hiller Companies
- Sun Pacific Solar Electric
- Maryland Transit Administration
- Util-Assist
- NHB Holdings
- Lasership / OnTrac Final Mile
- Gorham Sand & Gravel
- MoboTrex
- Antonio Sofo & Sons Importing Co / Sofo Foods

- Jaguar Land Rover
- Bridgestone Americas
- Sunsweet Growers
- The LoveSac Company
- Cornwell Quality Tools
- Talisman civil consultants
- Champagne Logistics
- Minaris Advanced Therapies
- Transart Graphics
- Farmer Brothers
- Phoenix Mechanical Contracting
- G&H Wire Company (G&H Orthodontics)
- Channel Fish
- Sellmark Corporation
- NPK International
- Phoenix Products
- Miller Construction
- Gale Associates
- ENCON Heating & Air Conditioning
- Boliden / Miljödata
- MGM Transformers
- Chroma ATE
- Monterey Mushrooms
- CSJB Holdings
- National Molding
- Havco Wood Products
- Minsait ACS
- Hello Cake
- PCE Constructors
- Morrisroe
- Collins Aerospace (Heathrow, Berlin, Brussels and Dublin airports)
- Stellantis
- Carus
- Thermofin
- All States Materials Group
- Tekni-Plex
- Volvo Group North America
- Braun Electric Company
- Dulany Industries
- Okuma Europe
- Refresco
- Georgetown Brewing Company
- T.R.A. Industries Inc. / Huntwood Industries
- Thai Diamond & Zebra Electric
- Belkorp Ag
- Karndean Designflooring
- LG Balakrishnan & Bros
- Kering S.A.

Attacks leading to denial of operations

Heim & Haus

Manufacturing

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

Ransomware

German building element manufacturer Heim & Haus was the target of a cyberattack in which parts of its IT systems were encrypted. The company immediately started working closely with IT forensics experts to restore the systems fully and in accordance with the Federal Office for Information Security's (BSI) requirements. According to a July 6 website update, production returned to full capacity and was running stably. Direct sales, assembly and customer service was fully operational nationwide. According to a website update from July 10, the company restored its communication channels by phone and email. Heim & Haus customer portal was available again, but restrictions or delays were still possible in the processing of individual inquiries and orders. The investigation revealed that, in addition to encrypting the systems, the attackers compromised personal data. The Kawa4096 ransomware group claimed responsibility for the July attack on Heim & Haus.

Hero España

Manufacturing

Denial of operations and services

Spanish food manufacturer Hero España announced that its computer systems were targeted by an external cyberattack on June 30, causing a temporary disruption to the functionality of its facility in Alcantarilla, Murcia. The attack temporarily restricted the company's production and logistics operations in Spain. Company sources confirmed that the incident only impacted Hero's local operations in Spain, without affecting other Hero Group divisions globally. According to company representatives, as an immediate response, the company carried out a controlled shutdown of the compromised systems to prevent the attack from spreading and to protect data. A team of cybersecurity and forensic analysis specialists, both internal and external, was set up to investigate the causes of the attack and facilitate the safe recovery of the systems.

Wibaie

Manufacturing

Denial of operations

Ransomware

Wibaie, a French manufacturer of windows and doors, suffered a cyberattack on the night of July 9-10, 2025, which led to a complete shutdown of the factory from July 10. The company's communications manager confirmed the attack to local media. Wibaie worked with experts to resolve the problem. Approximately 600 employees were unable to work because of the attack. The Qilin ransomware group claimed responsibility for the attack on Wibaie.

Novabev Group

Manufacturing

Denial of IT systems, operations and services

Ransomware

Russian liquor producer Novabev Group was the victim of a cyberattack on July 14 that temporarily disrupted part of its IT infrastructure, according to an official statement. The attack affected the availability of some services and tools of its subsidiary WineLab group, as well as its network. The attackers demanded a ransom, but the company refused to give in to their demands. Although the company's operations, including those of WineLab, were affected, customers' personal data did not appear to have been compromised. At the time of the announcement, the WineLab website was unavailable. The internal IT team worked around the clock to resolve the situation. To speed up the process, external experts were involved in the investigation.

Aeroflot

Transportation, logistics

Denial of IT systems, operations and services

On July 28, Russian airline Aeroflot experienced disruptions to its IT systems due to a cyberattack. As a result, the airline was forced to cancel flights and warned of potential disruptions to services. The Russian Prosecutor General's Office confirmed that the failure of the Aeroflot IT system was caused by a hacker attack and a criminal case was opened into the unauthorized access to information. Two hacker groups, Cyber-Partisans and Silent Crow, announced on July 28 that they had conducted an attack on Aeroflot. In their statements, Silent Crow and Cyber-Partisans said the cyberattack was the result of a year-long operation that had deeply penetrated Aeroflot's network, destroyed 7000 servers and gained control over employees' personal computers, including those of senior managers.

Pakistan Petroleum Limited

Energy

Denial of IT systems and operations, personal data leakage

Ransomware

Pakistani oil and gas company Pakistan Petroleum Limited (PPL) fell victim to a major ransomware cyberattack. According to Pakistan Today, hackers operating under the alias Blue Locker encrypted PPL's servers, blocked access to backups, and demanded a ransom. The company's entire financial system was brought to a standstill, as operations remained suspended. Sources said the encrypted systems included virtual machines and financial servers. The attackers claimed to have exfiltrated vital data related to operations, contracts, and employee information. In an official statement, PPL commented that the event was detected on August 6 and that the IT and cybersecurity teams, in collaboration with external experts, took prompt containment measures, including temporarily suspending select non-critical IT services. Core operational systems remained unaffected, and the company's joint venture partners and external stakeholders

continued to operate without disruption. There was no indication that business-critical or sensitive data had been compromised.

Pakistan's National Cyber Emergency Response Team issued a high-alert advisory, warning of severe risks from the Blue Locker ransomware, stating that it had compromised critical infrastructure, including Pakistan Petroleum Limited. Resecurity acquired binary samples of the Blue Locker and conducted a reverse engineering analysis. Linked to the Proton family variants like Shinra, the ransomware employs AES-RSA encryption, privilege escalation via registry modifications, and defense evasion through obfuscation and timestomping. Hackmanac stated that the threat actor yyy32111 claimed to have breached PPL, exfiltrating 1 TB of sensitive data in a leak dated August 1, 2025.

KNH Enterprise

Manufacturing

Denial of IT systems and operations

According to a bulletin from the Taiwan Stock Exchange portal published on August 24, Taiwanese nonwoven specialty manufacturer KNH Enterprise suffered a cyberattack. The bulletin stated that some of the group's information systems and its overseas subsidiaries were subjected to a hacker attack. The affected systems were progressively restored. According to assessments, there was no significant impact on the group's operations. The group engaged an internationally recognized cybersecurity firm to help resolve the incident. Following the incident, the company said it would continue to enhance network and IT infrastructure security controls.

Data I/O Corporation

Electronics, manufacturing

Denial of IT systems, operations and services

Ransomware

Data I/O Corporation, a US manufacturer of manual and automated security provisioning and device programming systems for flash, microcontroller and logic devices, reported an incident in a Form 8-K filing with the United States Securities and Exchange Commission on August 21. On August 16, Data I/O Corporation experienced a ransomware incident that affected certain internal IT systems. Upon discovery, the company proactively took certain platforms offline and implemented other mitigation measures. The company also engaged leading cybersecurity experts to support IT system recovery and conduct a thorough investigation. The incident temporarily impacted the company's operations, including internal and external communications, shipping, receiving, manufacturing production, and various other support functions. Although the company had restored some operational functions, the timeline for a full restoration was not known. As of the filing date, the incident did not appear to have had a material impact on the company's business operations. However, the expected costs related to the incident – including fees for cybersecurity experts and other advisors, as well as costs to restore impacted systems – were

reasonably likely to have a material impact on the company's results of operations and financial condition.

Chroma ATE

Electronics, manufacturing

Denial of IT systems and operations

Ransomware

Taiwanese manufacturer of electronic test and measurement instruments Chroma ATE suffered a cyberattack, according to a bulletin from the Taiwan Stock Exchange portal published on September 17. The company's information systems were attacked. The security team cooperated with external IT professionals to address the issue. According to the bulletin, no personal information, confidential documents or important data was leaked. The attack did not significantly impact Chroma ATE's operations. The company continuously examined and strengthened the security control of its network and information infrastructure. The Warlock ransomware group claimed responsibility for the September attack on Chroma ATE.

Thermofin

Manufacturing

Denial of operations and services, personal data leakage

Ransomware

German heat exchanger manufacturer Thermofin fell victim to a cyberattack, according to a statement on its website. Subsidiaries in China and Poland were also affected. The perpetrators gained unauthorized access to the company's IT systems and stole personal data, among other things. The following types of data may have been stolen: names, addresses, contact details, and bank account information. The company worked intensively to determine the exact scope of the attack. In accordance with Article 34 of the General Data Protection Regulation (GDPR), Thermofin informed the affected individuals. According to a local press report, the company had limited access via a hotline and struggled to maintain production as its operations were limited. The Sarcoma ransomware group claimed responsibility for the attack on Thermofin in September.

Refresco

Food and beverage, manufacturing

Denial of operations and services

On September 22, beverage manufacturer Refresco suffered a cyberattack that disrupted its production activities in Germany, affecting production systems and the inflow and outflow of goods. While working to restore normal operations, the company continued to accept customer orders via email. Further details of the incident were not confirmed, including the type of attack or the data compromised, while investigations were ongoing.

Major impact prevented by responders

Polish water supply

Utilities, water supply

Denial of operations

On August 14, Deputy Prime Minister of Poland and Minister of Digital Affairs Krzysztof Gawkowski confirmed to the Onet.pl news portal that an attack on an unnamed water and sewage infrastructure of a large Polish city had occurred on August 13. Gawkowski said the attack could have left one of the country's major cities without water, but it was prevented. The relevant services learned about the attack at the last minute and managed to shut everything down.

Incidents at large organizations

Jaguar Land Rover

Automotive, manufacturing

Denial of IT systems, operations and services, bankruptcy

Ransomware

Jaguar Land Rover (JLR), the British multinational automobile manufacturer owned by Tata Motors, confirmed a major IT security incident affecting its global business operations. The company first disclosed the breach in a regulatory filing to Indian stock exchanges on September 1, stating that it was working at pace to resolve global IT issues impacting its business. On September 2, JLR issued a statement on its website saying the company took immediate action to mitigate the impact of the incident by proactively shutting down systems. According to the September 2 statement, there was no evidence any customer data had been stolen, though retail and production activities were severely disrupted.

The first reports of severe disruptions to JLR operations came from dealers in the UK that were unable to register new cars or supply parts at service points. Responding to media queries, JLR stated that an attack had occurred over the weekend of August 30-31, which forced it to shut down several systems, including those used at the Solihull production plant. The Liverpool Echo reported that workers at the company's Halewood plant in Merseyside were told on the morning of September 1 not to go to work following the incident. The JLR attack also affected the company's suppliers. According to the BBC, several small suppliers to Jaguar Land Rover faced bankruptcy due to the prolonged shutdown. They were forced to suspend their own operations and send employees on leave. German company Eberspächer Gruppe GmbH & Co., which makes exhaust systems for JLR, was forced to suspend production at its Nitra plant in Slovakia after the cyberattack. Slovakian company Hollen, which ensures the quality of car parts, implemented restrictions because of the JLR shutdown, according to its CEO. At a meeting with the government's Business and Trade Committee on September 25, 10 companies within the supply chain voiced

concerns about their prospects, as some of them had just seven to 10 days of funds remaining.

On September 10, the company issued a statement saying that some data had been affected and that it had informed the relevant regulators. On September 27, the British government pledged a $2 billion loan guarantee to support JLR's supply chain in the wake of the production shutdown caused by the attack. The Financial Times reported on September 29 that JLR had also secured a new $2.69 billion funding facility from commercial banks, separate from the government's loan guarantee, citing individuals with knowledge of the discussions.

According to current estimates by the UK's Cyber Monitoring Centre (CMC), the attack on JLR impacted approximately 5,000 UK organizations, causing a total loss to the UK economy of $2.5 billion. The damage to the global automotive sector and the overall impact on the global economy is yet to be assessed.

On September 29, the company informed colleagues, retailers and suppliers that it would resume some sections of manufacturing operations in the coming days. JLR continued to work around the clock alongside cybersecurity specialists, the UK Government's NCSC, and law enforcement to ensure a safe and secure restart.

Production restarted by October 8, following a phased approach. Based on JLR's published financial results, the cyberattack created a significant dent in its profits. "Loss before tax and exceptional items was £485m for Q2 and £134m for H1, down from a profit of £398m and £1.1bn respectively a year ago," the company stated. The company went to state that one of the main factors behind the decrease in profitability was the cyberattack.

In early September, a group calling itself Scattered Lapsus$ Hunters, a loose coalition of hackers linked to three different groups, Scattered Spider, Lapsus$ and ShinyHunters, took credit for the breach of JLR in posts on the social media platform Telegram. The hackers published images depicting internal JLR systems and vehicle documentation, saying they had gained access after exploiting a vulnerability in a technology platform called SAP NetWeaver (CVE-2025-31324).

Stellantis

Automotive, manufacturing

Personal data leakage

Extortion

On September 21, Stellantis, a multinational automobile manufacturer headquartered in the Netherlands, announced a data leak. The company detected unauthorized access to a platform of a third-party service provider that supports its North American customer service operations. The personal data involved was limited to contact information. Upon discovery of the breach,

Stellantis immediately activated its incident response protocols, notified the relevant authorities and directly informed affected customers.

BleepingComputer learned that the attack was part of a recent wave of Salesforce data breaches linked to the ShinyHunters extortion group that affected numerous high-profile companies. On September 22, ShinyHunters claimed responsibility for the Stellantis data breach and informed BleepingComputer that they had stolen over 18 million Salesforce records, including names and contact details from the company's instance of the platform.

Bridgestone Americas hit by cyberattack

Manufacturing

Denial of operations

On September 2, Bridgestone Americas, the North American division of the Japanese tire manufacturer Bridgestone Corporation, confirmed an incident affecting two Bridgestone Americas manufacturing facilities in Aiken County, South Carolina. The following day, a Canadian media outlet reported similar disruptions at a BSA manufacturing facility in Joliette, Quebec. The mayor of Joliette, who said he spoke directly with Bridgestone executives, told the Canadian media outlet that the cyber incident had most likely affected all factories in North America. The company conducted a full investigation. Bridgestone Americas noted that its rapid response enabled it to contain the attack in its early stages, thereby preventing the theft of customer data and further penetration of the network. Specialists worked around the clock to minimize supply chain disruptions that could have led to product shortages.

Collins Aerospace

Transportation, logistics, aerospace, military defense

Denial of IT systems, operations and services, supply chain/trusted partner

Ransomware

A ransomware attack disrupted operations at several major European airports, including Heathrow, Berlin, Brussels and Dublin, causing delays. The attack, discovered on September 19, targeted ARINC cMUSE automatic check-in and boarding software provided by Collins Aerospace, a US software company owned by major defense conglomerate RTX. Airlines using the software were forced to use manual workarounds to board and check in passengers, resulting in several flights being delayed or canceled. The European Union Agency for Cybersecurity (ENISA) confirmed that the incident was a ransomware attack.

On September 20, Collins Aerospace released a statement saying that it was in the final stages of completing necessary software updates. According to a Heathrow memo seen by the BBC, after discovering the attack, Collins Aerospace initially rebuilt and relaunched its systems, only to find the hackers had maintained access. The memo also reportedly estimated that over a thousand Heathrow computers would have to be restored manually. Collins

Aerospace reportedly advised airlines not to turn off computers or log out of the Muse software if they were logged in.

A spokesperson for the National Cyber Security Centre said on September 20 that it was working with Collins Aerospace, the affected UK airports, the Department for Transport and law enforcement to understand the full impact of the incident. A man was arrested in the UK as part of an investigation into the incident. On September 24, RTX Corporation confirmed in a filing with federal regulators that ransomware was used in the hack of its airline passenger processing software. According to an SEC filing, the company said the attack was not expected to have a material impact on financial results.

Appendix. Full list of confirmed incidents

Victim	Industry / Profile	Country	Impact features	Date of notification Date of incident (if known) Suspected attackers
Rhode Island Airport Corporation	Logistics and transportation / Airport	USA	Personal data leakage	July 1, 2025 May 14, 2025
HEXPOL Compounding Americas	Manufacturing / Polymer compounding and manufacturer	USA	Personal data leakage Ransomware	July 3, 2025 December 22, 2024 Qilin
JCI Jones Chemicals	Chemicals, manufacturing / Water treatment chemicals manufacturer	USA	Personal data leakage	July 1, 2025 June 9, 2025
Dosatron International	Manufacturing / Manufacturer of water-powered dosing and mixing equipment	USA	Personal data leakage	July 14, 2025 March 4, 2025
Artivion	Manufacturing / Medical device manufacturer	USA	Personal data leakage	July 9, 2025 November 20, 2024

Ergonomic Products	Manufacturing / Dental equipment manufacturer	USA	Personal data leakage	July 15, 2025 October 2, 2024
Vero Foods	Food and beverage, manufacturing / Food producer	USA	Personal data leakage	July 14, 2025 December 2, 2024
Keystone Shipping	Logistics and transportation / Marine transportation company	USA	Personal data leakage Ransomware	July 21, 2025 June 3, 2025 Akira
Massachusetts Municipal Wholesale Electric Company	Utilities / Electricity provider	USA	Personal data leakage Ransomware	July 21, 2025 January 25, 2025 BlackSuit
Birdsong Peanuts	Food and beverage, manufacturing / Peanut processing	USA	Personal data leakage	July 18, 2025 June 23, 2025
Safe Fleet Holdings	Manufacturing / Manufacturer of safety solutions	USA	Personal data leakage	July 18, 2025 April 12, 2024
Top Hydraulic	Manufacturing / Hydraulic component manufacturer	USA	Personal data leakage	July 18, 2025 July 11, 2025
American Welding	Manufacturing / Manufacturer and distributor of industrial gases	USA	Personal data leakage	July 11, 2025
Tri State Electric	Construction and engineering / Installation of electrical roadway utilities, fiber optic, microwave vehicle detection systems	USA	Personal data leakage Ransomware	July 11, 2025 RansomHouse

NPK Construction Equipment	Manufacturing / Manufacturer of top mounting brackets, hydraulic hammer brackets, plate compactors, sheet pile drivers, pedestal boom systems, hard car unloaders, material handling systems	USA	Personal data leakage Ransomware	July 10, 2025 Worldleaks
Berridge Manufacturing Company	Manufacturing / Manufacturer of architectural sheet metal products, painted coil and flat sheet, portable roll formers	USA	Personal data leakage Ransomware	July 15, 2025 Brain Cipher
Mesa Natural Gas Solutions	Energy, manufacturing / Engineering, manufacturing and operations of power technology including natural gas and liquid propane-powered generator sets and microgrids	USA	Personal data leakage	July 14, 2025
GMK Associates	Construction and engineering / Provider of architecture, engineering, construction, and design-build services	USA	Personal data leakage	July 11, 2025
King Industries	Chemicals, manufacturing / Chemical manufacturing company	USA	Personal data leakage Ransomware	July 21, 2025 Akira
Distinctive Surfaces of Florida	Manufacturing / Countertop manufacturer	USA	Personal data leakage	July 23, 2025 April 1, 2025

Certis USA LLC (Certis Biologicals)	Manufacturing / Manufacturer of biological crop protection products	USA	Personal data leakage	July 24, 2025
Tower Manufacturing Corporation	Manufacturing / Manufacturer of electrical safety devices	USA	Personal data leakage	July 22, 2025 June 3, 2025
TIMEC Oil & Gas	Energy, construction / Maintenance and mechanical construction company	USA	Personal data leakage	July 30, 2025 April 7, 2025
Vest Tube	Manufacturing / Producer of electric welded carbon steel tubing	USA	Personal data leakage, denial of IT systems	July 29, 2025 February 14, 2025
Baillie Lumber	Manufacturing / Hardwood lumber manufacturer	USA	Personal data leakage Ransomware	July 28, 2025 February 07, 2025 Cactus
Sauers Lopez Construction	Construction and engineering / General contractor specializing in new construction and remodel of automobile dealerships	USA	Personal data leakage, denial of IT systems	July 21, 2025 May 22, 2024
Lollytogs (LT Apparel Group)	Manufacturing / Apparel manufacturer	USA	Personal data leakage, denial of IT systems Ransomware	July 25, 2025 February 19, 2024 Clop
Control Module	Manufacturing / Manufacturer of time clocks, fleet and fuel	USA	Personal data leakage	July 7, 2025

	systems and EV charging products			
FLOE International	Manufacturing / Manufacturer of docks, boat lifts, trailers	USA	Personal data leakage Ransomware	July 12, 2025 Qilin Play
American Cord & Webbing	Manufacturing / Manufacturer of narrow textiles, injected molded plastic, and sewn straps	USA	Personal data leakage	July 15, 2025
Versa Designed Surfaces	Manufacturing / Manufacturer of commercial wallcoverings and wall protection products	USA	Personal data leakage	July 16, 2025 April 12, 2025
EIZO Rugged Solutions	Manufacturing / Manufacturer of graphics and video solutions for the defense and ISR market	USA	Personal data leakage Ransomware	July 7, 2025 May 6, 2025 Play
Heim & Haus	Manufacturing / Building element manufacturer	Germany	Denial of IT systems, operations and services, personal data leakage Ransomware	July 4, 2025 Kawa4096
Qantas	Logistics and transportation / Airline	Australia	Personal data leakage Ransomware	July 1, 2025 June 30,2025 Scattered Spider
Louis Vuitton	Manufacturing / Luxury fashion goods manufacturer	France	Personal data leakage Extortion	July 2, 2025 June 7, 2025 ShinyHunters

Surmodics	Manufacturing / Medical equipment manufacturer	USA	Denial of IT systems	July 2, 2025 June 5, 2025
Hero España	Food and beverage, manufacturing / Food manufacturer	Spain	Denial of operations and services	July 1, 2025 June 30, 2025
AzureWave Technologies	Electronics, manufacturing / Manufacturer of wireless communication modules and imaging modules	Taiwan	Denial of IT systems Ransomware	July 8, 2025 July 7, 2025 Qilin
Wibaie	Manufacturing / Manufacturer of windows and doors	France	Denial of operations Ransomware	July 10, 2025 July 9, 2025 Qilin
Novabev Group	Food and beverage, manufacturing / Liquor manufacturer	Russia	Denial of IT systems, operations and services Ransomware	July 16, 2025 July 14, 2025
Delfingen	Automotive, manufacturing / Manufacturer of on-board networks protection solutions and fluid transfer tubing	France	Data leakage Ransomware	July 16, 2025 PayoutsKing
Exel Composites	Manufacturing / Manufacturer of composite profiles and tubes for industrial applications	Finland	Personal data leakage Ransomware	July 25, 2025 July 2025 World Leaks
Serviço Autônomo de Água e Esgoto de Barretos	Utilities / Water utility, sewerage services	Brazil	Denial of IT systems and services Ransomware	July 22, 2025

Air Serbia	Logistics and transportation / Airline	Serbia	Denial of IT systems and services	July 17, 2025 July 4, 2025
Aeroflot	Logistics and transportation / Airline	Russia	Denial of IT systems, operations and services	July 28, 2025 Cyber-Partisans Silent Crow
SEMCO Technologies	Electronics, manufacturing / Manufacturer of electrostatic chucks and key components for semiconductor devices	France	Personal data leakage Ransomware	July 7, 2025 Qilin
BARTEC	Manufacturing / Manufacturer of explosion protection	Germany	Personal data leakage Ransomware	July 17, 2025 Safepay
Kibernetik AG	Manufacturing / Manufacturer of heating, cooling, photovoltaics, and ice machines	Switzerland	Denial of IT systems and services, data leakage	July 31, 2025
PAC Strapping Products	Manufacturing / Strapping manufacturer	USA	Personal data leakage, denial of IT systems Ransomware	August 4, 2025 March 26, 2025 Play
Episciences (Epionce)	Manufacturing / Personal care product manufacturer	USA	Personal data leakage	August 6, 2025 April 27, 2025
Lumitex	Manufacturing / Manufacturer of light delivery systems	USA	Personal data leakage	August 15, 2025 July 30, 2025

Old Dutch Foods	Food and beverage, manufacturing / Food production company	USA	Personal data leakage	August 11, 2025 October 16, 2024
Farmer's Rice Cooperative	Food and beverage, manufacturing / Rice manufacturer	USA	Personal data leakage	July 1, 2025 August 30, 2024
The Seydel Companies	Chemicals, manufacturing / Chemical manufacturer	USA	Personal data leakage Ransomware	August 20, 2025 April 26, 2025 Play
Util-Assist	Utilities / Utilities management company	Canada	Personal data leakage	August 27, 2025 July 11, 2025
NHB Holdings (New Horizons Baking Company, Genesis Baking Company, Metraco Transportation Company, New Horizons Food Solutions)	Food and beverage, manufacturing / Baked goods production company	USA	Personal data leakage	August 27, 2025 January 6, 2025
Lithium Nevada (Lithium Americas Corp.)	Mining / Lithium mining company	USA	Personal data leakage, denial of IT systems Ransomware	July 24, 2025 April 7, 2025 Medusa
The Hiller Companies	Construction and engineering / Design and engineering of fire protection systems and equipment	USA	Personal data leakage	August 25, 2025 December 18, 2024
Lasership / OnTrac Final Mile	Logistics and transportation /	USA	Personal data leakage	August 27, 2025 April 13, 2025

	Transportation and logistics services			
Sun Pacific Solar Electric	Energy, construction / Solar energy system installation and services	USA	Personal data leakage	August 25, 2025
LBX Company	Manufacturing / Heavy equipment manufacturer	USA	Personal data leakage	August 14, 2025 June 18, 2025
Gorham Sand & Gravel	Construction and engineering / Construction materials and excavation services	USA	Personal data leakage Ransomware	August 28, 2025 April 23, 2025 Play
BB Diversified Services	Manufacturing / Manufacturing of machined and assembled components	USA	Personal data leakage	August 20, 2025 February 24, 2025
Shinn Fu Company of America	Manufacturing / Hydraulic lifting equipment manufacturer	USA	Personal data leakage Ransomware	August 11, 2025 Play
Cate Equipment Company	Manufacturing / Heavy equipment and machinery	USA	Personal data leakage	August 14, 2025 August 2, 2024
ENGIE Power & Gas	Utilities, energy / Electricity generation and distribution, natural gas, nuclear power, renewable energy, district energy, petroleum industry	France	Personal data leakage	August 14, 2025
Rohtstein Corporation	Food and beverage, Manufacturing / food	USA	Personal data leakage	August 14, 2025

	products manufacturer			
Peter Pauper Press	Manufacturing / Printing and publishing	USA	Personal data leakage	August 18, 2025 Teamxxx
MoboTrex	Manufacturing / Manufacturer of traffic control products	USA	Personal data leakage	August 28, 2025
Vaquero Underground Services	Construction and engineering / Underground utilities installation	USA	Personal data leakage	August 1, 2025
Brookshire Grocery Company	Food and beverage, manufacturing / Bakery, dairy, ice cream, yogurt, fresh-cut, ice and water/drink producer	USA	Personal data leakage	August 15, 2025
City of Wichita Falls Cypress Water Treatment Facility	Utilities / Water treatment and purification	USA	Personal data leakage	August 15, 2025
Antonio Sofo & Sons Importing (Sofo Foods)	Logistics and transportation / Food distribution	USA	Personal data leakage Ransomware	August 28, 2025 Payouts King
Air France and KLM	Logistics and transportation / Airline	France Netherlands	Personal data leakage Extortion	August 6, 2025 ShinyHunters
Pakistan Petroleum Limited	Energy / Oil and gas producer	Pakistan	Denial of IT systems and operations, personal data leakage	August 7, 2025 August 6, 2025 Blue Locker

			Ransomware	yyy32111
KNH Enterprise	Manufacturing / Nonwoven specialty manufacturer	Taiwan	Denial of IT systems and operations	August 24, 2025
Pandora	Manufacturing / Jewelry manufacturer	Denmark	Personal data leakage Extortion	August 5, 2025 ShinyHunters
Chanel	Manufacturing / Luxury goods manufacturer	France	Personal data leakage Extortion	August 1, 2025 July 25, 2025 ShinyHunters
Data I/O Corporation	Electronics, manufacturing / Manufacturer of manual and automated security provisioning and device programming systems	USA	Denial of IT systems, operations and services	August 21, 2025 August 16, 2025
Polish water supply	Utilities / Water utility	Poland	Denial of operations	August 14, 2025 August 13, 2025
The LoveSac Company	Manufacturing / Furniture manufacturer	USA	Personal data leakage Ransomware	September 4, 2025 February 12, 2025 RansomHub
Cornwell Quality Tools	Automotive, manufacturing / Automotive hand tools manufacturer	USA	Personal data leakage Ransomware	September 4, 2025 December 12, 2024 Cactus
Sellmark Corporation	Manufacturing / Outdoor and tactical product manufacturer	USA	Personal data leakage	September 11, 2025 March 10, 2025

NPK International	Manufacturing / Manufacturer of sustainable composite matting products	USA	Personal data leakage	September 11, 2025
Farmer Brothers	Food and beverage, manufacturing / Coffee, tea and culinary products manufacturer	USA	Personal data leakage Ransomware	September 9, 2025 March 6, 2025 Chaos
Carus	Chemicals, manufacturing / Chemical products for water treatment, air purification, soil remediation	USA	Personal data leakage, denial of IT systems Ransomware	September 22, 2025 August 7, 2025 Akira
Havco Wood Products	Manufacturing / Trailer flooring manufacturing company	USA	Personal data leakage	September 19, 2025 March 30, 2025
Minsait ACS	Utilities / Power grid control software solutions and advanced automation technology for utilities	USA	Personal data leakage	September 19, 2025 March 26, 2025
Monterey Mushrooms	Food and beverage, manufacturing / Mushrooms manufacturer	USA	Personal data leakage Ransomware	September 18, 2025 August 2, 2025 Payouts King
Georgetown Brewing Company	Food and beverage, manufacturing / Craft brewery	USA	Personal data leakage Ransomware	September 26, 2025 August 22, 2025 INC
T.R.A. Industries Inc. / Huntwood Industries	Manufacturing / Wood cabinet manufacturer	USA	Personal data leakage Ransomware	September 26, 2025 August 9, 2025 Interlock

Tekni-Plex	Manufacturing / Material science and packaging manufacturer	USA	Personal data leakage Ransomware	September 24, 2025 November 18, 2024 RansomHub
All States Materials Group	Manufacturing / Road products manufacturer	USA	Personal data leakage Ransomware	September 23, 2025 August 22, 2025 Play
Champagne Logistics	Logistics and transportation / Logistics, transportation supply chain company	USA	Personal data leakage	September 8, 2025
Phoenix Products	Manufacturing / Lighting manufacturing company	USA	Personal data leakage, denial of IT systems Ransomware	September 11, 2025 July 31, 2025
Phoenix Mechanical Contracting	Construction and engineering / Installation and construction services in plumbing, electricity, heating, natural gas, air conditioning sectors	USA	Personal data leakage	September 9, 2025
Gale Associates	Construction and engineering / Consulting engineering company	USA	Personal data leakage	September 12, 2025 June 4, 2025
ENCON Heating & Air Conditioning	Construction and engineering / Engineering, installation, and maintenance of HVAC systems	USA	Personal data leakage Ransomware	September 12, 2025 February 21, 2025 RansomHub
MGM Transformers	Manufacturing / Transformer manufacturer	USA	Personal data leakage Ransomware	September 17, 2025 Akira

CSJB Holdings	Manufacturing / Manufacturer of engineered foundry products	USA	Personal data leakage	September 18, 2025
Minaris Advanced Therapies	Pharmaceutical, manufacturing / GMP manufacturing, cell and gene therapy manufacturing	USA	Personal data leakage	September 8, 2025 October 3, 2024
Hello Cake	Manufacturing / Sexual wellness products manufacturer	USA	Personal data leakage	September 19, 2025 July 25, 2025
PCE Constructors	Construction and engineering / Industrial construction company	USA	Personal data leakage	September 19, 2025
National Molding	Manufacturing / Plastics manufacturing company	USA	Personal data leakage	September 18, 2025
Volvo Group North America	Automotive, manufacturing / Motor vehicle manufacturing company	USA	Personal data leakage Ransomware	September 24, 2025 DataCarry
Braun Electric Company	Energy, manufacturing / Electrical and instrumentation contractor in the oil and gas industry	USA	Personal data leakage Ransomware	September 24, 2025 July 26, 2025 Qilin
Dulany Industries	Chemicals, manufacturing / Fertilizer manufacturer	USA	Personal data leakage	September 25, 2025
G&H Wire Company	Manufacturing / Orthodontic products manufacturer	USA	Personal data leakage	September 10, 2025

(G&H Orthodontics)				
Belkorp	Logistics and transportation / Logistics, transportation, supply chain, retail company	USA	Personal data leakage Ransomware	September 29, 2025 April 18, 2025 Teamxxx
Channel Fish	Food and beverage, manufacturing / Fish manufacturer	USA	Personal data leakage	September 10, 2025
Sunsweet Growers	Food and beverage, manufacturing / Prune manufacturer	USA	Personal data leakage, denial of IT systems Ransomware	September 3, 2025 December 11, 2024 RansomHub
Karndean Designflooring	Manufacturing / Manufacturer of vinyl tile flooring	USA	Personal data leakage	September 30, 2025 July 5, 2025 CRYPTO24
Talisman civil consultants	Construction and engineering / Civil engineering company	USA	Personal data leakage Denial of IT systems Ransomware	September 5, 2025 May 6, 2025 Qilin
Miller Construction	Construction and engineering / Construction company	USA	Personal data leakage Ransomware	September 11, 2025 July 3, 2025
Jaguar Land Rover	Automotive, manufacturing / Automobile manufacturer	UK	Denial of IT systems, operations and services, Ransomware	September 1, 2025 August 30, 2025 Scattered Lapsus$ Hunters
Bridgestone Americas	Manufacturing / Tire manufacturer	USA	Denial of operations	September 2, 2025

Maryland Transit Administration	Logistics and transportation / Mass transit administration	USA	Denial of services, data leakage Ransomware	August 25, 2025 Rhysida
Collins Aerospace (Heathrow, Berlin, Brussels and Dublin airports)	Logistics and transportation, aerospace, military defense / Aviation and defense technology company	USA UK Germany Belgium Ireland	Denial of IT systems, operations and services, supply chain / trusted partner Ransomware	September 20, 2025 September 19, 2025
Stellantis	Automotive, manufacturing / Automobile manufacturer	Netherlands USA	Personal data leakage Extortion	September 21, 2025 ShinyHunters
Chroma ATE	Electronics, manufacturing / Manufacturer of electronic test and measurement instruments	Taiwan	Denial of IT systems and operations Ransomware	September 17, 2025 Warlock
Transart Graphics	Manufacturing / Screen-printing company	Taiwan	Denial of IT systems	September 8, 2025
Morrisroe	Construction and engineering / Construction company	UK	Personal data leakage	September 19, 2025 September 14, 2025
Thermofin	Manufacturing / Heat exchanger manufacturer	Germany China Poland	Denial of operations and services, personal data leakage Ransomware	September 22, 2025 Sarcoma

Okuma Europe	Manufacturing / CNC machine tools and process optimization	Germany Japan	Personal data leakage Denial of IT systems Ransomware	September 25, 2025
Thai Diamond & Zebra Electric	Electronics, manufacturing / Electronic component manufacturing company	Thailand Japan	Denial of IT systems Ransomware	September 26, 2025 September 8, 2025
Refresco	Food and beverage, manufacturing / Beverage manufacturer	Germany	Denial of operations and services	September 25, 2025
Boliden / Miljödata	Mining, manufacturing / Metals, mining, and smelting company	Sweden	Personal data leakage, supply chain / trusted partner Ransomware	September 15, 2025 August 23, 2025 DataCarry
LG Balakrishnan & Bros	Manufacturing / Manufacturer of powertrain products	India	Denial of IT systems Ransomware	September 30, 2025 Medusa
Kering S.A.	Manufacturing / Luxury apparel manufacturer	France	Personal data leakage	September 15, 2025 ShinyHunters

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