Kaspersky ICS CERT

kaspersky

A brief overview of the main incidents in industrial cybersecurity Q1 2026

18.06.2026

Version 1.0

Contents

In Q1 2026, 131 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

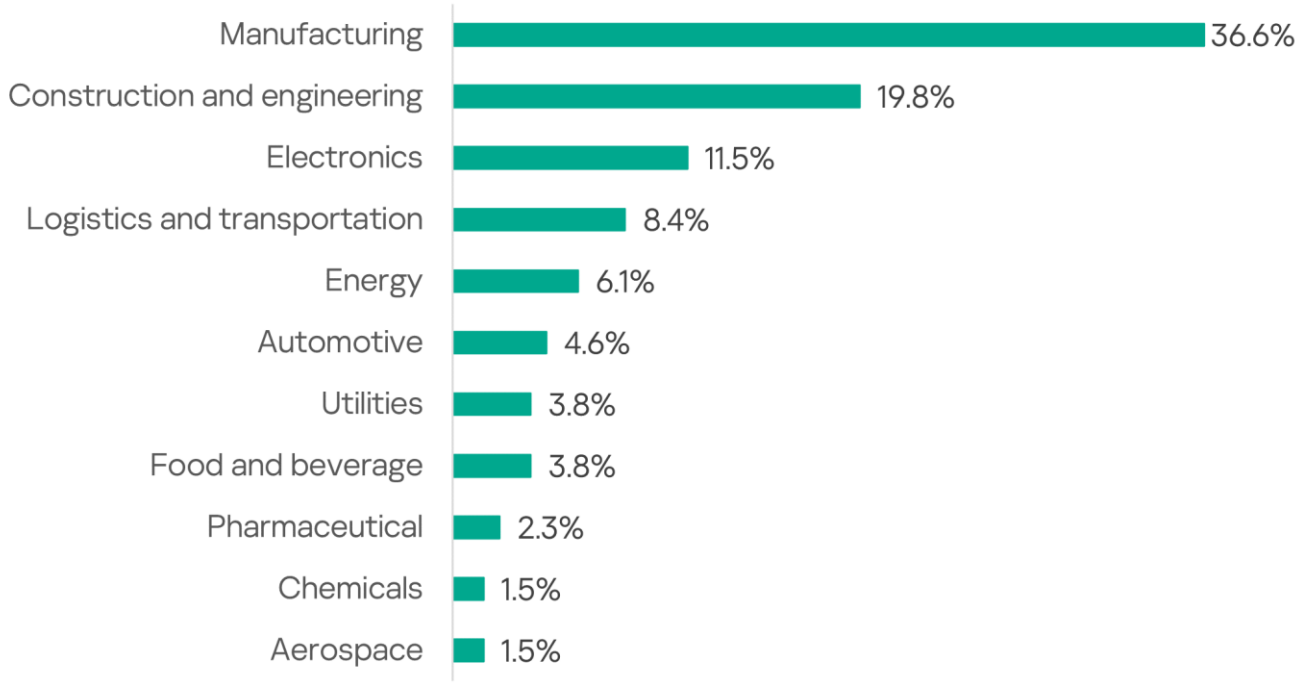
Several significant incidents were unveiled this quarter from the perspective of the threat landscape.

Reports of attacks on Poland's critical infrastructure – including traditional and renewable energy , in an attempt to gain access to automated control systems, as well as loud statements about attacks on nuclear power facilities, allegedly "avoided" any potential negative consequences for the facility's operation, clearly indicate that the Overton window is shifting in a dangerous direction for society.

The transportation industry once again demonstrated its vulnerability to attacks on third-party services that support numerous essential modern logistics tasks. For example, a breathalyzer vendor proved to be an unexpected weak point when a lack of access to its online device calibration service prevented many drivers from operating their trucks. Given real-world events, cyberattacks on transportation and logistics companies are becoming especially dangerous, as the process of disrupting global supply chains appears to have begun.

Attacks on healthcare organizations and pharmaceutical companies can limit the availability of medications and medical devices, directly threatening human health and lives. However, it seems that humanitarian considerations are becoming less important to hackers when they choose their targets.

Interesting shifts in the threat landscape can also be expected from a technical perspective. For example, in one incident, attackers destroyed data not only on the workstations and servers of the attacked organization but also on its employees' mobile devices (including personal devices) connected to corporate services. In the near future, the list of common target types may expand to include other unexpected equipment, at least when it comes to the most "creative" ransomware and hacktivist teams.



January

- Longchen Paper & Packaging Co., Ltd
- Legacy Manufacturing Company
- Gentex Optics Inc.
- Komar Industries LLC
- Designs For Vision Inc.
- Dot Foods Inc./ Dot Transportation Inc.
- Endesa Energía / Energía XXI
- Kyowon Group
- Posillico Inc.
- Polish energy grid
- Furuno USA
- Ingram Micro Inc.
- Port of Ancona (Autorità di Sistema Portuale del Mare Adriatico Centrale)
- FirstFruits Farms LLC
- KMS Solutions
- Advantage Dirt Contractors Inc.
- GEM Technologies
- Y.C.C Parts Mfg Co., Ltd
- Eversion Electronics
- BMP America
- JURA Inc.
- Genan Inc.
- Venezia Bulk Transport
- Verkehrsgesellschaft Main-Tauber Mbh (VGMT)
- Sellars Absorbent Materials Inc.
- Precipio Inc.
- ShopBot Tools Inc.
- Itasca Consulting Group
- EMC Water LLC
- Nova Biomedical Corp.
- Paragon Technologies Co., Ltd.
- DH Smith Company, Inc.
- Murex Petroleum Corporation
- The Vladimir Bread Factory
- GS Engineering
- Michigan Sugar Company
- Thornton Plumbing and Heating

February

- Wiseon Technologies Co. Ltd.
- Powerhouse Retail Services
- Gozo Channel
- Royal Machine and Tool Corporation
- Land Betterment Corporation
- Powertech Industrial Co. Ltd.
- Barnhart Group Inc.
- Athena Manufacturing LP
- Conpet
- Volvo Group North America
- HYTORC Division of UNEX Corporation
- Colson Group Holdings LLC
- Weekley Homes LLC (David Weekley Homes)
- Haley's Metal Shop
- Anchor Industries Inc.
- Karnes Electric Cooperative Inc.
- Prismier LLC
- Delta Electronics Inc.
- Tenga Co. Ltd.
- Tecan Technology Development Boston, Inc.
- Molded Products Inc.
- Nang Kuang Pharmaceutical Co., Ltd.
- Deutsche Bahn
- MAX USA Corp.
- Alpine Lumber Company
- Walters-Morgan Construction Inc.
- UFP Technologies
- Advantest Corporation
- Ahtna Inc.
- Hazeldenes
- Lobar Inc.
- Svealandstrafiken
- Sheffield Pharmaceuticals
- KC Installation, LLC (KCI Telecommunications)
- Susquehanna Glass Company
- AssetGenie Inc.
- Applied Natural Gas Fuels Inc.
- Melzer's Fuel Service Inc.
- U.S. Graphite Corporation
- Pinnacle Development Group Inc.
- CTC Building Solutions / American Energy Management
- The InterTech Group Inc.

March

- Intuitive Surgical, Inc.
- Hingham Municipal Lighting Plant
- LISI Group
- AkzoNobel
- Advanced Optoelectronic Technology Inc.
- MAKI Building Centers, Inc.
- Cabka
- Data Graphics Inc.
- Pyramid ETC Companies, LLC
- Structural Component Systems
- Ericsson Inc.
- O. Berk Company of New England LLC
- L&S Mechanical
- Tyree Oil Inc.
- ELECQ
- QualiChem, Inc.
- Michelin
- Stryker
- OSI Systems, Inc.
- Poland's National Centre for Nuclear Research
- Lohmann Corporation
- Hypertherm, Inc.
- TC Controls and Services, Inc.
- American Vintage Home
- Jean Co., Ltd.
- A&D Technology
- Elray Manufacturing Company
- Intoxalock
- Durvet, Inc.
- Capital Star Oil & Gas
- Trio-Tech International
- Mazda Motor Corporation
- TOMCO2 Systems Company
- National Coatings, Inc.
- Westport Fuel Systems Inc.
- Titan Roofing
- Segue Manufacturing Services LLC
- Royal Chemical Company
- Winmate Inc.
- TSU One Holdings, LLC
- Port of Vigo
- Mutti USA Inc.
- Brock Built Homes
- Alliance Industrial Refrigeration Services, Inc.
- TriMed, Inc.
- Hosokawa Micron Corporation
- Accu-Tube LLC
- Glenmark Pharmaceuticals Inc.
- Nan Liu Enterprise Co., Ltd.
- MESA Products, Inc.
- Master Millwork, LLC
- Palacios Marine & Industrial Coatings, Inc.

2026

ICS-targeting attack

Polish energy grid

Energy, manufacturing

APT

Wiper

Exploitation of network devices

On January 13, Poland's energy minister announced at a press conference that there had been attempted attacks on the Polish energy sector at the end of 2025. According to a January 15 statement on the Polish government website, the targeted systems included combined heat and power plants, as well as a system that manages power derived from renewable energy resources, such as wind turbines and photovoltaic farms. There were no negative consequences, such as the destabilization of the national energy system or a blackout. The technical details of the attack were studied and described by ESET and CERT Polska, and briefly covered in APT and financial attacks on industrial organizations in Q1 2026.

Attempted attack on nuclear power object

Poland's National Centre for Nuclear Research

Energy, manufacturing

On March 12, Poland's National Centre for Nuclear Research (NCBJ) announced in a statement that an attempted cyberattack on the institute's IT infrastructure took place. "Thanks to the rapid and effective response of the organization's security systems and procedures, the attack was thwarted and the integrity of the systems was not compromised. All safety systems operated according to procedure, the attack was blocked, and the actions taken enabled the immediate securing of the infrastructure and maintenance of the institute's operational continuity". The director of the National Centre for Nuclear Research reported that no production, operational, or research processes were disrupted, and that the MARIA reactor continued operating safely and smoothly at full power. NCBJ worked closely with NASK-PIB, the Ministry of Digital Affairs, Deputy Prime Minister and Minister Krzysztof Gawkowski, and the Ministry of Energy and Minister Miłosz Motyka to ensure the highest level of security for critical infrastructure. Poland's minister of digital affairs told private broadcaster TVN24+ that "the initial findings suggested the entry vectors had links to Iran".

Severe service disruption

Intoxalock

Automotive, manufacturing

Denial of IT systems and services

Intoxalock, a US automotive breathalyzer manufacturer, reported on March 16 that it had been the target of a cybersecurity incident, resulting in its systems experiencing downtime, according to an announcement posted to its website. Intoxalock said the interlock devices themselves remained operational, but calibrations and related service-center transactions were disrupted. The cybersecurity event left some drivers with vehicles equipped with ignition interlock devices unable to start or drive their vehicles. The lockouts appeared to be the result of Intoxalock's breathalyzers needing periodic calibrations that require a connection to the company's servers. Drivers who were due for a calibration and couldn't perform one due to the company's downtime were stranded. The company stated on its website that it was offering 10-day extensions on those calibrations due to its cybersecurity disruption, as well as towing services in some cases. The company told Cybernews that for customers requiring calibrations, Intoxalock had developed a new system app that was pushed to all of its calibration devices while coordinating with state regulators to provide a temporary solution until the company could resume its systems. Intoxalock did not explain what sort of cyberattack it faced or whether hackers obtained any of the company's user data. On March 22, Intoxalock issued an update stating that its systems had resumed, and installations, calibrations, and service center support was once again available.

Vladimir Bread Factory hit by cyberattack

Food and beverage, manufacturing

Denial of IT systems and services

According to a local media report, a cyberattack on a major Russian bakery manufacturer in the Vladimir region disrupted food deliveries. In a statement, the Vladimir Bread Factory said its internal digital systems were hit overnight on January 25, knocking out office computers, servers, electronic document management tools and the 1C enterprise accounting system. While production itself was not affected and the bakeries continued operating at full capacity, the outage complicated order processing and deliveries. Local residents, retail outlets and food suppliers for social institutions reported difficulties fulfilling existing contracts and temporary shortages of the company's products in stores. Large retail chains acknowledged the delivery issues but said there was no widespread shortage of bread on store shelves. To keep supplies moving, the company shifted all office staff to a round-the-clock schedule and temporarily reverted to manual processing of orders and shipments. The

factory did not provide a timeline for fully restoring its digital systems and apologized to partners and consumers for the disruption.

Attacks leading to denial of operations

Hazeldenes

Manufacturing, food and beverage

Denial of services and operations, personal data leakage

Ransomware

A cyberattack affected a plant owned by Australian chicken meat processor Hazeldenes, causing state-wide shortages in pubs and shops. The company said it was working with cybersecurity investigators to identify the cause of the attack. Retail and industry sources told the ABC that the chicken meat processor had been unable to fulfill some orders because it could not package its products. A manager at one meat wholesaler said it had to source chicken from another provider while Hazeldenes was offline. Workers at Hazeldenes told the ABC the problems began with the computer systems in the week of February 16-22, with some employees reporting difficulties logging on and using computers. They said that by February 19, the problem had become worsened, prompting the company to shut down the Wi-Fi at its Lockwood South site. Some customers said there had been a lack of communication from the meat processor. In March, the DragonForce ransomware group claimed responsibility for the attack on Hazeldenes.

In a statement published on its website on March 12, the company said that the investigation into the cyberincident confirmed that data, including personal information, was accessed. The review indicated that the data impact was largely limited to historical operational and corporate information. The company also stated that it was aware cybercriminals had named Hazeldenes online and had illegally shared data stolen from its environment. On March 30, Hazeldenes confirmed that it had safely and securely returned to regular production following the cyberincident.

Svealandstrafiken

Logistics, transportation

Denial of services and operations

According to a local news outlet, Swedish transportation company Svealandstrafiken experienced a major cyberattack on February 23. The attack impacted the company's digital infrastructure and caused significant disruptions to operations, although specific details about the attack and its effects on systems and data were not disclosed. An investigation was launched to assess the full impact of the attack.

Stryker

Manufacturing

Denial of IT systems, services and operations

Hacktivist

US medical devices and equipment manufacturing company Stryker announced on March 11 that it was experiencing a global network disruption in its Microsoft environment due to a cyberattack. The company found no indication of ransomware or malware and believed the incident was contained. Stryker reported the incident in a Form 8-K filing with the United States Securities and Exchange Commission (SEC) on March 11. According to the filing, the incident caused disruptions and limited access to some of the company's information systems and business applications that support its operations and corporate functions. On March 12, Stryker issued an update on its website, stating that the incident had disrupted order processing, manufacturing and shipping. In an update on March 15, the company stated that all its medical devices were safe to use, though electronic ordering systems remained offline and customers had to place orders manually through sales representatives.

Iranian hacktivist threat group Handala (aka Handala Hack Team, Hatef, or Hamsa) claimed responsibility for the attack on March 11. In their post, the group claimed to have wiped approximately 200,000 Stryker systems, servers and mobile devices, as well as exfiltrating 50 TB of company data. The attackers also defaced the company's Entra login page with a Handala logo. A Stryker employee told BleepingComputer that the incident began early on March 11, when devices enrolled in the company's mobile device management system were remotely wiped. The employee said that colleagues who had personal phones for work access also lost data when their devices were reset. Staff were instructed to remove corporate management and applications from their personal devices, including the Intune Company Portal, Teams, and VPN clients. Many employees also reported that the attack disrupted access to internal services and applications. A source familiar with the attack also told BleepingComputer that the threat actor used the wipe command in Intune, Microsoft's cloud-based endpoint management service, to erase data. The attacker carried out the action after compromising an administrator account and creating a new Global Administrator account.

Nova Biomedical

Manufacturing

Denial of operations, personal data leakage

Nova Biomedical Corp., a US manufacturer of advanced technology blood testing analyzers, in vitro diagnostic devices, and clinical laboratory instruments, announced that on July 22, 2025, it experienced a sophisticated cybersecurity attack that disrupted its operations. An investigation determined that an unauthorized actor had accessed Nova's electronic infrastructure and deployed malware. The company also determined that personally identifiable information may have been impacted.

Port of Vigo

Logistics, transportation

Denial of IT systems, services and operations

Ransomware

The Port Authority at Spain's Port of Vigo was the target of a ransomware attack, according to local media reports. The incident was detected at 5:45 am local time on March 24, and affected servers used for cargo traffic management, the port's website and other digital services. Some portions of the port's network were disconnected, and cargo operations were managed manually. The president of the Vigo Port Authority said that although the port's operational services and physical functioning were been affected, the programs would not reopen to the public until all security checks had been completed. There was no estimated date for resuming normal operations.

Incidents at large organizations

Deutsche Bahn

Logistics, transportation

Denial of IT services

DDoS

Deutsche Bahn, Germany's state-owned railway company, suffered a distributed denial-of-service (DDoS) attack that began on February 17 and continued into February 18. According to the company, the attack came in waves and was substantial in scale. The DDoS attack disrupted Deutsche Bahn's information and ticketing systems, including its websites and the DB Navigator app. The services were restored on February 18, though the company imposed temporary limitations on them. Deutsche Bahn wrote in a blog post that they were in close contact with the federal authorities.

Delta Electronics

Electronics, manufacturing

Denial of IT systems, personal data leakage

According to a bulletin from the Taiwan Stock Exchange (TWSE) portal published on February 10, an overseas subsidiary of the Taiwanese electronics manufacturing company Delta Electronics Inc. detected abnormal login attempts on its information systems. Upon investigation, systems at the overseas subsidiary were found to have been subject to cyberattacks, posing a potential risk of leakage of business-related data and employees' personal data. After detecting the anomaly, the Information Technology Division worked with professional cybersecurity consultants to conduct a comprehensive investigation. All affected systems at the overseas subsidiary underwent security reviews and resumed normal operations without affecting business operations. Network monitoring and access controls were strengthened to ensure the overall operation of the information systems remained secure and stable. There was no material impact on the company's operations based on the assessments.

AkzoNobel

Chemicals, manufacturing

Data leakage

Ransomware

In March, Dutch paints and coatings manufacturer AkzoNobel confirmed to BleepingComputer that hackers had breached the network of one of its US sites after the Anubis ransomware group claimed responsibility for an attack on the company. A company spokesperson said that the incident was limited to one of the company's sites in the United States and had been contained. The impact was minimal, and AkzoNobel took the appropriate steps to notify and support affected parties. The company also planned to work closely with relevant authorities. However, the Anubis ransomware group claimed to have stolen 170 GB of data and almost 170,000 files from AkzoNobel, and leaked samples on its leak site that included screenshots of select documents and a list of the stolen files. The published data contained confidential agreements with high-profile clients, email addresses, phone numbers, private email correspondence, passport scans, material testing documents, and internal technical specification sheets.

LISI Group

Manufacturing

Personal data leakage

Ransomware

LISI Group, a French manufacturer of assembly solutions and high-value components for the aerospace, automotive and medical sectors, confirmed that it had suffered a cyberincident after the Qilin ransomware group published statements about the attack on its data leak website. According to the company's CEO, the breach was confined to a very limited scope. Investigators confirmed that only a very small amount of data was exfiltrated, affecting two ancillary sites. According to the statement, the IT systems were entirely separate, and the breach did not affect the other sites of the aerospace and automotive divisions. The company confirmed that operations were not affected and no compromise of its infrastructure was identified.

Cybernews researchers examined the data samples provided by Qilin to back up its claims of a data breach. The samples included sales plans, internal business documents, files containing bank account details, employee consent forms, confidentiality agreements, provision contracts, and documents containing employees' full names and contact information.

Michelin

Automotive, manufacturing

Data leakage

Ransomware

French tire manufacturer Michelin confirmed to SecurityWeek that it was affected by a data breach stemming from a massive cybercrime campaign that targeted organizations using Oracle's E-Business Suite (EBS) solution. The company said its teams promptly conducted a thorough investigation and determined that an Oracle EBS zero-day was exploited in the attack. The

company confirmed that hackers accessed some files, but said only a small, localized volume of data with no sensitive or technical IT information was affected by the incident. Michelin also noted that no ransomware was involved in the attack and that there had been no impact on its global systems. The Clop ransomware and extortion group took credit for the EBS hacking campaign, which targeted Michelin among other organizations.

Mazda Motor Corporation

Automotive, manufacturing

Personal data leakage

In March, the Japanese multinational automotive manufacturer Mazda Motor Corporation reported that in mid-December 2025 it identified traces of unauthorized external access to a management system used for warehouse operations related to parts procured from Thailand. The following personal information of company and group company employees, as well as business partners, may have been affected (692 records): user IDs issued by the company, name, email address, company name, business partner IDs. Following the discovery, Mazda promptly reported the matter to the Personal Information Protection Commission, an external bureau of the Japanese Cabinet Office, and implemented appropriate security measures. The company also conducted an investigation with the support of an outside specialist organization.

Ericsson

Manufacturing

Personal data leakage

The US subsidiary of global telecommunications equipment company Ericsson Inc. disclosed a data breach in March affecting the personal information of thousands of individuals. According to Ericsson, the breach occurred at a third-party service provider, which detected unauthorized access to data on its systems on April 28, 2025. The unnamed service provider conducted an investigation and determined that files storing personal information may have been accessed between April 17 and 22, 2025. The type of personal information potentially impacted by the incident varied by individual, but it may have included first and last name, as well as Social Security number.

Appendix. Full list of confirmed incidents

Victim	Industry / Profile	Country	Impact features	Date of notification Date of incident (if known) Suspected attackers
Polish energy grid	Energy, manufacturing	Poland	Wiper	January 13, 2026 December 29, 2025 Sandworm Static Tundra
Endesa Energía / Energía XXI	Utilities, energy / Electricity generation and distribution	Spain	Personal data leakage	January 11, 2026 spain
Kyowon Group	Manufacturing / Home appliances manufacturer	South Korea	Denial of IT systems and IT services, data leakage Ransomware	January 12, 2026 January 10, 2026
Longchen Paper & Packaging Co., Ltd	Manufacturing / Manufacturer of low carbon papermaking and eco-packaging	Taiwan	Denial of IT systems Ransomware	January 2, 2026
Y.C.C Parts Mfg Co., Ltd	Automotive, manufacturing / Automotive parts manufacturer	Taiwan	Denial of IT systems Ransomware	January 18, 2026 Qilin
Eversion Electronics	Electronics, manufacturing / LCD and LCM manufacturer	Taiwan	Denial of IT systems	January 19, 2026

Verkehrsgesellschaft Main-Tauber mbH (VGMT)	Logistics and transportation / Transport company	Germany	Denial of IT systems and services	January 23, 2026
Paragon Technologies Co., Ltd.	Manufacturing / Manufacturing of electro-magnetic interference sputtering equipment	Taiwan	Denial of IT systems	January 27, 2026
The Vladimir Bread Factory	Food and beverage, manufacturing / Bakery manufacturer	Russia	Denial of IT systems and services	January 28, 2026 January 25, 2026
Designs For Vision Inc.	Manufacturing / Optical device manufacturer	USA	Personal data leakage	January 5, 2026 October 11, 2025 Akira
Furuno USA	Electronics, manufacturing / Marine electronics manufacturer	USA	Personal data leakage	January 14, 2026 September 12, 2025 Rhysida
KMS Solutions	Construction and engineering / Engineering services company	USA	Personal data leakage	January 16, 2026 November 27, 2025
Venezia Bulk Transport	Logistics and transportation / Transportation provider	USA	Personal data leakage	January 22, 2026 August 5, 2025 Akira
BMP America	Manufacturing / Industrial textile manufacturer	USA	Personal data leakage	January 20, 2026 October 2, 2025 Play

Nova Biomedical Corp.	Manufacturing / Manufacturer of advanced technology blood testing analyzers, in vitro diagnostic devices, and clinical laboratory instruments	USA	Denial of operations, personal data leakage	January 27, 2026 July 22, 2025
Murex Petroleum Corporation	Energy / Oil and gas producer	USA	Personal data leakage	January 27, 2026 May 27, 2025
EMC Water LLC	Utilities / Water utility	USA	Zero-day vulnerability Personal data leakage	January 26, 2026
Michigan Sugar Company	Food and beverage, manufacturing / Sugar manufacturer	USA	Personal data leakage	January 30, 2026 August 14, 2025 Akira
DH Smith Company, Inc.	Construction and engineering / Non-residential building construction services	USA	Personal data leakage	January 27, 2026 March 27, 2025 Lynx
Ingram Micro Inc.	Logistics and transportation / Global technology distribution and supply-chain logistics	USA	Personal data leakage	January 16, 2026 July 2, 2025 SafePay
Posillico Inc.	Construction and engineering / Heavy civil and industrial construction	USA	Denial of IT systems, personal data leakage	January 13, 2026 December 8, 2025 Akira

Dot Foods Inc./ Dot Transportation Inc.	Logistics and transportation / Large-scale food distribution and freight logistics	USA	Personal data leakage	January 7, 2026 December 3, 2025
Gentex Optics Inc.	Manufacturing / Protective gear helmet systems manufacturer	USA	Personal data leakage	January 2, 2026
Komar Industries LLC	Manufacturing / Waste processing equipment manufacturer	USA	Personal data leakage	January 5, 2026 September 12, 2025 Play
Sellars Absorbent Materials Inc.	Manufacturing / Industrial paper and absorbent products manufacturing	USA	Personal data leakage	January 23, 2026 Play
JURA Inc.	Manufacturing / Home appliances manufacturer	USA	Personal data leakage	January 21, 2026 December 23, 2025
ShopBot Tools Inc.	Manufacturing / CNC machinery manufacturer	USA	Personal data leakage	January 23, 2026 AiLock
Thornton Plumbing and Heating	Construction and engineering / Plumbing and heating construction company	USA	Denial of IT systems, personal data leakage	January 30, 2026 November 12, 2025
GS Engineering	Construction and engineering / Engineering services company	USA	Personal data leakage	January 29, 2026 October 27, 2025
Itasca Consulting Group	Construction and engineering / Engineering	USA	Personal data leakage	January 23, 2026

	consulting company			December 12, 2025 Akira
Genan Inc.	Manufacturing / Ambient rubber infill manufacturer	USA	Personal data leakage	January 21, 2026
FirstFruits Farms LLC	Food and beverage, manufacturing / Agricultural production	USA	Personal data leakage	January 16, 2026 September 12, 2025
Advantage Dirt Contractors Inc.	Construction and engineering / Construction services company	USA	Personal data leakage	January 16, 2026 December 11, 2025
Legacy Manufacturing Company	Manufacturing / Water and air hose manufacturer	USA	Denial of IT systems, personal data leakage	January 2, 2026 October 12, 2025
Port of Ancona (Autorità di Sistema Portuale del Mare Adriatico Centrale)	Logistics and transportation / Maritime organization	Italy	Personal data leakage Ransomware	January 16, 2026 December 11, 2025 Anubis
Precipio Inc.	Manufacturing / Manufacturer of diagnostic products	USA	Personal data leakage Ransomware	January 23, 2026 November 23, 2025
GEM Technologies	Construction and engineering / Construction services	USA	Personal data leakage	January 16, 2026 August 5, 2025
Advantest Corporation	Electronics, manufacturing / Semiconductor test equipment supplier	Japan	Denial of IT systems Ransomware	February 19, 2026

Hazeldenes	Food and beverage, manufacturing / Chicken meat processor	Australia	Denial of services and operations, personal data leakage Ransomware	February 23, 2026 February 19, 2026 DragonForce
Conpet	Energy / National oil pipeline operator	Romania	Denial of IT systems and IT services Ransomware	February 4, 2026 February 3, 2026 Qilin
Wiseon Technologies Co. Ltd.	Electronics, manufacturing / Manufacturer of interconnect components, wireless components, thermal modules, and automotive electronics products	Taiwan	Denial of IT systems	February 2, 2026
Powertech Industrial Co. Ltd.	Electronics, manufacturing / Manufacturer of power solutions	Taiwan	Denial of IT systems	February 3, 2026
Gozo Channel	Logistics and transportation / Ferry company	Malta	Denial of IT systems	February 3, 2026
Deutsche Bahn	Logistics and transportation / State-owned railway company	Germany	Denial of IT services DDoS	February 17, 2026
UFP Technologies	Manufacturing / Medical device manufacturer	USA	Denial of IT systems and services, data leakage	February 19, 2026
Delta Electronics Inc.	Electronics, manufacturing /	Taiwan	Denial of IT systems,	February 10, 2026

	Electronics manufacturing company		personal data leakage	
Nang Kuang Pharmaceutical Co., Ltd.	Pharmaceutical, manufacturing / Pharmaceutical manufacturing company	Taiwan	Denial of IT systems, data leakage Ransomware	February 16, 2026 INC RANSOM
Svealandstrafiken	Logistics and transportation / Transportation company	Sweden	Denial of services and operations	February 24, 2026
Haley's Metal Shop	Construction and engineering / HVAC contractor	USA	Personal data leakage	February 6, 2026 December 1, 2025
Royal Machine and Tool Corporation	Manufacturing / Workholding devices manufacturer	USA	Personal data leakage	February 3, 2026
Athena Manufacturing LP	Manufacturing / Precision machining, fabrication, mechanical assembly, and mechanical design	USA	Personal data leakage	February 4, 2026
Barnhart Group Inc.	Logistics and transportation / Transportation and warehousing services	USA	Denial of IT systems, personal data leakage	February 4, 2026 August 27, 2025
Volvo Group North America	Automotive, manufacturing / Motor vehicle manufacturing company	USA	Personal data leakage Ransomware	February 5, 2026 October 21, 2024 Safepay

Tecan Technology Development Boston, Inc.	Electronics, manufacturing / Laboratory equipment manufacturing	USA	Personal data leakage	February 12, 2026 December 2, 2025
Tenga Co. Ltd.	Manufacturing / Sexual health product manufacturer	Japan	Personal data leakage	February 12, 2026
Anchor Industries Inc.	Manufacturing / Outdoor structure and canopy manufacturer	USA	Personal data leakage	February 7, 2026 Play
Alpine Lumber Company	Manufacturing / Lumber products manufacturer	USA	Personal data leakage Ransomware	February 18, 2026 December 14, 2025
AssetGenie Inc.	Electronics, manufacturing / Electronic component distribution, technology repair services, custom LCD displays, battery energy storage systems	USA	Personal data leakage Ransomware	February 26, 2026 October 12, 2025 Akira
Ahtna Inc.	Construction and engineering / Construction, engineering and logistics services	USA	Personal data leakage Ransomware	February 20, 2026 April 20, 2025 Qilin
Powerhouse Retail Services	Logistics and transportation / Third-party logistics	USA	Personal data leakage	February 3, 2026 September 20, 2023
KC Installation, LLC (KCI Telecommunications)	Construction and engineering / Telecom	USA	Personal data leakage	February 25, 2026 August 22, 2025

	infrastructure installation		Ransomware	Akira
Land Betterment Corporation	Construction and engineering, manufacturing / Environmental remediation and land reuse	USA	Personal data leakage	February 3, 2026 January 10, 2026
HYTORC Division of UNEX Corporation	Manufacturing / Industrial bolting systems and tools manufacturing	USA	Personal data leakage Ransomware	February 5, 2026 Qilin
Colson Group Holdings LLC	Manufacturing / Caster and wheel manufacturer	USA	Personal data leakage	February 6, 2026 June 19, 2025
Molded Products Inc.	Manufacturing / Rubber and plastic molding manufacturer	USA	Personal data leakage	February 16, 2026
MAX USA Corp.	Manufacturing / Manufacturer of pneumatic nail guns	USA	Personal data leakage Ransomware	February 18, 2026 January 11, 2026 Lockbit 5.0
Sheffield Pharmaceuticals	Pharmaceutical, manufacturing / Pharmaceutical manufacturing company	USA	Personal data leakage	February 24, 2026
The InterTech Group Inc.	Aerospace, manufacturing / Packaging materials manufacturer	USA	Personal data leakage Ransomware	February 28, 2026 Akira
Walters-Morgan Construction Inc.	Construction and engineering / Construction services focused in the wastewater	USA	Personal data leakage Ransomware	February 18, 2026 Sinobi

	and water treatment fields			
CTC Building Solutions / American Energy Management	Construction and engineering / Energy management, temperature controls and systems integration company	USA	Personal data leakage	February 27, 2026
Pinnacle Development Group Inc.	Construction and engineering / Civil engineering construction	USA	Personal data leakage	February 27, 2026
Melzer's Fuel Service Inc.	Energy / Fuel distribution services	USA	Personal data leakage	February 26, 2026
Prismier LLC	Manufacturing / Precision metal and plastic manufacturing services	USA	Personal data leakage	February 10, 2026 November 7, 2025
Lobar Inc.	Construction and engineering / General construction and electrical company	USA	Personal data leakage	February 23, 2026 April 15, 2025
Karnes Electric Cooperative Inc.	Utilities / Electric distribution utility	USA	Personal data leakage Ransomware	February 9, 2026 Qilin
Weekley Homes LLC (David Weekley Homes)	Construction and engineering / Residential construction company	USA	Personal data leakage	February 6, 2026

Applied Natural Gas Fuels Inc.	Energy / Producer and distributor of liquefied natural gas	USA	Personal data leakage	February 26, 2026 December 22, 2025
Susquehanna Glass Company	Manufacturing / Glassware manufacturer	USA	Personal data leakage Ransomware	February 26, 2026 December 1, 2025 Akira
U.S. Graphite Corporation	Aerospace, manufacturing / Carbon and graphite materials production	USA	Personal data leakage	February 27, 2026 August 19, 2025
Stryker	Manufacturing / Medical devices and equipment manufacturing company	USA	Denial of IT systems, services and operations Wiper	March 11, 2026 Handala Hack Team
Poland's National Centre for Nuclear Research	Energy, manufacturing	Poland	Unknown	March 12, 2026 Iran-related
Intuitive Surgical, Inc.	Manufacturing / Manufacturer of robotic products	USA	Personal data leakage	March 2026
Port of Vigo	Logistics and transportation	Spain	Denial of IT systems, services and operations Ransomware	March 25, 2026 March 24, 2026
ELECQ	Electronics, manufacturing / Manufacturer of electric vehicle charging stations	China	Personal data leakage Ransomware	March 9, 2026 March 7, 2026

Advanced Optoelectronic Technology Inc.	Electronics, manufacturing / Manufacturer of light-emitting diodes and lasers	Taiwan	Denial of IT systems	March 3, 2026
AkzoNobel	Chemicals, manufacturing / Sustainable chemical manufacturer	Netherlands	Data leakage Ransomware	March 3, 2026
Winmate Inc.	Electronics, manufacturing / Manufacturer of rugged industrial computers, displays, and embedded technologies	Taiwan	Data leakage Ransomware	March 24, 2026 WorldLeaks
Nan Liu Enterprise Co., Ltd.	Manufacturing / Manufacturer of nonwoven fabrics and biotech materials	Taiwan	Denial of IT systems Ransomware	March 29, 2026 Qilin
Jean Co., Ltd.	Electronics, manufacturing / Manufacturer of color display tube (CDT), liquid crystal display (LCD) and projectors	Taiwan	Denial of IT systems Ransomware	March 15, 2026 March 13, 2026 LockBit 5.0.
Hosokawa Micron Corporation	Manufacturing / Manufacturer of mixing, drying and agglomeration technologies	Japan	Personal data leakage Ransomware	March 27, 2026 February 2, 2026 Everest
LISI Group	Manufacturing / Manufacturer of assembly solutions and high-	France	Personal data leakage Ransomware	March 3, 2026 Qilin

	value components for the aerospace, automotive and medical sectors			
Cabka	Manufacturing / Manufacturer of plastic pallets made from recycled plastics	Germany	Data leakage Ransomware	March 4, 2026 Play
Michelin	Automotive, manufacturing / Tire manufacturer	France	Zero-day vulnerability Data leakage Ransomware	March 11, 2026 Clop
Mazda Motor Corporation	Automotive, manufacturing / Automotive manufacturer	Japan	Personal data leakage	March 19, 2026 December 2025
Westport Fuel Systems Inc.	Automotive, manufacturing / Supplier of advanced alternative fuel components and systems	Canada	Ransomware	March 20, 2026 Embargo
Intoxalock	Automotive, manufacturing / Automotive breathalyzer manufacturer	USA	Denial of IT systems and services	March 17, 2026
Trio-Tech International	Electronics, manufacturing / Semiconductor testing company	USA	Denial of IT systems, data leakage Ransomware	March 18, 2026 March 11, 2026 Gunra
Ericsson Inc.	Manufacturing / Manufacturer of networking hardware	Sweden	Personal data leakage	March 6, 2026 April 17, 2025

L&S Mechanical	Construction and engineering / Plumbing, electrical, and HVAC company	USA	Personal data leakage	March 6, 2026 Space Bears
Elray Manufacturing Company	Manufacturing / Metal stamping manufacturer	USA	Personal data leakage	March 16, 2026 November 19, 2025
Hypertherm, Inc.	Manufacturing / Manufacturer of plasma cutting systems	USA	Zero-day vulnerability Personal data leakage Ransomware	March 13, 2026 August 9, 2025 Clop
OSI Systems, Inc.	Electronics, manufacturing / Electronic systems and components manufacturer	USA	Personal data leakage Ransomware	March 11, 2026 December 23, 2025 INC Ransom
QualiChem, Inc.	Manufacturing / Metalworking fluid manufacturer	USA	Personal data leakage Ransomware	March 10, 2026 October 23, 2025 Nitrogen
Segue Manufacturing Services LLC	Electronics, manufacturing / Electronics manufacturer	USA	Personal data leakage Ransomware	March 20, 2026 January 22, 2026 Qilin
Capital Star Oil & Gas	Energy / Oil and gas company	USA	Personal data leakage Ransomware	March 17, 2026 November 3, 2026 Dragonforce
Durvet, Inc.	Manufacturing / Animal health product manufacturer	USA	Personal data leakage Ransomware	March 17, 2026 October 17, 2025 Qilin

Palacios Marine & Industrial Coatings, Inc.	Construction and engineering / Coatings for marine and industrial applications, serving heavy industry	USA	Personal data leakage	March 30, 2026 September 30, 2025
Alliance Industrial Refrigeration Services, Inc.	Construction and engineering / Construction and maintenance of large-scale industrial refrigeration and HVAC system	USA	Personal data leakage	March 26, 2026 December 25, 2025
Master Millwork, LLC	Manufacturing / Millwork manufacturer	USA	Personal data leakage	March 30, 2026 February 1, 2026
Lohmann Corporation	Manufacturing / Adhesive product manufacturer	Germany	Personal data leakage Ransomware	March 13, 2026 January 27, 2026 INC Ransom
A&D Technology	Manufacturing / Testing solutions for mobility industries	USA	Personal data leakage	March 16, 2026
Royal Chemical Company	Chemicals, manufacturing / Chemical manufacturing company	USA	Personal data leakage Ransomware	March 24, 2026 April 25, 2025 Lynx
TSU One Holdings, LLC	Utilities / Utility installation and maintenance services	USA	Personal data leakage	March 25, 2026

Tyree Oil Inc.	Energy / Fuel distribution company	USA	Personal data leakage Ransomware	March 7, 2026 Play
Hingham Municipal Lighting Plant	Utilities / Electric utility	USA	Personal data leakage	March 3, 2026
MAKI Building Centers, Inc.	Manufacturing / Manufacturer of vinyl windows, doors, moldings, fencing, railing and patio doors	USA	Personal data leakage Ransomware	March 4, 2026 October 15, 2025 Interlock
O. Berk Company of New England LLC	Manufacturing / Manufacturer of packaging products	USA	Personal data leakage Ransomware	March 6, 2026 January 20, 2026 Qilin
Structural Component Systems	Manufacturing / Manufacturer of roof trusses, floor trusses and prefabricated wall panels	USA	Personal data leakage Ransomware	March 6, 2026 January 16, 2026 Securotrop
TOMCO2 Systems Company	Manufacturing / Manufacturer of CO2 and Dry Ice equipment solutions	USA	Personal data leakage	March 19, 2026
National Coatings, Inc.	Construction and engineering / Industrial coatings and sandblasting services	USA	Personal data leakage Ransomware	March 19, 2026 Play
Brock Built Homes	Construction and engineering / Homes construction	USA	Personal data leakage	March 26, 2026
Data Graphics Inc.	Manufacturing / Manufacturer	USA	Personal data leakage	March 5, 2026 DragonForce

	of quality nameplates, overlays and labels		Ransomware	
TC Controls and Services, Inc.	Construction and engineering / Project management, electrical wiring, and civil engineering services	USA	Personal data leakage	March 13, 2026 August 6, 2025
MESA Products, Inc.	Manufacturing / Manufacturer of cathodic protection systems	USA	Personal data leakage	March 30, 2026
Pyramid ETC Companies, LLC	Construction and engineering / General contractor construction company	USA	Personal data leakage Ransomware	March 5, 2026 Akira
American Vintage Home	Construction and engineering / HVAC and plumbing company	USA	Personal data leakage Ransomware	March 14, 2026 Akira
Glenmark Pharmaceuticals Inc.	Pharmaceutical, manufacturing / Pharmaceutical manufacturing company	USA	Personal data leakage Ransomware	March 27, 2026 INC Ransom
TriMed, Inc.	Manufacturing / Medical equipment manufacturing company	USA	Personal data leakage Ransomware	March 27, 2026 Lynx
Titan Roofing	Construction and engineering / Commercial roofing company	USA	Personal data leakage Ransomware	March 20, 2026 October 31, 2025

Mutti USA Inc.	Food and beverage, manufacturing / Food processing company	USA	Personal data leakage Ransomware	March 25, 2026 September 13, 2025 Clop
Accu-Tube LLC	Manufacturing / manufacturing of tubing	USA	Personal data leakage Ransomware	March 27, 2026 December 6, 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