Kaspersky ICS CERT

kaspersky

A brief overview of the main incidents in industrial cybersecurity Q4 2024

08.04.2025

Version 1.0

In Q4 2024, 107 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

- Total of 107 incidents publicly confirmed by victims.
- At least half of the victims (50%) were **affected by a ransomware attack**.
- 12% of all victims reported a **denial of operations** and 19% reported a **denial of IT systems** as a result of an incident.
- 31% of all victims reported a **denial of operations** and 29% reported a **denial of IT systems** as a result of an incident.
- **Countries with the highest number of confirmed incidents:**
  - USA –81% (87 incidents)
  - Germany – 6% (7 incidents)
  - Japan – 4% (4 incidents)
- This quarter, we saw incidents in certain countries where we rarely see public confirmation of incidents: **Costa Rica, Luxembourg, Latvia, Burkina Faso, and Pakistan.**
- We'd like to draw special attention to the following:
  - We know that cyberattacks harm businesses. Combined with other kinds of problems, a cyber incident can push company management over the edge to announce insolvency. Two such announcements were made this quarter, both victims manufacturing companies (one from Germany and the other from the U.S.).
  - Cyberattacks on key product or material suppliers may have consequences potentially devastating for the entire sector. In one case, incident responders claimed they had contained the incident impact and prevented major devastation.
  - Significant cybersecurity resources don't always mean the company can relax. At least three well-known global companies confirmed they had been hacked this quarter, confirming no one is 100% secure.
  - At least three organizations related to critical infrastructure experienced denial of internal and public services as the result of an attack. In one case, the utility had to switch to manual operations.

    - An attack on a fleet management product and service provider led to denials of service to its customers, one of which was the British DHL subsidiary.
    - Trains were delayed and certain digital customer services disrupted because of an attack on a Pittsburg public transportation company.
    - In two cases, two different ransomware gangs claimed responsibility for the same hack this quarter.
- For the full list of incidents confirmed by victims in Q4 2024, please refer to the Appendix.

October

- Dynapar
- Foley Material Handling Company Inc.
- Sierra Construction Company, Inc.
- Saeilo Enterprises, Inc.
- Industrial Scientific Corporation
- Dover Motion
- Pacific Scientific Energetic Materials Company LLC
- Setra Systems, Inc.
- Advanced Sterilization Products, Inc.
- American Water Works Company, Inc.
- Fluke Corporation
- TDX Construction Corporation
- Casio
- Kulicke and Soffa Industries
- Aero Simulation Inc.
- The Plastic Bag Company
- Polar
- Hubergroup
- Nidec
- Karat Packaging Inc.
- Yorozu
- Eastern Shipbuilding Group
- Saneamento Básico do Estado de São Paulo (Sabesp)
- MMI Services Inc.
- Wise Construction Corporation
- Berry Bros. General Contractors, Inc.
- S. Lichtenberg & Co
- Van Wingerden International, Inc.
- Rogers Foam Corporation
- Stadtwerke Burg
- EPI Breads
- Wright Consulting Engineers, LLC
- Elastec, Inc.
- SelectBlinds
- Microlise Group PLC

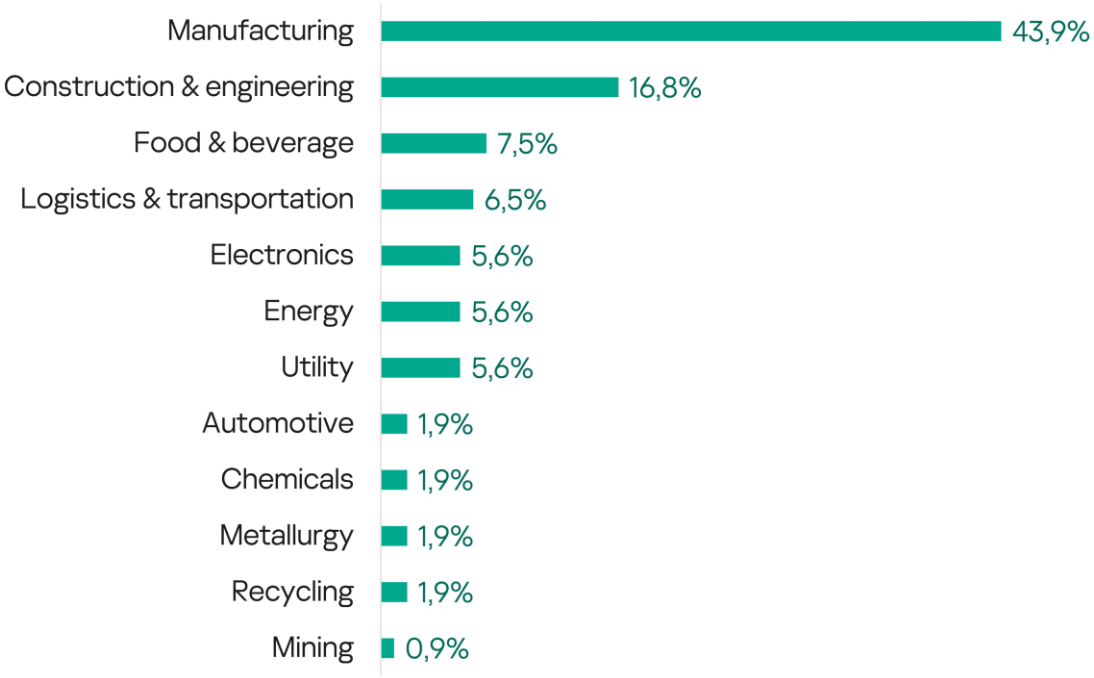
November

- Kemlon Products & Development Group
- Mauser Packaging Solutions
- TetraSoft
- Great Star Tools USA Inc.
- The Manual Woodworkers and Weavers Inc.
- Schneider Electric
- Diligent Delivery Systems
- Fiskars Group
- Phoenix Footwear Group
- Denkai America Inc.
- Newpark Resources, Inc.
- English Construction Company
- J.S. McCarthy Co., Inc.
- American Construction Corp.
- Misionero Vegetables
- Pallet Logistics of America
- Tibber
- Harmac Medical Products Inc.
- SOFITEX
- Kreisel GmbH & Co.
- Mark Cerrone Inc.
- American Gypsum LLC
- VOSSKO
- Dome Construction Corporation
- ShoreMaster, LLC
- Tedder Industries LLC
- Dynamic Air Inc.
- Ariel Corporation
- Graphique De France LTD
- RECOPE
- Eichelberger Construction Inc.
- New River Electrical Corporation
- Universal Pegasus International LLC
- Medion AG
- Stoli Group USA/Kentucky Owl
- Dewan Farooque Motors Limited

December

- BNBuilder
- Fermented Food Holdings Inc.
- ENGlobal
- Overseas Shipholding Group Inc.
- Delmar
- American Engineers Inc.
- Crowley Maritime Corporation
- Wheels Manufacturing, LLC
- Kurita America Inc.
- Artivion, Inc.
- Electrica Group
- Rumpke
- Ames Goldsmith Corporation
- Krispy Kreme Inc.
- Maggie Sottero Designs
- Hyperice Inc.
- OLA Consulting Engineers
- Keeco, LLC
- Pier Foundry & Pattern Shop Inc.
- Pirelli Tire LLC
- Fitzemeyer & Tocci Associates, Inc.
- PS Logistics
- Norwex USA, Inc.
- General Dynamics, Corp.
- R. Zoppo Corp.
- DBM Global, Inc.
- Pittsburgh Regional Transit
- Hubbard-Hall Inc.
- CR&R Inc.
- Ingenieurbüro Fritz Spieth Beratende Ingenieure GmbH
- Peikko
- Tycon Medical Systems, Inc.
- Troxler Electronic Laboratories Inc.
- Central Valley Meat Co, Inc.
- LBX Company LLC

2024



Attacks leading to insolvency

Kreisel

Manufacturing

Denial of operations, insolvency

Ransomware

German bulk material handling company Kreisel GmbH & Co. filed for insolvency on November 19, 2024. The company's current financial difficulties are primarily due to increased financing costs and a deterioration in earnings due to the consequences of COVID, an increase in raw material and energy prices, and a cyberattack that occurred in February. The cyberattack limited the company's ability to operate for several weeks in the first quarter of 2024. According to German press, the blackmail letter was sent by fax and the company didn't pay the ransom. No other details are known about the cyberattack or which group claimed responsibility.

Stoli Group

Manufacturing, food and beverage

Denial of operations, denial of IT services, data leakage, bankruptcy

Ransomware

Stoli Group USA and Kentucky Owl, U.S.-based subsidiaries of the Luxembourg-based vodka manufacturer Stoli Group, filed for Chapter 11 bankruptcy on November 29, months after a ransomware attack disrupted their operations. In August 2024, Stoli Group's IT infrastructure suffered severe disruption in the wake of a data breach and ransomware attack. The attack caused substantial operational issues throughout all companies within the Stoli Group, including Stoli USA and Kentucky Owl, due to Stoli Group's enterprise resource planning (ERP) system being disabled and most of Stoli Group's internal processes (including accounting) needing to be carried out manually. According to the filing, these systems will be fully restored no earlier than Q1 2025, and the cyberattack was among several factors leading the companies to seek relief. The incident also prevented Stoli U.S. subsidiaries from providing financial reports to lenders.

Biggest impact prevented by responders

TetraSoft

Energy, mining

Denial of operations and services, supply chain / trusted partner

A targeted cyberattack on TetraSoft, a Russian company that provides remote monitoring of hydrocarbon production and drilling, was detected and stopped. The Positive Technologies expert security center team investigated and responded to the incident, thus preventing any impact on the Russian mining industry. The incident was classified as a supply chain attack targeting the mining industry. If successful, the attack could have potentially resulted in interruptions in hydrocarbon supplies under domestic and international contracts. The

investigation revealed that initial penetration took place in July 2024, with the first attacker activities in the systems dating back to late September and early October 2024. The attack was carried out using a set of utilities, including remote access control and remote server management tools. Direct damage from downtime at TetraSoft is estimated at over RUB 65 million, and the cost of restoring internal services have already exceeded RUB 25 million. The company did not consider this figure to be final.

Incidents at large organizations

Schneider Electric

Energy, manufacturing

Personal data leakage

Ransomware

On November 4, French energy management and automation solutions company Schneider Electric confirmed a cyberattack involving unauthorized access to one of its internal project execution tracking platforms hosted in an isolated environment following claims by the Grep (Hellcat) group of an incident involving the theft of 40 GB and a ransom demand. Schneider Electric launched an investigation into the incident and audited its internal platforms. The company said its products and services remained unaffected. In a conversation with BleepingComputer, Grep group said they breached Schneider Electric's Jira server using exposed credentials. Once they gained access, they claimed to use a MiniOrange REST API to scrape 400,000 rows of user data, which Grep said includes 75,000 unique email addresses and full names for Schneider Electric employees and customers.

Medion

Manufacturing, electronics

Denial of operations, denial of IT systems, data leakage

Ransomware

German electronic products supplier Medion AG, a subsidiary of Lenovo, a Chinese multinational technology company, became the target of a cyberattack. The Black Basta ransomware group claimed responsibility for the attack on Medion on December 18. The attackers claimed on their data leak website to have stolen around 1.5 TB of data, including financial and accounting data, project files, development data and personal data of employees. Medion initially acknowledged an IT incident caused by unknown external attackers in a statement on November 28, but later deleted it. It said that internal systems and its store activities were partially affected. The team worked with external specialists to resolve the situation, clean up the systems, and clarify the causes. The company was in close contact with the responsible authorities but was only available by telephone to a limited extent and written inquiries couldn't be processed. On December 20, Medion sent a statement to the Golem.de editorial team that the company had experienced IT disruptions on November 26 due to a

ransomware attack that partially affected internal systems and shop operations for a few days. The BKA and Cologne public prosecutor's office investigated the case. It has been established that a criminal cyber group had penetrated parts of Medion's IT system and exfiltrated company data. Although some data was published on the darknet, it was not personal customer data, according to the company's statement. On December 20, the company issued a statement on its website informing that its IT systems were fully operational again following the disruption, the company was fully available by phone, and written inquiries will also be answered again. The delivery of orders could be subject to delays.

Casio

Manufacturing, electronics

Data leakage, personal data leakage, denial of services, denial of IT systems

Ransomware

Japanese electronics group Casio Computer Co., Ltd. confirmed a ransomware attack that allowed unauthorized parties to access its network, resulting in system outages and some services being unavailable to customers. The company said the intrusion into its network occurred on October 5 and that it promptly reported the incident to the relevant authorities and engaged cybersecurity experts to conduct a thorough investigation. Casio Computer Co., Ltd. has taken steps to strengthen its security and protect customer data, and is committed to improving its security protocols to prevent similar incidents in the future. According to Casio's statement, the attackers may have accessed personal information of employees, contractors, business partners, and people who interviewed with the company, as well as sensitive company data including invoices, human resources files, and some technical information belonging to the company, as reported to the Personal Information Protection Commission. In an update on October 21, the company said the ransomware attack had caused significant delays in the delivery of items requested for repair, and many items were backlogged. Casio Computer Co., Ltd. temporarily suspended the acceptance of repairs for its personal products and aimed to restore the system by the end of November.

Critical infrastructures under attack

Brazil Saneamento Básico do Estado de São Paulo

Water supply, utility

Denial of IT systems and services

Ransomware

The Saneamento Básico do Estado de São Paulo (Sabesp) water utility company (Brazil) specializing in water transport and wastewater treatment was the victim of a cyberattack as confirmed in an email to CISO Advisor Brazil on October 22. According to the note, the company immediately adopted all security and control measures and implemented its plan to restore the affected systems. No compromise of personal data has been identified. Water supply and sewage collection and treatment operations were not affected by the cyberattack. Sabesp undertook the necessary efforts to regularize the integrity of the entire digital network system. The company reported that waiting times for service may be above average at certain times due to system instability.

According to news published on the website of Sintaema, the São Paulo sanitation worker union, it received a complaint that Sabesp experienced an internet blackout starting October 17. Sintaema's management explained that since October 17, only the Reservoir Control System was working and other systems could only be accessed by workers online on their cell phones or external networks. Even Poupatempo, a government service that offers 400+ services related to official documents, was at a standstill for five days due to the blackout, which affected all Sabesp units across the country. The RansomHouse ransomware group claimed responsibility for the attack on Sabesp.

Refinadora Costarricense de Petróleo

Energy, utility

Denial of operations and services

Ransomware

Costa Rican energy provider Refinadora Costarricense de Petróleo (RECOPE) confirmed that it was the victim of a ransomware attack on November 27 that forced the organization to switch to manual operations, but assured the public that fuel distribution would not be affected. The company said they were forced to conduct fuel sales manually because of the attack, which took down all digital systems used to facilitate payments. Operations at tanker terminals were extended late into the night on November 27 and expanded on November 28. RECOPE added that it was working with the country's Ministry of Science, Innovation, Technology and Telecommunications (MICITT) to resolve the situation. On November 29, the President of RECOPE said cybersecurity experts from the U.S. arrived on Thanksgiving Day and were able to help gradually restore certain systems, but said the organization will continue to operate systems manually until it is fully guaranteed that processes are safe. The company saw a spike in fuel sales due to concerns about the potential for gas and oil scarcity.

Throughout the weekend, RECOPE extended hours to facilitate the sale of fuel. On November 30, RECOPE reported on the stabilization of service at terminals and guaranteed fuel supply. The company, MICITT, international experts and the DIS (Directorate of Intelligence and Security) continued to work together to address the incident. The RansomHub ransomware group claimed responsibility for the cyberattack against RECOPE.

Electrica Group

Energy, utility

Denial of services

Ransomware

Romanian electricity distributors Electrica Group announced on December 9 that it faced a cyberattack and worked closely with national cybersecurity authorities to manage and resolve the incident. The Group emphasized that its critical systems had not been affected, and any disruptions in interactions with consumers were the result of protective measures for internal infrastructure. All specific response protocols were activated in accordance with internal procedures and current regulations. The Minister of energy told a Romanian news channel that the company was the victim of a ransomware attack that did not impact Electrica's SCADA systems. The Romanian National Cybersecurity Directorate (DNSC) said on December 11 that the Lynx ransomware gang breached Electrica Group. It also said that based on available data, critical power supply systems had not been affected and were operational, and the investigation was ongoing. It provided a YARA rule and indicators of compromise to help other security teams detect signs of compromise on their networks.

A report from the Center for Internet Security (CIS) highlighted the growing threat of ransomware attacks targeting utility organizations, with a particular focus on the activities of the Lynx ransomware group (tracked by Microsoft as Storm-2113), providing its Indicators of Compromise.

Other major incidents of interest

Microlise

Transportation, logistics

Denial of IT systems, denial of services

Ransomware

Microlise, a British telematics and fleet management solution provider, was affected by the cyberattack known to have disrupted DHL's store deliveries for the retailer NISA. According to NISA's message, the attack led to the complete wiping of servers dedicated to the tracking system used by DHL. A DHL spokesperson confirmed the incident but said that it did not affect DHL-owned systems. NISA explained that due to the cyberattack, DHL had no visibility of the progress of any of its deliveries. Motor Transport wrote that it was aware of other companies affected by the security breach, but neither they nor other

companies relying on Microlise software responded to requests for comment. According to Financial Times, Serco, which handles the transport of prisoners for the Ministry of Justice, has seen vehicle tracking, panic alarms, navigation, and notifications related to estimated arrival times disabled. In a filing with the London Stock Exchange on October 31, Microlise said it had detected unauthorized activity on its networks disrupting a large portion of its services and rendering them inactive. In an updated filing with the London Stock Exchange on November 18, Microlise said it had notified international authorities regarding the exfiltration of corporate data from its HQ and continued to work with law enforcement regarding the incident. The company stressed that no customer systems data was compromised. The SafePay ransomware group claimed responsibility for the attack on Microlise.

Pittsburgh Regional Transit

Transportation

Denial of operations, denial of services, personal data leakage

Ransomware

Pittsburgh Regional Transit investigated a ransomware attack that the company detected on December 19 causing disruptions to public transportation. While rail service experienced temporary disruptions on the morning of December 19, transit services operated normally. Other rider services remained negatively impacted, including PRT's Customer Service Center, which was temporarily unable to accept or process senior and child ConnectCards. Local news outlets reported that trains were delayed by more than 20 minutes due to the ransomware attack. Pittsburgh Regional Transit's investigation into the ransomware attack revealed that personal data, including the Social Security Numbers and driver's license numbers of job applicants and past and current employees may have been compromised. Law enforcement was involved in the response and the investigation began in collaboration with cybersecurity experts.

Two ransomware groups claiming an attack

Nidec

Manufacturing

Data leakage, personal data leakage

Ransomware

Japanese electric motor manufacturer Nidec confirmed that various types of business and internal documents were stolen in an August 2024 ransomware attack. According to the company's news releases on its website, the incident impacted its Vietnam-based subsidiary Nidec Precision (NPCV) and was discovered after the attackers contacted Nidec to demand a ransom payment. The ransomware attack was limited to NPCV's network and was not followed by

other intrusions. According to the company, the threat actors stole a total of 50,694 files from NPCV, including internal documents related to green procurement, health and safety, policies, and transactions, as well as emails from business partners. Nidec also noted that the intrusion likely occurred after the attackers obtained the user ID and password of an NPCV general domain account and used them to log in to the server and view files the account was authorized to access. In response, Nidec and its subsidiaries conducted a thorough investigation, reviewed server access rights, and changed passwords. NPCV also suspended the use of the VPN application believed to have been used as part of the attack. In September, the NPCV filed a notification with the Department of Cybersecurity and High-Tech Crime Prevention and Control of the Ministry of Public Security of Vietnam in accordance with the Personal Information Protection Act.

Both the 8base and Everest ransomware groups listed the company on their leak sites in June and August, respectively. Nidec's incident notice suggests that Everest was behind the extortion attempt, as the group leaked data purportedly stolen from the company in early August.

CR&R

Manufacturing, recycling

Dedial of IT systems, personal data leakage

Ransomware

U.S. waste collection and recycling company CR&R Inc. reported to the attorneys general of Maine and Vermont that it had experienced a data breach in which sensitive personal identifiable information in its systems may have been accessed. According to the breach notice, on or about December 13, 2022, a network disruption was experienced that impacted certain systems. CR&R launched an investigation that was completed on October 30, 2024. The company confirmed that sensitive personal information in its systems may have been compromised by an unauthorized third party during the incident on October 19, 2022. As a result, CR&R began a review of the data to determine what information had been impacted and identify the specific individuals affected. CR&R has not publicly disclosed the exact nature of the personal information that may have been exposed. On December 26, 2024, CR&R began mailing data breach notification letters to impacted individuals. Vice Society ransomware group claimed responsibility for the attack on CR&R on November 6, 2022. A month later, in December 2022, BlackCat/ALPHV ransomware group also included CR&R among its victims.

Attacks leading to denial of operations

Hubergroup

Manufacturing

Denial of operations, denial of IT systems and services

German printing ink manufacturer Hubergroup was the target of a cyberattack. According to local media, the company's SAP system, internet access and production were restricted for nearly two weeks. Hubergroup confirmed the incident to the media, but remained vague about the exact impact – including on the site in Celle, Germany. The spokesperson said that a malware attack had affected individual, regional IT systems and emphasized that the company's security systems had reacted immediately. Thanks to these measures, large parts of the internationally active Hubergroup were not affected by the attack. For security reasons, the affected systems were temporarily isolated to prevent the attack from spreading further. Since then, the Hubergroup IT team has been working intensively with external cybersecurity experts to restore the regional systems as quickly as possible. Customers and employees were informed immediately after the incident that there may be temporary restrictions on exchanges and short-term delays in production and delivery.

Artivion

Manufacturing

Denial of operations and services, data leakage

US medical device manufacturer Artivion, Inc. reported a data security incident in a form 8-K filing with the United States Securities and Exchange Commission (SEC) on December 9. The incident occurred on November 21. The incident involved the acquisition and encryption of files. The company's response measures included taking certain systems offline, initiating an investigation, and engaging external advisors, including legal, cybersecurity, and forensics professionals to assess, contain, and remediate the incident. Artivion, Inc. worked to securely restore its systems as quickly as possible and evaluate any notification obligations. The company continued to provide its products and services to customers, but the incident caused disruptions to some ordering and shipping processes and certain corporate operations, which were largely mitigated. Artivion, Inc. remained subject to various risks as a result of the incident, including the impact of delays in recovery, so could provide no assurances that the incident would not have a material impact in the future.

Peikko

Manufacturing

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

Ransomware

Finnish building materials manufacturer Peikko experienced a cyberattack in late December. According to the company's statement on December 30, its websites, emails, and phones were working normally as were its Peikko Designer design tools, but there were a number of tools and systems Peikko employees could not use. On December 31, the company said its recovery efforts from the attack were progressing. The company said it was able to operate safely with the Tekla 3D modelling software. It was also able to work in the cloud with customers through the Tekla Model Sharing collaboration tool. Peikko had limited manufacturing activities and deliveries in some of its 12 factories. In addition, the company said there was a possibility that some customer-related data may have been accessed and stolen during the cyberattack. On January 2, Peikko said it was operating with its Microsoft D365 ERP in 21 countries. Some additional features of the system remained limited, but the system was functioning in all those countries. Peikko was able to manufacture and ship products, and there were some countries where Peikko operated normally with an older ERP system without any issues, while in some countries Peikko was forced to operate manually. On January 9, Peikko released an update stating that operations at Peikko units had returned to normal. The company reported the cyberattack to the police and other relevant authorities, including the National Cyber Security Centre in Finland. Peikko was added to the Akira ransomware gang data leak site on January 10, with 30 GB of data allegedly stolen.

Newpark

Energy, construction

Denial of operations, denial of IT systems

Ransomware

Newpark Resources, Inc., a US-based provider of oil drilling fluid systems and composite matting systems, detected a ransomware cybersecurity incident on October 29 in which an unauthorized third party gained access to portions of its internal information systems. The ransomware attack caused disruptions and limited access to certain parts of Newpark's information systems and business applications supporting aspects of its operations and corporate functions, including financial and operational reporting systems. The company's manufacturing and field operations continued in all material respects, utilizing established downtime procedures. Newpark Resources, Inc. reported the incident in a Form 8-K filing with the United States Securities and Exchange Commission.

VOSSKO

Manufacturing, food and beverage

Denial of operations, denial of IT systems

Ransomware

On November 14, German poultry company VOSSKO fell victim to a targeted cyberattack involving the use of ransomware, which encrypted the internal systems and databases. The malware affected operations, but affected systems and production were subsequently restored. After the incident, the internal IT department and several external specialists worked closely together to resolve the situation. The police and the State Criminal Police Office, including IT experts and forensics professionals, were also involved in the investigation in the first few days after the attack. The Black Basta ransomware group claimed to have breached VOSSKO. Allegedly, 800 GB of data were exfiltrated, including financial data, employees' personal data, projects, and personal documents.

Ingenieurbüro Fritz Spieth

Construction, engineering

Denial of operations, denial of IT systems

Ransomware

German engineering firm Ingenieurbüro Fritz Spieth Beratende Ingenieure GmbH was the victim of a targeted cyberattack. Immediately after discovering the attack, company management informed the authorities and filed a complaint. At the same time, all IT systems were shut down or isolated to protect customers, suppliers and employees. The company returned to normal operations through consistent implementation of an emergency protocol and IT contingency plan. According to the assessment of independent IT experts, there was no evidence that the portals and emails posed an increased risk. The Safepay ransomware group added Ingenieurbüro Fritz Spieth Beratende Ingenieure GmbH to its list of victims on November 19.

Attacks leading to denial of IT systems

Stadtwerke Burg

Energy, utility

Denial of IT systems and IT services

Stadtwerke Burg, a German utility company, posted a message on its website on October 29 announcing that it was back online and available via email and its online service center following a cyberattack. On August 22, in response to a cyberattack, the energy company immediately deactivated access to all IT services and isolated the affected IT systems. Working with IT service providers and IT forensics experts, the IT systems were thoroughly checked and restored. The company stated in an October message that almost all systems were back in operation. The supply of energy to its customers was uninterrupted and personal data continued to be protected. As a result of this incident, the company will further strengthen the already high level of protection of its IT

systems through additional measures, such as introducing even stricter rules for passwords and raising awareness of the careful handling of email attachments. According to an earlier statement from the municipal utility company, the market communication systems were particularly affected. It was temporarily impossible to switch from another energy supplier to Stadtwerke Burg.

ENGlobal

Construction, engineering, energy

Denial of IT systems

US specialty engineering services company ENGlobal Corporation, designer of automated control systems and a major contractor for the energy industry, discovered on November 25 that it had experienced a data security incident. On December 2, ENGlobal reported the incident in a Form 8-K filing with the United States Securities and Exchange Commission. The company's preliminary investigation revealed that a threat actor illegally accessed ENGlobal's information technology system and encrypted some of its data files. Upon detecting the unauthorized access, the company immediately took steps to contain, assess and remediate the cybersecurity incident, including initiating an internal investigation, engaging external cybersecurity specialists, and restricting access to its IT system. In addition, the company's IT system was limited to essential business operations, and the timing of the restoration of full access to ENGlobal's IT system remained unclear as of the date of the filing.

Dewan Farooque Motors Limited

Manufacturing, automotive

Denial of IT systems, cancellation of board meeting

Pakistani automobile manufacturer Dewan Farooque Motors Limited (DFML) was hit by a cyberattack that corrupted its data and crashed its IT servers, resulting in the cancellation of a board meeting. The company disclosed the development in its notice to the Pakistan Stock Exchange on November 29. DFML stated that the information system and financial data, including that from the first quarter up to September 30, 2024, needed to be restored.

Appendix. Full list of confirmed incidents

Industry	Victim	Profile	Country	Impact features	Date of notification /Incident (if known)	Suspected attackers
Manufacturing	Nidec	Electric motor manufacturer	Japan	Data leakage, personal data leakage Ransomware	October 17 August 12	8base Everest
Manufacturing	Polar	Smartwatch manufacturer	Finland	Data leakage, personal data leakage, denial of IT services	October 11	

Manufacturing	Karat Packaging Inc.	Manufacturer of beverage, foodservice and food packaging products	USA		October 18	
Manufacturing	Hubergroup	Manufacturer of printing inks	Germany	Denial of operations, denial of IT systems and services	October 11	
Manufacturing	Eastern Shipbuilding Group	Shipbuilder	USA	Personal data leakage Ransomware	October 21 February 1	LockBit
Manufacturing	Saeilo Enterprises, Inc.	CNC machining and firearms manufacturer	USA	Personal data leakage Ransomware	October 3 August 8	Metaencryptor
Manufacturing	Rogers Foam Corporation	Custom engineered foam manufacturer	USA	Personal data leakage	October 28 September 23	
Manufacturing	Elastec, Inc.	Manufacturer of oil spill cleanup and surface water pollution equipment	USA	Personal data leakage	October 31 June 4	
Manufacturing	S. Lichtenberg & Co	Manufacturer of curtains, draperies, and home fashion products	USA	Personal data leakage	October 24 August 30	
Manufacturing	SelectBlinds	Manufacturer of blinds and window shades	USA	Personal data leakage	October 31 January 7, 2024	
Manufacturing	Industrial Scientific Corporation	Gas detection equipment manufacturer	USA	Personal data leakage	October 3 January 25, 2023	
Manufacturing	Dover Motion	Automation machinery manufacturer	USA	Personal data leakage	October 3 January 25, 2023	
Manufacturing	Aero Simulation Inc.	Manufacturer of flight simulators for government and military units	USA	Personal data leakage	October 10 February 1, 2023	
Manufacturing	Fiskars Group	Global home designer and manufacturer	Finland USA	Personal data leakage Ransomware	November 6 March 31	Akira
Manufacturing	Phoenix Footwear Group	Footwear manufacturer	USA	Personal data leakage	November 6	
Manufacturing	The Manual Woodworkers and Weavers Inc.	Textile manufacturer	USA	Personal data leakage	November 4 July 4	
Manufacturing	Dynapar	Manufacturer of encoders, resolvers, and condition-monitoring solutions	USA	Personal data leakage	October	

Manufacturing	Pacific Scientific Energetic Materials Company LLC	Critical systems and components manufacturer	USA	Personal data leakage	October 3 January 25, 2023	
Manufacturing	SOFITEX	Cotton textiles manufacturer	Burkina Faso	Denial of IT systems	November 19 November 16	
Manufacturing	The Plastic Bag Company	Bag manufacturer	Australia	Data leakage Ransomware	October 10	Sarcoma
Manufacturing	Harmac Medical Products Inc.	Manufacturer of single-use medical devices	USA	Personal data leakage	November 15 September 13	
Manufacturing	American Gypsum LLC	Building materials manufacturer	USA	Personal data leakage	November 22 May 24	
Manufacturing	ShoreMaster, LLC	Waterfront equipment manufacturer	USA	Personal data leakage Ransomware	November 26 August 4	Akira
Manufacturing	Kemlon Products & Development Group	Electrical connectors, sensors, probes and related components for hostile environments manufacturer	USA	Personal data leakage Ransomware	November 1	Space Bears
Manufacturing	Foley Material Handling Company Inc.	Industrial machinery manufacturer and service provider	USA	Personal data leakage	October May 14	
Manufacturing	Mauser Packaging Solutions	Packaging solutions	USA	Personal data leakage	November	
Manufacturing	Great Star Tools USA Inc.	Tool manufacturer	USA	Personal data leakage	November August 2, 2023	
Manufacturing	Dynamic Air Inc.	Material handling solutions	USA	Personal data leakage	November 27 August 29	
Manufacturing	Tedder Industries LLC	Concealed carry gun holster and accessories manufacturer	USA	Personal data leakage	November 26 August 7	
Manufacturing	Ariel Corporation	Gas compression equipment manufacturer	USA	Personal data leakage	November 27 June 20	
Manufacturing	Artivion, Inc.	Medical device manufacturer	USA	Denial of operations and services, data leakage Ransomware	December 9 November 21	
Recycling, manufacturing	Rumpke	Waste and recycling company	USA	Personal data leakage Ransomware	December 10 July 20	Hunters International
Manufacturing	Peikko	Building materials manufacturer	Finland	Denial of operations and services, denial of IT systems,	December 30	Akira

				personal data leakage Ransomware		
Manufacturing	Kreisel GmbH & Co.	Bulk material handling company	Germany	Denial of operations, insolvency Ransomware	November 19 February	
Manufacturing	Keeco, LLC	Home textile manufacturer	USA	Personal data leakage	December 17 March 28, 2024	
Manufacturing	Maggie Sottero Designs	Bridal gown manufacturer	USA	Personal data leakage	December 12 June 3	
Manufacturing	Norwex USA, Inc.	Cleaning product manufacturer	USA	Personal data leakage	December 23 December 11	
Recycling, manufacturing	CR&R Inc.	Waste collection and recycling company	USA	Denial of IT systems, personal data leakage Ransomware	December 26 October 19, 2022	Vice Society BlackCat/ALPHV
Manufacturing	Tycon Medical Systems, Inc.	Medical equipment manufacturer	USA	Personal data leakage	December 30 October 15	
Manufacturing	Hyperice Inc.	Recovery and movement enhancement products manufacturer	USA	Personal data leakage Ransomware	December 12 June 25	Play
Manufacturing	Wheels Manufacturing, LLC	Production of bicycle components	USA	Personal data leakage	December 6 November 4	
Manufacturing	Pirelli Tire LLC	Tires manufacturer	USA Italy	Personal data leakage	December 19 September 18	
Manufacturing	General Dynamics, Corp.	Aerospace defense shipbuilding	USA	Personal data leakage	December 23 October 1	
Manufacturing	J.S. McCarthy Co., Inc.	Printing and packaging manufacturing	USA	Personal data leakage Ransomware	November 8 October 19	Play
Manufacturing	Graphique De France LTD	Decorative paper and gift wrap manufacturer	USA	Personal data leakage, denial of IT systems	November 27 September 20	
Manufacturing	Setra Systems, Inc.	Industrial sensors and measurement systems manufacturer	USA	Personal data leakage	October 3 January 25, 2023	
Manufacturing	Advanced Sterilization Products, Inc.	Medical equipment manufacturer	USA	Personal data leakage	October 3 January 25, 2023	
Utility	American Water Works Company, Inc.	Water supply	USA	Denial of services, denial of IT services	October 3	
Utility	Saneamento Básico do Estado de São Paulo (Sabesp)	Water transport and wastewater treatment	Brazil	Denial of IT systems and services Ransomware	October 21	RansomHouse
Utility	Stadtwerke Burg	Energy supply	Germany	Denial of IT systems and IT services	October 29 August 22	

Utility	Tibber	Energy supply	Germany	Personal data leakage Ransomware	November 13	888
Utility	RECOPE	Energy supply	Costa Rica	Denial of operations and services Ransomware	November 27	RansomHub
Utility	Electrica Group	Energy supply	Romania	Denial of services Ransomware	December 9	Lynx
Electronics, manufacturing	Casio Computer Co., Ltd.	Electronics group	Japan	Data leakage, personal data leakage, denial of services, denial of IT systems Ransomware	October 8 October 5	
Electronics, manufacturing	Denkai America Inc.	Electronic parts manufacturer	USA	Personal data leakage Ransomware	November 7	Cactus
Electronics, manufacturing	Medion AG	Electronic products supplier	Germany	Denial of operations, denial of IT systems, data leakage Ransomware	November 28 November 26	Black Basta
Electronics, manufacturing	Fluke Corporation	Manufacturer of industrial test, measurement, and diagnostic equipment	USA	Personal data leakage	October 3 January 25, 2023	
Electronics, manufacturing	Troxler Electronic Laboratories Inc.	Manufacturing of testing/quality control measurement equipment for the construction industry	USA	Personal data leakage	December 30 October 29	
Electronics, manufacturing	Kulicke and Soffa Industries	Semiconductor and electronics assembly solutions manufacturer	USA	Personal data leakage Ransomware	October 8 May 12	LockBit
Energy, construction & engineering, logistics & transportation	MMI Services Inc.	Well servicing contractor	USA	Personal data leakage, denial of IT systems	October 23 May 20	
Energy, construction & engineering	Newpark Resources, Inc.	Oil drilling fluids and composite matting systems	USA	Denial of operations, denial of IT systems Ransomware	November 7 October 29	
Mining, energy	TetraSoft	Remote monitoring of hydrocarbon production and drilling	Russia	Denial of operations and services, supply chain/trusted partner	November 1 July	
Energy, manufacturing	Schneider Electric	Energy management and automation	France	Personal data leakage Ransomware	November 4	Grep (Hellcat)
Food & beverage, manufacturing	EPI Breads	Food manufacturer	USA	Personal data leakage Ransomware	October 30 September 17	Play

Food & beverage, manufacturing	VOSSKO	Poultry company	Germany	Denial of operations, denial of IT systems Ransomware	November 22 November 14	Black Basta
Food & beverage, manufacturing	Stoli Group USA/Kentucky Owl	Vodka manufacturer	USA Luxembourg	Denial of operations, denial of IT services, data leakage, bankruptcy Ransomware	November 29 August	
Food & beverage, manufacturing	Amber Beverage Group	Alcoholic beverage manufacturer	Luxembourg Latvia	Ransomware	September 20	RansomHub
Food & beverage, manufacturing	Misionero Vegetables	Food and vegetable manufacturer	USA	Personal data leakage Ransomware	November 11 September 26	Play
Food & beverage, manufacturing	Krispy Kreme Inc.	Doughnut manufacturer	USA	Denial of operations, denial of services, data leakage Ransomware	December 11 November 29	Play
Food & beverage, manufacturing	Fermented Food Holdings Inc.	Food manufacturer	USA	Personal data leakage	December	
Food & beverage, manufacturing	Central Valley Meat Co, Inc.	Meat processing company	USA	Personal data leakage	December 30 May 23	
Construction & engineering	Wise Construction Corporation	Construction and industrial services	USA	Personal data leakage Ransomware	October 23 May 7	Qilin
Construction & engineering	Dome Construction Corporation	Construction company	USA	Personal data leakage Ransomware	November 22 October 19	Play
Construction & engineering	Ingenieurbüro Fritz Spieth Beratende Ingenieure GmbH	Engineering company	Germany	Denial of operations, denial of IT systems Ransomware	December 27	Safepay
Construction & engineering	English Construction Company	Construction company	USA	Personal data leakage Ransomware	November 7 September 27	LYNX
Construction & engineering	Sierra Construction Company, Inc.	Industrial, multi-family, commercial and tenant improvement construction	USA	Personal data leakage Ransomware	October August 14	LockBit
Construction & engineering	BNBuilder	Construction company	USA	Personal data leakage Ransomware	December July 17	Hunters International
Construction & engineering	Wright Consulting Engineers, LLC	Structural engineering and construction company	USA	Personal data leakage Ransomware	October 30 June 17	Akira
Construction & engineering	Mark Cerrone Inc.	Civil construction company	USA	Personal data leakage	November 20 September 7	
Construction & engineering	Eichelberger Construction Inc.	Construction company	USA	Personal data leakage	November 27	

Construction & engineering, utilities, energy	New River Electrical Corporation	Electrical construction company	USA	Personal data leakage Ransomware	November 27 April 30, 2024	ElDorado
Construction & engineering	American Engineers Inc.	Civil engineering company	USA	Personal data leakage Ransomware	December 4 October 22, 2023	LockBit
Construction & engineering	R. Zoppo Corp.	Construction in heavy/civil and underground utility sectors	USA	Personal data leakage Ransomware	December 23 June 19	Abyss
Construction & engineering	American Constructio n Corp.	Construction company	USA	Personal data leakage	November 8 September 4	
Energy, construction & engineering	ENGlobal	Automated control systems designer	USA	Denial of IT systems Ransomware	December 2 November 25	
Energy, construction & engineering	Universal Pegasus Internationa l LLC	Engineering, construction management for the energy industry	USA	Personal data leakage	November 27 June 13	
Construction & engineering	Fitzemeyer & Tocci Associates, Inc.	Construction and engineering services	USA	Personal data leakage Ransomware	December 19 September 14	Abyss
Construction & engineering	DBM Global, Inc.	Construction company	USA	Personal data leakage	December 23 November 12	
Construction & engineering	OLA Consulting Engineers	Engineering solutions	USA	Personal data leakage Ransomware	December 13 November 16, 2023	Play
Construction & engineering	TDX Constructio n Corporation	Design build and general construction	USA	Personal data leakage	October 3 May 5	
Manufacturing, construction & engineering	LBX Company LLC	Construction machinery	USA	Personal data leakage	December 31 September 09	
Construction & engineering, manufacturing	Berry Bros. General Contractor s, Inc.	Facility, pipeline, and marine construction, fabrication	USA	Personal data leakage, denial of IT systems	October 23 August 13	
Manufacturing, construction & engineering	Van Wingerden Internationa l, Inc.	Greenhouse construction and product company	USA	Personal data leakage, denial of IT systems Ransomware	October 25 January 22, 2024	Abyss
Logistics & transportation	Microlise Group PLC	Telematics and fleet management solutions	Great Britain	Denial of IT systems, denial of services Ransomware	October 31	SafePay
Logistics & transportation	Pallet Logistics of America	National supply chain solutions provider	USA	Personal data leakage	November 12 July 25	
Logistics & transportation	Diligent Delivery Systems	Shipping, transport, and logistics delivery services	USA	Personal data leakage Ransomware	November 5 July 8	Embargo
Energy, logistics & transportation	Overseas Shipholding Group Inc.	Energy transportatio n service provider	USA	Personal data leakage Ransomware	December 2 July 31	RansomHub

Logistics & transportation	Pittsburgh Regional Transit	Transportation services	USA	Denial of operations, denial of services, personal data leakage Ransomware	December 23 December 19	
Logistics & transportation	Delmar	Logistics and supply chain management company	Canada	Personal data leakage Ransomware	December 3 November 14	Rhysida
Logistics & transportation	PS Logistics	Transportation and logistics solutions	USA	Personal data leakage	December 19 February 20	
Logistics & transportation	Crowley Maritime Corporation	Maritime supply chain logistics services	USA	Personal data leakage	December 4 September 24	
Automotive, manufacturing	Dewan Farooque Motors Limited	Automobile manufacturer	Pakistan	Denial of IT systems, cancellation of board meeting	November 29	
Automotive, manufacturing	Yorozu	Automotive parts manufacturer	Japan	Denial of IT systems, personal data leakage Ransomware	October 18 October 14	RansomHub
Metallurgy, manufacturing	Ames Goldsmith Corporation	Silver refining and fabrication	USA	Personal data leakage	December 10 October 3	
Metallurgy, manufacturing	Pier Foundry & Pattern Shop Inc.	Foundry	USA	Personal data leakage Ransomware	December 17 April 16	BlackSuit
Chemicals, manufacturing	Kurita America Inc.	Water treatment chemical company	USA Japan	Denial of IT systems, personal data leakage Ransomware	December 7 November 29	3AM (ThreeAM)
Chemicals, manufacturing	Hubbard-Hall Inc.	Specialty chemicals and process solutions	USA	Personal data leakage, denial of IT systems Ransomware	December 24 August 23	Clop

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