Kaspersky ICS CERT

kaspersky

Q1 2024 – a brief overview of the main incidents in industrial cybersecurity

03.06.2024

Version 1.0

In this overview, we discuss incidents caused by attacks on industrial organizations. A separate report is devoted to technical researches of attacks, that have been published during the reporting quarter.

Some links to corporate website pages on which information on incidents was originally published may be broken by time of the report release because the information has been removed from these websites. Still, we keep all the links to emphasize the information below is based on statements made by victim companies themselves.

This overview includes information on the incidents such that either the affected organization or the responsible government officials publicly confirmed the compromise. Compromise reports and claims made by cybercriminal groups only are not discussed on purpose.

Quick stats for the quarter

- A total of **30 incidents** were confirmed by victims. This is in line with previous time periods (60+ publicly confirmed cases per half year).
- **37%** of victims reported **denial of operations or product shipment** caused by the incident – the proportion is almost the same as the previous time period (37.5% for H2 2023).
- Almost half (**47%**) of all incidents resulted in **disruption of the victims' public digital services**.
- The victims belong to the following industries/sectors: manufacturing (including automotive, aerospace, pharmaceutical, food and beverages, clothing, cosmetics and many other sub-sectors), **utility, energy, transportation and logistics, engineering**, and **mining**.
- **2/3** of victims are in the **manufacturing** sector. **50%** of all manufacturing victims reported denial of operations, which is **100%** of all victims that confirmed operational interruption as a result of an attack. Either the sector is less resilient to attacks, or organizations within the sector are simply more honest in their public reporting.
- None of the victims who operate critical infrastructure, such as those in the energy and utility sectors, reported any significant damage – something that we are all used to.
- **The most affected countries are:**
  - **US – 1/6th of all victims**
  - **Germany – 1/6th of all victims**
  - **France, Belgium, Netherlands – 1/10th each.**
- There are some countries from which we rarely see public confirmation of incidents: **North Macedonia, South Africa, Singapore.**

January

- Lush
- Foxsemicon
- Schneider Electric
- Benetton
- Veolia
- Hewlett Packard
- Southern Water
- Muscatine Power and Water

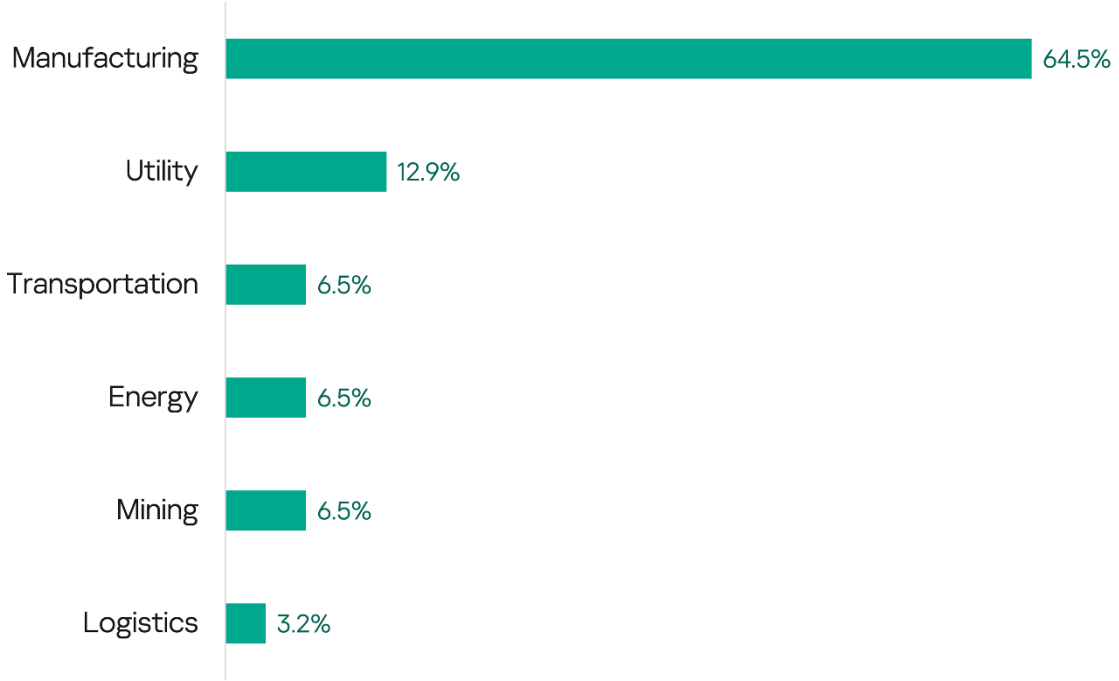
February

- Etesia
- Kind
- Varta
- Aztech Global
- ThyssenKrupp
- AB Texel
- GCA
- HAL Allergy
- Continental Aerospace
- International Paper
- Kampf
- EAS

March

- Koffie Beyers
- Stadtwerke Bruck
- Sprimoglass
- Duvel Moortgat
- MEPSO
- Radiant Logistics
- BerlinerLuft
- Polycab
- Nampak

2024



Manufacturing

Lush hit by ransomware

Manufacturing

Data leakage, denial of IT systems

Ransomware

UK cosmetics manufacturer Lush was the victim of cyberattack, it was reported on January 11. The company took immediate action to secure and screen all systems in order to contain the incident and limit the impact on its business. The company worked with external IT forensic specialists to carry out a thorough investigation. Lush also notified the relevant authorities. The nature of the incident was not initially disclosed. On January 25, Lush's name appeared on the Akira ransomware gang's data leak site. The group said it had stolen 110GB of data from Lush, allegedly including many personal documents such as passport scans, and company documents related to accounting, finance, tax, projects, and customers. On January 29, a Lush spokesperson said in an updated statement that the company had experienced a ransomware incident that resulted in temporary, unauthorized access to part of its UK IT system. The company took immediate steps to respond to the matter and, after a short period of limited disruption, the company was operating largely as normal. The external specialists worked to validate the attackers' claims regarding data they had taken relating to Lush.

Benetton hit by cyberattack

Manufacturing

Denial of IT systems, denial of service and operations

Italian clothing manufacturer Benetton Group was the victim of a cyberattack on the night of between January 18-19, the company announced. The company's e-commerce servers and systems at its logistics hub in Castrette di Villorba were affected. Workers were sent home and logistics operations were disrupted. According to the announcement, for a few days there were disruptions to services due to promptly shutting down the servers to secure the entire IT infrastructure and isolate it from external aggression. The IT intervention group responded immediately by implementing all countermeasures aimed at mitigating the attack, allowing normal operations in almost the entire global commercial network. By Monday January 23, the company expected to resume a significant portion of its operations at all locations.

Varta hit by cyberattack

Manufacturing, automotive

Denial of IT systems, denial of operations

Varta, a German manufacturer of batteries for the automotive, industrial and consumer sectors, disclosed that its systems were affected by a cyberattack on February 12. The incident disrupted production and administrative processes at five of the company's manufacturing plants. Varta shut down its IT systems and disconnected from the internet while it investigated the incident. The company said it had implemented the measures in its contingency plan and formed a task force of cybersecurity experts and data forensic specialists to assist with system recovery. On February 22, Varta issued an update stating that the company's availability was still limited and that there was no information on how long it would take to process and resolve the attack or when production at all five global production sites would be fully operational. The first of the plants were expected to start up again within the following week after the update. Non-IT processes resumed, including the deployment of personnel to all plants for maintenance, servicing and preparatory work. The authorities were informed and the police opened a formal investigation.

Aztech Global hit by ransomware

Manufacturing

Denial of IT systems

Ransomware

Aztech Global, a Singapore-based manufacturing services provider, announced on February 12 that it was the victim of a ransomware cyberattack that allowed cybercriminals to gain unauthorized access to its computer network. The company took immediate action, including shutting down its servers during the Chinese New Year holidays and using cybersecurity software to ensure that no other data was affected. Aztech Global also engaged third-party forensic consultants to investigate the incident and notified the relevant authorities, while seeking advice to strengthen its IT security.

Continental Aerospace hit by cyberattack

Manufacturing, aerospace

Denial of operations

Continental Aerospace, a US aircraft engine manufacturer, fell victim to a cyberattack that disrupted its operations. The company announced on its website banner on February 20 that it was working with experts to resolve the issue and hoped to resume normal operations soon. No further details were provided regarding the end of the attack, the extent of the disruption, or a possible data breach. Continental Aerospace actively engaged with a team of experts to resolve the issues as quickly as possible.

Etesia hit by cyberattack

Manufacturing

Denial of IT systems, services and operations

French mower manufacturer Etesia was the victim of a cyberattack on February 2, according to local press reports, forcing 160 employees to work part-time. The attack disrupted telephone calls, emails and internal manufacturing processes. Since February 20, the company's activities have gradually resumed after being completely blocked.

Kind hit by cyberattack

Manufacturing

Denial of IT systems, denial of services

German hearing aid manufacturer Kind was hit by a cyberattack on February 6. According to a company spokesperson, there were irregularities in the IT system. The company's own IT department began to take security measures. The police and the data protection officer were informed. Communication with more than 600 specialist stores was affected. After the IT failure, contact was only possible by telephone. Orders couldn't be entered directly on computers and were sometimes recorded with pen and paper. There was no evidence that customer data was stolen. The systems were immediately shut down, checked by external specialists, and gradually brought back online.

International Paper hit by cyberattack

Manufacturing

Denial of IT services, denial of operations

Supply chain / trusted relationship

US paper and packaging manufacturer International Paper was hit by a cyberattack, according to a statement. The company initiated response and containment plans, including notifying the appropriate authorities. Out of an abundance of caution, International Paper coordinated an orderly shutdown of the mill to address the issue and at the time of the statement was in the process of restarting the mill. A company spokesperson said the attacker accessed International Paper's system through a third-party vendor and did not directly target the company or the mill. The attack affected only a limited number of manufacturing systems at the Riegelwood mill. No other mills, sites or systems were affected. The company was not aware of any sensitive, proprietary, personnel or business data being compromised.

Polycab hit by ransomware

Manufacturing

Ransomware

Polycab, an Indian manufacturer of cables, wires and related products, was the target of a ransomware attack on its IT infrastructure on March 17. According to a regulatory filing, the incident did not affect the company's core systems and operations. The company's technical team, along with a specialized team of external cybersecurity experts, worked actively on analyzing the incident. On March 26, the Lockbit ransomware group added Polycab to its list of victims on its dark web site.

Nampak hit by ransomware

Manufacturing

Data leakage, personal data leakage, denial of IT systems

Ransomware

South African packaging manufacturer Nampak detected unauthorized activity on its IT systems on March 20. In a statement on its website, Nampak said an unknown third party had gained access to its IT systems despite its robust and embedded security protocols. The company immediately took the necessary steps to contain, assess and remediate the incident. Nampak took the necessary steps to determine the scope of the compromise, restore the integrity of its information systems and ensure that it was not exposed to further risk. The company said the breach had not affected its manufacturing facilities and operations, which continued to function as normal, with some manual systems being used where necessary. Nampak made an initial notification to the information regulator. On March 26, the Lockbit ransomware group added Nampak to its list of victims on its dark web site. On April 4, Nampak issued an update stating that the affected data may include files related to the company's legal, finance and human resources functions. Such files may contain certain personal information relating to individuals and legal entities.

Sprimoglass hit by ransomware

Manufacturing

Denial of services, operations and product delivery

Ransomware

Belgian glass manufacturer Sprimoglass was hit by a cyberattack that halted its production, which became known in early March. According to a local media video, the company knew about the cyberattack on February 23 and was shut down for about 10 days. About six to seven hundred computers had to be completely reformatted. At the time of the video story, a number of production lines had resumed operations three days earlier, and 20-30% of employees had already returned to work, with the rest of the workforce on technical unemployment. The attack had a serious impact on employees, and on customer deliveries, which were postponed. Representatives of the company said that they would begin production properly, step by step, without having to pay a ransom.

BerlinerLuft hit by cyberattack

Manufacturing, engineering

Denial of IT services, denial of operations

German engineering and manufacturing company BerlinerLuft fell victim to a cyberattack on March 16. According to a message on its website, the company became unavailable via its usual telephone numbers and email addresses. The company's team worked to restore normal availability as quickly as possible. The company warned that due to the IT emergency, there may be short-term limitations in business operations, and there would probably be disruptions in the production/manufacturing process and delivery delays. The relevant criminal and state data protection authorities were informed. On March 27, the company issued an update stating that production of duct components, louvre flaps and sound insulation baffles had resumed at its German and Polish facilities and that email and telephone communications had been restored.

EAS hit by ransomware

Manufacturing, engineering

Data leakage, denial of operations

Ransomware

Dutch mechanical engineering and manufacturing company EAS Europe was the victim of a ransomware attack on February 26, according to a notice on its website. The attackers encrypted EAS Europe servers and may have stolen sensitive data from the EAS servers. Customer and supplier data may have been taken. EAS worked with a cybersecurity firm to assess the scope of the incident and to further improve its cybersecurity and data protection. As a result of the incident, operations in the Netherlands were suspended while the company restored the backups. The Qilin ransomware group added EAS change systems to its list of victims on April 6.

Kampf hit by ransomware

Manufacturing

Denial of IT systems

Ransomware

German slitting and winding machines manufacturing company Kampf GmbH was the victim of a cyberattack on February 24 that used special software to partially encrypt its IT systems. According to a message on its website, the company immediately disconnected all external connections and shut down all IT systems. Kampf investigated the extent of the attack with the support of external cybersecurity experts and forensic specialists. The company notified and cooperated with all the relevant authorities. It couldn't rule out the possibility that data had been extracted. In the March 4 update, the company stated that all Kampf Group companies that were taken offline as a precautionary measure were back to normal operations, with the exception of Kampf GmbH and Atlas Converting Equipment Ltd. All other members of the Jagenberg Group were working without restrictions.

Electronics

Foxsemicon hit by ransomware

Manufacturing, electronics

Denial of IT services, data leakage, personal data leakage

Ransomware

On January 15, semiconductor equipment manufacturer Foxsemicon Integrated Technology, a subsidiary of Taiwanese electronics giant Foxconn, was the victim of a cyberattack. The company's website was defaced with a message claiming that data had been stolen and encrypted. The message said 5TB of data had been taken from the company's systems. The cybercriminals claimed to have obtained personal data belonging to customers and employees, and threatened to make it public on their leak website unless a ransom was paid. The ransomware group did not identify itself on the defaced Foxsemicon website, but the links provided to the company pointed to the LockBit Tor-based leak site. Shortly after, the company told the Taiwan Stock Exchange that it had

recovered the website immediately after detecting the ransomware attack and was working with security experts. However, various sections, including the English and Mandarin versions and the corporate and financial sections, remained inaccessible. Foxsemicon also added that the incident should not significantly affect its operations.

Hewlett Packard hit by cyberattack

Manufacturing, electronics

Data leakage

APT

On January 19, Hewlett Packard Enterprise filed a Form 8-K with the US Securities and Exchange Commission (SEC), reporting unauthorized access to the company's cloud-based email environment by a threat actor believed to be Midnight Blizzard (aka Dukes, CozyBear and NOBELIUM/APT29/BlueBravo). HPE was notified of the cyberattack by an unknown entity on December 12, 2023. It is believed that the attackers had been accessing and exfiltrating data since May 2023. Corporate data from a "small percentage" of HPE mailboxes and a "limited number" of SharePoint files belonging to employees in cybersecurity and other business units were accessed and stolen. The company, with the assistance of external cybersecurity experts, immediately activated its response process to investigate, contain, and remediate the incident and eradicate the activity.

Automotive

ThyssenKrupp hit by cyberattack

Manufacturing, automotive

Denial of IT systems, denial of operations

German steelmaker and automotive supplier ThyssenKrupp said in a statement that it suffered a cyberattack that affected its auto body manufacturing division, ThyssenKrupp Automotive Body Solutions. Automotive Body Solutions was able to detect the incident early and start working to contain the threat and mitigate the impact. At the same time, ThyssenKrupp clarified that no other business units or segments were affected. Various security measures were taken and certain applications and systems were temporarily taken offline. A German news agency was the first to reveal the attack, reporting that the incident directly affected ThyssenKrupp's plant in Saarland, which employs more than a thousand workers. The company confirmed to BleepingComputer that production was halted but clarified that deliveries to customers had not been affected.

Pharmaceutical

HAL Allergy hit by ransomware

Manufacturing, pharmaceutical

Data leakage, denial of services, product delivery delay

Ransomware

On February 19, Dutch pharmaceutical company HAL Allergy Group was hit by a ransomware attack, according to a statement on its website. The company may have experienced a delay in processing orders or delivering products. HAL Allergy immediately engaged external cybersecurity experts to help restore the affected network, and a forensic investigation was launched. The company could not rule out the possibility that personal data of individuals may have been compromised. The measures taken by the company included disconnecting the network from the internet, restoring data, notifying the Dutch Data Protection Authority and contacting the Dutch police. The Ransomhouse group added HAL Allergy to its list of victims on the dark web on February 28.

Food and beverages

Duvel Moortgat hit by ransomware

Manufacturing, food and beverages

Denial of IT systems, denial of operations

Ransomware

Belgian brewery Duvel Moortgat confirmed to local press that it fell victim to a ransomware attack. Production was largely halted. The cyberattack was discovered on March 6 at the brewery in the province of Antwerp. The servers were apparently infected with malware and were shut down. A company spokesperson explained that sites in Belgium and a site in the US were affected. The IT department acted immediately and worked to find out exactly what had happened. Production in Antwerp resumed on March 7. The Stormous ransomware group claimed responsibility for the cyberattack on Duvel Moortgat on March 7, saying that 88GB of data was stolen. On March 12, the Black Basta ransomware group also added Duvel Moortgat and Duvel-owned Boulevard Brewing in the United States to its list of victims on its dark web site.

Koffie Beyers hit by cyberattack

Manufacturing, food and beverages

Belgian coffee producer Koffie Beyers was hit by a cyberattack, police confirmed. The investigation was ongoing and it was not clear what the impact of the attack was. The police also investigated whether there was a link to the cyberattack on Duvel Moortgat – the companies were hit around the same time and are based less than a mile apart in the municipality of Puurs-Sint-Amands. It was specified that this was a separate case, but the police said they would compare them to see if there were any similarities.

Utility

Southern Water hit by cyberattack

Water supply, utility

Personal data leakage

Southern Water, a private utility company in the UK, acknowledged that cybercriminals claimed to have stolen data from some of its IT systems. The company said in a statement on January 23 that it had previously detected suspicious activity and had launched an investigation led by independent cybersecurity specialists. It said there was no evidence that customer relationships or financial systems had been affected. The company's services were unaffected and continued to operate normally. Southern Water reported the incident to the government, regulators and the Information Commissioner's Office. The Black Basta ransomware group claimed responsibility for the attack and published a selection of the data it claimed to have stolen, which included scans of identity documents such as passports and driving licenses; documents that appear to be HR-related and which show the personal data of what could be customers, including home and office addresses, dates of birth, nationalities and email addresses; and corporate car-leasing documents containing personal data.

Veolia hit by ransomware

Water supply, utility

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

Ransomware

The North American municipal water division of Veolia, a French transnational utility company, experienced a ransomware incident that impacted certain software applications and systems. The company's IT and security incident response teams mobilized quickly and collaborated with law enforcement and other third parties to investigate and resolve the incident. According to a statement published on January 19, the company implemented defensive measures, including taking the affected back-end systems and servers offline until they could be restored. Water and wastewater system operations were not disrupted by the ransomware attack. Some customers experienced delays when using online bill payment systems. During the investigation, the company identified a limited number of individuals whose personal information may have been compromised.

Muscatine Power and Water hit by ransomware

Water supply, energy, utility

Denial of IT services, personal data leakage

Ransomware

US utility company Muscatine Power and Water (MPW) discovered a cybersecurity incident impacting its corporate network environment. After a brief disruption to the company's corporate business systems and a careful internal and external review, all MPW business systems were restored to an operational state. According to a press release posted on its website on January 29, all office, field, and power generation operations were functioning as normal. The company worked with a team of forensic experts to fully understand the extent and implications of the incident and to restore operations within a secure and remediated network environment. Later, MPW issued an update confirming a ransomware incident identified on January 26. It stated that MPW's team quickly mobilized and deployed new equipment to restore internet services within eight hours. MPW's affected business systems were also restored that same weekend, allowing MPW to conduct normal operations when they opened for business at 8am on the Monday. MPW also notified state and federal law enforcement and regulatory agencies. The forensic investigation revealed that some current and former customer data, such as address, social security number, driver's license, etc., may have been compromised in the incident.

Stadtwerke Bruck hit by cyberattack

Energy, utility

Denial of IT systems, denial of services

Austrian utility company Stadtwerke Bruck discovered a security incident in the IT systems of the municipal utility administration on March 4. According to a message on its website, the affected services were quickly restored and the company was fully operational from March 11. The business data was reconstructed from the data backup. An IT forensic investigation was conducted to determine the nature and progression of the security incident and to determine the appropriate course of action. There was no indication that any data had been removed from the company's systems at the time of notification. For reasons of transparency, an initial preventive report was submitted to the relevant authorities.

Power and energy

MEPSO hit by cyberattack

Energy
Denial of IT systems, denial of IT services

The Electricity Transmission System Operator of the Republic of North Macedonia (MEPSO) confirmed that it was hit by a cyberattack. In a March 7 press release, the company emphasized that the cyber-incident did not target its critical energy infrastructure, which remained secure and fully operational. MEPSO assured that the power grid's integrity and the electricity supply were not compromised. The company reported the cyberattack to the relevant authorities in accordance with cybersecurity regulations. MEPSO's team, in collaboration with cybersecurity experts, worked to mitigate the effects of the cyberattack and normalize the company's day-to-day operations. On March 11, MEPSO announced that its website was up and running. MEPSO stated there was no ransom demand to unlock parts of the hacked information system.

Schneider Electric hit by ransomware

Energy
Data leakage, denial of IT services
Ransomware

BleepingComputer learned that on January 17 a ransomware attack hit the Sustainability Business division of the French multinational energy company Schneider Electric. Schneider Electric was targeted by the Cactus ransomware attack, resulting in the theft of corporate data. The attack disrupted part of Schneider Electric's Resource Advisor cloud platform. In a statement to BleepingComputer, Schneider Electric said the attack was limited to this one division and did not affect other parts of the company. Officials from the sustainability division contacted customers affected by the attack. A detailed analysis of the incident was conducted with leading cybersecurity firms. The company worked to restore operations in the division for the next two days after confirmation. Later, the company issued the same statement on its website, adding that access to business platforms was restored on January 31.

Logistics and transportation

GCA hit by cyberattack

Transportation, logistics
Denial of IT services

French transport and logistics company GCA (Groupe Charles André) suffered a cyberattack during the night of February 17-18, resulting in an interruption of its internet access and the disruption of its usual communications, according to a message sent to its customers. No data leakage was reported,

and the company investigated with external specialists and in conjunction with ANSSI. The usual email addresses, landlines, EDI connections, APIs, became inoperable. GCA didn't specify if the encryption of the systems was observed.

AB Texel hit by ransomware

Logistics

Ransomware

On February 15, Dutch logistics company AB Texel fell victim to the Cactus ransomware group, according to a statement on its website. The recovery process was started immediately. The attack had no impact on the company's services. Operations continued, the company supplied its customers and kept customers and employees informed. The incident was immediately reported to the Dutch Data Protection Authority. AB Texel also planned to report the incident to the police. The Cactus ransomware group added AB Texel Netherlands to its list of victims on February 28.

Radiant Logistics hit by cyberattack

Transportation, logistics

Denial of services

Radiant Logistics, an international freight company, isolated its Canadian operations following a cybersecurity incident. In a filing with the US Securities and Exchange Commission (SEC), Radiant specified that it detected the incident on March 14. Canadian customers experienced delays in service, but service in other countries was not affected. Upon detection, the company immediately initiated its incident response and business continuity protocols and began taking measures to disrupt the unauthorized activity.

Other

Alamos Gold hit by cyberattack

Mining

Data leakage, personal data leakage

Canadian mining company Alamos Gold fell victim to a cyberattack that took place sometime in April 2023. The attack resulted in the public disclosure of confidential corporate data last year, according to a local media report. The data included sensitive information such as social insurance numbers, payroll reports, financial information, and home addresses and mobile phone numbers for senior executives, all of which were published online by the hackers, the report said. The attack was apparently carried out by the Black Basta ransomware group. According to the Alamos statement, the company's operations were not affected at any time, the company remained vigilant in protecting its systems and put measures in place to address any loss of personal information.

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