Kaspersky ICS CERT

H1 2023 – a brief overview of main incidents in industrial cybersecurity

05.10.2023

Version 1.2

In this overview, we discuss cybercriminal and hacktivist attacks on industrial organizations. A separate report is devoted to APT attacks.

Many links to corporate website pages on which information on incidents was originally published are broken because the information has been removed from these websites. Still, we decided to keep the links because the information below is based on statements made by victim companies.

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.

Instead of an Introduction

Ransomware and other criminally motivated attacks have become a plague on industrial organizations around the world. Our report for H1 2022 includes seven cases of hacktivist attacks and 10 cases of criminal ransomware attacks. In H2 2022, this increased to 40 cases of cybercrime incidents, and one hacktivist attack. Now in the current report, we have 67 cybercrime cases. As you can see, the dynamic is far from encouraging.

Keep in mind that in our reports, we normally only focus on publicly disclosed incidents and cybercrimes confirmed officially by the affected organization or state officials. But these only show the tip of the iceberg, as the vast majority of organizations don't advertise the fact that they were compromised and refuse to confirm press reports when they're added to online lists of cybercrime victims. Journalists also usually only react when prominent names appear on these lists, whereas in reality the total number of affected organizations is many times greater. In our opinion, to get a more objective idea of the estimated number of organizations whose data has been put up for sale to the public, take the figures in our reports and multiply them by 10. Then there's the organizations that don't know they've been compromised (because the attackers didn't demand a ransom and didn't publicly post the name of the organization and examples of stolen data), which is at least 10 times larger too. So the real size of the iceberg turns out to be larger than its tip by two orders of magnitude. The overall picture that emerges is quite alarming.

If we stick to the tip of the iceberg and only focus on officially (and publicly!) confirmed data for the first half of 2023, we can make a few observations.

The first observation is the most obvious. Among all organizations that suffered attacks, the *vast majority relate to industrial manufacturing*, which is the most numerous and diverse category of potential victims among industrial organizations. They also have many secrets that potential buyers are willing to pay for, while being less regulated (in the sense of not being able to pay a ransom), and not as zealously protected by the state as, for example, the energy sector (which means less criminal liability for attackers).

In the industrial production sector, a particularly large number of attacked organizations were related to automobile production (a sad fact given the general difficulties facing the automobile market), and the transport industry as the whole, including organizations related to shipbuilding and logistics.

The second major area in the industrial production sector under attack was the production of microelectronics, which is a key industry that affects a large number of markets, including the automotive industry. Here we can see many well-known company names among the victims.

The second important observation is the *sheer variety of real sector industries affected,* including metallurgy, pharmaceuticals, mining, food production, automotive, and many others. We were surprised to see a well-known manufacturer of snowboarding equipment, clothing and gear, and even two manufacturers of firefighting equipment on the list as well. It's likely that the appearance of any organization in these lists, no matter the market or niche, will come as a surprise anymore.

Among the industries not directly related to production, the most affected sectors (by number of victims) were utilities, transport and logistics, oil and gas, and electricity suppliers.

As for the electric power industry as a whole, including manufacturers of specialized equipment and software, as well as suppliers of related services, it was one of the most affected sectors in this half of the year, second only to industrial production.

Our third observation is the *large number of major and recognizable names among victims*. Unfortunately, even big budgets allocated for information security turn out to be insufficient. And since such companies try not to disclose attack details (probably in fear of additional direct losses), it's difficult to judge the real scale of damage based on data from public sources. *Just keep in mind the theoretical possibility of their partners and clients being compromised as well.*

For our fourth observation, many organizations, including at least three major companies*, were compromised through an unpatched vulnerability in two different MFT (Managed File Transfer) products*. These file transfer solutions are used by large organizations, including to keep information "secure" (as their developers claim), yet continue to be a source of security issues for their clients. It's also worth noting that large industrial organizations are often unable to quickly patch dangerous vulnerabilities in the technological networks of their enterprises and on the perimeter of the office network.

Finally, our fifth and last observation. For many industrial organizations, in addition to data leaks and disruptions to internal IT systems, cyberattacks were also a direct cause of unscheduled shutdowns and downtime in the production and shipping of products, in some cases lasting for weeks and resulting in direct losses totaling hundreds of millions of dollars. Today, the risk of a cyberattack on any business has moved into a whole new category and can no longer be ignored by the top officials of any industrial enterprise in any sector and of any type.

2023

January

- DNV
- Morgan Advanced Materials
- Qulliq Energy Corporation
- The Fritzmeier Group
- Exco Technologies
- Solar Industries

February

- Super Bock Group
- Trodat
- Acea
- MKS Instruments
- Lumila
- Laremo
- Vesuvius
- Águas do Porto
- Ziegler
- Gates Corporation
- Burton
- Aker Solutions
- ACER
- Encino Energy
- Trèves Group
- Stiles Machinery
- Rosenbauer Group

March

- STEICO
- FIEGE Logistics
- Groupe SEB
- Hahn Group
- Hitachi Energy
- Puerto Rico Aqueduct and Sewer Authority
- Ferrari
- Storopack
- Rio Tinto
- Western Digital
- SAF Holland

April

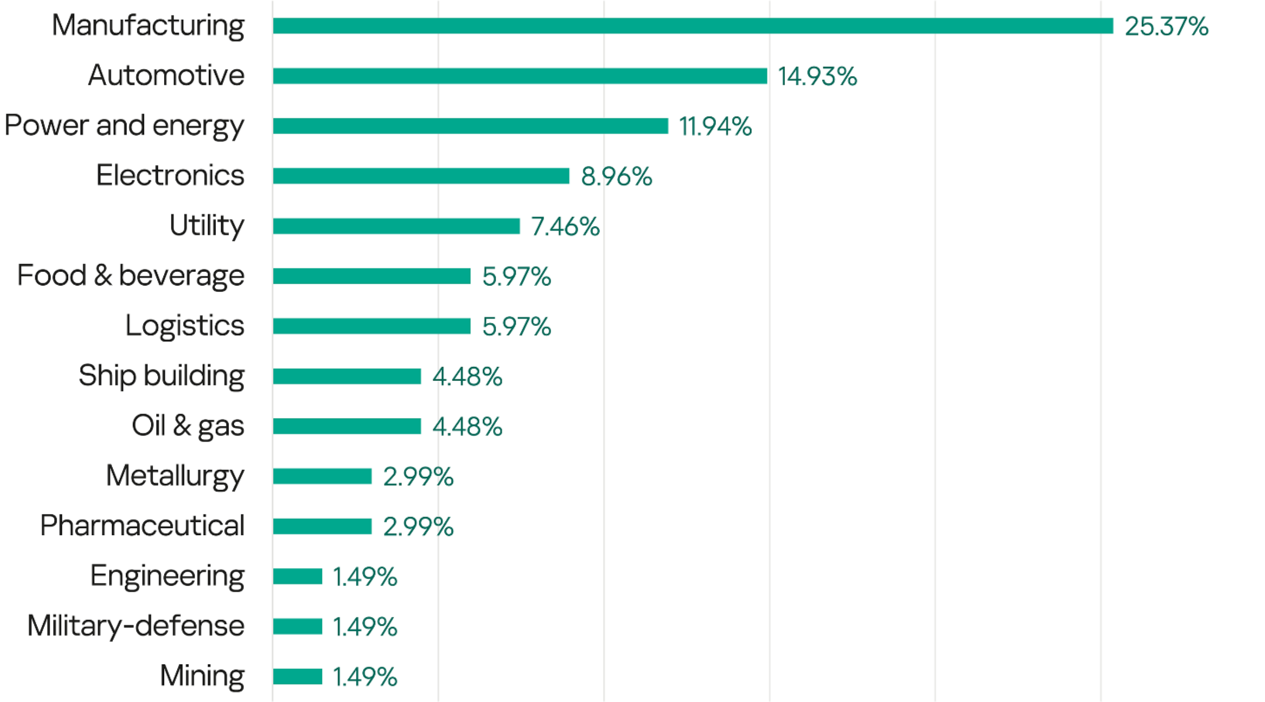
- Bernina
- Anton Paar Group
- Micro-Star International
- Bobst
- Israeli irrigation systems
- Hyundai
- Lürssen
- Fincantieri Marine Group
- Rheinmetall
- Sociedad Eléctrica Del Sur Oeste
- Grupo Nutresa
- Badische Stahlwerke
- Vopak
- Coca-Cola FEMSA
- Alto Calore Servizi

May

- ABB
- Suzuki Motorcycle India
- Lacroix Group
- MPPMC

June

- YKK
- Automatic Systems
- Hep Global
- Eisai
- Haynes International
- Brunswick Corporation
- Yamaha Corporation
- Shell
- Virbac
- Suncor Energy
- Siemens Energy
- Kinmax Technology
- Schwälbchen Molkerei



Manufacturing

Trodat hit by ransomware

Manufacturing

Denial of IT services

Ransomware

Austrian manufacturer of stamps and laser technology Trodat was hit by ransomware that led to the encryption of some servers. A large part of the central IT services was temporarily unavailable at numerous locations around the world. According to the statement, an emergency operation was immediately activated to ensure continuous operation. After the systems were shut down and a detailed forensic system analysis was performed, a "controlled reconstruction" took place. Within a week, the switch was made from emergency to normal operation.

Lumila hit by ransomware

Manufacturing, lighting, railways

Ransomware

French lighting manufacturer Lumila, which provides services to the French railways, was one of the victims of a ransomware attack on February 3 that targeted several French hosting companies, including Scaleway and OVHCloud. The company filed a complaint with the Central Office for Combating Information and Communication Technology Crime (OCLTIC). The extent of the cyberattack was determined and the company worked closely with the relevant authorities to investigate it. All services were restored and operational at the time of the announcement.

Bernina hit by ransomware

Manufacturing

Data leakage, personal data leakage, privacy

Ransomware

Swiss-based Bernina International AG, a leading manufacturer of sewing and embroidery machines, reported that it fell victim to a cyberattack after being added to the victim list of the ALPHV ransomware group. The company immediately initiated the necessary security measures, called in external specialists and involved the relevant authorities. BERNINA did not comply with the ransom demands of the blackmailers. The hackers published the stolen files on the night of April 26, 2023. The ransomware group claimed that the stolen data includes sensitive information, such as customer and client data, employee data and insurance details, NDA contracts and documents, drawings and developments, and bank data and reports.

Anton Paar Group hit by ransomware

Manufacturing

Denial of service, phishing, personal data leakage, privacy

Ransomware

The Austrian manufacturer of laboratory instruments and process measuring systems fell victim to a ransomware attack initiated via phishing emails received on April 6. On April 19, the attackers encrypted approximately 10% of the company's internal PCs and servers. According to a statement on its website, the company immediately took most of its systems and services offline worldwide and worked with the highest priority to get its IT systems up and running again. The company said it was cooperating fully and assisting the authorities and law enforcement agencies in their investigation. The cybersecurity incident resulted in the unauthorized disclosure of personal data in some instances. The Anton Paar Group immediately informed those affected. The Black Basta ransomware group added Anton Paar to the victim list on its dark web site.

Automatic Systems hit by ransomware

Manufacturing

Data leakage

Ransomware

On June 3, Automatic Systems, the Belgian manufacturer of vehicle, pedestrian and passenger access control equipment, discovered a ransomware attack claimed by the notorious ALPHV group. The information about the ransomware attack was posted on the company's website. According to a statement on the company's homepage, Automatic Systems immediately took specific protection measures to halt the advance of the ransomware. The company brought in external cybercrime experts to provide round-the-clock support to internal IT teams. Investigations were underway to assess the nature of the information that may have been made accessible to third parties. Automatic Systems has filed a complaint in Belgium and in France. According to the screenshot shared by Falcon Feeds, the hackers released 121 attachments containing data allegedly from the Automatic Systems data breach. The ALPHV group claimed to have stolen sales data, logistics information, and insurance-related documents, and also claimed to have passwords to accounts and access to various company resources and partners.

Yamaha Corporation hit by ransomware

Manufacturing

Ransomware

The Japanese musical instrument and audio equipment manufacturer announced on June 15 that its US sales subsidiary, Yamaha Corporation of America (YCA), had suffered unauthorized access via a ransomware attack. The company stated in its press release that it immediately removed the network connection of the illegally accessed device. The company also confirmed that its systems in Japan were not affected. There was a possibility that information related to local business partners may have been leaked, and the details were under investigation. The BlackByte ransomware group listed Yamaha Corporation as a victim on its extortion website.

Morgan Advanced Materials hit by cyberattack

Manufacturing

Denial of IT services

UK-based manufacturing company Morgan Advanced Materials was hit by a cyberattack. The exact nature of the attack hasn't been revealed but it is described as a "data security incident". The company said some of its servers were taken offline to contain the attack, leading to limited email service and other network restrictions. A third-party company was brought in to conduct a forensic analysis of the network to better understand the nature of the attack and help prevent further damage to the network.

Fritzmeier Group hit by cyberattack

Manufacturing

Fritzmeier Group, the German manufacturer of plastic assemblies, metalworking and environmental technology, was hit by a cyberattack according to several local media reports. The attack was detected on January 17. All relevant systems were then switched off. Large parts of the production were still operational, but running in emergency mode. Criminal charges were filed and external professional support was brought in to resolve the problem as quickly as possible. According to a spokesperson, the company has also consulted the State Criminal Police Office of Lower Saxony as the central contact point for cybercrime.

Gates Corporation hit by cyberattack

Manufacturing

Denial of IT systems, denial of operations and shipment

On February 11, Gates Industrial Corporation plc, a US manufacturer of fluid power and power transmission technology, determined that it was the target of a malware attack. The company immediately activated its incident response and business continuity plans designed to contain, assess and remediate the incident. The company also initiated an investigation, engaged the services of cybersecurity experts and outside advisors and notified appropriate law enforcement authorities. The attack affected certain of the company's IT systems, and as part of its containment efforts, the company suspended the affected systems and elected to temporarily suspend additional systems. These suspensions resulted in the temporary inability of most of the facilities to produce and ship products. Gates Industrial Corporation subsequently restored production and shipping at some of these facilities and was working to restore the remaining affected systems.

Stiles Machinery hit by cyberattack

Manufacturing supplier

Denial of IT systems

US-based industrial equipment supplier Stiles Machinery Inc. announced on its website that it had detected an attack and shut down its systems to protect them. The notice was still active on the website as of February 22. Out of an abundance of caution, Stiles completely shut down its systems to investigate the situation further. The security and data of customers and business partners is a top priority, officials said, adding that there was no indication of any data loss. Stiles worked to restore operations to full functionality as quickly as possible, but officials said their regular operations and ability to communicate were limited during this time.

Burton hit by cyberattack

Manufacturing

Denial of shipment

Burton Snowboards, a snowboard manufacturer, canceled all online orders following what it described as a “cyber incident” that occurred on February 11. In a separate statement, Burton said that it had started investigating the incident with the help of outside experts to determine its impact. The company did not provide details on the nature of the “cyber incident”.

STEICO hit by cyberattack

Manufacturing

Denial of production

The STEICO Group, a German manufacturer of energy-saving insulating materials, was the target of a cyberattack disclosed on March 1, with information published later on its website. The attack affected both production operations and administration. The extent of the impact was assessed. A task force was immediately set up, supported by cybersecurity experts and data forensics specialists, to resume normal operations as quickly as possible. No further details were provided and it was unclear whether this was a ransomware extortion attack.

Groupe SEB hit by cyberattack

Manufacturing

Groupe SEB, a French manufacturer of household appliances, announced that it detected an attempt to exploit a vulnerability. Following investigations, an intrusion into the information system was confirmed. The necessary measures were taken to limit the impact of the intrusion. Groupe SEB wrote that it was in close contact with its clients and partners as well as with the competent authorities, in accordance with the RGPD (General Data Protection Regulation). At the time of the announcement and after extensive research, Groupe SEB had still not identified any data leakage or damage to information systems.

Hahn Group hit by cyberattack

Manufacturing, automation & robotics

Denial of IT services, interruption in operations

HAHN Group, an industrial automation and robotics headquartered in Germany, announced that it was the victim of a cyberattack on March 17. According to the message on its website, IT staff quickly noticed the attack and were able to stop it. "All systems" were shut down. The internal IT staff and other external forensic experts and specialists worked tirelessly to better understand the incident and to gradually reset the systems and boot them up again in a safe manner. As of March 27, the company was in the process of restarting its operations. This included reinstalling the infrastructure in a clean environment and using the backup systems.

Storopack hit by cyberattack

Manufacturing

Denial of IT services

German packaging manufacturer Storopack recorded a cyberattack on March 21. According to a message posted on its website, the company was not reachable by email and limited by phone. Its website was unaffected, but its online store was unavailable. In accordance with its IT emergency protocol, Storopack took the necessary security measures immediately after becoming aware of the cyberattack and informed the police and other relevant authorities. Although there may have been some delays in delivery, Storopack worked at full speed to maintain its ability to deliver. Production and delivery capability were not interrupted at any time.

Bobst hit by cyberattack

Manufacturing

Operations degrade

Le Temps learned that Swiss machine manufacturer Bobst Group suffered two attacks over the Easter weekend, forcing the company to work in degraded mode. The company believes that "it's a good sign" that nothing about Bobst was found on the darknet. Emergency measures were taken to protect critical computer systems by isolating them, in order to limit the risk of any spread, that resulted in production, research and development and customer support to operate in a degrade mode. Between April 12 and 18, work gradually resumed at the group's various global sites while systems were reconnected. The quieter holiday period helped to mitigate the impact. Five days after the event, the manufacturer informed its customers and suppliers of a certain instability that could cause inconvenience. Bobst's CEO claimed to know who had attacked the company and where the attacks were launched from, but provided no details. No ransom note was received.

YKK hit by cyberattack

Manufacturing

Ransomware

Japanese zipper manufacturer YKK confirmed a cyberattack aimed at its US networks after being listed as the victim on the LockBit ransomware group leak site on June 2. According to a company spokesperson, once the cyberthreat was identified, the company's cybersecurity team was quick to respond, successfully containing it before it could cause significant damage or lead to the exfiltration of sensitive information. The company's quick and efficient response ensured that the attack did not affect its operations or the quality of service provided to its customers. It was also claimed that there was no material impact on its operations and the incident didn't compromise the ability to serve customers. The exact nature of the cyberattack remains undisclosed, and the company did not comment on whether a ransom was demanded. Notably, however, the LockBit ransomware group threatened to leak stolen data by June 16, but it is unclear whether any data was leaked.

Automotive

Trèves Group hit by ransomware

Manufacturing, automotive

Ransomware

Ransom demand

The IT systems of French automotive manufacturer Trèves Group were subjected to a major cyberattack over the weekend of February 18-19, 2023. According to a company press release, in order to limit the overall impact and to protect its partners, Trèves Group immediately implemented isolation protocols and decided not to pay the ransom. The Group started working closely with the authorities and took all the necessary measures in this regard. The entire Group mobilized to guarantee continuity of operations and a return to normalcy as quickly as possible. Trèves Group mentioned the Lockbit 3.0 ransomware group, which had added the company to the list of its victims, as the source of the attack in the press release.

Rosenbauer Group hit by ransomware

Manufacturing, automotive, fire-fighting equipment

Denial of IT services

Ransomware

Austria-based manufacturer of fire-service vehicles and firefighting equipment Rosenbauer Group, was the target of a cyberattack. According to a short press release issued on February 24, parts of the IT infrastructure were switched off as a precaution. The measures affected all Rosenbauer locations. A task force was immediately set up, bringing in external cybersecurity experts and forensic experts to securely and quickly restore system operation. To the company's knowledge, no customer or company data was stolen or encrypted. The relevant authorities have been involved. A few days after the confirmation, the LockBit 3.0 ransomware group listed the company as one of its victims.

Ferrari hit by ransomware

Manufacturing, automotive

Data leakage, personal data leaked, privacy

Ransomware

Italian luxury sports car manufacturer Ferrari reported a cyber-incident involving ransomware. The hacker demanded that the company pay a ransom for customer data. The company notified its customers of the potential data breach. According to the company's statement, after receiving the ransom demand, it immediately launched an investigation in cooperation with one of the world's leading cybersecurity companies and informed the relevant authorities. It added that according to the company's policy, Ferrari will not pay a ransom as this kind of payment finances criminal activity and allows threat actors to continue their attacks. Instead, the company informed its customers and alerted them to the potential data breach and the nature of the incident. The company states that the ransomware incident did not affect the company's operations in any way.

Exco Technologies hit by cyberattack

Manufacturing, automotive

Denial of IT systems

Canadian-based international manufacturer of die cast tools and car parts Exco Technologies announced on January 23 that three production facilities within its Large Mould Group were recovering from a cyber-incident. The company temporarily disabled some computer systems as it investigated this incident. It initiated bringing these systems back online and expected operations to be substantially restored over the following two weeks. The statement didn't detail the kind of attack, or whether personal or corporate data was accessed. It said independent experts were retained to help the company deal with the matter.

Ziegler hit by cyberattack

Manufacturing, automotive, firefighting vehicles

Denial of IT systems, denial of shipment

Albert Ziegler GmbH, the German manufacturer of firefighting vehicles, became the victim of a cyberattack that was detected on the morning of February 9. According to the news, all relevant systems were immediately shut down. As a result, all systems were taken offline at all locations, so the company was severely restricted in its ability to work and communicate by email. On February 20, the company issued another statement that all systems were restored, but that the company is partially reachable by email with some delays. The merchandise management system was available again with its core functions after several days. That allowed the company to restore the vehicle deliveries at the Giengen site.

SAF Holland hit by cyberattack

Manufacturing, automotive

Denial of IT systems, denial of production: 7-14 days

German manufacturer of chassis components for trailers and trucks SAF-Holland became the target of a cyberattack that was announced on March 27. As a result, systems were checked, shut down and disconnected from the internet and production has been interrupted at certain sites, which could last seven to 14 days, according to the company's statement. The extent of the impact of the cyberattack was being assessed. However, management expected to be able to make up for the resulting production backlog over the course of the next three months. The company estimated that it will take three months to make up for production losses.

Rheinmetall hit by cyberattack

Manufacturing, automotive

Denial of IT systems

Rheinmetall, an automotive and arms manufacturer based in Dusseldorf, Germany, disclosed that it experienced a cyberattack on April 14 that affected its industrial customer division. The attack hit the Rheinmetall business unit that serves industrial customers, particularly in the automotive sector. Rheinmetall told Recorded Future News that the company's defense division, which produces military vehicles, weapons, and ammunition, remained unaffected and continues to operate reliably. It is unclear who is behind the attack. It is known the hacktivist group Killnet posted a message on their Telegram channel in March urging its followers to launch a distributed denial-of-service attack against Rheinmetall.

Hyundai data breach

Manufacturing, automotive

Data leakage, personal data leakage, privacy

Automotive manufacturer Hyundai Motor notified vehicle owners in France and Italy of a data breach. The company warned that a hacker gained unlawful access to the personal information of the company's customers. The data breach involves phone numbers, email addresses, street locations, and vehicle chassis numbers. The alert stated that although the attackers entered Hyundai's database, they took no financial information or identity numbers. Hyundai said they had taken their systems offline in response to the attack until further security measures can be put in place. The company also notified the French and Italian data protection authorities. Hyundai advised its clients to be wary of phishing emails and unwanted text messages because these might be attempts at social engineering.

Suzuki Motorcycle India hit by cyberattack

Manufacturing, automotive

Denial of production

Suzuki Motorcycle India, a subsidiary of Suzuki Motor Corporation, was the victim of a cyberattack. On May 10, the company suspended production at its plant in Gurgaon, located in the northern Indian state of Haryana. A spokesperson for Suzuki Motorcycle India said that they were aware of the incident and immediately reported it, and that the matter was currently under investigation. There were no technical details. The cyberattack reportedly forced the company to postpone its annual supplier conference that was supposed to take place in May.

Laremo hit by ransomware

Steel construction

Denial of service, data loss, data leakage

Ransomware

German steel special vehicle equipment producer Laremo GmbH was hit by ransomware on February 5, the company announced that in a public statement on February 22. Data storage server systems were encrypted, so the data was considered lost according to the announcement. Customer database and financial accounting data were obtained by the attackers. The company has already turned to the relevant investigating authorities. The LockBit ransomware group claimed responsibility for the attack and uploaded the company's data on their dark web site on February 19.

Power and energy

Aker Solutions hit by ransomware

Energy

Denial of IT services

Ransomware

CSE Mecanica e Instrumentação SA, the Brazilian subsidiary of Aker Solutions, a Norwegian service provider for the energy industry, fell victim to a cyberattack that impacted its IT systems. Aker Solutions said it didn't know the full extent of the situation, and that they had been in dialogue with the authorities in Brazil about the incident. In addition, the company's global IT organization worked to resolve the situation with external expertise. Aker Solutions carried out several immediate mitigating actions, including temporarily shutting down most of the IT systems used in the CSE business entity. The attackers claimed that they had entered the IT systems, encrypted digital files and locked access to data. At the time of the update, there were no indications that any parts of Aker Solutions' IT systems other than those of the CSE subsidiary were infected.

ABB hit by ransomware

Manufacturing, electrical equipment, energy

Data leakage, denial of IT services

Ransomware

Swedish-Swiss electrical equipment manufacturer ABB confirmed that it was targeted in a ransomware attack, with the cybercriminals stealing some data. According to a press release, all of ABB's key services and systems are up and running, all factories are operating, and the company continues to serve its customers. The company also continues to restore any remaining impacted services and systems and is further enhancing the security of its systems. In private notifications sent to customers, ABB said its forensic investigation found no evidence of customer systems being directly impacted and there is no indication that it's unsafe to connect to ABB systems. Bleeping Computer was the first to report that ABB was targeted by the Black Basta ransomware group on May 7. The news outlet learnt from multiple employees that the ransomware attack affected the company's Windows Active Directory, affecting hundreds of devices. In response to the attack, ABB terminated VPN connections with its customers to prevent the spread of the ransomware to other networks. Cybersecurity researcher Kevin Beaumont stated the same. Beaumont posted on May 26 that the company paid the ransom, which would explain why it was not named on Black Basta's leak website.

MPPMC hit by ransomware

Power and energy

Denial of IT services

Ransomware

Madhya Pradesh Power Management Company Limited, based in Jabalpur, India, fell victim to a ransomware attack. The incident was detected in the company's IABS internal IT system on May 22. The Jabalpur state Cyber Cell's superintendent of police said that an investigation was underway in response to a complaint. MPPMC chief general manager said those behind the ransomware attack had provided email IDs to contact them. MPPMC scanned the servers as per the guidelines of the government and tried to restore them with precaution. No further technical details were released at the time of the announcement.

Qulliq Energy Corporation hit by cyberattack

Power and energy, utility

Denial of IT systems, denial of customer services

Qulliq Energy Corporation (QEC), the territorial utility that provides power to Nunavut in Canada, announced that its network was breached on January 15. It disclosed that the attack took down the systems at its Customer Care and administrative offices and didn't affect power plant operations, though customers were unable to pay their bills via credit card. The company enlisted external cybersecurity experts alongside QEC's and the Government of Nunavut's IT teams to investigate the scope of the attack and determine which data were accessed.

Hitachi Energy data theft

Manufacturing, power and energy

Data leakage

0-day vulnerability, GoAnywhere MFT, Ransomware

Hitachi Energy confirmed it suffered a data breach after the Clop ransomware gang stole data using a GoAnyway zero-day vulnerability and listed the company on its extortion portal. Hitachi Energy is a department of Japanese engineering and technology giant Hitachi focused on energy solutions and power systems. The attack was made possible by exploiting a zero-day vulnerability in the Fortra GoAnywhere MFT (Managed File Transfer), first disclosed on February 3, 2023, and now tracked as CVE-2023-0669. The security flaw enables attackers to gain remote code execution on unpatched GoAnywhere MFT instances with their administrative console exposed to internet access. The company responded to the incident immediately, disconnected the impacted system (GoAnywhere MFT), and initiated an internal investigation to determine the breach's impact. All affected employees, relevant data protection authorities and law enforcement agencies have been informed of the security incident directly by Hitachi. The company said in the statement that it had no information that its network operations or the security or reliability of customer data had been compromised. The statement didn’t specify whether any systems were disabled after the attack. The Clop ransomware group claimed it had breached over 130 organizations using the GoAnywhere MFT secure file transfer tool vulnerability. They also claimed that they could move laterally through their victims’ networks and deploy ransomware payloads to encrypt their systems, but chose not to and only stole the documents stored on the compromised GoAnywhere MFT servers.

Sociedad Eléctrica Del Sur Oeste hit by cyberattack

Power and energy, utility

Denial of IT services

The Peruvian electricity supply company Sociedad Eléctrica del Sur Oeste (SEAL) suffered a cyberattack on April 17. The company reported in a press release sent to local news outlets that some services and user data were not available until further notice. The expiration dates of electric service payments and other services were also suspended. According to SEAL’s General Manager, the attackers were seeking to steal information, however, the company had a security system that prevented it. The only thing they managed to obtain was access to the commercial part. The company reported that specialists were solving the problem in order to restore the service system.

Siemens Energy hit by cyberattack

Manufacturing, power and energy

0-day, MOVEit MFT, Ransomware

Siemens Energy, a Munich-based energy technology company, officially confirmed a MOVEit data-theft attack to several news outlets on June 27 after the Clop ransomware group added the company to its data leak website. The attackers exploited a zero-day vulnerability found in the MOVEit Transfer platform to gain unauthorized access to sensitive information. However, Siemens Energy said that no critical data was stolen, and business operations were not impacted, according to a company spokesperson. The company took immediate action upon learning about the incident. Siemens Energy did not respond to follow-up questions from news outlets about what systems or devices were affected and what data was stolen.

Hep Global hit by cyberattack

Manufacturing, renewable energy

Data leakage

Ransomware

Hep Global, a German renewable energy company that manufactures and operates solar power parks worldwide, was hit by a cyberattack. According to a statement on its website, all potentially affected systems were taken offline as an immediate measure and to avoid possible damage to the customers. At the time of publication, the company was unable to say whether data had actually been accessed. The company worked with authorities and external experts and filed a complaint against unknown persons. On June 19, Hep Global issued an update saying that immediate measures and close cooperation with authorities and external IT security experts ensured business continuity and the investigation into the cyberattack was still ongoing. The Darkrace ransomware group has claimed responsibility for the Hep Global data breach, listing the company as one of its victims.

Electronics

MKS Instruments hit by ransomware

Manufacturing, electronics, chip equipment

Denial of service, production & shipment suspended, financial loss: $200M

Ransomware

Chip equipment manufacturer MKS Instruments said it was hit by a ransomware attack on February 3 that affected business systems including production-related systems. The MKS website was still offline at the time of the announcement. MKS said it temporarily suspended operations at some of its facilities, as part of its containment efforts. The company reported the incident to law enforcement and was investigating the full extent of the costs and how much could be recovered through cyber insurance. The attackers encrypted business and manufacturing systems and may have stolen personal data, according to a filing with California regulators. The attack impacted the company's ability to process orders, ship products, and provide service to customers in the company's Vacuum Solutions and Photonics Solutions Divisions. The attack would result in at least a $200 million hit to company revenue during the first quarter, the company announced later in February. Prior to the incident, MKS Instruments expected to report about $1 billion in revenue.

Micro-Star International hit by ransomware

Manufacturing, computer & electronics

Data leakage

Ransomware

Taiwanese computer and electronics manufacturer MSI (short for Micro-Star International) confirmed on April 7 that its network was breached in a cyberattack after the Money Message ransomware gang claimed to have infiltrated some MSI systems and stolen files. In a statement, MSI urged users "to obtain firmware/BIOS updates only from its official website," and to avoid using files from other sources. MSI did not address the extent of the security breach, nor what was stolen, stating only that it detected network anomalies, and its IT department activated relevant defense mechanisms and carried out recovery measures. The company said it reported the intrusion to government law enforcement agencies and cybersecurity units. It also stated that it had returned to normal operations with no significant impact to its financials.

ACER data theft

Manufacturing, computer & electronics

Data leakage

Acer, a Taiwanese multinational hardware and electronics corporation, confirmed a data breach in one of its document servers after a hacker claimed to have stolen 160 GB of data from the company. Acer told SecurityWeek in an emailed statement that it had detected an incident of unauthorized access to one of its document servers for repair technicians. While the investigation was ongoing, there was no indication that any consumer data was stored on that server. The cybercriminal claimed the data was stolen in mid-February and the files included confidential slides, staff manuals, confidential product documentation, binary files, information on backend infrastructure, disk images, replacement digital product keys, and BIOS-related information.

Western Digital hit by cyberattack

Manufacturing, computer & electronics, data storage

Data leakage, personal data leakage, privacy, denial of customer services

On May 5, US data storage manufacturer Western Digital released a statement acknowledging that a March cyberattack against its computer systems resulted in data theft. According to the statement, compromised data included names, addresses, phone numbers, and encrypted hashed passwords and partial payment card numbers. Western Digital temporarily suspended access to its online store as a precautionary measure to secure its business operations. The company was aware that other alleged Western Digital information had been made public but didn't confirm the validity of this data.
TechCrunch reported that an "unnamed" hacking group breached Western Digital, claiming to have stolen 10 terabytes of data. While the threat actors claimed not to be part of the ALPHV ransomware operation, they used their data leak site to extort Western Digital. The threat actors released screenshots of stolen emails, documents, and applications that showed they still had access to the company's network even after being detected. The hackers also claimed to have stolen an SAP Backoffice database containing customer information and shared a screenshot of what appears to be customers' invoices.

Lacroix Group hit by cyberattack

Manufacturing, electronics

Denial of IT systems, denial of production

Lacroix Group, a multinational manufacturer of electronic equipment for the automotive, home automation, aerospace, industrial and health, and smart roads sectors and the management and operation of water and energy systems, announced that during the night of Friday, May 12, to Saturday, May 13, it was the victim of a targeted cyberattack.
The cyberattacks affected the French, German and Tunisian sites. Measures were immediately taken to secure all the Group's other sites. Some local infrastructures were encrypted and an analysis was carried out to identify any exfiltrated data. On May 31, the company issued an update informing that it had partially resumed production at its electronics activity sites in Tunisia, France, and Germany as of May 17.

Kinmax Technology data breach

Manufacturing, electronics, semiconductors

Data leakage

Taiwan Semiconductor Manufacturing Company (TSMC) confirmed to several news outlets on June 30 that it had experienced a data breach after being listed as a victim by the LockBit ransomware group on its dark web leak site. The group threatened to publish data stolen from the company but didn't provide any evidence of the data it had allegedly stolen. In a statement released to news outlets, a TSMC spokesperson confirmed that a data breach occurred due to cybersecurity incident at one of the company's IT hardware suppliers, named as Kinmax Technology, that led to a leak of information related to the initial server setup and configuration. According to the statement upon review, this incident did not affect TSMC's business operations, nor did it compromise any of TSMC's customer information. After the incident, TSMC immediately terminated its data exchange with the affected supplier in accordance with the company's security protocols and standard operating procedures.

Utility

Acea hit by ransomware

Energy, utility

Ransomware

Acea, an Italian public holding company that provides energy and other services to the city of Rome, confirmed a cyberattack at the beginning of February, allegedly carried out by the Black Basta ransomware group. According to the company's statement, the attack didn't impact essential services provided to users (distribution of water and electricity) thanks to the prompt management of the problem in collaboration with the relevant institutions, the National Cybersecurity Agency (Acn) and Cnaipic of the Postal Police. The company's internal IT services were involved in the necessary analysis and control activities.

Águas do Porto hit by ransomware

Water supply, utility

Denial of web services

Ransomware

Águas e Energia do Porto, a water utility in Portugal, stated on February 8 that it had been hit by a cyberattack, with its security team able to limit the damage. Public water supply and sanitation were not affected by the attack. As a result of the incident, some customer services were limited due to the company's restricted response capacity. The company was still able to process customer requests at in-person service desks, and it urged people to obtain virtual service tickets instead of standing in line. Águas e Energia do Porto contacted both the Portuguese National Cybersecurity Center and the Judiciary Police for assistance with the situation. The LockBit ransomware group took the responsibility for the attack.

Puerto Rico Aqueduct and Sewer Authority hit by ransomware

Water supply, utility

Data leakage, personal data leaked, privacy

Ransomware

With the help of the FBI and US CISA, government-owned water company Puerto Rico Aqueduct and Sewer Authority (PRASA) investigated a cyberattack that was announced on March 19. The threat actors had access to customer and employee information. The officials noted that the authority's critical infrastructure was not affected by the incident due to network segmentation. PRASA planned to notify impacted customers and employees via breach notification letters. The Vice Society ransomware gang added the authority to the list of victims on its Tor leak site. The ransomware gang leaked the passports, driver's licenses and other documents of the impacted individuals.

Israeli irrigation systems hit by cyberattack

Irrigation, wastewater treatment, utility

Denial of OT systems, denial of operations

Hacktivism

The Jerusalem Post reported that a cyberattack blocked several controllers monitoring irrigation and wastewater treatment systems in the Jordan Valley that are operated by the Galil Sewage Corporation. The company's experts spent the entire day restoring operations; at the time of the incident, the source of the attack was unclear. Local authorities were aware of the risk of a cyberattack and informed farmers in the region. Some of the farmers disconnected their irrigation systems from the internet and switched them to manual operation. According to Jerusalem Post, the National Cyber Directorate warned of the risk of cyberattacks that anti-Israeli hackers could carry out against national infrastructure during the month of Ramadan, saying that they were monitoring spikes in phishing attacks, direct login attempts to various site CMSs and scans for vulnerabilities in the web sites, such as possible SQL injections. In April, private and government organizations in Israel were hit by massive cyberattacks that were part of the #OPIsrael campaign launched by hacktivists against Israel's critical infrastructure.

Alto Calore Servizi hit by cyberattack

Water supply, sewage and purification, utility

Data leakage

Ransomware

Italian water supplier, sewage and purification company Alto Calore Servizi SpA confirmed a cyberattack on April 28. It appears the distribution of water was not affected, but the company database seems to have been compromised according to a note on its website. On May 2, Medusa Locker claimed the cyberattack on its data leak site, sharing some files belonging to ACS. The group said it took customer data, contracts, minutes from board meetings, reports, pipe distribution information, expansion documents and more.

Logistics

Wabtec hit by ransomware

Transportation, logistics, railways

Personal data leakage, privacy

Ransomware

US rail and locomotive company Wabtec Corporation disclosed a data breach that exposed personal and sensitive information after the LockBit group had published samples of data stolen from Wabtec and eventually leaked all stolen data on August 20, 2022. In an announcement, Wabtec said that hackers breached their network and installed malware on specific systems as early as March 15, 2022. On June 26, Wabtec detected unusual activity on their network leading to an investigation of the attack. On December 30, 2022, Wabtec began notifying affected individuals, per relevant regulations, with a formal letter to let them know their data was involved. The affected information includes: first and last name, date of birth, non-US national ID number, non-US social insurance number or fiscal code, passport number, IP address, employer identification number (EIN), and other data. Wabtec notified all applicable regulatory and data protection authorities, as required.

DNV hit by ransomware

Transportation, logistics, maritime

Denial of service, supply chain / trusted partner

Ransomware

Norwegian ship classification society DNV reported that it was a victim of a ransomware attack that occurred on January 7. As a result of the attack, the company took offline its ShipManager servers, as well as a marine fleet management software solution that supports the management of vessels and fleets in all technical, operational and compliance aspects. DNV estimated that the incident may had affected as many as 1000 vessels and impacted 70 customers. According to the news published by the organization, onboard software functionally continued to operate. The maritime software supplier launched an investigation into the incident with the help of global IT security partners. The company also reported the incident to the Norwegian authorities.

FIEGE Logistics hit by ransomware

Logistics

Data leakage, denial of IT services

Ransomware

Fiege Logistics based in Germany confirmed that it was the victim of a ransomware attack after the Lockbit 3.0 ransomware group had published stolen data on the dark web. Cybercriminals claim to have stolen 259 GB of the company’s internal data. In comments to local media, the company said three locations in Italy were affected by the cyberattack and around 15% of the Italian business was affected. The affected IT systems were immediately isolated. The IT staff worked flat out to restore normal performance. The cyberdefense team worked closely with specialized and long-standing IT partners as well as law enforcement and data protection authorities.

Vopak hit by ransomware

Logistics, tank storage

Data leakage

Ransomware

Dutch tank storage company Royal Vopak N.V. fell victim to a ransomware attack. The company confirmed that there was an IT incident at Pengerang Independent Terminals (PTSB) in Malaysia that resulted in the unauthorized access of some data. According to company's CEO, the cyberattack did not impact daily activities at that location or at other facilities around the world. Vopak was almost certainly attacked by the ALPHV/BlackCat ransomware group as the company was listed on its dark web site. Critical company information was allegedly stolen, including information about the company's tank infrastructure and systems.

Food & beverages

Grupo Nutresa hit by ransomware

Food processing

Data leakage, denial of product shipment

Ransomware

Grupo Nutresa, a leading processed food company in Colombia, disclosed a ransomware attack on April 20 that affected its business process and product shipments. According to the company, once the event was detected, the protocol established by the company for this type of incident was activated to mitigate its potential impact. On April 24, the Lockbit group claimed responsibility for the cyberattack on the Nutresa group and published internal documents several days later.

Super Bock Group hit by cyberattack

Manufacturing, food & beverage

Denial of IT systems, denial of product shipment

Super Bock Group, a brewery based in Portugal, was the target of a cyberattack that caused disruptions to computer services, limiting its normal operations. In a statement issued on LinkedIn, the company added that the situation caused major restrictions in its supply operation to the market for some of its products. The usual and necessary safety protocols were enacted by the company. It informed the relevant data authorities in Portugal and followed a contingency plan to resupply the market. No additional details were given by Super Bock Group.

Coca-Cola FEMSA hit by cyberattack

Manufacturing, beverage

Beverage company Coca-Cola FEMSA México disclosed that it fell victim to a cyberattack. The company conducted a forensic investigation and simultaneously put its cybersecurity protection and response mechanisms in place to determine the extent of the breach. The corporation did not elaborate on whether the event included a breach, the loss of data or passwords, or a breach of its networks. A statement to the Mexican Stock Exchange (BMV) said that “the company is working with experts on measures to avoid an adverse impact on its information technology applications.”

Schwälbchen Molkerei hit by cyberattack

Manufacturing, food & beverage

German dairy products manufacturer Schwälbchen Molkerei Jakob Berz AG was hit by a cyberattack that affected some areas of its IT infrastructure, according to a statement obtained by local news outlets. As a result of the attack, the company’s availability was impaired. Ongoing production and logistics were not affected. Work was underway to fully restore the systems. It is unclear to what extent company data was obtained by unauthorized third parties. The company worked closely with security authorities and an external IT security service provider. No further details were provided and the company didn’t specify the type of attack.

Oil & gas

Encino Energy hit by ransomware

Oil & gas

Data leakage

Ransomware

Encino Energy, a US-based natural gas and oil producer, acknowledged a cyberattack when contacted by The Record after the BlackCat/ALPHV ransomware group added the company to its data leak site on the dark web. An Encino Energy spokesperson didn’t say whether the cyberattack was a ransomware incident, whether the company paid a ransom or whether it had examined the 400GB of data on BlackCat/ALPHV's site, but said there was no impact on the company’s operations, and the company continues to operate business as usual. Encino Energy was previously aware of unauthorized activity, investigated the action, and remediated the issue.

Suncor Energy hit by cyberattack

Oil & gas

Denial of customer services

The Canadian oil company Suncor confirmed that a cyberattack was the cause of widespread outages that brought services to a halt on June 23. Customers reported problems logging in to the app and website for Petro-Canada, a gas station chain owned by Suncor. Employees told media that customers could only pay cash at a number of gas stations. According to the company’s statement, it took measures to mitigate the attack and informed the authorities of the situation. Suncor expected transactions with customers and suppliers to be negatively impacted until the incident was resolved. The company did not provide any details about the type of cybersecurity incident and whether or not it was a ransomware attack that affected its systems.

Shell hit by cyberattack

Oil & gas

0-day, MOVEit MFT

Ransomware

Shell, the British oil and gas multinational headquartered in London, confirmed on June 15 that it had been impacted by the Clop ransomware gang's breach of the MOVEit file transfer tool after the group listed the company on its extortion site. In a press release the company stressed there was "no evidence of impact to Shell's core IT systems" and said their IT teams continued to investigate the incident. The company specified that this was not a ransomware event. The company's spokesperson commented that they were not communicating with the hackers.

Shipbuilding

Lürssen hit by ransomware

Manufacturing, ship building

Denial of operations

Ransomware

German shipbuilder Lürssen confirmed on April 12 that it had fallen victim to a ransomware attack that occurred over the Easter holiday period. In coordination with internal and external experts, the company immediately initiated all necessary protective measures and informed the relevant authorities. The attack brought much of Lürssen's shipyard operations to a standstill, according to local news outlet Buten un Binnen, which first reported the incident.

Fincantieri Marine Group hit by cyberattack

Manufacturing, ship building

Denial of IT Systems, denial of production

US commercial and defense shipbuilder Fincantieri Marinette Marine acknowledged an alleged ransomware incident in a statement to USNI News and Green Bay Press-Gazette. The attack occurred on April 12 and affected its email server and some network operations and caused production delays. The statement indicated the company's network security officials immediately isolated systems and reported the incident to the relevant agencies and partners. Fincantieri Marine Group brought in additional resources to investigate and restore full functionality to the affected systems as quickly as possible. The company added that it had no evidence the incident compromised any employees' personal information.

Brunswick Corporation hit by cyberattack

Manufacturing, maritime, ship building

Denial of operations & shipment: 9 days

The US-based manufacturer of boats and marine propulsion systems experienced an IT security incident on June 13 that impacted some of its systems and global facilities. The company said it activated its response protocols, which include pausing operations in some locations, engaging leading security experts and coordinating with relevant law enforcement agencies. Brunswick said it was working to address the incident in order to restore the full functionality of the affected systems and minimize impact on the business, employees and customers. In a press release issued on June 22, the company stated that it had made significant progress restoring the functionality of its systems and restarting operations at facilities where production or distribution was paused. All of Brunswick's primary global manufacturing facilities and most distribution facilities were operational, and the remaining production and distribution facilities were expected to resume operations within a few business days.

Pharmaceutical

Eisai hit by ransomware

Manufacturing, pharmaceutical

Denial of IT services, denial of logistics systems

Ransomware

Japanese pharmaceutical company Eisai announced that it fell victim to a ransomware attack. Headquartered in Tokyo, the company has manufacturing facilities in Asia, Europe, and North America, and has subsidiaries on both American continents, in Asia-Pacific, Africa, and Europe.

The ransomware attack was identified on June 3, and resulted in the encryption of multiple servers. The attack impacted servers both in Japan and overseas, including logistics systems. The company's corporate websites and email systems remained operational.

Eisai said it immediately implemented its incident response plan, which involved taking systems offline to contain the attack, and launched an investigation. Eisai Group immediately established a company-wide task force, and worked on recovery efforts with the advice of external experts and undertaking measures to understand the scope of the incident. Additionally, Eisai Group consulted with law enforcement. Eisai said it had to determine whether any data was compromised or stolen during the attack.

Virbac hit by cyberattack

Manufacturing, pharmaceutical

Denial of IT services

French animal health pharmaceutical company Vibrac was the target of a cyberattack on several of its sites worldwide during the night of June 19-20, according to a statement on its website. As soon as the company became aware of the attack, it immediately took steps to contain it and set up a crisis unit including dedicated cybersecurity experts to assess the impact on the systems and organize remediation operations. As a result of this attack, the company experienced a slowdown or temporary interruption of some of its services. Vibrac didn't specify the type of attack and provided no further details.

Metallurgy

Badische Stahlwerke hit by cyberattack

Manufacturing, steel

Denial of IT systems

Badische Stahlwerke GmbH, a steel producer in Kehl, Germany, posted a message on its website stating that unauthorized access to the company's network occurred on April 20. The company was working hard to fully and quickly investigate the incident. Employees were temporarily unavailable by email and landline phone while the affected systems were shut down and reviewed. According to a report by the regional news portal, the attack was confirmed by the police in Offenburg and an investigation into the case was started.

Haynes International hit by cyberattack

Manufacturing, metallurgy, alloys

Denial of IT systems, denial of shipment

US-based alloy manufacturer Haynes International began experiencing a network outage indicative of a cybersecurity incident on June 10, according to a press release. Upon detection of the incident, the company engaged third-party specialists to assist in investigating the source of the outage, determine its potential impact on the company's systems, and securely restore full functionality to the company's systems. Although "various aspects of Haynes International networks" were down while the retained specialists remediated the incident, all of the company's manufacturing operations were running with some operating inefficiencies. In addition, the company substantially restored its administrative, sales, financial, and customer service functions. Haynes did not provide any information on what caused the incident, but said its investigation and restoration efforts were still ongoing. The company said the response caused some delay in product shipments.

Other

Military-defense. Solar Industries hit by ransomware

Manufacturing, military-defense

Data leakage

Ransomware

The parent company of a private defense ministry contractor and a manufacturer of defense equipment, Solar Industries Limited India, was allegedly compromised by the Windows Alphv ransomware (aka BlackCat), with the group releasing a number of documents on the dark web and claiming to have stolen 2TB of data. While the case wasn't officially confirmed by the organization, which declined to comment on it, it was confirmed by an unnamed government official. A case was also registered with Nagpur cyber police station on January 25, according to police officials. The website of the firm was down on January 29. According to local news sources, the hacker group penetrated the Solar Group on January 21, followed by a ransom demand. The company didn't respond to the demand and immediately reported it to the Computer Emergency Response Team India (CERT-In).

Engineering. Vesuvius hit by ransomware

Engineering, metal, ceramics

Denial of service

Ransomware

Vesuvius, a UK-based engineering company well known in the metals and ceramics market, announced a cyber-incident that led to a shutdown of its systems. The company worked with leading cybersecurity experts to support the investigations and identify the extent of the issue, including the impact on production and contract fulfilment. The company took steps to comply with all relevant regulatory obligations. The Vice Society ransomware gang claimed responsibility for the cyberattack against Vesuvius and published files that it stole from Vesuvius on the dark web.

Mining. Rio Tinto data breach

Mining

Data leakage, personal data leakage, privacy

GoAnywhere MFT vulnerability

Ransomware

On April 5, Anglo-Australian mining corporation Rio Tinto Group confirmed to local news outlets that employee data stolen in a March cyberattack through third-party file transfer service GoAnywhere was posted on the dark web. On 23 March, Rio Tinto revealed a third-party cyberattack could have exposed the personal data of current and former Australian employees. The company initially told its staff that while threats had "been made by a cybercriminal group" to release data on the dark web, it was unsure whether the cybercriminal group actually possessed the stolen data. The Cl0p ransomware group claimed responsibility for the Rio Tinto data hack. It has updated its dark web page to include a slew of Rio Tinto data.

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