Kaspersky ICS CERT

H2 2023 – a brief overview of main incidents in industrial cybersecurity

11.04.2024

Version 1.0

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 where information on incidents was originally published are broken because the information has already been removed. Still, we decided to keep the links because the information below is based on statements made by victim companies.

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

The number of stories is comparable to that for the previous six months (64 vs. 67), but on average the consequences of the attacks have become more severe (or at least more of the victims reported severe consequences).

Material consequences, such as denial of production or suspension of product shipments, were reported twice as often as in the previous six months (37.5% of incidents in H2 2023 vs. 18% in H1 2023).

Some victims reported financial losses as a result of an attack (maximum of $356 million reported by US chemical products manufacturer Clorox).

In one case, a cyberattack virtually killed a business (or at least that's what the company's management claimed – "It blocked the company's ability to secure additional investment and funding"). Most of the employees of one of Britain's oldest transportation companies, KNP Logistics, lost their jobs, with just one subsidiary surviving by being sold.

Some of the cases have almost involved infrastructural effects. The attack on DP World Australia, for example, stranded 30,000 containers in four major Australian ports. An attack on China's Yanfeng, the world's largest OEM manufacturer of automotive interior parts, caused another automotive giant, Stellantis, to halt its assembly lines.

In three cases, attackers were able to gain access to automated control systems and use them to cause physical damage. One attack by a pro-Israeli group shut down up to 70% of Iran's gas stations. An attack on Israeli-made Unitronics PLCs used in utilities in several countries around the world left 160 homes in Ireland temporarily without water. The third high-profile case – an attack on a Ukrainian energy company – was described in our review on APT attacks on industrial enterprises (listing the results of the technical investigations that have been published by experts for public access in H2 2023).

Among the cases that we believe may be of particular interest for various reasons, we would like to highlight the attack on ORBCOMM – the US service provider and IIoT and M2M device vendor. The attack affected their FleetManager platform and stopped their Blue Tree products from working – those used to log the activities of truck drivers, as required by local regulations. The attack is of particular interest to us because it may foreshadow the development of a new attack vector for cybercriminals – attacking the onboard equipment and telemetry systems installed in various vehicles and vessels, which could open up the possibility of locking the vehicle or vessel itself. This is something we mentioned in our recent threat forecast for 2024.

July

- KNP Logistics Group
- Japan Aerospace Exploration Agency
- Port of Nagoya
- Wildeboer Bauteile
- TOMRA
- Estée Lauder
- Tempur Sealy
- Seiko Group
- Campbell Soup
- BAZAN Group
- Stader Land Drinking Water Association

August

- Zaun Limited
- Freeport-McMoRan
- Clorox
- Kansai Nerolac
- Engie
- Stadtwerke Neumünster
- Kendrion Kuhnke

September

- KIA Motors
- ORBCOMM
- Alps Alpine
- Auckland Transport
- Somagic
- Wacoal
- Johnson Controls
- Baccarat

October

- D-Link
- Estes Express
- Hochsauerlandwasser and HochsauerlandEnergie
- Volex
- Simpson Manufacturing
- BHI Energy
- Verhelst Groep
- Röhr + Stolberg GmbH
- SIAAP
- Yamaha Motor
- Boeing
- BAUER Group

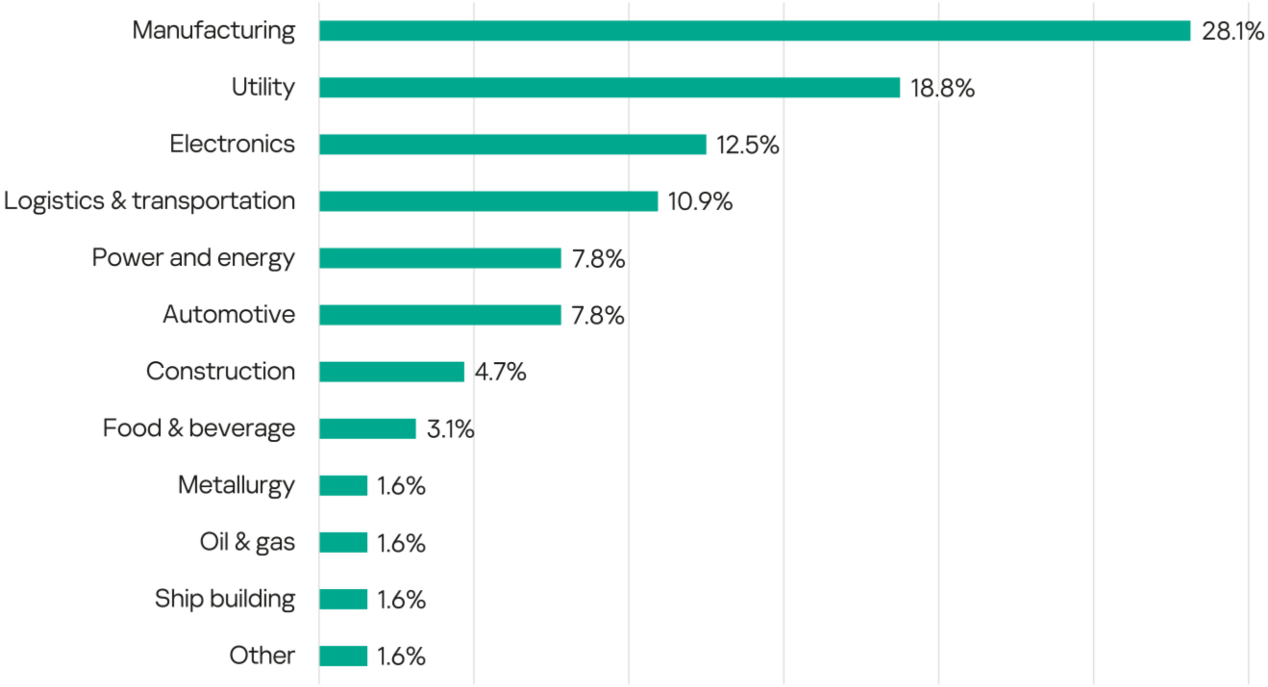
November

- Japan Aviation Electronics
- Bartec
- DP World
- North Texas Municipal Water District
- Yanfeng
- Idaho National Laboratory
- HSE
- PFAFF
- Municipal Water Authority of Aliquippa
- AVU
- Grimme
- Guyamier
- Drum/Binghamstown Group Water Scheme

December

- Gräbener Maschinentechnik
- Koh Brothers Eco
- Aqualectra
- Austal USA
- Nissan Australia
- Allgaier
- Jysk Energi
- VF Corporation
- Yakult Australia
- Iran's gas stations
- Elektroprivreda Srbije
- Lower Valley Energy

2024



Manufacturing

Wildeboer Bauteile hit by ransomware

Manufacturing

Denial of IT services, Denial of operations

Ransomware

German component manufacturer Wildeboer Bauteile was the target of a cyberattack on July 14. As the company reported on its website, it resulted in significant disruptions to the company's IT and communication systems. As a result of the attack and immediate separation of systems, there were restrictions in the communication options with customers, suppliers, authorities, and other business partners.

The attackers succeeded in breaking through the company's extensive IT security systems. It was unclear at the initial stage whether the cybercriminals were able to steal any data. To clarify this and other questions, Wildeboer commissioned external IT forensics specialists to analyze the cyberattack. Further measures were taken in close cooperation with the relevant authorities. A company spokesman confirmed to Norddeutscher Rundfunk that company data was encrypted in the attack. The perpetrators also left a file with a virtual contact address to extort ransom money. Instead of responding to the ransom demand, the company filed a police report.

On August 11, the company released an update stating that production had started again, thus confirming there had been a production halt almost a month long.

TOMRA hit by cyberattack

Manufacturing

Denial of IT services, Denial of operations, Data leakage

TOMRA, a Norwegian manufacturer of sorting machines, was hit by an extensive cyberattack directly impacting some of its data systems. The attack was discovered on July 16, and the company promptly took measures to contain and neutralize it. To mitigate the consequences, select services were disconnected, and a dedicated team of internal and external members worked to resolve the situation. While most digital services remained operational offline for a limited time, certain functionalities were affected. Major office locations went offline, with employees working remotely, while TOMRA's recycling and food divisions continued to operate, albeit with limited digital functionality.

TOMRA issued an update specifying certain details of the attack, mainly that the threat actor had gained access to some technical infrastructure systems, allowing them to traverse and access other sites. Initial investigation discovered that this was an ongoing cyberattack with access through compromised TOMRA user accounts. TOMRA found no trace of evidence that its clients, customers, partners, or their systems were at risk from the attack. It also saw no evidence of data encryption and did not receive any ransom demands.

The cyberattack required a complete restructuring of the IT infrastructure across the global organization. This included rebuilding core data centers, vetting of more than five thousand user accounts, and reworking and reestablishing underlying IT and network infrastructure. TOMRA states they implemented Zero Trust architecture. The lessons learned included that employee awareness plays a pivotal role. Comprehensive training and emphasizing the importance of vigilance are essential components. Establishing a defined incident recovery structure and procedure is also crucial, as incidents can often last longer than initially expected. Learning from the experiences of others with relevant expertise can be invaluable.

Estée Lauder hit by cyberattack

Manufacturing

Denial of IT services, Data leakage

0-day, MOVEit MFT, Ransomware

On July 18, 2023, U.S.-based cosmetics manufacturer The Estée Lauder Companies Inc. reported a cybersecurity incident involving unauthorized access by a third party to some of its systems. The company proactively shut down affected systems and launched an investigation in collaboration with cybersecurity experts and law enforcement. The unauthorized party managed to obtain certain data, prompting ongoing efforts to understand the scope and nature of the breach. Estée Lauder implemented security measures and remediation efforts to restore impacted systems and services. The incident caused disruptions to certain business operations, and the company took the necessary steps to secure its operations.

On the same day, the Clop and BlackCat ransomware groups named Estée Lauder Companies on their dark web leak site, following either the failure or non-occurrence of negotiations. The Clop ransomware gang might have gained access to the company after exploiting a vulnerability in the MOVEit Transfer platform for secure file transfers. In a message to the company, the BlackCat gang mocked their security measures, saying that they were still present on the network. Referring to the security experts that Estée Lauder brought in to investigate, BlackCat said that despite the company using Microsoft's Detection and Response Team (DART) and Mandiant, the network remained compromised and they still had access. The attacker also said that they did not encrypt any company systems, adding that unless Estée Lauder engaged in negotiations, they would reveal more details about the stolen data.

Tempur Sealy hit by cyberattack

Manufacturing

Denial of IT services, Denial of operations

U.S. mattress manufacturer Tempur Sealy International had to shutter parts of its IT systems because of a cybersecurity event that was identified on July 23. The company said the shutdown caused a temporary interruption of its operations. In an 8-K filed with the U.S. Securities and Exchange Commission, Tempur Sealy said it was in the process of bringing its critical IT systems back online and had resumed operations. Legal counsel, a cybersecurity forensic firm, and other incident response professionals were hired to advise Tempur Sealy, and law enforcement agencies were contacted. On August 2, the AlphV/Black Cat ransomware group took credit for the attack on the company, claiming to have sensitive documents from senior officials.

Zaun Limited hit by ransomware

Manufacturing

Data leakage

Ransomware

Zaun Limited, a British manufacturer of sports fencing and high security perimeter protection systems, faced a sophisticated cyberattack from the LockBit Ransomware group on August 5-6. In a statement released on the company's website, they reported that they prevented the encryption of their server, and their operations continued without interruption. The statement was released after Lockbit ransomware group claimed responsibility for the attack on August 13. The breach originated from a rogue Windows 7 PC running software for a manufacturing machine, which was since removed and the vulnerability closed.

Although initially believed to have thwarted data transfer during the attack, it has now been confirmed that LockBit managed to download approximately 10 GB of data, potentially limited to the vulnerable PC but with a risk of some data on the server being accessed (0.74% of stored data). The company collaborated with relevant agencies, including the National Cyber Security Center (NCSC) and the Information Commissioner's Office (ICO).

Clorox hit by cyberattack

Manufacturing

Denial of IT services

On August 14, U.S.-based chemical products manufacturer Clorox disclosed the discovery of unauthorized activity on some of its IT systems. Upon detecting this activity, the company promptly initiated measures to halt and remediate the situation, which included taking certain systems offline. Clorox was active in its response and resolution of the issue and collaborated with law enforcement agencies to address the matter. To maintain service for its customers as much as possible, Clorox implemented workarounds for certain operations that were affected by offline systems. Nevertheless, the incident resulted in disruptions to various aspects of the company's business operations.

The following month, the household brand filed another SEC report, which revealed they believed the hack was contained but resulted in slower production rates and "an elevated level of consumer product availability issues." Clorox claimed the total cost of the incident was as big as a $356 million decline in net sales.

Kansai Nerolac hit by ransomware

Manufacturing

Ransomware

Kansai Nerolac Ltd., an Indian subsidiary company of Kansai Paint, a Japanese paint manufacturing company, reported a ransomware incident that occurred on August 20. The statement assured stakeholders that the technical and cybersecurity teams, along with management, responded swiftly to the incident, implementing the necessary precautions and protocols to mitigate its impact and promptly report the incident to relevant organizations. Investigations into the causes and extent of the impact were underway in cooperation with specialized security agencies. The statement also mentioned that business operations had already resumed in KNPL, and there was no impact on systems in Japan.

Somagic hit by ransomware

Manufacturing

Ransomware

French barbecue manufacturer Somagic was hit by a cyberattack as reported by local media. Employees discovered that all data was inaccessible on September 18 and that files had been renamed with the ".medusa" extension, indicating the involvement of the Medusa hacker gang. The Medusa ransomware group added the company to its victims list.

Wacoal hit by cyberattack

Manufacturing

Denial of IT services

European subsidiary Wacoal Europe Co. Ltd. of Japanese lingerie manufacturer Walcoal was hit by a cyberattack on September 19 that affected its ordering systems, websites, and phone systems. The websites for Wacoal, Fantasie, Freya, and Elomi were down and displayed an error message stating that the sites are "under maintenance." Wacoal Europe conducted a full-scale investigation and system improvement with the advice of external experts. The company responded to recovery efforts and dealt with disruptions to business activities. No further details were specified.

Baccarat hit by cyberattack

Manufacturing

Denial of IT services, Denial of operations and shipment

French crystal goods manufacturer Baccarat S.A. was hit by cyberattack according to a statement shared on September 27. The attack partially disrupted the company's operations, and online orders and deliveries were temporarily suspended. According to Baccarat's statement, there was no indication that customers' personal or confidential data had been compromised. Baccarat called on external service providers to assess the damage, determine the information systems affected, and prepare for a gradual return to normal. Black Basta ransomware group added the company to its victims list on October 17. On October 21, Barracat issued a message saying that the publication originating from the threat actor was being analyzed by experts. After the cyberattack began, the company reacted with determination and implemented numerous cybersecurity and system security measures.

Johnson Controls hit by ransomware

Manufacturing

Denial of IT services

Ransomware

Johnson Controls International (JCI), a major U.S. manufacturer of HVAC equipment, security and automation systems for buildings, and auto parts, reported on September 27 in a filing with the U.S. Securities and Exchange Commission (SEC) that it suffered a cyberattack causing disruptions to its internal IT infrastructure. Promptly after detecting the issue, the company began an investigation with assistance from leading external cybersecurity experts and coordinated actions with its insurers.

The incident caused disruption to specific areas of the company's business operations. According to BleepingComputer, several subsidiaries of the company that produce fire suppression, HVAC, and security equipment for buildings, experienced IT outages as officials took systems offline in response to the attack.

A researcher at Nextron Systems shared a tweet including a ransom note from cybergang Dark Angels in its VMware ESXi encryptor stating a Johnson Controls International compromise, encryption, and leakage of critical data. CNN said they obtained an internal memo from the U.S. Department of Homeland Security raising alarm about the incident and warning that the attack on Johnson Controls may have compromised sensitive physical security information such as DHS floor plans.

The Dark Angels ransomware gang claimed to have stolen over 27 TB of confidential data from Johnson Controls. The threat actors then demanded a $51 million ransom to delete the data and provide a file decryptor.

According to the SEC, “The impact on net income for the three months ended December 31, 2023, of lost and deferred revenues, net of revenues deferred at the end of fiscal 2023 and recognized in the first quarter of fiscal 2024, and expenses during the quarter was approximately $27 million.”

Volex hit by cyberattack

Manufacturing

Volex, a UK-based manufacturer of critical power and data transmission cables, confirmed on October 9 that intruders accessed data after breaking into its tech infrastructure. The company said in a statement to investors that it enacted security protocols and took immediate steps to stop the unauthorized access to its systems and data as soon as the attack was noticed. Despite the incident, all sites remained operational with minimal disruption to global production levels, and the company continued trade with its customers and suppliers. The financial fallout from the breach was not expected to be material.

Simpson Manufacturing hit by cyberattack

Manufacturing

Denial of IT services

Simpson Manufacturing, one of the leading manufacturers of building and structural materials and anchors in North America, experienced disruptions in its IT infrastructure and applications resulting from a cybersecurity incident. Following the incident, the company was forced to shut down its infrastructure, which it notified about on October 10, 2023 through the SEC 8-K form. The company stated the incident had caused disruptions to its business operations. They engaged leading third-party cybersecurity experts to support its investigation and recovery efforts.

Yamaha Motor hit by ransomware

Manufacturing

Personal data leakage

Ransomware

Japanese mobility manufacturer Yamaha Motor Co., Ltd. said one of the servers managed by its motorcycle manufacturing and sales subsidiary in the Philippines, Yamaha Motor Philippines, Inc. (YMPH), was hit by a ransomware attack confirmed on October 25, and a partial leak of employee personal information was confirmed on November 16. On October 27, YMPH reported the incident to the Philippine authorities.

Upon learning of the attack, the IT Center at Yamaha Motor headquarters in Japan and YMPH immediately set up a countermeasures team and worked to prevent further damage while investigating the scope of the impact, the company said in a statement. In addition, the company said it worked on recovery together with an external internet security company.

The attack remained limited to one of the servers managed by YMPH, and the company confirmed it did not affect the headquarters or any other companies in the Yamaha Motor group.

The INC Ransomware gang claimed the attack and leaked alleged data from the Philippines' network. The threat actors added the company to its dark web leak site on November 15, and published multiple file archives with roughly 37 GB of data containing employee ID info, backup files, and corporate and sales information, among other data.

Boeing hit by ransomware

Manufacturing

Denial of IT services, Denial of operations

Ransomware

U.S.-based aerospace and defense company Boeing confirmed a cyberattack impacted its global services division five days after the Lockbit ransomware group claimed responsibility for an attack on October 28. The cyberattack impacted its parts and distribution business and did not impact flight safety, according to official comments. Boeing confirmed collaboration with law enforcement and regulatory agencies as part of an ongoing investigation. The Boeing services website was down with a message saying the ongoing outage was caused by "technical issues."

The cybercriminals later removed any mention of Boeing from their website, telling the cybersecurity research and threat intelligence organization VX-Underground that negotiations started on November 1. However, the company was listed again on November 7 when the hackers announced that their warnings had been ignored. Data allegedly from Boeing was finally published online on November 10. Most of the data listed on the hacker group's leak site are backups for various systems, the most recent of them with an October 22 timestamp. The MalwareHunterTeam research group noted that many of the files appear to be associated with Aviall, a Boeing-owned aviation and aerospace component manufacturing company.

In a Lockbit 3.0 ransomware advisory published on November 21, the CISA mentioned that Boeing observed LockBit 3.0 affiliates exploiting CVE-2023-4966 to obtain initial access to Boeing Distribution Inc., its parts and distribution business that maintains a separate environment, and this information was voluntarily shared by Boeing.

PFAFF hit by cyberattack

Manufacturing

Denial of operations, Denial of IT services

German tools manufacturer PFAFF Werkzeug- und Formenbau in Röthenbach fell victim to a cyberattack that paralyzed its systems as confirmed by the local press on November 23. In a letter to its customers, Managing Director explained that the incident occurred on November 20 and the plants in Röthenbach and Charlotte in the U.S. were affected. Production was only possible to a limited extent, and portion of the workforce stayed at home.

Grimme hit by cyberattack

Manufacturing

Denial of operations, denial of shipment

On November 28, German agricultural machinery factory Grimme became the target of a cyberattack, which led to the cessation of production and the dismissal of employees at home. The consequences of the attack weren't clear, but internal IT detected the incident early and set up a crisis headquarters while thoroughly examining all systems that were shut down. The company warned on its website that due to the hacker attack, there might be restrictions on spare parts and machine deliveries; the myGRIMME, supplier, sales partner, and job portal, as well as websites. A spokesperson also added that they hope that as few systems as possible were affected and that production could start again soon.

VF Corporation hit by ransomware

Manufacturing

Denial of IT services, Data leakage, Denial of operations

Ransomware

VF Corporation, a U.S. footwear and apparel manufacturer, detected a cybersecurity incident on December 13, according to its 8-K form. The company shared that the threat actors encrypted some of its IT systems and stole data. VF worked with cybersecurity experts to investigate the incident.

It noted that it worked through incident response and attempted to implement workarounds, but the cyberattack impacted its ability to fulfill orders. VF shut down some systems itself in response. The company said it tried to limit disruptions by moving some operations offline while it worked to restore the affected portions of its IT systems.

The company warned in a regulatory filing that the hack had a material impact on its business operations. VF announced the incident on the same day (December 15) that the U.S. Securities and Exchange Commission's new cyber disclosure rules took effect. The regulations mandate that companies report "material cybersecurity incidents" to their investors within four days of determining that a hack would influence their bottom lines.

According to a later update, following the shutdown of systems to contain the attack, the company was unable to replenish retail store inventory and order fulfillment was delayed, which resulted in order cancellations, reduced demand on certain web stores, and the delay of certain wholesale shipments.

The company also revealed that the hackers stole the personal information of approximately 35.5 million consumers.

Automotive

KIA Motors hit by ransomware

Manufacturing, automotive

Denial of operations

Ransomware

On September 6, the LaGrange Daily News was sent a message on social media indicating that an unknown entity had hacked into computer systems at car maker KIA Motors Manufacturing Georgia, causing the plant to shut down during the first shift and canceling the second shift. A spokesperson confirmed that Kia Georgia was alerted by a supplier of a cybersecurity issue that had resulted in a disruption of their regular production schedule. Kia Georgia worked closely with the supplier to minimize the impact and anticipated a prompt return to normal operations, but no further information on the incident was provided at the time of reporting. Another source obtained information that KIA Motors and other auto suppliers operating on the same software system had been hacked by attackers who demanded a ransom to restore data and service.

Gräbener Maschinentechnik hit by cyberattack

Manufacturing, automotive

German mechanical engineering company Gräbener Maschinentechnik GmbH & Co. KG was hit by a cyberattack on December 1-3, 2023. According to the official statement on its website, the perpetrators accessed parts of the internal databases, production processes were not affected, and emergency operations were successfully resumed. The company pointed out that it can't rule out possible publication of its data. Gräbener Maschinentechnik worked closely with law enforcement to investigate the incident and respond appropriately.

Yanfeng hit by cyberattack

Manufacturing, automotive

Denial of IT services, Denial of service, supply chain / trusted partner

Yanfeng, a major manufacturer of automotive components and the world's largest OEM manufacturer of automotive interior parts for leading auto assembly corporations (also known as Yanfeng Automotive Interiors and YFAI) headquartered in China, suffered a cyberattack in November, that affected Stellantis (a multinational automotive manufacturing corporation formed from the merger of the Italian–American conglomerate Fiat Chrysler Automobiles and French PSA Group, including FIAT, Citroen, Peugeot, Opel, Jeep, Chrysler, Dodge and many other car brands).

In a statement to The Detroit News, Stellantis spokesperson said that "Due to an issue with an external supplier, production at some of Stellantis' North America assembly plants has been disrupted." Stellantis monitored the situation and worked with the supplier to mitigate any further impact to its operations. The Yanfeng website wasn't working on November 13, and the Chinese company didn't respond to inquiries for comments regarding the situation. The Qilin ransomware group also known as Agenda claimed responsibility for the cyberattack on Yanfeng Automotive Interiors by adding them to their Tor data leak extortion site on November 27. The uploaded files included financial documents, non-disclosure agreements, quotation files, technical data sheets, and internal reports.

Nissan Australia hit by cyberattack

Manufacturing, automotive

Data leakage, Denial of operations

Japanese automobile manufacturer Nissan announced that its Australia and New Zealand arm suffered a significant cybersecurity incident at the beginning of December 2023 that affected the company's daily operations and which may have allowed hackers to access personal information. Nissan Oceania informed its customers of a potential data breach and warned them of the risk of upcoming scams.

The company worked with its global incident response team to assess the impact of the attack and worked to restore affected systems while clarifying that the dealer network was not impacted.

Nissan notified the Australian Cyber Security Center and New Zealand National Cyber Security Center. The company did not share details about the attack or its scope.

In their update released on March 13, 2024, Nissan said it was planning to notify approximately 100,000 individuals about the cyberbreach over the coming weeks. The type of information involved will be different for each person. Current estimates are that up to 10% of individuals have had some form of government identification compromised. The data set includes approximately 4,000 Medicare cards, 7,500 driver's licenses, 220 passports, and 1,300 tax file numbers. The remaining 90% of individuals notified had some other form of personal information impacted, including copies of loan-related transaction statements for loan accounts, employment or salary information, or general information such as dates of birth. The list of affected individuals includes some of Nissan's customers (including customers of Mitsubishi, Renault, Skyline, Infiniti, LDV and RAMS branded finance businesses), dealers, and some current and former employees.

Allgaier hit by cyberattack

Manufacturing, automotive

On December 8, German automotive supplier Allgaier Werke GmbH fell victim to a cyberattack, as reported by a local news outlet. The attack occurred amidst the company's ongoing insolvency proceedings. Despite the breach, production activities remained unaffected at the time of the incident, with both the company and the insolvency administrator refraining from disclosing further details regarding the extent of the impact. The nature and scope of the cyber-intrusion were not explicitly outlined in the initial report.

Power and energy

BHI Energy hit by ransomware

Energy

Data leakage, personal data leakage, supply chain / trusted partner

Ransomware

U.S. energy services firm BHI Energy detailed on October 18 in a data breach notification how the Akira ransomware operation breached their networks and stole data during an attack.

The group breached the company network on May 30, 2023 and reached the internal BHI network through a VPN connection using a third-party contractor's account. In the week following initial access, the threat actor used the same compromised account to perform reconnaissance of the internal network. The Akira operators revisited the network on June 16, 2023, to enumerate what data would be stolen. Between June 20 and 29, the threat actors stole 767,000 files containing 690 GB of data, including BHI's Windows Active Directory database. Finally, on June 29, 2023, having stolen all the data they could from BHI's network, the threat actors deployed the Akira ransomware on all devices to encrypt files.

The company said they immediately informed law enforcement and engaged with external experts to help them recover the impacted systems. The threat actor's foothold on BHI's network was removed on July 7, 2023. The company said it had been able to recover data from a cloud backup solution that hadn't been affected by the ransomware attack, so they were able to restore their systems without paying a ransom.

BHI identified that some of the files contained individuals' personal information and BHI was able to identify the specific data disclosed, which consisted of first, middle, and last names, addresses, dates of birth, Social Security Numbers, and potentially health information. BHI sent written notice to 896 affected residents on October 18, 2023.

Additionally, BHI bolstered its security measures by imposing multi-factor authentication on VPN access, performing a global password reset, extending the deployment of EDR and AV tools to cover all sections of its environment, and decommissioning legacy systems.

Idaho National Laboratory hit by cyberattack

Energy

Personal data leakage,
Data leakage

Hacktivism

Hacktivists group SiegedSec hacked the Idaho National Nuclear Laboratory (INL), a U.S. Department of Energy nuclear research center, and stole confidential data. This became known after SiegedSec published proof on the dark web on November 20.

INL has 50 experimental nuclear reactors and specializes in nuclear energy and national security. INL's current activities include the development of next-generation nuclear power plants, light water reactors, control system cybersecurity, advanced vehicle testing, bioenergy, robotics, and nuclear waste reprocessing.

SiegedSec hackers leaked detailed information on 45,047 former and current employees, spouses, and dependents on hacker forums and Telegram, including email and phone numbers, Social Security Numbers (SSNs), residential addresses, and employment information including bank information and salary details. SiegedSec also rolled out screenshots of the Oracle HCM system interfaces in INL, also simultaneously posting a message about the hack inside the corporate network. An INL representative confirmed the violation, noting that an investigation was underway with the participation of intelligence services and law enforcement agencies, which would have to establish the scale of the incident and the possible leak of scientific data.

HSE hit by ransomware

Energy

Denial of IT services

Ransomware

Slovenian power generation company Holding Slovenske Elektrarne (HSE) suffered a ransomware attack on November 22, with the company finally containing it on November 24. The attack compromised its systems and encrypted files, and was first reported by a local news outlet. The Director of the Information Security Office told the media that all power generation operations remained unaffected by the cyberattack while IT systems and files were "locked."

The organization immediately informed the National Office for Cyber Incidents at Si-CERT and the Ljubljana Police Administration and engaged with external experts to mitigate the attack and prevent the virus from spreading to other systems across Slovenia. The attack is believed to be the work of the Rhysida ransomware gang, which offers its victims an email address to contact the threat actors without making any financial demands.

According to Slovenian news outlet 24ur the incident was due to poor cyber hygiene (i.e., passwords stored in the cloud).

Jysk Energi hit by cyberattack

Energy

Denial of service

Hackers successfully penetrated the systems of a major energy supplier in Denmark, Jysk Energi, but there is no indication that they succeeded in stealing or encrypting data. The Danish energy company said it physically disconnected its internet connection following the cyberattack discovered on December 9, and some systems were shut down to the detriment of employees and customers. Relevant authorities were notified, and normal operations were expected to start the week after the published statement was issued.

Attacks on Iranian gas stations

Energy

Denial of service

Hacktivism

Around 70% of Iran's gas stations were disrupted as a result of a cyberattack. The attack affected the ability to pump fuel, leading to long queues at gas stations and traffic jams. Hacktivist group Predatory Sparrow ("Gonjeshk-e-Darande") claimed responsibility for the attack on its Telegram channel on December 18. The Iranian government has accused the gang, which previously carried out attacks on Iranian railway systems and a steel plant, of having ties to Israel. A member of the Energy Committee of the Iranian Parliament claimed that the cyberattack on Iran's fuel supply system was carried out "from inside" and that the attackers entered the system via a USB or program from inside.

Electronics

Seiko Group hit by cyberattack

Manufacturing, electronics

Data leakage

Japanese electronics manufacturer Seiko Group Corporation confirmed that it was dealing with a data breach in a statement on August 10. It discovered a possible data breach on July 28 and hired cybersecurity experts to examine the situation on August 2. The investigators found unauthorized access to at least one of their servers. In its statement, Seiko said it was reasonably certain that there was a breach and that some information stored by the company and/or group companies may have been compromised.

On August 21, the AlphV/Black Cat ransomware gang took credit for the attack, sharing screenshots of the stolen data that included spreadsheets and presentations.

Later on, Seico said it had completed a comprehensive review of the breach with outside cybersecurity experts. The leaked data had been stored by the business units known as Seiko Group Corporation, Seiko Watch Corporation, and Seiko Instruments Inc. About 60,000 pieces of personal data from customers, employees, business partners and job applicants were leaked.

Kendrion Kuhnke hit by cyberattack

Manufacturing, electronics

Denial of operations

In August, Kendrion, a control technology manufacturer headquartered in Amsterdam, experienced a cybersecurity incident involving an unauthorized third party gaining access to the company's systems.

In response to the incident, the company took all its systems offline as a containment measure and activated its response protocol, including contingency planning to ensure ongoing operations. Kendrion conducted investigations into the incident with the assistance of leading third-party cybersecurity experts.

The cyberattack affected Kendrion's location in Malente, Germany, where development and sales operations came to a standstill. However, production continued at the affected site. Most of the 300 employees in Malente were sent home as a result of the incident. While the investigation was ongoing, the company could not rule out the possibility that the unauthorized party may have accessed company data.

On September 5, the company reported that they had fully resumed operations.

Alps Alpine hit by ransomware

Manufacturing, electronics

Denial of operations, production and shipment

Data Leakage

Personal Data Leakage

Ransomware

Japanese manufacturer and supplier of audio, information, and communication equipment and electronic components Alps Alpine Co Ltd was hit by ransomware. According to the official statement, the attack was detected on September 10.

In order to minimize impact, the company immediately isolated the targeted servers from the network and started a detailed investigation to determine the impact with a security consultant. The company remained operational, though admitted that the attack affected some of its operations, including production and shipping. Alps Alpine restored its servers step-by-step, and continued to isolate servers from the network that remained of concern.

The BlackByte ransomware group added the company to its victim list on the dark web on September 12.

On November 28, Alps Alpine North America, Inc. filed a notice of data breach with the Attorney General of Texas after discovering that an unauthorized party being able to access the employees' sensitive information, which includes their names, Social Security Numbers, addresses, driver's license numbers, and other government-issued identification numbers.

D-Link hit by cyberattack

Manufacturing, electronics, network equipment

Data leakage

Taiwanese network equipment manufacturer D-Link confirmed a cyber-incident and data leak after a post about the breach was published on a hacking forum on October 1. Preliminarily, the incident led to the disclosure of certain low-sensitivity, semi-accessible information. It is stated that the data likely relates to the old D-View 6 system, which was used for registration and discontinued in 2015.

The violation was discovered when unidentified attackers claimed to have stolen the personal data of government officials in Taiwan, as well as the source code of the D-Link D-View network management software. Trend Micro specialists were involved in the investigation. According to the investigation, as a result of the breach, approximately 700 outdated and fragmented records were compromised, contrary to claims that the data of millions of users was leaked. Details of the attack were not disclosed, except that the breach was the result of a phishing attack that was carried out on one of the company's employees. D-Link specifically emphasized that its current customers are unlikely to be affected by this incident.

Kyocera AVX Corporation hit by cyberattack

Manufacturing, electronics

Denial of operations, Data leakage, Personal data leakage

U.S. manufacturer of advanced electronic components Kyocera AVX Components Corporation (KAVX), a subsidiary of the Japanese semiconductor giant Kyocera, said in a letter dated October 30 that it had suffered a cyberattack on March 30 on servers in its Greenville and Myrtle Beach, South Carolina locations that temporarily disrupted operations and led to a data leak.

Upon learning of the incident, the company launched an investigation into the attack, hired an outside third-party cybersecurity expert and notified law enforcement. KAVX's in-depth investigation determined that an unauthorized party gained access to and took information from certain systems between February 16, 2023, and March 30, 2023.

KAVX later discovered that the data contained on the impacted servers included the personal information of individuals globally. The following types of personal information may have been impacted: first and last name, address, date of birth, personal contact details such as phone numbers and emails, employment-related data such as employee ID, compensation, and salary information, employment performance, trade union data, health and medical-related information, gender identity, race and ethnicity, signatures, certain government-issued identifiers such as Social Security Numbers, driver's license numbers, passport numbers, other identification numbers, tax information, and financial account numbers.

The LockBit ransomware gang claimed to have compromised KAVX on May 26, 2023, when it added the firm to its data leak site.

Japan Aviation Electronics hit by ransomware

Manufacturing, electronics

Denial of IT systems, Data leakage

Ransomware

Electronics and aerospace manufacturer Japan Aviation Electronics confirmed that its systems faced a cyberattack on November 2 that forced the company to shut down its website. The company said that it investigated the status of damage and restored operations, but some systems had been suspended and there had been delays in sending and receiving emails.

Apart from failures in the operation of IT systems, no other consequences of the incident were initially disclosed. The company itself initially stated that there was no data leak. However, Japan Aviation Electronics was added to the ALPHV/BlackCat ransomware gang leak site on November 6. The company issued an update confirming a ransomware attack, as files on the servers had been encrypted and information stored on the server at the overseas subsidiary JAE Oregon, Inc. (Oregon, U.S.) had received unauthorized access and been leaked.

Japan Aviation Electronics set up a task force, investigated the damage, and worked on restoration with the support of external experts. It reported and consulted with the relevant organizations, said it would report to its customers and business partners who may have been affected, and proceeded with strengthening security and taking counter measures to prevent a recurrence.

Bartec hit by cyberattack

Manufacturing, electronics, engineering

German electronic equipment manufacturer and engineering company Bartec TOP HOLDING GmbH disclosed a cyber-incident that occurred on November 10 on their website. The company said that an unauthorized data access attempt was undertaken on parts of BARTEC's IT infrastructure. This attempt was largely prevented by the company's own security systems. Bartec immediately checked its existing IT infrastructure and has not identified any new attempts at unauthorized data access since then. Nevertheless, individual data leakage couldn't be excluded.

NXP hit by cyberattack

Manufacturing, electronics

Data leakage

APT

On November 24, 2023, the details of a substantial cybersecurity incident of Dutch microelectronics giant NXP were revealed to Dutch press. The Chinese-speaking APT network known as Chimera managed to spy while remaining undetected on the network from October 2017 to the beginning of 2020.

The first mention of the hack came after Fox-IT published details in January 2021 of two highly advanced cyberattacks that targeted an airline and an unnamed semiconductor company, later known to be NXP.

Hackers managed to gain access to NXP systems through employee accounts using classic brute force and bypassing 2FA by spoofing phone numbers. The hackers collected primary information about the accounts from previous LinkedIn or Facebook leaks. Once inside the company's network, the hackers gradually expanded their access rights, erased traces, and moved horizontally into protected segments. In search of new potentially interesting data, hackers visited the victim's network on a weekly basis. Confidential data of interest was collected into encrypted archives and exfiltrated through Google Drive, Microsoft One Drive, and Dropbox cloud services.

The presence of cyber spies in the network was only discovered after investigating another incident involving the hacking of Dutch airline Transavia in 2019, when hackers attempted to gain access to the reservation systems of a subsidiary of KLM. Since April 2020, Microsoft and Fox-IT specialists were involved in the investigation and localization of damages and assessed the volume of the leak and all the circumstances of the incident. As a result, it was reported that the APT group managed to steal a certain portion of the intellectual property of NXP, but what exactly was stolen remains unknown. However, according to NXP's annual reports for 2020 and 2021, no direct material damage was caused.

In addition, as NRC journalists found out, during subsequent operations in 2018 and 2019, in addition to Transavia, the group also hacked seven Taiwanese chip manufacturers. Taiwanese CyCraft published details of this case in April 2020 as a large-scale, well-coordinated attack on the Hsinchu Science Park in Taiwan, where the headquarters of chip giant TSMC is located.

Utility

Stader Land Drinking Water Association hit by ransomware

Water supply, utility

Denial of IT systems, Data leakage

Ransomware

The Stader Land Drinking Water Association released a statement on its website addressing a ransomware attack that occurred at the end of July. While the attackers aimed to encrypt the association's systems, their encryption attempt was successfully thwarted.

The IT infrastructure was in the final stages of secure reconstruction with support from external experts and close cooperation with data protection and law enforcement authorities.

The statement highlights that the drinking water supply remained unaffected and continues to meet high quality standards despite the cyber-incident. However, there was a possibility that the attackers may have accessed sensitive data, such as addresses or account information, although there was no evidence of such a breach.

The Lockbit ransomware group claimed responsibility for the attack and included the organization in its DLS (data leak site).

Stadtwerke Neumünster hit by cyberattack

Energy, utility

Denial of IT services

On August, Stadtwerke Neumünster (SWN), a regional energy supply and service company in Neumünster, Germany, fell victim to a cyberattack that was announced on their website, prompting a precautionary shutdown of all systems.

While the supply of electricity, gas, heat, and internet to customers remained unaffected, the attack had significant consequences on the company's operations and services. SWN's IT department detected the espionage attempt and quickly initiated the shutdown as a protective measure. According to a press spokeswoman, this swift response was crucial to prevent further damage. She assured the public that essential services for customers are guaranteed despite the system shutdown.

However, the impact on SWN's employees was substantial. They were unable to work effectively, with no access to email, phone systems, or the various programs and systems used by the company. Many hotlines were also unavailable, leading to recorded announcements explaining the situation. The customer center at Kuhberg remained open for advice and assistance, but accessing customer data and making changes to contracts is not possible due to the system shutdown.

The State Criminal Police Office (LKA) led the investigation. According to the spokeswoman, the process of individually starting up and securing all systems, as well as conducting a thorough analysis, could take days or even two to three weeks.

Engie hit by cyberattack

Energy, utility

Personal data leakage

On August 23, a member of a hacker forum calling himself “HommedeLombre” published a customer database of Engie, a French energy supplier, leading to the leak of the personal data of 110,000 customers. The hacker indicated that he had exploited a flaw in a system of a subcontractor managing the site for Engie's Prime Energy (monespaceprime.engie.fr).

Following this revelation, on August 30 Engie confirmed that it had fallen the victim of the cyberattack affecting its website. Engie filed a complaint and worked with the competent authorities to resolve the matter. Customers whose data was stolen were informed of the situation. Among the information leaked were the victims' first names, last names, email addresses, telephone numbers and customer numbers.

Hochsauerlandwasser and HochsauerlandEnergie hit by ransomware

Energy, water supply, utility

Denial of IT services

Ransomware

German Hochsauerlandwasser GmbH (HSW) and HochsauerlandEnergie GmbH (HE), water and energy supply companies, fell victim to a hacker attack that was announced on October 5.

Some services became available to customers to a limited extent, and parts of the IT infrastructure were infected with malware. Although much of the IT infrastructure was restored within a short period of time, the commercial operating software remained out of operation for several days for security reasons.

HSW and HE had a forensic audit of their systems carried out. The team from the two municipal companies could be reached in customer centers by telephone, email, or post. Services such as changes to advance payments, meter reading reports, or changes to contracts could not be implemented.

HSW and HE filed a criminal complaint against those responsible for the hacker attack. The managing director emphasized that they weren't considering an option to respond to the hackers' demand for a ransom payment.

SIAAP hit by cyberattack

Water supply, utility

Abuse of IT services

French water utility Syndicat Interdépartemental pour l'Assainissement de l'Agglomération Parisienne (SIAAP) became the victim of cyberattack on October 24. According to the message on its website, the attack resulted in the SIAAP mail server sending fraudulent emails to "other French administrations."

IT teams worked to secure industrial systems and closed off all external connections to prevent the attack from spreading. This attack was quickly contained and the SIAAP IT infrastructure remained operational. However, several hundred fraudulent messages were sent from the SIAAP mail server. Recipients of such messages were advised to be vigilant and check the veracity of the message received from their usual contacts at SIAAP without clicking on any suspicious links.

This event was the subject of an in-depth analysis, and reinforced protective measures were being deployed. The SIAAP filed a complaint and declarations were in progress at the National Information Systems Security Agency.

Municipal Water Authority of Aliquippa hit by cyberattack

Water supply, utility

Denial of operations

Unitronics

Hacktivism

The Municipal Water Authority of Aliquippa in Pennsylvania, a company that provides water and sewer services, confirmed to local news outlet KDKA-TV that hackers took control of a system associated with a booster station.

The company's chairman of the board for the Aliquippa water authority explained that alarms went off on November 25 at a station located on the outskirts of town and that local police were called to investigate the incident. According to the comments provided to local news outlet Beaver Countian, the hackers did not get access to anything in the actual water treatment plant or other parts of the system other than a pump that regulates pressure to elevated areas of the system. The pump was on its own computer network separated from the primary network and physically located miles away. Employees took the equipment offline and used backup tools to maintain water pressure. It was stated that there was no known risk to the drinking water or water supply.

The machine that was hacked used the Unitronics Vision system, a programmable logic controller (PLC) with an integrated human-machine interface (HMI). Unitronics Vision products are developed by an Israeli-owned technology company and have been known to be affected by critical vulnerabilities that could expose devices to attacks.

An Iran-supporting hacktivist group called Cyber Av3ngers took credit for the attack, posting a message about the hack on the screen of the compromised Unitronics Vision system. The group has filled its social media feed with references to the leaders of Iran and has pledged to attack any entities with products or ties to Israel, already claiming attacks on 10 water treatment plants in Israel.

CISA (Cybersecurity & Infrastructure Security Agency) issued an alert on November 28 that threat actors breached a U.S. water facility by hacking into Unitronics programmable logic controllers (PLCs) exposed online. CISA urged utilities to change default passwords, require multifactor authentication for all remote access to the operational technology network, disconnect PLCs from the open internet, or install firewalls and VPNs if remote access is necessary.

Drum/Binghamstown Group Water Scheme hit by cyberattack

Water supply, utility

Denial of operations

Unitronics

Hacktivism

The electronic system of the water scheme in the Drum/Binghamstown area of Erris in Ireland was hit by a cyberattack. As a result, residents served by the Drum/Binghamstown Group Water Scheme were without water on November 30, reportedly 180 people (160 households). Erris-based Deputy said crews tried desperately to repair the damaged equipment.

The water utility's representatives said the hackers may have breached the system due to their firewall not being "strong enough."

The target was the PLCs of Israeli company Unitronics. According to the Irish media, the caretaker went down and when he got to the pumphouse, "You have been hacked" and "Down with Israel" messages were displayed on the screen, as well as the hacker group's name. Although the name of the group that attacked Binghamstown/Drum was not revealed, it may be linked to the Cyber Av3ngers hack of the Municipal Water Authority of Aliquippa in Pennsylvania.

North Texas Municipal Water District hit by cyberattack

Water supply, utility

Denial of IT services

Data leakage

Ransomware

The North Texas Municipal Water District (NTMWD), which provides water supply, wastewater treatment, and solid waste management in 13 cities across the state, including Plano and Frisco, was hit by a cyberattack. The administration managed to restore the systems, declaring that the incident had no impact on the production process. The company's spokesperson announced that law enforcement was notified of the incident, but did not respond to requests for comment about whether NTMWD dealt with ransomware. According to official data, the company's phone lines were down on November 12.

However, the attack was claimed by the Daixin Team ransomware gang, which added NTMWD to its DLS on November 28, claiming to have stolen more than 33,000 customer information files.

AVU hit by cyberattack

Energy, utility

Denial of IT services

German energy supplier AVU, which serves Hattingen and Sprockhövel, was hit by a cyberattack. AVU systems were disconnected from the internet and taken out of service to prevent damage, making the online service point inaccessible. However, thanks to preventive measures and the intervention of security experts, no customer data was affected and the energy supply was never compromised.

Aqualectra hit by ransomware

Energy, water supply, utility

Denial of IT services

Ransomware

Water and electricity distribution company Aqualectra in Curaçao suffered a cyberattack which forced it to temporarily cut all its online connections, affecting its internal systems and customer service. The company's statement appeared after the Akira ransomware group took responsibility on December 6 and said it had compromised operational files, business documents, payment records, and more. Aqualectra acted quickly to counter the attack and conducted extensive analysis to prevent permanent damage. Services were fully restored, and according to the statement, recent power outages on the island were not linked to this cyberattack.

Elektroprivreda Srbije hit by ransomware

Energy, utility

Denial of IT services

Ransomware

Serbian power generation company Elektroprivreda Srbije (EPS) suffered a crypto cyberattack and claimed that electricity production and distribution as well as business activities were not affected thanks to their protective measures. For security reasons, IT systems were put out of action. The operation of the Account Insight portal was hampered. The company said that state authorities were informed about the cyberattack and took appropriate measures.

Ransomware hacking group Qilin took responsibility for the cyberattack on Serbia's electricity provider at the end of December and offered the download of hundreds of thousands of documents allegedly taken from the company on their dark web website. Qilin said it was offering more than 34 GB of Elektroprivreda Srbije (EPS) data on the dark web, and a second tranche would be available on January 27.

Lower Valley Energy hit by cyberattack

Energy, utility

U.S. electric utilities company Lower Valley Energy Inc disclosed a cyberattack on December 28. Upon discovery of this incident, Lower Valley Energy promptly engaged a law firm specializing in cybersecurity and data privacy to investigate the incident. Additionally, Lower Valley Energy engaged third-party forensic specialists to assist in its investigation of the incident. At the time of announcement, Lower Valley Energy had no evidence that personal information had been impacted.

Logistics & transportation

KNP Logistics Group hit by ransomware

Logistics

Denial of services, denial of operations

Ransomware

UK-based KNP Logistics Group declared insolvency after suffering a major ransomware attack in June that affected virtually all key systems, processes, and financial information, causing irreparable damage and significant budgetary costs.

In June, KNP Logistics Group was added to the Akira ransomware gang's list of victims. In September, it became known that the co-owners of the business were unable to attract additional investment and financing, and therefore were forced to take tough administrative measures. As reported by BBC, as a result of the attack, 730 group employees were fired, and Nelson Distribution Limited, part of the conglomerate, was sold, saving 170 jobs.

A company's spokesperson did not specify if KLP had contacted law enforcement or an external incident response company following the ransomware attack. It is unclear how exactly the attack influenced the decision of the business owners to shut down. According to the company, the "major ransomware attack … affected key systems, processes, and financial information. This adversely impacted the financial position of the group, and ultimately its ability to secure additional investment and funding."

KNP Logistics Group, which traded under a number of names, including Knights of Old, was added to the Akira ransomware gang's list of victims in June. In July, cybersecurity firm Avast publicly released a decryptor for the Akira ransomware.

Port of Nagoya hit by ransomware

Transportation, logistics, port

Denial of operations

Ransomware

On July 5, the Nagoya Harbor Transportation Authority announced that cargo operations had been suspended after a ransomware incident impacted the Nagoya United Terminal System (NUTS), the computer system used to operate the port's five cargo terminals. The port handles over two million containers and 165 million cargo tonnage annually, including the operations of Toyota Motor Corporation for car exports. Toyota said that it could not load or unload auto parts due to the glitch. But the company added that there was no disruption to its production so far, and the logistics of finished vehicles remain unaffected because it is managed using a different computer system.

All cargo operations, including the loading and unloading of containers onto trailers, were suspended as of July 4. The attack resulted in a temporary congestion of trailers at the port. The Nagoya port authority estimated that cargo operations would resume on July 6.

According to the Japan Times, the port authority also discovered that the LockBit 3.0 ransomware group was behind the attack. The port was fully restarted on July 6, as was estimated.

ORBCOMM hit by ransomware

Transportation, maritime, utilities, oil & gas

Denial of IT Services

Supply Chain

Ransomware

ORBCOMM, a U.S. company that provides industrial internet and machine to machine communications hardware, software and services designed to track, monitor, and control fixed and mobile assets for transportation, heavy equipment, maritime, oil and gas, utilities and government organizations, experienced a ransomware attack on September 6.

According to the comments provided to BleepingComputer, the attack temporarily impacted the FleetManager platform and Blue Tree product line (Electronic Logging Devices (ELD) that truckers use to log their hours to adhere to federal safety regulations). All other systems and service offerings remained completely operational, and customers used them as normal.

The company remained in contact with all impacted customers and continued to provide timely updates as the recovery and investigation processes progressed. The U.S. Federal Motor Carrier Safety Administration issued a waiver allowing truckers to continue using paper logs until the service is restored and no later than September 29.

BleepingComputer learned that this outage impacted some of the country's largest freight transportation companies, preventing them from tracking their fleets and inventory.

Auckland Transport hit by ransomware

Transportation

Denial of services

Ransomware

The Auckland Transport (AT) transportation authority in New Zealand responsible for public transport by ferries, busses, and trains, and for designing and building roads and other infrastructure, experienced widespread disruption caused by a cyber-incident that impacted a wide range of customer services.

The company announced that on September 13, 2023, it was impacted by a ransomware incident and experienced issues with its HOP services (integrated ticketing and fares system) as the cyber-incident impacted parts of its network. In a statement provided to a local media outlet, a spokesperson for AT stated that they had indications they had been targeted by ransomware but noted that investigations were still ongoing. The authority activated security protocols and worked with expert partners to resolve the issue as quickly as possible.

The Medusa ransomware group announced its responsibility for the ransomware attack targeted at the HOP card system of Auckland Transport on September 18.

AT chief executive Dean Kimpton confirmed it was a ransomware attack called Medusa and reassured commuters that no personal or financial data was believed to have been compromised in the incident. According to Dean Kimpton, the attackers got into the company’s transaction database storing information on HOP cards. No customer information, banking or private details have been breached nor any other systems.

Estes Express hit by cyberattack

Logistics

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

U.S. logistics company Estes Express confirmed it was the victim of a cyberattack that caused an outage in core infrastructure and impacted a number of systems according to the statement on its website and X posts on October 3. While the company was unable to share specific details at the time of the announcement, terminals and drivers effectively picked up and delivered freight while the company worked through this event. In response to a customer query, the company posted that with the outage in the online tracking system, they were unable to track and trace freight.

On October 24, Estes announced all the company's operations had returned back to normal. The company's API connections were available to integrate the shipping functionality into customer business applications and websites. The president of Estes Express also said the company had restored the image document retrieval API and worked hard to get all scanned images into the system so invoicing can resume soon with their APIs. The company's website was also restored, as was its phone service.

Forensic investigation into the incident was concluded on November 7. According to the Data Breach notification the company sent to the Main Attorney General's Office, the breach occurred on September 26 and was detected on October 1. Personal information on 21,884 individuals had been stolen, including names or other personal identifiers and social security numbers. Notification letters started being sent to affected individuals only in December, after law enforcement concluded their own investigation into the incident.

The LockBit ransomware gang claimed responsibility for the attack in early November. On November 13, the group published the data allegedly stolen from Estes on its Tor-based leak site.

DP World hit by cyberattack

Transportation, logistics, port

Data loss, denial of service and operations, personal data leakage

DP World, a Dubai-based international container terminal and supply chain operator that operates 82 terminals in 40 countries handling approximately 70 million containers annually, suffered a cyberattack that led to serious disruptions in the operation of Australia's international ports. The attack was detected on November 10 and led to the shutdown of terminals at the ports of Melbourne, Sydney, Brisbane, and Fremantle. As a result of the incident, approximately 30,000 containers of various types and values were reportedly blocked.

According to the company's official statement on its website, a third party gained access to some of the systems, including certain user accounts.

The forensic investigation identified that data was accessed and exfiltrated (removed) from the network. To contain the incident, the technology team disconnected the network from the internet, resulting in the disconnection of all external communications, including those required for land-side port operations. The company worked with the Australian Signals Directorate/Australian Cyber Security Centre, the National Cyber Security Coordinator, the Minister for Home Affairs and Cyber Security, the Minister for Infrastructure, Transport and Regional Development, and the Australian Federal Police.

Full operations across the terminals resumed on November 13. By 20 November, some seven days after port operations recommenced and 10 days after first detecting the incident, DP World Australia cleared 100% of the backlog, comprising some 30,137 containers. A company spokesman told the Financial Review that the company did not receive a ransom demand and that it didn't foresee a need to pay extortion money.

DP World Australia's investigation confirmed that the incident was confined to Australian operations and did not impact any other markets where DP World operates. It also confirmed that no ransomware was found or deployed within the DP World Australia network (no ransomware executables, no encrypted files, and no ransom demands). Some company files were accessed by the unauthorized third party and a small amount of data was exfiltrated from the DP World Australia network. The impacted data includes the personal information of current and previous employees of DP World Australia. DP World Australia notified impacted individuals.

Guyamier hit by ransomware

Transportation, logistics

Data loss, denial of service

Ransomware

French transport and logistics company Groupe Guyamier comprising several transport companies was affected by a cyberattack on November 29, resulting in the loss of access to customer files, emails, and computer files. A crisis unit was set up to try to maintain activity, while the server was “fully hacked” and a ransom demand was received without a specified amount. According to telephone comments to local press, the company was unable to contact its customers because it couldn't retrieve its order files or messages. The company isolated the affected systems to prevent the spread of the ransomware. The company switched to manual operations in order to continue operating without affecting customers.

Food & beverages

Campbell Soup hit by cyberattack

Manufacturing, food & beverage

Denial of IT systems, denial of operations

U.S. food manufacturer Campbell Soup Co. discovered a cyber-intrusion in part of its IT network during the end of its fiscal fourth quarter, according to a disclosure in its annual report filed with the Securities and Exchange Commission. (The company's fiscal fourth quarter ended July 30 and news of the attack surfaced on August 3.) The attack had a limited impact on the company's business and was not material to the company's financial results or operations, according to the SEC disclosure.

The company said it took immediate steps to investigate, contain, and eliminate the threat, hired third-party cybersecurity experts and notified federal law enforcement. According to a report by WTOL, Campbell Soup disclosed an "IT-related complication" at a factory in Napoleon, Ohio. The company told the station that impacted systems had been restored. The Toledo Blade reported the plant was offline for three days, with some production lines halted and employees temporarily sent home.

Yakult Australia hit by cyberattack

Manufacturing, food & beverage

Denial of IT systems, data leakage

Probiotic drinks manufacturer Yakult Australia confirmed experiencing a cyber-incident in a statement to BleepingComputer and on its website on December 23 that impacted the IT systems of its business in New Zealand and Australia.

Company representative said that they first became aware of the cyber-incident on December 15. The company said it was working with cyber-incident experts to investigate the extent of the incident. Yakult Australia notified the Australian Cyber Security Centre, the New Zealand National Cyber Security Centre, the Office of the Australian Information Commissioner, and the Office of the Privacy Commissioner New Zealand.

The group that claimed responsibility for the breach is DragonForce (aka DragonLeaks). It listed Yakult Australia on its onion leak site on December 20, later publishing 95.19 GB of data. A sample of leaked data was analyzed by ABC, where it found company records dating back to 2001. The cache included sensitive employee information, including scans of passports and drivers' licenses, and pre-employment information.

Oil & gas

BAZAN Group hit by DDoS attack

Oil & gas

Denial of service

Hacktivism

On July 30, Israel's largest oil refinery operator, BAZAN Group, experienced a DDoS attack, causing its website to be inaccessible from most parts of the world.

Iranian hacktivist group Cyber Avengers (aka CyberAv3ngers) claimed responsibility and leaked screenshots of the refinery's SCADA systems. BAZAN denied the leaked materials, labeling them as "entirely fabricated." They reported no damage to their servers or assets, and their cybersecurity measures are vigilant, working closely with the Israeli National Cyber Directorate.

The hacktivist group also implied that they breached the refinery via a Check Point firewall, but the cybersecurity company denied any vulnerability. The Cyber Avengers previously claimed responsibility for the 2021 fires and attacks on Israeli railway stations.

Shipbuilding

Austal USA hit by ransomware

Manufacturing, shipbuilding

At the beginning of December, Australian-based U.S. defense contractor Austal USA specializing in the production of advanced high-tech ships confirmed a cyberattack after the Hunters International ransomware group listed the company and shared samples of the stolen data as proof. Austal USA stated that they quickly managed to detect the incident and localize its consequences, which, according to official data, did not affect operational activities. It also stated that no personal or classified information was accessed or taken by the threat actor. The FBI and U.S. Naval Criminal Investigative Service (NCIS) joined the investigation of the incident and extent of information accessed. Hunters International threatened the publication of the stolen data, including certification, personnel, financial, and engineering documentation.

Metallurgy

Röhr + Stolberg GmbH hit by ransomware

Manufacturing, metallurgy

Denial of operations

Ransomware

German metal processing company Röhr + Stolberg GmbH became a victim to a ransomware attack on October 20. The company's IT team and a team of external specialists managed to restart the servers within a week, which meant that a large part of operations, including production, became operational. At the time of the announcement, the systems remained disconnected from the internet. Communications with customers, suppliers and service providers was guaranteed via secure computers that were located outside of the potentially affected environment. The police and data protection authorities were informed about the incident. Röhr+ Stolberg does not rule out the possibility that cybercriminals stole the company's data.

The LockBit ransomware gang listed Röhr+ Stolberg on their site.

Construction

Verhelst Groep hit by cyberattack

Construction

Denial of service and operations

Ransomware

Belgian construction company Verhelst Groep fell victim to a cyberattack according to the message on its website published on October 18. It notified that their general operations were affected. The company could no longer communicate with customers and lost overview of stock and transport. Some of the staff had to stay at home, and a team from State Security arrived on site and started working together with the IT team and other professional organizations. Gradually, they managed to start up new software and recover data from their own cloud. The Falcon ransomware gang listed the company on their website.

BAUER Group hit by cyberattack

Construction

Denial of IT systems and service

German construction company Bauer AG was the target of a cyberattack, which was announced on October 31. According to the statement, despite the considerable security measures, unknown persons managed to access the company's servers, leading to various systems of the company being shut down or switched off as a precaution on October 30, 2023. Among other things, this also affected the group's websites. Bauer called in additional experts who analyzed the situation together with the IT department.

Consequently, restrictions were put in place for the business partners of BAUER Group companies worldwide. Bauer informed the responsible authorities about the incident. The company worked at full speed to find a solution and restart the systems, and asked all affected business partners for their understanding for any disruptions. On December 13, the company published an update stating that all operations had been resumed.

Koh Brothers Eco hit by ransomware

Construction

Denial of IT systems

Ransomware

Singaporean construction company and sustainable engineering solutions provider Koh Brothers Eco Engineering was the target of a cyberattack in which the servers in certain subsidiaries of the company were subjected to unauthorized access and encryption. While the investigation indicated that the incident was under control, the company said on December 4 that it was unable to assess the extent of the impact of the cyberattack on the group and its operations. The group's business continued to be operational notwithstanding the incident. The company noted that it took prompt steps to contain the incident, including disconnecting the affected servers from the network and preventing further unauthorized access to its IT network. The group additionally engaged incident response experts and external legal counsel to assess, respond to, and manage the incident.

Other

Freeport-McMoRan hit by cyberattack

Mining

Denial of operations

Freeport-McMoRan (FCX), an international mining company headquartered in the U.S., fell victim to a cyberattack as announced on August 11, 2023.

The company evaluated the extent of the impact and took proactive measures to address the situation. FCX collaborated closely with third-party cybersecurity experts and law enforcement agencies in its response and was in the process of planning and implementing transitional solutions to swiftly secure its information systems. Safety and responsible production practices remain top priorities for FCX, but the company acknowledged that a prolonged disruption could potentially impact its future operations. Further details about the nature and scope of the cyberattack had not been disclosed at the time of publication.

Japan Aerospace Exploration Agency hit by cyberattack

Aerospace

Denial of IT services

The Japan Aerospace Exploration Agency (JAXA) was the target of a cyberattack over the summer as reported by The Japan News. Law enforcement notified JAXA that their systems had been compromised in autumn and no details were provided about exactly when the attack occurred.

Confirming the infiltration, Chief Cabinet Secretary of Japan revealed in a press conference that the attackers gained access to the agency's Active Directory (AD) server, a crucial component overseeing JAXA's network operations.

In response to the incident, JAXA worked with government cybersecurity experts and law enforcement as part of an ongoing investigation to determine the extent of the security compromise. Although no data leak linked to the JAXA breach had been confirmed, a JAXA official expressed concerns, stating that "as long as the AD server was hacked, it was very likely that most of the information was visible."

A local media outlet, Nippon, reported that the hackers allegedly exploited a vulnerability disclosed by a network equipment manufacturer in June 2023, citing sources within the agency. The manufacturer's name wasn't mentioned.

During the investigation, the agency temporarily shut down a part of its network to assess the extent of the incident. An official at the agency said no data leaks had been confirmed so far. JAXA did not respond to a request for comment.

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