Kaspersky ICS CERT

kaspersky

H2 2022 – brief overview of main incidents in industrial cybersecurity

15.03.2023

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 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.

Ransomware attacks

This overview includes incidents in which affected organizations officially confirmed the compromise. Compromise reported by cybercriminal groups only is not discussed.

Creos and Enovos

Luxembourg-based energy provider Encevo has acknowledged on July 25 that some of its subsidiaries – a natural gas pipeline and electricity network operator Creos and an energy supplier Enovos – were targeted by a cyberattack.

Encevo says that the attackers exfiltrated data and rendered data inaccessible. The attack took down both companies' customer portals. The incident response team was immediately activated and customers were advised to reset their account credentials. Encevo registered a complaint with the Grand Ducal Police, as well as notifying the CNPD (National Commission for Data Protection), the ILR (Luxembourg Institute of Regulation) and the competent ministries.

The ALPHV ransomware gang, aka BlackCat, claimed responsibility for the cyberattack against Creos and added it to its extortion site on Saturday, threatening to publish 180,000 stolen files totaling 150 GB in size, including contracts, agreements, passports, bills, and emails.

Cremo

Swiss dairy giant Cremo fell victim to a cyberattack in July. The company filed a criminal complaint with the police and an investigation was initiated. According to Cremo secretary general, data was stolen and the hackers demanded a ransom. Despite the attack, the company was able to maintain production and customer deliveries. An internal source confirmed that production was not impacted, but the electronic tools were down at least on some of the company's sites, resulting in emails, orders and invoices being unavailable.

Semikron

German semiconductor manufacturer Semikron announced on August 1 that it had fallen victim to a cyberattack, which resulted in "partial encryption of IT systems and files". The threat actors behind the attack claimed to have exfiltrated the company's data. Semikron immediately took all necessary measures to limit possible damage, investigated the incident and worked on minimizing the impact of the incident on its employees, customers and contractual partners.

The company didn't name the attacker, but BleepingComputer, which saw a ransom note on one of Semikron systems, reported that LV Ransomware might be behind the attack and that they claim to have stolen two terabytes of company data.

BRP

Canadian manufacturer of motorized recreational vehicles BRP (Bombardier Recreational Products) disclosed on August 9 that it had been the target of "malicious cybersecurity activity" and that it had taken "immediate measures to contain the situation." Those measures included activating its "internal network of IT professionals" and hiring cybersecurity experts to help secure its computer systems and assist with an internal investigation. Operations were temporarily suspended and were later resumed. Austrian engine manufacturer Rotax, a BRP subsidiary, was also affected by the cyberattack and had to suspend its operations.

On August 15, BRP reported that its efforts to restore systems and business operations were continuing and its manufacturing sites in four countries were ramping up production activities and would be fully operational on August 16. The rest of the production sites were planned to resume operations over the course of the week in a phased approach. In the same statement, the company presented the first results of its internal investigation, saying that the hackers had breached its systems via a third-party service provider.

The RansomEXX ransomware gang took responsibility for the "malicious cyberactivity" and for stealing 29.9GB of files pertaining to non-disclosure agreements, passports, IDs, contracts, and supply agreements.

On August 23, BRP issued a statement confirming that the leaked documents were authentic, adding that it was actively supporting impacted parties to mitigate any negative effects of the exposure. BRP confirmed that it had contacted the few employees possibly impacted by the incident.

Cisco

Cisco, a multinational technology conglomerate and network equipment manufacturer, released a security incident notice and a technical blog post detailing a breach that was detected on May 24. The company shared details about the attack on August 10, shortly after the cybercriminals published a list of files allegedly stolen from its systems.

According to Cisco, the attackers targeted one of its employees and only managed to steal files stored in a Box folder associated with that employee's

account, as well as employee authentication data from Active Directory. The company claims the information stored in the Box folder was not sensitive.

For initial access, the attackers targeted the personal Google account of an employee. The hackers obtained the employee's Cisco credentials via Chrome, which was configured to sync passwords. In order to bypass multi-factor authentication (MFA), the attackers used a technique known as MFA fatigue, which involves sending a high volume of push requests to the target's mobile device in hopes that they will accept a request either by accident or in an attempt to silence the notifications.

The targeted employee also received multiple phone calls over a period of several days, where the caller — claiming to be associated with a support organization — attempted to trick them into handing over information. Eventually, the attackers managed to enroll new devices for MFA and authenticate to the Cisco VPN. Once that was achieved, the attackers escalated to administrative privileges, allowing them to log in to multiple systems, then started dropping remote-access and post-exploitation tools. The hackers created backdoors for persistence and moved to other systems in the environment, including Citrix servers and domain controllers.

Cisco has attributed the attack to an initial access broker with ties to the threat actor UNC2447, a Russia-linked group known for using FiveHands and HelloKitty ransomware, as well as Lapsus$. The gang targeted several major companies before its alleged members were identified by law enforcement. The initial access broker has also been linked to the Yanluowang ransomware gang. The Yanluowang gang has taken responsibility for the attack, claiming to have stolen roughly 3,000 files having a total size of 2.8 Gb. The file names published by the hackers seem to reference VPN clients, source code, NDAs, and other documents.

South Staffordshire PLC

South Staffordshire PLC, a U.K. water supplier and the parent company of South Staffs Water and Cambridge Water, confirmed on August 15 that it was the victim of a cyber-attack. According to the official statement, the company experienced disruption to its corporate IT network, which did not affect its "ability to supply safe water" to all of its customers.

The alleged attack perpetrator—the Clop ransomware group—claimed the attack was on another, larger water utility Thames Water, which for its part called the claim a "cyber hoax." In its post, the Clop gang claimed to have exfiltrated more than 5 TB of data from the victim organization and to have

accessed some SCADA systems. Within a couple of days, Clop updated its website, saying it was South Staffordshire that it had attacked, and not Thames.

DESFA

Greece's largest natural gas distributor DESFA confirmed on August 20 that it had fallen victim to a cyberattack that impacted the availability of some systems, and as a result of which data was leaked. DESFA said it had proactively deactivated many of its internet-facing IT services to protect customer data and was gradually restoring them to normal operation. The company also informed the police cybercrime department, the national data protection office, the national defense department, and the ministry of energy and environment to help resolve the matter with minimal time losses and consequences.

The Ragnar Locker ransomware gang took responsibility for the attack, claiming to have stolen sensitive corporate data. The attackers published a list of information they claimed to have stolen on their extortion website, along with a small collection of stolen documents that didn't seem to contain any confidential data. Additionally, the ransomware gang claimed to have discovered numerous security flaws in DESFA's systems and notified the natural gas company, probably as part of their extortion scheme. DESFA did not respond to the threat actor's ransom demands.

Eni

Bloomberg News reported an attack on Italian oil giant Eni on August 31, speculating that Eni appeared to have been hit by a ransomware attack.

Eni confirmed an intrusion into its corporate network. According to the company's spokesperson, the intrusion had minimal consequences because it was quickly detected. The company reported the incident to the Italian authorities, who launched an investigation to determine the extent of the attack.

Eni provided no technical details and it is unknown how the attackers breached the company and what their motivation was.

Hensoldt

The IT infrastructure of the defense electronics manufacturer Hensoldt Nexeya France, a French subsidiary of HENSOLDT AG, was targeted by a cyberattack. According to Hensoldt, a significant amount of data was likely accessed and systems have been encrypted. Hensoldt initiated a comprehensive investigation into the incident, in close cooperation with the authorities. According to the

company, the IT infrastructure and data of other companies in the Hensoldt Group were not affected.

Elbit Systems

Elbit Systems of America, a subsidiary of Israeli defense contractor Elbit Systems, confirmed a data breach, several months after a ransomware gang claimed to have hacked the company's systems. In a breach notification filed with the Maine Attorney General's office, the company said the breach occurred on June 8 and was discovered on the same day. It said only 369 people were affected. Information stolen by the attackers may have included employee names, addresses, dates of birth, direct deposit information, ethnicity, and Social Security numbers. The company shared few details, only that "someone attempted to interfere with Elbit America's cyber operations" and that its investigation was ongoing. The Black Basta ransomware gang announced hacking Elbit Systems of America in late June. According to the group's Tor-based leak website, all of the files stolen from Elbit have been made public.

Läderach

Chocolate manufacturer Läderach in Switzerland has been targeted by a cyberattack. According to the company's statement, the attack was detected on the morning of September 5. It affected the chocolatier's production, logistics and administration. Over the course of two weeks the company was able to resume work almost to the full extent.

The online news portal Inside-IT found several data packages from the Läderach network on the dark web that had been uploaded by the Bianlian ransomware gang. According to the cybercriminals, those were business files such as management documents, files on product development and future projects, budget planning and analysis, and technical files. At the moment of publication, a spokesperson at Läderach was unable to confirm the validity of the data uploaded to the threat actor's resource and said that the company "will continue to monitor the situation together with the authorities involved – and inform those affected again if necessary".

Tata Power

On October 14, the largest Indian energy company, Tata Power Company Limited, confirmed that it was targeted by a cyberattack, which affected its IT infrastructure. The company said that all necessary steps had been taken to restore its systems, adding that all critical operational systems were functioning. As a precaution, limited access and preventive checks were introduced for

employees and customers when interacting with portals in order to prevent unauthorized access.

The Mumbai-based electricity company, which is part of the Tata Group conglomerate, did not release any further details about the nature of the attack or when it occurred.

The Hive ransomware group claimed responsibility for the attacks. Hive hackers claimed to have encrypted Tata Power systems on October 3, revealing the attack on October 24 in a message on their DarkWeb website. The hackers uploaded a sample of the stolen files, including employment contracts, supplier contracts, files on various employees, documents detailing executive compensation packages, and more.

German newspaper printing

A ransomware attack caused the shutdown of systems that are used to print several German newspapers. The attack disrupted the operation of the Stimme Mediengruppe, whose publications include Heilbronner Stimme, Pressedruck, Echo, and RegioMail.

According to Heilbronner Stimme editor-in-chief, the attack was conducted by a well-known cybercriminal group that encrypted their systems on the night of October 14 and left ransom notes behind. A crisis team was set up and cybersecurity experts launched an investigation. The police and the Ministry of the Interior were involved in the investigation. Interior Minister Strobl offered the support of cybersecurity experts from the state of Baden-Württemberg.

U-blox

U-blox, a Swiss company that creates wireless semiconductors and modules for consumer, automotive and industrial markets, said on October 28 that it had been targeted by a ransomware attack, which was detected and contained on October 24.

The attack caused outages in several internal IT systems. The company stated that neither customer data nor intellectual property had been compromised, production had not been impacted and recovery was far advanced. The cyberattack affected the availability of the ERP system and this might cause shipments to be delayed.

The company engaged external cybersecurity experts to assist in conducting a comprehensive forensic review of the incident. To further reduce the risk to customers, employees and the company, internal and external experts prepared

protection and mitigation plans. Furthermore, u-blox involved the local authorities to further investigate the attack and to prosecute.

Richard Wolf

Medical equipment manufacturer Richard Wolf suffered a cyberattack in early November. According to the company's press release, the attackers encrypted the company's data. Almost three weeks after the incident, the company stated that all restrictions on phones and email accounts had been resolved and the company expected its remaining IT services to be functional by the end of the week.

The company engaged external IT forensics experts to ensure the cybersecurity of its systems. Richard Wolf said it had prepared for precisely this scenario in recent years by taking technical and organizational precautions, employing specialist personnel, conducting internal training and consulting externally. After the attack, all relevant authorities, suppliers, major customers and the workforce were informed immediately. The company did not respond to the ransom demand.

Uponor

Finnish utility equipment manufacturer Uponor announced in its press release that the company's operations were affected by a ransomware attack discovered on November 5. Based on the investigations, Uponor also found evidence of a data breach affecting the company's employee, customer and partner data. Uponor believed that the breached data had not been made available in the public domain.

After the attack, the company took immediate action to investigate and remediate the situation. One of these actions was to shut down all systems and production as a precautionary measure. After one week of production shutdown, operating levels started to recover, and customer deliveries restarted in all divisions. After that, Uponor focused on accelerating operational performance back to the operating levels before the attack while protecting the company's systems.

Maple Leaf Foods

On November 6, Canadian food manufacturer Maple Leaf Foods released a statement, in which it said it was experiencing a system outage linked to a cybersecurity incident. The company executed its business continuity plans as it worked to restore the impacted systems. It expected that full resolution of the

outage would take time and did not rule out operational and service disruptions. After the company's announcement, the Black Basta ransomware gang took responsibility for the attack and listed Maple Leaf Foods as one of its victims. It uploaded several screenshots of technical documents, financial information and other corporate files to demonstrate that they had gained access to Maple Leaf Foods systems.

Sargent & Lundy

Sargent & Lundy, a Chicago-based construction and engineering firm that has designed hundreds of power stations in the US, fell victim to a cyberattack. Sargent & Lundy suffered a data breach on October 15, resulting in threat actors stealing personal identifiable information (PII) from the company's systems. According to Turke & Strauss, a law firm that issued the breach notification on the company's behalf on December 8, exposed information may include names and social security numbers of over 6,900 individuals. According to a memo describing the hack, which has been obtained by the CNN, investigators closely monitored darknet forums for data stolen in the attack and attributed the attack to the Black Basta ransomware gang.

JAKKS Pacific

On December 8, US-based toy manufacturer JAKKS Pacific was hit by ransomware that encrypted the company's servers. JAKKS hired cybersecurity experts to deal with the incident and restore their servers. The company filed documents confirming the incident with the U.S. Securities and Exchange Commission in mid-December. According to the company's statement, data that was unlawfully accessed potentially included personal information (including names, emails, addresses, taxpayer identification numbers, and banking information of affected individuals and businesses).

Two different ransomware gangs, Hive and BlackCat, took responsibility for the attack and posted data stolen from JAKKS. Hive leaked first, posting stolen information on December 19. BlackCat followed on December 28 with screenshots of information uploaded to their leak site. A spokesperson for the Hive ransomware gang told DataBreaches that both groups had bought access to the company's network from an initial access broker and agreed to split a $5 million ransom. The company refused to pay and did not negotiate, the spokesperson said.

Fruttagel

Italian food and beverage manufacturer Fruttagel suffered a cyberattack on December 11. As a result of the attack, some of the company's information systems were compromised.

According to Fruttagel's statement published by a local newspaper, the company promptly activated emergency procedures, resorting to the expertise of its own personnel and cybersecurity experts. However, it was not able to avoid a serious disruption of its production process and was temporarily unable to ship products to all customers.

After the statement was released, the BlackCat/ALPHV ransomware gang added Fruttagel to their victim list. They claimed to have access to 720 GB of corporate data, including financial information, contracts, and large volumes of other data.

EPM

In December, Empresas Públicas de Medellín (EPM), a Colombian energy provider, was hit with a ransomware attack, which disrupted the company's operations and took down online services. Employees were instructed to work from home as the company's IT systems were down. The BlackCat ransomware group, also known as ALPHV, claimed responsibility for the attack. Following the discovery by a Chilean security researcher of a recent sample of BlackCat's ExMatter data-theft tool, which was uploaded to a malware analysis site from Colombia, further discoveries indicated that hackers likely stole a large volume of data from EPM during the attack. The ExMatter variant from Colombia uploaded data to a remote server that was not secured, where it was stored in folders with different names prefixed with 'EPM-'. These computer names match known computer naming formats used by Empresas Públicas de Medellín.

Thyssenkrupp

The German industrial engineering and steel manufacturer Thyssenkrupp was hit by a cyberattack. The company's security service detected the incident at an early stage, and the attackers failed to cause significant damage. Only some segments of ThyssenKrupp IT were affected, including the Materials Services division and corporate headquarters. The company has found no evidence that any of its data has been stolen or altered. The possibility that other segments and business units were affected by the attack has also been ruled out.

A crisis team was quickly created to investigate the incident and eliminate its consequences. The company told reporters that organized crime was behind the

attack, but did not specify whether it was a ransomware attack. However, everything points to ransomware, because over the past few years Thyssenkrupp has also been targeted by several ransomware gangs, including Netwalker.

CMMC

The Canadian Copper Mountain Mining Corporation (CMMC) announced that it was affected by a ransomware attack, which occurred late on December 27. The company's IT team responded quickly by implementing predefined risk management systems and protocols. To contain the incident, CMMC isolated infected systems to examine them thoroughly and determine the ransomware attack's impact. CMMC's engineers had to shut down the mill as a preventative measure to determine the status of its control system, while other processes switched to manual operations.

According to the announcement, Copper Mountain was investigating the source of the attack and was in contact with the relevant authorities. CMMC's announcement clarifies that the cybersecurity incident did not compromise the safety measures or cause any kind of environmental damage. The company's main priority was to return to normal operations as soon as possible, limiting the financial impact of the incident.

Port of Lisbon

The Port of Lisbon became the target of a cyberattack on December 25. According to the announcement given to the local newspaper, the crime did not affect the port's operations. All security protocols and response measures planned for this type of occurrence were quickly activated. The company also notified the National Cybersecurity Center and the Judiciary Police. The company's website was unavailable at the time of the announcement.

On December 29, the LockBit ransomware gang took responsibility for the attack against the port, claiming to have stolen financial reports, audits, budgets, contracts, ship logs and other information about cargo and crews. The gang threatened to publish all of the files stolen in the computer attack if the company failed to satisfy their ransom demands of $1.5 million.

MOL

Belgian vehicle manufacturer and supplier of machine parts MOL Cy was hit by a cyberattack. According to a short message published on its website, the company promptly informed the authorities about the breach. It was also

decided to immediately call in a professional external company for help. The message stated that "the extent of the attack is now known and the entire team is doing everything to be 100% operational again as soon as possible" and "the company can be reached again by phone and very soon via the usual email addresses". The Royal ransomware gang listed MOL Cy on its Tor-based leak website and uploaded files stolen from the company.

Sumitomo Bakelite North America

Sumitomo Bakelite North America, a US subsidiary of a Japanese plastics manufacturer, fell victim to a cyberattack, according to an official statement. The company promptly reported the matter to the US authorities and launched an investigation of the details of the attack and the extent of its impact.

The U.S. subsidiary fully cooperates with the relevant U.S. authorities regarding the incident. The company has taken security measures in the past, but in response to this incident, it will review and strengthen their existing protection and security policies.

The BlackCat/ALPHV ransomware group claimed responsibility for the attack.

CISA alerts

Zeppelin Ransomware attacks

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) have released a joint Cybersecurity Advisory to disseminate known Zeppelin ransomware IOCs and TTPs associated with ransomware variants identified through FBI investigations as recently as 21 June 2022.

Zeppelin ransomware is a derivative of the Delphi-based Vega malware family and functions as a Ransomware as a Service (RaaS). From 2019 through at least June 2022, actors have used this malware to target a wide range of businesses and critical infrastructure organizations, including defense contractors, educational institutions, manufacturers, technology companies, and especially organizations in the healthcare and medical industries.

Zeppelin actors gain access to victim networks via RDP exploitation, exploiting SonicWall firewall vulnerabilities, and phishing campaigns. Prior to deploying Zeppelin ransomware, actors spend one to two weeks mapping or enumerating the victim network to identify data enclaves, including cloud storage and network backups. Prior to encryption, Zeppelin actors exfiltrate sensitive company data files to sell or publish in the event that the victim refuses to pay the ransom.

Hive Ransomware

The Cybersecurity and Infrastructure Security Agency (CISA), together with the Federal Bureau of Investigation (FBI) and the Department of Health and Human Services (HHS), published a joint alert about the Hive ransomware group, which targeted a wide range of businesses and infrastructure sectors, including Government Facilities, Communications, Critical Manufacturing, Information Technology, and especially Healthcare and Public Health.

The alert lists known Hive IOCs and TTPs identified through FBI investigations as recently as November 2022. It also states that the Hive ransomware group has received over US$100 million in ransomware payments. The actor's methods of initial intrusion include using single factor logins via RDP, VPNs, and other remote network connection protocols. In some cases, Hive actors have bypassed multifactor authentication and gained access to FortiOS servers by exploiting CVE-2020-12812. This vulnerability enables a malicious cyber actor to log in without a prompt for the user's second authentication factor (FortiToken) when the actor changes the case of the username. Hive actors have also gained initial access to victim networks by distributing phishing emails with malicious attachments and by exploiting three vulnerabilities against Microsoft Exchange servers.

Cuba Ransomware

Cybersecurity and Infrastructure Security Agency (CISA) published a joint alert with the Federal Bureau of Investigation (FBI) to disseminate known Cuba ransomware IOCs and TTPs associated with Cuba ransomware actors identified through FBI investigations, third-party reporting, and open-source reporting. The main targets of Cuba ransomware attacks are financial services, government, healthcare and public health, critical manufacturing, and information technology. The attackers used known vulnerabilities (CVE-2022-24521, CVE-2020-1472), phishing, PowerShell scripts, KerberCache tool, compromised credentials and RDP to gain access, then used the Hancitor loader to drop their ransomware.

Other cyberattacks and data thefts

Weidmüller

German electronics manufacturer Weidmüller has fallen victim to a cyberattack that was detected on July 18. According to the company's press release, Weidmüller used its technical capabilities and isolated all systems in order to carry out a precise analysis and also to protect its customers, partners and employees. The most important internal and external communication channels, as well as SAP systems, were not affected. The company's production process was largely uninterrupted and almost all of the affected systems have been restored.

Hettich Group

A Chinese production company of the Hettich Group, a manufacturer of furniture fittings, was targeted by a cyberattack. The IT specialists of the Hettich Group, supported by external experts, worked to successfully fend off the attack and enhance the security of the company's systems. In a press release published on August 15 the company couldn't say when the Chinese subsidiary would be able to fully access all of IT systems again but stated that the local production facility in China remained operational. The holding company believed that other companies of the Hettich Group were not affected.

Sembcorp Marine

Sembcorp Marine, a shipbuilding and engineering company, discovered a cybersecurity incident where an unauthorized party had accessed part of its IT network via third-party software. The company established that certain personally identifiable information relating to some of its incoming, existing and former employees, as well as non-critical information relating to its operations, was affected. It engaged cybersecurity experts to conduct a detailed analysis in order to address all breaches and related root causes, assist with impact assessment, and to review and enhance security. The company confirmed it had notified the relevant authorities in Singapore and was closely collaborating with them in this regard.

Continental

The automotive supplier and tire manufacturer Continental has been targeted by a cyberattack, which was detected in early August. In a statement released on August 24, Continental claimed that its business activities had not been

affected at any point and that it maintained full control over its IT systems. Third-party IT systems were not affected, either. The company conducted an investigation into the incident with support from external cybersecurity experts.

Eurocell

Eurocell, a UK-based PVC-U manufacturer, was hit by a cyberattack, which led to critical personal details of employees being leaked. The data leaked includes bank account details, dates of birth, next-of-kin information, national insurance numbers and tax information, health and well-being information, disciplinary and grievance related documents, etc. The company sent out a letter to employees, explaining that an unauthorized third party was able to gain access to their systems following an IT security incident. While Eurocell have claimed that there is 'no evidence' of this data being misused, there is no guarantee that this is the case, or will continue to remain the case in the future. Eurocell have noted that they have informed the Information Commissioner's Office and the police about the incident.

Enercity

Enercity, one of Germany's largest municipal energy suppliers, confirmed that it was targeted by a cyberattack on October 26. The company said its security systems reacted immediately, averting greater damage to the company. Enercity confirmed that it would continue supplying energy to customers, explaining that its operational technology and critical infrastructure was not affected. However, the attack impacted customer service, which was not fully available.

Aurubis

Aurubis, the largest copper producer and recycler in Europe, said in a statement that a cyberattack on its IT systems occurred on October 28. The attack did not stop production, but it did cause the company's IT systems to be temporarily shut down. As a preventative measure Aurubis disconnected its systems from the internet, but smelter sites across Europe and production facilities remained operational. The company worked closely with the authorities to investigate the attack. The company stated that this was apparently part of a larger attack on the metals and mining industry.

Eesti Energia

In November, the website and online channels of Estonian state electricity generator Eesti Energia and some of its related companies went offline following a large-scale denial of service attack. The attack affected Eesti Energia's site and mobile app, Enefit Green website, and also grid maintenance firm Elektrilevi's website, and its MARU mobile app. According to Eesti Energia's head of business and IT, customer data and the group's IT systems were fully protected and the attack was successfully repelled.

Iochpe-Maxion

Brazilian automobile components manufacturer Iochpe-Maxion announced that it had suffered a cyberattack on December 5 in its IT environment. The attack resulted in the unavailability of part of its systems and operations in some units in Brazil and abroad. The company explained in a statement sent to the Brazilian Securities Commission that it had activated its security protocols to contain the cyberattack and isolated some of its systems to protect the environment. The company confirmed that, together with its specialized advisors, it was acting diligently and making every effort to identify the causes of the incident, determine its extent and mitigate its effects.

Meyer&Meyer

German logistics and transportation company Meyer&Meyer fell victim to a cyberattack on December 6. According to the company's statement, the criminal attack affected the company's business activities. Despite having to shut down their systems, the company was able to maintain part of its business operations after the cyberattack by switching to manual processes. The company reacted to the targeted attack quickly and decisively and isolated their IT systems. It immediately informed its employees and business partners about the development and worked closely with law enforcement and data protection authorities.

NIO Inc

China-based electric automaker Nio Inc announced on December 20 that hackers had breached its computer systems and accessed data on the company's users and on its vehicle sales. According to media reports, the hackers had sent an email to the electric carmaker demanding $2.25 million in Bitcoin in return for not releasing the data. The company said it was working with government authorities to investigate the data breach.

Hacktivists

GhostSec attacks on Berghof PLCs

Researchers at OTORIO published a report about an attack on industrial control systems. On September 4, 2022 the hacktivist group GhostSec, which was previously observed targeting Israeli organizations and platforms, announced on social media and its Telegram channel that it had successfully breached 55 Berghof PLC devices in Israel. In the message that it published, GhostSec attached a video demonstrating a successful login to the admin panel of the PLC, together with an image of an HMI screen showing the current status and control of the PLC process and another image, which shows that the PLC has stopped.

The researchers decided to have a closer look at the incident's details to understand how GhostSec was able to gain control over these PLCs and to assess the underlying risks. At the time of the investigation, the devices' IPs were still accessible via the internet and access to the admin panel was password-protected. However, trying some default and common credentials resulted in a successful login. Although access to the admin panel allows full control over some functions of the PLC, it does not give direct control over the industrial process. The research also revealed that Berghof uses HMI based on the CODESYS technology and the HMI was also accessible via the browser at a specific address. An analysis of the GhostSec breach did not reveal whether GhostSec had gained access to the HMI. However, the researchers confirmed that the HMI screen was also publicly available.

The fact that GhostSec likely did not access the HMI or tamper with it and that the hackers did not exploit the Modbus interface shows that they are not familiar with the OT realm. There wasn't any evidence that GhostSec caused any critical damage to the affected systems. Apparently, they were merely trying to draw attention to the hacktivist group and its activities.

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global project of Kaspersky 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