Kaspersky ICS CERT

kaspersky

H1 2022 – a brief overview of the main incidents in industrial cybersecurity

08.09.2022

Version 1.0

From the very start of 2022 we see and hear about hair-raising incidents in the news where each new event causes yet another grey hair. Events in the cybersecurity world, including ICS, were also intense in H1 2022.

- The geopolitical situation caused a surge in hacktivist activities, whereby even industrial entities were attacked in addition to the obvious targets: government organizations and the media.

- In the meantime, we saw that nothing ever stops threat actors from trying to make profits. Ransom demands are seen everywhere – attacks were made on different sectors and in different regions of the world: automotive industry, renewable energy, electronics manufacturers and an oil-and-gas company. Naturally, we will not include every incident in our overview.

- APTs are still spying and they are interested not only in politics, but in technologies.

- Threat actors continue to perfect attack techniques, tactics and scenarios. We are observing a dangerous tendency to write new malware targeting industrial organizations.

The H1 2022 kaleidoscope of events kept industrial cybersecurity experts busy around the world. Let's take a look at some of the more colorful events of H1.

Hacktivists

Attack on Belarusian Railway

Hacktivism is definitely a noticeable trend in 2022 – threat actors are alive and kicking. One of the first attacks occurred in January 2022 where the threat actors penetrated the infrastructure of the Belarusian Railway. Numerous BR systems were encrypted as a result. The hackers demanded that the Belarus government cease aiding the Russian military. A group called Cyber Partisans claimed responsibility for this attack.

Attack on electric car charging stations in Russia

The shift in geopolitics as of February 24 also stimulated hacktivist attacks. On February 28 electric car charging stations on M-11 in Russia were deactivated and their screens showed political slogans. It turned out that their development had been outsourced to a company located in Kharkiv, Ukraine. The owner of the stations, Rosseti, reacted swiftly and replaced the firmware on the charging stations.

Attack on Rosneft Deutschland

In mid-March, Rosneft Deutschland GmbH (the German subsidiary of Rosneft – a Russian oil company) also underwent a cyberattack. The hacker group Anonymous claimed responsibility. Anonymous claimed that they had captured 20 terabytes of data from Rosneft Deutschland. It seems that as a result the company's internal processes, specifically contract management, were disrupted. According to official company statements no other consequences were apparent - pipelines and refineries continued normal operations without interruptions.

Attacks on a Russian food processing organizations

Seliatino Agrohub

On February 26 Seliatino Agrohub underwent an attack on their frozen foods facility in the Moscow region. An unknown user nicknamed 'Supervisor' penetrated the refrigeration remote monitoring network and changed the temperature settings from – 24° C to +30° in a facility where 40 tons of frozen meat and fish were stored.

Miratorg Agribusiness Holding

On March 18 Miratorg Holding, one of Russia's largest meat producers, was attacked using the Bitlocker ransomware. The attack targeted warehouse and accounting IT resources. It also interrupted the processing pipeline for electronic veterinary documentation. Eighteen companies in the Miratorg group were affected.

Rosselkhoznadzor (a government agency regulating agricultural affairs) announced that the group resumed normal operations on March 28. Unlike most ransomware attacks, the attackers did not demand money, so commercial interests were not the motivation for the attack.

Tavr corporate group

On March 24 a cyberattack was conducted on Tavr, a major Russian food processing group in the Rostov region, a member of the Agrokom group of companies. As per the official company statement, the company business processes, including production, were temporarily paralyzed and a significant economic loss was recorded. A company representative assessed the event as "meticulously planned and significant sabotage".

Attack on Iranian steel companies

In June we learned of a cyberattack on Iranian steel companies Hormozgan, Khouzestan and Mobarakeh. According to the attackers and several independent analysts, the attack disrupted the industrial process at the Khouzestan Steel works. However, the company itself denies that there were any disruptions in operations. The hacktivist group Gonjeshk'e Darandeh (also known as Indra) claimed responsibility. This same group had attacked Iranian Rail in June 2021, causing massive delays and disruptions in logistics.

Ransomware

Attacks on automotive producers

Attack on tire producer Bridgestone Americas

On February 27 Bridgestone Americas announced that they had launched an investigation of a possible compromise of their IT systems. To prevent the malware from spreading, computer networks were disconnected and production halted at many facilities in Latin and North America. On March 11 it was confirmed that the attack was conducted by the LockBit ransomware group. The group added Bridgestone to their victim list and demanded a ransom, threatening to release the stolen data if the money was not paid.

Attack on a Toyota supplier Kojima Industries – Toyota affected

On February 28 Toyota announced that they were suspending operations at 14 plants in Japan for 24 hours due to a cyberattack on a supplier – Kojima Industries. The victim produces key components for cars, without which production is impossible. Details of the attack on Kojima Industries were not revealed. In our opinion, ransomware is the most likely suspect.

In any case, here we have a classic example of a supply chain cyberattack which once again disrupted a major company and halted operations.

Pandora ransomware attack on automotive parts manufacturer DENSO

Just two weeks after the Toyota incident, on March 13, another cyberattack was reported – this time on DENSO Automotive Deutschland. DENSO is the second largest manufacturer of automotive parts in the world and the largest parts supplier for Toyota. The Pandora group claimed to have stolen 1.4 TB of data from DENSO Automotive Deutschland. DENSO confirmed "unauthorized access using ransomware". In this case, operations were not affected, but DENSO cannot be happy about the stolen data, which included proprietary documentation.

Attacks on wind turbine companies

Conti ransomware attack on wind turbine producer Nordex

In early April Nordex, a major producer of wind turbines, announced that they had undergone a cyberattack. When the attack was detected, Nordex shut down IT systems and closed remote access to managed wind turbines, thus preventing the malware from spreading further. As a result, only the internal IT network suffered. The Conti group claimed responsibility.

Black Basta attack on Deutsche Windtechnik

On April 11 systems of Deutsche Windtechnik, a German wind turbine servicing company, were targeted by a cyberattack. The company responded by switching off all internal systems as well as remote data monitoring connections to the wind turbines for security reasons. It took two days to restore normal operations. The company disclosed that the attackers used ransomware only after Black Basta added Windtechnik to their victim list, which is posted on their Tor site.

Enercon

Even though Enercon, a wind turbine producer, did not suffer a ransomware attack (see APT section in this report) and was only hit by ricochet, we will mention them in this section as well.

In February, as a result of an attack on Viasat, Enercon lost remote access to 5,800 wind turbines producing 11 gigawatts of power, which it remotely monitored and controlled via satellite. Company representatives stated that the systems were not endangered, as the turbines work automatically and shut down in case of any issues. However, Enercon was forced to replace their IT equipment as a result of this cybersecurity incident.

Conti attacks KP Snacks

In the beginning of February it was reported that the Conti group had attacked a large British snack producer – KP Snacks. As has lately been typical for ransomware, the victim's data was not only encrypted but stolen as well. Some of the data was released into the public domain to demonstrate that it was really stolen and to attempt to force the victim to pay.

Lapsus$ attacks chip and graphics card producer Nvidia

In the beginning of March Nvidia, a producer of chips and graphics cards, underwent a cyberattack during which it seems up to 1 TB of data was captured. At first the company admitted to the breach, but declared that nothing was encrypted. Then the Lapsus$ group took responsibility for the attack and posted the user credentials of Nvidia employees online. This usually leads to a wave of phishing, spear phishing, brute-force attacks and other attempts by other threat actors to breach the victim company's infrastructure.

REvil attacks Oil India

In April Oil India, an Indian company, was attacked by ransomware – probably REvil. The attack affected IT systems and computers in the head office were shut down. The attack did not affect oil production and drilling systems. The attackers demanded a ransom of $7.5 million. A highly placed official in the Indian police declared that the company was attacked by "Russian malware" coming from an a server in Nigeria.

News about the attack went public on April 14. On April 20 bleepingcomputer posted a story about REvil's "resurrection" – a new and improved version of the malware was on offer on RUTor. The REvil victim list on the group's website was updated with two companies, one of which was Oil India.

LockBit attacks electronics producer Foxconn

At the end of May Foxconn, a large electronics producer, was attacked by ransomware. In 2020 Foxconn had reporter a ransomware attack by DoppelPaymer. At that time the attackers claimed to have stolen up to 100 GB of data, erased 20-30 TB of backup data and encrypted around 1 200 servers.

In May 2022 one of Foxconn's factories in Mexico was attacked and business processes were interrupted. Foxconn has not announced which ransomware was used in this new attack. However, the LockBit group cleared things up – they threatened to release the stolen data to the public if the ransom was not paid.

APTs

Attacks on renewable energy

In January news was posted about a cyberespionage campaign that began as early back as 2019 or even earlier. The victim list included well-known companies such as Schneider Electric and Honeywell, as well as the Chinese telecommunication giant Huawei, semi-conductor producer HiSilicon, and Telekom Romania. However, investigators believe that the attackers are particularly interested in the renewable energy sector.

An interesting detail – the attackers used Zetta Hosting Solutions (AS44476), a service provider used by two APT groups – Fancy Bears and Konni (possibly based in North Korea).

Attack on Viasat systems and resulting interruptions in wind power generation

The first news about the attack on the KA-SAT communication satellite high volume network was posted on February 28. Later it was revealed that the attack occurred on February 24 and targeted Viasat systems, Viasat being one of the largest commercial satellite operators. The company statement revealed that the attack caused a partial outage in their system which affected internet access in Ukraine and other European countries served by the KA-SAT network.

The attack had an unexpected side effect – the downtime in the KA-SAT systems resulted in Enecron, a German wind power company, losing remote access to the controls of 5,800 wind turbines producing 11 GW of power. We mentioned this incident above, in the section on incidents affecting companies which produce or service wind turbines.

Growing threat levels from Turla and Curious Gorge

In May, researchers from the Google Threat Analysis Group (TAG) released a report about growing threats in Eastern Europe, focusing on the Turla group, a group active since 2008 that is believed to be based in Russia, in connection with February 2022 events. Turla targets government data and steals from government agencies, the military industrial complex, and cybersecurity entities.

TAG analysts also noted increased activity by the Curious Gorge group, attributed by TAG to China's PLA SSF (People Liberation Army Strategic Support Force). This group targets government, military, logistics and manufacturing organizations in Russia, Ukraine and Central Asia.

German auto industry under attack

The Check Point team has released a report about a malicious campaign which has been running for about a year now. The threat actors are attacking companies in the German auto industry using popular Malware-as-a-Service variants such as AZORult, BitRat and Racoon Stealer.

ShadowPad backdoor used to attack energy sector in India

The Indian power sector was attacked using the ShadowPad backdoor. The goal seems to be either information gathering or a preparation for additional infections and lateral movement. Initially, the RedEcho group was thought to be the perpetrator, but no forensic evidence was discovered. Until any such evidence is uncovered, the attack is temporarily named TAG-38.

ShadowPad attacks on ICS systems

Another series of ShadowPad attacks were identified by Kaspersky ICS CERT researchers. Malicious artifacts were discovered in manufacturing and telecommunications organizations in Pakistan and Afghanistan. Moreover, an attack using older but very similar tactics, techniques and procedures (TTPs) was conducted against a logistics and transport facility (a port) in Malaysia. This wave of attacks probably began in March 2021 and was described in a report published in June.

There were building automation systems among the victims of this campaign. These systems can be valuable sources of strictly confidential information. Threat actors could be able to use the captured data to penetrate other, more secure infrastructure.

TTPs – attack tactics, techniques and procedures

FBI warns of infected USB sticks arriving in the mail

In January the FBI released a warning about attacks using USB devices. Infected USB drives are mailed purportedly from the US Department of Health and Human Services or in gift boxes from Amazon and target logistics, insurance and military industrial complex companies. It is thought the infamous FIN7 group is behind this attack. As a rule, this group tries for financial gains.

Sending out infected USB drives is a rather unusual penetration method versus the now standard phishing, spam, perimeter breaches and so forth. Once a USB drive is attached, the attacker gains initial access to the victim machine and then moves laterally.

Malware targeting industrial automation systems

Industroyer 2.0

This malware, identified by Eset researchers in April, attacks via the IEC-104 protocol, aka IEC 60870-5-104. Industroyer 2.0, like the 1.0 variant, targets power systems in Ukraine. However, at the time of publication, April 12, 2022, researchers had not yet found the penetration vector.

Tools used to attack industrial equipment

In April a number of US agencies (CISA, FBI, DOE, and NSA) released a joint advisory describing a toolset designed to attack industrial automation systems that use Schneider Electric MODICON and MODICON Nano PLCs, OMRON Sysmac PLCs (versions NJ and NX), and OPC UA servers. The advisory did not include details about victims or geographical details about where the tools were used.

Awareness of current trends in cybersecurity is ensured by information about current events. Kaspersky ICS CERT releases monthly digests describing the latest events with indicators of compromise and our own analysis, where possible.

Sign up for our ICS Threat Intelligence Reporting service to receive this digest.

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