Kaspersky ICS CERT

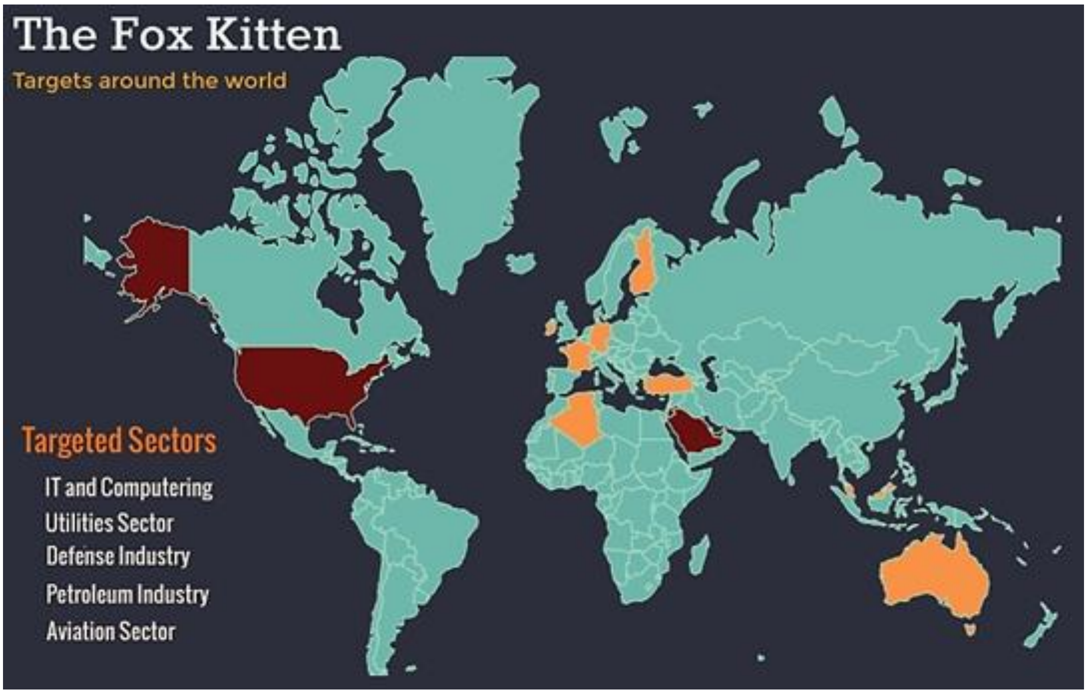
APT attacks on industrial companies in 2020

29.03.2021 Version 1.0

Since 2018, Kaspersky ICS CERT has published annual summaries of advanced persistent threat (APT) activity targeting industrial-related organizations. The summaries are based on Kaspersky threat intelligence research and external reports and provide a representative snapshot. This summary describes the main events of 2020 associated with APT attacks and includes expert insights that we believe could be useful both to cyberthreat researchers and to those who deal with practical tasks related to ensuring the cybersecurity of industrial enterprises on the ground.

APT 33/APT 34

In February 2020, ClearSky described a campaign observed in the last quarter of 2019, designed to compromise the networks of organizations in the IT, telecoms, oil and gas, aviation, government and security sectors around the world. Researchers have attributed it to an Iranian threat actor. The campaign, which was dubbed “Fox Kitten”, was used for reconnaissance, but it could also be used to spread destructive malware such as the ZeroCleare and Dustman malware associated with the APT34 group. An overlap in infrastructure was revealed between Fox Kitten and other threat actors operating in the Middle East – APT33 and APT34. This suggests a cooperation between these groups in infrastructure and possibly beyond that.

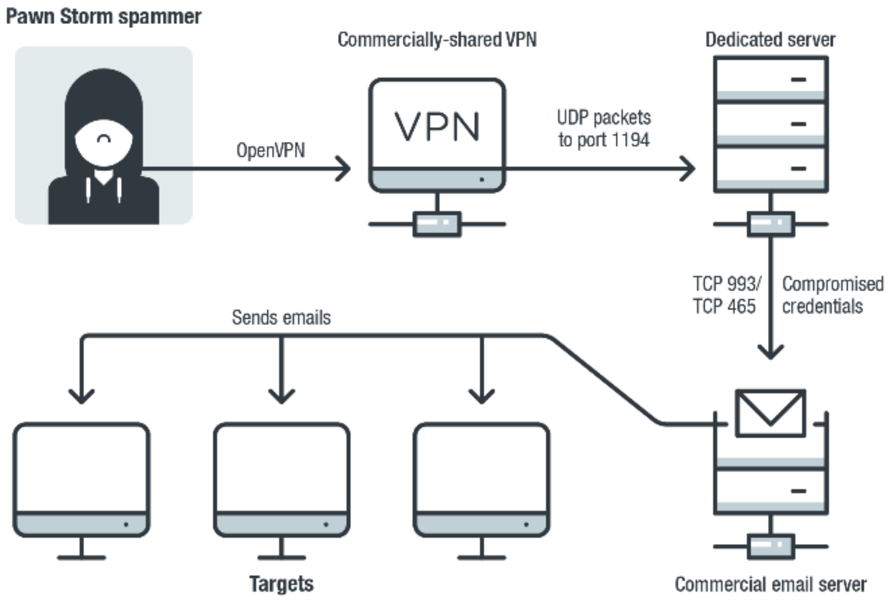


Countries and industries attacked by Fox Kitten (Source: ClearSky)

The initial breach of the targeted organizations in this campaign was performed by exploiting known vulnerabilities in systems with unpatched VPN and RDP services in order to infiltrate and take control of critical corporate information storage systems.

Sofacy

In March TrendMicro described a Sofacy (aka Pawn Storm, Fancy Bear, Sednit, STRONTIUM and APT28) campaign targeting organizations in different parts of the world. Its activities over 2019 and 2020 included the abuse of compromised email addresses to send credential phishing spam. The majority of the compromised systems belonged to defense companies in the Middle East. Other targets included organizations in the transportation, utilities, and government sectors.



Sofacy spam attack flowchart (Source: TrendMicro)

The group also regularly probed many vulnerable email and Microsoft Exchange Autodiscover servers across the world, attempting to brute force credentials, exfiltrate email data, and send out waves of spam.

APT41/BARIUM/Winnti

FireEye observed a campaign by APT41 (aka BARIUM), where the group attempted to exploit vulnerabilities in Citrix NetScaler/ADC, Cisco routers and Zoho ManageEngine Desktop Central. The campaign took place between January 20, 2019 and March 11, 2020 and targeted companies in the financial, construction, defense, industrial-based, government healthcare, hi-tech, higher education, legal, manufacturing, media, transportation, travel and utilities sectors. Victims of the attacks have been seen in Australia, Canada, Denmark, Finland, France, India, Italy, Japan, Malaysia, Mexico, Philippines, Poland, Qatar, Saudi Arabia, Singapore, Sweden, Switzerland, UAE, UK and US. In a postexploitation phase the group was seen to use a trial version of the Cobalt Strike BEACON loader, a VMProtected Meterpreter downloader and a Cobalt Strike BEACON shellcode.

Researchers from PaltoAlto have observed a campaign in which the APT41 threat actor exploited the CVE-2019-19781 vulnerability to distribute the Speculoos backdoor. The vulnerability affects the Citrix Application Delivery Controller, Citrix Gateway and Citrix SD-WAN WANOP appliances, allowing an attacker to remotely execute arbitrary commands. The attacks targeted organizations in the healthcare, higher education, manufacturing, government, and technology sectors, in multiple regions around the world, including North America, South America and Europe.

As we have mentioned in our previous APT reviews, some researchers believe that APT41 and Winnti are the same group. The use of Winnti samples was observed in 2020 in attacks on a German chemical company and a South Korean video and gaming company. The analysis revealed a previously unreported C2 technique never attributed to any of the Winnti group's toolkits. The technique relies on a DNS Tunneling communication channel through a custom implementation of iodine source code. Iodine is open-source software that enables IPv4 data to be tunneled through a DNS server.

According to an analysis from BlackBerry released at Black Hat 2020, Linux malware used to conduct espionage against various companies in the semiconductor industry in Taiwan is being used as a shared resource by five different Chinese-speaking APT groups that turned out to be splinters of the Winnti group. The toolset consists of six different elements. The first is an installer bash script, compressed inside another shell script, whose job is to work with a remote build server. The build server custom-compiles a malware package for a specific target on the fly, which is then downloaded to the victim's system by the installer. The malware payload includes a rootkit and a backdoor, complete with an installation script for the target. The fifth item, an attacker control panel, is capable of managing both Windows and Linux targets simultaneously. Finally, the last item is the Linux XOR DDoS botnet.

PoetRAT

In April 2020, researchers at Cisco observed a new RAT targeting energy companies and the government sector in Azerbaijan, including SCADA systems, with various tools designed to steal credentials and gather valuable data, record footage from webcams, and steal browser credentials. The droppers are Microsoft Word documentsю

The Python-based RAT has been named “PoetRAT” because there are various references in the macros embedded in malicious Word documents to sonnets by William Shakespeare.

In September and October new spear-phishing campaigns with updated malware were observed, in which LUA scripts were used instead of Python.

Attacks on Israel's water systems

In April, news came out on a major cyberattack targeting Israel’s critical infrastructure, which has been attributed to Iran. The “synchronized and organized attack” was aimed at the country’s water system. The incident took place in late April of 2020. It is unclear if the attackers managed to take control of any systems: according to an internal report, the incident was thwarted by the authority's cyber division. Israeli Water Authority officials ordered all personnel to immediately change passwords, “with emphasis on operational system and chlorine control in particular.”

In May, shortly after the release of the news about the attack on Israel’s water system, it was reported that Israel was behind a cyberattack on Iran’s Shahid Rajaee port.

Mikroceen

In May, ESET provided a technical analysis of a backdoor that has been used in various targeted attack campaigns against public and private organizations since late 2017. The targets include companies in the telecoms, government entities and gas industries in Central Asia. ESET believes that the malware may be connected with past high-profile attacks, including an attack on Russian military personnel analyzed by Kaspersky, an attack on the Belarusian government reported by Palo Alto and an attack on the Mongolian public sector described by Check Point. The attackers’ arsenal includes Mikroceen RAT (client-side backdoor), lateral movement via Mimikatz, lateral movement via WMI and Gh0st RAT. Open directories in the C2 servers observed in earlier and current research, as well as leaked tools, suggest poor operational security of the attackers.

Chafer/APT39/Remix Kitten

According to Bitdefender research, Chafer (aka APT39 and Remix Kitten) has been conducting a cyber-espionage campaign since 2018, targeting air transportation and government organizations in Kuwait and Saudi Arabia, likely for data exploration and exfiltration purposes. The campaign makes use of living-off-the-land tools, as well as hacking tools, scanning tools and a custom backdoor written in Python. Attacker activity occurred on weekends and relied on social engineering to compromise victims.

TA410

In June 2020, Proofpoint issued a report on a new malware family named "FlowCloud", which was used in campaigns targeting US utility providers between July and November 2019.

The malware has RAT functionality that provides complete control over a compromised system, including access to installed applications, keyboard, mouse, screen, files, services and processes; and the ability to exfiltrate information via C2. The malware was first distributed in PE attachments but in November the attackers switched to Microsoft Office documents with macros. The content of the phishing emails with malware in the November 2019 campaigns impersonated the American Society of Civil Engineers (ASCE) and masqueraded as the legitimate domain of ASCE.

FlowCloud was deployed at the same time as the "LookBack" malware, which was also used to target US utility companies. Based on the use of common attachment macros, malware installation techniques and overlapping delivery infrastructure, Proofpoint attributes both LookBack and FlowCloud to the TA410 threat actor. Researchers have also found some similarities between TA410 and TA429 (APT10) actors in terms of the attachment macros and infrastructure used, but a possibility remains that these overlaps represent intentional false flag efforts.

Lazarus

Kaspersky continues to track the Lazarus group extensively and the group continues to be very active. It was noticed in early 2020 that Lazarus had shifted their target to individuals in the academic field and the automotive industry using strategies similar to those initially used to target cryptocurrency related businesses. In those campaigns, Lazarus used a downloader that sends information about the compromised host and selectively fetches the next-stage payload. The campaign was dubbed "DeathNote" after the downloader used in it and it made use of lure documents containing aerospace and defense-related job descriptions.

The Lazarus group has adopted new methods to deliver their tools. First of all, they developed their weaponized document by adopting remote template injection techniques. Previously, they had delivered macro-embedded documents to the victim, but applied an additional stage to hinder detection. They have also used an open-source PDF reader named Sumatra PDF to make Trojanized applications. They send a Trojanized PDF reader to the victim with a crafted PDF file. If the victim opens the file, the Trojanized PDF viewer implants malicious files and shows decoy documents to deceive the victim. The actor delivers the final payload very carefully, and executes it in memory. Fortunately, the final payload has been caught. It turned out to be a variant of Manuscrypt, a tool actively used by Lazarus. It's the same malware variant on which CISA (the US Cybersecurity and Infrastructure Security Agency) published a report, referring to it as COPPERHEDGE.

On July 22, Kaspersky found a suspicious archive file uploaded to VirusTotal from an Italian source. The file contained malicious scripts, access logs, malicious document files and several screenshots related to suspicious file detections from security solutions. Kaspersky researchers have identified that these malicious document files are related to the Lazarus group's "DeathNote" campaign and are confident that these documents are related to a reported attack on an Israeli defense company. Webshell scripts, C2 server scripts and malicious documents were uncovered, several victims that had connected to the compromised C2 server, as well as the method used to access the C2 server, were identified.

In summer 2020, Kaspersky found out that Lazarus group had launched attacks on the defense industry on a global scale using the ThreatNeedle cluster. The group made use of COVID-19 themes in its spear-phishing emails that also contained personal information gathered using publicly available sources. After gaining an initial foothold, the attackers gathered credentials and moved laterally, seeking crucial assets in the victim's environment. The attackers overcame network segmentation by gaining access to an internal router machine and configuring it as a proxy server, which allowed them to exfiltrate stolen data from the intranet network to their remote server. The group configured multiple stage C2 servers, reusing several scripts seen in previous Lazarus attacks.

ESET researchers have analyzed targeted attacks against aerospace and military companies in Europe and the Middle East that took place from September to December 2019. The attacks, dubbed "Operation In(ter)ception", relied on social engineering over LinkedIn and custom, multi-stage malware. To operate under the radar, the attackers frequently recompiled their malware, abused native Windows utilities and impersonated legitimate software and companies. While they did not find strong evidence connecting the attacks to a known threat actor, researchers discovered several hints suggesting a possible link to the Lazarus group, including similarities in targeting, the development environment, and anti-analysis techniques used.

Gorgon APT

In August Seqrite has described a wave of attacks against micro, small and medium-sized businesses in India, which has been attributed to the Gorgon group (aka Subaat), a threat actor thought to be aligned with Pakistan-based interests. It should be noted that small and medium-sized businesses, which employ about 40% of India's workforce, are considered the backbone of the country's economy. They account for almost 45% of India's manufacturing industry.

COVID-based themes were used to lure victims into opening malicious documents: one example included an attached file named "face mask order.zip", which exploited the CVE-2017-11882 vulnerability to execute arbitrary code on the computer. The final payload used was Agent Tesla.

CactusPete

In August 2020, Kaspersky issued a report summarizing the activity of CactusPete, a Chinese-speaking cyber-espionage APT group (aka LoneRanger, Karma Panda, and Tonto Team) in recent years.

The group was reported to have targeted South Korean, Japanese, US, and Taiwanese organizations during the 2012-14 timeframe at the least. CactusPete's activity broadened substantially in 2018. 2019 campaigns show that the group has shifted its focus towards organizations in other Asian, as well as East European, countries. Their activity has been focused on military, diplomatic, defense, manufacturing, military and government targets. In addition, targets in the mining, energy, financial institutions, and telecoms sectors have been observed starting from 2018.

The CactusPete APT has quite likely relied on much the same codebase and implant variants for the past six years. The group spear-phishes its targets, deploys Word and Equation Editor exploits and an appropriated/repackaged DarkHotel VBScript zero-day, delivers modified and compiled unique Mimikatz variants, credential stealers, a keylogger, some escalation-of-privilege exploits, various older utilities, an updated set of backdoors and backdoor modules. The threat actor's signature backdoor was called Bisonal or Korlia (Dustbiscuit variants). It was updated and has been used in attacks since 2019. In its 2019 campaign, the CactusPete threat actor also used a new method to drop an updated version of the DoubleT backdoor onto computers. The attackers implanted a new dropper module in the Microsoft Word Startup directory, most likely through a malicious document. This malicious dropper was responsible for dropping and executing a new version of the DoubleT backdoor, which uses a new method of encrypting the C2 server's address.

Kaspersky has found a connection between the ShadowPad malware and the CactusPete group. CactusPete started deploying the ShadowPad malware to a few victims at the beginning of 2019 through its HighProof backdoor. Since late 2019, ShadowPad has been commonly used in CactusPete attacks.

ShadowPad was first discovered by Kaspersky in 2017. After a thorough investigation, a legitimate software module that had been compromised and backdoored by an advanced threat actor in a sophisticated software supply-chain attack was found. Since then, the ShadowPad malware has been observed in a number of major cyberattacks, with different subsets of plugins used in different attack cases: the 2017 CCleaner incident and the 2018 ShadowHammer attacks are major examples of such attacks.

Palmerworm/BlackTech

In September, Symantec observed the Palmerworm group (aka BlackTech) use previously unseen malware in espionage attacks on organizations in Japan, Taiwan, the US, and China. The attacks, which started in 2019 and continued in 2020, were focused on organizations in the media, construction, engineering, electronics and finance sectors. The threat actor used a combination of custom malware, dual use tools, and living-off-the-land tactics in this campaign. Palmerworm also used stolen code-signing certificates to sign its payloads. Symantec has not found out what infection vector Palmerworm used to gain initial access to victim networks in this campaign; however, in the past the group has been documented as using spear-phishing emails to gain access to victim networks.

IAmTheKing

On October 1, 2020, CISA published a report on a malware family called SlothfulMedia, which they attribute to a sophisticated threat actor. Kaspersky has been tracking this set of activity through its private reporting service since 2018 and shared some information on it in a report.

The cluster of activities was called IAmTheKing, based on strings discovered in a malware sample from an unknown family. Over time, different malware families used by that threat actor were identified. They were called KingOfHearts, QueenOfHearts and QueenOfClubs, the latter of which was called SlothfulMedia by CISA. Apart from these malware families, the group used a PowerShell backdoor, a screenshot capturing utility, and ProcDump and PsExec Windows utilities, as well as publicly available LaZagne and Mimikatz utilities for lateral movement.

Until 2020 IAmTheKing had focused exclusively on collecting intelligence from high-profile Russian entities. Victims include government bodies and defense contractors, public agencies for development, universities and companies in the energy sector. In 2020 rare incidents involving IAmTheKing were discovered in central Asian and Eastern European countries. CISA also reports activity in Ukraine and Malaysia.

MontysThree

In October 2020, Kaspersky issued a report on a new malware toolset. In summer 2020, Kaspersky uncovered a previously unknown multi-module C++ toolset used in highly targeted industrial espionage attacks dating back to 2018. Since no similarities with known malicious activity in terms of code, infrastructure or TTPs have been observed, the toolset and the actor behind it is considered to be new. The malware authors named the toolset “MT3”, and based on this abbreviation the toolset was named “MontysThree”. MontysThree is configured to search for specific document types, including those stored on removable media. It contains natural language artifacts in Russian and is configured to search for directories that exist only in Windows versions with Cyrillic localizations. The malware uses major legitimate cloud services, such as Google, Microsoft and Dropbox, for C2 communications. It also uses custom steganography and several encryption schemes: besides custom XOR-based encryption, the modules rely on 3DES and RSA algorithms for configuration decryption and communications. The initial loader module is distributed in RAR self-extracting archives (SFX) that have names referring to employees’ phones list, technical documentation and medical test results and masquerade as pdf or doc files.

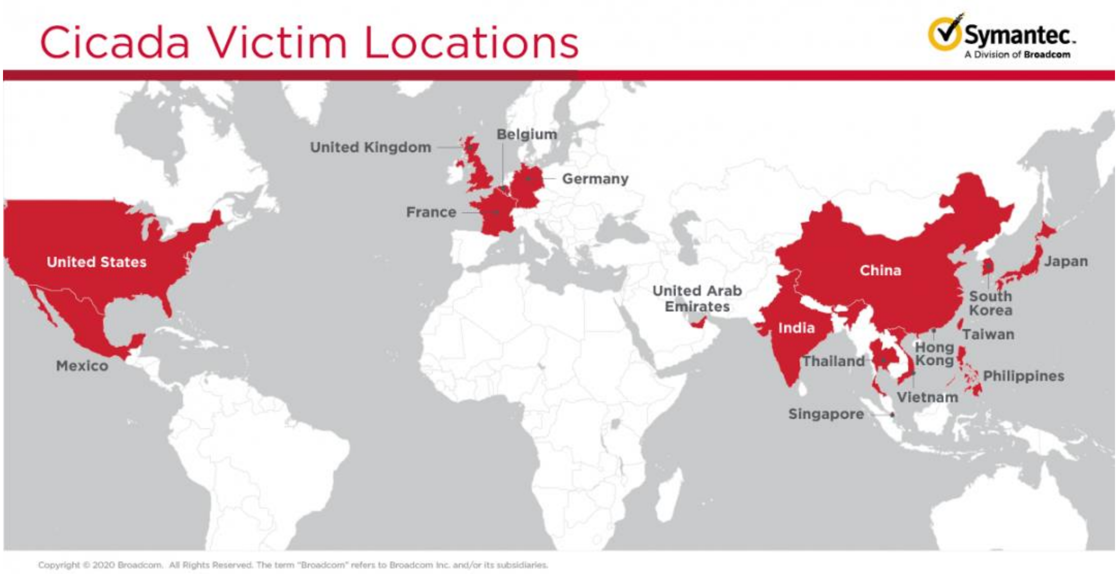
MuddyWater

According to a Telsy report published in October, in May MuddyWater used social engineering to target individuals working in the aerospace and avionics sector. The victims, all operating in Italy, were targeted via a LinkedIn account masquerading as the HR recruiter of a satellite imagery company. They were invited to download an attachment containing information about a fake vacancy. The attachment was an archive containing a vCard File (VCF) that exploits last year's vulnerability (ZDI-19-013, ZDI-CAN-6920), which allows a local file to be executed when the user clicks on a link on a website.

The attackers used a complex, multi-stage infection chain based on PowerShell scripts and executable files that resulted in a powerful and previously unseen RAT being implanted. According to Telsy, the attack originated from a threat actor specifically interested in obtaining information about space and aerospace research activities.

Cicada/APT10

In November Symantec published a report about a year-long campaign targeting Japanese companies, including subsidiaries in 17 countries around the globe, which has been attributed to Cicada (aka APT10, Stone Panda and Cloud Hopper). The campaign targets companies in multiple sectors, including the automotive, pharmaceutical, and engineering sectors, as well as managed service providers (MSPs).



Locations of some of the companies targeted in this campaign (Source: Symantec)

The threat actor used a wide variety of living-off-the-land, dual-use, and publicly available tools and techniques in these attacks. It used custom malware named Backdoor.Hartip, made use of DLL side-loading and exploited the ZeroLogon vulnerability.

SolarWinds

On December 13th, 2020, FireEye, Microsoft, and SolarWinds announced the discovery of a large, sophisticated supply chain attack leveraging Orion IT, an infrastructure monitoring and management platform by SolarWinds. The SolarWinds supply chain attack was designed very professionally, with a clear focus on staying undetected for as long as possible. The Sunburst malware used in the attack includes a complex victim reporting, validation and upgrading scheme, which in some ways reminds of other supply chain attacks such as Shadowhammer or Shadowpad. It has been officially confirmed that about 18,000 users may have installed backdoored versions of SolarWinds, though there is limited information on the number of organizations where the attack has evolved and second-stage tools may have been deployed.

Kaspersky ICS CERT has analyzed publicly available data with DNS names and its own telemetry to see how many industrial organizations used backdoored SolarWinds versions but obtained no evidence that any of the industrial organizations in the telemetry had an escalation from the attackers. There are some speculations on the list of organizations that are of interest to the actor based on an analysis of the historical C2 DNS response, which includes several industrial organizations. Some companies from the list of possible second-stage victims have already confirmed being compromised by the attack.

Conclusions

Here are the main trends that we have seen in APT reports in 2020:

1. Some actors expanded their targeting by including industrial organizations in their lists, as well as expanding their geographical targeting.
2. Some actors exploited the COVID-19 pandemic as a theme to lure potential victims.
3. Geo-politics remains an important motive for some APT threat actors, as shown in the activities of MuddyWater, the compromise of Israeli water systems, PoetRAT, and others.
4. A highly sophisticated supply chain attack compromising SolarWinds software was discovered last year. It stands apart from all other attacks in terms of scale and sophistication level.

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