Kaspersky ICS CERT

kaspersky

Threat landscape for industrial automation systems

H2 2019

24.04.2020

Version 1.0

Contents

2019 Report at a glance

- In 2019, Kaspersky ICS CERT identified 103 vulnerabilities in industrial, IIoT/IoT, and other types of solutions.
  - 33 of them are still not fixed by the vendors, though although all the information needed to identify the problem has been provided to them.
  - If exploited, 30.1% of the vulnerabilities identified could lead to remote code execution, 14.6% to a DoS condition. The exploitation of 13.6% of the vulnerabilities could result in privilege escalation or session hijacking.
  - The absolute majority of the flaws identified have CVSS v.3 base scores of 7.0 or more, which places them in the most severe group.
  - All the vulnerabilities arise from errors made in the process of developing software, including solution architecture. The most popular error type was CWE-787, "Out-of-bounds Write", according to the Common Weakness Enumeration specification.
- In H2 2019, malicious objects were blocked on 39.2% of all ICS computers globally – this is lower than in H1 2019 by 2 percentage points. The percentage for the entire year 2019 was 46.4%.
  - The percentage varies for different industrial environments, such as Building Automation (38%), Car Manufacturing (37.6%), Power & Energy (36.6%), Oil & Gas (36.3%) and Engineering and ICS Integration (32.7%).
  - The five most attacked countries in the ranking based on the percentage of ICS computers on which malicious activity was prevented have remained the same for a year and a half now: Vietnam (65.5%), Algeria (64.6%), Tunisia (58.8%), Morocco (56.6%) and Egypt (55.3%).
  - The five most secure countries and territories in H2 2019 were Ireland (7.3%), Sweden (10.3%), Denmark (11.6%), the Netherlands (12%) and Hong Kong (13%).
  - The most noticeable increases in the percentages of ICS computers on which malicious activity was prevented were observed in Singapore (an increase of 9.2 p.p.), Belarus (7.6 p.p.) and South Africa (6.2 p.p). It is worth noting that the percentages for Singapore had been decreasing during the previous 3 reporting periods
  - The internet is still the main source of threats in all regions of the world. However, the percentage of ICS computers on which internet threats were blocked is much lower in Northern (6.8%) and Western Europe (10%) and in North America (12.6%) than in other regions, such as Eastern Europe (17.2%), the Middle East (21.7%), Latin America (24.2%), Central Asia (30.8%), Africa (34.6%), and South-East Asia (35.8%).
  - In 2019, we saw the same seasonal dynamics that we have observed in recent years: the numbers are higher in spring and autumn. Since the absolute majority of malicious transactions are highly automated, we believe these dynamics reflect seasonal changes in employee presence and thus demonstrate the effect of the human factor on the cybersecurity of industrial organizations.

- Although many different malware types, if not blocked on ICS computers, could pose significant threats to operation, ransomware would be the most devastating of these threats. Overall, in H2 2019 ransomware was blocked on 0.61% of ICS computers. According to the refined data, in H1 2019 that figure was 0.76%. The percentage for the entire year 2019 was 1.0%.
  - The highest percentage of ICS computers on which ransomware was blocked in 2019 was in South-East Asia (2.09%), the lowest – in Northern Europe (0.19%).
  - The most attacked country in 2019 was Bangladesh (3.43%), followed by Algeria, Vietnam, Indonesia, Egypt, China, Chile, Belarus, India, Kazakhstan, Ukraine, Malaysia, Tunisia, Italy, and Thailand, which were the top countries attacked by ransomware in 2019.
  - The infamous WannaCry ransomware is still alive. Among all users of Kaspersky products who were attacked by ransomware Trojans in 2019, over 23% were attacked by WannaCry. This percentage is even greater for ICS computers – over 35%.
  - Some ransomware attacks could be even more dangerous than others. Thus, the GandCrab malware was operated via a malware-as-a-service platform until the summer of 2019, when the malicious service was discontinued. This made the malware even more dangerous, since the data could no longer be decrypted – by malicious actors or by any other means (the latest GandCrab version uses strong encryption algorithms). In late 2019, we still detected – and prevented – attacks by the GandCrab malware on ICS machines.

Vulnerabilities identified in 2019

Vulnerabilities in various ICS components

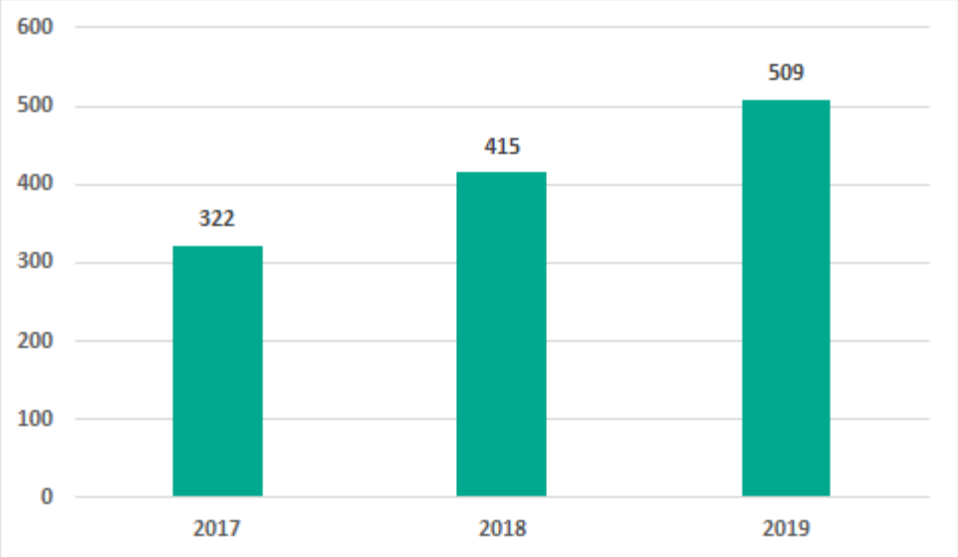
The analysis of vulnerabilities was performed based on vendor advisories, publicly available information from open vulnerability databases (US ICS-CERT, CVE, Siemens Product CERT), as well as the results of Kaspersky ICS CERT's own research.

Vulnerability information published on the US ICS-CERT website in 2019 was used as the source of statistical data for this report.

Number of vulnerabilities identified

In 2019, the number of vulnerabilities identified in different ICS components and published on the US ICS-CERT website was 509. This number has increased over the 2017 and 2018 figures. In our opinion, this increase relates to the increased attention of security researchers to the security of industrial automation solutions and does not mean that there has been a decrease in the quality of product development.

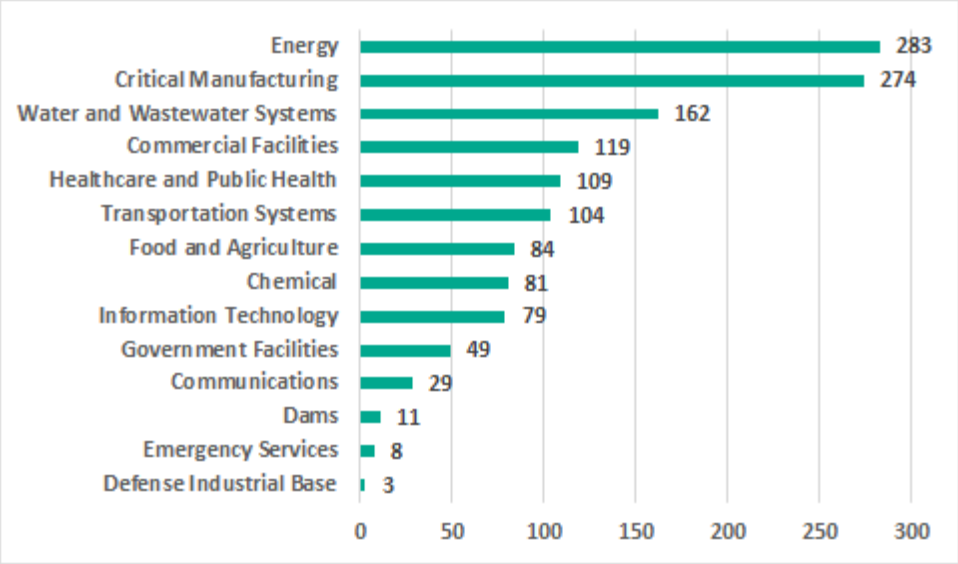
Number of vulnerabilities in different ICS components, as published on the US ICS-CERT website



Analysis by industry

The largest number of vulnerabilities affect industrial control systems in the energy sector (283), systems used to control industrial processes at various enterprises categorized as critical infrastructure facilities in the US (274); and water supply and sewage systems (162).

Number of vulnerable products used in different industries (according to US ICS-CERT classification). Vulnerabilities published in 2019



Severity levels of vulnerabilities identified

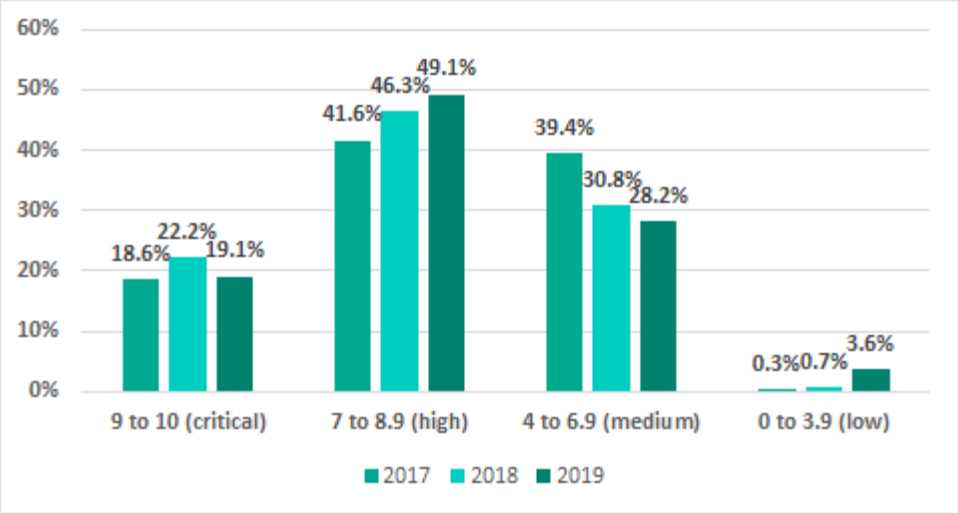
More than half of the vulnerabilities identified in ICS systems (358, compared with 284 in 2018) were assigned CVSS v.3.0 base scores of 7 or higher, corresponding to a high or critical level of risk. Two vulnerabilities were not assigned risk levels, since they are attributed to numerous CVEs and did not receive a unique CWE ID.

Table 1 — Distribution of published vulnerabilities by risk level

Severity score	from 9- to 10 (critical)	from 7 to 8.9 (high)	from 4 to 6.9 (medium)	from 0 to 3.9 (low)
Number of vulnerabilities	97	249	143	18

Compared with the previous year's data, the proportion of vulnerabilities that have a high or critical severity score has grown.

Percentage of vulnerabilities by risk level (based on CVSS v.3 base scores), 2019 vs 2018 and 2017



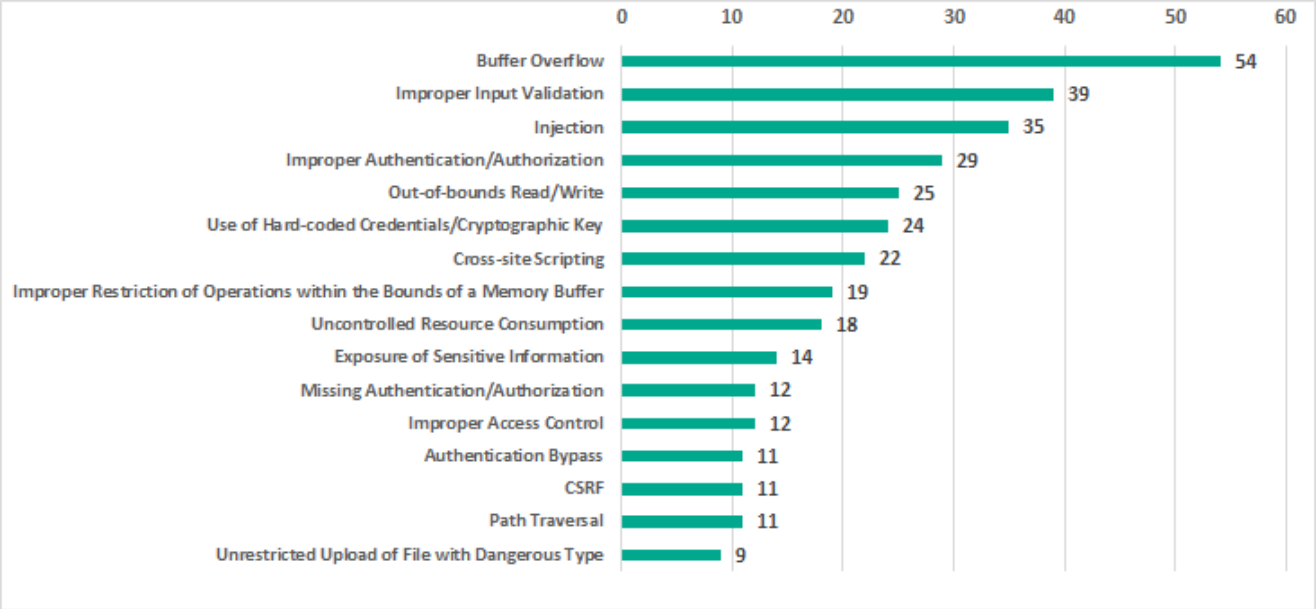
The highest possible base score of 10 was calculated for vulnerabilities identified in the following products:

- Alaris Gateway Workstation
- Proton/Enterprise Building Management System
- Spectrum Power 4.7
- CODESYS V3 web server
- Relion 670 Series
- FlexAir
- RSLinx Classic
- WibuKey Digital Rights Management (DRM)
- PR100088 Modbus gateway

It should be noted that the CVSS base score does not account for the aspects of security that are specific to industrial automation systems or for the distinctive characteristics of each organization's industrial process. This is why, when assessing the severity of a vulnerability, we recommend keeping in mind, in addition to the CVSS score, the possible consequences of its exploitation, such as the non-availability or limited availability of ICS functionality affecting the continuity of the industrial process.

Types of vulnerabilities identified

The most common types of vulnerabilities in 2019, just like in 2018, include buffer overflow (Stack-based Buffer Overflow, Heap-based Buffer Overflow, Classic Buffer Overflow), improper input validation and injection (SQL Injection, Code Injection, Command Injection).

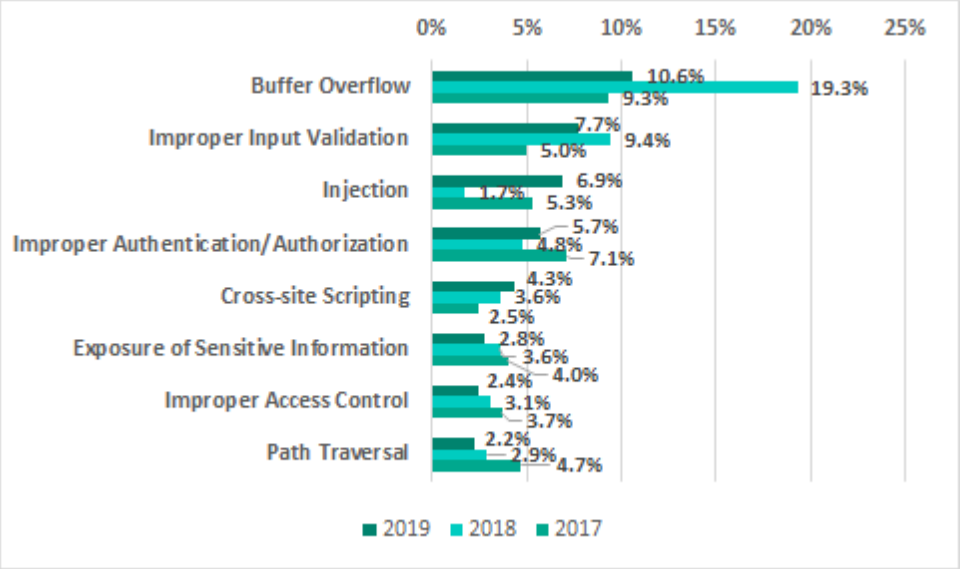


Most common vulnerability types. Vulnerabilities published in 2019

17.3% of published vulnerabilities affect authentication (Improper Authentication, Authentication Bypass, Missing Authentication for Critical Function) and access control (Access Control, Incorrect Default Permissions, Improper Privilege Management, Credentials Management).

15.5% of published vulnerabilities are web vulnerabilities (Injection, Path traversal, Cross-site request forgery (CSRF), Cross-site scripting). Compared with 2018 this number has increased by 5.5 p.p.

Percentage of different vulnerability types to all vulnerabilities. 2019 vs 2018 and 2017



Exploitation of vulnerabilities in various ICS components by attackers can lead to arbitrary code execution, unauthorized control of industrial equipment and denial-of-service conditions (DoS) affecting that equipment.

It should also be noted that:

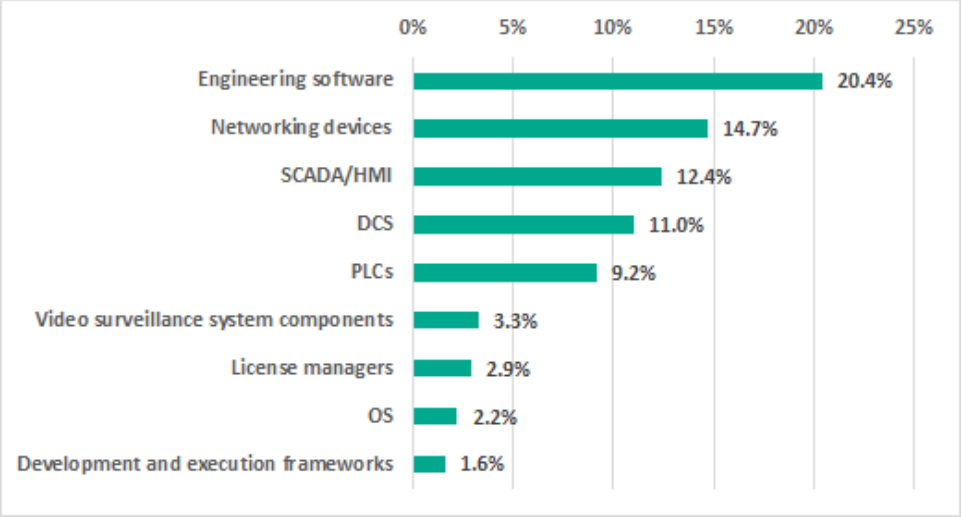
- Most of these vulnerabilities (420) can be exploited remotely without authentication,
- The majority of the vulnerabilities (480) can be exploited without the attackers having any specialized knowledge or high skill levels,
- Exploits have been published for 23 vulnerabilities, which increases the risk of malicious actors using them.

Vulnerable ICS components

The largest number of vulnerabilities were identified in:

- engineering software (103; 20%),
- networking devices designed for industrial environments (78;15%),
- SCADA/HMI components (63; 12%),
- DCS (56; 11%),
- PLCs (47, 9%).

Percentage of vulnerabilities identified in various ICS components to all vulnerabilities. Vulnerabilities published in 2019



Security issues in industrial automation systems are often due to vulnerabilities in third-party common software components used by vendors in many ICS solutions. Such components include operating systems (OS), license managers, modules implementing various security mechanisms, as well as frameworks used to develop and execute industrial control system software.

Vulnerabilities in operating systems

The operating system is one of the main components of any industrial automation system. Since vendors could be using the same operating system in various products, a single OS vulnerability will most often affect entire product lines.

For instance, in 2019 the security issues around the RUGGEDCOM ROX II OS meant that all of the Siemens RUGGEDCOM industrial devices based on this OS ended up vulnerable.

Additionally, multiple vulnerabilities discovered in the VxWorks real-time OS affected solutions from Rockwell Automation, Schneider Electric, Xerox and Dräger.

Another example of an OS vulnerability with sweeping security effects was the TCP SACL Panic vulnerability discovered in the Linux kernel. This vulnerability affected multiple Siemens products.

Vulnerabilities in license managers

In 2019 security researchers reported vulnerabilities in several license managers at the same time:

- Yokogawa License Manager Service
- Schneider Electric Floating License Manager
- RC-LicenseManager
- SafeNet Sentinel LDK License Manager
- FlexNet Publisher

License managers are often used in different solutions, therefore vulnerabilities in them can affect several industrial control products simultaneously. For instance, Yokogawa's CENTUM VP distributed control system and their ProSafe-RS safety instrumented system (SIS) were both affected by vulnerabilities discovered in Yokogawa's License Manager Service.

In a similar case, vulnerabilities in the Floating License Manager affected several Schneider Electric products simultaneously, including the EcoStruxure Control Expert engineering software, the EcoStruxure Hybrid Distributed Control System (also known as the Plant Struxure PES), Power SCADA Expert and others. Vulnerabilities in this license manager also affected Vijeo Citect and Citect SCADA from AVEVA, a Schneider Electric subsidiary. It is worth noting that the vulnerabilities in the Floating License Manager are in turn connected with multiple vulnerabilities in third party software -- Flexera FlexNet Publisher.

In addition, products from several industrial vendors at once, including Siemens, Phoenix Contact, Sprecher Automation and COPA-DATA, were found to be affected by vulnerabilities in the WibuKey Digital Rights Management (DRM) solution.

Vulnerabilities in program development and execution frameworks

It is worth taking a separate look at the security of frameworks used by vendors for the development and execution of ICS software. Vulnerabilities were discovered in 2019 at the same time in several components of CoDeSys, an industrial automation software solution, including the web server, the communication server and the OPC UA server.

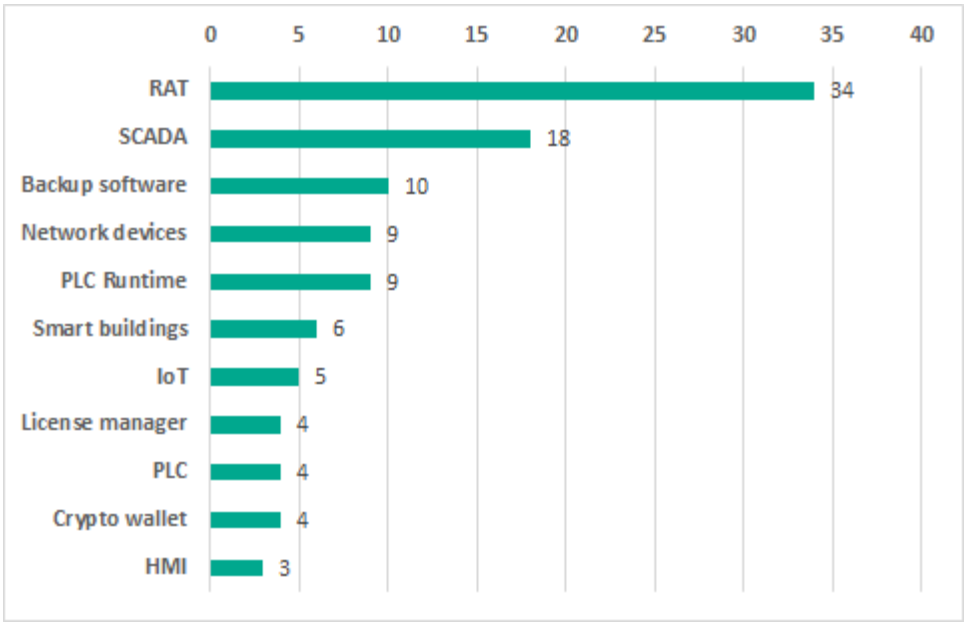
Vulnerabilities identified by Kaspersky ICS CERT

In 2019, Kaspersky ICS CERT experts continued their research on security issues affecting third-party hardware-based and software solutions that are widely used in industrial automation systems, internet of things (IoT) and industrial internet of things (IIoT) solutions, etc. A special emphasis was made on cross-platform solutions and open-source products. Such solutions and their components are widely used as standalone products or as part of commercial solutions.

Number of vulnerabilities identified

In 2019, Kaspersky ICS CERT identified 103 vulnerabilities in industrial, IIoT/IoT, and other types of solutions.

Distribution of vulnerabilities identified by Kaspersky ICS CERT in 2019 by types of components analyzed



Every time we identified a vulnerability, we promptly notified the respective product's vendor.

Possible consequences of exploitation of the vulnerabilities identified

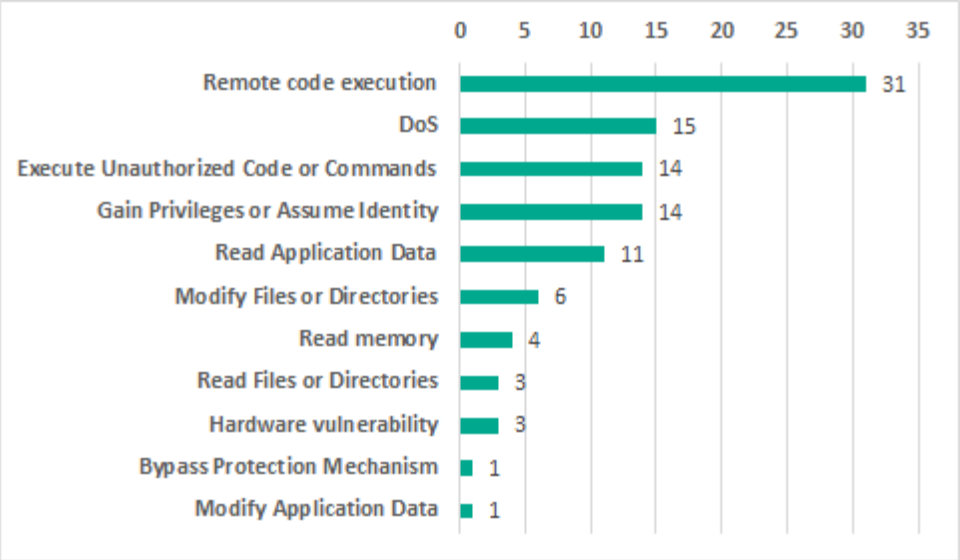
In 2019, we divided vulnerabilities that can be exploited to execute code into two types:

1. Execute Unauthorized Code or Commands – execution of code in the context of the application/execution environment. Examples: XSS, SQLi, XXE, ReadObject.
2. Remote code execution (RCE) – execution of arbitrary machine code. Examples: execution of system commands / operating system commands and machine code.

It should also be noted that RCE often gives rise to various issues, including reading and modifying arbitrary folders and files, denial of service, etc.

In the statistics below, RCE and Execute Unauthorized Code or Commands are two distinct categories.

Distribution of vulnerabilities identified by Kaspersky ICS CERT in 2019 by possible exploitation consequences



If exploited, 30.1% of the vulnerabilities identified could lead to remote code execution, 14.6% to a DoS condition. The exploitation of 13.6% of vulnerabilities could allow privilege escalation or session hijacking. The statistics also include three hardware vulnerabilities. If exploited, such vulnerabilities could provide the attackers with access to sensitive data due to the hardware platform or component base of the solution analyzed being insufficiently secure.

Results we consider the most important

Software / solution	Number of vulnerabilities identified	Possible consequences of exploitation	Status
RAT based on VNC protocol	34	Vulnerabilities of different severity levels, some allowing arbitrary code to be executed both on the server side and on the client side	Vulnerabilities fixed by the vendor. Article published
License managers	4	Vulnerabilities of different severity levels allowing threat actors to develop an attack on the internal infrastructure	Vulnerabilities fixed by the respective vendors

Popular PLC execution environment	9	The vulnerabilities identified are potentially the most destructive for the industrial process, because the exploitation of such vulnerabilities is difficult to detect. The vulnerabilities allow attackers to make stealthy changes to the industrial process. As a consequence, the attack can be highly persistent and can have grave consequences with possible physical impact	Information on the vulnerabilities provided to the vendor
Non-industrial solutions			
Smart city infrastructure devices	6	The vulnerabilities identified allow attackers to: 1. spoof the data transferred; 2. gain access to the information being protected; 3. exploit memory handling faults.	Vulnerabilities fixed by the vendor
Hardware wallet for storing cryptocurrency	4 (in software and hardware)	The vulnerabilities identified allow attackers to gain full control of the wallet and conduct any operations with it.	Vulnerabilities fixed by the vendor

Assessing the severity of the vulnerabilities identified

To assess the severity of the vulnerabilities identified, Kaspersky ICS CERT used a vulnerability rating system based on the metrics defined in CVSS v3.0 (Common Vulnerability Scoring System). The following vulnerability severity levels were identified:

- least severe: CVSS v3.0 base score of 5.0 or less;
- medium severity: CVSS v3.0 base score of 5.1 to 6.9 (inclusive);
- most severe: CVSS v3.0 base score of 7.0 or more.

The absolute majority of those vulnerabilities identified by Kaspersky ICS CERT for which CVEs were published in 2019 have CVSS v.3 base scores of 7.0 or more, which places them in the most severe group. Ten of these vulnerabilities were assigned the highest possible base score of 10. These include vulnerabilities in software components that are common to many products – cross-platform solutions which work over the VNC protocol.

Why vulnerabilities occur

All existing vulnerabilities arise from errors made in the process of developing software, including solution architecture. A classification of such errors exists, called the Common Weakness Enumeration. Based on Kaspersky ICS CERT research conducted in 2019, the most popular error was CWE-787, “Out-of-bounds Write”, which was identified in the process of analyzing RAT solutions. This type of error is a necessary, but not sufficient condition for exploiting a Remote Code Execution vulnerability.

Number of CVE entries published

In 2019, 43 CVE entries were published based on Kaspersky ICS CERT research.

APT attacks on industrial companies in 2019

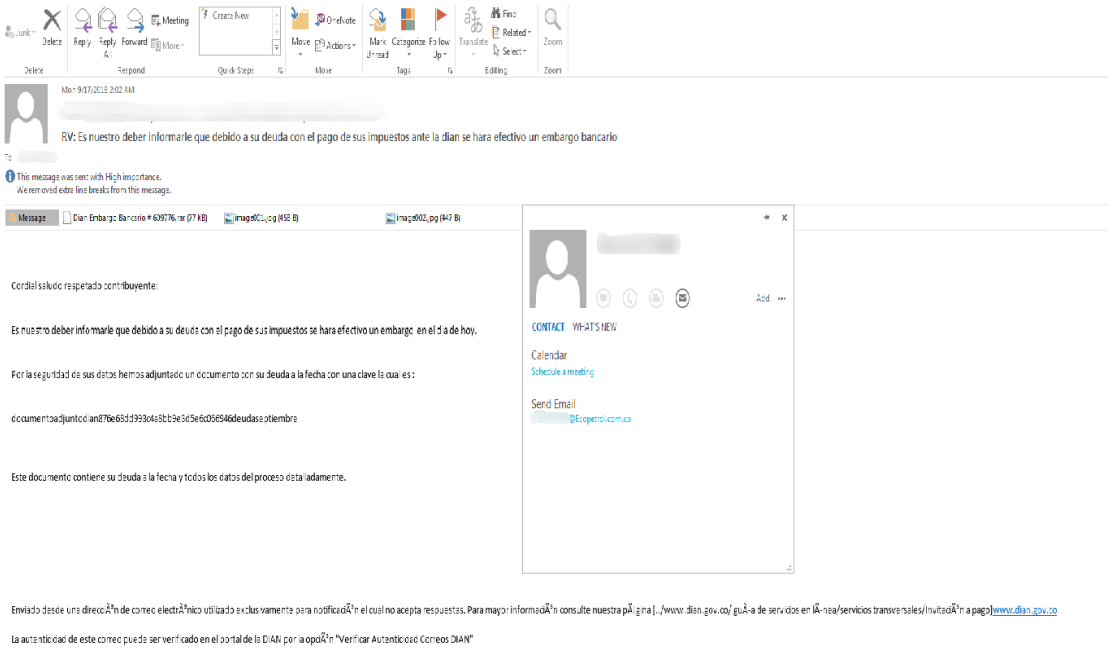
Attacks on Colombian companies

In February 2019, researchers from the 360 Threat Intelligence Center reported continuing targeted attacks on Colombian government institutions and large companies in the financial sector, petroleum industry, manufacturing and other sectors. The attacks were carried out by the APT-C-36 group (aka Blind Eagle). The researchers believe that the group's members come from South America.

The attackers target the Windows platform. They deliver malware via phishing emails that contain password-protected RAR attachments, which can help evade detection at the email gateway. The decryption password is provided in the message body.

The attachment contains a document with the extension DOC. The document contains an MHTML macro designed to install the Imminent backdoor, which has extensive functionality and is used to gain a foothold in the target network. The researchers believe that the attackers are focusing on strategic-level intelligence and could attempt to steal business intelligence and intellectual property.

Phishing email for Ecopetrol (Source: 360 Threat Intelligence Center)

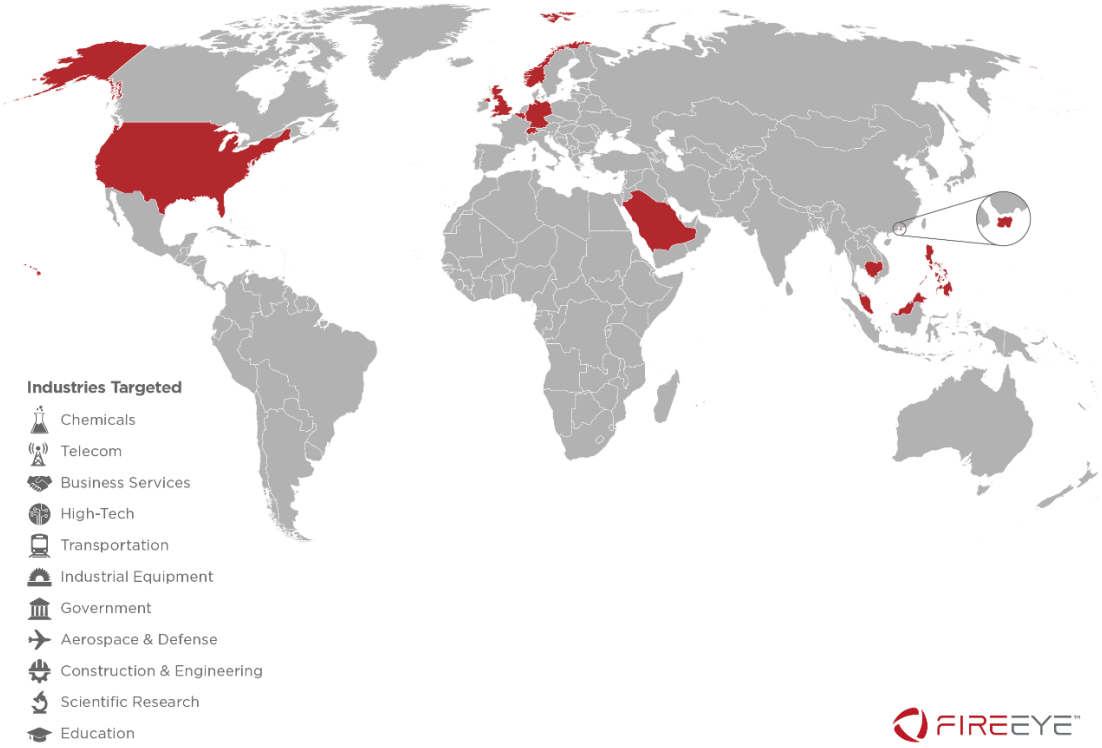


Attacks by APT40 group

In March 2019, FireEye reported attacks carried out by APT40, which researchers believe to be a Chinese state-sponsored group. The group has conducted operations in support of China's naval modernization effort since at least 2013. The Chinese cyber-espionage group is also known as TEMP.Periscope, TEMP.Jumper and Leviathan.

APT40 has targeted the engineering, transportation, and defense industries, particularly where these sectors overlap with maritime technologies. FireEye researchers have also observed attacks on targets that are strategically important for China's One Belt, One Road initiative, including Cambodia, Belgium, Germany, Hong Kong, the Philippines, Malaysia, Norway, Saudi Arabia, Switzerland, the US and the UK.

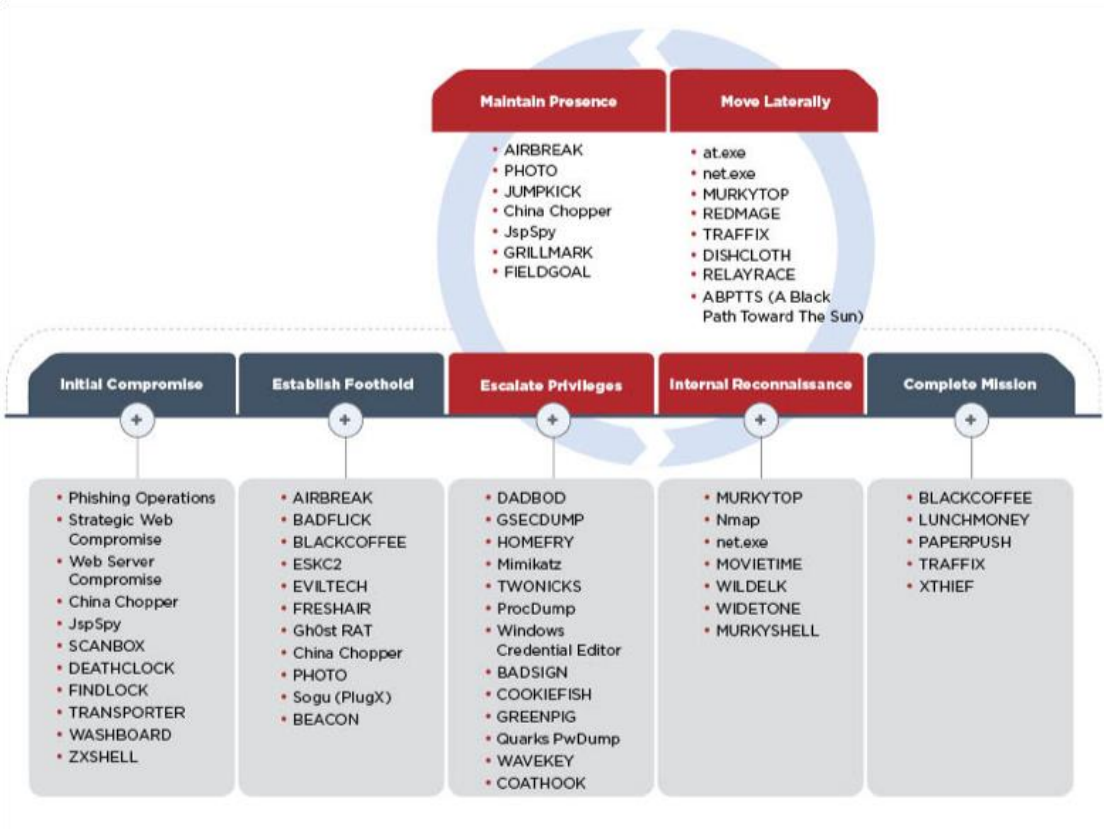
Attacked countries and industries (Source: FireEye)



APT40 leverages various techniques for initial compromise. These include exploiting victims' web servers, running phishing campaigns with vulnerable documents that install both publicly available and custom backdoors. In addition to malicious attachments, phishing emails have been observed to contain links to Google Drive. In some cases, the group has leveraged malicious executables with code signing certificates to avoid detection. It is also worth noting that the group's arsenal includes web shells (malicious scripts that can be used to control infected machines from outside the network) that are used to gain a foothold in the organization. This enables the attackers to make their access more extended in time and to re-infect systems.

APT40 often targets VPN and remote desktop credentials to establish a foothold in a targeted organization. This methodology is very convenient for attackers, since once the credentials are obtained, they need not rely on malware to continue their attack.

APT40 attack lifecycle (Source: FireEye)



Hexane/OilRig/APT34

On August 1, 2019 Dragos published an overview of attacks entitled Global Oil and Gas Threat Perspective, in which a new group dubbed Hexane is mentioned. According to the report, Hexane targets the oil and gas and telecommunications sectors in Africa, the Middle East and Southwest Asia. Dragos says it identified the group in May 2019, associating it with OilRig and CHRYSENE groups, which are believed to be Iranian. Hexane seems to have begun its activity around September 2018 года, with a second activity wave in May 2019.

Although no indicators of compromise have been published, some researchers shared hashes in a Twitter thread in response to the announcement made by Dragos that they had identified a new group. An analysis performed by Kaspersky has also identified some similarities between TTPs used in the new wave of attacks and TTPs used by the OilRig group.

In all of these cases, the artifacts used in attacks were relatively simple. The constant evolution of droppers apparently indicates a trial-and-error period, when the threat actor was searching for the best way to evade detection.

The TTPs that Kaspersky can link to the OilRig activity preceding the emergence of Hexane include:

- the trial-and-error process mentioned above;
- using simple documents with macros as droppers, distributed via phishing emails;
- Using DNS-based exfiltration to C&C servers.

The source code of tools used by Iranian attackers, which was leaked through Lab Dookhtegan and GreenLeakers Telegram channels, provides a clue as to the way in which the

Hexane group may have emerged. Because of the exposure and leaks, the OilRig group may simply have changed its toolset and continued its operations as usual: this would explain the group's quick and flexible response to the leaks. Another possibility is that some of OilRig's TTPs may have been adopted by a new group whose interests are similar to those of OilRig.

Later in August, Secureworks released a report, where they described the toolset of the same group, which they called Lyceum. The report described a phishing document, a first-stage RAT and PowerShell scripts used in attacks.

IBM X-Force analysts believe that the APT34 group (aka OilRig and Crambus) is behind an attack on energy facilities in the Middle East, which made use of data-wiping malware called "ZeroCleare". According to a report published by IBM, OilRig, as well as at least one other group, likely also based in Iran, used compromised VPN accounts to access machines in at least one case.

In December, Bapco, Bahrein's national petroleum company, was attacked by a wiper, which was dubbed Dustman. Saudi Arabia's National Cybersecurity Authority (NCA) released a security alert on the attack. An analysis of the malware showed that Dustman is an upgraded and improved version of the ZeroCleare wiper.

APT33

Attacks by one more Iranian group, APT33 (aka NewsBeef, Charming Kitten, and Elfin) target the petroleum and aviation industries. Recent findings by TrendMicro show that the group has been using about a dozen command-and-control servers for targeted attacks on organizations in the Middle East, the US, and Asia.

The group uses several layers of hosts to obfuscate its real C&C servers.

The malware used by the attackers is relatively simple and has limited capabilities, including downloading and running additional malware.

In 2018, the group attacked tens of thousands of companies, attempting to guess user account passwords by trying several commonly used passwords (password-spraying attacks). According to Microsoft, by the end of 2019, APT33 had narrowed its activity to about 2,000 organizations per month, while increasing the number of accounts attacked in each of these organizations almost tenfold on average. About half of the group's 25 main targets, ranked by the number of accounts attacked, were manufacturers, suppliers or maintainers of ICS equipment. Microsoft says it has seen APT33 target dozens of industrial equipment and software firms since mid-October. What remains unclear is the hackers' motivation and which industrial control systems they have been able to breach. Microsoft experts believe that the group is seeking to gain a foothold to carry out cyberattacks with physically disruptive effects.

Symantec has reported that in the past three years, the group has attacked at least 50 organizations in Saudi Arabia, the US and a range of other countries. Symantec experts believe that some of the organizations in the US have been targeted by the group in order to mount supply chain attacks. In one instance, a large US company was attacked in the same month that a Middle Eastern company it co-owns was compromised.

In the wave of attacks in February 2019, APT33 attempted to exploit a known vulnerability (CVE-2018-20250) in WinRAR. The exploit was used against an organization in Saudi Arabia's chemical sector. Two users in the organization received a file named "JobDetails.rar", which was likely delivered via a spear-phishing email. It has also been noted that APT33 uses both custom and numerous commodity backdoors, such as Remcos, DarkComet NanoCore, etc.

In August 2019 Forbes and WSJ ran stories on attacks of Iranian hackers on Bahrain's government institutions and critical infrastructure, drawing parallels with 2012 Shamoon attacks. They also mentioned that in July 2019 hackers had shut down several systems in Bahrain's Electricity and Water Authority. According to the authorities, that was a rehearsal or demonstration of the vulnerability of heavily secure control systems, which would deliver a significant impact if fully compromised.

Operation Wocao

Fox-IT researchers have reported on the activity of a hacker group, which, they believe, was tasked with obtaining information for espionage purposes. The activity was dubbed "Operation Wocao". It has the same TTPs as a Chinese group known in the industry as APT20. Its victims have been identified in ten countries – in government entities, among managed service providers and across a wide variety of industries, including Energy, Health Care and High-Tech.

In several cases the initial access point into a victim network was a vulnerable webserver, often versions of JBoss. It was observed that such vulnerable servers had often already been compromised with web shells, placed there by other threat actors.

Operation Wacao actually leverages other groups' web shells for reconnaissance and initial lateral movement. Then the group uploads one of its own web shells to the webserver. Access through the uploaded web shell is kept by the group as a precaution in the event of losing the other primary method of persistent access, for example in case the credentials for VPN accounts are reset.

In one case, VPN access to the victim's network was protected with two-factor authentication (2FA) using RSA SecurID software. The group bypassed the 2FA implementation using a technique that Fox-IT believes they had developed independently.

An algorithm patented by RSA is used to generate the password (token code) for two-factor authentication. Each token has an initial generation vector (seed) assigned to it. A new token code is generated once a minute and its value is defined only by the seed and the time at which it is generated.

In the hardware implementation of RSA SecurID, the initial generation vector is reliably protected and can only be obtained by stealing the physical token. However, Fox-IT experts have determined that the RSA SecurID software token only uses the unique key generated for each software installation (and linked to the system's unique parameters) to validate the token's import, while the initial generation vector is a unique value that is not linked to the system in any way. According to Fox-IT, this means that the attackers only need to patch one instruction in the RSA SecurID software to be able to use the software to generate token codes valid for any system from which they were able to steal a software token installed on it. Thus, Fox-IT researchers believe that the attackers could have stolen a software token from the victim and used patched RSA SecurID software on their own machine to generate valid two-factor authentication tokens that could be used to connect to VPN.

APT41/Winnti

In August 2019, FireEye reported on the activity of a Chinese group that has been operating since 2012 and is involved in strategic espionage in areas related to China's five-year economic development plan. Attacked organizations are in healthcare, semiconductor manufacturing, advanced computer software, battery and electric car manufacturing, and other

industries. These organizations are located in 14 countries, including France, India, Italy, Japan, South Korea, the UK, and the US.

A distinguishing feature of the group, which was dubbed APT41, is that it combines attacks on various organizations targeted for cyberespionage activities and financially motivated attacks on the gaming industry, in which the group has manipulated virtual game currencies and attempted to deploy ransomware.

The group gained access to Windows and Linux machines on organizations' networks, stole source code and digital certificates from the machines that were of interest to them, subsequently using the certificates to sign their malware.

APT41 is also known to have embedded their malicious code into legitimate files of gaming companies. The resulting malicious files were signed with those companies' legitimate certificates. The files were subsequently deployed in other organizations, which means that the group implemented supply-chain attacks.

Among the more interesting aspects of the group's TTPs, it is worth mentioning that its attacks were highly targeted. Specifically, the unique system IDs of target machines could be checked prior to deploying some of the next-stage malware used by the group. It should also be mentioned that APT41 makes limited use of rootkits and MBR bootkits, which is generally quite uncharacteristic of Chinese APT groups.

An analysis of the time of day when both types of attacks – cyberespionage attacks on companies in strategic industries and for-profit attacks on gaming companies – were carried out showed that the group's participants engage in the latter type of attacks in their spare time, probably for their personal financial gain. They may be operating under the protection of the authorities.

According to reports published earlier by other companies, APT41 partly overlaps in their activity with Barium and Winnti. FireEye also attributes CCleaner, ShadowPad, and ShadowHammer attacks to APT41.

ESET researchers believe that the APT41 group described by FireEye, which is behind the high-profile supply-chain attacks on the gaming industry, is in fact Winnti. They have determined that the Winnti group continues to upgrade its arsenal and uses a new modular Windows backdoor called PortReuse, which has been used to infect a major Asian mobile hardware and software vendor. ESET has also identified third-stage malware in one Winnti attack on gaming companies – it was a customized version of the XMRig cryptocurrency miner.

Several large German industrial companies, including BASF, Siemens and Henkel, announced in July that they had fallen victim to a state-sponsored hacker group from China. In April, Bayer reported discovering an intrusion. All these attacks may have been carried out by different sub-groups, but what united them was that they all used the Winnti backdoor.

Attacks on the aerospace industry

The European aerospace giant Airbus has suffered a series of attacks mounted presumably by Chinese hackers for the purposes of cyberespionage. In January 2019, the company issued a press release, in which it stated that the company had detected an intrusion into its systems related to the commercial aircraft business, but the incident had made no impact on the company's commercial operations. Some sources in the company also reported a series of attacks during the previous year.

There have also been reports of hacker attacks on British engine maker Rolls-Royce, the French technology consultancy and supplier Expleo, as well as two other French contractors working for Airbus. According to sources, attacks on contractors enabled the attackers to gain access to VPN connecting these companies with Airbus.

In October 2019, Crowdstrike released a report (later removed from the company's website), which uncovered one of China's most ambitious hacker operations. The goal of a coordinated hacking campaign that lasted for many years was to help the Chinese state-owned aerospace manufacturer Comac to build its own airliner C919. The ultimate objective, says Crowdstrike, was to steal intellectual property that would make it possible to manufacture all of the aircraft's components in China. According to Crowdstrike's report, The Ministry of State Security (MSS) assigned this task to its Jiangsu Bureau (MSS JSSD). During the period from 2010 to 2015, the hacker team successfully hacked such companies as Ametek, Honeywell, Safran, Capstone Turbine, GE, and others.

According to Crowdstrike and US Department of Justice data, the group, which the researchers dubbed Turbine Panda, enlisted local hackers and information security researchers, including those who are well-known in underground communities. They were tasked with finding entry points into target networks, where they commonly used malware from such families as Sakula, PlugX, and Winnti, searching for confidential information and stealing it.

APT32/Ocean Lotus

According to FireEye researchers, APT32/OceanLotus, a Vietnamese hacker group that has been active since at least 2014 and is known primarily for its attacks on journalists and government organizations, started aggressively targeting multinational automotive companies in 2019 in what is apparently an attempt to support the domestic auto industry. Since February 2019, the group has sent phishing emails to between five and ten organizations in the automotive sector. The group has also created fake domains for Toyota Motor Corp. and Hyundai Motor Co. in attempts to gain access to the auto makers' networks. It is not known whether these attacks were successful.

According to a Toyota representative, in March the company discovered that it was targeted in Vietnam and Thailand, as well as through its Japanese subsidiary, Toyota Tokyo Sales Holdings Inc. A Toyota official confirmed that APT32 was responsible.

Key events – H2 2019

Ransomware attacks on industrial enterprises

This section presents an overview of threats related to ransomware activity against municipal institutions, industrial enterprises and critical infrastructure facilities.

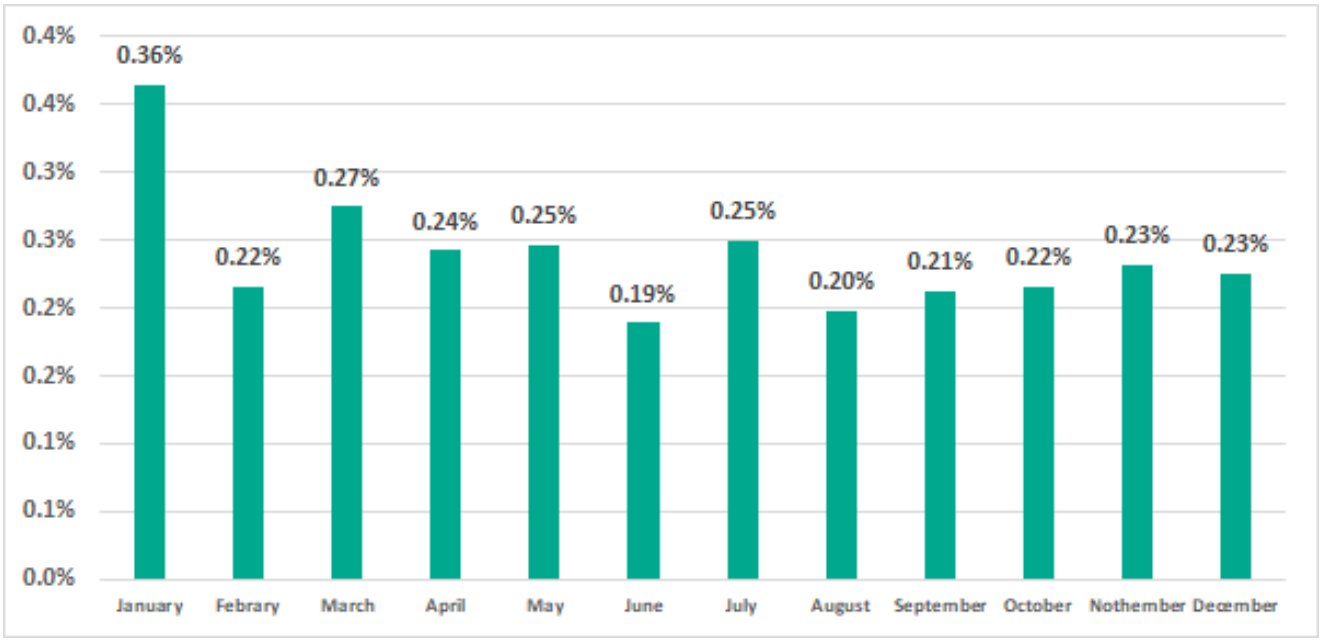
Statistics on ransomware attacks against industrial enterprises

In H2 2019, we did a detailed analysis of data on detected Trojan-Ransom attacks and corrected a number of inconsistencies in the classification of malicious objects. The Trojans and worms that had been mistakenly identified as Trojan-Ransom because they demonstrated similar binary code and/or behavior patterns were removed from the sample and the data for past periods was recalculated to provide more accurate estimates.

In H2 2019 ransomware was blocked on 0.61% of ICS computers. According to the refined data, in H1 2019 that figure was 0.76%

Overall, in 2019 ransomware infection attempts were prevented on 1.0% of ICS computers.

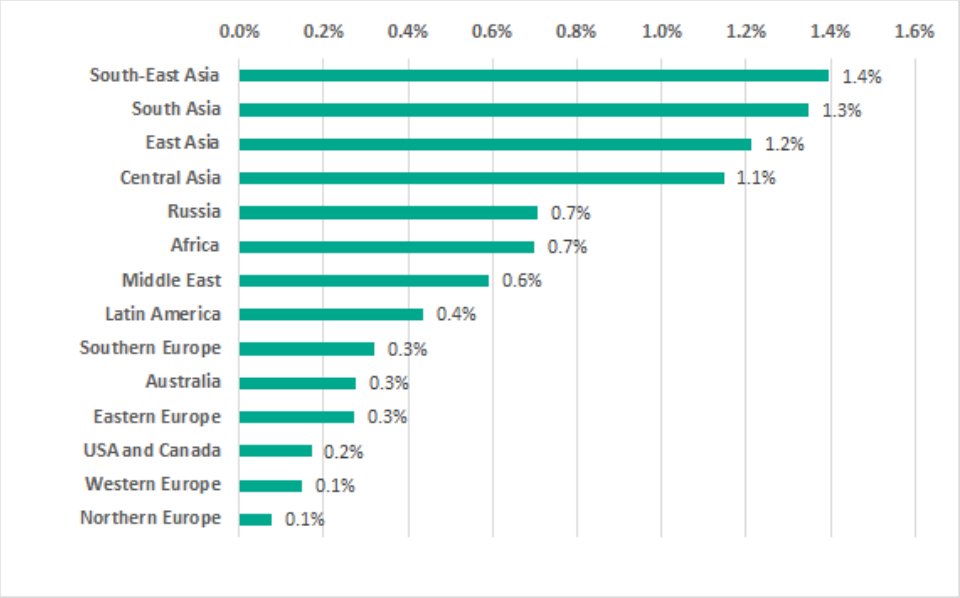
The data for each month of 2019 is shown below.



Percentage of ICS computers on which ransomware was blocked in 2019

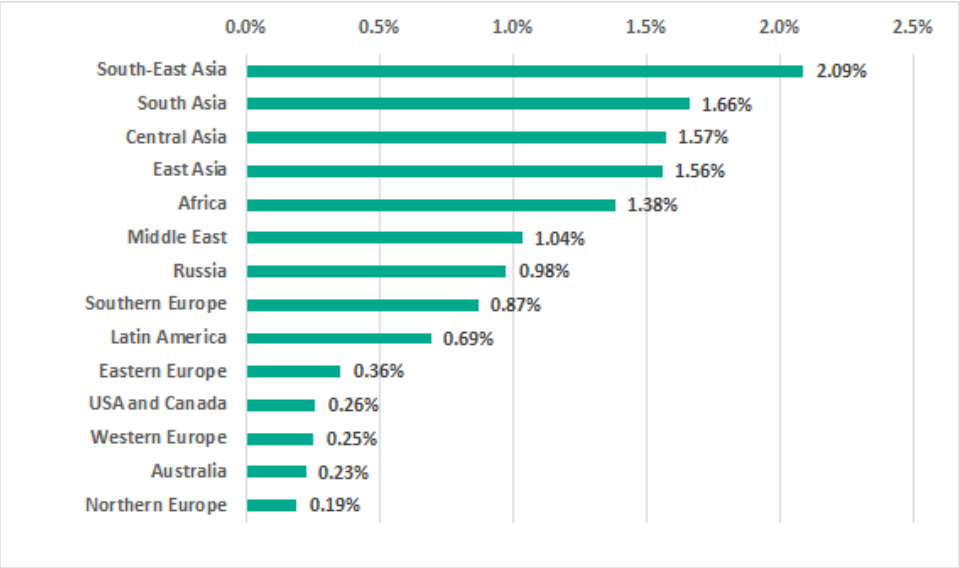
The highest percentage of ICS computers on which ransomware was blocked in H2 2019 was in Asia.

Regions ranked by the percentage of ICS computers on which ransomware was blocked, H2 2019



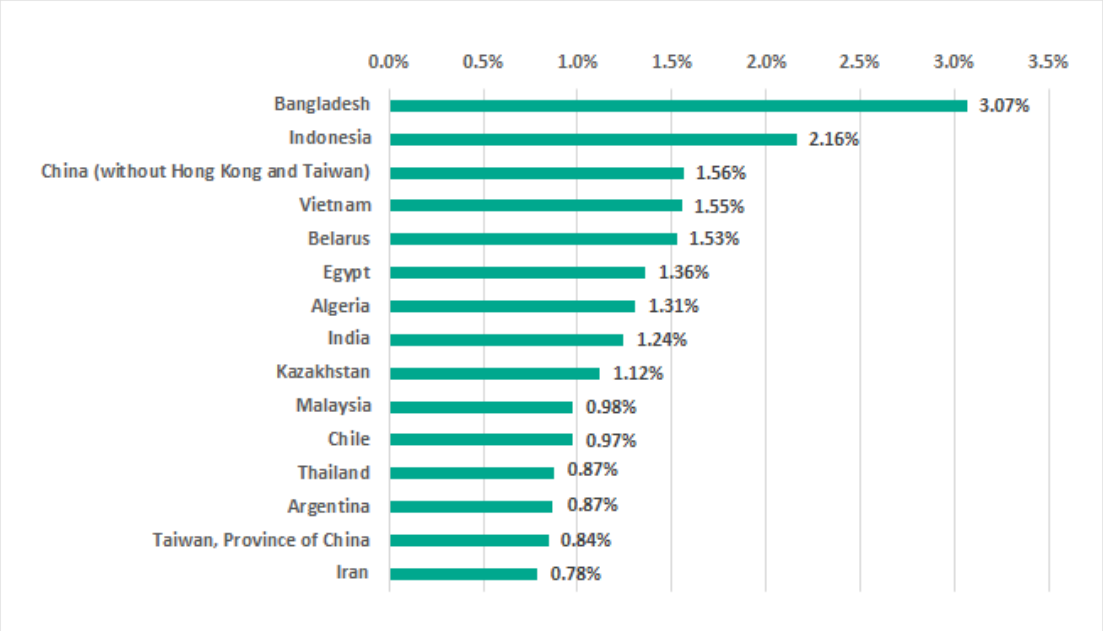
Regions of Asia were in top positions in the ranking for the entire year 2019.

Regions ranked by the percentage of ICS computers on which ransomware was blocked in 2019



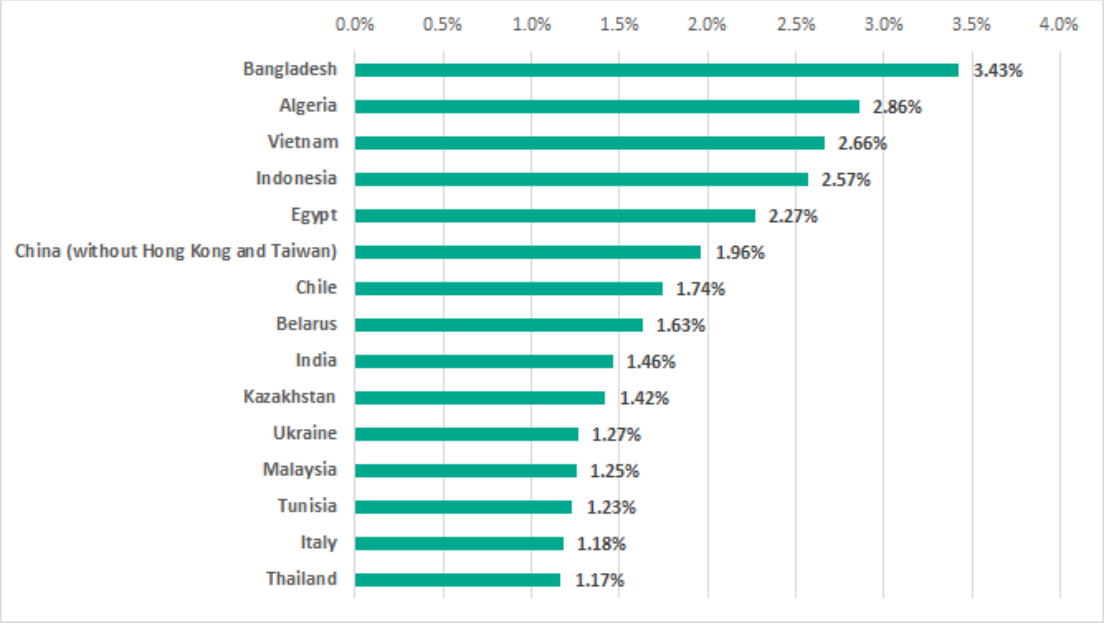
However, Asian countries did not take all of the positions on the TOP 15 ranking for H2 2019.

TOP 15 countries by percentage of ICS computers on which ransomware was blocked, H2 2019



It is worth noting that three European countries, Italy, Ukraine and Belarus, ranked among the TOP 15 countries for the whole year 2019.

TOP 15 countries by percentage of ICS computers on which ransomware was blocked, 2019



Based on the results of the entire year 2019, the percentage of ICS computers in Russia on which ransomware was blocked amounted to 1.0%.

Cities and industrial facilities targeted by ransomware

A wave of ransomware attacks was observed across the globe throughout 2019. Attack victims included, among others, various critical infrastructure organizations and industrial companies. There has been a significant increase in the number of ransomware attacks on municipal services. Based on publicly available statistics and statements tracked by

Kaspersky experts, at least 174 municipal organizations were targeted by ransomware in 2019. This is about 60% more than in the previous year.

Ryuk

In many cases, operators of the Ryuk ransomware (verdict: Trojan-Ransom.Win32.Hermez) were behind the highest-profile encryption ransomware attacks. Throughout 2019, Ryuk infections were mentioned in reports on incidents affecting large enterprises and municipal services.

One example is an attack on Lake City in Florida, USA. As a result of a Ryuk attack, the servers of all city services were disabled, with the exception of police and fire departments, which were on a separate server. The city administration's phone system was also down (this can happen if IP telephony is used). It has been reported that the city's services had backed up their systems, but the backup copies could not be used because they had been deleted by the attackers. As a result, the city had to pay a $460,000 ransom.

It should be kept in mind that it is important not only to back up critical systems in a timely fashion, but also to take other measures, designed to safeguard the backup copies created. Specifically, backup copies should be stored on a separate server with access rights configured to enable only creating new and reading existing backup copies. The integrity of backup copies should be verified on a regular basis and the condition of the hardware on which they are stored should be monitored.

In December 2019, the US Coast Guard released an information bulletin on an attack of Ryuk ransomware against a Maritime Transportation Security Act (MTSA) regulated facility. The bulletin did not identify the attacked facility. What is known about the attack is that it used a phishing email campaign and the malware was downloaded to the system after an employee had followed a malicious link. The malware infected the industrial control systems that monitor and control cargo transfer and encrypted files critical to process operations. As a result, all operations on the affected facility were shut down for over 30 hours. Other consequences of the Ryuk infection included the disruption of the facility's camera and physical access control systems.

Ryuk malware also harmed five oil and gas facilities. The attacks did not bring down any of the facilities, but remote monitoring of the industrial equipment was paralyzed for up to 72 hours, forcing the facilities to switch to manual mode.

The absolute majority of attacks involving Ryuk follow the same pattern. In the first stage, a victim receives a phishing email containing a document with a malicious macro embedded into it. If the victim allows the macro to be executed, the TrickBot malware is downloaded to the machine. The malware enables the attackers to connect to the infected computer and explore the network of the organization being attacked. TrickBot operators attempt to find vulnerable systems and to steal user credentials.

The attackers seek to infiltrate systems running services that are critical for the organization under attack. These are the systems on which the Ryuk malware encrypts data.

Ryuk uses cryptographically secure encryption algorithms. This means that, unfortunately, decrypting files without the private decryption key is impossible. However, risks associated with losing access to data can be mitigated if the organization is prepared for attacks of this type or detects them in their initial stages. You can find our recommendations here.

RobinHood

One of the highest-profile encryption ransomware attacks on municipalities in 2019 was the infection of systems in Baltimore, Maryland in the US with RobinHood malware (verdict: Trojan-Ransom.Win32.Robin). Although the city government's IT specialists were quick to take action (which included disconnecting all computers and servers to prevent the ransomware from spreading), the malware had taken down about 10,000 devices, including databases used by municipal services. As a result of the attack, some of the city's services were completely paralyzed. After a short while, a message was posted on the city's website that contacting the authorities was only possible by telephone.

According to The New York Times, the attackers had used the EternalBlue exploit for the CVE-2017-0144 vulnerability in SMB v1 service. The vulnerability exists in different versions of Windows. EternalBlue got massive coverage in connection with other ransomware, WannaCry, which caused a major outbreak in 2017, infecting millions of computers.

The Baltimore incident highlights another serious issue, which affects both municipal services and systems that are part of the industrial infrastructure – outdated versions of operating systems and other software, which have critical vulnerabilities. In the absolute majority of incidents involving encryption ransomware, the attackers exploit known vulnerabilities, security updates for which have long since been released. For example, Microsoft released the MS17-010 update, which fixes the vulnerability exploited by EternalBlue, on March 14, 2017.

In the case of industrial enterprises, this situation is often due to systems being based on obsolete hardware, which makes updating the software impossible. However, replacing such systems requires substantial financial investment. In such cases, we recommend creating a reliable network perimeter to make it harder for attackers to gain access to vulnerable systems. You can find more details on the techniques used by threat actors to exploit such vulnerabilities and on methods that can be used to provide protection against such attacks in our article.

Sodinokibi (REvil)

In August 2019, systems of 22 towns in Texas, US were attacked at the same time using the Sodinokibi ransomware, also known as REvil (verdict: Trojan.Win32.DelShad). The mass attack became possible when the network of a managed service provider (MSP) used to remotely manage the infrastructure of these towns was breached. Based on available data, the provider in question could be CyrusOne. After compromising the MSP's systems, the attackers gained remote access to systems of municipalities served by the provider. Their files were encrypted and part of the social services became unavailable. According to public statements, all victim towns refused to pay the attackers for decrypting their files. However, the incident recovery process took several weeks and required significant resources, both human and financial.

Unfortunately, attacks that involve compromising the systems of contractor organizations and third-party software vendors are increasingly common. Such attacks can be based on a wide variety of scenarios. Threat actors can attack a potential victim's business partner to steal the contents of the business correspondence. The information stolen can subsequently be used, for example, to create phishing emails. In other cases, such as the incident described above, the attackers may use the remote access tools that the contractor uses to serve the organization being attacked. Finally, third-party software vendors can be attacked, as in the case of attacks involving the ExPetr encryption malware, which was installed on a victim's computer with an update of M.E.Doc accounting software.

To reduce the risk of such incidents, it is essential to control the connections between the organization's network and the networks of other companies (suppliers, contractors, etc.). A special emphasis should be made on controlling the use of remote administration tools. As a rule, incidents involving ransomware attacks on large enterprises occur over a long period of time, during which the attackers explore the enterprise network and select the systems to be encrypted. This means that the incident response team stands a good chance of nipping the criminals' activity in the bud. An arrangement whereby contractor organizations need to get all remote connection sessions approved in advance would help identify such incidents. Testing all application software updates before installing them on critical systems is also recommended.

New encryption ransomware is designed to disrupt the operation of industrial software

Why the operation of industrial software is under threat

Encryption ransomware identified in 2019 attacks includes new malware, MegaCortex and Snake. These malicious programs were of particular interest to researchers because of their lists of processes that are terminated before data encryption starts. In addition to processes of anti-malware solutions, database servers and browsers, these lists include processes of industrial automation system software.

MegaCortex, which was discovered in mid-2019 in attacks on the corporate sector, was the first such malicious program. It actively evolved during the year and saw new versions with new functionality emerge. The MegaCortex list of processes terminated before starting encryption includes over 1,000 process names.

In mid-December, one more encryption ransomware program, which was dubbed Snake (or EKANS) was identified. Snake also contains a list of processes that are terminated before starting encryption. It is worth noting that the process list mostly matches that used by MegaCortex, including processes specific to industrial systems.

These are processes associated with industrial automation system software:

- General Electric Proficy data historian (client and server parts);
- General Electric Fanuc licensing server;
- Honeywell's HMIWeb application;
- FLEXNet licensing server;
- Sentinel HASP license managers;
- ThingWorx Industrial Connectivity Suite;
- Various database processes used in various Historian servers.

It is important to note that both ransomware programs only terminate processes and don't do anything else to them. In other words, they cannot enter commands or manipulate industrial processes in any way. However, the fact that they terminate processes specific to ICS software can lead to negative cyber-physical consequences. It is most likely that the attackers need to terminate application processes to be able to encrypt databases whose files may be in use and whose modification may be blocked.

The emergence of two different ransomware programs designed, among other things, to disrupt industrial automation systems is one more proof of threat actors' interest in attacking industrial enterprises. In the event of having to shut down the industrial process due to the failure of a system whose files have been encrypted, an organization may suffer severe

losses, making it likely that the victim of such an attack would be prepared to pay a large sum for getting its files decrypted.

Attack details

We believe that MegaCortex and Snake attacks are highly targeted and this belief is in line with other experts' conclusions. Consequently, it can be assumed that, as in other similar cases, such infections are mostly carried out manually. As a rule, the initial attack vector is brute forcing the credentials for accounts of those employees who have remote access to systems over RDP.

Upon gaining remote access to the first system, the attackers commonly use Mimikatz or similar utilities to steal credentials for accounts used on the infected system. By collecting more and more credentials, the attackers gain access to more and more systems, until they reach a computer on which an account with domain administrator privileges has been used.

Conclusions on the techniques used to distribute this malware are indirectly supported by the fact that in MegaCortex attacks, the attackers were able to compromise the domain controller of the attacked organization, possibly by using previously stolen credentials.

The file encryption process used by MegaCortex and Snake is standard, with no major differences from the process used by other malware in this class.

Remarkably, in MegaCortex attacks, the malicious executables had valid digital signatures. One signature had been issued to Mursa Pty Ltd., the other to ABADAN PIZZA Ltd. It is most likely that the criminal group behind MegaCortex either stole the digital signatures from these organizations itself or bought it from other criminals on the black market.

In the latest versions of MegaCortex, the attackers not only demand a ransom for decrypting the files, but also threaten to make public the victim's sensitive data should the victim refuse to pay the ransom.

A curious feature of Snake is the ability of the attackers to configure the malware to start encryption at a specific moment in time, e.g., outside the organization's working hours, when the IT security staff or IT administrators may not be available. This can delay and complicate the victim organization's incident response.

Connections with other attacks

As mentioned above, a major part of the process list used by Snake (including processes specific to industrial system software) matches the list used by MegaCortex. This has given rise to theories that there is a connection between these two ransomware families. We believe that matching lists is not sufficient grounds for such conclusions, because the MegaCortex malware was analyzed before the emergence of Snake, and the developers of Snake may have got the list of processes from public sources. Importantly, no other technical evidence of connections between the two ransomware families has been found.

After completing the encryption, Snake leaves a message with instructions and demands that the victim connect to the operators by email. The address specified in the ransom message is bapcocrypt@ctemplar.com. This has given rise to a theory that one of the main targets of Snake attacks was BAPCO, an oil-and-gas company that had fallen victim to the Dustman wiper's attacks. In addition, according to publicly available information, BAPCO uses General Electric equipment, and processes of General Electric software are on the list of processes terminated by MegaCortex and Snake.

However, there is no technical evidence connecting Snake with Dustman. At the same time, the fact that the same enterprise has been attacked by both malicious programs is insufficient to make such conclusions. The theory of these attacks being connected is also contradicted by the different characters of the malicious programs: while Dustman is a wiper, i.e., it attempts to destroy the victim's data, Snake has the technical capability to decrypt the files.

According to available data, the Snake ransomware is in no way associated with the Snake criminal group, also known as Turla – the name match is a coincidence.

Thus, at this time there is not sufficient evidence to support the attribution of MegaCortex and Snake malware to specific known criminal groups.

LockerGoga: up-to-date information

In the previous report, we wrote about attacks of the LockerGoga encryption ransomware on industrial enterprises. Its victims included Norsk Hydro, a Norwegian metallurgical company, Altran Technologies, a French consulting company, and two US chemical companies, Hexion and Momentive.

The consequences of the attack on Norsk Hydro were substantial: according to an official statement posted on the company's website, the total financial damage from the attack amounts to 550–650 million Norwegian crowns (about 60.5–71.5 million US dollars).

LockerGoga attacks continued in the second half of the year. In December 2019, the Federal Bureau of Investigation (FBI) issued an alert on the danger of MegaCortex and LockerGoga ransomware attacks. According to the alert, the attackers use phishing emails, SQL injections, and stolen authentication credentials, as well as exploiting vulnerabilities.

In March 2020, the story of the Norsk Hydro attack took a new, unexpected turn. Dragos published a report, in which it expressed doubts as to whether LockerGoga operators had wanted to encrypt files to get a ransom. According to the report, the attackers aimed to destroy files, not encrypt them.

This is supported by the additional functionality that was implemented in the LockerGoga sample used to attack Norsk Hydro. After encrypting files, the malware changed all user account passwords to the same encrypted value, the system's network card was disabled (apparently to prevent other accounts from authenticating via requests to the domain controller) and a logoff was performed.

In this situation, users were not even able to read the ransom demand left by the malware on the hard drive, so they could not contact the criminals to discuss the conditions on which they might recover access to their files. All of this prevented the attack's monetization.

Dragos experts believe that the same criminal group called FIN6 (according to FireEye classification) is behind both LockerGoga and Ryuk malware. They also believe that the Norsk Hydro attack may have been sponsored by another country's government. They argue that other facilities in Norway were attacked at the same time, but these attacks were thwarted thanks to the quick exchange of information between Norsk Hydro and government authorities.

This is not the first instance of data wiping malware being disguised as ransomware. In 2017, Kaspersky experts had discovered that it was technically impossible to decrypt systems infected by ExPetr malware.

WannaCry is still alive

Almost three years have passed since the outbreak of the WannaCry malware, in which systems were infected in 150 countries across the globe and the total damage reached 1 billion US dollars. Victims of the outbreak included companies involved in different kinds of manufacturing, oil refineries, city infrastructure and electric power distribution facilities.

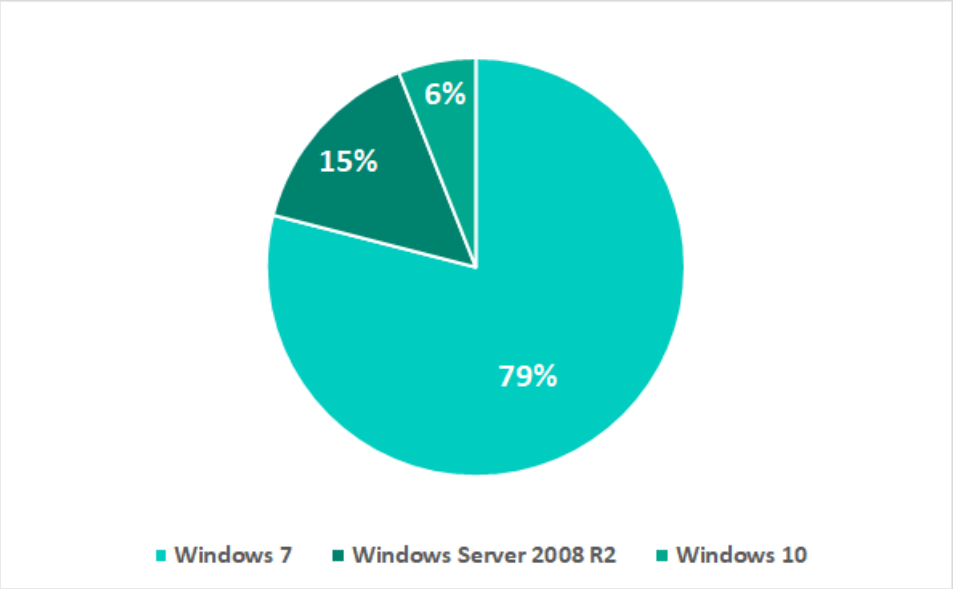
In one of our publications, we provided details on the way networks of industrial enterprises are infected with the WannaCry worm and on the measures that should be taken for protection.

According to our statistics, among all users of Kaspersky products who were attacked by ransomware Trojans in 2019, over 23% were attacked by the WannaCry malware (verdict: Trojan-Ransom.Win32.Wanna). For industrial organizations, the proportion of users attacked by WannaCry in 2019 to all users attacked by ransomware is in excess of 35%. Both these figures mean that WannaCry continues to spread over the internet and still poses a significant threat, particularly to industrial automation systems.

It should be noted that, in most cases, this means that the MS17-010 security update was not installed on the attacked system, enabling WannaCry to exploit the vulnerability in the SMB v1 service. However, the malicious code was not executed because it was blocked by the Kaspersky product.

The diagram below provides information on operating systems used on ICS computers attacked by WannaCry:

Operating systems used on ICS computers attacked by WannaCry



As we can see, the overwhelming majority of systems run Windows 7 (79%) and Windows Server 2008 R2 (15%). The extended support of these systems was discontinued in January 2020. This is particularly worrying, since updates for such systems are released only in exceptional cases.

GandCrab: ransoware-as-a-service in attacks on industrial enterprises

GandCrab (verdict: Trojan-Ransom.Win32.GandCrypt) is notorious encryption ransomware, whose developers chose the RaaS (Ransomware-as-a-Service) business model. GandCrab developers used a web portal to grant various criminal groups access to the malware, after which these groups distributed the ransomware on their own. The service also took care of the ransom payments.

In 2019, law enforcement agencies of several countries and anti-malware companies carried out a set of measures aimed at combating GandCrab. The result was a fully functional utility for decrypting data encrypted by the ransomware, which can successfully handle data encrypted by all GandCrab versions up to 5.1. However, the last version of the ransomware is 5.2. It uses strong encryption based on the RSA and AES algorithms, making it impossible to decrypt data without the private key.

In summer 2019, the group behind GandCrab announced they were closing the ‘service’. In spite of this, GandCrab attacks are still being conducted today. They affect enterprises from various sectors of the economy. Since the ransom payment mechanisms are no longer functional, in the event of infection with the last version of the ransomware (5.2), there is no chance of getting the files decrypted, even by paying a ransom. This has essentially turned the ransomware into a wiper.

Attack details

Two system infection scenarios are currently in use. In both cases, the attack starts with phishing emails, the text in which is written in the language of the country in which the organization under attack operates.

The attack’s further scenario varies depending on the attachment type. In some cases, the attackers use an Excel document with an obfuscated VBA macro, which downloads the GandCrab executable from the attackers’ server and runs it.

After opening the document, the user is prompted to enable active content in the document. If the user agrees to do this, the malicious macro is executed.

Request for the user to enable macros

In other cases, the GandCrab executable is attached to the email. In most cases, attackers use a double extension, such as .doc.exe or .pdf.exe. This technique enables them to deceive

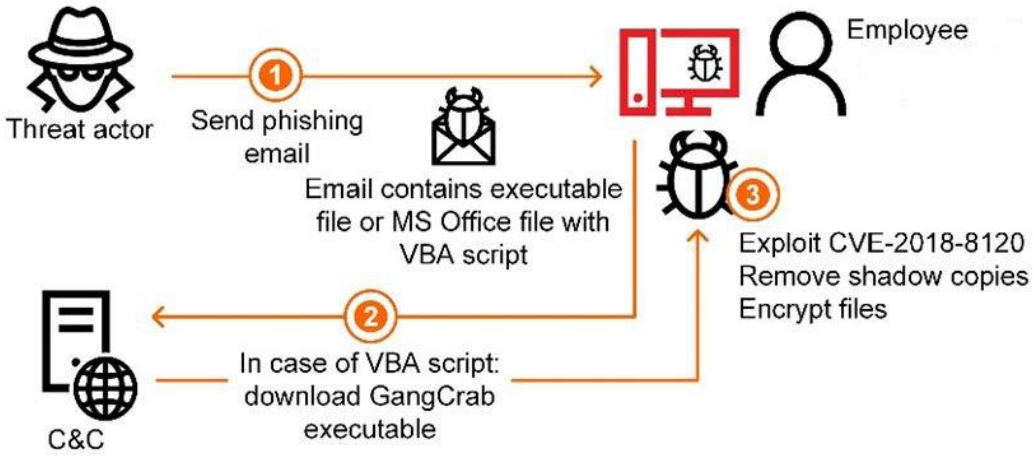
the user, because by default Windows hides extensions for known file types. On a system with default settings, the visible part of the file name will end in .doc or .pdf, respectively. Combined with a replaced application icon, this can convince the user that the attachment is a document rather than an executable file.

Until the middle of 2019, some of the known GandCrab infections used brute forced user authentication data to connect to the system under attack via RDP and execute the ransomware 'manually'. Today, this attack vector us used by other encryption ransomware.

After launching, the GandCrab executable exploits the CVE-2018-8120 vulnerability. This is an improper handling of objects in memory vulnerability in the Windows Win32k component. To make recovering the information more difficult, the malware also deletes all Windows shadow copies.

The diagram below shows the attack kill chain for GandCrab ransomware attacks:

GandCrab attack kill chain



Indian Kudankulam nuclear power plant infected with malware

In September 2019 information was published regarding the discovery of malware at India's Kudankulam nuclear power plant. Later, on October 30, the Nuclear Power Corporation of India Ltd (NPCIL) confirmed that a computer in the Kudankulam power plant's administrative network was infected on September 4. Malware was discovered only on this computer and the plant's ICS systems were not affected.

The subsequent investigation revealed that the most likely infection vector was a phishing attack via either an infected website or a phishing email.

Some researchers believe that the computer in the Kundakulam plant administrative network was infected with the Dtrack malware, which allows attackers to collect and harvest data from the victim computer.

One of the Dtrack samples captured contained user credentials and IP addresses from the Kudankulam internal network. This could point to a targeted attack on the Indian nuclear power plant.

Attack on Rheinmetall technology group

On September 24, 2019 Rheinmetall Group, a large German technology group, discovered that the IT infrastructure of Rheinmetall Automotive plants in Brazil, Mexico, and the USA had undergone malware attacks.

The attacks caused significant disruptions in production at these plants. The infrastructure at other divisions and Rheinmetall group companies was not affected.

According to the company's estimates, attack mitigation and restoration of normal system functioning would require 2-4 weeks and the expected costs would run between 3 and 4 million euro a week.

Attack on sPower wind and solar power installations

In September 2019 it was reported that an electric power generation supplier in western US had been hit by a cyberattack, which had caused temporary disruptions in the electrical systems.

Later it was announced that the target of this attack were the wind and solar stations belonging to the Sustainable Power Group (sPower) in Wyoming and California, as well as their 24 hour control center and corporate headquarters in Utah.

According to the US National Energy Technology Laboratory, several power facilities belonging to sPower experienced periodic firewall outages for about 10 hours between 9:12 AM and 6:57 PM on March 5, 2019. These firewalls controlled communications between the control center and several remote solar and wind farms.

Incident investigation showed that Cisco firewalls had rebooted periodically and became inaccessible for about 5 minutes at a time during each reboot. This in turn disrupted connections between the control center and devices located at remote generation sites, whereby power grid operators temporarily lost sight of device data at generation sites producing a total of 500 megawatts. However, these disrupted connections did not affect power generation and no consumers lost power.

The North American Electric Reliability Corporation (NERC) released a report which concluded that the reboots of the firewalls were caused by an attack exploiting a known vulnerability in the firewall's web interface. Some researchers believe that the vulnerability in question is a DoS vulnerability in the Cisco Adaptive Security Appliance (ASA) (CVE-2018-0296).

New wipers attack industrial enterprises

Bapco, the Bahrain national oil company, was attacked by the Dustman malware on December 29, 2019. According to the National Cybersecurity Authority (NCA) of Saudi Arabia the attack did not cause any severe consequences. Only part of the computers in the Bapco network were affected by the malware and the company was able to continue operations.

Dustman belongs to the wiper malware class (i.e., malware designed to destroy data on the victim computer's drives) and is designed to delete (wipe) data from infected machines. The malware analysis showed that Dustman is an upgraded version of the previously discovered ZeroCleare wiper. ZeroCleare was used in targeted attacks in the energy and industrial sectors in the Middle East and shares certain features with the Shamoon malware.

Attacks on Mitsubishi Electric

In January 2020 Mitsubishi Electric reported an incident that had occurred on June 28, 2019. The cyberattack allowed the threat actors to gain access to internal networks and systems in around 14 divisions in Japan, China, Russia and other countries.

Mitsubishi Electric staff discovered the attack after they noticed some suspicious activity on a company server. An analysis of this activity revealed that data from the network was collected on one computer and then sent out of the company. The investigation showed that data was sent out several times.

At least 120 computers were compromised in Japan and beyond during this attack. Various data were stolen, including confidential information. The company issued a press release stating that about 200 MB of data was stolen overall.

The attack on Mitsibishi Electric is attributed to the Tick criminal group (also known as The Bald Knight, BronzeButler, and ShadowWali), as well as the BlackTech group (also known as Copper Turtle and PLEAD).

According to media reports, the unauthorized access began with hacking a user account of an employee in China and then the attack spread to sites in Japan. A zero-day vulnerability in an antivirus solution was exploited to gain unauthorized access, however the antivirus solution was not named.

It is most likely that the attackers exploited the CVE-2019-18187 directory traversal vulnerability in Trend Micro OfficeScan (now called Apex One). The vulnerability allows arbitrary files to be uploaded, which in turn makes remote code execution (RCE) possible. In October 2019, Trend Micro fixed the vulnerability and warned that cybercriminals were already exploiting it as part of their attacks.

Также It is thought that the 2019 attack was preceded by an attack by Black Tech in 2017, also through a division in China.

After the 2019 attack was revealed, information was disclosed that over the past 10 years Mitsubishi Electric had undergone a number of attacks at various times. In addition to the Tick and Black Tech groups, it is possible that Aurora Panda (APT 17) and Stone Panda (APT 10, Cloud Hopper) may have also been responsible for some of these.

Overall global statistics

In this section, we present the findings of an analysis of statistical data obtained using the Kaspersky Security Network (KSN), a distributed antivirus network. The data was received from those KSN users who gave their voluntary consent to have data anonymously transferred from their computers and processed for the purpose described in the KSN Agreement for the Kaspersky product installed on their computer.

Connecting to the KSN network enables our customers to reduce the time it takes the security solutions installed on their systems to respond to previously unknown threats and to improve the overall detection quality provided by the security products through querying the cloud infrastructure in which malicious object data is stored. That data is technically impossible to transfer entirely to the client side due to its large size and resource consumption.

The telemetry data transferred by the user includes only those types and categories of information which are described in the relevant KSN Agreement. That data is not only significantly helpful in analyzing the threat landscape, but it is also necessary to identify new threats, including targeted attacks and APTs[1].

Methodology used to prepare statistics

The statistical data presented in the report was received from ICS computers protected by Kaspersky products that Kaspersky ICS CERT categorizes as part of the industrial infrastructure at organizations. This group includes Windows computers that perform one or several of the following functions:

- supervisory control and data acquisition (SCADA) servers,
- data storage servers (Historian),
- data gateways (OPC),
- stationary workstations of engineers and operators,
- mobile workstations of engineers and operators,
- Human Machine Interface (HMI),
- computers used for industrial network administration,
- computers used to develop software for industrial automation systems.

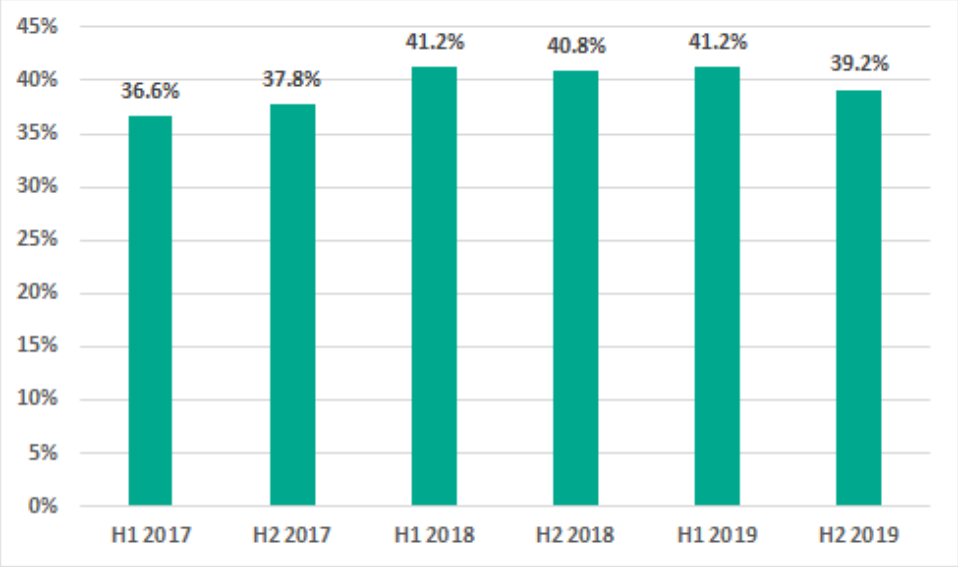
For the purposes of this report, attacked computers are those on which Kaspersky security solutions blocked one or more threats during the reporting period. When determining percentages of machines on which malware infections were prevented, we use the ratio of the number of computers attacked during the reporting period to the total number of computers in our sample from which we received anonymized information during the reporting period.

[1] We recommend that organizations which have any restrictions in place with respect to transferring data outside the organization's perimeter should consider using the Kaspersky Private Security Network service.

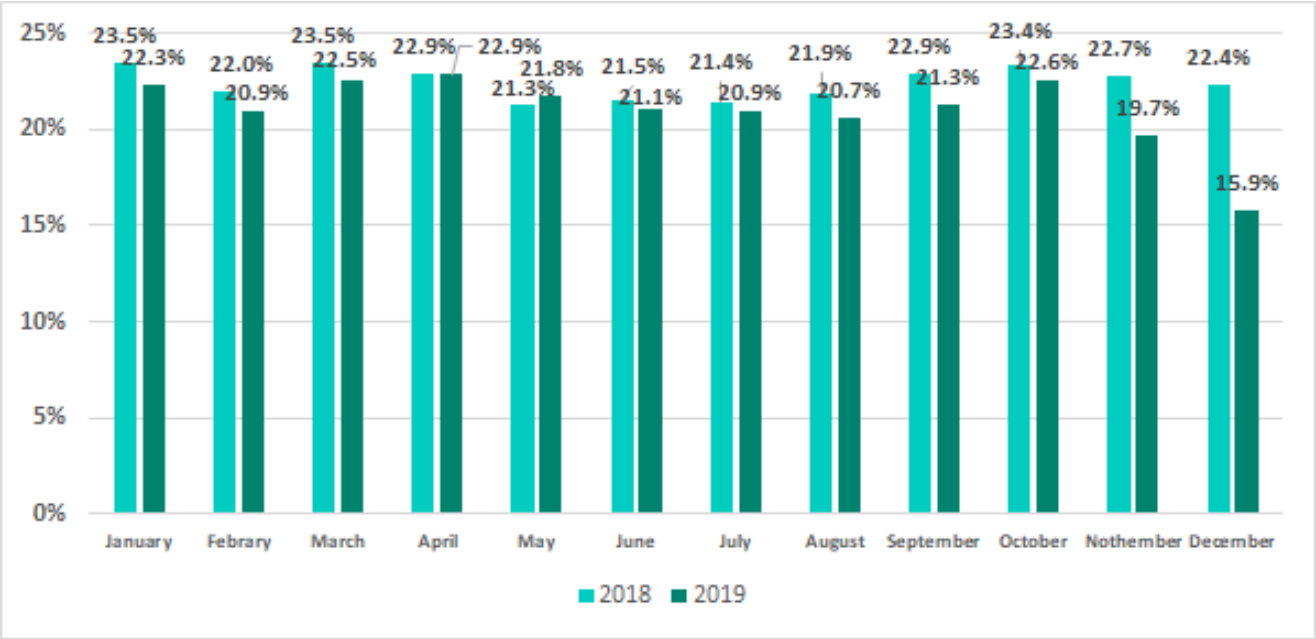
Percentage of computers on which malicious objects were blocked

In H2 2019, malicious objects were blocked on 39.2% of ICS computers – this is lower than H1 2019 by 2 percentage points.

Percentage of ICS computers on which malicious objects were blocked



In H2 2019 the highest percentage of ICS computers on which malicious objects were blocked was recorded in October. The numbers for October are only 0.3% less than in April, the leader in H1 2019.

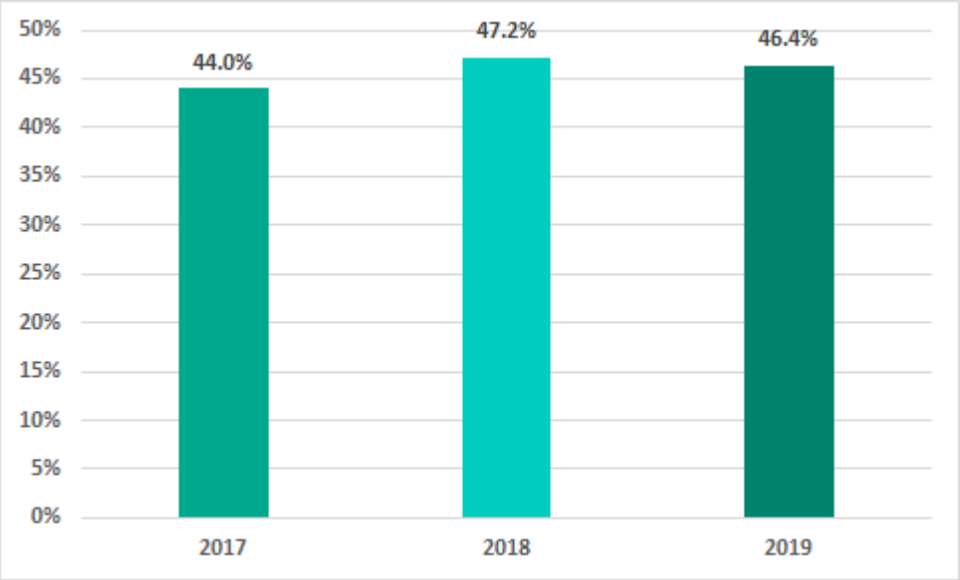


Percentage of ICS computers on which malicious objects were blocked, by month, H2 2019 vs H2 2018

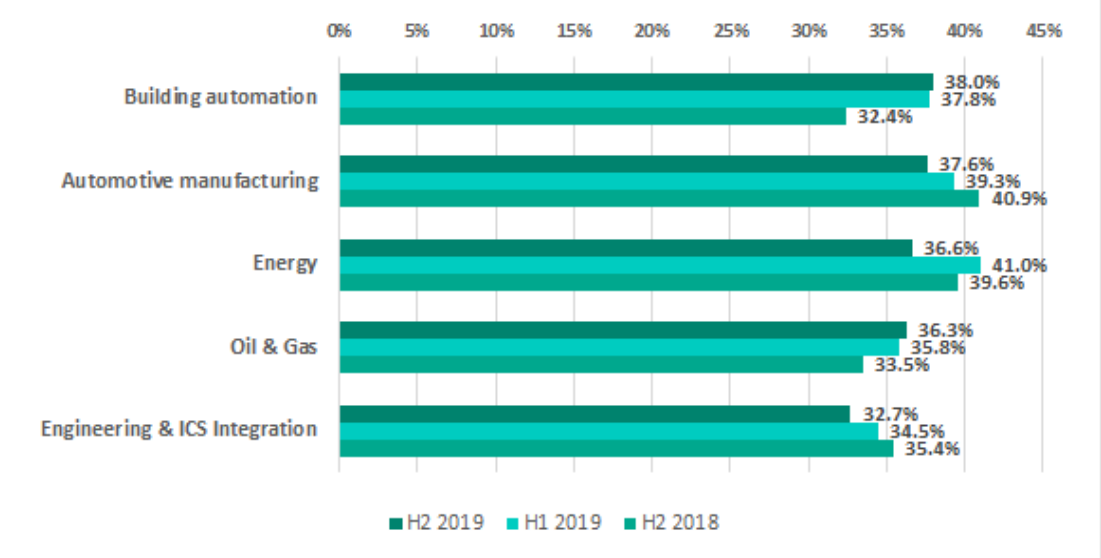
It's worth noting that the seasonal dynamics that we have observed in recent years continued in 2019: the highest percentage of ICS computers on which threats were blocked was recorded in in spring and autumn. However, the decrease in numbers over November and December 2019 was greater than in 2018.

Altogether, in 2019 the percentage of ICS computers on which malicious objects were blocked decreased by 0.8 p.p.

Percentage of ICS computers on which malicious objects were blocked



Percentage of ICS computers on which malicious objects were blocked in some industries



The variety of malware detected

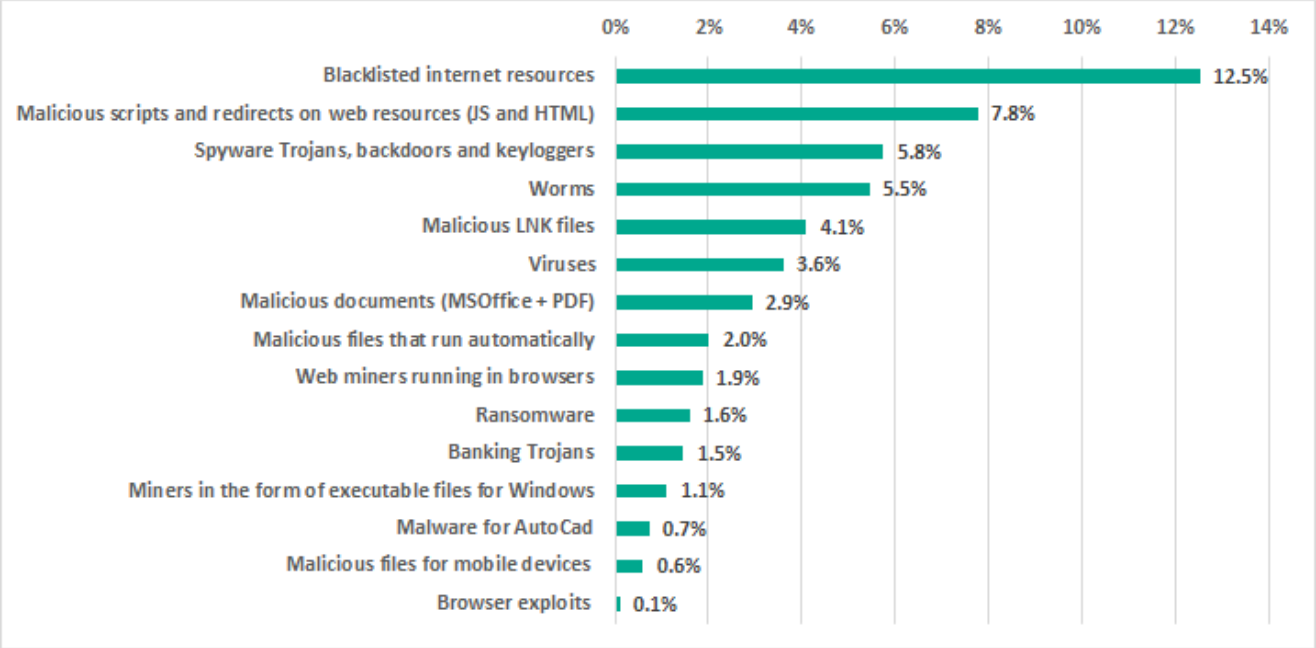
In H2 2019, Kaspersky security solutions blocked over 19.5 thousand malware modifications from 2.3 thousand different families on industrial automation systems.

Malicious object categories

Malicious objects blocked by Kaspersky products on ICS computers fall into many categories.

To give a better idea of types of detected threats, we conducted a detailed classification, which in turn required significant amounts of manual analysis. The resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period.

The results of our detailed analysis revealed the following estimates of the percentages of ICS computers on which malware from different categories had been blocked:



Percentage of ICS computers on which malicious objects were blocked, by malware class, H2 2019

- 12.5% – blacklisted internet resources.

  Web-antivirus protects a computer when programs installed on it (browsers, email clients, automatic application update modules and others) attempt to connect to blacklisted IP addresses and URLs. Such web resources are associated in some way with distributing or controlling malware.

  Specifically, blacklisted resources include, among others, those used to distribute such malware as Trojan-Spy or ransomware disguised as utilities for cracking or resetting passwords on controllers of various manufacturers, or as cracks/patches for industrial and engineering software used in industrial networks.
- 7.8% – malicious scripts and redirects on web resources (JS and HTML) executed in the context of the browser, as well as browser exploits – 0.16%.

- 5.8% – Spy Trojans, backdoors and keyloggers, which appear in numerous phishing emails sent to industrial enterprises. As a rule, the ultimate goal of such attacks is to steal money.
- 5.5% – worms (Worm), which usually spread via removable media and network shares, as well as worms distributed via email (Email-Worm), network vulnerabilities (Net-Worm) and instant messengers (IM-Worm). Most worms are obsolete from the network infrastructure viewpoint. However, there are also worms like Zombaque (0.02%) which implement a P2P network architecture allowing threat actors to activate them at any point.
- 4.1% – malicious LNK files.

  These files are mainly blocked on removable media. They are part of the distribution mechanism for older families such as Andromeda/Gamarue, Dorkbot, Jenxcus/Dinihou and others.

  This category also includes a wide variety of LNK files with the CVE-2010-2568 vulnerability (0.62%), which was first exploited to distribute the Stuxnet worm and has later been exploited to spread many other families, such as Sality, Nimnul/Ramnit, ZeuS, Vobfus, etc.

  Today, LNK files disguised as legitimate documents can be used as part of a multistage attack. They run a PowerShell script that downloads a malicious file.

  In rare cases, the malicious PowerShell script downloads binary code – a specially crafted modification of a passive TCP backdoor from the Metasploit kit – and injects the code into memory.
- 3.6% – Virus class malware.

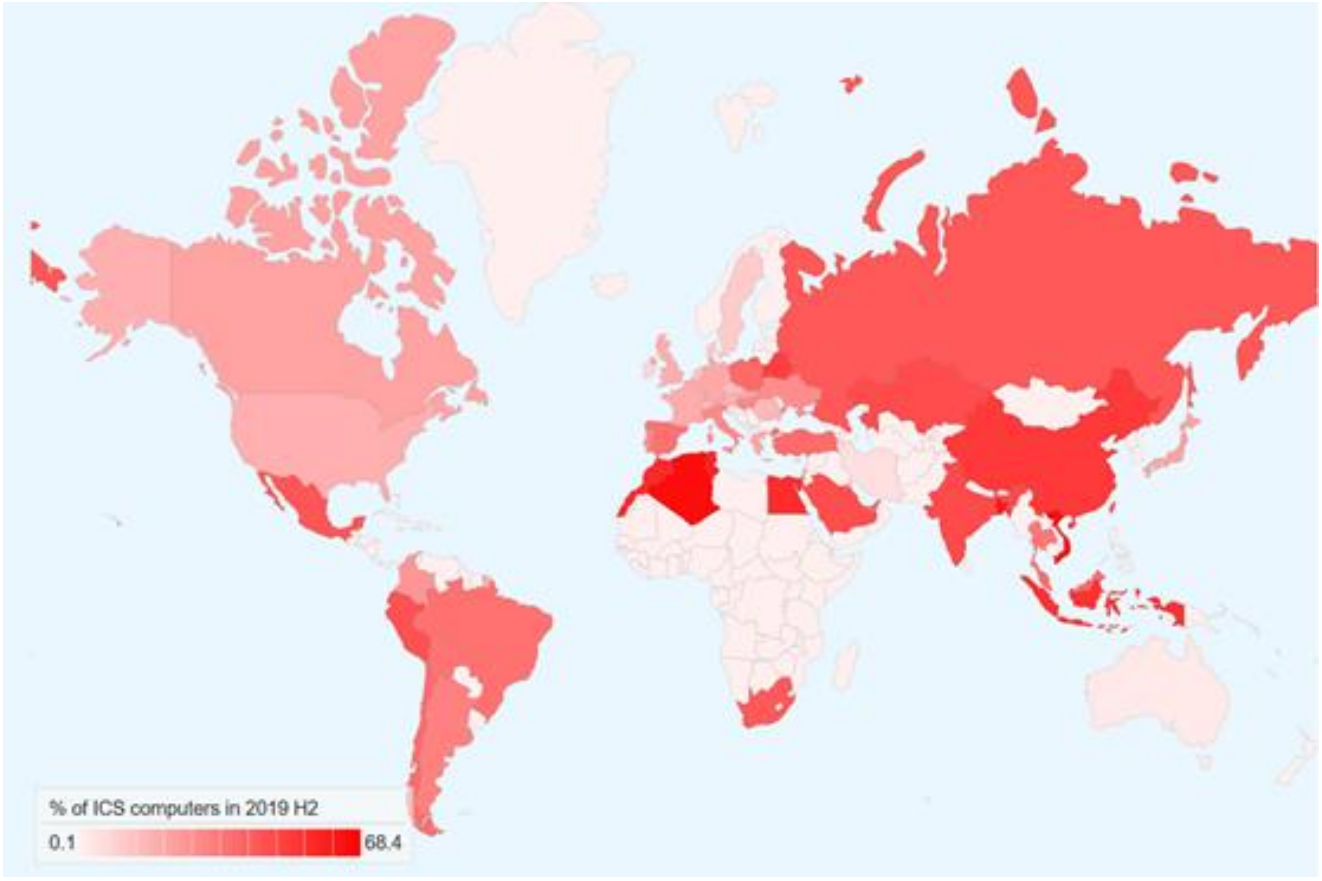
  These programs include such families as Sality (1.1%), Nimnul (0.7%), and Virut (0.5%), which have been detected for many years. Although these malicious families are considered obsolete because their command-and-control servers have long been inactive, they usually make a significant contribution to the statistics due to their self-propagation and insufficient measures taken to completely neutralize them.
- 2.9% – malicious documents (MSOffice + PDF) containing exploits, malicious macros or malicious links.
- 2.0% – malicious files (executables, scripts, autorun.inf, .LNK and others) that run automatically at system startup or when removable media are connected.

  These files come from a variety of families that have one thing in common – autorun. The least harmful functionality of such files is automatically launching the browser with a predefined home page. In most cases, malicious programs that use autorun.inf are modifications of malware from old families (Palevo, Sality, Kido, etc.).
- 1.9% – web miners running in browsers. 1.1% – miners in the form of executable files for Windows.
- 1.6% – ransomware.
- 1.5% – banking Trojans.
- 0.7% – malware for AutoCad.

  It is worth noting that malware for AutoCad, specifically viruses, is mainly detected on computers that are part of industrial networks, including network shares and engineering workstations, in East Asia.
- 0.6% – malicious files for mobile devices that are blocked when such devices are connected to computers.

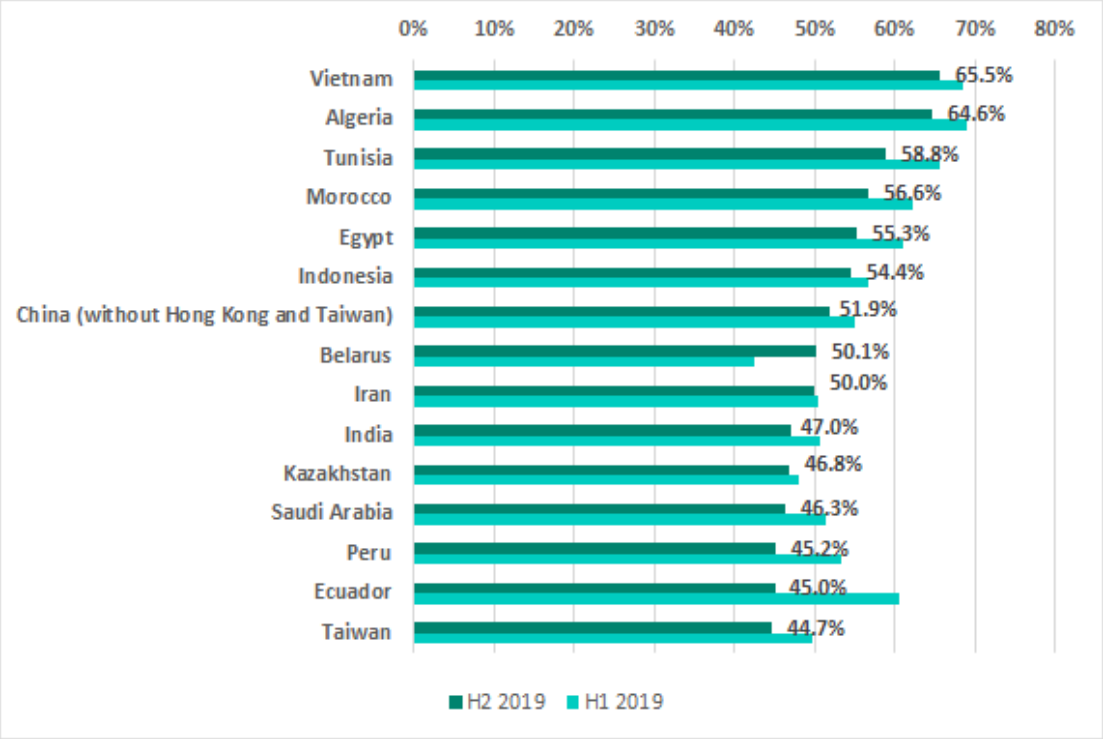
Geographical distribution

The map below shows, for each country, the percentage of industrial automation systems in which malicious objects were blocked to the total number of such systems in that country.



Geographical distribution of attacks* on industrial automation systems, H2 2019
***** *percentage of ICS computers on which malicious objects were blocked***

TOP 15 countries by percentage of ICS computers on which malicious objects were blocked, H2 2019



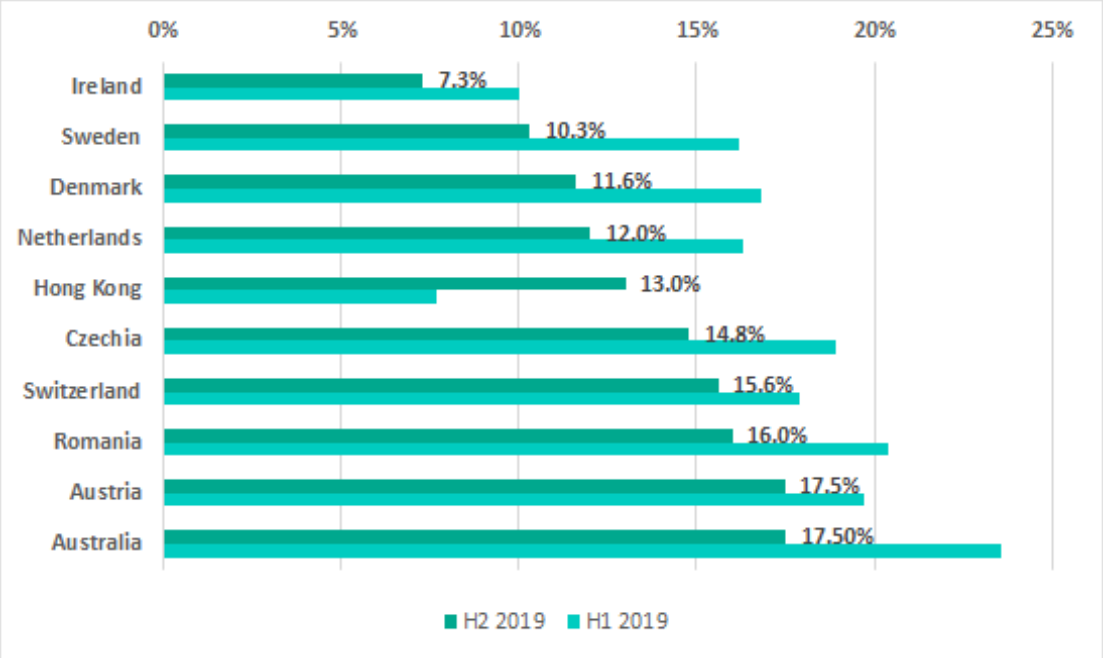
The top five positions in the ranking based on the percentage of ICS computers on which malicious activity was prevented have remained the same for a year and a half now. The only exception was H1 2019 when Bolivia unexpectedly jumped to second place and squeezed Egypt out of the TOP 5.

The most noticeable increases in the percentages of ICS computers on which malicious activity was prevented were observed in Singapore (an increase of 9.2 p.p.), Belarus (7.6 p.p.) and South Africa (6.2 p.p). It is worth noting that the percentages for Singapore had decreased during the previous 3 reporting periods.

In Russia, malicious objects were blocked at least once during H2 2019 on 43.1% of ICS computers, which is 1.7 p.p. lower than the level observed in H1 2019 (44.8%).

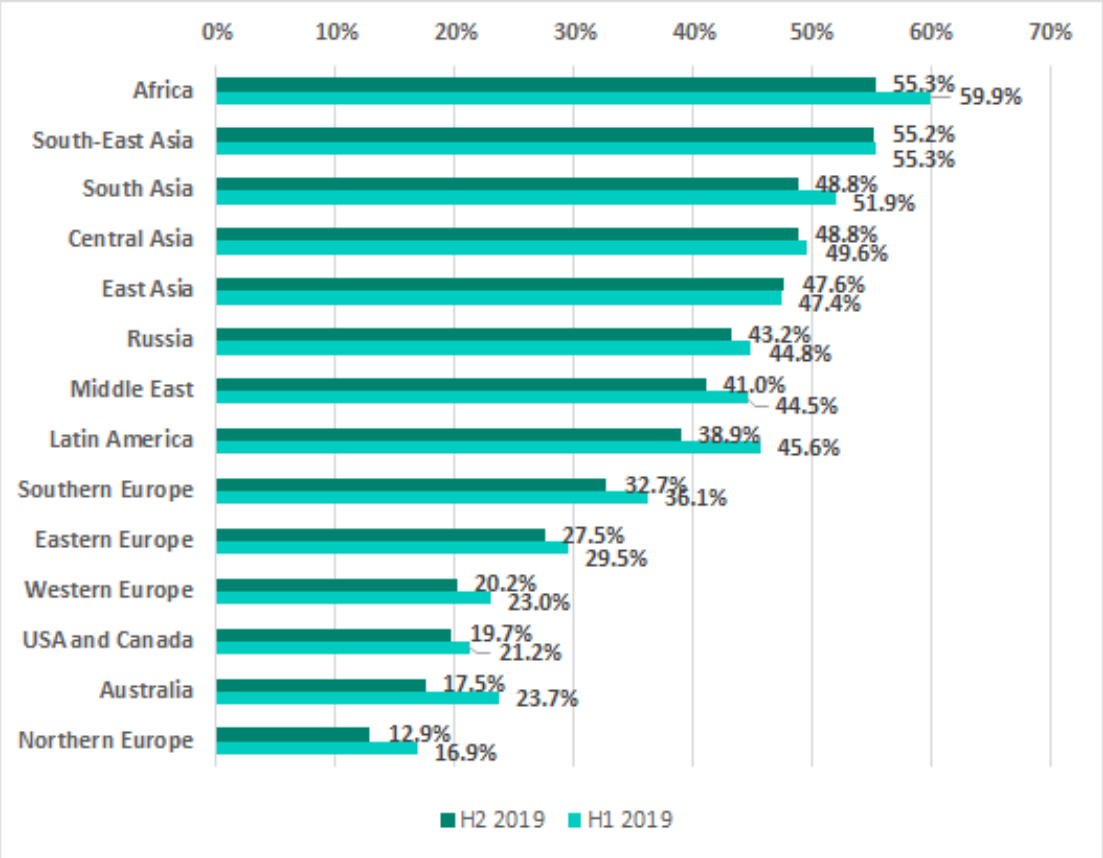
In H2 2019 the US (18.3%) dropped out of the TOP 10 ranking of most secure countries. Great Britain (19%) and Singapore (24.2%) were replaced in the ranking by Romania, Austria and Australia.

10 countries with the lowest percentage of ICS computers on which malicious objects were blocked, H2 2019



Africa, Southeast Asia and South Asia continue as the traditional leaders in the ranking of regions of the world based on the percentage of ICS machines on which malicious activity was prevented.

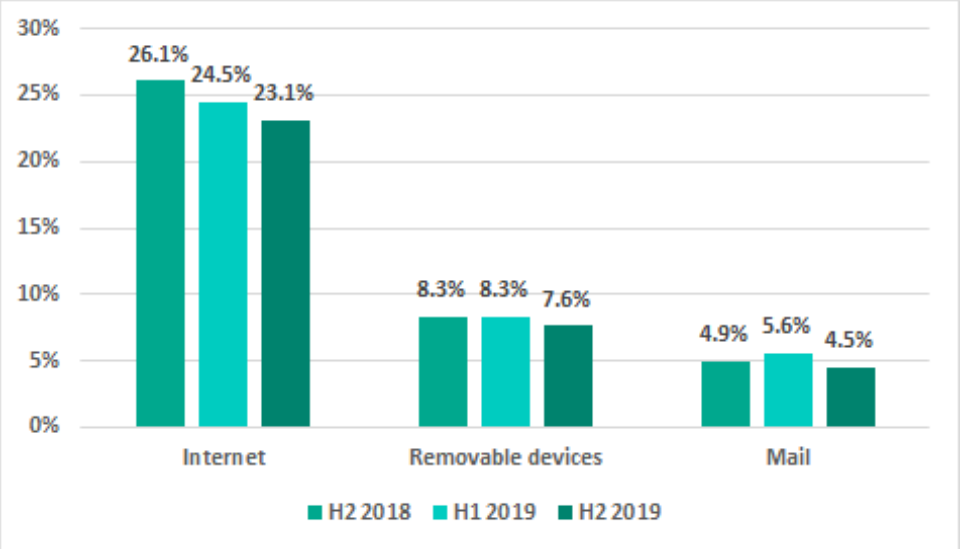
Percentage of ICS computers on which malicious objects were blocked, by regions of the world



Threat sources

In recent years, the internet, removable media and email have been the main sources of threats for computers in the industrial infrastructure of organizations.

Main sources of threats blocked on ICS computers*

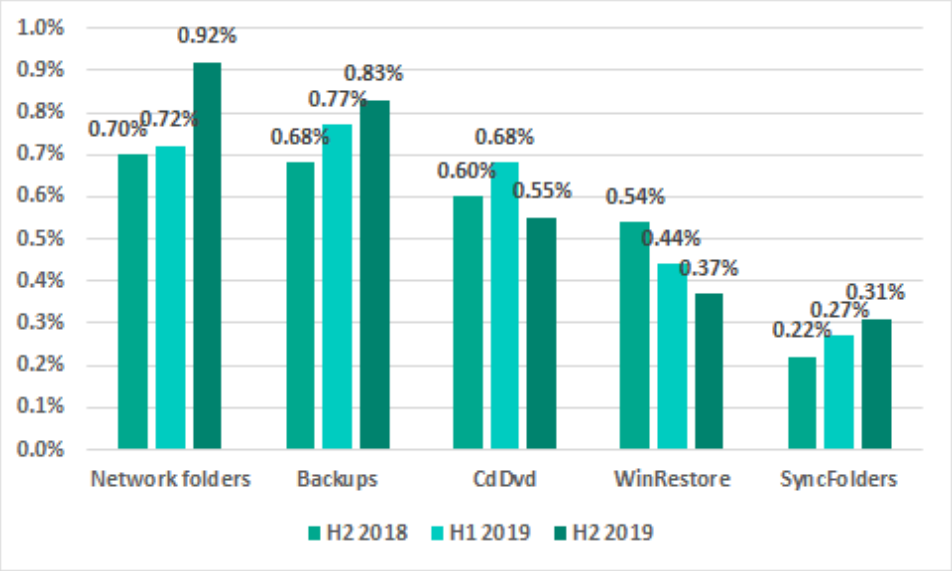


** percentage of ICS computers on which malicious objects from different sources were blocked*

The downward trend continues for the percentage of ICS computers on which malicious objects from the internet were blocked. In H2 2019, this percentage has decreased by another 1.4 p.p.: the internet is now the source of threats blocked on 23.1% of ICS computers.

A significant proportion of internet threats are associated with web pages on various sites infected with web miners, Trojan downloaders and scripts designed to steal cookie files. A decrease in the percentage of ICS computers exposed to these threats is due in part to a smaller number of page views on such sites and to infections being eliminated from web resources.

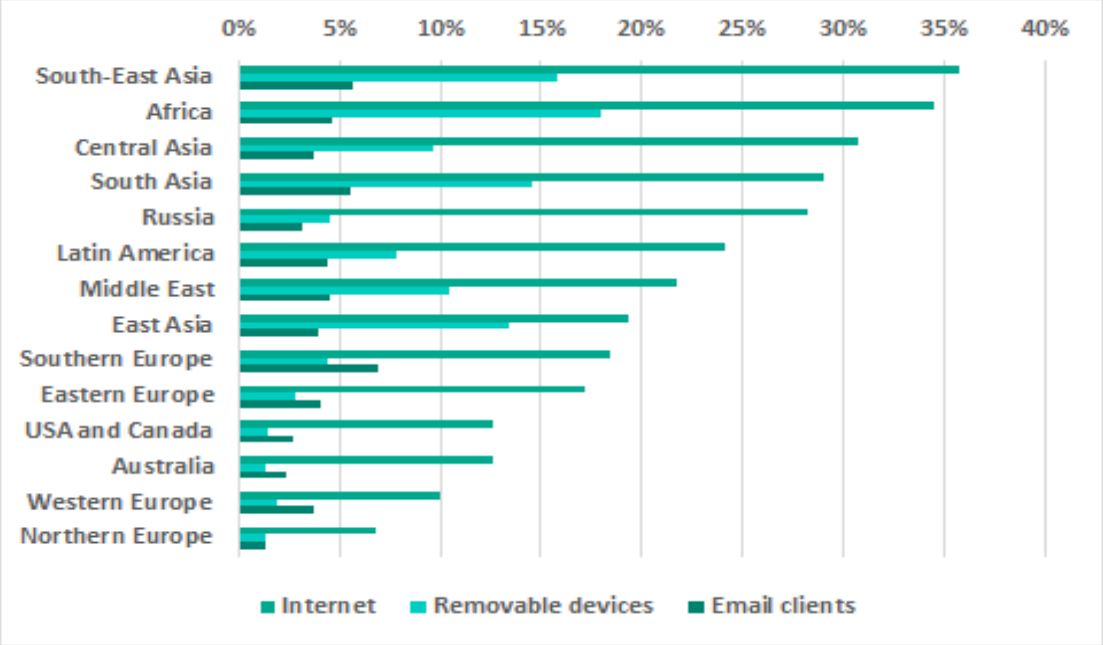
Minority sources of threats blocked on ICS computers*



** percentage of ICS computers on which malicious objects from different sources were blocked*

Main threat sources: geographical distribution

Main sources of threats blocked on ICS computers* by region

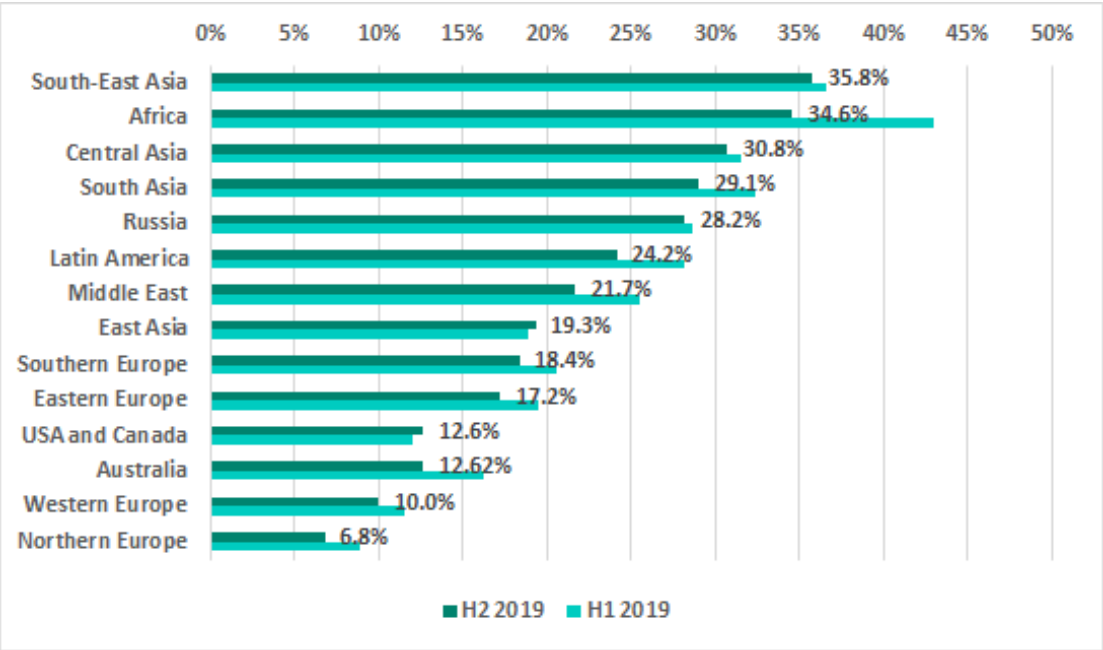


** percentage ICS computers on which malisious objects from different sources were blocked*

Internet

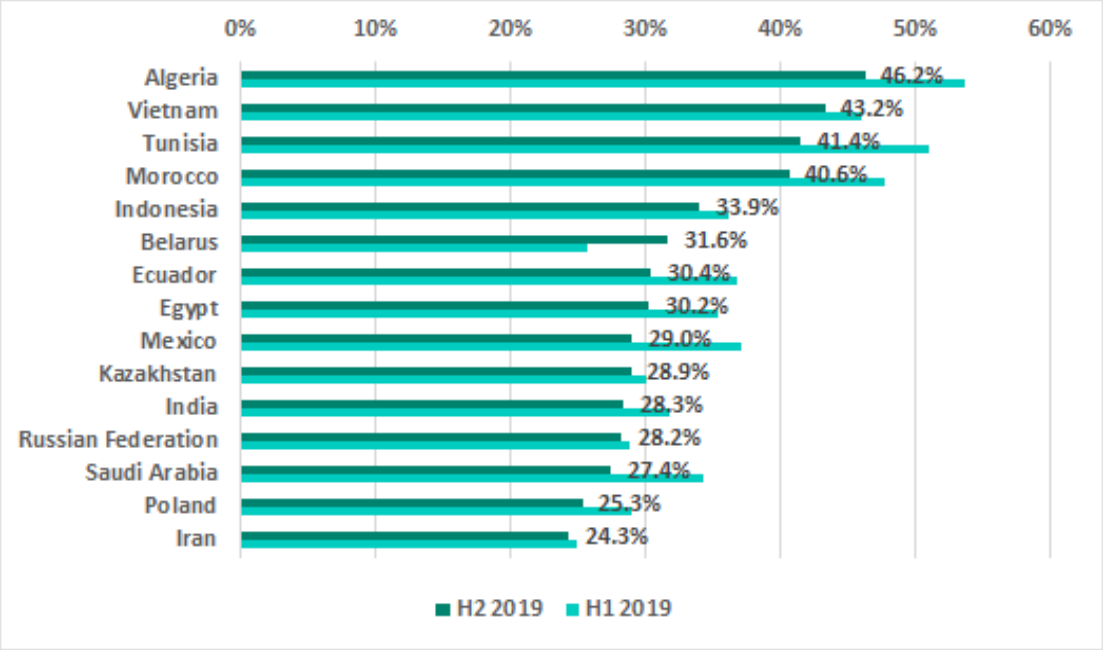
The internet is the main source of threats in all regions of the world. However, the percentage of ICS computers on which internet threats were blocked is much lower in Northern and Western Europe and in North America than in other regions.

Regions ranked by percentage of ICS computers on which internet threats were blocked, H2 2019



Most countries in the TOP 15 by percentage of ICS computers on which internet threats were blocked have remained on the ranking. Chile, Ukraine and Bolivia have been replaced by “newcomers” Belarus, Russia and Iran.

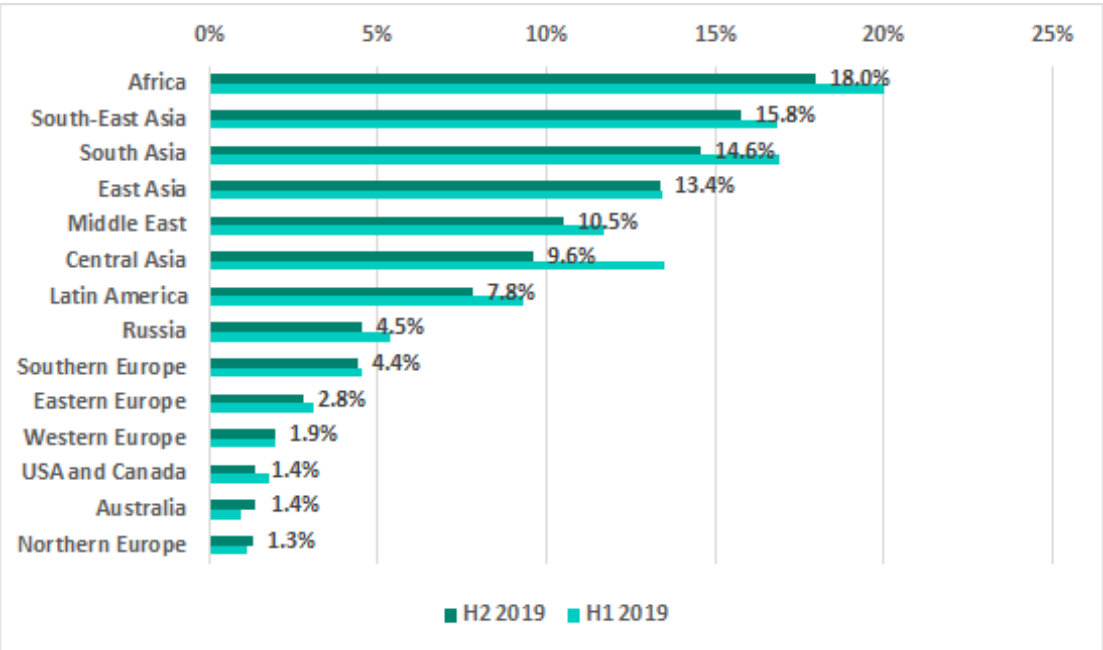
Top 15 countries by percentage of ICS computers on which internet threats were blocked, H2 2019



Removable media

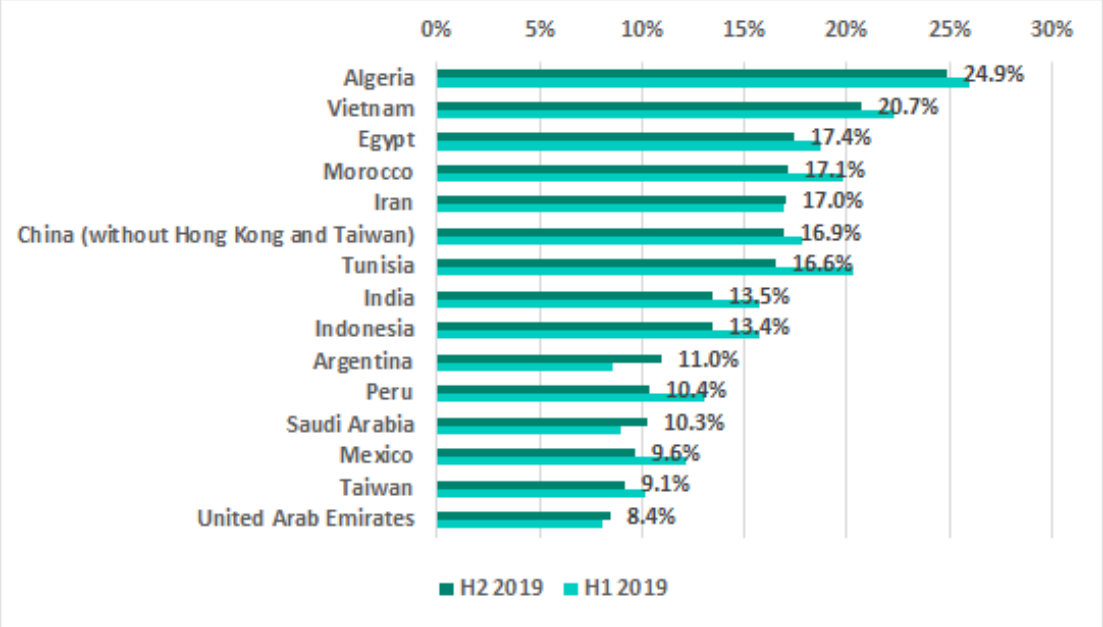
There are no changes in the ranking of regions by the percentage of ICS computers where threats were blocked when removable media was attached. The highest percentage of ICS computers on which threats were blocked when removable media were connected to them was recorded in Africa, South Asia and South-East Asia. That percentage was the lowest in Australia, Northern Europe and North America.

Regions ranked by percentage of ICS computers on which malware was blocked when removable media were connected to them, H2 2019



In H2 2019 the TOP 15 countries ranked by percentage of ICS computers on which malware was blocked when removable media were connected to them did see a few changes: Turkey, Kazakhstan, Thailand and Bolivia were ousted by Taiwan, Saudi Arabia, Argentina and the United Arab Emirates.

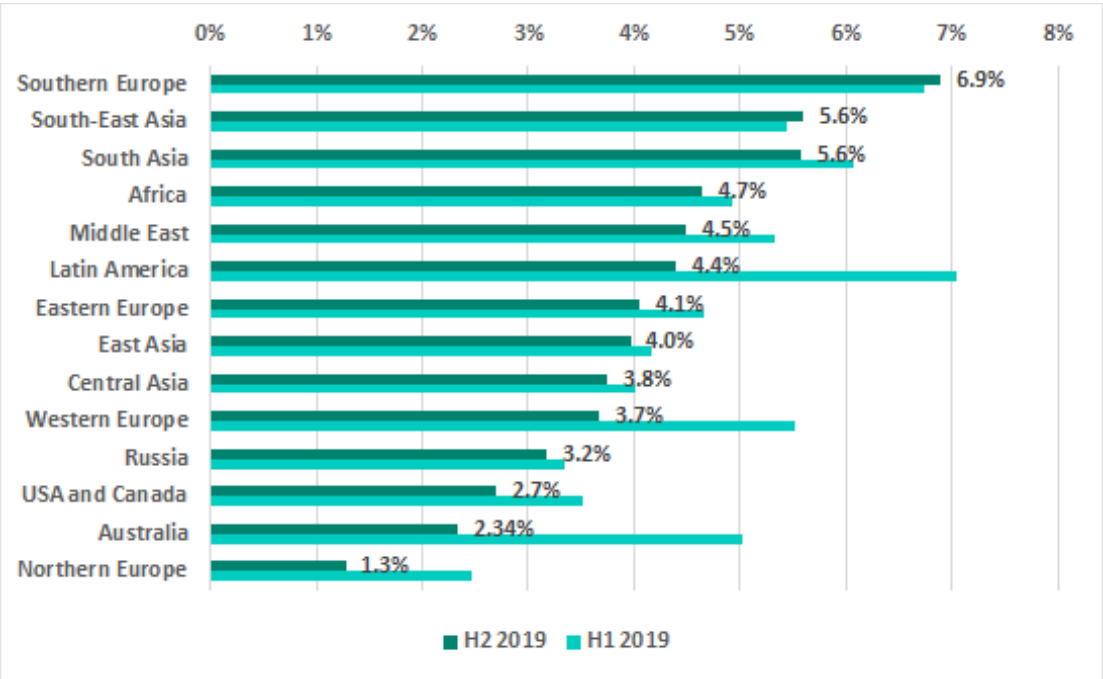
TOP 15 countries by percentage of ICS computers on which malware was blocked when removable media were connected to them, H2 2019



Email clients

For the first time we see Southern Europe lead in the ranking of regions based on the percentage of ICS computers on which malicious email attachments were blocked.

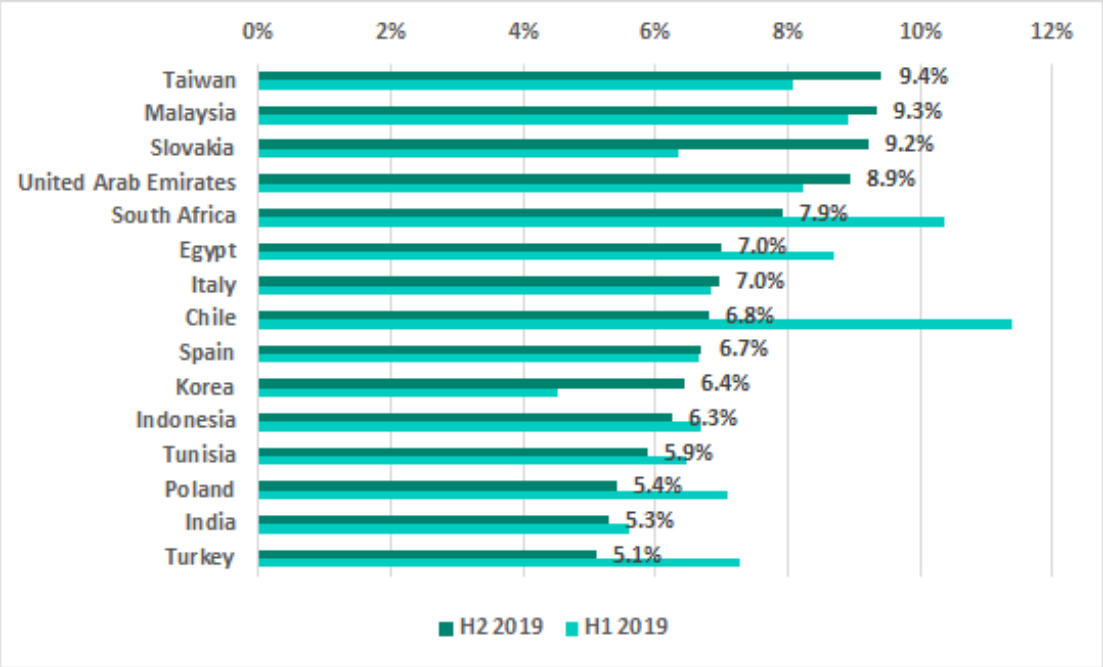
Regions ranked by percentage of ICS computers on which malicious email attachments were blocked, H2 2019



In H2 2019 we saw changes in a third of the TOP 15 countries ranked by the percentage of ICS computers on which malicious email attachments were blocked.

Germany, Japan, Mexico, Argentina and Ecuador left the ranking, while the newcomers included Slovakia, which immediately jumped to third place, as well as Spain, South Korea, Tunisia and India.

TOP 15 countries by percentage of ICS computers on which malicioius email attachments were blocked, H2 2019



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