Kaspersky ICS CERT

kaspersky

Threat landscape for industrial automation systems

H1 2019H1 2019

Kaspersky ICS CERT

24.09.2019 Version 1.0

Contents

© KASPERSKY, 1997 – 2019

© KASPERSKY, 1997 – 2019

Key events

Cyberattack on HOYA results in partial suspension of production in Thailand

In late February, 2019 Japanese optics manufacturer HOYA was hit by a cyberattack, which resulted in a partial shutdown of production lines at its key factory in Thailand.

About 100 of the company's computers were infected with malware designed to steal user credentials and subsequently distribute a cryptocurrency miner.

The attack was discovered on March 1, when the company's specialists noticed a significant degradation in the performance of a server used to manage orders and production, which rendered the order and production management software impossible to use. Although the company was able to prevent the cryptocurrency mining operation, the output of its affected industrial facilities fell to about 40% of its normal level.

The incident also affected computers at HOYA headquarters in Japan that were connected to the network, disrupting the issuing of invoices.

Cyberattack on a US power facility causes multiple firewall outages

The National Energy Technology Laboratory has published information on a cyber event, which took place on March 5, 2019 at an unnamed power sector facility in Western United States and caused interruptions of electrical system operations. This information was included in the Electric Disturbance Events report for 2019.

March	03/05/2019	9:12 AM	03/05/2019	6:57 PM	California: Kern County, Los Angeles County; Utah: Salt Lake County; Wyoming: Converse County;	WECC	Cyber event that causes interruptions of electrical system operations.	System Operations

According to a report published by the North American Electric Reliability Corporation (NERC), firewalls on the enterprise's network perimeter were attacked by an unidentified entity over a 10-hour period. The attackers exploited a vulnerability existing in that device model.

The attacks caused firewalls to reboot, making them briefly unavailable (for about 5 minutes during each reboot). This resulted in brief communication outages between the control center and devices on the enterprise's multiple sites. However, these outrages did not affect power generation and did not cause any power cuts.

The attacks exploited a known vulnerability. The firewall manufacturer offered a firmware update fixing the vulnerability. However, at the time of the attacks the update was not installed on the firewalls used by the enterprise.

After identifying the cause of the incident, the enterprise decided to install the update in three stages: first, update the firmware on a firewall within a non-critical environment at the control center that would not impact operational assets, then, if no negative impact on the organization's industrial process was identified, install the update on vulnerable devices of one generation site and after that, if the first two stages were successful, install the update on all the remaining devices affected by the vulnerability.

This incident has demonstrated yet again the importance of timely installation of software and firmware updates on devices used on industrial enterprises' networks.

© KASPERSKY, 1997 – 2019

Ransomware attacks

In H1 2019, experts noted a surge in ransomware attacks across the globe. Industrial companies were among the organizations that reported ransomware infections. In some cases, these attacks had significant consequences.

Attack on integrated mining and metals company Nyrstar

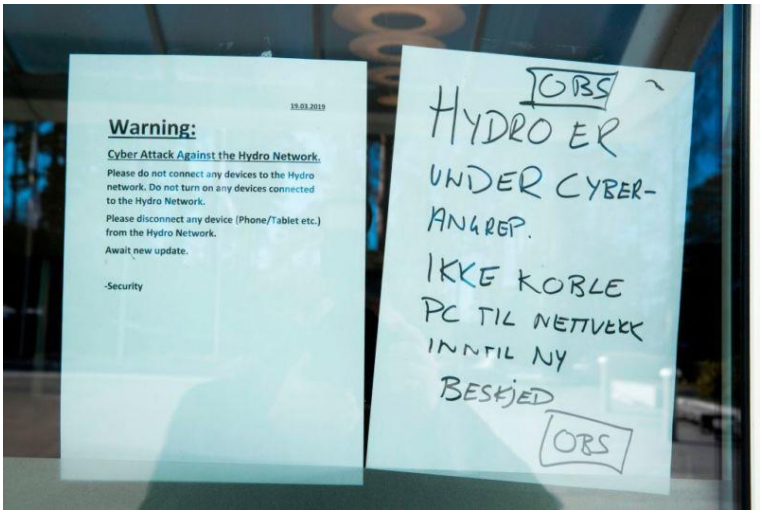
In January 2019, Nyrstar, a Belgian integrated mining and metals company, fell victim to a ransomware attack. The cyberattack affected some IT systems, including the email system, in the company's headquarters in Zurich and at production facilities in different countries of the world. Fortunately, metal processing and mining operations were not affected.

Attacks of LockerGoga encryption malware

LockerGoga was perhaps the most notorious encrypting ransomware of H1 2019.
It successfully attacked several companies.

Attack on aluminum producer Norsk Hydro

In March of 2019, one of the world's largest aluminum producers, the Norwegian metallurgical giant Norsk Hydro, fell victim to a LockerGoga ransomware attack, which began on March 18 and disrupted the operation of the company's industrial facilities in different countries, including Norway, Qatar and Brazil.



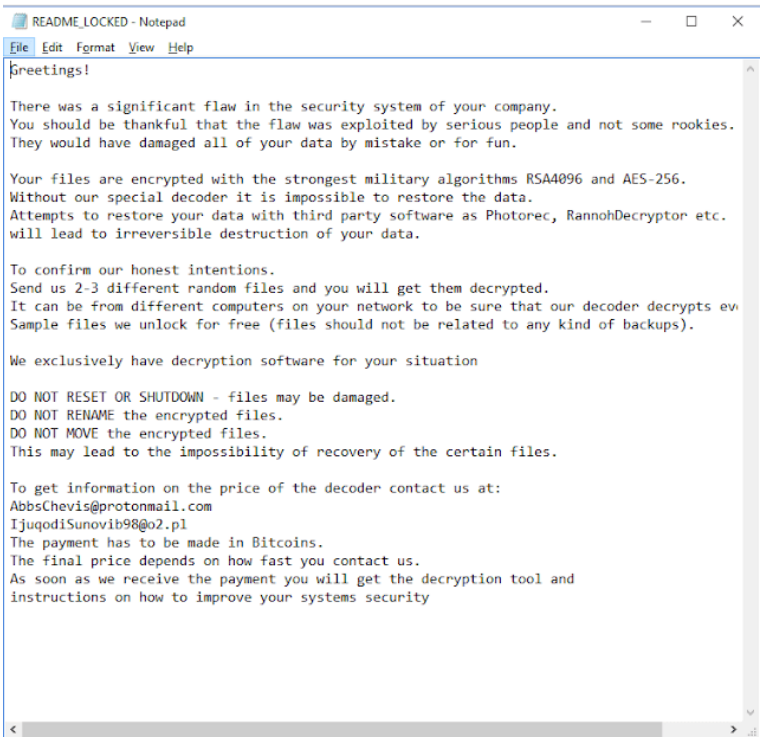
Notes posted in a window of the company's headquarters Source: arstechnica

Despite the Norsk Hydro security service's efforts to prevent the infection from spreading, the malware infected IT systems across the company's distributed network. The attack claimed 22,000 computers at 170 different sites in 40 countries.

The attack disrupted both business processes and the industrial process. Specifically, the malware infected the industrial networks of several rolled product and extrusion plants, blocking some production systems. This caused difficulties and temporary stoppages in production.

© KASPERSKY, 1997 – 2019

Message on an infected computer



According to Norsk Hydro, the incident did not affect the company's power plants, which have isolated IT systems.

By March 21, all plants had been isolated and the propagation of the malware over the company network stopped. However, some production operations were performed in manual mode for an extended period of time. Both operations and sales continued to recover during the quarter following the incident. To restore the enterprise's network to normal operation, Norsk Hydro specialists used existing backups of IT systems.

During the investigation, it became clear that Norsk Hydro had fallen victim to LockerGoga encryption malware. This is a new family of encryption malware. The Trojan is written in C++ using Boost and CryptoPP libraries. It uses hybrid AES + RSA-1024 encryption, with encrypted files getting the additional extension .locked.

It has been suggested that the network of Norsk Hydro may have been infected via a compromised privileged account. The extent of the infection is likely due to the network not being properly segmented.

According to the Norwegian company's financial report for Q1 2019, Norsk Hydro lost 300-350 million Norwegian crowns (about $35 million - $41 million) as a result of the incident. The company's financial losses in Q2 2019 were estimated at 200-250 million Norwegian crowns.

Attacks on other companies

Altran Technologies, a French consulting company, was the first to fall victim to an attack by LockerGoga encryption malware in 2019. The attack occurred on January 24. The malware infection of the company's information systems affected business operations in some European countries. To protect its customers, employees and partners, Altran temporarily shut down its IT network and all applications. The company engaged third-party technical experts to investigate the attack.

© KASPERSKY, 1997 – 2019

It was also reported by mass media that on March 12, i.e., before the attack on Norsk Hydro, two US chemicals companies, Hexion and Momentive, which make resins, silicones and other materials, suffered a LockerGoga ransomware attack. A 'blue screen of death' appeared on some corporate computers in both companies on the day of the attack and files on affected computers turned out to be encrypted.

An email from Momentive CEO, obtained by journalists, referred to a "global IT outage" caused by the malware. According to the email, the company had to order hundreds of new computers to replace the infected ones.

Hexion published a press release, which referred to the attack as a network security incident that prevented access to certain systems and data within the company's network.

Attack on water utility Odintsovsky Vodokanal

On April 15, 2019 water utility Odintsovsky Vodokanal was attacked by ransomware. The malware encrypted data both on the infected device and on network shares. This jeopardized the company's technical documentation and customer data, as well as its billing system.

The attackers' goal was to make the company pay to get its data back, but Odintsovsky Vodokanal refused to pay ransom and asked Kaspersky for help. After analyzing encrypted data samples and the malware itself, Kaspersky experts found a way to recover all the information and sent decryption software to the victim company within a few hours.

The attackers had penetrated the organization's network via the standard Remote Desktop Protocol service built into the Windows operating system. The service was running on one of the company's computers. The attackers were able to crack the password for the account remotely and become authorized on the system. Next, they executed the malware on the compromised computer in manual mode and it started to encrypt the files.

According to Kaspersky data, the majority of victims of this encryption malware are located in Russia.

Attack on aircraft component manufacturer ASCO Industries

On June 7, 2019, ASCO Industries was attacked by ransomware. ASCO is a major supplier of aerospace components, whose customers include US plane manufacturer Boeing and European Airbus. It also supplies parts for Lockheed Martin's F-35 fighter aircraft. Operations had to be suspended at the company's four manufacturing plants due to the attack. As a result, the company sent 1000 employees on temporary leave.

According to media reports, the ransomware infection occurred at the company's Belgian plant at Zaventem. However, the company also suspended operations at its plants in Germany, Canada and the US. It has not been disclosed whether this was due to malware spreading to other plants or was a precautionary step. The company's non-production offices in France and Brazil were not affected.

No information has been disclosed on the malware that attacked the company's Belgian facility, whether ASCO has paid ransom to regain access to its systems or what measures are being taken to restore them to normal operation.

© KASPERSKY, 1997 – 2019

Statistics on relevant threats

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.

© KASPERSKY, 1997 – 2019

Important highlights

This section includes some of the findings we arrived at while analyzing statistics on the threats blocked in H1 2019, which, we believe, could be important for a wide range of our readers. The section includes descriptions of dangerous threats, as well as some suggestions, which we believe to be valid, on vectors possibly used by malware to penetrate ICS computers.

Ransomware again

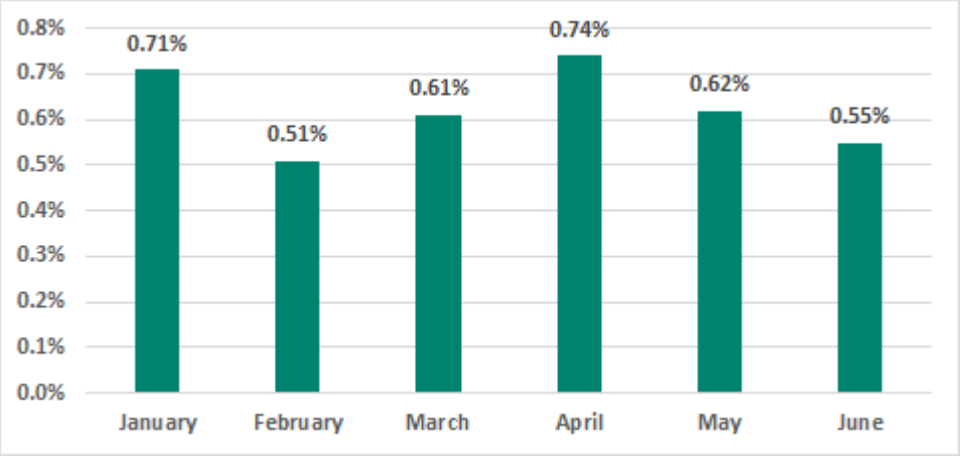
In H1 2019, threat actors actively distributed ransomware. According to mass media reports, several industrial companies were among the victims of this type of malware. It is worth noting that, in all likelihood, not all such cases were reported to the general public, because not all companies are prepared to share such information – particularly if they chose to pay the ransom.

As a rule, ransomware infects computers on industrial enterprises' office networks. The consequences of such infections can be very severe and can include production failure, for example when enterprise planning and management (MES and ERP) systems are infected. However, such malware is at its most dangerous when it infects the industrial network.

According to Kaspersky ICS CERT data, in H1 2019 ransomware infection attempts were prevented on 1.8% of ICS computers. On 19.6% of these computers, the infamous WannaCry ransomware was blocked.

The highest levels of activity associated with ransomware infection attempts on ICS computers were observed in January and April.

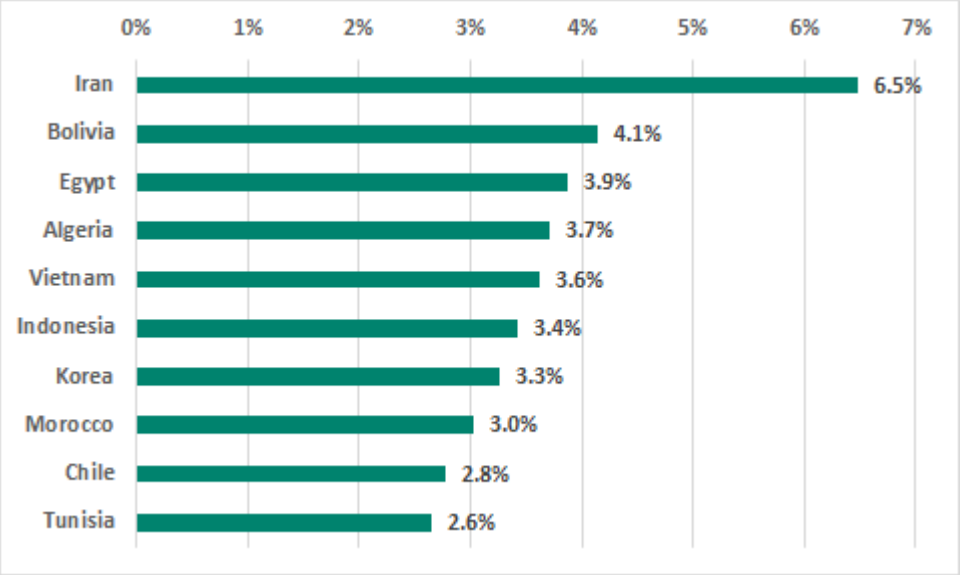
Percentage of ICS computers on which ransomware was blocked, H1 2019



In some countries, this percentage significantly exceeds the global average.

© KASPERSKY, 1997 – 2019

TOP 10 countries in the ranking of countries and territories by percentage of ICS computers on which ransomware was blocked, H1 2019



The top three countries based on the percentage of ICS computers attacked by ransomware were Iran, Bolivia and Egypt.

Italy had the highest percentage (2.0%) of ICS computers attacked by ransomware among Western European countries. The figure for Russia was 1.1%.

Worms distributed via removable media as a malware propagation vector

Self-propagating malicious programs are very active in some countries. In the cases that we analyzed, these were worms (malicious objects from the Worm class) designed to infect removable media (USB flash drives, removable hard drives, mobile phones, etc.). Users who are not aware of cyberthreats connect infected devices to ICS computers and unwittingly execute worms disguised as legitimate files. Most such files are blocked as a result of scanning the removable drive when it is connected to the computer or later, when an attempt is made to execute a malicious file. However, in some cases, users ignore the antivirus solution's decision to block the threat, believing it to be a false alarm, or exclude removable media from scanning, apparently because they are unaware of the risk involved. This results in worms infecting their computers and downloading next-stage malware.

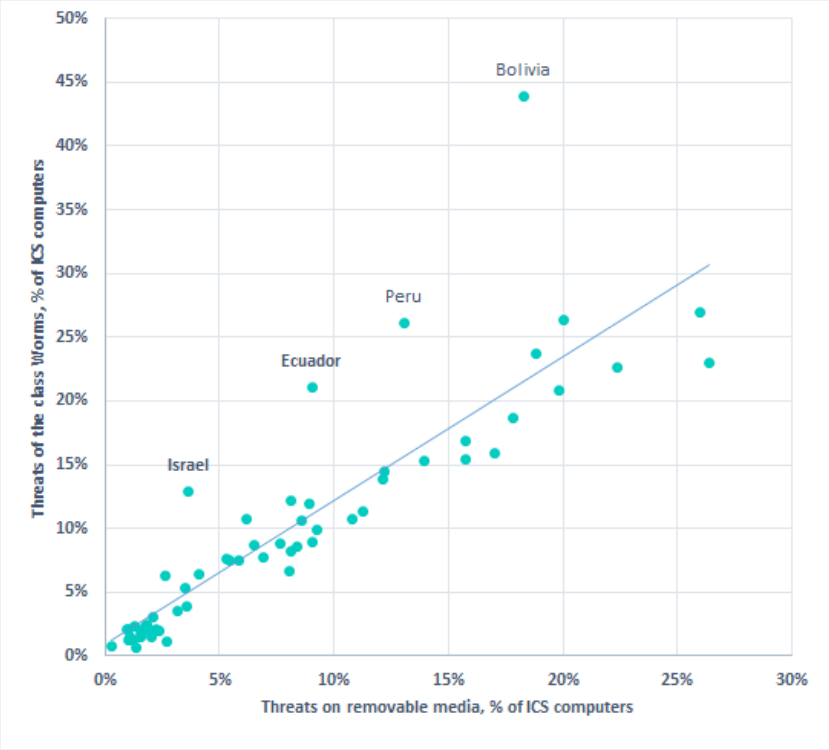
The technique most commonly used to disguise the worm samples we analyzed that spread via removable media is LNK files. Worms save malicious instructions (scripts) in these files as CMD, Powershell or VisualBasicScript parameters. In some cases, this approach enables malware to evade security solutions which check only files that are executed but not command-line parameters for trusted interpreter programs.

If an infected computer is connected to the internet, the worm sends information about the infected system to the command-and-control center (C&C) and downloads next-stage malware to the computer – in most cases, malicious cryptocurrency miners and ransomware. For example, in Iran, where the percentage of ICS computers attacked by encryption malware is the highest (compared with other countries), such worms are used to distribute Cerber ransomware.

It appears that infection with worms via removable media is the most common scenario for ICS computers. This is confirmed by the strong positive correlation shown in the diagram below: $R>.95$, $p<.001$.

© KASPERSKY, 1997 – 2019

Correlation* between percentages of ICS computers on which malicious objects from the Worm class were blocked and percentages of ICS computers on which malicious objects were blocked on removable media



**** correlation parameters: R>.95, p<.001, excluding the anomalous figures for Bolivia, Peru, Ecuador, and Israel***

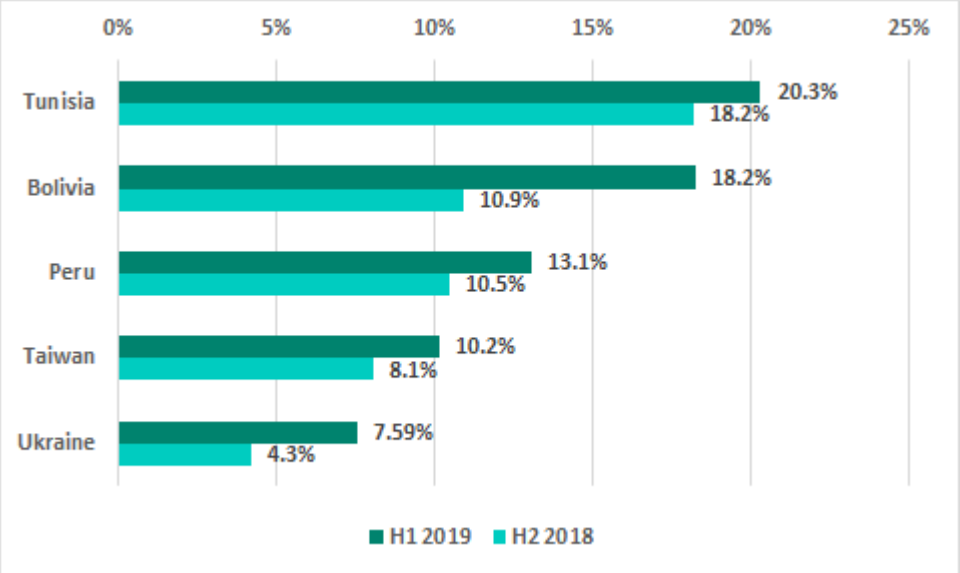
It should be noted that the correlation parameters were calculated without taking into account the anomalous figures for Bolivia, Peru, Ecuador and Israel, where worms are often found not only on removable media, but also in user and system archives and network shares.

Thus, in Bolivia in H1 2019, worms were blocked on a record-breaking 43.9% of ICS computers. At the same time, malicious objects were blocked on 18.2% of ICS computers in Bolivia when removable media were connected to them. This is 7.3 p.p. more than in H2 2018 (for comparison, the global average remained unchanged at 8.3%).

The frequent attempts to infect ICS computers with worms in countries with anomalous percentages apparently reflect the background situation of high worm activity in each of these countries. Thus, in H1 2019, worms were detected on more than 35% of ***all*** computers in Bolivia (ICS, corporate and home computers) when removable media were connected to them.

© KASPERSKY, 1997 – 2019

The five countries and territories with the highest increase in the percentage of ICS computers on which malicious objects were blocked when removable media were connected to them are shown in the following diagram:



In addition, in some countries (such as Bolivia, Ecuador, Peru and Israel), sources of worm distribution are in most cases not initially located outside the ICS perimeter (e.g., on a removable drive connected to an ICS computer), but inside the ICS network perimeter. In most cases, such internal sources of repeated infection are computers on which no effective antivirus protection is installed.

TOP 3 cyberthreats for the energy sector

In H1 2019, we carried out a more detailed analysis of the threat landscape for several industries. Below we present brief results of our research on threats that affect one of these industries – the energy sector.

Object of research

Computers on industrial networks used to configure, maintain and control equipment in power generation, transmission and distribution systems, as well as control systems at energy sector facilities, on which Kaspersky products are installed. This includes Windows computers on which various software packages designed for the energy industry are installed.

Summary

Overall, in H1 2019 Kaspersky products were triggered on 41.6% of ICS computers in the energy sector. A large number of conventional (i.e., not designed for ICS) malware samples were blocked.

Among the malicious programs blocked, the greatest danger is posed by cryptocurrency miners (2.9%), worms (7.1%), and a variety of versatile spyware (3.7%). Infection with such malware can negatively affect the availability and integrity of ICS and systems that are part of the industrial network.

© KASPERSKY, 1997 – 2019

Although malware blocked on the computers analyzed is not ICS-specific, the danger posed by it should not be underestimated.

Such malware is capable of:

- stealing confidential information, including that which can potentially be used for further developing an attack in the direction required by the attackers;
- loading and executing arbitrary malicious software selected by the attackers;
- providing attackers with the ability to control infected computers remotely.

Thus, the side effects of an active infection could have a significant impact on the availability and integrity of the ICS and systems on the industrial network.

At the same time, some of the threats detected have properties characteristic of targeted attacks. We are currently analyzing these attacks.

AgentTesla spyware

AgentTesla is one of the most dangerous threats among those detected. This specialized Trojan Spy malware is written on the .NET platform and is designed for a single purpose – to steal data, specifically authentication data, screenshots, and data captured from the web camera and keyboard. The first samples, which were identified in 2017, sent the data collected to command-and-control servers over HTTP. In samples detected in 2018, the protocol had been changed to SMTP. In all of the cases analyzed, the attackers sent data via compromised mailboxes of various companies.

In most cases, the malware was distributed via phishing emails that had a Microsoft Word document with an embedded AgentTesla downloader written in VisualBasic attached to them.

The command servers / mailboxes used by the malware are specific to each attack and are used not only to send stolen data but also to download malware updates. It is worth noting that the Trojan can handle an “uninstall” command, which enables the malware to remove any trace of infection and self-destruct.

The AgentTesla spyware poses a serious threat to industrial systems because it is used in targeted attacks and the data stolen can be used to plan and carry out subsequent stages of the attack.

Meterpreter backdoor

Kaspersky products have identified several cases of the Meterpreter backdoor being used to remotely control computers on industrial networks of energy systems.

Meterpreter is part of the notorious Metasploit framework and is designed to provide manual or semi-automatic control of attacked computers.

Meterpreter has significant capabilities related to providing stealthy remote control of infected machines, because it uses a reflective malicious code injection technique. The technique enables attackers to load arbitrary malware directly into executable memory on a computer attacked by the backdoor. This allows the attackers to ensure that the attack remains undetected for a long time because it uses bodiless malware that is not written to the hard drive.

The initial vector of the attacks, their origin and objectives are currently being analyzed.

© KASPERSKY, 1997 – 2019

Attacks that use the Meterpreter backdoor are targeted and stealthy and are often conducted in manual mode. The ability of the attackers to control infected ICS computers stealthily and remotely poses a huge threat to industrial systems.

Syswin, a wiper worm

Another serious threat blocked by Kaspersky products on computers in the energy industry is Syswin, a new wiper worm written in Python and packed into the Windows executable format.

The worm spreads via network shares and removable media that are connected to an infected system.

When launched, the worm infects the system, registering itself as an autorun application. Next, it sets the deletion flag for each executable file on the computer's hard drives. As a result of this, all flagged files are deleted by the operating system when it restarts, putting the computer out of operation.

When infecting removable media, the worm changes the size of each file to 0, thereby destroying information in these files.

The threat can have a significant impact on ICS computers due to its ability to self-propagate and destroy data.

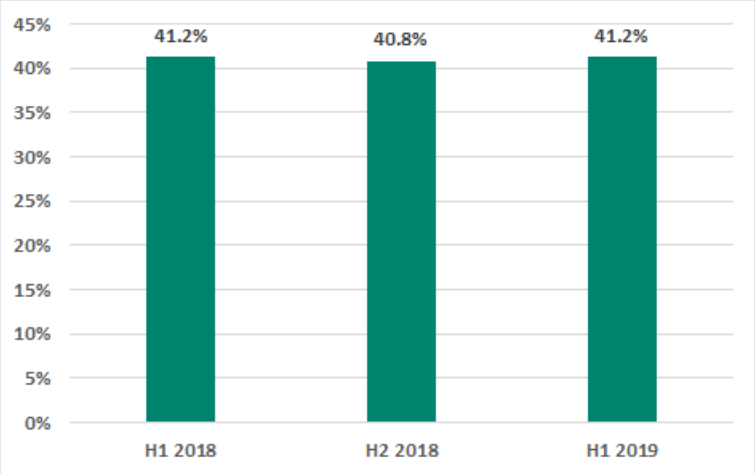
© KASPERSKY, 1997 – 2019

Overall global statistics

Percentage of computers on which malicious objects were blocked

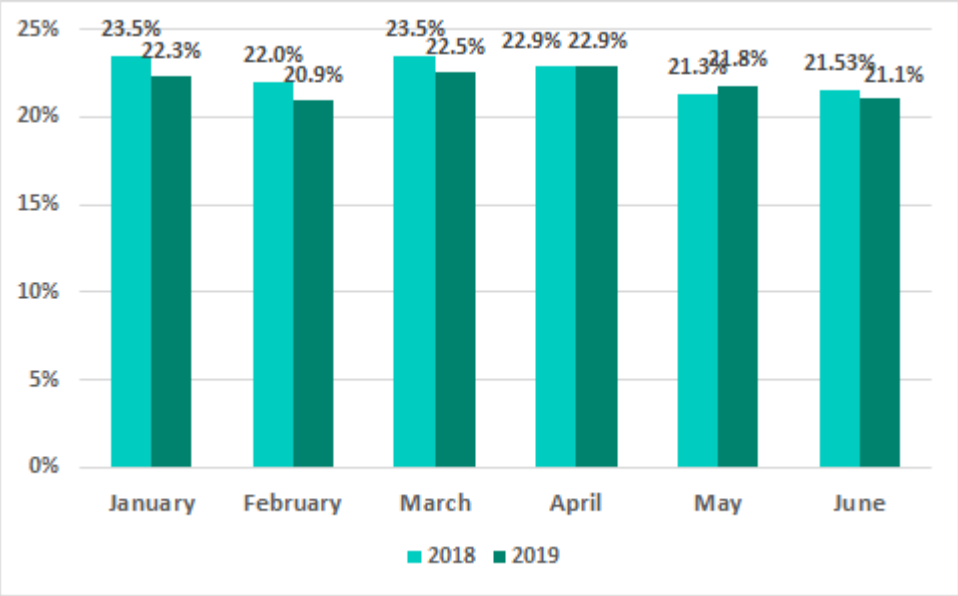
In H1 2019, malicious objects were blocked on 41.21% of ICS computers – the same percentage as in H1 2018 and a slight increase of 0.37 p.p. over the H2 2018 figure.

Percentage of ICS computers on which malicious objects were blocked



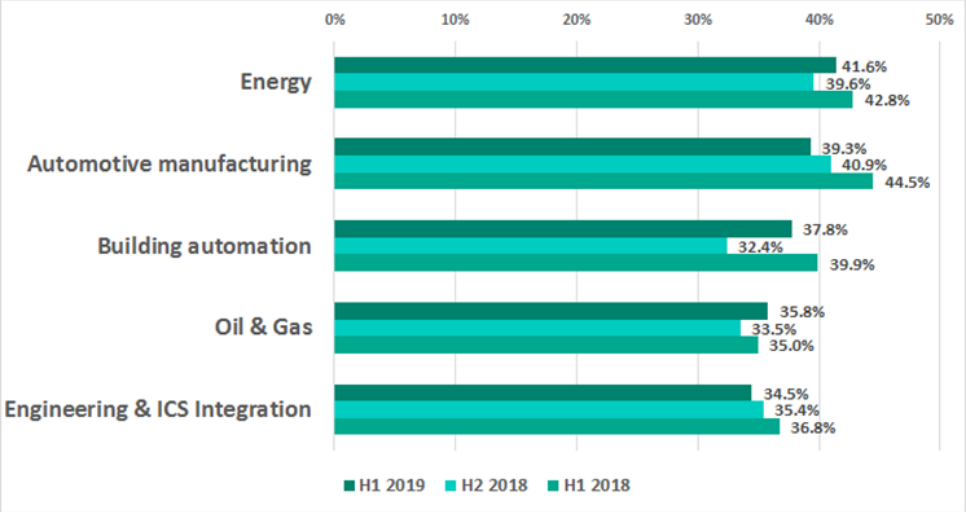
The highest percentages of ICS computers on which malicious objects were blocked were observed in January and March 2019.

Percentage of ICS computers on which malicious objects were blocked, by month, H1 2019 vs H1 2018



© KASPERSKY, 1997 – 2019

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



The variety of malware detected

In H1 2019, Kaspersky security solutions blocked over 20.8 thousand malware modifications from 3.3 thousand different families on industrial automation systems. This is 1.7 thousand modifications more than in H2 2018, when over 19.1 thousand malware modifications from 2.7 thousand different families were blocked.

Malicious object categories

Malicious objects blocked by Kaspersky products on ICS computers fall into many categories. A list of the main categories is provided below, together with the percentages of ICS computers on which malicious activity by objects in those categories was prevented.

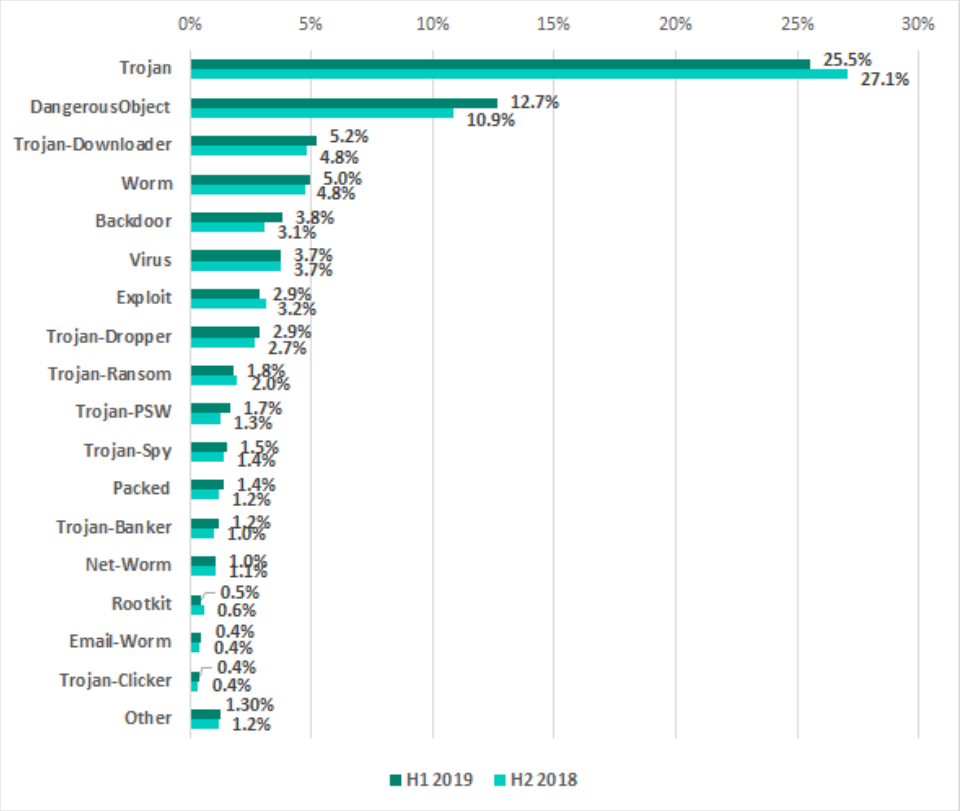
Results of automatic malicious object categorization

Below, we show the results of categorizing the malicious objects blocked based on verdicts returned by protection technologies in Kaspersky products. These are the verdicts as they are seen by users of our products.

Please note that the analysis of malware classes and families shown below reflects the results of signature-based and heuristic detection only, whereas many malicious objects are detected by Kaspersky products using behavioral methods and assigned the Generic verdict, which does not support automatically distinguishing between the actual types of malware. Therefore, the percentage of attacked ICS computers is in fact higher for some categories of malware.

© KASPERSKY, 1997 – 2019

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



Trojan malware remains relevant to ICS computers, although in the past years we have observed a decline in the percentage of ICS computers on which malware of this type was blocked. Compared with H2 2018, it has decreased by 1.52 p.p.

Compared with the previous six-month period, the percentage of ICS computers on which attempted backdoor (Backdoor) infections were prevented increased by 0.75 p.p.
The increase for spy Trojans (Trojan-PSW) was 0.41 p.p.

Results of detailed classification of the malicious objects blocked

To give a better idea of the types of threats that were blocked, we provided a more detailed classification, which required, among other things, a significant amount of manual analysis. It is important to note that the resulting percentages (as well as the figures in the diagram above) should not be added up, because in many cases threats of two or more types were blocked on the same computer during the reporting period.

As a result of our detailed analysis, we developed the following estimates of the percentages of ICS computers on which the activity of malicious objects from different categories was prevented:

- 11.8% – blacklisted internet resources.

  Web Antivirus protects a computer when programs installed on it (browsers, email clients, automatic updating components for application software, etc.) attempt to connect to blacklisted IP or URL addresses. Such resources are associated with the distribution or control of some malware.
  Specifically, blacklisted resources include, among others, those used to distribute such malware as Trojan-Spy or ransomware programs disguised as utilities for cracking or

© KASPERSKY, 1997 – 2019

resetting passwords on controllers of various manufacturers, or as cracks/patches for industrial and engineering software used on the industrial network.

- 8.5% – malicious scripts and redirects on web resources (JS and HTML), as well as browser exploits – 0.16%.
- 6.0% – 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, they include such specimens as Zombaque (0.02%) – which implements a P2P network architecture enabling attackers to activate it at any moment.
- 3.29% – web miners running in browsers.
  1.31% – miners in the form of executable files for Windows.
- 5.16% – 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.
- 2.82% – malicious documents (MSOffice + PDF) containing exploits, malicious macros or malicious links.
- 2.16% – 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.).
- 3.76% – Virus class malware.

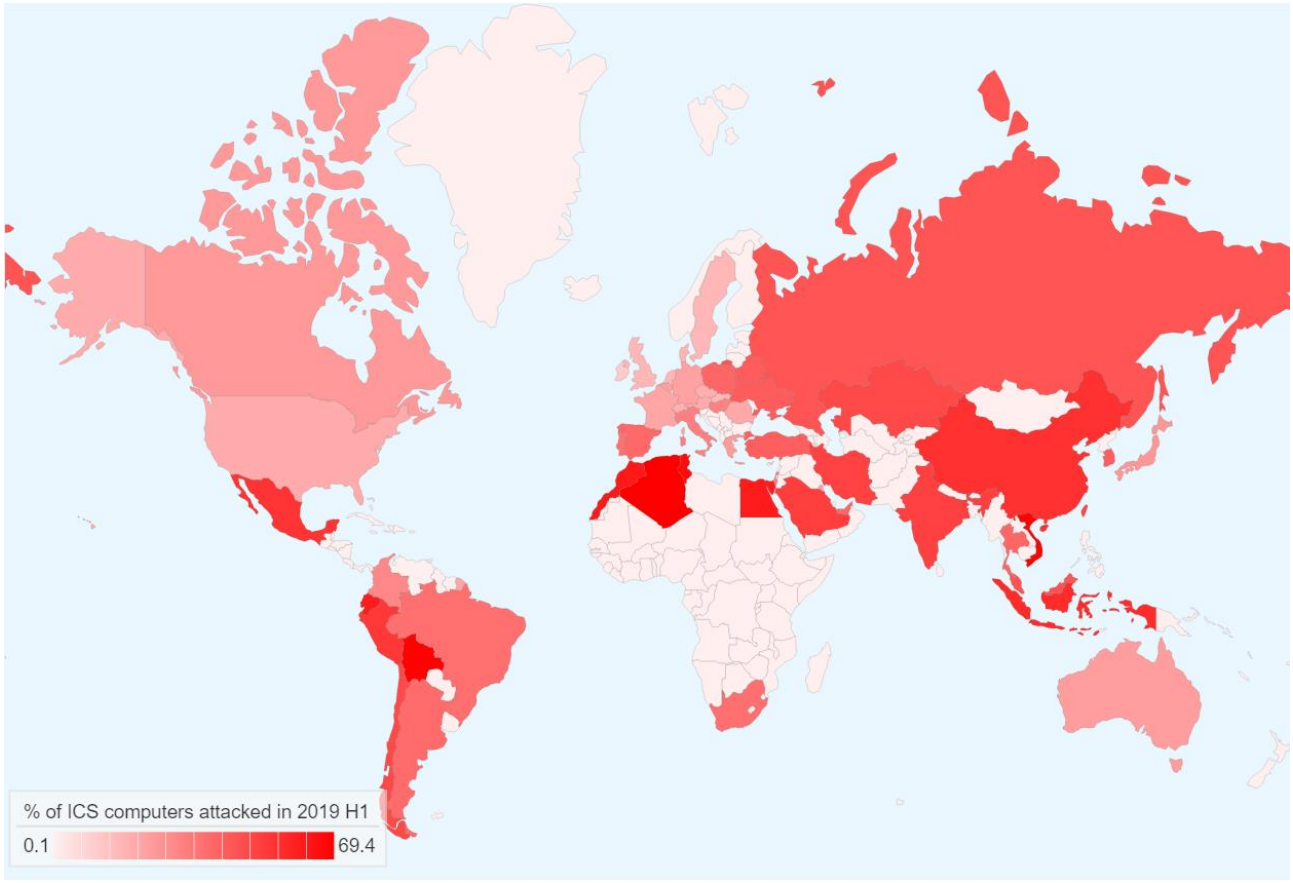
  These programs include such families as Sality (1.18%), Nimnul (0.77%), and Virut (0.54%), which have been detected for many years. Although these malicious families are considered obsolete because their command-and-control servers have long been inactive, they usually make a significant contribution to the statistics due to their self-propagation and insufficient measures taken to completely neutralize them.
- 1.81% – ransomware.
- 1.32% – banking Trojans.
- 0.88% – 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.
- 0.64% – malicious files for mobile devices that are blocked when a device is connected to a computer.

© KASPERSKY, 1997 – 2019

Geographical distribution

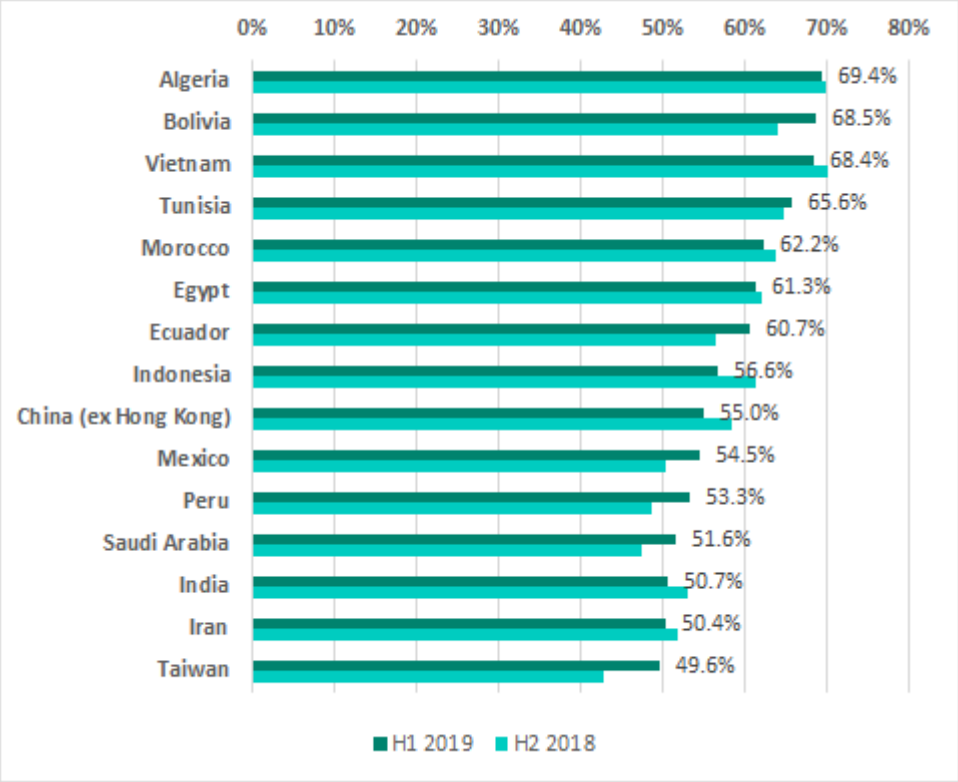
The map below shows the percentage of industrial automation systems on which malicious objects were blocked to the total number of such systems (by countries and territories).



Geographical distribution of attacks* on industrial automation systems, H1 2019
**** percentage of ICS computers on which malicious objects were blocked***

© KASPERSKY, 1997 – 2019

TOP 15 countries and territories by percentage of ICS computers on which malicious objects were blocked



In H1 2019, Algeria led the ranking of countries and territories based on the percentage of ICS computers on which malicious activity was prevented. The TOP 5 also included Bolivia, which climbed into second place, pushing Vietnam, Tunisia and Morocco down into third, fourth and fifth positions, respectively.

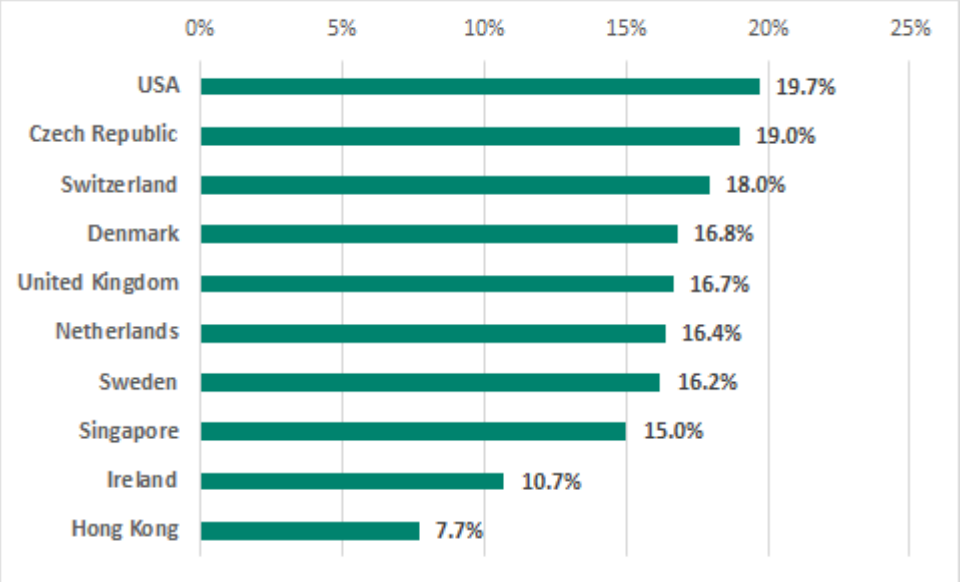
Noticeable increases in the percentages of ICS computers on which malicious activity was prevented were observed in Israel (an increase of 9.8 p.p.), Argentina (7.2 p.p.) and Taiwan (6.9 p.p.).

In Russia, malicious objects were blocked at least once during H1 2019 on 44.8% of ICS computers, which is slightly lower than the level observed in H2 2018 (45.3%). Russia ranks 19th based on this parameter.

The list of the ten most secure countries and territories has not changed significantly over the past several half-year periods.

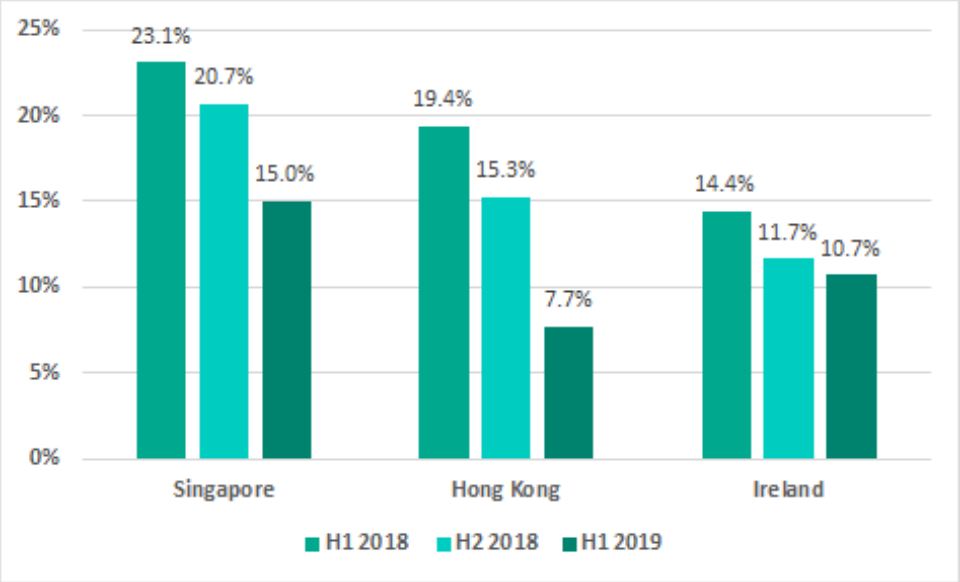
© KASPERSKY, 1997 – 2019

10 countries and territories with the lowest percentage of ICS computers on which malicious objects were blocked, H1 2019



The most secure countries and territories in the ranking are Hong Kong (7.7%), Ireland (10.7%), and Singapore (15%). Notably, the percentage of ICS computers on which malicious activity was prevented has been declining there for several six-month periods in a row.

Percentage of ICS computers on which malicious objects were blocked in Singapore, Hong Kong and Ireland

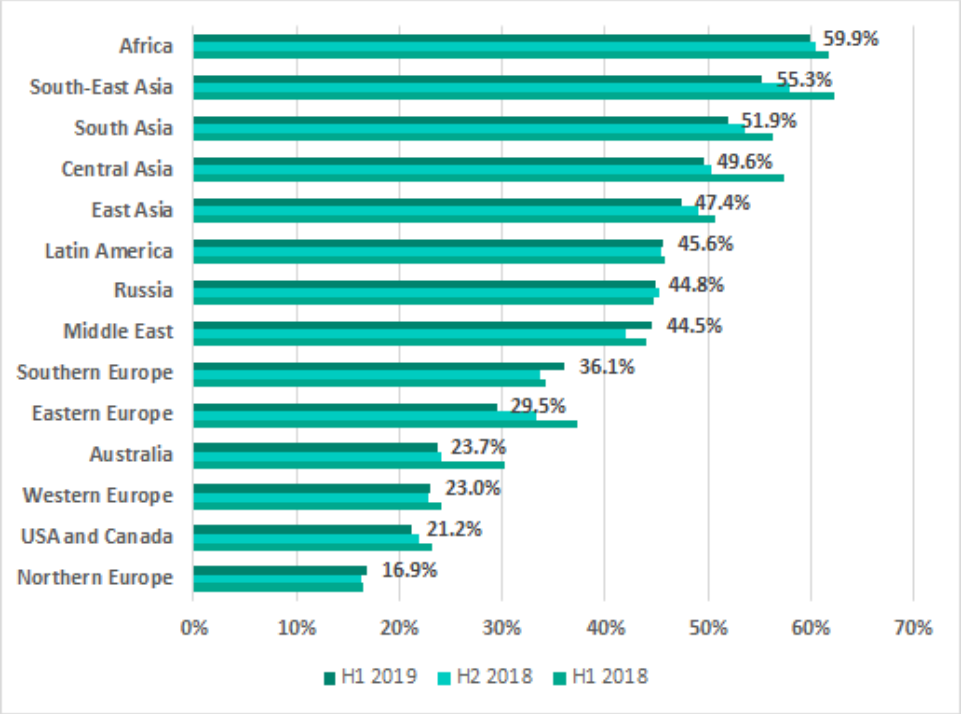


At the same time, we have been observing a gradual increase in this percentage in Denmark: it has grown from 14.0% to 16.8% since H1 2018.

The ranking of regions of the world based on the percentage of ICS machines on which malicious activity was prevented has not changed for several years. Africa, South-East Asia and South Asia have traditionally led the ranking.

© KASPERSKY, 1997 – 2019

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



Factors that affect the percentage of attacked computers in a country

As we discussed in one of our reports, we have identified a positive correlation between the percentage of attacked computers in a country and that country's GDP ranking, which, among other things, gives a rough idea of the amount of resources available to industrial organizations for various purposes, including protection from cyberattacks.

We believe that this may largely determine the extent to which industrial networks in each country are isolated from external threats. This can depend on many factors, such as:

- Effective measures and tools for the protection of the OT perimeter and the corporate network perimeter,
- Standards and practices of working with company-wide resources inside the OT segment, specifically restrictions and access control for internet and corporate email access,
- Measures and tools in place to restrict and control the use of remote connections by engineers, network administrators, integrators, and ICS system vendors,
- The extent to which the architecture and structure of the organization's information network is thought through,
- Measures, tools and practices used to update software and to control the use of unauthorized software,
- The awareness of personnel at industrial enterprises of threats related to cyberattacks and random infections, the level of cyber-hygiene demonstrated by employees,
- The extent to which enterprises are automated, the number of personnel and workplaces equipped with computers,
- The overall level of IT development in the country, whether enterprise employees have computers of their own and whether the internet is available to them outside the enterprise.

© KASPERSKY, 1997 – 2019

We have also determined (see above) that the activity of self-propagating malware (worms) in the ICS segment can be an important factor. In the specific cases that we identified, that activity was probably due to the high overall activity of worms in the country.

This observation brings up the question of the extent to which, in general, the level of malicious activity inside the ICS segment is connected with the 'background' malware activity in the country.

What color is the 'background'?

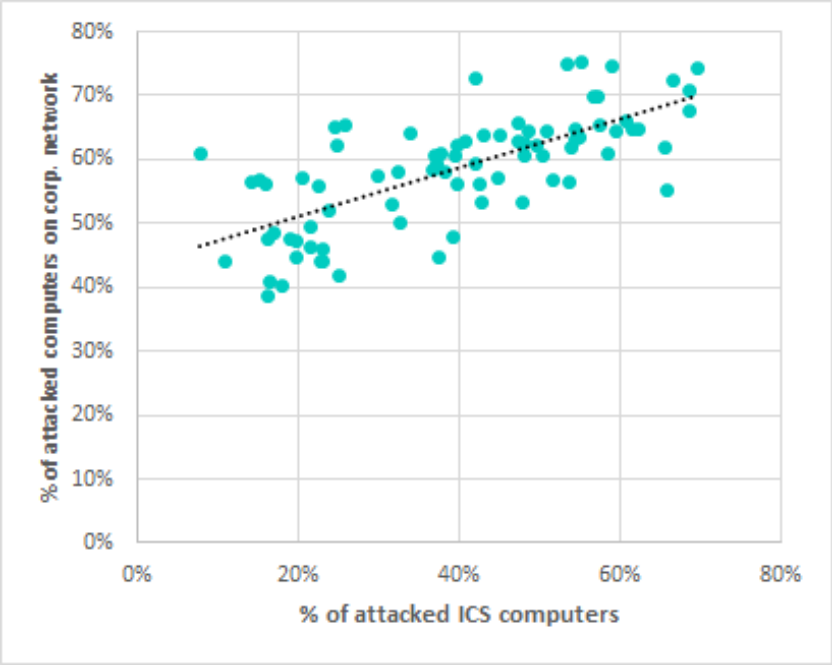
To find out what defines the malicious 'background' for ICS computers from our sample, we look at whether there is a correlation between the percentage of attacked ICS computers and the corresponding percentage for computers in the corporate environment as a whole, as well as that for computers of home users in each country.

To draw the line between the 'corporate environment' and the 'rest of the IT space' in a country, we can take advantage of the fact that the conditions on which corporate products are purchased and used are very rarely suitable for individuals. The opposite is also true: buying products designed for home users makes no economic sense for organizations.

This means that two samples offering a good insight into the relevant figures can be built – one demonstrating statistics received from Kaspersky corporate products installed in the country, the other – statistics received from products for home users.

The diagram below demonstrates the correlation between statistics for ICS computers and those for computers in the corporate segment.

Correlation* between percentages of computers on which malicious objects were blocked in the ICS segment and on the corporate network, in a country-by-country comparison



** correlation parameters: R>.70, p<.001*

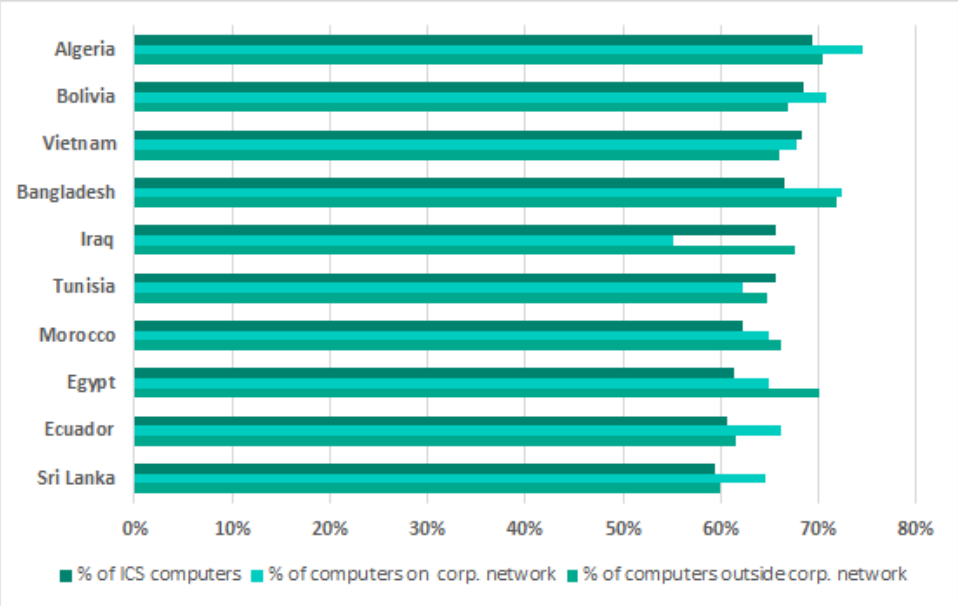
As it turns out, there definitely is a correlation between the figures for the corporate environment and the ICS environment and it is sufficiently high (R>.70).

It should be noted that all three indicators, i.e., the percentages of computers on which malicious objects were blocked in the ICS environment, in the corporate environment and

© KASPERSKY, 1997 – 2019

computers outside it – are more closely matched where the percentages of attacked computers are high.

Comparison of the highest percentages* of computers on which malware was blocked in the ICS environment with similar figures for computers in the corporate environment and computers outside it



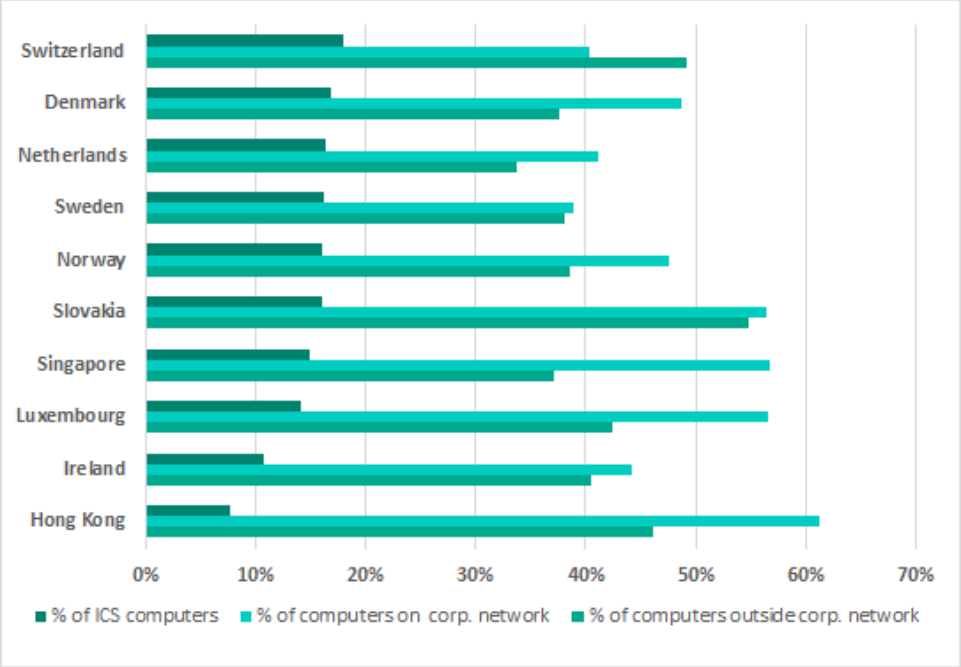
**** TOP 10 countries by percentage of ICS computers on which malicious objects were blocked , H1 2019***

Specifically, in countries which rank highest in the above ranking, the percentage of attacked ICS computers is close to that of attacked computers in the corporate environment. To a large extent, the reason for this situation is that a broad variety of malware with self-propagating functionality, which spreads primarily via USB, is detected both on ICS computers and on corporate computers in these countries. Another factor is that the activity of cryptocurrency miners, which spread over the local network by exploiting vulnerabilities, is blocked both on ICS and corporate computers.

Another noteworthy fact is that in countries and territories with low percentages of ICS computers on which malware was blocked, these percentages are significantly lower than those for computers that are not part of industrial control systems.

© KASPERSKY, 1997 – 2019

Comparison of the lowest percentages* of computers on which malware was blocked in the ICS environment with similar figures for computers in the corporate environment and computers outside it

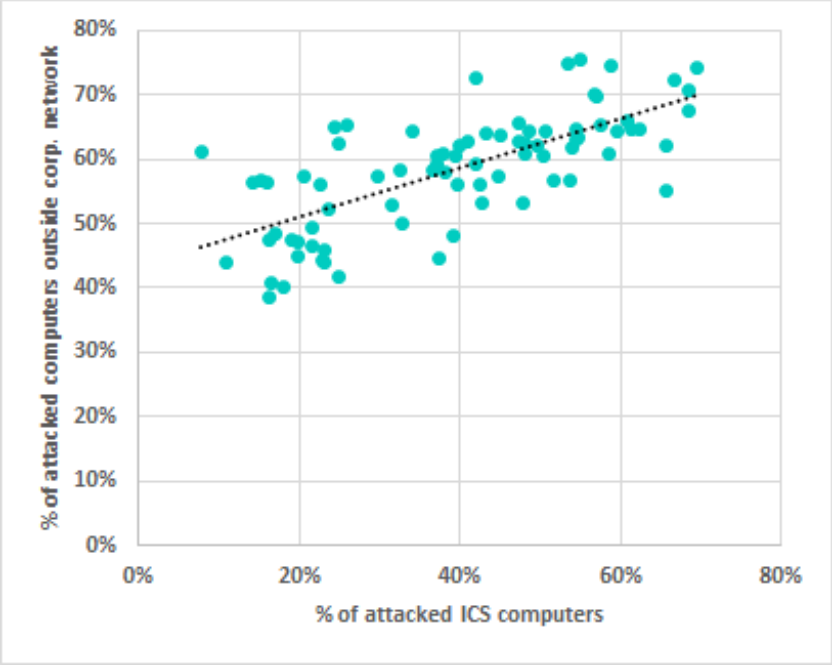


** 10 countries and territories with the lowest percentages of ICS computers on which malicious objects were blocked*

This could indicate that, on average, in countries and territories where the situation with the security of the ICS segment is favorable, the low percentages of attacked ICS computers are attributable to the protection measures and tools used rather than a generally low background level of malicious activity.

At first glance, the results of our analysis of the correlation between the percentages for ICS and home user computers could seem somewhat unexpected.

Correlation* between percentages of computers on which malicious objects were blocked in the ICS environment and outside the corporate network, in a country-by-country comparison



** correlation parameters: R>.80, p<.001*

© KASPERSKY, 1997 – 2019

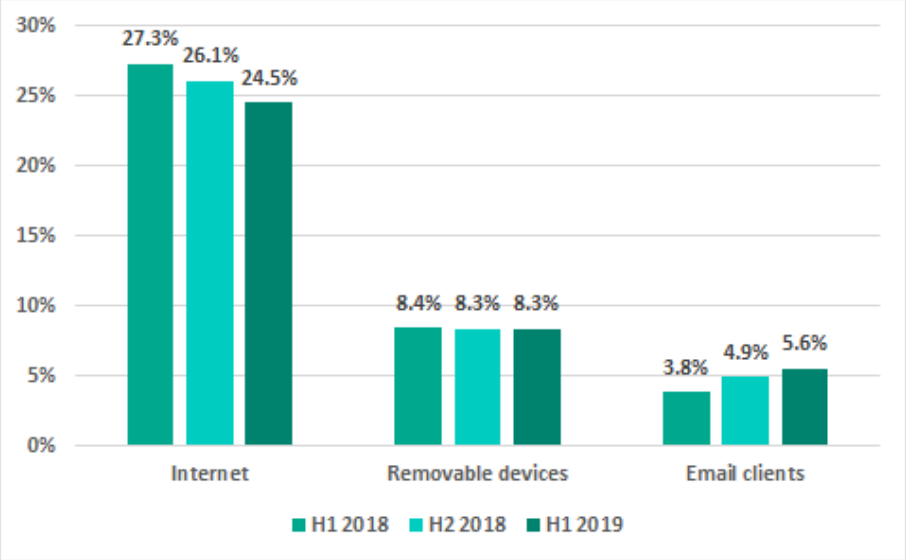
The part that can seem unexpected is that this correlation is greater than the correlation with the percentages for computers in the corporate environment (R>.80 vs R>.70, with p<.001).

However, this finding is in line with our 'field' observations made while providing our customers with services related to ensuring the security of their industrial facilities (training, audits, penetration tests, incident investigations and targeted attack analysis). In light of the expertise accumulated on these projects, this correlation identified 'on paper' could mean in practice that, on average, ICS computers do not operate entirely inside a security perimeter typical of corporate environments, and are, to a large extent, protected from many threats, which are also relevant to home users, using their own measures and tools. In other words, tasks related to protecting the corporate segment and the ICS segment are to some extent unrelated.

Threat sources

In the past 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*



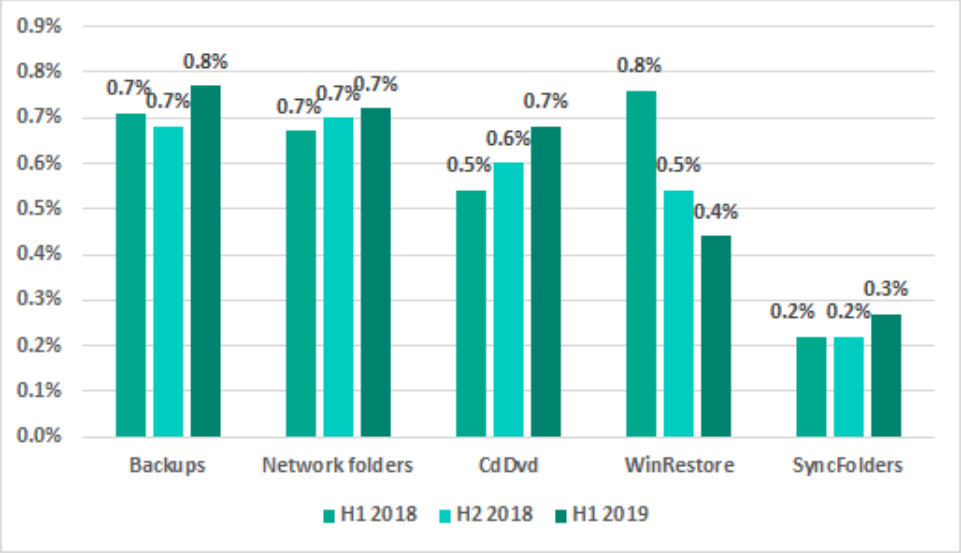
** percentage of ICS computers on which malicious objects from different sources were blocked*

Since 2018, we have observed a downward trend for the percentage of ICS computers on which malicious objects from the internet were blocked. In H1 2019, the internet was the source of threats blocked on 24.5% of ICS computers. Compared with H2 2018, this percentage has decreased by 1.6 p.p. At the same time, we observed an increase (by 0.7 p.p.) in the percentage of ICS computers on which malicious email attachments were blocked.

Other figures for the main threat sources remained roughly at the previous six months' levels.

© KASPERSKY, 1997 – 2019

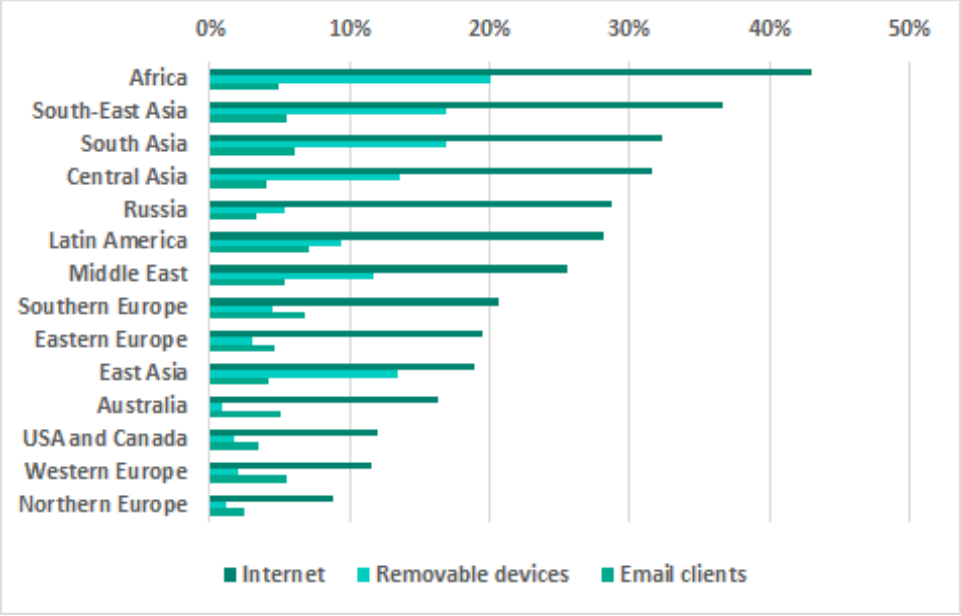
Minority sources of threats blocked on ICS computers (percentage of attacked ICS computers)



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

Main sources of threats: geographical distribution

Main sources of threats blocked on ICS computers* by region



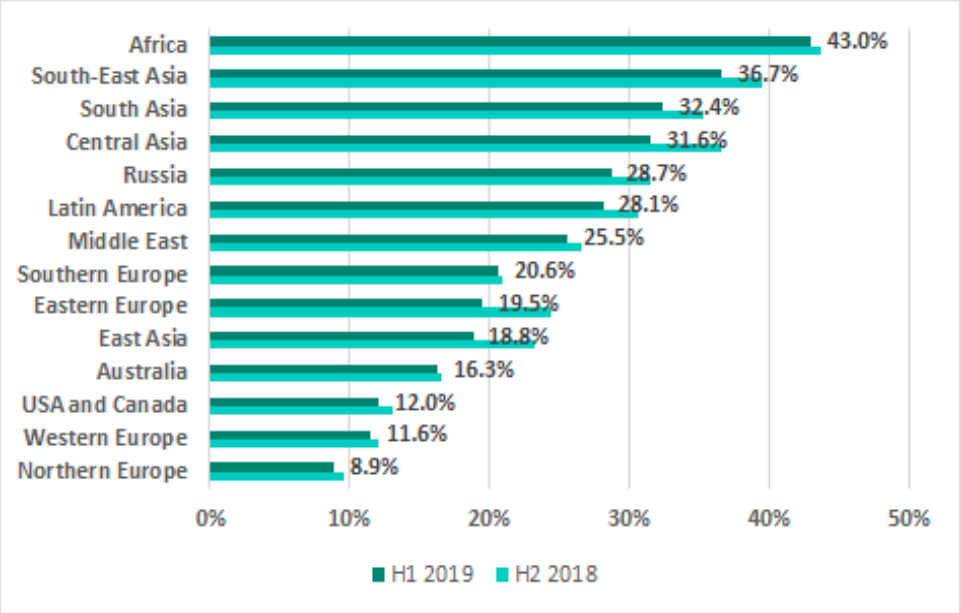
* *percentage of attacked ICS computers*

© KASPERSKY, 1997 – 2019

Internet

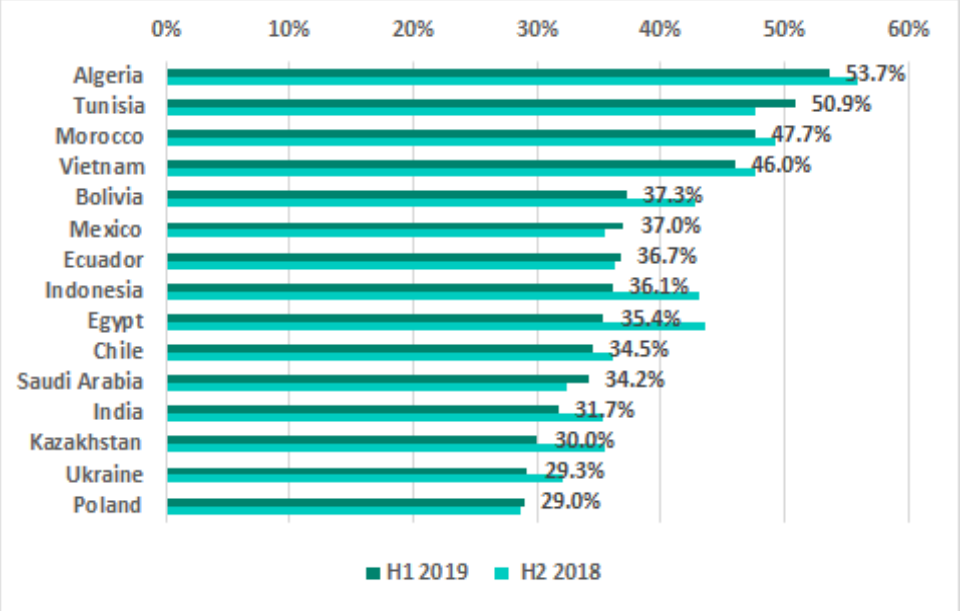
The internet is the main source of threats in all regions of the world. However, the percentage of ICS computers on which internet threats were blocked is much lower in Northern and Western Europe and in North America than in other regions.

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



The list of TOP 15 countries by percentage of ICS computers on which internet threats were blocked has largely remained unchanged. “Newcomers” to this ranking in H1 2019 were Bolivia and Poland.

TOP 15 countries by percentage of ICS computers on which internet threats were blocked

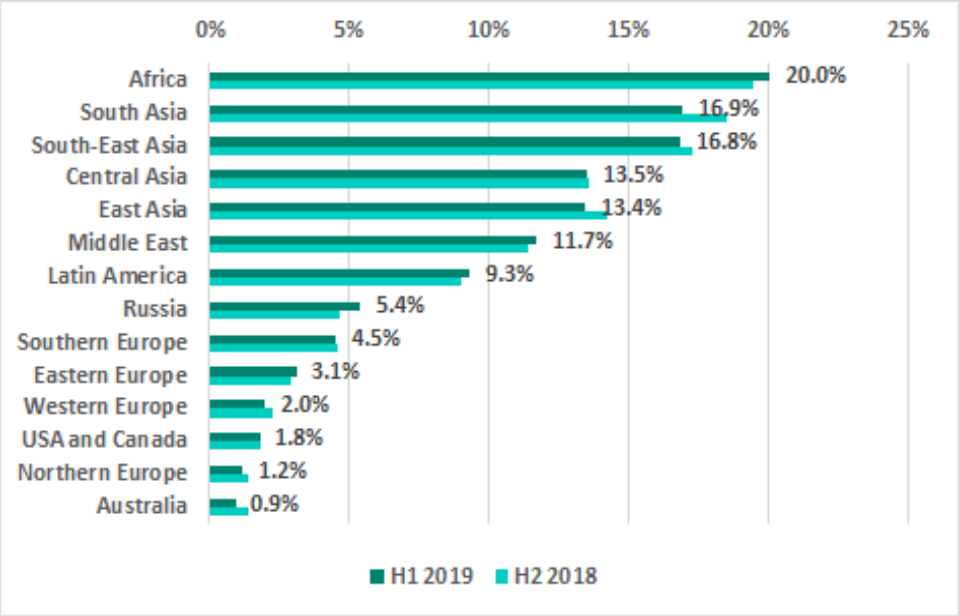


© KASPERSKY, 1997 – 2019

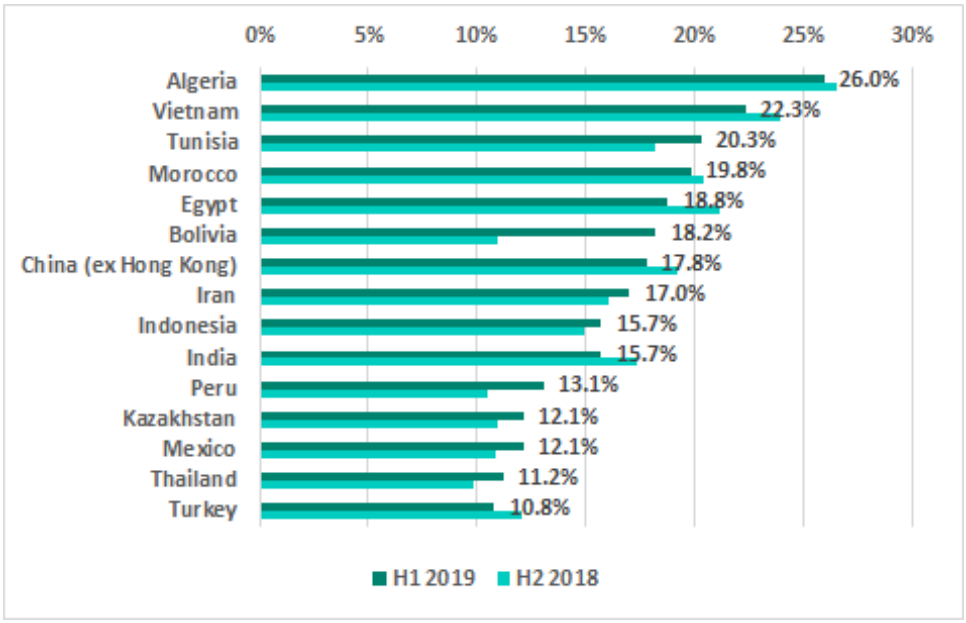
Removable media

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



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

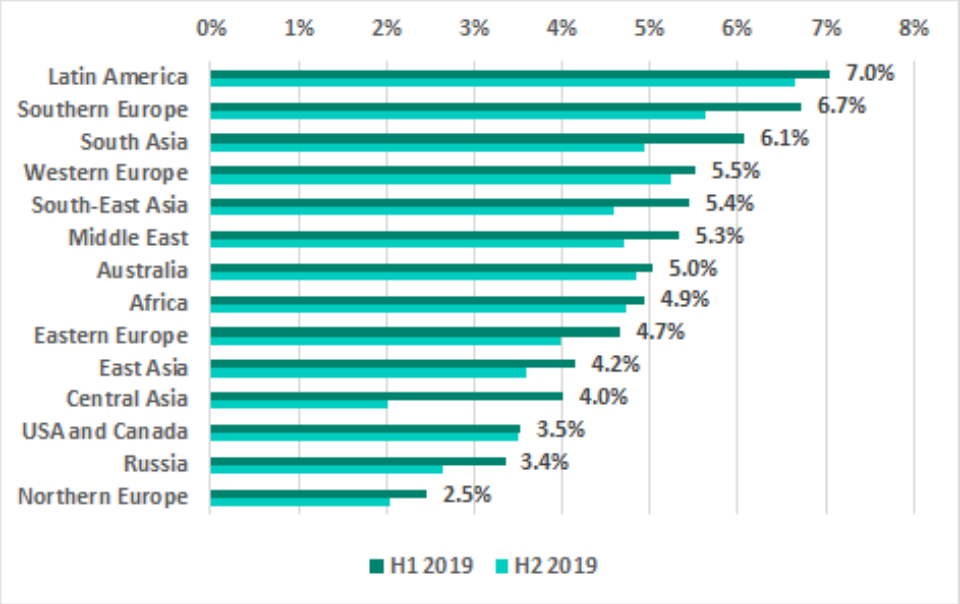


© KASPERSKY, 1997 – 2019

Email clients

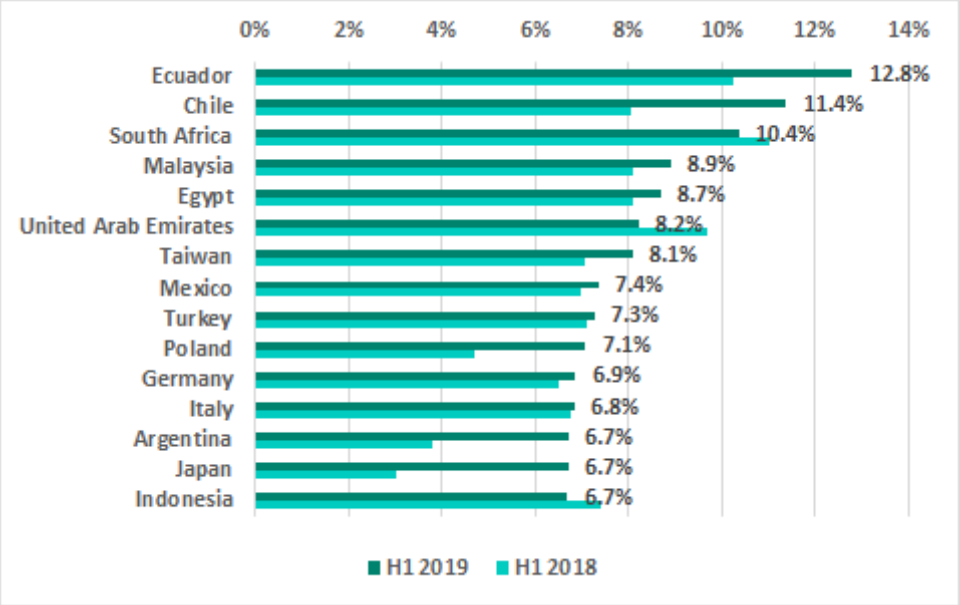
In the ranking of regions based on the percentage of ICS computers on which malicious email attachments were blocked, there are no major differences between regions. The ranking is led by Latin America, with high percentages also observed in Southern Europe and South Asia.

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



In H1 2019, Japan, Argentina and Poland displaced Korea, Brazil and Peru in the ranking of TOP 15 countries and territories based on the percentage of ICS computers on which malicious email attachments were blocked.

TOP 15 countries and territories by percentage of ICS computers on which malicioius email attachments were blocked



© KASPERSKY, 1997 – 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

Authorized to Use CERT™
CERT is a mark owned by
Carnegie Mellon University

© KASPERSKY, 1997 – 2019