kaspersky

Threat landscape for industrial automation systems

H1 2020

Kaspersky ICS CERT

24.09.2020 Version 1.0

Contents

H1 2020 Report at a glance

Overall downward trend for percentages of attacked computers globally

Beginning in H2 2019 we have observed a tendency for decreases in the percentages of attacked computers, both in the ICS and in the corporate and personal environments.

1. In H1 2020 the percentage of ICS computers on which malicious objects were blocked has decreased by 6.6 percentage points to 32.6%.
2. The number was highest in Algeria (58.1%), and lowest in Switzerland (12.7%).
3. Despite the overall tendency for the percentages of attacked computers to decrease, we did see the number grow in the Oil & Gas sector by 1.6 p.p. to 37.8% and by 1.9 p.p. to 39.9 % for computers used in building automation systems. These numbers are higher than the percentages around the world overall.

Variety of malware

Threats are becoming more targeted and more focused, and as a result, more varied and complex.

4. Kaspersky solutions in ICS environments blocked over 19.7 thousand malware modifications from 4,119 different families.
5. We are seeing noticeably more families of backdoors, spyware, Win32 exploits and malware built on the .Net platform.
6. Ransomware was blocked on 0.63% of ICS computers. This is very similar to the total of 0.61% in H2 2019.

Main threat sources

The internet, removable media and email continue to be the main sources of threats in the ICS environment. Predictably, the percentages in the rankings for these threats have decreased.

7. Internet threats were blocked on 16.7% of ICS computers (-6.4 p.p.).
8. Threats penetrating when removable media are connected were blocked on 5.8% of computers (-1.9 p.p.).
9. Malicious email attachments were blocked on 3.4% of ICS computers (-1.1 p.p.).

Regional differences

Asia and Africa were **the least secure**.

10. Asian regions occupy 4 out of the TOP 5 positions in the regional rankings based on the percentage of ICS computers which were attacked. Africa comes second.
11. Southeast Asia is the worst hit - it leads in several ratings:
    - Percentage of ICS computers where malicious activity was blocked – 49.8%.
    - percentage of ICS computers where internet threats were blocked – 14.9%.
    - Percentage of ICS computers where malicious email attachments were blocked - 5.8%.
12. Africa leads in the ranking of regions by percentage of ICS computers where malicious activity was blocked when removable media were connected with (14.9%).

The situation is best in Australia, Europe, USA and Canada, which are in at the bottom in all of the rankings except by malicious email attachments.

13. Northern Europe is the most secure region with the lowest positions in rankings in H1 2020:
    - by percentage of ICS computers attacked – 10.1%,
    - by percentage of ICS computers on which internet threats were blocked – 4.6%,
    - By percentage of ICS computers where malicious email attachments were blocked (1.1%).
14. The lowest percentage of ICS computers on which threats were blocked when removable media were connected was in Australia – 0.8%. Northern Europe came in with a close second of 0.9%.
15. In Australia, Europe, USA and Canada the percentages in the rankings by malicious email attachments were higher than by threats on removable media with Eastern Europe as the exception – 3.5% and 3.7% respectively.

Southern and Eastern Europe were **the least secure regions in Europe**.

16. Southern and Eastern Europe were in the TOP 5 of the rankings by percentages of ICS computers where malicious email attachments were blocked. Southern Europe came in second with 5.2% and Eastern Europe fifth with 3.5%.
17. Eastern Europe was the only region in the world where we saw an increase of 0.9 p.p. in the percentage of computers where threats were blocked when removable media were connected, coming in with 3.7%.

Key events of H1 2020

Attack on steel maker BlueScope

On May 15, steel maker BlueScope reported an attack which caused disruptions to some of the company's enterprises.

The cybersecurity incident was detected in one of the company's US businesses. In addition to enterprises in the US, the attack had a slight effect on the company's businesses in Asia and New Zealand. The greatest impact was on manufacturing and sales operations in Australia: some processes were paused and others, including steel dispatches, continued mostly without using automation tools.

No other details of the attack have been disclosed so far.

APT attacks on industrial companies

WildPressure targeted campaign

In March 2020, Kaspersky experts discovered a previously unknown APT campaign distributing a Trojan that was dubbed Milum. According to research results, the malware had been used at least since early 2019 exclusively for attacks on targets in the Middle East, which included industrial organizations. The campaign was named WildPressure.

Milum has the capability to control devices remotely. It can download and execute commands sent by its operator, collect a variety of information from the target device and send it to its C&C server. For their campaign infrastructure, the operators used rented OVH and Netzbetrieb virtual private servers (VPS) and a domain registered with the Domains by Proxy anonymization service.

A code analysis of the new malware did not show any notable overlaps or similarities with any previously known APT campaign.

Malicious campaigns against government and industrial organizations of Azerbaijan

In April 2020, a report was published on targeted attacks that involved a previously unknown remote-access Trojan (RAT), which was dubbed PoetRAT.

According to the researchers, the attacks targeted Azerbaijan's government sector, transportation and industrial companies, primarily those in the energy sector. The investigation established that the attackers were particularly interested in SCADA systems connected with wind turbines.

Cisco Talos experts have tracked these attacks since February 2020. Kaspersky experts identified them in December 2019, reporting them in a private report. The attackers used a malicious document containing an image that looked like the logo of the Defense R&D Organization of the Indian ministry of defense. Two more attack waves followed in April, one of which used what looked like the Azerbaijani government's documents on COVID-19 as decoys. In the other case, the attackers used a file named "C19.docx" with no readable content, possibly also a reference to COVID-19.

Microsoft Word documents were used as droppers that installed the Trojan without the user's knowledge. After a document was opened, a macro (Visual Basic script) or code using DDE (Dynamic Data Exchange) was run, extracting the malware and executing it.

The first–stage PoetRAT malware is written in Python. Numerous additional tools, most also written in Python, were found on victims' computers. Malware written in Python has been used in attacks on industrial companies before – such as in the case of the Triton attack.

Another finding made in the course of the investigation was a phishing website imitating the webmail of the Government of Azerbaijan and designed to steal user credentials.

Targeted attacks on Israeli water supply and wastewater treatment facilities

On April 23, the Israel National Cyber Directorate (INCD) issued a security advisory, which reported attempted attacks on SCADA systems of water treatment plants, water pumping stations and sewage networks. It was recommended that water and power supply utilities urgently change passwords for all systems connecting to the internet as an intrusion prevention measure. The importance of implementing these measures for systems used to manage the amount of chlorine added to water was particularly emphasized. Other recommendations included updating the software and equipment firmware used.

Similar warnings were also published by Israel's Computer Emergency Response Team (CERT) and by the Israeli government's Water Authority.

There were no official reports of confirmed intrusion into any Israeli water treatment or water supply company, but according to mass media, attacks took place on Friday and Saturday (April 24 and 25) and affected a number of organizations in different parts of the country.

Ransomware attacks on industrial companies

The wave of ransomware attacks that hit the world in 2019 continued through the first six months of 2020.

Ransomware attack paralyzes production at Picanol plants in Belgium, Romania and China

On January 13, 2020 Picanol Group, a large manufacturer of high-tech weaving machines, fell victim to a massive ransomware attack. The attack seriously disrupted the operations of the company's manufacturing plants in Belgium, Romania and China. No information has been released on the ransomware used in the attack.

The attack was discovered during the night, when Picanol employees in China were unable to access the company's IT systems. Similar issues also arose in Ypres in Belgium. The company's operations were nearly completely paralyzed. Picanol's 2300 employees were out of work for over a week.

Ryuk attacks on medical organizations

In H1 2020, Ryuk operators perpetrated massive attacks on hospitals, demanding ransom to decrypt the files. In March alone, 10 hospitals fell victim to Ryuk attacks in the US.

The attacks were based on the already familiar Ryuk infection scheme involving phishing emails and TrickBot malware, which enables the attackers to connect to an infected computer and explore the network of the organization under attack. TrickBot operators try to find vulnerable systems and to steal user credentials.

Ransomware attacks on pumping solution manufacturer DESMI

On the night of April 7-8, DESMI, a Danish manufacturer of pumping solutions for marine and industrial applications, suffered a ransomware attack. No information is available on the malware used in the attack.

According to an official statement, the attack affected the company's communication systems, including email, which had to be temporarily disconnected. The company was able to recover these systems by April 14. The ERP and financial systems were not affected, enabling the company's manufacturing sites in China, India, America and Denmark to continue working as normal, with only minor disturbances.

Ragnar Locker attack on energy company EDP

On April 13, Energias de Portugal (EDP), a large Portuguese energy company, suffered a ransomware attack. As a result of the attack, which involved the Ragnar Locker malware, the company's systems were encrypted. Moreover, the cybercriminals claimed to have stolen 10 TB of sensitive company files before encrypting the data. They threatened to make that information public unless they were paid a ransom of 1580 BTC (about $10.9 million).

To prove that they really held sensitive information belonging to EDP, Ragnar Locker operators published some of the stolen data, including employee account names and passwords.

According to the ransom note, the attackers had also gained access to confidential information on the company's billing, contracts, transactions, clients and partners.

After analyzing different samples of the ransomware, Kaspersky experts concluded that the entire text of the ransom note is created specifically for each individual victim, which means that Ragnar Locker attacks are targeted in nature.

Attack on Stadler industrial facilities

On May 7, 2020 Stadler, a Swiss manufacturer of railway rolling stock, reported a cyberattack on its industrial facilities. According to the company's statement, some computers on their corporate network were infected with malware and data was stolen from the compromised machines. The threat actors behind the attack contacted company personnel, demanded a ransom and threatened to publish the stolen data if the victim refused to pay up.

Stadler turned to the appropriate government agencies and hired external IT security experts to assist with incident investigation. Backup copies were used to restore the affected systems and operational processes were not affected by the attack.

The company did not reveal which malware was used in the attack. However, since a ransom was demanded and systems needed to be restored from backups, it is highly likely that Stadler was the victim of a ransomware attack.

Mailto and Nefilim attacks on logistics company Toll Group

In the first half of 2010, Toll Group, an Australian logistics company, was attacked by ransomware on two occasions.

The first attack took place in late January. A variant of Mailto ransomware was used. To prevent the malware from spreading, the company disabled some of its information systems, resulting in delayed shipments to both corporate and individual customers. Australia's national postal service, Australia Post, was among the Toll Group customers whose shipments were delayed.

Toll Group experienced the second attack in May, when one of the company's corporate systems was infected with Nefilim ransomware. Data stored on the affected system included information on the company's employees, as well as some agreements with corporate customers. Before encrypting files, the attackers stole about 200 gigabytes of data and demanded a ransom to unblock the IT systems. However, the management of Toll Group refused to make a deal with them. In response to the incident, all of the company's IT systems were shut down.

On May 20, it became known that Nefilim operators had published part of the stolen data.

By May 29, Toll Group had restored all of its information systems and logistics operations.

Attack of Sodinokibi encryption malware on energy companies

On May 14, 2020, Elexon, a major British electric utility company, reported a malware infection of their IT network. Only systems on the internal IT network suffered as a result of the attack, including the email system and laptops. Key IT services and electricity supply systems were not impacted.

In June, it was reported that the company had been attacked with the Sodinokibi encryption ransomware, also known as REvil.

Later, the Brazilian electric power utility Light S.A. became another victim of Sodinokibi. According to mass media, the company was attacked by the ransomware in late June. The operators of the ransomware demanded a ransom in Monero cryptocurrency amounting to about $7 mln. After June 19, the ransom doubled to about $14 million.

The attack did not have a negative impact on power supply but it disrupted the company's billing-related business processes. Although it was officially confirmed that the attack had taken place, no other details of the incident were disclosed.

Later, researchers found a sample of Sodinokibi malware, which is likely to have been used in the attack on Light S.A. The malware is distributed using the Ransomware-as-a-Service, (RaaS) model and is likely to be associated with the Pinchy Spider criminal group, which was behind the GandCrab ransomware.

Attack on beverage manufacturer Lion

On June 9, Australian beverage manufacturer Lion fell victim to a ransomware attack. The company had to shut down infected IT systems, resulting in the suspension of some industrial processes and impacting product shipments to customers. Specifically, the company paused production at its breweries in Australia and New Zealand. The attack also affected the operation of Lion Dairy & Drinks production sites responsible for making a variety of dairy products.

No information has been published on the ransomware used in the attack on Lion.

On June 18, Lion suffered another ransomware attack. According to mass media, Sodinokibi (REvil) malware was used in the second attack. The attackers demanded a ransom of 12234.28 XMR (about $800,000) and threatened to publish sensitive data stolen from the company. They also threatened to double their ransom demands if the money was not paid by June 19.

According to the latest information on the company's official website, by June 26 all of the company's production sites had been restored to normal operation but the work to recover their IT systems had not been completed.

Targeted attacks on industrial companies involving Snake ransomware

On June 8, 2020 issues were reported which affected the computer networks of Honda, a Japanese motorcycle and auto manufacturer, in Europe and Japan. Specifically, it was announced that Honda Customer Service and Honda Financial Services were experiencing technical difficulties.

Information security experts believe that, in all likelihood, one of the company's servers was infected with Snake (EKANS) ransomware: a sample of the Snake malware was discovered on VirusTotal, which checks for Honda's domain name, "mds.honda.com" (which is probably used on the company's internal network). If the domain name cannot be resolved (i.e., if the corresponding IP address cannot be determined), the ransomware terminates without encrypting any files. According to the researchers, this could indicate that the attackers' activity is targeted in nature.

Kaspersky ICS CERT experts used their own telemetry data to identify other samples that were similar to the sample uploaded to VirusTotal.

The results of our research clearly indicate that the attackers carry out multistage hacker attacks, each attack targeting a specific organization. Encrypting files using Snake is the final stage of these attacks. The Snake ransomware is written in Golang programming language, which is not very widely used and is found today primarily in malware samples used by APT groups.

It is known that, in addition to Honda, victims include power company Enel Group. According to Kaspersky ICS CERT data, attack targets also include a German company that supplies its products to auto makers and other industrial manufacturers and a German manufacturer of medical equipment and supplies. Apparently, other auto makers and manufacturing companies have also been attacked: similar Snake samples have been detected on computers in China, Japan and Europe.

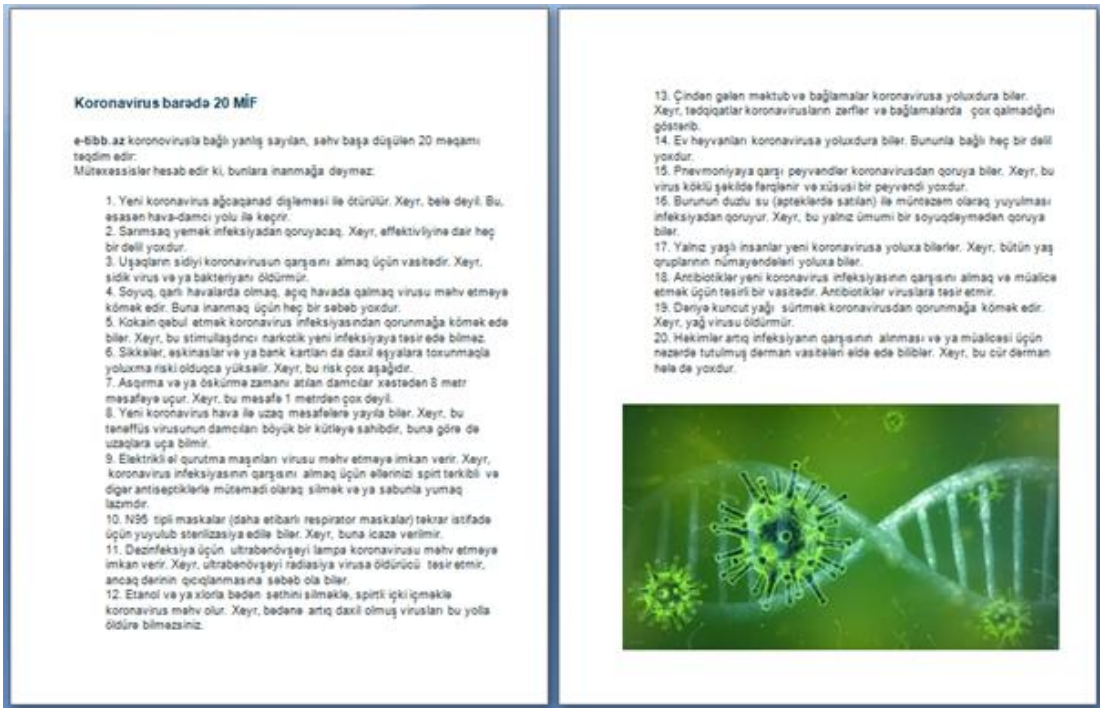
Impact of COVID-19 pandemic

In the course of our research, we couldn't ignore the widely discussed issue of the impact that the COVID-19 pandemic had on the threat landscape for industrial organizations as a whole and their OT networks in particular.

It was only to be expected that threat actors would use the pandemic and the global changes caused by it in their own interests. As numerous sources have reported on many occasions, the subject of the COVID-19 pandemic is exploited in a large number of phishing attacks, both mass-scale and targeted.

In one of our private reports available by subscription, we described an APT attack that targets Azerbaijani enterprises and institutions and makes use of COVID-related documents.

One of the malicious documents exploiting the subject of COVID-19 which were used in an APT attack



Koronavirus barədə 20 MİF

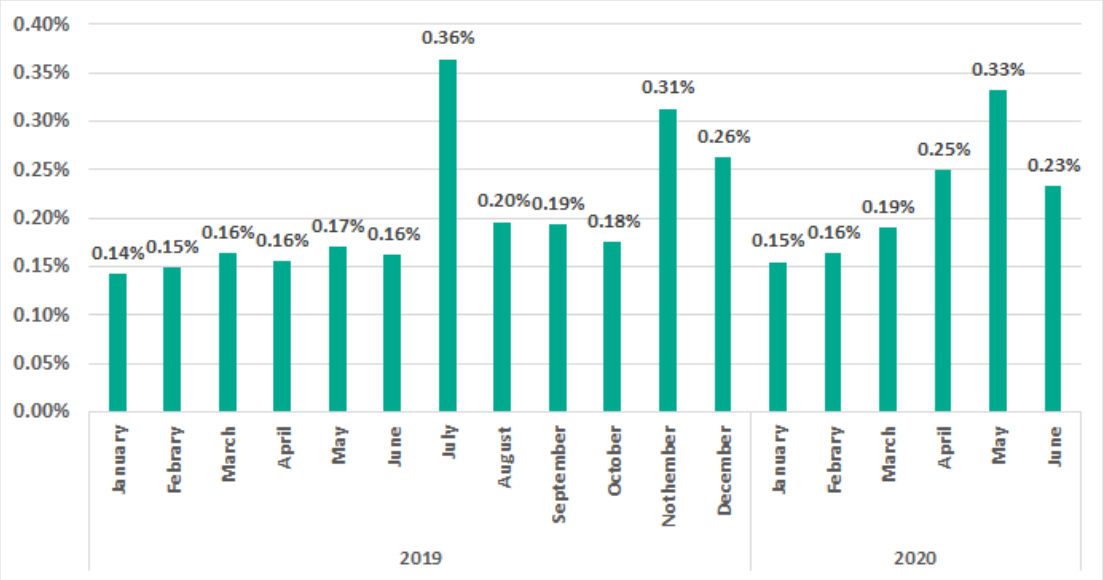
e-tibb.az koronovirusla bağlı yanlış sayılan, səhv başa düşülən 20 məqamı təqdim edir:
Mütəxəssislər hesab edir ki, bunlara inanmağa dəyməz:

1. Yeni koronavirus ağcaqanad dişləməsi ilə ötürülür. Xeyr, belə deyil. Bu, əsasən hava-damcı yolu ilə keçir.
2. Sarımsaq yemək infeksiyadan qoruyacaq. Xeyr, effektivliyinə dair heç bir dəlil yoxdur.
3. Uşaqların sidiyi koronavirusun qarşısını almaq üçün vasitədir. Xeyr, sidik virus və ya bakteriyanı öldürmür.
4. Soyuq, qarlı havalarda olmaq, açıq havada qalmaq virusu məhv etməyə kömək edir. Buna inanmaq üçün heç bir səbəb yoxdur.
5. Kokain qəbul etmək koronavirus infeksiyasından qorunmağa kömək edə bilər. Xeyr, bu stimullaşdırıcı narkotik yeni infeksiyaya təsir edə bilməz.
6. Sikkələr, əskinaslar və ya bank kartları da daxil əşyalara toxunmaqla yoluxma riski olduqca yüksəlir. Xeyr, bu risk çox aşağıdır.
7. Asqırma və ya öskürmə zamanı atılan damcılar xəstədən 8 metr məsafəyə uçur. Xeyr, bu məsafə 1 metrdən çox deyil.
8. Yeni koronavirus hava ilə uzaq məsafələrə yayıla bilər. Xeyr, bu tənəffüs virusunun damcıları böyük bir kütləyə sahibdir, buna görə də uzaqlara uça bilmir.
9. Elektrikli əl qurutma maşınları virusu məhv etməyə imkan verir. Xeyr, koronavirus infeksiyasının qarşısını almaq üçün əllərinizi spirt tərkibli və digər antiseptiklərlə mütəmadi olaraq silmək və ya sabunla yumaq lazımdır.
10. N95 tipli maskalar (daha etibarlı respirator maskaları) təkrar istifadə üçün yuyulub sterilizasiya edilə bilər. Xeyr, buna icazə verilmir.
11. Dezinfeksiya üçün ultrabənövşəyi lampa koronavirusu məhv etməyə imkan verir. Xeyr, ultrabənövşəyi radiasiya virusa öldürücü təsir etmir, ancaq dərinin qıcıqlanmasına səbəb ola bilər.
12. Etanol və ya xlorla bədən səthini silməklə, spirtli içki içməklə koronavirus məhv olur. Xeyr, bədənə artıq daxil olmuş virusları bu yolla öldürə bilməzsiniz.
13. Çindən gələn məktub və bağlamalar koronavirusa yoluxdura bilər. Xeyr, tədqiqatlar koronavirusların zərflər və bağlamalarda çox qalmadığını göstərib.
14. Ev heyvanları koronavirusa yoluxdura bilər. Bununla bağlı heç bir dəlil yoxdur.
15. Pnevmoniyaya qarşı peyvəndlər koronavirusdan qoruya bilər. Xeyr, bu virus köklü şəkildə fərqlənir və xüsusi bir peyvəndi yoxdur.
16. Burunun duzlu su (aptəklərdə satılan) ilə müntəzəm olaraq yuyulması infeksiyadan qoruyur. Xeyr, bu yalnız ümumi bir soyuqdəymədən qoruya bilər.
17. Yalnız yaşlı insanlar yeni koronavirusa yoluxa bilərlər. Xeyr, bütün yaş qruplarının nümayəndələri yoluxa bilər.
18. Antibiotiklər yeni koronavirus infeksiyasının qarşısını almaq və müalicə etmək üçün təsirli bir vasitədir. Antibiotiklər viruslara təsir etmir.
19. Dəniyə kuncut yağı sürtmək koronavirusdan qorunmağa kömək edir. Xeyr, yağ virusu öldürmür.
20. Həkimlər artıq infeksiyanın qarşısının alınması və ya müalicəsi üçün nəzərdə tutulmuş dərman vasitələri əldə edə bilirlər. Xeyr, bu cür dərman hələ də yoxdur.

However, a quantitative assessment of changes to the ICS threat landscape has yielded unexpected results. The only noticeable global trend for growth in the percentage of attacked ICS computers can only be traced when analyzing the statistics of attacks on RDP (Remote Desktop Protocol) on industrial computers.

In February – May 2020, there was a clear month-to-month growth (with a subsequent decrease in June) in the percentage of ICS computers on which Kaspersky solutions detected attempts to crack RDP passwords through brute force attacks.

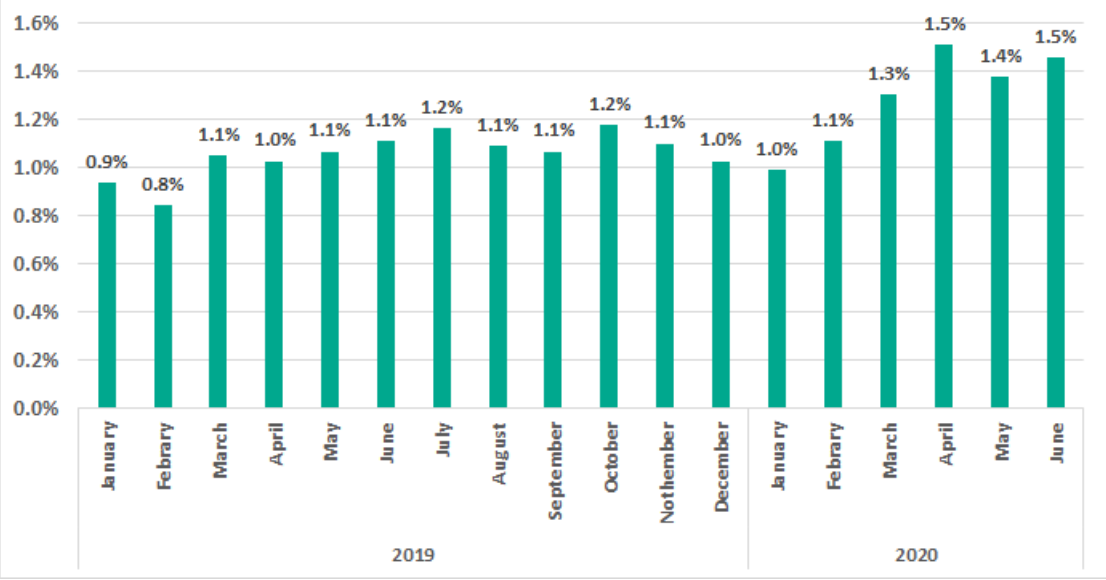
Percentage of ICS computers on which attempts to brute force RDP passwords were identified



As we can see in the diagram, the amplitude of the spring growth in the percentage of ICS computers subjected to brute force attacks does not exceed that of the annual fluctuations, although, in this case, the growth was more extended in time than all the previous surges.

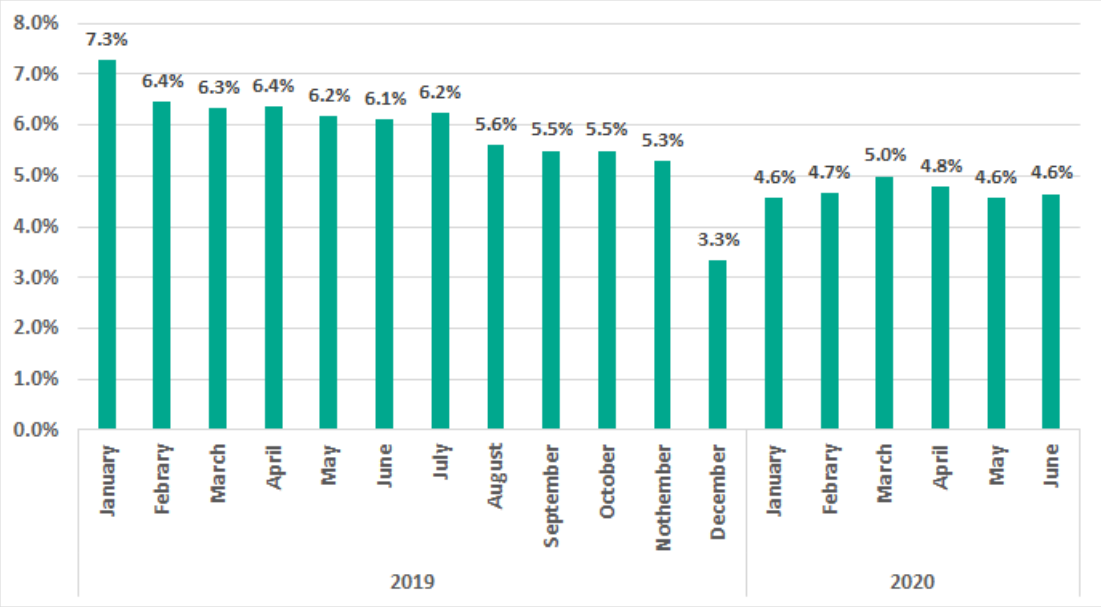
Apparently, the increases in the percentage of attacked ICS computers based on this parameter were provoked by RDP being used more often in February – June 2020.

Percentage of ICS computers available via RDP, January 2019 – June 2020



Curiously, the growth in the percentage of ICS computers on which RDP was enabled in the first quarter of 2020 occurred against the background of a sufficiently long period of attempts to reduce the use of RATs by industrial enterprises. The diagram below clearly shows the decrease in the percentage of ICS computers on which remote administration tools were used throughout the year 2019. It is worth noting that this parameter stabilized in H1 2020 (and there was even a slight growth in February – April compared to January) – a phenomenon not observed in winter and spring 2019. This may also be due to the pandemic.

Percentage of ICS computers on which RATs were used, January 2019 – June 2020



We believe that the increase in the percentage of ICS computers on which RDP is used could be an indication that most new RDP sessions were authorized by IT and information security services. In fact, all other things being equal, it may be easier to configure and control the secure operation of RDP services than that of any other RAT applications. It would seem that allowing new RDP installations was a compromise caused by the objective need to perform production-related tasks remotely in a pandemic.

The increase in the percentage of attacked ICS computers on which attempts to brute force the RDP password were detected (and prevented) may seem insignificant, but it should be remembered that any such attack, if successful, would immediately have provided the attackers with remote access to engineering computers and ICS systems. The danger posed by such attacks should not be underestimated.

As mentioned above, we have so far been unable to identify any other abnormal surges in malicious activity that could be attributed to the pandemic's consequences. We hope this was due to an actual absence of negative changes in the ICS threat landscape.

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.

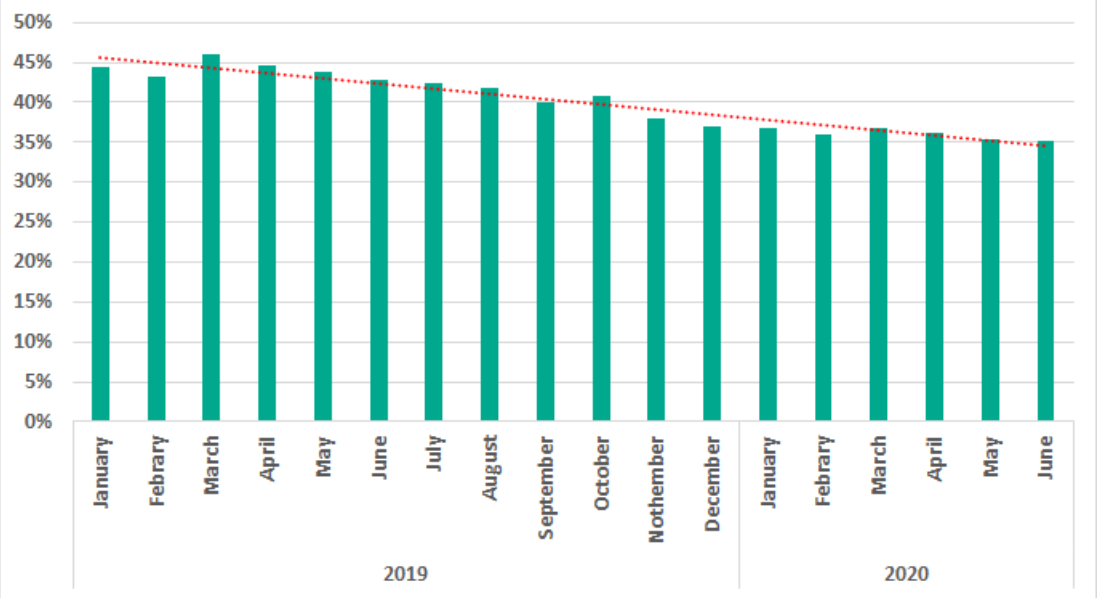
For the purposes of this report, attacked computers are those on which Kaspersky security solutions blocked one or more threats during the reporting period. When determining percentages of machines on which malware infections were prevented, we use the ratio of the number of computers attacked during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

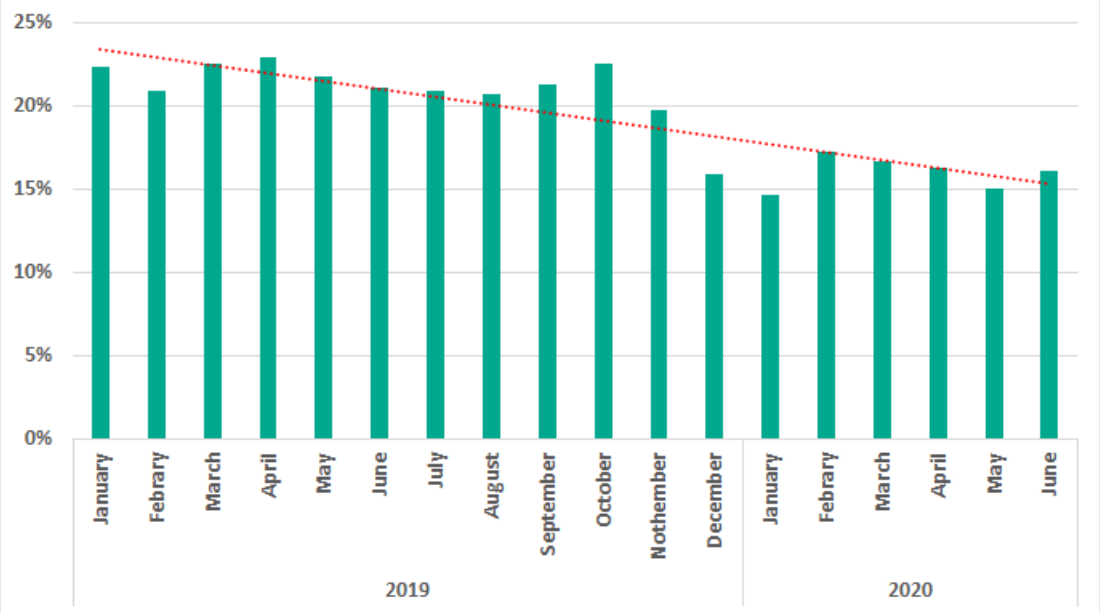
Common tendencies in the threat landscape for ICS, corporate and personal computers

We have observed a decline in the percentages of attacked computers since H2 2019 in ICS environments as well as in corporate and personal computing.

Percentage of computers *(all Kaspersky customers)* on which malicious objects were blocked by month (January 2019 – June 2020)



Percentage of *ICS computers* on which malicious objects were blocked by month (January 2019 – June 2020)



The reasons for this decrease are many including the following:

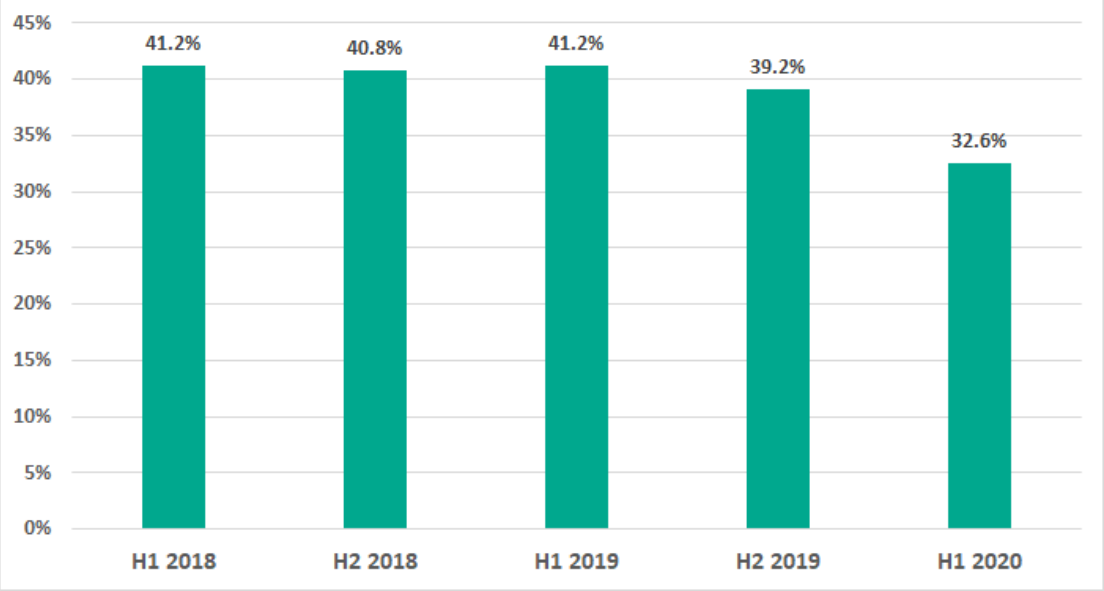
- A decrease in mass attacks focusing on infecting computers with spyware, botnet agents, cryptominers and adware;
- A shift from mass-scale attacks to more localized ones, specifically:
  - A transition from massive phishing campaigns to smaller localized attacks;
  - A decrease in malicious and infected web resources utilized for large-scale malware spreading;
- A decrease in machines infected with old self-propagating malware – worms and viruses.

At the same time, threats are becoming more local, targeted and, as a result, more complex and less noticeable.

Percentage of computers on which malicious objects were blocked

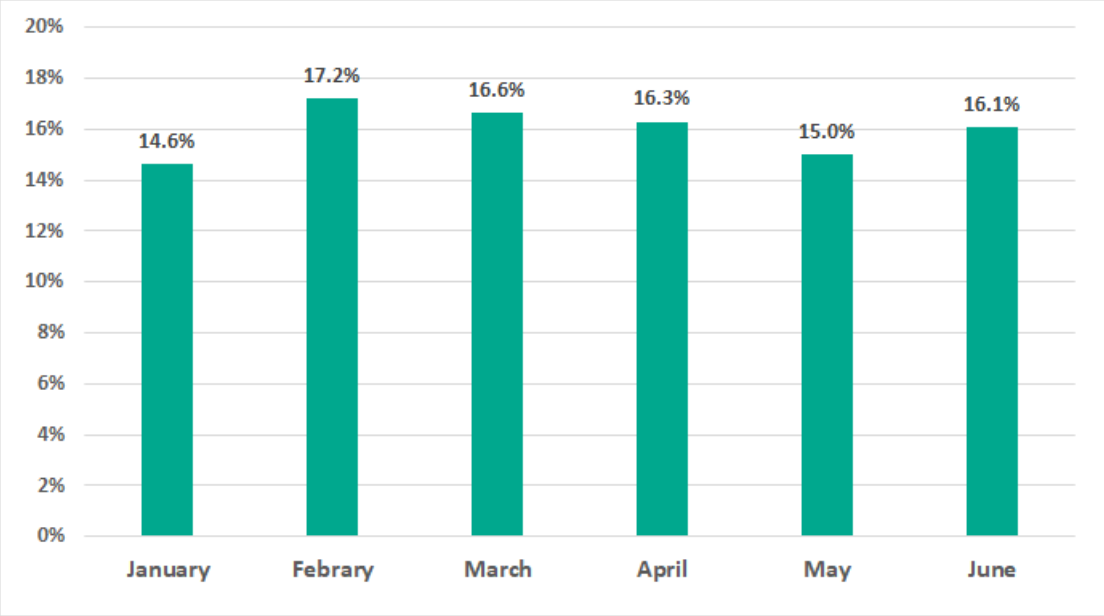
In H1 2020, malicious objects were blocked on 32.6% of ICS computers – this is lower than H2 2019 by 6.6 percentage points.

Percentage of ICS computers on which malicious objects were blocked



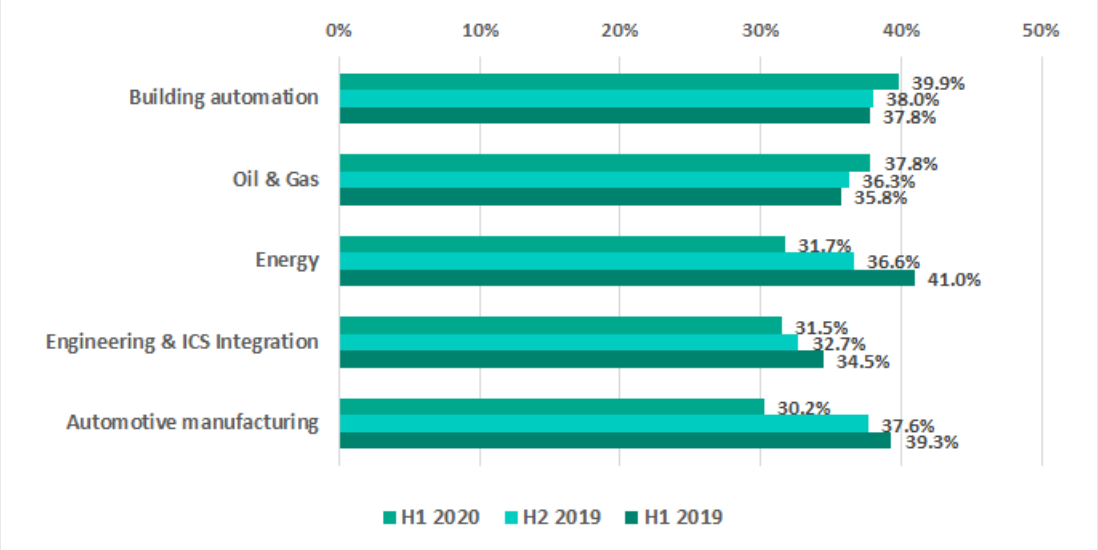
In H1 2020 the highest percentage of ICS computers on which malicious objects were blocked was recorded in February and the lowest in January.

Percentage of ICS computers on which malicious objects were blocked by month (January – June 2020)



Situation in selected industries

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



Despite the overall tendency for decreasing percentages of attacked computers in H1 2020, the numbers have risen slightly in the Oil & Gas sector, as well as in building automation systems.

Computers in building automation systems are often connected to corporate networks and have access to various services, including the internet, corporate email, domain controllers and so forth. In other words, these machines have the same attack surfaces as computers in the regular corporate network, and certainly larger when compared to ICS computers.

For instance, a recent investigation of an attack involving the Snake ransomware showed that Kaspersky solutions had blocked malware not only in the corporate network of an industrial facility, but also on the video surveillance servers, which were connected to the corporate domain controller.

Building automation systems often belong to contractor organizations and even when these systems have access to the client's corporate network, they are not always controlled by the corporate information security team. Given that the decrease in mass attacks is offset by an increase in the number and complexity of targeted attacks where we see active utilization of various lateral movement tools, building automation systems might turn out to be even less secure than corporate systems within the same network.

In H1 2020 Kaspersky solutions blocked numerous new variants of worms written in script languages, specifically Python and PowerShell, on computers used for design, maintain and automate industrial systems in the Oil & Gas sector. The surge in these detections occurred from the end of March to mid-June 2020, mainly in China and the Middle East.

All of the detected worm samples, both in Python and in PowerShell, are capable of collecting authentication credentials from the memory of system processes on the attacked machines in order to spread within the network. In most cases, the malware uses different versions of Mimikatz to steal authentication credentials from memory. However, there were some PowerShell samples which used the comsvsc.dll system library (MS Windows) to save a memory dump of the system process in which the malware then searched for authentication credentials.

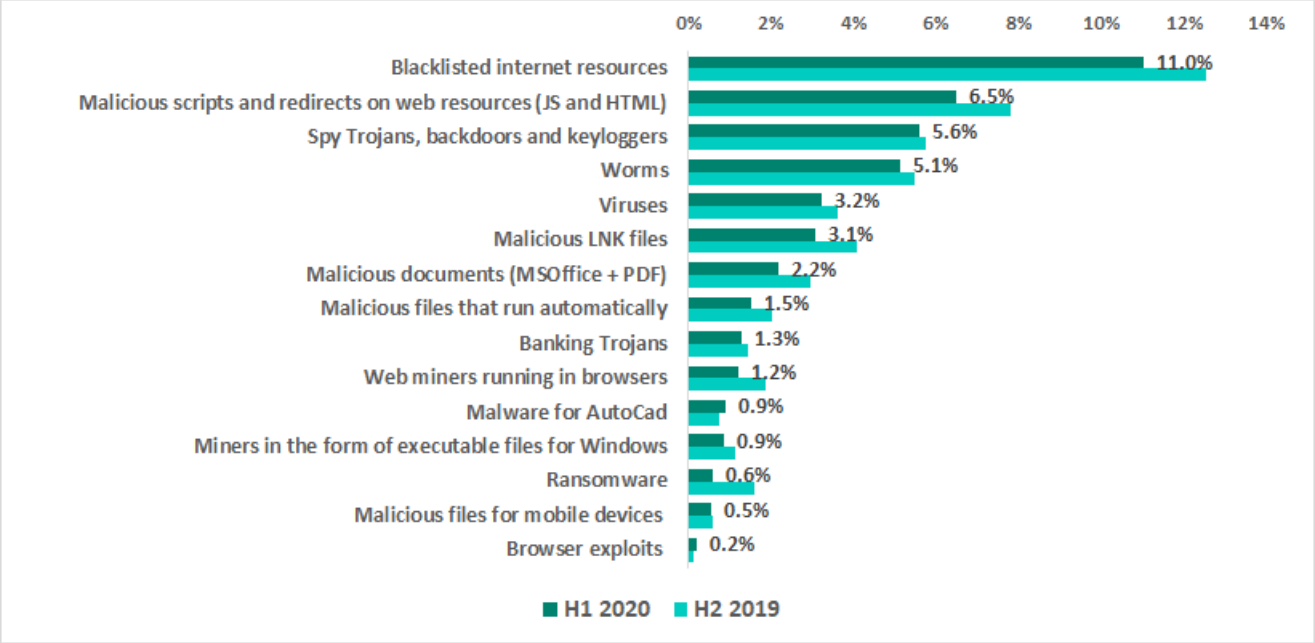
The variety of malware detected

In H1 2020, Kaspersky security solutions blocked over 19.7 thousand malware modifications from 4,119 different families on industrial automation systems. We have tracked noticeably larger numbers of families in the following categories: backdoor, spyware, Win32 exploits and .NET malware.

Malicious object categories

The malicious objects blocked by Kaspersky solutions fall into many different categories. To give a better idea of the types of threats blocked by Kaspersky products, we conducted a detailed classification. Note that 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 estimated percentages of ICS computers on which the activity of malicious objects from different categories had been prevented:



Percentage of ICS computers on which the activity of malicious objects was prevented by malware class

- 11.0% – 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.
- 6.5% – malicious scripts and redirects on web resources (JS and HTML) executed in the context of the browser, as well as browser exploits – 0.2%.
- 5.6% – 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.
- 5.1% – 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.
- 3.2% – Virus class malware.

  These programs include such families as Sality (0.9%), Nimnul (0.6%), and Virut (0.4%), 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.

- 3.1% – 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 (0.4%), 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.
- 2.2% – malicious documents (MSOffice + PDF) containing exploits, malicious macros or malicious links.
- 1.5% – 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.).
- 1.3% – banking Trojans.
- 1.2% – web miners running in browsers. 0.9% – miners in the form of executable files for Windows.
- 0.9% – malware for AutoCad.

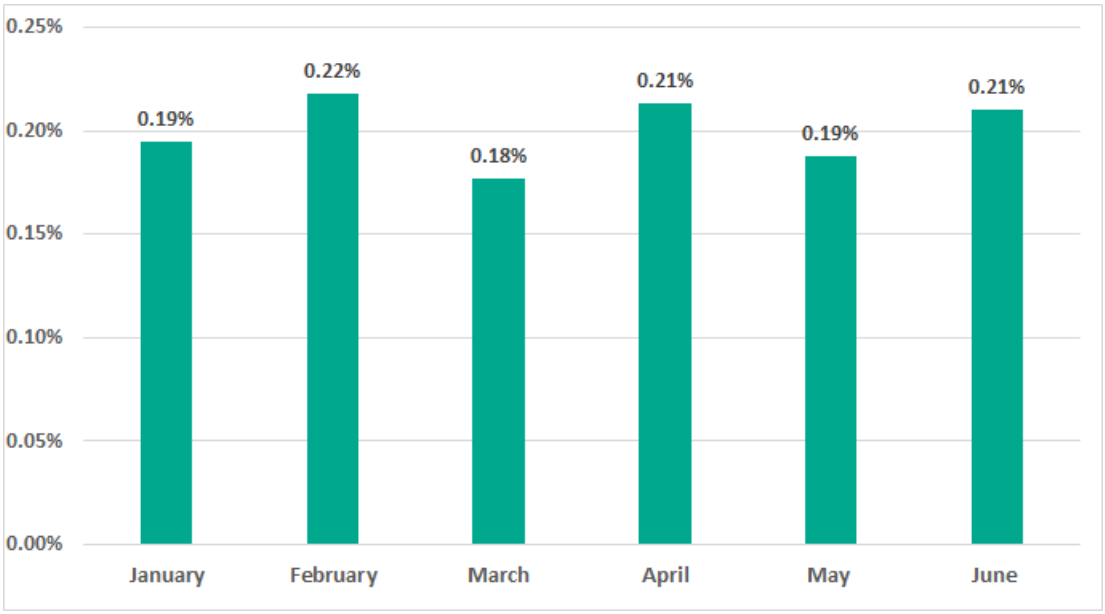
  It is worth noting that malware for AutoCad, specifically viruses, is mainly detected on computers that are part of industrial networks, including network shares and engineering workstations, in East Asia.
- 0.6% – ransomware.
- 0.5% – malicious files for mobile devices that are blocked when such devices are connected to computers.

Ransomware

In H1 2020 ransomware was blocked on 0.63% of ICS computers, which does not differ significantly from the previous six months (0.61%).

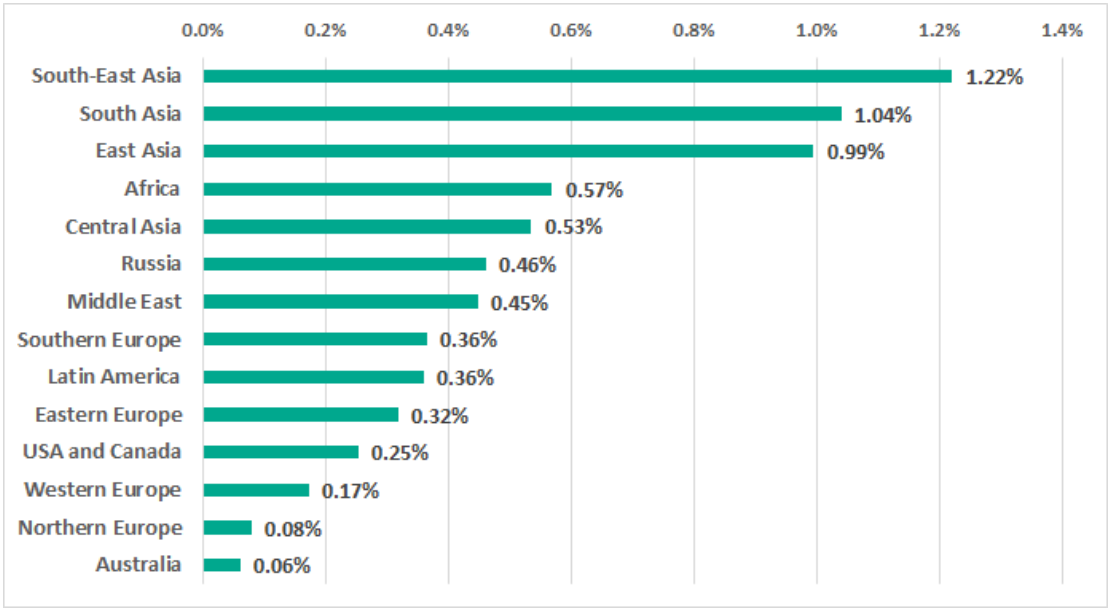
Throughout H1 2020 this number fluctuated between a low of 0.18% in March and a high of 0.22% in February.

Percentage of ICS computers on which ransomware was blocked by month (January – June 2020)



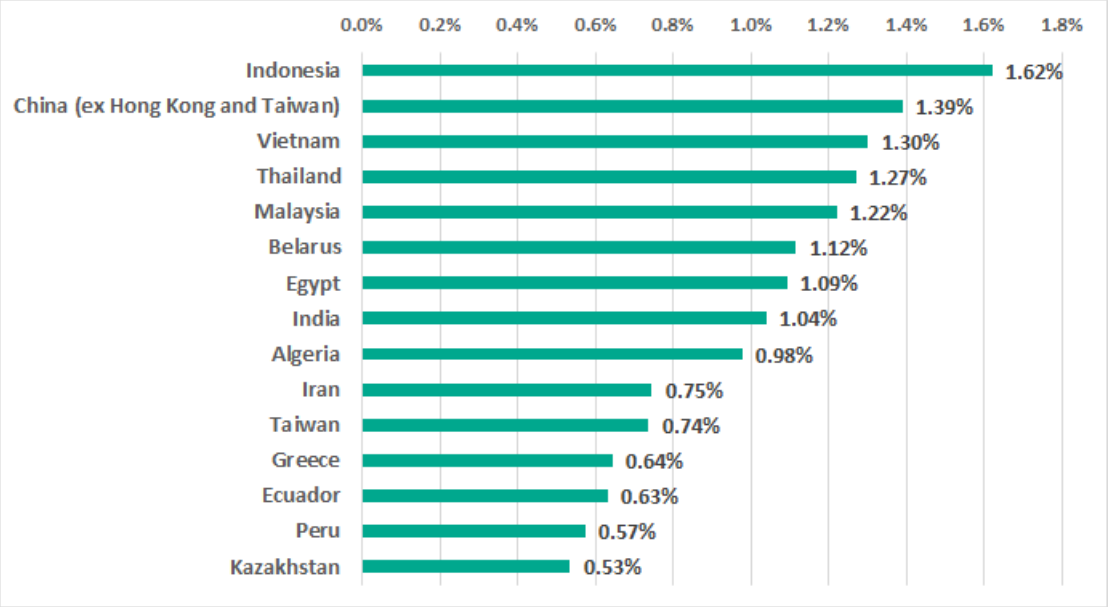
Southeast, South and East Asia led with a noticeable margin in the regional rating by the percentage of ICS computers attacked by ransomware.

Regions ranked by the percentage of ICS computers on which ransomware was blocked in H1 2020



Over half of the countries in the TOP 15 ranking are Asian. Greece and Belarus are the only European countries among the TOP 15 (see below).

TOP 15 countries and territories by percentage of ICS computers on which ransomware was blocked in H1 2020

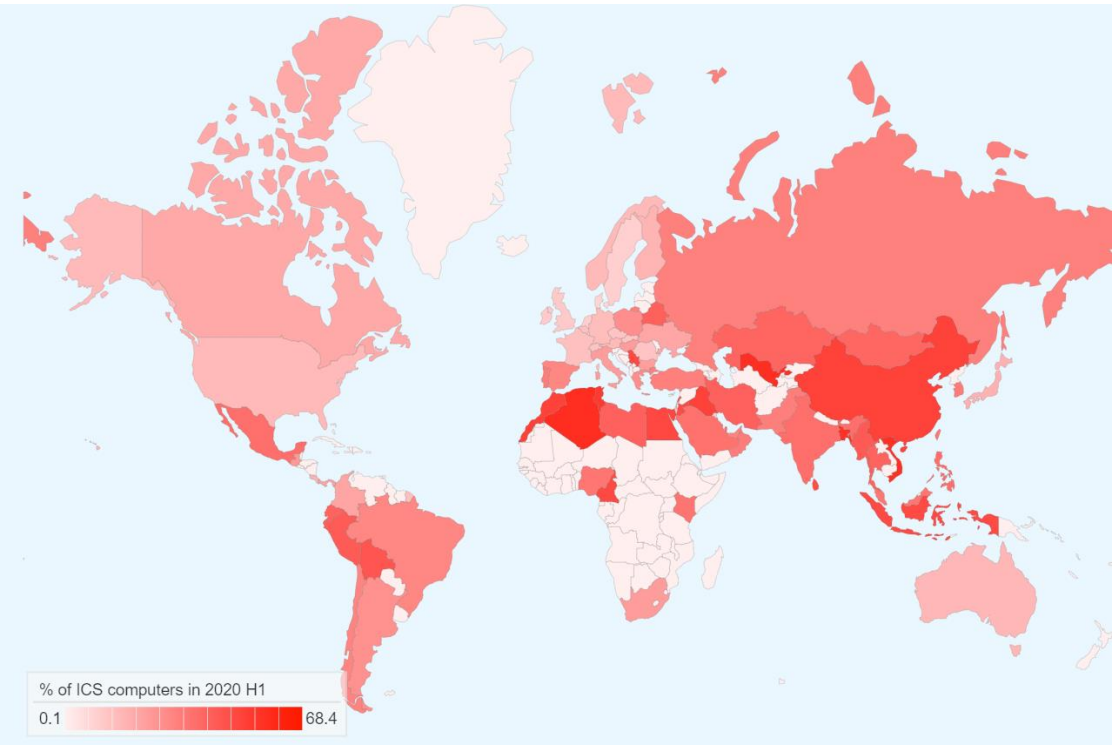


Russia is in the middle of the list with 0.46%.

Geographical distribution

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

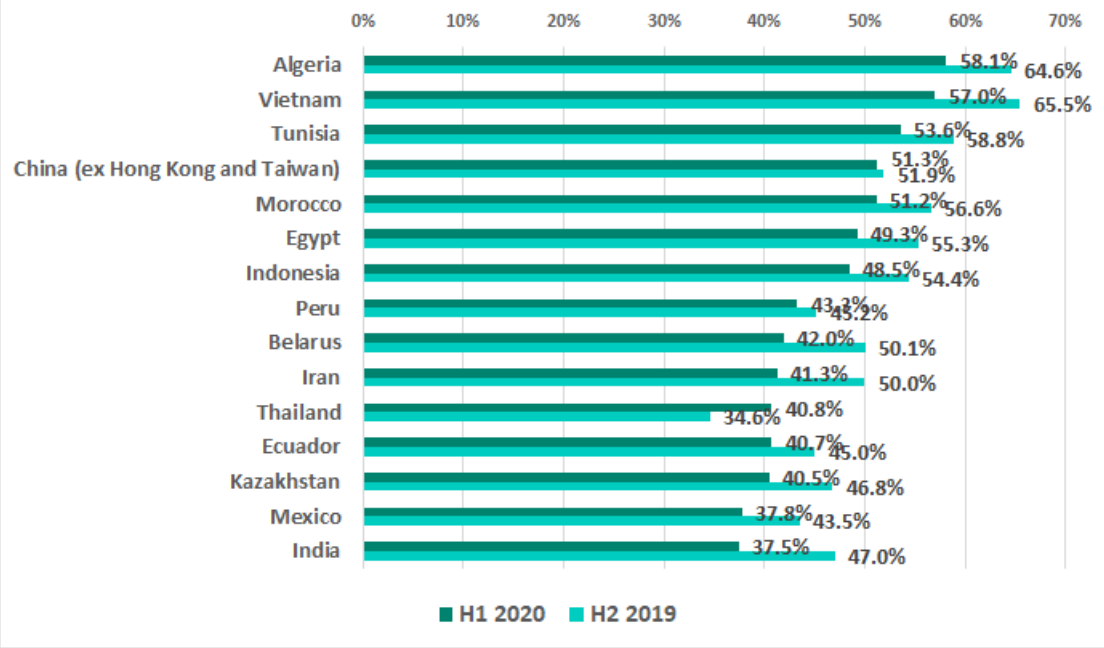
Geographical distribution of attacks* on industrial automation systems in H1 2020



** percentage of ICS computers on which malicious objects were blocked*

Distribution by country

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

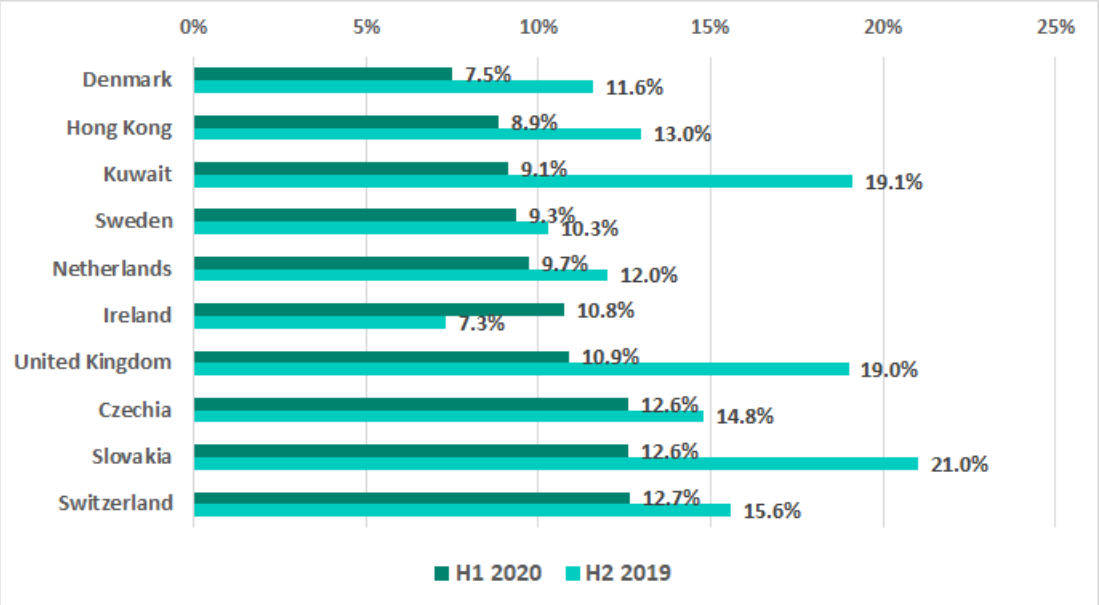


The H1 2020 results see China return to one of the top five positions in the ranking for the first time since 2017.

The most significant increase in the percentage of ICS computers where malicious activity was prevented occurred in Greece (by 7.8 p.p.), Thailand (by 6.2 p.p.) and Portugal (by 4.3 p.p.).

The numbers decreased in the vast majority of countries, most noticeably in South Africa (by 19.1 p.p.), Israel (by 12.8 p.p.), Russia (by 13.9 p.p.) and Kuwait (by 10 p.p.). As a result Kuwait has now even appeared in the list of the 10 most secure countries. It is worth noting that two Eastern European countries are also on this list once again: Czech Republic and Slovakia.

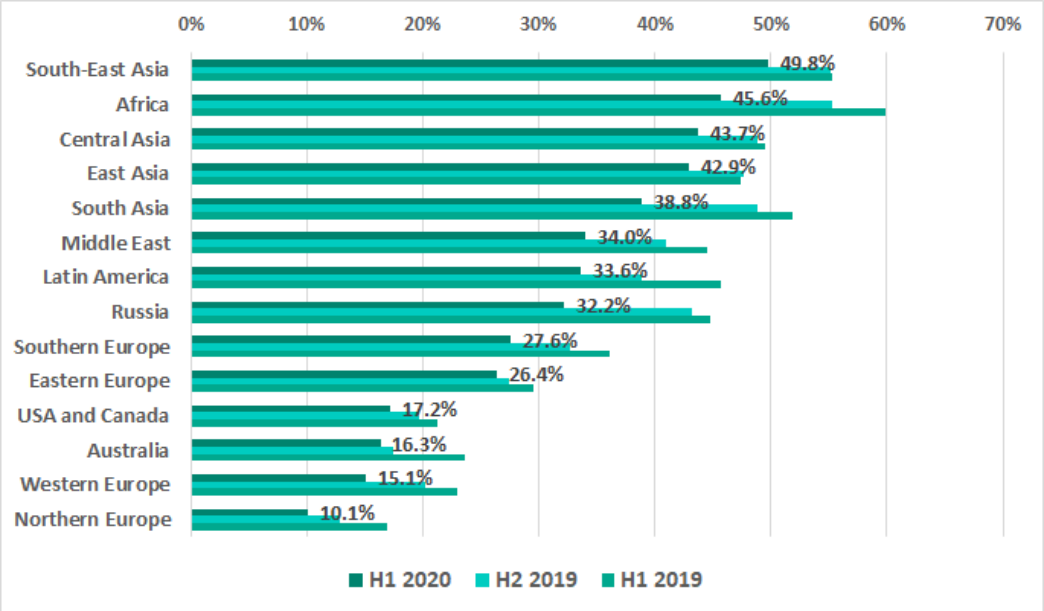
10 countries and territories with the lowest percentage of ICS computers on which malicious objects were blocked



Distribution by region

Southeast Asia, Africa and Central Asia lead in the rating of regions based on the proportion of ICS computers on which malicious activity was prevented.

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

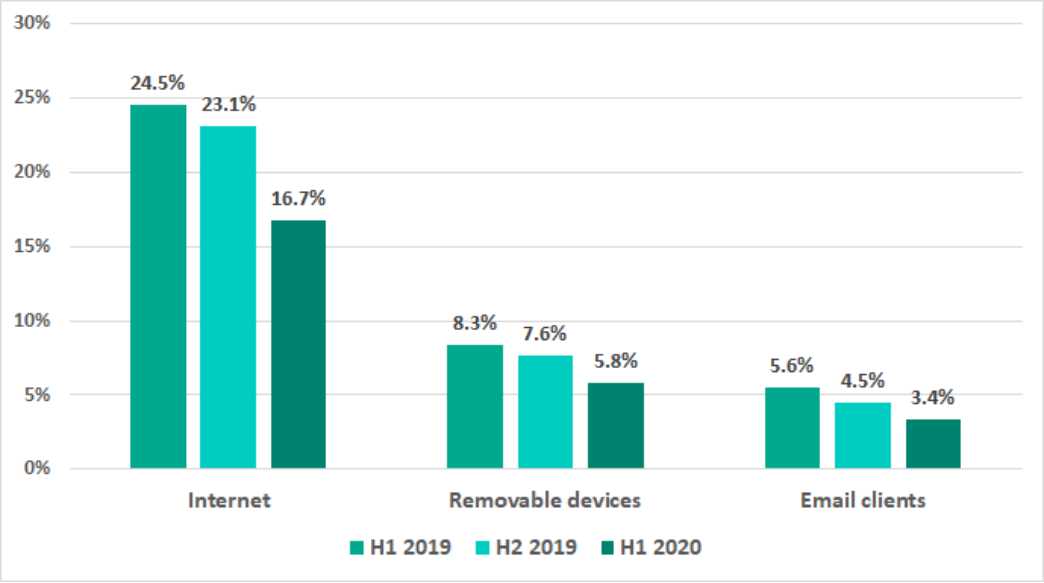


Europe, Australia, the United States and Canada are the most secure as usual: the numbers in these regions are less than 30%.

Threat sources

The internet, removable media and email continue to be the main sources of threats to computers in the ICS environment.

Main sources of threats blocked on ICS computers*

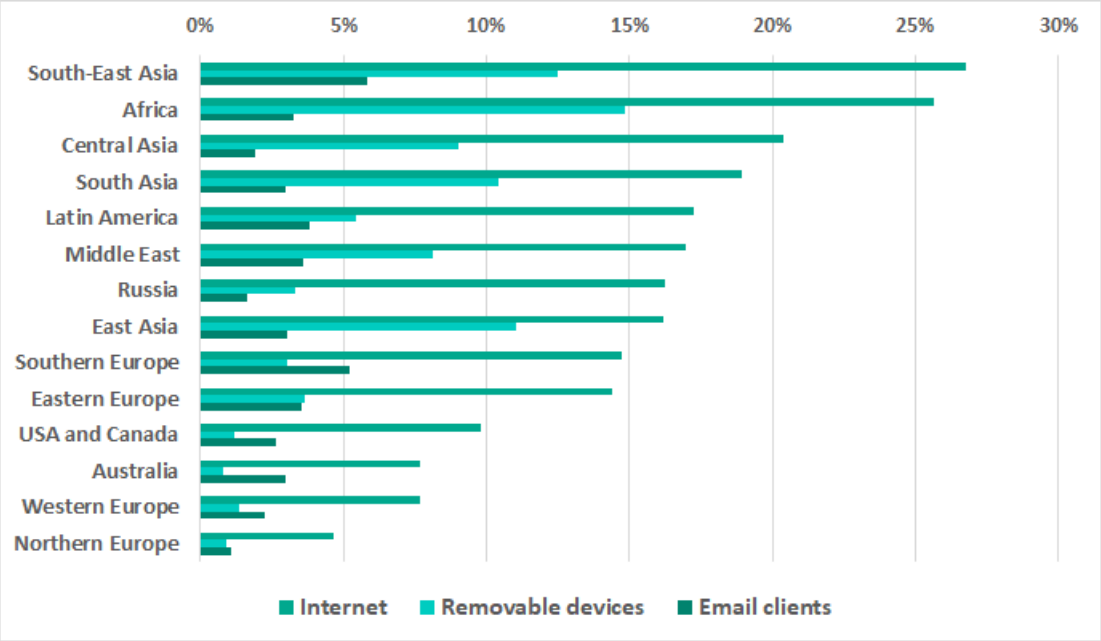


** percentage of ICS computers on which malicious objects from different sources were blocked*

In H1 2020 threats blocked on 16.7% of ICS computers came from the internet. This is 6.4 p.p. less than in H2 2019.

Main threat sources: geographical distribution

Main sources of threats blocked on ICS computers* by region in H1 2020



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

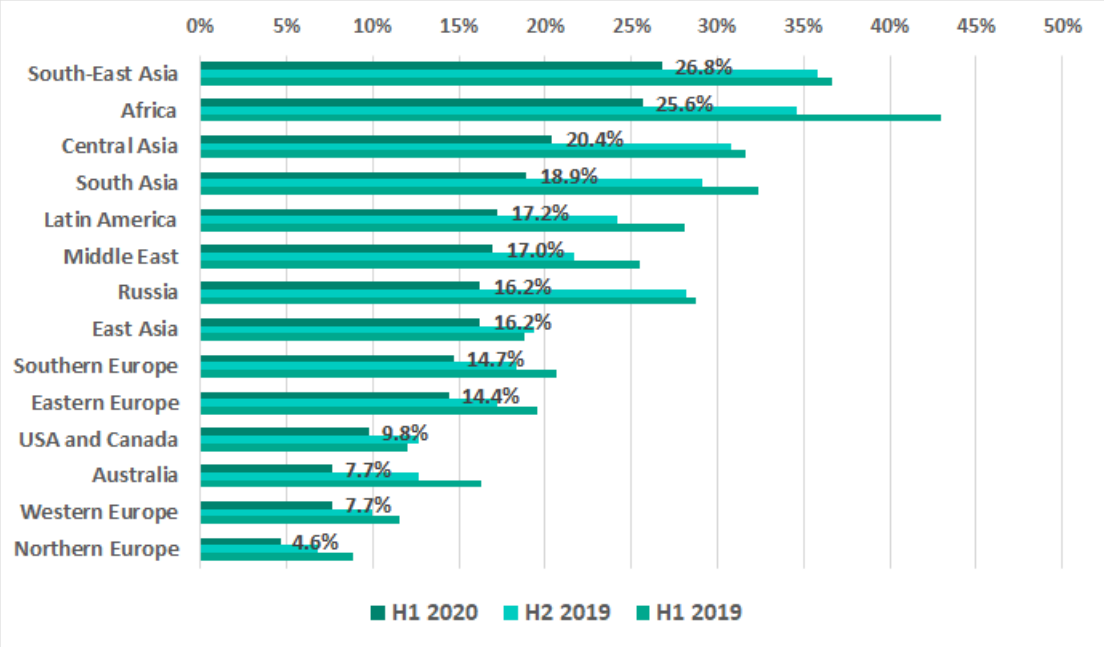
We need to emphasize that in those regions where the smallest percentages of internet threats were blocked on ICS computers, aka Europe, USA and Canada, and Australia, the percentages of threats arriving via email attachments are greater than the percentages of threats borne by removable media. Eastern Europe is the exception where these numbers are similar.

In the remaining regions the percentage of ICS computers where threats penetrating when removable media were connected is significantly larger than the percentage of ICS computers where malicious email attachments were blocked.

Internet

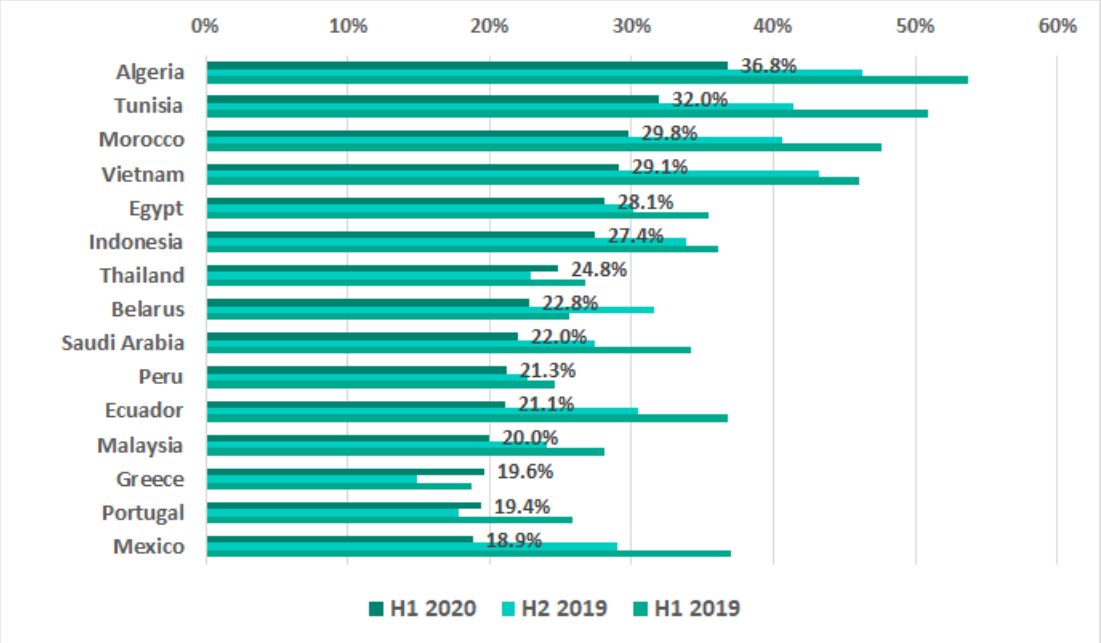
The internet is the main source of threats worldwide. The percentage of ICS computers on which internet threats were blocked in Northern and Western Europe, Australia and in North America is less than 10%. At the same time, this percentage is over 20% in Africa, Southeast and Central Asia.

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



H1 2020 sees Greece and Portugal moving up to the TOP 15 of countries where internet threats were blocked on ICS computers from 29th and 33rd places, respectively. Thailand is the only other country in the TOP 15 to experience any growth.

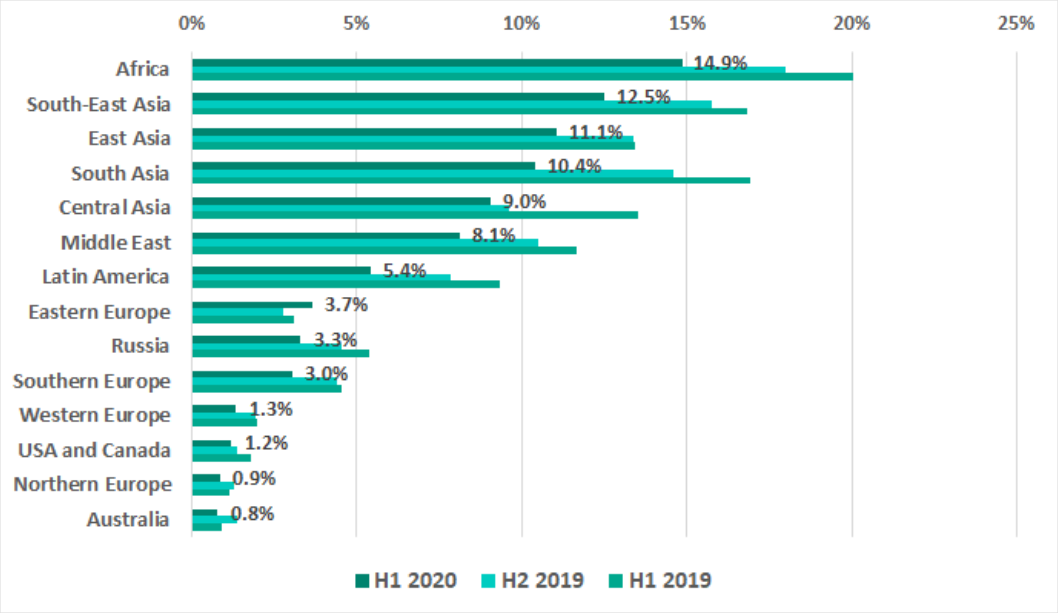
Top 15 countries and territories by percentage of ICS computers on which internet threats were blocked



Removable media

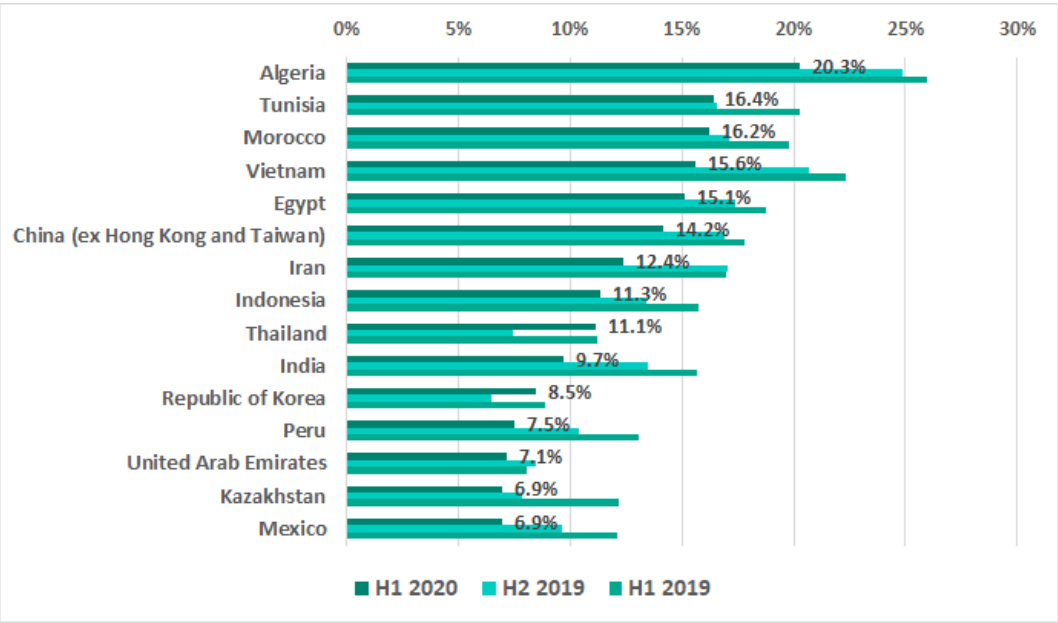
The largest percentages of ICS computers where malicious threats were blocked when removable media were connected were in Africa, Southeast, East and South Asia. The numbers remain minimal in Australia, Northern and Western Europe, and North America. Note that Eastern Europe is the only region where this percentage increased (by 0.9 p.p.) in H1 2020.

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



In H1 2020 Taiwan, Saudi Arabia, and Argentina were ousted by Thailand, Korea and Kazakhstan in the TOP 15 countries ranked by percentage of ICS computers on which malware was blocked when removable media were connected. Notably, no countries from North America, Europe and Australia are in the TOP 15 rating at all.

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



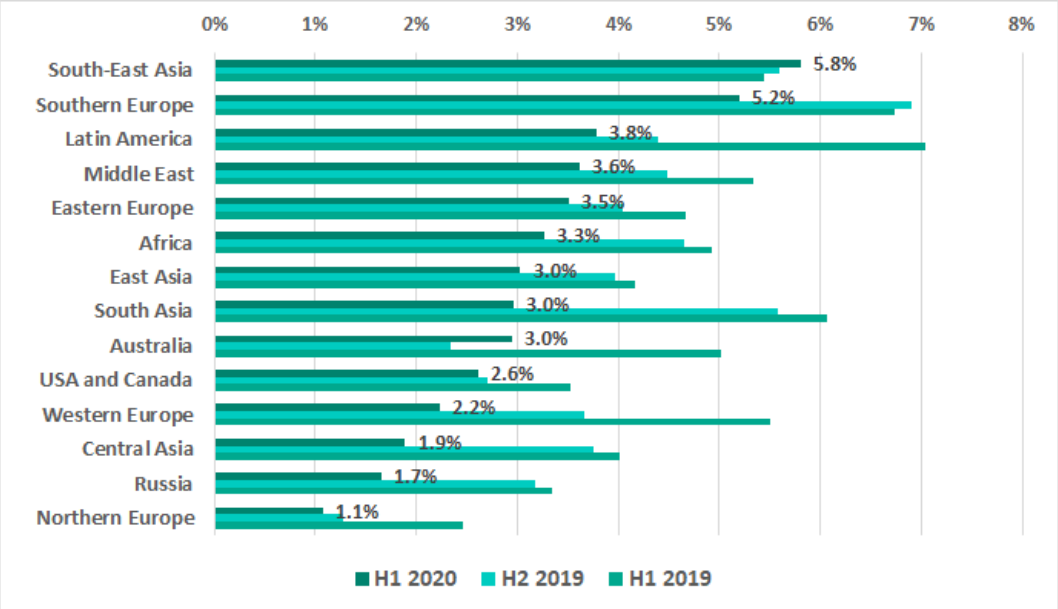
The percentages have decreased in H1 2020 in all TOP 15 countries except Thailand and South Korea.

Email clients

In H1 2020 Southeast Asia led the rating of regions based on the percentage of ICS computers on which malicious email attachments were blocked. In addition to the leading region we see an unexpected growth in Australia (by 0.7 p.p.).

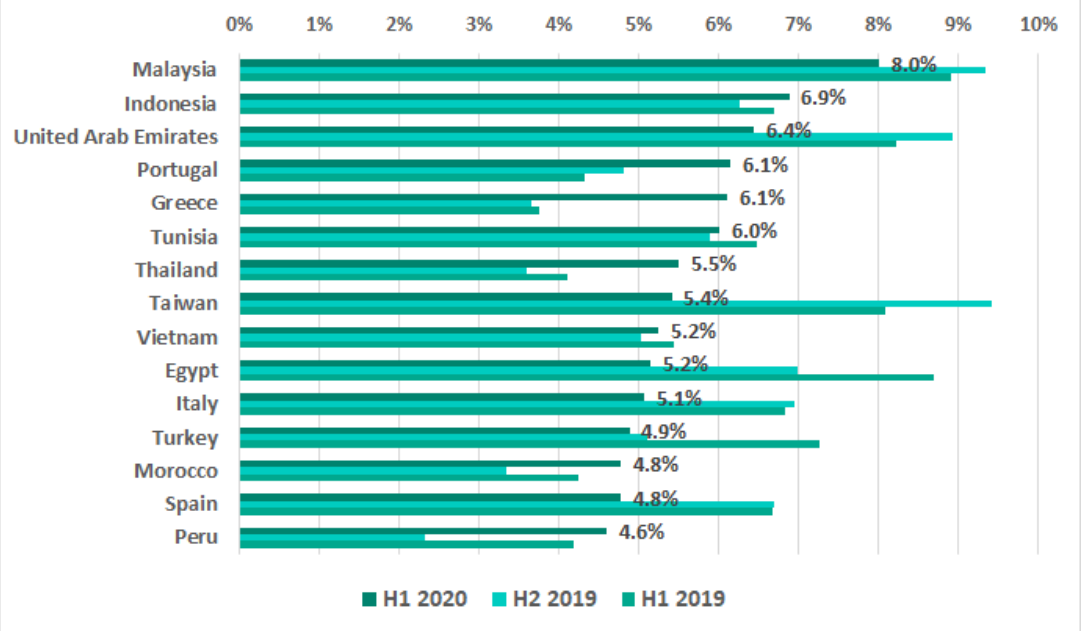
Two European regions – Southern and Eastern – appear in the TOP 5, unlike in the other two attack vectors.

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



The numbers have increased in seven of the TOP 15 countries ranked by the percentage of ICS computers on which malicious email attachments were blocked. The most significant changes have occurred in Greece (2.5 p.p.), Peru (2.3 p.p.) and Thailand (1.9 p.p.).

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



In H1 2020 we see the percentage of ICS computers on which malicious email attachments were blocked in Slovakia, which had leaped to third place in the TOP 15 in H2 2019, dropping dramatically by 8 p.p. We also see a decrease of 4 p.p. in Taiwan and South Africa. It is worth noting that Taiwan, unlike Slovakia and South Africa, stayed in the TOP 15 – in 8th place.

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@laspersky.com