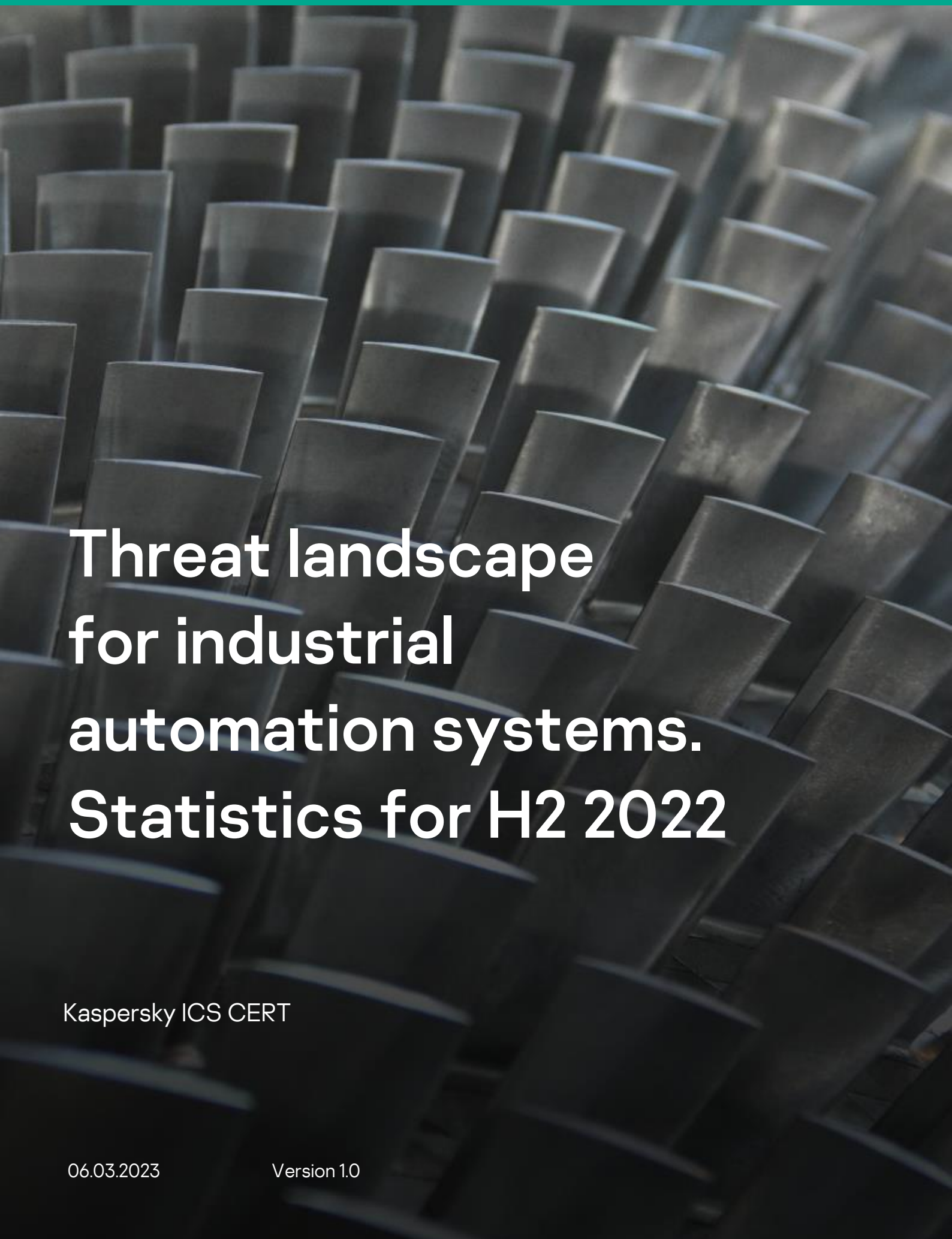
kaspersky



Threat landscape for industrial automation systems. Statistics for H2 2022

Kaspersky ICS CERT

06.03.2023 Version 1.0

2022 in numbers

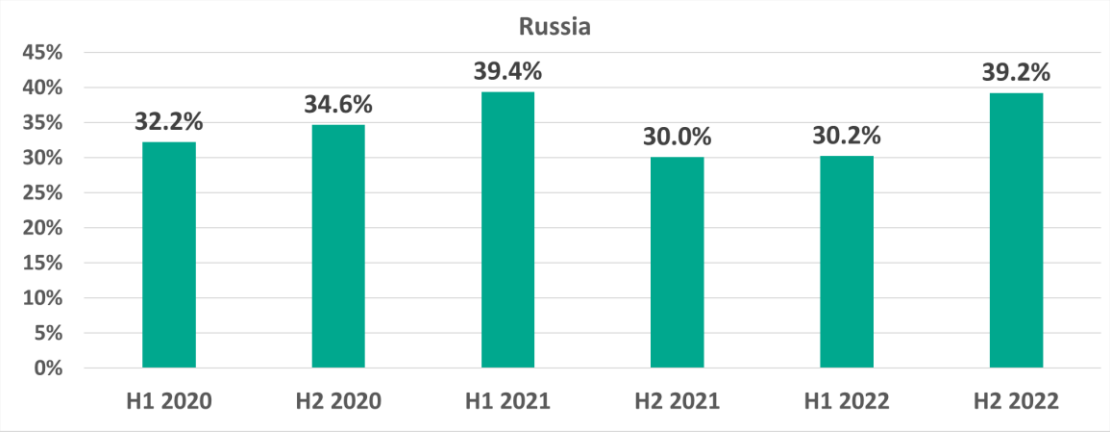
Parameter	H1 2022	H2 2022	2022
Percentage of attacked ICS computers globally	31.8%	34.3%	40.6%
Main threat sources			
Internet	16.5%	19.9%	24.0%
Email clients	7.0%	6.4%	7.9%
Removable devices	3.5%	3.8%	5.2%
Network folders	0.6%	0.6%	0.8%
Percentage of ICS computers on which malicious objects from different categories were blocked			
Malicious scripts and phishing pages (JS and HTML)	12.9%	13.5%	17.3%
Denylisted internet resources	9.5%	10.1%	13.2%
Spy Trojans, backdoors and keyloggers	8.6%	7.1%	9.2%
Malicious documents (MSOffice+PDF)	5.5%	4.5%	6.2%
Worms	2.8%	2.5%	3.5%
Viruses	2.4%	2.4%	3.2%
Miners – executable files for Windows	2.3%	1.5%	2.7%
Web miners running in browsers	1.8%	1.8%	2.5%
Malware for AutoCAD	0.6%	0.6%	0.8%
Ransomware	0.6%	0.4%	0.7%

Russia, H2 2022

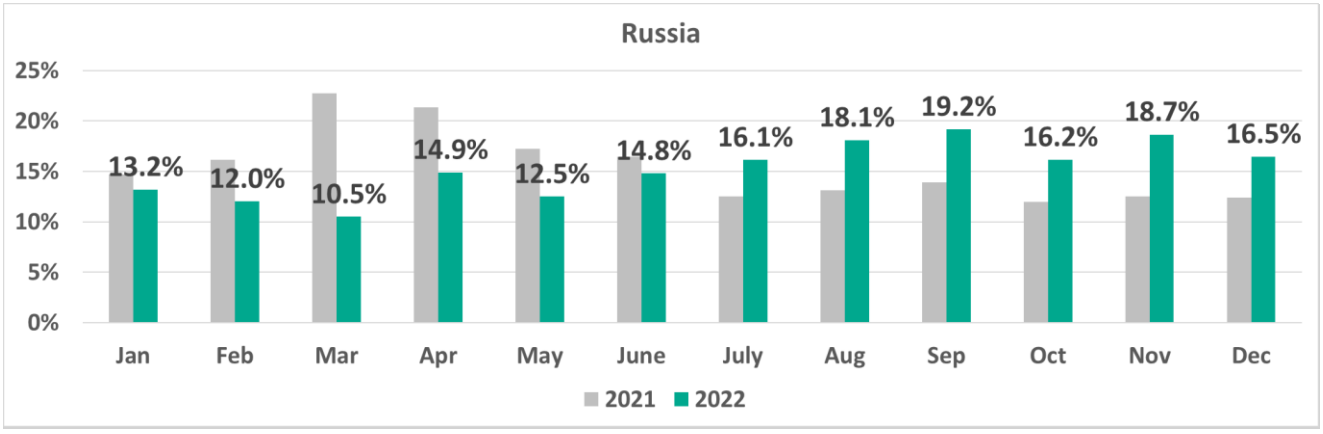
In H2 2022, **the most significant change among all countries** in the percentage of ICS computers on which malicious objects were blocked was observed in Russia, where that percentage increased by 9 p.p.

With its 39.2%, Russia jumped from eighth to third place in the ranking based on this parameter (it is worth noting that, in our reports, Russia is treated both as a country and as a region that includes a single country).

Russia. Percentage of ICS computers on which malicious objects were blocked

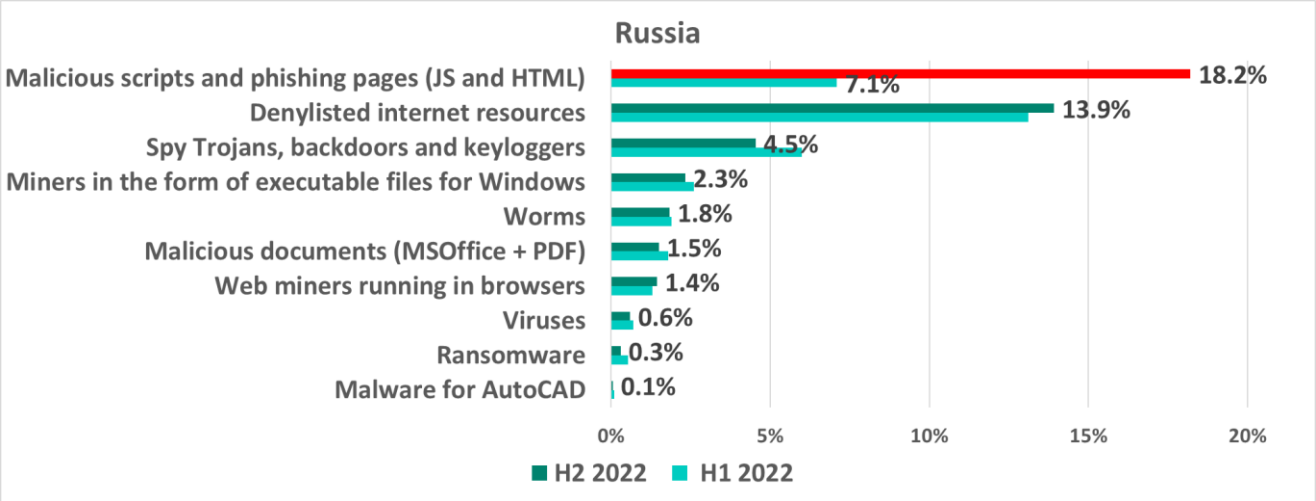


After rising and falling during H1 2022, monthly percentages of ICS computers on which malicious objects were blocked increased during the first three months of H2 2022. It is worth noting that the month-by-month dynamics of these figures in 2022 were completely different from those observed during the previous year, i.e., 2021.

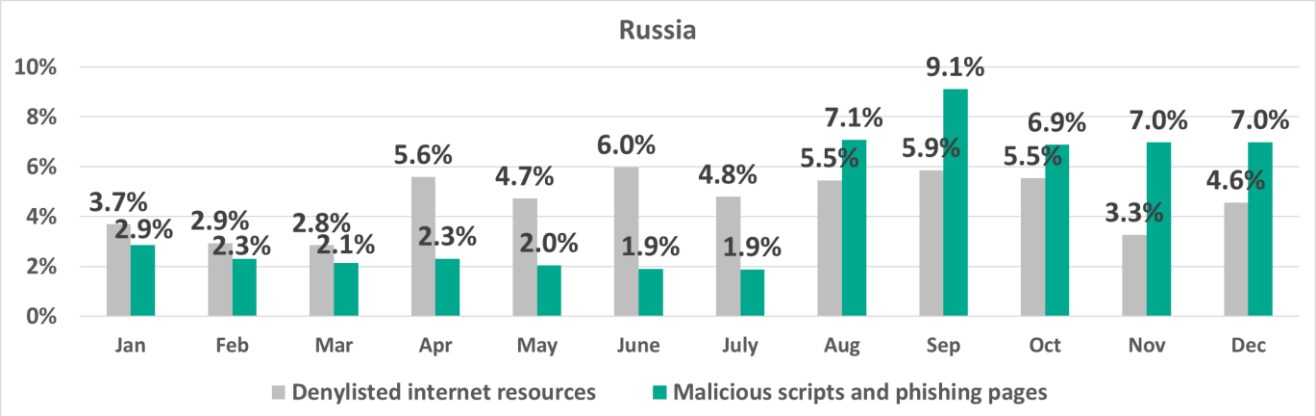


Russia. Percentage of ICS computers on which malicious objects were blocked, January – December of 2021 and 2022

The increase in the percentage of ICS computers in Russia on which malicious objects were blocked in H2 2022 was due to a sharp increase of 11.1 p.p. in the percentage of ICS computers on which malicious scripts and phishing pages were blocked.



Russia. Percentage of ICS computers on which malicious objects from different categories were blocked



Russia. Percentage of ICS computers on which denylisted internet resources, as well as malicious scripts and phishing pages were blocked, January – December 2022

The sudden surge in the percentage of ICS computers on which malicious scripts and phishing pages were blocked in August and September 2022, as well as the high figures in the following months, were due to mass infections of websites (including those of industrial organizations) that use the Bitrix CMS. It should be noted that ICS computers from which arbitrary websites can be accessed are mostly ICS operator or engineering workstations.

The CVE-2022-27228 vulnerability in the Bitrix CMS "Polls, Votes" module, which was discovered back in March 2022, enables an attacker to execute arbitrary code on the web server. In the process of carrying our mass infections of

websites, the attackers infected JavaScript files used on each site, injecting code that redirects browsers to third-party malicious web resources and phishing pages.

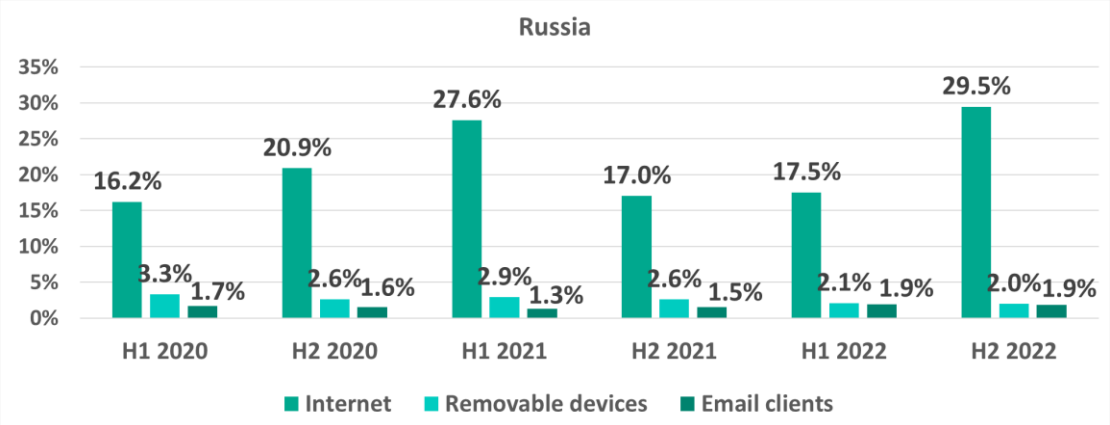
Apart from Russia, the distribution of malicious scripts resulting from the mass infections of websites managed by the Bitrix CMS also affected ICS computers in Belarus and countries in Central Asia. In H2 2022, the percentage of ICS computers on which malicious scripts and phishing pages were blocked increased:

- in Belarus, by 10.3 p.p., yielding 17.8% in H2 2022;
- in Kyrgyzstan, by 16.4 p.p., yielding 26.4% in H2 2022;
- in Uzbekistan, by 7.8 p.p., yielding 15.6% in H2 2022;
- in Kazakhstan, by 6.1 p.p., yielding 14.1% in H2 2022.

As regards the increase (starting in April 2022) in the percentage of ICS computers on which attempts to access malicious web resources were blocked, it was largely due to a surge in the activity of potentially dangerous advertising platforms that are often used to spread malware disguised as advertising displayed on various web resources.

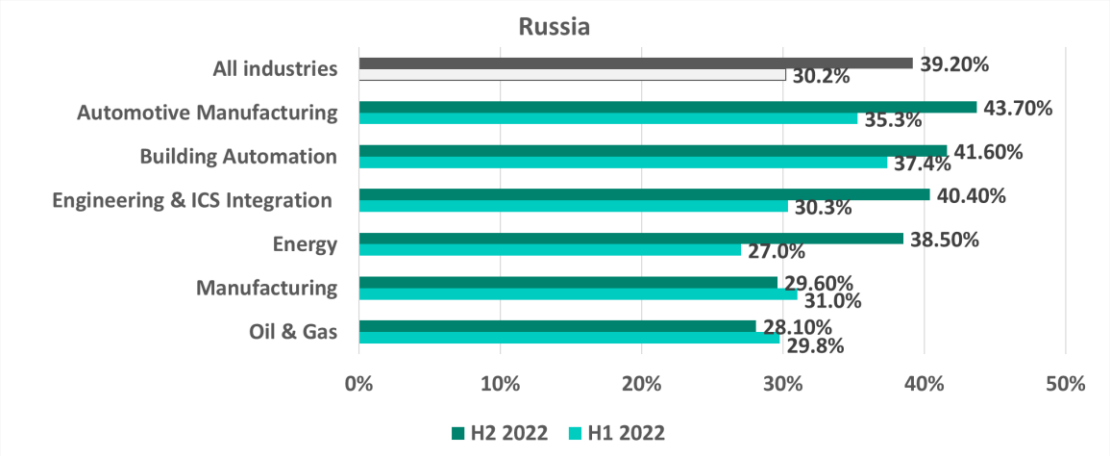
In H2 2022 Russia saw an increase of 12 p.p. in the percentage of ICS computers on which internet threats were blocked.

Russia. Percentage of ICS computers on which malicious objects from different sources were blocked



In H2 2022 in Russia, most industries saw an increase (in some cases, quite significant) in the percentage of ICS computers on which malicious objects were blocked – both as a consequence of mass distribution of malicious scripts and due to a relatively small increase in the percentage of ICS computers in Russia on which spyware was blocked.

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

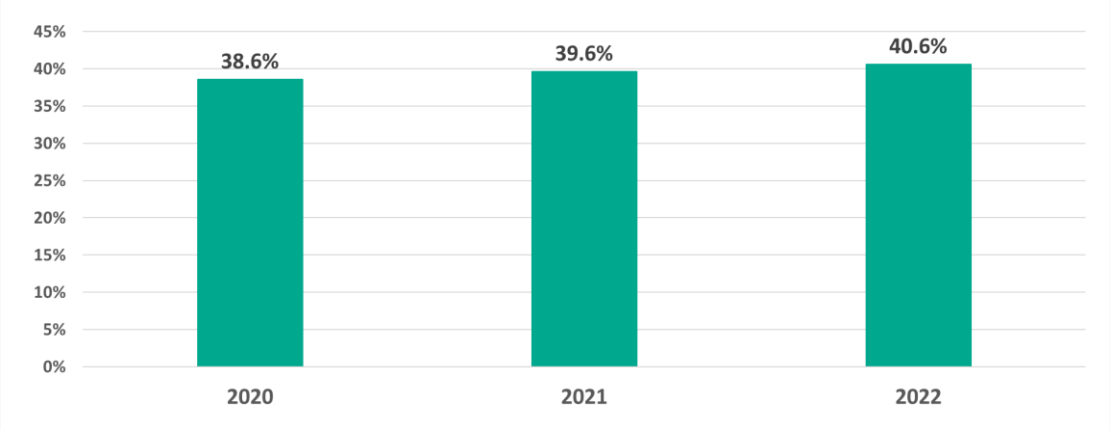


The decrease in percentage compared to H1 2022 in the manufacturing and oil and gas industries was due to the lower figures recorded for internet and email threats.

Global threat statistics

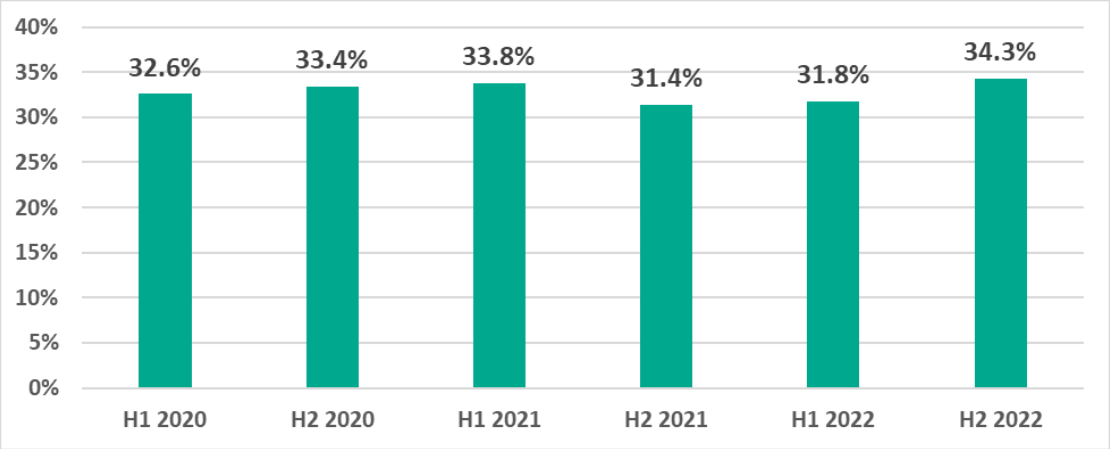
In 2022, the overall percentage of ICS computers on which malicious objects were blocked was 40.6%. As in 2021, the percentage increased, compared to the previous year, by 1 p.p.

Percentage of ICS computers on which malicious objects were blocked, 2020 – 2022



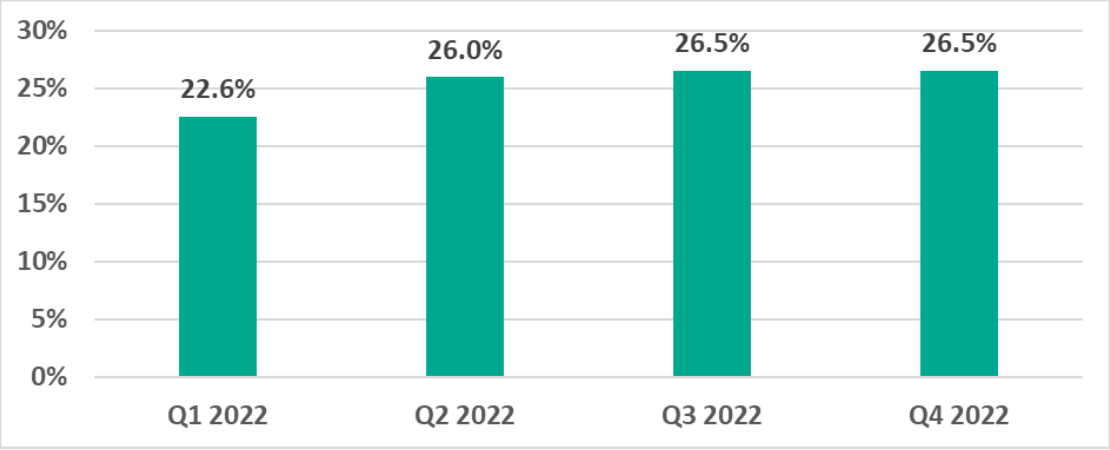
However, while in H1 2022 the percentage of ICS computers on which malicious objects were blocked increased only by 0.4 p.p. compared to the previous six-month period, in H2 2022 the percentage increased by 3.5 percentage points, reaching 34.3%. This was higher than the percentages for 2021 and even 2020, albeit not by much.

Percentage of ICS computers on which malicious objects were blocked

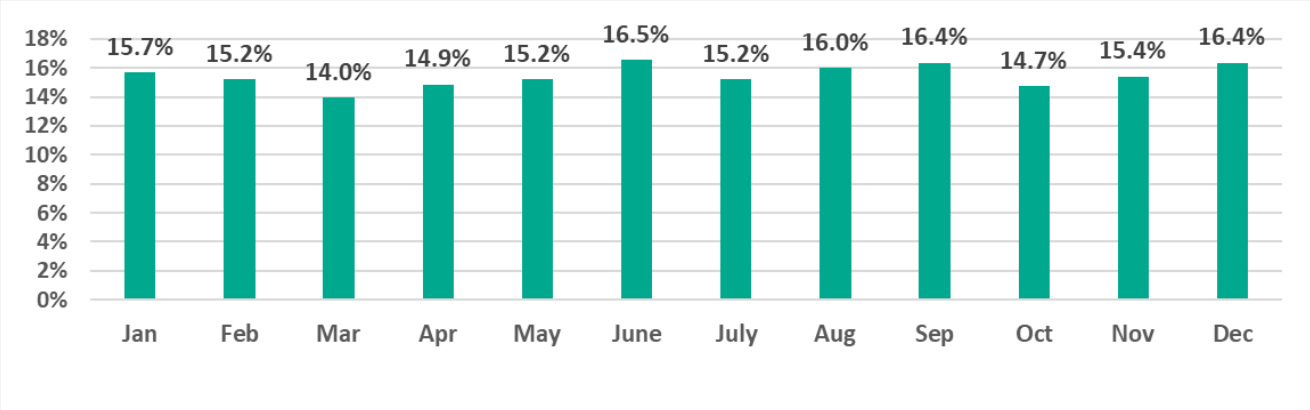


It can be seen in the diagram below that in 2022, the smallest percentage of ICS computers on which malicious objects were blocked was observed in Q1 and the main growth was observed in Q2. The percentages were the same in Q3 and Q4.

Percentage of ICS computers on which malicious objects were blocked, by quarter, 2022



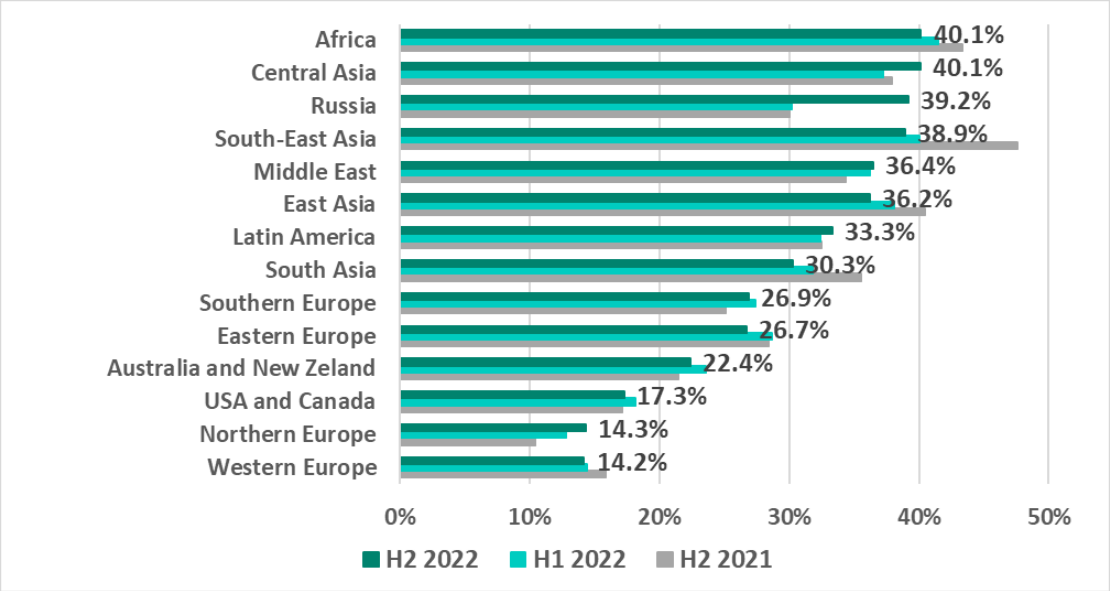
June, September and December were the 'hottest' months. The lowest percentage values were observed in March and October.



Percentage of ICS computers on which malicious objects were blocked, January – December 2022

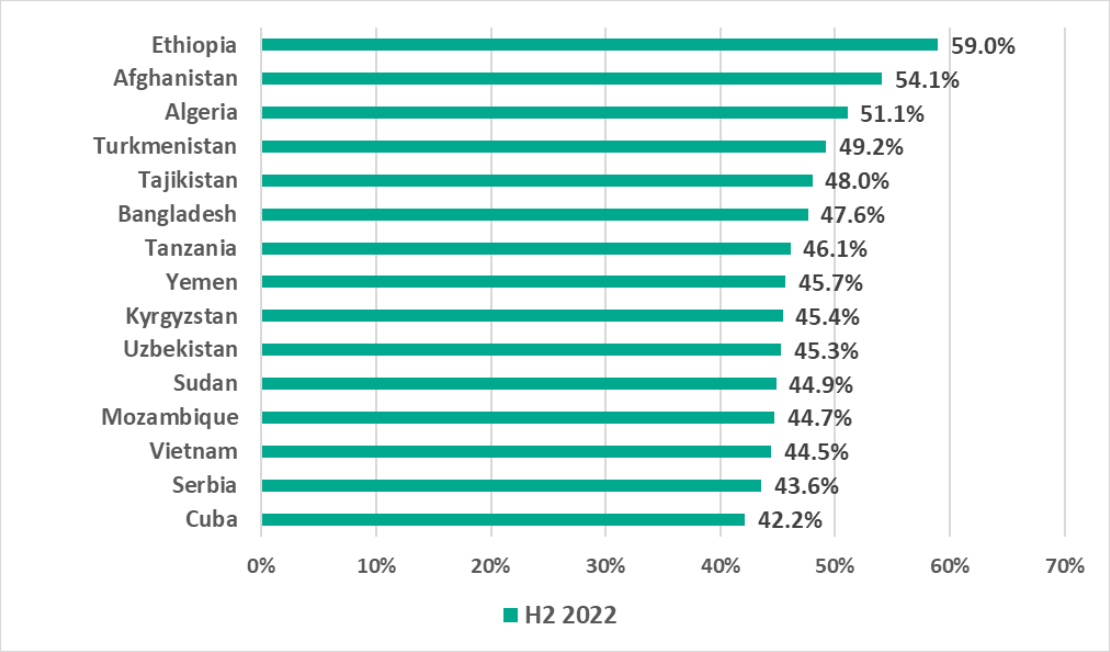
In different regions of the world, the percentage of ICS computers on which malicious activity was prevented ranged from 40.1% in Africa and Central Asia, which led the ranking, to 14.2% and 14.3%, respectively, in Western and Northern Europe, which were the most secure regions.

Regions of the world ranked by percentage of ICS computers on which malicious objects were blocked in H2 2022



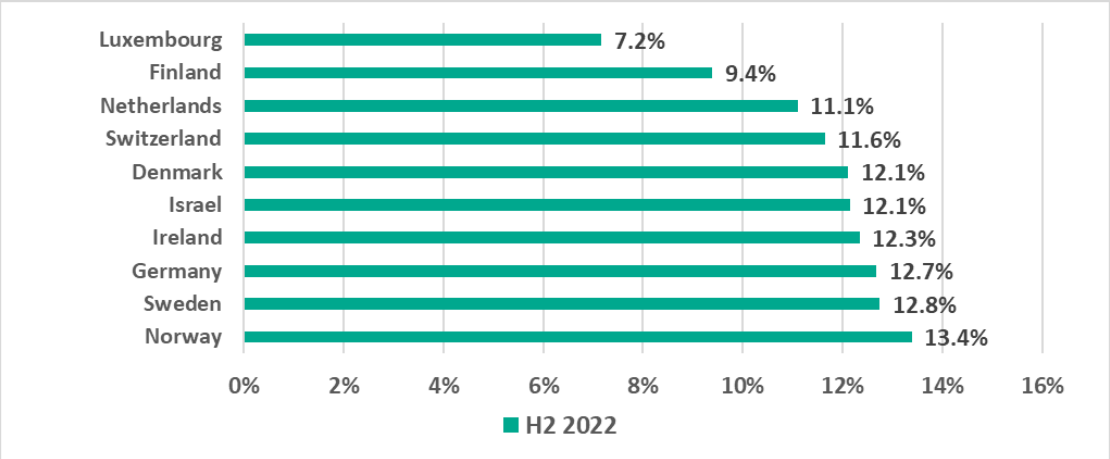
The situation in different countries can vary greatly – even within the same region. For example, in most countries of the Middle East the percentage of ICS computers on which malicious objects were blocked in H2 2022 was within the range from 30% to 40%. However, the percentage in Yemen was 45.7% and, at the same time, the percentage in Israel was 12.1%. As a result, Yemen was among the ten countries and territories with the highest percentage and Israel – among the ten countries and territories with the lowest percentage.

15 countries and territories with the highest percentage of ICS computers on which malicious objects were blocked in H2 2022



African and Central Asian countries were prevalent among the 15 countries and territories with the highest percentage of ICS computers on which malicious objects were blocked in H2 2022. In the Top 10 countries with the lowest percentage, all countries, with the exception of Israel, were European.

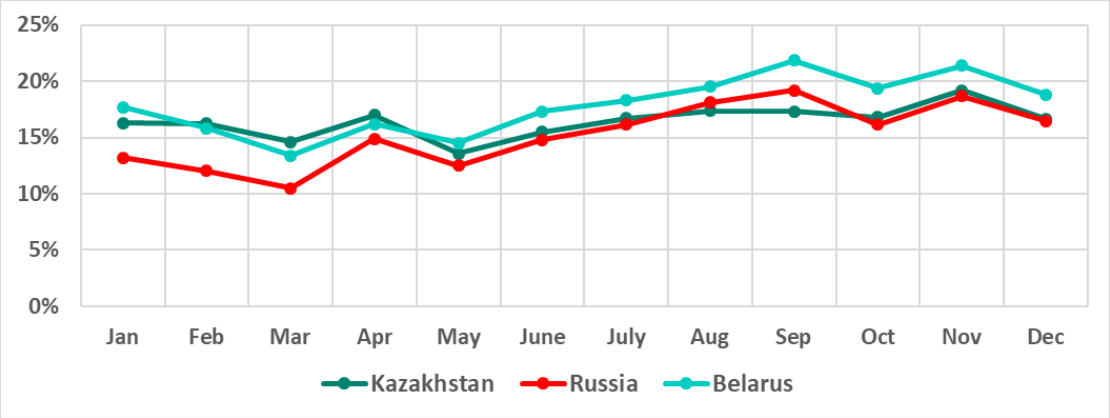
10 countries and territories with the lowest percentage of ICS computers on which malicious objects were blocked in H2 2022



In H2 2022, the greatest increase in the percentage of ICS computers on which malicious objects were blocked was observed in Russia (+9 p.p.) and Belarus (+6.9 p.p).

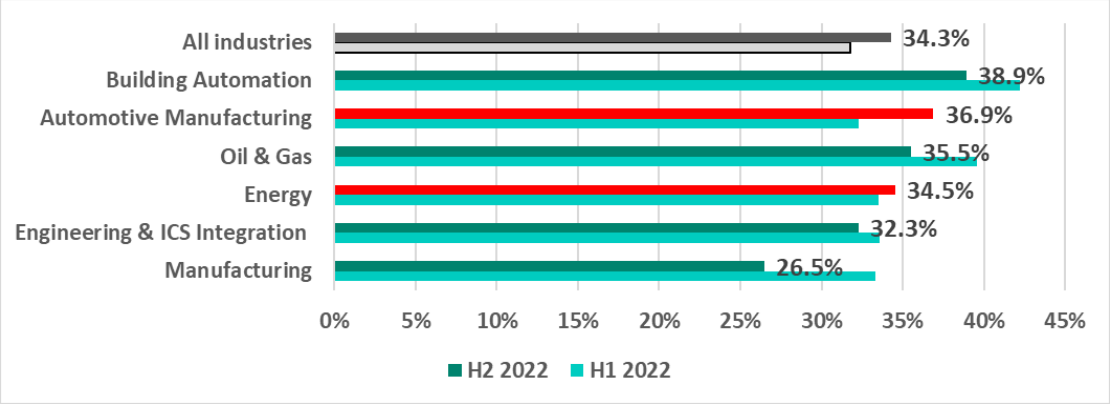
We noticed certain similarities in the monthly dynamics of the percentage of ICS computers on which malicious objects were blocked in these two countries. Kazakhstan was another country with similar dynamics.

Russia, Belarus and Kazakhstan. Percentage of ICS computers on which malicious objects were blocked, by months of 2022



The situation was also different in different industries. It can be seen in the diagram below that in H2 2022 the percentage of ICS computers on which malicious objects were blocked increased in the automotive industry (+4.6 p.p.) and in the energy sector (+1 p.p.). In other industries tracked, the percentage decreased.

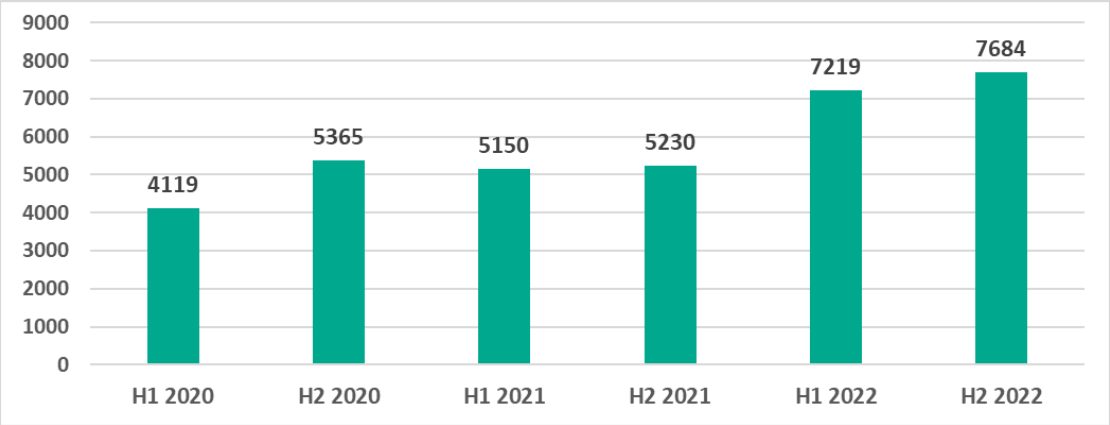
Percentage of ICS computers on which malicious objects were blocked in some industries



Variety of the malware detected

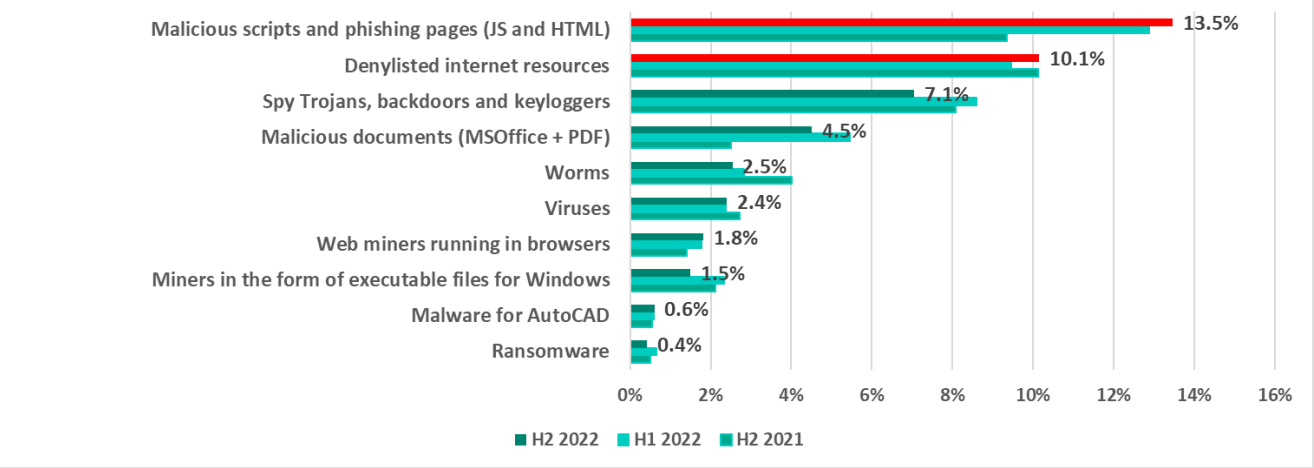
In H2 2022, Kaspersky security solutions blocked malware from 7,684 different families on industrial automation systems.

Number of malware families blocked on ICS computers



Malware categories

Malicious objects blocked by Kaspersky products on ICS computers fall into many categories. You can find a brief description of each category in a separate document.



Percentage of ICS computers* on which the activity of malicious objects from different categories was prevented

*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.

In H1 2022, we noted an increase in the percentage of ICS computers on which the malicious activity of several malicious object categories had been prevented.

In H2 2022, the percentage increased only for the two categories that led the ranking. These were malicious scripts and phishing pages (JS and HTML) and denylisted internet resources. In H2 2022, the percentage figures for other categories of malicious objects either decreased or remained unchanged.

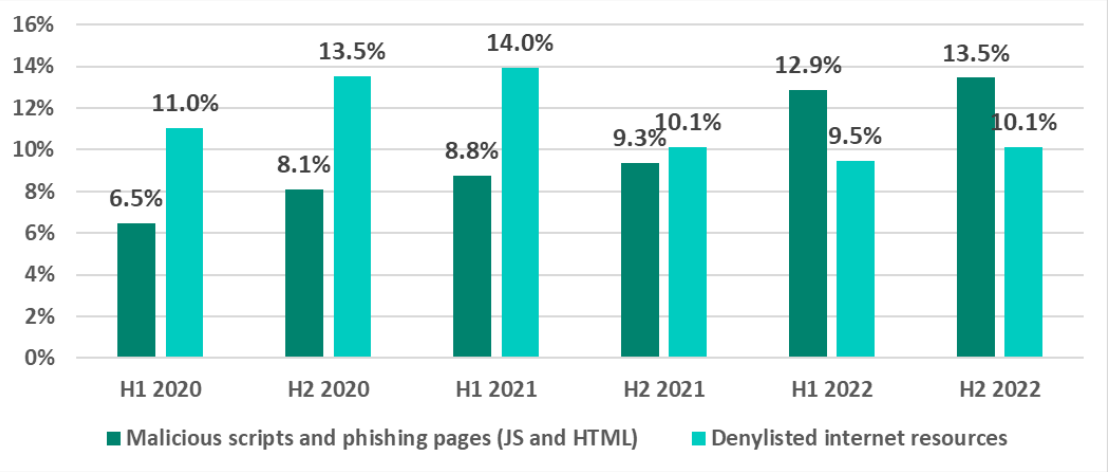
Malicious scripts and phishing pages (JS and HTML) and denylisted internet resources

Malicious scripts and phishing pages (JS and HTML) are distributed both online and via email. A significant part of denylisted internet resources are used to distribute malicious scripts and phishing pages.

Threat actors use malicious scripts for a broad range of tasks – from collecting information, tracking activity and redirecting browser requests to malicious web resources, to downloading various malicious programs or loading malware (e.g., spyware or tools for covert cryptocurrency mining) in the user's browser.

In 2022, malicious scripts and phishing pages climbed to the top of the ranking, pushing down the leader of many years, denylisted internet resources.

Percentage of ICS computers on which malicious scripts and phishing pages, and denylisted internet resources were blocked



The increase in the activity of threats in these two categories clearly made a major contribution to the increase, in H2 2022, of the percentage of ICS computers on which threats coming from the internet were blocked (see below).

Among regions of the world, the highest percentages of ICS computers on which denylisted internet resources were blocked were observed in Central Asia and in Russia (15.2% and 13.9%, respectively). It is no surprise that these regions led the ranking based on the percentage of ICS computers on which internet threats were blocked.

The same regions were also the largest contributors to the increase in the percentage of ICS computers on which malicious scripts and phishing pages were blocked. This was due to mass infections of websites (including those of

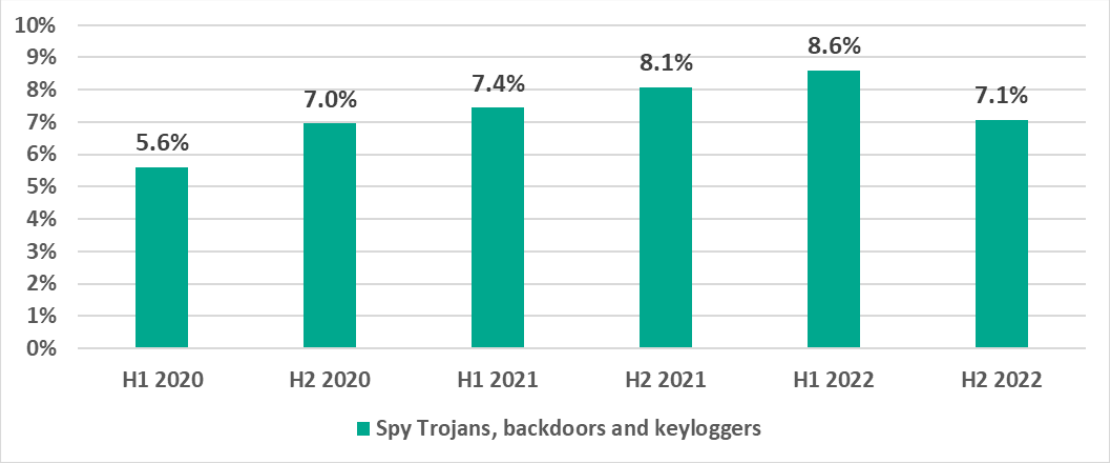
industrial organizations) that use the Bitrix CMS, which are mentioned above. Russia was the region where the highest percentage among all regions (18.2%) and the most significant increase (+11 p.p. compared to H1 2022) were observed. Central Asia was in fourth place among regions based on the former parameter (14.2%), but the region also saw a significant increase in that parameter in H2 2022 (+5.7 p.p.).

In other regions of the world, the percentage of ICS computers on which malicious scripts and phishing pages were blocked did not increase.

Spyware

The percentage of ICS computers on which spyware was blocked decreased by 1.5 p.p. This percentage had been growing during the period from 2020 through H1 2022.

Percentage of ICS computers on which spyware was blocked



It is worth noting that in H2 2022 in Africa the percentage of ICS computers on which spyware was blocked was 12%, which was the highest figure for any region of the world. The figures were also high in South-East Asia (10%) and the Middle East (9.8%).

Among countries and territories, this percentage was the highest in Yemen (22.3%), Algeria (18.3%), Sri Lanka (18.3%), and Serbia (17.2%).

Malicious documents (MSOffice+PDF)

The percentage of ICS computers on which malicious documents (MSOffice + PDF) were blocked also decreased – by 1 p.p., from 5.5% to 4.5%. Threat actors distributed malicious documents via phishing emails and used them in attacks designed to achieve initial infections of target computers.

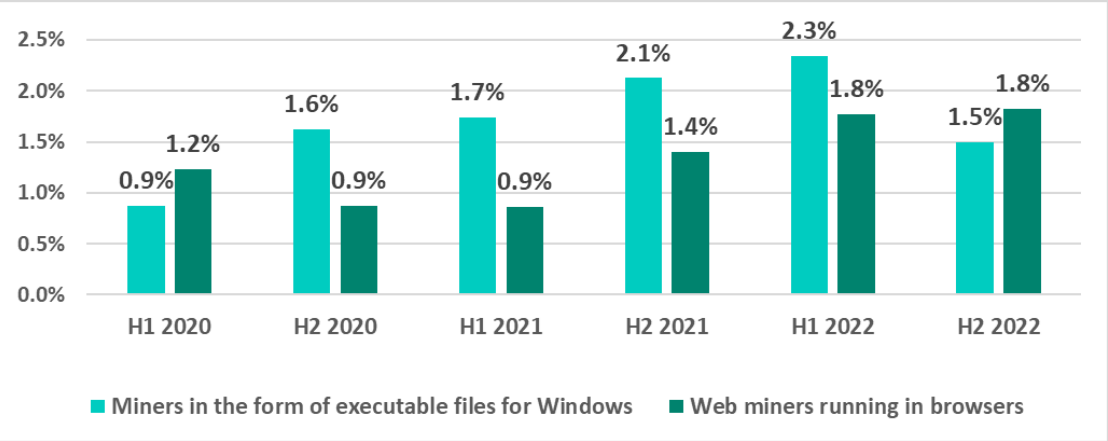
Among regions of the world, the highest percentage of ICS computers on which malicious documents were blocked was observed in Southern Europe (6.9%) and

Latin America (6.9%). These same regions also had the highest percentage of ICS computers on which email threats were blocked.

Malicious cryptocurrency miners

The percentage of ICS computers on which malicious cryptocurrency miners implemented as Windows executable files were blocked decreased by 0.8 p.p. The figures for web miners remained at the same level as in H1 2022.

Percentage of ICS computers on which malware for covert cryptocurrency mining was blocked



Cryptocurrency miners are often distributed via websites to which users have been redirected by malicious scripts. These are hosted by threat actors on media resources and sites providing pirated content.

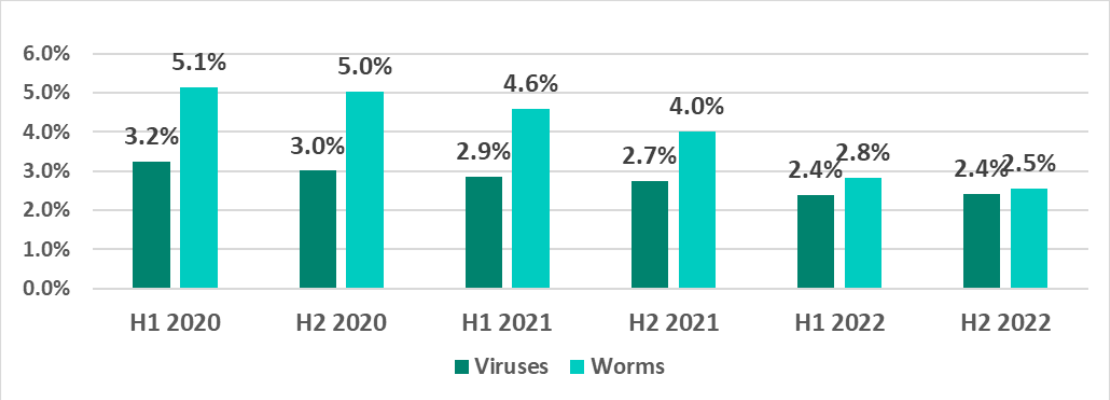
In H2 2022, regions with the highest percentage of ICS computers on which cryptocurrency miners were blocked were: Central Asia (miners implemented as Windows executable files, 3.8%) and Africa (web miners, 3.4%).

The three countries with the highest percentage of web miners blocked were Yemen (9.3%), Egypt (7.8%) and, unexpectedly, a European country, Serbia (7.5%).

Viruses and worms

The percentage of ICS computers on which viruses and worms were blocked continued to decrease. We believe this indirectly reflected systematic work related to deploying security solutions in OT environments, which helps eliminate pockets of infection and prevent self-propagating malware from spreading.

Percentage of ICS computers on which viruses and worms were blocked



Viruses and worms are distributed on ICS networks via removable devices, network folders, infected files (including backups) and network attacks on outdated software, such as Radmin2.

The decrease in the percentage of ICS computers on which such malware was blocked was due, among other things, to more careful scanning of removable devices.

At the same time, the percentage of ICS computers on which worms were detected remained very high in Africa (7.1%), which, as a result, topped the ranking of regions based on the percentage of ICS computers on which threats were blocked when connecting removable devices. Viruses, on the other hand, remained a relevant threat in South-East Asia (8.1%).

There is a number of relatively old viruses and worms which are still spreading, although their command-and-control servers have long been shut down. In addition to undermining the security of infected systems, e.g., by opening network ports and changing settings, these older worms and viruses can potentially cause software crashes or denial-of-service conditions.

New versions of worms are also sometimes found on ICS networks. Threat actors use these worms to spread spyware, ransomware and malicious miners in target networks. In most cases, these worms spread by exploiting vulnerabilities in network services (such as SMB and RDP) that have been fixed by vendors but are still unpatched in OT networks, using previously stolen authentication credentials or brute forcing passwords.

Malware for AutoCAD

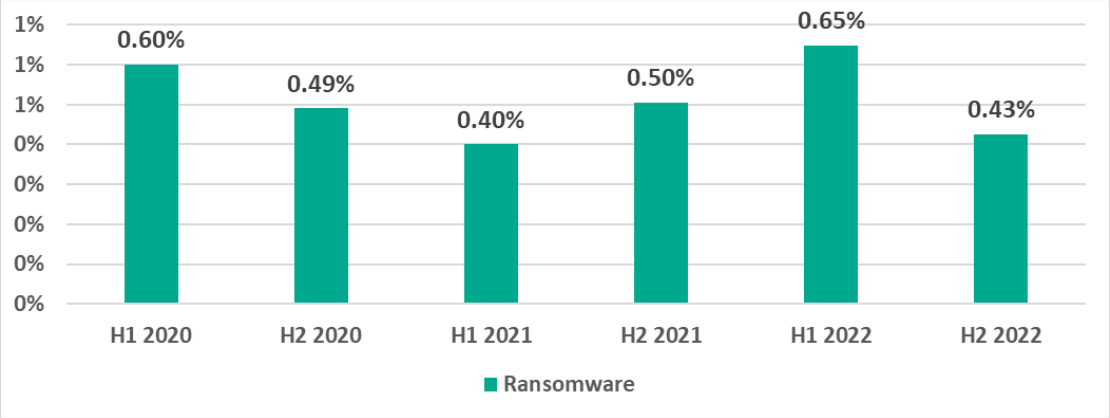
Malware for AutoCAD, including viruses, was detected primarily in East Asia (3.1%) on computers that are part of OT networks, including network folders and engineering workstations.

The ranking of countries based on the percentage of ICS computers on which malware for AutoCAD was blocked was led by Ethiopia (5.8%), Sri Lanka (5.0%), and China (4.9%). Percentage figures for other countries ranged between 3.2% and 0.01%.

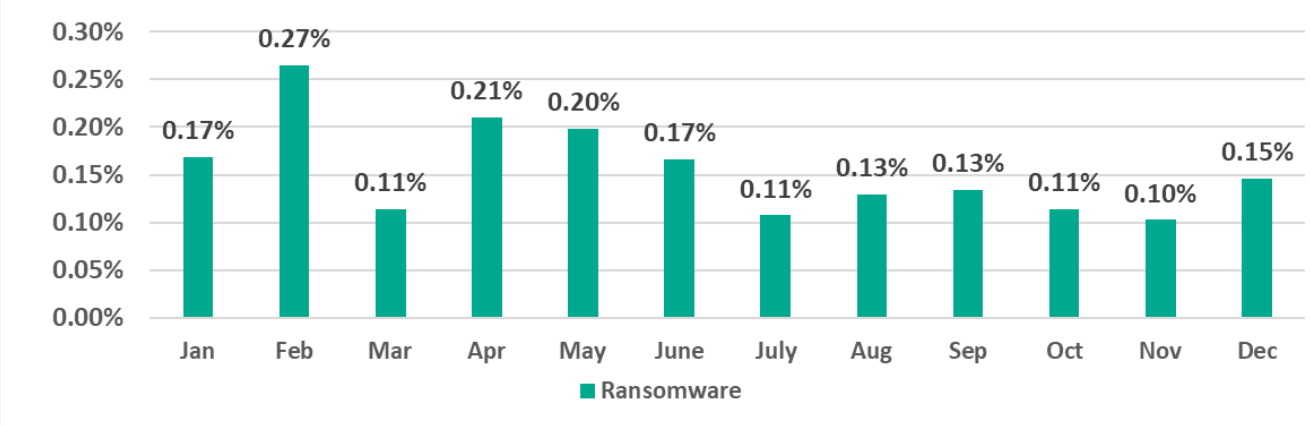
Ransomware

Ransomware was blocked in H2 2022 on 0.43% of ICS computers.

Percentage of ICS computers on which ransomware was blocked



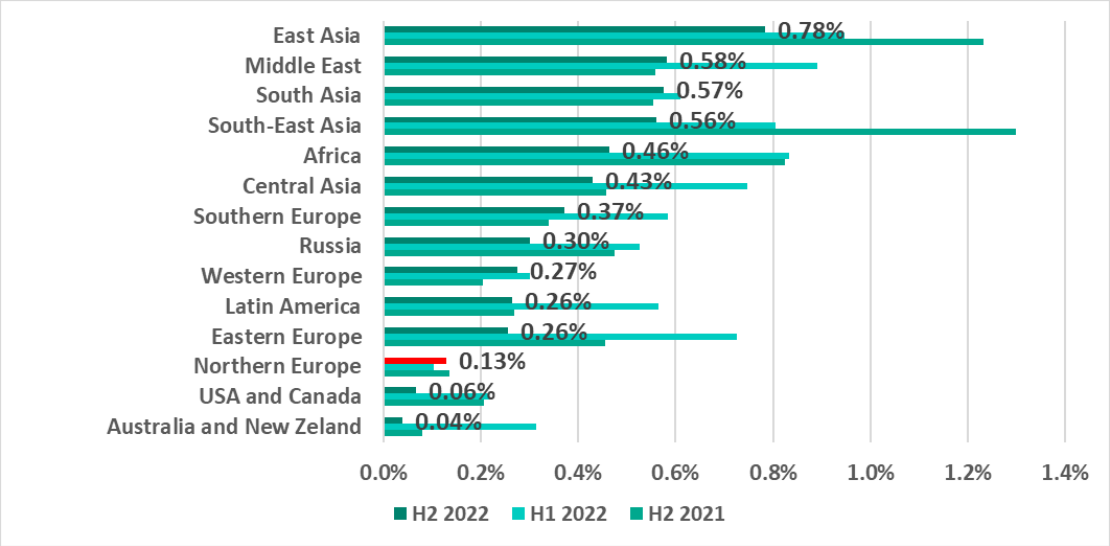
During all of 2022, the highest percentage of ICS computers on which ransomware was blocked was observed in February (0.27%), the lowest in November (0.10%).



Percentage of ICS computers on which ransomware was blocked, January – December 2022

In H2 2022, the percentage of ICS computers attacked by ransomware decreased in almost all regions. The only exception was Northern Europe, where a small increase (+0.03 p.p.) was observed.

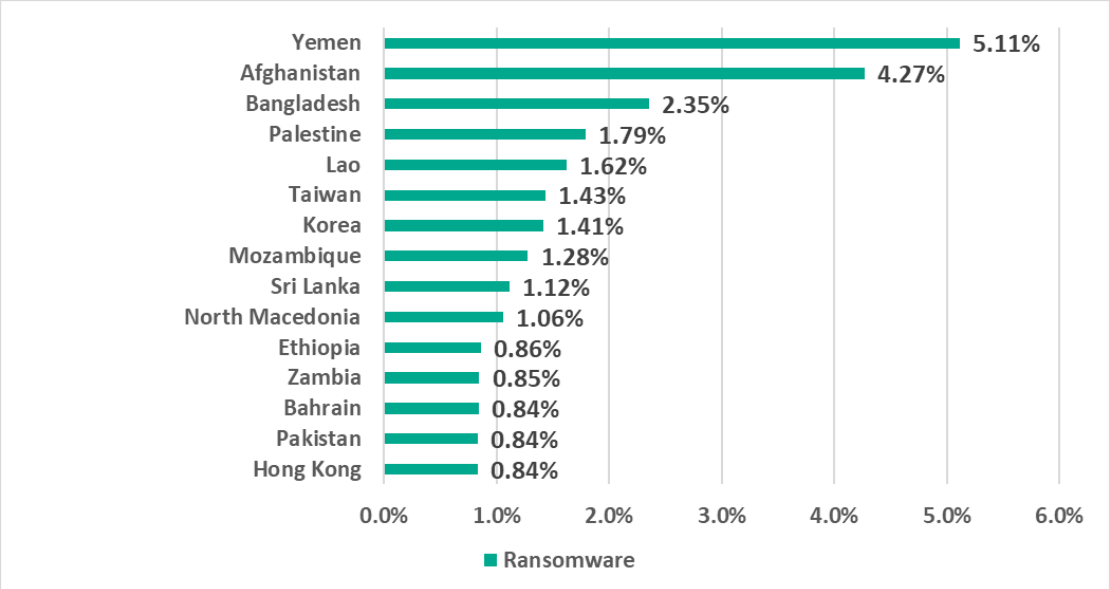
Regions ranked by percentage of ICS computers on which ransomware was blocked, H2 2022



East Asia and the Middle East continued to lead the ranking, while Africa was pushed down from third place by South and South-East Asia.

In H2 2022, Yemen and Afghanistan led the TOP 15 ranking of countries and territories with the highest percentage of ICS computers on which ransomware was blocked. In Afghanistan, the percentage increased in H2 2022 by 3.22 p.p., which was the greatest increase for any country.

15 countries and territories with the highest percentage of ICS computers on which ransomware was blocked, H2 2022



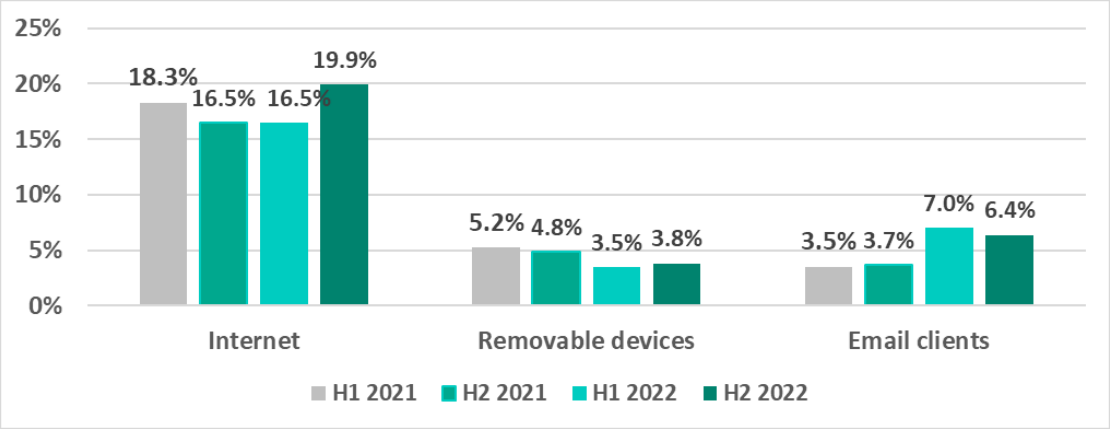
Note that in H2 2022, the ranking included one European country, North Macedonia.

Main threat sources

The internet, removable devices and email clients remained the main sources of threats for computers in the operational technology infrastructure of organizations. It should be noted that, in some cases, the sources of blocked threats could not be reliably identified.

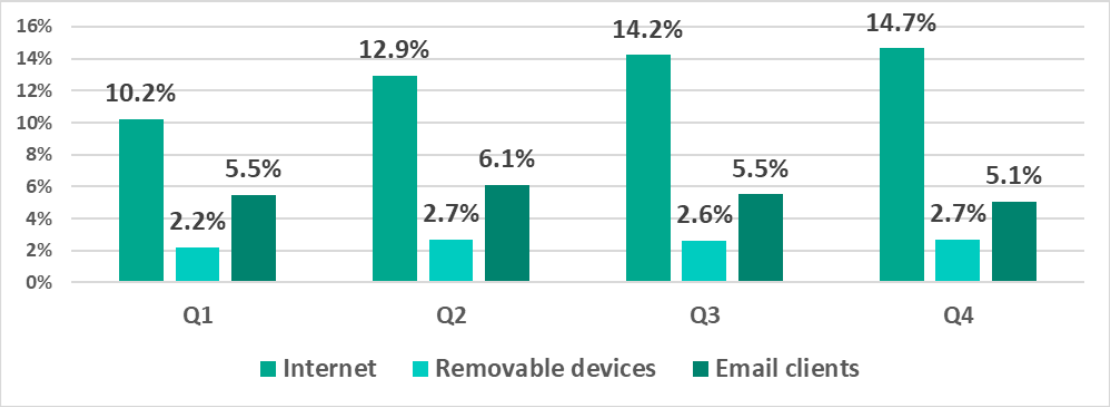
World

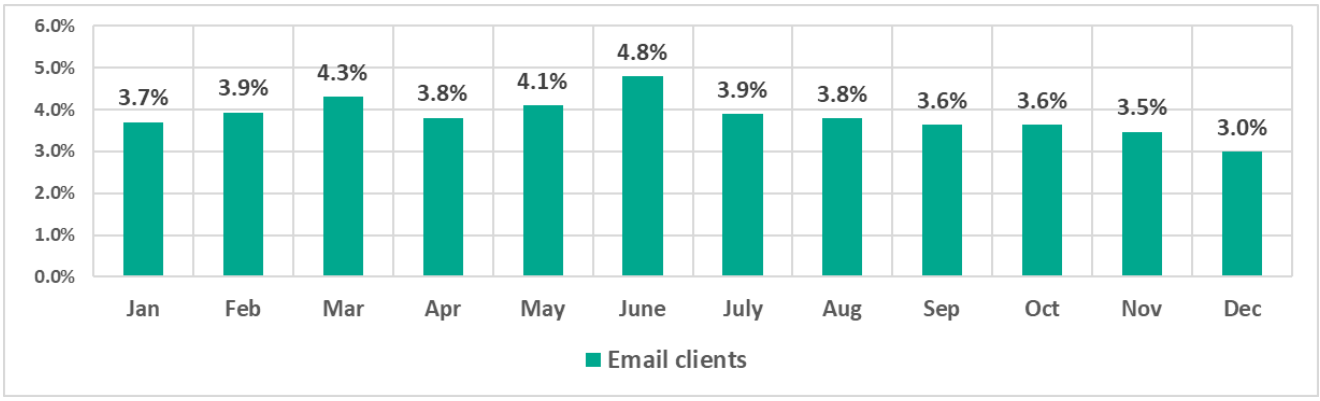
Percentage of ICS computers on which malicious objects from different sources were blocked



The percentage of ICS computers on which internet threats were blocked increased from one quarter to the next throughout 2022. At the same time, the percentage of email threats peaked in Q2, with a noticeable increase in the percentage figures recorded in June.

Percentage of ICS computers on which malicious objects from different sources were blocked, Q1 – Q4 2022

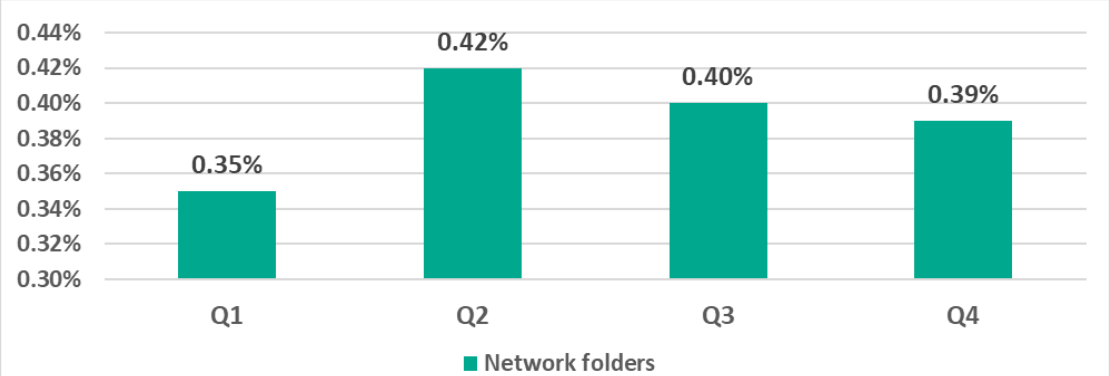




Percentage of ICS computers on which malicious objects from email were blocked, January – December 2022

There was also a noticeable increase in Q2 2022 in the percentage of ICS computers on which threats were blocked in network folders.

Percentage of ICS computers on which malicious objects were blocked in network folders, Q1 – Q4 2022



In H2 2022, threats whose source was network folders were blocked on 0.6% of ICS computers.

As with overall statistics on all threats, the percentage of ICS computers on which malicious objects from different sources were blocked varied according to country and region.

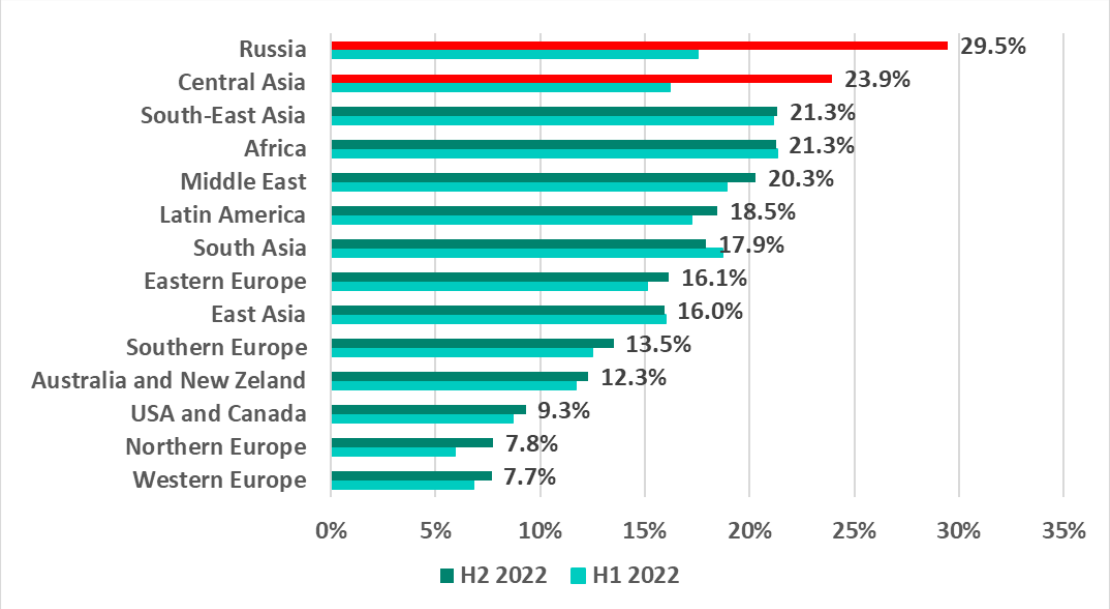
Regions and countries

Internet

In H2 2022, a very significant growth in the percentage of ICS computers on which internet threats were blocked – 12 p.p. and 7.8 p.p., respectively – was recorded in the regions Russia and Central Asia. As a result, these regions took

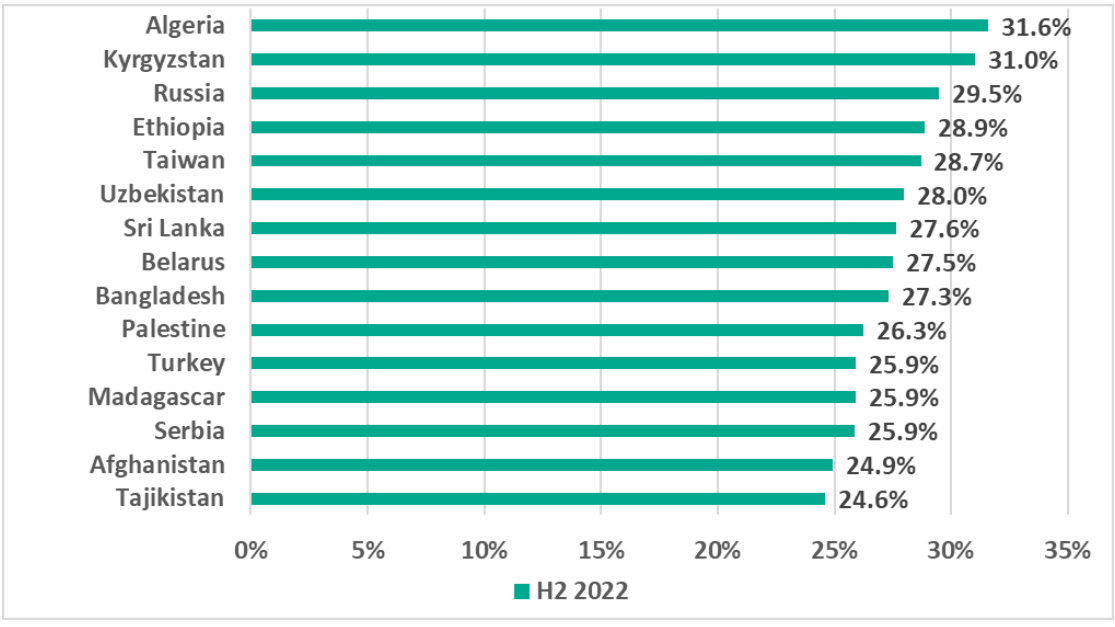
top positions in the ranking based on this parameter, displacing traditional leaders – Africa, South-East Asia, and the Middle East.

Regions ranked by percentage of ICS computers on which internet threats were blocked, H2 2022



As a result of a sharp increase in the percentage of ICS computers on which internet threats were blocked in Russia, the country became one of the top three countries and territories based on this parameter.

15 countries and territories with the highest percentage of ICS computers on which internet threats were blocked, H2 2022

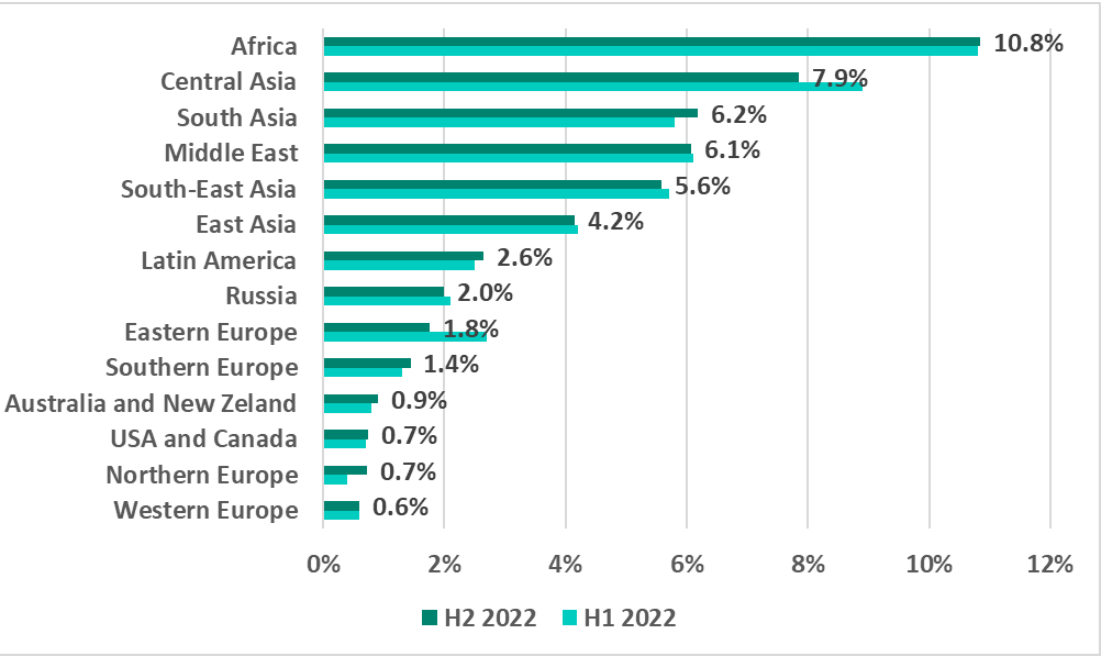


It should be noted that such high positions in both rankings are not characteristic of Russia.

Removable devices

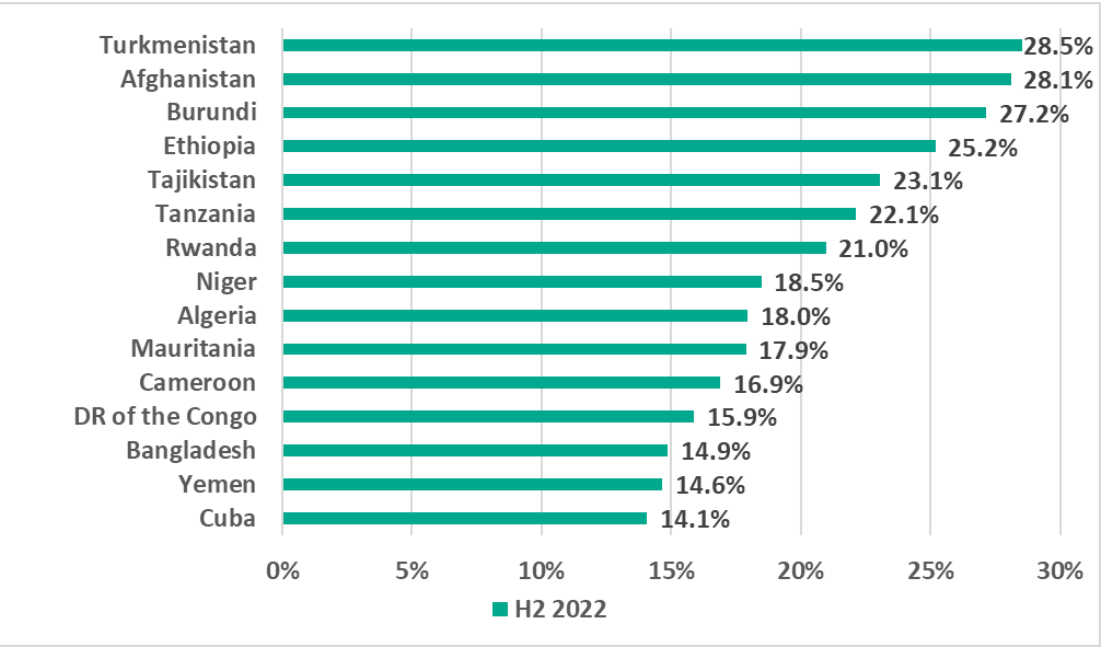
As per tradition, Africa topped the ranking of regions based on the percentage of ICS computers on which malware was blocked when removable devices were connected.

Regions ranked by percentage of ICS computers on which malware was blocked when removable devices were connected, H2 2022



African countries were also prevalent in the ranking of 15 countries and territories with the highest percentage of ICS computers on which malware was blocked when removable devices were connected.

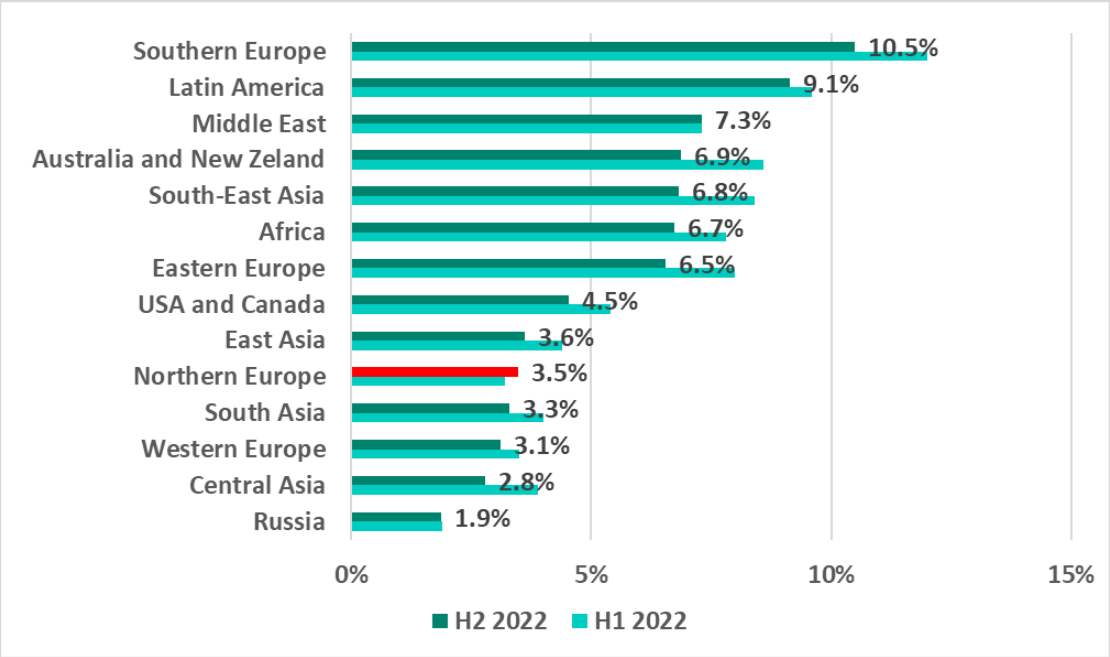
15 countries and territories with the highest percentage of ICS computers on which malware was blocked when removable devices were connected, H2 2022



Email clients

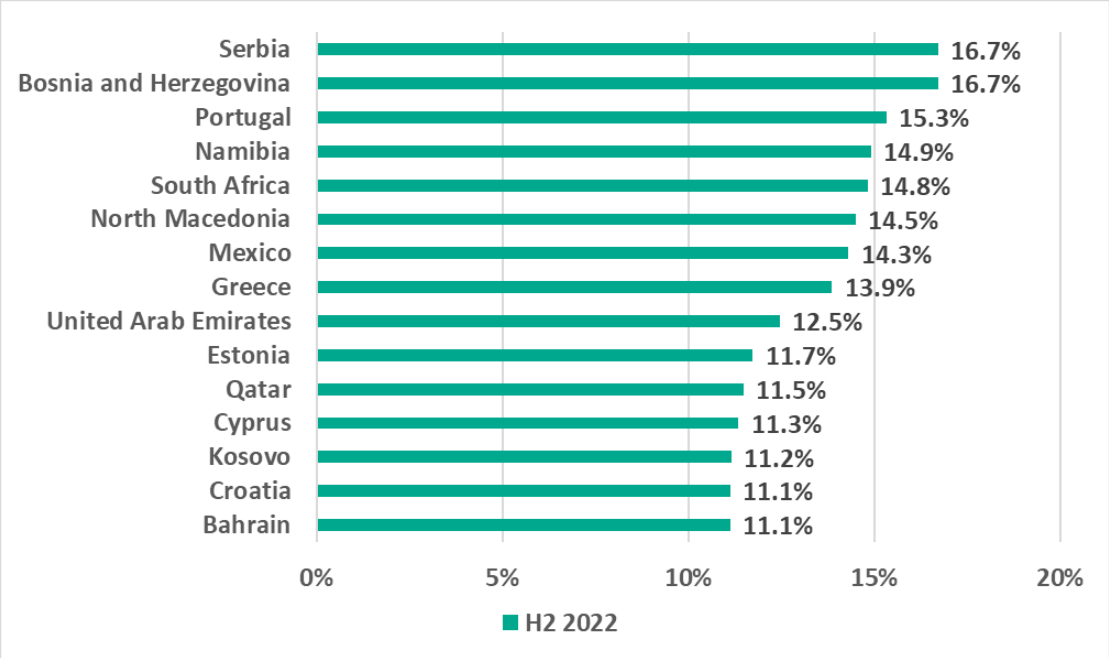
Southern Europe, which, in H1 2022, topped the ranking of regions based on the percentage of ICS computers on which malicious email attachments and phishing links were blocked, remained at the top of the ranking in H2. Northern Europe was the only region in which the percentage increased in H2 2022, albeit insignificantly (+0.3 p.p.).

Regions ranked by percentage of ICS computers on which malicious email attachments and phishing links were blocked, H2 2022



The list of 15 countries and territories with the highest percentage of ICS computers on which email attachments and phishing links were blocked included countries located in Southern Europe, as well as other regions.

15 countries and territories with the highest percentage of ICS computers on which malicious email attachments and phishing links were blocked, H2 2022

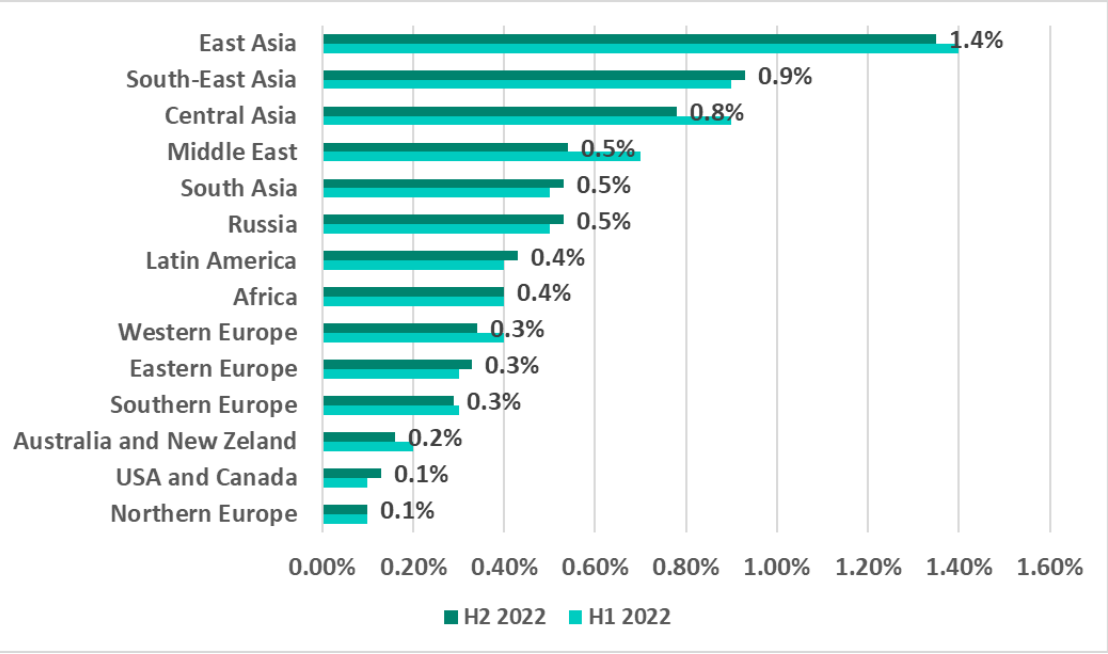


We recommend that security experts in these countries make a special emphasis on protecting enterprise employees from phishing emails.

Network folders

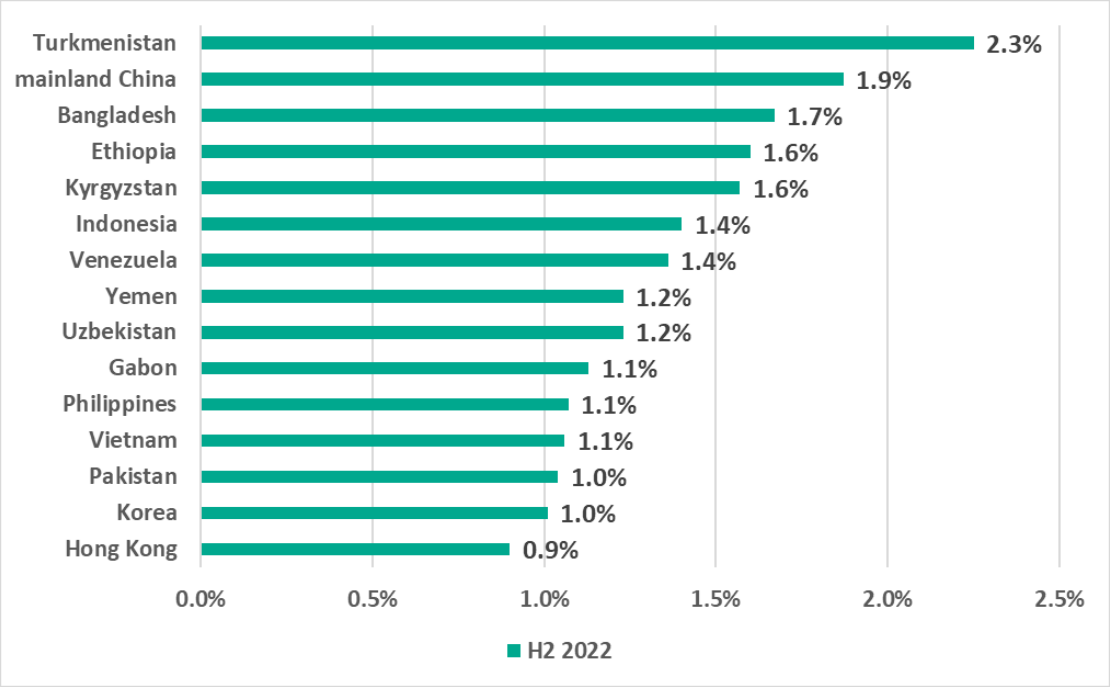
Network folders was a minor source of malicious objects. The highest percentage of ICS computers on which threats were blocked in network folders was seen in East, South-East and Central Asia.

Regions ranked by percentage of ICS computers on which malicious objects were blocked in network folders, H2 2022



Turkmenistan, mainland China and Bangladesh led the Top 15 ranking of countries and territories with the highest percentage of ICS computers on which malicious objects were blocked in network folders in H2 2022.

15 countries and territories with the highest percentage of ICS computers on which malicious objects were blocked in network folders, H2 2022



Methodology used to prepare statistics

This report is based on an analysis of statistical data collected through the Kaspersky Security Network (KSN), a distributed antivirus network. The data was received from those KSN users who have given 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 provides an opportunity for our clients to improve the reaction speed of our security solution to new and unknown threats. It also improves the detection quality of the solution due to the access to the cloud infrastructure where data on malicious objects is stored. This data is only accessible via the cloud due to the size of the database and the resources required to store it locally.

The information transferred by the user includes only the types and categories of data described in the relevant KSN Agreement. This information not only

assists in analyzing the threat landscape, but is also needed to detect new threats, including targeted attacks and APTs.[1].

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.

For the purposes of this report, "attacked computers" are those on which Kaspersky security solutions blocked one or more threats during the reporting period (in the diagrams above, a reporting period can be a month, a six-month period or a year, depending on the context). When determining the 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 depersonalized information during the reporting period.

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

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