kaspersky

Threat landscape for industrial automation systems

Statistics for H2 2023

Kaspersky ICS CERT

19.03.2024 Version 1.0

2023 in numbers

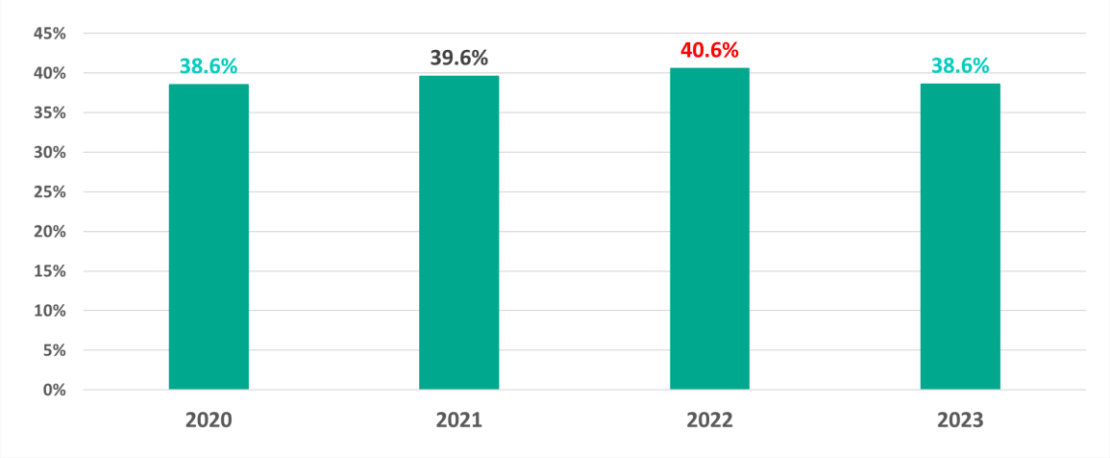
Parameter	H1 2023	H2 2023	2023
Global percentage of attacked ICS computers	34.0%	31.9%	38.6%
Main threat sources			
Internet	19.3%	18.1%	22.8%
Email clients	6.0%	4.0%	5.4%
Removable media	3.4%	1.9%	3.2%
Network folders	0.49%	0.25%	0.45%
Percentage of ICS computers on which malicious objects from different categories were blocked			
Malicious scripts and phishing pages (JS and HTML)	12.7%	10.9%	14.7%
Denylisted internet resources	11.3%	10.1%	13.7%
Spy Trojans, backdoors and keyloggers	6.1%	5.3%	7.1%
Malicious documents (Microsoft Office and PDF)	4.0%	2.9%	4.0%
Worms	2.3%	2.1%	3.0%
Viruses	2.4%	2.1%	2.8%
Web miners running in browsers	1.3%	0.76%	1.3%
Miners in the form of executable files for Windows	0.59%	0.85%	1.1%
Ransomware	0.32%	0.25%	0.37%

2023

Back to the minimum

Following the increase of 2021 and 2022, the percentage of ICS computers on which malicious objects were blocked dropped by 2 pp and returned to the same level as in 2020.

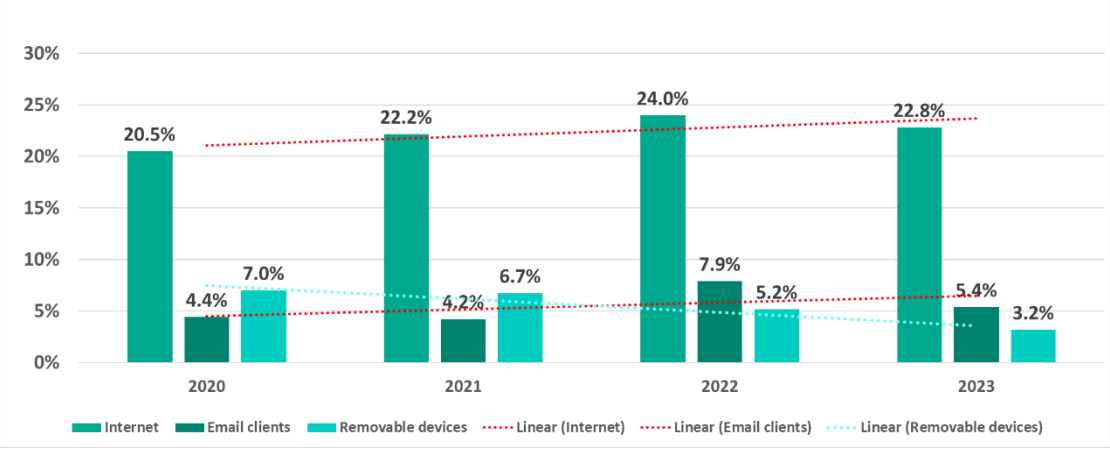
Percentage of ICS computers on which malicious objects were blocked, 2020-2023



Compared with 2020, the contributions of the main threat sources in 2023 changed as follows:

- The percentage of ICS computers on which internet and email threats were blocked increased.
- The percentage of ICS computers on which removable media threats were blocked more than halved.

Percentage of ICS computers on which malicious objects from various sources were blocked, 2020–2023

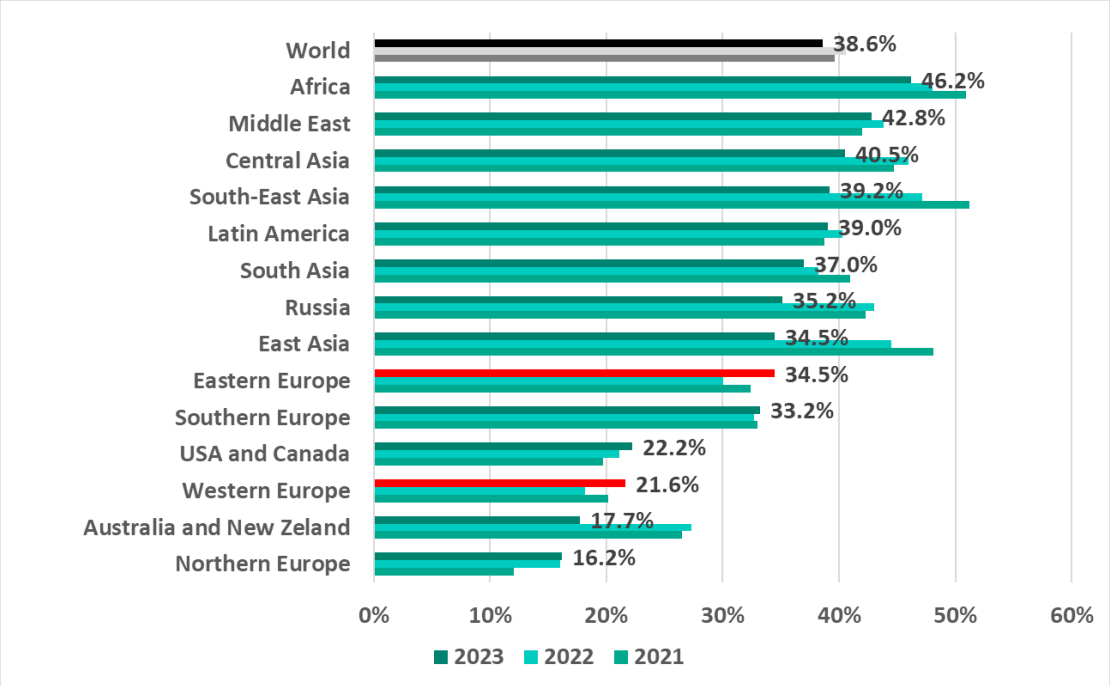


Red lines of 2023

By the end of 2023, the percentage of ICS computers on which malicious objects were blocked increased in two regions:

- Eastern Europe, by 4.4 pp
- Western Europe, by 3.5 pp

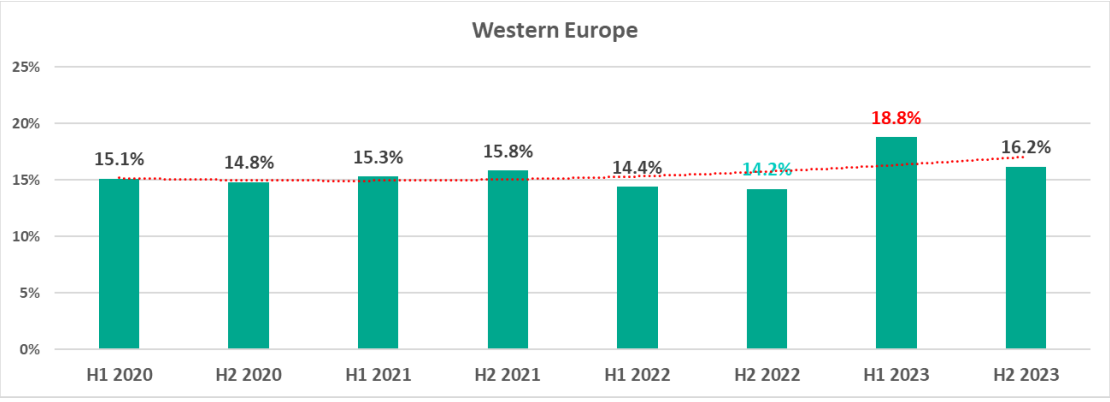
Regions and world. Percentage of ICS computers on which malicious objects were blocked, 2021-2023



As you can see from the charts below, the situations in these two regions differ significantly.

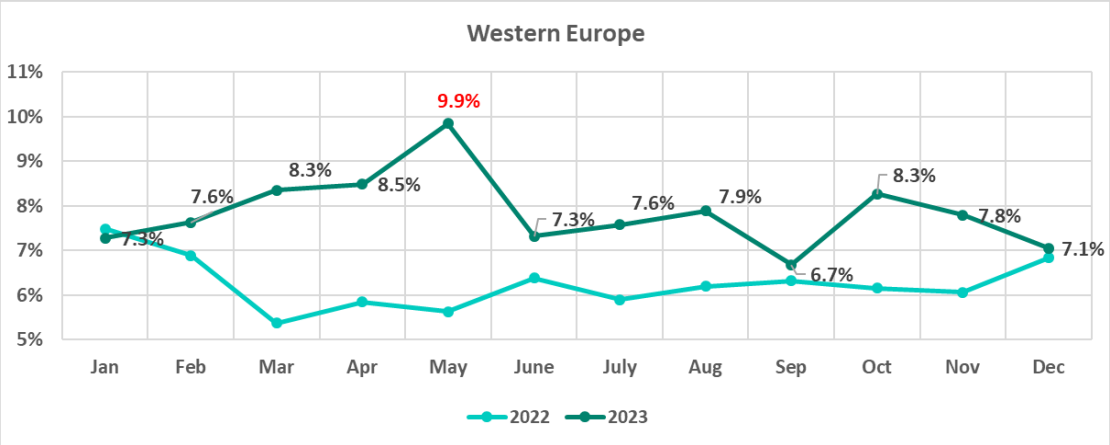
H1 2023 saw the largest share of attacked ICS computers in Western Europe in the period from 2020 through 2023. H2 ranked second.

Western Europe. Percentage of ICS computers on which malicious objects were blocked, by half year, 2020–2023



The percentage of attacked ICS computers in Western Europe each month in 2023, with the exception of January, represented a year-on-year increase. It peaked in May, when Europe saw a spate of phishing attacks, with industrial organizations among the targets.

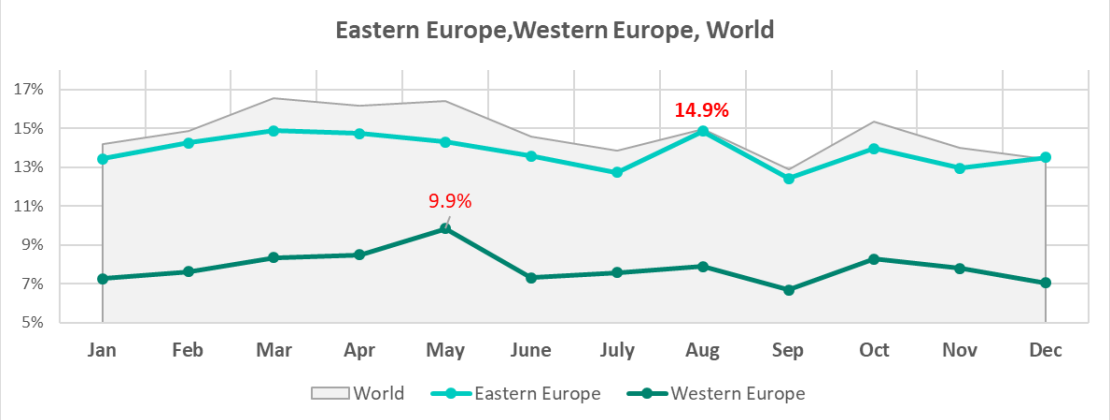
Western Europe. Percentage of ICS computers on which malicious objects were blocked, January–December 2022 and 2023



In Eastern Europe, H1 2023 saw the lowest figures since 2020, and H2, the highest percentage of attacked ICS computers in 2020-2023 (30.9%). Malicious scripts and phishing pages contributed the bulk of the increase.

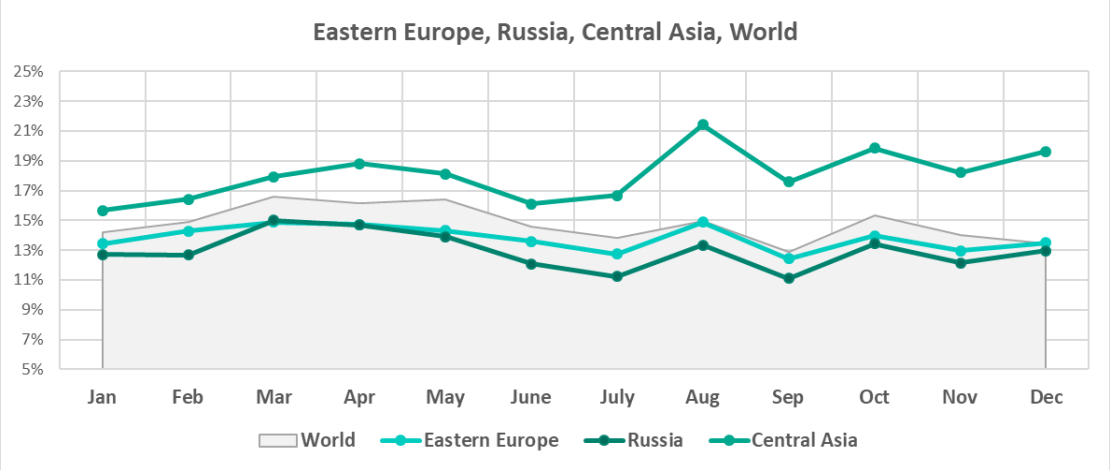
The monthly statistics for Eastern Europe differ from that for Western Europe.

Eastern Europe, Western Europe, world. Percentage of ICS computers on which malicious objects were blocked, January–December 2022 and 2023



That said, we can see certain similarities in the changes in Eastern Europe, Russia, and Central Asia.

Eastern Europe, world. Percentage of ICS computers on which malicious objects were blocked, January–December 2022 and 2023



The monthly changes in the percentages of attacked ICS computers in these regions correlate with the global trend.

Details on Eastern Europe can be found in the H2 2023 statistics below.

Statistics for H2 2023

In the second half of 2023, the percentage of ICS computers on which malicious objects were blocked decreased from the first half of the year.
Most of the statistical indicators dropped accordingly. Yet, there are subtleties we would like to draw attention to, as they highlight dangerous spots on the cyberthreat landscape.

Red lines

World

The percentage of ICS computers on which malicious objects were blocked **increased in only one category**

- **Miners in the form of executable files for Windows,** by 1.4 times.
  Russia, Eastern Europe, and South Asia were the regions that saw noticeable increases in the percentage of ICS computers on which miners in the form of executable files for Windows were blocked.
  Central Asia led this ranking, followed by **Russia**.

Regions

Africa

Africa **leads the rankings** for

- Percentage of ICS computers on which **spyware** was blocked
- Percentage of ICS computers on which **worms** were blocked
- Percentage of ICS computers on which **web miners** were blocked
- Percentage of ICS computers on which **removable media** threats were blocked.

It is safe to say that the region continues to occupy last place in the ranking of regions in terms of the level of information security maturity of industrial enterprises.

Southern Europe

- **Leads** the regions by percentage of ICS computers on which email threats **(malicious email attachments and phishing links)** were blocked. This is a worrying sign. Phishing is one of the preferred initial compromise methods for attackers focused on targeted attacks – APT, ransomware, BEC, and hacktivist attacks.
- **Second** among the regions by percentage of ICS computers on which **malicious documents** were blocked.
- One of the two regions where the percentage of ICS computers on which **spyware** was blocked rose in the six-month period. This has likely led to an increased flow of compromised authentication credentials into the technology systems of industrial enterprises, increasing the risk of subsequent targeted attacks.

Eastern Europe

- One of three regions that saw an **increase in the percentage** of ICS computers on which malicious objects were blocked in H2 2023 compared to the previous six months: **4.6 pp**, the highest of any region.
- In the six months of the year, the **region saw a rise in the percentage** of ICS computers on which the following were blocked:
  - **Malicious scripts and phishing pages:** by 2.9 pp.
  - **Miners in the form of executable files for Windows:** by 0.9 pp.
  - **Worms:** by 0.43 pp (the only region where this percentage rose).
  - **Denylisted internet resources:** by 0.4 pp (the only region where this percentage rose).

- **Second** among the regions by percentage of ICS computers on which **malicious scripts and phishing pages were blocked**.

All these changes do not in any way support a trend towards an increase in the overall level of security maturity of industrial enterprises. As we can see, the availability of OT systems for different types of threats is growing for reasons that are primarily related to the human factor and the lack of funding for information security of industrial facilities that is common in the region.

Russia

- **Second** among the regions by percentage of ICS computers on which **miners in the form of executable files for Windows** were blocked.

Central Asia

- **Leads** the regions by percentage of ICS computers on which **denylisted internet resources** were blocked.
- **Leads** by percentage of ICS computers on which **miners in the form of executable files for Windows** were blocked.
- **Second among the regions** by percentage of ICS computers on which **worms** were blocked.

The region has traditionally had a very low overall information security maturity. Industrial organizations in the region should clearly pay more attention to employee training.

East Asia

- **Leads** the regions by percentage of ICS computers on which **malware for AutoCAD** was blocked.
- **Second** among the regions by percentage of ICS computers on which **viruses** were blocked.
- **In the region, spyware ranked second** among malware categories by percentage of ICS computers on which it was blocked.

South-East Asia

- **Leader** among the regions by percentage of ICS computers on which **viruses** were blocked.
- **In the region, viruses ranked third** among malware categories by percentage of ICS computers on which they were blocked.

Industrial organizations in the region need to ensure better protection of their systems in the technology network with at least a minimum set of protective measures and tools.

South Asia

- **Leader** (tied with the Middle East) among the regions by percentage of ICS computers on which **ransomware** was blocked.

Middle East

- **Leads** (tied with South Asia) the regions by percentage of ICS computers on which **ransomware** was blocked. Industrial organizations in the region clearly need to consider the risk of extortion from small, obscure groups and individual attackers – they are the main contributors to the threat detection statistics.
- **Second** among the regions by percentage of ICS computers on which **spyware** was blocked.
- **Second** among the regions by percentage of ICS computers on which **web miners** were blocked.

Latin America

- **Leads** the regions by percentage of ICS computers on which **malicious scripts and phishing pages** were blocked. Industrial organizations in the region should also consider the risk of targeted attacks on technology network segments to be high.
- **Leader** by percentage of ICS computers on which **malicious documents** were blocked. This appears to be a consequence of the high percentage of systems that have experienced phishing. Malicious documents (e.g., attached to an email or available to download via a link) are one of the most popular ways for attackers to compromise via phishing emails.
- Second **among the regions by percentage of ICS computers on which** malicious email attachments and phishing links **were blocked**.

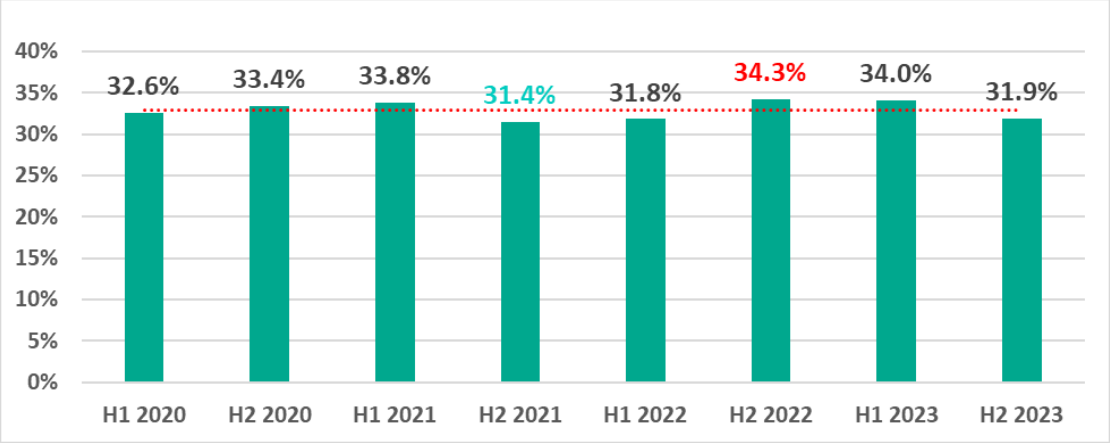
Australia and New Zealand

- The only region where the percentage of ICS computers on which **malicious documents** were blocked rose in the six-month period.

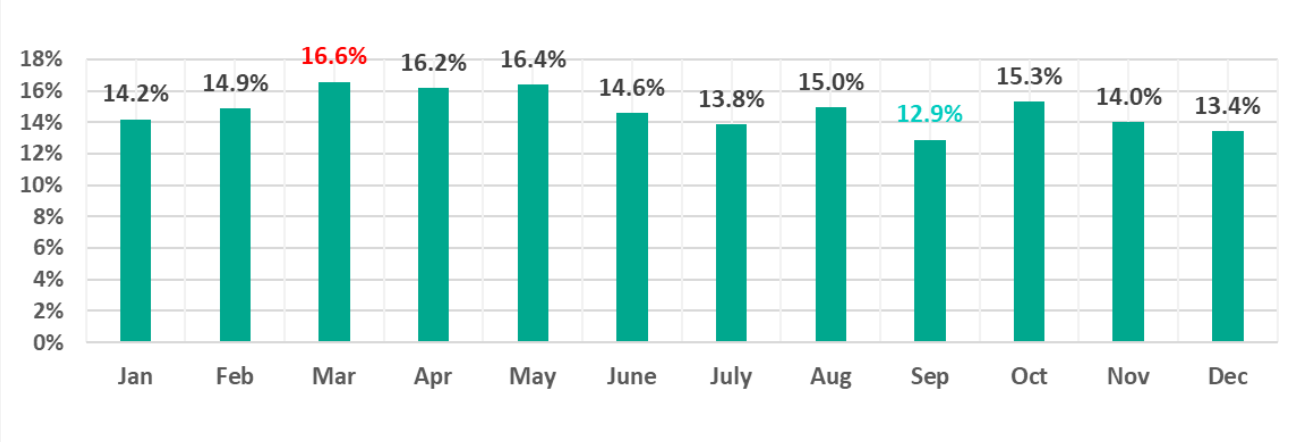
Global statistics across all threats

In the second half of 2023, the percentage of ICS computers on which malicious objects were blocked decreased by 2.1 pp compared to the previous six months to 31.9%.

Percentage of ICS computers on which malicious objects were blocked, by half year

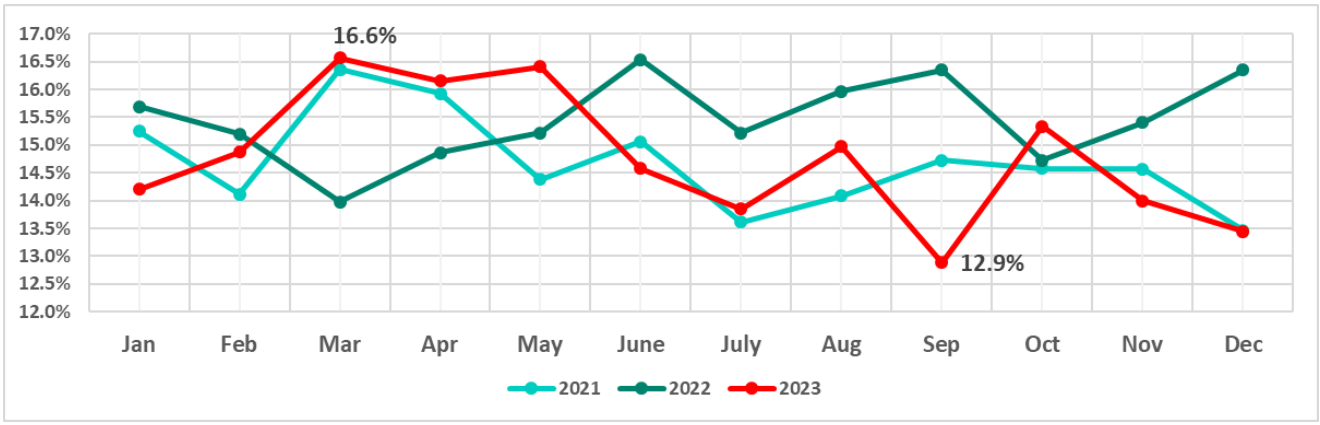


The percentage of ICS computers on which malicious objects were blocked in 2023 was highest in March and lowest in September.



Percentage of ICS computers on which malicious objects were blocked, January-December 2023

The March and September percentages represented the highest monthly figures both for 2023 and the three-year period of 2021-2023.



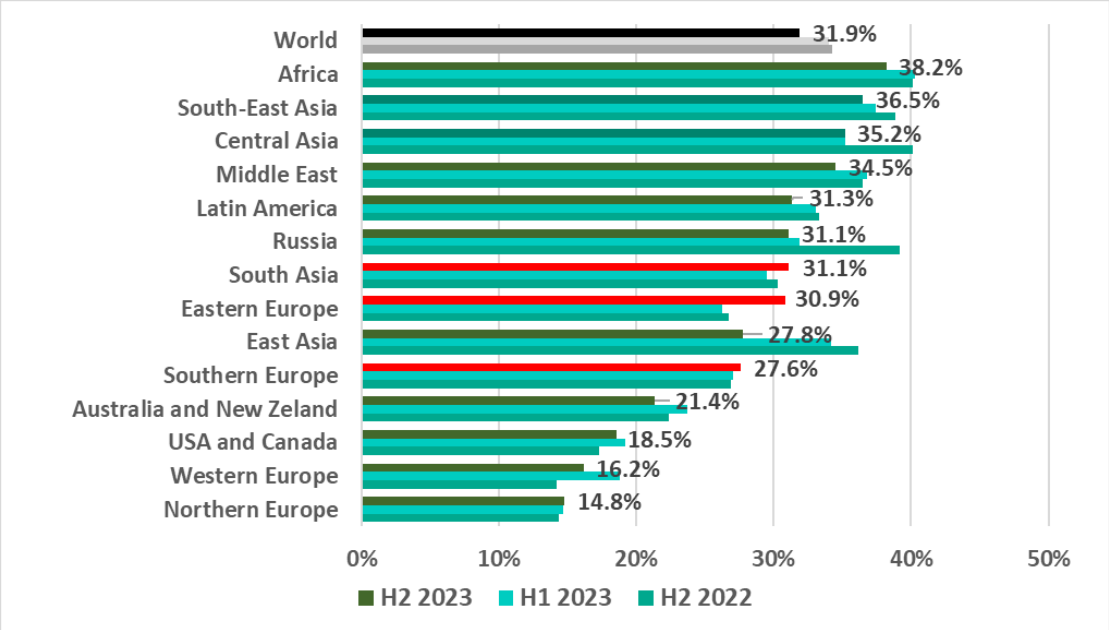
Percentage of ICS computers on which malicious objects were blocked, by month, 2021-2023

In terms of month-to-month fluctuations, the year 2023 differs from the two that preceded it, while being closer to 2021 than to 2022.

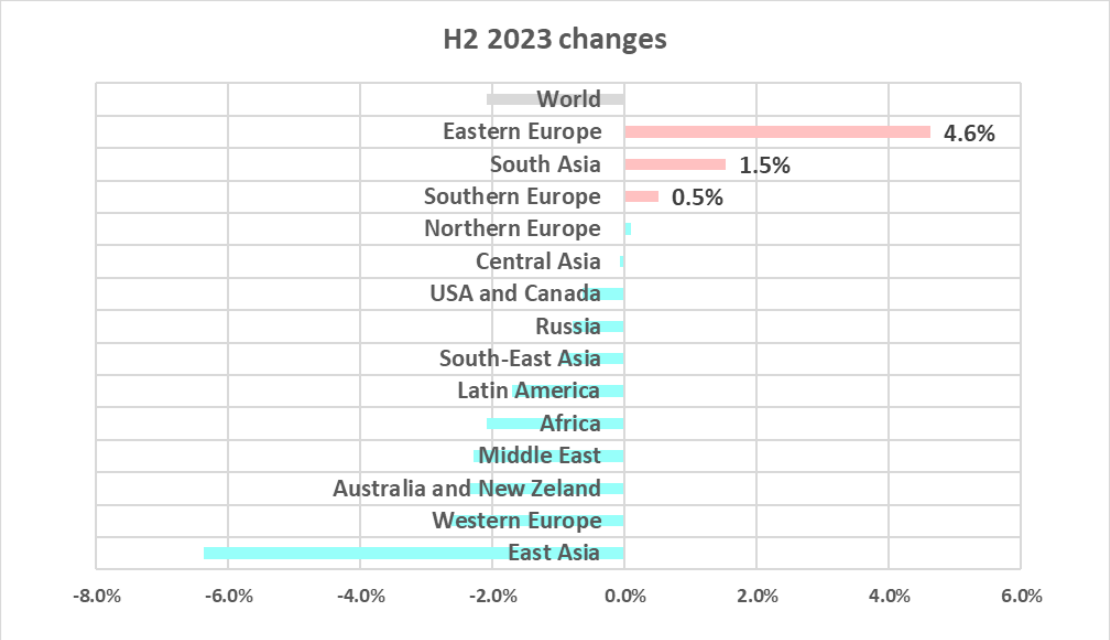
Regions

In H2 2023, the percentage of computers on which malicious activity was prevented varied across regions from 38.2% in Africa to 14.8% in Northern Europe. The percentage increased in South Asia, Eastern Europe, and Southern Europe.

Regions ranked by percentage of ICS computers where malicious objects were blocked, H2 2023

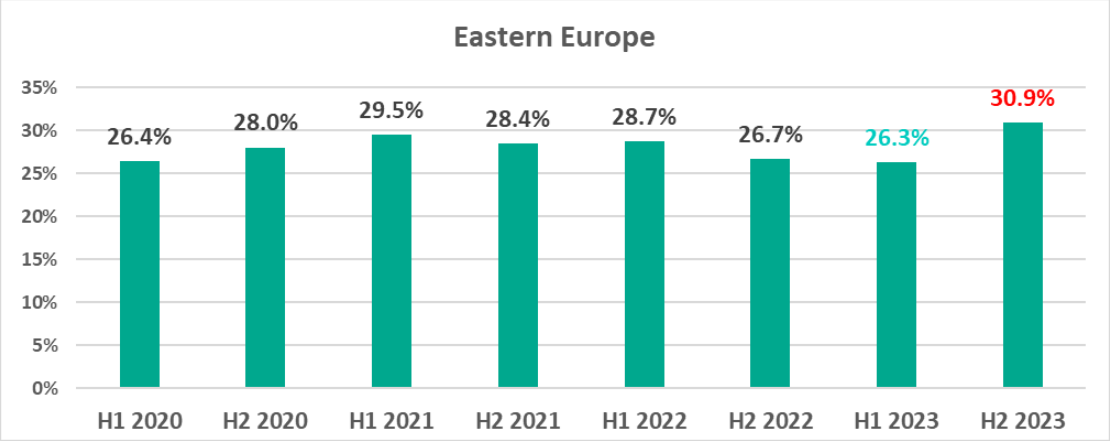


Regions and world. Changes in the percentage of attacked ICS computers in H2 2023



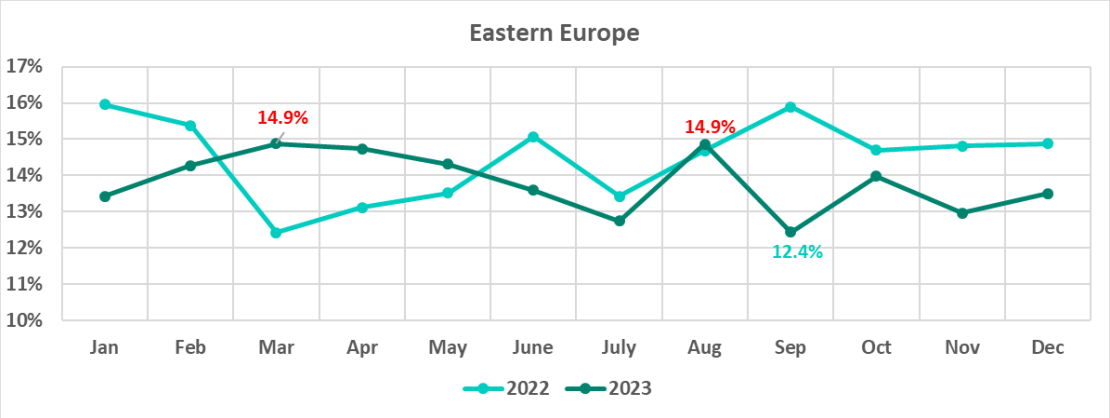
Eastern Europe saw the highest increase in H2 2023, by 4.6 pp. The previous half-year saw the lowest percentage in the region since 2020, whereas the H2 figure was the highest in four years.

Eastern Europe. Percentage of ICS computers on which malicious objects were blocked



The percentage of attacked ICS computers in Eastern Europe was highest in March and August, and lowest in September. Month-to-month changes in 2022 differ noticeably from 2023.

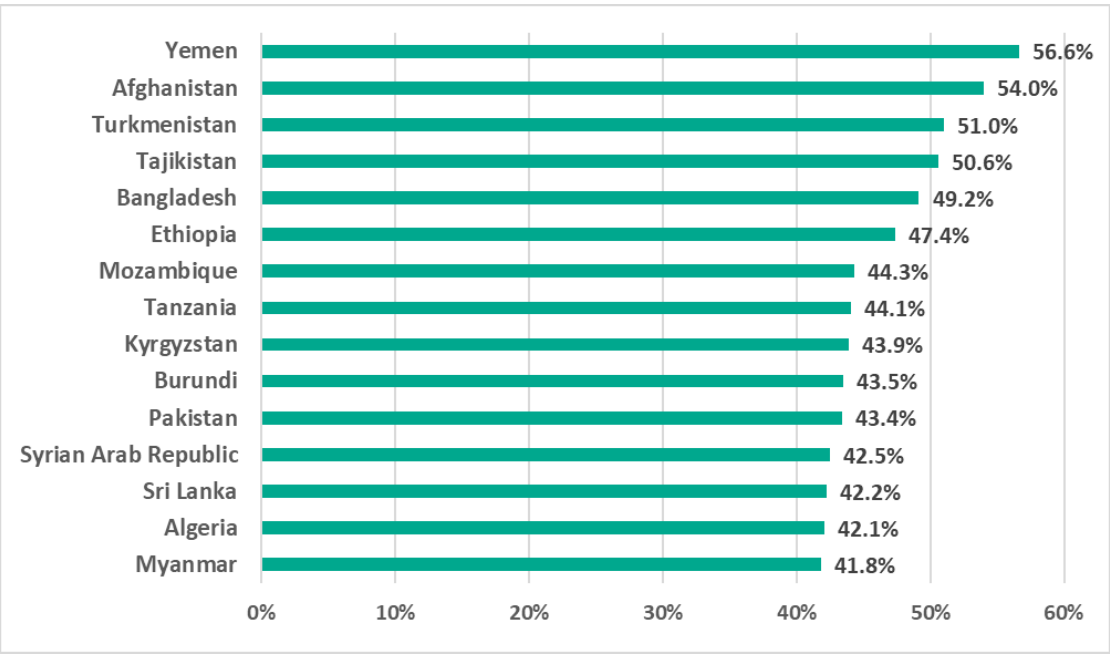
Eastern Europe. Percentage of ICS computers on which malicious objects were blocked, January-December 2022 and 2023



Countries

The percentage of ICS computers on which malicious objects were blocked varied from 56.6% in Yemen to 7.4% in Iceland.

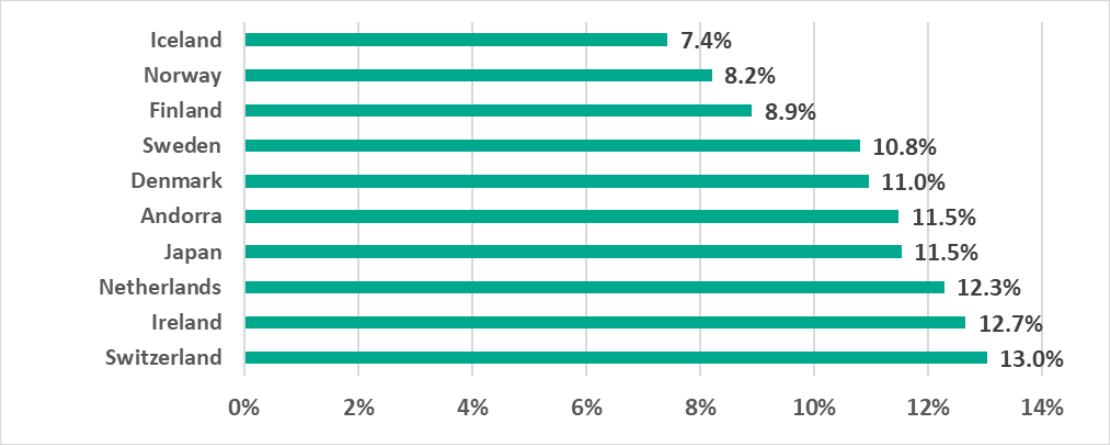
Fifteen countries and territories with the highest percentage of ICS computers on which malicious objects were blocked in H2 2023



The 15 countries and territories with the highest percentage of ICS computers on which malicious objects were blocked in H2 2023 included five countries in Africa, and four in South Asia.

Among the 10 countries with the smallest percentage, six were in Northern Europe.

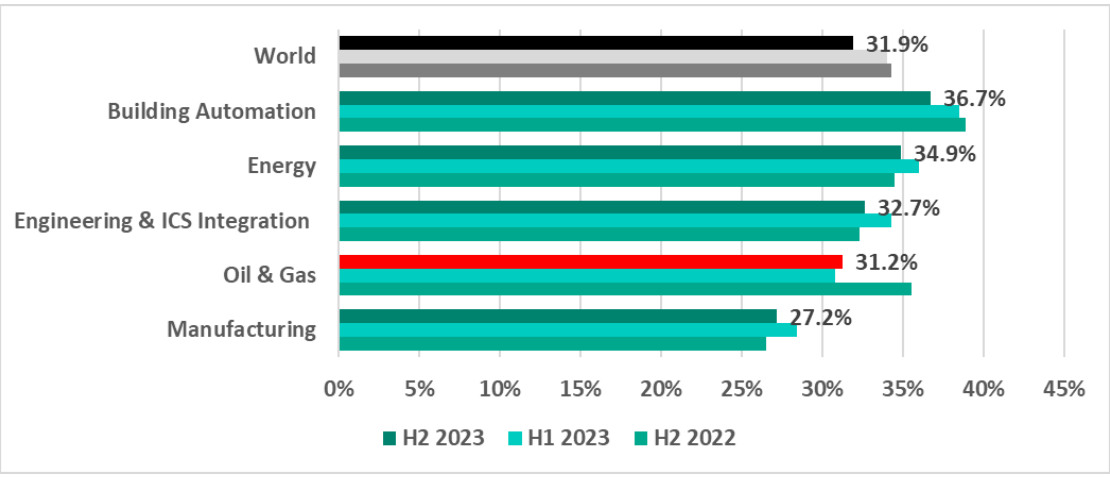
Ten countries and territories with the lowest percentage of ICS computers on which malicious objects were blocked in H2 2023



Selected industries

In H2 2023, building automation once again had the highest percentage of ICS computers on which malicious objects were blocked of all industries that we studied.

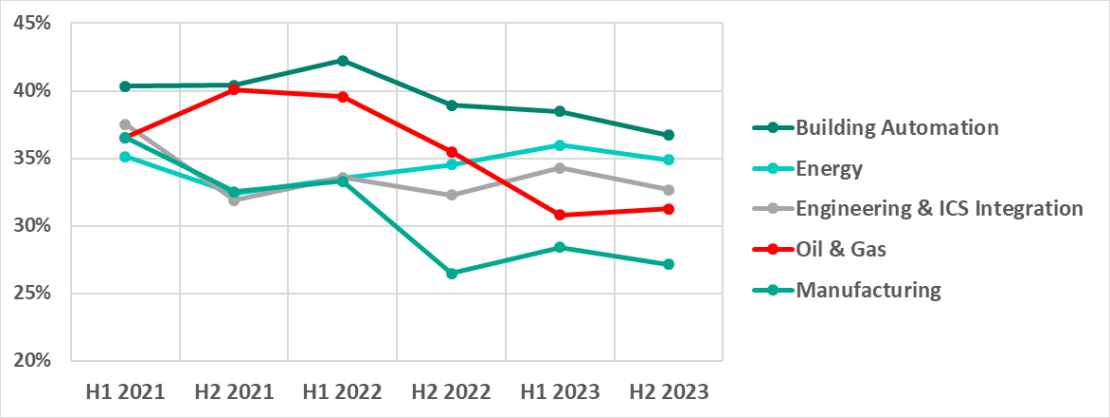
Percentage of ICS computers on which malicious objects were blocked in selected industries



Energy had the second-highest percentage. The percentage of attacked ICS computers in this industry increased for three consecutive half-years: from H1 2022 through H1 2023, only dropping by 1.1 pp in H2 2023.

Oil and Gas saw the opposite trend: starting in 2022, the percentage of ICS computers on which malicious objects were blocked decreased, and then increased slightly (by 0.5 pp) in H2 2023. This is the only industry where the percentage increased in the second half of the year.

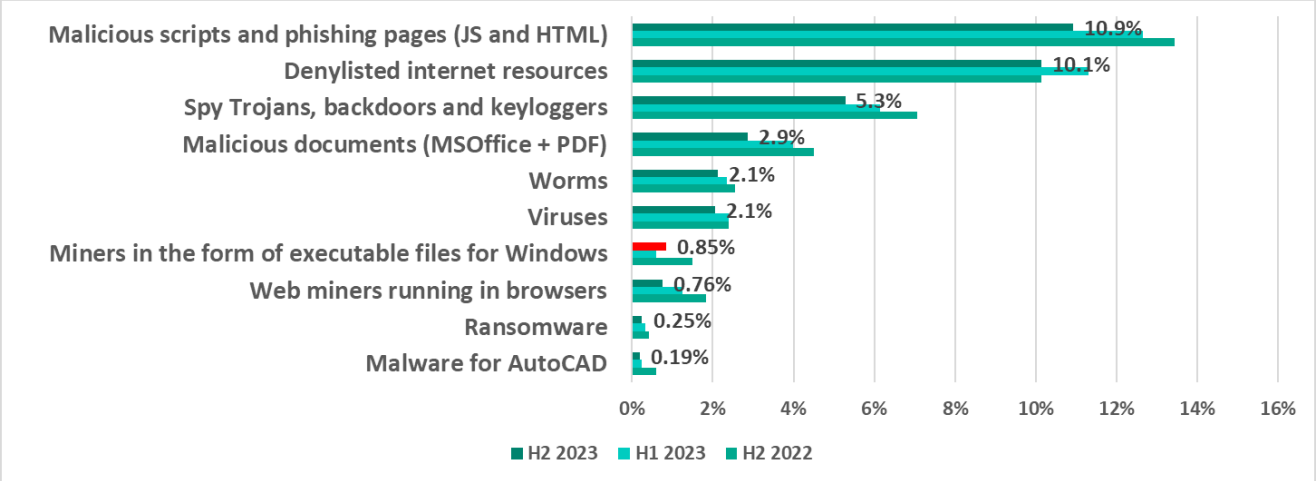
Percentage of ICS computers on which malicious objects were blocked in selected industries



Diversity of detected malware

In the second half of 2023, Kaspersky security solutions blocked malware that belonged to 12,618 families on industrial automation systems.

Malicious objects blocked by Kaspersky products on ICS computers belonged to many categories. In H2 2023, only one category saw an increase: ICS computers on which **miners in the form of executable files for Windows** were blocked, by 1.4 times.



Percentage of ICS[1] computers on which the activity of malicious objects of various categories was prevented

We then grouped the statistics on malicious objects, breaking these down into the following three groups by spread method and purpose:

1. Malicious objects used for initial infection;
2. Next-stage malware;
3. Self-propagating malware.

[1] Note that it would not be appropriate to sum up the percentages, as in many cases, more than one threat type could be blocked on one computer in the period under review.

Malicious objects used for initial infection include dangerous web resources, malicious scripts, and malicious documents. These are directly associated with next-stage malware, which they deliver to the victim computer: spyware, ransomware, or miners. Most times, the source of these threats is the internet or email.

Countries and regions with a high percentage of ICS computers on which initial infection malware is blocked also have a high percentage of next-stage malware.

Self-propagating malware (worms and viruses) is a category unto itself. Worms and virus-infected files were originally used for initial infection, but as botnet functionality evolved, they took on next-stage characteristics.

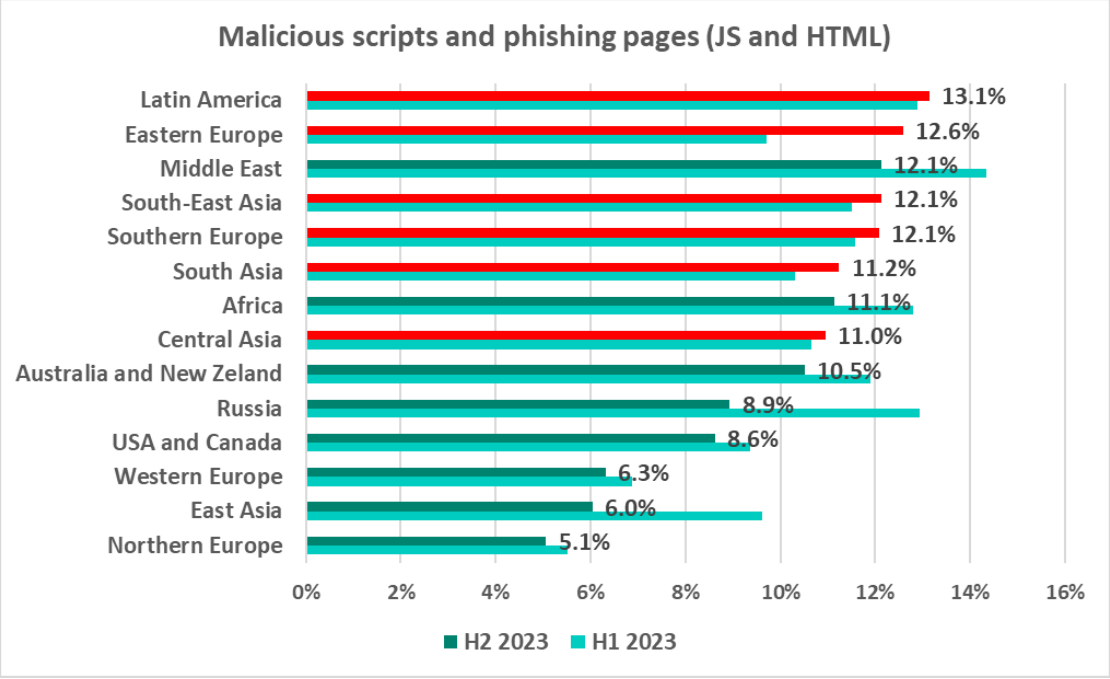
Malicious objects used for initial infection

Malicious scripts and phishing pages (JS and HTML)

Malicious actors use scripts for a wide range of objectives: collecting information, tracking, redirecting the browser to a malicious site, and uploading various types of malware (spyware and/or silent crypto mining tools) to the user's system or browser. These spread via the internet and email.

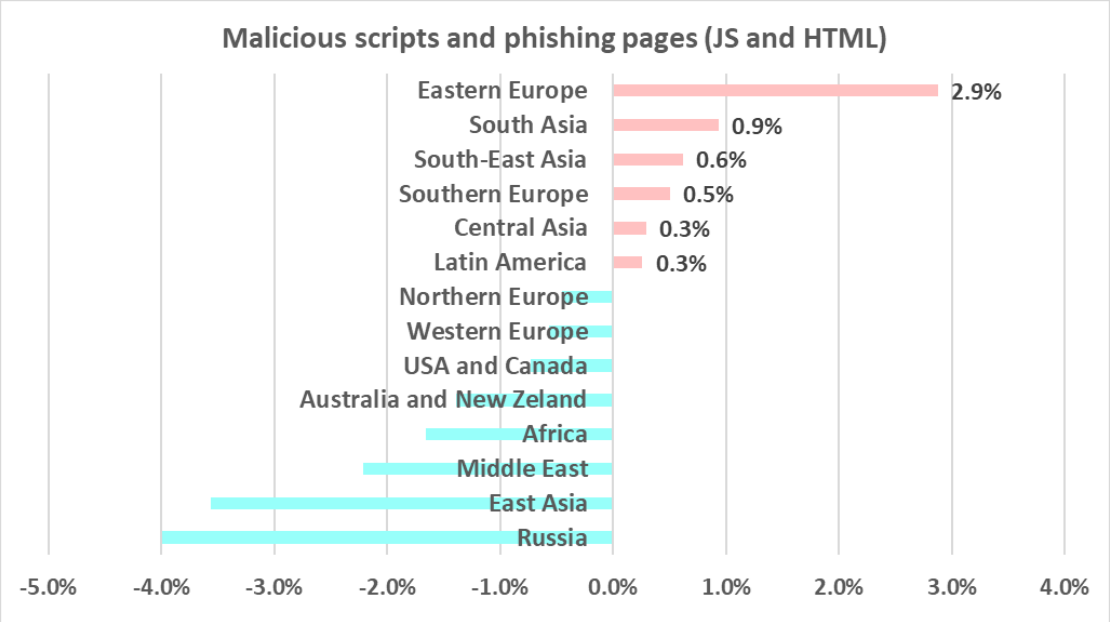
Among the regions, Latin America and Eastern Europe had the highest percentage of ICS computers on which malicious scripts and phishing pages were blocked.

Regions ranked by percentage of ICS computers on which malicious scripts and phishing pages were blocked, H2 2023



The percentage of ICS computers on which malicious objects in this category were blocked increased in six regions within the six-month period, most of all in Eastern Europe (by 2.9 pp).

Changes in the regional percentages of ICS computers on which malicious scripts and phishing pages (JS and HTML) were blocked, H2 2023



Kyrgyzstan leads the countries by percentage of ICS computers on which malicious scripts and phishing pages were blocked with 21.2%. It is followed by North Macedonia (20.7%) and Greece (19.8%).

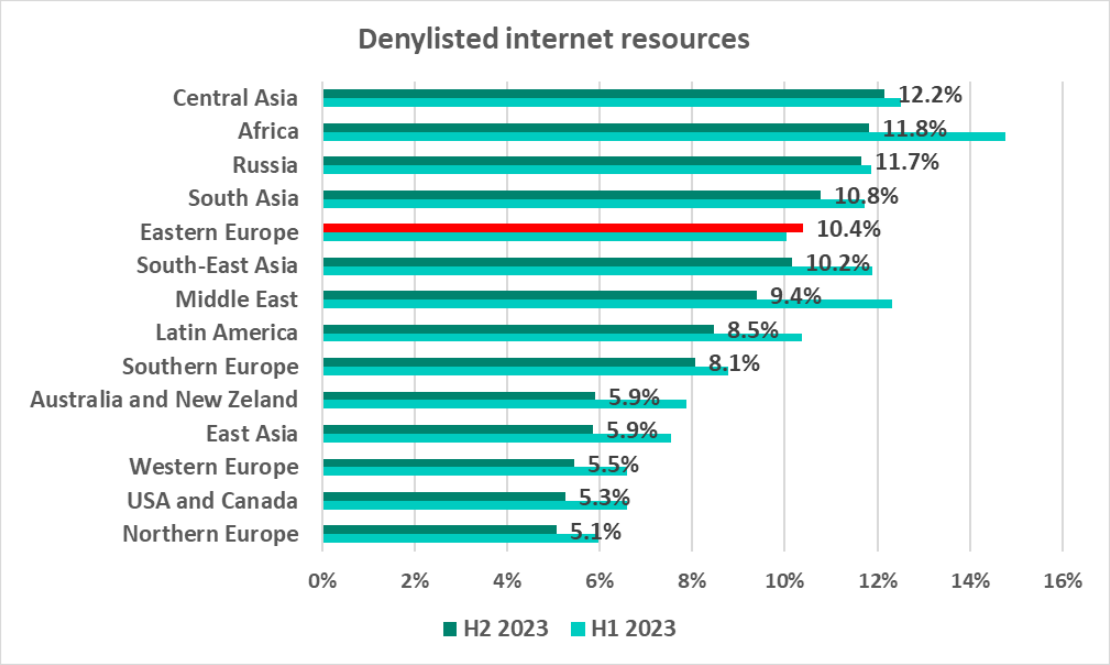
Denylisted internet resources

Denylisted internet resources are associated with malware spread or control. A significant percentage of these resources is used for spreading malicious scripts and phishing pages (HTML).

Of all regions, Central Asia had the highest percentage of ICS computers on which denylisted internet resources were blocked.

Eastern Europe was the only region where the percentage increased slightly, by 0.4 pp.

Regions ranked by percentage of ICS computers on which denylisted internet resources were blocked, H2 2023



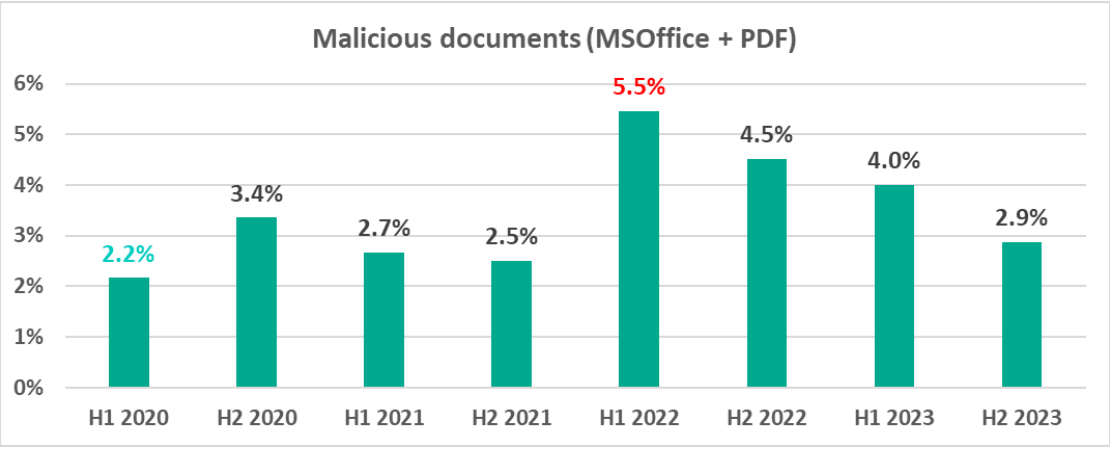
Tajikistan and Yemen led the country ranking by percentage of ICS computers on which denylisted internet resources were blocked, with 18.2% and 16.6%, respectively.

Malicious documents (Microsoft Office and PDF)

Attackers send malicious documents attached to phishing messages and use them in attacks aimed at initial infection of computers. Malicious documents typically contain exploits, malicious macros, and malware links.

The global percentage of ISC computers on which threats in this category were blocked had been declining since H2 2022. In the second half of 2023, it dropped by 1.1 pp when compared to the preceding six-month period.

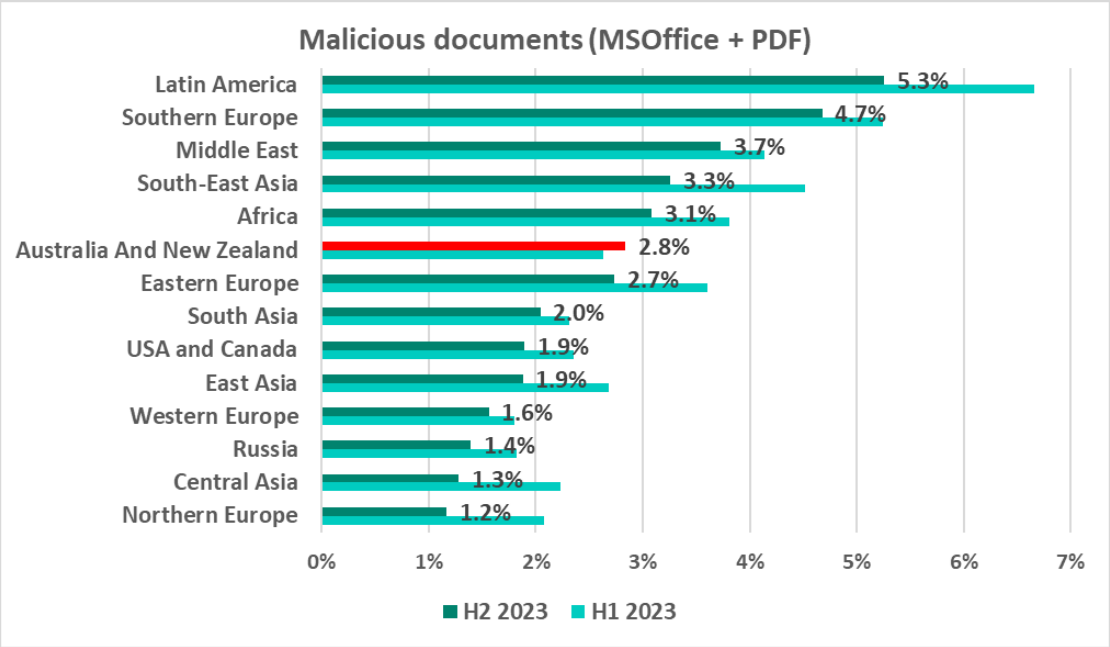
Percentage of ICS computers on which malicious documents (Microsoft Office and PDF) were blocked



Latin America, Southern Europe, and Middle East once again occupied the top three places in the ranking. The same regions topped the ranking by percentage of ICS computers on which email threats were blocked.

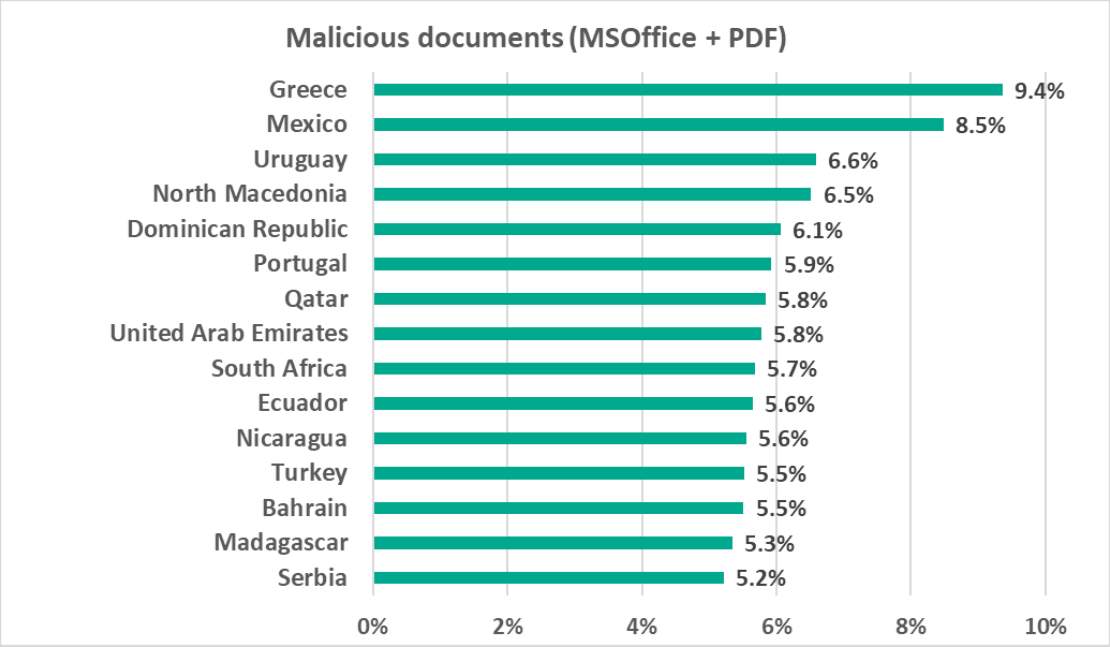
In the six-month period, the figure slightly increased (by 0.2 pp) only in Australia and New Zealand.

Regions ranked by percentage of ICS computers on which malicious documents were blocked, H2 2023



Greece and Mexico led the country and territory ranking by percentage of ICS computers on which malicious documents were blocked with 9.4% and 8.5%, respectively.

Fifteen countries and territories with the largest percentage of ICS computers on which malicious documents were blocked, H2 2023.



Three of the 15 leaders were in Latin America, four in the Middle East, and three in Southern Europe.

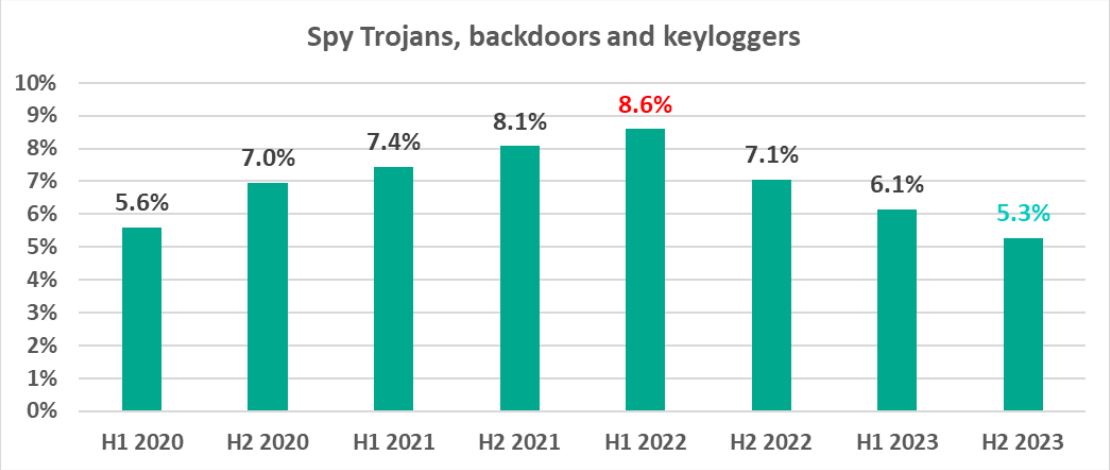
Next-stage malware

Spyware

Spyware (spy Trojans, backdoors, and keyloggers) can be found in lots of phishing email sent to industrial organizations. Spyware is used for unauthorized remote access and confidential data theft. The ultimate goal of most spyware attacks is stealing money, but spyware is also used in targeted attacks, for cyberespionage.

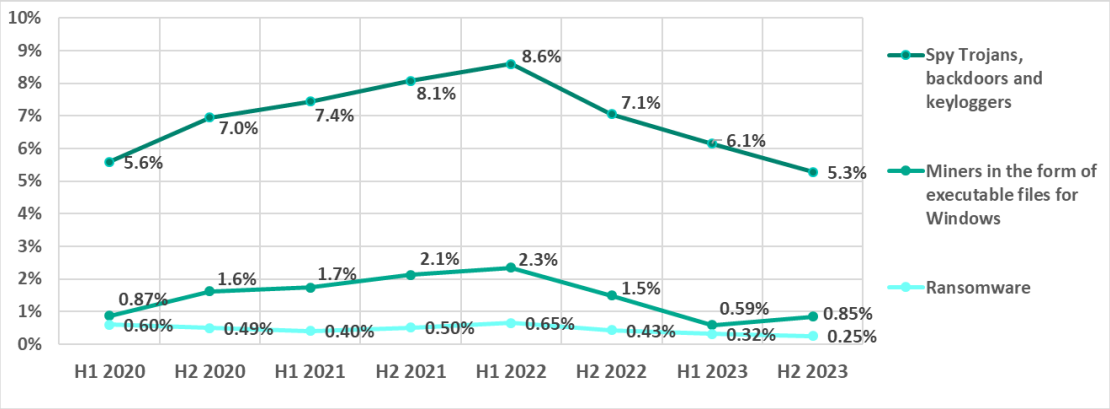
In the second half of 2023, the global percentage of ICS computers on which spyware was blocked was the lowest since 2020 at 5.3%.

Percentage of ICS computers on which spyware was blocked



It should be noted that spyware is also used to steal information needed to deliver other types of malware, such as ransomware and silent miners, and to prepare for targeted attacks. As a rule, a change in the percentage of computers on which spyware is blocked will have an effect on the risk of targeted attacks and resulting in a corresponding change in the percentage of computers attacked by miners or ransomware.

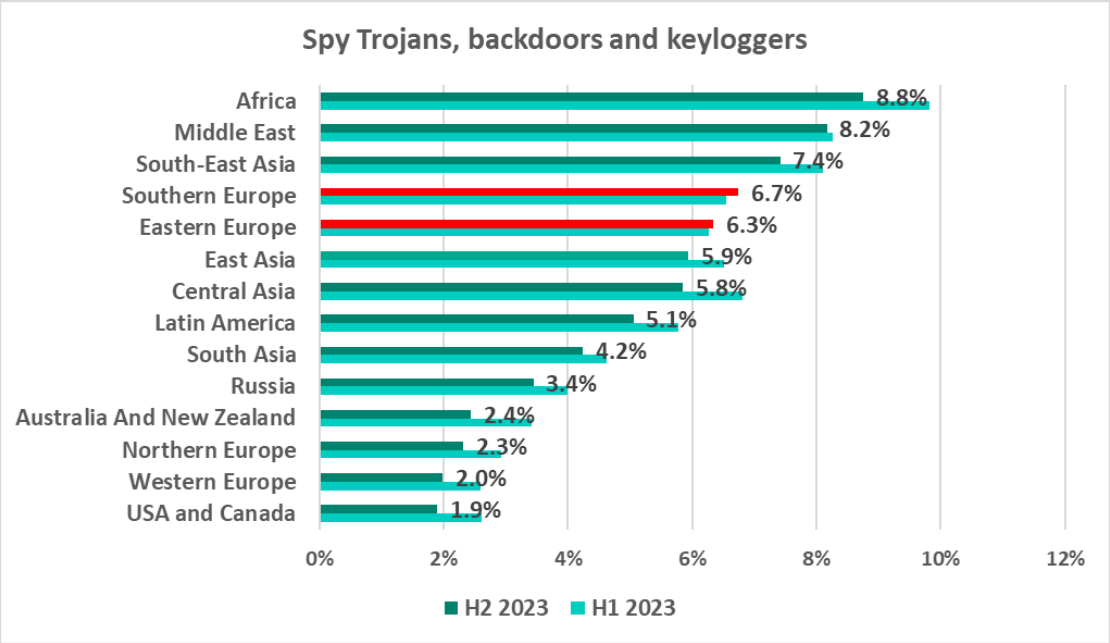
Percentage of ICS computers on which spyware, malicious miners and malware were blocked



As before, Africa was the region with the highest percentage of ISC computers on which spyware was blocked. The figure also remained high in the Middle East and South-East Asia.

While globally, the percentage of ICS computers on which spyware was blocked declined in H2 2023, the figure rose slightly in Southern Europe (by 0.2 pp) and Eastern Europe (by a paltry 0.07 pp) by contrast. Southern Europe ranked fourth and Eastern Europe, fifth.

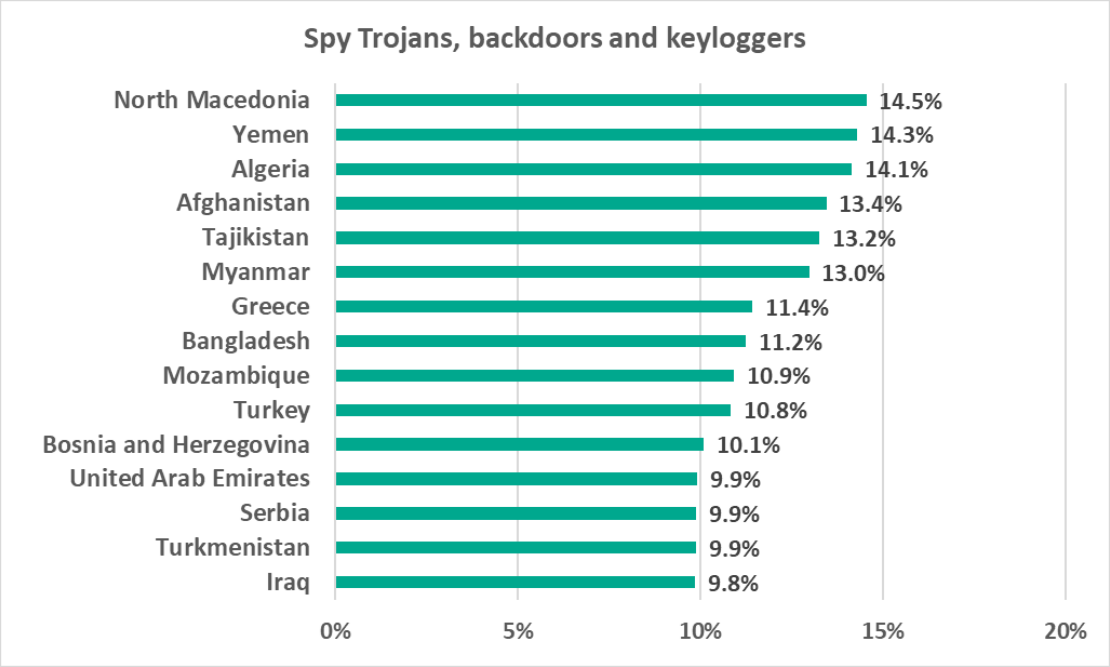
Regions ranked by percentage of ICS computers on which spyware was blocked, H2 2023



It should be noted that in East Asia, spyware ranked second among all malware categories by percentage of ICS computers on which it was blocked.

North Macedonia, Yemen, and Algeria topped the country and territory ranking by percentage of ICS computers on which spyware was blocked.

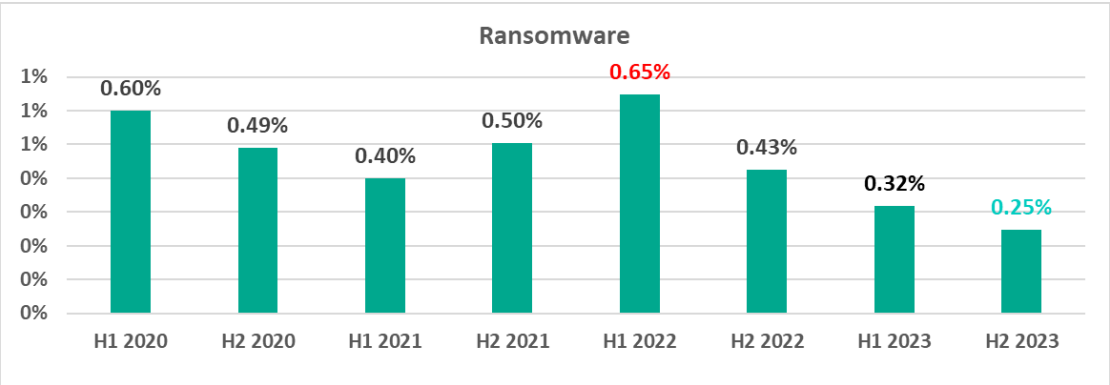
Fifteen countries and territories with the highest percentage of ICS computers on which spyware was blocked, H2 2023



Ransomware

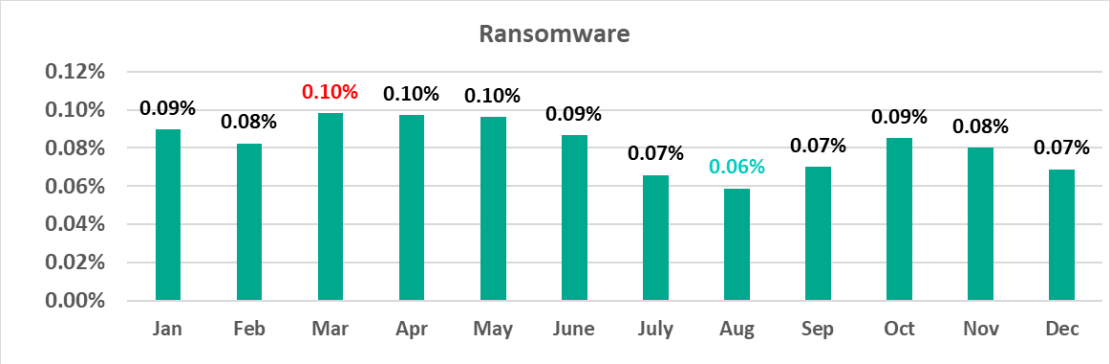
In the second half of 2023, the percentage of ICS computers on which ransomware was blocked dropped to the four-year minimum of 0.25%.

Percentage of ICS computers on which ransomware was blocked, by half year, 2020-2023



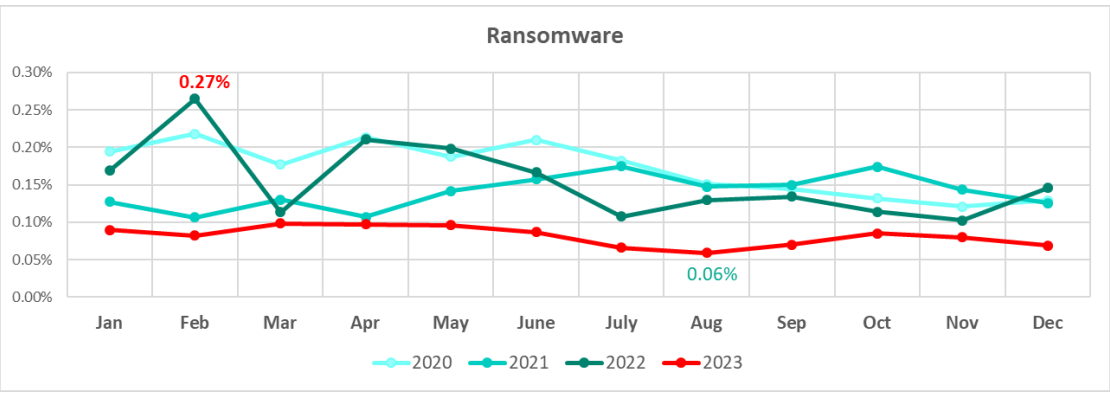
The highest monthly percentage of ICS computers attacked by ransomware in 2023 was recorded in March, and the lowest in August.

Percentage of ICS computers on which ransomware was blocked, January-December 2023



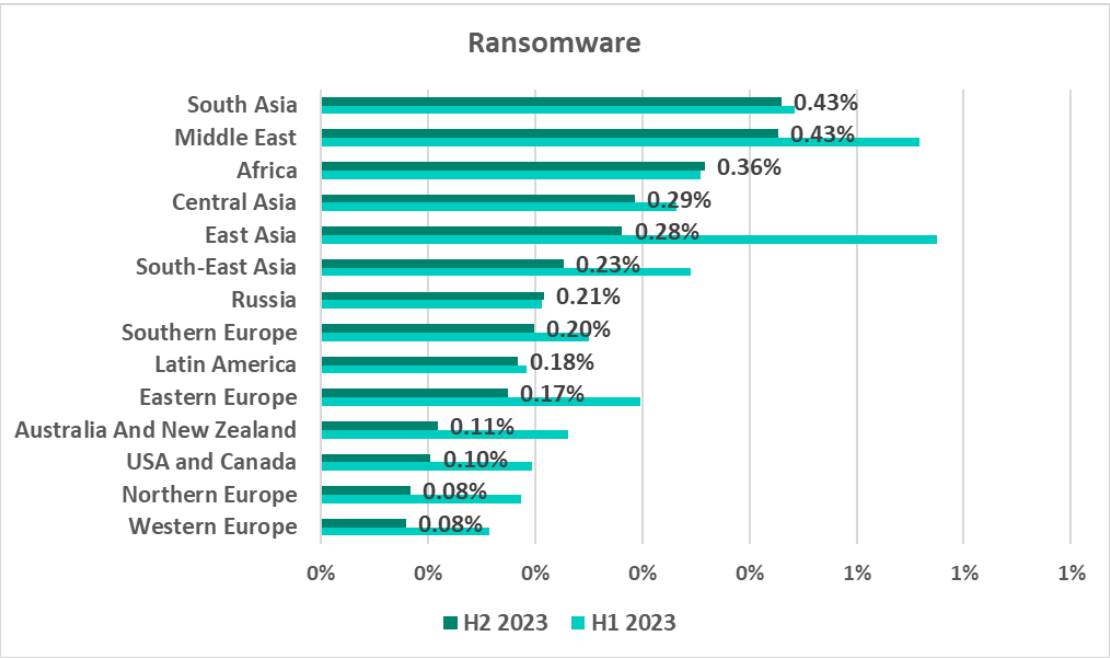
Throughout 2023, the monthly percentages were lower year on year. August saw the lowest monthly figure, both in 2023 and since 2020. The highest percentage for the same period was recorded in February 2022.

Percentage of ICS computers on which ransomware was blocked, by month, 2020-2023



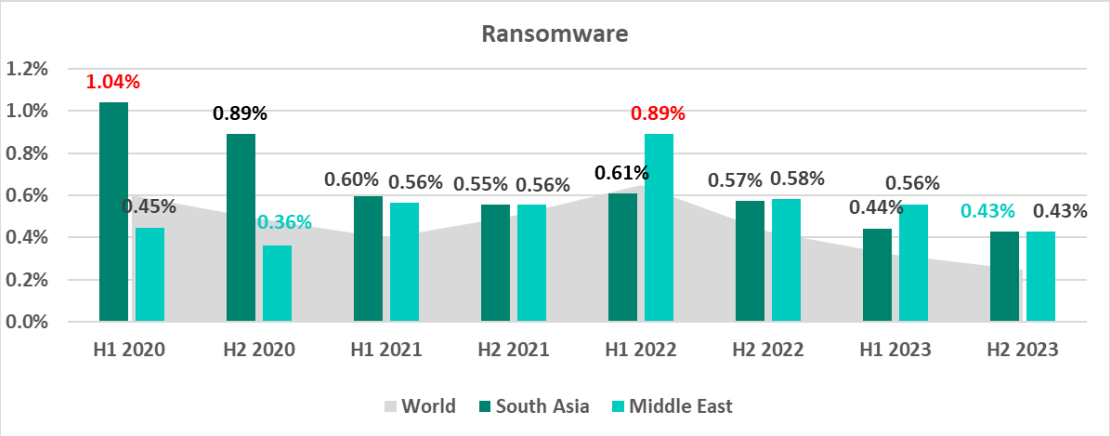
South Asia and the Middle East led the region ranking by percentage of ICS computers on which ransomware was blocked.

Regions ranked by percentage of ICS computers on which ransomware was blocked, H2 2023



The Middle East climbed from seventh place in H1 2020 to the top in H2 2023. The percentage of ICS computers attacked by ransomware in the Middle East was at its highest since 2020 (0.89%) in H1 2022. South-East Asia had the highest percentage in the same period among all regions at 1.3% in H2 2021.

South Asia, Middle East, and world. Percentage of ICS computers on which ransomware was blocked, by half year



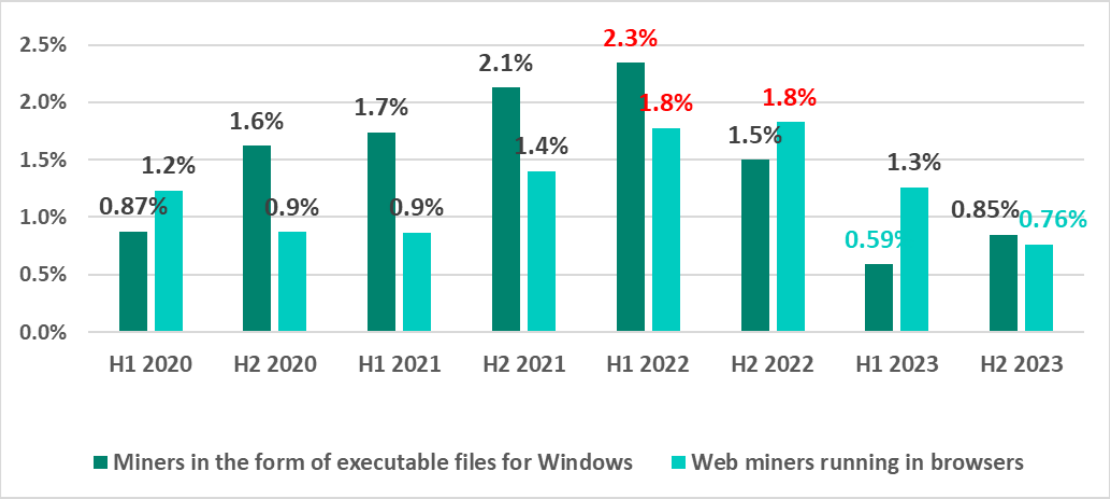
The list of 15 countries and territories with the highest percentage of ICS computers on which ransomware was blocked included four countries from each of the leading regions: South Asia, Africa, and the Middle East.

Malicious cryptocurrency miners

In the second half of 2023, the global percentage of ICS computers on which web miners were blocked was the lowest since 2020.

The percentage of ICS computers on which malicious miners in the form of executable files for Windows were blocked hit its four-year low in H1 2023 before rising again in H2. As a reminder, this was the only malware category globally in H2 2023 that saw its share of attacked computers increase.

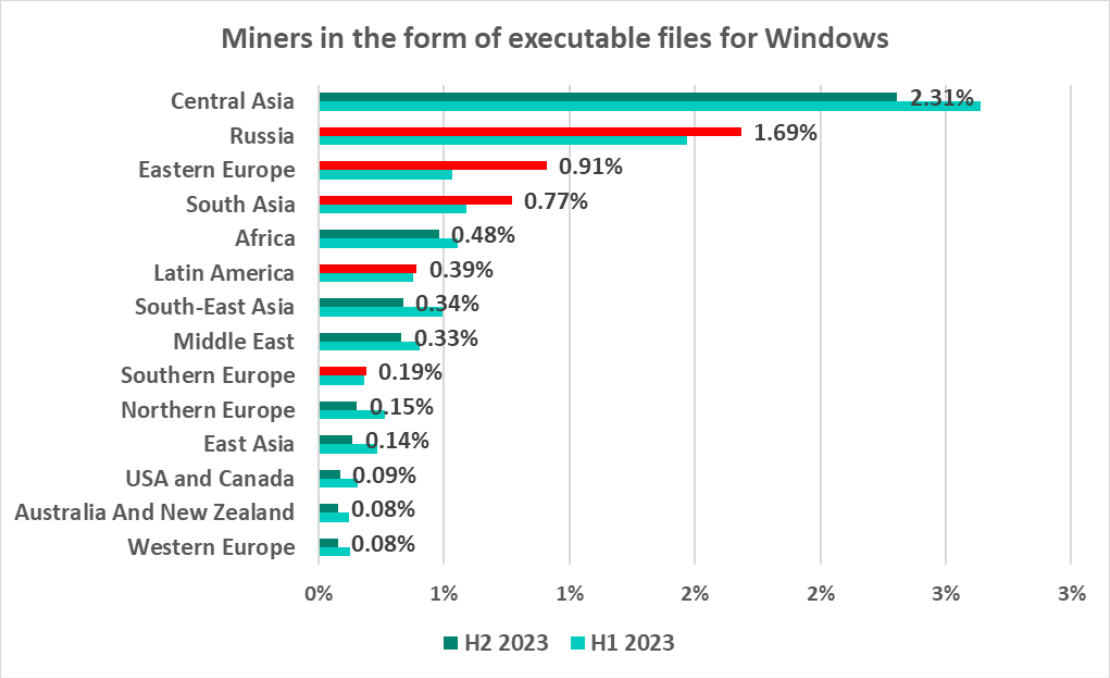
Percentage of ICS computers on which malware for covert cryptocurrency mining was blocked



Miners in the form of executable files for Windows

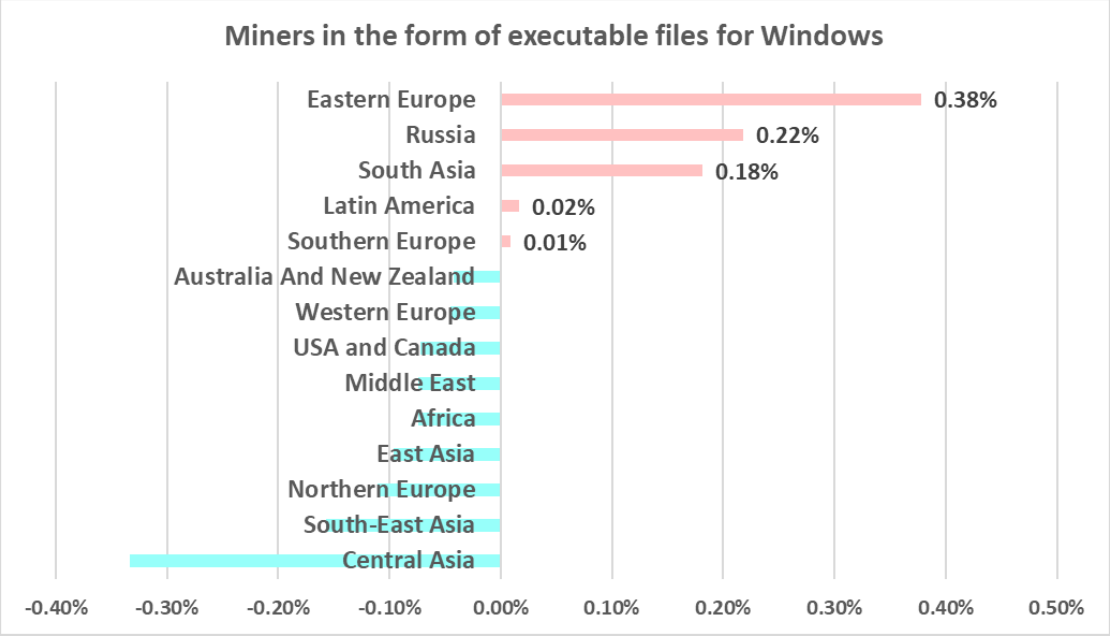
Central Asia and Russia led the region ranking in H2 2023 by percentage of ICS computers on which miners in the form of executable files for Windows were blocked.

Regions ranked by percentage of ICS computers on which miners in the form of executable files for Windows were blocked, H2 2023



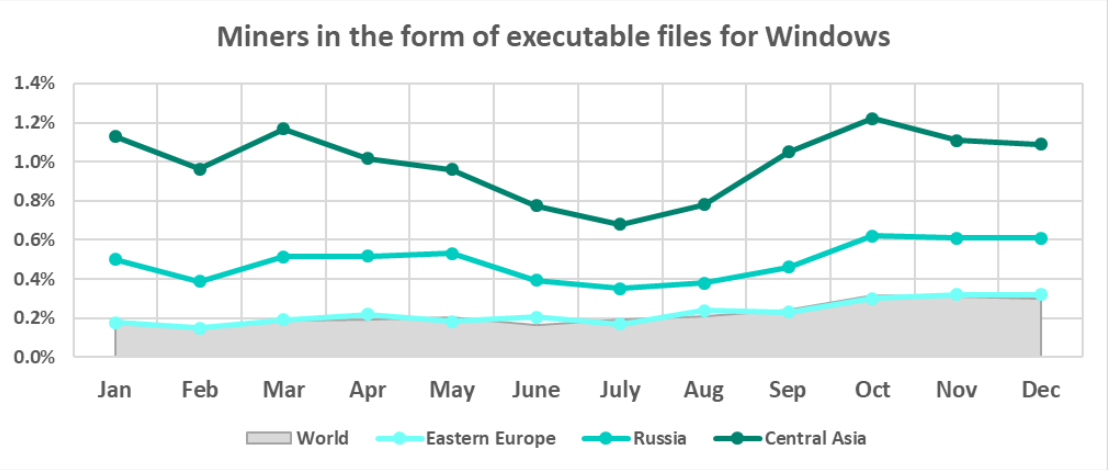
Five regions saw the percentage rise on the previous six-month period, most of all Eastern Europe, by 0.38 pp. The leader, Central Asia, saw this percentage drop.

Changes in the percentage of ICS computers on which miners in the form of executable files for Windows were blocked in H2 2023



While looking at the percentages of ICS computers on which malicious objects of all categories were blocked, we highlighted the similarity between the monthly changes in Eastern Europe, Russia, and Central Asia. The similarity is also noticeable in the case of miner executables, especially in Russia and Central Asia.

Percentage of ICS computers on which miners in the form of executable files for Windows were blocked, H2 2023

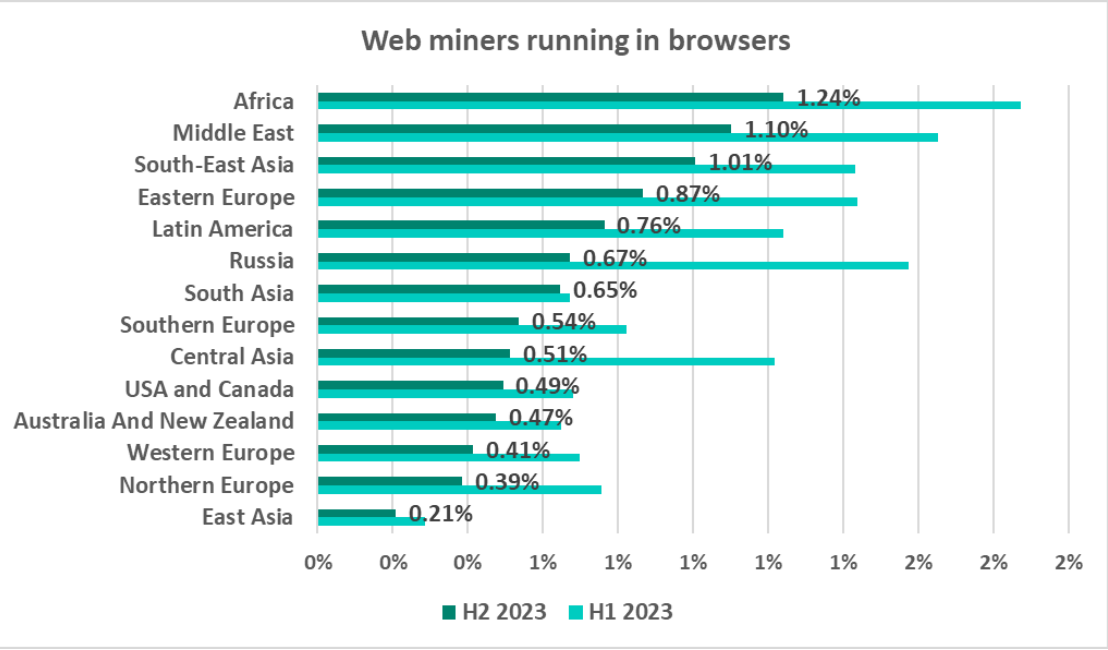


Tajikistan (7.1%) and Turkmenistan (6.3%) were well ahead in the ranking of countries and territories by percentage of ICS computers on which miners in the form of executable files for Windows were blocked.

Web miners

Africa and the Middle East led the region ranking by percentage of ICS computers on which web miners were blocked.

Regions ranked by percentage of ICS computers on which browser-based web miners were blocked, H2 2023



Yemen (3.9%) and Serbia (3.5%) topped the ranking of countries and territories by percentage of ICS computers on which web miners were blocked.

Self-propagating malware. Viruses and worms

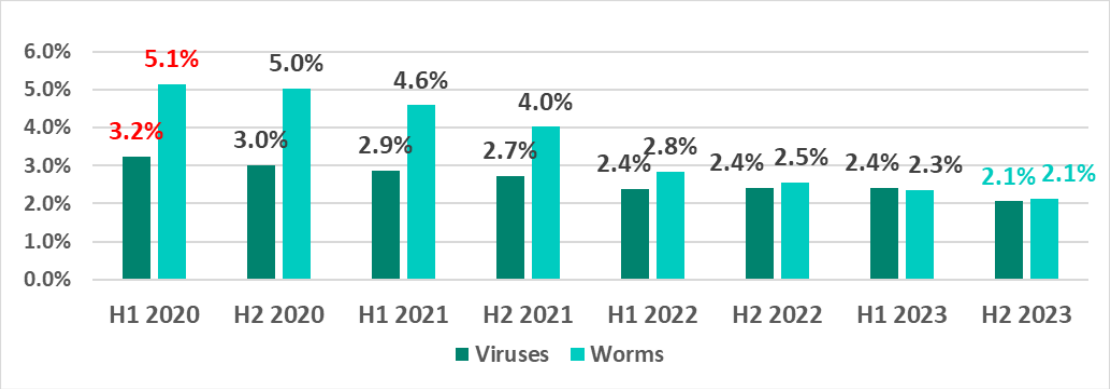
To spread across ICS networks, viruses and worms rely on removable media, network folders, infected files including backups, and network attacks on outdated software, such as Radmin2.

A lot of those still spreading are legacy viruses and worms whose command-and-control servers have been shut down. However, these types of malware can compromise infected systems by opening network ports or changing configurations, cause software failures, denial of service, and so on.

New worm versions used by malicious actors for spreading spyware, ransomware, and miners can be found on ICS networks as well. More often than not, they rely on network service (e.g. SMB or RDP) exploits that have been addressed by the vendors but still persist on OT networks, previously stolen credentials, or password boot-forcing.

The global percentage of ICS computers on which viruses and works were blocked kept declining. For each of these two threat categories, the H2 2023 percentage was the lowest since 2020.

Percentage of ICS computers on which viruses and worms were blocked

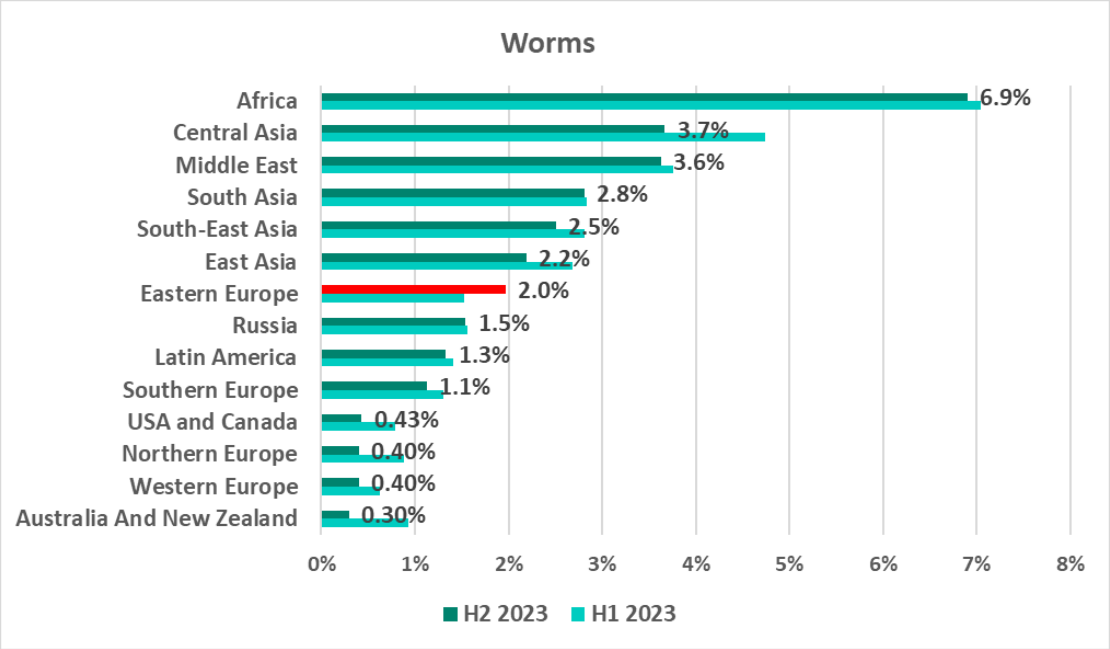


Worms

Africa remained a leader among the regions by percentage of ICS computers on which worms were detected. The malware in this category blocked in Africa included worms written in Python, which are used for spreading malicious miners. The region is also well ahead in the percentage of ICS computers on which threats were blocked when connecting removable media, which worms use to spread.

The only region where the worm percentage had increased in the six-month period was Eastern Europe, by 0.43 pp.

Regions ranked by percentage of ICS computers on which worms were blocked, H2 2023



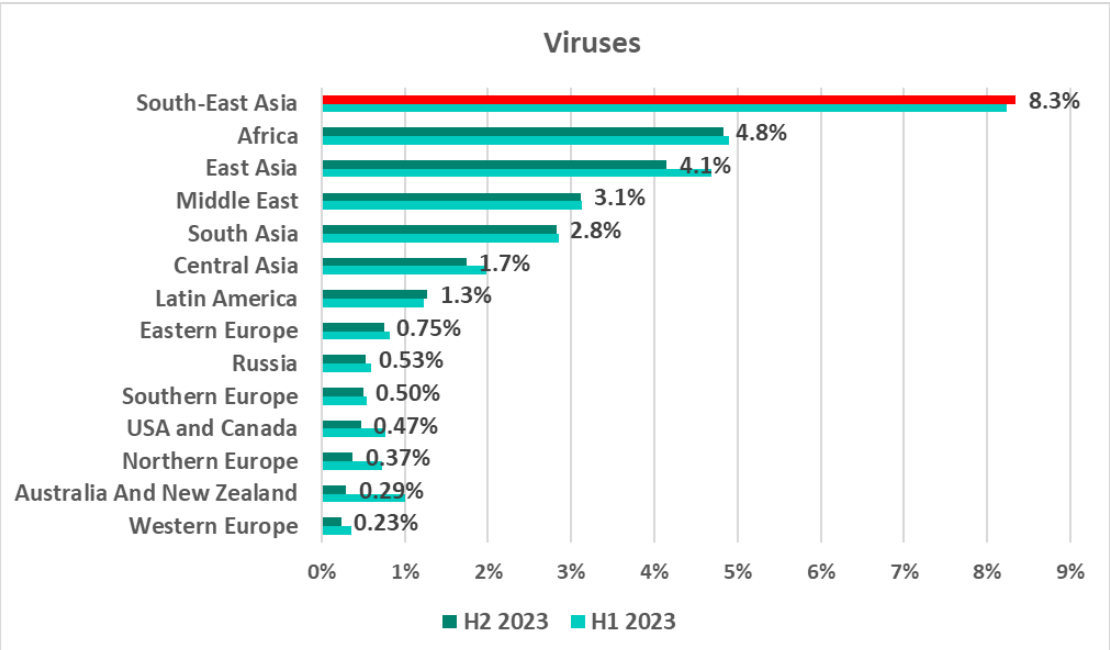
Twelve out of 15 countries in the ranking were located in Africa. Two countries in Central Asia, one of them being Turkmenistan with 19.7%, topped the ranking.

Viruses

The percentage of ICS computers on which viruses were blocked in H2 2023 rose, by 0.11 pp, in the region that led the ranking, South-East Asia.

Viruses remain an urgent issue for South-East Asia. They were the third-biggest category in the H2 2023 malware rankings by percent of ICS computers on which they were blocked.

Regions ranked by percentage of ICS computers on which viruses were blocked, H2 2023



Yemen (17.4%) and Vietnam (14.3%) were at the top of the ranking by percentage of ICS computers on which viruses were blocked.

AutoCAD malware

East Asia led the ranking by percentage of ICS computers on which AutoCAD malware was blocked, with 1.2%. This category of threats is blocked on computers connected to OT networks, including network folders and engineer workstations.

China (7.84%), Vietnam (1.4%), and Ethiopia (1.32%) led the ranking of countries and territories by percentage of ICS computers on which AutoCAD malware was blocked.

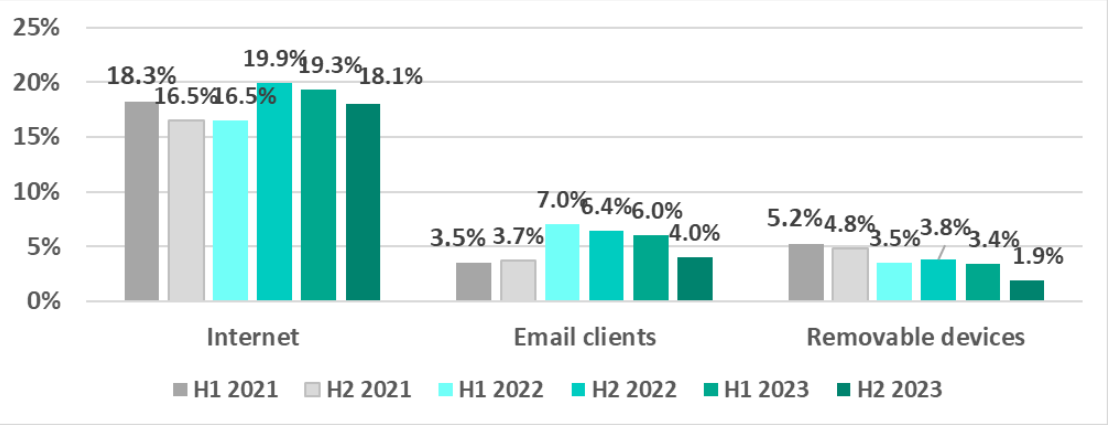
Main threat sources

The internet, email clients, and removable media remained the main sources of threats to computers connected to enterprise OT networks. It should be noted that the exact source of a blocked threat cannot always be ascertained.

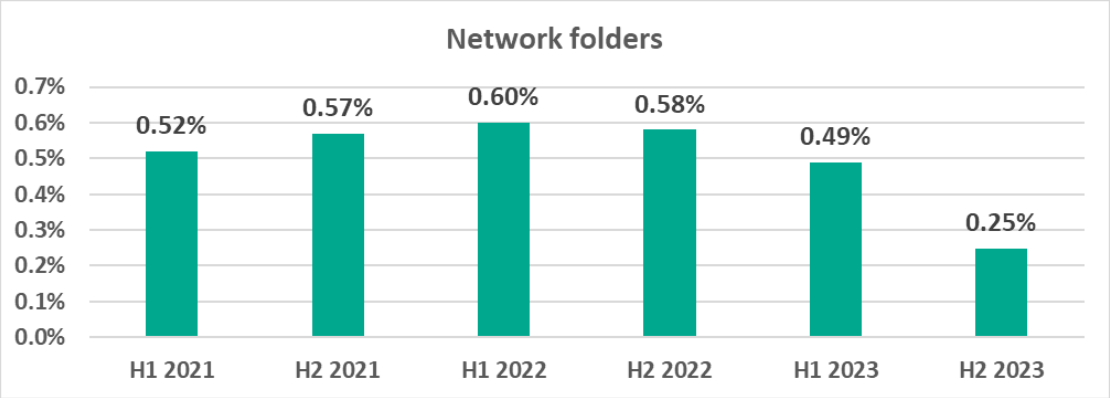
World

In the second half of 2023, the percentage of ICS computers on which malicious objects were blocked dropped for each of the main sources.

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



Percentage of ICS computers on which threats from network folders were blocked



As in the case of the statistics across all threats, the percentage of ICS computers where malicious objects from various sources were blocked varied with region.

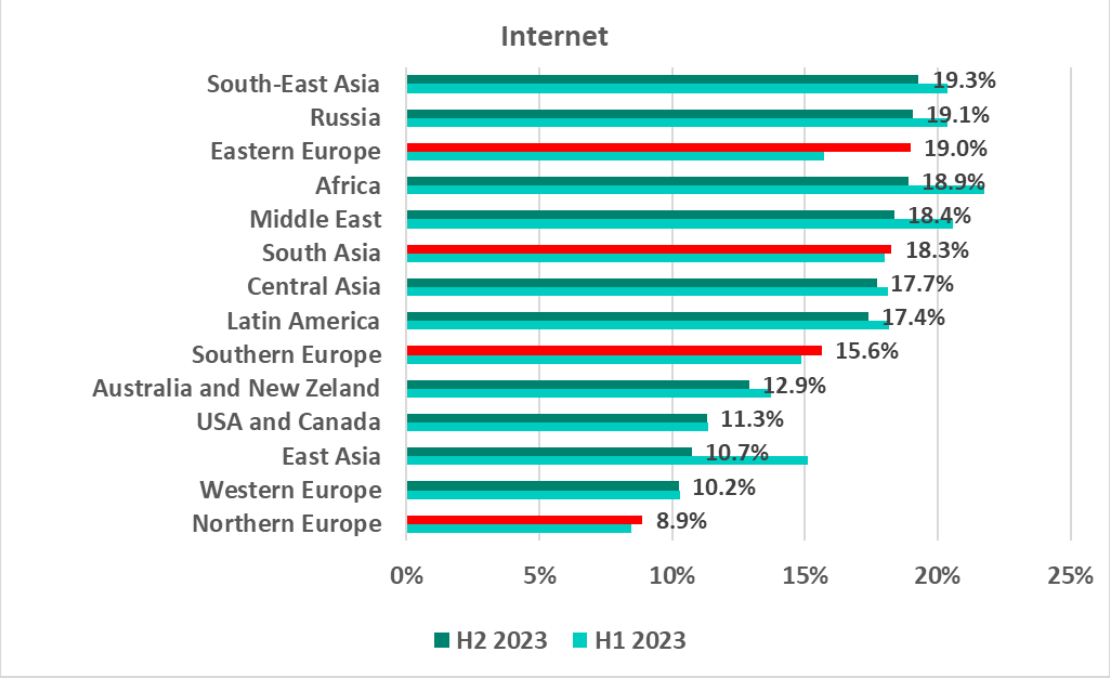
Regions

Internet

South-East Asia, Russia, and Eastern Europe led the H2 2023 region ranking by percentage of ICS computers on which internet threats were blocked.

This percentage increased in four regions, most of all in Eastern Europe, by 3.2 pp.

Regions ranked by percentage of ICS computers on which internet threats were blocked, H2 2023

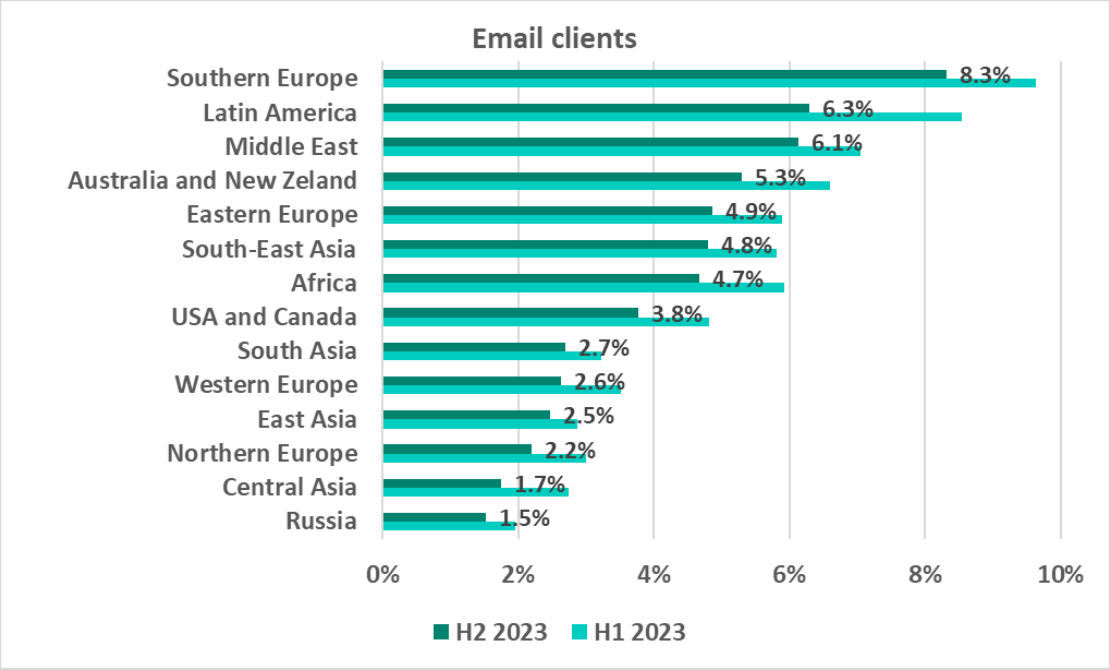


Email clients

South Europe retained its top position in the region ranking by percentage of ICS computers on which malicious email attachments and phishing links were blocked from H1 2022. Latin America was in second place over the same period of time. The Middle East ranked third from H2 2022.

In H2 2023, the percentage of ICS computers on which email threats were blocked decreased in each region.

Regions ranked by percentage of ICS computers on which malicious email attachments and phishing links were blocked, H2 2023

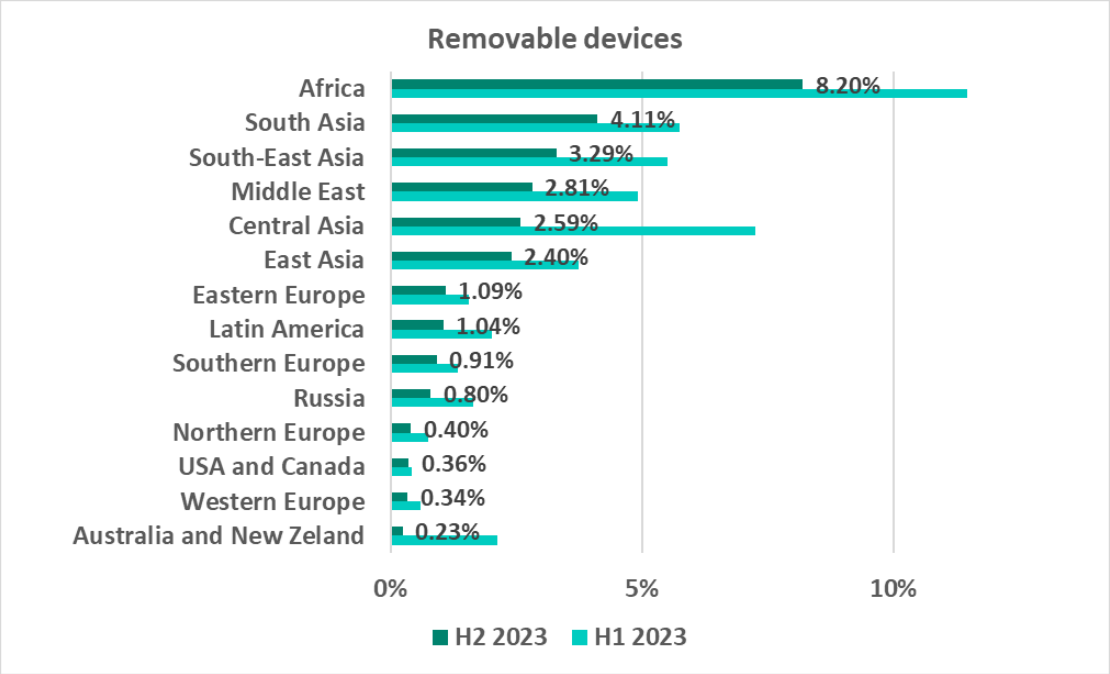


Removable media

As before, Africa led the regional ranking by percentage of ICS computers on which removable media threats were blocked. This region, too, was far ahead of the others by the percentage of ICS computers on which worms were blocked.

The percentage of ICS computers on which removable media threats were blocked declined in each region in H2 2023.

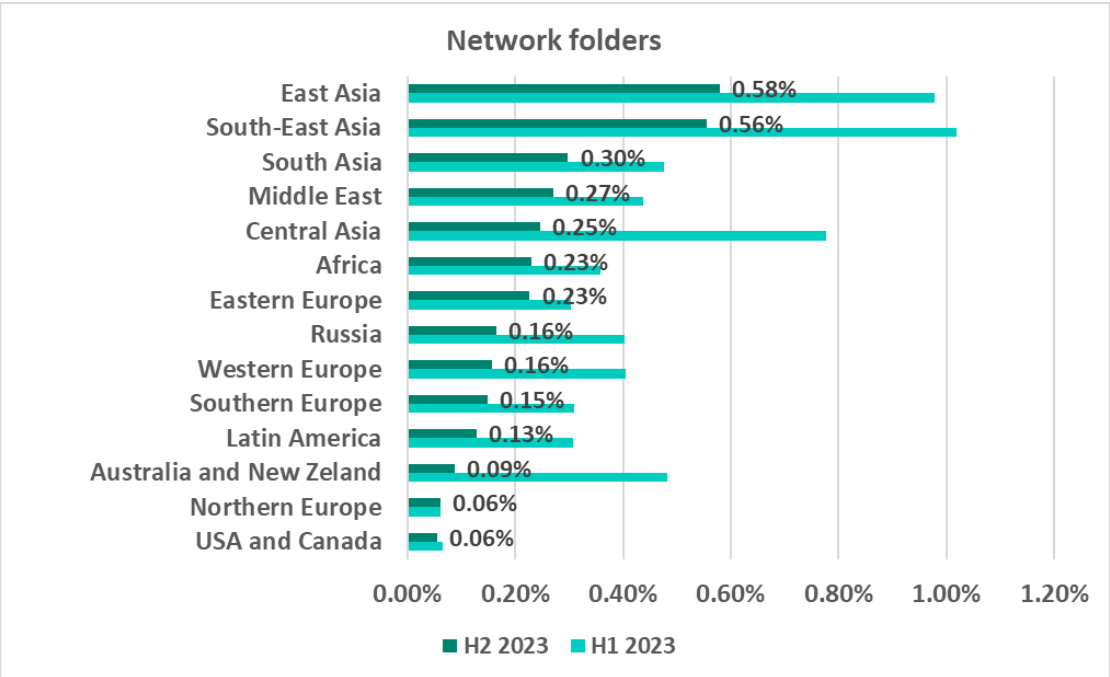
Regions ranked by percentage of ICS computers on which removable media threats were blocked, H2 2023



Network folders

Network folders are a minor source of malicious objects. The largest percentage of ICS computers on which threats were blocked inside network folders was recorded in East and South-East Asia.

Regions ranked by percentage of ICS computers on which malicious objects were blocked inside network folders, H2 2023



Methodology used to prepare statistics

This report presents the results of analyzing statistics obtained with the help of Kaspersky Security Network (KSN). The data was received from those KSN users who had consented to its anonymous sharing and processing for the purpose described in the KSN Agreement for the Kaspersky product installed on their computer.

The benefits of joining KSN for our customers include faster response to previously unknown threats and a general improvement in the quality of detection by their Kaspersky installation achieved by connecting to a cloud-based repository of malware data that is not transferable to the customer in its entirety by nature of its size and the amount of resources that it uses.

Data shared by the user contains only the data types and categories described in the appropriate KSN Agreement. This data helps to a significant extent in analyzing the threat landscape and serves as a prerequisite for detecting new threats including targeted attacks and APTs[2].

Statistical data presented in the report was obtained from ICS computers that were protected with Kaspersky products and which Kaspersky ICS CERT categorized as enterprise OT infrastructure. This group includes Windows computers that serve one or several of the following purposes:

- Supervisory control and data acquisition (SCADA) servers
- Data storage (Historian) servers
- Data gateways (OPC)
- Stationary workstations of engineers and operators
- Mobile workstations of engineers and operators
- Human machine interface (HMI)
- OT network administration computers
- ICS software development computers

We consider a computer as attacked if a Kaspersky security solution blocked one or more threats on that computer during the period in review: a month, six months, or a year depending on the context as can be seen in the charts above. To calculate the percentage of machines whose malware infection was prevented, we take the ratio of the number of computers attacked during the period in review to the total number of computers in the selection from which we received anonymized information during the same period.

[2] We recommend that organizations subject to restrictions on sharing any data outside the corporate perimeter consider using Kaspersky Private Security Network.

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global Kaspersky project 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