Kaspersky ICS CERT

Threat landscape for industrial automation systems

Statistics for H1 2023

Kaspersky ICS CERT

13.09.2023 Version 1.0

Mid-year highlights

Figures

All threats

- In the first half of 2023, malicious objects (all types of threats) were blocked on 34% of ICS computers. This was 0.3 pp less than in the second half of 2022.
- In the second quarter of 2023, this percentage reached the highest quarterly level globally since 2022, 26.8%.
- The figure varied between 40.3% in Africa and 14.7% in Northern Europe by region, and
- between 53.3% in Ethiopia and 7.4% in Luxembourg by country.

Categories of malicious objects

- Malicious scripts and phishing pages were blocked on 12.7% of ICS computers
- Denylisted internet resources, on 11.3%
- Spyware, on 6%
- Malicious documents, on 4%
- Ransomware, on 0.32%. This is the lowest percentage since the beginning of 2020.

Main threat sources

- The internet was the source of threats blocked on 19.3% of ICS computers.
- Email clients – 6%
- Removable devices – 3.4%

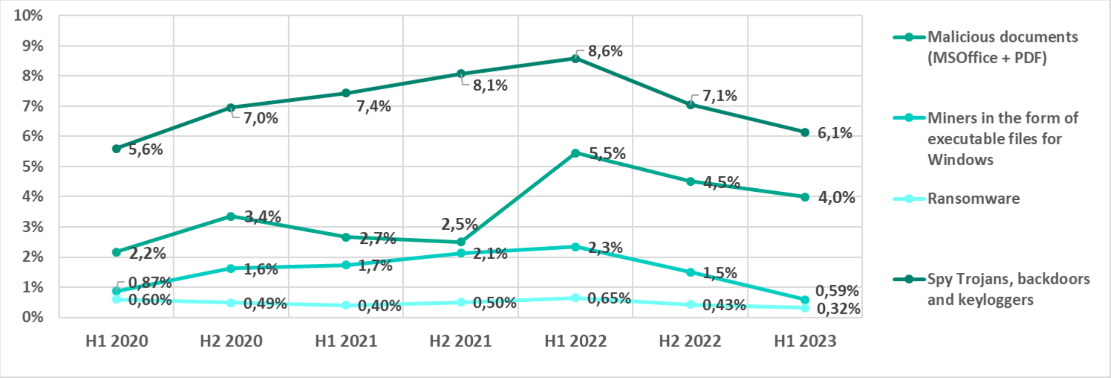
Good news

H1 2022 saw a noticeable increase in the percentage of ICS computers on which the following threats were blocked:

- Spyware
- Malicious documents
- Malicious miners in the form of Windows executables
- Ransomware

That was the bad news. Here comes the good news. The percentages of ICS computers on which all these threat categories were blocked had been declining since mid-2022.

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



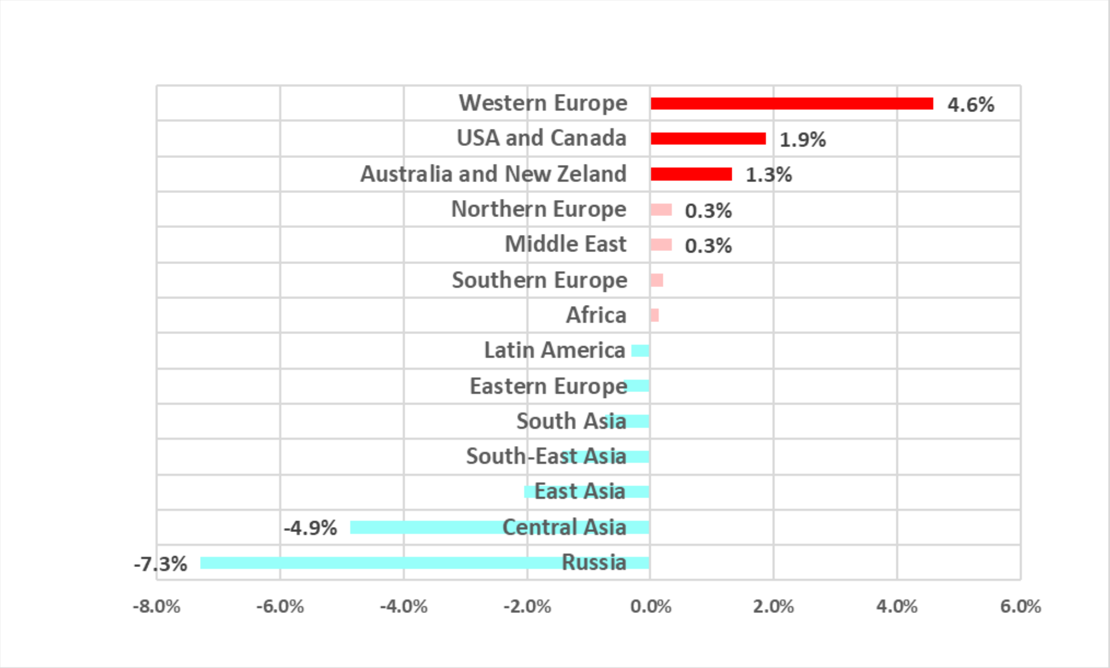
In H1 2023, the percentage of ICS computers on which these categories of threats were blocked, dropped in virtually every region. A few unlikely exceptions to this will be dealt with below.

Rankings where regions that do best were doing worst

Australia and New Zealand, the United States and Canada, Western Europe, and Northern Europe historically have had the lowest percentages of ICS computers on which malicious objects are blocked.

In H1 2023, however, those were the very regions where the percentages of attacked ICS computers increased by the most percentage points.

H1 2023 changes in the percentages of ICS computers on which malicious objects were blocked, by region

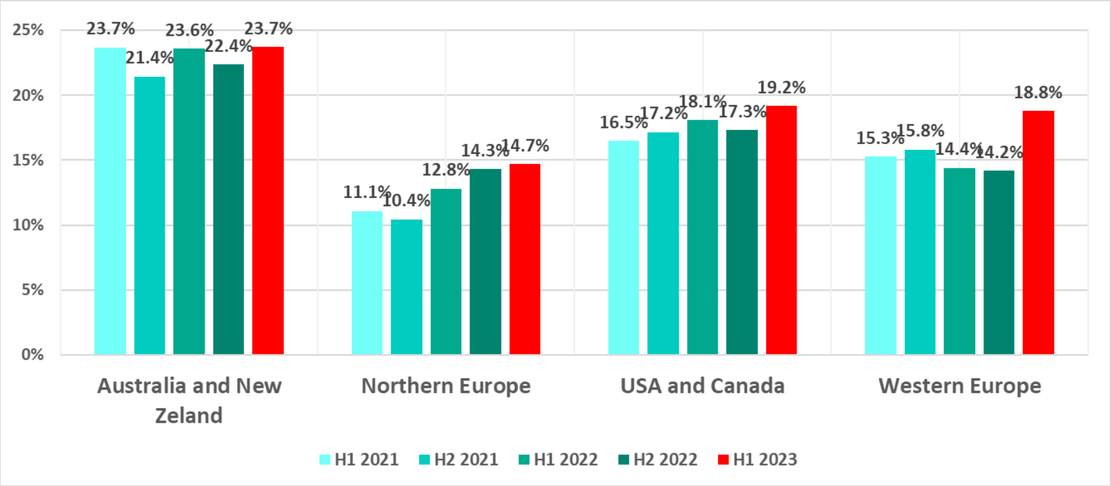


Australia and New Zealand see this figure vary from half-year to half-year, and it did not exceed previous periods' values in H1 2023.

In Northern Europe, and the United States and Canada, we recorded an upward trend in the percentage of attacked ICS computers.

In Western Europe, the percentage of computers on which malicious objects were blocked declined in 2022 before spiking in H1 2023 to exceed the previous two years' figures.

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

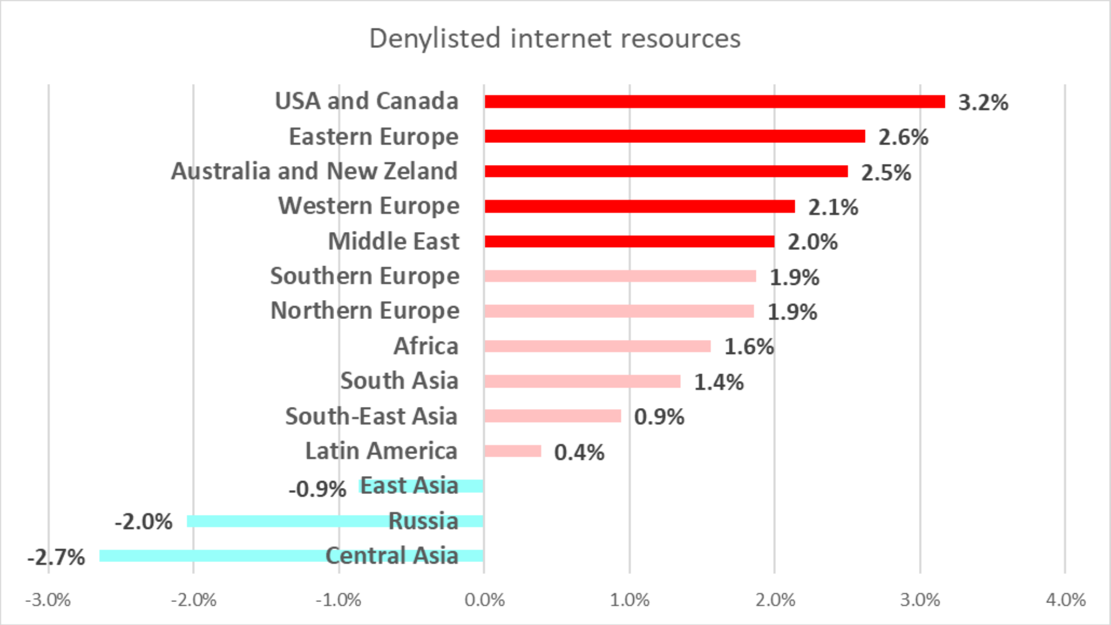


Let us anticipate a question by saying that **despite the increase in the percentage of attacked computers, these regions retained a minimal percentage by virtually every criterion**.

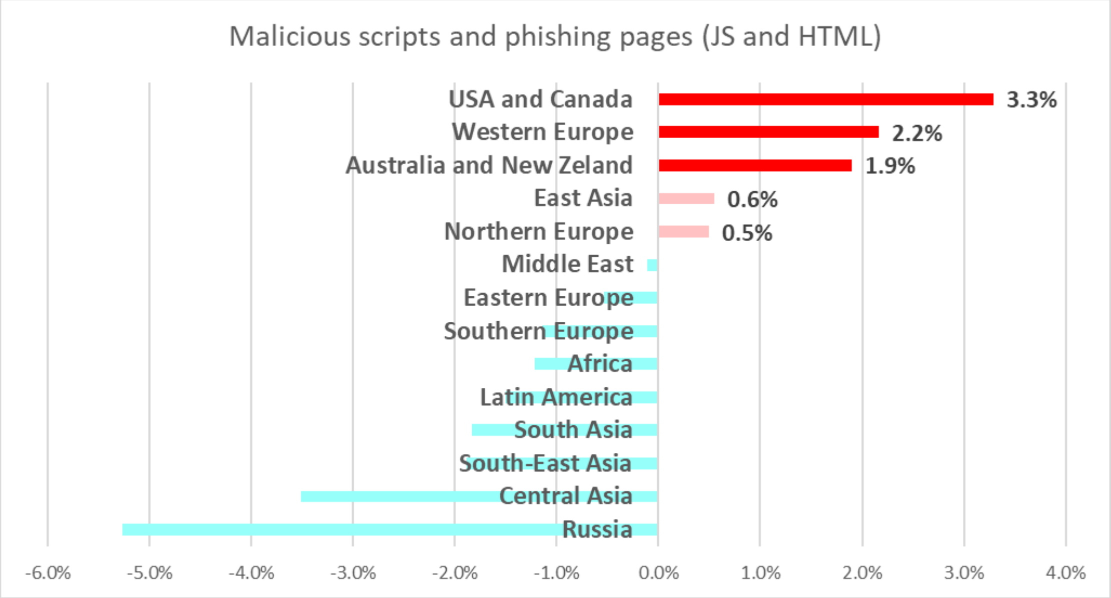
As for the **half-year increase**, these regions did top many lists in H1 2023.

Blocked denylisted internet resources, and malicious scripts and phishing pages were the biggest contributors to this increase in the historically safer regions.

H1 2023 changes in the percentages of ICS computers on which denylisted internet resources were blocked, by region



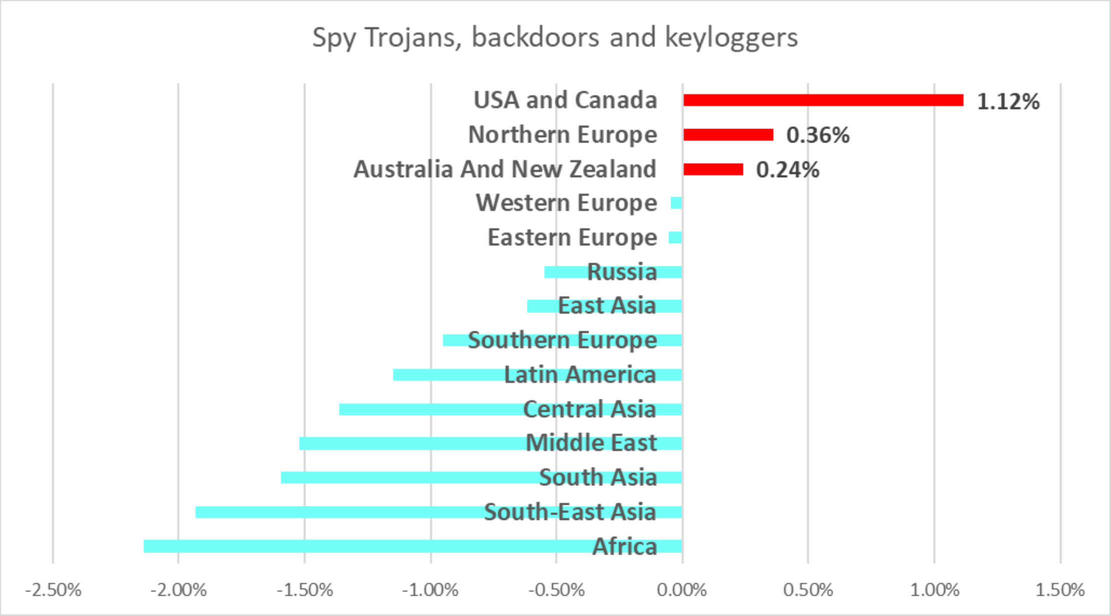
H1 2023 changes in the percentages of ICS computers on which malicious scripts and phishing pages were blocked, by region



Both threat types spread via the internet, while malicious scripts and phishing pages also spread via email. The percentage of ICS computers on which threats from these two sources were blocked in the United States and Canada, and Western Europe also increased the most among all regions.

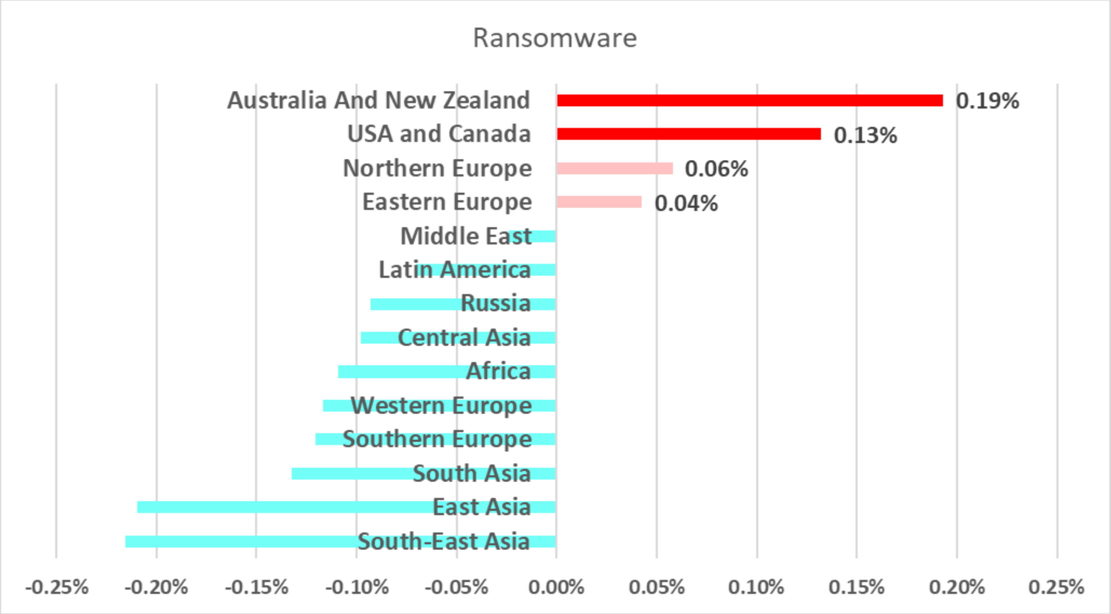
These are not the only bad lists these regions topped. The United States and Canada, Northern Europe, and Australia and New Zealand saw the largest growth in the percentage of computers on which spyware was blocked.

H1 2023 changes in the percentages of ICS computers on which spyware was blocked, by region



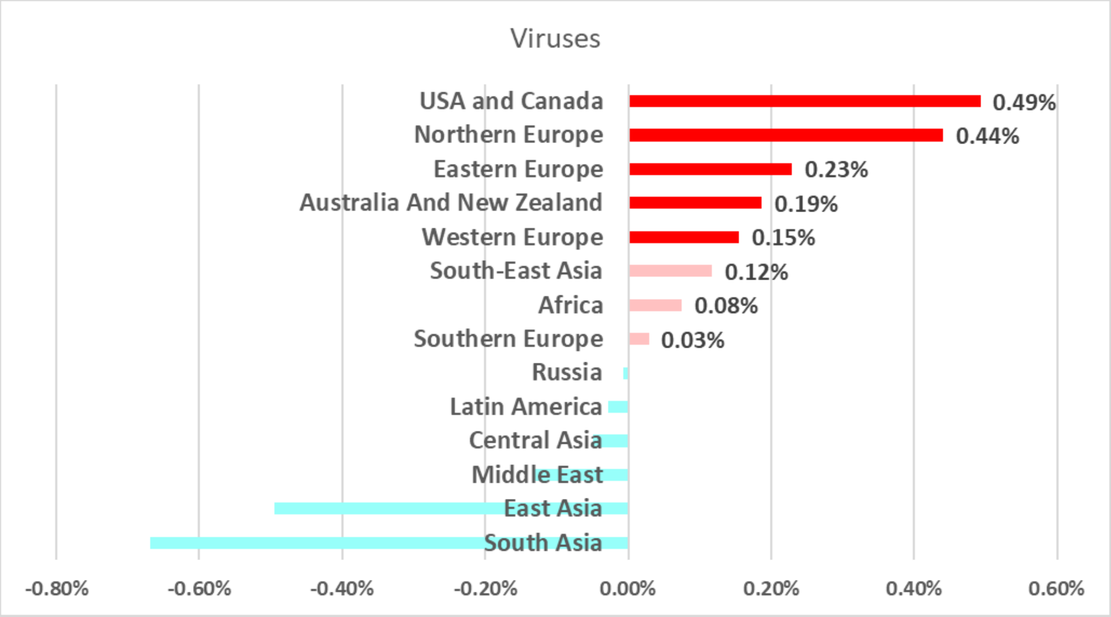
Note that the percentage of ICS computers attacked by ransomware in H1 2023 increased in four regions including Australia and New Zealand, and the United States and Canada, by the relatively significant respective values of 0.19 pp and 0.13 pp, and in Northern Europe.

H1 2023 changes in the percentages of ICS computers on which ransomware was blocked, by region

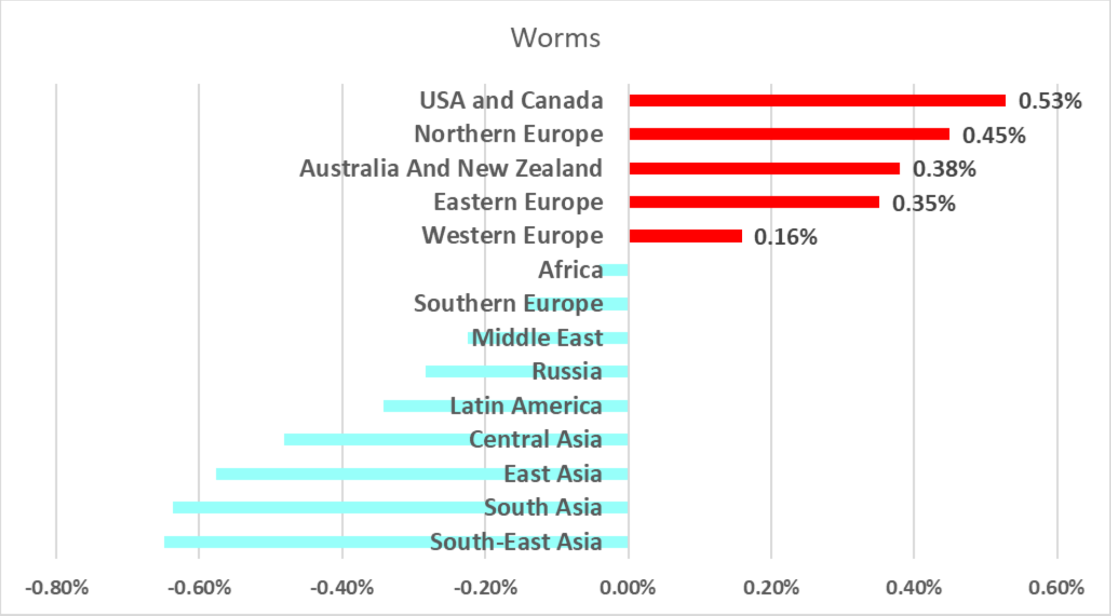


The percentages of computers on which viruses and worms were blocked were similarly unexpected. The five regions where these figures increased the most were the United States and Canada, Northern Europe, Australia and New Zealand, and Western Europe.

H1 2023 changes in the percentages of ICS computers on which viruses were blocked, by region

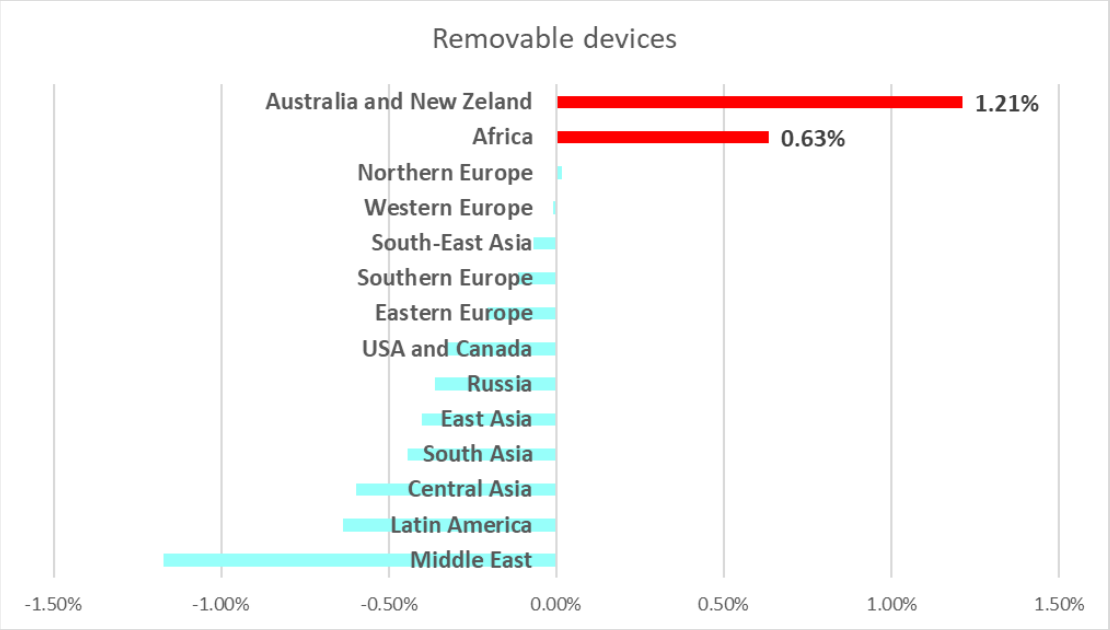


H1 2023 changes in the percentages of ICS computers on which worms were blocked, by region



Australia and New Zealand saw an increase in the number of computers on which threats were blocked after removable devices were connected.

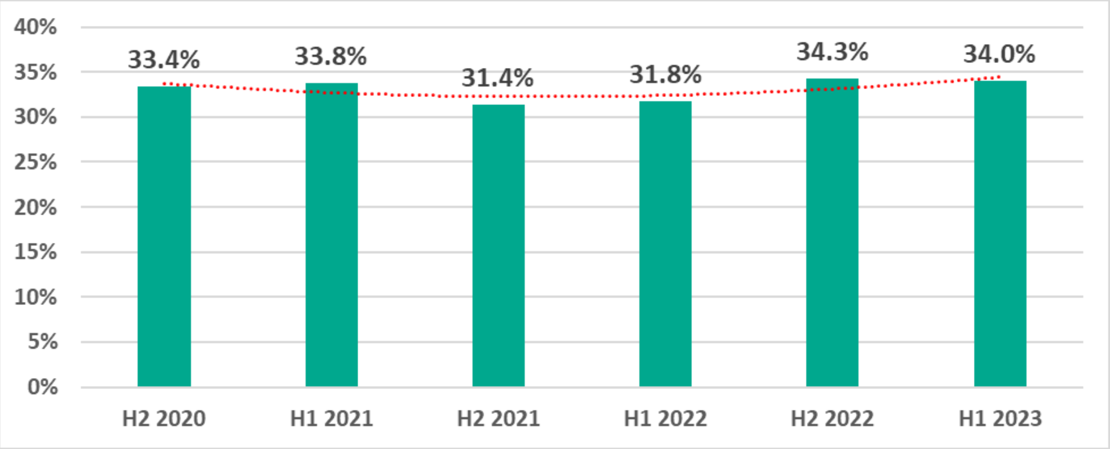
H1 2023 changes in the percentages of ICS computers on which threats were blocked after removable devices were connected, by region



Global threat statistics

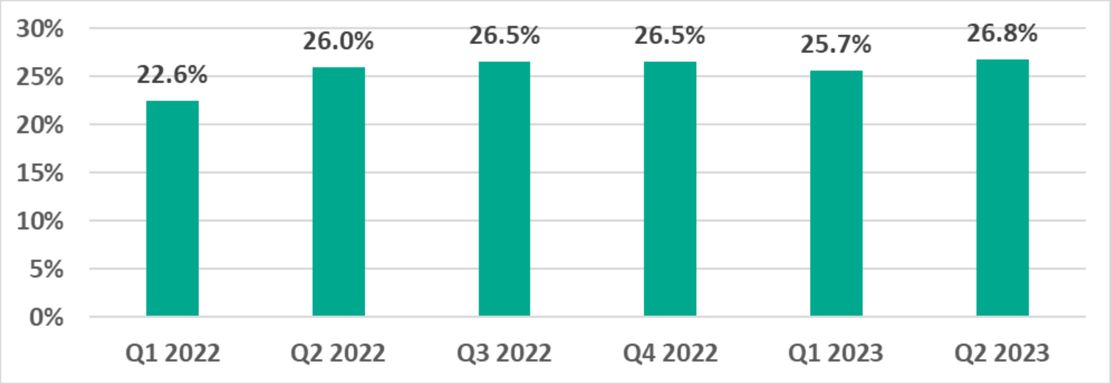
In the first half of 2023, the percentage of ICS computers on which malicious objects were blocked decreased from H2 2022 by just 0.3 pp to 34%.

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



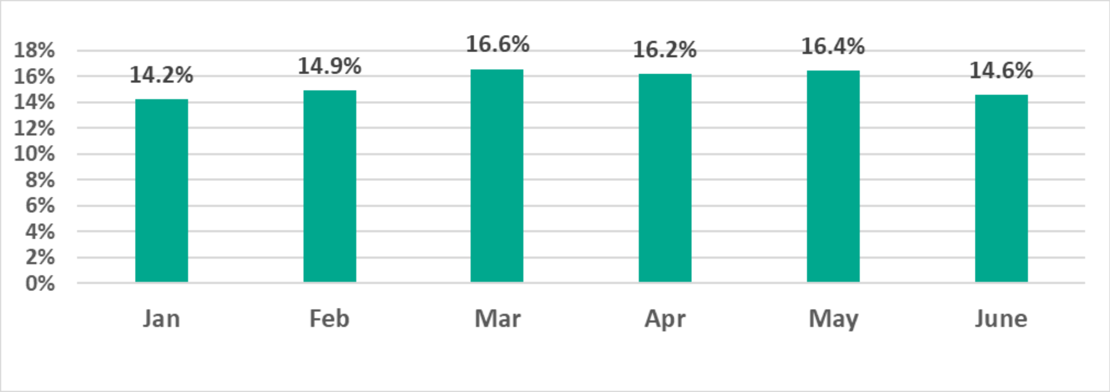
That said, the percentage of attacked ICS computers dropped in Q1 2023, but then rose again in Q2 2023, reaching highest quarterly figure since 2022.

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



In spring (March through May), the percentage of ICS computers on which malicious objects were blocked remained higher than in the other three months.

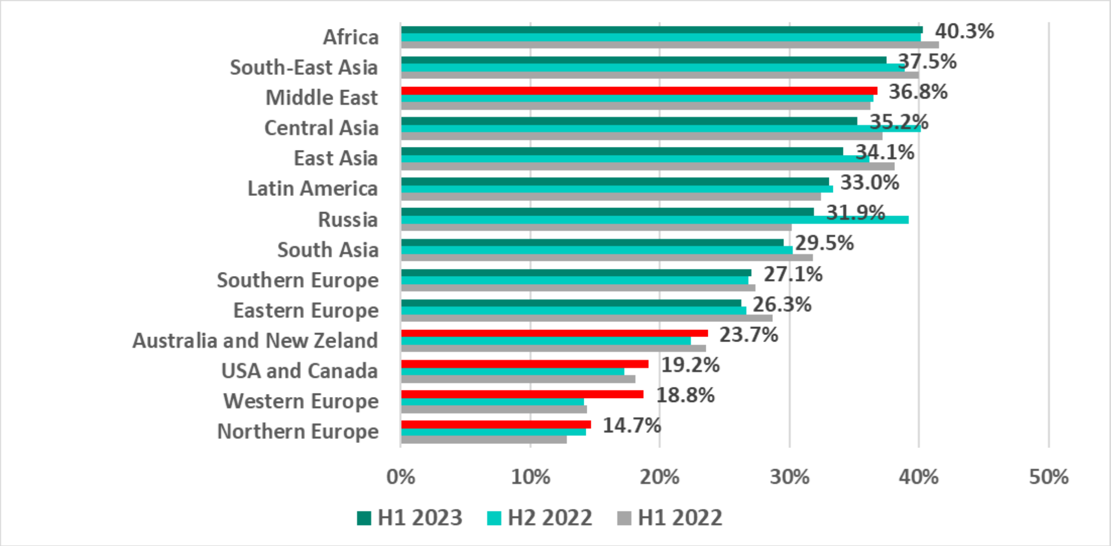
Percentage of ICS computers on which malicious objects were blocked, January-June 2023



Regions

The percentage of computers on which malicious activity was prevented varied across regions from 40.3% in Africa to 14.7% in Northern Europe.

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

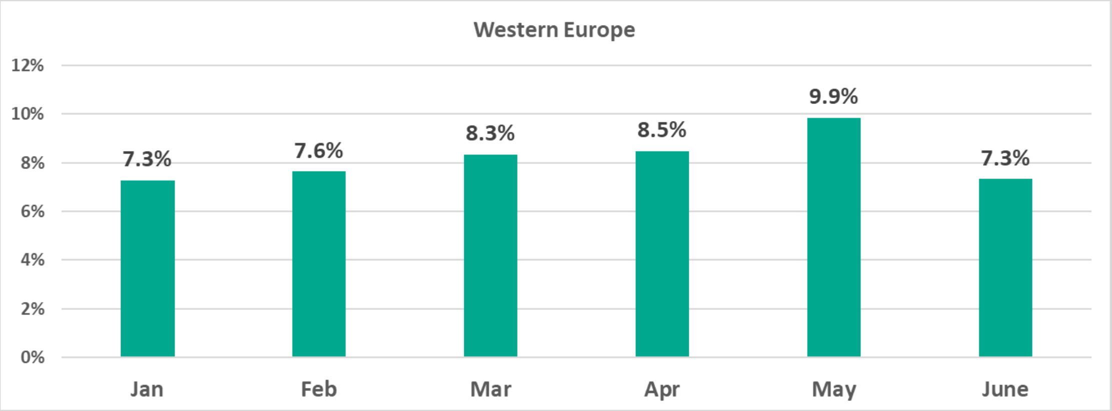


You may remember that in the previous half-year, the percentage of ICS computers in Russia and Central Asia on which malicious objects were blocked increased noticeably due to mass infection of websites, including those run by industrial companies, that used an outdated version of a popular Russian CMS. In H1 2023, the figures in both regions returned to values close to those of H1 2022.

As mentioned above, the most significant increases in the percentage of ICS computers on which malicious objects were blocked were recorded in Western Europe (4.6 pp), the United States and Canada (1.9 pp), as well as Australia and New Zealand (1.3 pp). Note the minor but steady growth in that percentage in Northern Europe and the Middle East (by 0.3 pp each).

Western Europe, which recorded the largest increase among all regions, saw the percentage of attacked ICS computers in H1 2023 grow every month up to May, and then drop to January's level in June.

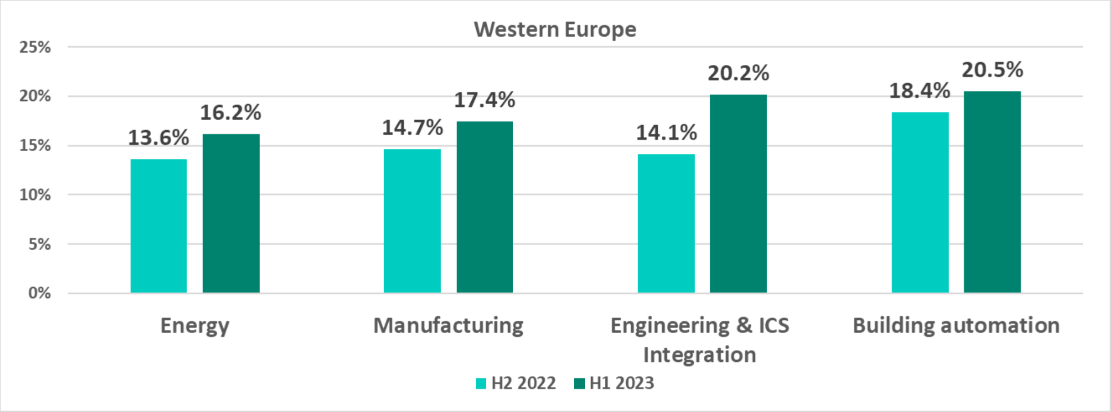
Western Europe. Percentage of ICS computers on which malicious objects were blocked, January-June 2023



Our data indicates that in H1 2023, some threat actors reinvented an old phishing technique that was first seen back in 2010 to target organizations in Europe, including industrial ones. The technique involves infecting a website with a malicious script that triggers a pop-up window resembling a Microsoft tech support window. The pop-up does not contain any links, but instead presents a phishing message and a local phone number to call. When a user calls the number, a threat actor answers the call and communicates in the local language, manipulating the unsuspecting user to download and install a remote access tool or a piece of multifunctional spyware. This technique leverages social engineering tactics to deceive users and gain unauthorized access to their systems, posing a serious threat to organizations, including industrial ones.

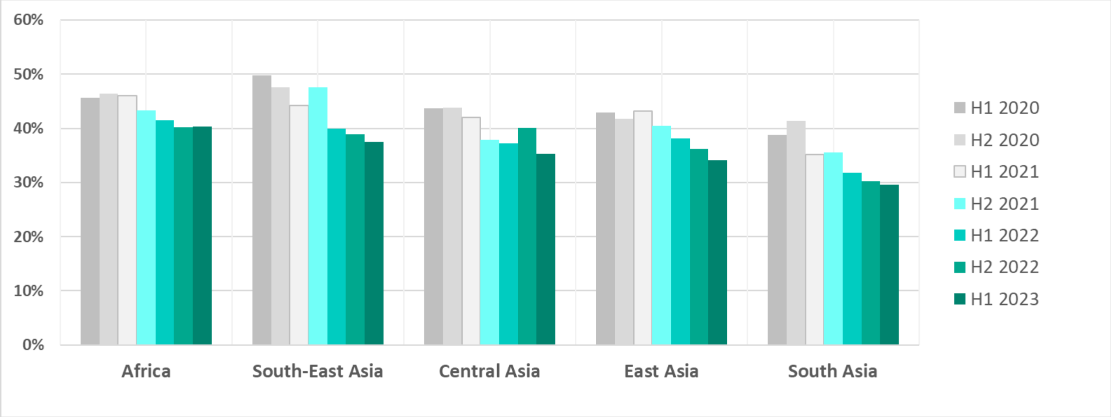
The industries under review in that region that saw the percentages increase the most were engineering and ICS integration (by 6.1 pp).

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



Most of the regions where the percentage of attacked computers increased in H1 2023 (Northern and Western Europe, the United States and Canada, and Australia and New Zealand) are usually at the bottom of the list. Africa and the Asian regions where the percentage of ICS computers on which malicious objects are blocked historically has been high, showed a downward trend.

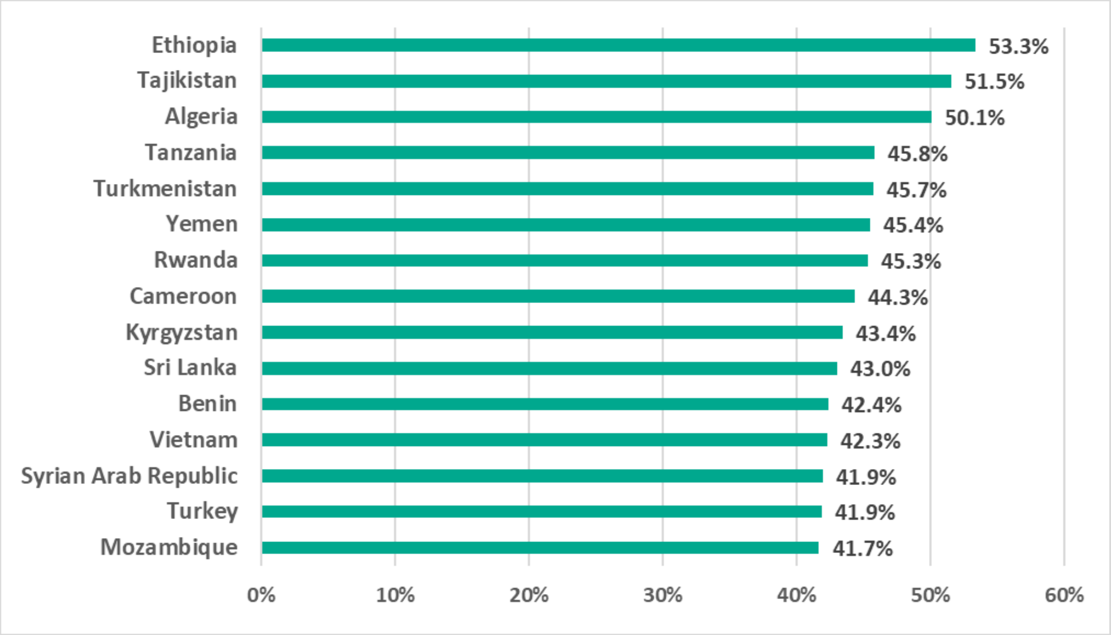
Percentage of ICS computers on which malicious objects were blocked in Africa and regions of Asia



Countries

The percentage of ICS computers on which malicious objects were blocked varied across countries from 53.3% in Ethiopia to 7.4% in Luxembourg.

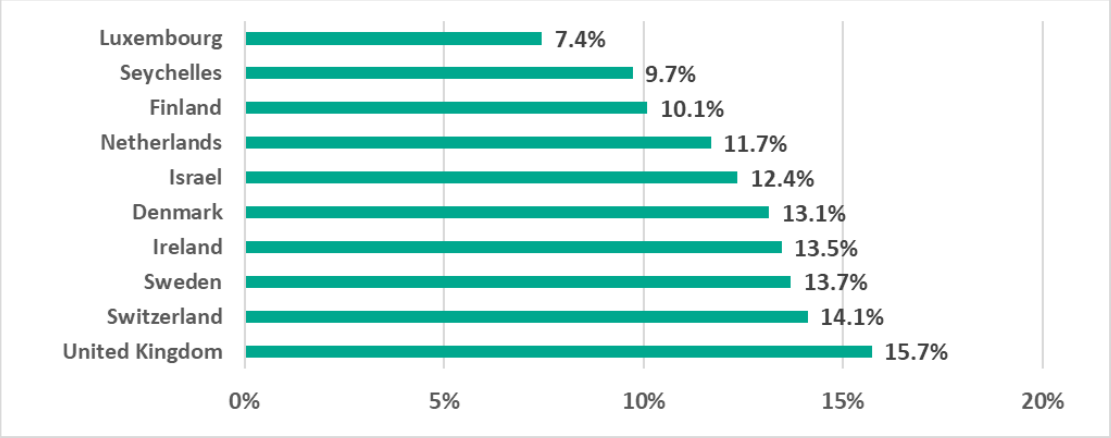
Fifteen countries and territories with the highest percentage of ICS computers on which malicious objects were blocked, H1 2023



Seven African, three Middle Eastern and three Central Asian countries were among the fifteen countries and territories in H1 2023 with the highest percentage of ICS computers on which malicious objects were blocked.

Half of the 10 countries that had the lowest figures were located in Northern Europe.

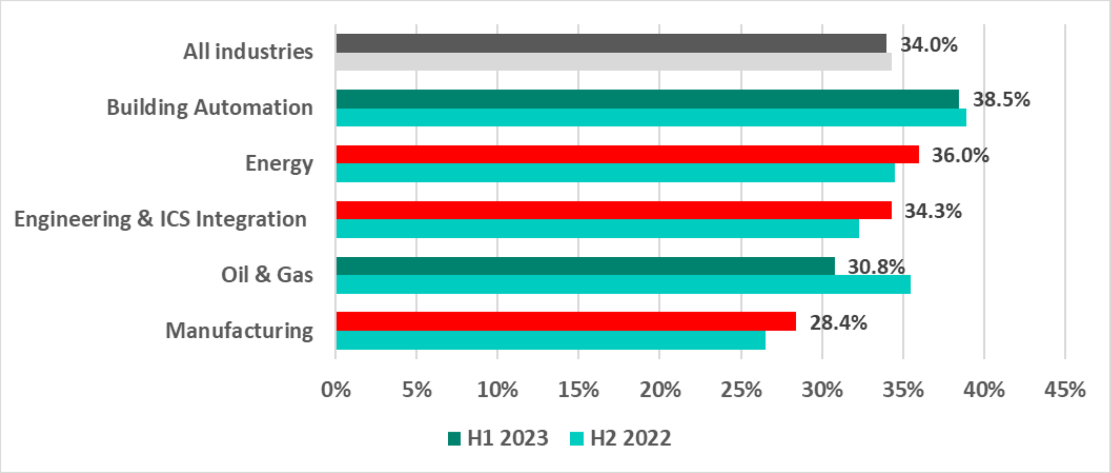
Ten countries and territories with the lowest percentage of ICS computers on which malicious objects were blocked, H1 2023



Individual industries

In H1 2023, the percentage of ICS computers on which malicious objects were blocked increased in engineering and ICS integration (by 2 pp), manufacture (by 1.9 pp) and energy (by 1.5 pp).

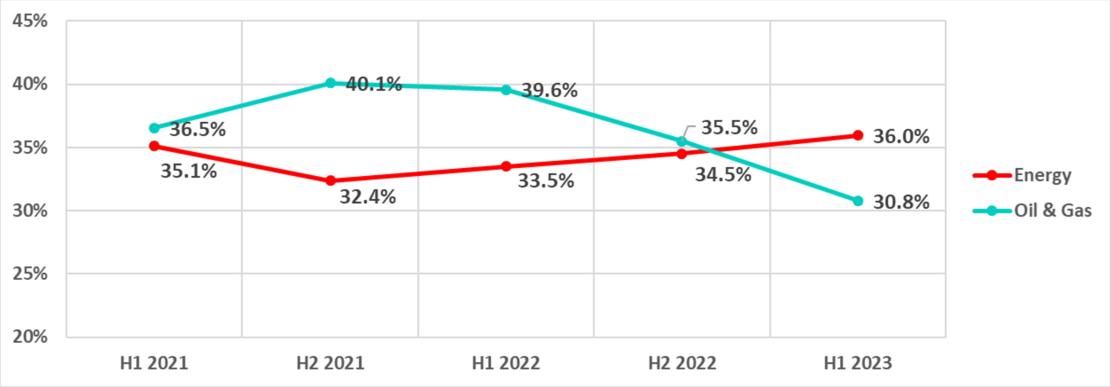
Percentage of ICS computers on which malicious objects were blocked in selected industries



Building automation is still the leader among the industries under review.

Energy and oil and gas have seen opposite trends in the percentage of ICS computers on which malicious objects were blocked since 2021.

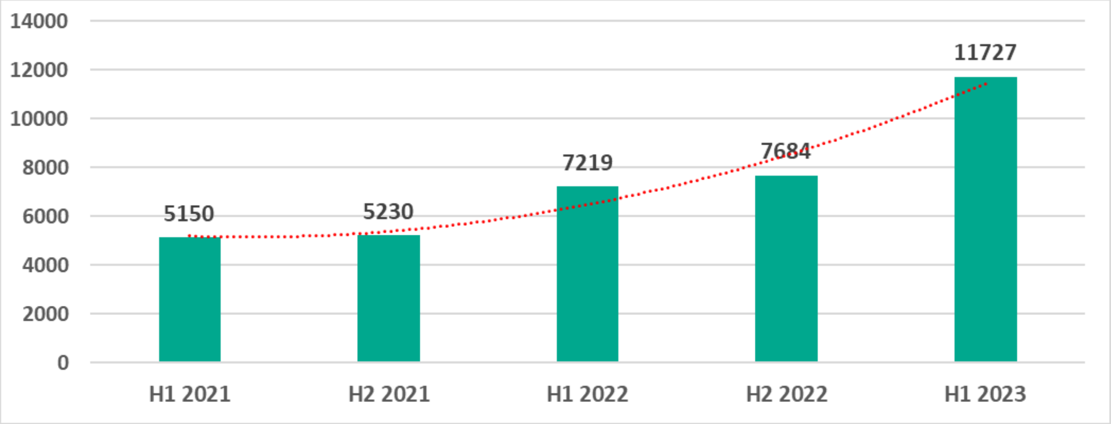
Percentage of ICS computers on which malicious objects were blocked in selected industries



The variety of malware detected

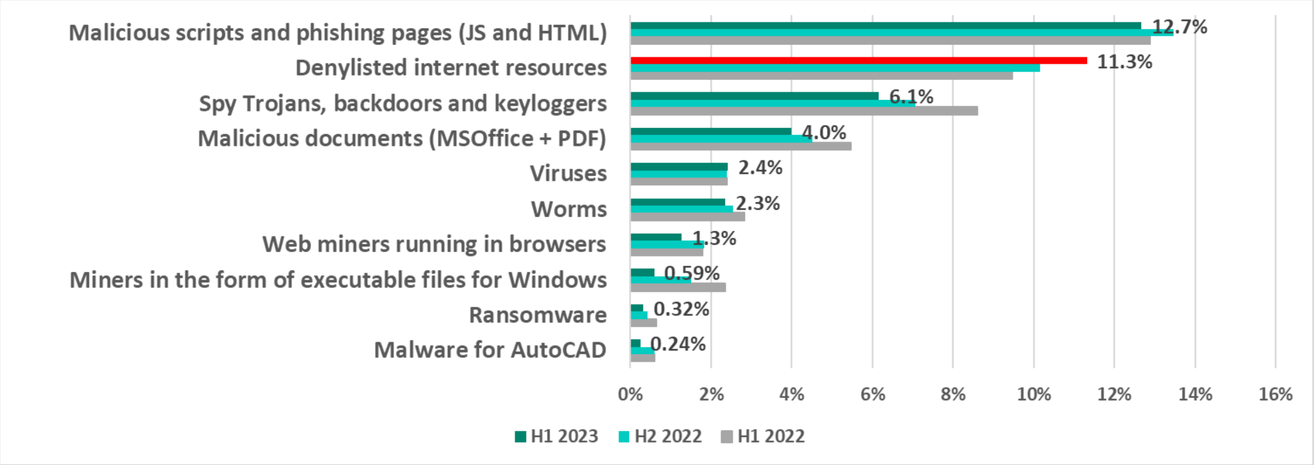
In H1 2023, Kaspersky security solutions blocked 11,727 different malware families in industrial automation systems.

Malware families blocked on ICS computers



Categories of malicious objects

Malicious objects that Kaspersky products block on ICS computers fall under many categories. A brief description of each type of threat is provided in a separate document.



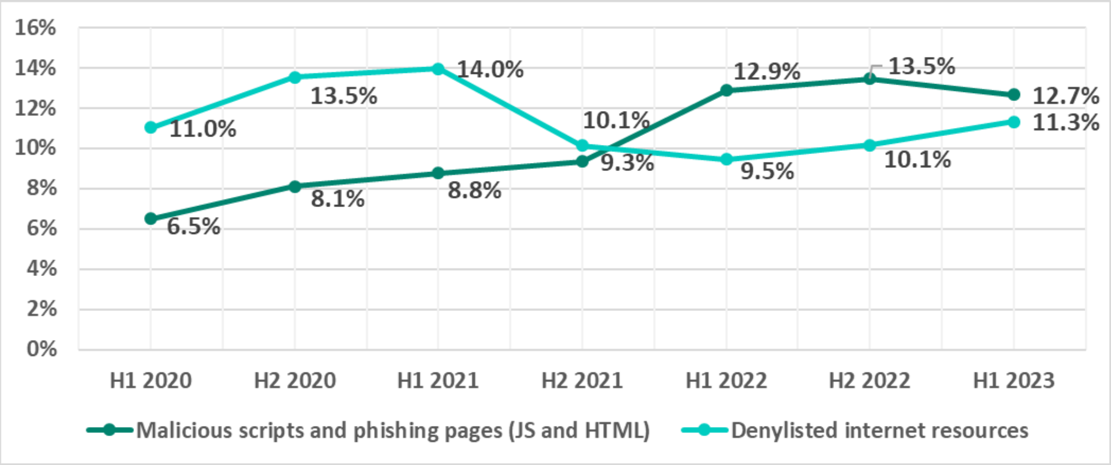
Percentage of ICS* computers on which the activity of malicious objects of various categories was prevented

**In many cases, two or more types of threats may have been blocked on a single computer during the reporting period. Therefore, the resulting percentages should not be added together.*

Only one of the categories grew in H1 2023: denylisted internet resources. The percentage of ICS computers on which threats in this category are blocked has grown for the second half-year in a row.

Until 2022, denylisted internet resources had topped the list of threat categories, but in 2022, they took second place to malicious scripts and phishing pages, which still remain at the top of the list. Yet, the values for these two types of threats were converging.

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



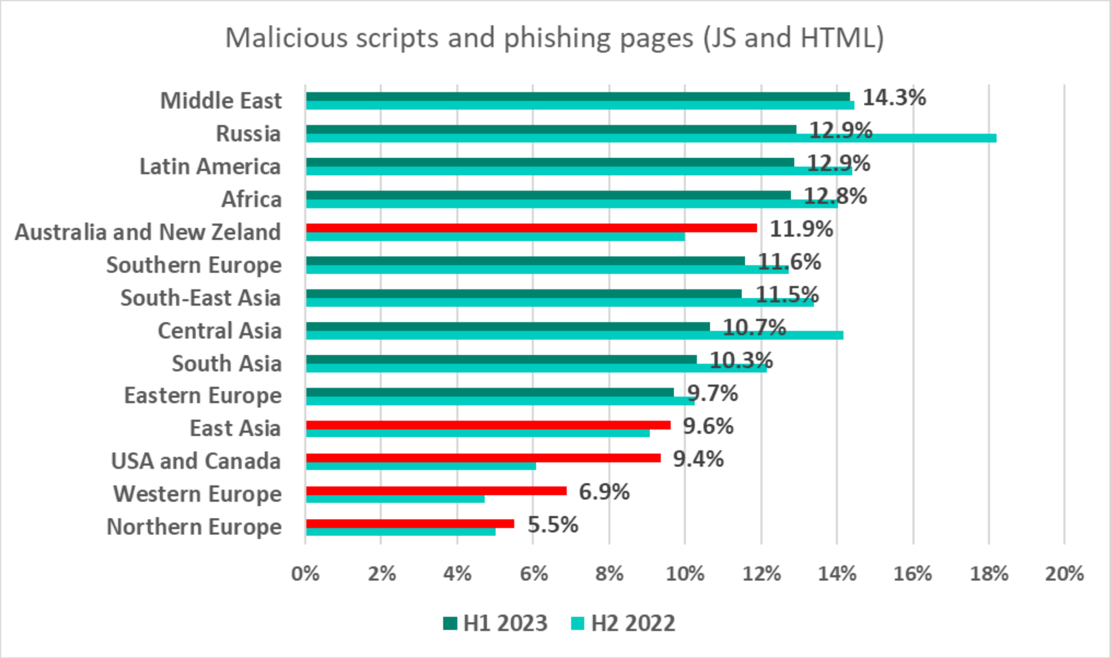
Malicious scripts and phishing pages (JS and HTML)

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

Malicious scripts serve a broad range of goals: from collecting data, tracking and forwarding users to malicious websites, to downloading various malware, such as spyware and/or covert crypto miners, to the system or the browser.

The regions with the highest percentage of ICS computers on which malicious scripts and phishing pages were blocked were the Middle East and Russia. The figure increased in five regions over the half-year, mostly in the United States and Canada (by 3.3 pp), Western Europe (by 2.2 pp), and Australia and New Zealand (by 1.9 pp).

Regions ranked by percentage of ICS computers on which malicious scripts and phishing pages were blocked, H1 2023

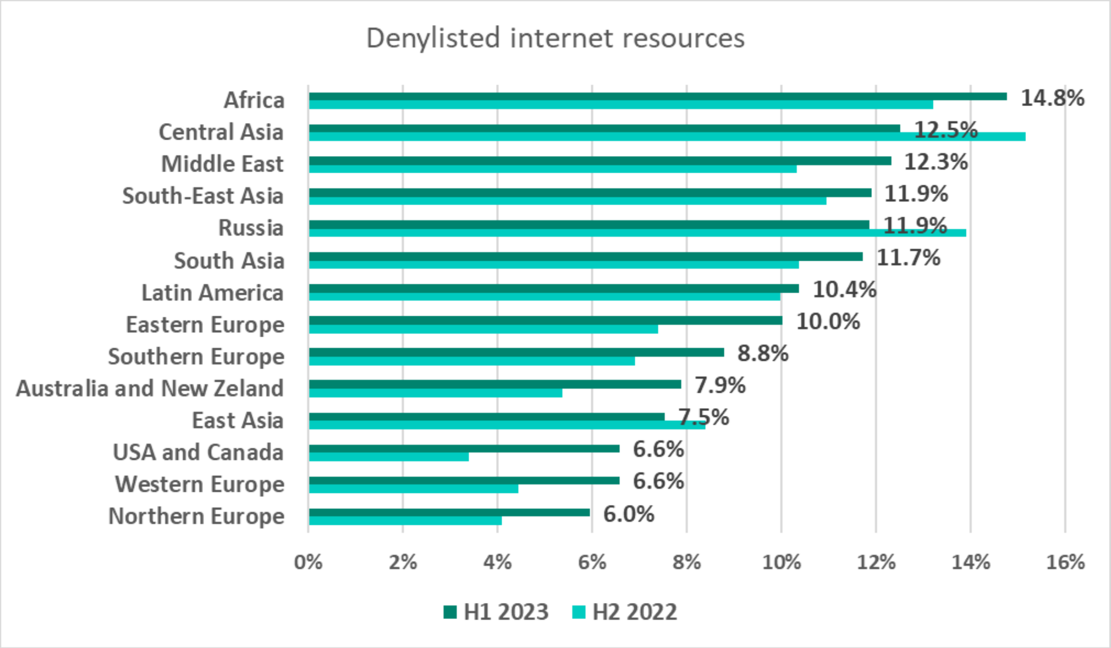


The countries with the highest percentage of ICS computers on which malicious scripts and phishing pages were blocked were Kyrgyzstan (21%) and Afghanistan (20.9%).

Denylisted internet resources

Africa was the region with the highest percentage of ICS computers on which denylisted internet resources were blocked. Not surprisingly, Africa also had the highest percentage of ICS computers on which threats that originated on the internet were blocked (see below under "Main threat sources").

Regions ranked by percentage of ICS computers on which denylisted internet resources were blocked, H1 2023



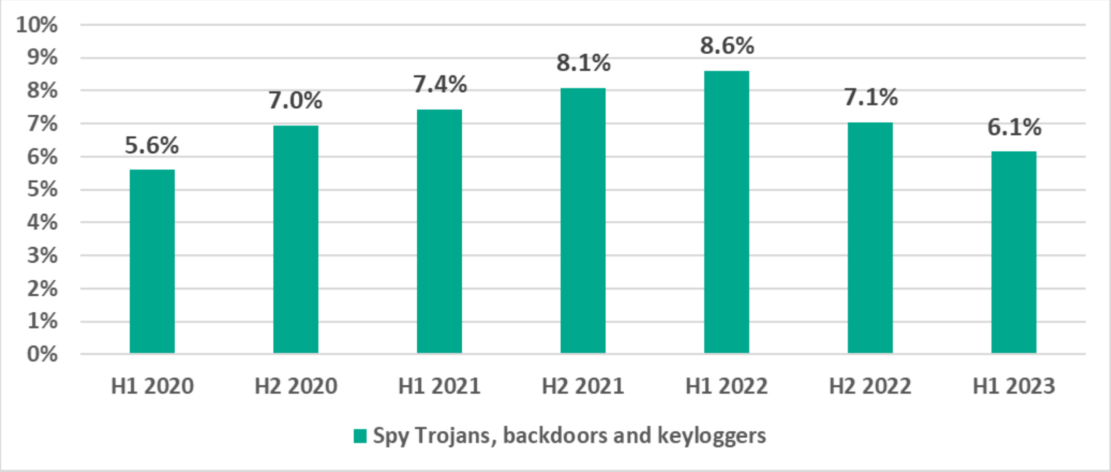
As mentioned above, denylisted internet resources were the only threat category where the percentage of ICS computers on which the threat was blocked increased worldwide. This figure grew in most regions during the half-year, with the largest increases recorded in the United States and Canada (3.2 pp), Eastern Europe (2.6 pp), and Australia and New Zealand (2.5 pp).

The countries with the highest percentage of ICS computers on which denylisted internet resources were blocked were Algiers (21.8%) and Afghanistan (20.2%).

Spyware

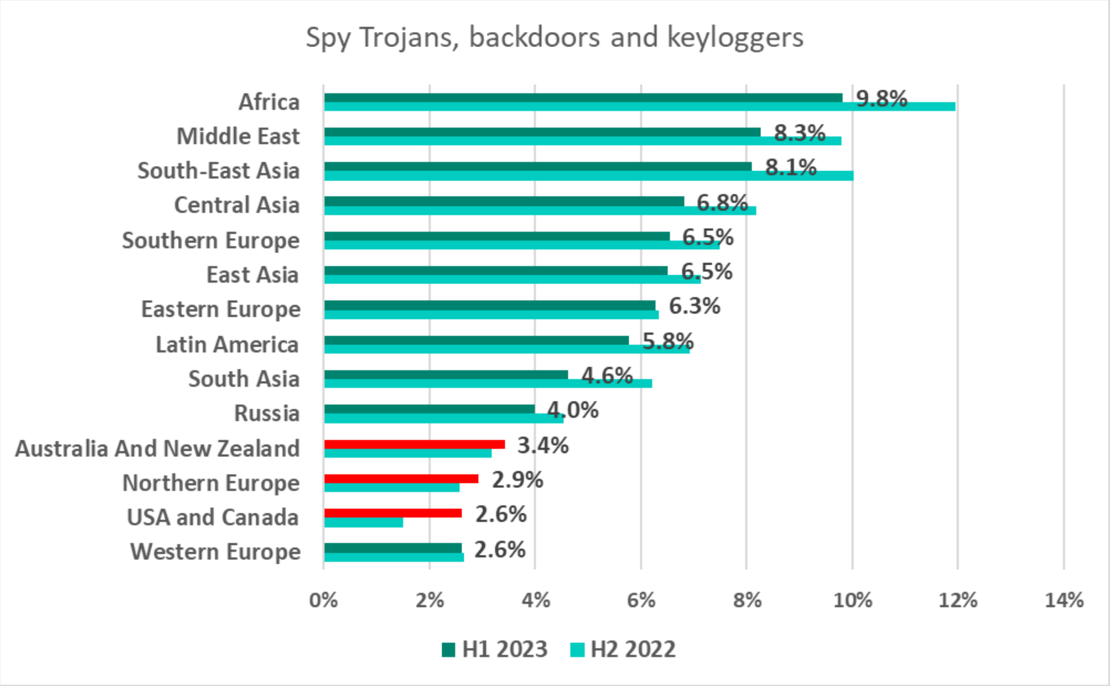
The percentage of ICS computers on which spyware is blocked continued to decline. Earlier, we saw the figure rise from 2020 through H1 2022.

Percentage of ICS computers on which spyware was blocked



Africa had the highest percentage of ICS computers on which spyware was blocked in H1 2023. The Middle East and Southeast Asia had similarly high percentages.

Regions ranked by percentage of ICS computers on which spyware was blocked in H1 2023

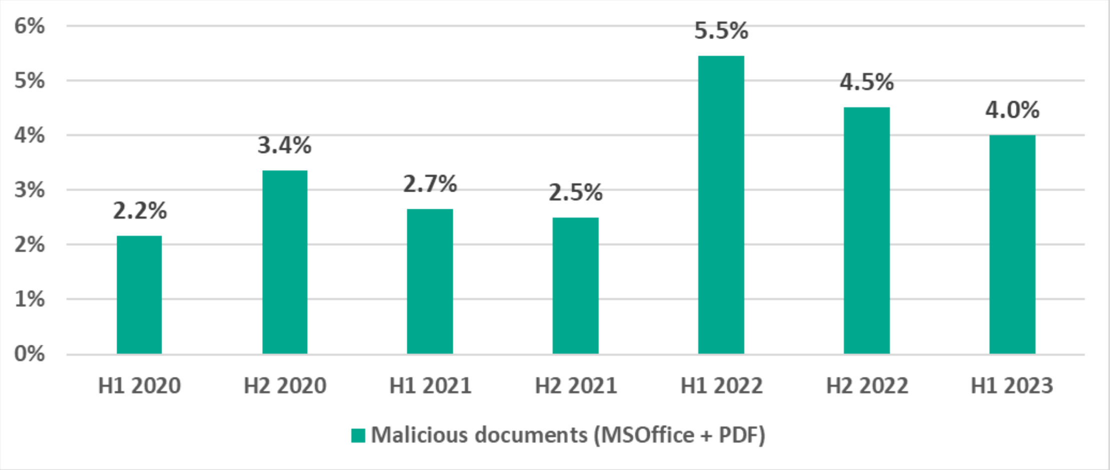


The leaders among countries and territories were Tajikistan (18.9%), Algiers (16.7%) and Afghanistan (16.6%).

Malicious documents (MSOffice+PDF)

Hackers spread malicious documents via phishing messages and use them in attacks which aim for primary infection. The global percentage of ICS computers on which threats in this category were blocked more than doubled in H1 2022 and had declined since. Yet in H1 2023, it remained higher than in 2020–2021.

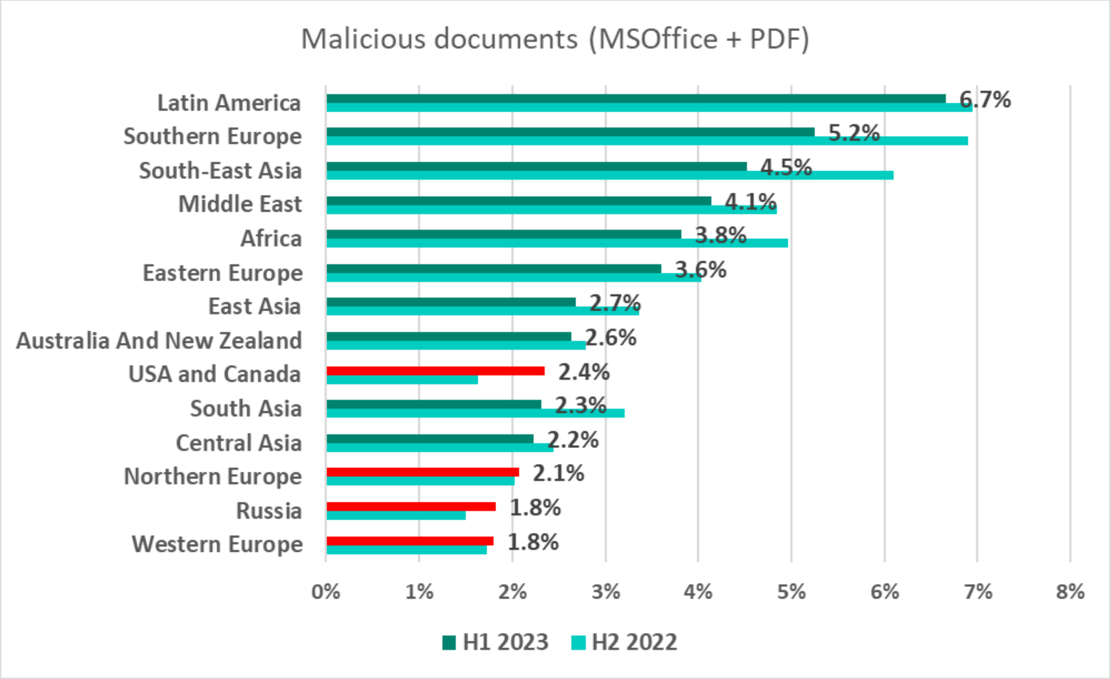
Percentage of ICS computers on which malicious documents were blocked



The regions with the highest figures were Latin America and Southern Europe. These regions also had the highest percentages of ICS computers on which email threats were blocked.

The United States and Canada saw the largest increase (by 0.72 pp) in the percentage of computers on which malicious documents were blocked.

Regions ranked by percentage of ICS computers on which malicious documents were blocked, H1 2023



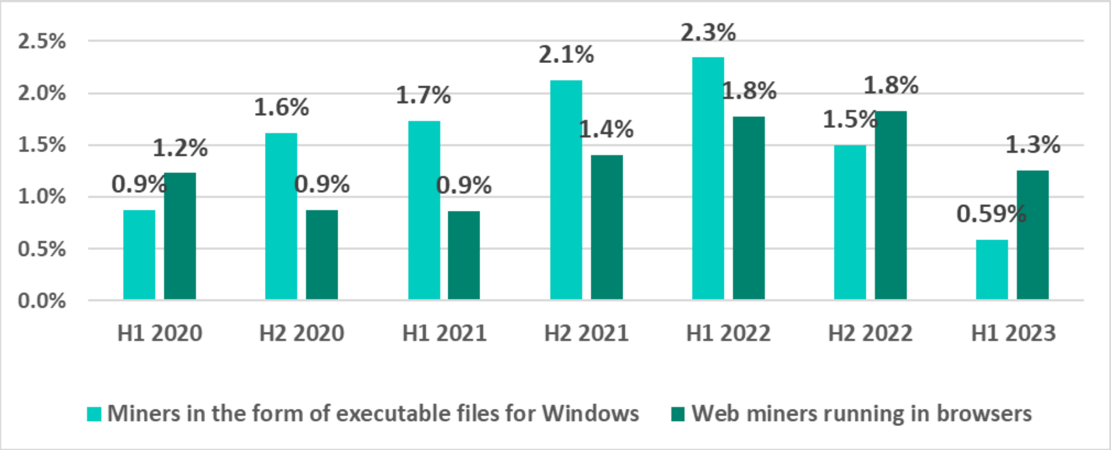
The countries with the highest percentage of ICS computers on which malicious documents were blocked were Algiers (16.7%) and Afghanistan (16.6%).

Malicious cryptocurrency miners

Miners often spread via websites to which users are redirected with the help of malicious scripts that hackers deploy on various media and pirating sites.

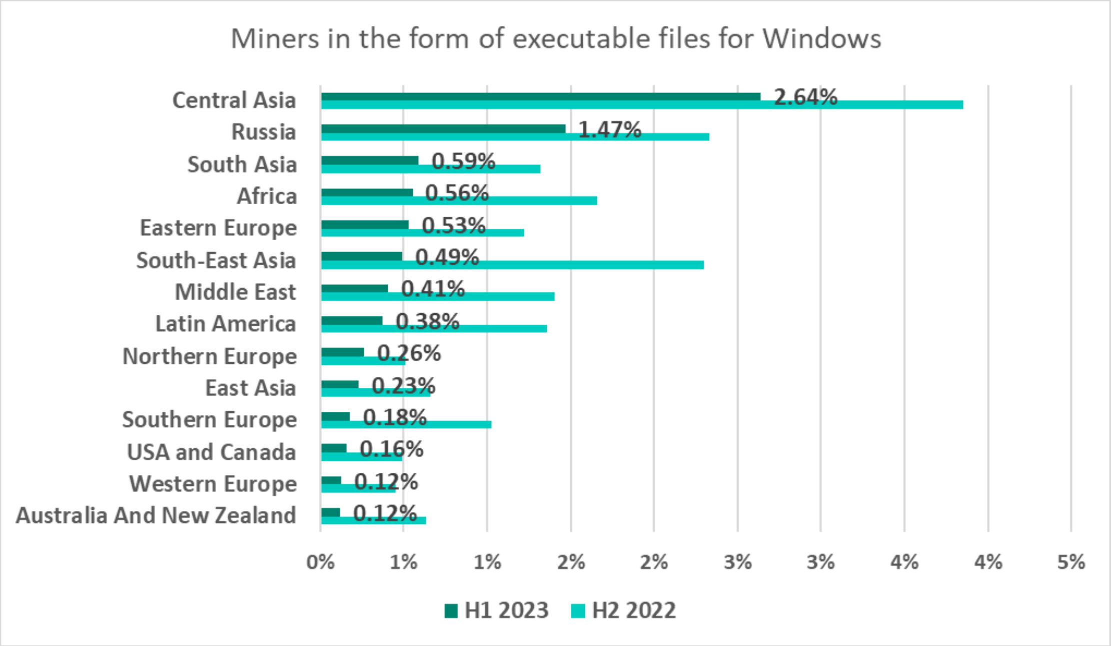
The global percentage of ICS computers on which malicious miners (both Windows executables and web miners) were blocked decreased in H1 2023.

Percentage of ICS computers on which malicious programs for covert crypto mining were blocked



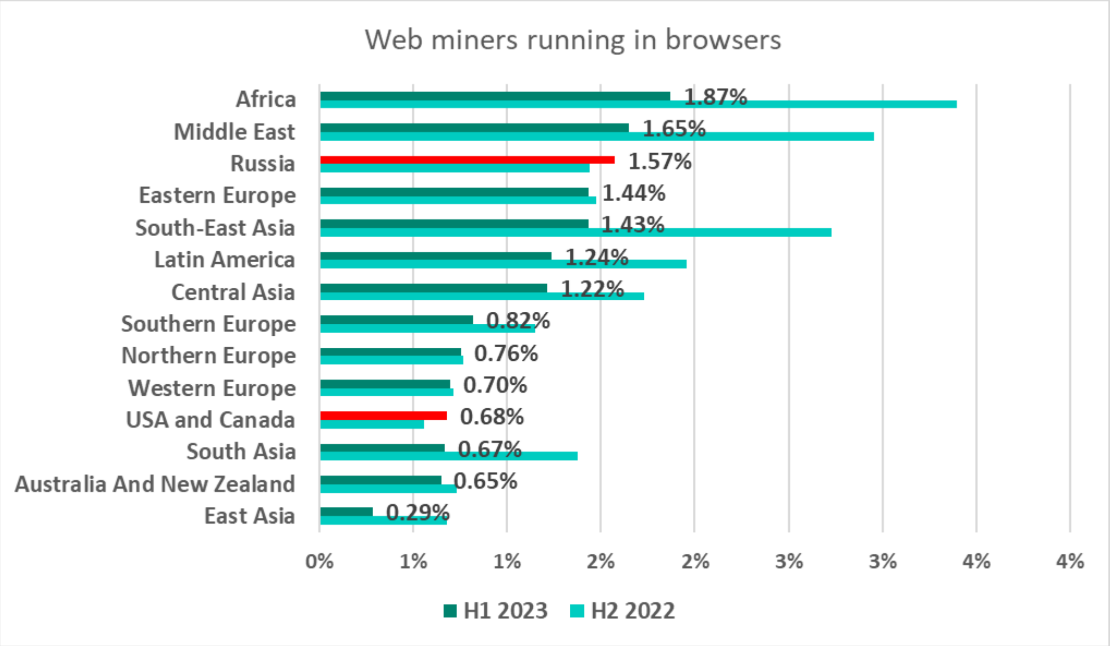
Central Asia was the region with the highest percentage of ICS computers on which miners – Windows executable files were blocked in H1 2023. The countries and territories with the highest percentage were Tajikistan (7.9%) and Turkmenistan (7.4%).

Regions ranked by percentage of ICS computers on which miners – executable files were blocked in H1 2023



Africa was the leader among regions by percentage of computers on which web miners were blocked. Russia, and the United States and Canada saw the percentage increase over the half-year, by 0.13 pp and 0.12 pp, respectively.

Regions ranked by percentage of ICS computers on which web miners running in browsers were blocked in H1 2023



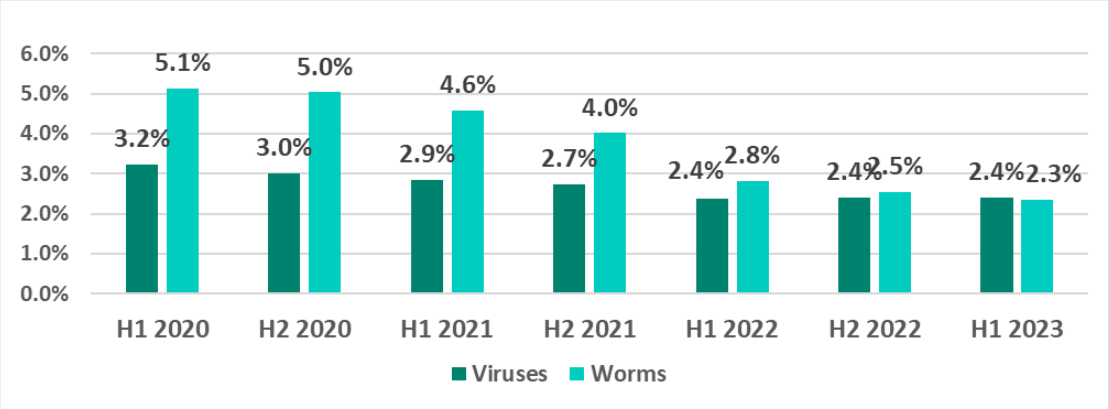
Serbia was the leader among the countries and territories with the highest percentage of ICS computers on which web miners were blocked, with 6.4%.

Viruses and worms

The percentage of ICS computers on which worms were blocked continued to decrease. We believe this is an indirect indication of the systematic use of security solutions in OT environments, which eliminates infection hotspots and prevents the spread of self-propagating malware.

The percentage of ICS computers on which viruses were blocked did not change in H1 2023.

Percentage of ICS computers on which viruses and worms were blocked



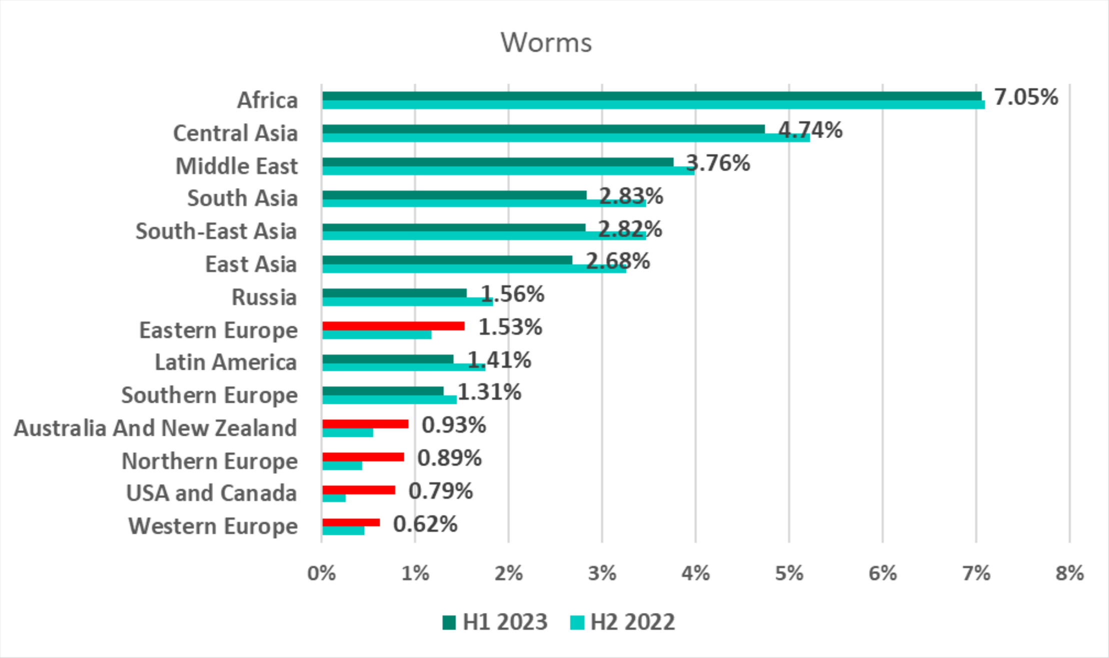
Viruses and worms spread across ICS networks by means of removable media, shared folders, infected files, such as backups, and network attacks on outdated software, such as Radmin2.

Many viruses and worms still circulating are old, and their command-and-control servers have long been shut down. Besides undermining the security of infected systems, for example, by opening network ports and changing settings, these older worms and viruses can potentially cause software to quit unexpectedly or create denial-of-service conditions.

Newer worm varieties, which malicious actors use to spread spyware, ransomware and miners, can be found on ICS networks as well. 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 on OT networks, using previously stolen authentication credentials or bruteforcing passwords.

The percentage of ICS computers on which worms were detected was still very high in Africa, making that region the leader by percentage of ICS computers on which threats were blocked after removable devices were connected. The United States and Canada, and Northern Europe saw the largest increases during the half-year, by 0.53 pp and 0.45 pp, respectively.

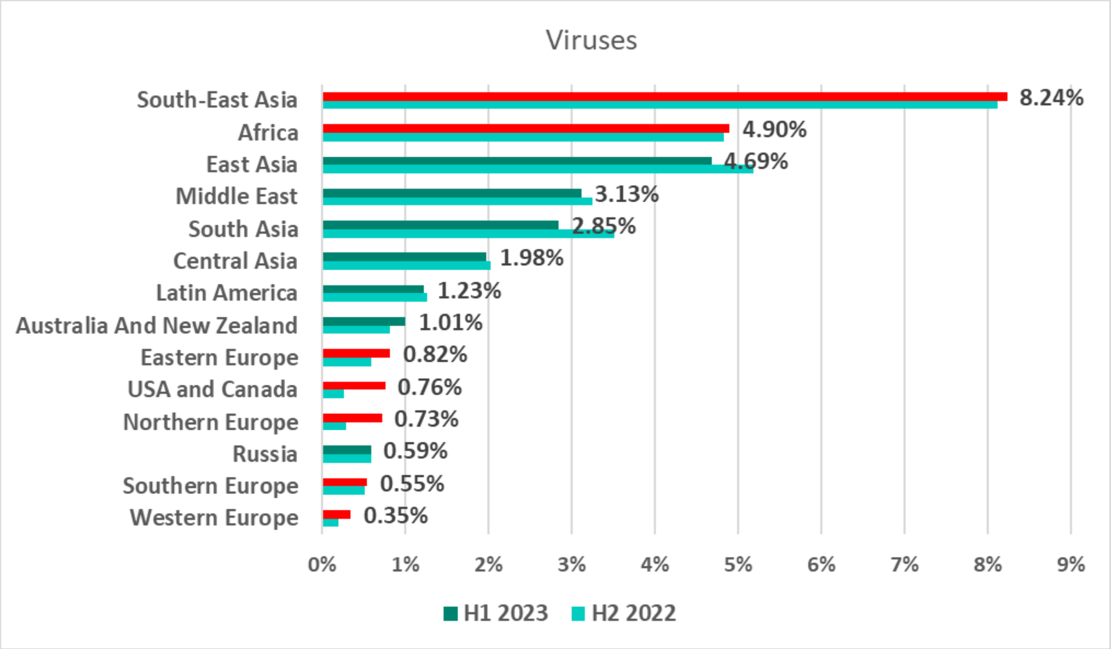
Regions ranked by percentage of ICS computers on which worms were blocked in H1 2023



The highest percentage of ICS computers on which worms were detected was recorded in Mali (20.8%). Note that Turkmenistan (18%) was among the five countries with the highest figures alongside African countries.

The virus issue remained relevant for Southeast Asia. The percentage of ICS computers on which viruses were blocked grew in many regions, mostly the United States and Canada (by 0.49 pp), and Northern Europe (by 0.44 pp).

Regions ranked by percentage of ICS computers on which viruses were blocked in H1 2023

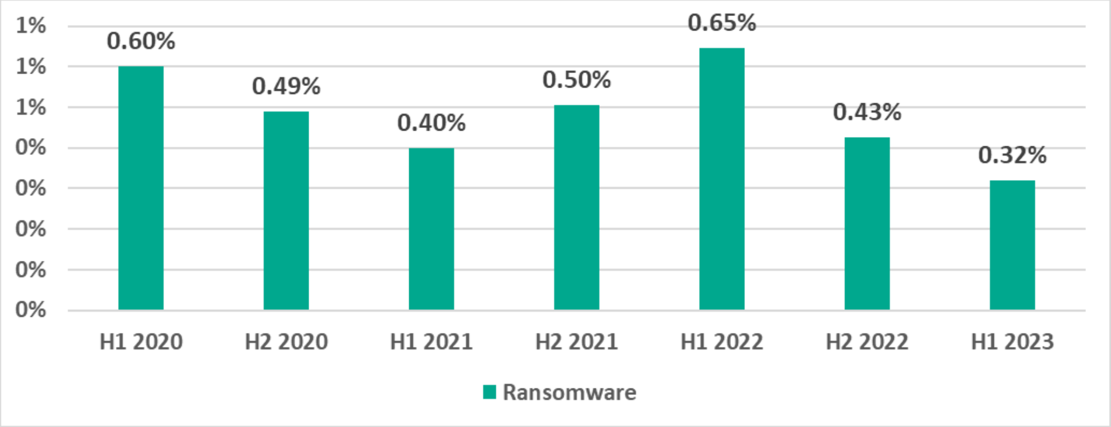


Afghanistan (16.6%), Vietnam (14.1%) and Yemen (13.8%) were among the countries and territories with the highest percentage of ICS computers on which viruses were blocked.

Ransomware

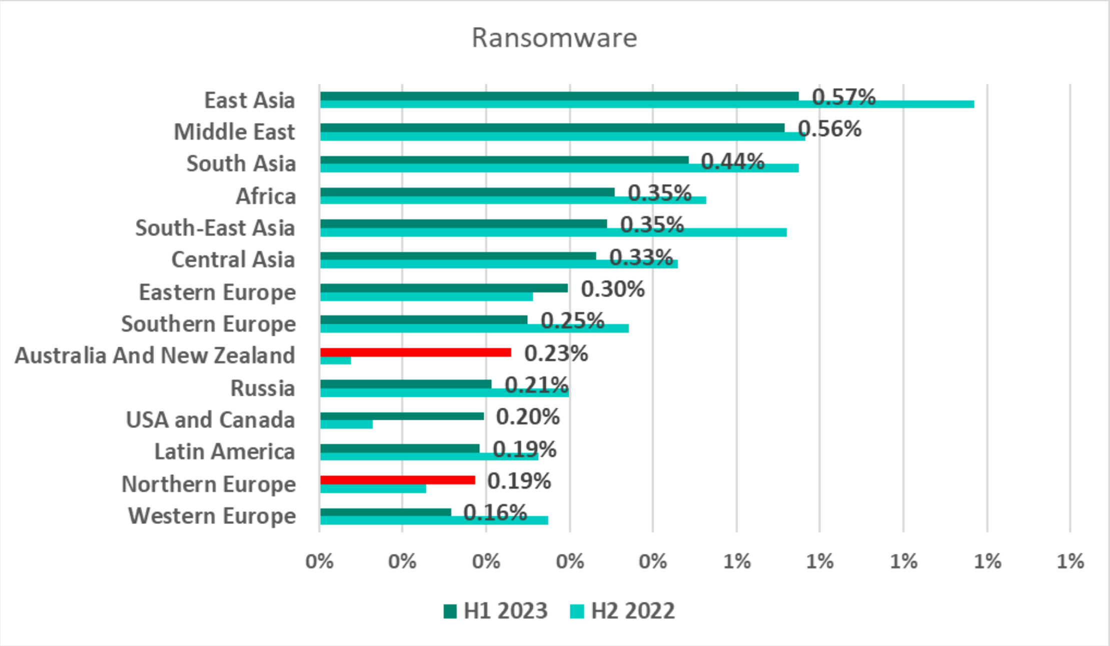
After the percentage of ICS computers on which ransomware was blocked increased in H1 2022, it dropped to the lowest level since 2020 in H1 2023.

Percentage of ICS computers on which ransomware was blocked



East Asia and the Middle East were the regions with the highest percentage of ICS computers attacked by ransomware in H1 2023.

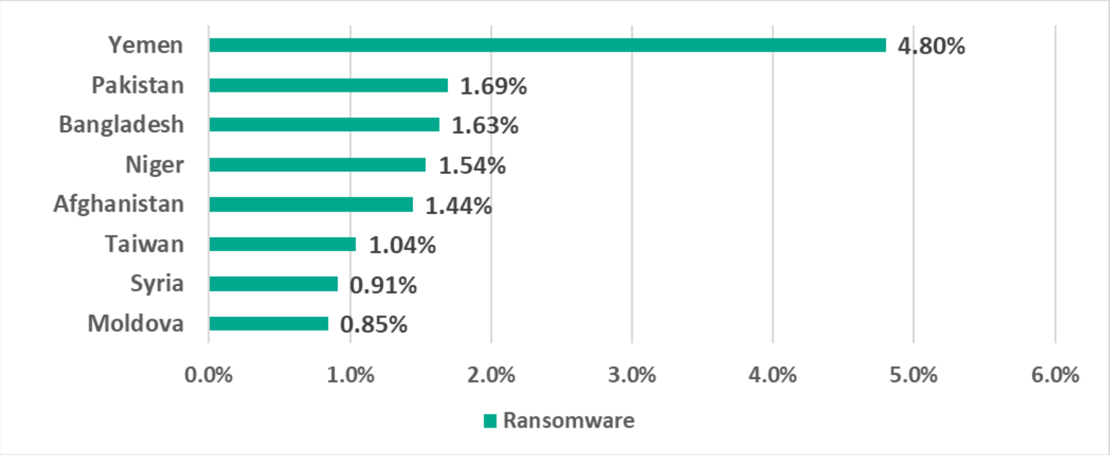
Regions ranked by percentage of ICS computers on which ransomware was blocked in H1 2023



The percentage of ICS computers attacked by ransomware shrank in most regions of the world. It grew by 0.19 pp in Australia and New Zealand, by 0.13 pp in the United States and Canada, and slightly in Northern and Eastern Europe.

Of all countries and territories, Yemen had by far the highest percentage of ICS computers on which ransomware was blocked in H1 2023.

Ten countries and territories with the highest percentage of ICS computers on which ransomware was blocked in H1 2023



One European country, Moldova, unexpectedly became one of the half-year's 10 leaders.

Malware for AutoCAD

East Asia had the highest percentage (3.1%) of ICS computers on which AutoCAD malware, viruses specifically, was blocked. This category of threats is detected on computers that are part of OT networks, for instance, in network folders and on engineering workstations.

The countries with the highest percentage of ICS computers on which malicious AutoCAD malware was blocked were China (2.6%) and Vietnam (1.5%).

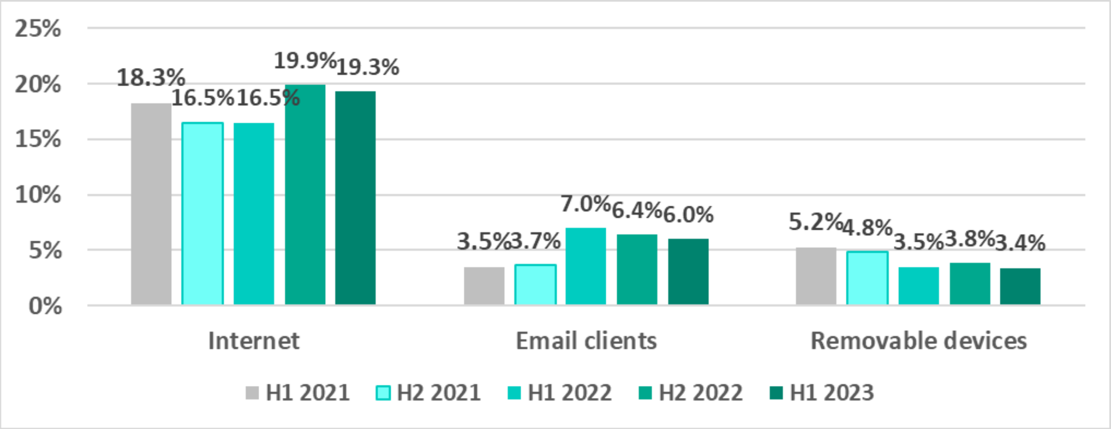
Main threat sources

The internet, email clients and removable devices remained the key sources of threats to computers in the operational technology infrastructure of organizations. Note that the sources of blocked threats cannot always be reliably determined.

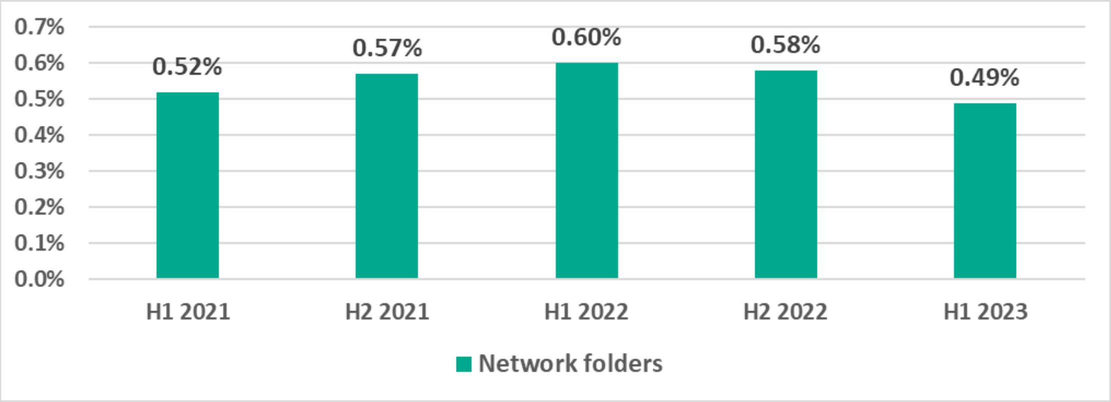
World

In the first half of 2023, the percentage of ICS computers on which malicious objects were blocked, dropped for virtually every main threat source.

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



The percentage of ICS computers on which network folder threats were blocked



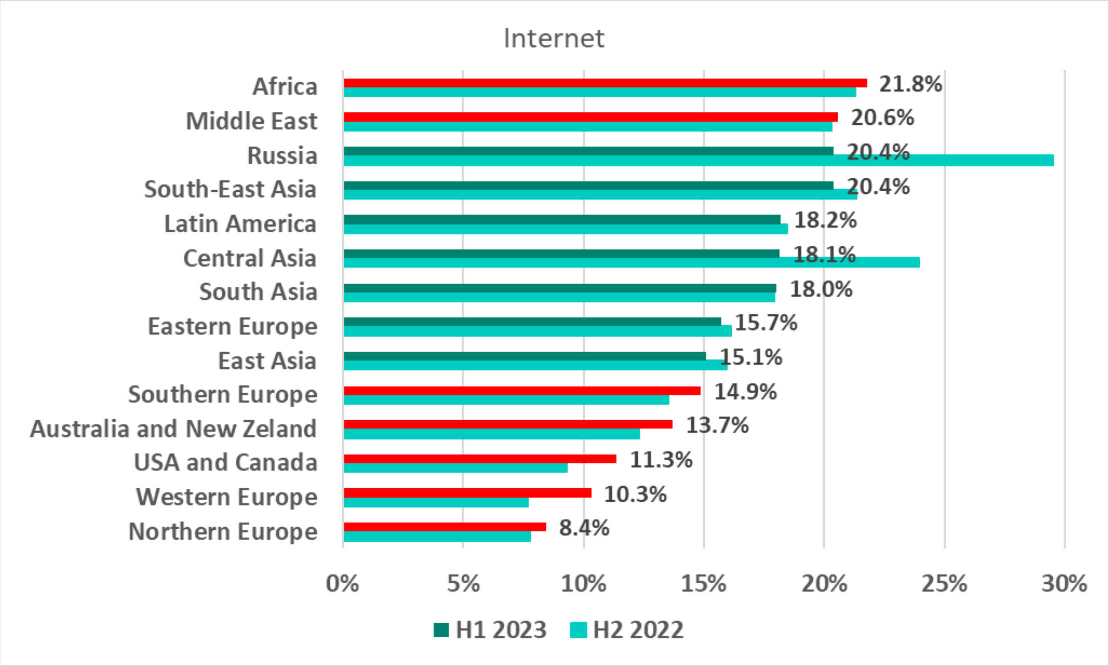
As is the case with the overall threat statistics, the percentage of ICS computers on which malicious objects from various sources were blocked varies by region and country.

Regions and countries

Internet

In the first half of 2023, Africa, the Middle East and Russia were the regions with the highest percentage of ICS computers on which internet threats were blocked.

Regions ranked by percentage of ICS computers on which threats from the internet were blocked, H1 2023

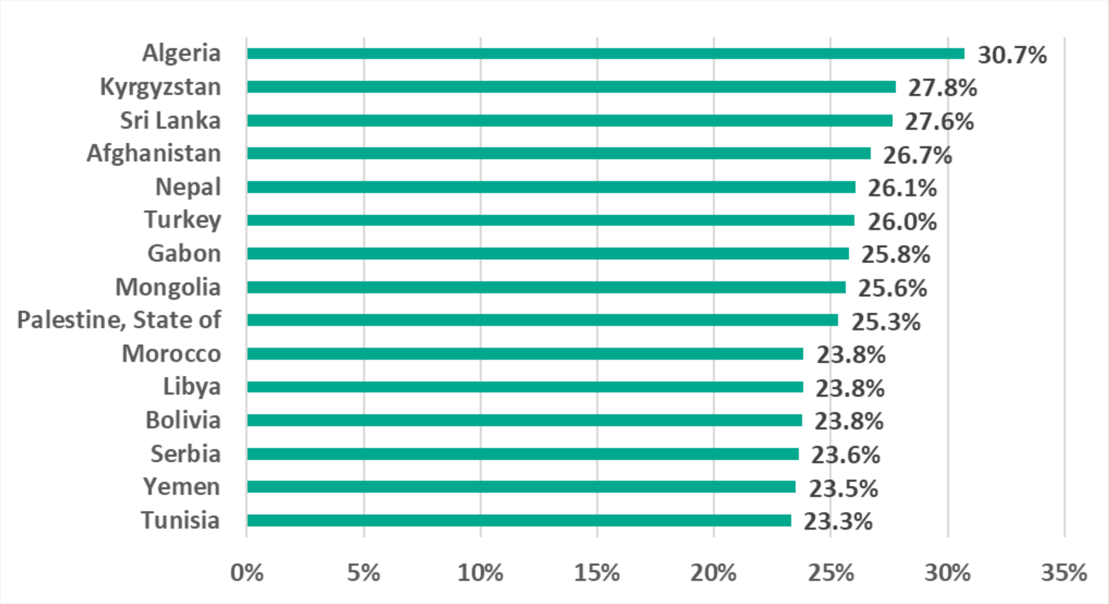


The largest increase in the percentage of ICS computers on which internet threats were blocked in the first half of 2023 was recorded in the regions that were historically the safest: Western Europe (by 2.6 pp), the United States and Canada (by 2 pp), and Australia and New Zealand (by 1.4 pp).

The Russia and Central Asia figures dropped noticeably. In the previous half-year, these regions saw a sharp increase in the percentage of ICS computers on which internet threats were blocked. The increase was due to mass infection of websites, including those run by industrial companies, that used an outdated version of a popular CMS.

One European country, Serbia, remained among the 15 countries and regions where that percentage was the highest.

Fifteen countries and territories with the highest percentage of ICS computers on which internet threats were blocked, H1 2023

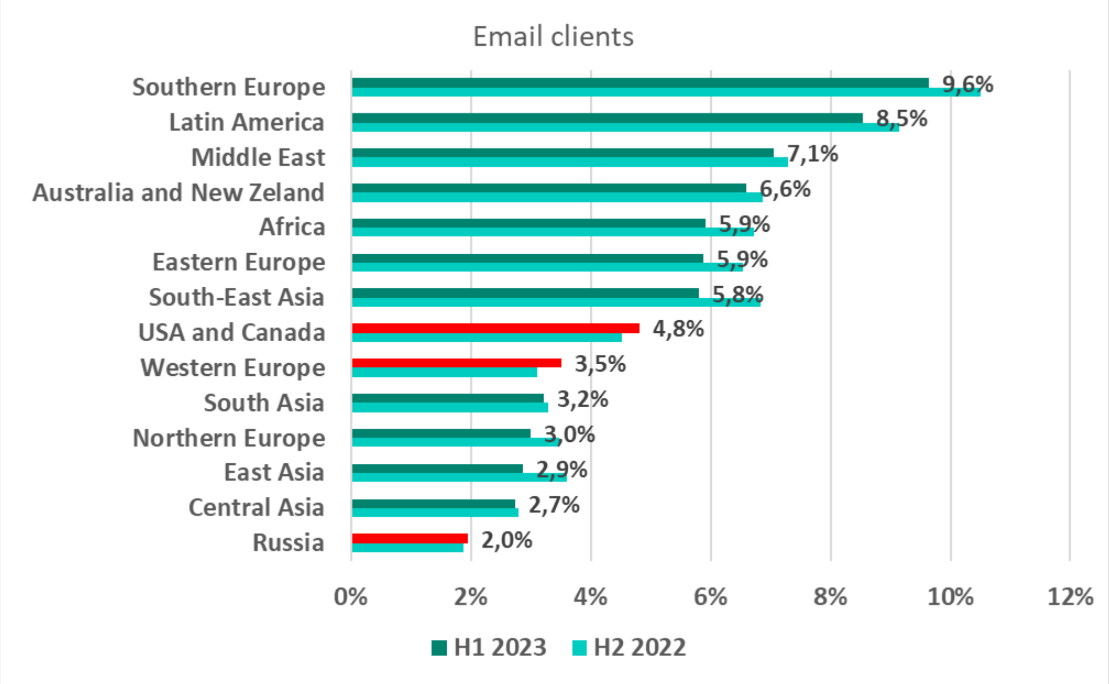


Email clients

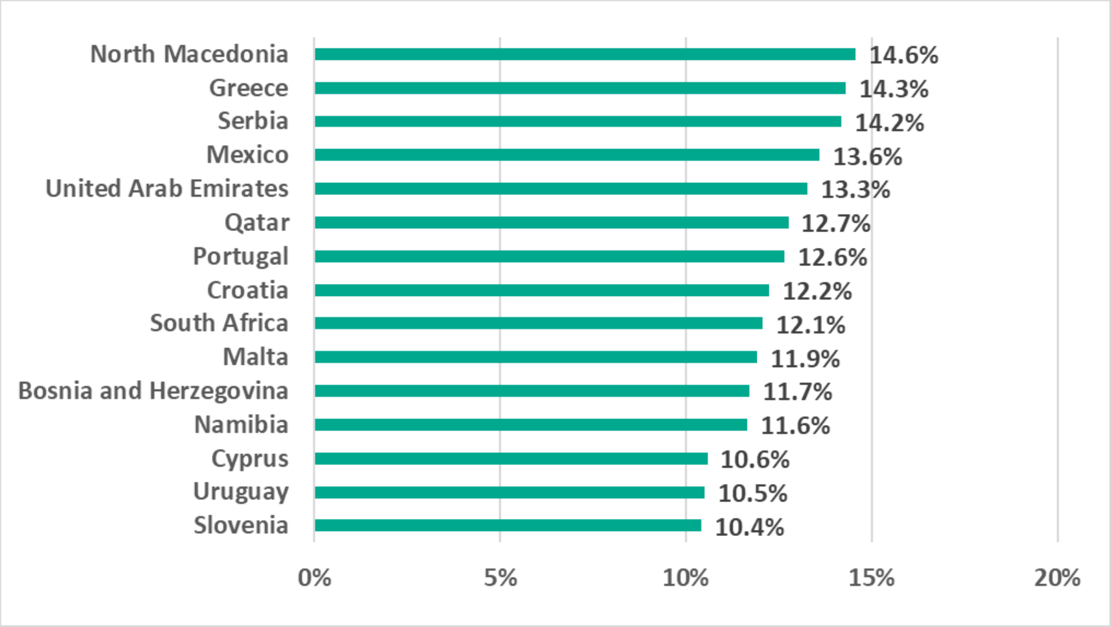
Since the first half of 2022, Southern Europe has remained the region with the highest percentage of ICS computers on which malicious email attachments and phishing links were blocked.

The percentage of ICS computers on which email threats were blocked grew in the United States and Canada (by 0.3 pp), Western Europe (by 0.4 pp) and Russia (by 0.1 pp).

Regions ranked by percentage of ICS computers on which malicious email attachments and phishing links were blocked, H1 2023



Southern and Eastern Europe dominated the list of 15 countries and territories with the highest percentage of ICS computers on which malicious email attachments and phishing links were blocked.



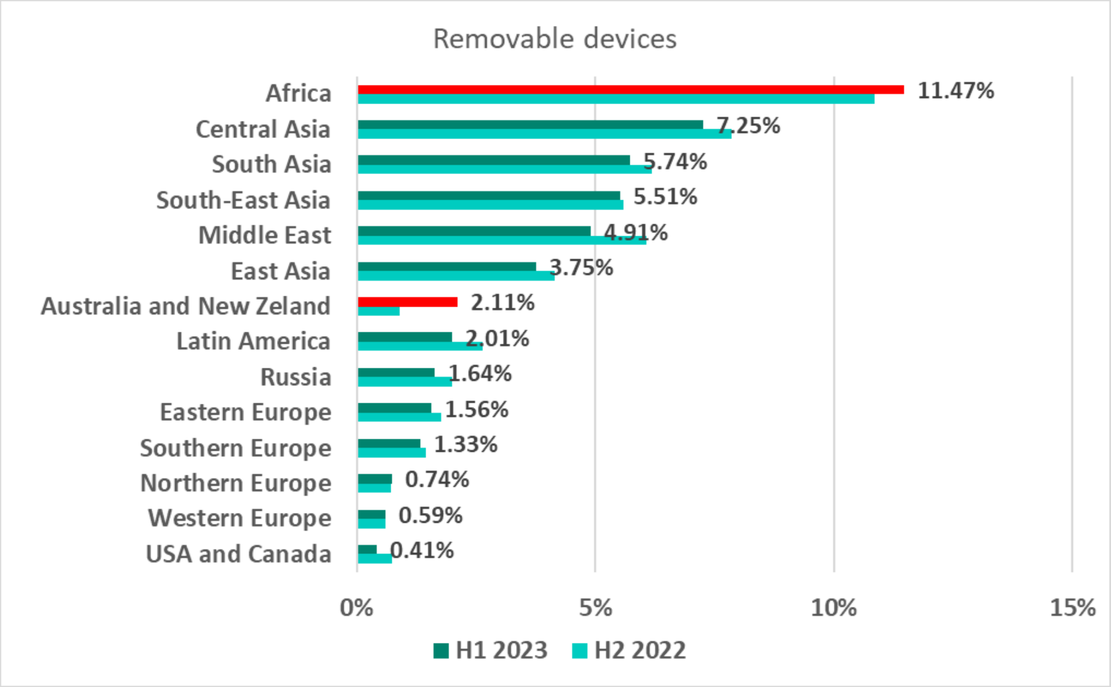
Fifteen countries and territories with the highest percentage of ICS computers on which malicious email attachments and phishing links were blocked, H1 2023

We recommend that information security professionals in these countries pay special attention to protecting employees from phishing email campaigns.

Removable devices

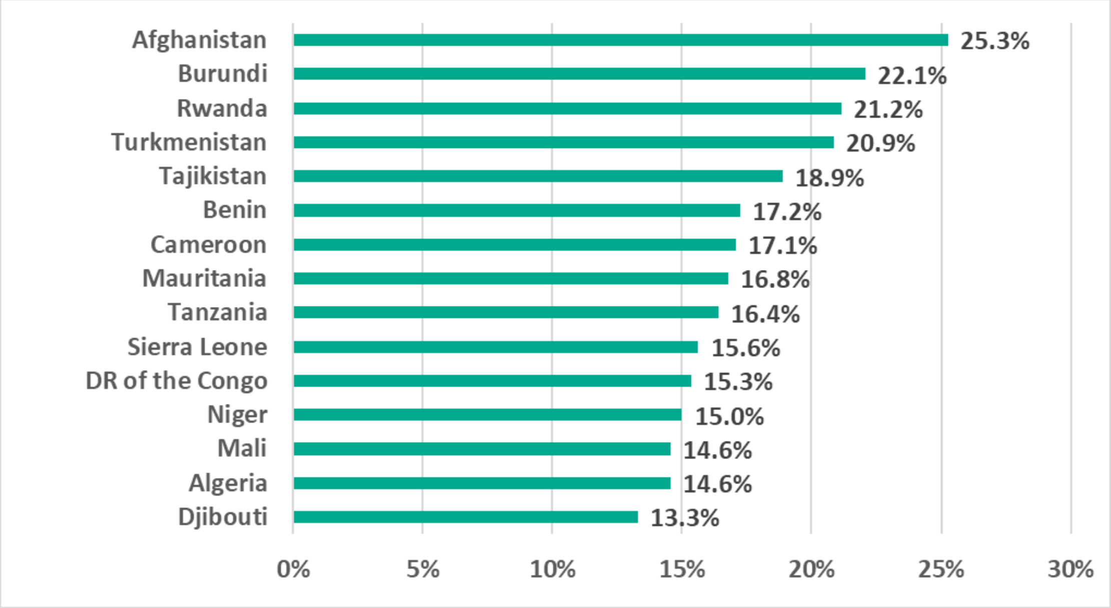
Africa and the Asian regions, historically the regions with the highest percentage of ICS computers on which malware is blocked when removable devices are connected, kept their positions. In the first half of 2023, the figure increased slightly in Africa (by 0.63 pp), and more than doubled in Australia and New Zealand (by 1.2 pp).

Regions ranked by percentage of ICS computers on which malware was blocked after removable devices were connected, H1 2023



Africa dominated the list of 15 countries and territories with the highest percentage of ICS computers on which malware was blocked when removable devices were connected.

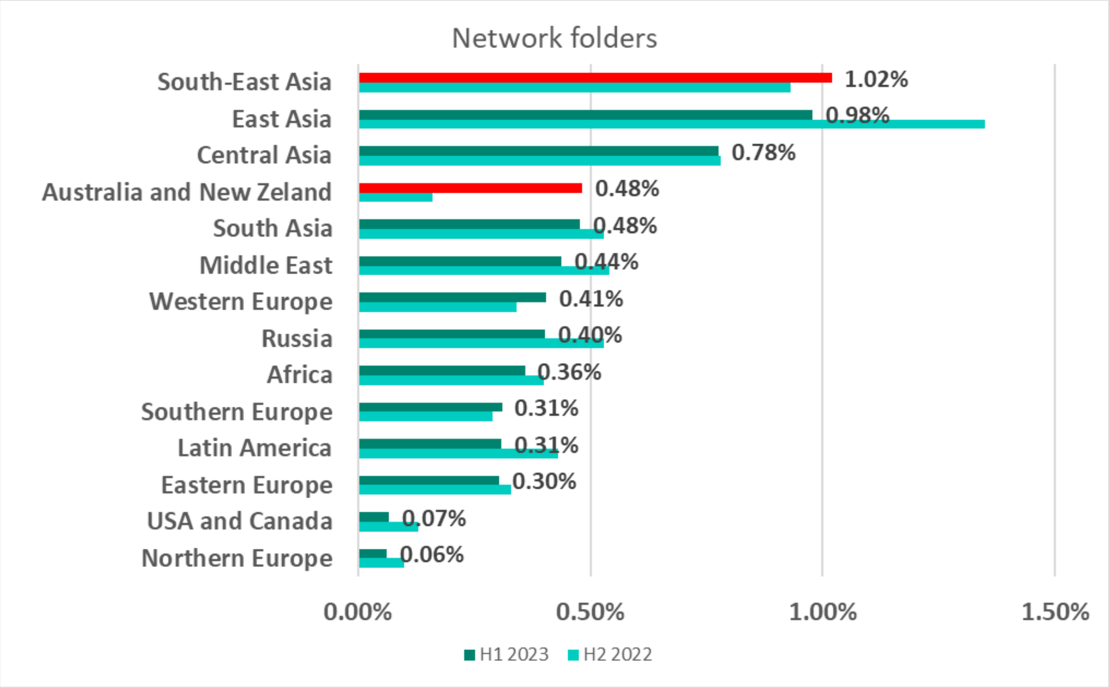
Fifteen countries and territories with the highest percentage of ICS computers on which malware was blocked when removable devices were connected, H1 2023



Network folders

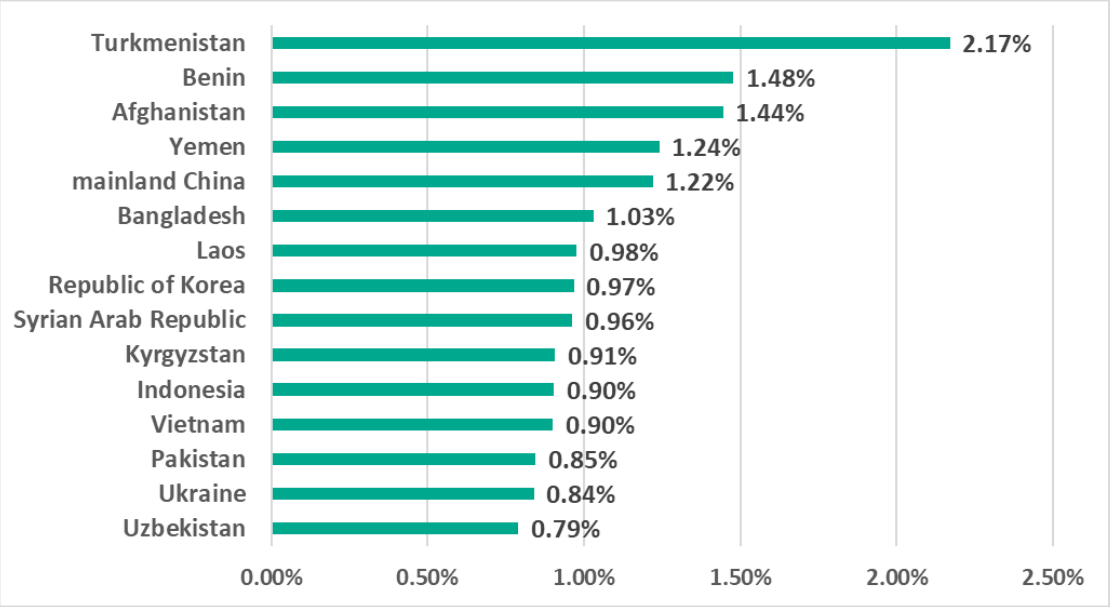
Network folders were a minor source of malicious objects. East, Southeast and Central Asia saw the highest percentage of ICS computers on which threats were blocked in network folders. The figure doubled over the half-year in Australia and New Zealand, pushing the region to fourth place on the list.

Regions ranked by percentage of ICS computers on which malicious objects in network folders were blocked, H1 2023



Turkmenistan had the highest percentage among countries and territories, as in H2 2022.

Fifteen countries and territories with the highest percentage of ICS computers on which malicious objects were blocked in network folders, H1 2023



Methodology used to prepare statistics

The report presents the findings of the analysis of statistical data obtained using the Kaspersky Security Network (KSN) 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 information transferred by the user includes only those types and categories of data that are described in the relevant KSN Agreement. This data is not only significantly helpful in analyzing the threat landscape, but it is also necessary for identifying new threats, including targeted attacks and advanced persistent threats (APT)[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 systems

For the purposes of this report, “attacked computers” are those on which Kaspersky security solutions blocked one or more threats during the period in review (in the diagrams above, this can be a month, half-year or 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 which have any restrictions in place with respect to transferring data outside the organization’s perimeter should consider using the Kaspersky Private Security Network service.

Kaspersky 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