Kaspersky ICS CERT

kaspersky

Threat landscape for industrial automation systems

Q1 2025

15.05.2025

Version 1.0

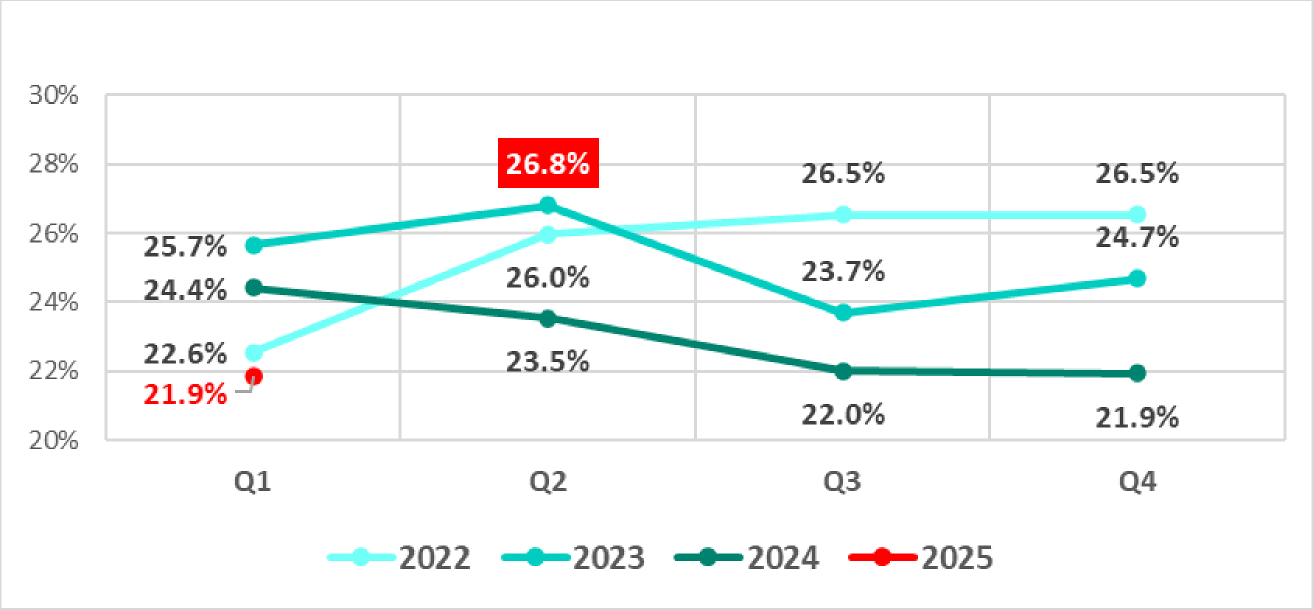
Q1 in numbers

Parameter	Q4 2024	Q1 2025	Quarterly changes
Global percentage of attacked ICS computers	21.9%	21.9%	0 pp
Percentage of ICS computers on which malicious objects from different categories were blocked			
Malicious scripts and phishing pages (JS and HTML)	7.11%	7.16%	▲0.05 pp
Denylisted internet resources	5.52%	5.12%	▼0.40 pp
Spy Trojans, backdoors and keyloggers	4.30%	4.20%	▼0.10 pp
Malicious documents (MSOffice + PDF)	1.71%	1.85%	▲0.14 pp
Viruses	1.61%	1.53%	▼0.08 pp
Worms	1.37%	1.31%	▼0.06 pp
Miners in the form of executable files for Windows	0.70%	0.78%	▲0.08 pp
Web miners running in browsers	0.39%	0.53%	▲0.14 pp
Malware for AutoCAD	0.38%	0.34%	▼0.04 pp
Ransomware	0.21%	0.16%	▼0.05 pp
Main threat sources			
Internet	9.98%	10.11%	▲0.13 pp
Email clients	2.72%	2.81%	▲0.09 pp
Removable media	0.64%	0.52%	▼0.12 pp
Network folders	0.08%	0.07%	▼0.01 pp

Trends

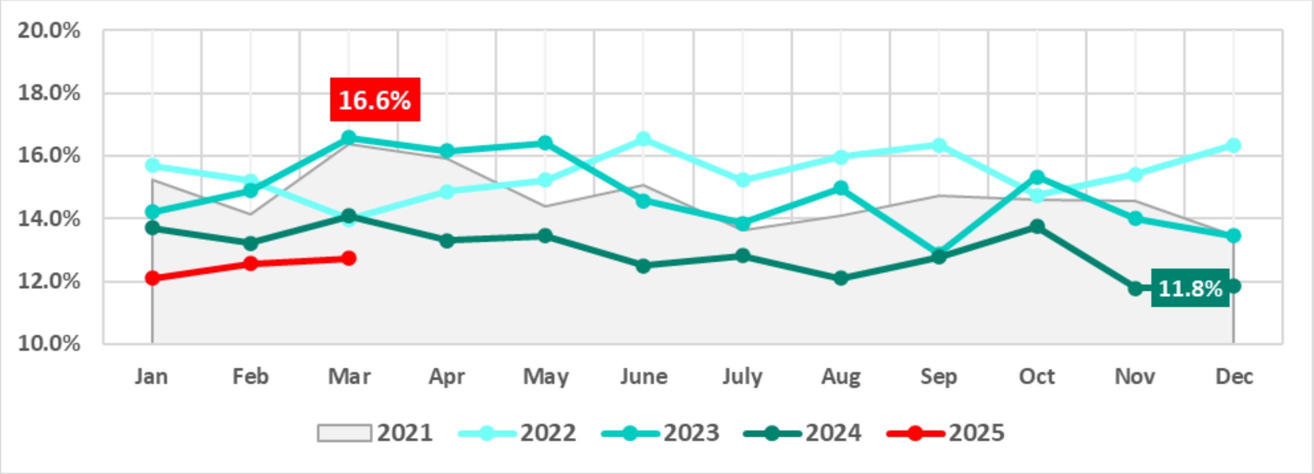
Relative stability from quarter to quarter. The percentage of ICS computers on which malicious objects were blocked remained unchanged from Q4 2024 at 21.9%. Over the last three quarters, the value has ranged from 22.0% to 21.9%.

The quarterly figures are decreasing from year to year. Since Q2 2023, the percentage of ICS computers on which malicious objects were blocked has been lower than the indicator of the same quarter of the previous year. Compared to Q1 2024, the figure decreased by 2.5 pp.



Percentage of ICS computers on which malicious objects were blocked, Q1 2022–Q1 2025

In January–March 2025, the figures were the lowest compared to the same months in the previous four years.

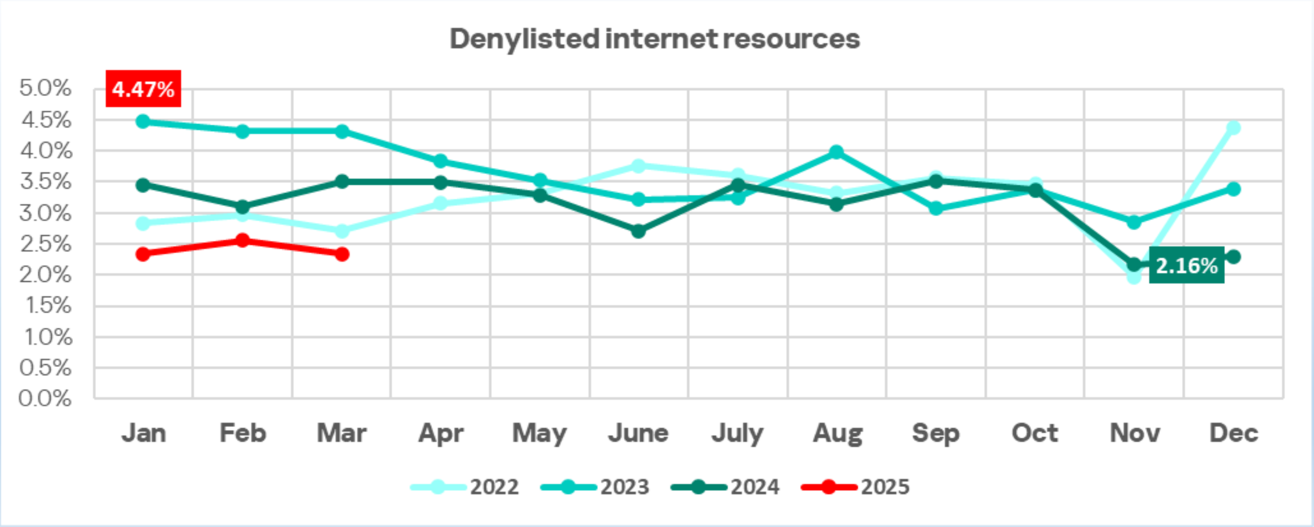


Percentage of ICS computers on which malicious objects were blocked, Jan 2021–Mar 2025

The biometrics sector continues to lead the selected industries / OT infrastructure types. This is the only OT infrastructure type where the percentage of ICS computers on which malicious objects were blocked increased during the quarter.

Regions still vary. In Q1 2025, the percentage ranged from 10.7% in Northern Europe to 29.6% in Africa. In eight out of 13 regions, the figures ranged from 19.0% to 25.0%.

The percentage of ICS computers on which denylisted internet resources were blocked continues to decrease. The percentage reached its lowest level since the beginning of 2022. In the first three months of 2025, the corresponding figures were lower than in January–March of the previous three years.



The percentage of ICS computers on which denylisted internet resources were blocked, Jan 2022–Mar 2025

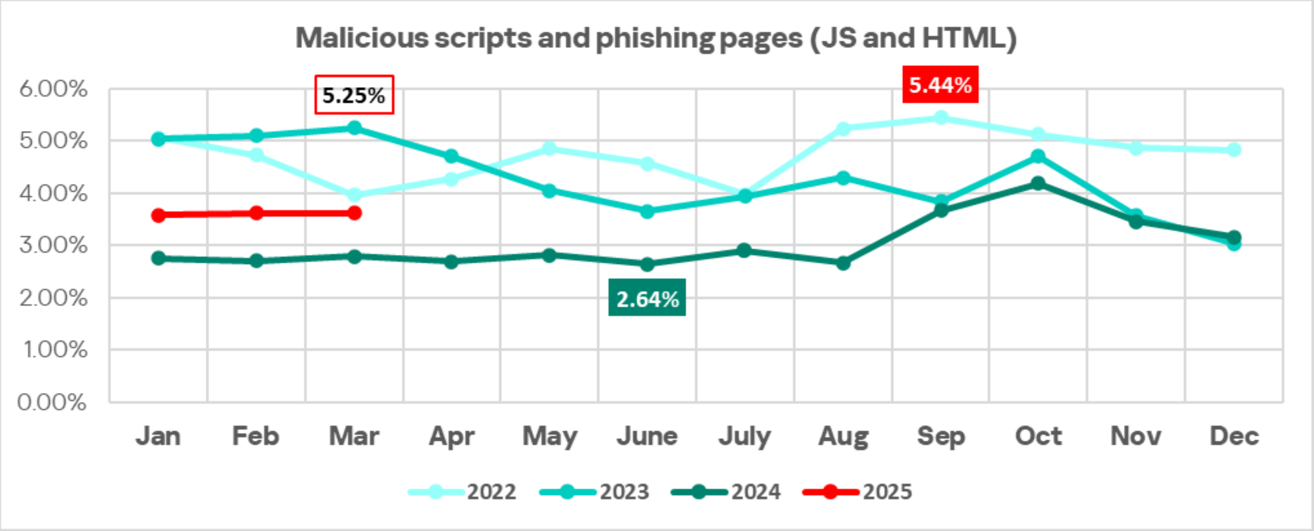
Changes in the percentage of ICS computers on which the initial infection malware was blocked lead to changes in the percentage of next-stage malware.

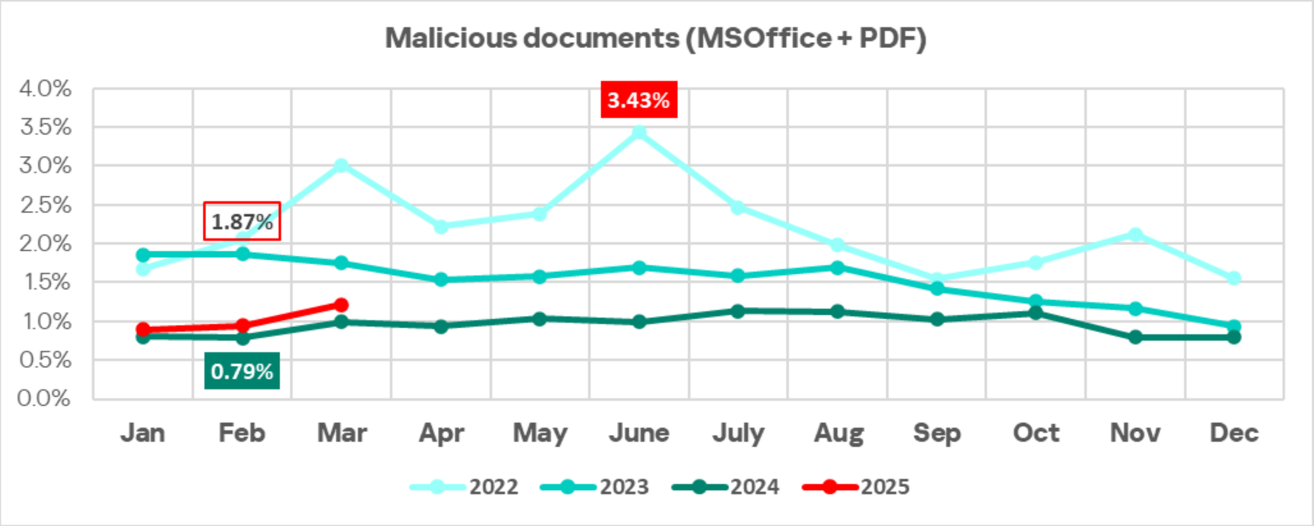
In Q1 2025, the percentage of ICS computers on which various types of malware spread via the internet and email were blocked increased for the first time since the beginning of 2023.

The internet is the primary source of threats to ICS computers. The main categories of threats from the internet are denylisted internet resources, malicious scripts and phishing pages.

The main categories of threats spreading via email are malicious documents, spyware, malicious scripts and phishing pages.

The percentage of ICS computers on which malicious scripts and phishing pages as well as malicious documents were blocked increased in Q1 2025. In January–March the monthly values of these two categories of threats were higher than for the same months of 2024.

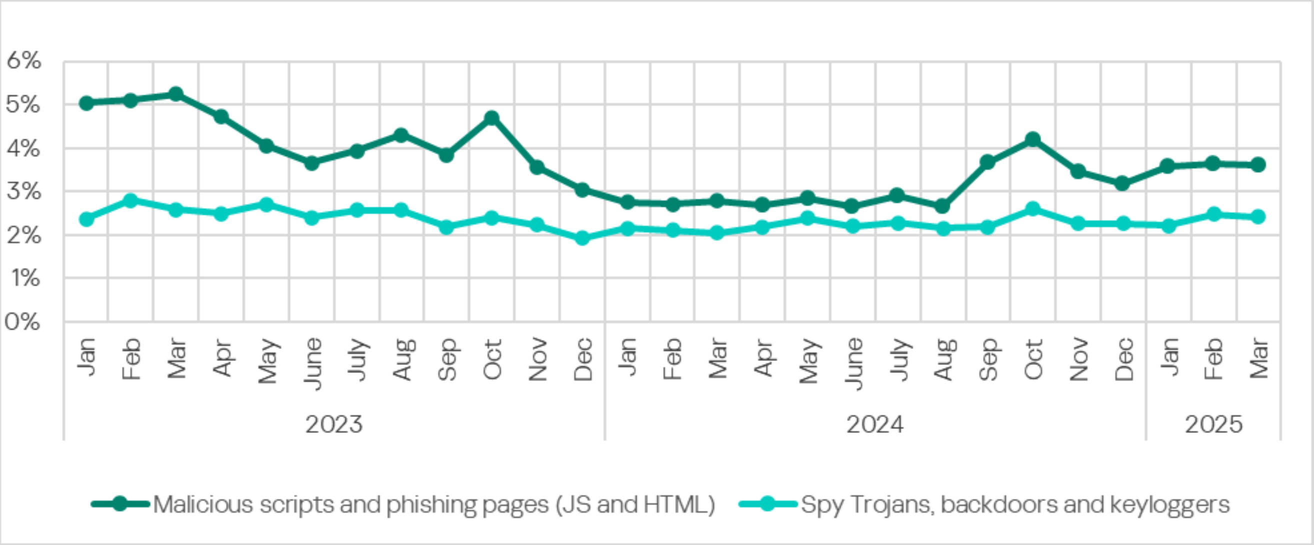




Percentage of ICS computers on which malicious objects were blocked, Jan 2022–Mar 2025

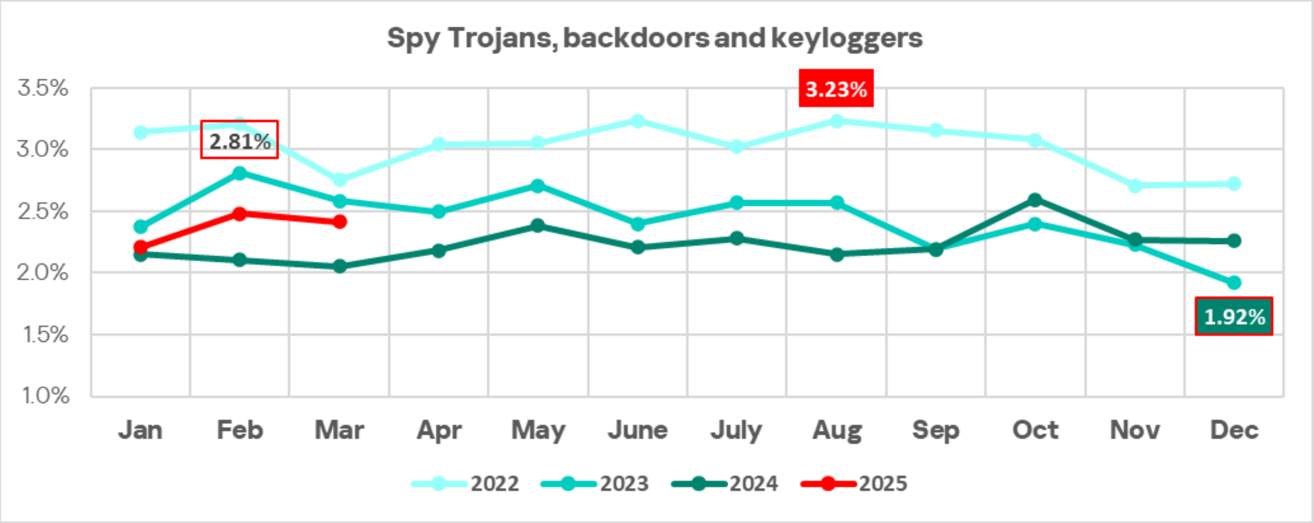
The leading category of malware used for initial infection of ICS computers (see below) is malicious scripts and phishing pages.

Most malicious scripts and phishing pages act as droppers or loaders of next-stage malware (spyware, crypto miners and ransomware). The strong correlation (r=0.705, p<0.001) between the values for malicious scripts and phishing pages and spyware is clearly visible in the graph below.



Percentage of ICS computers on which malicious objects were blocked, Jan 2023–Mar 2025

The percentage of ICS computers on which spyware as well as malicious scripts and phishing pages were blocked was higher in the first three months of 2025 than in the same months of 2024.

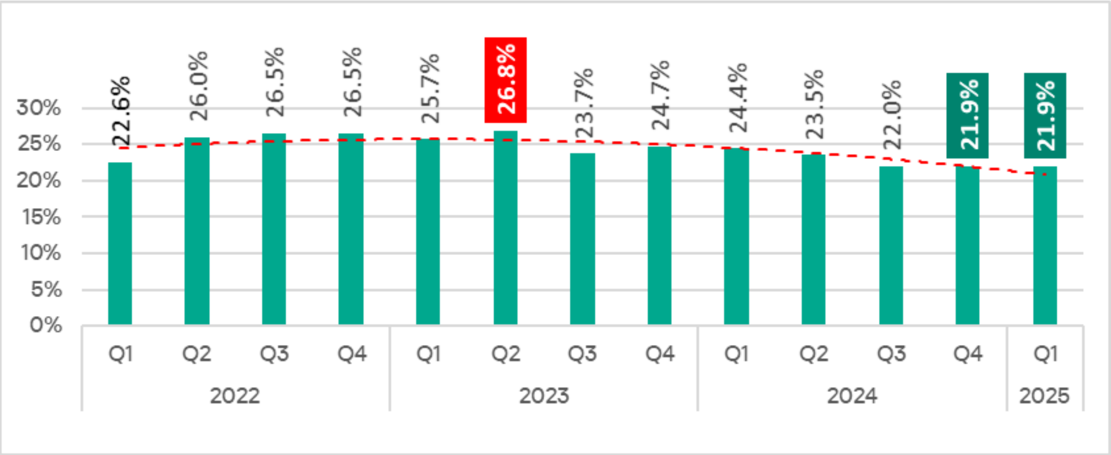


Percentage of ICS computers on which spyware was blocked, Jan 2022–Mar 2025

The percentage of ICS computers on which miners (web miners and miners in the form of executable files for Windows) were blocked in Q1 2025 also increased.

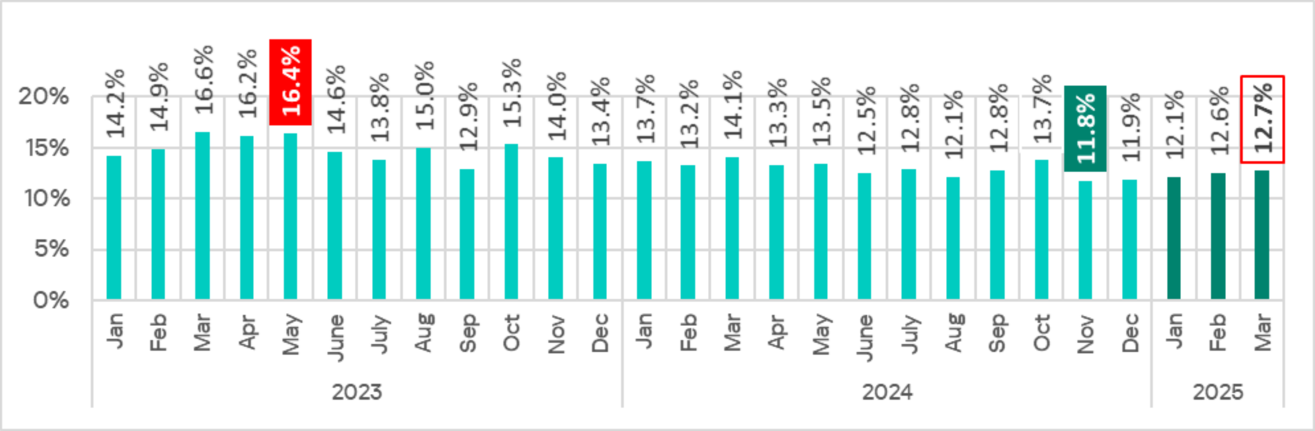
Statistics across all threats

In Q1 2025, the percentage of ICS computers on which malicious objects were blocked was unchanged from the previous quarter at 21.9%.



Percentage of ICS computers on which malicious objects were blocked, Q1 2022–Q1 2025

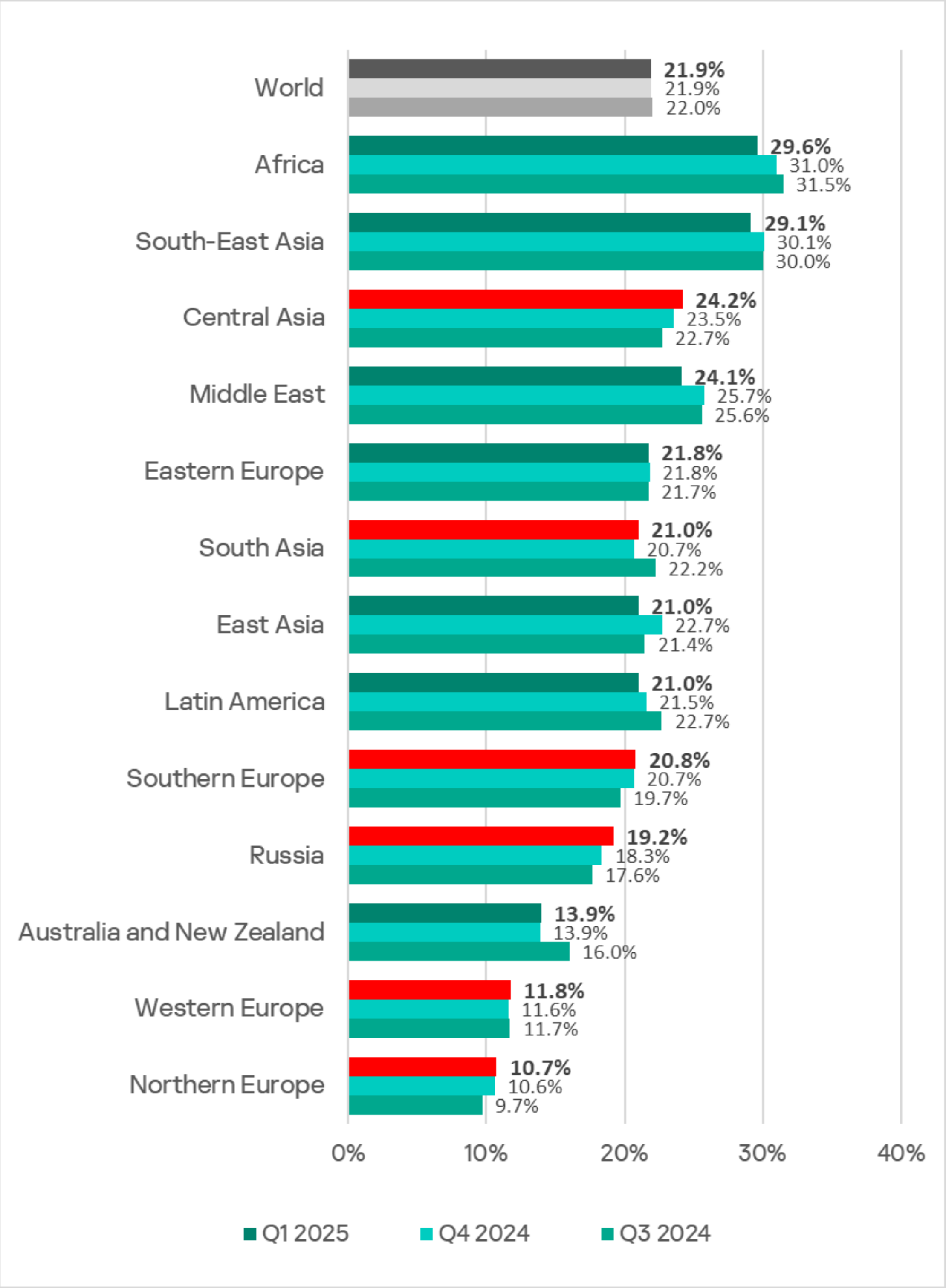
Compared to Q1 2024, the percentage of ICS computers on which malicious objects were blocked decreased by 2.5 pp. The rate increased from January to March of 2025 when it reached its highest value of the quarter.



Percentage of ICS computers on which malicious objects were blocked, Jan 2023–Mar 2025

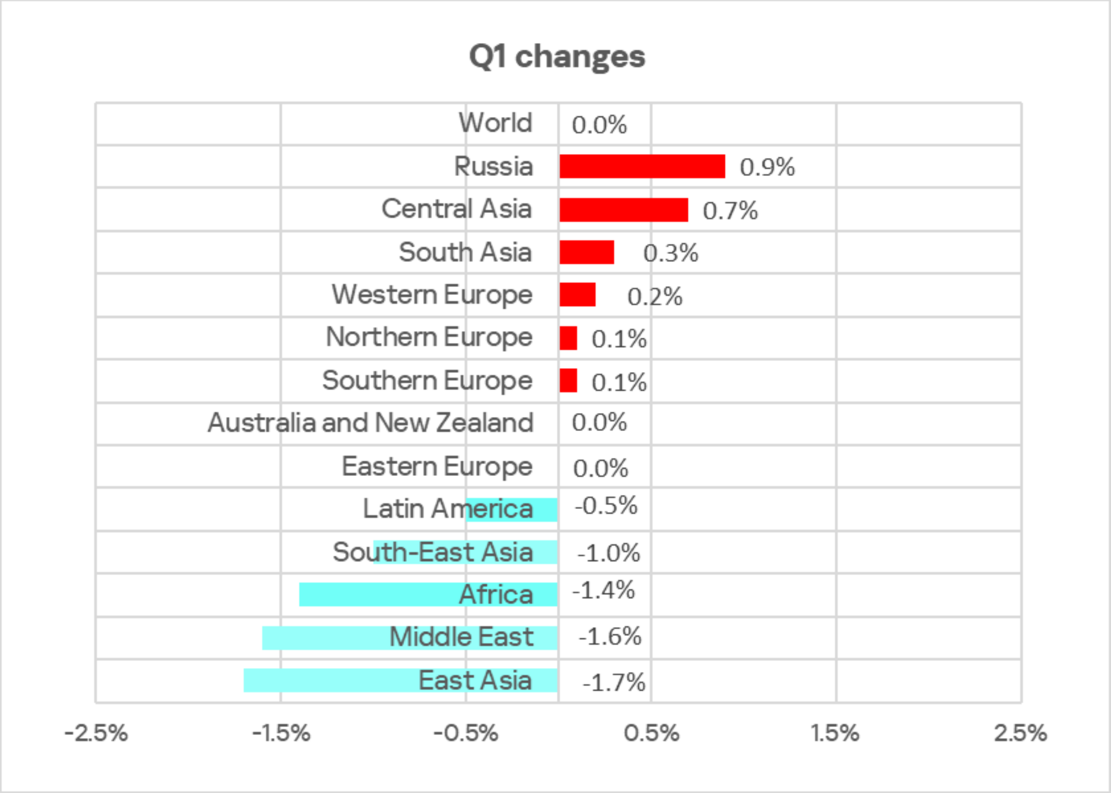
Regionally, the percentage of ICS computers on which malicious objects were blocked ranged from 10.7% in Northern Europe to 29.6% in Africa.

Regions ranked by percentage of ICS computers on which malicious objects were blocked, Q1 2025



In six of the 13 regions surveyed in this report, the figures increased from the previous quarter, with the largest change in Russia.

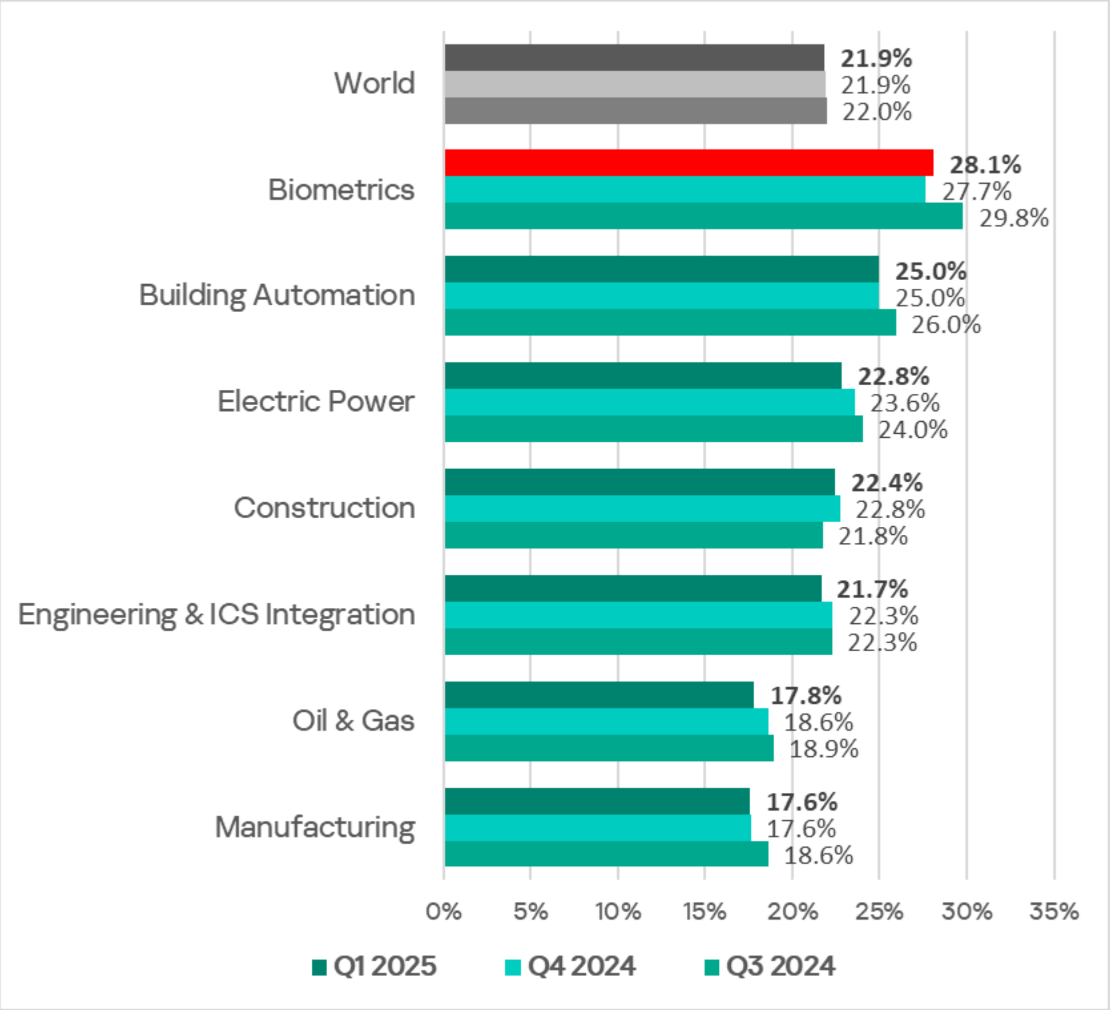
Changes in percentage of ICS computers on which malicious objects were blocked, Q1 2025



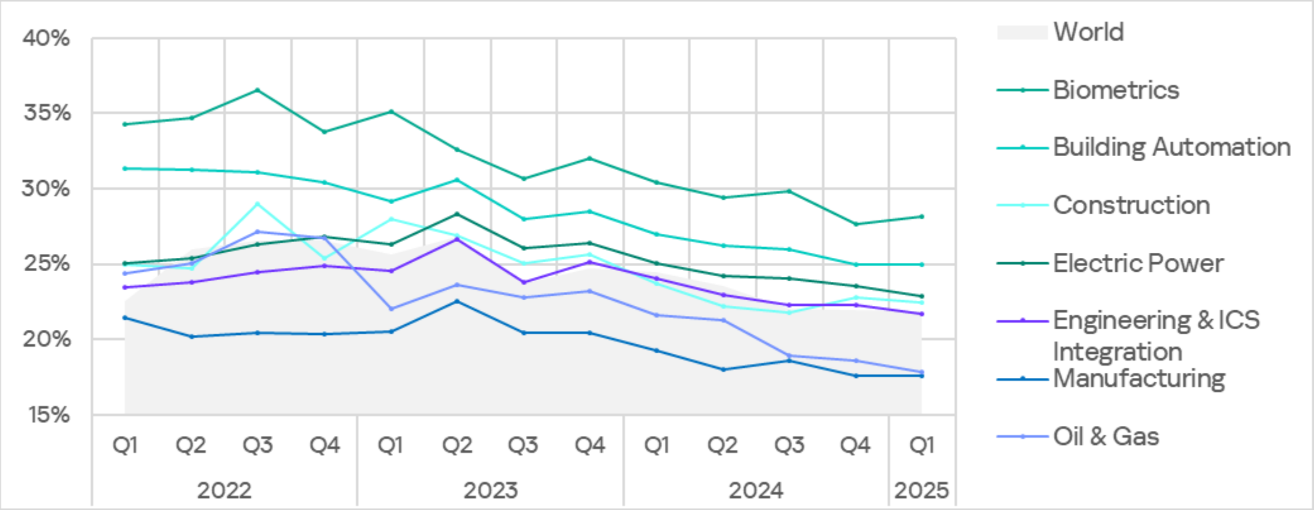
Selected industries

The biometrics sector led the ranking of the industries and OT infrastructures surveyed in this report in terms of the percentage of ICS computers on which malicious objects were blocked.

Ranking of industries and OT infrastructures by percentage of ICS compute rs on which malicious objects were blocked, Q1 2025



The biometrics sector was also the only OT infrastructure type where the percentage of ICS computers on which malicious objects were blocked increased slightly. Despite this, the long-term trend is clearly downward.



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

Diversity of detected malicious objects

Malicious objects of various categories, which Kaspersky products block on ICS computers, can be divided into three groups according to their distribution method and purpose.

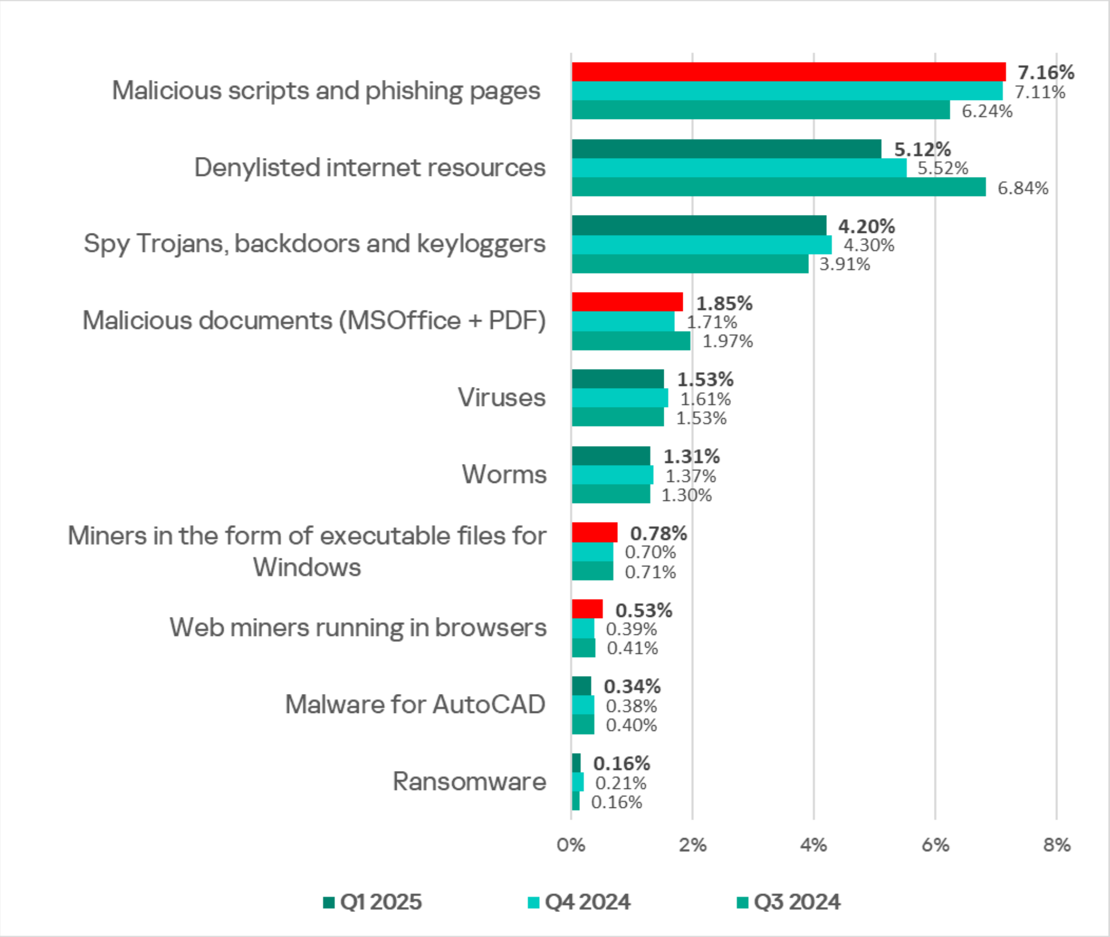
1. Malicious objects used for initial infection.
   This category includes predominantly denylisted internet resources, malicious scripts and phishing pages, and malicious documents.
2. Next-stage malware.
   Spyware, ransomware, miners in the form of executable files for Windows, and web miners are the most common types.
3. Self-propagating malware.
   This category includes worms and viruses.

Malware for AutoCAD does not belong to a specific group, as it can spread in a variety of ways.

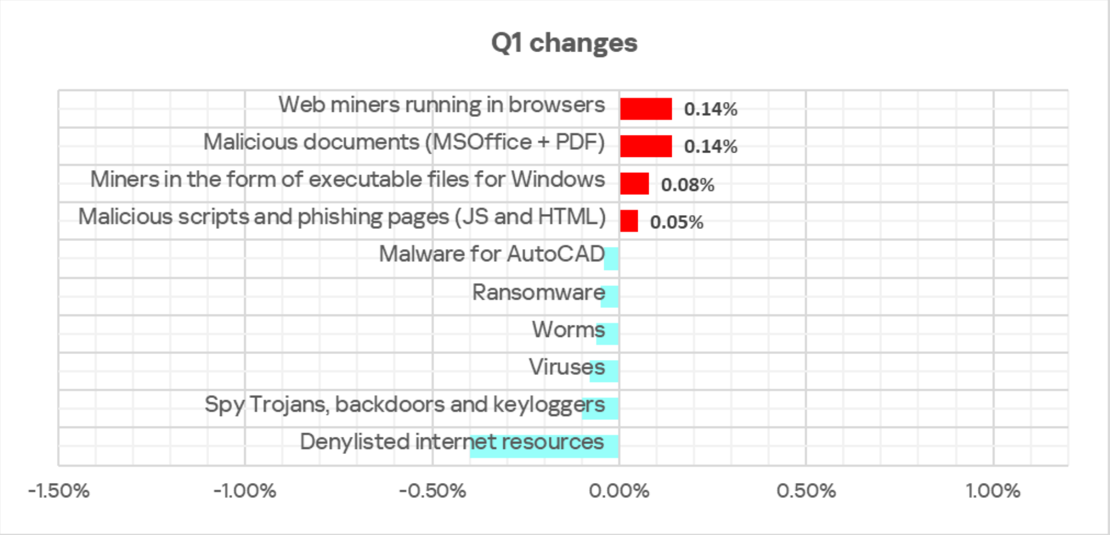
In Q1 2025, Kaspersky protection solutions blocked malware from 11,679 different malware families of various categories on industrial automation systems.

Malicious objects categorized as initial infection threats typically rank highest among threat categories in terms of the percentage of ICS computers on which threats were blocked. This is reflected in our statistics: globally and in almost all regions, malicious scripts and phishing pages, as well as denylisted internet resources are the top threat categories.

Percentage of ICS computer s on which the activity of malicious objects from various categories was blocked



Changes in percentage of ICS computers on which malicious objects from different categories were blocked, Q1 2025



The largest proportional increase in Q1 2025 was in the percentage of ICS computers on which web miners (1.4 times more than in the previous quarter) and malicious documents (1.1 times more) were blocked.

Threat categories

Typical attacks blocked within an OT network are a multi-stage process, where each subsequent step of the attackers is aimed at increasing privileges and gaining access to other systems by exploiting the security problems of industrial enterprises, including technological infrastructures.

It is worth noting that during the attack, intruders often repeat the same steps (TTP), especially when they use malicious scripts and established communication channels with the management and control infrastructure (C2) to move laterally within the network and advance the attack.

Malicious objects used for initial infection

Denylisted internet resources

The list of denied internet resources is used to prevent initial infection attempts. In particular, it helps to block the following on ICS computers:

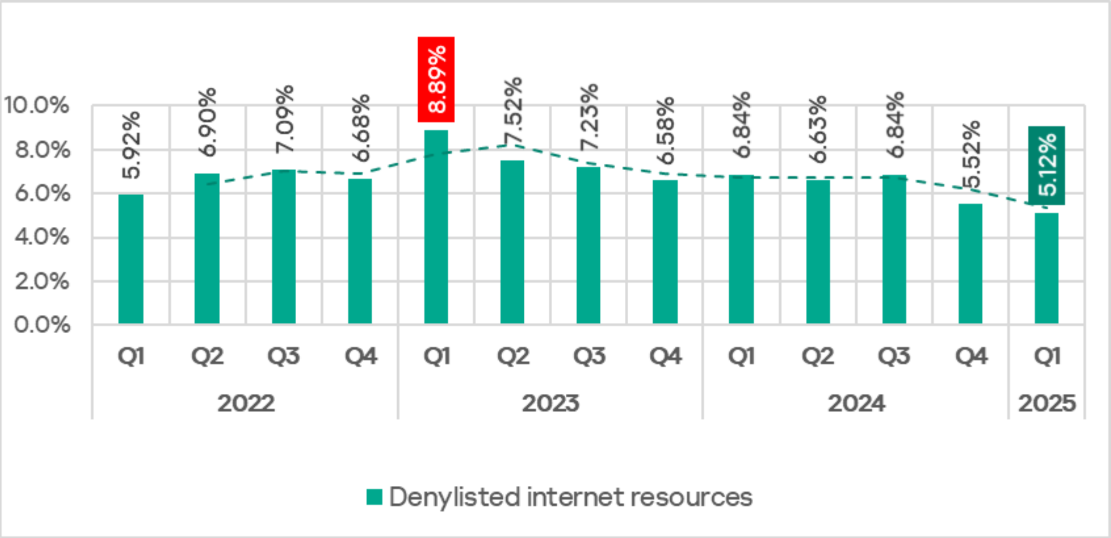
- Known malicious URLs and IP addresses used by threat actors to host payloads and configurations.
- Suspicious (unreliable) web resources with entertainment and gaming content, often used to deliver unwanted software, crypto miners and malicious scripts.
- CDN nodes used by attackers to distribute malicious scripts on popular sites.
- File and data exchange services, including repositories, often used by attackers to host next-stage payloads and configurations.

Denylisted internet resources are mainly used by threat actors to spread malware as well as phishing attacks and command and control infrastructure (C2). A significant portion of these resources is used to distribute malicious scripts and phishing pages (HTML).

High parameter values usually indicate weak control over the implementation of information security policies (ICS computers have access to the internet in one way or another), phishing protection weaknesses (many malicious links are delivered via phishing messages) and deficiencies in information security culture (employees visit insecure internet resources and follow malicious links from suspicious email and social media messages).

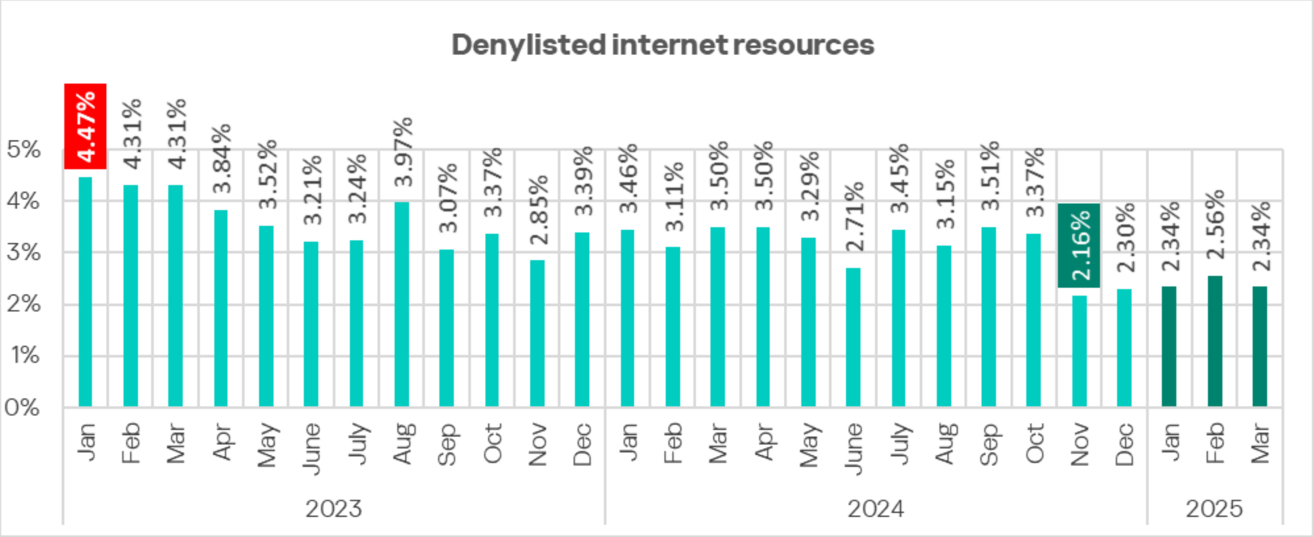
In Q1 2025, the percentage of ICS computers on which denylisted internet resources were blocked decreased to its lowest value since the beginning of 2022.

Percentage of ICS computers on which denylisted internet resources were blocked, Q1 2022–Q1 2025



During the quarter, the monthly figures were lower than the January–March figures for the previous three years.

The chart below shows the monthly percentage rates for the period under review.



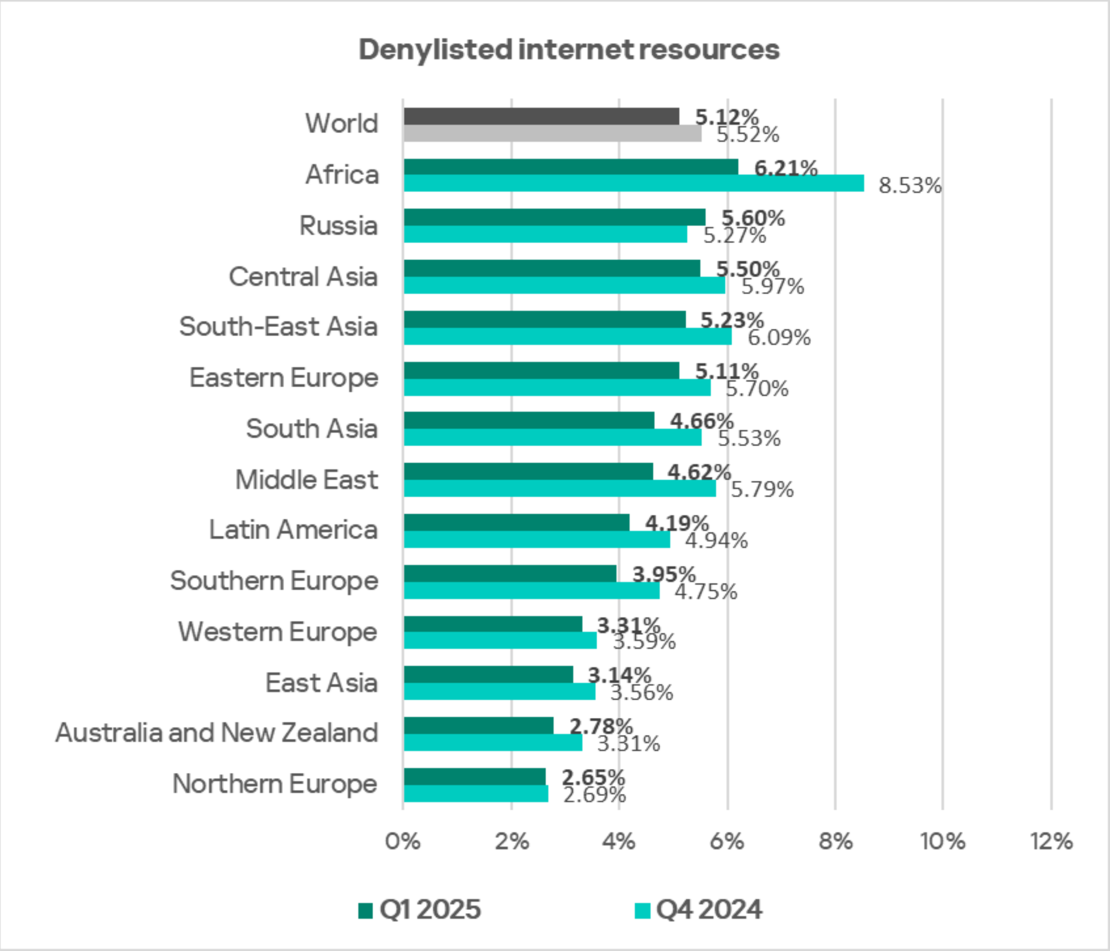
Percentage of ICS computers on which denylisted internet resources were blocked, Jan 2023–Mar 2025

The decline in the percentage of denylisted internet resources since November 2024 was likely influenced not only by proactive threat mitigation at various levels, but also by techniques used by attackers to circumvent the blocking of the resource's reputation – redistributing the protection burden to other detection technologies.

A detected malicious web resource may not always be added to a denylist because attackers are increasingly using legitimate internet resources and services such as content delivery network (CDN) platforms, messengers, and cloud storage. These services allow malicious code to be distributed through unique links to unique content, making it difficult to use reputation blocking tactics. We strongly recommend that industrial organizations implement policy-based blocking of such services, at least for OT networks where the need for such services is extremely rare for objective reasons.

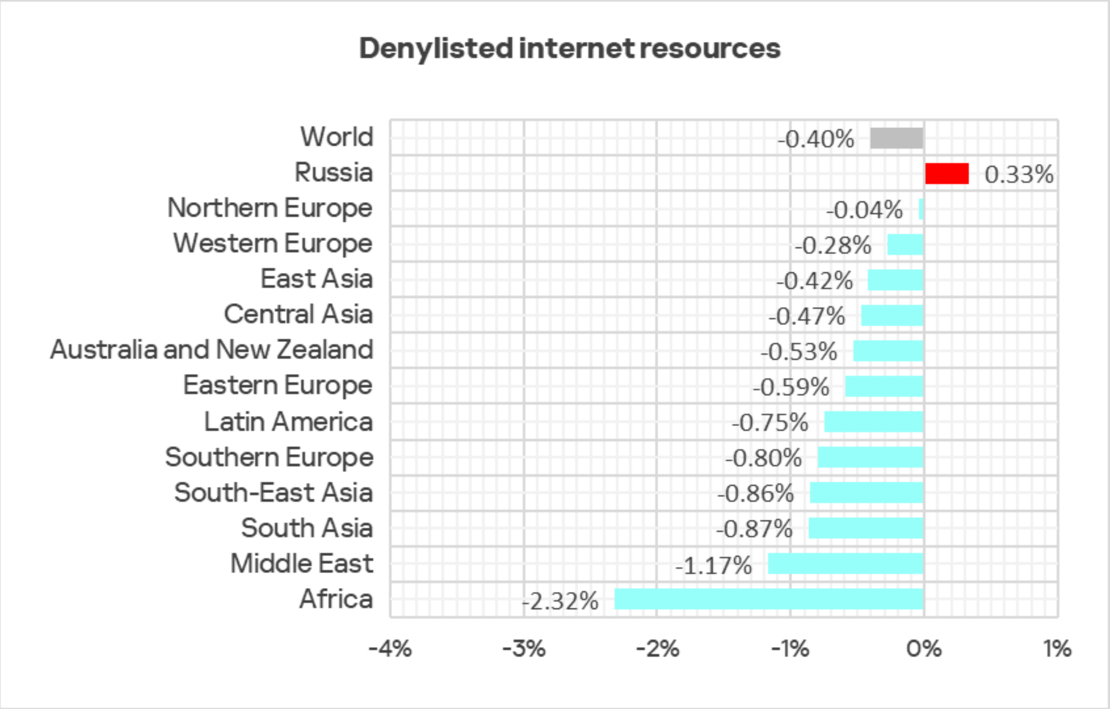
In Q1 2025, Africa, Russia, and Central Asia were the top three regions by the percentage of ICS computers on which denylisted internet resources were blocked.

Regions ranked by percentage of ICS computers on which denylisted internet resources were blocked, Q1 2025



The percentage decreased in all regions except Russia.

Changes in percentage of ICS computers on which denylisted internet resources were blocked, Q1 2025

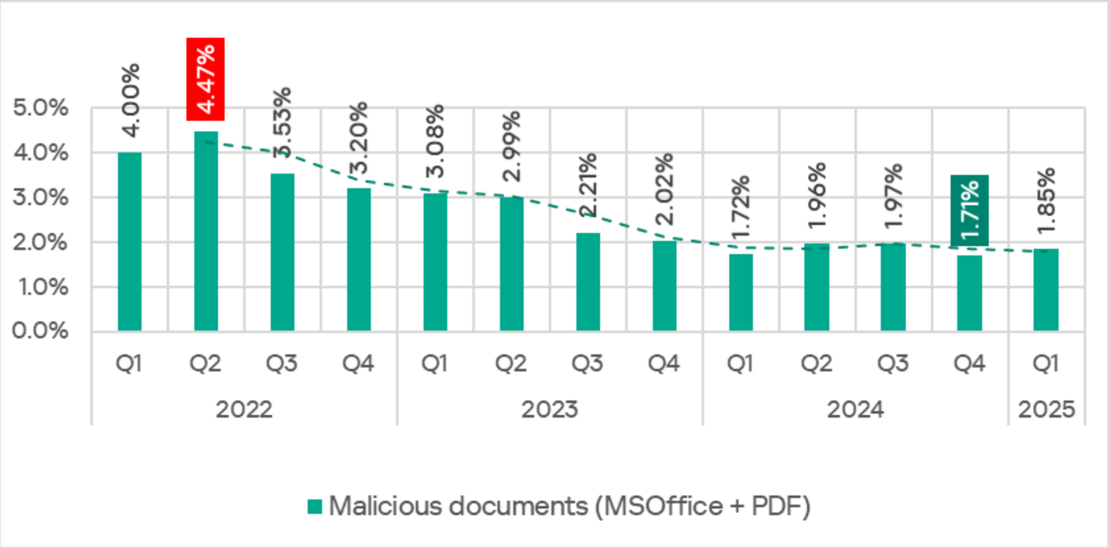


Malicious documents (MSOffice + PDF)

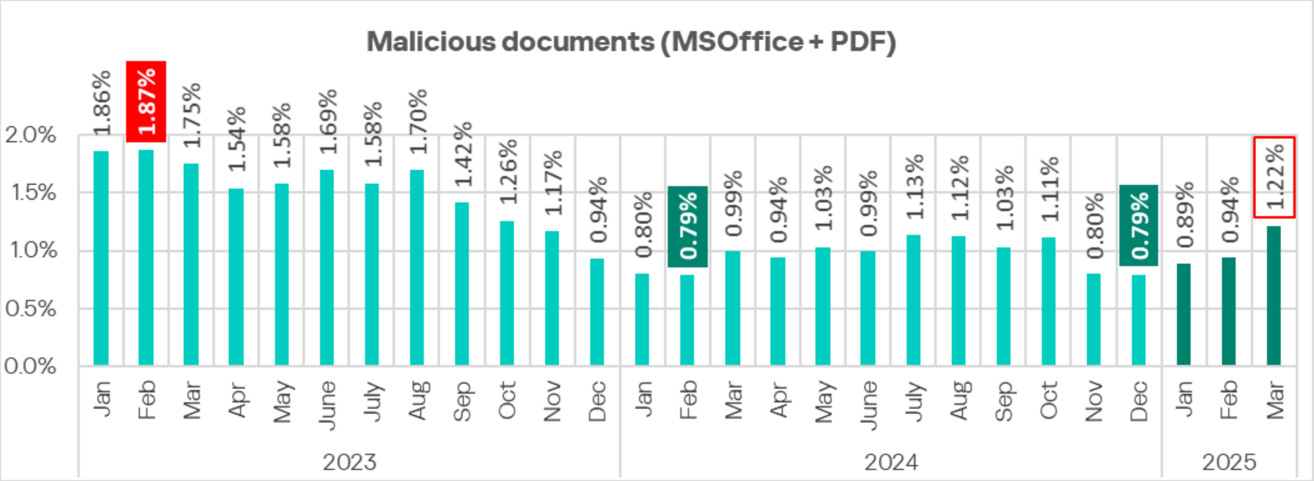
Attackers mainly send malicious documents attached to phishing messages and use them in attacks aimed at initial infection of computers. Malicious documents typically contain exploits, malicious macros, and malware links.

In the first quarter of 2025, the percentage of ICS computers on which malicious documents were blocked increased.

Percentage of ICS compute rs on which malicious documents were blocked, Q1 2022– Q1 2025



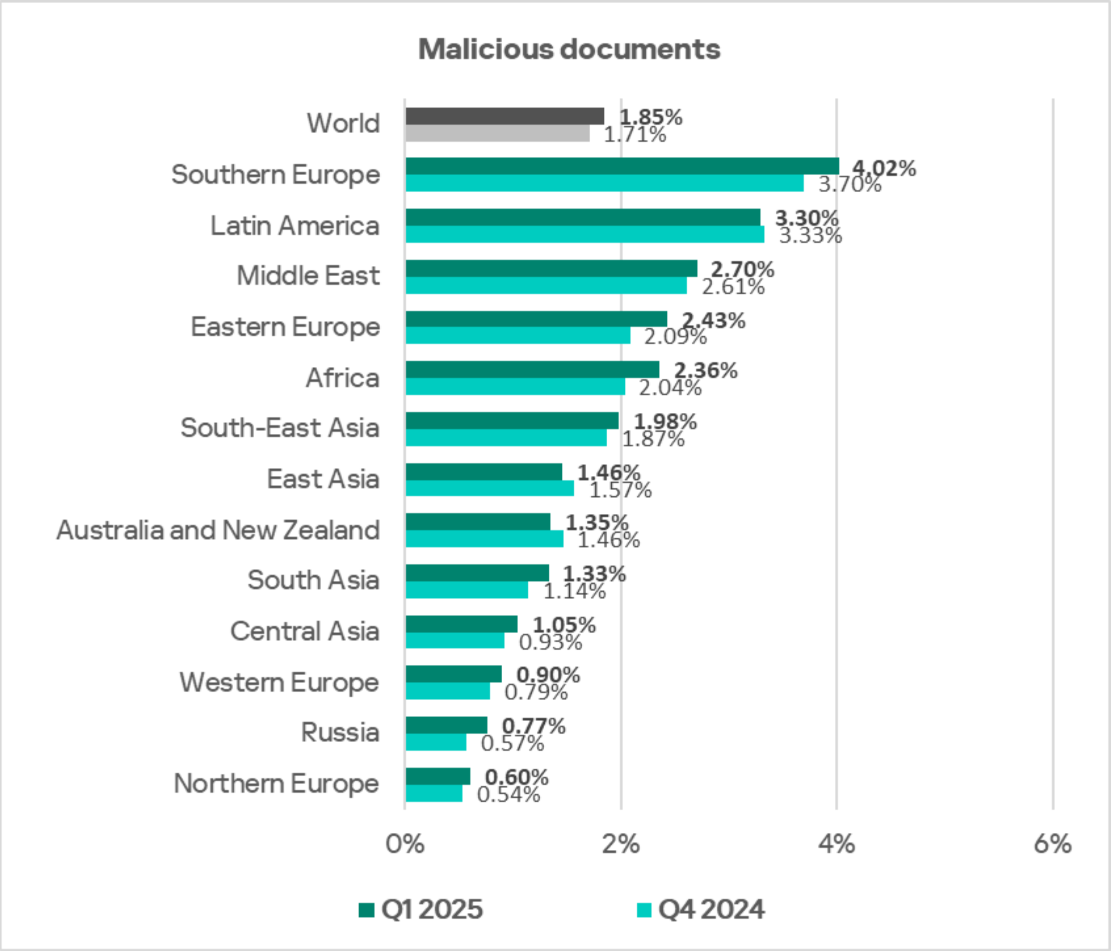
At the end of 2024, the figures were the lowest in two years, both for the quarter and for the month (with the exception of February 2024). In March 2025, the percentage of ICS computers on which malicious documents were blocked was the highest since November 2023.



Percentage of ICS computers on which malicious documents were blocked, Jan 2023–Mar 2025

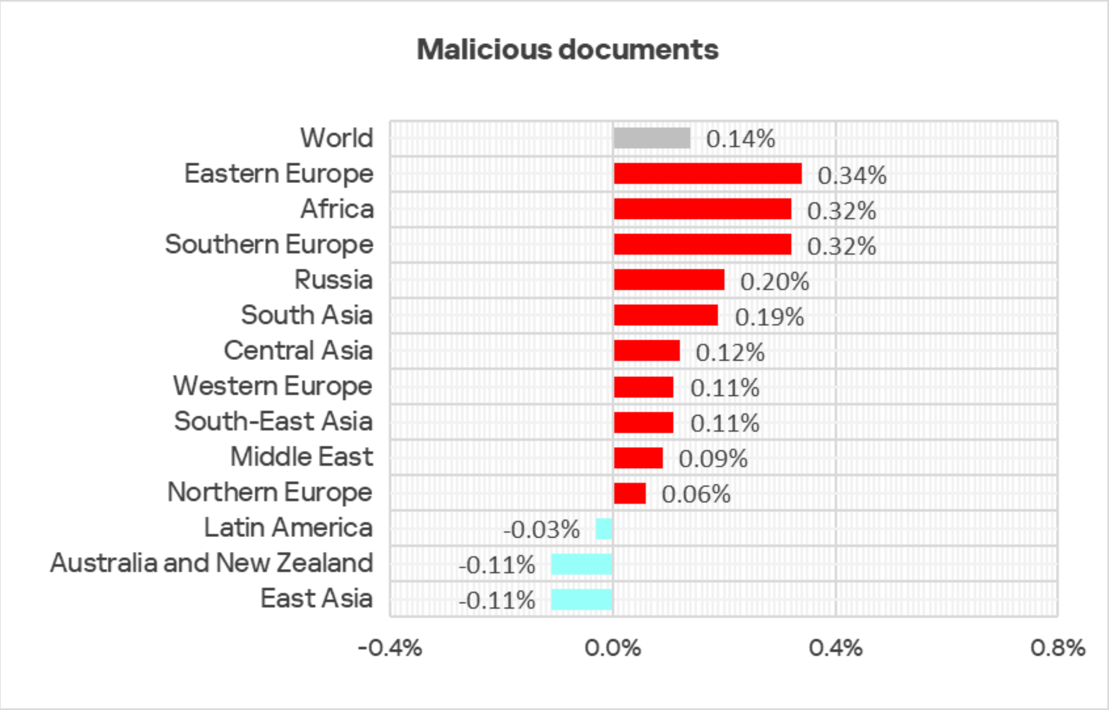
The top three regions by percentage of ICS computers on which malicious documents were blocked were Southern Europe, Latin America, and the Middle East.

Regions ranked by percentage of ICS computers on which malicious documents were blocked, Q1 2025



The top three regions in terms of growth for this indicator were Eastern Europe, Africa, and Southern Europe.

Changes in percentage of ICS computers on which malicious documents were blocked, Q1 2025

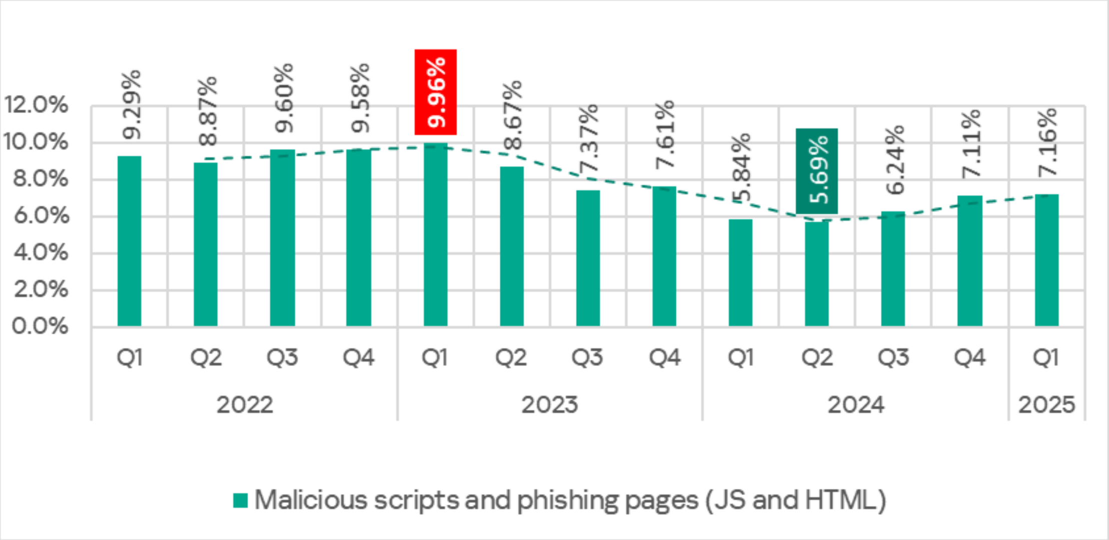


Malicious scripts and phishing pages (JS and HTML)

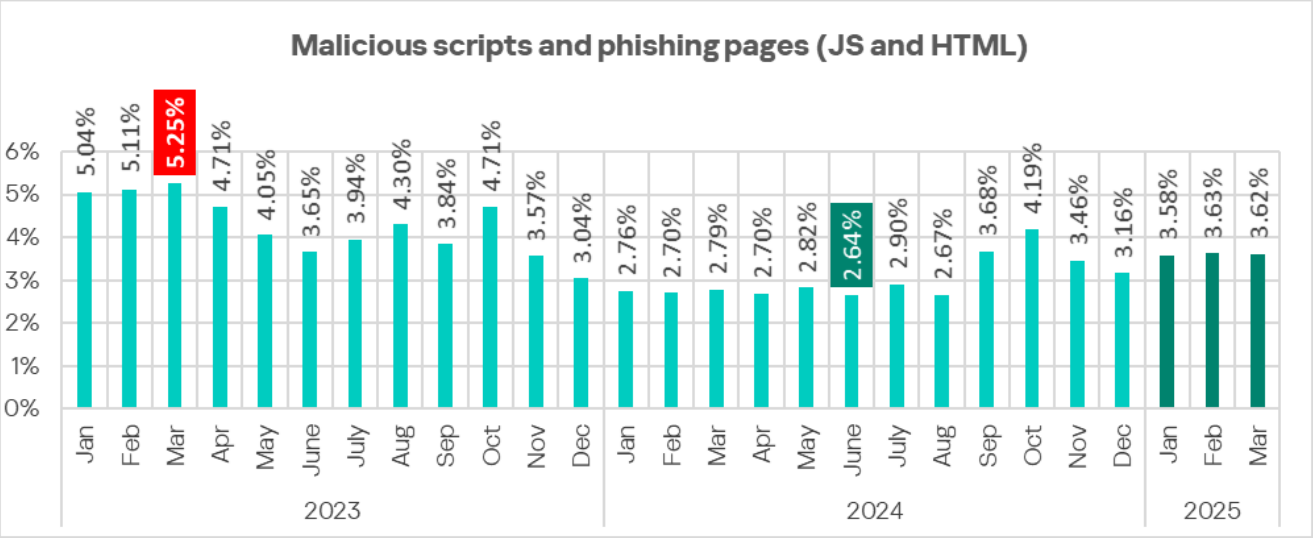
Malicious actors use scripts for a wide range of objectives: collecting information, tracking, redirecting the browser to a malicious site, and uploading various types of malware (spyware, silent crypto mining tools, ransomware) to the user's system or browser. These spread via the internet and email.

In Q1 2025, the percentage of ICS computers on which malicious scripts and phishing pages were blocked increased slightly.

Percentage of ICS computers on which malicious scripts and phishing pages were blocked, Q1 2022–Q1 2025



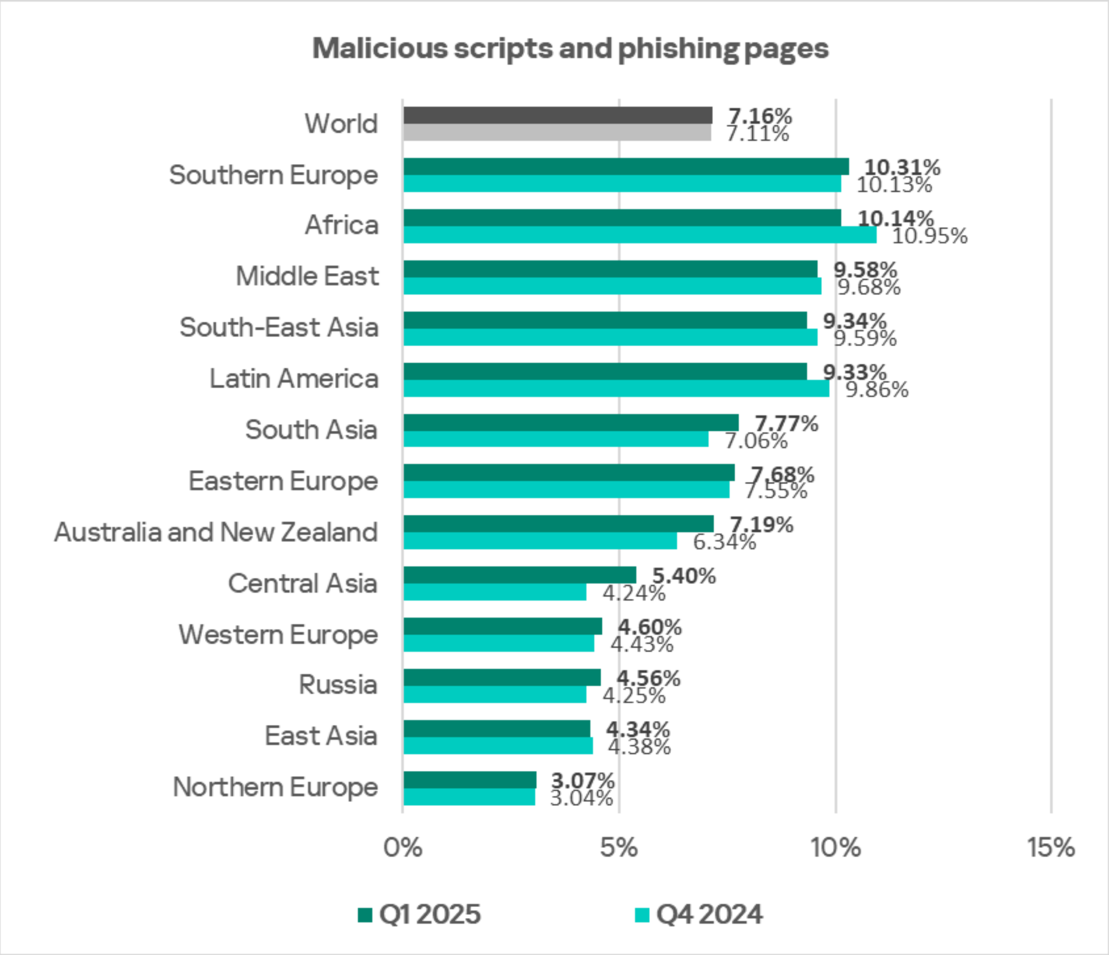
The monthly value of this indicator in January–March 2025 ranged from 3.58% to 3.62%. These figures were much higher than for the same period of 2024.



Percentage of ICS computers on which malicious scripts and phishing pages were blocked, Jan 2023–Mar 2025

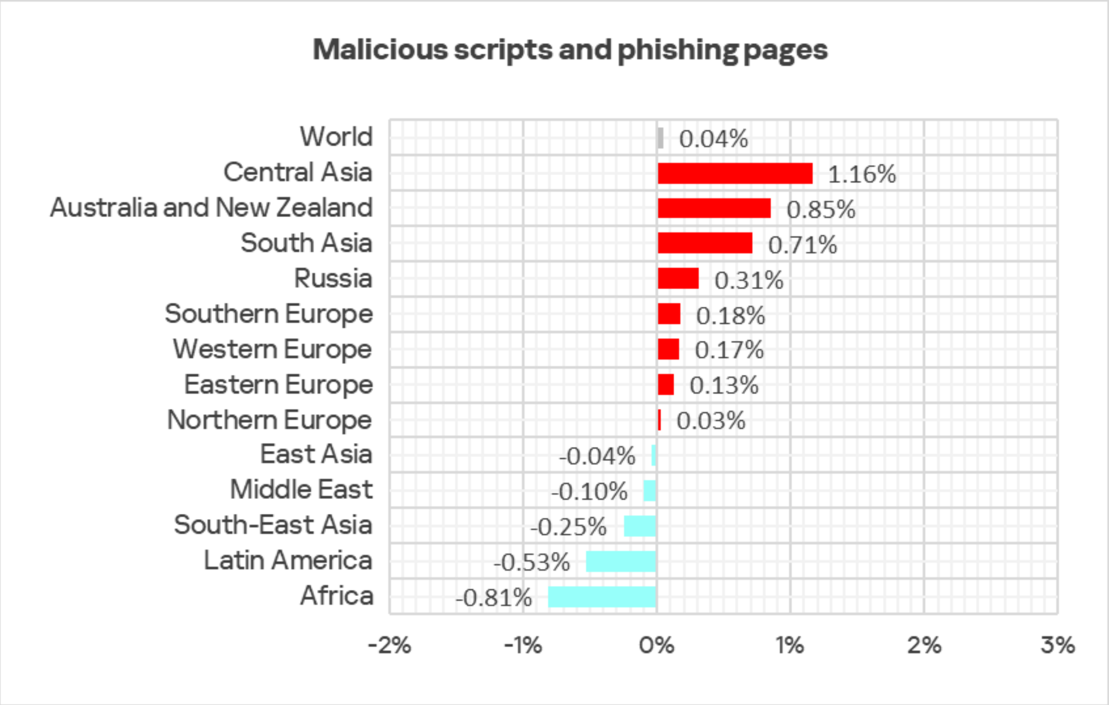
The top three regions by percentage of ICS computers on which malicious scripts and phishing pages were blocked were Southern Europe, Africa, and the Middle East.

Regions ranked by percentage of ICS computers on which malicious scripts and phishing pages were blocked, Q1 2025



The top three regions in terms of growth for this indicator were Central Asia, Australia and New Zealand, and South Asia.

Changes in percentage of ICS computers on which malicious scripts and phishing pages were blocked, Q1 2025



Next-stage malware

Malicious objects used to initially infect computers deliver next-stage malware – spyware, ransomware, and miners – to victims' computers. As a rule, the higher the percentage of ICS computers on which the initial infection malware is blocked, the higher the percentage for next-stage malware.

Spyware

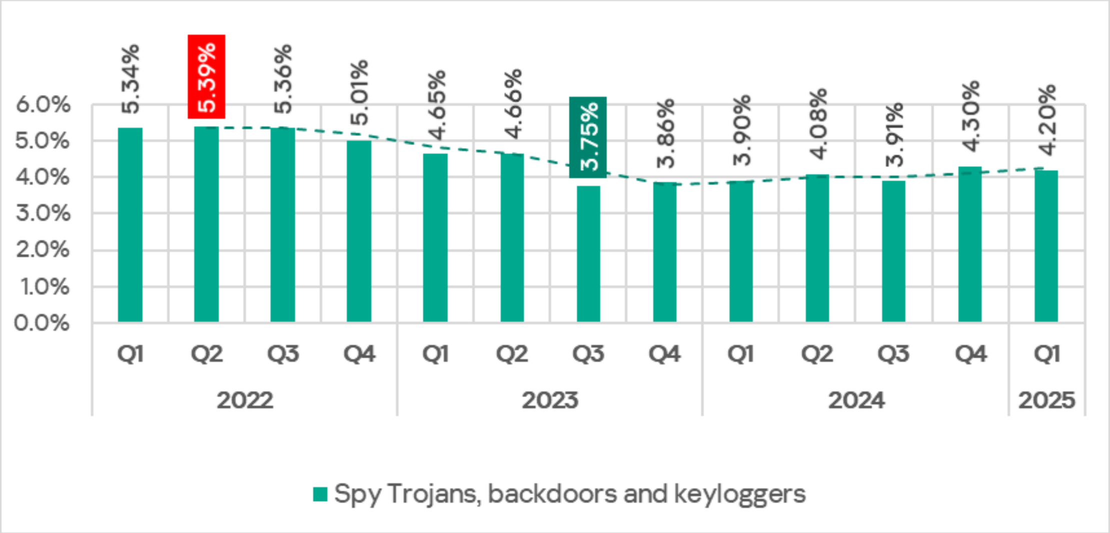
Spyware (spy Trojans, backdoors, and keyloggers) can be found in lots of phishing emails sent to industrial organizations. Spyware is the most frequently detected next-stage malware. It is used as a tool for the intermediate stages of a cyberattack (for example, intelligence and distribution over the network), or as a tool for the last stage of the attack that is used to steal and exfiltrate confidential data. The ultimate goal of most spyware attacks is to steal money, but spyware is also used in targeted attacks for cyberespionage.

Spyware is also used to steal the information needed to deliver other types of malware, such as ransomware and silent miners, as well as to prepare for targeted attacks.

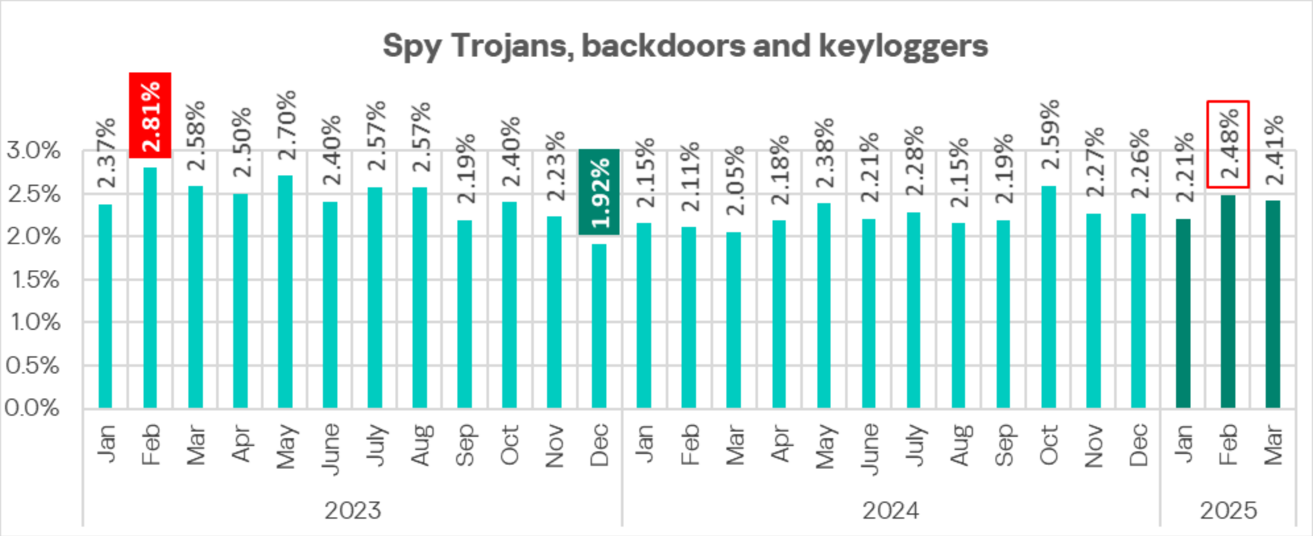
Detection of spyware on an ICS computer usually indicates that the initial infection vector has worked, whether it is clicking on a malicious link, opening an attachment from a phishing email, or connecting an infected USB drive. This indicates the absence or ineffectiveness of measures to protect the perimeter of the OT network (such as monitoring the security of network communications and implementing policies for the use of removable media).

In Q1 2025, the percentage of ICS computers on which spyware was blocked decreased.

Percentage of ICS compute rs on which spyware was blocked, Q1 2022–Q1 2025



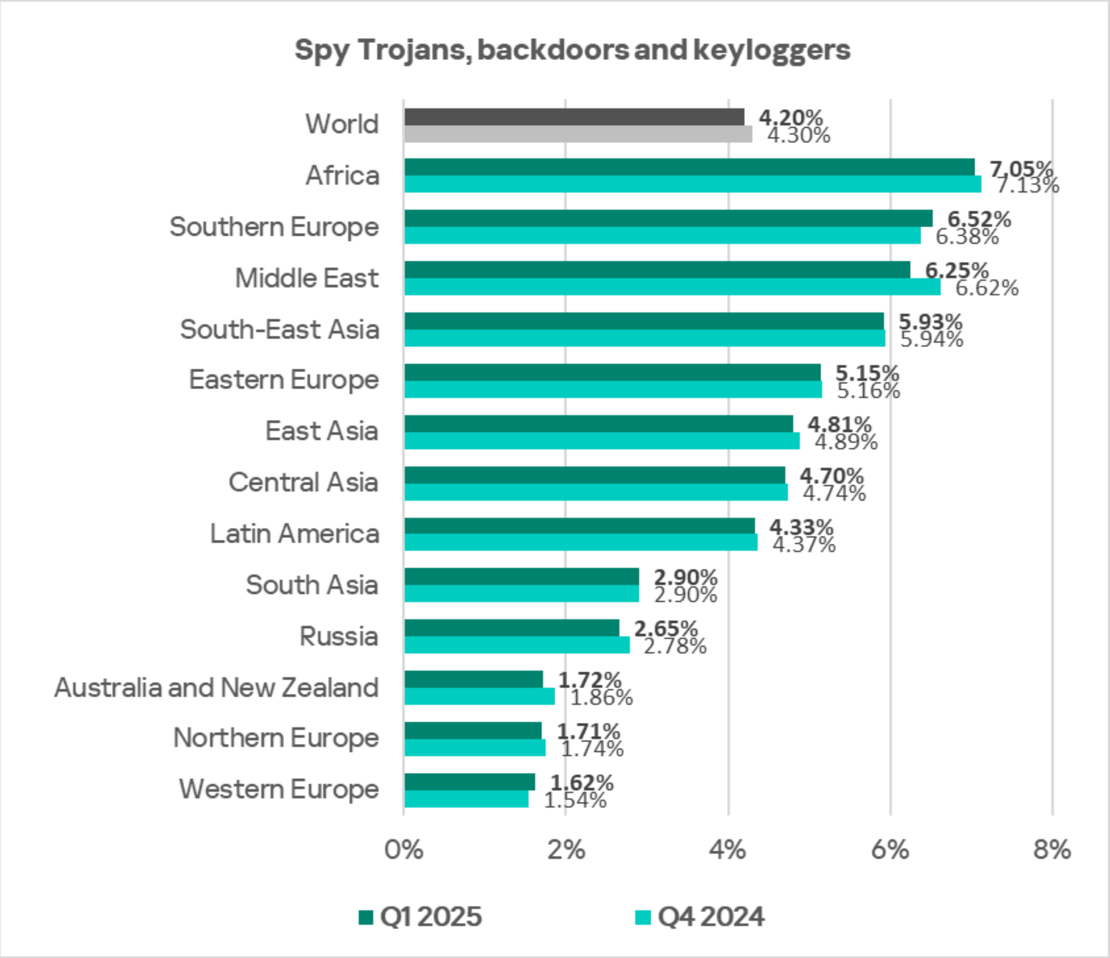
The highest monthly value for Q1 2025 was in February.



Percentage of ICS computers on which spyware was blocked, Jan 2023–Mar 2025

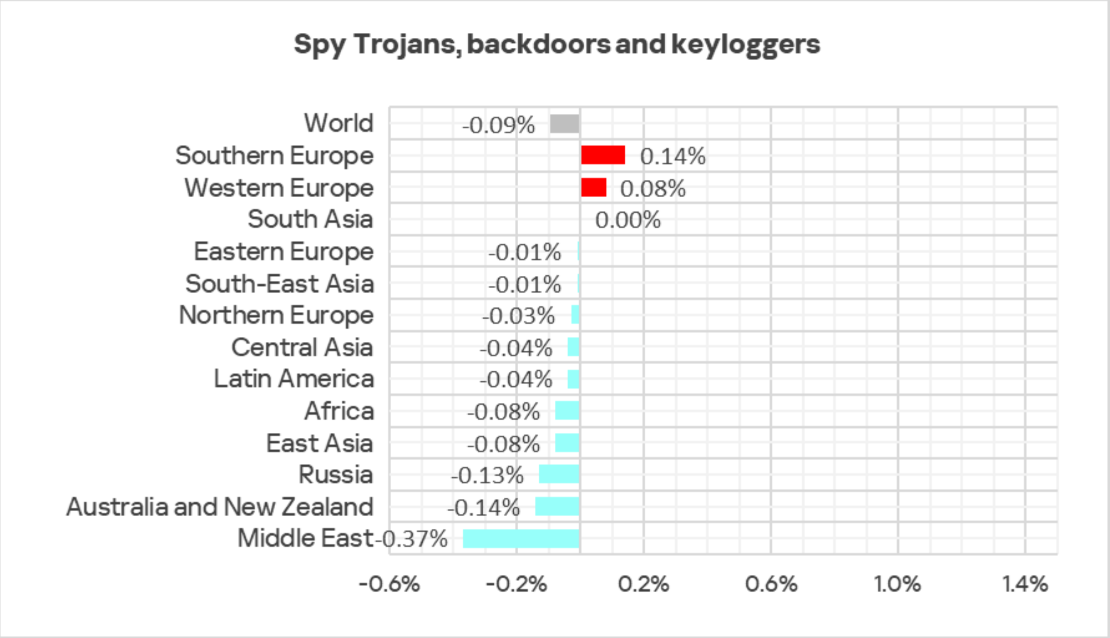
The top three regions by percentage of ICS computers on which spyware was blocked were Africa, Southern Europe and the Middle East. They were also the top regions by percentage of ICS computers on which malicious scripts and phishing pages were blocked.

Regions ranked by percentage of ICS computers on which spyware was blocked, Q1 2025



During the quarter, the percentage of ICS computers on which spyware was blocked increased in Southern and Western Europe.

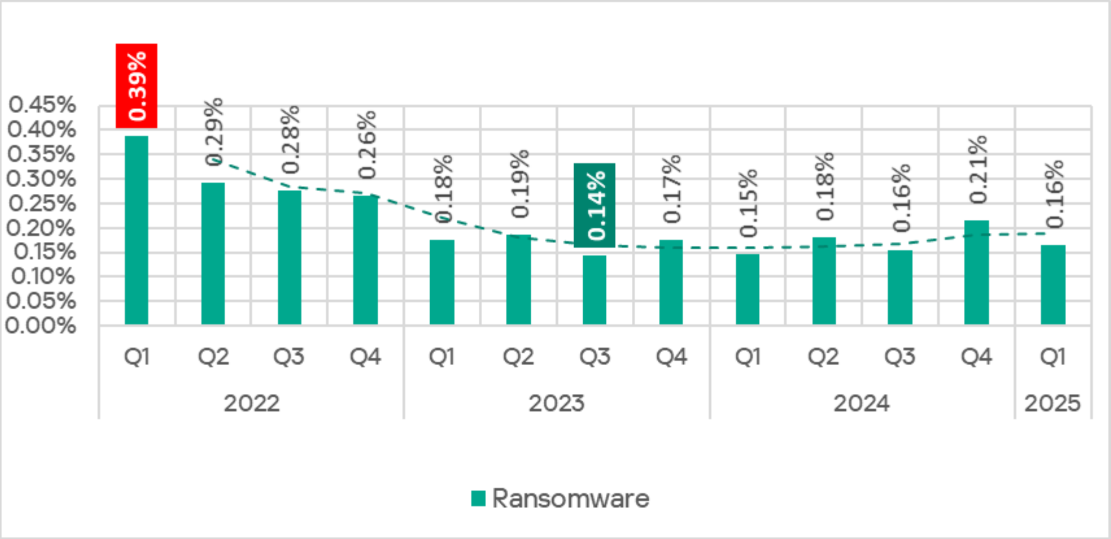
Changes in percentage of ICS computers on which spyware was blocked, Q1 2025



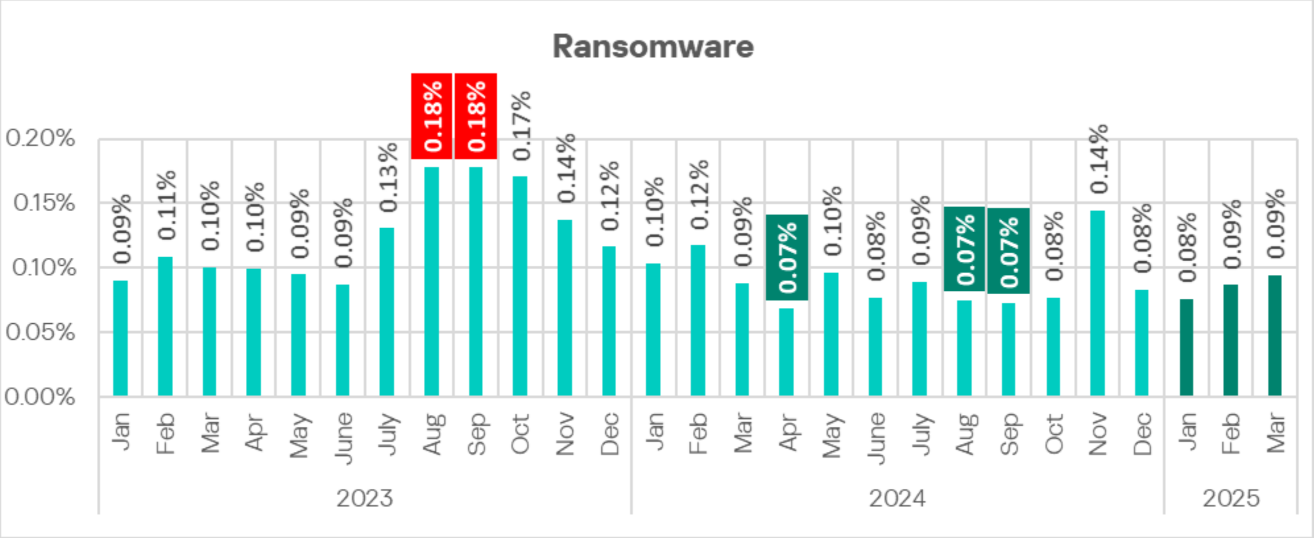
Ransomware

The percentage of ICS computers on which ransomware was blocked decreased after increasing at the end of 2024.

Percentage of ICS compute rs on which ransomware was blocked, Q1 2022–Q1 2025



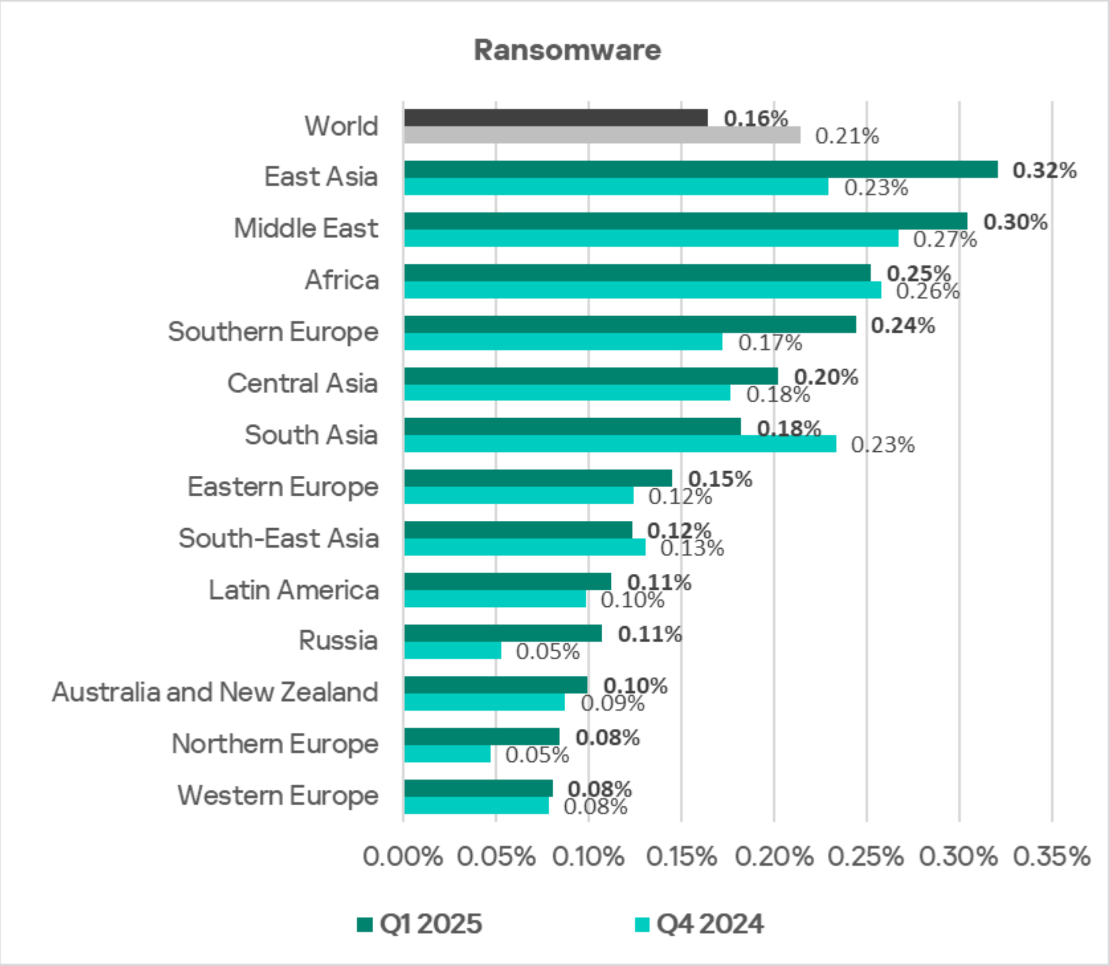
The numbers increased slightly in the first three months of 2025.



Percentage of ICS computers on which ransomware was blocked, Jan 2023–Mar 2025

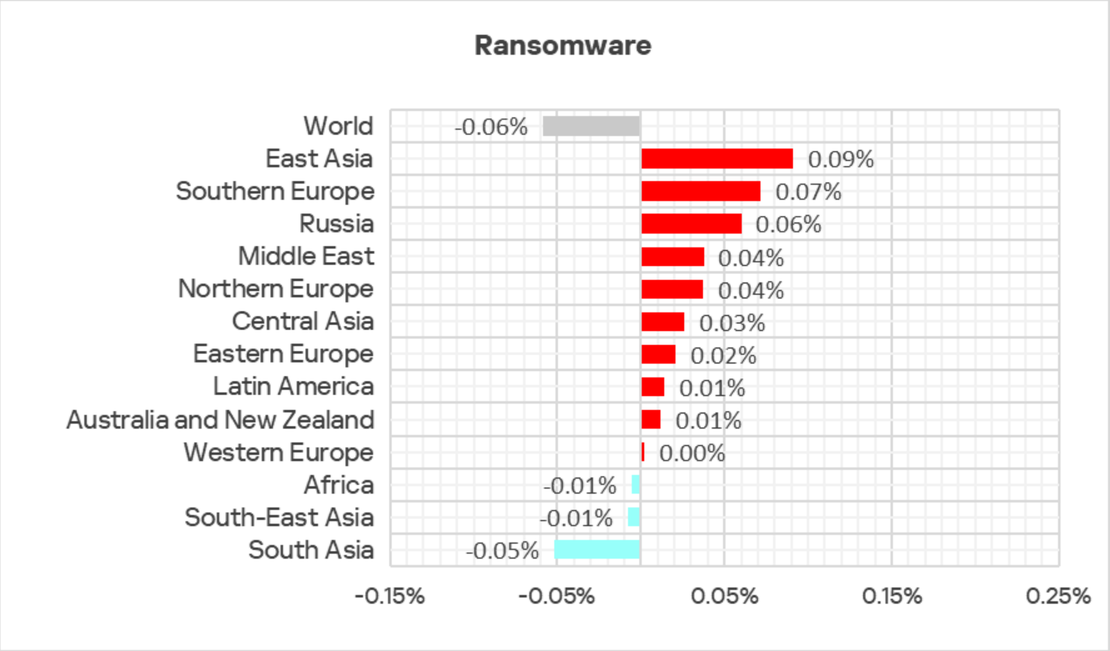
The top three regions by percentage of ICS computers on which ransomware was blocked were East Asia, the Middle East, and Africa.

Regions ranked by percentage of ICS computers on which ransomware was blocked, Q1 2025



The top three regions in terms of growth for this indicator were East Asia, Southern Europe, and Russia.

Changes in percentage of ICS computers on which ransomware was blocked, Q1 2025

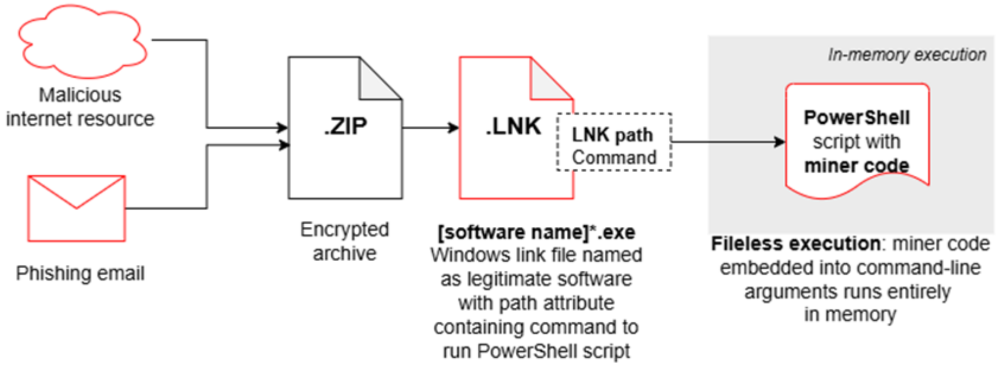


Miners in the form of executable files for Windows

In addition to “classic” miners – applications written in .Net, C++, or Python and designed for hidden crypto mining – new forms are emerging. Popular “fileless” execution techniques continue to be adopted by various threat actors, including those implanting crypto miners on OT machines.

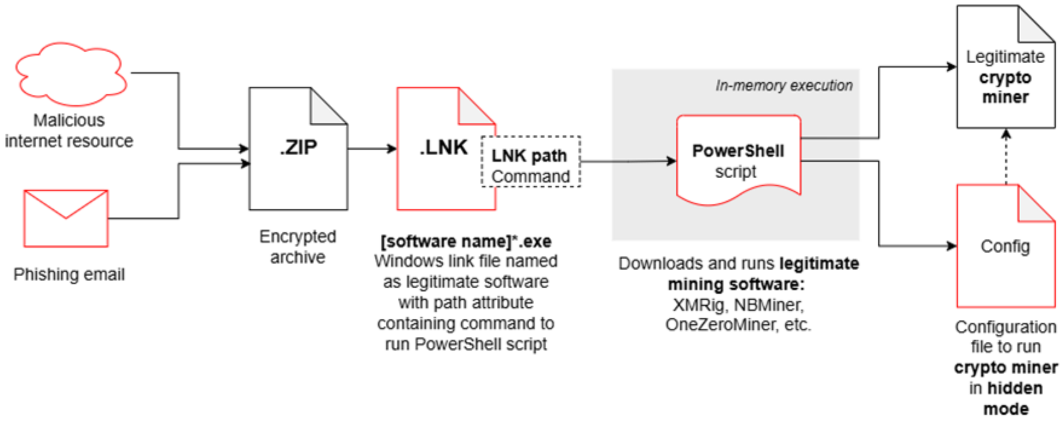
A significant portion of the Windows miners found on ICS computers consisted of archives with names that mimicked legitimate software. These archives did not contain actual software, but did include a Windows LNK file, commonly known as a shortcut. However, the target (or path) that the LNK file points to is not a legitimate application, but rather a command capable of executing malicious code, such as a PowerShell script. Threat actors are now increasingly using PowerShell to execute malware, including crypto miners, by embedding malicious code directly into command line arguments. This code runs entirely in memory, enabling fileless execution and minimizing detection.

Kill chain example: fileless executio n in cryptomining attacks


Malicious internet resource
Phishing email
.ZIP
Encrypted archive
.LNK
LNK path Command
[software name]*.exe Windows link file named as legitimate software with path attribute containing command to run PowerShell script
In-memory execution
PowerShell script with miner code
Fileless execution: miner code embedded into command-line arguments runs entirely in memory

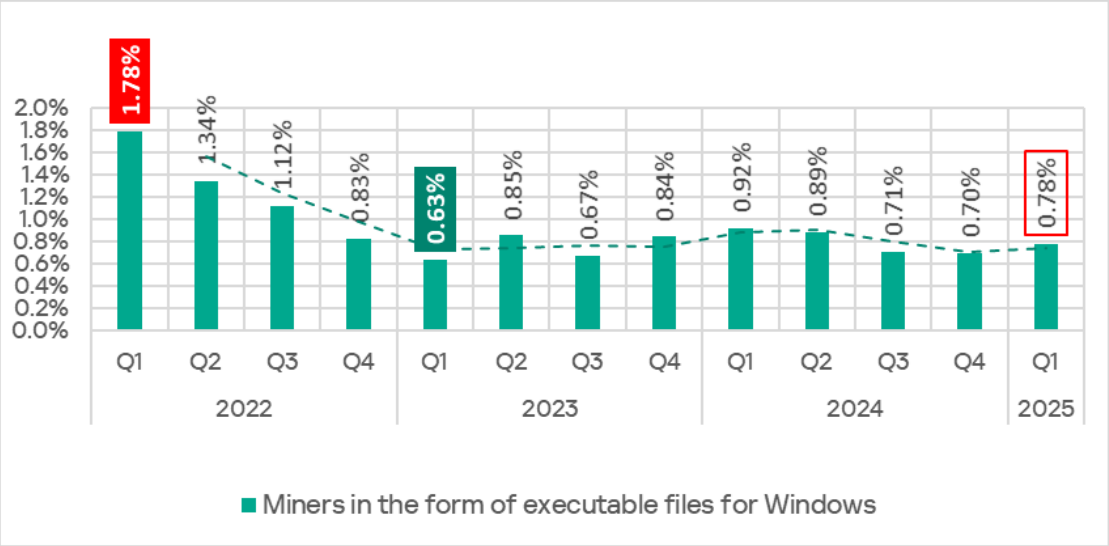
Another common method of deploying miners on ICS computers involves using legitimate cryptocurrency mining software such as XMRig, NBMiner, OneZeroMiner, and others. While these miners are not inherently malicious, they are classified as RiskTools by security systems. Attackers exploit these miners by combining them with customized configuration files that enable the miner’s activity to be concealed from the user’s view.

Kill chain example: use of legitimate mining tools in cryptomining attacks

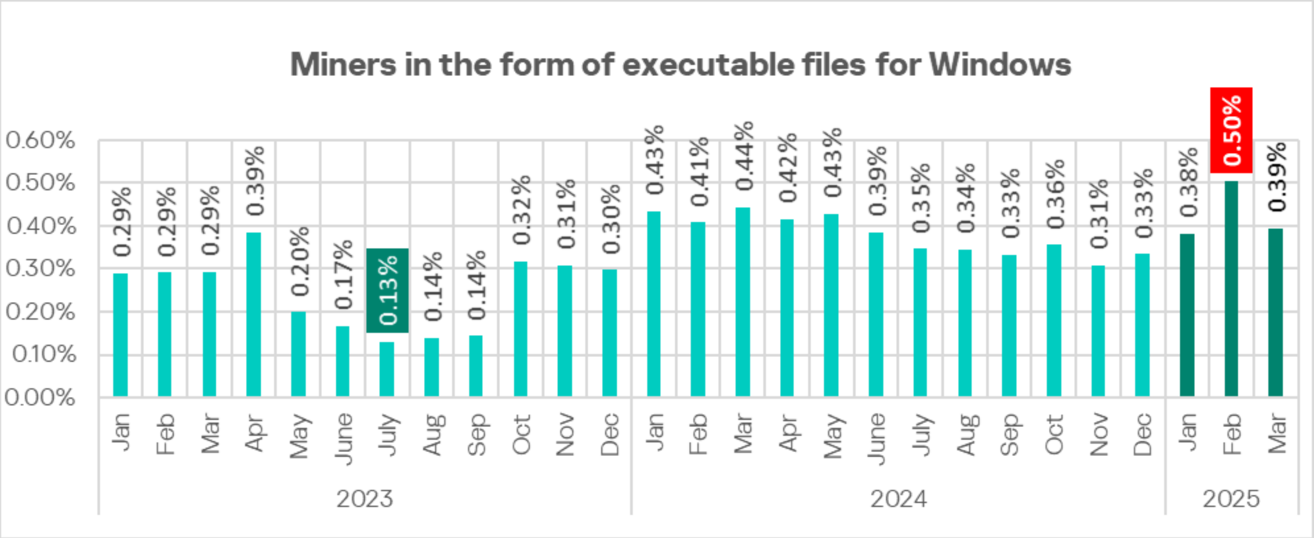

Malicious internet resource
Phishing email
.ZIP
Encrypted archive
.LNK
LNK path Command
[software name]*.exe
Windows link file named as legitimate software with path attribute containing command to run PowerShell script
In-memory execution
PowerShell script
Downloads and runs **legitimate mining software:** XMRig, NBMiner, OneZeroMiner, etc.
Legitimate **crypto miner**
Config
Configuration file to run **crypto miner** in **hidden mode**

In Q1 2025, the percentage of ICS computers on which miners in the form of executable files for Windows were blocked increased.

Percentage of ICS compute rs on which miners in the form of executable files for Windows were blocked, Q1 2022–Q1 2025

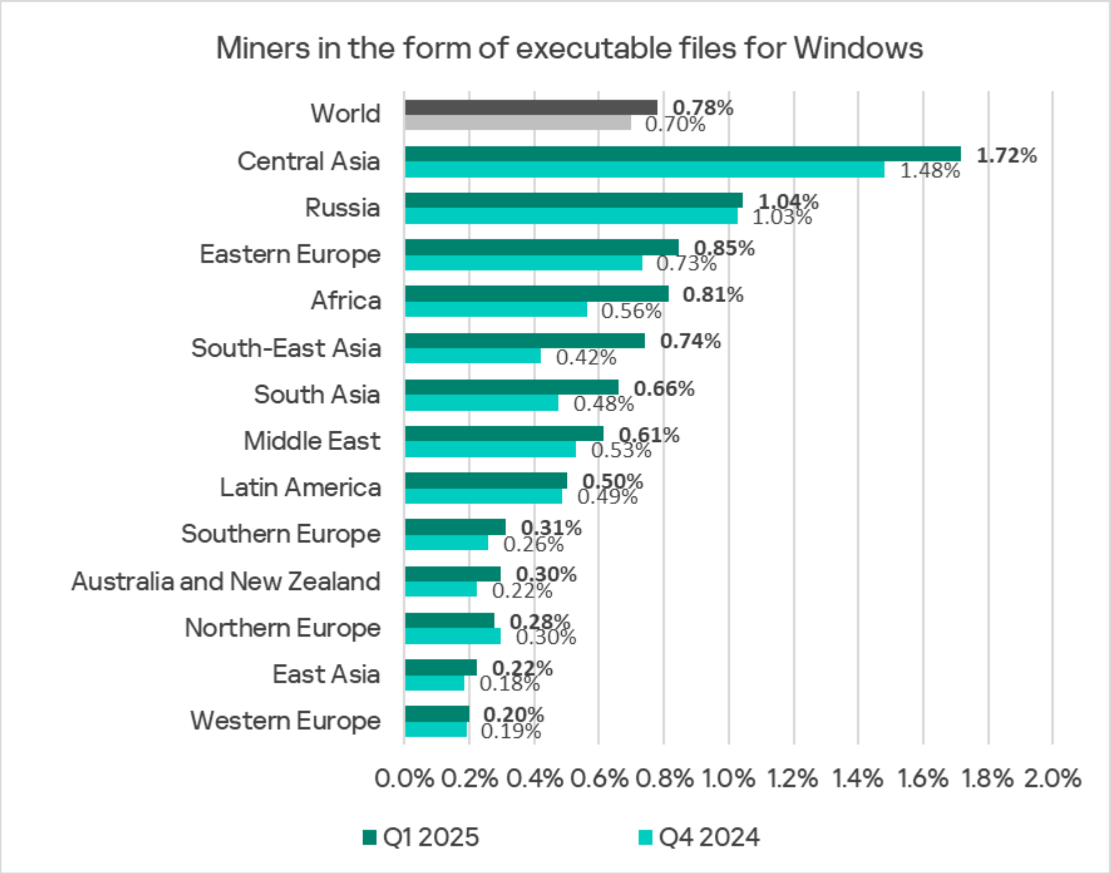


In February 2025, the monthly rate reached its highest monthly value since the beginning of 2023.



Percentage of ICS computers on which miners in the form of executable files for Windows were blocked, Jan 2023–Mar 2025

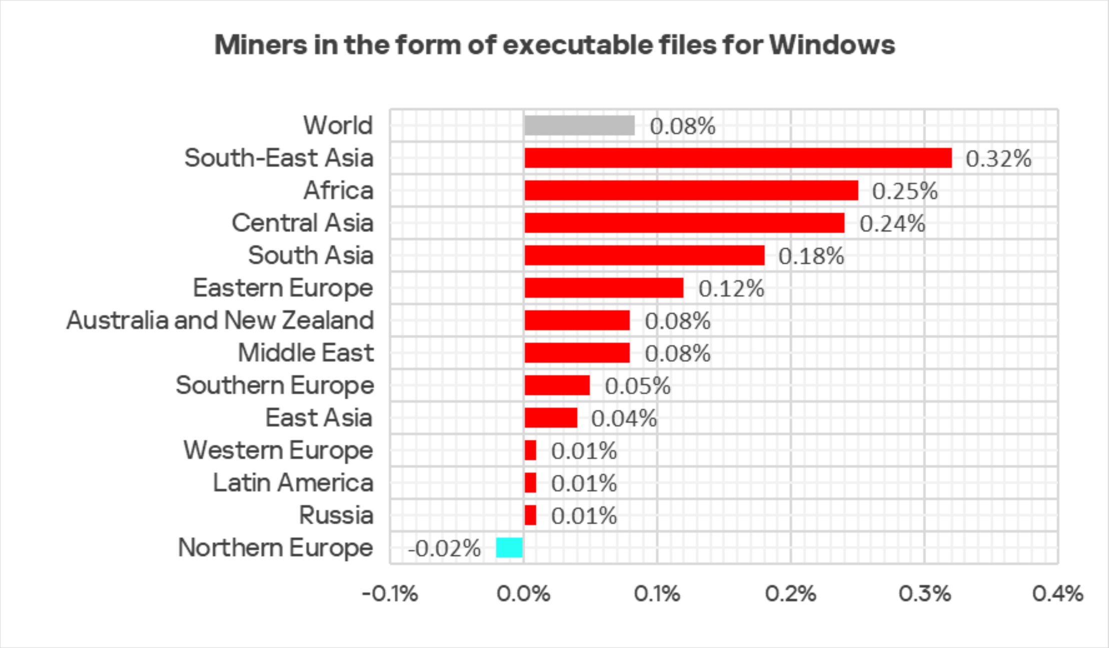
Central Asia, Russia, and Eastern Europe were the top three regions by percentage of ICS computers on which miners in the form of executable files for Windows were blocked.



Regions ranked by percentage of ICS computers on which miners in the form of executable files for Windows were blocked, Q1 2025

In Q1 2025, the percentage increased in all regions except Norther Europe. The top three regions in terms of growth for this indicator were South-East Asia, Africa, and Central Asia.

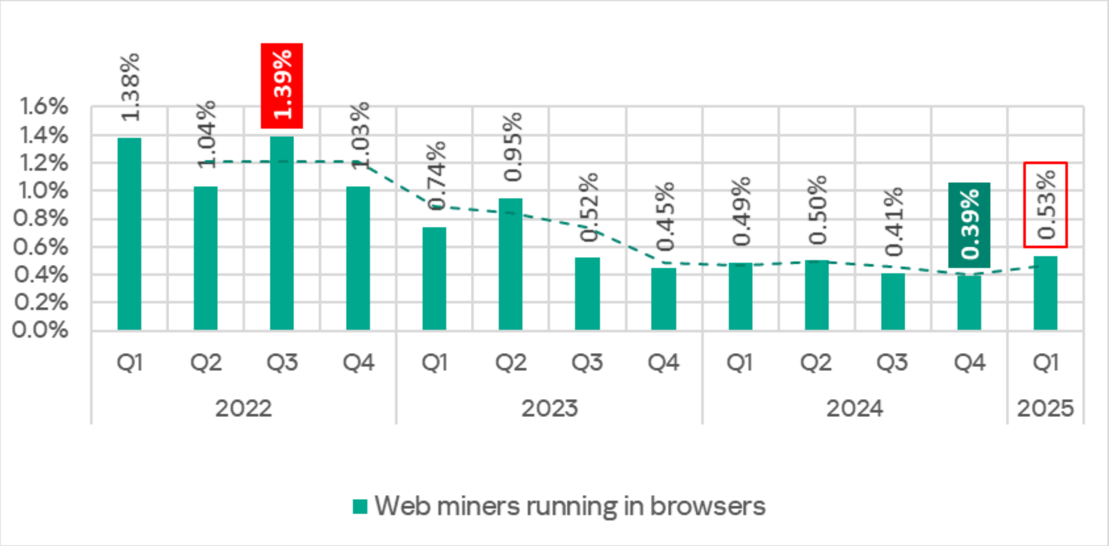
Changes in percentage of ICS computers on which miners in the form of executable files for Windows were blocked, Q1 2025



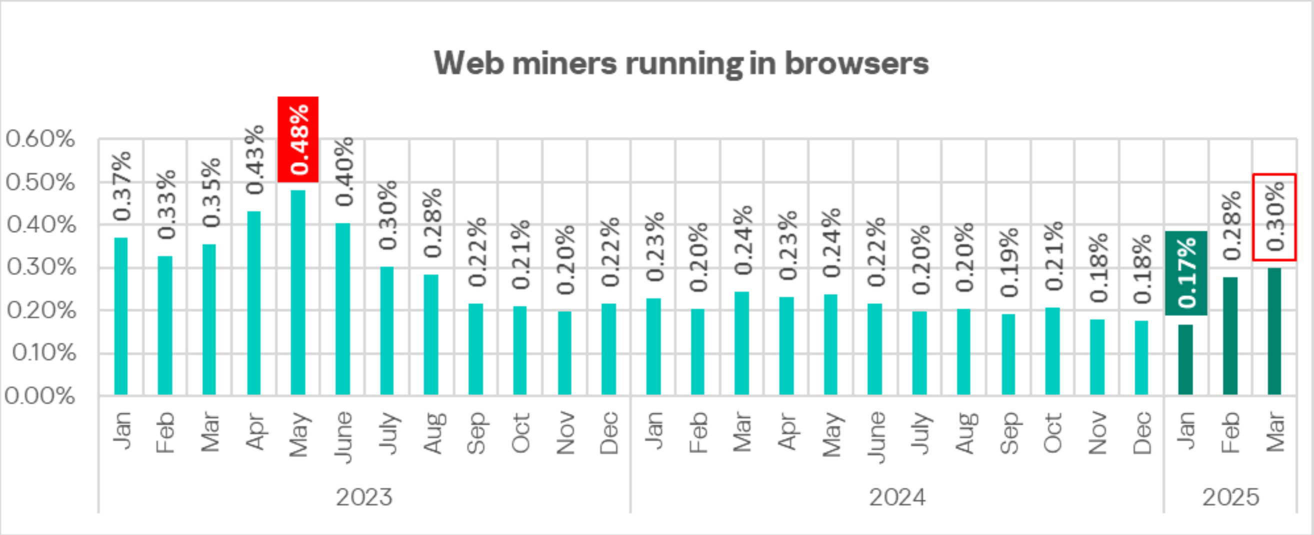
Web miners

In Q1 2025, the percentage of ICS computers on which web miners were blocked increased, reaching its highest level since Q3 2023.

Percentage of ICS compute rs on which web miners were blocked, Q1 2022–Q1 2025



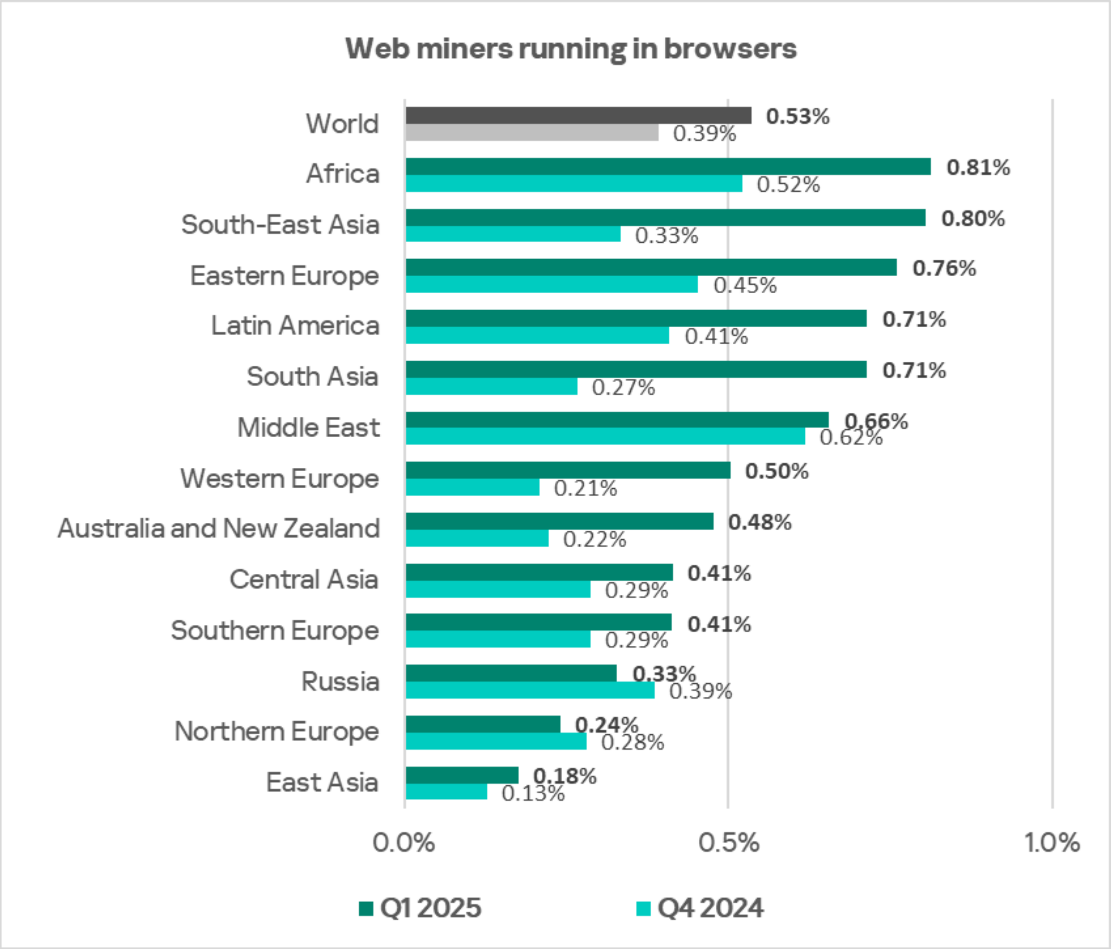
In January 2025, the monthly rate fell to its lowest point since the beginning of 2023, but increased over the next two months to its highest level since July 2023.



Percentage of ICS computers on which web miners were blocked, Jan 2023–Mar 2025

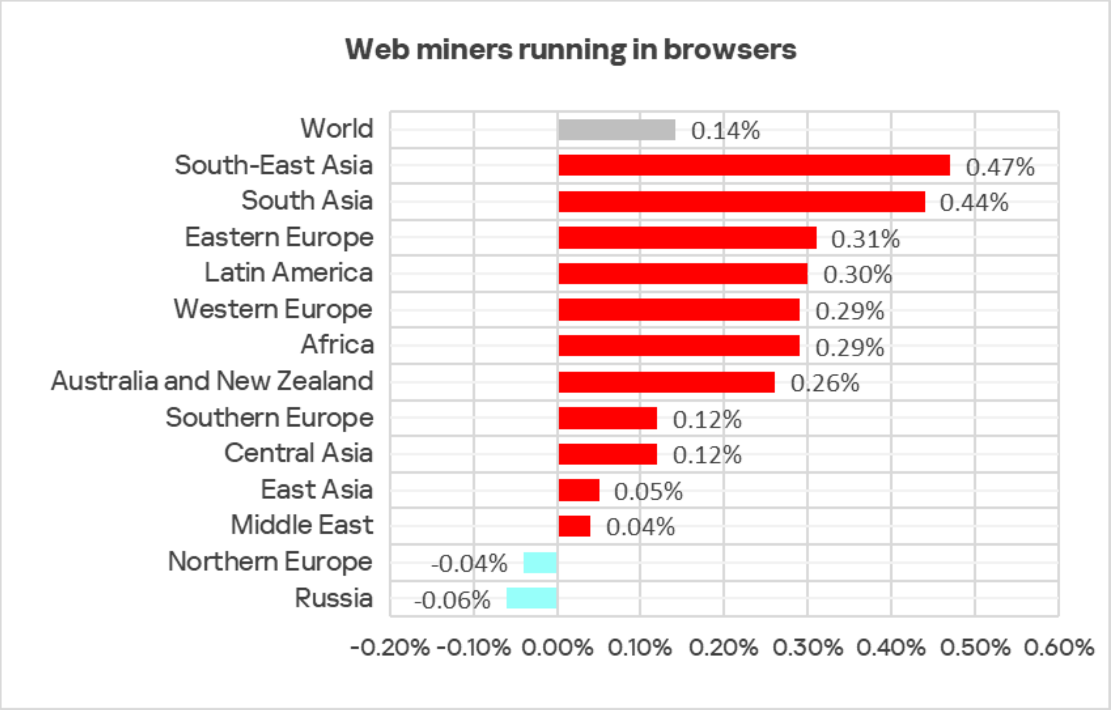
The top three regions by percentage of ICS computers on which web miners were blocked were Africa, South-East Asia, and Eastern Europe.

Regions ranked by percentage of ICS computers on which web miners were blocked, Q1 2025



In Q1 2025, the percentage of ICS computers on which web miners were blocked increased in all regions, with the exception of Northern Europe and Russia. South-East Asia and South Asia were the leading regions for this indicator.

Changes in percentage of ICS computers on which web miners were blocked, Q1 2025



Self-propagating malware. Worms and viruses

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.

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.

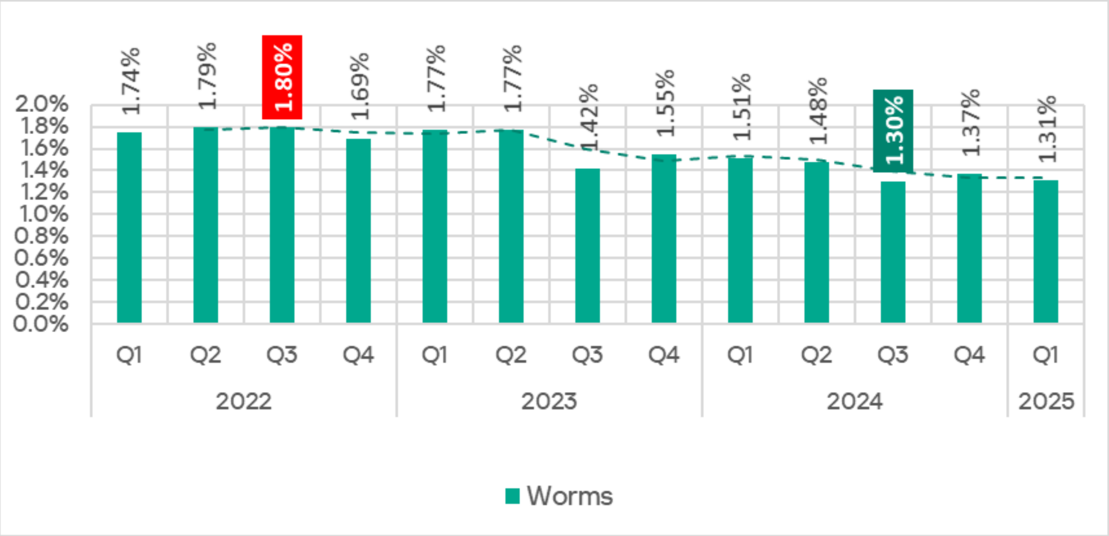
High rates of self-propagating malware and malware spreading via network folders at the industry, country or regional level likely indicate the presence of unprotected OT infrastructure that lacks even basic endpoint protection. These unprotected computers become sources of malware propagation. The situation may be exacerbated by the weak segmentation of an enterprise network, and a lack of control over the use of removable media.

Worms

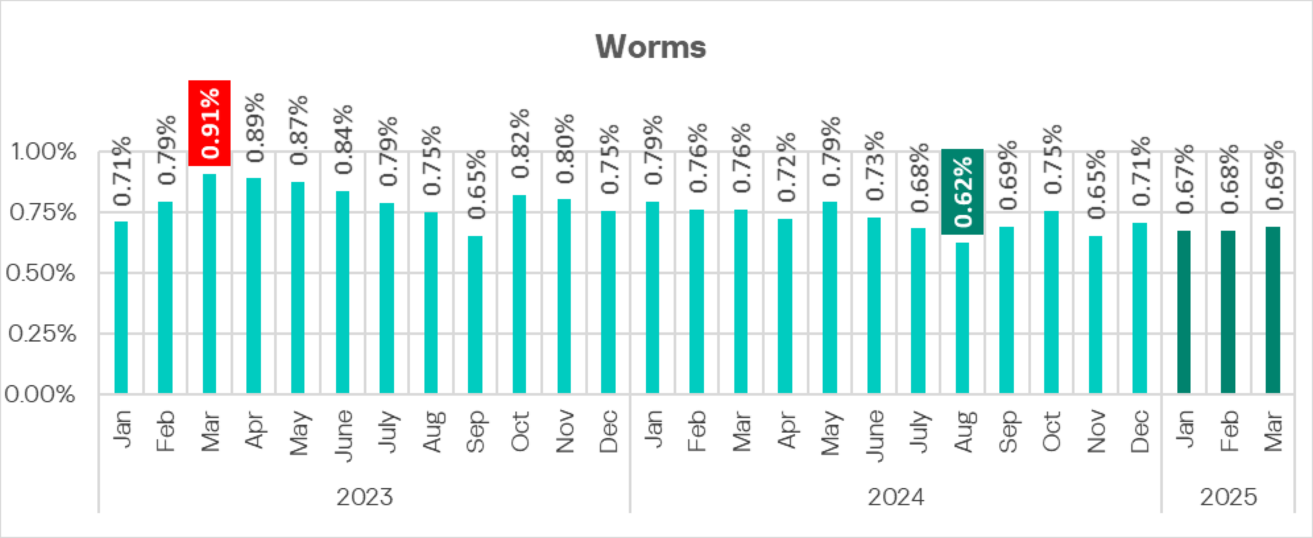
New worm versions used by malicious actors to spread spyware, ransomware and miners can also be found on ICS networks. In most cases, they rely on network service (e.g., SMB or RDP) exploits that have been addressed by the vendors but still persist on OT networks, previously stolen credentials, or password brute-forcing.

In Q1 2025, the percentage of ICS computers on which worms were blocked decreased.

Percentage of ICS compute rs on which worms were blocked, Q1 2022–Q1 2025



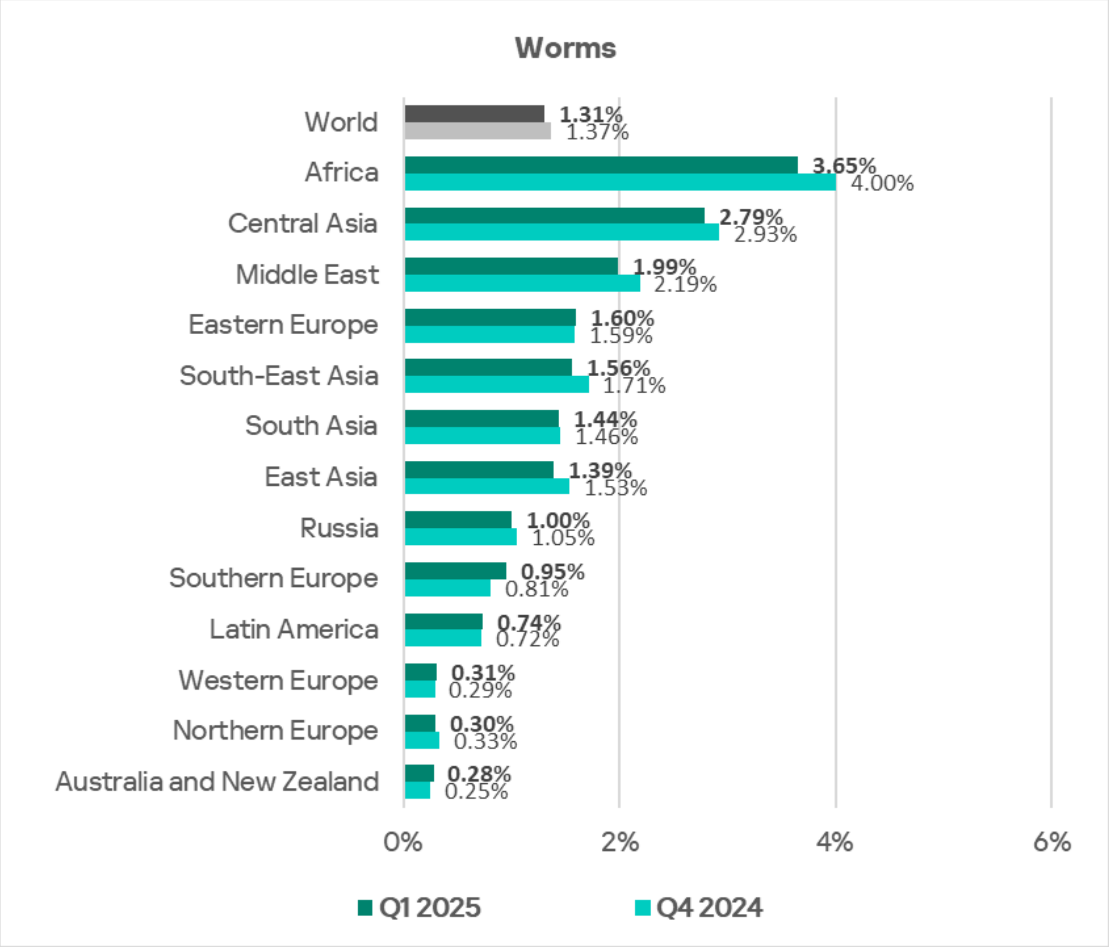
At the same time, the monthly rate increased slightly each month during the quarter.



Percentage of ICS computers on which worms were blocked, Jan 2023–Mar 2025

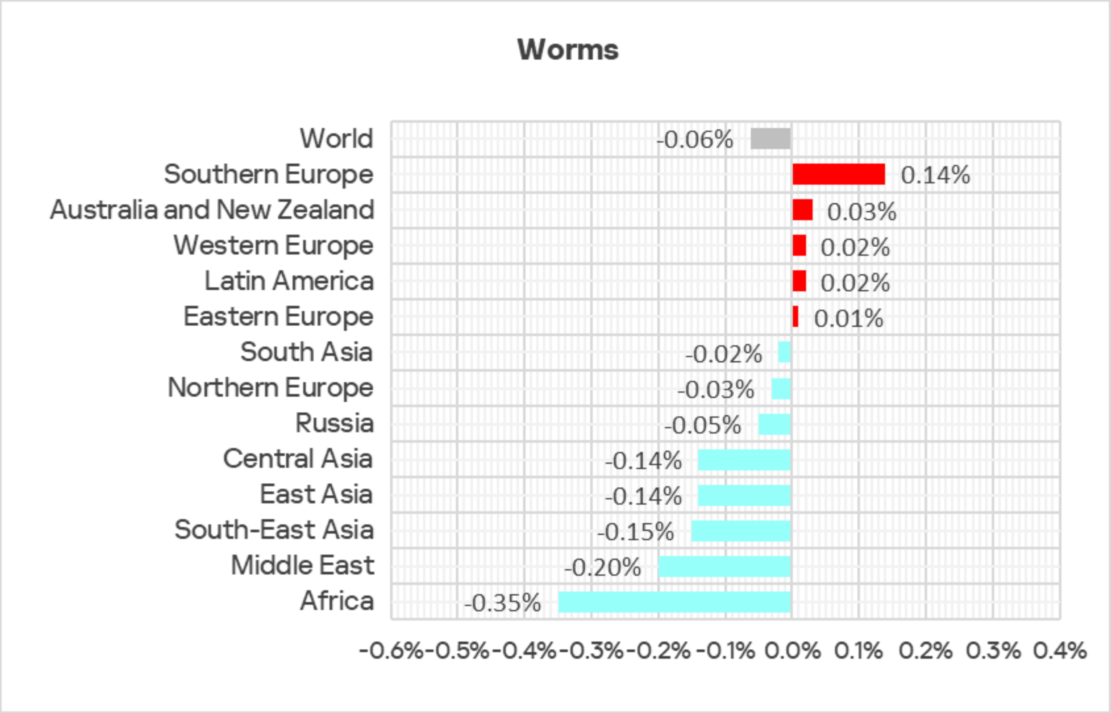
The top three regions by percentage of ICS computers on which worms were blocked were Africa, Central Asia, and the Middle East.

Regions ranked by percentage of ICS computers on which worms were blocked, Q1 2025



Southern Europe was the leader in terms of growth for this indicator.

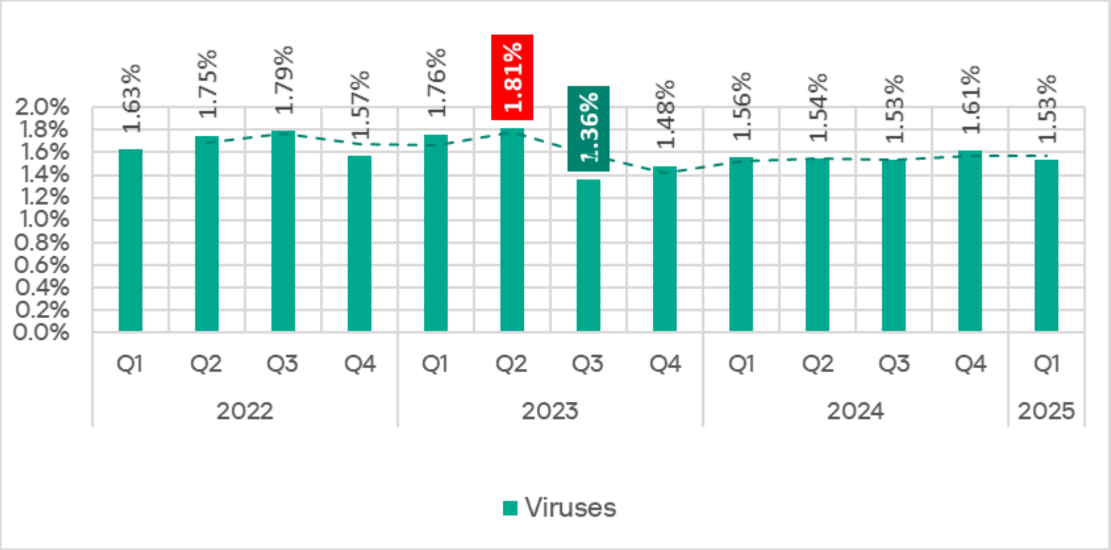
Changes in percentage of ICS computers on which worms were blocked, Q1 2025



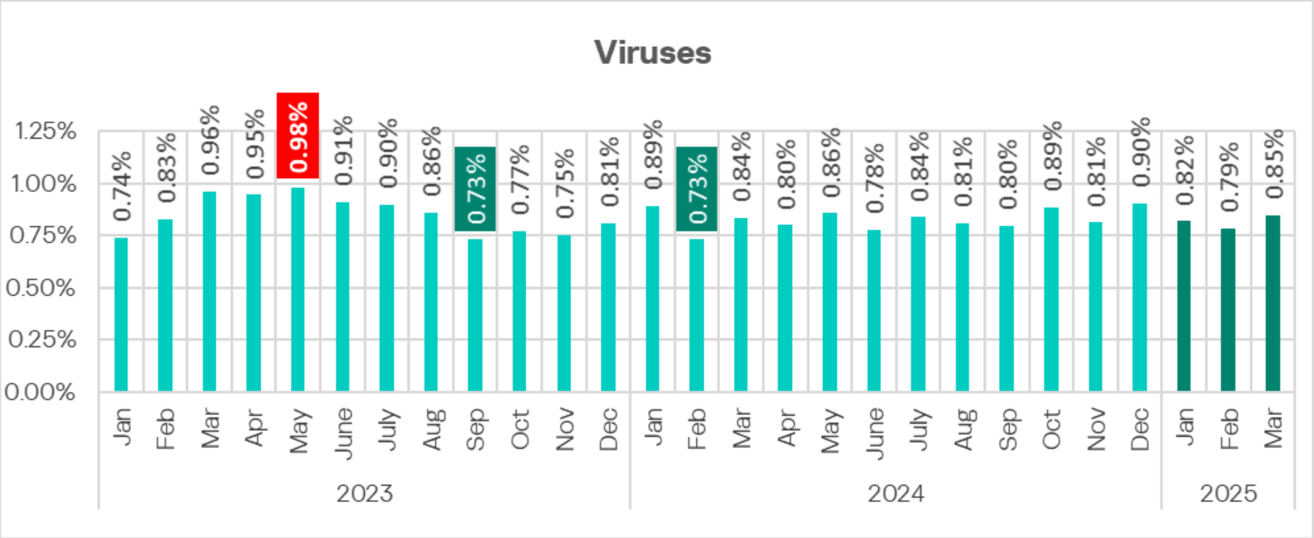
Viruses

In Q1 2025, the percentage of ICS computers on which viruses were blocked decreased.

Percentage of ICS compute rs on which viruses were blocked, Q1 2022– Q1 2025

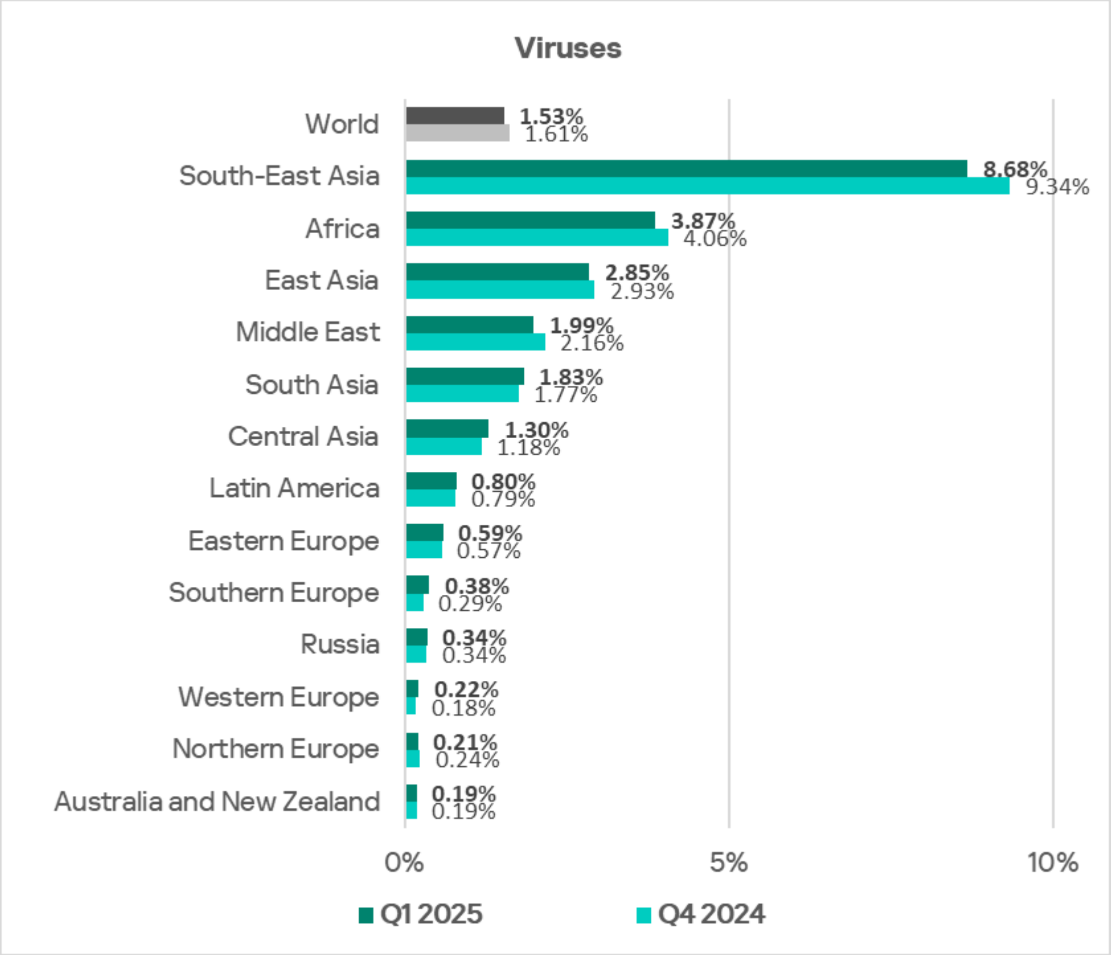


The monthly rate varied over the course of the quarter.



Percentage of ICS computers on which viruses were blocked, Jan 2023–Mar 2025

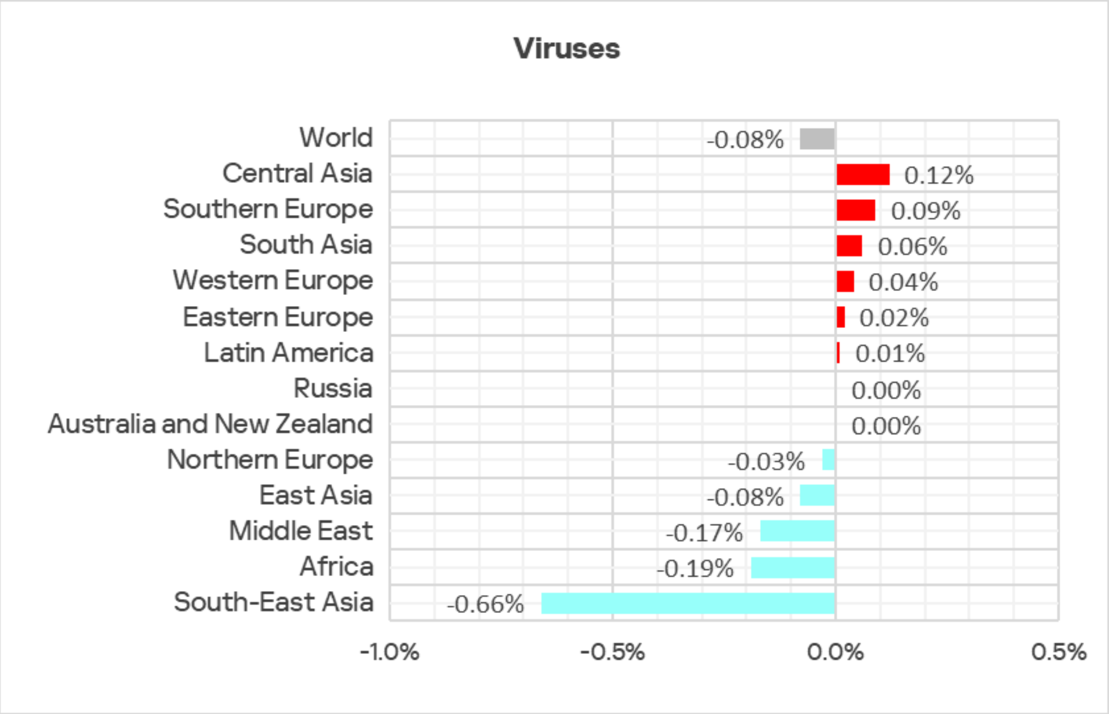
The top three regions by percentage of ICS computers on which viruses were blocked were South-East Asia, Africa, and East Asia.



Regions ranked by percentage of ICS computers on which viruses were blocked, Q1 2025

Central Asia was the leader in terms of growth for this indicator.

Changes in percentage of ICS computers on which viruses were blocked, Q1 2025



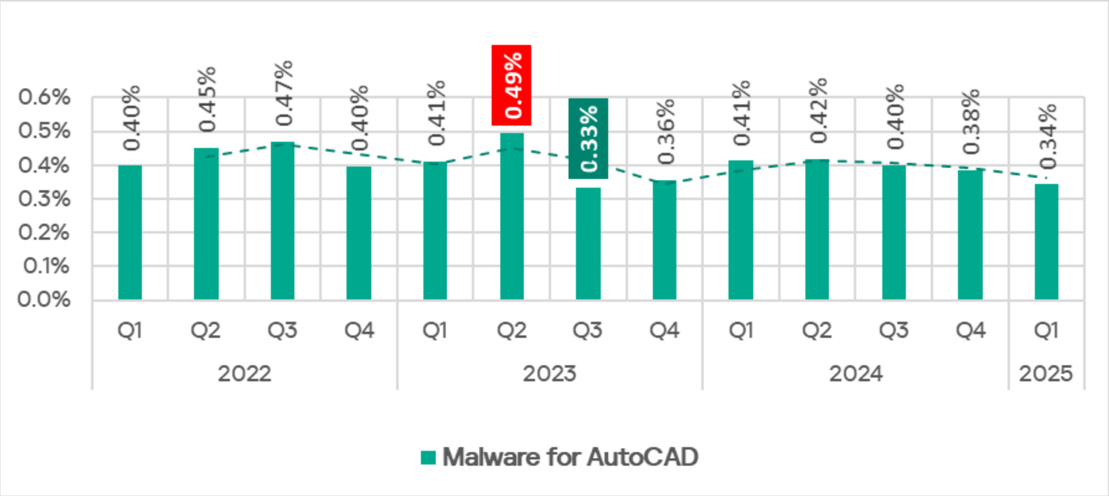
AutoCAD malware

This category of malware can spread in a variety of ways, so it does not belong to a specific group.

AutoCAD malware is typically a low-level threat, coming last in the malware category rankings in terms of the percentage of ICS computers on which it was blocked.

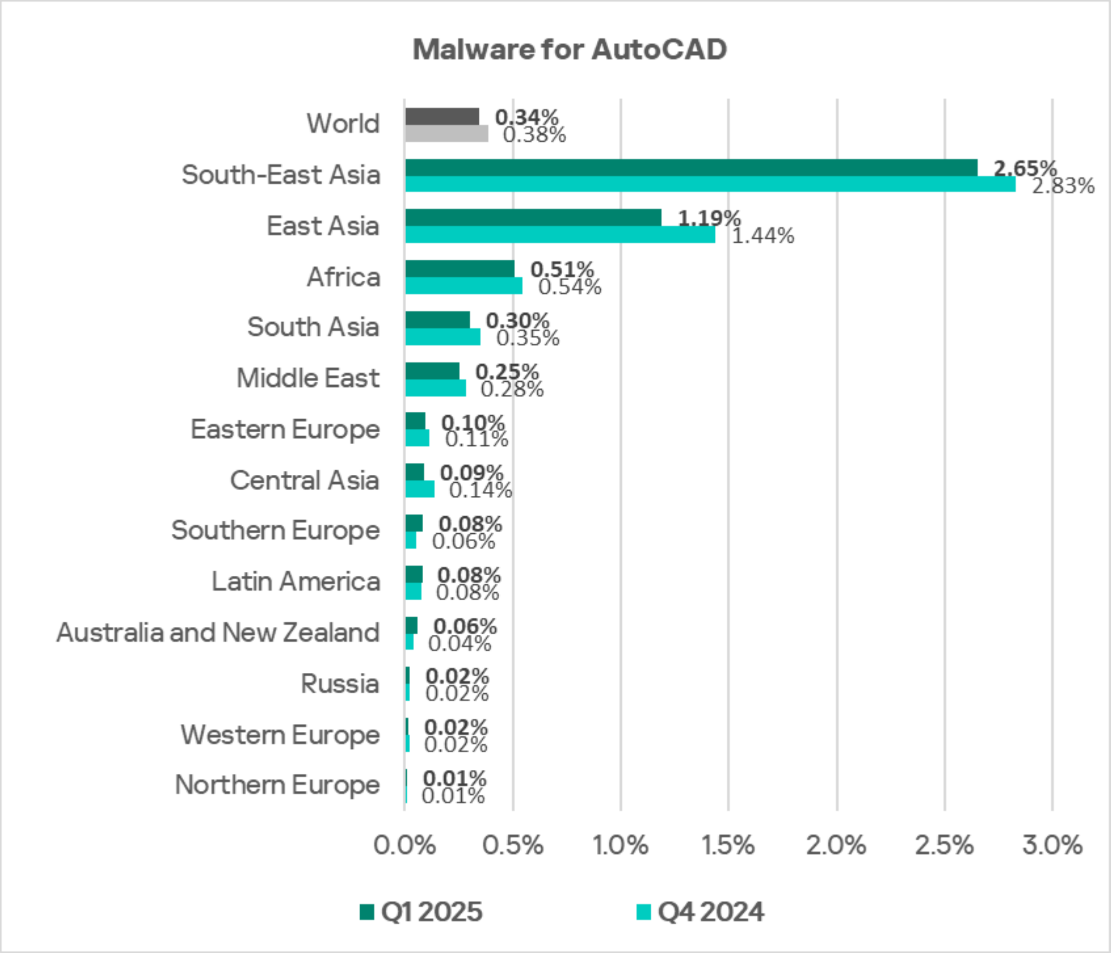
In Q1 2025, the percentage of ICS computers on which AutoCAD malware was blocked continued to decrease.

Percentage of ICS compute rs on which AutoCAD malware was blocked, Q1 2022– Q1 2025



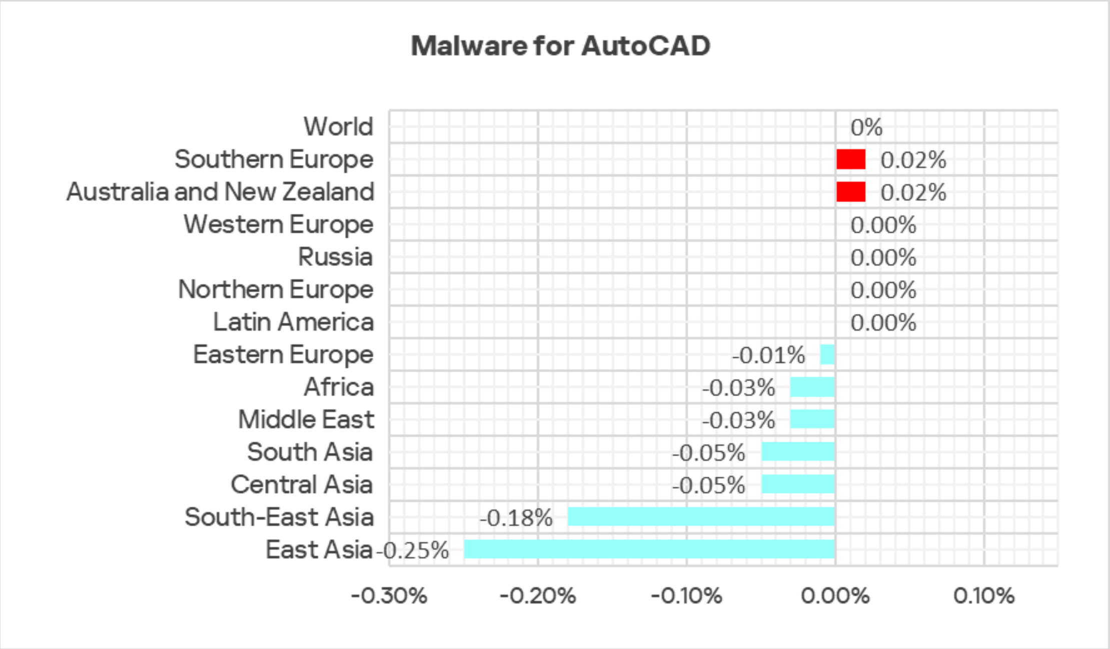
The same regions that led the virus ranking were also the leaders in terms of the percentage of ICS computers on which AutoCAD malware was blocked: South-East Asia, East Asia, and Africa.

Regions ranked by percentage of ICS compute rs on which AutoCAD malware was blocked, Q1 2025



Southern Europe, and Australia and New Zealand were the leaders in terms of growth for this indicator.

Changes in percentage of ICS compute rs on which AutoCAD malware was blocked, Q1 2025



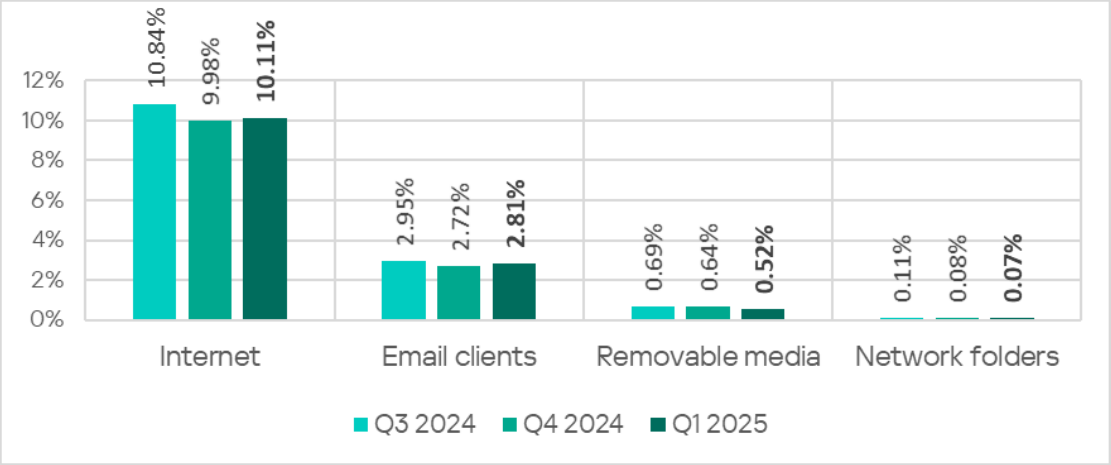
Main threat sources

Depending on the threat detection and blocking scenario, it is not always possible to reliably identify the source. The circumstantial evidence for a specific source can be the blocked threat's type (category).

The internet (visiting malicious or compromised internet resources; malicious content distributed via messengers; cloud data storage and processing services and CDNs), email clients (phishing emails), and removable storage devices remain the primary sources of threats to computers in an organization's technology infrastructure.

In Q1 2025, the percentage of ICS computers on which threats from the internet and email clients were blocked increased for the first time since the end of 2023.

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



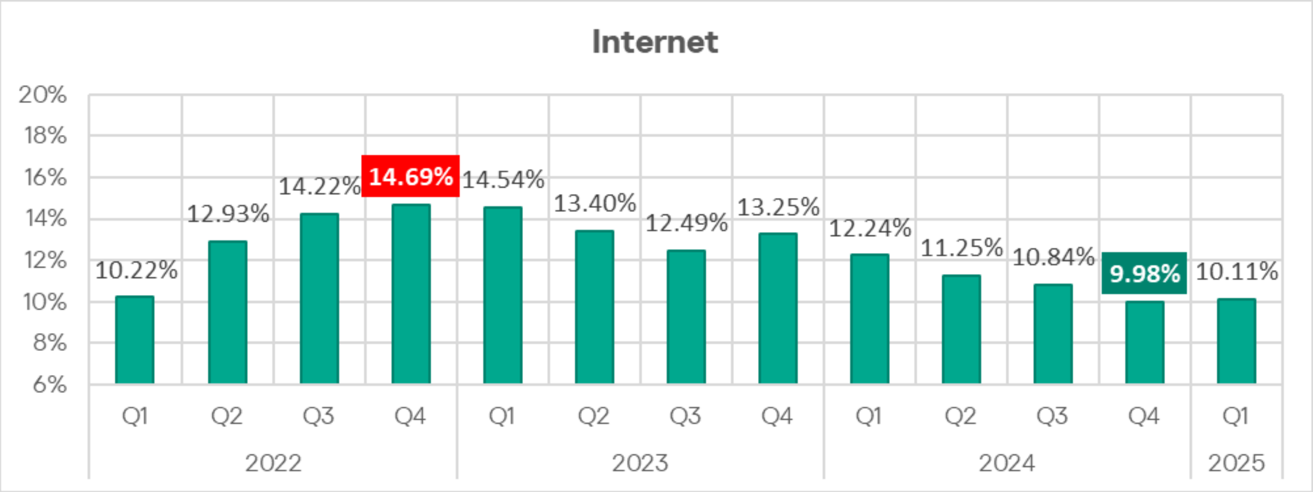
The rates for all threat sources varied across the observed regions.

- The percentage of ICS computers on which threats from the internet were blocked ranged from 5.2% in Northern Europe to 12.8% in Africa.
- The percentage of ICS computers on which threats from email clients were blocked ranged from 0.88% in Russia to 6.8% in Southern Europe.
- The percentage of ICS computers on which threats from removable media were blocked ranged from 0.06% in Australia and New Zealand to 2.4% in Africa.

Internet

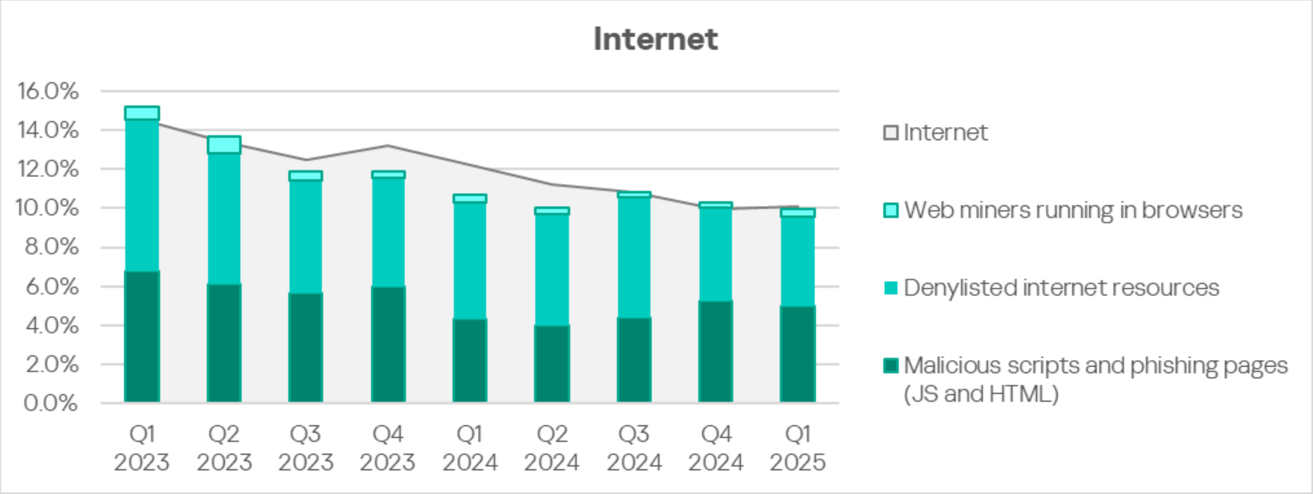
Detection and blocking of internet threats on ICS computers protected by Kaspersky products means that access to external services was allowed from these computers at the time of detection.

In Q1 2025, the percentage of ICS computers on which threats from the internet were blocked increased for the first time since Q4 2023.



Percentage of ICS computers on which threats from the internet were blocked, Q1 2022–Q1 2025

The main categories of threats from the internet blocked on ICS computers are denylisted internet resources, malicious scripts and phishing pages, and web miners.

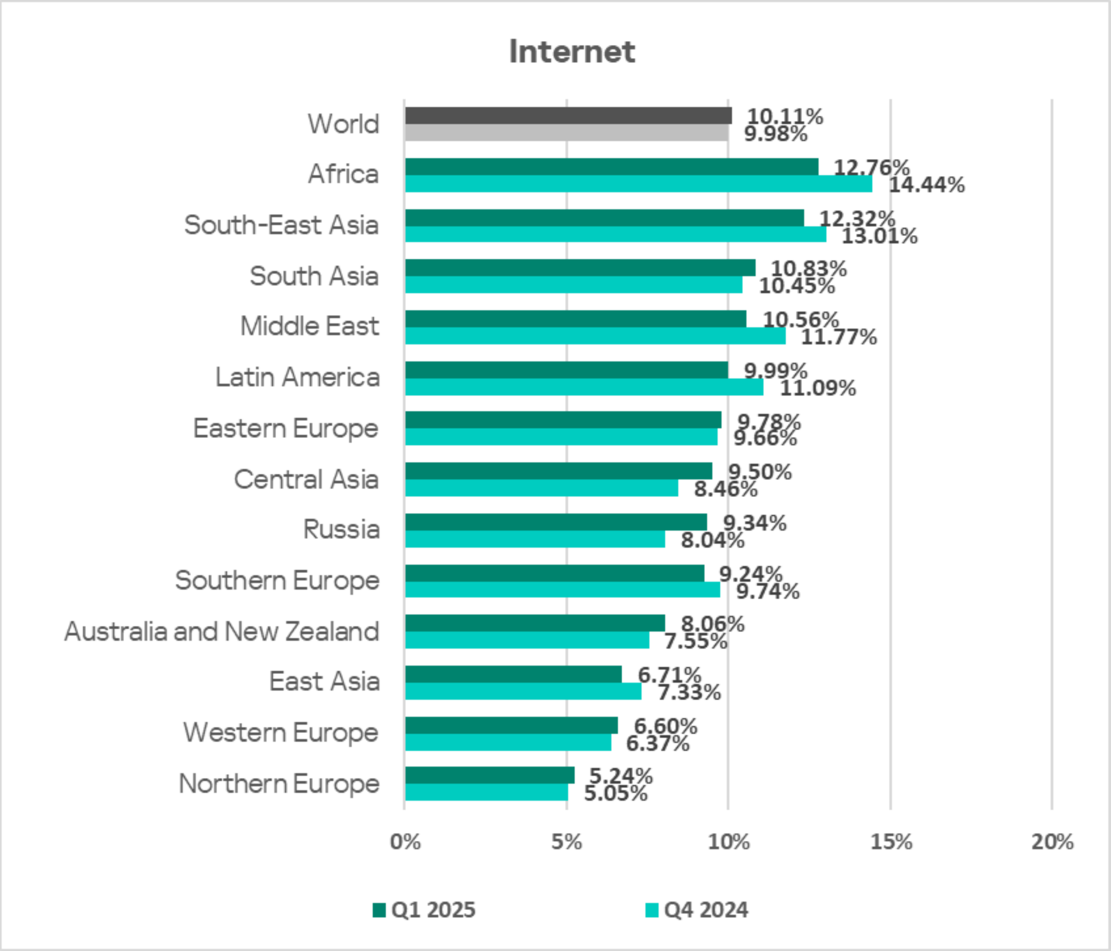


Percentage of ICS computers on which threats from the internet were blocked, Q1 2023–Q1 2025

The same computer can be attacked by several categories of malware from the same source during a quarter. That computer is counted when calculating the percentage of attacked computers for each threat category, but is only counted once for the threat source (we count unique attacked computers). In addition, it is not always possible to accurately determine the initial infection attempt. Therefore, the total percentage of ICS computers on which various categories of threats from a certain source were blocked exceeds the percentage of threats from the source itself.

The top three regions by percentage of ICS computers on which threats from the internet were blocked were Africa, South-East Asia, and South Asia.

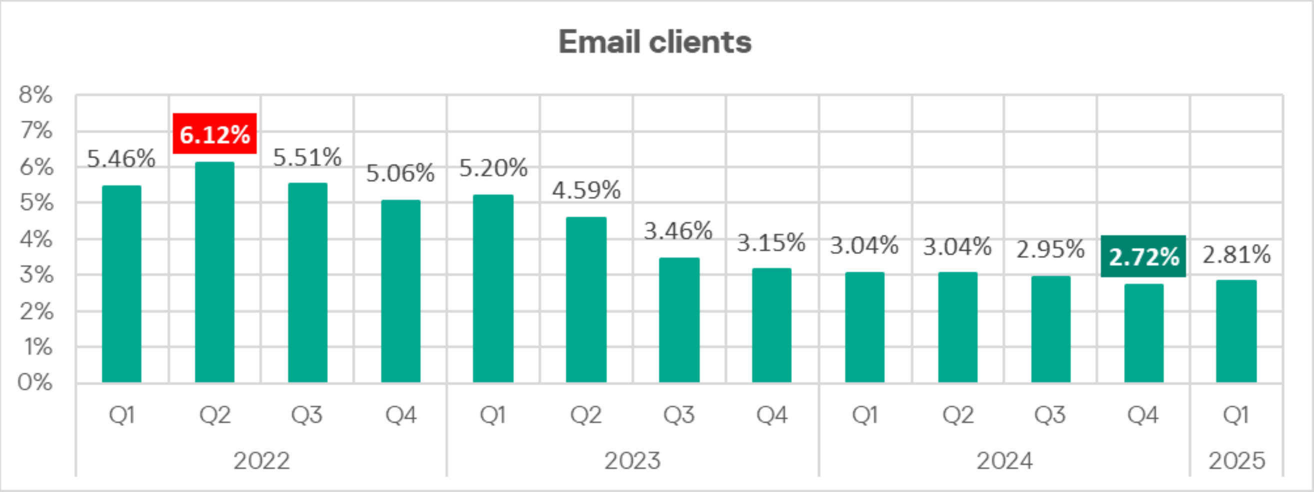
Regions ranked by percentage of ICS computers on which threats from the internet were blocked, Q1 2025



Email clients

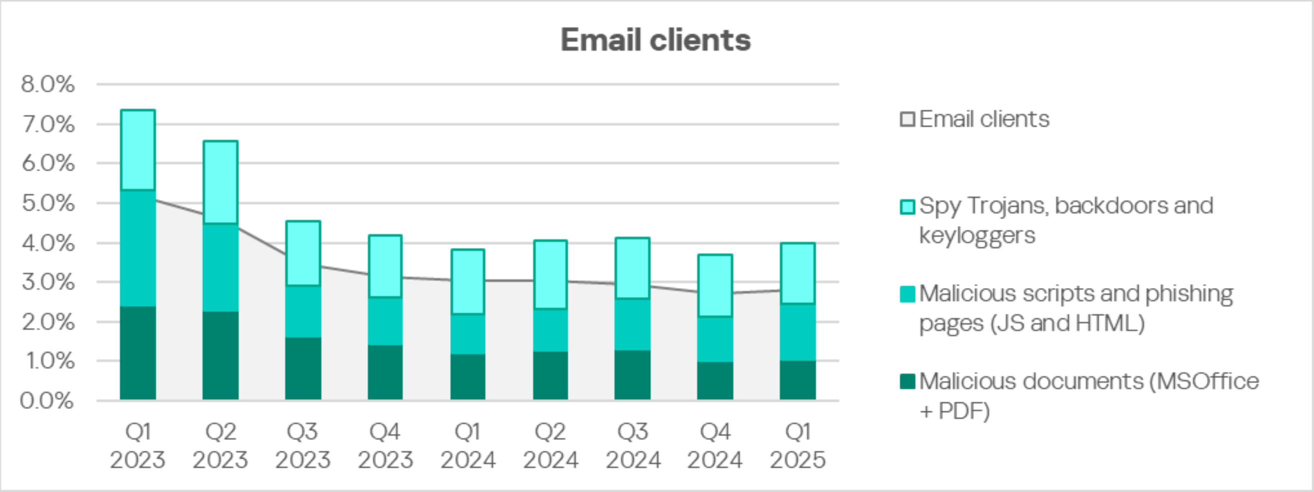
Some detected and blocked threats are delivered to protected computers by the mail delivery system and/or attempt to gain access through the email client application.

In Q1 2025, the percentage of ICS computers on which threats from email clients were blocked increased for the first time since the beginning of 2023.



Percentage of ICS computers on which threats from email clients were blocked, Q1 2022–Q1 2025

The main categories of threats from email clients blocked on ICS computers are malicious documents, spyware, malicious scripts and phishing pages.

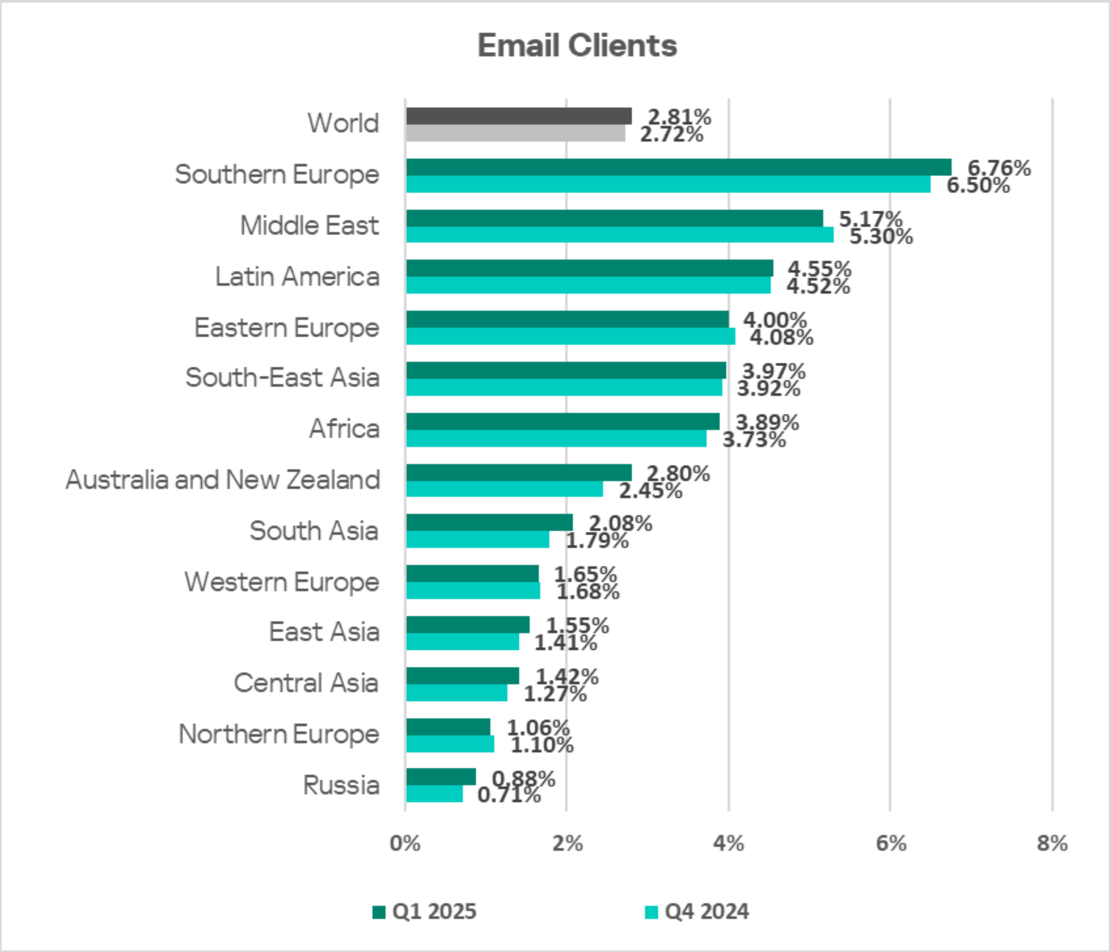


Percentage of ICS computers on which threats from email clients were blocked, Q1 2023–Q1 2025

To avoid detection, most of the spyware detected in phishing emails was delivered in the form of an archive or multilayered script, either as a separate file or embedded in office document formats.

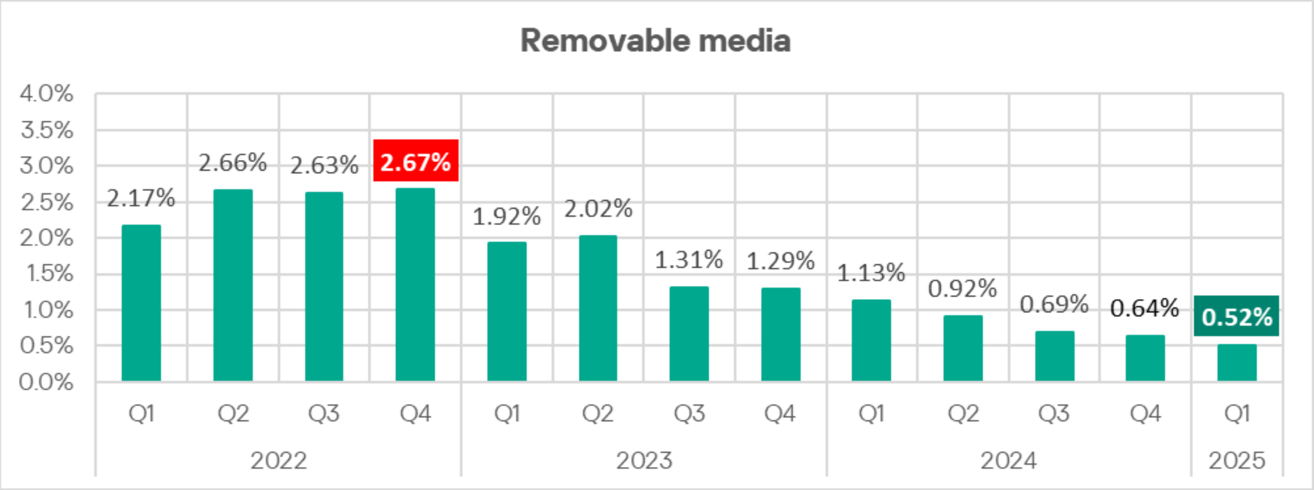
The top three regions by percentage of ICS computers on which threats from email clients were blocked were Southern Europe, the Middle East, and Latin America.

Regions ranked by percentage of ICS computers on which threats from email clients were blocked, Q1 2025



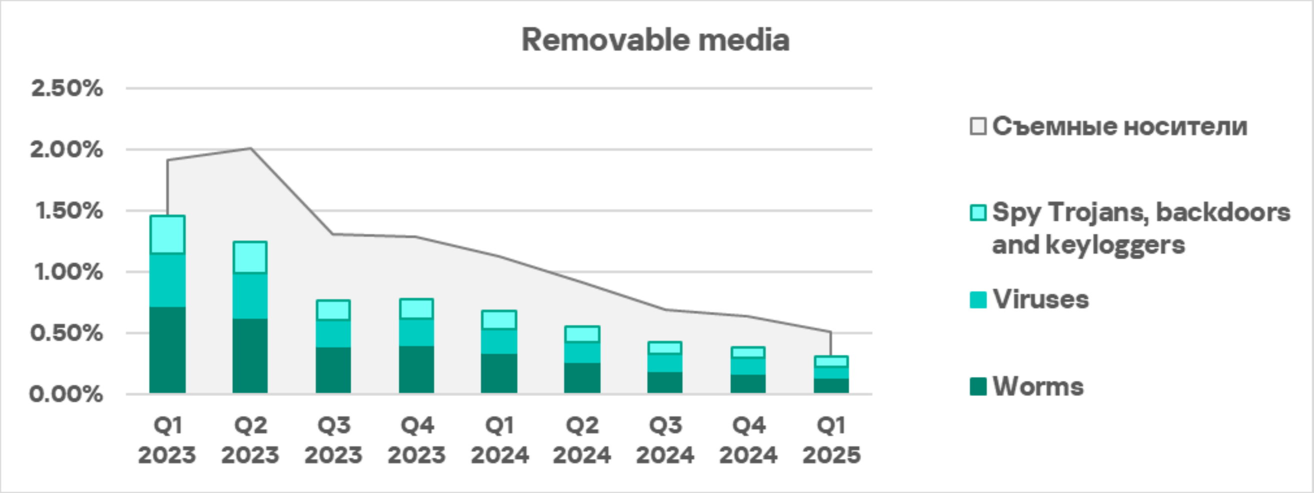
Removable media

In Q1 2025, the percentage of ICS computers on which threats from removable media were blocked continued to decrease and reached its lowest level since the beginning of 2023.



Percentage of ICS computers on which threats from removable media were blocked, Q1 2022–Q1 2025

The main categories of threats that are blocked when removable media is connected to ICS computers are worms, viruses, and spyware.



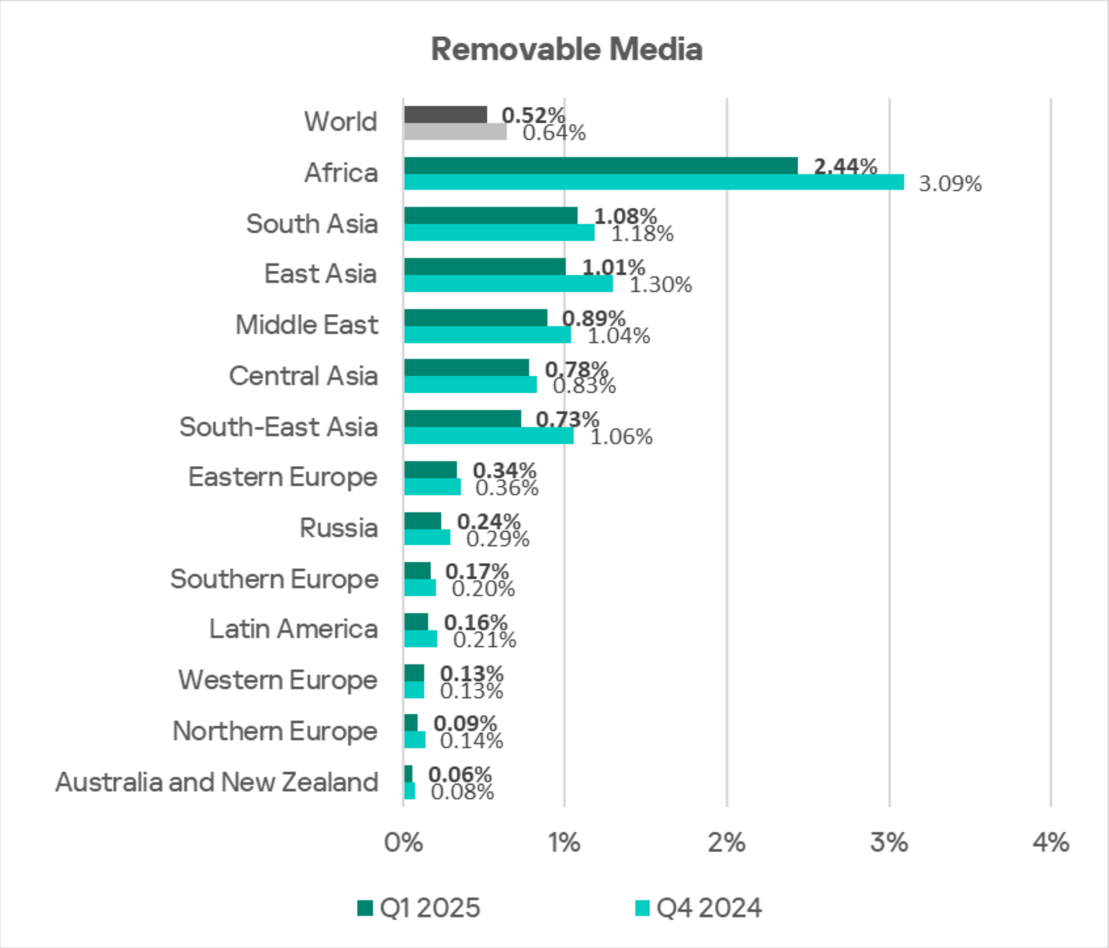
Percentage of ICS computers on which threats from removable media were blocked, Q1 2023–Q1 2025

Most of the worms and viruses detected on removable media are either variants of outdated polymorphic malware (appeared around 2010) or modern modular crypto miners. These modern crypto miners can spread over local networks by stealing credentials from infected hosts, exploiting known but unpatched vulnerabilities, and performing brute-force attacks on network services.

Most of the spyware detected on removable media consisted of universal components of both modern and outdated worms, such as stealers, loaders, and AV killers.

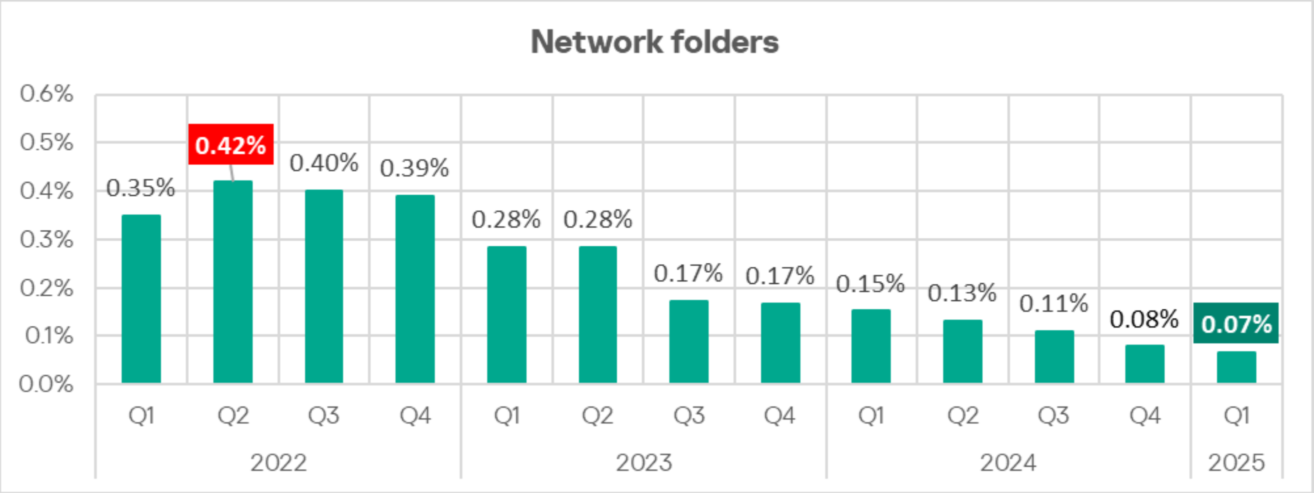
The top three regions by percentage of ICS computers on which threats from removable media were blocked were Africa, South Asia, and East Asia.

Regions ranked by percentage of ICS computers on which threats from removable media were blocked, Q1 2025

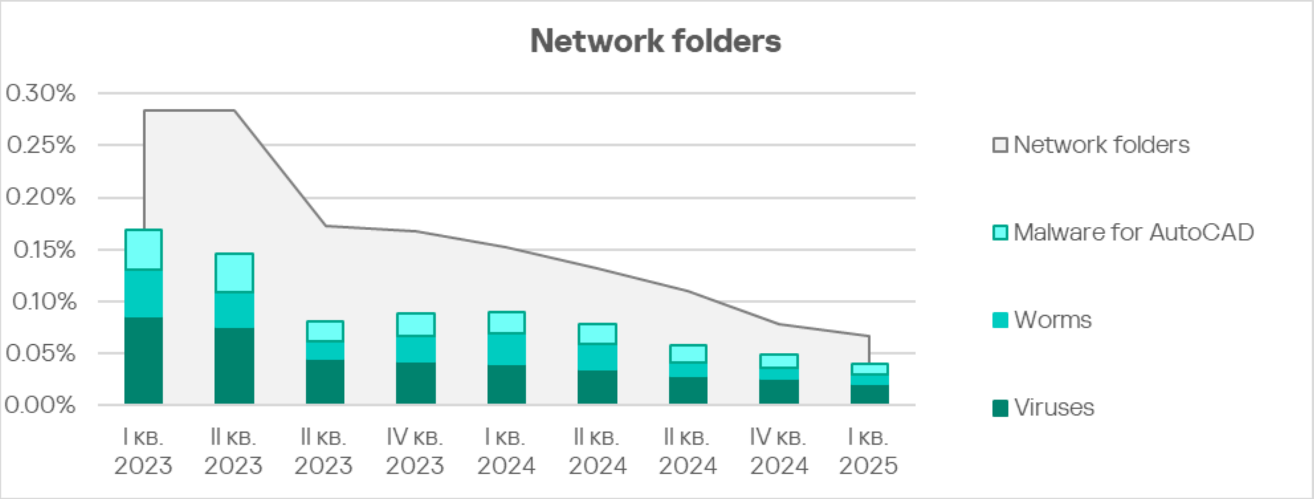


Network folders

In Q1 2025, the percentage of ICS computers on which threats from network folders were blocked reached its lowest level since early 2022. This is typically a low-level threat source, but do not underestimate it – worms, viruses and malware for AutoCAD spread via network folders.



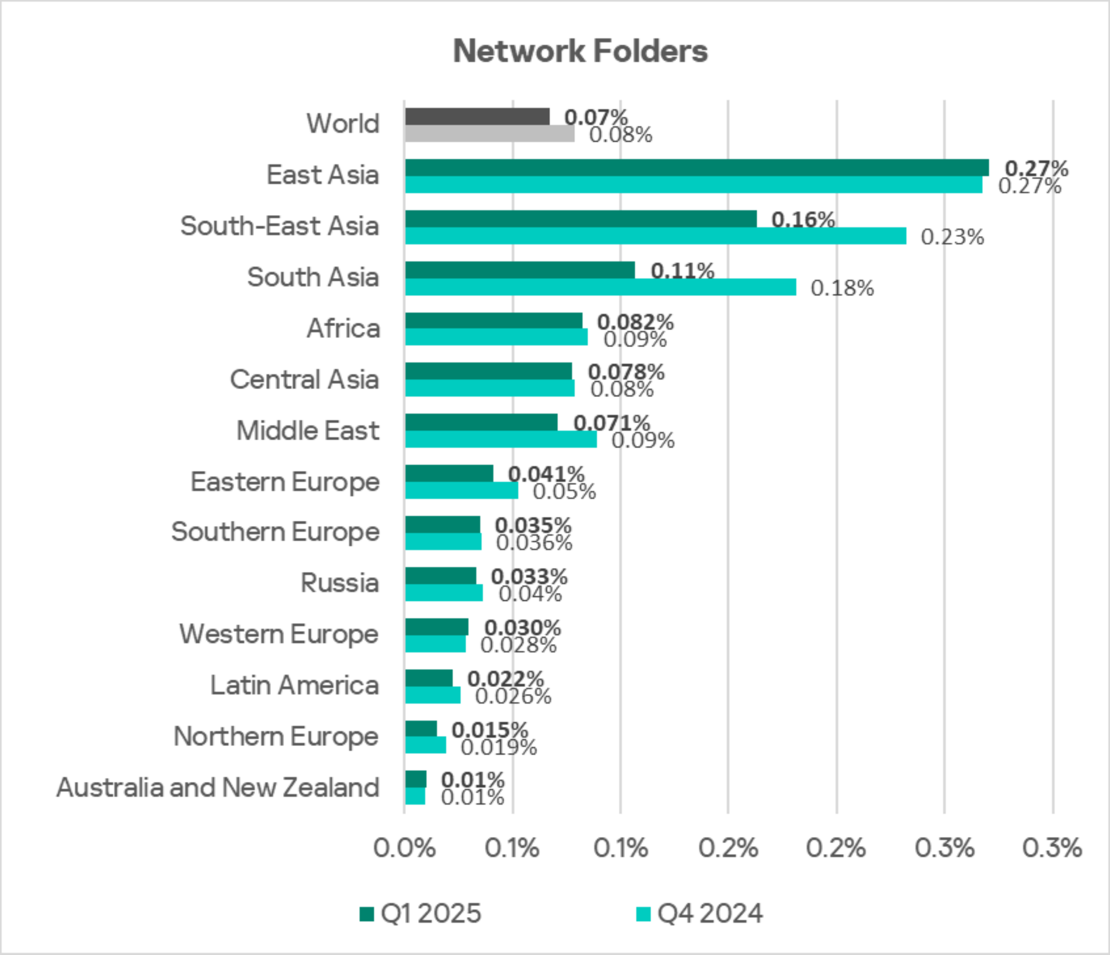
Percentage of ICS computers on which threats from network folders were blocked, Q1 2022–Q1 2025



Percentage of ICS computers on which threats from network folders were blocked, Q1 2023–Q1 2025

The top three regions by percentage of ICS computers on which threats from network folders were blocked were East Asia, South-East Asia, and South Asia.

Regions ranked by percentage of ICS computers on which threats from network folders were blocked, Q1 2025



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 KSN users who consented to its anonymous sharing and processing for the purposes 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*[1]*.*

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
- Building automation servers
- Data storage (Historian) servers
- Data gateways (OPC)
- Stationary workstations of engineers and operators
- Mobile workstations of engineers and operators
- Human machine interface (HMI)
- Computers used to manage technological and building automation networks
- Computers of ICS/PLC programmers

Computers that share statistics with us belong to organizations from various industries. The most common are the chemical industry, metallurgy, ICS design and integration, oil and gas, energy, transport and logistics, the food industry, light industry, pharmaceuticals. This also includes systems from engineering and integration firms that work with enterprises in a variety of industries, as well as building management systems, physical security, and biometric data processing.

We consider a computer as attacked if a Kaspersky security solution blocked one or more threats on that computer during the period under 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 under review to the total number of computers in the selection from which we received anonymized information during the same period.

[1] 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