Kaspersky ICS CERT

Threat landscape for industrial automation systems

Q2 2025

11.09.2025

Version 1.0

Q2 in numbers

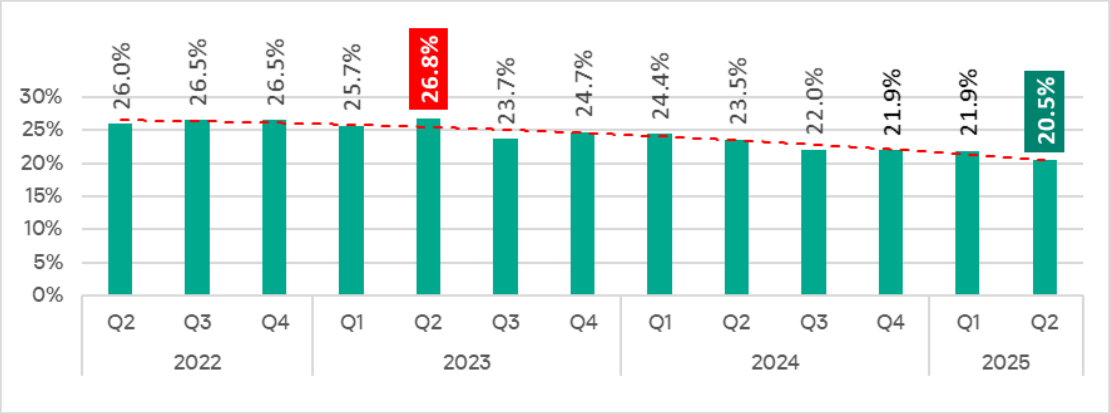
Parameter	Q1 2025	Q2 2025	Quarterly changes
Global percentage of attacked ICS computers	21.9%%	20.5%	▼1.4 pp
Percentage of ICS computers on which malicious objects from different categories were blocked			
Malicious scripts and phishing pages (JS and HTML)	7.16%	6.49%	▼0.67 pp
Denylisted internet resources	5.12%	5.91%	▲0.79 pp
Spy Trojans, backdoors and keyloggers	4.20%	3.84%	▼0.36 pp
Malicious documents (MSOffice + PDF)	1.85%	1.97%	▲0.12 pp
Viruses	1.53%	1.29%	▼0.24 pp
Worms	1.31%	1.22%	▼0.09 pp
Miners in the form of executable files for Windows	0.78%	0.63%	▼0.15 pp
Web miners running in browsers	0.53%	0.30%	▼0.23 pp
Malware for AutoCAD	0.34%	0.29%	▼0.05 pp
Ransomware	0.16%	0.14%	▼0.02 pp
Main threat sources			
Internet	10.11%	9.76%	▼0.35 pp
Email clients	2.81%	3.06%	▲0.25 pp
Removable media	0.52%	0.37%	▼0.15 pp
Network folders	0.07%	0.05%	▼0.02 pp

Statistics across all threats

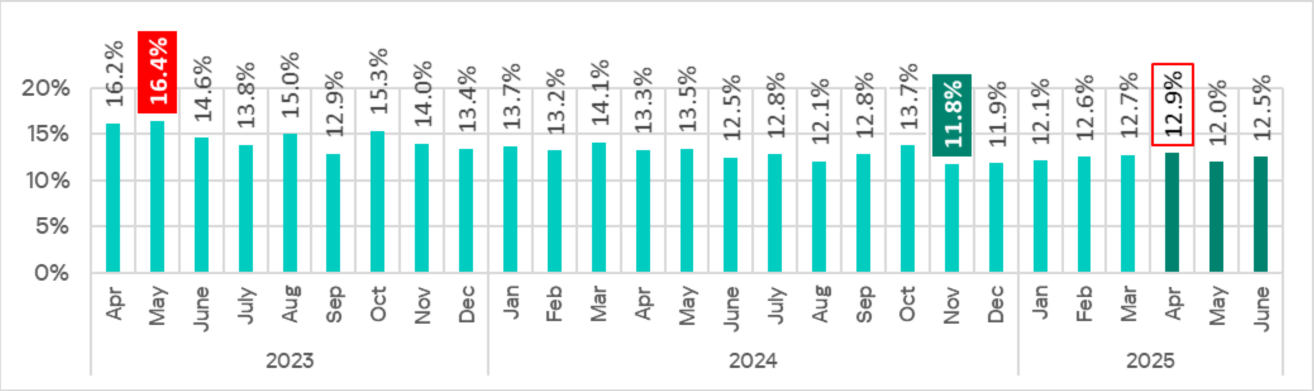
In Q2 2025, the percentage of ICS computers on which malicious objects were blocked decreased by 1.4 pp from the previous quarter to 20.5%.

Compared to Q2 2024, the rate decreased by 3.0 pp.

Percentage of ICS computers on which malicious objects were blocked, Q2 2022–Q2 2025



The highest percentage of ICS computers on which malicious objects were blocked during Q2 2025 occurred in April.

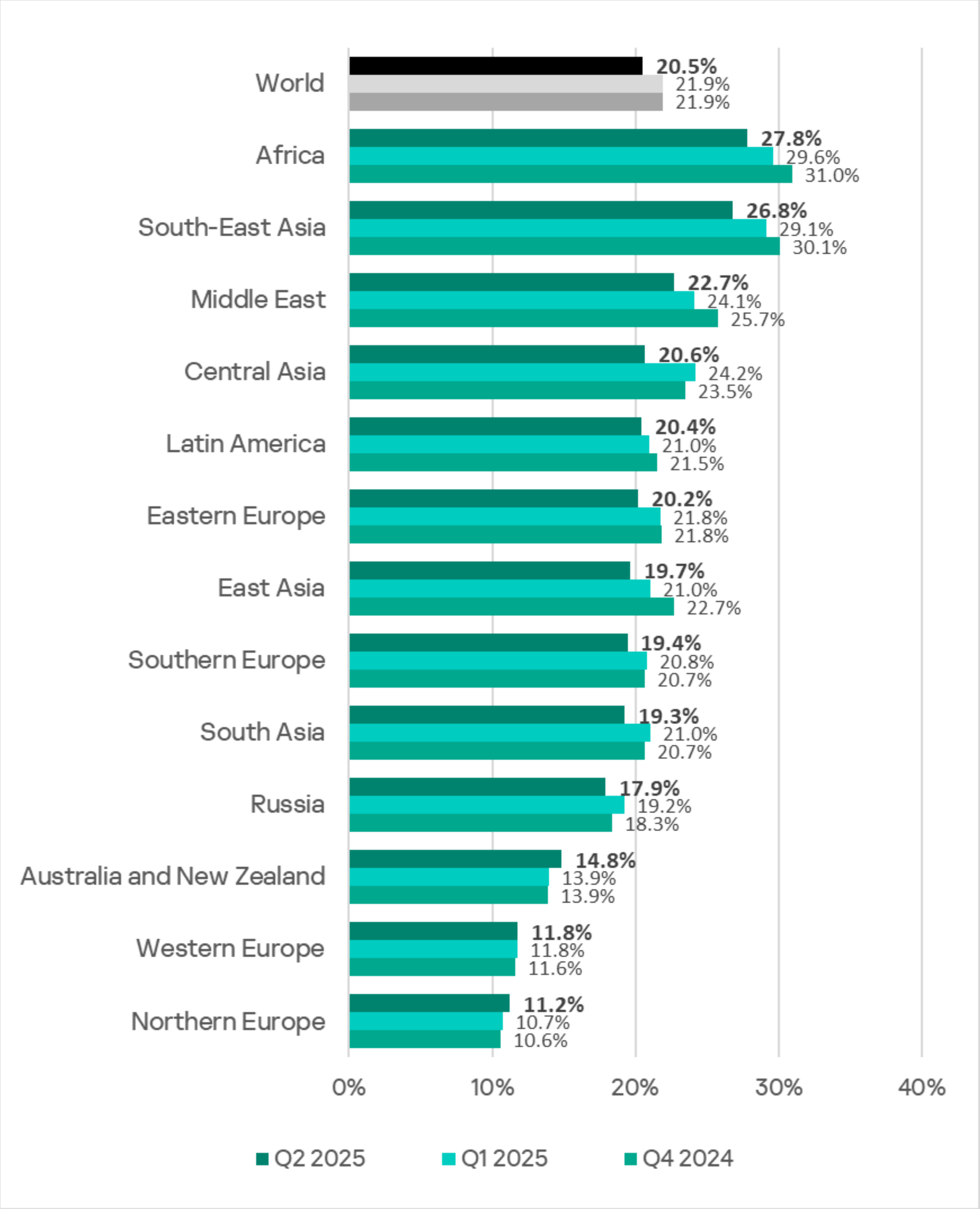


Percentage of ICS computers on which malicious objects were blocked, April 2023–June 2025

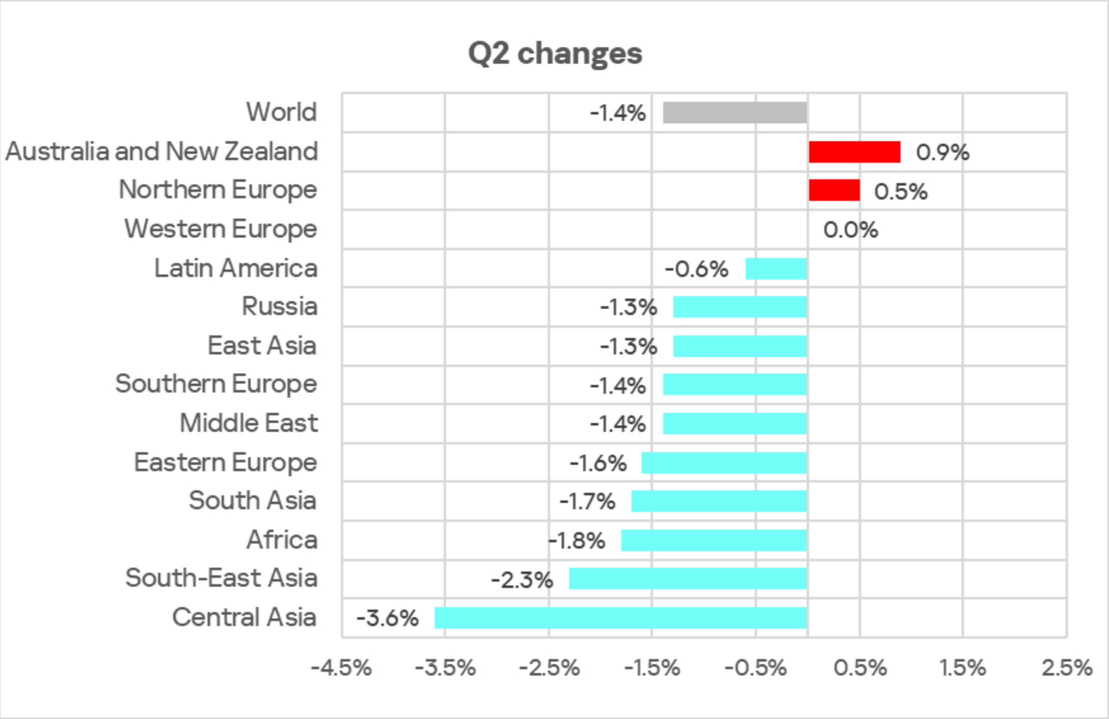
Regionally, the percentage of ICS computers on which malicious objects were blocked ranged from 11.2% in Northern Europe to 27.8% in Africa.

In most of the regions surveyed in this report, the figures decreased from the previous quarter. They increased only in Australia and New Zealand, as well as Northern Europe.

Regions ranked by percentage of ICS computers on which malicious objects were blocked, Q2 2025



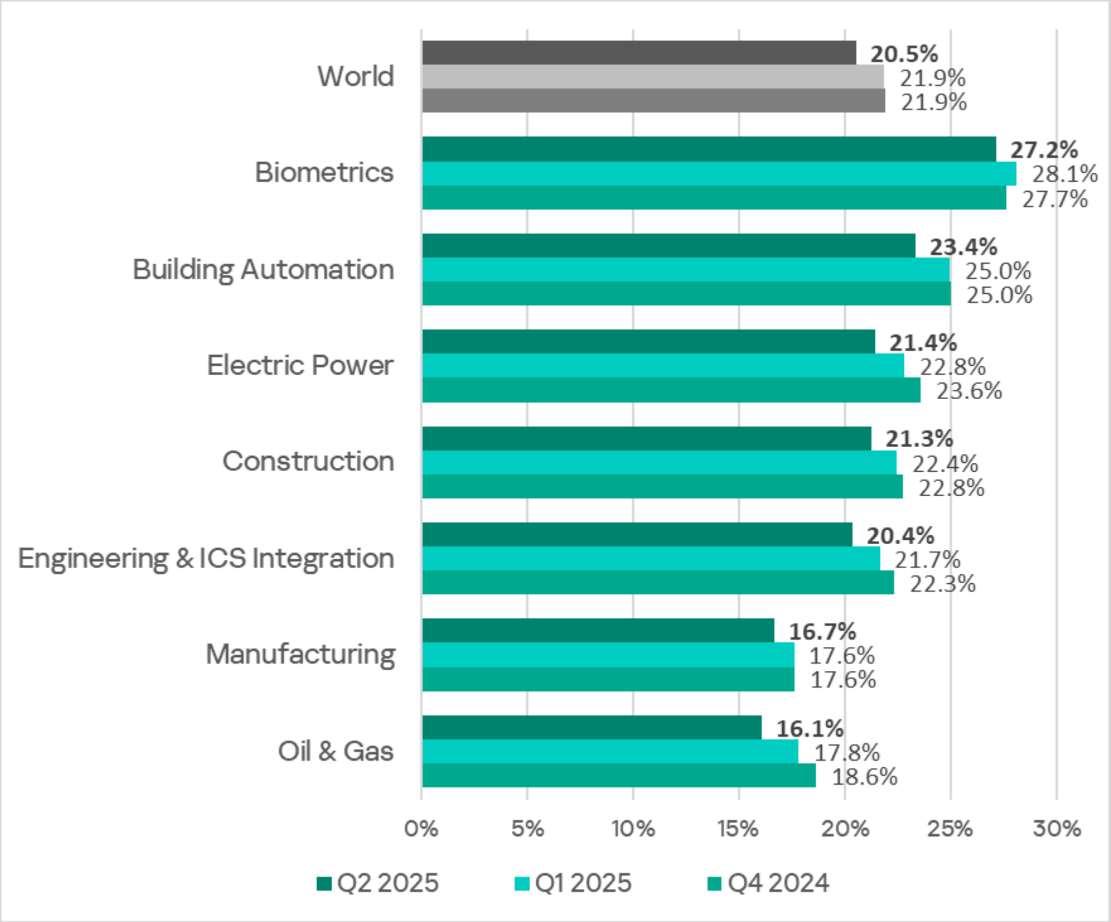
Changes in percentage of ICS computers on which malicious objects were blocked, Q2 2025



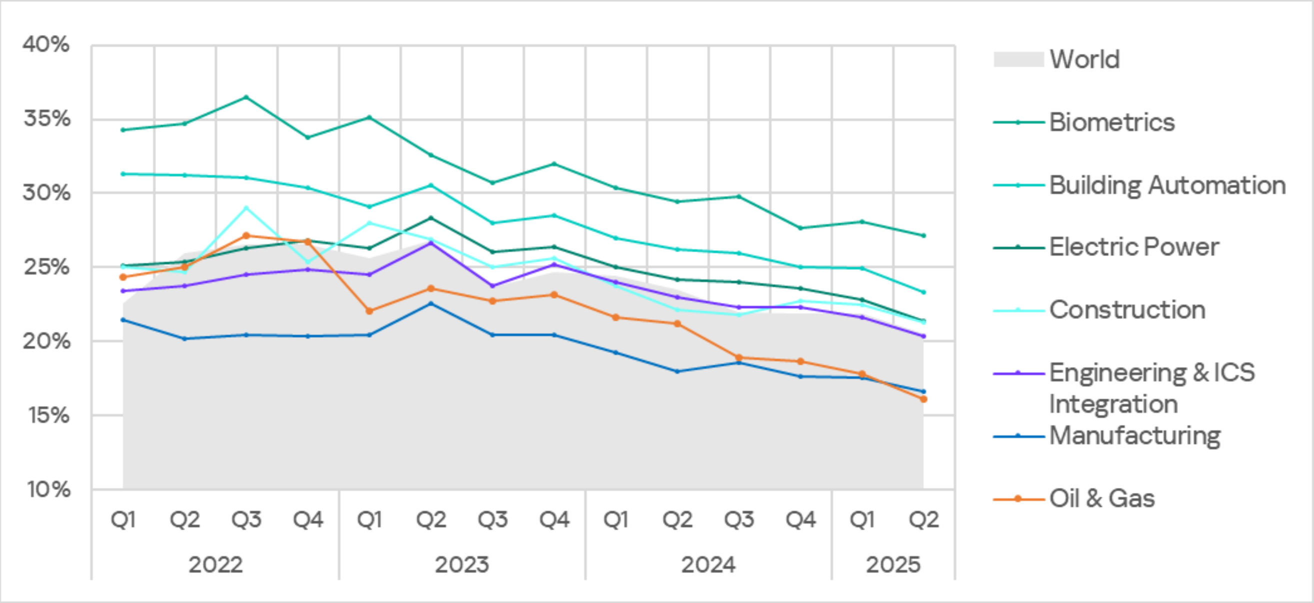
Selected industries

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 computers on which malicious objects were blocked, Q2 2025



In Q2 2025, the percentage of ICS computers on which malicious objects were blocked decreased across all industries.



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.

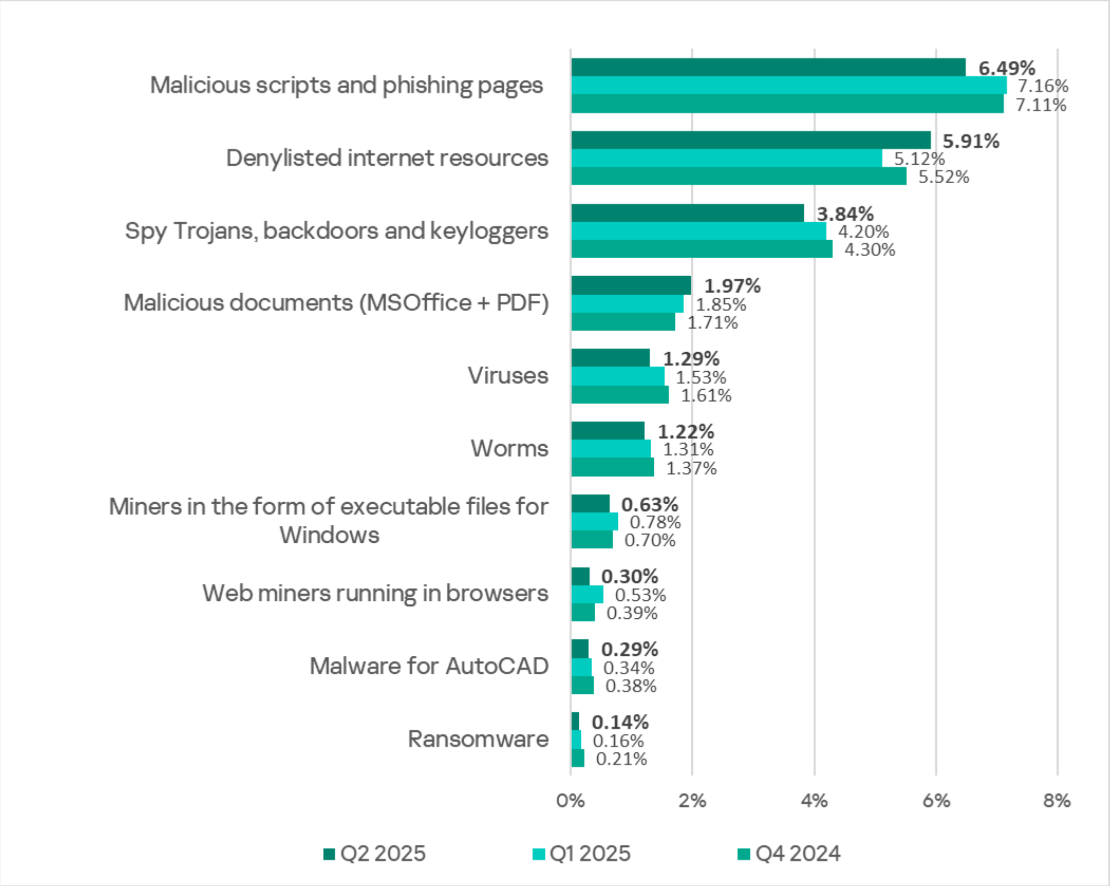
1. Malicious objects used for initial infection.
   This category includes predominantly denylisted internet resources, malicious scripts and phishing pages, and malicious documents.
2. Next-stage malware.
   Spyware, ransomware, miners in the form of executable files for Windows, and web miners are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

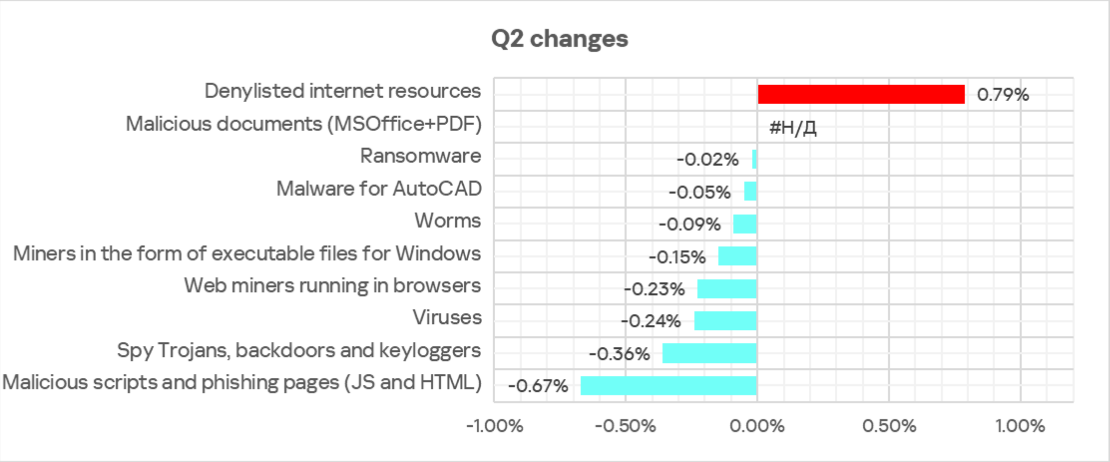
Malicious objects categorized as initial infection threats typically rank highest among threat categories in terms of the percentage of ICS computers on which threats were blocked. This is reflected in our statistics: globally and in almost all regions, malicious scripts and phishing pages, as well as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

It should be noted that in a small percentage of cases, the threat categories that we classify as malicious objects used for initial infection, such as malicious links, can be used in subsequent stages of an attack. For example, a link to a malicious resource may be detected while scanning the computer registry. It obviously appeared there as a result of activity by another malicious program before it was identified and blocked. A stricter segmentation of the attacked ICS computers into categories based on the malware blocked and the sources of its entry is described in the article "Dynamics of external and internal threats to industrial control systems". This article opens a new cycle of publications presenting the results of deeper research on the ICS threat landscape based on statistics of the activation of our products' protective components.

Percentage of ICS computers 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, Q2 2025



In Q2 2025, the only increases were in the percentages of ICS computers on which denylisted internet resources (1.2 times more than in the previous quarter) and malicious documents (1.1 times more) were blocked.

Threat categories

In Q2 2025, Kaspersky protection solutions blocked malware from 10,408 different malware families of various categories on industrial automation systems.

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.

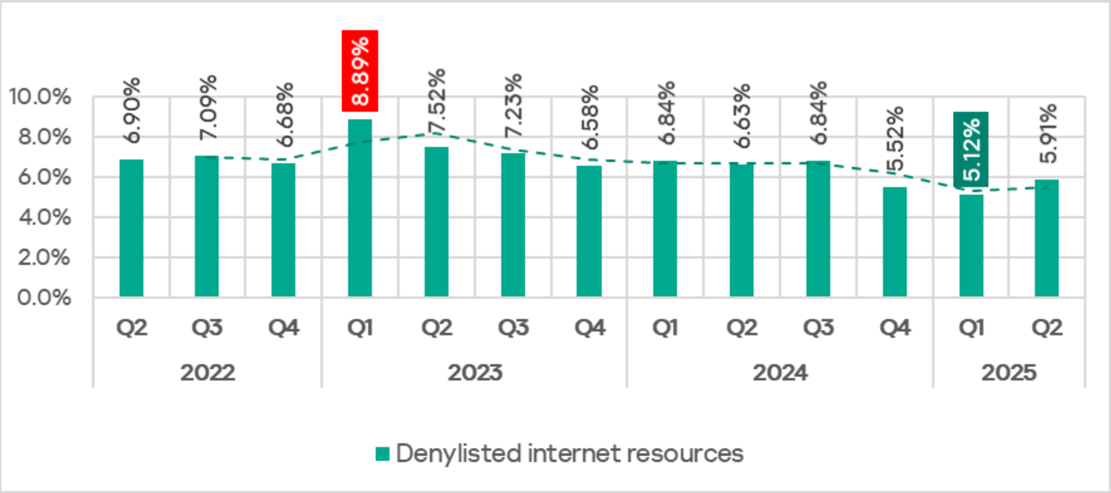
A detected malicious web resource may not always be added to a denylist because attackers are increasingly using legitimate internet resources and services such as content delivery network (CDN) platforms, messengers, and cloud storage. These services allow malicious code to be distributed through unique 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.

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).

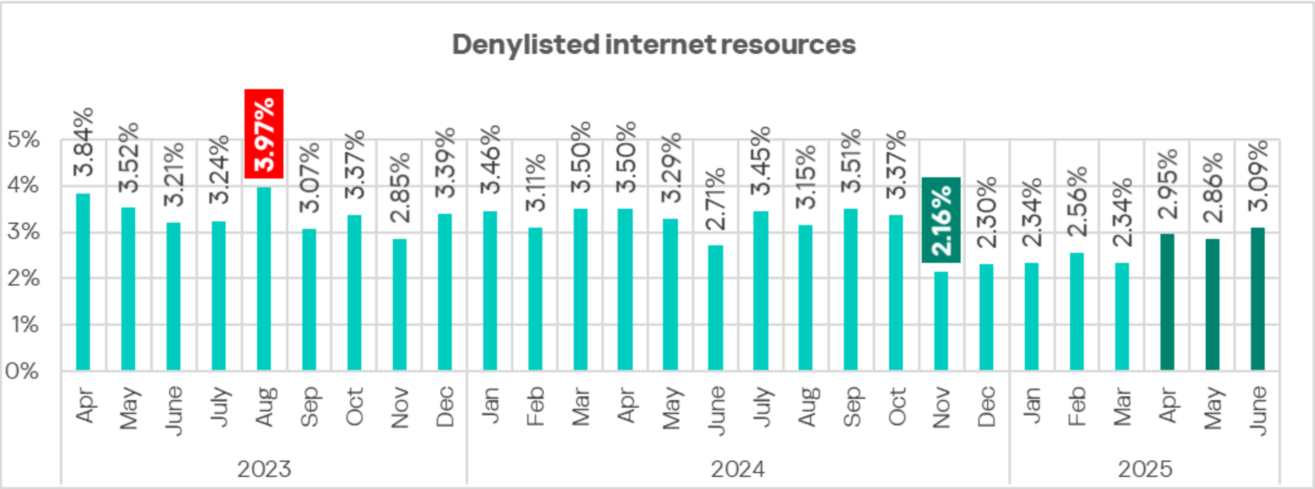
High parameter values usually indicate weak control over the implementation of information security policies (ICS computers have access to the internet in one way or another), phishing protection weaknesses (many malicious links are delivered via phishing messages) and deficiencies in information security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

In Q2 2025, the percentage of ICS computers on which denylisted internet resources were blocked increased to 5.91%.



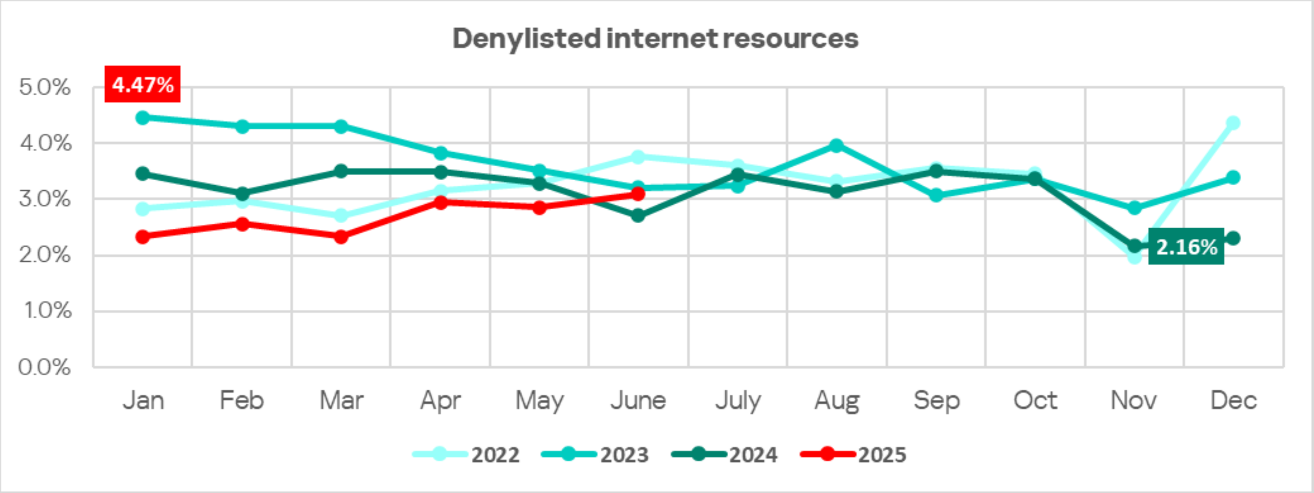
Percentage of ICS computers on which denylisted internet resources were blocked, Q2 2022–Q2 2025

The chart below shows the monthly percentage rates since April 2023.



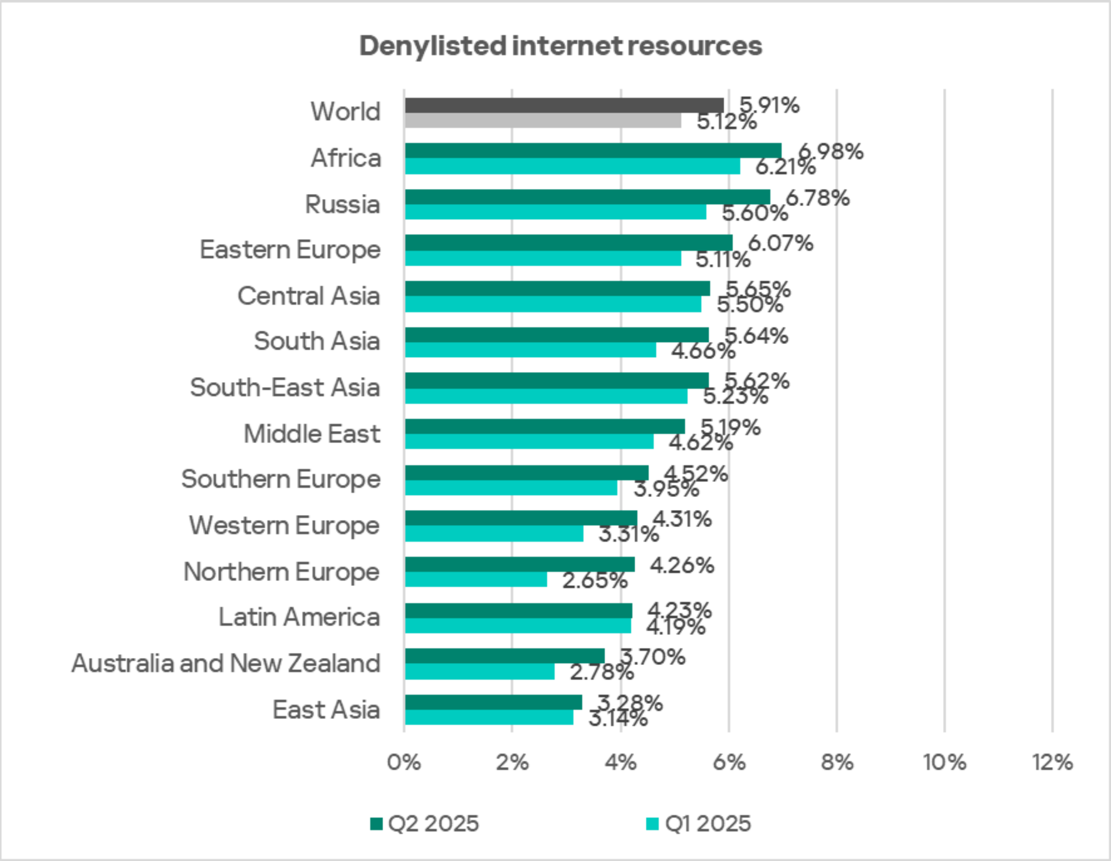
Percentage of ICS computers on which denylisted internet resources were blocked, April 2023–June 2025

In the first half of 2025, there was an upward trend in the percentage of ICS computers on which denylisted internet resources were blocked over the course of a month. This came after the indicator had reached its lowest value over the specified period in November 2024.



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

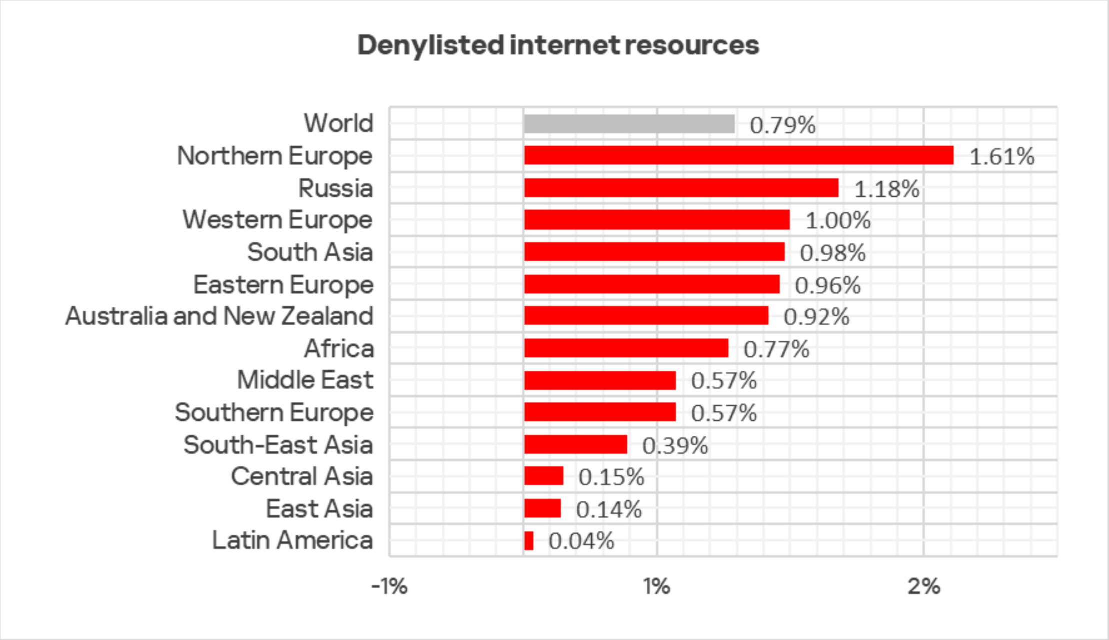
The percentage of ICS computers on which denylisted internet resources were blocked ranged from 3.28% in East Asia to 6.98% in Africa. Russia and Eastern Europe were also among the top three regions for this indicator.



Regions ranked by percentage of ICS computers on which denylisted internet resources were blocked, Q2 2025

After a decline in the previous quarter, the indicator increased in all regions in Q2 2025. This growth in all regions is associated with the addition of direct links to malicious code hosted on popular public websites and file services.

Changes in percentage of ICS computers on which denylisted internet resources were blocked, Q2 2025

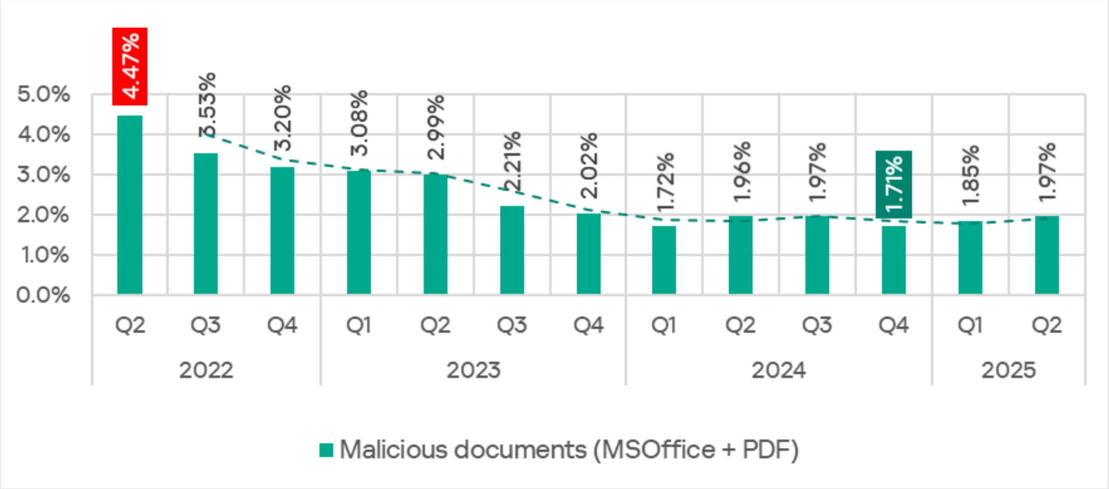


Malicious documents (MSOffice + PDF)

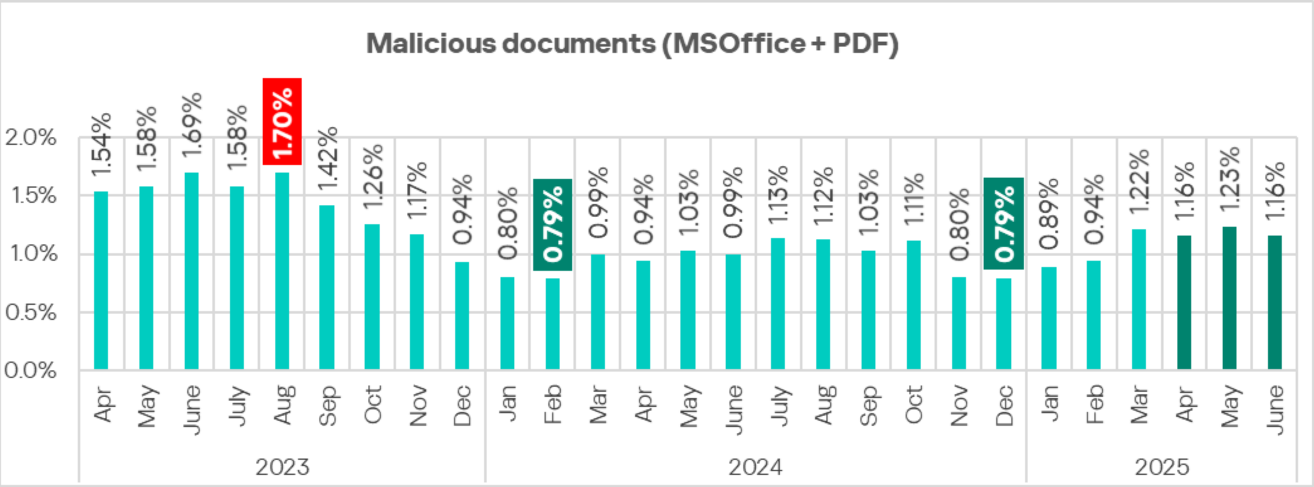
Attackers mainly send malicious documents attached to phishing messages and use them in attacks aimed at initial infection of computers. Malicious documents typically contain exploits, malicious macros, and malware links.

Following a decline at the end of 2024, the percentage of ICS computers on which malicious documents were blocked has grown for two consecutive quarters, returning to the level seen in Q3 2024.

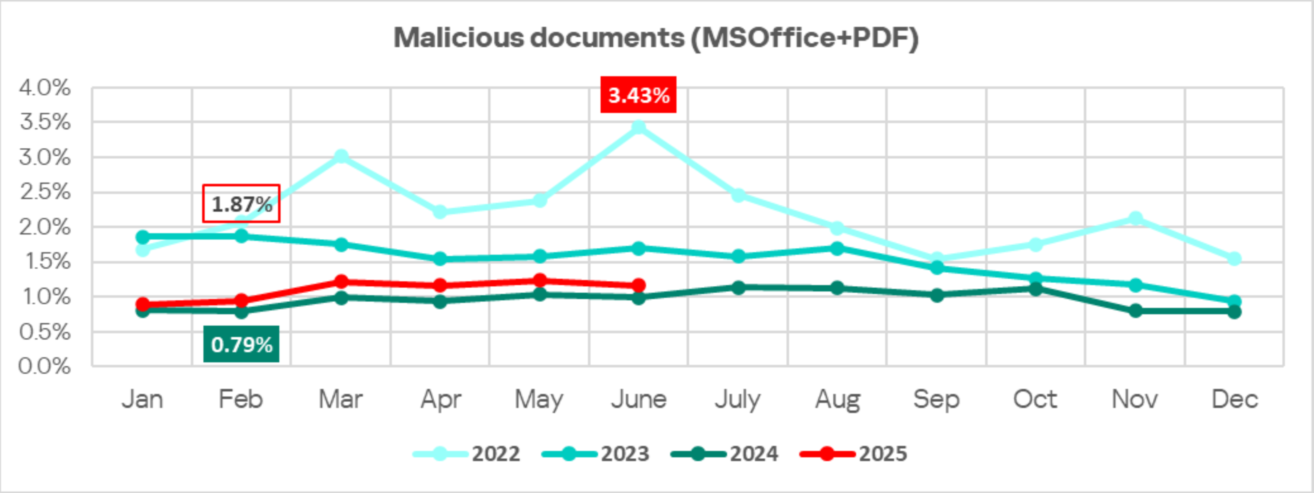
Percentage of ICS computers on which malicious documents were blocked, Q2 2022–Q2 2025



The monthly value of this indicator in April–June 2025 was higher than for the same period of 2024.



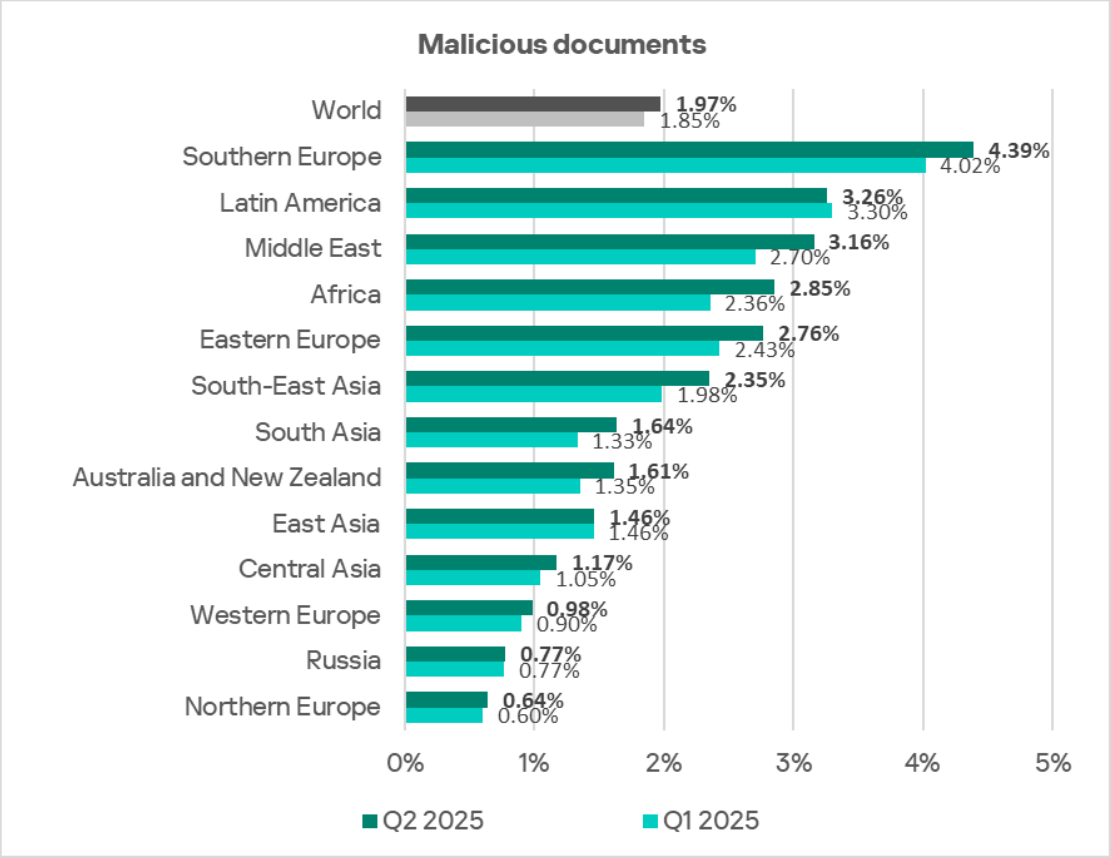
Percentage of ICS computers on which malicious documents were blocked, April 2023–June 2025



Percentage of ICS computers on which malicious documents were blocked, January 2022–June 2025

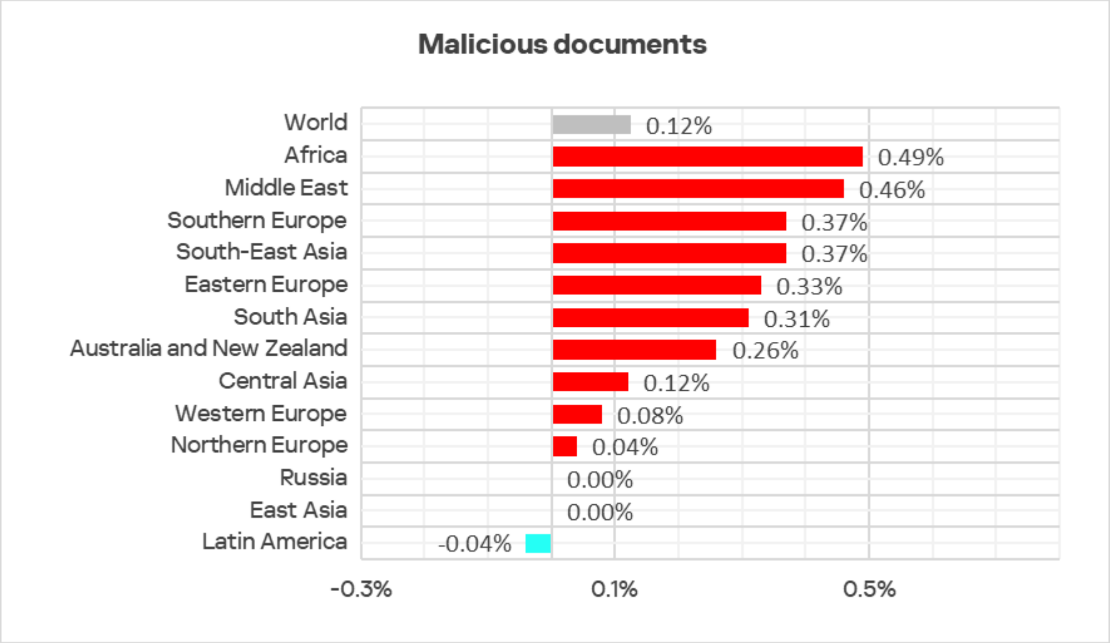
Regionally, the percentage of ICS computers on which malicious documents were blocked ranged from 0.64% in Northern Europe to 4.39% in Southern Europe. Southern Europe, Latin America, and the Middle East remained the top three regions for this indicator.

Regions ranked by percentage of ICS computers on which malicious documents were blocked, Q2 2025



In Q2 2025, the percentage increased in all regions except Latin America.

Changes in percentage of ICS computers on which malicious documents were blocked, Q2 2025

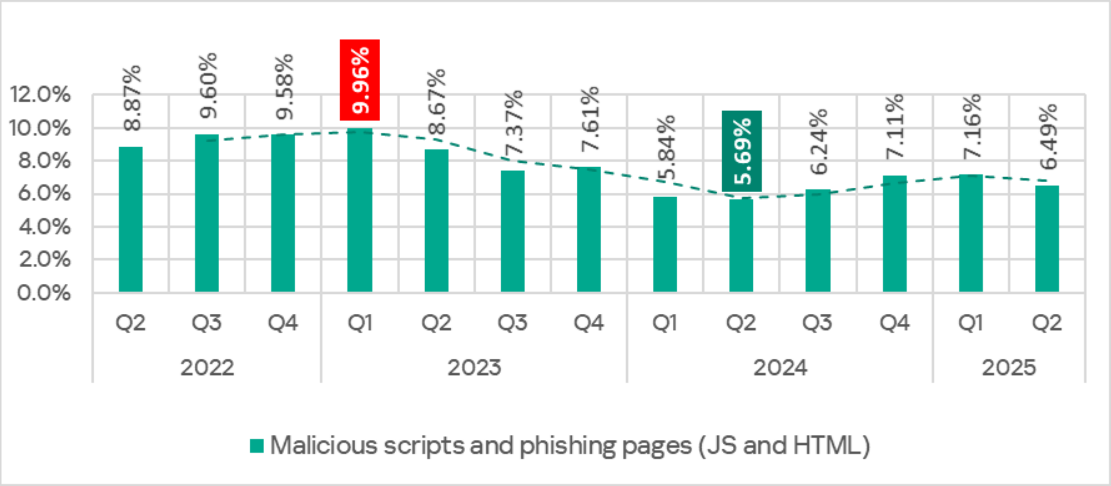


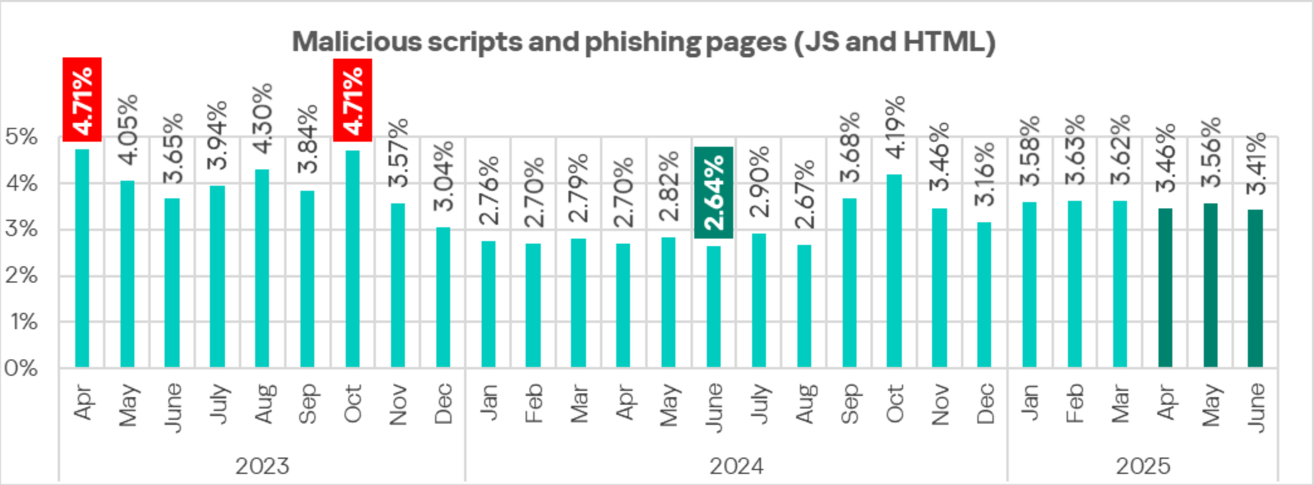
Malicious scripts and phishing pages (JS and HTML)

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 Q2 2025, the percentage of ICS computers on which malicious scripts and phishing pages were blocked decreased.

Percentage of ICS computers on which malicious scripts and phishing pages were blocked, Q2 2022–Q2 2025

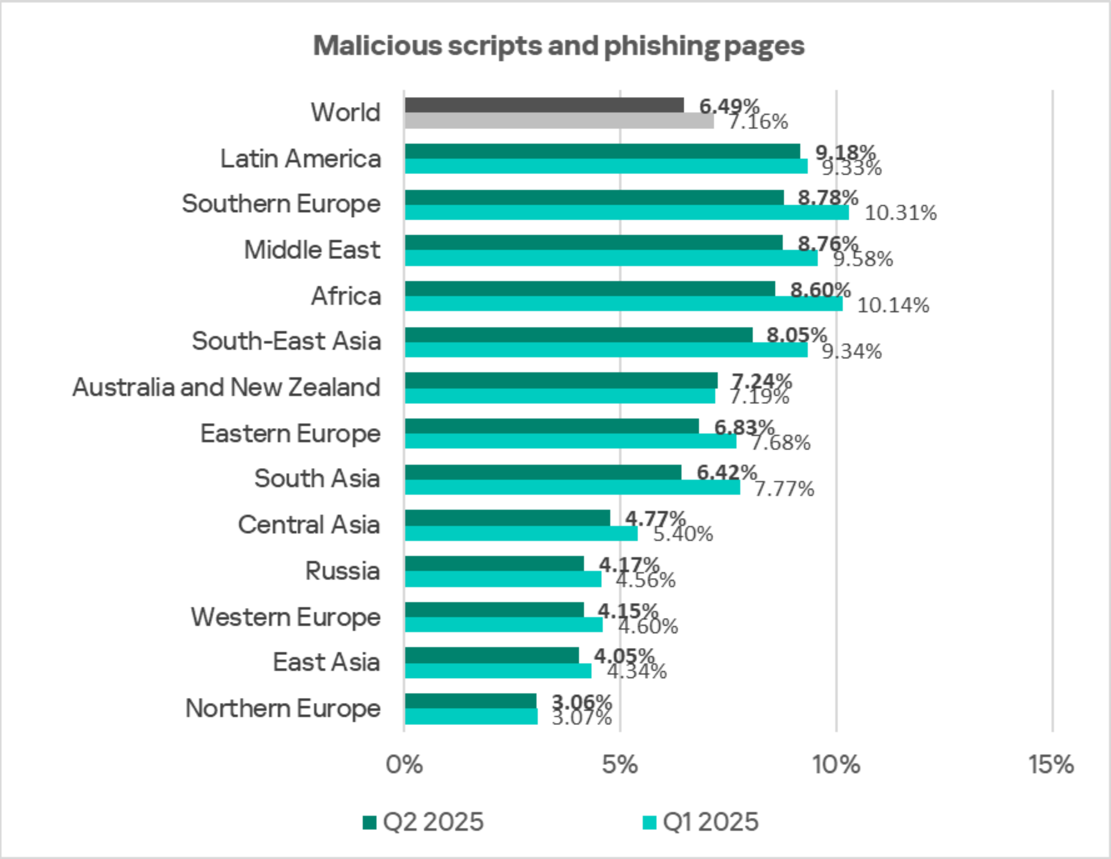




Percentage of ICS computers on which malicious scripts and phishing pages were blocked, April 2023–June 2025

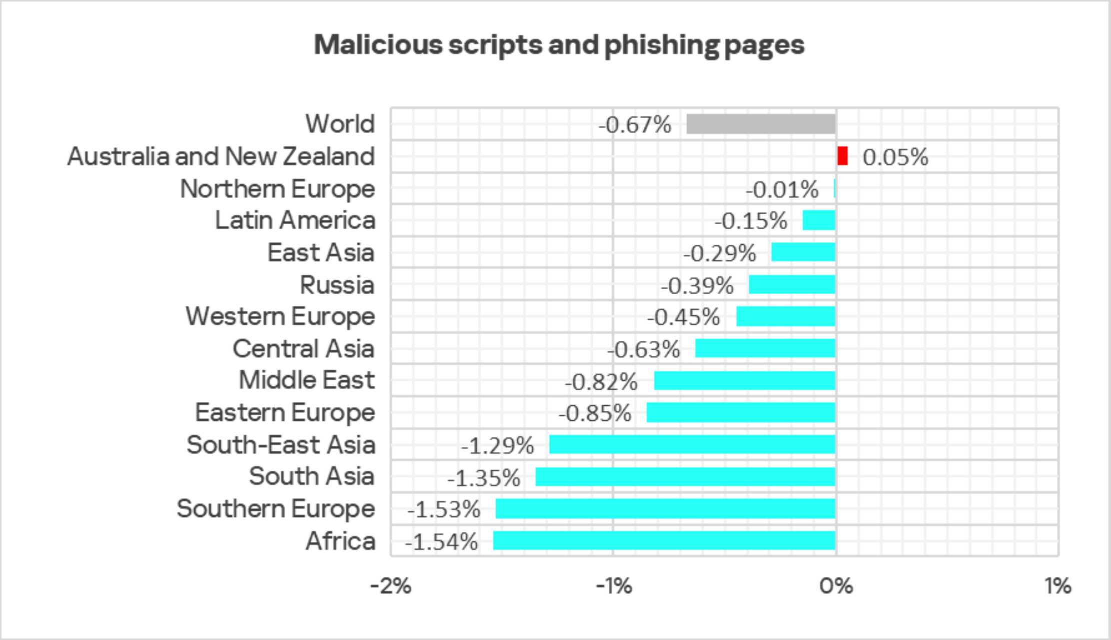
Regionally, the percentage of ICS computers on which malicious scripts and phishing pages were blocked ranged from 3.06% in Northern Europe to 9.18% in Latin America. The top three regions for this indicator were Latin America, Southern Europe, and the Middle East.

Regions ranked by percentage of ICS computers on which malicious scripts and phishing pages were blocked, Q2 2025



In Q2 2025, the percentage decreased in all regions except Australia and New Zealand.

Changes in percentage of ICS computers on which malicious scripts and phishing pages were blocked, Q2 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

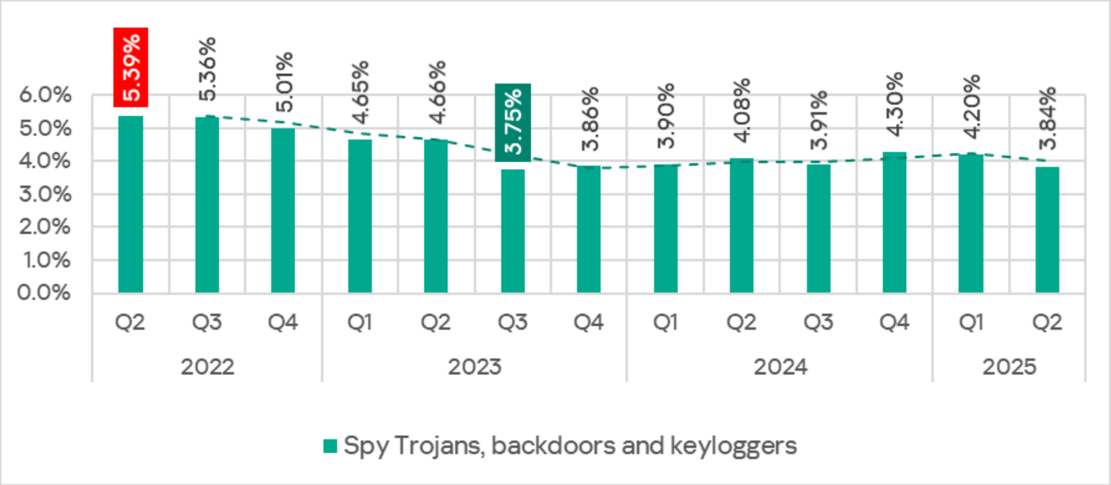
Spyware (spy Trojans, backdoors, and keyloggers) can be found in lots of phishing emails sent to industrial organizations. Spyware is the most frequently detected next-stage malware. It is used as a tool for the intermediate stages of a cyberattack (for example, intelligence and distribution over the 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.

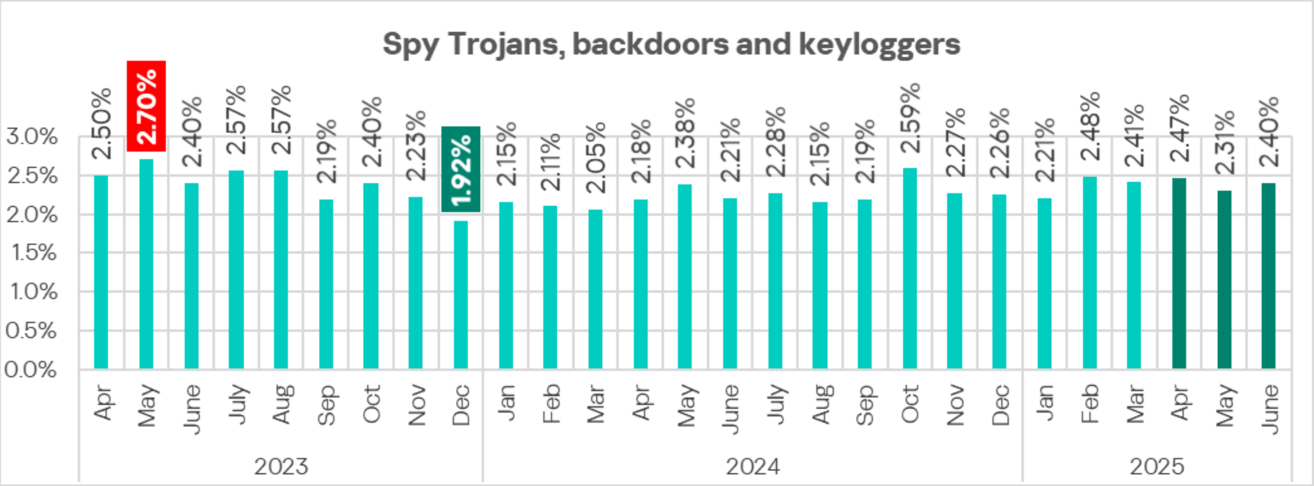
Detection of spyware on an ICS computer usually indicates that the initial infection vector has worked, whether it is clicking on a malicious link, opening an attachment from a phishing email, or connecting an infected USB drive. This indicates the absence or ineffectiveness of measures to protect the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

In Q2 2025, the percentage of ICS computers on which spyware was blocked decreased.

Percentage of ICS computers on which spyware was blocked, Q2 2022–Q2 2025



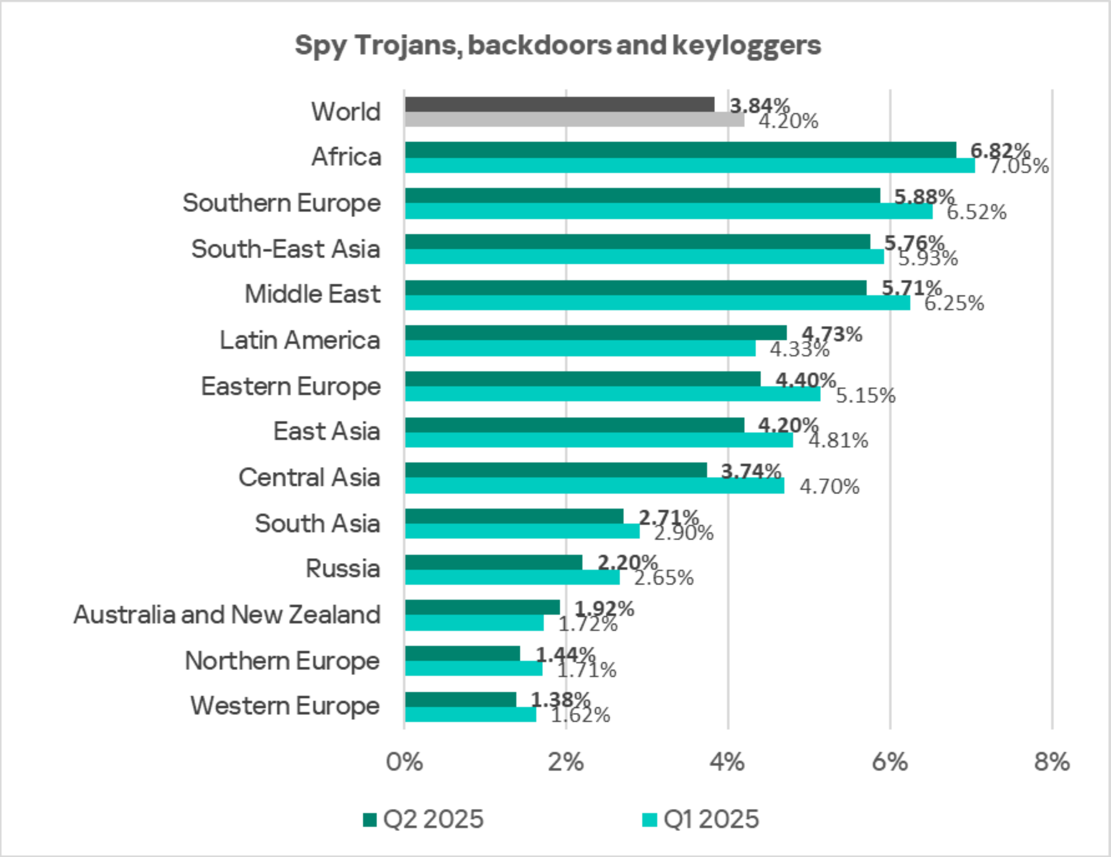
The highest monthly value for Q2 2025 was in April.



Percentage of ICS computers on which spyware was blocked, April 2023–June 2025

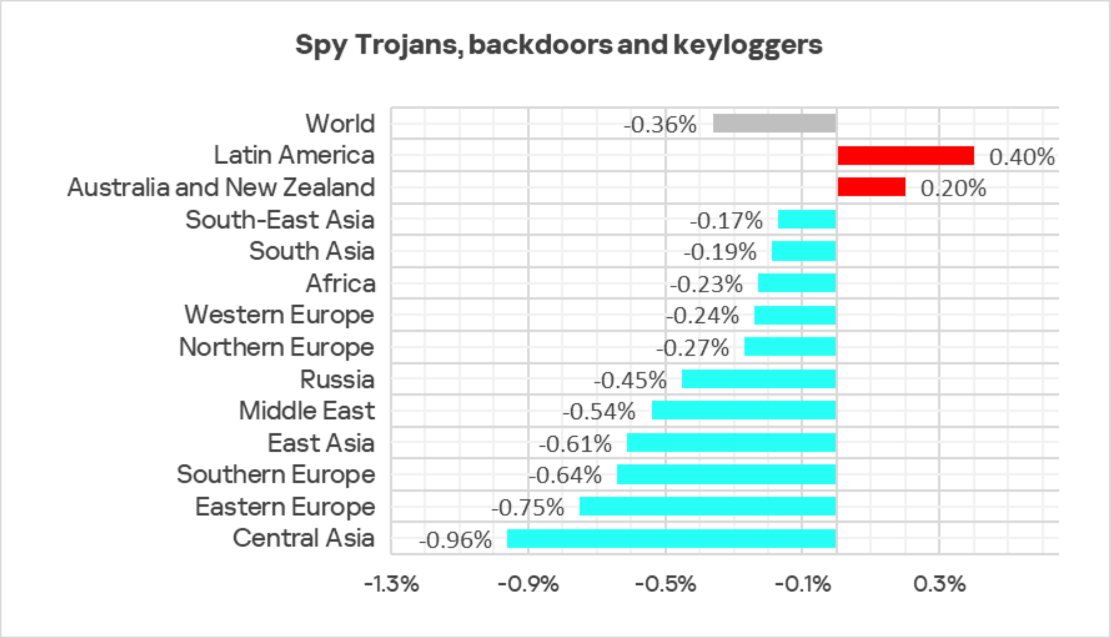
Regionally, the percentage of ICS computers on which spyware was blocked ranged from 1.38% in Western Europe to 6.82% in Africa. The top three regions for this indicator were Africa, Southern Europe, and South-East Asia.

Regions ranked by percentage of ICS computers on which spyware was blocked, Q2 2025



During the quarter, the percentage of ICS computers on which spyware was blocked increased in Latin America, and Australia and New Zealand.

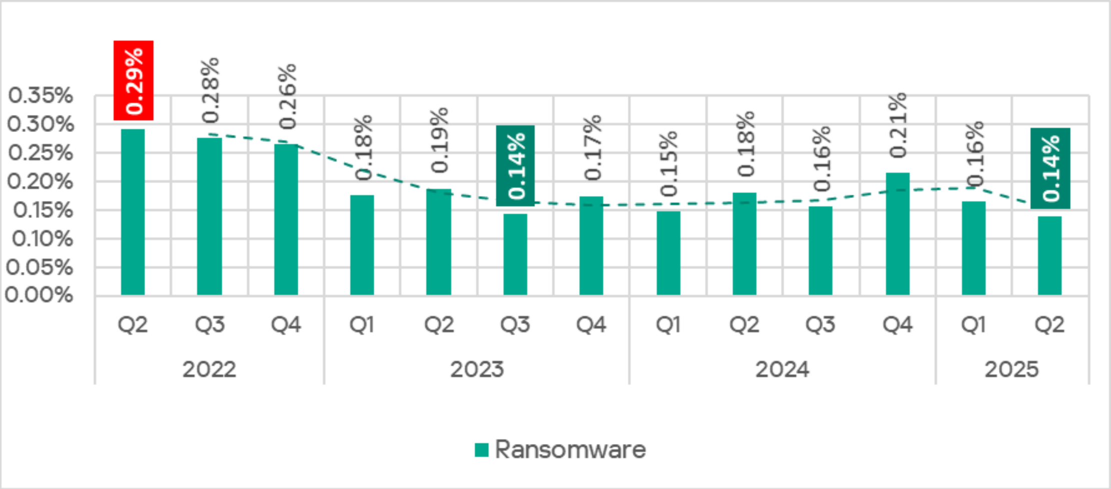
Changes in percentage of ICS computers on which spyware was blocked, Q2 2025



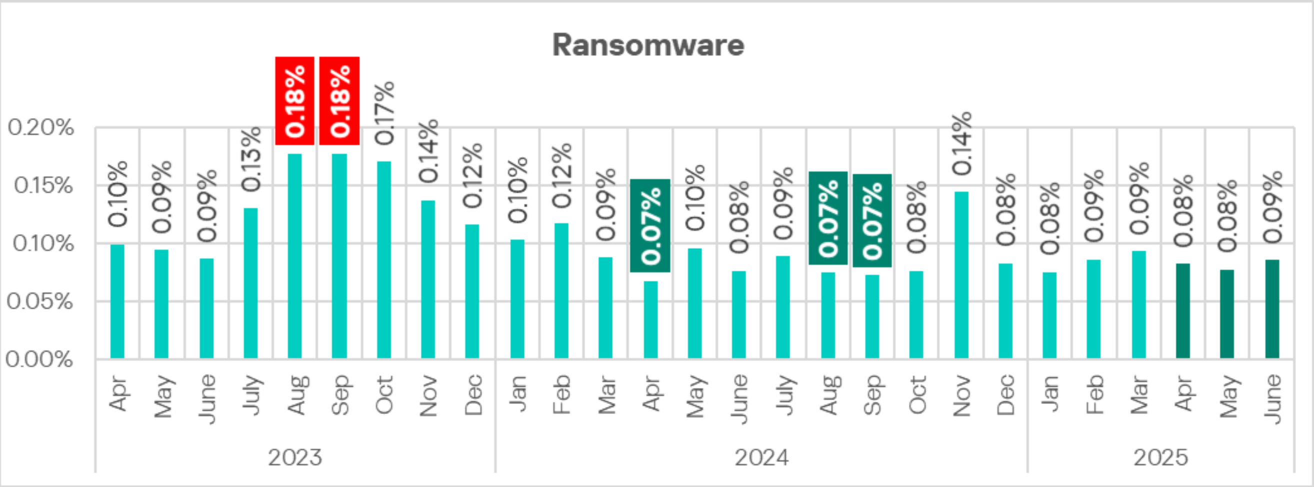
Ransomware

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

Percentage of ICS computers on which ransomware was blocked, Q2 2022–Q2 2025



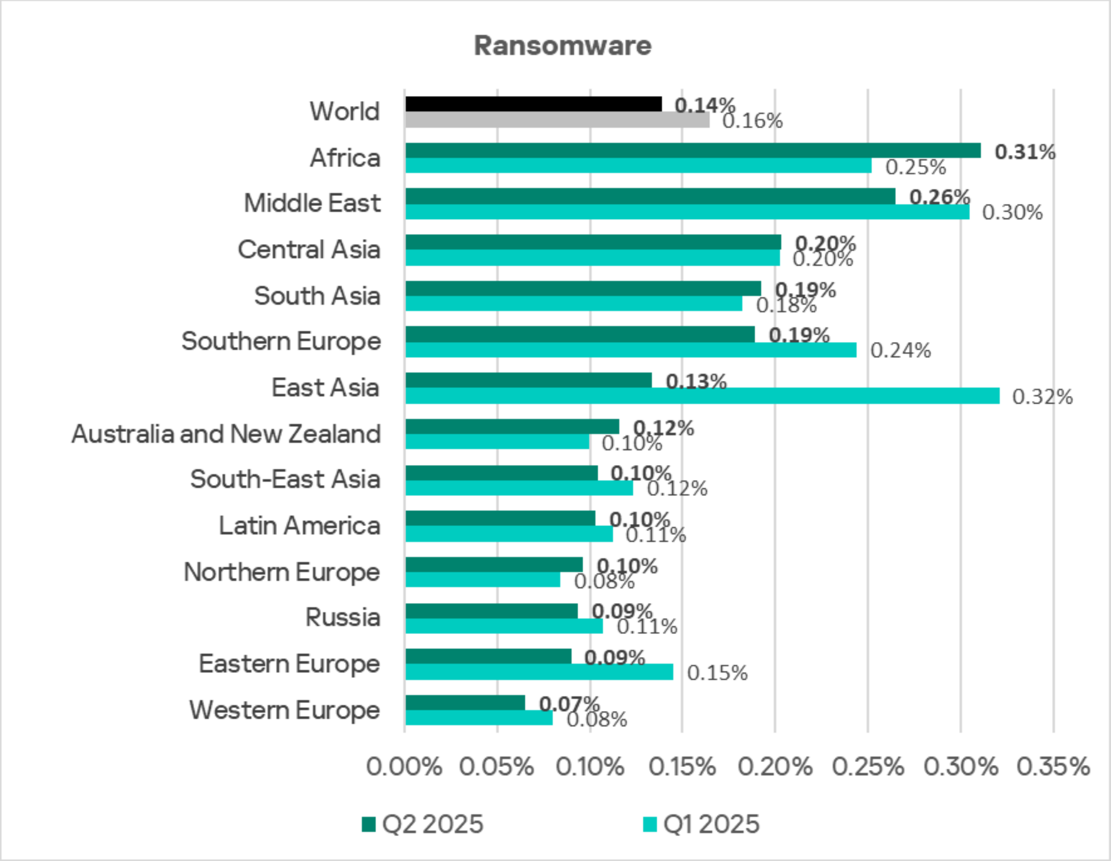
The monthly values for the quarter are comparable to those of the first three months of 2025.



Percentage of ICS computers on which ransomware was blocked, April 2023–June 2025

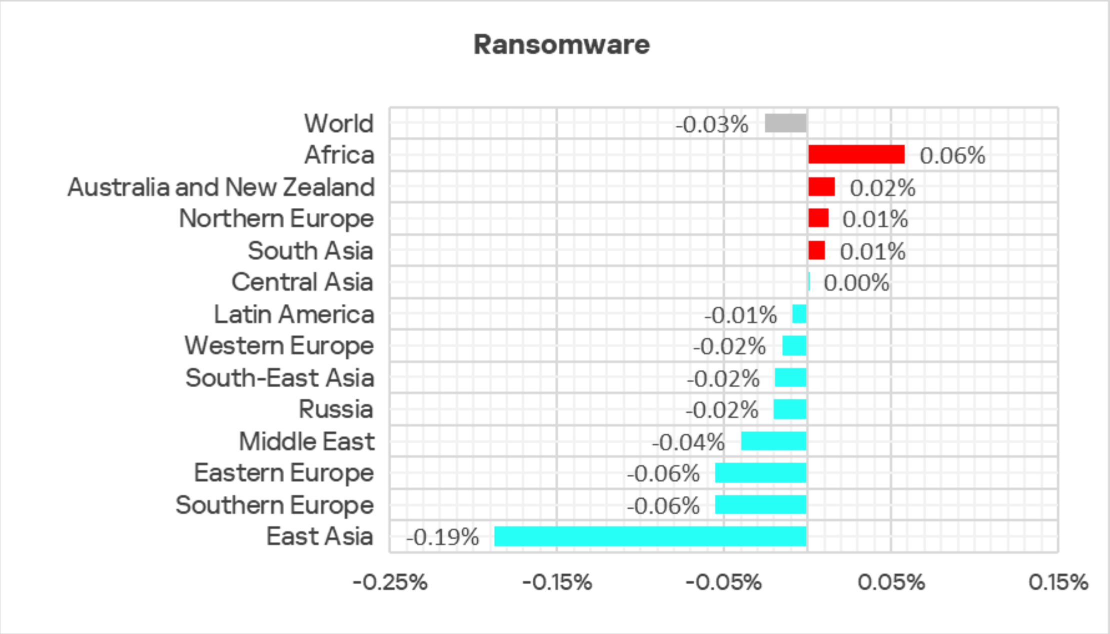
Regionally, the percentage of ICS computers on which ransomware was blocked ranged from 0.07% in Western Europe to 0.31% in Africa. The top three regions for this indicator were Africa, the Middle East, and Central Asia.

Regions ranked by percentage of ICS computers on which ransomware was blocked, Q2 2025



Africa was the leader in terms of growth for this indicator.

Changes in percentage of ICS computers on which ransomware was blocked, Q2 2025

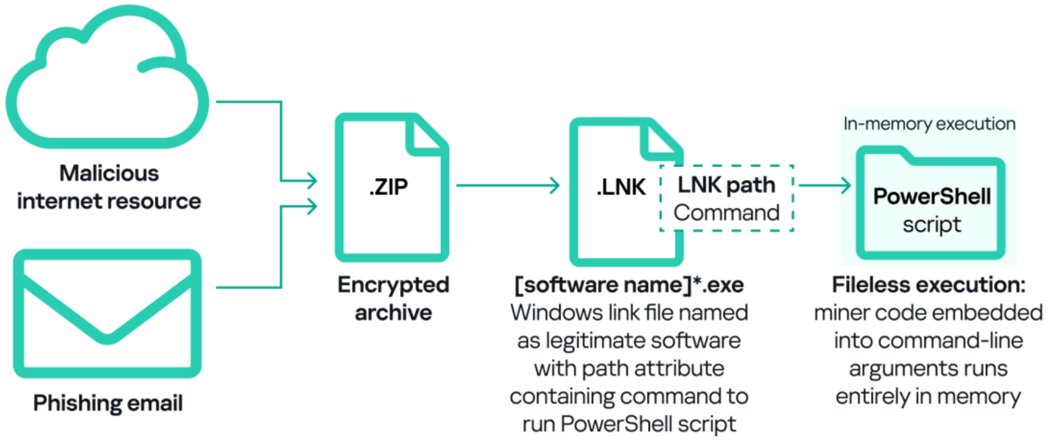


Miners in the form of executable files for Windows

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.

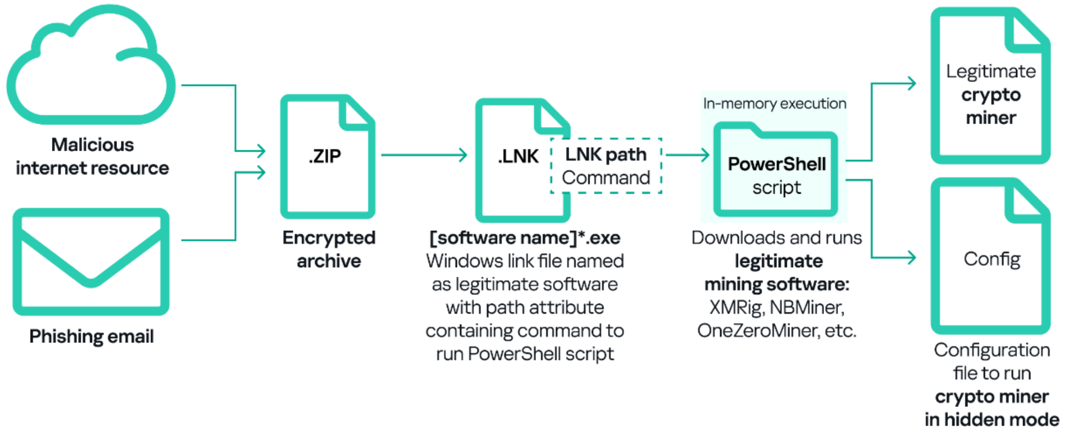
A significant portion of the Windows miners found on ICS computers consisted of archives with names that mimicked legitimate software. These archives did not contain actual software, but did include a Windows LNK file, commonly known as a shortcut. However, the target (or path) that the LNK file points 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 execution in cryptomining attacks

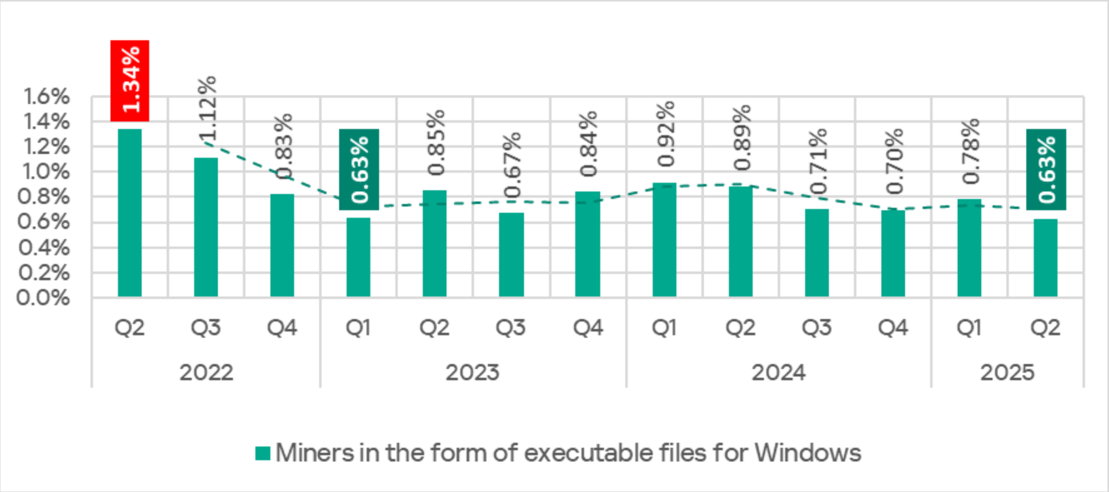

Malicious internet resource
Phishing email
.ZIP
Encrypted archive
.LNK
LNK path Command
[software name]*.exe Windows link file named as legitimate software with path attribute containing command to run PowerShell script
In-memory execution
PowerShell script
Fileless execution: miner code embedded into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

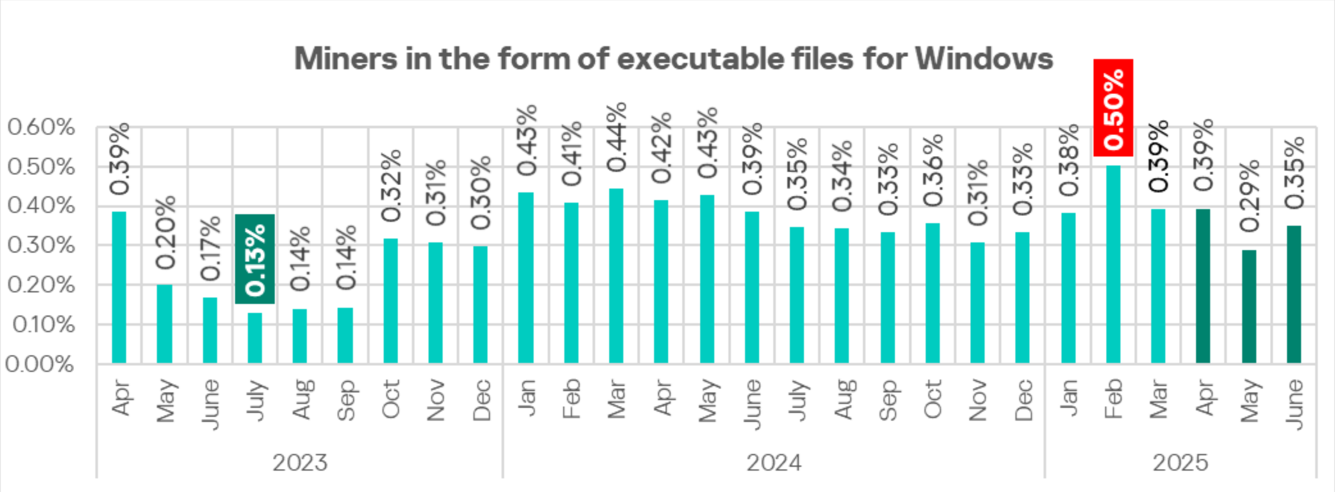

Malicious internet resource
Phishing email
.ZIP
Encrypted archive
.LNK
LNK path Command
[software name]*.exe Windows link file named as legitimate software with path attribute containing command to run PowerShell script
In-memory execution
PowerShell script
Downloads and runs legitimate mining software: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

In Q2 2025, the percentage of ICS computers on which miners in the form of executable files for Windows were blocked decreased to 0.63%.



Percentage of ICS computers on which miners in the form of executable files for Windows were blocked, Q2 2022–Q2 2025

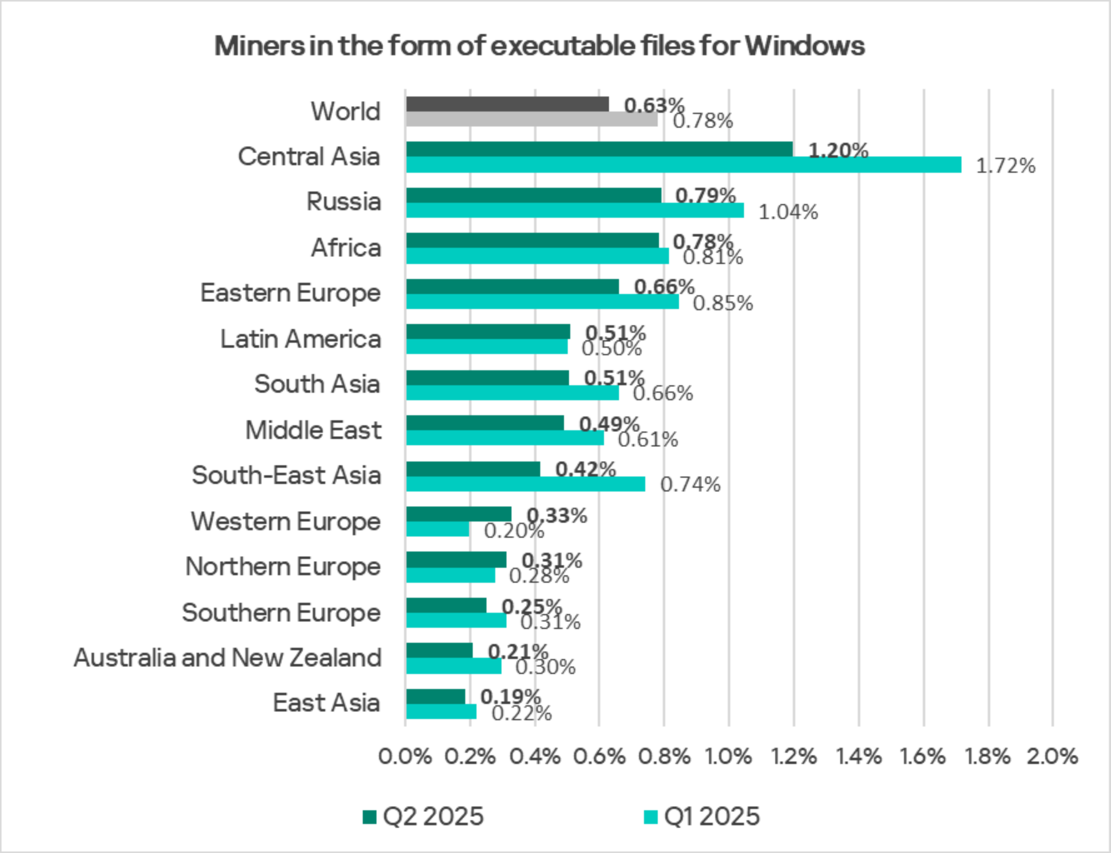
The monthly rate was highest in April at 0.39%.



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

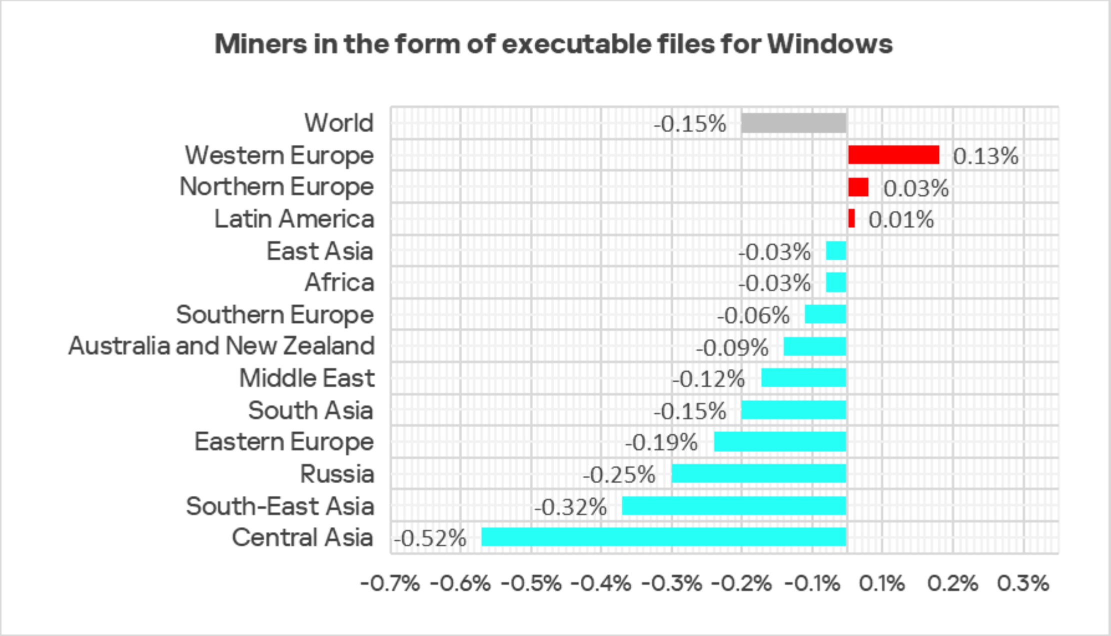
Regionally, the percentage of ICS computers on which miners in the form of executable files for Windows were blocked ranged from 0.19% in East Asia to 1.20% in Central Asia. The top three regions for this indicator were Central Asia, Russia, and Africa.

Regions ranked by percentage of ICS computers on which miners in the form of executable files for Windows were blocked, Q2 2025



In Q2 2025, the percentage of ICS computers on which miners in the form of executable files for Windows were blocked increased the most in Western Europe.

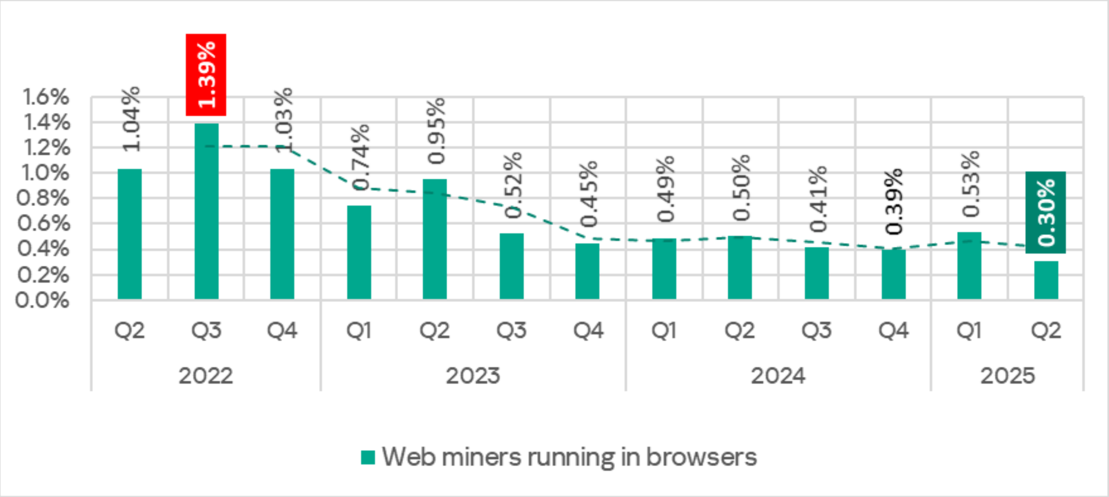
Changes in percentage of ICS computers on which miners in the form of executable files for Windows were blocked, Q2 2025



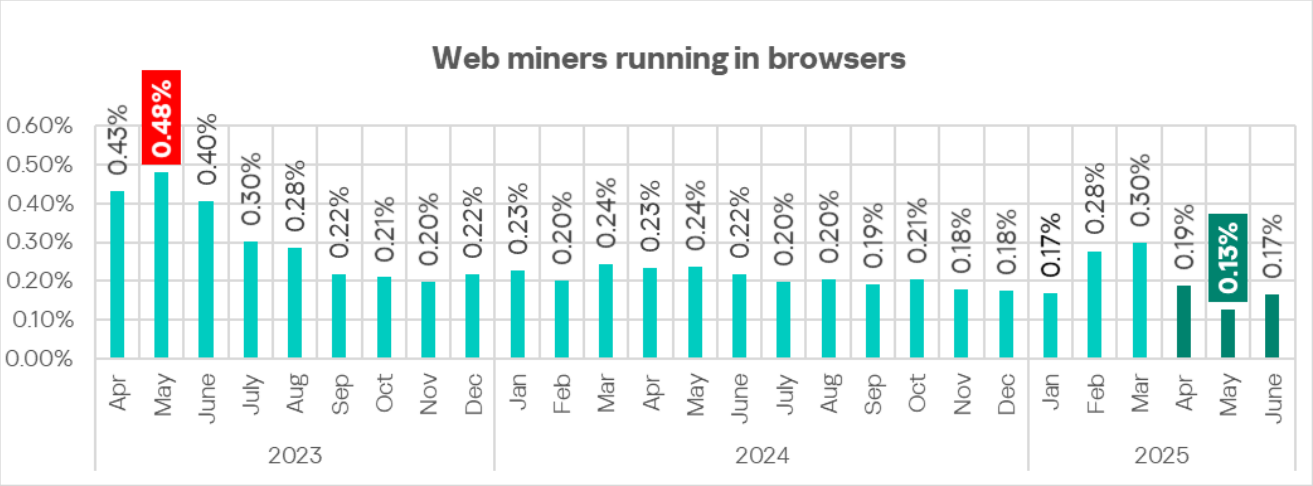
Web miners

In Q2 2025, the percentage of ICS computers on which web miners were blocked decreased to 0.30%. It is the lowest value since Q2 2022.

Percentage of ICS computers on which web miners were blocked, Q2 2022–Q2 2025



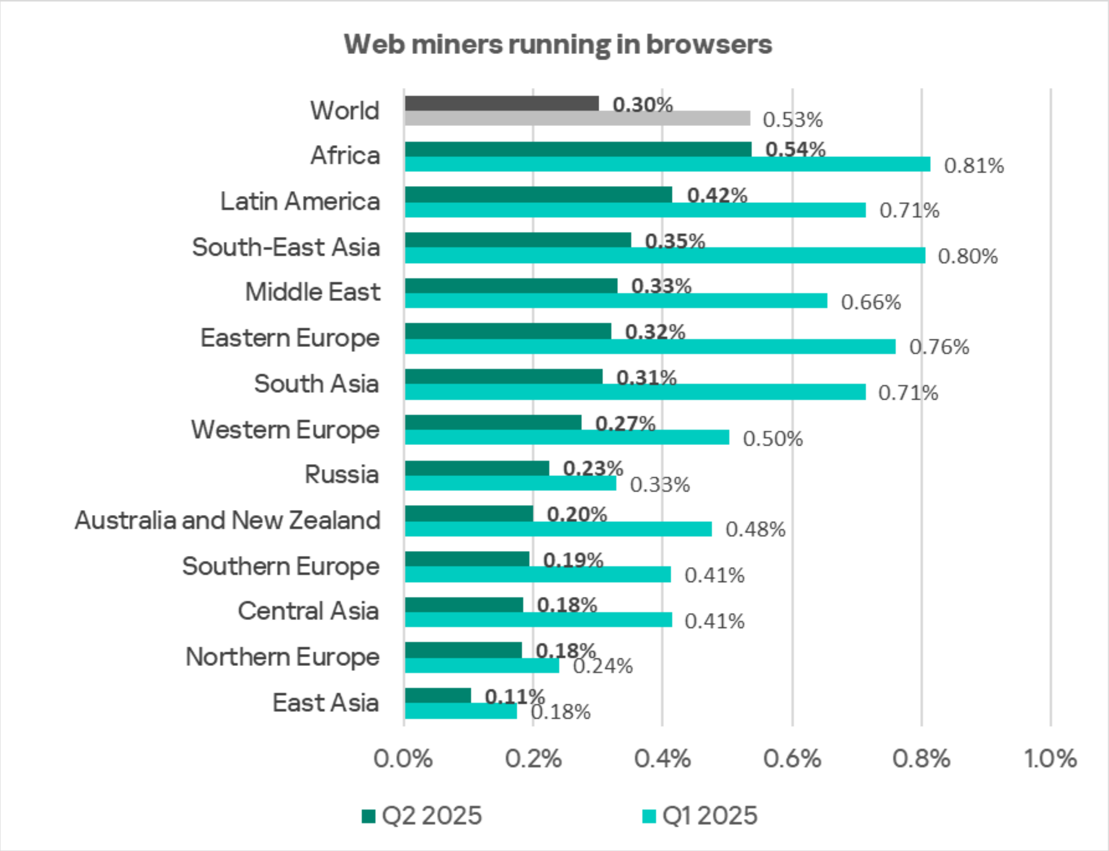
In May 2025, the monthly rate fell to its lowest point since April 2023.



Percentage of ICS computers on which web miners were blocked, April 2023–June 2025

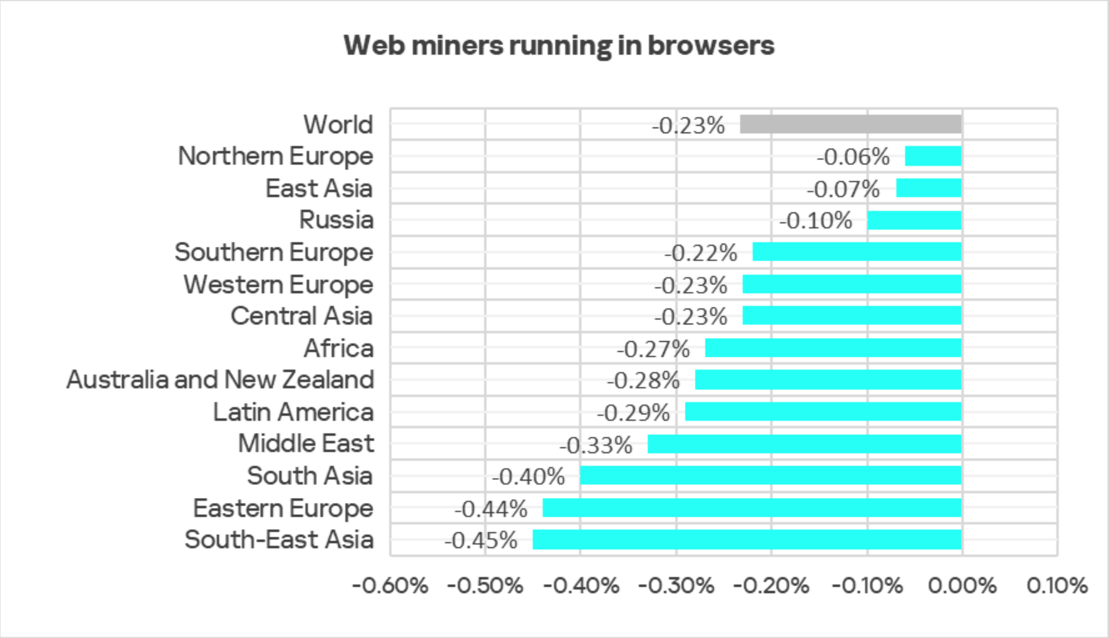
Regionally, the percentage of ICS computers on which web miners were blocked ranged from 0.11% in East Asia to 0.54% in Africa. The top three regions for this indicator were Africa, Latin America, and South-East Asia.

Regions ranked by percentage of ICS computers on which web miners were blocked, Q2 2025



In Q2 2025, the percentage of ICS computers on which web miners were blocked decreased in all regions.

Changes in percentage of ICS computers on which web miners were blocked, Q2 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.

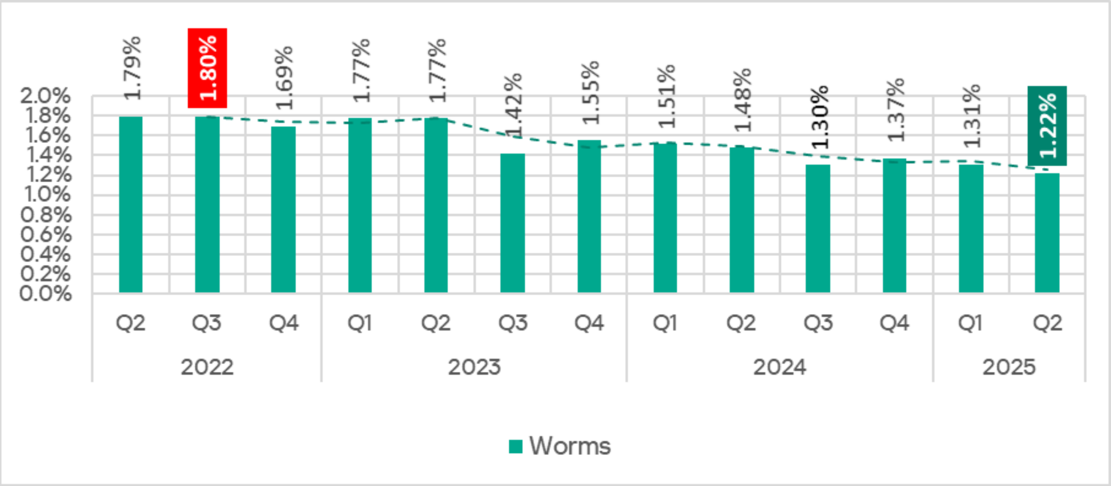
High rates of self-propagating malware and malware spreading via network folders at the industry, country or regional level likely indicate the presence of unprotected OT infrastructure that lacks even basic endpoint protection. These unprotected computers become sources of malware propagation. The situation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

Worms

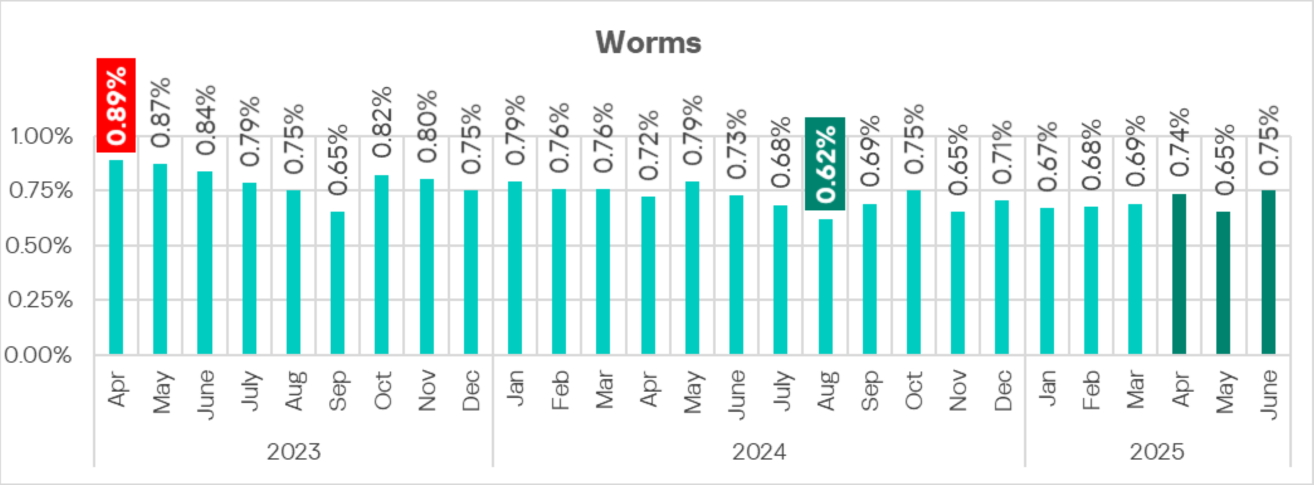
New worm versions used by malicious actors to spread spyware, ransomware and miners can also be found on ICS networks. In most cases, they rely on network service (e.g., SMB or RDP) exploits that have been addressed by the vendors but still persist on OT networks, previously stolen credentials, or password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

In Q2 2025, the percentage of ICS computers on which worms were blocked decreased to 1.22%. That is the lowest value since Q2 2022.

Percentage of ICS computers on which worms were blocked, Q2 2022–Q2 2025



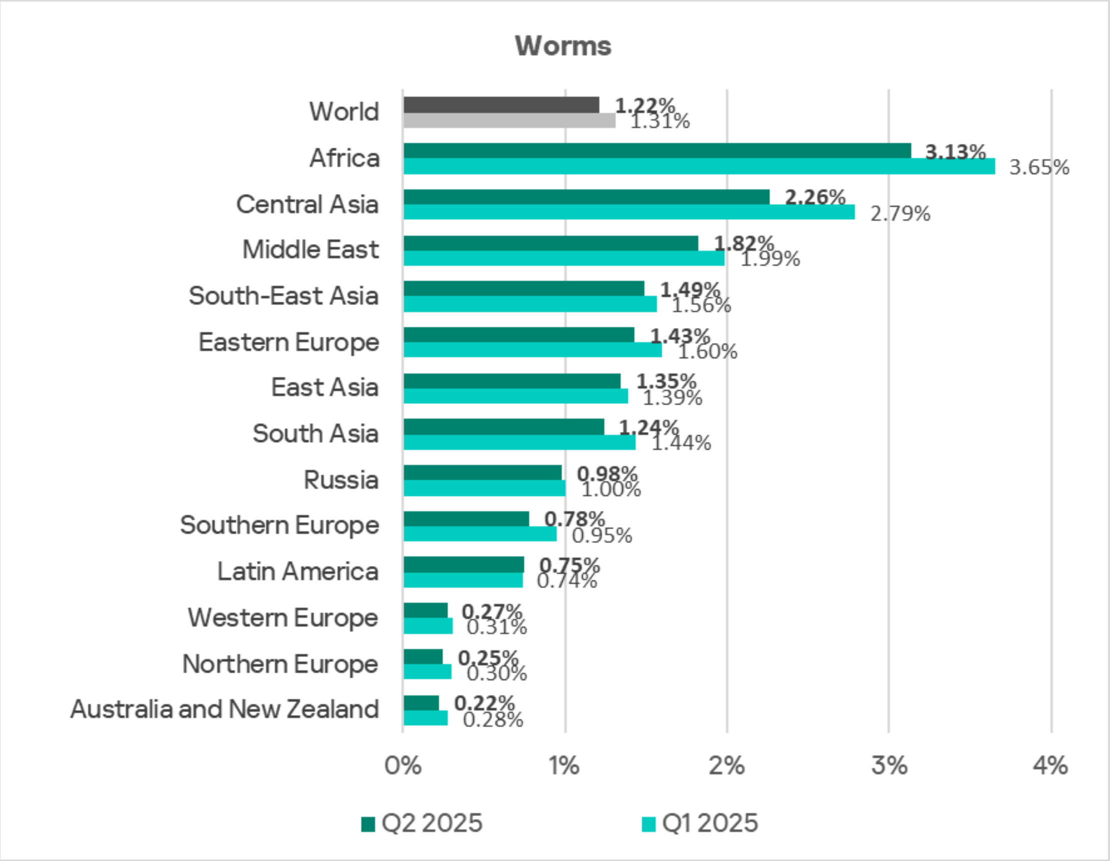
The highest monthly rate of Q2 occurred in June.



Percentage of ICS computers on which worms were blocked, April 2023–June 2025

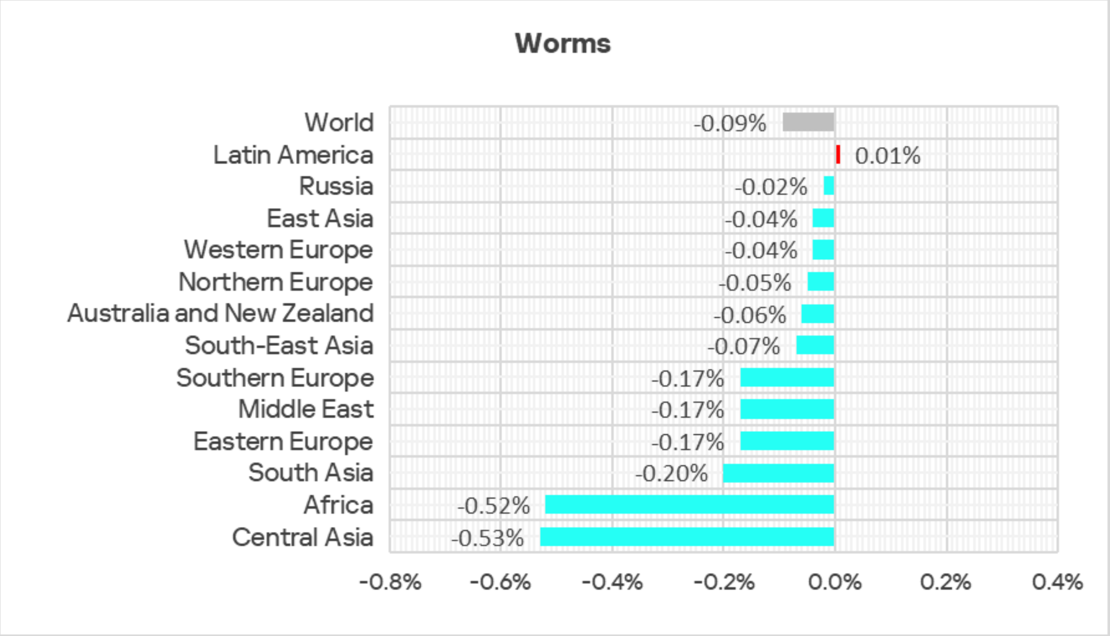
Regionally, the percentage of ICS computers on which worms were blocked ranged from 0.22% in Australia and New Zealand to 3.13% in Africa. The top three regions for this indicator were Africa, Central Asia, and the Middle East.

Regions ranked by percentage of ICS computers on which worms were blocked, Q2 2025



The percentage decreased in all regions except Latin America.

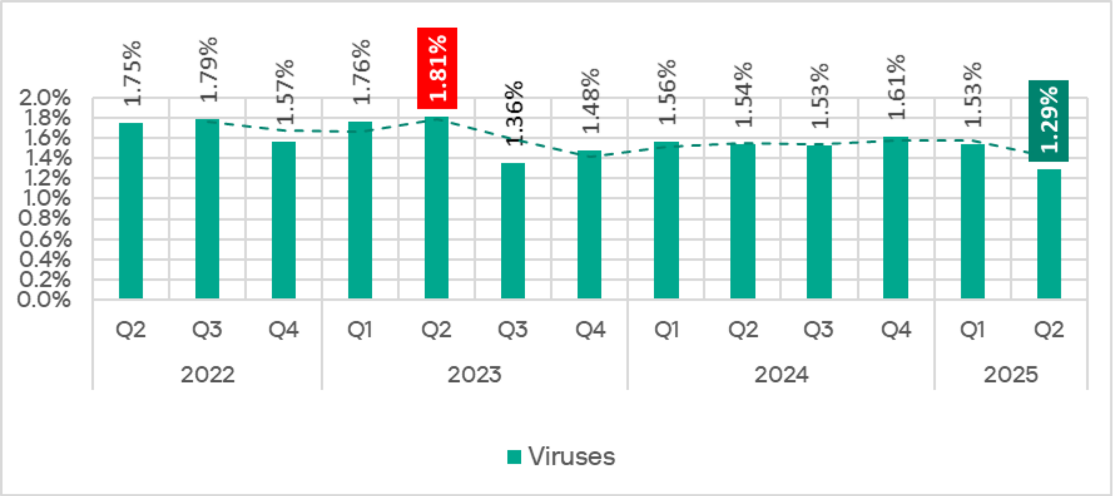
Changes in percentage of ICS computers on which worms were blocked, Q2 2025



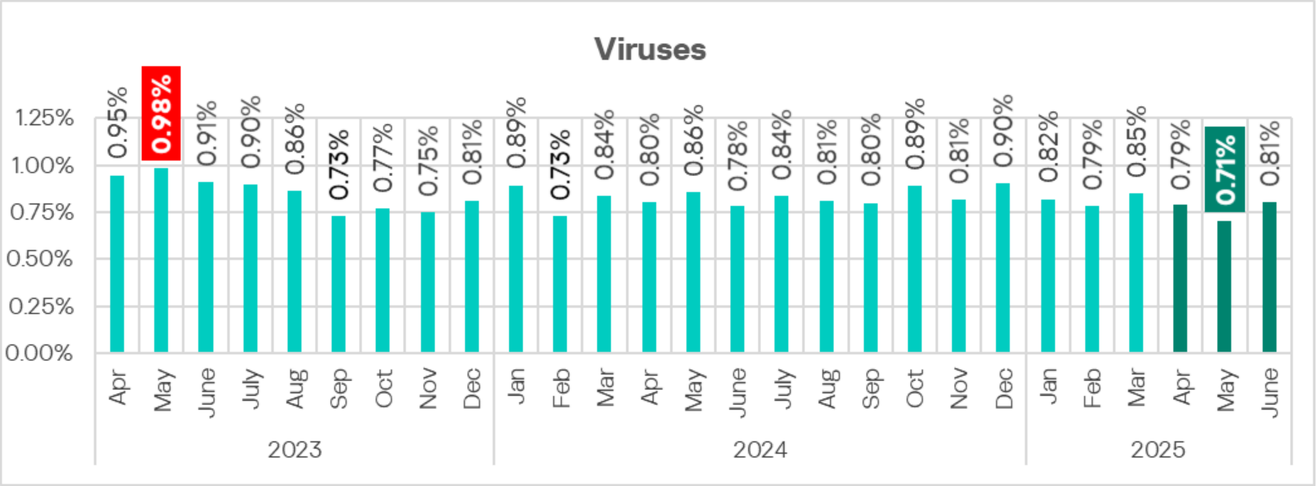
Viruses

As was the case with worms, the percentage of ICS computers on which viruses were blocked decreased in Q2 2025 and reached its lowest level (1.29%) since Q2 2022.

Percentage of ICS computers on which viruses were blocked, Q2 2022–Q2 2025



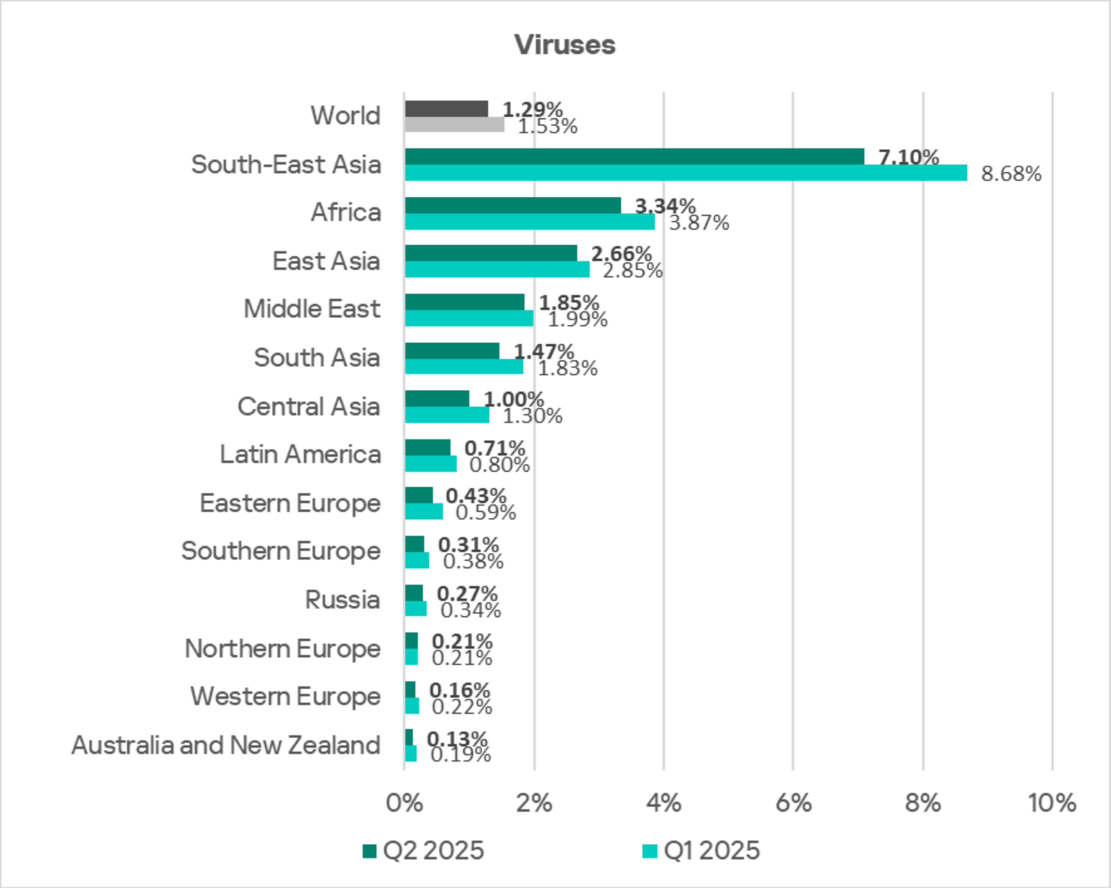
In May, the monthly rate reached its lowest point since April 2023.



Percentage of ICS computers on which viruses were blocked, April 2023–June 2025

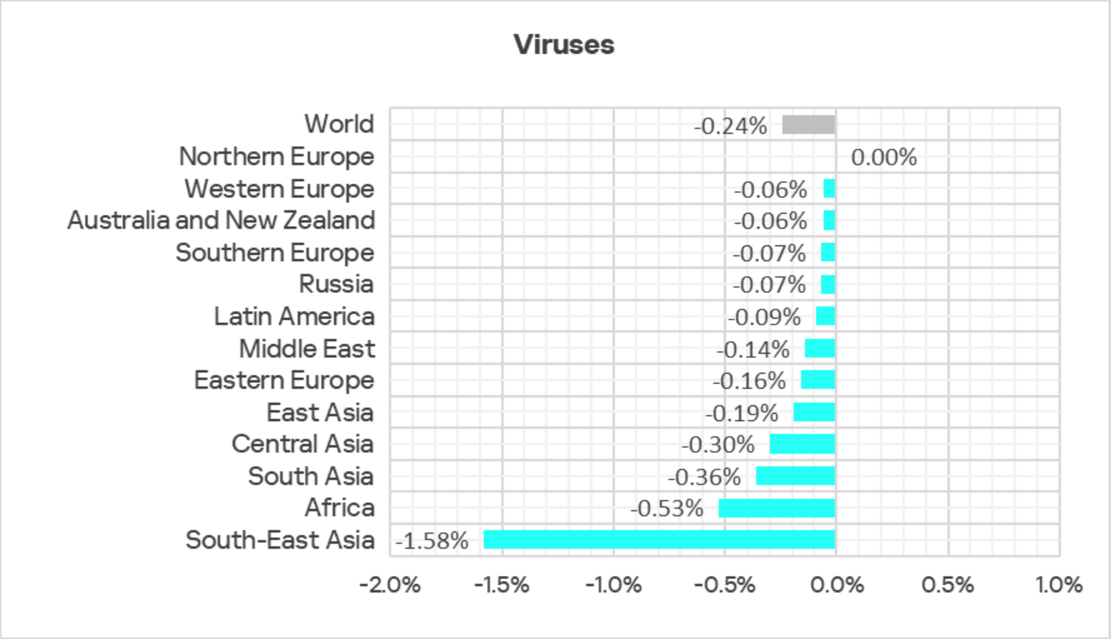
Regionally, the percentage of ICS computers on which viruses were blocked ranged from 0.13% in Australia and New Zealand to 7.10% in South-East Asia. The top three regions for this indicator were South-East Asia, Africa, and East Asia.

Regions ranked by percentage of ICS computers on which viruses were blocked, Q2 2025



In Q2 2025, the percentage decreased in all regions except Northern Europe.

Changes in percentage of ICS computers on which viruses were blocked, Q2 2025



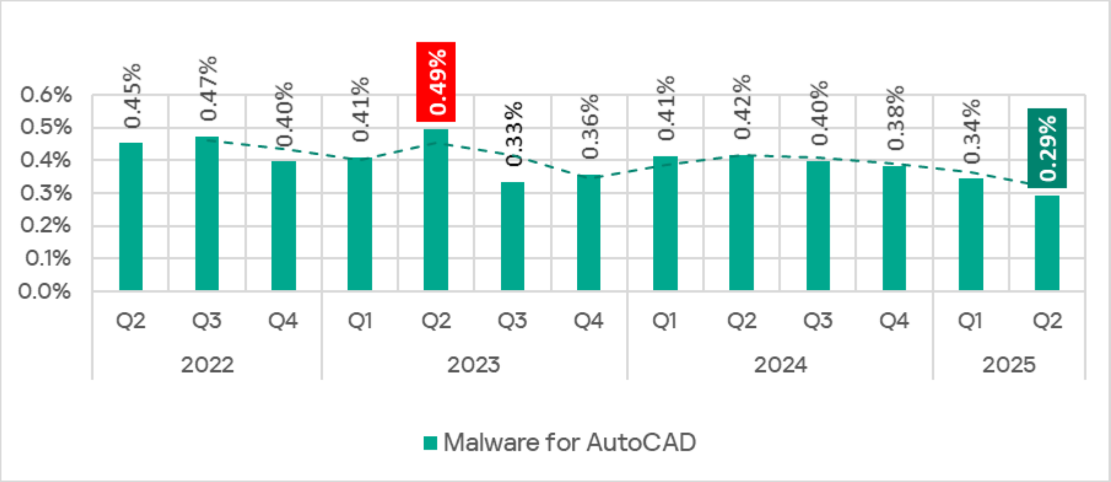
AutoCAD malware

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.

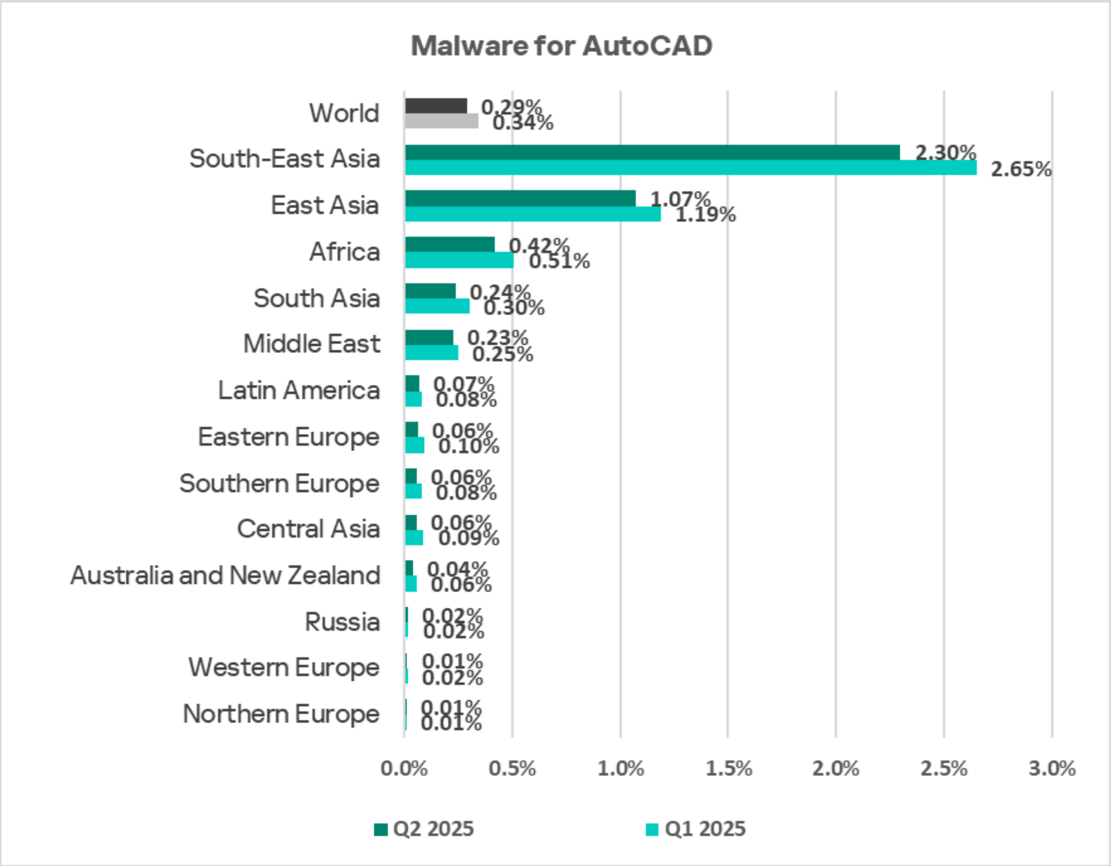
In Q2 2025, the percentage of ICS computers on which AutoCAD malware was blocked continued to decrease and reached its lowest level since Q2 2022.

Percentage of ICS computers on which AutoCAD malware was blocked, Q2 2022–Q2 2025



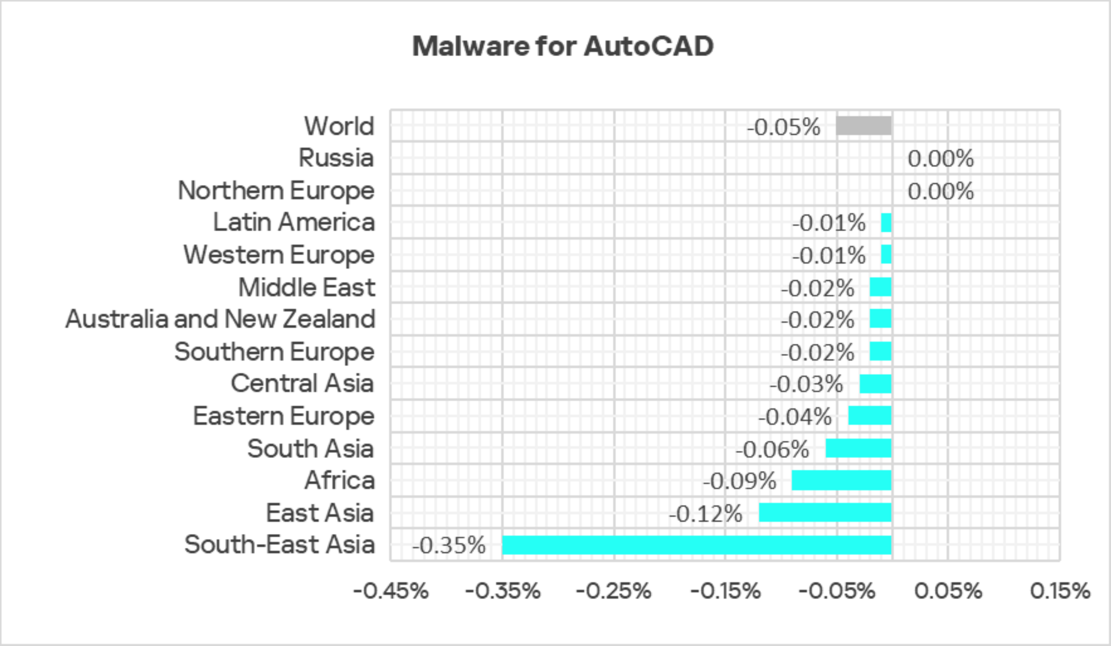
Regionally, the percentage of ICS computers on which AutoCAD malware was blocked ranged from 0.01% in Northern and Western Europe to 2.30% in South-East Asia. The same regions that led the virus ranking were also the leaders in terms of the percentage of ICS computers on which AutoCAD malware was blocked: South-East Asia, East Asia, and Africa.

Regions ranked by percentage of ICS computers on which AutoCAD malware was blocked, Q2 2025



As with viruses, the percentage of ICS computers on which AutoCAD malware was blocked decreased in all regions.

Changes in percentage of ICS computers on which AutoCAD malware was blocked, Q2 2025



Main threat sources

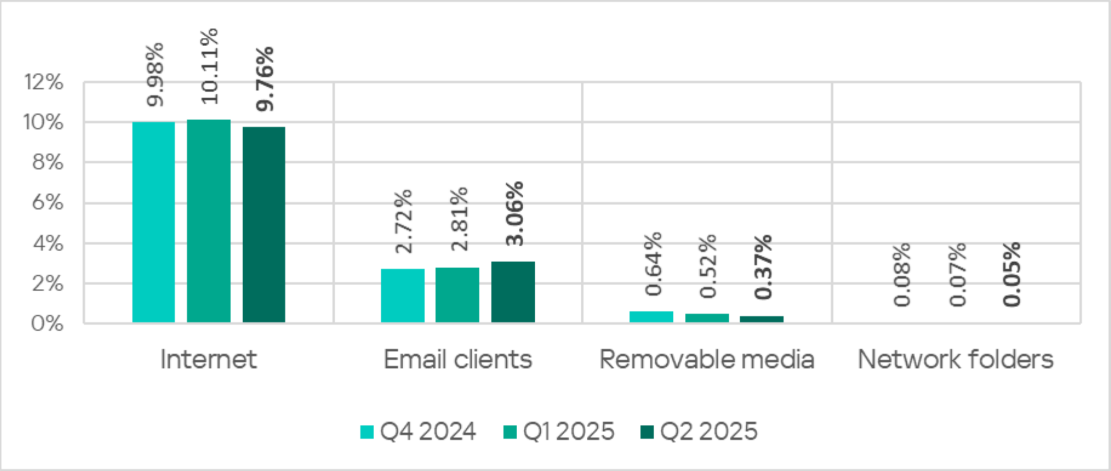
Depending on the threat detection and blocking scenario, it is not always possible to reliably identify the source. The circumstantial evidence for a specific source can be the blocked threat's type (category).

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 Q2 2025, the percentage of ICS computers on which threats from email clients were blocked continued to increase. This indicator increased in all regions during the quarter.

In contrast, the global average for other threat sources decreased.

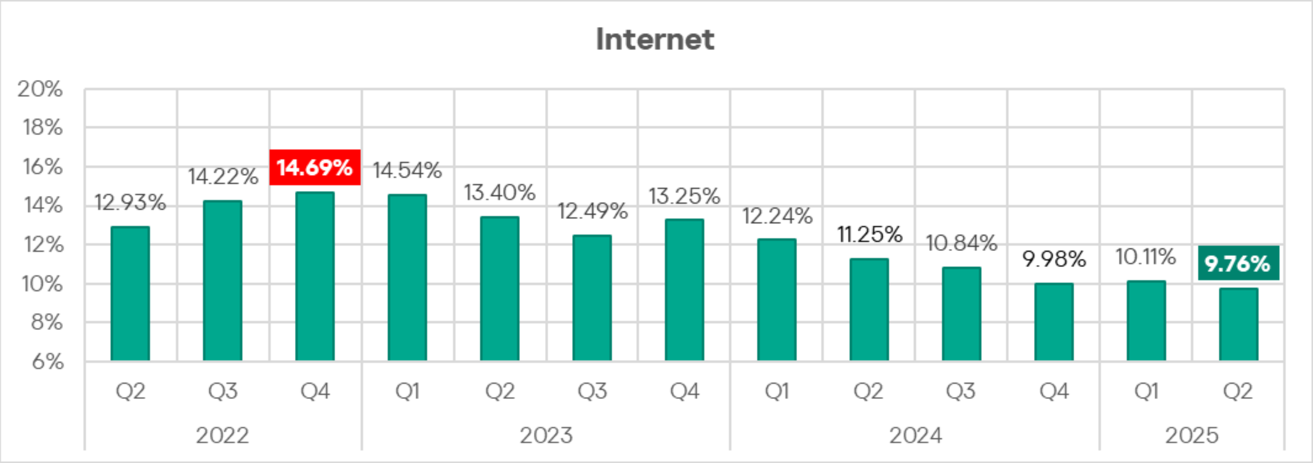
Percentage of ICS computers on which malicious objects from various sources were blocked



Internet

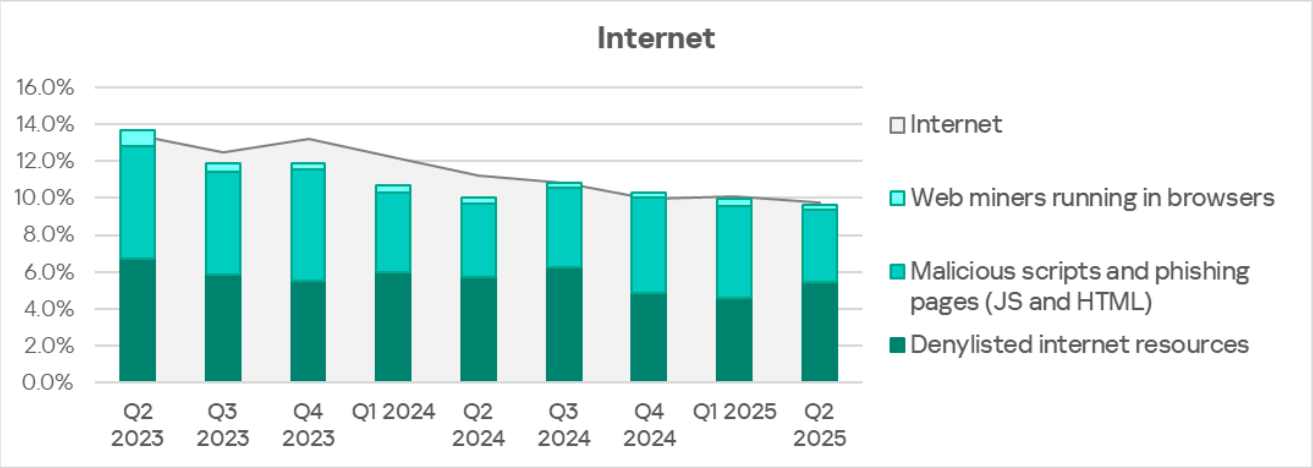
Detection and blocking of internet threats on ICS computers protected by Kaspersky products means that access to external services was allowed from these computers at the time of detection.

In Q2 2025, the percentage of ICS computers on which threats from the internet were blocked decreased to 9.76% and reached its lowest level since Q2 2022.



Percentage of ICS computers on which threats from the internet were blocked, Q2 2022–Q2 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.

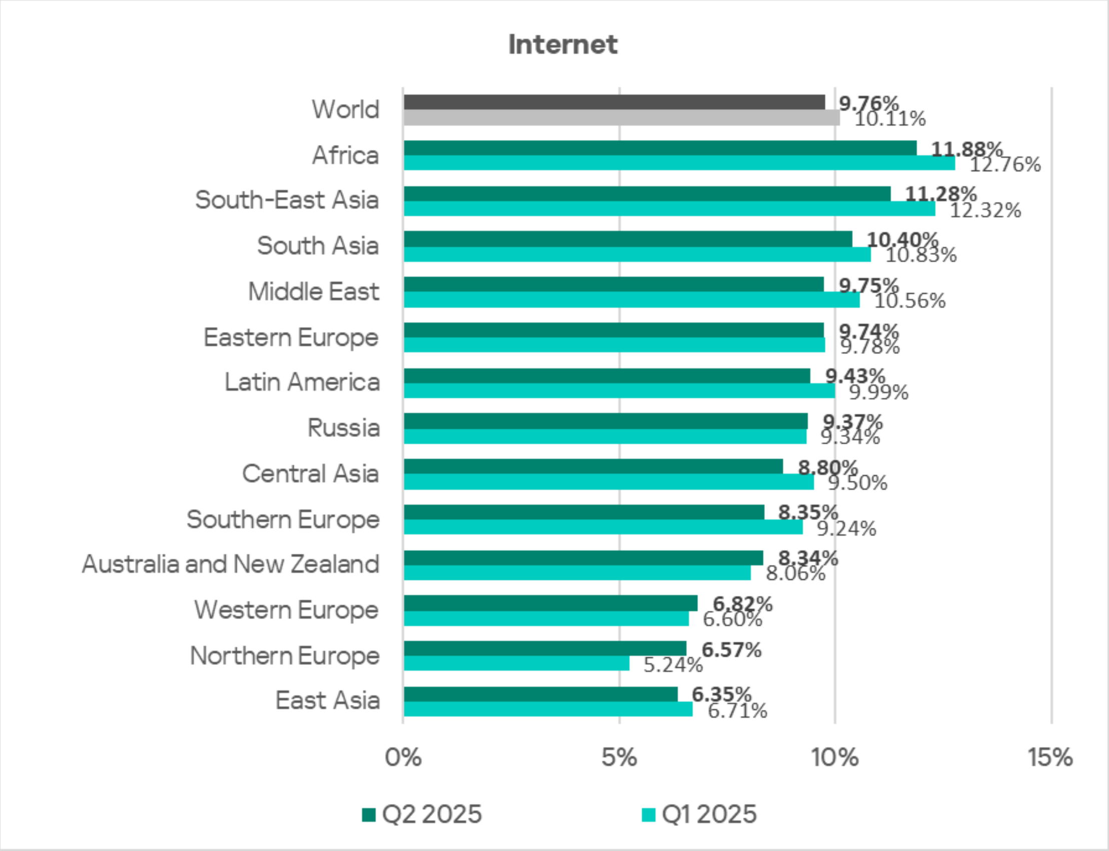


Percentage of ICS computers on which threats from the internet were blocked, Q2 2023–Q2 2025

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.

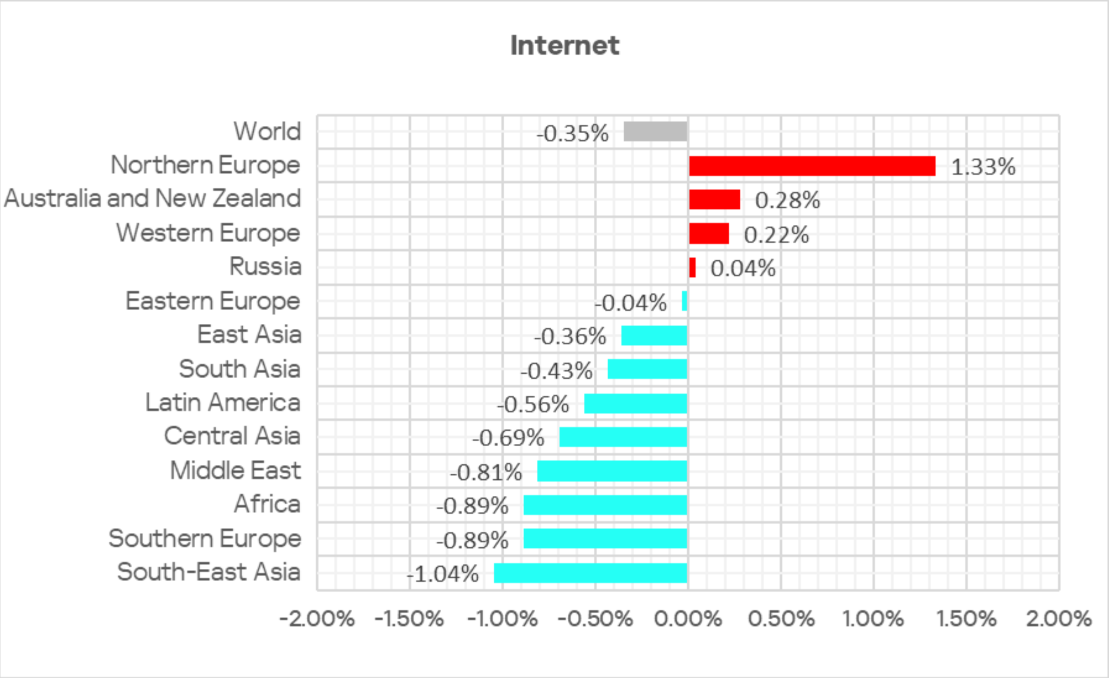
Regionally, the percentage of ICS computers on which threats from the internet were blocked ranged from 6.35% in East Asia to 11.88% in Africa. The top three regions for this indicator were Africa, South-East Asia, and South Asia.

Regions ranked by percentage of ICS computers on which threats from the internet were blocked, Q2 2025



In Q2 2025, the percentage increased in four regions, the most notable increase being in Northern Europe.

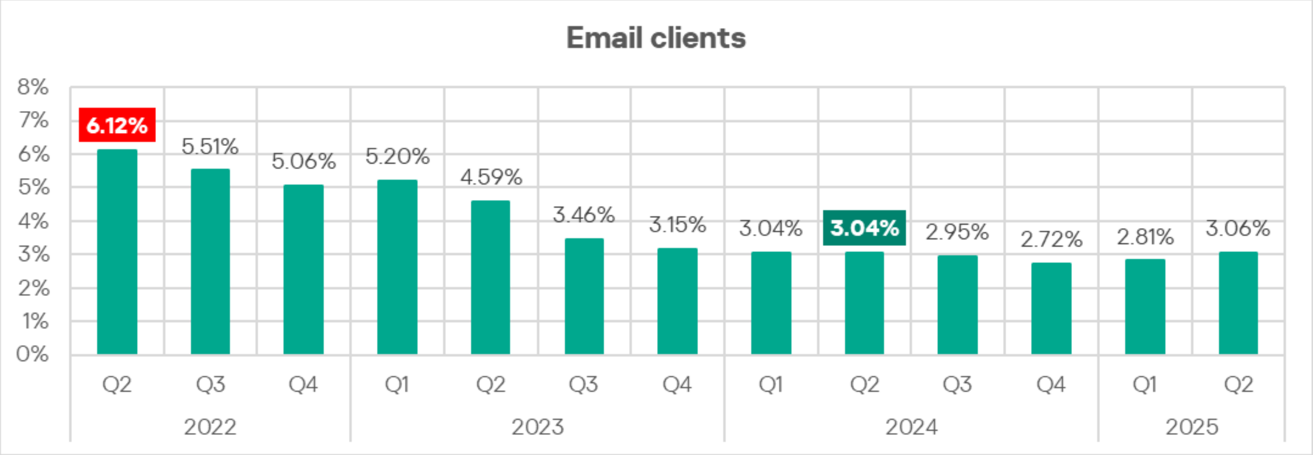
Changes in percentage of ICS computers on which threats from the internet were blocked, Q2 2025



Email clients

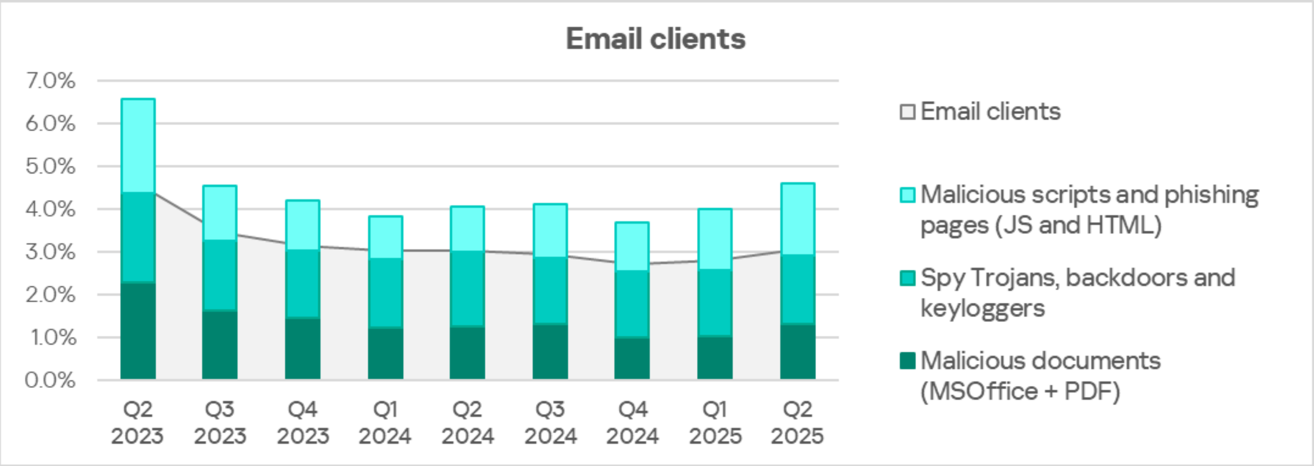
Some detected and blocked threats are delivered to protected computers by the mail delivery system and/or attempt to gain access through the email client application.

In Q2 2025, the percentage of ICS computers on which threats from email clients were blocked continued to increase.



Percentage of ICS computers on which threats from email clients were blocked, Q2 2022–Q2 2025

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

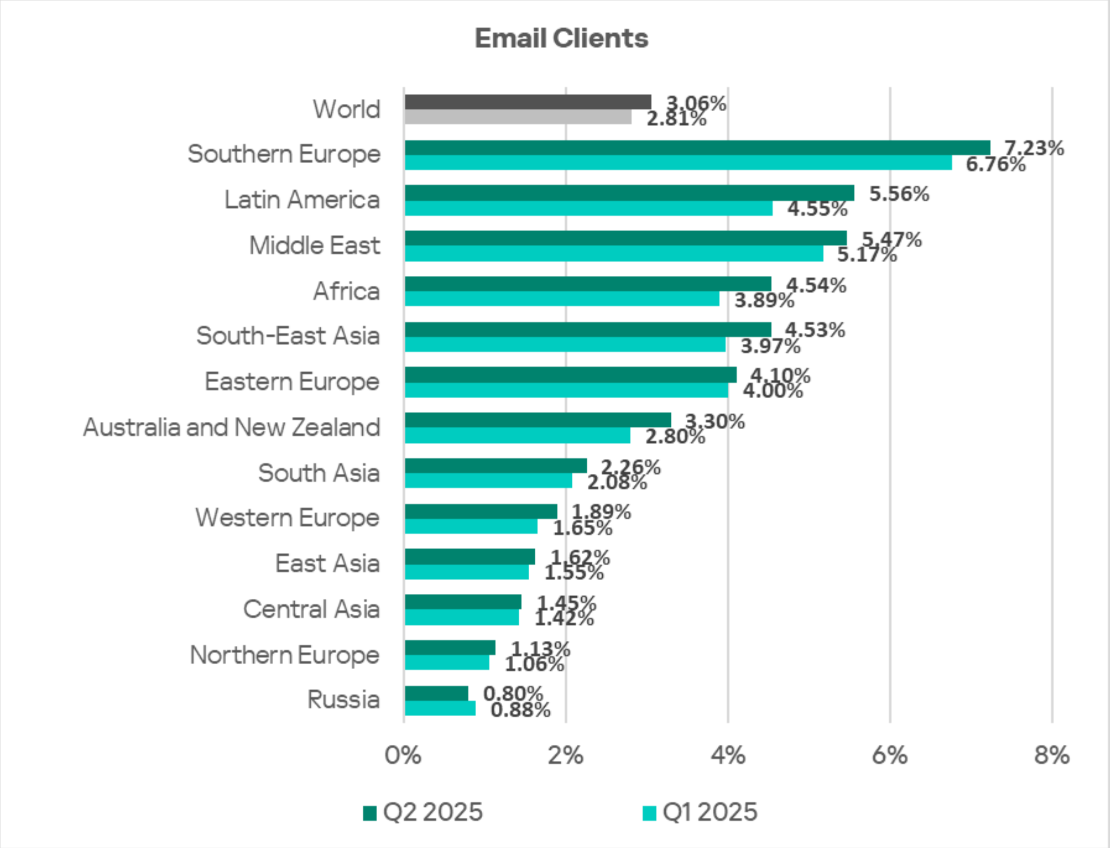


Percentage of ICS computers on which threats from email clients were blocked, Q2 2023–Q2 2025

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.

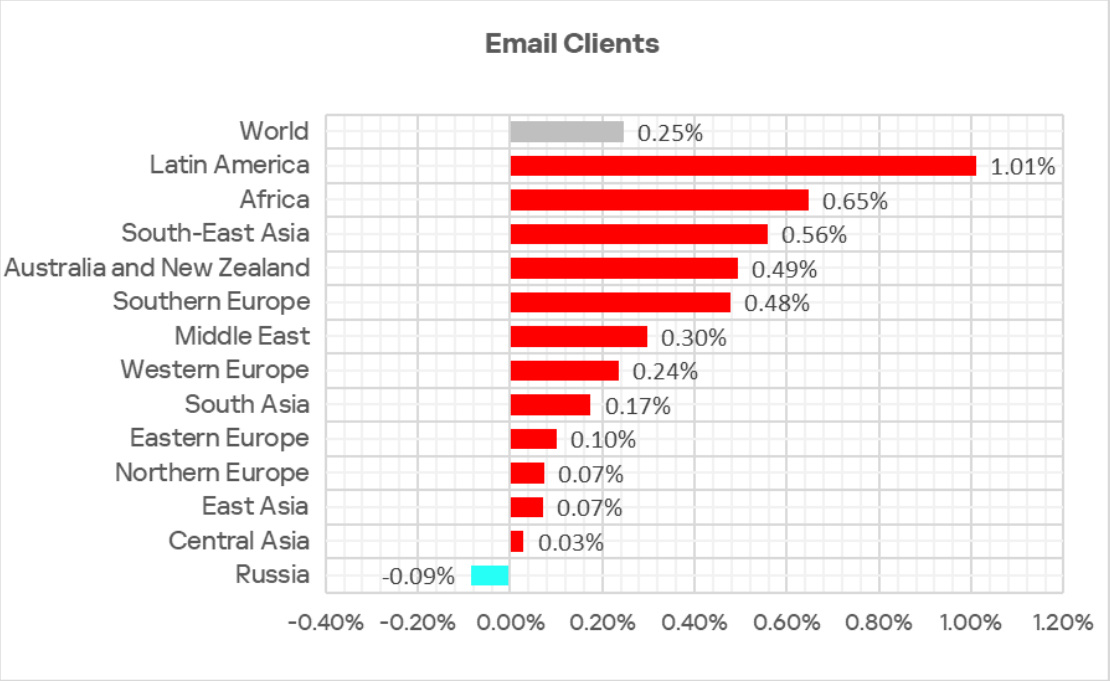
Regionally, the percentage of ICS computers on which threats from email clients were blocked ranged from 0.80% in Russia to 7.23% in Southern Europe. The top three regions for this indicator were Southern Europe, Latin America, and the Middle East.

Regions ranked by percentage of ICS computers on which threats from email clients were blocked, Q2 2025



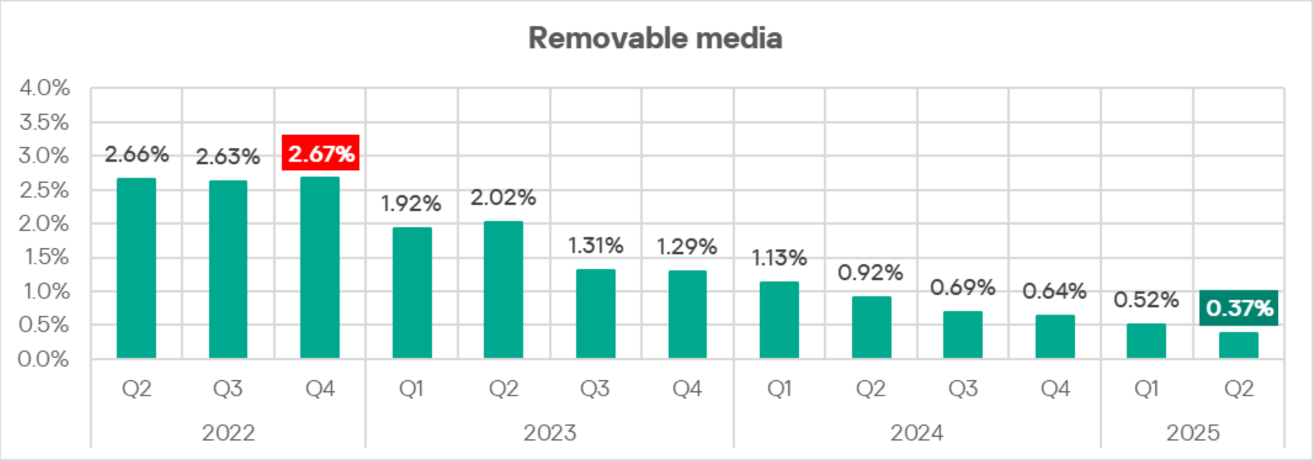
In Q2 2025, the percentage of ICS computers on which threats from email clients were blocked increased in all regions except Russia. The largest increase was seen in Latin America.

Changes in percentage of ICS computers on which threats from email clients were blocked, Q2 2025



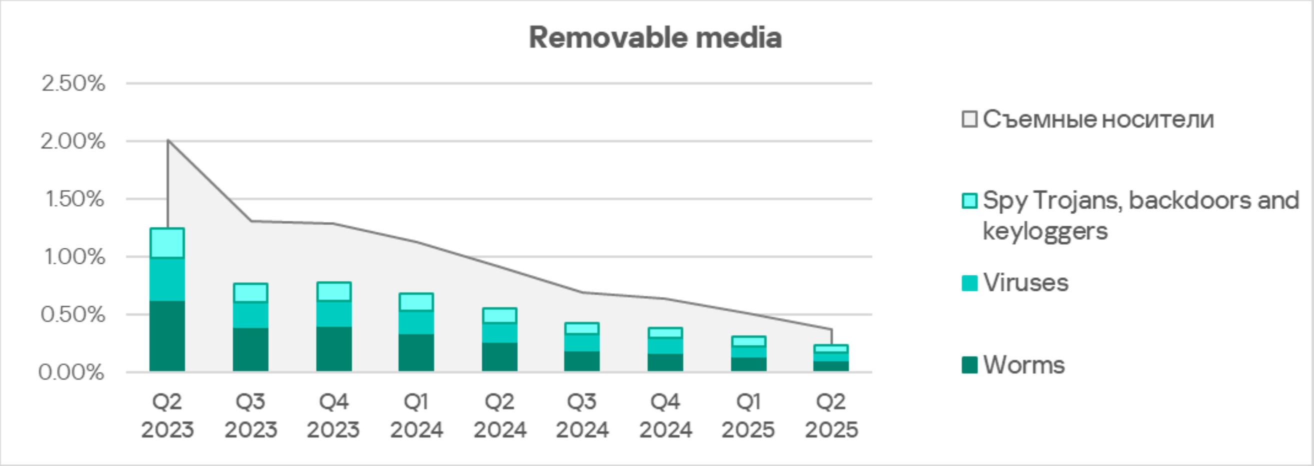
Removable media

In Q2 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 2022.



Percentage of ICS computers on which threats from removable media were blocked, Q2 2022–Q2 2025

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



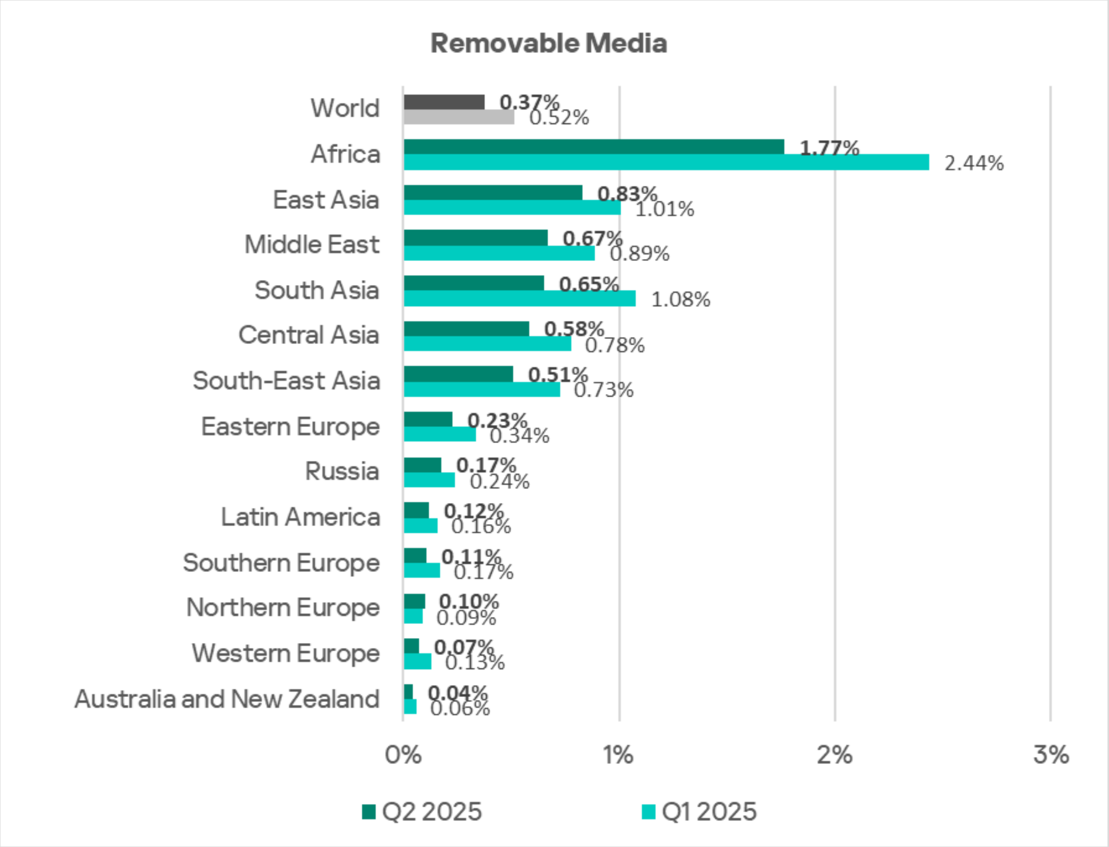
Percentage of ICS computers on which threats from removable media were blocked, Q2 2023–Q2 2025

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.

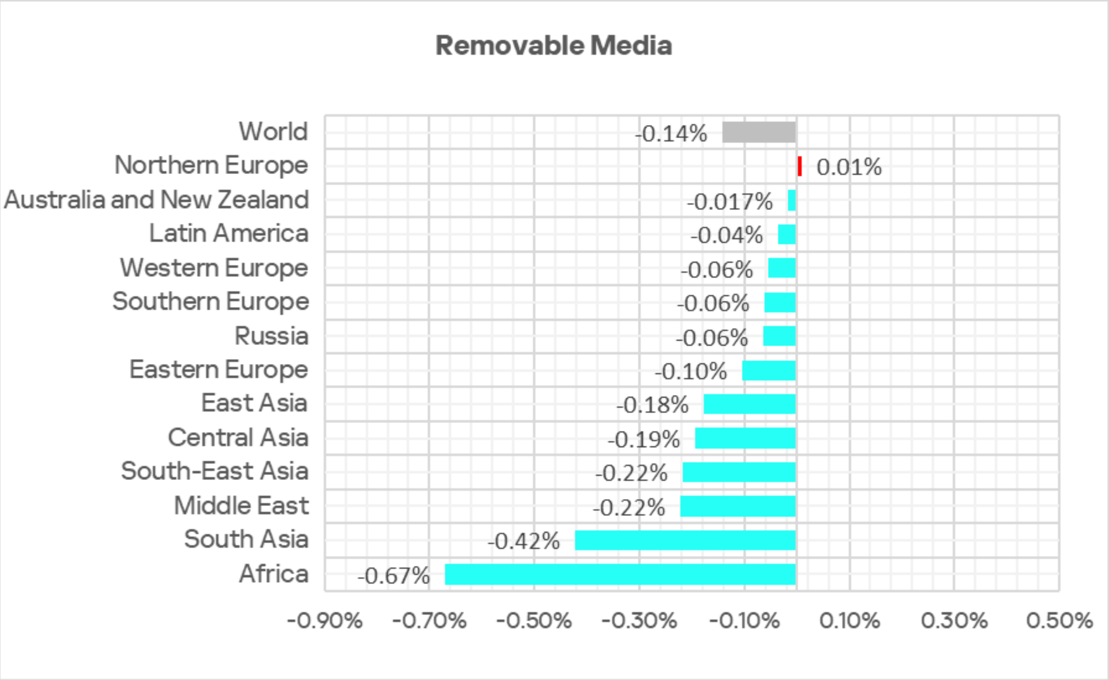
Regionally, the percentage of ICS computers on which threats from removable media were blocked ranged from 0.04% in Australia and New Zealand to 1.77% in Africa. The top three regions for this indicator were Africa, East Asia and the Middle East.

Regions ranked by percentage of ICS computers on which threats from removable media were blocked, Q2 2025



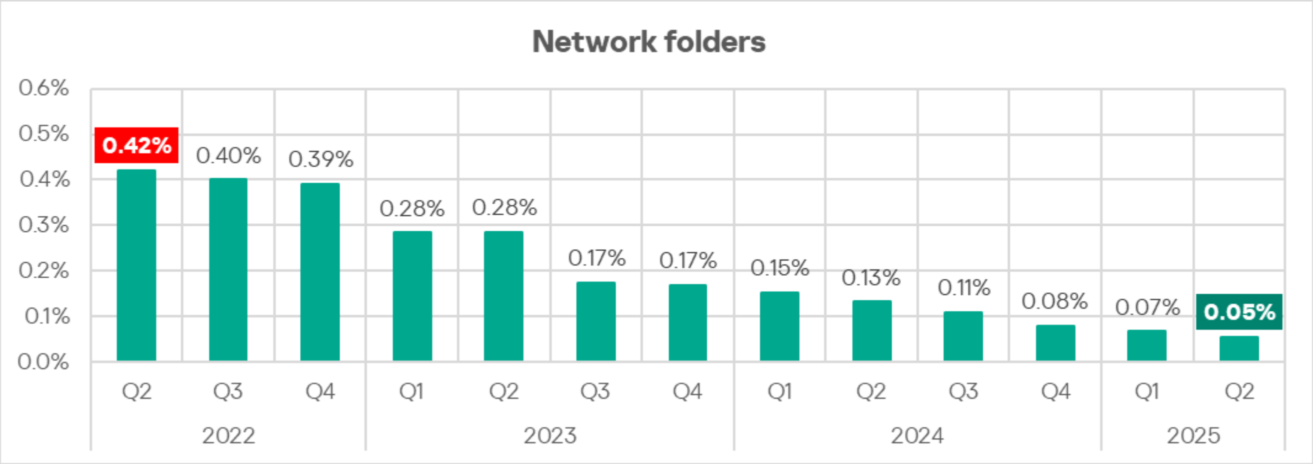
In Q2 2025 the percentage decreased in all regions except Northern Europe.

Changes in percentage of ICS computers on which threats from removable media were blocked, Q2 2025



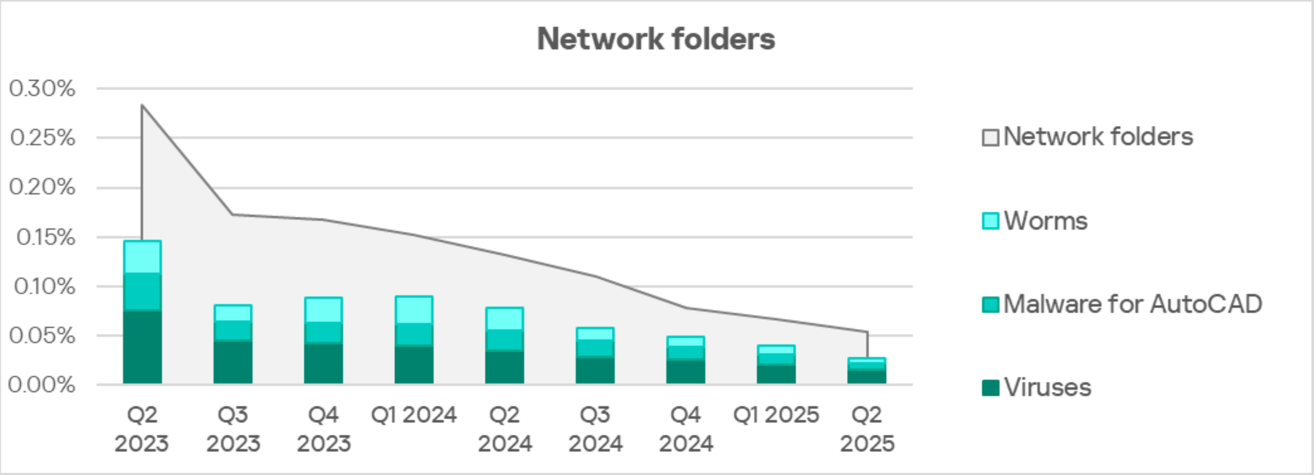
Network folders

In Q2 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.



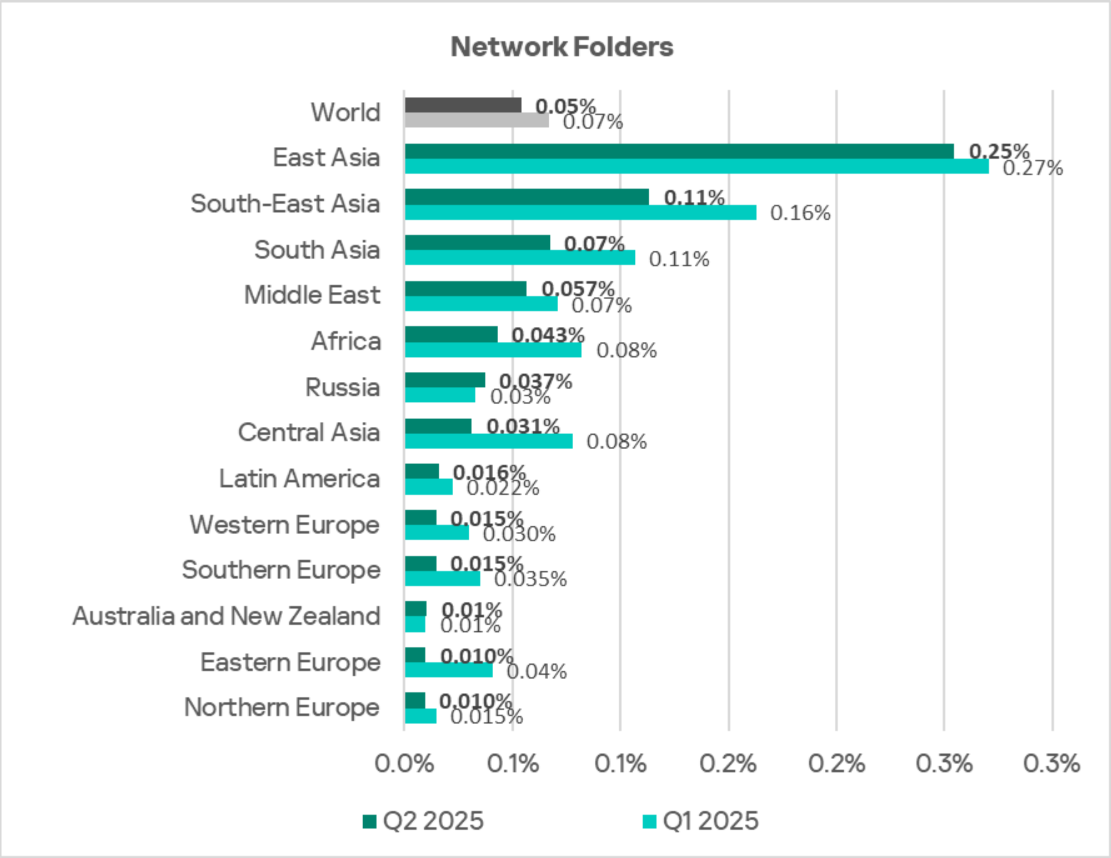
Percentage of ICS computers on which threats from network folders were blocked, Q2 2022–Q2 2025

The main categories of threats that spread through network folders are worms, viruses, and AutoCAD malware.



Percentage of ICS computers on which threats from network folders were blocked, Q2 2023–Q2 2025

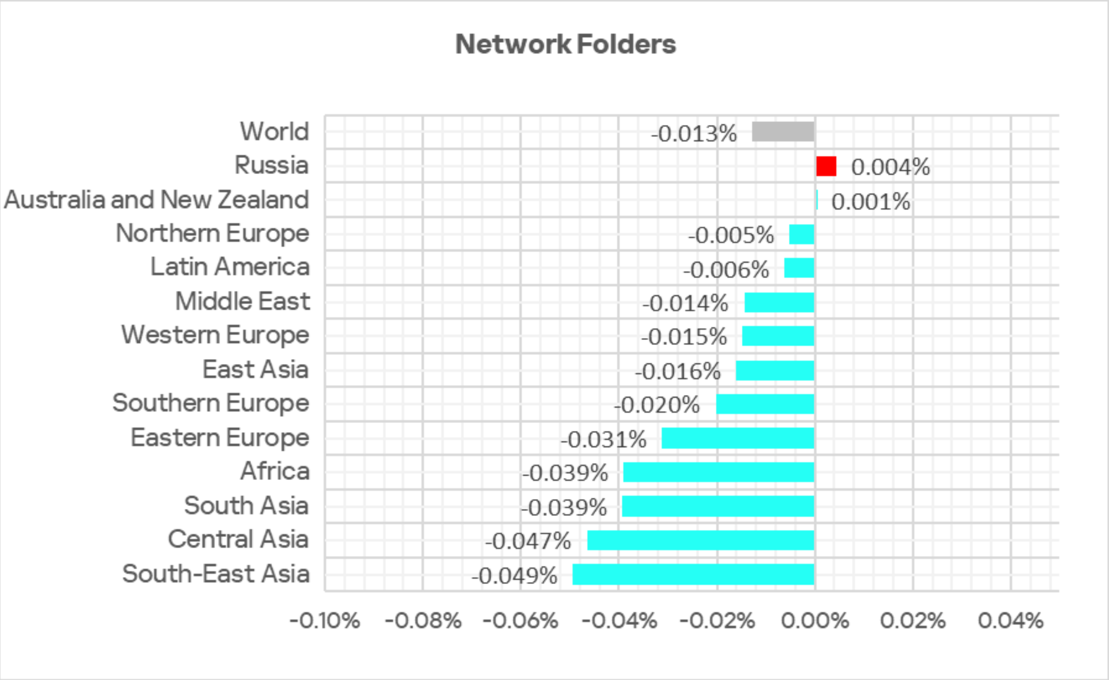
Regionally, the percentage of ICS computers on which threats from network folders were blocked ranged from 0.01% in Northern Europe to 0.25% in East Asia. The top three regions for this indicator were East Asia, South-East Asia, and South Asia.



Regions ranked by percentage of ICS computers on which threats from network folders were blocked, Q2 2025

In Q2 2025, the percentage decreased in all regions except Russia and Australia and New Zealand.

Changes in percentage of ICS computers on which threats from network folders were blocked, Q2 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,

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

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.

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