Kaspersky ICS CERT

Threat landscape for industrial automation systems

Q3 2025

11.12.2025 Version 1.0

Q3 in numbers

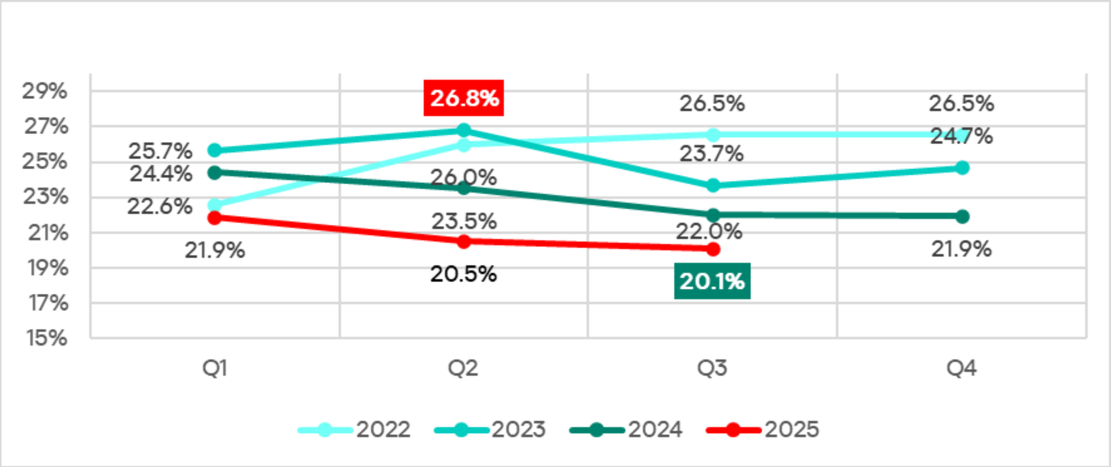
Parameter	Q2 2025	Q3 2025	Quarterly changes
Global percentage of attacked ICS computers	20.5%	20.1%	▼0.4 pp
Percentage of ICS computers on which malicious objects from different categories were blocked			
Malicious scripts and phishing pages (JS and HTML)	6.49%	6.79%	▲0.30 pp
Spy Trojans, backdoors and keyloggers	3.84%	4.04%	▲0.20 pp
Denylisted internet resources	5.91%	4.01%	▼1.90 pp
Malicious documents (MSOffice + PDF)	1.97%	1.98%	▲0.01 pp
Viruses	1.29%	1.40%	▲0.11 pp
Worms	1.22%	1.26%	▲0.04 pp
Miners in the form of executable files for Windows	0.63%	0.57%	▼0.06 pp
Malware for AutoCAD	0.29%	0.30%	▲0.01 pp
Web miners running in browsers	0.30%	0.25%	▼0.05 pp
Ransomware	0.14%	0.17%	▲0.03 pp
Main threat sources			
Internet	9.76%	7.99%	▼1.77 pp
Email clients	3.06%	3.01%	▼0.05 pp
Removable media	0.37%	0.33%	▼0.04 pp
Network folders	0.05%	0.04%	▼0.01 pp

Changes over the quarter

The percentage of ICS computers on which malicious objects were blocked

In Q3 2025, the percentage of ICS computers on which malicious objects were blocked continued to decrease, reaching its lowest level since 2022 — 20.1%.

Percentage of ICS computers on which malicious objects were blocked, Q1 2022–Q3 2025

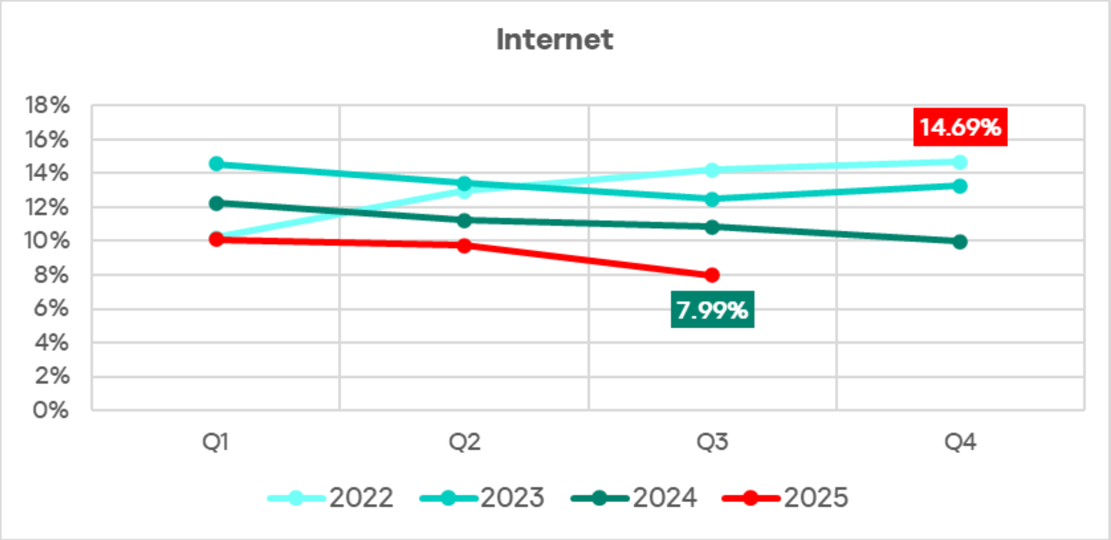


Regionally, the percentage ranged from 9.2% in Northern Europe to 27.4% in Africa. Increases were seen in five regions. East Asia was the leader in terms of growth for this indicator.

Main threat sources and categories

The main threat sources to computers in enterprise OT infrastructure are still the internet, email clients, and removable media. In Q3 2025, the global average for all threat sources decreased. The percentage of ICS computers on which threats from the internet were blocked reached its lowest level since 2022.

Percentage of ICS computers on which threats from the internet were blocked, Q1 2022–Q3 2025

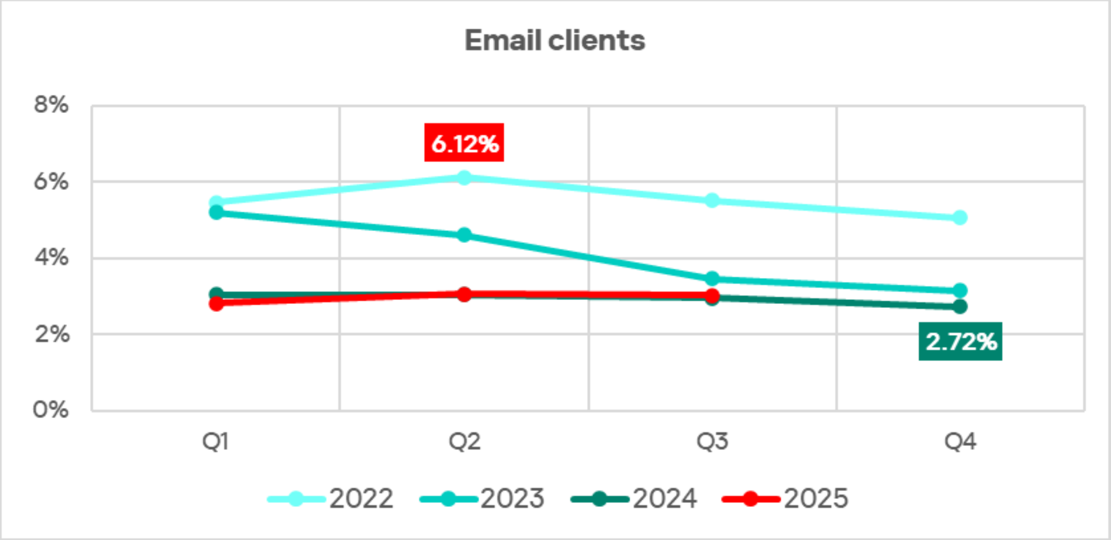


The main categories of threats from the internet blocked on ICS computers in Q3 20225 were malicious scripts and phishing pages, and denylisted internet resources.

After an increase in the previous quarter, the percentage of ICS computers on which denylisted internet resources were blocked decreased significantly (-1.9 pp) and reached its lowest level since 2022 — 4.01%.

The percentage of ICS computers on which threats from email clients were blocked has remained relatively stable since the beginning of 2024.

Percentage of ICS computers on which threats from email clients were blocked, Q1 2022–Q3 2025



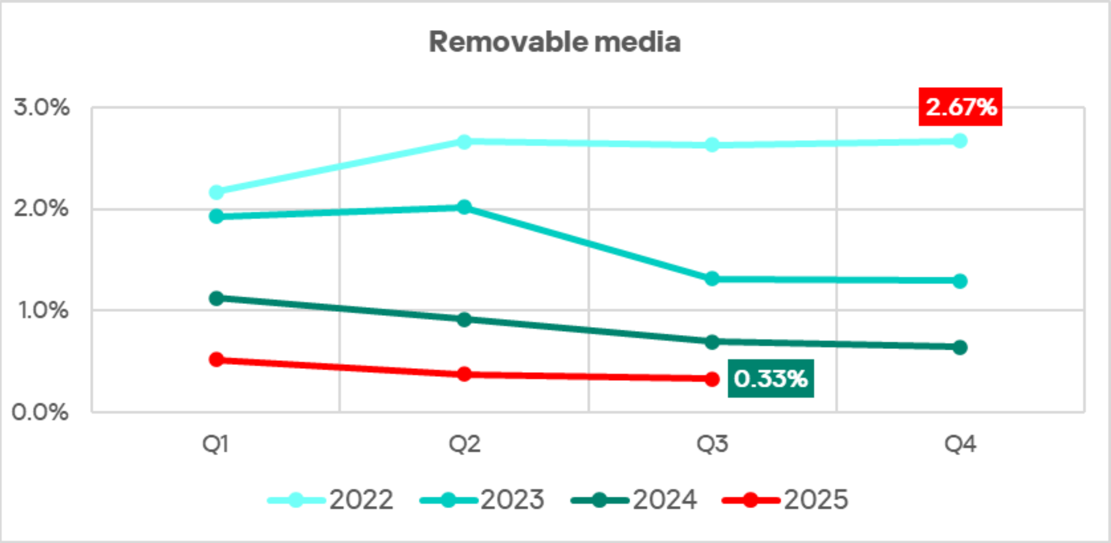
Despite the decrease in the global average rate of threats from the internet, it was still more than 2.6 times higher than the rate of threats from email clients. However, in some regions the difference was not that significant. For example, in Southern Europe the values were comparable: 6.97% and 6.85%, respectively. This region leads in the percentage of ICS computers on which threats from email clients were blocked.

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

Malicious scripts and phishing pages are primarily spread via the internet and phishing emails, but are also found in the next stages of attacks — to gain persistence in the system, collect data, and connect with C2 servers. In Q3 2025, this category of threats led in terms of growth for this indicator (+0.3 pp). Spyware was second in this rating (+0.2 pp).

In Q3 2025, the percentage of ICS computers on which threats from removable media were blocked reached its lowest level since the beginning of 2022 — 0.33%

Percentage of ICS computers on which threats from removable media were blocked, Q1 2022–Q3 2025



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

In Q3 2025, the percentage of ICS computers on which viruses and worms were blocked increased slightly.

Detecting specific threat categories

The two main categories of internet threats — denylisted internet resources and malicious scripts and phishing pages — are interrelated.

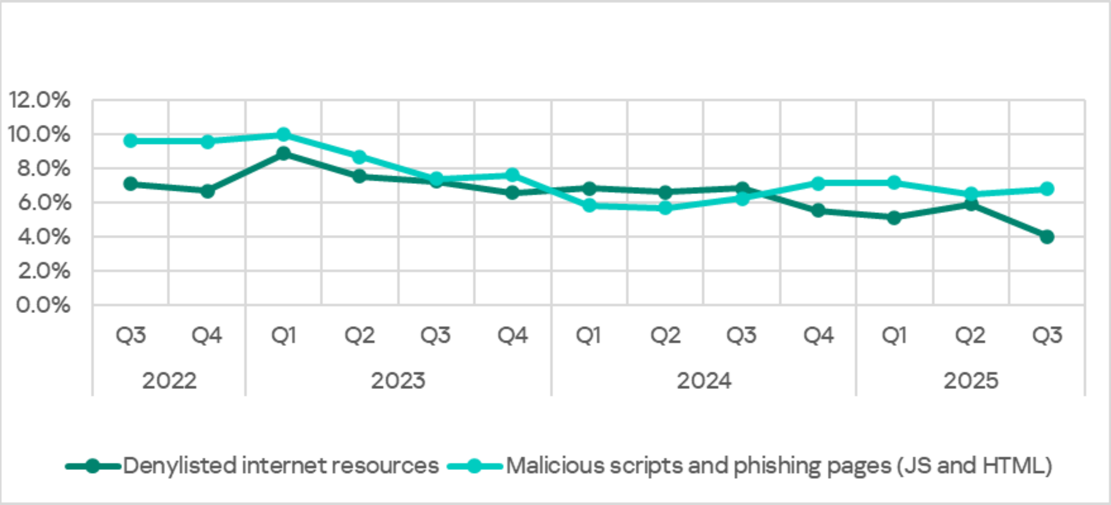
Many web resources included in denylists are used by attackers to propagate malicious scripts and phishing pages (HTML).

Addresses added to denylists are promptly distributed via KSN. This prevents malicious code from being downloaded, so it is not blocked as a malicious script or miner. As a result, the corresponding indicators decrease.

Attackers are constantly searching for and using new web resources and alternative techniques to propagate malicious code, which leads to an inevitable increase in script detection and a decrease in detection on denylisted internet resources at some point in the future.

These interdependencies are reflected in our statistics. You can see how these indicators fluctuate in opposite phases on a quarterly basis.

Percentage of ICS computers on which malicious objects were blocked, Q3 2022–Q3 2025

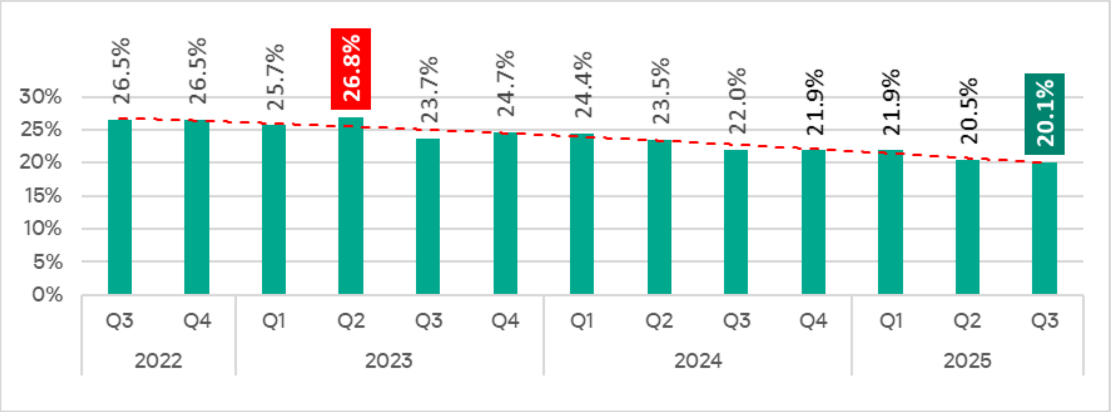


In Q3 2025, the malicious scripts and phishing pages category led the other threat categories in terms of both the percentage of ICS computers on which this threat was blocked and the growth rate.

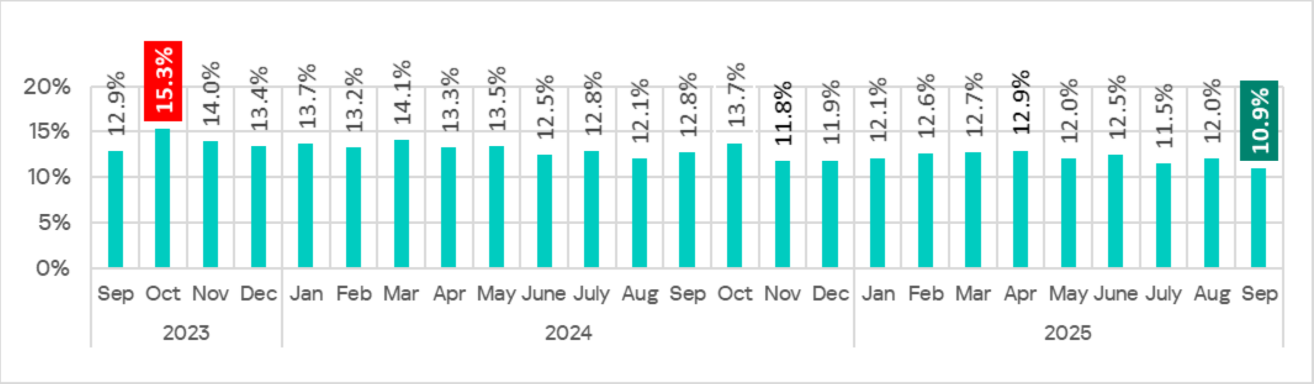
Statistics across all threats

In Q3 2025, the percentage of ICS computers on which malicious objects were blocked decreased by 0.4 pp from the previous quarter to 20.1%. This is the lowest level for the observed period.

Percentage of ICS computers on which malicious objects were blocked, Q3 2022–Q3 2025



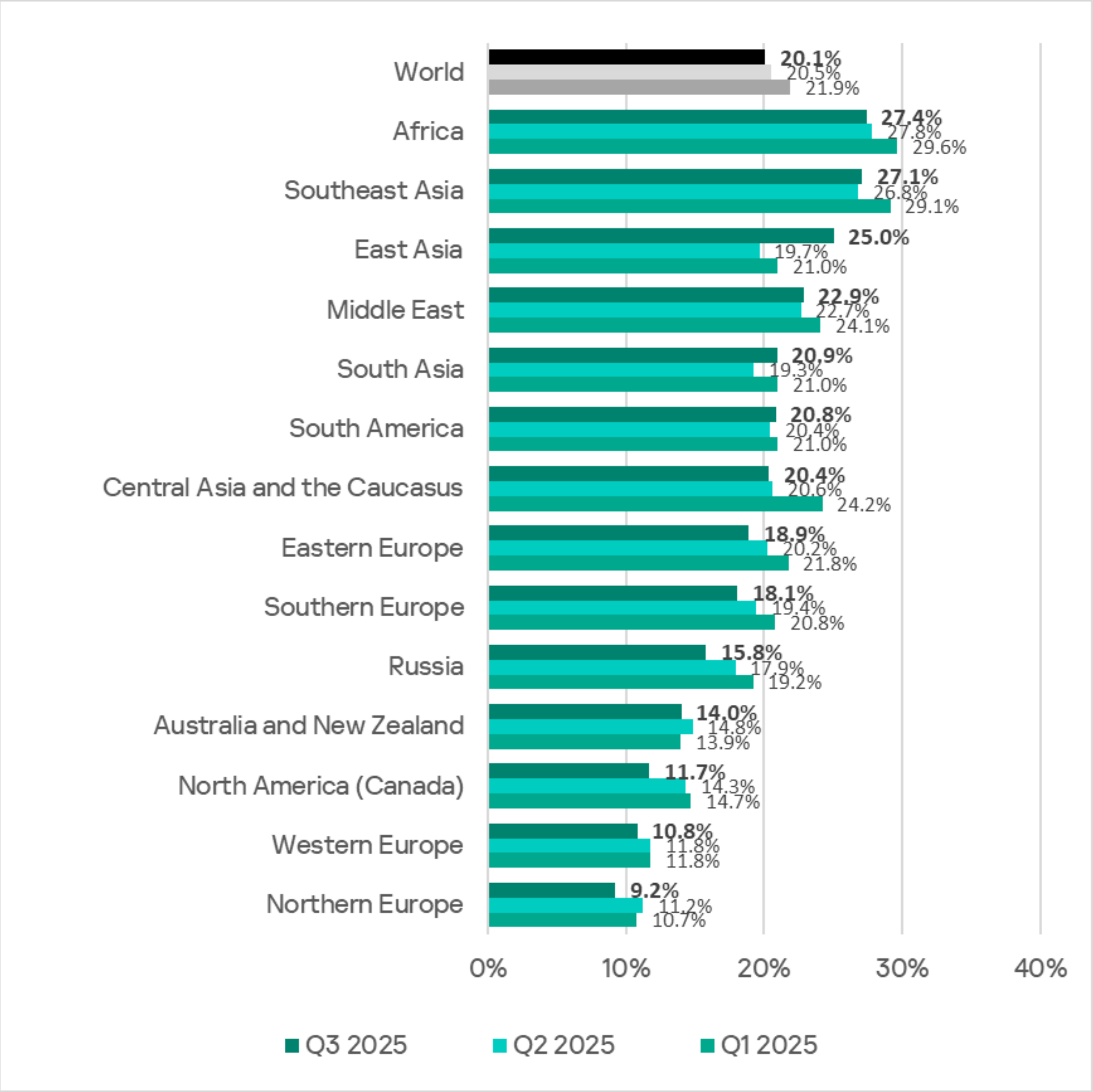
The highest percentage of ICS computers on which malicious objects were blocked during Q3 2025 occurred in August. In September, the rate was the lowest for two years.



Percentage of ICS computers on which malicious objects were blocked, September 2023—September 2025

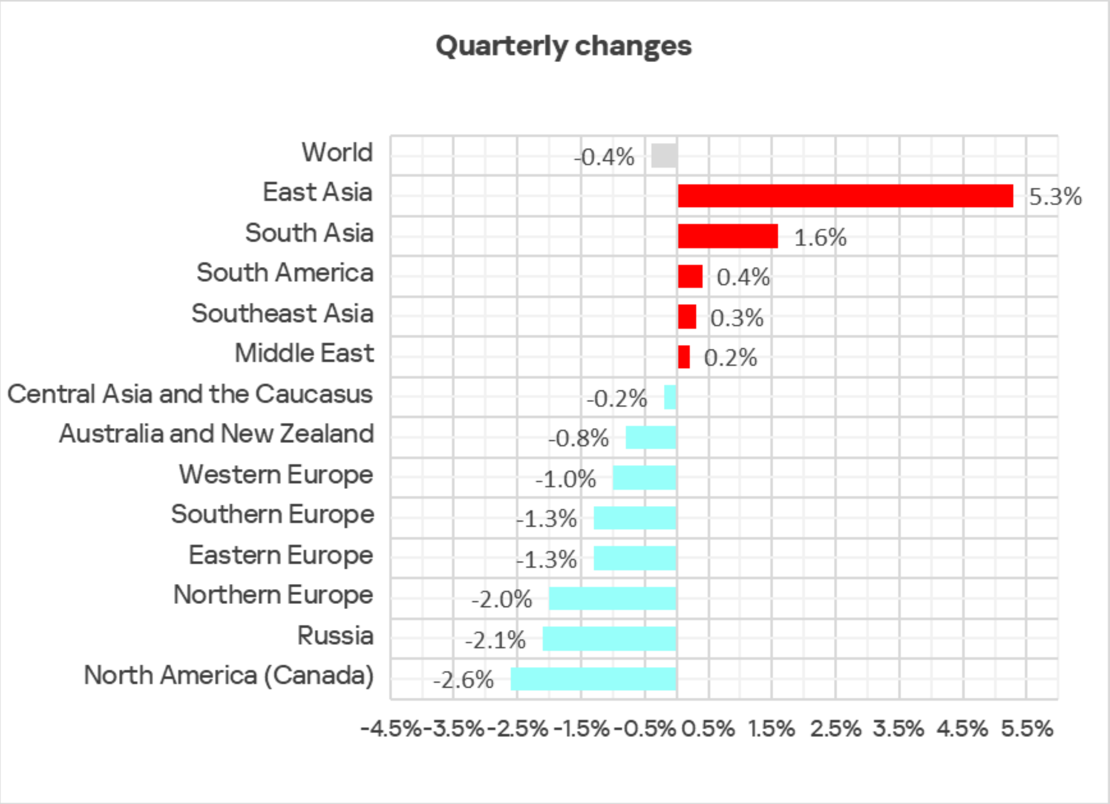
Regionally, the percentage of ICS computers on which malicious objects were blocked ranged from 9.2% in Northern Europe to 27.4% in Africa.

Regions ranked by percentage of ICS computers on which malicious objects were blocked, Q3 2025



In Q3 2025, the percentage increased in five regions. The most notable increase occurred in East Asia, triggered by the local spread of malicious scripts in the OT infrastructure of engineering organizations and ICS integrators.

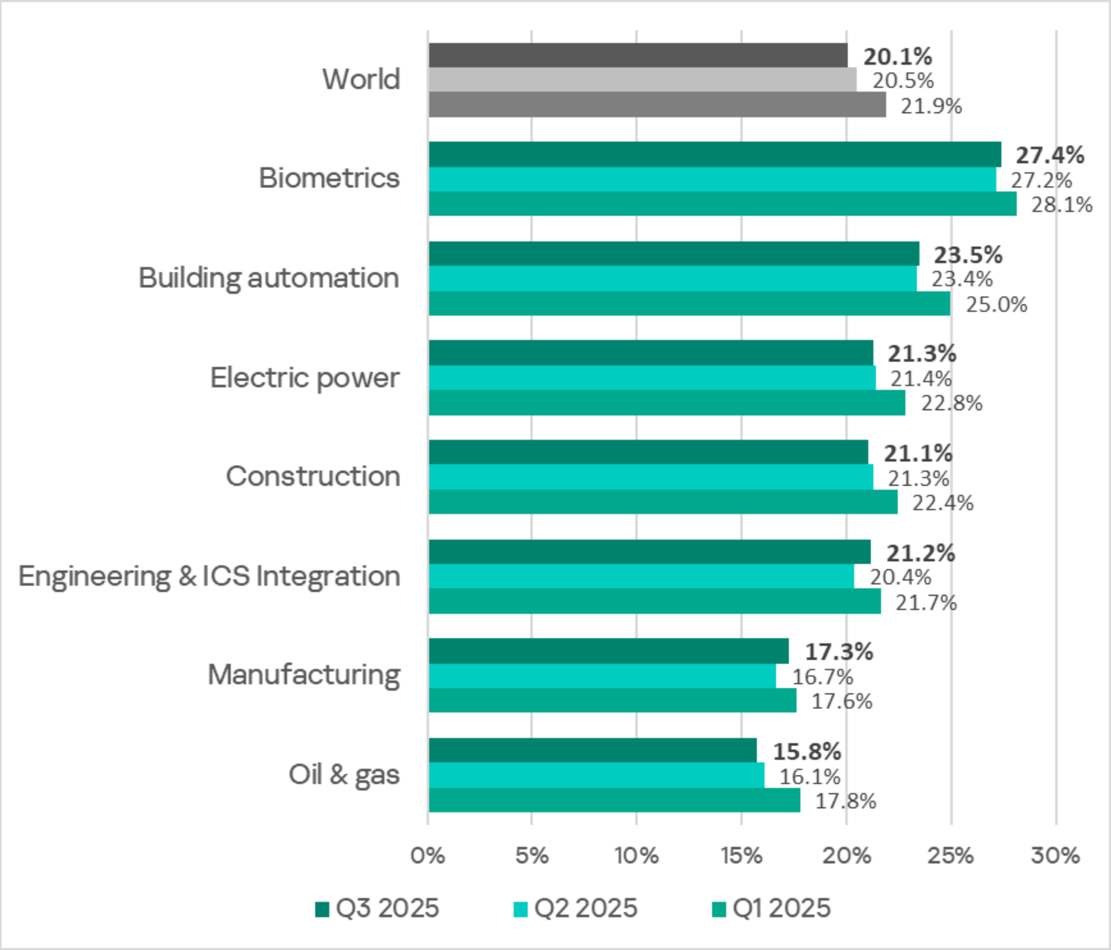
Changes in percentage of ICS computers on which malicious objects were blocked, Q3 2025



Selected industries

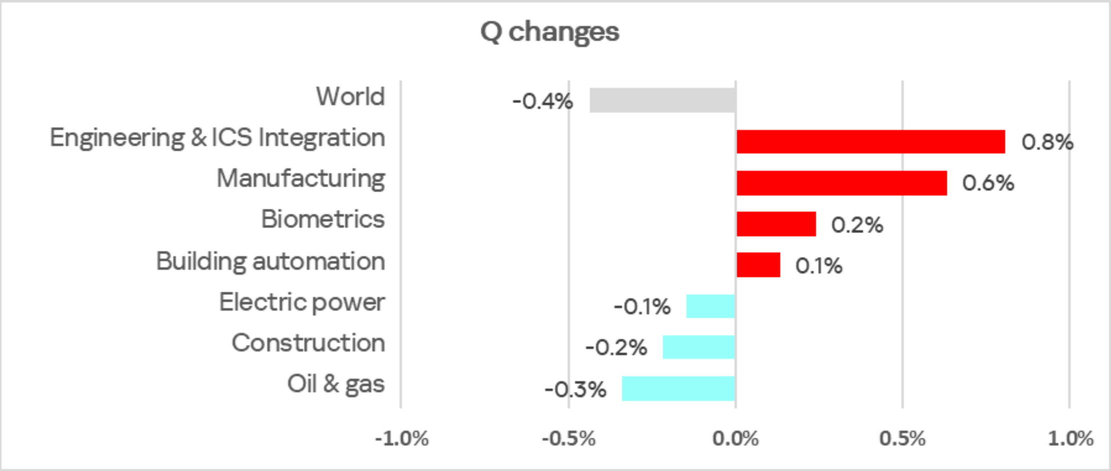
The biometrics sector traditionally led the ranking of the industries and OT infrastructures surveyed in this report in terms of the percentage of ICS computers on which malicious objects were blocked.

Ranking of industries and OT infrastructures by percentage of ICS computers on which malicious objects were blocked, Q3 2025

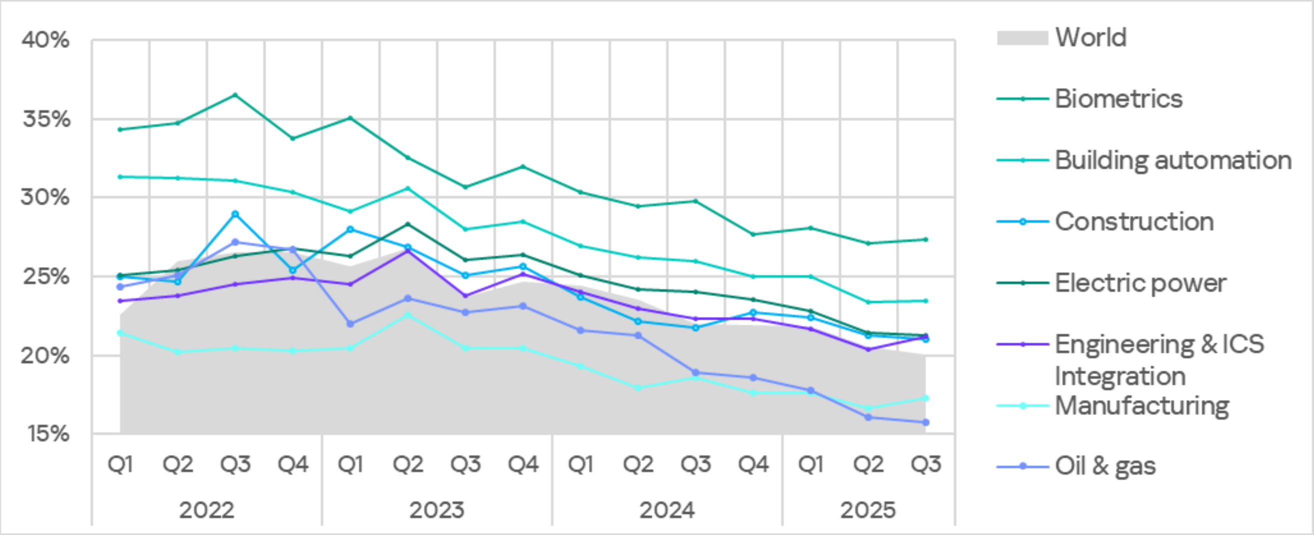


In Q3 2025, the percentage of ICS computers on which malicious objects were blocked increased in four of the seven surveyed industries. The most notable increases were in engineering and ICS integrators, and manufacturing.

Changes in percentage of ICS computers on which malicious objects were blocked in selected industries, Q3 2025



In all surveyed industries, there is a downward trend relative to the peak values seen in Q3 of 2022.



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.

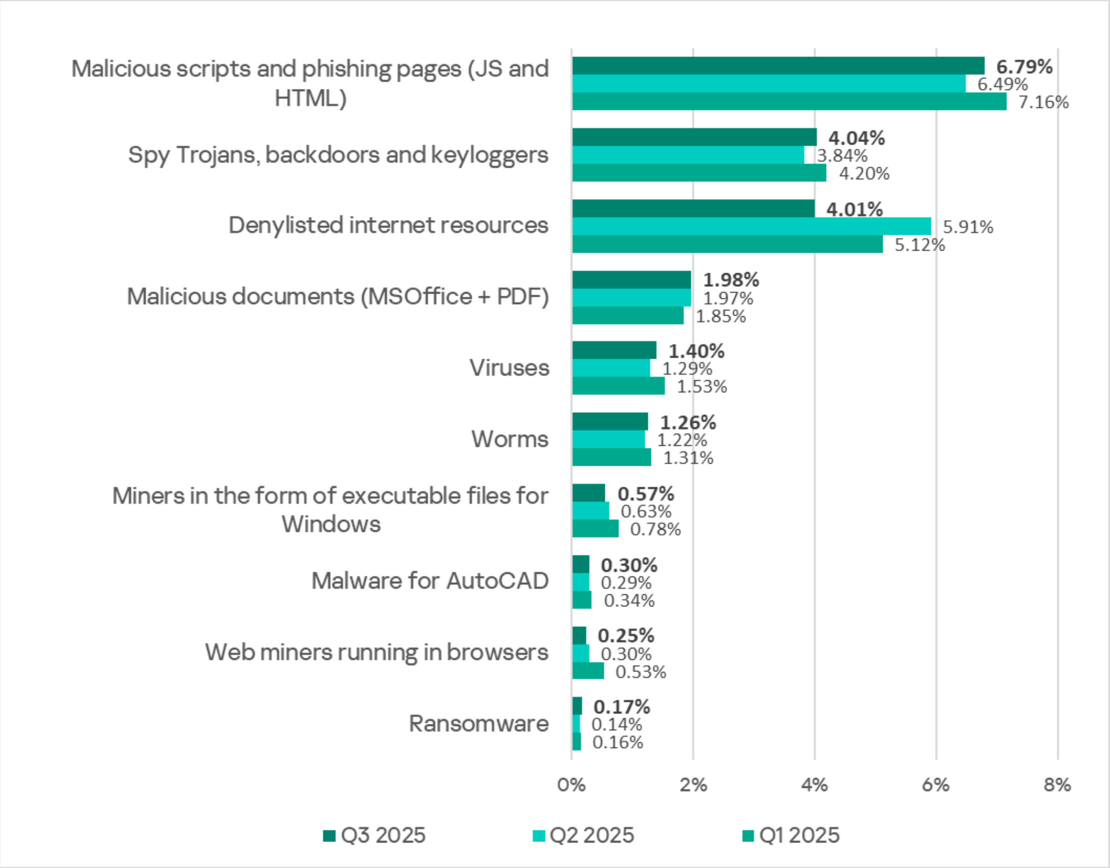
Malware for AutoCAD does not belong to a specific group, as it can spread in a variety of ways.

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.

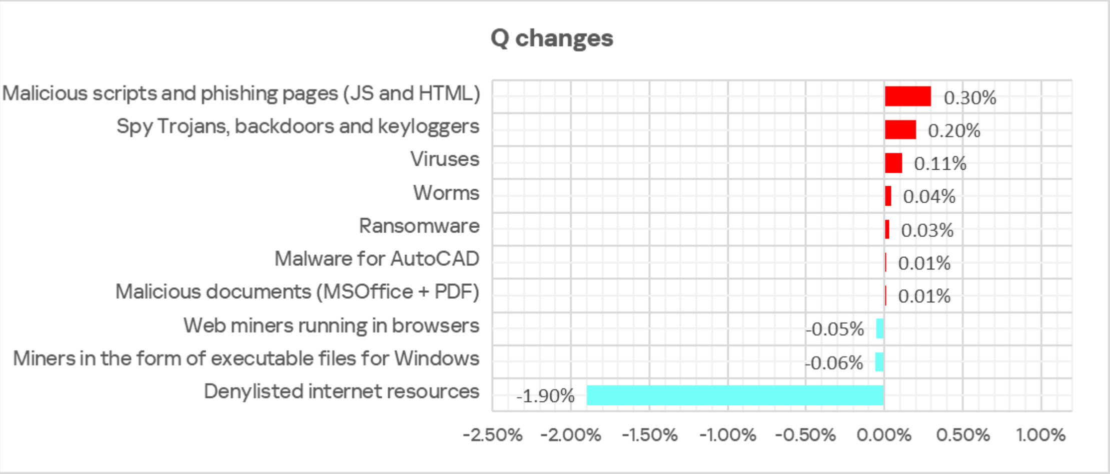
In Q3 2025, the malicious scripts and phishing pages category led the other threat categories in terms of the percentage of ICS computers on which this threat was blocked. Spyware ranked second.

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



In Q3 2025, there was a decrease in the percentage of ICS computers on which denylisted internet resources and miners of both categories were blocked. These were the only categories that exhibited a decrease.

Changes in percentage of ICS computers on which malicious objects from different categories were blocked, Q3 2025



After an increase in the previous quarter, the percentage of ICS computers on which denylisted internet resources were blocked decreased by 1.9 pp. Consequently, this category dropped from second to third place in the threat category ranking.

Threat categories

In Q3 2025, Kaspersky protection solutions blocked malware from 11,356 different malware families of various categories on industrial automation systems.

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

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:

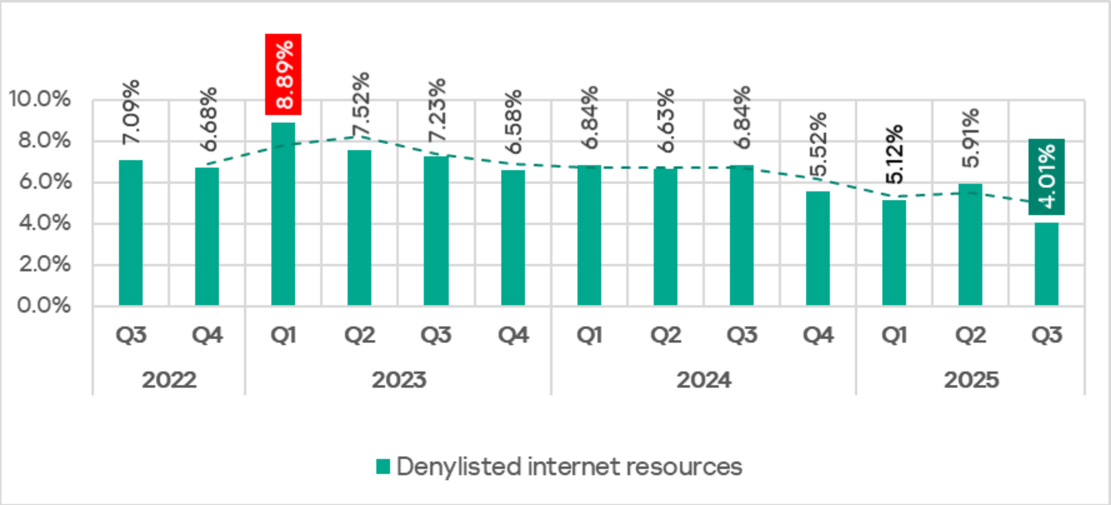
- Known malicious URLs and IP addresses used by threat actors to host payloads and configurations.
- Suspicious (insecure) web resources with entertainment and gaming content, often used to deliver unwanted software, crypto miners and malicious scripts.
- CDN nodes used by attackers to distribute malicious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

A significant portion of these resources is used to distribute malicious scripts and phishing pages (HTML).

A detected malicious web resource may not always be easily added to a denylist because attackers are increasingly using legitimate internet resources and services such as content delivery network (CDN) platforms, messengers, repositories, 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.

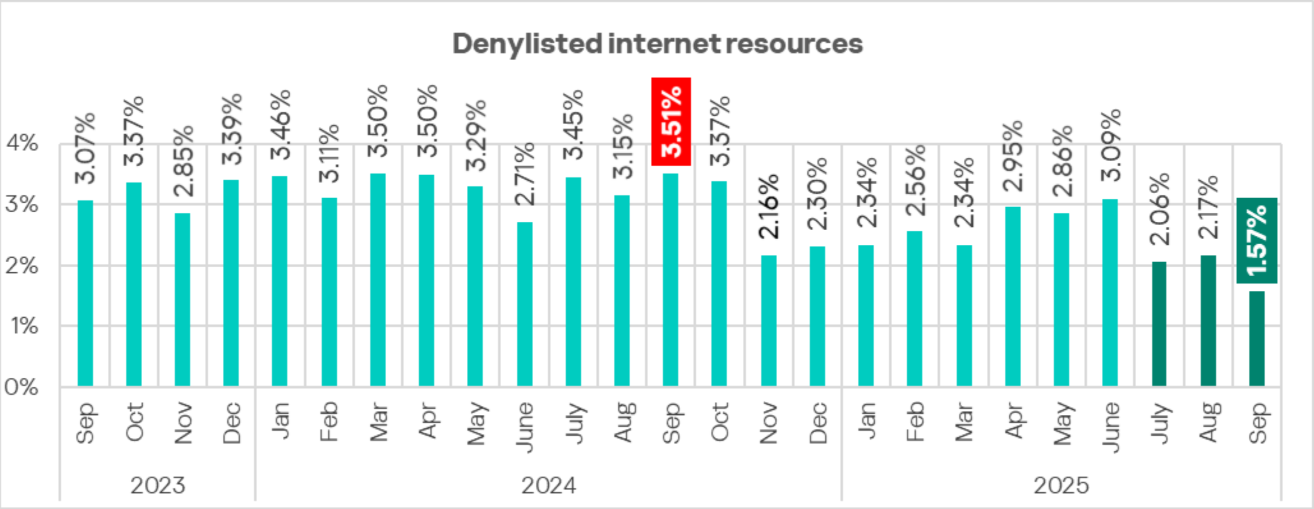
High parameter values usually indicate weak control over the implementation of information security policies (ICS computers have access to the internet in one way or another), phishing protection weaknesses (many malicious links are delivered via phishing messages) and deficiencies in information security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

In Q3 2025, the percentage of ICS computers on which denylisted internet resources were blocked decreased to 4.01%. This is the lowest quarterly figure since the beginning of 2022. This category dropped from second to third place in the ranking of threat categories by percentage of ICS computers on which they were blocked.



Percentage of ICS computers on which denylisted internet resources were blocked, Q3 2022–Q3 2025

During the quarter, the percentage of ICS computers on which denylisted internet resources were blocked was highest in August. The monthly figure in September was the lowest in three years.

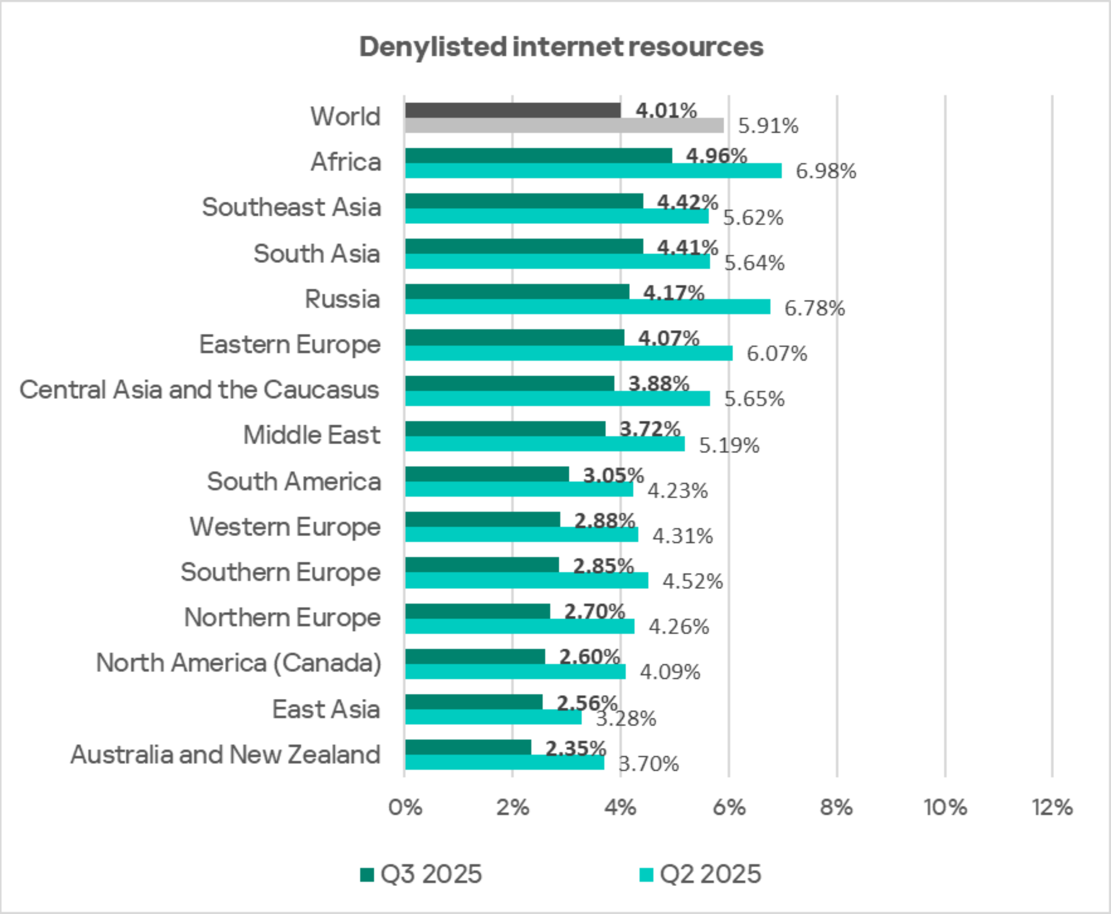


Percentage of ICS computers on which denylisted internet resources were blocked, September 2023—September 2025

Regionally, the percentage of ICS computers on which denylisted internet resources were blocked ranged from 2.35% in Australia and New Zealand to

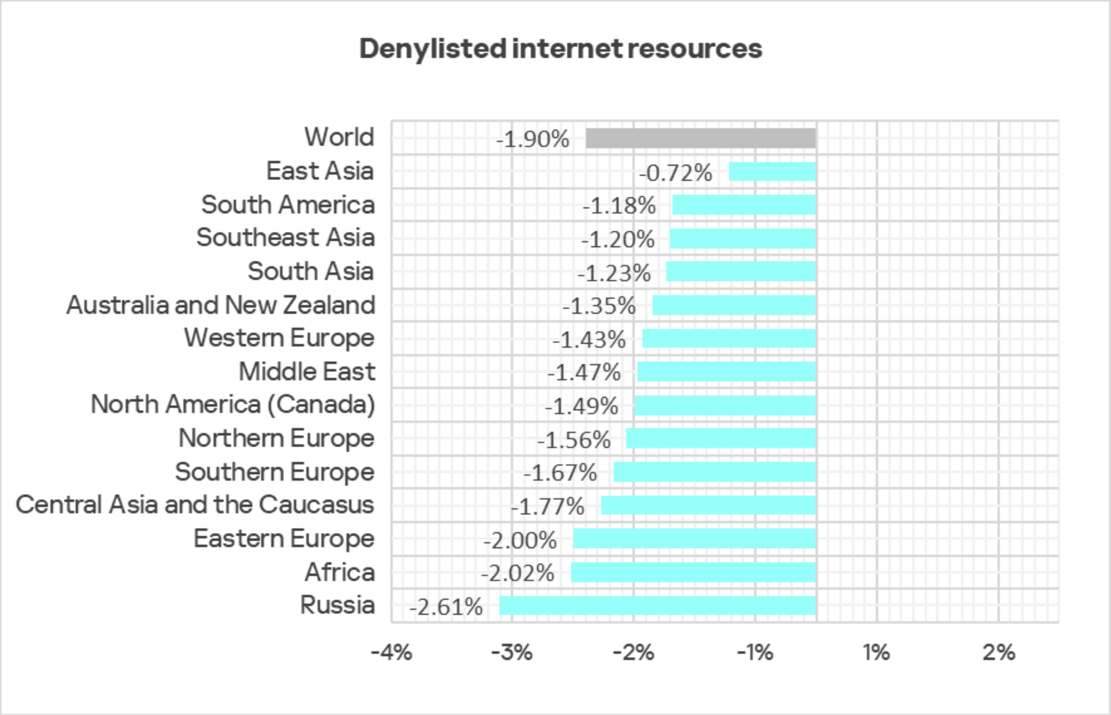
4.96% in Africa. Southeast Asia and South Asia were also among the top three regions for this indicator.

Regions ranked by percentage of ICS computers on which denylisted internet resources were blocked, Q3 2025



After an increase in the previous quarter, this indicator decreased in all regions in Q3 2025.

Changes in percentage of ICS computers on which denylisted internet resources were blocked, Q3 2025

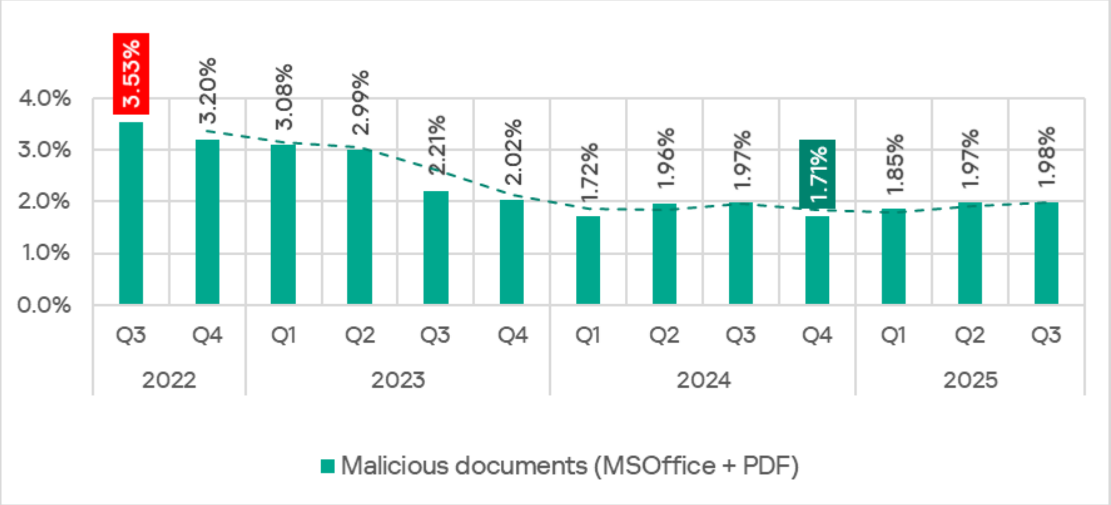


Malicious documents (MSOffice + PDF)

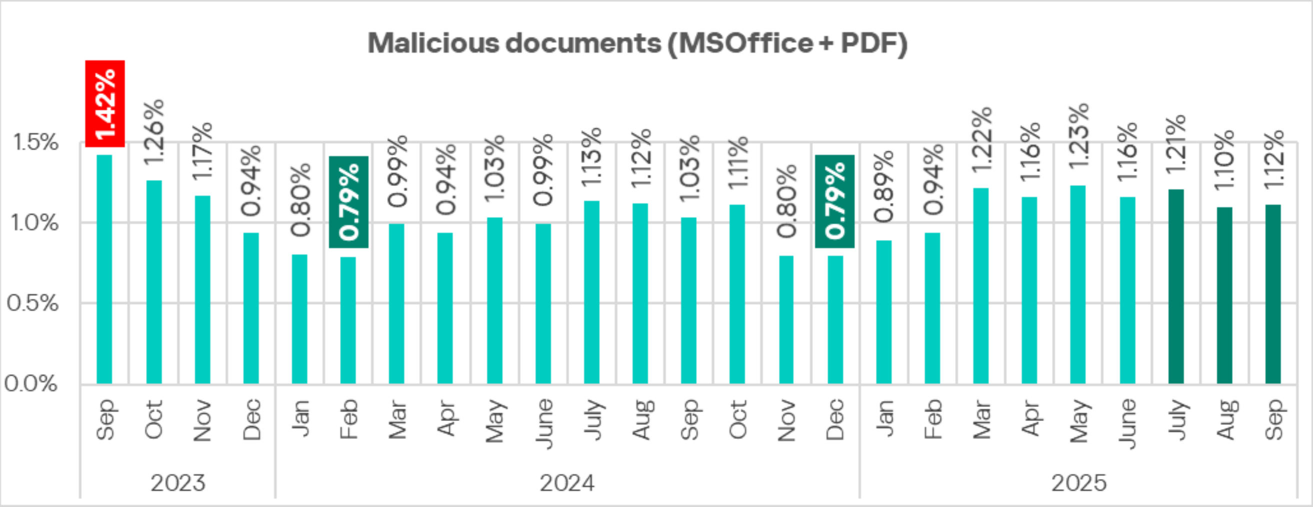
Attackers mainly send malicious documents attached to phishing messages and use them in attacks aimed at initial infection of computers. Malicious documents typically contain exploits, malicious macros, and malware links.

Following a decline at the end of 2024, the percentage of ICS computers on which malicious documents were blocked has grown for three consecutive quarters.

Percentage of ICS computers on which malicious documents were blocked, Q3 2022– Q3 2025



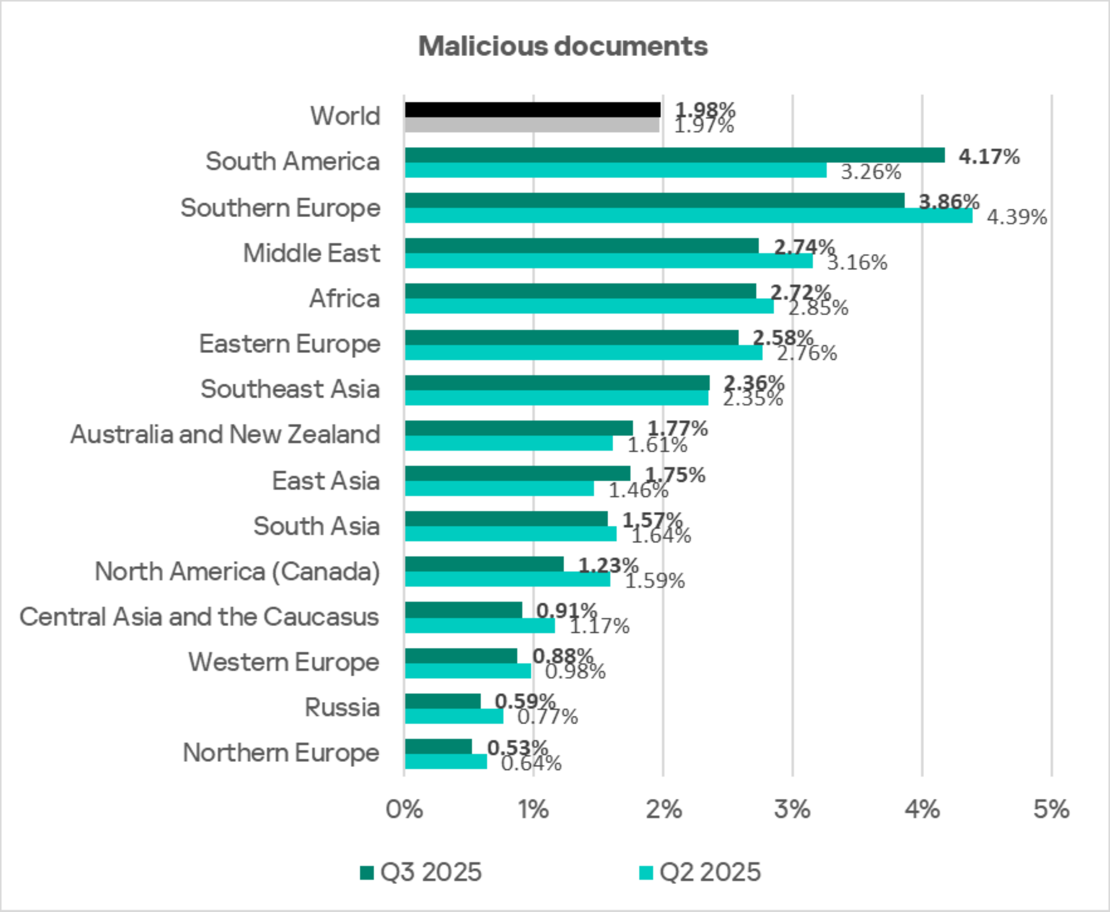
The monthly value of this indicator in Q3 2025 was highest in July.



Percentage of ICS computers on which malicious documents were blocked, September 2023—September 2025

Regionally, the percentage of ICS computers on which malicious documents were blocked ranged from 0.53% in Northern Europe to 4.17% in South America. South America, Southern Europe, and the Middle East remained the top three regions for this indicator.

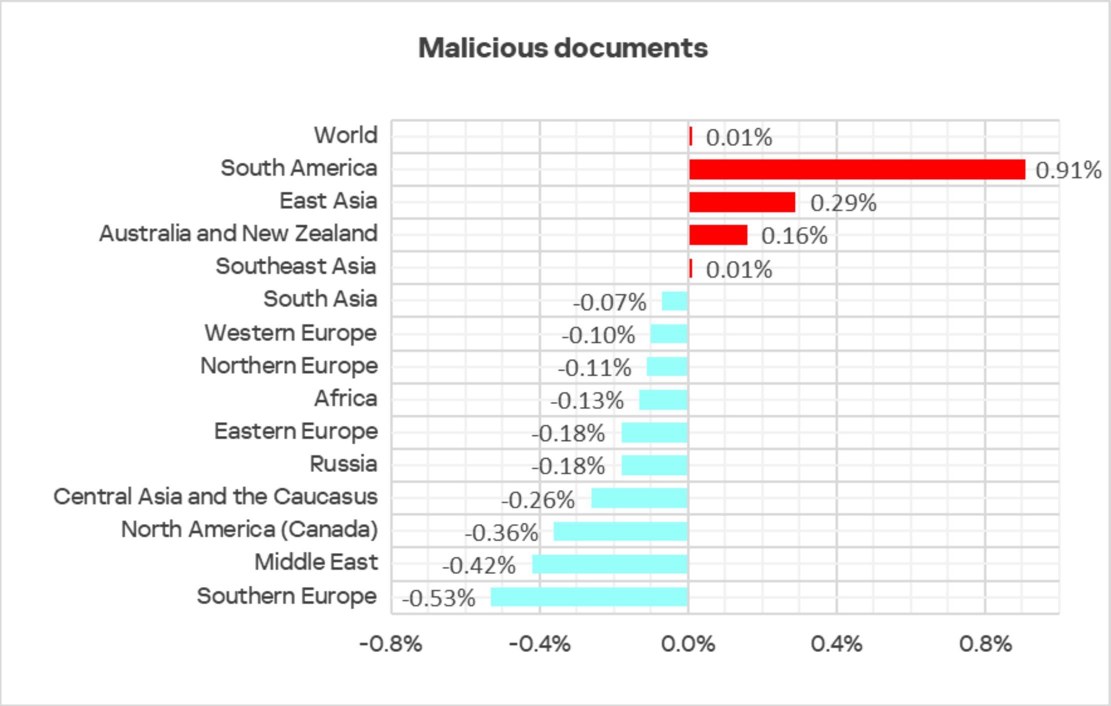
Regions ranked by percentage of ICS computers on which malicious documents were blocked, Q3 2025



In Q3 2025, the indicator increased in four regions — South America, East Asia, Southeast Asia, and Australia and New Zealand. South America saw the largest increase as a result of a large-scale phishing campaign in which attackers used new exploits for an old vulnerability (CVE-2017-11882) in Microsoft Office Equation Editor to deliver various spyware to victims' computers.

It is noteworthy that the attackers in this phishing campaign used localized Spanish-language email texts disguised as business correspondence.

Changes in percentage of ICS computers on which malicious documents were blocked, Q3 2025

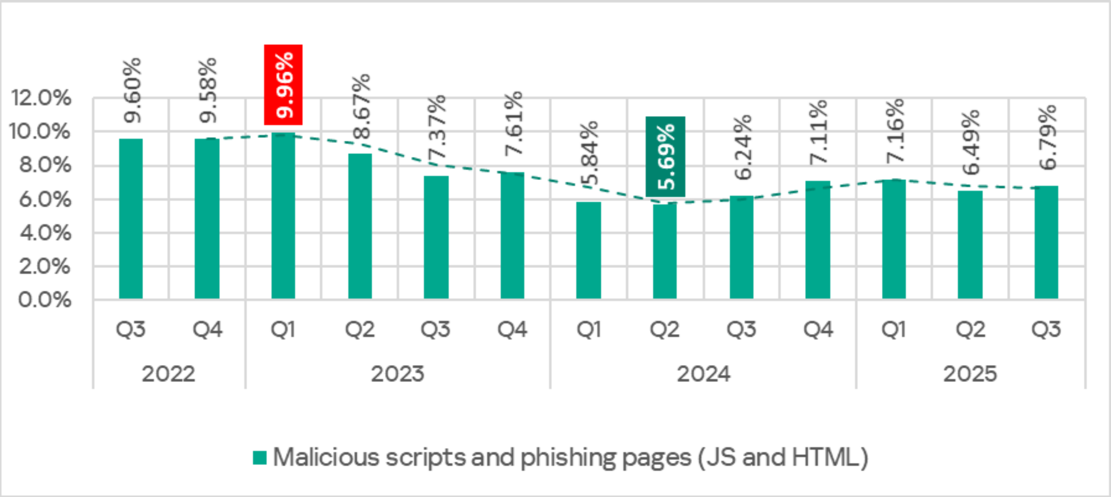


Malicious scripts and phishing pages (JS and HTML)

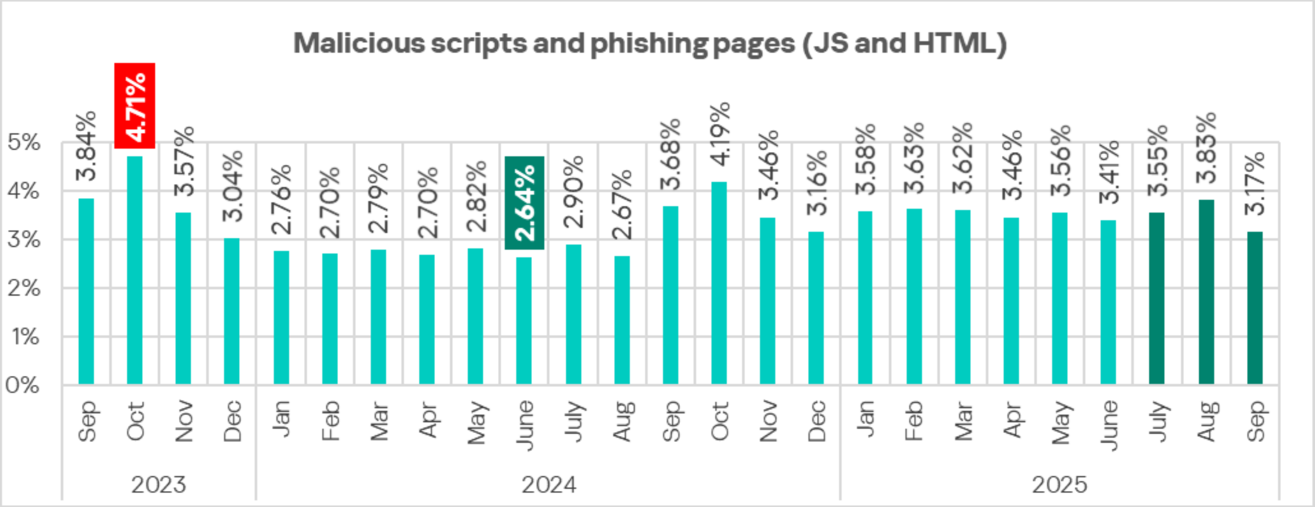
Malicious actors use scripts for a wide range of objectives: collecting information, tracking, redirecting the browser to a malicious site, and uploading various types of malware (spyware, silent crypto mining tools, ransomware) to the user's system or browser. These spread via the internet and email.

In Q3 2025, the percentage of ICS computers on which malicious scripts and phishing pages were blocked increased to 6.79%. This category led the ranking of threat categories in terms of percentage of ICS computers on which they were blocked.

Percentage of ICS computers on which malicious scripts and phishing pages were blocked, Q3 2022–Q3 2025



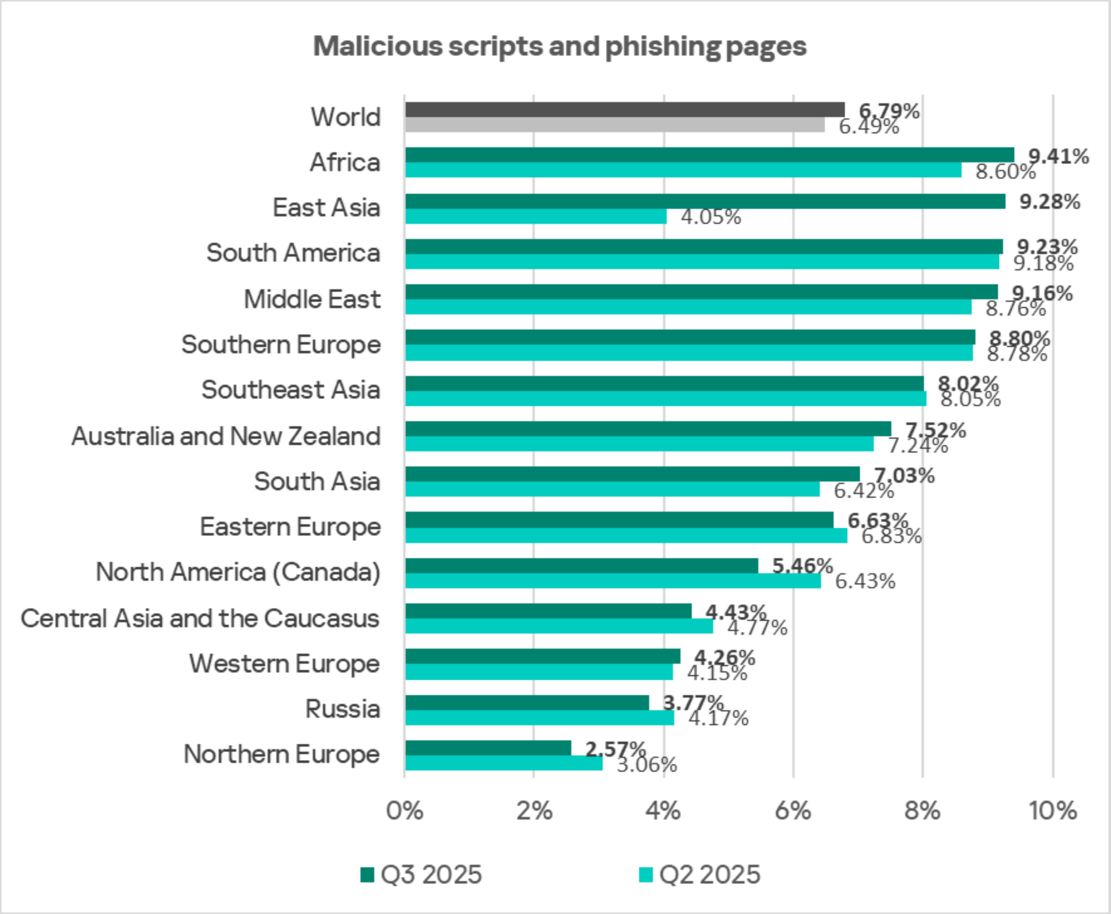
The highest monthly value of this indicator in Q3 2025 was in August.



Percentage of ICS computers on which malicious scripts and phishing pages were blocked, September 2023—September 2025

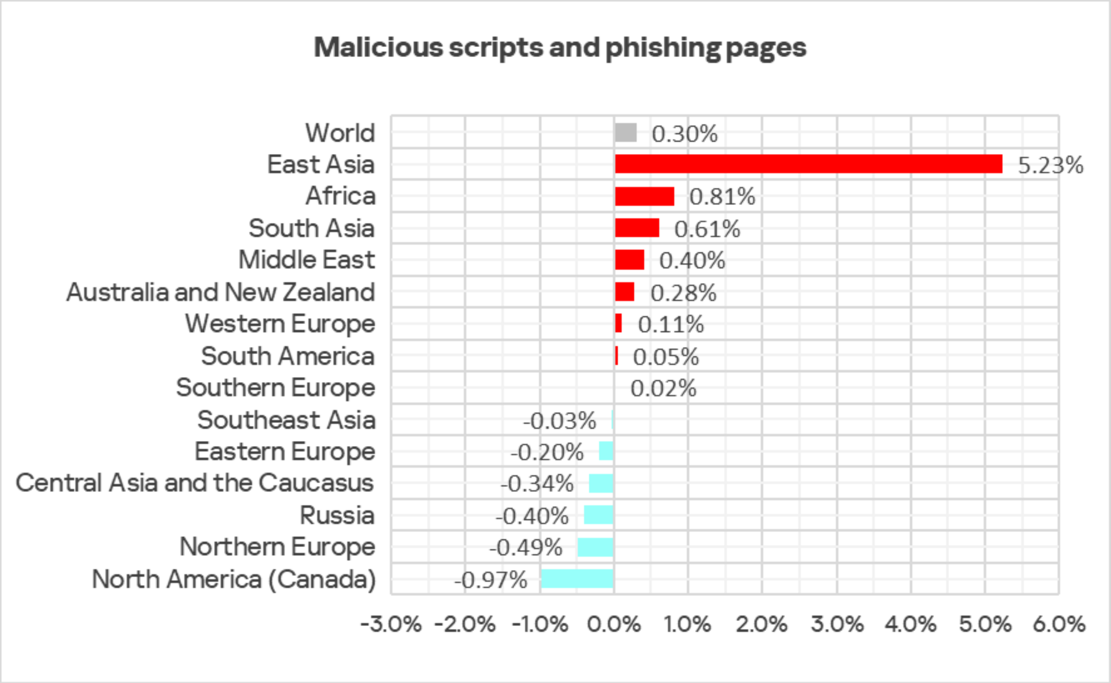
Regionally, the percentage of ICS computers on which malicious scripts and phishing pages were blocked ranged from 2.57% in Northern Europe to 9.41% in Africa. The top three regions for this indicator were Africa, East Asia, and South America.

Regions ranked by percentage of ICS computers on which malicious scripts and phishing pages were blocked, Q3 2025



Regionally, the indicator increased the most in East Asia (by a dramatic 5.23 pp) as a result of the local spread of malicious spyware scripts loaded into the memory of popular torrent clients including MediaGet.

Changes in percentage of ICS computers on which malicious scripts and phishing pages were blocked, Q3 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

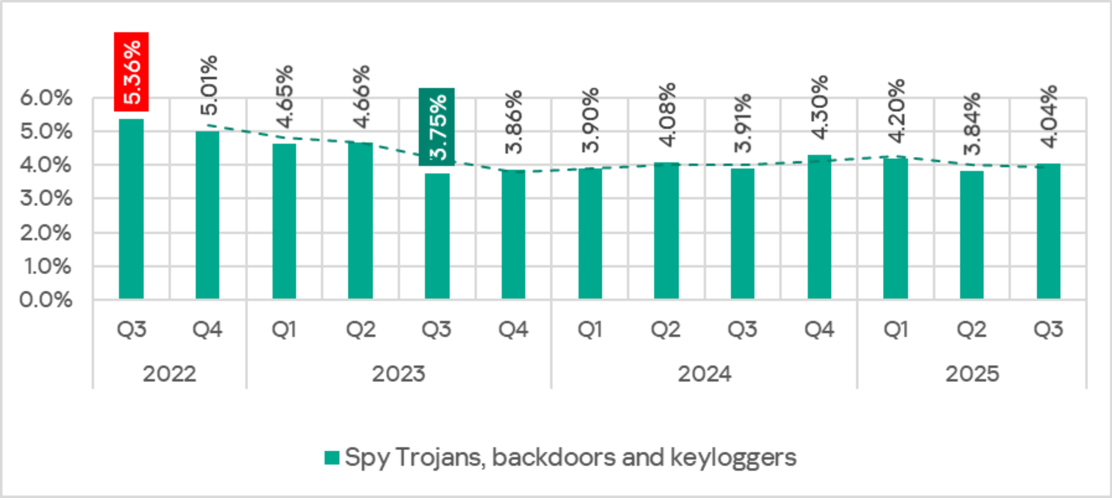
Spyware (spy Trojans, backdoors, and keyloggers) can be found in lots of phishing emails sent to industrial organizations. Spyware is the most frequently detected next-stage malware. It is used as a tool for the intermediate stages of a cyberattack (for example, intelligence and distribution over the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

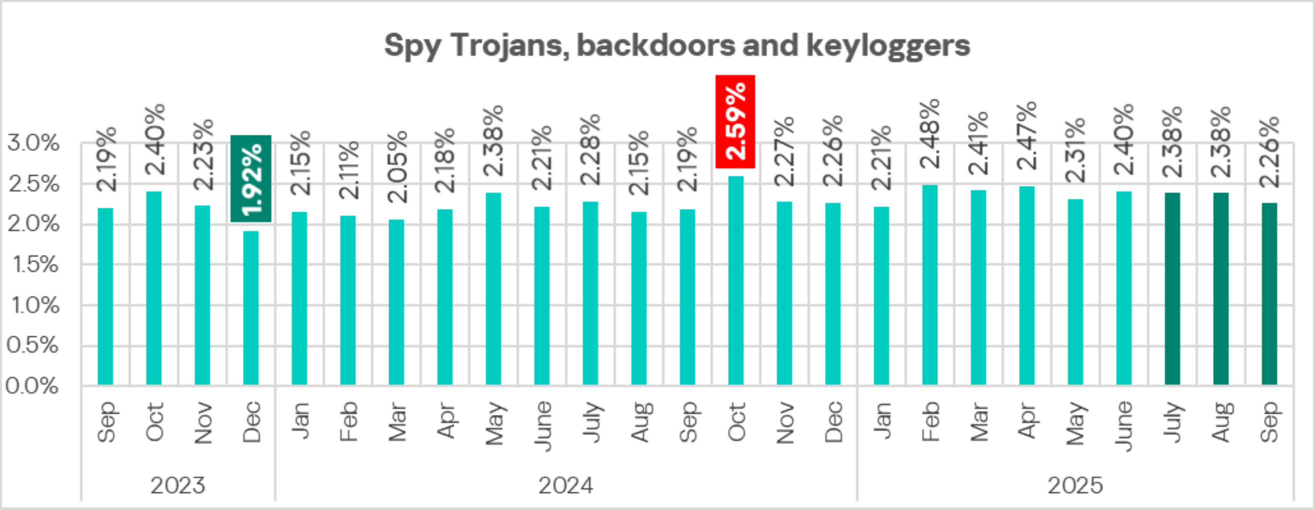
Detection of spyware on an ICS computer usually indicates that the initial infection vector has worked, whether it is clicking on a malicious link, opening an attachment from a phishing email, or connecting an infected USB drive. This indicates the absence or ineffectiveness of measures to protect the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

In Q3 2025, the percentage of ICS computers on which spyware was blocked increased to 4.04%. While this was not the highest figure during the period under review, it was the first time that spyware took second place in the ranking of threat categories in terms of the percentage of ICS computers on which it was blocked.

Percentage of ICS computers on which spyware was blocked, Q3 2022–Q3 2025



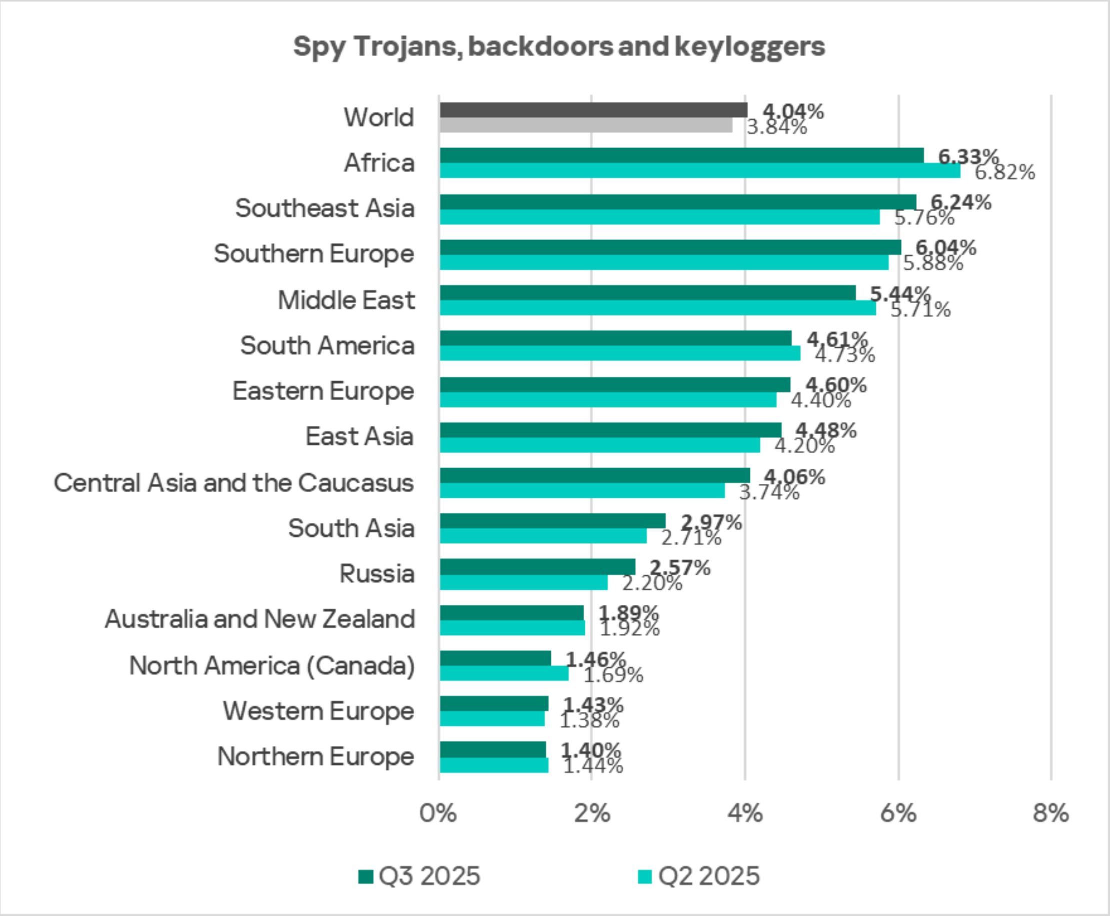
The monthly value did not change in July or August, but decreased in September.



Percentage of ICS computers on which spyware was blocked, September 2023—September 2025

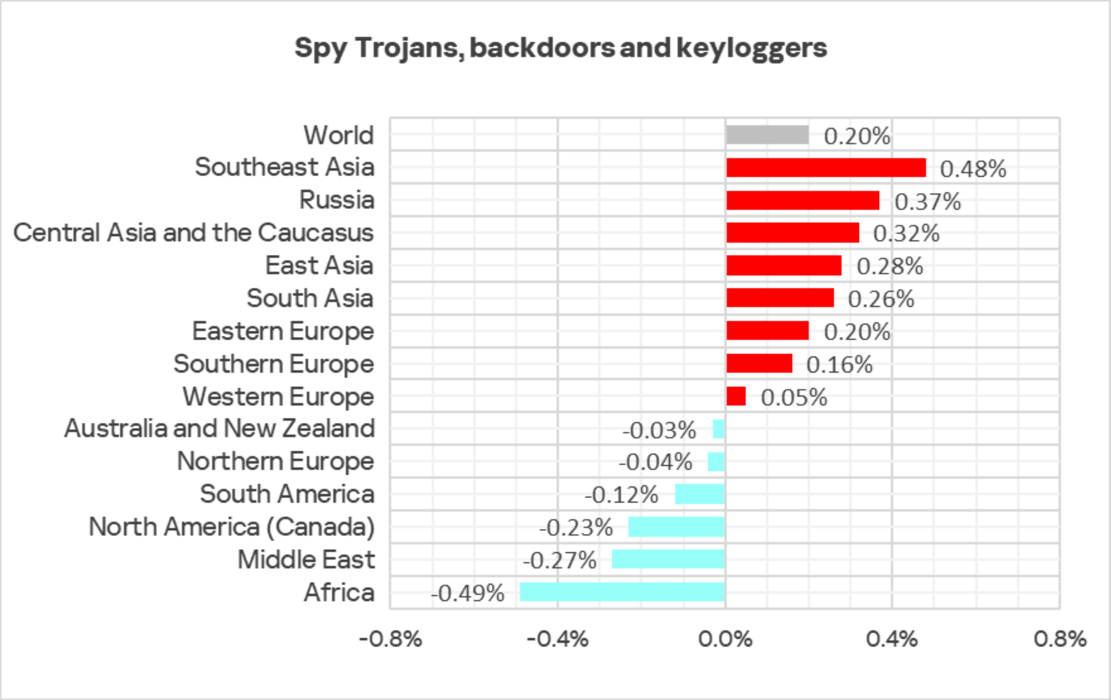
Regionally, the percentage of ICS computers on which spyware was blocked ranged from 1.40% in Northern Europe to 6.33% in Africa. As in the previous quarter, the top three regions for this indicator were Africa, Southeast Asia and Southern Europe.

Regions ranked by percentage of ICS computers on which spyware was blocked, Q3 2025



The percentage increased in eight regions in Q3 2025. The most notable increases were in Southeast Asia, Russia, and Central Asia and the South Caucasus.

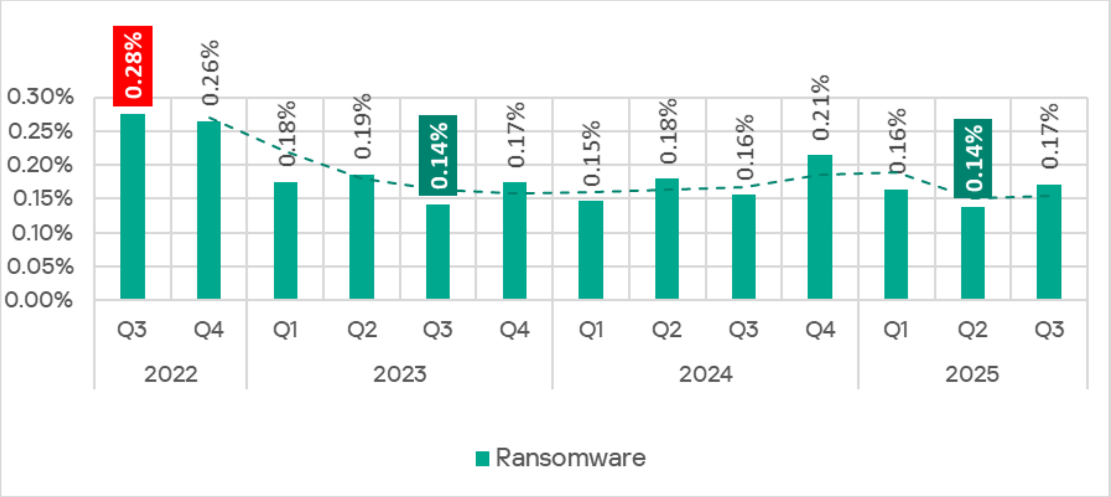
Changes in percentage of ICS computers on which spyware was blocked, Q3 2025



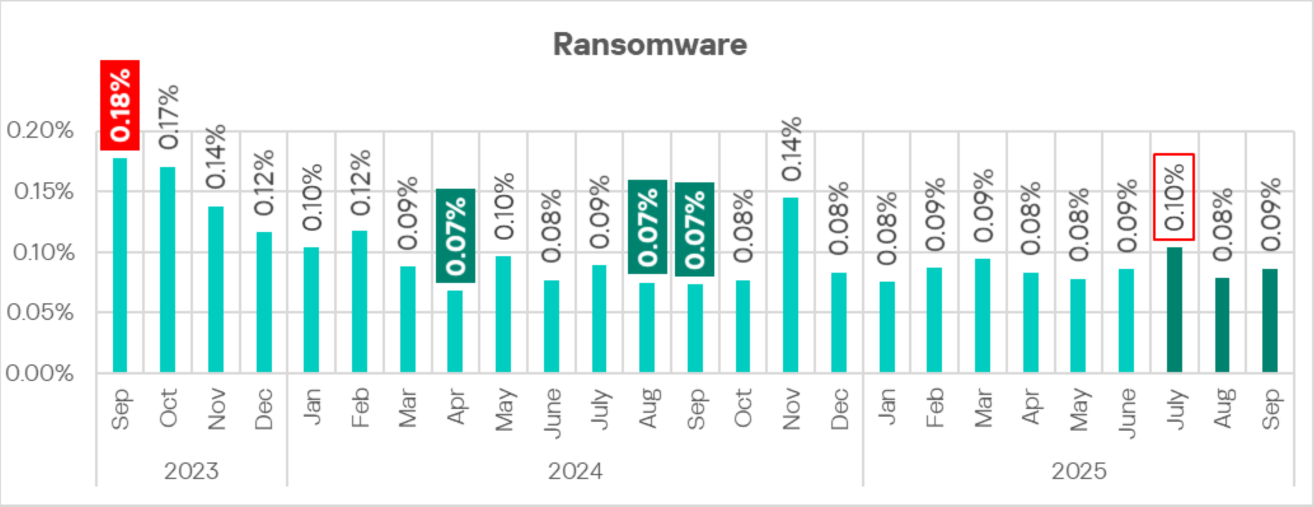
Ransomware

In Q3 2025, the percentage of ICS computers on which ransomware was blocked increased to 0.17%. This figure is slightly higher than that of Q1 2025.

Percentage of ICS computers on which ransomware was blocked, Q3 2022–Q3 2025

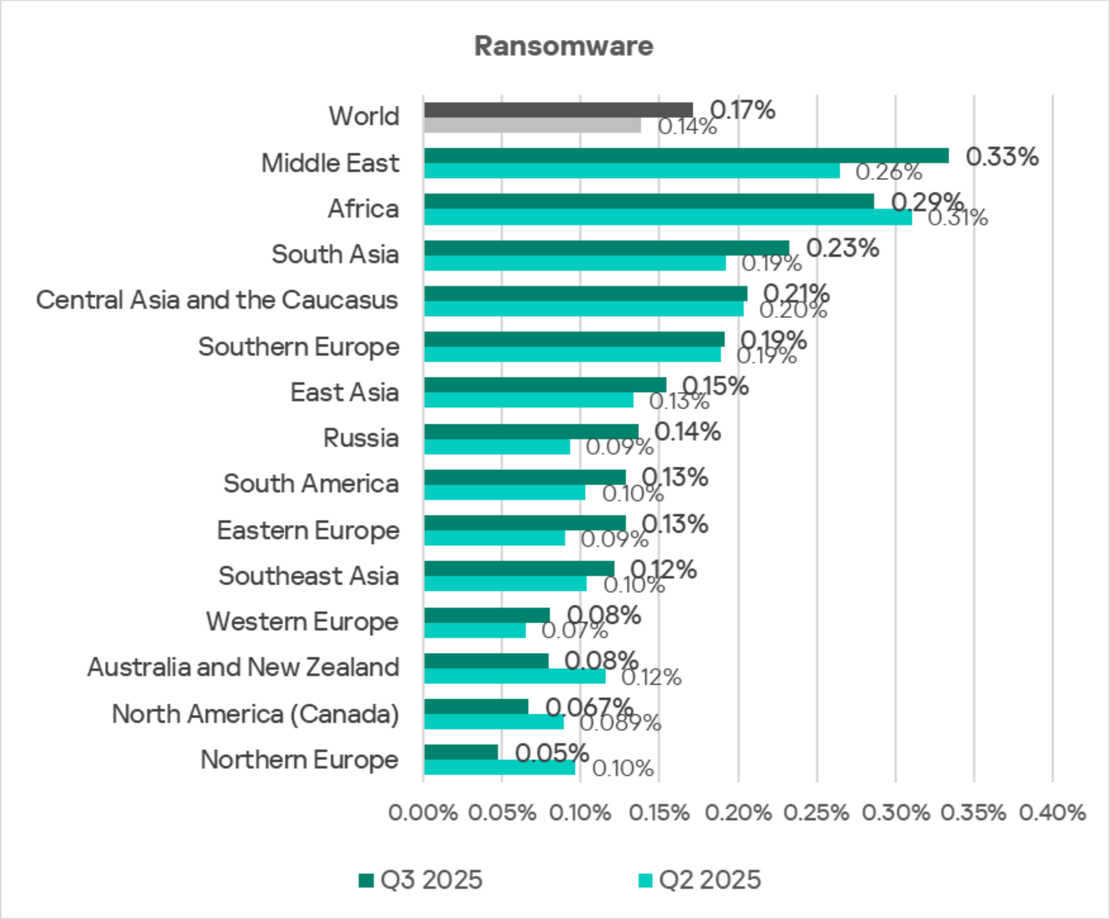


July’s monthly value was the highest since December of 2024. The values for August and September are comparable to those of previous months in 2025.



Percentage of ICS computers on which ransomware was blocked, September 2023—September 2025

Regionally, the percentage of ICS computers on which ransomware was blocked ranged from 0.05% in Northern Europe to 0.33% in the Middle East, which lead the ranking again. The top three regions for this indicator were the Middle East, Africa, and South Asia.

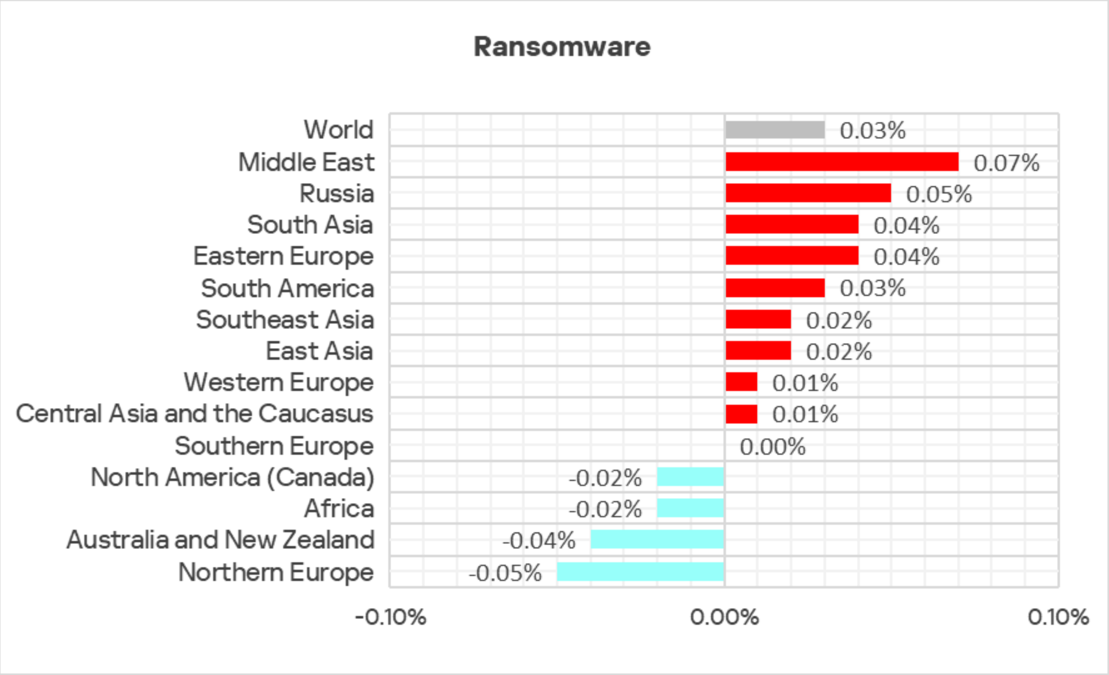


Regions ranked by percentage of ICS computers on which ransomware was blocked, Q3 2025

In Q3 2025, the percentage of ICS computers on which ransomware was blocked increased in nine regions. The Middle East was the leader in terms of growth for this indicator.

In this region, the percentage of ICS computers on which ransomware was blocked saw significant growth in the oil and gas industry, as well as in building automation, engineering and ICS integration. The malware was distributed under the guise of remote access client software, pirated games, and hacked licensed applications, including those used in biometric systems, building automation, and engineering.

Changes in percentage of ICS computers on which ransomware was blocked, Q3 2025

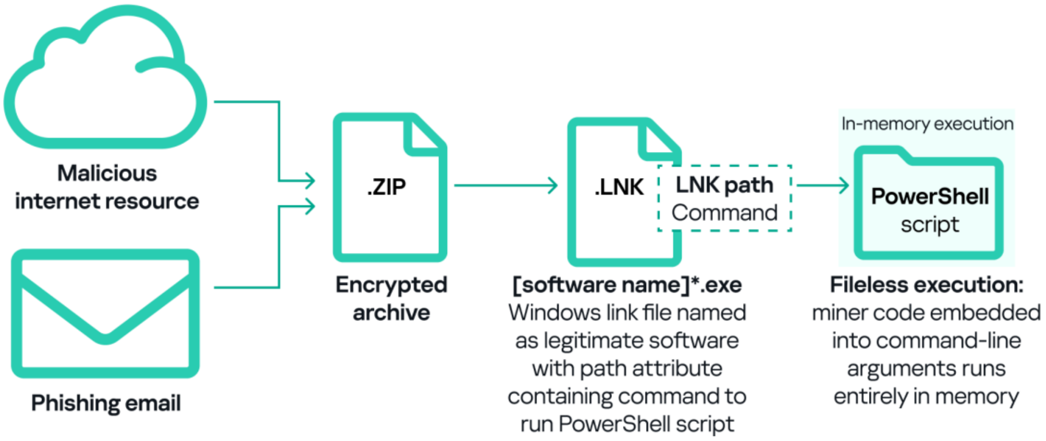


Miners in the form of executable files for Windows

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.

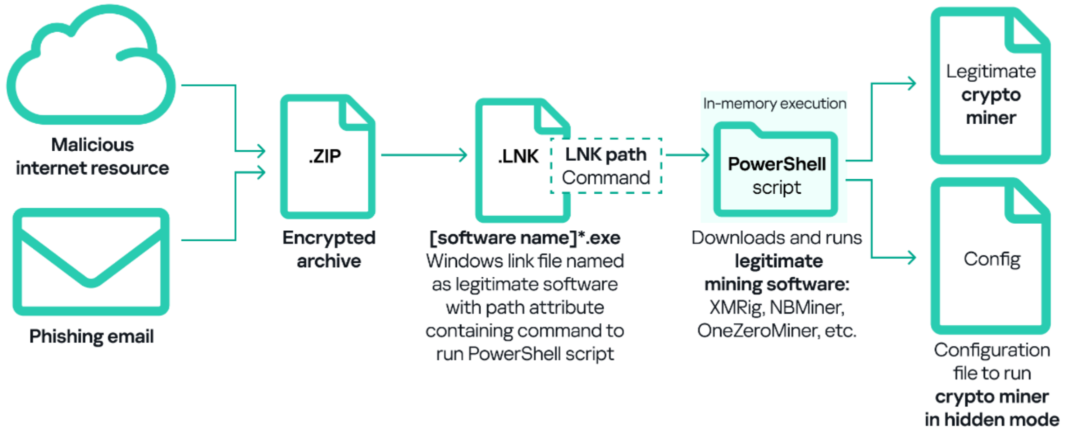
A significant portion of the Windows miners found on ICS computers consisted of archives with names that mimicked legitimate software. These archives did not contain actual software, but did include a Windows LNK file, commonly known as a shortcut. However, the target (or path) that the LNK file points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

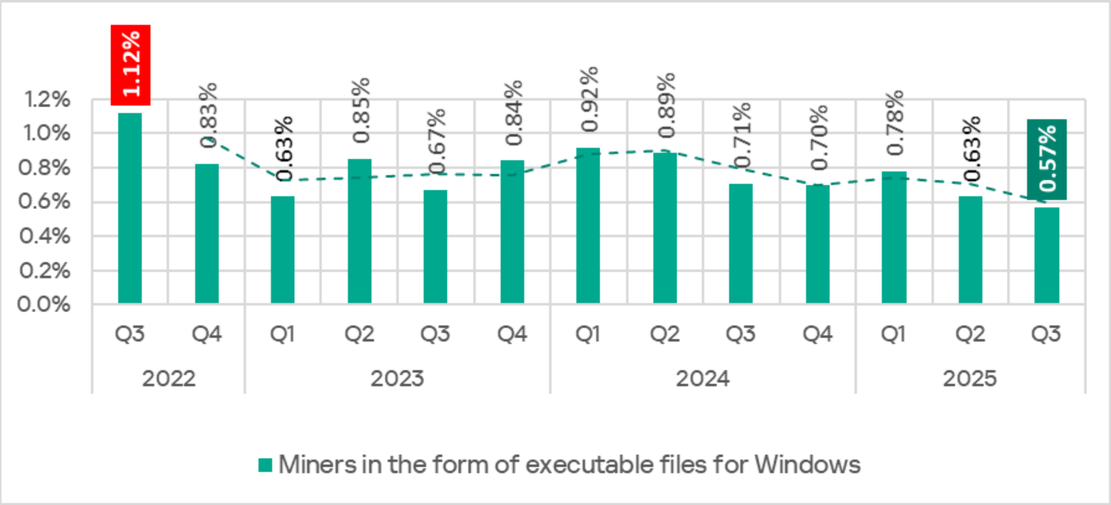
Another common method of deploying miners on ICS computers involves using legitimate cryptocurrency mining software such as XMRig, NBMiner, OneZeroMiner, and others. While these miners are not inherently malicious, they are classified as RiskTools by security systems. Attackers exploit these miners by 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

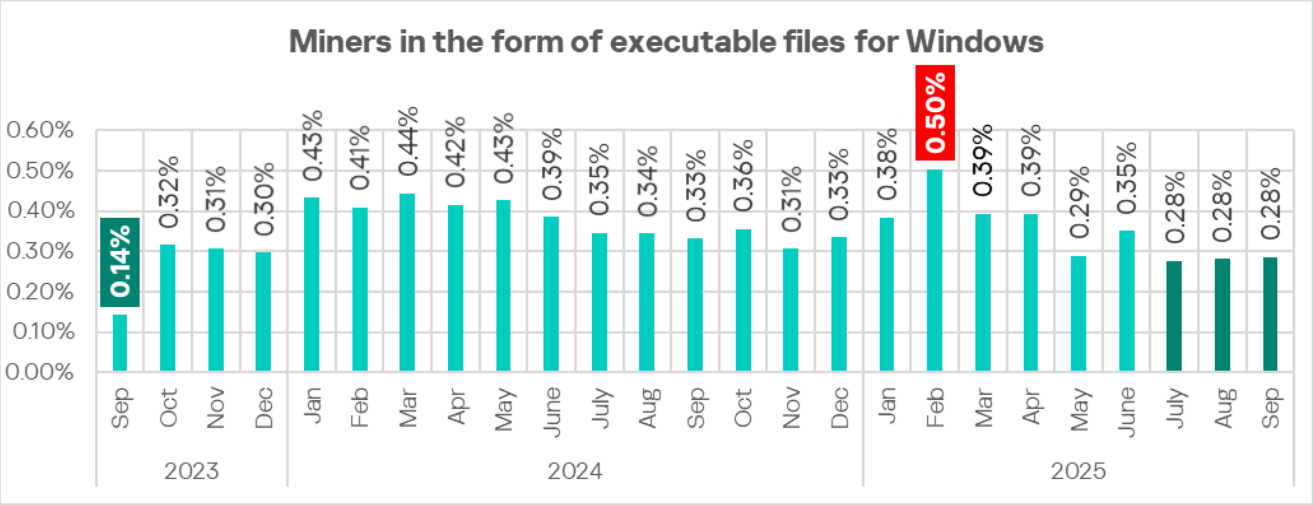

Malicious internet resource
Phishing email
.ZIP
Encrypted archive
.LNK
LNK path Command
[software name]*.exe Windows link file named as legitimate software with path attribute containing command to run PowerShell script
In-memory execution
PowerShell script
Downloads and runs legitimate mining software: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

In Q3 2025, the percentage of ICS computers on which miners in the form of executable files for Windows were blocked decreased to 0.57%. This is the lowest value in three years.

Percentage of ICS computers on which miners in the form of executable files for Windows were blocked, Q3 2022–Q3 2025



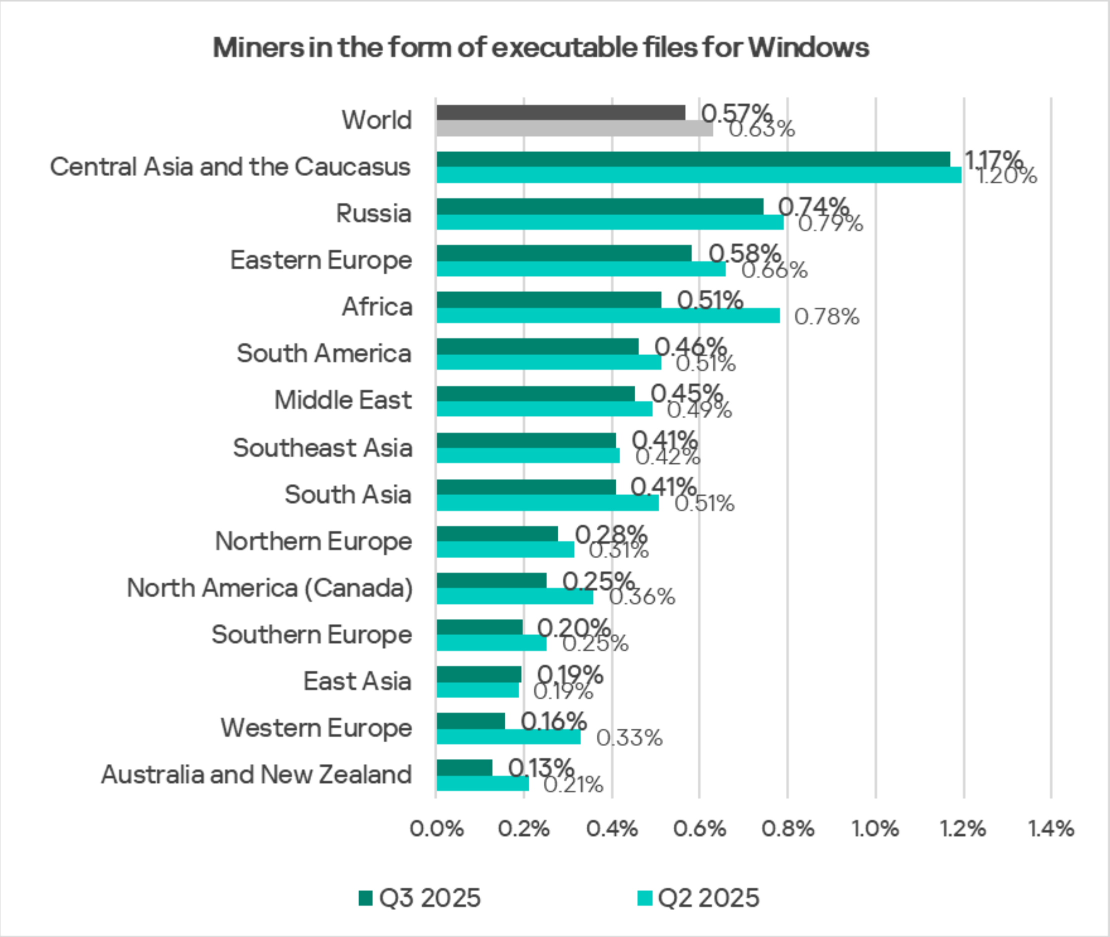
The monthly values within the quarter was equal — 0.28%.



Percentage of ICS computers on which miners in the form of executable files for Windows were blocked, September 2023—September 2025

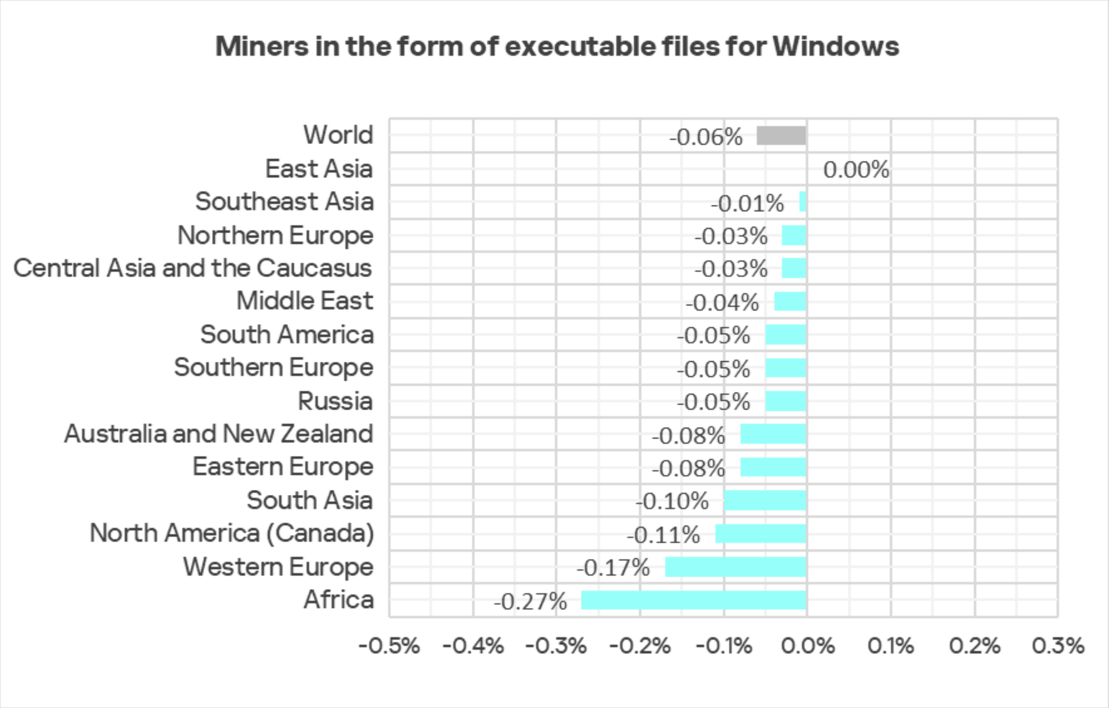
Regionally, the percentage of ICS computers on which miners in the form of executable files for Windows were blocked ranged from 0.13% in Australia and New Zealand to 1.17% in Central Asia and the South Caucasus. The top three regions for this indicator were Central Asia and the South Caucasus, Russia, and Eastern Europe.

Regions ranked by percentage of ICS computers on which miners in the form of executable files for Windows were blocked, Q3 2025



In Q3 2025, the percentage of ICS computers on which miners in the form of executable files for Windows were blocked decreased in all regions except East Asia.

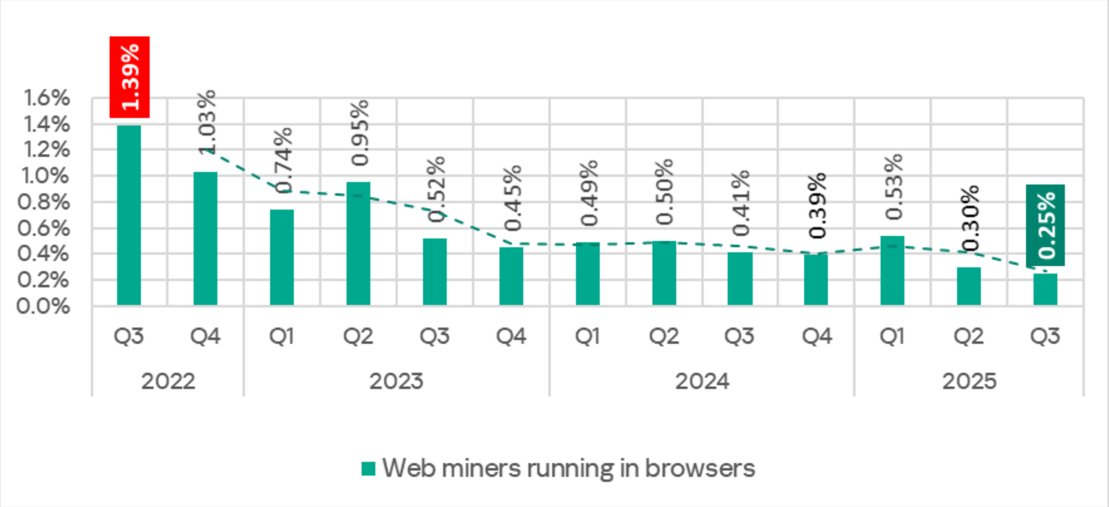
Changes in percentage of ICS computers on which miners in the form of executable files for Windows were blocked, Q3 2025



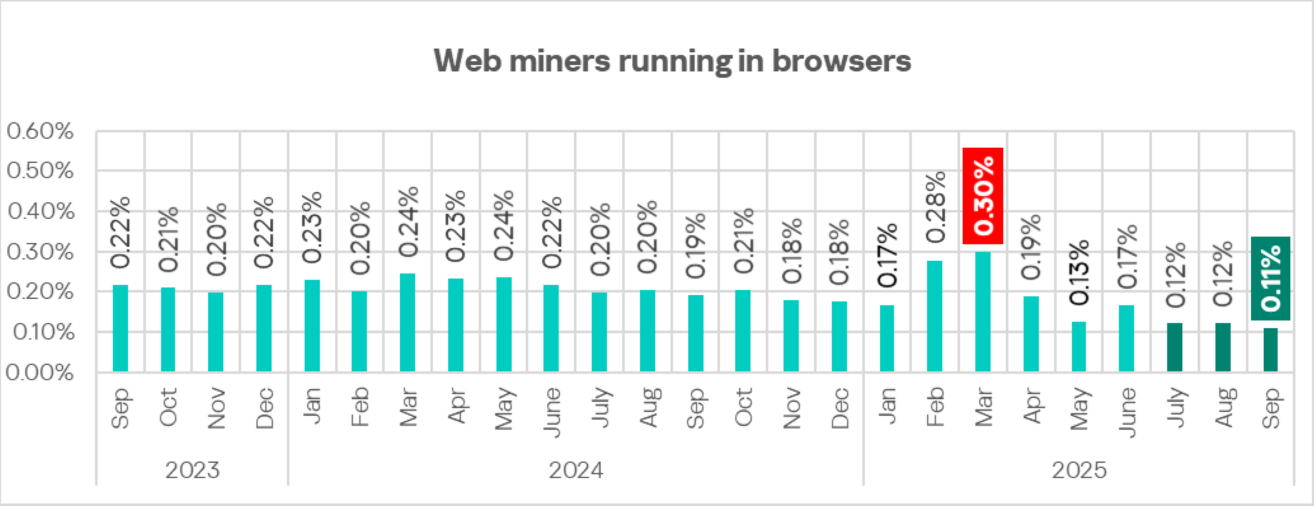
Web miners

In Q3 2025, the percentage of ICS computers on which web miners were blocked decreased to 0.25%. It is the lowest level since Q3 2022.

Percentage of ICS computers on which web miners were blocked, Q3 2022–Q3 2025



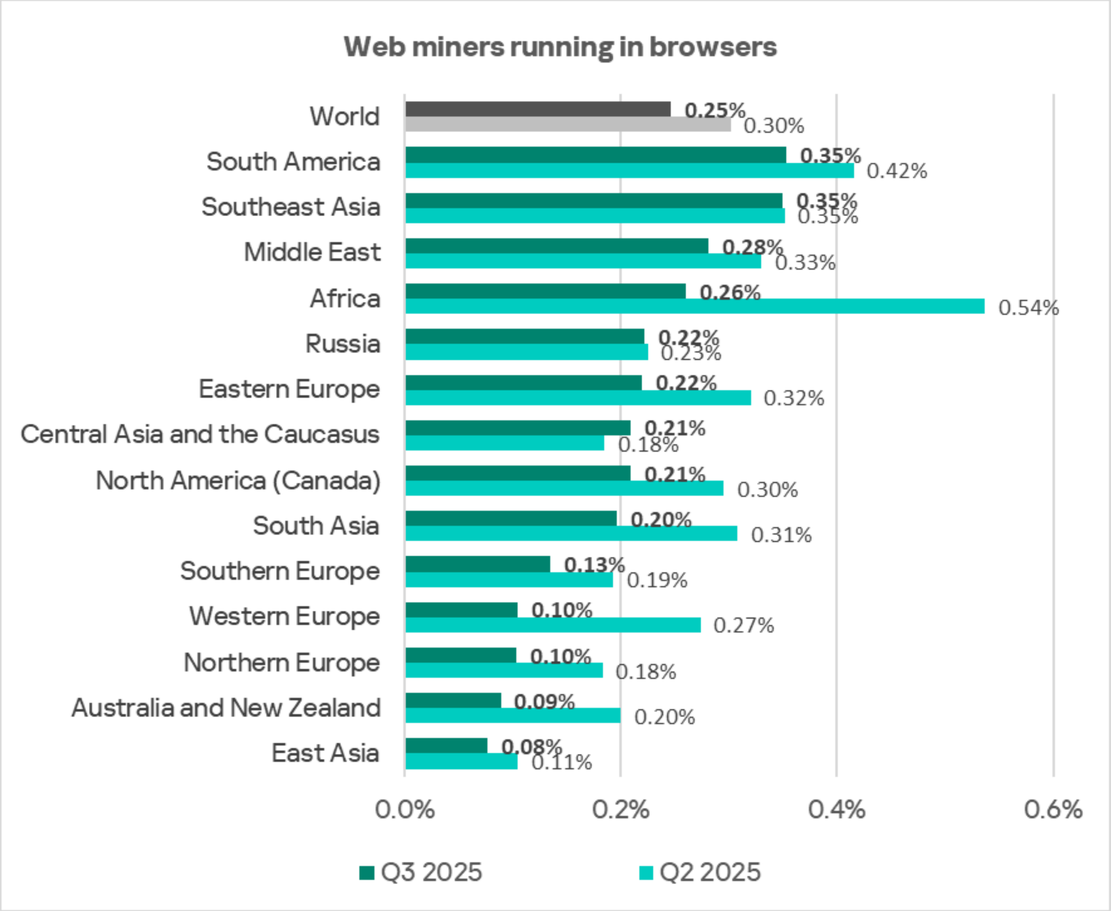
In September 2025, the monthly rate fell to its lowest point since January 2022.



Percentage of ICS computers on which web miners were blocked, September 2023—September 2025

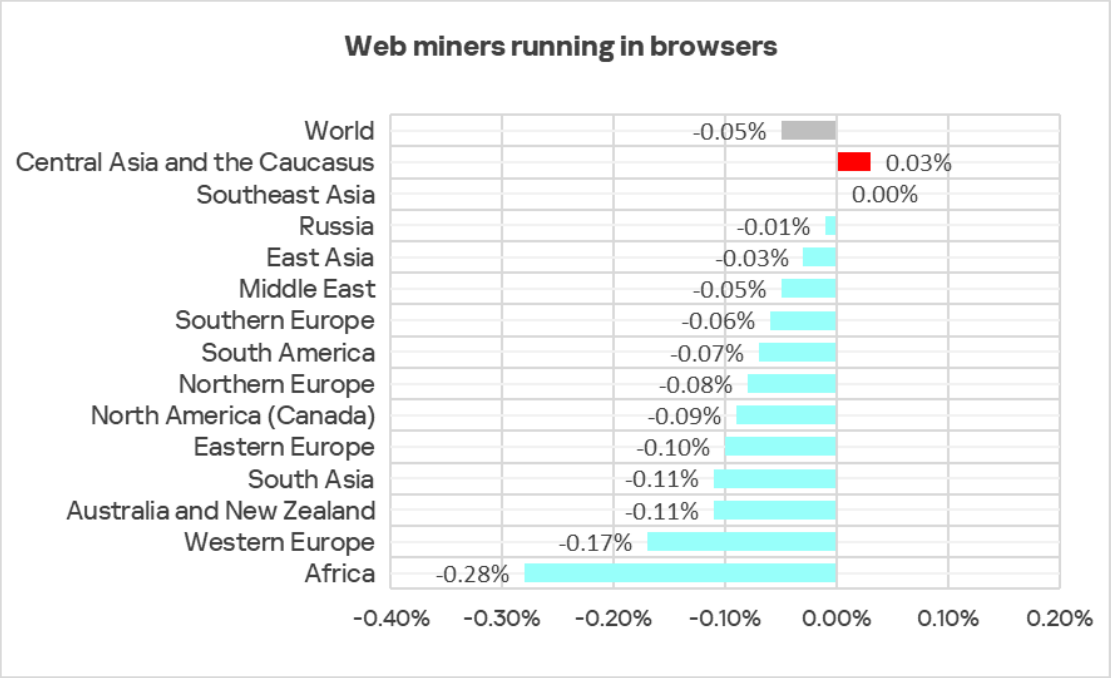
Regionally, the percentage of ICS computers on which web miners were blocked ranged from 0.08% in East Asia to 0.35% in South America. The top three regions for this indicator were South America, Southeast Asia, and the Middle East.

Regions ranked by percentage of ICS computers on which web miners were blocked, Q3 2025



In Q3 2025, the percentage of ICS computers on which web miners were blocked decreased in all regions except Central Asia and the South Caucasus, and Southeast Asia.

Changes in percentage of ICS computers on which web miners were blocked, Q3 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 and network folders in the form of infected files, such as archives with backups, office documents, pirated games and hacked applications. In rarer and more dangerous cases, web pages with network equipment settings, as well as files stored in internal document management systems, product lifecycle management (PLM) systems, resource management (ERP) systems and other web services are infected.

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.

It should be noted that the spread can also occur in an active form. This can be done through techniques such as password brute-force attacks, theft of user authentication data (including access tokens), and network attacks on vulnerable software. All these methods have long been included in the modular toolkit of any modern worm-miner.

Although modern versions of worms are not often found in ICS networks, the damage caused by an infection is always significant. Even basic maintenance of an infected network becomes much more expensive due to longer downtime and the additional man-hours required to restore performance. And if a ransomware program is downloaded through a worm to a computer in a technological network after preliminary profiling, the cost is exponentially higher.

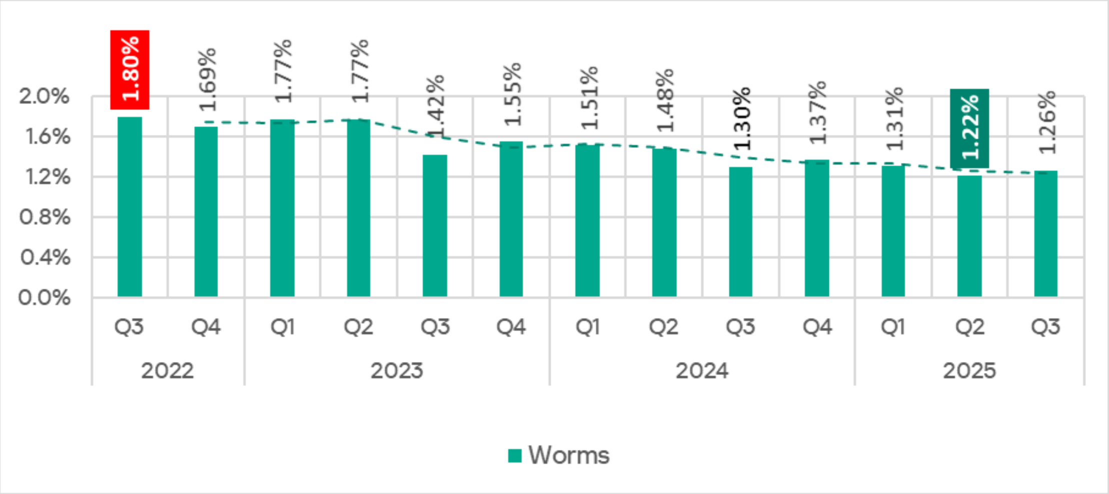
Alongside this, a lot of those still spreading are legacy viruses and worms whose command and control servers have been shut down. However, these types of malware can compromise infected systems by opening network ports or changing configurations, cause software failures, denial of service, and so on.

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.

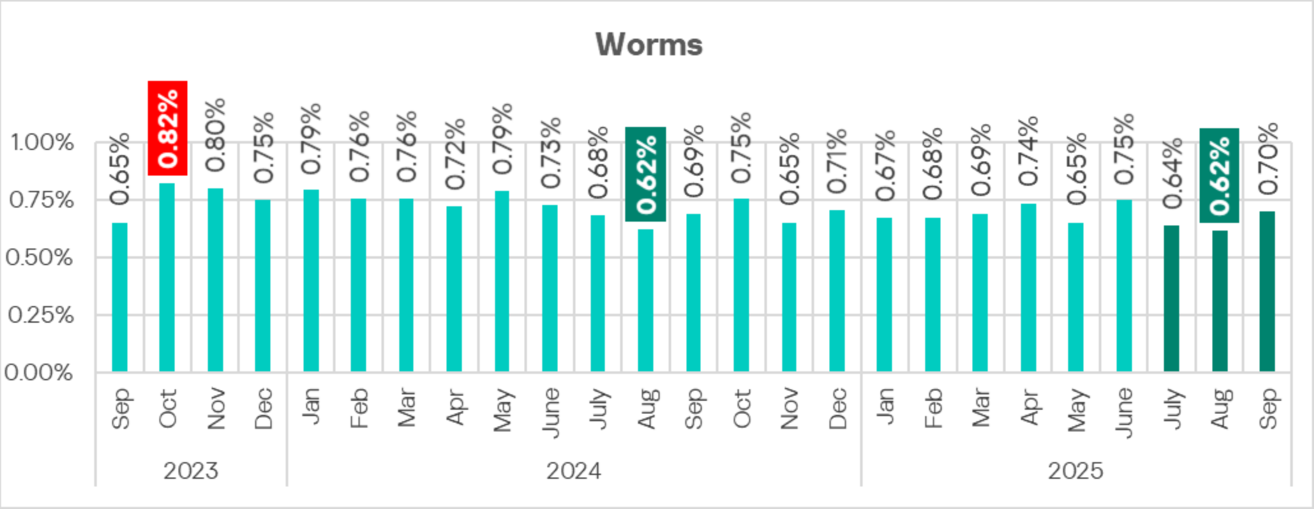
Worms

In Q3 2025, the percentage of ICS computers on which worms were blocked increased to 1.26%, up from its lowest value in the previous quarter.

Percentage of ICS computers on which worms were blocked, Q3 2022–Q3 2025



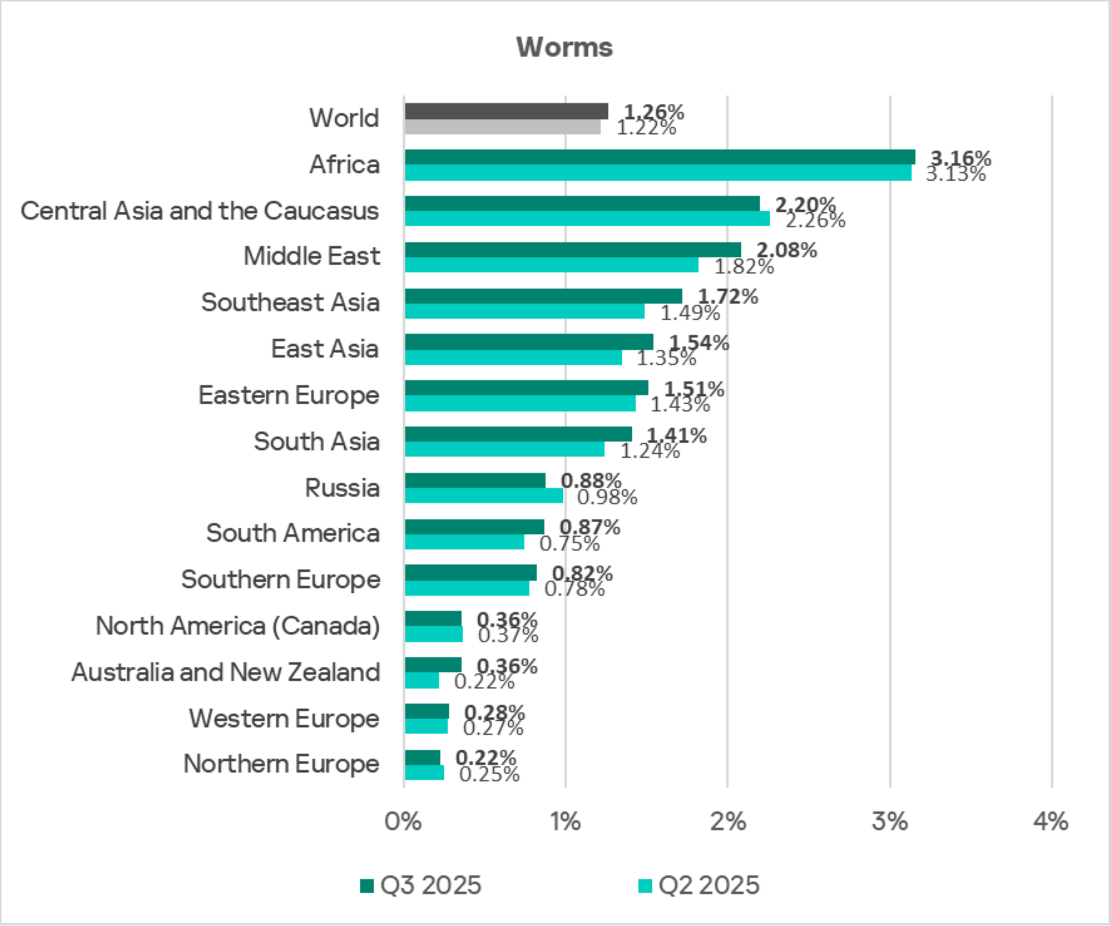
The highest monthly rate of Q3 occurred in September.



Percentage of ICS computers on which worms were blocked, September 2023—September 2025

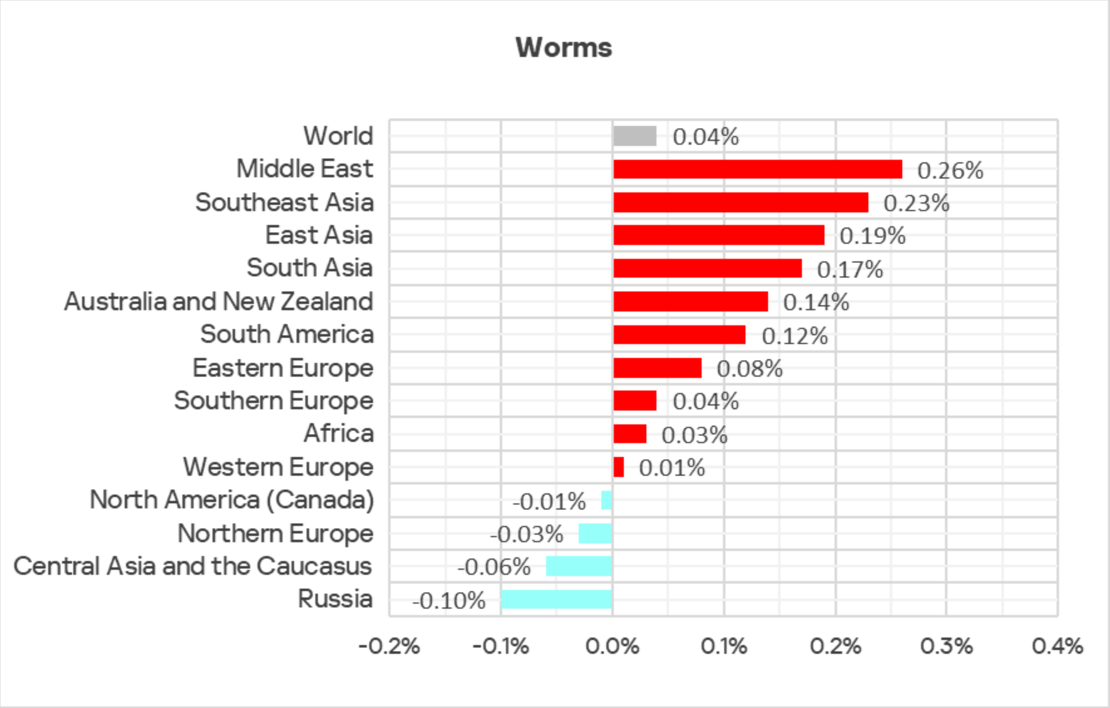
Regionally, the percentage of ICS computers on which worms were blocked ranged from 0.22% in Northern Europe to 3.16% in Africa. The top three regions for this indicator were Africa, Central Asia and the South Caucasus, and the Middle East.

Regions ranked by percentage of ICS computers on which worms were blocked, Q3 2025



The percentage increased in all regions except North America (Canada), Northern Europe, Russia, and Central Asia and the South Caucasus.

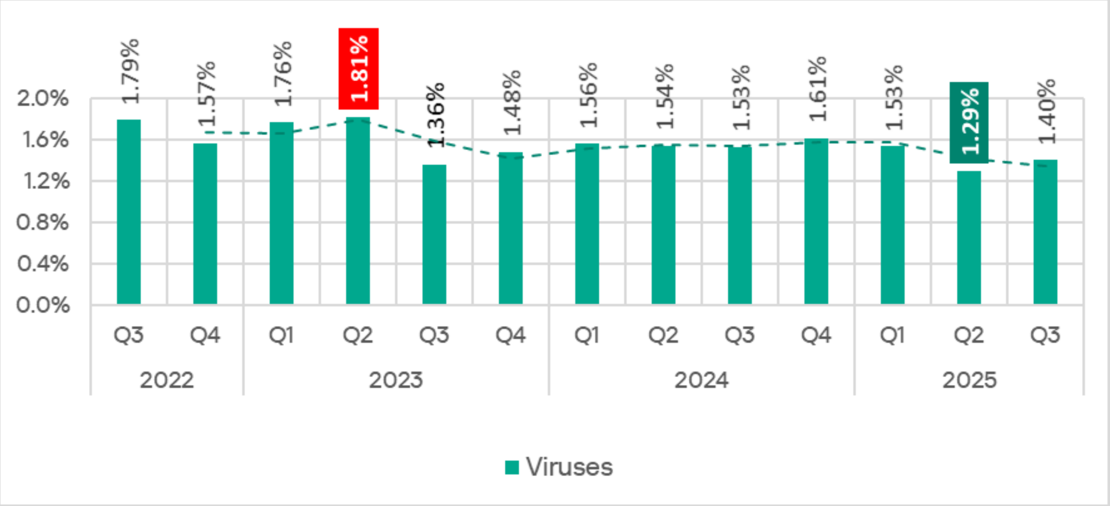
Changes in percentage of ICS computers on which worms were blocked, Q3 2025



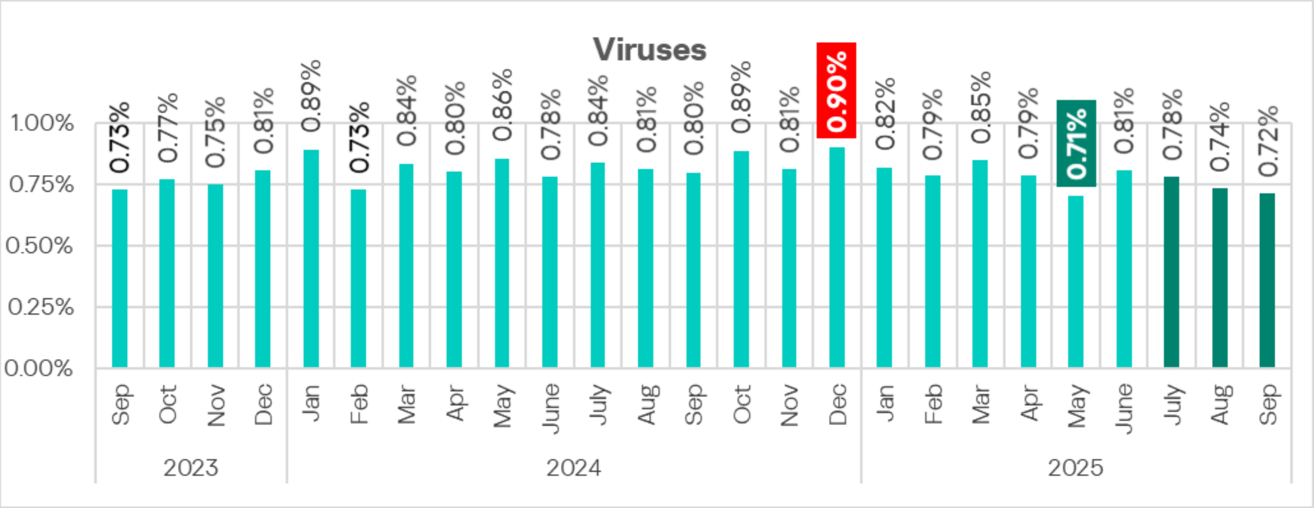
Viruses

In Q3 2025, the percentage of ICS computers on which viruses were blocked increased to 1.40%, up from its lowest value in the previous quarter.

Percentage of ICS computers on which viruses were blocked, Q3 2022–Q3 2025



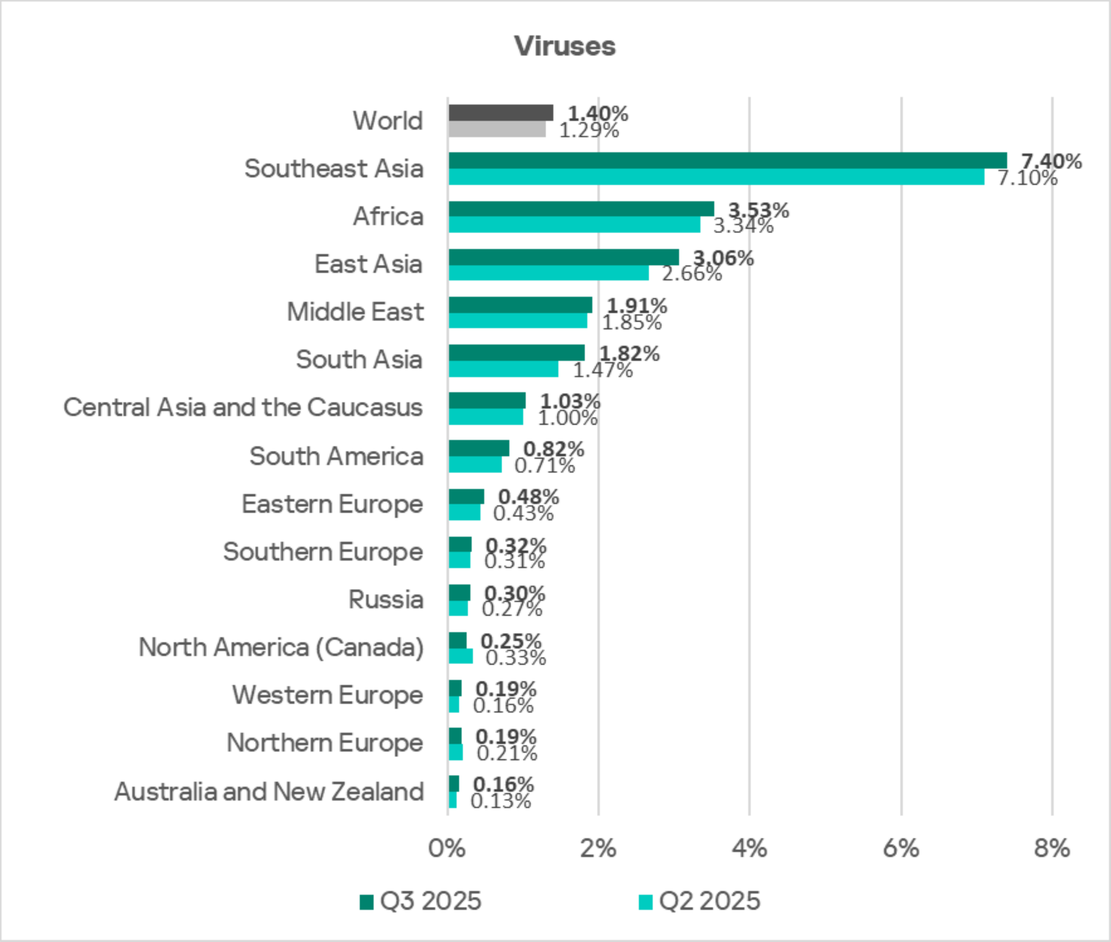
The highest monthly rate of Q3 occurred in July.



Percentage of ICS computers on which viruses were blocked, September 2023—September 2025

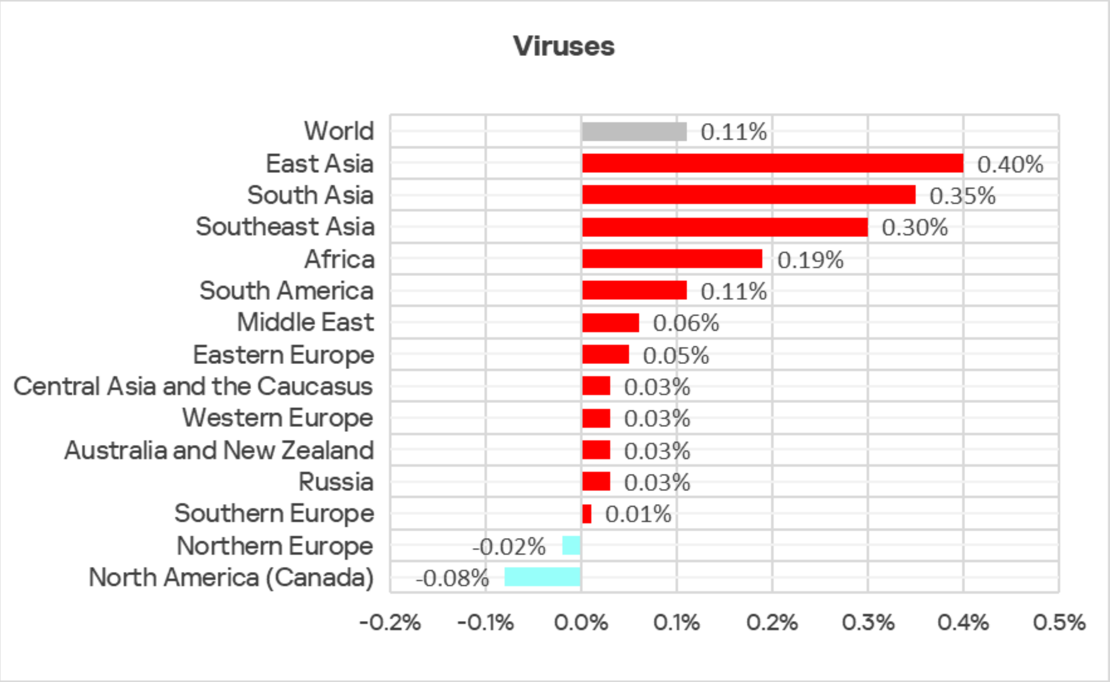
Regionally, the percentage of ICS computers on which viruses were blocked ranged from 0.16% in Australia and New Zealand to 7.40% in Southeast Asia. The top three regions for this indicator in Q3 2025 remained the same: Southeast Asia (by a wide margin), followed by Africa, and East Asia. These are the same regions that led the AutoCAD malware ranking.

Regions ranked by percentage of ICS computers on which viruses were blocked, Q3 2025



In Q3 2025, the percentage increased in all regions except Northern Europe and North America (Canada). The indicator increased the most in East Asia, South Asia, and Southeast Asia.

Changes in percentage of ICS computers on which viruses were blocked, Q3 2025



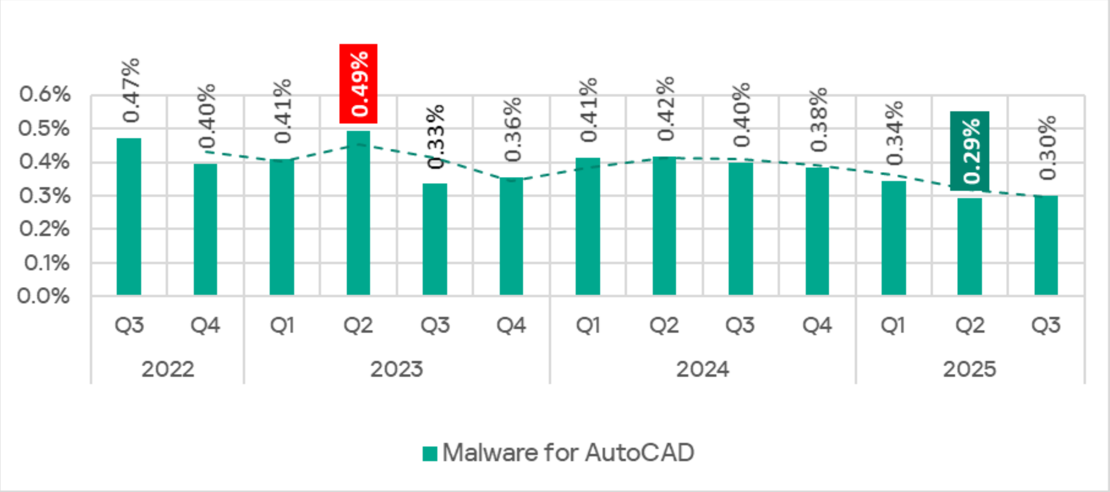
AutoCAD malware

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.

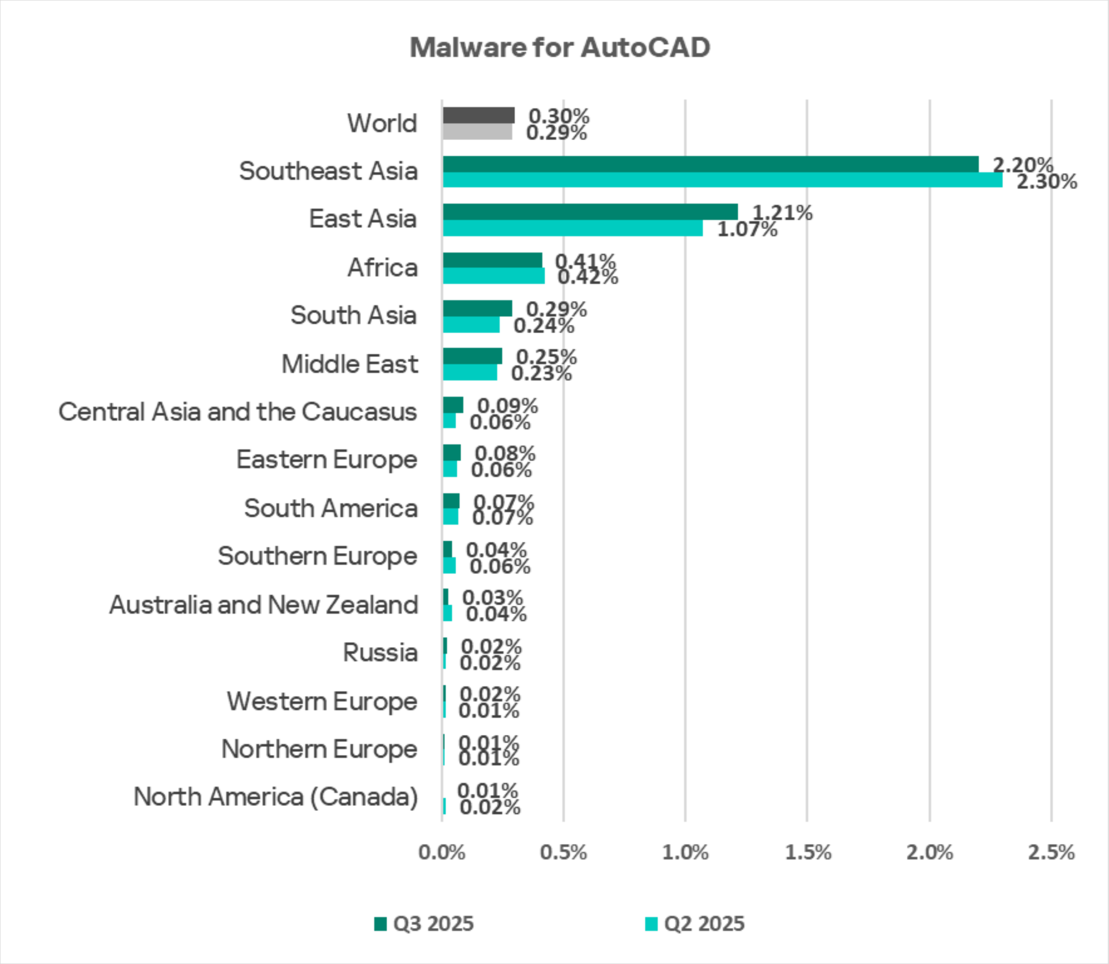
In Q3 2025, the percentage of ICS computers on which AutoCAD malware was blocked after reaching the lowest level in the previous quarter increased to 0.30%.

Percentage of ICS computers on which AutoCAD malware was blocked, Q3 2022–Q3 2025



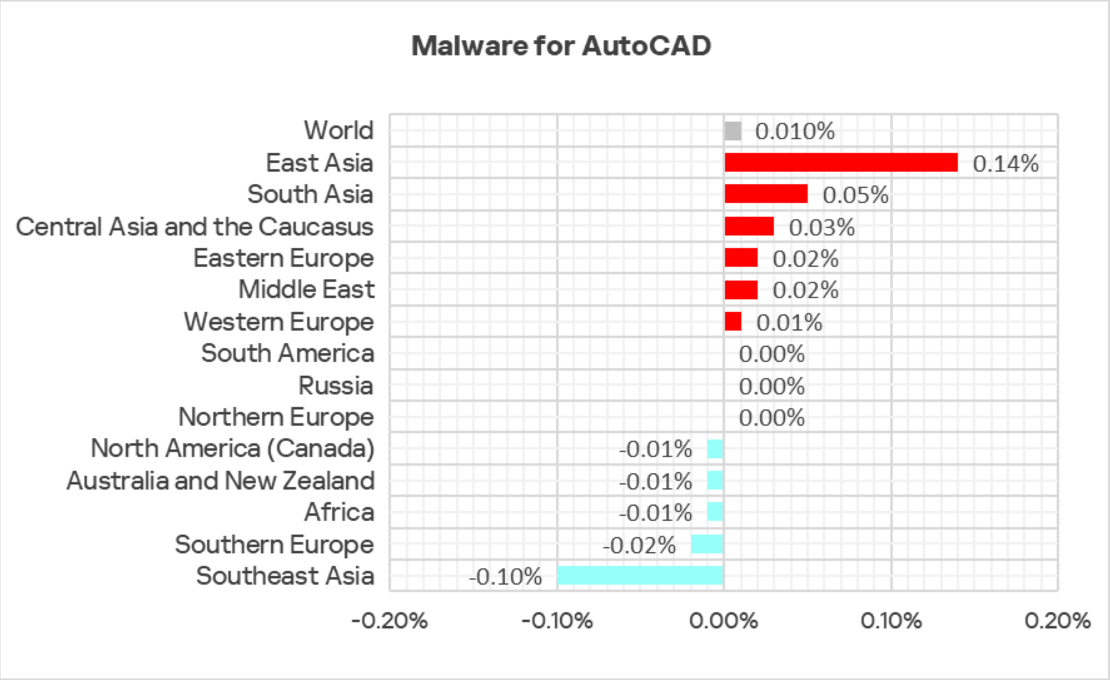
Regionally, the percentage of ICS computers on which AutoCAD malware was blocked ranged from 0.01% in North America (Canada) to 2.20% in Southeast Asia. The same regions that led the virus ranking were also the leaders in terms of the percentage of ICS computers on which AutoCAD malware was blocked: Southeast Asia, East Asia (both by a wide margin), and Africa.

Regions ranked by percentage of ICS computers on which AutoCAD malware was blocked, Q3 2025



In Q3 2025, the percentage increased in six regions, the most notable increase being in East Asia.

Changes in percentage of ICS computers on which AutoCAD malware was blocked, Q3 2025



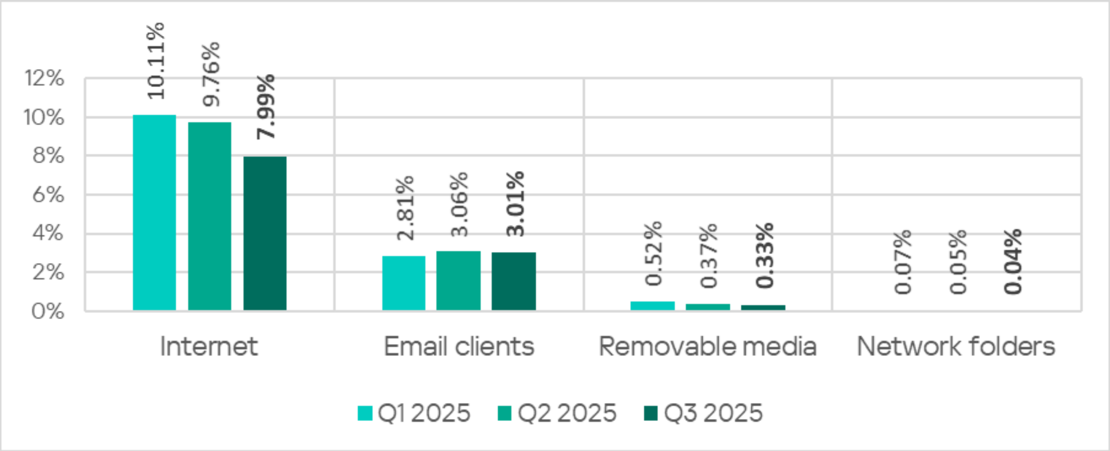
Main threat sources

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 Q3 2025, the percentage of ICS computers on which malicious objects from various sources were blocked decreased.

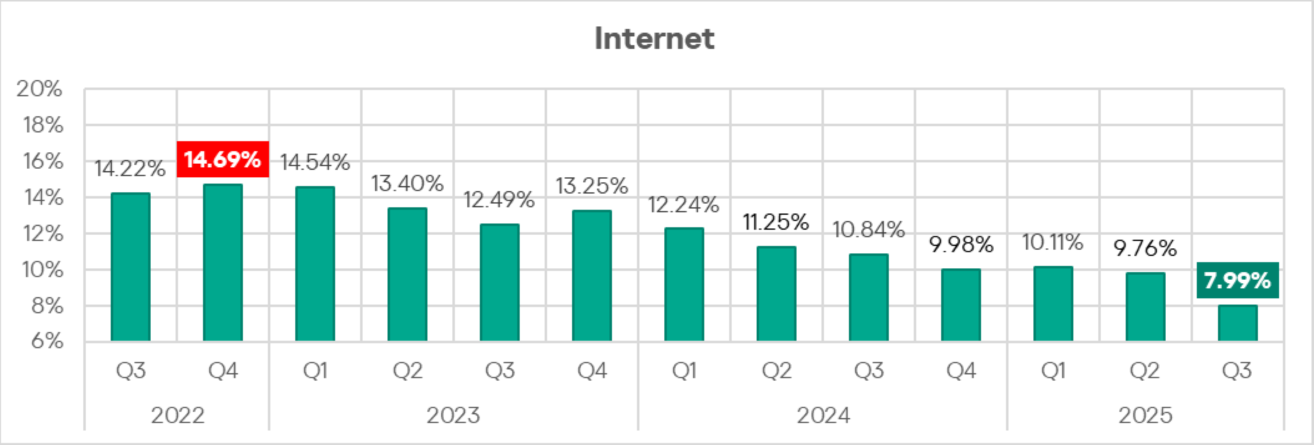
Percentage of ICS computers on which malicious objects from various sources were blocked



Internet

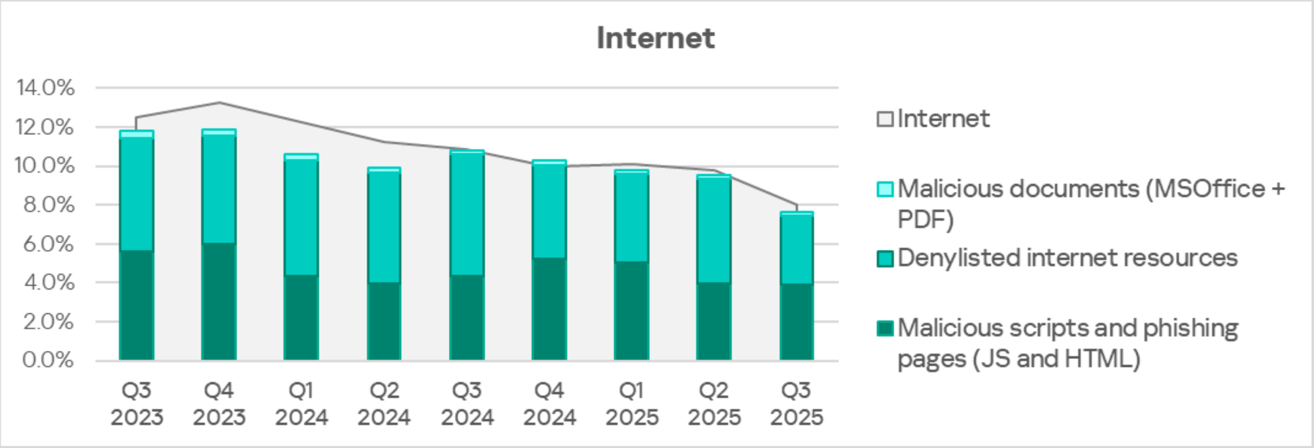
Detection and blocking of internet threats on ICS computers protected by Kaspersky products means that access to external services was allowed from these computers at the time of detection.

In Q3 2025, the percentage of ICS computers on which threats from the internet were blocked decreased to 7.99% and reached its lowest level since Q2 2022.



Percentage of ICS computers on which threats from the internet were blocked, Q3 2022—Q3 2025

The main categories of threats from the internet* blocked on ICS computers in Q3 2025 are malicious scripts and phishing pages, and denylisted internet resources.

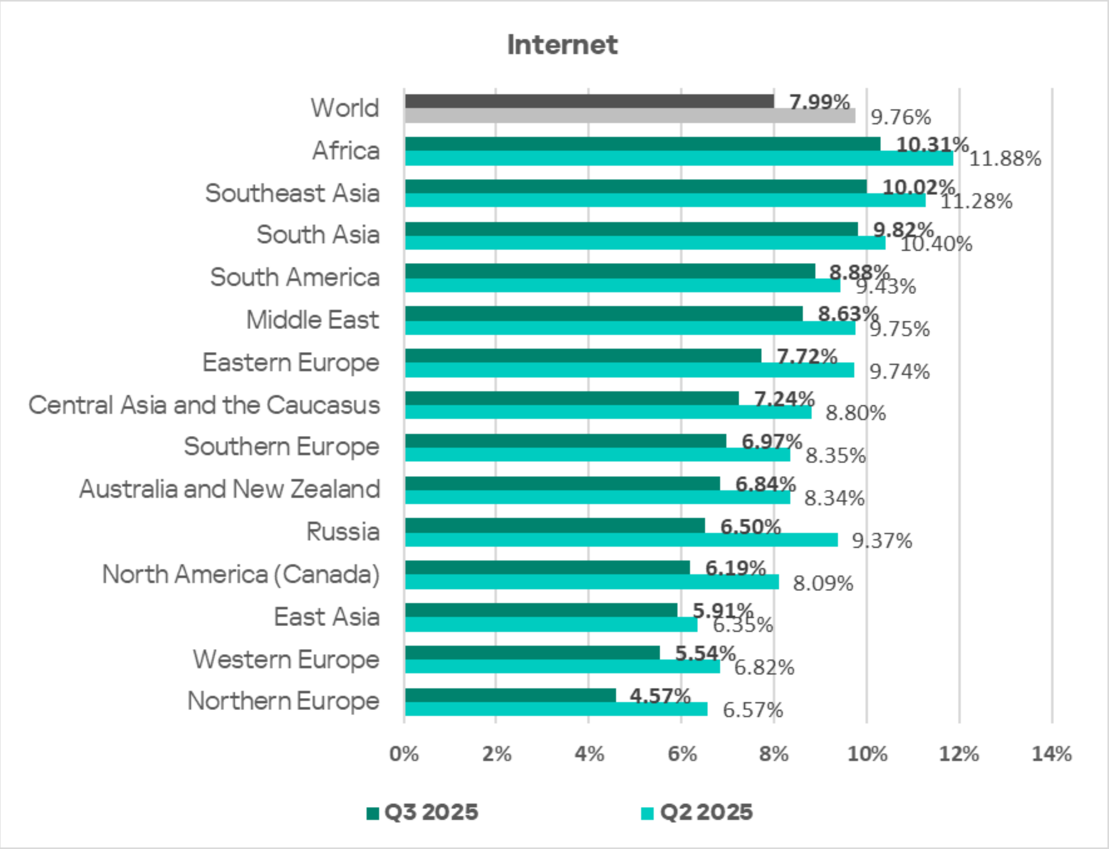


Percentage of ICS computers on which threats from the internet were blocked, Q3 2023—Q3 2025

*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 can exceed the percentage of threats from the source itself.

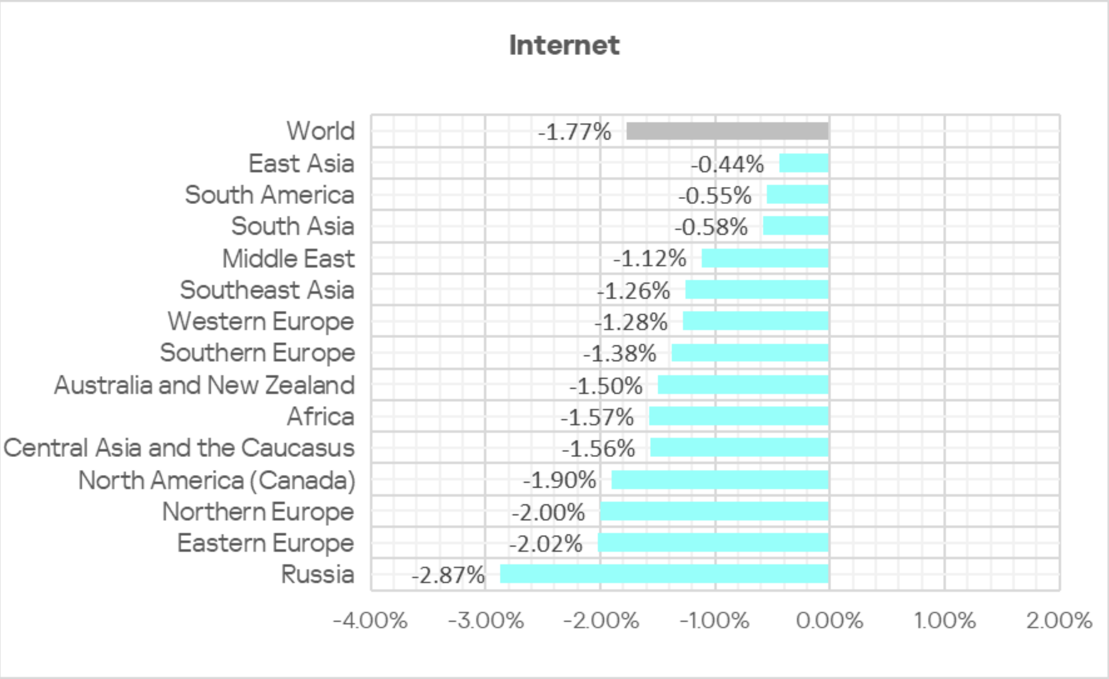
Regionally, the percentage of ICS computers on which threats from the internet were blocked ranged from 4.57% in Northern Europe to 10.31% in Africa. The top three regions for this indicator were Africa, Southeast Asia, and South Asia.

Regions ranked by percentage of ICS computers on which threats from the internet were blocked, Q3 2025



In Q3 2025, the percentage decreased in all regions.

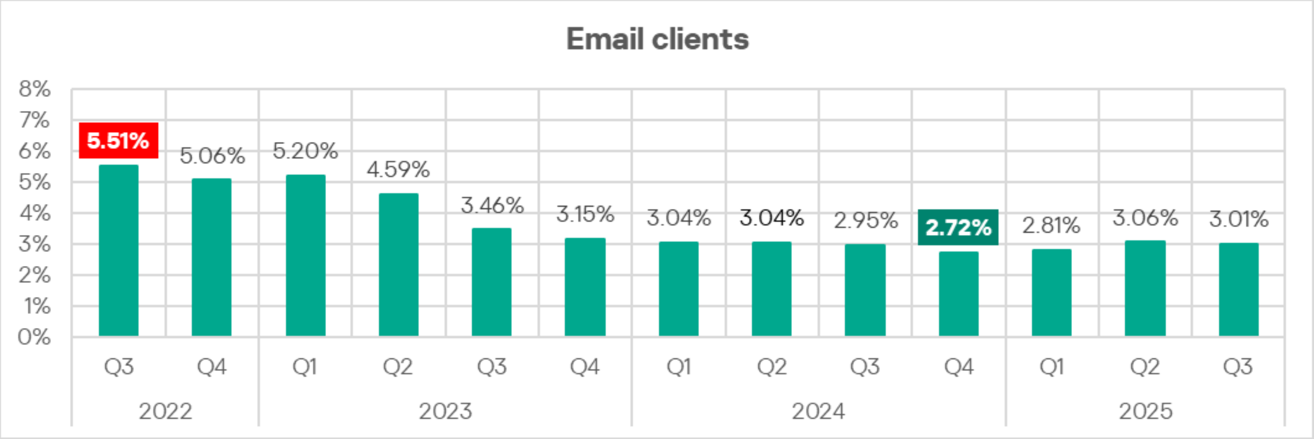
Changes in percentage of ICS computers on which threats from the internet were blocked, Q3 2025



Email clients

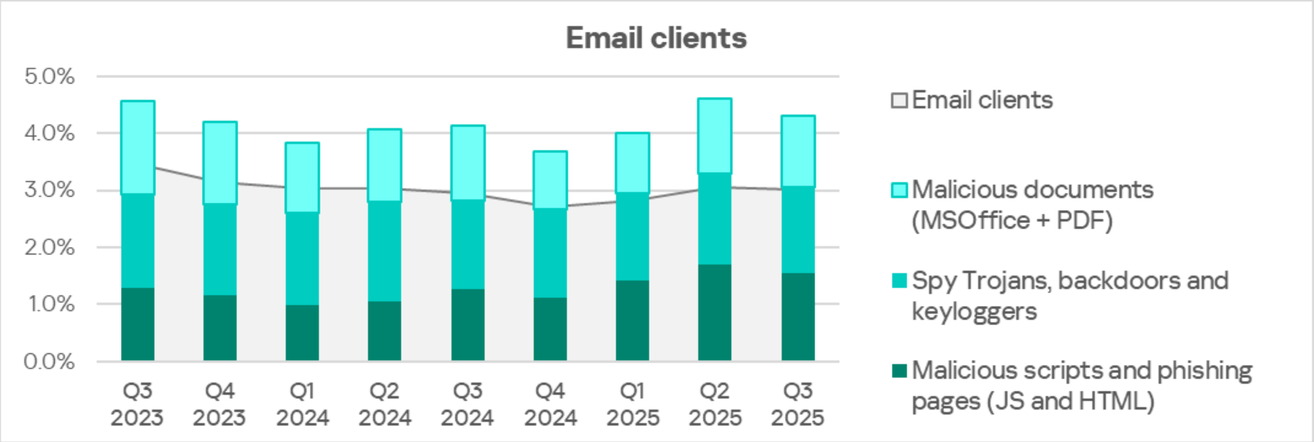
Some detected and blocked threats are delivered to protected computers by the mail delivery system and/or attempt to gain access through the email client application.

In Q3 2025, the percentage of ICS computers on which threats from email clients were blocked slightly decreased to 3.01%.



Percentage of ICS computers on which threats from email clients were blocked, Q3 2022—Q3 2025

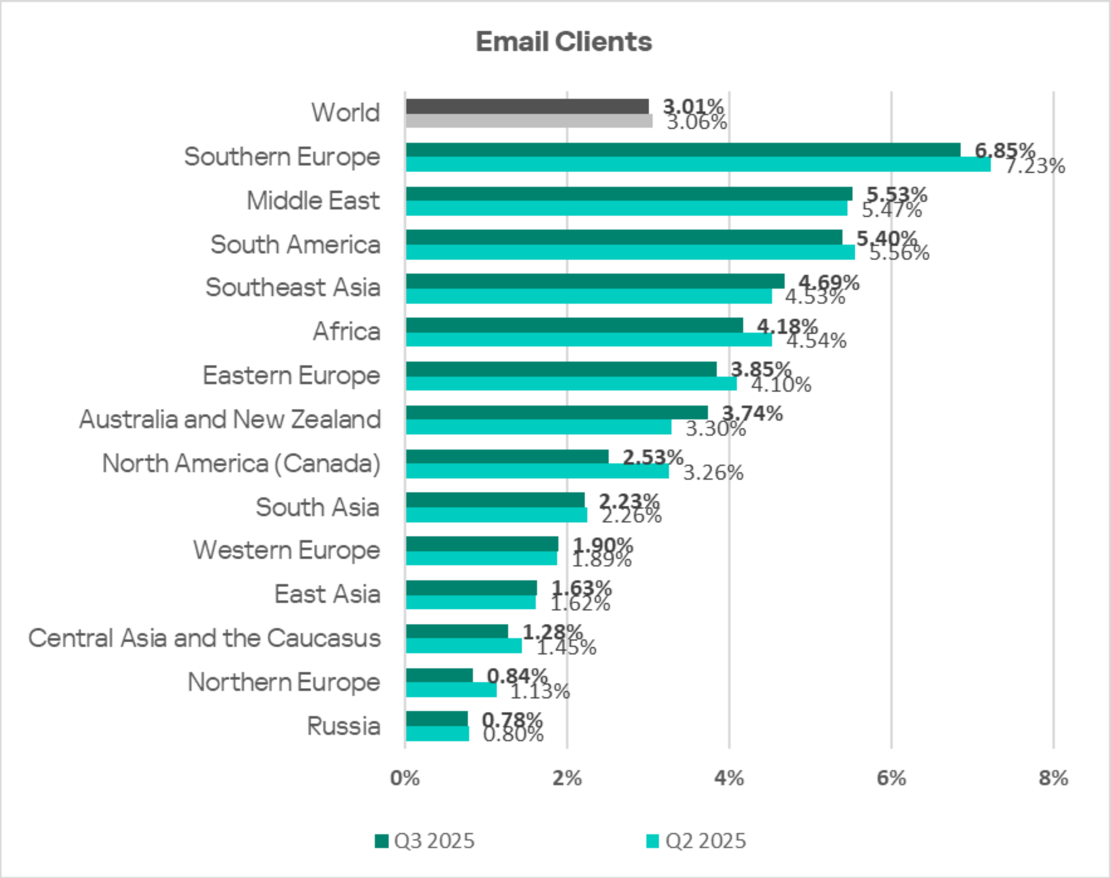
The main categories of threats from email clients blocked on ICS computers in Q3 2025 are malicious scripts and phishing pages, spyware, and malicious documents.



Percentage of ICS computers on which threats from email clients were blocked, Q3 2023—Q3 2025

Most of the spyware detected in phishing emails was delivered as a password archive or a multi-layered script embedded in office document files.

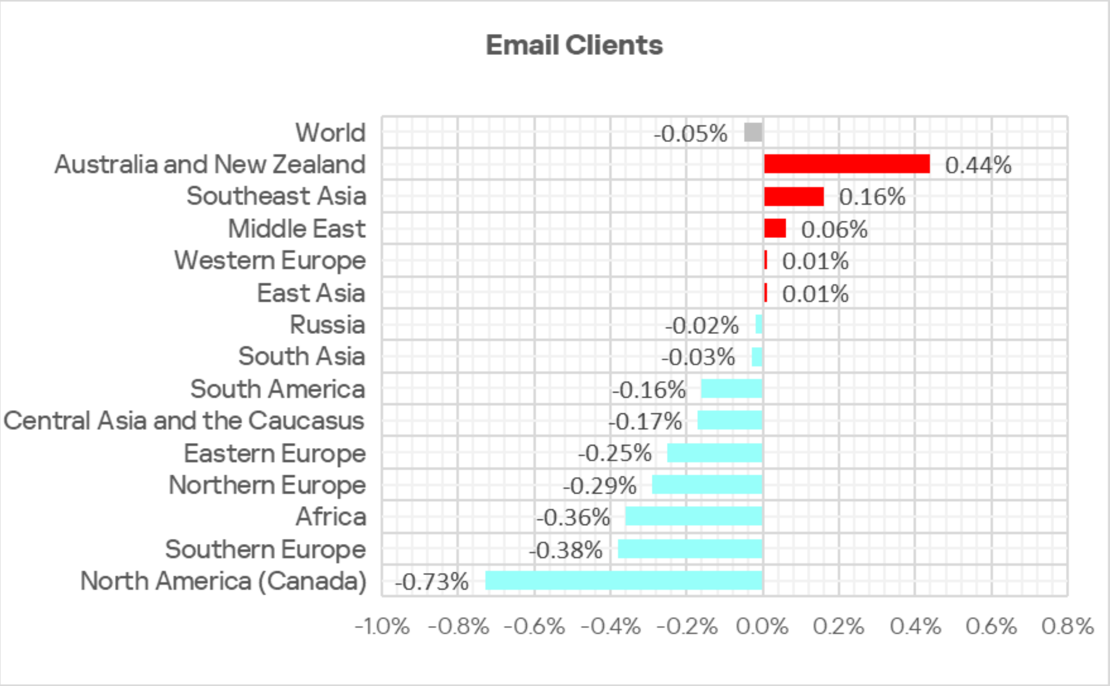
Regionally, the percentage of ICS computers on which threats from email clients were blocked ranged from 0.78% in Russia to 6.85% in Southern Europe. The top three regions for this indicator were the same as in the previous quarter: Southern Europe, the Middle East, and South America.



Regions ranked by percentage of ICS computers on which threats from email clients were blocked, Q3 2025

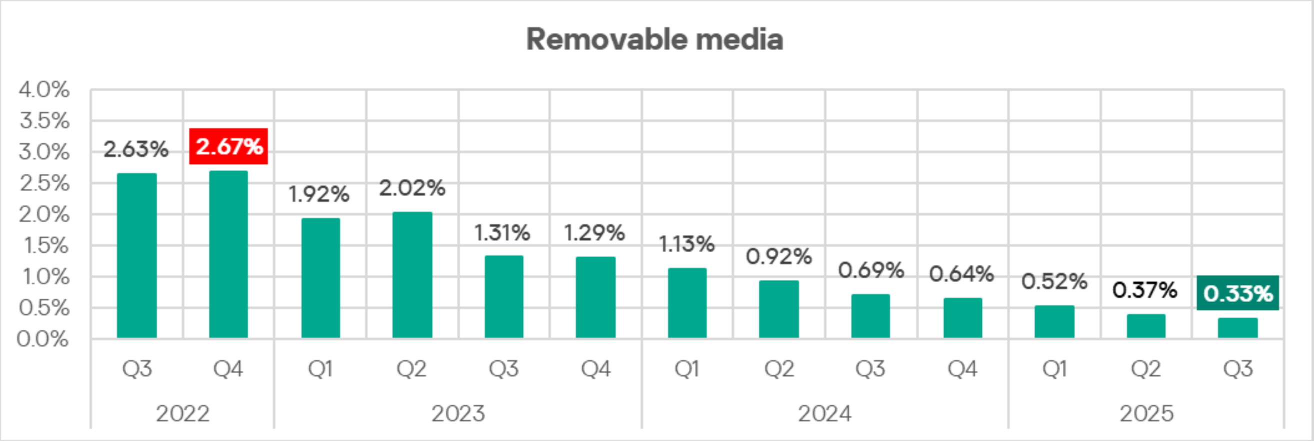
In Q3 2025, the percentage of ICS computers on which threats from email clients were blocked increased in five regions. The largest increase was seen in Australia and New Zealand.

Changes in percentage of ICS computers on which threats from email clients were blocked, Q3 2025



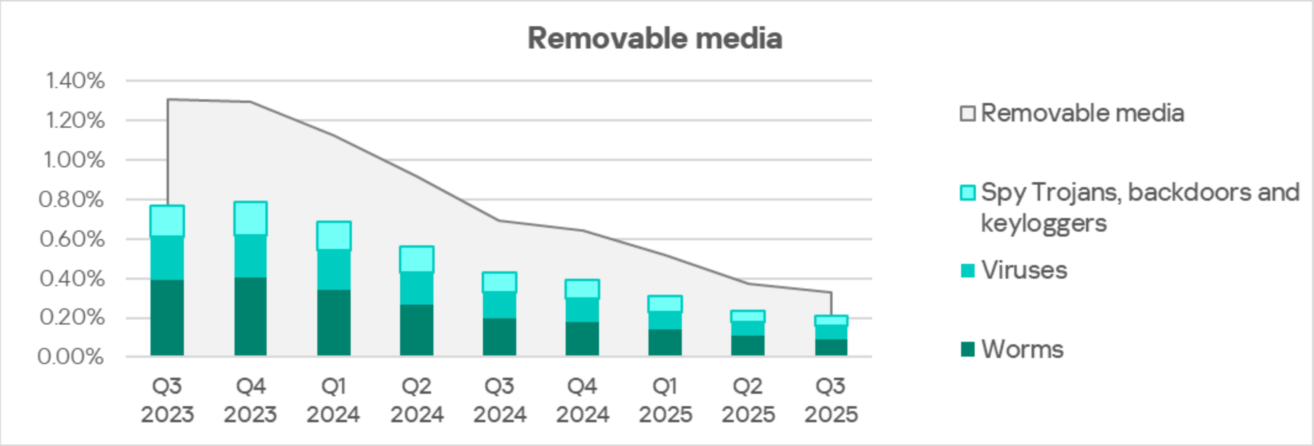
Removable media

In Q3 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 — 0.33%.



Percentage of ICS computers on which threats from removable media were blocked, Q3 2022—Q3 2025

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



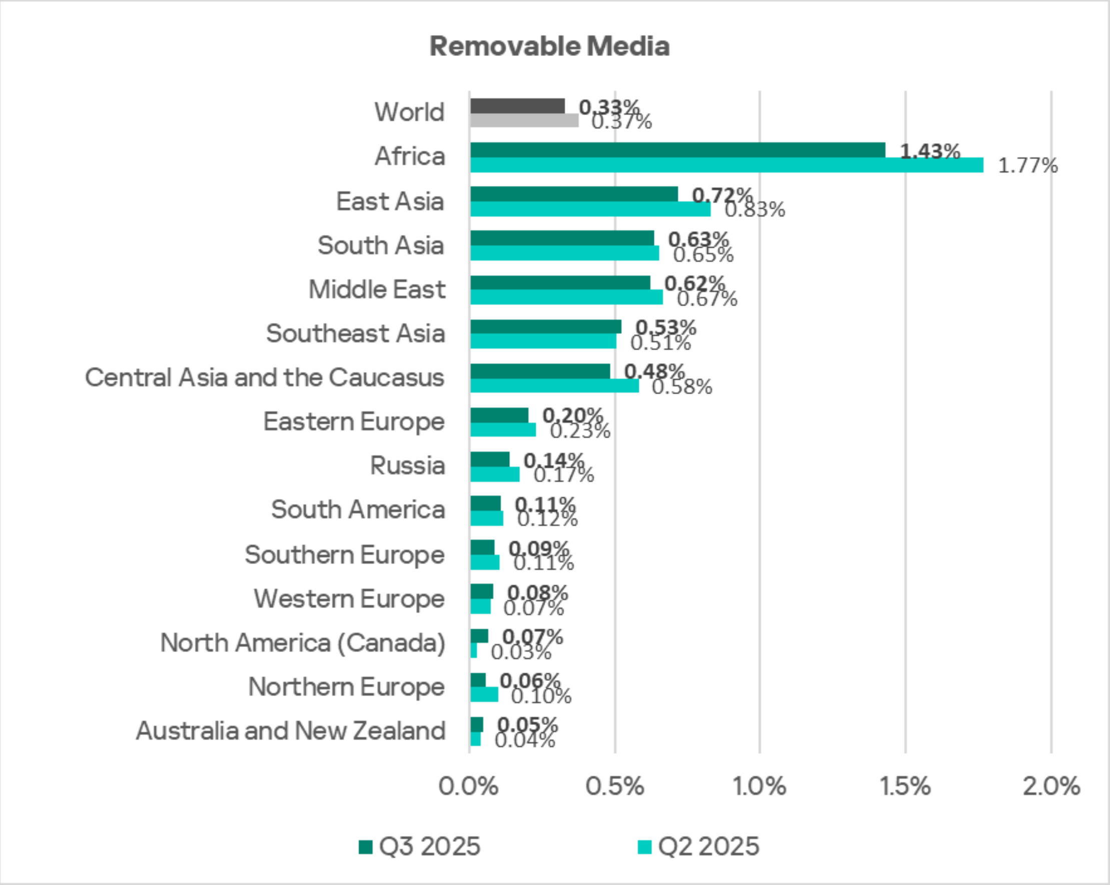
Percentage of ICS computers on which threats from removable media were blocked, Q3 2023—Q3 2025

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.

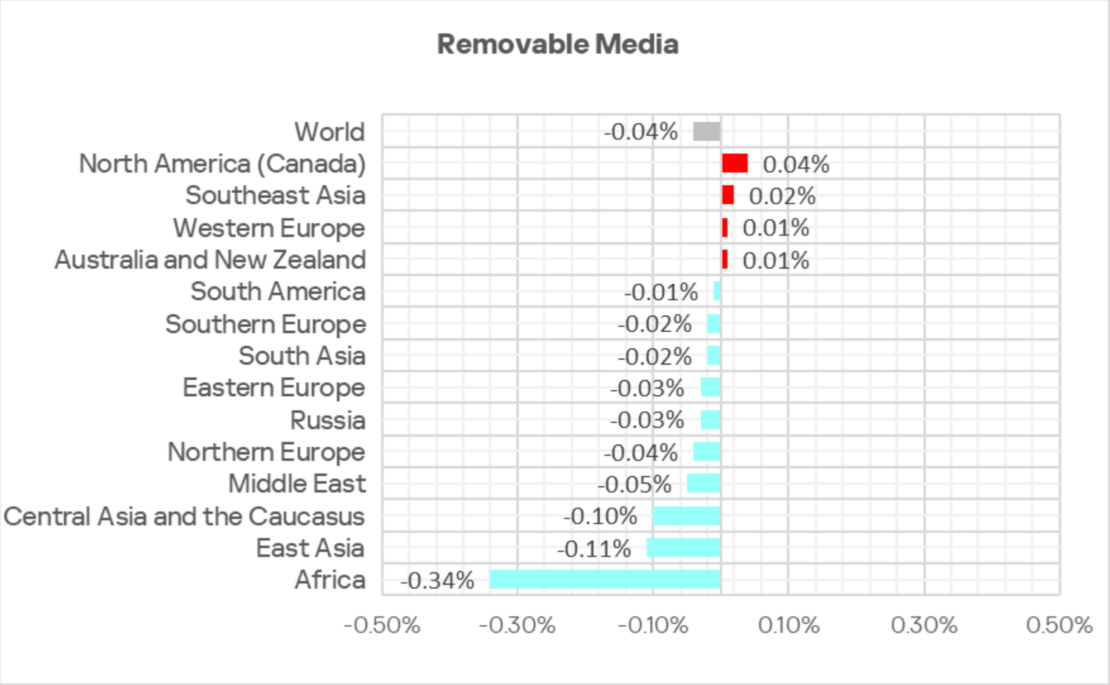
Regionally, the percentage of ICS computers on which threats from removable media were blocked ranged from 0.05% in Australia and New Zealand to 1.43% in Africa. The top three regions for this indicator were Africa (by a wide margin), followed by East Asia and South Asia.

Regions ranked by percentage of ICS computers on which threats from removable media were blocked, Q3 2025



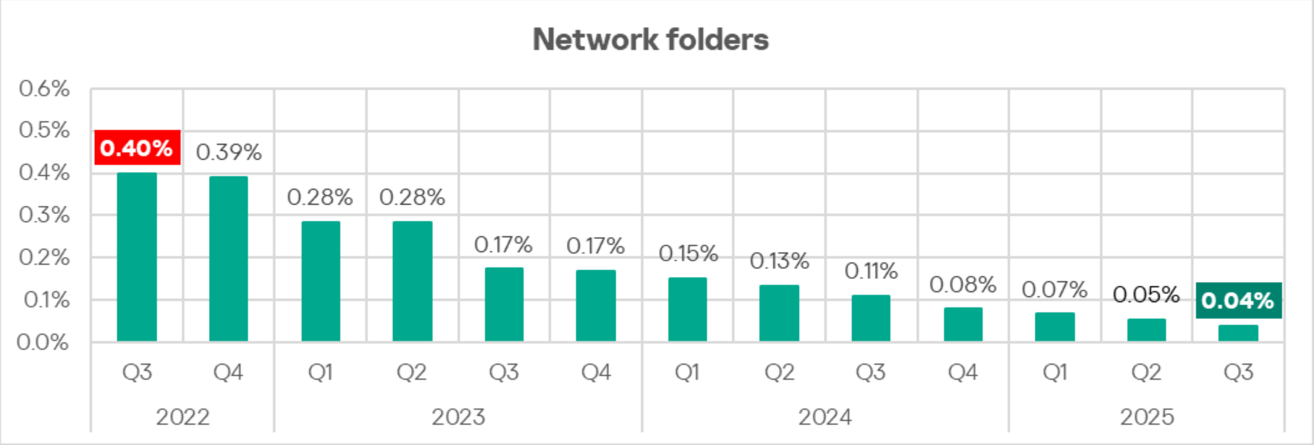
In Q3 2025 the percentage decreased in all regions except North America (Canada), Southeast Asia, Western Europe, and Australia and New Zealand.

Changes in percentage of ICS computers on which threats from removable media were blocked, Q3 2025



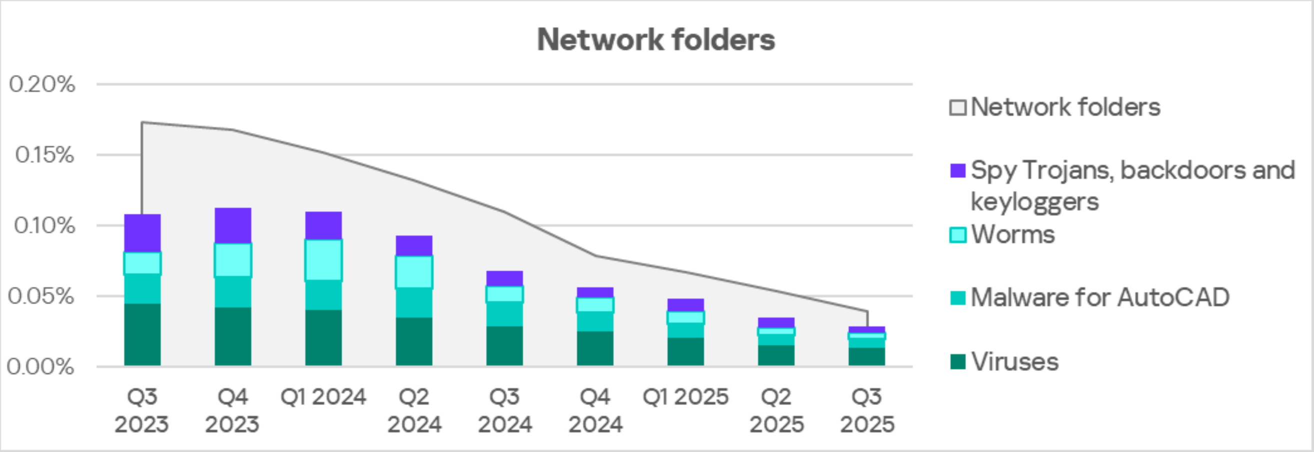
Network folders

In Q3 2025, the percentage of ICS computers on which threats from network folders were blocked reached its lowest level since early 2022.



Percentage of ICS computers on which threats from network folders were blocked, Q3 2022—Q3 2025

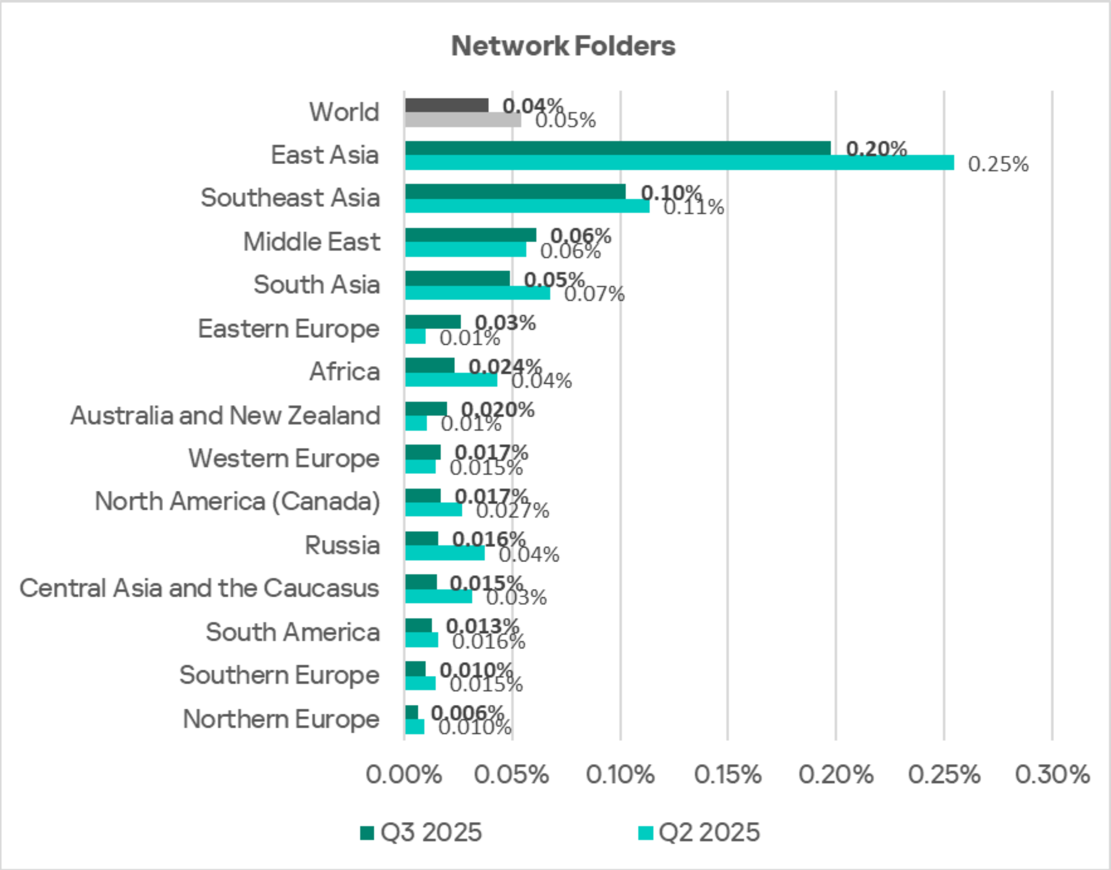
The main categories of threats that spread through network folders in Q3 2025 are viruses, AutoCAD malware, worms, and spyware.



Percentage of ICS computers on which threats from network folders were blocked, Q3 2023—Q3 2025

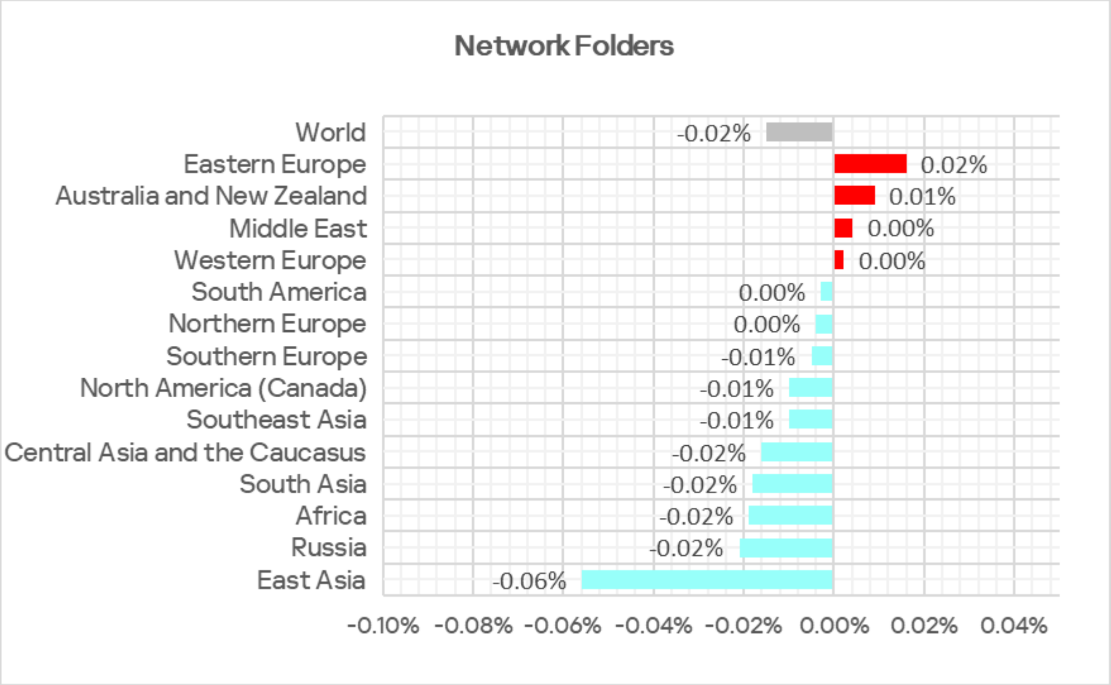
Regionally, the percentage of ICS computers on which threats from network folders were blocked ranged from 0.006% in Northern Europe to 0.20% in East Asia. The top three regions for this indicator were East Asia, Southeast Asia, and the Middle East.

Regions ranked by percentage of ICS computers on which threats from network folders were blocked, Q3 2025



The percentage increased in four regions in Q3 2025, with the most notable increase occurring in Eastern Europe.

Changes in percentage of ICS computers on which threats from network folders were blocked, Q3 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

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

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.

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