Kaspersky ICS CERT

kaspersky

Threat landscape for industrial automation systems

Q4 2025

02.04.2026

Version 1.0

Q4 in numbers

Parameter	Q3 2025	Q4 2025	Quarterly changes
Global percentage of attacked ICS computers	20.1%	19.7%	▼0.4 pp
Percentage of ICS computers on which malicious objects from different categories were blocked			
Malicious scripts and phishing pages (JS and HTML)	6.79%	6.58%	▼0.21 pp
Spy Trojans, backdoors and keyloggers	4.04%	3.80%	▼0.24 pp
Denylisted internet resources	4.01%	3.26%	▼0.75 pp
Malicious documents (MSOffice + PDF)	1.98%	1.76%	▼0.22 pp
Worms	1.26%	1.60%	▲0.34 pp
Viruses	1.40%	1.33%	▼0.07 pp
Miners in the form of executable files for Windows	0.57%	0.60%	▲0.03 pp
Malware for AutoCAD	0.30%	0.29%	▼0.01 pp
Web miners running in browsers	0.25%	0.24%	▼0.01 pp
Ransomware	0.17%	0.16%	▼0.01 pp
Main threat sources			
Internet	7.99%	7.67%	▼0.32 pp
Email clients	3.01%	2.76%	▼0.25 pp
Removable media	0.33%	0.31%	▼0.02 pp
Network folders	0.04%	0.04%	0.00 pp

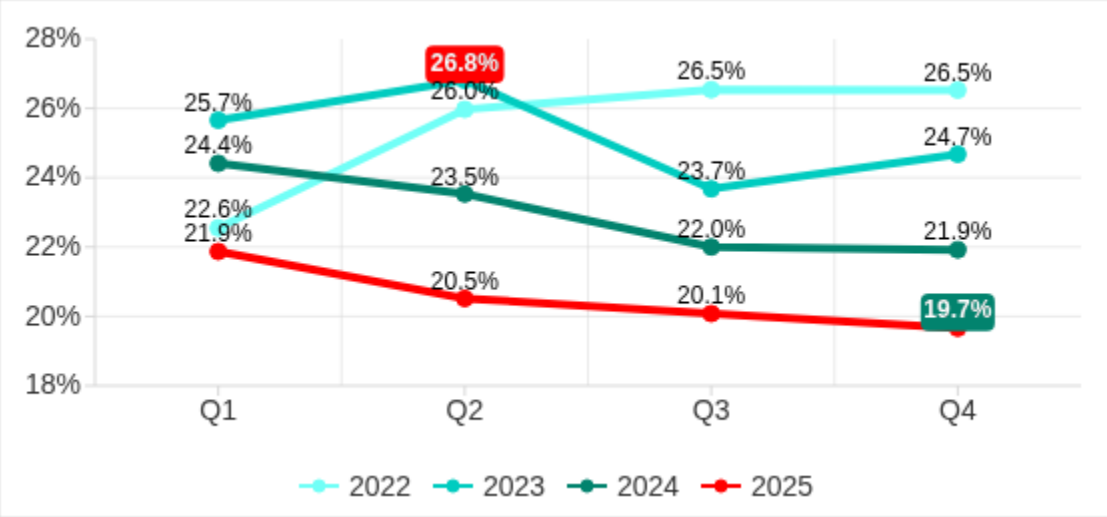
Changes over the quarter

The percentage of ICS computers on which malicious objects were blocked

In Q4 2025, the percentage of ICS computers on which malicious objects were blocked continued to decrease, reaching its lowest level since 2022 — 19.7%.

Regionally, the percentage ranged from 8.5% in Northern Europe to 27.3% in Africa. Four regions saw increases. Southern Europe led the way in terms of growth for this indicator.

Percentage of ICS computers on which malicious objects were blocked, Q1 2022–Q4 2025



The percentage of ICS computers on which malicious objects were blocked has been steadily decreasing since 2024. The quarterly figures for 2025 were the lowest since 2022.

Main threat sources and categories

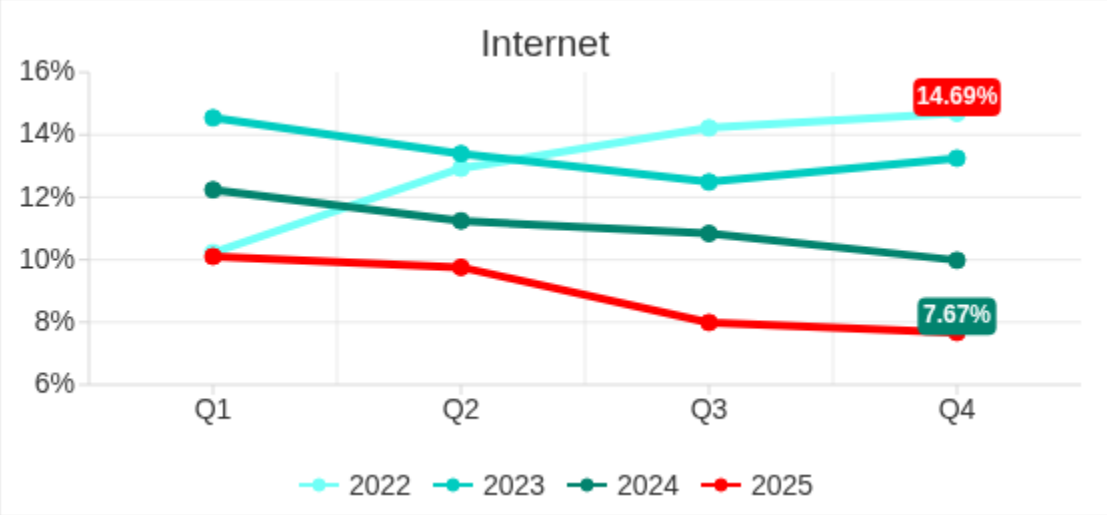
The main threat sources to computers in enterprise OT infrastructure are still the internet, email clients, and removable media. In Q4 2025, the global average for all threat sources except email clients decreased. The percentage of ICS computers on which threats from the internet were blocked reached its lowest level since 2022.

In terms of threat categories, the percentage of ICS computers on which malicious objects from various categories were blocked only increased during the quarter for worms and miners in the form of executable files for Windows. The rates for denylisted internet resources were the lowest since 2022.

The internet remains the primary source of threats for OT networks. The downward trend over the past three years indicates that:

1. More and more malicious URLs and other web threats are being blocked at the network perimeter, i.e., before reaching ICS computers, where web security components are the last line of defense.
2. Techniques for deploying malware on the internet are becoming more versatile and accessible. The cost of creating links to malicious content has decreased to nearly nothing because almost any public web service can be used to store malware. Furthermore, delivery techniques are becoming more varied, which decreases the effectiveness of detecting malicious URLs.

Percentage of ICS computers on which threats from the internet were blocked, Q1 2022–Q4 2025

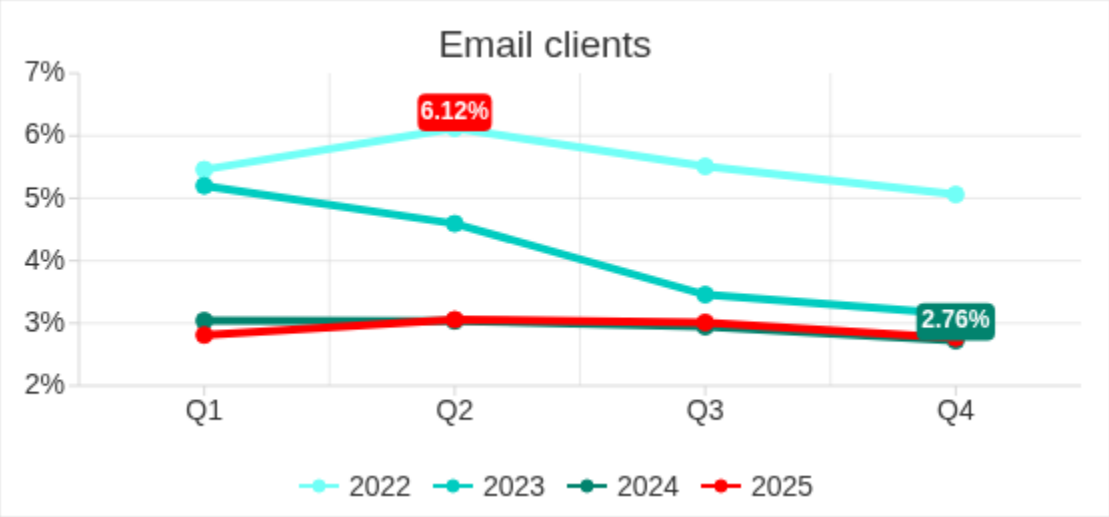


Clearly, poorly controlled internet access from an OT network is not only a source of accidental infections with initial malware. If the network is successfully compromised, internet access becomes a channel for the delivery of next-stage malware, data exfiltration, and remote control.

The main categories of threats from the internet blocked on ICS computers in Q4 2025 were malicious scripts and phishing pages, and denylisted internet resources.

Since the beginning of 2024, the percentage of ICS computers on which threats from email clients were blocked has remained relatively stable. The figure for Q4 2025 (2.76%) is slightly higher than the lowest level since 2022 (2.72%), which was recorded in Q4 of 2024.

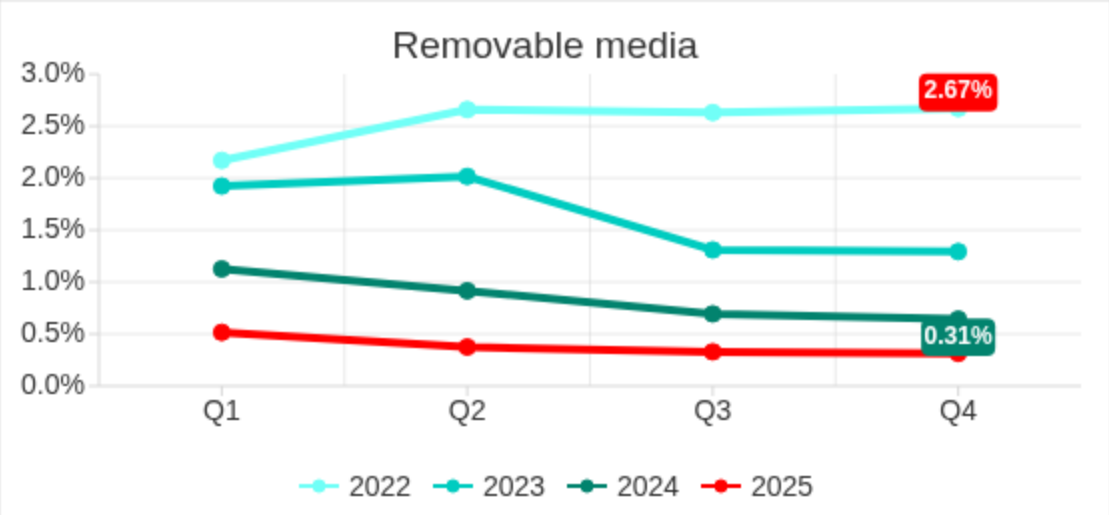
Percentage of ICS computers on which threats from email clients were blocked, Q1 2022–Q4 2025



The main categories of threats from email clients blocked on ICS computers are malicious scripts and phishing pages, spyware, and malicious documents. In Q4 2025, the percentage of ICS computers on which worms in email attachments were blocked doubled as a result of an increase in the number of phishing attacks aimed at delivering Backdoor.MSIL.XWorm.

Over the past three years, the percentage of ICS computers on which threats from removable media were blocked has steadily decreased. Compared to Q4 2022, this figure has decreased by a factor of 8.6.

Percentage of ICS computers on which threats from removable media were blocked, Q1 2022–Q4 2025



Mass infection of computers with viruses and worms via removable media and infected files on the internet has given way to smaller localized outbreaks. Such outbreaks within a single OT network are often caused by infected backups or infected computers considered too old to support modern security technologies.

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

Feature of the quarter: worms in email

In Q4 2025, the percentage of ICS computers on which worms in email attachments were blocked increased in all regions of the world.

Many of the blocked threats related to the worm Backdoor.MSIL.XWorm. This malware is designed to persist in the system and then remotely control it.

Interestingly, this threat was not detected on ICS computers in the previous quarter, yet it appeared in all regions in Q4 2025.

A study found that the active spread of Backdoor.MSIL.XWorm via phishing emails is likely linked to the use by hackers of another malware obfuscation technique that was actively used during massive phishing campaigns in Q4 2025. These campaigns have been known since 2024 as “Curriculum-vitae-catalina”.

During the campaign, the attackers distributed phishing emails to HR managers, recruiters, and employees responsible for hiring. The messages were disguised as responses from job applicants with subjects such as "Resume" or "Attached Resume" and contained a malicious executable file under the guise of a curriculum vitae. Typically, the file was named Curriculum Vitae-Catalina.exe. When executed, it infected the system.

In Q4 2025, the threat spread across regions in two waves — one in October and another in November. Russia, Western Europe, South America, and North America (Canada) were attacked in October. A spike in Backdoor.MSIL.XWorm blocking was observed in other regions in November. The attack subsided in all regions in December.

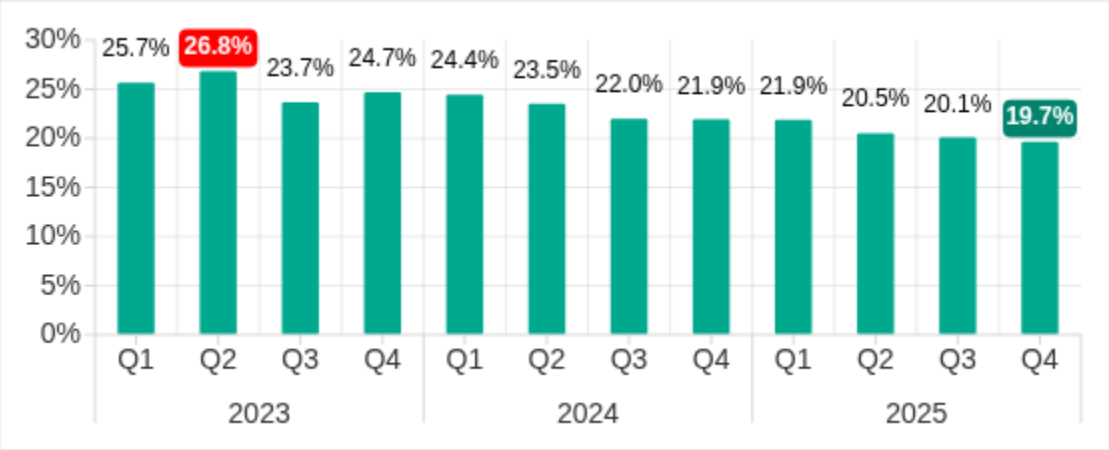
The highest percentage of ICS computers on which Backdoor.MSIL.XWorm was blocked was observed in regions where threats from email clients were traditionally blocked at high rates on ICS computers: Southern Europe, South America, and the Middle East.

At the same time, in Africa, where USB storage media are still actively used, the threat was also detected when removable devices were connected to ICS computers.

Statistics across all threats

The percentage of ICS computers on which malicious objects were blocked has been decreasing since the beginning of 2024. In Q4 2025, it was 19.7%. Over the past three years, the percentage has decreased 1.35 times, and 1.25 times since Q4 2023.

Percentage of ICS computers on which malicious objects were blocked, Q1 2023–Q4 2025

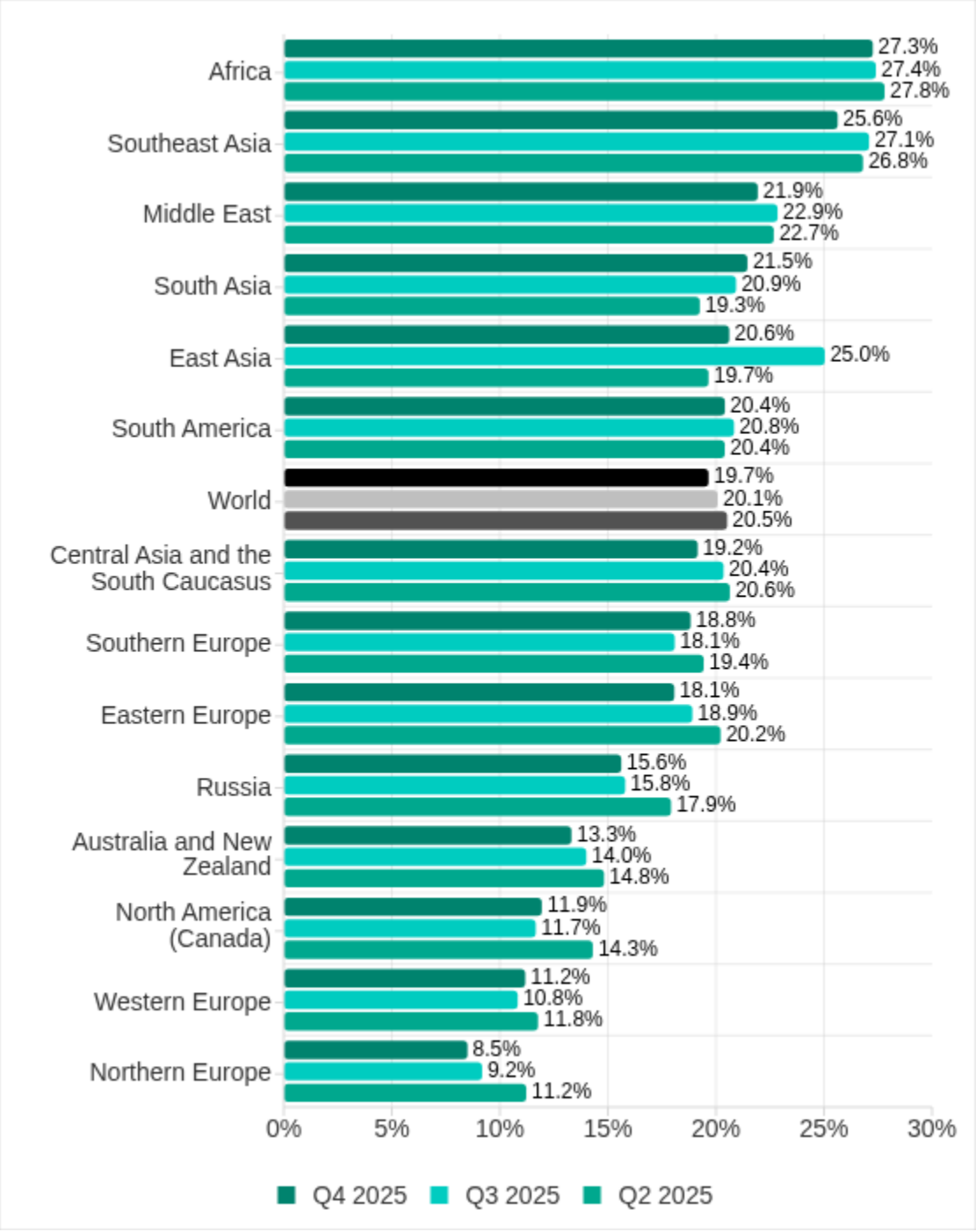


The highest percentage of ICS computers on which malicious objects were blocked during 2025 occurred in April, and in December during Q4 2025.

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

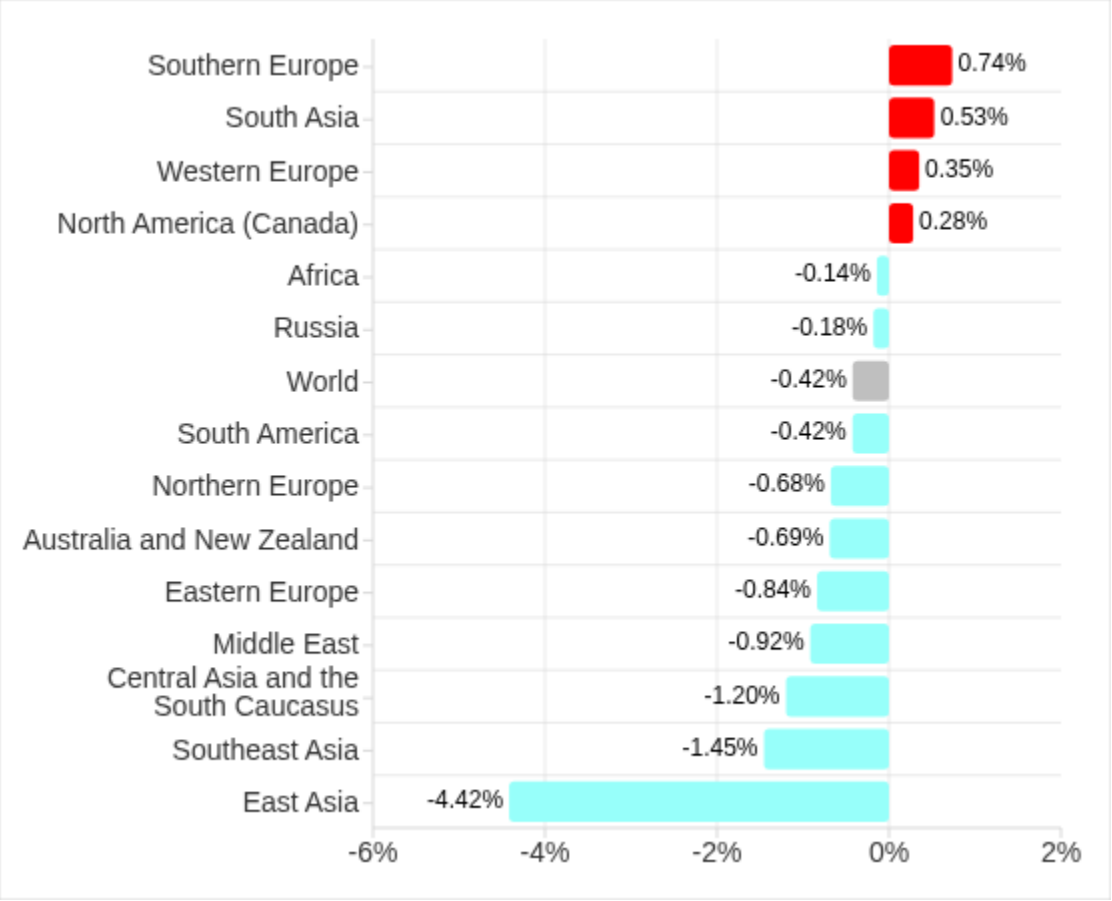
Regionally, in Q4 2025, the percentage of ICS computers on which malicious objects were blocked ranged from 8.5% in Northern Europe to 27.3% in Africa.

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



Four regions saw an increase in the percentage of ICS computers on which malicious objects were blocked. The most notable increases occurred in Southern Europe and South Asia. In Q3 2025, East Asia experienced a sharp increase triggered by the local spread of malicious scripts, but the figure has since returned to normal.

Changes in percentage of ICS computers on which malicious objects were blocked, Q4 2025

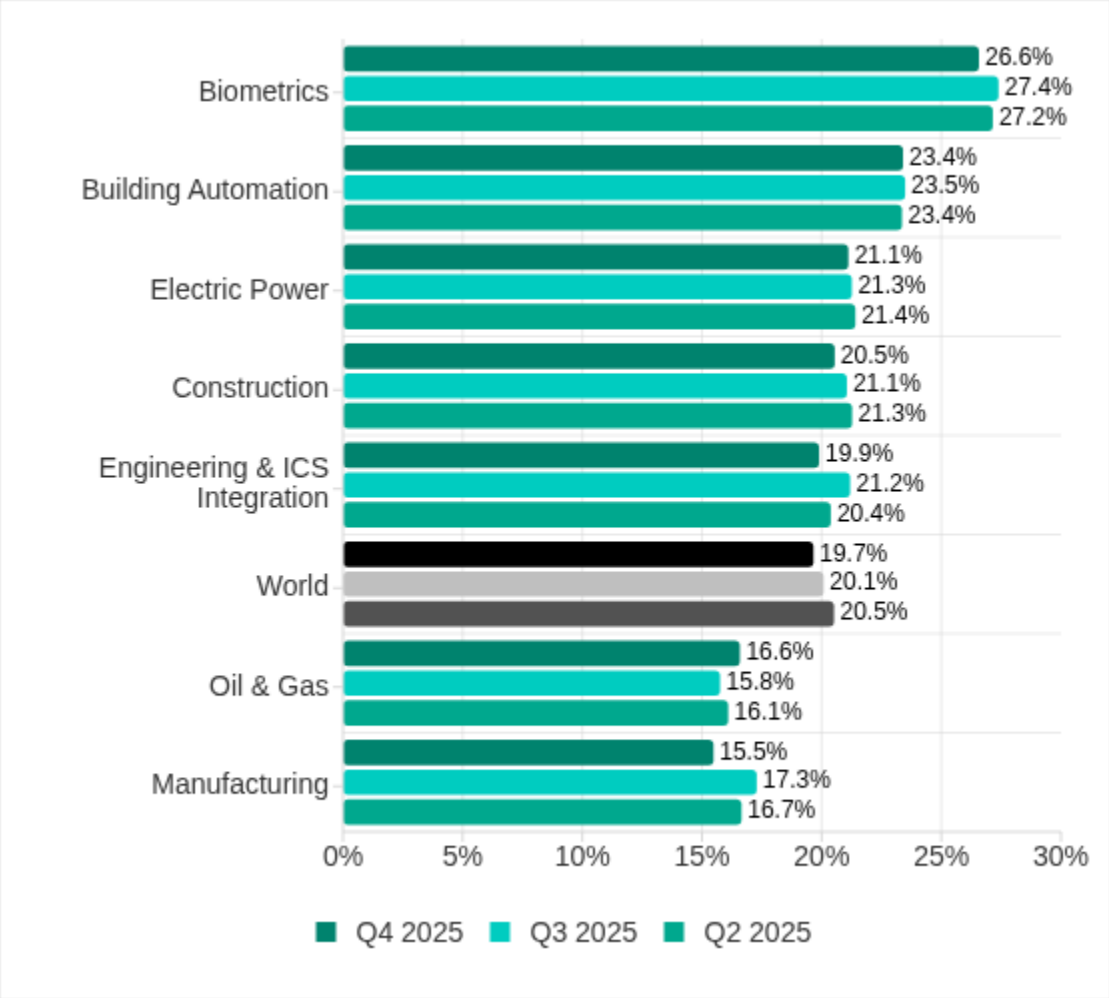


Selected industries

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

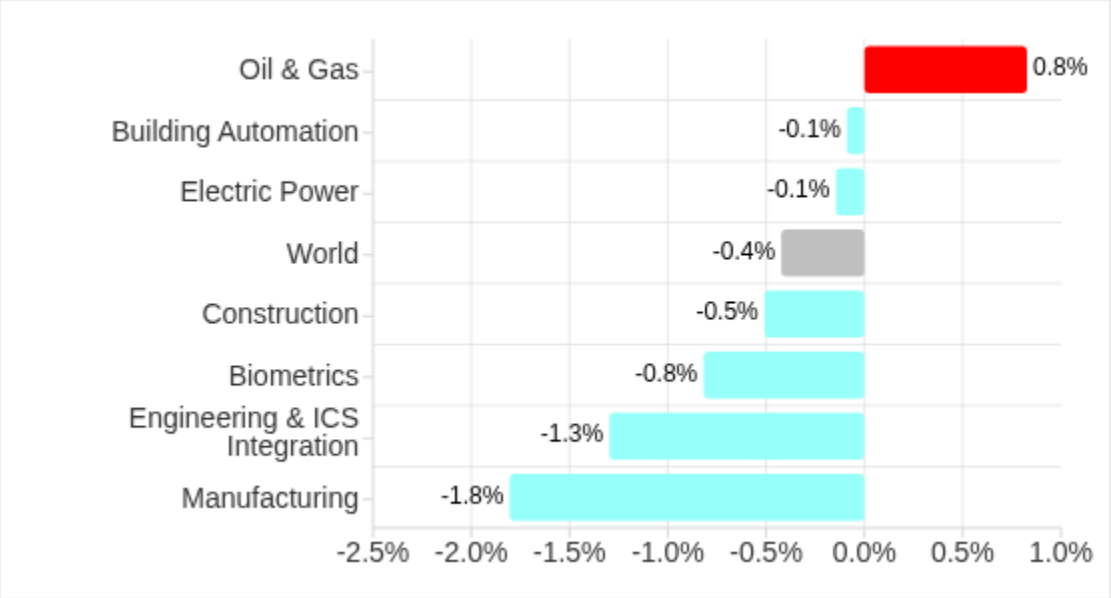
These systems are characterized by accessibility to and from the internet, as well as and minimal cybersecurity controls by the consumer organization.

Ranking of industries and OT infrastructure by percentage of ICS computers on which malicious objects were blocked

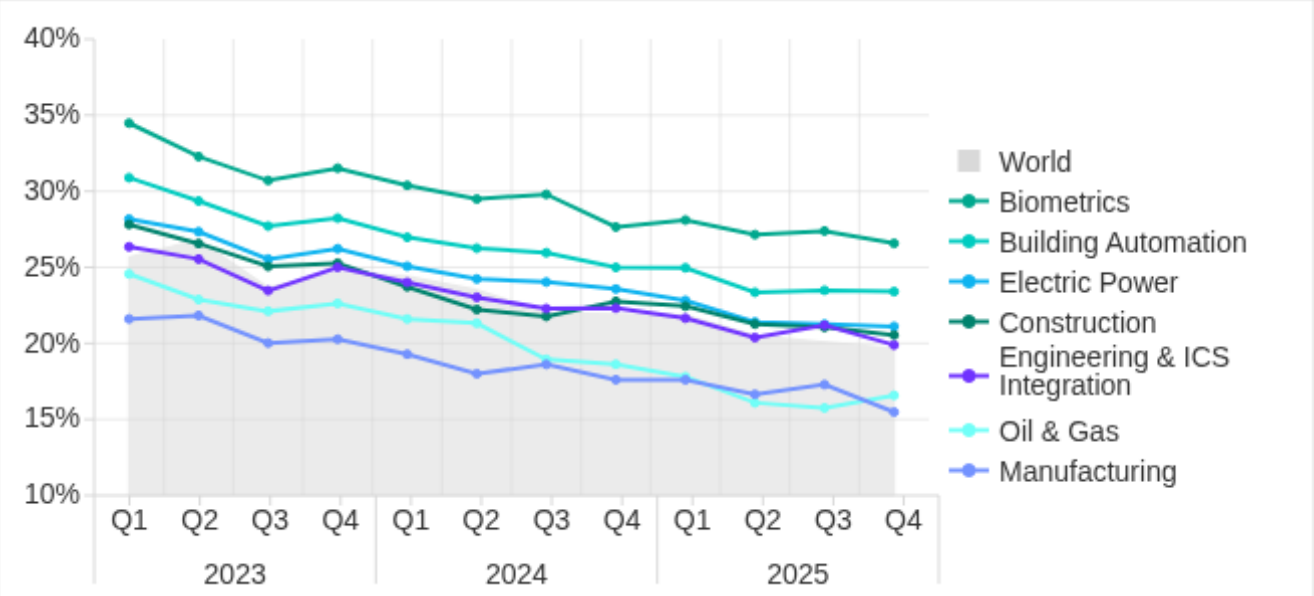


In Q4 2025, the percentage of ICS computers on which malicious objects were blocked increased only in one sector: oil and gas. The corresponding figures increased in two regions: Russia, and Central Asia and the South Caucasus.

Changes in percentage of ICS computers on which malicious objects were blocked in selected industries, Q4 2025



There is a downward trend in all the surveyed 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.

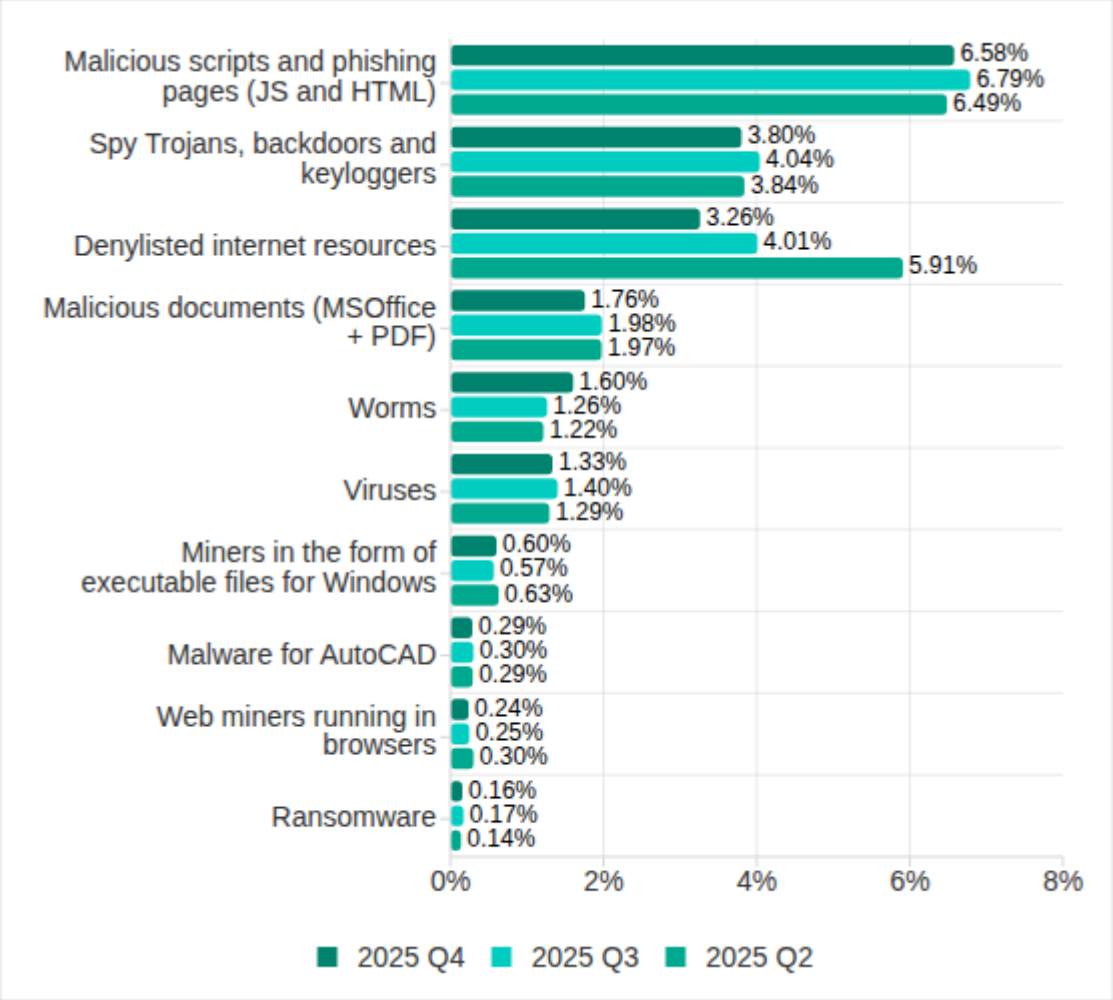
Malware for AutoCAD does not belong to a specific group, as it can spread in a variety of ways.

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.

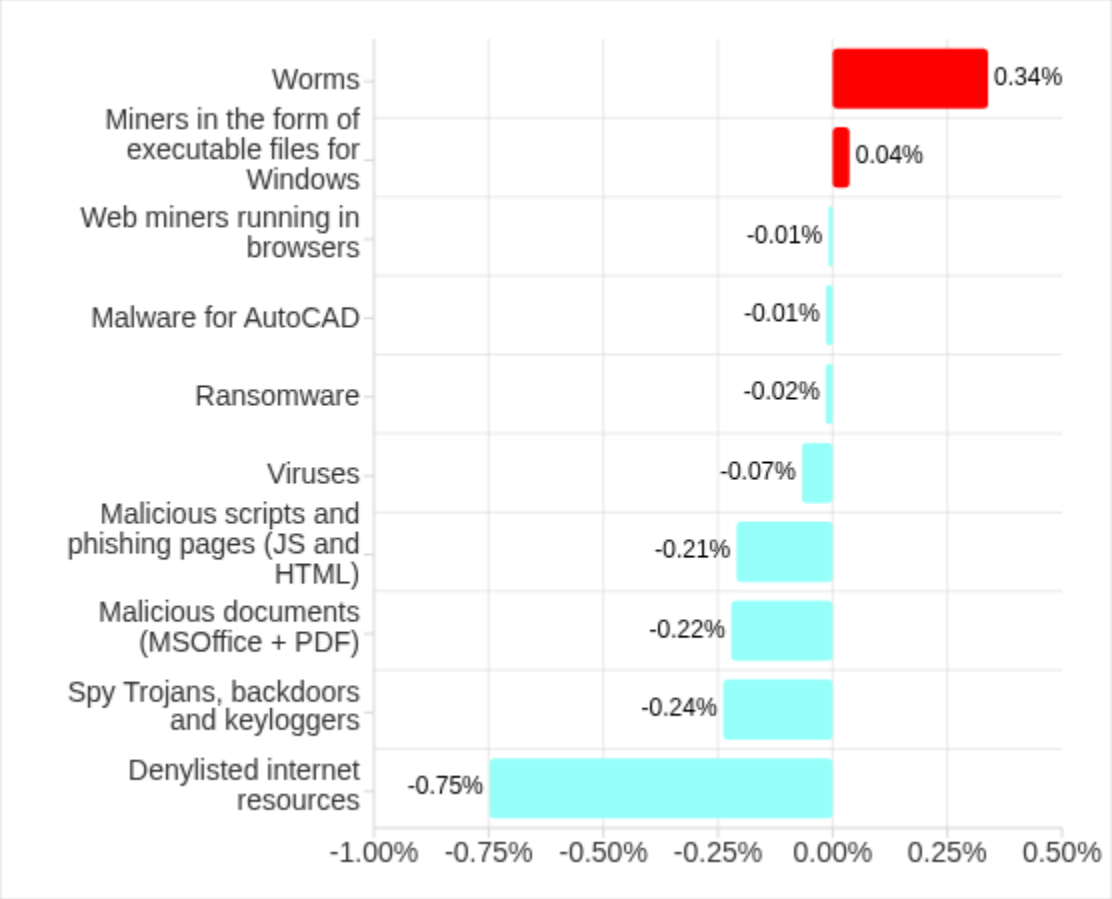
In Q4 2025, the malicious scripts and phishing pages category led the other threat categories in terms of the percentage of ICS computers on which this threat was blocked. As in the previous quarter, spyware ranked second.

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



In Q4 2025, there was an increase in the percentage of ICS computers on which worms, and miners in the form of executable files for Windows were blocked. These were the only categories that exhibited an increase.

Changes in percentage of ICS computers on which malicious objects from different categories were blocked, Q4 2025



For the second consecutive quarter, there was a decrease in the percentage of ICS computers on which denylisted internet resources were blocked. This figure has almost halved (a decrease of 1.8 times) since Q2 2025.

It is worth noting that the techniques for deploying malware on the internet are diverse, extensive and accessible to any attacker. Any web service, even the most secure, can be used as a web storage if it allows data to be stored and requested. In practice, this means that, like any other environment, the OT-environment must be protected by the entire security technology stack, not just the network perimeter.

Threat categories

In Q4 2025, Kaspersky protection solutions blocked malware from 10,142 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.

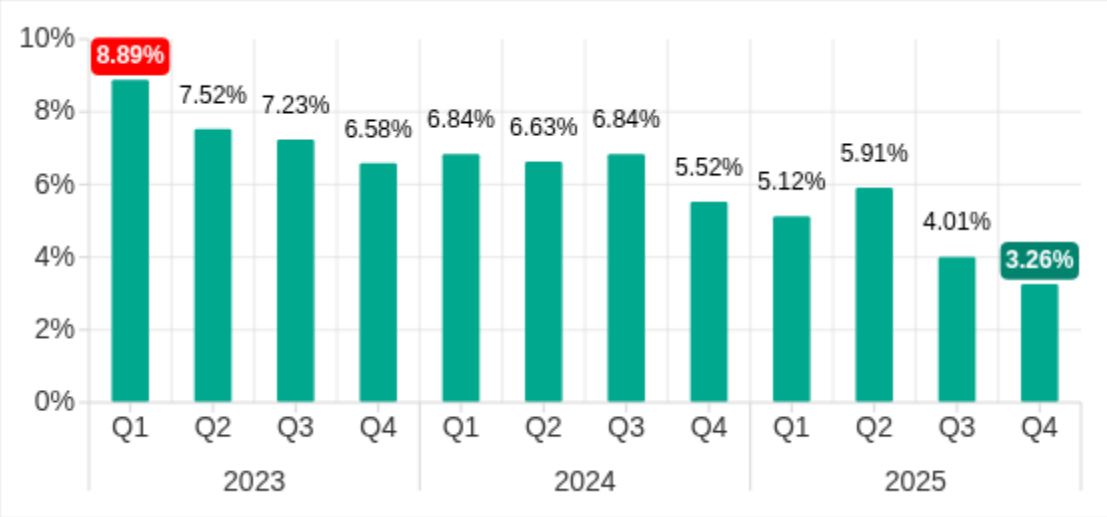
A significant portion of these resources is used to distribute malicious scripts and phishing pages (HTML).

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.

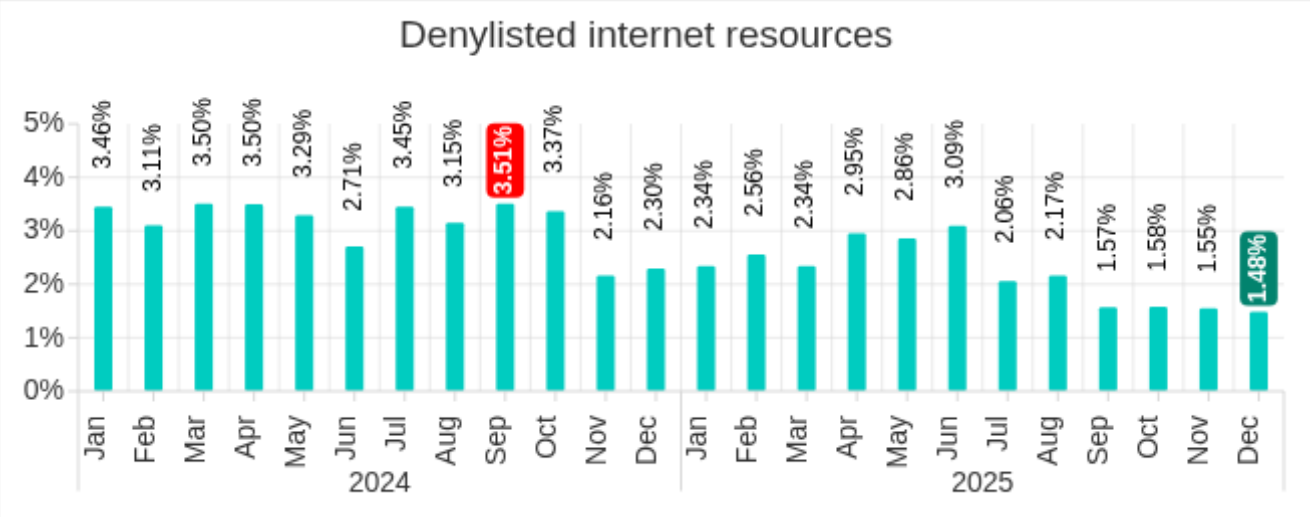
High parameter values usually indicate weak control over the implementation of information security policies (ICS computers have access to the internet in one way or another), phishing protection weaknesses (many malicious links are delivered via phishing messages) and deficiencies in information security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

In Q4 2025, the percentage of ICS computers on which denylisted internet resources were blocked decreased to 3.26%. This is the lowest quarterly figure since the beginning of 2022, and it has decreased 1.8 times since Q2 2025.

Percentage of ICS computers on which denylisted internet resources were blocked, Q1 2023–Q4 2025



From December 2024 until June 2025, the figure increased month on month with minor fluctuations. In the second half of the year, however, it began to decrease again, reaching its lowest level of the entire review period in December.

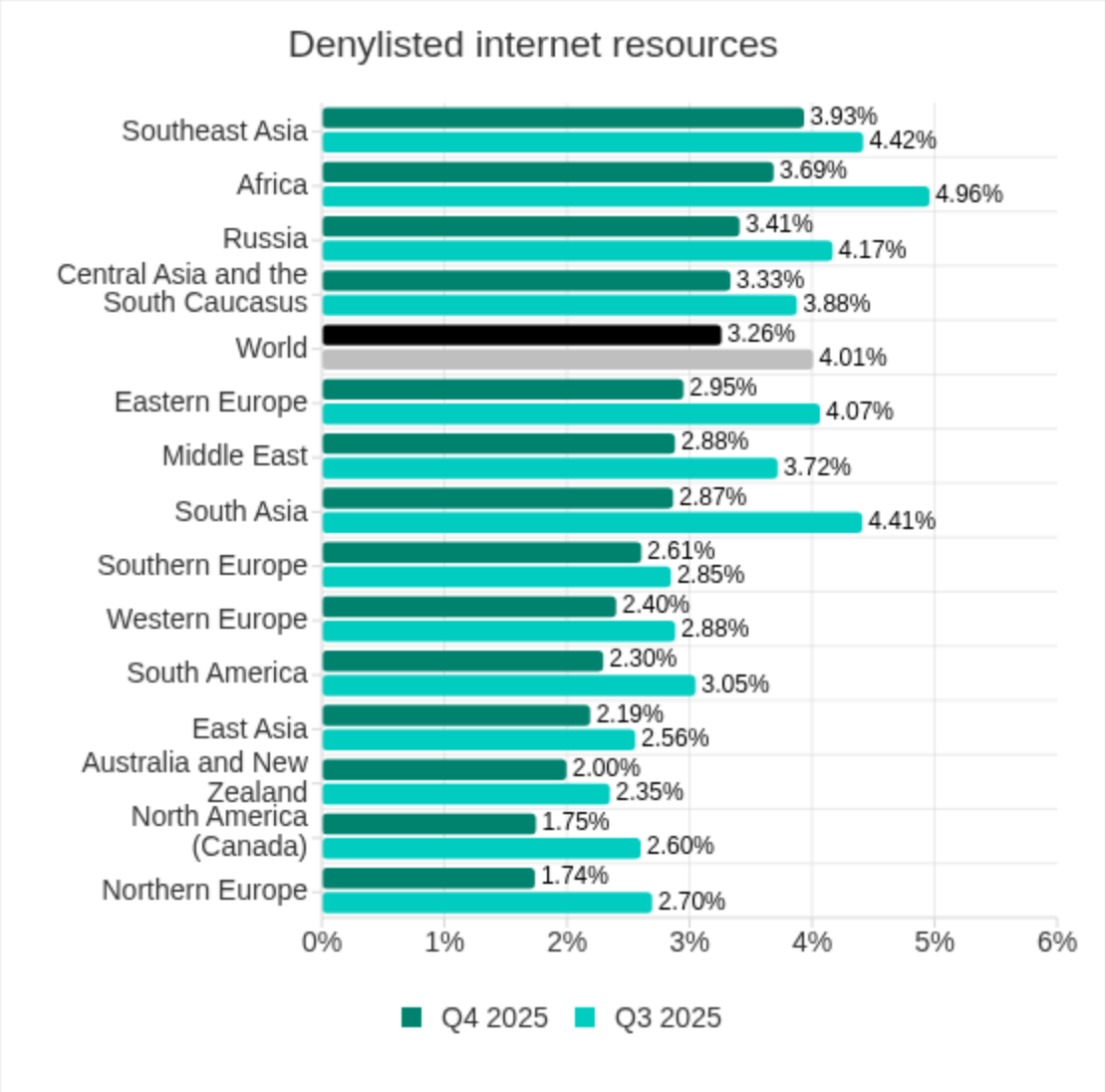


Percentage of ICS computers on which denylisted internet resources were blocked, January 2024—December 2025

For a long time denylisted internet resources ranked first or second in the ranking of malware categories by the percentage of attacked computers. In Q3 2025, this category dropped to third place for the first time, where it remained in Q4.

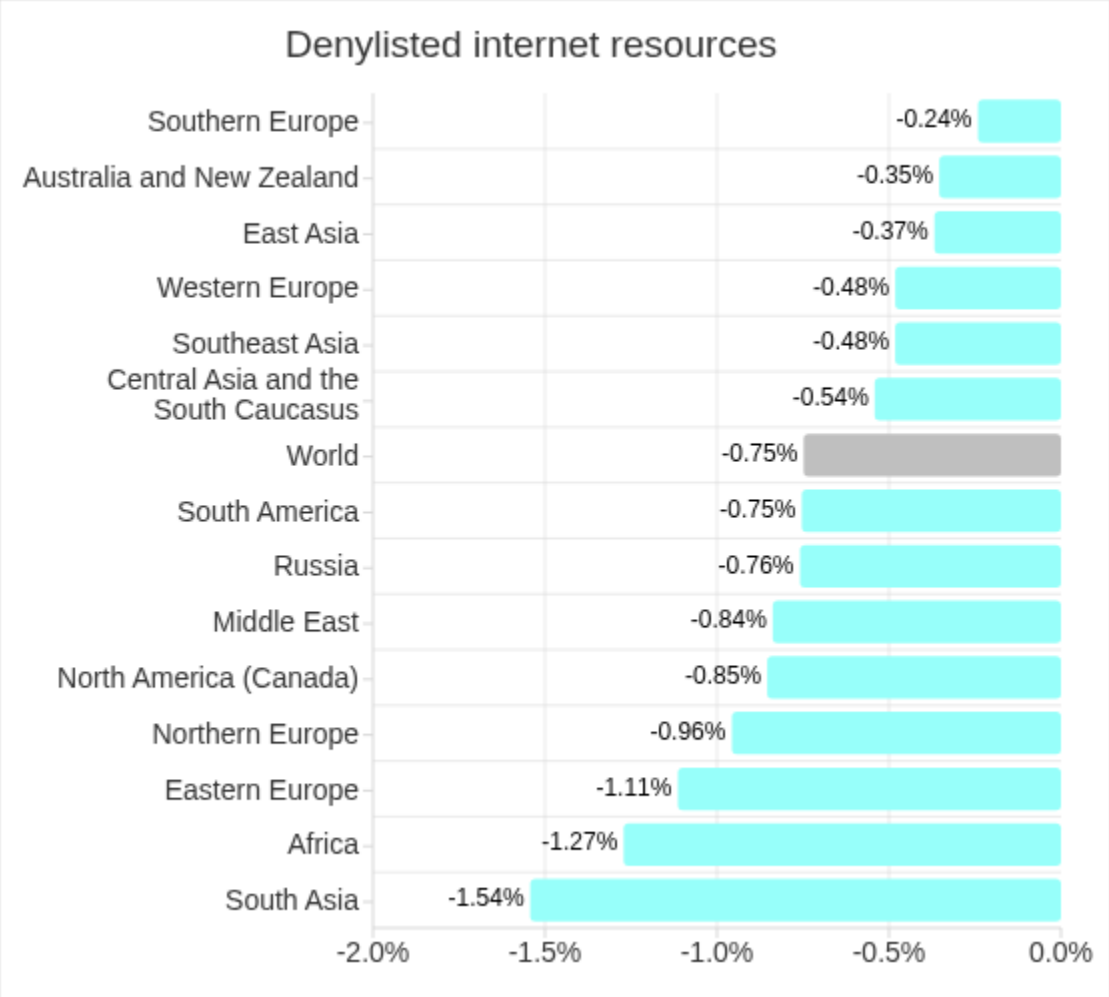
Regionally, the percentage of ICS computers on which denylisted internet resources were blocked ranged from 1.74% in Northern Europe to 3.93% in Southeast Asia, which displaced Africa from first place. Russia rounded out the top three regions for this indicator.

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



As in the previous quarter, the percentage decreased in all regions in Q4 2025.

Changes in percentage of ICS computers on which denylisted internet resources were blocked, Q4 2025



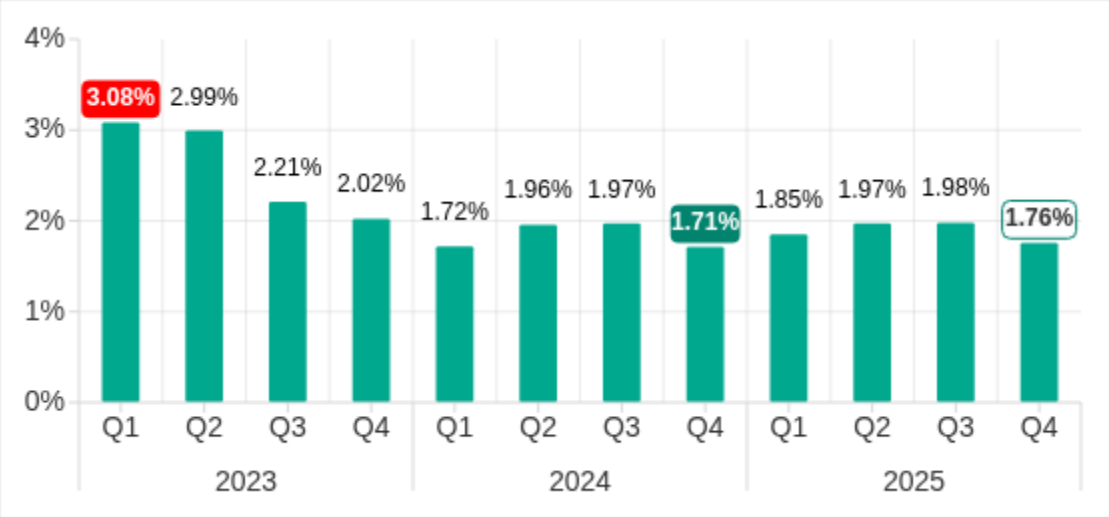
Malicious documents (MSOffice + PDF)

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.

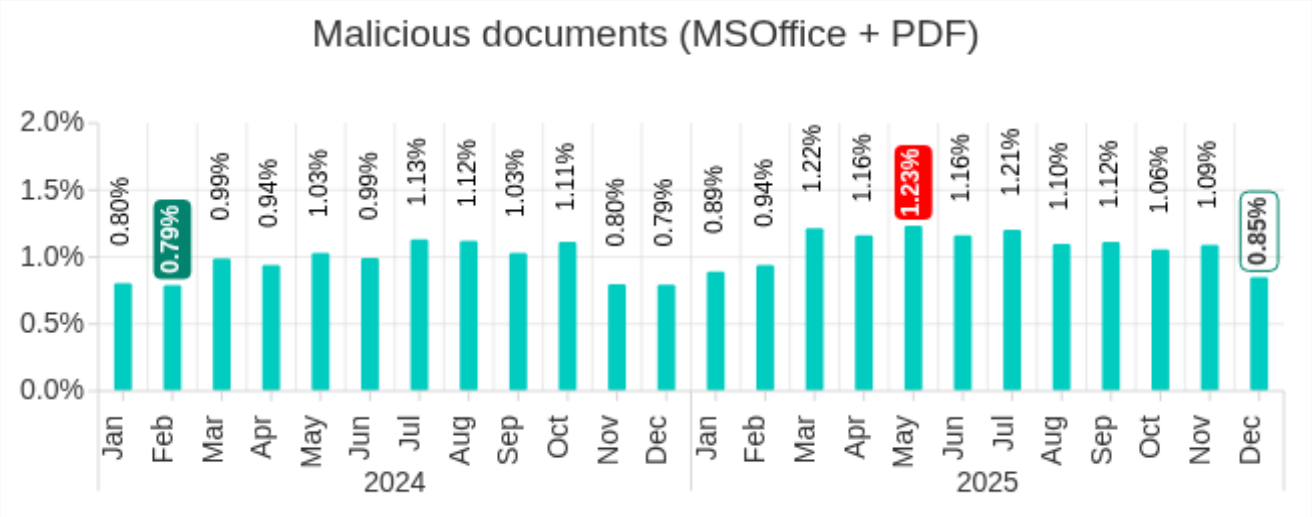
Malicious documents remain a popular vector for targeted attacks, especially those using zero-day exploits. In 2025, CISA issued more than 450 advisories, many of which were related to file handling, including popular document formats.

Following a decline at the end of 2024, the percentage of ICS computers on which malicious documents were blocked increased for three consecutive quarters. However, in Q4 2025 it decreased by 0.22 pp to 1.76%.

Percentage of ICS computers on which malicious documents were blocked, Q1 2023–Q4 2025



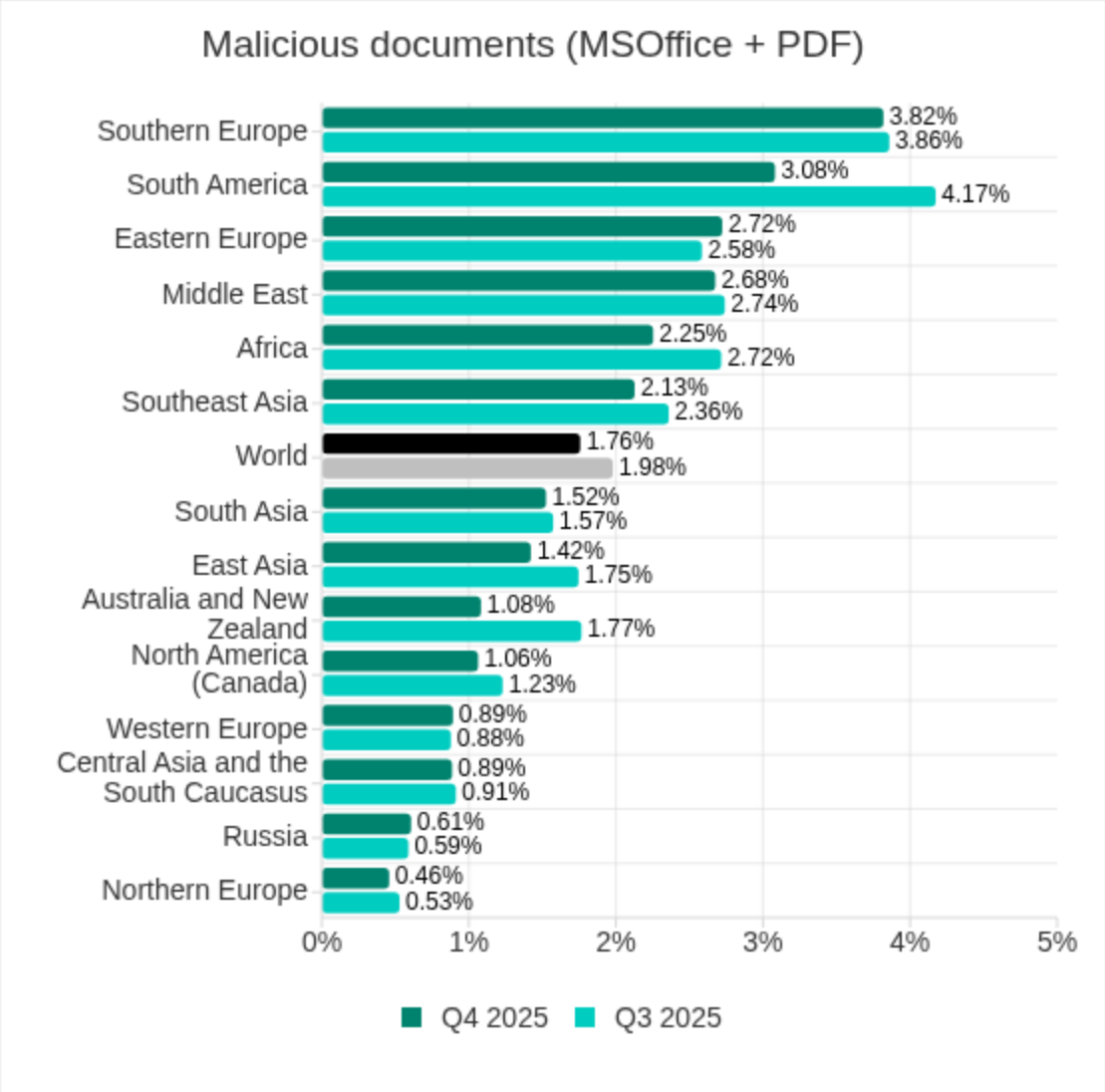
In 2025, the percentage increased every month until May, when it reached its highest level in two years. After that, it gradually decreased. In December, the percentage of ICS computers on which malicious documents were blocked reached its lowest point in a year.



Percentage of ICS computers on which malicious documents were blocked, January 2024—December 2025

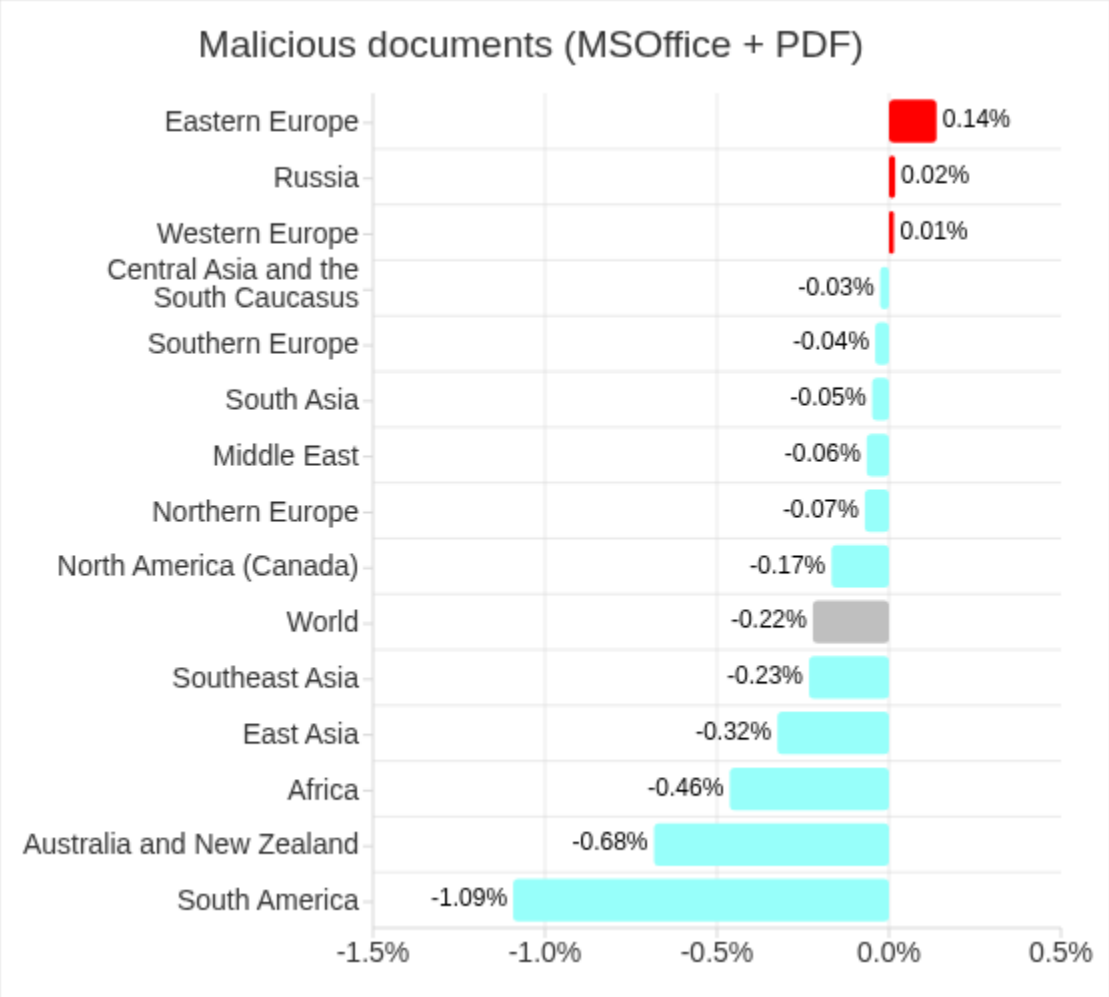
Regionally, the percentage of ICS computers on which malicious documents were blocked ranged from 0.46% in Northern Europe to 3.82% in Southern Europe. Southern Europe and South America remained among the top three regions for this indicator, but the Middle East was replaced by Eastern Europe.

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



In Q4 2025, the percentage increased in three regions: Eastern Europe, Russia, and Western Europe.

Changes in percentage of ICS computers on which malicious documents were blocked, Q4 2025

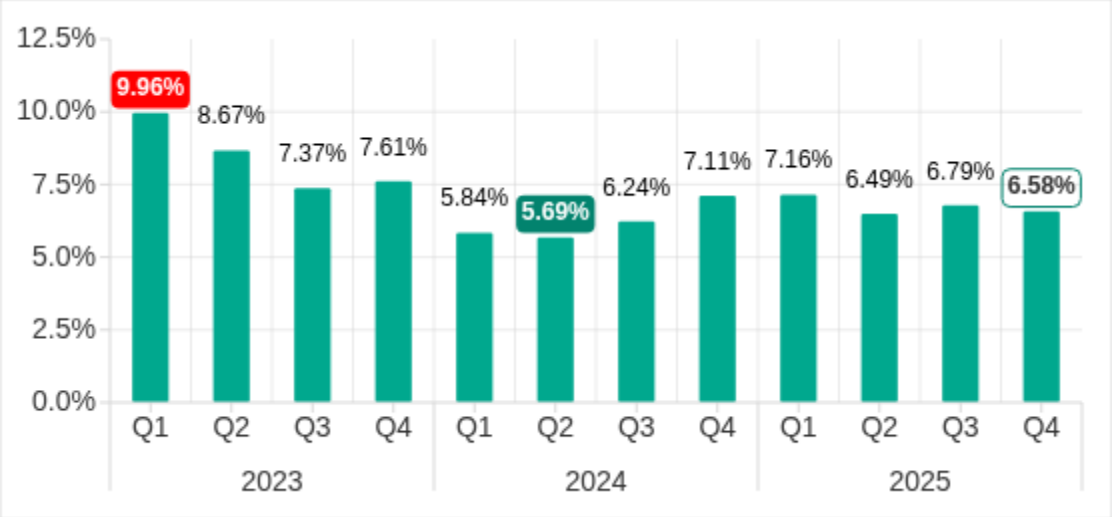


Malicious scripts and phishing pages (JS and HTML)

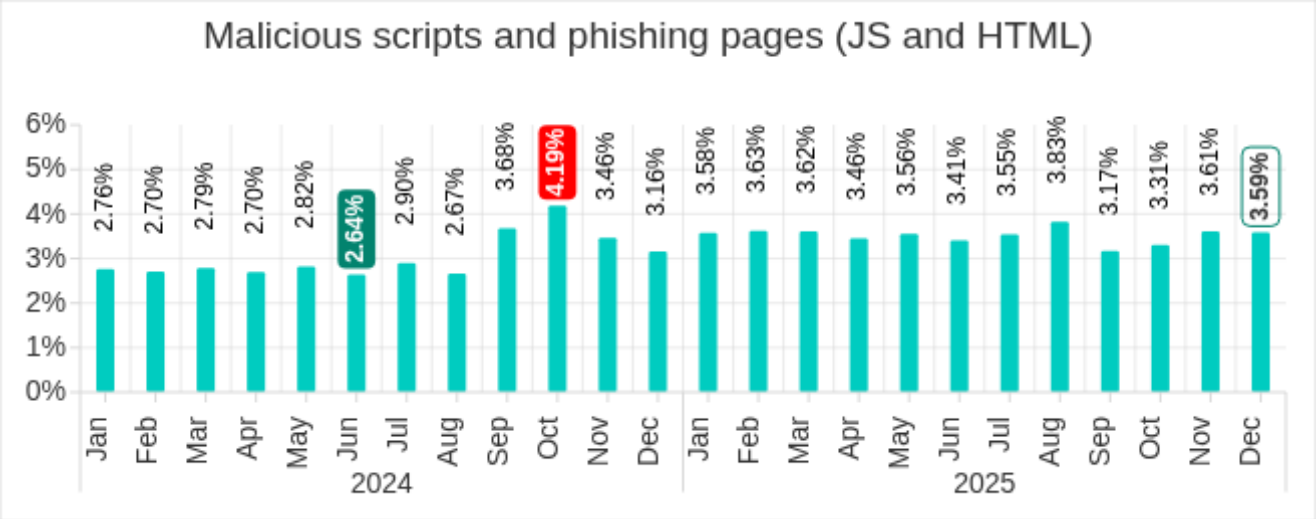
Malicious actors use scripts for a wide range of objectives: collecting information, tracking, redirecting the browser to a malicious site, and uploading various types of malware (spyware, silent crypto mining tools, ransomware) to the user's system or browser. These spread via the internet and email.

In Q4 2025, the percentage of ICS computers on which malicious scripts and phishing pages were blocked decreased to 6.58%. Despite the decline, 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, Q1 2023–Q4 2025



The highest monthly value for this indicator in 2025 was recorded in August. Of the three months in Q4, the highest value was recorded in November.

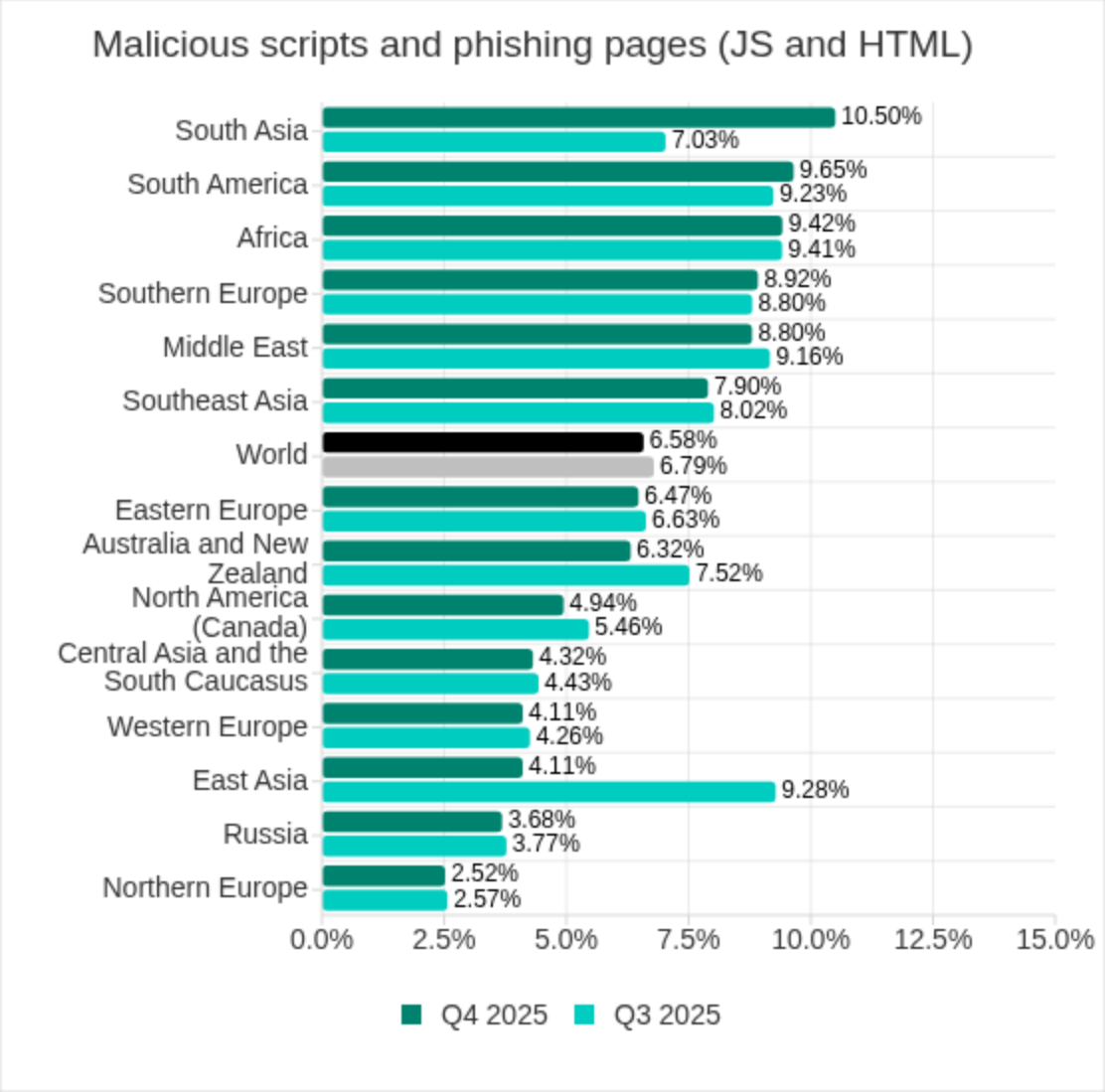


Percentage of ICS computers on which malicious scripts and phishing pages were blocked, January 2024—December 2025

Regionally, the percentage of ICS computers on which malicious scripts and phishing pages were blocked ranged from 2.52% in Northern Europe to 10.50% in South Asia, which jumped from eighth to first place in the corresponding regional ranking.

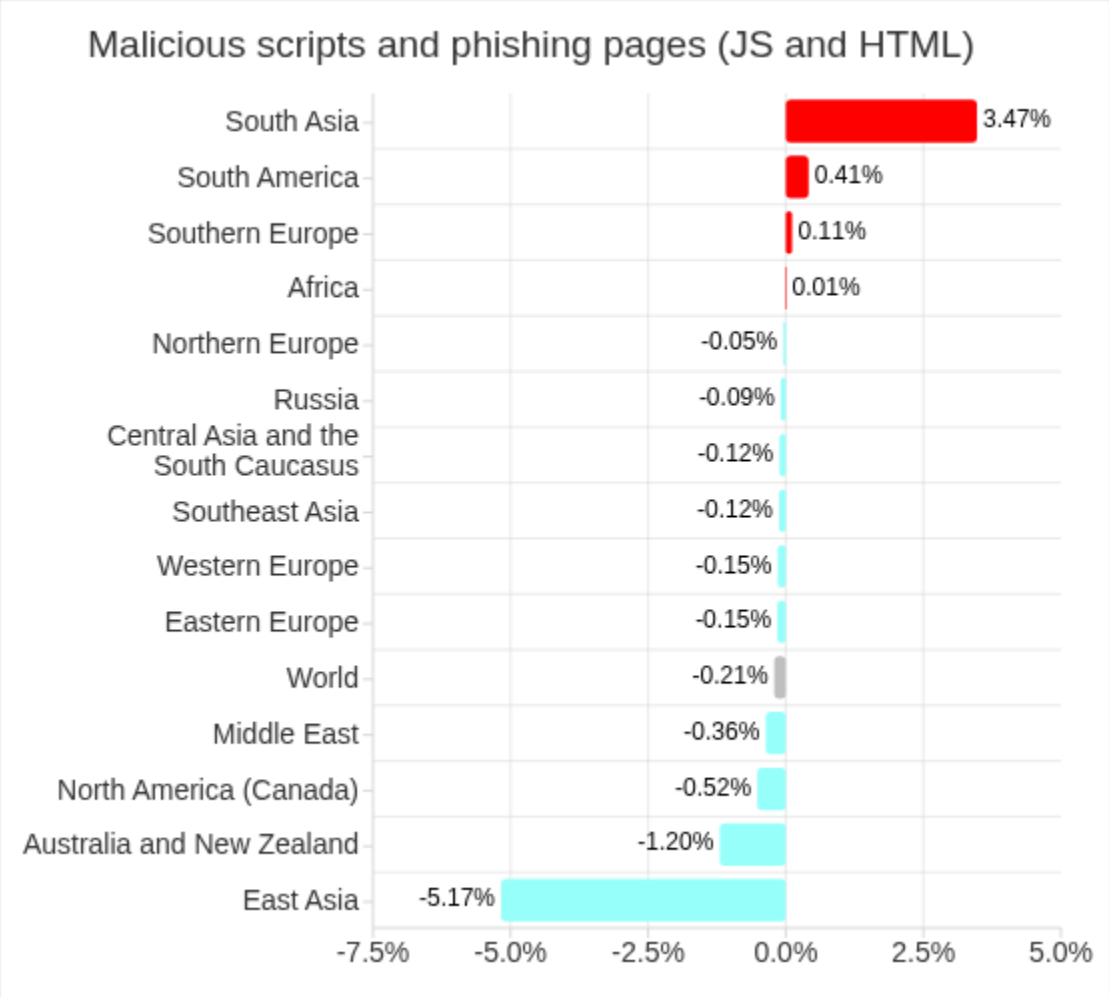
Meanwhile, East Asia dropped from second to 12th place. In Q3 2025, the region's percentage increased by 5.23 pp as a result of the local spread of malicious spyware scripts loaded into the memory of popular torrent clients, including MediaGet. In Q4, the percentage returned to near its usual rate for the region.

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



In Q4 2025, this indicator increased in four regions: South Asia, South America, Southern Europe, and Africa. South Asia saw the most notable increase, at 3.47 pp.

Changes in percentage of ICS computers on which malicious scripts and phishing pages were blocked, Q4 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

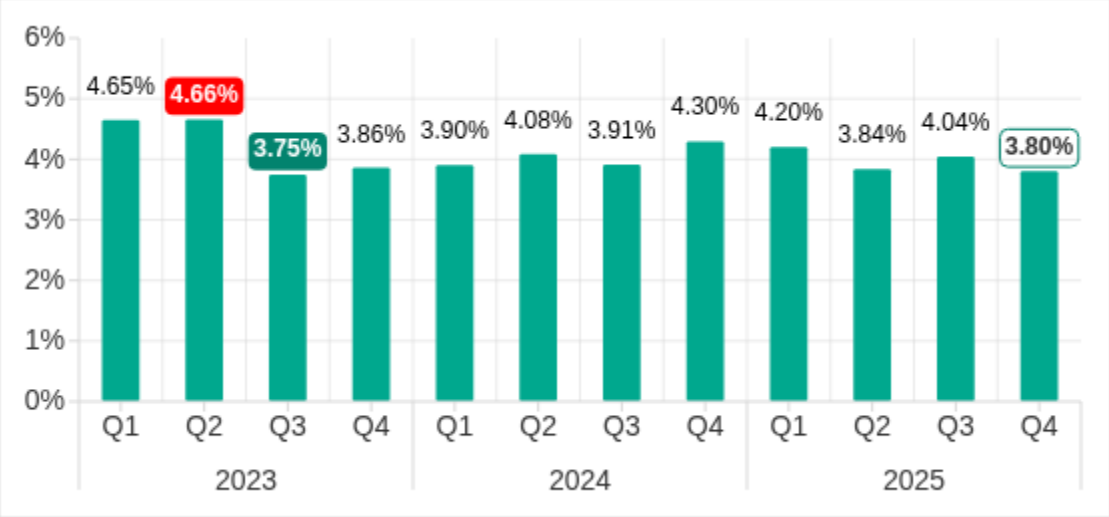
Spyware (spy Trojans, backdoors, and keyloggers) can be found in lots of phishing emails sent to industrial organizations. Spyware is the most frequently detected next-stage malware. It is used as a tool for the intermediate stages of a cyberattack (for example, intelligence and distribution over the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

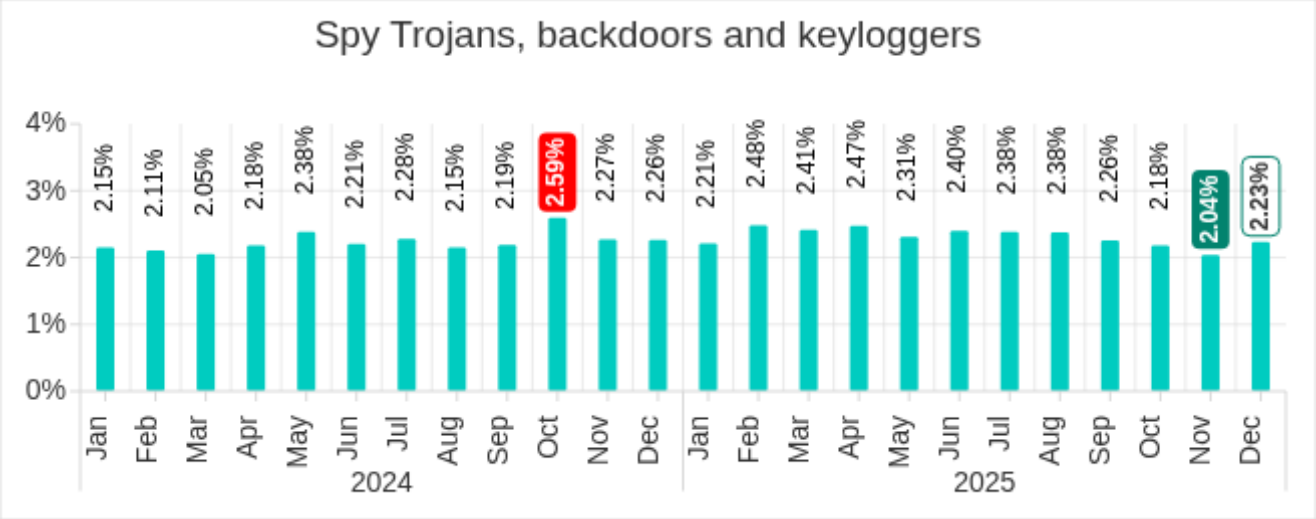
Detection of spyware on an ICS computer usually indicates that the initial infection vector has worked, whether it is clicking on a malicious link, opening an attachment from a phishing email, or connecting an infected USB drive. This indicates the absence or ineffectiveness of measures to protect the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

In Q4 2025, the percentage of ICS computers on which spyware was blocked decreased to 3.80%. For the second quarter in a row, 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, Q1 2023–Q4 2025



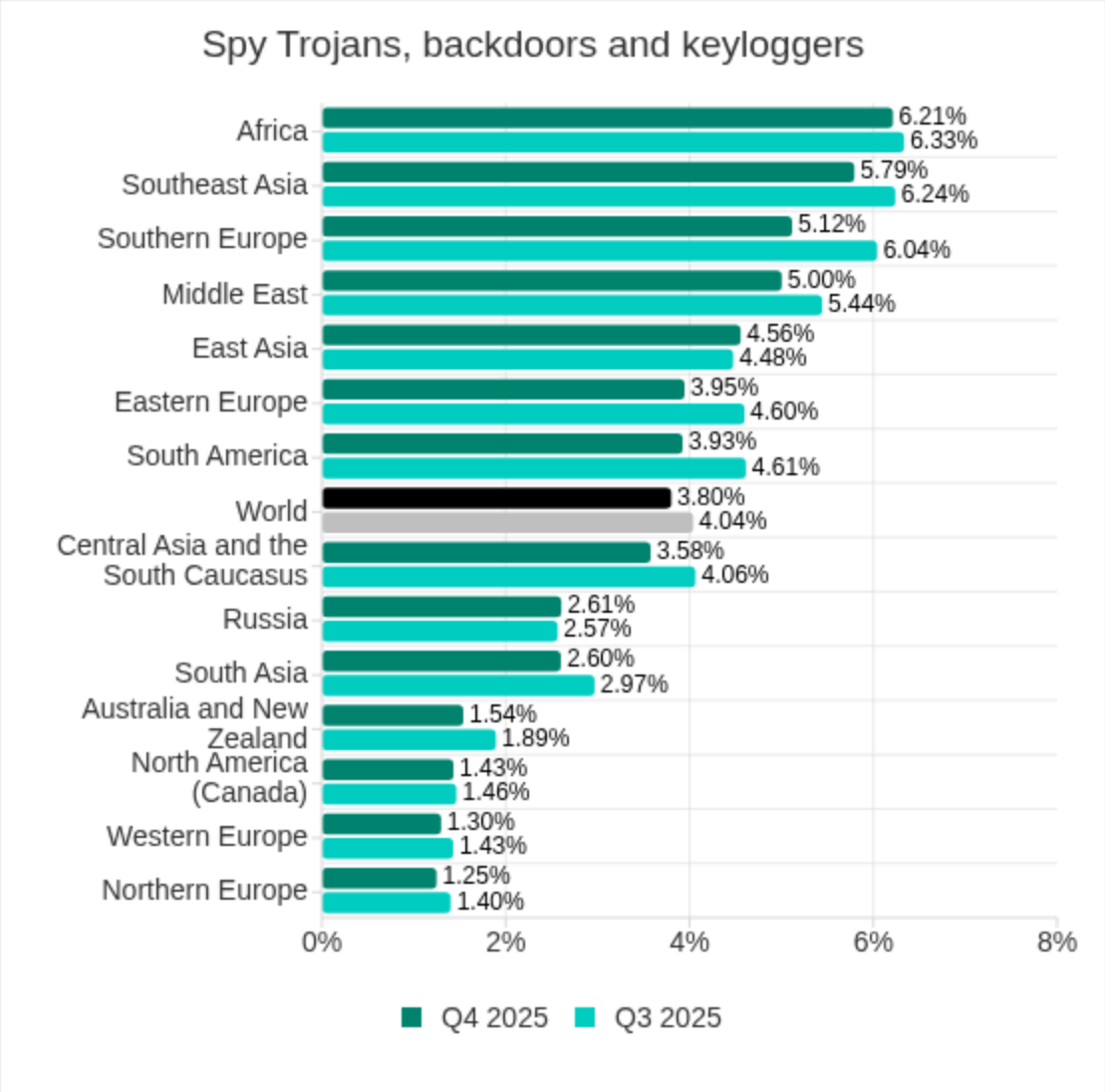
The highest monthly value for this indicator in 2025 was in February. In Q4, the figures for October and November were lower than those for the other months of the year.



Percentage of ICS computers on which spyware was blocked, January 2024—December 2025

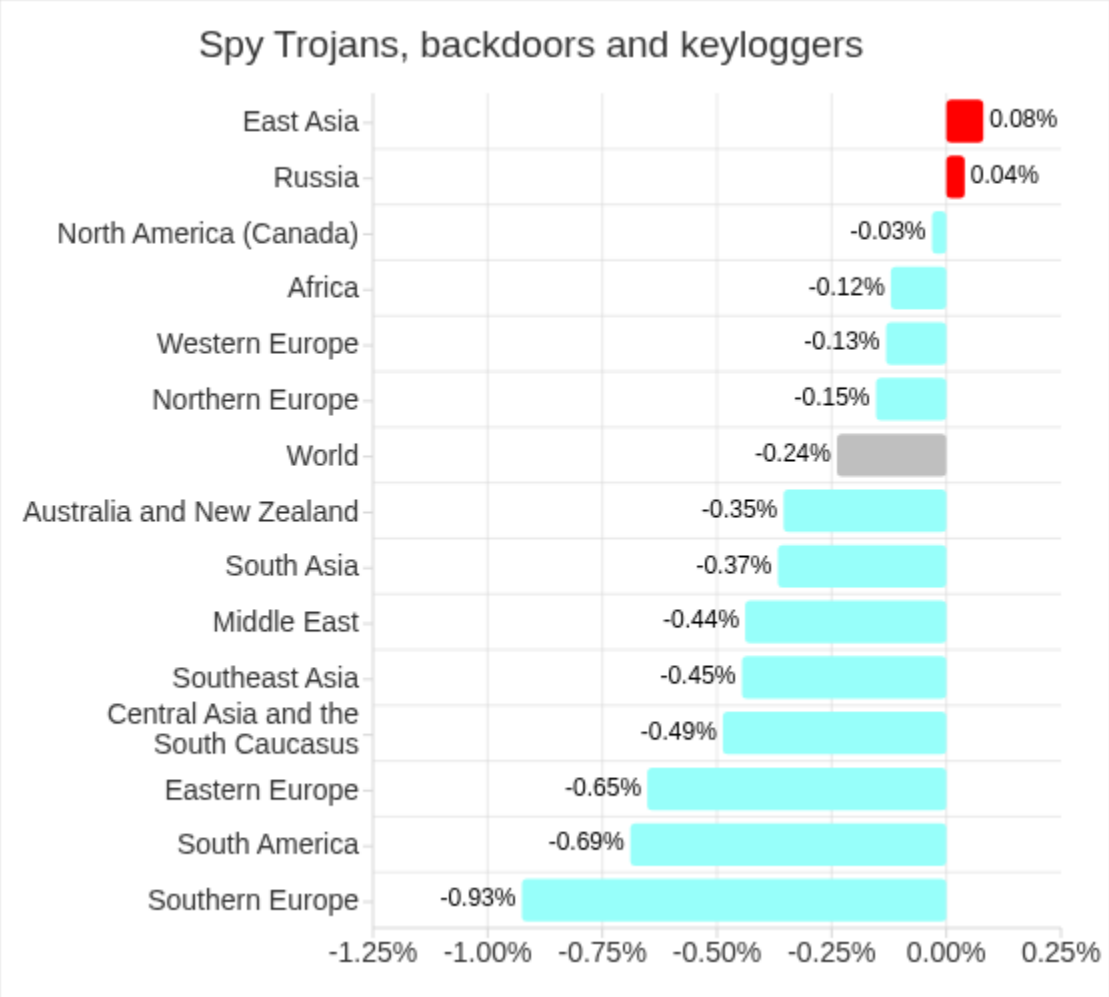
Regionally, the percentage of ICS computers on which spyware was blocked ranged from 1.25% in Northern Europe to 6.21% in Africa. The top three regions for this indicator remained unchanged: Africa, Southeast Asia, and Southern Europe.

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



In Q4 2025, the percentage of ICS computers on which spyware was blocked increased in East Asia and Russia.

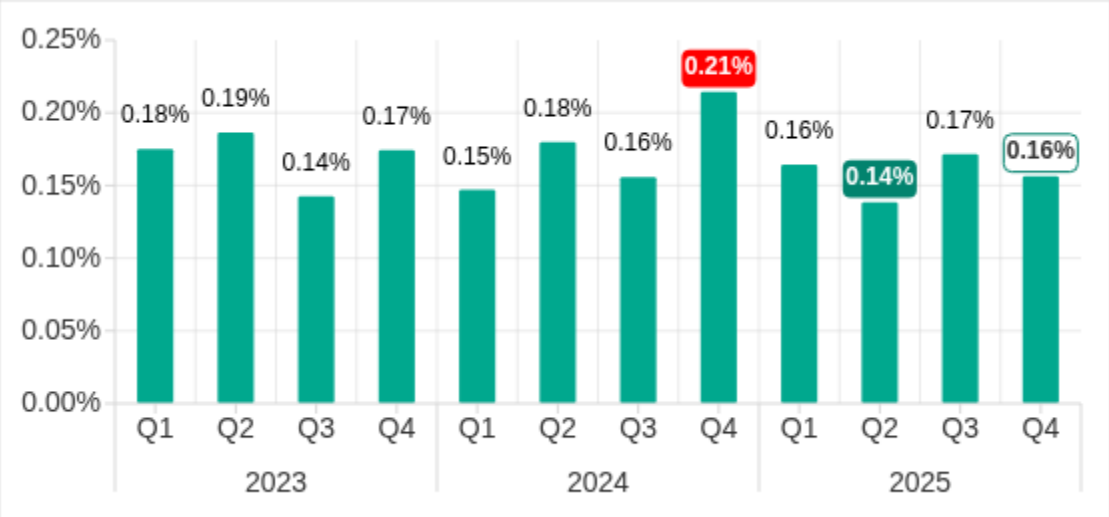
Changes in percentage of ICS computers on which spyware was blocked, Q4 2025



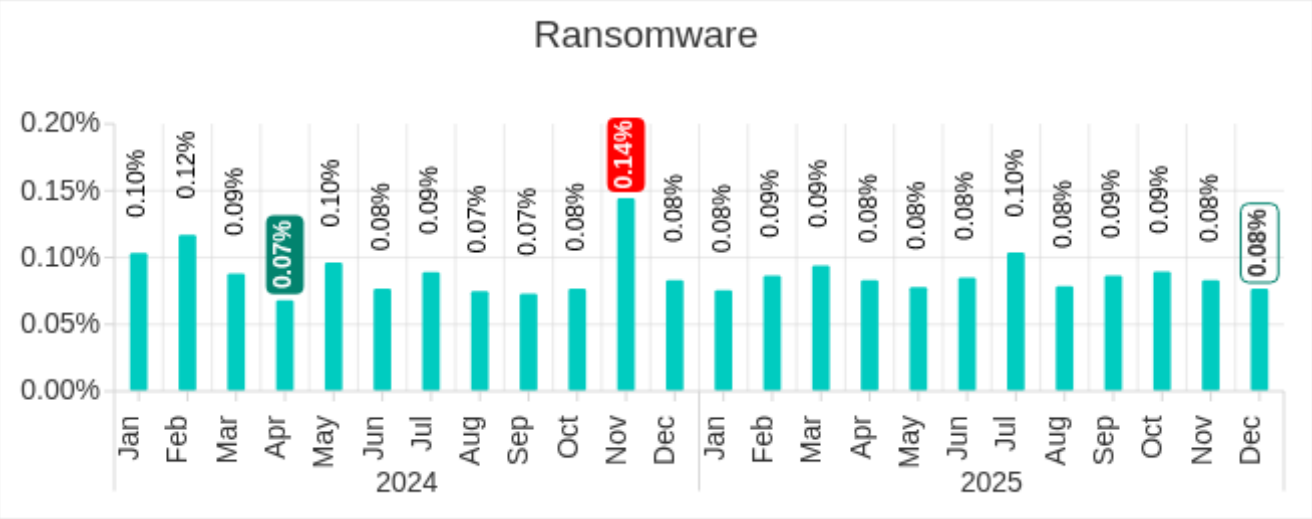
Ransomware

In Q4 2025, the percentage of ICS computers on which ransomware was blocked decreased to 0.16%.

Percentage of ICS computers on which ransomware was blocked, Q1 2023–Q4 2025



The highest monthly value in 2025 was in July.

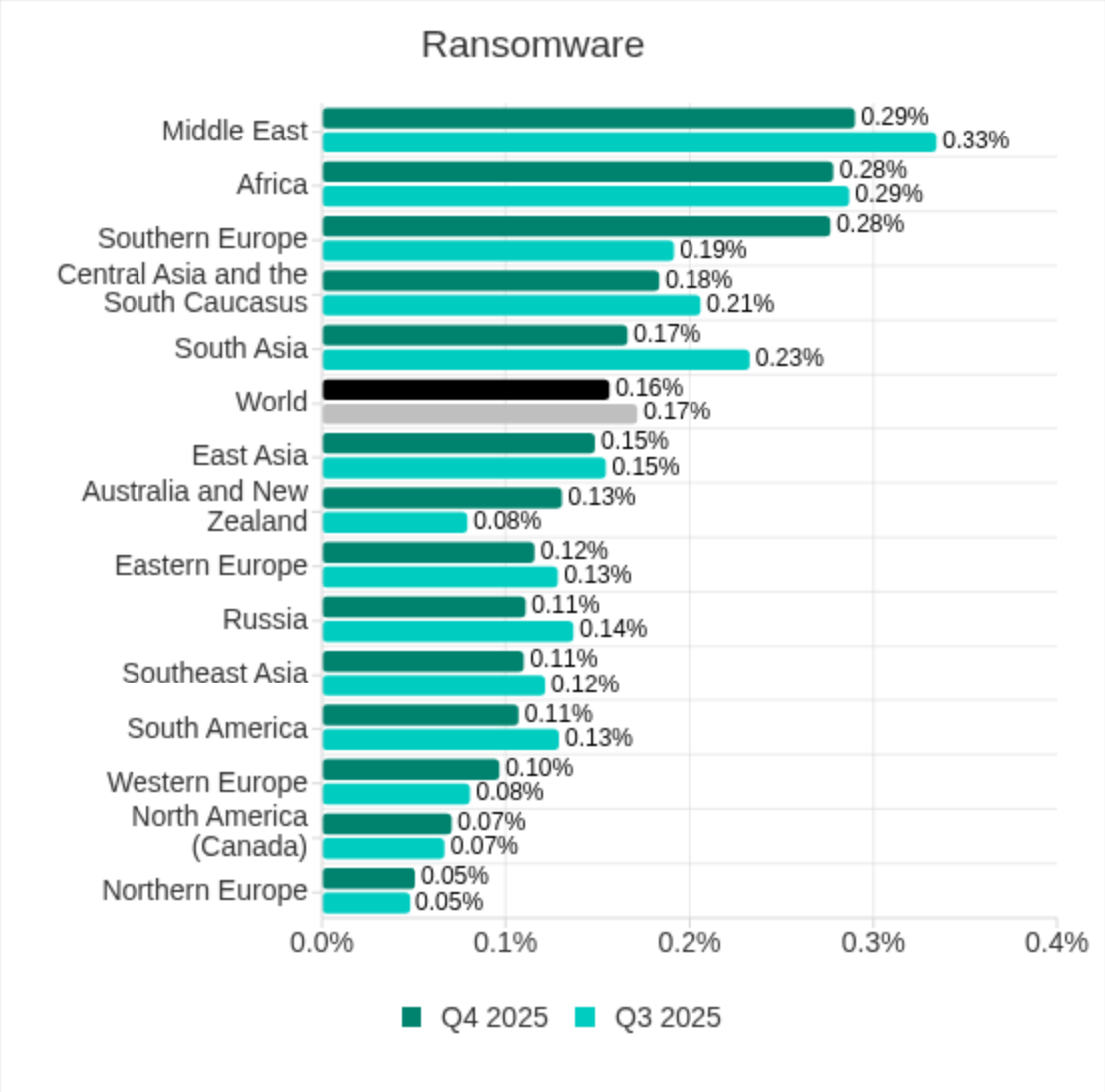


Percentage of ICS computers on which ransomware was blocked, January 2024—December 2025

Regionally, the percentage of ICS computers on which ransomware was blocked ranged from 0.05% in Northern Europe to 0.29% in the Middle East. Besides the Middle East, the top three regions included Africa, and Southern Europe, which rose from fifth to third place in the ranking in Q4 2025. The percentage in Southern Europe increased by a factor of 1.47.

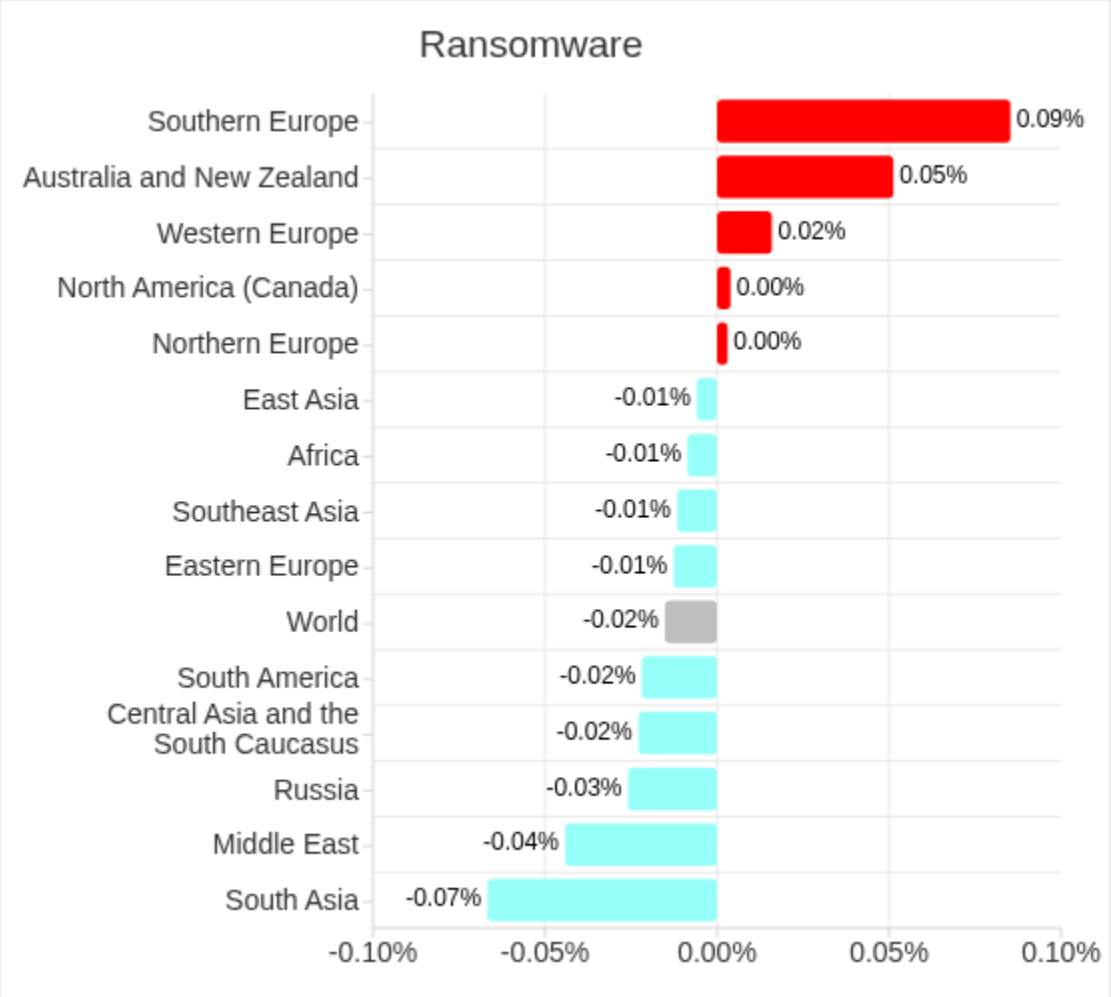
In Q4 2025, Southern Europe led the regions in terms of ransomware in the building automation industry, with 0.61%, up 1.5 times from the previous quarter (0.41%).

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



In Q4 2025, the percentage of ICS computers on which ransomware was blocked significantly increased in three regions: Southern Europe, Australia and New Zealand, and Western Europe.

Changes in percentage of ICS computers on which ransomware was blocked, Q4 2025

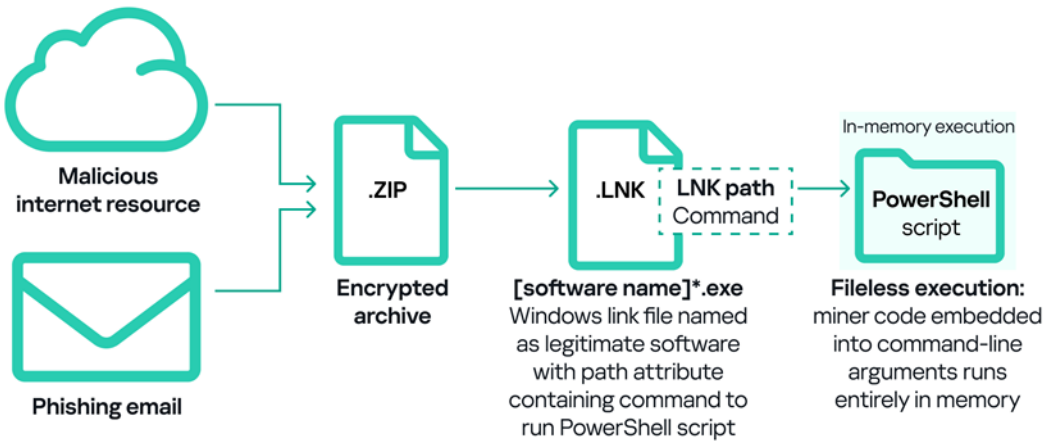


Miners in the form of executable files for Windows

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.

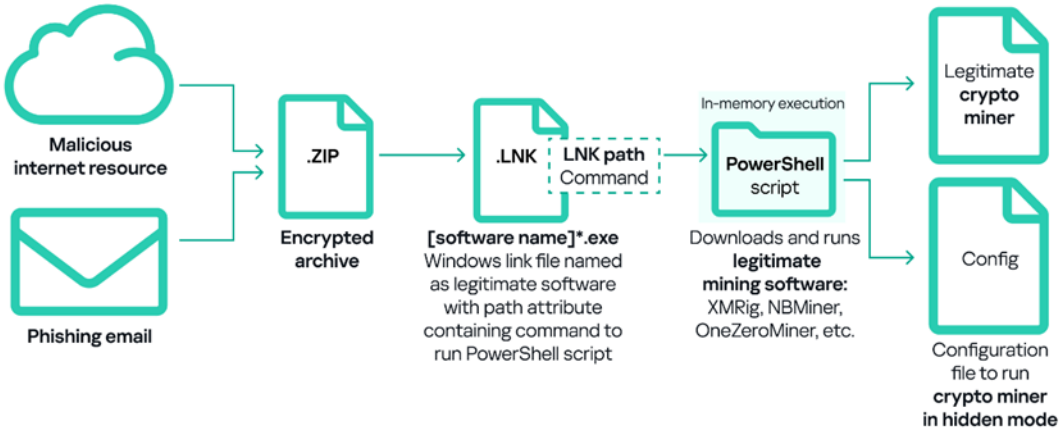
A significant portion of the Windows miners found on ICS computers consisted of archives with names that mimicked legitimate software. These archives did not contain actual software, but did include a Windows LNK file, commonly known as a shortcut. However, the target (or path) that the LNK file points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



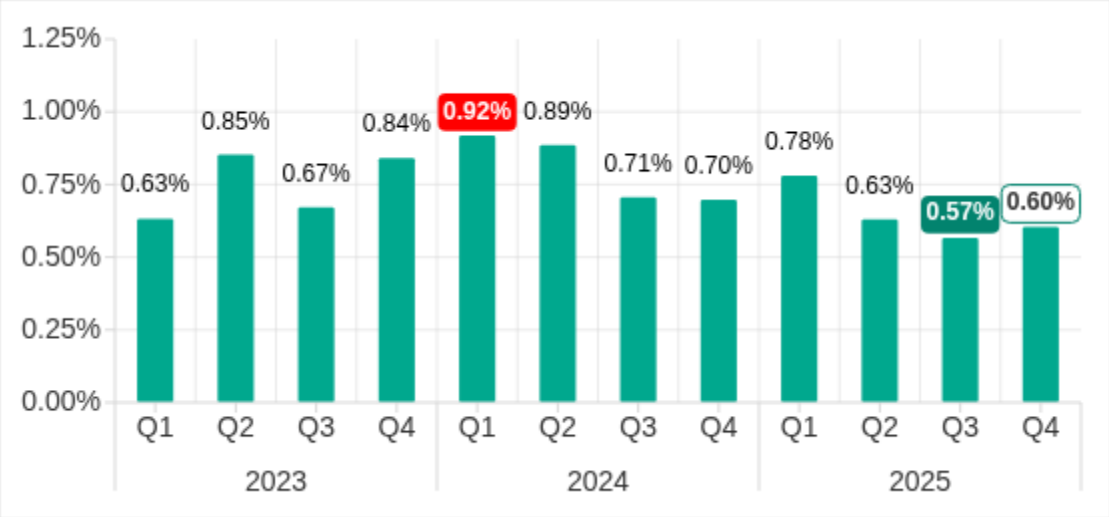
Another common method of deploying miners on ICS computers involves using legitimate cryptocurrency mining software such as XMRig, NBMiner, OneZeroMiner, and others. While these miners are not inherently malicious, they are classified as RiskTools by security systems. Attackers exploit these miners by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

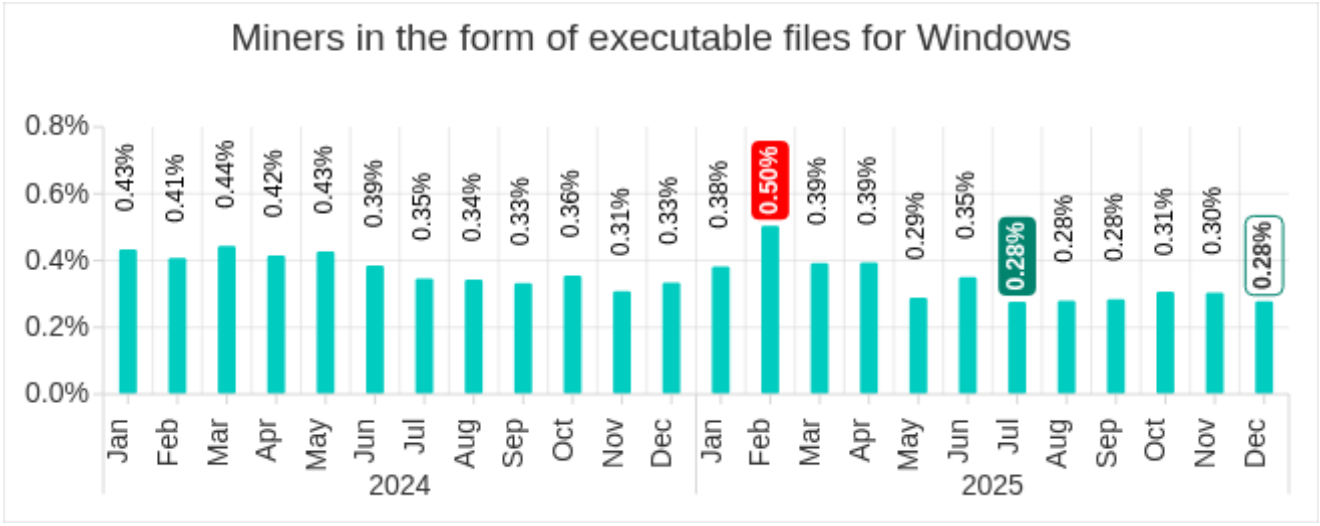


In Q4 2025, the percentage of ICS computers on which miners in the form of executable files for Windows were blocked increased to 0.60%.

Percentage of ICS computers on which miners in the form of executable files for Windows were blocked, Q1 2023–Q4 2025



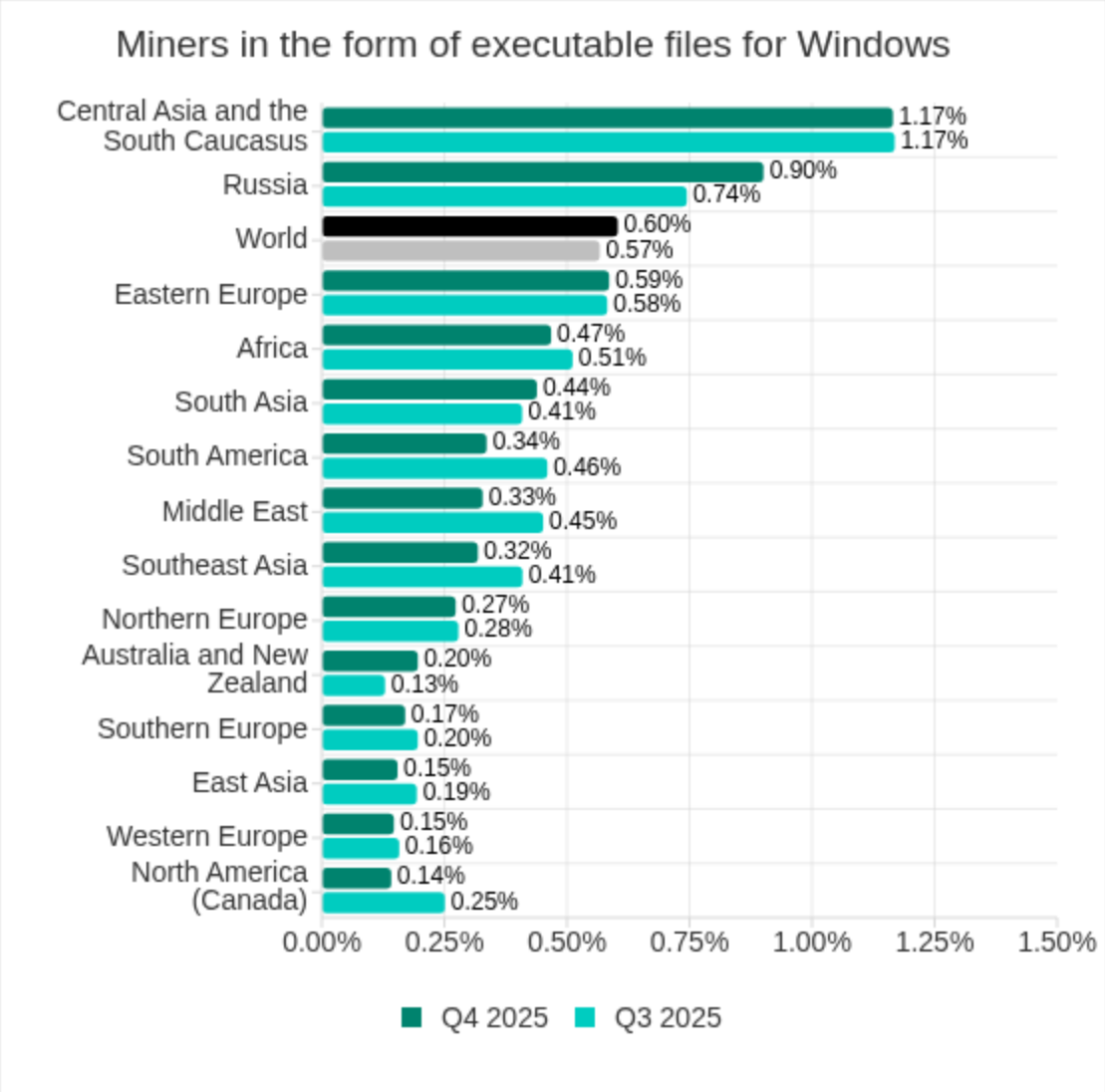
The highest monthly value in 2025 was in February, while the lowest values were in July, August, September, and December.



Percentage of ICS computers on which miners in the form of executable files for Windows were blocked, January 2024—December 2025

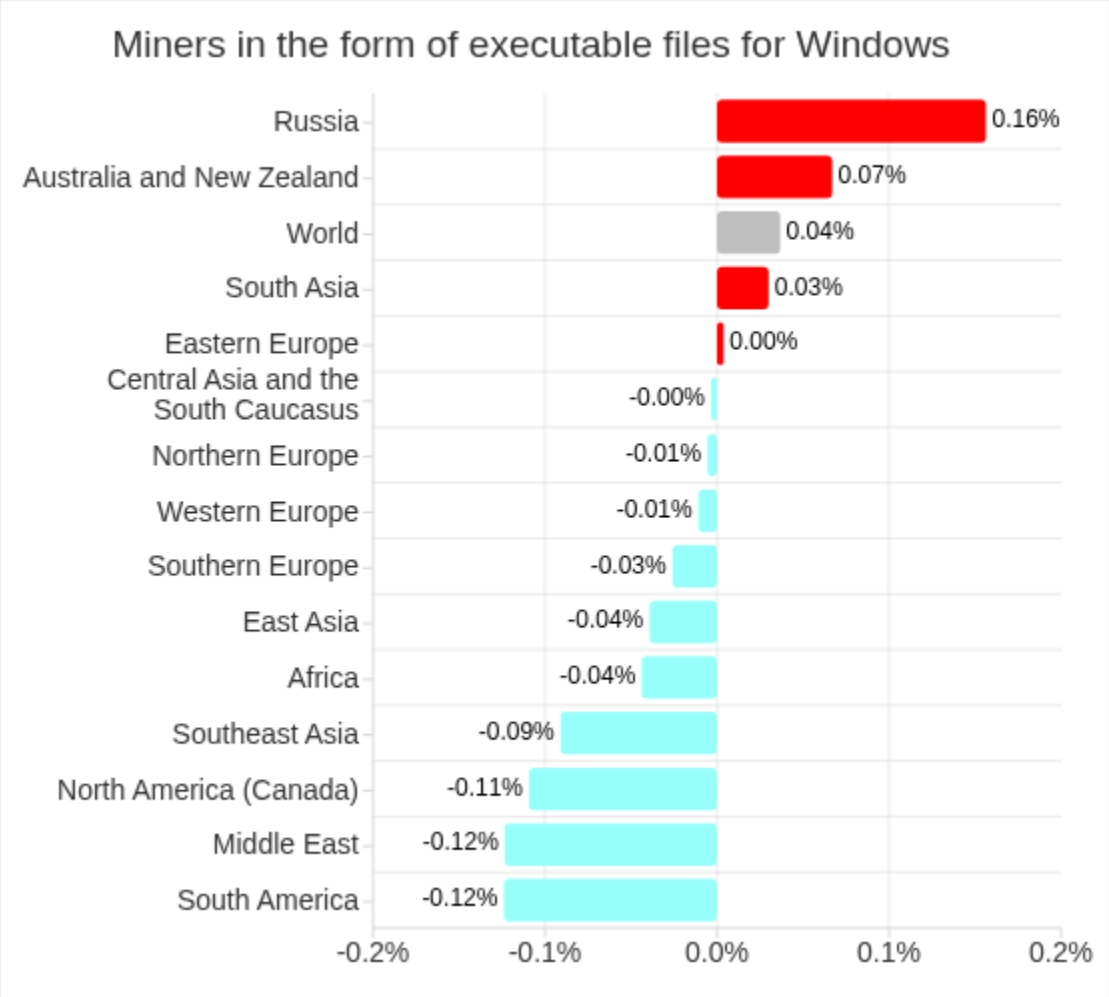
Regionally, the percentage of ICS computers on which miners in the form of executable files for Windows were blocked ranged from 0.14% in North America (Canada) to 1.17% in Central Asia and the South Caucasus. The top three regions for this indicator were Central Asia and the South Caucasus, Russia, and Eastern Europe.

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



In Q4 2025, the percentage of ICS computers on which miners in the form of executable files for Windows were blocked increased in four regions: Russia, Australia and New Zealand, South Asia, and Eastern Europe. Russia saw the biggest increase.

Changes in percentage of ICS computers on which miners in the form of executable files for Windows were blocked, Q4 2025

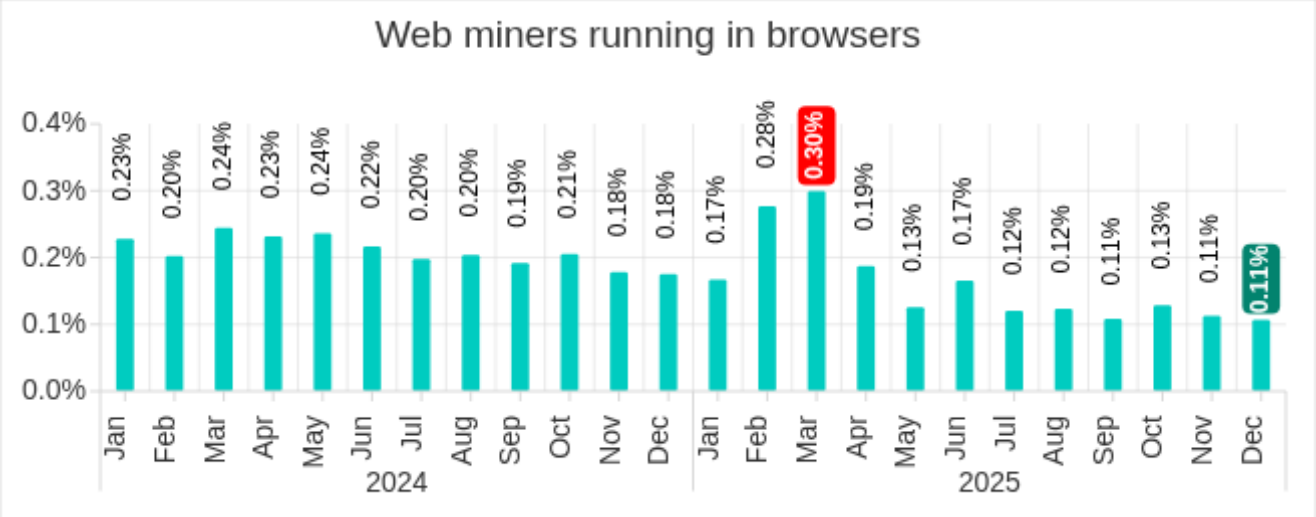


Web miners

In Q4 2025, the percentage of ICS computers on which web miners were blocked decreased to 0.24%. This is the lowest level observed thus far in the period under review.

Percentage of ICS computers on which web miners were blocked, Q1 2023–Q4 2025

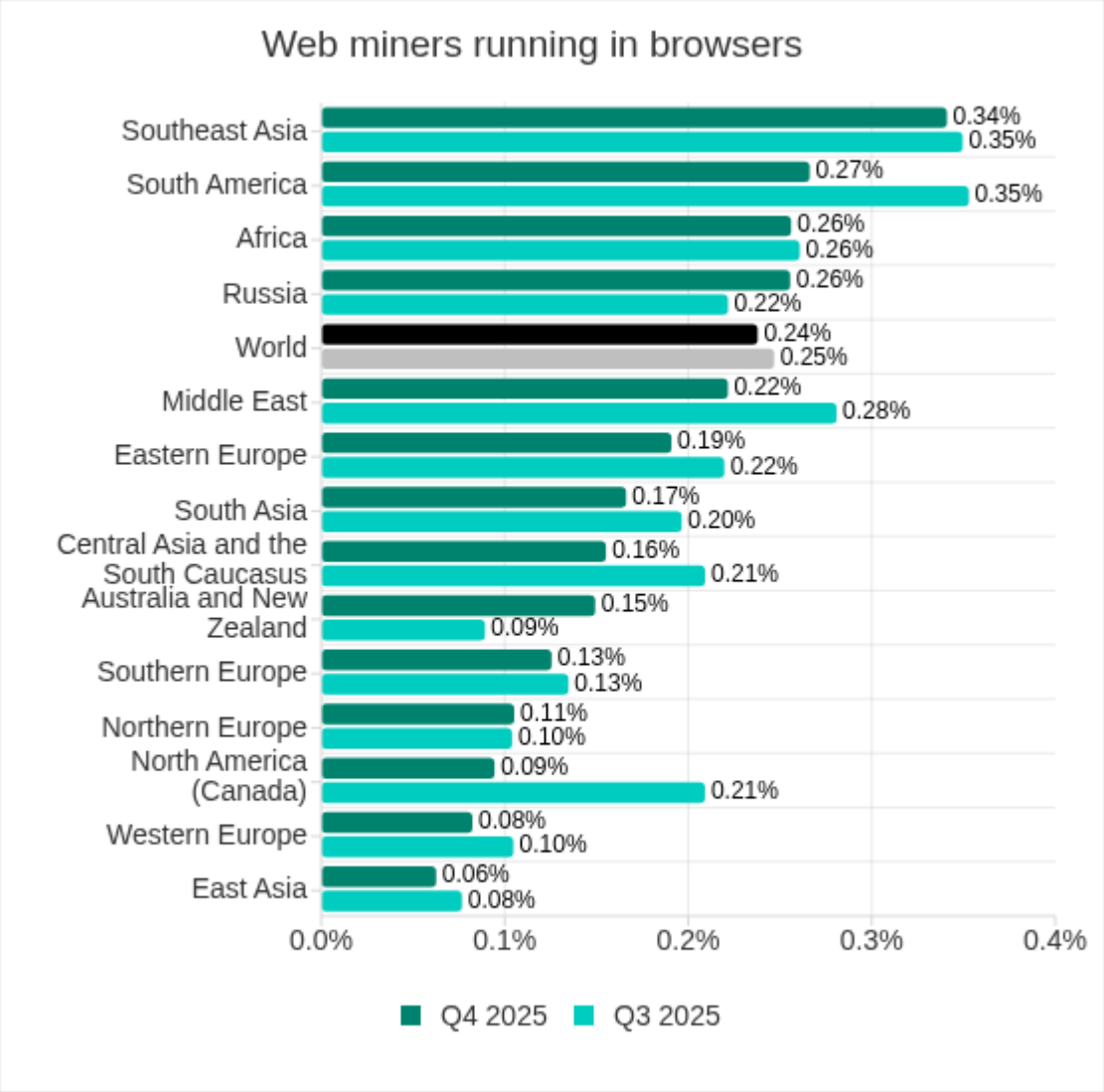
During this period, the highest monthly level was in March 2025. The lowest monthly levels were in September and December of 2025.



Percentage of ICS computers on which web miners were blocked, January 2024—December 2025

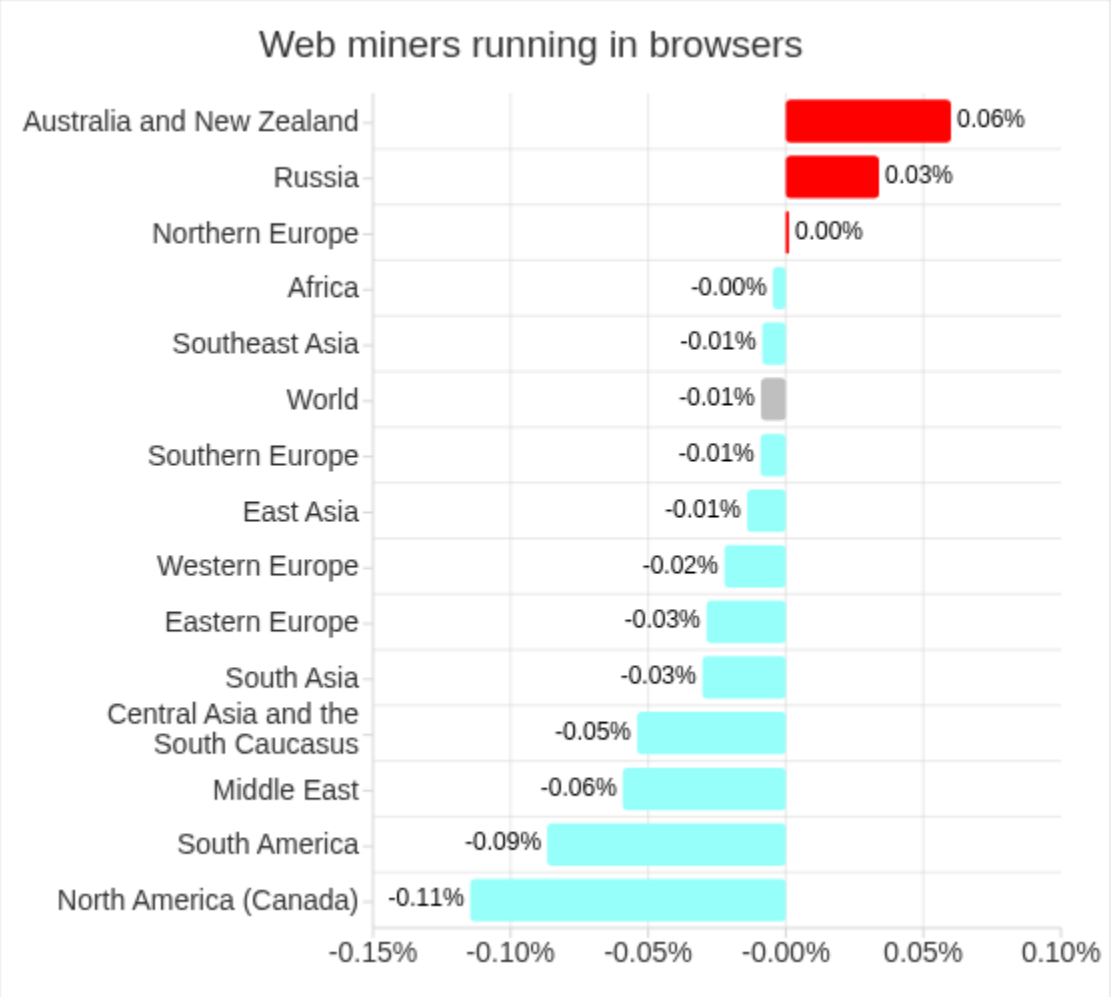
Regionally, the percentage of ICS computers on which web miners were blocked ranged from 0.06% in East Asia to 0.34% in Southeast Asia. The top three regions for this indicator were Southeast Asia, South America, and Africa.

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



In Q4 2025, the percentage of ICS computers on which web miners were blocked increased in three regions: Australia and New Zealand (up 1.67 times), Russia, and Northern Europe. The most notable increase in Australia was in the building automation industry, which increased almost threefold, from 0.09% to 0.26%.

Changes in percentage of ICS computers on which web miners were blocked, Q4 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.

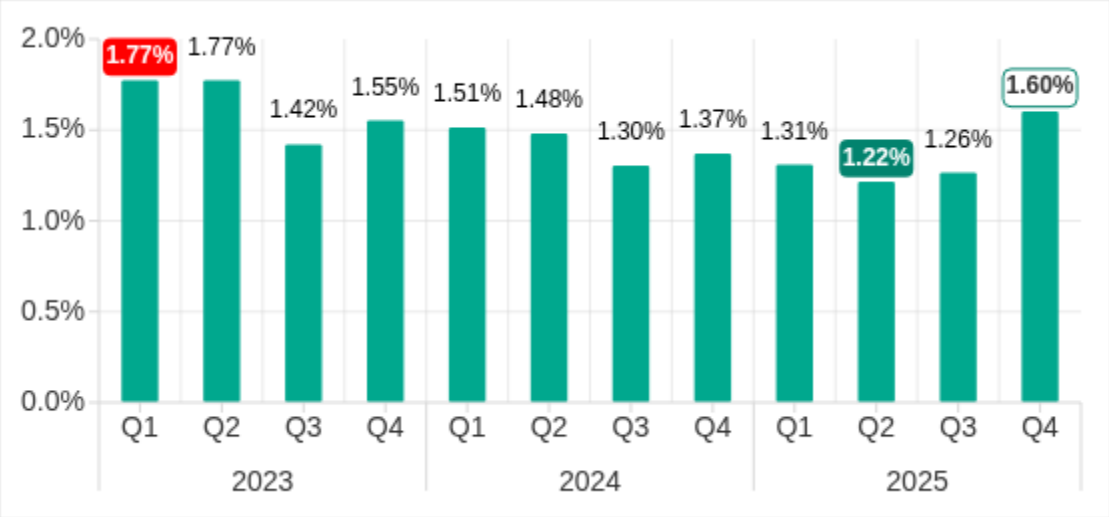
Alongside this, a lot of those still spreading are legacy viruses and worms whose command and control servers have been shut down. However, these types of malware can compromise infected systems by opening network ports or changing configurations, cause software failures, denial of service, and so on.

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.

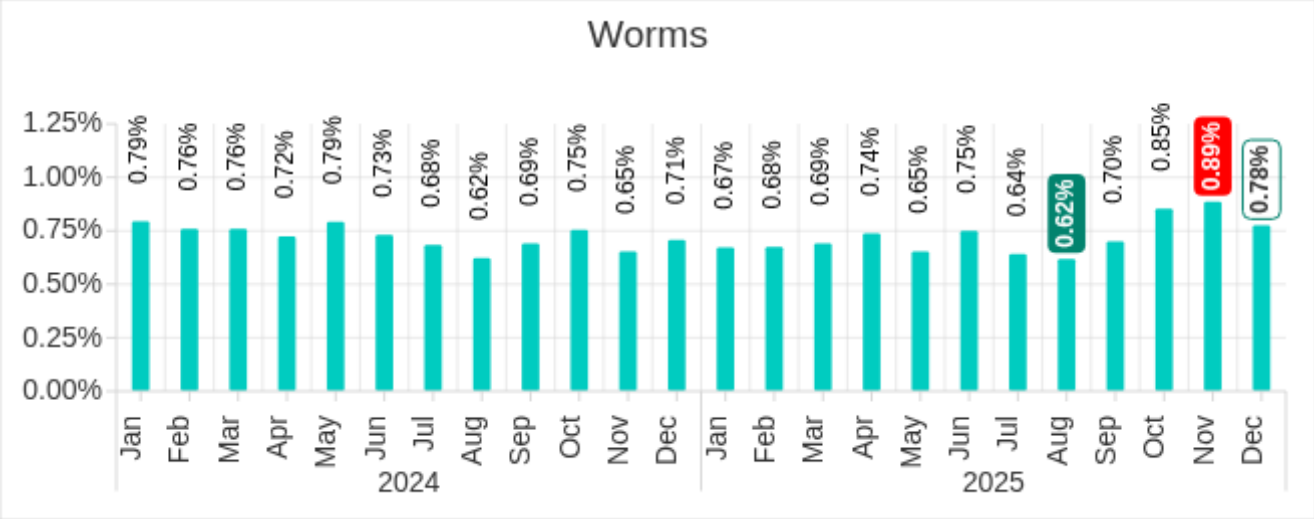
Worms

In Q4 2025, the percentage of ICS computers on which worms were blocked increased 1.6 times to 1.60%. As mentioned above, this increase is related to a global phishing attack that spread the Backdoor.MSIL.XWorm backdoor worm across all regions of the world.

Percentage of ICS computers on which worms were blocked, Q1 2023–Q4 2025



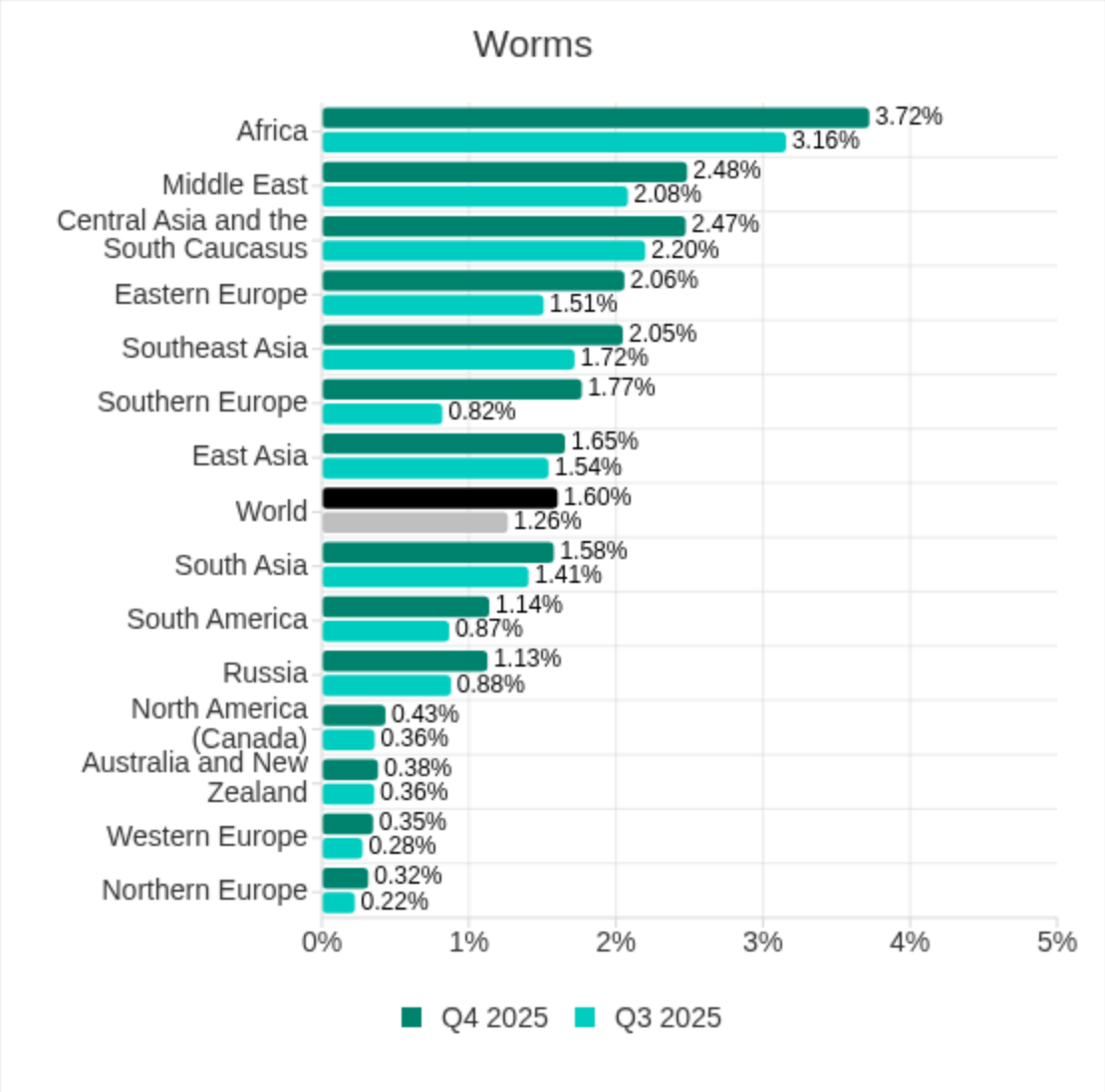
The highest monthly levels in 2025 were in the fourth quarter. During two waves of phishing attacks in October and November, the indicator increased. In December, the percentage of ICS computers on which worms were blocked decreased, but the figure still exceeded those for the other months of 2025.



Percentage of ICS computers on which worms were blocked, January 2024—December 2025

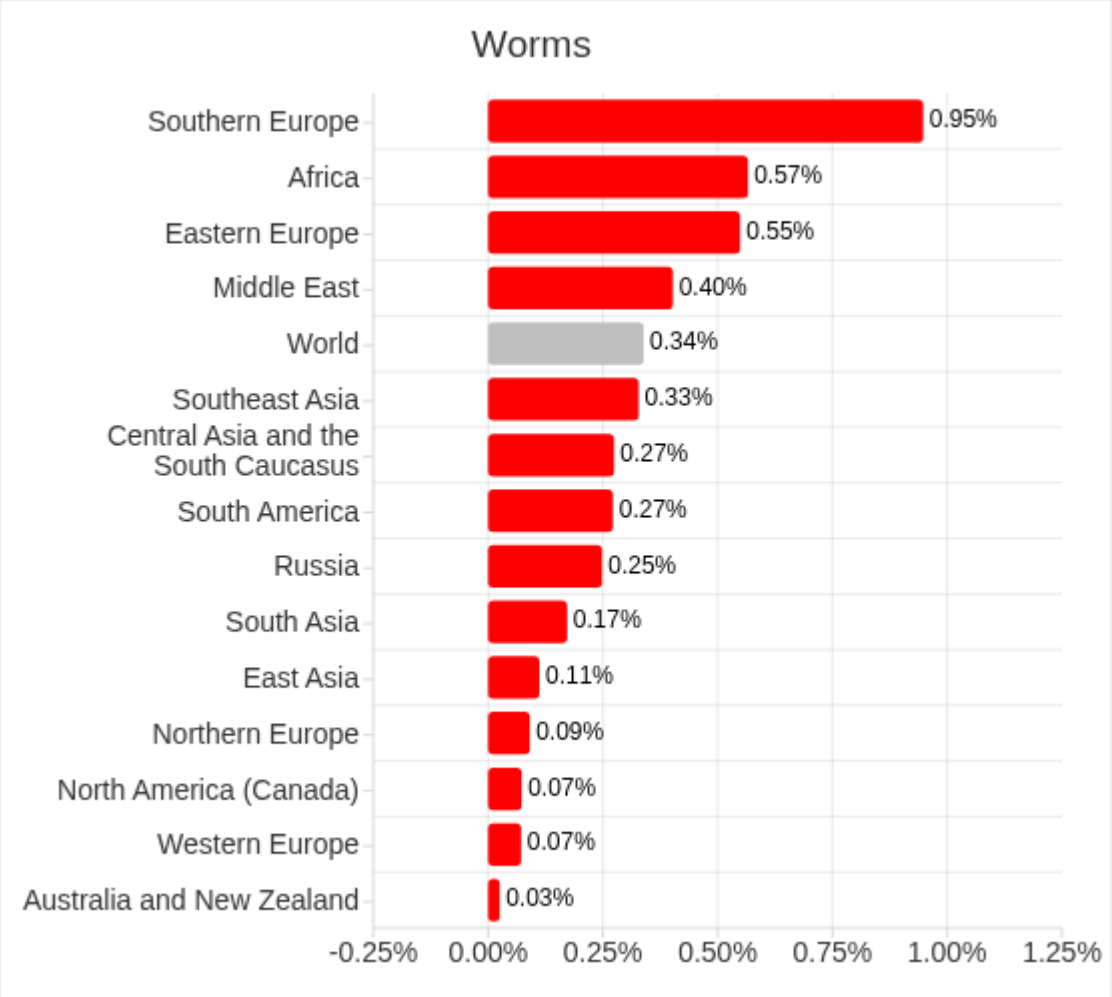
Regionally, the percentage of ICS computers on which worms were blocked ranged from 0.32% in Northern Europe to 3.72% in Africa. The top three regions for this indicator were Africa, the Middle East, and Central Asia and the South Caucasus.

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



In Q4 2025, the percentage of ICS computers on which worms were blocked increased in all regions. The biggest increase (up 2.16 times) was in Southern Europe. The malware was primary distributed through email clients, and Southern Europe led the way in terms of the percentage of ICS computers on which threats from email clients were blocked. At the same time, in Africa, where USB storage media is still actively used, Backdoor.MSIL.XWorm was also blocked when removable devices were connected to ICS computers.

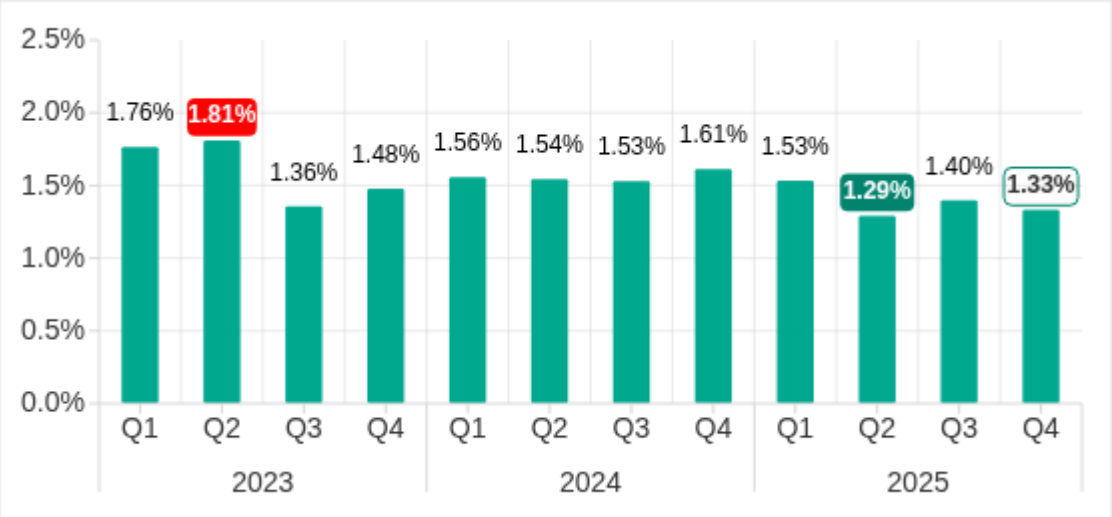
Changes in percentage of ICS computers on which worms were blocked, Q4 2025



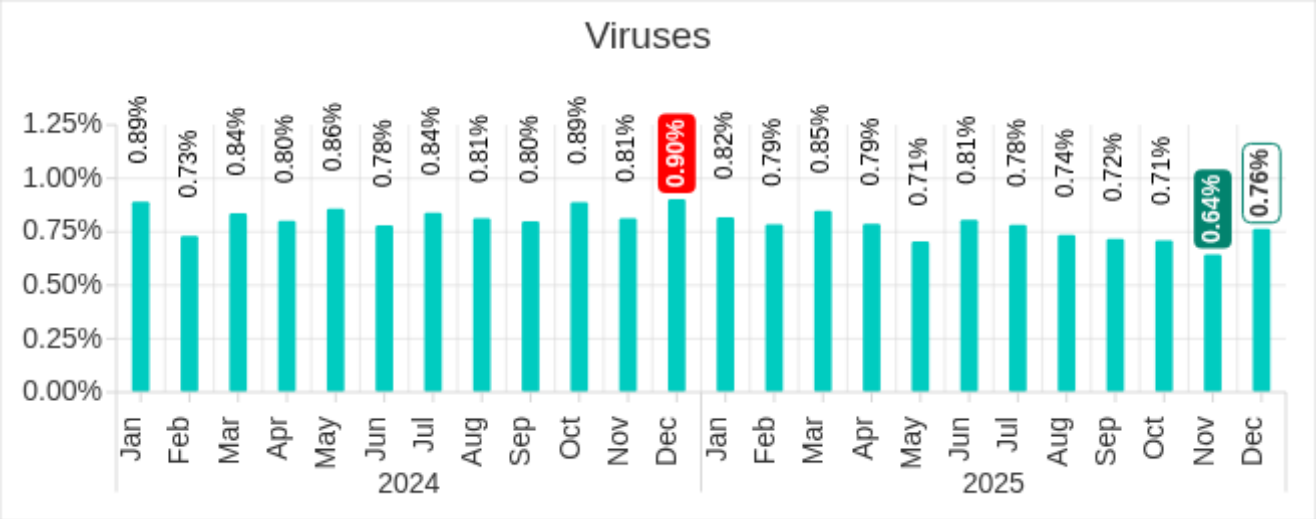
Viruses

In Q4 2025, the percentage of ICS computers on which viruses were blocked decreased to 1.33%.

Percentage of ICS computers on which viruses were blocked, Q1 2023–Q4 2025



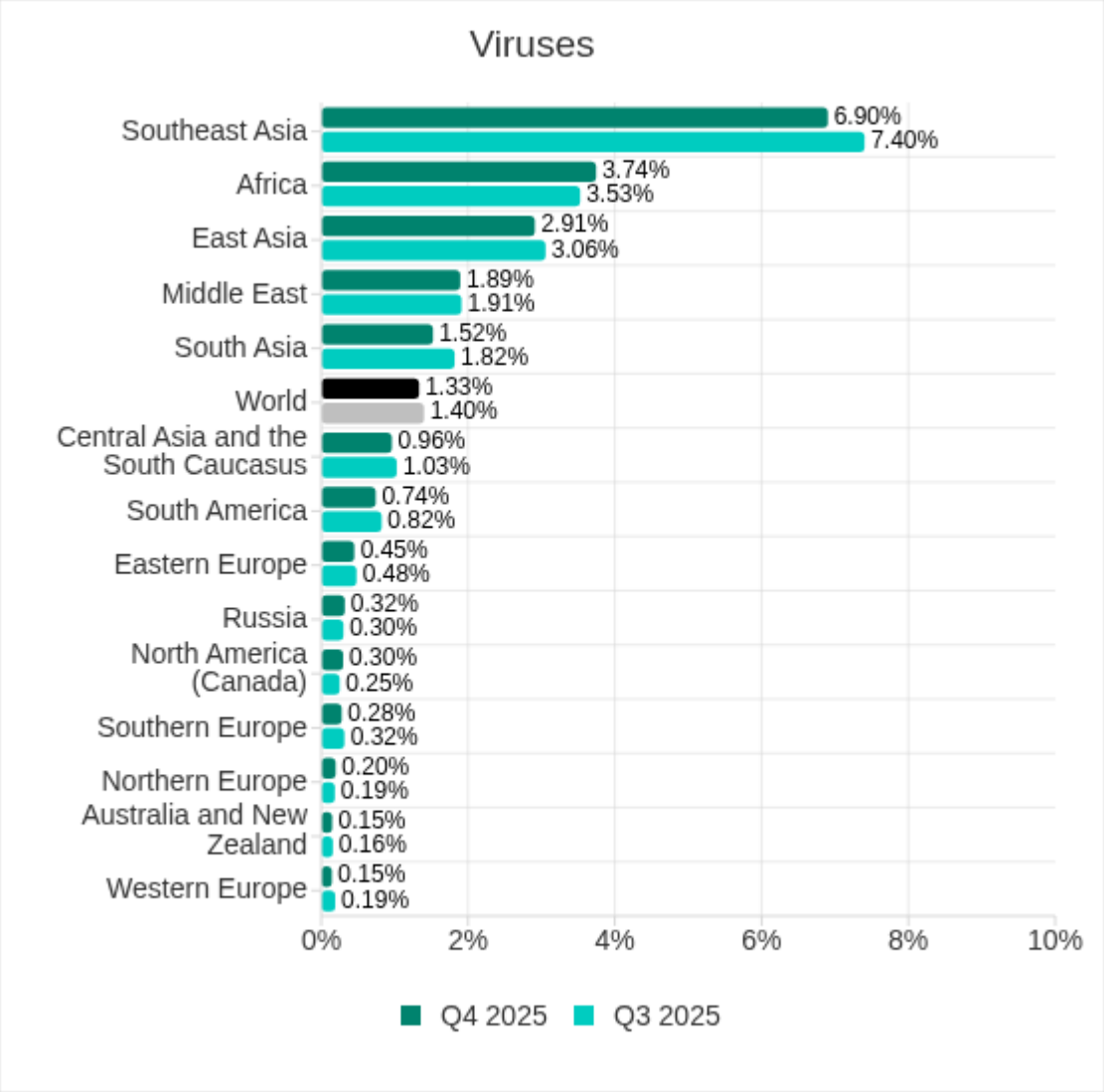
The highest monthly level in 2025 was in March. The lowest level was in November, but that was followed by an increase in December.



Percentage of ICS computers on which viruses were blocked, January 2024—December 2025

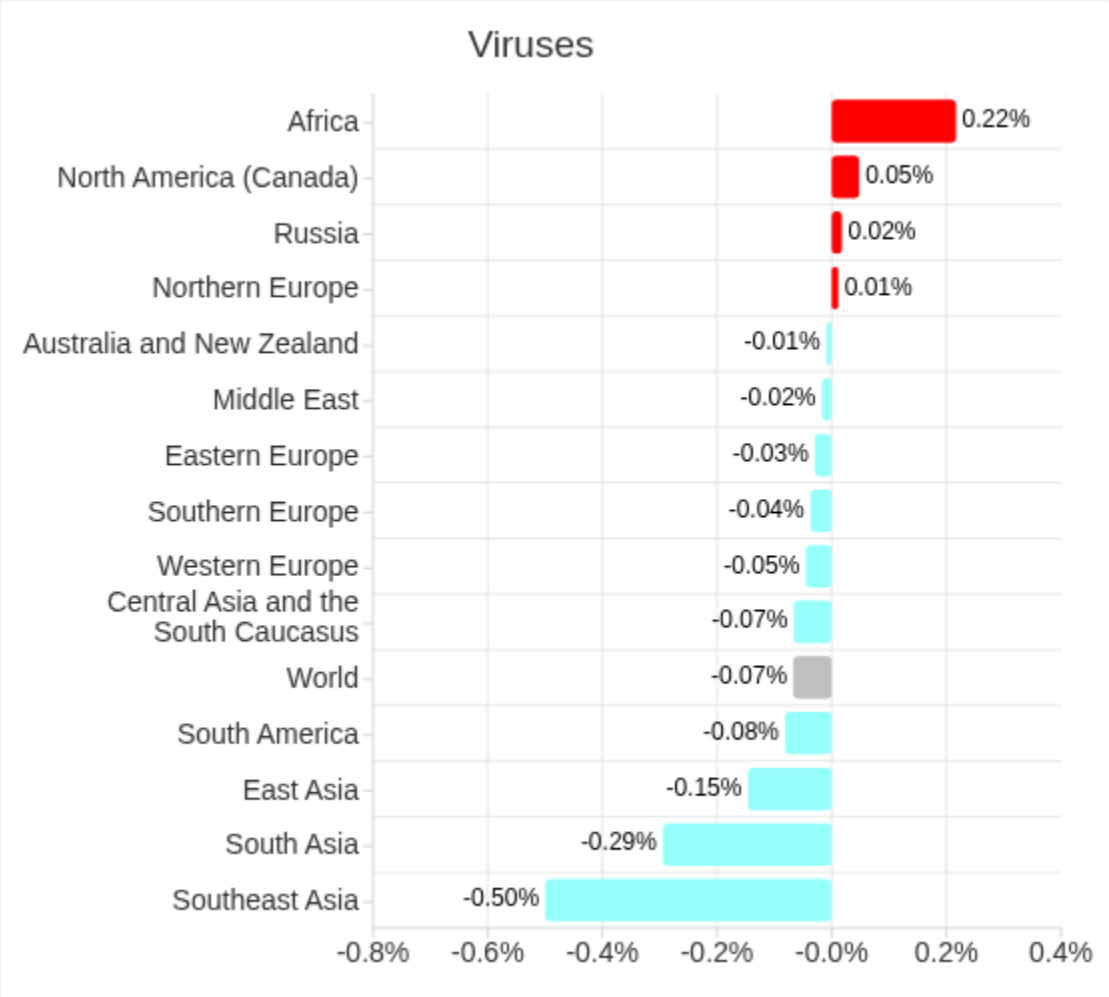
Regionally, the percentage of ICS computers on which viruses were blocked ranged from 0.15% in Western Europe to 6.90% in Southeast Asia. The top three regions for this indicator in Q4 2025 remained the same: Southeast Asia (by a wide margin), followed by Africa, and East Asia. These are the same regions that led the AutoCAD malware ranking.

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



In Q4 2025, the percentage of ICS computers on which viruses were blocked increased in four regions: Africa, North America (Canada), Russia, and Northern Europe. The indicator increased the most in Africa.

Changes in percentage of ICS computers on which viruses were blocked, Q4 2025



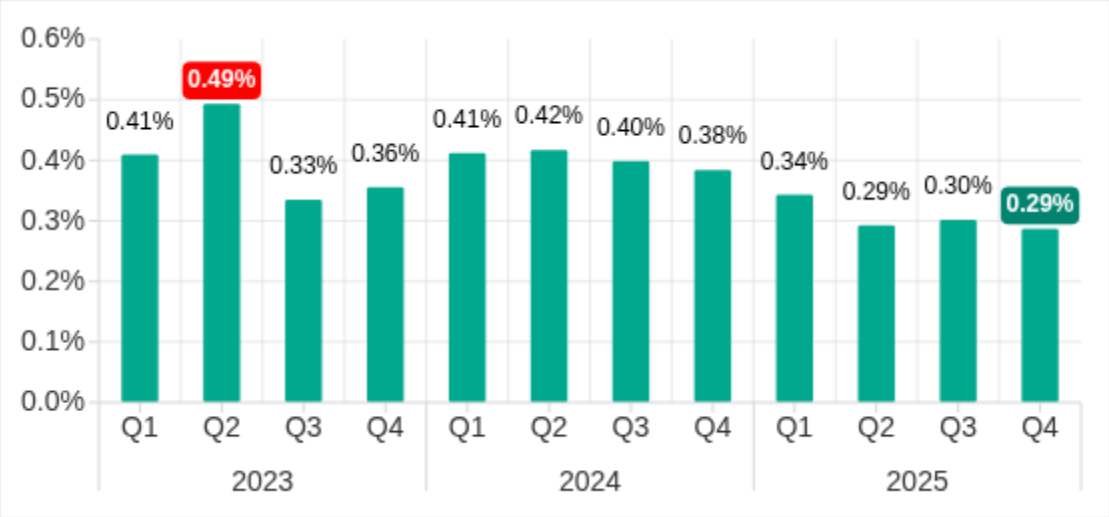
AutoCAD malware

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

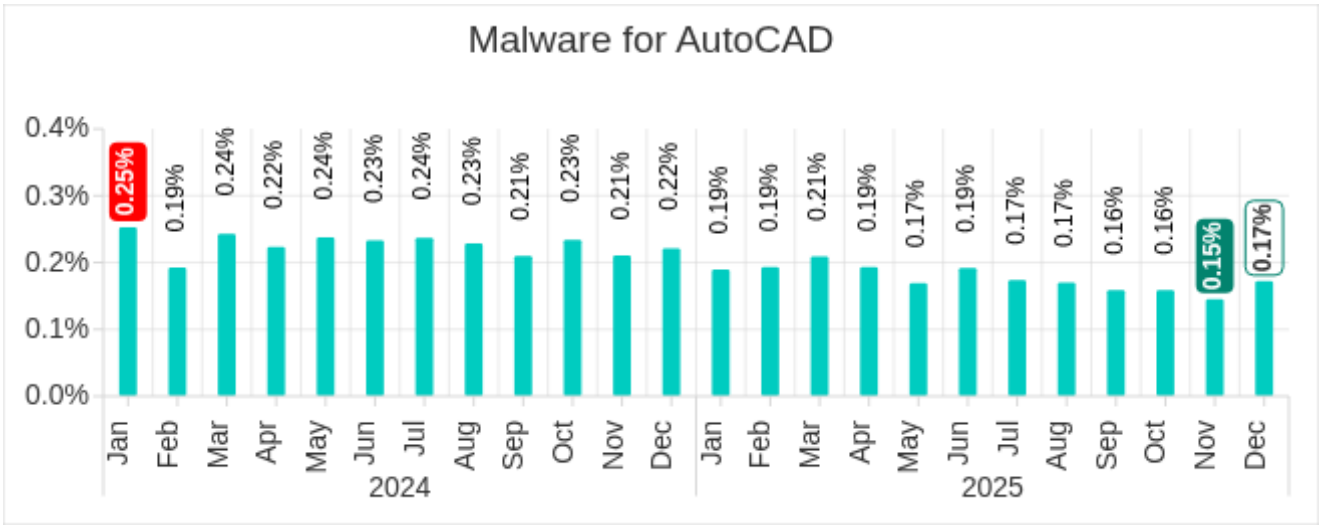
AutoCAD malware is typically a low-level threat, coming last in the malware category rankings in terms of the percentage of ICS computers on which it was blocked.

After an increase in the previous quarter, the percentage of ICS computers on which AutoCAD malware was blocked decreased to 0.29% in Q4 2025.

Percentage of ICS computers on which AutoCAD malware was blocked, Q1 2023–Q4 2025



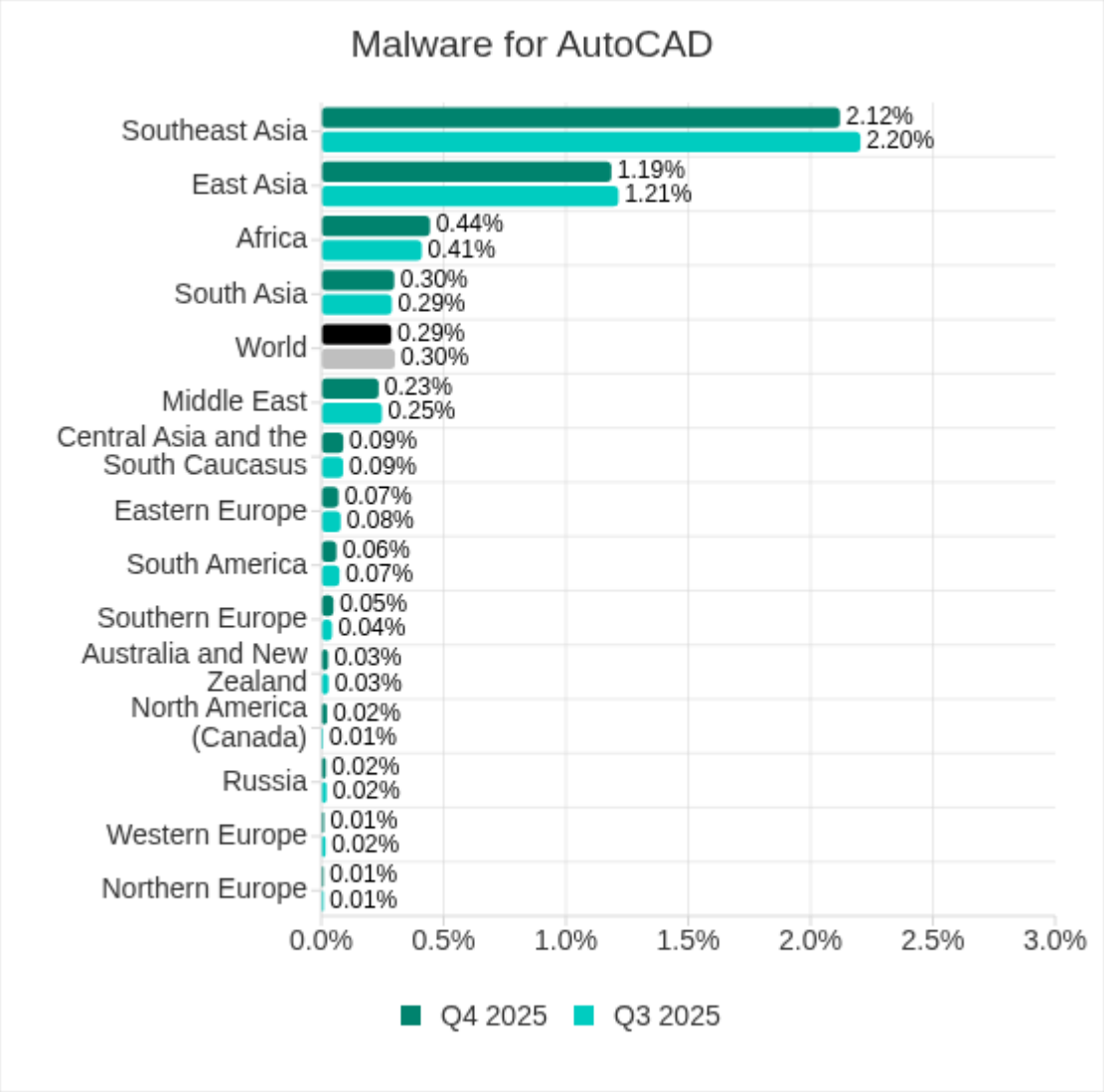
As in the case of viruses, the highest monthly figure in 2025 was in March, while the lowest level was in November.



Percentage of ICS computers on which AutoCAD malware was blocked, January 2024—December 2025

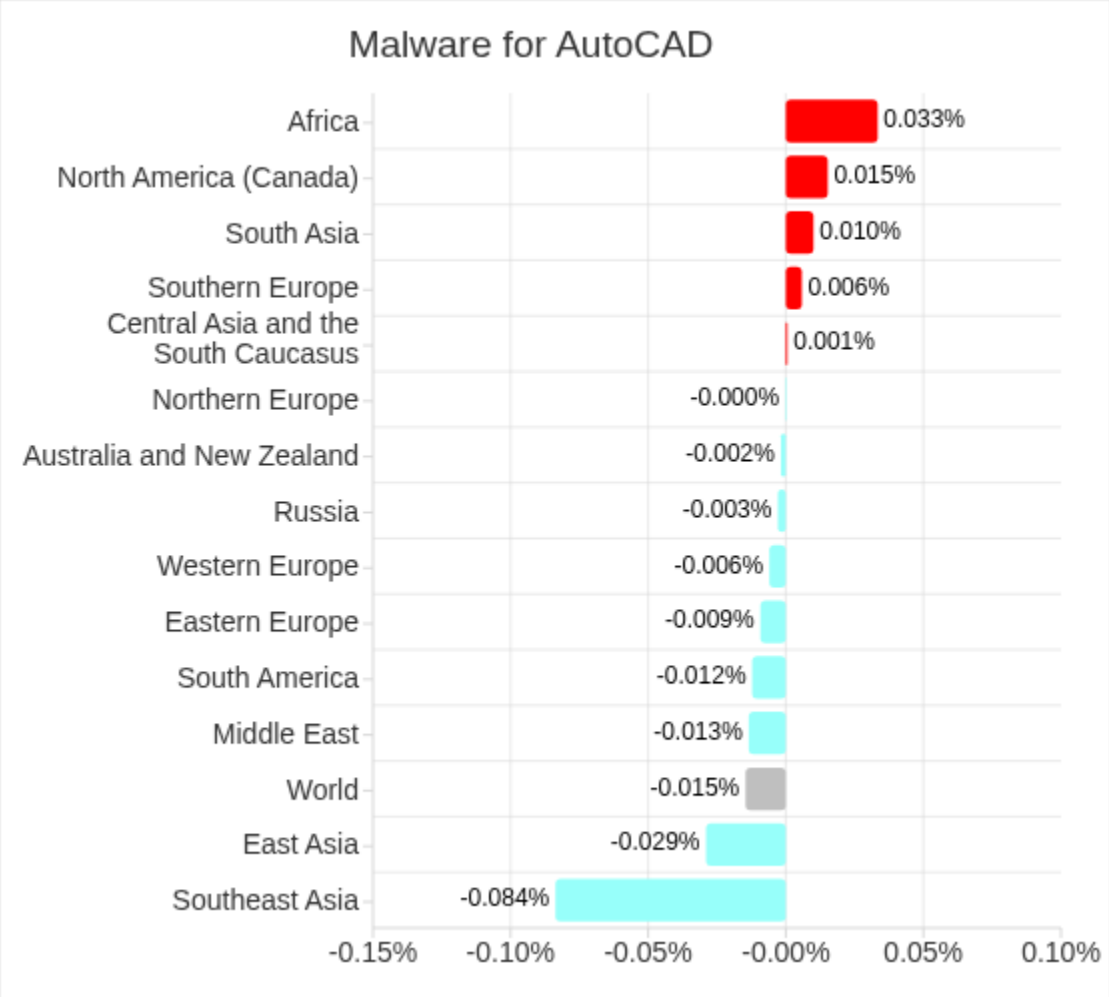
Regionally, the percentage of ICS computers on which AutoCAD malware was blocked ranged from 0.01% in Northern Europe to 2.12% in Southeast Asia. The same regions that led the virus ranking were also the leaders in terms of the percentage of ICS computers on which AutoCAD malware was blocked: Southeast Asia, East Asia (both by a wide margin), and Africa.

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



In Q4 2025, the percentage increased in five regions, with the most notable increase occurring in Africa.

Changes in percentage of ICS computers on which AutoCAD malware was blocked, Q4 2025



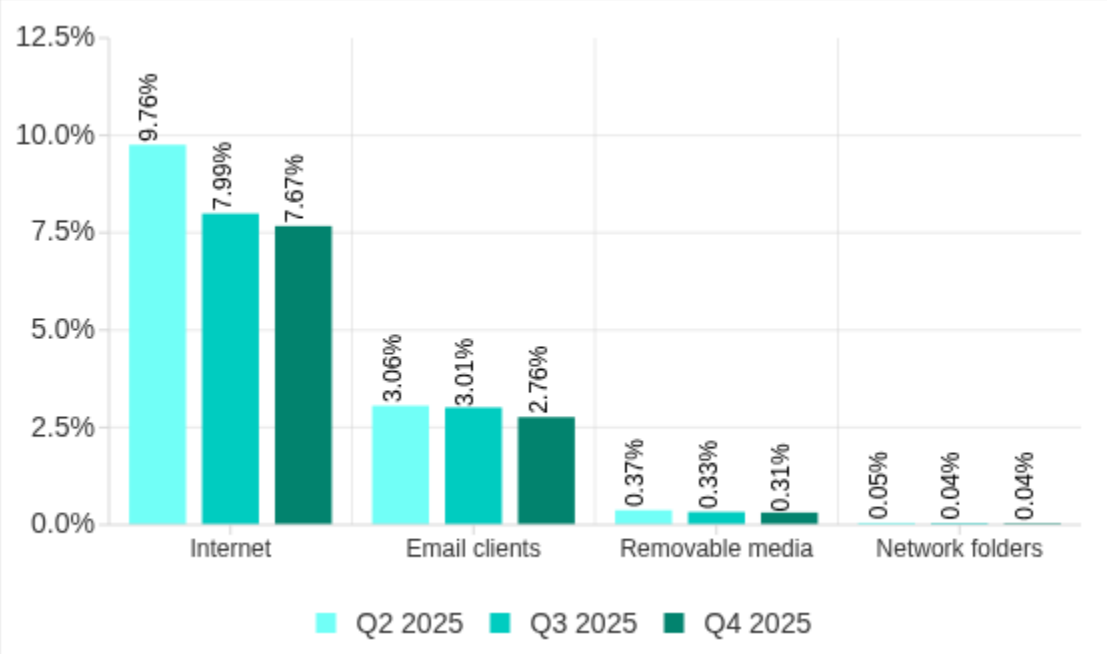
Main threat sources

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 Q4 2025, the percentage of ICS computers on which malicious objects from various sources were blocked decreased. All sources except email clients saw their lowest levels in three years.

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

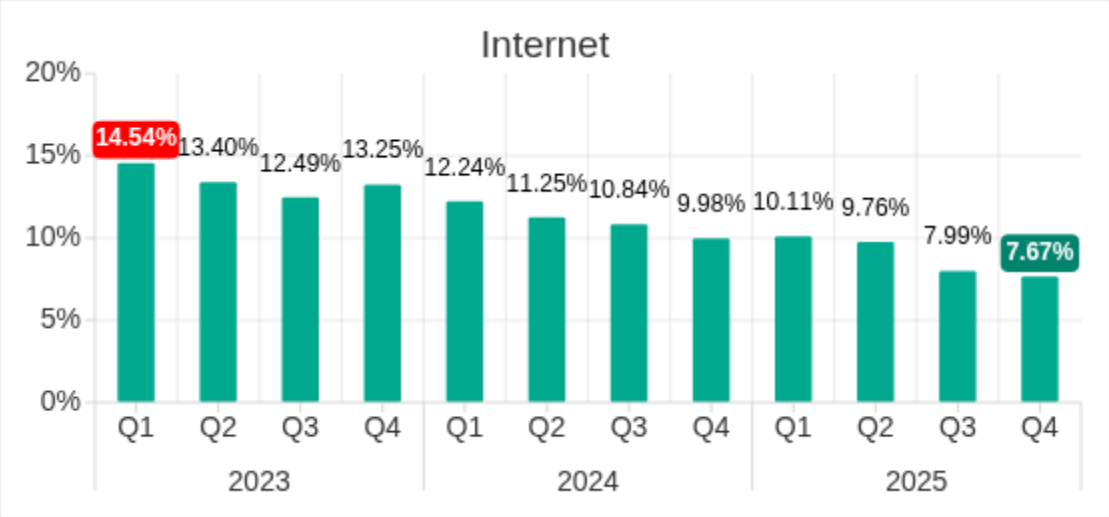


Internet

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.

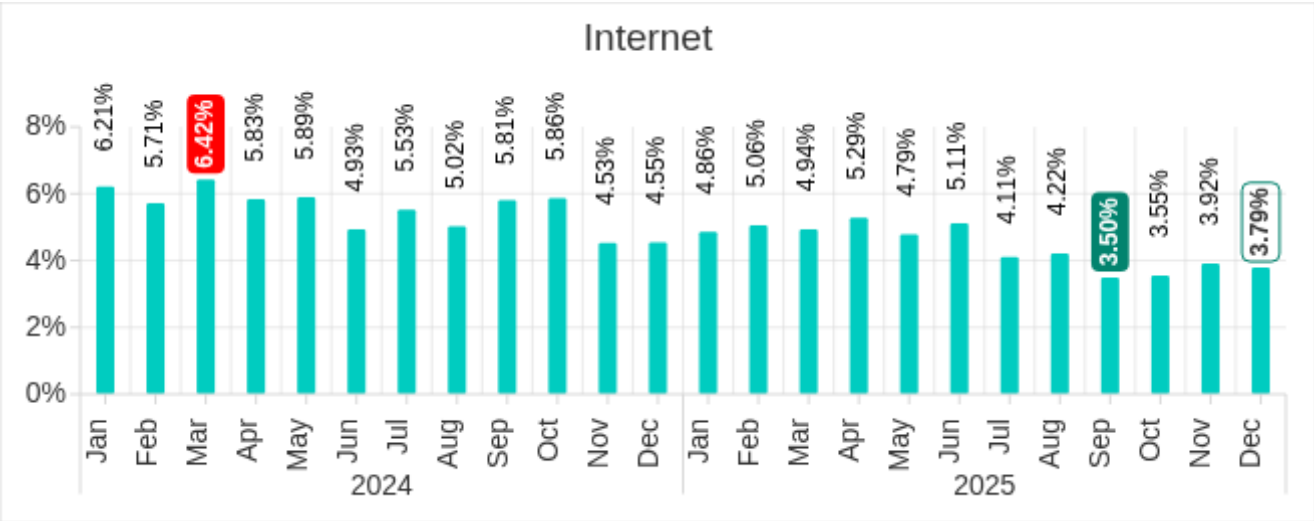
In Q4 2025, the percentage of ICS computers on which threats from the internet were blocked decreased to 7.67% and reached its lowest level since the beginning of 2023.

Percentage of ICS computers on which threats from the internet were blocked, Q1 2023—Q4 2025



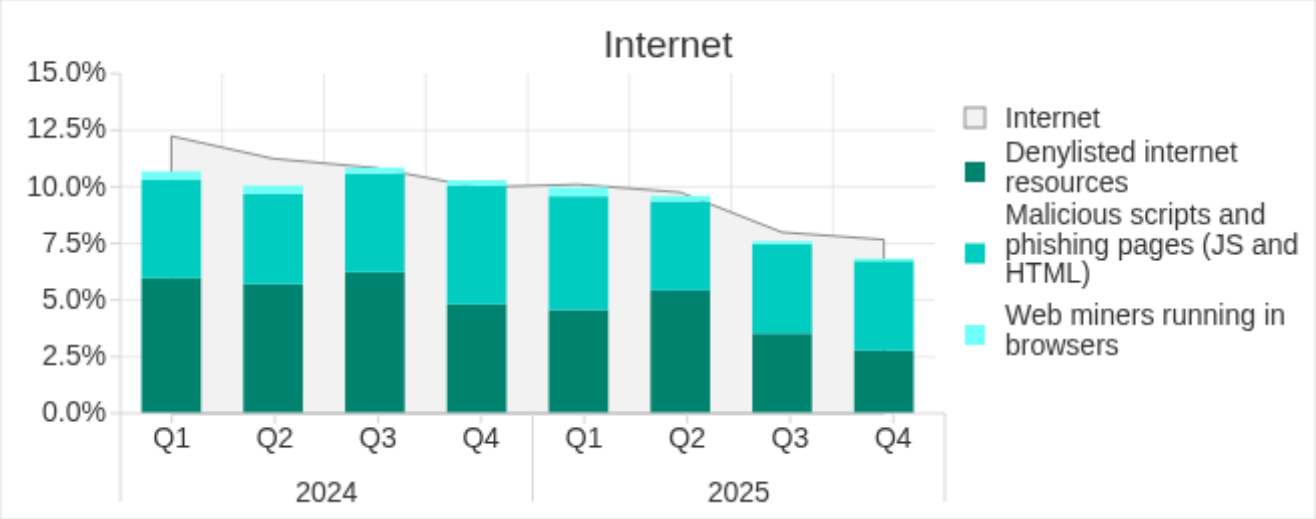
The highest monthly level in 2025 was in April, while the lowest level was in September.

In Q4 2025, the highest percentage of ICS computers on which threats from the internet were blocked occurred in November.



Percentage of ICS computers on which threats from the internet were blocked, January 2024—December 2025

The main categories of threats from the internet* blocked on ICS computers in Q4 2025 are malicious scripts and phishing pages, and denylisted internet resources.

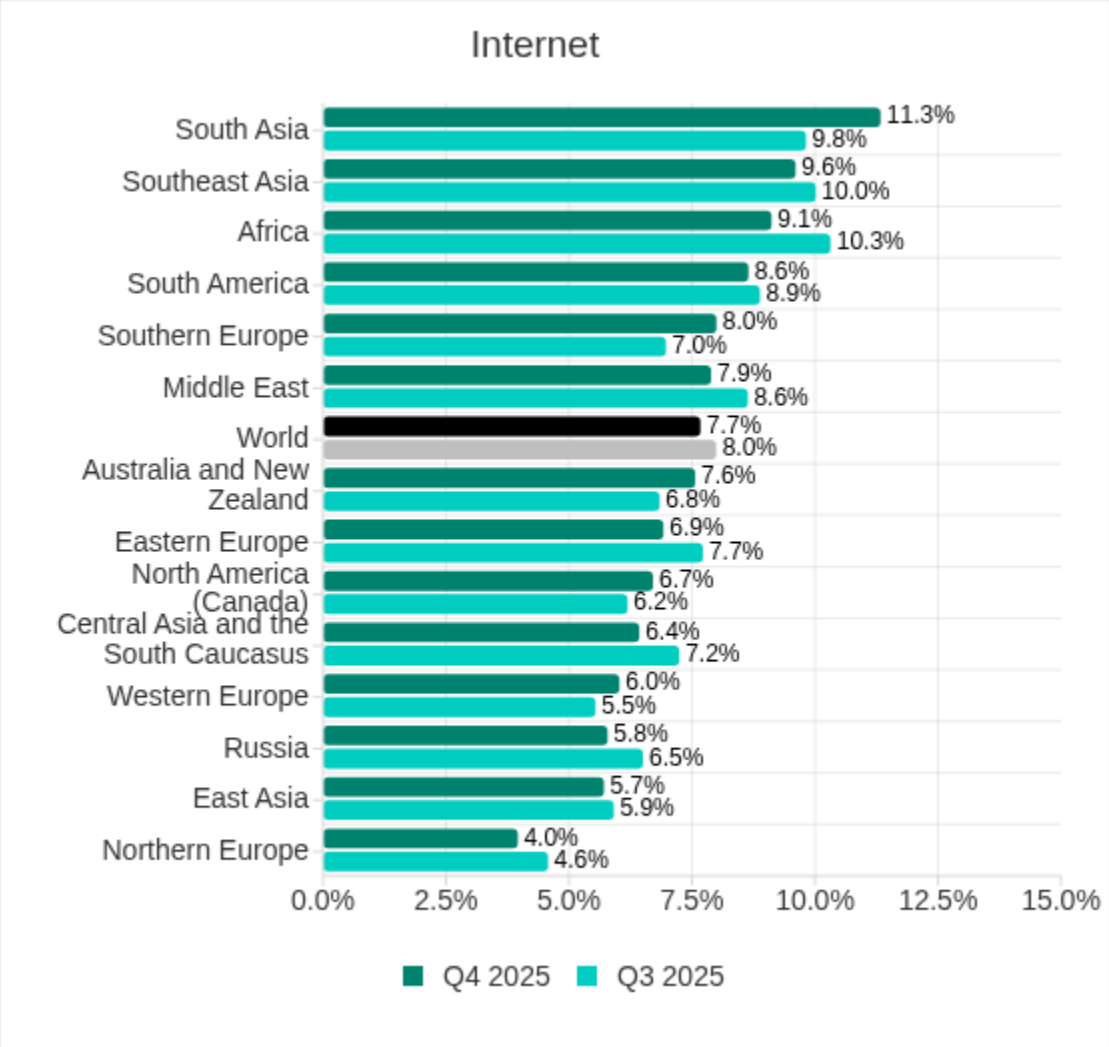


Percentage of ICS computers on which threats from the internet were blocked, Q1 2024—Q4 2025

*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.

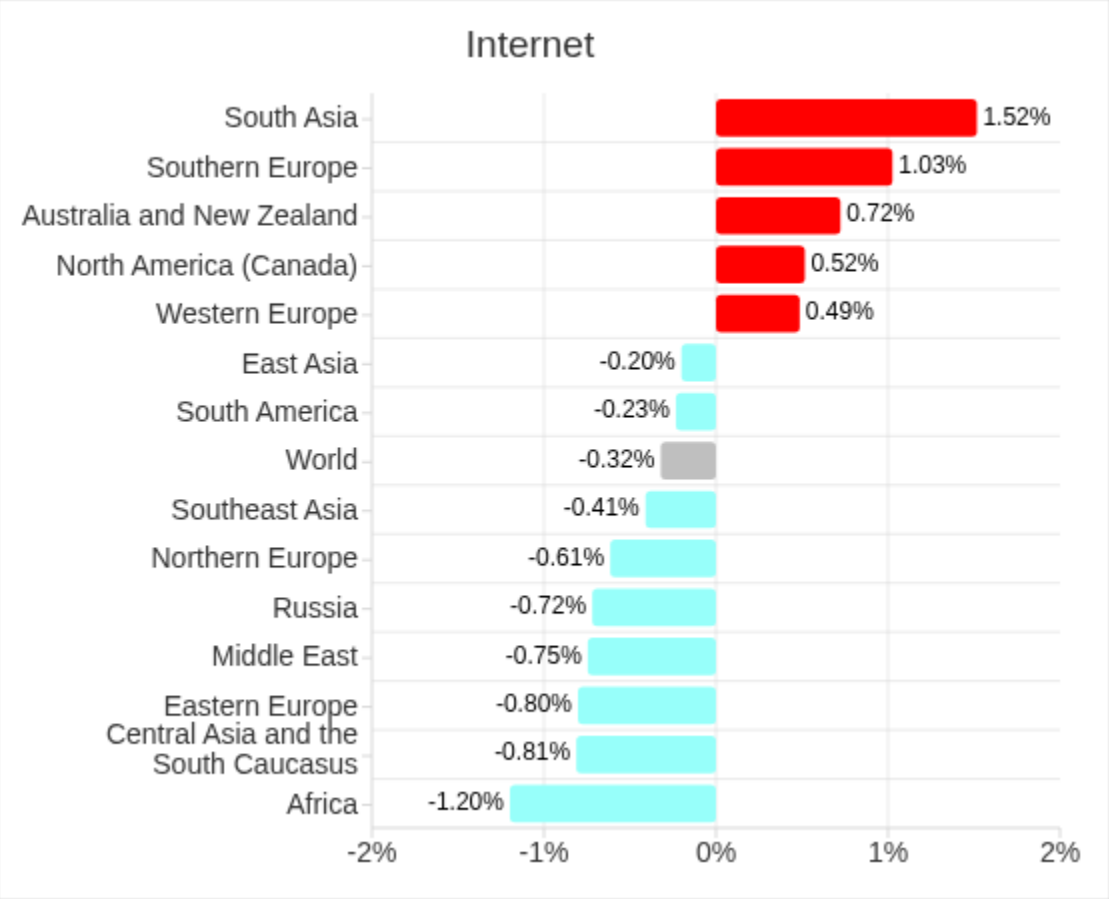
Regionally, the percentage of ICS computers on which threats from the internet were blocked ranged from 3.96% in Northern Europe to 11.33% in South Asia. The top three regions for this indicator remained the same: South Asia, Southeast Asia, and Africa. However, Africa and South Asia switched places, with Africa dropping to third place and South Asia rising to first.

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



In Q4 2025, the percentage increased in five regions, with the biggest increase occurring in South Asia.

Changes in percentage of ICS computers on which threats from the internet were blocked, Q4 2025

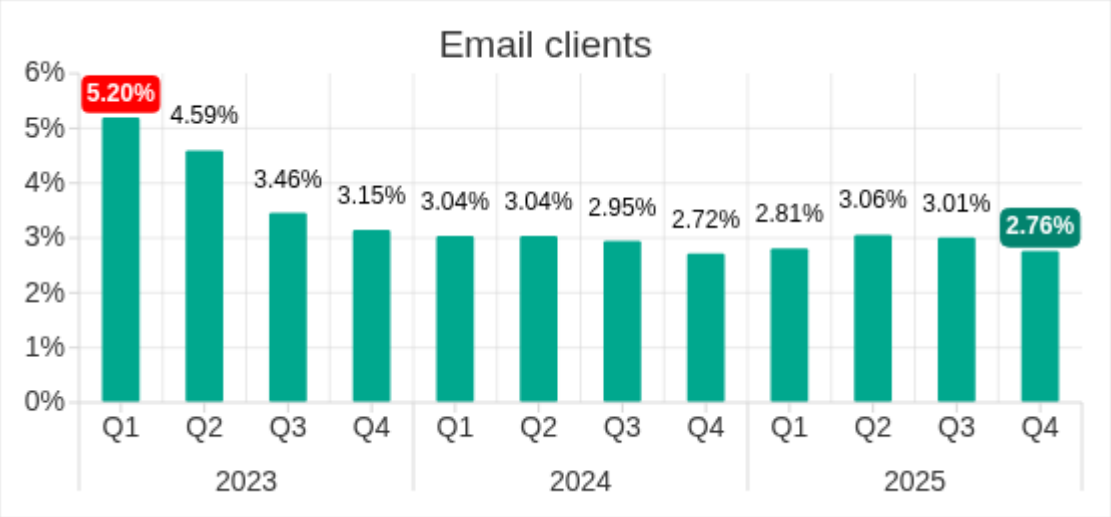


Email clients

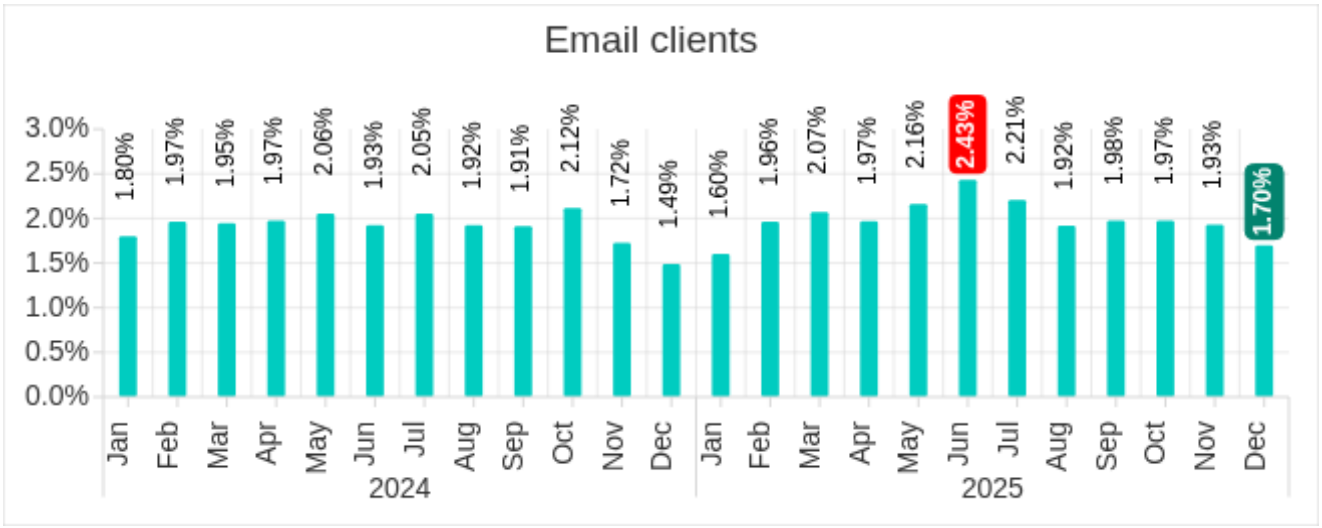
Some detected and blocked threats are delivered to protected computers by the mail delivery system and/or attempt to gain access through the email client application.

In Q4 2025, the percentage of ICS computers on which threats from email clients were blocked decreased to 2.76%. This is the second-highest value in three years.

Percentage of ICS computers on which threats from email clients were blocked, Q1 2023—Q4 2025



The highest monthly level in 2025 was in June. From July onward, the percentage of ICS computers on which threats from email clients were blocked each month decreased.



Percentage of ICS computers on which threats from email clients were blocked, January 2024—December 2025

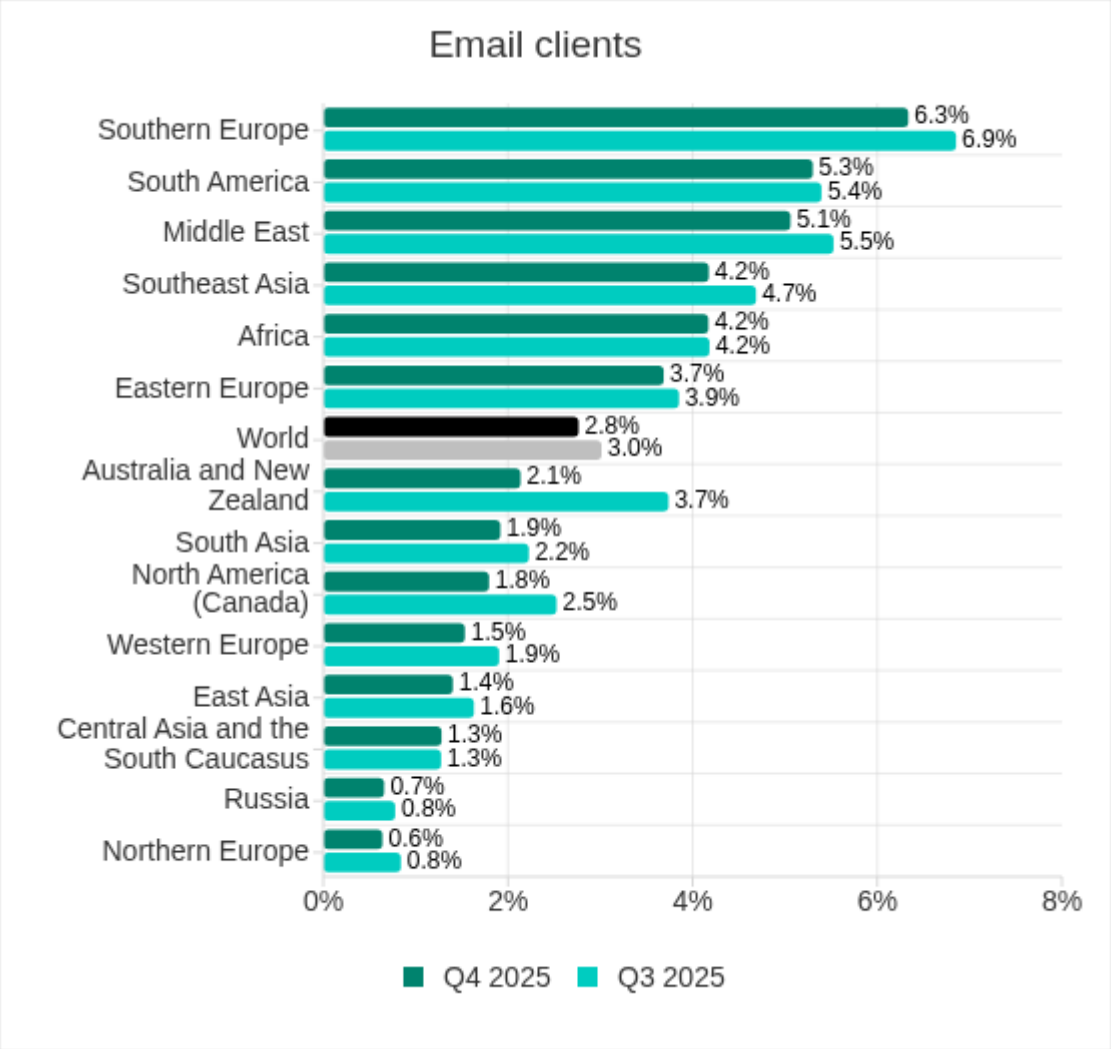
The main categories of threats from email clients blocked on ICS computers in Q4 2025 were malicious scripts and phishing pages, spyware, and malicious documents. The chart below also shows an increase in the percentage of ICS computers on which worms from email clients were blocked in Q4 2025.

Percentage of ICS computers on which threats from email clients were blocked, Q1 2024—Q4 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.

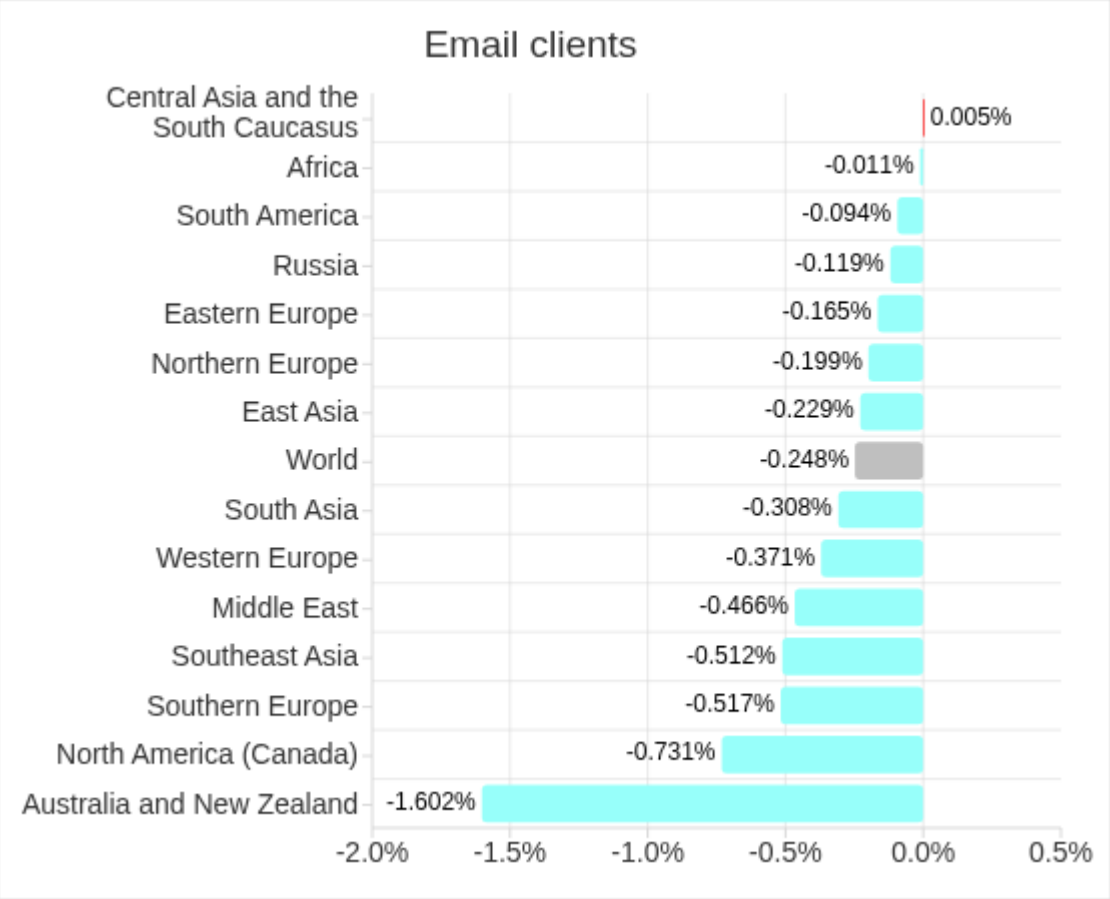
Regionally, the percentage of ICS computers on which threats from email clients were blocked ranged from 0.64% in Northern Europe to 6.34% in Southern Europe. The top three regions for this indicator were the same as in the previous quarter: Southern Europe, South America, and the Middle East.

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



In Q4 2025, the percentage of ICS computers on which threats from email clients were blocked decreased in almost all regions.

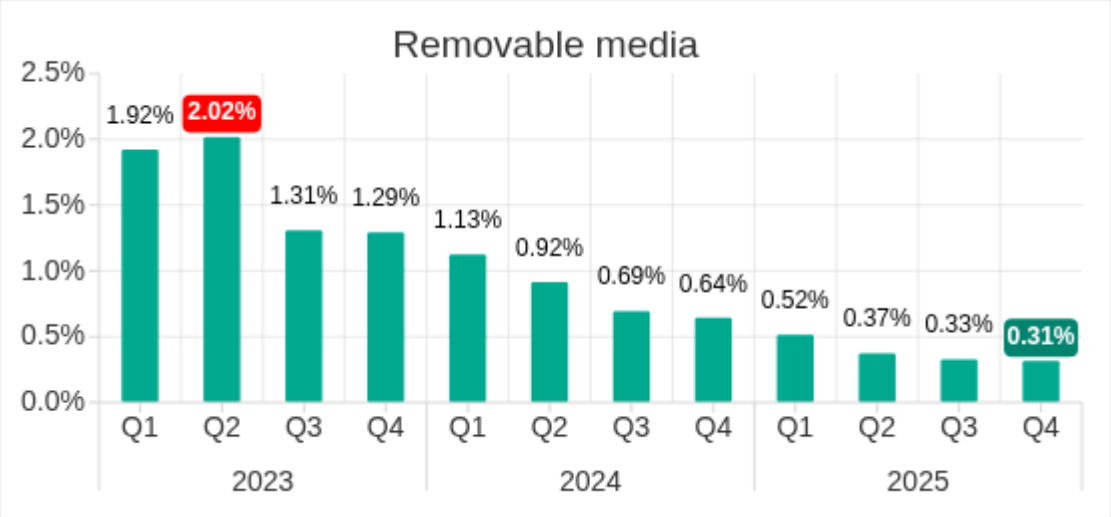
Changes in percentage of ICS computers on which threats from email clients were blocked



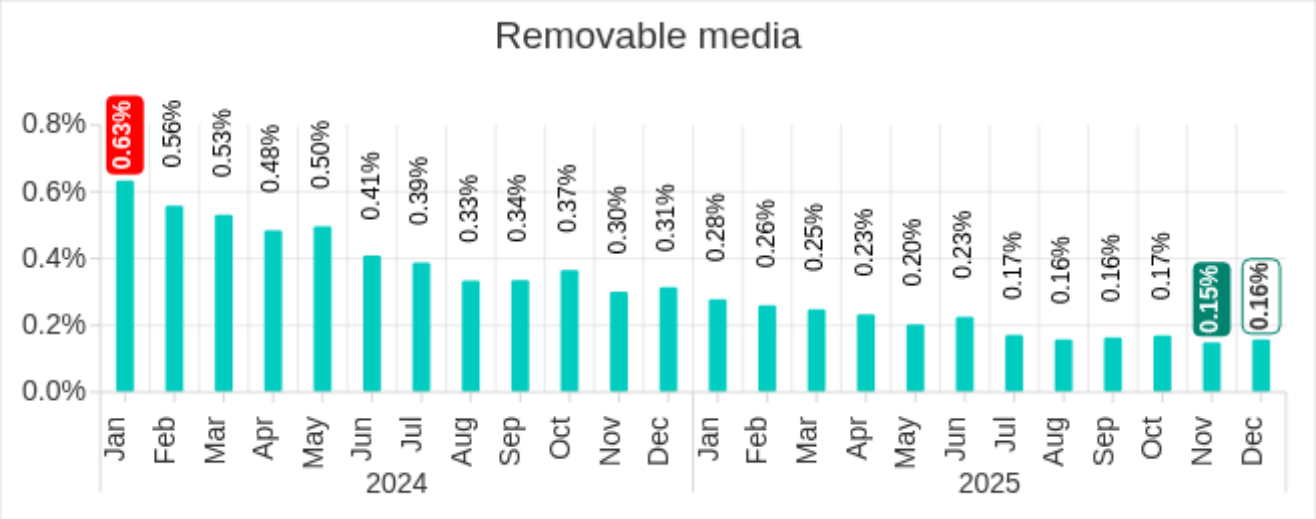
Removable media

In Q4 2025, the percentage of ICS computers on which threats from removable media were blocked continued to decrease and reached its lowest level since the beginning of 2023 — 0.31%.

Percentage of ICS computers on which threats from removable media were blocked, Q1 2023—Q4 2025

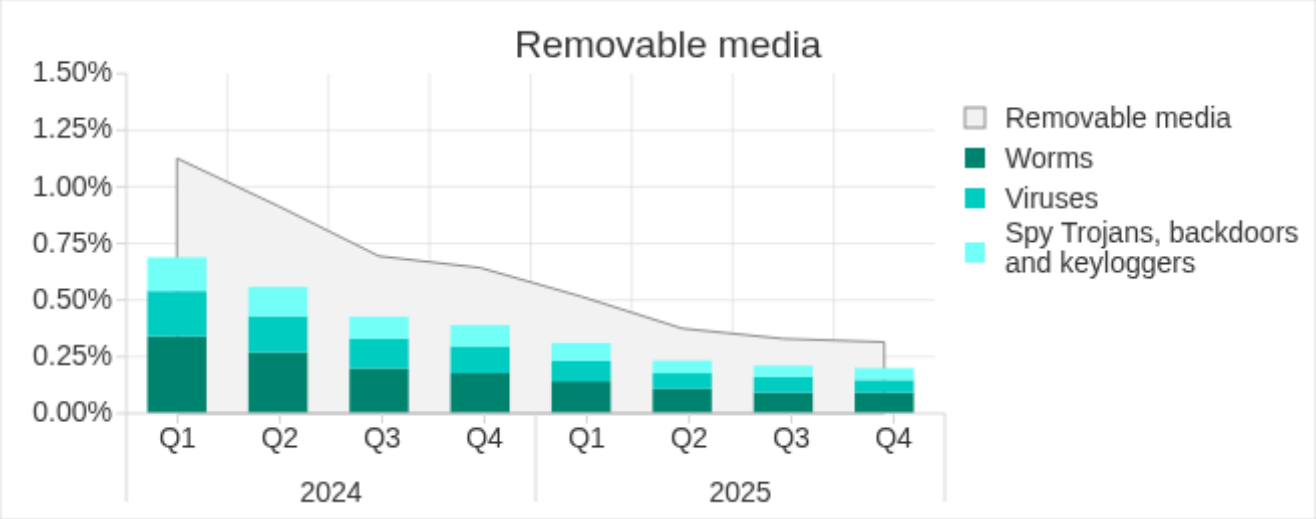


The monthly indicator also decreased, with slight fluctuations from month to month, reaching its lowest value in November.



Percentage of ICS computers on which threats from removable media were blocked, January 2024—December 2025

In Q4 2025, the main categories of threats that were blocked when removable media was connected to ICS computers were worms, viruses, and spyware.



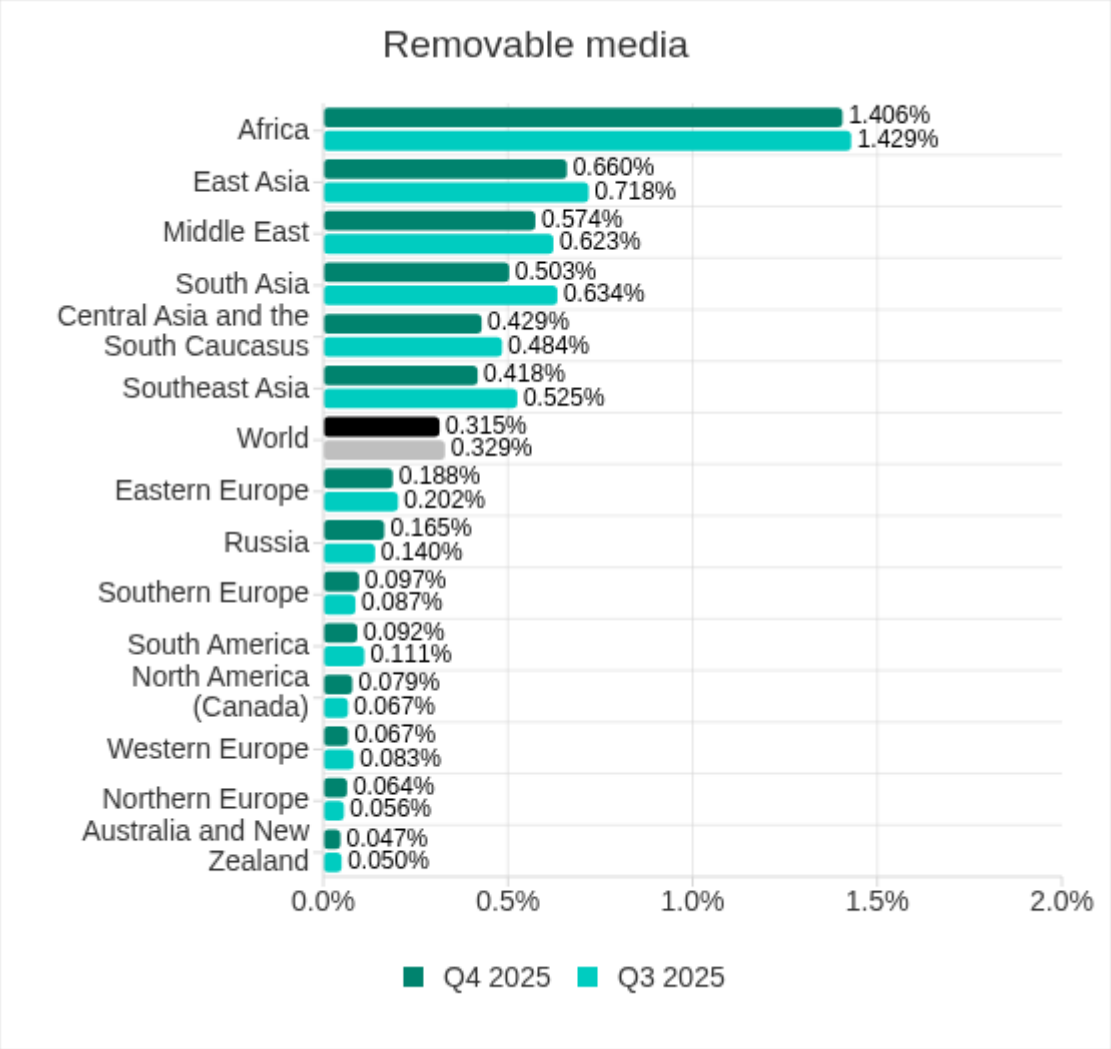
Percentage of ICS computers on which threats from removable media were blocked, Q1 2024—Q4 2025

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.

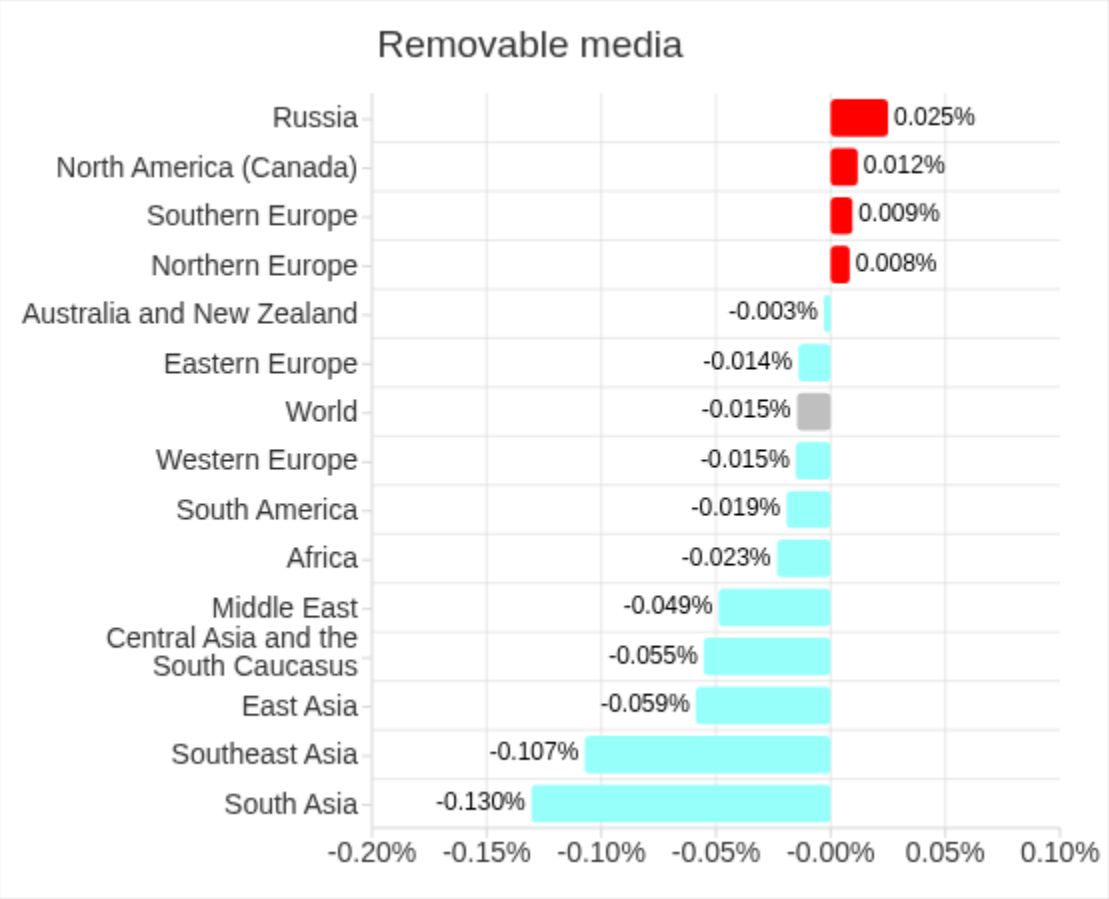
Regionally, the percentage of ICS computers on which threats from removable media were blocked ranged from 0.05% in Australia and New Zealand to 1.41% in Africa. The top three regions for this indicator were Africa (by a wide margin), followed by East Asia and South Asia.

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



In Q4 2025, the percentage increased in Russia, North America (Canada), Southern Europe, and Northern Europe.

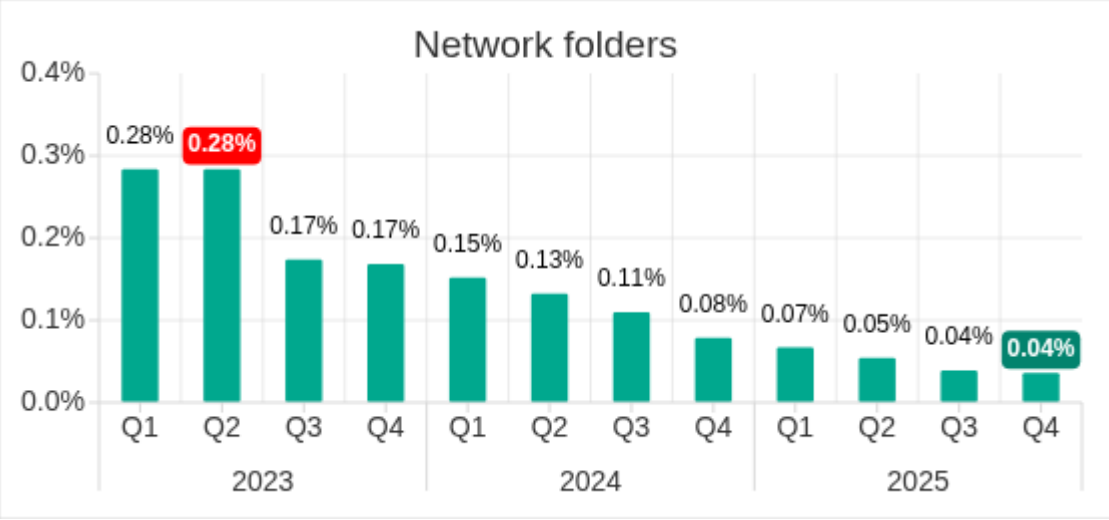
Changes in percentage of ICS computers on which threats from removable media were blocked, Q4 2025



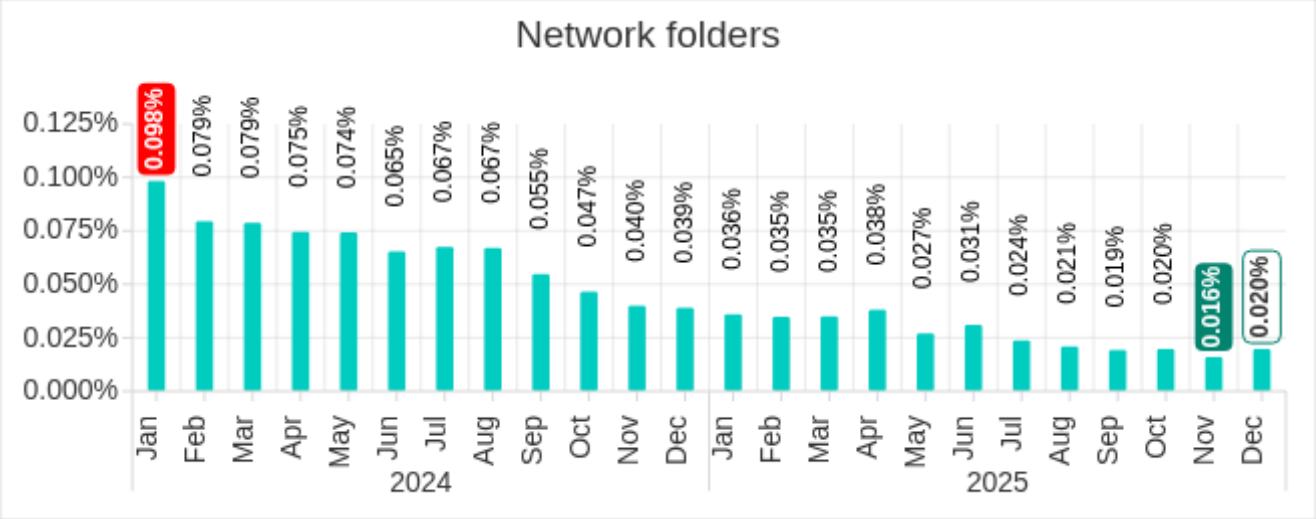
Network folders

In Q4 2025, the percentage of ICS computers on which threats from network folders were blocked reached its lowest level since the beginning of 2023.

Percentage of ICS computers on which threats from network folders were blocked, Q1 2023—Q4 2025

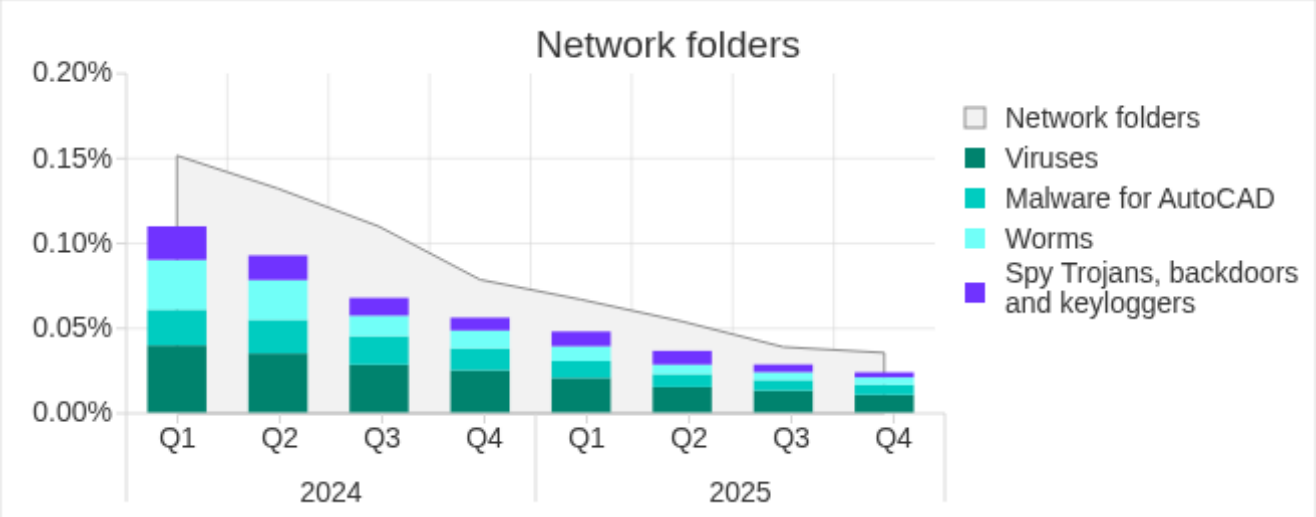


Monthly indicators show a clear downward trend. The highest level in 2025 was in April, and the lowest level was in November.



Percentage of ICS computers on which threats from network folders were blocked, January 2024—December 2025

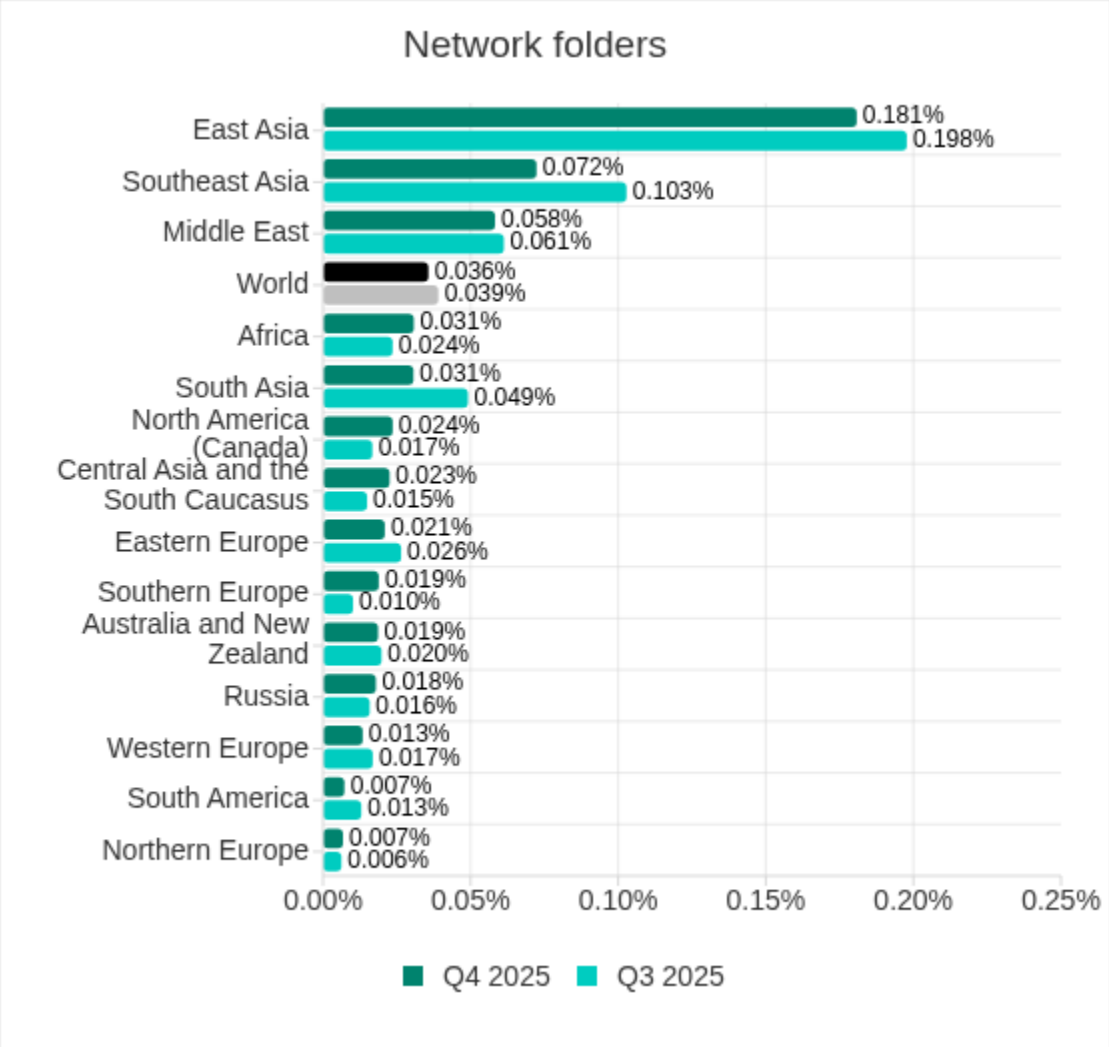
The main categories of threats that spread through network folders in Q4 2025 were viruses, AutoCAD malware, worms, and spyware.



Percentage of ICS computers on which threats from network folders were blocked, Q1 2024—Q4 2025

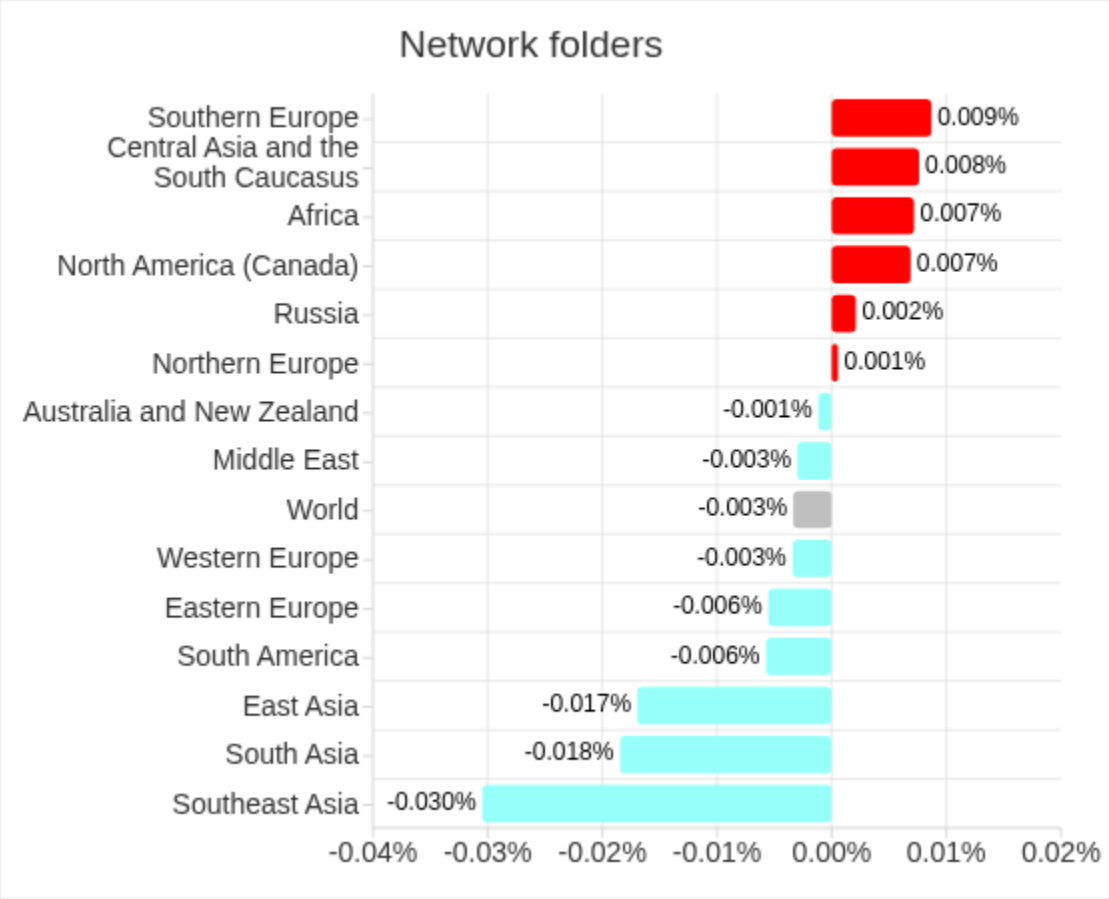
Regionally, the percentage of ICS computers on which threats from network folders were blocked ranged from 0.01% in Northern Europe to 0.18% in East Asia. The top three regions for this indicator were East Asia, Southeast Asia, and the Middle East. East Asia has traditionally led this indicator by a wide margin over other regions.

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



In Q4 2025, the percentage increased in six regions, with the most notable increases occurring in Southern Europe, and Central Asia and the South Caucasus.

Changes in percentage of ICS computers on which threats from network folders were blocked, Q4 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