

Threat landscape for industrial automation systems

Q1 2026

Changes over the quarter	3
Q1 in numbers.....	3
All threats	4
Selected industries	6
Threat categories.....	9
Main threat sources.....	21
Statistics across all threats	26
All threats	26
Selected industries	29
Threat categories.....	32
Malicious objects used for initial infection.....	35
Next-stage malware	45
Self-propagating malware. Worms and viruses.....	56
Main threat sources.....	64
Internet.....	65
Email clients.....	68
Removable media.....	72
Network folders.....	75
Methodology used to prepare statistics	79

Changes over the quarter

Q1 in numbers

Parameter	Q4 2025	Q1 2026	Quarterly changes
Global percentage of attacked ICS computers	19.7%	19.6%	▼ 0.1 pp
Percentage of ICS computers on which malicious objects from different categories were blocked			
Malicious scripts and phishing pages	6.58%	6.56%	▼ 0.02 pp
Spy Trojans, backdoors and keyloggers	3.80%	3.73%	▼ 0.07 pp
Denylisted internet resources	3.26%	3.54%	▲ 0.28 pp
Malicious documents (MSOffice + PDF)	1.76%	1.56%	▼ 0.20 pp
Worms	1.60%	1.33%	▼ 0.27 pp
Viruses	1.33%	1.31%	▼ 0.02 pp
Miners in the form of executable files for Windows	0.60%	0.59%	▼ 0.01 pp
Malware for AutoCAD	0.29%	0.30%	▲ 0.01 pp
Web miners running in browsers	0.24%	0.22%	▼ 0.02 pp
Ransomware	0.16%	0.14%	▼ 0.02 pp
Main threat sources			
Internet	7.67%	7.88%	▲ 0.21 pp
Email clients	2.76%	2.59%	▼ 0.17 pp
Removable media	0.31%	0.26%	▼ 0.05 pp
Network folders	0.04%	0.03%	▼ 0.01 pp

All threats

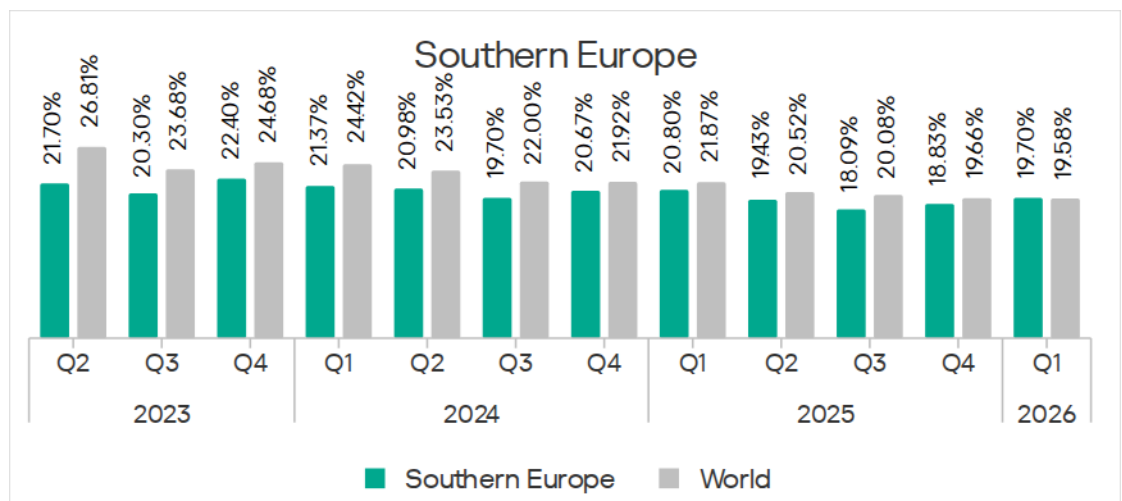
The percentage of ICS computers on which malicious objects were blocked continued to decrease, reaching 19.6% in Q1 2026. This is the lowest value in three years, and it is 1.4 times lower than in Q2 2023.

Regionally, the percentage figures ranged from 9.1% in Northern Europe to 27.4% in Africa. The difference between the highest and lowest percentage figures across regions is quite significant: the percentage in Africa is 3.0 times that in Northern Europe (see the chart in the “Statistics across all threats. All threats” section).

The percentage of ICS computers on which malicious objects were blocked increased in five regions over the quarter, most notably in Southern Europe, Northern Europe, and Russia.

In **Southern Europe**, the percentage of ICS computers on which malicious objects were blocked increased over two consecutive quarters and, for the first time in the observed period, slightly exceeded the global average.

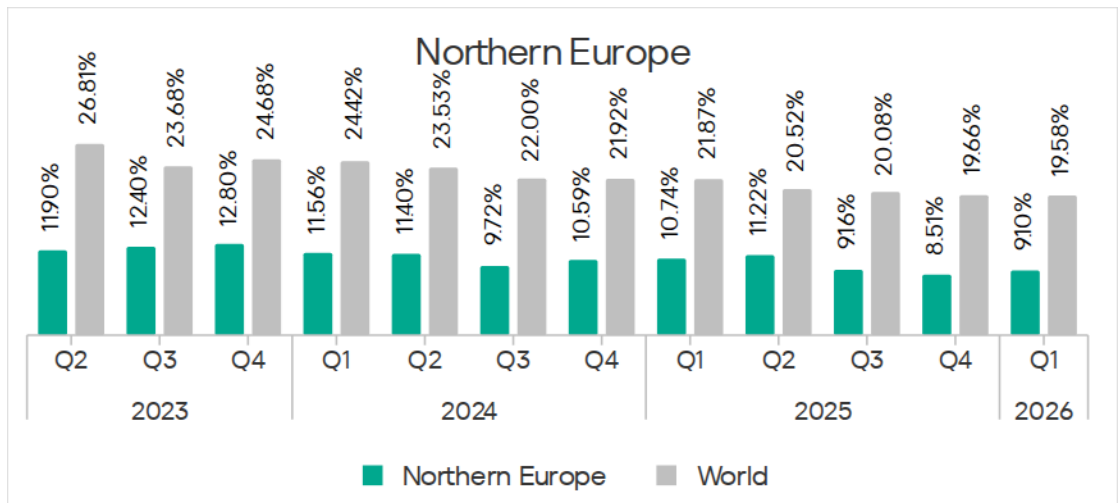
Percentage of ICS computers on which malicious objects were blocked in Southern Europe, Q2 2023 – Q1 2026



In Q1 2026, Southern Europe led the way in the increase in percentage figures for internet and email threats. The region also ranks first in the increase in the percentage figures for spyware, as well as malicious scripts and phishing pages.

For **Northern Europe**, which traditionally ranks at the bottom of the regional ranking, a 0.6 pp increase means that the number of attacked ICS computers in the region increased by 7%.

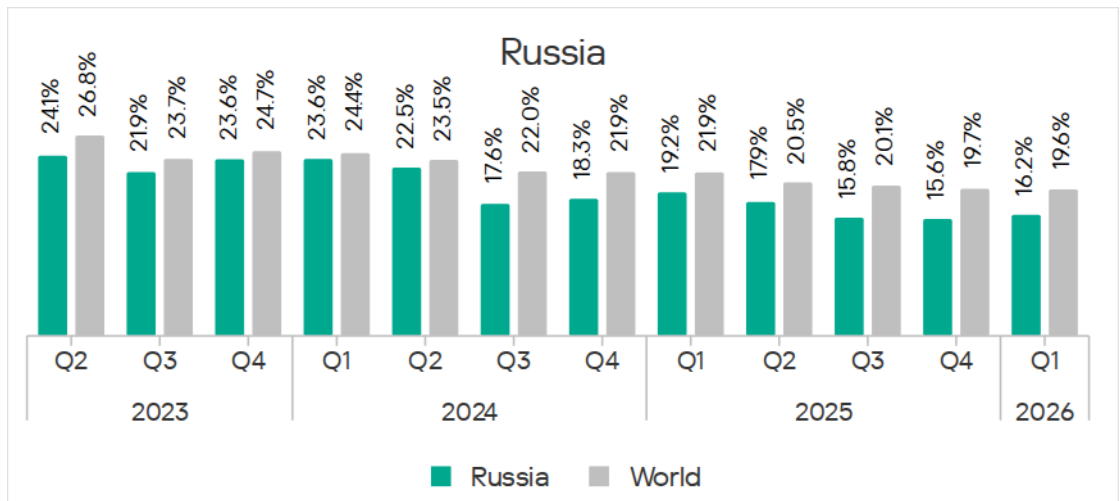
Percentage of ICS computers on which malicious objects were blocked in Northern Europe, Q2 2023 – Q1 2026



Northern Europe saw increases in percentage figures for threats from the internet and four threat categories: denylisted internet resources, malicious scripts and phishing pages (second place among regions in terms of the increase), spyware, and ransomware (one of two regions where the value increased).

In **Russia**, the percentage of ICS computers on which malicious objects were blocked exceeded the figures for the previous two quarters.

Percentage of ICS computers on which malicious objects were blocked in Russia, Q2 2023 – Q1 2026



Russia saw an increase in the percentage figure for threats from the internet, and a slight increase in the figure for threats from email clients (Russia is one of three regions where this figure did not decrease).

Among the threat categories, the greatest increases were observed in the percentage figures for denylisted internet resources, as well as spyware (distributed in the region via the internet and email clients).

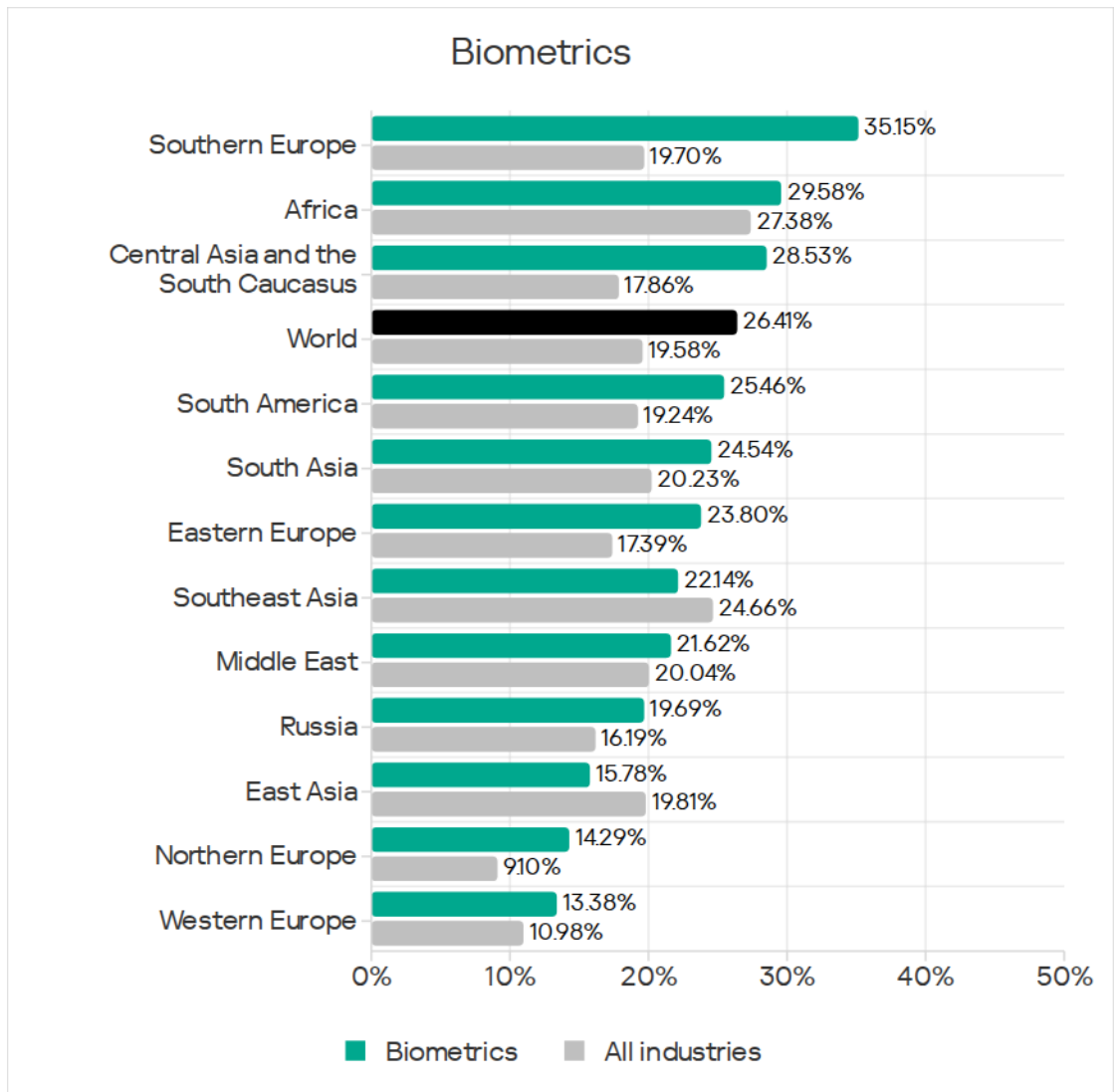
Selected industries

Biometric systems traditionally rank top among the industries and OT infrastructure types covered in this report in terms of the percentage of ICS computers on which malicious objects were blocked, with 26.4%. These systems are characterized by the availability of internet access, extensive email use, and, in many cases, minimal cybersecurity controls within the organizations that use these systems.

Biometric systems rank first among industries in terms of email threats. At the same time, unlike other industries, the percentage figure for email threats in biometric systems exceeds that for internet threats.

Regionally, Southern Europe leads the ranking based on the percentage figures for biometric systems, with 35.15%. It also ranks first for threats from email clients.

Regions ranked by percentage of ICS computers on which malicious objects were blocked in biometric systems, Q1 2026



In all selected industries, the global average follows a downward trend.

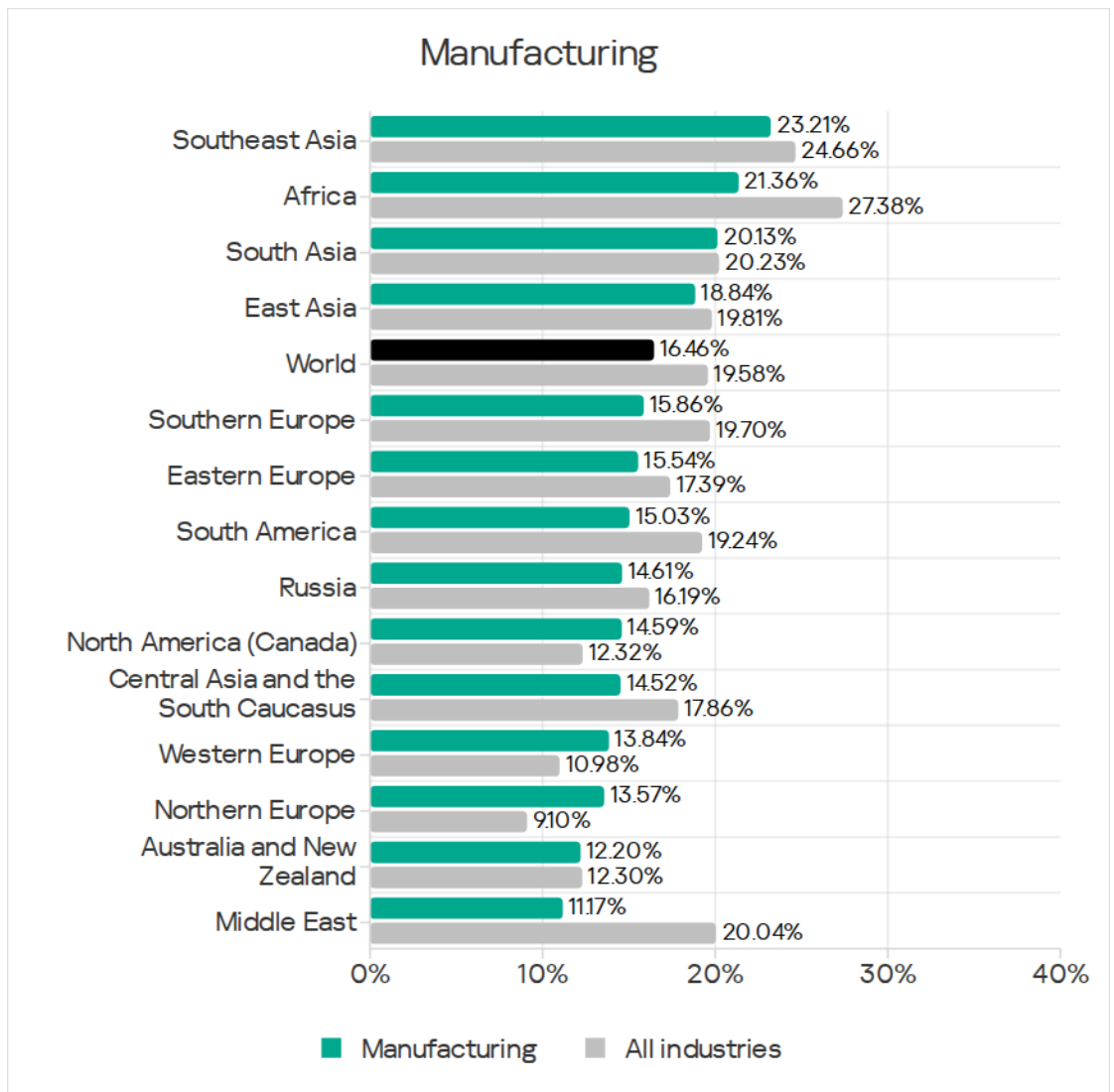
In Q1 2026, the percentage of ICS computers on which malicious objects were blocked increased only in the manufacturing sector – by 1.0 pp.

Manufacturing in Q1 2026

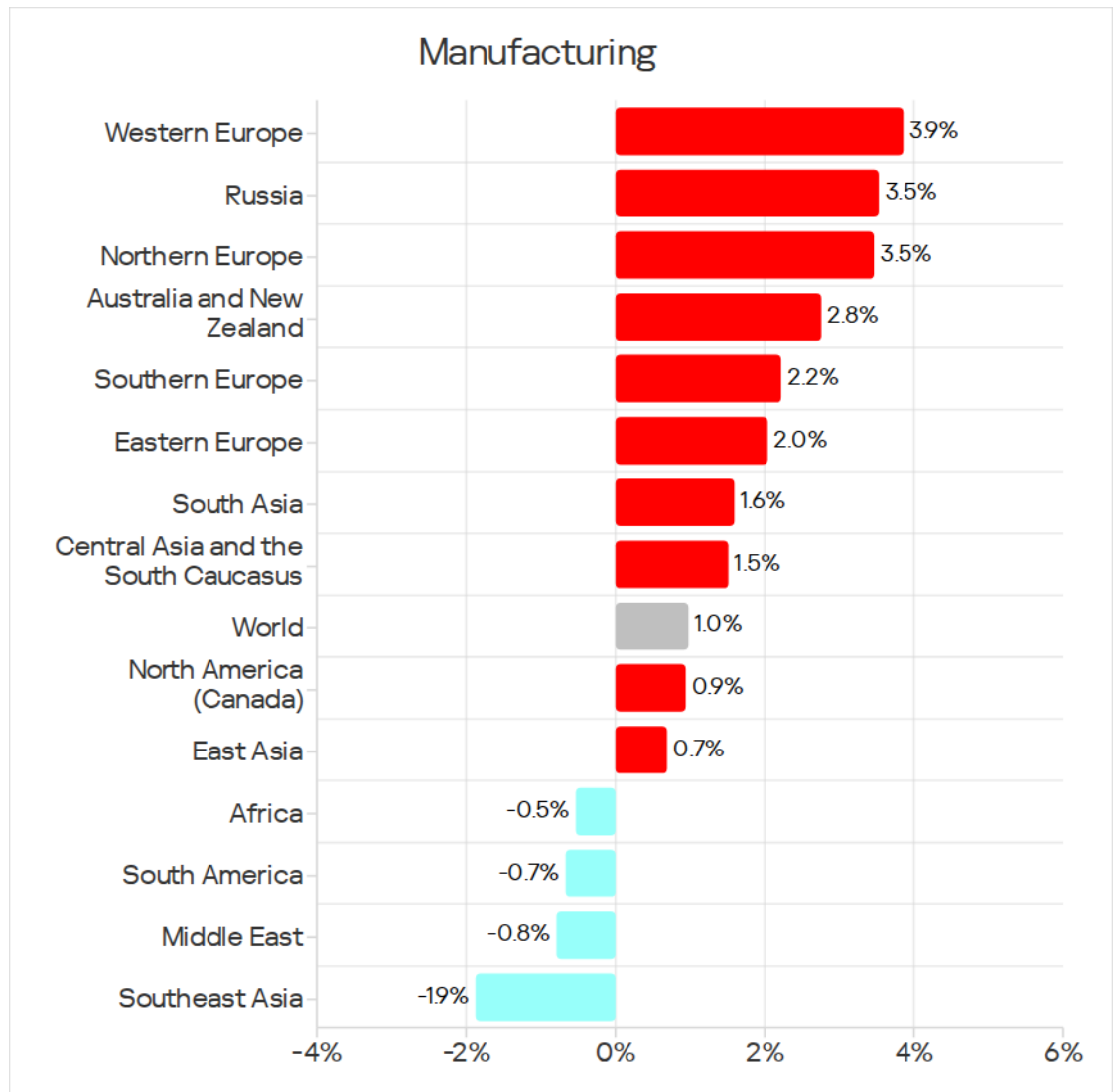
Southeast Asia ranks first among regions in terms of the percentage of ICS computers attacked in the manufacturing industry.

In East Asia, Western and Northern Europe, and in the Central Asia and South Caucasus region, the percentage figures in the manufacturing industry are above the overall average figures for the respective regions.

Regions ranked by percentage of ICS computers on which malicious objects were blocked in manufacturing, Q1 2026



Changes in percentage of ICS computers on which malicious objects were blocked in manufacturing, Q1 2026



The percentage figures for the manufacturing industry increased in ten regions, with the most notable increases in Western Europe, Northern Europe, and Russia.

In these three regions, the manufacturing industry saw the greatest increases (in percentage points) in the percentage of ICS computers on which malicious scripts and denylisted internet resources were blocked.

Additionally, Western Europe and Russia saw increases in the percentage figures for spyware in the manufacturing industry (by factors of 1.36 in Western Europe and 1.50 in Russia).

Other increases observed in the manufacturing industry were in the percentage figures for ransomware in Russia (by a factor of 2.5) and for miners in the form of executable files for Windows in Western Europe (by a factor of 2.35).

Threat categories

In Q1 2026, Kaspersky security solutions blocked malware from 10,052 different malware families of various categories on industrial automation systems.

Over the quarter, the percentage of ICS computers on which denylisted internet resources were blocked increased (after decreasing over the previous two quarters), and there was a slight increase in the percentage figure for AutoCAD malware.

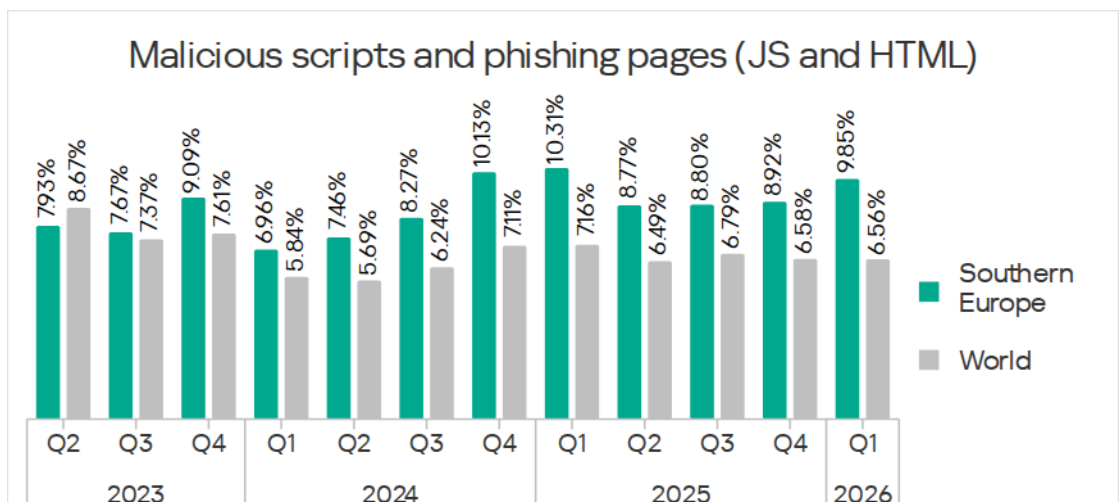
Malicious scripts and phishing pages (JS and HTML)

Malicious scripts and phishing pages retained their first-place ranking in the threat category ranking by the percentage of ICS computers on which the respective threats were blocked. The global average in Q1 2026 was 6.56%.

Regionally, the percentage of ICS computers on which malicious scripts and phishing pages were blocked ranged from 2.73% in Northern Europe to 9.85% in Southern Europe.

Over the quarter, the percentage figures increased in four regions. The most significant change was observed in **Southern Europe**. The percentage figures for malicious scripts in the region increased over three consecutive quarters.

Percentage of ICS computers on which malicious scripts were blocked in Southern Europe, Q2 2023 – Q1 2026



In Southern Europe, the highest percentage figures for malicious scripts in the selected industries were recorded in biometric systems and building automation. Over the quarter, the values increased in all selected industries.

Among the selected industries, across all regions, the highest percentage figures for the malicious scripts and phishing pages category were recorded in Southern Europe for biometric systems (19.59%) and building automation (15.43%). These same industries lead in similar rankings for malicious documents and spyware.

Spyware

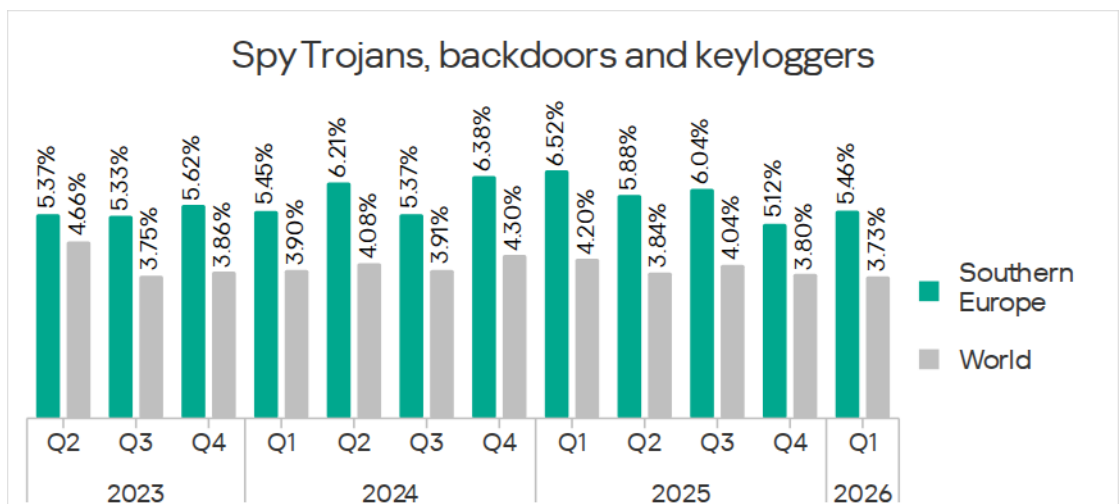
Globally, the percentage of ICS computers on which spyware was blocked decreased over two consecutive quarters, reaching 3.73%. Despite the decline, spyware has ranked second among threat categories by the percentage of attacked computers for three quarters now.

Regionally, the percentage of ICS computers on which spyware was blocked ranged from 1.34% in Northern Europe to 5.94% in Africa. In the relevant ranking, Southern Europe has pushed Southeast Asia down from second place.

The percentage figures increased in five regions over the quarter, most notably in Southern Europe and Russia (see the section “Next-stage malware. Spyware”).

Southern Europe ranks second only to Africa in spyware, at 5.46%. Spyware mainly reaches ICS computers in the region via email clients.

Percentage of ICS computers on which spyware was blocked in Southern Europe, Q2 2023 – Q1 2026



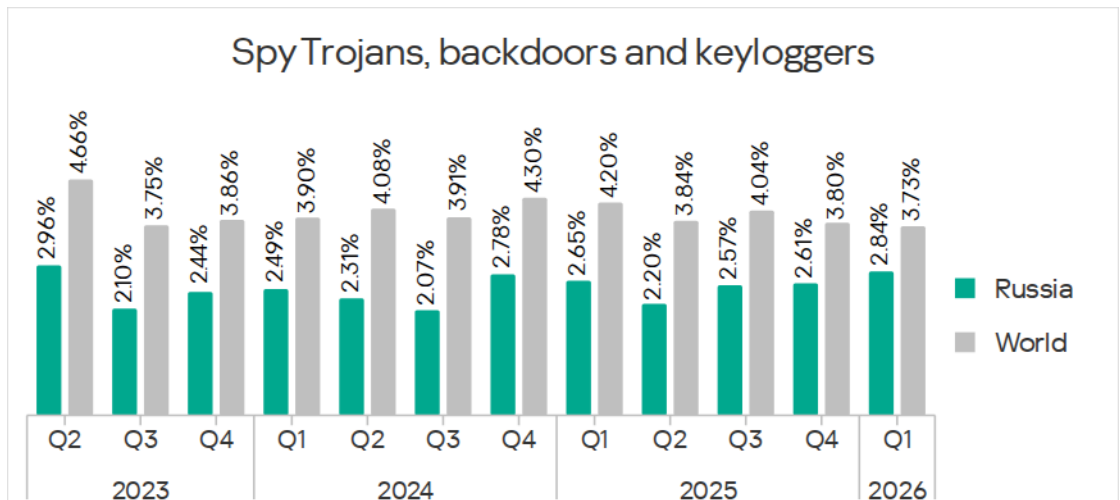
It is worth recalling that Southern Europe ranks first among regions in both the percentage figures and their increase for malicious scripts, which are used, among other things, to infect computers with spyware.

In Southern Europe, among the selected industries, the percentage of ICS computers on which spyware was blocked increased in all industries except manufacturing. The greatest increase was observed in biometric systems.

In Russia, the percentage of ICS computers on which spyware was blocked increased over three consecutive quarters; compared with Q2 2025, the figure increased by a factor of 1.3, reaching 2.84%. Over the past three years, this percentage was higher only in Q2 2023.

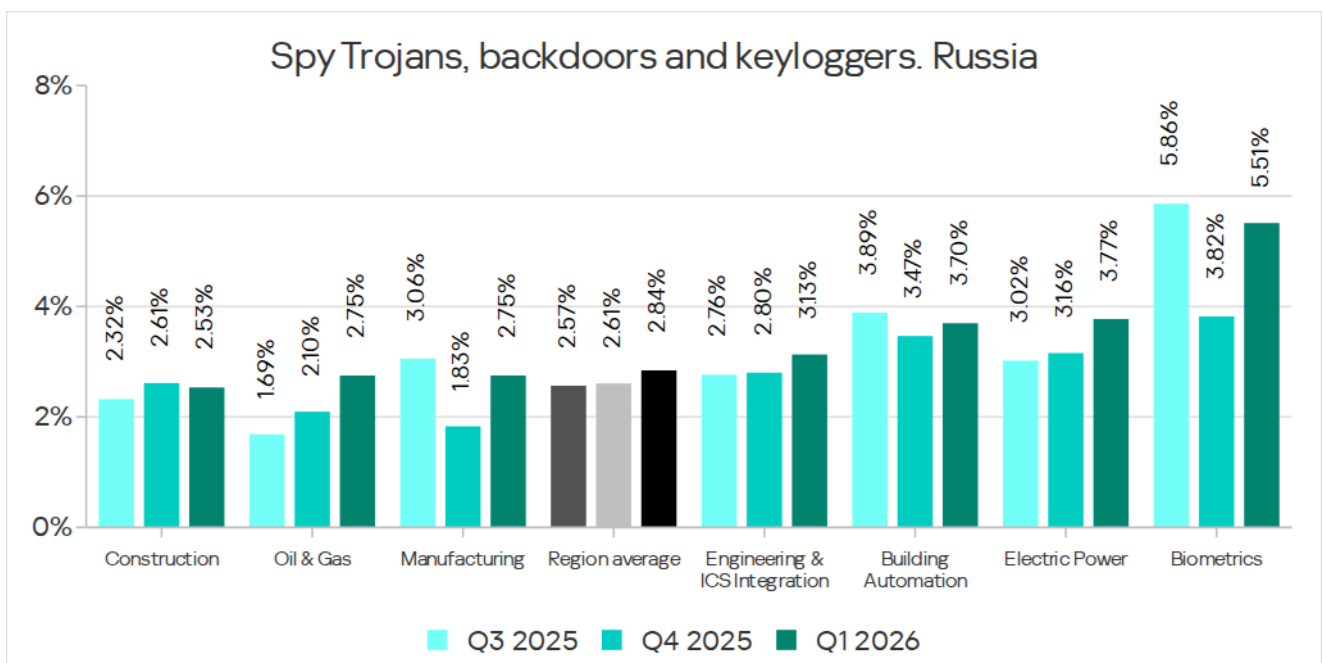
Spyware is distributed in the region via the internet and email.

Percentage of ICS computers on which spyware was blocked in Russia, Q2 2023 – Q1 2026



Among the selected industries, the highest percentage of spyware in Russia was recorded in biometric systems.

The percentage of ICS computers on which spyware was blocked in Russia increased in all industries except construction. The percentage figure has increased for two consecutive quarters in the oil and gas industry (by a factor of 1.63 over six months), and for three consecutive quarters in engineering and ICS integration, as well as electric power. In the remaining sectors, the values have been fluctuating.



Percentage of ICS computers on which spyware was blocked in various industries in Russia, Q3 2025 – Q1 2026

Spyware is also commonly used to steal the information needed to deliver other types of malware, such as ransomware. It should be noted that in Russia, the percentage figures for ransomware increased across all selected industries, except oil and gas and building automation.

Among the selected industries across all regions, the highest percentage figures for spyware were also recorded in Southern Europe – in biometric systems (17.48%) and building automation (9.57%). These same industries rank top for malicious scripts and malicious documents.

Denylisted internet resources

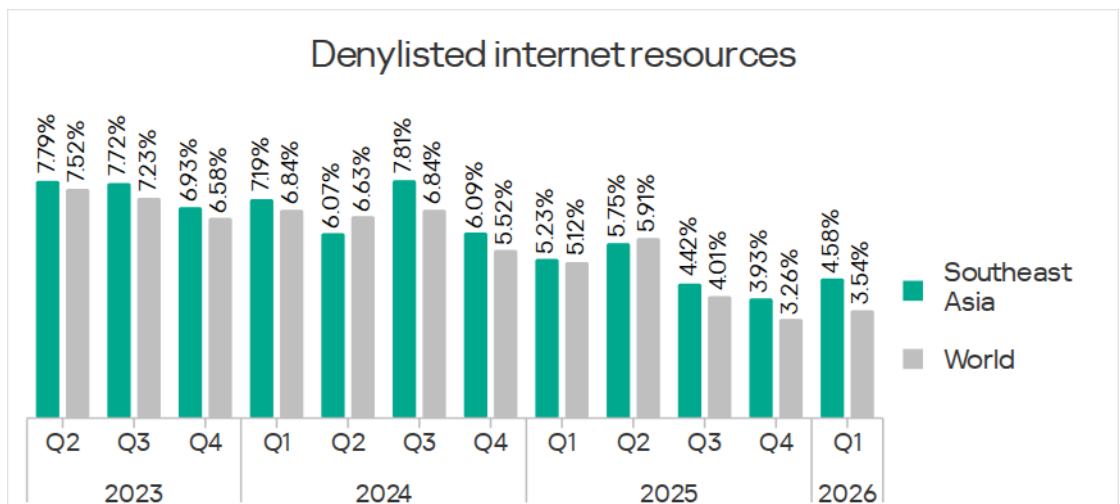
Denylisted internet resources ranked third in the threat category ranking by the percentage of ICS computers on which each threat was blocked.

Globally, the percentage of ICS computers on which denylisted internet resources were blocked increased to 3.54%. Nevertheless, this is lower than the other quarterly figures over the past three years.

Regionally, the percentage of ICS computers on which denylisted internet resources were blocked ranged from 2.06% in Northern Europe to 4.58% in Southeast Asia.

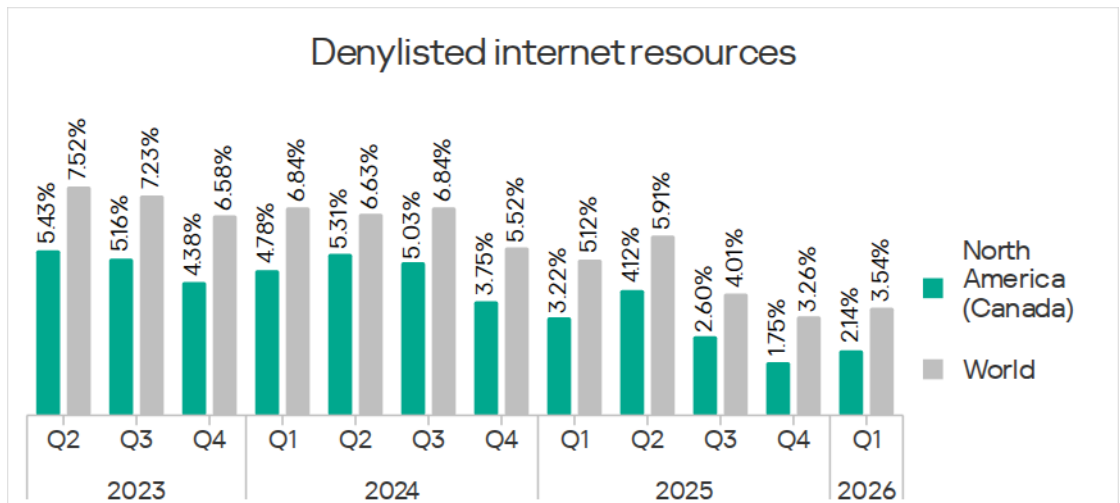
The most notable increase over the quarter occurred in **Southeast Asia**. Among the industries in the region, the highest percentage figures for this threat category were recorded in electric power and construction. Over the quarter, the largest increases in percentage figures were observed in the electric power and manufacturing industries.

Percentage of ICS computers on which denylisted internet resources were blocked in Southeast Asia, Q2 2023 – Q1 2026



In **North America (Canada)**, denylisted internet resources showed the greatest increase in terms of growth among all categories, with the value increasing by a factor of 1.22.

Percentage of ICS computers on which denylisted internet resources were blocked in North America (Canada), Q2 2023 – Q1 2026



Among the selected industries across all regions, the highest percentage figures for the denylisted internet resources category were in Southeast Asia in the electric power (7.11%) and construction (6.25%) industries.

It should be noted that electric power and construction in Southeast Asia, in Central Asia and the South Caucasus, and in Africa, electric power in Russia, and construction in Eastern Europe were in the top eight places in the ranking of industries across all regions by the percentage of ICS computers on which denylisted internet resources were blocked in various industries.

Malicious documents (MSOffice + PDF)

Malicious documents rank fourth in the threat category ranking by the percentage of ICS computers on which threats in each category were blocked.

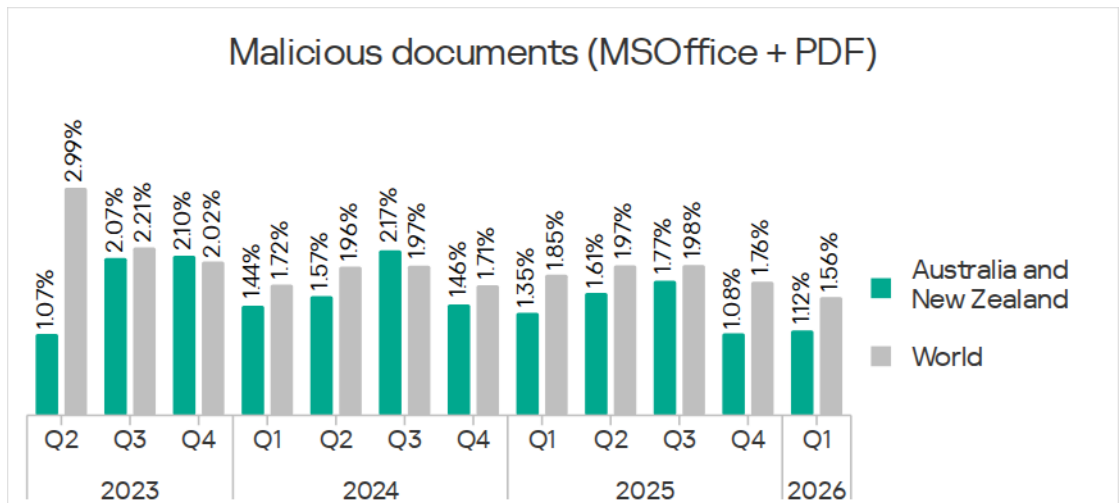
The percentage figure for this category decreased over two consecutive quarters, reaching its lowest value (1.56%) for the entire period of observations in Q1 2026.

Regionally, the percentage of ICS computers on which malicious documents were blocked ranged from 0.43% in Northern Europe to 3.14% in Southern Europe. The Middle East moved up from fourth to second place in this ranking.

Over the quarter, the percentage figures for malicious documents increased in two regions – Australia and New Zealand, and Russia – but only slightly.

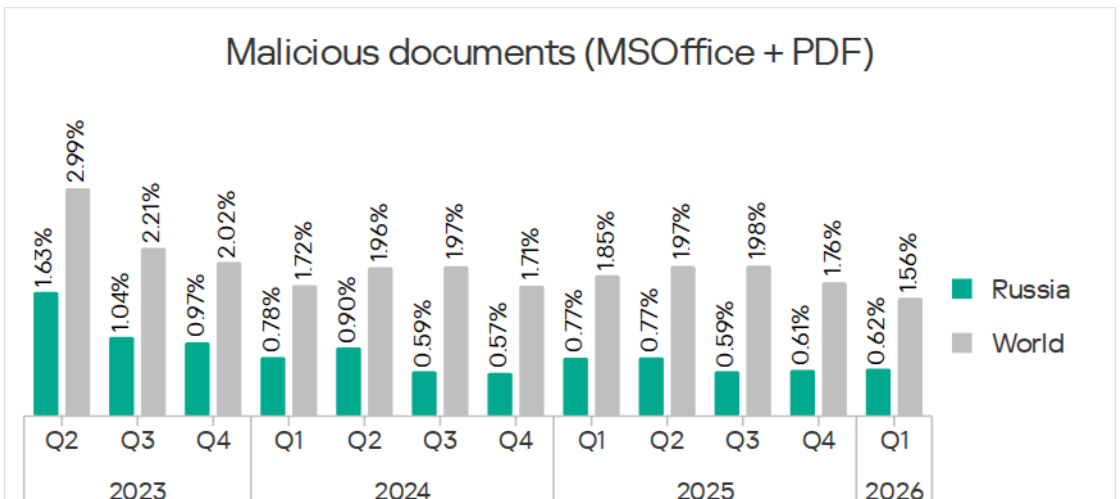
In **Australia and New Zealand**, the percentage figure for Q1 2026 is among the lowest over the past three years.

Percentage of ICS computers on which malicious documents were blocked in Australia and New Zealand, Q2 2023 – Q1 2026



In **Russia**, the percentage figure has increased for two consecutive quarters.

Percentage of ICS computers on which malicious documents were blocked in Russia, Q2 2023 – Q1 2026



Among the selected industries across all regions, the highest percentage figures for malicious documents were recorded in Southern Europe for biometric systems (9.02%) and building automation (6.97%). These same industries also lead in similar rankings for malicious scripts and spyware.

Ransomware

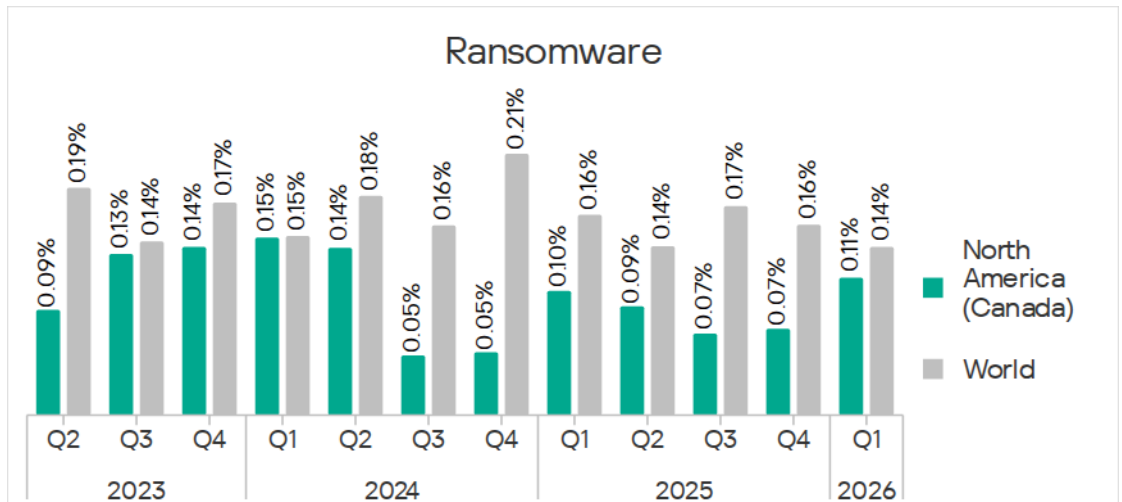
Globally, in Q1 2026, the percentage of ICS computers on which ransomware was blocked has decreased for two consecutive quarters, reaching 0.14%. This is the lowest value among all categories.

Regionally, the percentage of ICS computers on which ransomware was blocked ranged from 0.06% in Australia and New Zealand to 0.26% in the Middle East.

The percentage of ICS computers on which ransomware was blocked increased in two regions: North America (Canada) and, slightly, in Northern Europe (by 0.01 pp).

North America (Canada) rose in the corresponding regional ranking from next-to-last to seventh place with 0.11%. Ransomware is mainly distributed in the region via email clients.

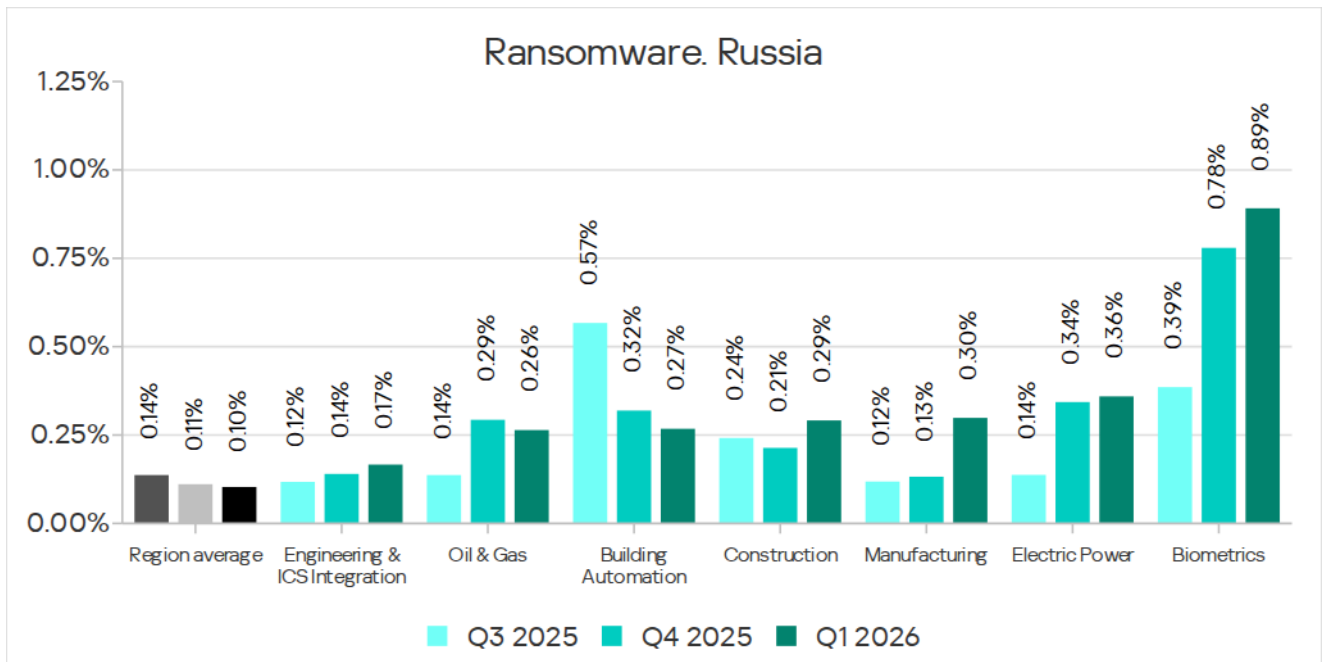
Percentage of ICS computers on which ransomware was blocked in North America (Canada), Q2 2023 – Q1 2026



Among the selected industries in North America (Canada), ransomware was blocked in building automation (0.16%) and construction (0.09%).

In **Northern Europe**, percentage figures for ransomware increased across all selected industries.

It is worth noting that in **Russia**, the percentage of ICS computers on which ransomware was blocked increased across all selected industries, except oil and gas and building automation. The highest increase, by a factor of 2.3, was observed in the manufacturing industry.



Percentage of ICS computers on which ransomware was blocked in various industries in Russia, Q3 2025 – Q1 2026

Among the selected industries across all regions, the highest percentage figures for ransomware were recorded in Central Asia and the South Caucasus in the oil and gas and manufacturing industries (0.92% and 0.65%, respectively), and in Russia in biometric systems (0.89%).

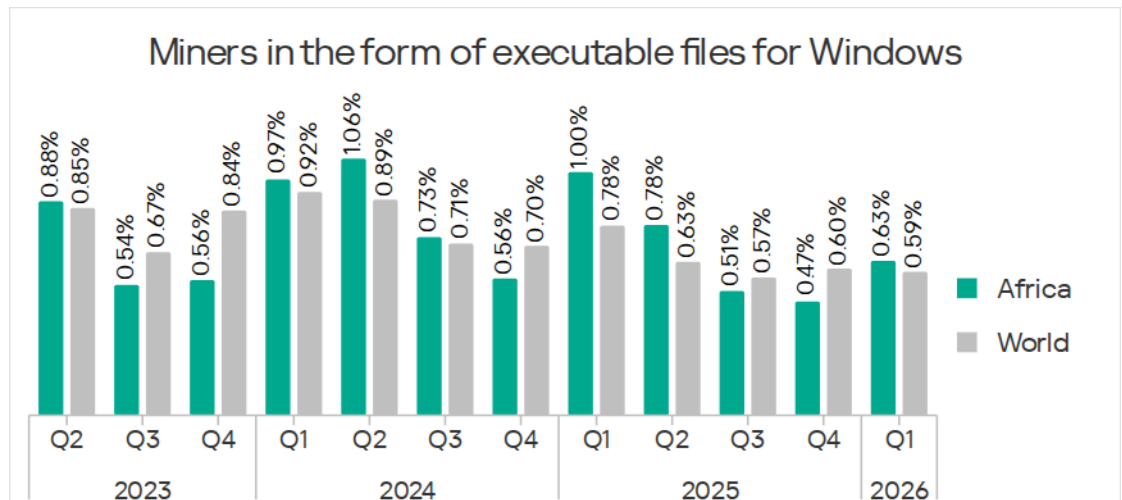
Miners in the form of executable files for Windows

Globally, in Q1 2026, the percentage of ICS computers on which miners in the form of executable files for Windows were blocked decreased to 0.59%.

Regionally, the percentage ranged from 0.14% in Australia and New Zealand to 1.12% in Central Asia and the South Caucasus. Africa has moved into third place in the top three, pushing Eastern Europe down. Russia still ranks second at 0.82%.

The percentage increased in seven regions (see the section “Next-stage malware. Miners in the form of executable files for Windows”). The largest increase was observed in **Africa**. Among the selected industries, the largest increases in the region were in the manufacturing and oil and gas industries.

Percentage of ICS computers on which miners in the form of executable files for Windows were blocked in Africa, Q2 2023 – Q1 2026



Among the selected industries across all regions, the highest percentage figures for miners in the form of executable files were recorded in Central Asia and the South Caucasus. The top 10 industries for this parameter in the region included all selected industries except the engineering and ICS integration sector. The top spots were taken by construction (1.99%), biometric systems (1.98%), and the oil and gas industry (1.97%).

Web miners

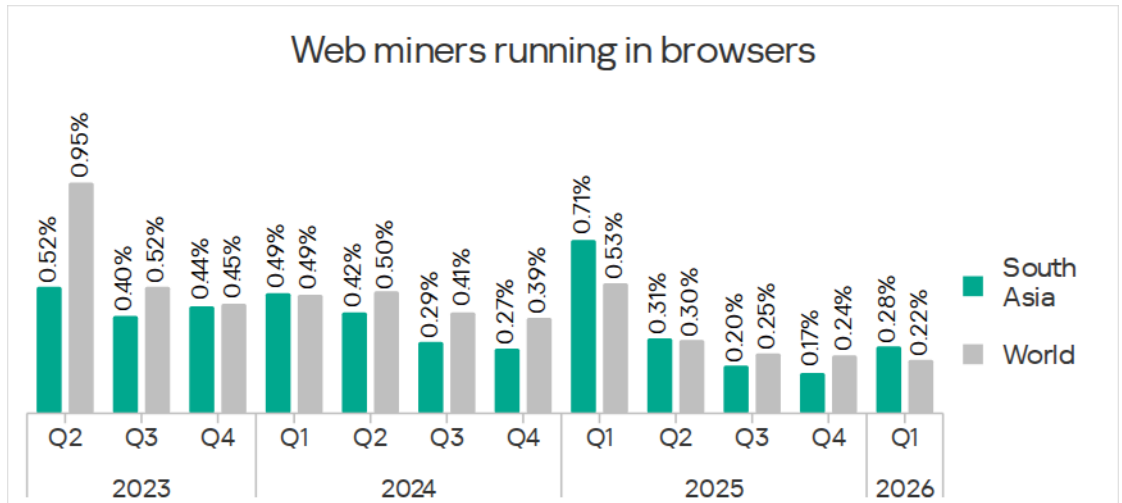
Globally, the percentage of ICS computers on which web miners were blocked has been declining for a year, and in Q1 2026, it reached the lowest value over the entire period under review – 0.22%.

Regionally, the percentage ranged from 0.06% in East Asia to 0.34% in Africa.

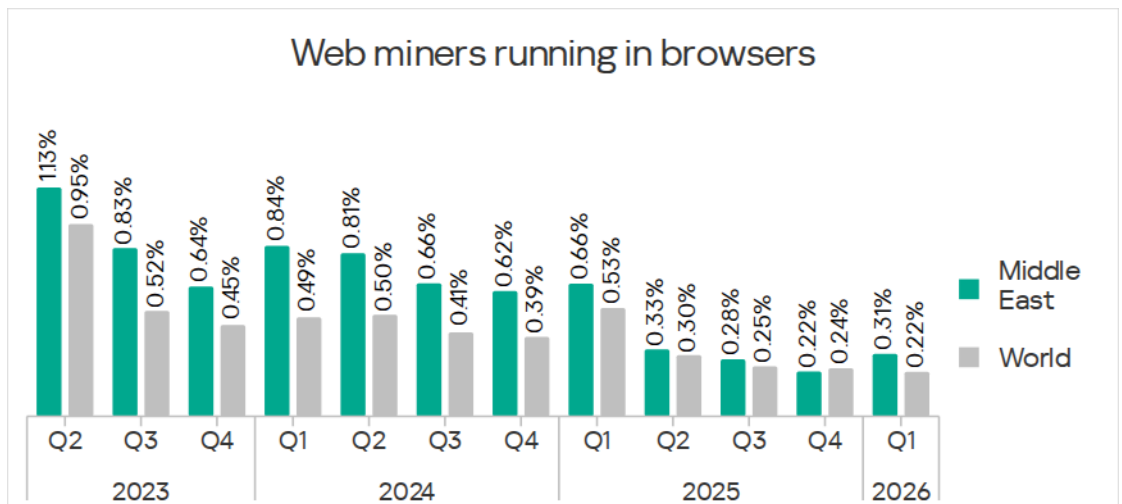
In Q1 2026, Africa rose in the corresponding regional ranking from third to first place, and the Middle East from sixth to second place.

The largest increases in the percentage of ICS computers on which web miners were blocked were observed in **South Asia** (by a factor of 1.6), the **Middle East** (by a factor of 1.4), and **Africa** (by a factor of 1.3). Despite the increases, the percentage figures in these regions for Q1 2026 did not exceed those observed in 2023–2024 and in Q1 2025.

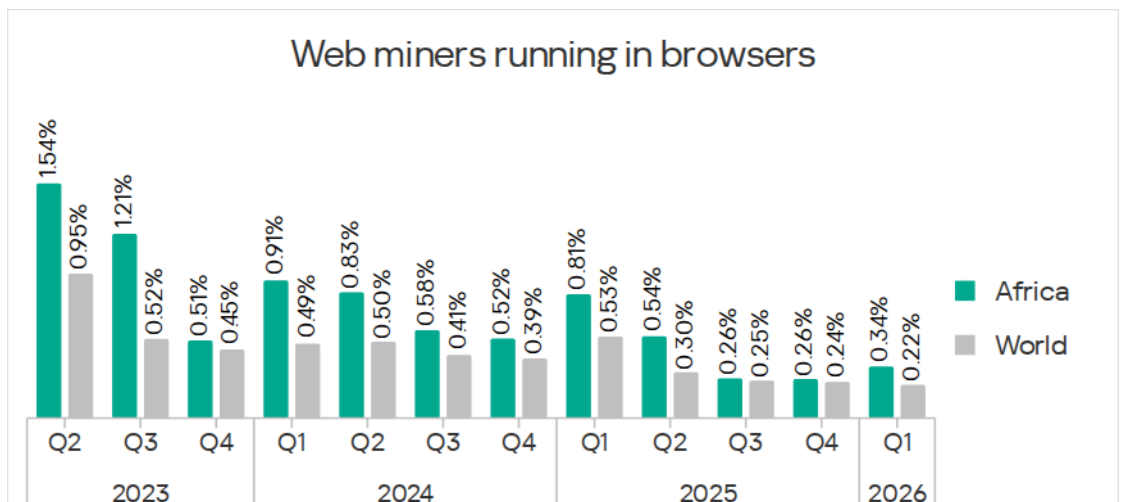
Percentage of ICS computers on which web miners were blocked in South Asia, Q2 2023 – Q1 2026



Percentage of ICS computers on which web miners were blocked in the Middle East, Q2 2023 – Q1 2026



Percentage of ICS computers on which web miners were blocked in Africa, Q2 2023 – Q1 2026



Among the selected industries across all regions, the highest percentage figures for web miners were recorded in Russia for biometric systems (0.97%). Biometric systems in South Asia (0.79%) ranked second, and the electric power sector in Southeast Asia (0.76%) ranked third.

Worms

Globally, in Q1 2026, the percentage of ICS computers on which worms were blocked decreased to 1.33%.

The percentage decreased across all regions following an increase in the previous quarter (due to a new wave of phishing attacks that distributed the Backdoor.MSIL.XWorm backdoor worm across all regions of the world).

Regionally, the percentage ranged from 0.21% in Australia and New Zealand to 3.26% in Africa.

Among the selected industries across all regions, the highest percentage figure for worms was recorded in Central Asia and the South Caucasus for biometric systems (4.80%). Second and third places for this parameter were taken by industries in Africa – biometric systems (4.04%) and electric power (3.53%).

Viruses

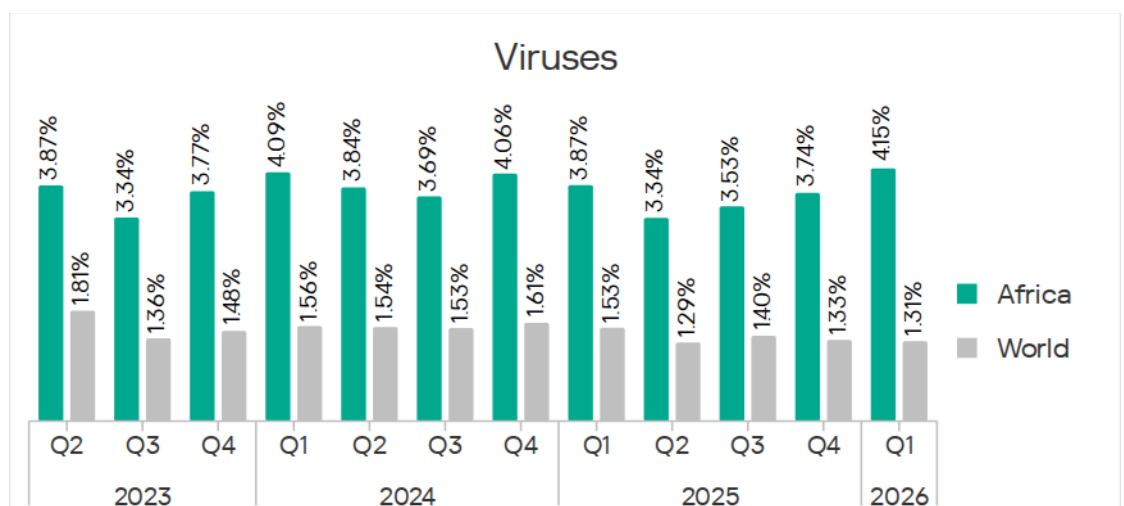
Globally, the percentage of ICS computers on which viruses were blocked decreased to 1.31% in Q1 2026.

Regionally, the percentage ranged from 0.13% in Australia and New Zealand to 6.11% in Southeast Asia. The top 3 regions for this parameter remained the same: Southeast Asia (first by a wide margin), Africa, and East Asia. These same regions are also among the leaders for AutoCAD malware.

The largest increase in this percentage figure was observed in Africa.

The percentage of ICS computers on which viruses were blocked in **Africa** grew over three consecutive quarters and reached its highest value for the entire period under review – 4.15%.

Percentage of ICS computers on which viruses were blocked in Africa, Q2 2023 – Q1 2026



Among the selected industries in Africa, the highest percentage for viruses is in construction (5.35%).

Among the selected industries across all regions, the highest percentage figures for viruses were recorded in Southeast Asia in the construction industry (6.35%) and building automation (5.50%).

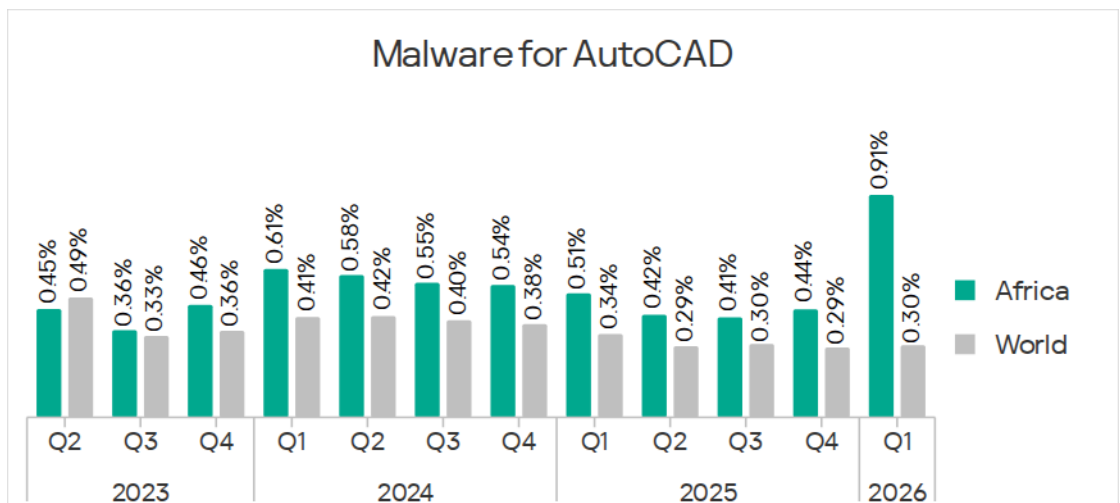
Malware for AutoCAD

The percentage of ICS computers on which malware for AutoCAD was blocked increased to 0.30%.

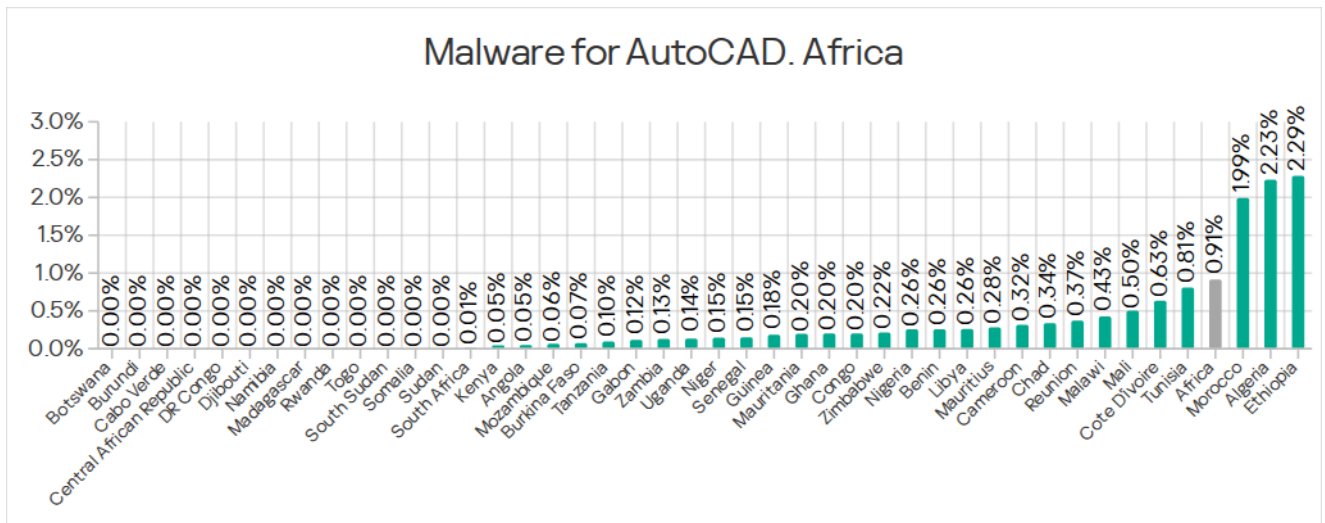
Regionally, the percentage ranged from 0.00% in Northern Europe to 1.87% in Southeast Asia. The leaders for this parameter are the same regions as in the virus ranking: Southeast and East Asia (both regions by a wide margin over the rest), and Africa.

The most notable increase over the quarter was observed in **Africa**, with the region’s percentage figure rising by 0.47 pp, a very significant increase for this category, and almost doubling.

Percentage of ICS computers on which malware for AutoCAD was blocked in Africa, Q2 2023 – Q1 2026



Among African countries, Ethiopia, Algeria, and Morocco lead in terms of the percentage of ICS computers on which AutoCAD malware was blocked, with unusually high figures for this threat category (around 2%). The largest increases in the percentage of ICS computers on which AutoCAD malware was blocked were recorded in Algeria and Morocco, by 0.96 pp and 1.40 pp, respectively.



As with viruses, the highest percentage figure for AutoCAD malware in the region among the selected industries was recorded in the construction industry (1.95%).

Among the selected industries across all regions, the highest percentage figures for AutoCAD malware were recorded in the construction industry in East Asia (5.58%) and Southeast Asia (3.87%).

Main threat sources

In Q1 2026, the average percentage figures across all threat sources, except threats from the internet, decreased globally.

Internet

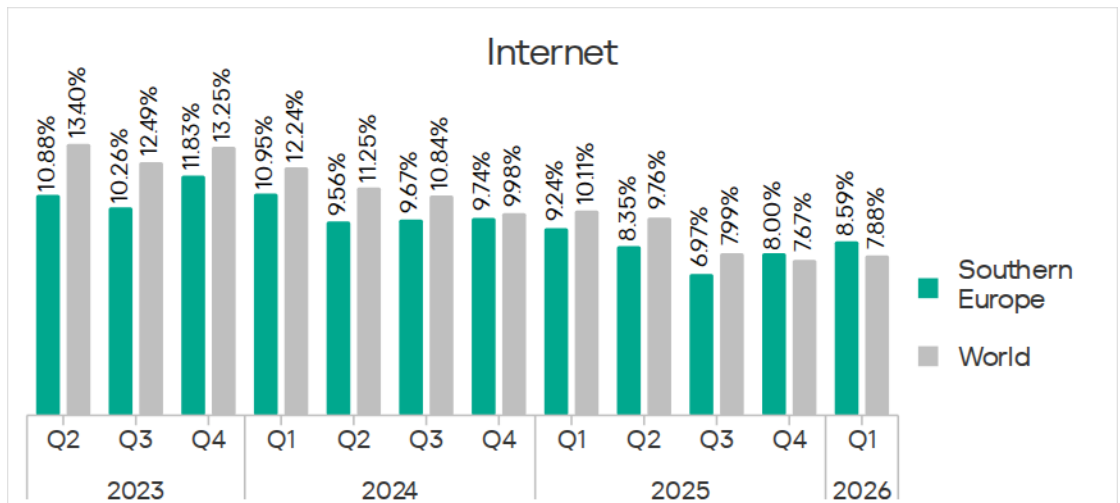
Globally, the percentage of ICS computers on which threats from the internet were blocked increased to 7.88% in Q1 2026. However, over the past three years, the percentage figure for internet threats has followed a downward trend.

Regionally, the percentage of ICS computers on which threats from the internet were blocked ranged from 4.48% in Northern Europe to 10.16% in Southeast Asia.

The largest increases in percentage figures were recorded in Southern Europe, Southeast Asia, and Northern Europe.

In **Southern Europe**, the percentage of ICS computers on which threats from the internet were blocked has grown for two consecutive quarters, exceeding the global average in the last quarter for the first time.

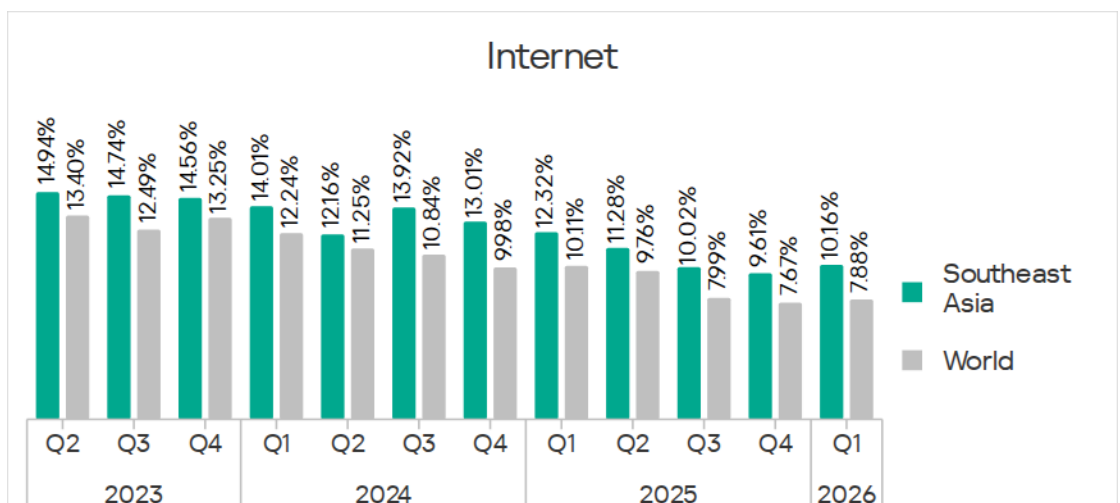
Percentage of ICS computers on which threats from the internet were blocked in Southern Europe, Q2 2023 – Q1 2026



Among the selected industries, the largest increases in percentage figures in the region in Q1 2026 were observed in the manufacturing and construction industries.

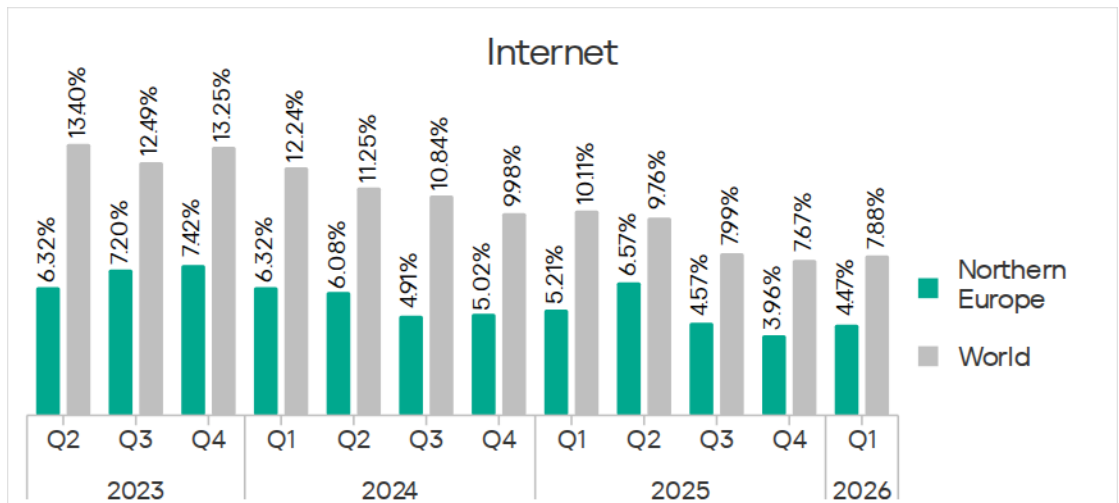
In **Southeast Asia**, the percentage figure increased for the first time since Q3 2024. Among the selected industries, the highest percentage figures for threats from the internet in the region are in electric power and construction; the largest increase over the quarter was observed in the electric power sector.

Percentage of ICS computers on which threats from the internet were blocked in Southeast Asia, Q2 2023 – Q1 2026



The dynamics of this parameter in **Northern Europe** are close to the global average trend. Among the selected industries in the region, the highest percentage figures for threats from the internet were recorded in biometric systems and the electric power sector; the percentage figures in these industries also saw the largest increases over the quarter.

Percentage of ICS computers on which threats from the internet were blocked in Northern Europe, Q2 2023 – Q1 2026



Among the selected industries across all regions, the highest percentage figures for threats from the internet were recorded in Southeast Asia in electric power (13.16%) and construction (12.55%), and in South Asia in the engineering and ICS integration sector (12.33%).

Email clients

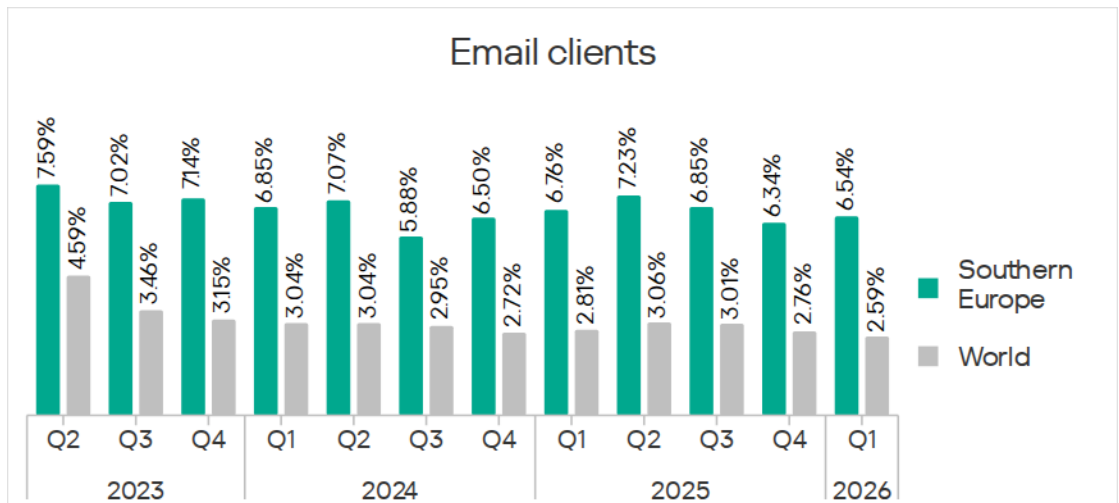
Globally, the percentage of ICS computers on which threats from email clients were blocked decreased to 2.59%. This is the lowest value in three years.

Regionally, the percentage ranged from 0.58% in Northern Europe to 6.54% in Southern Europe.

In Q1 2026, the percentage of threats from email clients increased in three regions: Southern Europe, East Asia, and, slightly, in Russia.

The largest increase in the parameter was recorded in **Southern Europe**. Among the selected industries, the biometric systems industry is the undisputed leader in terms of percentage figures for threats from email clients, as well as the increase in this parameter over the quarter.

Percentage of ICS computers on which threats from email clients were blocked in Southern Europe, Q2 2023 – Q1 2026



Among the selected industries across all regions, the highest percentage figures for threats from email clients were recorded in Southern Europe for biometric systems (19.78%) and building automation (12.34%). In these two industries, the percentage of ICS computers on which threats from email clients are blocked is higher than the percentage for threats from the internet. A similar situation was observed in two other instances, both in biometric systems (in South America and Southeast Asia).

Removable media

Globally, the percentage of ICS computers on which threats were detected when connecting removable media continued to decrease, reaching its lowest value for the period under review – 0.26%.

The percentage figures did not increase in any region over the quarter. Regionally, the percentage ranged from 0.04% in Australia and New Zealand to 1.23% in Africa.

Africa has been a long-time leader in this ranking. Although the figure for the region is declining, the gap between Africa and other regions remains quite significant. Compared to Australia and New Zealand, which ranks lowest, the figure in Africa is 29.3 times higher.

Among the selected industries, the highest percentage figures for threats on removable media in Africa are in the electric power sector (1.16%) and biometric systems (1.15%).

Among the selected industries across all regions, the highest percentage figures for threats blocked on ICS computers when removable media are connected are observed in the electric power sector in Central Asia and the South Caucasus (1.45%), East Asia (1.34%), and Africa (1.16%).

Network folders

The percentage of ICS computers on which threats are blocked in network folders is steadily decreasing. In Q1 2026, it was the lowest for the period under review, at 0.029%.

Regionally, the percentage ranged from 0.005% in Northern Europe to 0.135% in East Asia.

East Asia has traditionally led on this parameter by a wide margin. The percentage figure for East Asia is 27 times higher than the lowest regional value (recorded in Northern Europe).

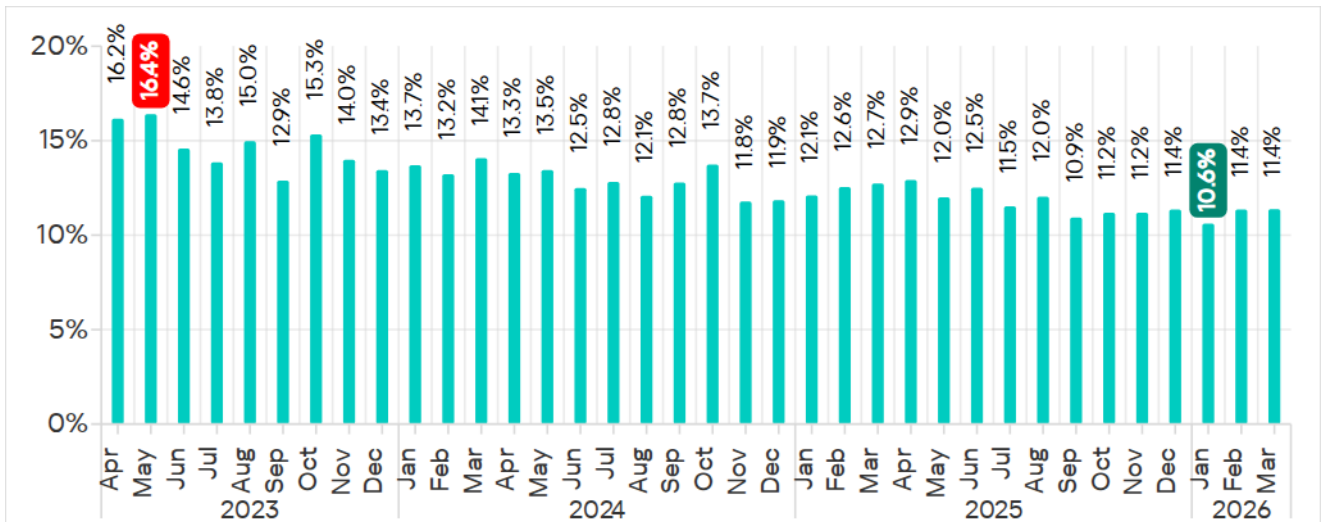
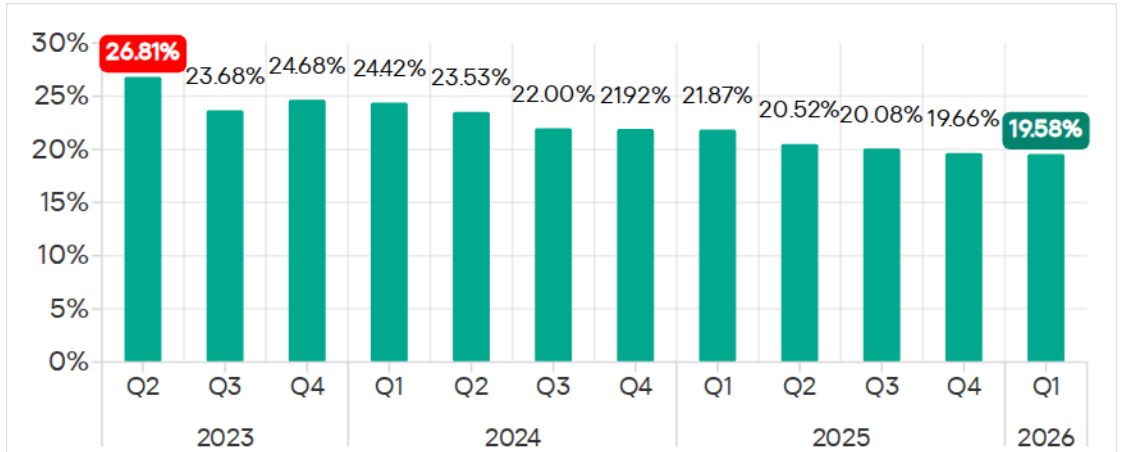
The largest increases in the percentage figures for threats from network folders were observed in Africa and South America.

Among the selected industries across all regions, the top positions in the ranking by the percentage of ICS computers on which threats are blocked in network folders are held by industries in East Asia (which is not unexpected, given the overall percentage figure for network folders in the region). The highest value is in the construction industry (0.36%).

Statistics across all threats

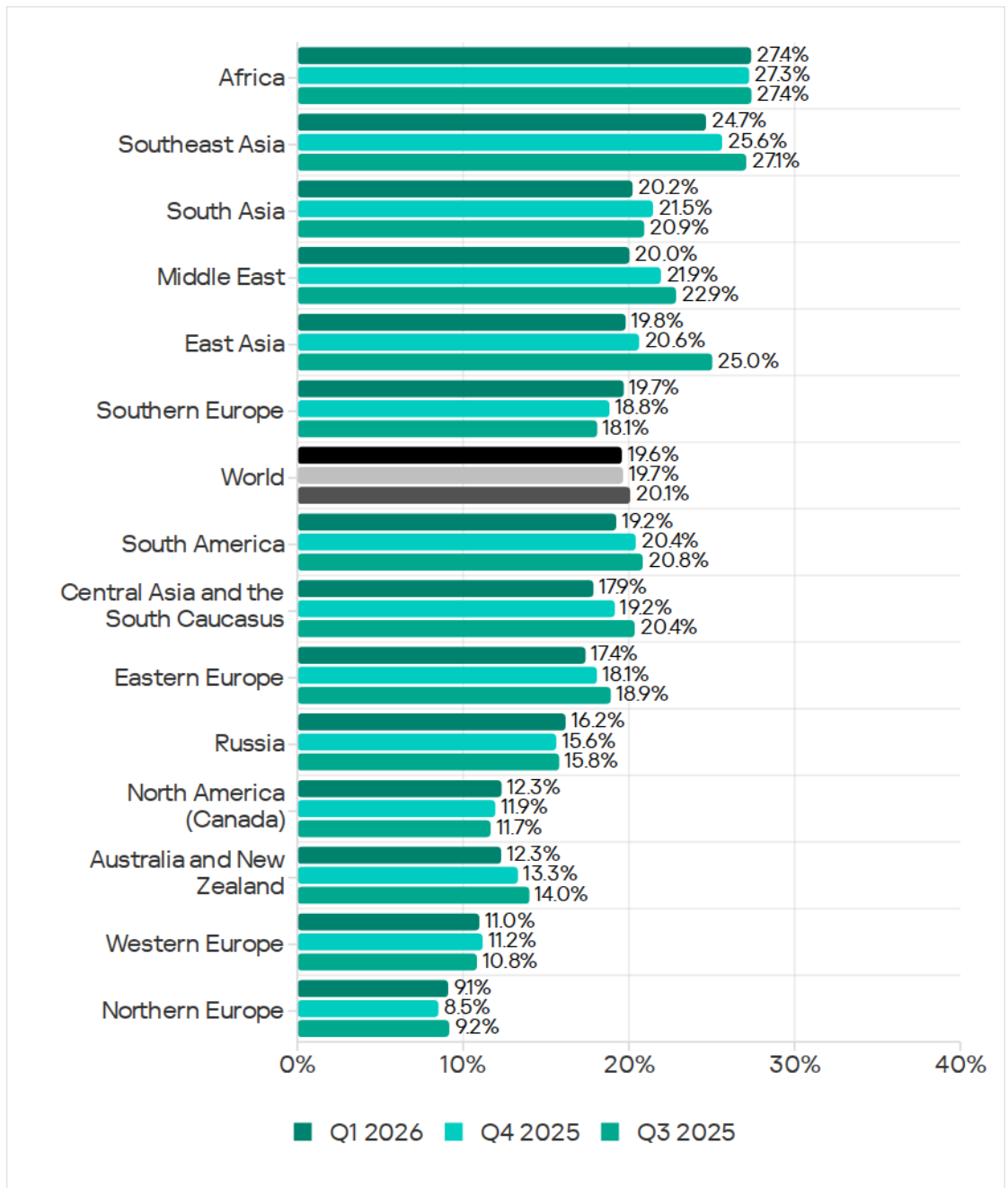
All threats

Percentage of ICS computers on which malicious objects were blocked, Q2 2023 – Q1 2026

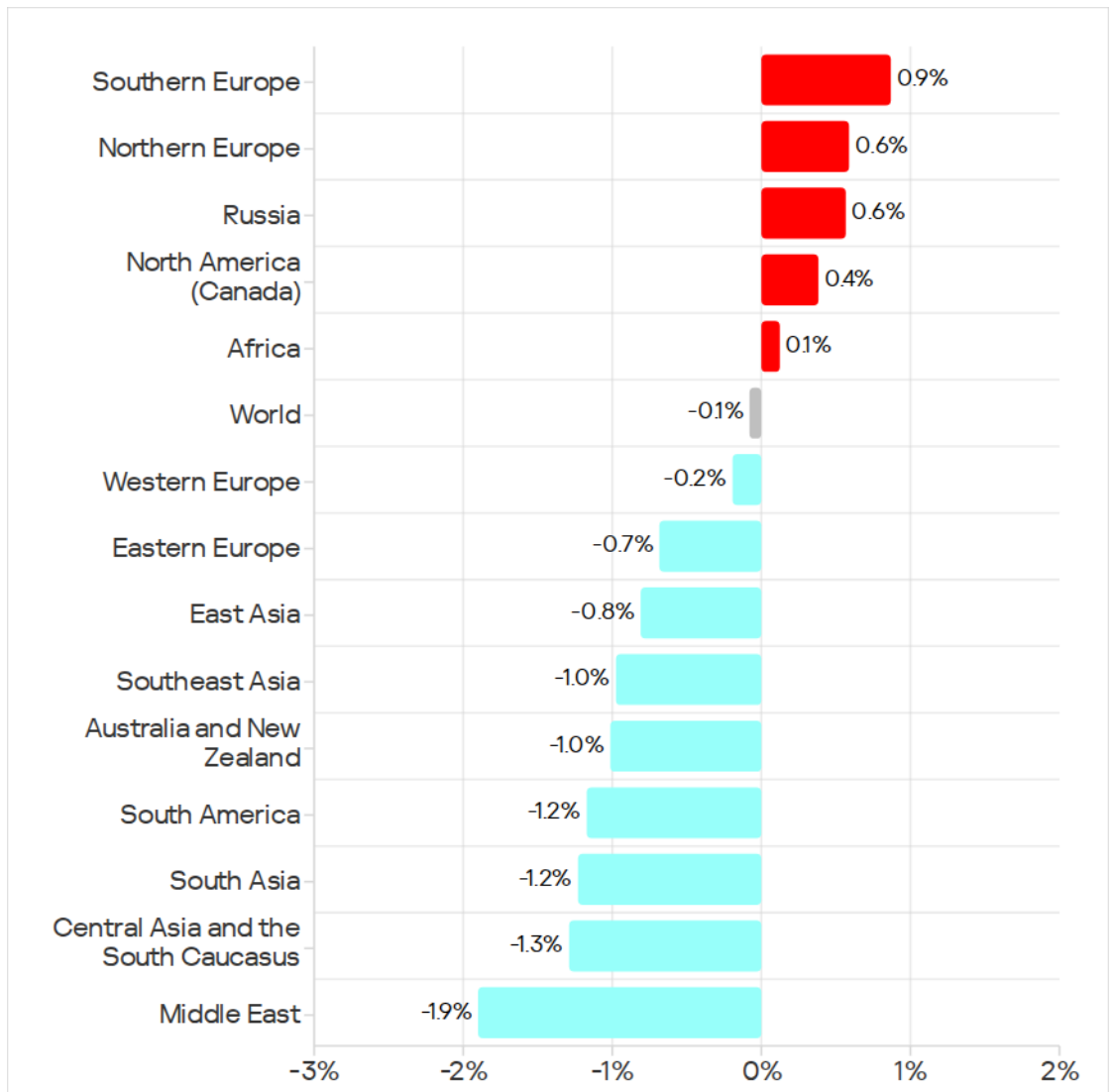


Percentage of ICS computers on which malicious objects were blocked, April 2023 – March 2026

Regions ranked by percentage of attacked ICS computers

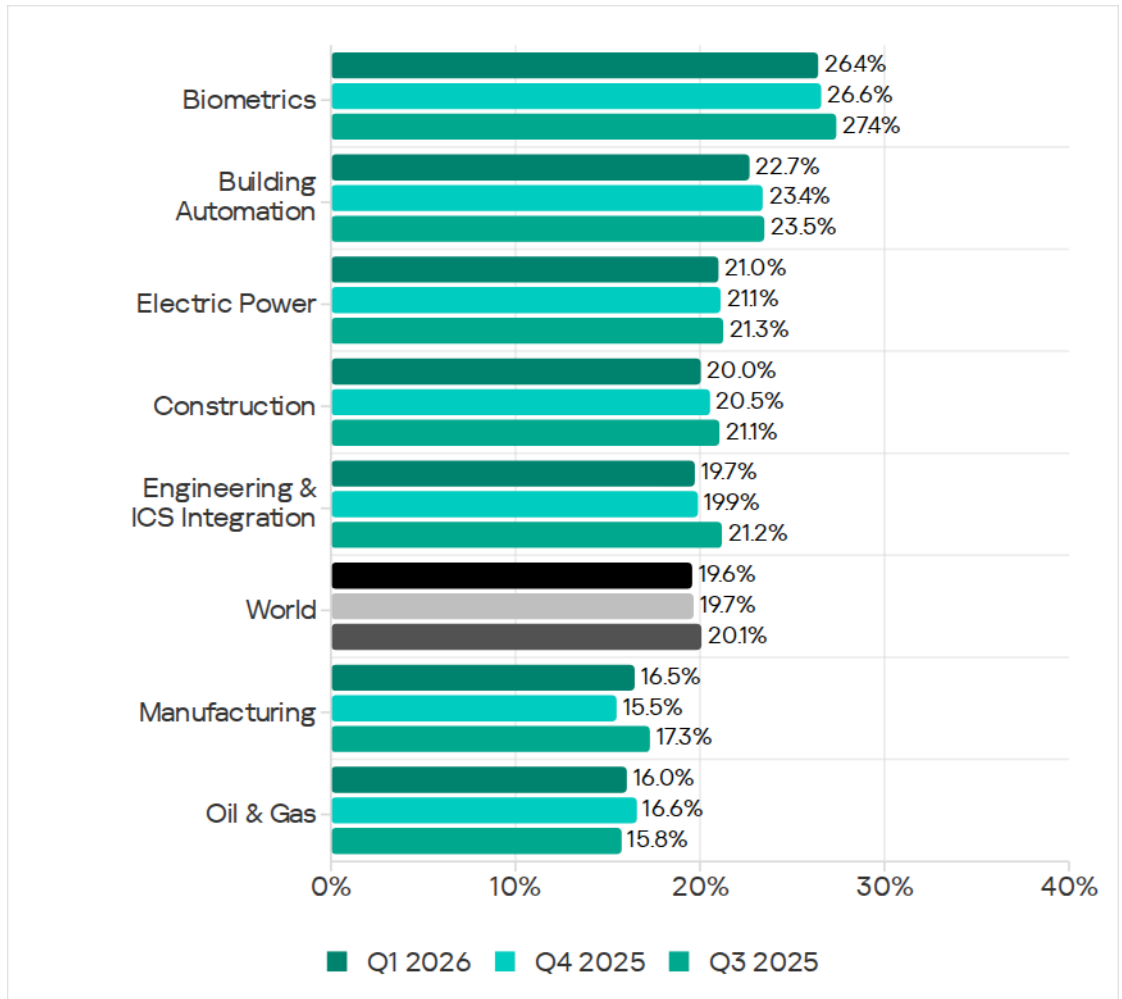


Changes in percentage of ICS computers on which malicious objects were blocked, Q1 2026

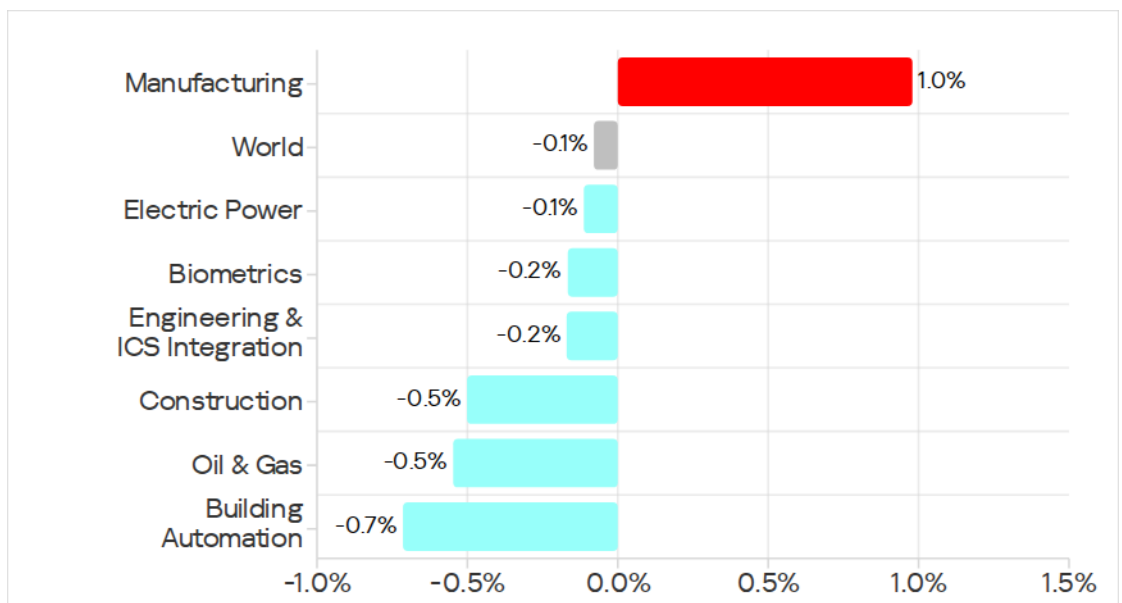


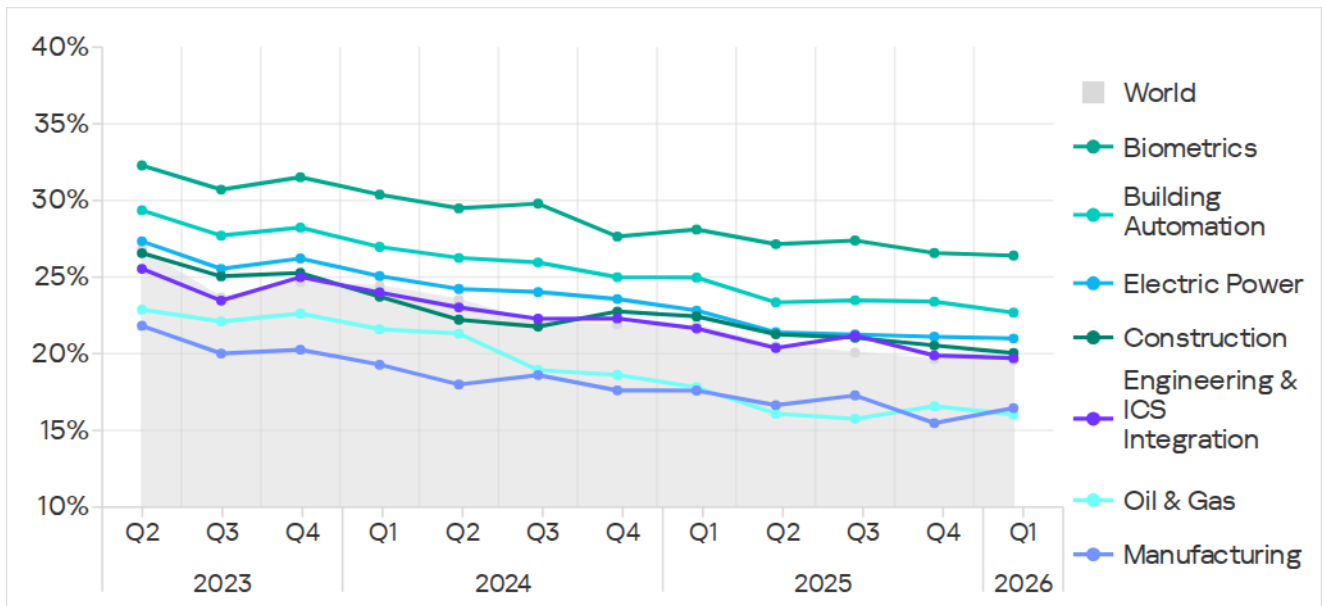
Selected industries

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



Changes in percentage of ICS computers on which malicious objects were blocked in selected industries, Q1 2026





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

Threat sources and malware categories in selected industries

We use heat maps when assessing the challenges across industries. Colors on the heat map indicate an indicator's position in the global industry ranking by threat category or threat source. The color red indicates that the value is close to the maximum. Yellow highlights the highest values across industries for a specific threat category or threat source.

Threat source indicators by industry (global), Q1 2026

Industry / Threat source	Biometrics	Building Automation	Electric Power	Construction	Engineering & ICS Integration	Manufacturing	Oil & Gas	Category metric worldwide
Internet	8.49%	8.63%	9.46%	9.50%	8.78%	7.40%	6.22%	7.88%
Email clients	9.53%	5.32%	2.31%	2.55%	2.14%	2.06%	1.48%	2.59%
Removable media	0.27%	0.30%	0.47%	0.23%	0.26%	0.25%	0.41%	0.26%
Network folders	0.03%	0.04%	0.03%	0.04%	0.04%	0.02%	0.02%	0.03%
Industry metric worldwide	26.41%	22.69%	21.00%	20.05%	19.72%	16.46%	16.04%	

Threat category indicators by industry (global), Q1 2026

Industry / Threat type	Biometrics	Building Automation	Electric Power	Construction	Engineering & ICS Integration	Manufacturing	Oil & Gas	Category metric worldwide
Malicious scripts and phishing pages (JS and HTML)	13.38%	9.69%	7.09%	7.55%	6.66%	6.18%	4.77%	6.56%
Spy Trojans, backdoors and keyloggers	8.11%	5.44%	3.82%	3.30%	3.45%	2.62%	3.05%	3.73%
Denylisted internet resources	2.81%	3.42%	4.40%	3.74%	3.69%	2.95%	3.60%	3.54%
Malicious documents (MSOffice + PDF)	4.44%	3.10%	1.81%	1.46%	1.40%	1.20%	1.27%	1.56%
Worms	2.12%	1.81%	1.81%	1.11%	1.15%	1.21%	1.31%	1.33%
Viruses	1.69%	1.71%	1.87%	1.96%	1.29%	1.09%	1.07%	1.31%
Miners in the form of executable files for Windows	0.45%	0.59%	0.71%	0.69%	0.61%	0.44%	0.82%	0.59%
Malware for AutoCAD	0.09%	0.15%	0.33%	1.12%	0.31%	0.18%	0.29%	0.30%
Web miners running in browsers	0.27%	0.28%	0.40%	0.44%	0.29%	0.27%	0.45%	0.22%
Ransomware	0.27%	0.25%	0.20%	0.16%	0.13%	0.13%	0.21%	0.14%
Industry metric worldwide	26.41%	22.69%	21.00%	20.05%	19.72%	16.46%	16.04%	

Biometric systems rank highest across industries in terms of percentage figures for email threats. It is worth noting that, unlike in other industries, the percentage figure for threats from email clients in biometric systems exceeds that for threats from the internet.

Email is a source of malicious scripts and malicious documents. Following a malicious link in an email or opening an attachment from a phishing email can cause the computer to become infected with spyware. Spyware, in turn, can be used (among other things) to steal information needed to deliver other types of malware, such as ransomware.

Biometric systems lead in all of these malware categories – malicious scripts, malicious documents, spyware, and ransomware. They also rank first in the worms category.

The electric power industry ranks first based on the percentage of ICS computers on which threats are blocked when connecting removable media, and second in the category of worms (which are distributed primarily via removable media).

Threats from the internet are also relevant to this industry, and the percentage figure for the electric power sector for this threat source is close to the maximum across all industries. At the same time, the electric power sector ranks first in terms of denylisted internet resources.

The construction industry ranks first in terms of threats from the internet and second for the percentage of ICS computers on which denylisted internet resources are blocked.

The industry also ranks first in terms of threats from network folders. Network folders are the main distribution channel for viruses and AutoCAD malware. The construction industry also ranks first in these threat categories.

The oil and gas industry, which ranks lowest among the selected industries in the percentage of ICS computers attacked, is in first place for both web miners and miners in the form of executable files.

Threat categories

Attacks blocked within an ICS network are typically multi-step sequences of malicious operations, in which each subsequent step by attackers is designed to gather additional information, elevate privileges, and/or gain access to other systems by exploiting security issues existing in industrial enterprises, including their OT infrastructures.

Malicious objects blocked by Kaspersky products on ICS computers can be divided into three groups based on their distribution methods and purposes.

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.
This typically includes spyware, ransomware, miners in the form of executable files for Windows, and web miners.
3. Self-propagating malware.
This category includes worms and viruses.

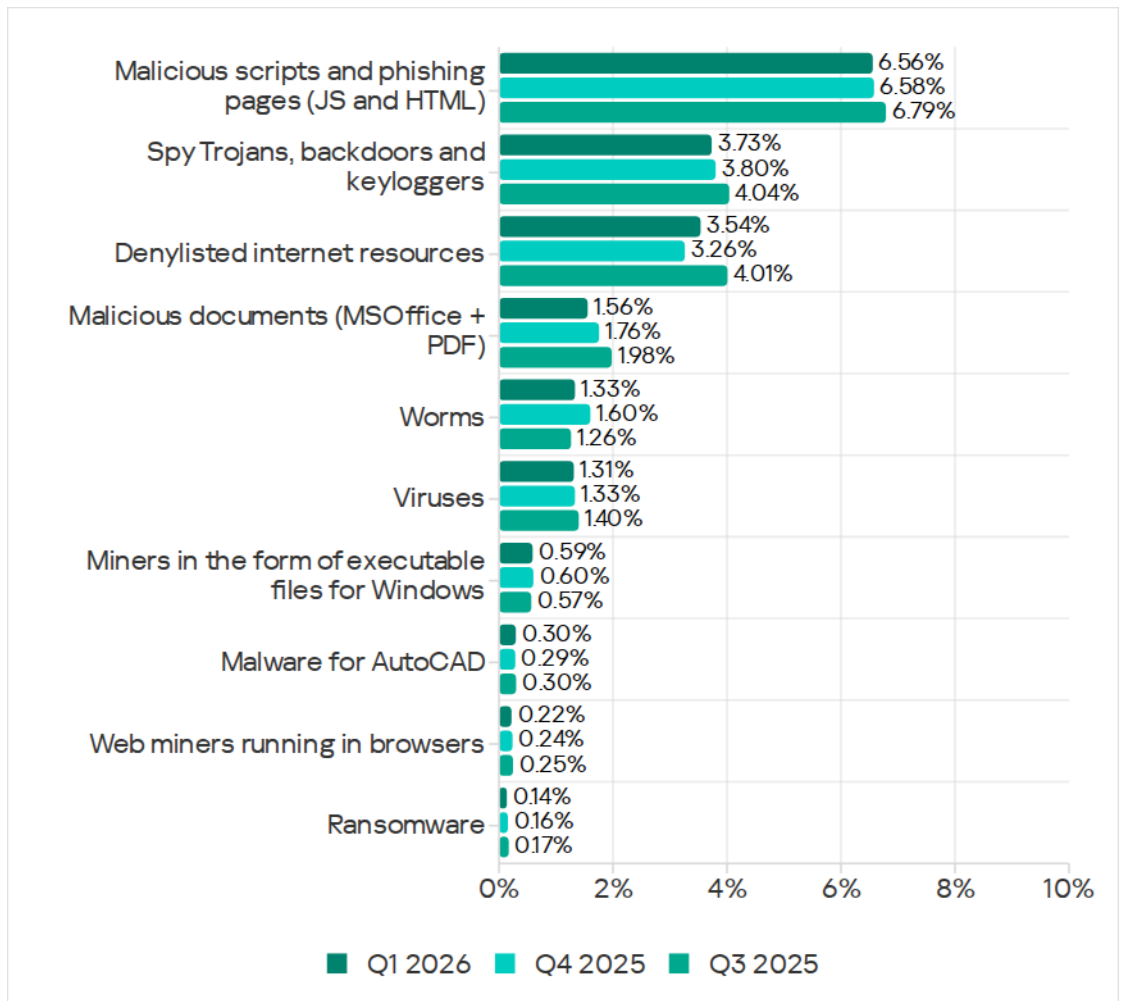
Malware for AutoCAD is not grouped by distribution method, as it can spread in various ways.

Attackers extensively use malicious objects designed for the initial infection of ICS computers, so security solutions block these objects more often than other groups. Our statistics reflect this: globally and in almost all regions, malicious scripts and phishing pages, as well as denylisted internet resources, rank at the top of threat category rankings by the percentage of ICS computers on which they were blocked.

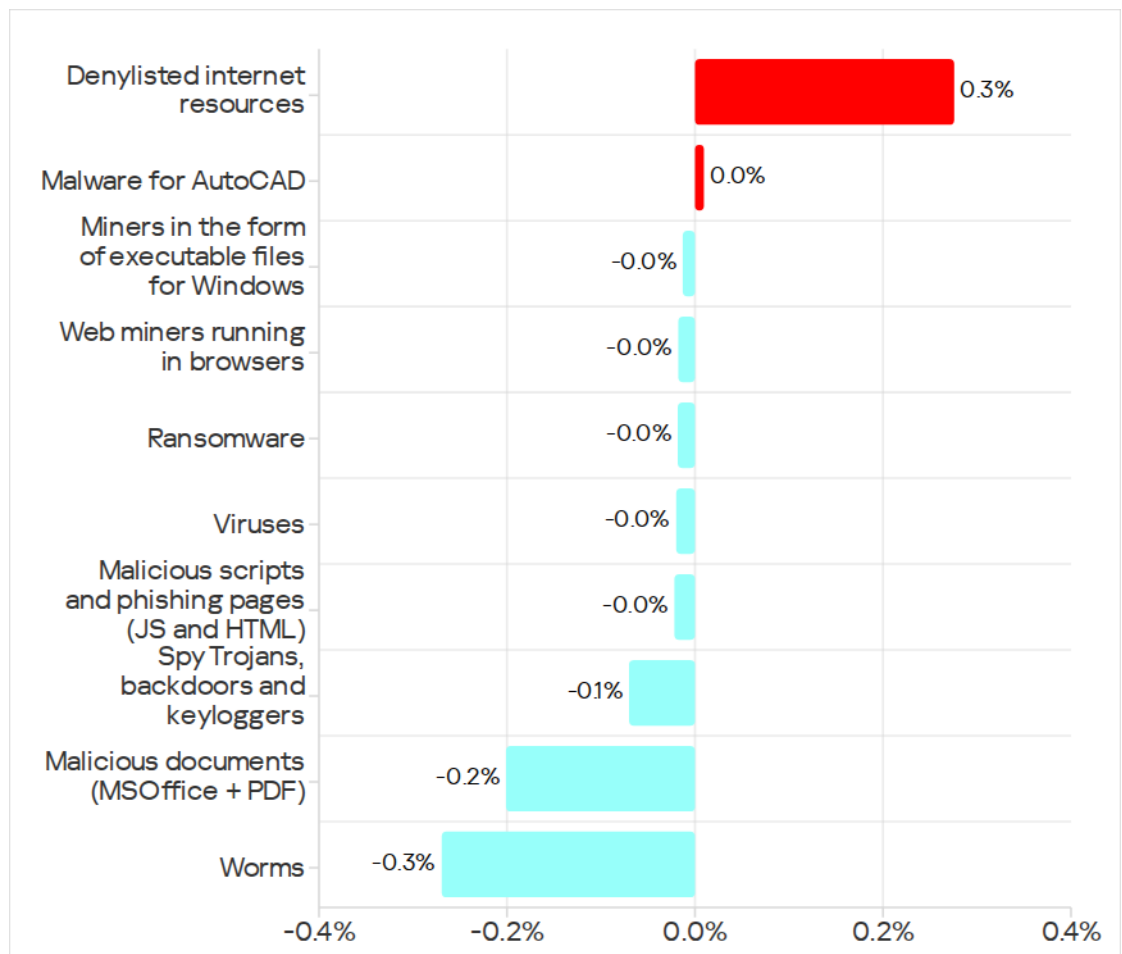
It should be noted that, in a small percentage of cases, the threat categories that we classify as malicious objects used for initial infection, such as malicious links, can also be used in subsequent stages of an attack. For example, a link to a malicious resource may sometimes be detected while scanning the system registry on a computer, where it evidently appeared as a result of activity by another malicious program, before that malware was identified and blocked. A stricter classification of attacked ICS computers based on the categories of malware blocked and the sources of infection is described in our article, [“Dynamics of external and internal threats to industrial control systems”](#), which opens a new series of publications presenting the results of deeper research on the ICS threat landscape based on statistics on when different components of our security products were triggered.

It is worth noting that the techniques used to deploy malware online 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 retrieved. In practice, this means that protection of an ICS network (like any other) should rely on the entire stack of protection technologies, not just protection of the network perimeter.

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



Changes in percentage of ICS computers on which malicious objects from different categories were blocked, Q1 2026



Malicious objects used for initial infection

Denylisted internet resources

The denylist of internet resources is used to prevent initial infection attempts. It helps block mainly the following objects on ICS computers:

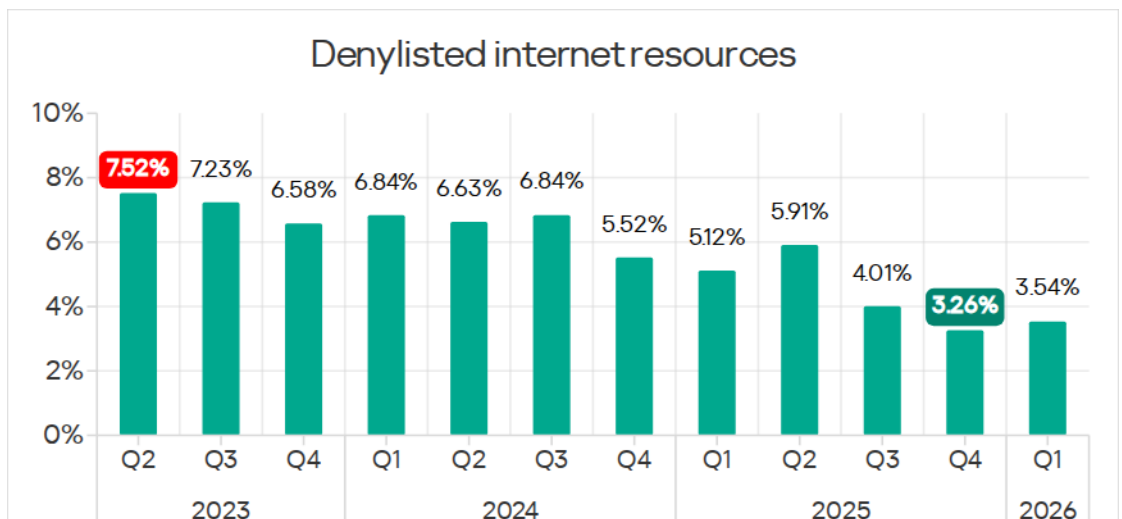
- Known malicious URLs and IP addresses used by threat actors to host payloads and configurations.
- Suspicious (insecure) web resources with entertainment and gaming content, often used to deliver unwanted software, cryptocurrency miners, and malicious scripts.
- CDN nodes used by attackers to distribute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

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

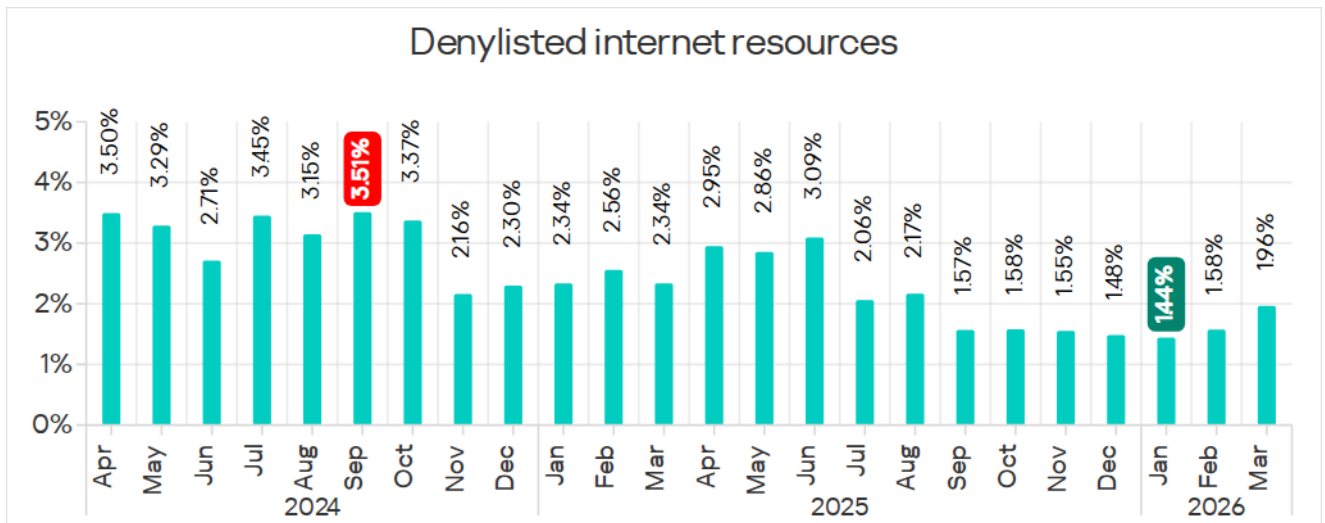
A detected malicious web resource may not always be easily added to a denylist because attackers are increasingly using legitimate internet resources and services, such as content delivery network (CDN) platforms, messengers, repositories, and cloud storage. These services allow malicious code to be distributed via 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 they are needed extremely rarely 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, and this access is frequently used), 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 emails and social media messages).

Percentage of ICS computers on which denylisted internet resources were blocked, Q2 2023 – Q1 2026



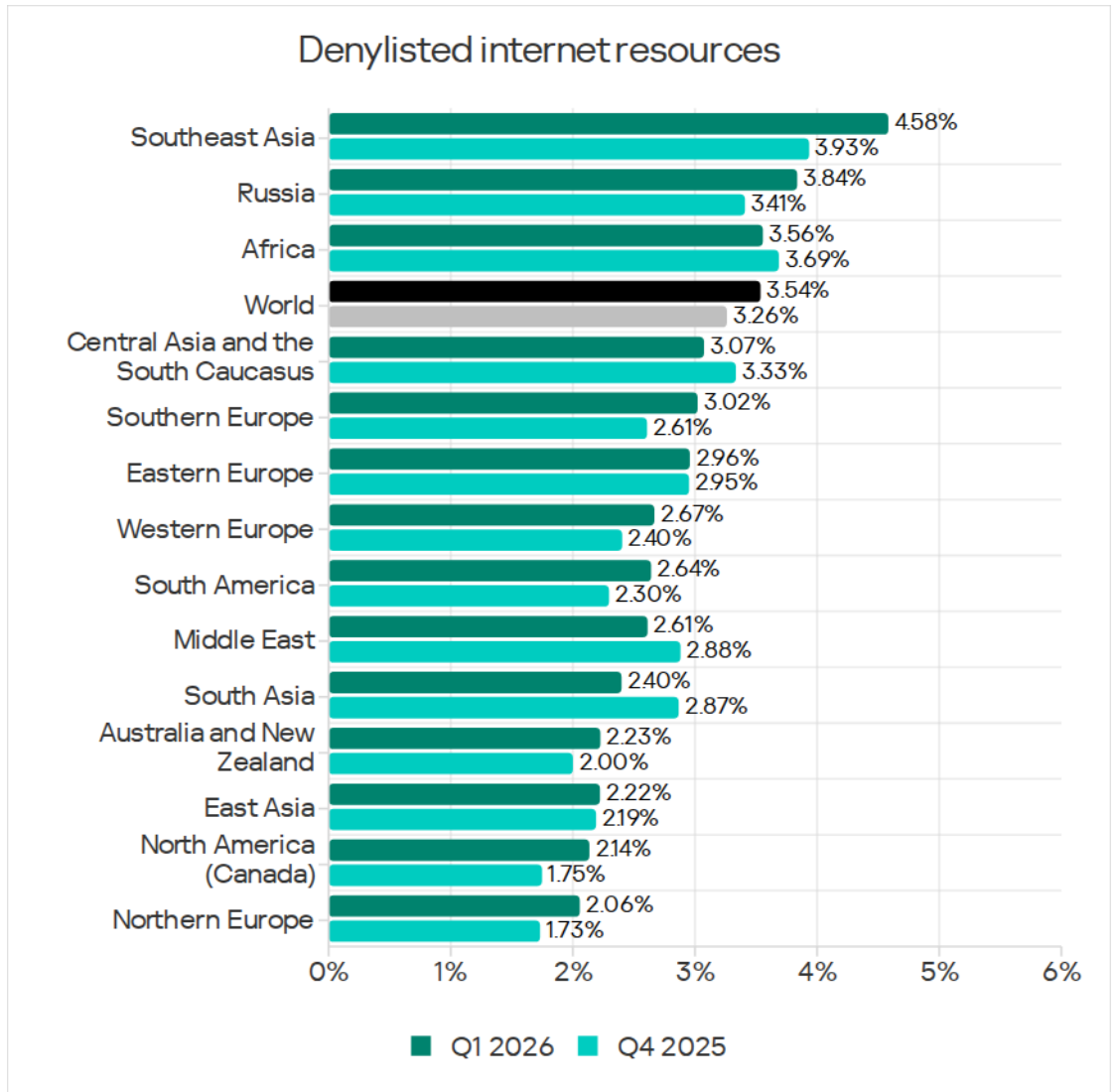
In January 2026, the percentage of ICS computers on which denylisted internet resources were blocked was the lowest in two years.



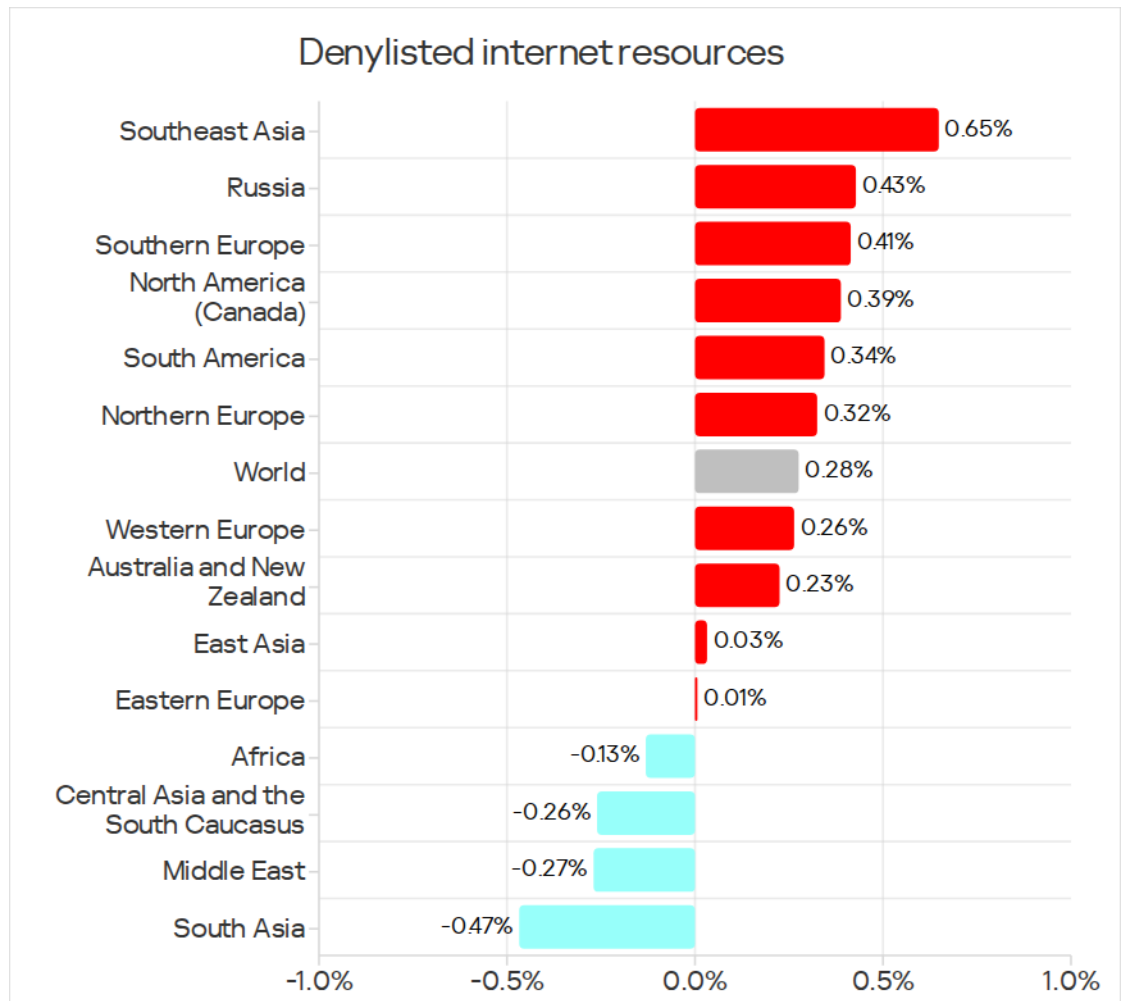
Percentage of ICS computers on which denylisted internet resources were blocked, April 2024 – March 2026

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 and has remained there for three quarters.

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



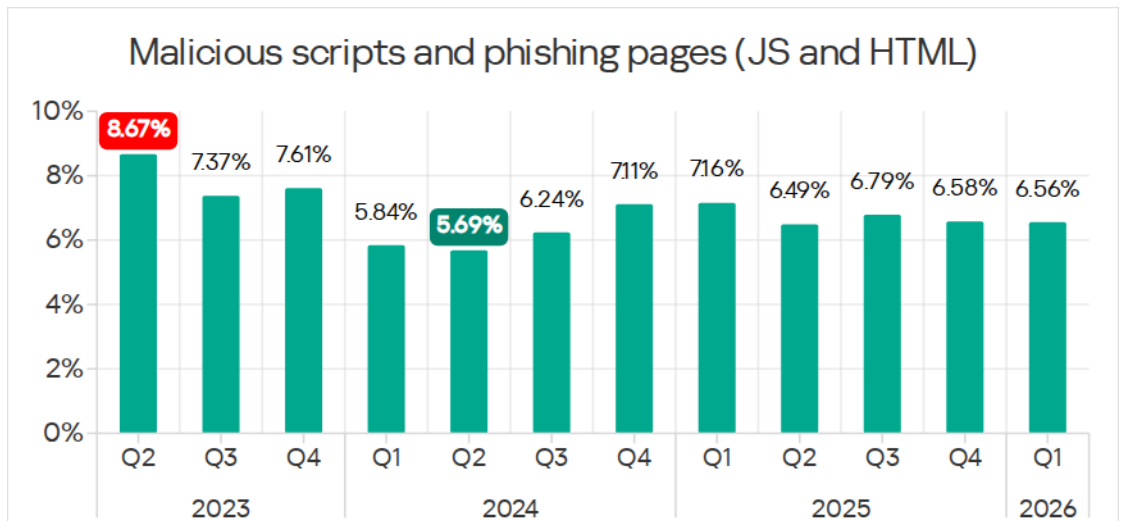
Changes in percentage of ICS computers on which denylisted internet resources were blocked, Q1 2026



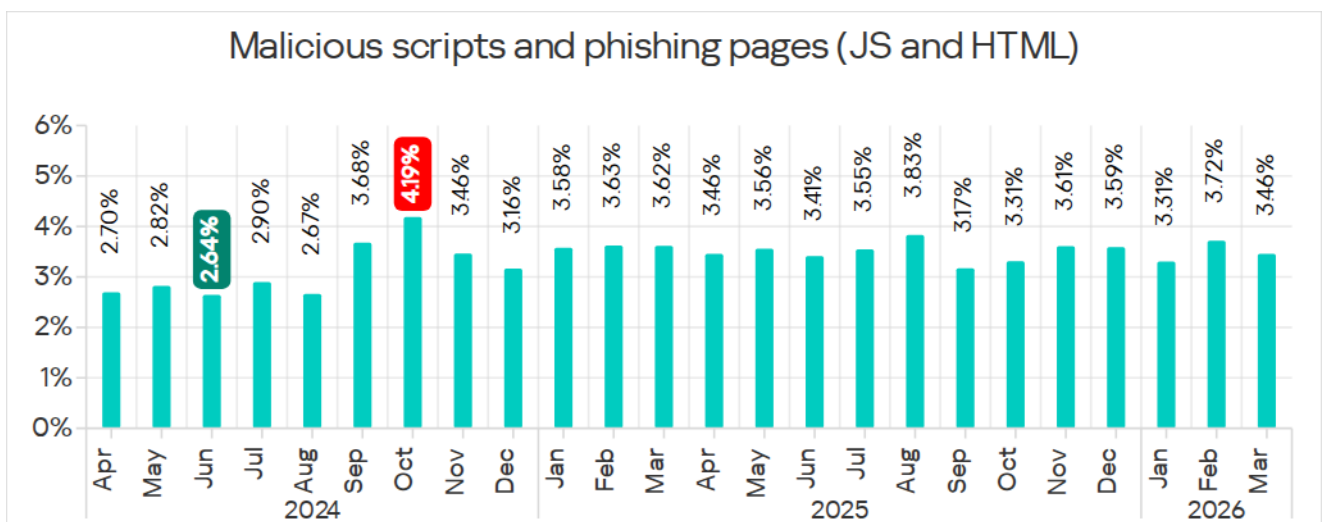
Malicious scripts and phishing pages (JS and HTML)

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

Percentage of ICS computers on which malicious scripts and phishing pages were blocked, Q2 2023 – Q1 2026

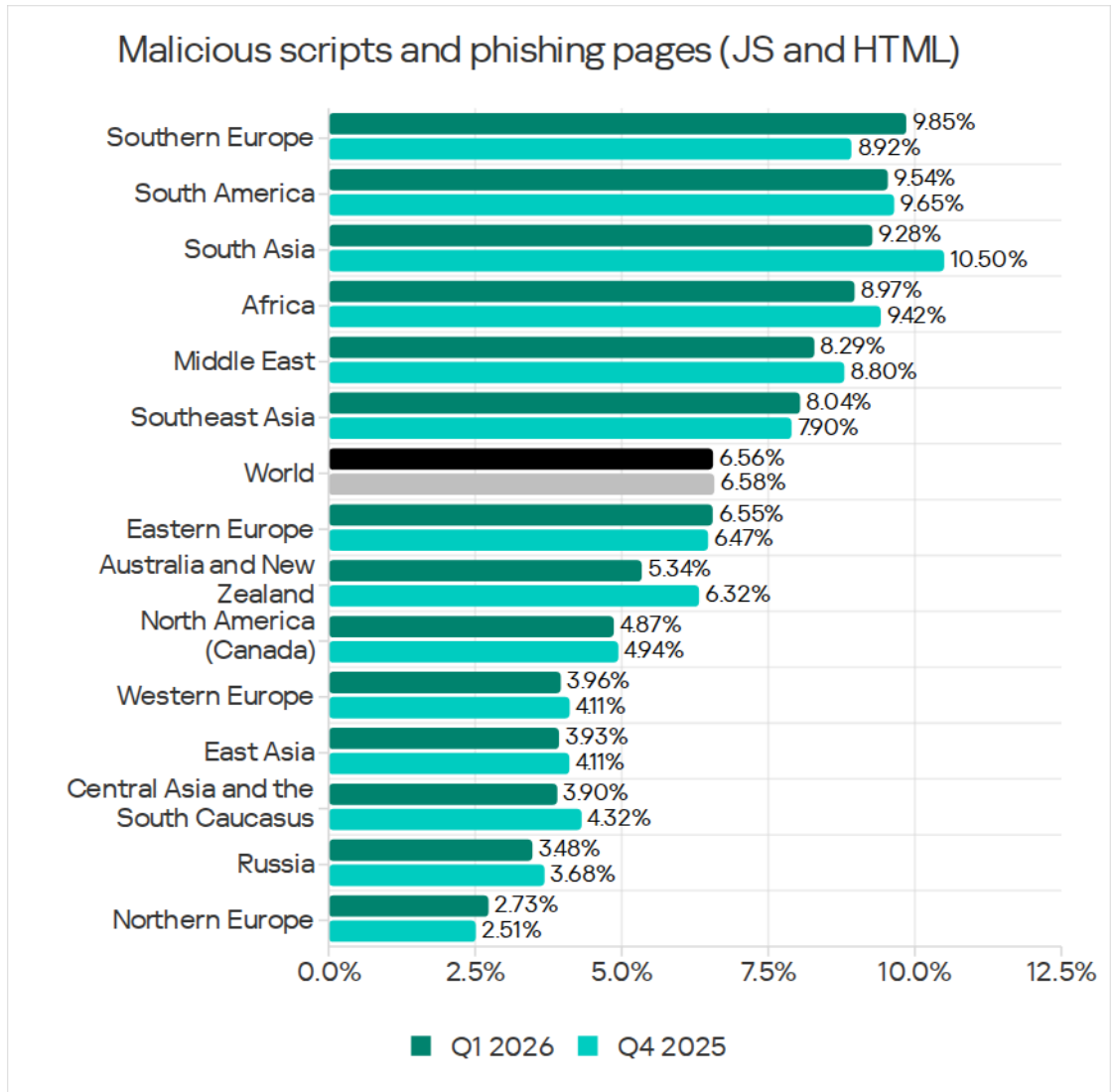


In Q1 2026, the monthly percentage figure was the highest in February. Its value exceeded those of the previous five months.

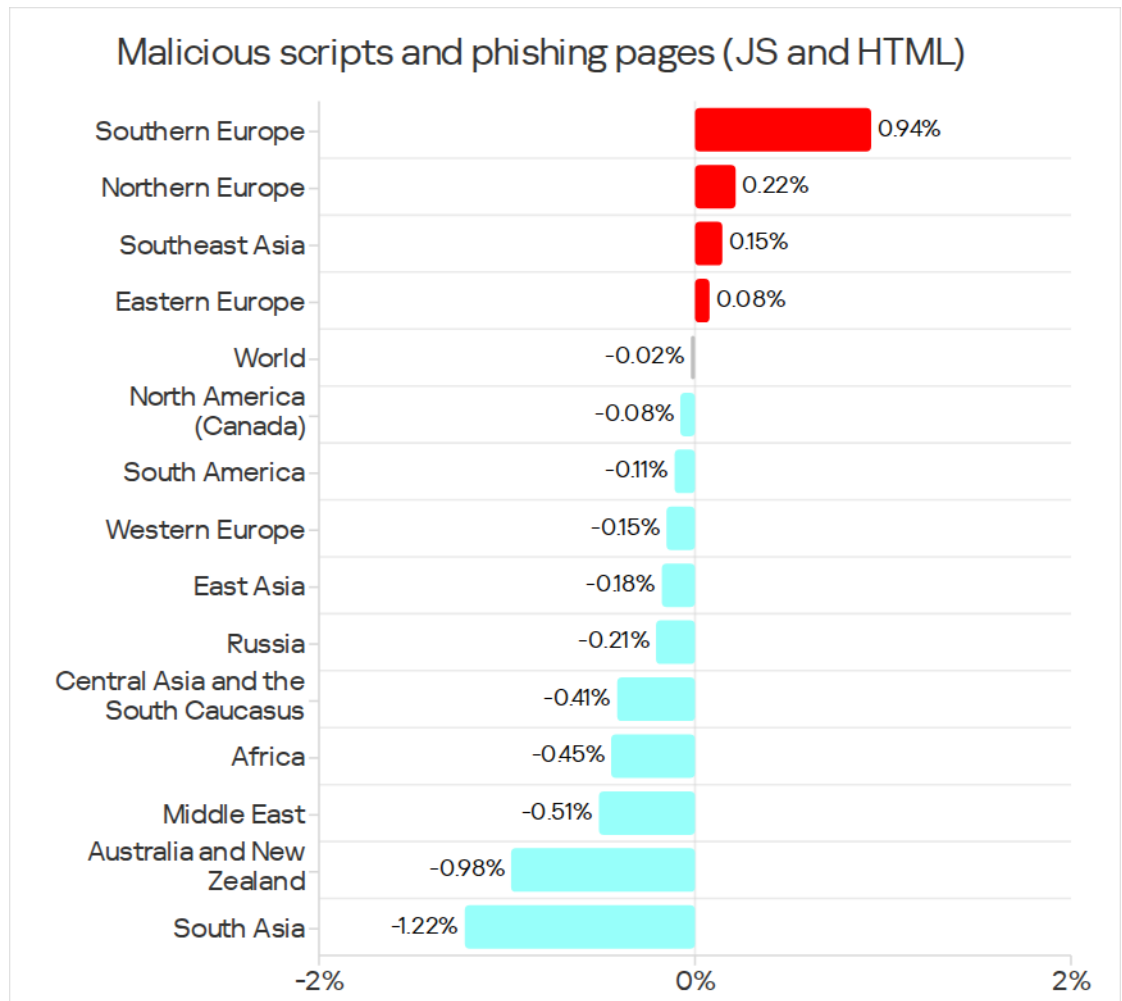


Percentage of ICS computers on which malicious scripts and phishing pages were blocked, April 2024 – March 2026

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



Changes in percentage of ICS computers on which malicious scripts and phishing pages were blocked, Q1 2026

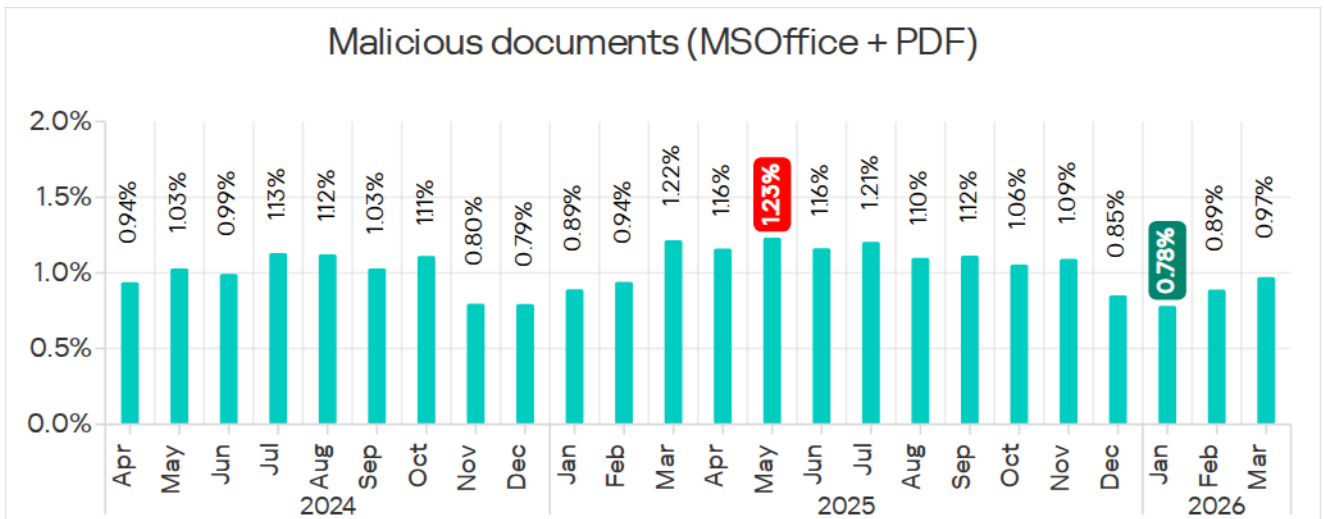
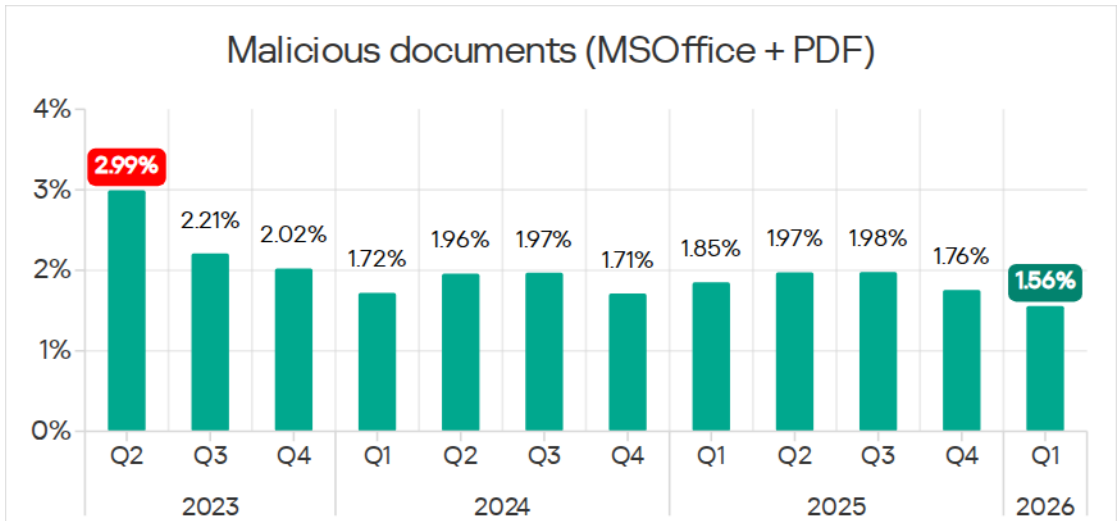


Malicious documents (MSOffice + PDF)

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

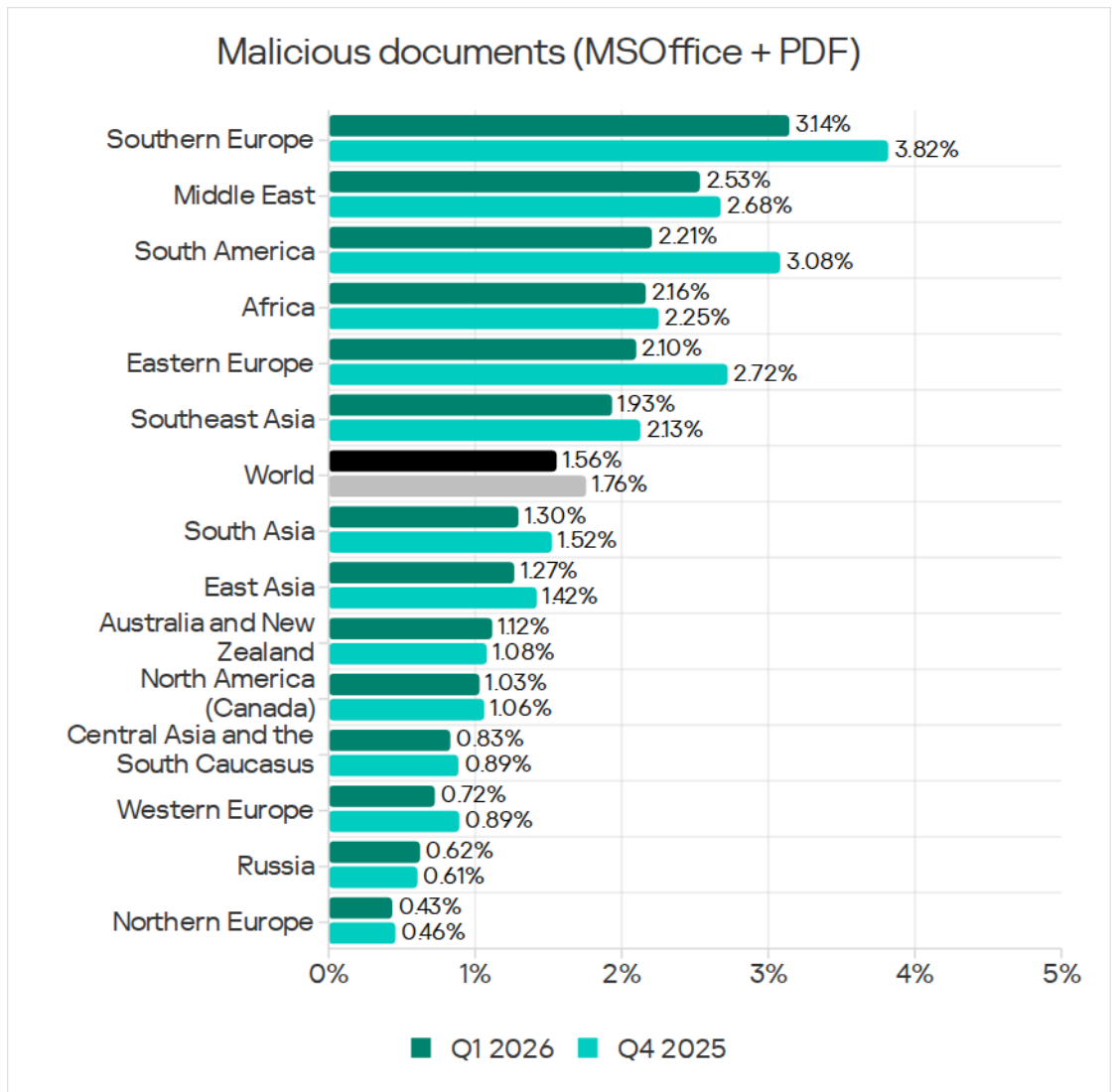
Malicious documents, especially those using zero-day exploits, remain a popular vector for targeted attacks. In 2025, CISA released more than 450 security advisories, many of which concerned file handling, including popular document formats.

Percentage of ICS computers on which malicious documents were blocked, Q2 2023 – Q1 2026

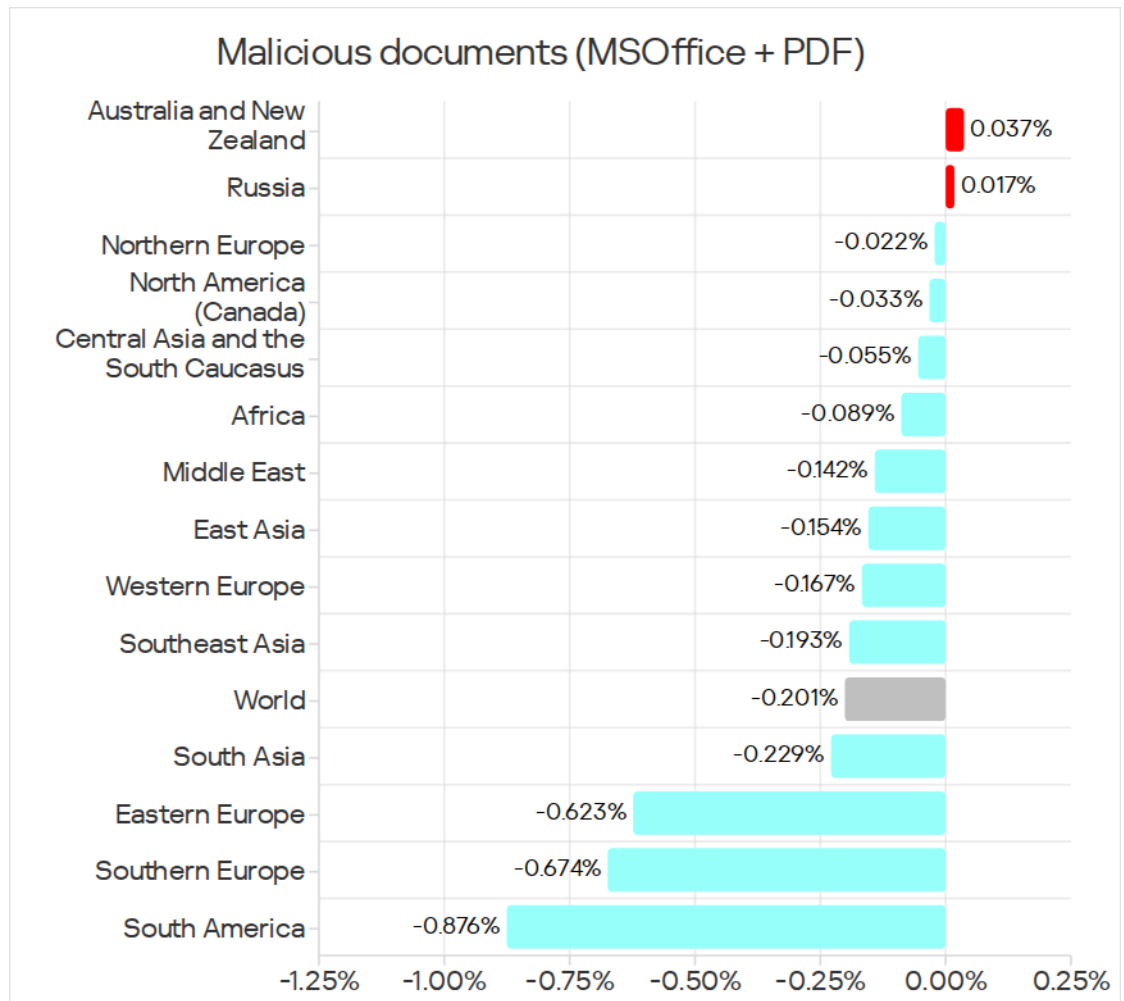


Percentage of ICS computers on which malicious documents were blocked, April 2024 – March 2026

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



Changes in percentage of ICS computers on which malicious documents were blocked, Q1 2026



Next-stage malware

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

Spyware

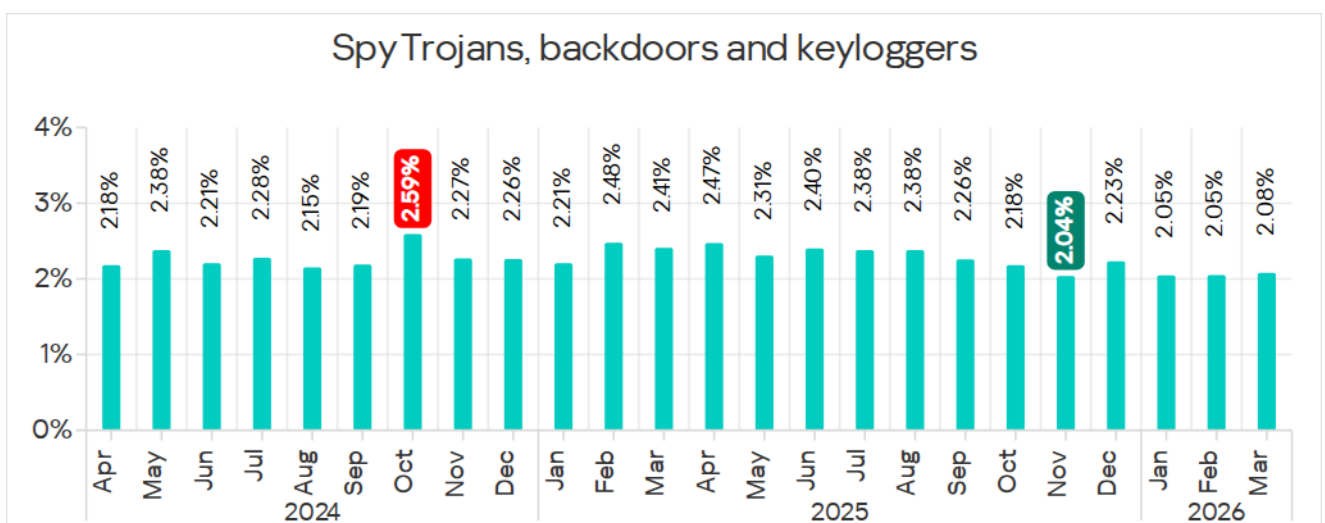
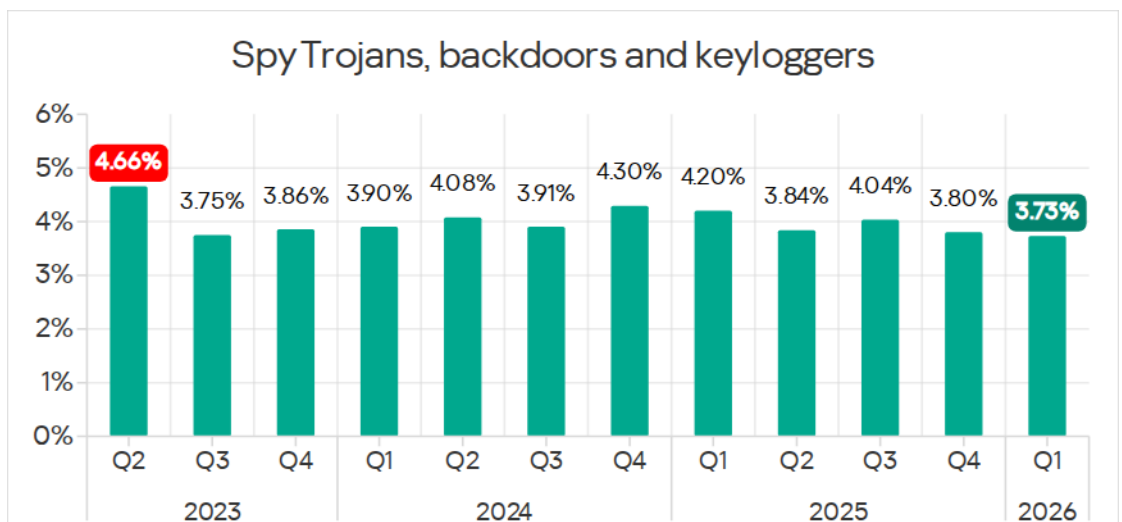
Spyware (spy Trojans, backdoors, and keyloggers) can be found in lots of phishing emails sent to industrial organizations. Spyware (Trojans, backdoors, and keyloggers) is the most frequently detected next-stage malware. It is used as a tool for the intermediate stages of a cyberattack (for example, reconnaissance and lateral movement) or in the final stage of the attack 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 information needed to deliver other types of malware, such as ransomware and silent cryptocurrency mining tools, and to prepare for targeted attacks.

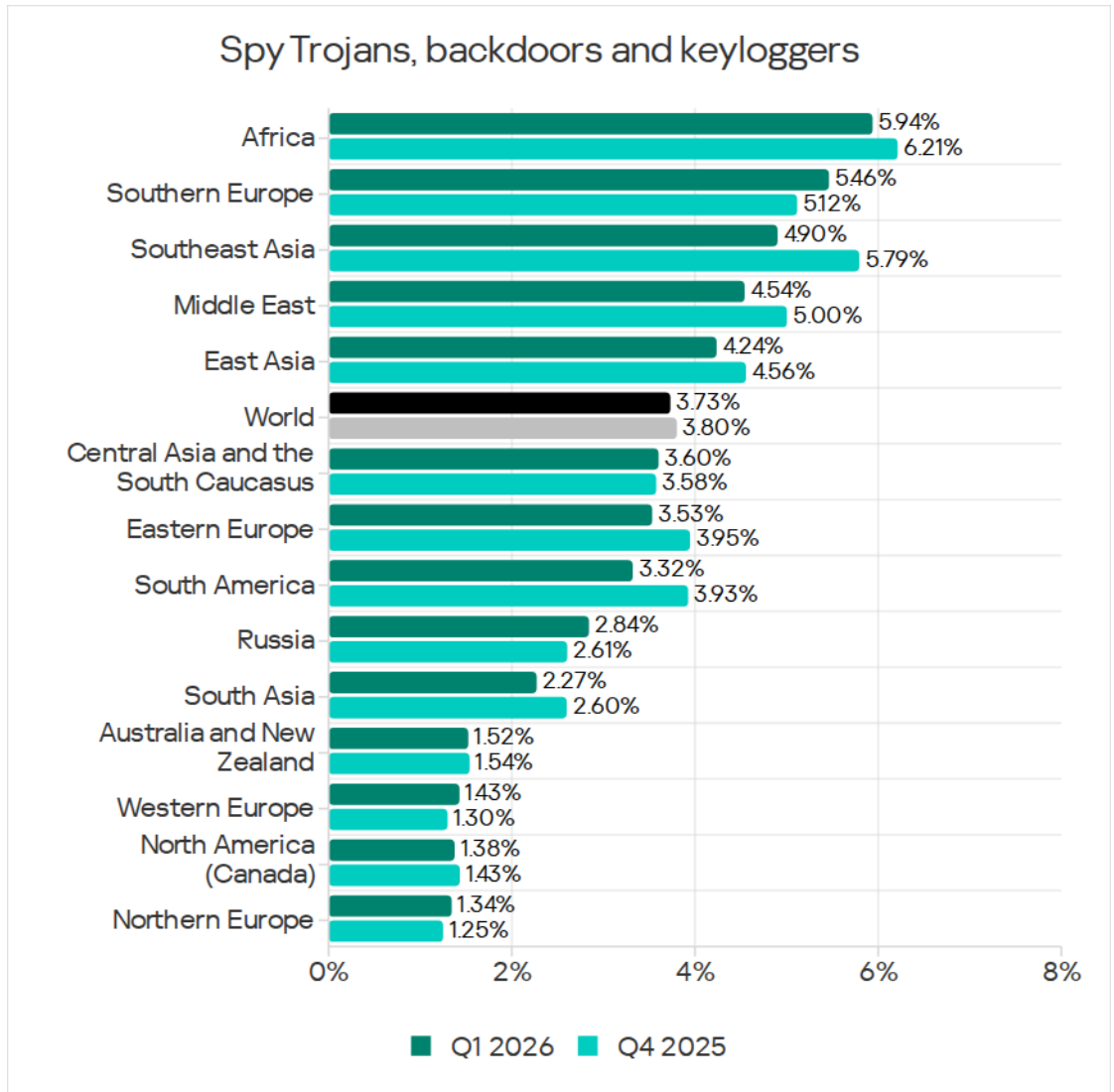
Detection of spyware on an ICS computer usually indicates that the initial infection vector succeeded, whether it was clicking on a malicious link, opening an attachment from a phishing email, or connecting an infected USB drive. This points to the absence or ineffectiveness of measures to protect the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

Percentage of ICS computers on which spyware was blocked, Q2 2023 – Q1 2026

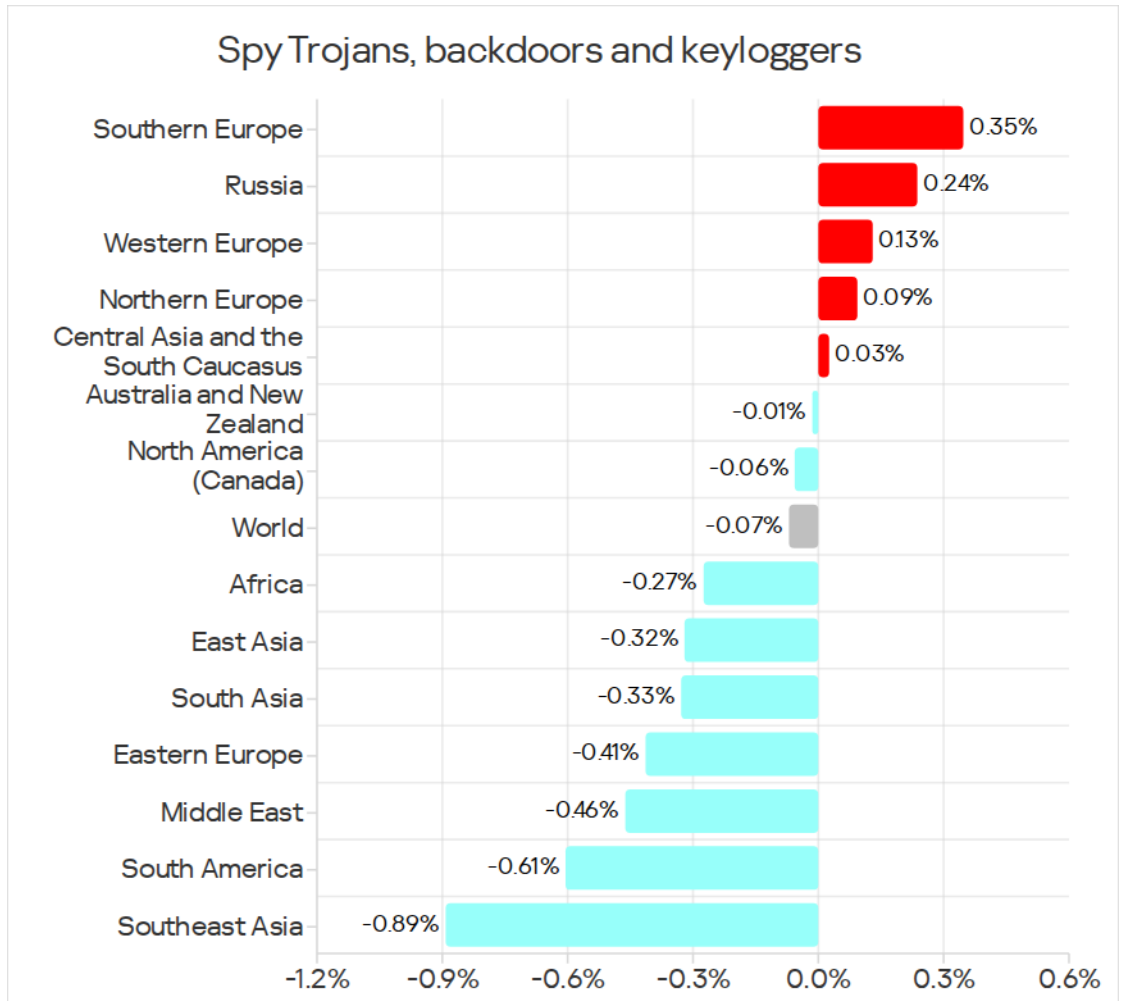


Percentage of ICS computers on which spyware was blocked, April 2024 – March 2026

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

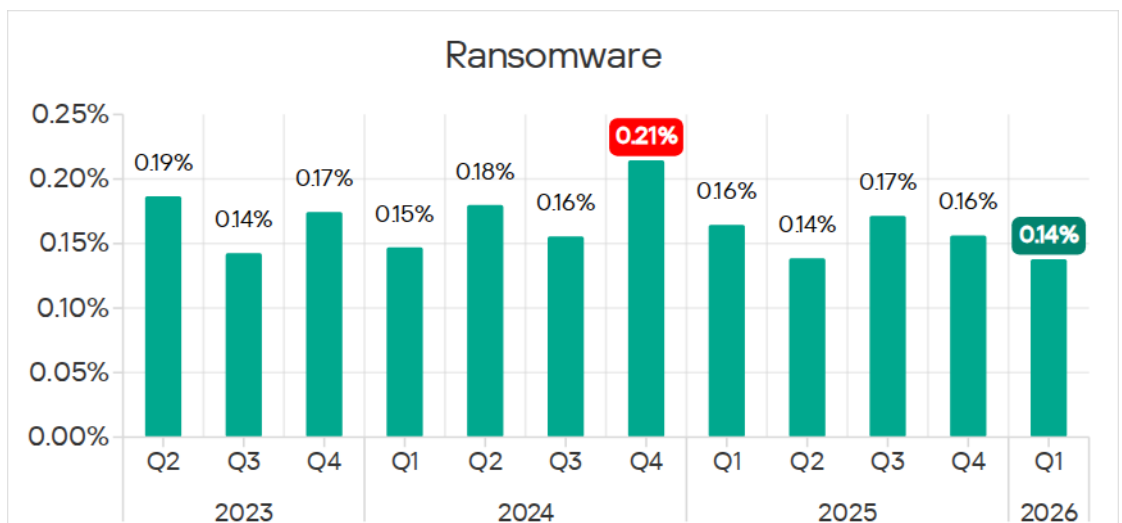


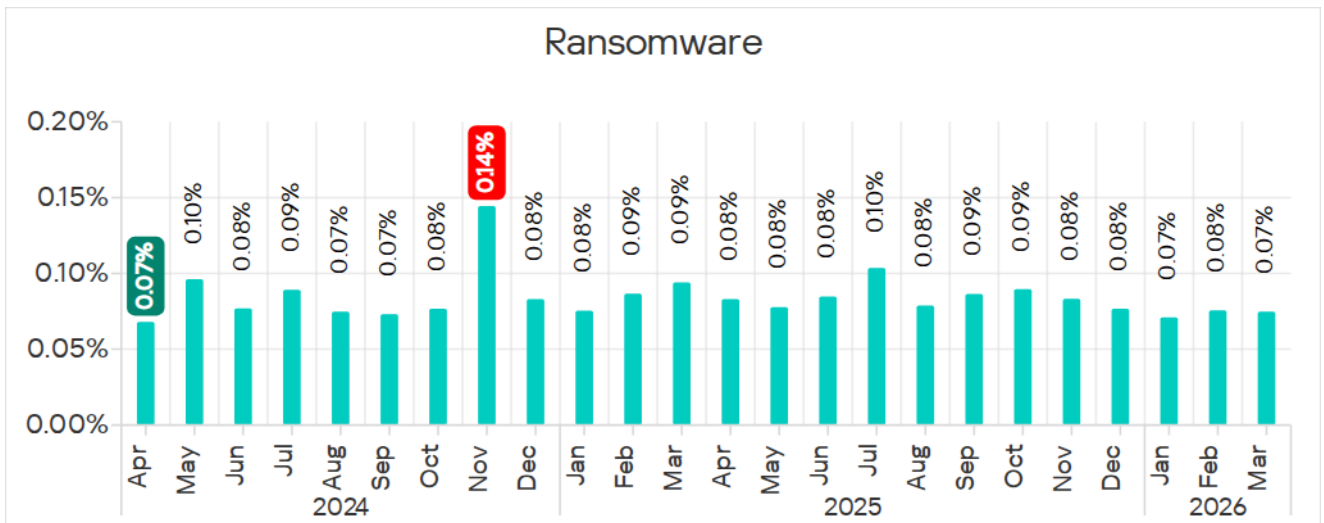
Changes in percentage of ICS computers on which spyware was blocked, Q1 2026



Ransomware

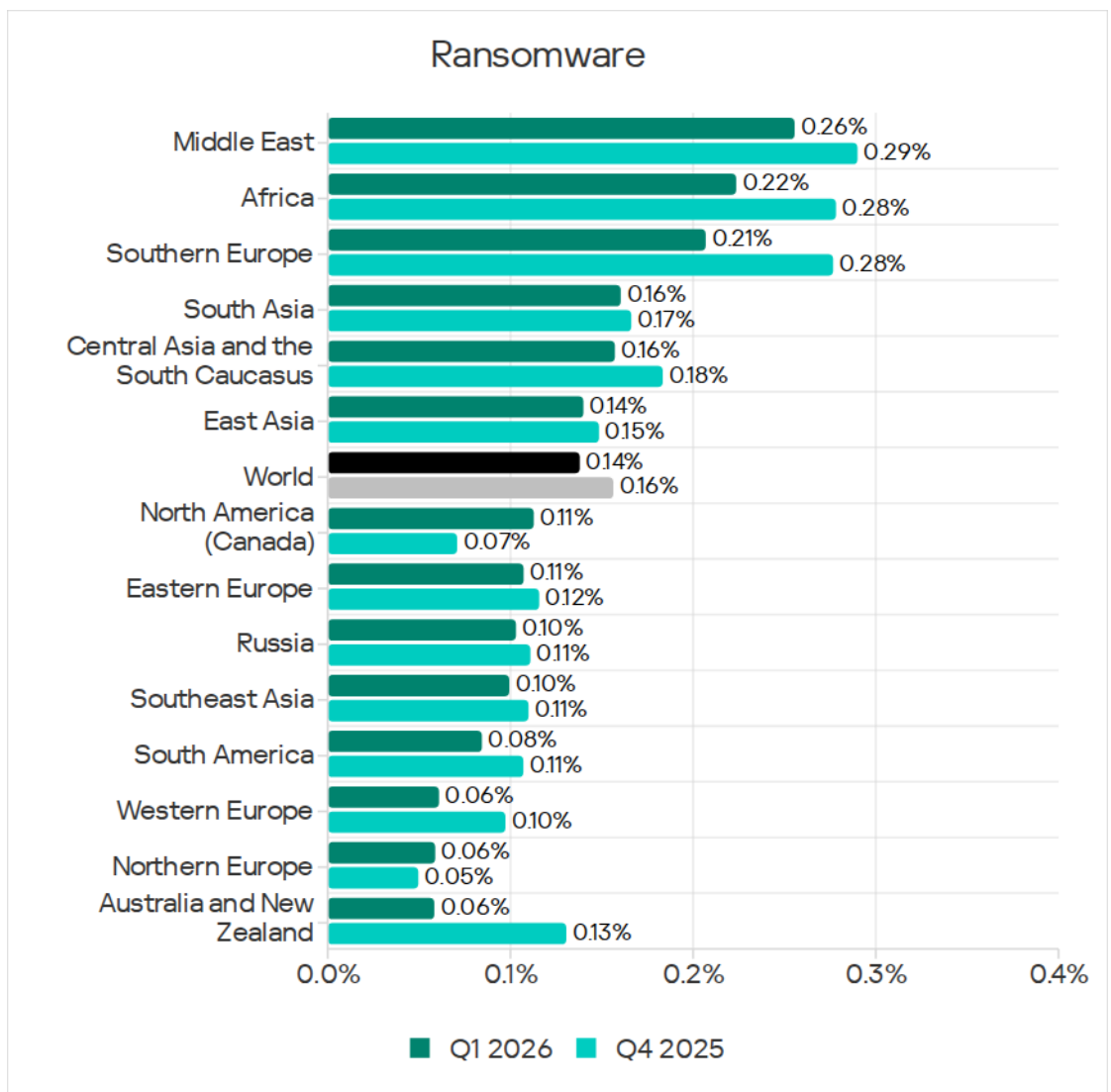
Percentage of ICS computers on which ransomware was blocked, Q2 2023 – Q1 2026



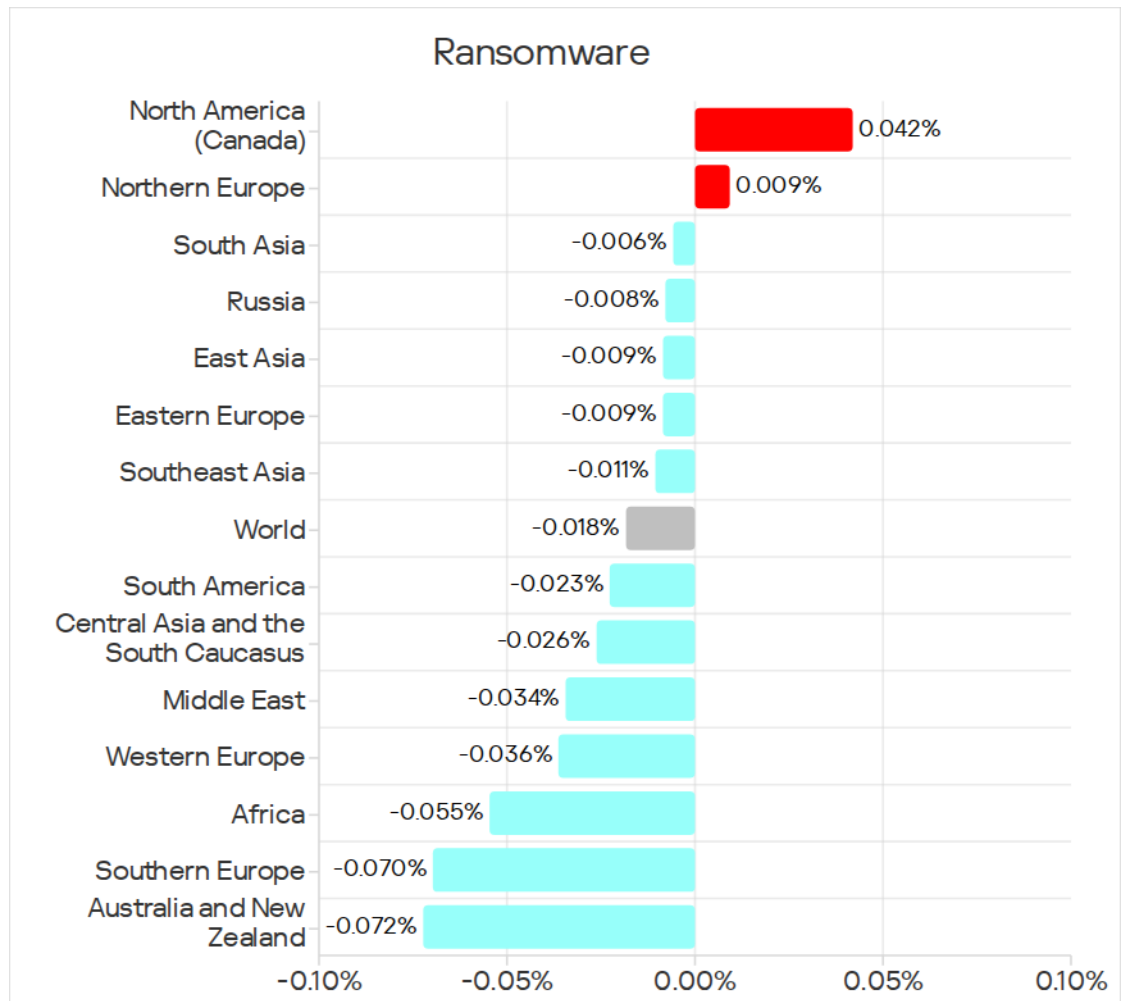


Percentage of ICS computers on which ransomware was blocked, April 2024 – March 2026

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



Changes in percentage of ICS computers on which ransomware was blocked, Q1 2026

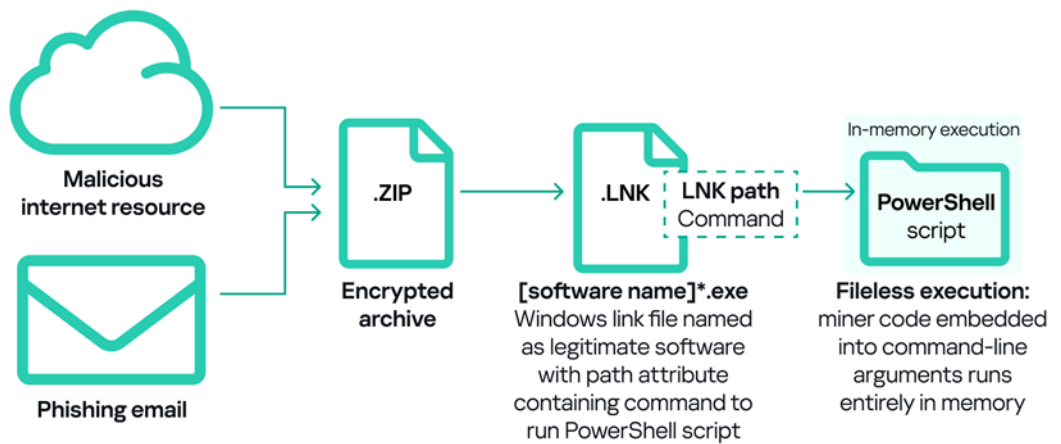


Miners in the form of executable files for Windows

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

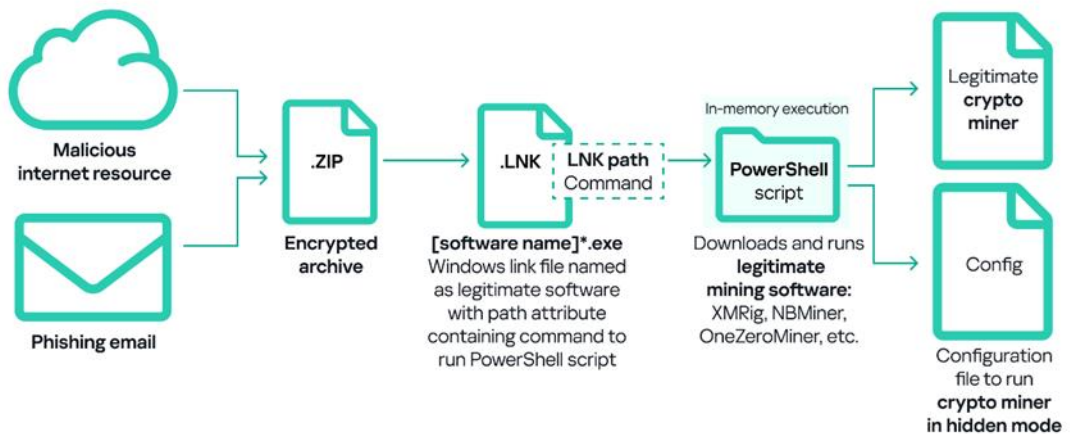
A significant portion of Windows miners found on ICS computers consists of archives with names that mimic legitimate software. These archives contain no actual software, but include a Windows LNK file, commonly known as a shortcut. However, the target (or path) that the LNK file points to is not a legitimate application but rather a command that can execute malicious code, such as a PowerShell script. Attackers increasingly use PowerShell, with malware code (including miners) embedded in the command line arguments and executed entirely in memory – that is, via fileless execution. The fileless execution of a miner makes it difficult for security tools to detect.

Kill chain example: fileless execution in cryptomining attacks

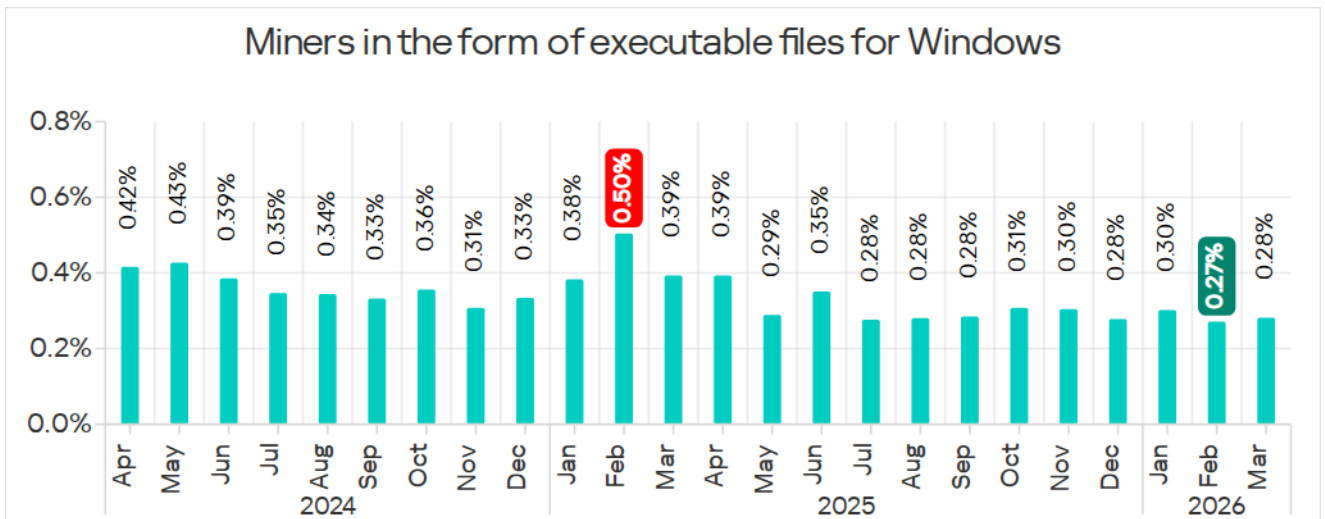
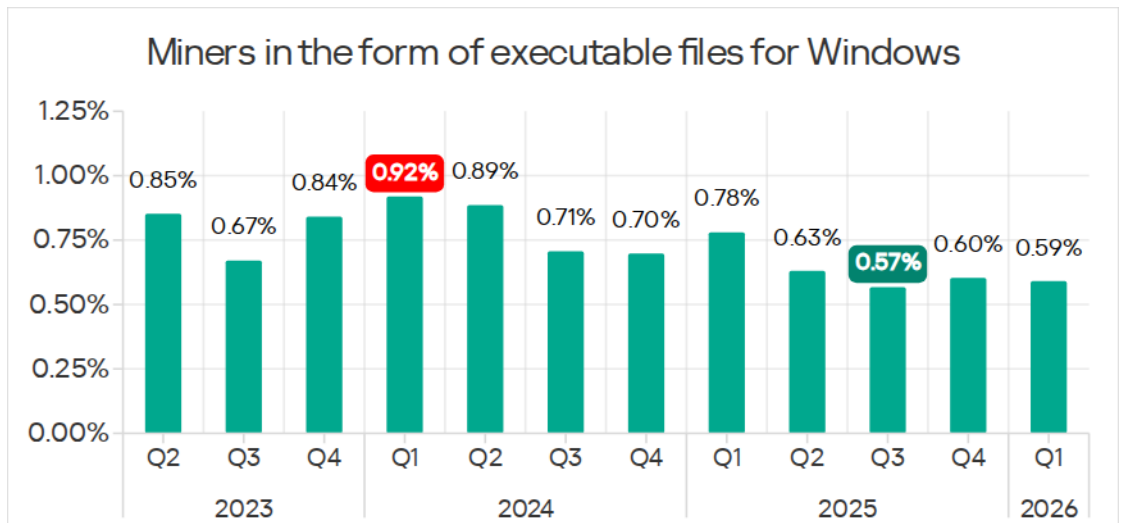


Another common method for deploying miners in the OT infrastructure involves using legitimate cryptocurrency mining software such as XMRig, NBMiner, OneZeroMiner, etc. While these miners are not inherently malicious, security systems classify them as [RiskTools](#). Attackers exploit these miners by combining them with customized configuration files that enable the miner's activity to be concealed from the user.

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



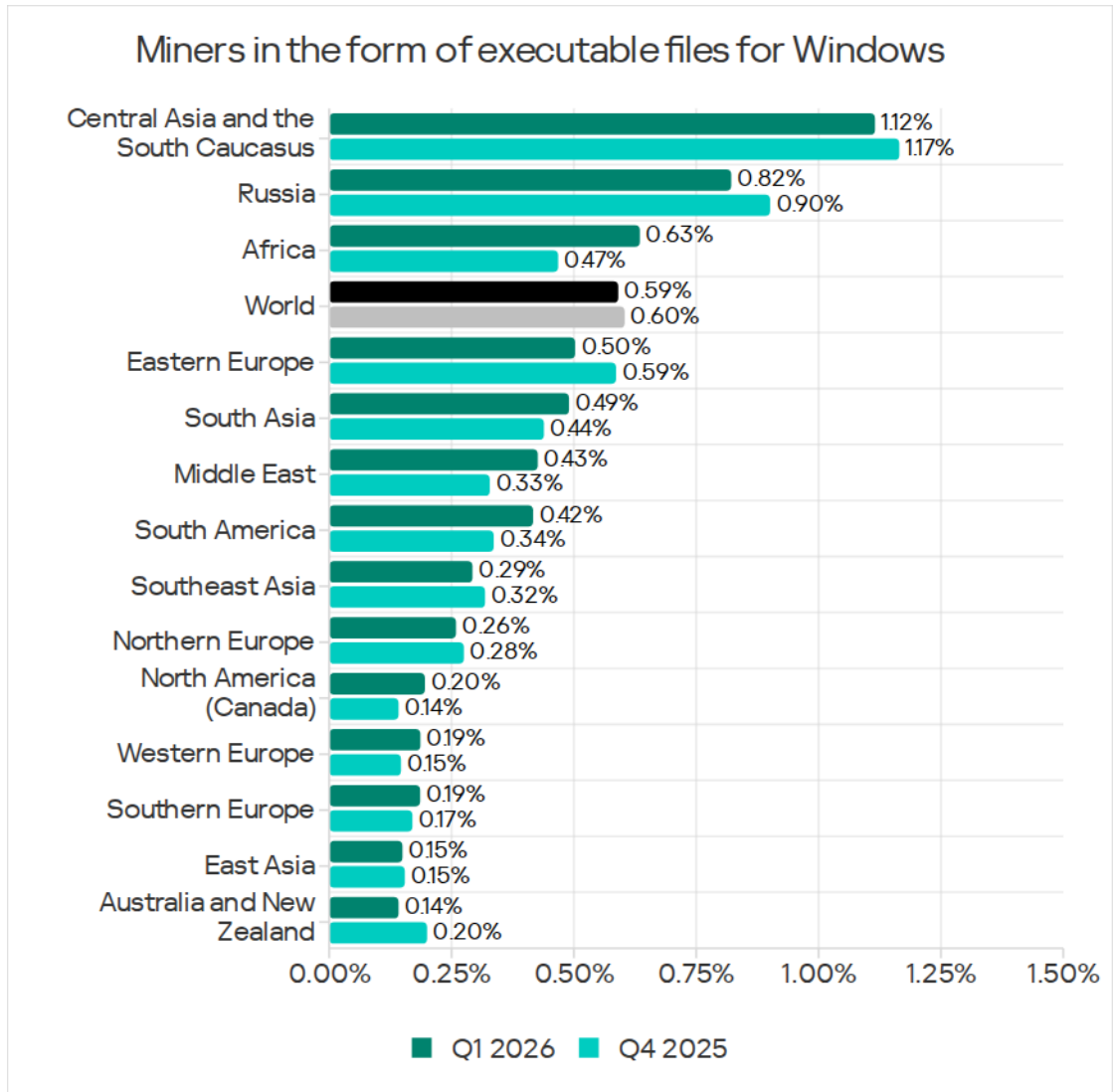
Percentage of ICS computers on which miners in the form of executable files for Windows were blocked, Q2 2023 – Q1 2026



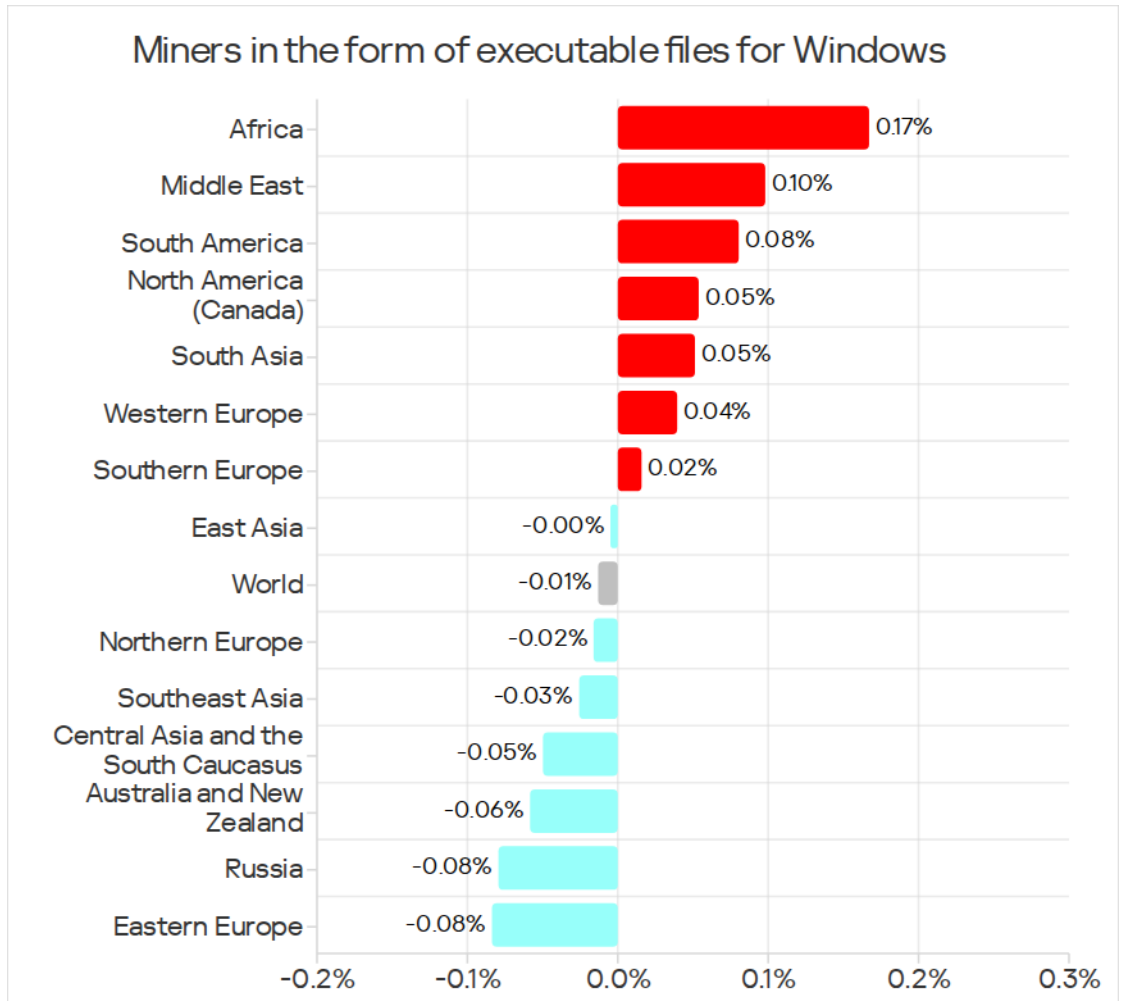
Percentage of ICS computers on which miners in the form of executable files for Windows were blocked, April 2024 – March 2026

In February 2026, the monthly percentage figure was the lowest for the entire period under review.

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

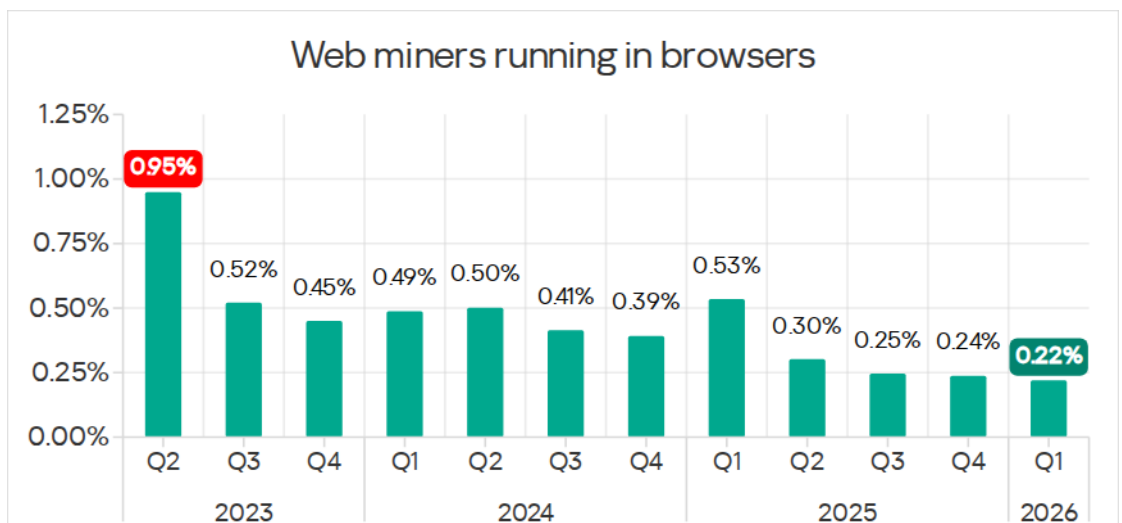


Changes in percentage of ICS computers on which miners in the form of executable files for Windows were blocked, Q1 2026

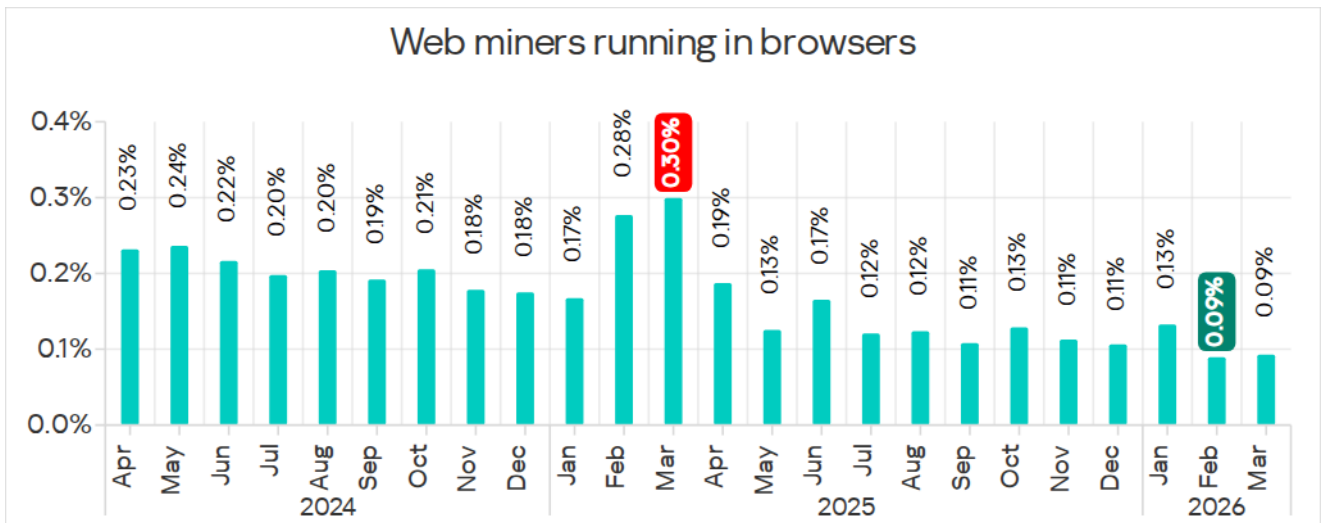


Web miners

Percentage of ICS computers on which web miners were blocked, Q2 2023 – Q1 2026

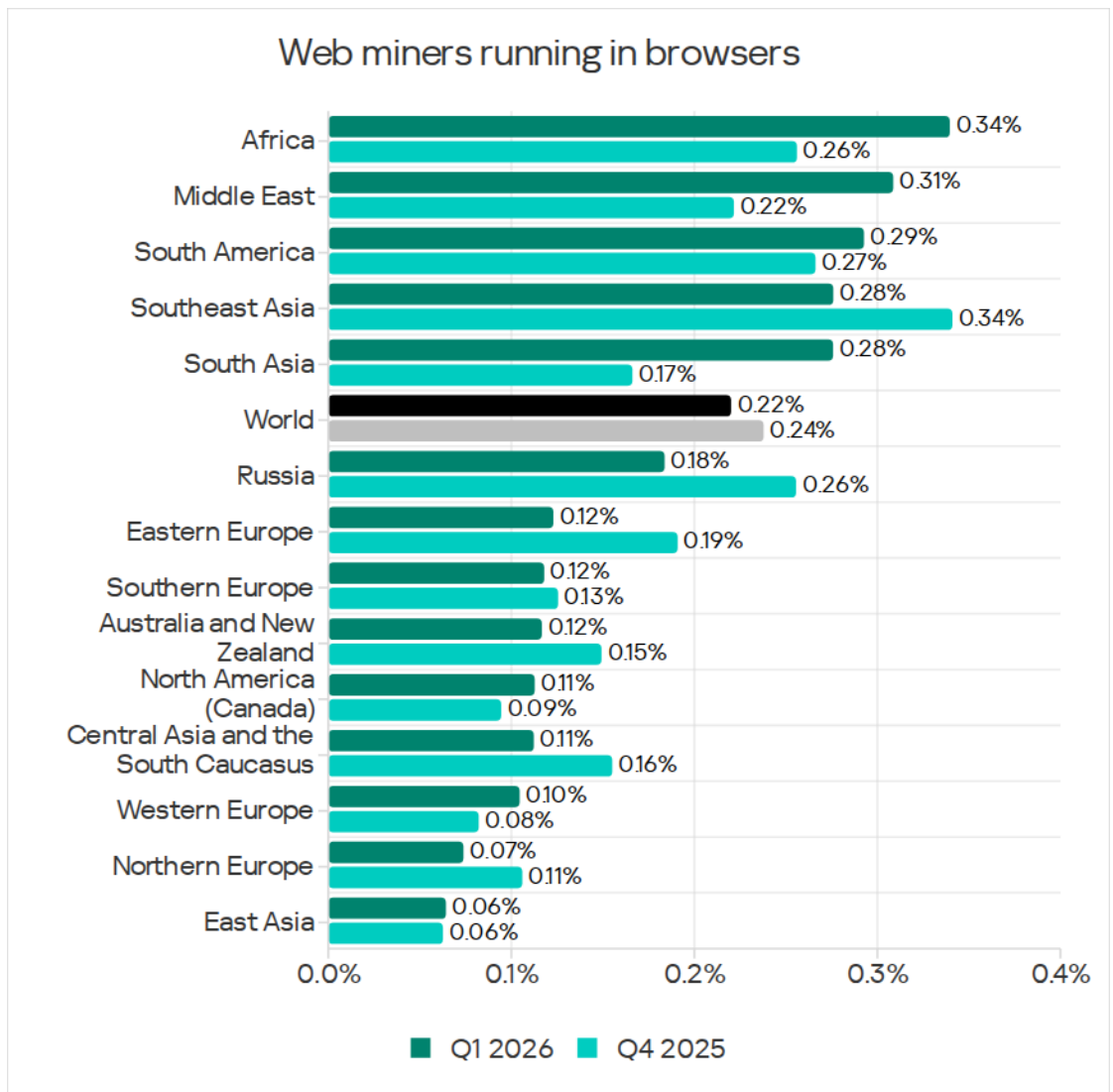


In February 2026, the monthly percentage figure was also the lowest for the entire period under review.

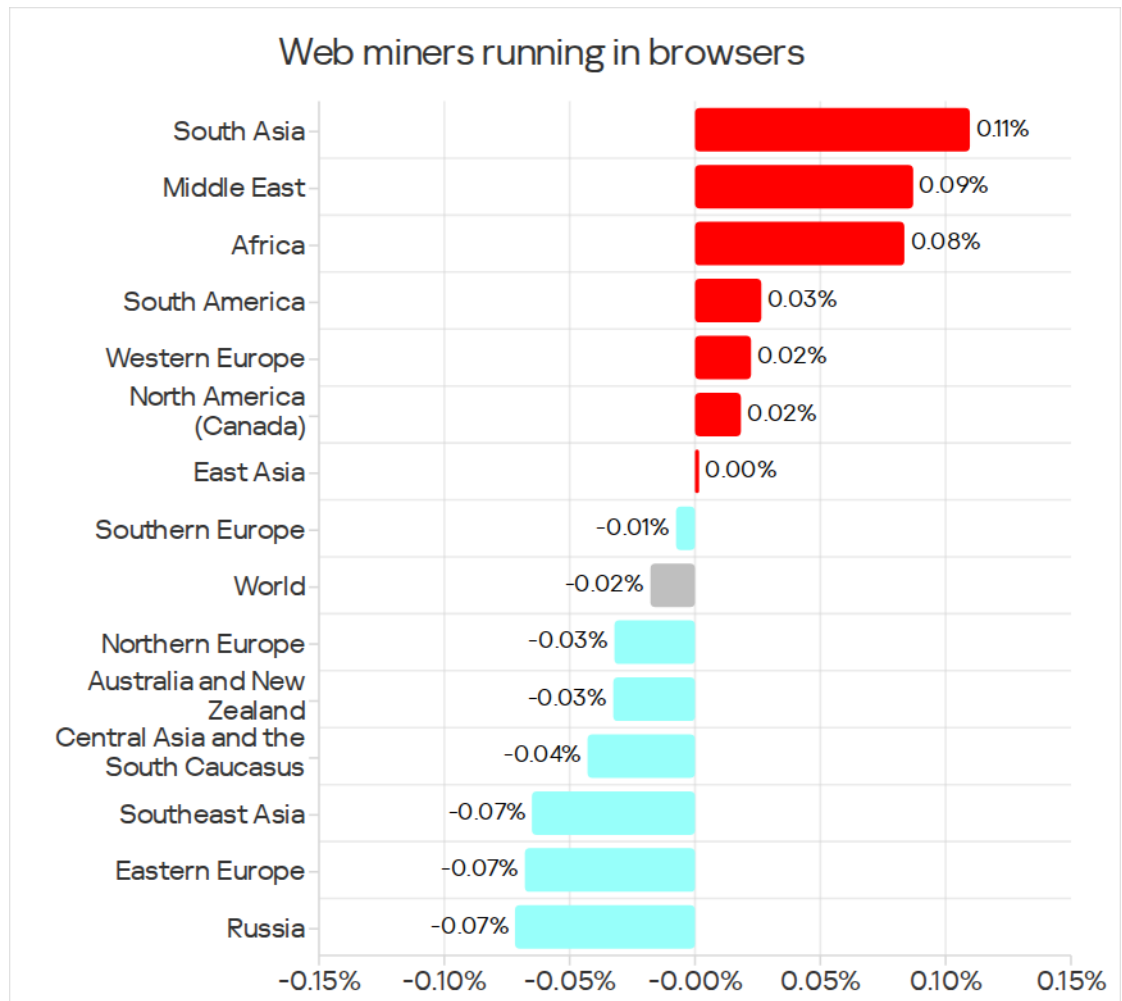


Percentage of ICS computers on which web miners were blocked, April 2024 – March 2026

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



Changes in percentage of ICS computers on which web miners were blocked, Q1 2026



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, propagating as infected files, such as archives containing backups, office documents, pirated games, and hacked applications. In rarer and more dangerous cases, infected objects include web pages with network equipment settings or files stored in internal document management systems, product lifecycle management (PLM) systems, resource management (ERP) systems, and other intranet services.

Most worms and viruses detected on removable media are either variants of outdated polymorphic threats (which appeared around 2010) or modern modular cryptocurrency miners.

It should be kept in mind that some worms and viruses spread through active techniques, such as password brute-force attacks, theft and use of user authentication data (including access tokens), and network attacks on vulnerable software, all of which have long been part of the modular toolkit of any modern worm-miner.

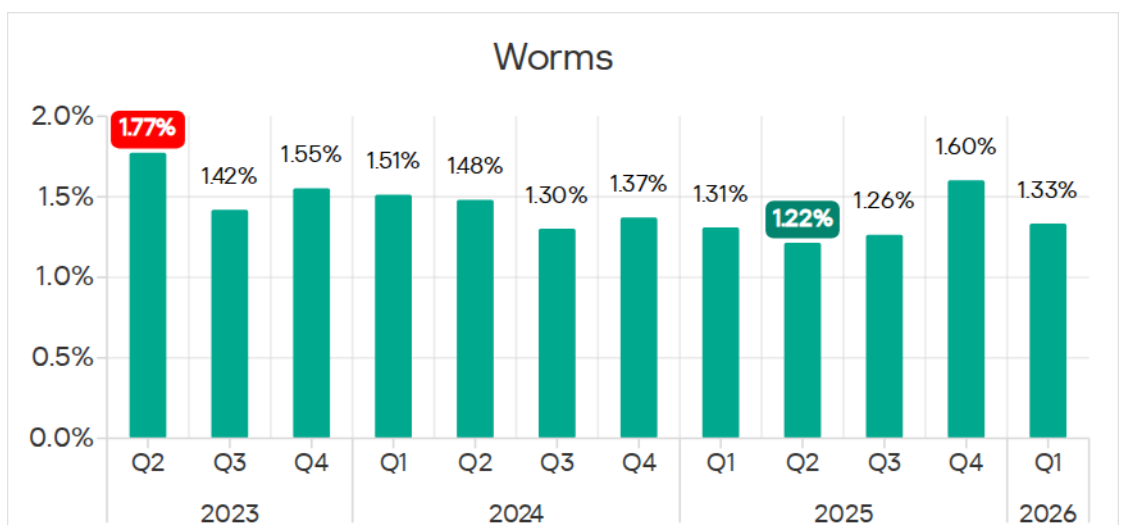
Modern versions of worms are not often found in ICS networks, but the damage caused by an infection is always significant: even basic maintenance of a network infected with worm-miners becomes several times more expensive due to longer downtime and the additional man-hours required to restore performance. And if a worm is used to download ransomware to a computer in an OT network after preliminary profiling, the cost is exponentially higher.

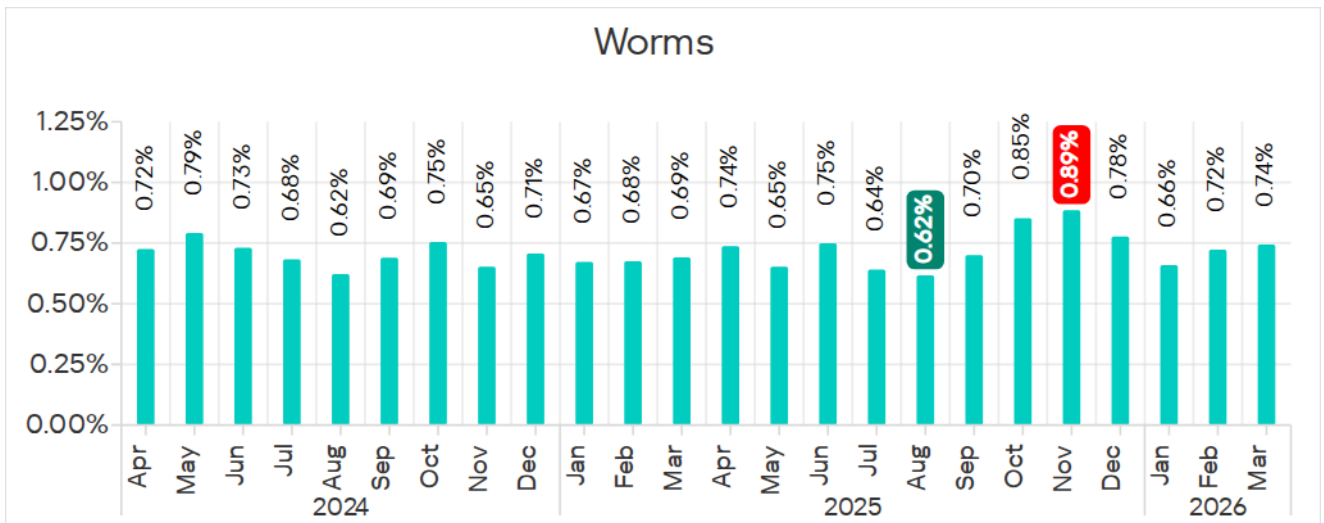
At the same time, a significant part of the viruses and worms that spread today are legacy modifications whose command-and-control servers have been shut down. However, these types of malware can not only compromise infected systems, for example, by opening network ports and changing configurations, but also cause software failures, denial of service, etc.

High percentage figures for 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 weak segmentation of the enterprise network and a lack of control over the use of removable media.

Worms

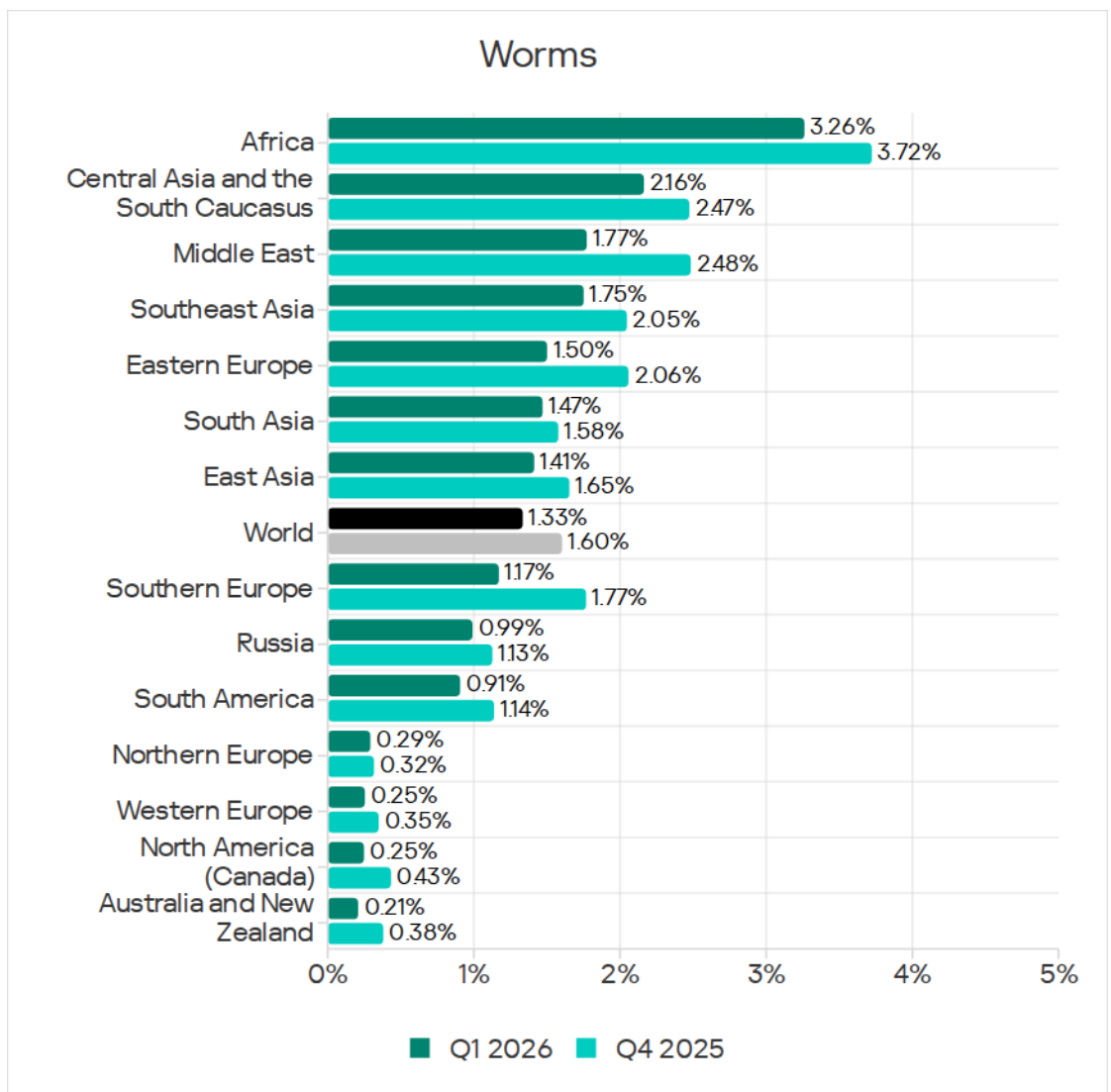
Percentage of ICS computers on which worms were blocked, Q2 2023 – Q1 2026



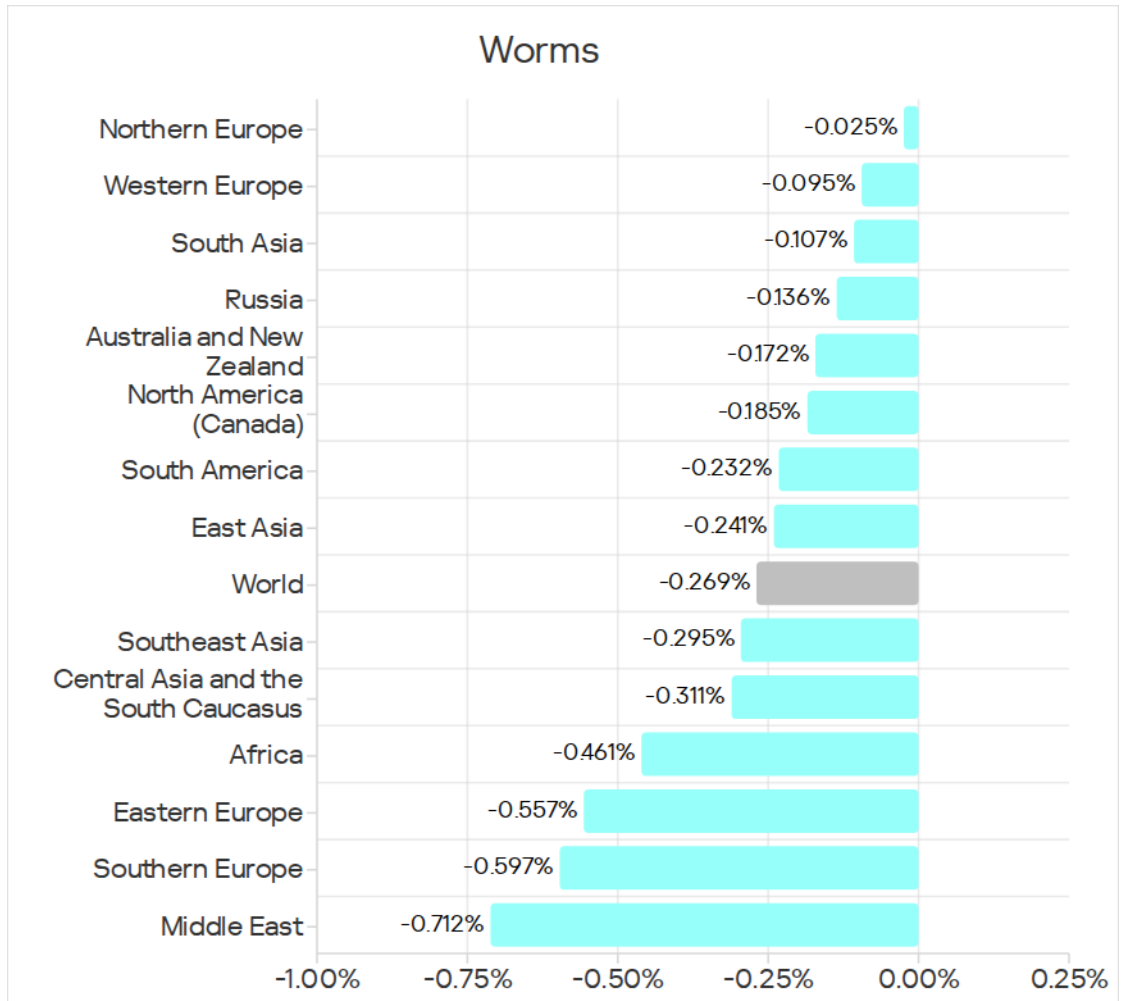


Percentage of ICS computers on which worms were blocked, April 2024 – March 2026

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

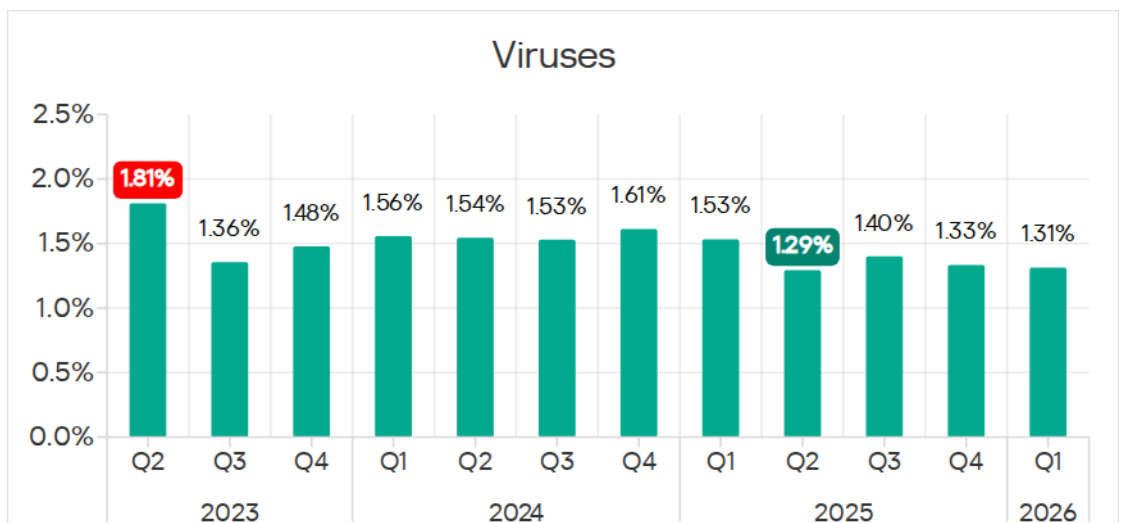


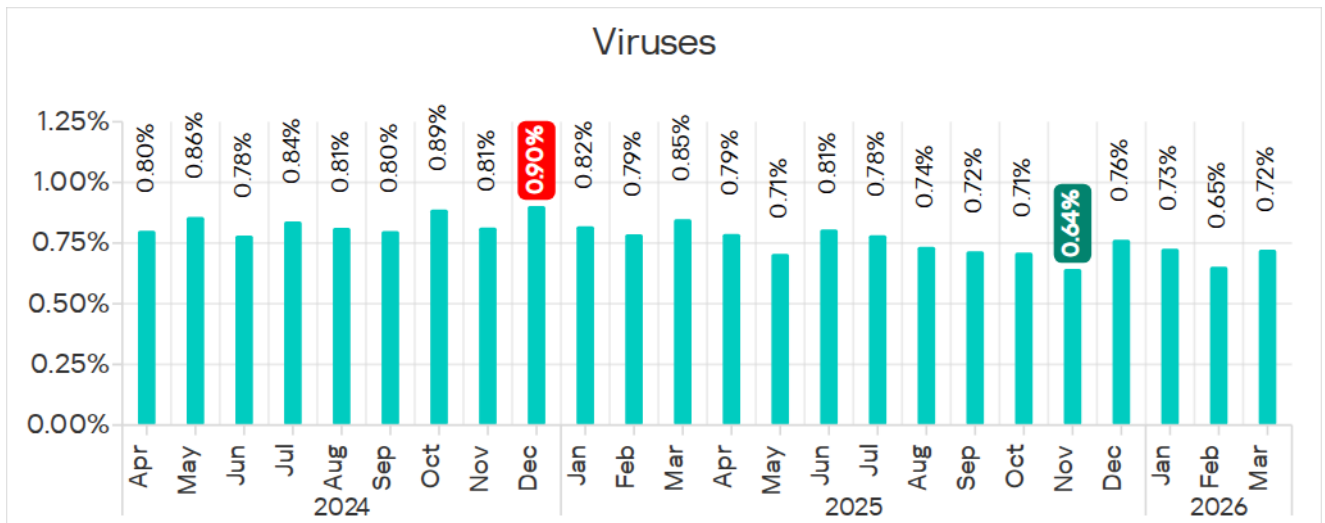
Changes in percentage of ICS computers on which worms were blocked, Q1 2026



Viruses

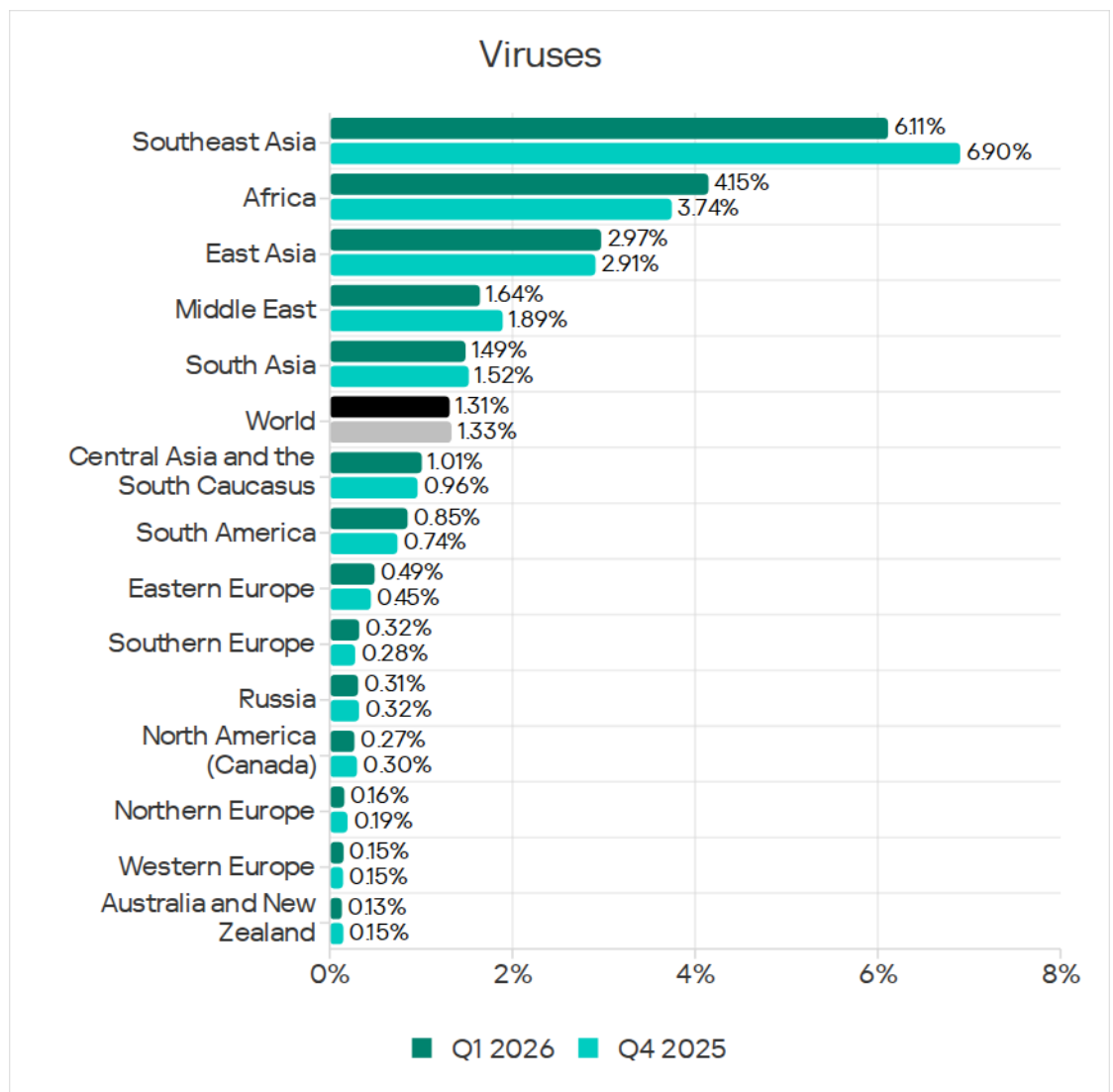
Percentage of ICS computers on which viruses were blocked, Q2 2023 – Q1 2026



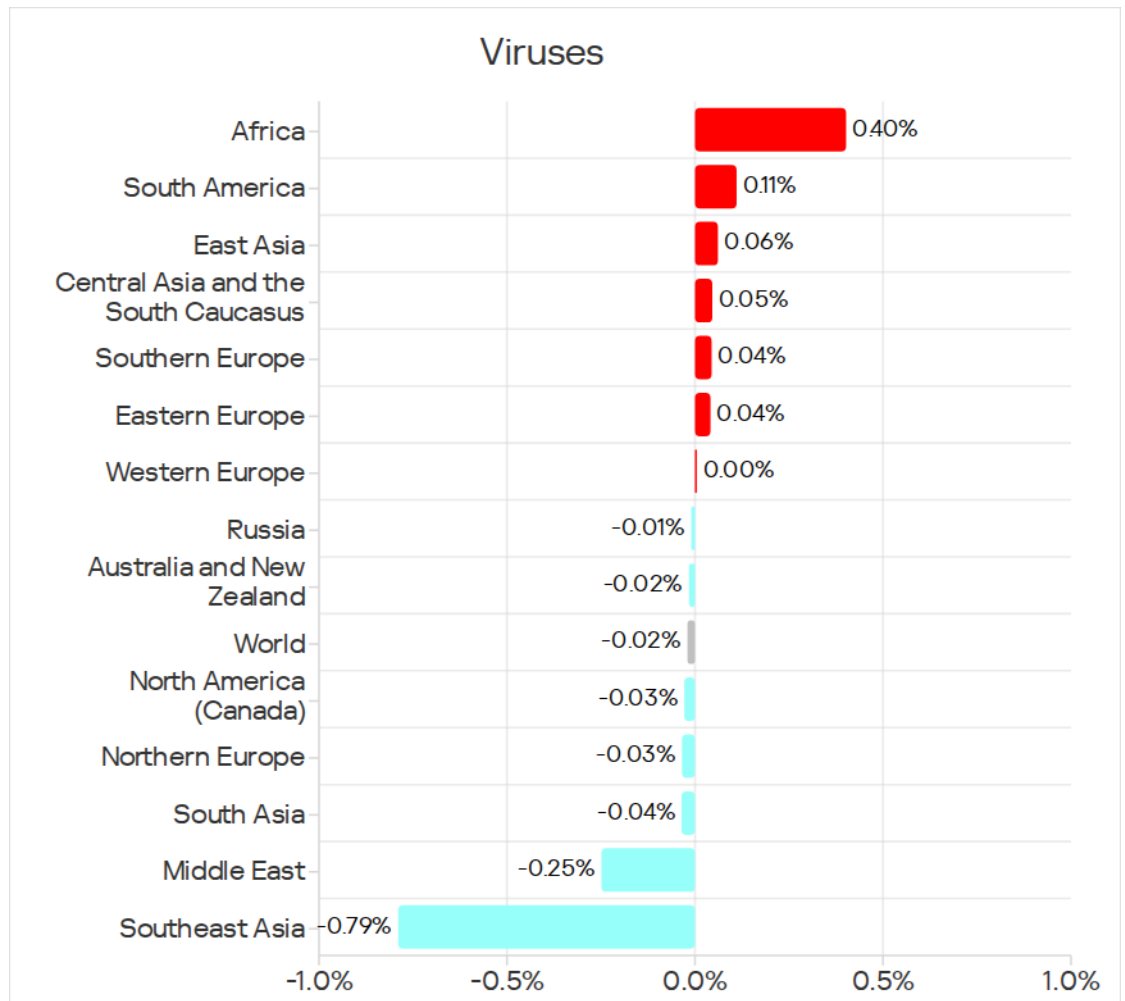


Percentage of ICS computers on which viruses were blocked, April 2024 – March 2026

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



Changes in percentage of ICS computers on which viruses were blocked, Q1 2026

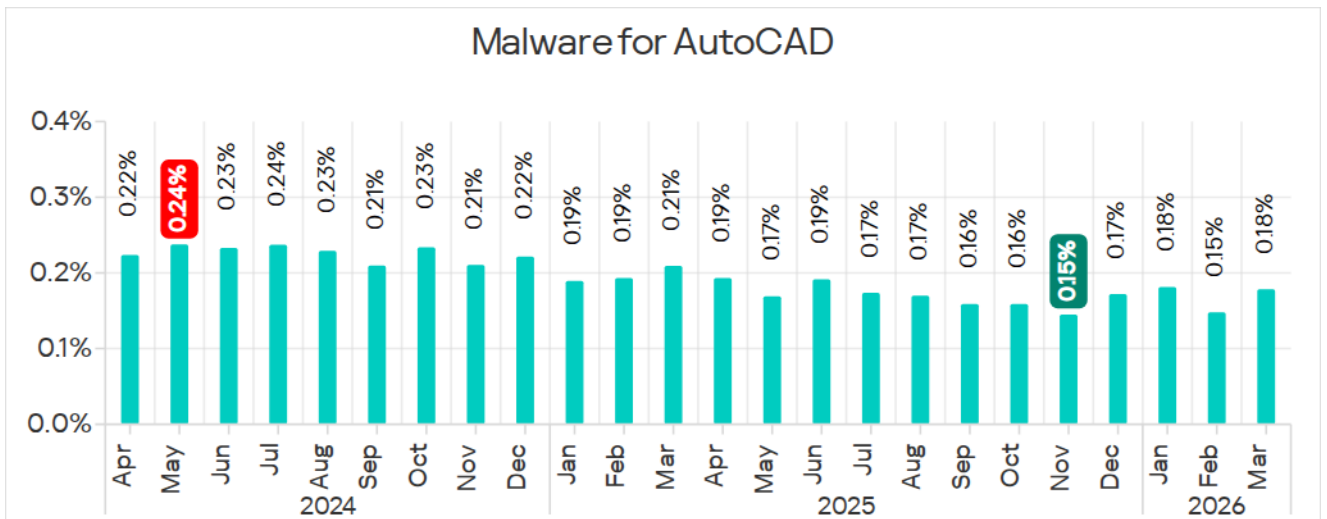
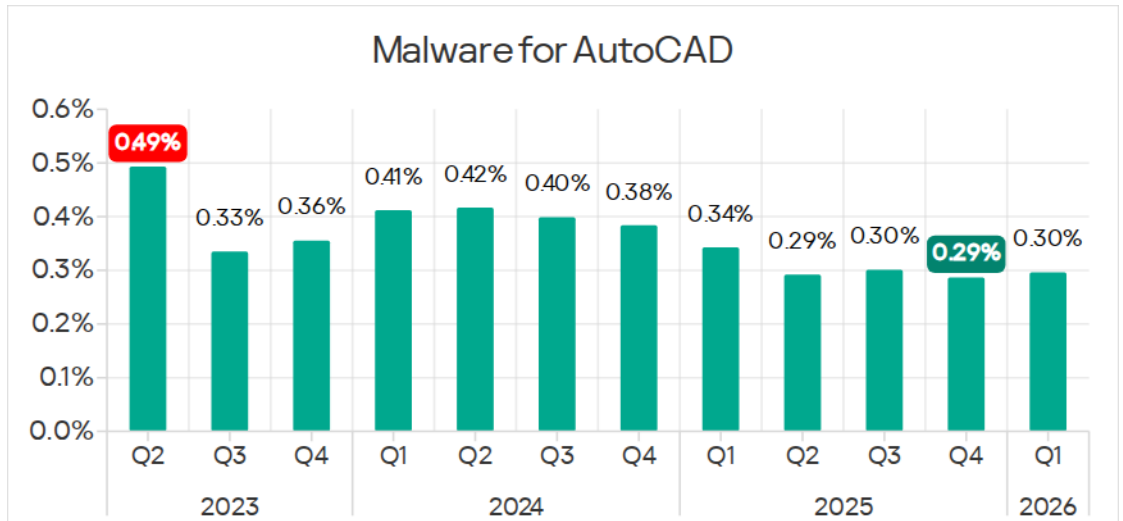


Malware for AutoCAD

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

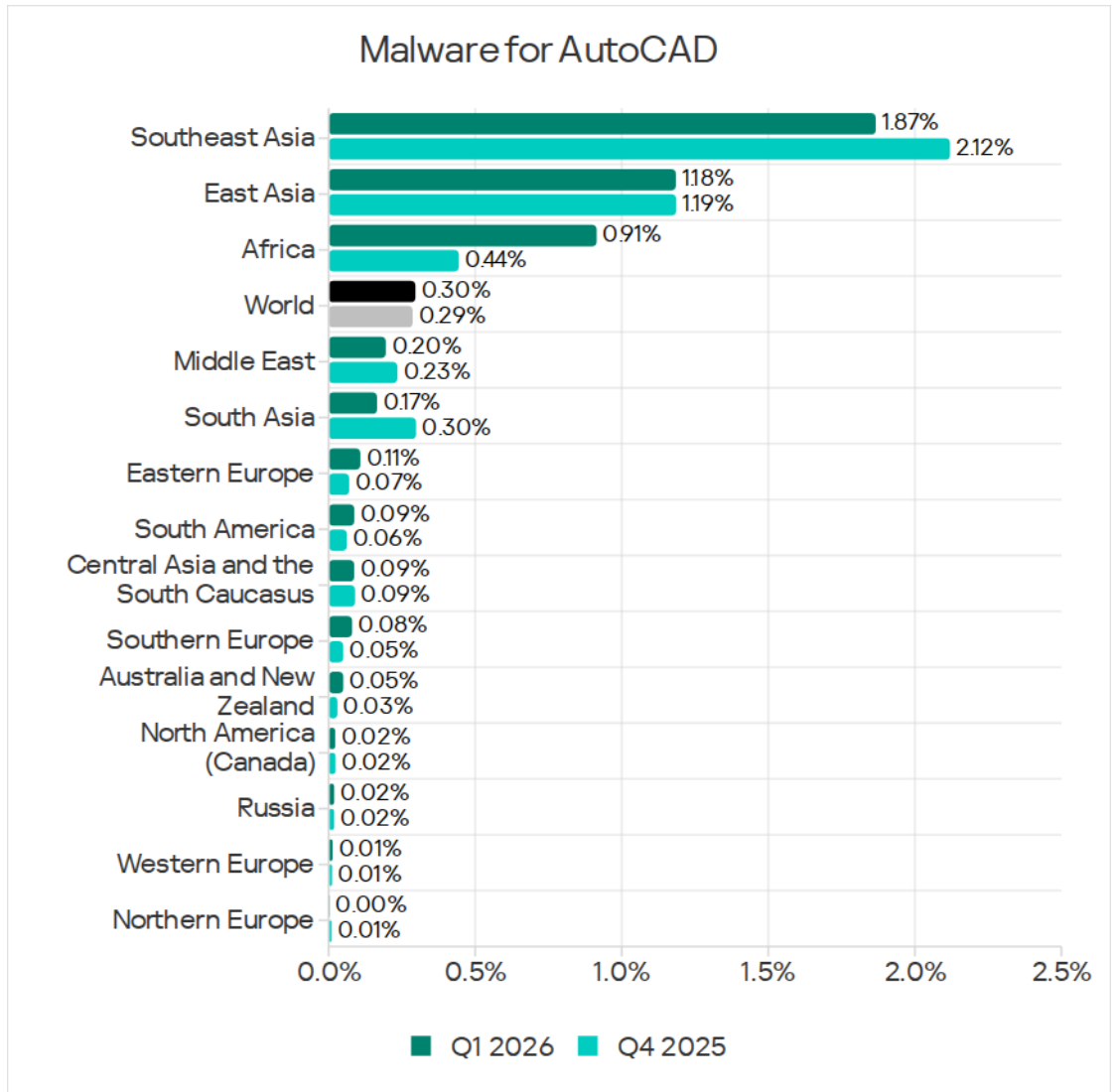
Malware for AutoCAD is typically a low-level threat, which ranks last in the malware category rankings by the percentage of ICS computers on which it was blocked.

Percentage of ICS computers on which malware for AutoCAD was blocked, Q2 2023 – Q1 2026

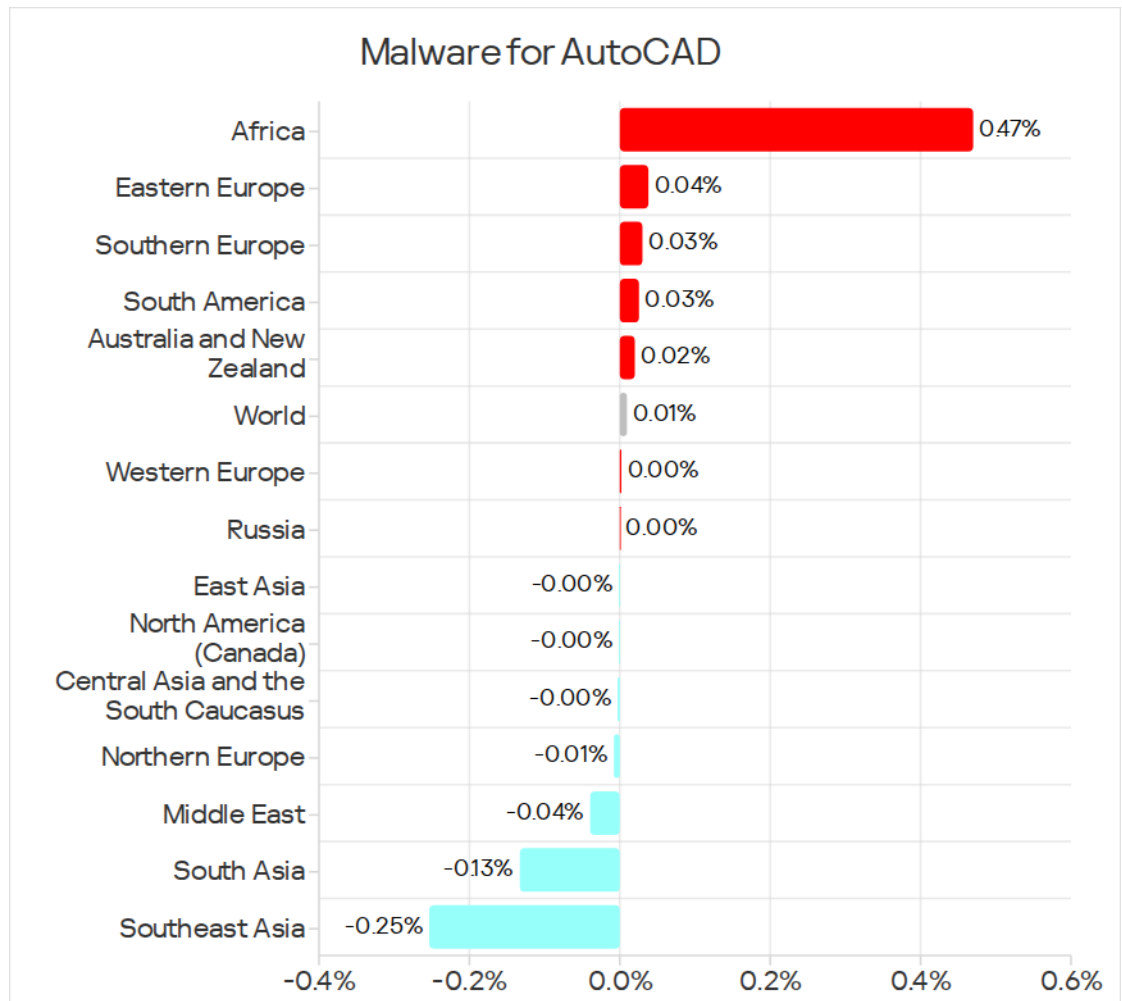


Percentage of ICS computers on which malware for AutoCAD was blocked, April 2024 – March 2026

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



Changes in percentage of ICS computers on which malware for AutoCAD was blocked, Q1 2026

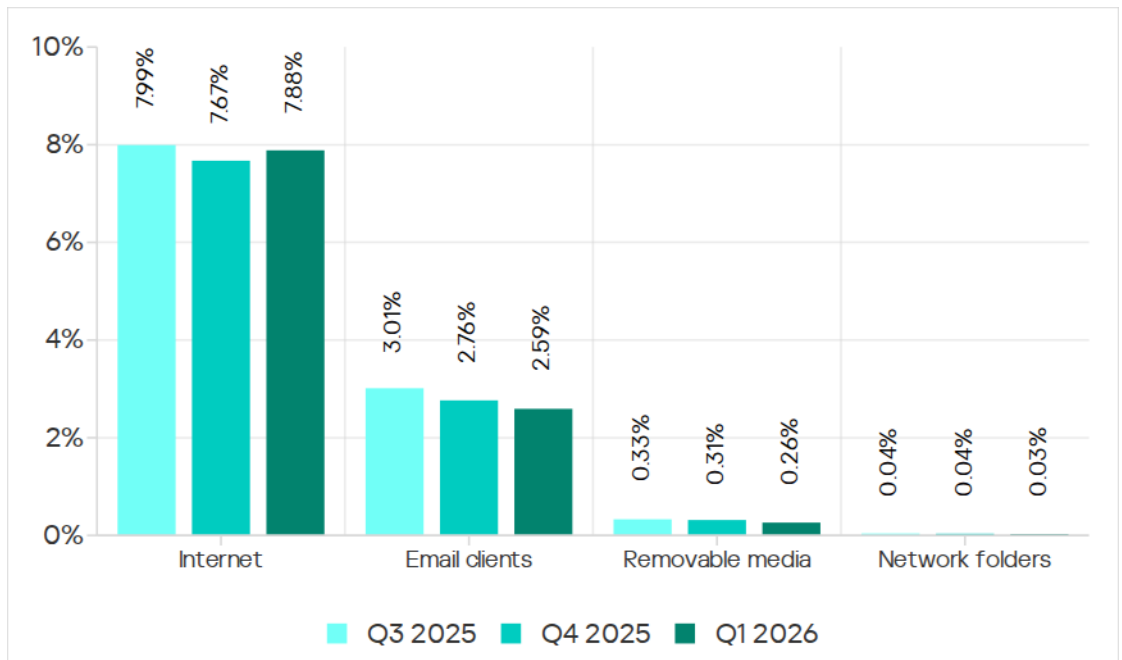


Main threat sources

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

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 media remain the primary sources of threats to computers in organizations' OT infrastructure.

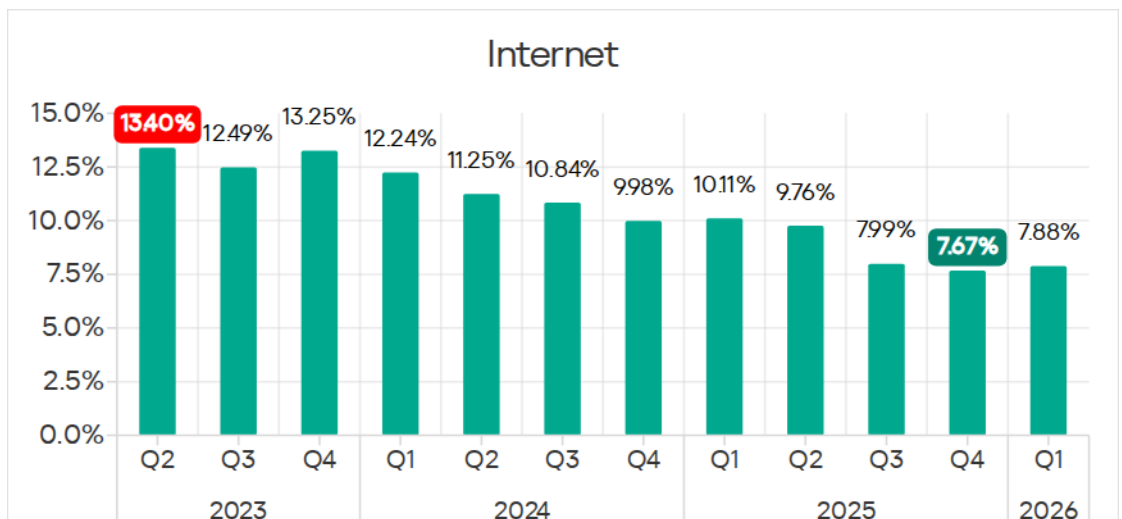
Percentage of ICS computers on which malicious objects from various sources were blocked



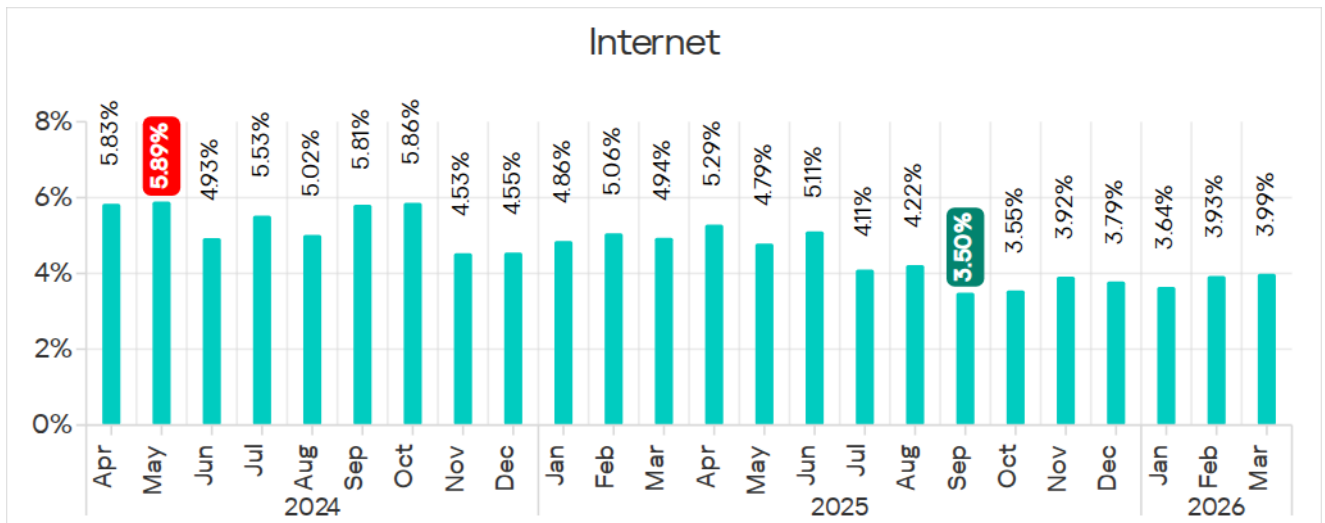
Internet

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.

Percentage of ICS computers on which threats from the internet were blocked, Q2 2023 – Q1 2026

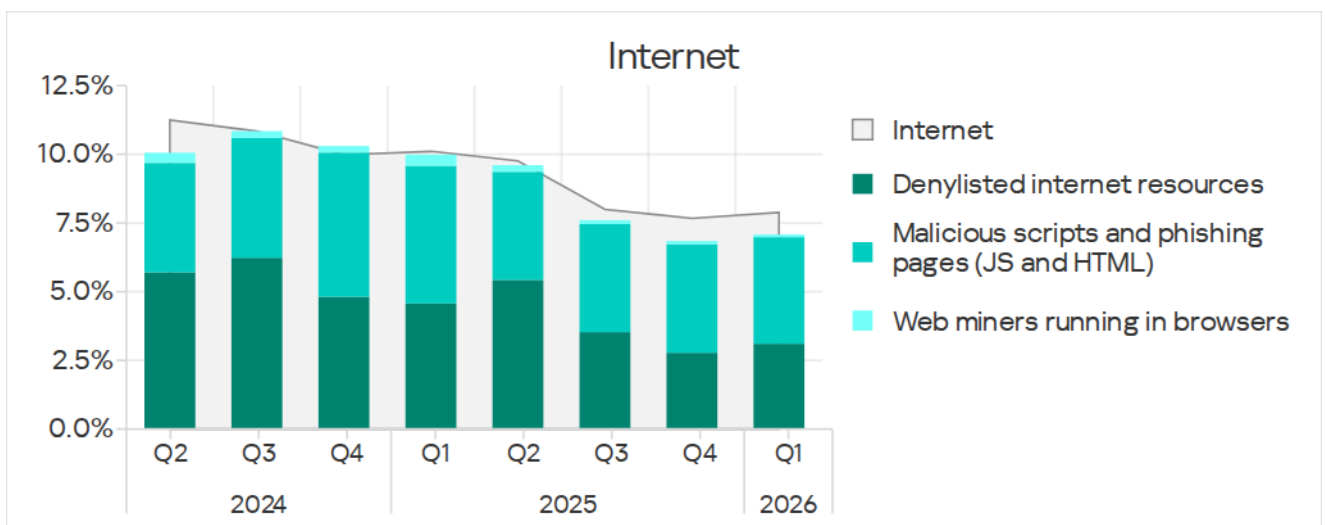


In the first quarter of 2026, the monthly percentage figure increased for two consecutive months.



Percentage of ICS computers on which threats from the internet were blocked, April 2024 – March 2026

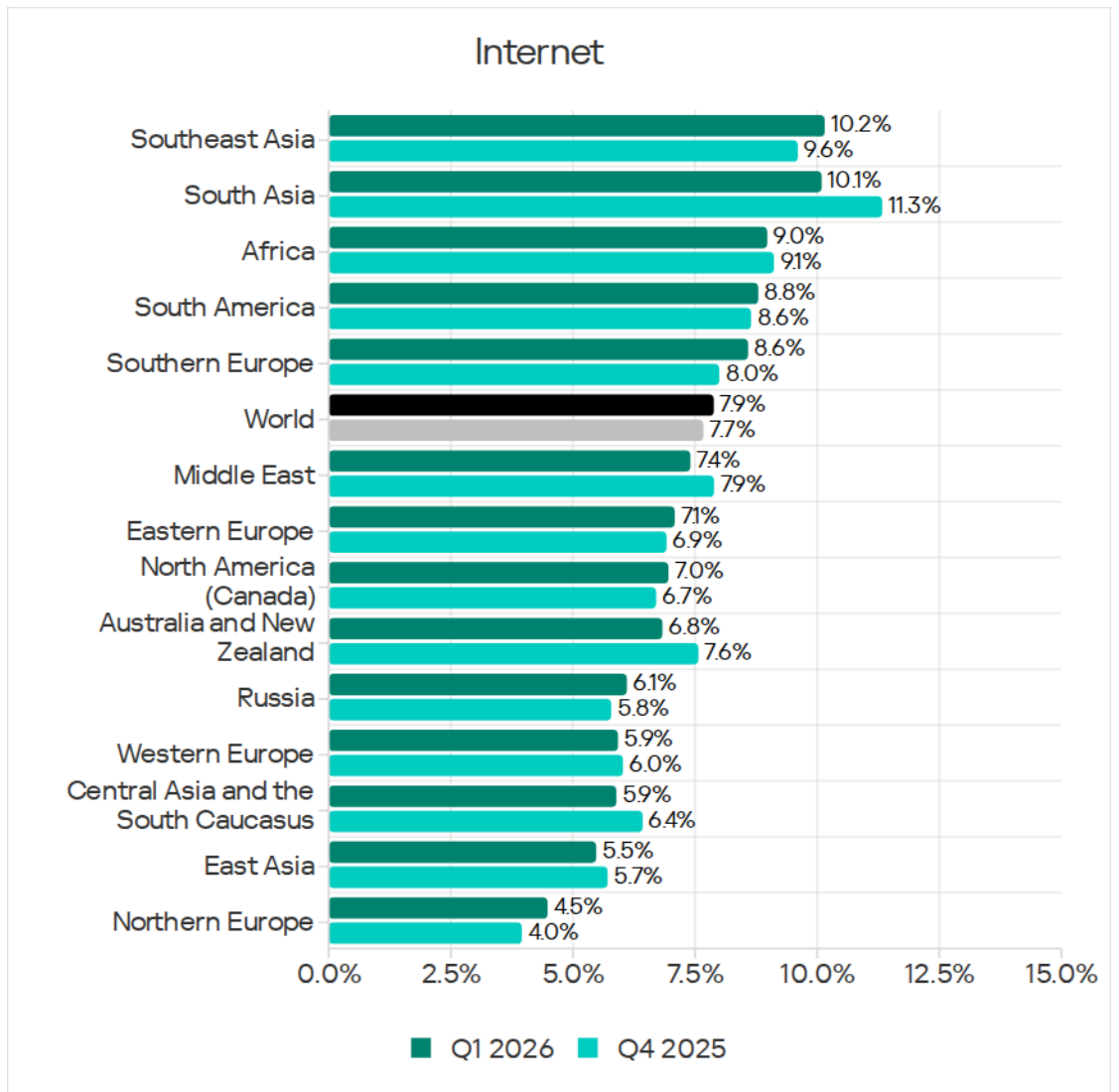
The main categories of threats from the internet* blocked on ICS computers in Q1 2026 are malicious scripts and phishing pages, and denylisted internet resources.



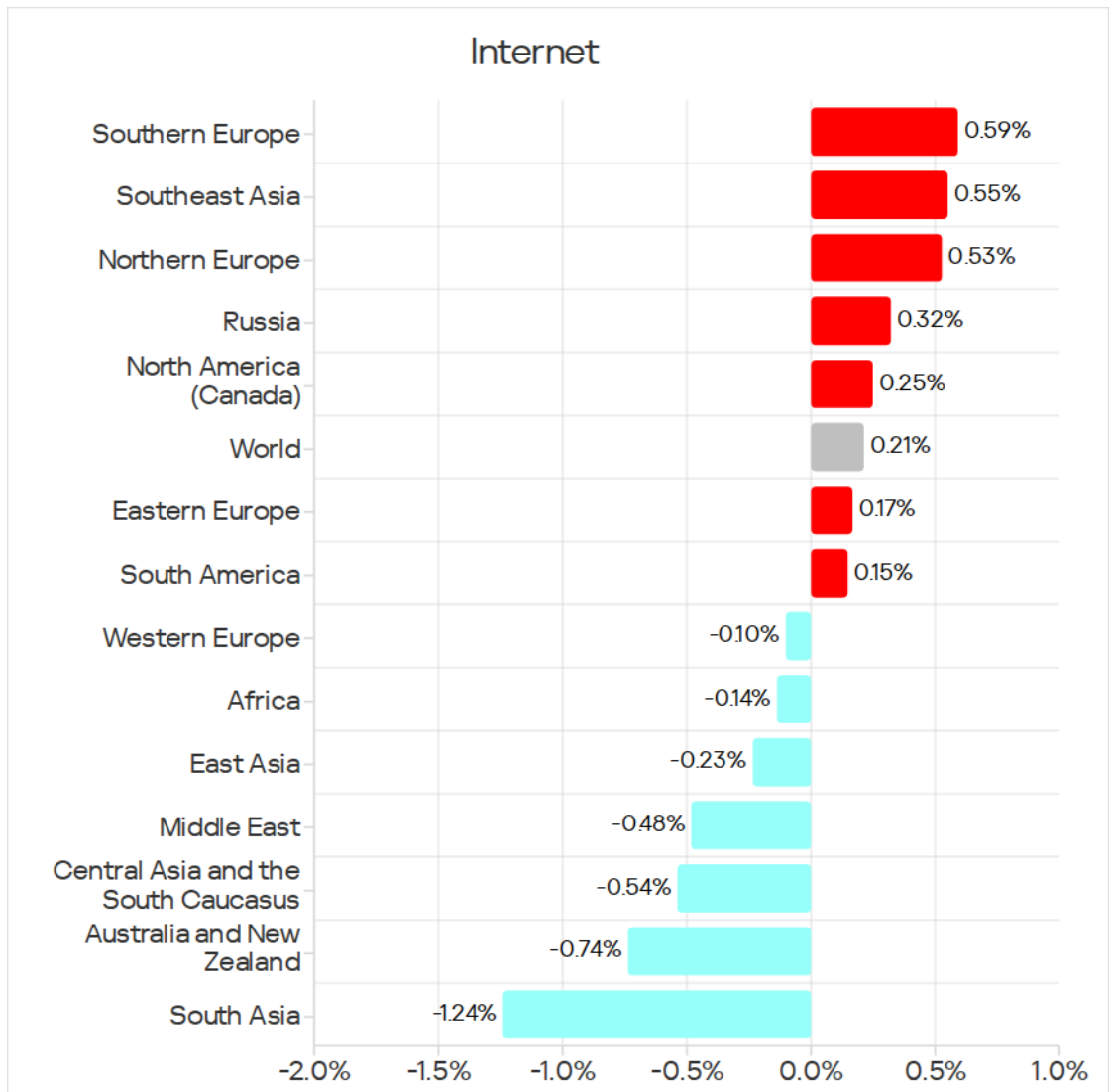
Threats from the internet and main threat categories from the internet, Q2 2024 – Q1 2026

*It should be kept in mind that 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 source of 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 that source.

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



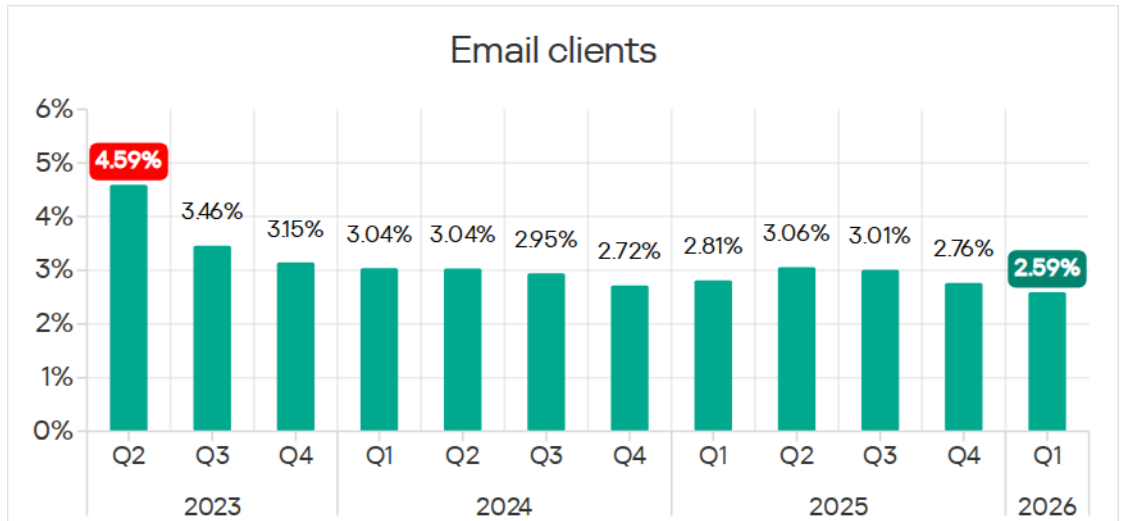
Changes in percentage of ICS computers on which threats from the internet were blocked, Q1 2026



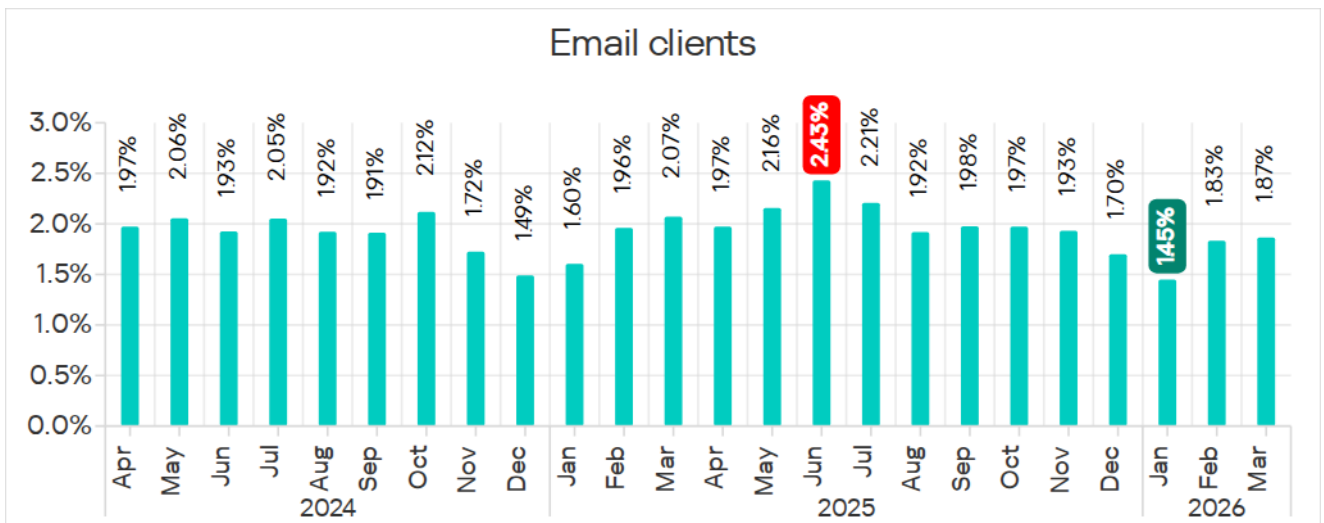
Email clients

Some detected and blocked threats were delivered to protected computers via the email delivery system and/or attempted to gain access through the email client application.

Percentage of ICS computers on which threats from email clients were blocked, Q2 2023 – Q1 2026

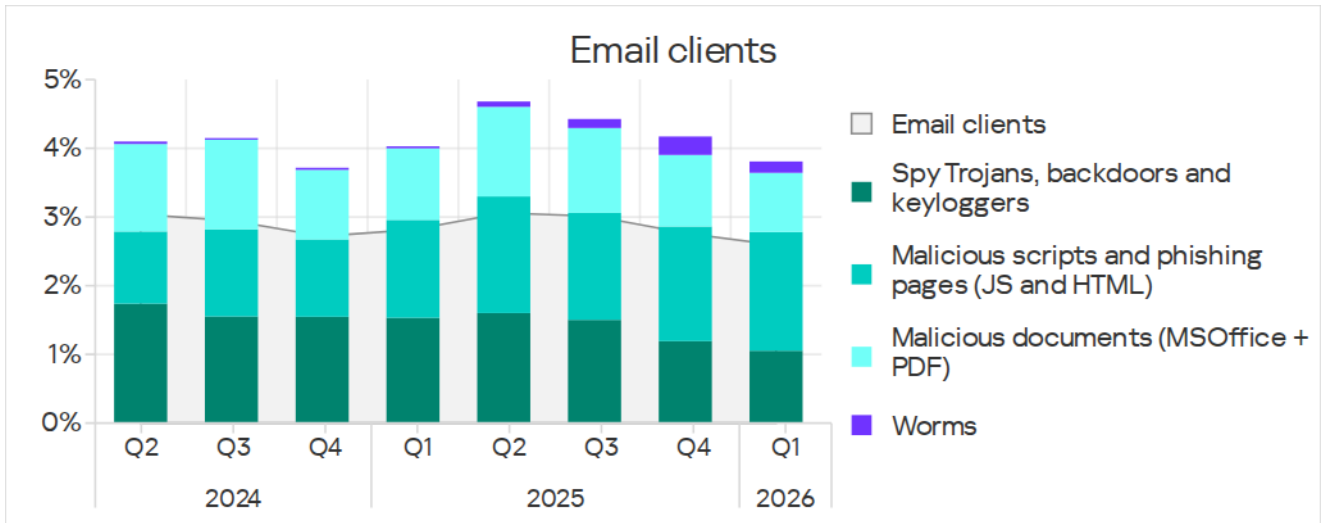


The monthly percentage figure for January was the lowest in two years.



Percentage of ICS computers on which threats from email clients were blocked, April 2024 – March 2026

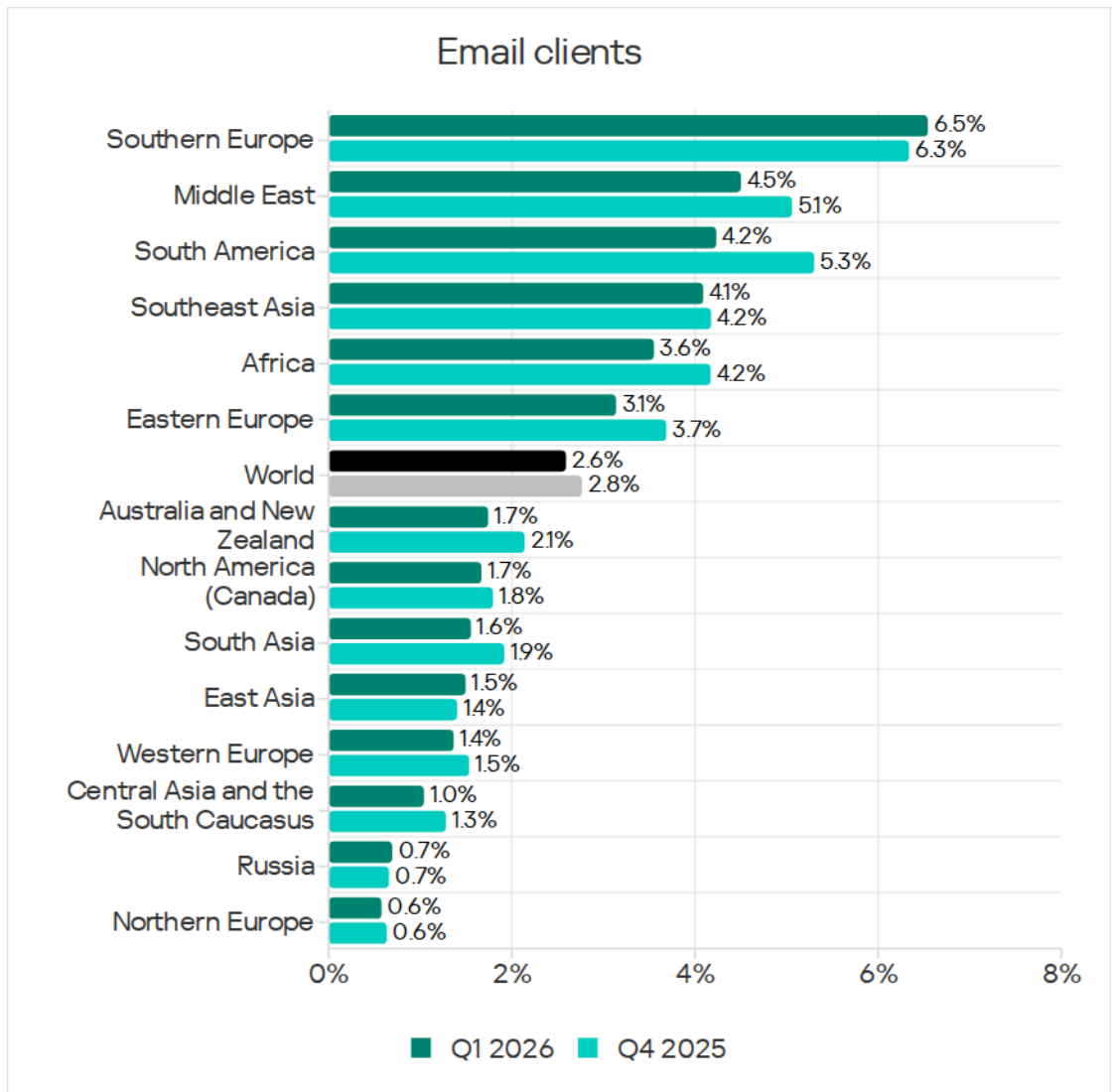
The main categories of email threats blocked on ICS computers in Q1 2026 are malicious scripts and phishing pages, spyware, and malicious documents. The percentage of computers on which worms from email clients were blocked has decreased, but it is still noticeable.



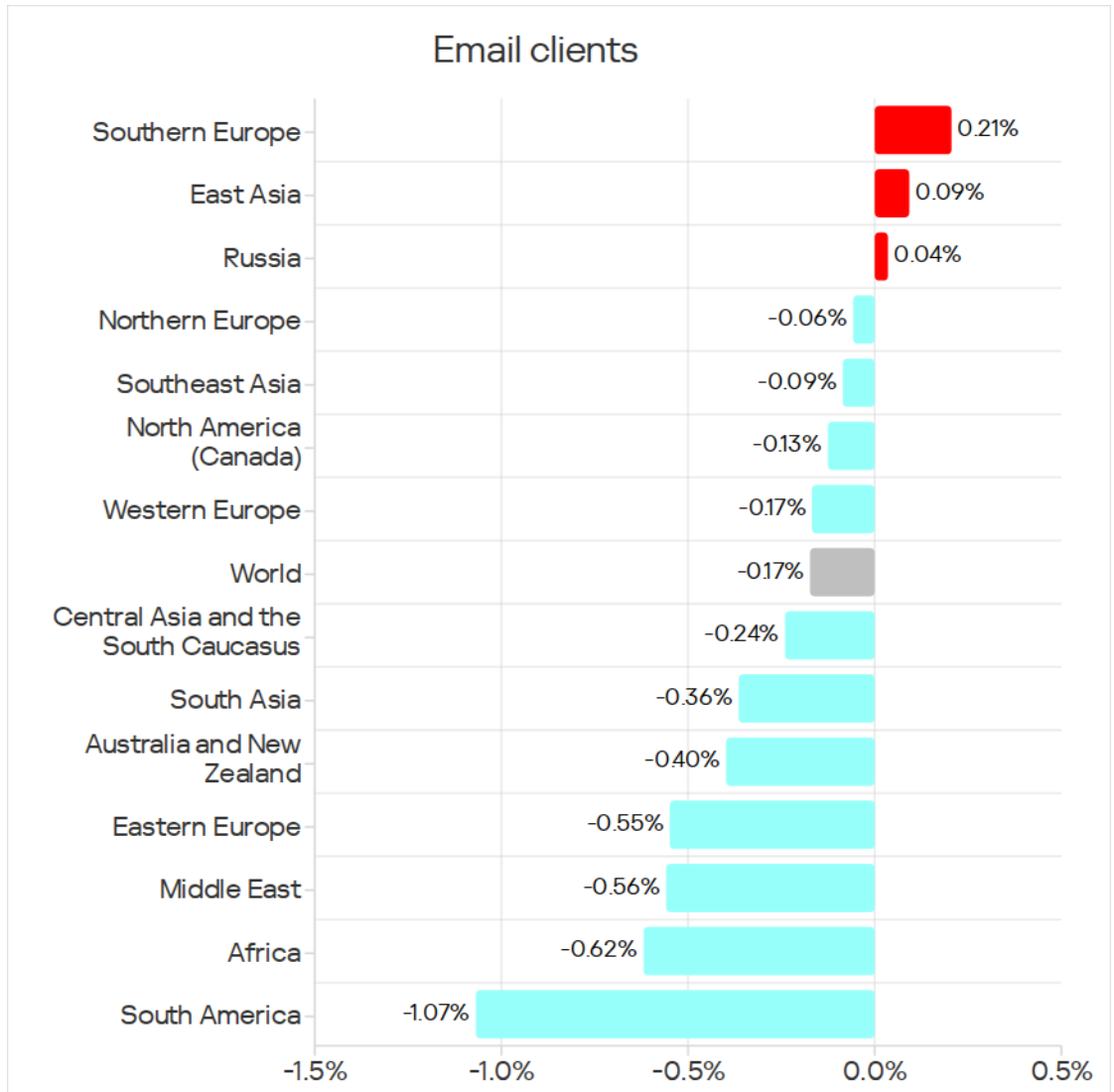
Threats from email clients and main categories of email threats, Q1 2024 – Q1 2026

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

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

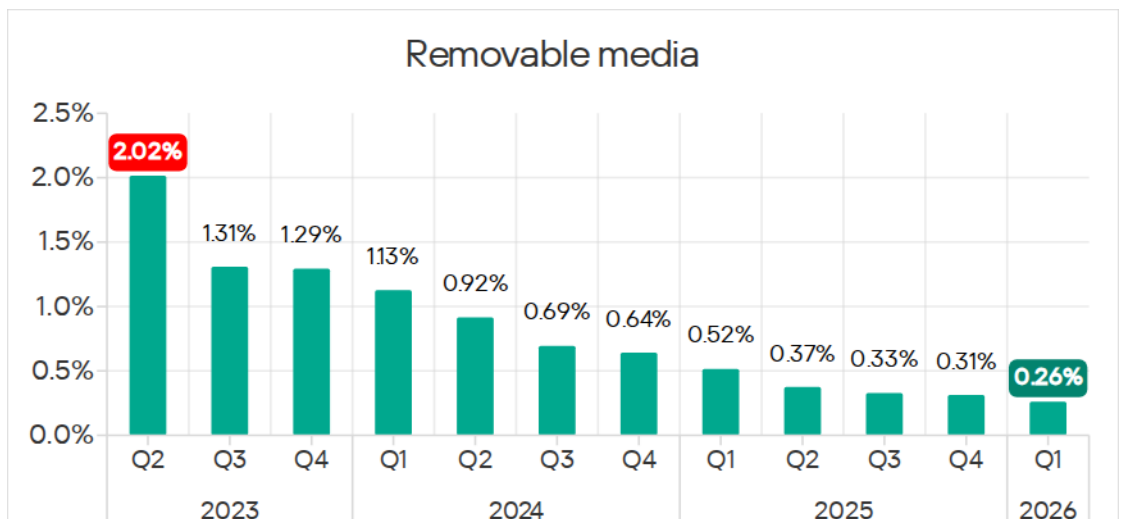


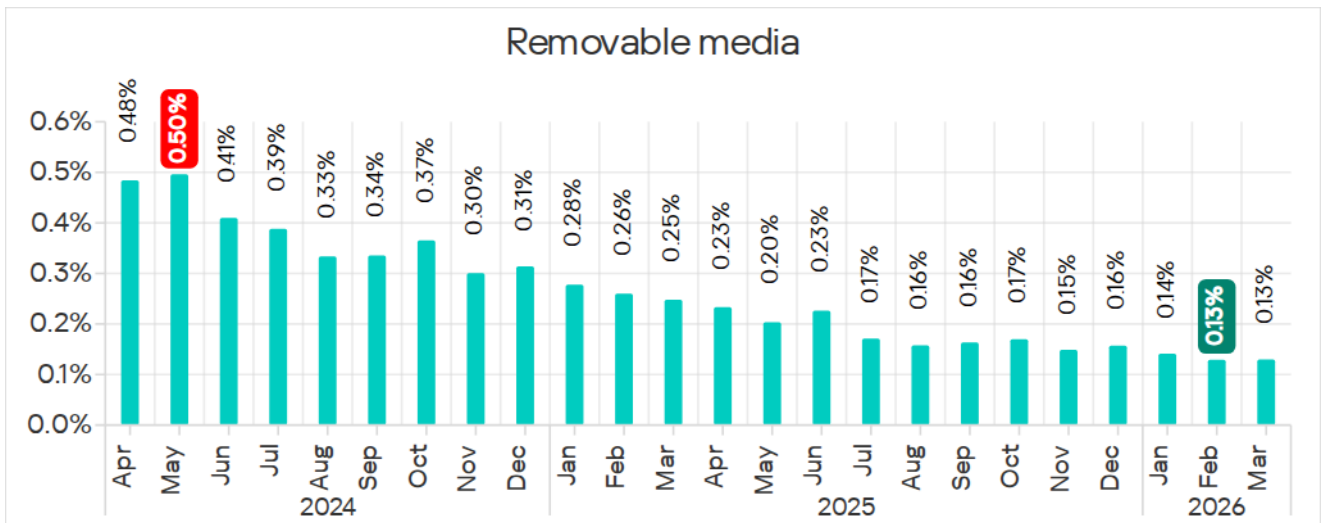
Changes in percentage of ICS computers on which threats from email clients were blocked, Q1 2026



Removable media

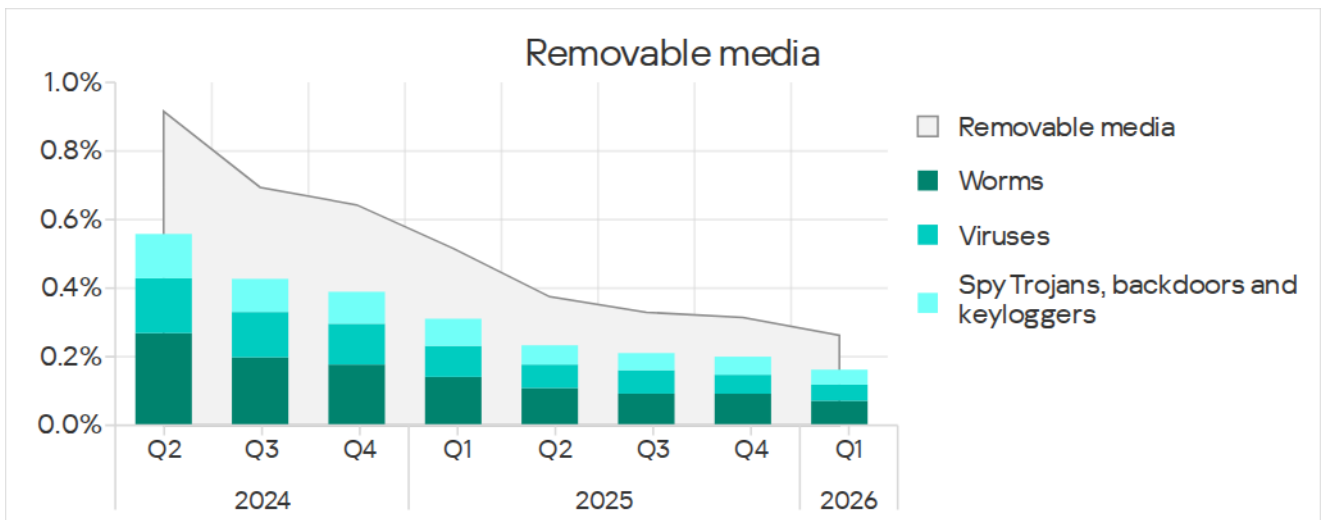
Percentage of ICS computers on which threats from removable media were blocked, Q2 2023 – Q1 2026





Percentage of ICS computers on which threats from removable media were blocked, April 2024 – March 2026

The main categories of threats blocked in Q1 2026 when removable media were connected to ICS computers are worms, viruses, and spyware.

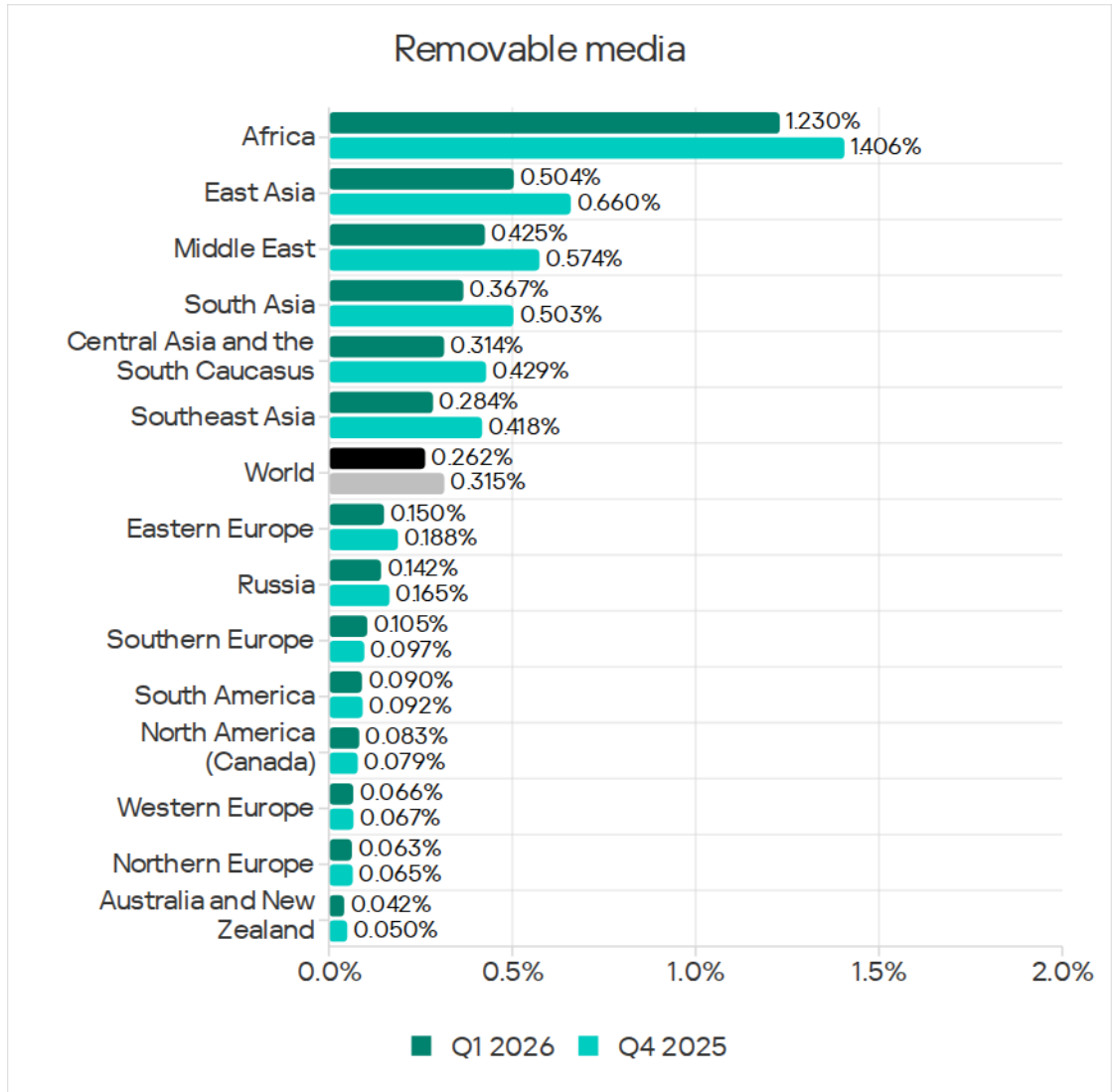


Threats from removable media and main categories of threats from removable media, Q2 2024 – Q1 2026

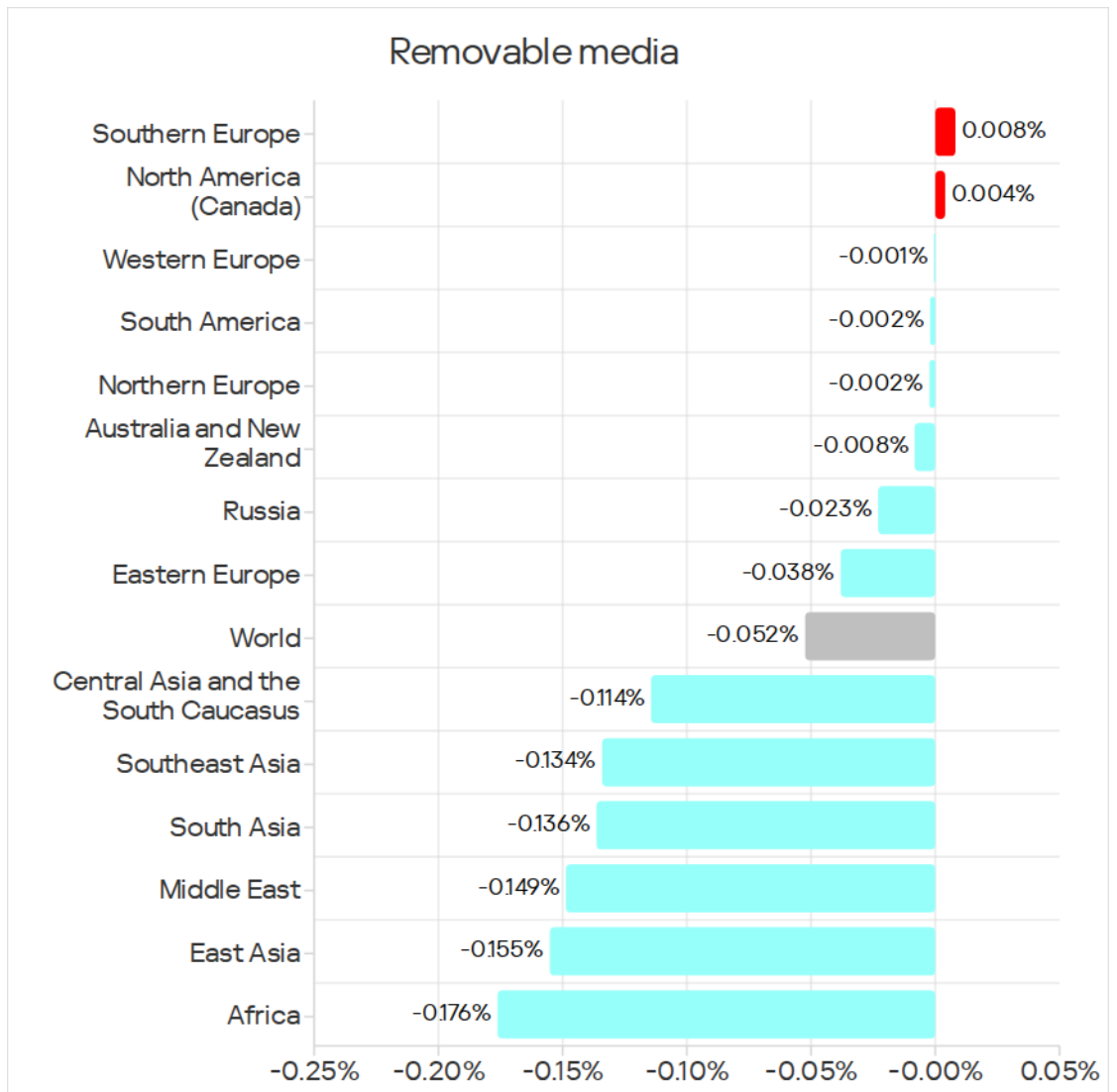
Most worms and viruses detected on removable media are either variants of outdated polymorphic threats (which appeared around 2010) or modern modular cryptocurrency miners. These modern cryptocurrency miners can spread across local networks by stealing credentials from infected hosts, exploiting known 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.

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

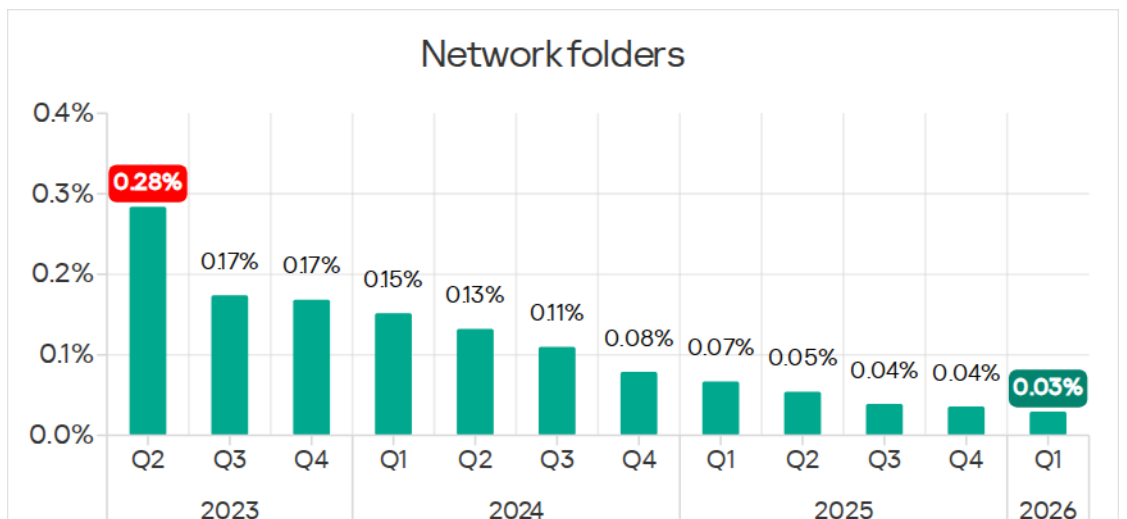


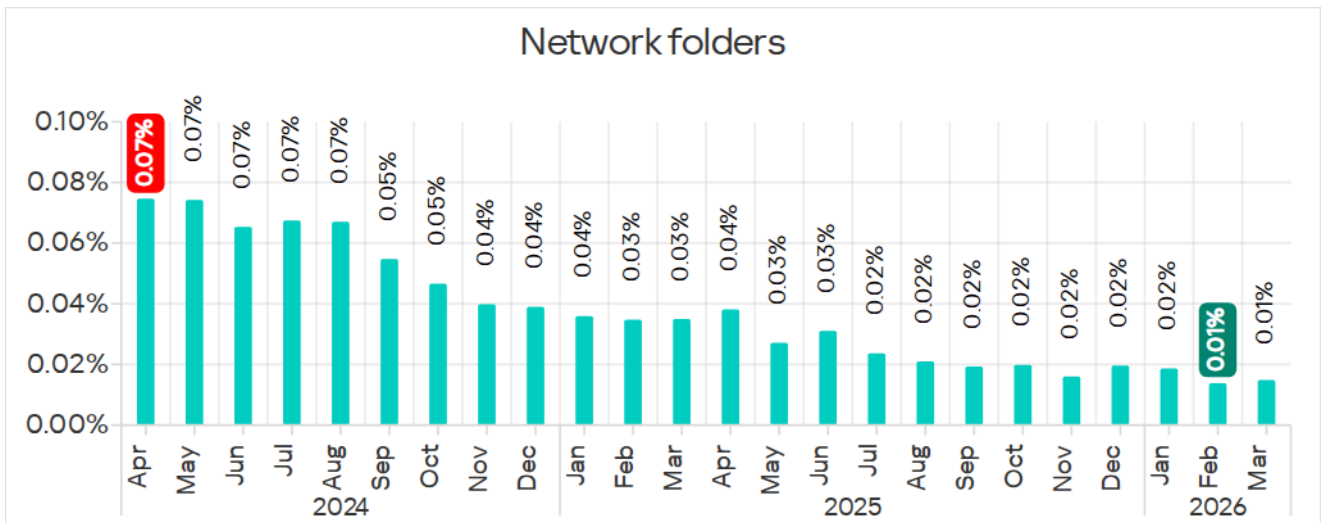
Changes in percentage of ICS computers on which threats from removable media were blocked, Q1 2026



Network folders

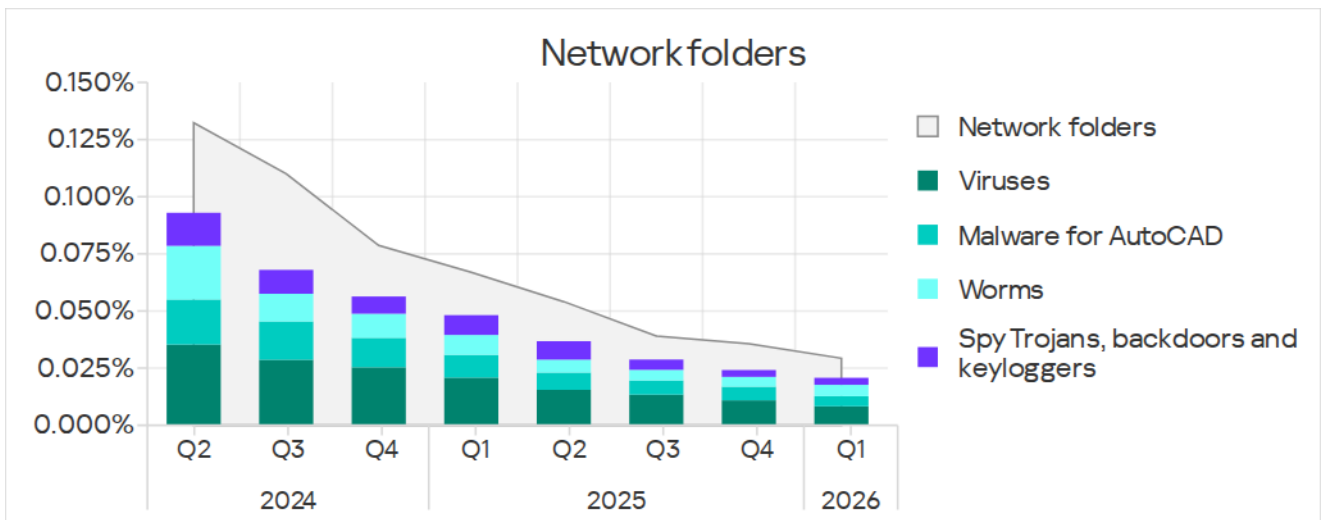
Percentage of ICS computers on which threats from network folders were blocked, Q1 2023 – Q1 2026





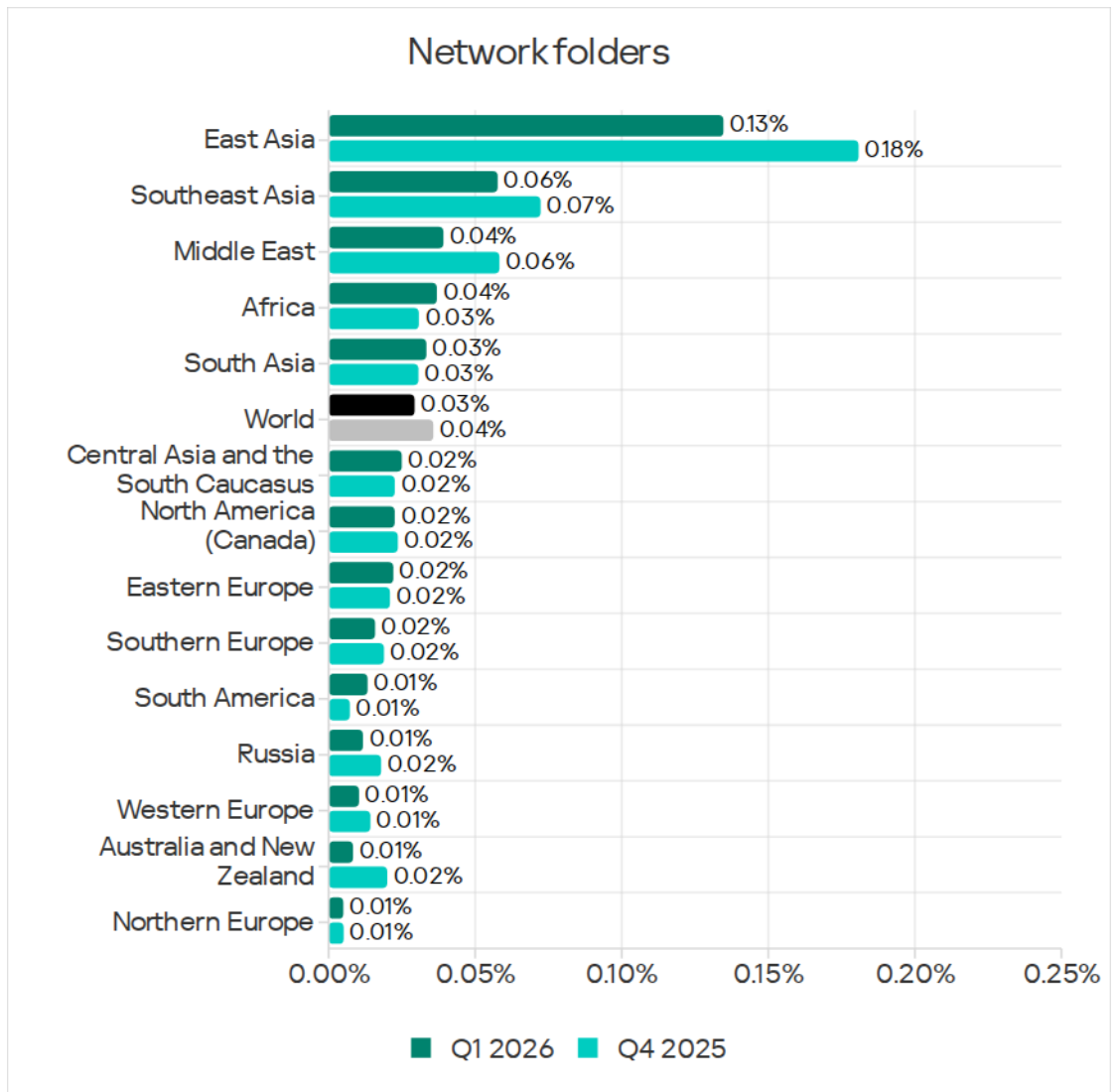
Percentage of ICS computers on which threats from network folders were blocked, April 2024 – March 2026

The main categories of threats distributed via network folders in Q1 2026 were viruses, malware for AutoCAD, worms, and spyware.

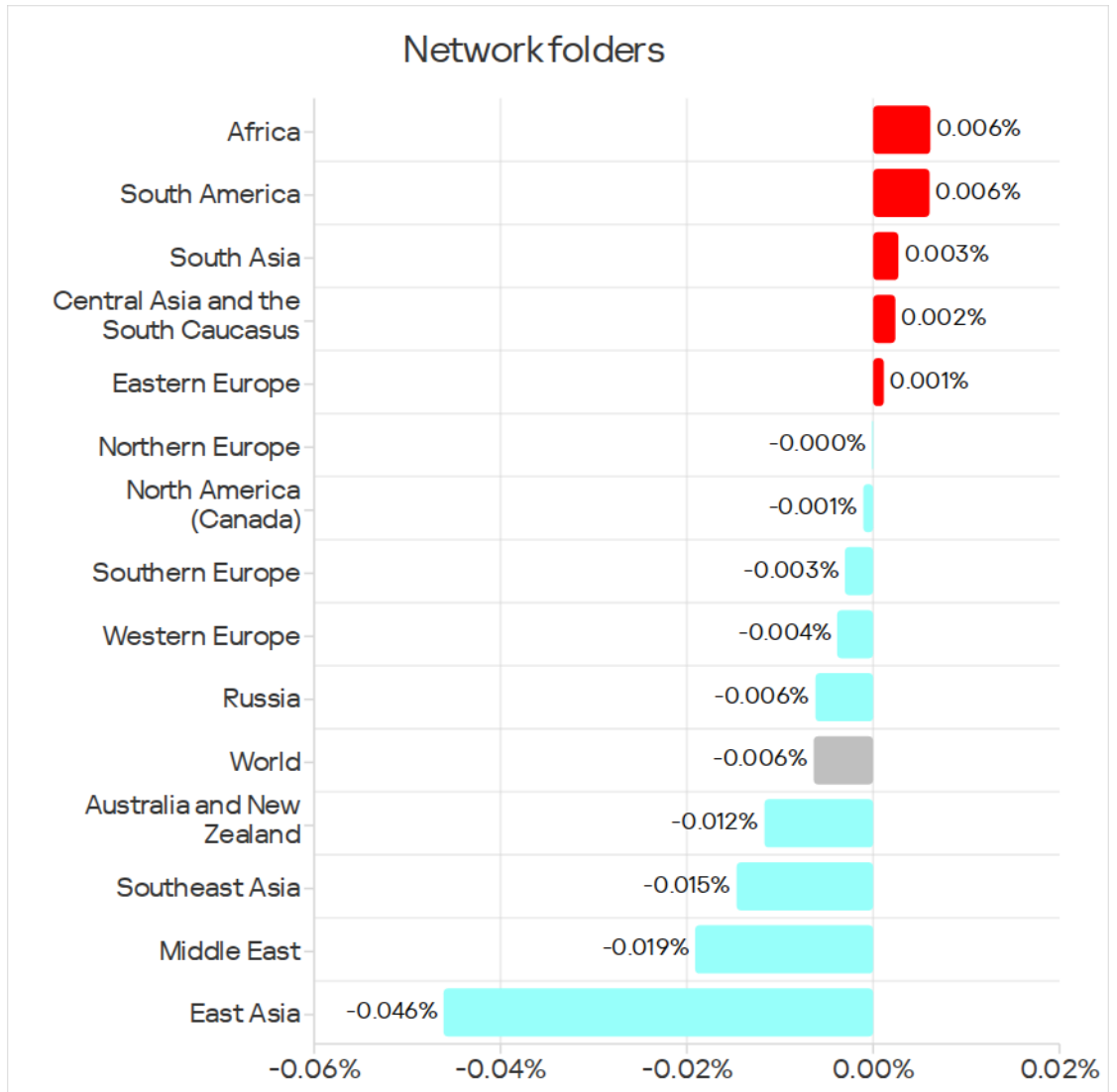


Threats from network folders and main categories of threats from network folders, Q2 2024 – Q1 2026

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



Changes in percentage of ICS computers on which threats from network folders were blocked, Q1 2026



Methodology used to prepare statistics

This report presents the results of analyzing statistics obtained with the help of a distributed antivirus network called the [Kaspersky Security Network \(KSN\)](#). The data was received from KSN users who confirmed their voluntary consent to share data anonymously and to have it processed 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 APTs¹.

Statistical data presented in the report was obtained from ICS computers that were protected with Kaspersky products and categorized by Kaspersky ICS CERT 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 OT 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, and pharmaceuticals. This also includes systems from engineering and integration firms that work with enterprises in a variety of industries, as well as building management systems, physical security, and biometric data processing.

¹ We recommend that organizations that have any restrictions in place with respect to transferring data outside the organization's perimeter consider using the [Kaspersky Private Security Network](#) service.

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