Kaspersky ICS CERT

kaspersky

Threat landscape for industrial automation systems

Asia. Q4 2025

27.04.2026

Version 1.0

Southeast Asia

Key cybersecurity issues in the region

A significant part of the infrastructure is unprotected, becoming a source of secondary infection (malware propagation)

Southeast Asia has high rates of self-propagating malware.

The region ranked first in the world in terms of the percentage of ICS computers on which viruses and malware for AutoCAD were blocked. In both cases, it led by a wide margin.

In most cases, malware for AutoCAD is distributed in the same way as viruses. This explains the high percentage exhibited by this malware category.

In Southeast Asia, viruses ranked second in the regional ranking of malware categories by percentage of ICS computers on which they were blocked. This was the highest position for viruses among all regional threat category rankings. Viruses ranked sixth in the corresponding global rankings, and they ranked sixth or seventh in most regions.

In Southeast Asia, the figure for viruses exceeded the global average by a factor of 5.2 and was the highest in the world.

Lack of segmentation in enterprise networks in the region

With its rate of 0.07%, Southeast Asia ranked second among regions based on the percentage of ICS computers on which threats were blocked in network folders. This figure was higher than the global average by a factor of 1.8.

This was primarily because of the situation in Vietnam, which led by a wide margin among countries of the region in terms of viruses, malware for AutoCAD, and second in terms of network folder threats.

Availability of internet resources on OT computers

In Q4 2025, Southeast Asia ranked second by the percentage of ICS computers on which internet threats were blocked, and ranked first for denylisted internet resources and web miners.

Cybercriminals use denylisted internet resources primarily for malware distribution, for phishing attacks, and as command and control (C2) infrastructure. A significant percentage of these resources is used for spreading malicious scripts and phishing pages (HTML).

High figures for this threat category are normally determined by the following:

- Weak control over the implementation of information security policies (ICS computers are internet-facing in some capacity).
- Failings in the information security culture (employees access unsafe internet resources).

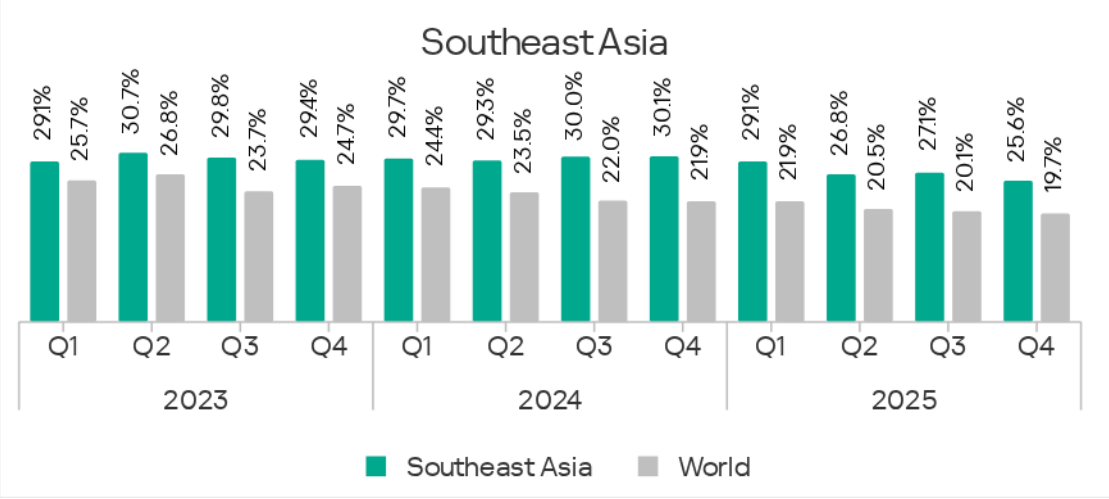
One distinguishing feature of this region is that the internet here is used not only to distribute threats that are typical for this threat source, but also to distribute viruses and malware for AutoCAD. These threat categories are distributed in Southeast Asia through all sources, but most frequently over the internet.

Vietnam, which led the rankings of countries for many threat categories, also ranked first for internet threats.

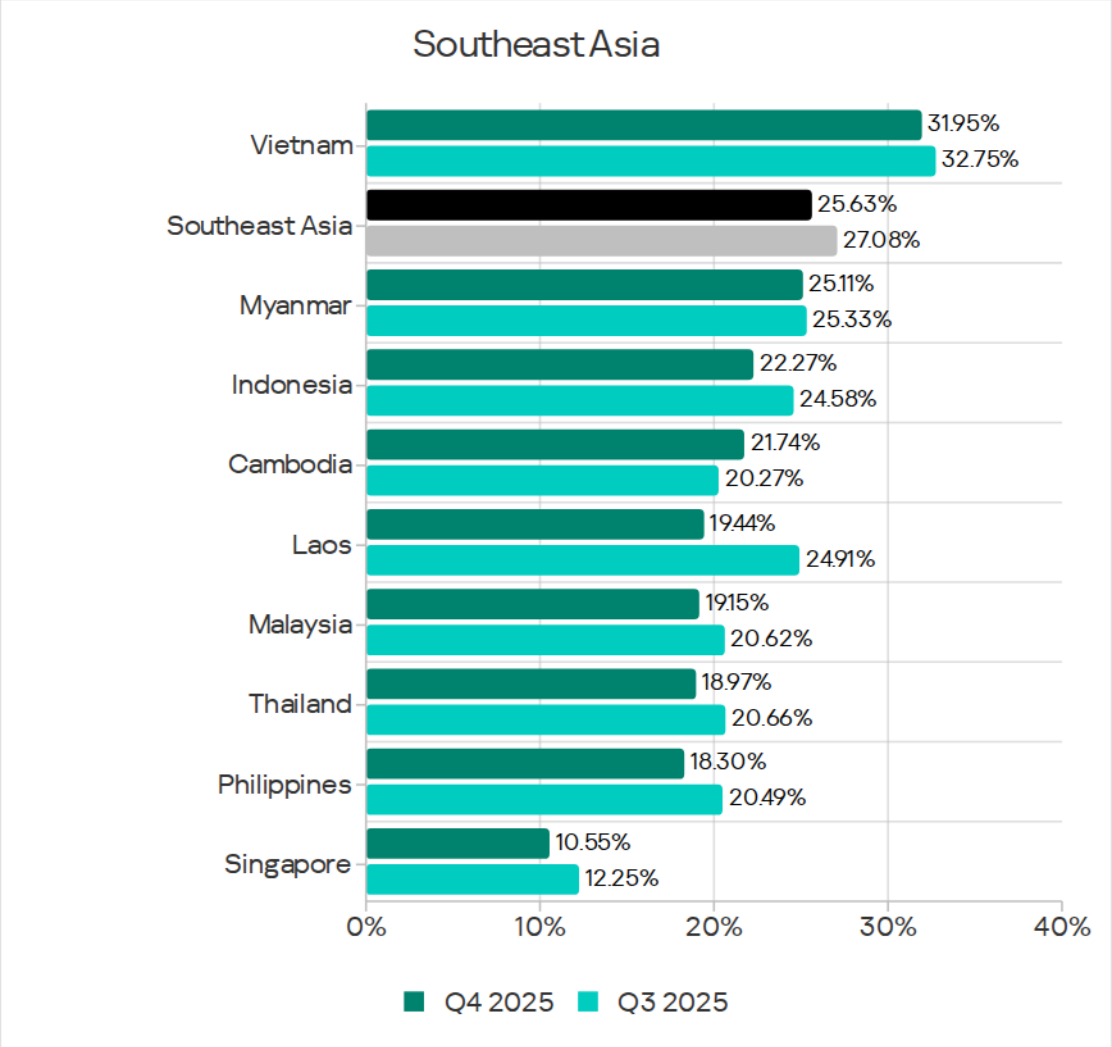
Statistics across all threats

With its rate of 25.6%, Southeast Asia ranked second globally based on the percentage of ICS computers on which malicious objects were blocked. This figure was 1.3 times higher than the global average and three times higher than the minimum figure among regions as recorded in North Europe.

After the figure for the region grew during the previous quarter, in Q4 2025 the percentage of ICS computers on which malicious objects were blocked in Southeast Asia decreased.



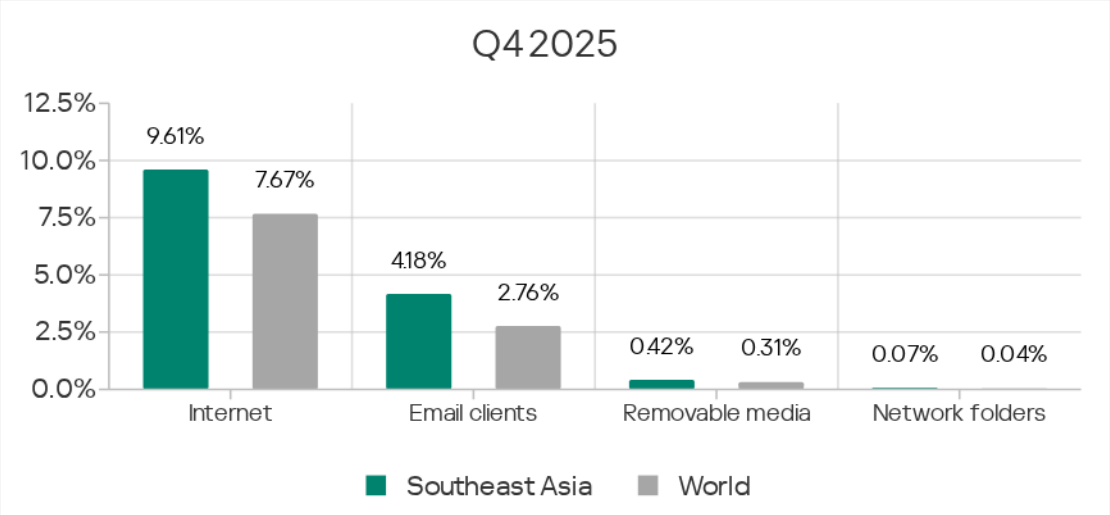
The percentage of ICS computers on which malicious objects were blocked varied among the region's countries, ranging from 10.55% in Singapore to 31.95% in Vietnam. Other countries' rates fell between 18% and 26%.



Threat sources

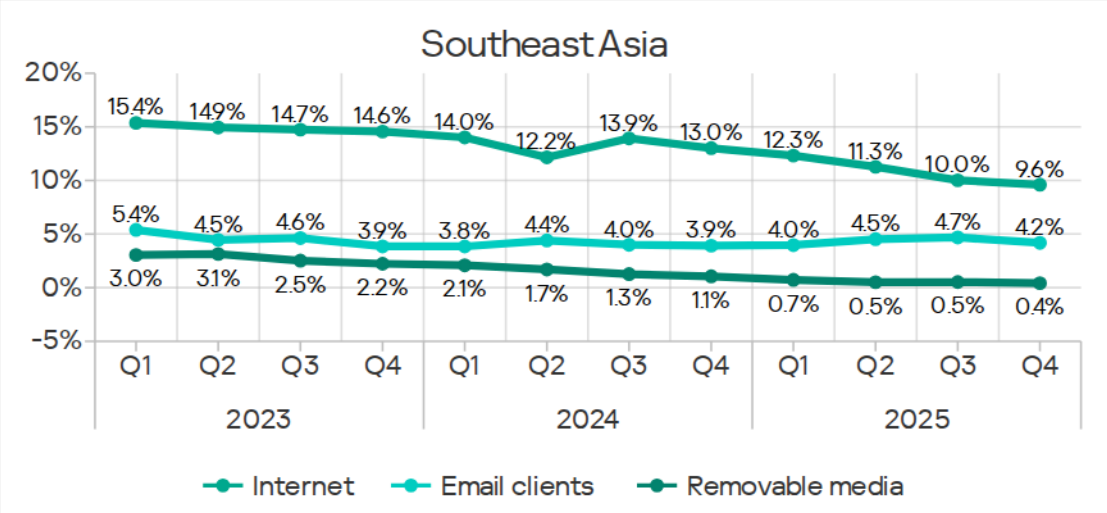
The percentage of ICS computers on which threats were blocked in the Middle East was higher than the global average across almost all sources.

- Internet: 1.3 times higher.
- Email clients: 1.5 times higher.
- Removable media: 1.4 times higher.
- Network folders: 1.8 times higher.



Southeast Asia came second in the corresponding rankings of regions for internet threats and network folder threats.

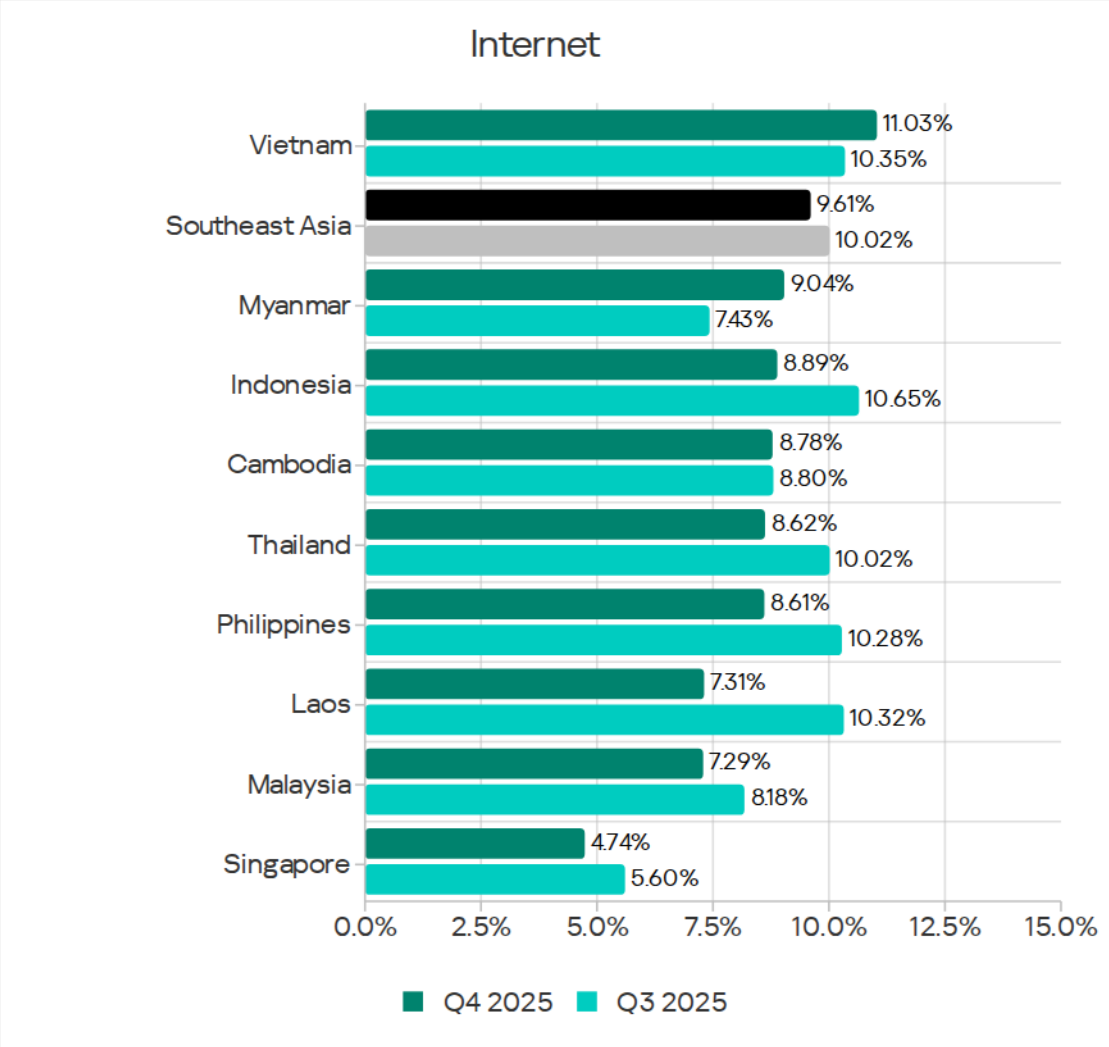
In Q4 2025, the figure decreased across all threat sources.



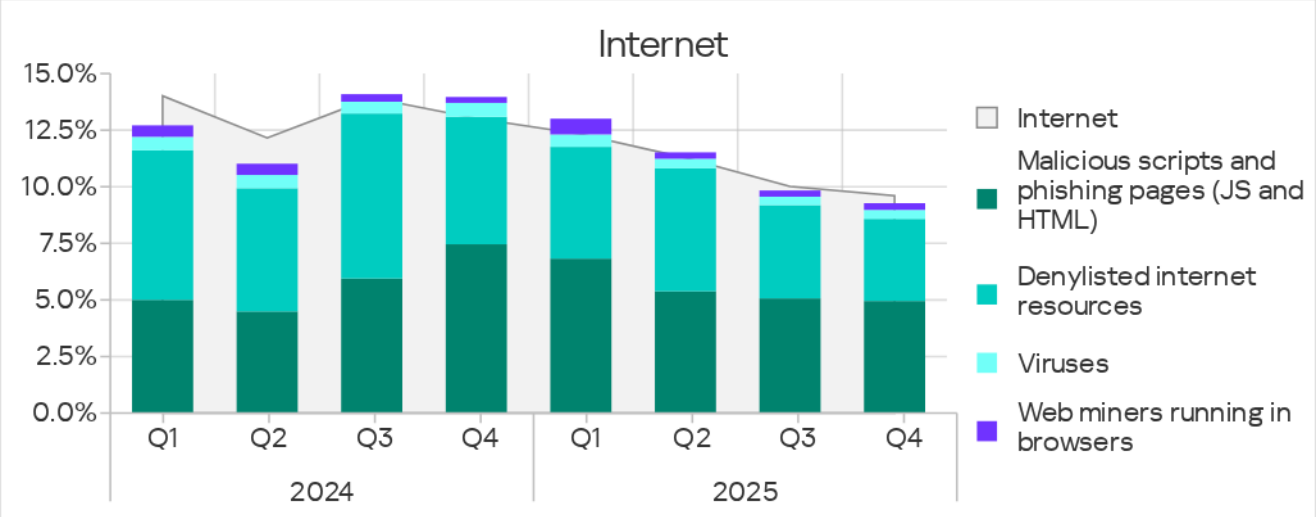
Internet

Based on the percentage of ICS computers on which internet threats were blocked, Southeast Asia ranked second among regions with a figure that exceeded the minimum (North Europe) by a factor of 2.4.

The indicators for countries in the region ranged from 4.74% in Singapore to 11.03% in Vietnam.



The main categories of internet threats blocked on ICS computers in the region were malicious scripts and phishing pages, denylisted internet resources, viruses, and web miners. Southeast Asia leads all the regions in terms of the metrics for viruses and web miners.

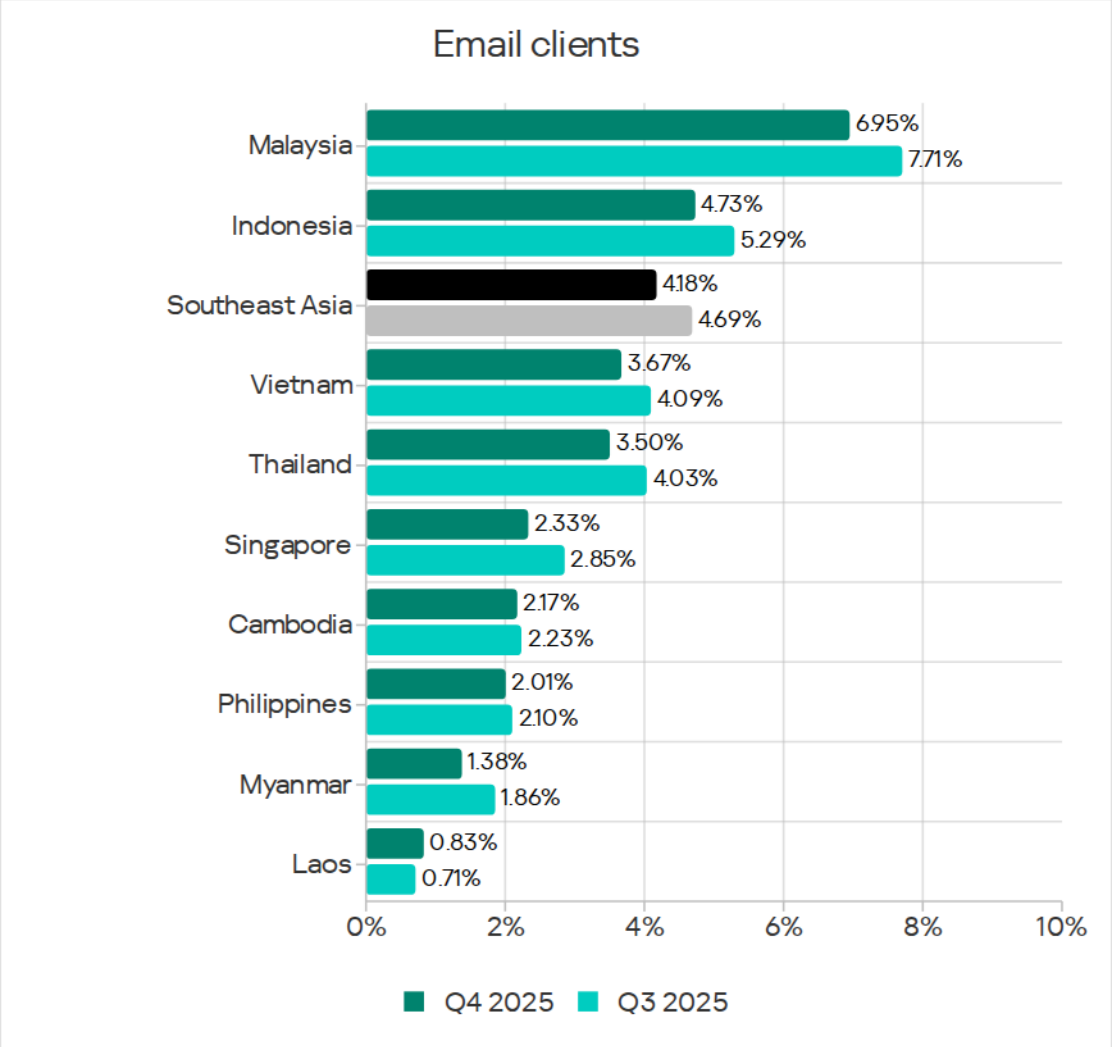


Email clients

Based on the percentage of ICS computers on which email client threats were blocked, Southeast Asia ranked fourth in the rankings of regions, with 4.18%. This figure was 6.5 times higher than in Northern Europe, which had the lowest percentage value.

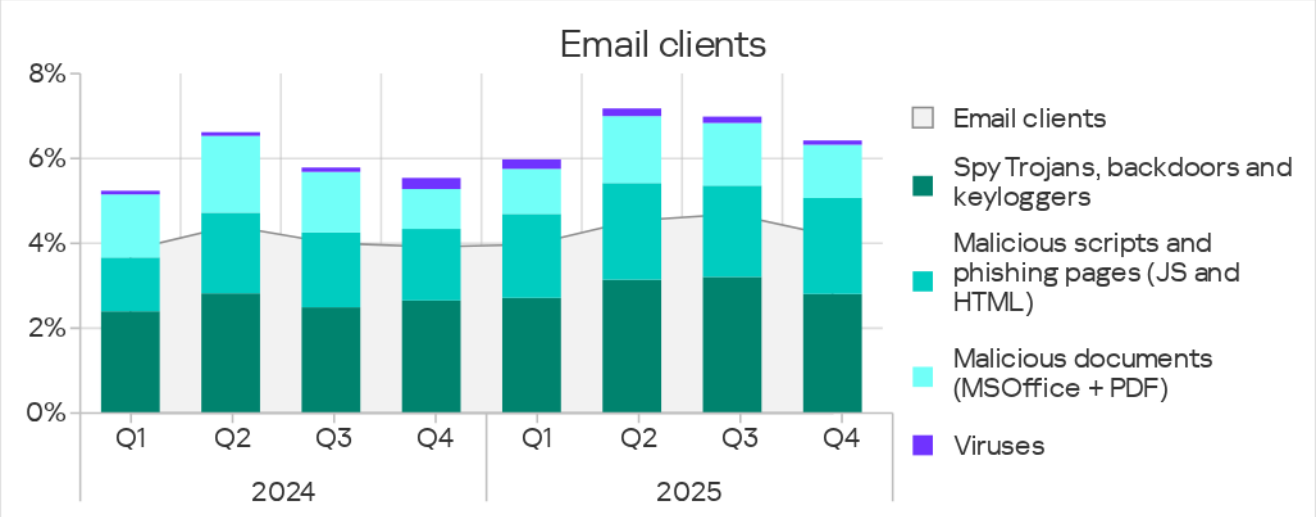
Since 2024, the trend for email clients in the region has matched the average global trend for this metric. In Q4 2025, this figure decreased after growing over the three previous quarters.

Among countries in the region, Malaysia led by a noticeable margin in this metric, with 6.95%. The lowest figure, 0.83%, was observed in Laos.



The main categories of email-borne threats blocked on ICS computers were spyware, malicious scripts and phishing pages, and malicious documents.

Email is the region's main channel for spyware distribution. Southeast Asia ranked second among all regions for spyware.



Q4 2025 saw a noticeable increase in the percentage of ICS computers on which worms from email clients were blocked. This was connected with the latest wave of phishing campaigns known as Curriculum-vitae-catalina, which launched attacks against organizations across all regions of the world. In Southeast Asia, these attacks peaked in November.

The hackers distributed phishing emails disguised as job applications. Disguised as a resume (Curriculum Vitae), these emails contained a malicious executable file, a remote administration backdoor worm known as Backdoor.MSIL.XWorm. Running that file caused system infection.

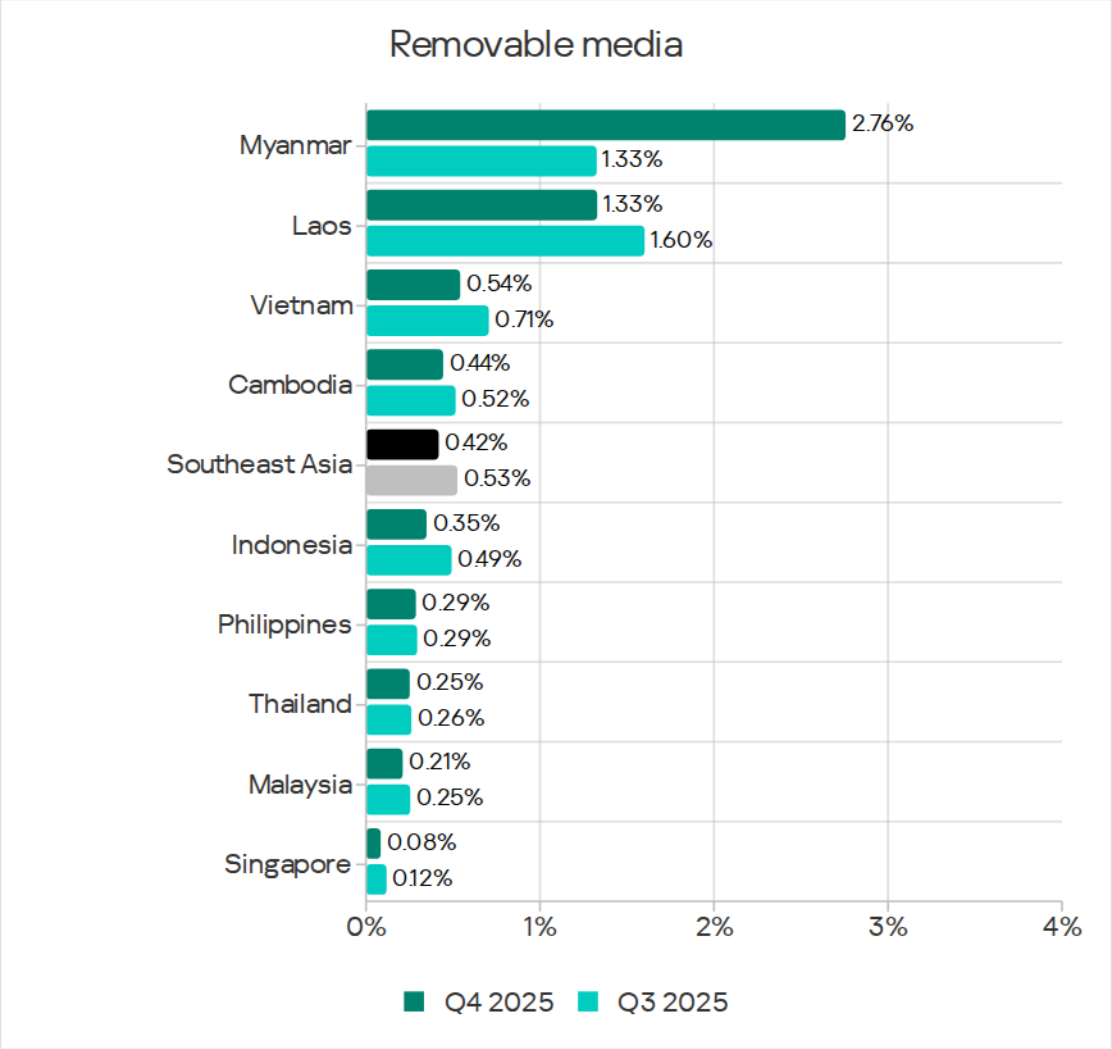
Normally, these campaigns are designed to deliver malware for data theft, spyware, or remote administration tools (RATs).

Removable media

Southeast Asia ranked sixth among regions based on the percentage of ICS computers on which removable media threats were blocked upon connection. Notably, the first six positions in this ranking were held by the Asia, Africa, and Middle East regions with figures that fell within the range of 0.42% to 1.41%, while the figures for all other regions did not exceed 0.19%.

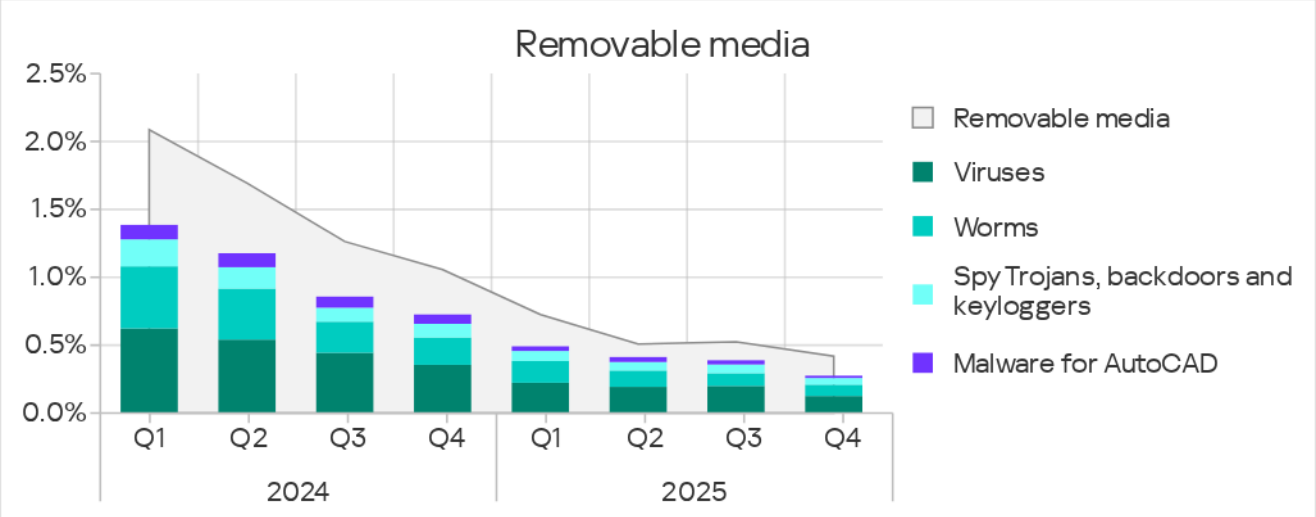
The percentage of ICS computers where threats were blocked when connecting removable media in Southeast Asia decreased to 0.42%. This was 8.9 times higher than the Australia and New Zealand region, which ranked last.

Among the region's countries, Myanmar (2.76%) and Laos (1.33%) led all others by a wide margin. The lowest figure, 0.08%, was observed in Singapore.



The leaders in the removable media rankings, Myanmar and Laos, had the lowest figures for email client threats out of all countries in the region.

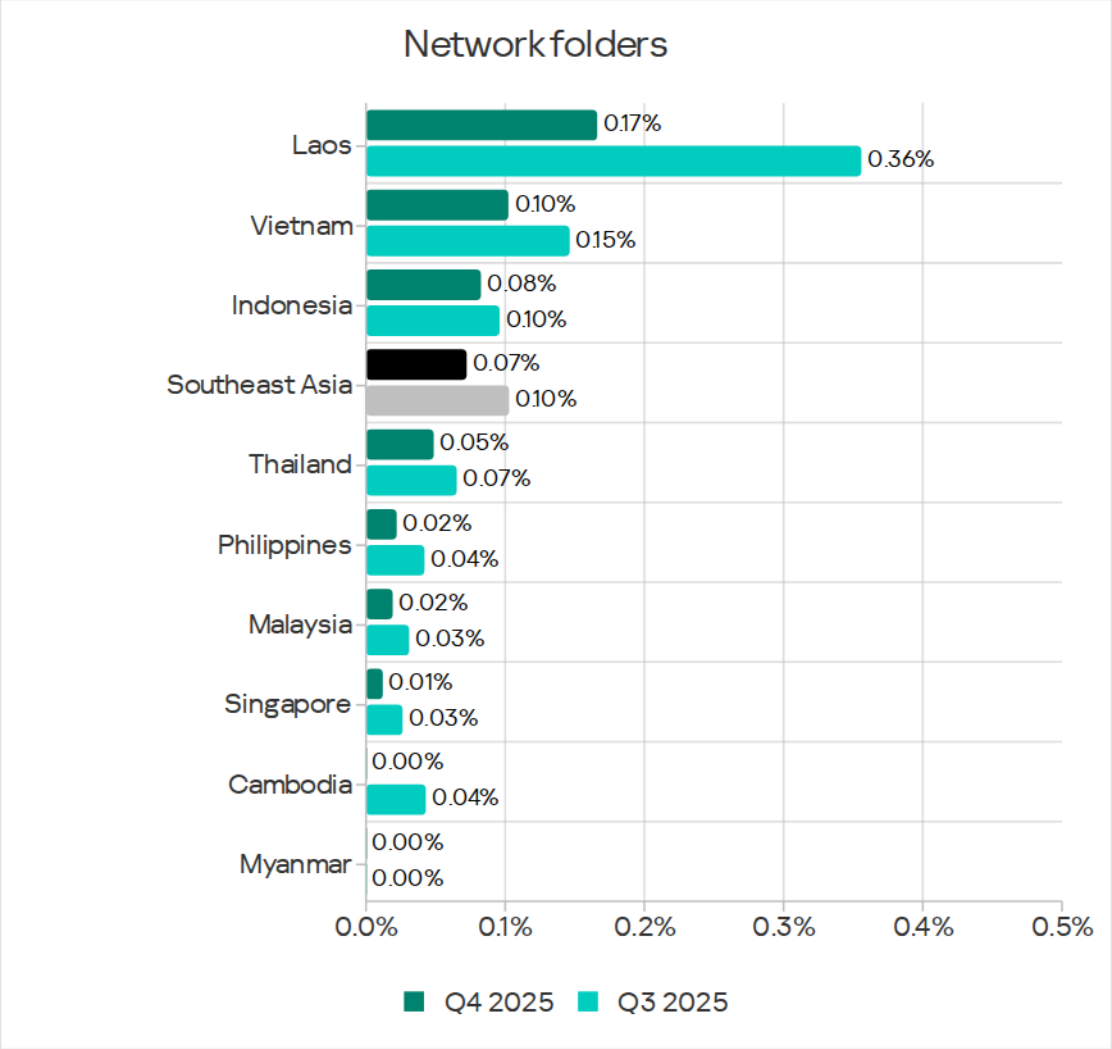
The main categories of threats blocked when connecting removable devices to ICS computers were viruses, worms, and spyware. In terms of viruses, Southeast Asia led all the regions by a wide margin.



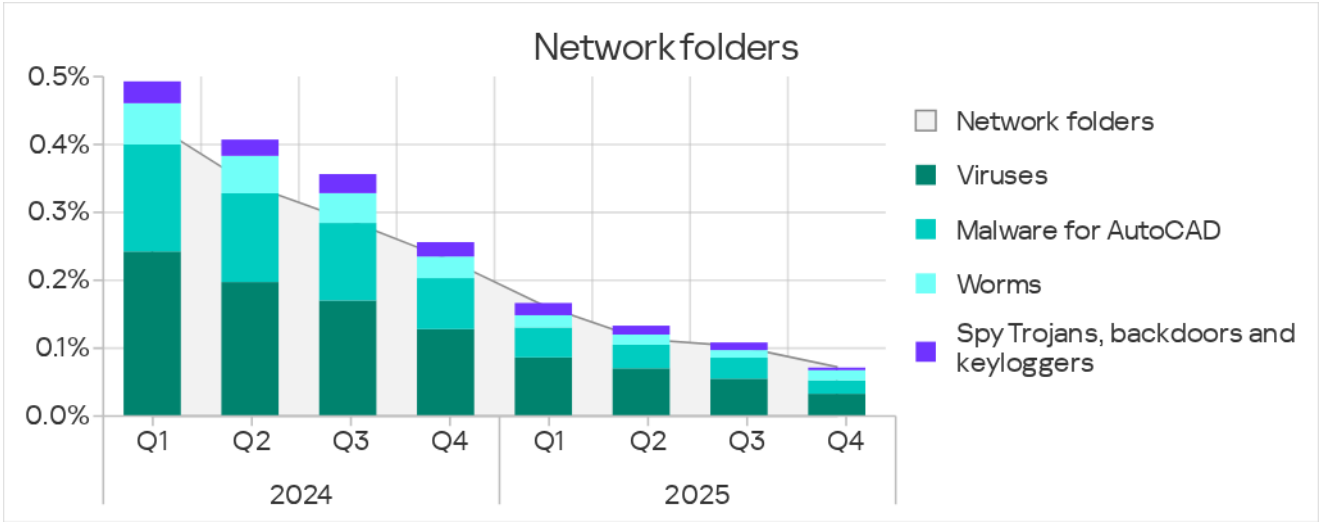
Network folders

With its rate of 0.07%, Southeast Asia ranked second among regions based on the percentage of ICS computers on which threats were blocked in network folders. The rate is 7.0 times higher than Northern Europe, which ranked last.

Among countries in the region, Laos at 0.17% led in Q4 2025 by a noticeable margin in the percentage of ICS computers on which network folder threats were blocked. The figures decreased across all countries in the region where network folder threats were blocked.



The main categories of threats that spread via network folders in Q4 were viruses, malware for AutoCAD, and worms. In terms of malware for AutoCAD, Southeast Asia led the ranking of regions by a wide margin.



Threat categories

In Southeast Asia, the percentage of ICS computers on which malicious objects were blocked was higher than the respective global averages for all threat categories except two (miners in the form of executable files for Windows, and ransomware).

The region's figures exceeded the global averages most substantially in the following threat categories:

- Web miners: 1.5 times higher.
- Spyware: 1.5 times higher.
- Viruses: 5.3 times higher.
- Malware for AutoCAD: 7.0 times higher.

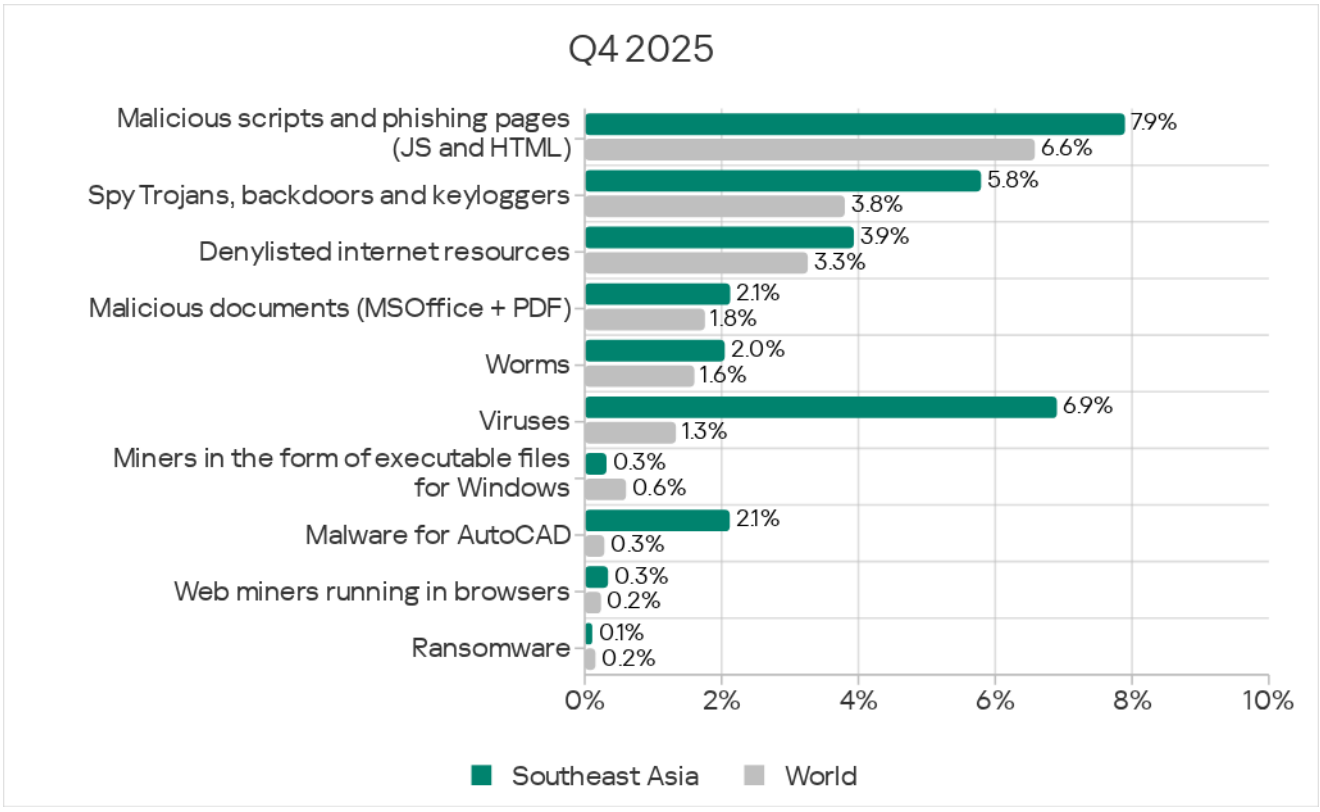
In Q4 2025, Southeast Asia ranked first among regions in the following categories:

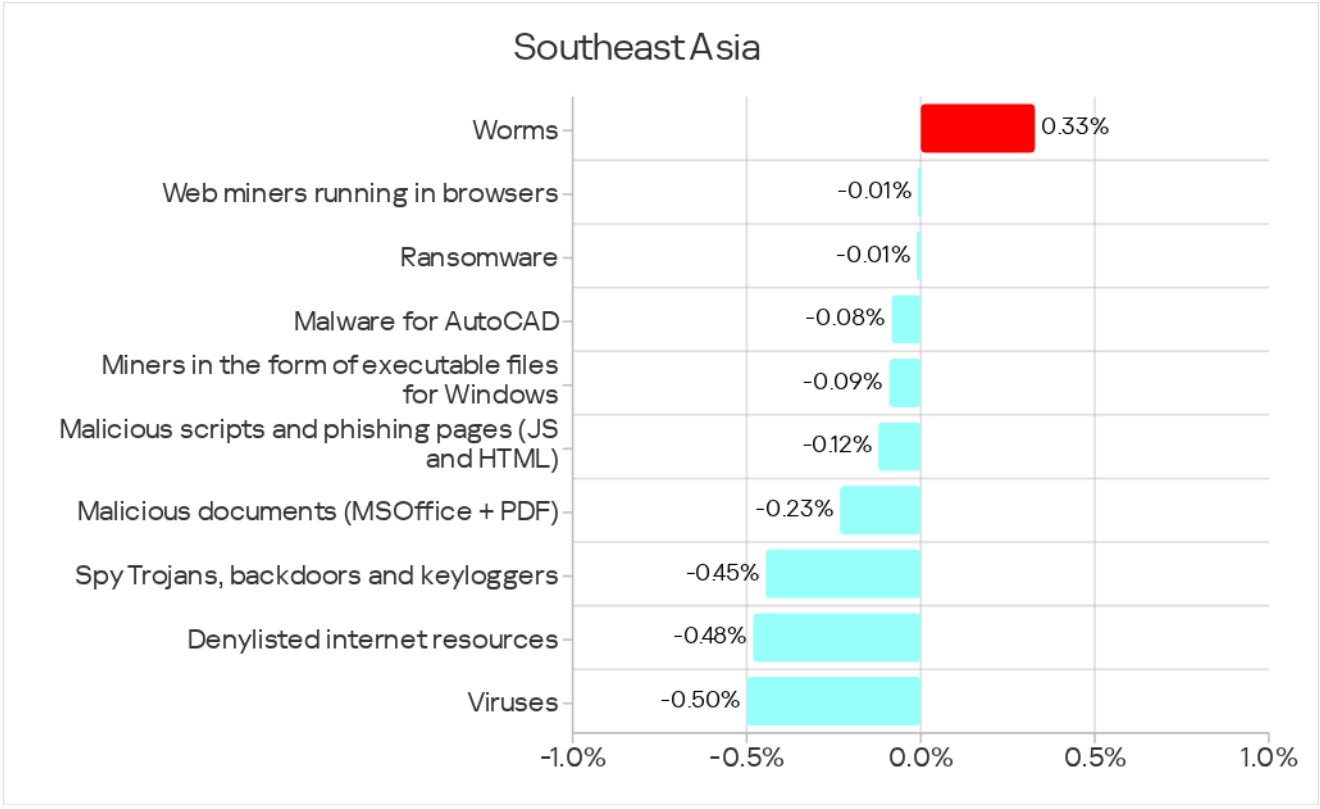
- Denylisted internet resources
- Web miners.
- Viruses.
- Malware for AutoCAD.

It should be noted that the main source of all threats listed above was the internet, and Southeast Asia ranked second for internet threats.

The region ranked second for spyware. Email was the main channel for spreading this threat.

In Southeast Asia, viruses ranked second among all threat categories. This was the only region where this threat category was so high.

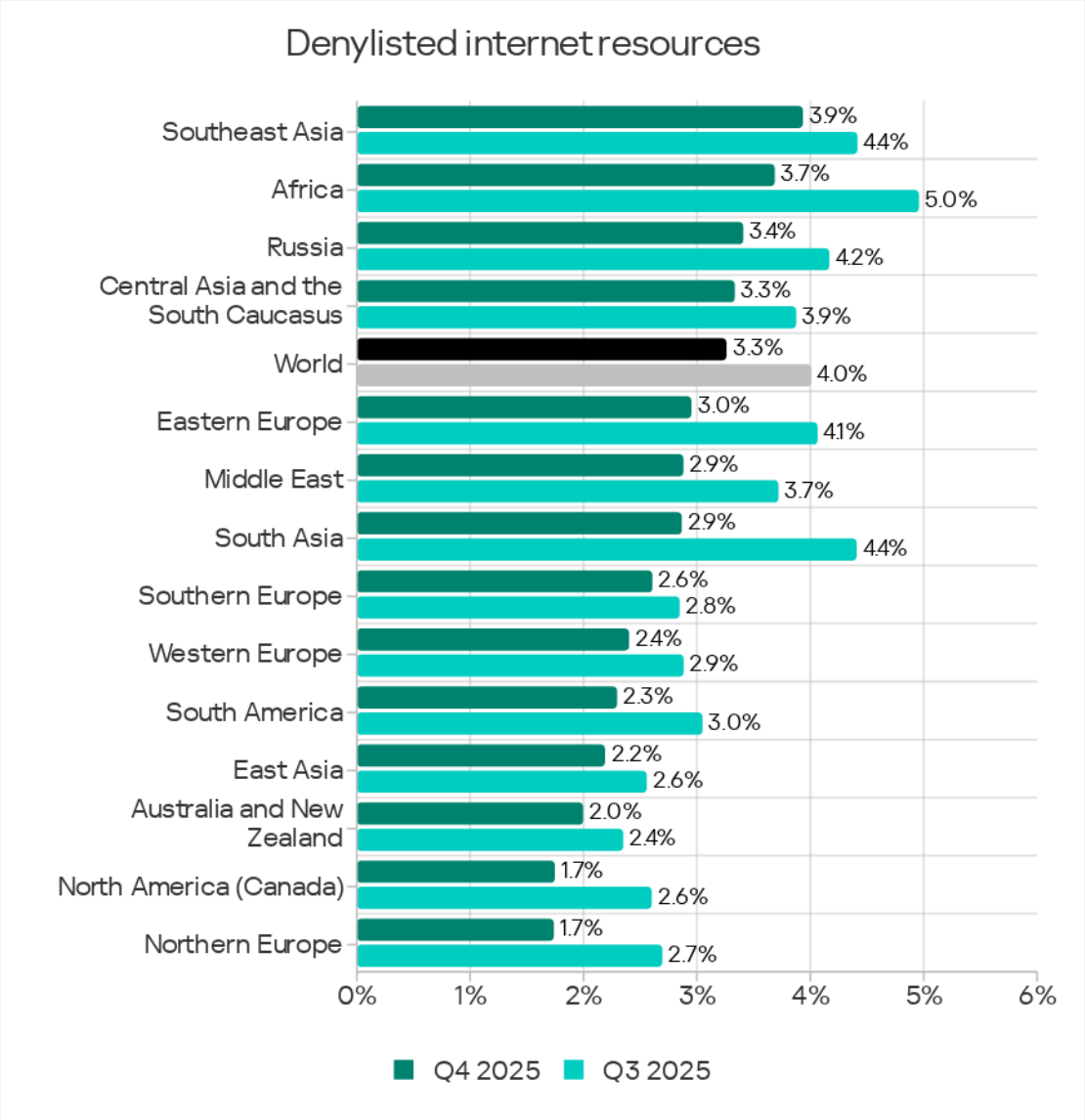




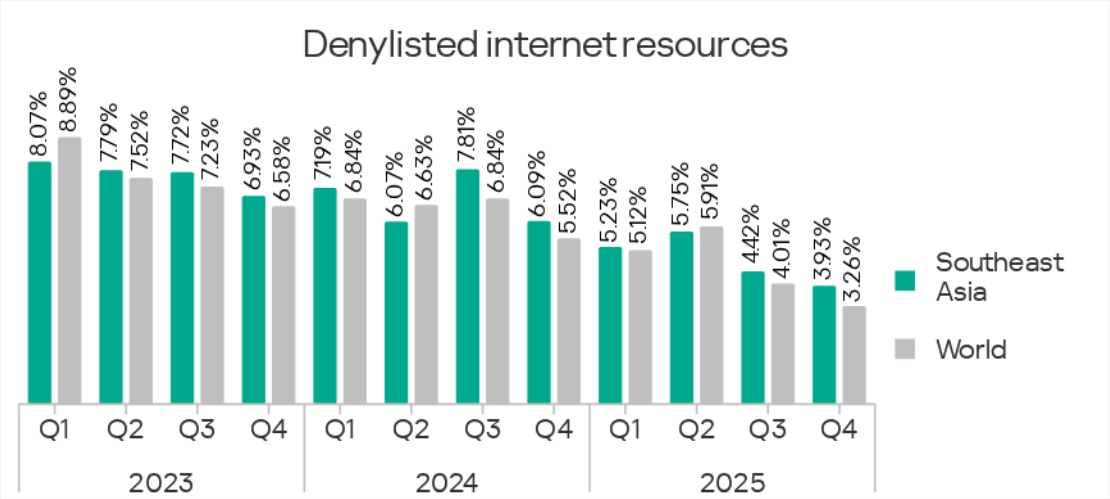
Of all the threat categories we tracked in Q4, this metric increased only for worms.

Denylisted internet resources

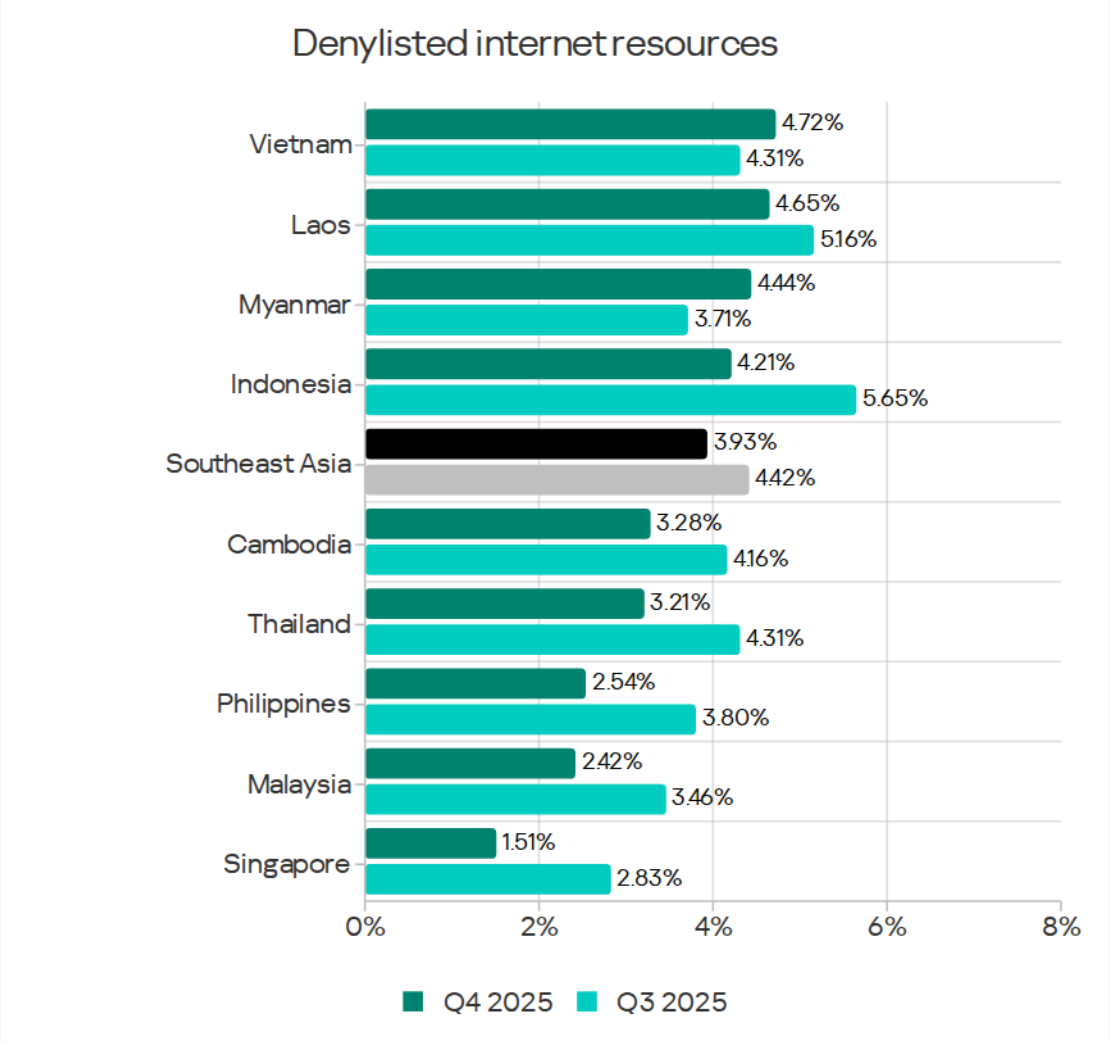
In the Q4 2025 rankings of regions for the percentage of ICS computers on which denylisted internet resources were blocked, Southeast Asia overtook Africa to take first place with 3.93%. This was 2.2 times higher than Northern Europe, which ranked last in this category.



This figure has declined in Southeast Asia for two consecutive quarters.

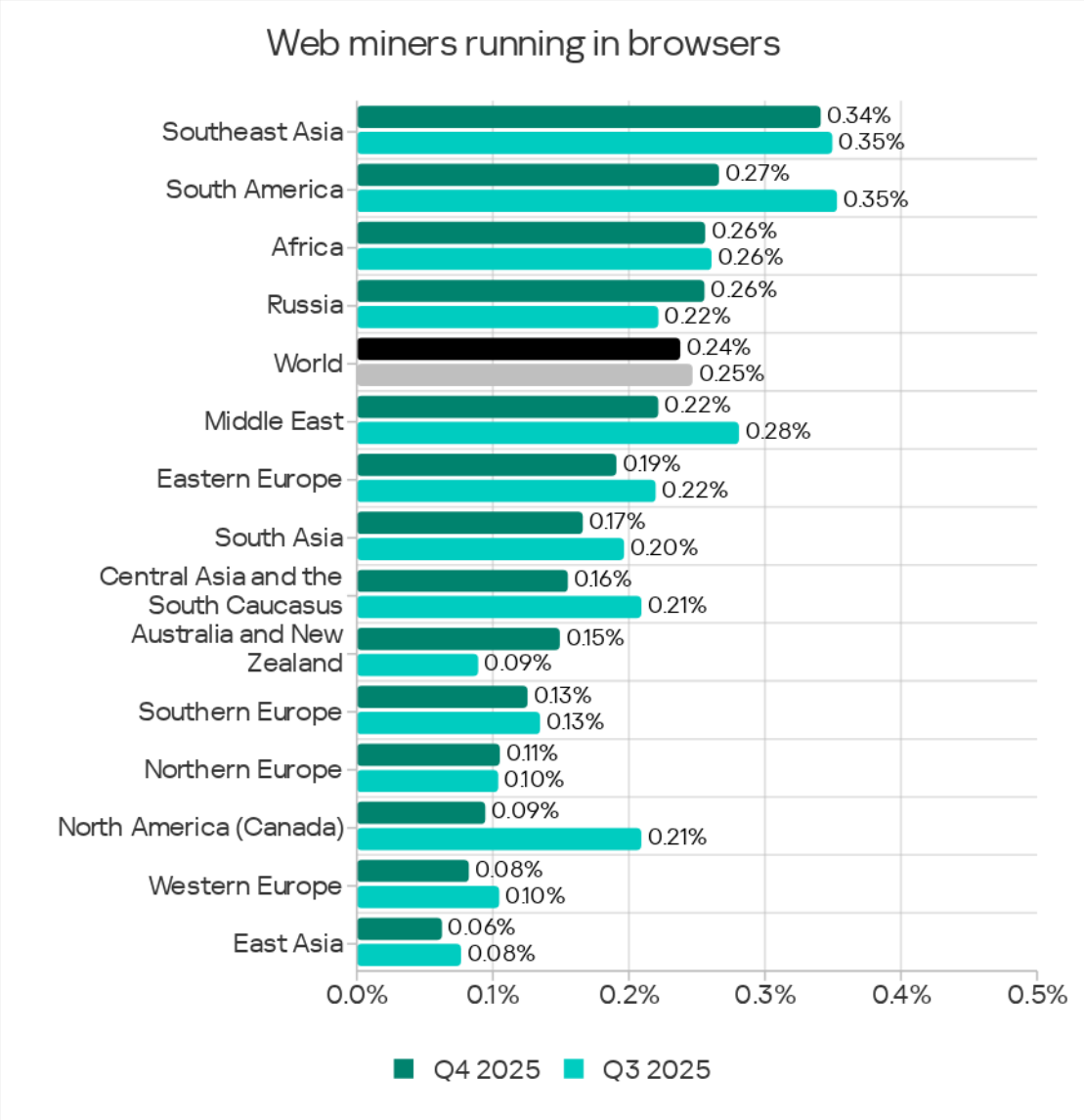


Among countries of the region, Vietnam led with 4.72% in the percentage of ICS computers on which denylisted internet resources were blocked. Singapore had the lowest rate at 1.51%.

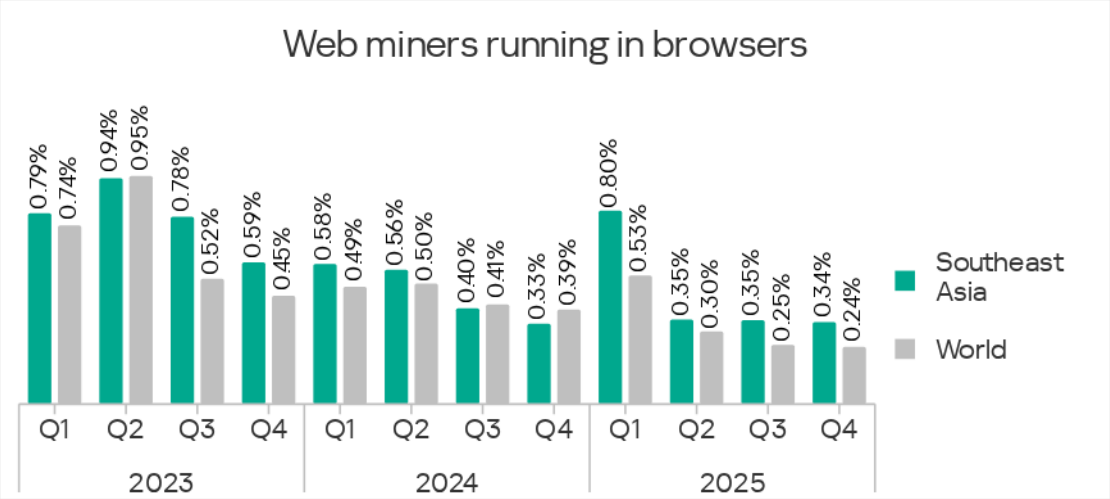


Web miners running in browsers

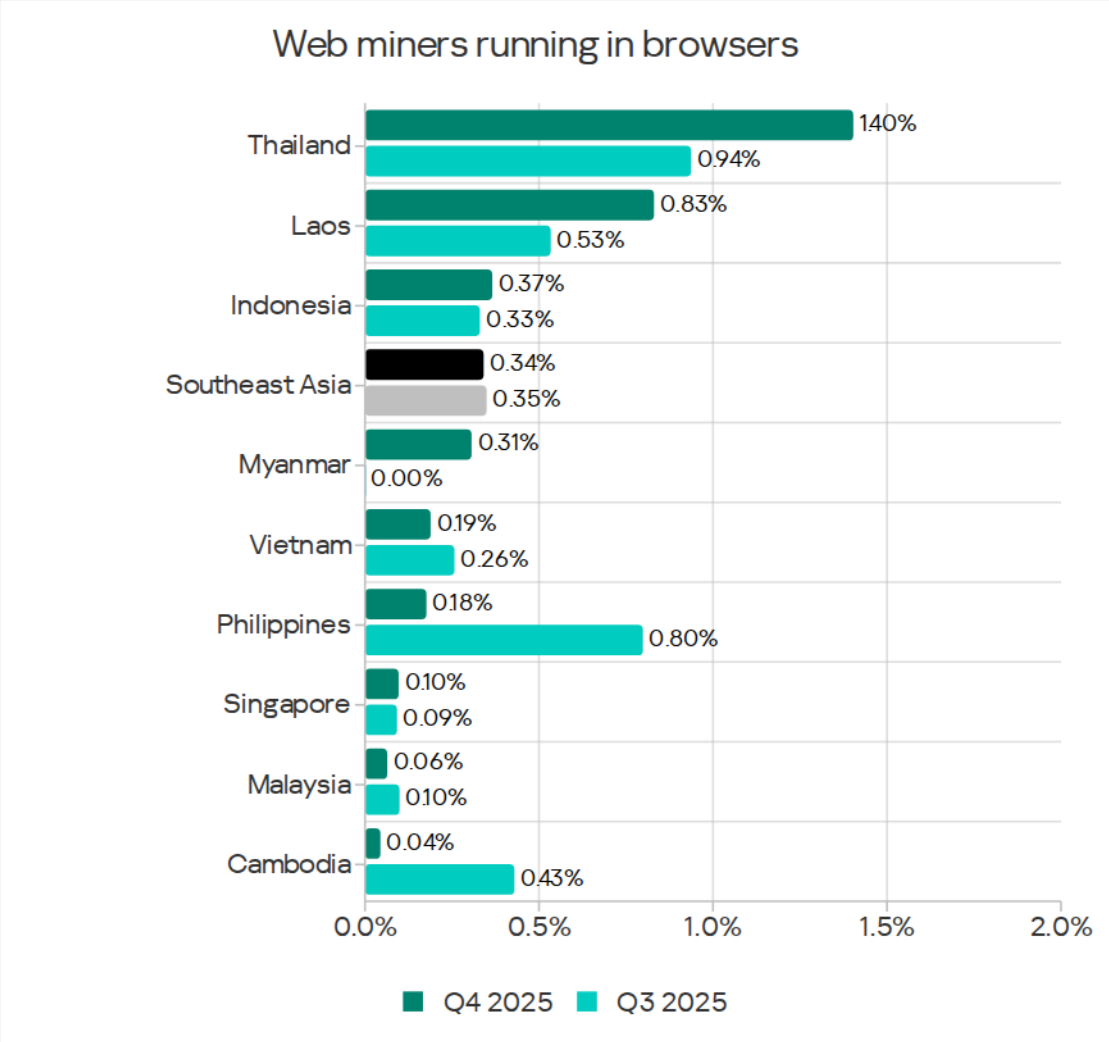
In Q4 2025, Southeast Asia led by the percentage of ICS computers on which web miners were blocked with 0.34%. This was 5.7 times higher than in East Asia, which ranked last.



This metric fluctuates in the region.



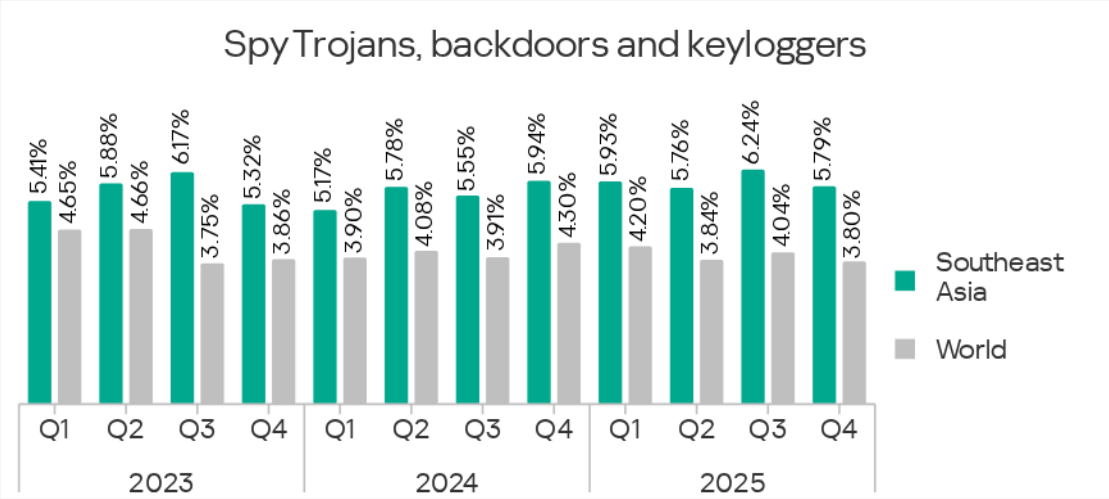
Among countries in the region, Thailand led by a wide margin with 1.40% in the percentage of ICS computers on which web miners were blocked.



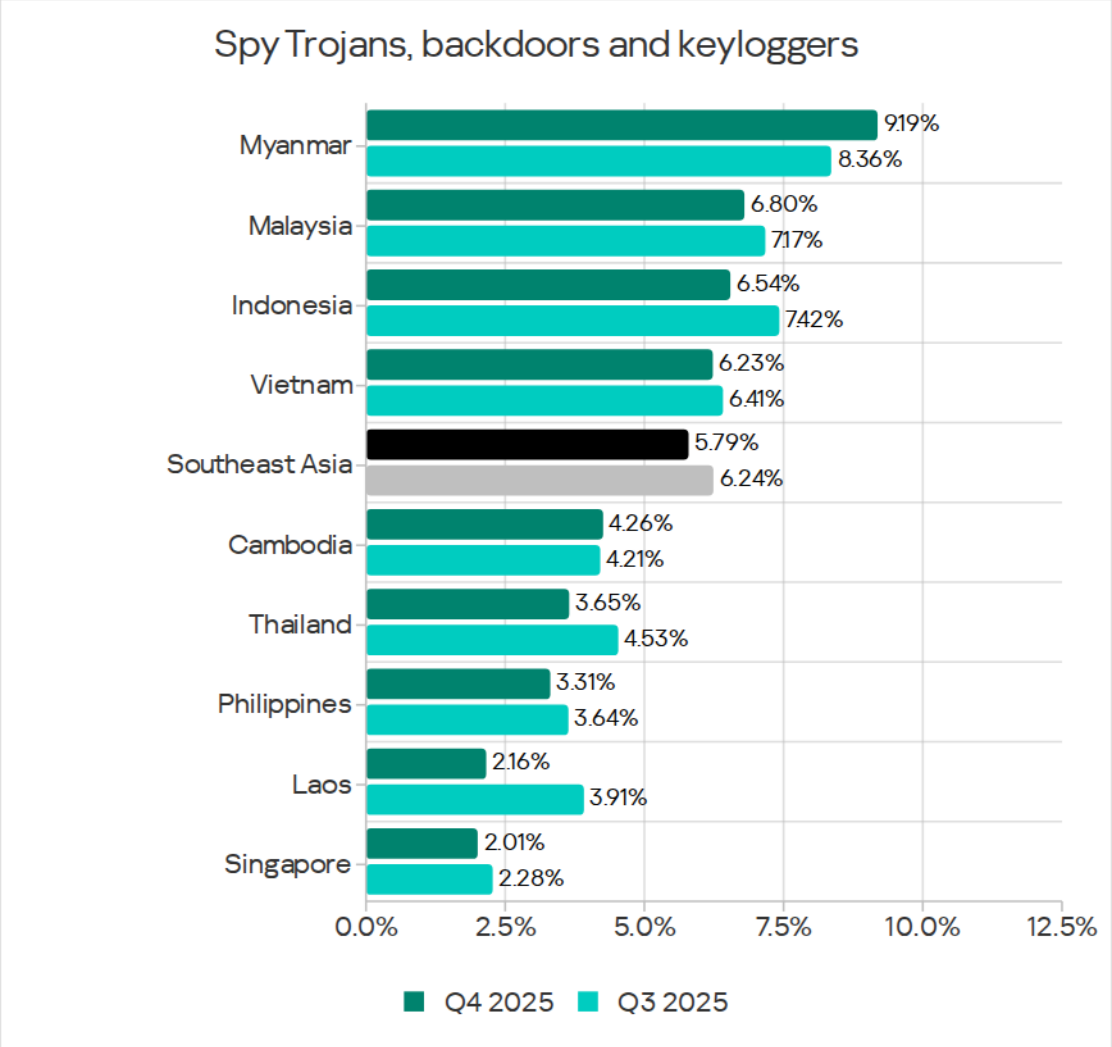
Spyware

In the rankings of regions for the percentage of ICS computers on which spyware was blocked, Southeast Asia took second place with 5.79% in Q4 2025. This figure was 4.6 times higher than in North Europe, which had the lowest percentage value.

In 2025, the figure for the region was relatively stable.



Among countries of the region, Myanmar led in the percentage of ICS computers where spyware was blocked with 9.19%. Singapore had the lowest rate at 2.01%.

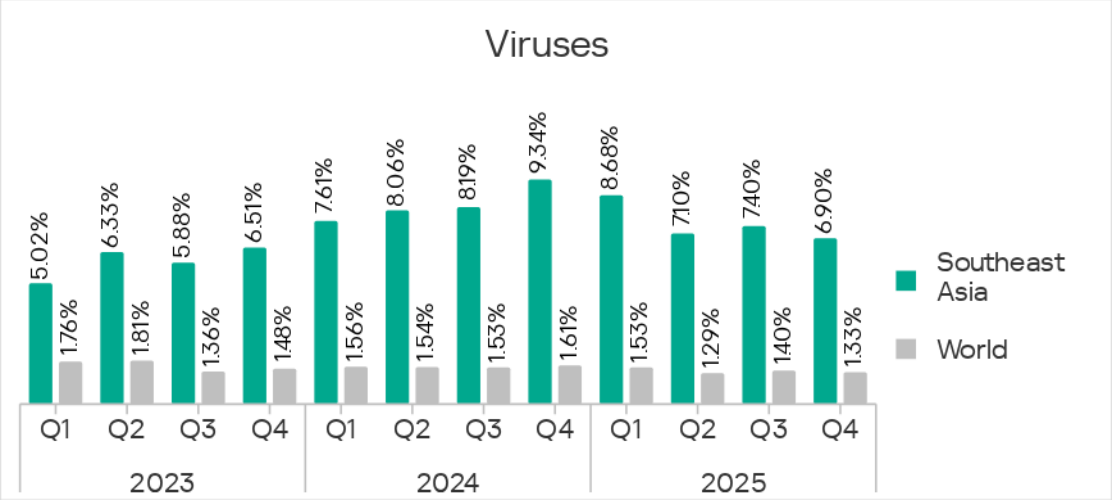


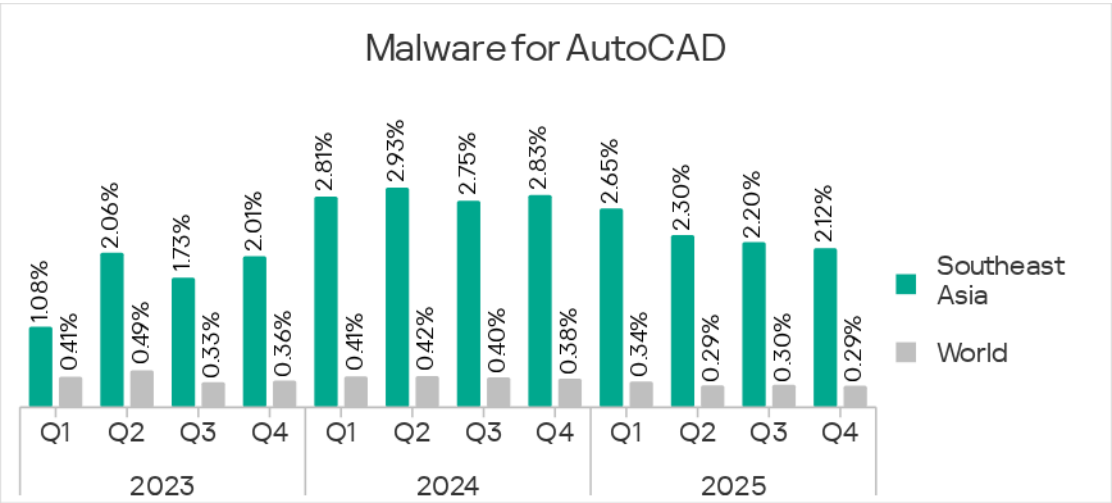
Although spyware was blocked in the region across all sources of threats, email was its main distribution channel. Malaysia, Indonesia, and Vietnam, which follow Myanmar in the ranking for spyware, were also the top three countries in the region for threats from email clients. However, in Myanmar the situation was different. Myanmar ranked second in the percentage of ICS computers on which threats were blocked when connecting removable media.

Viruses, and malware for AutoCAD

In most cases, malware for AutoCAD spreads in the same way as viruses — by infecting user files. This is why these two threat categories have much in common.

Although the figures for both categories grew noticeably in 2024, they clearly trended downward in 2025. In Q4 2025, the figures for both viruses and malware for AutoCAD were at their lowest since the beginning of 2024.

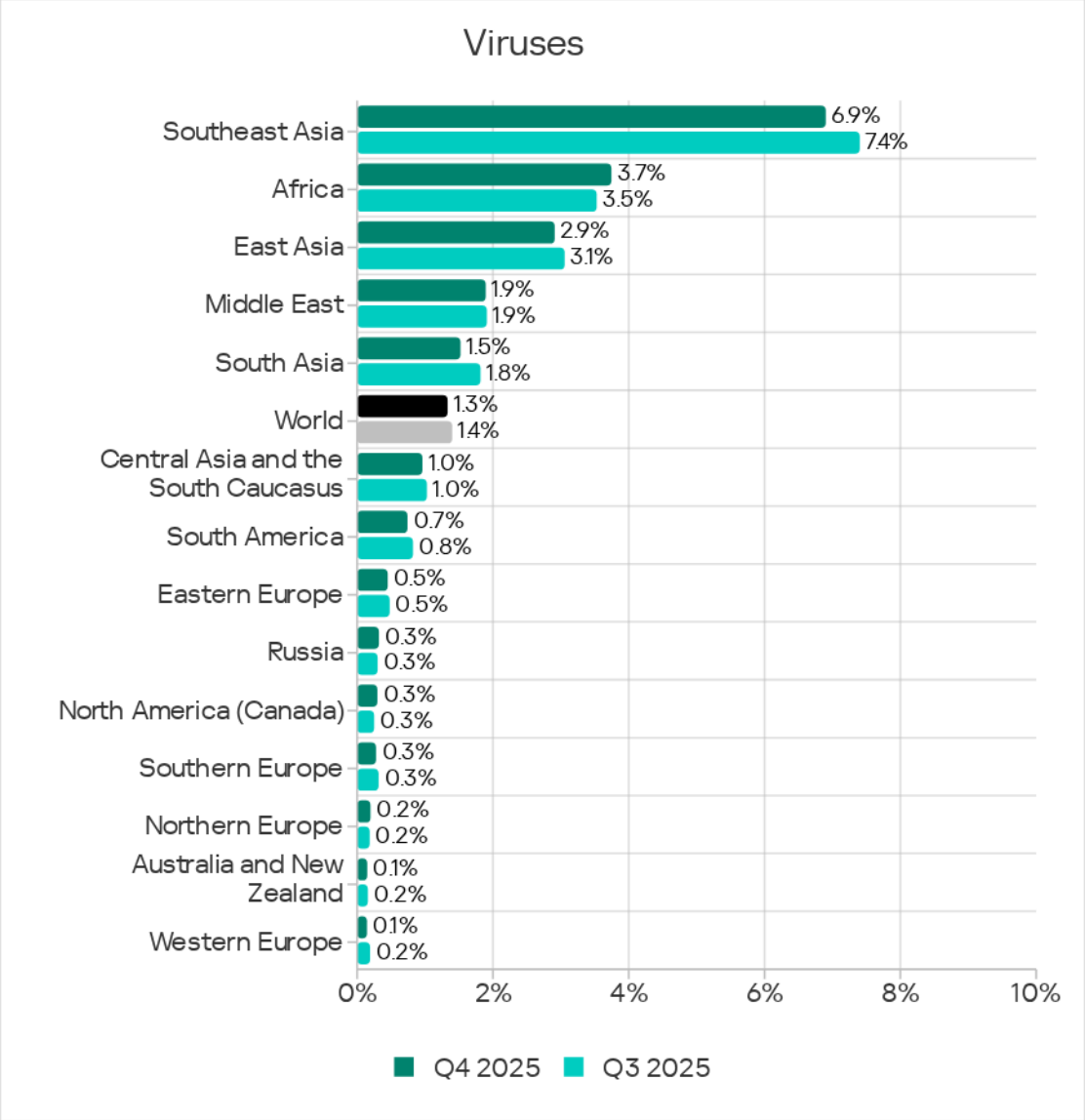




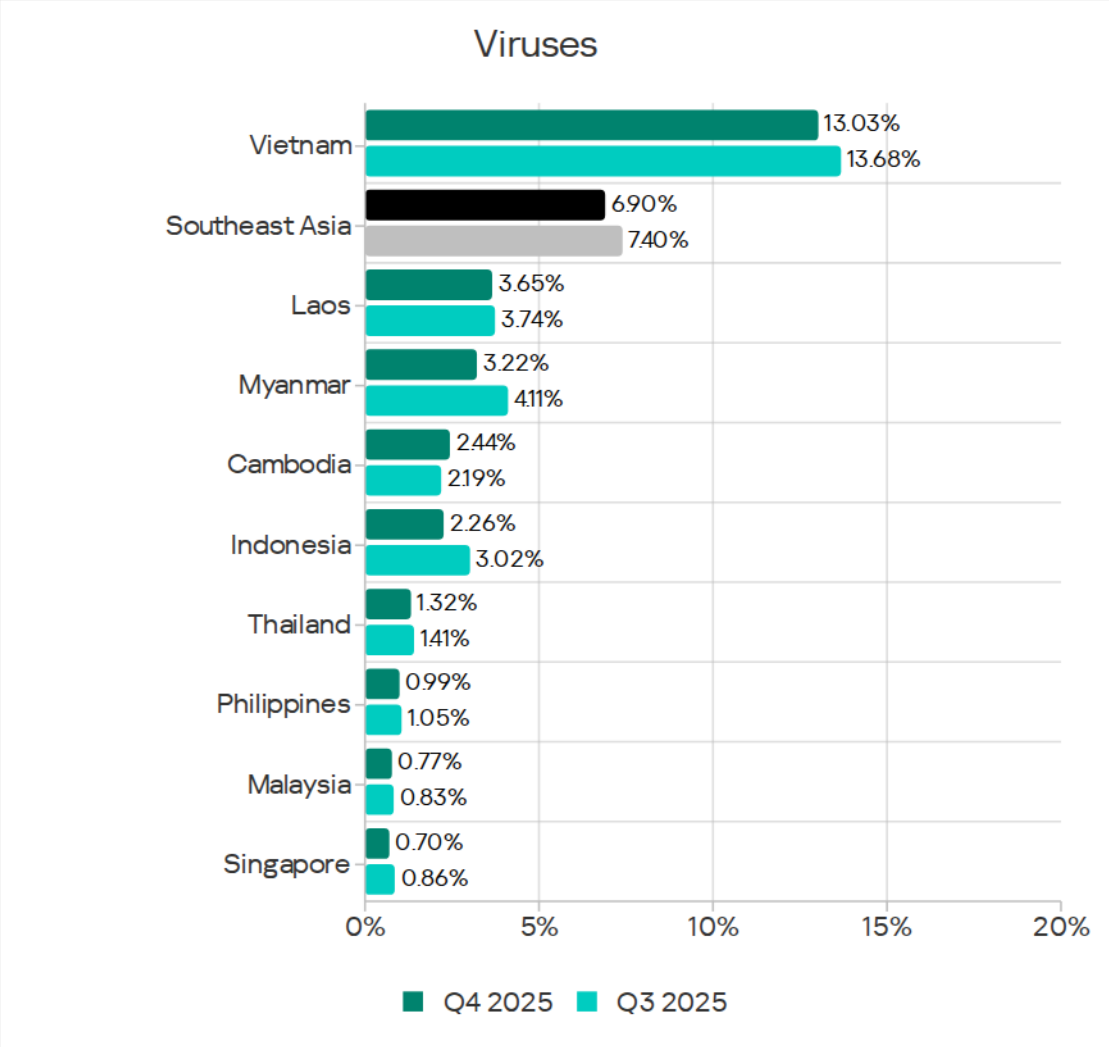
Viruses

Based on the percentage of ICS computers on which viruses were blocked, Southeast Asia led all other regions in these rankings by a huge margin, with 6.90%.

The figure in Southeast Asia was 1.8 times higher than in Africa (the next-ranked region), while it was 46 times higher than lowest-ranked Western Europe.



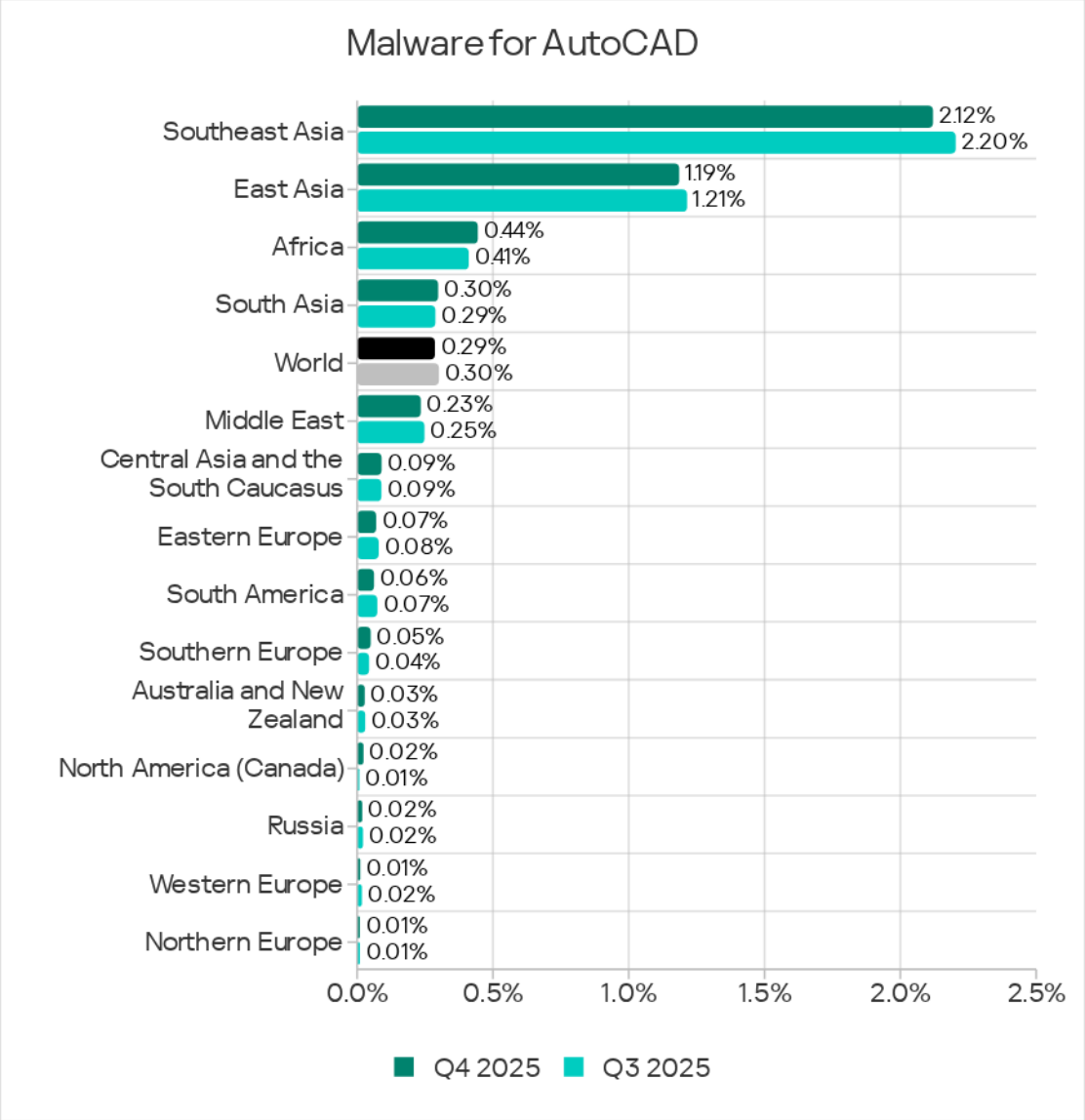
Such a strong lead for Southeast Asia was provided by Vietnam with its 13.0%. In this country, the indicator was 3.6 times higher than next-ranked Laos. Singapore had the lowest figure among the region's countries at 0.70%.



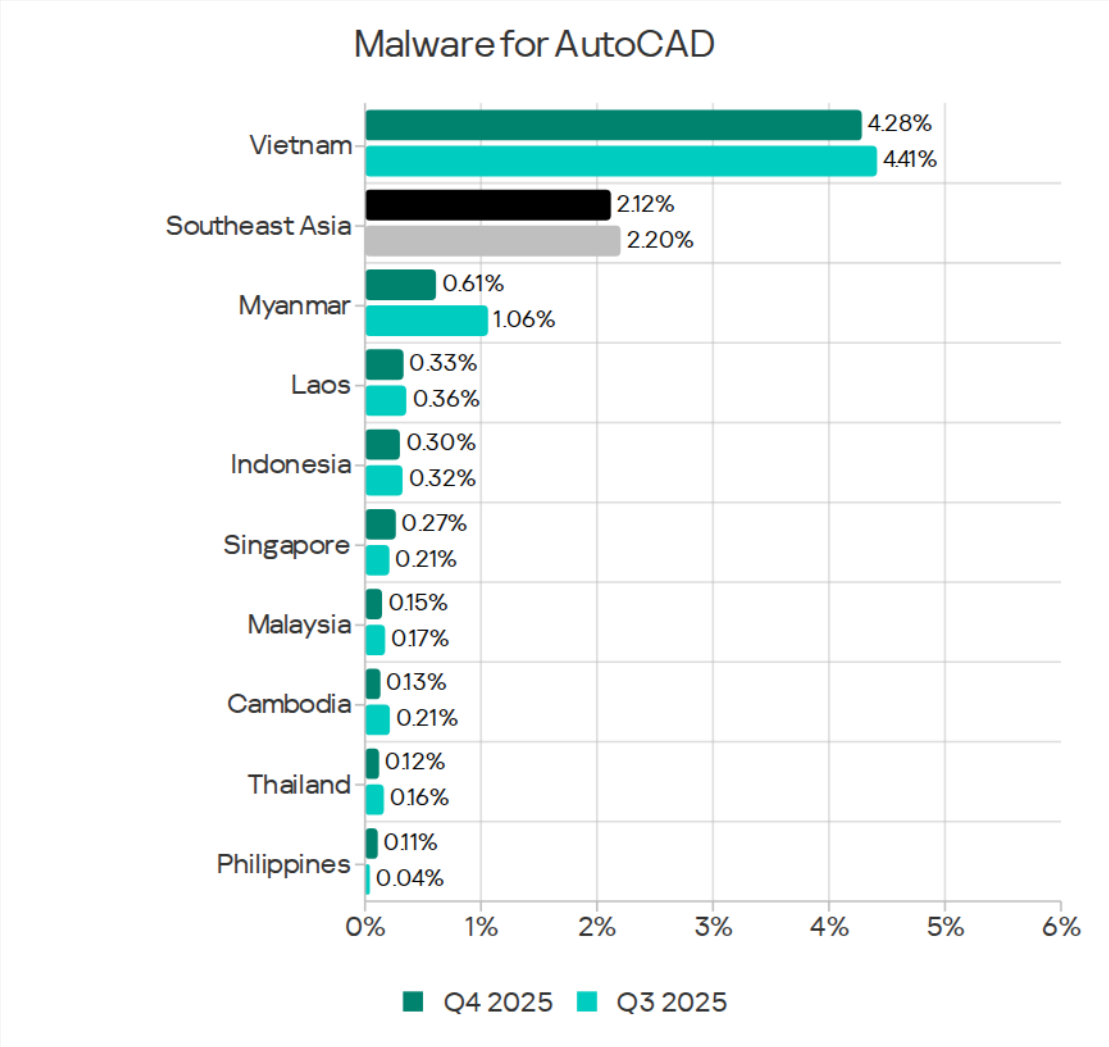
Viruses in the region are blocked across all sources of threats, but most frequently on the internet. It's worth noting that the most common category of viruses in Vietnam is MS Excel macroviruses (the first versions of these viruses appeared as early as 1997), and the largest industry in terms of percentage of detected viruses is construction. It seems that the root of the problem lies in infected Excel documents stored on file-sharing services and on the websites of various government agencies in Vietnam, such as district utilities and municipal services.

Malware for AutoCAD

In terms of the percentage of ICS computers on which malware for AutoCAD was blocked, Southeast Asia also led the corresponding ranking of regions by a wide margin. Southeast Asia's metric of 2.12% was 212 times(!) higher than the lowest figure among the regions, which was recorded in Northern Europe.



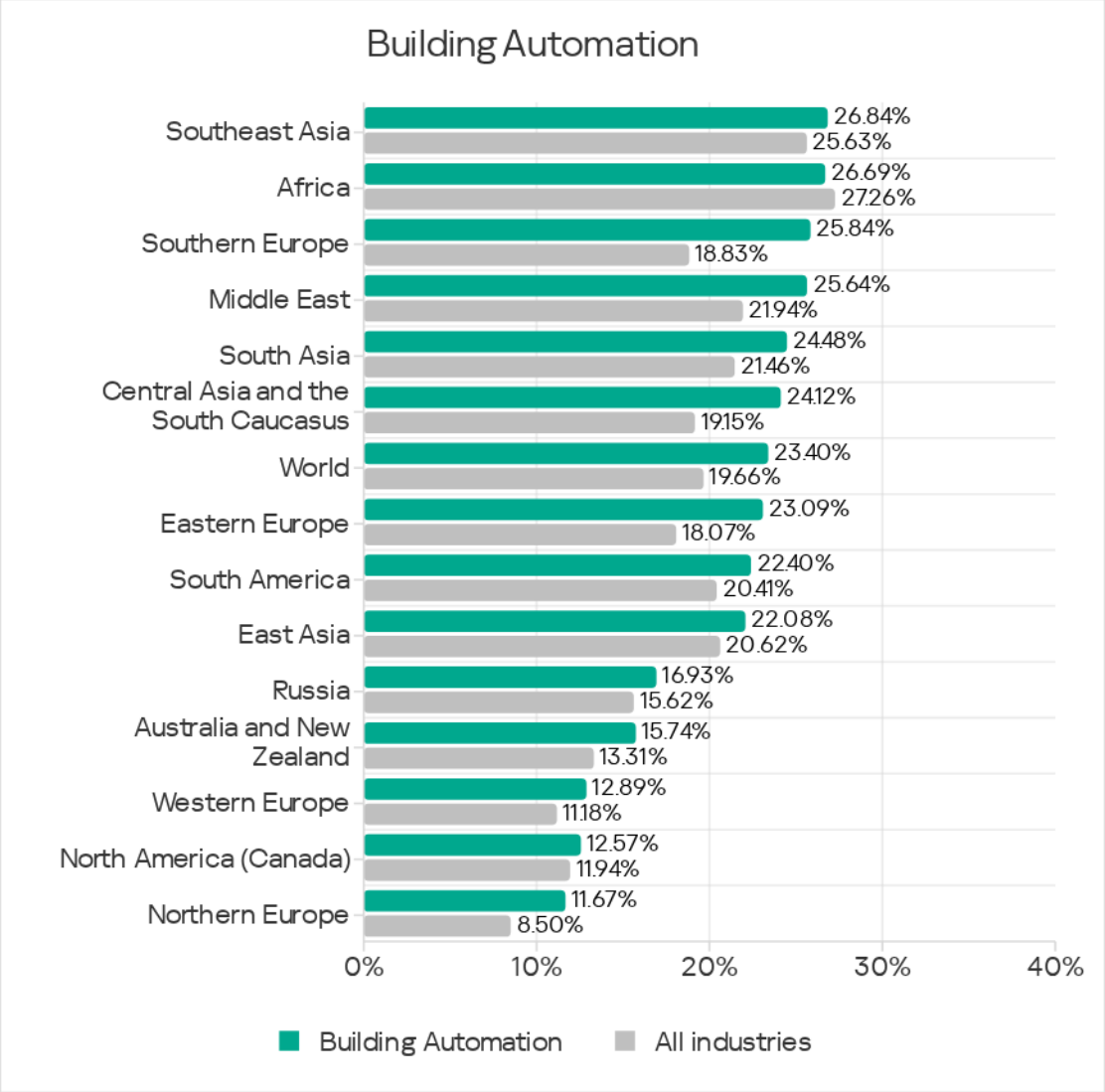
The leading position in the percentage of ICS computers on which malware for AutoCAD was blocked was held by this region again thanks to Vietnam, which had an enormous figure for this category, at 4.28%.

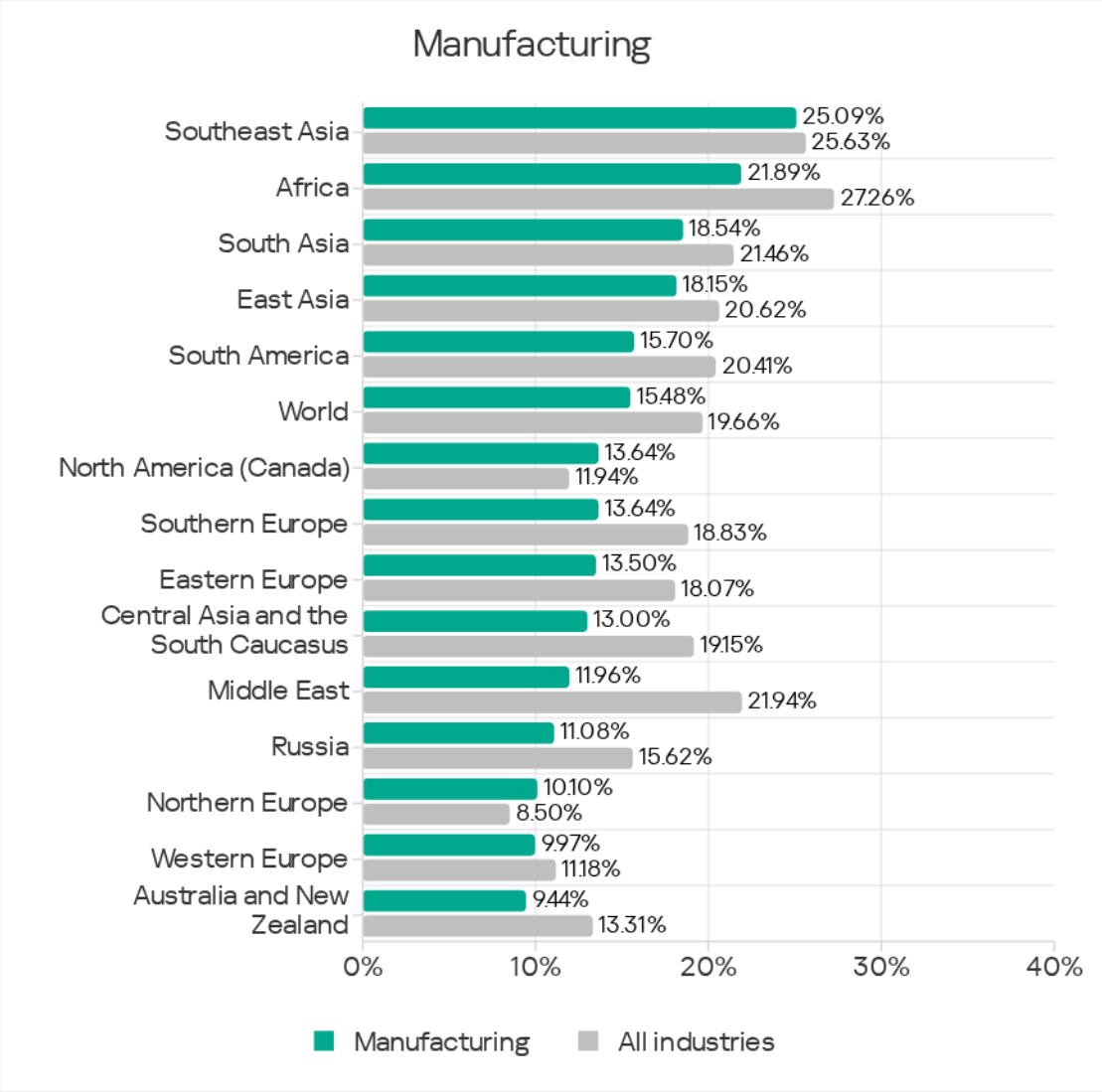


Like viruses, malware for AutoCAD in the region spreads through all sources, but mostly via internet.

Industries

In Q4 2025, Southeast Asia led among regions in the percentage of ICS computers on which malicious objects were blocked in the building automation and manufacturing industries.

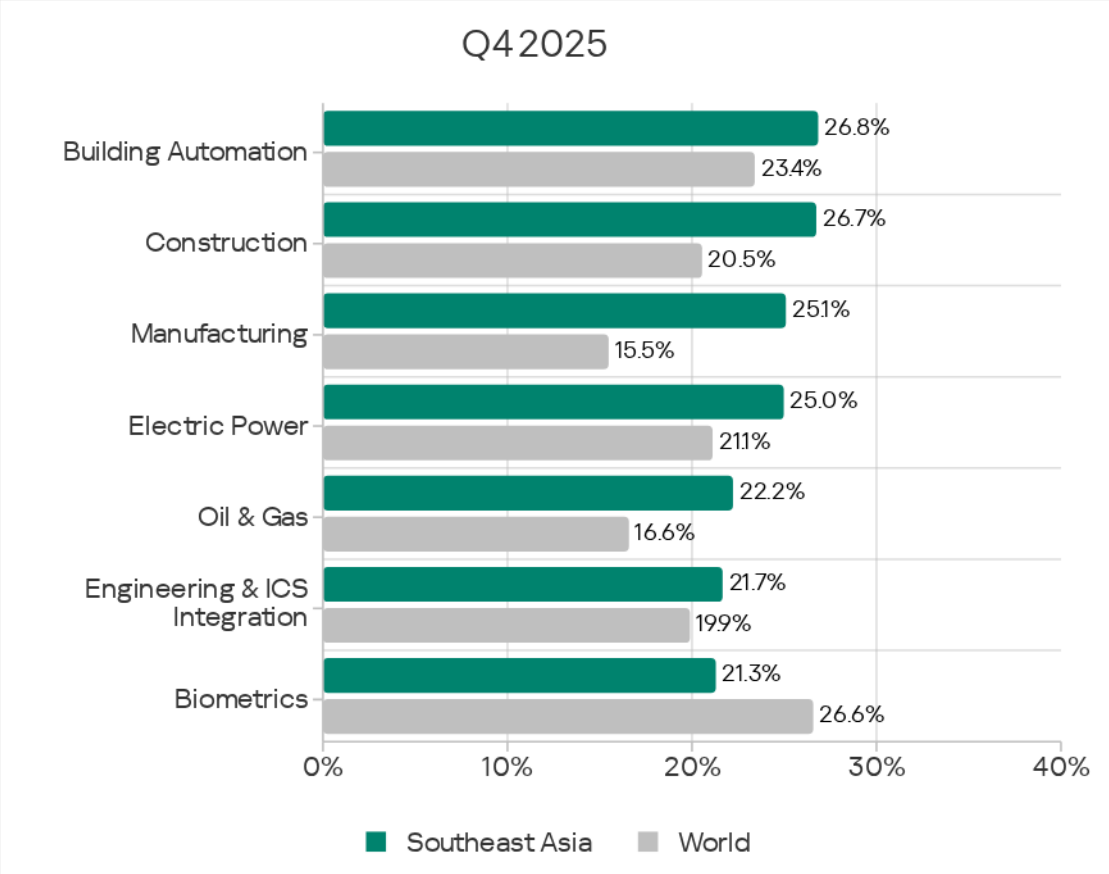




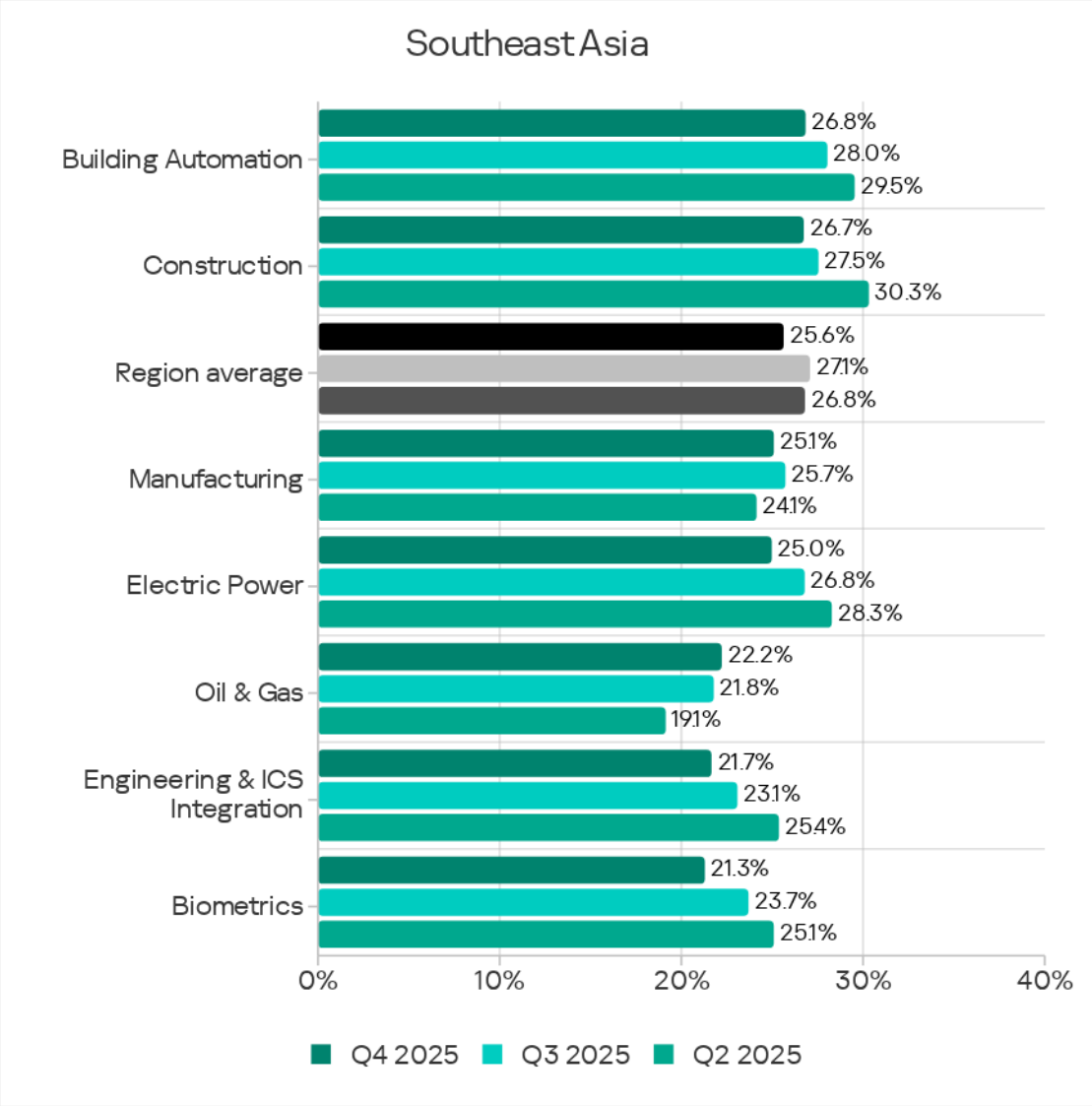
Based on the figures for industries, the region ranked second in the construction industry and engineering and ICS integrators industry, and ranked third in the electric power industry.

In Q4 2025, among all industries under review in the report, the building automation industry led in the percentage of ICS computers on which malicious objects were blocked in Southeast Asia.

In this region, the figures for all industries except biometrics exceeded the respective global averages. The largest differences were in the manufacturing industry (1.6 times) and construction industry (1.3 times).

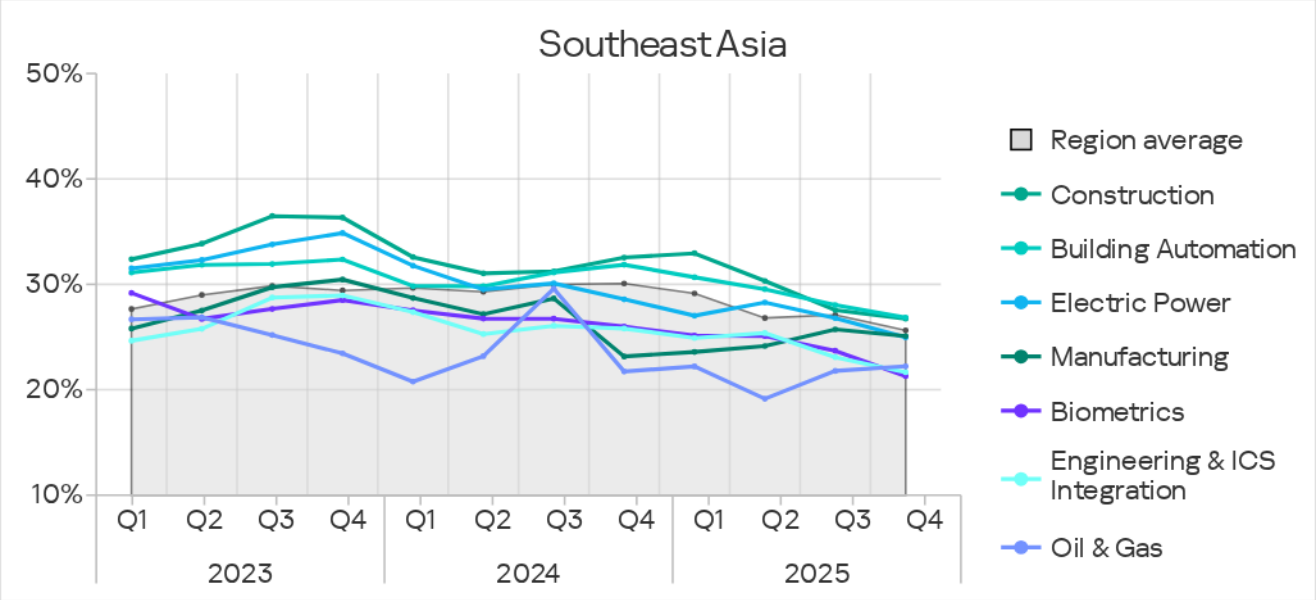


Over the quarter, the figures for all industries, except oil and gas, decreased.



A distinctive feature of the region is the position of biometrics in the industry rankings. It ranked near the top in most regions, and last only in Southeast Asia and East Asia.

All industries reviewed have shown a positive long-term trend (i.e., declining figures) since Q4 2023, with periodic fluctuations.



Threat sources and malware categories in industries: 'hotspots'

We use heat maps when assessing threats to industries in the regions. The color on the heatmap indicates the position in the global industry rankings across regions for each individual threat category or source. Red signifies that the figure is close to the maximum.

Threat source indicators for industries in Southeast Asia, Q4 2025

Industry / Threat source	Biometrics	Building Automation	Engineering & ICS Integration	Electric Power	Oil & Gas	Construction	Manufacturing	Category metric in region
Internet	7.34%	9.87%	9.77%	11.08%	10.79%	12.35%	8.74%	9.61%
Email clients	6.99%	5.83%	3.72%	2.37%	5.48%	3.13%	5.65%	4.18%
Removable media	0.40%	0.40%	0.38%	0.54%	0.32%	0.22%	0.54%	0.42%
Network folders	0.08%	0.06%	0.02%	0.03%	—	0.15%	0.06%	0.07%
Industry metric in region	21.29%	26.84%	21.66%	24.97%	22.22%	26.74%	25.09%	

Threat category indicators for industries in Southeast Asia, Q4 2025

Industry / Threat type	Biometrics	Building Automation	Engineering & ICS Integration	Electric Power	Oil & Gas	Construction	Manufacturing	Category metric in region
Denylisted internet resources	2.35%	3.83%	3.96%	5.26%	5.15%	5.31%	3.33%	3.93%
Malicious scripts and phishing pages (JS and HTML)	9.84%	9.51%	7.80%	7.89%	9.18%	8.64%	8.86%	7.90%
Malicious documents (MSOffice + PDF)	3.88%	2.96%	1.58%	1.91%	2.09%	2.25%	2.44%	2.13%
Spy Trojans, backdoors and keyloggers	8.07%	7.40%	4.78%	5.23%	6.60%	4.50%	8.20%	5.79%
Ransomware	0.32%	0.13%	0.09%	0.13%	—	0.20%	0.12%	0.11%
Miners in the form of executable files for Windows	0.45%	0.38%	0.31%	0.54%	0.64%	0.66%	0.59%	0.32%
Web miners running in browsers	0.47%	0.37%	0.43%	0.52%	0.48%	1.00%	0.65%	0.34%
Malware for AutoCAD	0.26%	0.75%	0.95%	1.47%	1.45%	4.23%	0.71%	2.12%
Worms	1.93%	2.21%	1.49%	2.45%	0.64%	1.30%	2.44%	2.05%
Viruses	2.48%	6.17%	3.29%	6.03%	2.90%	7.27%	4.22%	6.90%
Industry metric in region	21.29%	26.84%	21.66%	24.97%	22.22%	26.74%	25.09%	

Building automation

Southeast Asia led among regions based on the percentage of ICS computers on which malicious objects in the building automation industry were blocked.

Based on the industry indicators among regions, Southeast Asia had the following rankings:

- Second place in the percentage of ICS computers on which internet threats were blocked.
- Third place in network folder threats.

- First place in the percentage of ICS computers on which viruses were blocked.
- Second place in the following threat categories: spyware, web miners, and AutoCAD malware.
- Third in denylisted internet resources.

In the regional cross-industry rankings, building automation occupied the following positions:

- Second place in the percentage of ICS computers on which threats in email clients were blocked.
- Third in terms of threats from the internet, removable media, and network folders.
- Second for malicious scripts and phishing pages, malicious documents, and viruses.
- Third in spyware, ransomware, and worms.

Construction

Southeast Asia ranked second among regions based on the percentage of ICS computers on which malicious objects were blocked in the construction industry.

Based on the industry indicators among regions, Southeast Asia had the following rankings:

- First place in the percentage of ICS computers on which internet threats were blocked.
- Second place in network folders.
- First for the percentage of ICS computers on which denylisted internet resources, viruses, and web miners were blocked.
- Second place in malware for AutoCAD.
- Third place for spyware.

In the regional cross-industry rankings, the construction sector ranked:

- First in the percentage of ICS computers on which internet threats and network folder threats were blocked.
- First in threats of the following categories: denylisted internet resources, malicious documents, viruses, malware for AutoCAD, and miners of both categories.
- Second place in ransomware.

Manufacturing

Southeast Asia led among all regions based on the percentage of ICS computers on which malicious objects in the industry were blocked.

Based on the industry indicators among regions, Southeast Asia had the following rankings:

- First place in the percentage of ICS computers on which threats in email clients were blocked.
- Third in terms of threats from the internet, removable media, and network folders.
- First place in the percentage of ICS computers on which the following categories of threats were blocked: malicious documents, spyware, viruses, and web miners.
- Second place in the following threat categories: denylisted internet resources, malicious scripts and phishing pages, and malware for AutoCAD.

In the regional cross-industry rankings, the manufacturing sector ranked:

- Second in the percentage of ICS computers on which threats were blocked when connecting removable media.
- Third for threats from email clients.
- First place for spyware.
- Second place in worms and both types of miners.
- Third place in the percentage of ICS computers on which malicious scripts and documents and phishing pages were blocked.

Electric power

Southeast Asia ranked third among regions based on the percentage of ICS computers on which malicious objects were blocked in the electrical energy industry.

Based on the industry indicators among regions, Southeast Asia had the following rankings:

- First place in the percentage of ICS computers on which internet threats were blocked.
- First place in the percentage of ICS computers on which viruses were blocked.
- Second for denylisted internet resources and malware for AutoCAD.
- Third in spyware and web miners.

In the regional cross-industry rankings, the electrical energy industry ranked:

- First in the percentage of ICS computers on which removable media threats were blocked.
- Second in internet threats.
- First for worms.
- Second in denylisted internet resources and malware for AutoCAD.
- Third for viruses and miners from both categories.

Engineering and ICS integrators

Southeast Asia ranked second among regions based on the percentage of ICS computers on which malicious objects in the engineering and ICS integrators industry were blocked.

Based on the industry indicators among regions, Southeast Asia had the following rankings:

- Second place in the percentage of ICS computers on which threats in email clients were blocked.
- Third for internet threats.
- First place in the percentage of ICS computers on which web miners are blocked.
- Second place in the following threat categories: denylisted internet resources, spyware, and malware for AutoCAD.
- Third for viruses.

In the regional cross-industry rankings, engineering and ICS integrators had the following positions:

- Third place in the following threat categories: denylisted internet resources and malware for AutoCAD.

Biometrics

Southeast Asia ranked eighth among regions based on the percentage of ICS computers on which malicious objects were blocked in biometrics.

Based on indicators for biometrics among regions, Southeast Asia had the following rankings:

- Third place in the percentage of ICS computers on which threats from email clients and network folders were blocked.
- First in terms of the percentage of ICS computers on which malware for AutoCAD was blocked.
- Third for malicious documents, spyware, and web miners.

The regional industry rankings for biometrics was as follows:

- First place in the percentage of ICS computers on which email client threats were blocked.
- Second in network folder threats.
- First for malicious scripts and phishing pages, malicious documents, and ransomware.
- Second place for spyware.

South Asia

Key cybersecurity issues in the region

Lack of control over the use of removable media

Unprotected parts of technological infrastructure become sources of secondary infection (malware spread).

South Asia ranked fourth among regions by the percentage of ICS computers on which threats from removable media were blocked. The region's figure was 1.6 times higher than the global average.

South Asia ranked fifth globally for ICS computers on which threats in network folders were blocked.

Removable media and network folders in the region are becoming sources of self-propagating malware, malware for AutoCAD, and ransomware.

South Asia ranked fifth globally for ICS computers on which viruses were blocked, fourth in terms of malware for AutoCAD, and fifth for ransomware. These threat categories spread in the region through all sources but mainly via removable media.

High level of internet threats

In Q4 2025, South Asia rose from third to first place in the rankings of regions in terms of the percentage of ICS computers on which internet threats were blocked. The region ranked first for the growth in this metric in Q4 2025.

India and Afghanistan were the only countries in the region where internet threats decreased over the quarter. While the changes in Afghanistan were negligible, this figure for India increased by a factor of 1.34.

South Asia ranked first among regions for the percentage of ICS computers on which internet threats were blocked across all industries except for the construction industry and electric power industry.

Highlights of the quarter: malicious scripts and phishing pages

In Q4 2025, the region saw a sharp increase in the percentage of ICS computers on which malicious scripts and phishing pages were blocked. As a result, South Asia rose from eighth to first place in the regions ranking for this metric.

The figure for South Asia grew by a factor of 1.49 over the quarter, and the region also ranked first for growth in this metric.

The main driver of this significant growth was a wave of infections of websites powered by WordPress that are popular in India. As a result of these infections, website visitors received malicious JS code alongside legitimate content, which was designed to redirect the user to a phishing website.

Across the region, the malicious scripts and phishing pages threat category showed the most growth in the manufacturing industry and the engineering and ICS integrators industry. The internet threat metric also showed the most growth in these industries.

India drove the regional growth in both internet threats and malicious scripts and phishing pages, with these indicators increasing by 1.34 and 1.87 times respectively over the quarter.

Differences among countries in the region

The region's figures are all heavily influenced by India. India was near the bottom of most rankings by both threat source and category, with a percentage of attacked ICS computers significantly lower than in most other countries of the region and below the regional average.

In Q4, it was the situation namely in this country that propelled the region to first place for internet threats and in the malicious scripts and phishing pages threat category.

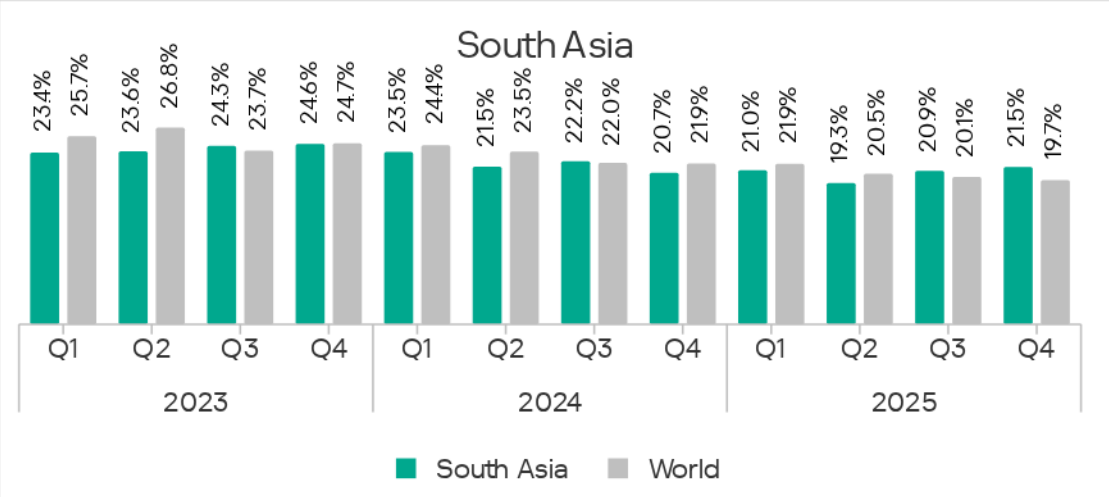
Afghanistan's cybersecurity situation differs markedly from other countries in the region regarding removable media control. This is evident in its much higher rates of removable-media-based and self-propagating malware threats compared to the other countries. The same is true for network folder threats in Afghanistan.

Statistics across all threats

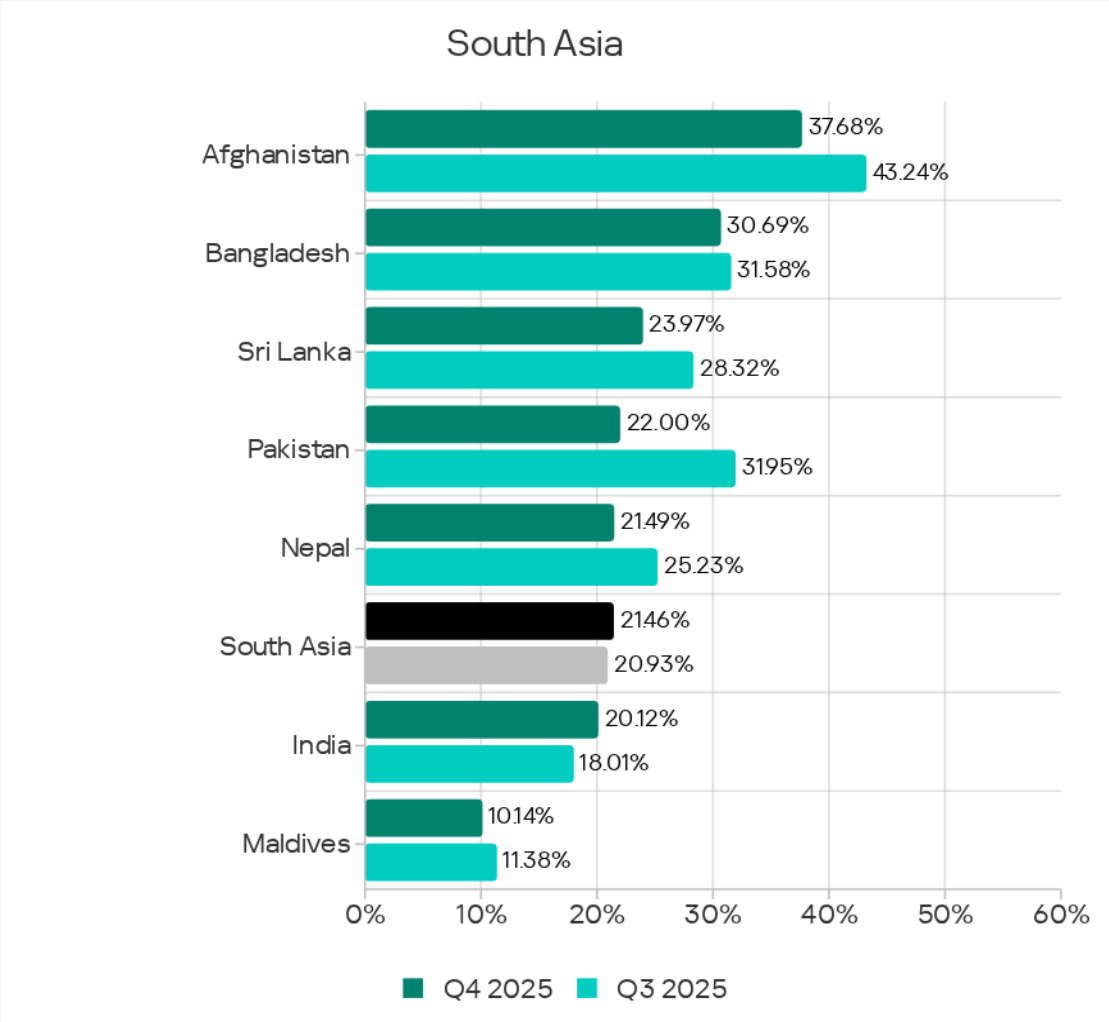
In Q4 2025, South Asia rose from fifth to fourth place in the regional rankings in the percentage of ICS computers on which malicious objects were blocked. Back in Q2 2025, the region was in ninth place.

South Asia was one of four regions where the percentage of ICS computers on which malicious objects were blocked increased over the quarter. This metric has been growing in the region for two consecutive quarters.

The region's 21.5% figure is the highest since Q4 2024. This was 2.5 times higher than Northern Europe, which ranked last.



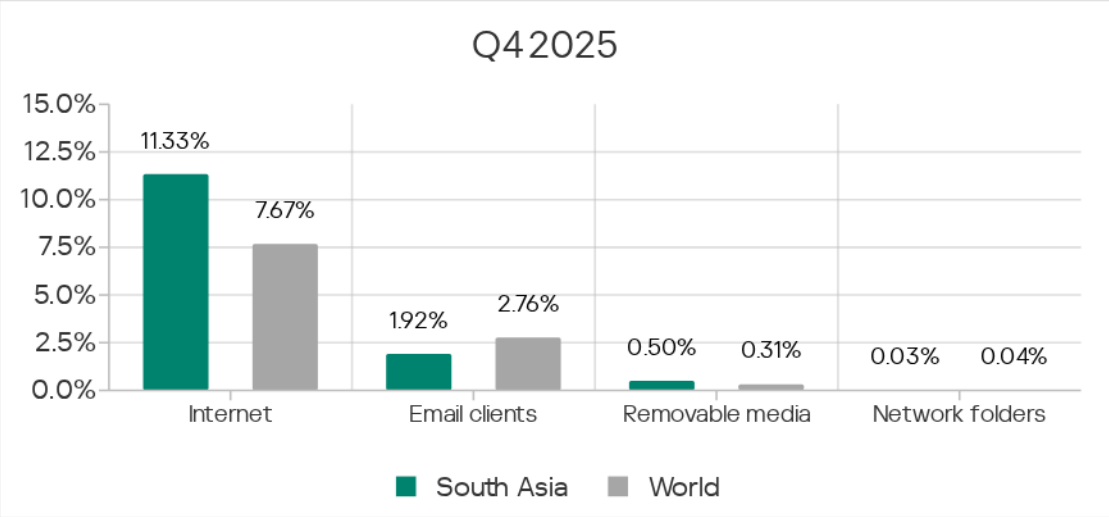
The percentage of ICS computers on which malicious objects were blocked varies among the region's countries, from 10.14% in the Maldives to 37.68% in Afghanistan.



Threat sources

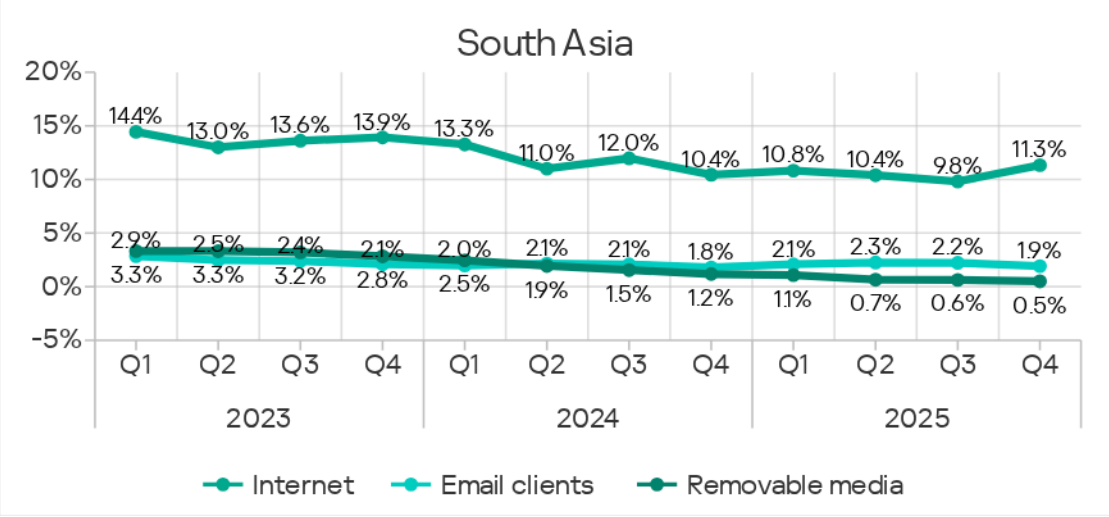
In Q4 2025, South Asia exceeded the global averages for two threat sources:

- Internet: by 1.5 times, first place globally
- Removable media: by 1.6 times, fourth place globally



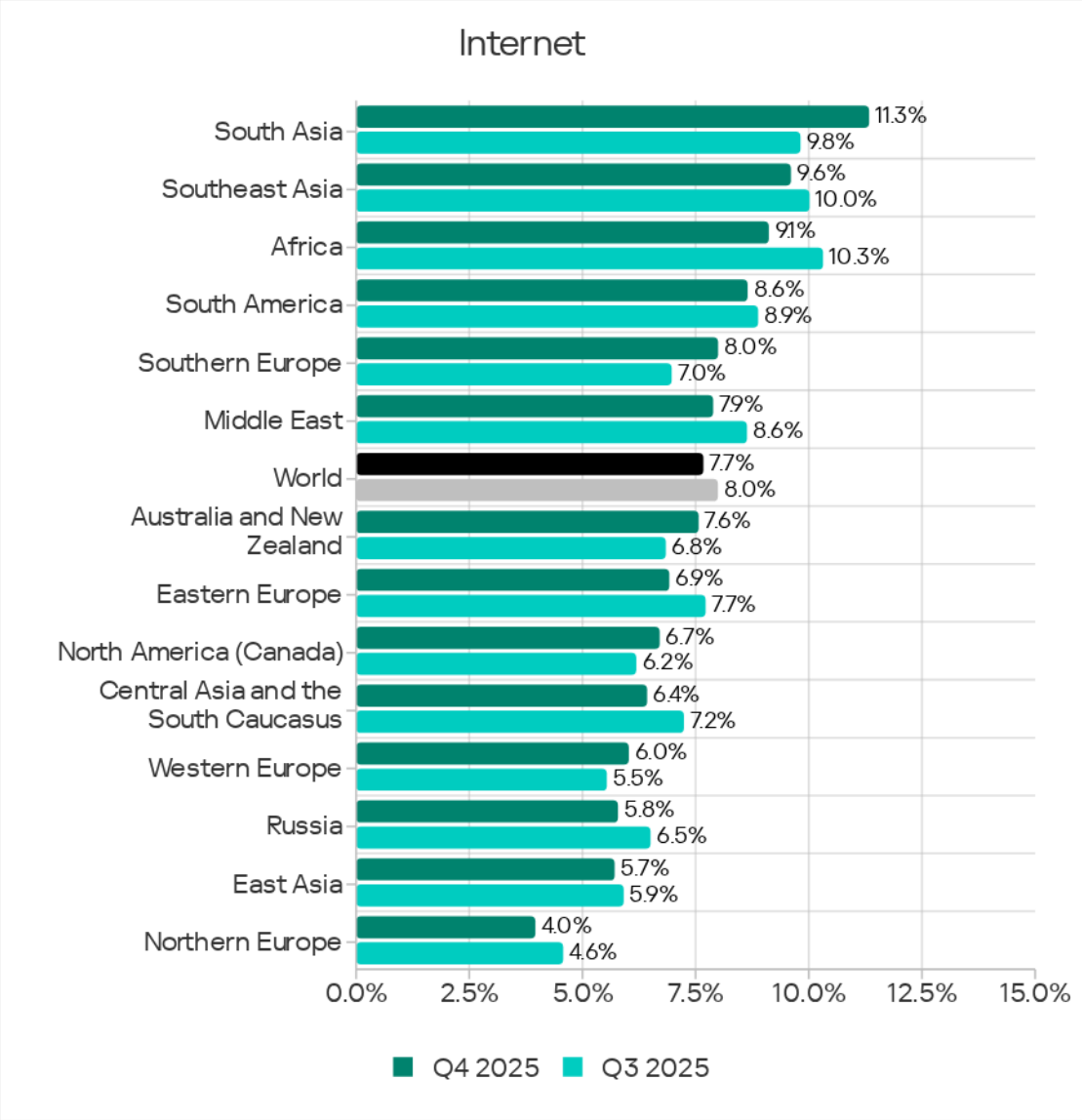
The percentage of ICS computers on which malicious objects from various threat sources were blocked increased only for internet threats.

Overall, all major threat sources show a long-term downward trend.

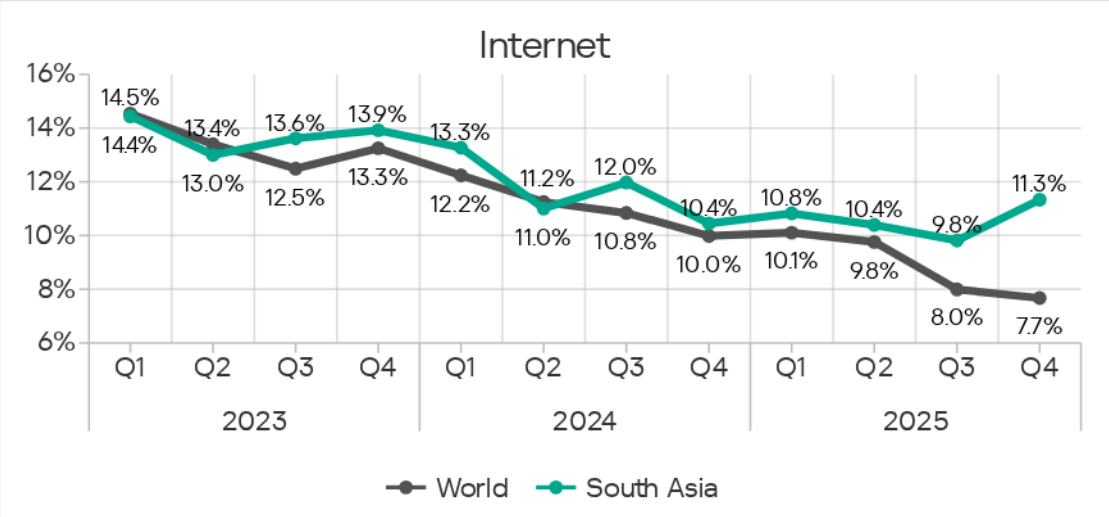


Internet

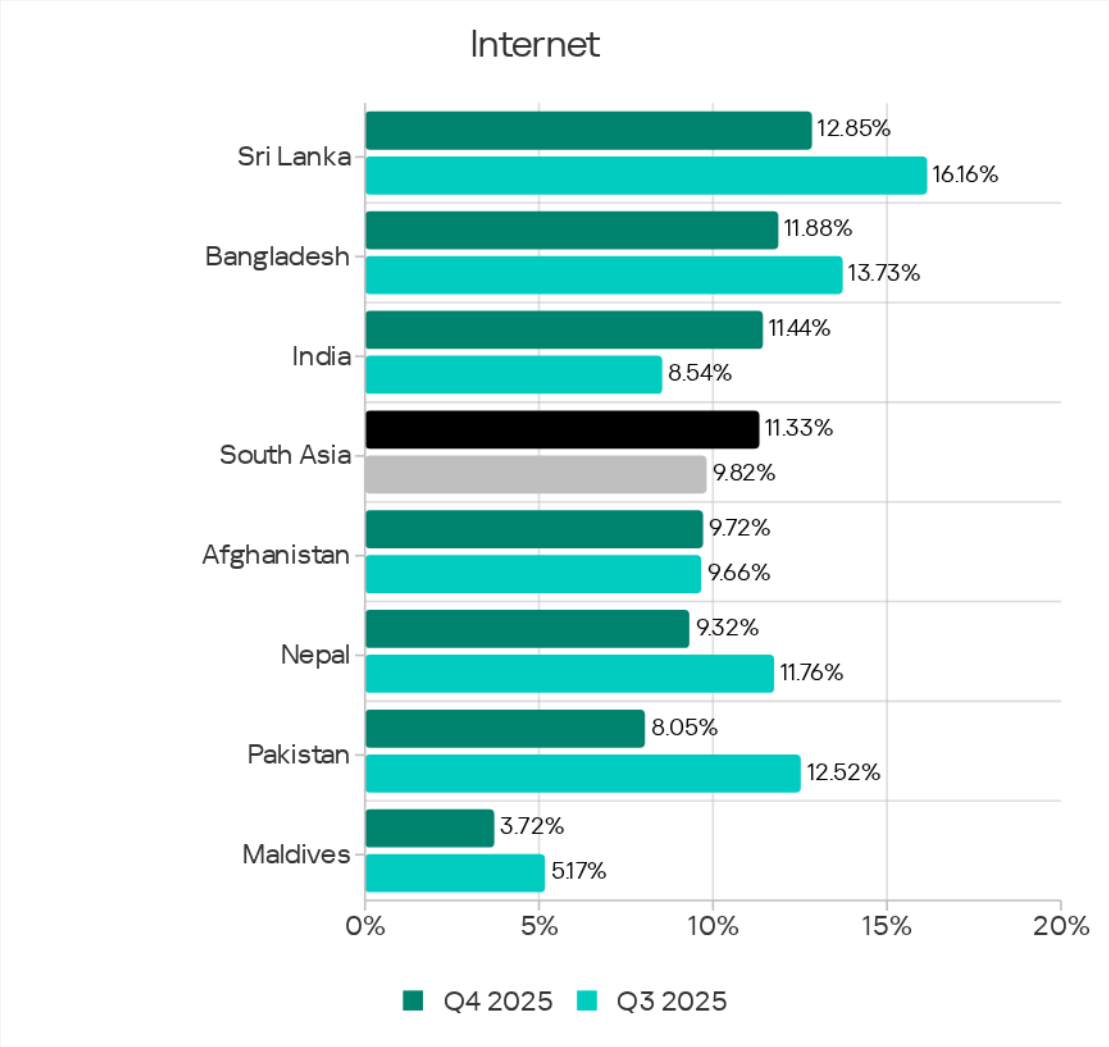
In Q4 2025, South Asia rose from third to first place globally in terms of the percentage of ICS computers on which internet threats were blocked (11.33%). This was 2.9 times higher than Northern Europe, which came last in the regional ranking.



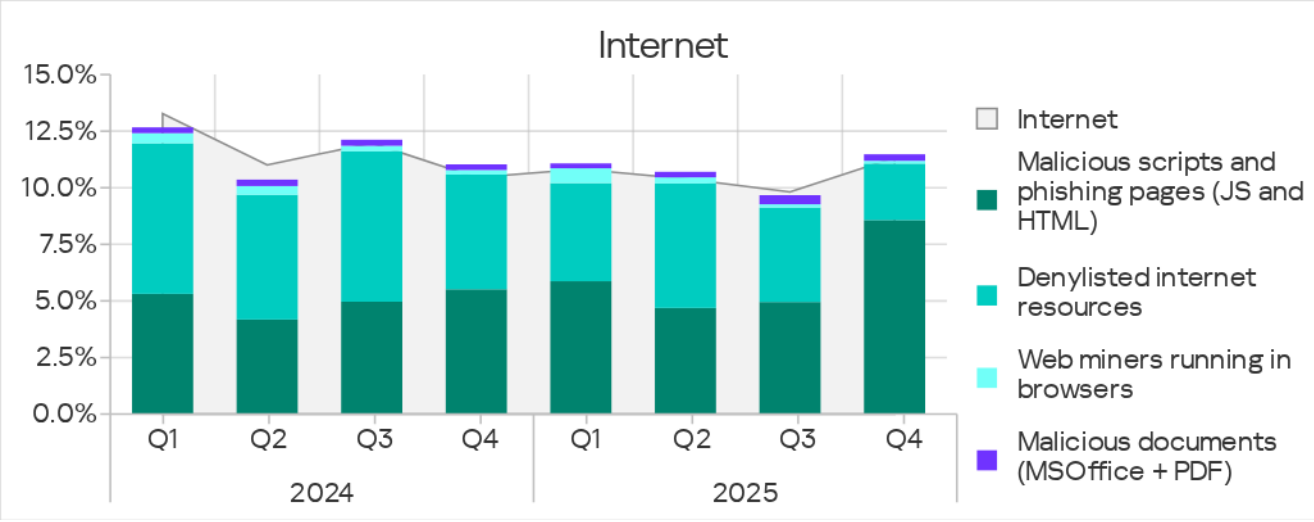
Based on growth in the percentage of ICS computers on which internet threats were blocked, South Asia ranked first among regions in Q4. The metric for South Asia in Q4 2025 was the highest since Q4 2024.



Country figures range from 3.72% in the Maldives to 12.85% in Sri Lanka. India and Afghanistan were two countries in the region where the percentage of ICS computers on which internet threats were blocked increased over the quarter. In India, it increased by a factor of 1.34.



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



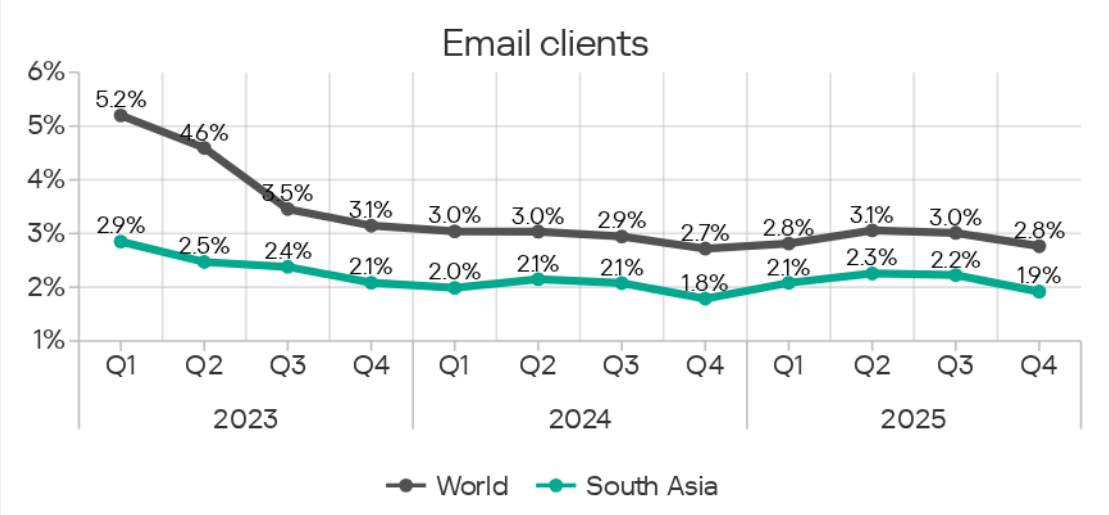
In Q4 2025 in South Asia, the percentage of ICS computers on which malicious scripts and phishing pages were blocked increased by a factor of 1.73.

Afganistan led the region in terms of the percentage of ICS computers on which denylisted internet resources were blocked.

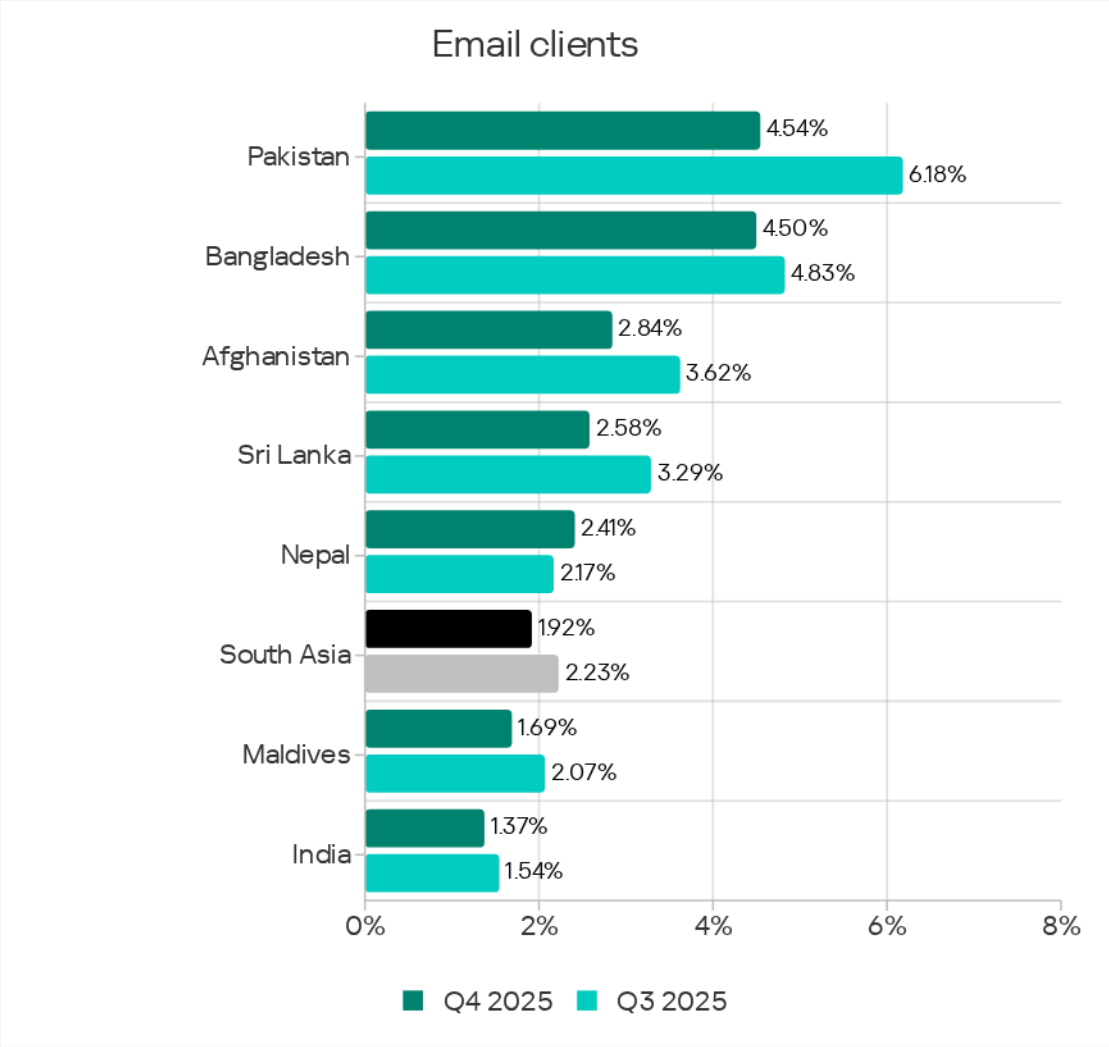
Email clients

In terms of ICS computers on which mail client threats were blocked, South Asia ranked eighth globally with 1.92%. This figure was 3.0 times higher than in Northern Europe, which had the lowest rate.

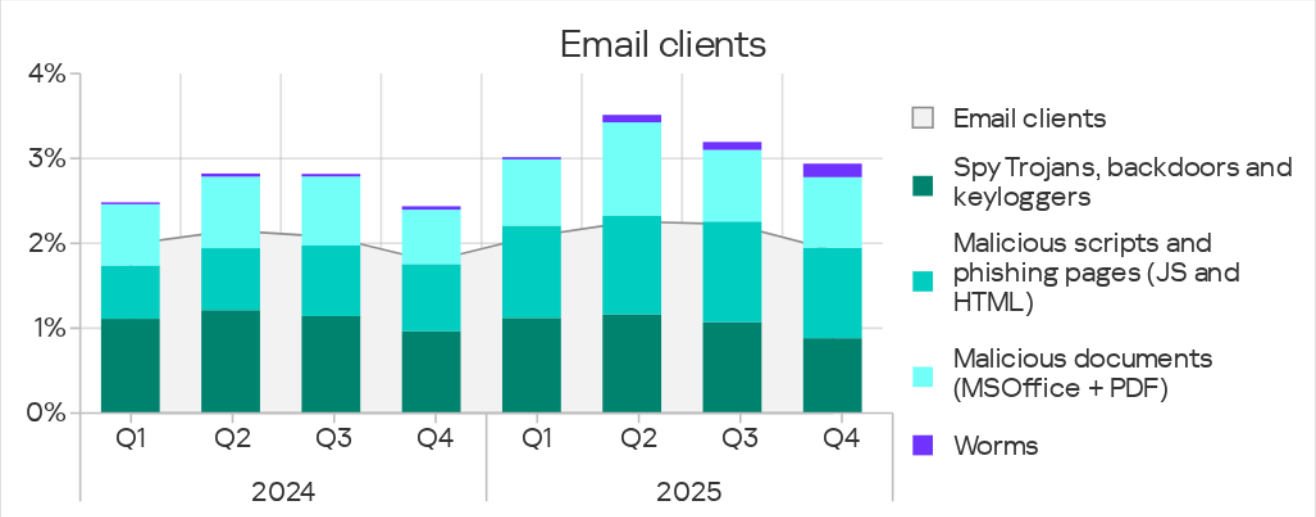
After growing during the three previous quarters, this region-specific figure decreased but still remained above the Q4 2024 level.



Among the region's countries, Pakistan (4.54%) and Bangladesh (4.50%) led in the percentage of ICS computers on which mail client threats were blocked. The lowest figure observed was in India, at 1.37%.



The main categories of email client threats blocked on ICS computers were malicious documents, spyware, and malicious scripts and phishing pages. Pakistan also ranked first for malicious documents, while Bangladesh ranked first for spyware.



Q4 2025 saw a noticeable increase in the percentage of ICS computers on which worms from email clients were blocked. This was connected with the latest wave of phishing campaigns known as Curriculum-vitae-catalina, which launched attacks against organizations across all regions of the world. In South Asia, these attacks peaked in November.

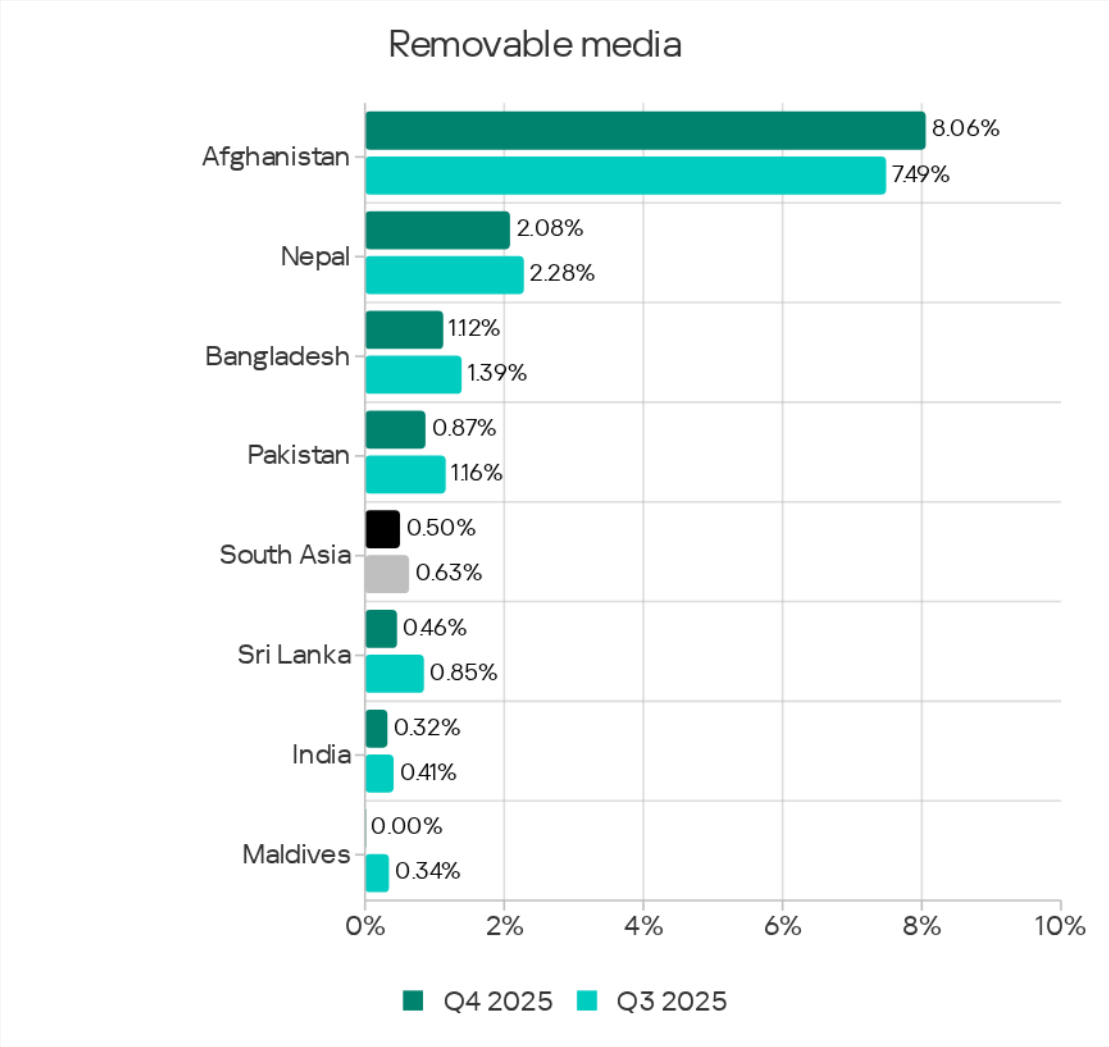
The hackers distributed phishing emails disguised as job applications. Disguised as a resume (Curriculum Vitae), these emails contained a malicious executable file, a remote administration backdoor worm known as Backdoor.MSIL.XWorm. Running that file caused system infection.

Normally, these campaigns are designed to deliver malware for data theft, spyware, or remote administration tools (RATs).

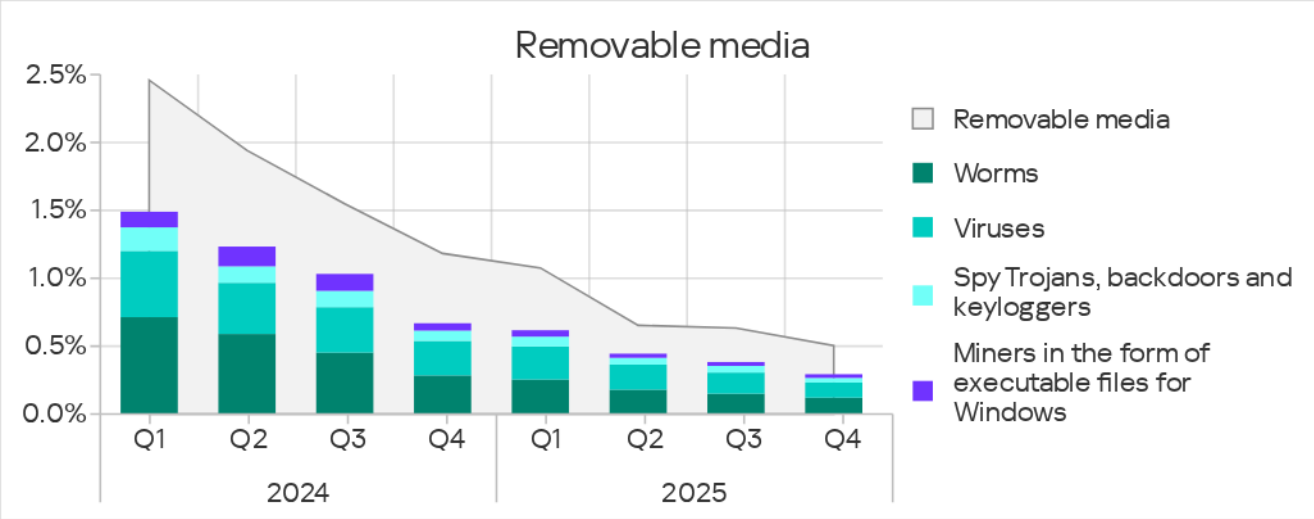
Removable media

By percentage of ICS computers on which removable media threats were blocked, South Asia ranked fourth globally, with 0.50%. This was 10 times higher than in the Australia and New Zealand region, which was at the bottom of this ranking.

Among countries in the region, Afghanistan led by a wide margin in the percentage of ICS computers on which removable media threats were blocked, with 8.06%. Other countries' rates ranged from near-zero in the Maldives to 2.08% in Nepal.



The main categories of removable media threats blocked on ICS computers in the region were worms, spyware, and viruses.

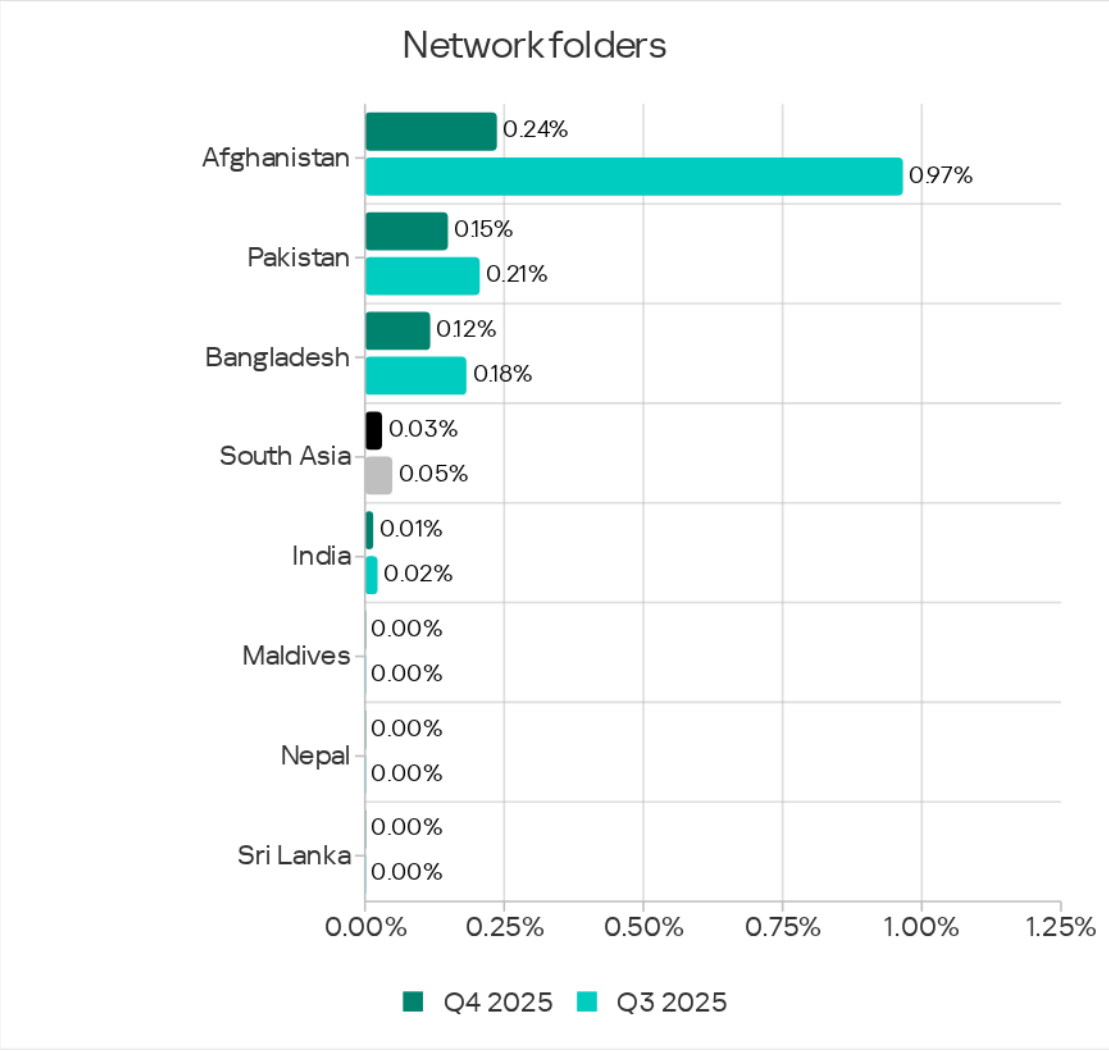


Afghanistan also led (again by a wide margin) in the percentage of ICS computers on which viruses and worms were blocked.

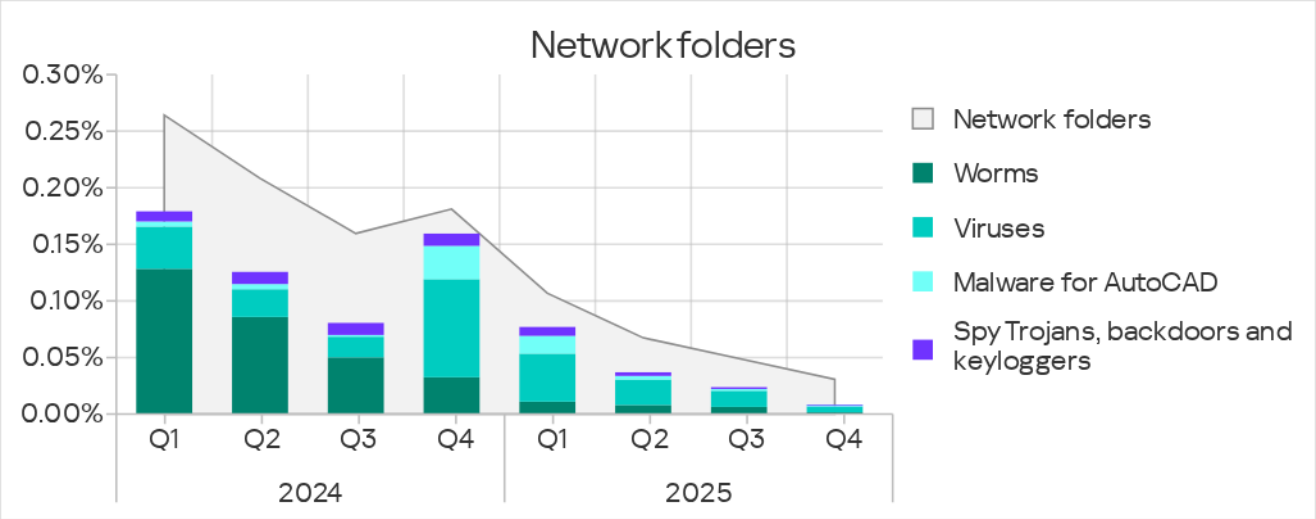
Network folders

South Asia, with 0.03%, ranked fourth among regions globally in the percentage of ICS computers on which network folder threats were blocked. In Q4 2025, South Asia's figure was 4.4 times higher than in Northern Europe, which was at the bottom of the ranking.

Based on the percentage of ICS computers on which network folder threats were blocked, Afghanistan led the region's other countries, with 0.24%. After growing sharply during the previous quarter, the metric for the country returned to its usual values. The lowest figures were observed in the Maldives, Nepal, and Sri Lanka.

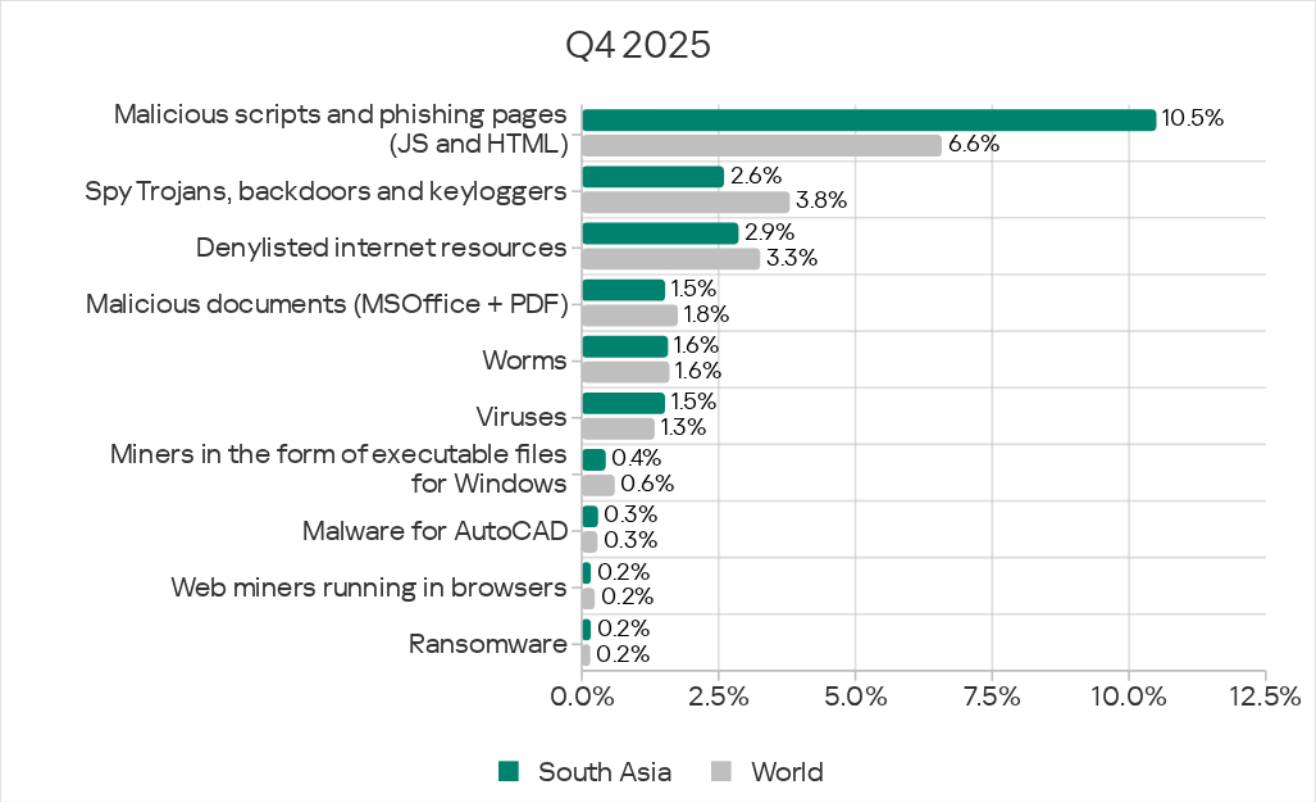


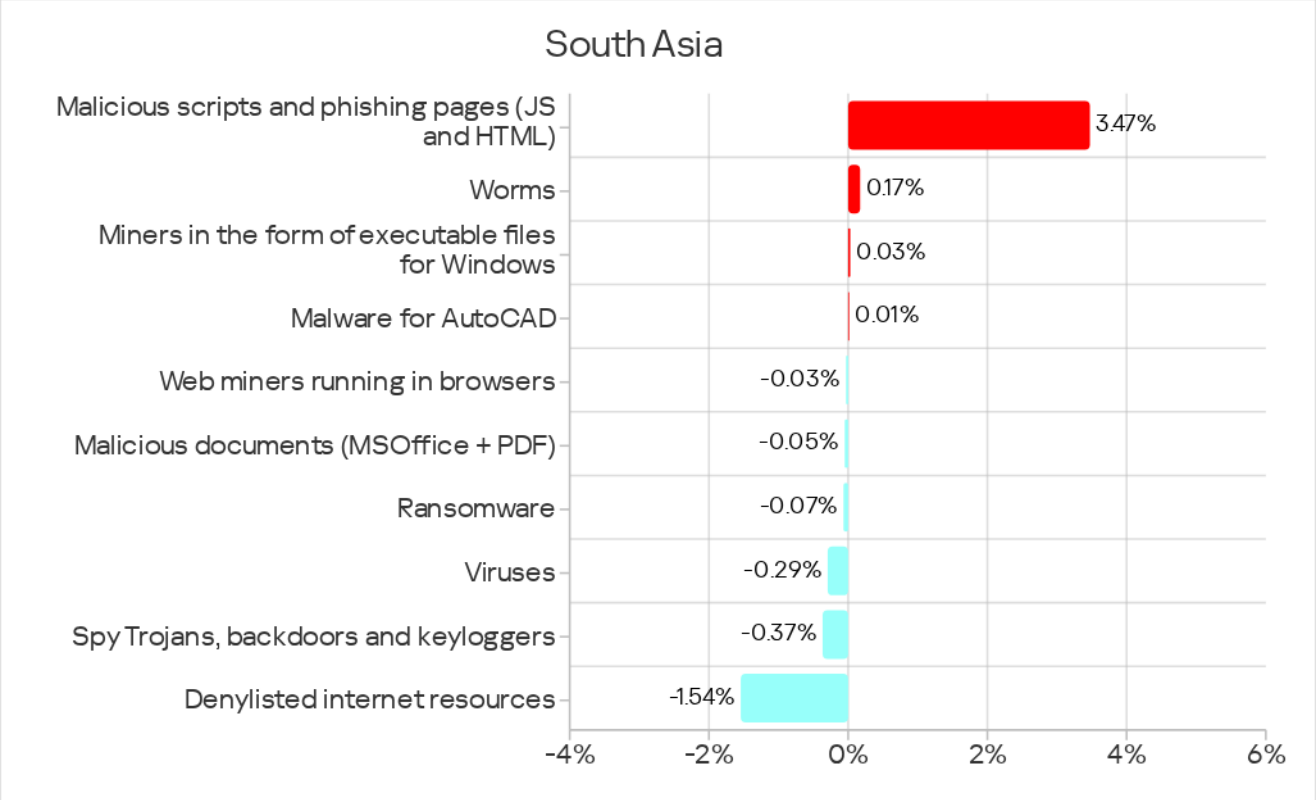
The main categories of threats that spread through network folders in the region were viruses, malicious scripts, worms, and malware for AutoCAD.



Threat categories

Malicious scripts and phishing pages led the threat category rankings for South Asia in Q4 2025, based on their detection rate on ICS computers.





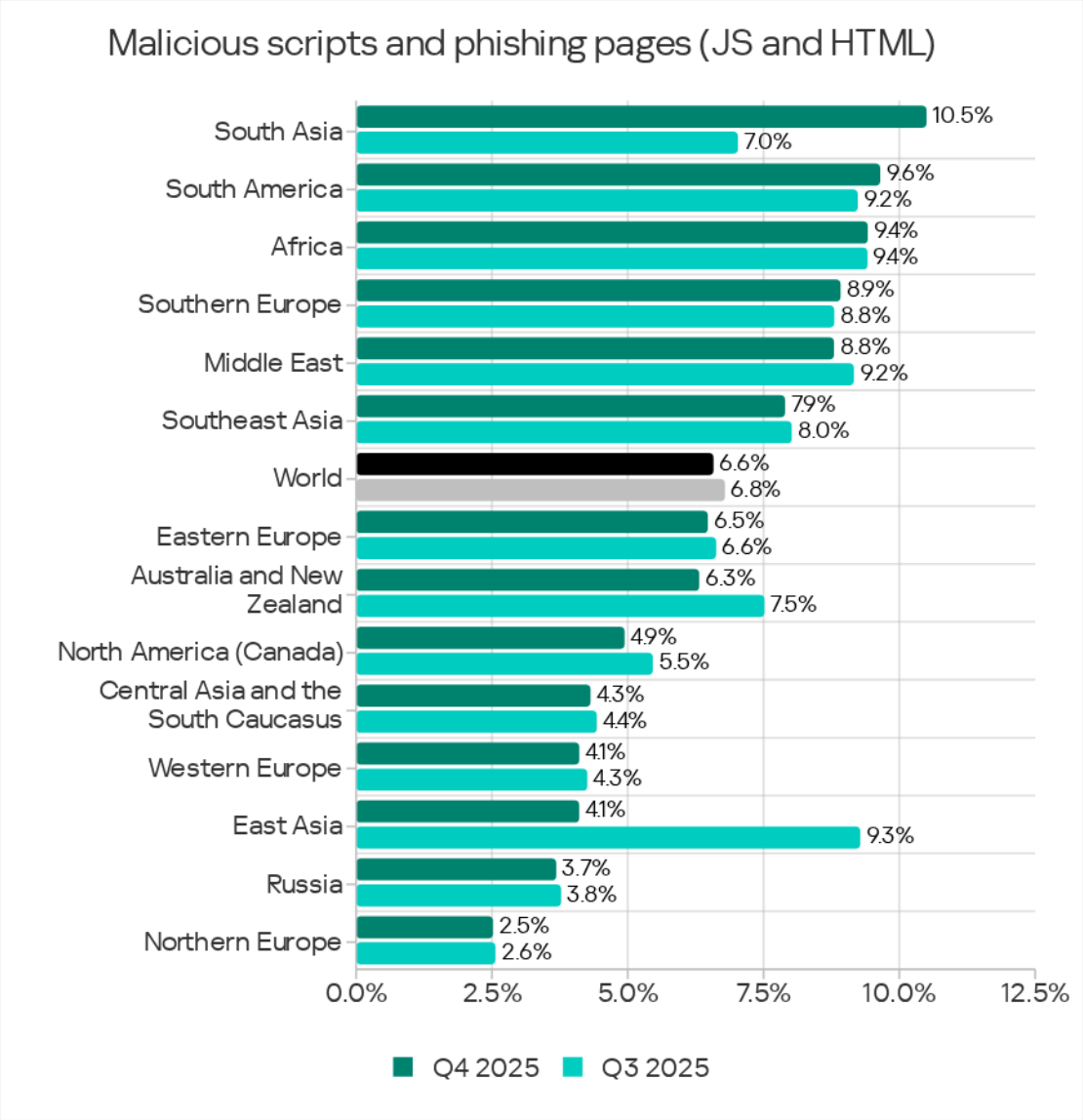
During Q4, the malicious scripts and phishing pages threat category in the region grew by a factor of 1.49. As a result, in the rankings of regions, South Asia ranked first for growth in this metric and for the percentage of ICS computers on which this threat was blocked.

Compared with global averages, the region had higher percentages of ICS computers on which the following were blocked:

- Malicious scripts and phishing pages: 1.6 times higher
- Viruses: 1.1 times higher.
- Ransomware: 1.1 times higher.

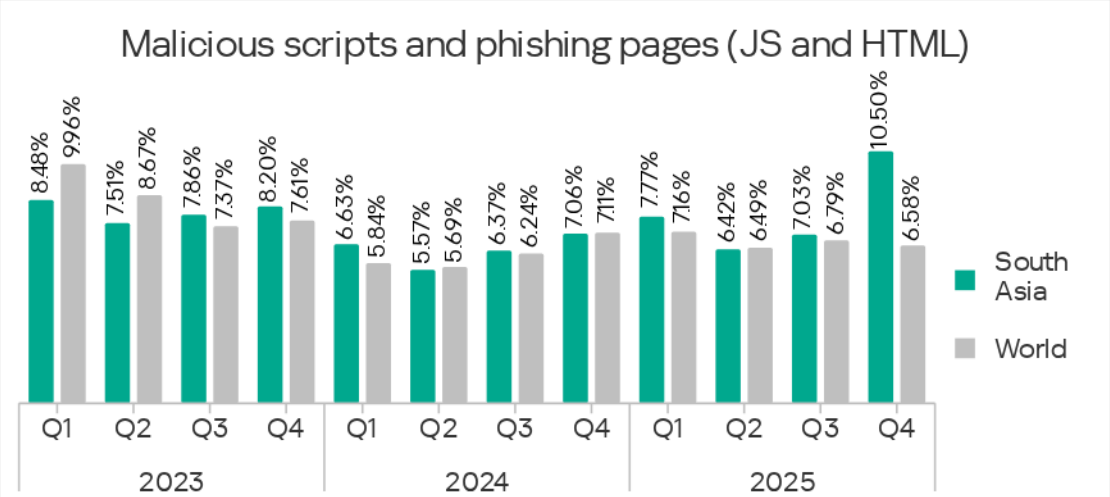
Malicious scripts and phishing pages

Based on the percentage of ICS computers on which malicious scripts and phishing pages were blocked, South Asia ranked first among regions in Q4 2025 after rising from eighth place in the rankings.

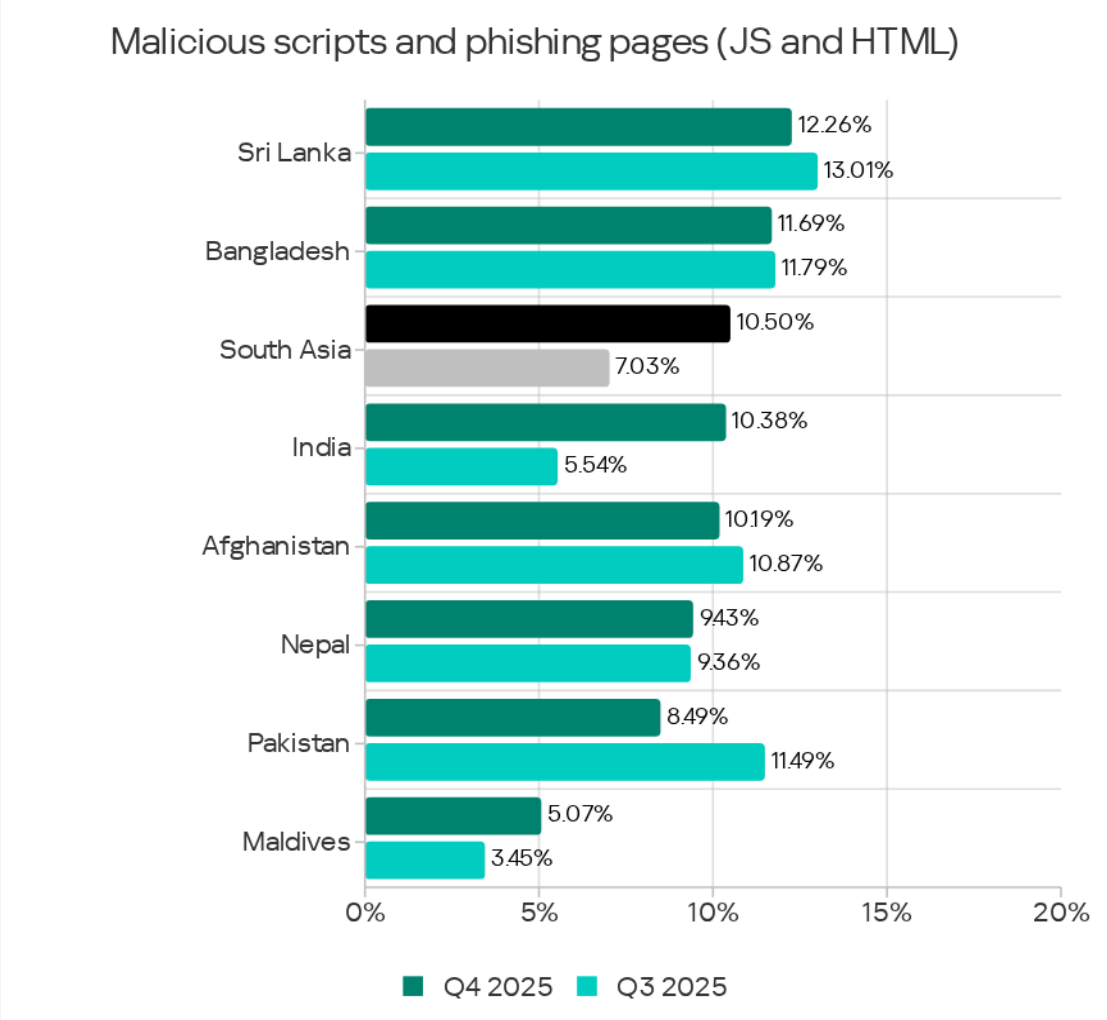


Over the quarter, this figure grew by a factor of 1.49, reaching 10.50%. This figure was 4.2 times higher than in Northern Europe, which ranked lowest. This threat was distributed through all sources, but predominately over the internet.

The metric's growth in the region was driven by India, where it increased by a factor of 1.87 over the quarter. You may recall that the internet threats figure for this country grew by a factor of 1.34.



Among countries in the region, Sri Lanka led with 12.26% by the percentage of ICS computers on which malicious scripts and phishing pages were blocked. The Maldives had the lowest figure at 5.07%. As stated earlier, this metric grew by a factor of 1.87 in India, while it grew by a factor of 1.62 in the Maldives.

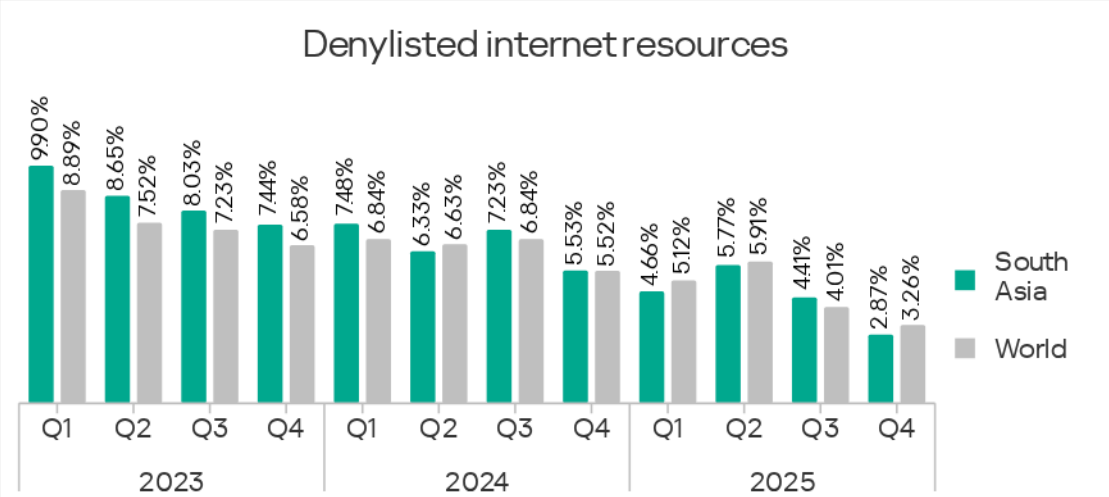


In Q4 2025, the percentage of ICS computers on which malicious scripts and phishing pages were blocked reached a three-year high in India.

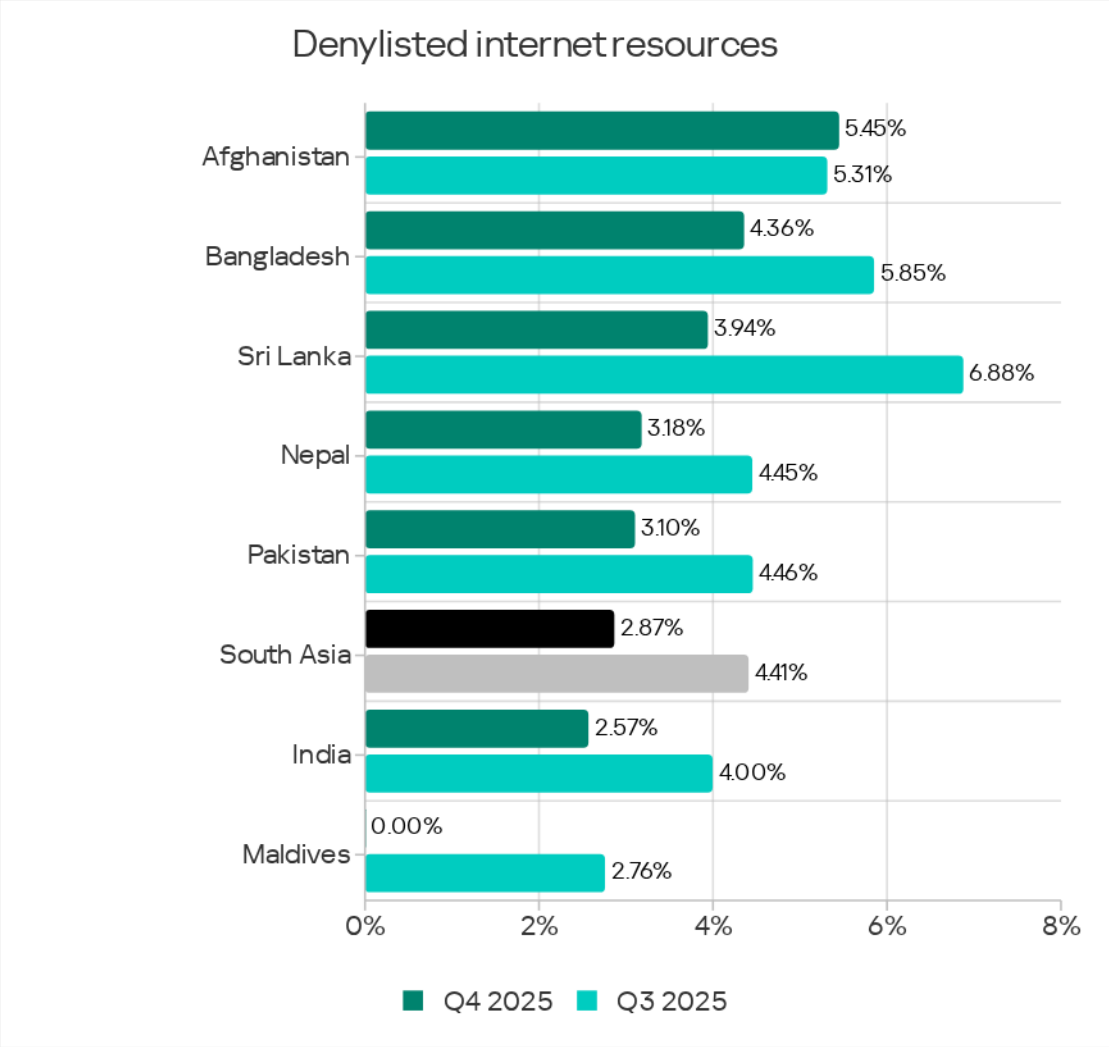
Denylisted internet resources

The region occupied seventh place in the percentage of ICS computers on which denylisted internet resources were blocked, with 2.87%. This was 1.6 times higher than Northern Europe, which had the lowest rate.

The region's trend for this metric generally aligns with the global average.



Within the region, Afghanistan led with 5.45% in the percentage of ICS computers on which denylisted internet resources were blocked. Aside from the Maldives, where the metric for Q4 2025 was close to zero, the next lowest figure was in India at 2.57%.

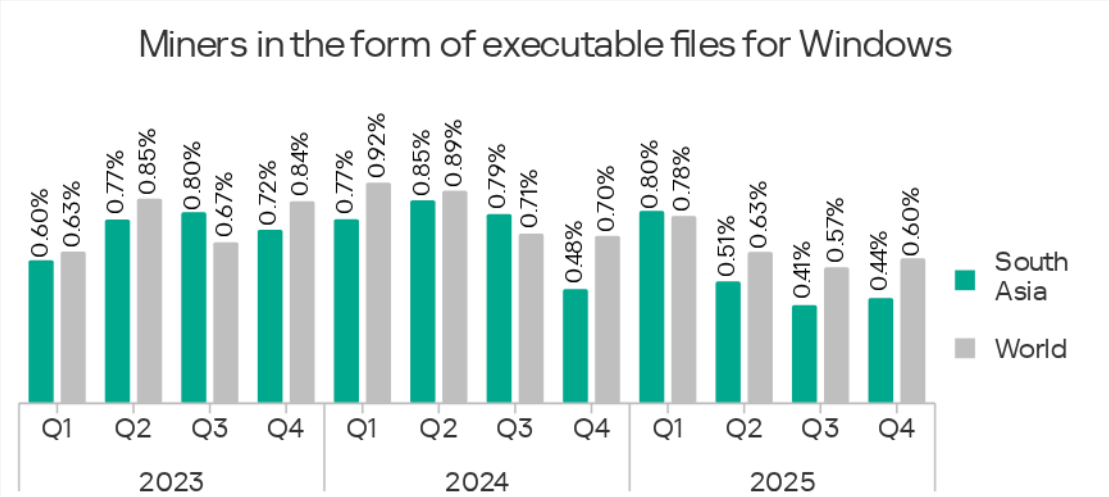


The internet was the sole threat source for this category. Sri Lanka led by the percentage of ICS computers on which internet threats were blocked.

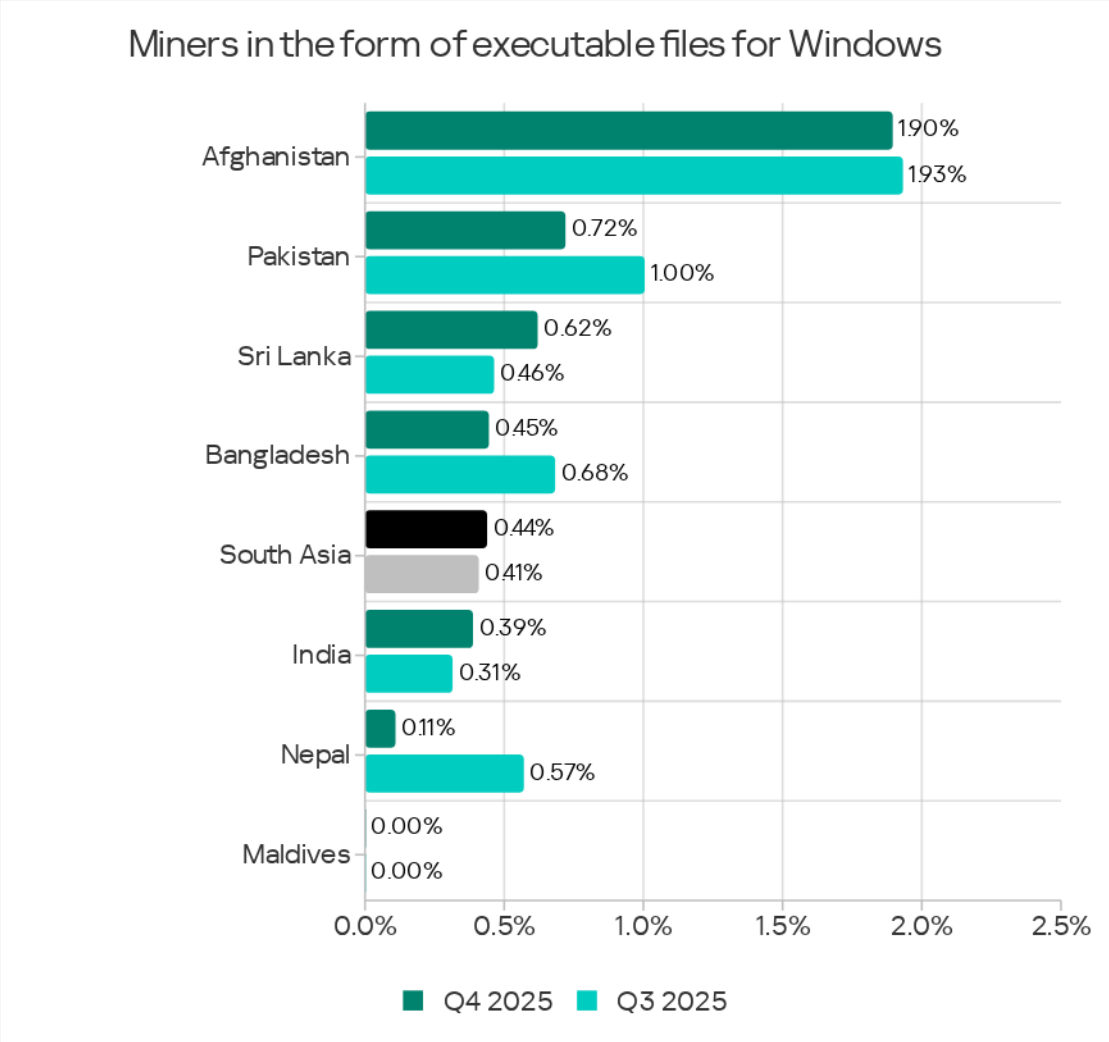
Miners in the form of executable files for Windows

At 0.44%, South Asia came fifth among all regions by percentage of ICS computers on which miners in the form of executable files for Windows were blocked. This figure was 3.1 times higher than in North America (Canada), which had the lowest rate.

Miners in the form of executable files for Windows were one of four threat categories in the region that increased over the quarter.



Among countries of the region, Afghanistan led by a wide margin with 1.90%. During the quarter, these figures increased in Sri Lanka and India.

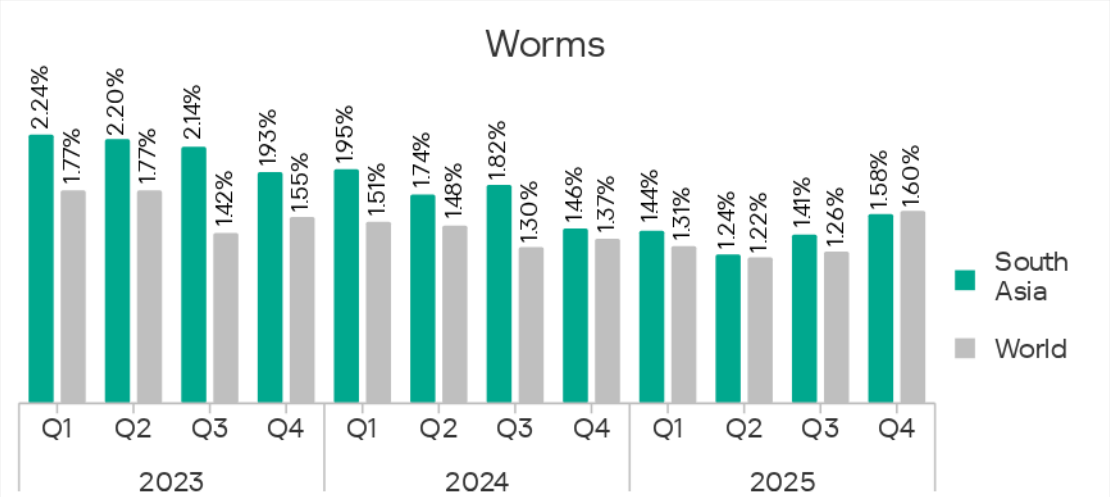


This threat was distributed over the internet and through removable media, but much more frequently over the internet.

Worms

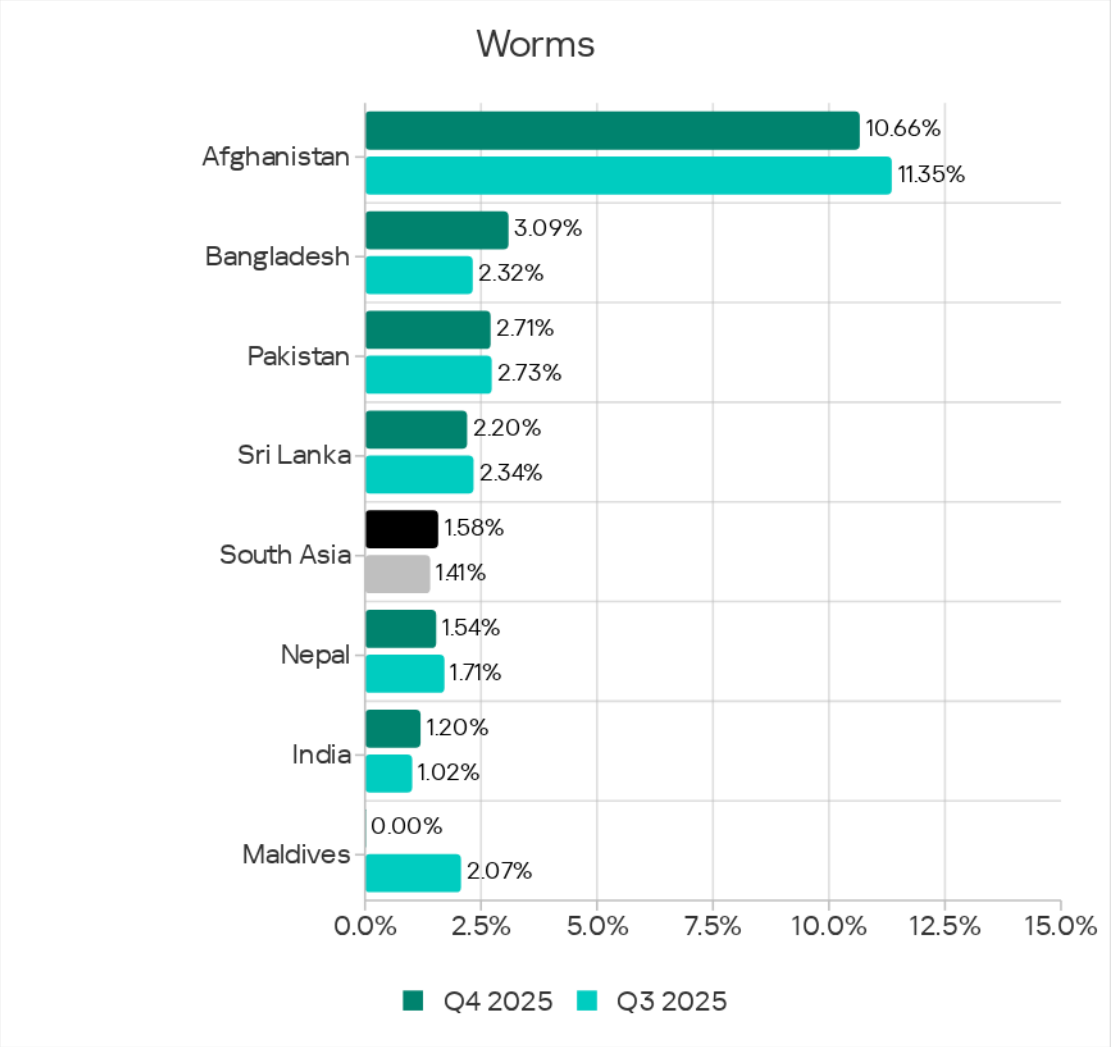
South Asia ranked eighth regionally in the percentage of ICS computers on which worms were blocked.

In Q4 2025, the worms metric grew across all regions due to the latest wave of phishing campaigns known as Curriculum-vitae-catalina which we described earlier. In South Asia, this figure grew to 1.58%, which was 4.9 times higher than in Northern Europe, which had the lowest figure among regions.



Among threat categories in South Asia, worms placed fourth. In addition to South Asia, worms also occupied a high position in the regional rankings in the following three regions: Russia, Central Asia and South Caucasus, and Africa.

Within South Asia, Afghanistan was the clear leader with an extremely high worm blocking rate of 10.66% on ICS computers. The figures over the quarter grew only in Bangladesh and India.



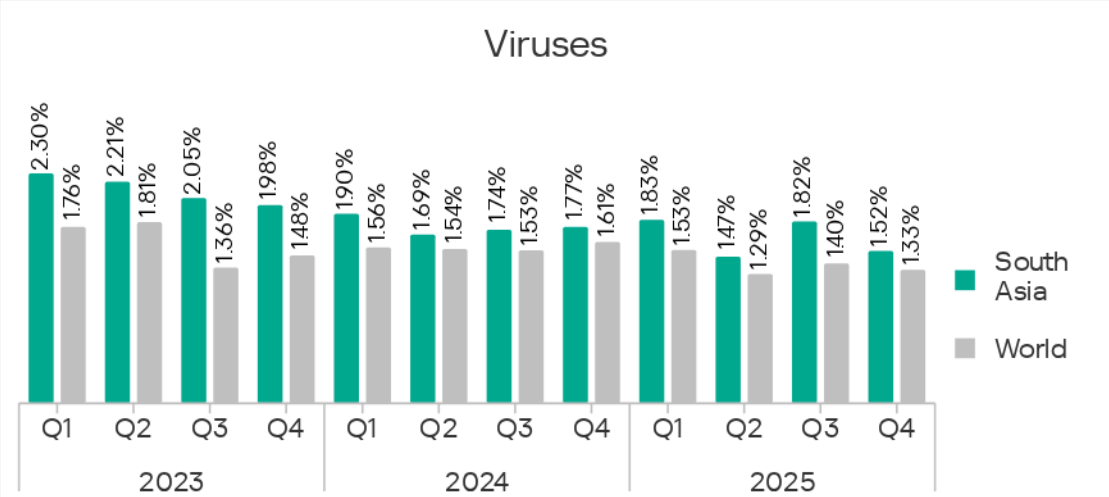
Worms in the region spread via every threat source, but they were most commonly blocked when removable media were connected. Afghanistan also led the region for this threat source and by a similarly significant margin.

Viruses, and malware for AutoCAD

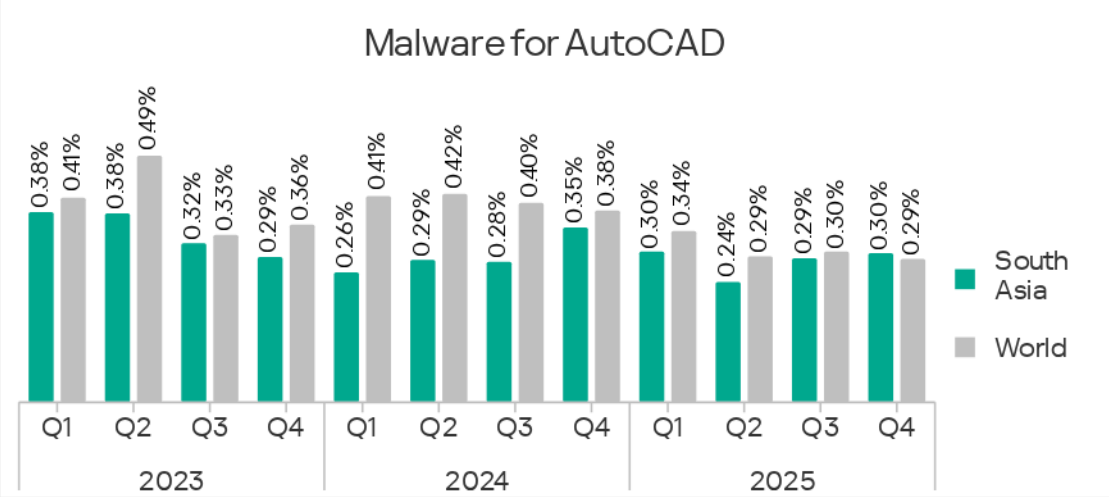
South Asia ranked fifth for ICS computers on which viruses were blocked, and fourth by malware for AutoCAD.

As in East and Southeast Asia, malware for AutoCAD in South Asia usually spreads the same way as viruses. This explains the high percentage for this category.

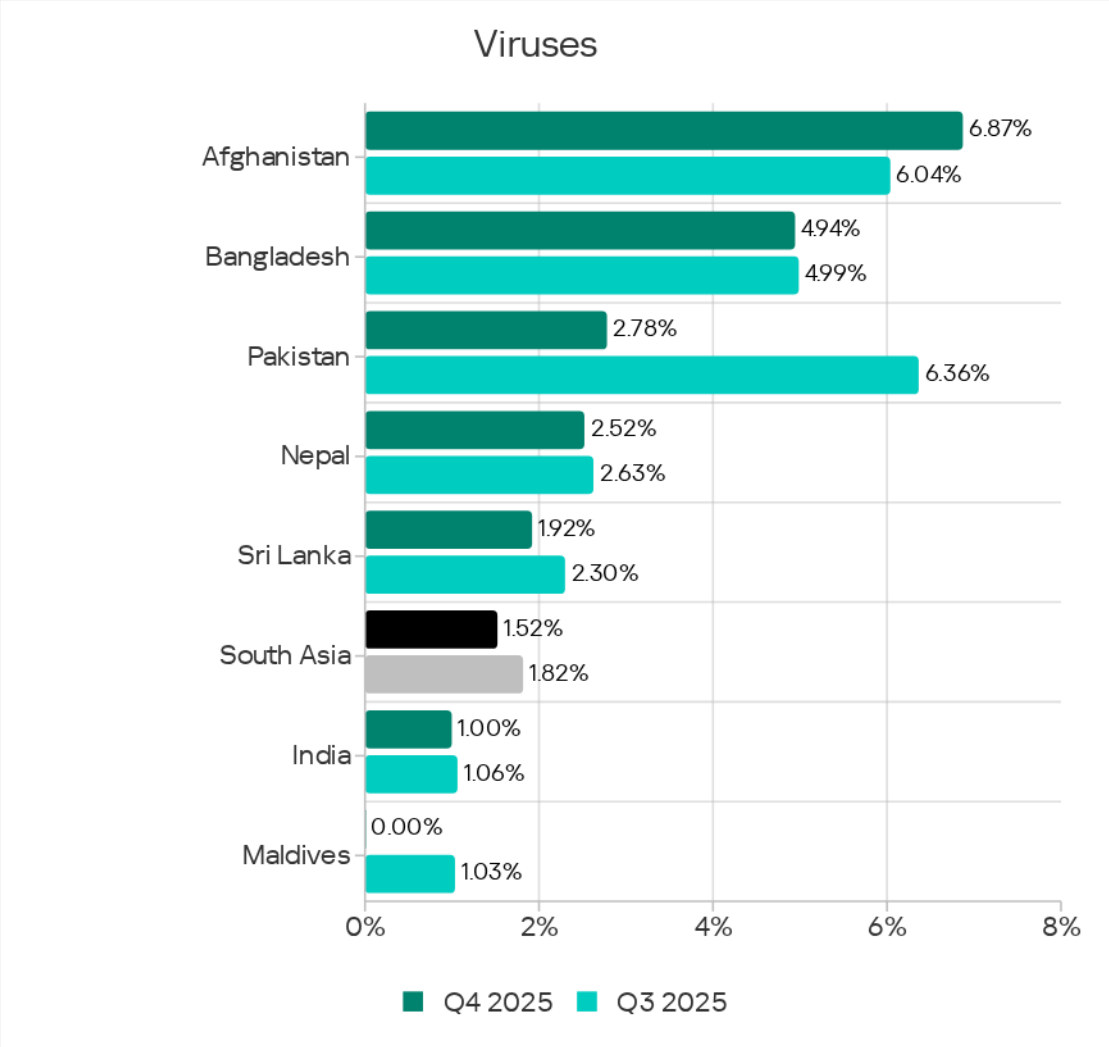
The virus count in South Asia has been declining. In Q4 2025, it decreased to 1.52%, which was 10.1 times higher than in Western Europe, which had the lowest figure among regions.



The percentage of ICS computers in South Asia on which malware for AutoCAD was blocked increased slightly, reaching 0.30%. This was 30 times higher than in Northern Europe, which was last in this ranking of regions.

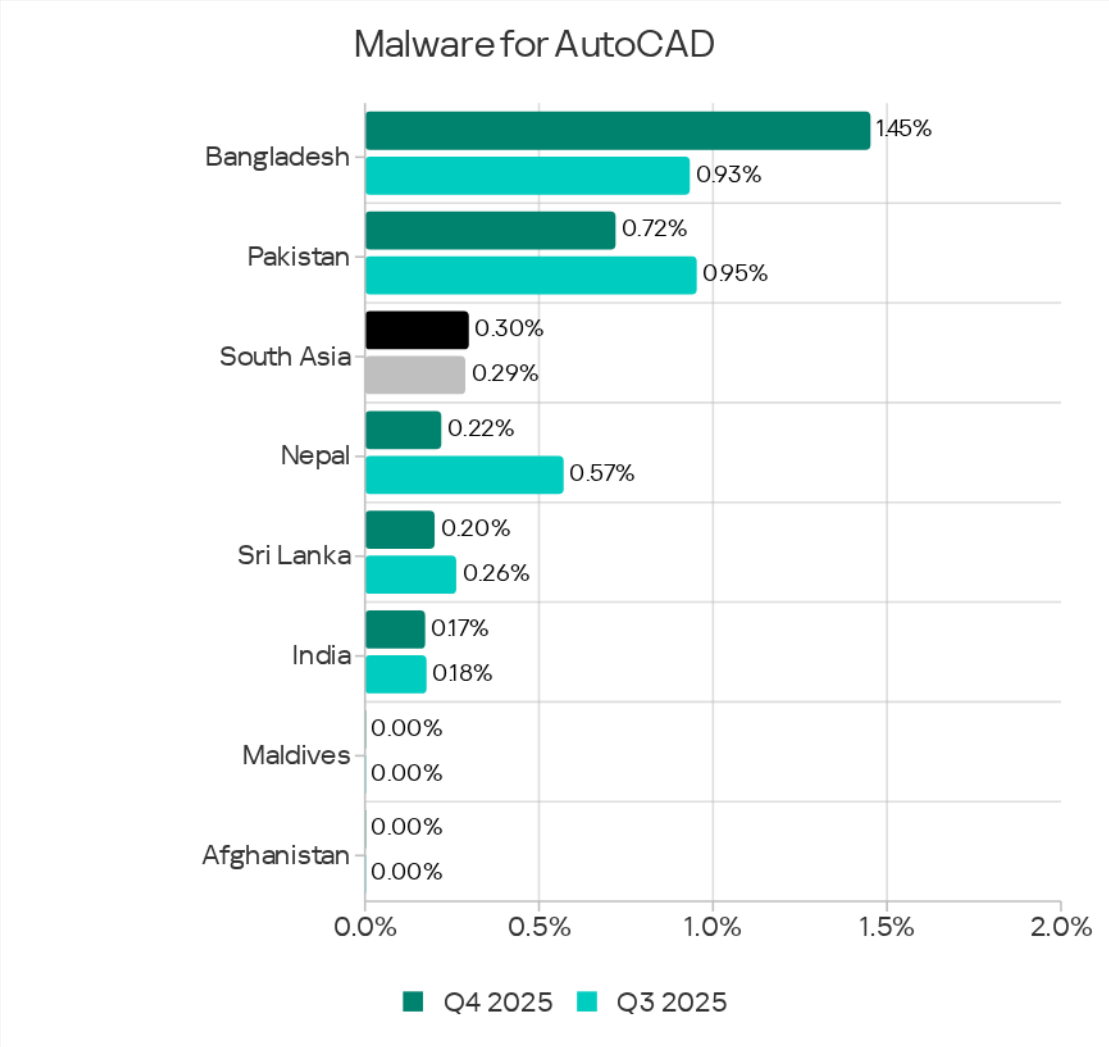


Among the region's countries, Afghanistan led in the percentage of ICS computers on which viruses were blocked, at 6.87%. The figure for Pakistan, which almost doubled during the previous quarter, returned to a more typical level.



Viruses in the region spread through all threat sources, but mainly via removable media. Afghanistan also led the region in the percentage of ICS computers on which threats from removable media were blocked.

Bangladesh ranked first in the percentage of ICS computers on which malware for AutoCAD was blocked, with 1.45%. The figure for this country almost doubled during the previous quarter, and this growth continued during Q4.

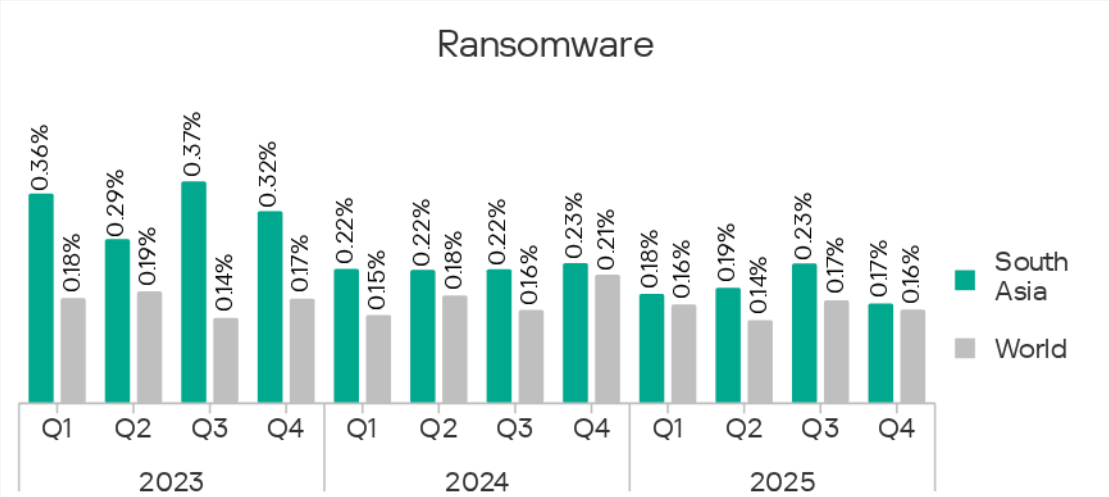


Malware for AutoCAD in the region was most frequently distributed through network folders.

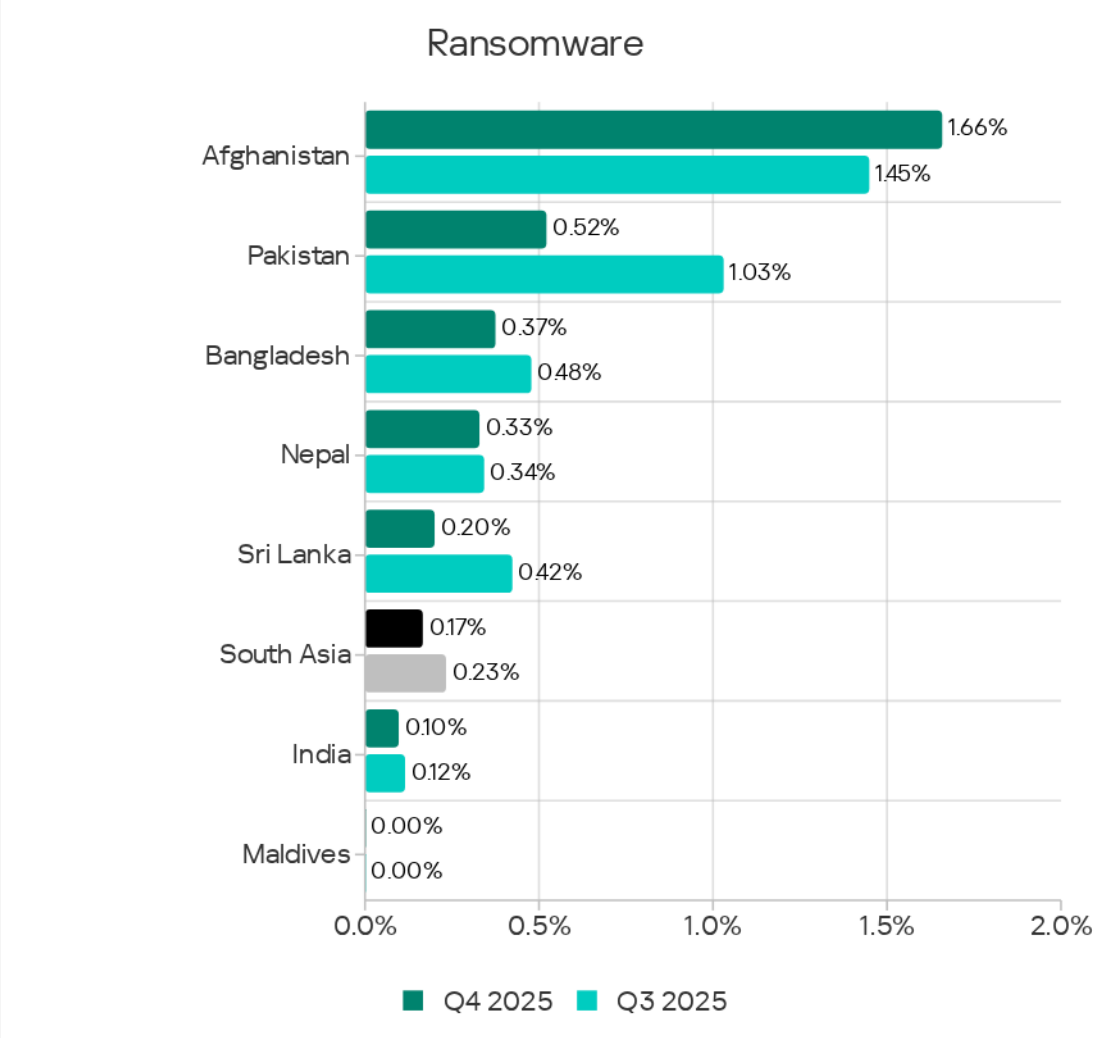
Ransomware

In terms of ICS computers on which ransomware was blocked, South Asia ranked fifth globally, with 0.17%. This figure was 3.4 times higher than in Northern Europe, which had the lowest rate.

The percentage of ICS computers on which ransomware was blocked fluctuates in the region.



Afghanistan led the region with 1.66% of ICS computers on which ransomware was blocked. As with viruses, the figure for Afghanistan almost doubled over the previous quarter. It continued to grow in Q4.



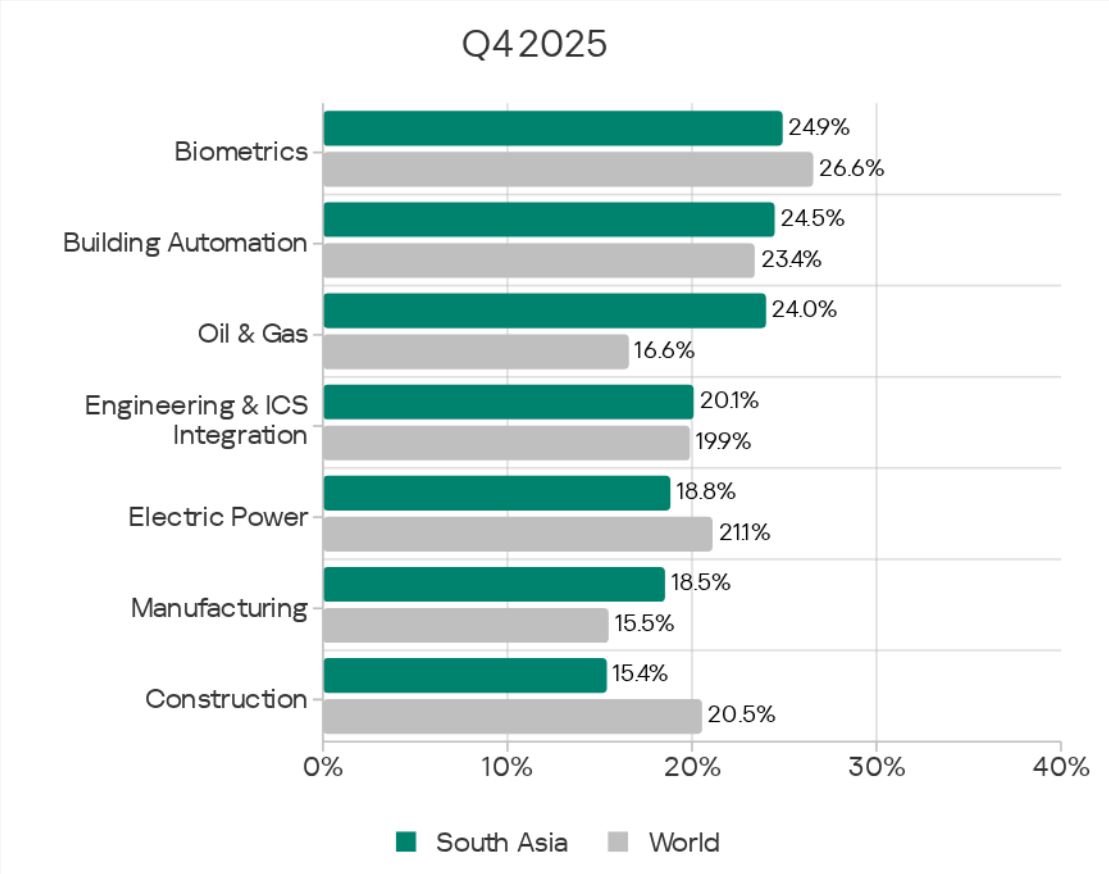
In South Asia, ransomware most often spreads via removable media. Afghanistan was also the regional leader for this threat source.

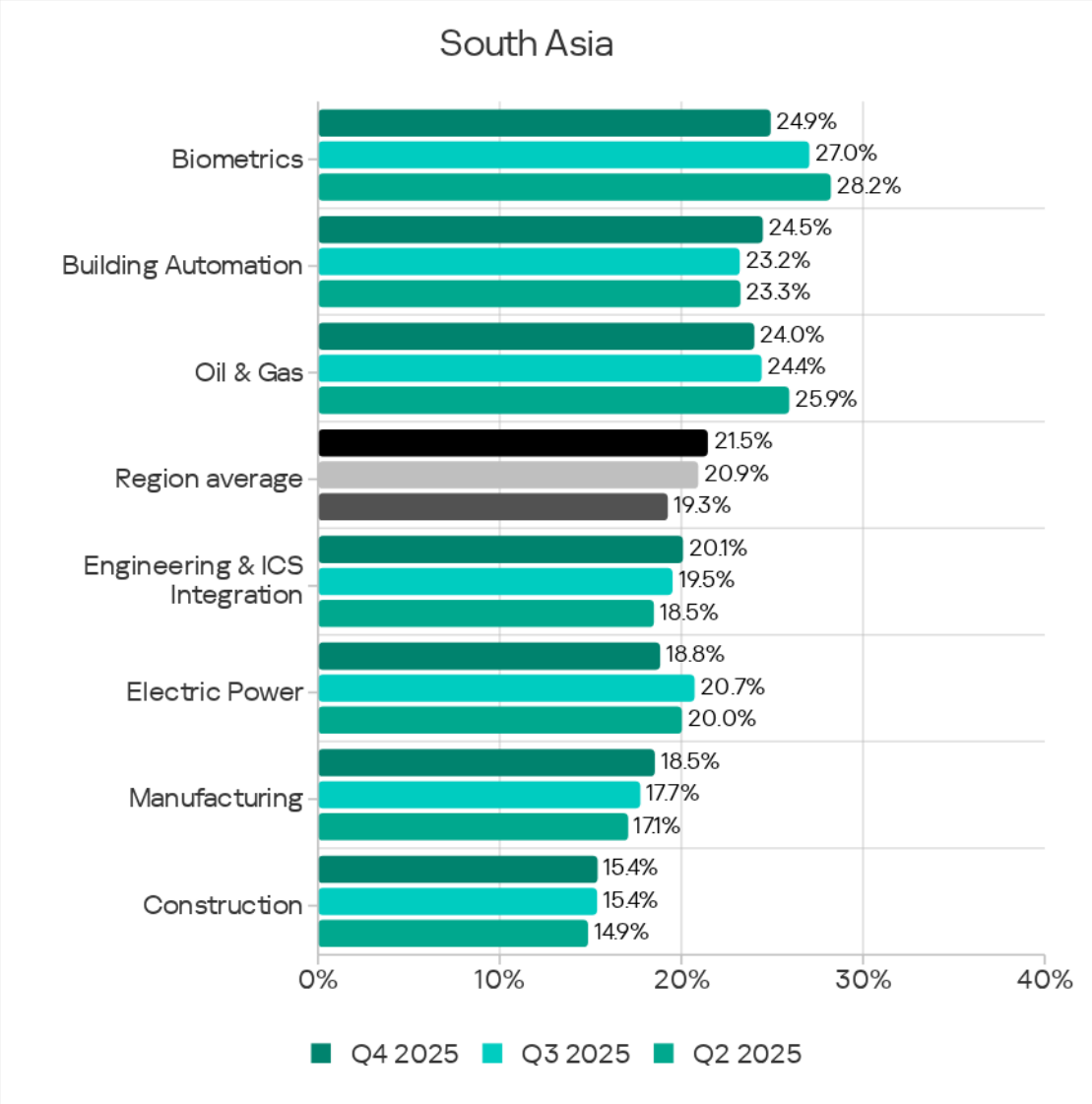
Industries

Among the region's industries covered in this report, the one most frequently facing threats is biometrics.

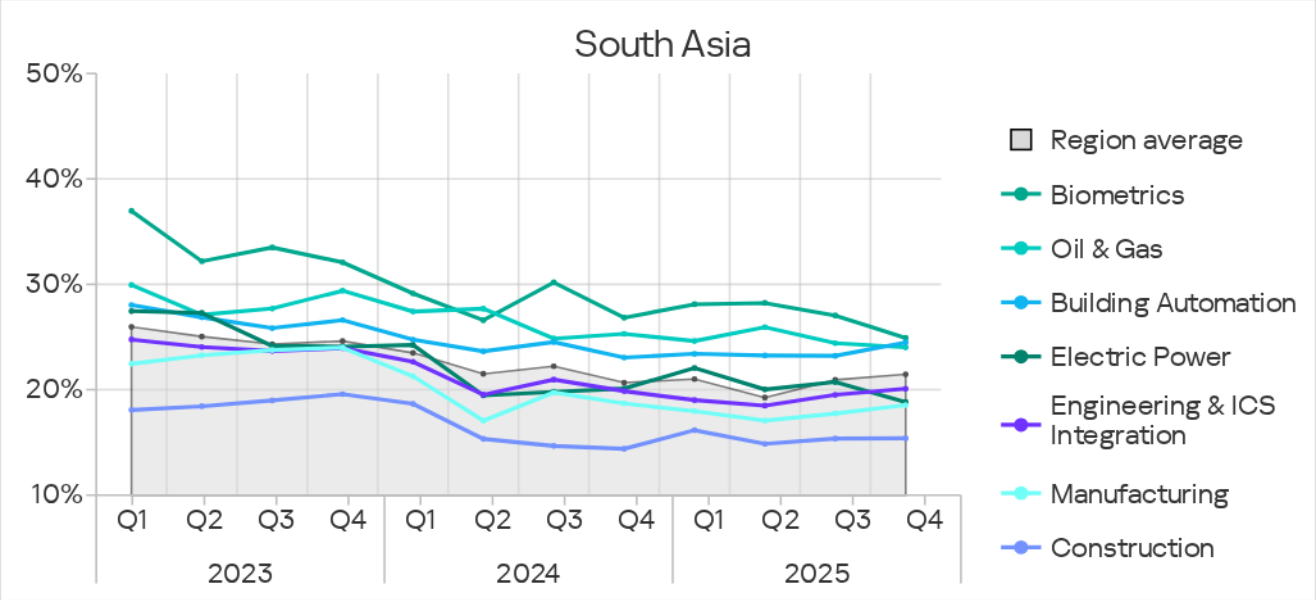
Compared with global averages, the figures were higher in the building automation industry and in the engineering and ICS integrators industry. These industries saw the metric grow over the quarter.

The largest difference from global averages was seen in the manufacturing industry, which was 1.2 times higher in the region than the global average.





All industries reviewed have shown a positive long-term trend (i.e., declining figures) since Q4 2023, with periodic fluctuations.



Threat sources and malware categories in industries: 'hotspots'

We use heat maps when assessing threats to industries in the regions. The color on the heatmap indicates the position in the global industry rankings across regions for each individual threat category or source. Red signifies that the figure is close to the maximum.

Threat source indicators for industries in South Asia, Q4 2025

Industry / Threat source	Biometrics	Building Automation	Engineering & ICS Integration	Electric Power	Oil & Gas	Construction	Manufacturing	Category metric in region
Internet	11.12%	12.08%	12.08%	8.61%	10.63%	8.80%	10.12%	11.33%
Email clients	4.43%	2.95%	0.76%	2.34%	4.72%	1.01%	1.37%	1.92%
Removable media	1.42%	0.67%	0.29%	0.44%	—	0.20%	0.39%	0.50%
Network folders	—	0.05%	0.02%	—	0.79%	0.05%	—	0.03%
Industry metric in region	24.92%	24.48%	20.09%	18.83%	24.02%	15.39%	18.54%	

Threat category indicators for industries in South Asia, Q4 2025

Industry / Threat type	Biometrics	Building Automation	Engineering & ICS Integration	Electric Power	Oil & Gas	Construction	Manufacturing	Category metric in region
Denylisted internet resources	3.18%	3.00%	2.98%	2.53%	6.69%	2.11%	2.87%	2.87%
Malicious scripts and phishing pages (JS and HTML)	11.20%	11.80%	10.38%	8.66%	9.84%	7.72%	9.14%	10.50%
Malicious documents (MSOffice + PDF)	3.43%	2.22%	0.80%	1.56%	1.57%	0.52%	0.98%	1.52%
Spy Trojans, backdoors and keyloggers	5.43%	3.59%	1.63%	2.77%	3.94%	1.25%	2.15%	2.60%
Ransomware	0.67%	0.20%	0.11%	—	0.39%	0.05%	0.07%	0.17%
Miners in the form of executable files for Windows	0.67%	0.49%	0.38%	0.19%	0.79%	0.17%	0.59%	0.44%
Web miners running in browsers	0.42%	0.16%	0.18%	0.05%	0.39%	0.07%	0.13%	0.17%
Malware for AutoCAD	0.17%	0.18%	0.38%	0.19%	0.79%	1.06%	0.33%	0.30%
Worms	3.18%	2.27%	0.96%	1.36%	0.39%	0.88%	1.37%	1.58%
Viruses	3.34%	1.84%	1.02%	2.53%	0.39%	1.43%	1.89%	1.52%
Industry metric in region	24.92%	24.48%	20.09%	18.83%	24.02%	15.39%	18.54%	

Characteristics of the region

Industries in the region show a high level of internet threats. Based on the percentage of ICS computers on which internet threats were blocked, the region ranked first for the metrics across all industries except for construction and electric power.

In the region, the figures for internet threats increased across all industries except for biometrics. The manufacturing industry and engineering and ICS integrators industry lead in terms of the growth in this metric.

The malicious scripts and phishing pages metric grew across all industries except for biometrics. In this region, the engineering and ICS integrators and manufacturing industries also led in terms of growth in the percentage of ICS computers on which this threat was blocked.

Based on the percentage of ICS computers on which malicious scripts and phishing pages were blocked, South Asia ranked first among all regions in the electric power, engineering and ICS integrators, and manufacturing industries. The region ranked second for this metric in the building automation industry.

South Asia rose from sixth to third place by percentage of ICS computers on which malicious objects were blocked in the manufacturing industry and in the engineering and ICS integrators industry.

Biometrics

South Asia was fifth in the regional rankings in the percentage of ICS computers on which malicious objects were blocked in biometrics.

Based on industry indicators among regions, South Asia had the following rankings:

- First place in the percentage of ICS computers on which internet threats were blocked.
- Second place in removable media threats.
- Second by percentage of ICS computers on which viruses were blocked.
- Third for malicious scripts and phishing pages, miners in the form of executable files, and ransomware.

Among industries in the region, biometrics had the following rankings:

- First place in the percentage of ICS computers on which internet threats and removable media threats were blocked.
- Third for internet threats.
- First place across all threat categories except malicious scripts and phishing pages, and malware for AutoCAD.
- Second in malicious scripts and phishing pages.

Building automation

South Asia Europe was fifth among all regions based on the percentage of ICS computers on which malicious objects were blocked in the building automation industry.

Based on industry indicators among regions, South Asia had the following rankings:

- First place in the percentage of ICS computers on which internet threats were blocked.
- Third place for removable media threats.
- Second by percentage of ICS computers on which malicious scripts and phishing pages were blocked.

In the regional cross-industry rankings, building automation occupied the following positions:

- First place in network folder threats. Second place in all other threat sources.
- First in malicious scripts and phishing pages.
- Second place in the following threat categories: denylisted internet resources, malicious documents, spyware, ransomware, and worms.
- Third for miners from both categories.

Electric power

South Asia was seventh among regions in the percentage of ICS computers on which malicious objects were blocked in the electrical energy industry.

South Asia ranked first among all regions in terms of the metrics for malicious scripts and phishing pages in this industry.

In the regional cross-industry rankings, the electrical energy industry ranked:

- Third place regionally in email client threats and removable media threats.
- Second place for viruses.
- Third place for malicious documents and spyware.

Engineering and ICS integrators

South Asia was fourth among regions in the percentage of ICS computers on which malicious objects were blocked in engineering and ICS integrators.

Based on industry indicators among regions, South Asia had the following rankings:

- First place in the percentage of ICS computers on which internet threats were blocked.
- First in malicious scripts and phishing pages.
- Third in terms of malware for AutoCAD.

In the regional cross-industry rankings, engineering and ICS integrators had the following positions:

- First place in internet threats.

- Third place in network folder threats.
- Second place in the following threat categories: web miners, and malware for AutoCAD.
- Third place in the following threat categories: denylisted internet resources, malicious scripts and phishing pages, and ransomware.

Manufacturing

South Asia ranked third among regions in the percentage of ICS computers with blocked malicious objects in manufacturing.

Based on industry indicators among regions, South Asia had the following rankings:

- First place in internet threats.
- First in malicious scripts and phishing pages.
- Third place in the percentage of ICS computers on which denylisted internet resources and malware for AutoCAD were blocked.

In the regional cross-industry rankings, the manufacturing sector ranked:

- Second in miners in the form of executable files.
- Third in the following threat categories: worms, viruses, and malware for AutoCAD.

Construction

South Asia was eighth among regions in the percentage of ICS computers on which malicious objects were blocked in the construction industry.

In the regional cross-industry rankings, the construction sector ranked:

- Second in network folder threats.
- First in terms of malware for AutoCAD.

East Asia

Key cybersecurity issues in the region

Absence or ineffectiveness of perimeter defenses for OT networks

In East Asia, the level of spyware detections remains consistently high for the region. In the fourth quarter of 2025, this category ranked first among all malware categories in the percentage of ICS computers on which it was blocked. East Asia was the only region were spyware occupied first place in these rankings.

Finding spyware on ICS computers usually indicates that the initial infection vector — whether a malicious link, an attachment from a phishing email, or an infected USB device — has already succeeded. This points to the lack or ineffectiveness of OT network perimeter defenses, such as monitoring network communications and enforcing removable media usage policies.

Presence of unprotected OT infrastructure acting as a source of secondary infection (malware spread)

East Asia has high rates of malware spreading via network folders.

By the percentage of ICS computers on which network folder threats were blocked, East Asia ranked first globally. Network folders are typically used to spread viruses and malware for AutoCAD, which are similar in this respect — both infect user files.

Among all industries and regions globally, detections of malware for AutoCAD in East Asia ranked first in the construction sector, second in oil and gas, and fourth in electrical energy.

For threats blocked when accessing data on removable media, the electrical energy industry in East Asia ranked third.

The oil and gas, manufacturing, and construction industries in East Asia occupied the top three positions in the global ranking of all industries and regions for threats blocked when accessing network folders.

East Asia led all the regions for malware for AutoCAD across all industries except for biometrics, where this region ranked second.

High detection rates of self-propagating malware at the industry, country, or regional level likely indicate unprotected OT infrastructures lacking even basic endpoint protection. Such unprotected computers become sources of further malware spread.

Weak enterprise network segmentation and lack of control over removable media further exacerbate the situation.

Lack of control over the use of removable media

By percentage of ICS computers on which removable media threats were blocked, East Asia ranked second among regions, behind only Africa. Worms were the most frequently blocked threat on removable media in the region. Removable media also carry spyware and viruses.

Based on the percentage of ICS computers on which removable drive threats were blocked on connection, East Asia ranked no lower than third across all industries except for biometrics.

Frequent attempts to infect protected systems via USB drives may indicate:

- A low level of enterprise digitalization (lack of secure internal file storage and transfer systems);
- The existence of significant unprotected enterprise infrastructure acting as a source of USB infections;
- A poor overall information security culture.

Cybersecurity adoption lags behind the pace of rapidly developing industries

Based on the percentage of ICS computers on which threats were blocked in the industry, East Asia led all the regions in the electric power industry in Q4 2025 with 31.59%. In the engineering and ICS integration sector, the region ranked third.

East Asia is the world's largest consumer of electricity. Consumption and, consequently, generation in the region continue to grow almost continuously. The high exposure of OT systems in the sector to cyberthreats is therefore unsurprising. When new facilities are commissioned, adequate cybersecurity measures are typically implemented with a considerable delay.

Differences among countries in the region

The cybersecurity situation differs significantly across countries and territories in the region.

The region's overall figures largely depend on the situation in Mainland China,

the leader in removable media threats, network folder threats, and threats distributed through these sources. This was the main driver behind the region's high rankings for viruses and malware for AutoCAD.

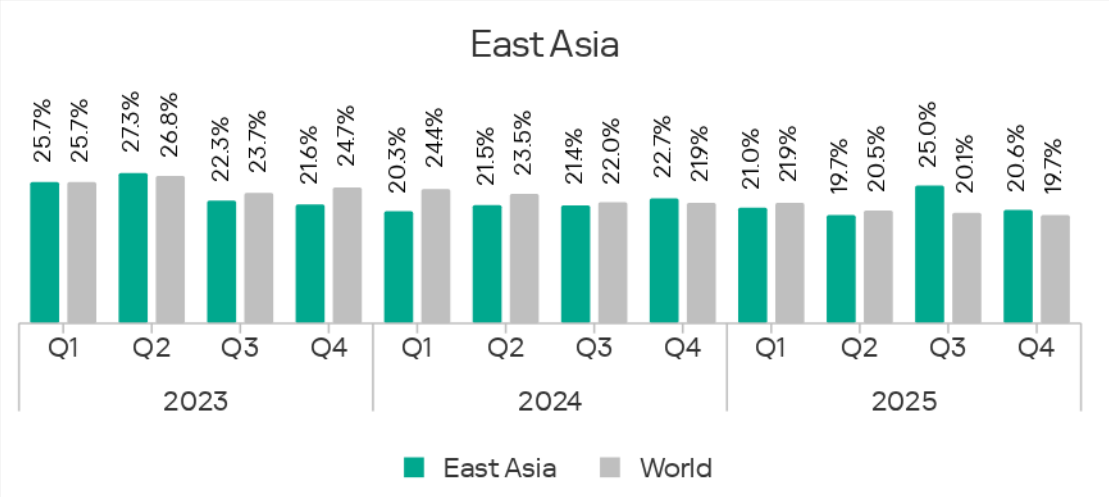
China also led by a wide margin for spyware, pushing this threat category to first place in the regional rankings, while the region ranked third globally in spyware.

Mainland China led the rankings for six out of 10 threat categories. Japan consistently ranks last in most categories.

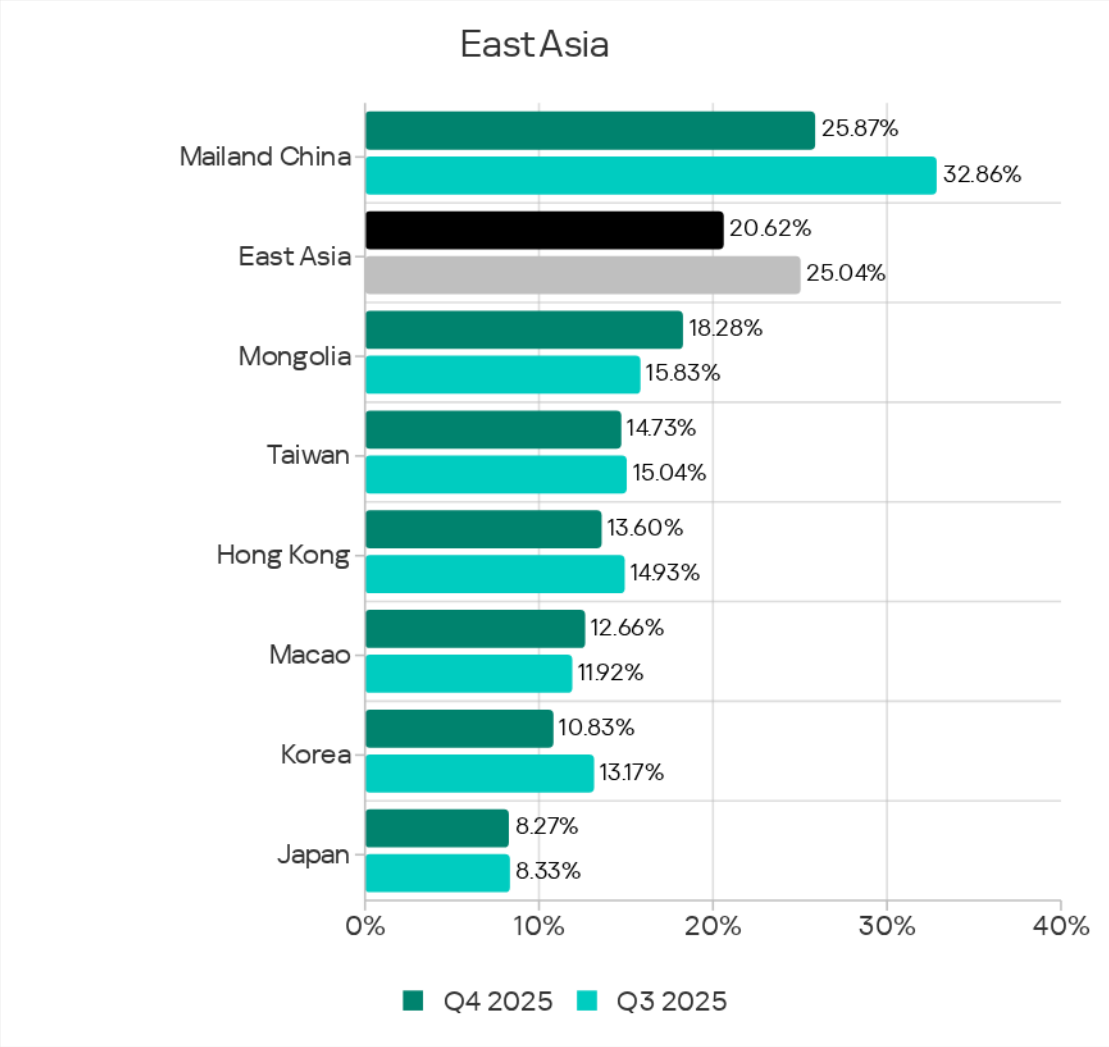
Statistics across all threats

In Q4 2025, East Asia fell from third to fifth place in the regional rankings in the percentage of ICS computers on which malicious objects were blocked. During the previous quarter, the region's figure grew by a factor of 1.3 due to a spike in blocked malicious scripts on computers in the engineering and ICS integrators sector in Mainland China. The metric returned to its normal level in Q4.

The figure in East Asia exceeded the lowest figure, seen in Northern Europe, by a factor of 2.4.



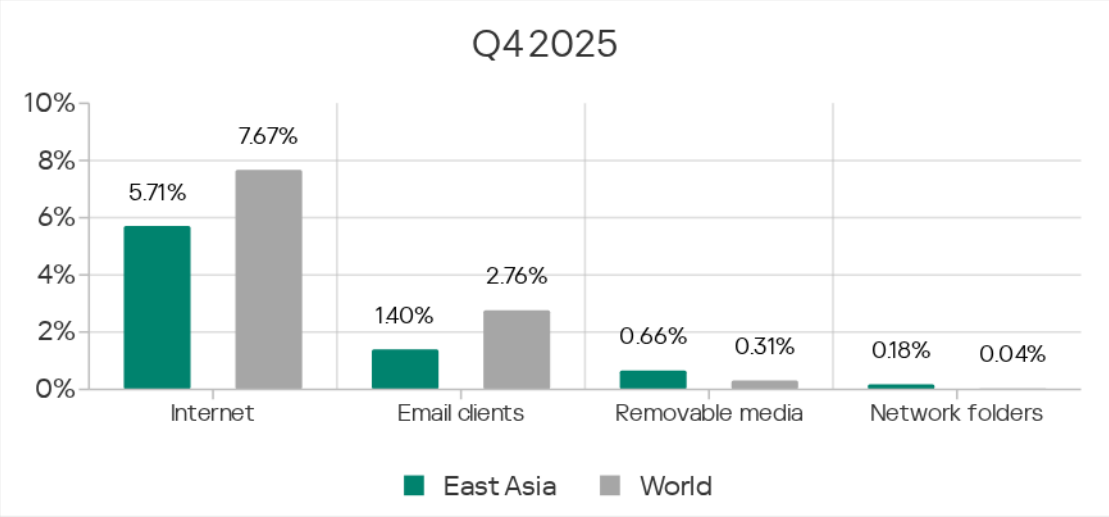
Across the region's countries and territories, rates ranged from 8.27% in Japan to 25.87% in Mainland China.



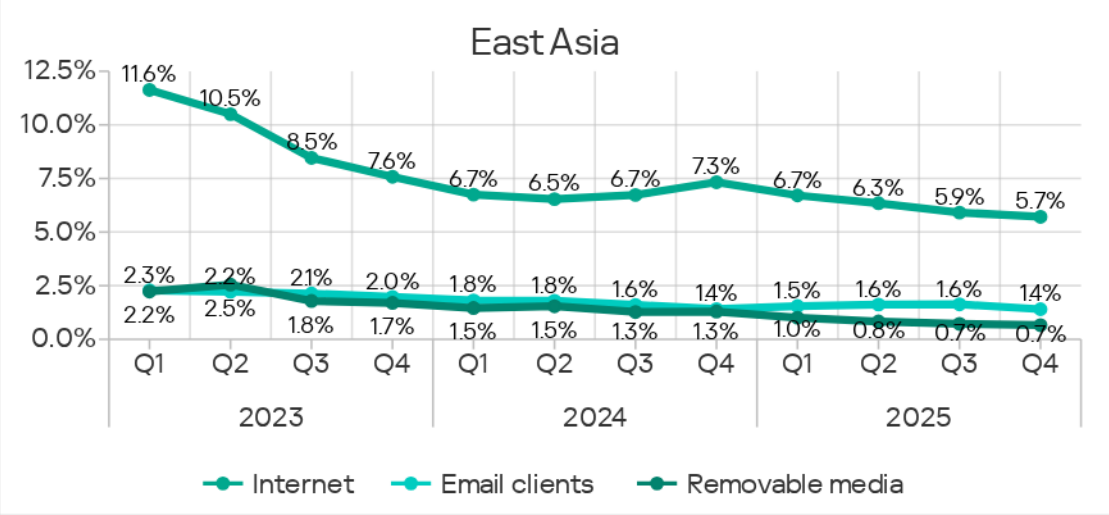
Threat sources

In Q4 2025, East Asia exceeded the global averages for two threat sources:

- Removable media: by 2.1 times, second place globally.
- Network folders: by 4.5 times, ranking first globally.



The percentage of ICS computers on which malicious objects were blocked decreased for all threat sources. Overall, all major threat sources show a long-term downward trend.

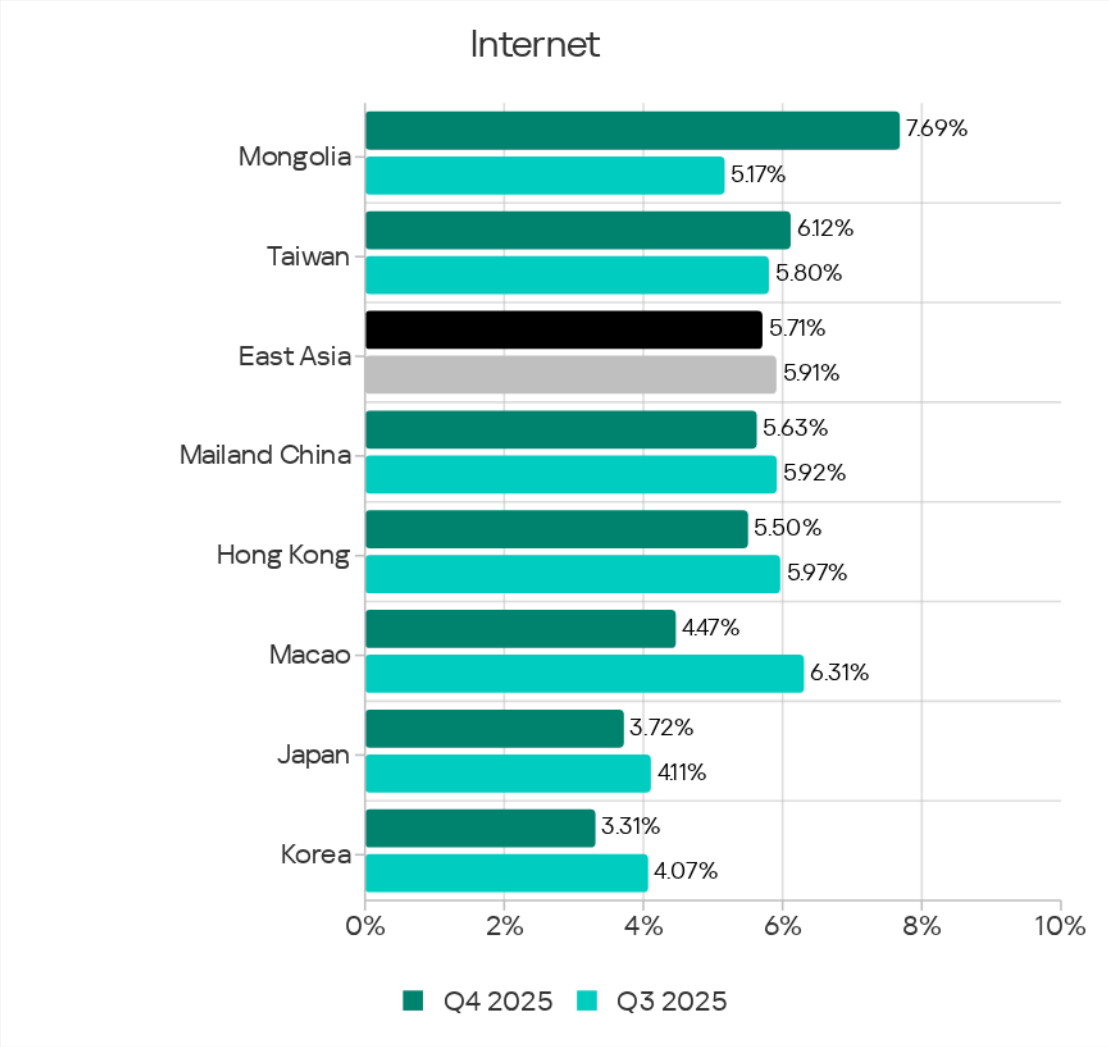


Internet

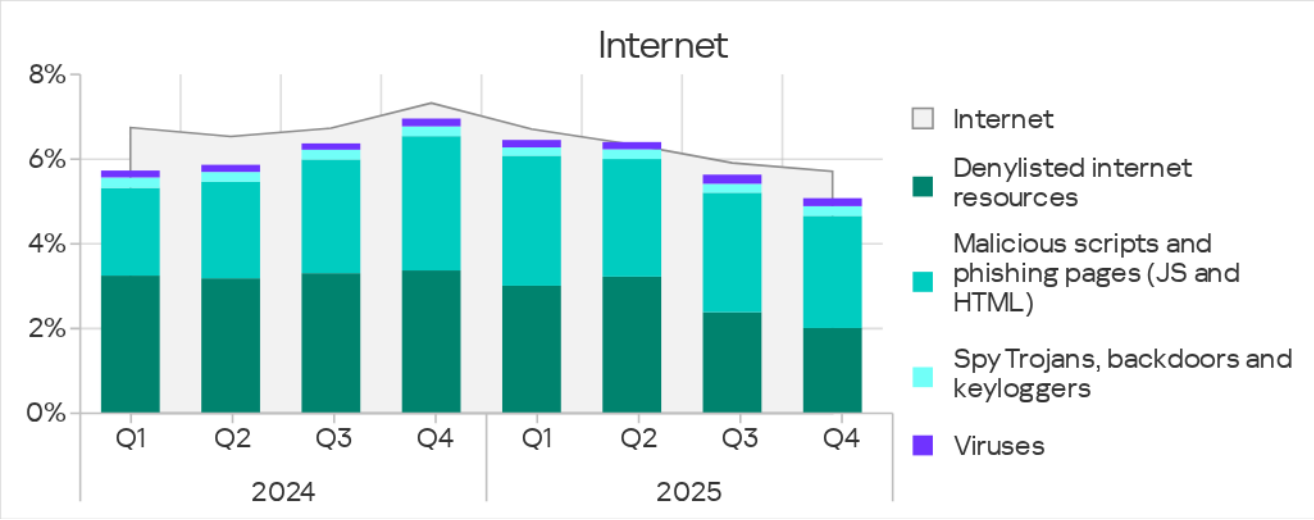
In terms of the percentage of ICS computers on which internet threats were blocked, East Asia placed 13th among all regions.

The indicator for internet threats fell for the fourth straight quarter and reached its lowest level in the past three years – 5.71%. This was 1.4 times higher than the lowest regional value, recorded in Northern Europe.

Across the region, the percentage of ICS computers on which internet threats were blocked ranged from 3.31% in Korea to 7.69% in Mongolia. Although the figure for Mongolia nearly halved during the previous quarter, it returned to levels more typical for the country in Q4.



The main categories of internet threats blocked on ICS computers in the region were malicious scripts and phishing pages, denylisted internet resources, spyware, and viruses.

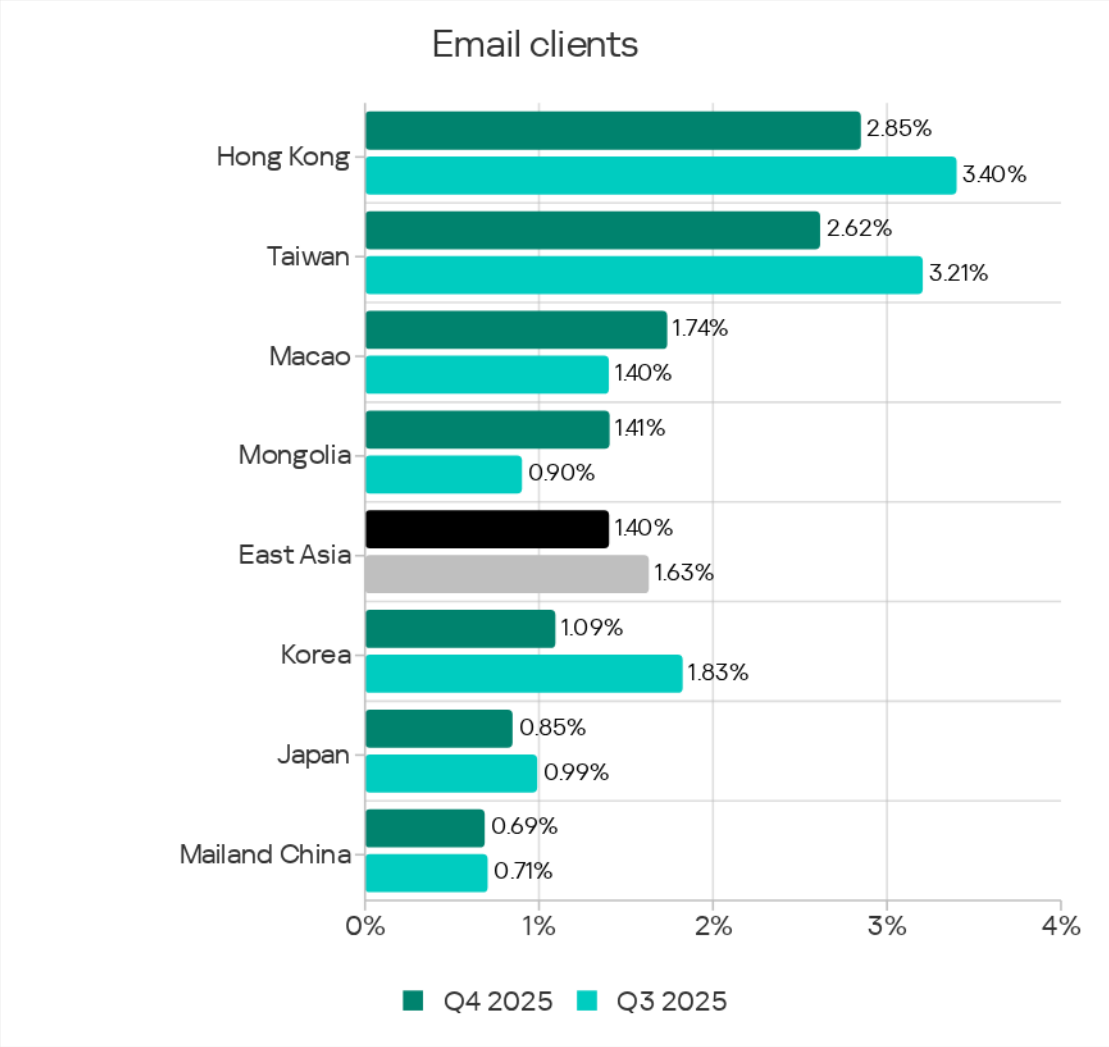


Within the region, Mainland China led by the percentage of ICS computers on which denylisted internet resources were blocked, while Mongolia led in terms of malicious scripts.

Email clients

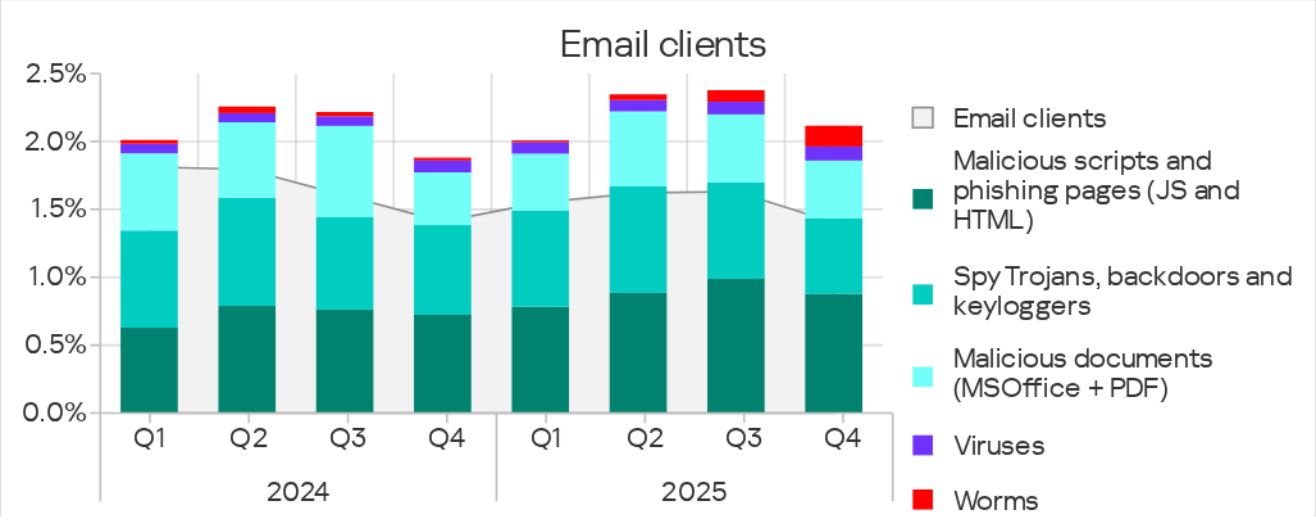
In terms of ICS computers on which mail client threats were blocked, East Asia ranked 11th globally, with 1.40%. This figure was 2.2 times higher than in Northern Europe, which had the lowest rate.

Hong Kong (2.85%) and Taiwan (2.62%) led among the countries and territories in the region. The lowest figure was recorded in Mainland China: 0.69%.



Hong Kong also led in the threat category that spreads mainly via email – malicious documents.

The main categories of mail client threats blocked on ICS computers were malicious documents, spyware, malicious scripts, and phishing pages.



Q4 2025 saw a noticeable increase in the percentage of ICS computers on which worms from email clients were blocked. This increase was connected with the latest wave of phishing campaigns known as Curriculum-vitae-catalina, which launched attacks against organizations across all regions of the world. In East Asia, these attacks peaked in November.

The hackers distributed phishing emails disguised as job applications. Disguised as a resume (Curriculum Vitae), these emails contained a malicious executable file, a remote administration backdoor worm known as Backdoor.MSIL.XWorm. Running that file caused system infection.

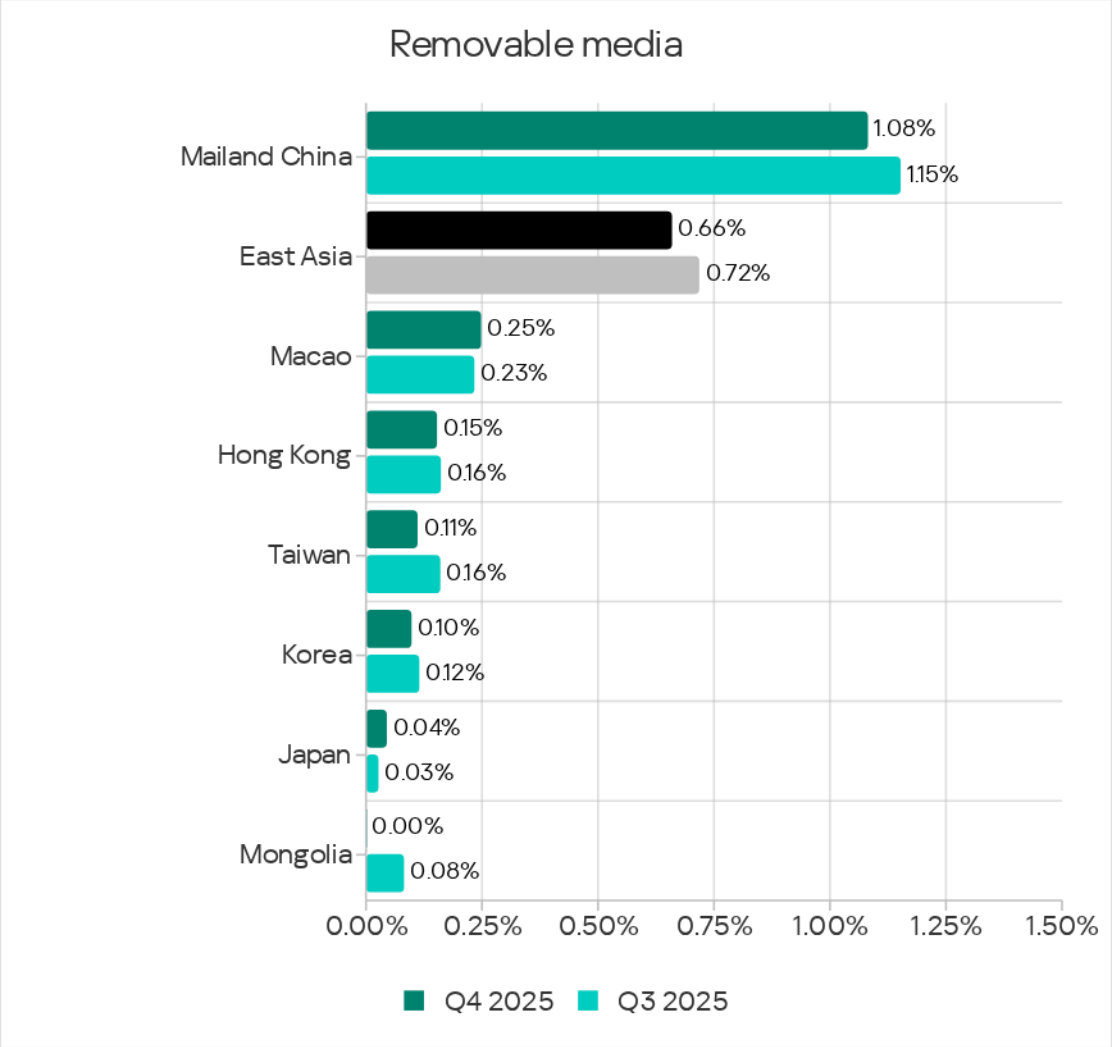
Normally, these campaigns are designed to deliver malware for data theft, spyware, or remote administration tools (RATs).

Removable media

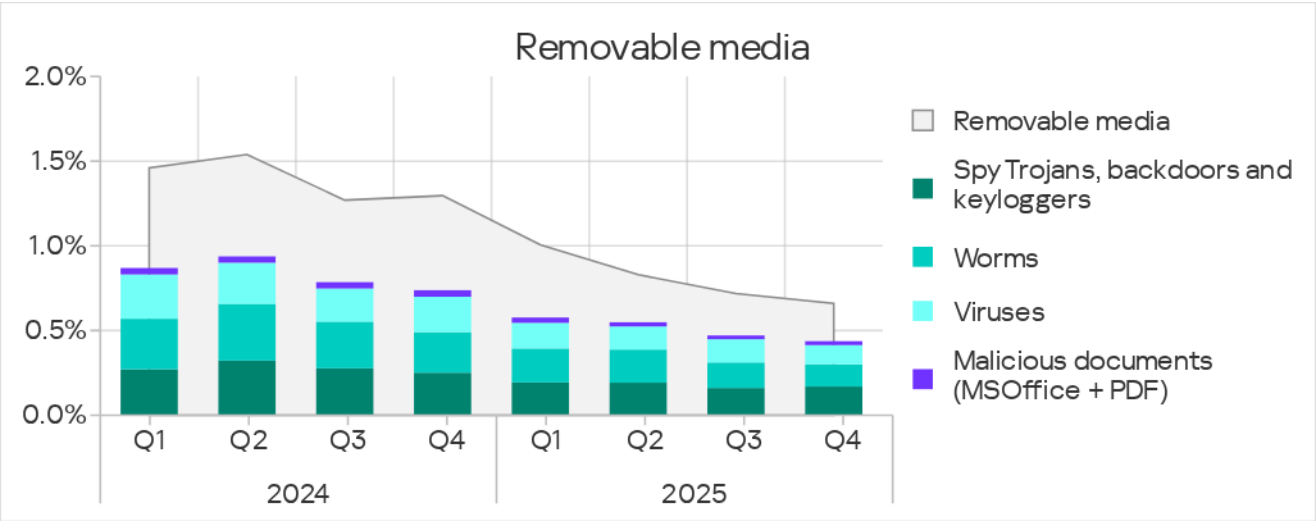
By percentage of ICS computers on which removable media threats were blocked, East Asia ranked second among regions, behind only Africa.

The figure for the region was 0.66%. This was 14.0 times higher than Australia and New Zealand, which had the lowest rate among all regions.

Among the region's countries and territories, Mainland China led by a significant margin, with 1.08%. Other figures ranged from 0.04% in Japan to 0.25% in Macau. In Mongolia, the percentage of ICS computers on which removable media threats were blocked on connection was negligible.

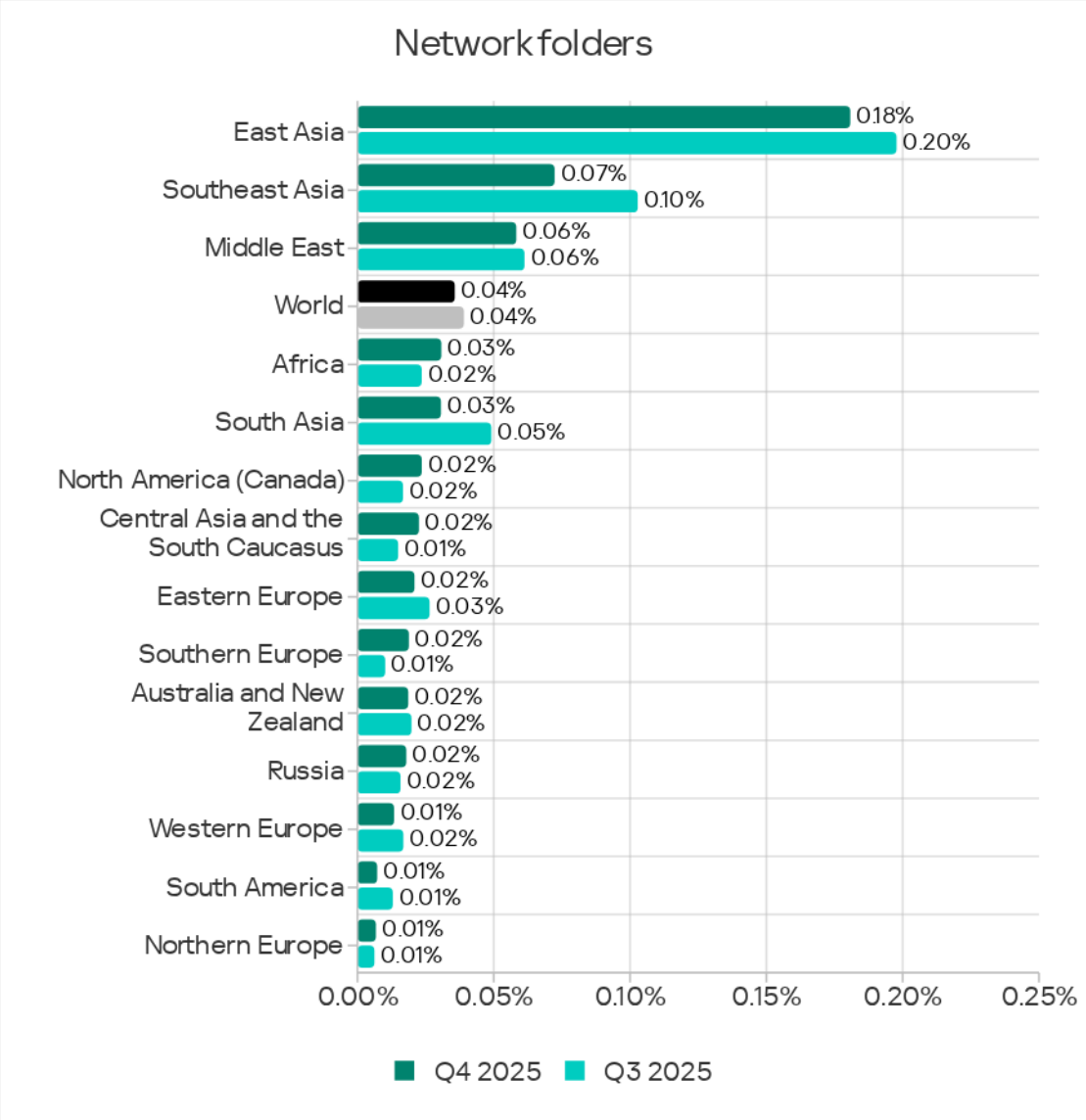


The main categories of threats blocked when connecting removable media to ICS computers were spyware, worms, and viruses. Notably, Mainland China led the ranking in all these threat categories.

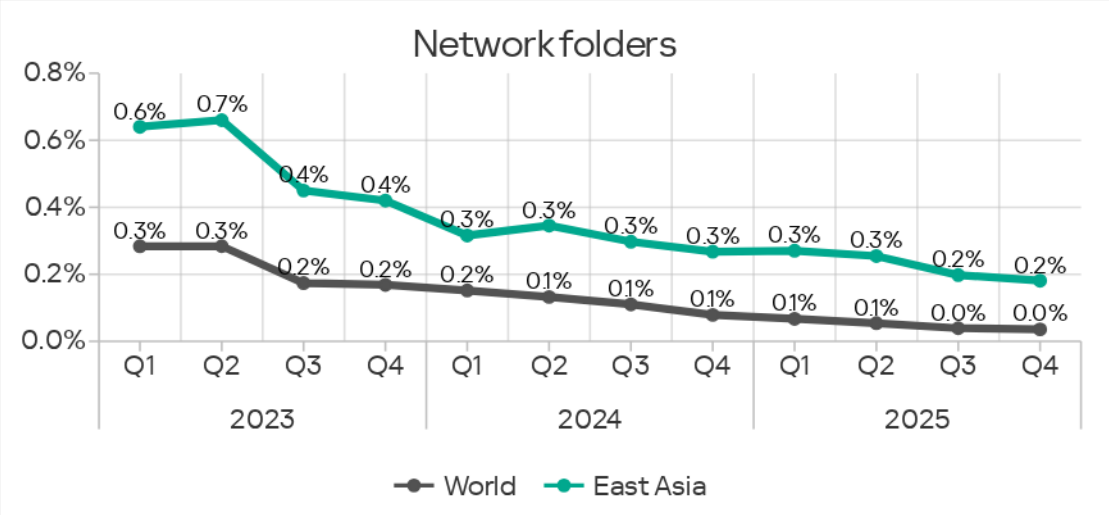


Network folders

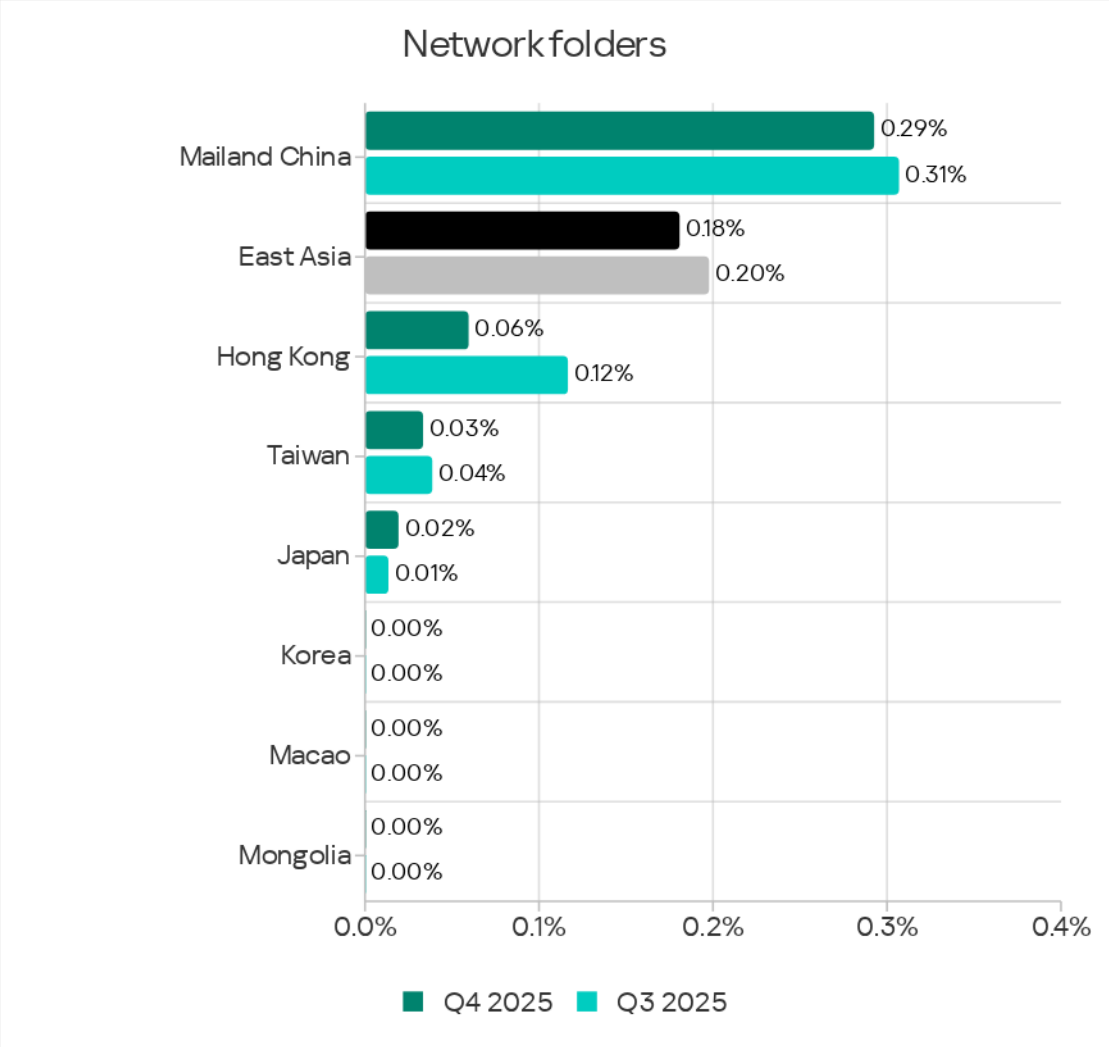
East Asia continues to rank first globally in the percentage of ICS computers on which network folder threats were blocked. In Q4 2025, the figure for the region stood at 0.18%. This figure was 25.9 times higher than in Northern Europe, which boasted the lowest percentage among all regions. The figure for Southeast Asia, which holds second place in these rankings, was 2.5 times less than that for East Asia.



The percentage of ICS computers with threats blocked in network folders in East Asia shows a downward trend. The Q4 2025 figure was the lowest in three years.

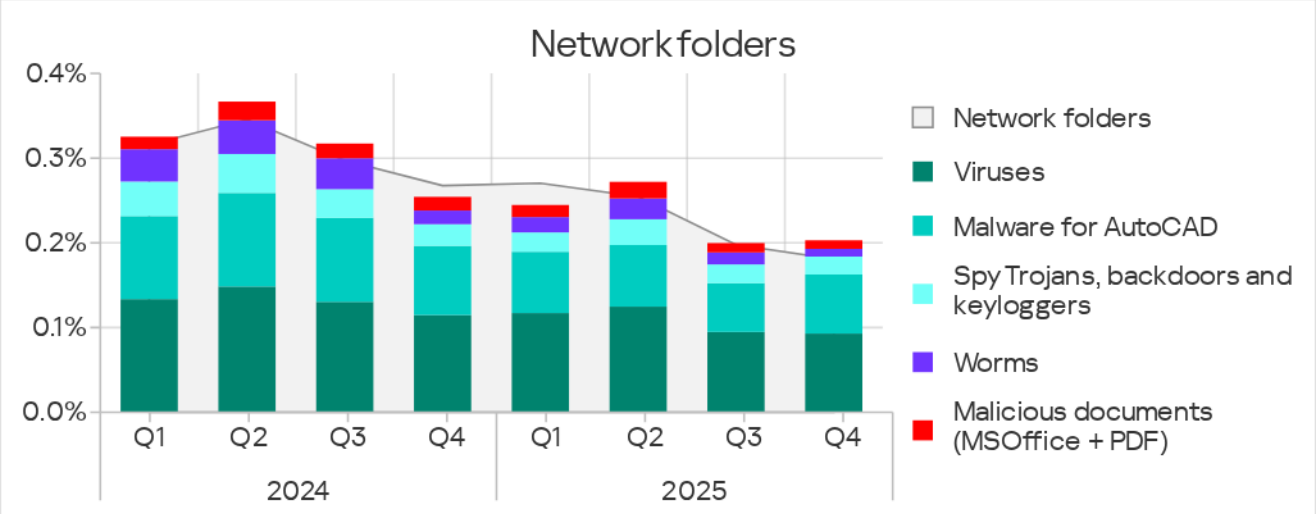


East Asia's first place by the percentage of ICS computers on which network folder threats were blocked was driven by Mainland China, which led by a wide margin for this metric among the region's countries and territories, at 0.29%.



It should be noted that network folder threats were not detected across all countries and territories in the region.

The main threats spreading through network folders were viruses, malware for AutoCAD, and spyware.



Viruses in the region spread through all threat sources, but mainly via the internet and removable media. The network folders threat figure was only 1.1 times lower than the mail client threats and removable media threats figures.

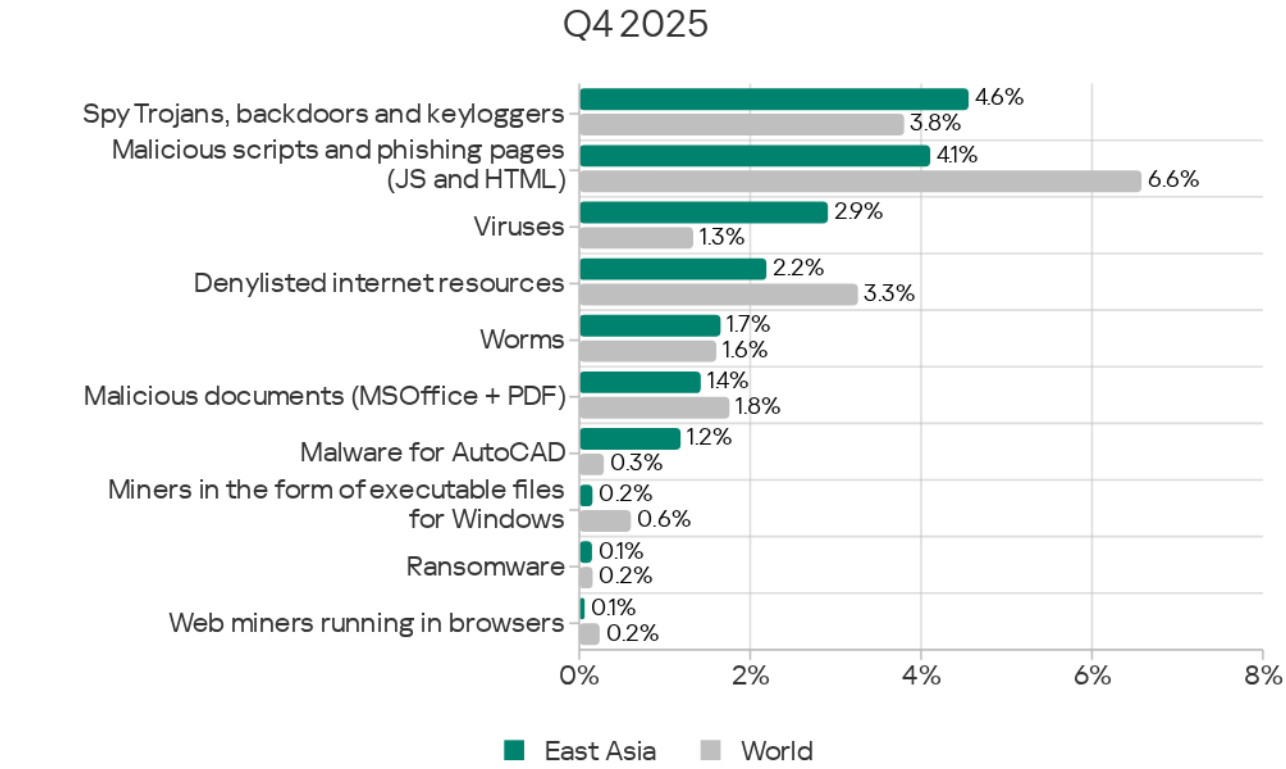
By the percentage of ICS computers on which malware for AutoCAD was blocked, East Asia ranked second globally.

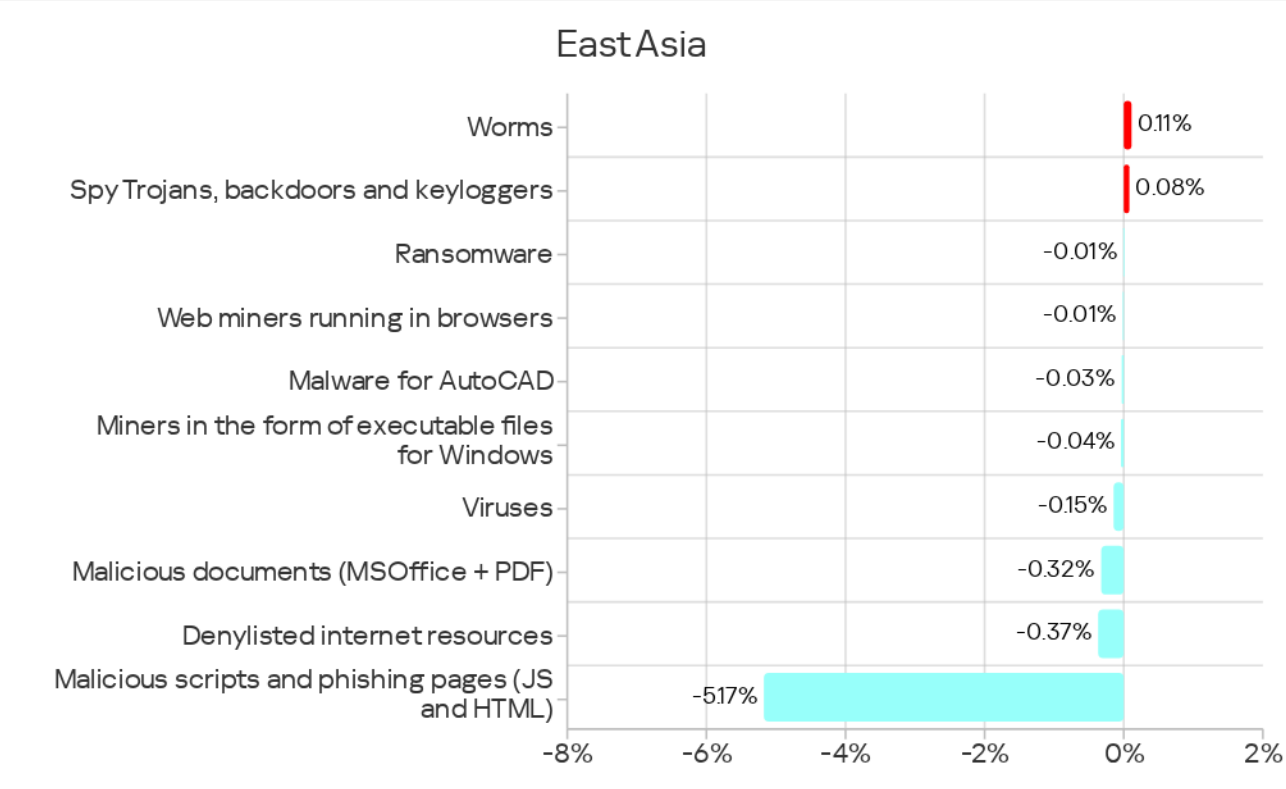
For both viruses and malware for AutoCAD, Mainland China led the region.

Threat categories

In Q4 2025 in East Asia, the most prevalent threat category blocked on ICS computers was spyware. East Asia was the only region where spyware tops these rankings.

The figure for malicious scripts and phishing pages in the previous quarter rose sharply due to the distribution of malicious spy scripts on computers in Mainland China's engineering and ICS integrators sector. This category topped the rankings. In Q4, this metric returned to its typical level for the region, while malicious scripts took second place in these rankings.





The spyware and worm figures grew over the quarter.

Compared with global averages, the region had higher percentages of ICS computers on which the following were blocked:

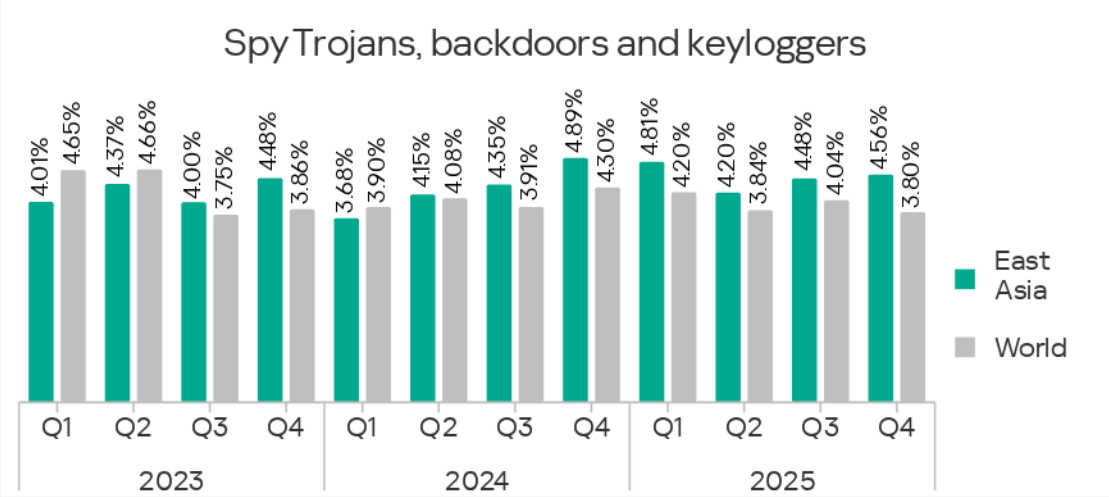
- Worms.
- Spyware: 1.2 times higher.
- Viruses: 2.2 times higher, third globally.
- Malware for AutoCAD: 4.1 times higher, second globally.

Spyware

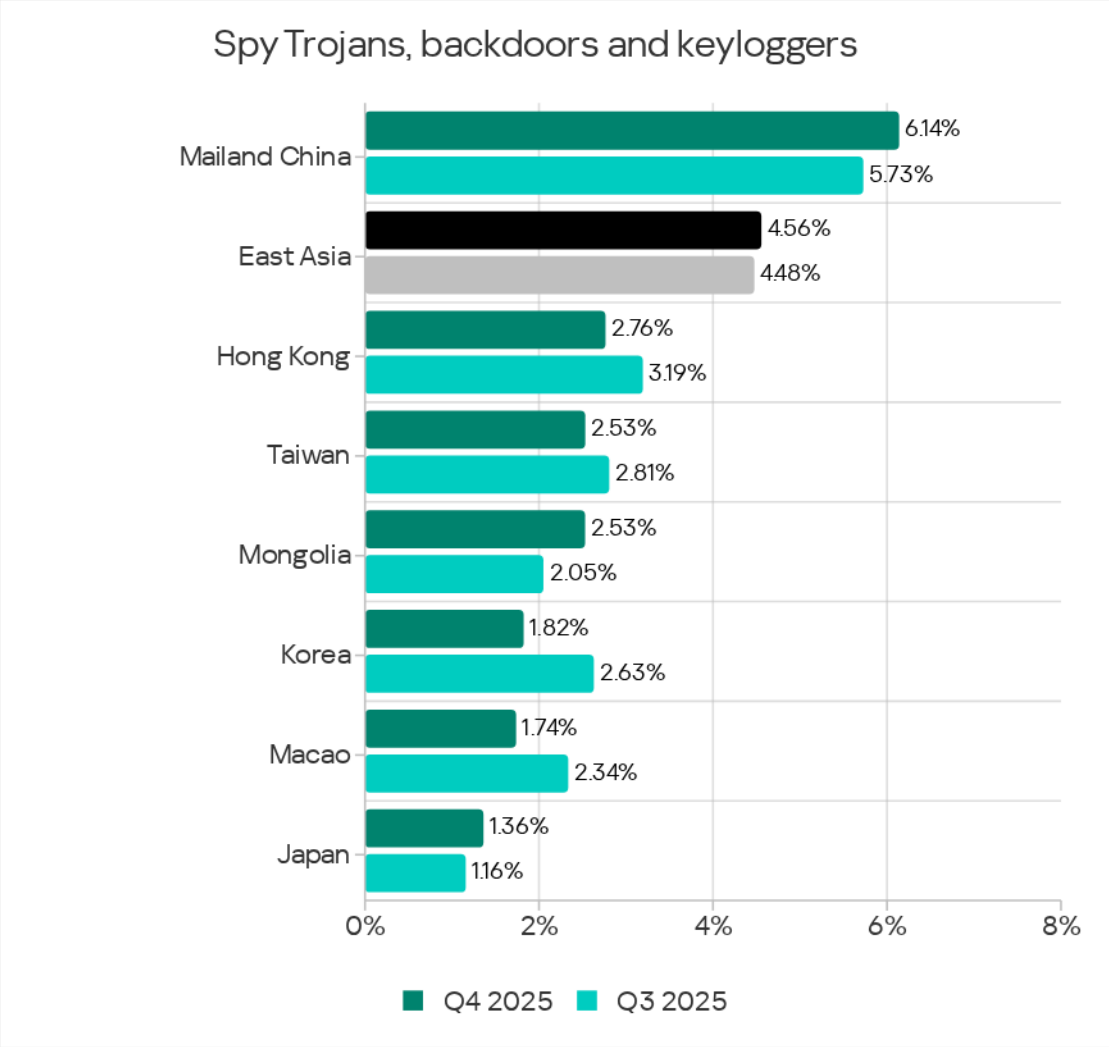
In the percentage of ICS computers on which spyware was blocked, East Asia ranked fifth globally. This was the only region where spyware ranked first among threat categories by the percentage of ICS computers on which the corresponding threat categories were blocked.

The percentage of ICS computers on which spyware was blocked in the region was quite stable and relatively high.

This figure had been growing in the region for two consecutive quarters, reaching 4.56%. This was 3.6 times higher than Northern Europe, where the value was the lowest.



Among the region's countries and territories, Mainland China led in the percentage of ICS computers with blocked spyware, at 6.14%. Japan has the lowest rate at 1.36%.



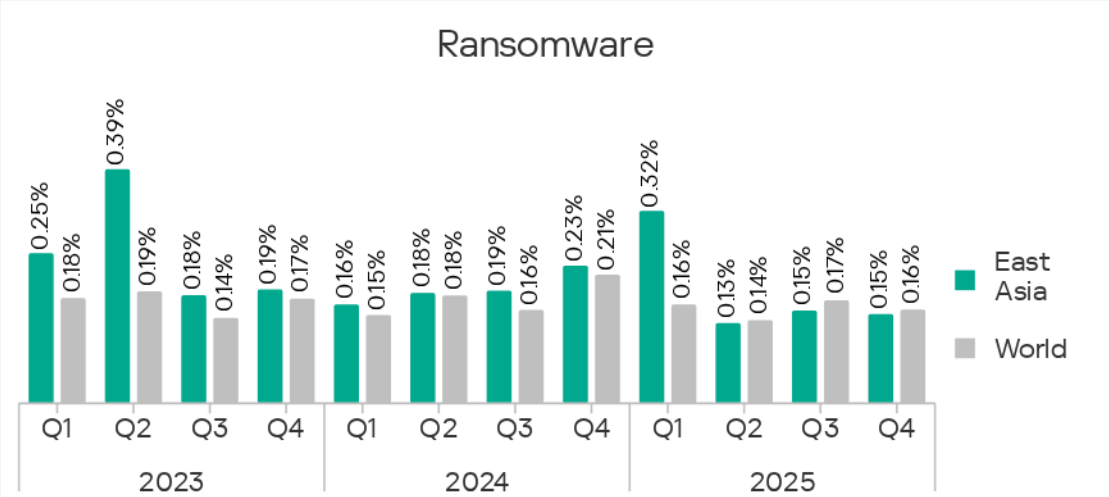
Spyware in the region spreads through all sources; most often through email clients in Q4 2025.

Mainland China, which ranked highest for spyware, also ranked top by the percentage of computers on which threats from removable media on connection and network folder threats were blocked. Hong Kong and Taiwan occupied the top two spots for threats from email.

Ransomware

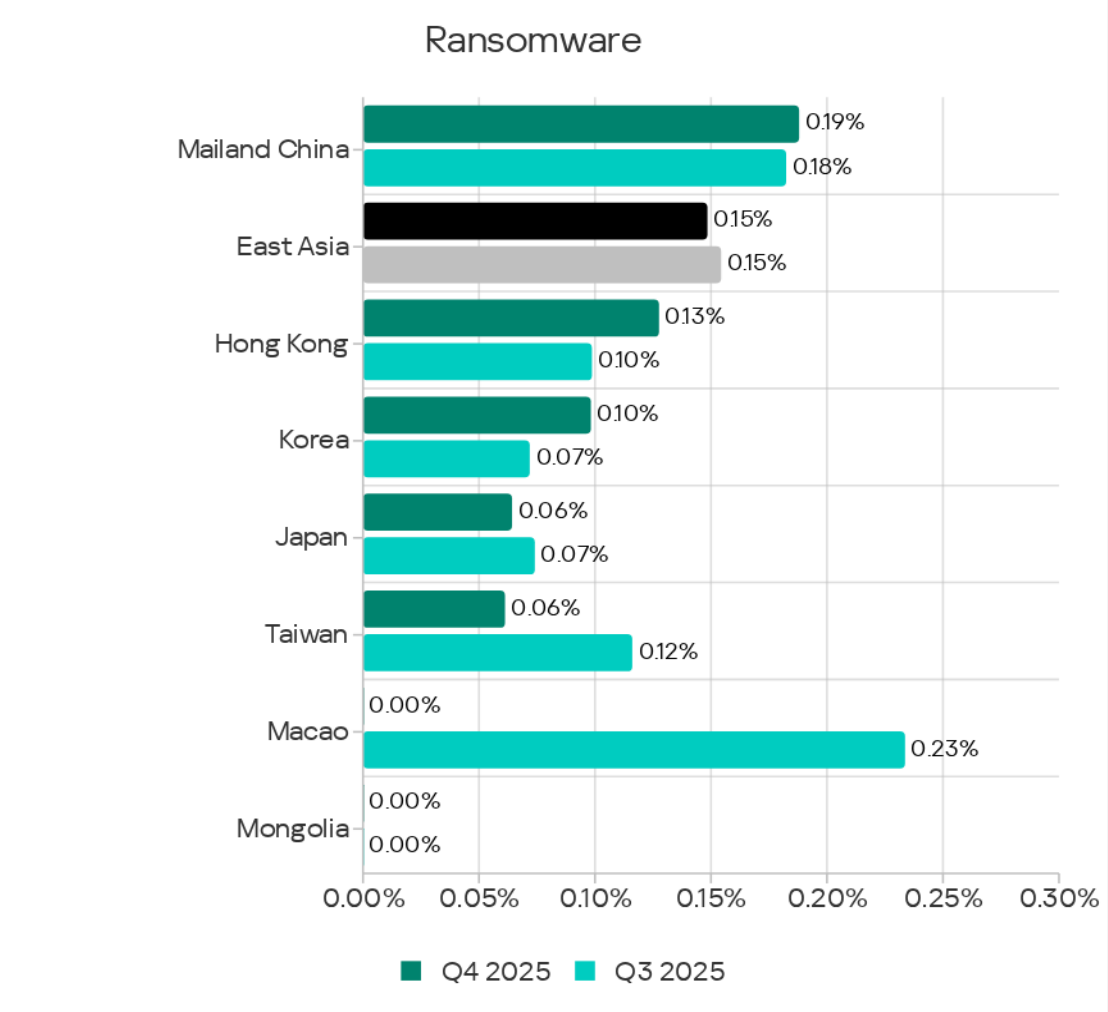
With a figure of 0.15%, East Asia ranked sixth among regions by the percentage of ICS computers on which ransomware was blocked. This figure was 3.0 times higher than in Northern Europe, which had the lowest rate.

In contrast to most other threat categories in the region, the figure for ransomware did not decrease during the quarter.



Among the region's countries and territories, Mainland China led in this metric, with 0.19%. Notably, some countries in the region did not register a significant amount of ransomware.

The figure grew in Mainland China, Hong Kong, and Korea.



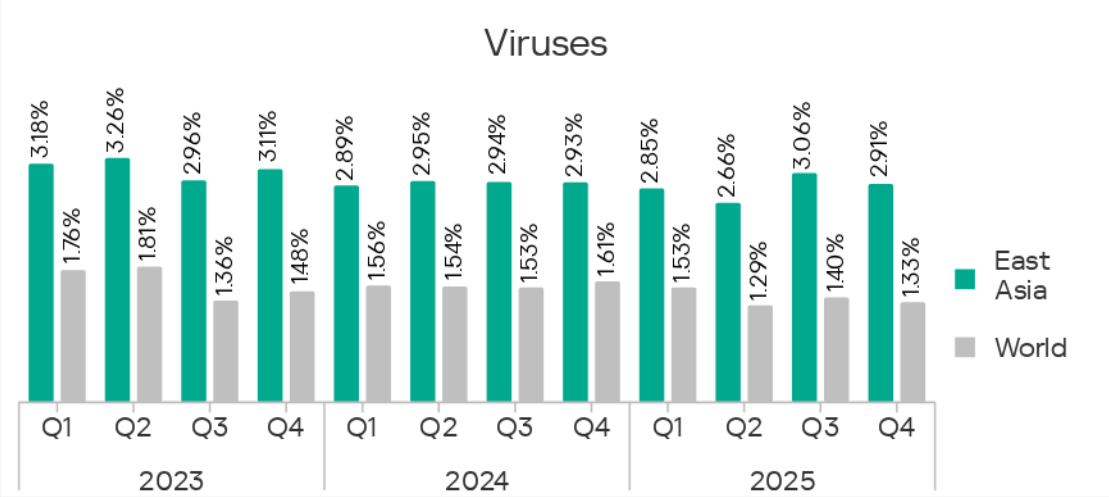
Viruses, and malware for AutoCAD

East Asia ranked third among regions in the percentage of ICS computers on which viruses were blocked and second in malware for AutoCAD, behind only Southeast Asia.

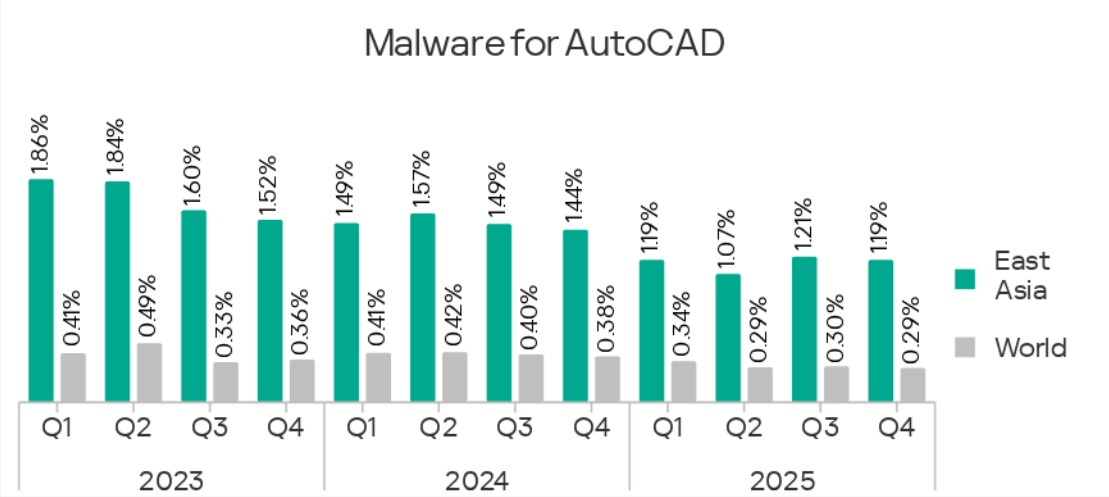
In both East and Southeast Asia, the situation with malware for AutoCAD was similar: in most cases, it spread the same way as viruses. This explains the high percentage for this malware category.

Both categories decreased over the quarter.

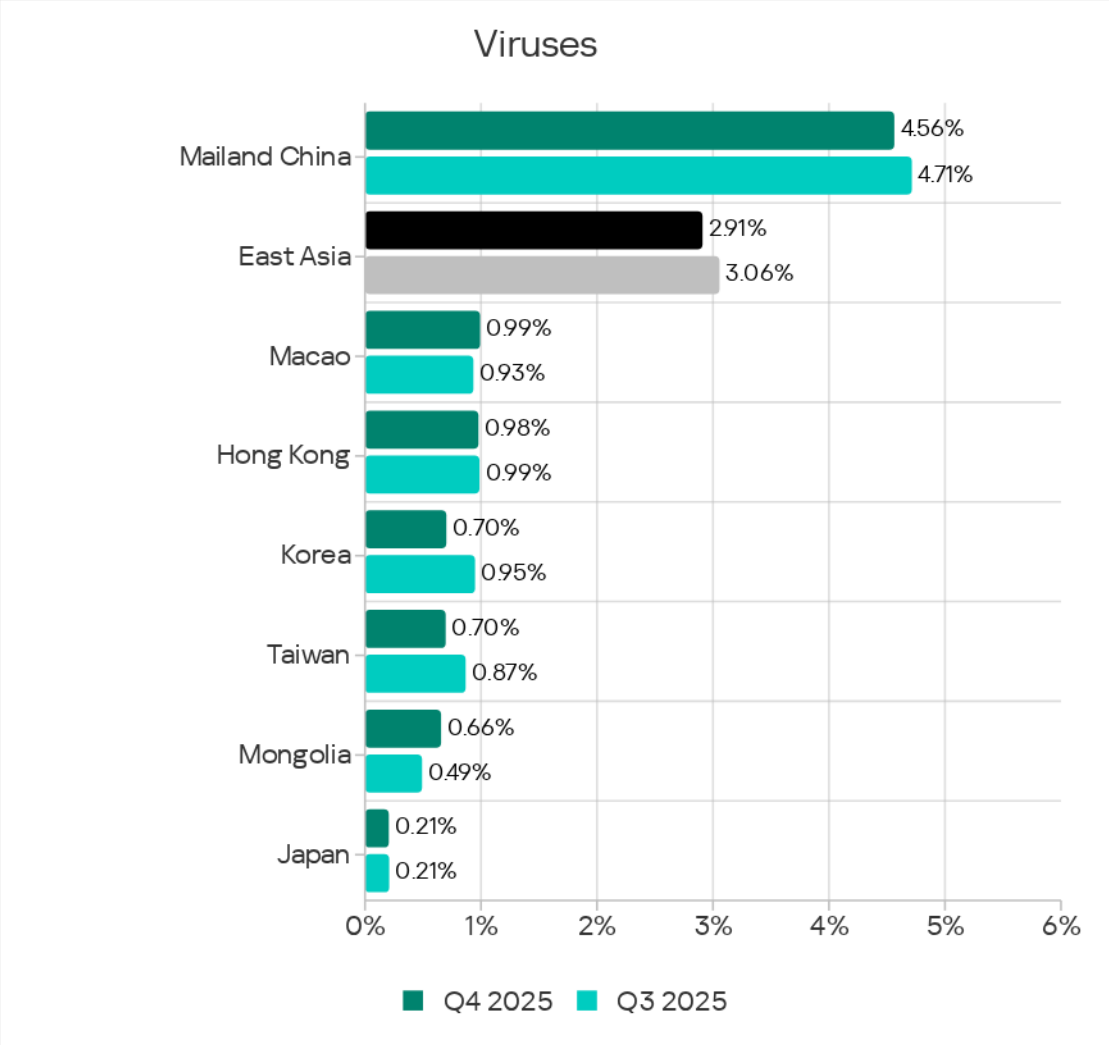
The percentage of ICS computers on which viruses were blocked in East Asia was 2.91%. This was 19.4 times higher than in Western Europe, which had the lowest figure.

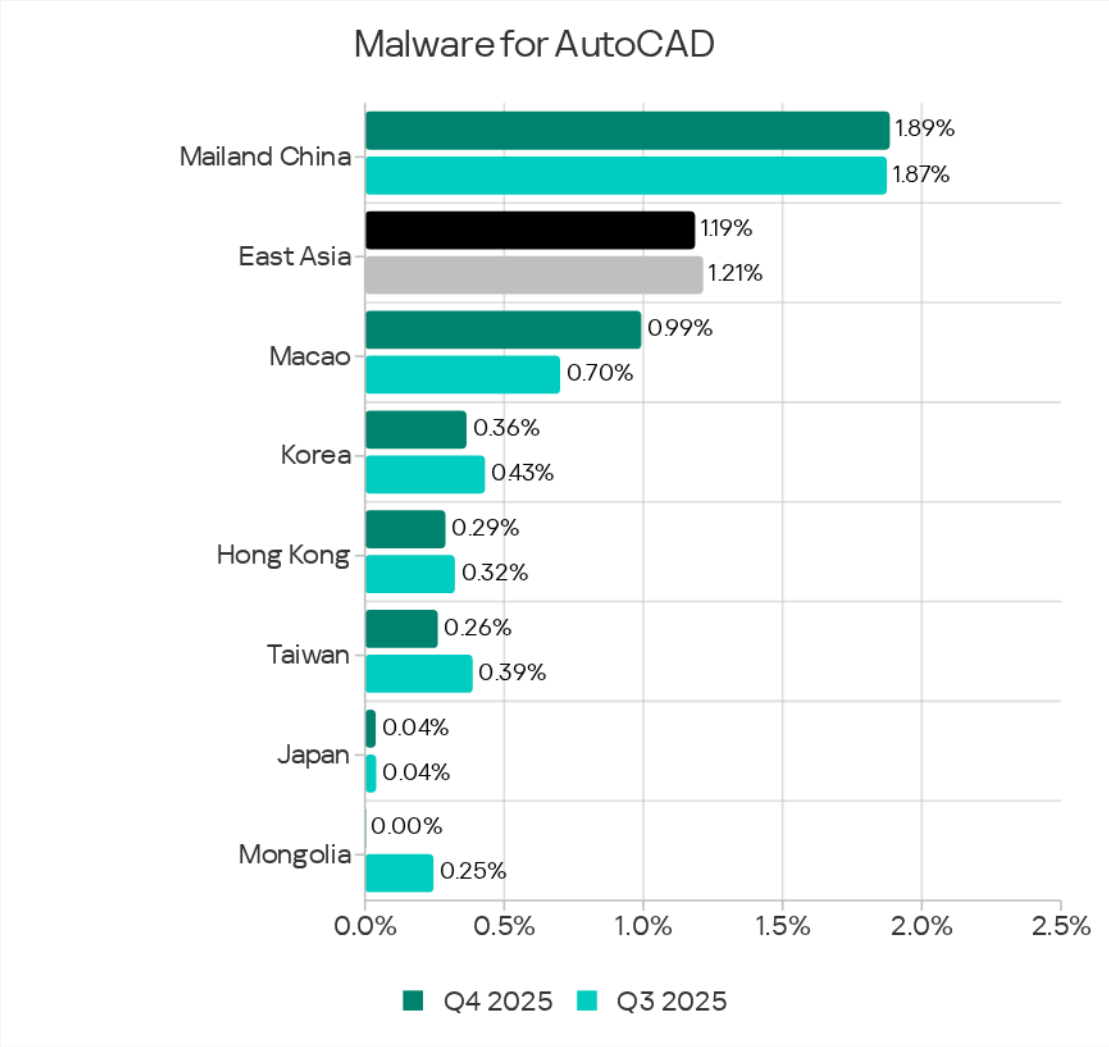


At 1.19%, the malware for AutoCAD figure for East Asia was 119 times (!) higher than that for Northern Europe, which ranked lowest among regions.



The region's leadership in the percentage of ICS computers on which malware from both categories was blocked was driven by Mainland China, which led by a wide margin in both viruses and malware for AutoCAD.





Viruses in the region spread via all threat sources. The internet was the leading source of viruses, while the network folders figure for this threat was only 1.1 times lower than the mail client threats and removable media threats metrics.

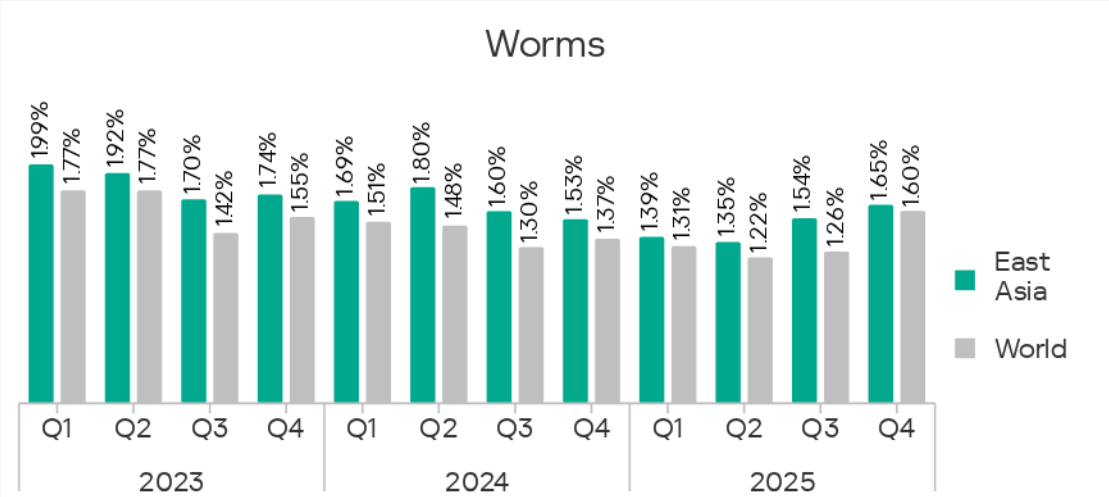
The main source of malware for AutoCAD was network folders, with Mainland China leading the figures in this source.

Worms

By the percentage of ICS computers with blocked worms, East Asia ranked seventh among regions.

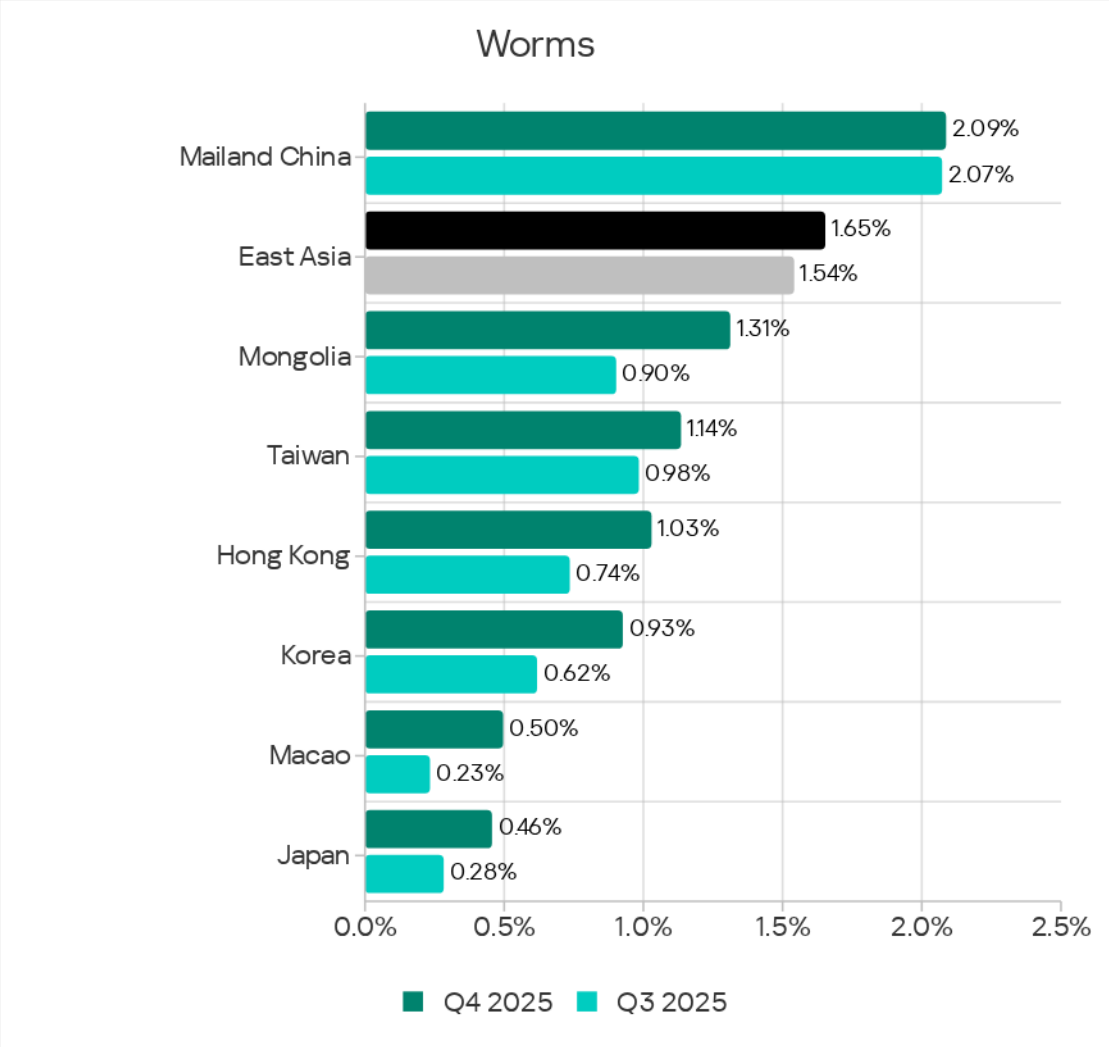
In Q4 2025, the worms metric grew across all regions due to the latest wave of phishing campaigns known as Curriculum-vitae-catalina which we described earlier. Notably, East Asia was one of the top five regions where this metric saw the least changes.

In East Asia, the percentage of ICS computers on which worms were blocked increased to 1.65%. This figure was 5.2 times higher than in Northern Europe, which had the lowest percentage among all regions.



Among the region's countries and territories, Mainland China led in the percentage of ICS computers with blocked worms, at 2.09%. Japan has the lowest rate at 0.46%.

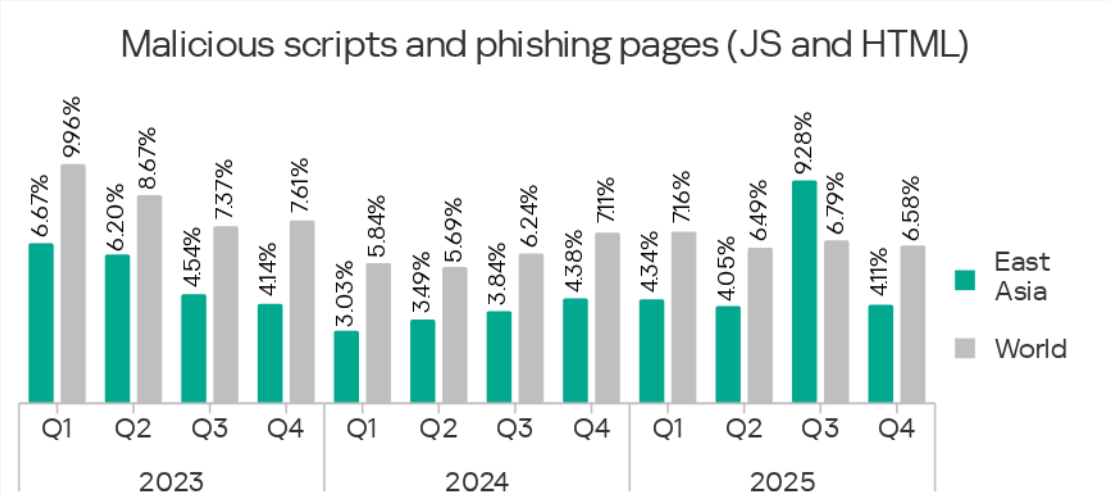
These values grew across all countries and territories.



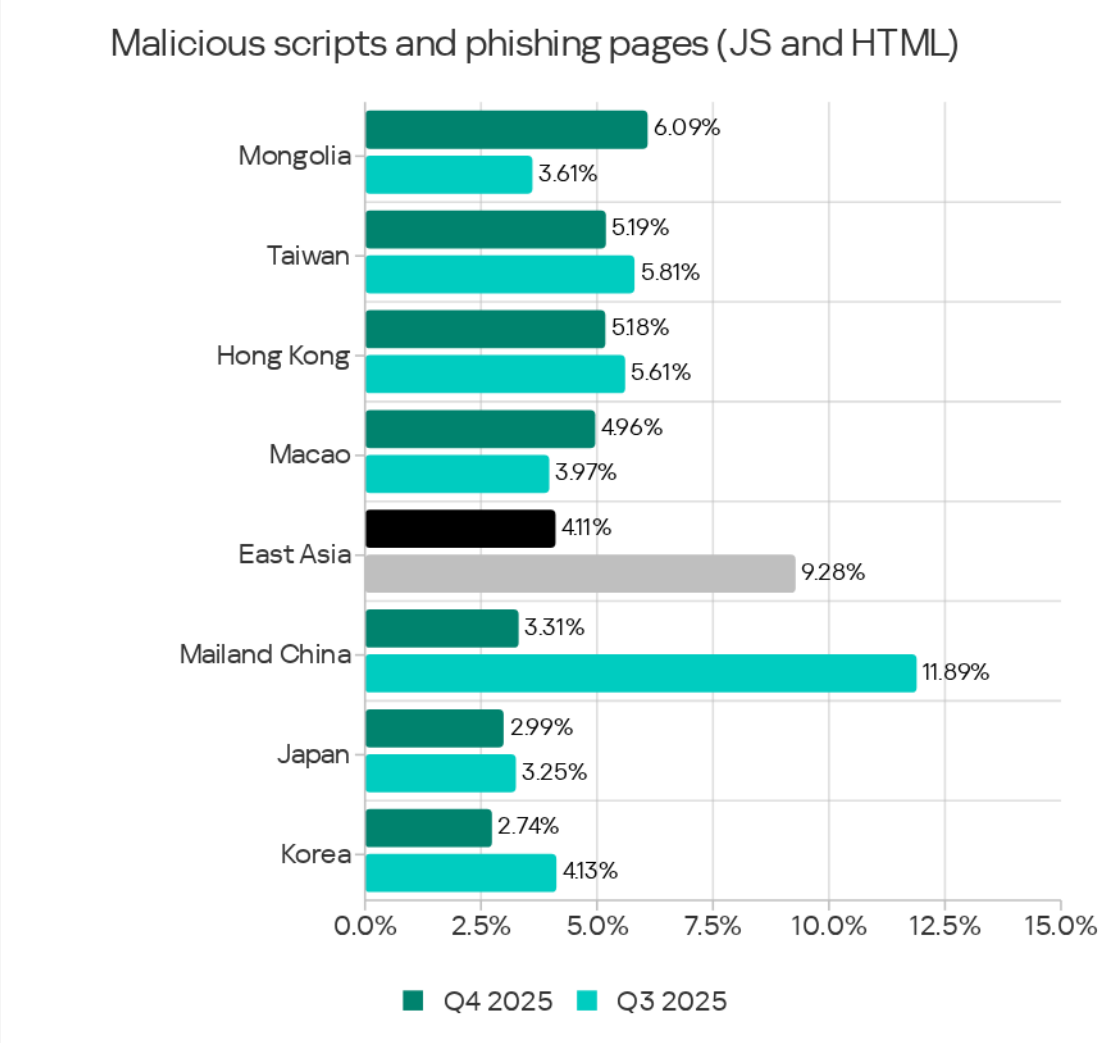
Worms spread through all threat sources, but mainly via removable media. Mainland China, the regional leader in worms, also ranked first in the percentage of ICS computers on which threats were blocked when connecting removable media.

Malicious scripts and phishing pages

Based on the percentage of ICS computers on which malicious scripts and phishing pages were blocked, East Asia ranked 12th among all regions. After growing by 5.23% in the previous quarter, this metric for the region decreased by 5.17% to 4.11%. This was 1.6 times higher than in Northern Europe, which had the lowest percentage value.

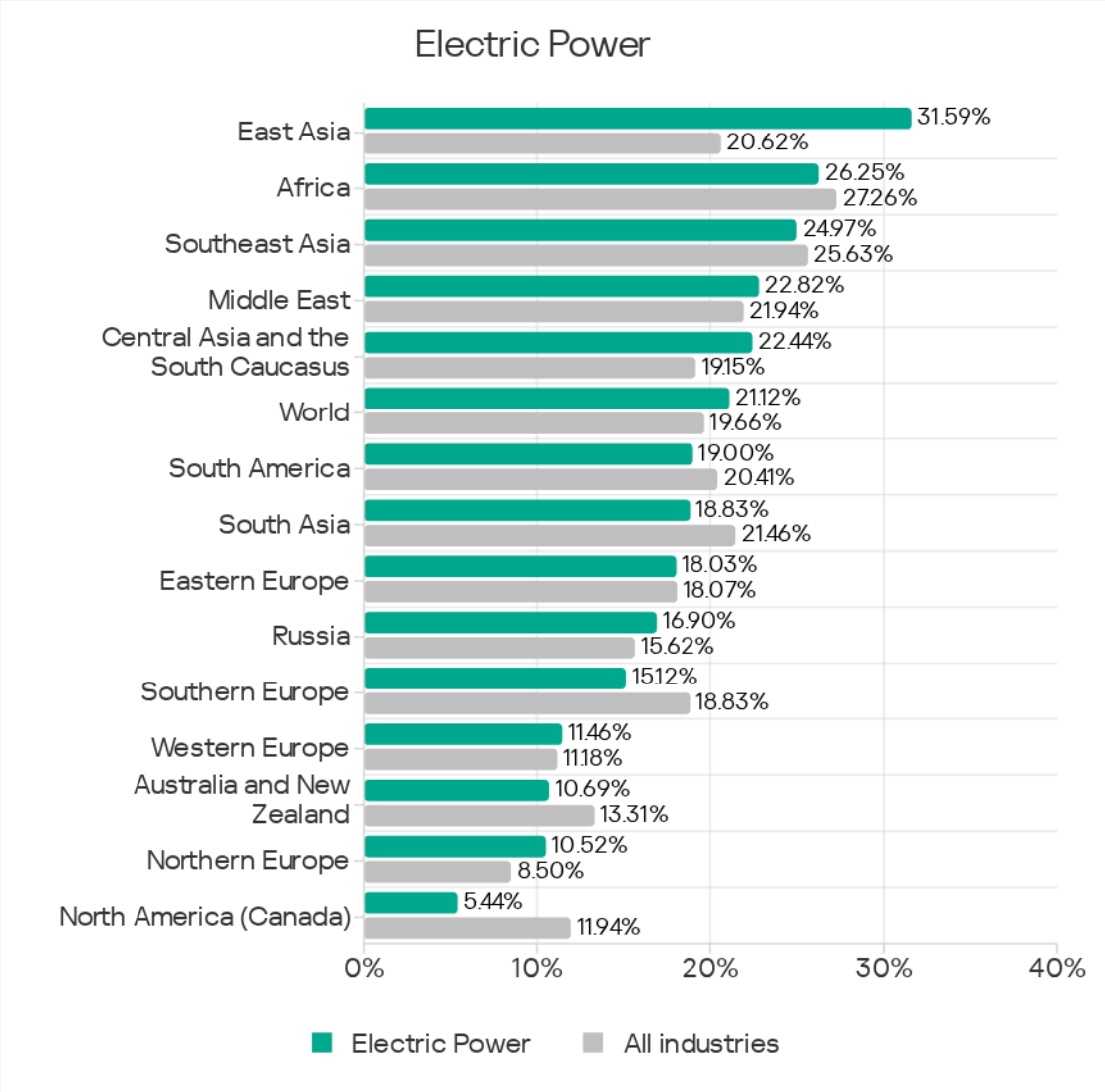


Among the region's countries and territories, Mongolia led in this metric with 6.09%. In Mainland China, this metric returned to normal, falling from first to fifth place for this ranking.



Industries

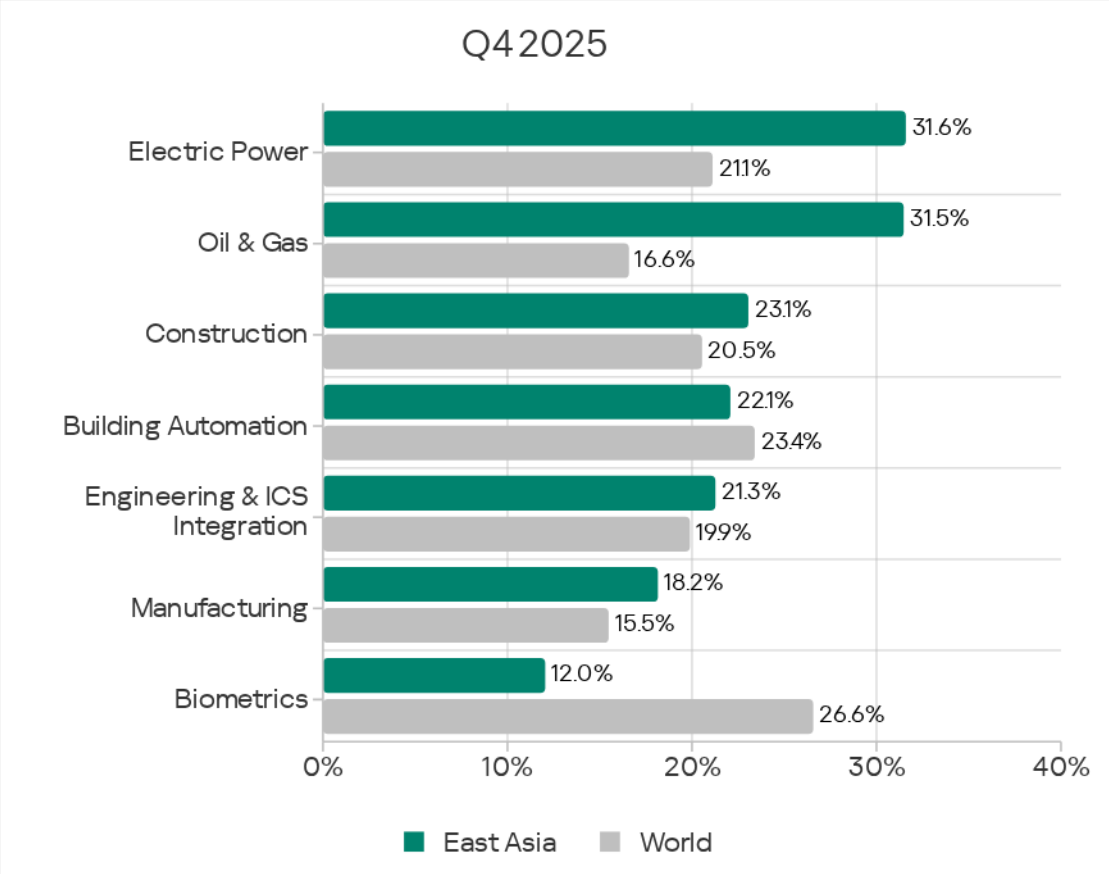
In Q4 2025, East Asia led all the regions in terms of the electric power industry metric, with 31.59%. This figure was 5.8 times higher than that in North America (Canada), which ranked last.



For engineering and ICS integration, East Asia ranked third among regions.

East Asia was the only region where electric power ranked first among industries by the percentage of ICS computers on which malicious objects were blocked.

Another distinctive feature of the region is the position of biometrics in the industry rankings. It ranked near the top in most regions, and ranked last only in East Asia and Southeast Asia.

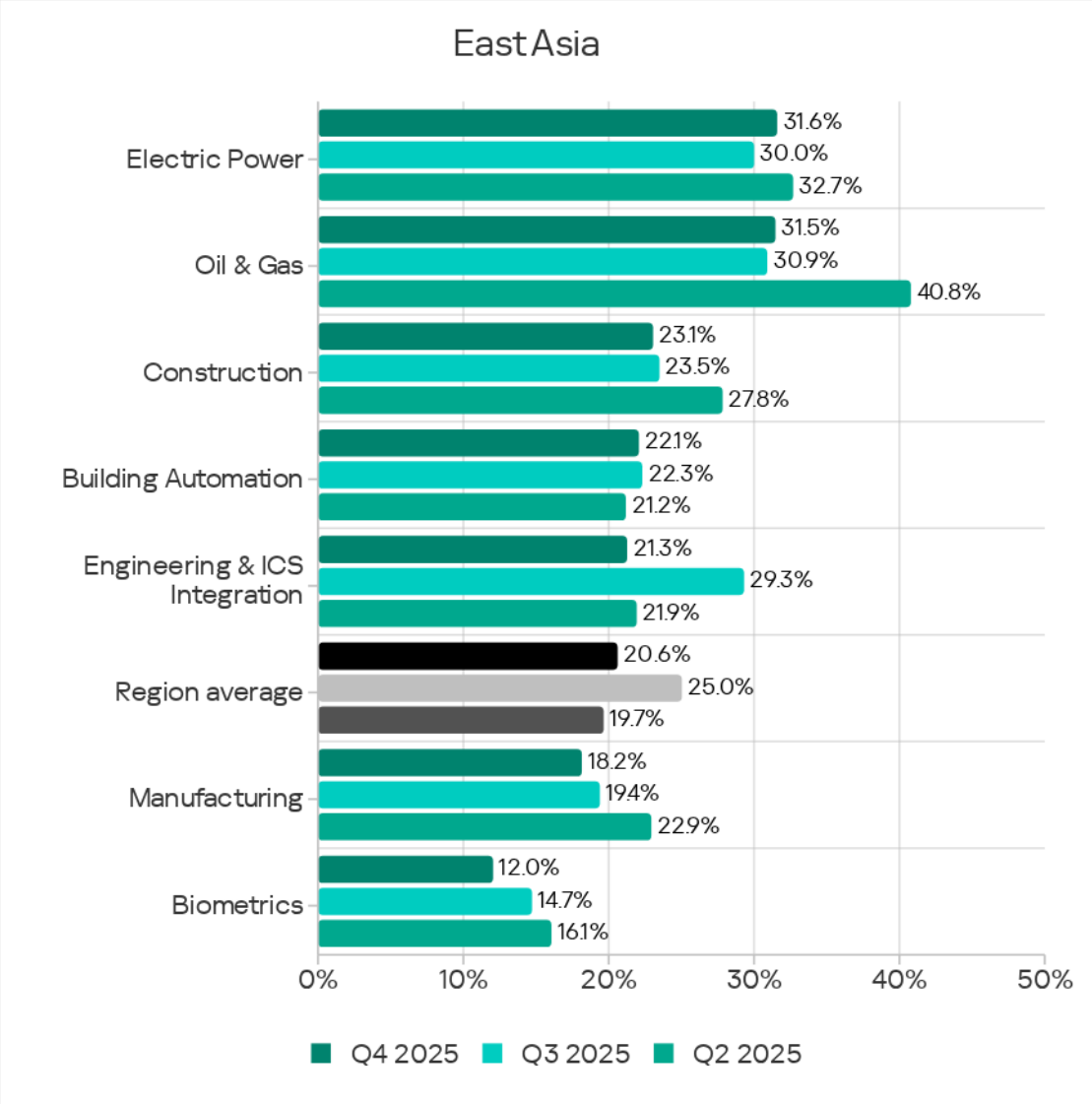


Compared to global averages, East Asia recorded a higher percentage of ICS computers on which malicious objects were blocked in the following industries:

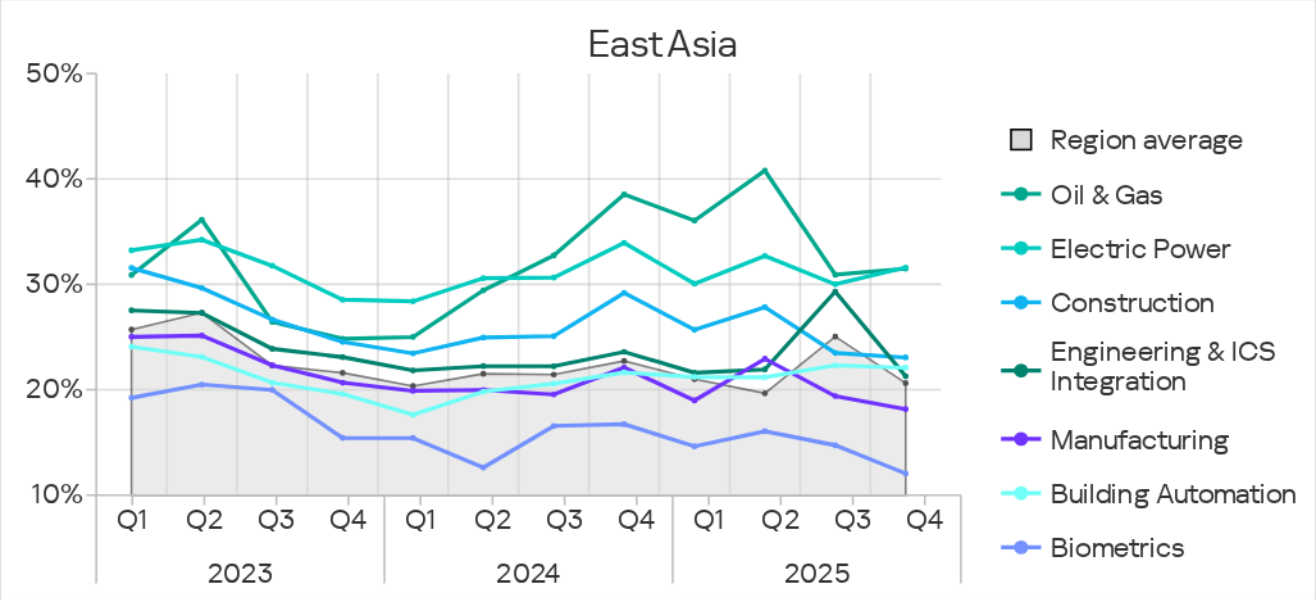
- Electric power: 1.5 times higher;
- Construction: 1.1 times higher;
- Engineering and ICS integrators: 1.1 times higher;
- Manufacturing: 1.2 times higher.

In Q4 2025, the percentage of ICS computers on which malicious objects were blocked increased only in the electric power industry.

After rising sharply during the previous quarter, the engineering and ICS integrators industry metric returned to the level typical of this industry.



Throughout the entire period under review, electrical energy has consistently been the industry with the highest percentage in this metric. Its value in the sector significantly exceeds not only the regional average but also the global average. This industry is rapidly developing in the region, but when new facilities are commissioned, adequate cybersecurity measures are typically implemented with a noticeable delay.



Threat sources and malware categories in industries: 'hotspots'

We use heat maps when assessing threats to industries in the regions. The color on the heatmap indicates the position in the global industry rankings across regions for each individual threat category or source. Red signifies that the figure is close to the maximum.

Threat source indicators for industries in East Asia, Q4 2025

Industry / Threat source	Biometrics	Building Automation	Engineering & ICS Integration	Electric Power	Oil & Gas	Construction	Manufacturing	Category metric in region
Internet	4.55%	6.15%	5.76%	9.18%	11.55%	8.47%	5.74%	5.71%
Email clients	4.77%	2.90%	1.35%	0.82%	—	1.89%	1.01%	1.40%
Removable media	0.23%	0.83%	0.64%	1.86%	1.20%	0.46%	1.10%	0.66%
Network folders	—	0.20%	0.22%	0.28%	—	0.29%	0.46%	0.18%
Industry metric in region	12.05%	22.08%	21.27%	31.59%	31.47%	23.05%	18.15%	

Threat category indicators for industries in East Asia, Q4 2025

Industry / Threat type	Biometrics	Building Automation	Engineering & ICS Integration	Electric Power	Oil & Gas	Construction	Manufacturing	Category metric in region
Denylisted internet resources	1.36%	2.33%	2.25%	4.41%	5.98%	2.80%	2.11%	2.19%
Malicious scripts and phishing pages (JS and HTML)	7.50%	5.51%	3.97%	5.40%	8.76%	6.29%	4.09%	4.11%
Malicious documents (MSOffice + PDF)	3.18%	2.46%	1.42%	2.63%	2.39%	2.46%	1.84%	1.42%
Spy Trojans, backdoors and keyloggers	3.64%	6.19%	4.53%	9.52%	7.57%	4.86%	4.27%	4.56%
Ransomware	0.23%	0.31%	0.14%	0.31%	0.40%	0.29%	0.14%	0.15%
Miners in the form of executable files for Windows	—	0.21%	0.17%	0.17%	—	0.23%	0.09%	0.15%
Web miners running in browsers	—	0.10%	0.06%	0.06%	—	0.11%	0.09%	0.06%
Malware for AutoCAD	0.23%	1.07%	1.41%	2.57%	4.38%	5.89%	1.47%	1.19%
Worms	1.82%	2.90%	1.49%	3.48%	3.19%	2.12%	2.62%	1.65%
Viruses	1.14%	2.58%	3.49%	5.88%	5.58%	5.72%	3.35%	2.91%
Industry metric in region	12.05%	22.08%	21.27%	31.59%	31.47%	23.05%	18.15%	

Characteristics of the region

A high percentage of ICS computers on which spyware was blocked. In terms of this threat, East Asia ranked no lower than third for this metric across all industries except for building automation and biometrics.

High level of removable media threats. Based on the percentage of ICS computers on which removable drive threats were blocked on connection, East Asia ranked no lower than third across all industries except for biometrics.

High level of network folder threats. Based on the percentage of ICS computers on which network folder threats were blocked, East Asia led across all industries except for biometrics.

A high percentage of ICS computers on which malware for AutoCAD was blocked. For this metric, East Asia led all the regions across all industries except biometrics, where this region ranks second. This threat is propagated predominately inside network folders.

Electric power

East Asia was the global leader in the percentage of ICS computers on which malicious objects were blocked in the electrical energy industry.

Among all regions, in the electrical energy sector East Asia ranked:

- First in the percentage of ICS computers on which threats were blocked on removable media and in network folders;
- First in the percentage of ICS computers on which malicious documents, spyware, and malware for AutoCAD were blocked;
- Second in viruses and worms.

In the regional cross-industry rankings, the electrical energy industry ranked:

- First in the percentage of ICS computers on which internet threats from the internet and on removable media were blocked, and third in network folders;
- First for denylisted internet resources, spyware, worms, viruses, and ransomware.
- Second in the following threat categories: malicious documents and malware for AutoCAD.
- Third place in miners in the form of executable files, as well as viruses.

Engineering and ICS integrators

East Asia ranked third among regions based on the percentage of ICS computers on which malicious objects in the engineering and ICS integrators industry were blocked.

Among all regions, in the engineering and ICS integrators sector East Asia ranked:

- First in the percentage of ICS computers on which network folder threats were blocked, second in removable media threats;
- First in terms of the percentage of ICS computers on which malware for AutoCAD was blocked.
- Second in viruses.

- Third for spyware.

In the regional cross-industry rankings, engineering and ICS integrators had the following positions:

- Third in viruses.

Construction

East Asia ranked fourth among regions in the percentage of ICS computers on which malicious objects were blocked in construction.

Among all regions, in the construction sector East Asia ranked:

- First in the percentage of ICS computers on which network folder threats were blocked and third in removable media threats;
- First in the percentage of ICS computers on which malicious documents and malware for AutoCAD were blocked;
- Second in spyware;
- Third in worms, viruses, and ransomware.

In the regional cross-industry rankings, the construction sector ranked:

- Second in threats from the internet and network folders; third for email client threats;
- First in malicious documents, both types of miners and malware for AutoCAD.
- Second in the following threat categories: denylisted internet resources, malicious scripts and phishing pages, and viruses.
- Third for the following threat categories: malicious documents, spyware, and ransomware.

Building automation

East Asia ranked ninth globally in the percentage of ICS computers on which malicious objects were blocked in building automation.

Among all regions, in the building automation sector East Asia ranked:

- First in the percentage of ICS computers on which network folder threats were blocked and second in removable media threats;
- First in terms of the percentage of ICS computers on which malware for AutoCAD was blocked.
- Third in viruses.

In the regional cross-industry rankings, building automation occupied the following positions:

- Second in threats from email, third in internet threats and threats from removable media;
- Second place in the following threat categories: spyware, ransomware, worms, and both categories of miners.
- Third in malicious documents and scripts and phishing pages.

Manufacturing

East Asia ranked fourth among regions in the percentage of ICS computers with blocked malicious objects in manufacturing.

Among all regions, in the manufacturing sector East Asia ranked:

- First in the percentage of ICS computers on which network folder threats and removable media threats were blocked;
- First in terms of the percentage of ICS computers on which malware for AutoCAD was blocked.
- Second in spyware, worms, and viruses;

In the regional cross-industry rankings, the manufacturing sector ranked:

- First in the percentage of ICS computers on which network folder threats were blocked and second in terms of removable media threats;
- Third place in the following threat categories: worms, web miners, and malware for AutoCAD.

Biometrics

East Asia ranked 11th among regions in the percentage of ICS computers with blocked malicious objects in biometrics.

Based on industry indicators among regions, East Asia ranked second in the percentage of ICS computers on which worms, viruses, and malware for AutoCAD were blocked.

The regional industry rankings for biometrics was as follows:

- First in threats from network folders.
- First place in the following threat categories: malicious scripts and phishing pages, and malicious documents.

Central Asia and the South Caucasus

Key cybersecurity issues in the region

Lack of control over the use of removable media

In Central Asia and the South Caucasus, the percentage of ICS computers on which threats are blocked when connecting removable media has historically been high. In Q4 2025, this indicator in the region was 1.4 times higher than the global average.

The main categories of removable media threats blocked on ICS computers are worms, viruses, spyware, and miners in the form of executable files for Windows.

Based on the percentage of ICS computers on which miners in the form of executable files for Windows were blocked, the Central Asia and South Caucasus region led all the regions. The region ranked third for worms. These categories were 2.0 and 1.5 times higher than the global average, respectively.

Frequent attempts to infect protected systems via USB drives may indicate:

- A low level of enterprise digitalization (lack of secure internal file storage and transfer systems)
- The presence of an unprotected part of the enterprise infrastructure acting as a source of self-propagating malware
- A poor overall information security culture

Lack of control over software installation by users on ICS computers

By the percentage of miners in the form of executable files for Windows, Central Asia and the South Caucasus region ranked first globally. The main distribution channel for such malware is the internet.

In Q4 2025, this region's percentage of ICS computers with blocked miners in the form of executable files for Windows was the highest among all regions. Across all industries and regions, the construction industry in the Central Asia and South Caucasus region ranks first for the percentage of miners in the form of executable files that were blocked on ICS computers.

Across all industries covered by the report except for the engineering and ICS integrators industry, the Central Asia and South Caucasus region leads among regions by the percentage of miners in the form of executable files for Windows. Based on the engineering and ICS integrators metrics, the region ranked second.

A small study conducted in the region revealed that cryptocurrency mining software was often installed on ICS computers by their legitimate users. However, employees frequently download such software without realizing that it has been tampered with by attackers — resulting in mining profits going to someone completely different from the one who installed it.

Additionally, malicious mining executables have long used worm-like self-propagation techniques: stealing credentials, searching for and extracting insecurely stored secrets, and exploiting local and network vulnerabilities. Therefore, their potential threat to an OT network should not be underestimated.

Consistently high level of ransomware incidents

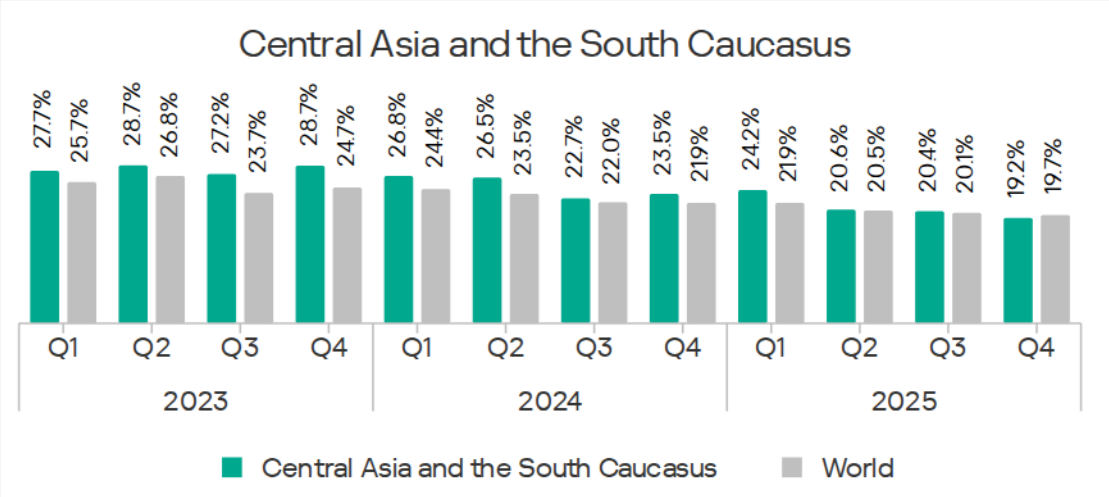
By the percentage of ICS computers on which ransomware was blocked, Central Asia and the South Caucasus rank fourth, with a rate 1.1 times higher than the global average. In Q4 2025, this category of threats spread in the region via the internet, email, and removable media.

Based on ransomware metrics, the Central Asia and South Caucasus region is at least third in the rankings of regions across all industries. Based on the metrics for biometrics, construction, electric power, and manufacturing industries, the Central Asia and South Caucasus region ranks first among regions.

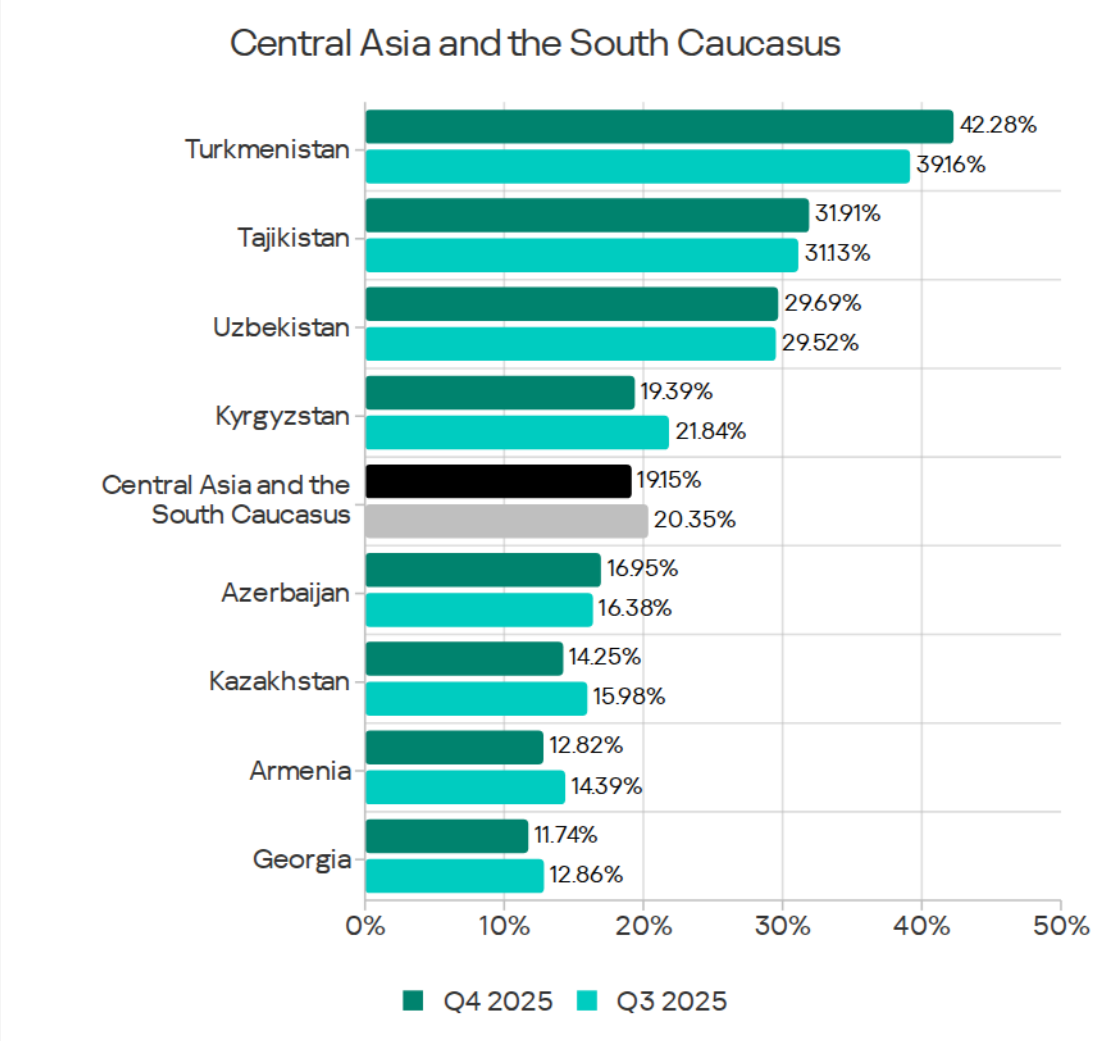
Statistics across all threats

In Q4 2025, Central Asia and the South Caucasus ranked seventh globally by the percentage of ICS computers on which malicious objects were blocked with 19.2%. This figure was 2.3 times higher than in Northern Europe, which had the lowest percentage among all regions.

However, this figure is gradually decreasing — in Q4 2025, it reached a three-year low.

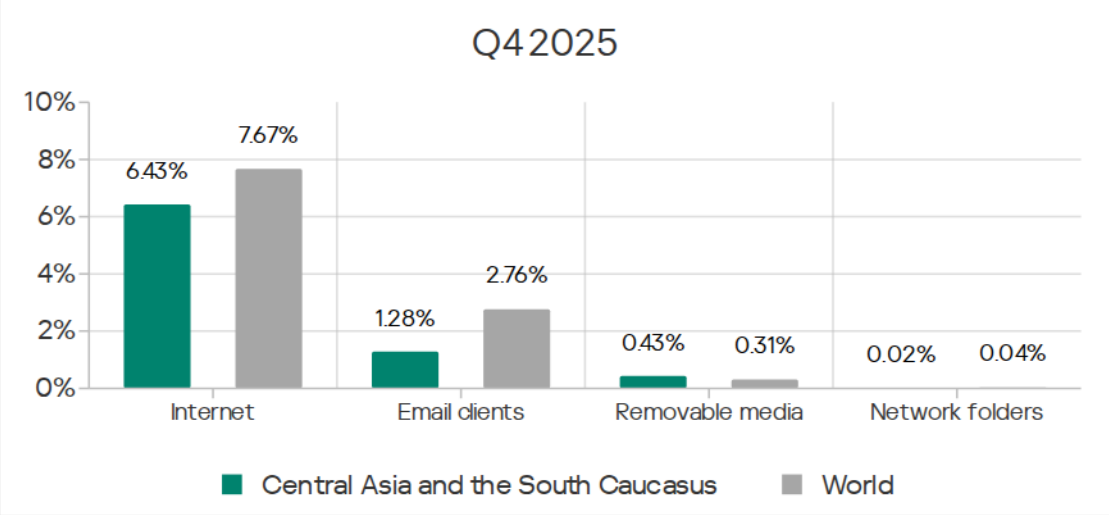


The percentage of ICS computers on which malicious objects were blocked varies among the region's countries, from 11.74% in Georgia to 42.28% in Turkmenistan.

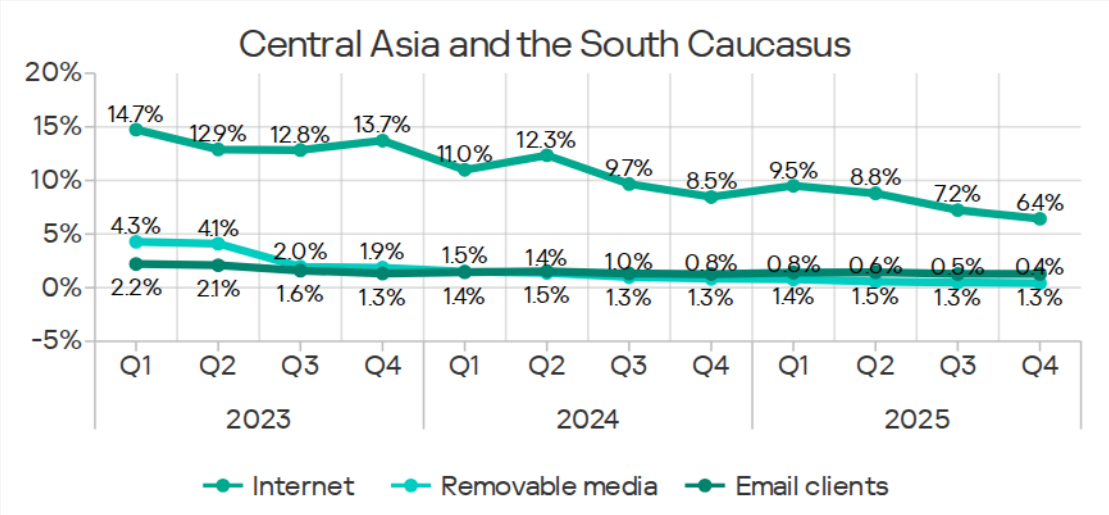


Threat sources

In Central Asia and the South Caucasus, only threats from removable media exceeded the global average on ICS computers, by 1.4 times.



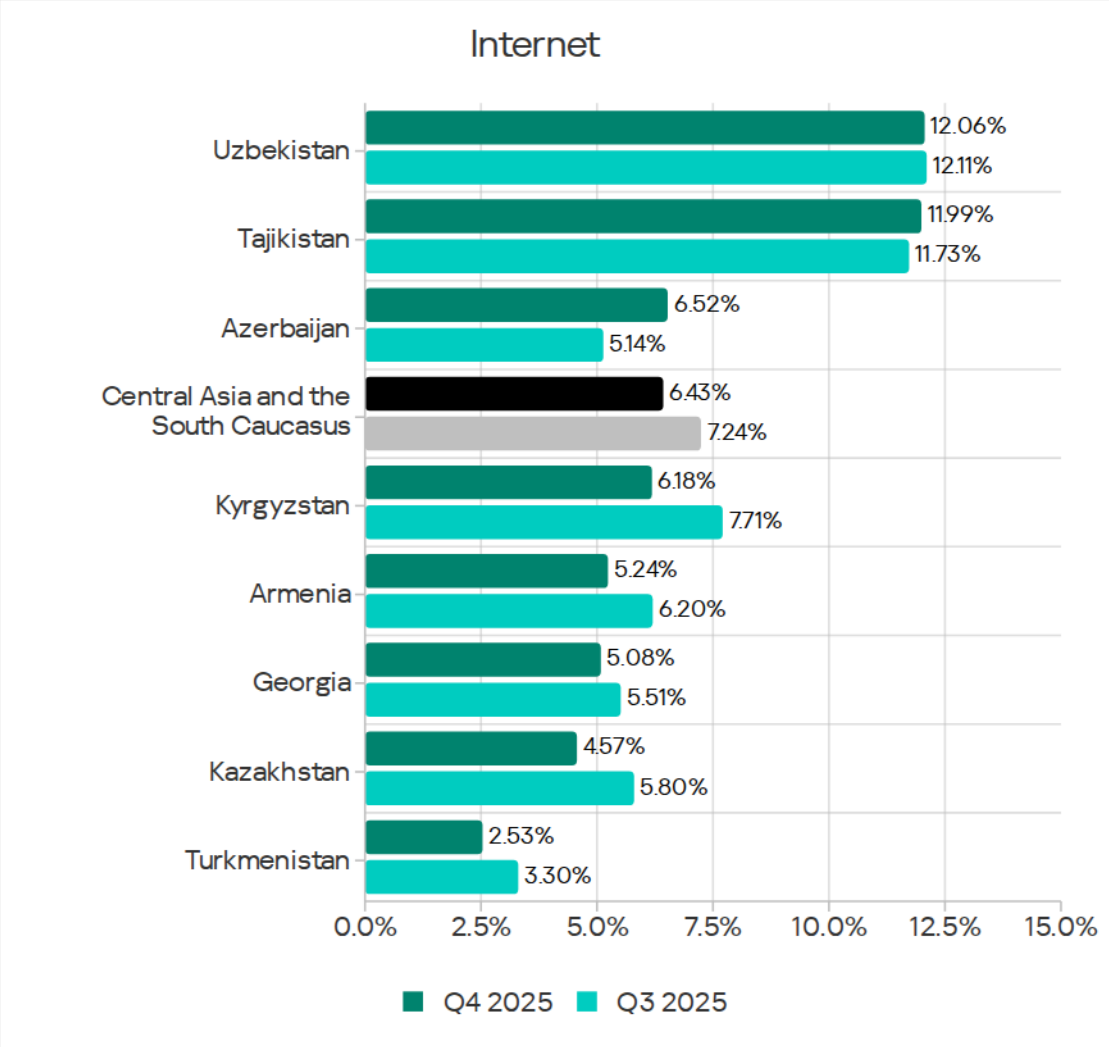
In Q4 2025, the percentage of ICS computers on which malicious objects were blocked fell across all threat sources except for mail clients.



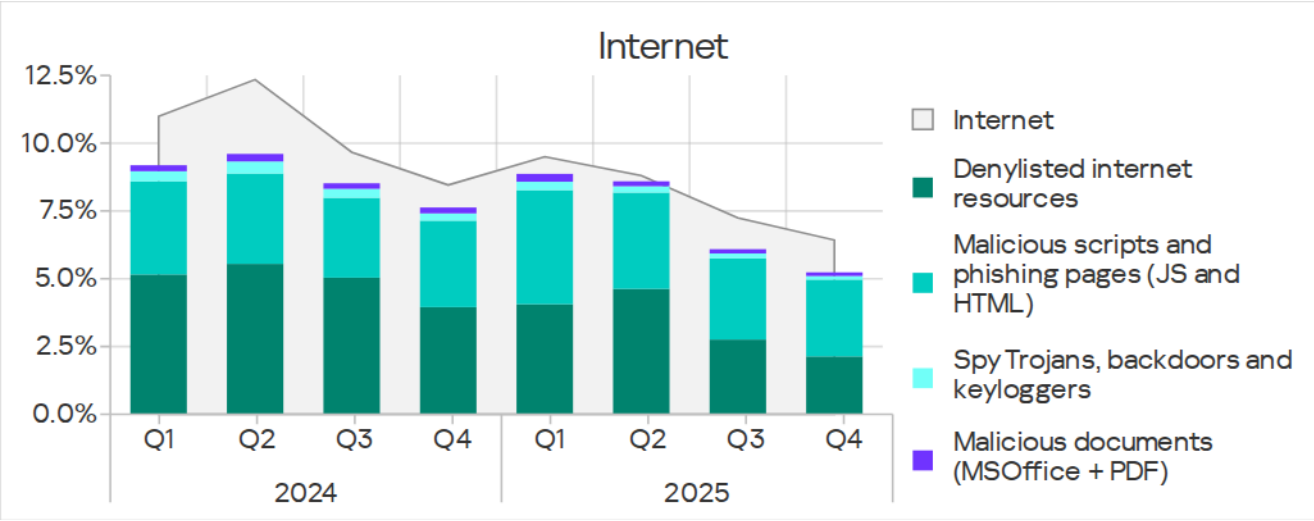
Internet

By the percentage of ICS computers on which internet threats were blocked, Central Asia and the South Caucasus rank 10th globally at 6.43%, which is 1.6 times higher than the lowest level (Northern Europe).

Based on the percentage of ICS computers on which internet threats were blocked, Uzbekistan and Tajikistan lead with 12.06% and 11.99%, respectively. The lowest figure is in Turkmenistan — 2.53%.



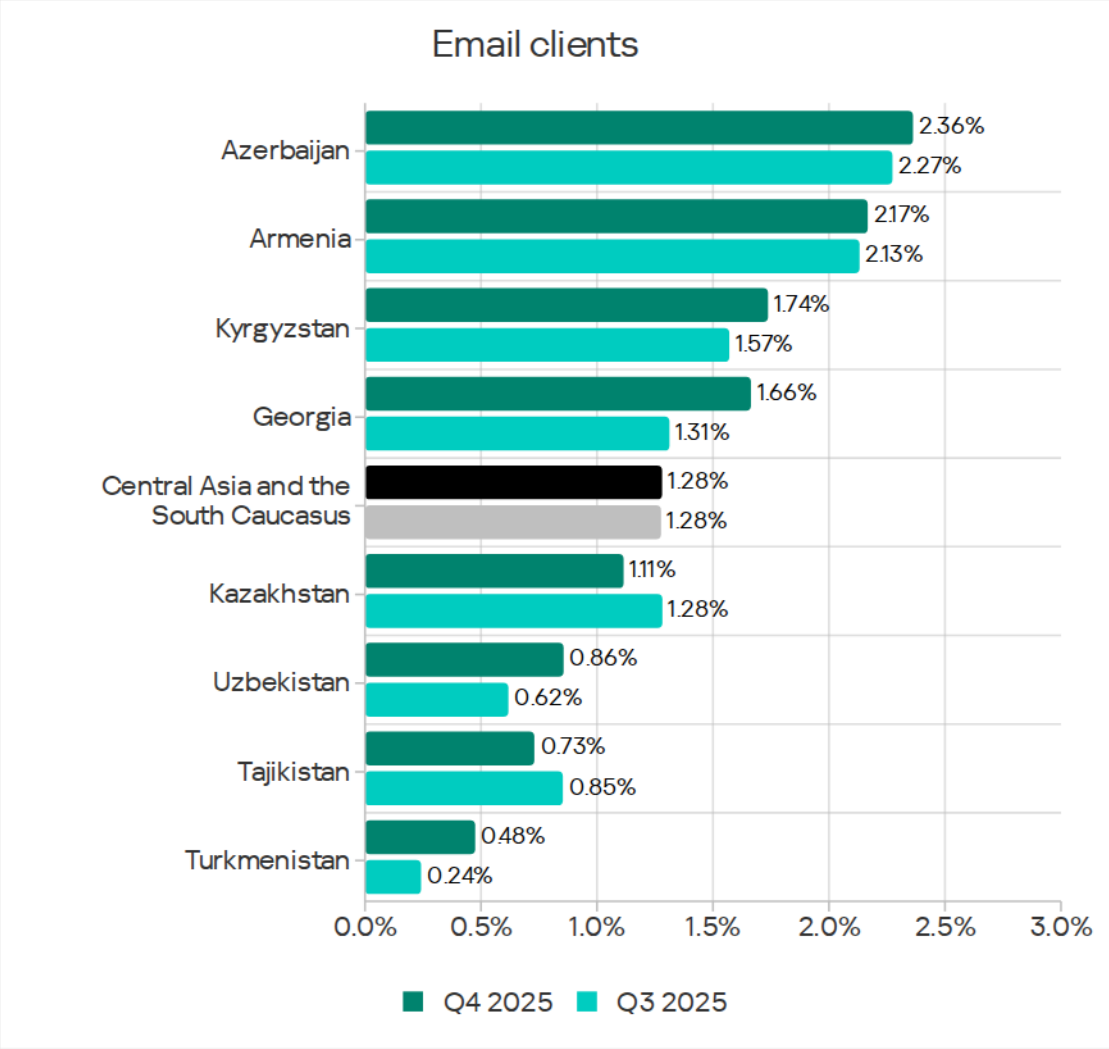
The main categories of internet threats blocked on ICS computers in the region were denylisted internet resources and malicious scripts and phishing pages.



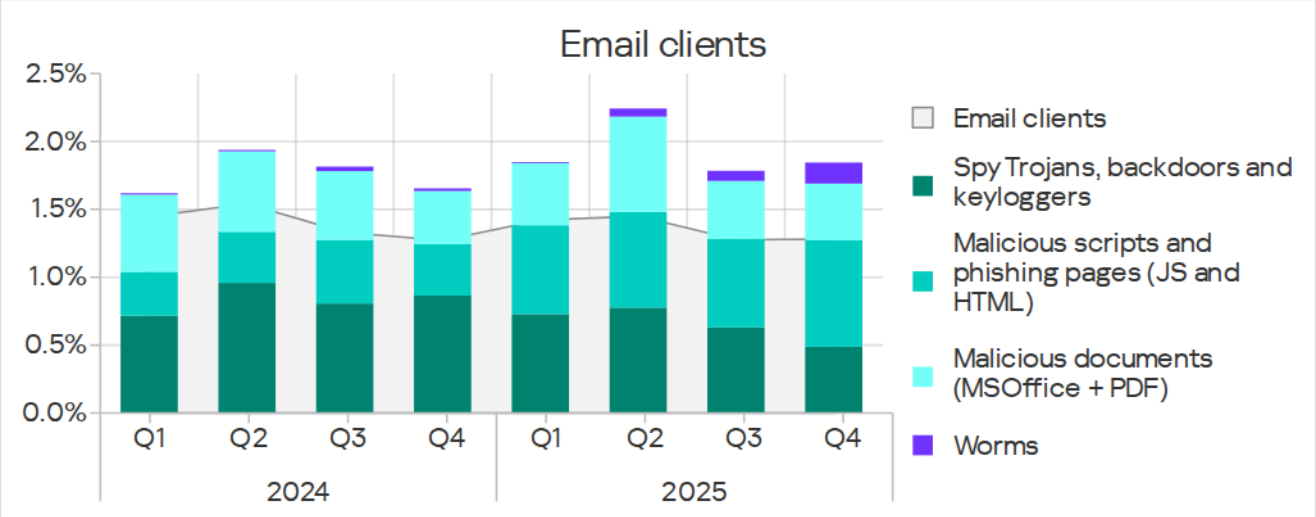
Email clients

In terms of the percentage of ICS computers on which threats from email clients were blocked, Central Asia and the South Caucasus occupied 12th place globally with 1.28%. This was 2.0 times higher than in Northern Europe, which was last in the ranking.

Among the countries of the region, Azerbaijan led with 2.36%, while Turkmenistan had the lowest at 0.48%. The rate increased across all countries in the region except for Kazakhstan and Tajikistan.



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



Q4 2025 saw a noticeable increase in the percentage of ICS computers on which worms from mail clients were blocked. This was caused by a wave of phishing campaigns known as Curriculum-vitae-catalina, which launched attacks against organizations across all regions of the world. In Central Asia and the South Caucasus, these attacks peaked in November.

The hackers distributed phishing emails disguised as job applications. Disguised as a resume (Curriculum Vitae), these emails contained a malicious executable file, a remote administration backdoor worm known as Backdoor.MSIL.XWorm. Running that file caused system infection.

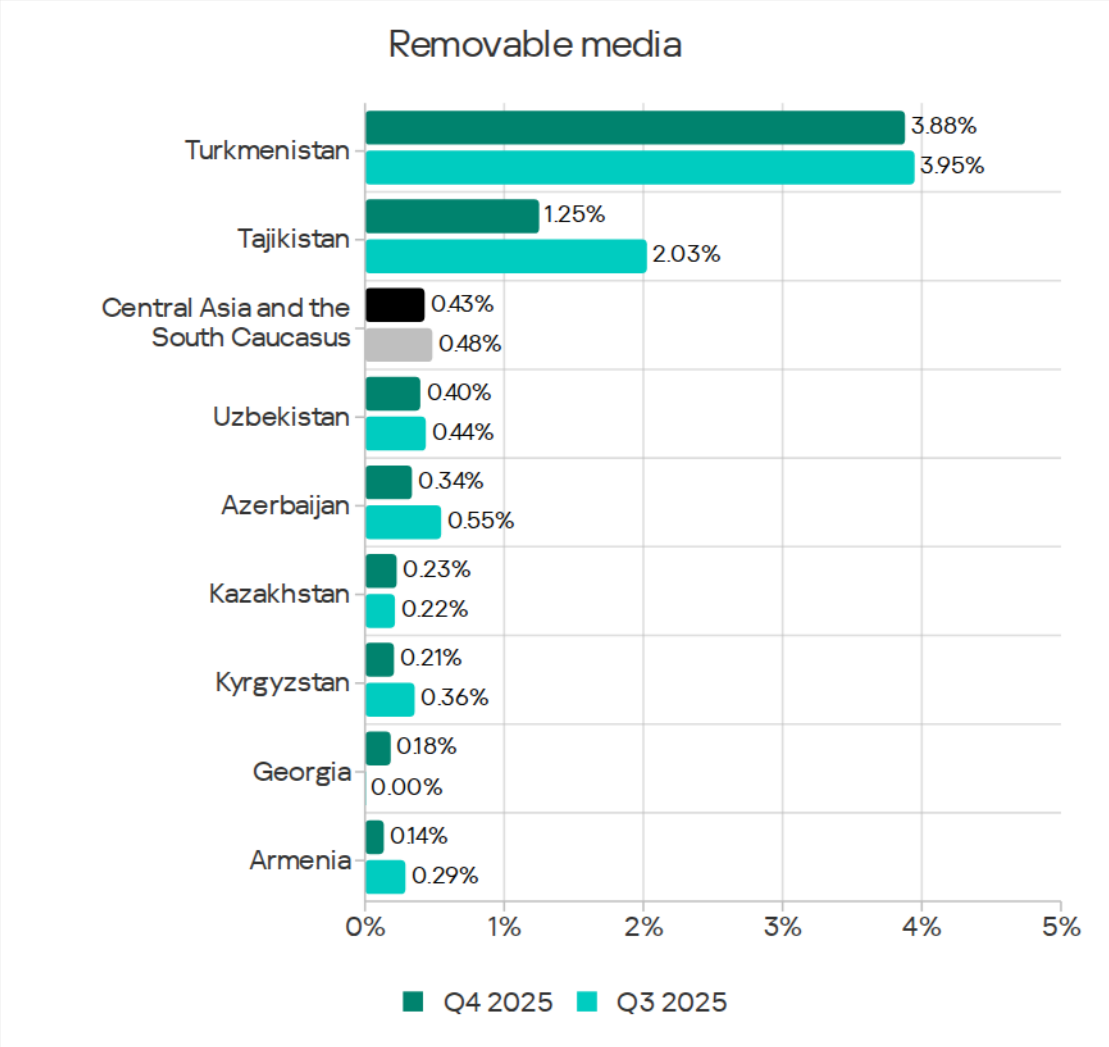
Normally, these campaigns are designed to deliver malware for data theft, spyware, or remote administration tools (RATs).

Removable media

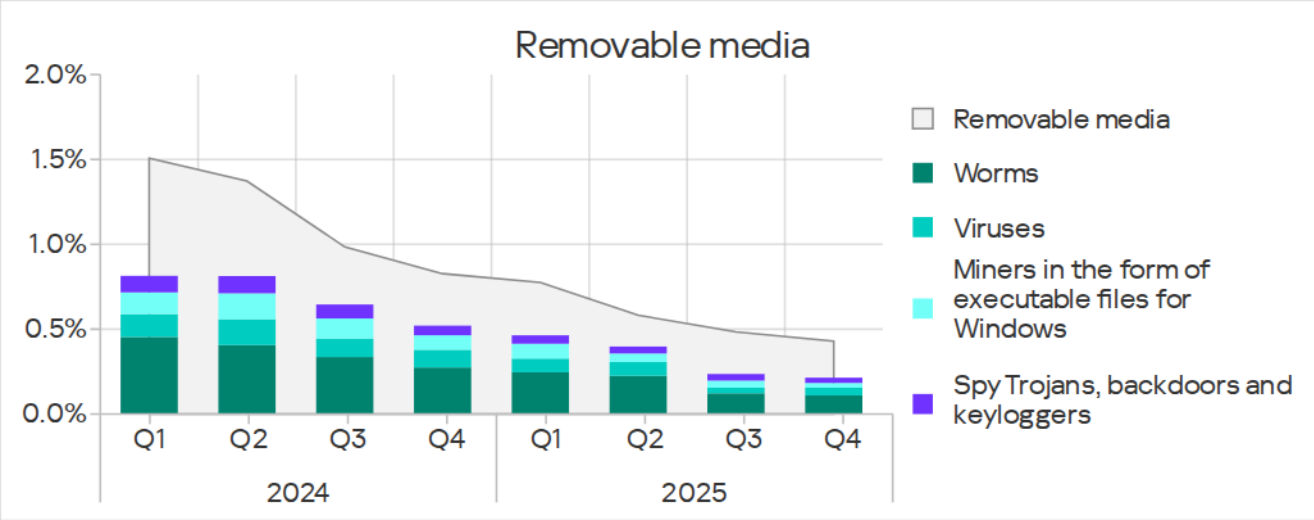
The top six regions by the percentage of ICS computers on which threats were blocked when connecting removable media: Africa, the Middle East, and the various regions of Asia. The figures for these regions exceeded those for all others at least by a factor of 2.2.

Central Asia and the South Caucasus ranked fifth with 0.43%. This figure was 8.6 times higher than in the Australia and New Zealand region, which ranked last.

Among the countries in the region, Turkmenistan led by a wide margin in the percentage of ICS computers on which threats were blocked upon connecting removable media, with 3.88%. Notably, this country ranked last for mail client threats and internet threats.

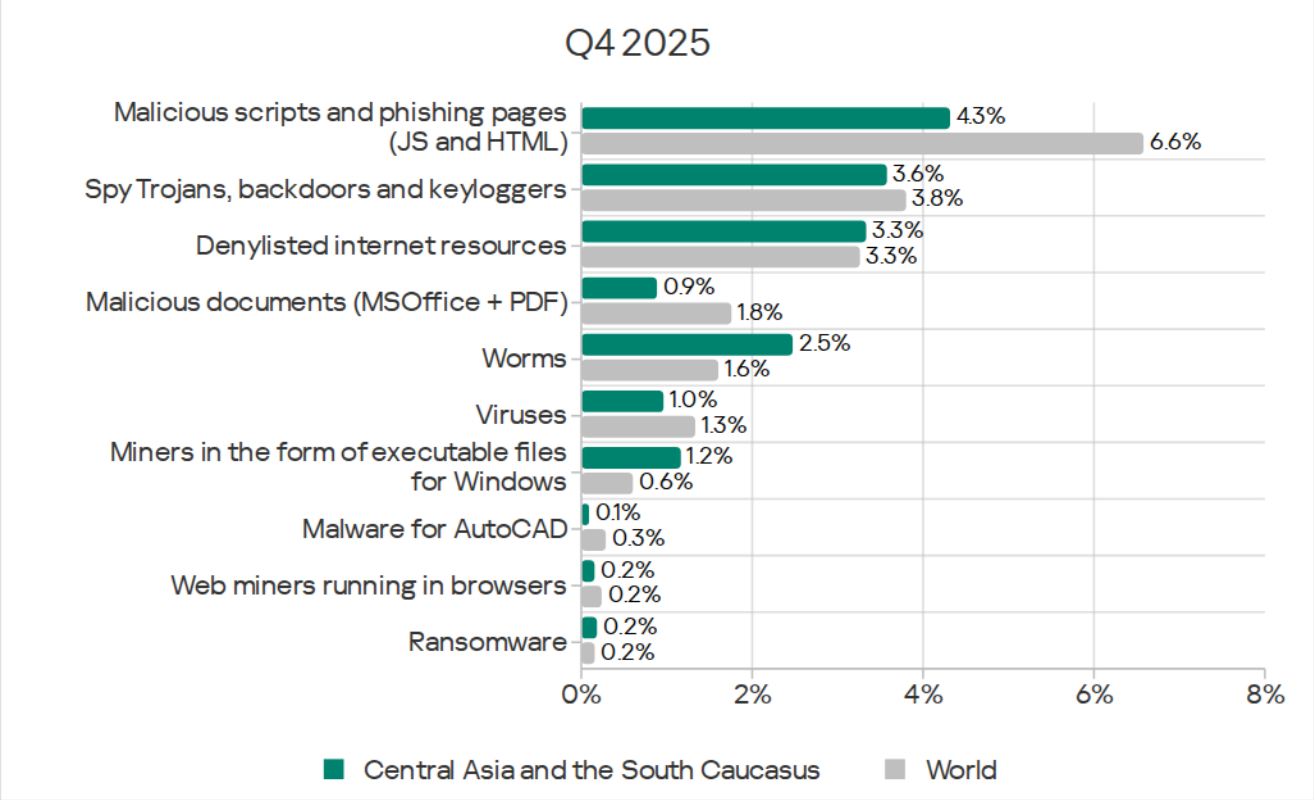


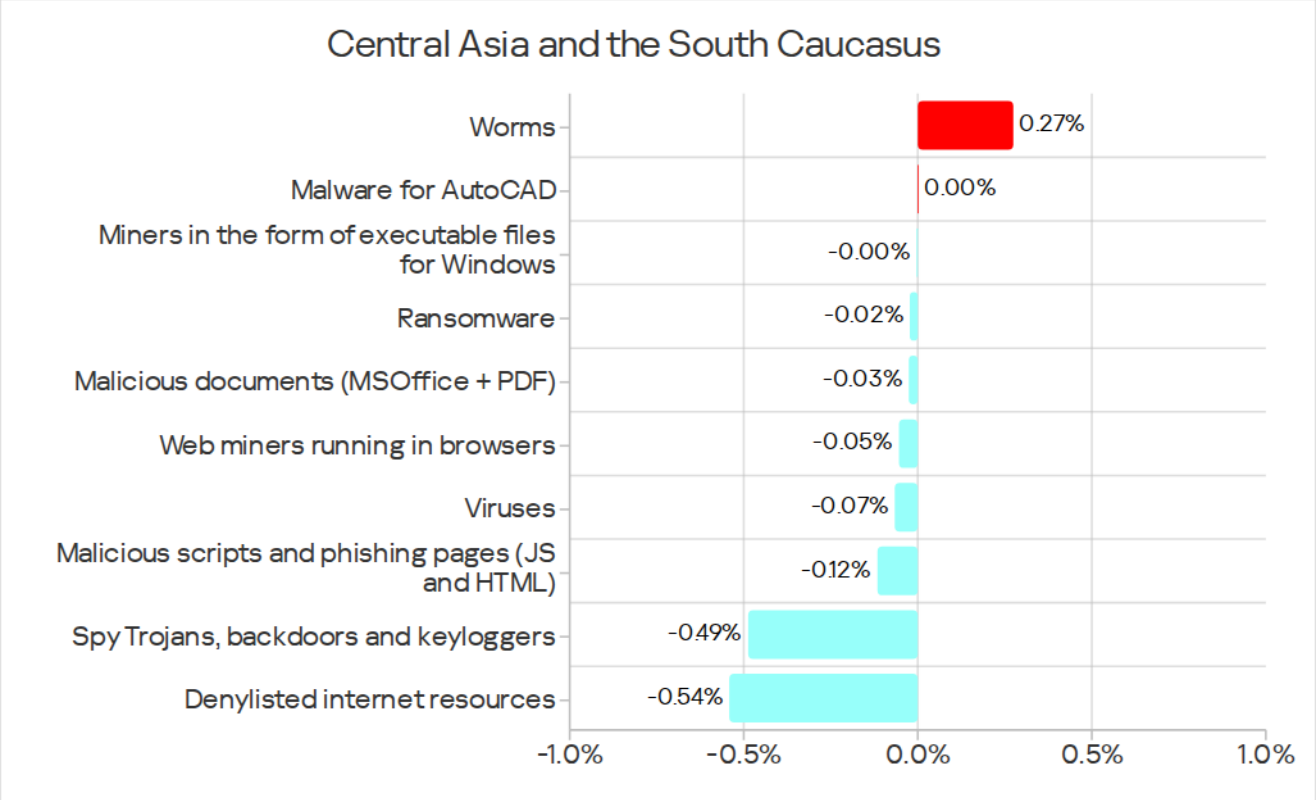
The main categories of removable media threats blocked on ICS computers were worms, spyware, viruses, and miners in the form of executable files for Windows.



Based on the percentage of ICS computers on which miners in the form of executable files were blocked, Central Asia and South Caucasus led all other regions. In terms of worms, the region was third.

Threat categories





Of all the threat categories we tracked in Q4, this metric increased only for worms.

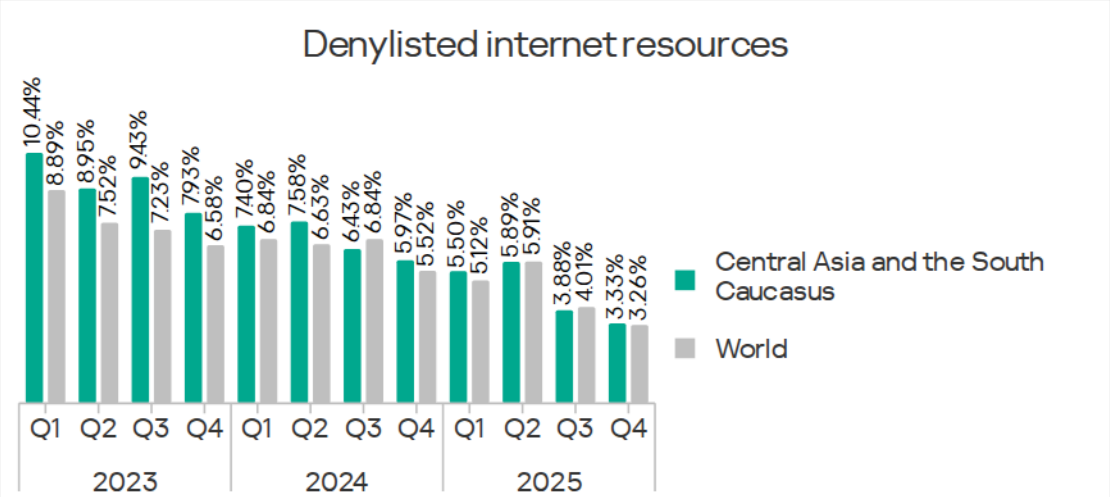
Compared to the global averages, the region had higher percentages of ICS computers with the following categories of blocked threats:

- Miners in the form of executable files for Windows: 2.0 times higher. Central Asia and the South Caucasus led globally in this metric.
- Worms: 1.5 times higher. The region ranked third.
- Ransomware: 1.1 times higher. The region ranked fourth.
- Denylisted internet resources.

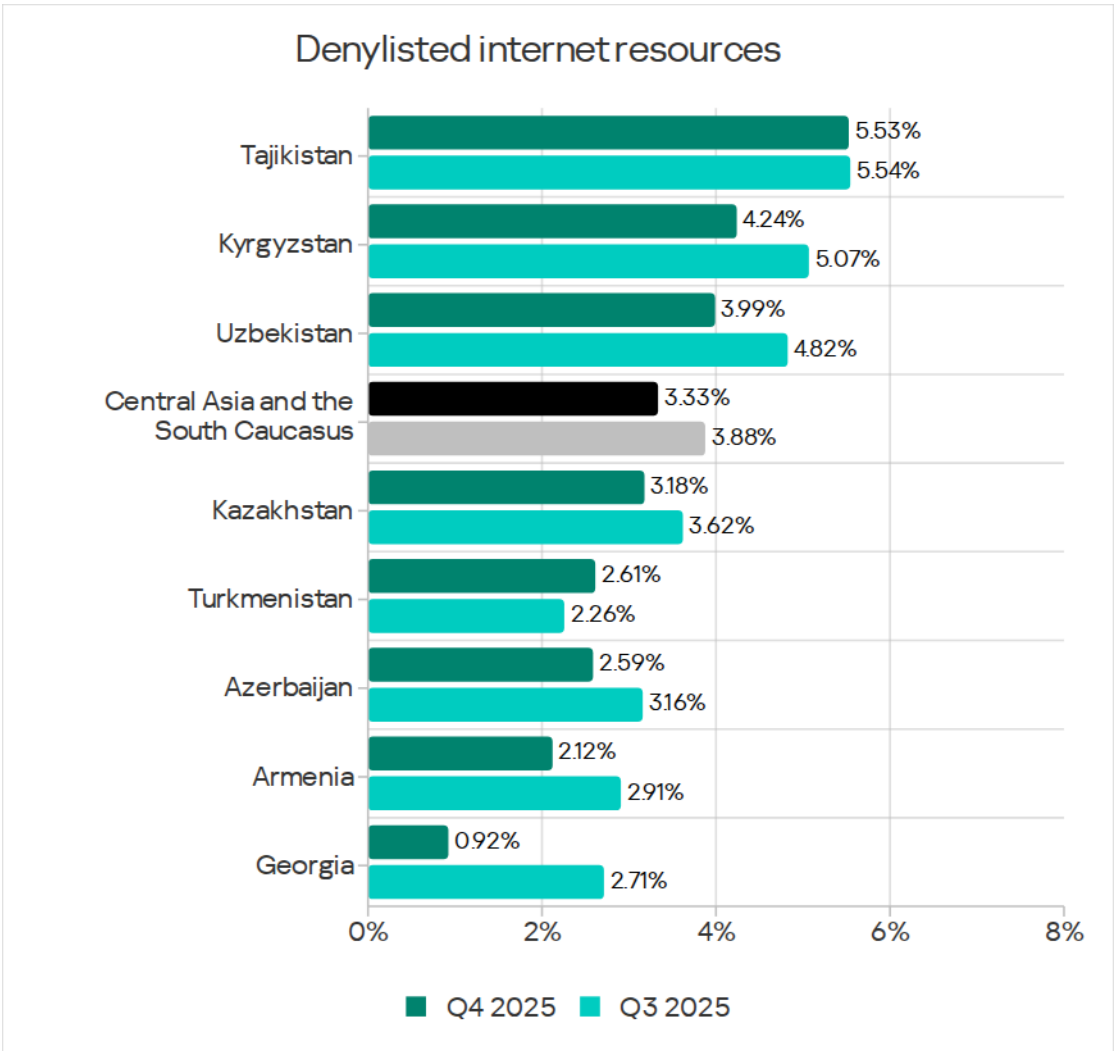
Denylisted internet resources

By the percentage of ICS computers on which denylisted internet resources were blocked, Central Asia and the South Caucasus ranked fourth among the regions, at 3.33%. This is 1.9 times higher than Northern Europe, which had the lowest rate.

This metric is gradually decreasing across all regions of the world, dropping to a three-year low in the Central Asia and South Caucasus region in Q4 2025.



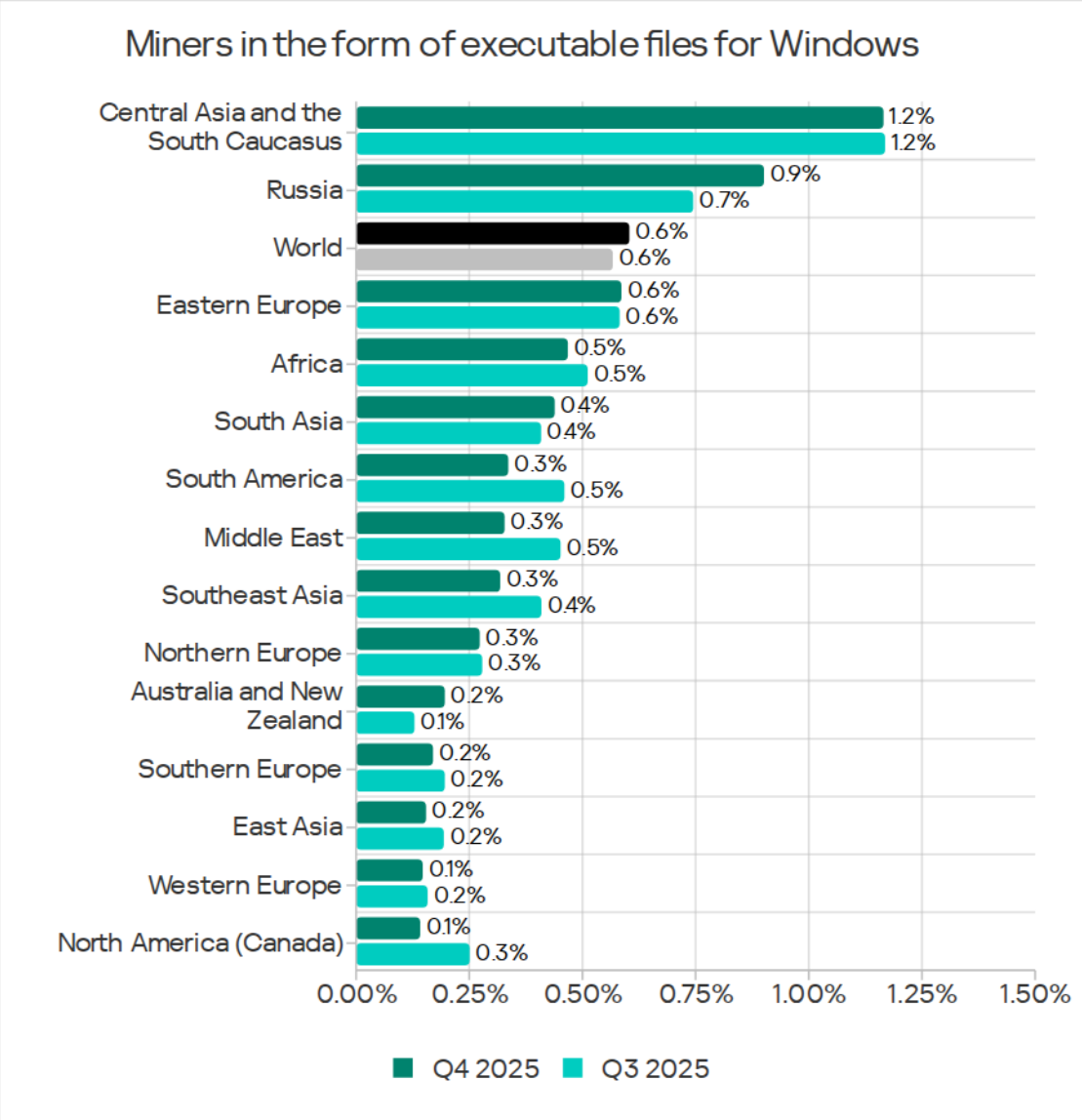
Among countries of the region, Tajikistan led with 5.53% in the percentage of ICS computers on which denylisted internet resources were blocked. The lowest figure observed was in Georgia at 0.92%.



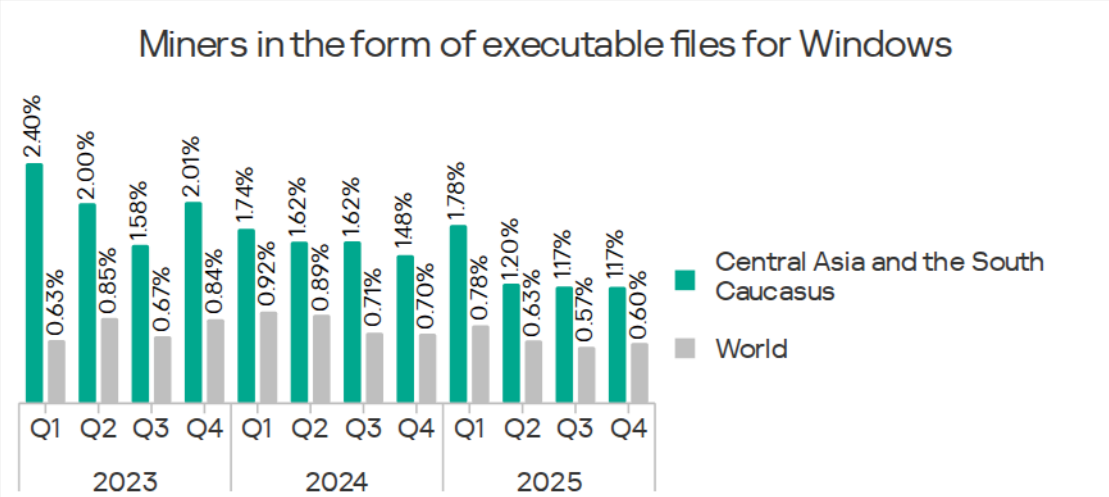
The internet is the sole threat source for this category. Tajikistan was one of the two leading countries in terms of internet threats.

Miners in the form of executable files for Windows

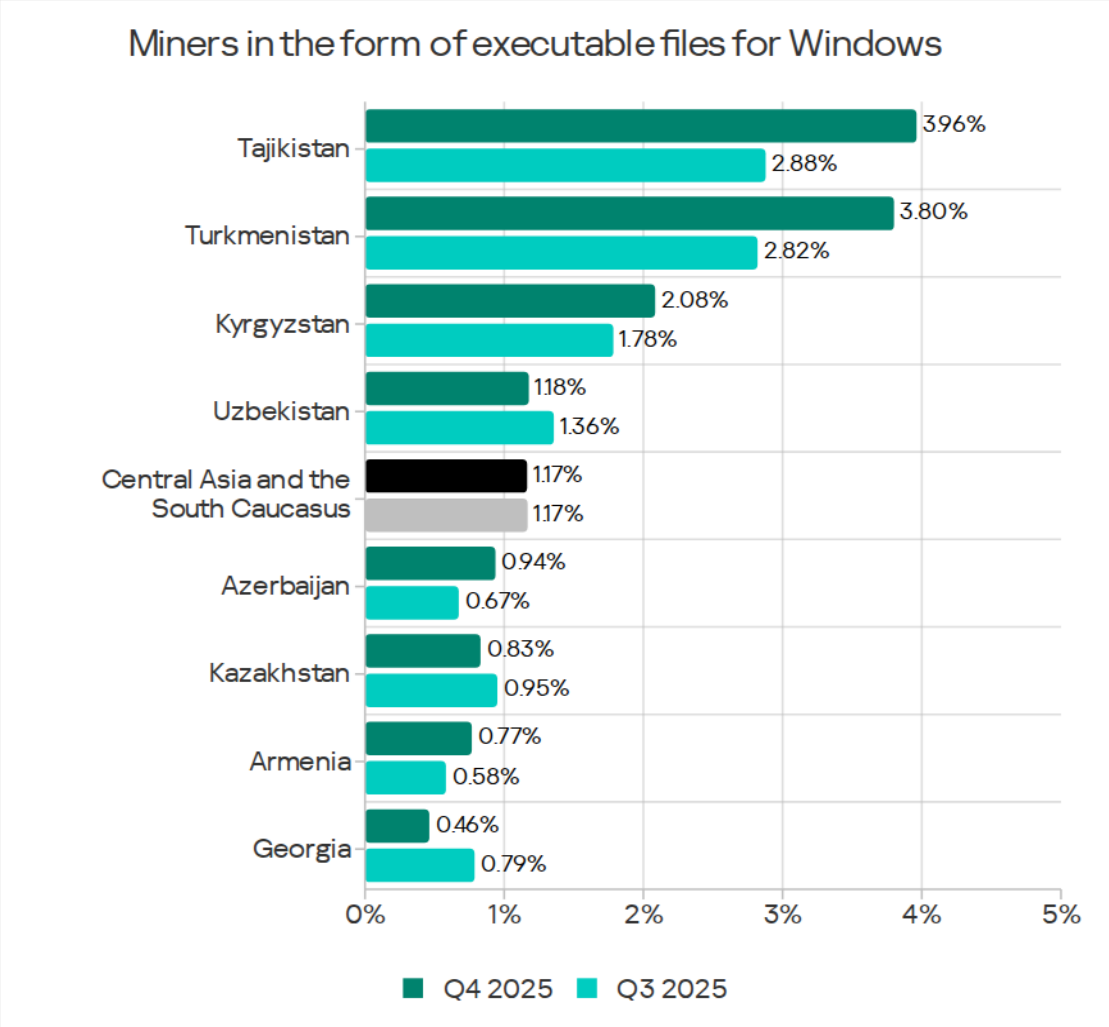
By the percentage of ICS computers with blocked miners in the form of executable files for Windows, Central Asia and the South Caucasus led all regions with 1.17%. The rate was 8.4 times higher than that in the Australia and New Zealand region, which has the lowest figure among all regions.



The percentage of ICS computers on which miners in the form of executable files for Windows were blocked is trending downward in the region. This figure did not change over the quarter and is still at its three-year low.



Among the countries in the region, Tajikistan (3.96%) and Turkmenistan (3.80%) led in the percentage of ICS computers with blocked miner executables. The metrics for both of these countries almost fully recovered from their drop in the last quarter to approach the previous levels.



Miners in the form of executable files for Windows are distributed primarily over the internet and through removable media.

Tajikistan was second among the region's countries in internet threats, while Turkmenistan led in ICS computers on which threats were blocked upon connecting removable media.

Importantly, miners in the form of executable files for Windows are using worm functionality to spread. That's why the metrics for miners in the form of executable files and for worms showed largely similar trends in the Central Asia and South Caucasus region.

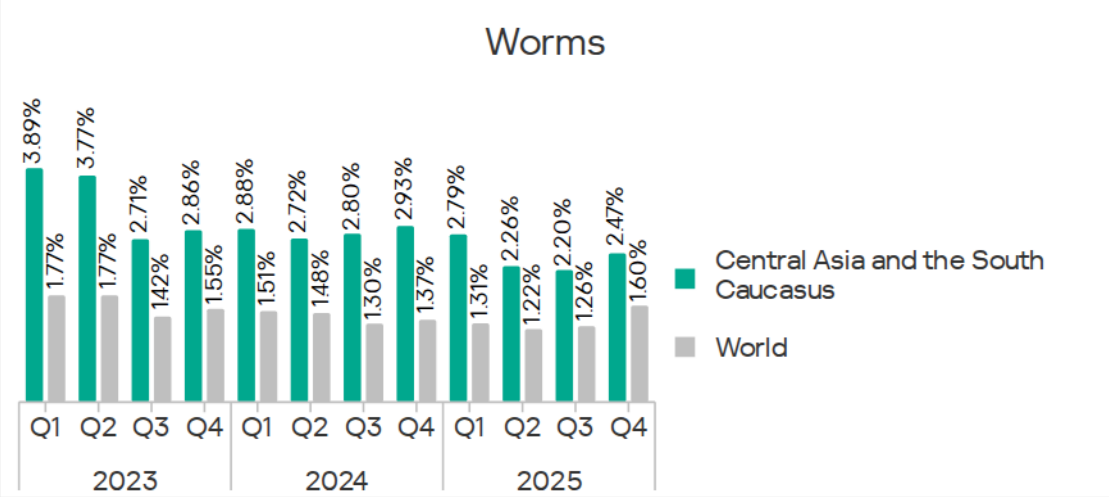
Worms

Based on the percentage of ICS computers on which worms were blocked, the Central Asia and South Caucasus region ranked third among regions.

Among threat categories in the region, worms placed fourth. Worms occupied a similarly high position in the regional rankings in the three more regions: Russia, South Asia, and Africa.

In Q4 2025, the worm metric grew across all regions due to the latest wave of phishing campaigns known as Curriculum-vitae-catalina which we described earlier.

In the Central Asia and South Caucasus region, this figure increased to 2.47%. This figure was 7.7 times higher than in Northern Europe, which had the lowest percentage among all regions.

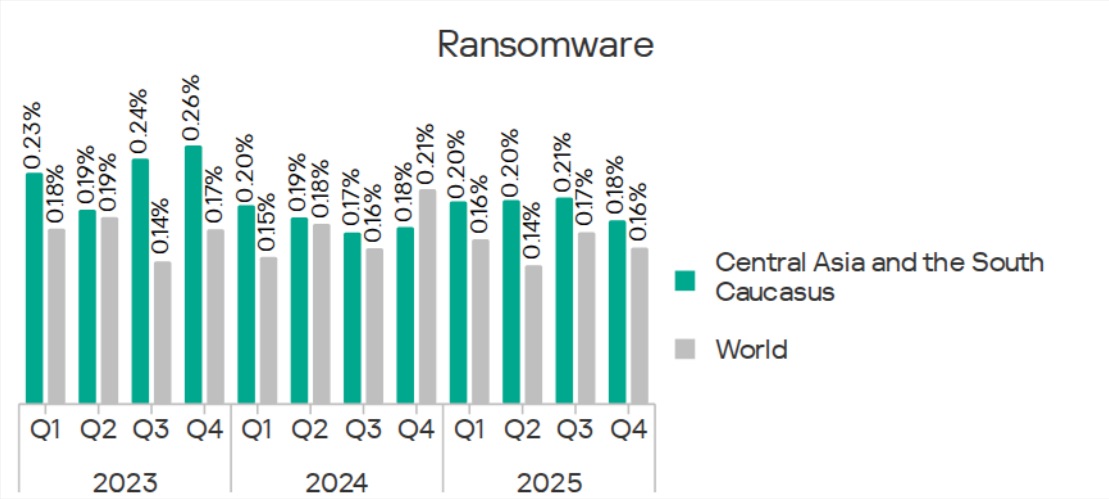


Among the region's countries, Turkmenistan led in the percentage of ICS computers on which worms were blocked, at 11.64%. The rate increased across all countries of the region except Armenia.

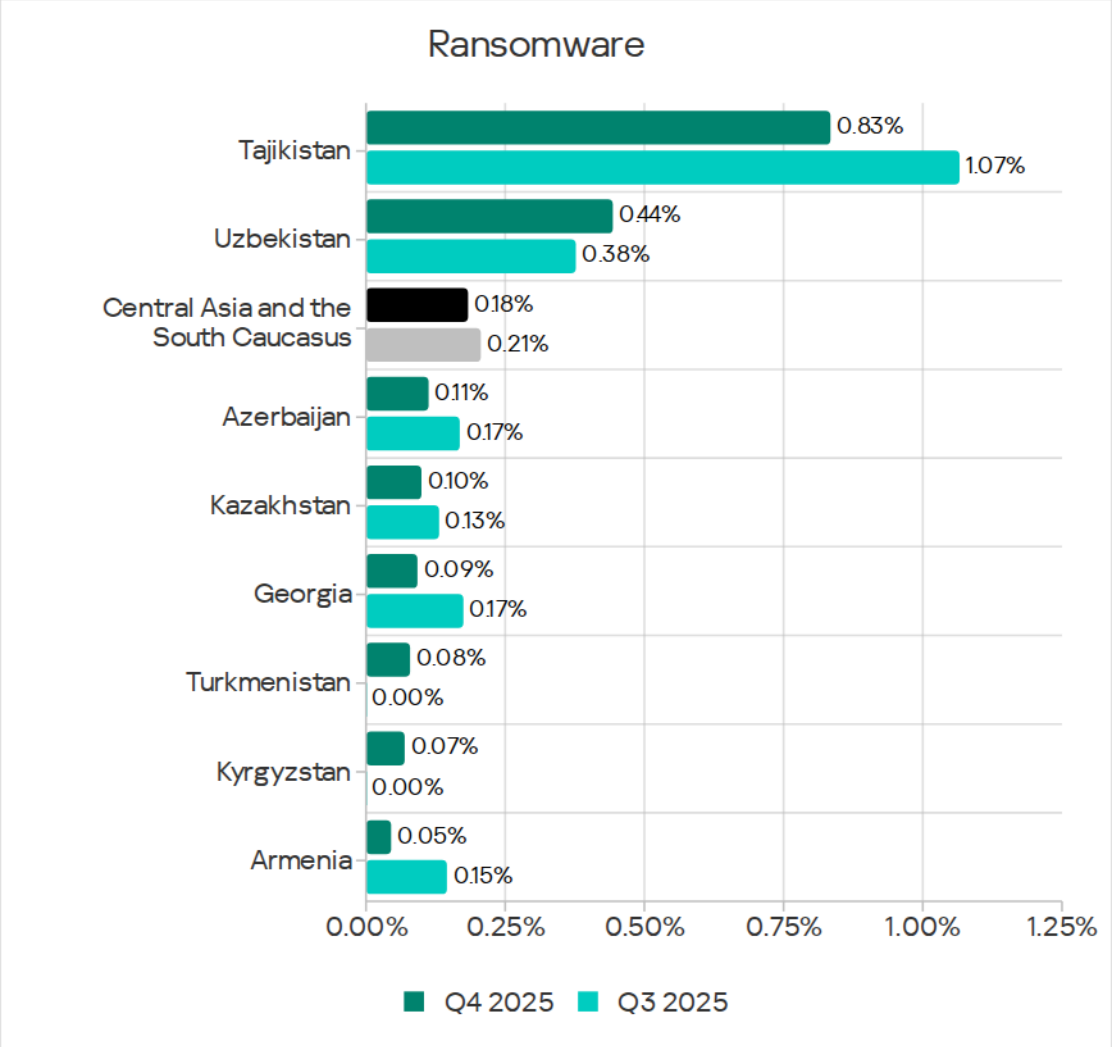
Ransomware

By percentage of ICS computers on which ransomware was blocked, Central Asia and the South Caucasus ranked fourth globally with 0.18%. The region's rate was 3.6 times higher than Northern Europe, which ranked last.

Meanwhile, the region's ransomware rate was fairly stable, increasing slightly over the quarter.



Among the region's countries, Tajikistan had a significant lead in the percentage of ICS computers on which ransomware was blocked, at 0.83%.

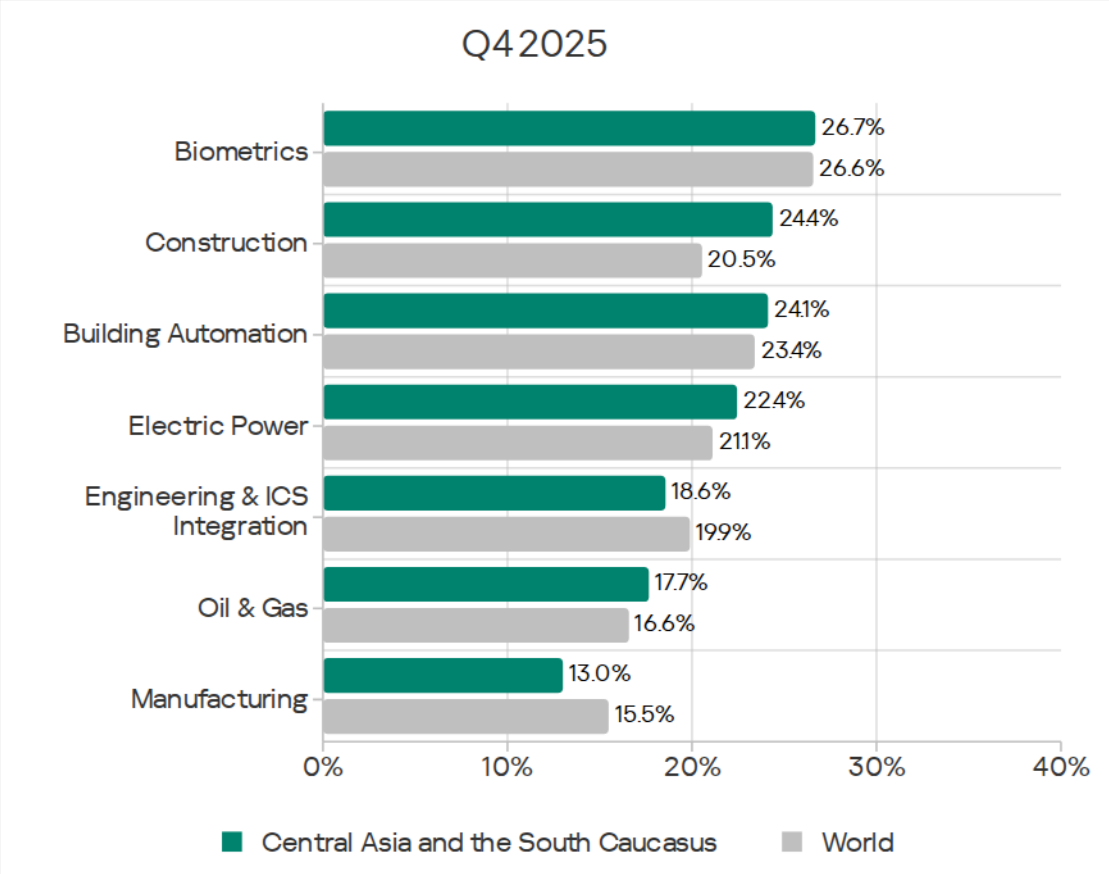


Industries

In the rankings for regions based on the percentage of ICS computers on which threats were blocked in various industries, the Central Asia and South Caucasus region ranked highest for the following metrics across all industries:

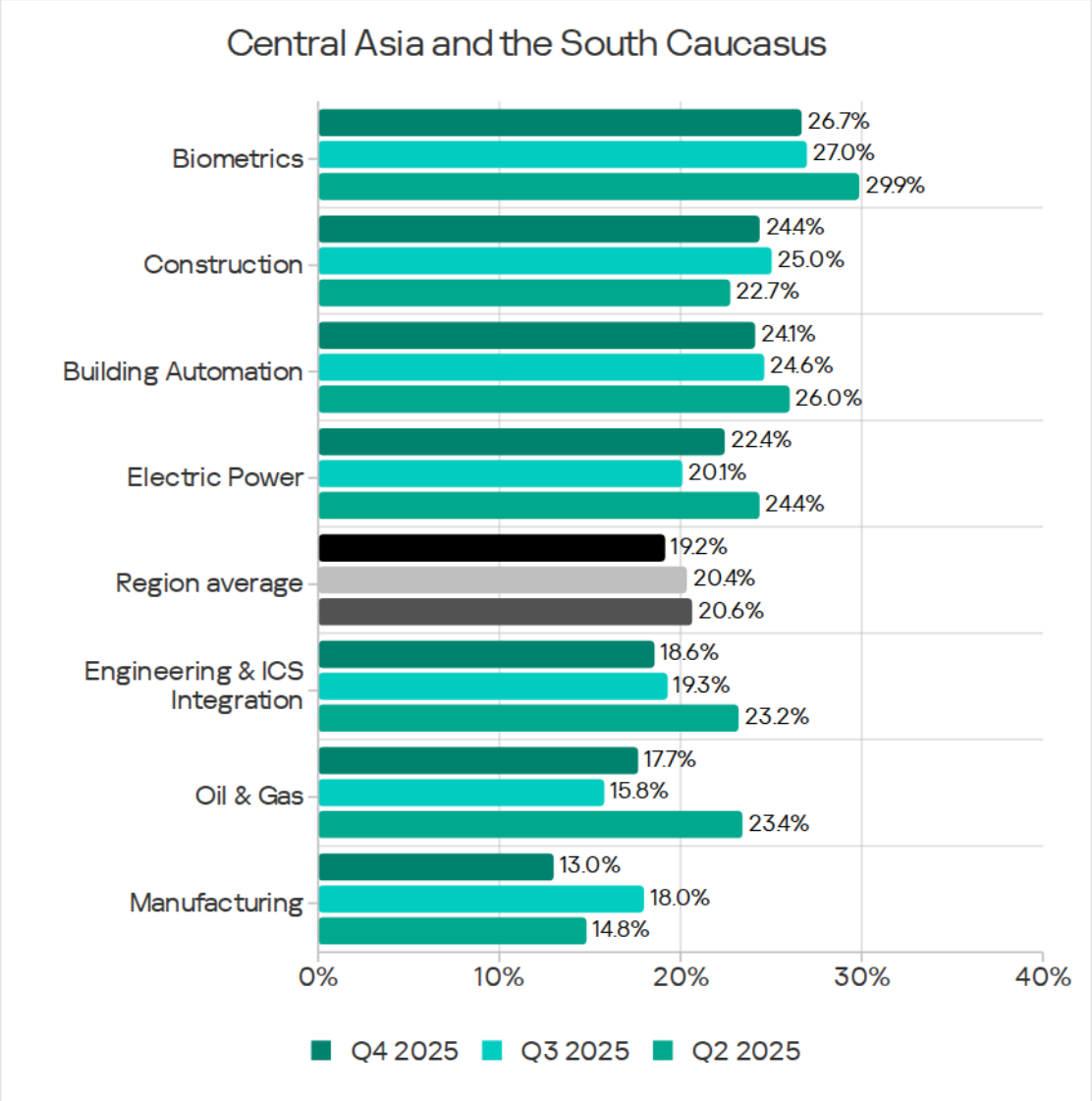
- Construction: third.
- Biometrics: fourth.
- Oil and gas: fourth.

Among the region's industries analyzed in the report, threats were most frequently encountered in biometrics.

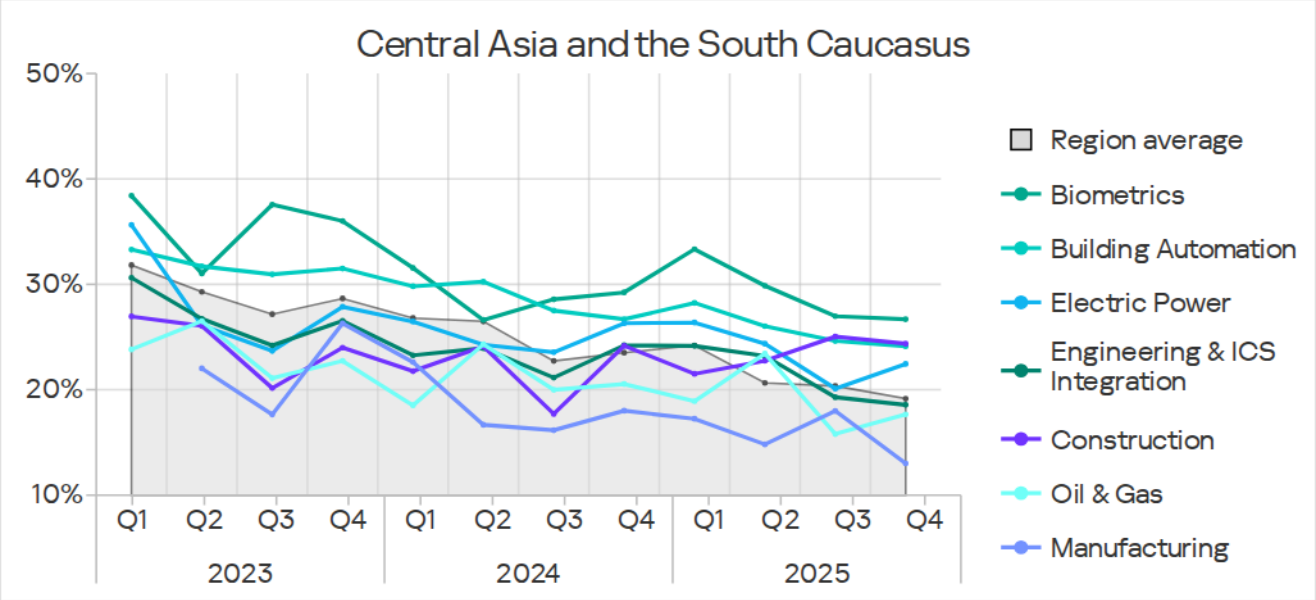


This metric exceeded the global average across all reviewed industries except for manufacturing, and engineering and ICS integrators. The construction industry showed the largest positive gain, by a factor of 1.2.

The percentage of ICS computers on which malicious objects were blocked increased in the following two industries over the quarter: oil and gas, and electric power.



Trends across all industries generally showed an improvement (declining rates), although some industries displayed noticeable fluctuations.



Threat sources and malware categories in industries: 'hotspots'

We use heat maps when assessing threats to industries in the regions. The color on the heatmap indicates the position in the global industry rankings across regions for each individual threat category or source. Red signifies that the figure is close to the maximum.

Threat source indicators for industries in Central Asia and the South Caucasus, Q4 2025

Industry / Threat source	Biometrics	Building Automation	Engineering & ICS Integration	Electric Power	Oil & Gas	Construction	Manufacturing	Category metric in region
Internet	5.93%	7.81%	7.25%	8.23%	6.51%	10.07%	4.64%	6.43%
Email clients	3.77%	2.17%	1.16%	2.12%	1.06%	1.32%	0.31%	1.28%
Removable media	—	0.54%	0.25%	0.62%	0.40%	0.93%	0.62%	0.43%
Network folders	—	0.03%	0.02%	0.12%	—	—	0.31%	0.02%
Industry metric in region	26.68%	24.12%	18.57%	22.44%	17.66%	24.37%	13.00%	

Threat category indicators for industries in Central Asia and the South Caucasus, Q4 2025

Industry / Threat type	Biometrics	Building Automation	Engineering & ICS Integration	Electric Power	Oil & Gas	Construction	Manufacturing	Category metric in region
Denylisted internet resources	5.39%	3.84%	3.82%	5.74%	4.52%	4.37%	1.86%	3.33%
Malicious scripts and phishing pages (JS and HTML)	6.47%	5.50%	4.76%	7.11%	4.38%	5.96%	3.10%	4.32%
Malicious documents (MSOffice + PDF)	2.43%	1.41%	0.84%	1.25%	0.80%	0.53%	0.62%	0.89%
Spy Trojans, backdoors and keyloggers	7.01%	5.84%	3.40%	4.74%	2.79%	3.84%	2.48%	3.58%
Ransomware	0.81%	0.33%	0.27%	0.62%	0.40%	0.53%	0.31%	0.18%
Miners in the form of executable files for Windows	1.62%	1.51%	0.96%	1.75%	0.93%	1.99%	1.24%	1.17%
Web miners running in browsers	0.81%	0.19%	0.17%	0.62%	0.27%	0.26%	0.62%	0.16%
Malware for AutoCAD	—	0.04%	0.17%	0.37%	0.13%	0.53%	—	0.09%
Worms	3.77%	3.66%	1.53%	2.99%	1.86%	2.38%	0.62%	2.47%
Viruses	1.08%	1.44%	0.84%	2.37%	0.80%	1.46%	1.24%	0.96%
Industry metric in region	26.68%	24.12%	18.57%	22.44%	17.66%	24.37%	13.00%	

Characteristics of the region

High figure for the internet as a threat source. As a result, relevant threat categories included denylisted internet resources, and malicious scripts and phishing pages.

High figure for miners in the form of executable files for Windows. Central Asia and the South Caucasus led globally in the percentage of ICS computers

on which miners in the form of executable files for Windows were blocked. All industries in the region face this threat, which comes mainly from the internet.

Across all industries covered in the report except for the engineering and ICS integrators industry, the Central Asia and South Caucasus region led among regions for this metric. Based on the engineering and ICS integrators metrics, the region ranked second.

Another major threat is worms. Based on the metric for worms across all industries except for manufacturing, the Central Asia and South Caucasus region was second or third in the corresponding rankings of regions.

Ransomware was also prevalent in the region's industries: the Central Asia and South Caucasus region was at least third among regions for this metric in the industry rankings:

- First place among regions in biometrics, construction, electric power, and manufacturing industries.
- Second place in the engineering and ICS integrators industry and oil and gas industry.
- Third place in the building automation industry.

Biometrics

Central Asia and the South Caucasus ranked fourth among regions in the percentage of ICS computers on which malicious objects were blocked in biometrics.

Based on industry indicators among regions, Central Asia and the South Caucasus had the following rankings:

- First in the percentage of ICS computers on which denylisted internet resources and ransomware were blocked.
- Third in terms of worms.

Among industries in the region, biometrics had the following rankings:

- First place for threats from email clients.
- First place in the following threat categories: malicious documents, spyware, ransomware, worms, and web miners.
- Second place for denylisted internet resources, malicious scripts and phishing pages.
- Third place in miners in the form of executable files.

Construction

Central Asia and the South Caucasus ranked third globally in the percentage of ICS computers on which malicious objects were blocked in the construction sector.

Among all the regions and industries, construction in Central Asia and the South Caucasus ranked:

- First in the percentage of ICS computers on which miners in the form of executable files for Windows were blocked.

Within industries in the region, construction ranked:

- Second in the percentage of ICS computers on which threats from removable media were blocked.
- First in the percentage of ICS computers on which miners in the form of executable files for Windows and ransomware were blocked.
- Second for worms.
- Third in denylisted internet resources.

Among industries in all regions, the construction industry had the following rankings:

- First place based on the percentage of ICS computers on which internet threats were blocked.
- First place by the percentage of ICS computers on which miners in the form of Windows executable files and malware for AutoCAD were blocked.
- Second in viruses.
- Third place in malicious scripts, phishing pages, and ransomware.

Building automation

Central Asia and the South Caucasus ranked sixth globally by the percentage of ICS computers on which malicious objects were blocked in the building automation industry.

Based on industry indicators among all regions, Central Asia and the South Caucasus had the following rankings:

- First place in the percentage of ICS computers on which miners in the form of executable files for Windows were blocked.
- Second place for denylisted internet resources and worms.
- Third place in ransomware.

Among the region's industries, building automation was the only one where ICS computers blocked network folder threats. Additionally, it ranked:

- Second in mail client threats.
- Third in terms of threats from the internet, removable media, and network folders.
- Second in the percentage of ICS computers on which malicious documents, spyware, and worms were blocked.
- Third in viruses.

Electric power

Central Asia and the South Caucasus ranked fifth globally in the percentage of ICS computers on which malicious objects were blocked in the electrical energy industry.

Based on industry indicators among all regions, Central Asia and the South Caucasus had the following rankings:

- Second place in the percentage of ICS computers on which network folder threats were blocked.
- Third place in removable media threats.
- First place in the percentage of ICS computers on which the following threat categories were blocked: denylisted internet resources, both categories of miners, and ransomware.
- Third place in worms.

In the regional cross-industry rankings, the electrical energy industry ranked:

- Second by percentage of ICS computers on which threats from the internet and in network folders were blocked.
- Third for threats from email clients.
- First by percentage of ICS computers on which threats in the following categories were blocked: denylisted internet resources, malicious scripts and phishing pages, viruses.
- Second place in both categories of miners, ransomware, and malware for AutoCAD.
- Third in malicious documents, spyware, and worms.

Engineering and ICS integrators

Central Asia and the South Caucasus ranked seventh globally in the percentage of ICS computers on which malicious objects were blocked in engineering and ICS integrators.

Based on industry indicators among all regions, Central Asia and the South Caucasus had the following rankings:

- Third for the percentage of ICS computers on which network folder threats were blocked.
- Second place in the percentage of ICS computers on which miners in the form of executable files for Windows, and ransomware were blocked.
- Third place in denylisted internet resources, and worms.

In the regional cross-industry rankings, engineering and ICS integrators had the following positions:

- First place in the percentage of ICS computers on which threats were blocked when connecting removable media.
- Third place in the percentage of ICS computers on which malware for AutoCAD was blocked.

Manufacturing

Central Asia and the South Caucasus ranked ninth globally in the percentage of ICS computers on which malicious objects were blocked in the industry.

Based on industry indicators among all regions, Central Asia and the South Caucasus had the following rankings:

- Second place in the percentage of ICS computers on which threats from removable media and network folders were blocked.
- First place in the percentage of ICS computers on which miners in the form of executable files for Windows and ransomware were blocked.
- Third place in web miners.

In the regional cross-industry rankings, the manufacturing sector ranked:

- First for the percentage of ICS computers on which network folder threats were blocked.
- Third for ICS computers on which web miners were blocked.

Oil and gas

Based on the percentage of ICS computers on which malicious objects were blocked in the oil and gas industry, the Central Asia and South Caucasus region ranked fourth among regions.

Based on industry indicators among all regions, Central Asia and the South Caucasus had the following rankings:

- Second in the percentage of ICS computers on which threats from removable media were blocked.
- Third for threats from email clients.
- First place in the percentage of ICS computers on which denylisted internet resources and miners in the form of executable files for Windows were blocked.
- Second place in the following threat categories: spyware, ransomware, and worms.
- Third in viruses and malware for AutoCAD.

In the regional cross-industry rankings, oil and gas was:

- Second in the percentage of ICS computers on which threats from removable media were blocked.
- Third in the percentage of ICS computers on which denylisted internet resources were blocked.

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 to have been attacked if a Kaspersky security solution blocked one or more threats on that computer during the review period: 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 review period 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