Kaspersky ICS CERT

kaspersky

Threat landscape for industrial automation systems

Asia. Q3 2025

24.12.2025

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 ranks 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 leads 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 rank second in the regional ranking of malware categories by percentage of ICS computers on which they were blocked. This is the highest position for viruses among all regional rankings. The regional indicator exceeds the global average by a factor of 5.3 and is the highest figure in the world.

Among all categories of threats, in Q3 2025 the global rankings showed that malware for AutoCAD ranks seventh out of ten in the percentage of ICS computers on which a threat was blocked. In all regions except South Asia, East Asia, and Southeast Asia, this category ranks last. However, the regional ranking of Southeast Asia is sixth with a figure that exceeds the global average by a factor of 7.3 and is the highest in the world.

Lack of segmentation in enterprise networks in the region

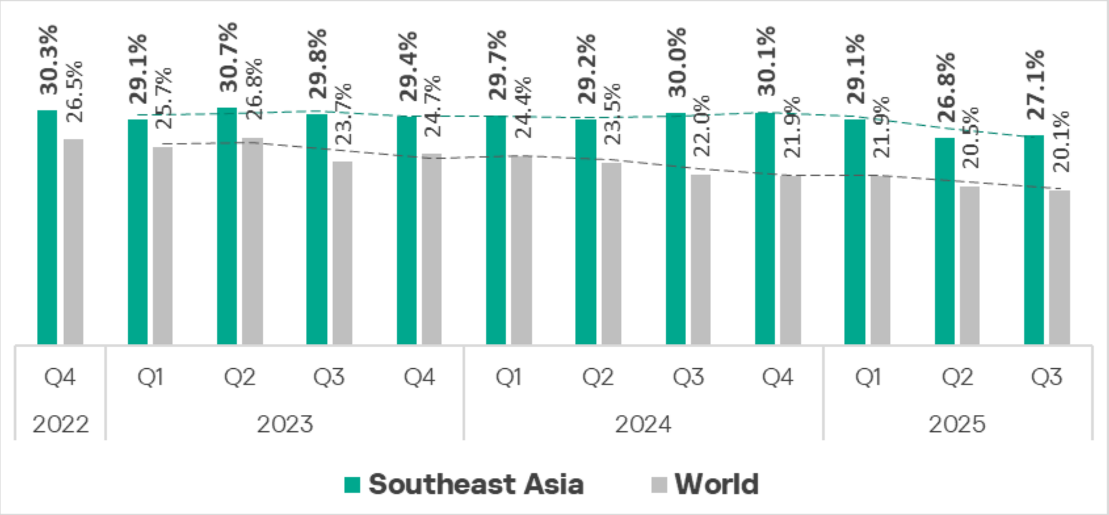
With its rate of 0.10%, Southeast Asia ranks second among regions based on the percentage of ICS computers on which threats were blocked in network folders. This figure is higher than the global average by a factor of 2.5.

This is predominately the result of the situation in Vietnam, which leads by a wide margin among countries of the region in terms of viruses, malware for AutoCAD, and network folder threats.

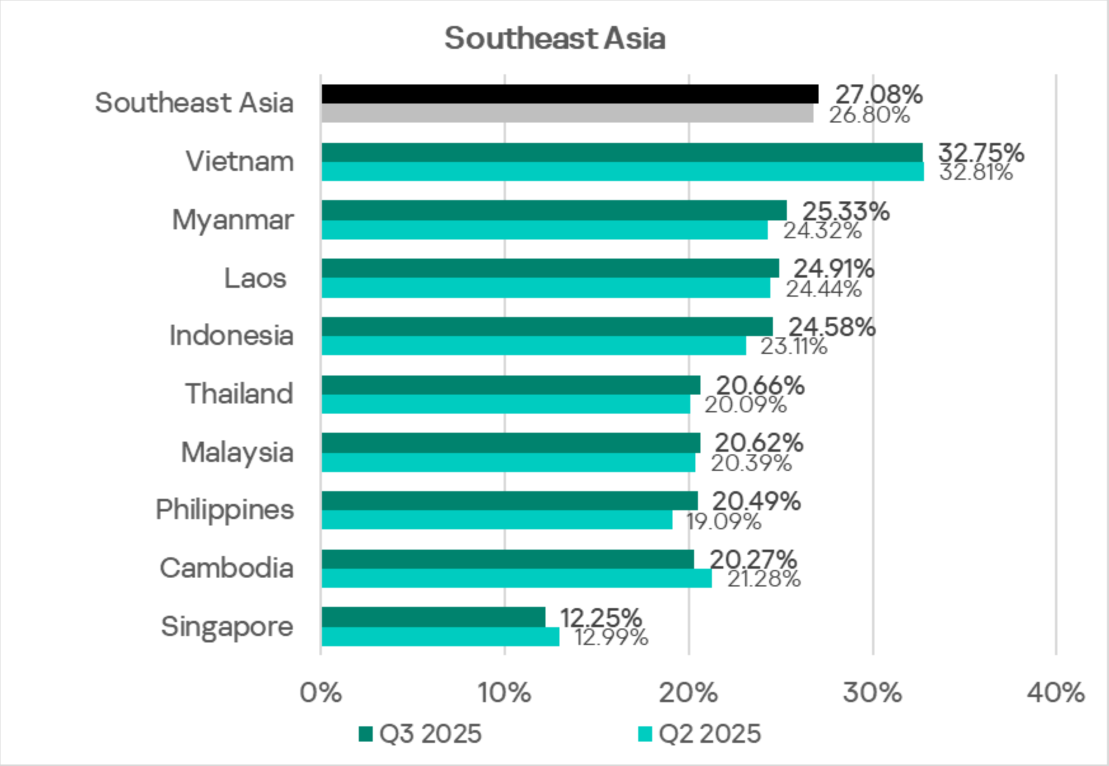
Statistics across all threats

With its rate of 27.1%, Southeast Asia ranks second globally based on the percentage of ICS computers on which malicious objects were blocked. This figure is 1.3 times higher than the global average and 2.9 times higher than the minimum figure among regions as recorded in Northern Europe.

After the decrease in the regional indicator during the two previous quarters, in Q3 2025 the percentage of ICS computers on which malicious objects were blocked in Southeast Asia increased but did not return to the figures observed at the end of 2024.

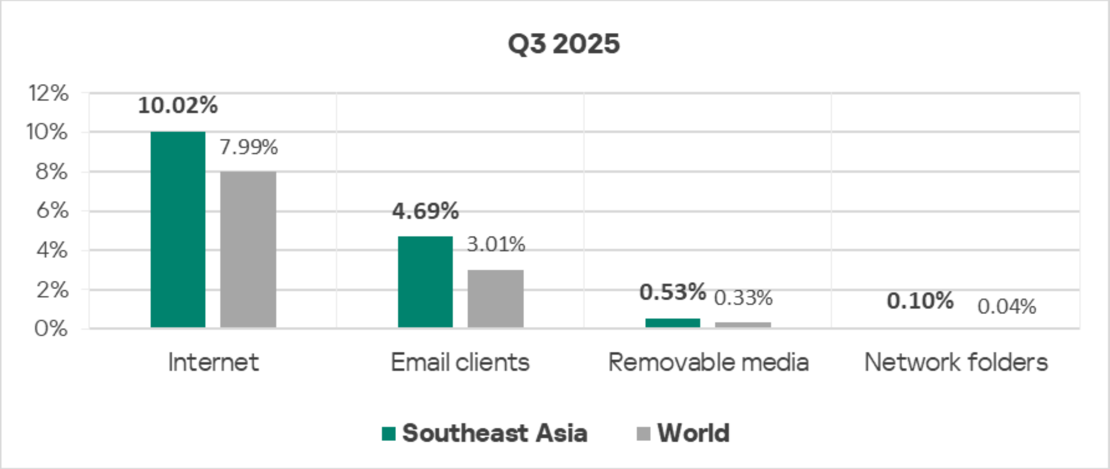


The percentage of ICS computers with blocked malicious objects varies among the region's countries, ranging from 12.25% in Singapore to 32.75% in Vietnam. Other countries' rates fall between 20% and 26%.

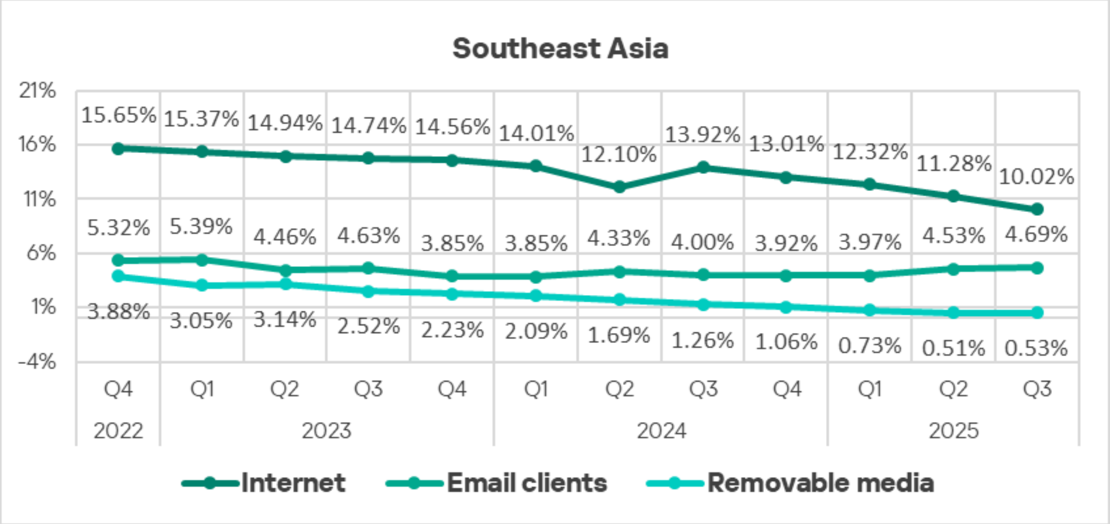


Threat sources

The percentage of ICS computers on which threats from various sources were blocked was higher than the global averages for all sources in the region. The percentage of ICS computers on which email clients and removable media were the source of a threat is 1.6 times higher in the region than the global percentages for each of these sources. The regional figure for network folders exceeds the global average by a factor of 2.5.



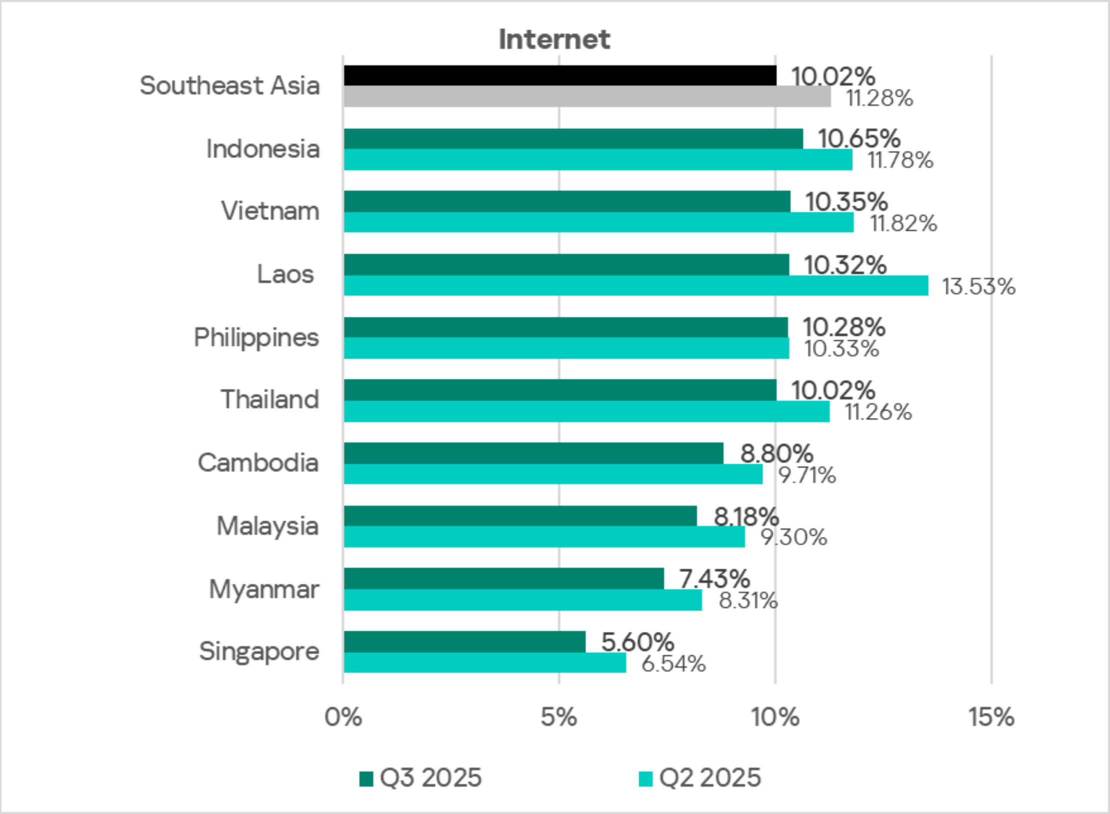
In Q3 2025, this indicator increased for email clients and slightly grew for removable media.



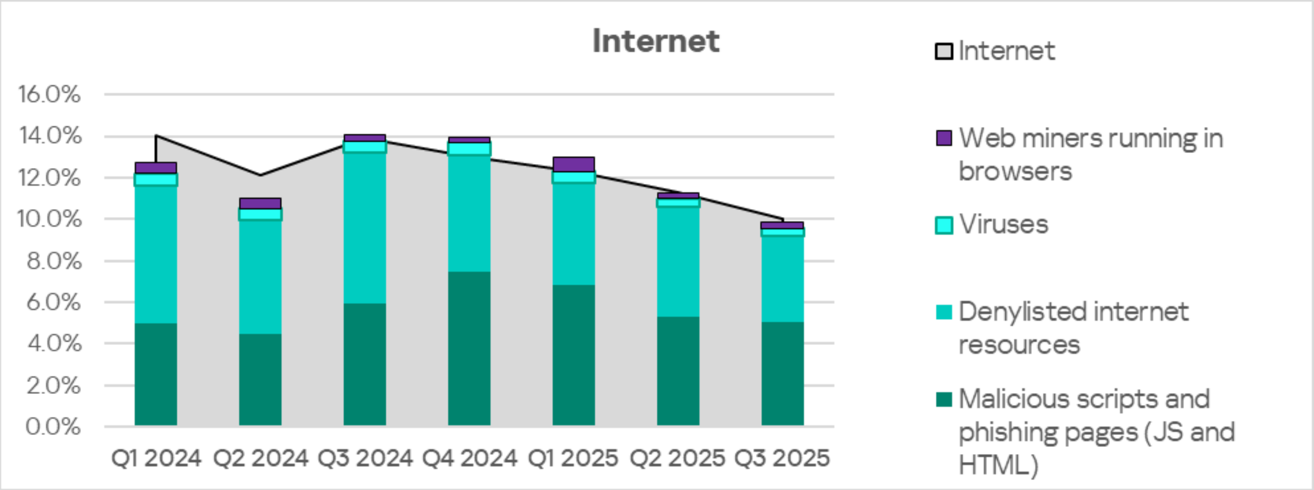
Internet

Based on the percentage of ICS computers on which internet threats were blocked, Southeast Asia ranks second among regions with a figure that exceeds the minimum (Northern Europe) by a factor of 2.2.

The indicators for countries in the region range from 5.60% in Singapore to 10.65% in Indonesia.

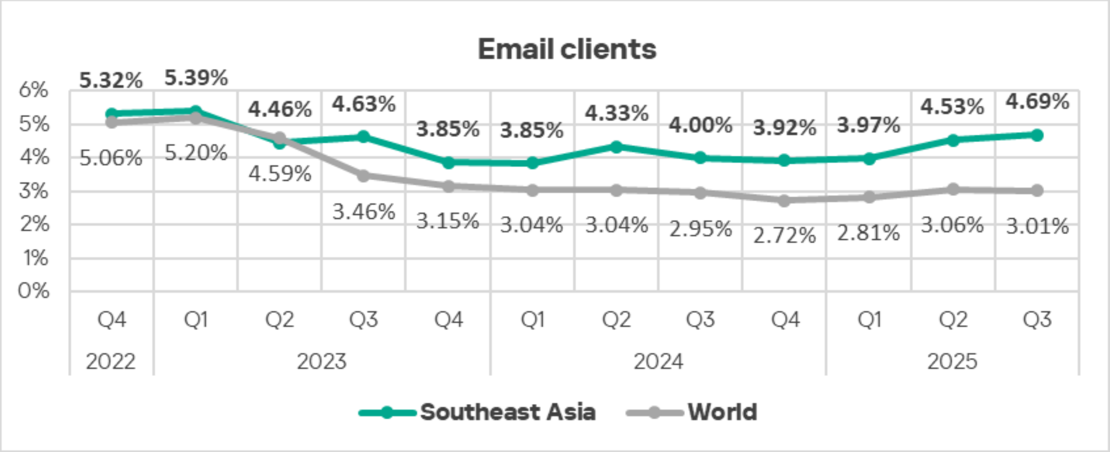


The main categories of internet threats blocked on ICS computers in the region are malicious scripts and phishing pages, denylisted internet resources, viruses, and web miners.

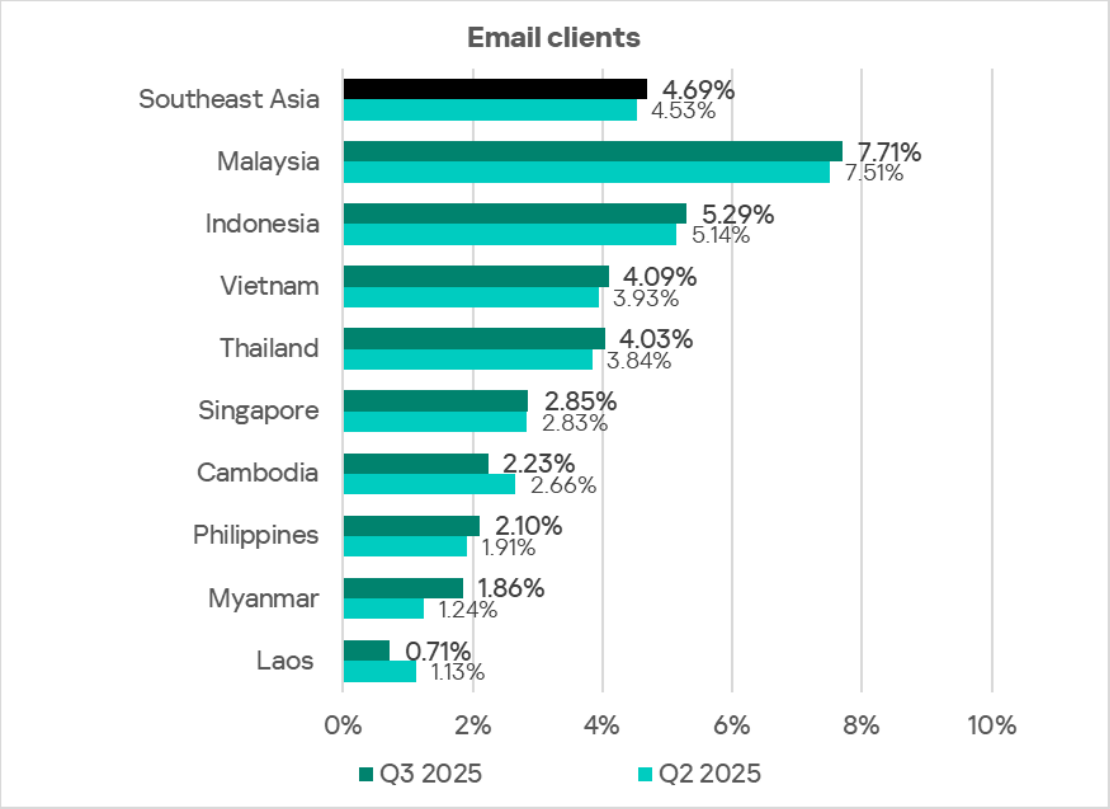


Email clients

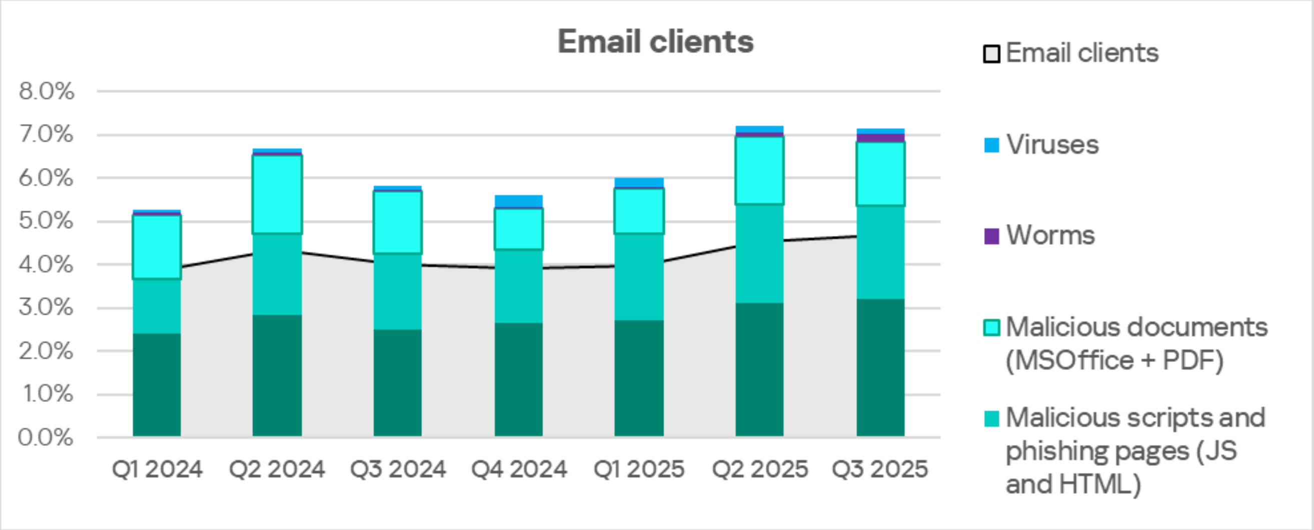
Email clients are a threat source that has been growing for three consecutive quarters in the region.



Among countries of the region, Malaysia leads by a noticeable margin with 7.71%. The lowest percentage of ICS computers on which email client threats were blocked was observed in Laos (0.71%). In contrast to most countries of the region (all except Cambodia), the indicator for Laos decreased during the quarter.



The main categories of email-borne threats blocked on ICS computers are spyware, malicious scripts and phishing pages, and malicious documents. Southeast Asia ranks second among regions for spyware.

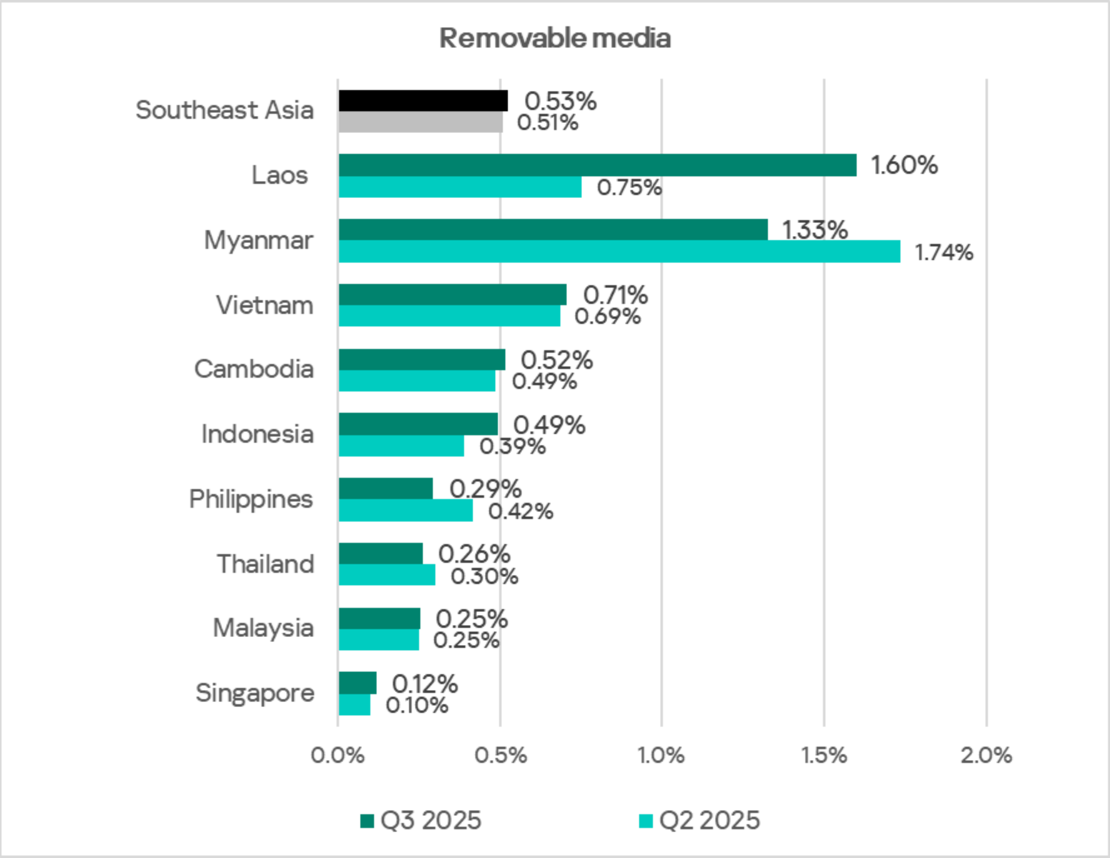


Removable media

Southeast Asia ranks fifth among regions based on the percentage of ICS computers on which removable media threats were blocked upon connection. The first six positions in this ranking are occupied by Africa (leading by a wide margin), Asian regions, and the Middle East. The figures of not only Africa but also in all of these regions are significantly higher than the figures in all other regions.

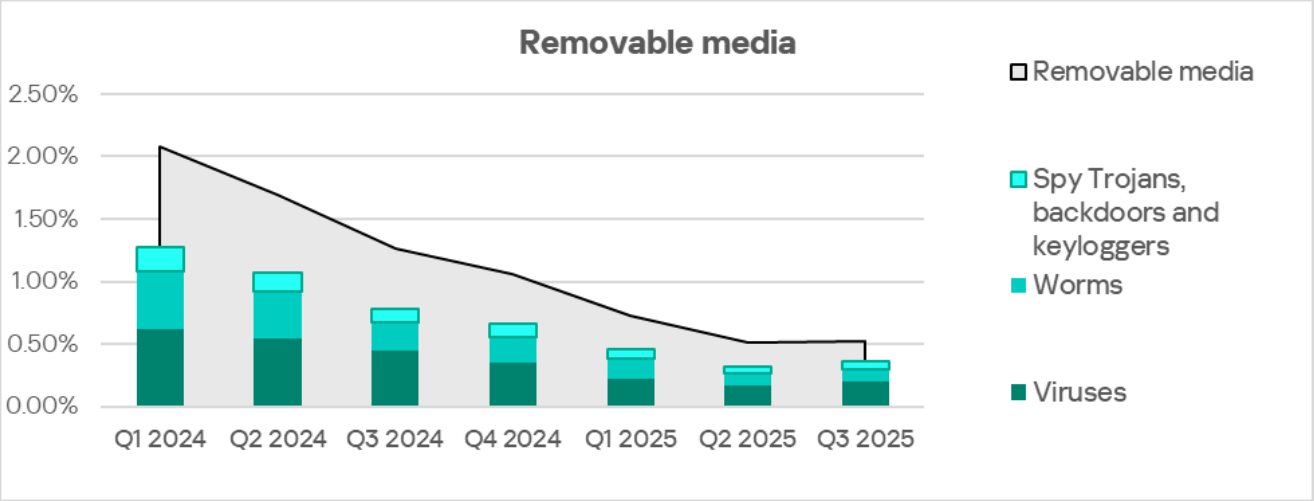
The figure for Southeast Asia grew to 0.53% and is 10.6 times higher than the figure in the Australia and New Zealand region, which ranks last.

Among countries of the region, the leaders by a wide margin are Laos with 1.60% (the indicator over the quarter in this country grew by a factor of 2.1) and Myanmar with 1.33%. The lowest figure, 0.12%, was observed in Singapore.



Both countries that led the ranking in removable media, Laos and Myanmar, had the lowest indicators for email client threats out of all countries of the region.

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

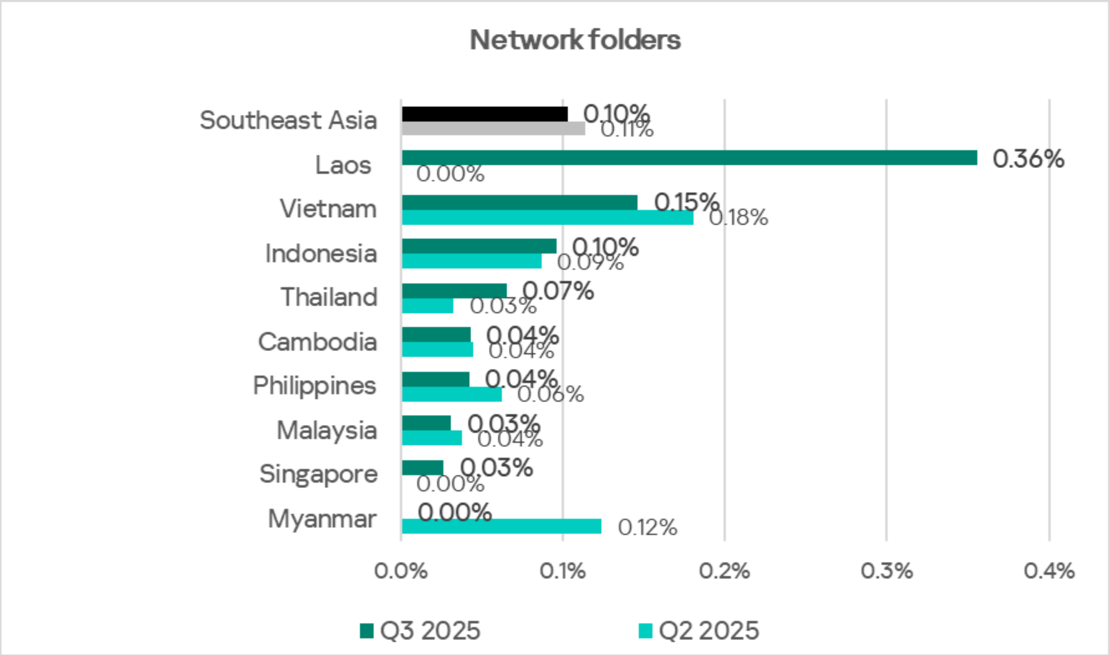


Network folders

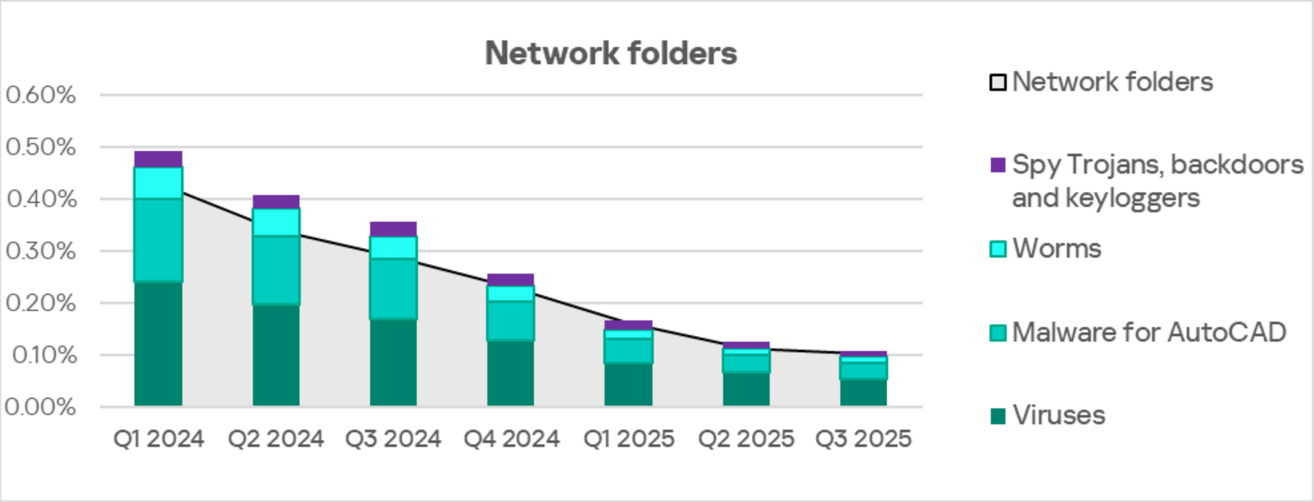
Southeast Asia ranks second among regions based on the percentage of ICS computers on which threats were blocked in network folders with 0.10%, which is bested only by East Asia.

The figures for the two leading regions are significantly higher than those for the others. The figure for Southeast Asia is 1.7 times higher than the next-ranked region, the Middle East. Compared to Northern Europe, which ranks last, the rate is 17.2 times higher.

Among countries in the region, Laos at 0.36% leads in Q3 2025 by a noticeable margin in the percentage of ICS computers on which threats in network folders were blocked.



The main threats spreading through network folders are viruses, malware for AutoCAD, worms, and spyware. In terms of malware for AutoCAD, Southeast Asia leads the ranking of regions by a wide margin.



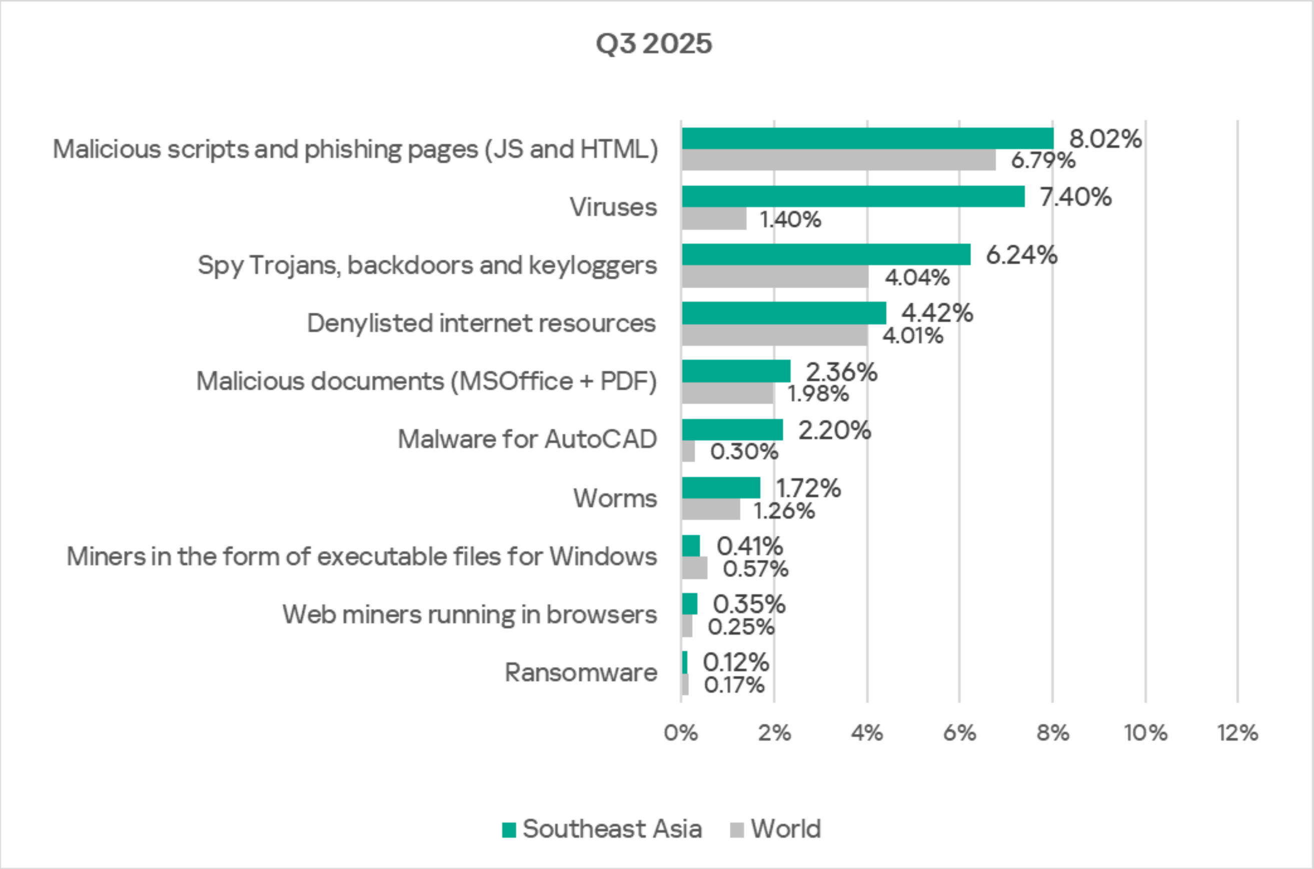
Threat categories

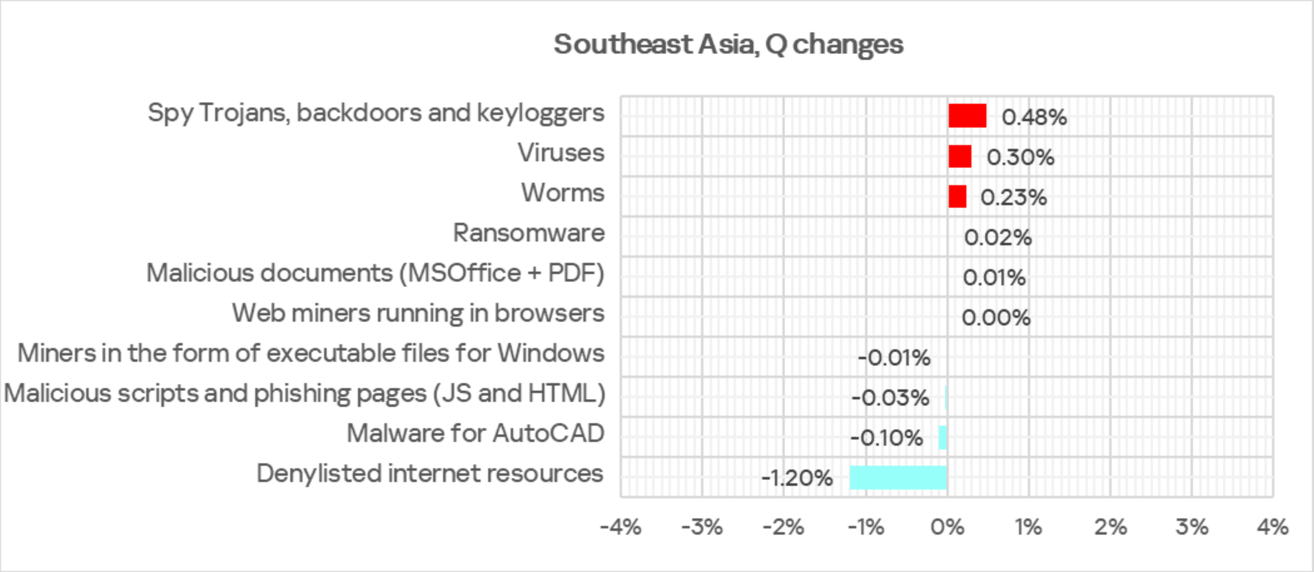
In Southeast Asia, the percentage of ICS computers on which malicious objects were blocked is higher than the respective global averages for all threat categories except three (denylisted internet resources, miners in the form of executable files for Windows, and ransomware).

Regional figures most substantially exceed the global averages for the following threat categories:

- Spyware: 1.5 times higher.
- Viruses: 5.3 times higher.
- Malware for AutoCAD: 7.3 times higher.

In Southeast Asia, viruses rank second among all threat categories. This is the only region where this threat category ranks this high.

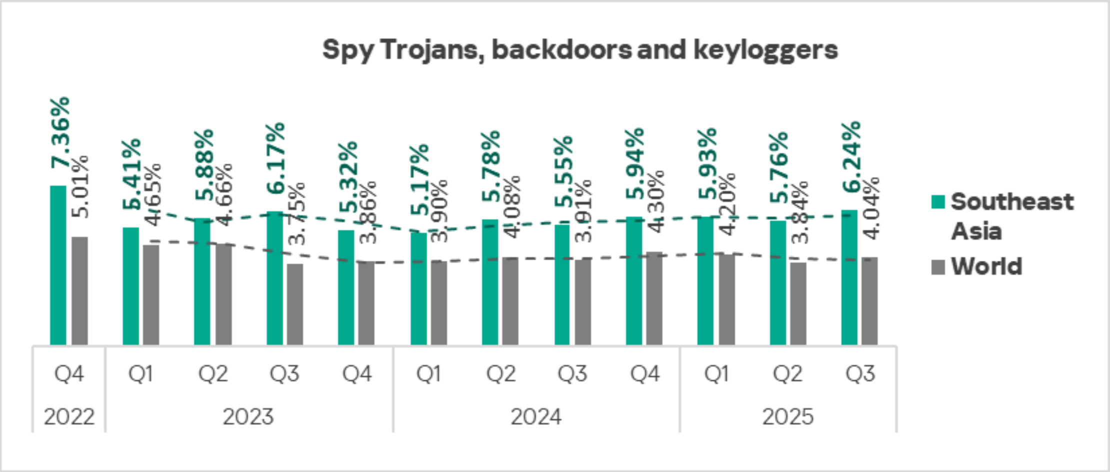




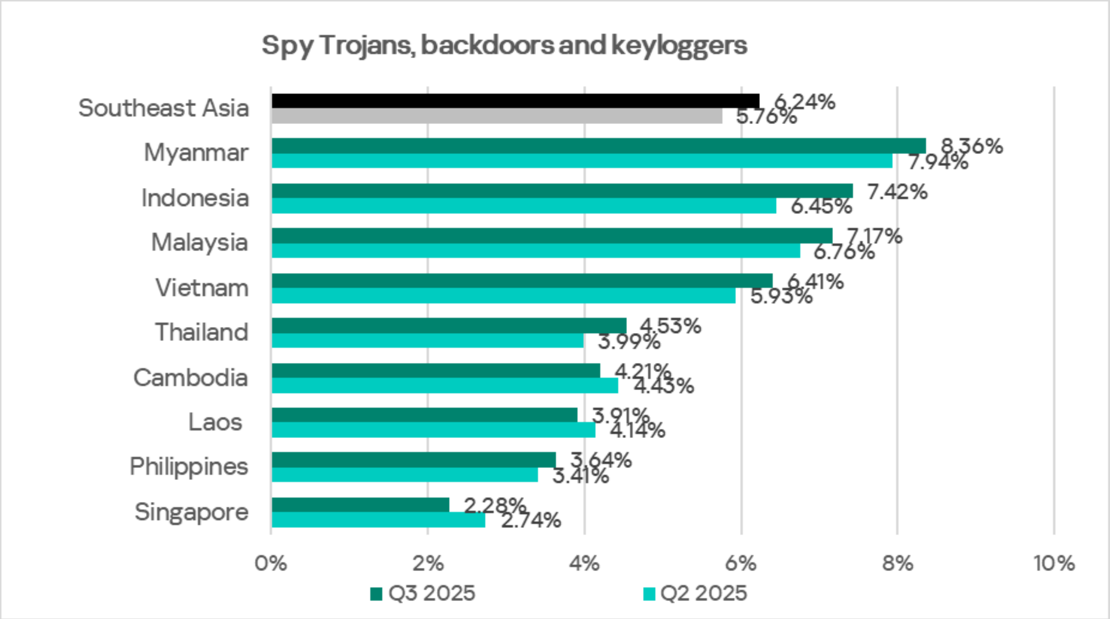
Out of all the threat categories over the quarter, the figures increased for spyware, viruses, and worms.

Spyware

In the rankings of regions for the percentage of ICS computers on which spyware was blocked, Southeast Asia jumped up one position to take second place with 6.24% in Q3 2025. This figure is 4.5 times higher than in Northern Europe, which has the lowest percentage value.



Among countries of the region, Myanmar leads in the percentage of ICS computers on which spyware was blocked with 8.36%. Singapore has the lowest rate at 2.28%. This indicator increased in all countries except Singapore, Laos, and Cambodia.

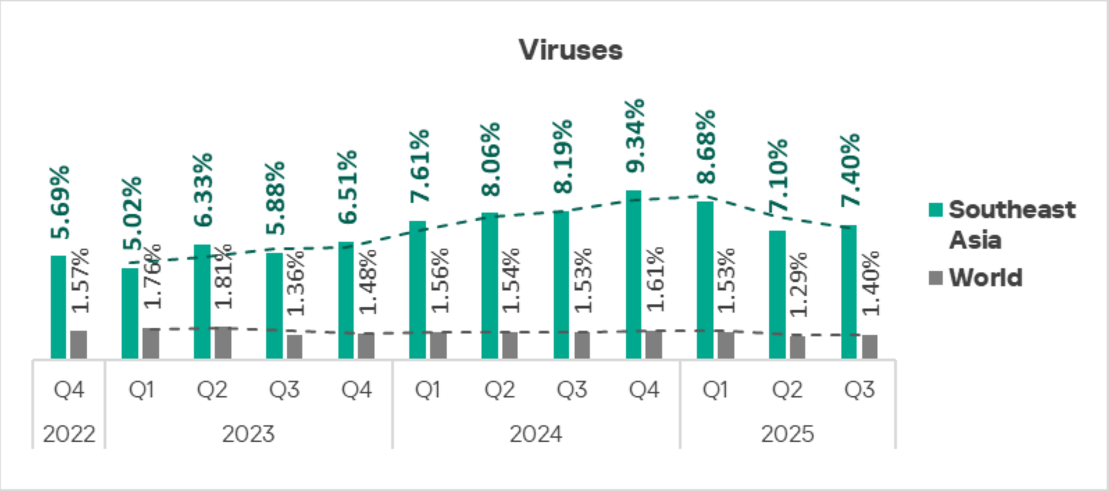


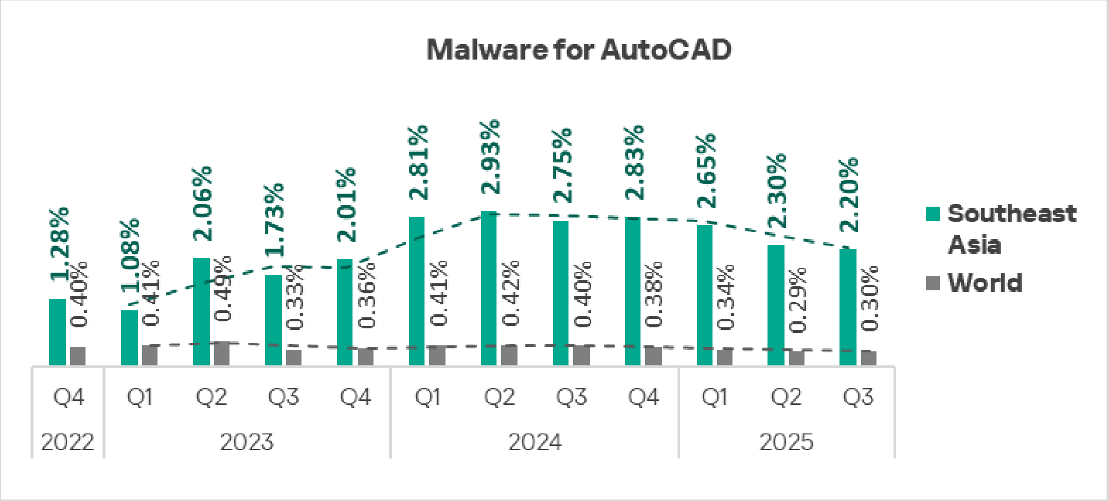
Although spyware is blocked in the region across all sources of threats, email is its main distribution channel. Malaysia, Indonesia, and Vietnam, which follow Myanmar in the ranking for spyware, are also the top three countries in the region for threats from email clients. However, in Myanmar the situation is different. Myanmar ranks 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.

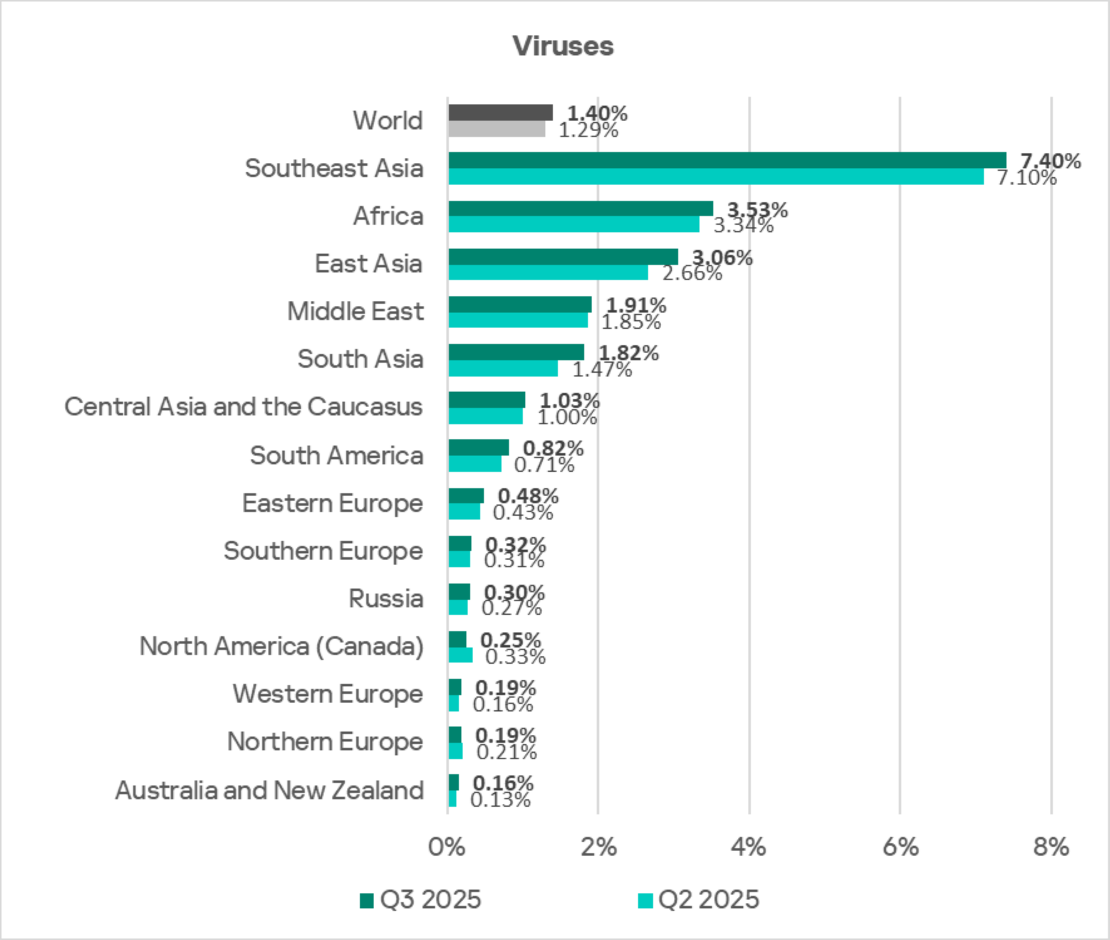
The indicators of both categories noticeably grew in 2024, but in 2025 they are lower than they were a year ago.





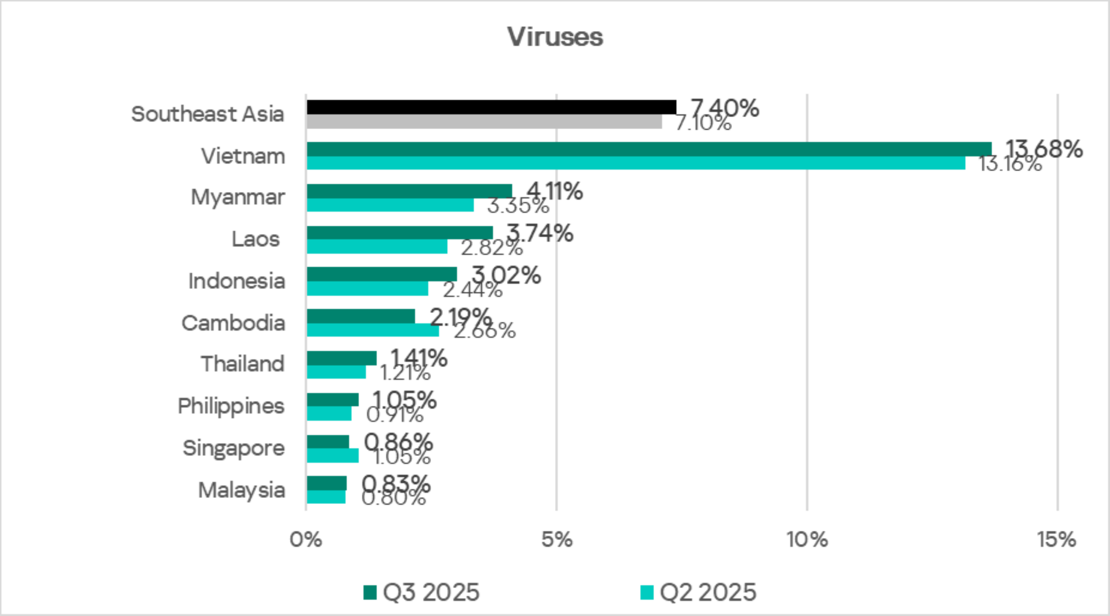
Viruses

In terms of the percentage of ICS computers attacked by viruses, Southeast Asia leads the regional ranking by a huge margin.



The figure in Southeast Asia is 2.1 times higher than in Africa (the next-ranked region), while it's 46.3 times higher than the lowest-ranked Australia and New Zealand region.

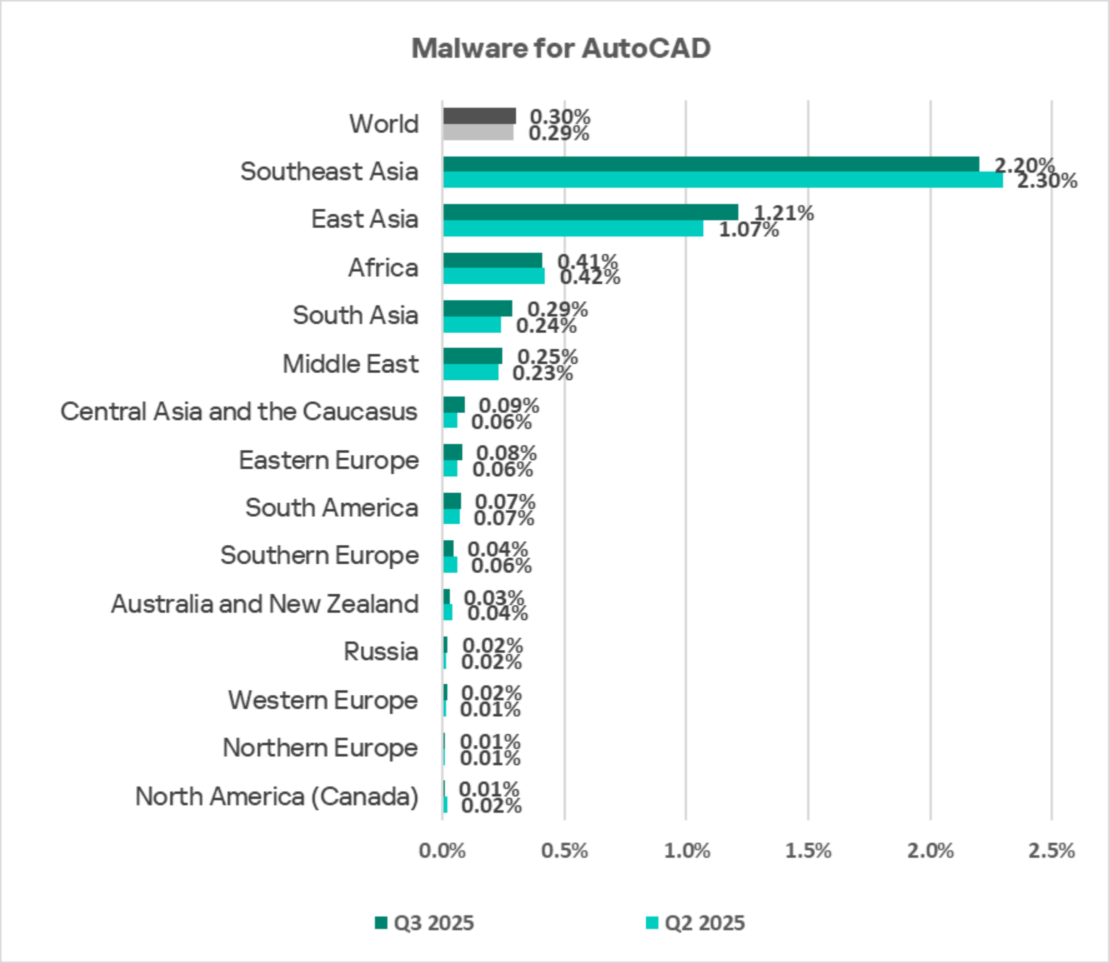
Such a strong lead for Southeast Asia was provided by Vietnam with its 13.6%. In this country, the indicator is 3.3 times higher than next-ranked Myanmar.



In the region, viruses are blocked across all sources of threats. We should note that Vietnam ranks second among countries of the region based on the percentage of ICS computers on which internet threats and network folder threats were blocked, and it ranks third in mail client threats and removable media threats.

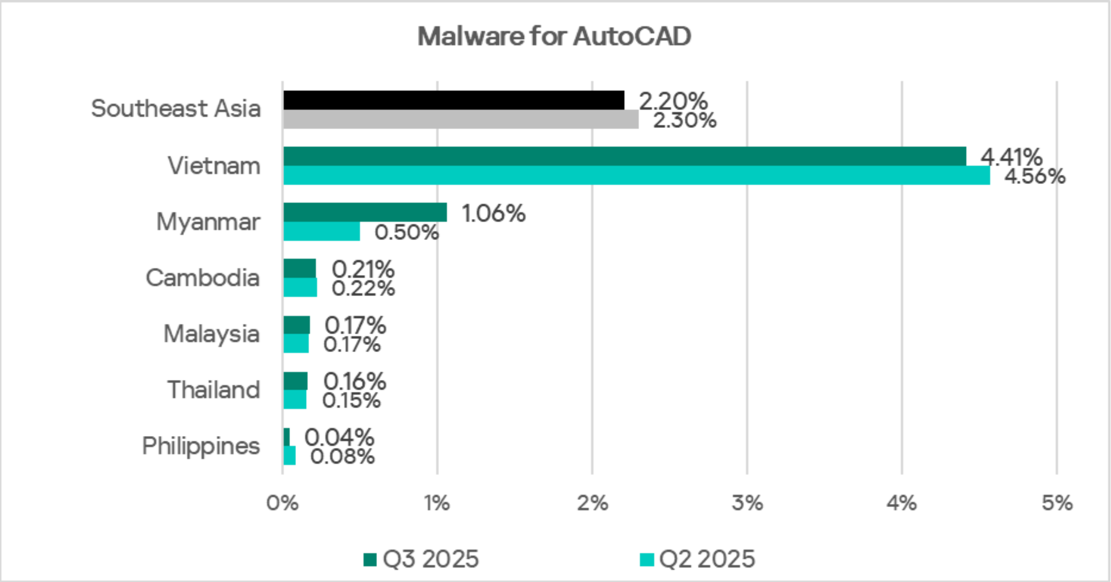
Malware for AutoCAD

In terms of the percentage of ICS computers on which malware for AutoCAD was blocked, Southeast Asia also leads the corresponding ranking of regions by a wide margin.



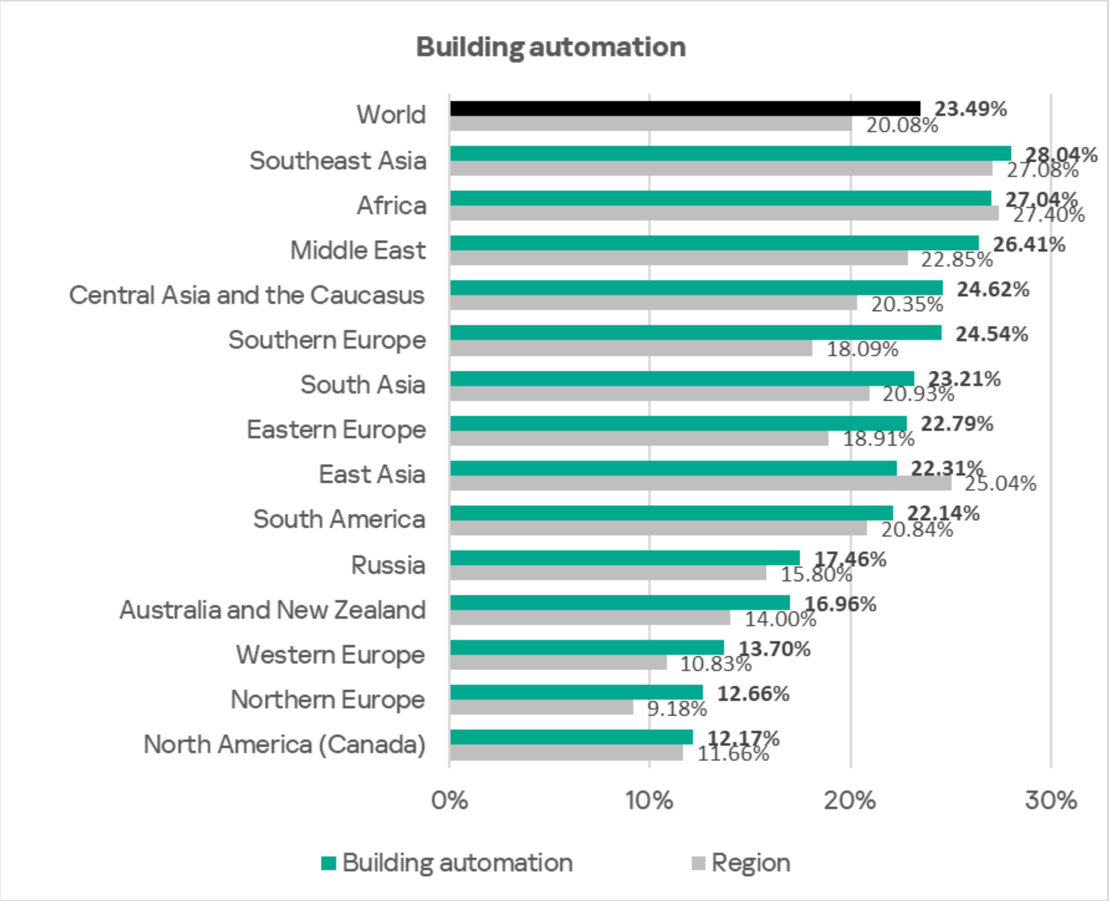
In Southeast Asia, this figure is 220 times (!) higher than the lowest among the regions, North America (Canada).

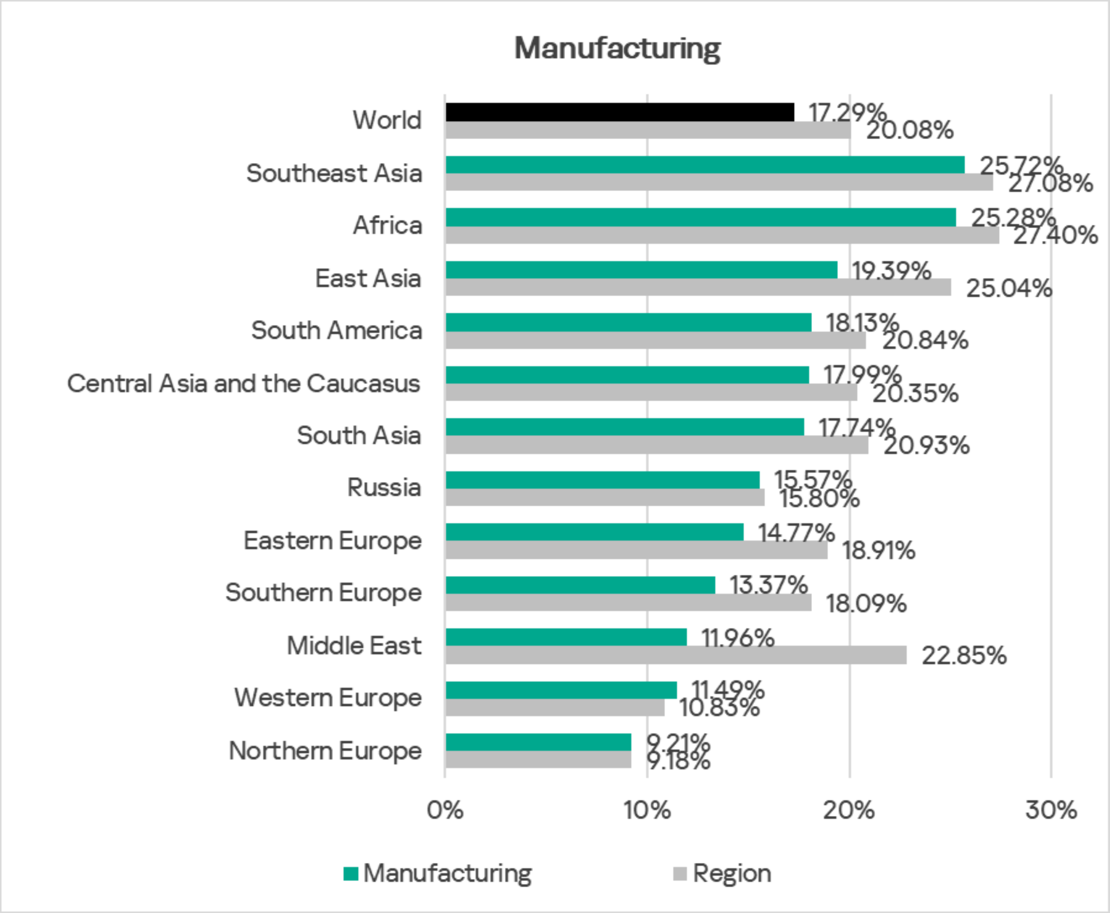
The leading position in the percentage of ICS computers on which malware for AutoCAD was blocked is held by this region again thanks to Vietnam, which has an enormous figure for this category at 4.41%.



Industries

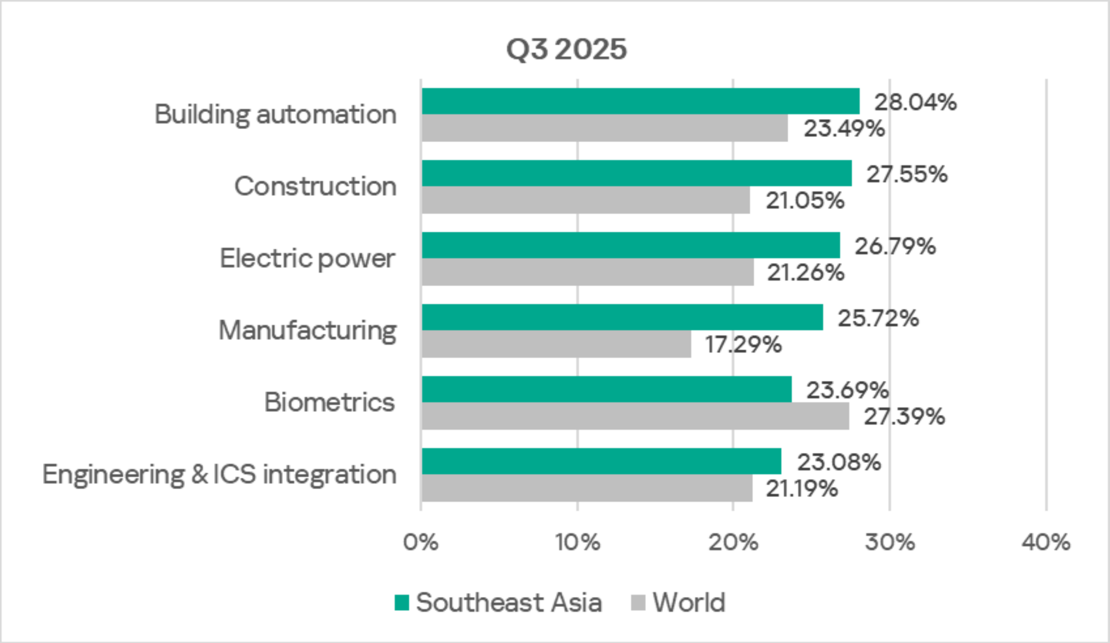
In Q3 2025, Southeast Asia leads among regions for the percentage of ICS computers on which malicious objects were blocked in the building automation and manufacturing industries.


Building automation
World
23.49%
20.08%
Southeast Asia
28.04%
27.08%
Africa
27.04%
27.40%
Middle East
26.41%
22.85%
Central Asia and the Caucasus
24.62%
20.35%
Southern Europe
24.54%
18.09%
South Asia
23.21%
20.93%
Eastern Europe
22.79%
18.91%
East Asia
22.31%
25.04%
South America
22.14%
20.84%
Russia
17.46%
15.80%
Australia and New Zealand
16.96%
14.00%
Western Europe
13.70%
10.83%
Northern Europe
12.66%
9.18%
North America (Canada)
12.17%
11.66%
0%
10%
20%
30%
Building automation
Region



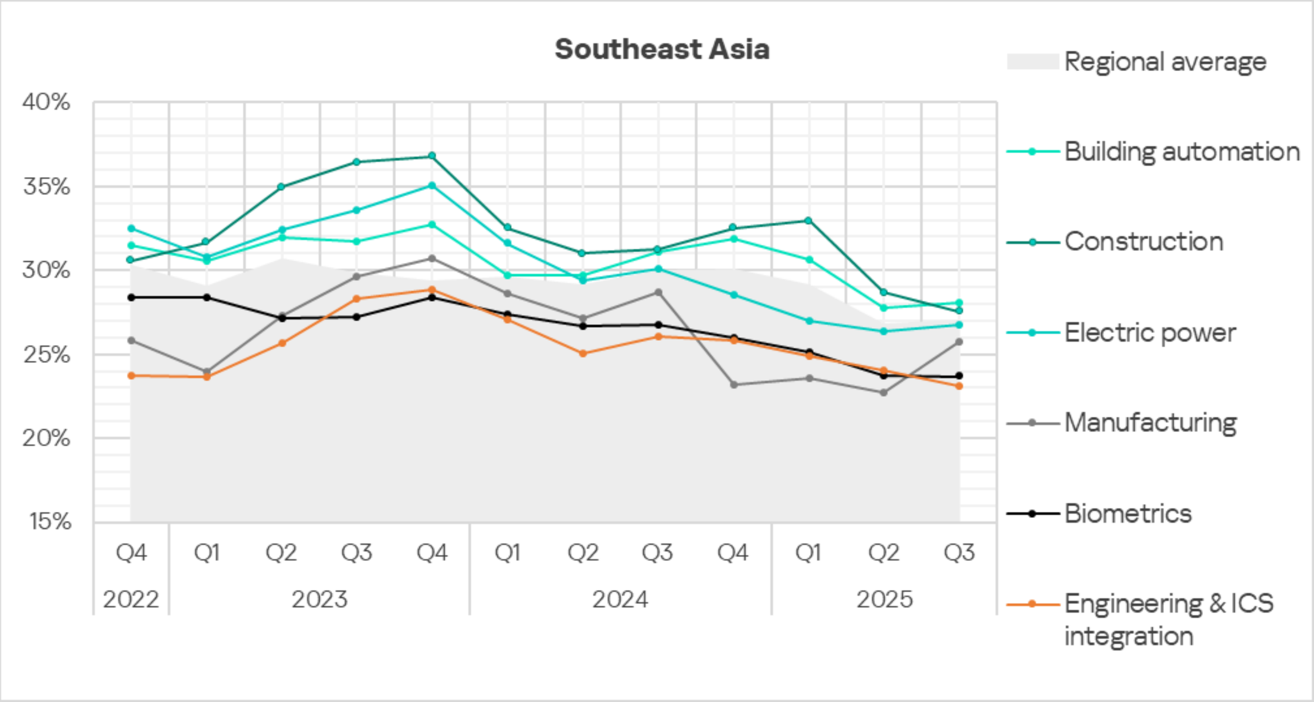
In Q3 2025, among all industries under review in the report, the building automation industry overtook the construction industry in the percentage of ICS computers on which malicious objects were blocked in Southeast Asia.

In this region, the figures for all industries exceed their respective global averages. The biggest difference is seen in the manufacturing industry, which is higher by a factor of 1.5.



The indicators for the building automation, electrical energy, and manufacturing industries increased over the quarter. The manufacturing industry showed the biggest increase.

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. The color red signifies that the figure approaches the maximum.

Threat source indicators for industries in Southeast Asia, Q3 2025

Industry / Threat source	Biometrics	Building automation	Electric power	Engineering & ICS integration	Oil & gas	Construction	Manufacturing	Threat category total in the region
Internet	8.47%	9.97%	11.61%	10.67%	12.66%	9.40%	9.76%	10.02%
Email clients	8.24%	6.65%	2.50%	4.13%	3.60%	6.27%	5.52%	4.69%
Removable media	0.56%	0.50%	0.55%	0.42%	0.32%	0.65%	0.42%	0.53%
Network folders	0.05%	0.09%	0.03%	0.05%	0.12%	0.00%	0.00%	0.10%
Industry total in the region	23.69%	28.04%	26.79%	23.08%	21.78%	27.55%	25.72%	

Threat category indicators for industries in Southeast Asia, Q3 2025

Industry / Threat category	Biometrics	Building automation	Electric power	Engineering & ICS integration	Oil & gas	Construction	Manufacturing	Threat category total in the region
Denylisted internet resources	3.35%	4.10%	5.81%	4.93%	5.69%	4.08%	4.81%	4.42%
Malicious scripts and phishing pages (JS and HTML)	10.08%	9.47%	8.20%	7.86%	8.54%	9.34%	7.07%	8.02%
Spy Trojans, backdoors and keyloggers	8.93%	8.10%	5.68%	5.36%	5.52%	6.74%	5.09%	6.24%
Worms	2.00%	1.61%	2.50%	1.25%	1.14%	2.37%	0.71%	1.72%
Miners in the form of executable files for Windows	0.61%	0.46%	0.83%	0.44%	0.71%	0.53%	0.28%	0.41%
Malicious documents (MSOffice + PDF)	4.20%	3.36%	1.85%	1.90%	2.41%	2.60%	1.56%	2.36%
Viruses	2.66%	6.66%	6.14%	3.34%	7.47%	4.08%	3.54%	7.40%
Ransomware	0.28%	0.18%	0.29%	0.08%	0.19%	0.30%	0.42%	0.12%
Web miners running in browsers	0.59%	0.40%	0.68%	0.40%	0.73%	0.53%	0.14%	0.35%
Malware for AutoCAD	0.26%	0.79%	1.38%	1.02%	4.67%	0.59%	0.99%	2.20%
Industry total in the region	23.69%	28.04%	26.79%	23.08%	21.78%	27.55%	25.72%	

Building automation

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

In the global rankings by industry in all regions, the building automation industry in Southeast Asia has the following rankings:

- Second place in the percentage of computers where viruses were blocked.

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

- Second place in the percentage of ICS computers on which threats were blocked when connecting removable media, and third place in network folder threats.
- First place in the percentage of ICS computers on which viruses are blocked.
- Second place in the following threat categories: spyware, web miners, and AutoCAD malware.

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

- Second place in the percentage of ICS computers on which threats in email clients and network folders were blocked.
- Second place in the following threat categories: malicious scripts and phishing pages, malicious documents, spyware, and viruses.

Construction

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

In the global rankings by industry in all regions, the construction industry in Southeast Asia has the following rankings:

- First place in internet threats.
- First place in the percentage of computers where viruses were blocked.
- Second place in the percentage of computers where malware for AutoCAD was blocked.
- Fourth place in the percentage of computers where web miners were blocked.

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

- First place in the percentage of ICS computers on which internet threats were blocked, and second place in network folder threats.
- First place in the percentage of ICS computers on which viruses are blocked.

- Second place in the following threat categories: denylisted internet resources, web miners, and malware for AutoCAD.

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

- First place in the percentage of ICS computers on which internet threats and network folder threats were blocked.
- First place in the following threat categories: viruses, malware for AutoCAD, and web miners.
- Second place in the following threat categories: denylisted internet resources and miners in the form of executable files for Windows.

Electric power

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

In the global rankings by industry in all regions, the electrical energy industry in Southeast Asia has the following rankings:

- Third place in the percentage of ICS computers on which viruses were blocked.
- Fifth place in internet threats.

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

- Second place in the percentage of ICS computers on which internet threats are blocked.
- First place in the percentage of ICS computers on which viruses are blocked.
- Second place in spyware and malware for AutoCAD, and third place for miners of both categories and denylisted internet resources.

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

- Second place in the percentage of ICS computers on which internet threats are blocked, and third place in removable media threats.
- First place in denylisted internet resources.
- Second place in the following threat categories: web miners, malware for AutoCAD, and ransomware.

Manufacturing

Southeast Asia leads among 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 has the following rankings:

- First place in the percentage of ICS computers on which threats in email clients are blocked, and second place in internet threats.
- First place in the percentage of ICS computers on which the following categories of threats are blocked: malicious scripts and phishing pages, spyware, viruses, and web miners.
- Second place in the following threat categories: malicious documents, ransomware, and malware for AutoCAD. The region also occupies third place in denylisted internet resources.

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

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

Biometric systems

Southeast Asia ranks seventh among regions based on the percentage of ICS computers on which malicious objects were blocked in OT infrastructure for biometric systems.

Based on indicators for OT infrastructure for biometric systems among regions, Southeast Asia has the following rankings:

- Third place in the percentage of ICS computers on which email client threats are blocked.
- First place in the percentage of ICS computers on which web miners are blocked.
- Second place in the percentage of ICS computers on which malware for AutoCAD is blocked, and third place in malicious documents and spyware.

The regional industry rankings for OT infrastructure for biometric systems is as follows:

- First place in the percentage of ICS computers on which email client threats were blocked.
- Second place in removable media, and third place in network folder threats.

- First place in the following threat categories: malicious scripts and phishing pages, malicious documents, and spyware.
- Third place in ransomware, worms, and miners of both categories.

Engineering and ICS integrators

Southeast Asia ranks third 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 has the following rankings:

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

Among industries in the region, engineering and ICS integrators have the following rankings:

- Third place in internet threats.
- Third place in the following threat categories: denylisted internet resources and 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 previous quarter, this threat category even ranked first among all malware categories in the percentage of ICS computers on which it was blocked.

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 ranks 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 rank 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 ranks third.

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

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 ranks second among regions, behind only Africa. Worms are the most frequently blocked threat on removable media in the region. Removable media also carry spyware and viruses.

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

By the percentage of ICS computers on which threats were blocked across industries globally, East Asia led all regions in Q3 2025 in the electrical energy (30.01%) and engineering and ICS integrator sectors (29.31%). In the manufacturing 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.

Striking differences among countries in the region

The cybersecurity situation differs significantly across countries and territories in the region. This is particularly evident in how sources of blocked malicious objects on ICS computers rank differently between countries:

- Macau and Hong Kong lead in threats from the internet.
- Taiwan and Hong Kong lead in email threats.
- Mainland China leads in removable media and network folder threats, driving the region's high rates of viruses and malware for AutoCAD.

In terms of threat category rankings, Hong Kong leads in threats spread via the internet and email (denylisted resources and malicious documents). Mongolia typically leads in miners, while Macau leads in ransomware.

In all the other threat categories, Mainland China holds the top spot.

Japan consistently ranks last in most categories.

Quarter highlights

In Q3 2025, the region saw a sharp increase in the percentage of ICS computers on which malicious scripts and phishing pages were blocked. This surge pushed

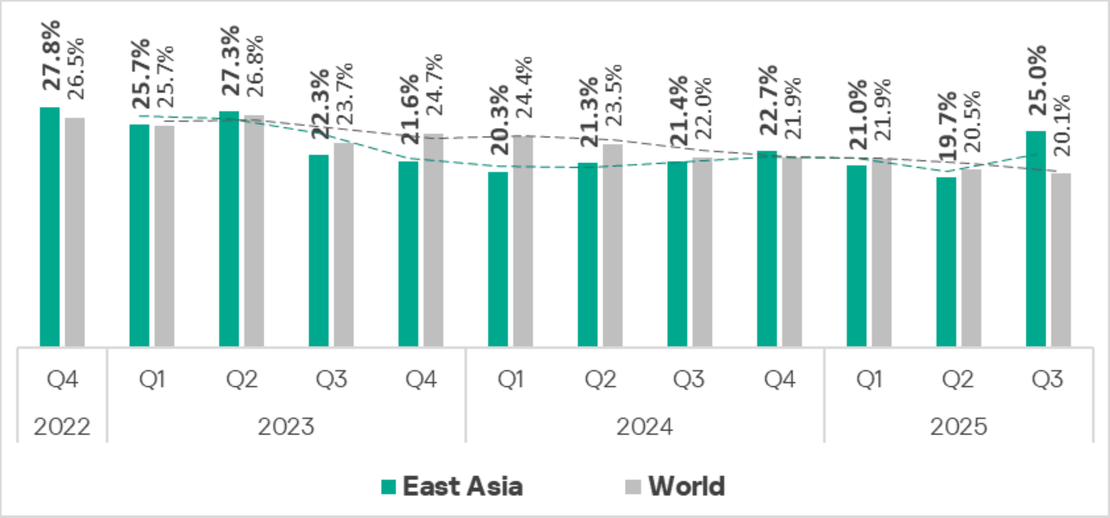
East Asia from seventh to third place in the global ranking of ICS computers where malicious objects were blocked.

The spike is linked to a rise in blocked malicious scripts on ICS computers in the engineering and ICS integrators sector in Mainland China. Malware was found in the memory and folders of customized Torrent and MediaGet client applications. The detected malicious scripts were designed to steal system information. The spread of these scripts is likely tied to advertising integrations in various applications; for example, some alternative installation packages may include additional, undisclosed applications alongside the intended one.

These scripts were blocked only after being detected in decrypted form on the disk and in memory post-infection, so the exact source remains unknown. As a result, the dramatic rise in the percentage of attacked ICS computers in East Asia did not affect the region's rankings for threat sources.

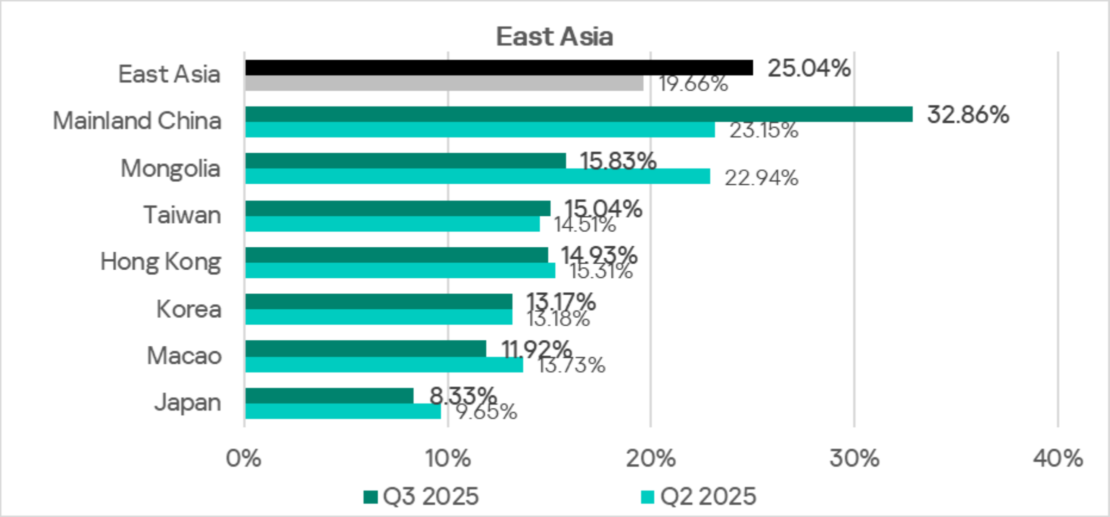
Statistics across all threats

In Q3 2025, East Asia rose from seventh to third place globally in terms of the percentage of ICS computers on which malicious objects were blocked. The region's figure increased 1.3 times – from 19.7% to 25.0%. This is 2.7 times higher than the lowest-ranking region, Northern Europe.



In terms of quarter-on-quarter growth (5.3 p.p.), East Asia leads all other regions by a wide margin.

Across the region's countries and territories, rates range from 8.33% in Japan to 32.86% in Mainland China.

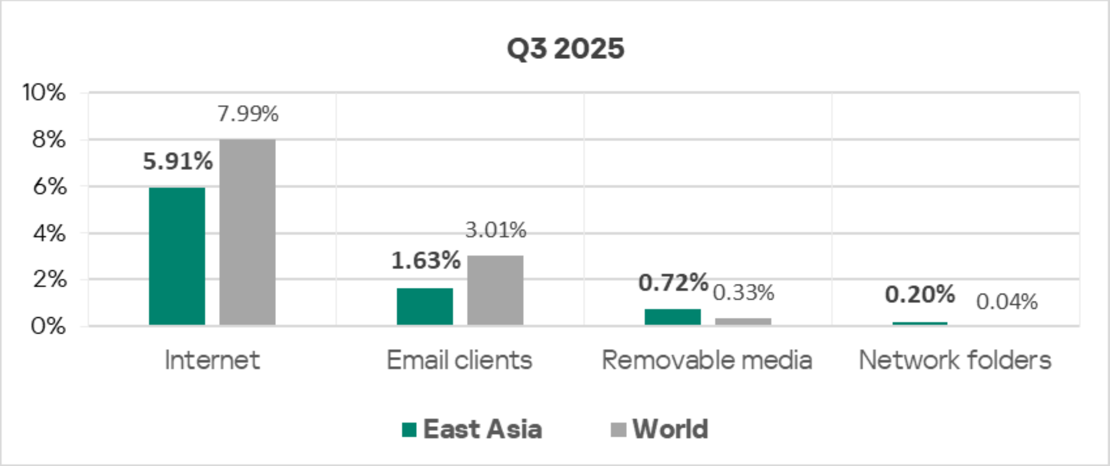


In this quarter, these figures increased only in Mainland China and Taiwan. But while Taiwan's quarter-on-quarter change was 0.53 p.p., Mainland China showed an unusually high 9.71 p.p. – meaning that the region's overall growth was driven primarily by Mainland China. As noted above, this rise is linked to the spread of malicious scripts in the engineering and ICS integrators sector.

Threat sources

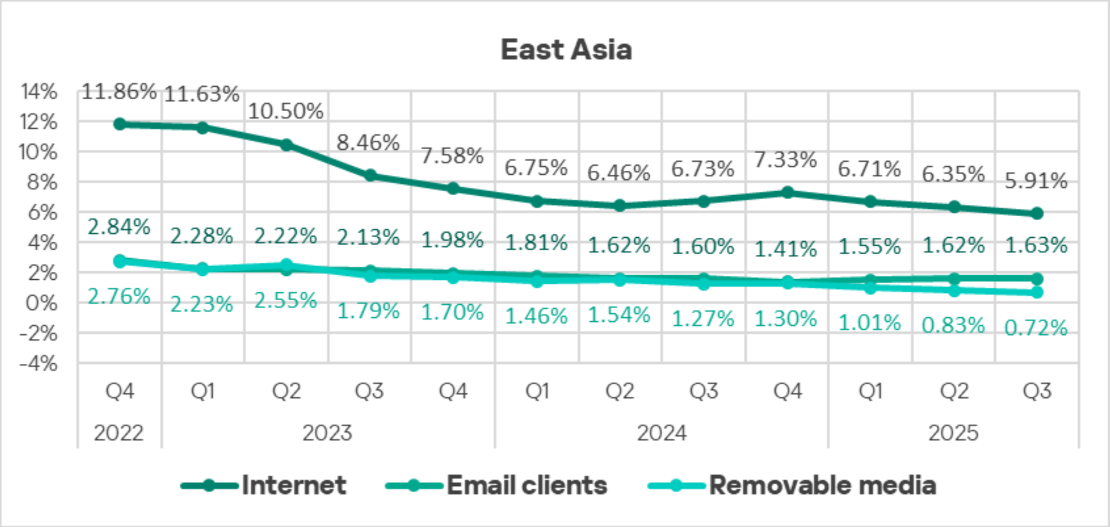
In Q3 2025, East Asia exceeded the global averages for two threat sources:

- Removable media: by 2.2 times, second place globally.
- Network folders: by 5.0 times, ranking first globally.



The percentage of ICS computers with blocked malicious objects decreased for all threat sources except mail clients, where the value increased by a negligible 0.01 p.p.

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

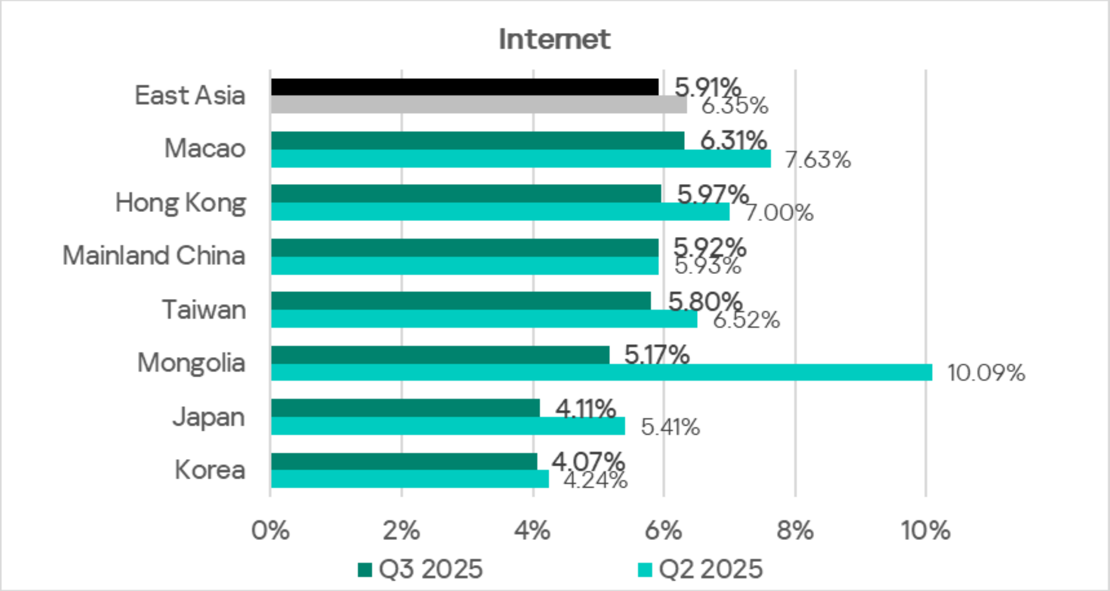


Internet

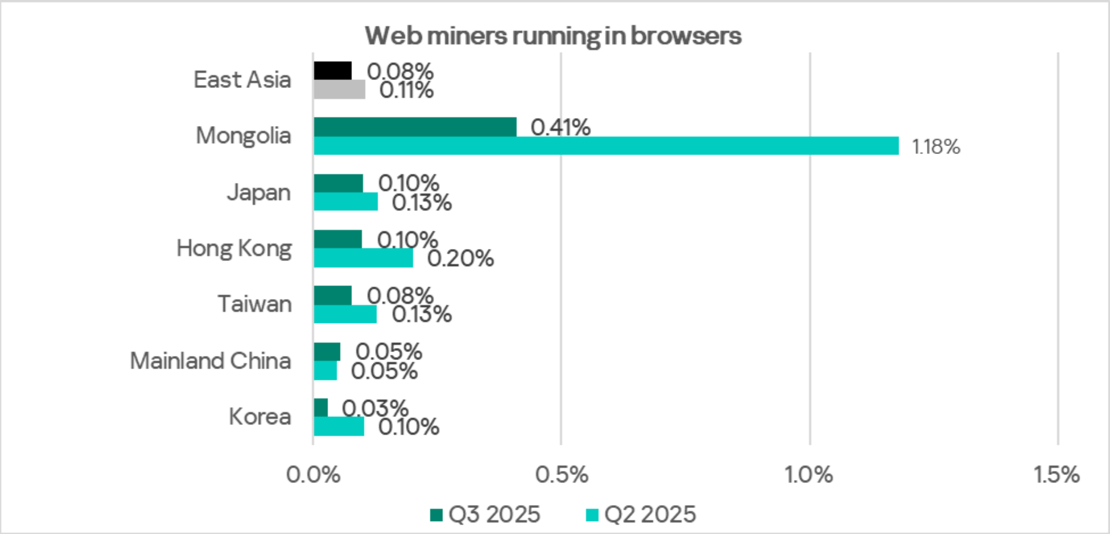
In terms of the percentage of ICS computers on which internet threats are blocked, East Asia placed 12th among regions.

The indicator for internet threats has been falling for the third straight quarter and has reached its lowest level in the past three years – 5.91%. This is 1.3 times higher than the lowest regional value, recorded in Northern Europe.

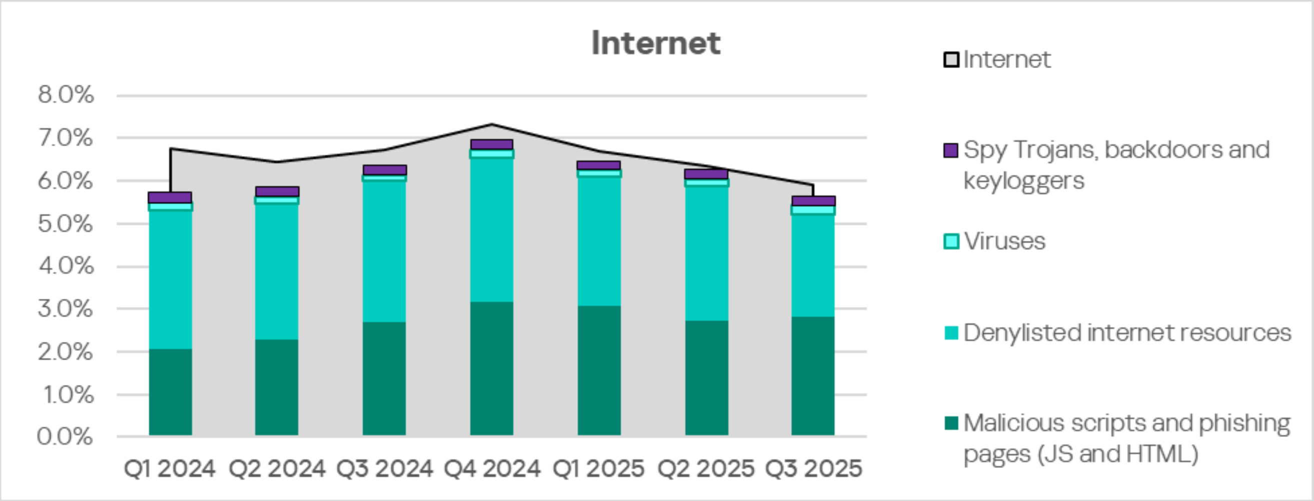
Across the region, the percentage of ICS computers blocking internet threats ranges from 4.07% in Korea to 6.31% in Macau.



In Mongolia – which led this ranking last quarter – the figure nearly halved, partly due to a sharp drop in the percentage of ICS computers blocking denylisted internet resources and web miners.



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

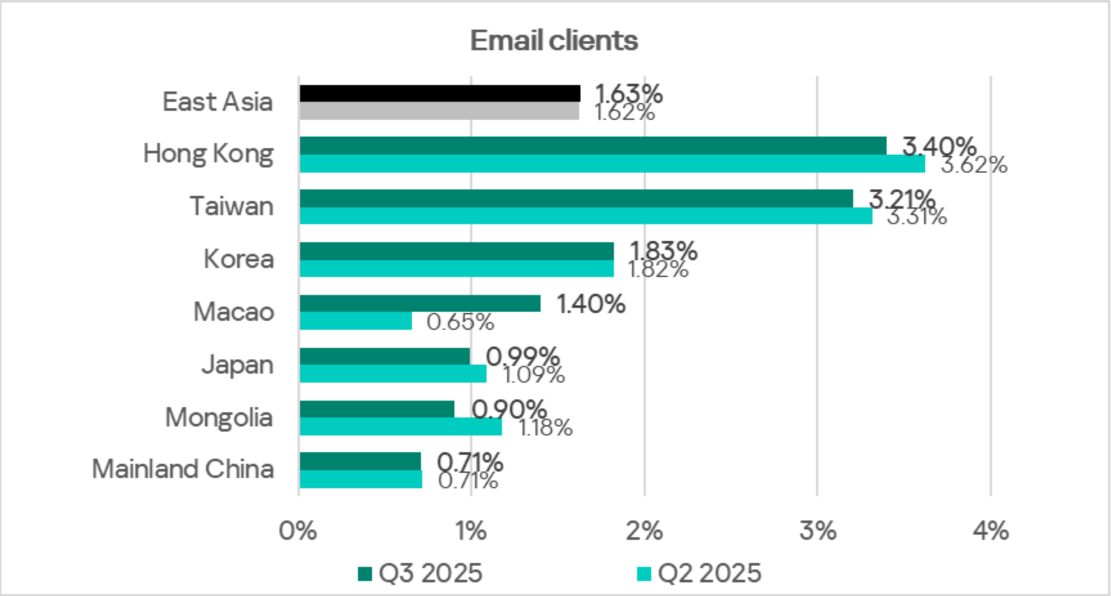


By the percentage of ICS computers on which denylisted internet resources were blocked, Hong Kong leads in the region.

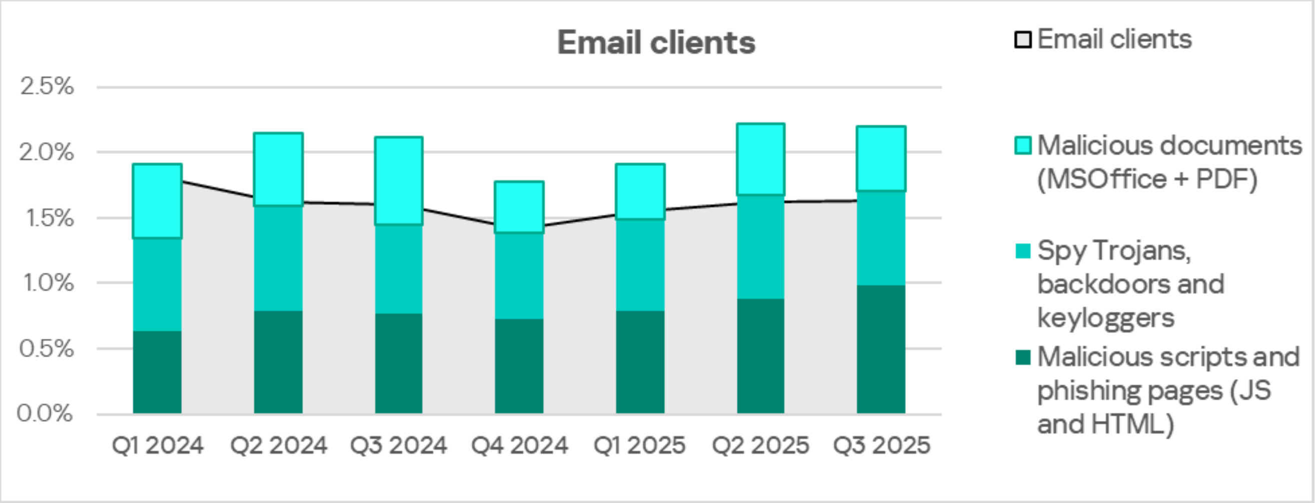
Email clients

In terms of ICS computers where mail client threats were blocked, East Asia ranks 11th globally with 1.63%. This is 2.1 times higher than in Russia, which has the lowest figure.

Among countries and territories in the region, Hong Kong (3.40%) and Taiwan (3.21%) lead. The lowest figure was recorded in Mainland China: 0.71%.



The main categories of mail client threats blocked on ICS computers are malicious documents, spyware, malicious scripts, and phishing pages. Spyware spreads through all threat sources, but email is the primary one.

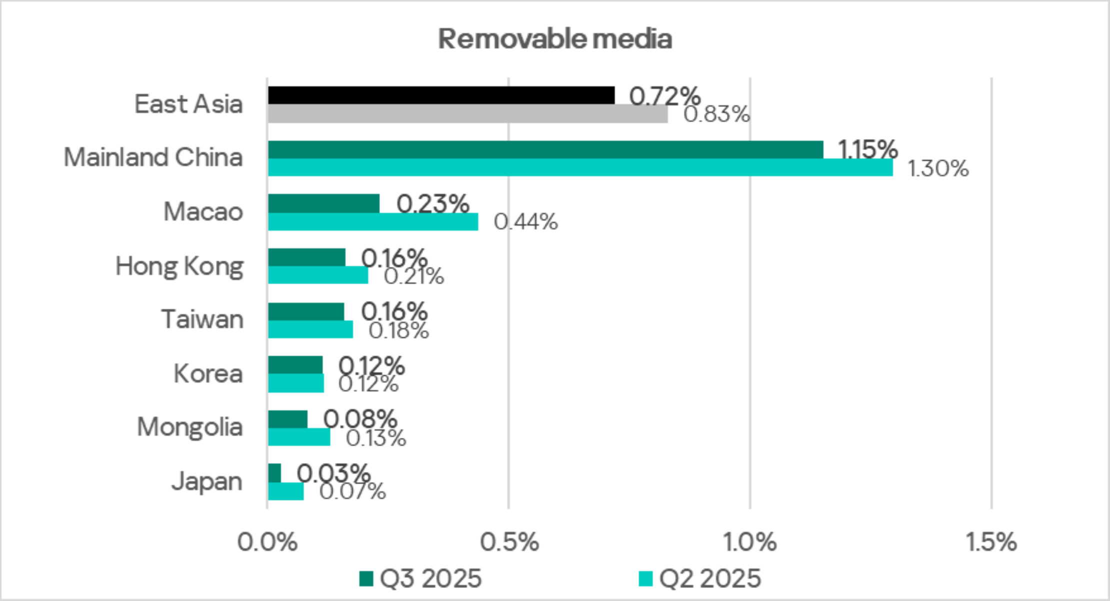


Hong Kong also leads in the threat category that spreads mainly via email – malicious documents. The indicator for this threat category has been steadily increasing in Hong Kong for a full year.

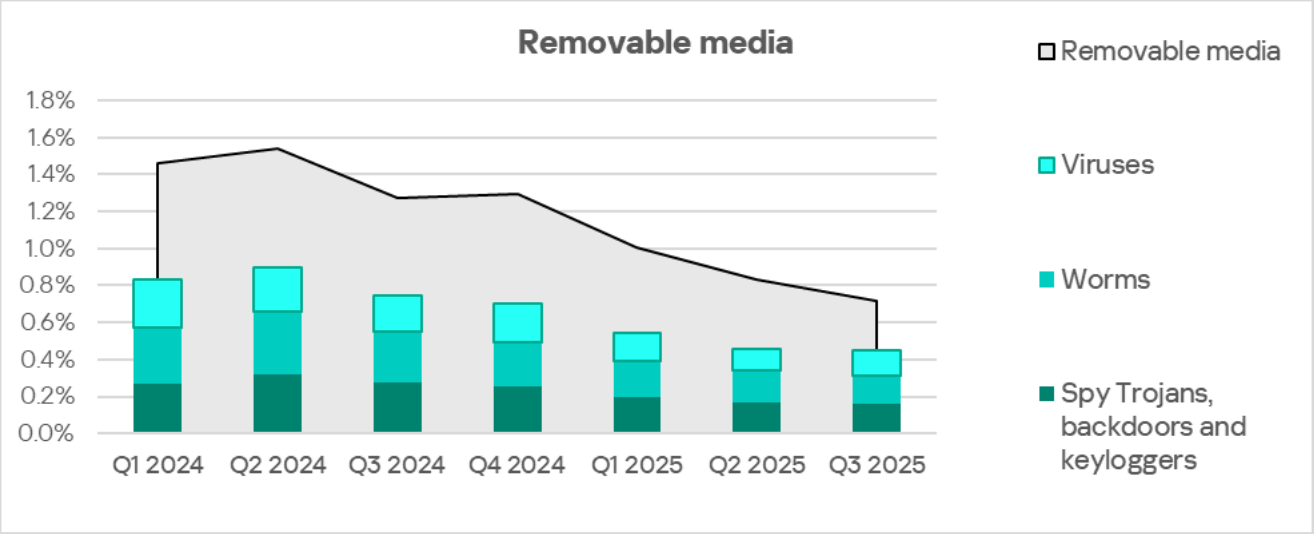
Removable media

By percentage of ICS computers on which removable media threats were blocked, East Asia ranks second among regions, behind only Africa. The regional figure (0.72%) is 14.4 times higher than that in Australia and New Zealand, which rank last.

Among the region's countries and territories, Mainland China leads by a significant margin with 1.15%. Other figures range from 0.03% in Japan to 0.23% in Macau.

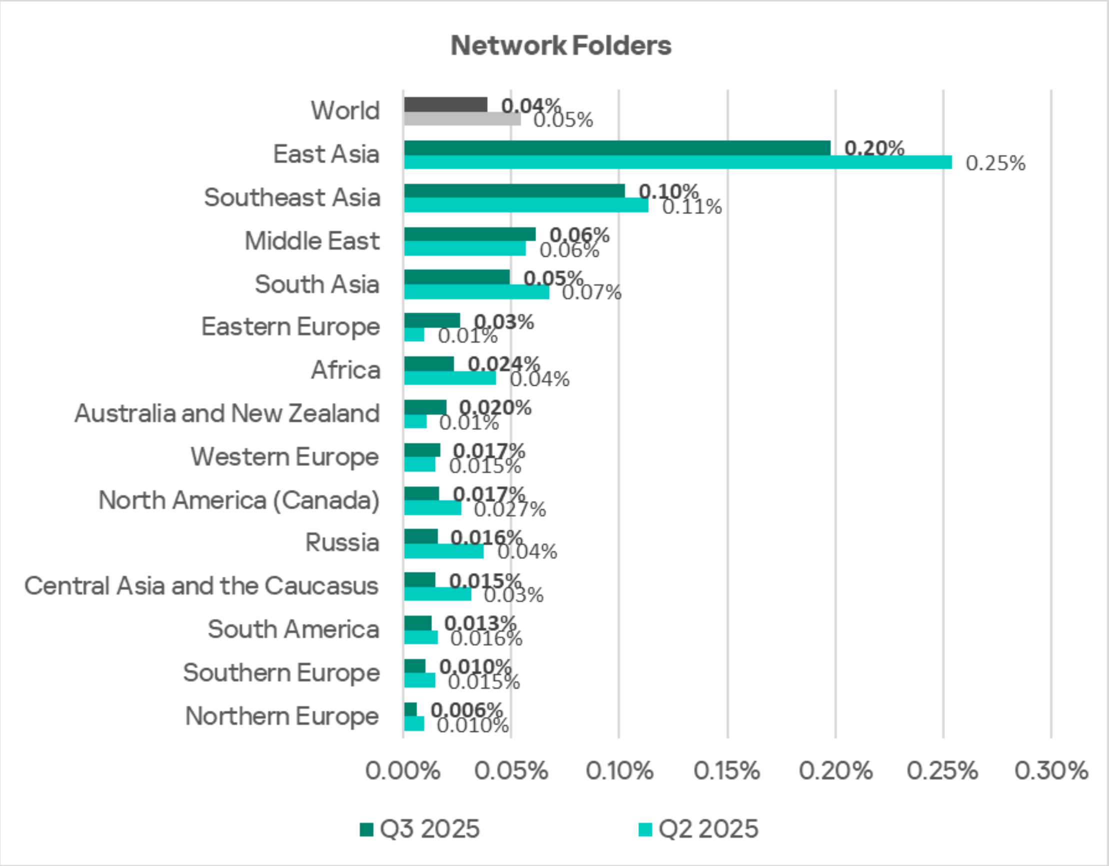


The main categories of threats blocked when connecting removable media to ICS computers are spyware, worms, and viruses. Notably, Mainland China leads the ranking in all these threat categories.

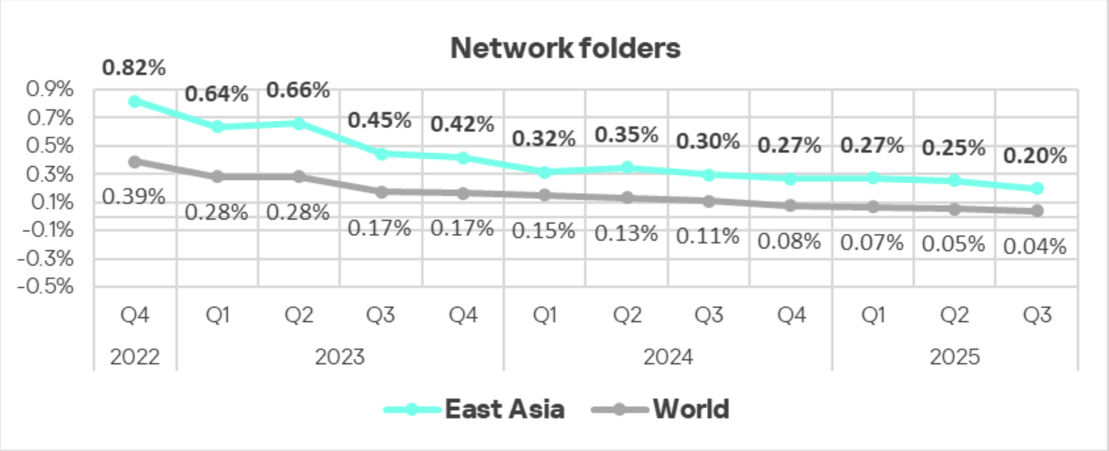


Network folders

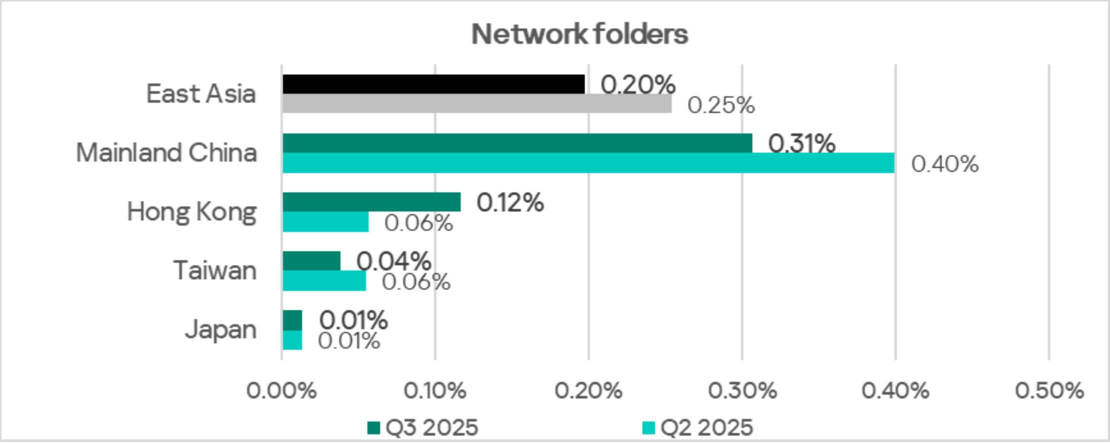
East Asia continues to rank first globally in the percentage of ICS computers on which network folder threats were blocked. In Q3 2025, the region's figure (0.20%) exceeded the global average by five times and was 33 times higher than in Northern Europe, which ranks lowest.



The percentage of ICS computers with threats blocked in network folders in East Asia shows a downward trend. The Q3 2025 figure was the lowest in three years.

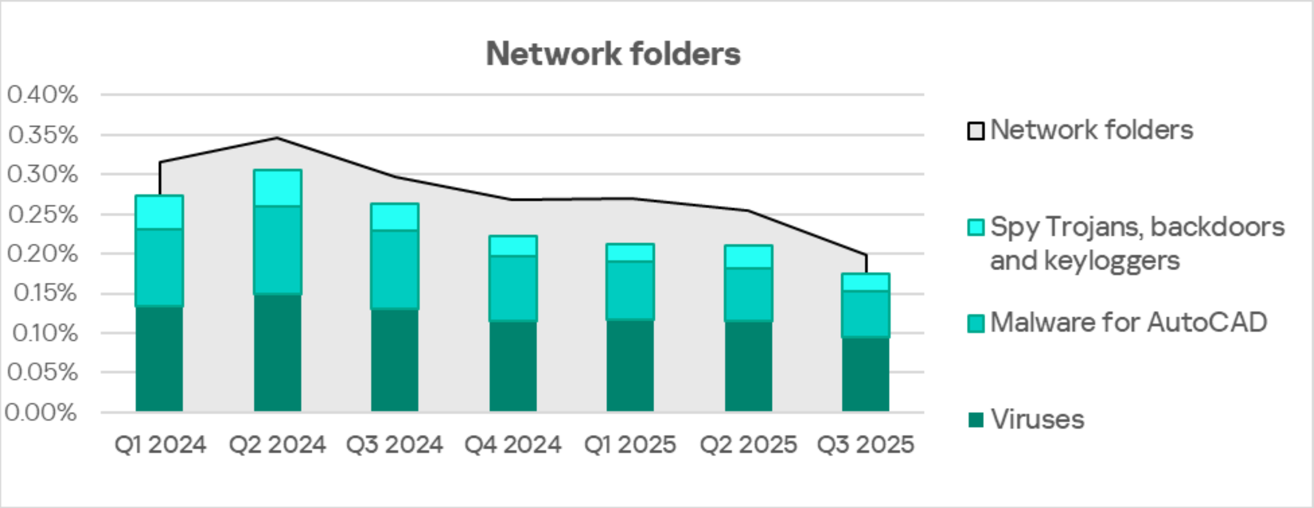


This trend is primarily driven by Mainland China, which dominates among other countries and territories in the region with 0.31%.



It should be noted that network folder threats were not detected in every country in the region.

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

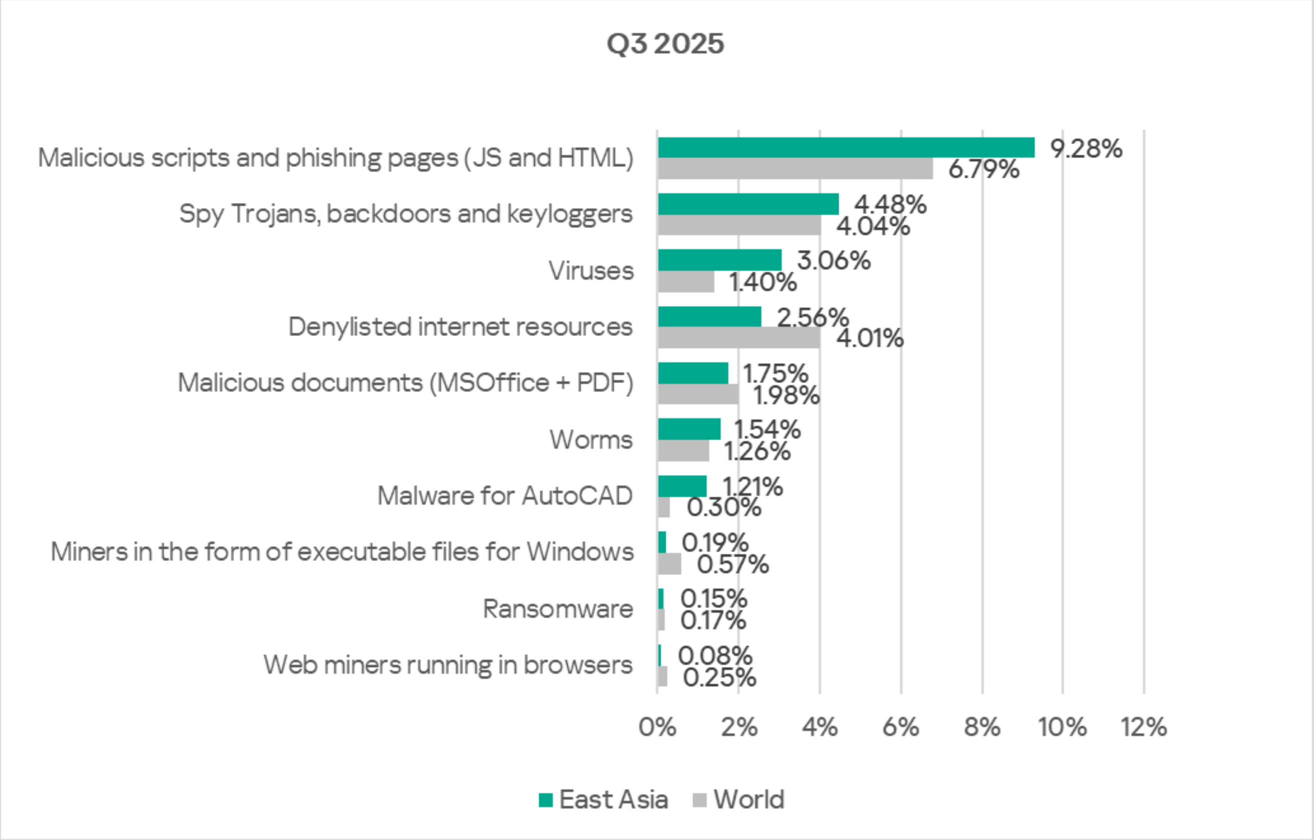


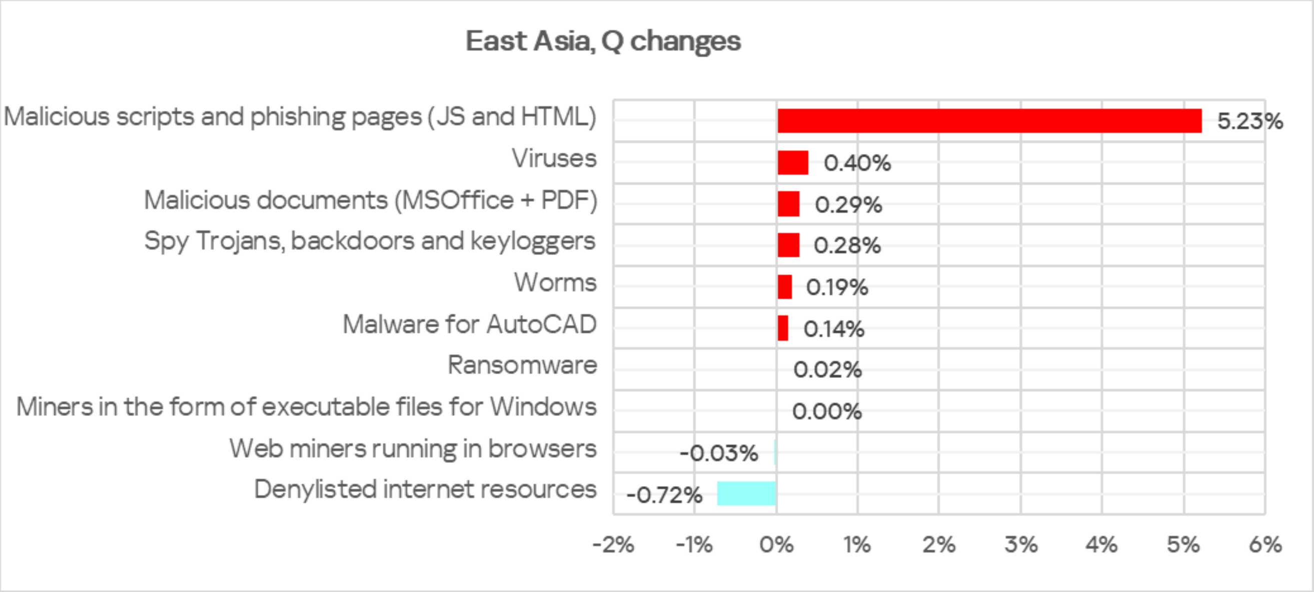
Viruses in the region spread through all threat sources, but mainly via the internet and removable media. However, the figure for network folders is also high, comparable to removable media.

By the percentage of ICS computers on which malware for AutoCAD is blocked, East Asia ranks second globally. For both viruses and malware for AutoCAD, Mainland China leads the region.

Threat categories

As in most regions, in Q3 2025 East Asia the most prevalent threat category found and blocked on ICS computers was malicious scripts and phishing pages, knocking spyware off the top spot. East Asia leads all regions in the increase of malicious scripts and phishing pages.





Compared with global averages, the region has higher percentages of ICS computers where the following were blocked:

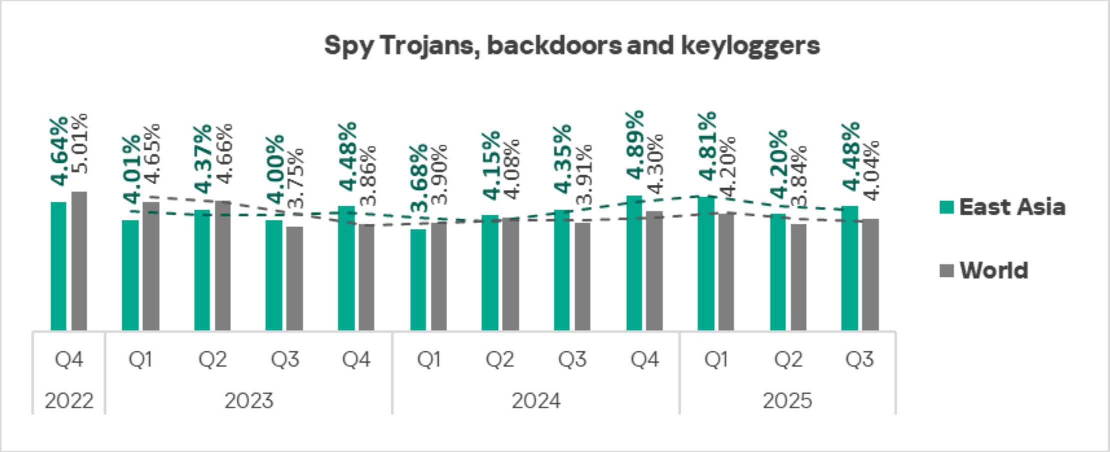
- Malicious scripts and phishing pages: 1.4 times higher, ranking second place globally.
- Spyware: 1.1 times higher.
- Worms: 1.2 times higher.
- Viruses: 2.2 times higher, third globally.
- Malware for AutoCAD: 4.0 times higher, second globally.

Spyware

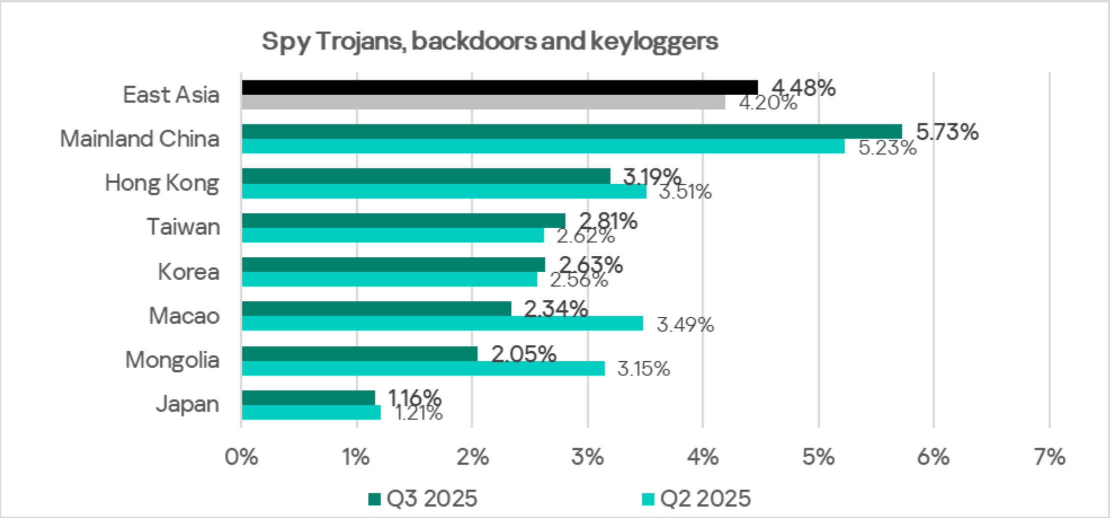
In the percentage of ICS computers on which spyware is blocked, East Asia ranks seventh globally.

The region's spyware rate is stable and relatively high; this category was the global leader last quarter.

The previous two quarters showed a decline in this indicator. In Q3 2025 it rose to 4.48%. This is 3.2 times higher than Northern Europe, where the value is the lowest.



Among the region's countries and territories, Mainland China leads in the percentage of ICS computers with blocked spyware, at 5.73%. Japan has the lowest rate at 1.16%.



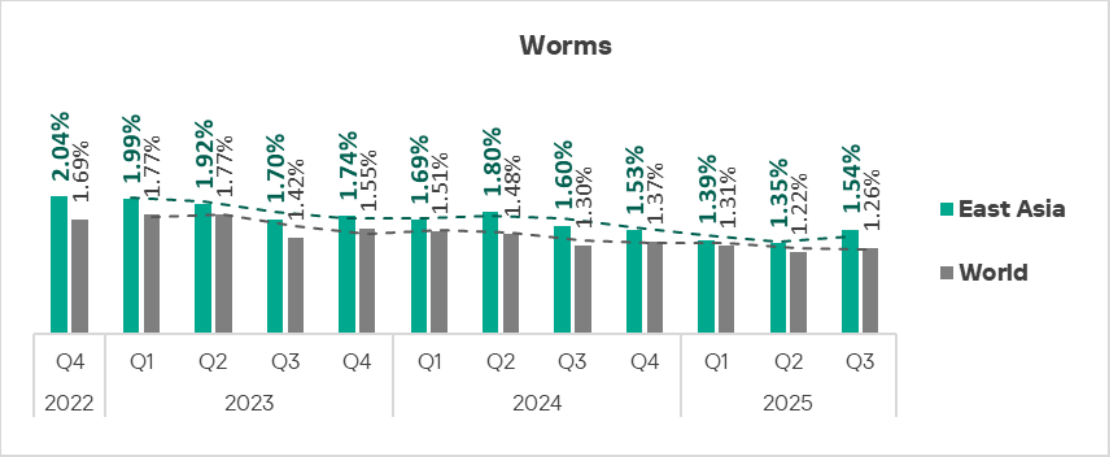
Spyware in the region spreads through all sources; in Q3 2025 mainly through email clients.

Mainland China, which leads in spyware, also ranks at the top in terms of blocked threats from removable media and network folders. Hong Kong and Taiwan lead in email-borne threats.

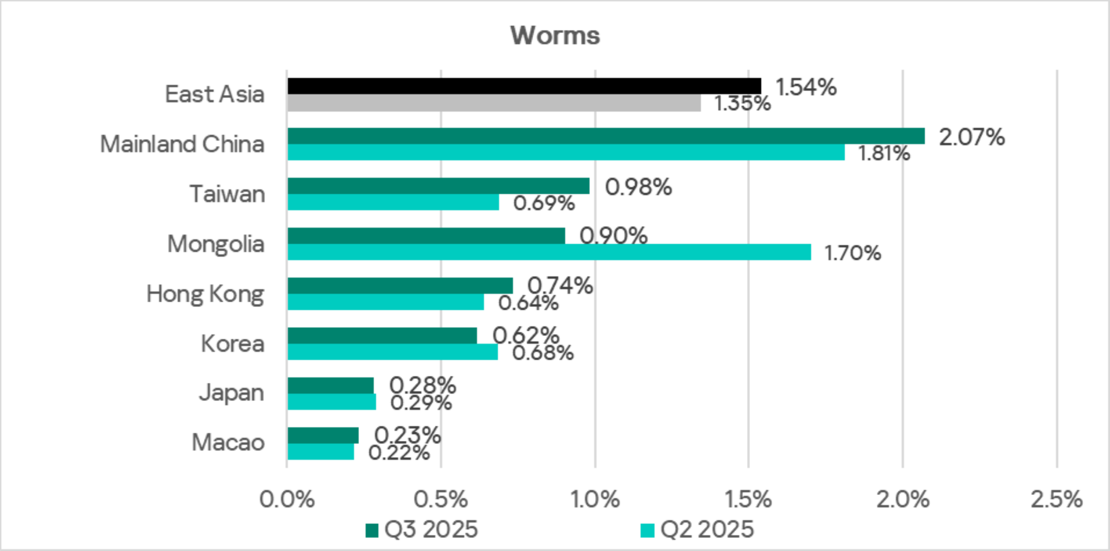
Worms

By the percentage of ICS computers with blocked worms, East Asia ranks fifth among regions, with 1.54%. This figure is 7.0 times higher than in Northern Europe, which boasts the lowest percentage among all regions.

The percentage of ICS computers on which worms are blocked in East Asia had declined for the previous three quarters, but in Q3 2025 it rose back to a level comparable to Q4 2024.



Among the region's countries and territories, Mainland China leads in the percentage of ICS computers with blocked worms, at 2.07%. In Mongolia – second place last quarter – the rate fell significantly.



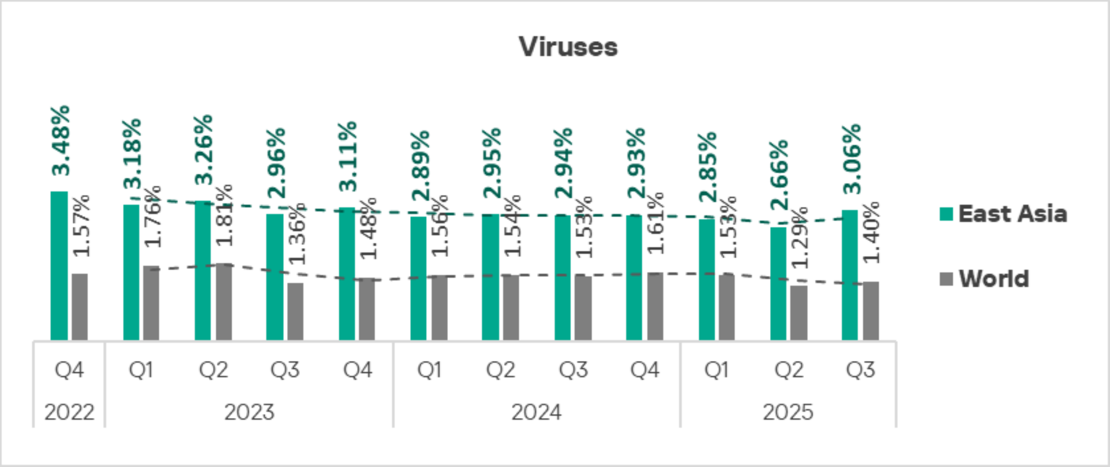
Worms spread through all threat sources, but mainly via removable media. Mainland China, the regional leader in worms, also ranks first in the percentage of ICS computers on which threats were blocked when connecting removable media.

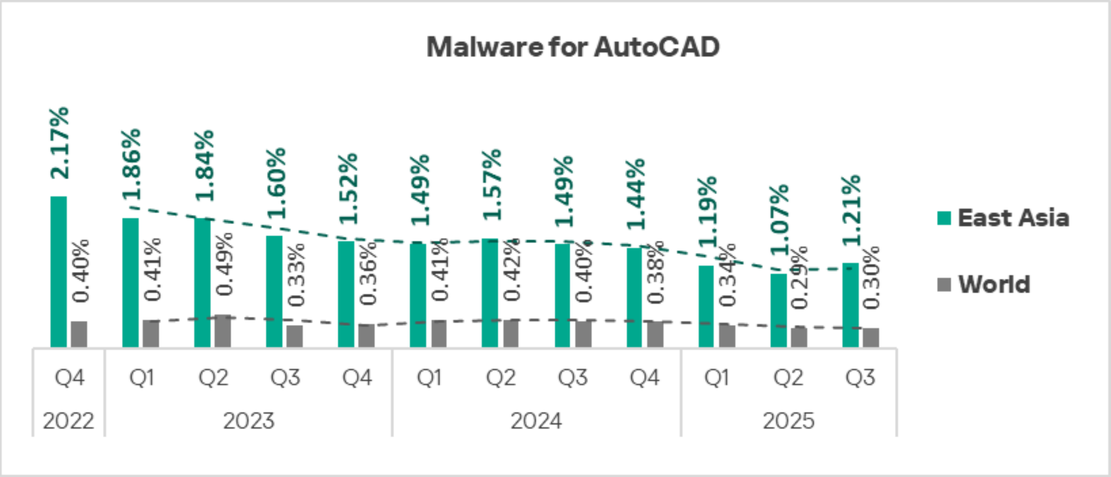
Viruses and malware for AutoCAD

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

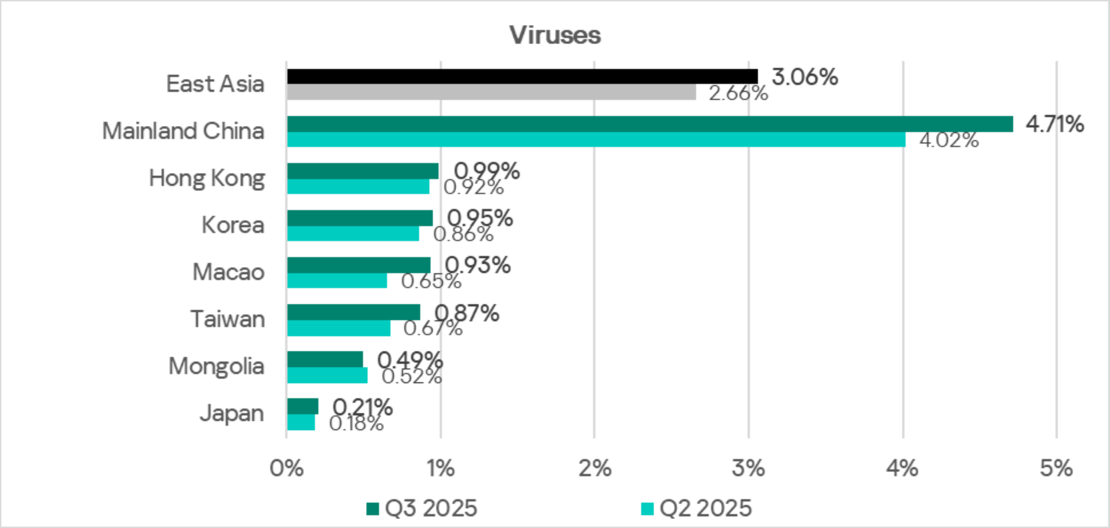
In both East and Southeast Asia, the situation with malware for AutoCAD is similar: in most cases, it spreads the same way as viruses. This explains the high percentage for this malware category.

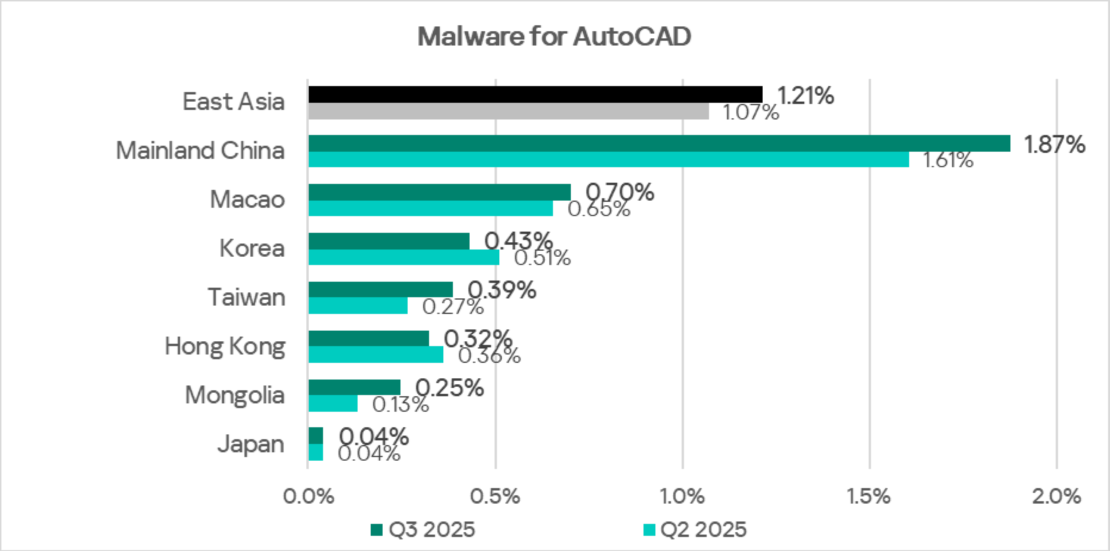
Both categories increased over the quarter.





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



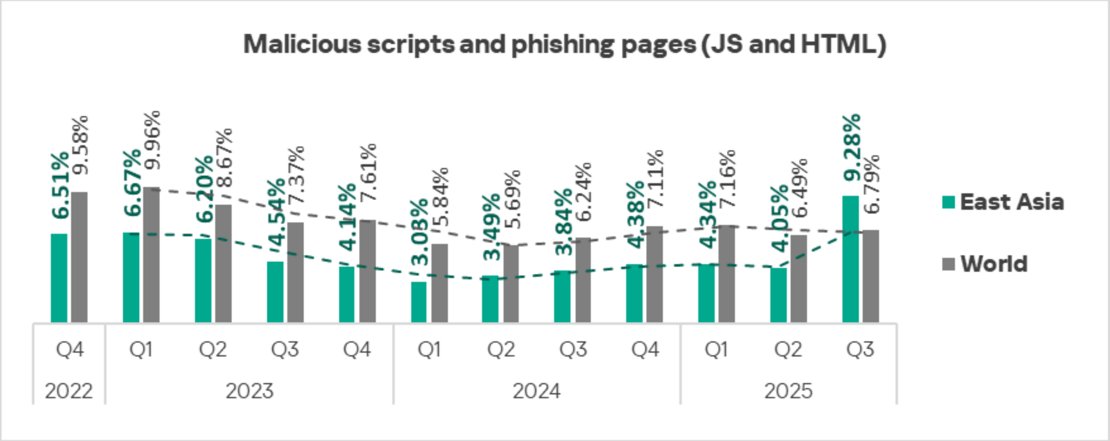


Viruses in the region spread via all threat sources. The top source is the internet, removable media ranks second, and the figure for network folders is comparable to email clients.

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

Threat of the quarter: malicious scripts and phishing pages

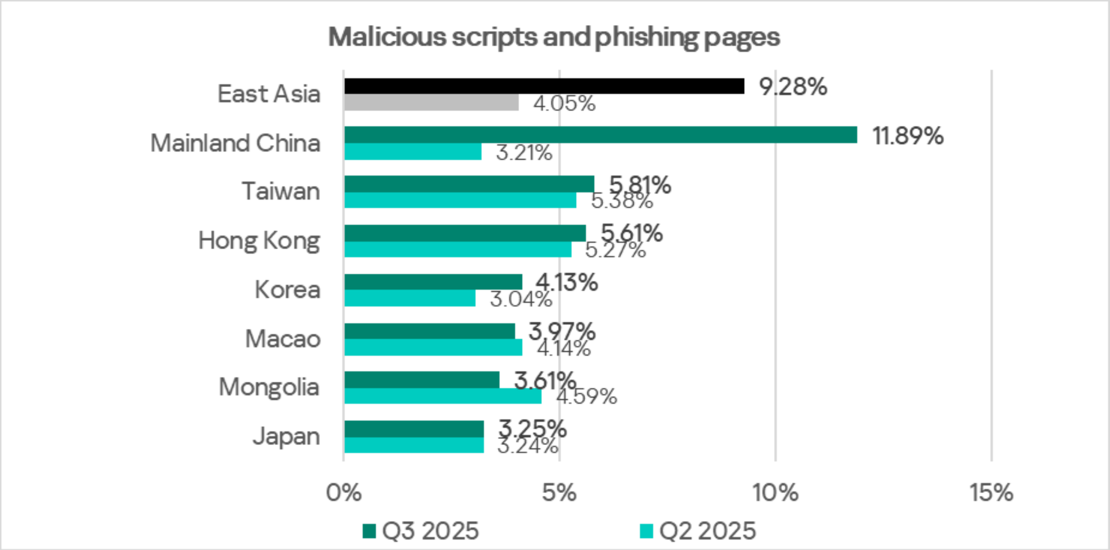
By the percentage of ICS computers on which malicious scripts and phishing pages were blocked, East Asia rose from 13th to second place globally, behind Africa. The rate increased by 5.23 p.p. and reached 9.28% – 3.6 times higher than Northern Europe, the lowest-ranking region.



In Q3 2025, this category rose in eight regions, but East Asia saw the greatest increase.

The rise is due to malicious spy scripts spreading in Mainland China in the engineering and ICS integrators sector, detected inside customized Torrent and

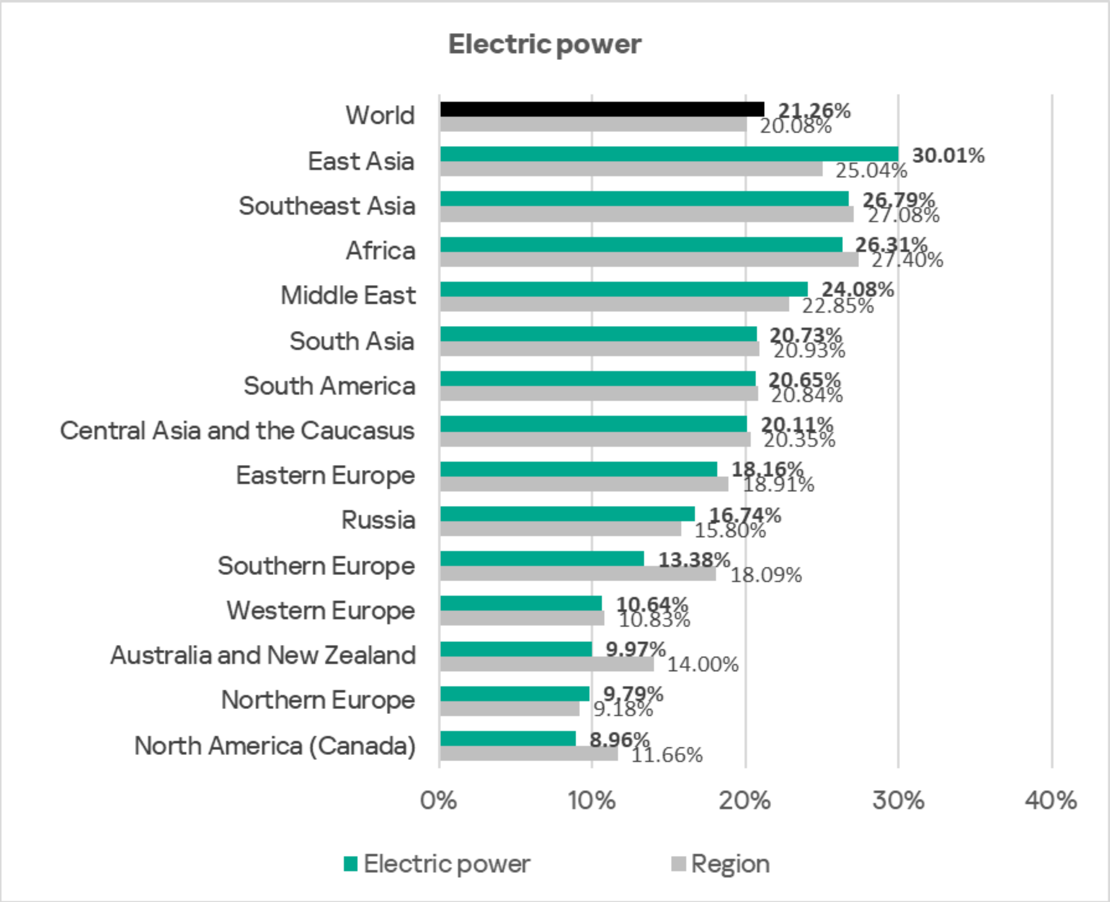
MediaGet clients (in memory and on disk). As a result, Mainland China's percentage of ICS computers on which this threat category was blocked jumped by 8.68 p.p. to 11.89%, making it the clear regional leader.



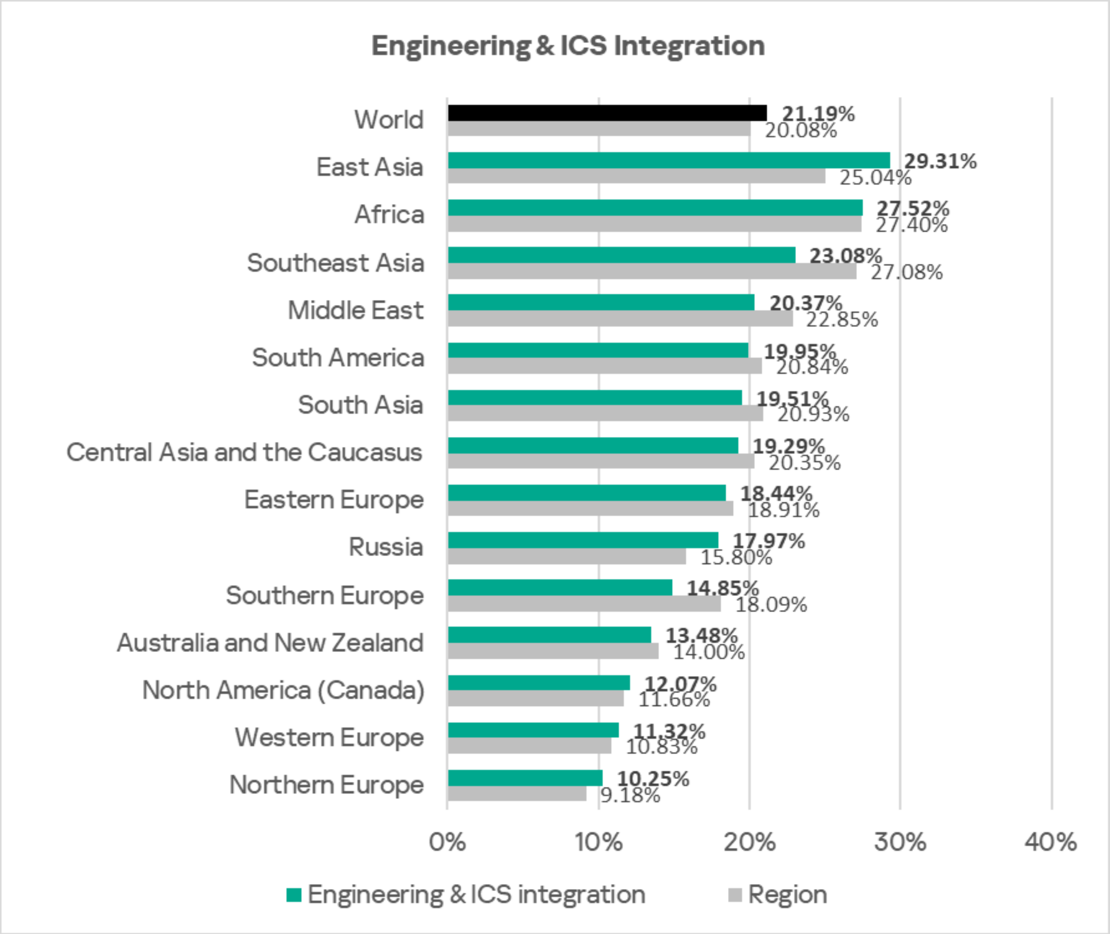
Industries

In Q3 2025, East Asia leads all regions in two sectors: electrical energy and engineering and ICS integrators.

The electrical energy figure in East Asia (30.01%) is 3.3 times higher than in North America (Canada), where it is lowest.

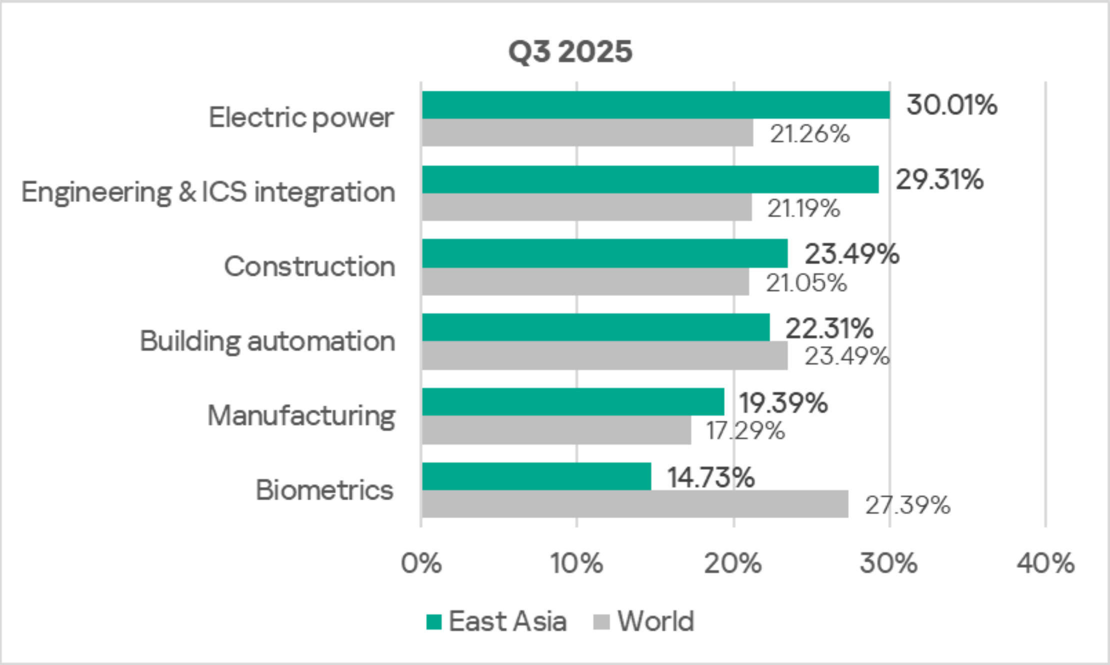


The engineering and ICS integrators sector value (29.31%) is 2.9 times higher than Northern Europe, the lowest-ranking region.



For manufacturing, East Asia ranks third among regions.

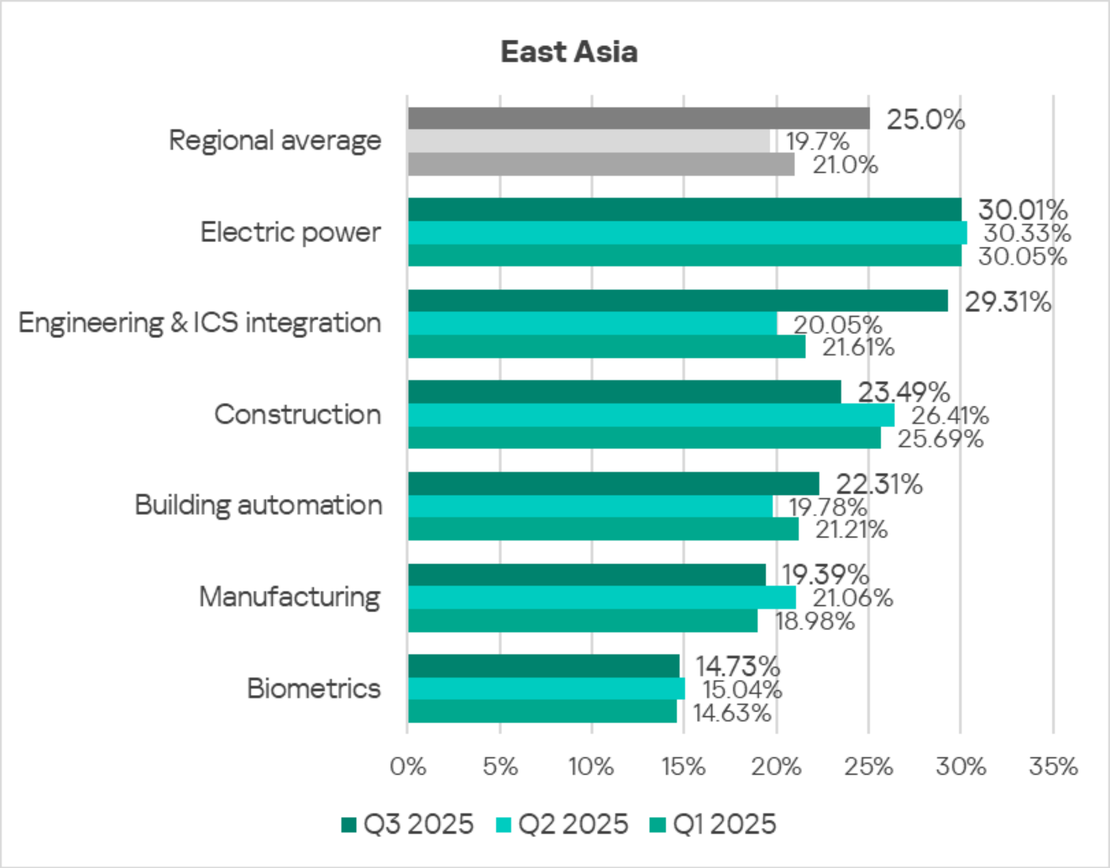
In East Asia, the electric power industry is the most frequently affected by threats among the industries covered in the report.



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

- Electrical energy: 1.4 times higher;
- Engineering and ICS integrators: 1.4 times higher;
- Construction: 1.1 times higher;
- Manufacturing: 1.1 times higher.

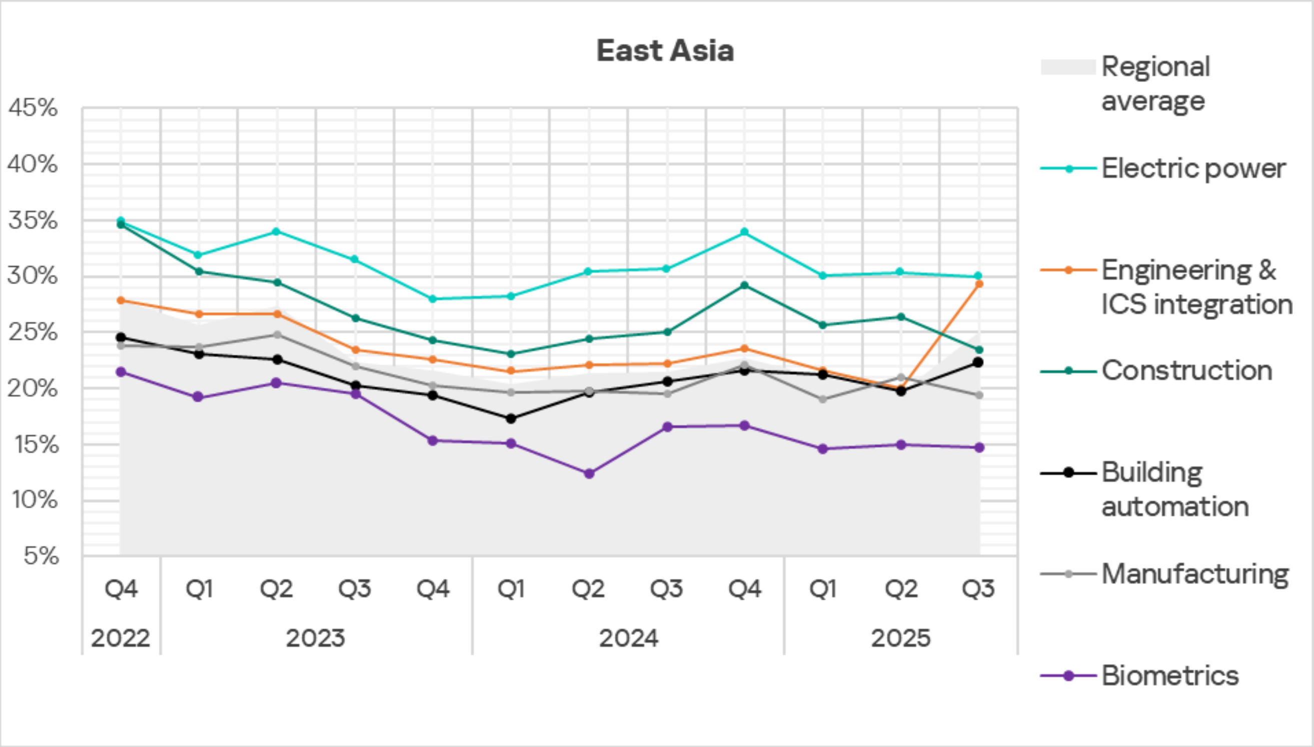
In Q3 2025, the percentage of ICS computers on which malicious objects were blocked increased in only two industries: building automation and engineering and ICS integrators.



The figure for engineering and ICS integrators increased by a significant 9.26 p.p. due to the detection of spy scripts mentioned above. This is what led to the increase in ICS computers with blocked threats.

Throughout the entire period under review, electrical energy has consistently been the industry with the highest percentage in this metric. Its value 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.

Another distinctive feature of the region is the position of OT infrastructure biometric systems in the industry rankings. In most regions they appear near the top, but in East Asia, they rank last.



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. The color red signifies that the figure approaches the maximum.

Threat source indicators for industries in East Asia, Q3 2025

Industry / Threat source	Biometrics	Building automation	Electric power	Engineering & ICS integration	Construction	Manufacturing	Threat category total in the region
Internet	4.40%	6.08%	8.84%	5.92%	7.91%	6.65%	5.91%
Email clients	4.84%	3.02%	1.06%	1.62%	1.93%	1.59%	1.63%
Removable media	0.00%	0.88%	1.78%	0.64%	0.80%	1.29%	0.72%
Network folders	0.00%	0.24%	0.34%	0.21%	0.46%	0.50%	0.20%
Industry total in the region	14.73%	22.31%	30.01%	29.31%	23.49%	19.39%	

Threat category indicators for industries in East Asia, Q3 2025

Industry / Threat category	Biometrics	Building automation	Electric power	Engineering & ICS integration	Construction	Manufacturing	Threat category total in the region
Denylisted internet resources	1.10%	2.30%	4.04%	2.63%	3.03%	6.82%	2.56%
Malicious scripts and phishing pages (JS and HTML)	6.81%	5.93%	6.68%	12.86%	6.65%	8.64%	9.28%
Spy Trojans, backdoors and keyloggers	5.71%	6.44%	8.98%	4.32%	4.41%	8.18%	4.48%
Worms	0.44%	2.30%	3.01%	1.48%	2.98%	2.73%	1.54%
Miners in the form of executable files for Windows	0.22%	0.32%	0.29%	0.20%	0.30%	0.45%	0.19%
Malicious documents (MSOffice + PDF)	2.86%	2.94%	2.95%	1.86%	2.03%	1.36%	1.75%
Viruses	1.54%	2.61%	5.19%	3.73%	3.82%	7.27%	3.06%
Ransomware	0.22%	0.32%	0.37%	0.15%	0.25%	0.45%	0.15%
Web miners running in browsers	0.22%	0.16%	0.06%	0.07%	0.20%	0.00%	0.08%
Malware for AutoCAD	0.00%	1.20%	2.50%	1.39%	1.39%	6.36%	1.21%
Industry total in the region	14.73%	22.31%	30.01%	29.31%	23.49%	19.39%	

Electric power

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

Across all sectors and regions globally, electrical energy in East Asia ranks:

- Third place in removable media threats.
- Third place in network folder threats.
- Third by the percentage of computers where malware for AutoCAD was blocked.
- Fifth by the percentage of computers where spyware was blocked.

Among regions, in the electrical energy sector East Asia ranks:

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

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

- First place in the percentage of ICS computers on which internet threats from the internet and on removable media are blocked, and third in network folders.
- First in the following threat categories: denylisted internet resources, malicious documents, spyware, worms, and ransomware.
- Second in viruses and malware for AutoCAD.

Engineering and ICS integrators

East Asia leads all regions in the percentage of ICS computers on which malicious objects were blocked in the engineering and ICS integrators sector.

Across all sectors and regions globally, East Asia's engineering and ICS integrators sector ranks:

- Fifth in network folder threats.
- Third in the percentage of computers where malicious scripts and phishing pages were blocked.

Among regions, in the electrical energy sector East Asia ranks:

- First in the percentage of ICS computers on which network folder threats are blocked, second in removable media threats.
- First in the percentage of ICS computers on which malicious scripts and phishing pages, viruses, and malware for AutoCAD are blocked.
- Third in spyware and worms.

Among industries in the region, engineering and ICS integrators have the following rankings:

- First in malicious scripts and phishing pages.
- Third for AutoCAD malware.

Construction

East Asia ranks fifth among regions in the percentage of ICS computers with blocked malicious objects in construction.

Across all sectors and regions globally, the construction sector in East Asia ranks:

- Second place in network folder threats.
- Fifth in the percentage of computers where viruses were blocked.

Among regions, in the electrical energy sector East Asia ranks:

- First in the percentage of ICS computers on which network folder threats are blocked and second in removable media threats.

- First in the percentage of ICS computers on which malicious documents and malware for AutoCAD are blocked.
- Second in spyware and third in viruses.

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

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

Building automation

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

Across all sectors and regions globally, building automation in East Asia ranks:

- Fourth in network folder threats.

Among regions, in the electrical energy sector East Asia ranks:

- First in the percentage of ICS computers on which network folder threats are blocked and second in removable media threats.
- First in the percentage of ICS computers on which malware for AutoCAD is blocked.

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

- Second in threats from email, third in removable media.
- Second in malicious documents, miners in the form of executable files for Windows, and ransomware.
- Third in spyware and worms.

Manufacturing

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

Across sectors and regions globally, manufacturing in East Asia ranks:

- First place in network folder threats.

Among regions, in the electrical energy sector East Asia ranks:

- First in the percentage of ICS computers on which network folder threats are blocked; second in removable media threats.

- First in the percentage of ICS computers on which worms and malware for AutoCAD are blocked.
- Second in spyware and viruses.
- Third place in ransomware.

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

- First in the percentage of ICS computers on which network folder threats are blocked, second in removable media threats, and third in internet threats.
- Second place for worms.
- Third in denylisted internet resources, viruses, ransomware, and both types of miners.

Biometric systems

East Asia ranks last among regions in the percentage of ICS computers with blocked malicious objects in the OT infrastructure for biometric systems.

The regional industry rankings for OT infrastructure for biometric systems is as follows:

- First in threats from network folders.
- Second in web miners.
- Third in malicious scripts and phishing pages, as well as malicious documents.

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 ranks third among regions by the percentage of ICS computers on which threats from removable media were blocked. The region's figure is 1.9 times higher than the global average.

South Asia ranks fourth globally for ICS computers where threats in network folders were blocked. The figure for this threat source in the region is 1.3 times higher than the global average.

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

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

High level of internet threats

South Asia ranks third globally by the percentage of ICS computers on which internet threats were blocked.

Differences among countries in the region

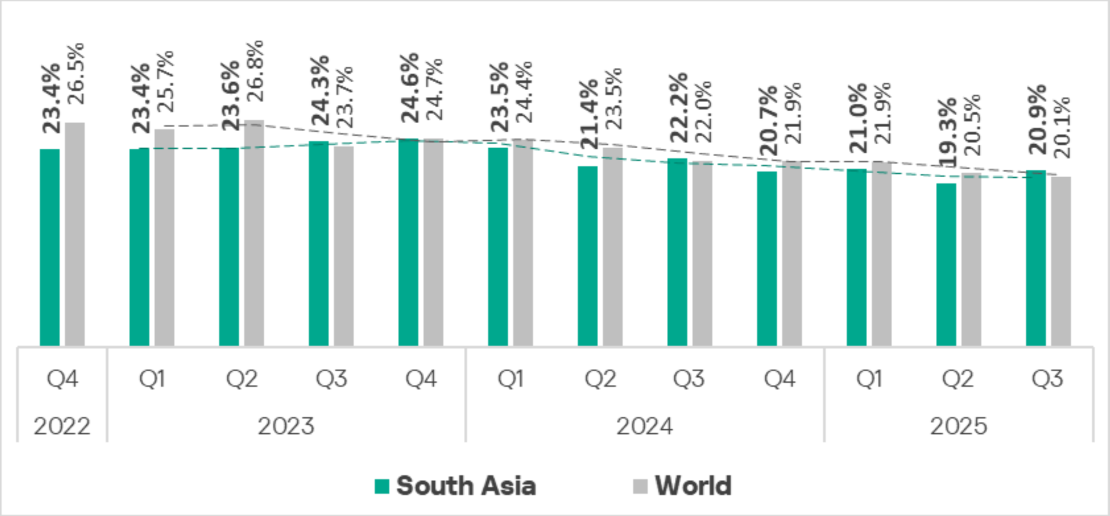
- The region's figures are all heavily influenced by India. India is near the bottom of most rankings by both threat source and category, with a percentage of attacked ICS computers significantly lower than in most other countries of the region and below the regional average.
- Afghanistan's cybersecurity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

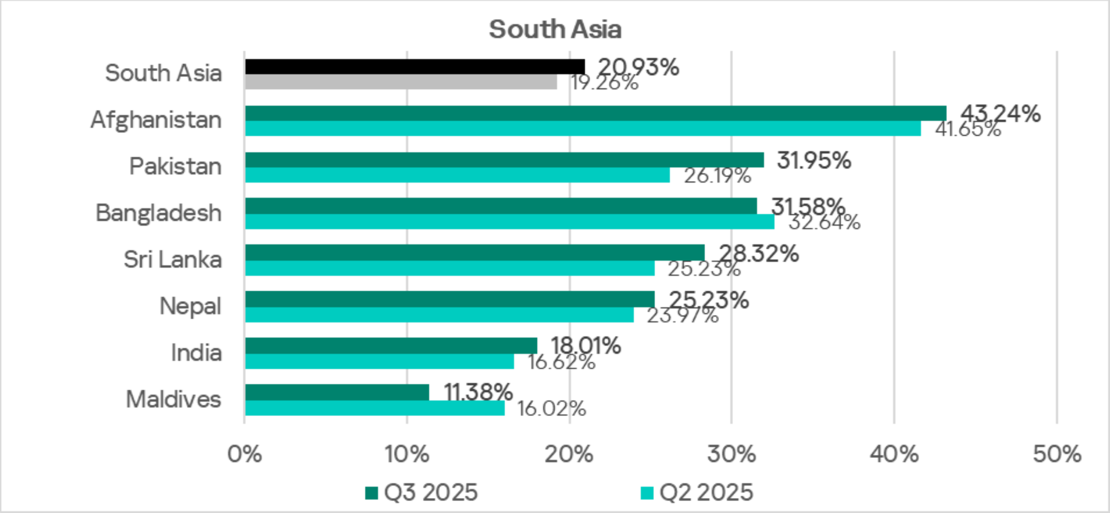
In Q3 2025, South Asia rose from ninth to fifth place in the regional rankings in the percentage of ICS computers on which malicious objects were blocked.

The region's rate rose by 1.6 p.p. over the quarter, to 20.9%. This is 2.3 times higher than Northern Europe, which ranks last.

The region shows a gradual downward trend with some fluctuations.



The percentage of ICS computers on which malicious objects were blocked varies among the region's countries, from 11.38% in the Maldives to 43.24% in Afghanistan. The rate increased across all countries in the region except for Bangladesh and the Maldives.

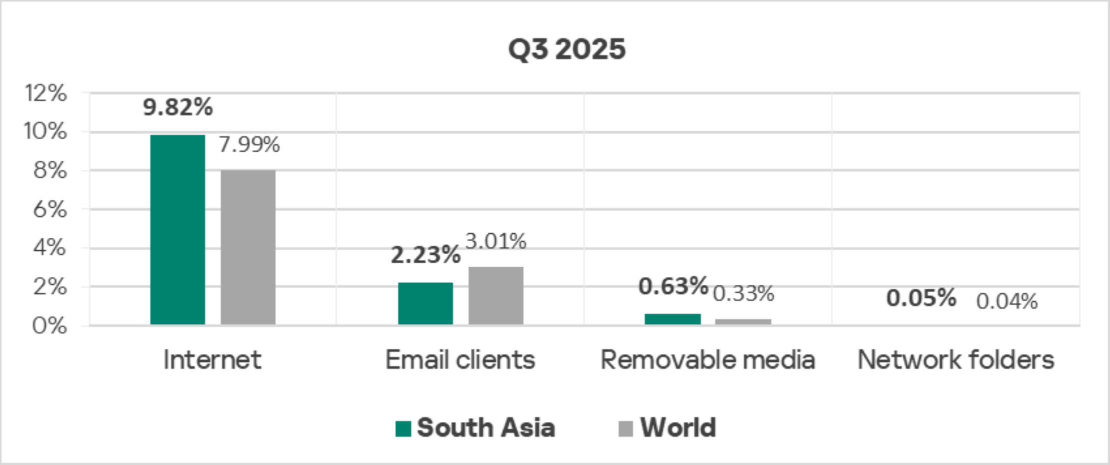


Threat sources

In Q3 2025, South Asia exceeded global averages for all threat sources except mail clients:

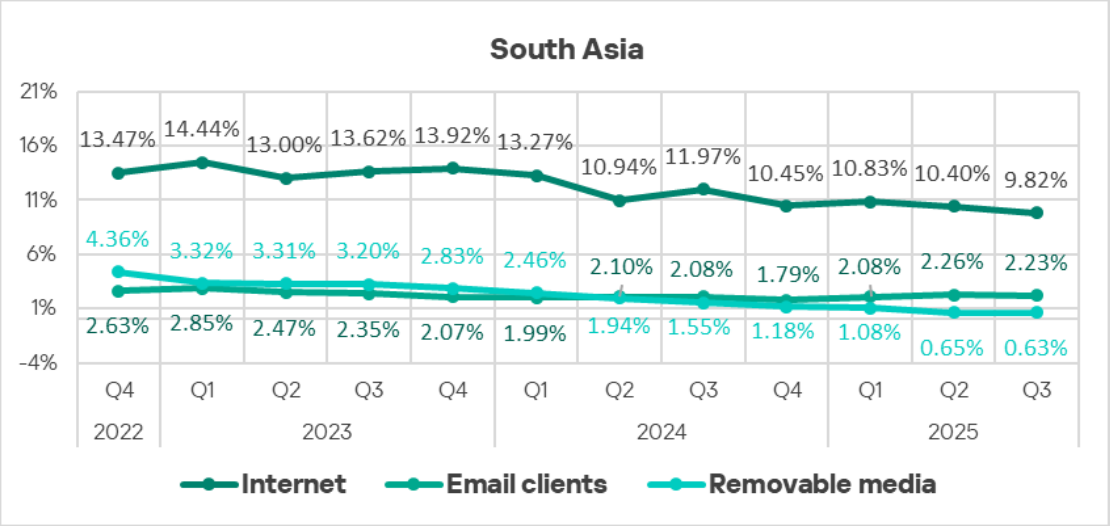
- Internet: by 1.2 times, third place globally.
- Removable media: by 1.9 times, third place globally.

- Network folders: by 1.3 times, fourth place globally.



The percentage of ICS computers on which malicious objects were blocked decreased for all threat sources.

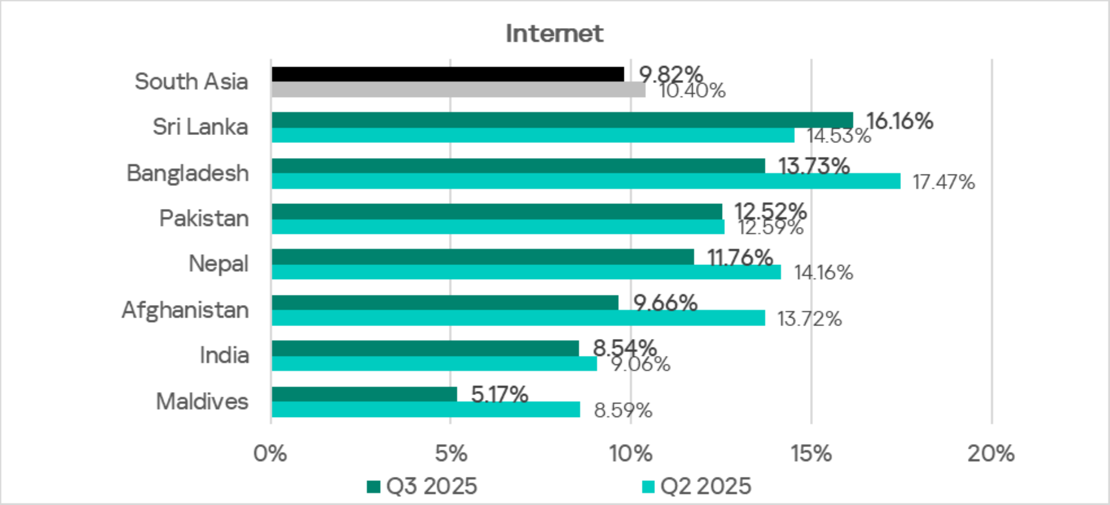
Overall, all major threat sources show a long-term downward trend.



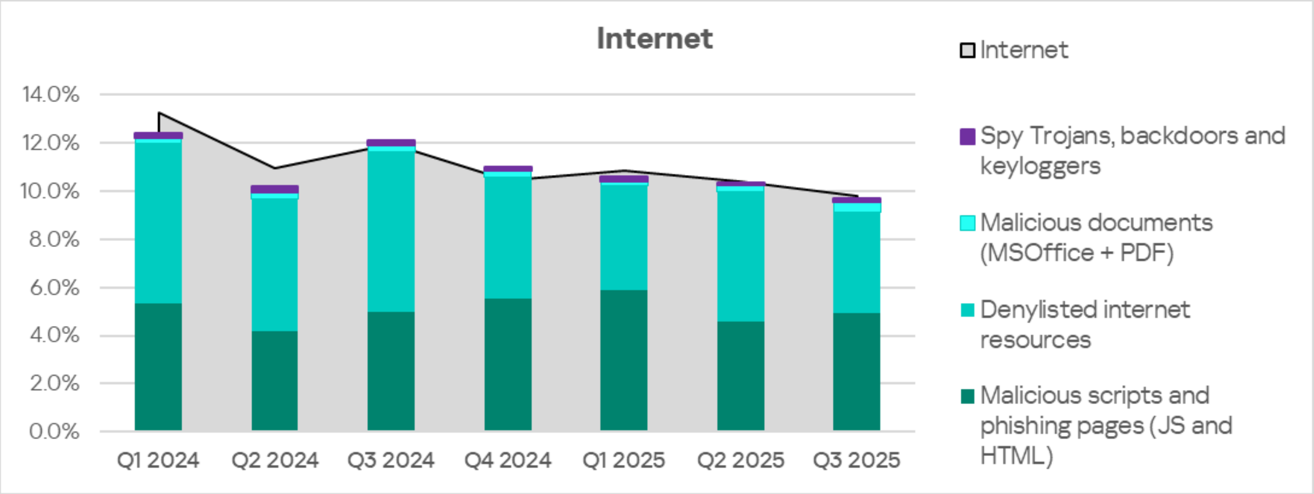
Internet

In Q3 2025, South Asia ranked third globally in terms of the percentage of ICS computers on which internet threats were blocked (9.82%). This is 2.1 times higher than Northern Europe, which ranks last in the regional ranking. It is also the region's three-year low.

Country figures range from 5.17% in the Maldives to 16.16% in Sri Lanka. Sri Lanka was the only country in the region where internet threats decreased over the quarter.



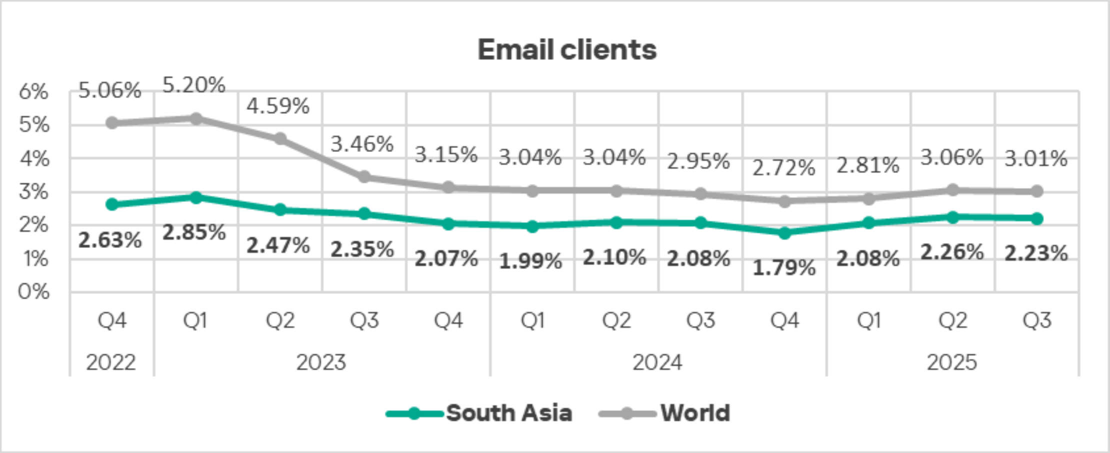
The primary categories of internet threats blocked on ICS computers in the region in Q3 2025 were malicious scripts and phishing pages, denylisted internet resources, malicious documents, and spyware.



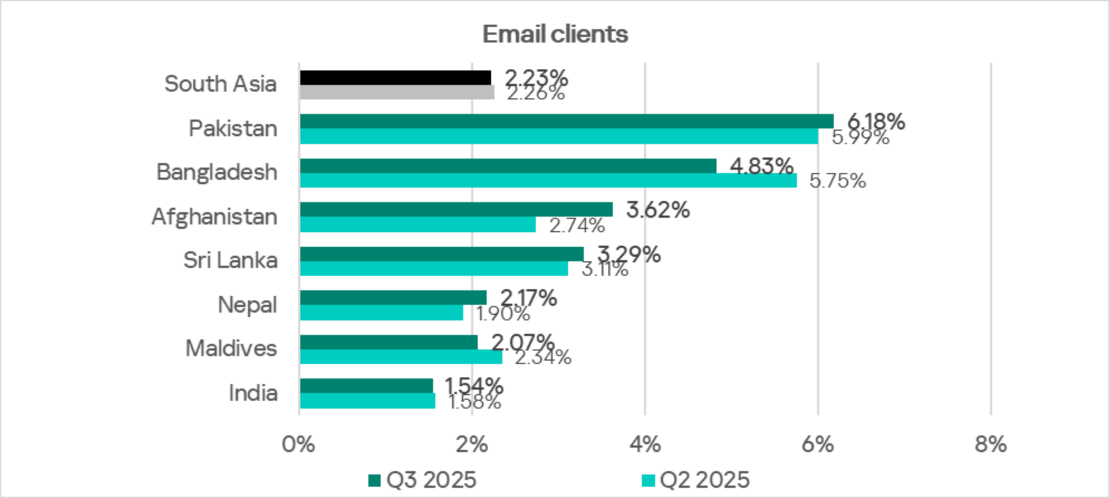
By the percentage of ICS computers on which denylisted internet resources were blocked, Sri Lanka leads in the region.

Email clients

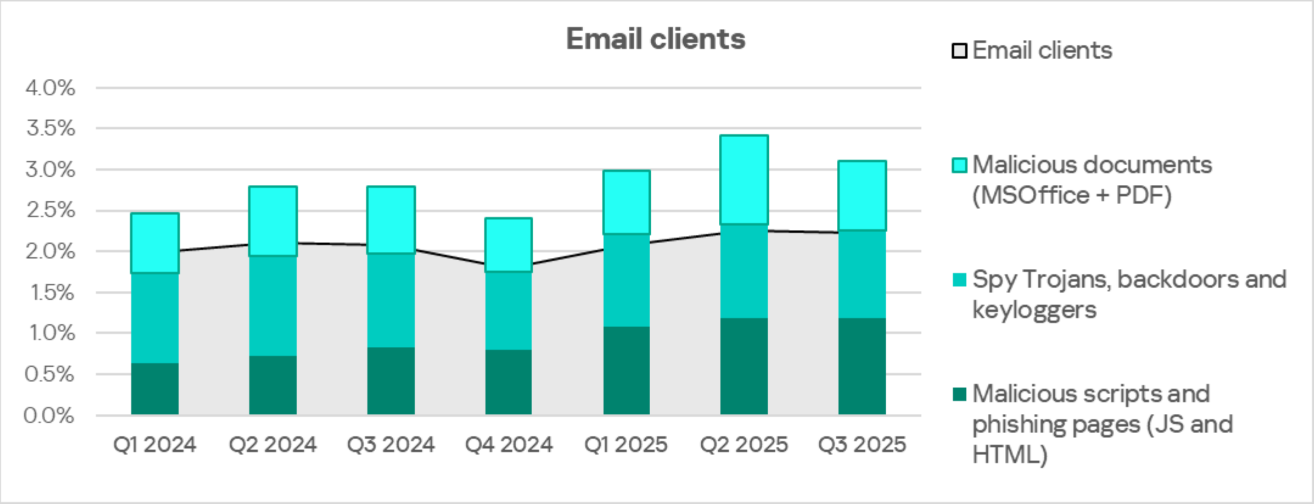
In terms of ICS computers where mail client threats were blocked, South Asia ranks ninth globally with 2.23%. This is 2.9 times higher than in Russia, which has the lowest figure.



Among the region's countries, Pakistan (6.18%) and Bangladesh (4.83%) lead in the percentage of ICS computers on which mail client threats were blocked. The lowest figure observed was in India, at 1.54%. Pakistan has seen this metric grow for three consecutive quarters.



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

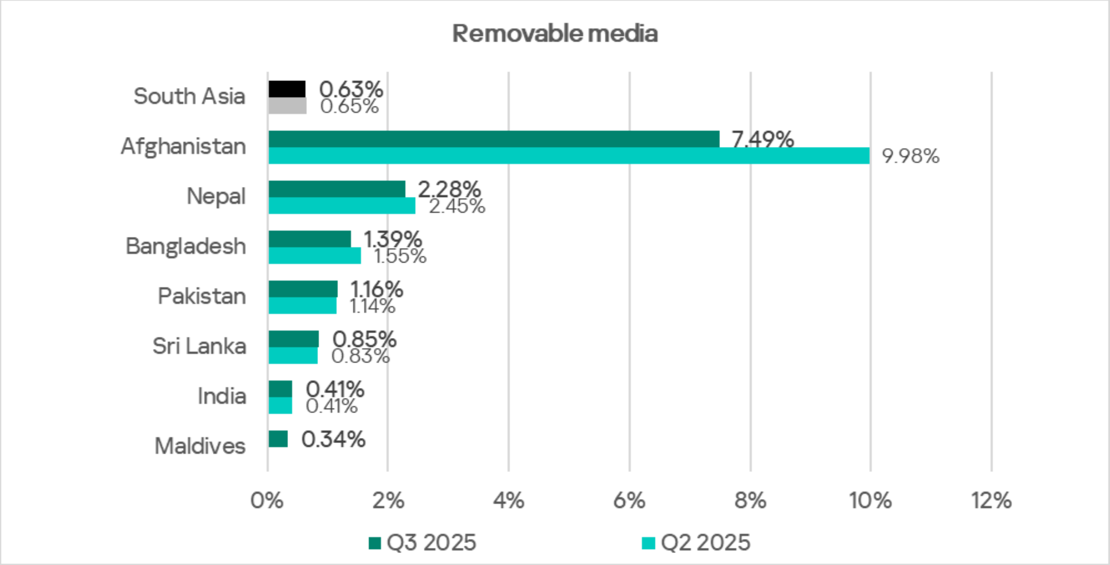


Pakistan and Bangladesh are among the leading countries in terms of email-borne threats. They lead in malicious documents and rank in the top 3 for both malicious scripts and phishing pages. Bangladesh leads in terms of spyware.

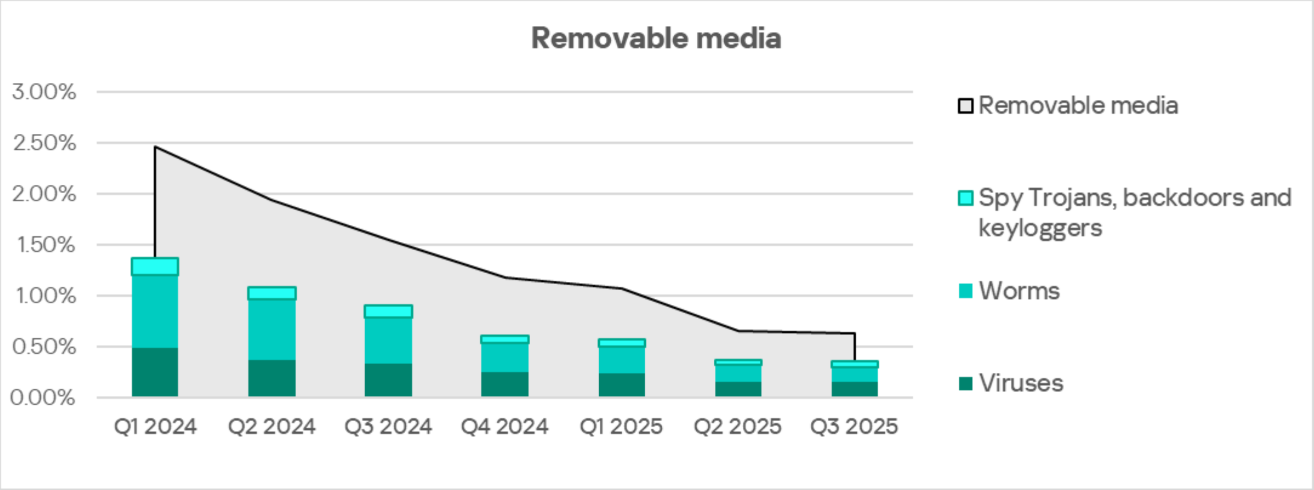
Removable media

By percentage of ICS computers on which removable media threats were blocked, South Asia ranks third globally at 0.63%. This is 12.6 times higher than in the Australia and New Zealand region, which is at the bottom of this ranking.

Among countries in the region, Afghanistan leads by a wide margin in the percentage of ICS computers on which removable media threats were blocked, with 7.94%. Other countries' rates range from 0.34% in the Maldives to 2.28% in Nepal.



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

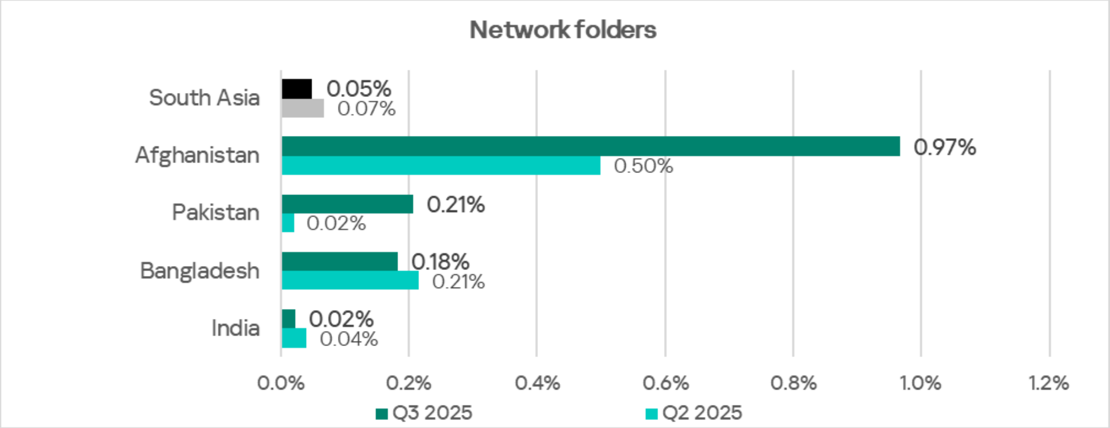


Afghanistan also leads (again by a wide margin) in the percentage of ICS computers on which worms were blocked.

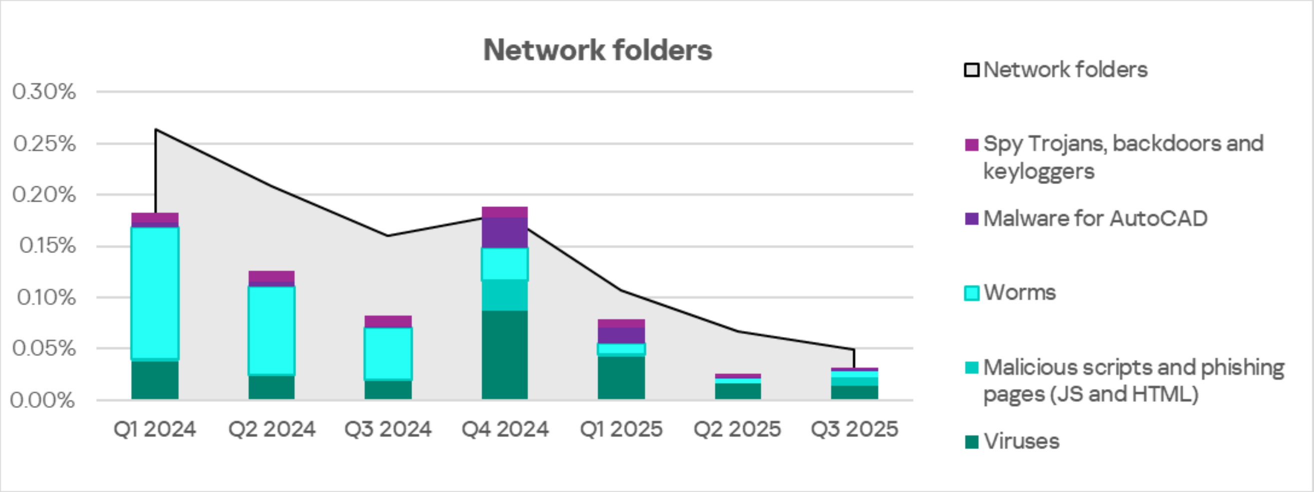
Network folders

South Asia, with 0.05%, ranks fourth among regions globally in the percentage of ICS computers on which network folder threats are blocked. In Q3 2025, the region's figure was 8.2 times higher than in Northern Europe, which was at the bottom of the ranking.

In Q3 2025, Afghanistan, with a rate of 0.97%, was responsible for South Asia's high position in the regional rankings for the percentage of ICS computers on which network folder threats were blocked. While Sri Lanka led this metric in Q2 2025, no network folder threats were detected there in Q3 — a finding consistent with Nepal's results.

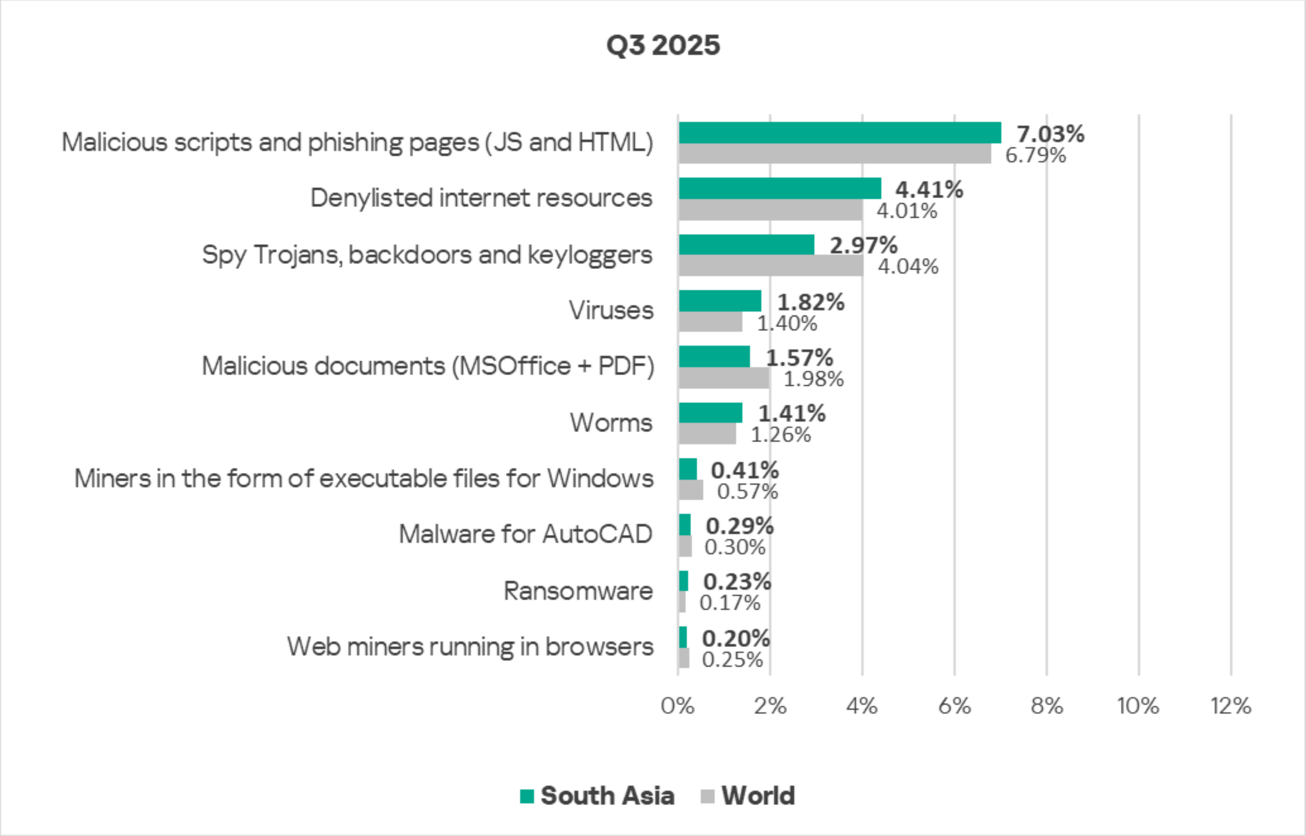


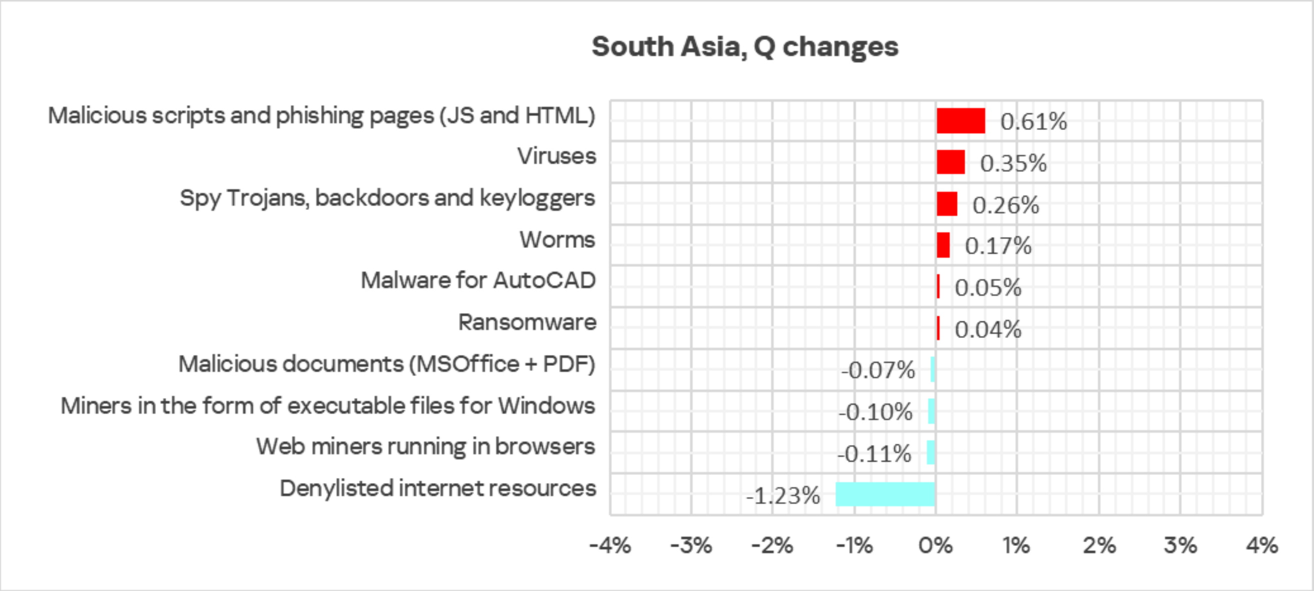
In Q3 2025, the primary categories of threats that spread via network folders in the region were viruses, malicious scripts, and worms.



Threat categories

As in most regions, malicious scripts and phishing pages led the threat category rankings for South Asia in Q3 2025, based on their detection rate on ICS computers. This same category also led the region in quarter-over-quarter growth.





Compared with global averages, the region has higher percentages of ICS computers where the following were blocked:

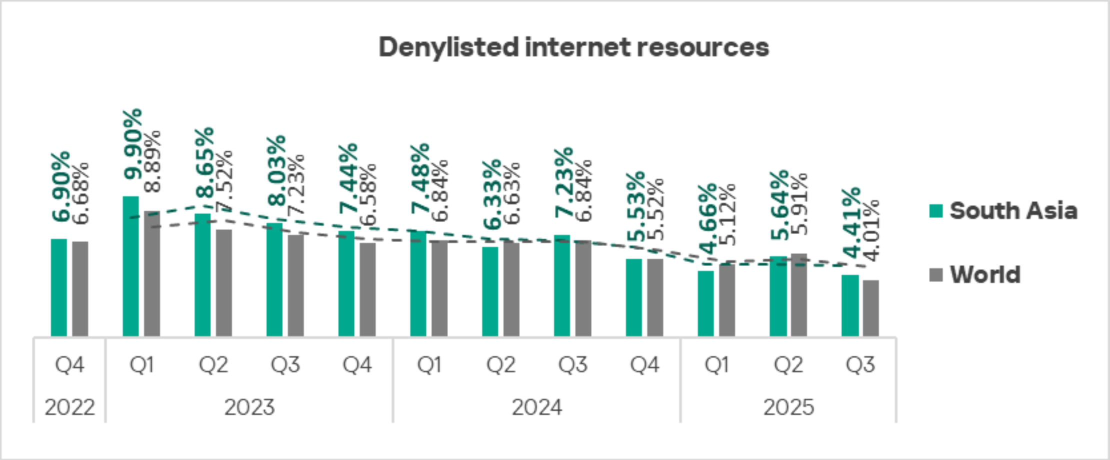
- Denylisted internet resources, by 1.1 times. South Asia is third for this threat metric regionally.
- Worms: 1.1 times higher.
- Viruses: 1.3 times higher.
- Ransomware, by 1.4 times. This is third place in the regional rankings.

South Asia also ranks fourth among all regions by malware for AutoCAD.

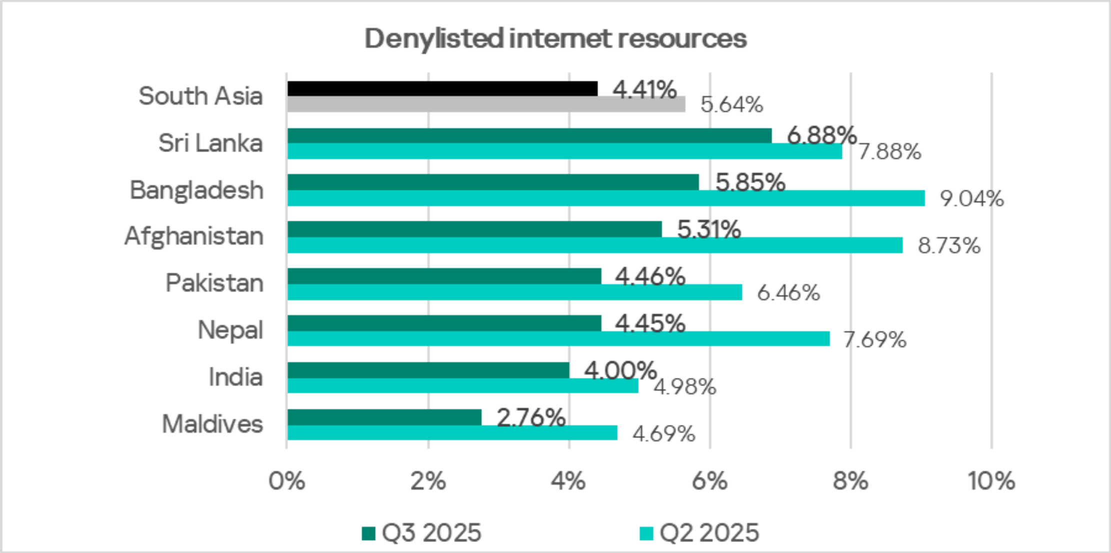
Denylisted internet resources

The region holds third place in the percentage of ICS computers on which denylisted internet resources were blocked, with 4.41%. South Asia's rate is 1.9 times higher than that in the Australia and New Zealand region, which has the lowest figure among all regions.

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



Within the region, Sri Lanka leads with 6.88% in the percentage of ICS computers on which denylisted internet resources were blocked.

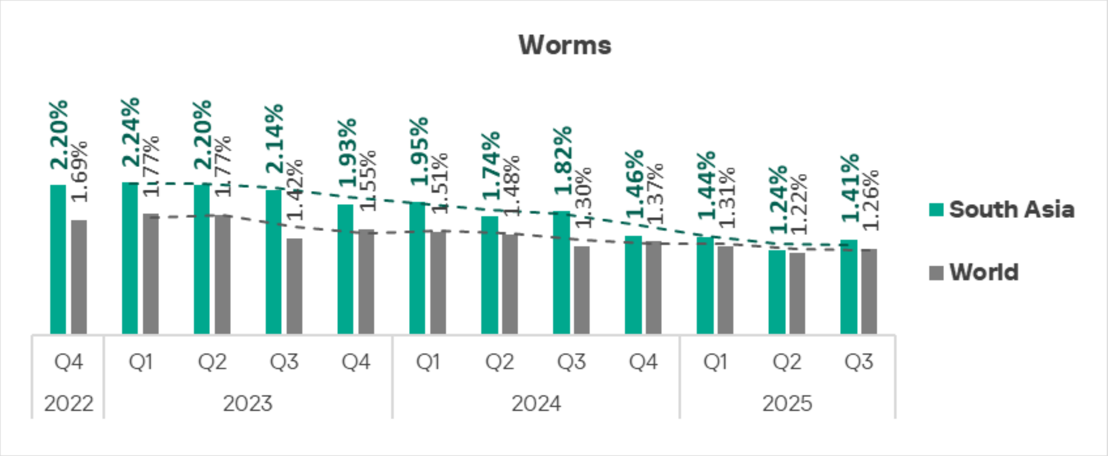


The internet is the sole threat source for this category. Sri Lanka also ranks first in the percentage of ICS computers on which internet threats are blocked.

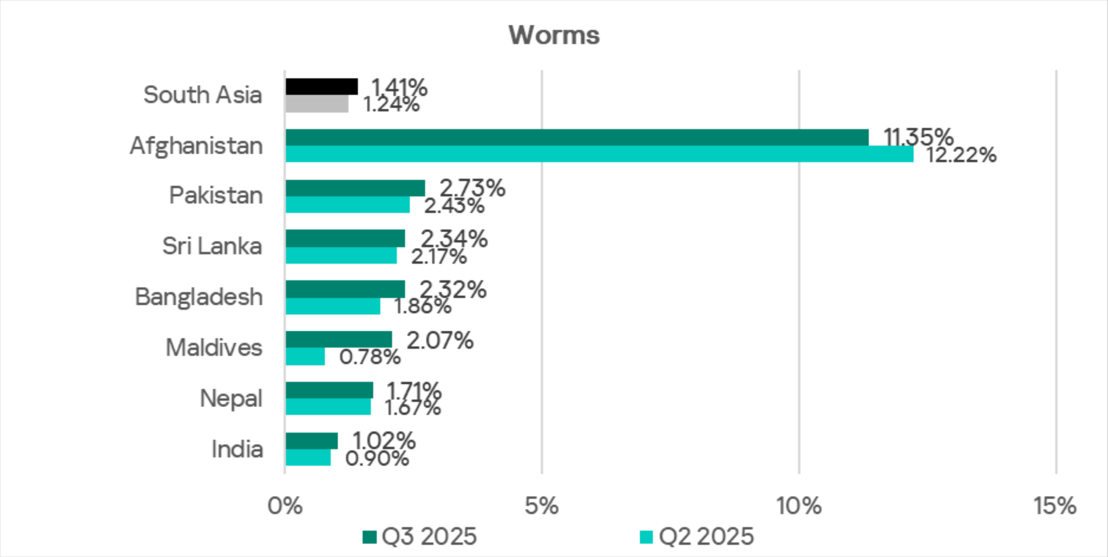
Worms

South Asia ranks seventh regionally in the percentage of ICS computers on which worms were blocked.

In Q3 2025, the worm rate (1.41%) was 6.4 times higher than that in Northern Europe, which has the lowest regional rate. In terms of growth in the worm rate, the region holds third place.



Within South Asia, Afghanistan leads decisively with an extremely high worm blocking rate of 11.35% on ICS computers.



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

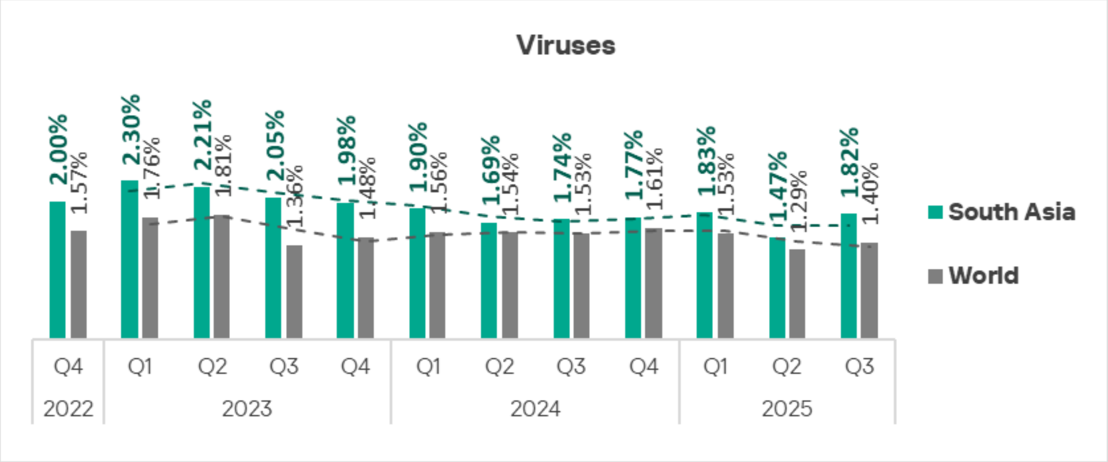
Viruses and malware for AutoCAD

South Asia ranks fifth for ICS computers where viruses were blocked, and fourth by malware for AutoCAD.

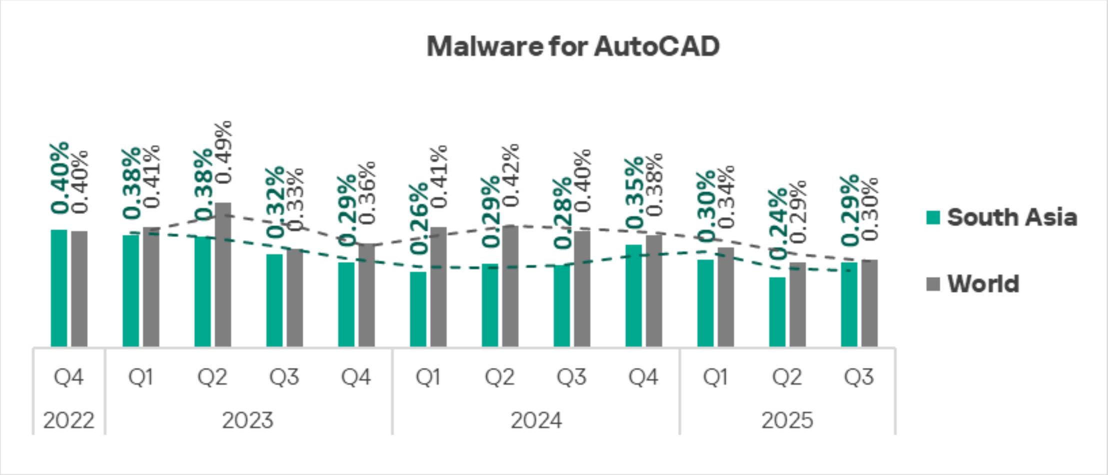
As in East and Southeast Asia, malware for AutoCAD in South Asia usually spreads the same way as viruses. This explains the high percentage for this category.

The virus count in South Asia has been declining. In Q3 2025, the virus rate in the region rose to 1.82%. This is 11.4 times higher than that in the Australia and New

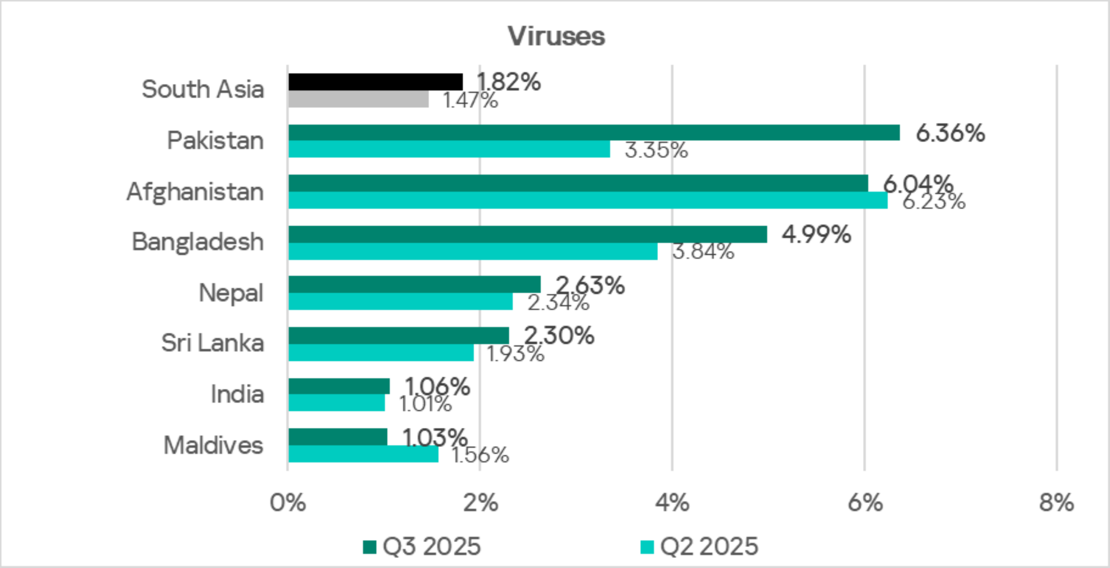
Zealand region, which has the lowest regional rate. South Asia ranks second among regions for growth in this metric.



The percentage of ICS computers in South Asia where malware for AutoCAD was blocked also increased over the quarter, reaching 0.29%. This is 29.0 times higher than North America (Canada), which comes last in the regional rankings.

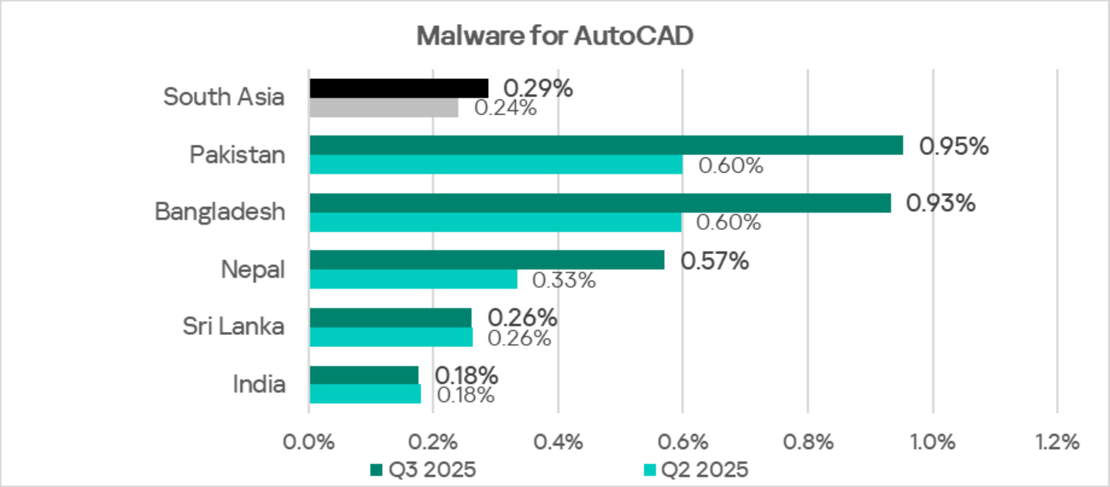


Among the region's countries, Pakistan leads in the percentage of ICS computers with blocked viruses, at 6.36%. The country's rate nearly doubled during the quarter, allowing it to surpass Afghanistan, the previous consistent leader in the rankings.



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

Pakistan, with 0.95%, and Bangladesh, with 0.93%, share the lead for the percentage of ICS computers on which malware for AutoCAD was blocked. In both countries, the quarterly rate increased from 0.6%.



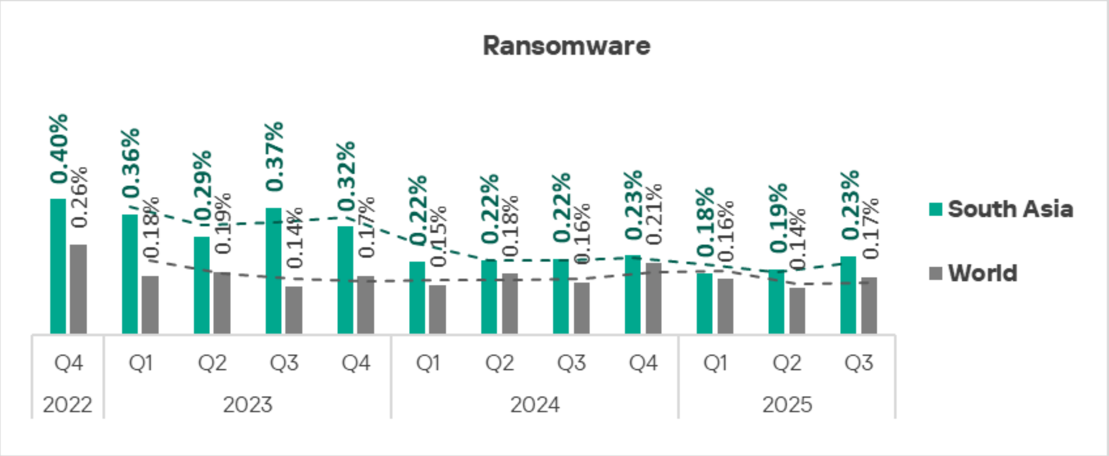
Like viruses, malware for AutoCAD in the region spreads through all sources, but mostly via removable media.

Ransomware

In terms of the percentage of ICS computers on which ransomware is blocked, South Asia is in third place regionally, behind only Africa and the Middle East.

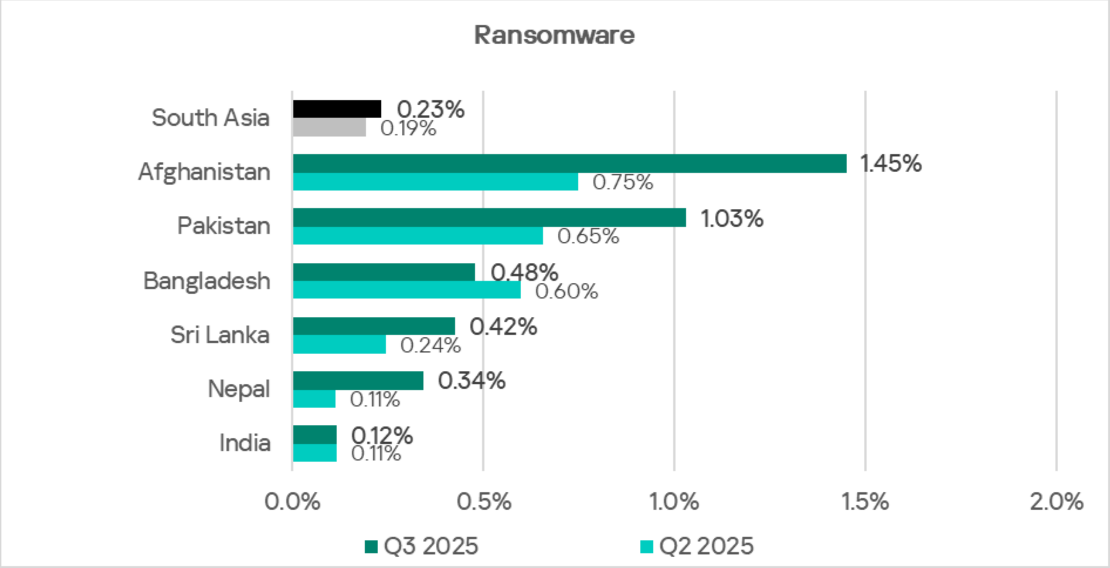
South Asia's figure (0.23%) is 4.6 times higher than that of Northern Europe, which ranks lowest.

The region's figure has been growing for the second consecutive quarter.



Afghanistan leads the region with 1.45% of ICS computers where ransomware is blocked. The next country in the rankings, Pakistan, also has a high value, 1.03%.

The metric increased over the quarter in all countries except for Bangladesh. In Afghanistan, it almost doubled.

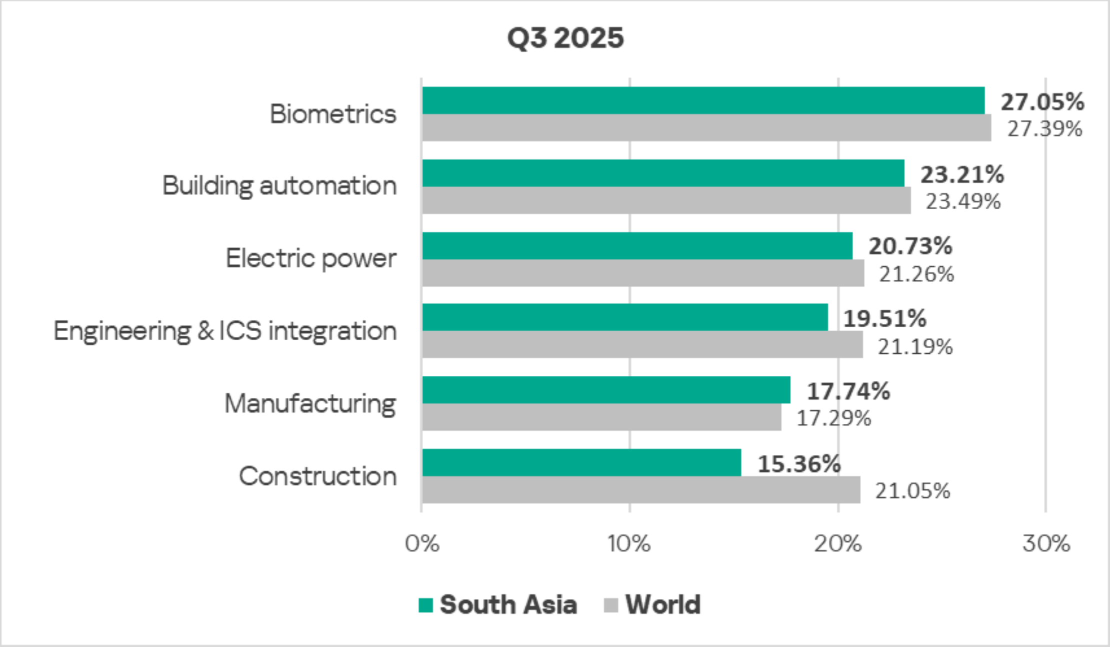


In South Asia, ransomware most often spreads via removable media. Afghanistan is also the regional leader for this threat source.

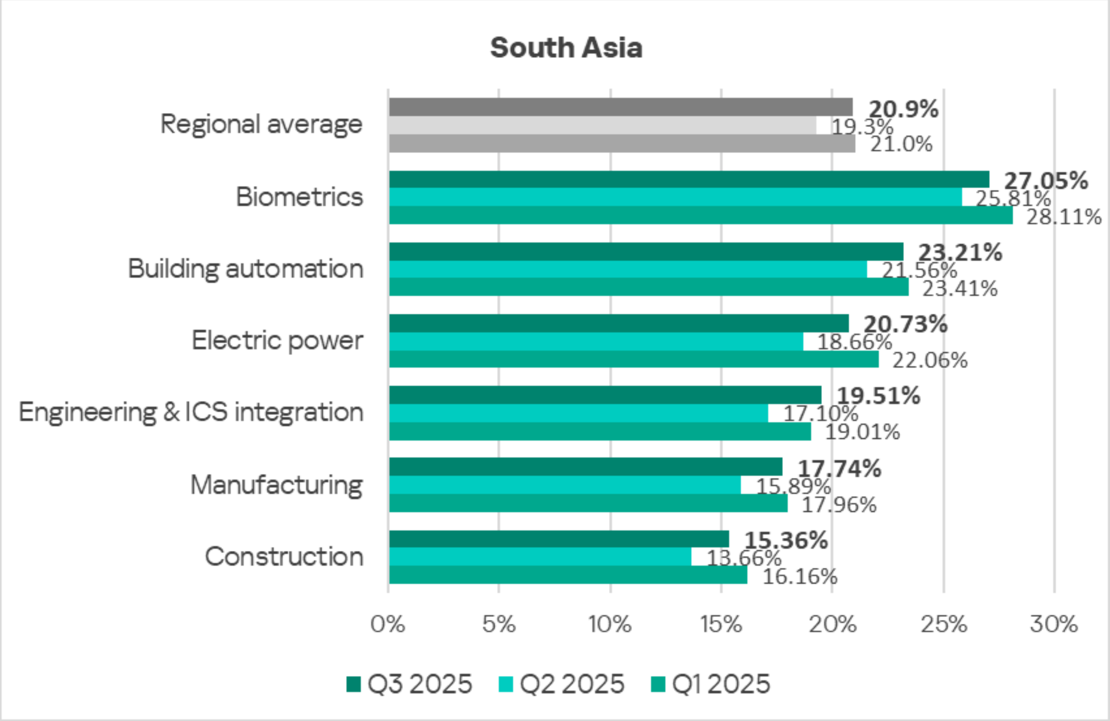
Industries

Among the region's industries covered in this report, the one most frequently facing threats is the OT infrastructure for biometric systems.

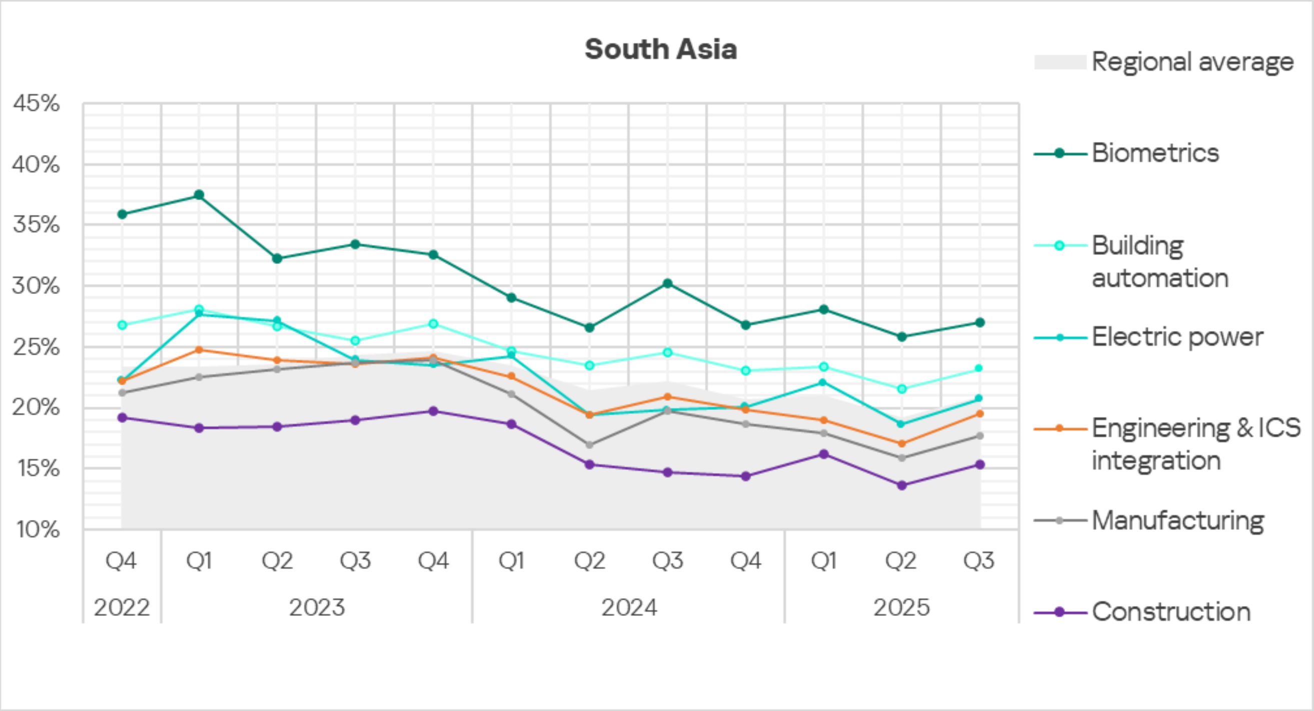
Compared with global averages, the figures for all sectors, with the exception of manufacturing, are lower.



In Q3 2025, the percentage of ICS computers on which malicious objects were blocked increased across all reviewed industries.



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. The color red signifies that the figure approaches the maximum.

Threat source indicators for industries in South Asia, Q3 2025

Industry / Threat source	Biometrics	Building automation	Electric power	Engineering & ICS integration	Construction	Manufacturing	Threat category total in the region
Internet	11.21%	10.52%	8.08%	9.90%	7.60%	7.53%	9.82%
Email clients	5.08%	3.23%	2.73%	0.98%	2.10%	1.41%	2.23%
Removable media	1.82%	0.78%	0.54%	0.38%	0.20%	0.67%	0.63%
Network folders	0.08%	0.09%	0.00%	0.02%	0.05%	0.00%	0.05%
Industry total in the region	27.05%	23.21%	20.73%	19.51%	15.36%	17.74%	

Threat category indicators for industries in South Asia, Q3 2025

Industry / Threat category	Biometrics	Building automation	Electric power	Engineering & ICS integration	Construction	Manufacturing	Threat category total in the region
Denylisted internet resources	4.92%	4.44%	4.09%	4.68%	3.44%	4.10%	4.41%
Malicious scripts and phishing pages (JS and HTML)	11.59%	8.53%	5.35%	5.75%	5.05%	4.77%	7.03%
Spy Trojans, backdoors and keyloggers	7.12%	4.07%	3.41%	1.81%	1.67%	2.76%	2.97%
Worms	3.26%	1.72%	2.73%	0.94%	0.48%	1.81%	1.41%
Miners in the form of executable files for Windows	0.91%	0.45%	0.15%	0.36%	0.18%	0.34%	0.41%
Malicious documents (MSOffice + PDF)	3.48%	2.19%	1.56%	0.91%	0.86%	0.87%	1.57%
Viruses	3.86%	2.13%	2.58%	1.46%	1.47%	2.42%	1.82%
Ransomware	0.45%	0.34%	0.10%	0.11%	0.13%	0.20%	0.23%
Web miners running in browsers	0.30%	0.23%	0.00%	0.19%	0.20%	0.07%	0.20%
Malware for AutoCAD	0.23%	0.18%	0.24%	0.36%	1.04%	0.34%	0.29%
Industry total in the region	27.05%	23.21%	20.73%	19.51%	15.36%	17.74%	

All industries in the region show high values for internet threats — both as a source and by category (denylisted internet resources, malicious scripts, and phishing pages).

Biometric systems

South Asia is in fourth place in the regional rankings in the percentage of ICS computers on which malicious objects were blocked in the OT infrastructure for biometric systems.

In the global rankings across all industries in all regions, the OT infrastructure for biometric systems in East Asia holds:

- Second place in removable media threats.
- Third place in the percentage of computers where worms were blocked.

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

- First place in the percentage of ICS computers on which internet threats and removable media threats are blocked.
- Second place in network folders.

- First place in the percentage of ICS computers on which viruses are blocked.
- Second place for worms.
- Third place in denylisted internet resources, malicious scripts and phishing pages, malware for AutoCAD, and both types of miners.

Among industries in the region, the biometric systems has the following rankings:

- First place in all threat sources except for network folders.
- Second place in network folder threats.
- First place in all threat categories except for malware for AutoCAD.

Building automation

South Asia is in sixth place among regions in the percentage of ICS computers on which malicious objects were blocked in the building automation industry.

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

- First place in the percentage of ICS computers on which internet threats are blocked.
- Third place in removable media and fourth for network folder threats.
- Second place in the percentage of ICS computers on which denylisted internet resources are blocked.
- Fourth place in malware for AutoCAD and ransomware.

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

- First place in network folder threats. Second place in all other threat sources.
- Second place in malicious scripts and phishing pages, spyware, malicious documents, ransomware, and both types of miners.
- Third place in denylisted internet resources.

Electric power

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

Based on industry indicators among regions, South Asia is fourth in the percentage of ICS computers on which worms, viruses, and malware for AutoCAD are blocked.

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

- Third place in email client threats.

- Second place in viruses and worms.
- Third place in spyware and malicious documents.

Engineering and ICS integrators

South Asia is sixth 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 has the following rankings:

- Third place in the percentage of ICS computers on which internet threats are blocked.
- Fourth place in denylisted internet resources, viruses, and malware for AutoCAD.

Among industries in the region, engineering and ICS integrators have the following rankings:

- Third place in internet threats.
- Second place in denylisted internet resources and malware for AutoCAD.
- Third place in malicious scripts and phishing pages and miners in the form of executable files for Windows.

Manufacturing

South Asia ranks sixth in the percentage of ICS computers on which malicious objects were blocked in the manufacturing sector.

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

- Third place in the percentage of ICS computers on which threats are blocked when removable media are connected.
- Fourth place in internet threats.
- Second place in the percentage of ICS computers on which denylisted internet resources are blocked.
- Third place in malware for AutoCAD and fourth for viruses and ransomware.

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

- Third place in removable media threats.
- Third place in viruses, worms, ransomware, and malware for AutoCAD.

Construction

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

Based on industry indicators among regions, South Asia is fourth in the percentage of ICS computers on which network folder threats are blocked.

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

- Third place in network folder threats.
- First place in malware for AutoCAD.
- Third in the region in terms of web miners.

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 Q3 2025, this indicator in the region was 1.5 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.

By the percentage of ICS computers on which executable miners are blocked, Central Asia and the South Caucasus ranks first among all regions; in terms of worms, it ranks second after Africa. These categories are 2.1 and 1.7 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 ranks first globally. The main distribution channel for such malware is the internet.

In Q3 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 and industries.

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.

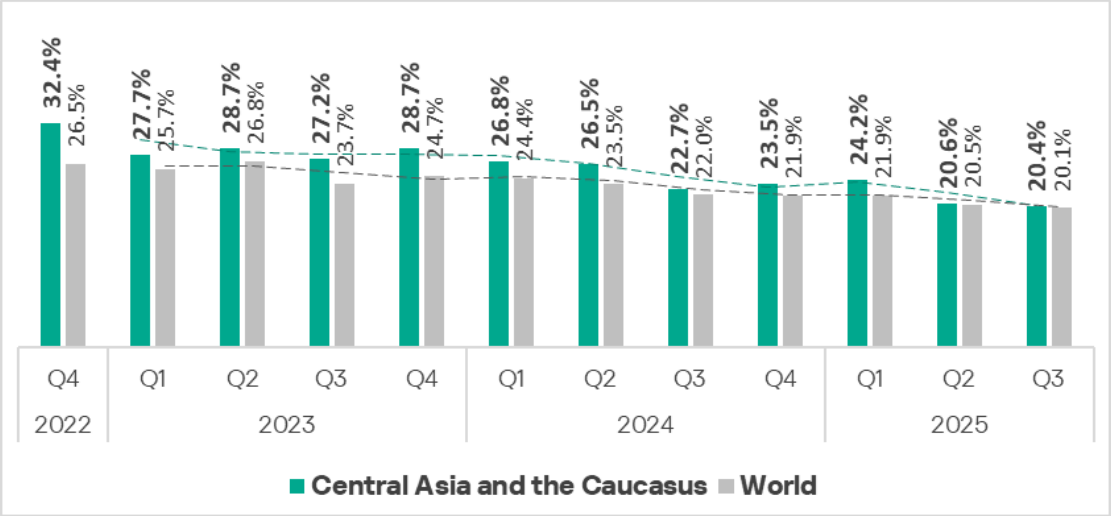
Consistently high level of ransomware incidents

By the percentage of ICS computers on which ransomware was blocked, Central Asia and the South Caucasus ranks fourth, with a rate 1.2 times higher than the global average. In Q3 2025, this category of threats spread in the region via the internet, email, and removable media. In terms of ransomware, Central Asia and the South Caucasus ranks first globally in the electrical energy industry and engineering/ICS integrators, second in OT infrastructure for biometric systems, and third place in the oil and gas sector.

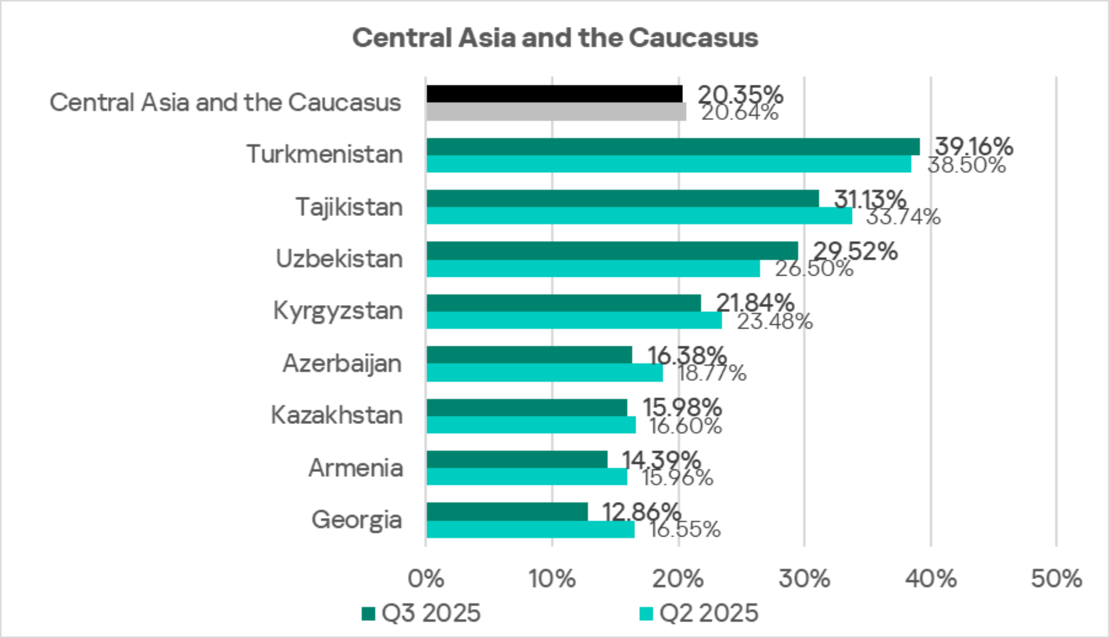
Statistics across all threats

In Q3 2025, Central Asia and the South Caucasus ranks seventh globally by the percentage of ICS computers on which malicious objects were blocked with 20.4%. This figure is 2.2 times higher than in Northern Europe, which boasts the lowest percentage among all regions.

However, this figure is gradually decreasing — in Q3 2025, it reached a three-year low.

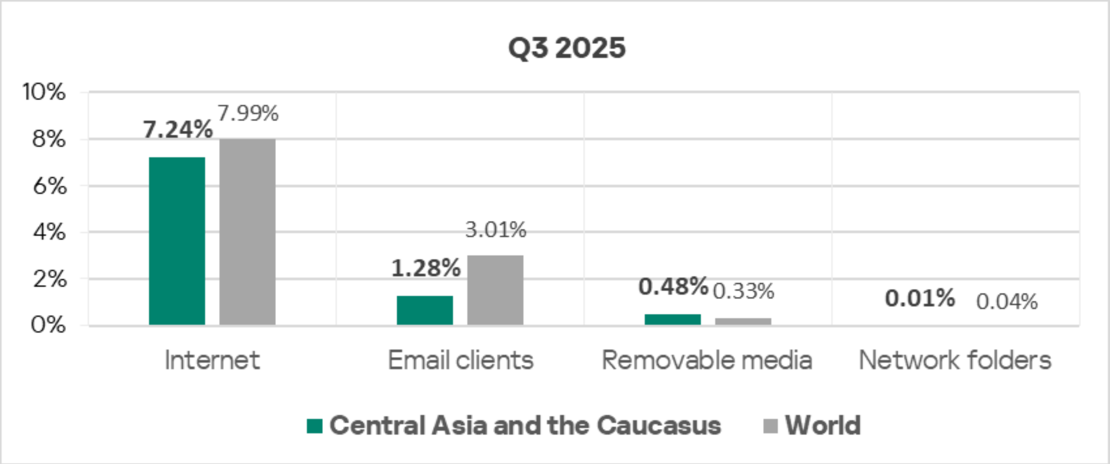


The percentage of ICS computers on which malicious objects were blocked varies among the region's countries, from 12.86% in Georgia to 39.16% in Turkmenistan.

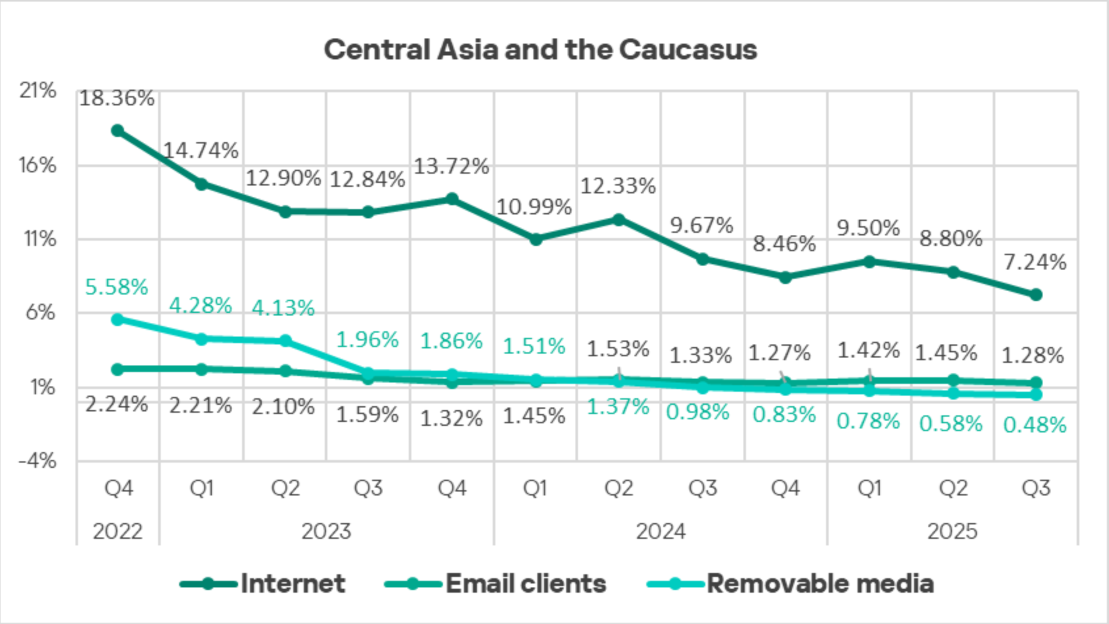


Threat sources

In Central Asia and the South Caucasus, only threats from removable media exceeded the global average on ICS computers, by 1.5 times.



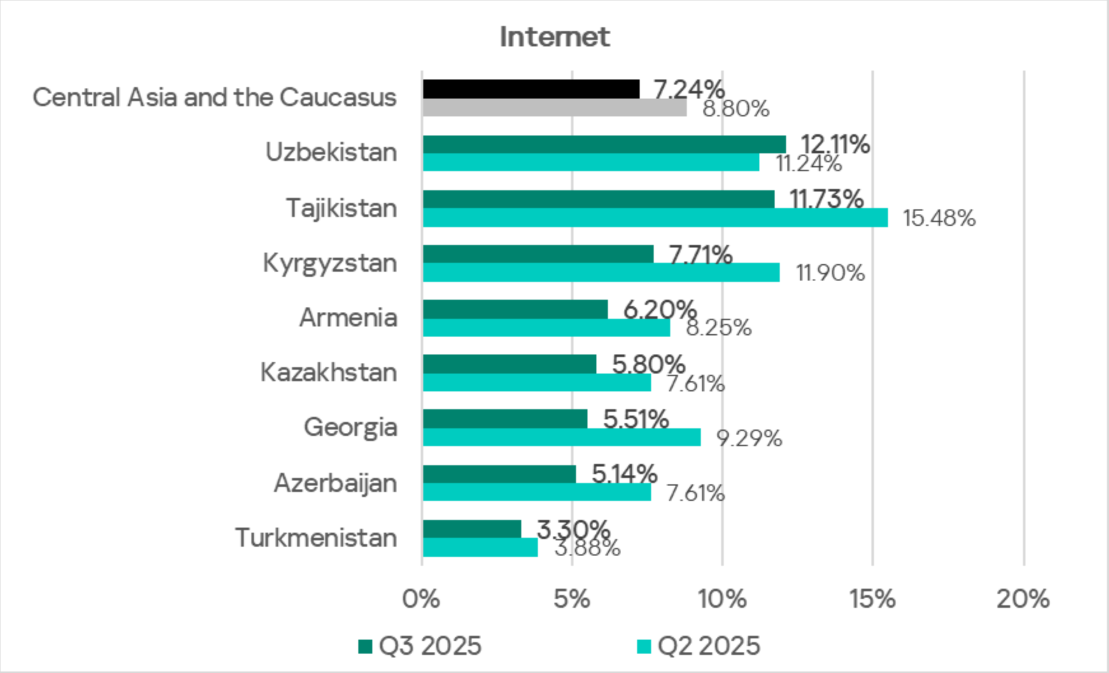
In Q3 2025, the percentage of ICS computers on which malicious objects were blocked fell across all threat sources.



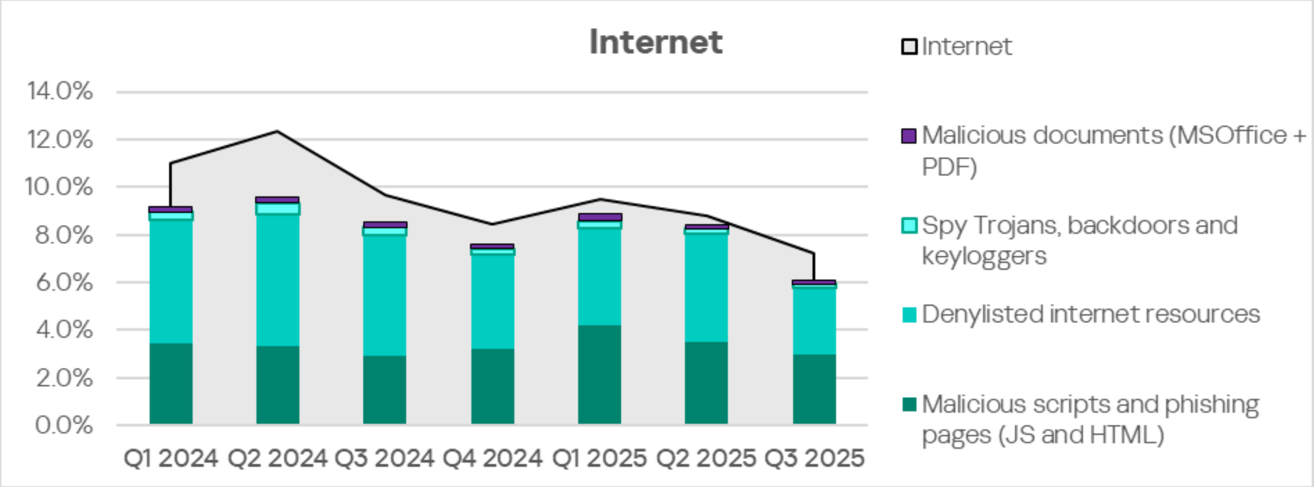
Internet

By the percentage of ICS computers on which internet threats were blocked, Central Asia and the South Caucasus ranks seventh globally at 7.24%, which is 1.6 times higher than the lowest level (Northern Europe, 6.35%).

Country-level rates range from 3.30% in Turkmenistan to 12.11% in Uzbekistan. Uzbekistan is the region's only country where this rate increased.



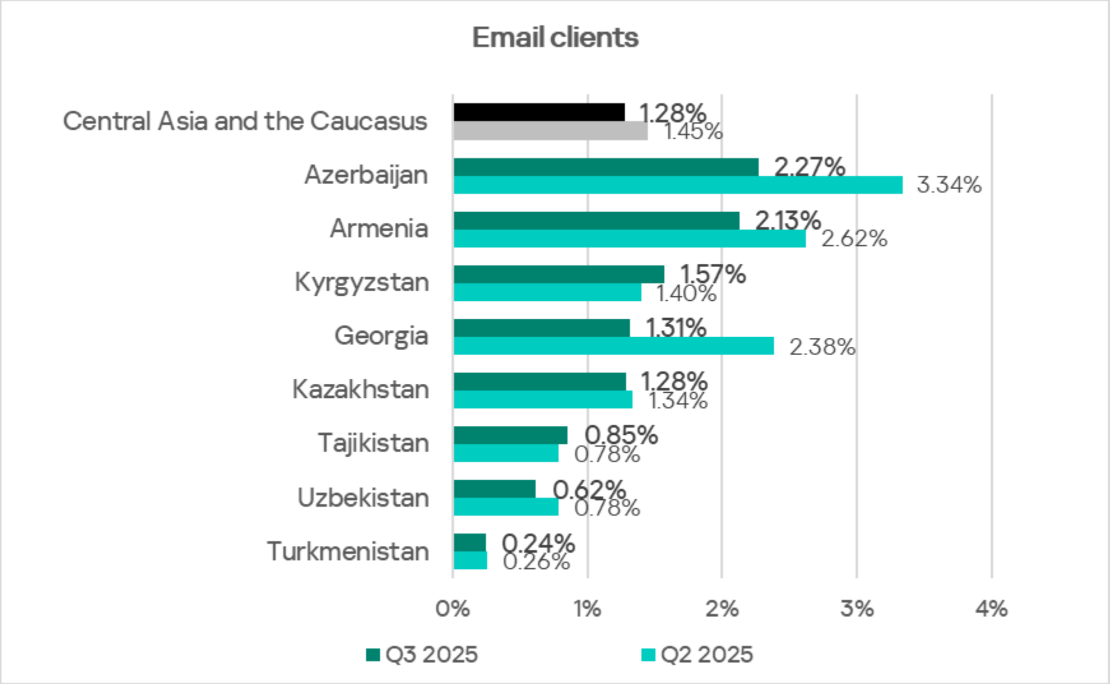
The main categories of internet threats blocked on ICS computers in the region are denylisted internet resources, malicious scripts and phishing pages, spyware, and malicious documents.



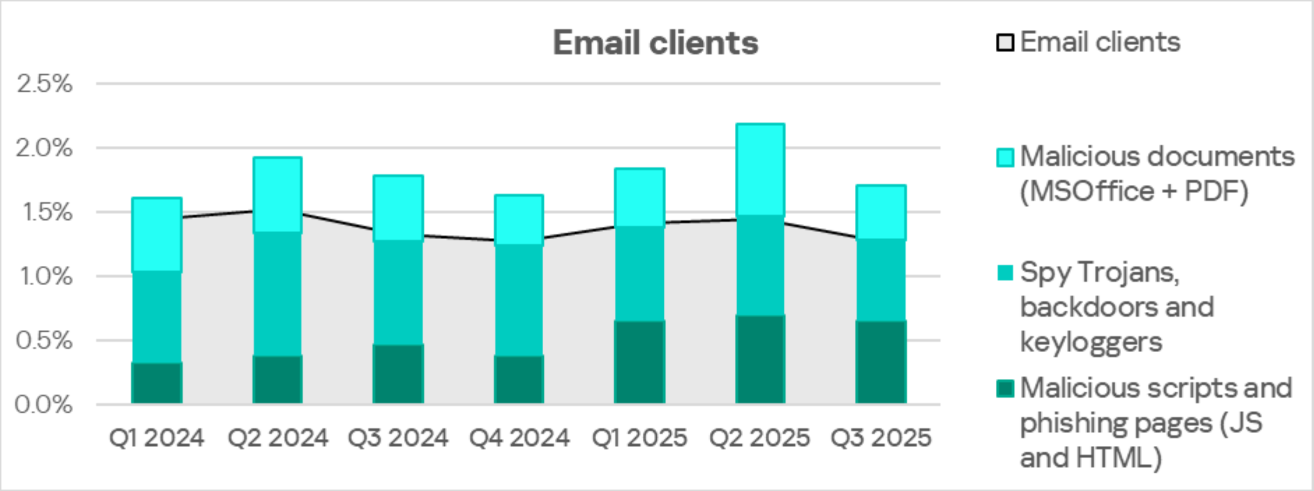
Email clients

In terms of the percentage of ICS computers on which threats from email clients were blocked, Central Asia and the South Caucasus occupies 12th place globally with 1.28%. This is 1.6 times higher than in Russia, which is last in the ranking.

Among the countries of the region, Azerbaijan leads with 2.27%, while Turkmenistan has the lowest at 0.24%.



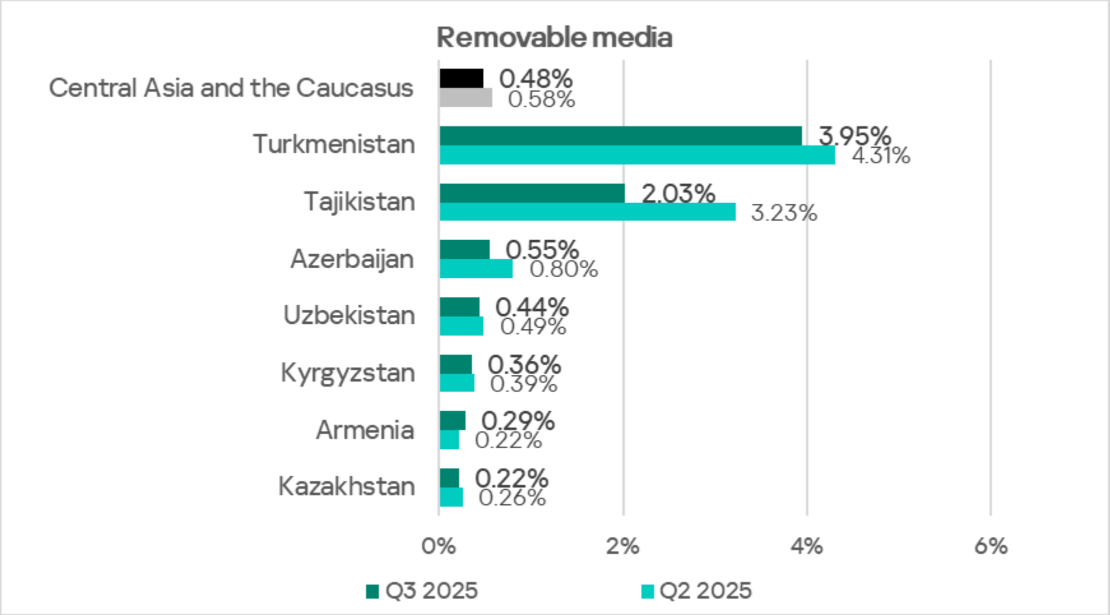
The main categories of email-borne threats blocked on ICS computers are malicious documents, spyware, malicious scripts, and phishing pages.



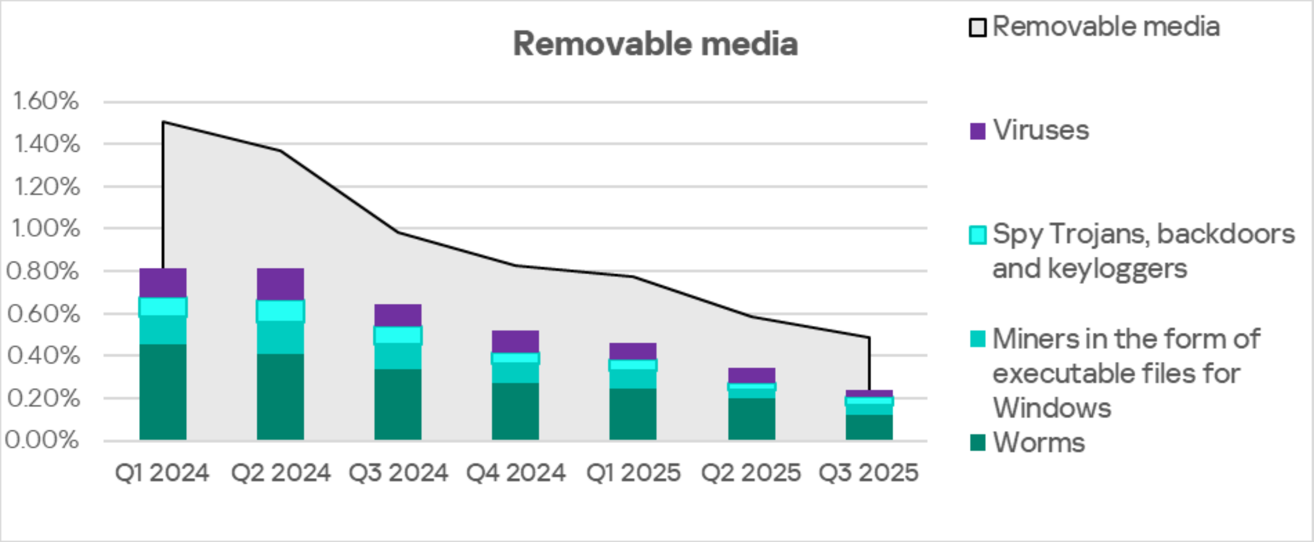
Removable media

The top six regions by the percentage of ICS computers on which threats are blocked when connecting removable media: Africa, the Middle East, and the regions of Asia. Central Asia and the South Caucasus ranks sixth with 0.48%. This figure is 9.6 times higher than in the Australia and New Zealand region, which ranks last.

Among the countries in the region, Turkmenistan leads by a wide margin in the percentage of ICS computers on which threats were blocked upon connecting removable media, with 3.95%. Notably, this country was at the bottom of the mail client threat ranking.

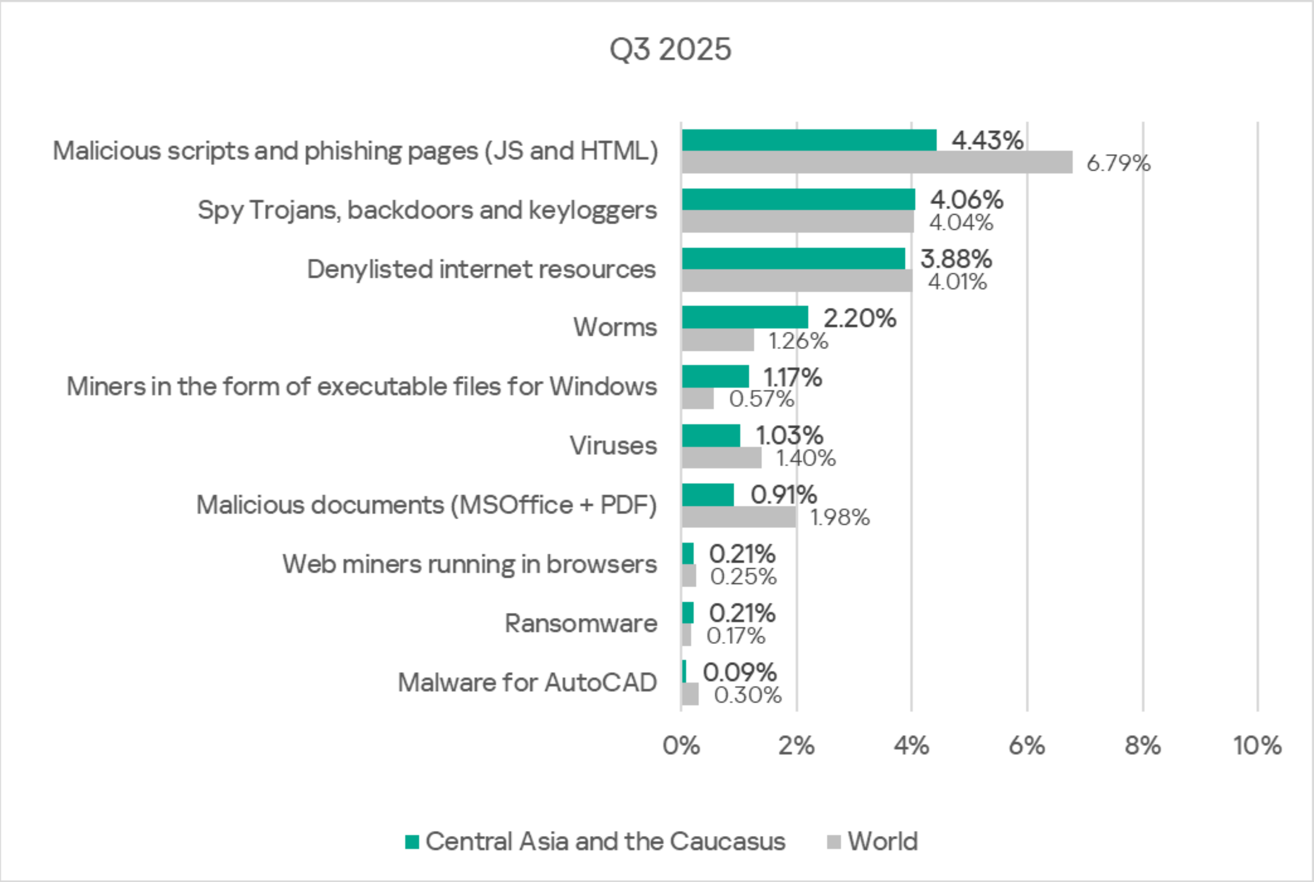


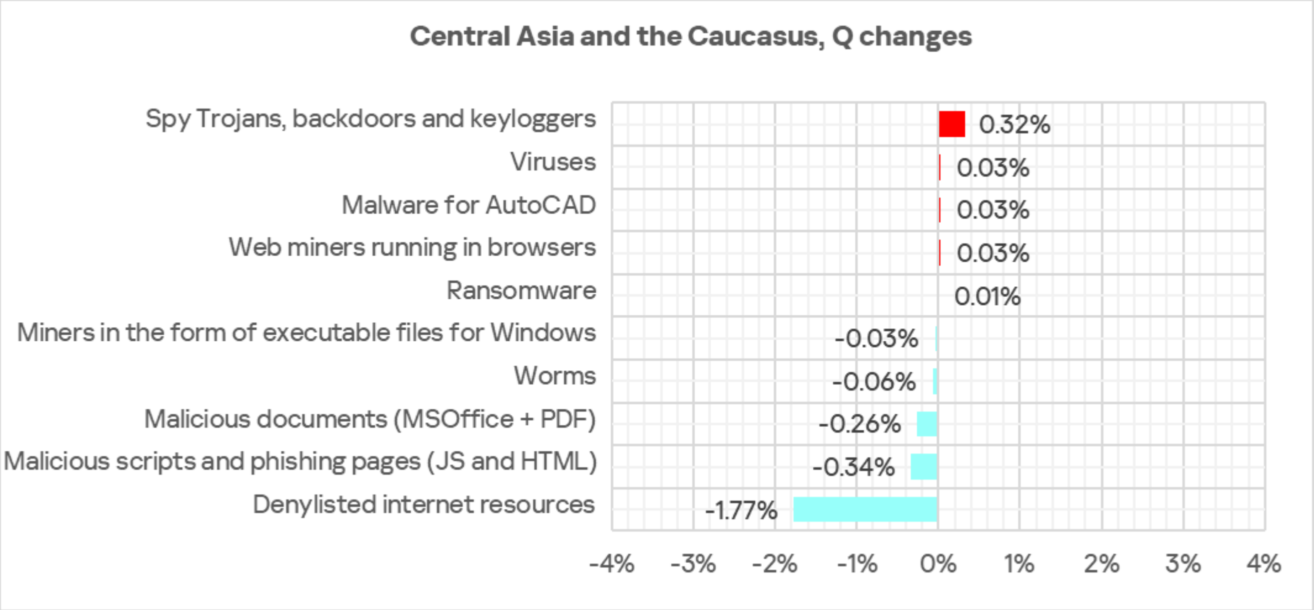
The main categories of removable media threats blocked on ICS computers are worms, viruses, spyware, and miners in the form of executable files for Windows.



By the percentage of ICS computers on which executable miners are blocked, Central Asia and the South Caucasus ranks first among all regions. In terms of worms, the region is second, following Africa.

Threat categories

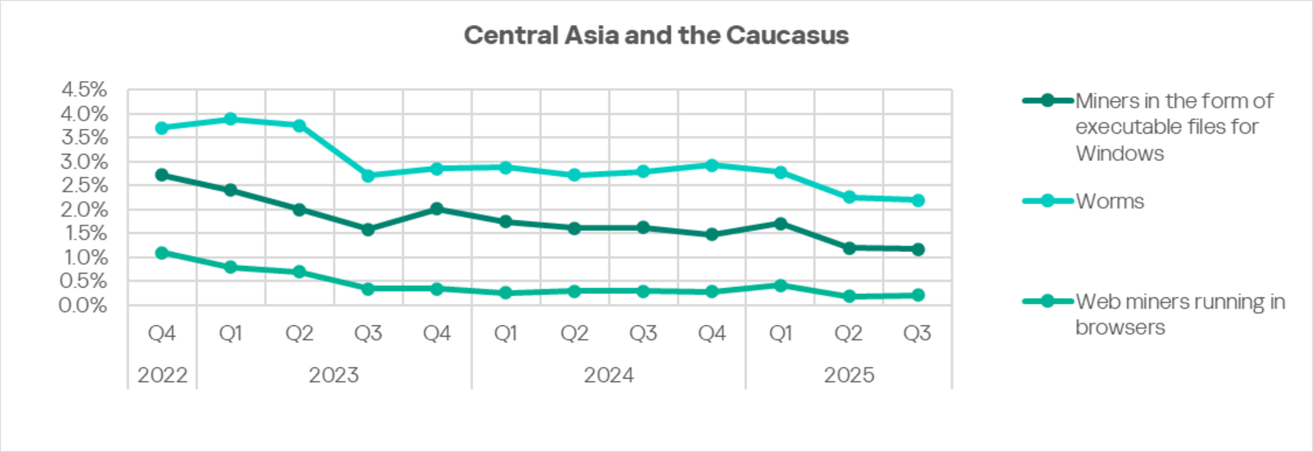




Among all threat categories in this quarter, the spyware rate in this region increased the most — slightly exceeding the global average.

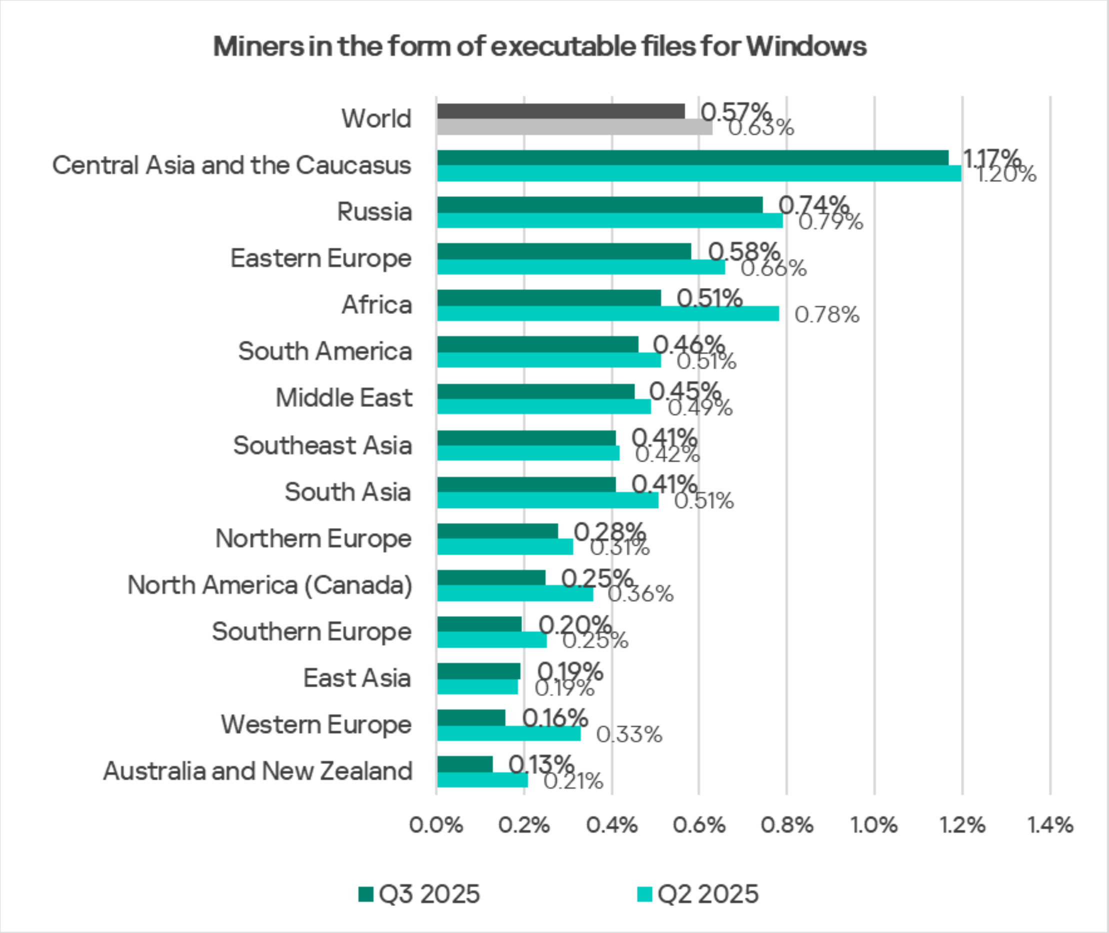
Besides spyware, this region also surpasses the global average in ICS computers with the following categories of blocked threats:

- Miners in the form of executable files for Windows: 2.1 times higher. Central Asia and the South Caucasus leads globally in this metric.
- Worms: 1.7 times higher. The region ranks second.
- Ransomware: 1.2 times higher. The region ranks fourth.

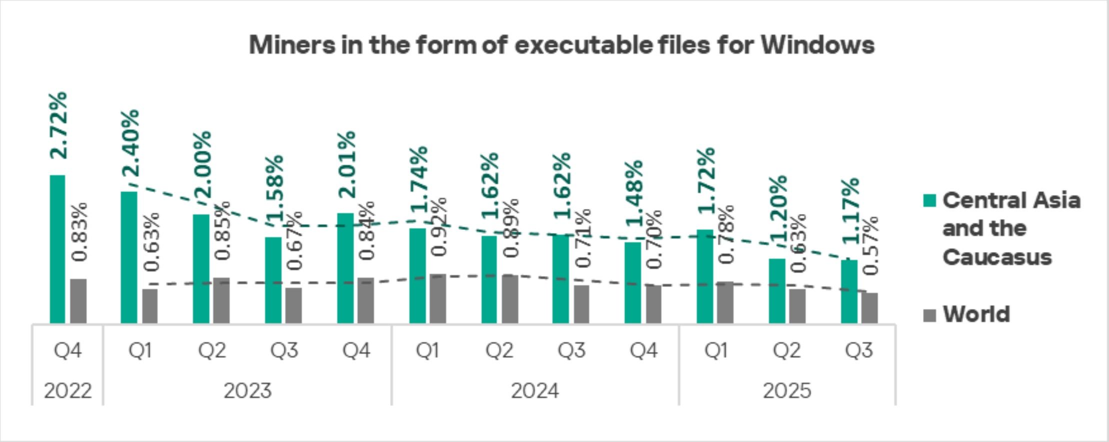


Miners in the form of executable files for Windows

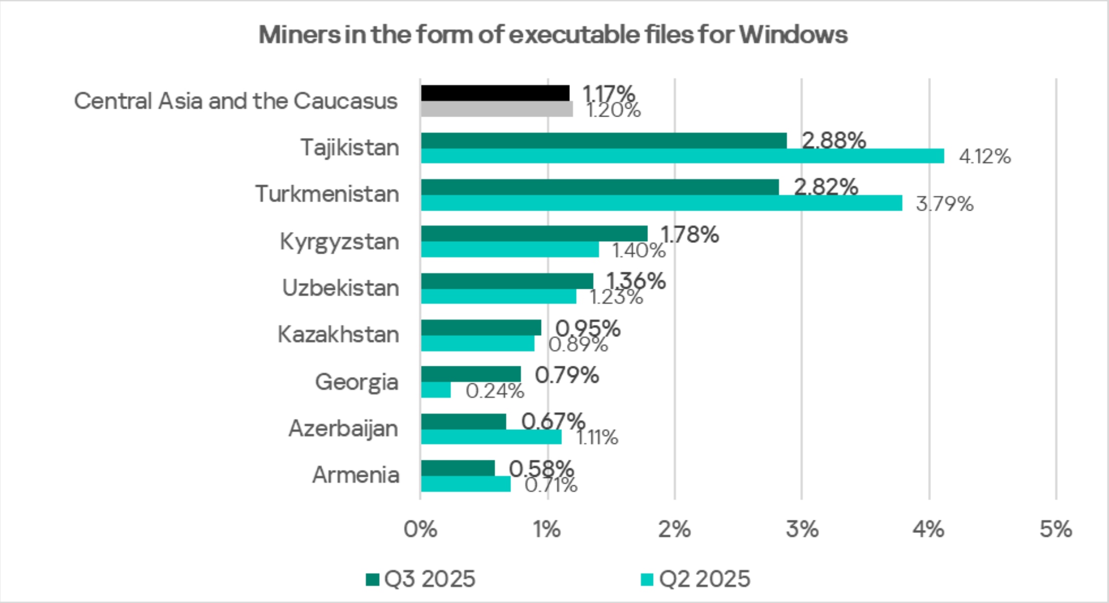
By the percentage of ICS computers with blocked miners in the form of executable files for Windows, Central Asia and the South Caucasus leads all regions with 1.17%. This is 9 times higher than Australia and New Zealand, which has the lowest rate among all regions.



The percentage of ICS computers with blocked miners in the form of executable files for Window decreased for the second consecutive quarter, reaching a three-year low.



Among the countries in the region, Tajikistan (2.88%) and Turkmenistan (2.82%) lead in the percentage of ICS computers with blocked miner executables. In both countries, this figure decreased noticeably in this quarter.

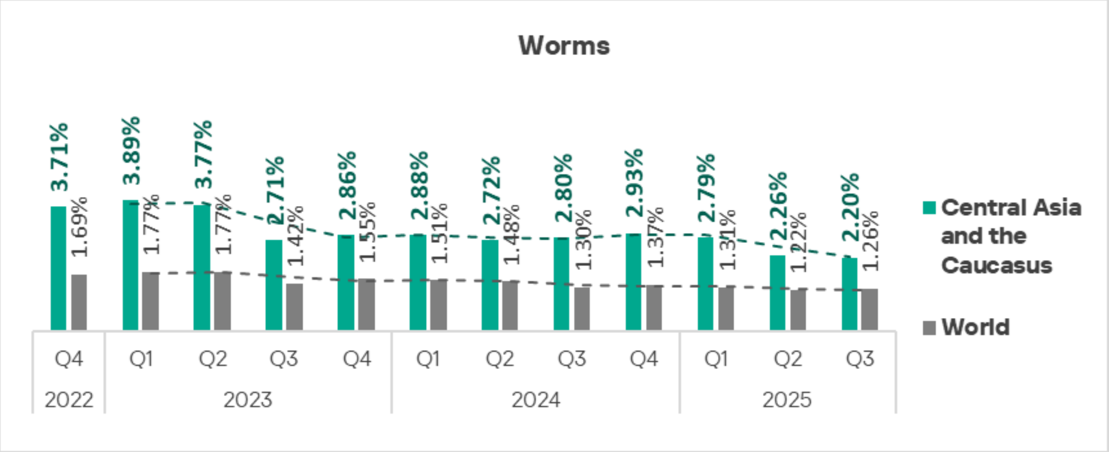


Such threats spread via the internet and removable media. Tajikistan takes second place among the region's countries in internet threats, while Turkmenistan leads in ICS computers where threats were blocked upon connecting removable media.

Worms

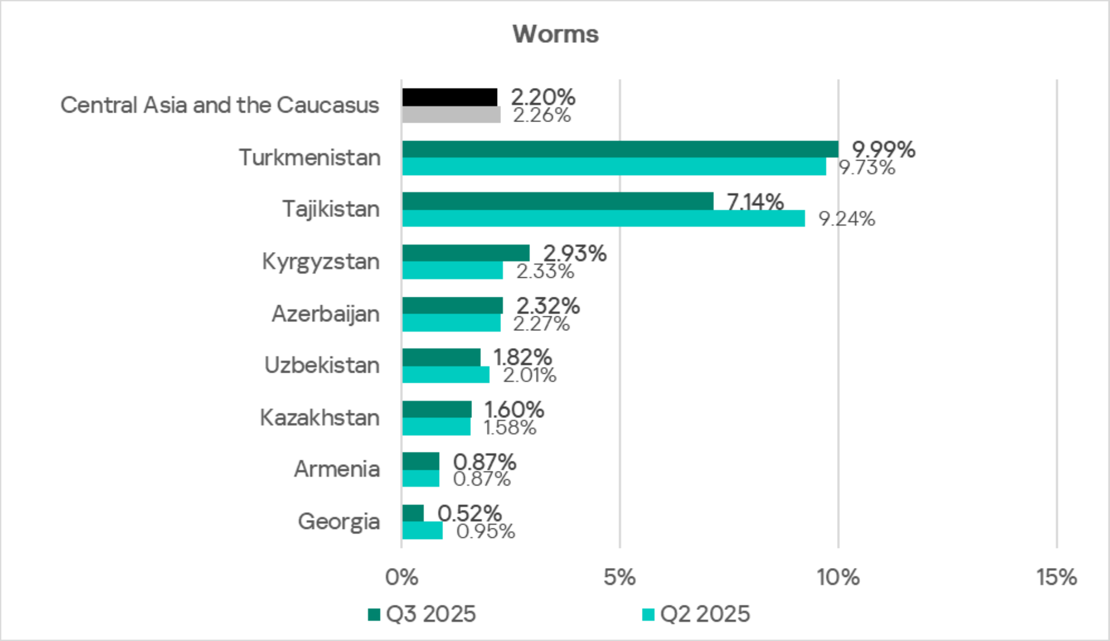
By the percentage of ICS computers with blocked worms, Central Asia and the South Caucasus ranks second among regions, behind only Africa. The rate for the region is 2.20%, which is 10 times higher than in Northern Europe (the lowest globally).

This figure has decreased for the third consecutive quarter. In Q3 2025, it reached a three-year low.



Among threat categories in the region, worms place fourth. Russia is the only other region with such a high worm ranking.

Among the region's countries and territories, Tajikistan leads in the percentage of ICS computers with blocked worms, at 9.99%.



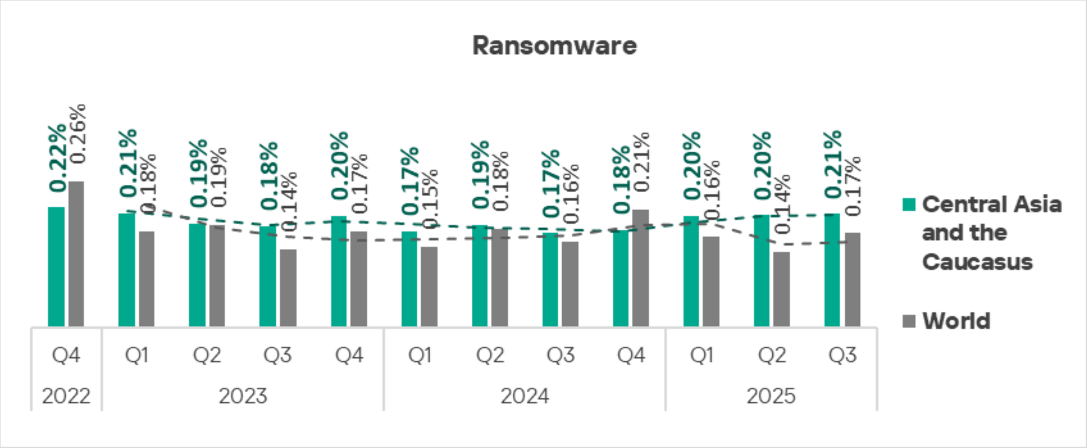
These threats spread mainly through removable media. The leaders Tajikistan and Turkmenistan also lead by the percentage of ICS computers on which threats were blocked upon connecting removable media.

Notably, Tajikistan and Turkmenistan also lead in terms of miners in the form of executable files for Windows infections.

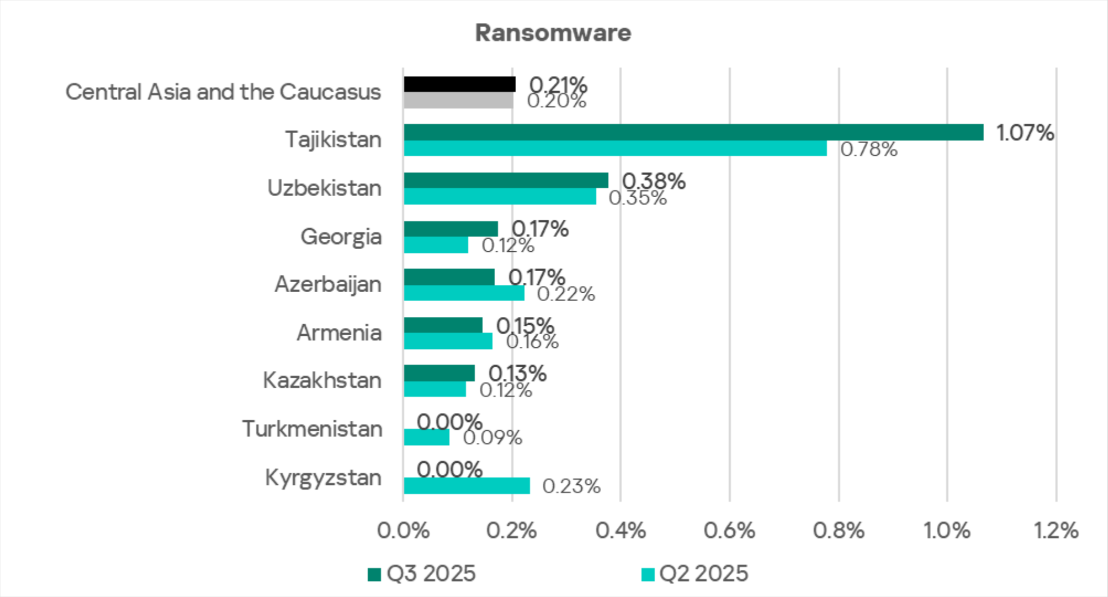
Ransomware

By the percentage of ICS computers with blocked ransomware, Central Asia and the South Caucasus ranks fourth globally with 0.21%. The region's rate is 4.2 times higher than Northern Europe, which ranks last.

Meanwhile the region's ransomware rate is fairly stable, increasing slightly this quarter.

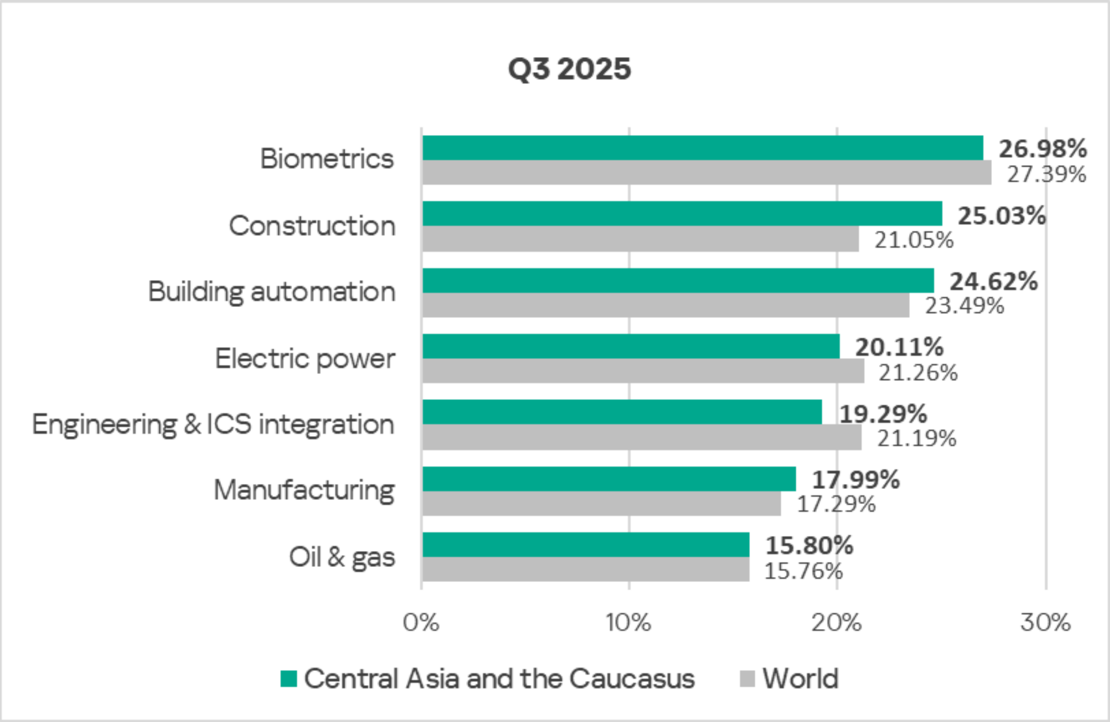


Among the region's countries, Tajikistan has a significant lead in the percentage of ICS computers with blocked ransomware, at 1.07%.

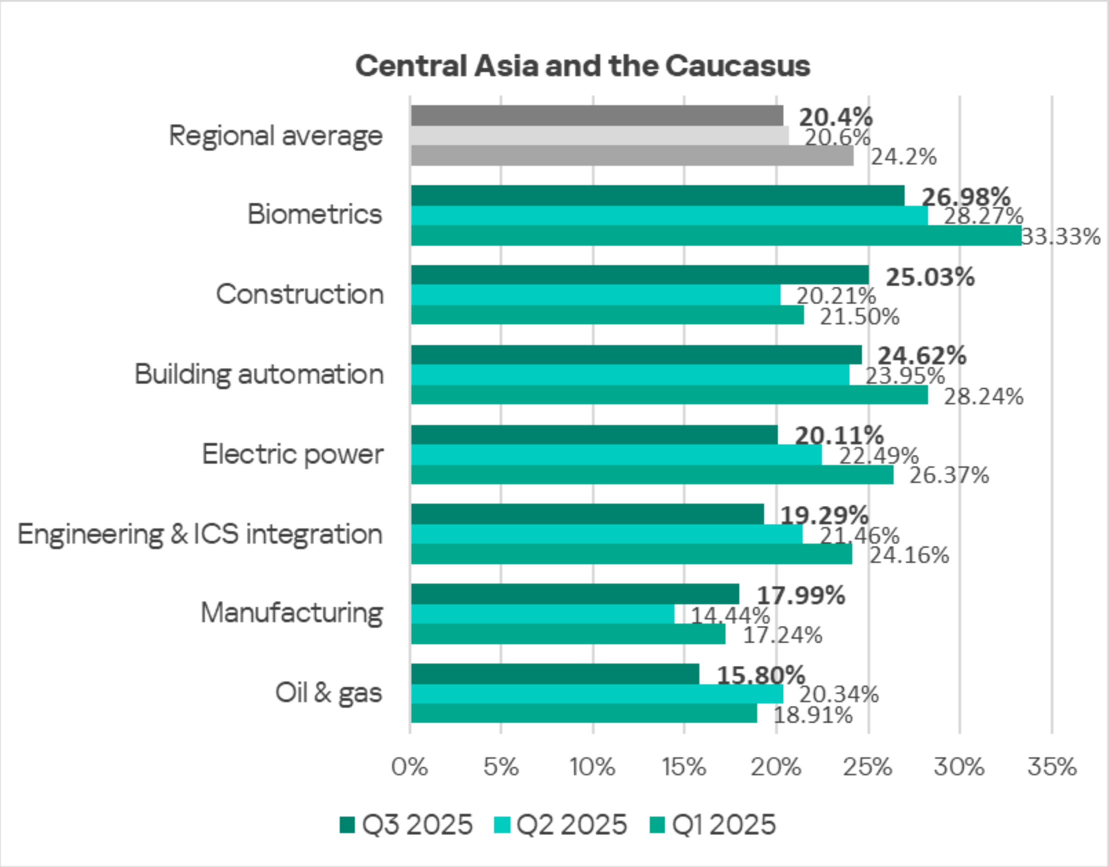


Industries

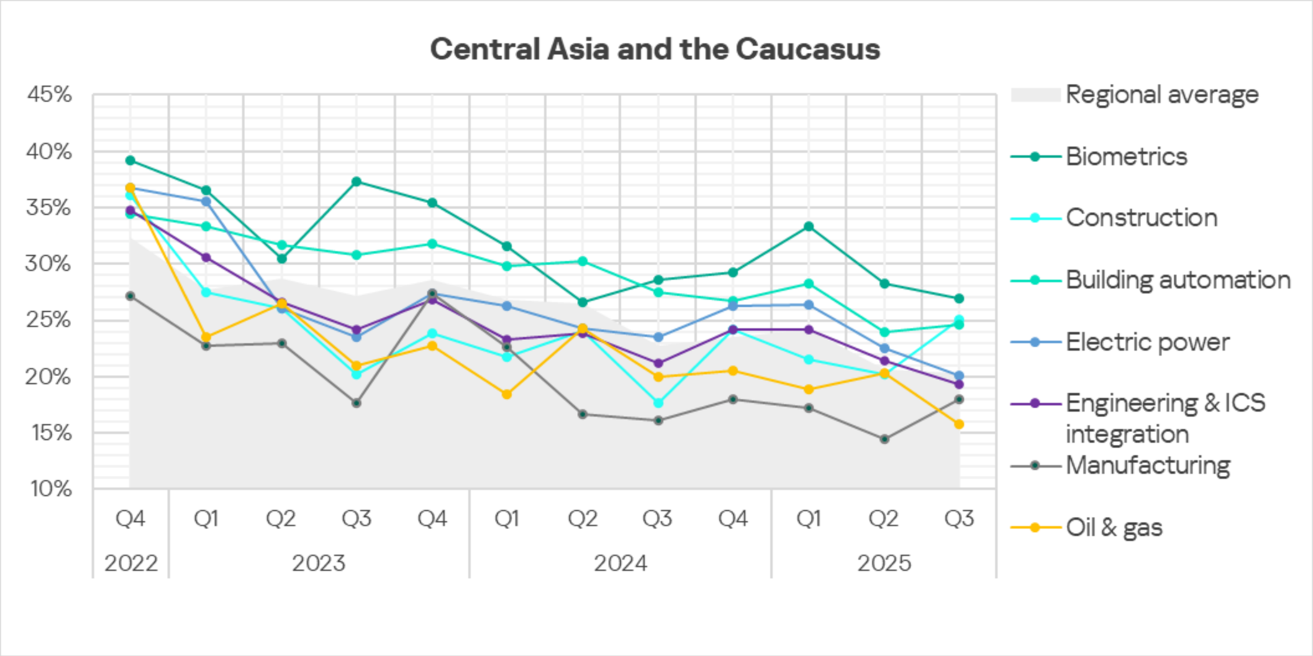
Among the region's industries analyzed in the report, threats are most frequently encountered in OT infrastructure for biometric systems.



The construction, building automation, and manufacturing sectors all encountered threats more frequently than the global average, with the biggest difference in construction: 1.2 times higher. The figure also grew in these industries in this quarter.



Trends across all industries generally show an improvement (declining rates), although some industries display 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. The color red signifies that the figure approaches the maximum.

Threat source indicators for industries in Central Asia and the South Caucasus, Q3 2025

Industry / Threat source	Biometrics	Building automation	Electric power	Engineering & ICS integration	Oil & gas	Construction	Manufacturing	Threat category total in the region
Internet	11.21%	10.52%	8.08%	9.90%	12.40%	7.60%	7.53%	7.24%
Email clients	5.08%	3.23%	2.73%	0.98%	5.81%	2.10%	1.41%	1.28%
Removable media	1.82%	0.78%	0.54%	0.38%	0.39%	0.20%	0.67%	0.48%
Network folders	0.08%	0.09%	0.00%	0.02%	0.00%	0.05%	0.00%	0.01%
Industry total in the region	26.98%	24.62%	20.11%	19.29%	15.80%	25.03%	17.99%	

Threat category indicators for industries in Central Asia and the South Caucasus, Q3 2025

Industry / Threat category	Biometrics	Building automation	Electric power	Engineering & ICS integration	Oil & gas	Construction	Manufacturing	Threat category total in the region
Denylisted internet resources	5.18%	4.33%	6.18%	4.28%	4.42%	5.16%	3.96%	3.88%
Malicious scripts and phishing pages (JS and HTML)	7.08%	5.51%	5.65%	5.14%	4.15%	5.41%	6.12%	4.43%
Spy Trojans, backdoors and keyloggers	7.08%	6.13%	4.34%	3.66%	2.14%	2.77%	4.32%	4.06%
Worms	3.00%	2.93%	3.15%	1.48%	1.74%	2.26%	2.88%	2.20%
Miners in the form of executable files for Windows	1.91%	1.44%	1.45%	1.19%	1.47%	1.89%	1.08%	1.17%
Malicious documents (MSOffice + PDF)	3.54%	1.44%	1.18%	0.96%	0.13%	0.38%	0.36%	0.91%
Viruses	1.63%	1.44%	1.45%	1.14%	0.94%	1.76%	2.52%	1.03%
Ransomware	0.54%	0.29%	0.53%	0.44%	0.13%	0.13%	0.00%	0.21%
Web miners running in browsers	0.27%	0.26%	0.79%	0.29%	0.54%	0.88%	0.36%	0.21%
Malware for AutoCAD	0.00%	0.05%	0.13%	0.10%	0.00%	0.63%	0.00%	0.09%
Industry total in the region	26.98%	24.62%	20.11%	19.29%	15.80%	25.03%	17.99%	

In all industries, the main source of threats is the internet. Therefore, the relevant threat categories include denylisted links, malicious scripts, and phishing pages.

Central Asia and the South Caucasus leads 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.

Central Asia and the South Caucasus has the highest rate for miners in the form of executable files for Windows among all regions globally.

Another major threat is worms.

The region ranks second globally in worm detections across all industries, except for: building automation (1st place), electrical energy industry (1st place), and engineering and ICS integrators (4th place).

Ransomware rates are also high across the region's industries.

In terms of ransomware activity, Central Asia and the South Caucasus rank first globally in electrical energy industry and engineering/ICS integrators, second in OT infrastructure for biometric systems, and third in the oil and gas sector.

Biometric systems

Central Asia and the South Caucasus ranks fifth among regions in the percentage of ICS computers on which malicious objects were blocked in OT infrastructure for biometric systems.

Among all industries and regions, OT infrastructure for biometric systems in Central Asia and the South Caucasus ranks:

- First place in the percentage of ICS computers on which miners in the form of executable files were blocked.
- Third place in the percentage of ICS computers on which ransomware was blocked.

Among regions, this metric ranks:

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

The regional industry rankings for OT infrastructure for biometric systems is as follows:

- First place in the percentage of ICS computers on which email client threats were blocked.

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

Construction

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

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

- First place in the percentage of ICS computers on which web miners were blocked.
- Second place in the percentage of ICS computers on which miners in the form of executable files were blocked.

Within industries in the region, construction ranks:

- Third place in the percentage of ICS computers on which threats from removable media are blocked.
- Fourth place in internet and network folder threats.
- First place in the percentage of ICS computers on which miners of both categories are blocked.
- Second place in worms and fourth in denylisted internet resources.

Among industries in regions, the construction industry has the following rankings:

- First place in the percentage of ICS computers on which internet threats were blocked.
- Third place for removable media threats.
- First place in the percentage of ICS computers on which web miners and malware for AutoCAD were blocked.
- Second place in miners in the form of executable files, as well as viruses.
- Third place in denylisted internet resources.

Building automation

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

Among all regions and industries, building automation in Central Asia and the South Caucasus ranks:

- Fifth place in the percentage of ICS computers on which miners in the form of executable files were blocked.

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

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

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

- Second place in mail client threats.
- Second place in the percentage of ICS computers on which malicious documents and spyware were blocked.
- Third place in worms.

Electric power

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

Among all regions and industries, electrical energy industry in this region ranks:

- Second place in the percentage of ICS computers on which web miners were blocked.
- Fourth place in the percentage of ICS computers on which miners in the form of executable files for Windows, worms, and ransomware were blocked.

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

- First place in the percentage of ICS computers on which both types of miners, worms, and ransomware are blocked.
- Second place in denylisted internet resources.

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

- Third place in the percentage of ICS computers on which threats from the internet and email clients were blocked.
- First place in the percentage of ICS computers on which denylisted internet resources and worms were blocked.

- Second place in web miners, ransomware, and malware for AutoCAD.
- Third place in malicious scripts and phishing pages, malicious documents, and spyware.

Engineering and ICS integrators

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

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

- First place in the percentage of ICS computers on which miners in the form of executable files for Windows and ransomware are blocked.
- Fourth place in worms.

Among industries in the region, engineering and ICS integrators have the following rankings:

- Third place in the percentage of ICS computers on which ransomware and malware for AutoCAD were blocked.

Manufacturing

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

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

- First place in the percentage of ICS computers on which threats from removable media are blocked.
- First place in the percentage of ICS computers on which miners in the form of executable files for Windows are blocked.
- Second place in web miners and worms, third in spyware and viruses, and fourth in denylisted internet resources.

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

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

Oil and gas

Central Asia and the South Caucasus ranks fourth globally in the percentage of ICS computers on which malicious objects were blocked in the oil and gas sector.

Oil and gas sector in Central Asia and the South Caucasus has the following global ranking among all industries in all regions:

- Third place in the percentage of ICS computers on which miners in the form of executable files were blocked.

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

- First by percentage of ICS computers on which threats from email clients were blocked.
- Second place in internet threats, third in terms of removable media threats.
- First place in the percentage of ICS computers on which miners in the form of executable files for Windows are blocked.
- Second place in denylisted internet resources, web miners, and worms.
- Third place in ransomware.

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

- Third in the percentage of ICS computers on which miners of both categories 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 as attacked if a Kaspersky security solution blocked one or more threats on that computer during the period under review: a month, six months, or a year depending on the context as can be seen in the charts above. To calculate the percentage of machines whose malware infection was prevented, we take the ratio of the number of computers attacked during the period under review to the total number of computers in the selection from which we received anonymized information during the same period.

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global Kaspersky project aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky ICS CERT

ics-cert@kaspersky.com