Kaspersky ICS CERT

kaspersky

Threat landscape for industrial automation systems

Asia. Q2 2025

19.09.2025

Version 1.0

South-East Asia

Key cybersecurity issues in the region

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

South-East 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 South-East 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 figure exceeds the global average by a factor of 5.5, making it the highest value in the world.

Malware for AutoCAD is in second-to-last place in the global ranking of threat categories by percentage of ICS computers on which various threats were blocked, while in the regional ranking, it is in sixth place, with a percentage that exceeds the global average by a factor of 7.9 and is the highest value in the world.

Lack of segmentation in enterprise networks in the region

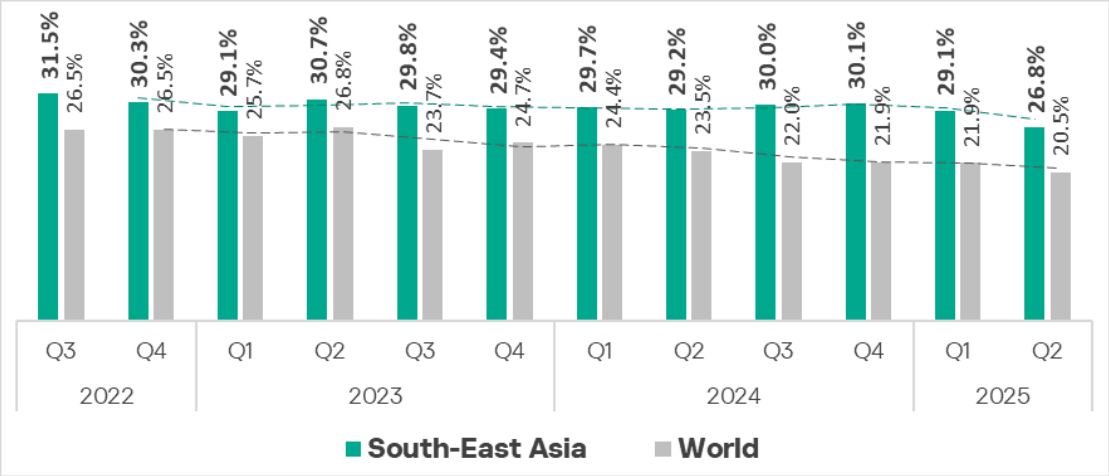
South-East Asia ranks second among regions in terms of the percentage of ICS computers on which threats from network folders were blocked, at 0.11%. This figure is 2.1 times higher than the global average.

This is mainly due to the situation in Vietnam, which leads the region by a wide margin in terms of threats blocked in network folders, viruses, and malware for AutoCAD.

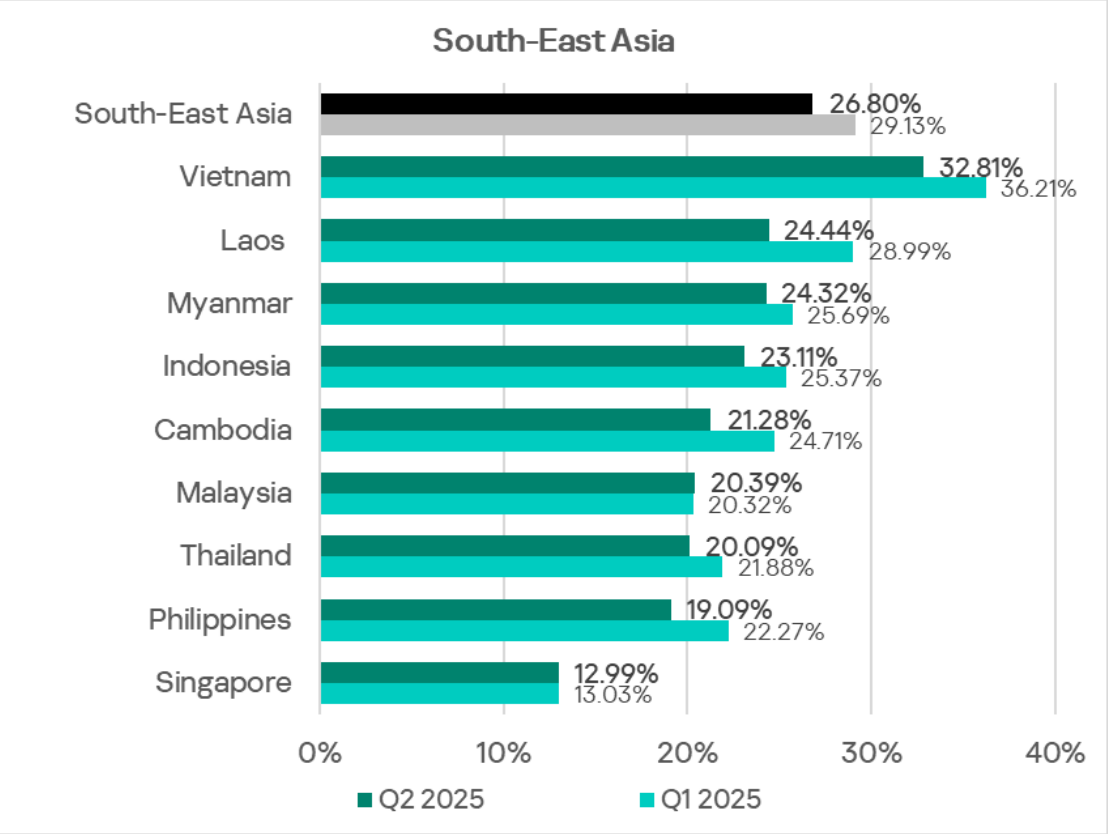
Statistics across all threats

South-East Asia ranks second globally in terms of the percentage of ICS computers on which malicious objects were blocked, at 26.8%. This figure is 1.3 times higher than the global average and 2.4 times higher than the lowest regional figure, recorded in Northern Europe.

In Q2 2025, the percentage of ICS computers on which malicious objects were blocked in South-East Asia decreased by a notable 2.3 p.p. The region's percentage figure has been declining for two consecutive quarters.

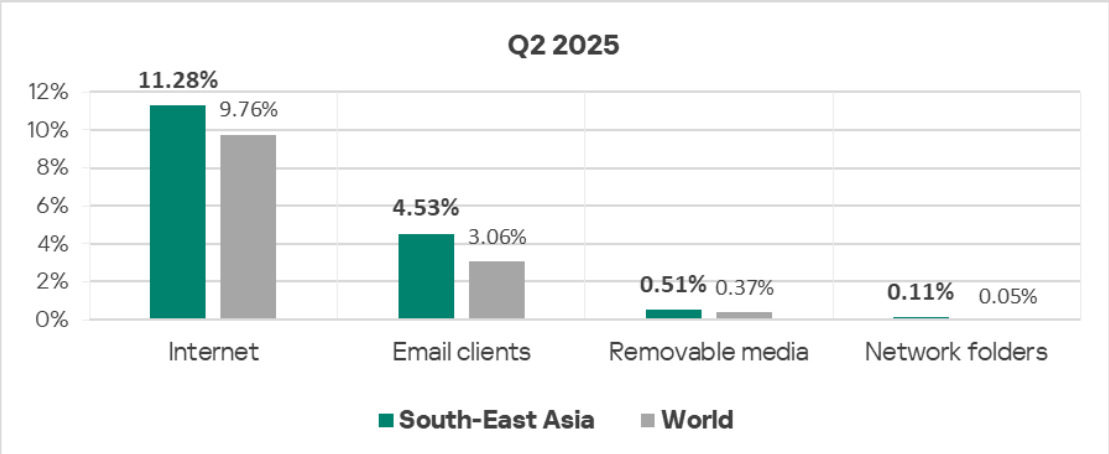


Across the countries of the region, the percentage of ICS computers on which malicious objects were blocked ranges from 12.99% in Singapore to 32.81% in Vietnam. The figures for the other countries range from 19% to 25%.

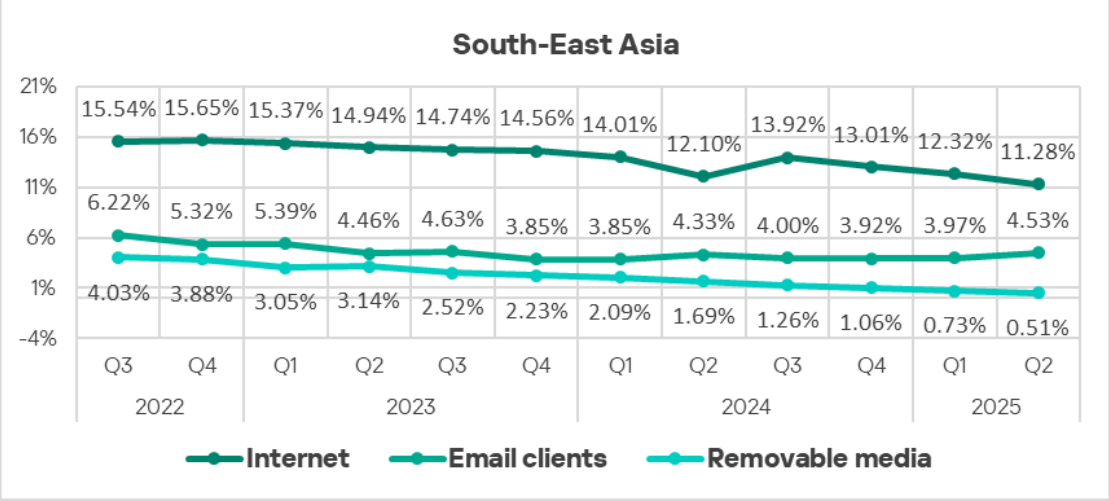


Threat sources

The percentages of ICS computers on which threats from different sources were blocked in the region are higher than the respective global averages for all threat sources. Compared to global averages, the percentage of ICS computers on which internet threats were blocked is 1.2 times higher, email clients — 1.5 times higher, removable media — 1.4 times higher, network folders — 2.2 times higher.



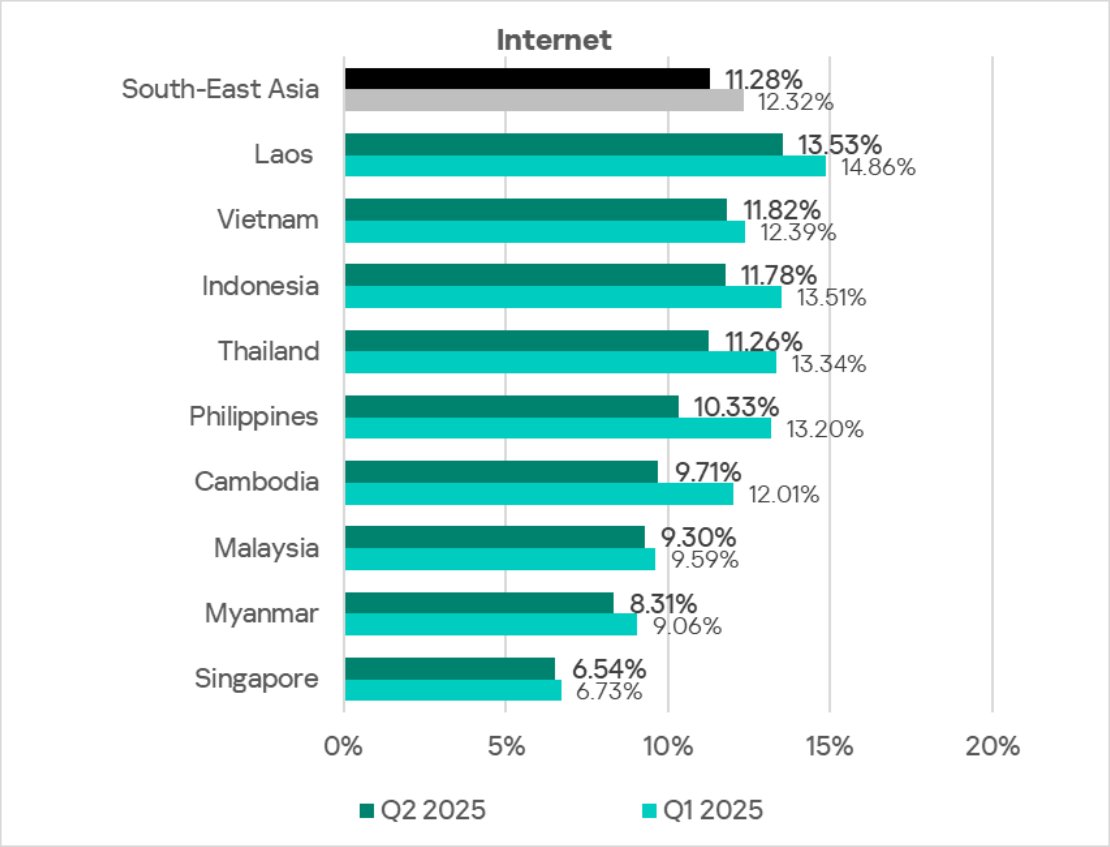
Among all threat sources, the only percentage that increased was for email clients.



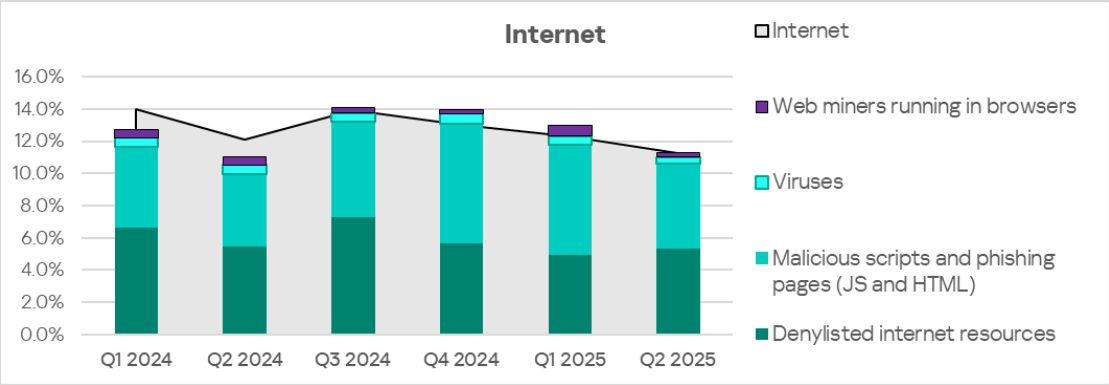
Internet

In terms of the percentage of ICS computers on which threats from the internet were blocked, South-East Asia ranks second among regions, with a figure that is 1.8 times higher than the lowest regional figure, recorded in East Asia.

Country figures in the region range from 6.54% in Singapore to 13.53% in Laos.

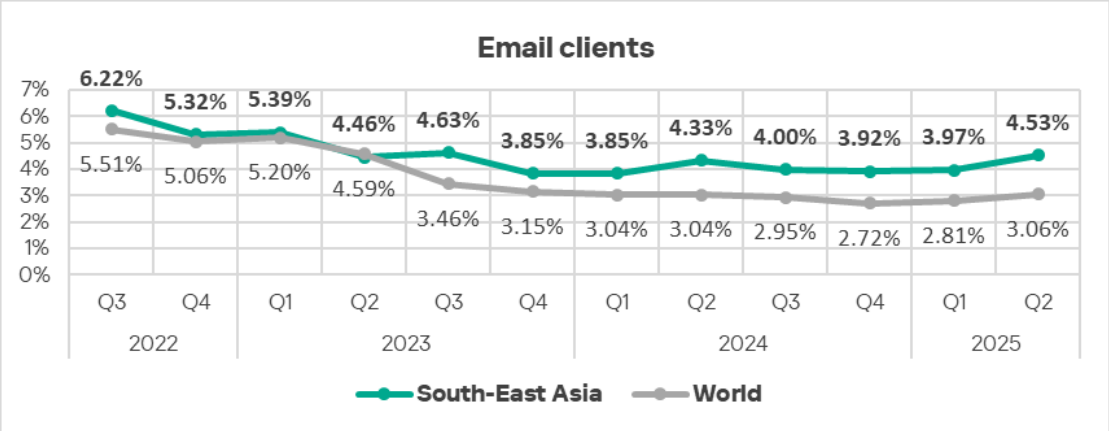


The main categories of internet threats blocked on ICS computers in the region are: denylisted internet resources, malicious scripts and phishing pages, viruses, and web miners.

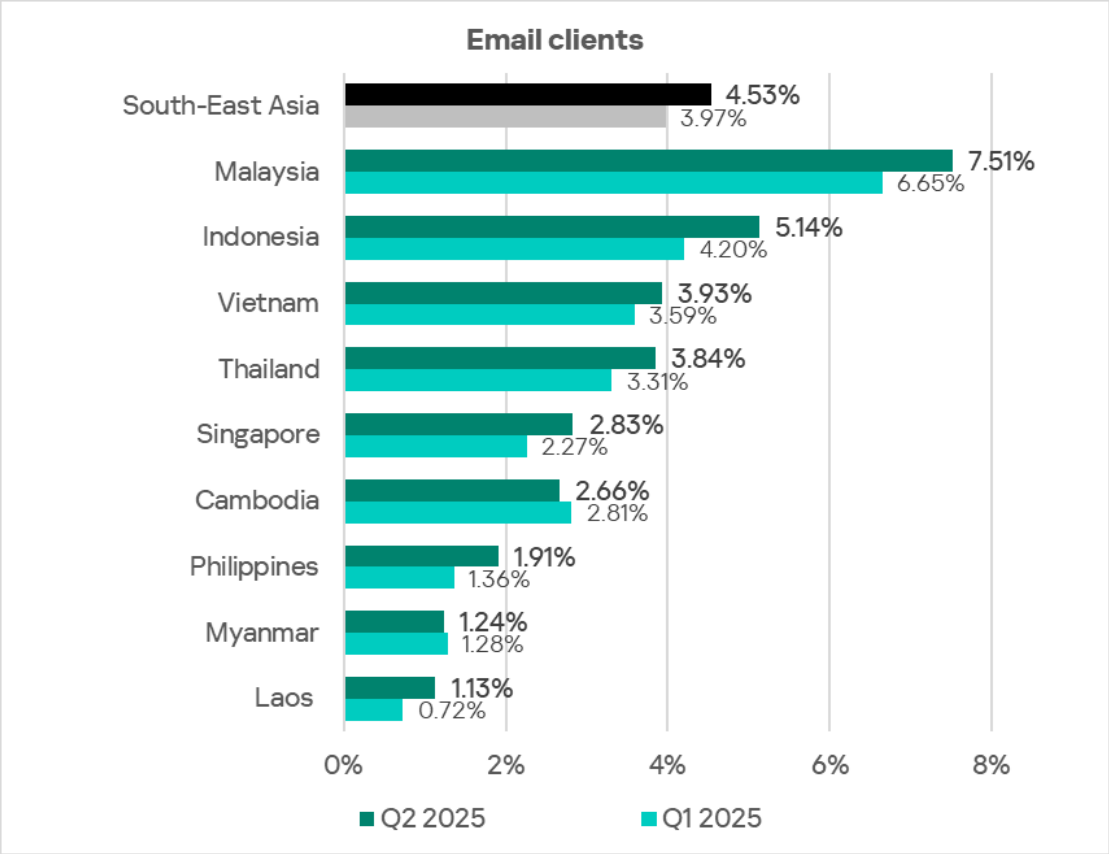


Email clients

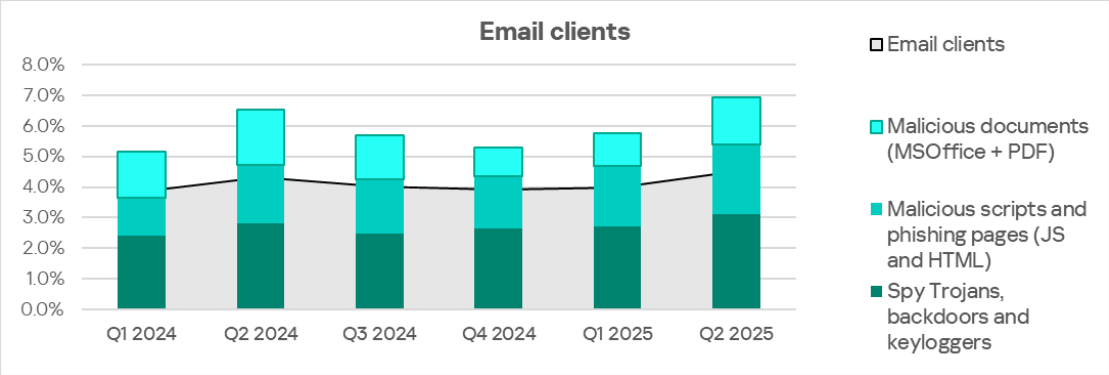
The percentage of email clients as a source of threats in the region has been increasing for two consecutive quarters.



Among the countries in the region, Malaysia leads by a wide margin, with 7.51%. The lowest percentage of ICS computers on which threats from email clients were blocked was in Laos, at 1.13%.



The main categories of email threats blocked on ICS computers include malicious documents, malicious scripts and phishing pages, and spyware. In the ranking of regions for spyware, South-East Asia ranks third.

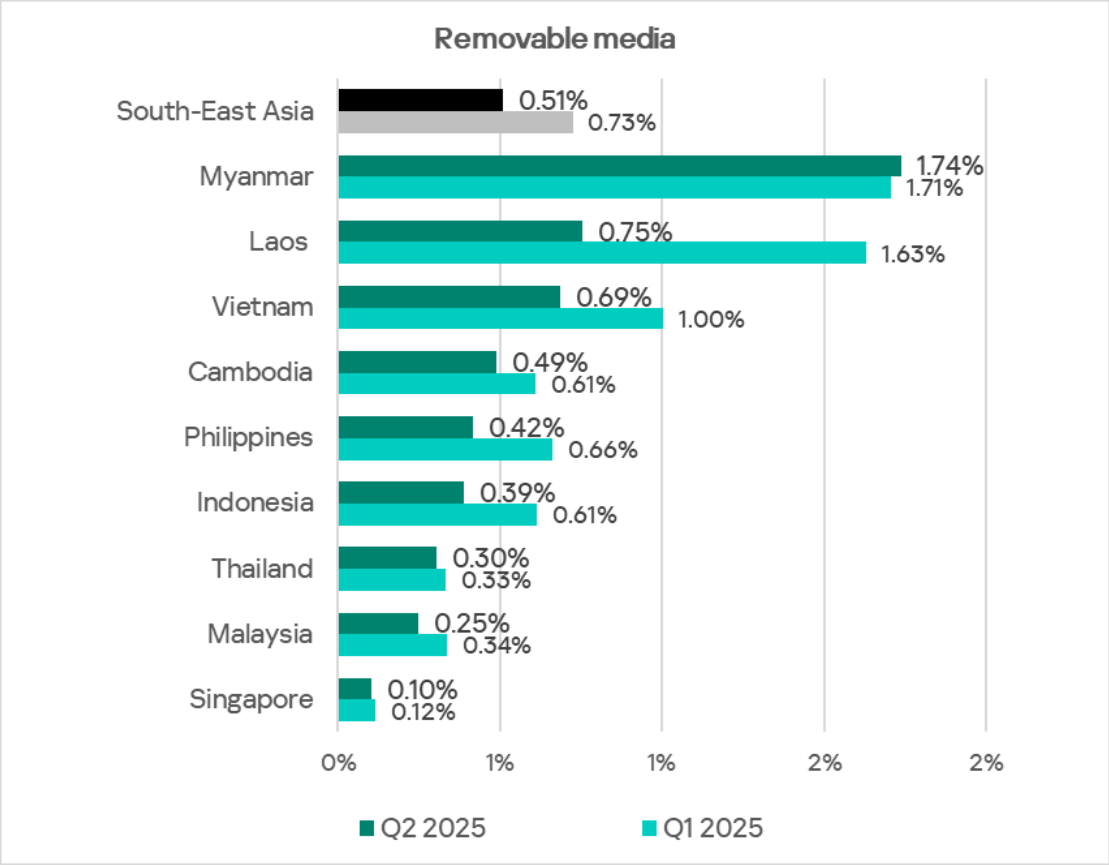


Removable media

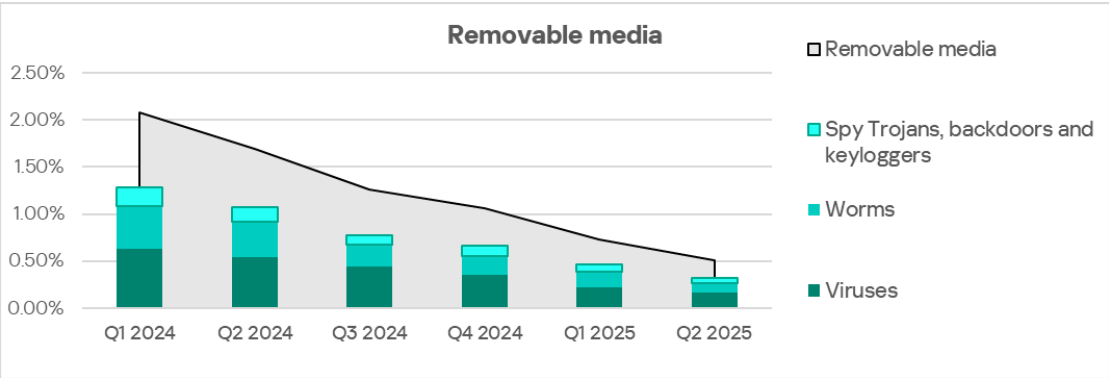
In the ranking of regions based on the percentage of ICS computers on which threats were blocked when removable media were connected, the top six positions are held by Africa and different regions of Asia. South-East Asia ranks sixth, with 0.51%.

Although South-East Asia has the lowest percentage among the Asian regions, its percentage value is 2.2 times higher than that of Eastern Europe, which immediately follows it in the ranking. Compared to North America (Canada), which ranks last, the percentage value is 18.9 times higher.

Among the countries of the region, Myanmar leads by a wide margin, with 1.74% of ICS computers on which threats from removable media were blocked. Notably, the country was second to last in the ranking for email clients. Percentage values for the other countries range from 0.10% in Singapore to 0.75% in Laos.



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

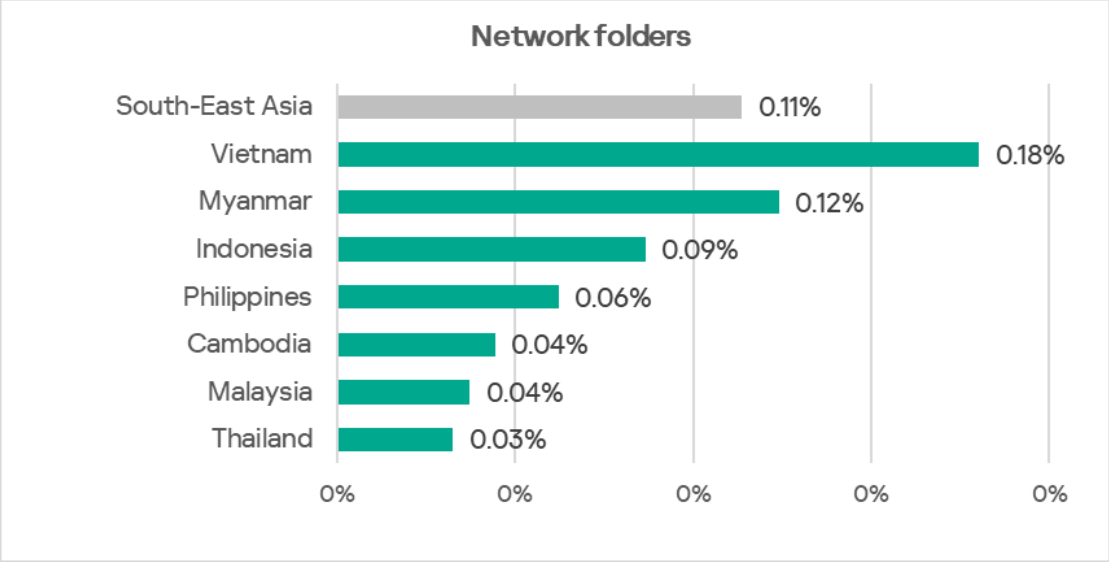


Network folders

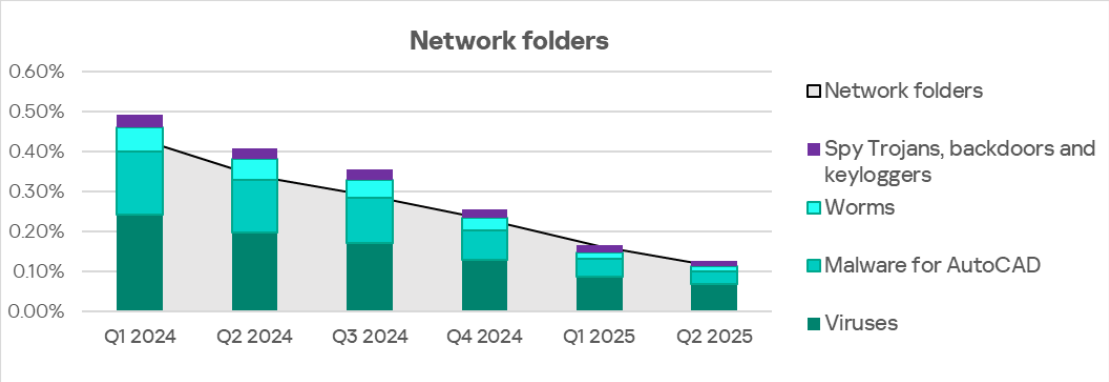
South-East Asia ranks second among regions in terms of the percentage of ICS computers on which threats from network folders were blocked, at 0.11%, second only to East Asia.

The figures for the two leading regions are significantly higher than those for the others. The percentage value for South-East Asia is 1.7 times higher than that for South Asia, which is the next region in the ranking. Compared to Northern Europe, which ranks last, the percentage is 11.7 times higher.

Among the countries of the region, Vietnam leads by a wide margin, with 0.18% of ICS computers on which threats from network folders were blocked.



The main categories of threats that spread through network folders are worms, viruses, malware for AutoCAD, and spyware. In terms of malware for AutoCAD, South-East Asia leads the ranking of regions by a wide margin.



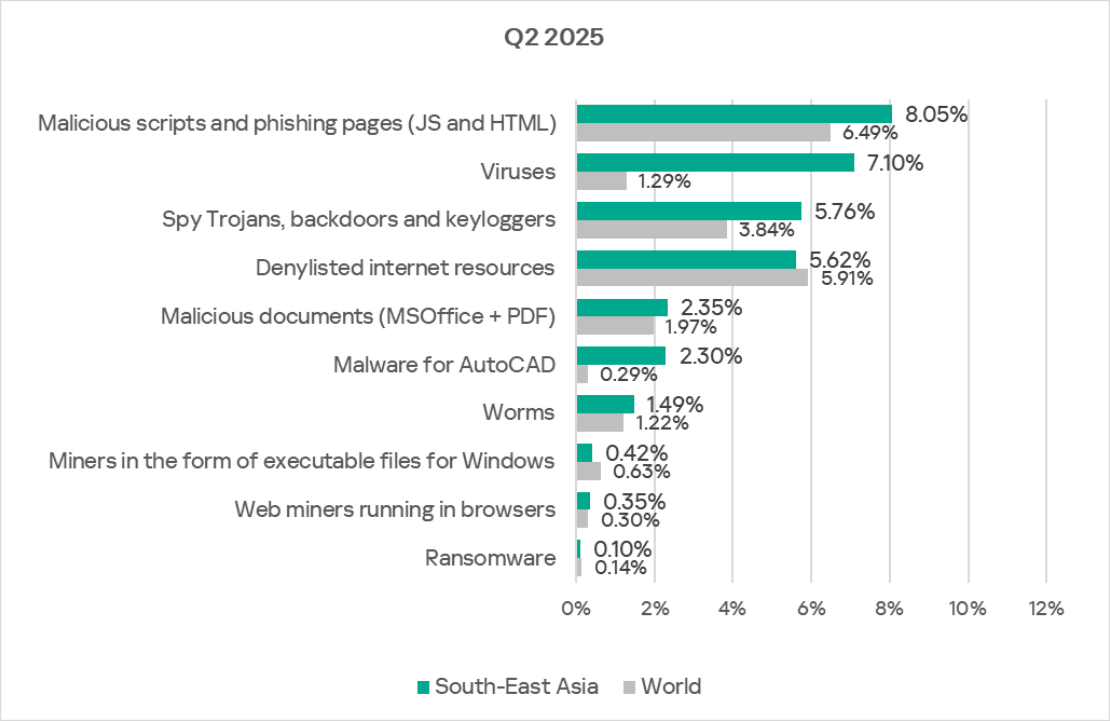
Threat categories

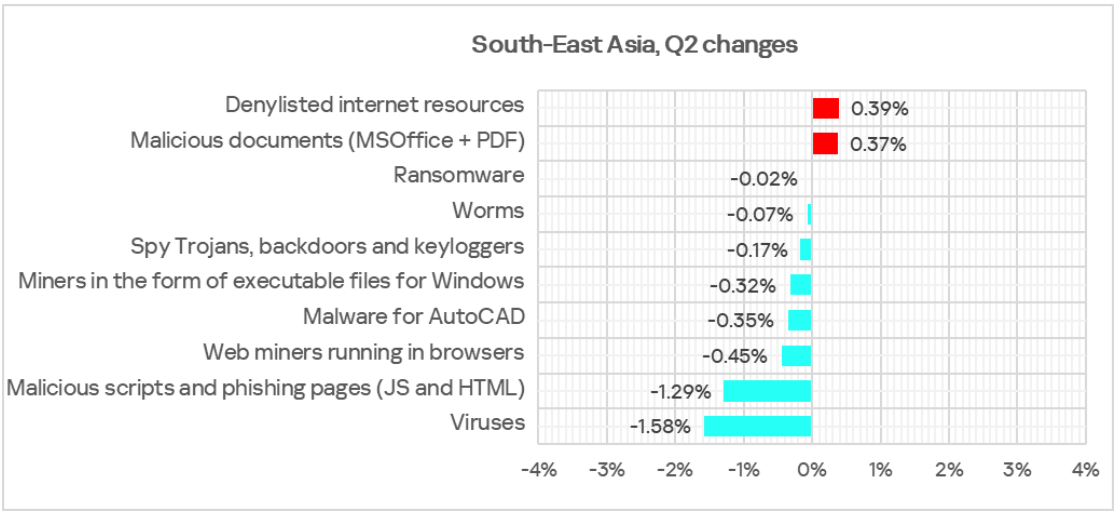
In South-East Asia, the percentage of ICS computers on which malicious objects were blocked is higher than the respective global averages for all threat categories except three (denylisted internet resources, miners in the form of executable files for Windows, and ransomware).

The categories for which the region's figures significantly exceed the global averages are:

- Spyware — by a factor of 1.5;
- Viruses — by a factor of 5.5;
- Malware for AutoCAD — by a factor of 7.9.

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



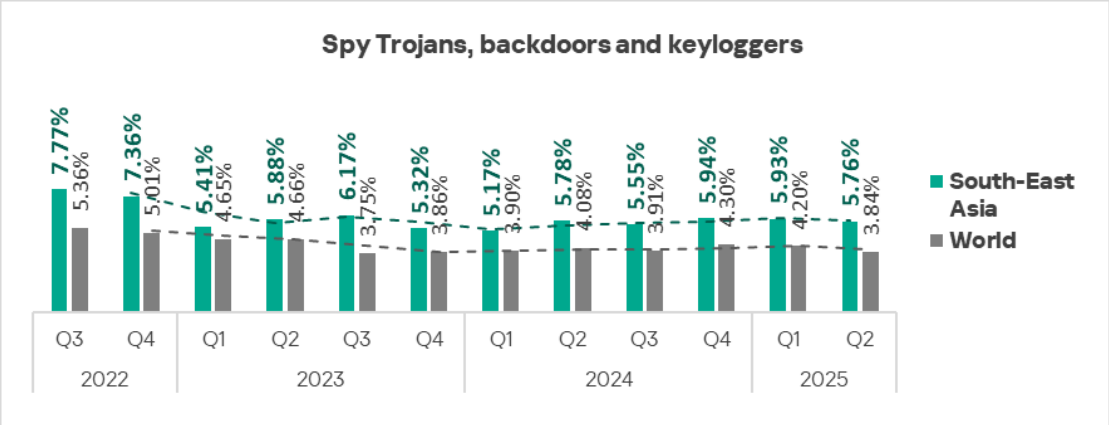


Compared to the previous quarter, the percentage increased only for two categories: denylisted internet resources and malicious documents.

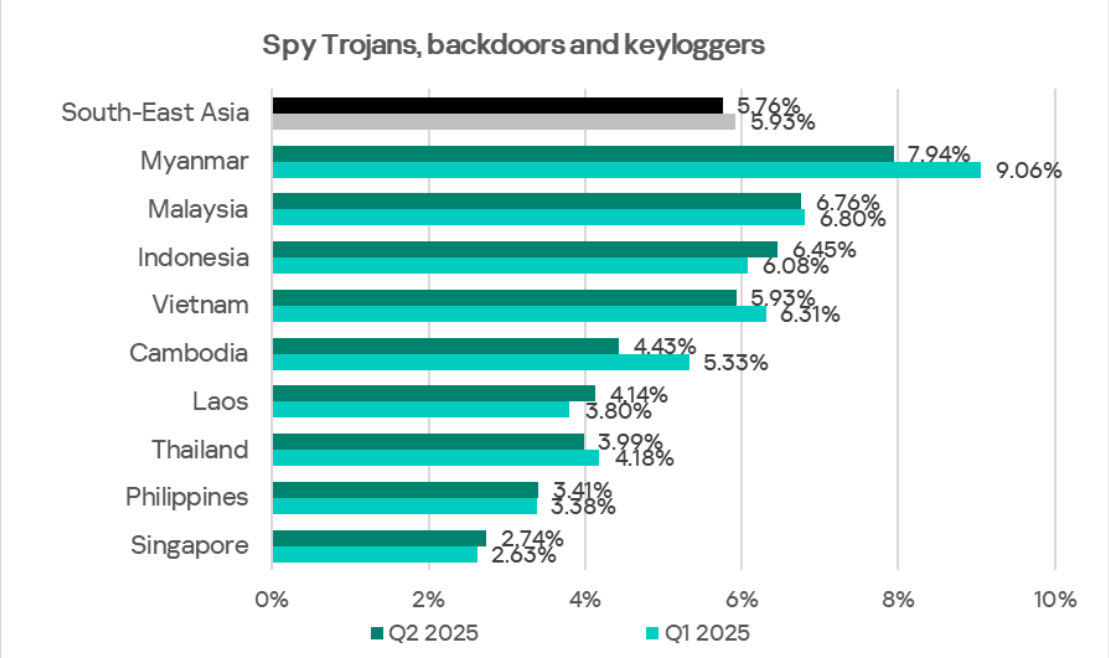
Spyware

South-East Asia ranks third among regions in terms of the percentage of ICS computers on which spyware was blocked, with 5.76%.

This percentage remains fairly stable in the region, fluctuating between 5.17% and 6.17% since Q1 2023.



Among the countries of the region, Myanmar leads in terms of the percentage of ICS computers on which spyware was blocked, with 7.94%. Singapore has the lowest percentage figure, at 2.74%.



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. Myanmar, however, appears to have a

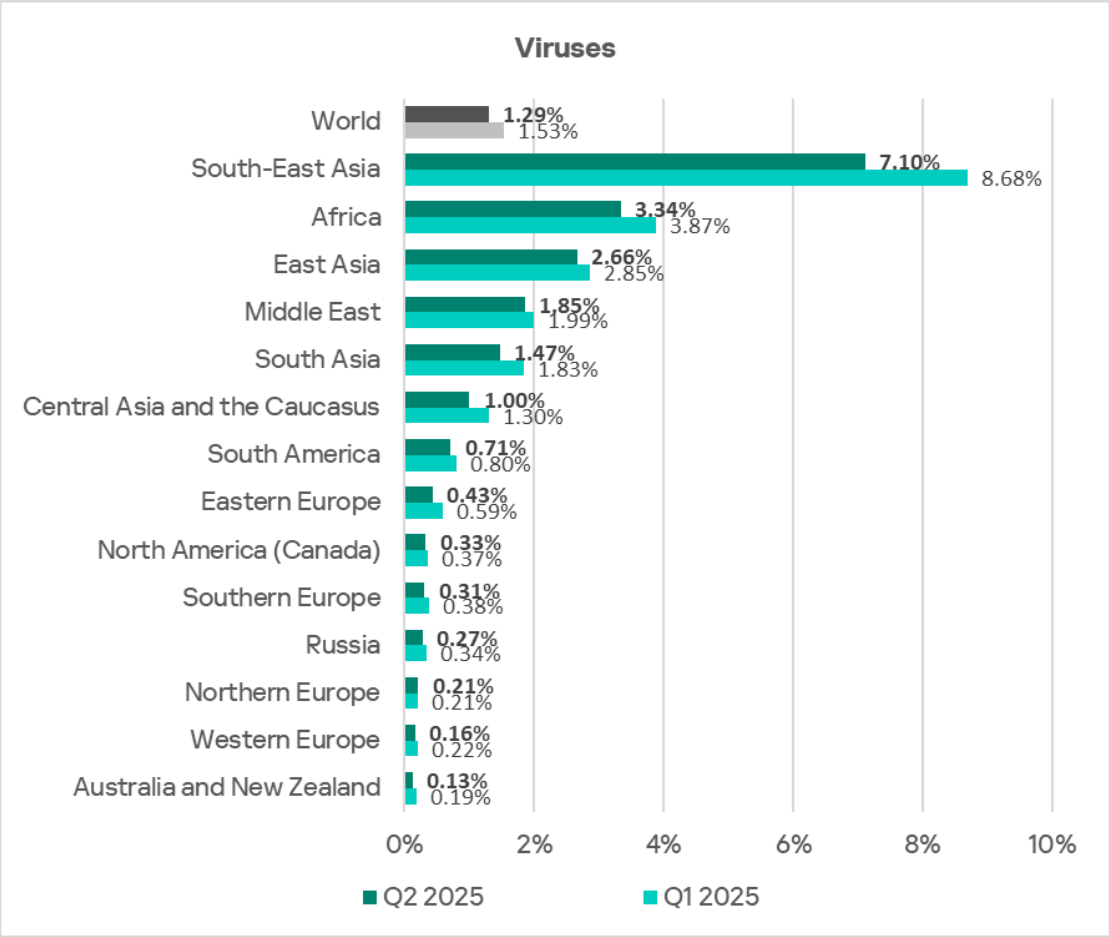
different situation: the country leads in the percentage of ICS computers on which threats from removable media were blocked.

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.

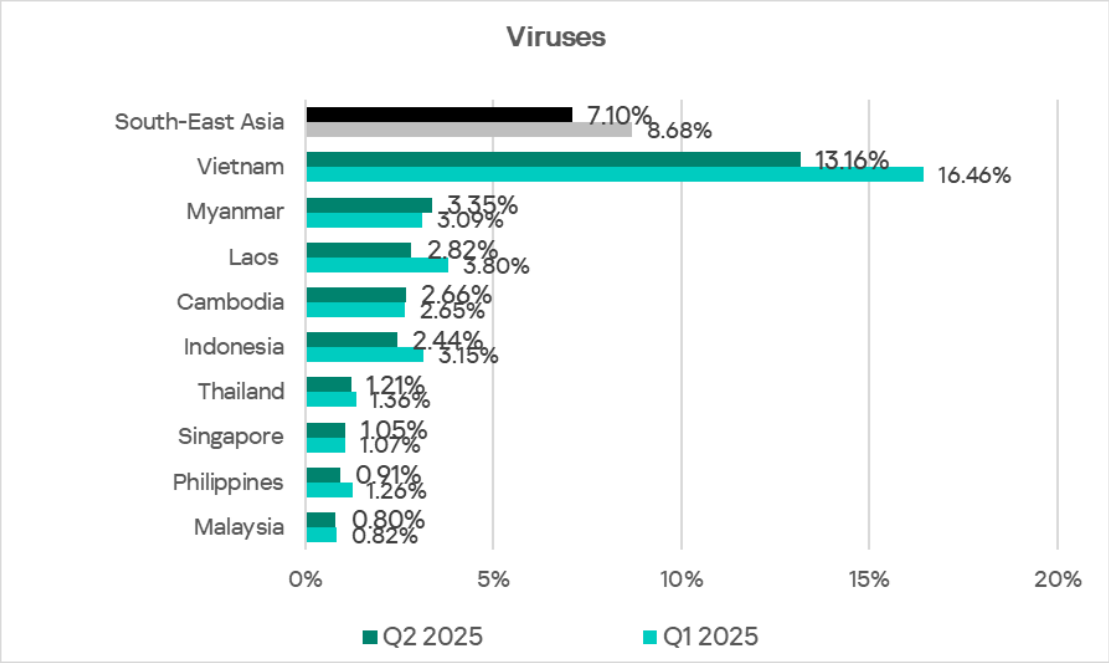
Viruses

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



The percentage in South-East Asia is 2.1 times higher than in Africa (which immediately follows it in the ranking), and 55 times (!) higher than in Australia and New Zealand, which ranks last.

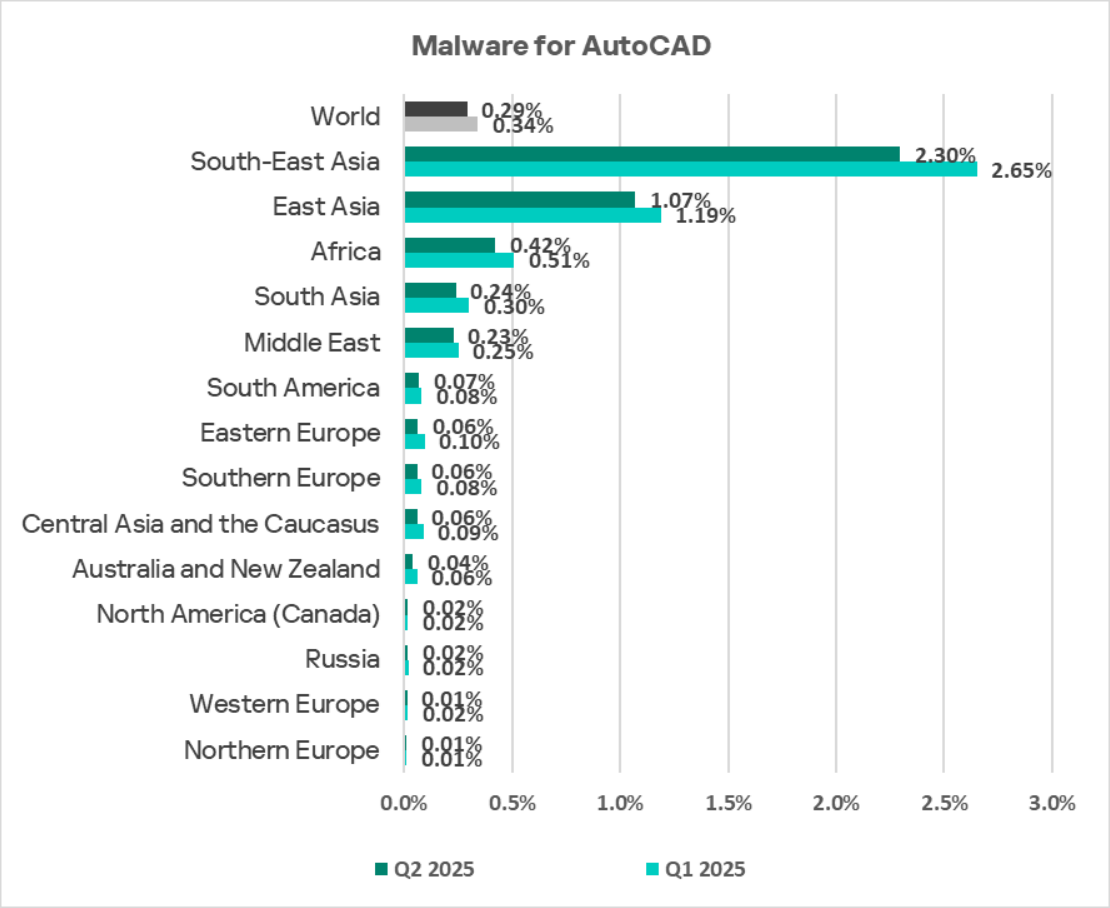
This striking leadership of South-East Asia is ensured by Vietnam. The country's figure is 3.9 times higher than that of Myanmar, which ranks second.



In the region, viruses are blocked across all sources of threats. It is worth noting that Vietnam ranks third based on the percentages of ICS computers on which threats from the internet, email clients, and removable media were blocked. The country also leads the ranking for network folders.

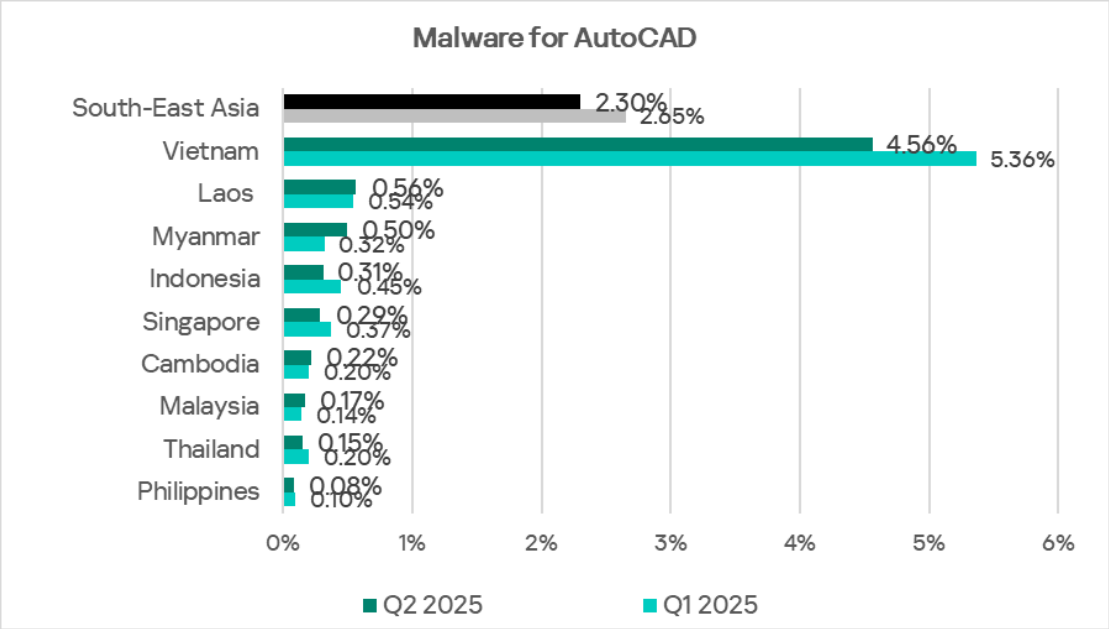
Malware for AutoCAD

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



In South-East Asia, the figure is 2.1 times higher than in East Asia, which ranks second. East Asia itself also differs significantly from the other regions: its percentage value is 2.5 times higher than that of Africa, which ranks one position below it.

The region's leadership in the percentage of ICS computers on which malware for AutoCAD was blocked is likewise ensured by Vietnam.

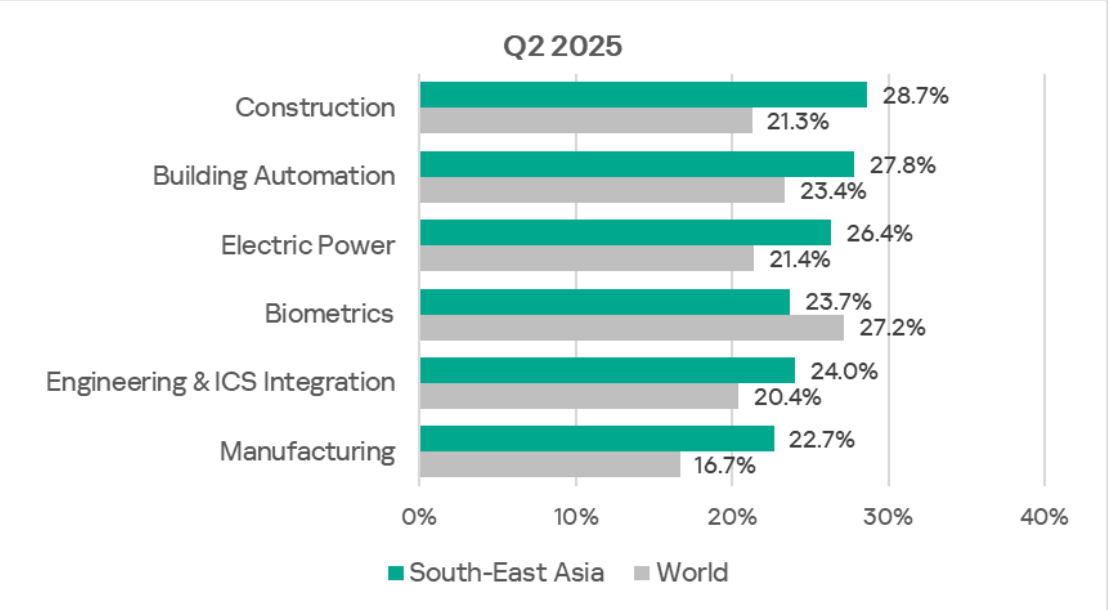


Industries

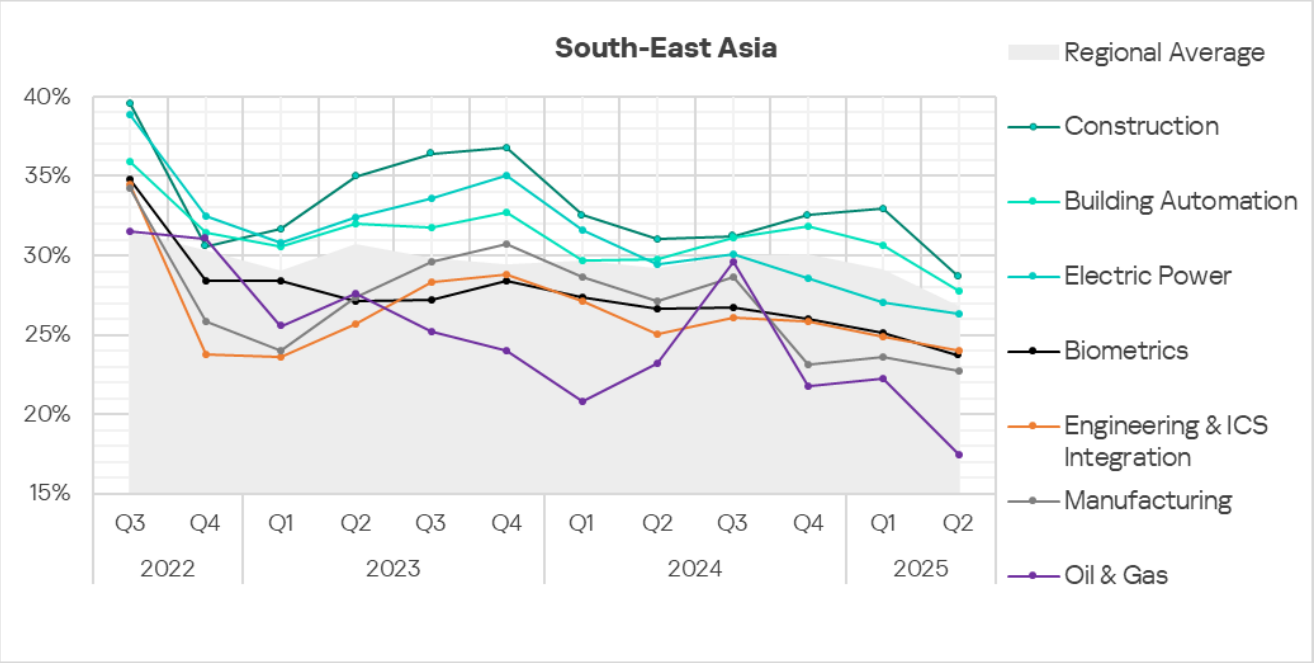
In South-East Asia, construction remains the industry that is most frequently confronted with threats among those reviewed for this report.

The figures for all industries in the region exceed the corresponding global averages. The greatest difference — by a factor of 1.4 — is observed in manufacturing.

The region ranks first in terms of the percentage of ICS computers on which malicious objects were blocked in the building automation industry.



The figures for all industries decreased over the quarter. 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: hot spots

We use heat maps as a tool for assessing industry-specific issues. On these maps, cells are colored in a gradient from red to green, where red indicates the maximum value for a threat source or threat type across all regions and industries. In South-East Asia, the maximum value is observed in the category of malware for AutoCAD, blocked on computers in the construction industry.

Heat maps make it easy to see industry hot spots — positions of threat sources and malware categories for which the figures are higher than expected, given the industry's position and that of the threat or threat source in the corresponding regional rankings.

Threat source indicators for industries in South-East Asia, Q2 2025

Industry / Threat source	Biometrics	Building automation	Electric Power	Engineering & ICS Integration	Oil & Gas	Construction	Manufacturing	Threat category total in the region
Internet	9.90%	11.46%	13.25%	12.19%	10.12%	14.17%	10.41%	11.28%
Email clients	8.49%	6.43%	2.56%	4.04%	3.47%	3.46%	5.18%	4.53%
Removable media	0.53%	0.48%	0.60%	0.47%	0.42%	0.38%	0.47%	0.51%
Network folders	0.08%	0.09%	0.00%	0.04%	0.00%	0.13%	0.00%	0.11%
Industry total in the region	23.70%	27.79%	26.35%	24.01%	17.48%	28.67%	22.69%	

Threat category indicators for industries in South-East Asia, Q2 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	5.26%	5.47%	7.33%	6.47%	5.13%	7.07%	5.70%	5.62%
Malicious scripts and phishing pages (JS and HTML)	9.90%	9.63%	7.72%	7.86%	5.96%	9.13%	7.97%	8.05%
Spy Trojans, backdoors and keyloggers	8.29%	7.40%	4.98%	5.22%	4.02%	5.04%	6.40%	5.76%
Worms	1.92%	1.35%	1.90%	1.27%	0.55%	1.12%	1.69%	1.49%
Miners in the form of executable files for Windows	0.78%	0.47%	0.70%	0.50%	0.55%	0.74%	0.41%	0.42%
Malicious documents (MSOffice + PDF)	4.67%	3.24%	1.96%	1.94%	0.97%	2.75%	2.68%	2.35%
Viruses	2.68%	6.72%	5.82%	3.55%	2.36%	7.53%	3.90%	7.10%
Ransomware	0.40%	0.14%	0.08%	0.06%	0.14%	0.13%	0.17%	0.10%
Web miners running in browsers	0.71%	0.41%	0.76%	0.51%	0.55%	0.79%	0.47%	0.35%
Malware for AutoCAD	0.33%	0.88%	1.85%	1.17%	1.25%	4.94%	0.70%	2.30%
Industry total in the region	23.70%	27.79%	26.35%	24.01%	17.48%	28.67%	22.69%	

The internet is the main source of threats for all industries in the region. Consequently, the most relevant threat categories are denylisted internet resources, and malicious scripts and phishing pages.

Industry hot spots

Construction

- Construction is the leader among industries in the region in terms of the percentages of ICS computers on which threats from the internet and threats from network folders were blocked.
- Construction is also ahead of other industries in the region in terms of the following threat categories: malware for AutoCAD, web miners.

- Ranks first among all industries across all regions based on the percentage of ICS computers on which viruses and denylisted internet resources were blocked.
- Second among industries in the region for the following categories: denylisted internet resources, miners in the form of executable files for Windows.
- Third in the region for the following categories: malicious documents, malicious scripts and phishing pages.

Building automation

- Ranks second among industries in the region in terms of the percentage of ICS computers on which threats from email clients and threats from network folders were blocked.
- Ranks second in the region among industries for the following threat categories: malicious scripts and phishing pages, malicious documents, and spyware.
- Ranks third in the region among industries for viruses and ransomware.

Electric power

- Leader among industries in the region in terms of the percentage of ICS computers on which threats from removable media were blocked. Second in terms of internet threats.
- Leader among industries in the region for denylisted internet resources.
- Second among industries in the region for the categories of worms and web miners.
- Third among industries in the region for the categories of malware for AutoCAD and miners in the form of executable files for Windows.

Engineering and ICS integrators

- Third among industries in the region for internet threats.
- Third among industries in the region for denylisted internet resources.
- Fourth among industries in the region for malware for AutoCAD and both categories of miners.

Biometric systems

- Leader among industries in the region in terms of the percentage of ICS computers on which threats from email clients were blocked. Second in terms of threats from removable media, third in terms of threats from network folders.
- Leader among industries in the region for the following threat categories: malicious scripts and phishing pages, malicious documents, spyware,

ransomware, worms, and miners in the form of executable files for Windows.
- Third among industries in the region for worms.

Manufacturing

- Third among industries in the region in terms of threats from email clients.
- Second among industries in the region for ransomware.
- Third among industries in the region in terms of the percentage of ICS computers on which spyware and worms were blocked.

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 from removable media were blocked has historically been high. In Q2 2025, this indicator in the region was 1.6 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 miners in the form of executable files for Windows were blocked, Central Asia and the South Caucasus ranks first among all regions; in terms of worms, it ranks second after Africa. Both categories are 1.9 times higher than the global average.

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 ICS computers on which miners in the form of executable files for Windows were blocked, Central Asia and the South Caucasus ranks first globally. The main distribution channel for such malware is the internet.

A comparison of the region by industry shows that miners are most often found on computers used in biometric systems (ranking first among all regions and industries), as well as in the power, manufacturing, and construction sectors.

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 and tokens, impersonating users, and exploiting local and network vulnerabilities. Therefore, their potential threat to an OT network should not be underestimated.

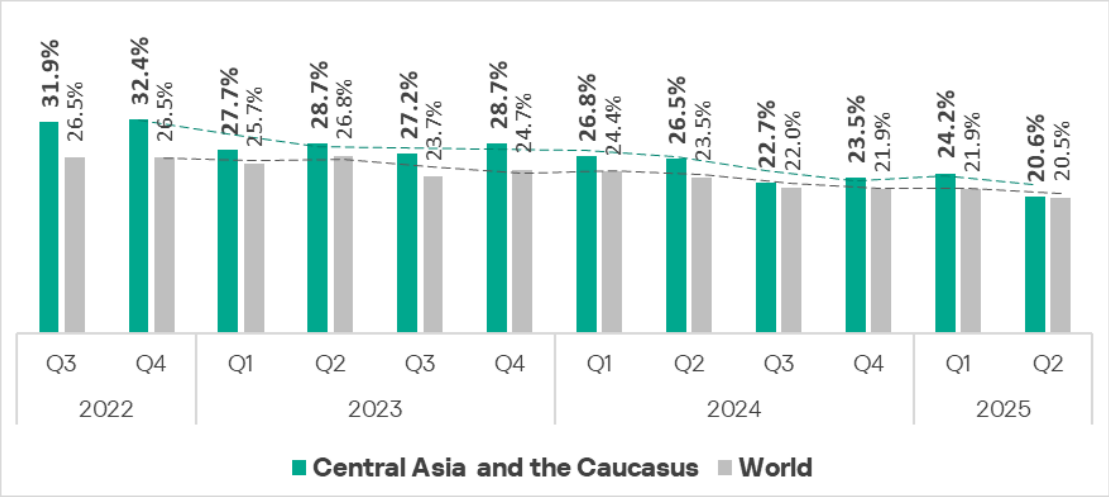
Consistently high level of ransomware incidents

By the percentage of ICS computers on which ransomware was blocked, Central Asia and the South Caucasus ranks third, with a rate 1.4 times higher than the global average. This category of threats spreads in the region both via the internet and removable media.

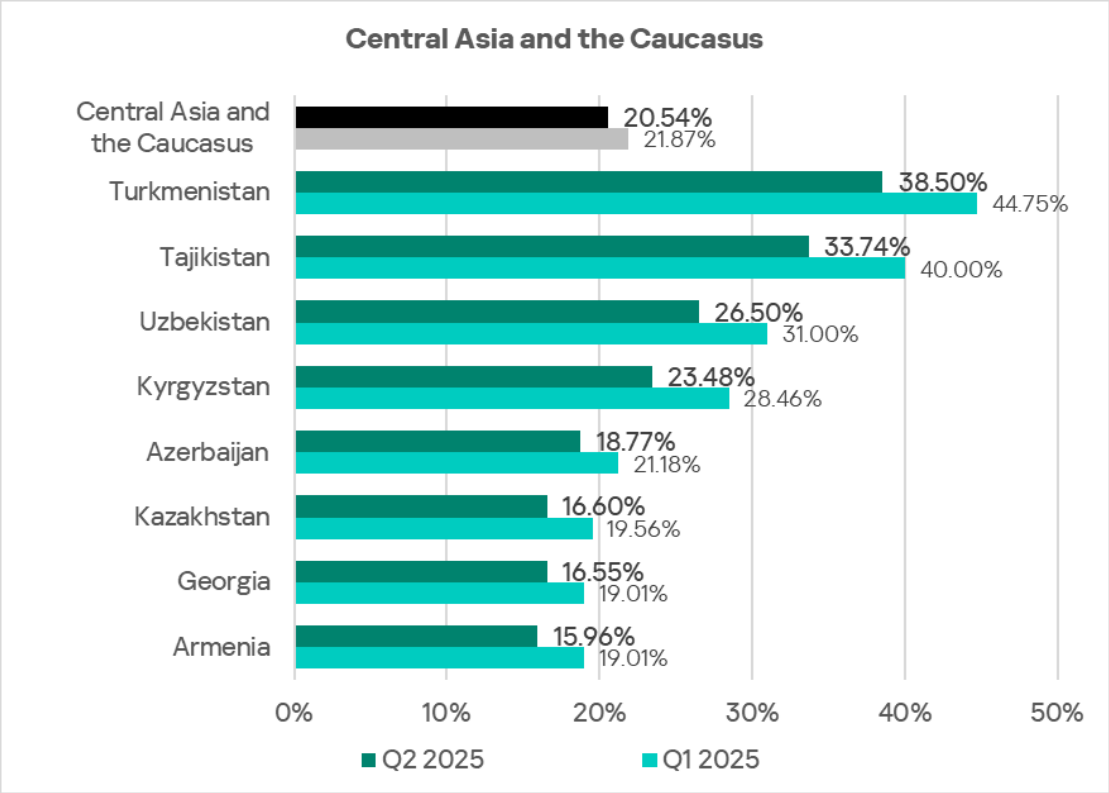
Statistics across all threats

Central Asia and the South Caucasus ranks fourth globally by the percentage of ICS computers on which malicious objects were blocked with 20.6%.

In Q2 2025, the regional rate decreased by 3.6 pp. However, compared to the region with the lowest percentage of attacked ICS computers (Northern Europe with 11.2%), Central Asia and the South Caucasus still had 1.8 times more.

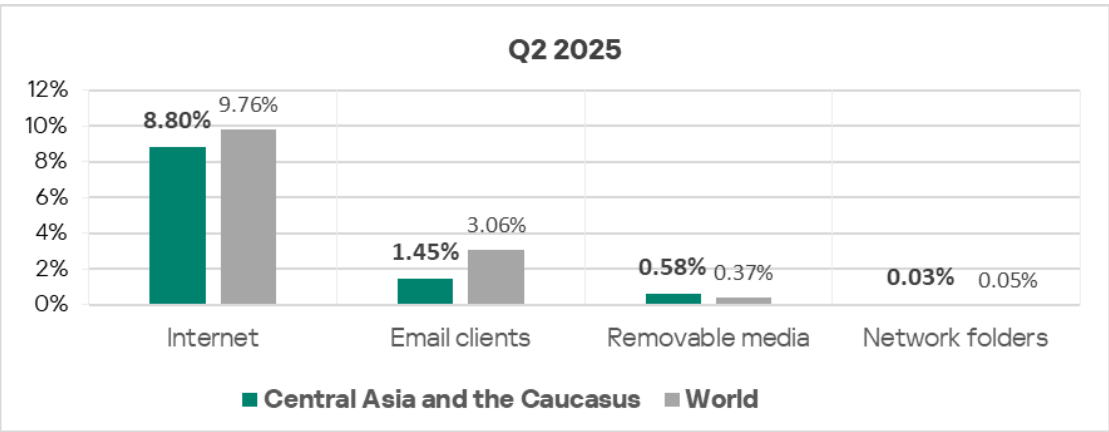


The percentage of ICS computers on which malicious objects were blocked varies among the region's countries, from 15.96% in Armenia to 38.50% in Turkmenistan. Tajikistan is also high, ranking second with 33.74%. Other countries' rates fall between 16% and 27%.

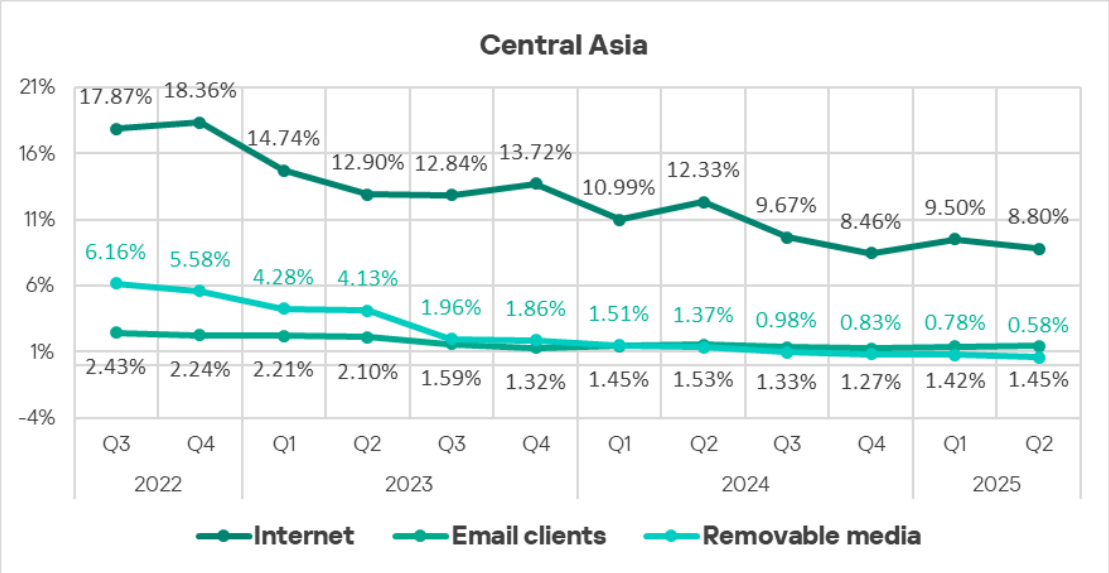


Threat sources

In Central Asia and the South Caucasus, only threats from removable media exceeded the global average on ICS computers, by 1.6 times.



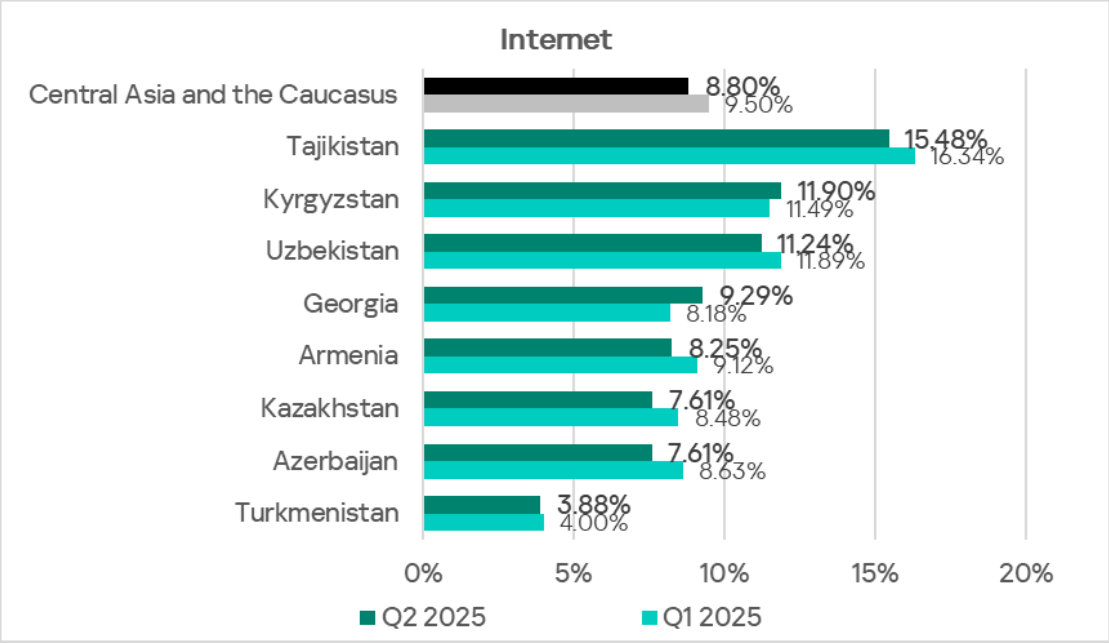
In Q2 2025, the percentage of ICS computers on which malicious objects were blocked fell across all threat sources except for email clients.



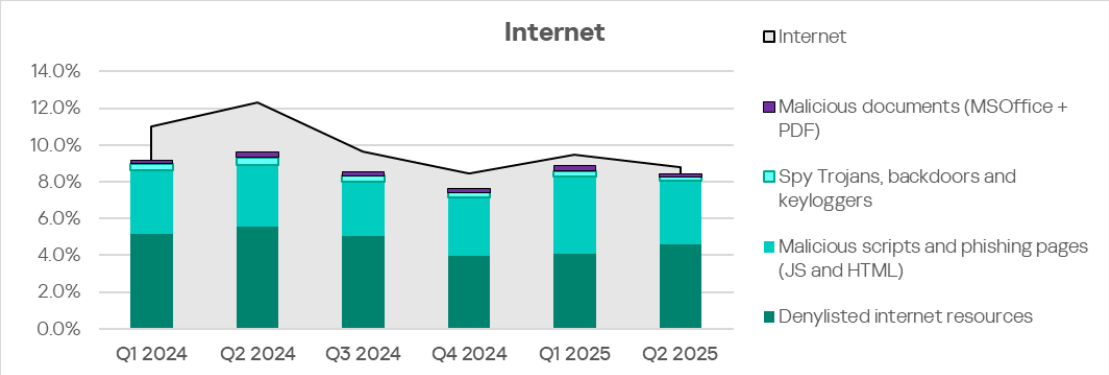
Internet

By the percentage of ICS computers on which threats from the internet were blocked, Central Asia and the South Caucasus ranks eighth globally at 8.80%, which is 1.4 times higher than the lowest level (East Asia, 6.35%).

Country-level rates range from 3.88% in Turkmenistan to 15.48% in Tajikistan.



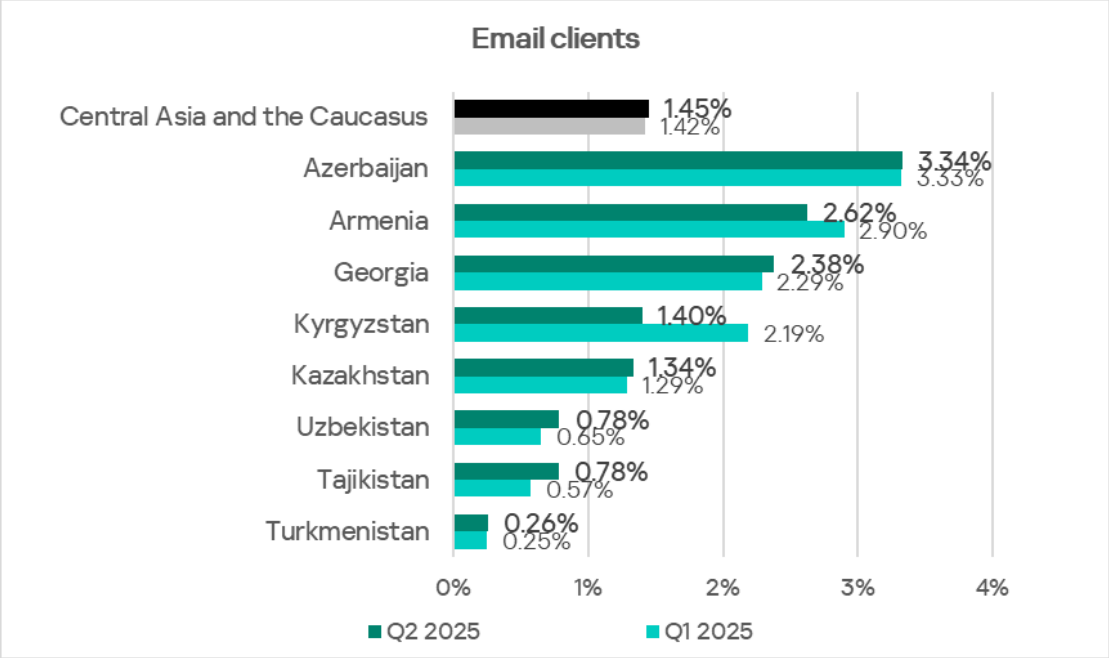
The main categories of internet threats blocked on ICS computers in the region are denylisted internet resources, malicious scripts and phishing pages, spyware, and malicious documents.



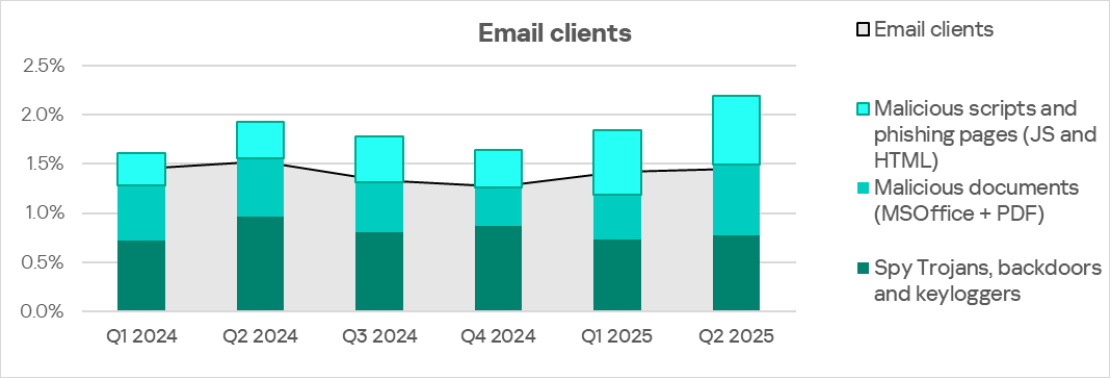
Email clients

Compared to other regions, the percentage of ICS computers where threats from email clients were blocked in Central Asia and the South Caucasus is relatively low: 1.45%, ranking 12th. Nevertheless, this is 1.8 times higher than in Russia, which is last in the ranking.

Among the countries of the region, Azerbaijan leads with 3.34%, while Turkmenistan has the lowest at 0.26%.



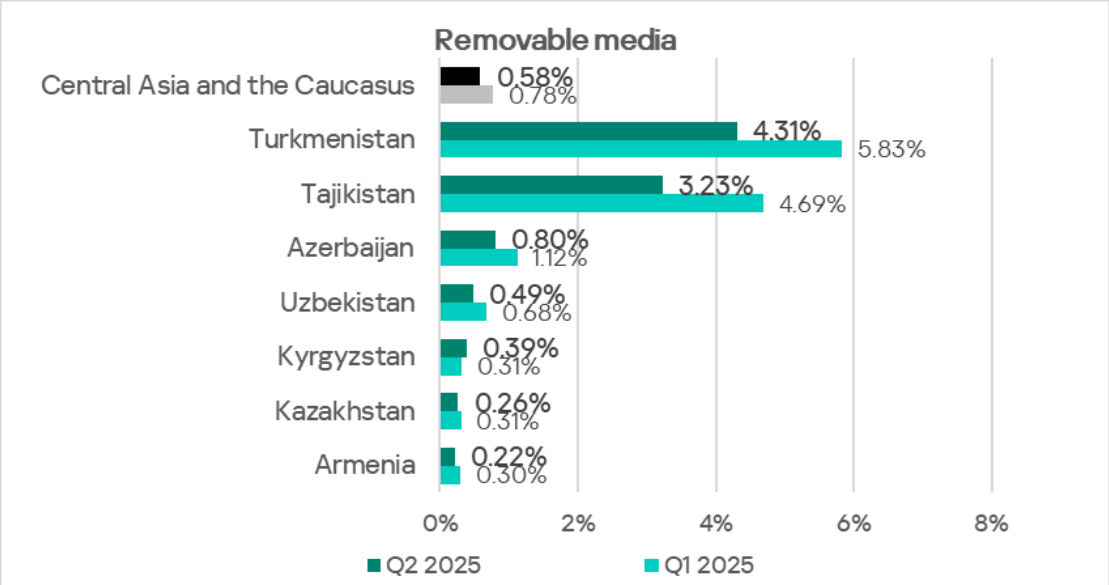
The main categories of email threats blocked on ICS computers are spyware, malicious documents, malicious scripts and phishing pages.



Removable media

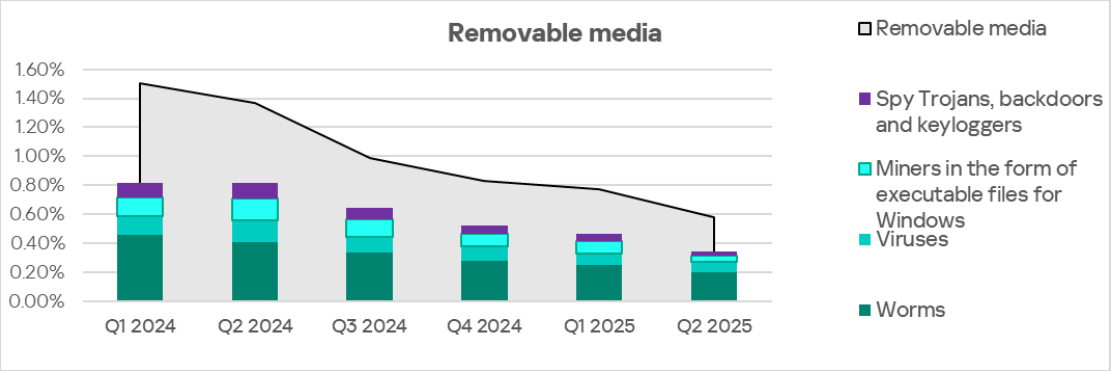
The top six regions by the percentage of ICS computers on which threats from removable media were blocked are Africa and Asian regions. Central Asia and the South Caucasus ranks fifth with 0.58%. This figure is 21.7 times higher than in North America (Canada) (0.03%), which is at the bottom of the list.

Among the countries in the region, Turkmenistan (4.31%) and Tajikistan (3.23%) lead by a wide margin in the percentage of ICS computers on which threats from removable media were blocked. Notably, these countries were at the bottom of the email clients threats ranking. The other countries range from 0.22% in Armenia to 0.80% in Azerbaijan.

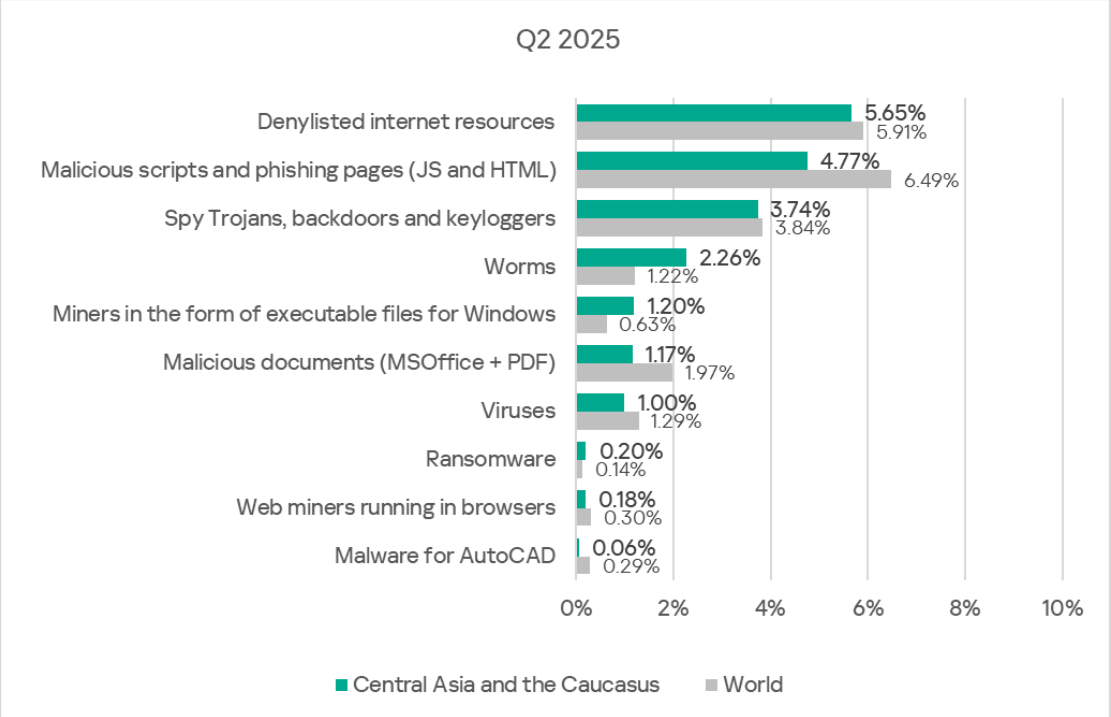


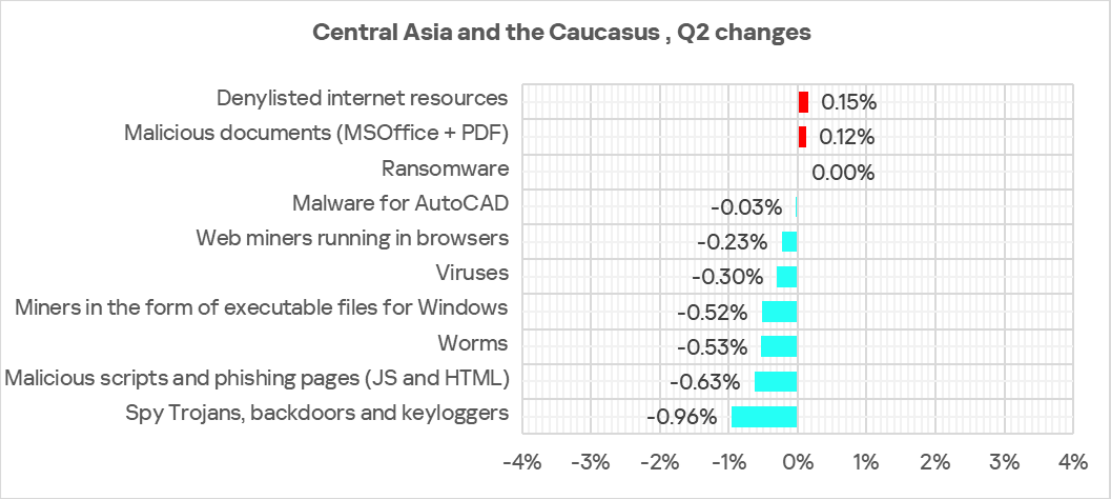
The main categories of removable media threats blocked on ICS computers are worms, viruses, spyware, and miners in the form of executable files for Windows.

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



Threat categories





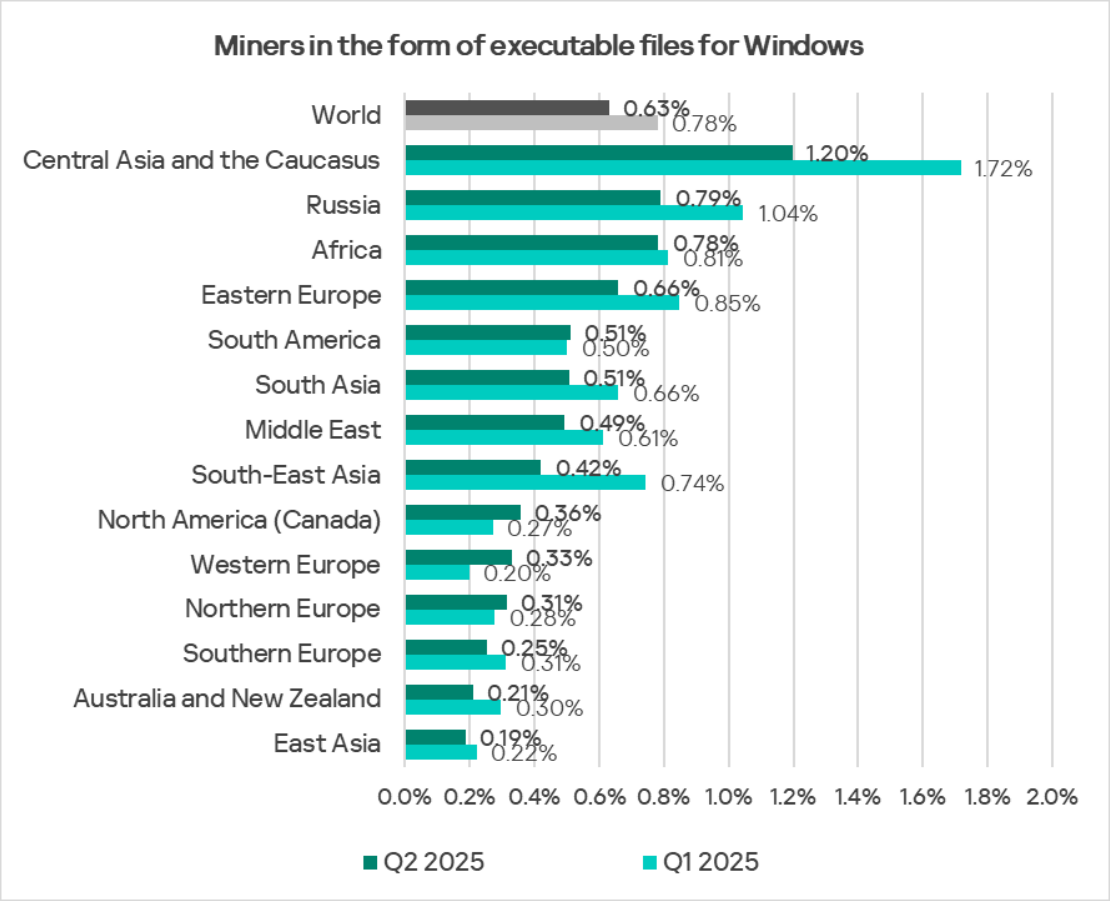
Compared to the global averages, the region has a higher percentage of ICS computers with the following categories of blocked threats:

- Miners in the form of executable files for Windows — 1.9 times higher. Central Asia and the South Caucasus leads globally in this metric.
- Worms — 1.9 times higher. The region ranks second.
- Ransomware — 1.4 times higher. The region ranks third.

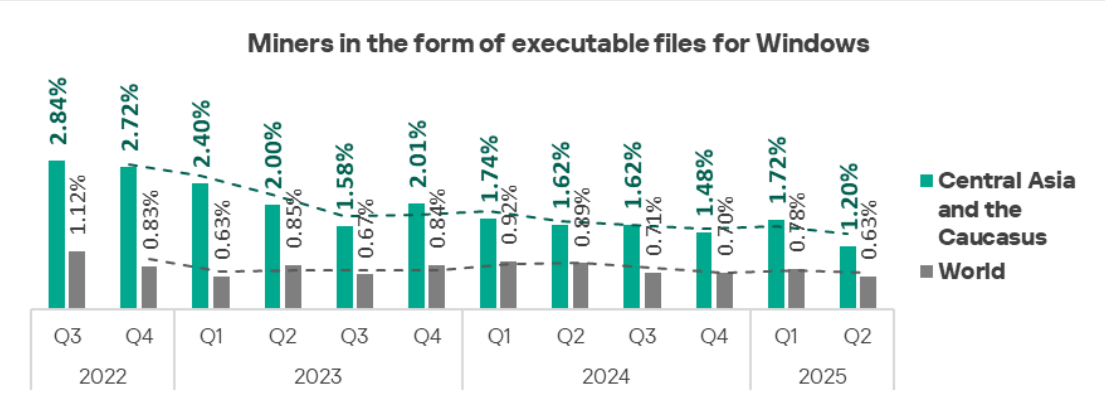
Of all threat categories, only two increased over this quarter: denylisted internet resources and malicious documents.

Miners in the form of executable files for Windows

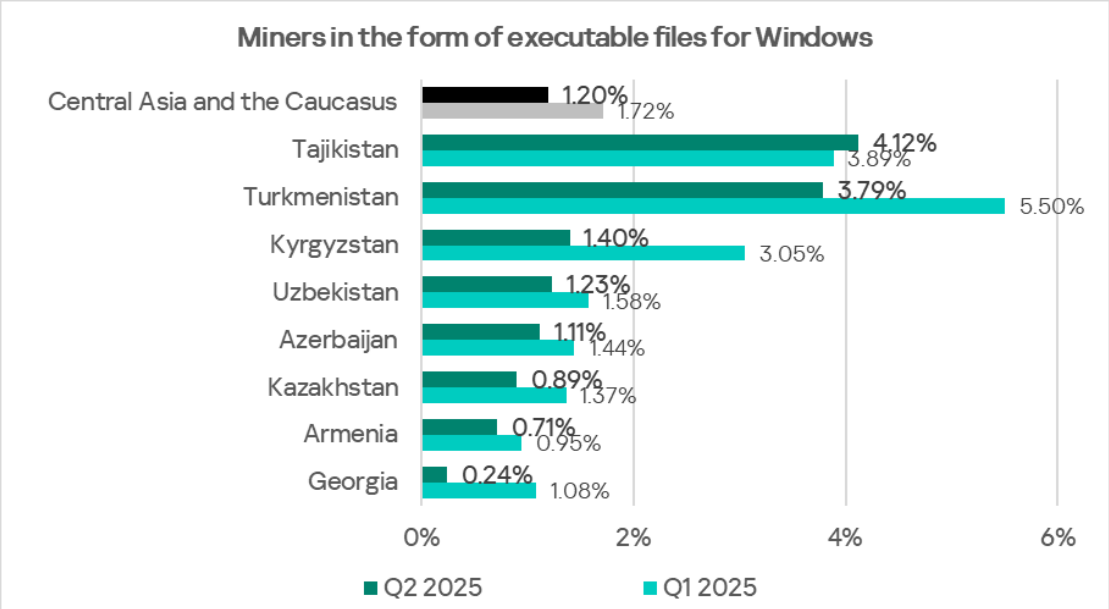
By the percentage of ICS computers on which miners in the form of executable files for Windows were blocked, Central Asia and the South Caucasus leads all regions with 1.20%. This is 6.3 times higher than East Asia, which has the lowest rate among all regions.



Despite increasing in the previous quarter, the percentage of ICS computers on which miners in the form of executable files for Windows were blocked fell to its lowest level since Q3 2022.



Among the countries in the region, Tajikistan (4.12%) and Turkmenistan (3.79%) lead in the percentage of ICS computers on which miners in the form of executable files for Windows were blocked. Georgia has the lowest rate at 0.24%.

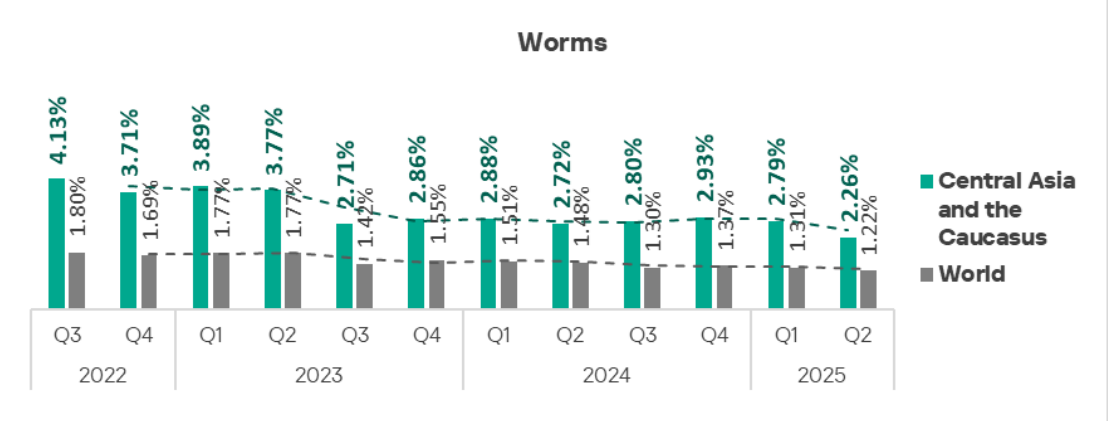


Such threats spread via the internet and removable media. The leaders Tajikistan and Turkmenistan also lead by the percentage of ICS computers where threats from removable media were blocked.

Worms

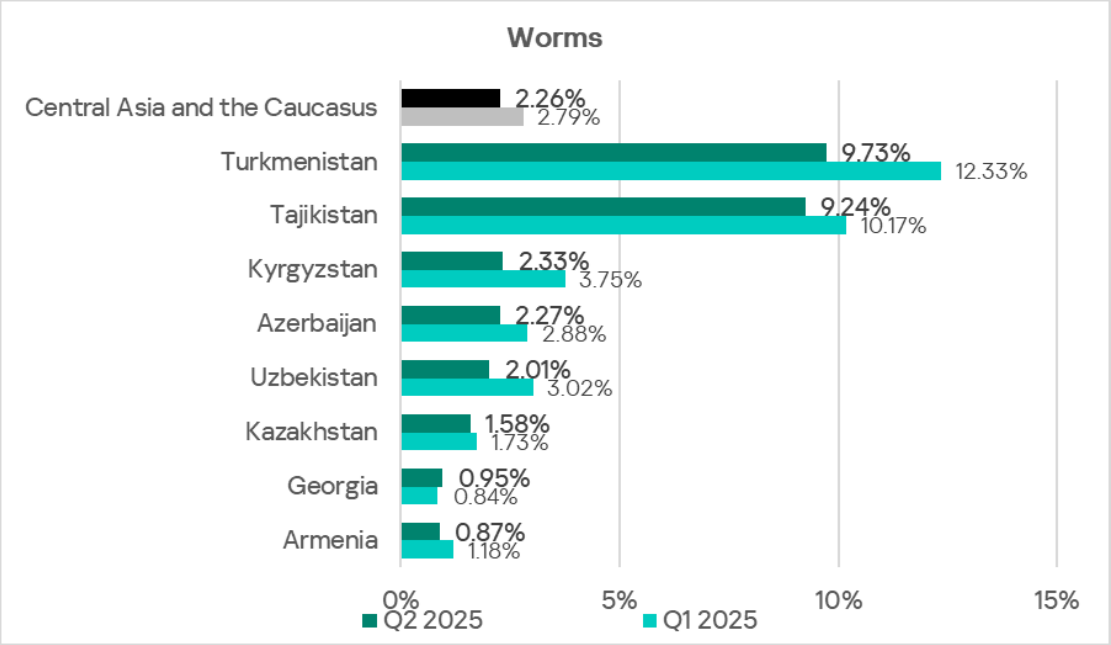
By the percentage of ICS computers on which worms were blocked, Central Asia and the South Caucasus ranks second among regions, behind only Africa. The rate for the region is 2.26%, which is 10.2 times higher than in Australia and New Zealand (the lowest globally).

The worms rate in the region has been decreasing for two consecutive quarters. In Q2 2025, it reached its lowest level since Q3 2022.



In Q2 2025, as in the previous quarter, worms ranked fourth among threat categories in Central Asia and the South Caucasus. Russia is the only other region with such a high worm ranking.

Among the countries of the region, Tajikistan (9.73%) and Turkmenistan (9.24%) lead by the percentage of ICS computers on which worms were blocked. Armenia has the lowest rate at 0.87%.



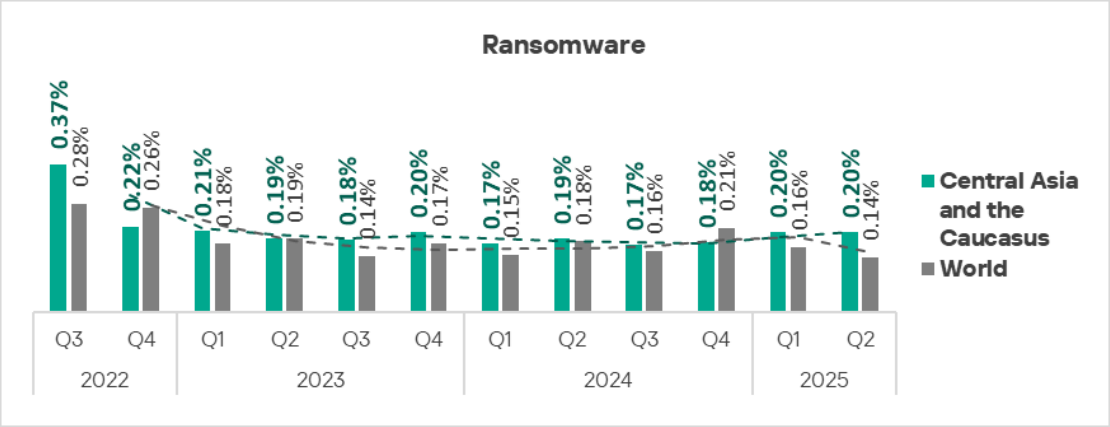
These threats spread mainly through removable media. The leaders Tajikistan and Turkmenistan also lead by the percentage of ICS computers on which threats from removable media were blocked.

Notably, these same countries also lead in terms of Windows executable miner infections.

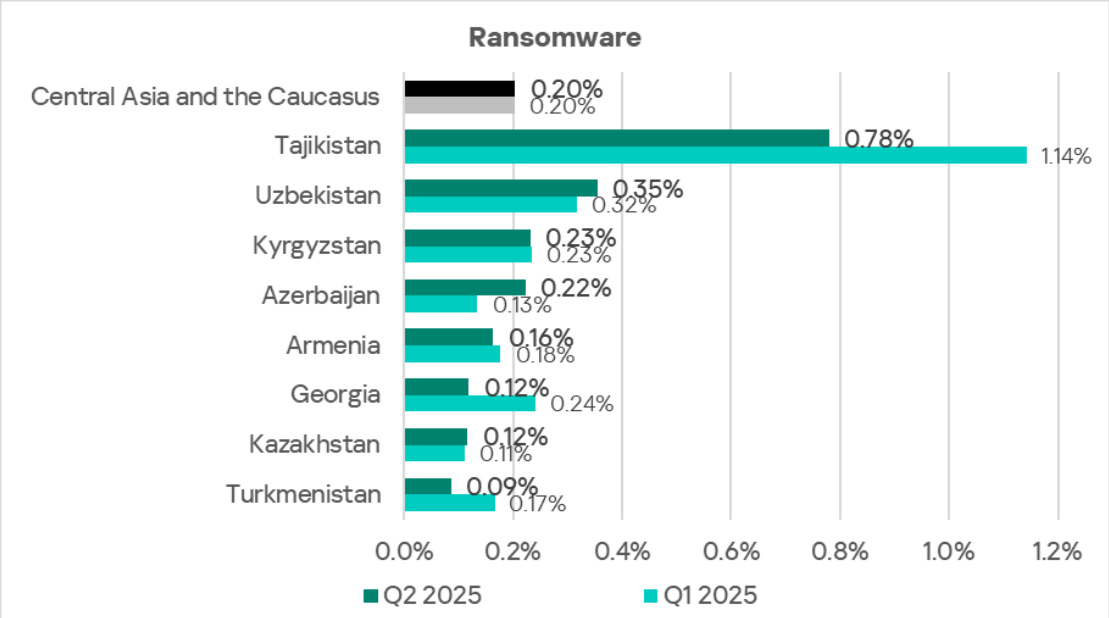
Ransomware

By the percentage of ICS computers on which ransomware was blocked, Central Asia and the South Caucasus ranks third globally. The region's rate is 3.1 times higher than Western Europe, which ranks last.

The ransomware rate in Central Asia and the South Caucasus is fairly stable and, unlike most other threat categories, did not change over the quarter.

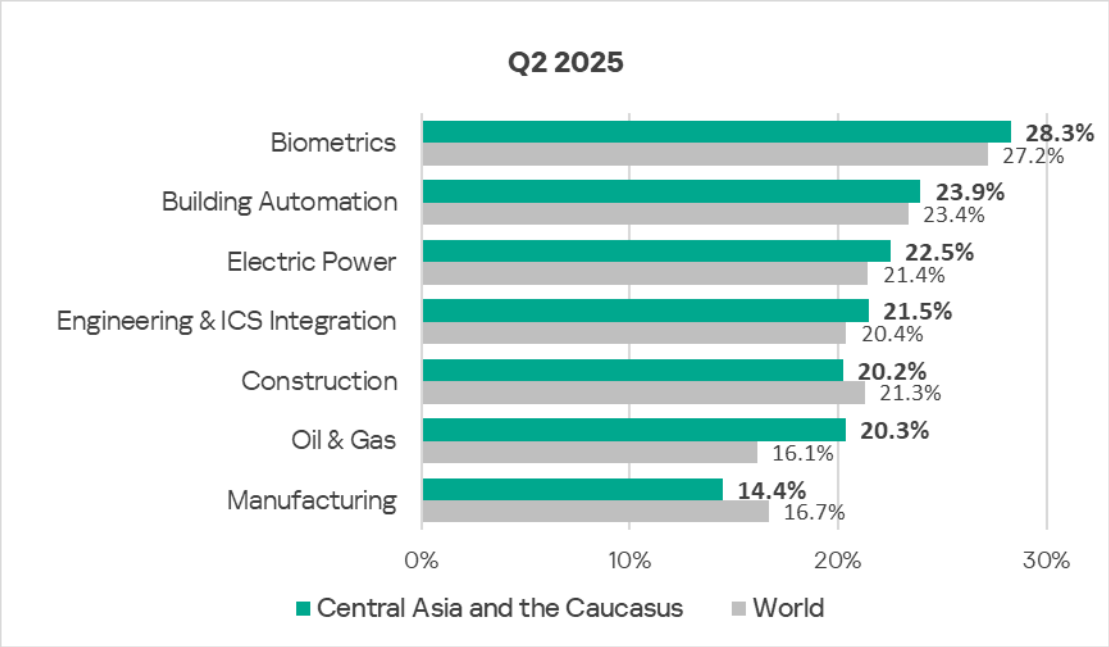


The region's high rate of ICS ransomware incidents is primarily driven by Tajikistan, with 0.78%.



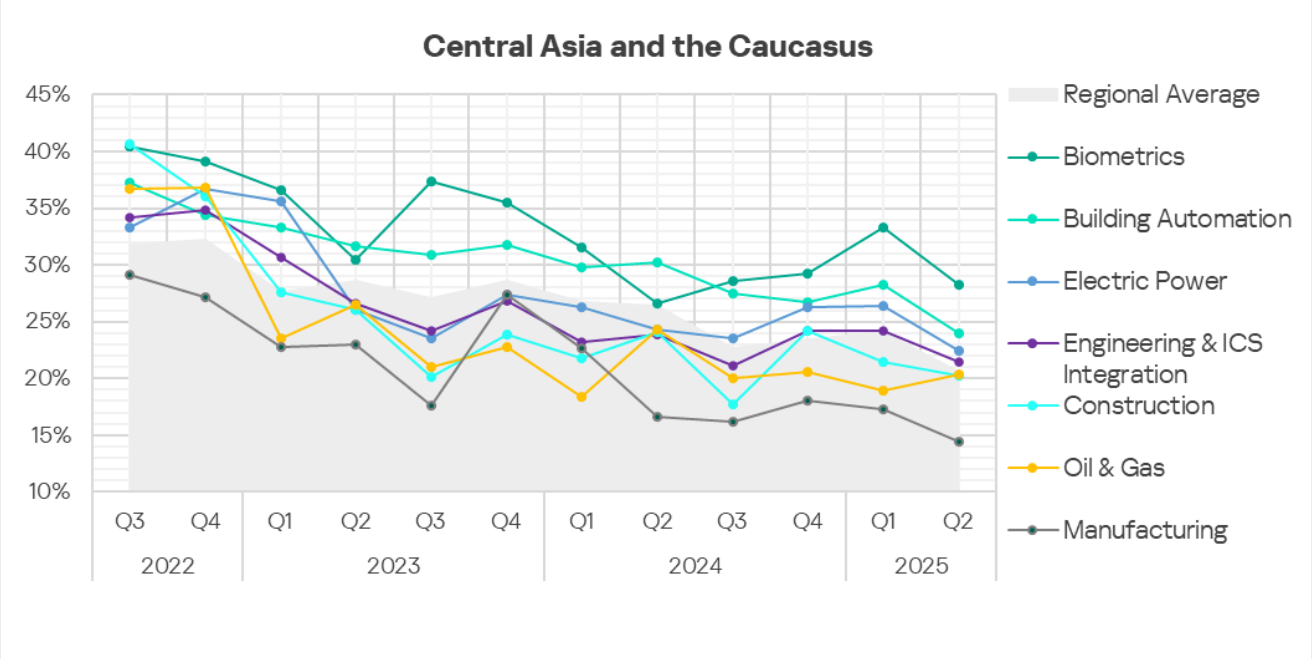
Industries

Among the region's industries analyzed in the report, OT infrastructure for biometric systems and building automation encounter threats most frequently.



All industries — except construction and manufacturing — have rates above the global average. The regional indicator exceeds the global average the most in the oil and gas industry, by 1.26 times. This is the only industry where the rate increased over the quarter, by a notable 4.2 pp. In the previous quarter, it decreased, and despite finally rising to 20.3%, it did not reach the Q4 2024 level (20.5%).

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



Threat sources and malware categories for industries: hot spots

We use heatmaps to assess threats facing industries. On these maps, cells are colored from red to green, where red indicates the maximum value for a threat source or type among all regions and industries. In Central Asia and the South Caucasus, we observed the maximum value for miners (executables) blocked on computers in biometric data collection, processing, and storage systems.

Threat source indicators for industries in Central Asia and the South Caucasus, Q2 2025

Industry / Threat source	Biometrics	Building Automation	Electric Power	Engineering & ICS Integration	Oil & Gas	Construction	Manufacturing	Threat category total in the region
Internet	10.67%	9.29%	10.84%	11.09%	7.71%	9.35%	5.56%	8.80%
Email clients	4.80%	2.41%	1.61%	1.06%	2.81%	0.81%	0.74%	1.45%
Removable media	0.80%	0.71%	1.07%	0.53%	0.14%	0.58%	0.37%	0.58%
Network folders	0.00%	0.05%	0.00%	0.00%	0.00%	0.00%	0.00%	0.03%
Industry total in the region	28.27%	23.95%	22.49%	21.46%	20.34%	20.21%	14.44%	

Threat category indicators for industries in Central Asia and the South Caucasus, Q2 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	8.27%	5.93%	8.17%	7.31%	4.49%	6.81%	4.07%	5.65%
Malicious scripts and phishing pages (JS and HTML)	6.67%	5.73%	6.16%	5.56%	7.15%	5.08%	2.96%	4.77%
Spy Trojans, backdoors and keyloggers	6.13%	5.62%	3.88%	3.61%	1.54%	3.00%	3.70%	3.74%
Worms	4.53%	3.08%	2.01%	1.89%	1.12%	1.96%	2.22%	2.26%
Miners in the form of executable files for Windows	2.67%	1.37%	2.14%	1.36%	0.98%	1.73%	1.85%	1.20%
Malicious documents (MSOffice + PDF)	3.73%	1.80%	0.80%	1.20%	0.98%	0.81%	1.11%	1.17%
Viruses	1.33%	1.35%	1.74%	1.03%	0.70%	1.39%	1.48%	1.00%
Ransomware	0.27%	0.35%	0.40%	0.33%	0.28%	0.35%	0.37%	0.20%
Web miners running in browsers	0.53%	0.20%	0.40%	0.28%	0.14%	0.23%	0.37%	0.18%
Malware for AutoCAD	0.00%	0.02%	0.40%	0.17%	0.00%	0.35%	0.00%	0.06%
Industry total in the region	28.27%	23.95%	22.49%	21.46%	20.34%	20.21%	14.44%	

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

Industry hot spots

Biometric systems

- Highest email clients threat rate among all industries. Second place for removable media threats.
- Leader in most threat category indicators.

Building automation

- The only industry where threats from network folders were blocked.
- Second place for malicious documents, spyware, worms.

Electrical energy industry

- Regional leader in the percentage of ICS computers on which threats from removable media were blocked.
- Leads in terms of viruses, ransomware, and malware for AutoCAD. Second place for both categories of miners.

Engineering and ICS integrators

- Leader in internet threats.
- Third place in terms of denylisted internet resources and malicious documents.

Oil and gas

- Second place in terms of email threats.
- Leader in malicious scripts and phishing pages.

Construction

- Fourth place in terms of removable media threats.
- Second place in terms of malware for AutoCAD, third in terms of viruses and ransomware (tied with building automation).

Manufacturing

- Threats from email clients.
- Second place in terms of viruses and ransomware, third in terms of worms and both categories of miners on ICS computers.

East Asia

Key cybersecurity issues in the region

Absence or ineffectiveness of perimeter defenses for OT networks

East Asia is the only region where spyware ranks first among malware categories by 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 threats from network folders 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.

Across all industries and regions, the construction industry in East Asia ranks first in malware for AutoCAD.

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.

The electrical energy industry in East Asia leads all industries worldwide in the percentage of computers where threats were blocked on removable and network drives.

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 threats from removable media were blocked, East Asia ranks second among regions, behind only Africa. In addition to worms, spyware is most frequently blocked on removable media in the region.

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 in the electrical energy industry where threats were blocked, East Asia ranked first globally in Q2 2025 with 30.33%. In construction and manufacturing, the region ranks 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 noticeable delay.

Striking differences among countries in the region

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

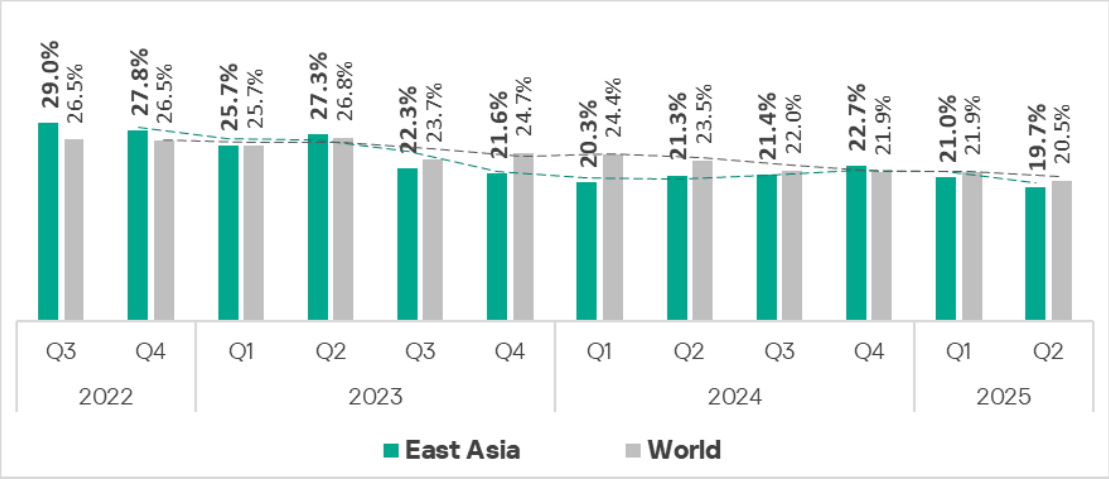
- Mongolia leads in internet threats
- Taiwan and Hong Kong lead in email threats
- Mainland China leads in removable media and network folder threats, driving the region's high rates of viruses and malware for AutoCAD.

Japan consistently ranks last in most categories.

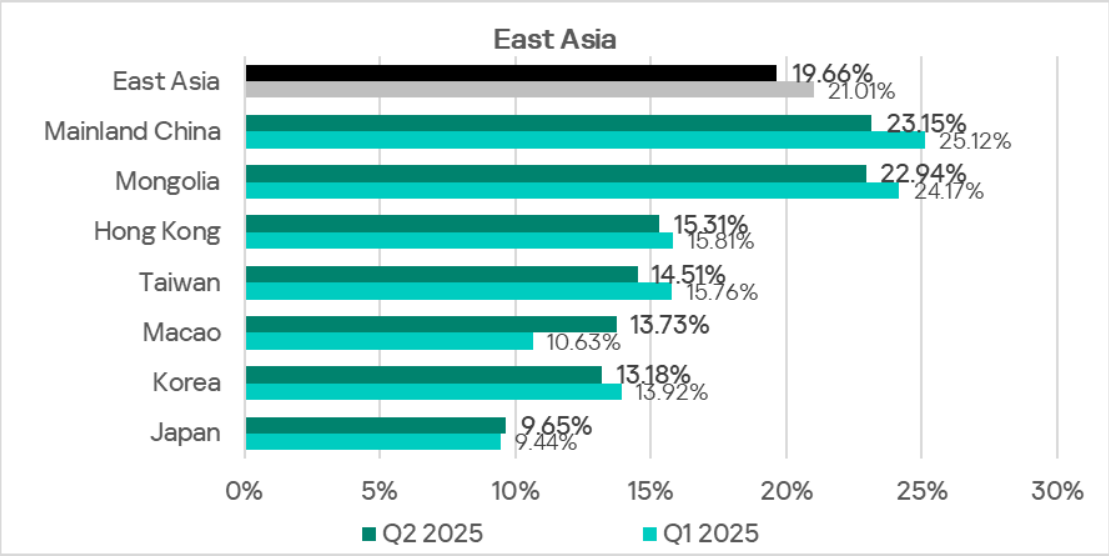
Statistics across all threats

East Asia ranks seventh globally by the percentage of ICS computers on which malicious objects were blocked, at 19.7%.

This indicator has been declining for two consecutive quarters. Nevertheless, the Q2 2025 figure is still 1.8 times higher than the lowest ranking region, Northern Europe.



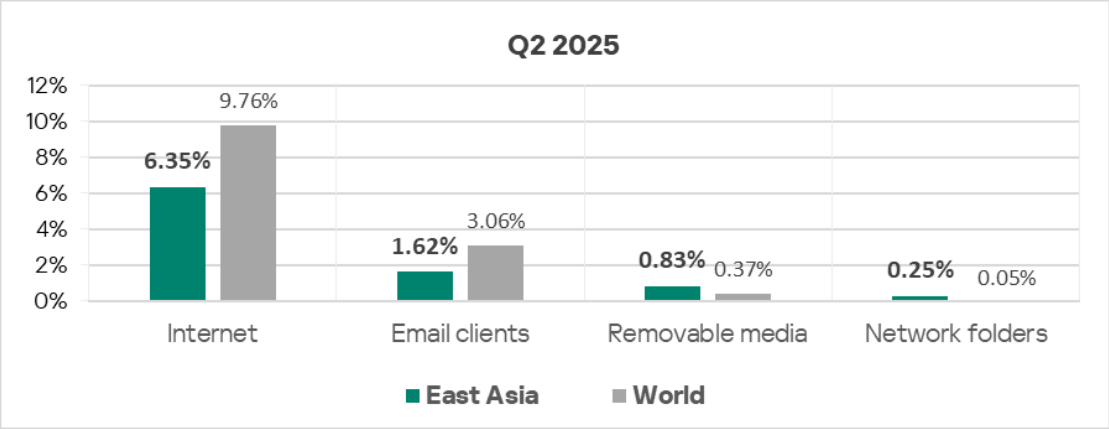
The percentage of ICS computers on which malicious objects were blocked varies among the region's countries, from 9.65% in Japan to 23.15% in Mainland China. Mongolia also has a high rate, ranking second with 22.94%. The figures for other countries fall between 13% and 16%.



Threat sources

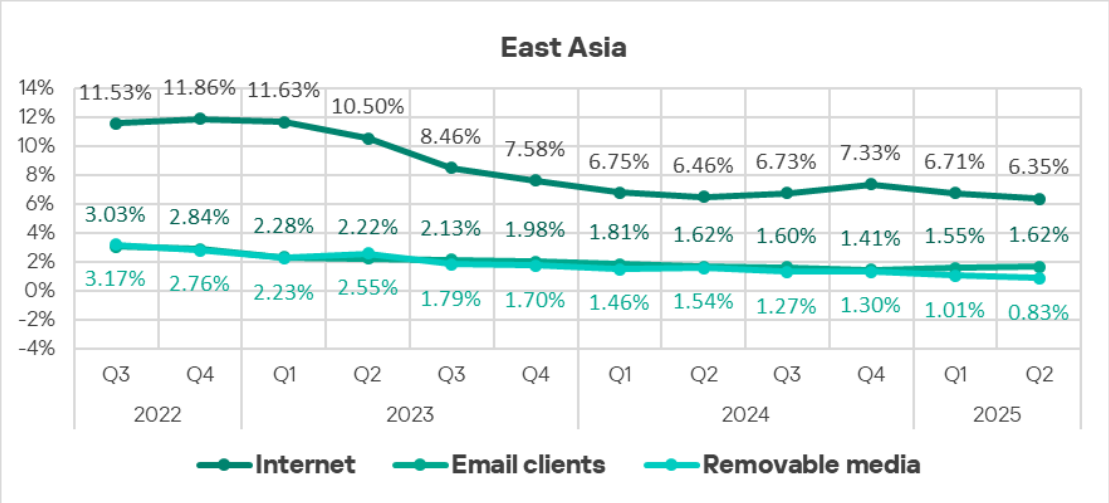
In Q2 2025, East Asia exceeded the global averages for two threat sources:

- Removable media — by 2.2 times, second place globally
- Network folders — by 4.7 times, ranking first globally



In Q2 2025, the percentage of ICS computers on which malicious objects were blocked fell across all threat sources except for mail clients, which returned to Q2 2024 levels.

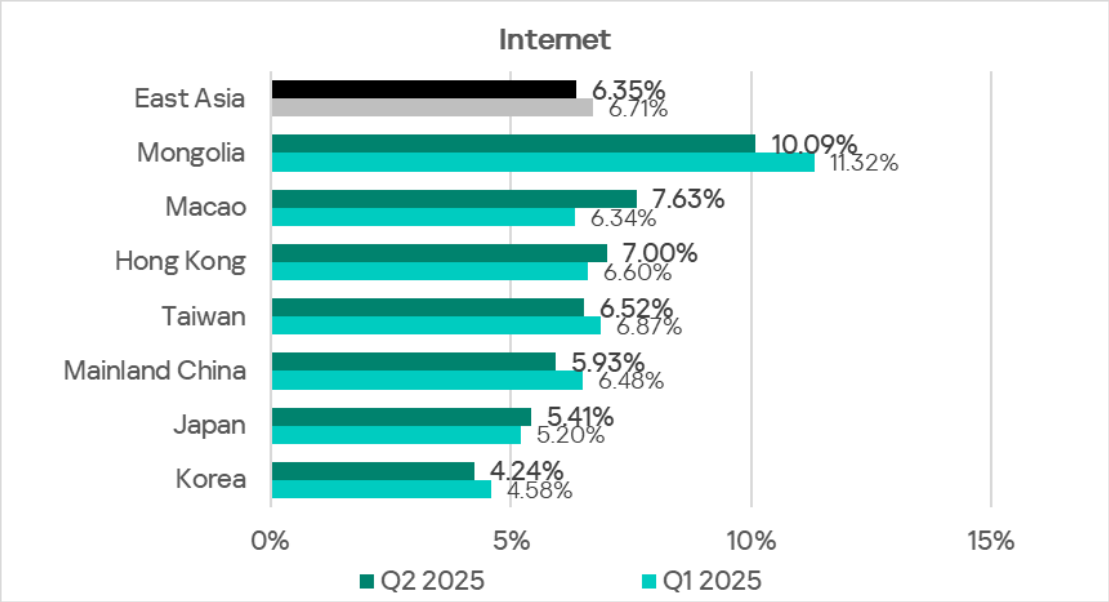
Overall, all major threat sources show a long-term downward trend.



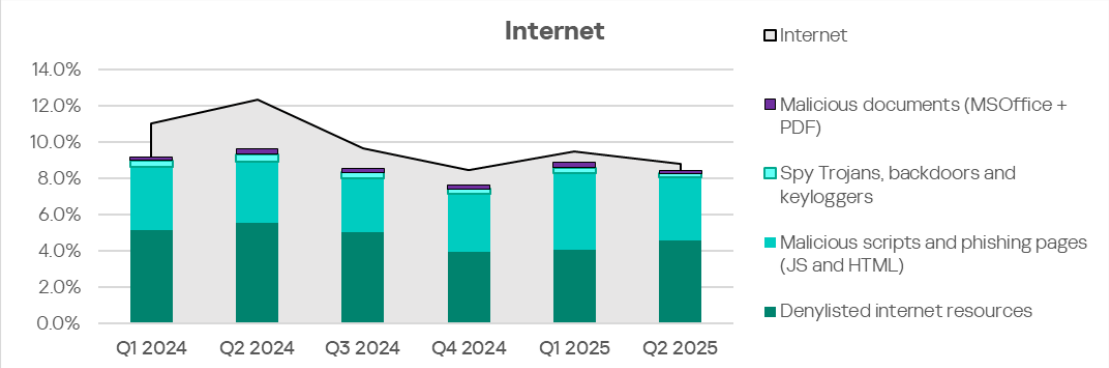
Internet

In Q2 2025, East Asia had the lowest rate of internet threats among all regions at 6.35%. This is also the lowest figure for the region since Q3 2022.

Country-level rates range from 4.24% in Korea to 10.09% in Mongolia.



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

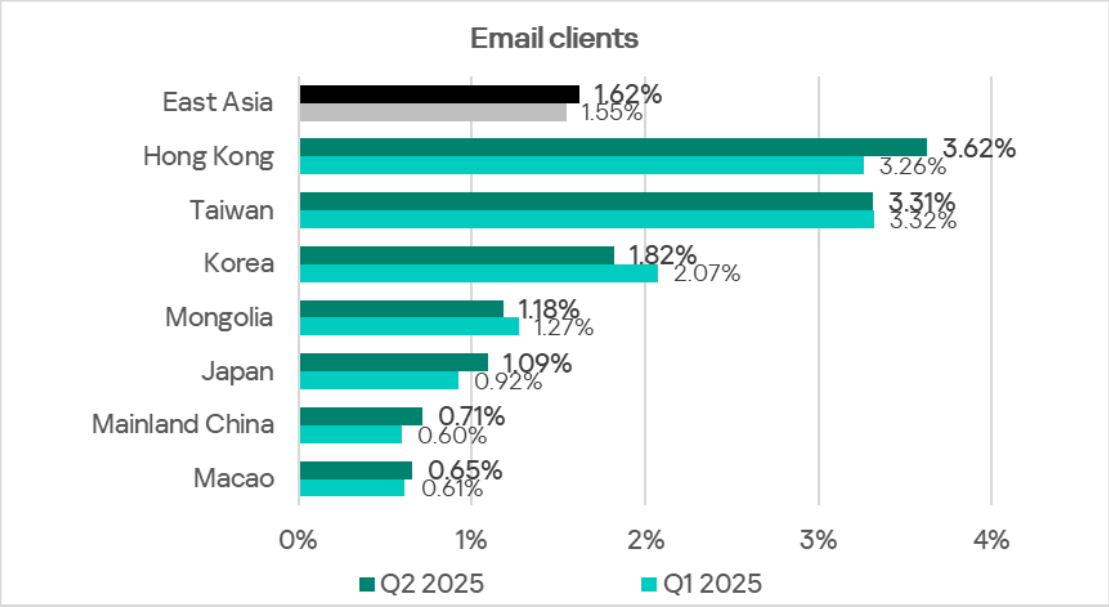


By the percentage of ICS computers on which denylisted internet resources were blocked, Mongolia leads in the region.

Email clients

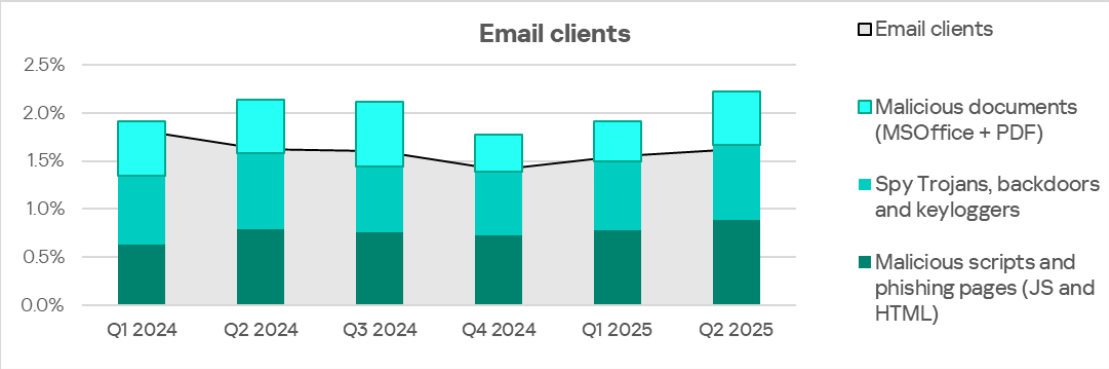
In terms of ICS computers on which threats from email clients were blocked, East Asia ranks 11th globally with 1.62%. This is twice as high as in Russia, which has the lowest rate.

Among countries and territories in the region, Hong Kong (3.62%) and Taiwan (3.31%) lead. Macau records the lowest figure at 0.65%.



Hong Kong and Taiwan also rank among the leaders for threats spreading primarily via email: malicious documents (Taiwan first, Hong Kong third) and malicious scripts and phishing pages (first and second place, respectively).

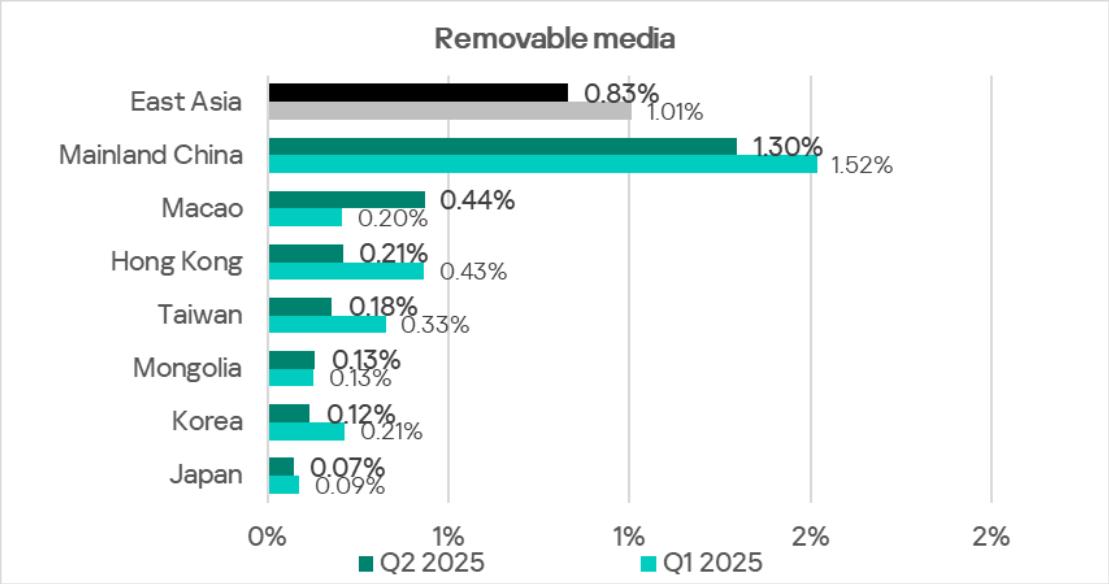
The main categories of mail client threats blocked on ICS computers are malicious documents, spyware, malicious scripts, and phishing pages. Spyware, which ranks first in the region by the percentage of affected ICS computers, spreads across all threat sources, but email is the primary one.



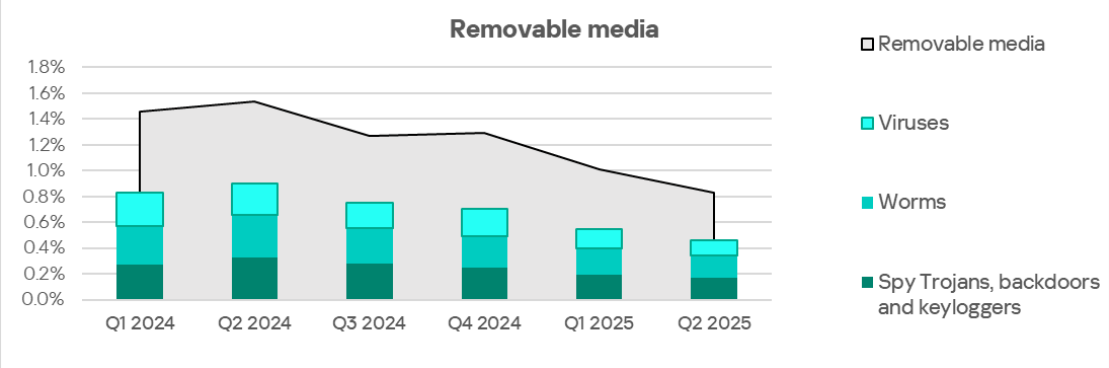
Removable media

By percentage of ICS computers on which threats from removable media were blocked, East Asia ranks second among regions, behind only Africa. The regional figure (0.83%) is 30.9 times higher than that in North America (Canada), which ranks last.

Among the region's countries and territories, Mainland China leads by a significant margin with 1.30%. Other figures range from 0.07% in Japan to 0.44% in Macau.

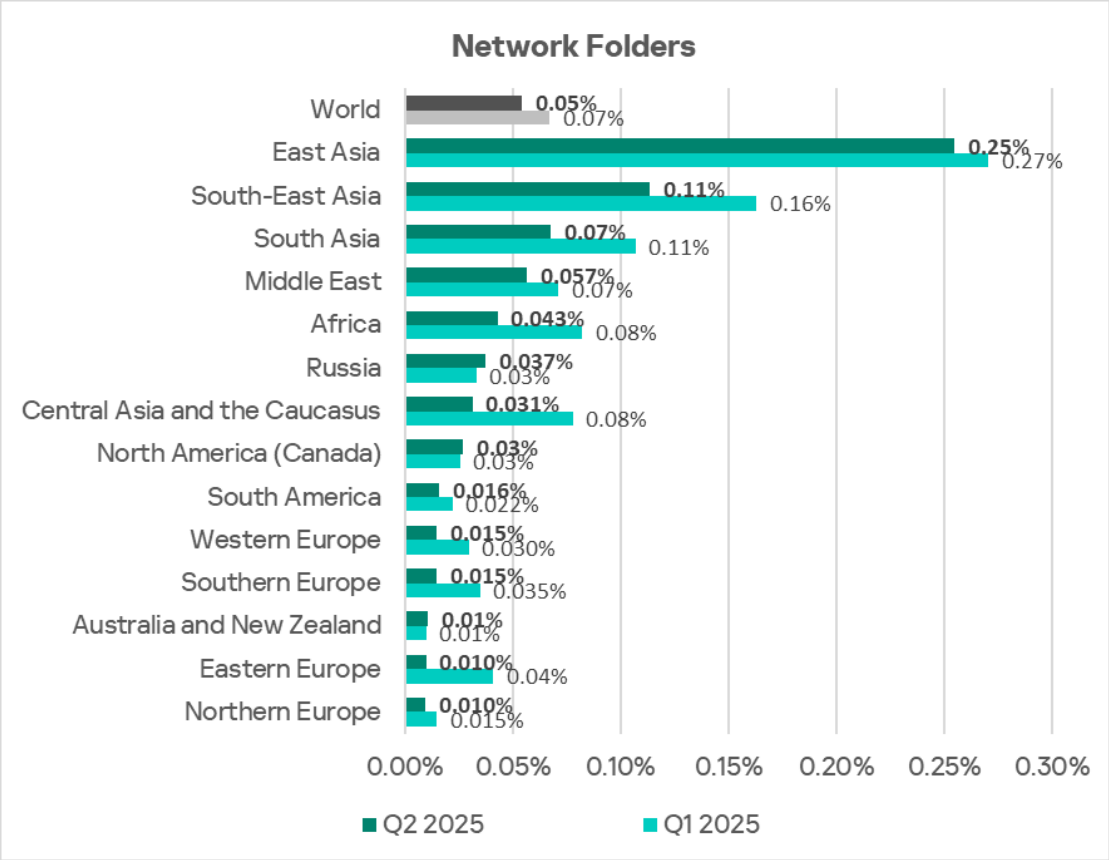


The main categories of threats blocked when connecting removable media to ICS computers are spyware, worms, and viruses. For worms, this is the main distribution channel. Notably, Mainland China also leads in the percentage of ICS computers on which worms were blocked.

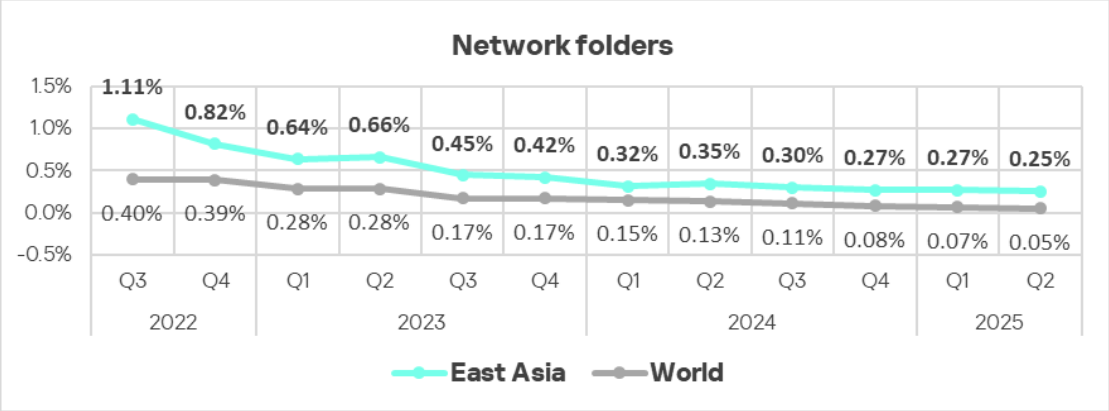


Network folders

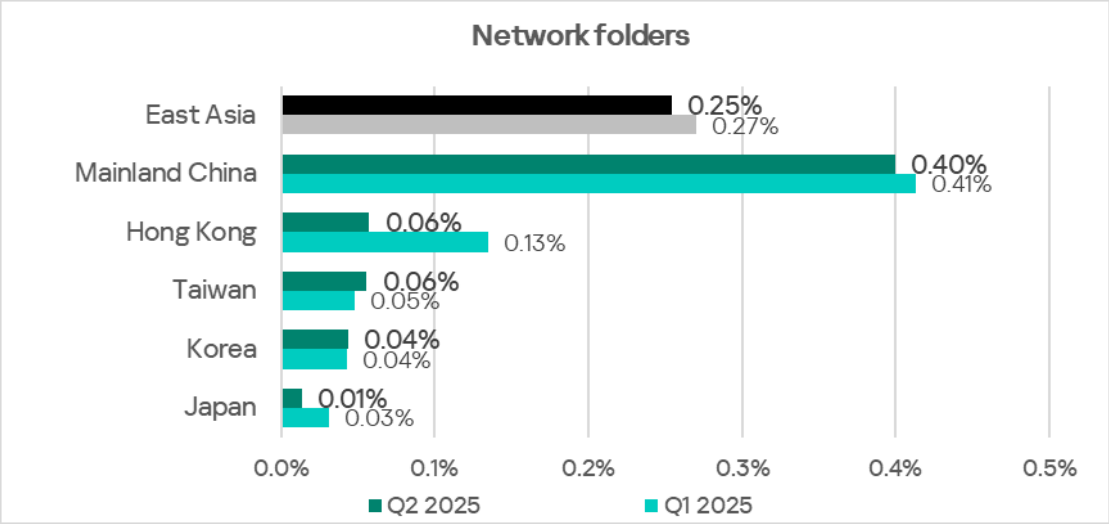
East Asia continues to rank first globally in the percentage of ICS computers on which threats from network folders were blocked. In Q2 2025, the region's figure (0.25%) exceeded the global average by 4.7 times and was 26.3 times higher than in Northern Europe, which ranks lowest.



The percentage of ICS computers on which threats from network folders were blocked in East Asia shows a downward trend, with Q2 2025 recording the lowest rate since Q3 2022.

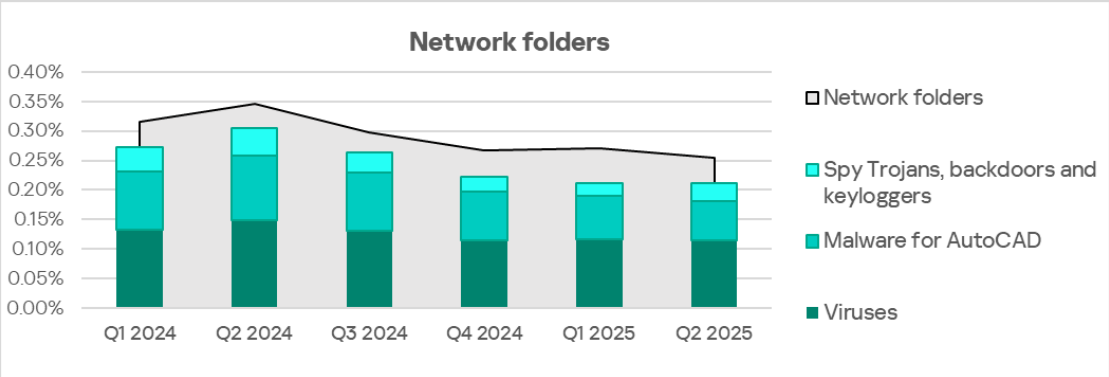


This trend is primarily driven by Mainland China, which dominates among other countries and territories in the region with 0.40%.



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

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

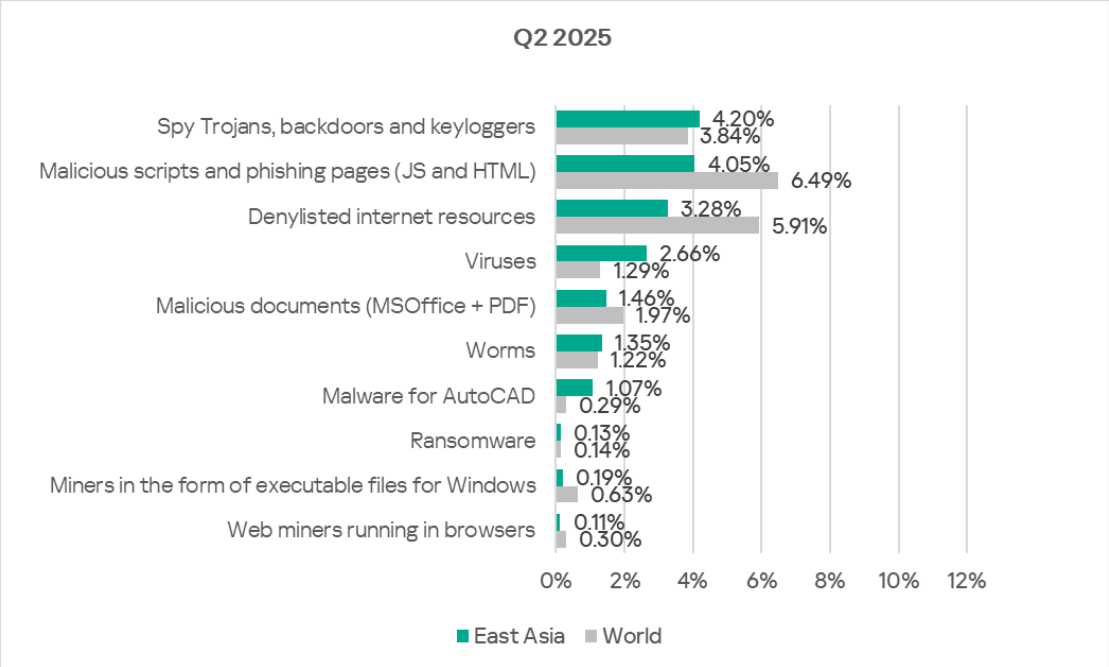


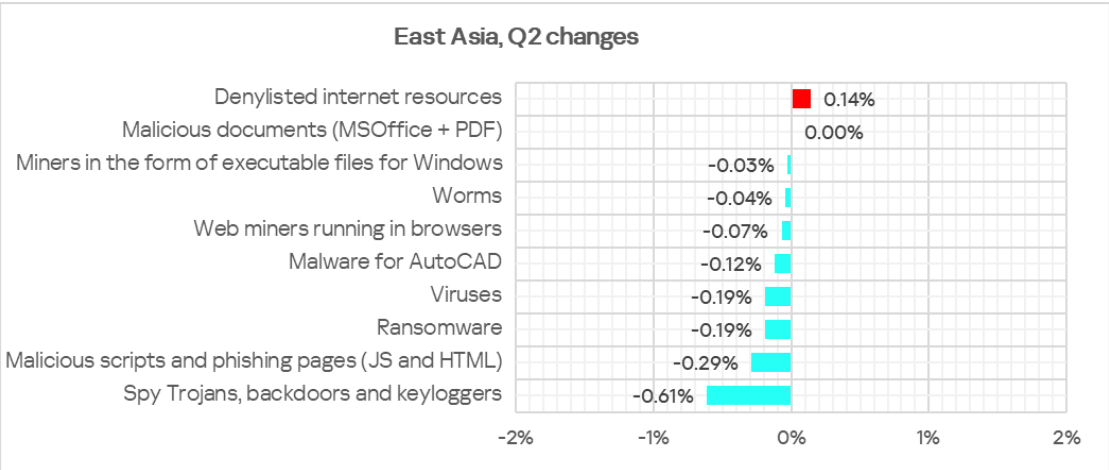
Viruses in the region spread through all threat sources, but the network folder figure for viruses is high, comparable to that for removable media.

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

Threat categories

East Asia is the only region where spyware ranks first among threat categories.





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

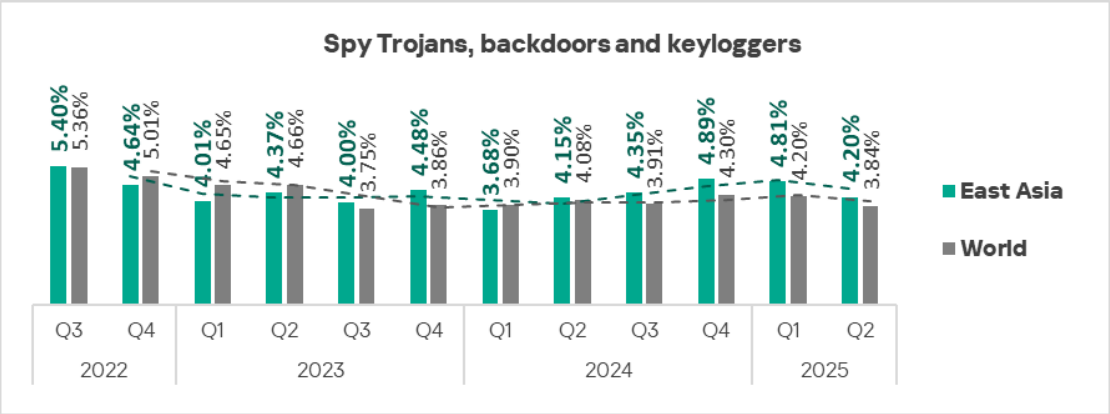
- Spyware — 1.1 times higher
- Viruses — 2.1 times higher, third globally
- Worms — 1.1 times higher
- Malware for AutoCAD — 3.7 times higher, second globally

Spyware

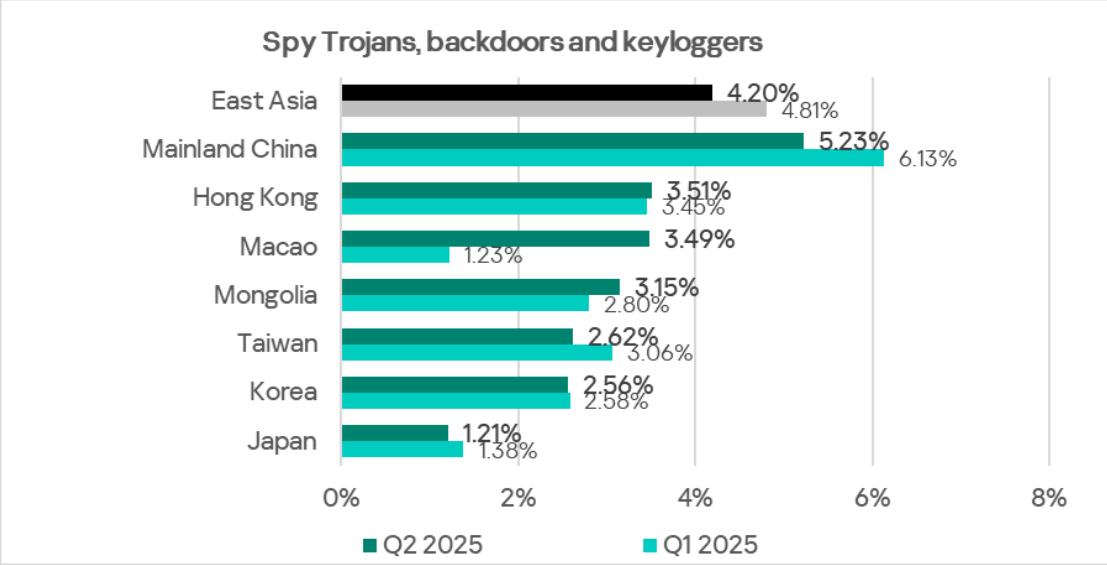
As noted above, East Asia is the only region where spyware tops the threat category rankings.

By the percentage of ICS computers on which spyware was blocked, East Asia ranks seventh among regions, with 4.20%. This is three times higher than Western Europe, which has the lowest rate.

Since late 2022, this metric has remained fairly stable, ranging between 3.68% and 4.89%. The last two quarters have seen a decline.



Among the region's countries and territories, Mainland China leads in the percentage of ICS computers on which spyware was blocked, at 5.23%. Japan has the lowest rate at 1.21%.



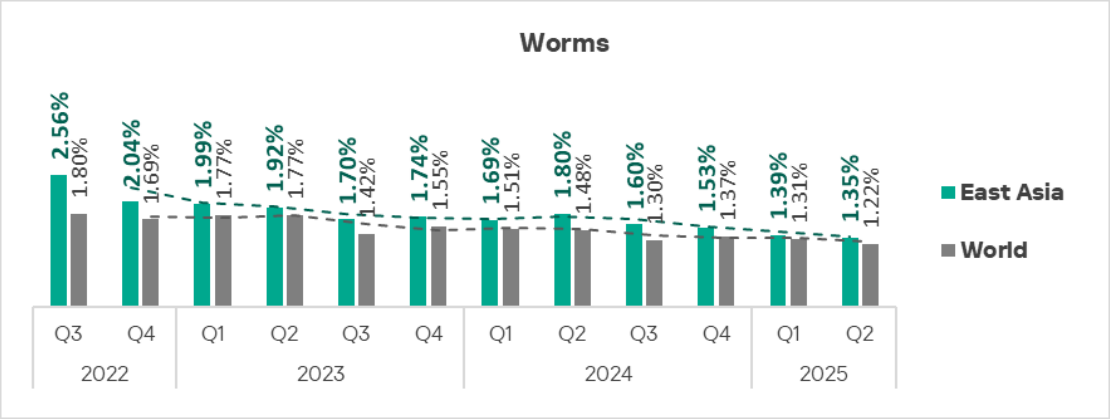
These threats spread through all sources in the region, but primarily via removable media.

Mainland China, which leads in spyware, also ranks at the top in terms of blocked threats from removable media and network folders.

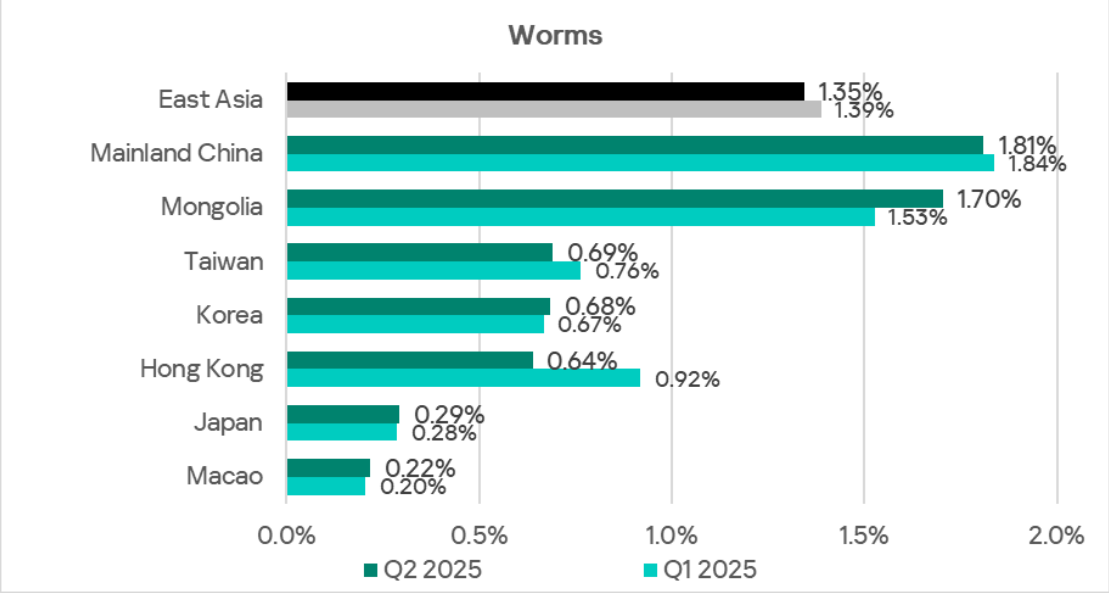
Worms

By the percentage of ICS computers on which worms were blocked, East Asia ranks sixth among regions, with 1.35%. This is 6.1 times higher than Australia and New Zealand, which have the lowest rate globally.

The region's percentage of ICS computers on which worms were blocked has declined for three consecutive quarters. In Q2 2025, it reached its lowest level since Q3 2022.



Among the countries of the region, Mainland China (1.81%) and Mongolia (1.70%) lead in this indicator.



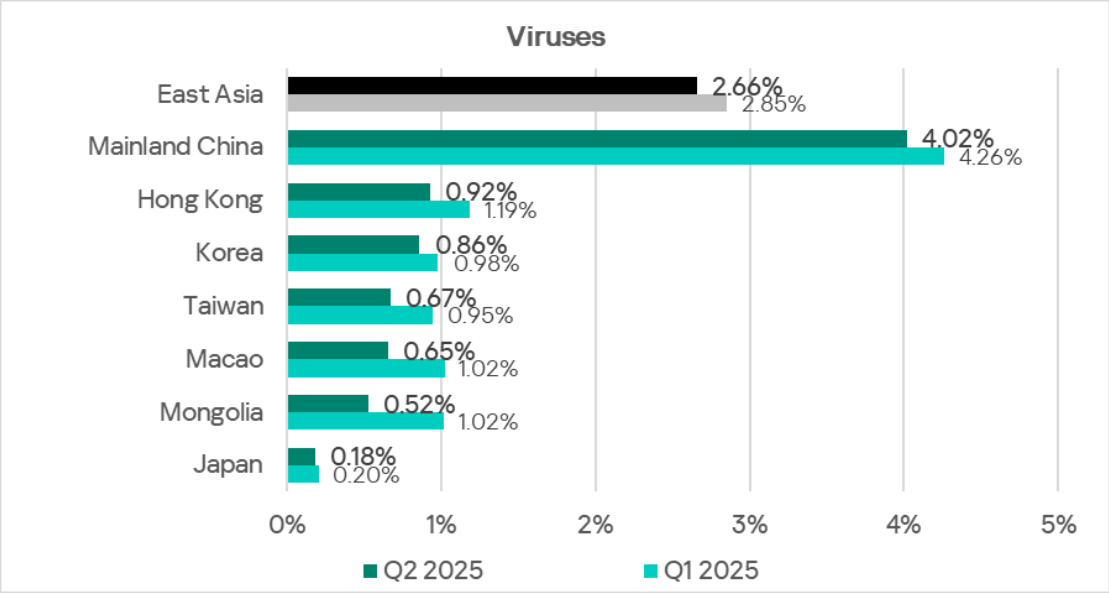
Worms spread mainly through removable media. China, the regional leader in worms, also ranks first in the percentage of ICS computers on which threats from removable media were blocked.

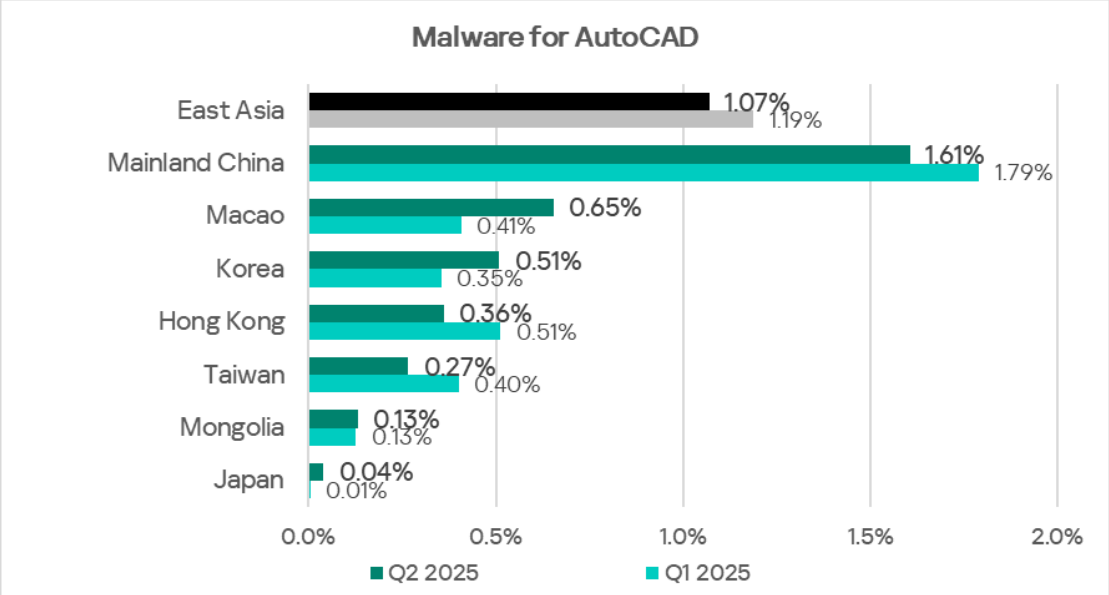
Viruses and malware for AutoCAD

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 South-East Asia.

In both East and South-East 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.

The region's high rate for both categories of malware is primarily driven by Mainland China, which leads the region by a wide margin.





Viruses in the region spread through all threat sources, with the network folder figure comparable to that of removable media.

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

Industries

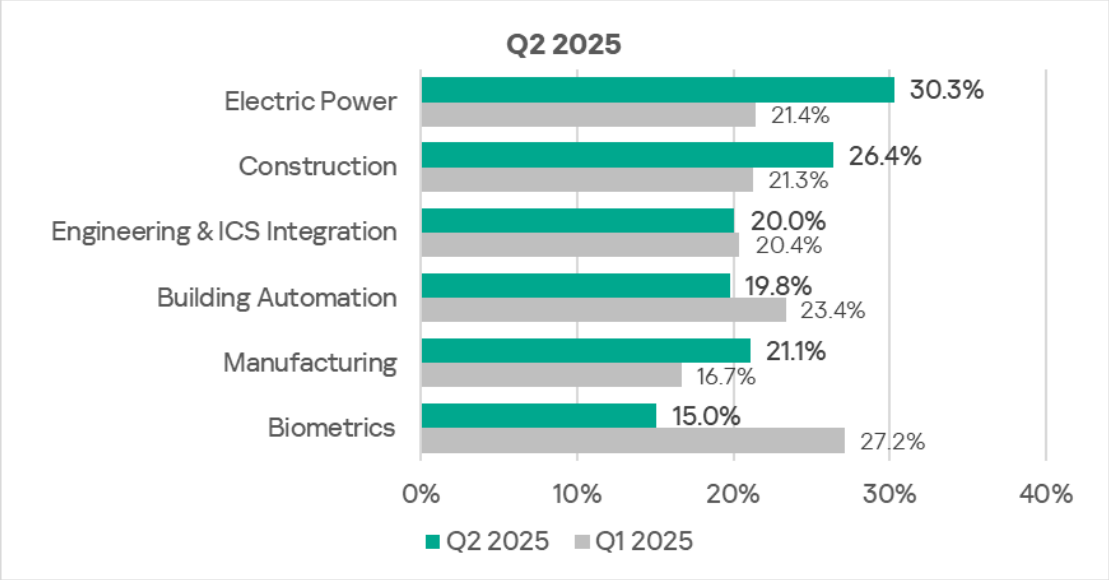
Of the region's industries considered in this report, the most frequently threatened is electrical energy.

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
- Manufacturing — 1.3 times higher
- Construction — 1.2 times higher

In Q2 2025, East Asia led the world in the electrical energy industry with 30.33%.

In manufacturing and construction, East Asia ranks third globally.

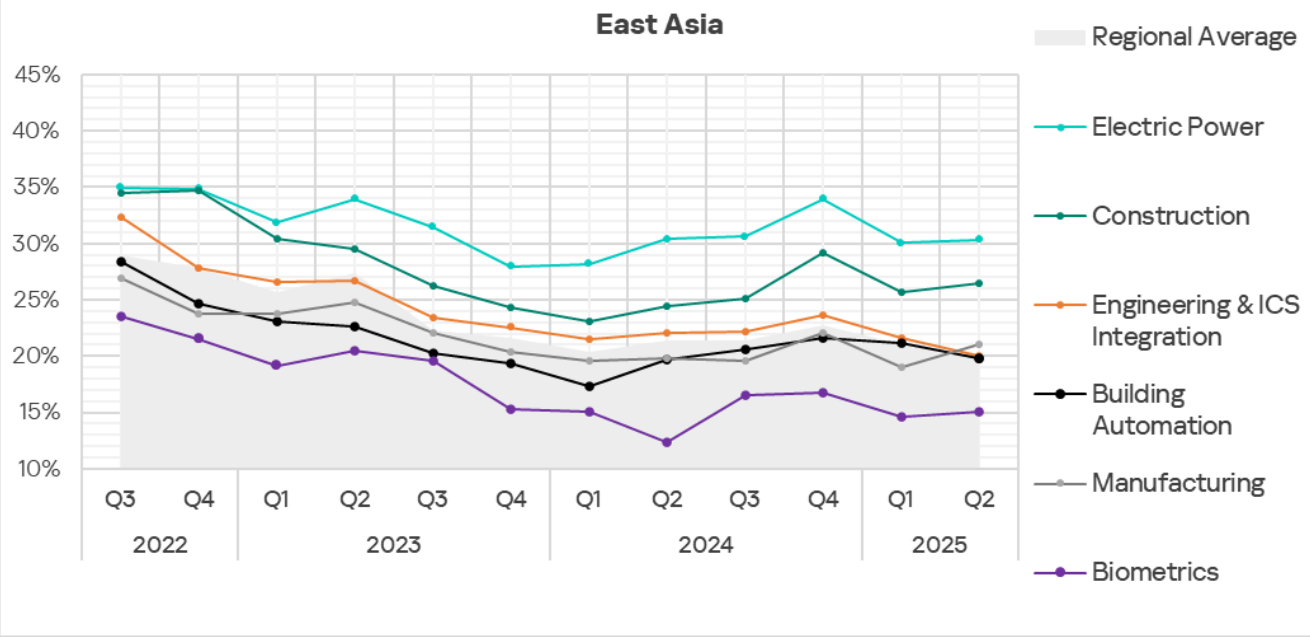


In Q2 2025, the percentage of ICS computers on which malicious objects were blocked declined in only two industries: building automation, and engineering and ICS integrators.

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: hot spots

We use heat maps to assess threats facing industries. On these maps, cells are colored from red to green, where red indicates the maximum value for a threat source or type among all regions and industries. In East Asia, the highest value is in malware for AutoCAD blocked on computers in the construction sector.

The heatmaps highlight industry hot spots: malware sources or categories with values higher than expected given the regional or global ranking of the industry or threat.

Threat source indicators for industries in East Asia, Q2 2025

Industry / Threat source	Biometrics	Building Automation	Electric Power	Engineering & ICS Integration	Construction	Manufacturing	Threat category total in the region
Internet	4.88%	6.44%	10.64%	6.23%	10.61%	7.26%	6.35%
Email clients	5.89%	3.00%	1.19%	1.54%	2.05%	1.73%	1.62%
Removable media	0.00%	1.02%	2.16%	0.77%	0.51%	1.35%	0.83%
Network folders	0.00%	0.33%	0.73%	0.30%	0.57%	0.72%	0.25%
Industry total in the region	15.04%	19.78%	30.33%	20.05%	26.41%	21.06%	

Threat category indicators for industries in East Asia, Q2 2025

Industry / Threat category	Biometrics	Building Automation	Electric Power	Engineering & ICS Integration	Construction	Manufacturing	Threat category total in the region
Denylisted internet resources	2.03%	3.16%	5.74%	3.14%	5.08%	4.13%	3.28%
Malicious scripts and phishing pages (JS and HTML)	5.49%	5.19%	5.48%	3.90%	7.02%	4.81%	4.05%
Spy Trojans, backdoors and keyloggers	5.28%	5.49%	8.57%	4.13%	6.45%	5.00%	4.20%
Worms	0.81%	1.71%	3.18%	1.32%	1.88%	3.17%	1.35%
Miners in the form of executable files for Windows	0.81%	0.37%	0.32%	0.16%	0.34%	0.34%	0.19%
Malicious documents (MSOffice + PDF)	3.05%	2.22%	2.71%	1.54%	2.45%	2.64%	1.46%
Viruses	0.61%	2.04%	5.33%	3.28%	5.42%	3.85%	2.66%
Ransomware	0.00%	0.23%	0.26%	0.12%	0.23%	0.29%	0.13%
Web miners running in browsers	0.61%	0.20%	0.17%	0.08%	0.46%	0.19%	0.11%
Malware for AutoCAD	0.20%	0.92%	2.51%	1.23%	6.33%	1.92%	1.07%
Industry total in the region	15.04%	19.78%	30.33%	20.05%	26.41%	21.06%	

All industries show high levels of spyware, as well as malicious scripts and phishing pages.

Industry hot spots

Electrical energy industry

- Regional leader in internet threats.
- Global leader across all industries in removable media and network folder threats.

- First in the region in spyware, denylisted internet resources, and worms.
- Second place globally in the percentage of ICS computers with blocked threats.
- Second in the region in terms of malicious documents, viruses, malware for AutoCAD, and ransomware.
- Third in the region in terms of malicious scripts and phishing pages.

Construction

- Global leader across all industries in malware for AutoCAD.
- Second in the region in terms of internet threats. Third in the region in terms of mail client and network folder threats.
- Second in the region in terms of spyware, denylisted internet resources, and web miners.

Manufacturing

- Second globally across all industries in network folder threats.
- Second in the region in terms of removable media and network folder threats. Third in the region in terms of internet threats.
- Second in the region in terms of worms.
- Third in terms of denylisted internet resources, malicious documents, viruses, and malware for AutoCAD.

Engineering and ICS integrators

- Fourth in the region in terms of removable media threats.
- Also fourth in viruses and malware for AutoCAD.

Building automation

- Second in the region in terms of email threats. Third in terms of removable media threats. Fourth in internet and network folder threats.
- Second in the region in terms of miners in the form of executable files for Windows.
- Third in spyware, ransomware, and web miners.
- Fourth place in terms of malicious scripts and phishing pages, denylisted internet resources, and worms.

Biometric systems

- Regional leader in email client threats.
- Regional leader in terms of malicious documents and both types of miners.
- Second in the region in terms of malicious scripts and phishing pages.
- Fourth in spyware.

South Asia

Key cybersecurity issues in the region

Lack of control over the use of removable media

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

South Asia ranks fourth among regions by the percentage of ICS computers on which threats from removable media were blocked. The region's figure is 1.7 times higher than the global average.

South Asia ranks third globally for ICS computers on which threats from network folders were blocked. The figure for this threat source is 1.2 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 in terms of ICS computers on which viruses were blocked, and fourth for malware for AutoCAD and 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 threats from the internet were blocked.

Differences among countries in the region

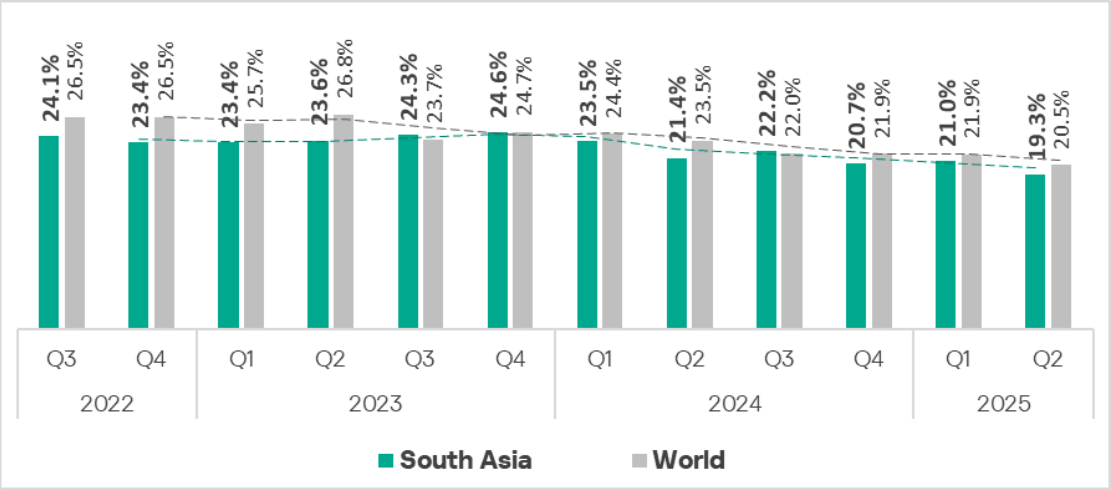
- The region's figures are all heavily influenced by India. India is near the bottom of most rankings by both threat source and category, with a percentage of attacked ICS computers significantly lower than in most other countries of the region and below the regional average.
- Afghanistan's cybersecurity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

Statistics across all threats

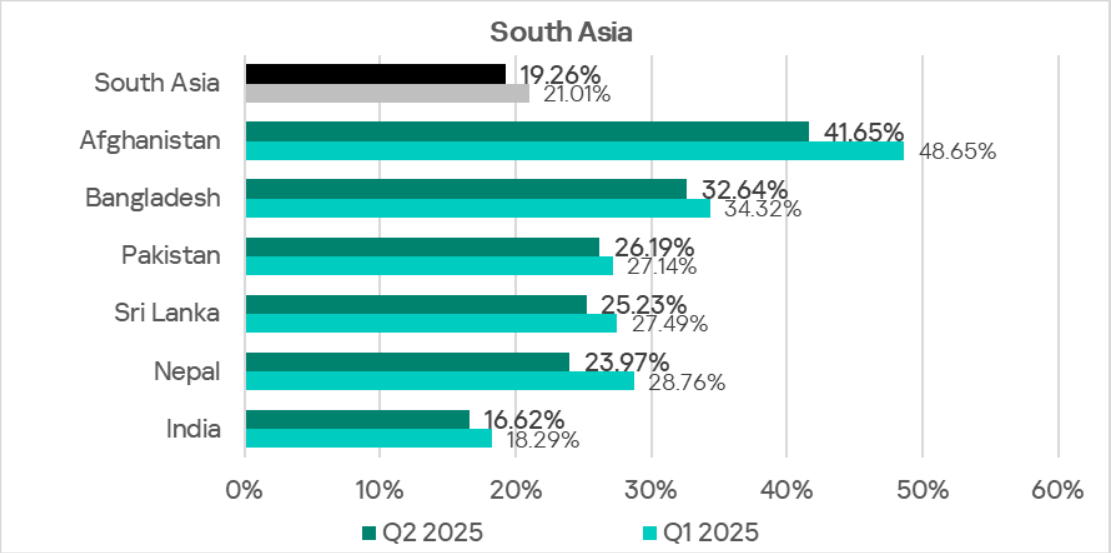
In Q2 2025, South Asia ranked ninth among all regions for the percentage of ICS computers on which malicious objects were blocked. The region's rate dropped

by 1.7 pp over the quarter, ending at 19.3%. This is 1.7 times higher than in Northern Europe, which ranks last.

The region shows a gradual downward trend with some fluctuations.



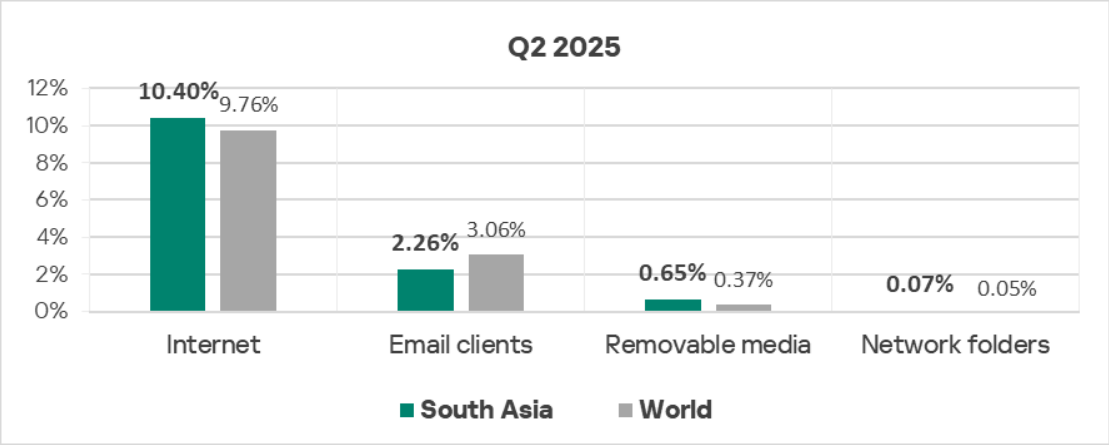
The percentage of ICS computers on which malicious objects were blocked varies among the region's countries, from 16.62% in India to 41.65% in Afghanistan.



Threat sources

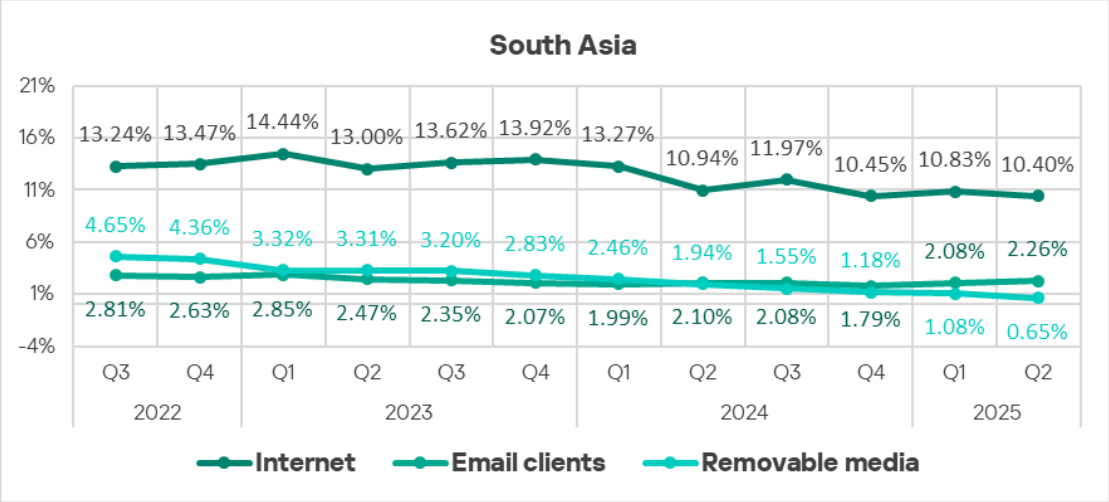
In Q2 2025, South Asia exceeded global averages for all threat sources except email clients:

- Internet — by 1.1 times, third place globally
- Removable media — by 1.7 times, fourth place globally
- Network folders — by 1.2 times, third place globally



The percentage of ICS computers on which malicious objects were blocked decreased for all threat sources except email clients, where the percentage grew to 2.26%.

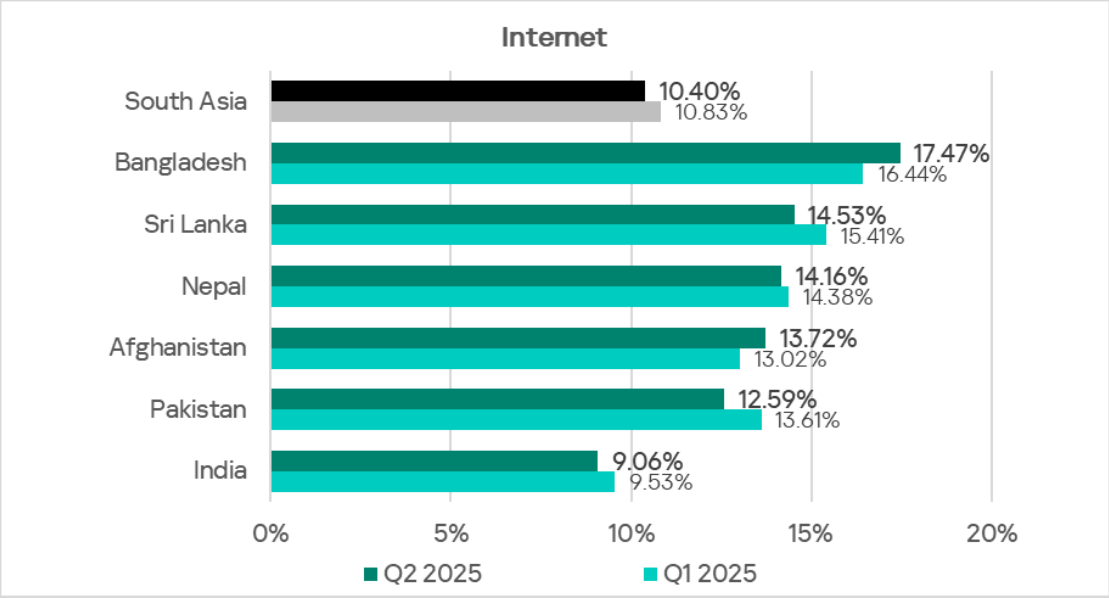
Overall, all major threat sources show a long-term downward trend.



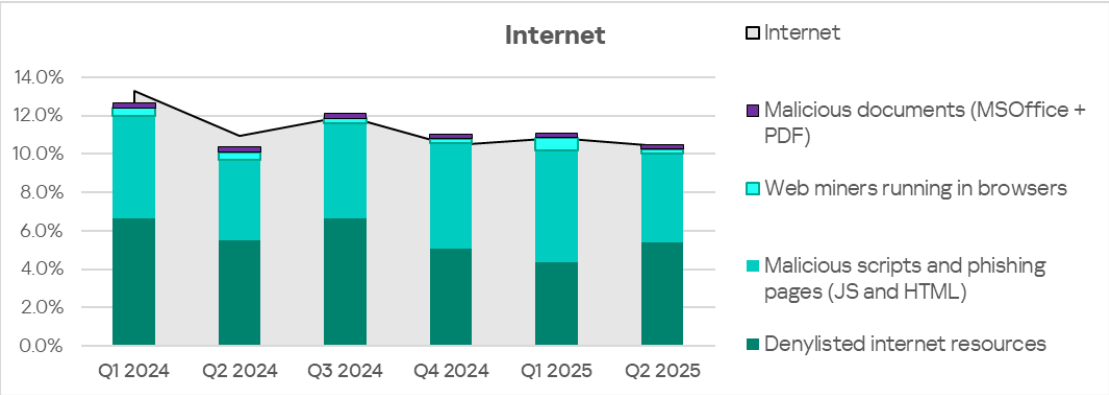
Internet

In Q2 2025, South Asia ranked third globally in terms of the percentage of ICS computers on which threats from the internet were blocked (10.40%). This is 1.6 times higher than East Asia, which ranks last in the regional ranking. This is also the lowest figure for the region since Q3 2022.

Rates among the region's countries range from 9.06% in India to 17.47% in Bangladesh.



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

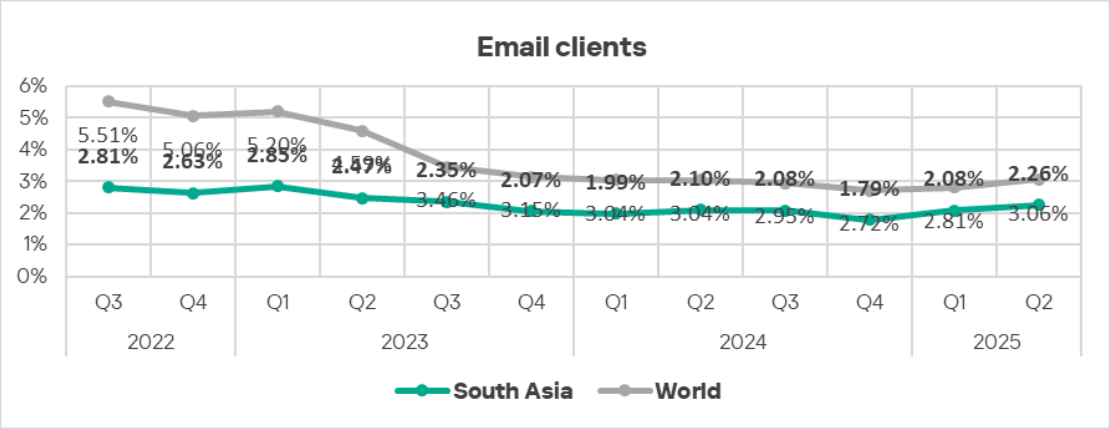


By the percentage of ICS computers on which denylisted internet resources were blocked, Bangladesh leads in the region.

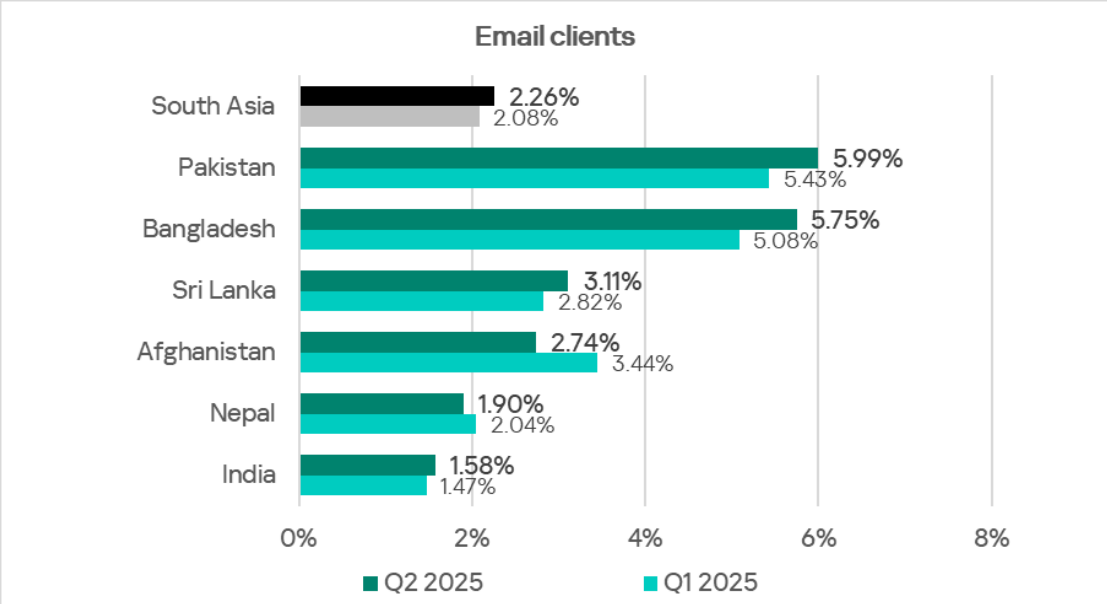
Email clients

In terms of ICS computers on which threats from email clients were blocked, South Asia ranks ninth globally with 2.26%. This is 2.8 times higher than in Russia, which has the lowest figure.

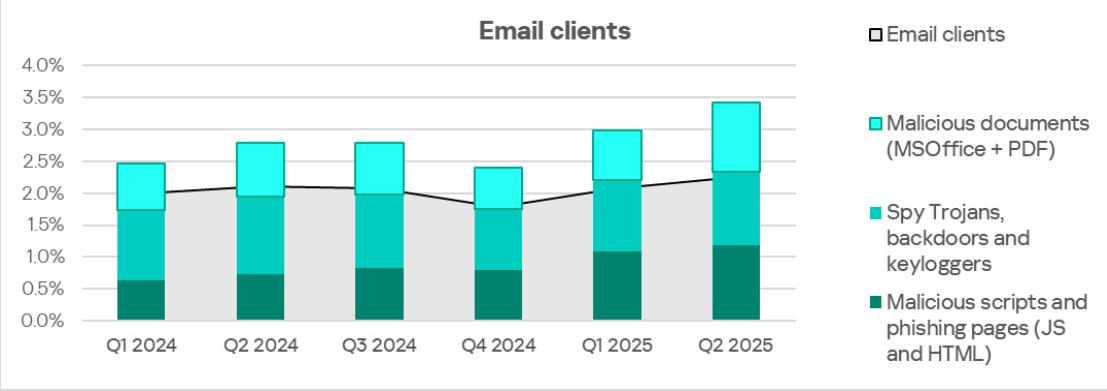
The email clients rate has been rising in the region for two consecutive quarters.



Among the region's countries, Pakistan (5.99%) and Bangladesh (5.75%) lead in the percentage of ICS computers on which threats from email clients were blocked. The lowest figure, 1.58%, is in India.



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

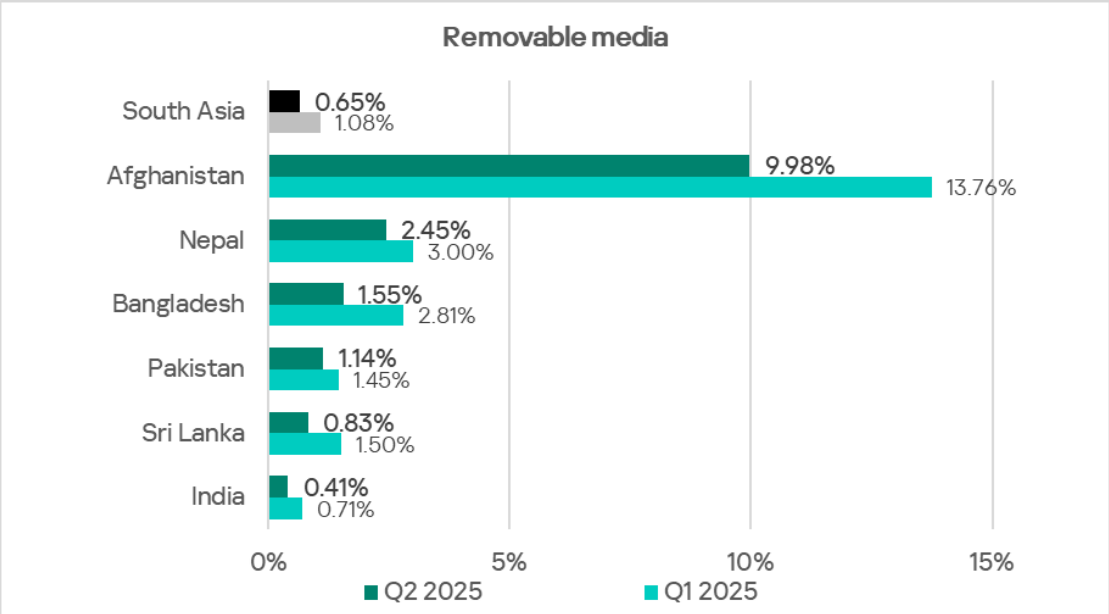


Pakistan and Bangladesh are also among the leaders for threats spread primarily via email (malicious documents, malicious scripts and phishing pages). Bangladesh additionally leads in spyware.

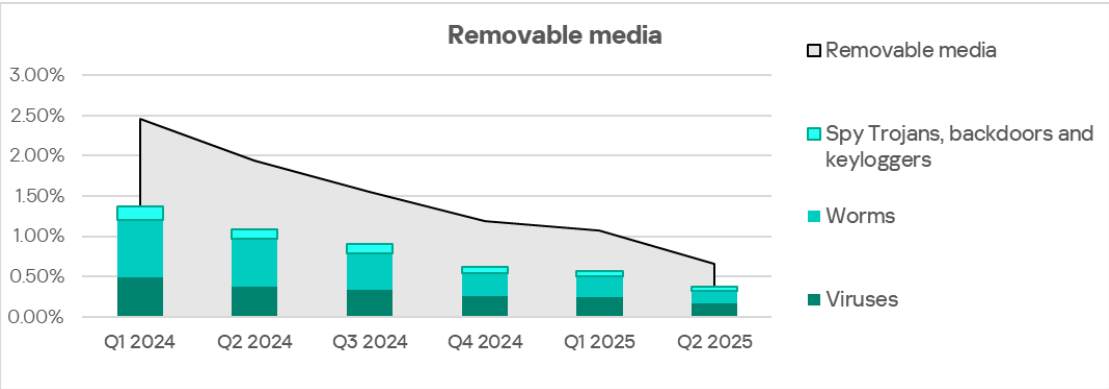
Removable media

By percentage of ICS computers on which threats from removable media were blocked, South Asia ranks fourth globally at 0.65%. This is 24.4 times higher than in North America (Canada), which is at the bottom of this ranking.

Among the region's countries and territories, Afghanistan leads by a wide margin in this metric, at 9.98%. Other countries' percentages range from 0.41% in India to 2.45% in Nepal.



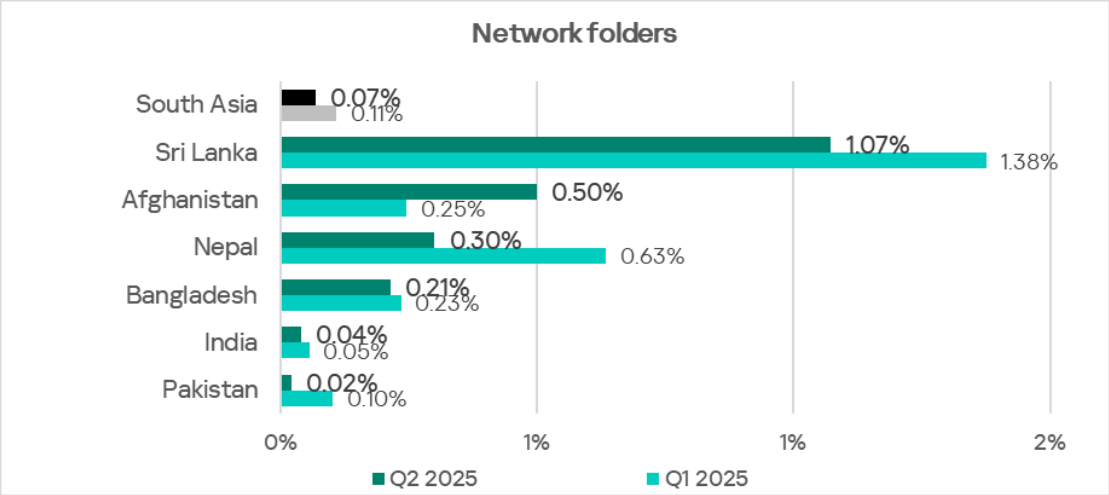
The main categories of removable media threats blocked on ICS computers in the region are worms, spyware, and viruses. Afghanistan also leads (again by a wide margin) in the percentage of ICS computers on which worms were blocked.



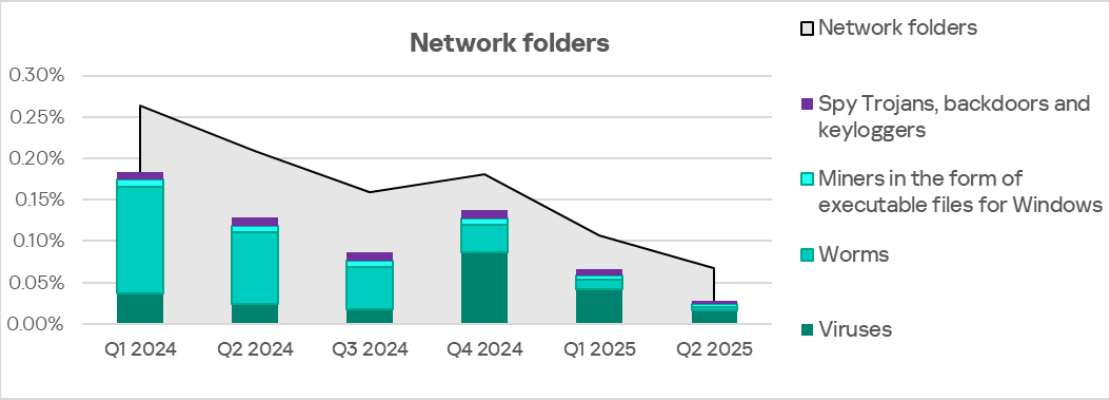
Network folders

South Asia ranks third among regions globally for the percentage of ICS computers on which threats from network folders were blocked. In Q2 2025, the region's figure (0.07%) was 7 times higher than in Northern Europe, which was at the bottom of the ranking.

This high position is due to Sri Lanka, which leads by a wide margin in this metric with 1.07%.

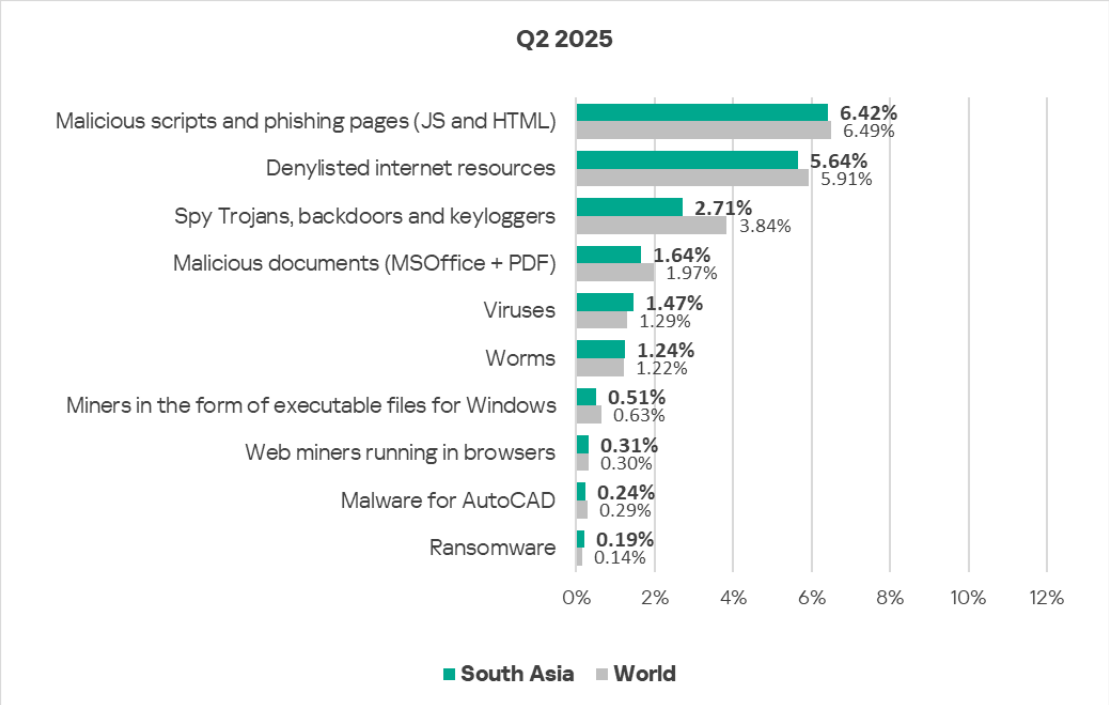


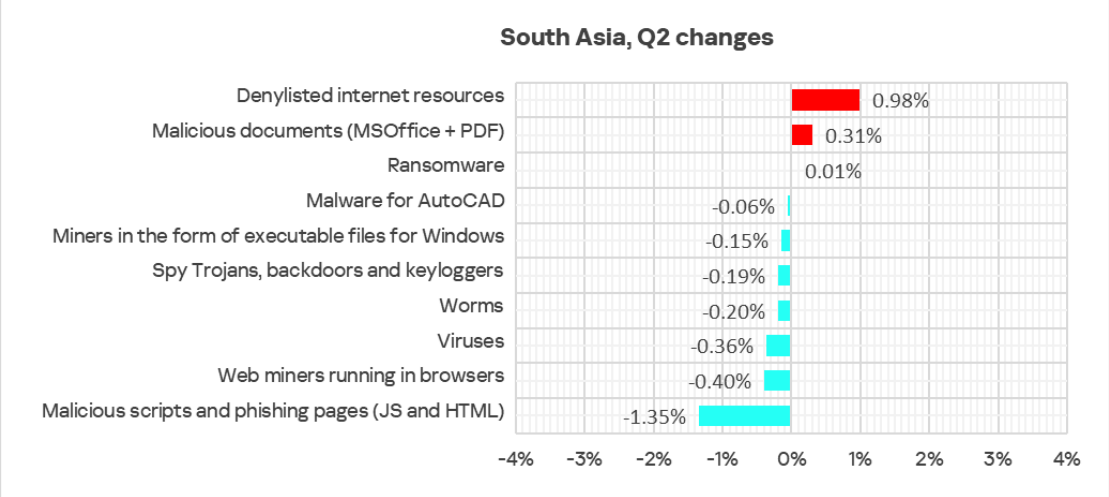
The main threats spreading through network folders are viruses, worms, miners in the form of executable files for Windows, and spyware.



Threat categories

South Asia's ranking of threat categories matches that seen globally.





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

- Viruses — 1.1 times higher
- Ransomware — 1.4 times higher (fourth globally)

South Asia also ranks fourth among all regions by malicious AutoCAD software.

Viruses and malware for AutoCAD

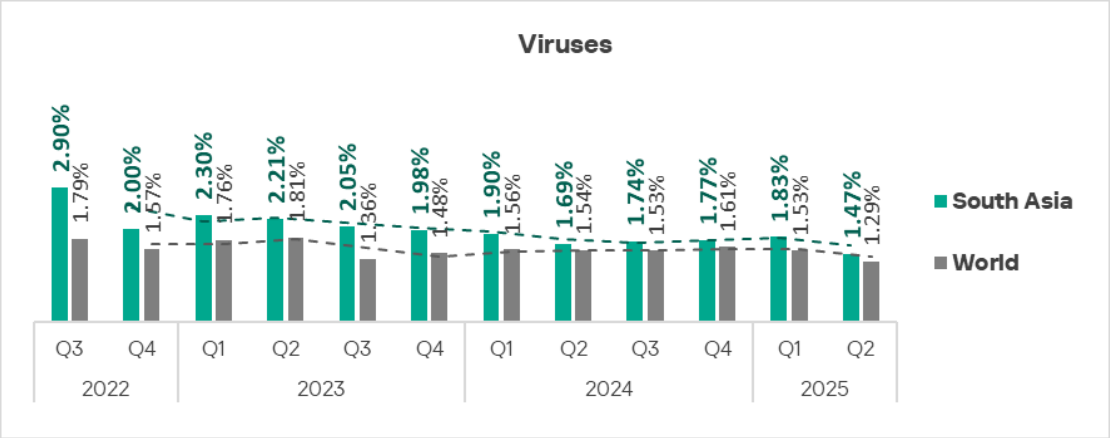
South Asia ranks fifth for ICS computers on which viruses were blocked, and fourth by malware for AutoCAD.

In Q2 2025, the virus rate (1.47%) was 11.6 times higher than in Australia and New Zealand, which were at the bottom of the ranking.

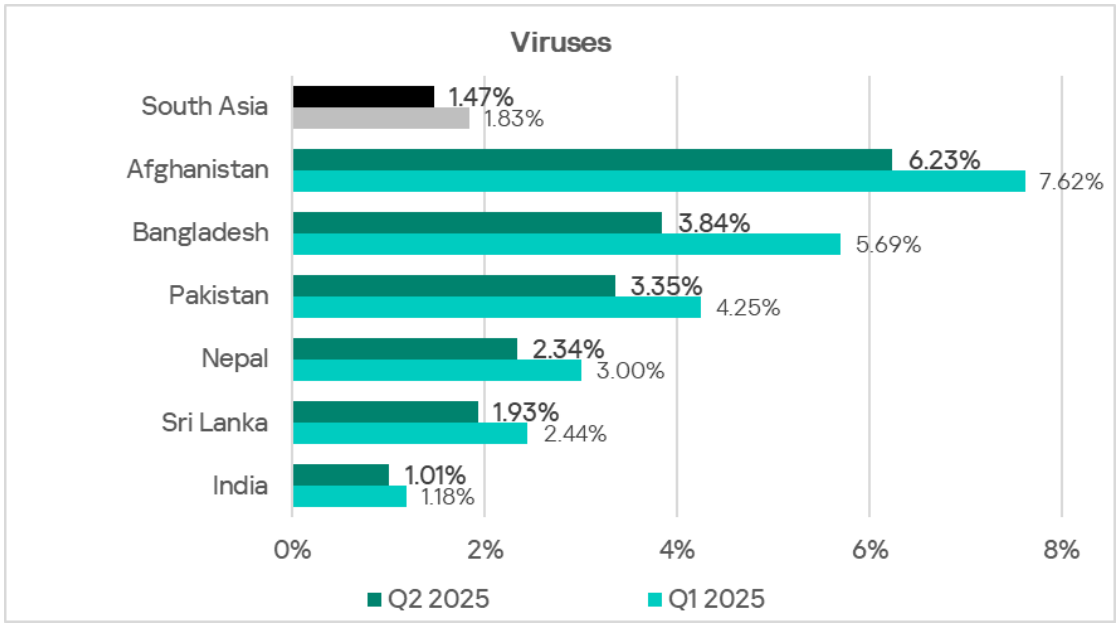
The percentage of ICS computers on which malware for AutoCAD were blocked (0.24%) is 20 times higher than in Northern Europe (the lowest).

As in East and South-East 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 Q2 2025, it reached its lowest since Q3 2022.

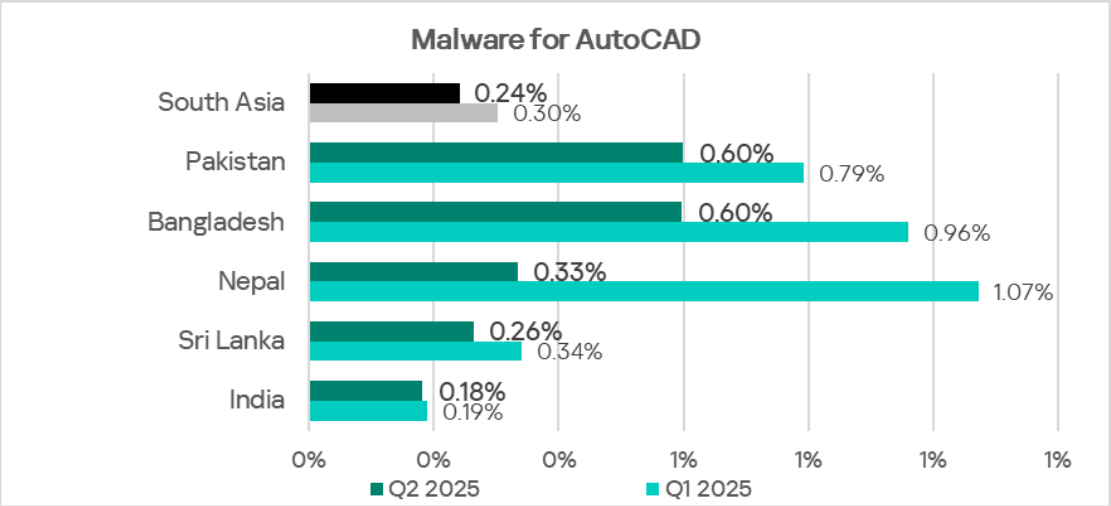


Among the region's countries, Afghanistan leads in the percentage of ICS computers with blocked viruses, at 6.23%.



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

Pakistan and Bangladesh percentage the lead in blocked malware for AutoCAD (0.6% each).

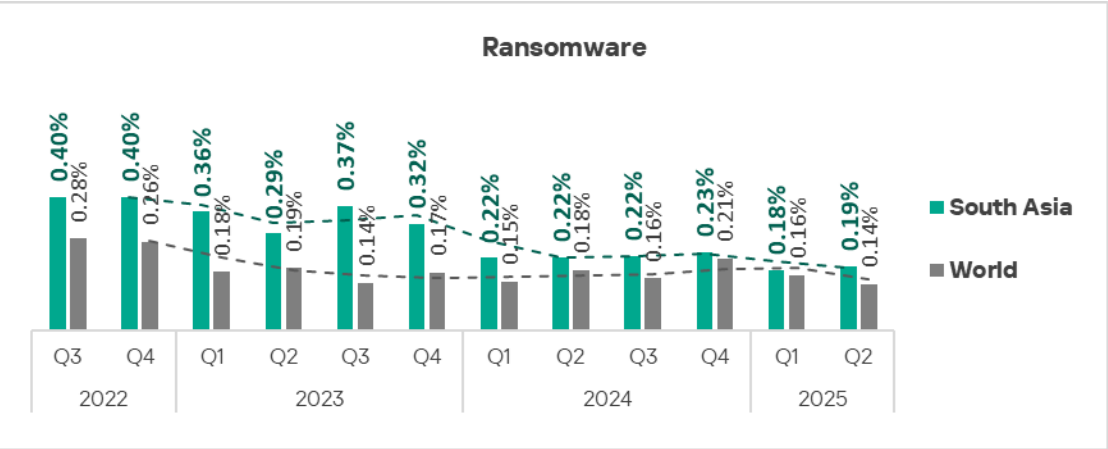


Like viruses, malware for AutoCAD in the region spreads through all sources, but mostly via removable media.

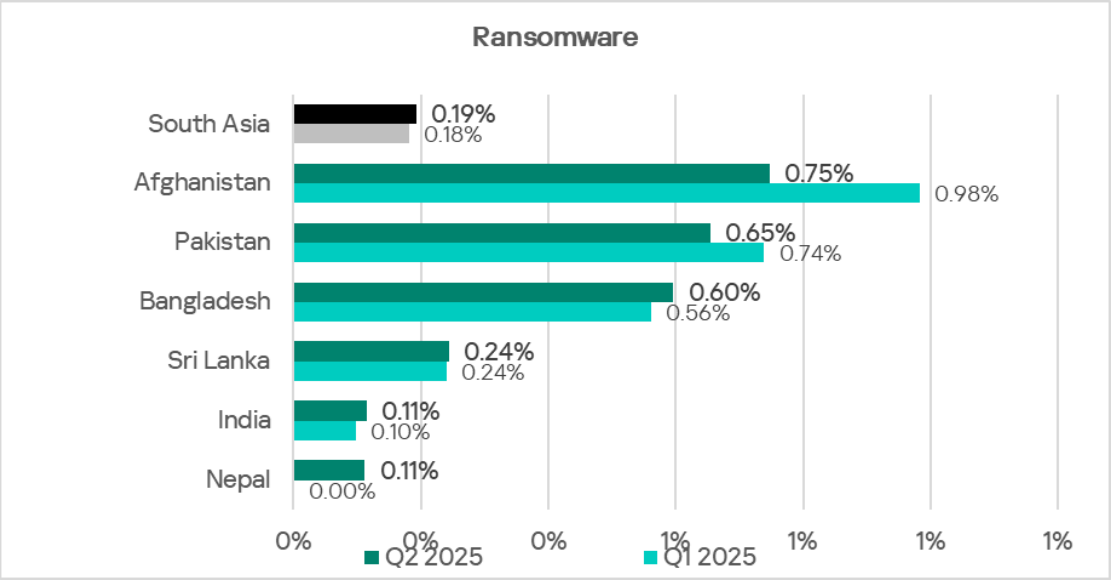
Ransomware

In terms of ICS computers on which ransomware was blocked, South Asia ranks fourth globally. The region's figure (0.19%) is 3 times higher than in Western Europe, which ranks lowest.

Since early 2024, this metric has ranged between 0.18% and 0.23%. The last two quarters have been the lowest since Q3 2022.



Afghanistan leads the region with 0.75%. Next in the ranking are Pakistan and Bangladesh, also showing high rates (0.65% and 0.60%, respectively).

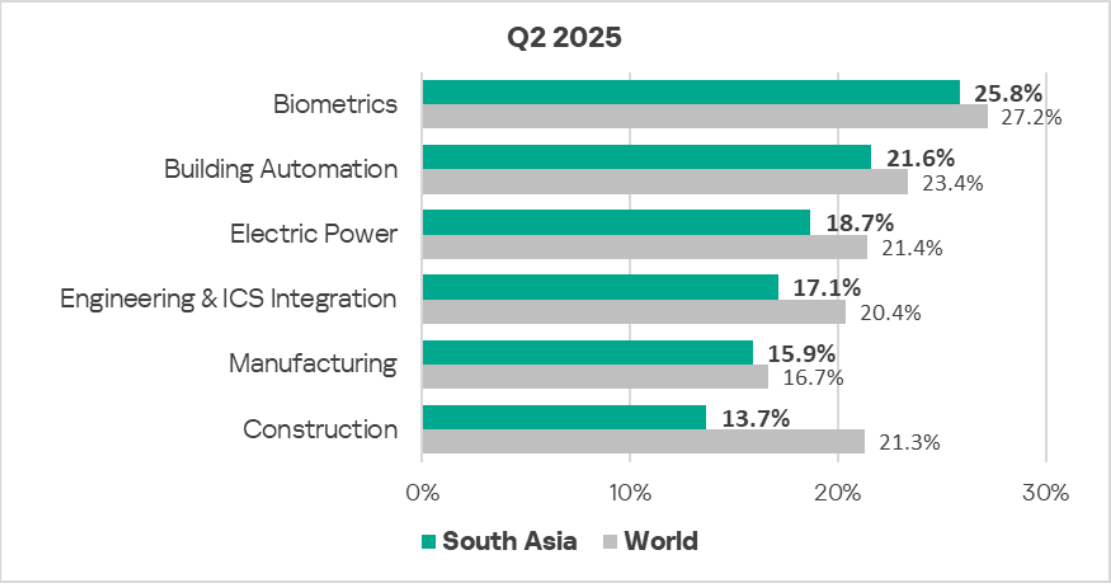


In South Asia, ransomware spreads via email and, most often, via removable media.

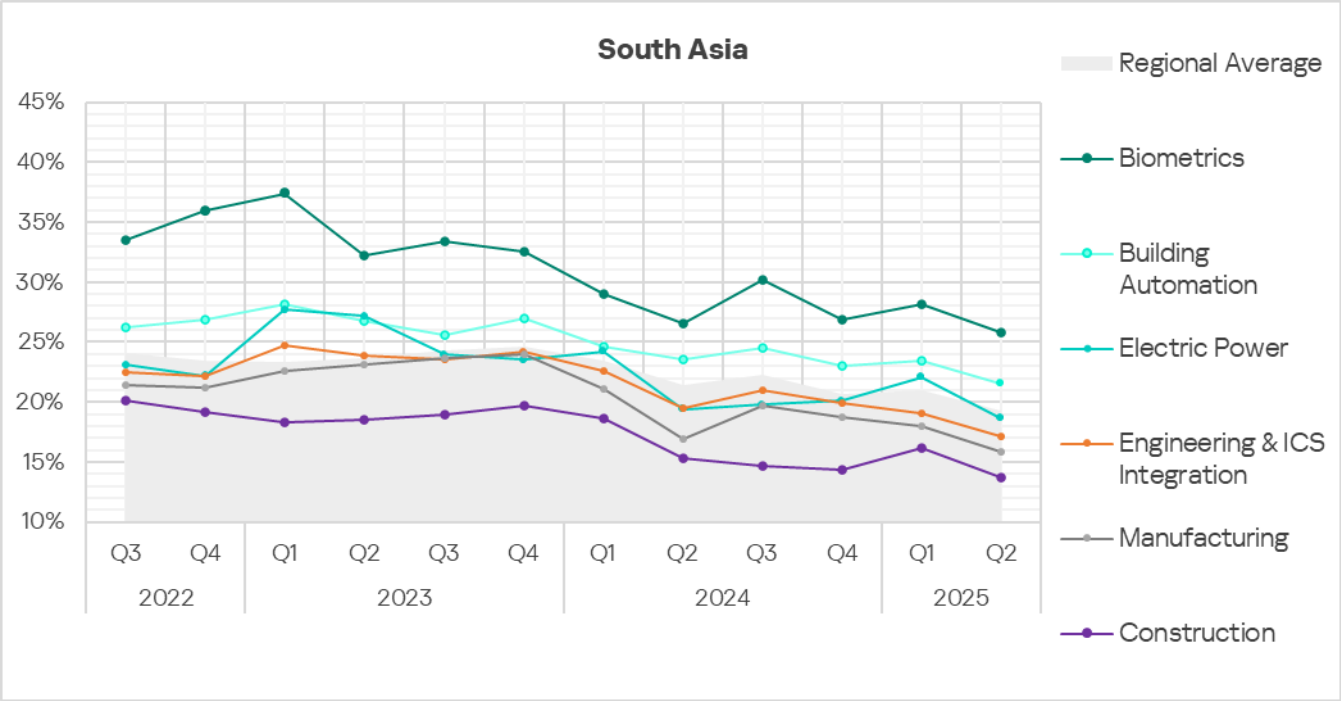
Industries

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 industries are lower.



In Q2 2025, the percentage of ICS computers on which malicious objects were blocked fell across all industries.



Threat sources and malware categories in industries: hot spots

We use heatmaps to assess threats facing industries. On these maps, cells are colored from red to green, where red indicates the maximum value for a threat source or type among all regions and industries. In South Asia in Q2 2025, near-maximum values were observed for the internet and removable media in biometric systems.

The heatmaps highlight industry hot spots — malware sources or categories with values higher than expected given the regional ranking of the industry or threat.

Threat source indicators for industries in South Asia, Q2 2025

Industry / Threat source	Biometrics	Building Automation	Electric Power	Engineering & ICS Integration	Construction	Manufacturing	Threat category total in the region
Internet	12.83%	11.14%	8.19%	10.33%	7.62%	7.70%	10.40%
Email clients	4.68%	3.30%	2.43%	1.02%	1.62%	1.67%	2.26%
Removable media	1.89%	0.81%	0.25%	0.38%	0.23%	0.56%	0.65%
Network folders	0.08%	0.13%	0.05%	0.02%	0.08%	0.00%	0.07%
Industry total in the region	25.81%	21.56%	18.66%	17.10%	13.66%	15.89%	

Threat category indicators for industries in South Asia, Q2 2025

Industry / Threat category	Biometrics	Building Automation	Electric Power	Engineering & ICS Integration	Construction	Manufacturing	Threat category total in the region
Denylisted internet resources	7.32%	5.88%	4.81%	5.85%	3.67%	4.72%	5.64%
Malicious scripts and phishing pages (JS and HTML)	9.89%	7.80%	5.21%	5.16%	3.93%	4.65%	6.42%
Spy Trojans, backdoors and keyloggers	5.66%	3.70%	3.09%	1.59%	1.41%	2.64%	2.71%
Worms	1.66%	1.51%	1.47%	0.71%	0.62%	1.25%	1.24%
Miners in the form of executable files for Windows	0.45%	0.51%	0.25%	0.39%	0.26%	0.49%	0.51%
Malicious documents (MSOffice + PDF)	3.40%	2.36%	1.72%	0.88%	0.85%	0.83%	1.64%
Viruses	3.17%	1.77%	1.47%	0.95%	1.10%	1.46%	1.47%
Ransomware	0.53%	0.26%	0.10%	0.11%	0.00%	0.14%	0.19%
Web miners running in browsers	0.23%	0.32%	0.30%	0.26%	0.28%	0.21%	0.31%
Malware for AutoCAD	0.15%	0.12%	0.15%	0.32%	0.80%	0.49%	0.24%
Industry total in the region	25.81%	21.56%	18.66%	17.10%	13.66%	15.89%	

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).

Industry hot spots

Biometric systems

- Leader among the region's industries in all threat sources except network folders (third place for this source).
- Leader in all threat categories except miners in the form of executable files for Windows (third place), web miners, and malware for AutoCAD.

Building automation

- Regional leader in threats from network folders. Ranks second in all other threat sources.
- Regional leader in both types of miners. Ranks second in all other categories except malware for AutoCAD.

Electrical energy industry

- The region's third place in email threats. Ranks fourth in internet threats and network folder threats.

- Second place in web miners.
- Third place in malicious scripts and phishing pages, spyware, malicious documents, viruses, and worms.
- Ranks fourth in malware for AutoCAD.

Engineering and ICS integrators

- Third place in internet threats, fourth in removable media.
- Ranks third in denylisted internet resources and malware for AutoCAD.
- Fourth in malicious scripts and phishing pages, malicious documents, both types of miners, and malware for AutoCAD.

Manufacturing

- Ranks third in the region in removable media threats, and fourth for email threats.
- Ranks second in miners in the form of executable files for Windows and malware for AutoCAD.
- Third place in ransomware and fourth in spyware, viruses, and worms.

Construction

- Ranks second regionally in terms of network folder threats.
- Leads the ranking for malware for AutoCAD.
- Third place in web miners.

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