Kaspersky ICS CERT

kaspersky

Threat landscape for industrial automation systems

South and North America (Canada). Q3 2025

23.12.2025

Version 1.0

South America

Key cybersecurity issues in the region

High risk of targeted attacks

In South America, the percentage of ICS computers on which threats from mail clients were blocked is 1.8 times higher than the global average. On this metric, the region ranks third globally.

High levels of email threats (phishing) and spyware clearly indicate that industrial OT systems in the region are highly exposed to advanced attackers.

Likewise, the large percentage of malicious scripts and phishing pages further demonstrates the high risk of targeted attacks against the technological infrastructures of industrial enterprises in the region. Many of these scripts and pages are aimed directly at stealing employee authentication data for corporate services.

High rate of malicious documents

Based on the percentage of ICS computers on which malicious documents were blocked in Q3 2025, South America is the leader among regions. The region's figure is 2.1 times higher than the global average.

Attackers distribute malicious documents in phishing emails and use them as an initial infection vector. Malicious documents usually contain exploits, malicious macros, and malicious links.

In Q3 2025, South America also leads in growth of the malicious documents indicator. The significant growth in the percentage of ICS computers on which malicious documents were blocked was caused by a large-scale phishing campaign in which the threat actors used new exploits for the old vulnerability CVE-2017-11882 in Microsoft Office Equation Editor to deliver various spyware to victims' computers.

Notably, the threat actors in this phishing spree used localized texts for messages in Spanish, and the contents of the text compared to standard phishing text was more similar to business letters.

High rate of malicious scripts and phishing pages

Based on the percentage of ICS computers on which malicious scripts and phishing pages were blocked, South America ranks third among regions with a rate that is 1.4 times higher than the global average.

Malicious scripts are used by attackers for a wide range of purposes — from data collection, tracking, and redirecting the user's browser to malicious web resources, to downloading various malware into the system or browser (such as spyware, cryptominers, and ransomware). They are distributed both via the internet and through spam emails.

High rate of spyware

The percentage of ICS computers on which spyware was blocked in South America is 1.1 times higher than the global average. In the regional ranking of threat categories, spyware occupies second place.

Spyware is used by attackers to steal confidential data. In targeted attacks, it is also used for lateral movement within compromised networks and for downloading final-stage malware.

Spyware is also used for stealing information required for delivering other types of malware, such as ransomware.

Threats in industries

In the regional rankings based on the percentage of ICS computers on which malicious documents are blocked in various industries, South America is in the top 3 based on the indicators for this threat category in all industries. This region leads in indicators for the oil and gas industry and the engineering and ICS integrators industry.

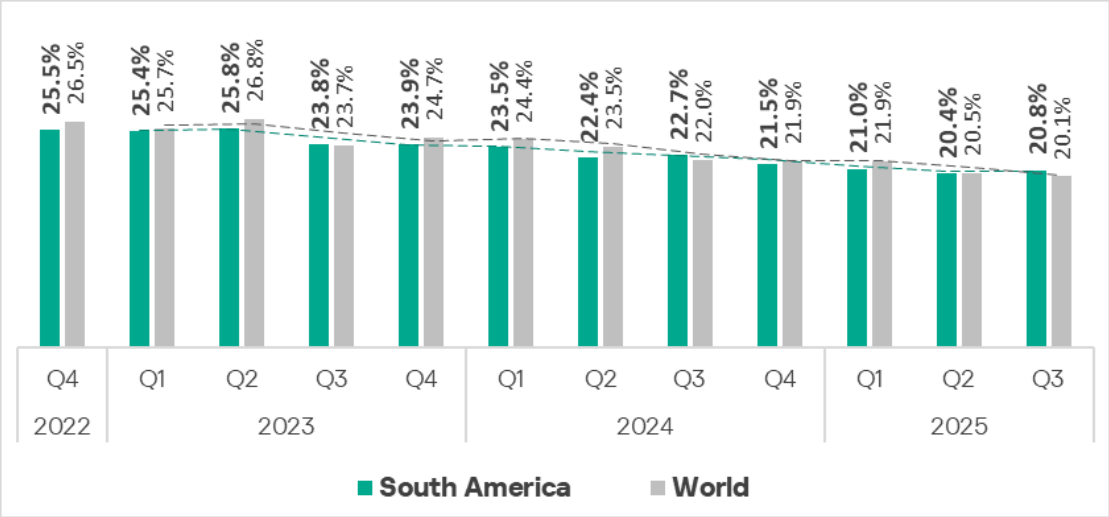
Most industries are showing high indicators for malicious scripts and phishing pages, and for spyware. Based on the indicator for malicious scripts in the electrical energy industry, South America is the leader among regions.

Based on the ransomware indicator in the engineering and ICS integrators industry, South America occupies fourth place among regions.

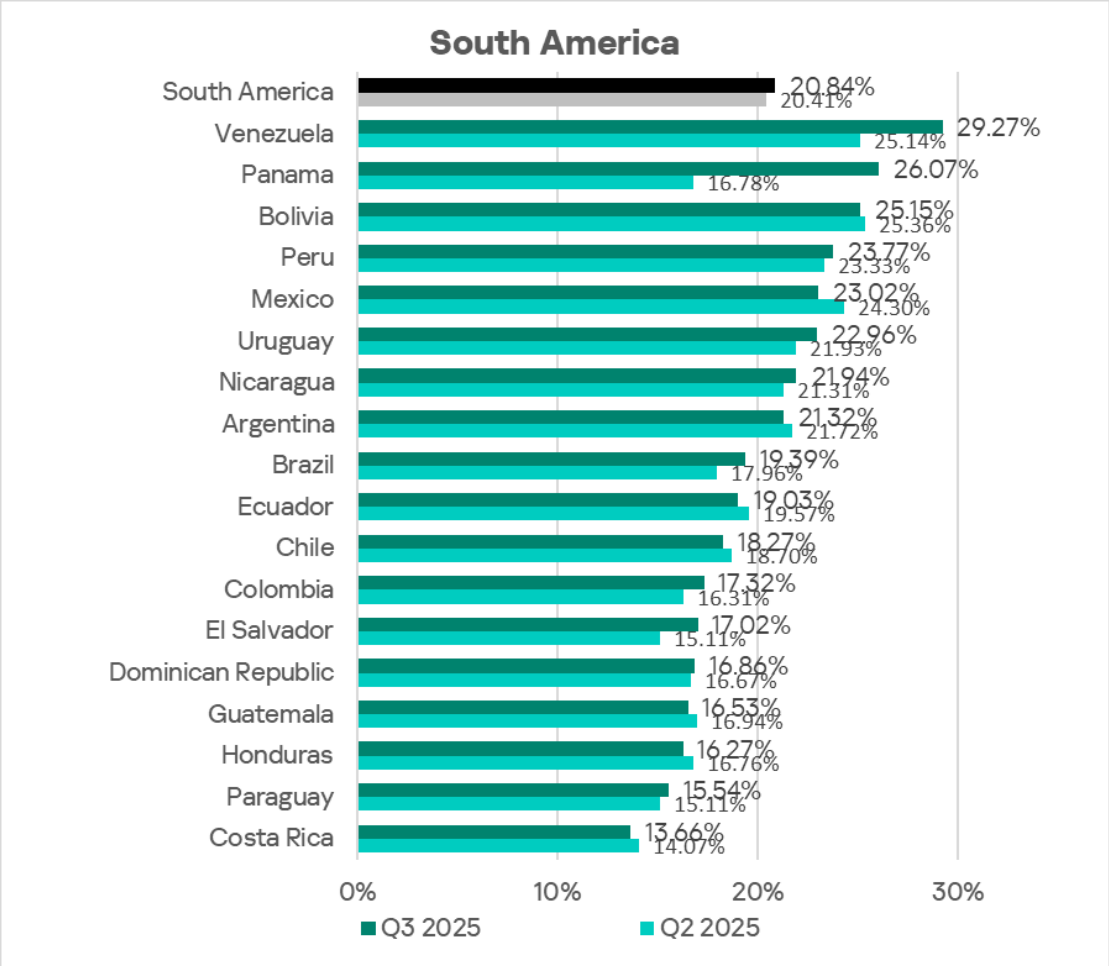
Statistics across all threats

In Q3 2025, South America ranks sixth among regions in the percentage of ICS computers on which malicious objects were blocked with its rate of 20.8%. This is 2.3 times higher than in Northern Europe, which boasts the lowest percentage among all regions.

A downward trend is evident. In Q3 of 2025, after this indicator decreased over the course of the three previous quarters, South America saw an increase in the percentage of ICS computers on which malicious objects were blocked.

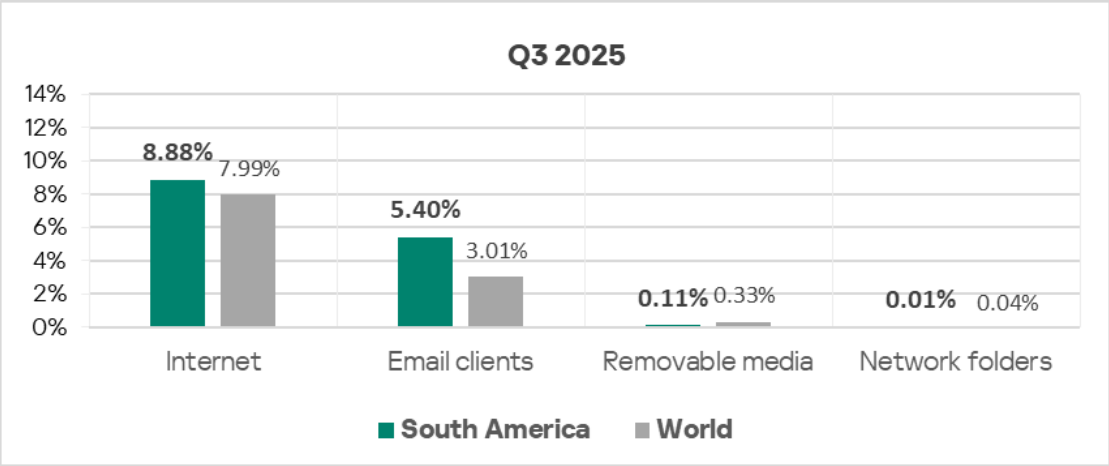


The percentage of ICS computers with blocked malicious objects varies among the region's countries, from 13.66% in Costa Rica to 29.27% in Venezuela.



Threat sources

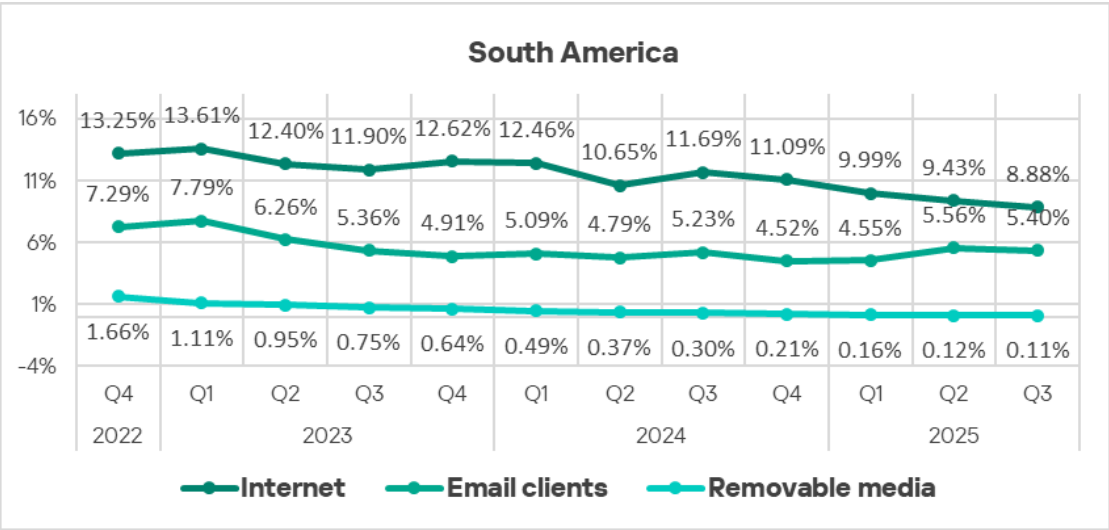
Malicious objects in the region spread primarily via the internet and email.



In Q3 2025, compared to global indicators, the region has a higher percentage of ICS computers on which threats were blocked from the following sources:

- Internet: 1.1 times higher.
- Email clients: 1.8 times higher.

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

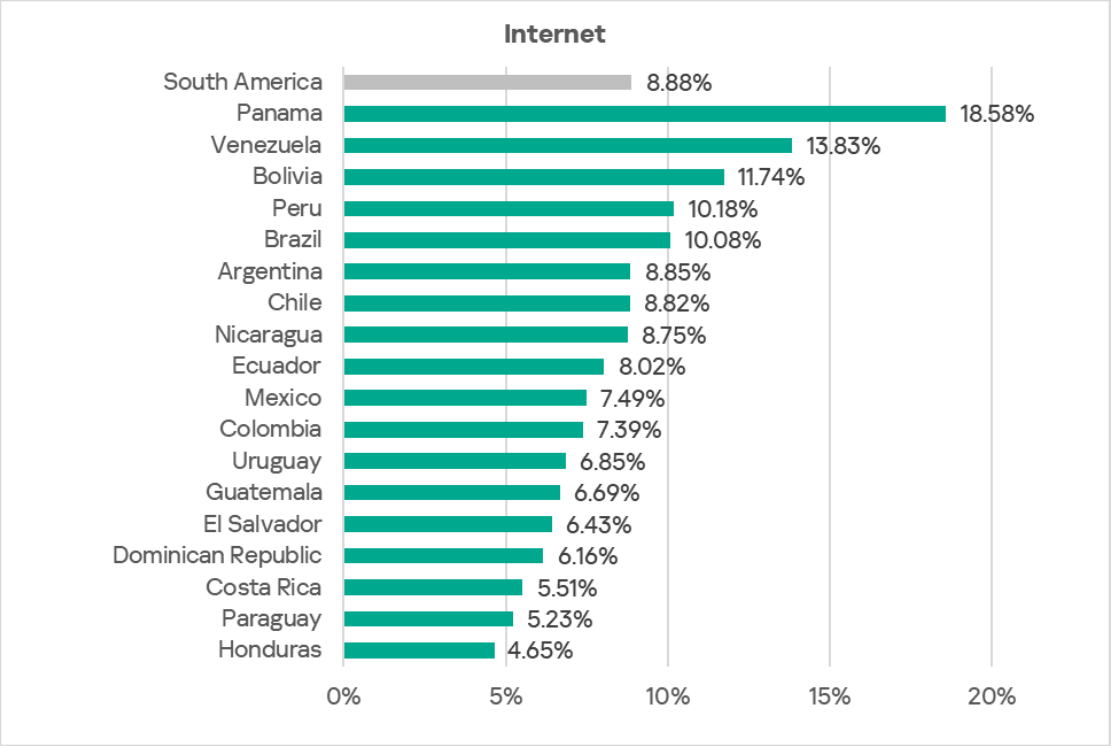


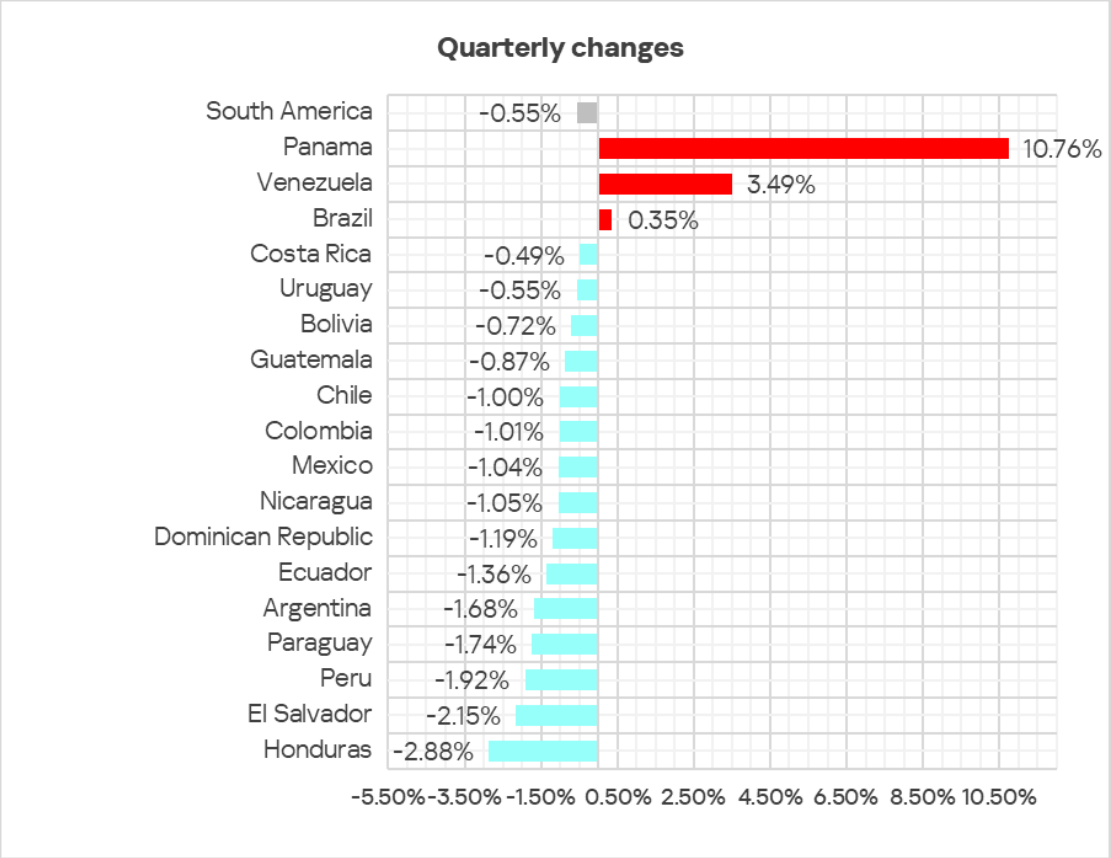
Internet

In Q3 2025, despite the reduced indicator, South America rose from sixth place to fourth place among the regional rankings for ICS computers where threats from the internet were blocked.

The region's figure is 8.88%, 1.9 times higher than in Northern Europe, which ranks last.

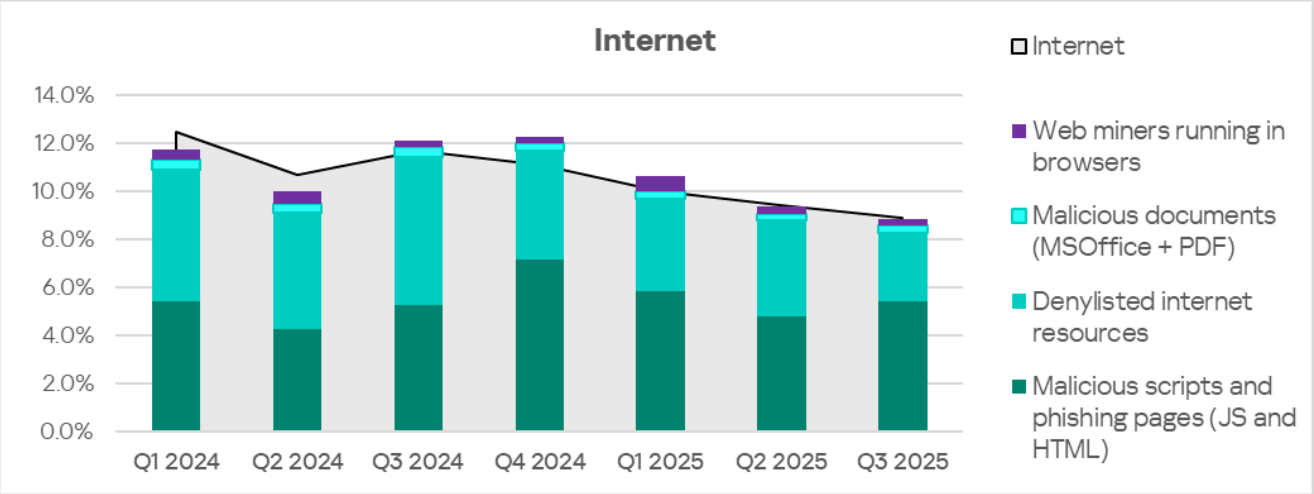
The indicators for countries in the region range from 4.65% in Honduras to 18.58% in Panama.





This indicator decreased in almost all countries of the region. However, in Panama it grew by a factor of 2.4. This substantial growth was caused by a burst of blocked threats from the malicious scripts and phishing pages category during attempts to access infected websites. This burst was caused by a mass infection of WordPress websites in the country, including in government institutions.

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

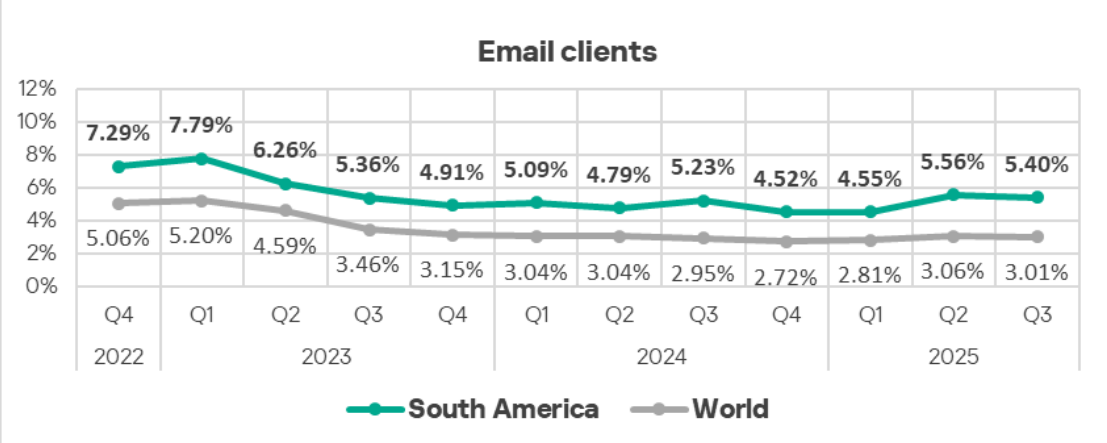


Email clients

Based on the percentage of ICS computers on which threats from email clients were blocked, South America ranked third among regions in Q3 2025, behind only Southern Europe and the Middle East. This indicator for South America (5.40%) is 6.9 times higher than in Russia, which ranks last.

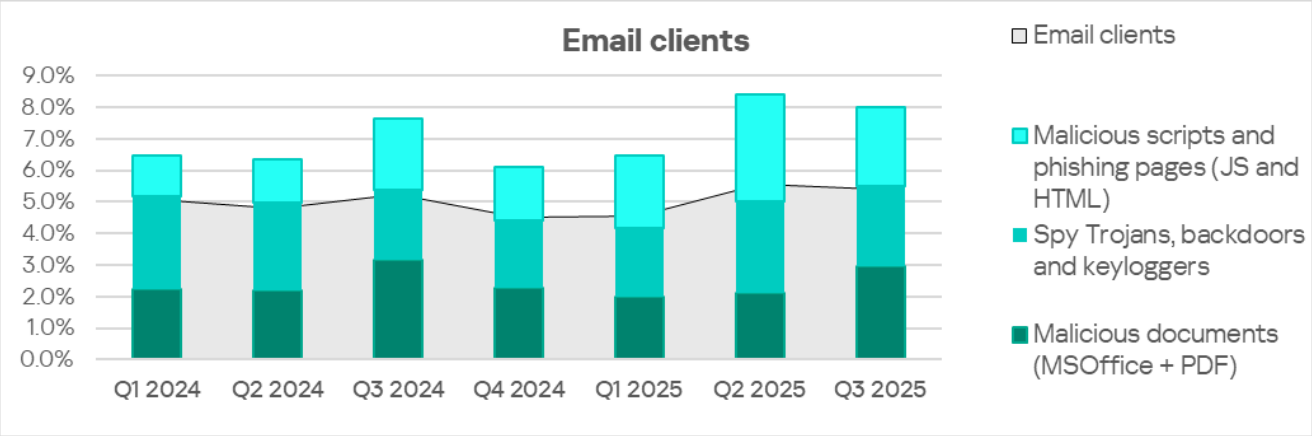
This high rate of threats from email clients combined with the high rate of malicious scripts and phishing pages indicates that OT systems in the region are highly exposed to targeted attacks.

The dynamics of the email clients indicator in the region match the average global dynamics.



Among countries in the region, Mexico (9.4%) and Uruguay (11.0%) lead by a wide margin. Elsewhere, rates range from 2.10% in Venezuela to 6.43% in Argentina.

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

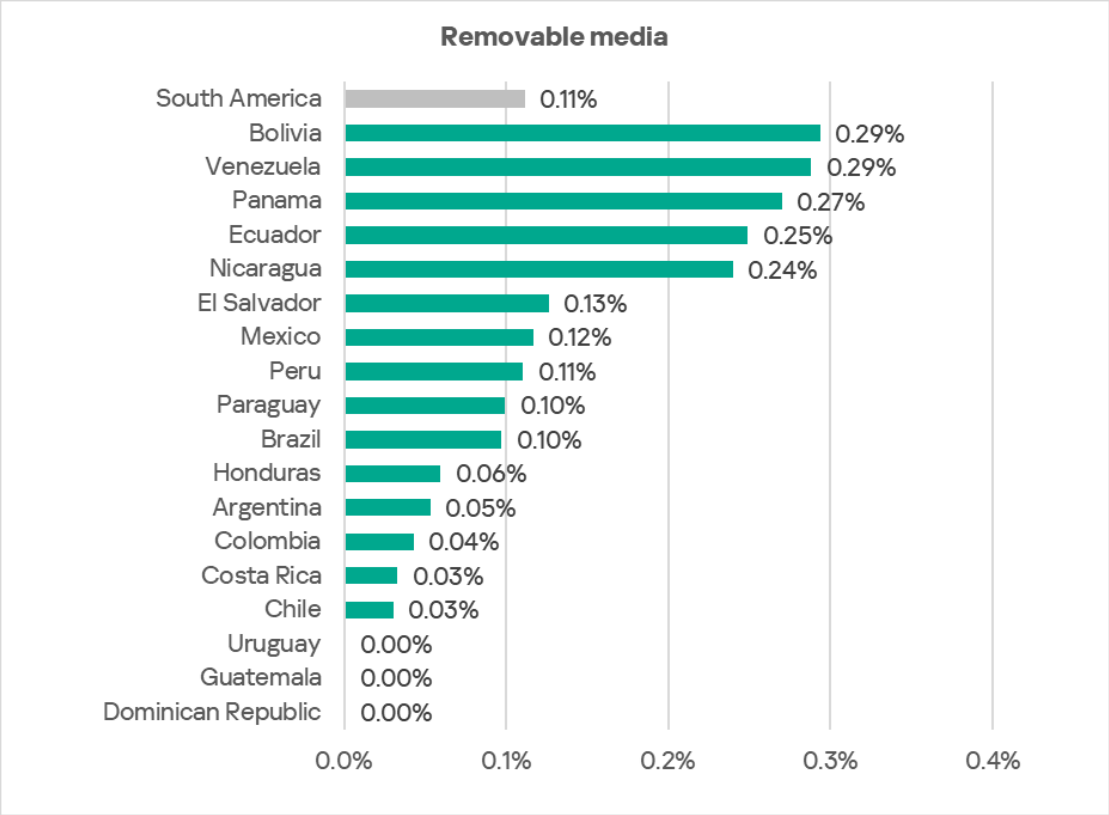


The top three countries for email client threats — Uruguay, Mexico, and Argentina — also rank high in spyware. Uruguay and Mexico also lead the rankings for malicious documents.

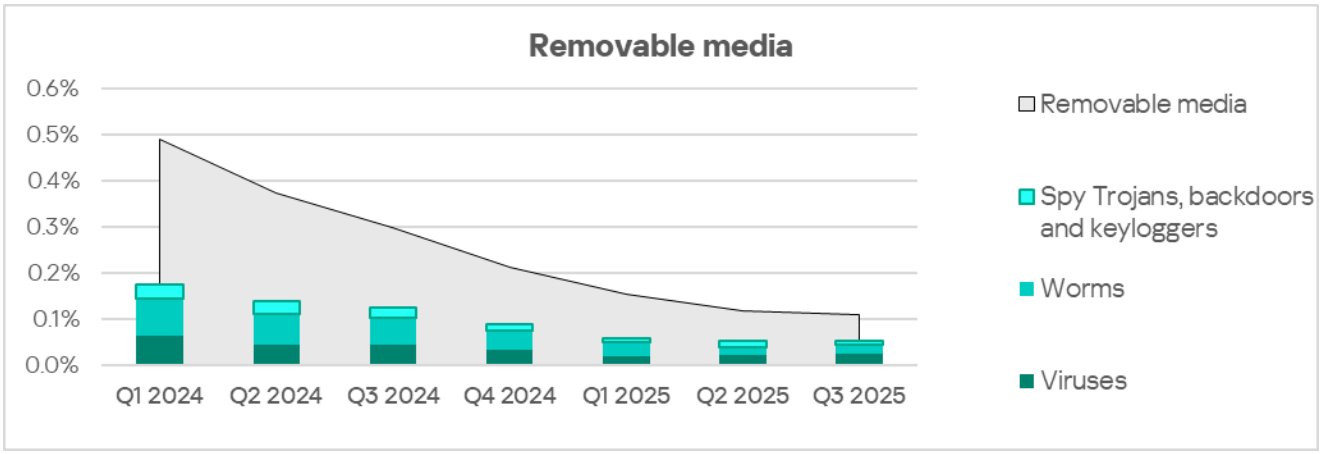
Removable media

Based on the percentage of ICS computers on which threats were blocked when connecting removable media, South America ranked ninth among regions in Q3 2025 with its rate of 0.11%. This figure is 2.2 times higher than in the Australia and New Zealand region, which ranks last for this indicator.

Among countries in the region, Bolivia and Venezuela lead in the percentage of ICS computers on which removable media threats were blocked on connection at a rate of 0.29%.



The main categories of threats blocked when connecting removable devices to ICS computers are viruses, worms, and spyware.

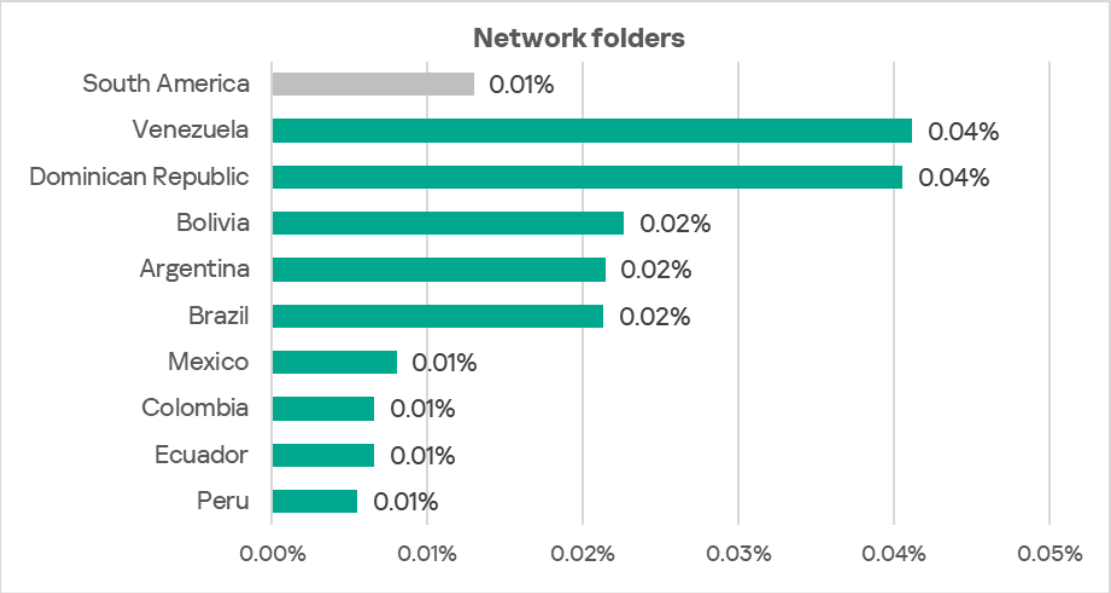


Network folders

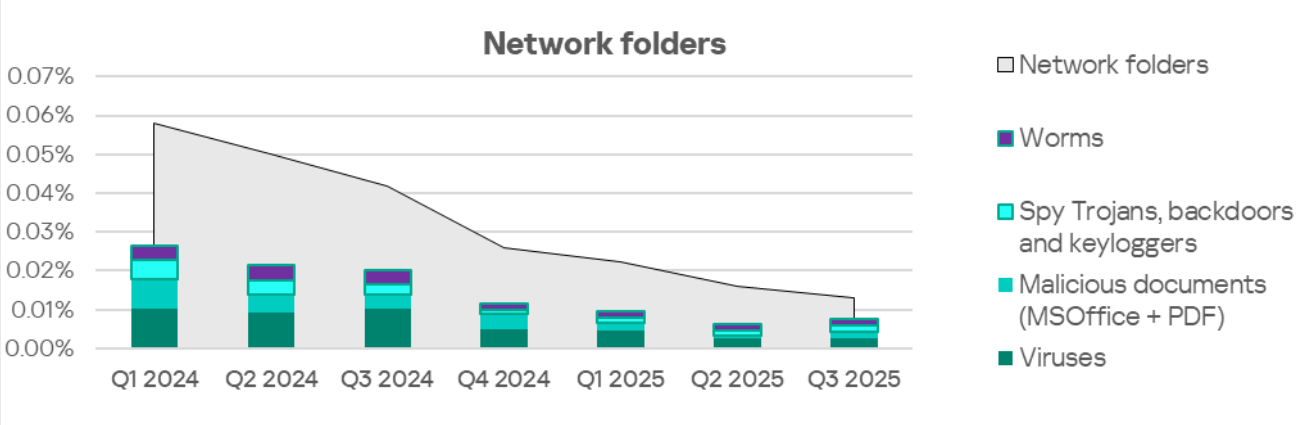
South America ranks 12th among regions based on the percentage of ICS computers on which threats were blocked in network folders with a rate of

0.013%. This is 2.2 times higher than Northern Europe, which had the lowest figure.

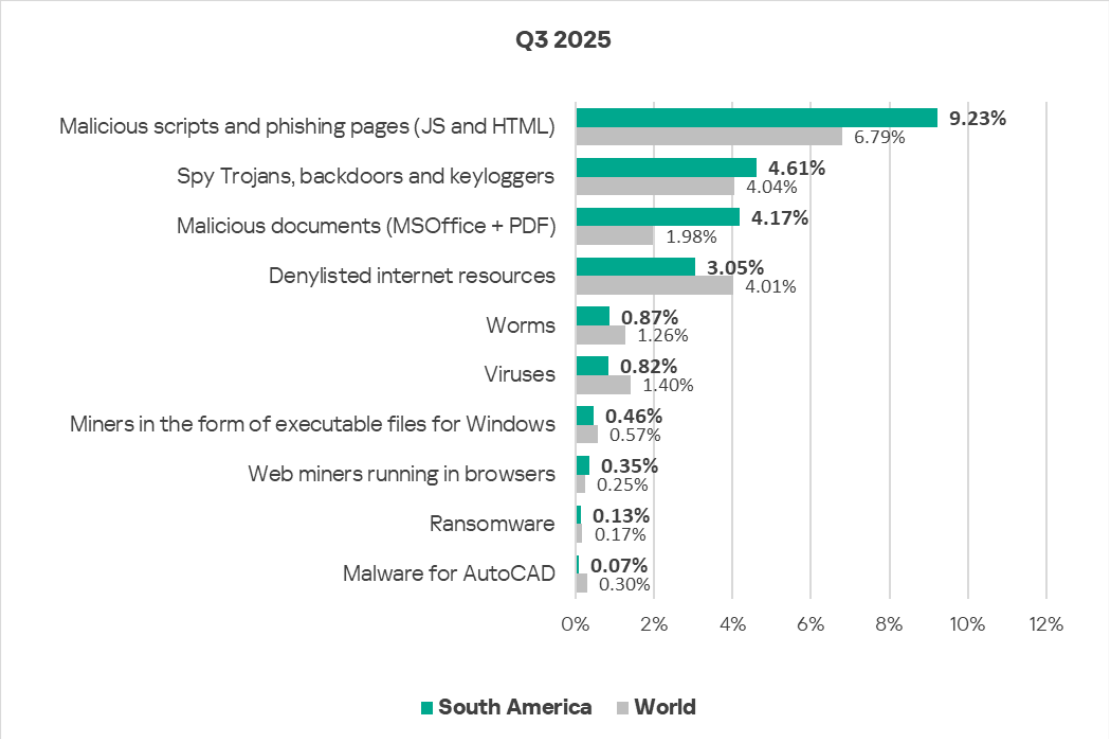
Based on the percentage of ICS computers on which threats in network folders were blocked, Venezuela and the Dominican Republic lead among countries in the region with their rate of 0.04%.

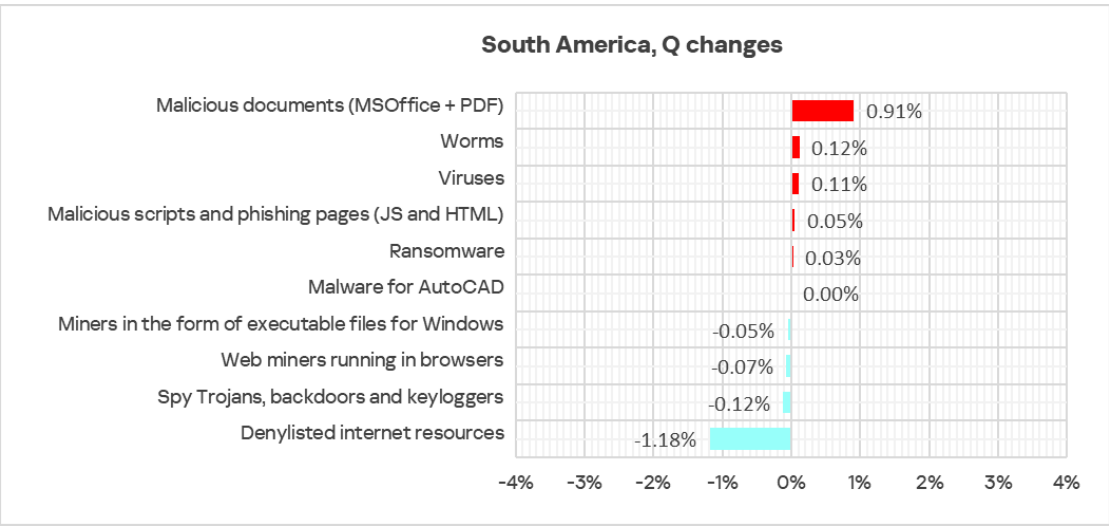


The main categories of threats spreading through network folders in the region are viruses, worms, malicious documents, and spyware.



Threat categories





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

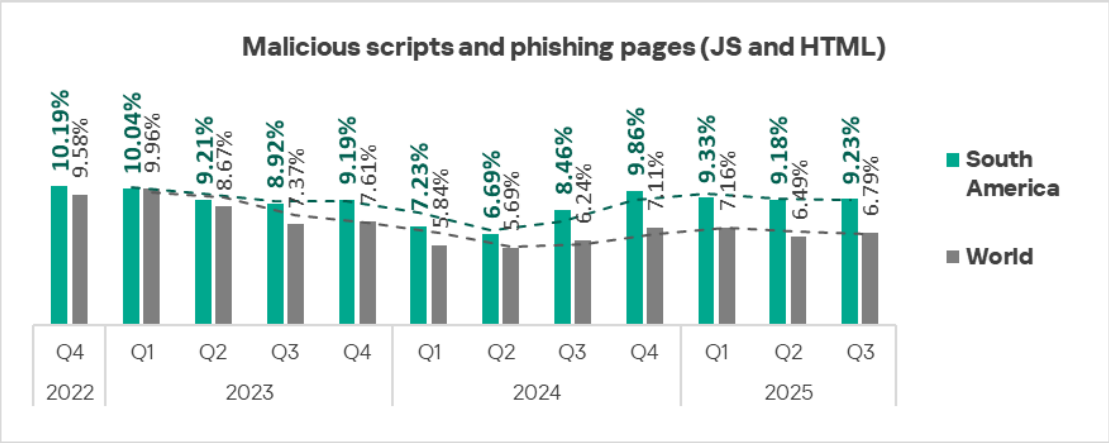
- Malicious documents: 2.1 times higher (first place among regions in the percentage of ICS computers on which the threat was blocked, and first place in the growth of this indicator over the quarter).
- Malicious scripts and phishing pages: 1.4 times higher (third place among regions).
- Web miners: 1.4 times higher (first place among regions).

- Spyware: 1.1 times higher.

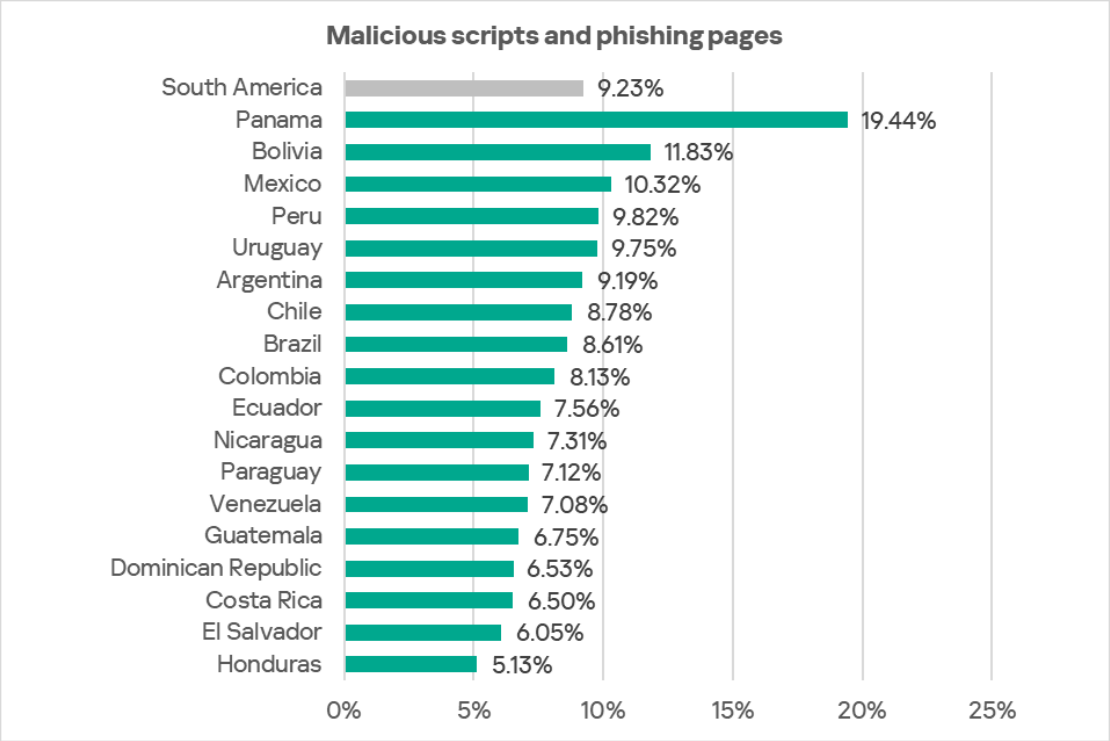
Malicious scripts and phishing pages

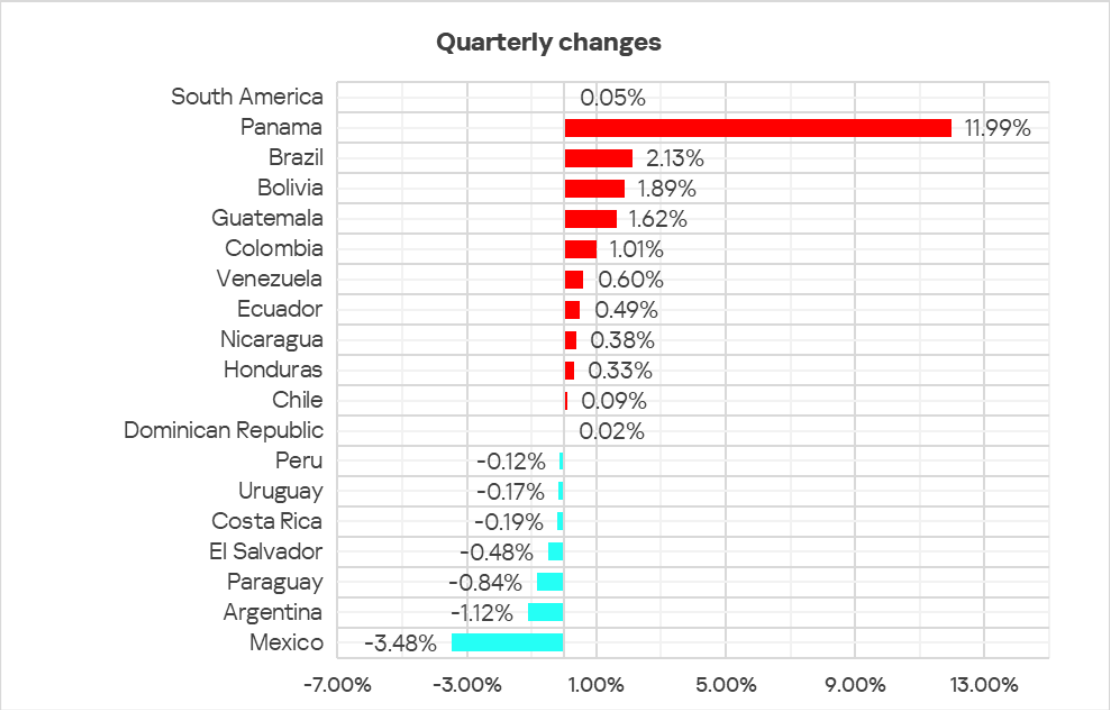
Based on the percentage of ICS computers on which malicious scripts and phishing pages were blocked, South America ranks third in the corresponding ranking among regions with 9.23%. This figure is 3.6 times higher than in Northern Europe, which boasts the lowest percentage among all regions.

The indicator in the region slightly increased over the quarter.



Among countries in the region, Panama leads in this metric with 19.44%. In this country, the indicator grew by a substantial 11.99 p.p. As a result, Panama jumped ahead to lead in not only the malicious scripts and phishing pages indicator but also in internet threats.

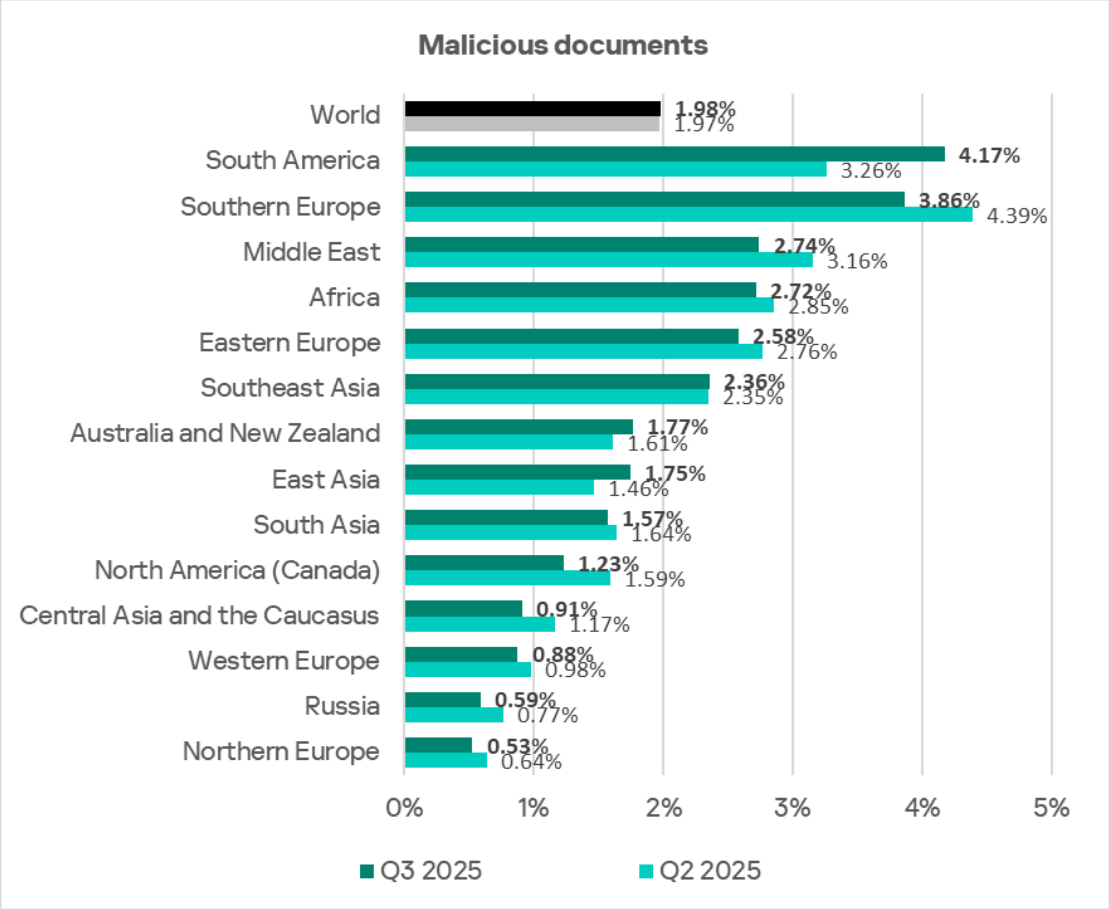




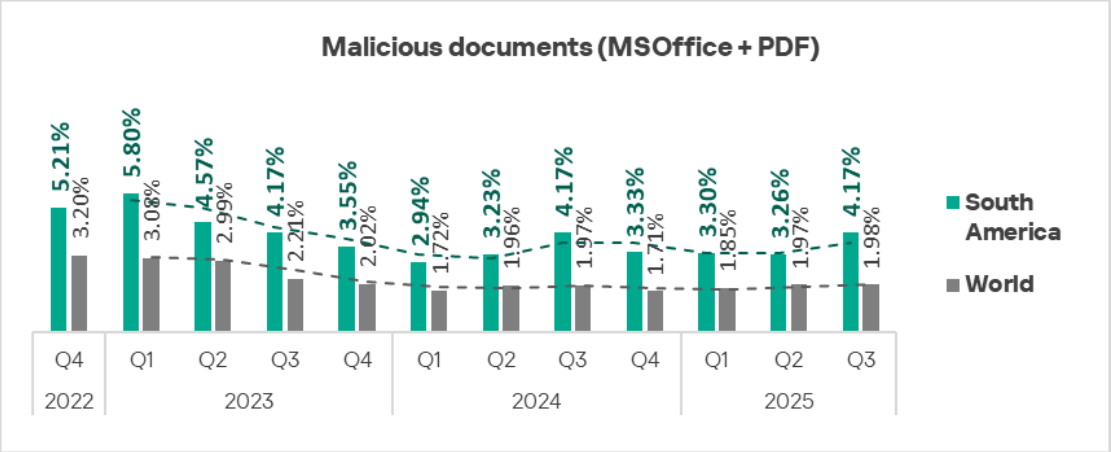
Malicious scripts and phishing pages spread both via the internet and through email. The sharp growth in the percentage of ICS computers on which malicious scripts and phishing pages were blocked in Panama is linked to the infection of popular websites on the WordPress engine, particularly websites of government organizations.

Malicious documents

South America ranks first among regions based on the percentage of ICS computers on which malicious documents were blocked.



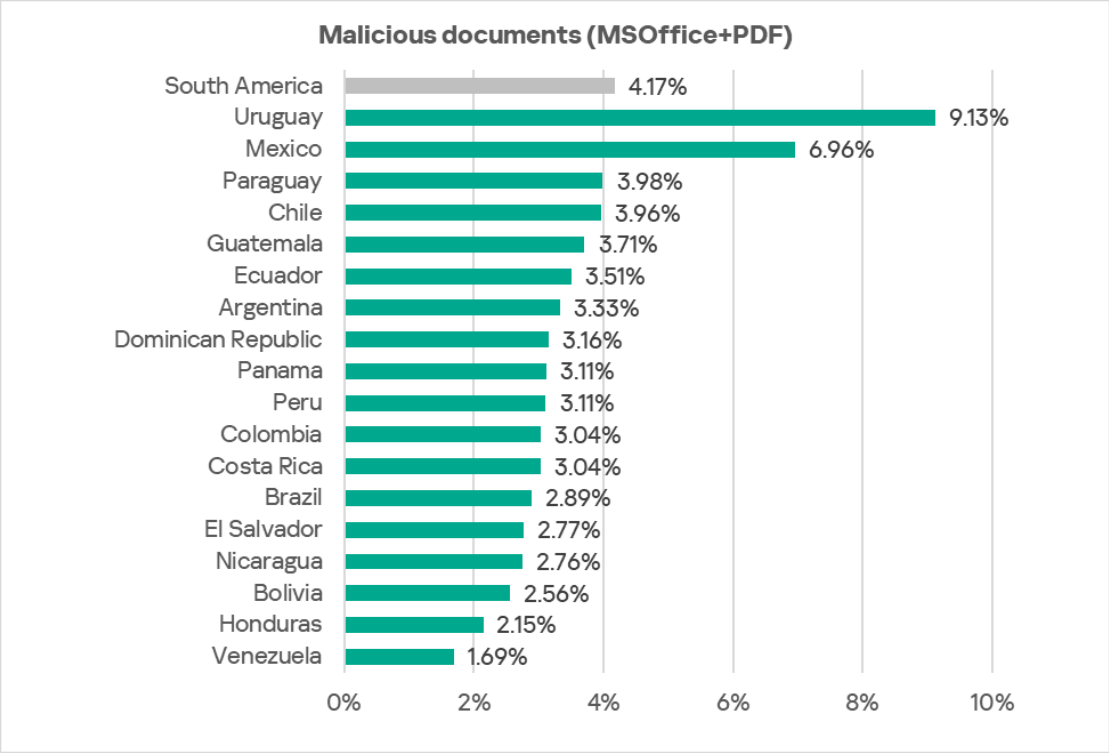
In Q3 2025 in South America, the percentage of ICS computers on which malicious documents were blocked rose to 4.17%. This is 7.9 times higher than in Northern Europe, which ranks last in this category. Based on the growth of this indicator, South America leads among regions.



The growth of the malicious documents indicator in the region was linked to a large-scale phishing campaign in which the threat actors used new exploits for the old vulnerability CVE-2017-11882 in Microsoft Office Equation Editor to deliver various spyware to victims' computers.

Notably, the threat actors in this phishing spree used localized texts for messages in Spanish, and the contents of the text compared to standard phishing text was more similar to business letters.

Among the region's countries, Uruguay and Mexico lead by a wide margin with 9.13% and 6.96%, respectively, based on the percentage of ICS computers on which malicious documents were blocked. Over the quarter, this indicator rose in all countries except Venezuela and Honduras, which are ranked last.

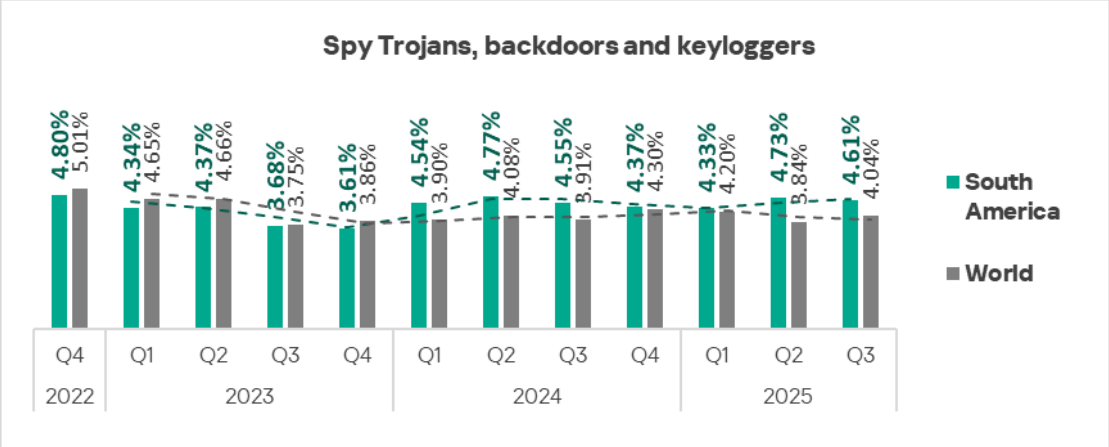


Malicious documents are spread primarily via email. Uruguay and Mexico also top the regional ranking for ICS computers where mail client threats were blocked.

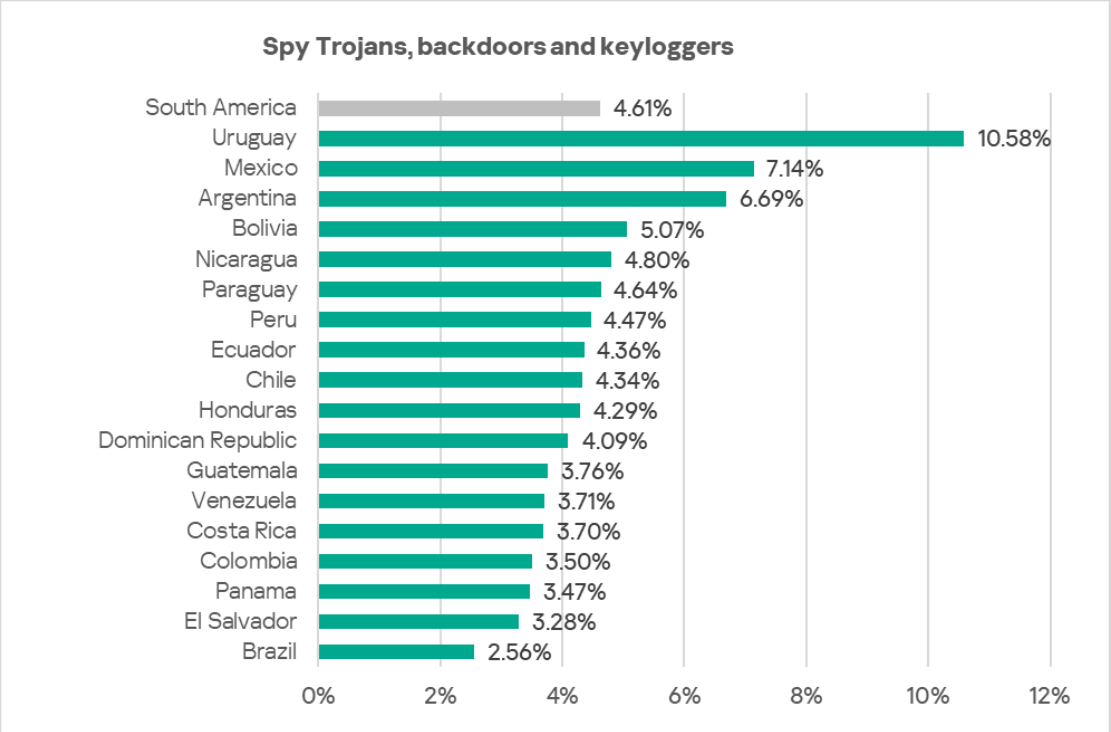
Spyware

By the percentage of ICS computers on which spyware was blocked, South America ranks fifth globally with 4.61%. This figure is 3.3 times higher than in Northern Europe, which has the lowest rate.

The percentage of ICS computers on which spyware was blocked in South America fluctuates, and this indicator decreased in Q3 2025.



Among the region's countries, Uruguay leads by a wide margin with 10.58% as its percentage of ICS computers on which spyware was blocked. Brazil has the lowest rate (2.56%).

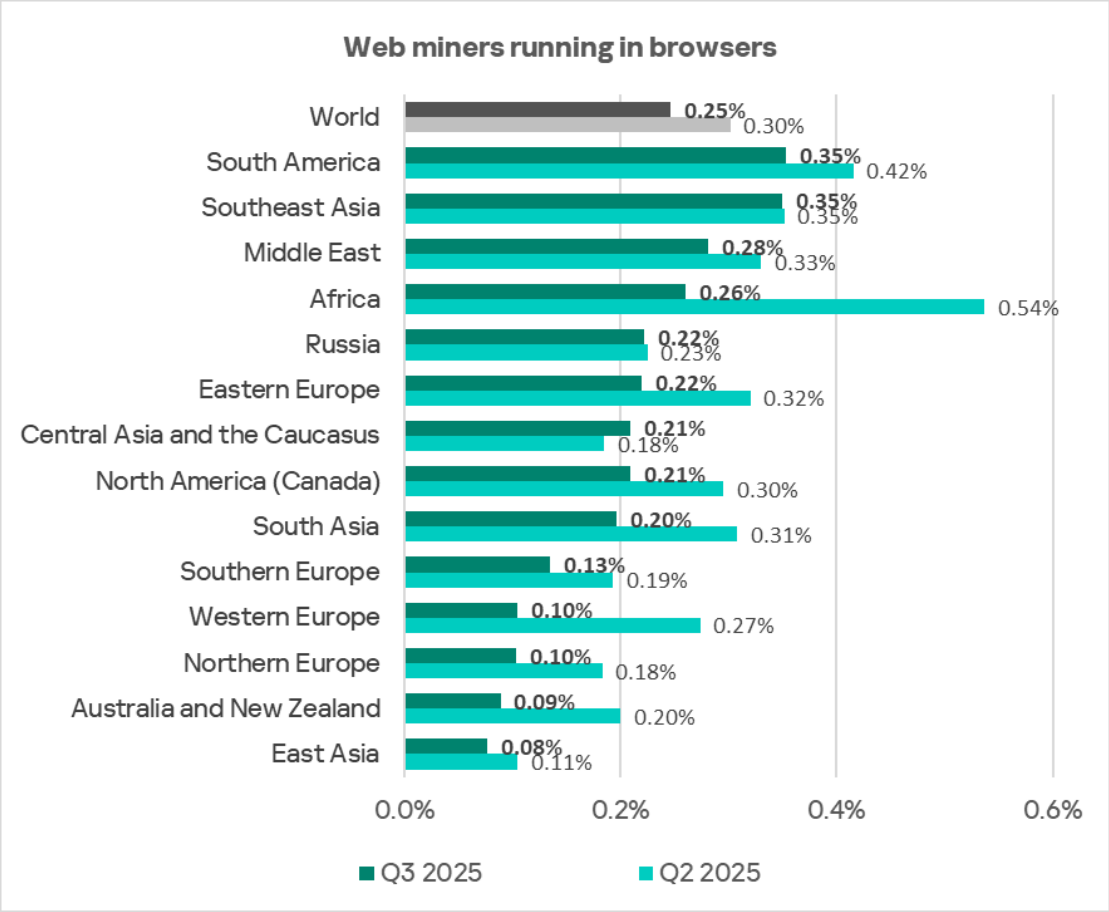


Spyware is blocked across all threat sources in Latin America but is most common in email clients.

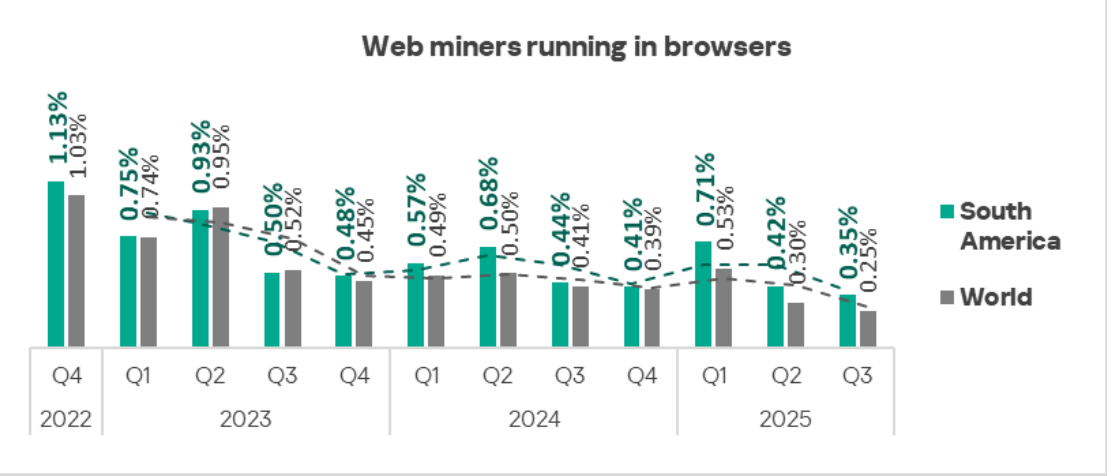
The top three countries for spyware also rank among the region's leaders for mail client threats.

Web miners

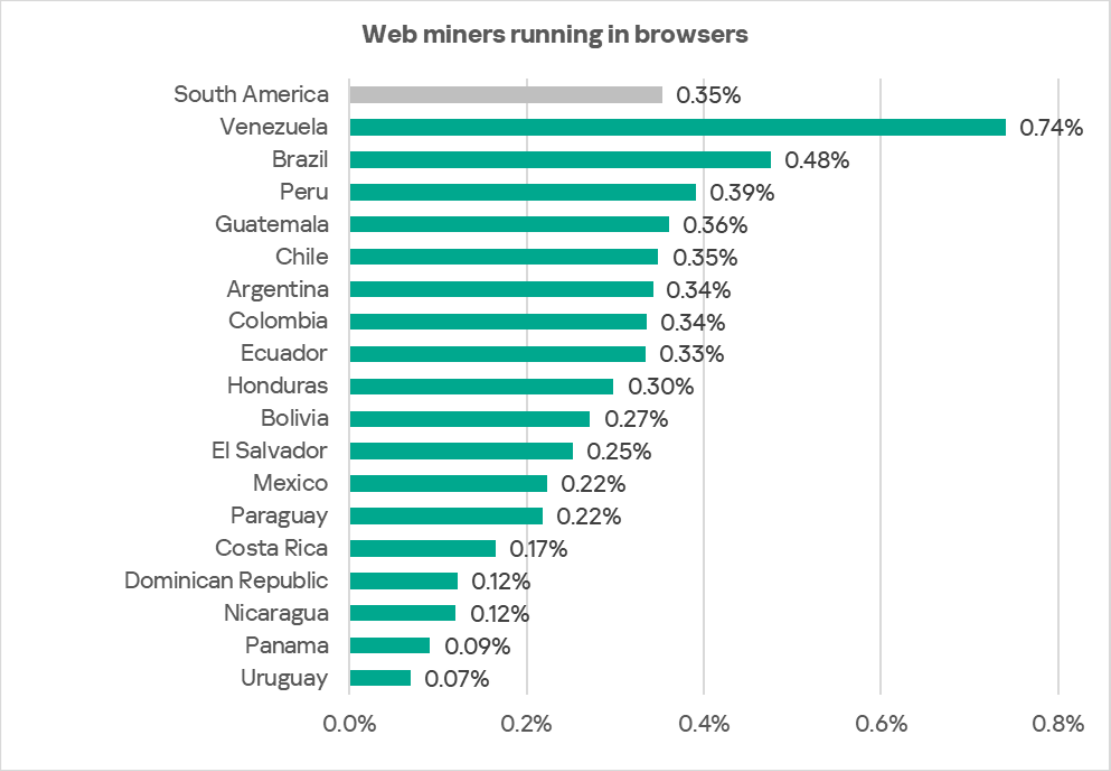
Based on the percentage of ICS computers on which web miners were blocked in Q3 2025, South America is the leader among regions.



Despite its first place in the ranking, the web miners indicator in the region in Q3 2025 was the lowest over the course of three years at 0.35%. This is 4.4 times higher than in East Asia, which ranks last.



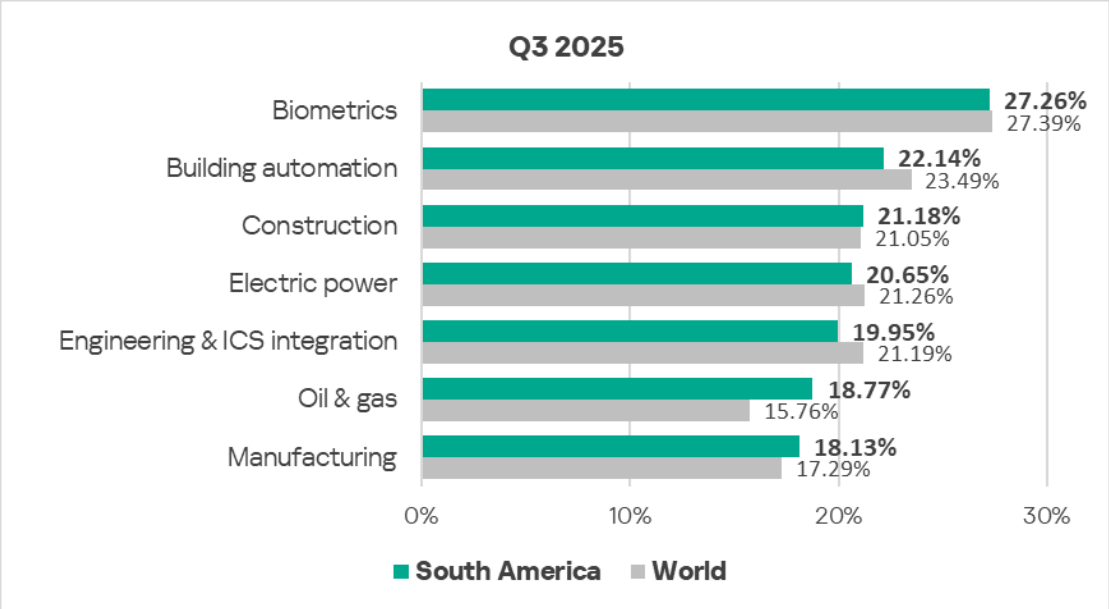
Among countries in the region, Venezuela leads at 0.74% in the percentage of ICS computers on which web miners were blocked. This is the region's only country in which the indicator grew.



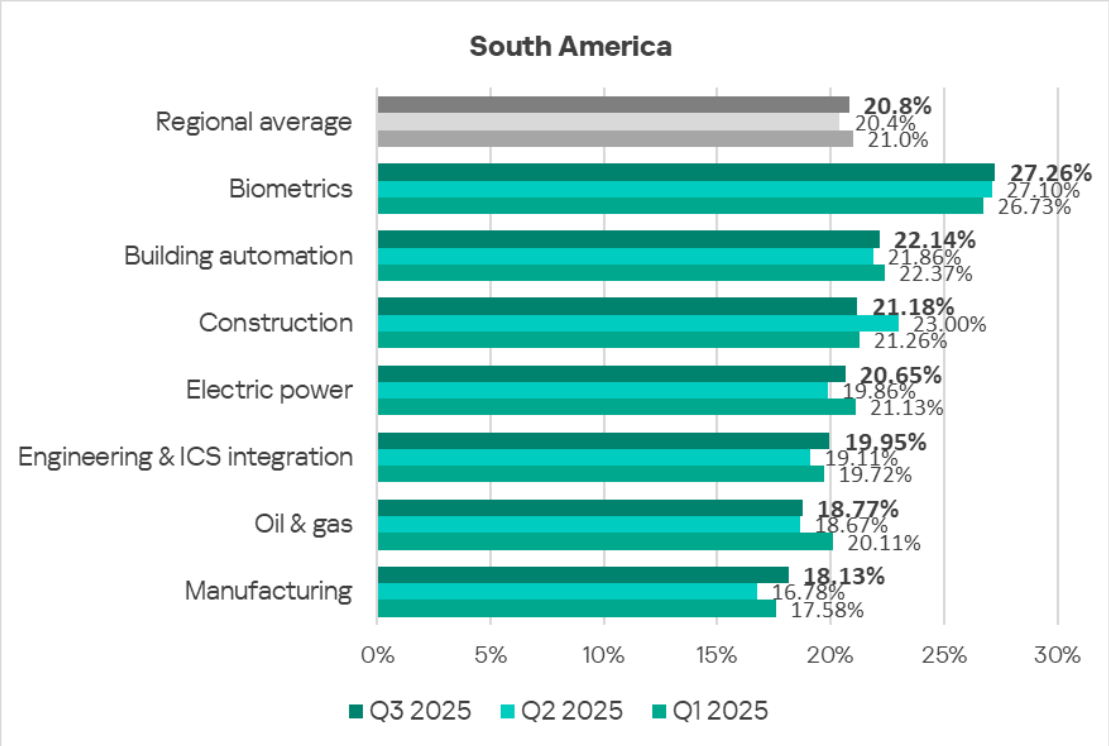
Industries

In South America, of all the industries covered in the report, malicious objects are most often blocked in biometric systems.

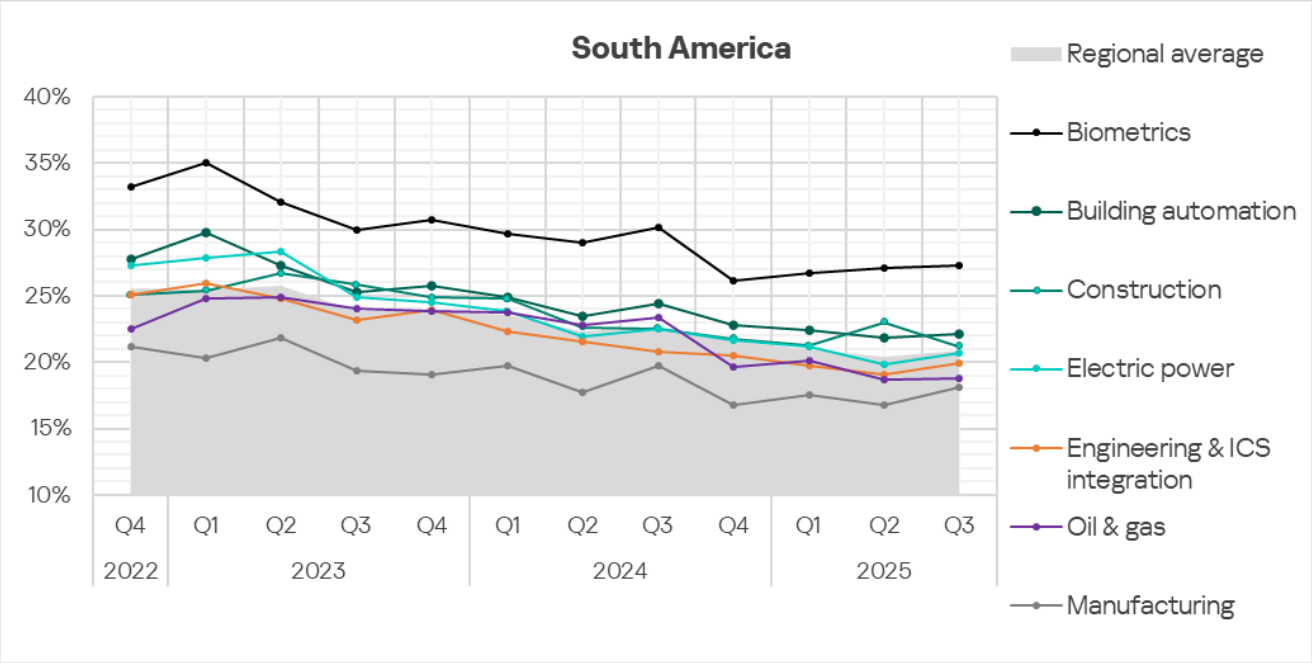
The percentage of ICS computers on which malicious objects were blocked exceeds the global average in three industries: construction, oil and gas, and manufacturing. This difference is most prevalent in the oil and gas industry indicators, which is 1.2 times higher in the region than in the rest of the world.



In Q3 2025, the percentage of ICS computers on which malicious objects were blocked increased in all industries except construction.



Despite fluctuations, the sectors under review show a predominately positive (downward) long-term trend since Q3 2023.



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 America, Q3 2025

Industry / Threat source	Biometrics	Building automation	Electric power	Engineering & ICS integration	Oil & gas	Construction	Manufacturing	Threat category total in the region
Internet	8.44%	8.26%	10.83%	9.37%	8.23%	11.21%	8.04%	8.88%
Email clients	11.51%	7.65%	2.85%	3.19%	3.40%	3.29%	2.45%	5.40%
Removable media	0.10%	0.10%	0.25%	0.10%	0.44%	0.15%	0.14%	0.11%
Network folders	0.02%	0.02%	0.00%	0.01%	0.00%	0.00%	0.00%	0.01%
Industry total in the region	27.26%	22.14%	20.65%	19.95%	18.77%	21.18%	18.13%	

Threat category indicators for industries in South America, 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	2.81%	2.79%	3.84%	3.26%	3.51%	4.07%	3.08%	3.05%
Malicious scripts and phishing pages (JS and HTML)	12.28%	9.99%	9.43%	8.31%	6.37%	9.02%	8.26%	9.23%
Spy Trojans, backdoors and keyloggers	9.13%	6.14%	3.11%	3.02%	3.07%	3.33%	3.79%	4.61%
Worms	1.25%	1.04%	1.08%	0.74%	1.10%	0.74%	0.75%	0.87%
Miners in the form of executable files for Windows	0.45%	0.46%	0.47%	0.50%	0.88%	0.46%	0.38%	0.46%
Malicious documents (MSOffice + PDF)	8.27%	5.68%	2.30%	2.60%	2.31%	2.68%	2.62%	4.17%
Viruses	1.03%	0.96%	1.11%	0.69%	0.99%	1.33%	0.63%	0.82%
Ransomware	0.19%	0.14%	0.07%	0.18%	0.11%	0.04%	0.09%	0.13%
Web miners running in browsers	0.26%	0.36%	0.37%	0.38%	0.66%	0.40%	0.27%	0.35%
Malware for AutoCAD	0.04%	0.05%	0.15%	0.08%	0.33%	0.74%	0.04%	0.07%
Industry total in the region	27.26%	22.14%	20.65%	19.95%	18.77%	21.18%	18.13%	

South America ranks fourth among regions in threats from the internet. In all industries, the main source of threats is the internet. Therefore, the most relevant threat categories include denylisted links, malicious scripts, and phishing pages (spread both via the internet and by email).

South America also ranks fourth in the percentage of ICS computers on which email client threats were blocked. Threat actors use email messages to spread malicious documents, malicious scripts and phishing pages that are employed to download spyware and ransomware onto the user's system.

South America leads among regions in malicious documents, ranks third in malicious scripts, and ranks fifth in spyware.

All industries in the region show high indicators for malicious documents, malicious scripts and phishing pages, and spyware. We should note that these are clear signs of the high exposure of technological systems to advanced categories of threat actors.

South America is in the top 3 in the percentage of ICS computers on which malicious documents were blocked in all industries. The region leads in this indicator in the oil and gas industry and in the engineering and ICS integrators industry. South America ranks third in malicious documents in the electrical energy industry, and ranks second in all other industries under review.

The region is in the top 3 based on the indicators for malicious scripts and phishing pages in the electrical energy industry (first place), biometric systems (second place), engineering and ICS integrators industry and the oil and gas industry (third place).

South America ranks second among regions in spyware in OT infrastructure for biometric systems and ranks third in the oil and gas industry.

Based on the ransomware indicators in the engineering and ICS integrators industry, South America ranks fourth among regions.

Biometric systems

South America ranks third among regions based on the percentage of ICS computers on which malicious objects were blocked in OT infrastructure for biometric systems.

Biometric systems in South America have the following global ranking among all industries in all regions:

- Second place in the percentage of ICS computers on which malicious documents were blocked.
- Fourth place in the percentage of ICS computers on which malicious scripts and phishing pages were blocked.

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

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

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

- First place in threats from email clients and in network folders.
- First place among industries in the region in the following categories: malicious scripts and phishing pages, spyware, malicious documents, worms, and ransomware.
- Third place in viruses.

Building automation

South America ranks ninth among regions in the percentage of ICS computers on which malicious objects were blocked in the building automation industry.

Building automation in South America has the following global ranking among all industries in all regions:

- Fifth place in the percentage of ICS computers on which malicious documents were blocked.

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

- Fourth place in the percentage of ICS computers on which email client threats were blocked.
- Second place in the percentage of ICS computers on which malicious documents were blocked.
- Fourth place in web miners.

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 malicious scripts and phishing pages, spyware, and malicious documents.
- Third place in ransomware.

Construction

South America ranks sixth in the percentage of ICS computers on which malicious objects were blocked in the construction industry.

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

- Third place in the percentage of ICS computers on which internet threats were blocked.
- Second place in the percentage of ICS computers on which malicious documents were blocked.
- Fourth place in malicious scripts and phishing pages.

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

- First place in the percentage of ICS computers on which internet threats were blocked.
- Third place in removable media threats.
- First place in the percentage of ICS computers on which denylisted internet resources, viruses, and malware for AutoCAD were blocked.
- Third place in web miners.
- Third place for removable malicious documents.

Electrical energy industry

South America ranks sixth 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 America has the following rankings:

- Third place in the percentage of ICS computers on which internet threats and email client threats were blocked.
- First place in the percentage of ICS computers on which malicious scripts and phishing pages were blocked.
- Third place in the percentage of ICS computers on which malicious documents were blocked.
- Fourth place in web miners.

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

- Second place in the percentage of ICS computers on which internet threats and removable media threats were blocked.
- Second place in denylisted internet resources and viruses.
- Third place in malicious scripts and phishing pages, worms, miners in the form of executable files for Windows, and malware for AutoCAD.

Engineering and ICS integrators

South America ranks fifth among regions based on the percentage of ICS computers on which malicious objects in the engineering and ICS integrators industry were blocked.

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

- Fourth place in the percentage of ICS computers on which internet threats and email client threats were blocked.
- First place in the percentage of ICS computers on which malicious documents were blocked.
- Third place in web miners.
- Third place in malicious scripts and phishing pages.
- Fourth place in ransomware.

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

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

- Second place in miners in the form of executable files for Windows and ransomware.
- Third in the region in terms of web miners.

Oil and gas

South America ranks third among the five oil and gas industry regions in the percentage of ICS computers on which malicious objects were blocked in the industry.

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

- First place in the percentage of ICS computers on which threats in email clients were blocked.
- Second place in internet threats and third place in threats on removable media.
- First place in the percentage of ICS computers on which malicious documents and web miners were blocked in the industry.
- Second place in miners in the form of executable files and malware for AutoCAD.
- Third place in malicious scripts and phishing pages, spyware, and viruses.

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

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

Manufacturing

South America ranks fourth in the percentage of ICS computers on which malicious objects were blocked in the industry.

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

- Third place in the percentage of ICS computers on which internet threats were blocked.
- First place in the percentage of ICS computers on which malicious documents were blocked.
- Third place in malicious scripts and phishing pages.
- Fourth place in web miners.

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

- Third place in the percentage of ICS computers on which spyware was blocked.

North America (Canada)

Key cybersecurity issues in the region

The cybersecurity situation in North America (Canada) is among the most favorable across all regions. Based on the percentage of ICS computers on which malicious objects were blocked, North America (Canada) ranked 12th among regions in Q3 2025.

At the same time, the region was in higher positions in the relevant rankings for some threat sources and categories:

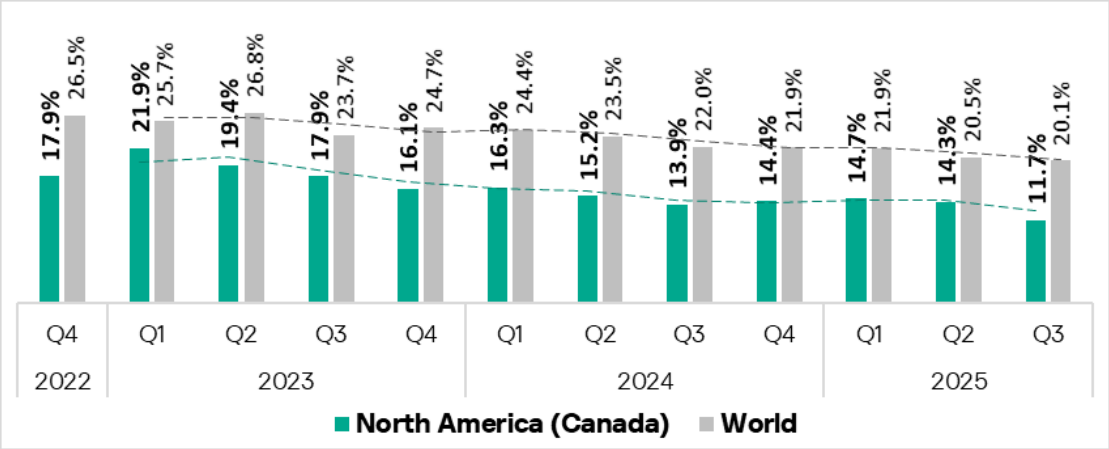
- Eighth place in web miners.
- Eighth place in email client threats.
- Tenth place in malicious scripts and phishing pages.
- Tenth place in miners in the form of Windows executable files.

It is obvious that computers on which web miners (which run in a web browser) were blocked are highly likely to have unprotected internet connections. It is also evident that the computers on which email threats were blocked have access to an unprotected email service. In North America (Canada), spam and phishing emails containing malicious scripts and miners in the form of executable files most likely infiltrated computers in an industrial network via access to a mail server in an enterprise network that was open to external mass mailings.

Relatively high percentage figures for threats distributed via email clients (phishing), malicious scripts, and both categories of miners may indicate that OT systems in the region are accessible to the more advanced categories of threat actors.

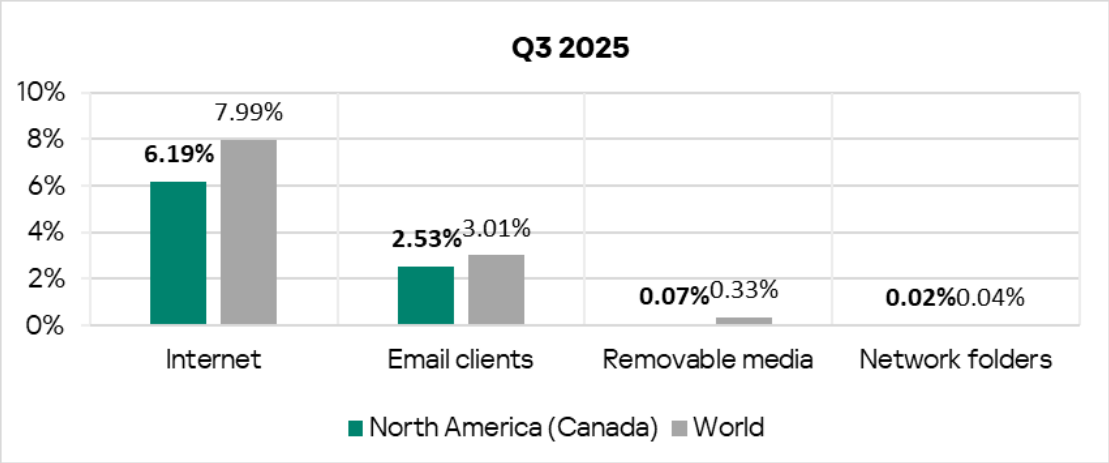
Statistics across all threats

North America (Canada) ranks 12th based on the percentage of ICS computers on which malicious objects were blocked. This figure (11.7%) is substantially lower than the global average but is 1.3 times higher than in Northen Europe, which ranks last in this category.



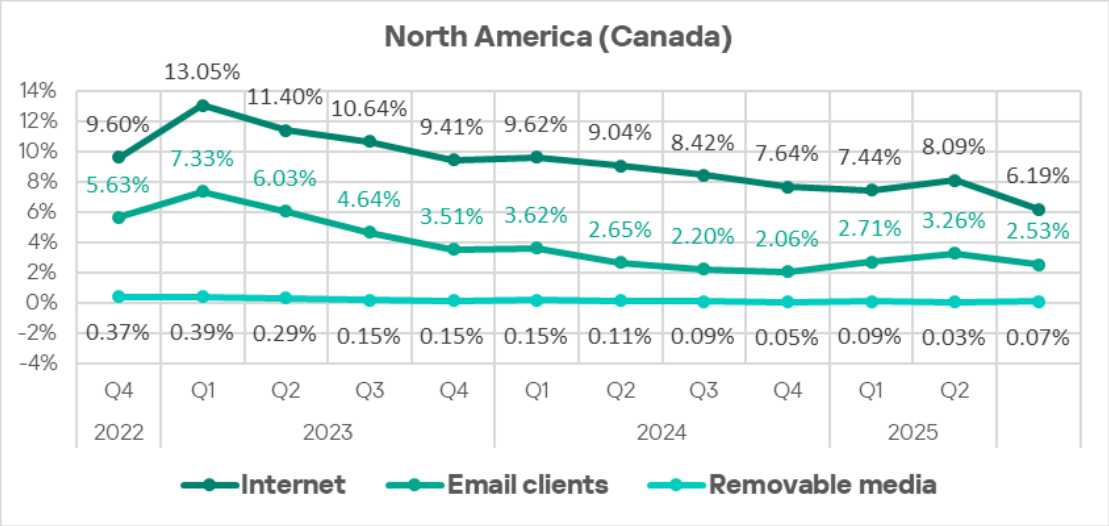
Threat sources

The indicators of all threat sources in North America (Canada) are lower than the global averages.



Malicious objects in the region spread primarily via the internet and email. North America (Canada) ranks 12th in the percentage of ICS computers on which threats were blocked when connecting removable media.

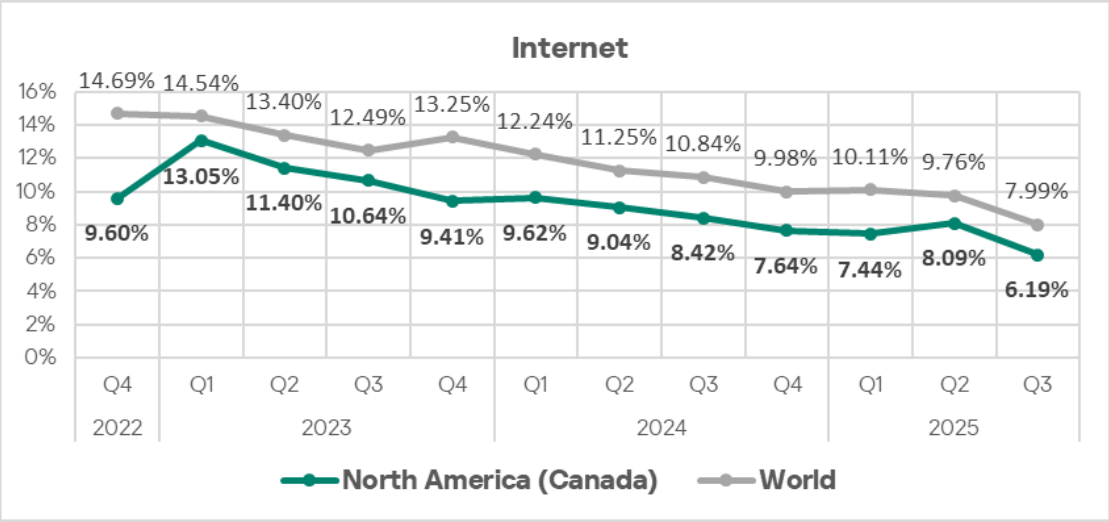
In Q3 2025, of all threat sources, only removable media showed a slight increase in the percentage of ICS computers with blocked malicious objects.



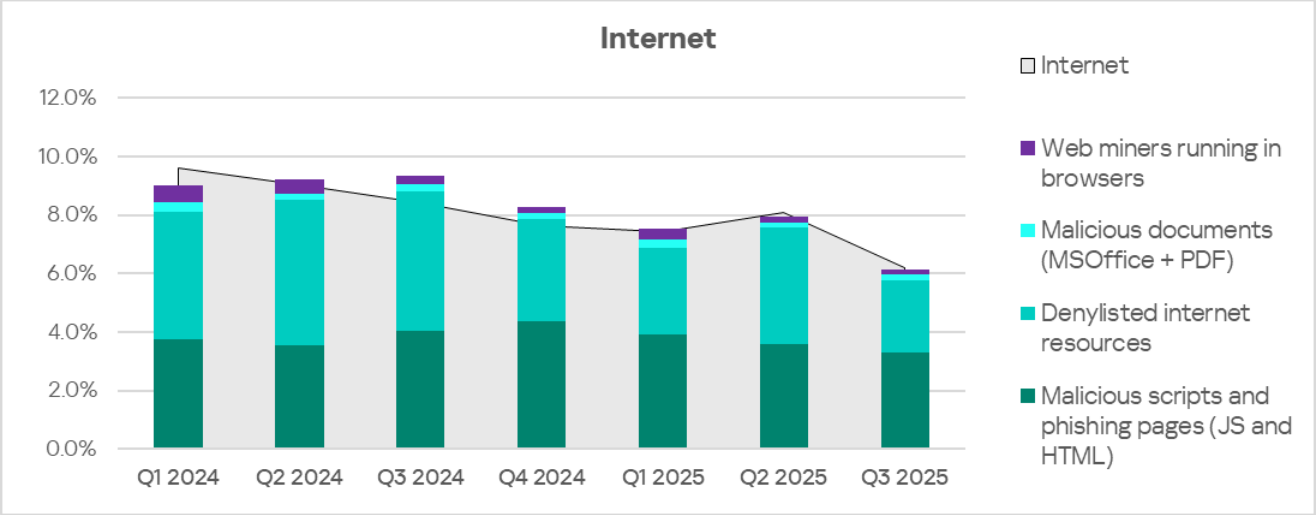
Internet

Based on the percentage of ICS computers on which internet threats were blocked, North America (Canada) ranks 11th with 6.19%. This is 1.4 times higher than the minimum figure of the regions (Northern Europe).

In Q3 2025, the percentage of internet threats in the region decreased as it did in all other regions.



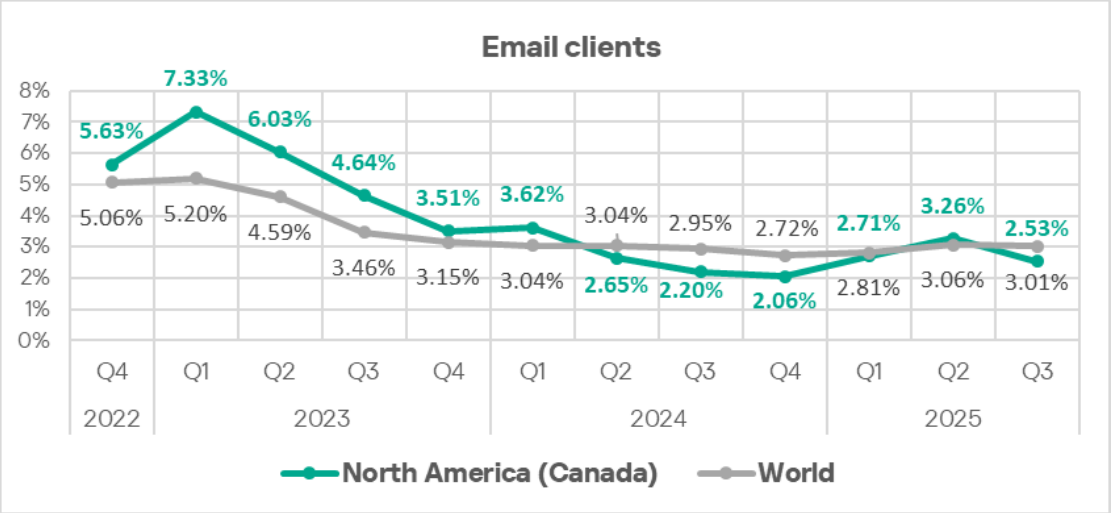
The main categories of internet threats blocked on ICS computers in the region include malicious scripts and phishing pages, as well as denylisted internet resources.



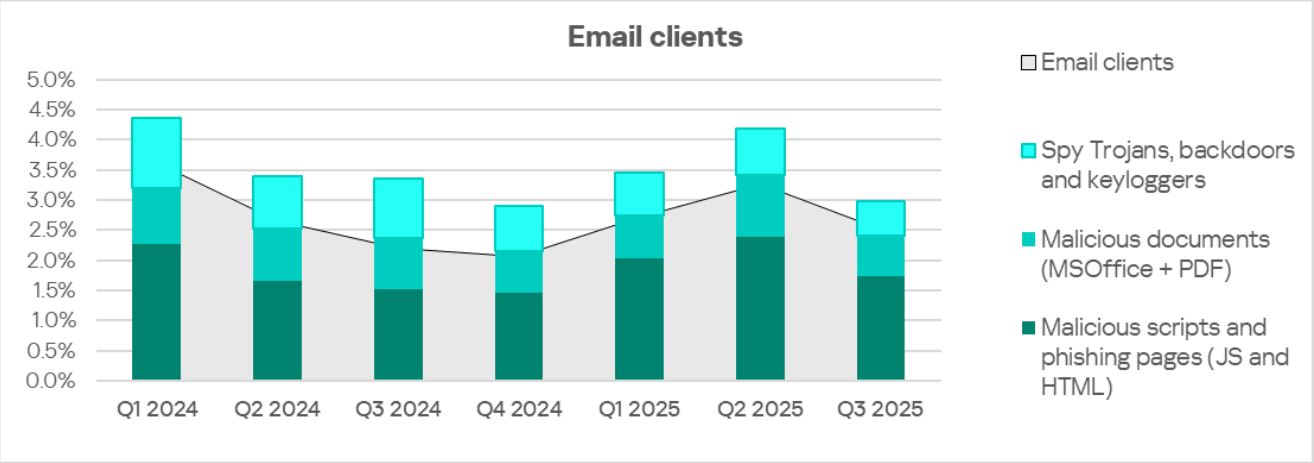
Email clients

In Q3 2025, North America (Canada) ranked eighth in the percentage of ICS computers on which threats from email clients were blocked. This is the region's highest position in the rankings, both by sources and by threat categories.

The figure in North America (Canada) is 2.53%, which is 3.2 times higher than in Russia, which ranks last.



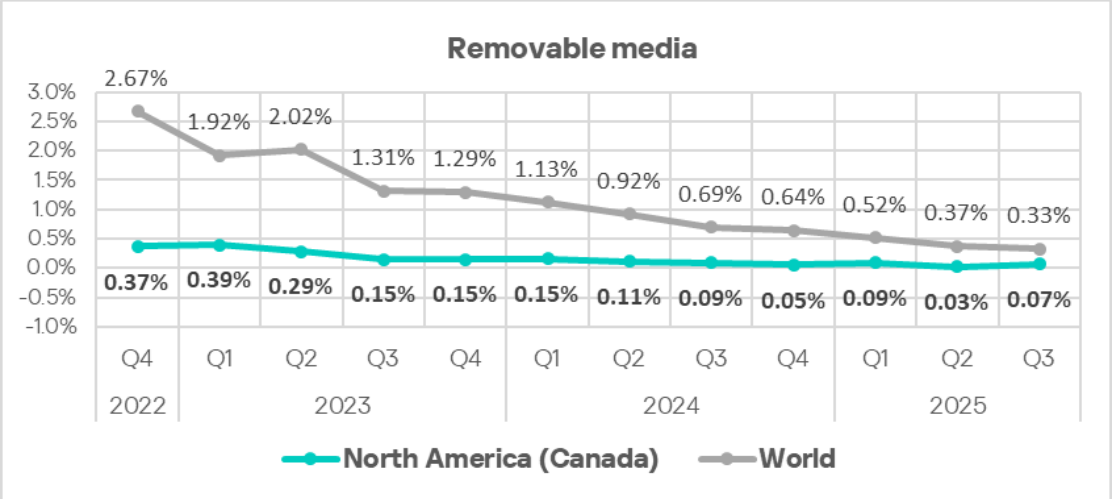
The main categories of email-borne threats blocked on ICS computers in the region are malicious scripts and phishing pages, malicious documents, and spyware.



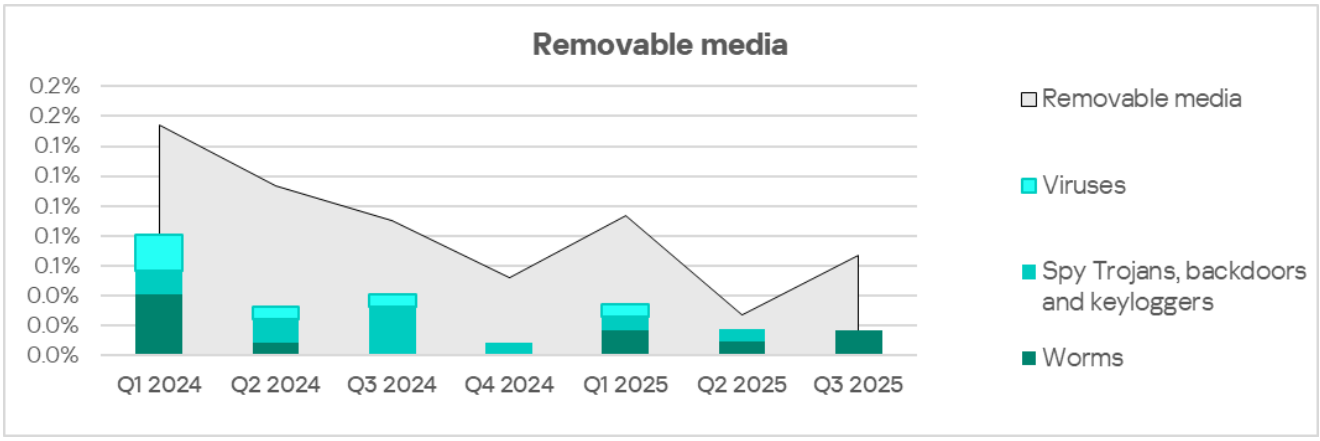
Removable media

Based on the percentage of ICS computers on which threats on removable media were blocked in Q3 2025, North America (Canada) ranked 12th with 0.07%. This figure is 1.4 times higher than in the Australia and New Zealand region, which ranks last.

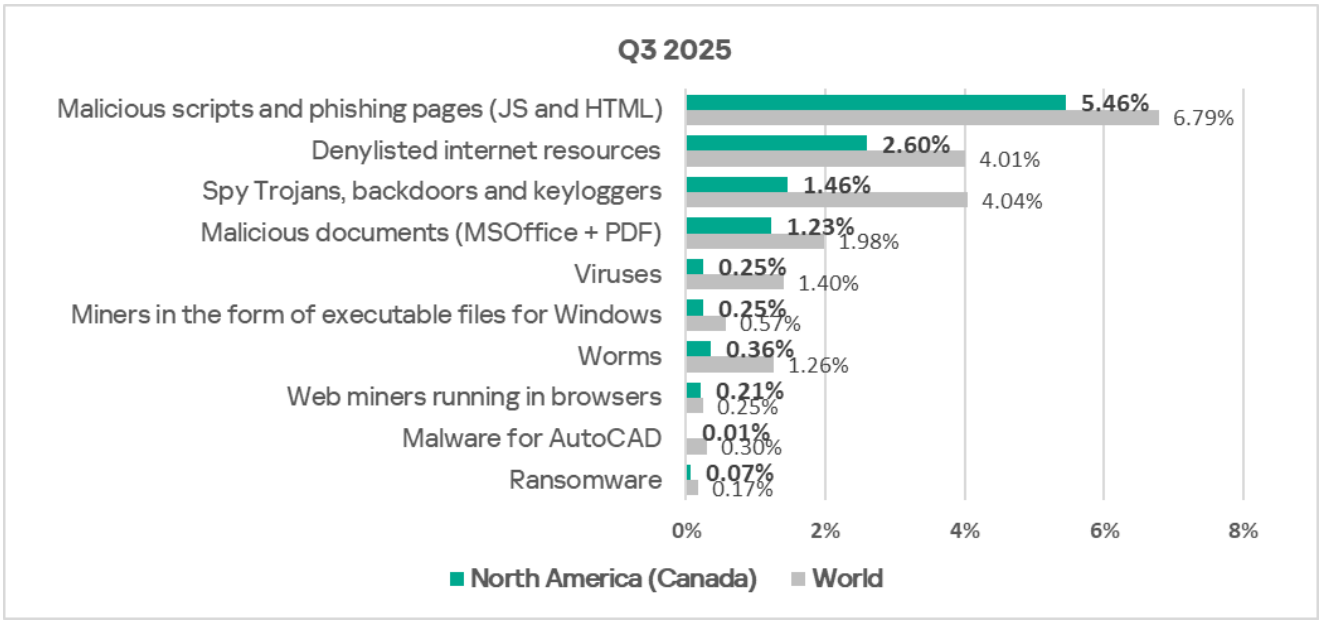
This metric fluctuates in the region. It rose in Q3 2025, and based on this growth North America (Canada) ranks first among regions.

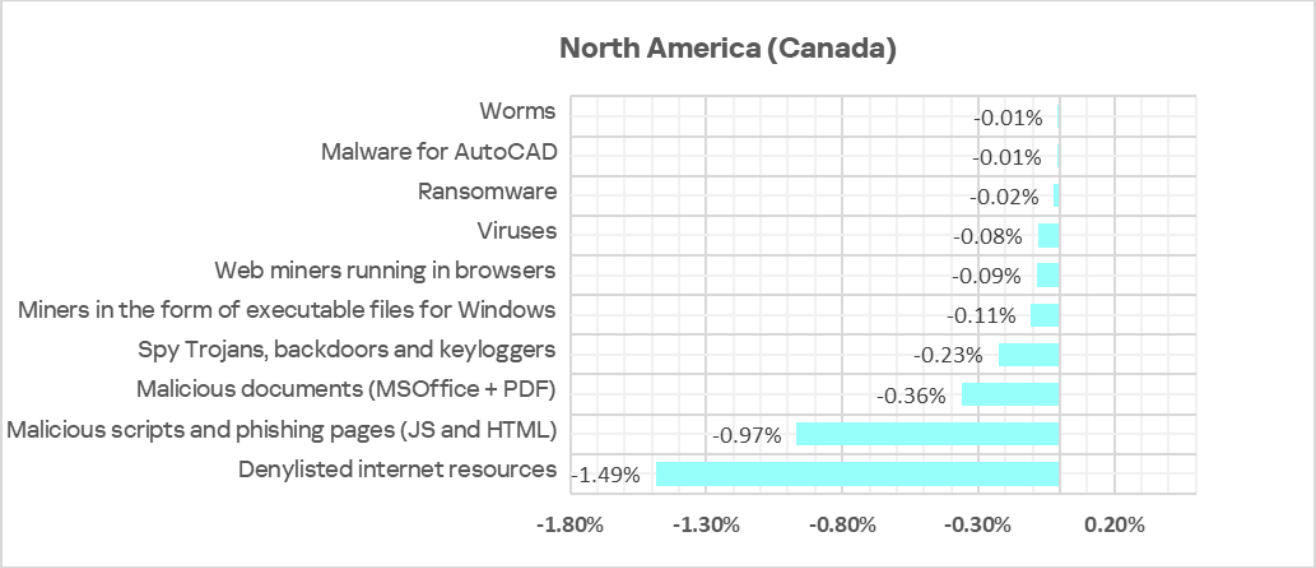


The main categories of threats that are blocked on ICS computers when connecting removable media are worms, viruses, and spyware. In Q3 2025, predominately worms were spread on removable media.



Threat categories





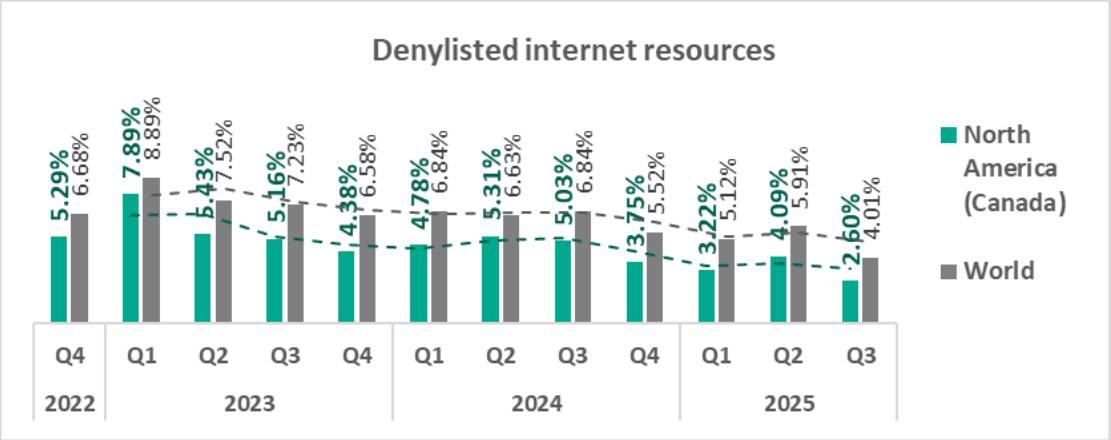
In North America (Canada), the indicators of all categories are lower than the global averages. They decreased in Q3 2025.

North America (Canada) is one of four regions in which the denylisted internet resources category did not drop below second place in the ranking.

The highest position of North America (Canada) in the regional threat-category rankings is eighth place in the percentage of ICS computers on which web miners were blocked.

Denylisted internet resources

By the percentage of ICS computers on which denylisted internet resources were blocked, North America (Canada) ranks 12th among regions, with a figure of 2.60%. During the quarter, this figure decreased to its minimum of the past three years.

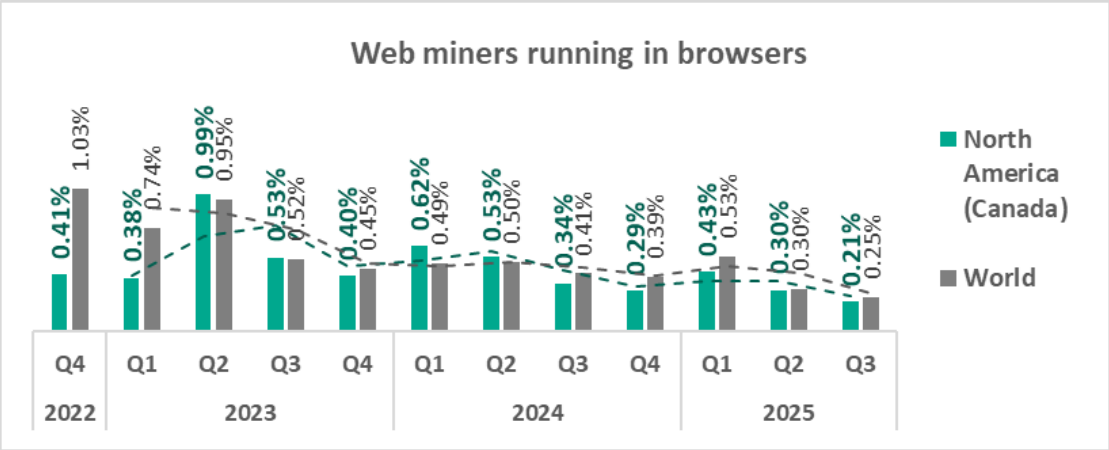


Web miners

North America (Canada) ranks eighth in the percentage of ICS computers on which web miners were blocked. This is the region's highest position in the rankings, both by threat categories and by threat sources.

The figure for web miners in the region (0.21%) is 2.6 times higher than East Asia, which ranks the lowest.

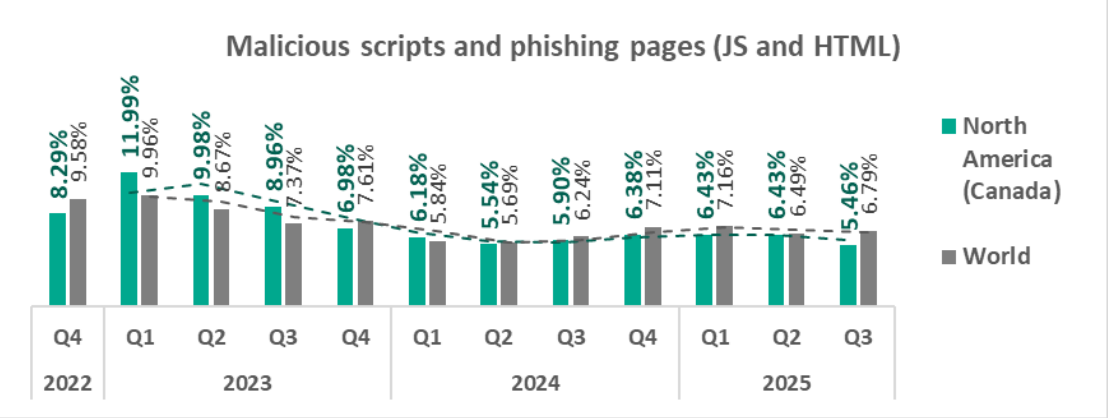
The figure in the region fluctuates, and decreased after its growth in Q1 2025.



Malicious scripts and phishing pages

Based on the percentage of ICS computers on which malicious scripts and phishing pages were blocked, North America (Canada) ranks 10th with 5.46%. This is 2.1 times higher than in Northern Europe, which boasts the lowest percentage among all regions.

In Q3 2025, the percentage of ICS computers on which malicious scripts and phishing pages were blocked decreased in the region.

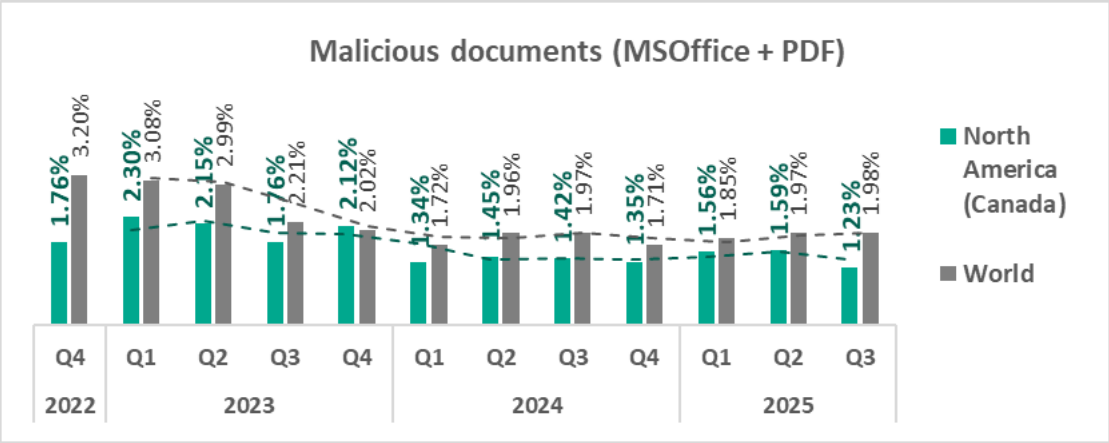


Malicious scripts and phishing pages spread both via the internet and through email.

Malicious documents

North America (Canada) ranks 10th among regions based on the percentage of ICS computers on which malicious documents were blocked. The region's figure was 1.23%, which is 2.3 times higher than in Northern Europe, the lowest-ranked region.

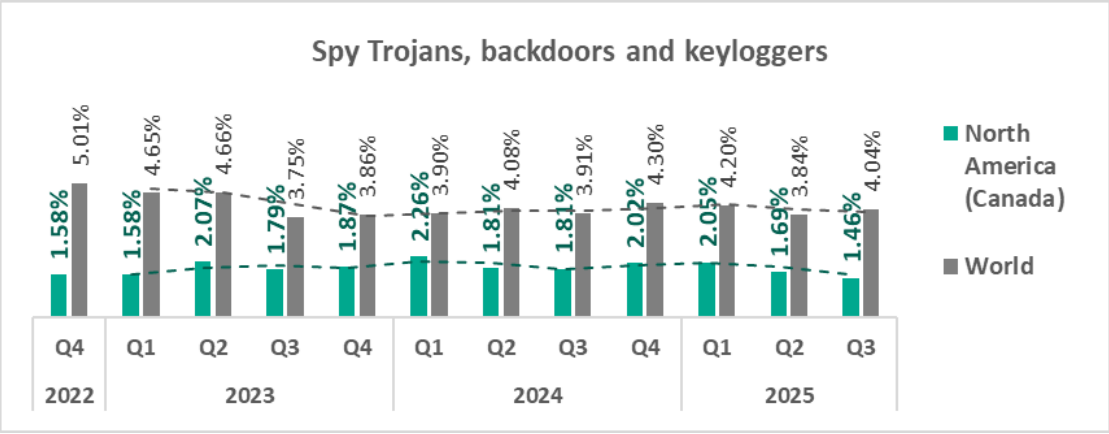
The percentage of ICS computers on which malicious documents were blocked fluctuates in the region. In Q3 2025, it decreased to its lowest figure of the past three years.



Malicious documents are distributed primarily via email.

Spyware

By the percentage of ICS computers on which spyware was blocked, North America (Canada) ranks 12th globally with 1.46%. The region's figure has declined for two consecutive quarters.

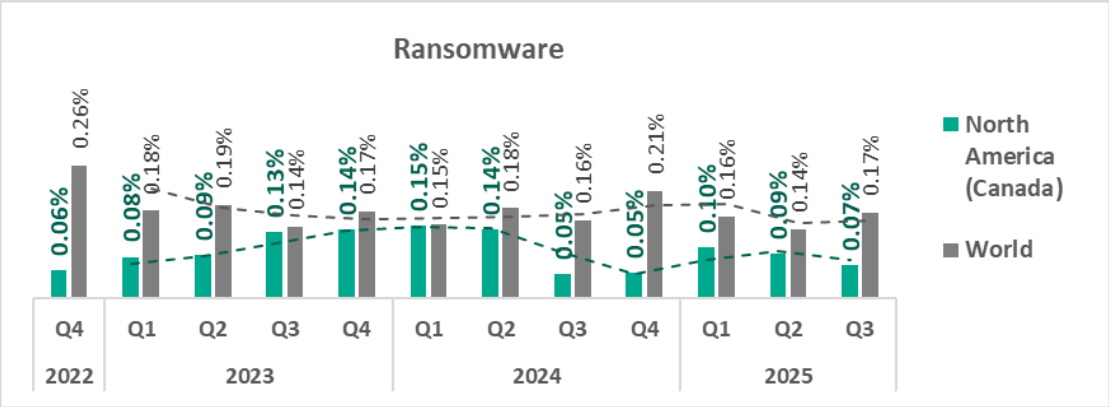


Spyware is blocked in the region across all threat sources, primarily in email clients.

Ransomware

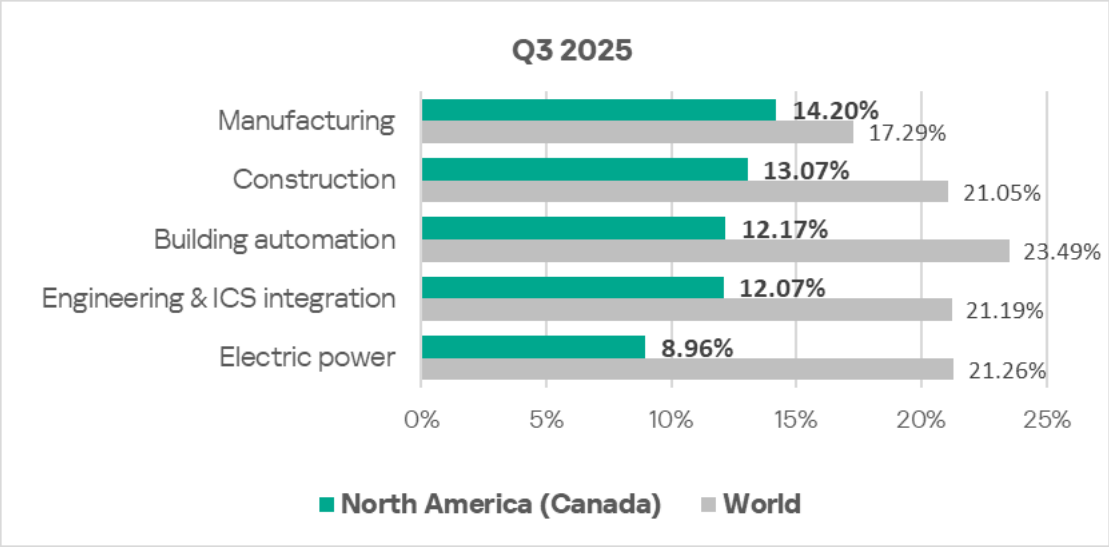
Based on the percentage of ICS computers on which ransomware was blocked, North America (Canada) is in second-to-last place (13th) with 0.07%, which is slightly higher than lowest-ranked Northern Europe.

The figure in the region fluctuates and decreased after its substantial growth in Q1 2025.

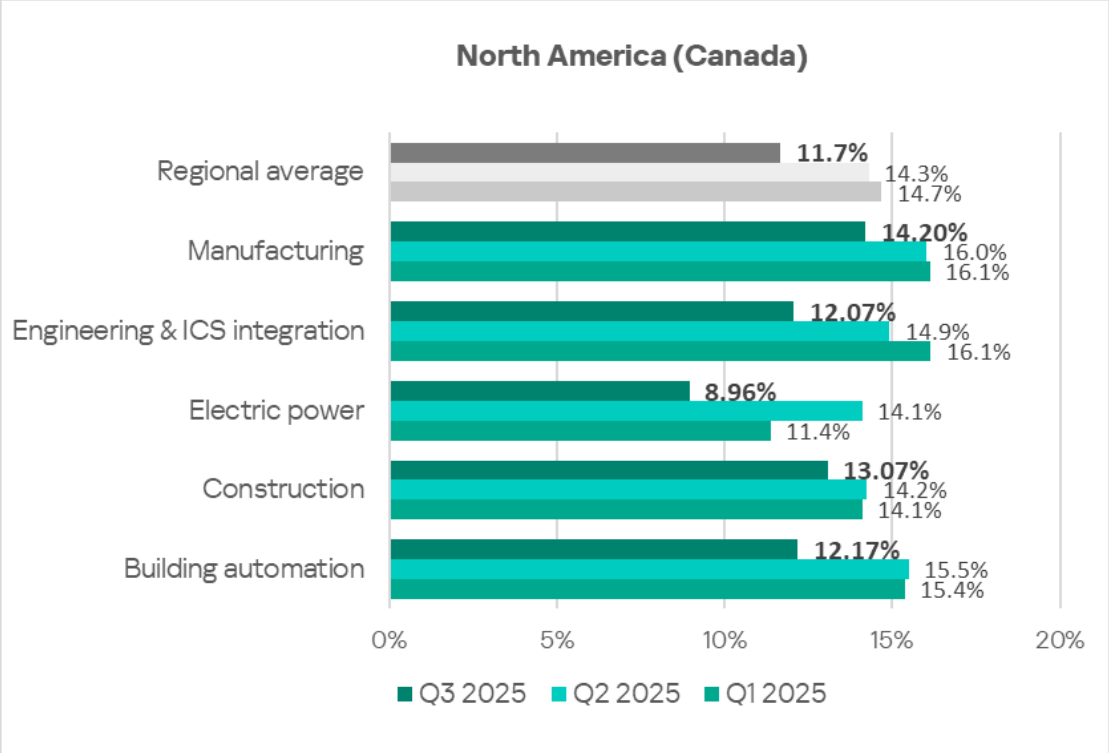


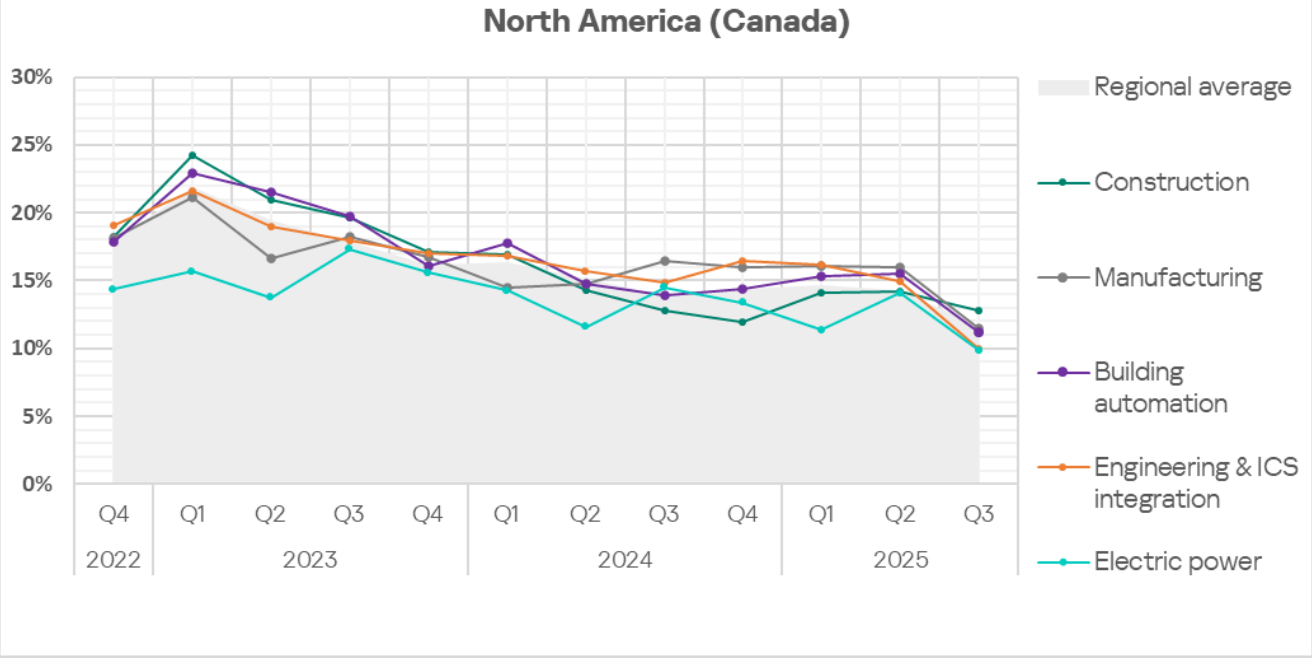
Industries

Among the industries reviewed in the report, the highest percentage of ICS computers on which malicious objects were blocked in North America (Canada) is the manufacturing sector.



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





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 North America (Canada), Q3 2025

Отрасль / Источник угрозы	Building automation	Electric power	Engineering & ICS integration	Construction	Manufacturing	Threat category total in the region
Internet	4.93%	4.05%	7.34%	6.99%	7.51%	6.19%
Email clients	4.08%	1.16%	1.82%	3.52%	2.64%	2.53%
Removable media	0.12%	0.58%	0.08%	0.00%	0.20%	0.07%
Network folders	0.04%	0.00%	0.00%	0.00%	0.00%	0.02%
Industry total in the region	12.17%	8.96%	12.07%	13.07%	14.20%	

Threat category indicators for industries in North America (Canada), Q3 2025

Industry / Threat category	Building automation	Electric power	Engineering & ICS integration	Construction	Manufacturing	Threat category total in the region
Denylisted internet resources	1.86%	1.45%	3.19%	2.33%	4.06%	2.60%
Malicious scripts and phishing pages (JS and HTML)	6.31%	2.31%	5.35%	6.81%	5.88%	5.46%
Spy Trojans, backdoors and keyloggers	2.47%	1.16%	1.38%	0.96%	0.81%	1.46%
Worms	0.69%	0.29%	0.18%	0.23%	0.41%	0.36%
Miners in the form of executable files for Windows	0.49%	0.29%	0.31%	0.09%	0.41%	0.25%
Malicious documents (MSOffice + PDF)	2.35%	0.00%	0.88%	1.37%	0.81%	1.23%
Viruses	0.24%	0.58%	0.18%	0.32%	0.20%	0.25%
Ransomware	0.16%	0.00%	0.03%	0.09%	0.00%	0.07%
Web miners running in browsers	0.49%	0.00%	0.23%	0.09%	0.00%	0.21%
Malware for AutoCAD	0.00%	0.00%	0.00%	0.05%	0.00%	0.01%
Industry total in the region	12.17%	8.96%	12.07%	13.07%	14.20%	

Building automation

Among industries in the region, the OT building automation industry has the following rankings:

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

Engineering and ICS integrators

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

- Second place based on the percentage of ICS computers on which internet threats were blocked.
- Second place in denylisted internet resources and spyware.

Electrical energy industry

Among the industries in the region, the electric power industry has the following rankings:

- First place in removable media threats.
- First place in viruses.

Construction

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

- Second place in the percentage of ICS computers on which threats in email clients were blocked.
- First place in malicious scripts and phishing pages, and malware for AutoCAD.
- Second place in viruses and ransomware.

Manufacturing

Among industries in the region, the manufacturing industry has the following rankings:

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

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