Kaspersky ICS CERT

kaspersky

Threat landscape for industrial automation systems

South and North America (Canada). Q4 2025

29.04.2026

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 email clients were blocked was significantly higher than the global average, by a factor of 1.9. On this metric, the region ranked second globally.

High percentage figures for threats distributed via email clients (phishing) and spyware clearly indicate that OT systems in the region are highly exposed to advanced categories of threat actors.

High percentage figures for malicious scripts and phishing pages, many of which target specifically employee authentication data for corporate services, also point to a high risk of targeted attacks against the OT infrastructure of industrial enterprises in the region.

South America ranked second in the regional rankings for the following threat categories: malicious documents, and malicious scripts and phishing pages.

High percentage figures for malicious documents

South America ranked second among regions in Q4 2025 based on the percentage of ICS computers on which malicious documents were blocked. The region's percentage figure was 1.8 times the global average.

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

High percentage figure for malicious scripts and phishing pages

Based on the percentage of ICS computers on which malicious scripts and phishing pages were blocked, South America ranked second among regions, with a percentage figure 1.5 times the global average.

Attackers use malicious scripts to perform a wide range of tasks, from collecting information, tracking the user's browsing activity, and redirecting the user's browser to malicious web resources to downloading various types of malware (such as spyware, surreptitious cryptocurrency miners, and ransomware) onto the user's system or browser. They are distributed both online and by email.

High percentage figures for spyware

South America ranked seventh among regions based on the percentage of ICS computers on which spyware was blocked. Spyware was in second place in the regional ranking of threat categories.

Attackers use spyware to steal confidential data. In targeted attacks, spyware is also used for lateral movement within compromised networks and to download final-stage malware.

Spyware is also used to steal information required to deliver other types of malware, such as ransomware.

Threats in industries

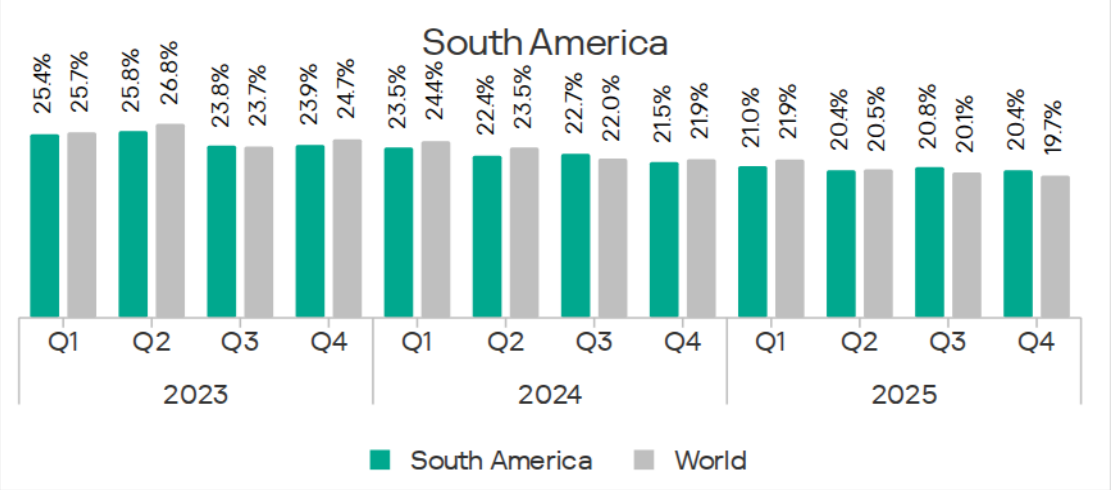
South America ranked in the top three in the regional rankings by percentage of ICS computers on which malicious scripts and phishing pages were blocked, across all industries except manufacturing. The region topped the ranking for the oil and gas industry.

In most industries, percentage figures for malicious documents were also high. South America led the regional ranking for this threat source in the oil and gas industry.

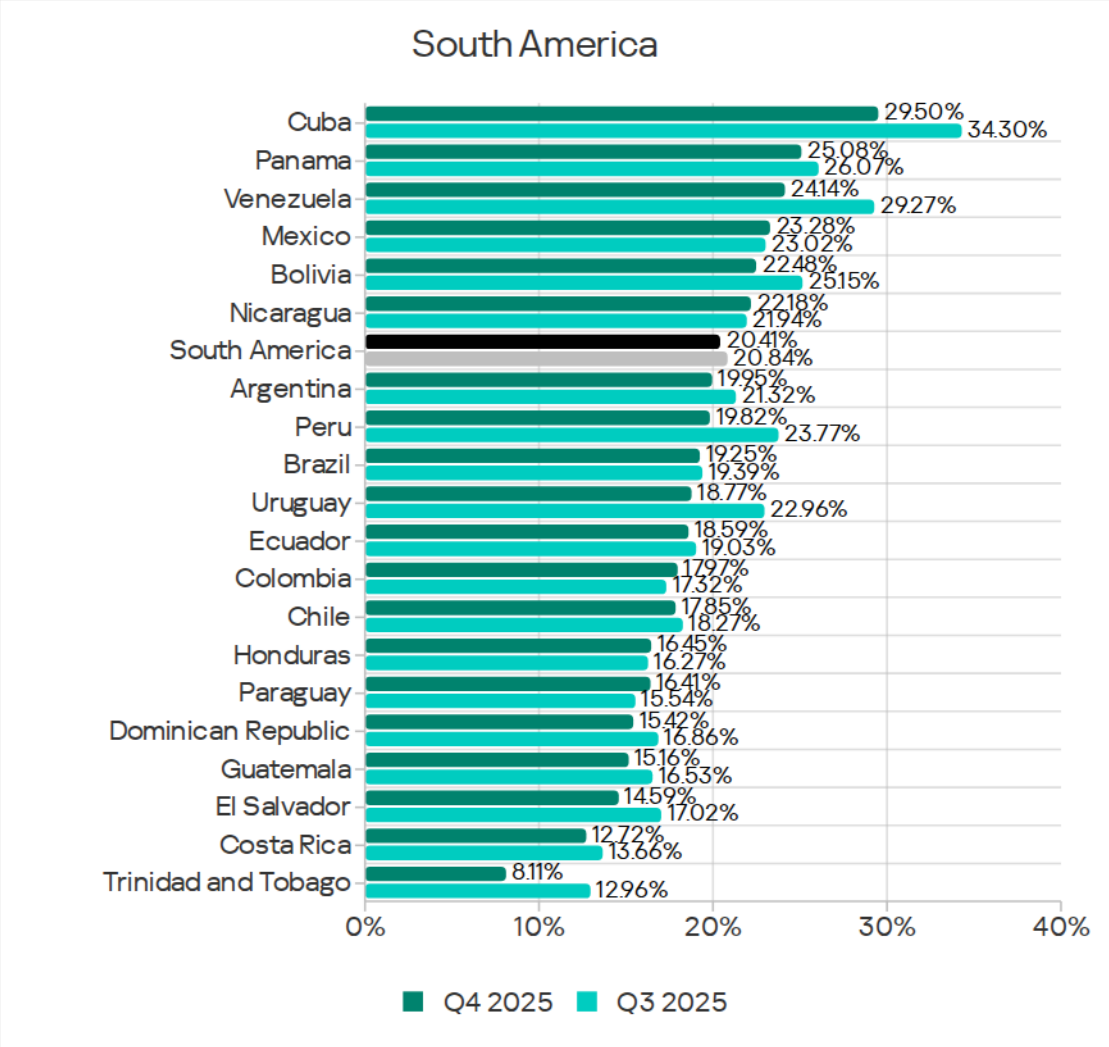
Statistics across all threats

In Q4 2025, South America ranked sixth among regions based on the percentage of ICS computers on which malicious objects were blocked, at 20.4%. This was 2.4 times the percentage figure in Northern Europe, which had the lowest value of all regions.

A downward trend was observed in South America. In Q4 2025, the percentage of ICS computers on which malicious objects were blocked returned to the level recorded in Q2 2025, after increasing in the previous quarter.

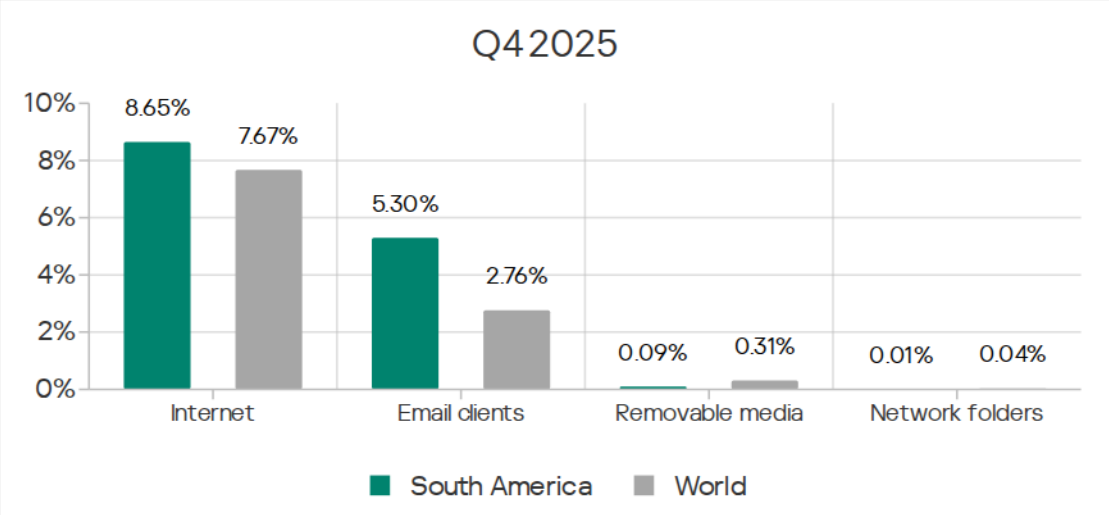


Among the region's countries, the percentage of ICS computers on which malicious objects were blocked ranged from 8.11% in Trinidad and Tobago to 29.50% in Cuba.



Threat sources

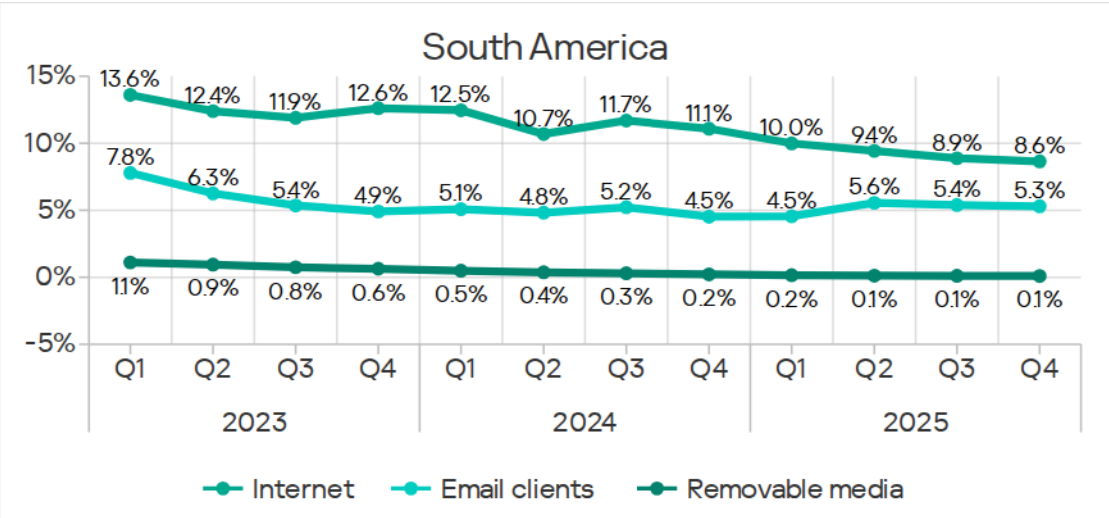
Malicious objects in the region were distributed primarily via the internet and email.



In Q4 2025, compared to global figures, the region had a higher percentage of ICS computers on which threats from the following sources were blocked:

- Internet – by a factor of 1.1;
- Email clients – by a factor of 1.9.

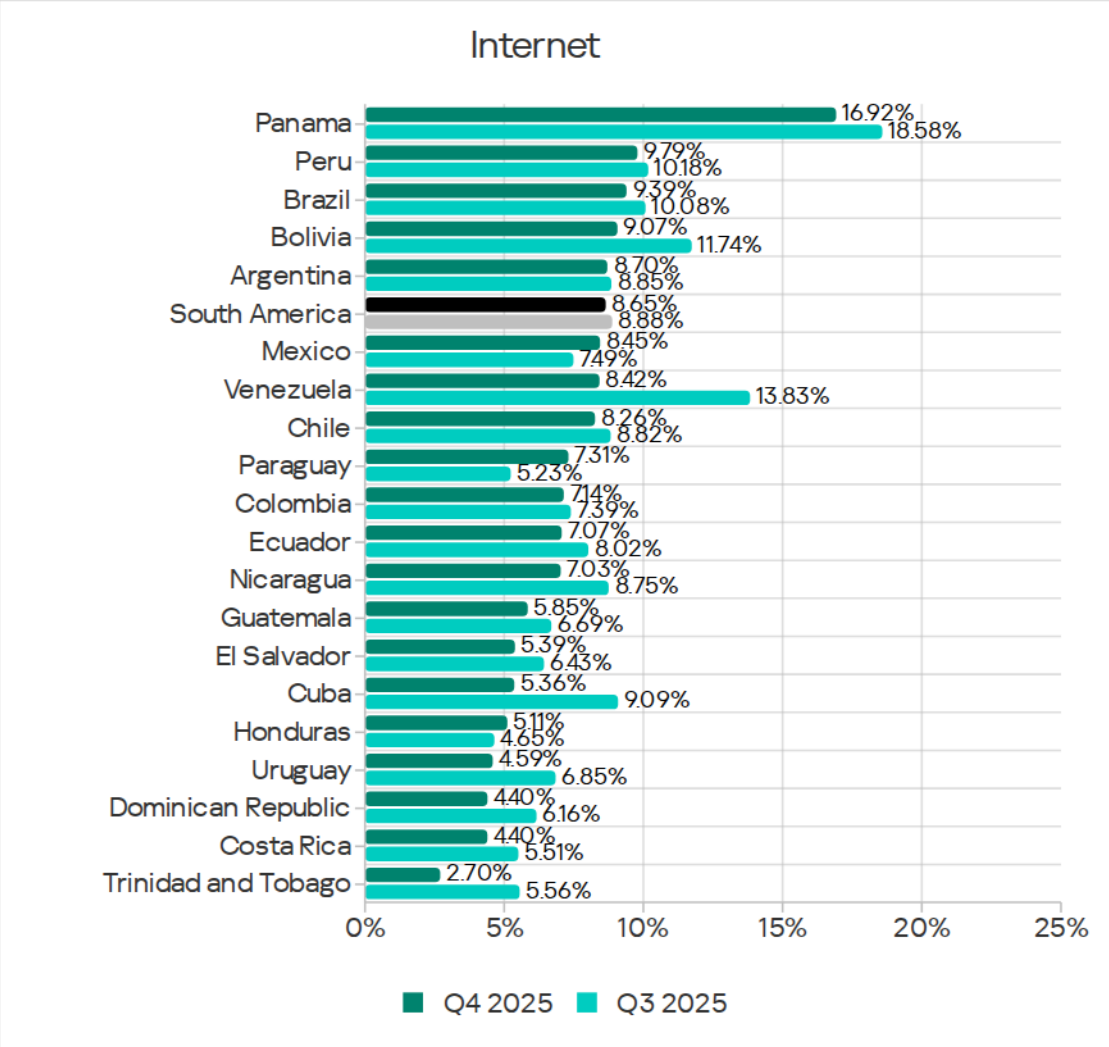
The percentage of ICS computers on which malicious objects were blocked decreased for all threat sources.



Internet

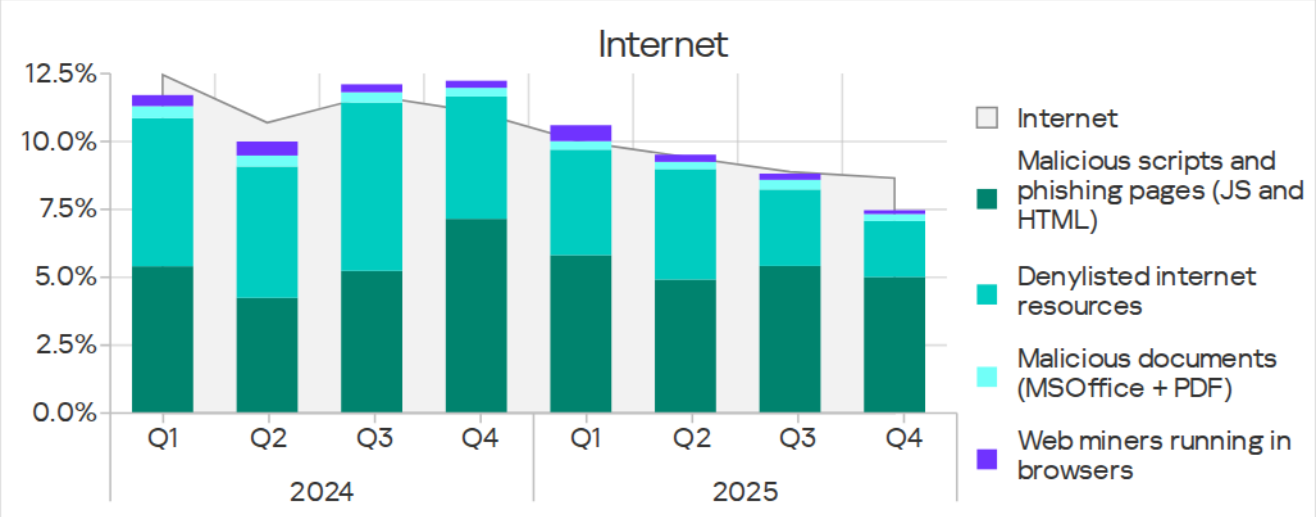
In Q4 2025, South America ranked fourth in the regional ranking by the percentage of ICS computers on which threats from the internet were blocked, at 8.65%. The region's percentage figure was 2.2 times that of Northern Europe, which ranked last.

Percentage figures for countries in the region ranged from 2.70% in Trinidad and Tobago to 16.92% in Panama.



In the previous quarter, the percentage for Panama increased by a factor of 2.4 due to a surge in threats in the malicious scripts and phishing pages category that were blocked when users attempted to access infected websites. Although the figure decreased in Panama in Q4, it did not return to its earlier levels.

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



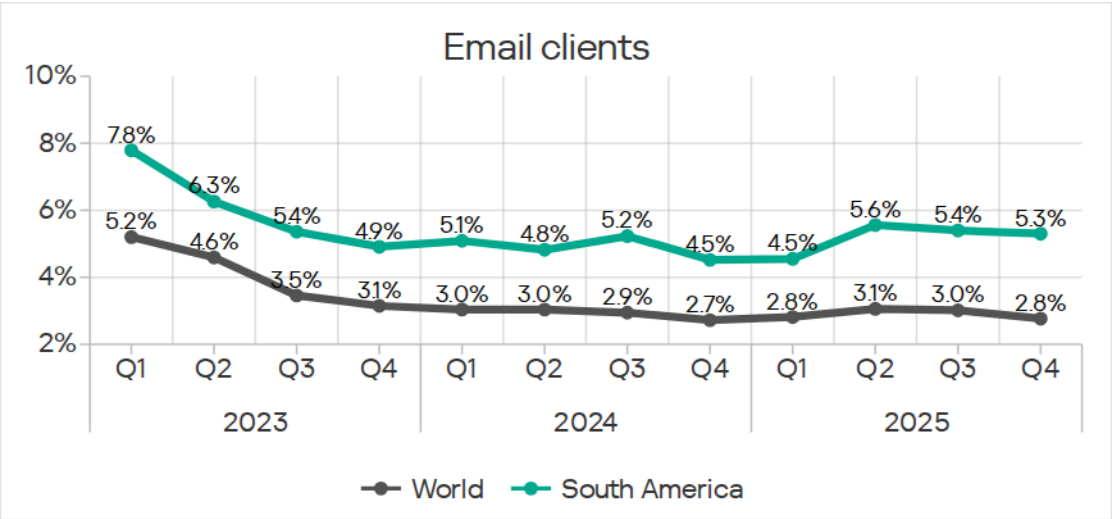
Email clients

In Q4 2025, South America rose from third to second place in the regional ranking based on the percentage of ICS computers on which threats from email clients were blocked, remaining behind only Southern Europe.

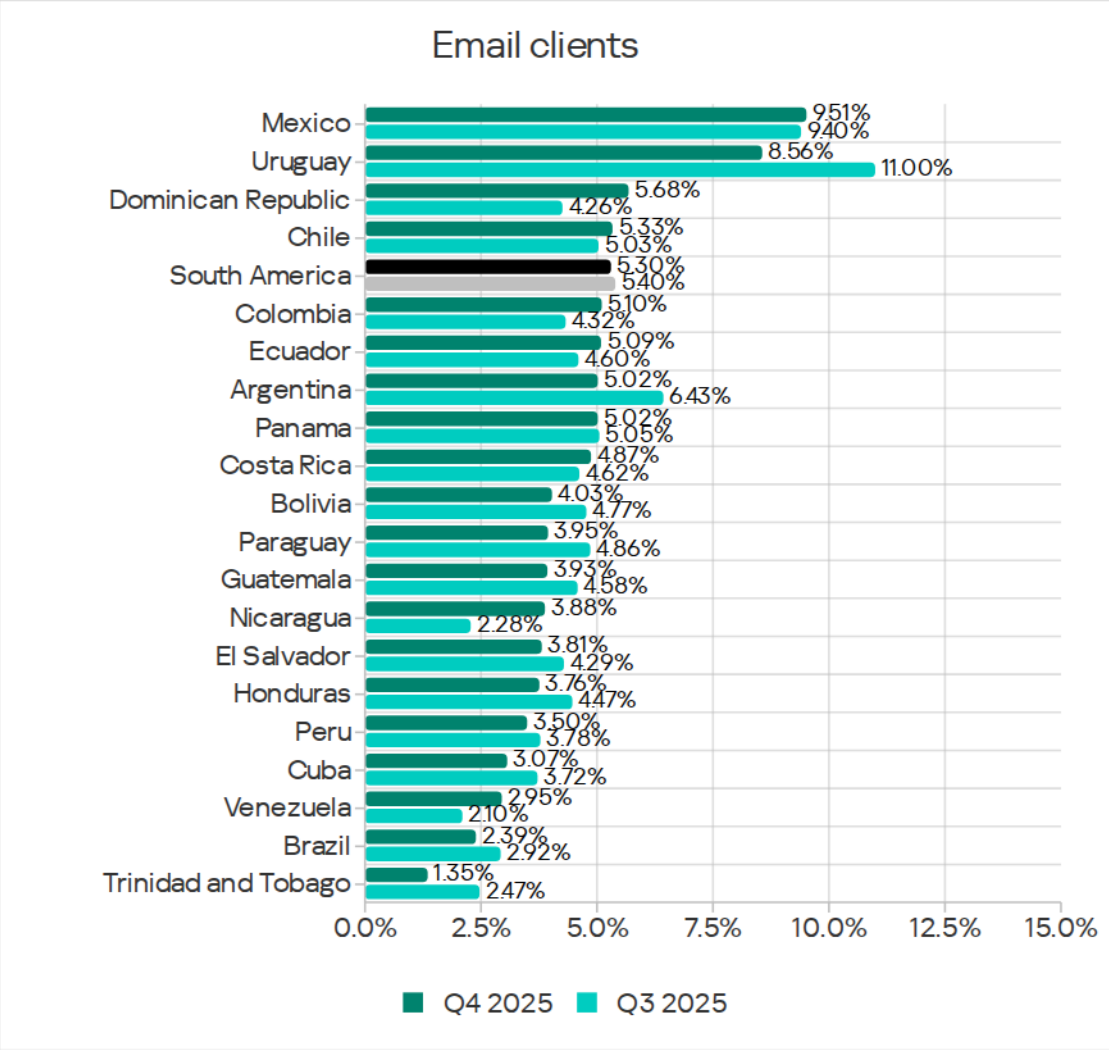
The high percentage figures for threats from email clients, as well as malicious scripts and phishing pages, indicate that OT infrastructure systems in the region are highly exposed to targeted attacks.

The percentage figure for South America, 5.30%, was 8.3 times that of Northern Europe, which was at the bottom of this ranking.

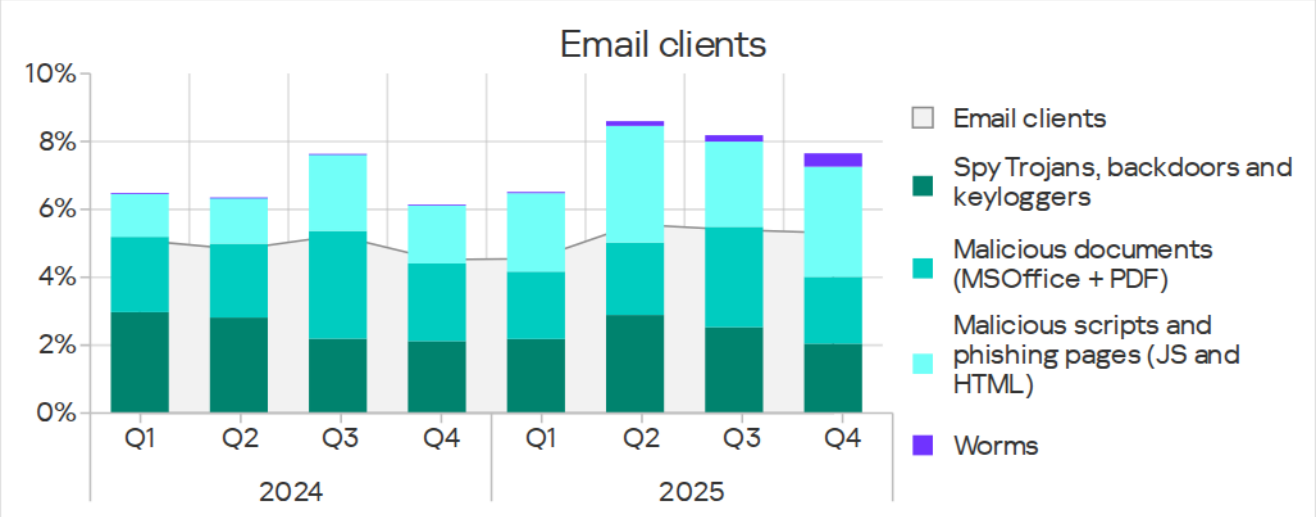
The percentage figure for threats from email clients in the region has been fluctuating. From Q2 through Q4 2025, the value was higher than in the previous eighteen months.



In terms of the percentage of ICS computers on which threats from email clients were blocked, Mexico (9.51%) and Uruguay (8.56%) led among the region's countries by a wide margin. Percentage figures for other countries ranged from 1.35% in Trinidad and Tobago to 5.68% in the Dominican Republic.



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



In Q4 2025, a noticeable increase was recorded in the percentage of ICS computers on which worms from email clients were blocked. This was linked to a new wave of phishing campaigns known as "Curriculum-vitae-catalina," which targeted all regions of the world. In South America, the attacks peaked in October.

Attackers sent phishing emails disguised as job applications. Posing as a curriculum vitae (CV), such emails contained a malicious executable file (Backdoor.MSIL.Xworm, a worm-backdoor for remote administration). If the file was launched, the system became infected.

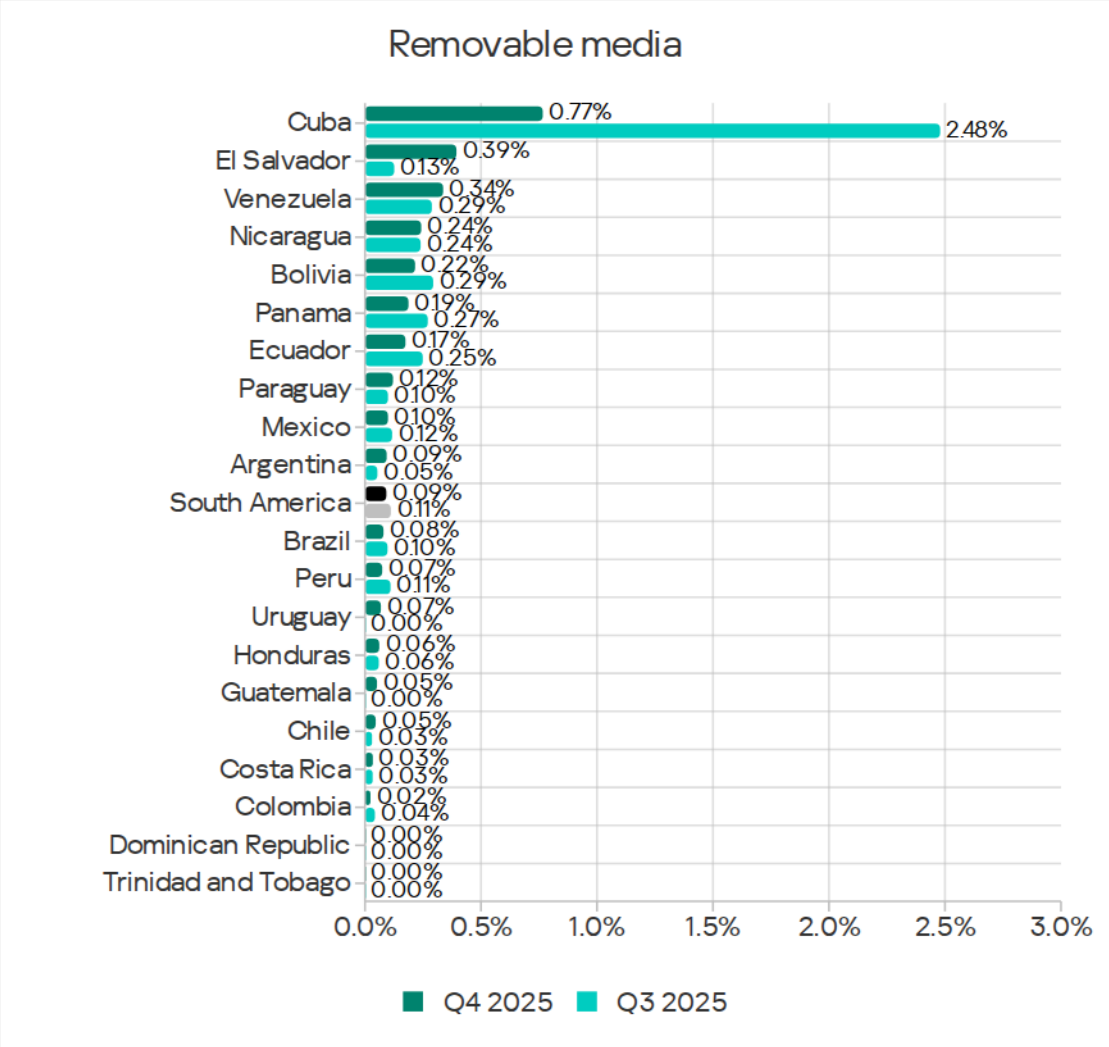
Such campaigns are typically designed to deliver data-stealing malware, spyware, or remote administration tools (RATs).

The countries that led the email clients ranking, Mexico and Uruguay, also ranked at the top for spyware and malicious documents.

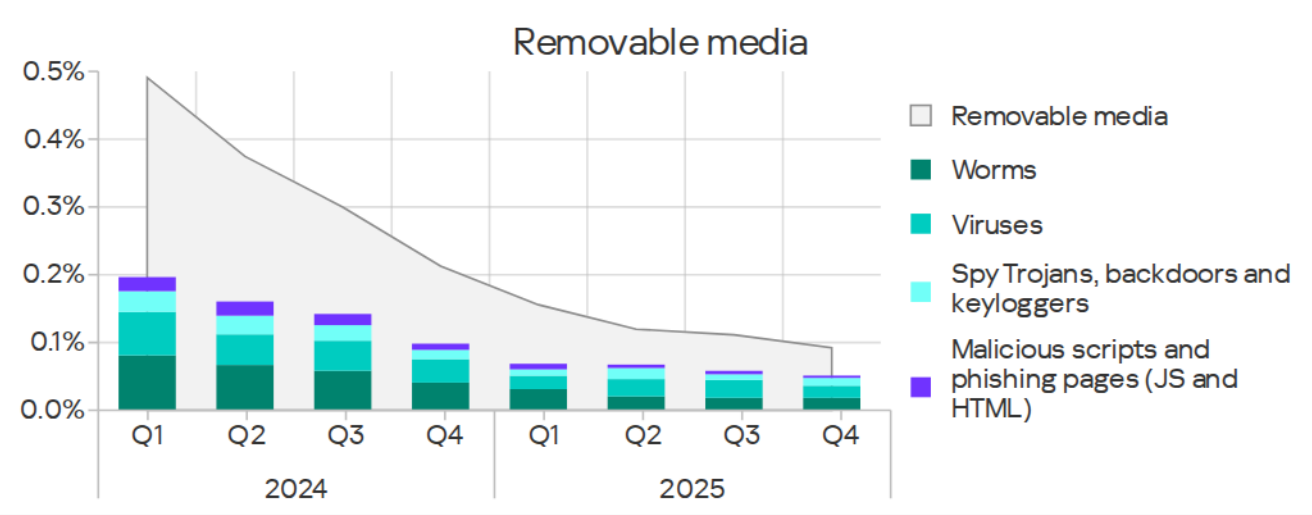
Removable media

In Q4 2025, South America ranked 10th among regions, at 0.09%, based on the percentage of ICS computers on which threats were blocked when connecting removable media. This was 1.8 times the percentage for the Australia and New Zealand region, which ranked last.

Cuba led among countries in the region in the percentage of ICS computers on which threats were blocked when connecting removable media, at 0.77%.

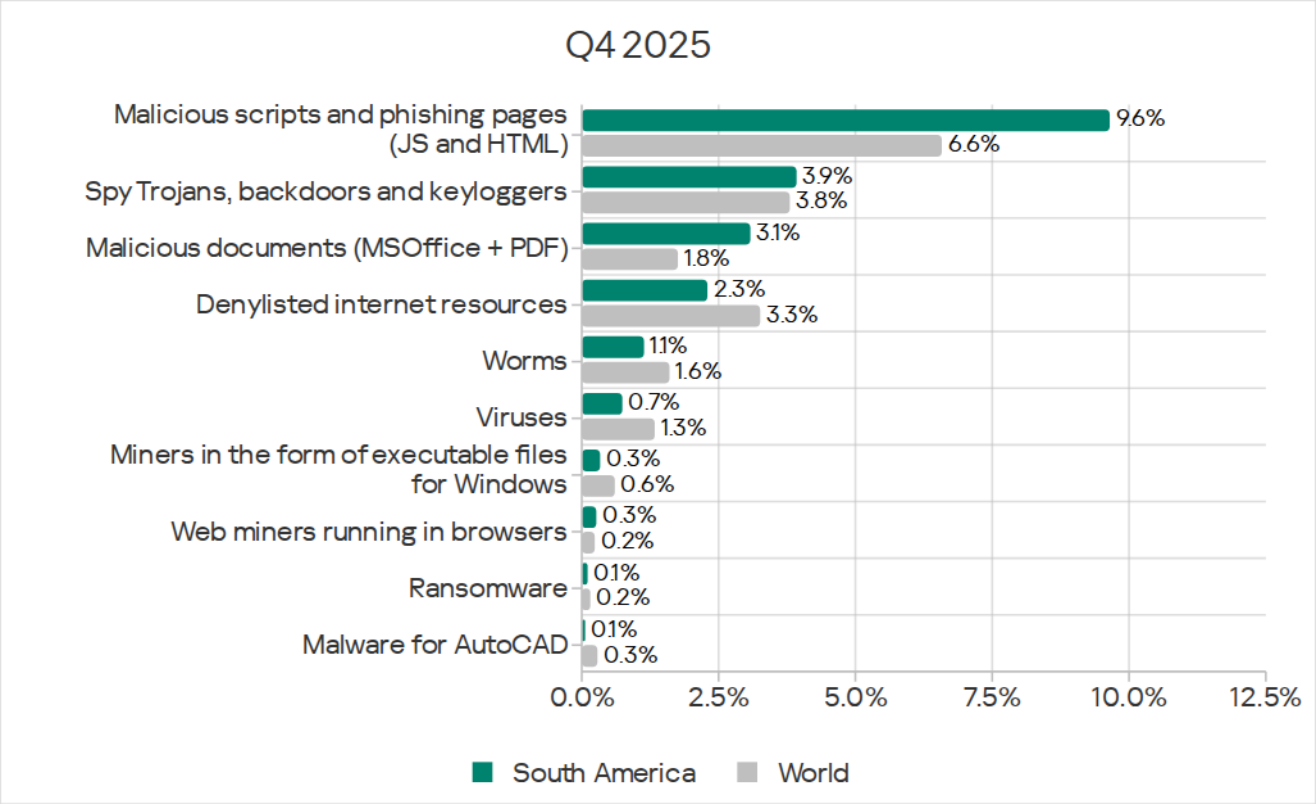


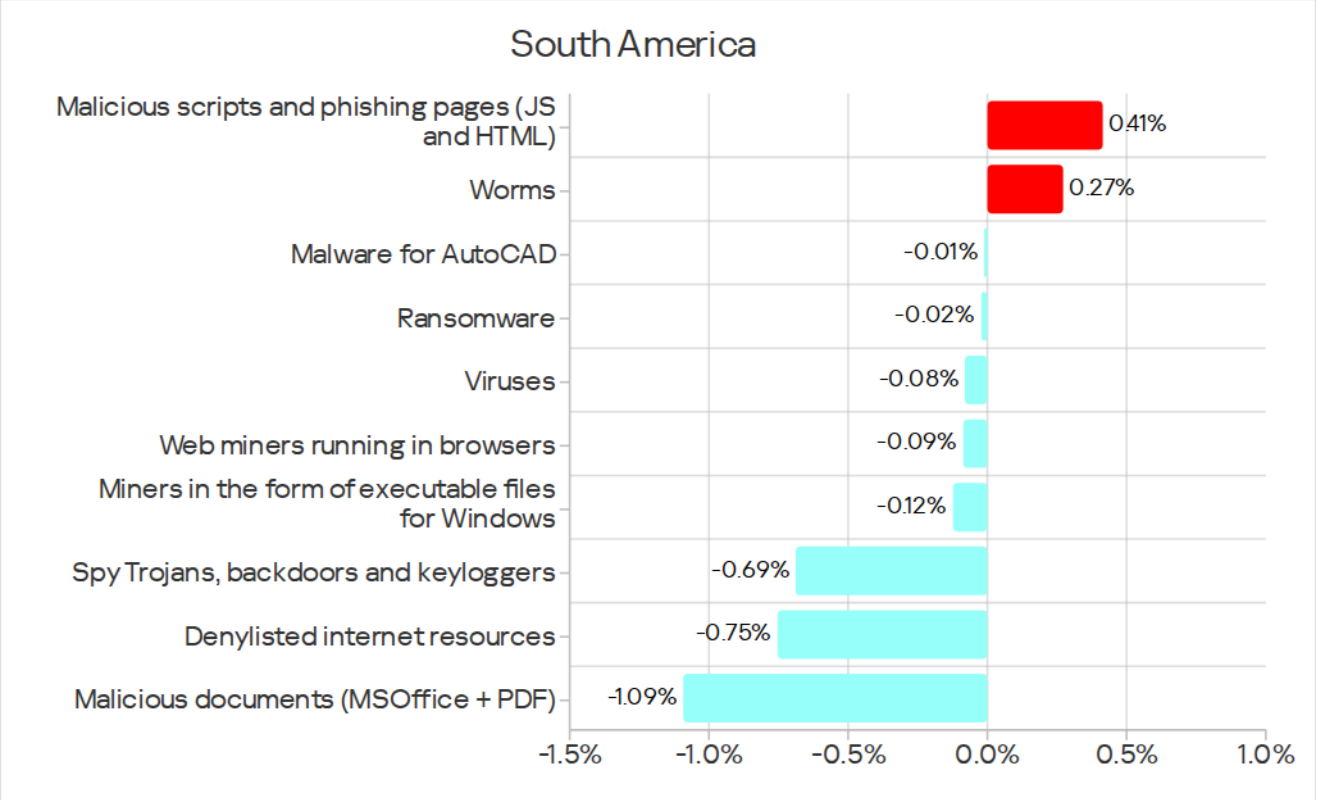
The main categories of threats blocked when connecting removable media to ICS computers were worms, viruses, and spyware.



Threat categories

Threats that spread primarily via email clients – spyware and malicious documents – ranked second and third in the regional ranking of threat categories by the percentage of ICS computers on which they were blocked. Malicious scripts, which top this ranking, spread via the internet and email.





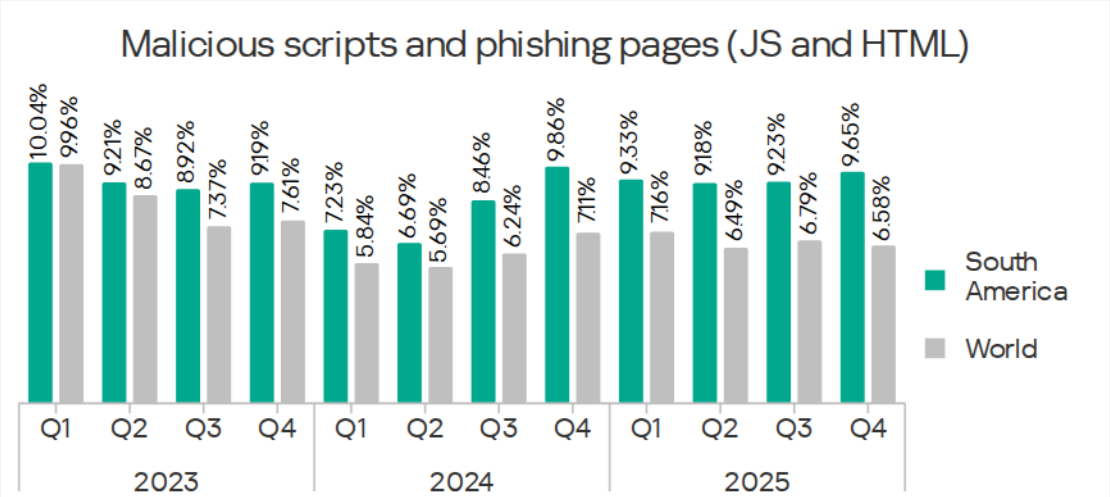
Compared to global figures, the region had a higher percentage of ICS computers on which the following threat categories were blocked:

- Malicious documents – by a factor of 1.8, second place among regions based on the percentage of ICS computers on which the threat was blocked.
- Malicious scripts and phishing pages – by a factor of 1.5, second place among regions, both by the percentage of ICS computers on which the threat was blocked and by the increase in the percentage figure;
- Web miners – by a factor of 1.1, second place among regions;
- Spyware.

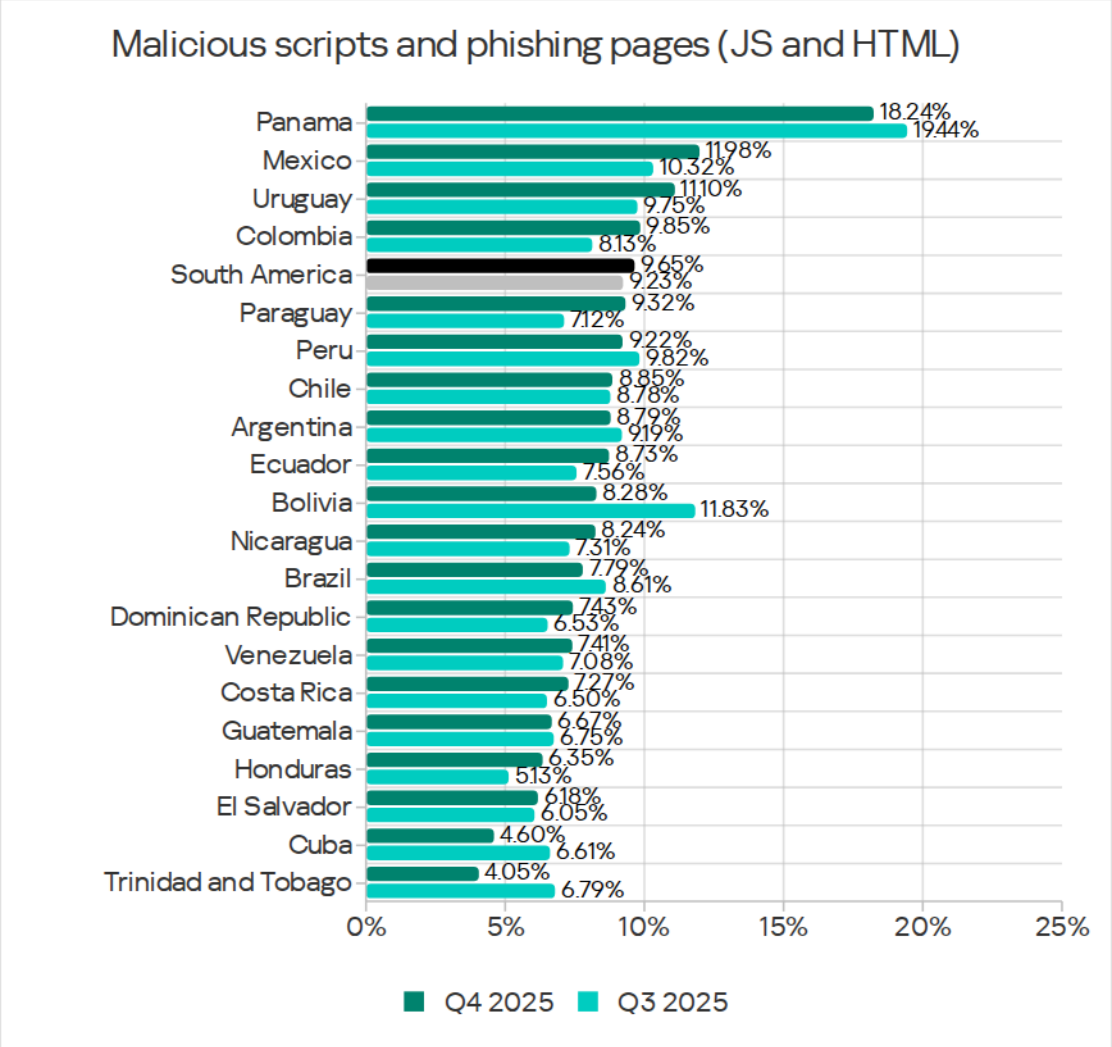
Malicious scripts and phishing pages

South America ranked second among regions, with 9.65%, based on the percentage of ICS computers on which malicious scripts and phishing pages were blocked. This was 3.8 times the percentage figure in Northern Europe, which had the lowest value among all regions.

The regional figure grew for the second consecutive quarter, reaching its highest level of 2025. Among the four regions where the value increased over the quarter, South America ranked second in growth.



Panama led among countries in the region by a wide margin, with 18.24%, based on the percentage of ICS computers on which malicious scripts and phishing pages were blocked. In the previous quarter, the country's figure surged sharply due to attempts to infect popular WordPress-powered websites, specifically those of government organizations. In Q4, the figure did not return to its earlier levels.

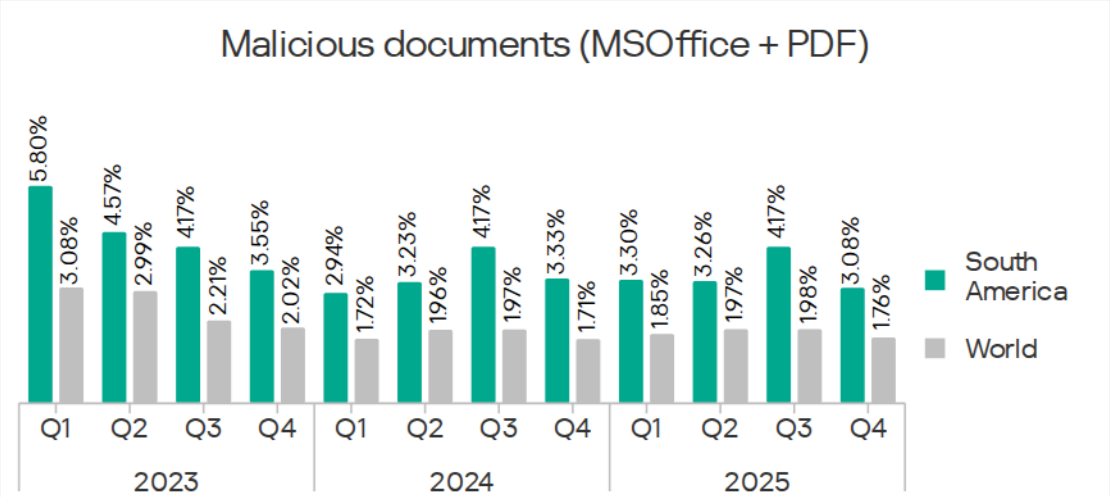


Malicious scripts and phishing pages were distributed via both the internet and email.

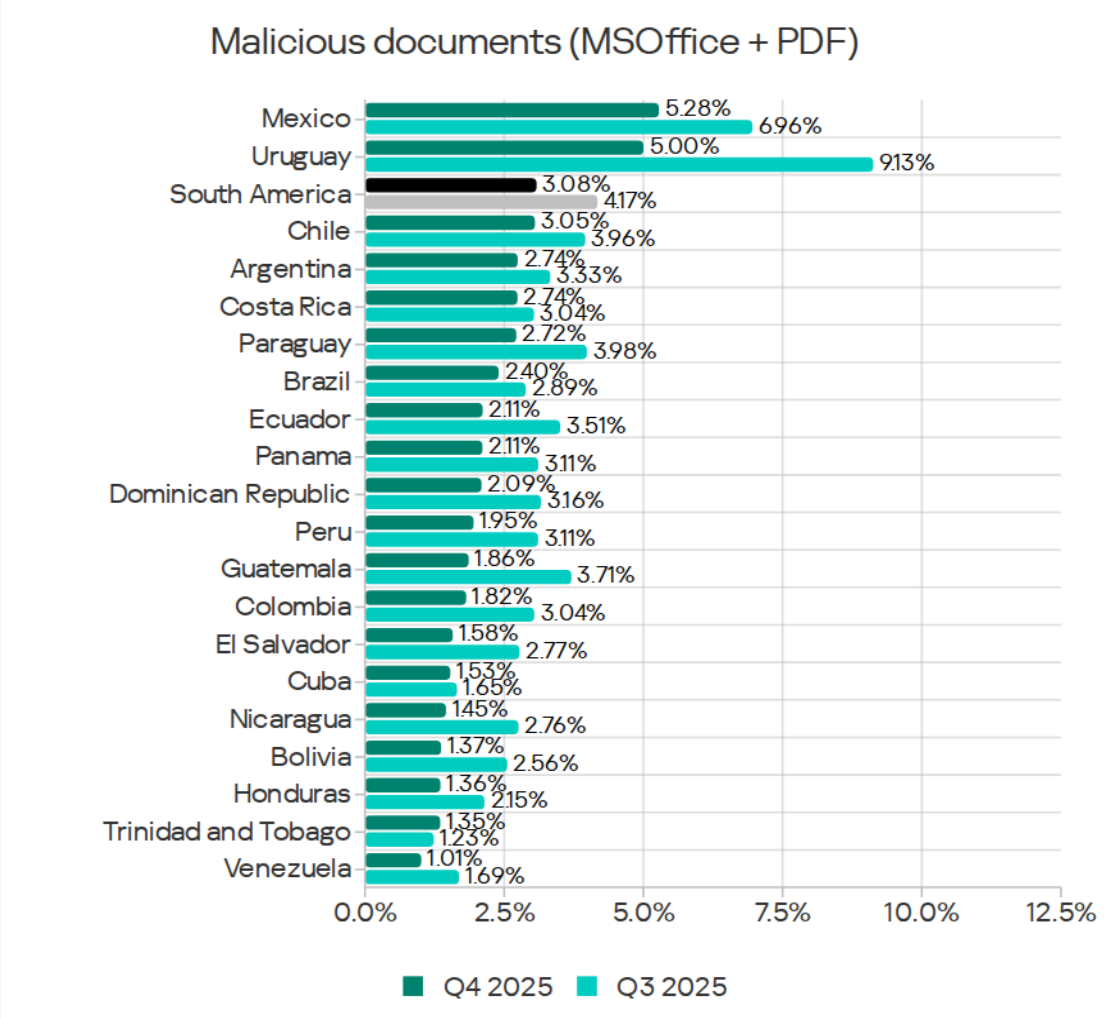
Malicious documents

South America ranked second among regions in the percentage of ICS computers on which malicious documents were blocked, at 3.08%. This was 6.7 times higher than in Northern Europe, which was at the bottom of this ranking.

The percentage figure in the region has been fluctuating; it decreased in Q4.



Mexico (5.28%) and Uruguay (5.00%) led among countries in the region by a wide margin in terms of the percentage of ICS computers on which malicious documents were blocked. After an increase in the previous quarter, the percentage figures decreased in all countries.

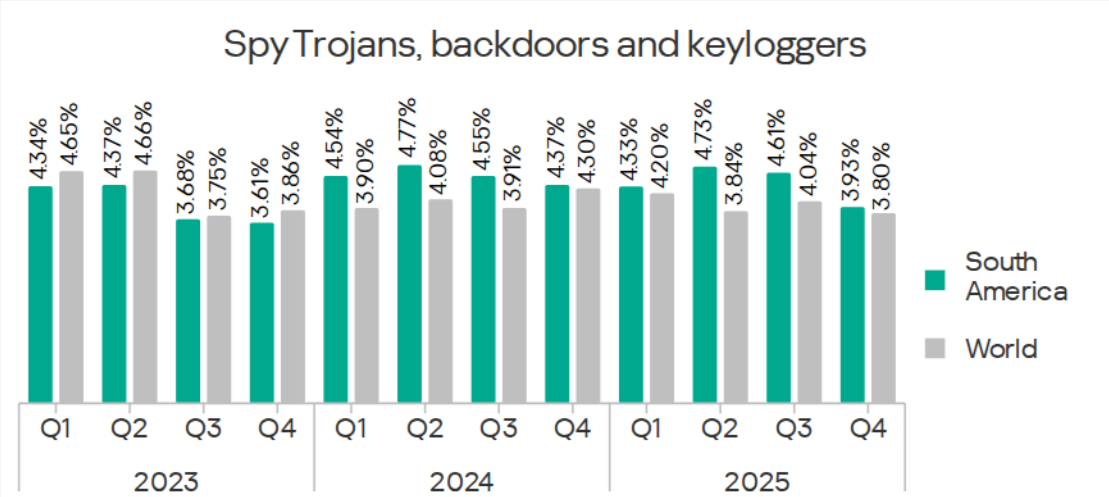


Malicious documents were distributed primarily via email. Mexico and Uruguay also topped the ranking of the region's countries by the percentage of ICS computers on which threats were blocked in email clients.

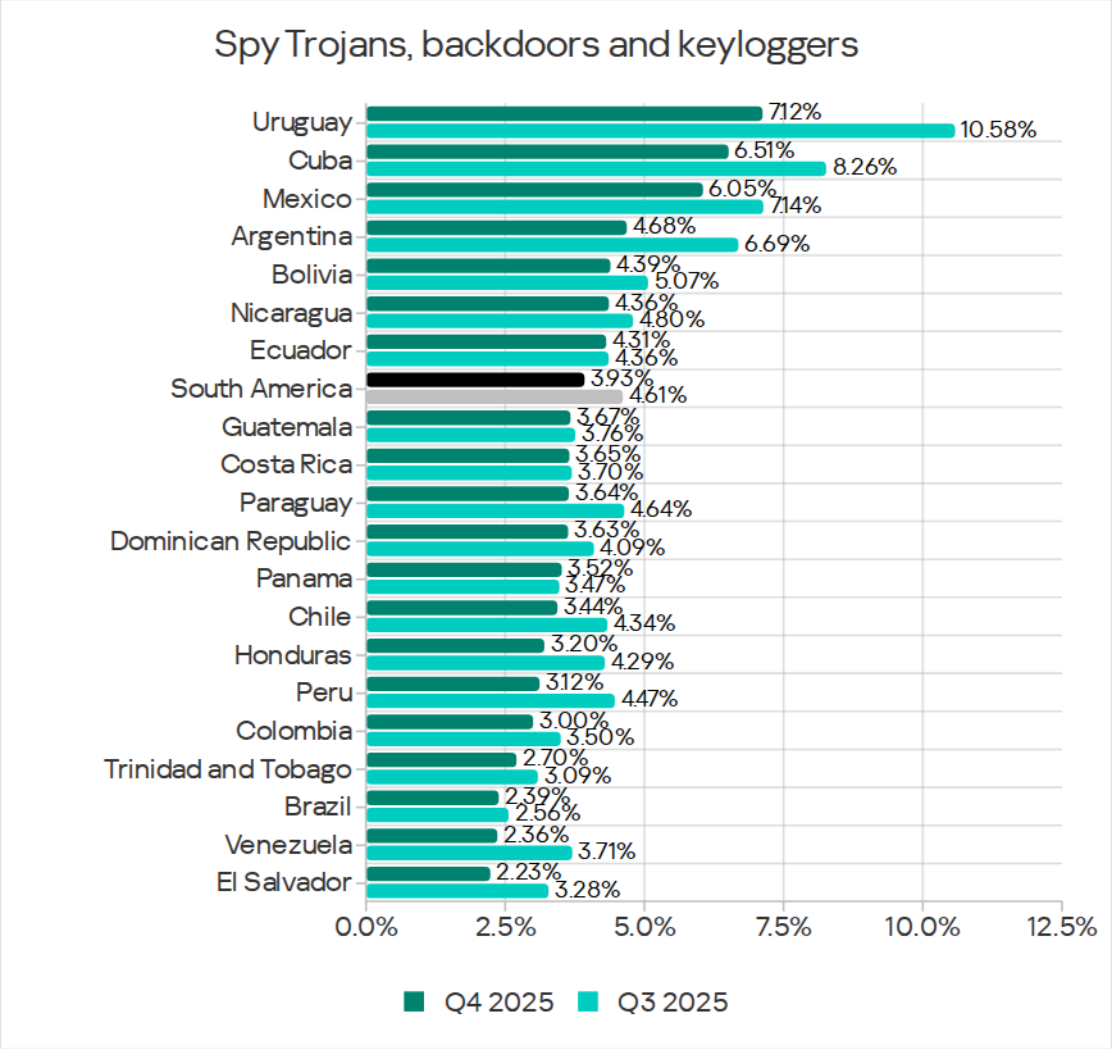
Spyware

South America ranked seventh among regions, with 3.93%, based on the percentage of ICS computers on which spyware was blocked. This was 3.1 times the percentage in Northern Europe, which had the lowest value.

The percentage of ICS computers on which spyware was blocked in South America has been fluctuating; it decreased in Q3 and Q4 2025.



Among the region's countries, Uruguay led in the percentage of ICS computers on which spyware was blocked, with 7.12%. The lowest figure was in El Salvador, at 2.23%. The percentage values decreased in all countries except Panama.

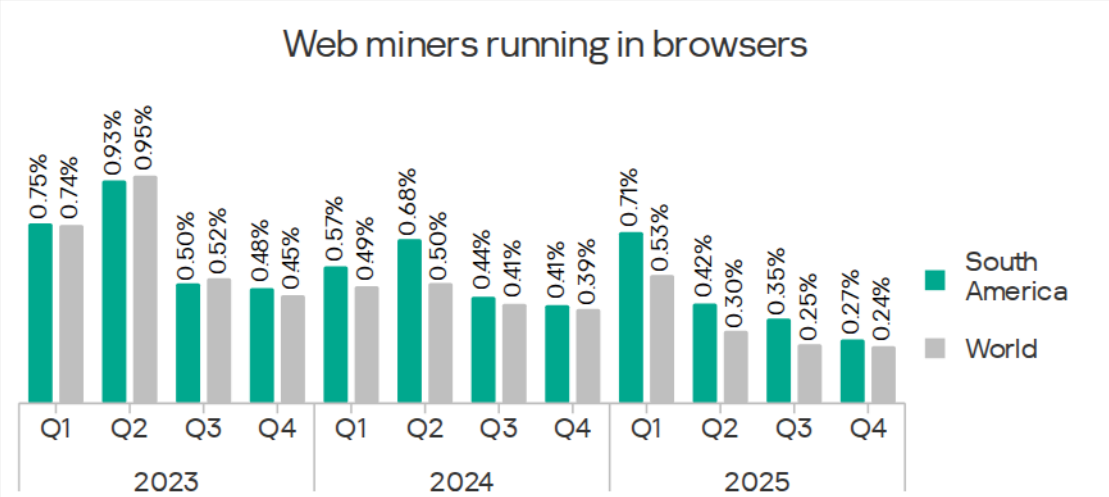


Spyware in the region was primarily blocked in email clients. Uruguay and Mexico, which led the ranking for spyware, also ranked among the leaders for threats from email clients.

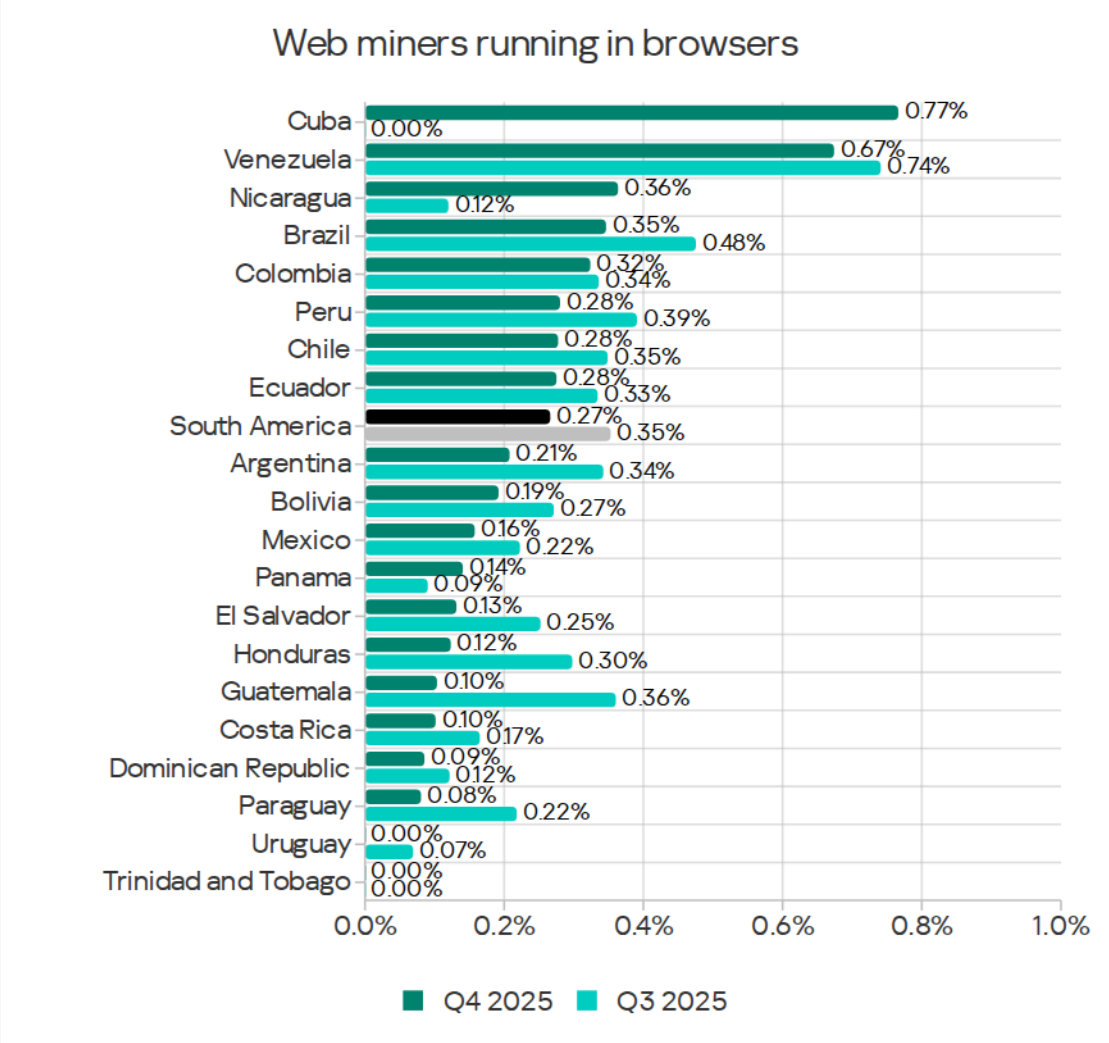
Web miners

South America, at 0.27%, ranked second among regions in Q4 2025 by the percentage of ICS computers on which web miners were blocked. This was 4.5 times the percentage figure in East Asia, which ranked last.

The percentage figures for web miners declined in the region for the third consecutive quarter, reaching their lowest level in three years in Q4 2025.



Among countries in the region, Cuba (0.77%) and Venezuela (0.67%) led by a wide margin in the percentage of ICS computers on which web miners were blocked.

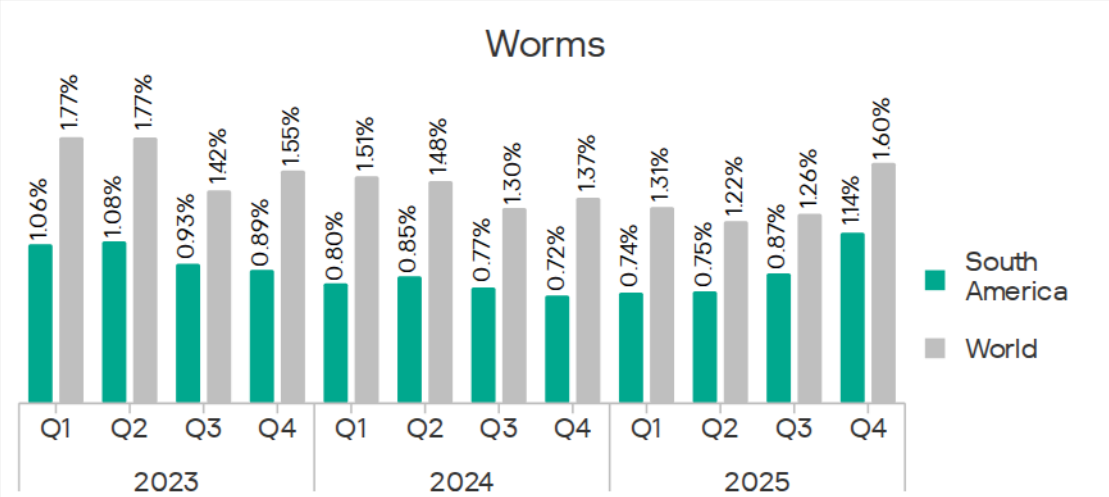


Worms

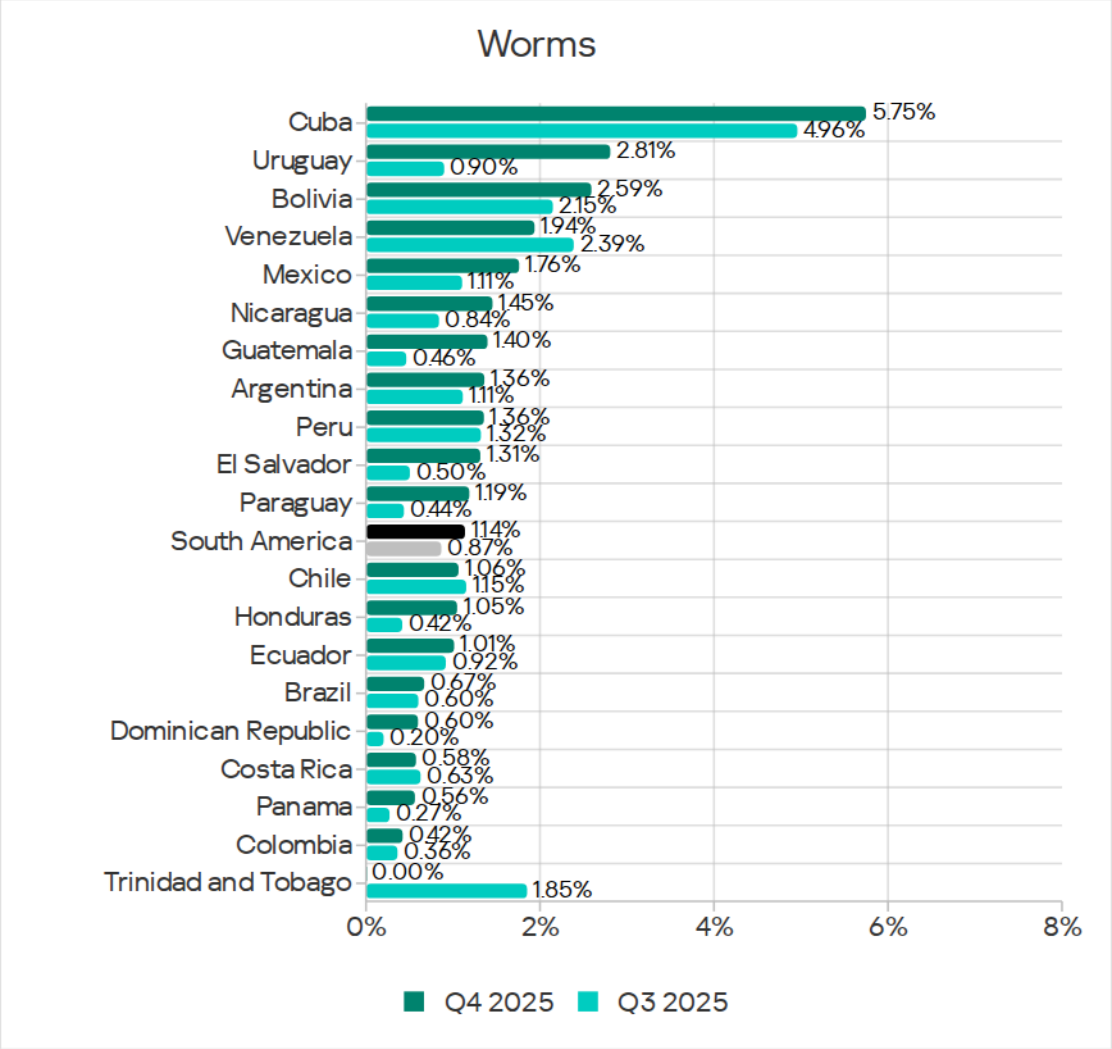
South America ranked ninth among regions based on the percentage of ICS computers on which worms were blocked.

In Q4 2025, the percentage figures for worms increased across all regions due to a new wave of phishing campaigns known as "Curriculum-vitae-catalina," described above.

In South America, the percentage increased to 1.14%. This was 3.6 times higher than in Northern Europe, which had the lowest value among all regions.



Among countries of the region, Cuba led by a wide margin in the percentage of ICS computers on which worms were blocked, with 5.75%. In Uruguay, the percentage increased by a factor of 3.1 over the quarter. The value increased in all countries of the region except Venezuela, Chile, Costa Rica, and Trinidad and Tobago.

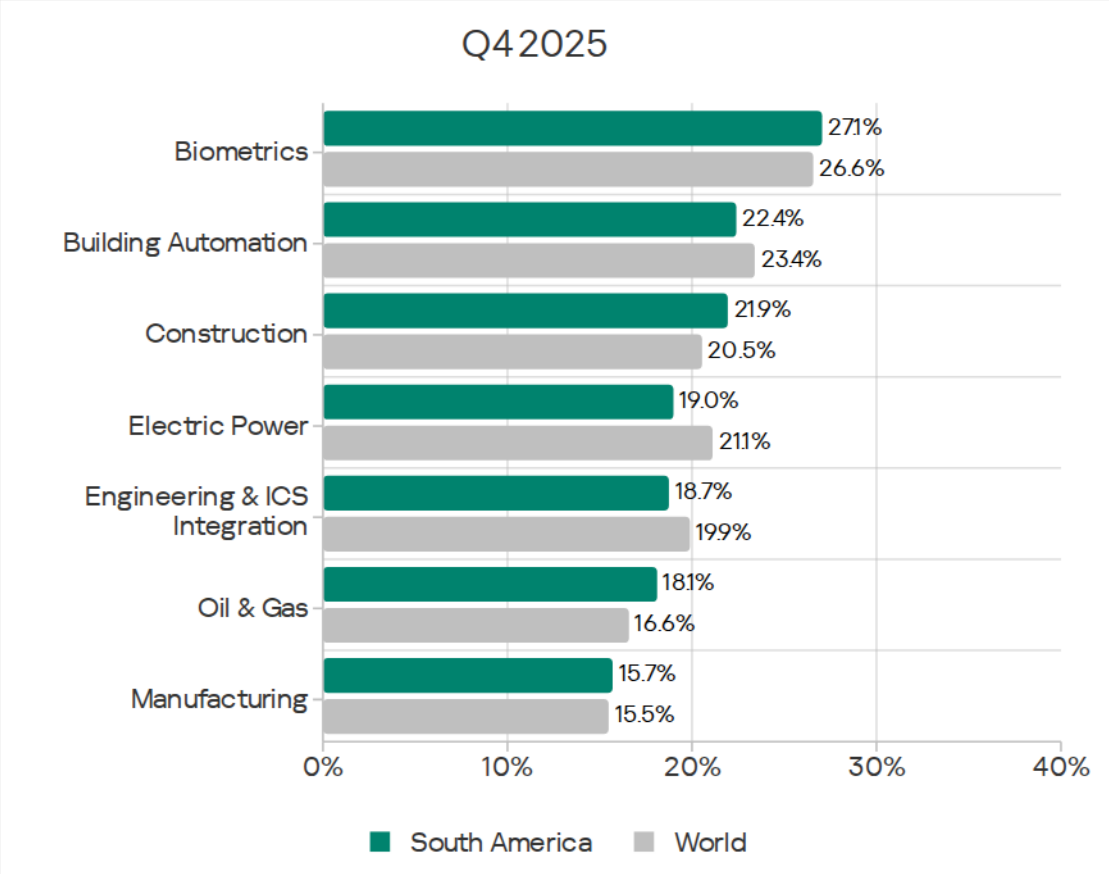


Although worms spread through all channels, email was the primary source of worms in Q4 due to phishing campaigns.

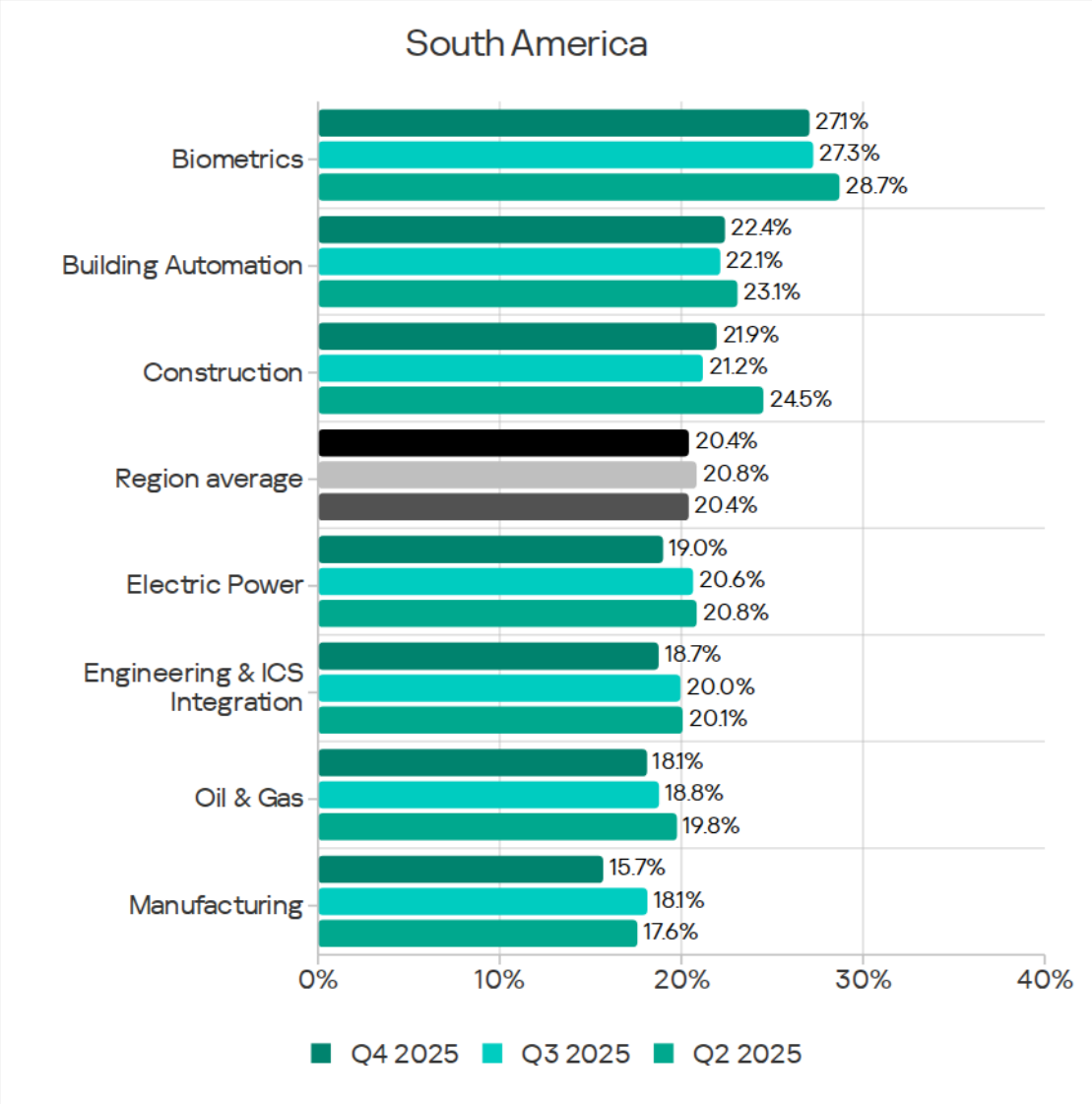
Industries

In South America, malicious objects were most frequently blocked in biometrics among all industries covered in this report.

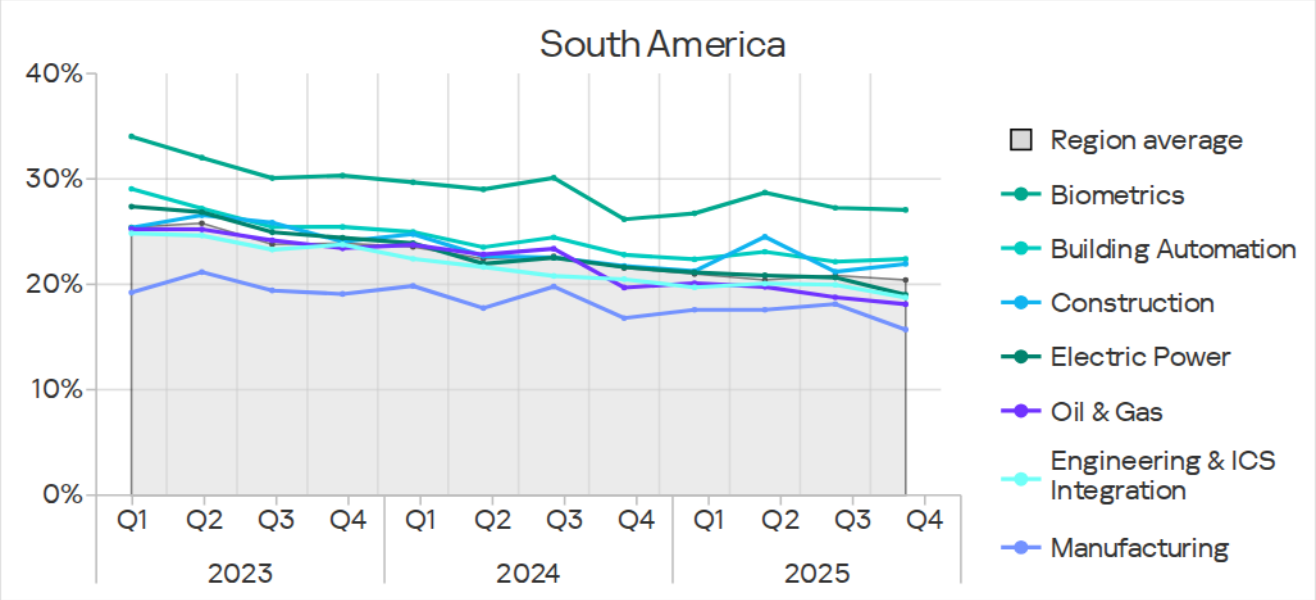
The percentage of ICS computers on which malicious objects were blocked in the region exceeded the global averages in four industries: biometrics, construction, oil and gas, and manufacturing. The greatest difference was in the oil and gas industry, where the regional figure was 1.1 times higher than the global figure.



In Q4 2025, the percentage of ICS computers on which malicious objects were blocked decreased in all industries except building automation and construction.



Despite fluctuations, the industries covered in this report have shown a predominantly positive (declining) 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. Red signifies that the figure is close to the maximum.

Threat source indicators for industries in South America, Q4 2025

Industry / Threat source	Biometrics	Building Automation	Engineering & ICS Integration	Electric Power	Oil & Gas	Construction	Manufacturing	Category metric in region
Internet	8.35%	8.36%	9.17%	9.54%	8.67%	11.45%	7.06%	8.65%
Email clients	12.07%	7.49%	2.96%	2.80%	3.56%	3.58%	2.31%	5.30%
Removable media	0.09%	0.09%	0.08%	0.13%	0.22%	0.14%	0.05%	0.09%
Network folders	0.01%	0.01%	0.00%	—	—	—	0.01%	0.01%
Industry metric in region	27.05%	22.40%	18.75%	19.00%	18.11%	21.94%	15.70%	

Threat category indicators for industries in South America, Q4 2025

Industry / Threat type	Biometrics	Building Automation	Engineering & ICS Integration	Electric Power	Oil & Gas	Construction	Manufacturing	Category metric in region
Denylisted internet resources	1.95%	2.21%	2.44%	2.73%	2.22%	3.01%	1.89%	2.30%
Malicious scripts and phishing pages (JS and HTML)	14.32%	11.49%	7.84%	8.14%	8.11%	9.70%	6.26%	9.65%
Malicious documents (MSOffice + PDF)	5.98%	4.03%	2.16%	2.22%	2.89%	2.26%	2.03%	3.08%
Spy Trojans, backdoors and keyloggers	7.82%	5.20%	2.60%	2.64%	2.22%	3.23%	2.50%	3.93%
Ransomware	0.14%	0.14%	0.09%	0.16%	0.22%	0.08%	0.09%	0.11%
Miners in the form of executable files for Windows	0.33%	0.35%	0.36%	0.33%	0.44%	0.43%	0.26%	0.34%
Web miners running in browsers	0.21%	0.28%	0.30%	0.26%	0.56%	0.35%	0.18%	0.27%
Malware for AutoCAD	0.04%	0.04%	0.07%	0.06%	—	0.41%	0.02%	0.06%
Worms	1.77%	1.49%	0.86%	1.08%	1.33%	0.79%	0.77%	1.14%
Viruses	1.00%	0.82%	0.65%	0.97%	0.44%	1.12%	0.64%	0.74%
Industry metric in region	27.05%	22.40%	18.75%	19.00%	18.11%	21.94%	15.70%	

Characteristics of the region

South America ranked second among regions based on the percentage of ICS computers on which threats from email clients were blocked.

South America also ranked second among regions in terms of the percentage of ICS computers on which threats from email clients were blocked in biometrics.

Attackers use email to distribute malicious documents and malicious scripts and phishing pages, which are used, among other purposes, to download spyware onto the user's system.

South America ranked second among regions for malicious scripts and malicious documents, and seventh for spyware. These threat categories were relevant for all industries in the region.

It should be noted that high percentage figures for these threats clearly indicate that OT systems in the region are highly exposed to advanced categories of threat actors.

South America was among the top three regions based on the percentage of ICS computers on which malicious scripts and phishing pages were blocked, for all industries except manufacturing:

- Oil and gas industry – the region ranked first;
- Biometrics, construction, and the electric energy industry – the region ranked second;
- Building automation, and engineering and ICS integrators – the region ranked third.

In many cases, malicious scripts were specifically designed to steal employee authentication data for corporate services.

South America was among the top three regions based on the percentage of ICS computers on which malicious documents were blocked, for the following industries:

- Oil and gas industry – the region ranked first;
- Biometrics, engineering and ICS integrators, and manufacturing – the region ranked second;
- Construction and the electric energy industry – the region ranked third.

In the oil and gas industry, South America ranked third among regions in terms of spyware.

In Q4 2025, email clients became a source of a worm-backdoor distributed in emails in a new wave of phishing campaigns. Among industries in South America, biometrics and building automation led in terms of the percentage of ICS computers on which threats from email clients were blocked. These same two industries also ranked first and second in the regional industry rankings for malicious scripts, malicious documents, spyware, and worms.

Biometrics

South America ranked third among regions based on the percentage of ICS computers on which malicious objects were blocked in biometrics.

South America ranked as follows among regions in terms of percentage figures for biometrics:

- Second, by the percentage of ICS computers on which threats from email clients were blocked;
- Second, by the percentage of ICS computers on which malicious documents, and malicious scripts and phishing pages were blocked.

Biometrics ranked as follows among industries in the region:

- First, in terms of the percentage figures for threats from email clients, and third, in terms of the percentage figures for threats in network folders;
- First, in terms of the percentage figures for the following threat categories: malicious scripts and phishing pages, malicious documents, spyware, and worms;
- Second, in terms of percentage figures for viruses.

Building automation

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

South America ranked as follows among regions based on its percentage figures for this industry:

- Third, in terms of the percentage of ICS computers on which malicious scripts and phishing pages were blocked.

Building automation ranked as follows among industries in the region:

- Second, based on the percentage of ICS computers on which threats were blocked in email clients and in network folders;
- Second, based on the percentage figures for the following threat categories: malicious scripts and phishing pages, malicious documents, spyware, and worms;
- Third, based on percentage figures for ransomware.

Construction

South America ranked sixth among regions based on the percentage of ICS computers on which malicious objects were blocked in the construction industry.

South America ranked as follows among regions based on its percentage figures for this industry:

- Third, based on the percentage of ICS computers on which threats from the internet and from email clients were blocked;
- Second, based on the percentage of ICS computers on which malicious scripts and phishing pages were blocked;
- Third, based on percentage figures for malicious documents.

Construction ranked as follows among industries in the region:

- First, based on the percentage of ICS computers on which threats from the internet were blocked;
- Second, based on percentage figures for threats on removable media.
- Third, based on percentage figures for threats from email clients;
- First, based on the percentage of ICS computers on which denylisted internet resources, viruses, and malware for AutoCAD were blocked;
- Second, based on percentage figures for both categories of miners;
- Third, based on percentage figures for malicious scripts and spyware.

Electric power

South America ranked sixth among regions based on the percentage of ICS computers on which malicious objects were blocked in the electric energy industry.

South America ranked as follows among regions, based on percentage figures for this industry:

- Third, based on the percentage of ICS computers on which threats from the internet and from email clients were blocked;
- Second, based on the percentage of ICS computers on which malicious scripts and phishing pages were blocked;
- Third, based on the percentage of ICS computers on which malicious documents were blocked.

The electric energy industry ranked as follows among industries in the region:

- Second, based on the percentage of ICS computers on which threats from the internet were blocked;
- Third, based on percentage figures for threats on removable media;

- Second, based on the percentage of ICS computers on which denylisted internet resources and ransomware were blocked;
- Third, based on percentage figures for viruses and malware for AutoCAD.

Engineering and ICS integrators

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

South America ranked as follows among regions, based on its percentage figures for this industry:

- Second, based on the percentage of ICS computers on which malicious documents were blocked;
- Third, based on the percentage figures for the following threat categories: malicious scripts and phishing pages, and web miners.

The engineering and ICS integrators industry ranks as follows among industries in the region:

- Third, based on the percentage of ICS computers on which threats from the internet were blocked;
- Second, based on the percentage of ICS computers on which malicious programs for AutoCAD were blocked;
- Third, based on percentage figures for denylisted internet resources and both categories of miners.

Oil and gas

South America ranked third among the five regions where the oil and gas industry is represented, based on the percentage of ICS computers on which malicious objects were blocked in that industry.

South America ranked as follows among regions, based on its percentage figures for the industry:

- First, based on the percentage of ICS computers on which threats from the internet and from email clients were blocked;
- First, based on the percentage of ICS computers on which malicious documents, malicious scripts and phishing pages, and web miners were blocked;
- Third, based on percentage figures for spyware and miners in the form of executable files.

The oil and gas industry ranked as follows among industries in the region:

- First, based on the percentage of ICS computers on which threats on removable media were blocked;
- First, based on percentage figures for both categories of miners and ransomware;
- Third, based on percentage figures for malicious documents and worms.

Manufacturing

South America ranked fifth among regions based on the percentage of ICS computers on which malicious objects were blocked in this industry.

South America ranked as follows among regions, based on percentage figures for this industry:

- Second, based on the percentage of ICS computers on which malicious documents were blocked.

Manufacturing ranked as follows among industries in the region:

- First, based on the percentage of ICS computers on which threats in network folders were 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 Q4 2025.

At the same time, the region ranked above 10th place for some threat sources and categories:

- Threats from network folders – sixth place;
- Threats from the internet – ninth place;
- Threats from email clients – ninth place;
- Malicious scripts and phishing pages – ninth place.

The region ranked 10th for malicious documents and viruses.

In North America (Canada), spam and phishing emails containing malicious scripts and miners in the form of executable files most likely reached computers on the OT network via a mail server on the corporate network that was open to external mail.

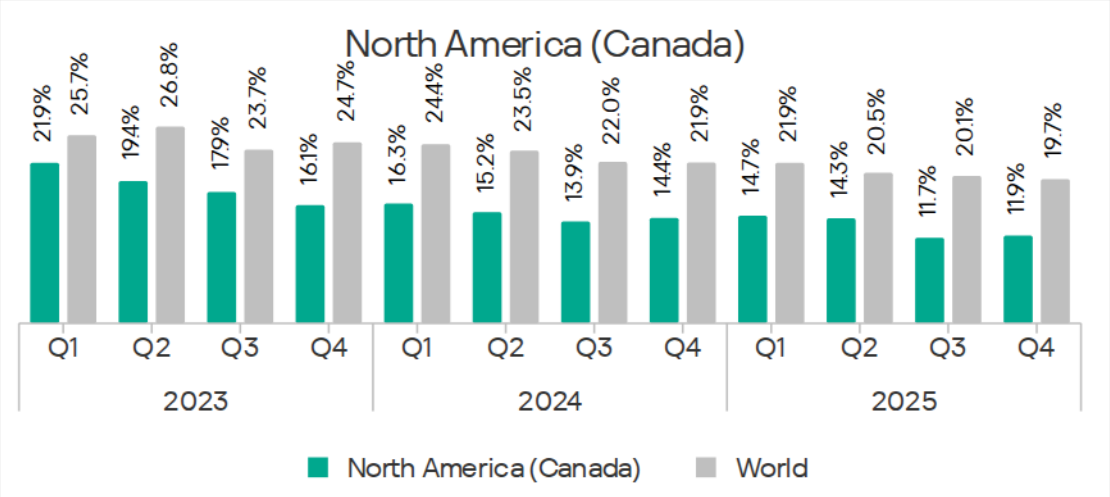
Relatively high percentage figures for threats distributed via email clients (phishing), malicious scripts, and both categories of miners may indicate that OT systems in the region are exposed to advanced categories of threat actors.

Statistics across all threats

North America (Canada) ranked 12th among regions based on the percentage of ICS computers on which malicious objects were blocked.

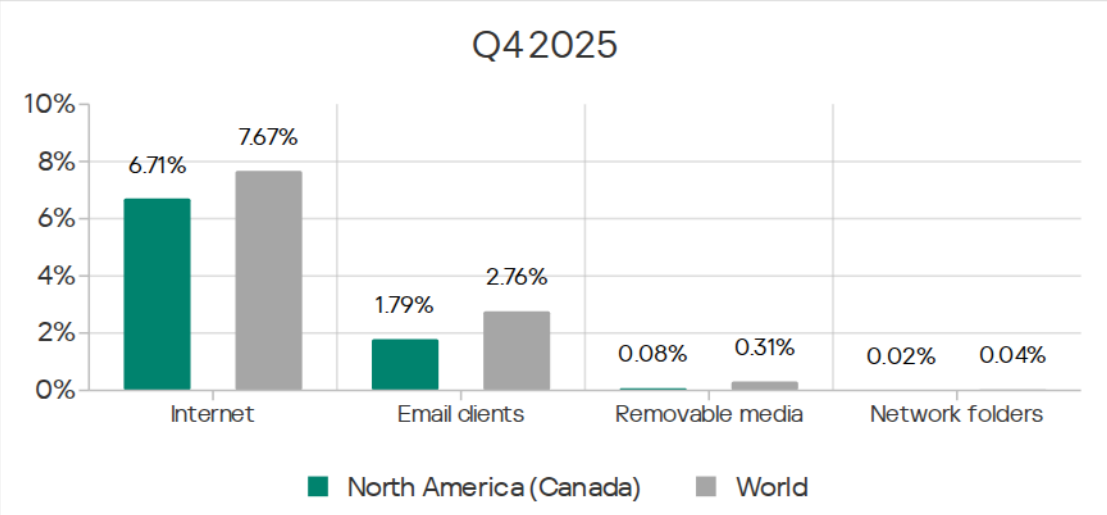
The percentage figure for the region has been gradually declining, with periodic fluctuations.

In Q4 2025, the percentage of ICS computers on which malicious objects were blocked in the region increased to 11.9%. This was significantly below the global average, but 1.4 times higher than in Northern Europe, which had the lowest value.



Threat sources

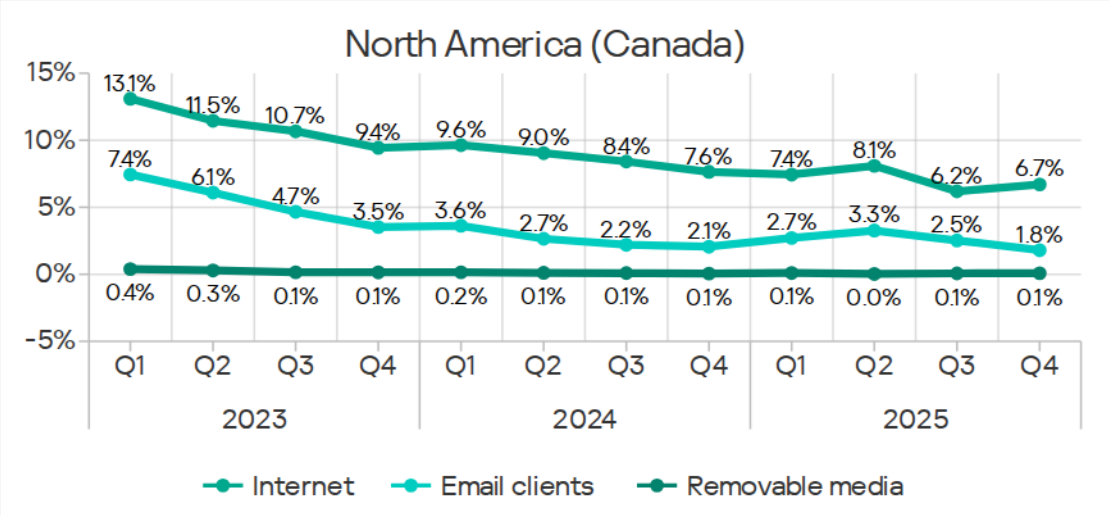
For all threat sources, the percentage figures for North America (Canada) were below the respective global averages.



Malicious objects in the region were distributed primarily via the internet and email.

The region ranked unexpectedly high in the percentage of ICS computers on which threats were blocked in network folders: North America (Canada) ranked sixth in that ranking. This was the region's highest position across all rankings, both by threat source and by threat category. The only industry in the region where such threats were observed is engineering and ICS integrators.

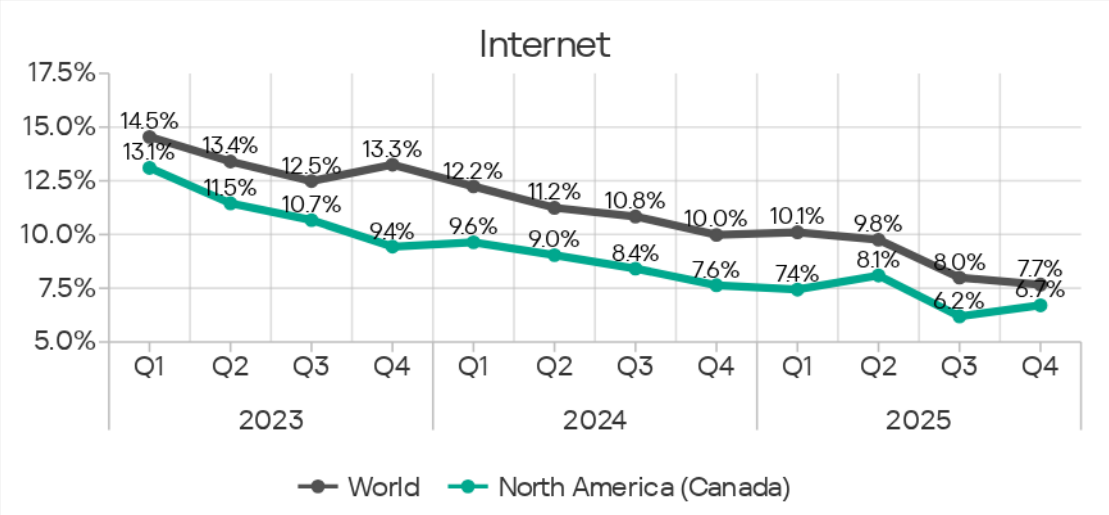
In Q4 2025, the percentage of ICS computers on which malicious objects were blocked increased in terms of threats from the internet and threats on removable media.



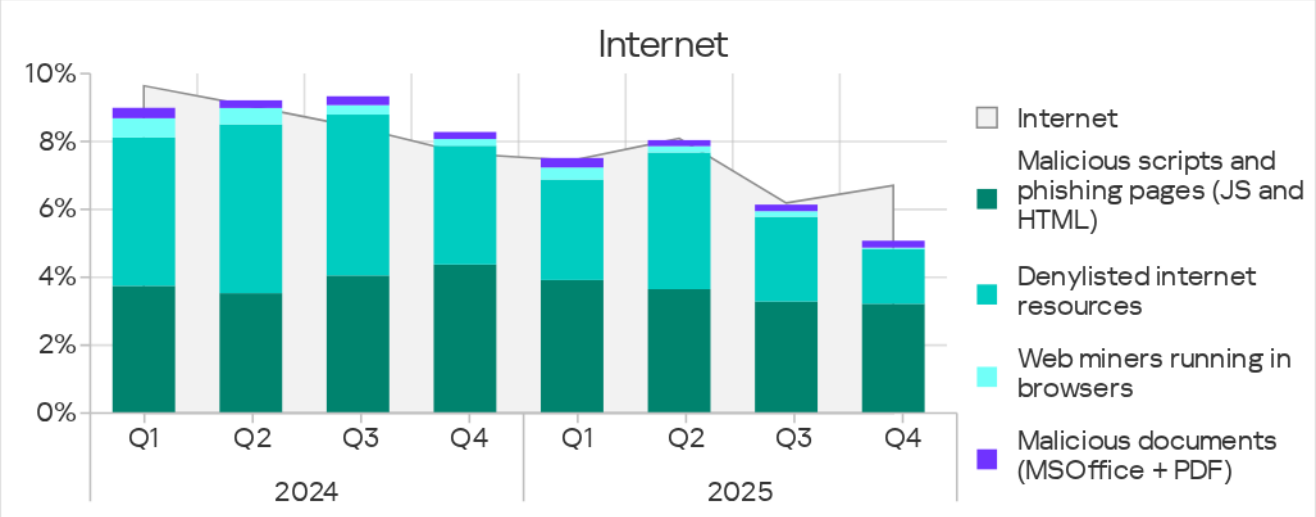
Internet

North America (Canada) ranked ninth, with 6.71%, based on the percentage of ICS computers on which threats from the internet were blocked. This is 1.7 times the lowest regional value, recorded in Northern Europe.

North America (Canada) was one of five regions where the percentage figure for internet threats increased in Q4 2025.



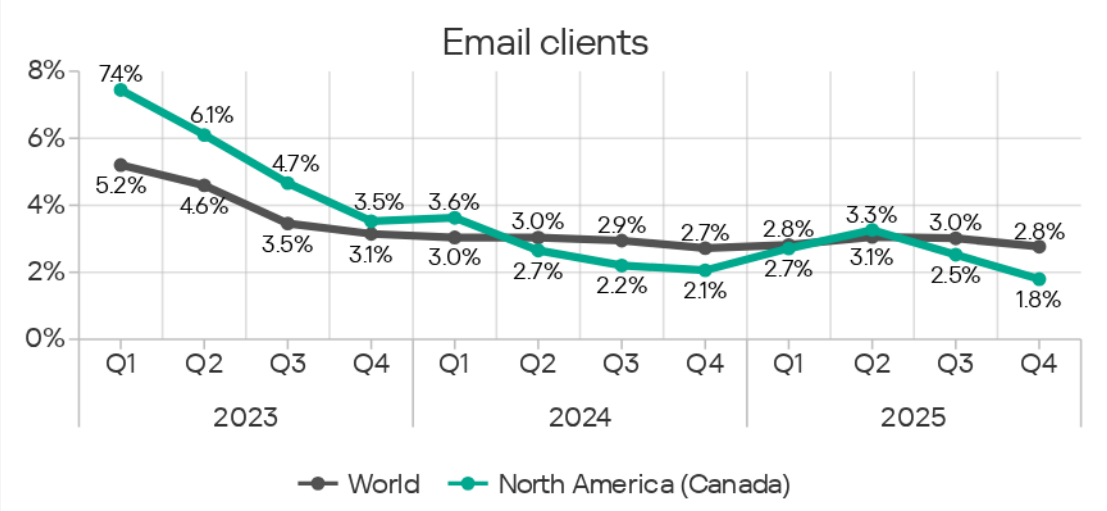
The main categories of internet threats blocked on ICS computers in the region were malicious scripts and phishing pages, and denylisted internet resources.



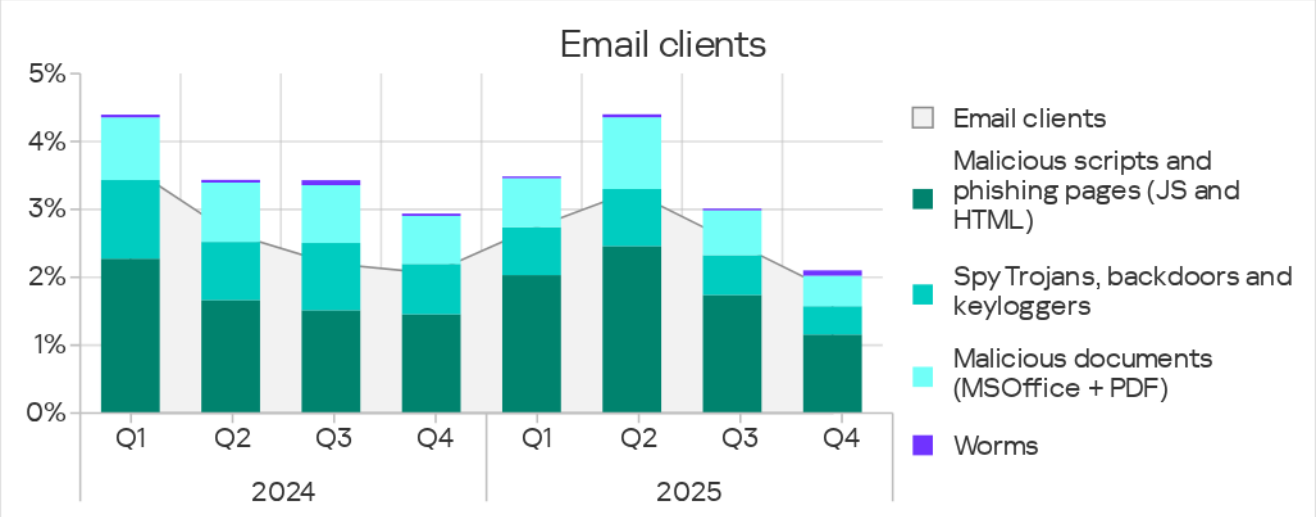
Email clients

North America (Canada) ranked ninth in Q4 2025 based on the percentage of ICS computers on which threats from email clients were blocked.

Over the quarter, the percentage figure for North America (Canada) decreased to 1.79%. This was 2.8 times higher than in Northern Europe, which ranked last.



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



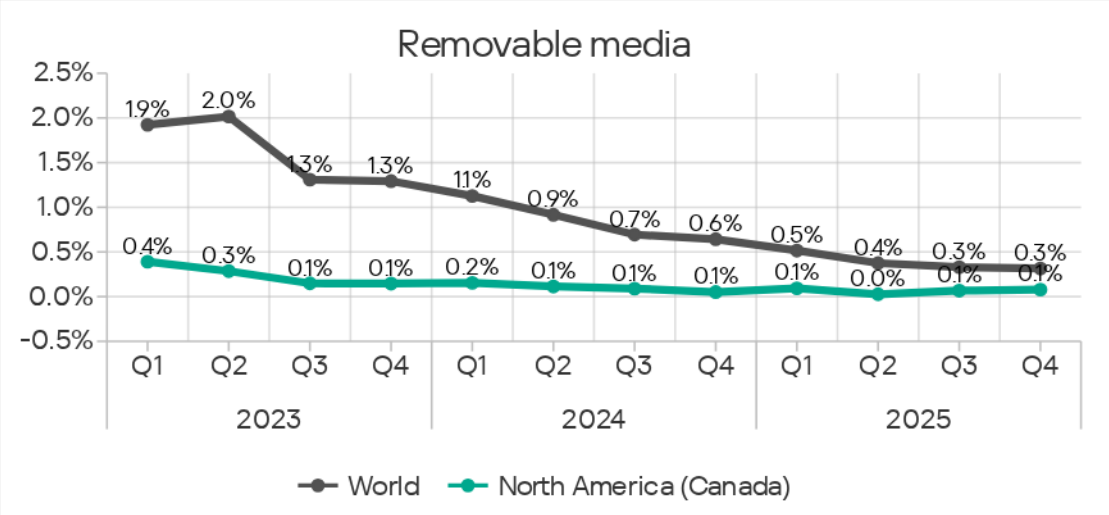
In Q4 2025, the percentage of ICS computers on which worms from email clients were blocked increased in all regions. This was due to the global phishing campaign known as “Curriculum-vitae-catalina”. In North America (Canada), the attack peaked in October.

North America (Canada), Western Europe, and Australia and New Zealand are the top three regions with the lowest quarter-over-quarter increases in the percentage figures for worms.

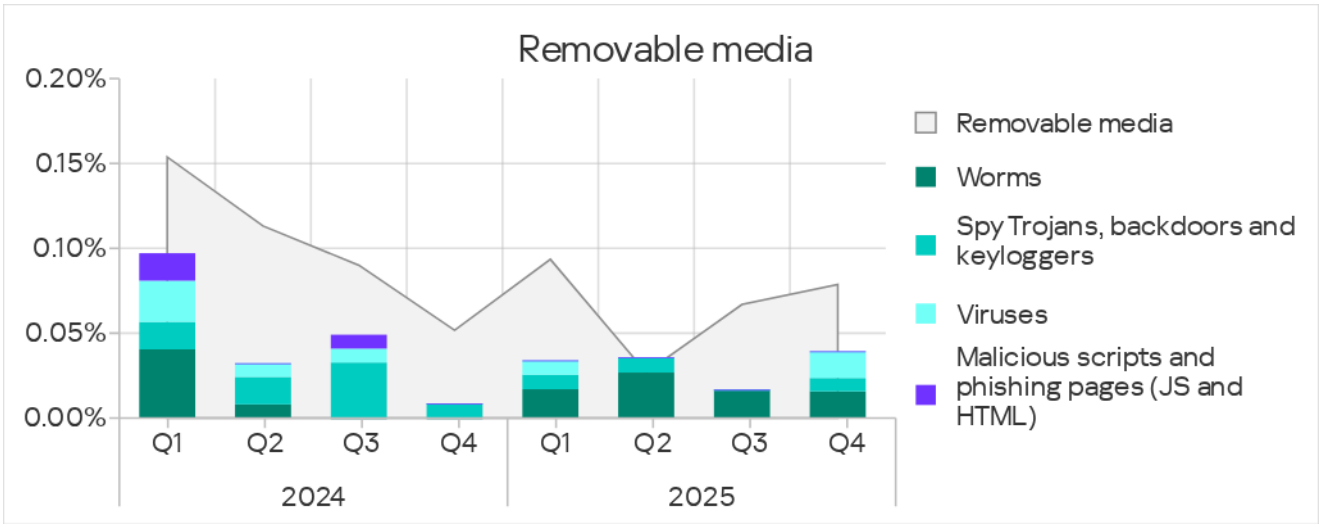
Removable media

North America (Canada) ranked 11th, with 0.08%, based on the percentage of ICS computers on which threats on removable media were blocked in Q4 2025. This was 1.7 times the value in the Australia and New Zealand region, which ranked last.

The figure has been fluctuating in the region. North America (Canada) was one of three regions where this percentage figure increased in Q4 2025.



The main categories of threats blocked on ICS computers when removable media were connected were worms and viruses. In Q4 2025, spyware and miners in the form of executable files were also blocked on removable media.



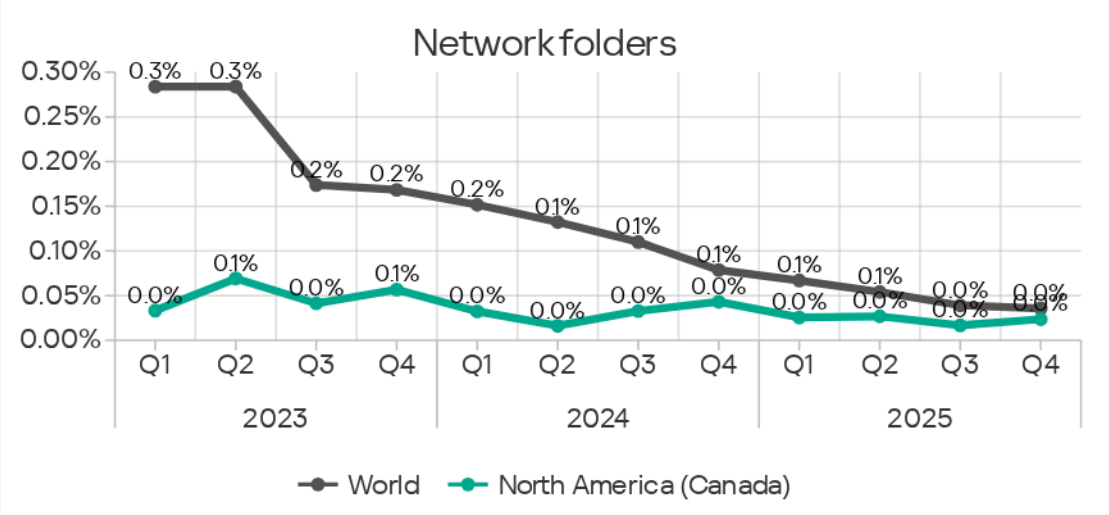
Network folders

North America (Canada) ranked sixth based on the percentage of ICS computers on which threats in network folders were blocked in Q4 2025. This was the region's highest position across all rankings – both by threat source and by threat category.

The region's percentage, 0.024%, was 3.4 times higher than in Northern Europe, which ranked last.

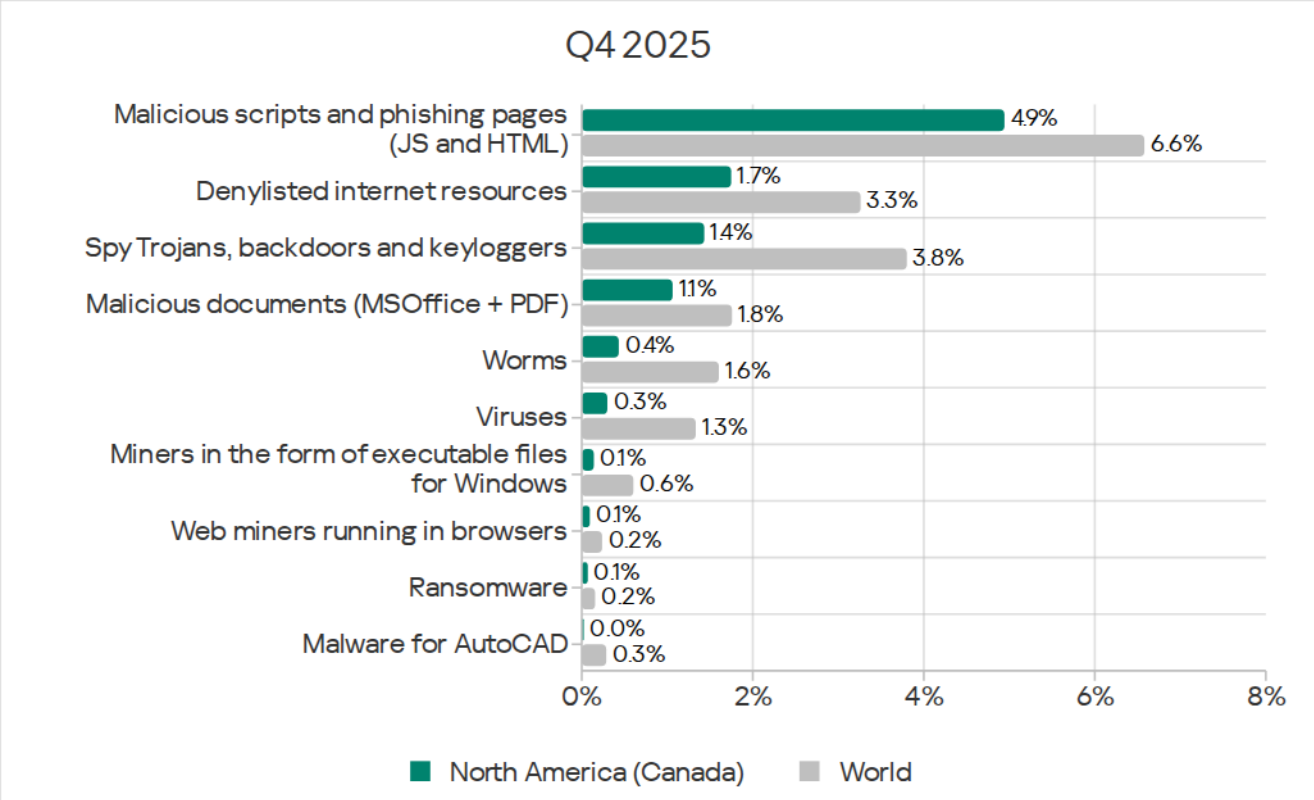
While the global average for threats from network folders has been steadily declining, the value in the region has been fluctuating. North America (Canada)

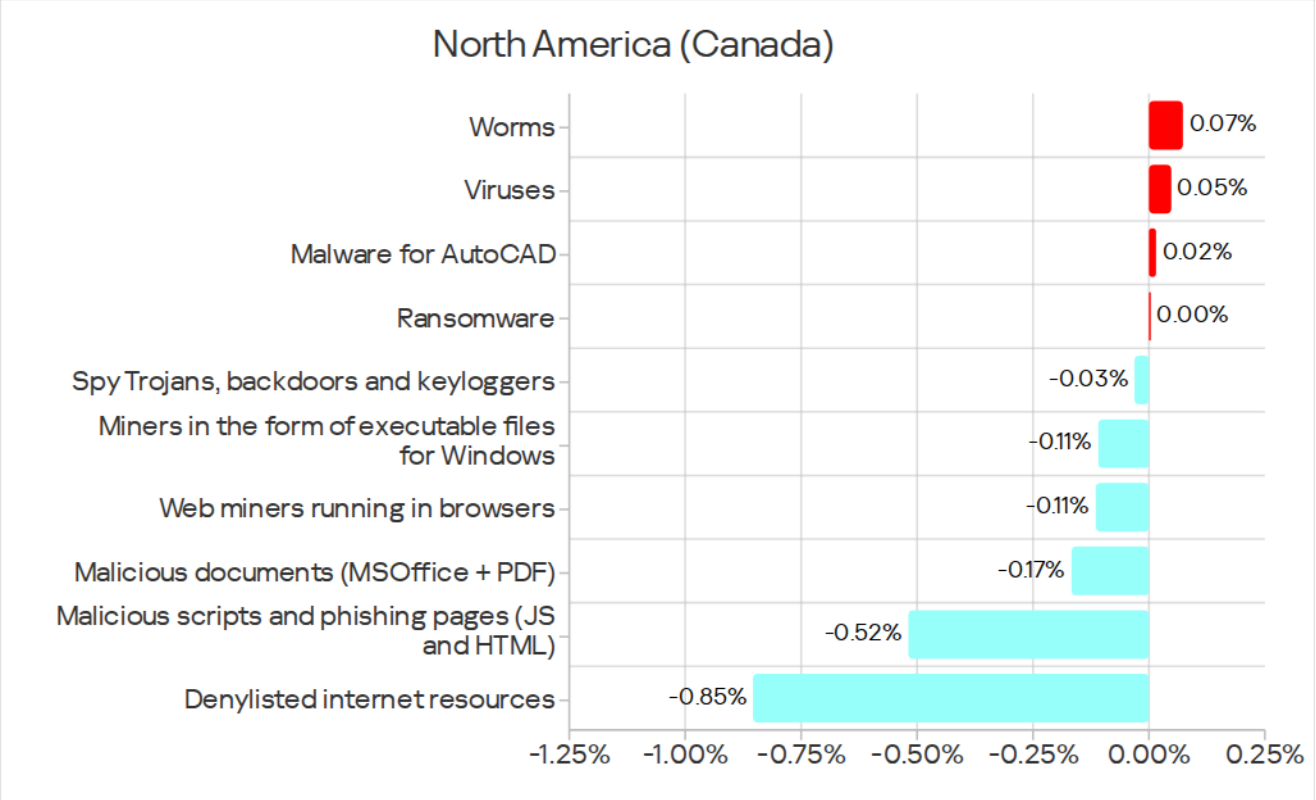
was one of four regions where the percentage figure for network folders increased in Q4 2025.



In Q4, spyware was the main threat distributed via network folders. Threats from network folders were blocked in the engineering and ICS integrators industry.

Threat categories





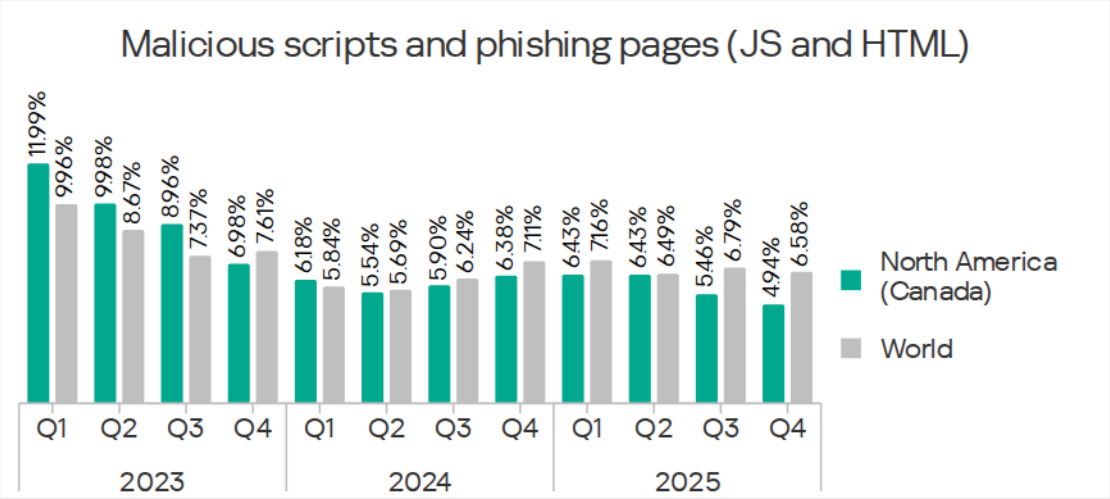
In North America (Canada), the percentage figures for all categories were below the respective global averages. In Q4 2025, the percentage figures for all threat categories decreased, except for worms, viruses, malware for AutoCAD, and ransomware.

North America (Canada)'s highest position in the regional rankings by threat category was ninth, in the ranking by the percentage of ICS computers on which malicious scripts and phishing pages were blocked.

Malicious scripts and phishing pages

North America (Canada) ranked ninth, with 4.94%, based on the percentage of ICS computers on which malicious scripts and phishing pages were blocked. This is 2.0 times higher than in Northern Europe, which had the lowest value of all regions.

The percentage of ICS computers in the region on which malicious scripts and phishing pages were blocked decreased for the second consecutive quarter.



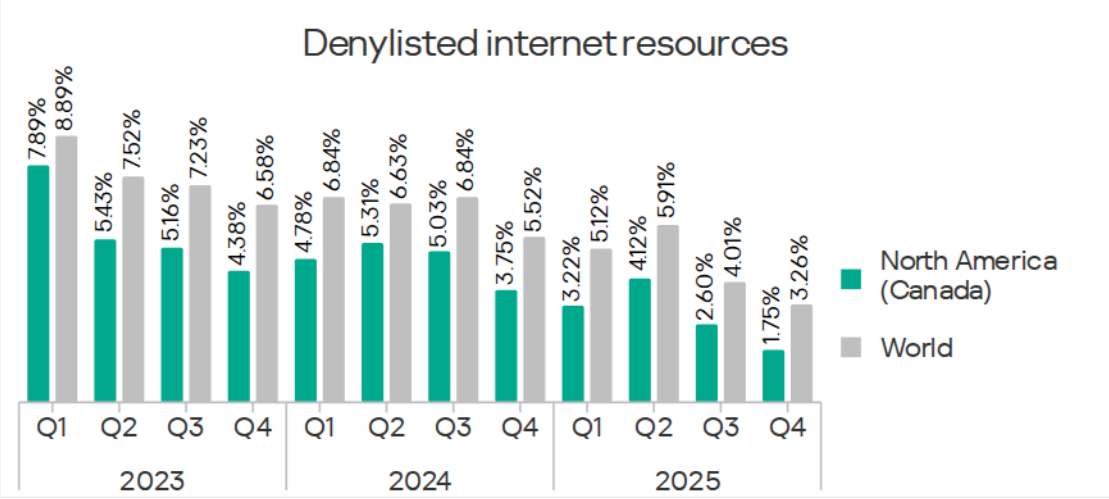
Malicious scripts and phishing pages were distributed both via the internet and via email.

Denylisted internet resources

North America (Canada) ranked 13th, with 1.75%, based on the percentage of ICS computers on which denylisted internet resources were blocked.

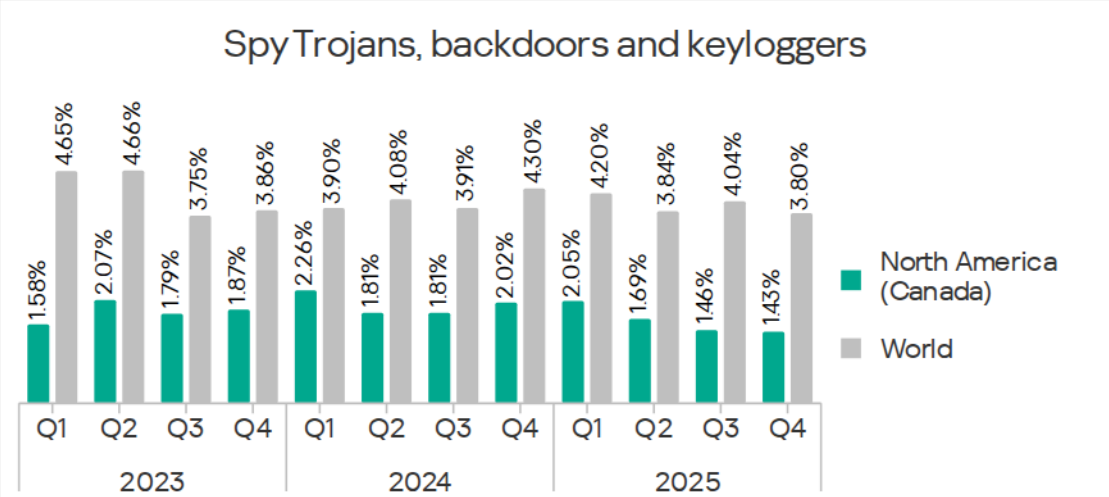
Denylisted internet resources ranked second (after malicious scripts) in North America (Canada) in the regional ranking of threat categories by the percentage of ICS computers on which they were blocked.

The percentage figure in the region decreased for the second consecutive quarter, reaching its lowest level in three years in Q4 2025.



Spyware

North America (Canada) ranked 12th among regions, with 1.43%, based on the percentage of ICS computers on which spyware was blocked. This was the third consecutive quarter that the percentage decreased in the region.

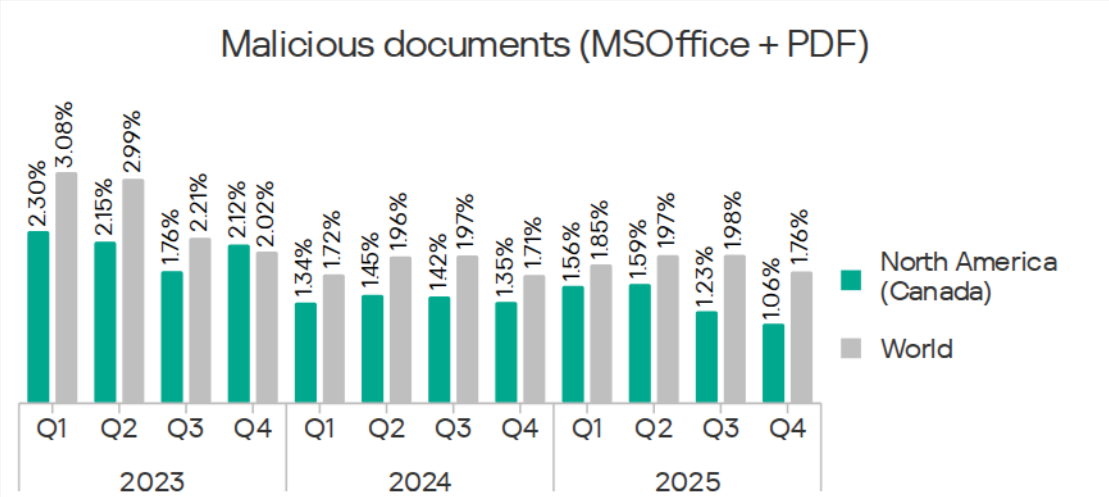


Spyware was blocked in the region across all threat sources, primarily in email clients.

Malicious documents

North America (Canada) ranked 10th among regions based on the percentage of ICS computers on which malicious documents were blocked. The region's percentage figure, 1.06%, was 2.3 times that of Northern Europe, which ranked last.

The percentage of ICS computers on which malicious documents were blocked has been fluctuating in the region. In Q4 2025, it decreased to its lowest value in three years.

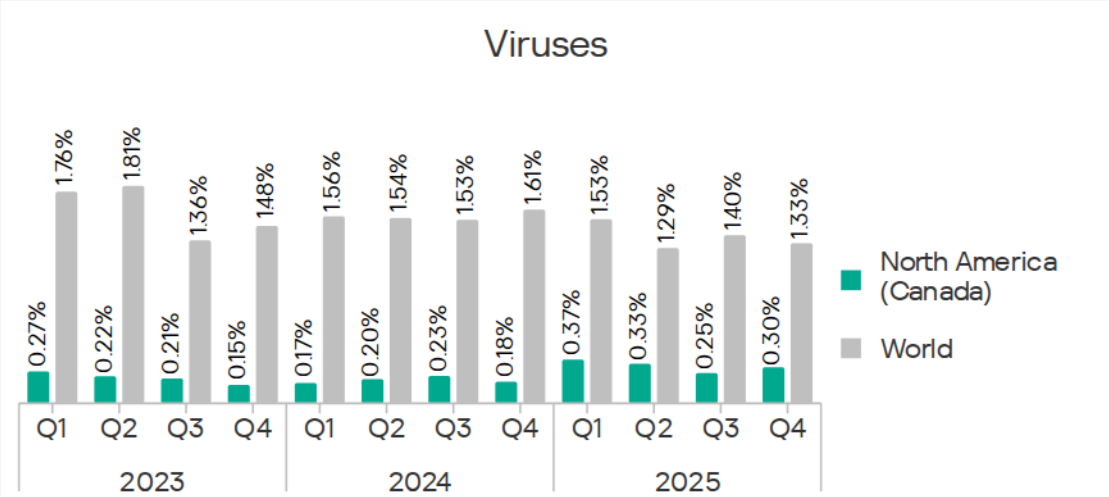


Malicious documents were distributed primarily via email.

Viruses

North America (Canada) ranked 10th, with 0.30%, based on the percentage of ICS computers on which viruses were blocked. This was significantly below the global average, but 2.0 times higher than in Western Europe, which ranked last.

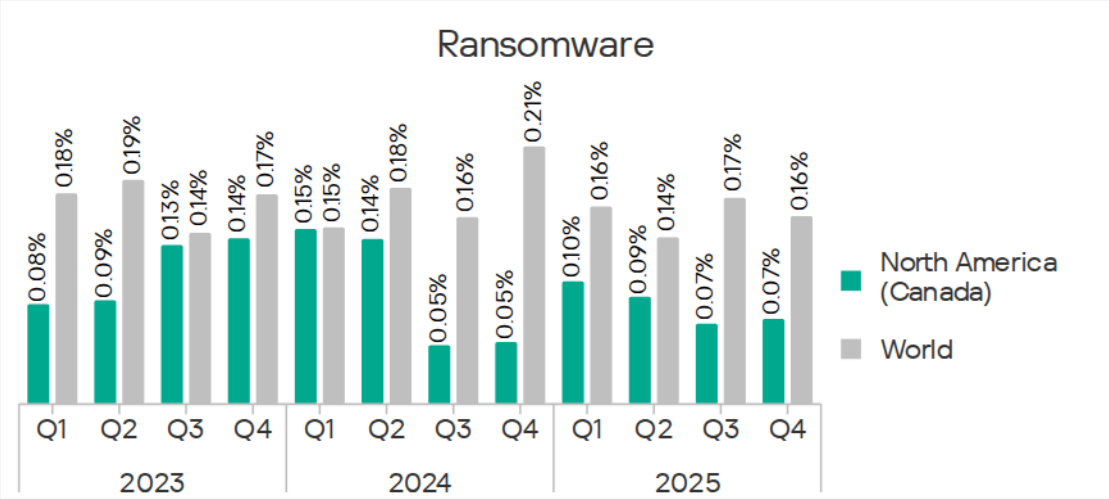
North America (Canada) was one of four regions in which the percentage figure for viruses increased over the quarter. It should be noted that the values were higher in 2025 than in the previous two years (with the exception of Q1 2023).



Ransomware

North America (Canada) ranked second to last (13th) at 0.07%, based on the percentage of ICS computers on which ransomware was blocked. This was 1.4 times the percentage in Northern Europe, which ranked last.

The percentage figure in the region has tended to fluctuate; it did not change in Q4 2025.

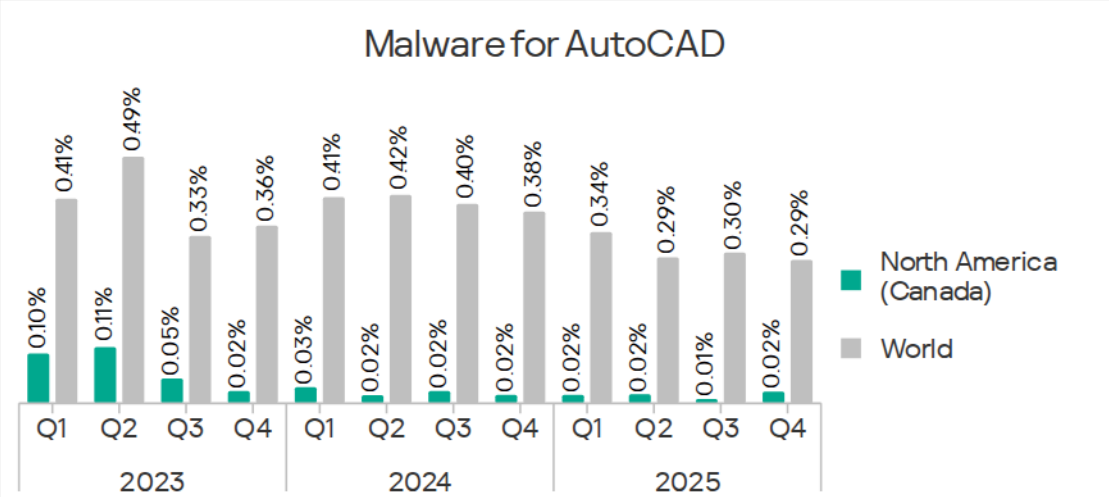


Malware for AutoCAD

North America (Canada) ranked 11th, with 0.02%, based on the percentage of ICS computers on which malware for AutoCAD was blocked. This was more than 14.5 times lower than the global average, but 2.0 times higher than in Northern Europe, which ranked last.

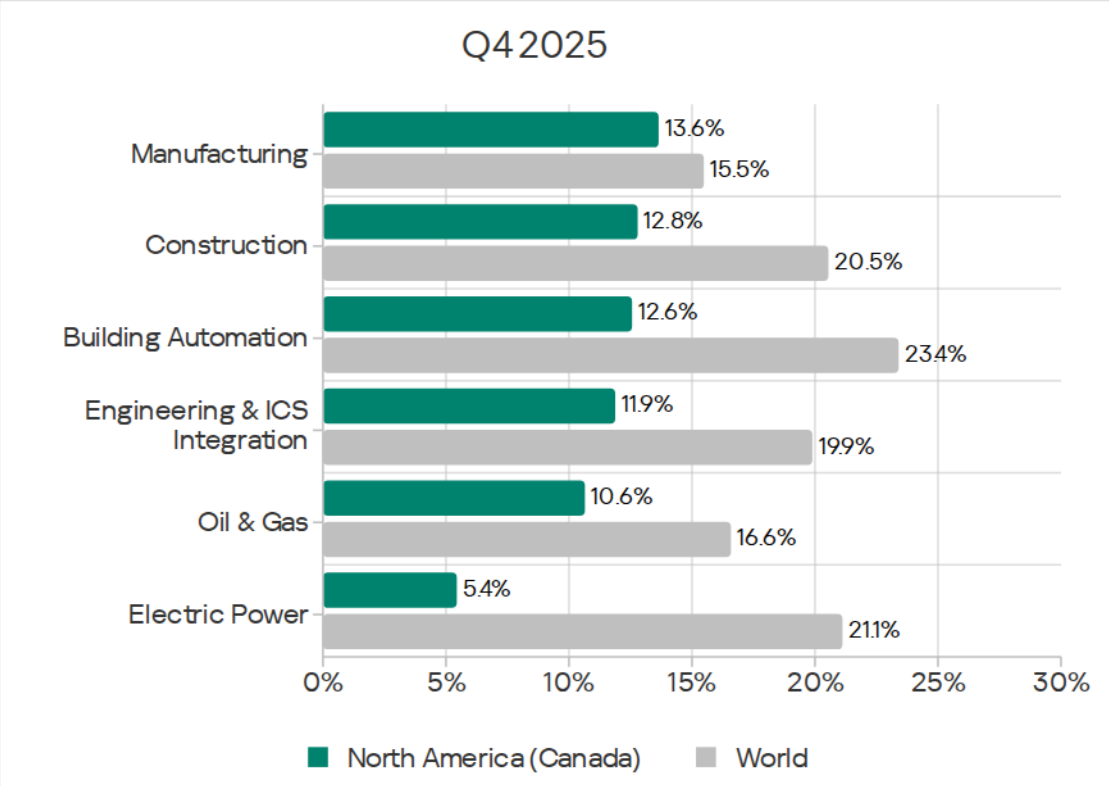
In Q4 2025, this threat was relevant only for one of the industries covered in this report – specifically, construction.

North America (Canada) is one of four regions where the percentage figures for malware for AutoCAD increased over the quarter.



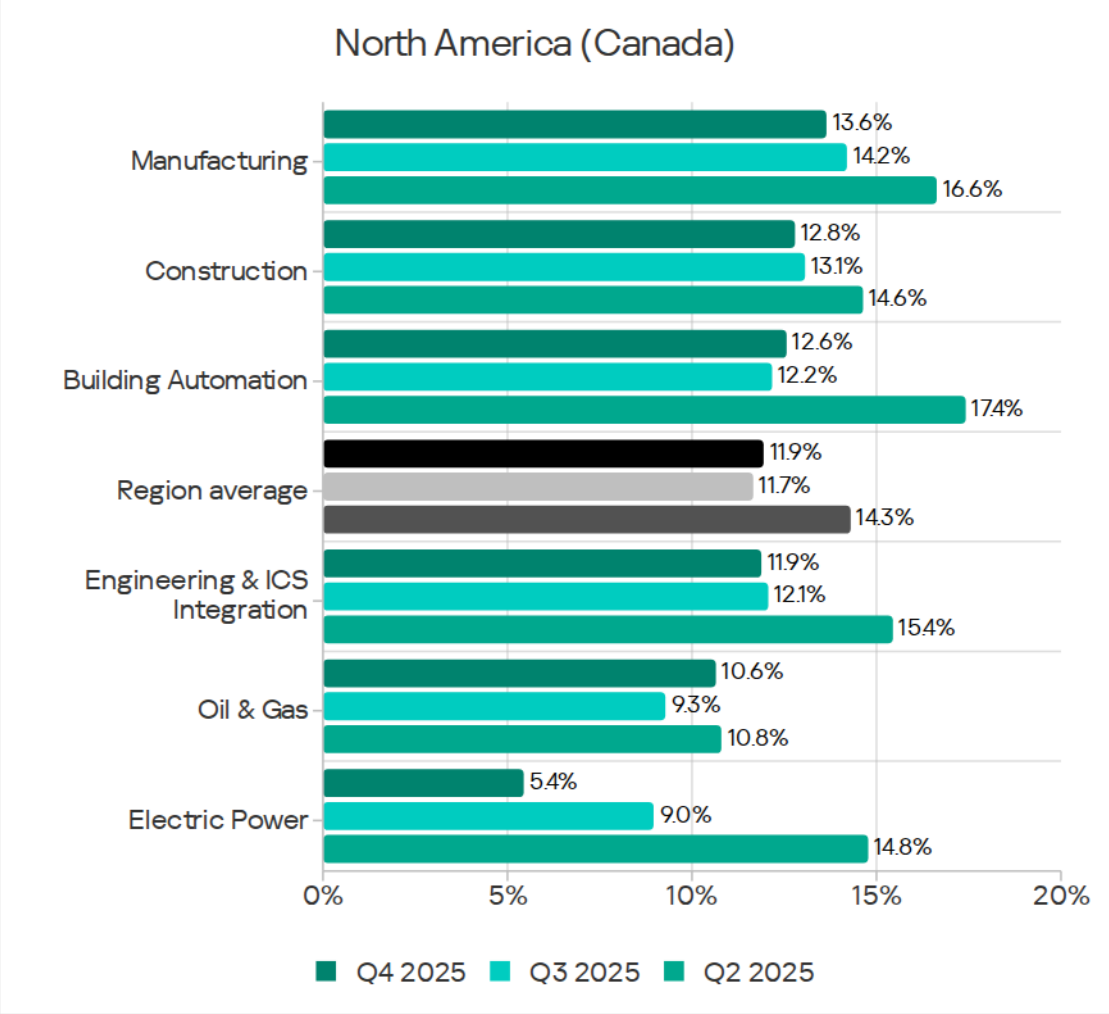
Industries

Among the industries covered in this report, the manufacturing sector had the largest percentage of ICS computers on which malicious objects were blocked in North America (Canada).

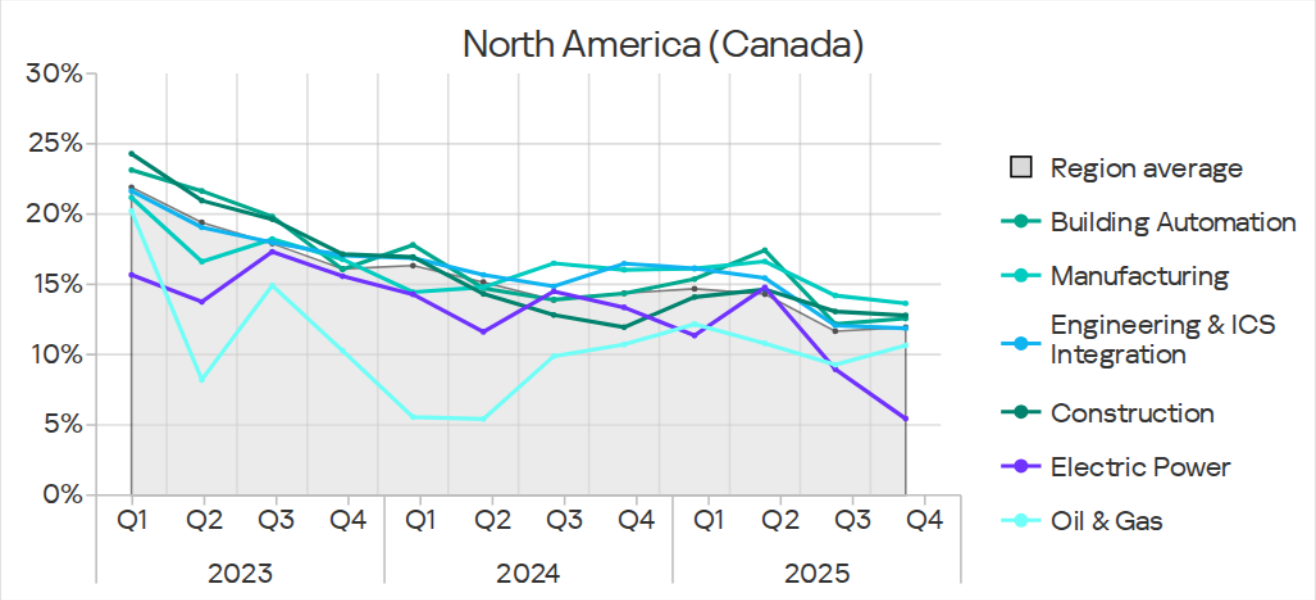


The percentage of ICS computers on which malicious objects were blocked decreased for the second consecutive quarter across all industries except oil and gas, and building automation. The most significant changes were in the

electric energy industry, where the figure decreased by a factor of 2.7 over the six-month period.



For all industries covered in this report, except electric energy, the percentage figures were close to those of the region as a whole. In the electric energy industry, the percentage values were below the overall regional values in most quarters.



Threat sources and malware categories in industries: 'hotspots'

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

Threat source indicators for industries in North America (Canada), Q4 2025

Industry / Threat source	Building Automation	Engineering & ICS Integration	Electric Power	Oil & Gas	Construction	Manufacturing	Category metric in region
Internet	5.76%	7.09%	2.59%	2.31%	7.92%	8.26%	6.71%
Email clients	3.28%	1.40%	0.78%	1.39%	2.25%	0.90%	1.79%
Removable media	0.20%	0.10%	—	—	0.05%	—	0.08%
Network folders	—	0.02%	—	—	—	—	0.02%
Industry metric in region	12.57%	11.88%	5.44%	10.65%	12.79%	13.64%	

Threat category indicators for industries in North America (Canada), Q4 2025

Industry / Threat type	Building Automation	Engineering & ICS Integration	Electric Power	Oil & Gas	Construction	Manufacturing	Category metric in region
Denylisted internet resources	1.36%	1.94%	1.04%	0.93%	1.55%	2.87%	1.75%
Malicious scripts and phishing pages (JS and HTML)	6.08%	4.74%	1.30%	2.31%	5.90%	3.95%	4.94%
Malicious documents (MSOffice + PDF)	2.00%	0.80%	—	0.93%	1.45%	0.54%	1.06%
Spy Trojans, backdoors and keyloggers	2.24%	1.33%	1.04%	0.93%	1.08%	1.26%	1.43%
Ransomware	0.16%	0.07%	—	—	—	0.18%	0.07%
Miners in the form of executable files for Windows	0.28%	0.15%	—	—	0.14%	—	0.14%
Web miners running in browsers	0.24%	0.10%	—	—	0.05%	—	0.09%
Malware for AutoCAD	—	—	—	—	0.05%	—	0.02%
Worms	0.80%	0.34%	0.26%	0.46%	0.28%	—	0.43%
Viruses	0.32%	0.12%	—	0.46%	0.52%	0.54%	0.30%
Industry metric in region	12.57%	11.88%	5.44%	10.65%	12.79%	13.64%	

Manufacturing

North America (Canada) ranked sixth among regions based on the percentage of ICS computers on which malicious objects were blocked in the industry. This was the region's highest ranking based on the percentage of computers attacked in any industry.

North America (Canada) ranks third among regions by the percentage of ICS computers in the industry on which denylisted internet resources are blocked.

Manufacturing ranked as follows among industries in the region:

- First, based on the percentage of ICS computers on which threats from the internet were blocked;
- First, based on the percentage of ICS computers on which denylisted internet resources, viruses, and ransomware were blocked;
- Third, based on percentage figures for spyware.

Construction

North America (Canada) ranked 12th among regions based on the percentage of ICS computers on which malicious objects were blocked in this industry.

Construction ranked as follows among industries in the region:

- Second, based on the percentage of ICS computers on which threats from the internet and from email clients were blocked;
- Third, based on percentage figures for threats on removable media;
- First, based on the percentage of ICS computers on which malware for AutoCAD was blocked (this was the only industry in the region where such threats were blocked);
- Second, based on the percentage of ICS computers on which malicious scripts and phishing pages, malicious documents, and viruses were blocked;
- Third, based on percentage values for the following threat categories: denylisted internet resources, worms, and miners of both types.

Building automation

North America (Canada) ranked 13th among regions based on the percentage of ICS computers on which malicious objects were blocked in this industry.

Building automation ranked as follows among industries in the region:

- First, based on the percentage of ICS computers on which threats were blocked in email clients and when connecting removable media;
- First, based on the percentage of ICS computers on which malicious scripts and phishing pages, malicious documents, spyware, worms, and miners of both categories were blocked;
- Second, based on percentage figures for ransomware;
- Third, based on percentage figures for viruses.

Engineering and ICS integrators

North America (Canada) ranked 13th among regions based on the percentage of ICS computers on which malicious objects were blocked in this industry.

The engineering and ICS integrators industry ranked as follows among industries in the region:

- First, based on percentage figures for threats in network folders (this was the only industry in the region where such threats were blocked);
- Second, based on percentage figures for threats on removable media;
- Third, based on the percentage of ICS computers on which threats from the internet and from email clients were blocked;
- Second, based on percentage figures for the following threat categories: denylisted internet resources, spyware, worms, and miners of both categories;
- Third, based on the percentage of ICS computers on which malicious scripts and phishing pages, malicious documents, and ransomware were blocked.

Electric energy industry

North America (Canada) ranked last (14th) among regions based on the percentage of ICS computers on which malicious objects were blocked in this industry.

Methodology used to prepare statistics

This report presents the results of analyzing statistics obtained with the help of Kaspersky Security Network (KSN). The data was received from KSN users who consented to its anonymous sharing and processing for the purposes described in the KSN Agreement for the Kaspersky product installed on their computer.

The benefits of joining KSN for our customers include faster response to previously unknown threats and a general improvement in the quality of detection by their Kaspersky installation achieved by connecting to a cloud-based repository of malware data that is not transferable to the customer in its entirety by nature of its size and the amount of resources that it uses.

Data shared by the user contains only the data types and categories described in the appropriate KSN Agreement. This data helps to a significant extent in analyzing the threat landscape and serves as a prerequisite for detecting new threats including targeted attacks and APTs[1].

Statistical data presented in the report was obtained from ICS computers that were protected with Kaspersky products and which Kaspersky ICS CERT categorized as enterprise OT infrastructure. This group includes Windows computers that serve one or several of the following purposes:

- Supervisory control and data acquisition (SCADA) servers
- Building automation servers
- Data storage (Historian) servers
- Data gateways (OPC)
- Stationary workstations of engineers and operators
- Mobile workstations of engineers and operators
- Human machine interface (HMI)
- Computers used to manage technological and building automation networks
- Computers of ICS/PLC programmers

Computers that share statistics with us belong to organizations from various industries. The most common are the chemical industry, metallurgy, ICS design and integration, oil and gas, energy, transport and logistics, the food industry, light industry, pharmaceuticals. This also includes systems from engineering and integration firms that work with enterprises in a variety of industries,

[1] We recommend that organizations subject to restrictions on sharing any data outside the corporate perimeter consider using Kaspersky Private Security Network.

as well as building management systems, physical security, and biometric data processing.

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

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

Kaspersky ICS CERT ics-cert@kaspersky.com