Kaspersky ICS CERT

kaspersky

Threat landscape for industrial automation systems

Australia and New Zealand. Q3 2025

23.12.2025

Version 1.0

© 2025 AO KASPERSKY LAB

Australia and New Zealand

Key cybersecurity issues in the region

The cybersecurity situation in Australia and New Zealand is among the most favorable across all regions. The region ranked 11th in Q3 2025 based on the percentage of ICS computers on which malicious objects were blocked.

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

- Seventh place in malicious scripts and phishing pages.
- Seventh place in malicious documents.
- Seventh place in threats from email clients.
- Seventh place in threats in network folders.

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.

Threat actors send malicious documents in phishing messages and use them in initial infection attacks. Malicious documents usually contain exploits, malicious macros, and malicious links.

In Q3 2025, Australia and New Zealand rank first in growth of the email client threat indicator. This is one of the four regions that saw an increased percentage of ICS computers on which malicious documents are blocked.

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

In Q3 2025, the Australia and New Zealand region saw growth of the indicator for threats from network folders, and this growth puts Australia and New Zealand in second place among those four regions in which this indicator increased. There was also an increase in the percentage of ICS computers on which threats on removable media were blocked.

Country specifics

In Australia, the percentage of ICS computers on which threats from email clients were blocked was 2.8 times higher than in New Zealand.

© 2025 AO KASPERSKY LAB

The figures of the region for threats on removable media and in network folders are primarily due to the situation in Australia, as the indicators for these threat sources are negligible in New Zealand.

The percentage of ICS computers on which viruses are blocked in Q3 2025 increased in both countries of the region, while it increased by a factor of 3.0 in New Zealand.

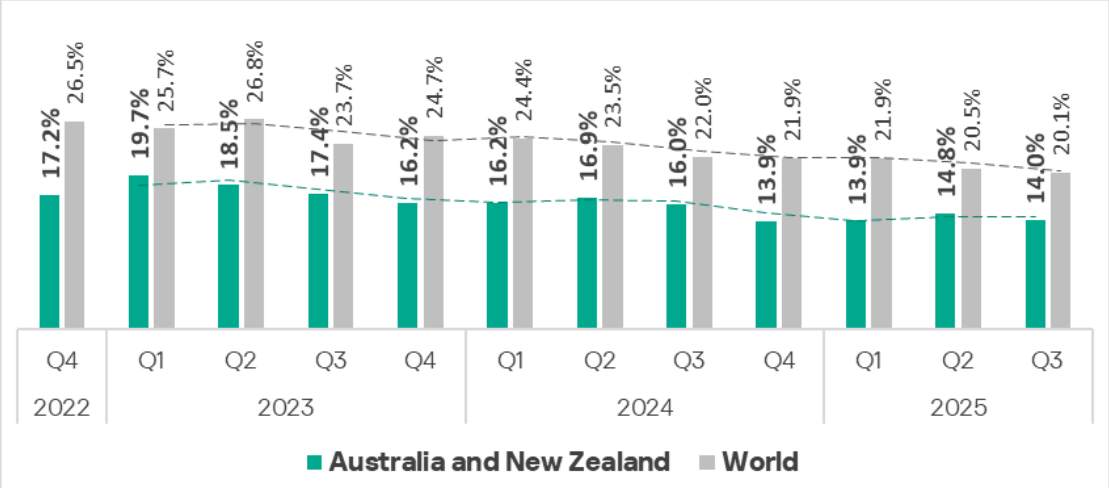
Industries

In the regional rankings based on the percentage of ICS computers on which malicious objects were blocked in various industries, Australia and New Zealand were only able to reach 11th place.

However, in two industries the region made it into the top 3 based on the indicators for threats from email clients (in the construction industry) and for the categories of threats that are propagated predominately through email, such as malicious documents, malicious scripts, and phishing pages (in the electrical energy industry).

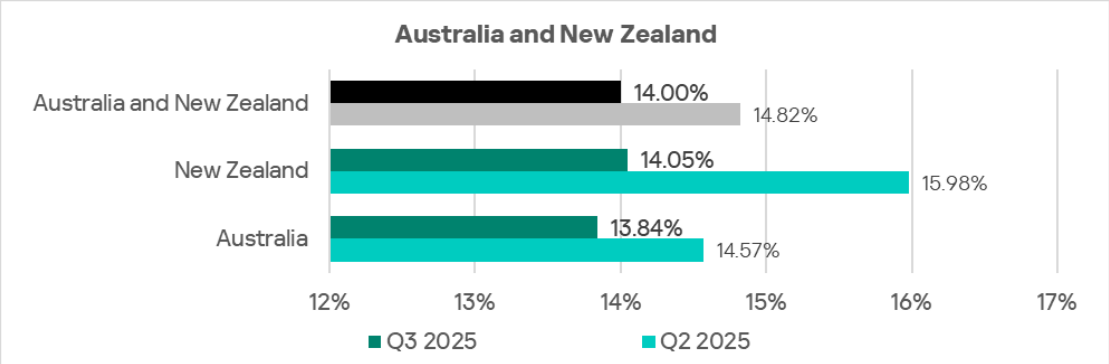
Statistics across all threats

The Australia and New Zealand region ranks 11th among regions based on the percentage of ICS computers on which malicious objects were blocked. Its percentage value of 14.0% is significantly lower than the global average, but 1.5 times higher than that of Northern Europe, which ranks last.



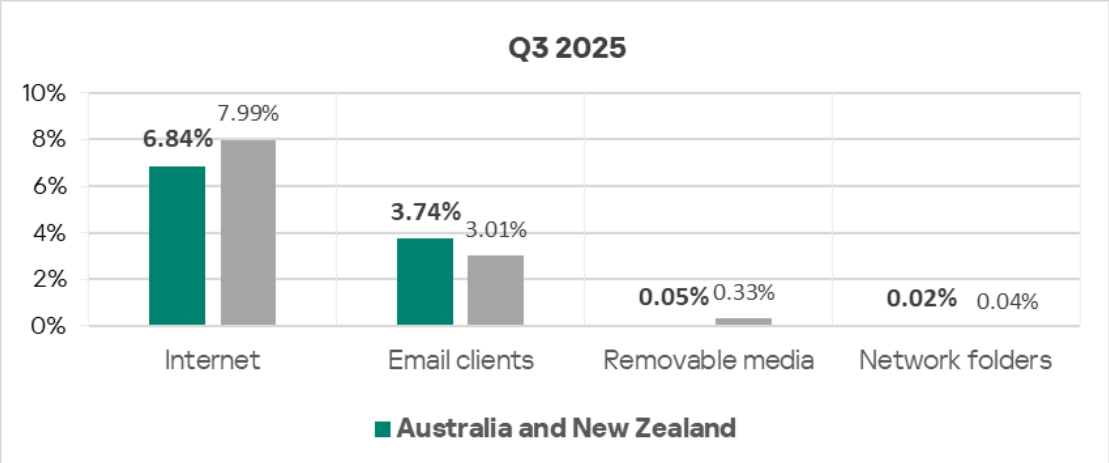
The region's overall figure largely depends on the situation in Australia. The percentage of ICS computers on which malicious objects were blocked in Australia was lower than in New Zealand. This indicator noticeably decreased in both countries.

© 2025 AO KASPERSKY LAB



Threat sources

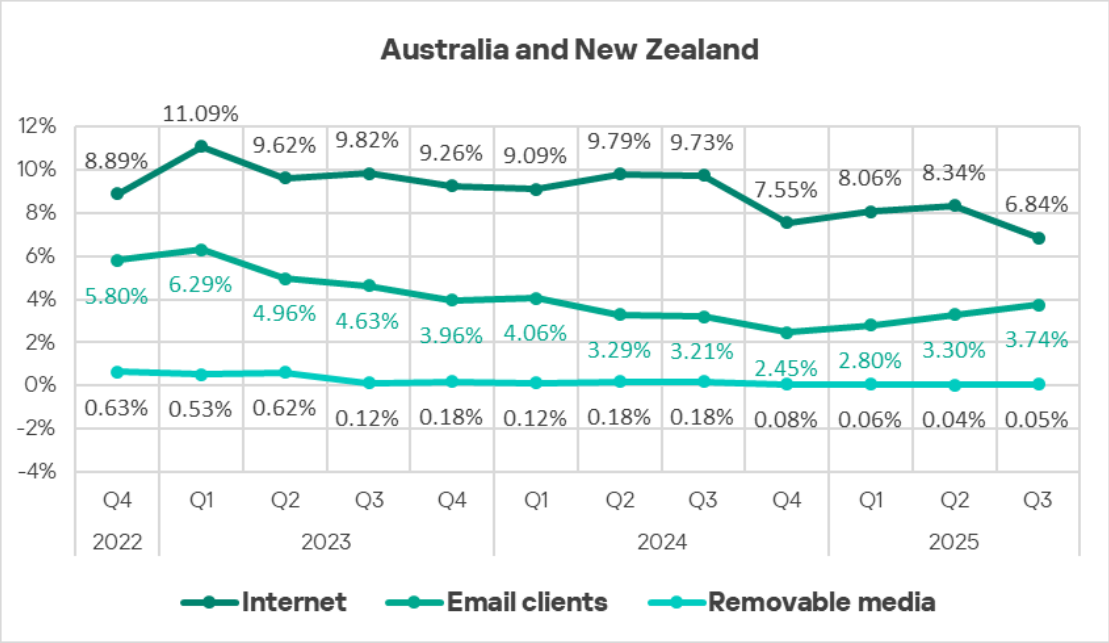
In Australia and New Zealand, percentage figures for all threat sources, except email clients, are lower than the global averages. The percentage of ICS computers in the region on which threats from email clients were blocked is 1.2 times higher than the global average.



Malicious objects in the region spread primarily via the internet and email. The Australia and New Zealand region ranks last among all regions based on the percentage of ICS computers on which threats from removable media were blocked.

In Q3 2025, the percentage of ICS computers on which malicious objects were blocked in the region increased for all sources of threats except the internet. The Australia and New Zealand region leads in growth of the email client threat indicator while it takes second place in growth of the indicator for threats from network folders.

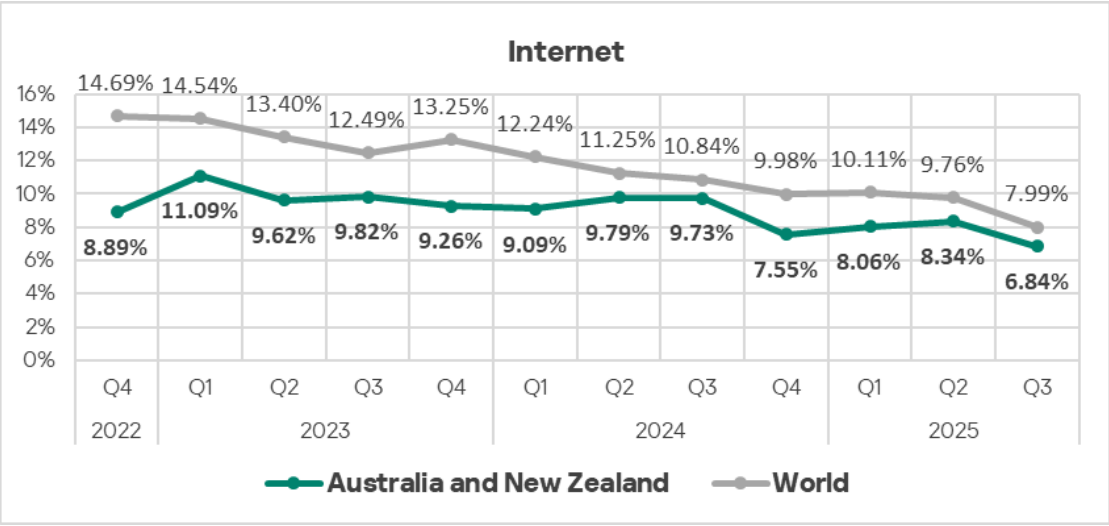
© 2025 AO KASPERSKY LAB



Internet

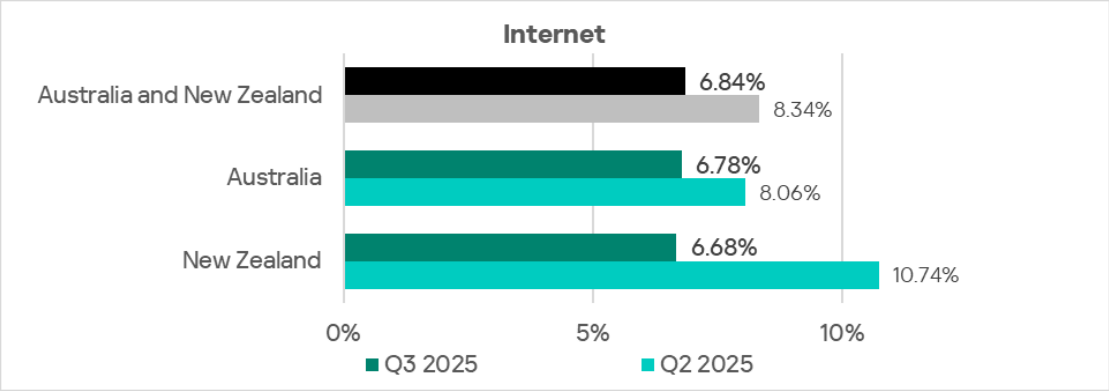
Australia and New Zealand ranks ninth, with 6.84%, based on the percentage of ICS computers on which internet threats were blocked. This is 1.5 times higher than Northern Europe, which ranks last in this category.

In Australia and New Zealand, like in all other regions, the indicator for the quarter decreased.

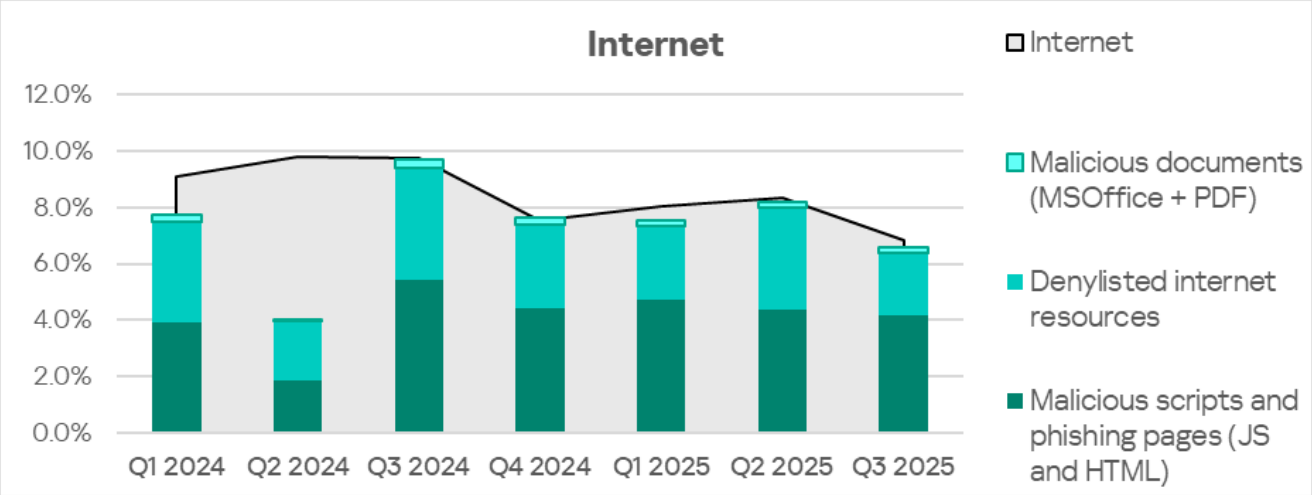


The percentage of ICS computers on which internet threats were blocked during the quarter decreased in both countries of the region. This indicator is higher in Australia than in New Zealand.

© 2025 AO KASPERSKY LAB



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



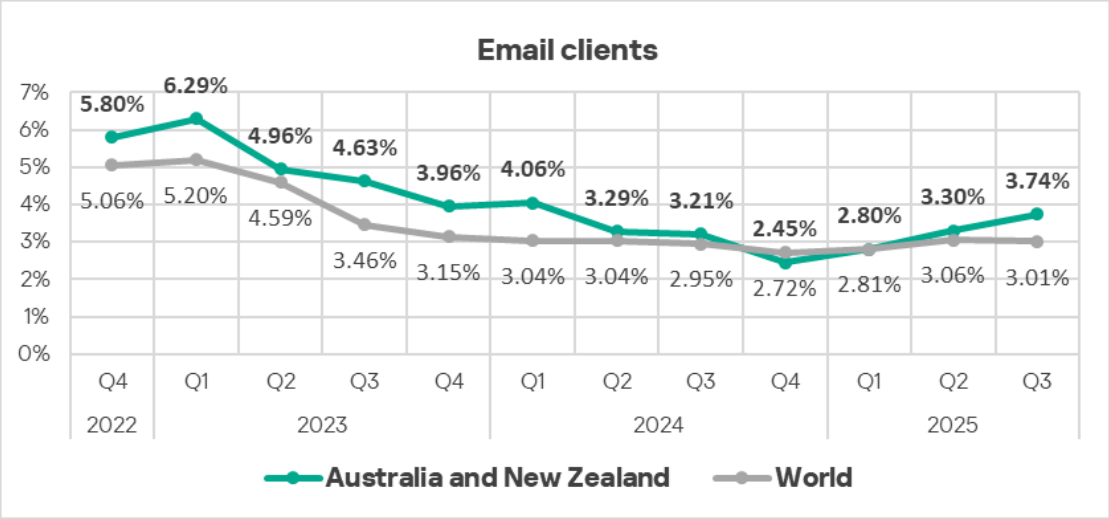
Email clients

In Q3 2025, the Australia and New Zealand region ranked seventh 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.

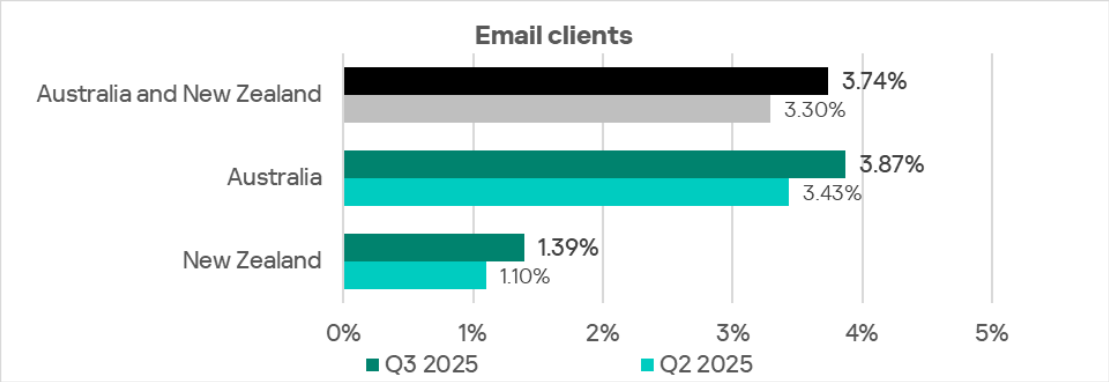
The indicator in Australia and New Zealand (3.74%) is 4.8 times higher than in Russia, which is the lowest-ranked region.

The email clients indicator in the region has been growing for three consecutive quarters. In Q3 2025, Australia and New Zealand occupies first place among regions for this growth.

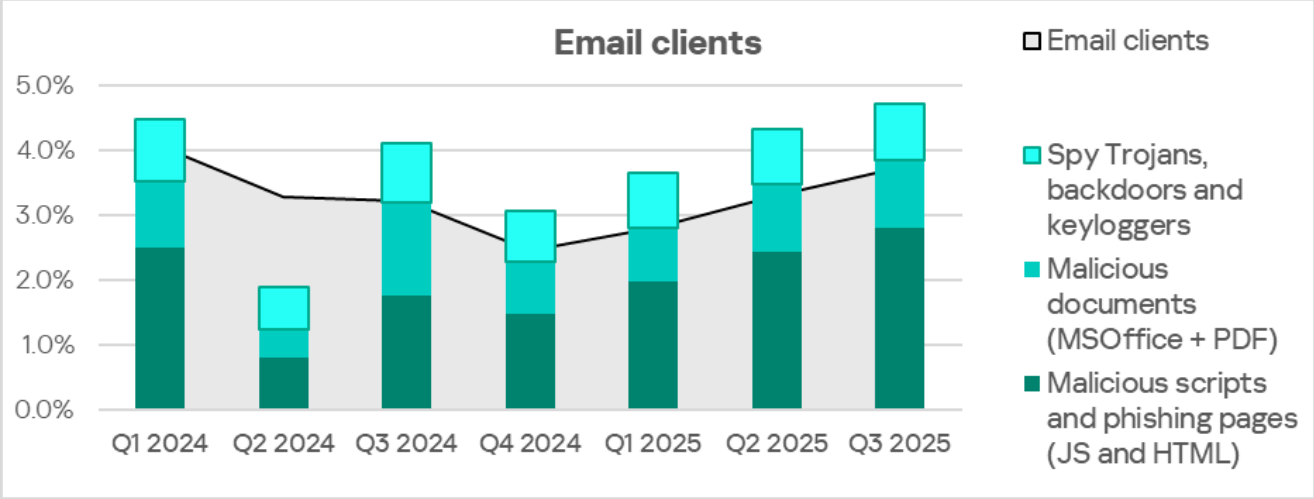
© 2025 AO KASPERSKY LAB



The percentage of ICS computers on which email client threats are blocked are 2.8 times higher in Australia than in New Zealand.



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

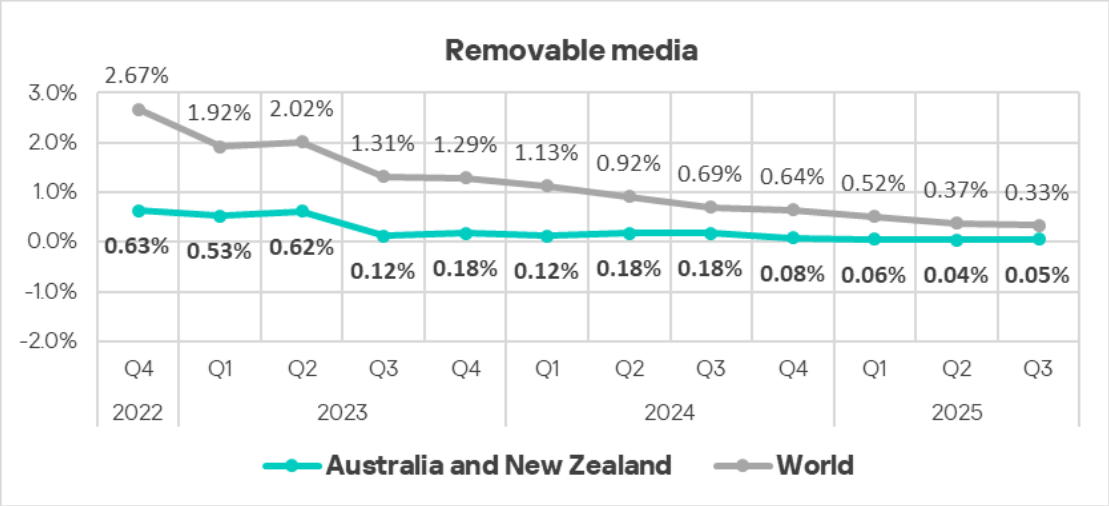


© 2025 AO KASPERSKY LAB

Removable media

Based on the percentage of ICS computers on which threats on removable media were blocked in Q3 2025, the Australia and New Zealand region ranked 14th with the lowest indicator of all regions (0.05%).

The quarterly indicator has showed a stable decrease since Q2 2023. In Q3 2025, Australia and New Zealand was one of the four regions that showed a quarterly growth in the percentage of ICS computers on which threats on removable media were blocked.



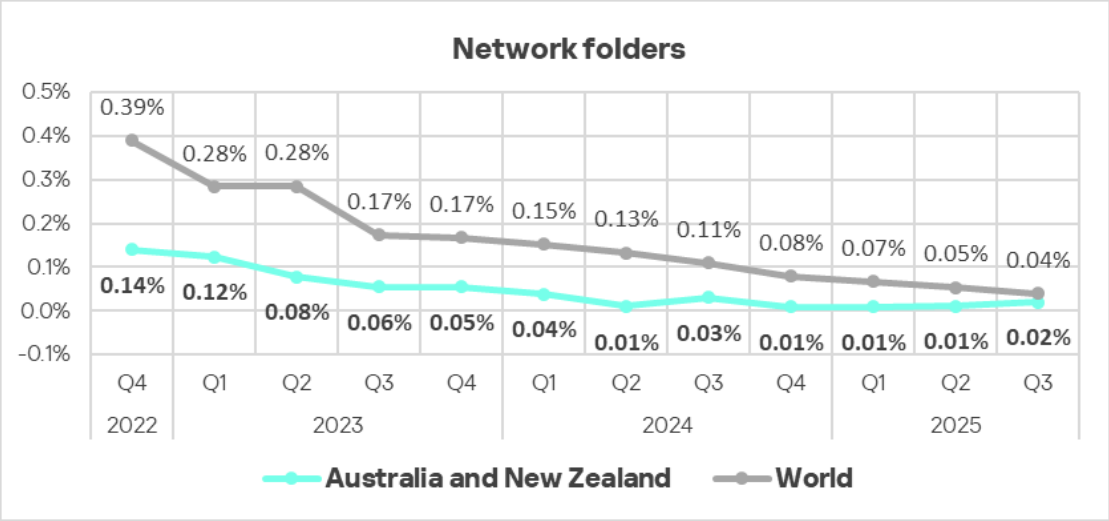
Threats on removable media in the region are blocked predominately in Australia, with the country indicator matching the regional indicator as a whole.

Network folders

Based on the percentage of ICS computers on which threats in network folders were blocked, the Australia and New Zealand region ranked seventh in Q3 2025 at 0.020%. This is the region's highest position in the rankings, both by sources and by threat categories.

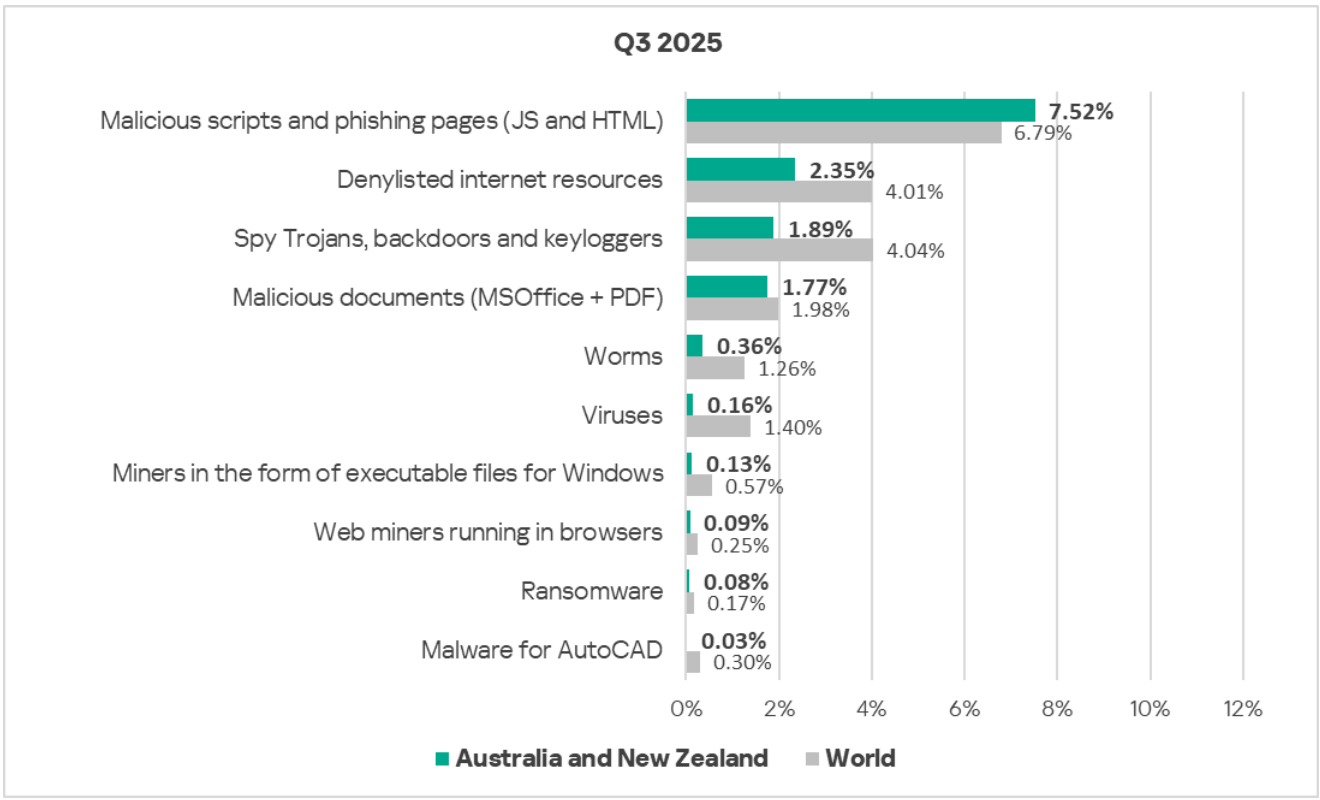
The quarterly indicator in the region grew to put Australia and New Zealand at second place among those four regions in which it increased.

© 2025 AO KASPERSKY LAB

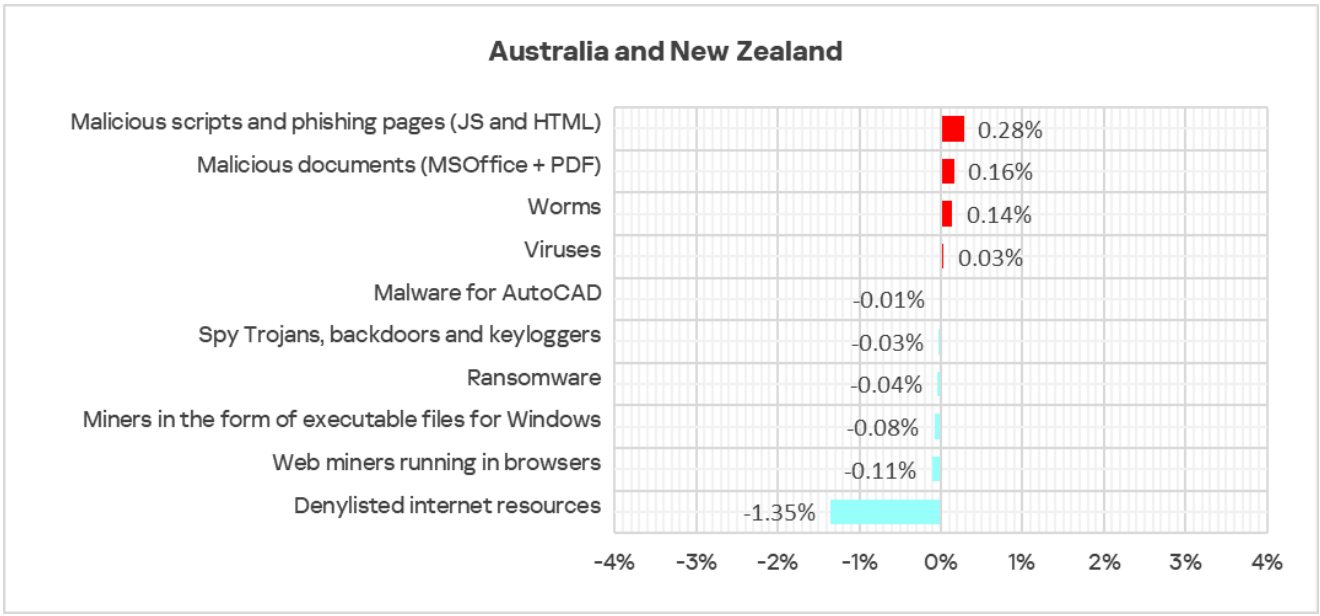


Just like with threats on removable media, threats in network folders are detected predominately in Australia.

Threat categories



© 2025 AO KASPERSKY LAB



Among all threat categories, only the percentage of ICS computers on which malicious scripts and phishing pages were blocked in Australia and New Zealand exceeded the global average — by a factor of 1.2.

Quarter-over-quarter increases were recorded in the percentages of ICS computers on which the following categories of malicious objects were blocked:

- malicious scripts and phishing pages;
- malicious documents: 1.1 times higher;
- viruses: 1.2 times higher;
- worms: 1.6 times higher.

In the regional rankings by the percentage of ICS computers on which different categories of malicious objects are blocked, Australia and New Zealand occupied their highest positions for malicious documents and malicious scripts, which put the region at seventh place in the rankings for both categories.

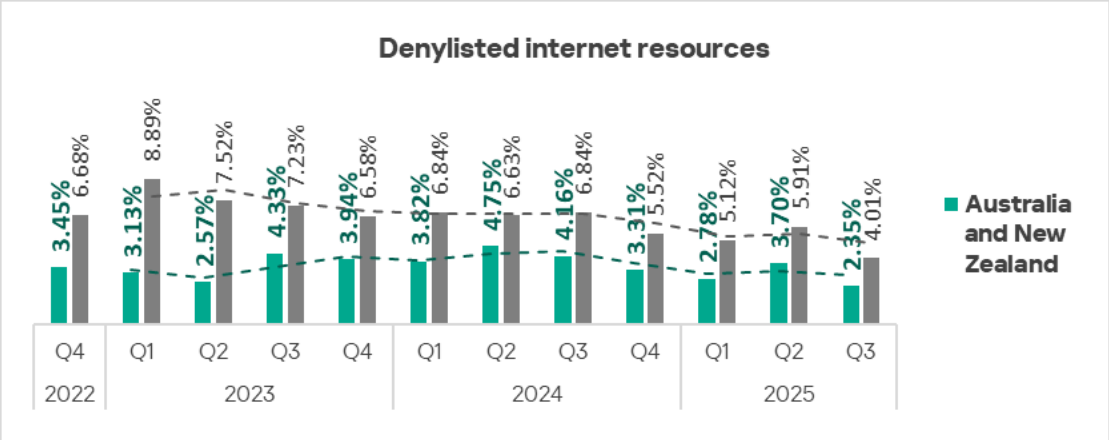
Australia and New Zealand is one of four regions in which the denylisted internet resources category did not drop below second place in the ranking.

Denylisted internet resources

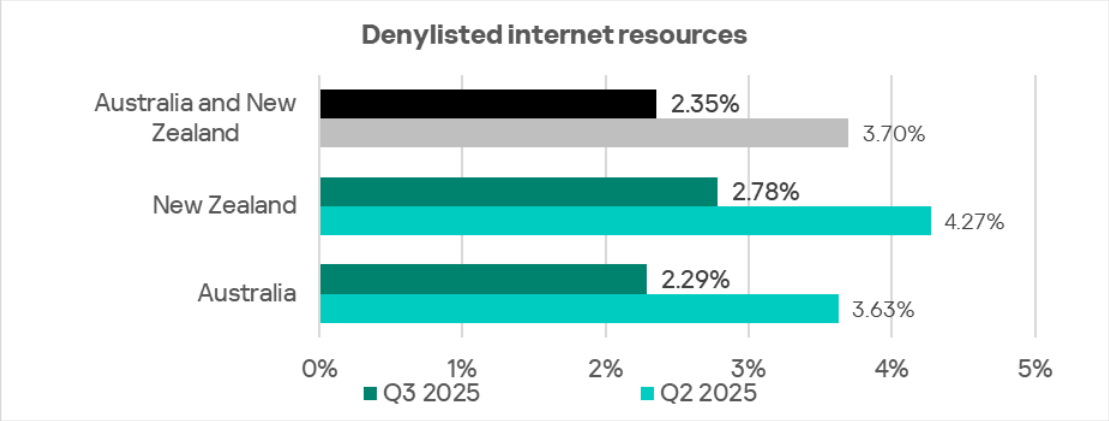
The Australia and New Zealand region ranks 14th, with 2.35%, based on the percentage of ICS computers on which denylisted internet resources were blocked.

Like in all regions, the indicator decreased over the quarter in Australia and New Zealand.

© 2025 AO KASPERSKY LAB



The percentage of ICS computers on which denylisted internet resources were blocked was 1.2 times higher in New Zealand than in Australia. This indicator decreased in both countries of the region.



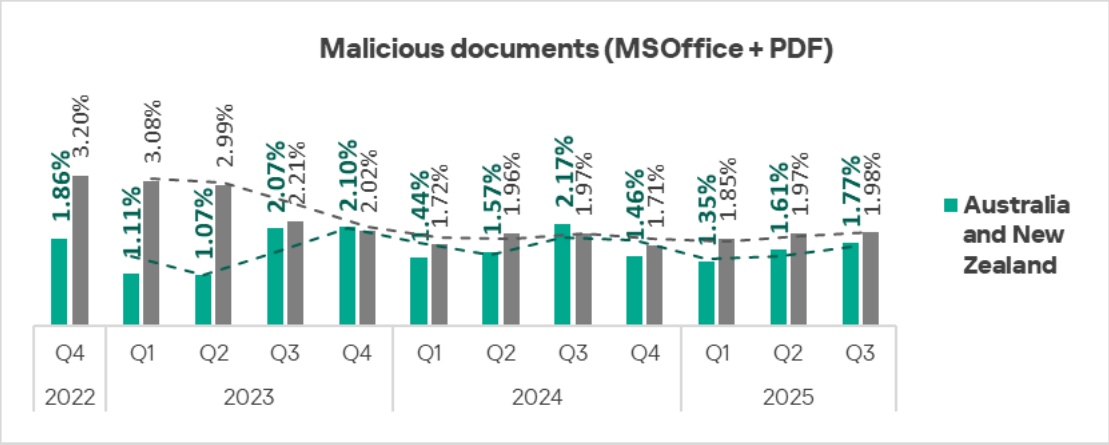
Malicious documents

Australia and New Zealand ranks seventh among regions based on the percentage of ICS computers on which malicious documents were blocked. This is the region's highest position in the rankings, both by sources and by threat categories.

The region's figure is 1.77%, 3.3 times higher than in Northern Europe, which ranks last.

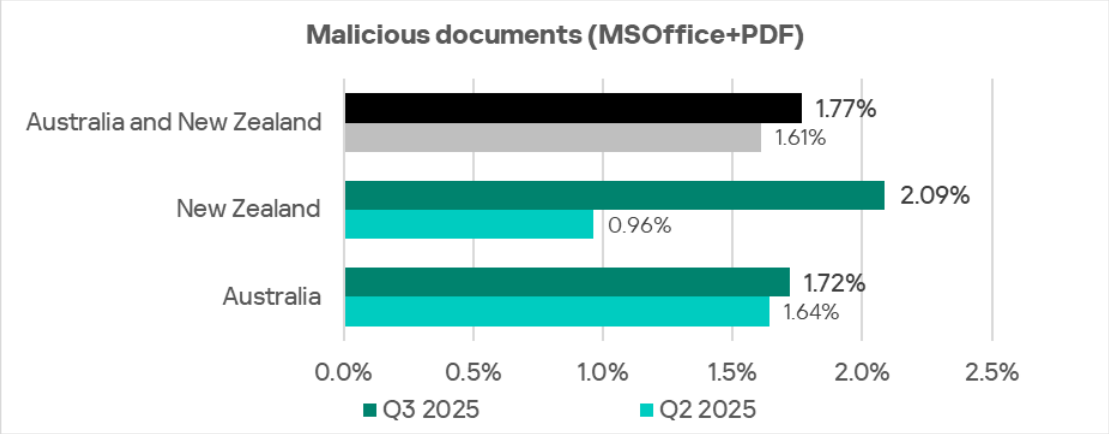
The percentage of ICS computers on which malicious documents were blocked fluctuates in the region. The indicator increased in Q3 2025. It should be mentioned that it grew only in three regions other than Australia and New Zealand.

© 2025 AO KASPERSKY LAB



The indicator increased in both countries of the region.

In the previous quarter, the percentage of ICS computers on which malicious documents were blocked was higher in Australia than in New Zealand. In Q3 2025, New Zealand outpaced Australia.



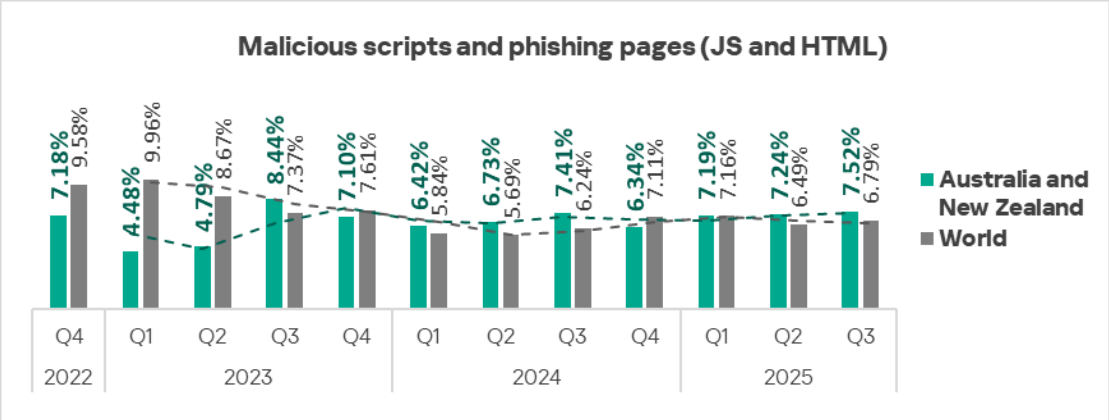
Malicious documents were distributed primarily via email.

Malicious scripts and phishing pages

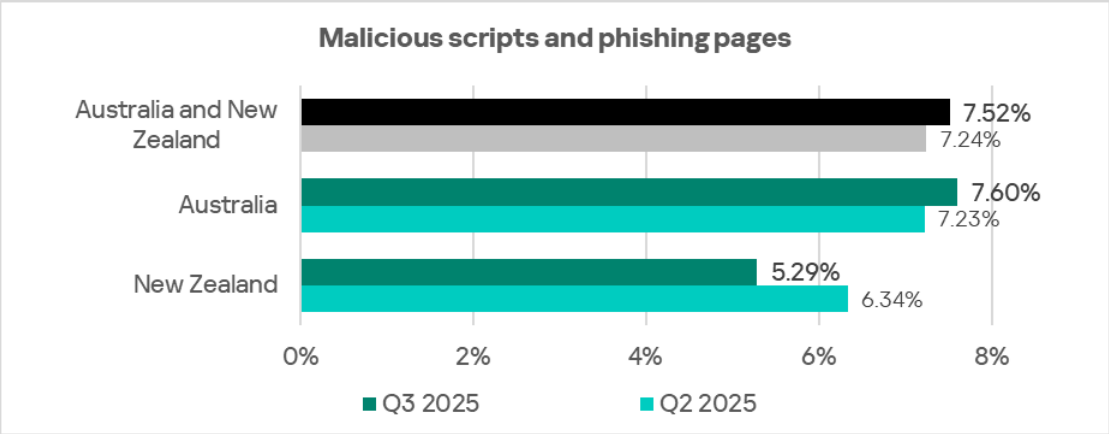
The Australia and New Zealand region occupies seventh place in the percentage of ICS computers on which malicious scripts and phishing pages were blocked. This is the region's highest position in the rankings, both by sources and by threat categories.

In Q3 2025, the percentage of ICS computers on which malicious scripts and phishing pages were blocked in the region increased to 7.52%. This is 2.9 times higher than in Northern Europe, which boasts the lowest percentage among all regions.

© 2025 AO KASPERSKY LAB



The percentage figure in Australia was 1.4 times that in New Zealand. Over the quarter, this figure rose in Australia while decreasing in New Zealand.



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

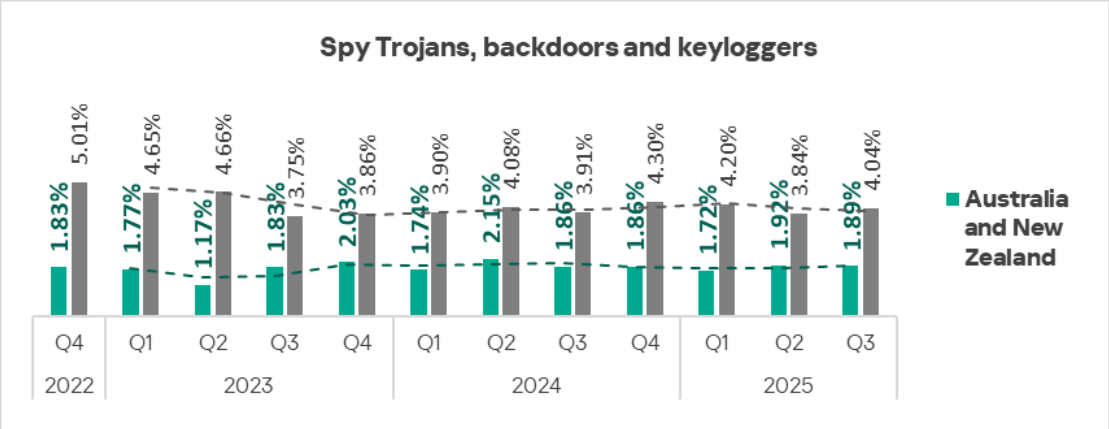
Malicious scripts may be used by threat actors for a whole number of tasks, including to load spyware onto a computer.

Spyware

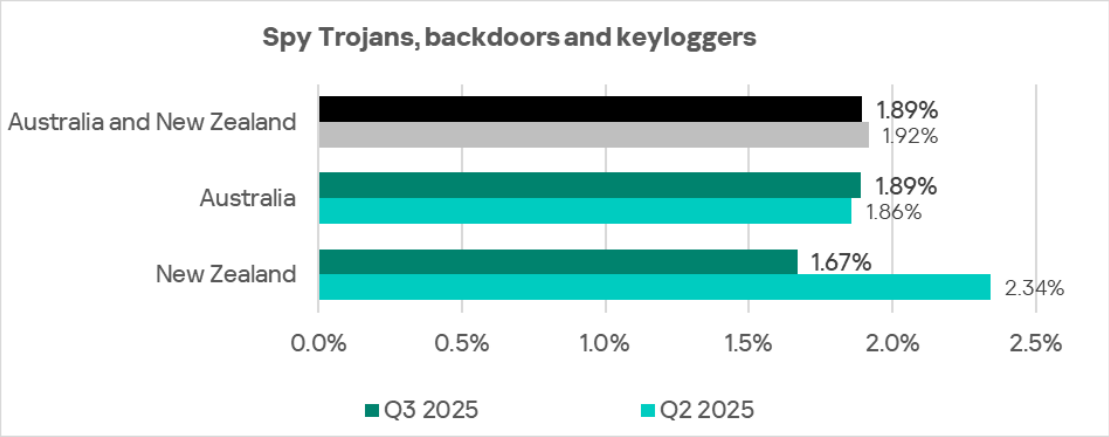
Based on the percentage of ICS computers on which spyware was blocked, the Australia and New Zealand region occupies 11th place in this ranking with 1.89%. This is 1.4 times higher than in Northern Europe, which has the lowest percentage value.

The percentage of ICS computers on which spyware was blocked in the region fluctuates. This indicator slightly decreased in Q3 2025.

© 2025 AO KASPERSKY LAB



In the previous quarter, the percentage of ICS computers on which spyware is blocked was significantly higher in New Zealand than in Australia. During the quarter, the indicator for New Zealand decreased and yielded the lead to Australia.



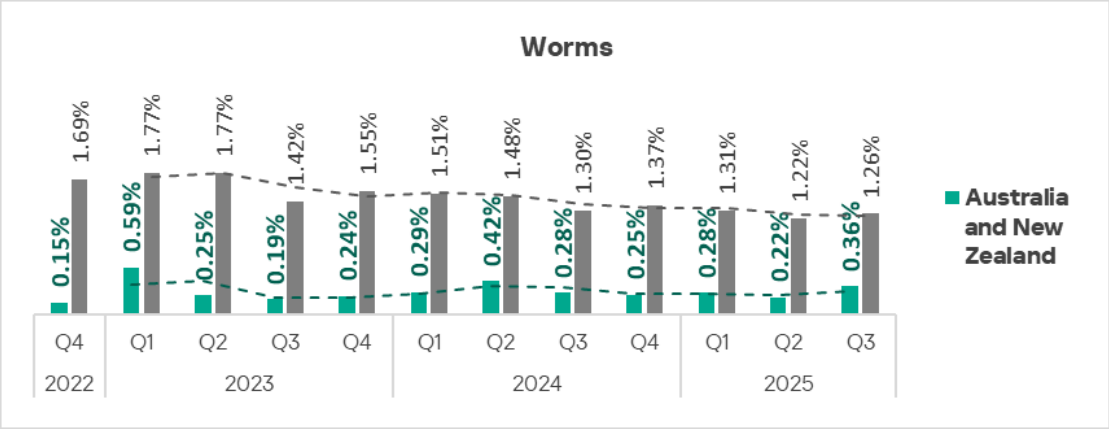
In the region, spyware was blocked on the internet and predominately in email clients.

Worms

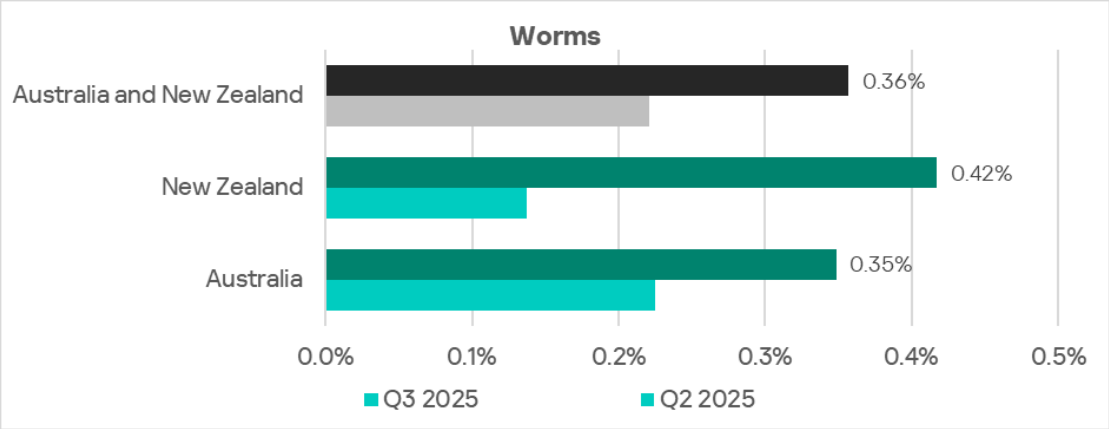
Based on the percentage of ICS computers on which worms were blocked, the Australia and New Zealand region ranks 12th at 0.36%. This is 1.6 times higher than in Northern Europe, which ranks last in this category.

The indicator in the region fluctuates. In Q3 2025, it grew to its largest figure since Q2 2024.

© 2025 AO KASPERSKY LAB



The percentage of ICS computers on which worms were blocked during the quarter significantly grew in both countries of the region. The percentage value in New Zealand was higher than in Australia.



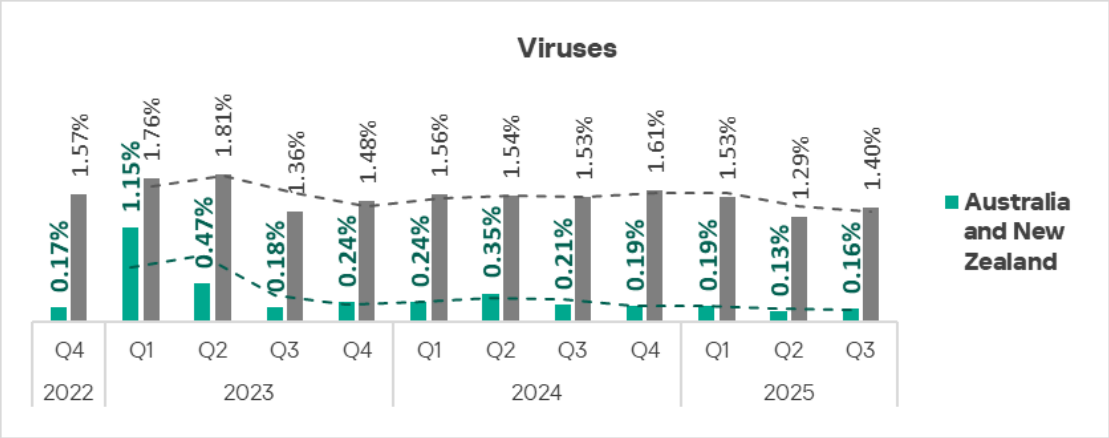
Worms spread through all threat sources. In Q3 2025, they most frequently spread in email clients and removable media.

Viruses

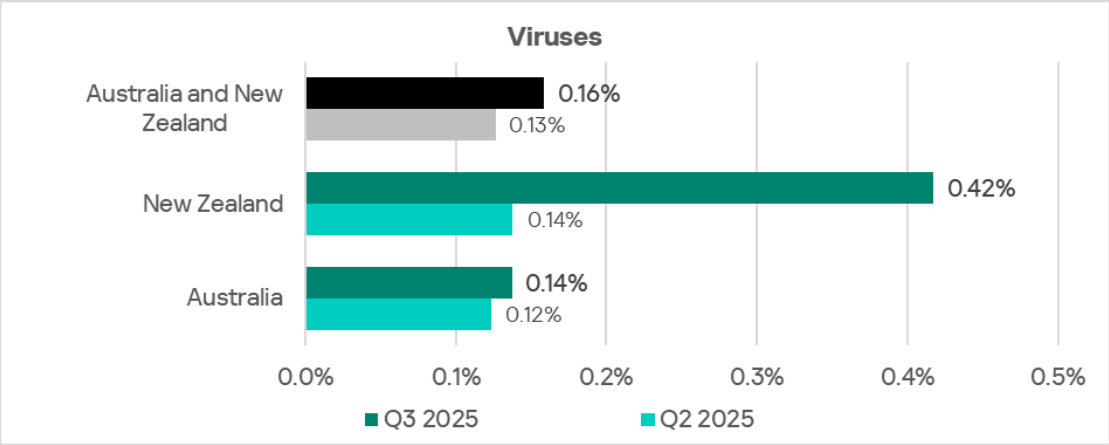
Based on the percentage of ICS computers on which viruses were blocked, Australia and New Zealand ranks 14th among regions with an indicator of 0.16%.

The indicator in the region grew for the first time since Q2 2024.

© 2025 AO KASPERSKY LAB



The percentage of ICS computers on which viruses are blocked increased in both countries of the region, particularly increasing by a factor of 3.0 in New Zealand. This indicator in New Zealand was just as high compared to the same indicator in Australia in Q3 2025.

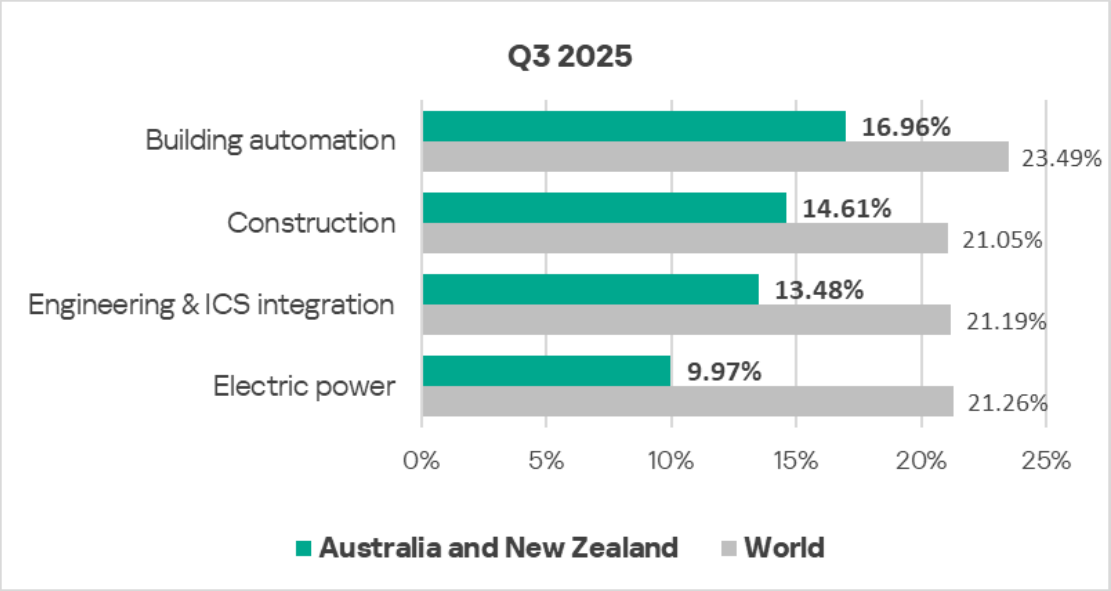


Like worms, viruses in the region spread through all threat sources. In Q3 2025, they most frequently spread in email clients and removable media.

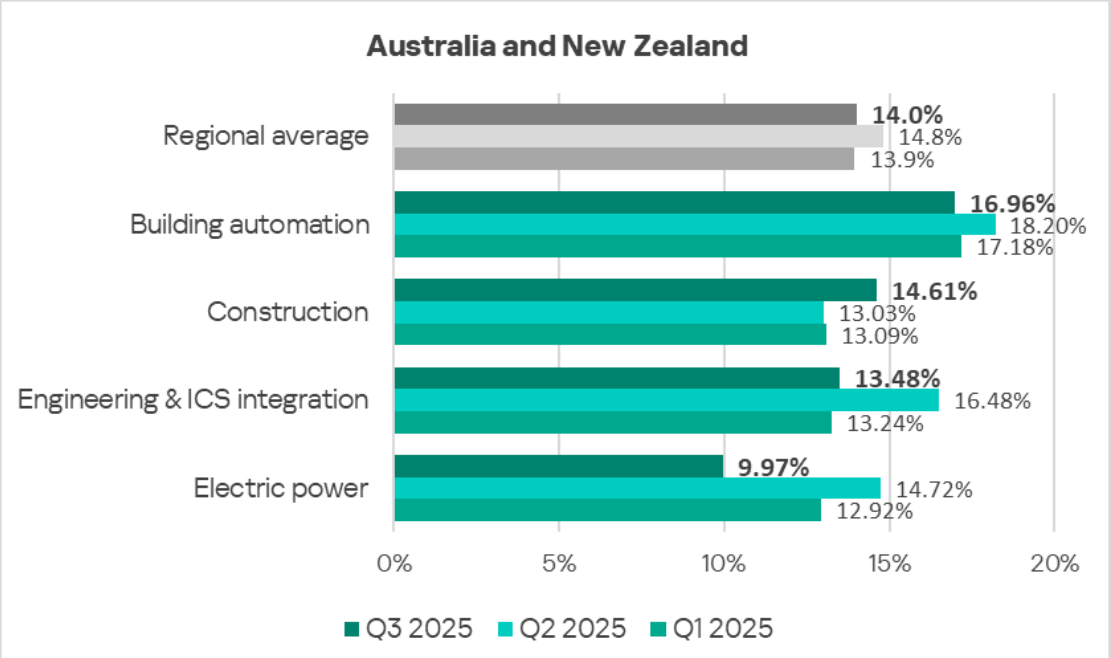
Industries

Among the industries examined in the report, building automation threats are most frequently encountered in Australia and New Zealand.

© 2025 AO KASPERSKY LAB

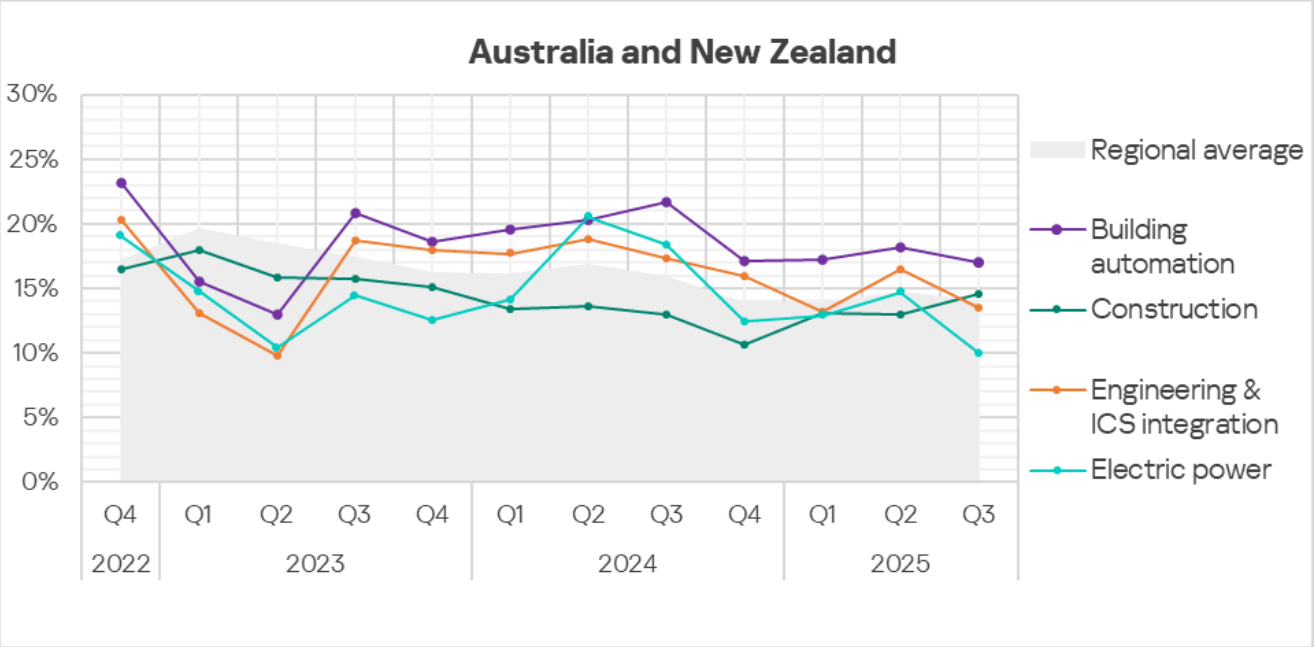


In Q3 2025, the percentage of ICS computers on which malicious objects were blocked decreased across all of the reviewed industries except construction.



The percentage figures for building automation, as well as engineering and ICS integrators, were above the regional average.

© 2025 AO KASPERSKY LAB



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 Australia and New Zealand, Q3 2025

Industry / Threat source	Building automation	Electric power	Engineering & ICS integration	Construction	Threat category total in the region
Internet	6.65%	2.66%	7.20%	6.60%	6.84%
Email clients	6.46%	1.66%	2.56%	4.80%	3.74%
Removable media	0.05%	0.00%	0.04%	0.00%	0.05%
Network folders	0.00%	0.00%	0.00%	0.00%	0.02%
Industry total in the region	16.96%	9.97%	13.48%	14.61%	

© 2025 AO KASPERSKY LAB

Threat category indicators for industries in Australia and New Zealand, Q3 2025

Industry / Threat category	Building automation	Electric power	Engineering & ICS integration	Construction	Threat category total in the region
Denylisted internet resources	2.80%	0.33%	2.32%	1.67%	2.35%
Malicious scripts and phishing pages (JS and HTML)	8.99%	3.99%	6.50%	9.29%	7.52%
Spy Trojans, backdoors and keyloggers	3.03%	1.99%	1.83%	1.19%	1.89%
Worms	0.50%	0.33%	0.35%	0.35%	0.36%
Miners in the form of executable files for Windows	0.23%	0.00%	0.14%	0.09%	0.13%
Malicious documents (MSOffice + PDF)	3.07%	2.66%	1.19%	1.72%	1.77%
Viruses	0.28%	0.33%	0.04%	0.18%	0.16%
Ransomware	0.23%	0.00%	0.07%	0.00%	0.08%
Web miners running in browsers	0.09%	0.00%	0.14%	0.09%	0.09%
Malware for AutoCAD	0.00%	0.00%	0.00%	0.13%	0.03%
Industry total in the region	16.96%	9.97%	13.48%	14.61%	

In the regional rankings based on the percentage of ICS computers on which malicious objects were blocked in various industries, Australia and New Zealand were only able to reach 11th place.

In two industries (construction and electrical energy industry), the region made the top 3 based on industry indicators for email client threats, malicious documents, and malicious scripts.

- Based on indicators in the construction industry among the regions, Australia and New Zealand occupy third place in email client threats, malicious scripts and phishing pages.
- Based on indicators in the electrical energy industry among regions, the Australia and New Zealand region occupies second place in malicious documents.

© 2025 AO KASPERSKY LAB

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

Building automation

Australia and New Zealand rank 11th among regions based on the percentage of ICS computers on which malicious objects were blocked in the building automation industry.

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

- First place in the percentage of ICS computers on which threats in email clients and removable media were blocked.
- Second place in internet threats.
- First place in the percentage of ICS computers on which threats of the following categories were blocked: denylisted internet resources, spyware, malicious documents, worms, and miners in the form of executable files for Windows.
- Second place in threats of the following categories: malicious scripts and phishing pages, viruses, web miners, and ransomware.

Construction

The Australia and New Zealand region ranks 11th among regions based on the percentage of ICS computers on which malicious objects were blocked in the construction industry.

Based on industry indicators among regions, this region has the following rankings:

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

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

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

© 2025 AO KASPERSKY LAB

Engineering and ICS integrators

The Australia and New Zealand region ranks 11th among regions based on the percentage of ICS computers on which malicious objects in the engineering and ICS integrators industry were blocked.

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

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

Electrical energy industry

The Australia and New Zealand region ranks 12th among regions based on the percentage of ICS computers on which malicious objects were blocked in the electrical energy industry.

Based on industry indicators among regions, this region has the following rankings:

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

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

- First place in the percentage of ICS computers on which viruses are blocked.
- Second place in spyware and malicious documents.

© 2025 AO KASPERSKY LAB

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.

© 2025 AO KASPERSKY LAB

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.

© 2025 AO KASPERSKY LAB

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

© 2025 AO KASPERSKY LAB