Kaspersky ICS CERT

Threat landscape for industrial automation systems

Europe. Q3 2025

22.12.2025

Version 1.0

Eastern Europe

Key cybersecurity issues in the region

High risk of targeted attacks

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

In Eastern Europe, the percentage of ICS computers on which threats from email clients were blocked is 1.3 times higher than the global average.

The percentage of ICS computers on which malicious documents are blocked also exceeds the global average by a factor of 1.3.

Attackers distribute malicious documents in phishing emails and use them as an initial infection vector. Typically, such documents contain exploits, malicious macros, or harmful links.

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 authentication data for corporate services.

In Eastern Europe in Q3 2025, the percentage of ICS computers on which malicious scripts and phishing pages are blocked is comparable to the global average.

High rate of spyware

The percentage of ICS computers on which spyware was blocked in Eastern Europe is 1.1 times higher than the global average. Spyware is used by attackers to steal confidential data. In targeted attacks, it is also used for lateral movement within compromised networks and for deploying final-stage malware.

Industries

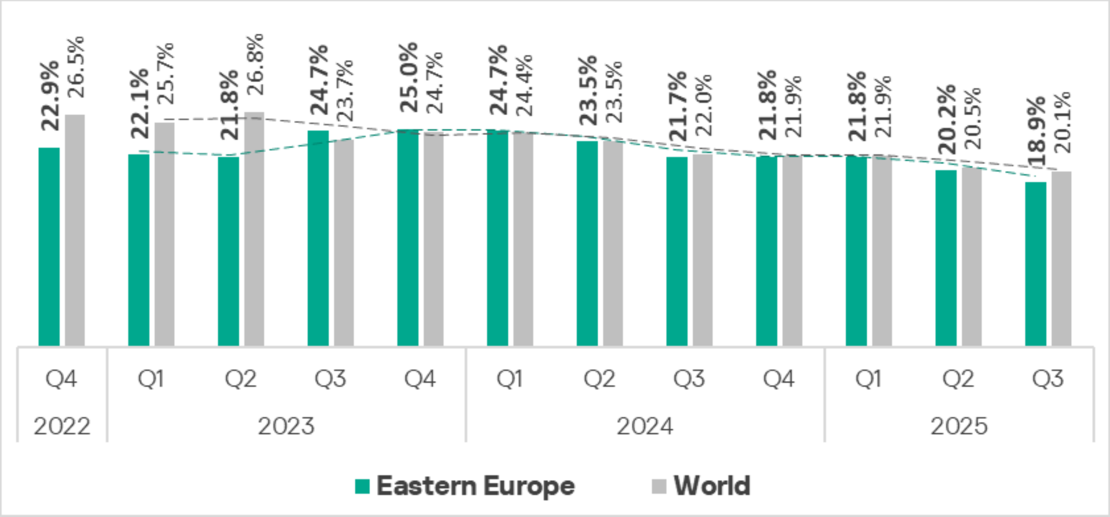
The threat of targeted attacks in the region are especially relevant for the building automation industry. Based on the indicators for malicious documents and spyware in this industry, Eastern Europe occupies third place among regions, and it ranks fourth in malicious scripts and phishing pages.

Among industries in Eastern Europe, the building automation industry leads in these three threat categories.

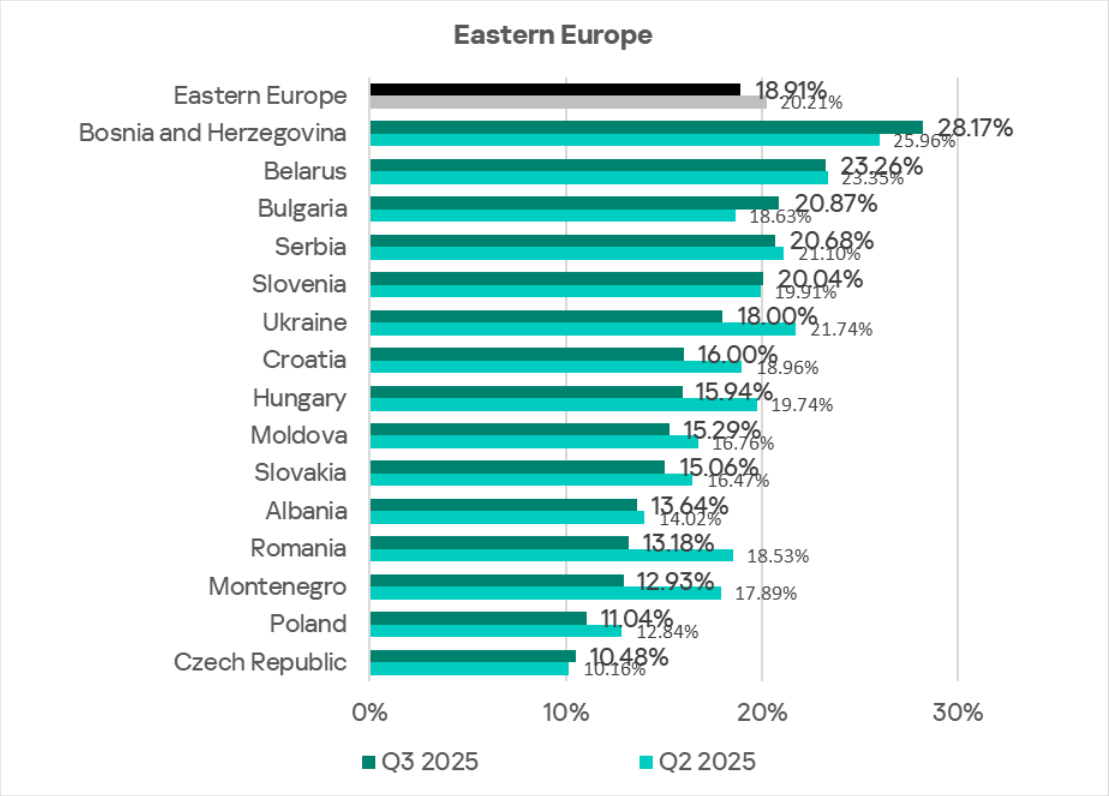
Statistics across all threats

In Q3 2025, Eastern Europe ranked eighth among all regions for the percentage of ICS computers on which malicious objects were blocked. The indicator for Eastern Europe is larger than in all other European regions.

In Q3 2025, the indicator in the region decreased to 18.9%, which is the lowest value over three years. It is slightly lower than the global average and is 2.1 times higher than in Northern Europe, which has the lowest figure among regions.

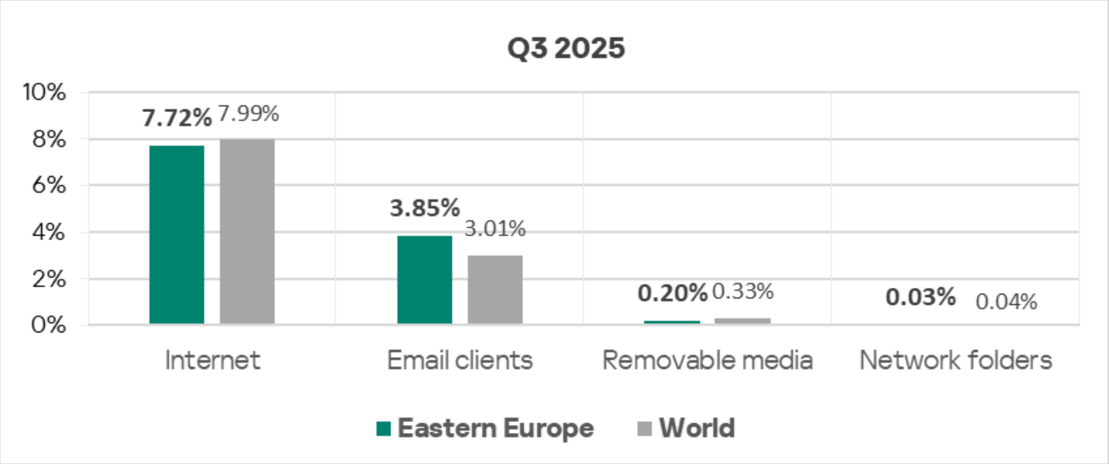


Among the region's countries, Bosnia and Herzegovina leads in this metric with 28.17%. The Czech Republic had the lowest figure at 10.48%. Over the quarter, this indicator grew only in four countries: in Bosnia and Herzegovina, Bulgaria, Czech Republic, and just slightly in Slovenia.

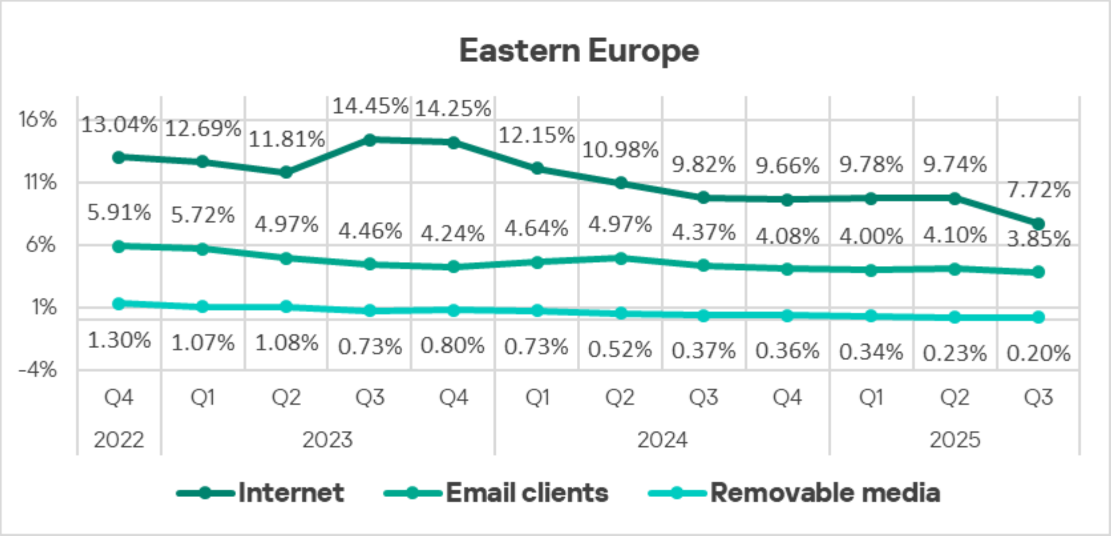


Threat sources

With the exception of email clients, all threat source rates in Eastern Europe are below the global average. The percentage of ICS computers on which email client threats were blocked is 1.3 times higher than the global average.



Malicious objects in the region spread primarily via the internet and email. Network folders are a minor source of threats, but in Q3 2025 among all threat sources the percentage of ICS computers on which malicious objects were blocked slightly increased only for network folders.

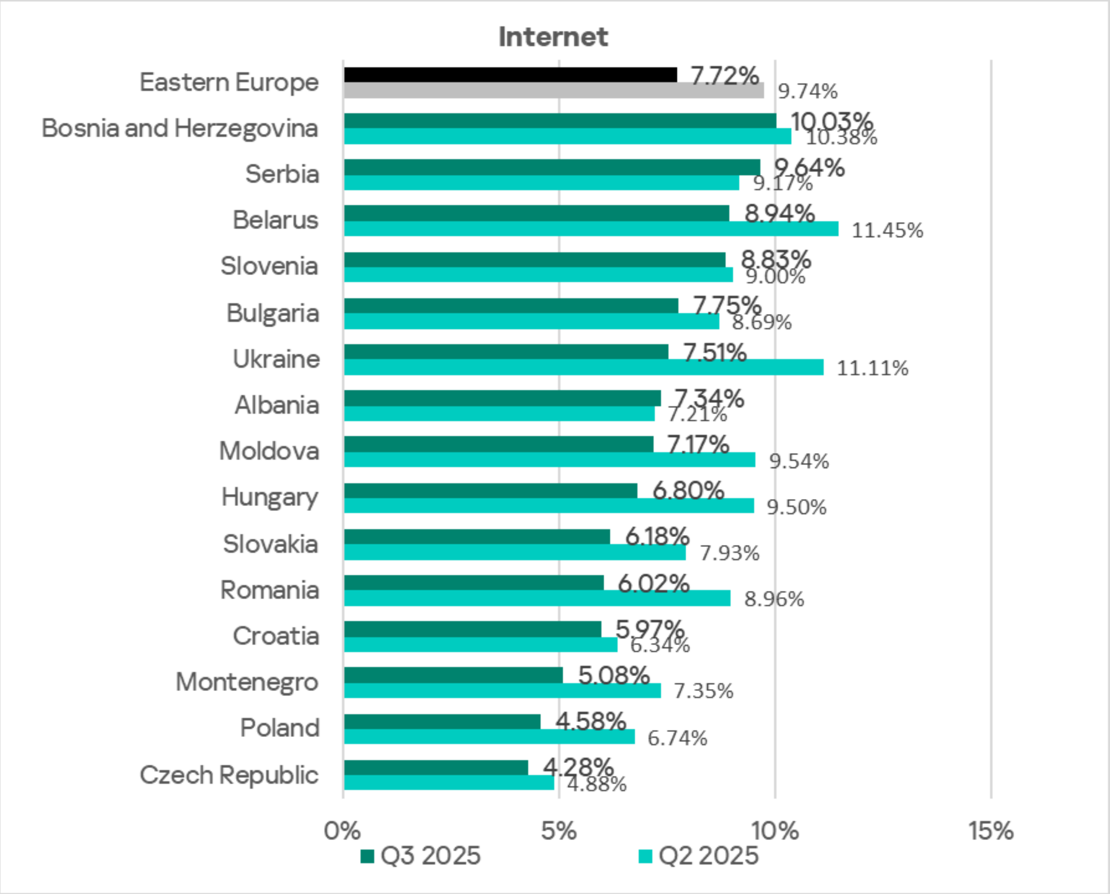


Eastern Europe rose from 13th place to fifth place in the rankings of regions in the percentage of ICS computers on which threats in network folders are blocked.

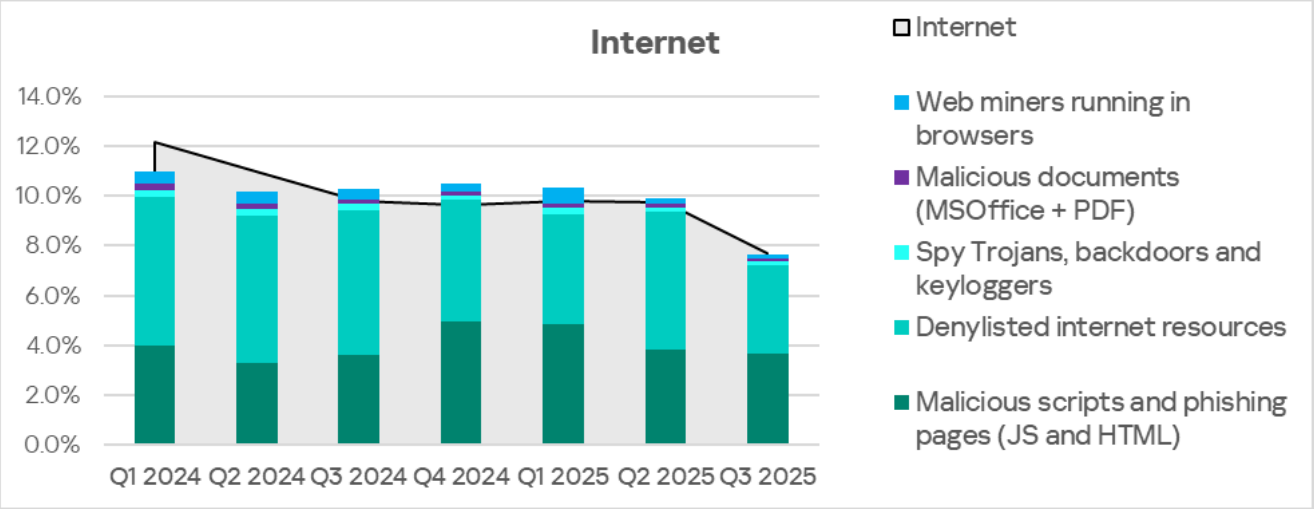
Internet

Based on the percentage of ICS computers on which internet threats are blocked, Eastern Europe ranks sixth globally at 7.72%, which is 1.7 times higher than the lowest figure (Northern Europe).

Country-level rates range from 4.28% in the Czech Republic to 10.03% in Bosnia and Herzegovina.



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.

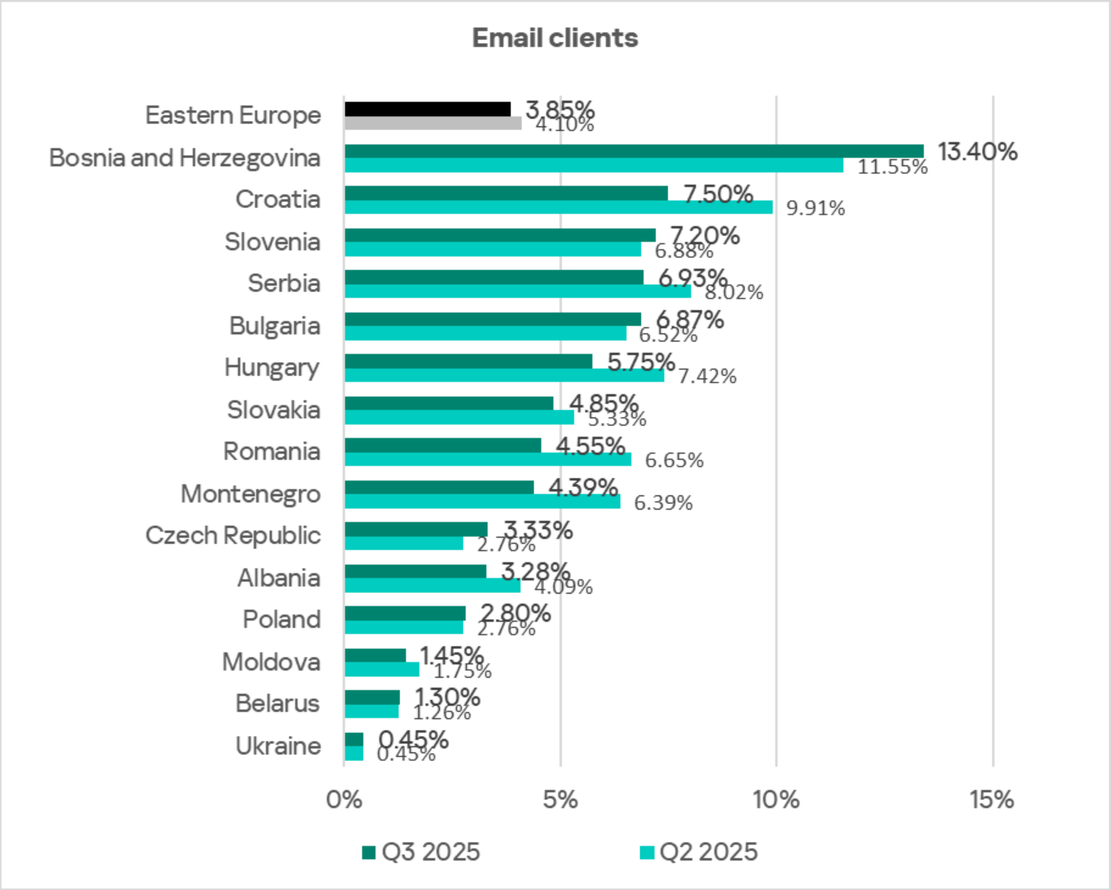


Based on the indicator for denylisted internet resources, Eastern Europe ranks fifth in the corresponding ranking of regions.

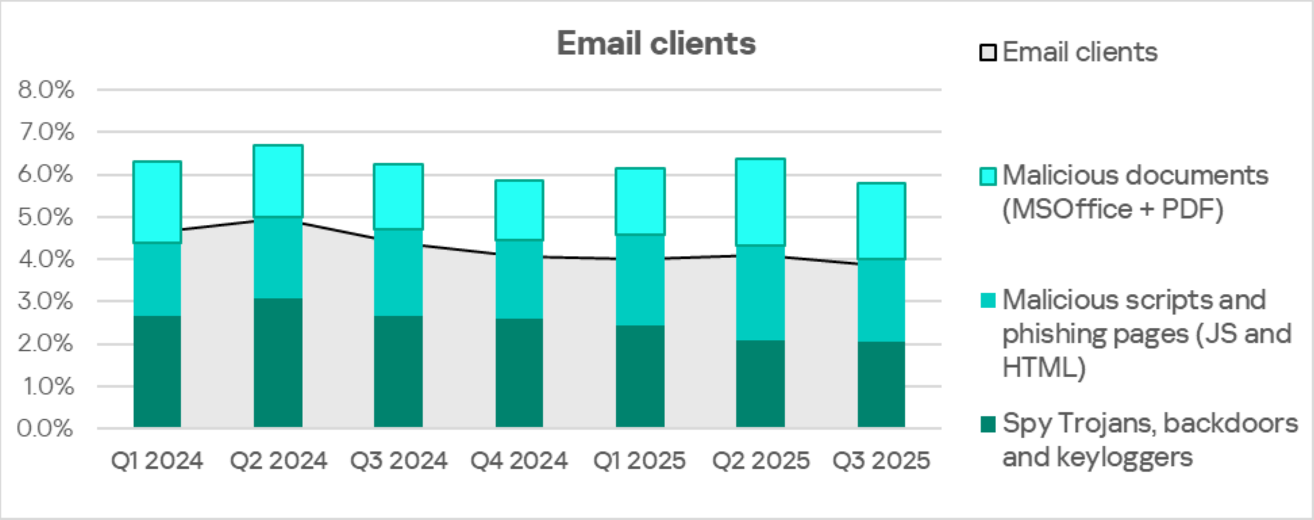
Email clients

By the percentage of ICS computers on which threats from email clients were blocked, Eastern Europe ranked sixth globally in Q3 2025, at 3.85%. This is 4.9 times higher than in Russia, which ranks last.

Among countries in the region, Bosnia and Herzegovina (13.40%) lead all other countries by a wide margin in the percentage of ICS computers on which email client threats were blocked. The lowest figure observed was in Ukraine at 0.45%.



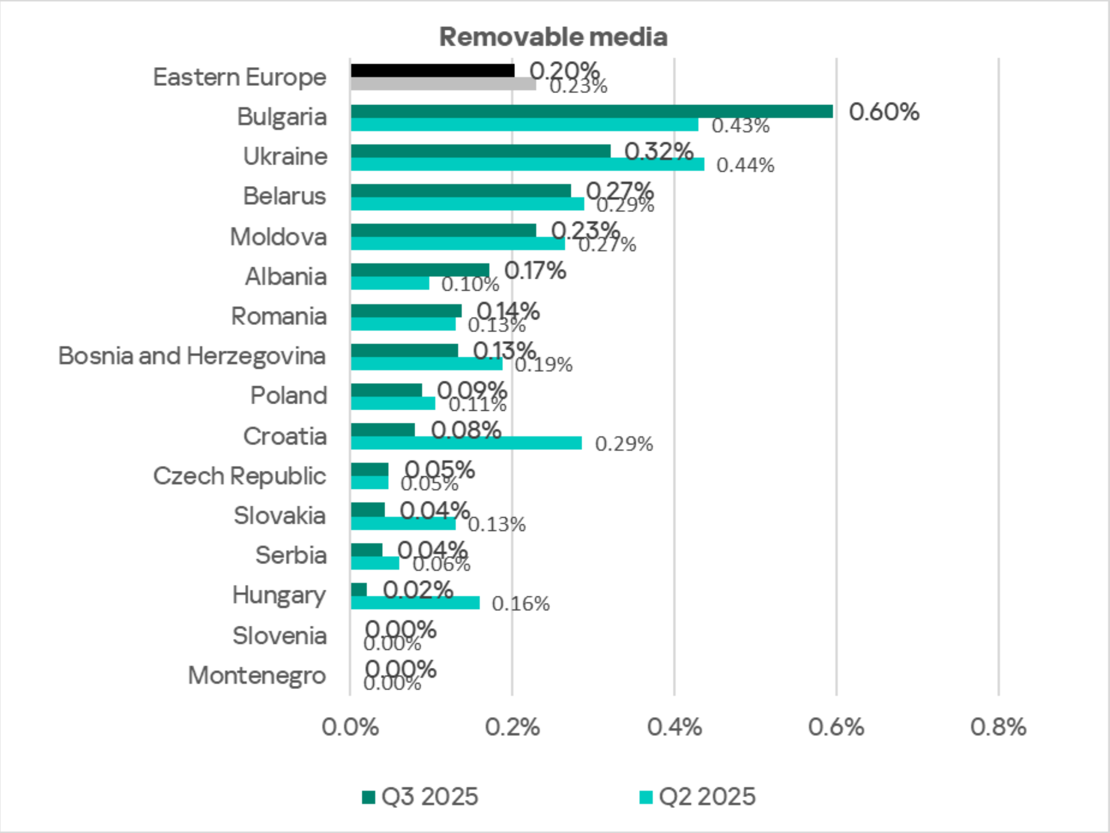
The main categories of email client threats that were blocked on ICS computers are spyware, malicious scripts and phishing pages, and malicious documents.



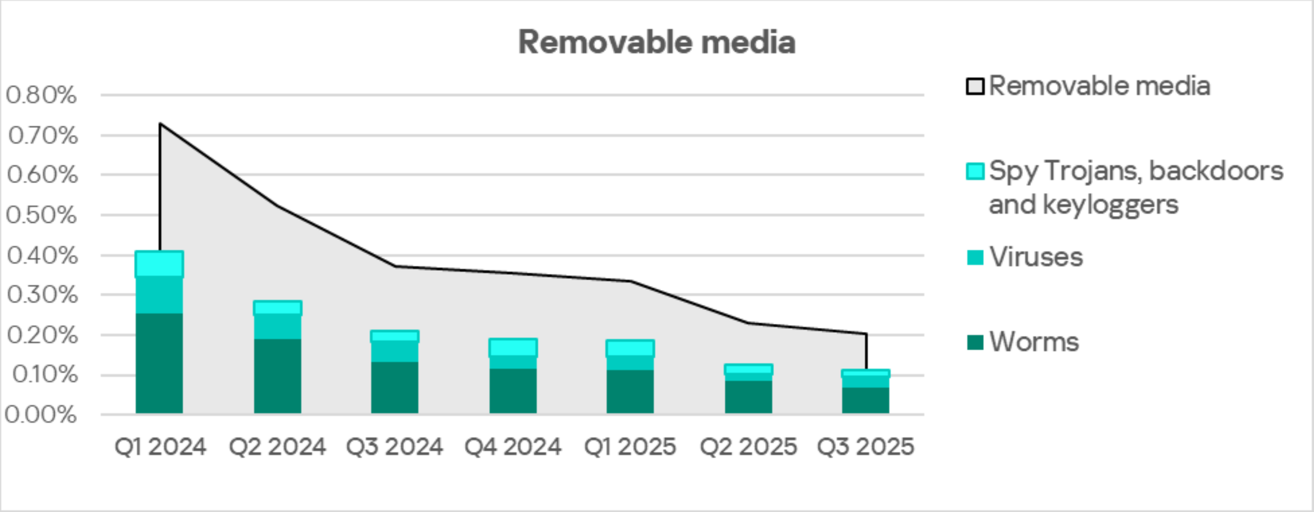
Removable media

In terms of ICS computers where threats were blocked when connecting removable media, Eastern Europe ranked seventh globally in Q3 2025, at 0.20%. This is 4.0 times higher than the Australia and New Zealand region, which ranks last in the corresponding ranking.

Among the countries in the region, Bulgaria leads significantly in the percentage of ICS computers on which threats were blocked upon connecting removable media, with 0.60%.

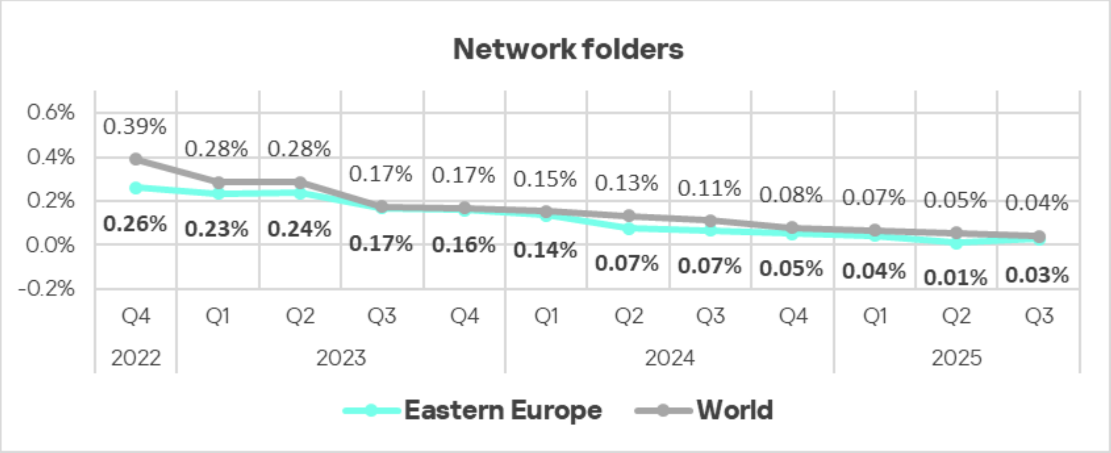


The main categories of removable media threats blocked on ICS computers in the region are worms, spyware, and viruses.



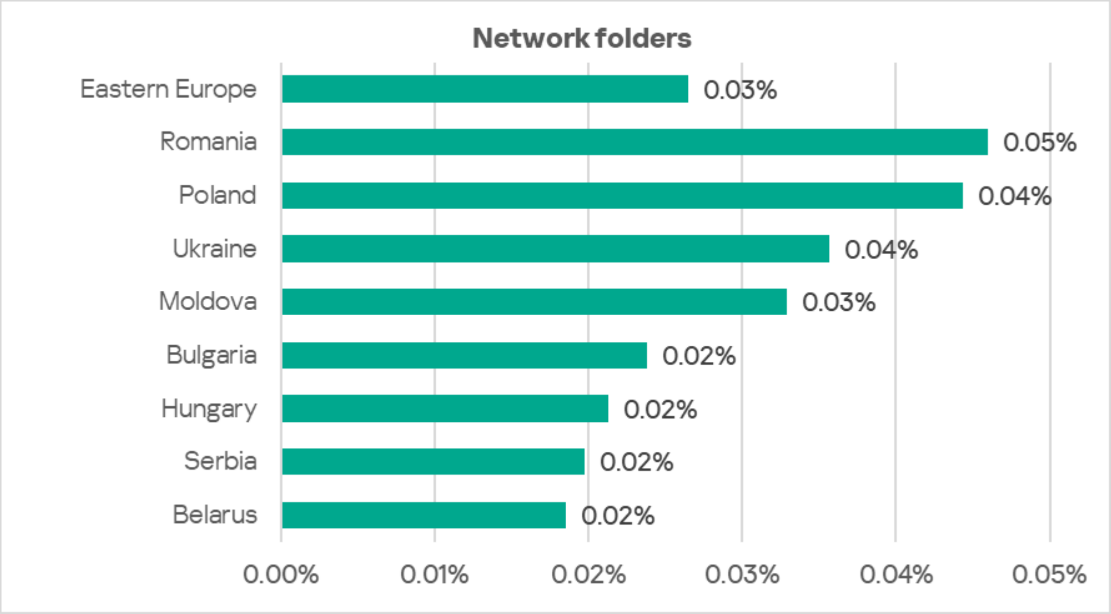
Network folders

Eastern Europe rose from 13th place to fifth place in the rankings of regions in the percentage of ICS computers on which threats in network folders are blocked. Over the quarter, the network folders indicator in the region increased by a factor of 2.6 to 0.026%. This is 4.3 times higher than Northern Europe, which ranks last.

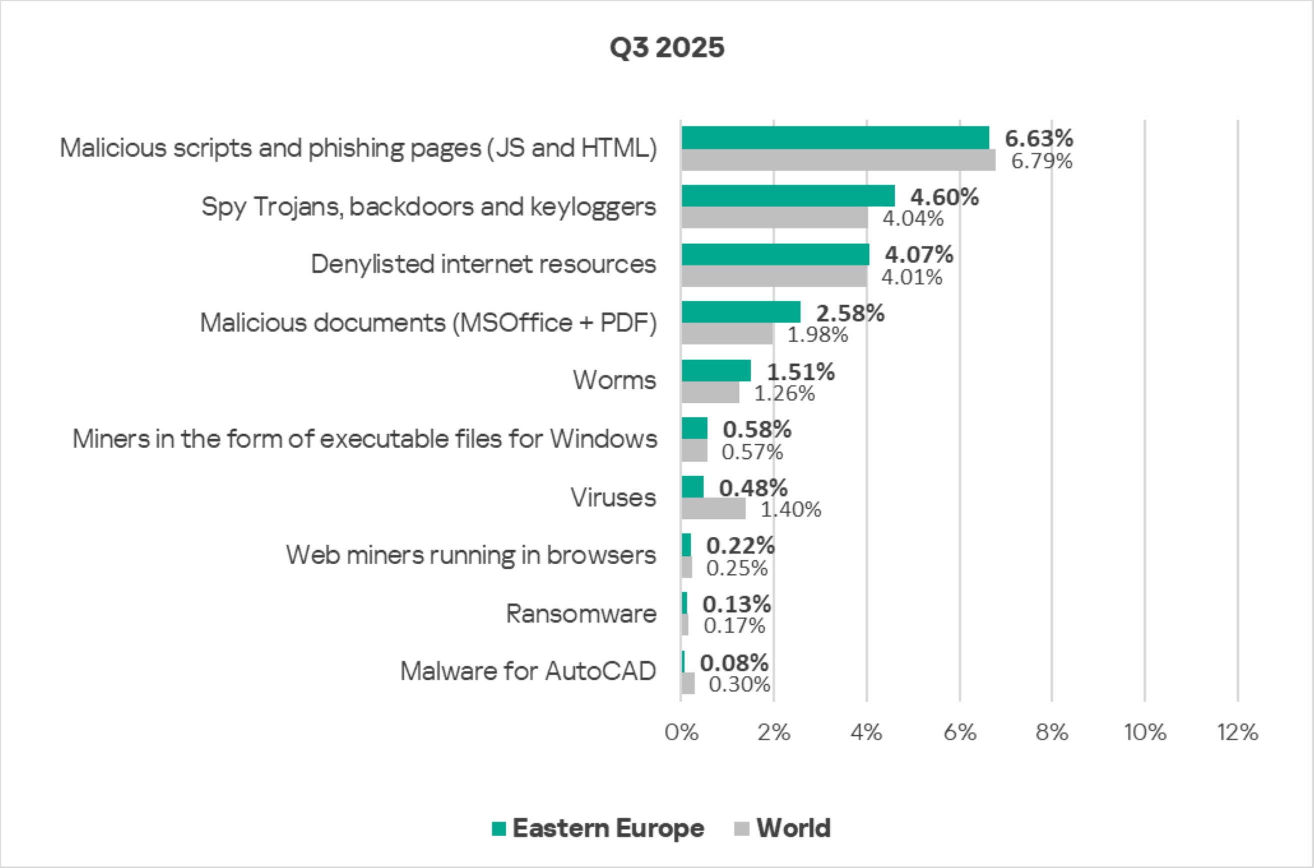


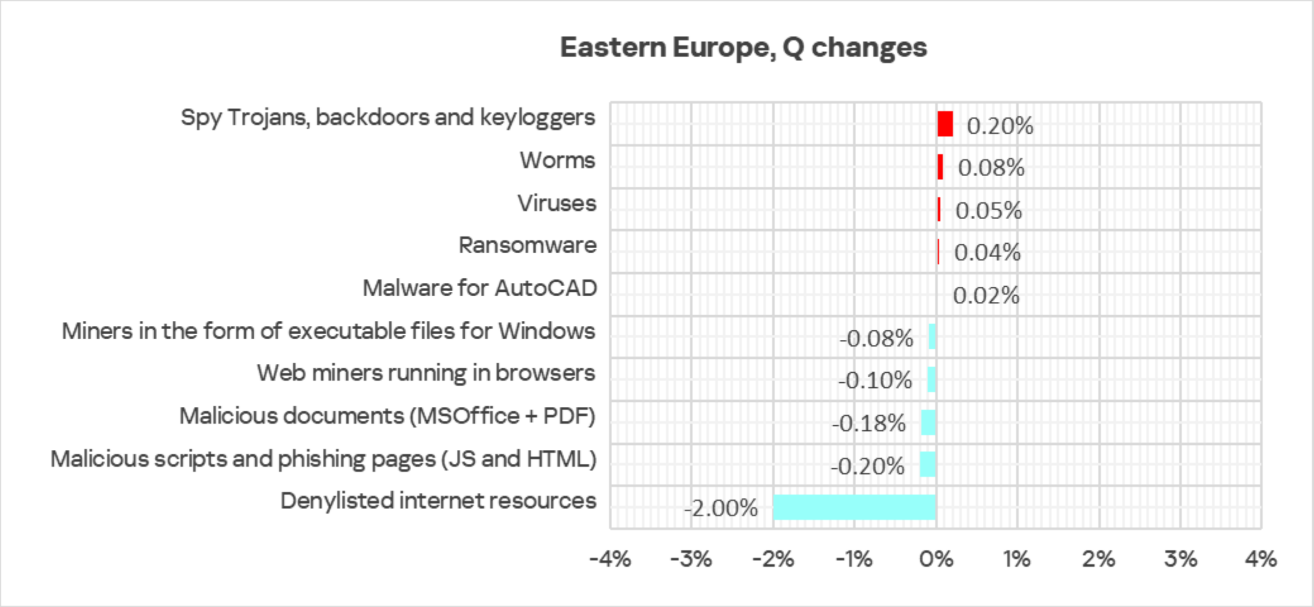
In Q3 2025, Eastern Europe leads among European regions in growth of the percentage of ICS computers on which network folder threats were blocked. Despite the noticeable growth of the indicator for this threat source, in a protected infrastructure threats in network folders are encountered fairly rarely and not in all countries of the region. The same is true for industries. Network folder threats were detected only in two industries: building automation, and engineering and ICS integrators.

Among countries in the region, Romania leads in the percentage of ICS computers on which network folder threats were blocked with a figure of 0.05%.



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: 1.3 times higher.

- Worms: 1.2 times higher.
- Spyware: 1.1 times higher.

Malicious documents are often used by attackers to deliver targeted malware — including spyware. In the region, the indicator for spyware grew more than anything else over the quarter.

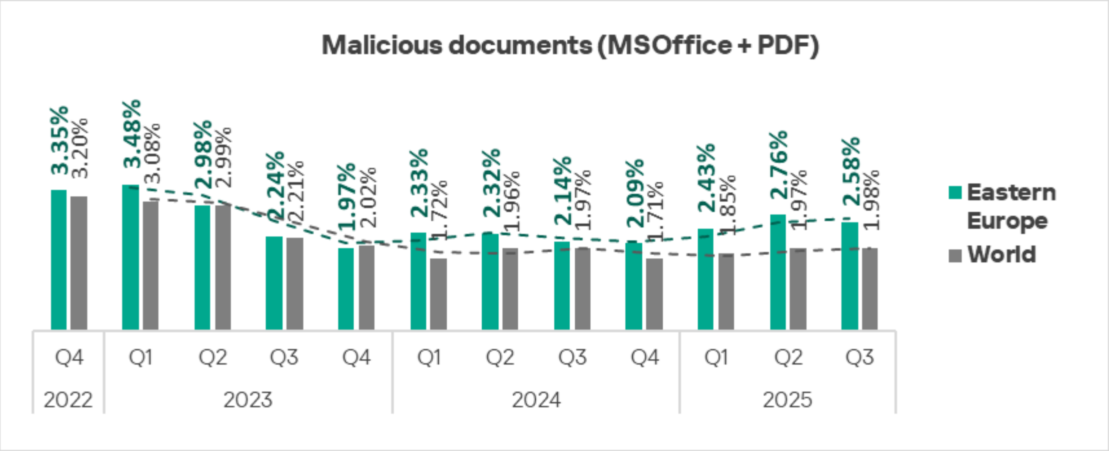
The indicators for denylisted internet resources and miners in the form of executable files for Windows slightly exceed the global averages.

In terms of miners in the form of executable files, Eastern Europe ranks third among regions.

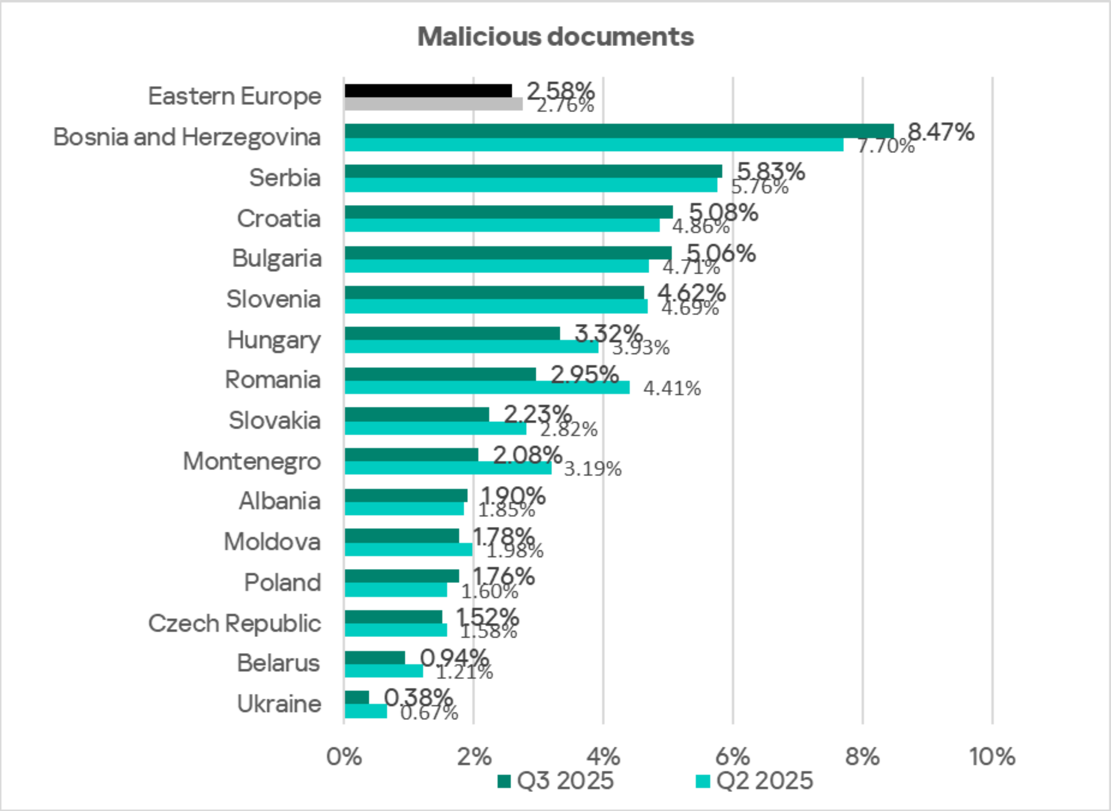
Malicious documents

Eastern Europe ranks fifth globally by the percentage of ICS computers on which malicious documents were blocked. In Q3 2025, the region's figure was 2.58%, which is 4.9 times higher than in Northern Europe, the lowest-ranked region.

In Q3 2025, the percentage of ICS computers on which malicious documents are blocked decreased after its growth over the two previous quarters.



Among countries in the region, Bosnia and Herzegovina leads with 8.47%. Ukraine is last in the ranking with 0.38%.

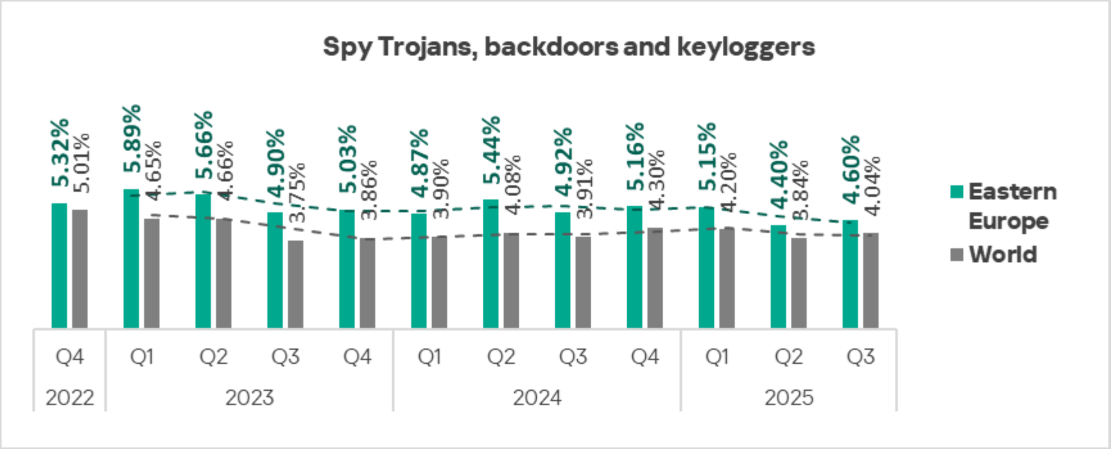


Malicious documents are distributed primarily via email.

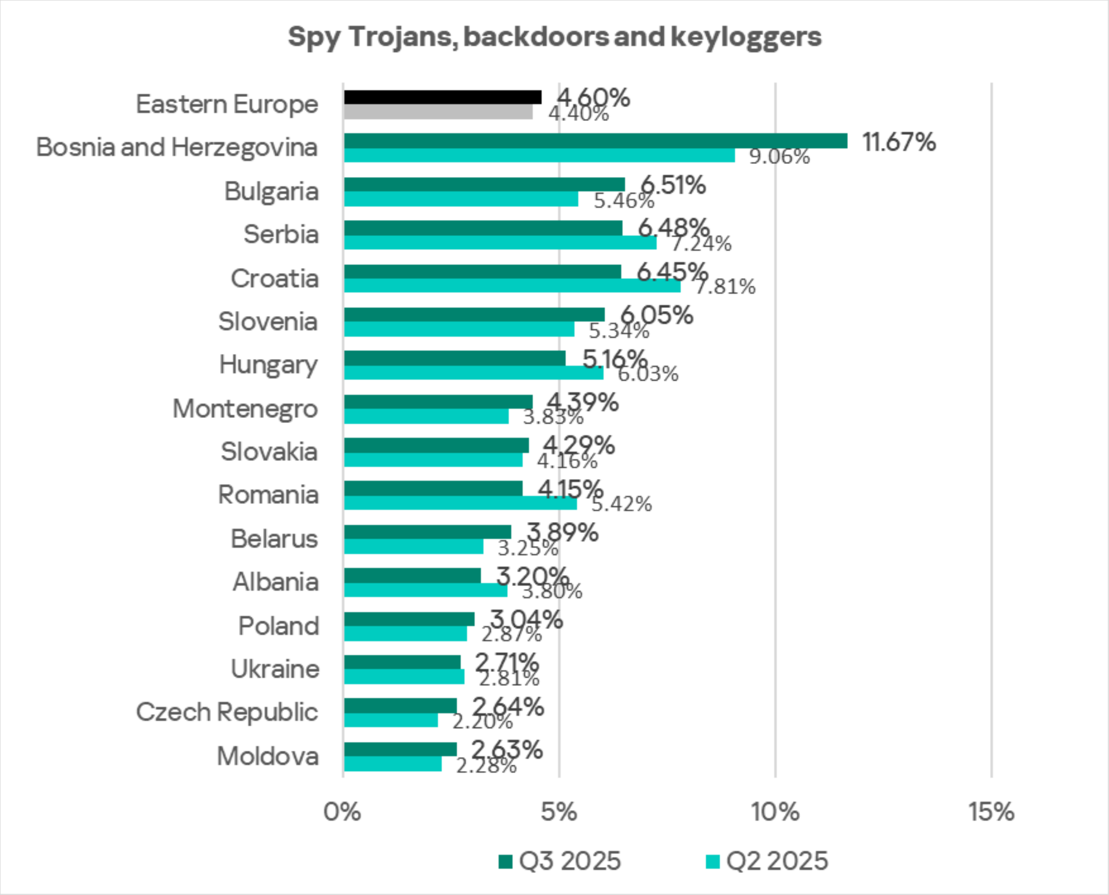
Spyware

By the percentage of ICS computers on which spyware was blocked, Eastern Europe ranks sixth globally with 4.60%. This figure is 3.3 times higher than in Northern Europe, which has the lowest rate.

The percentage of ICS computers in Eastern Europe where spyware was blocked fluctuates over time. In Q3 2025, the indicator slightly increased after reaching its minimum during the previous quarter.



Among the region's countries, Bosnia and Herzegovina leads in the percentage of ICS computers on which spyware is blocked with 11.67%. The lowest figure observed was in Moldova at 2.63%.

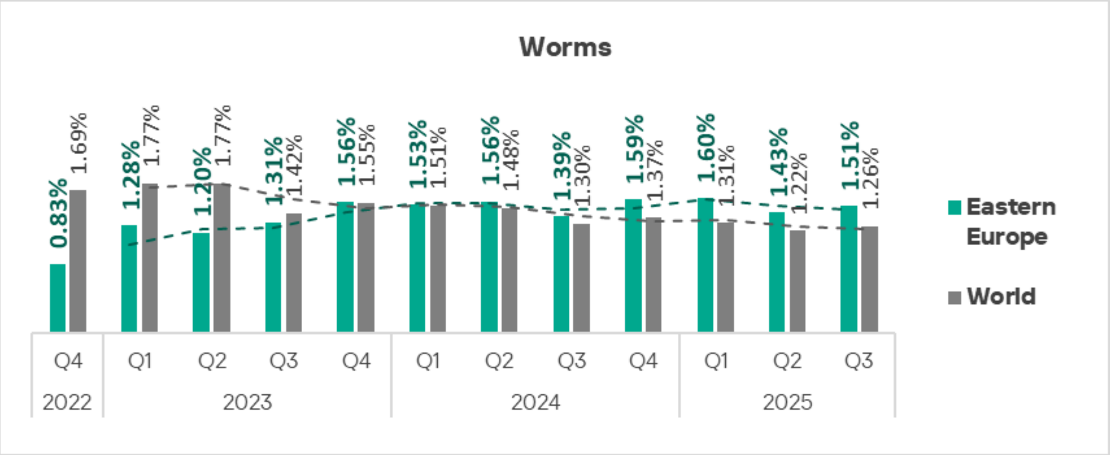


Spyware is blocked in the region across all threat sources, primarily in email clients.

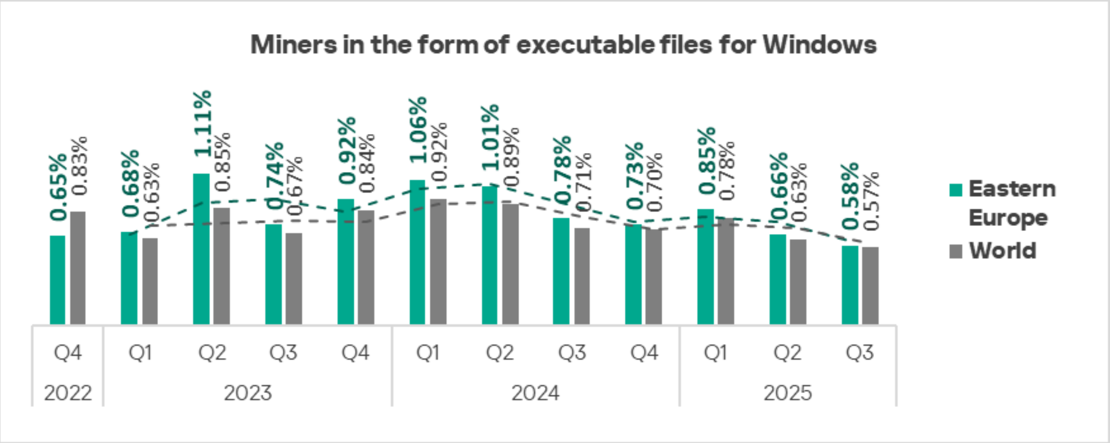
Worms and miners in the form of executable files for Windows

By the percentage of ICS computers with blocked worms, East Europe ranks sixth globally, with 1.51%. This is 6.9 times higher than Northern Europe, which ranks last.

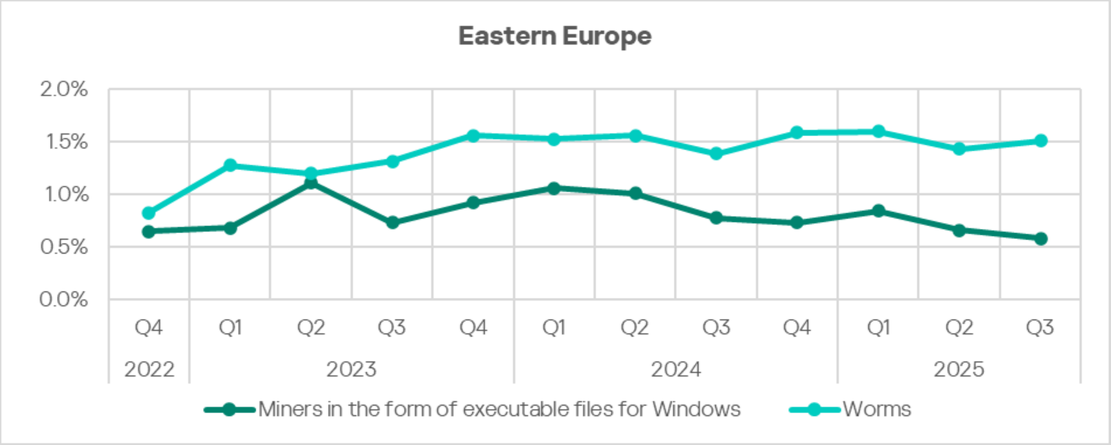
Since the end of 2023, the indicator for worms in the region fluctuates in the range of 1.4–1.6%. In Q3 2025, the percentage of ICS computers on which worms are blocked increased in the region.



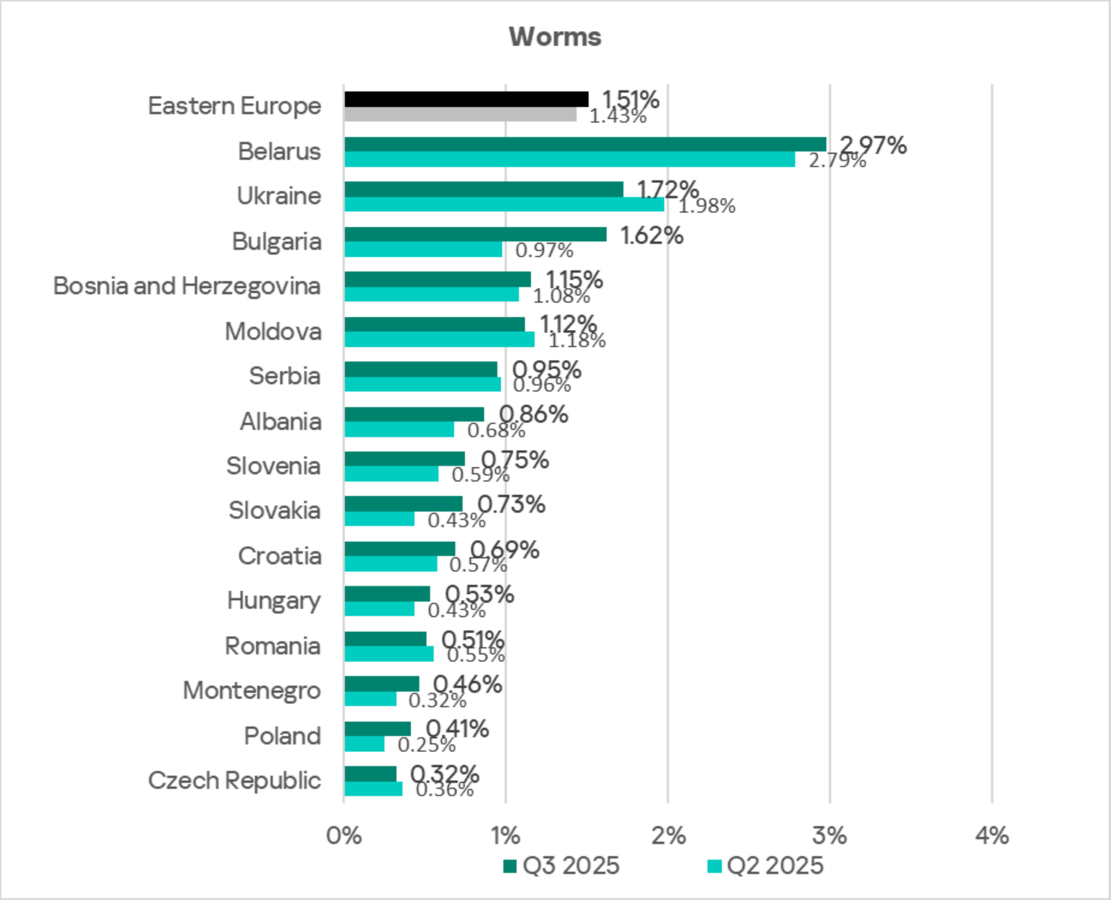
For miners in the form of executable files for Windows, the region ranks third, with 0.58%. This indicator is 4.5 times higher than in the Australia and New Zealand region, which has the lowest figure among regions.



In Eastern Europe, the trends in indicators for miners in the form of executable files and for worms are very similar. This is because miners for Windows use modules and components that are essentially worms and serve to deliver the miner to other computers in the network (automated lateral movement). A similar situation is observed in Russia.

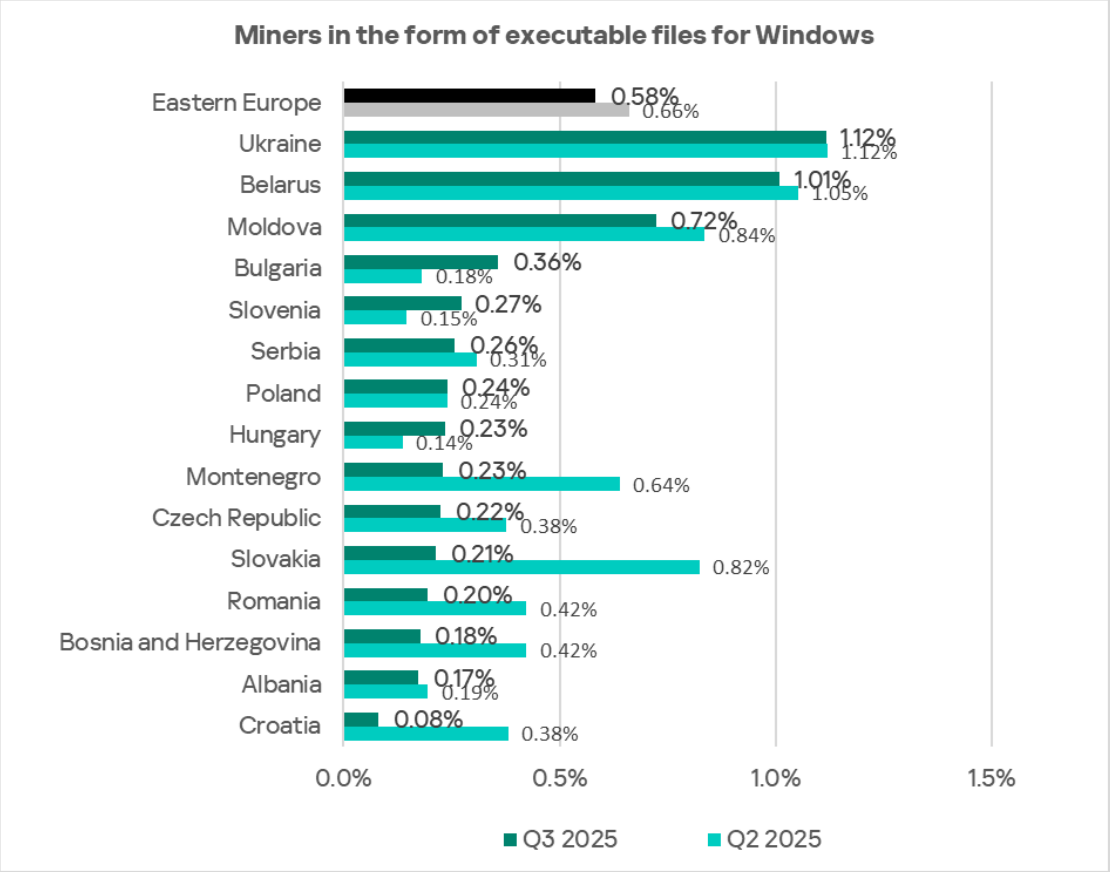


Among countries in the region, Belarus leads with a noticeable margin at 2.97% in the percentage of ICS computers on which worms are blocked.



The top three countries of this ranking, Bulgaria, Ukraine, and Belarus, also lead the ranking of countries in the region in the percentage of ICS computers on which threats were blocked when connecting removable media. This is the main source of worm propagation.

Ukraine and Belarus also lead in the ranking for miners in the form of executable files for Windows with 1.12% and 1.01%, respectively.

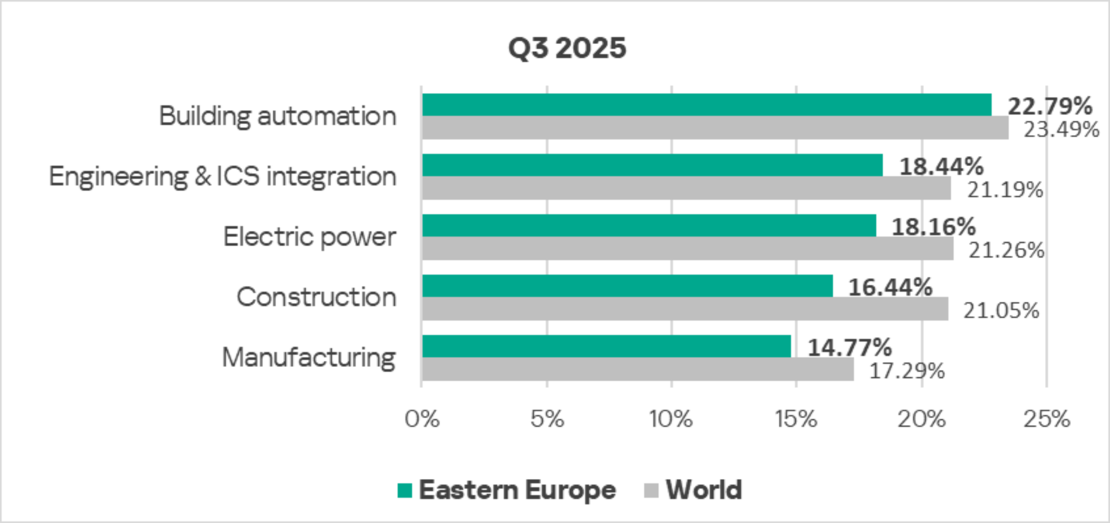


In this ranking, Bulgaria rose from 13th place to fourth place over the quarter.

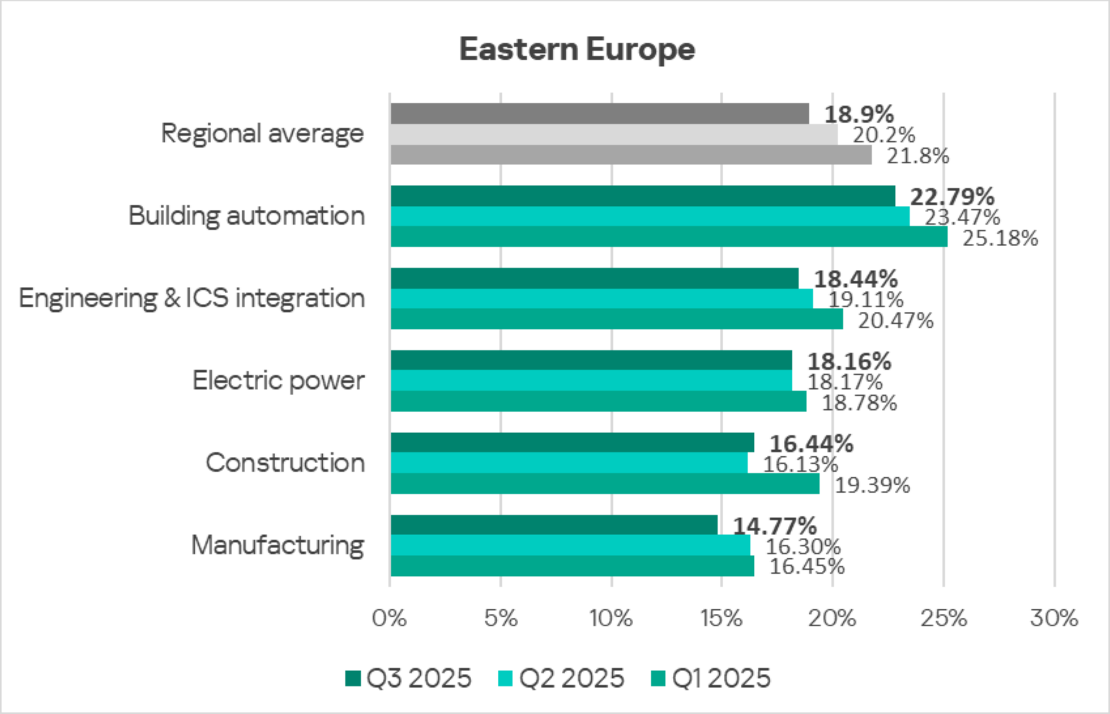
Industries

Of the region's industries considered in this report, building automation is the most frequently targeted.

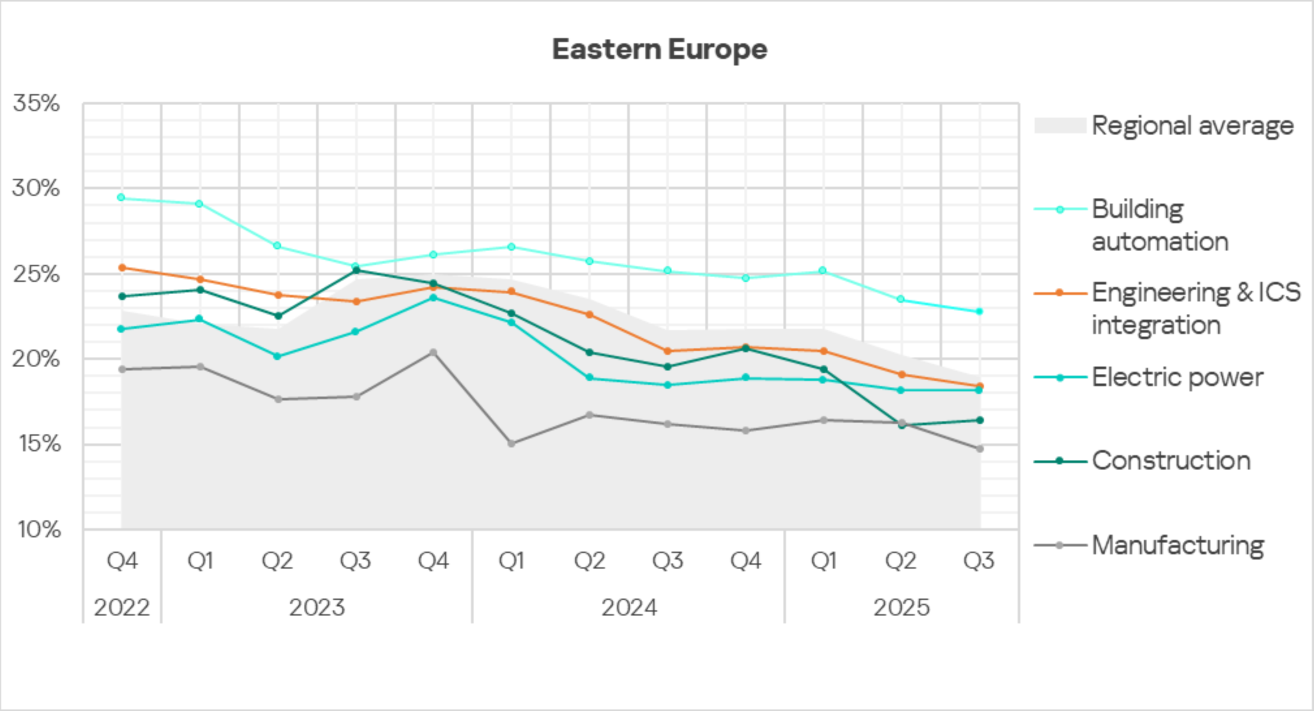
All considered industries show indicators lower than the global averages.



Construction is the only industry in the region where this indicator increased in Q3 2025.



Trends across the reviewed industries suggest stabilization after significant growth in 2022.



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 Eastern Europe, Q3 2025

Industry / Threat source	Building automation	Electric power	Engineering & ICS integration	Construction	Manufacturing	Threat category total in the region
Internet	8.30%	9.57%	8.25%	9.47%	6.78%	7.72%
Email clients	8.05%	3.05%	2.95%	2.14%	2.78%	3.85%
Removable media	0.31%	0.18%	0.13%	0.30%	0.61%	0.20%
Network folders	0.03%	0.00%	0.02%	0.00%	0.00%	0.03%
Industry total in the region	22.79%	18.16%	18.44%	16.44%	14.77%	

Threat category indicators for industries in Eastern Europe, Q3 2025

Industry / Threat category	Building automation	Electric power	Engineering & ICS integration	Construction	Manufacturing	Threat category total in the region
Denylisted internet resources	3.90%	5.13%	4.45%	5.48%	3.51%	4.07%
Malicious scripts and phishing pages (JS and HTML)	10.03%	7.21%	6.33%	5.96%	6.66%	6.63%
Spy Trojans, backdoors and keyloggers	7.95%	3.97%	3.79%	3.28%	3.39%	4.60%
Worms	1.70%	1.29%	1.12%	1.31%	1.57%	1.51%
Miners in the form of executable files for Windows	0.69%	0.46%	0.58%	0.71%	0.36%	0.58%
Malicious documents (MSOffice + PDF)	5.17%	2.13%	2.02%	1.61%	1.82%	2.58%
Viruses	0.56%	0.51%	0.45%	0.71%	0.48%	0.48%
Ransomware	0.25%	0.14%	0.09%	0.12%	0.00%	0.13%
Web miners running in browsers	0.33%	0.14%	0.27%	0.30%	0.12%	0.22%
Malware for AutoCAD	0.03%	0.09%	0.06%	0.36%	0.00%	0.08%
Industry total in the region	22.79%	18.16%	18.44%	16.44%	14.77%	

The high risk of targeted attacks against the technological infrastructures of industrial enterprises is demonstrated by the high indicators for threats that are propagated via email clients (phishing), spyware, and malicious scripts and phishing pages.

All of these signs of high exposure of technological systems to advanced categories of threat actors are present in the indicators of the building automation industry.

Building automation

Eastern Europe ranks seventh globally in the percentage of ICS computers on which malicious objects were blocked in the building automation industry.

In the global rankings by industry in all regions, the building automation industry in Eastern Europe has the following rankings:

- Sixth place in the percentage of computers where malicious documents were blocked.

Based on the industry indicators among regions, Eastern Europe 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 documents, spyware, and miners in the form of executable files for Windows are blocked.
- Fourth place in malicious scripts and phishing pages.

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 network folders were blocked.
- Second place in removable media threats.
- Third for internet threats.
- First place in the following threat categories: malicious scripts and phishing pages, spyware, malicious documents, worms, web miners, and ransomware.
- Second place in miners in the form of executable files for Windows and viruses.

Engineering and ICS integrators

Eastern Europe ranks ninth among regions in the percentage of ICS computers on which malicious objects were blocked in the engineering and ICS integrators industry.

Based on the industry indicators among regions, Eastern Europe has the following rankings:

- Third place in the percentage of ICS computers on which malicious documents were blocked.
- Fourth place in miners in the form of executable files for Windows.

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

- Second place in the percentage of ICS computers on which threats in network folders were blocked.
- Third for threats from email clients.
- Third place in the following threat categories: denylisted internet resources, malicious documents, spyware, miners of both categories, and malware for AutoCAD.

Electrical power

Eastern Europe ranks ninth among regions in the percentage of ICS computers on which malicious objects were blocked in the electrical energy industry.

Based on the industry indicators among regions, Eastern Europe has the following rankings:

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

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

- First place based on the percentage of ICS computers on which internet threats were blocked.
- Second place in email client threats.
- Second place in the percentage of ICS computers on which threats from the following categories were blocked: denylisted internet resources, malicious documents, malicious scripts and phishing pages, spyware, ransomware, and malware for AutoCAD.
- Third place in viruses.

Construction

Eastern Europe ranks eighth among regions in the percentage of ICS computers on which malicious objects were blocked in the construction industry.

Based on the industry indicators among regions, Eastern Europe has the following rankings:

- Third place in the percentage of ICS computers on which denylisted internet resources are blocked.

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

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

Manufacturing

Eastern Europe ranks eighth among regions in the percentage of ICS computers on which malicious objects were blocked in the manufacturing industry.

Based on the industry indicators among regions, Eastern Europe has the following rankings:

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

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

- First place in the percentage of ICS computers on which threats from removable media are blocked.
- Second by percentage of ICS computers on which worms were blocked.
- Third place in denylisted internet resources.

Southern Europe

Key cybersecurity issues in the region

High risk of targeted attacks

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

Threats from email are relevant for all industries of the region, foremost for biometric systems and building automation systems. Attacks on computers in these industrial automation sectors significantly raise the risk of supply-chain attacks on other industries.

Southern Europe leads all regions in the percentage of ICS computers on which threats were blocked in email clients — 2.3 times higher than the global average.

It also ranks second globally in the percentage of ICS computers on which malicious documents were blocked — 1.9 times higher than the global average.

Attackers distribute malicious documents in phishing emails and use them as an initial infection vector. Typically, such documents contain exploits, malicious macros, or harmful links.

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 authentication data for corporate services.

By the percentage of ICS computers on which malicious scripts and phishing pages were blocked, Southern Europe ranks fifth among regions globally, with a rate 1.3 times 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

By the percentage of ICS computers on which spyware was blocked, Southern Europe ranks third, with a rate 1.5 times higher than the global average.

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. In some cases, spyware infections end with ransomware being deployed.

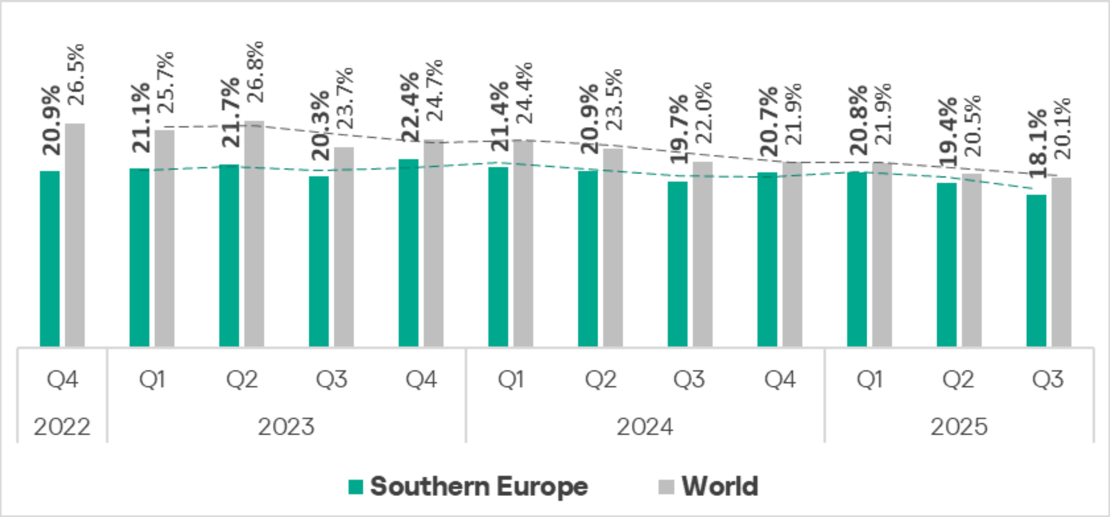
High ransomware rate

The region's percentage of ICS computers on which ransomware was blocked is 1.1 times higher than the global average.

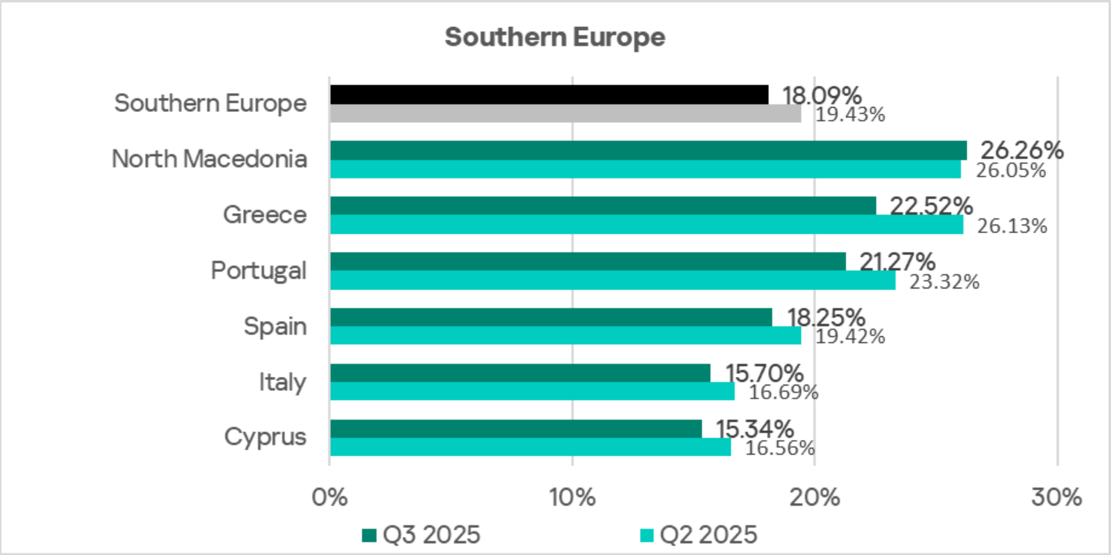
Statistics across all threats

In Q3 2025, Southern Europe ranked ninth globally in the percentage of ICS computers on which malicious objects were blocked.

The figure in the region decreased to its three-year low of 18.1%. This is below the global average but still 2.0 times higher than in Northern Europe, the region with the lowest rate.



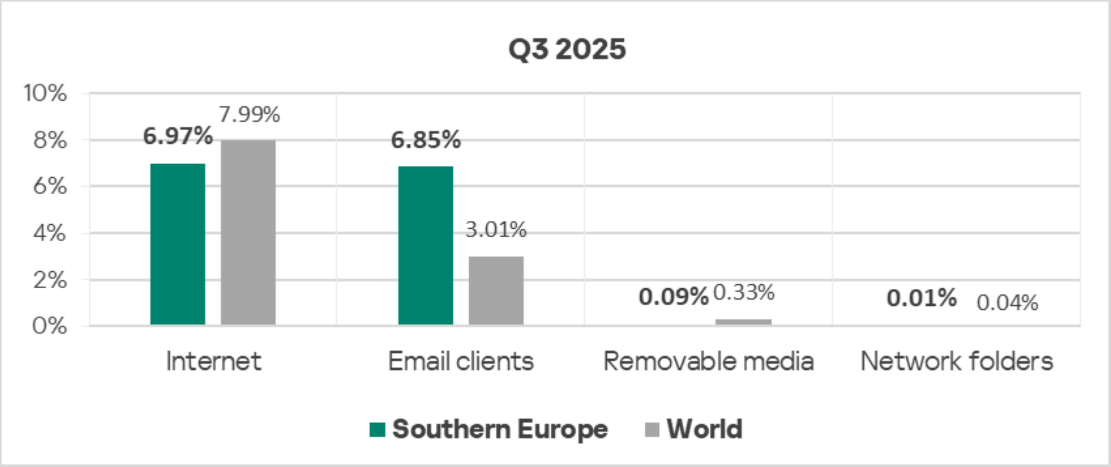
Among the region's countries, North Macedonia leads in the percentage of ICS computers with blocked malicious objects at 26.26%. Over the quarter, this indicator decreased in all countries of the region except North Macedonia.



Threat sources

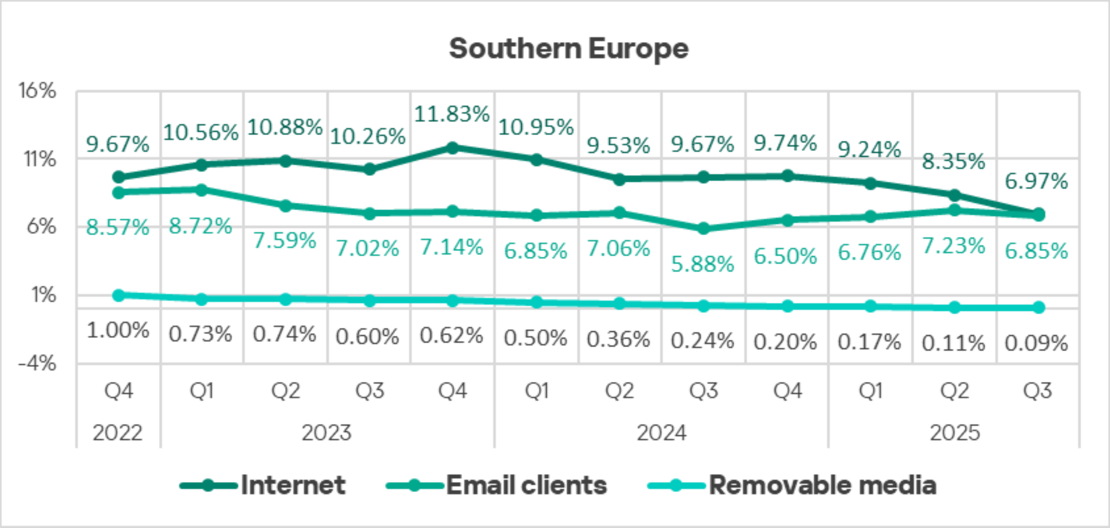
Southern Europe ranks first globally in the percentage of ICS computers on which threats were blocked in email clients. The rate for the region (6.85%) is 2.3 times higher than the global average.

The figures for all other threat sources in Southern Europe are below the global averages.



The main malware distribution channels in the region are the internet and email.

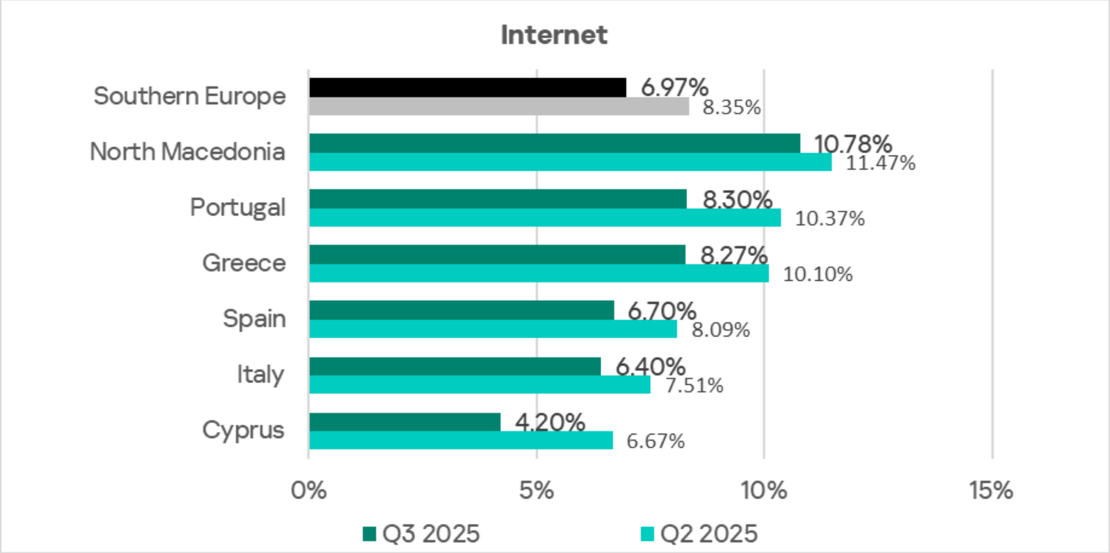
In Q3 2025, the figures for all threat sources decreased.



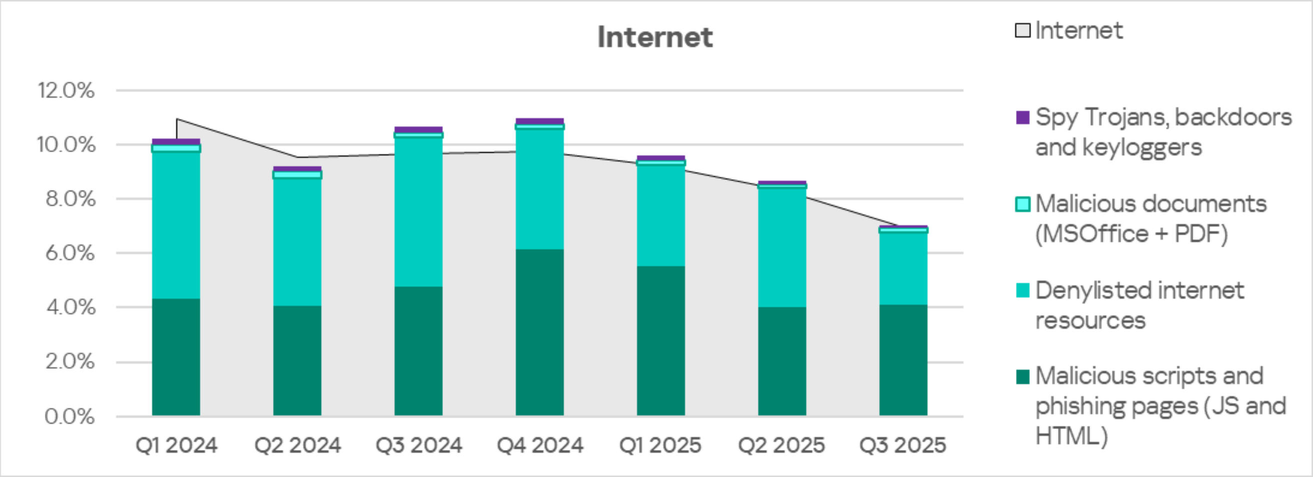
Internet

Based on the percentage of ICS computers on which internet threats are blocked, Southern Europe ranks eighth globally at 6.97%, which is 1.5 times higher than the lowest figure (Northern Europe).

The figures for countries of the region decreased in all countries and vary from 4.20% in Cyprus to 10.78% in North Macedonia.

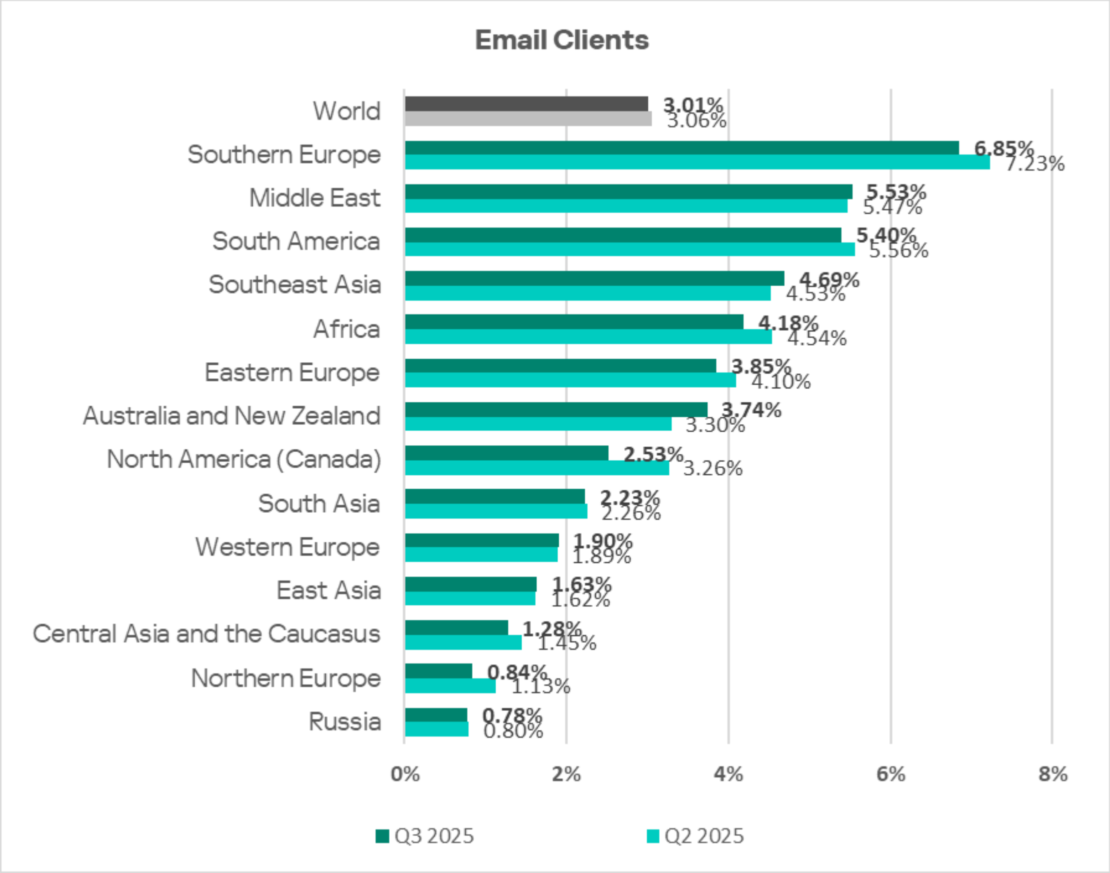


The main categories of internet threats blocked on ICS computers in the region are denylisted internet resources and malicious scripts and phishing pages.

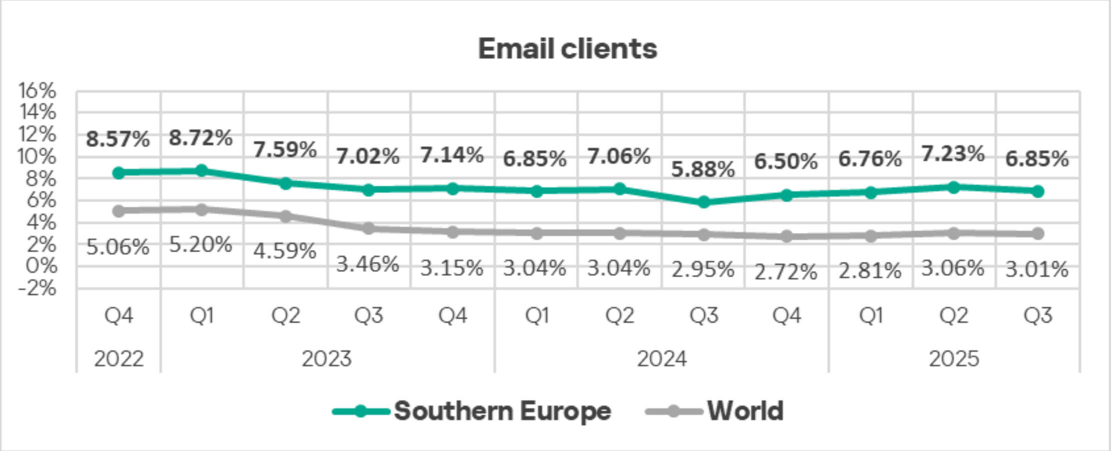


Email clients

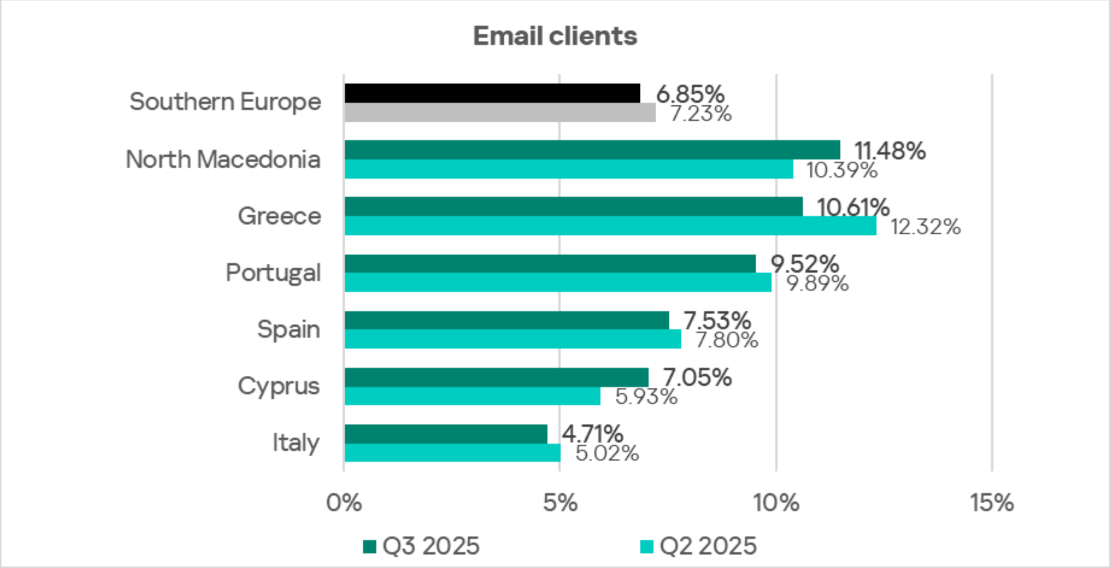
By the percentage of ICS computers on which threats from email clients were blocked, Southern Europe leads globally, with 6.85% in Q3 2025. This figure is 8.8 times higher than in Russia, which ranks last.



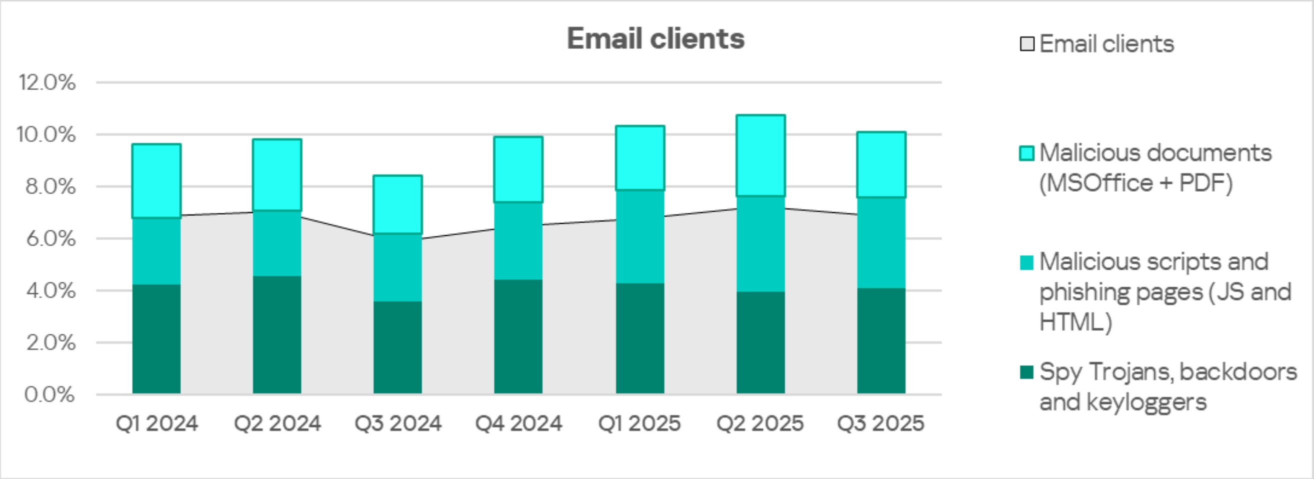
The percentage of ICS computers on which threats in email clients were blocked in Southern Europe rose during the previous three quarters but decreased in Q3 2025.



Among countries in the region, North Macedonia leads with 11.48% in the percentage of ICS computers on which email client threats were blocked. The lowest figure observed was in Italy at 4.71%.



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

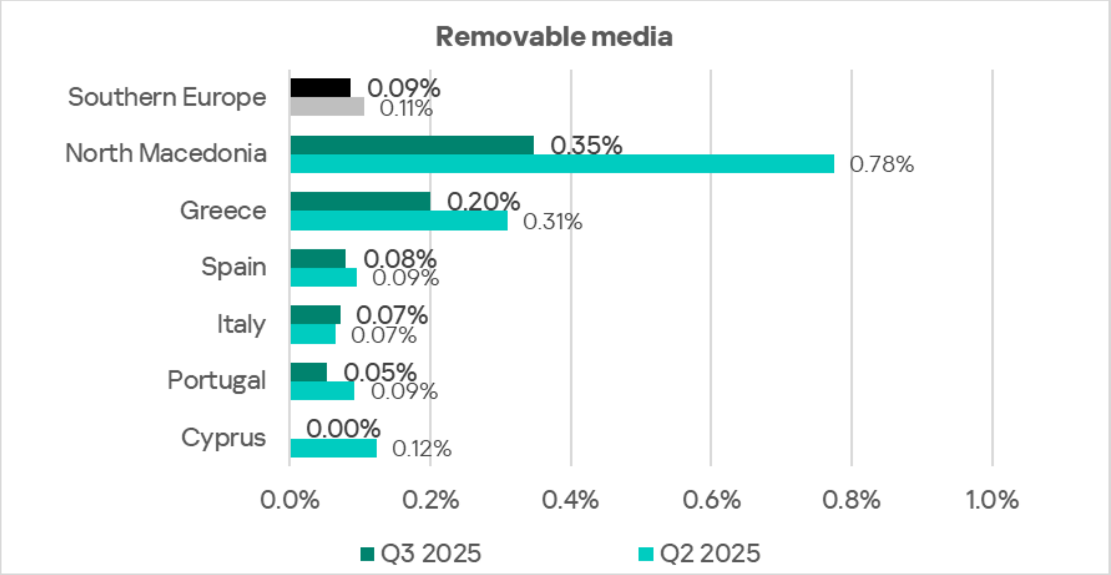


Based on the percentage of ICS computers on which malicious documents are blocked, Southern Europe ranks second globally.

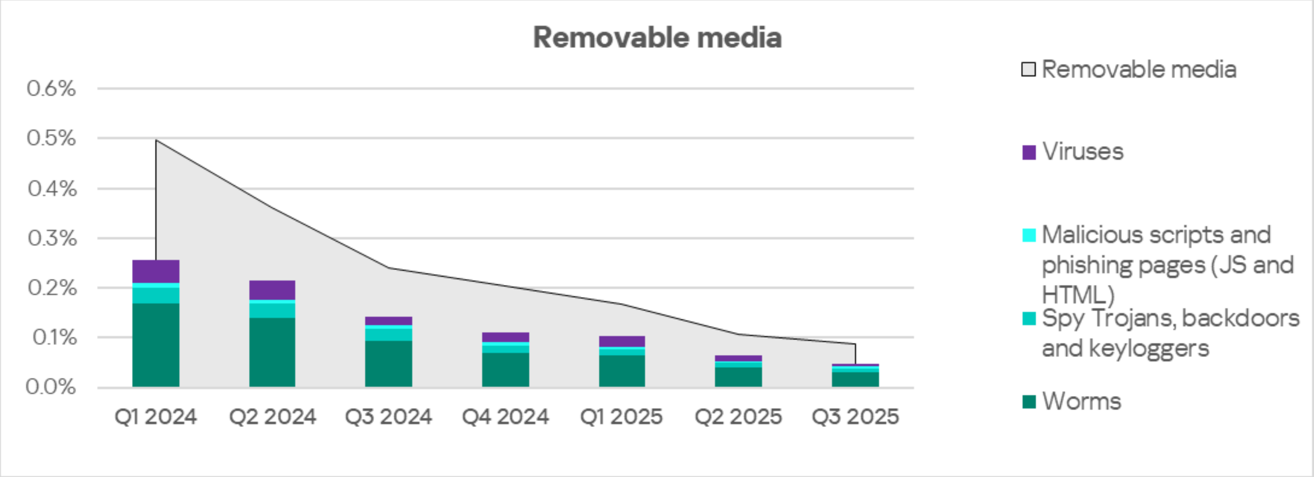
Removable media

By the percentage of ICS computers on which threats were blocked when connecting removable media, Southern Europe ranks 10th among regions in Q3 2025. The regional figure (0.09%) is 1.8 times higher than that in Australia and New Zealand, which rank last.

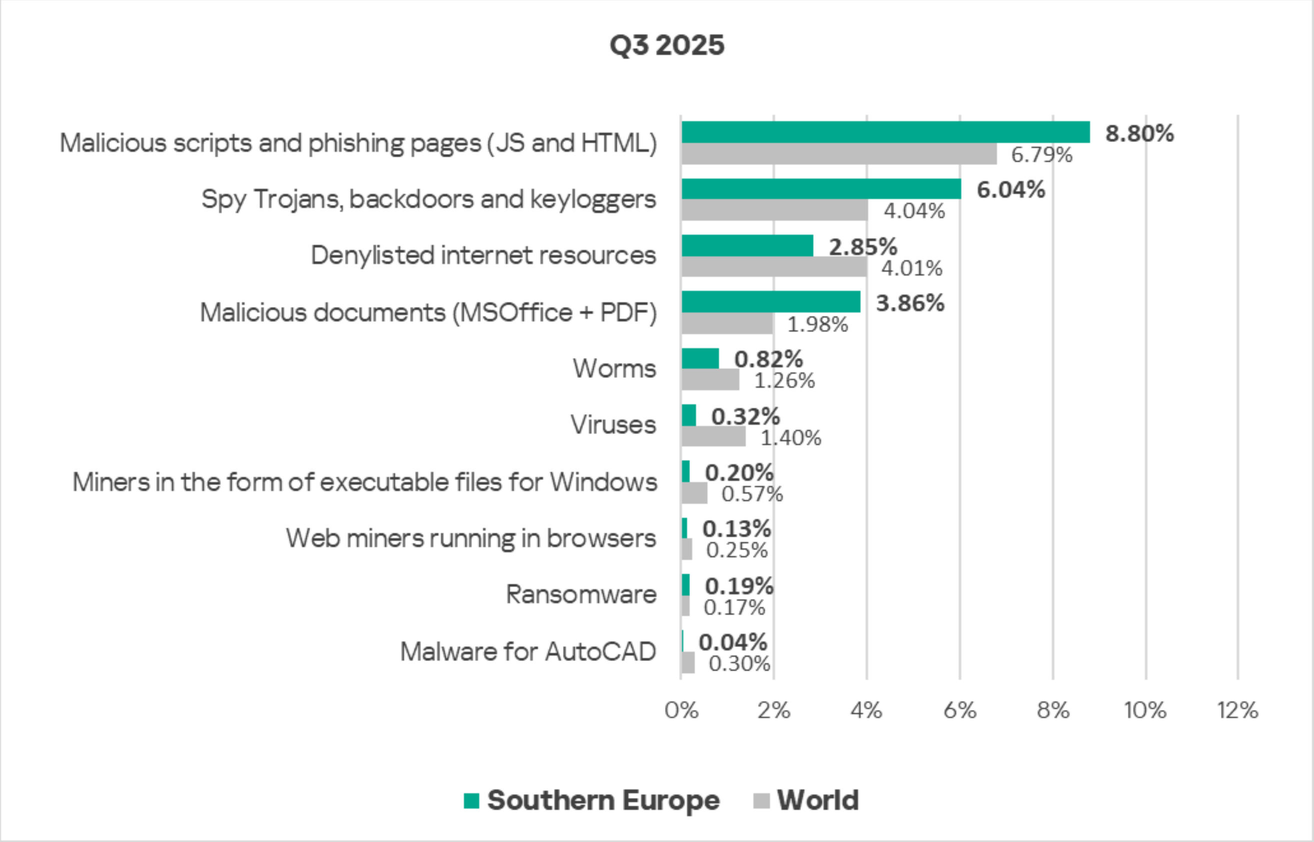
Among countries in the region, North Macedonia leads in the percentage of ICS computers on which removable media threats were blocked on connection at a rate of 0.35%. This indicator decreased in all countries of the region except Italy.

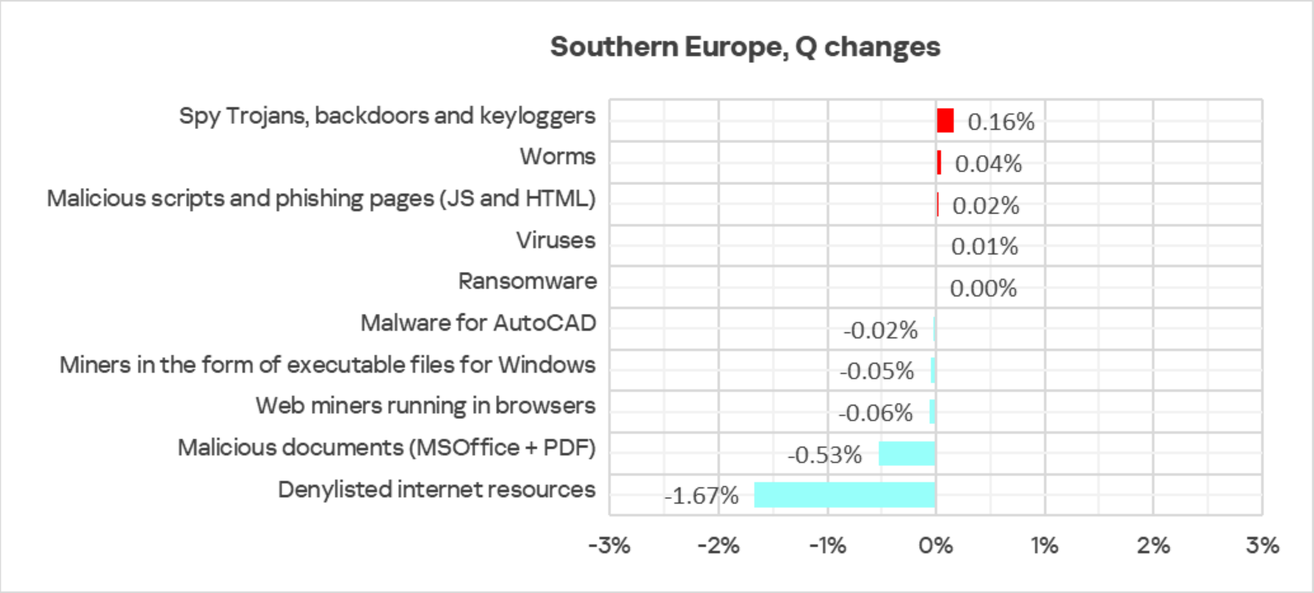


The main categories of threats blocked when connecting removable media to ICS computers are worms, spyware, viruses, and malicious scripts and phishing pages.



Threat categories





Compared to the global averages, Southern Europe has higher percentages of ICS computers with the following categories of threats blocked:

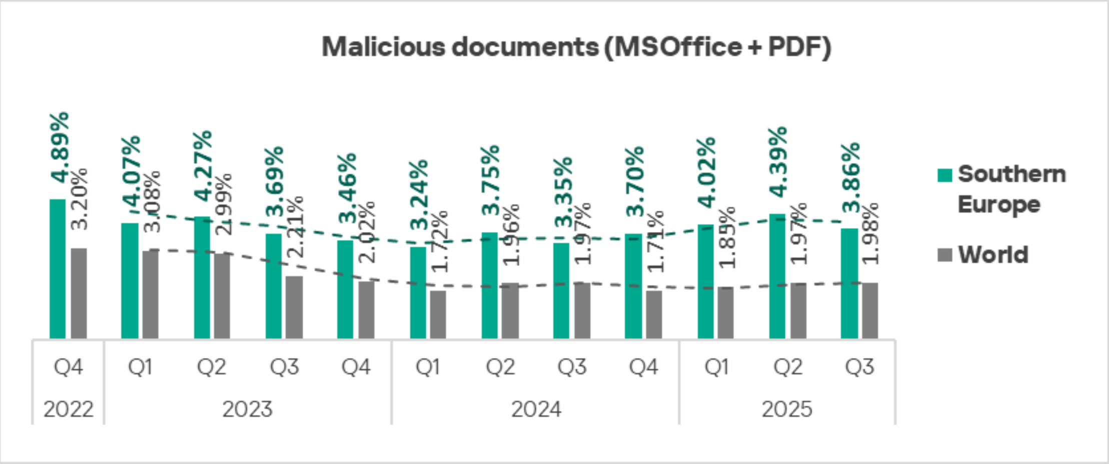
- Malicious documents: 1.9 times higher.
- Spyware: 1.5 times higher.
- Malicious scripts and phishing pages: 1.3 times higher.
- Ransomware: 1.1 times higher.

Attackers use malicious scripts, phishing pages, and malicious documents to deliver targeted malware, including spyware and ransomware**.**

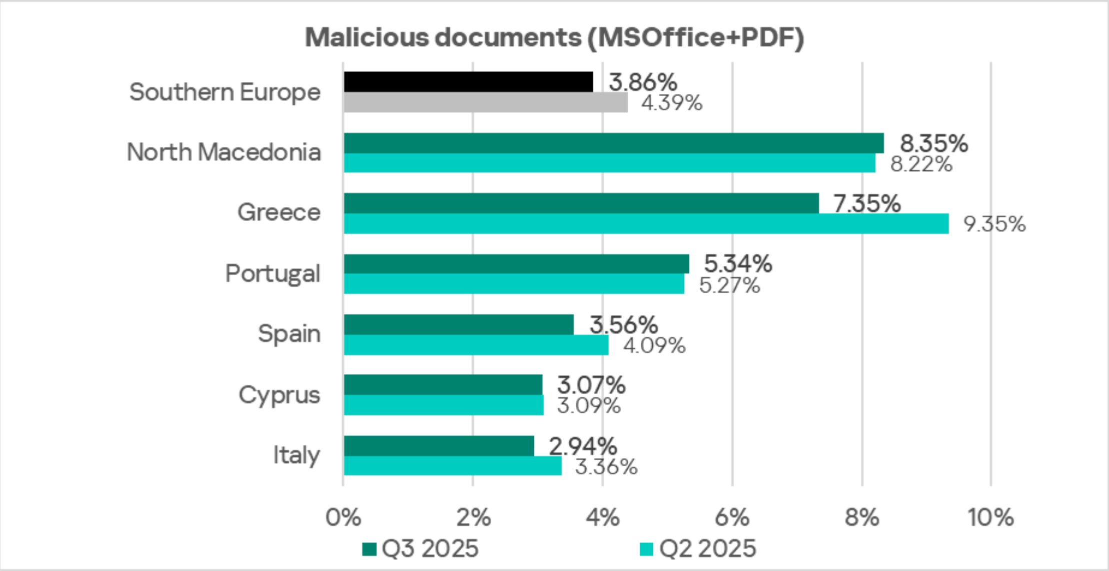
Malicious documents

Over the past three quarters, Southern Europe leads globally based on the percentage of ICS computers on which malicious documents are blocked. In Q3 2025, South America regained its lead while Southern Europe occupied second place in this ranking with 3.86%. This figure is 7.3 times higher than in Northern Europe, which boasts the lowest percentage among all regions.

The percentage of ICS computers on which malicious documents are blocked grew three quarters in a row in the region, but decreased in Q3 2025.



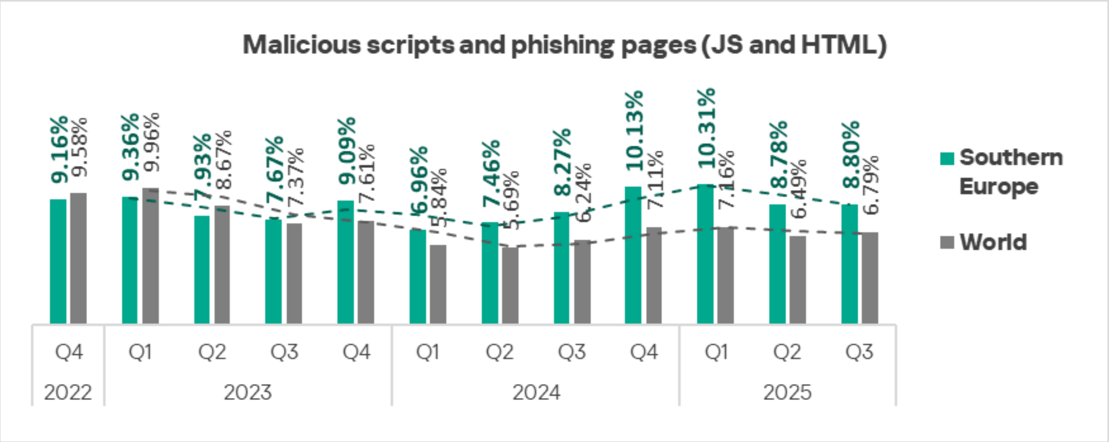
Among the region's countries, North Macedonia leads with 8.35% in the percentage of ICS computers on which malicious documents are blocked. Over the quarter, this indicator decreased in all countries of the region except Portugal and North Macedonia.



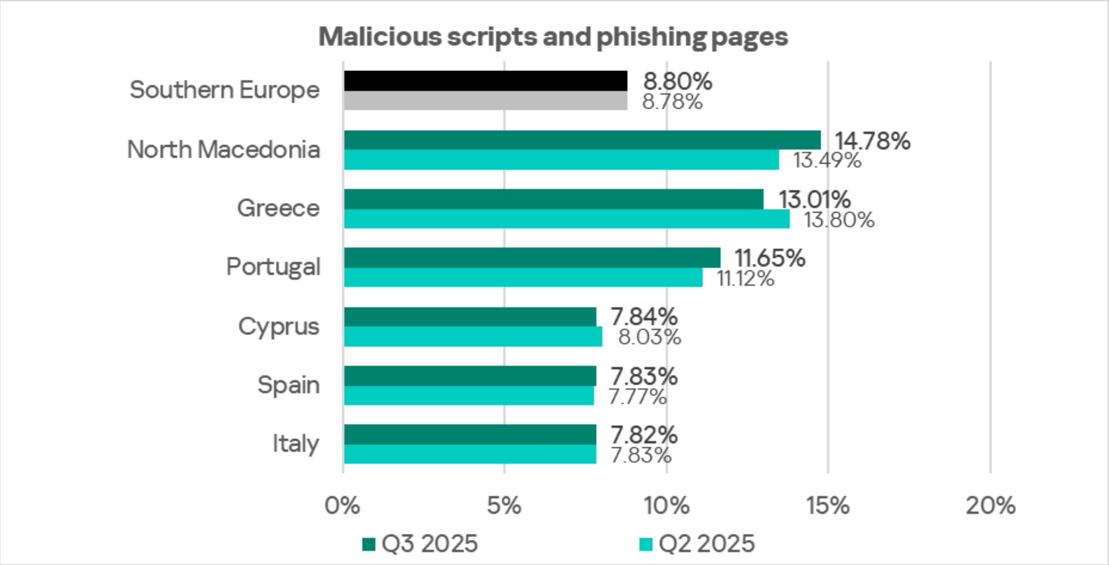
Malicious documents are distributed primarily via email.

Malicious scripts and phishing pages

Based on the percentage of ICS computers on which malicious scripts and phishing pages are blocked, Southern Europe dropped from second place to fifth place with 8.80%. This figure is 3.4 times higher than in Northern Europe, which has the lowest rate.



Among countries in the region, North Macedonia leads with 14.78% in the percentage of ICS computers on which malicious scripts and phishing pages were blocked.

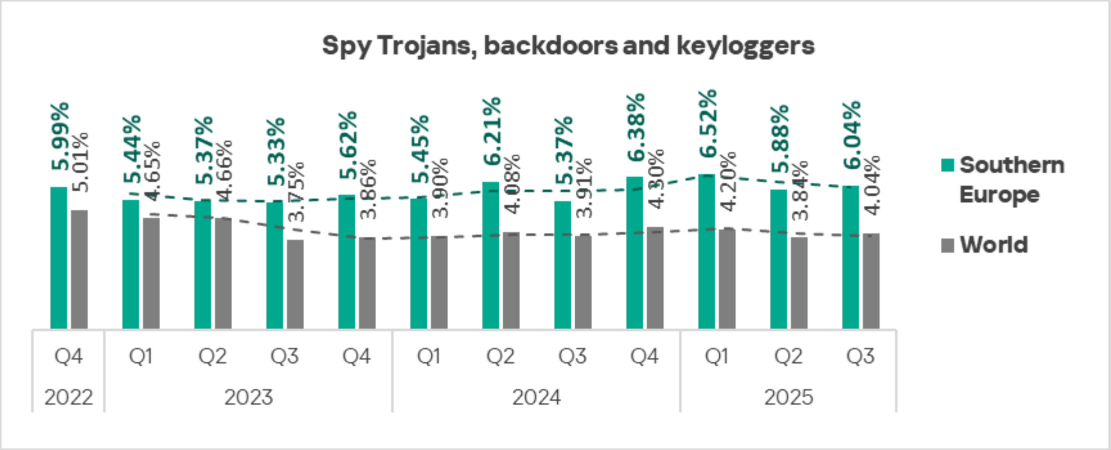


Malicious scripts and phishing pages spread both via the internet and through email.

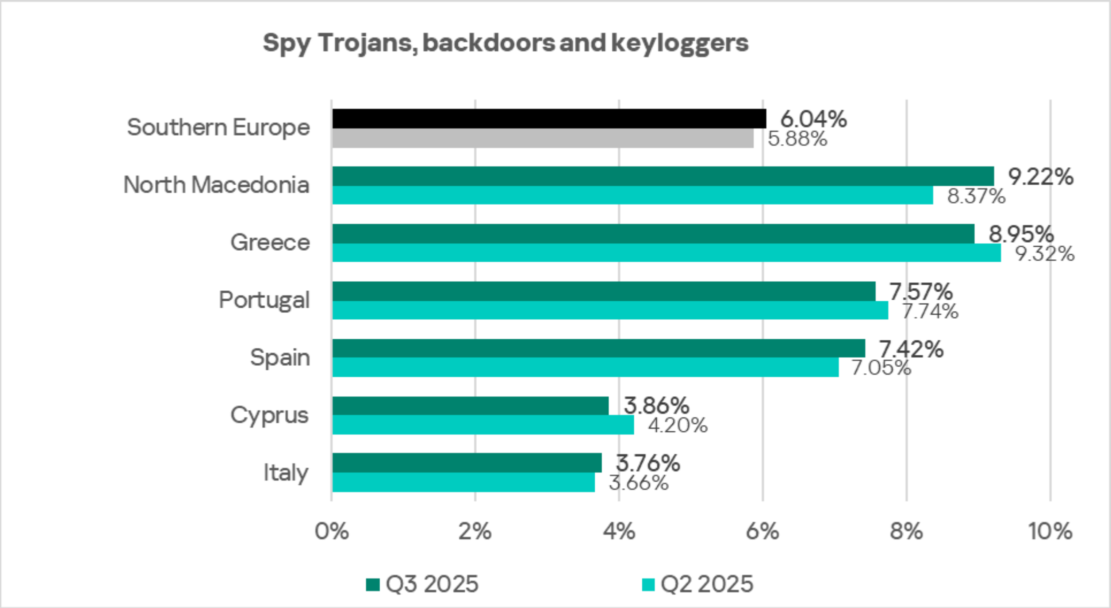
Spyware

Based on the percentage of ICS computers on which spyware is blocked, Southern Europe ranks third globally, behind only Africa and Southeast Asia.

The percentage of ICS computers on which spyware is blocked in Southern Europe fluctuates, and this indicator grew to 6.04% in Q3 2025. This figure is 4.3 times higher than in Northern Europe, which boasts the lowest percentage among all regions.



Among the region's countries, North Macedonia leads in the percentage of ICS computers on which spyware was blocked at 9.22%. Over the quarter, this indicator grew in North Macedonia, Spain, and Italy.

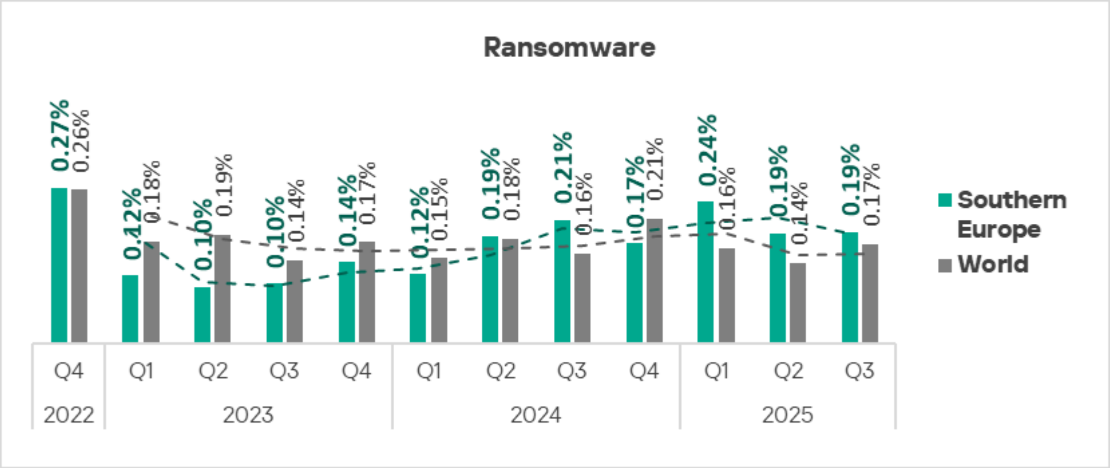


The main source of spyware in the region is email, though it is also encountered on the internet. You may recall that Southern Europe leads the global ranking in the percentage of ICS computers on which email threats were blocked.

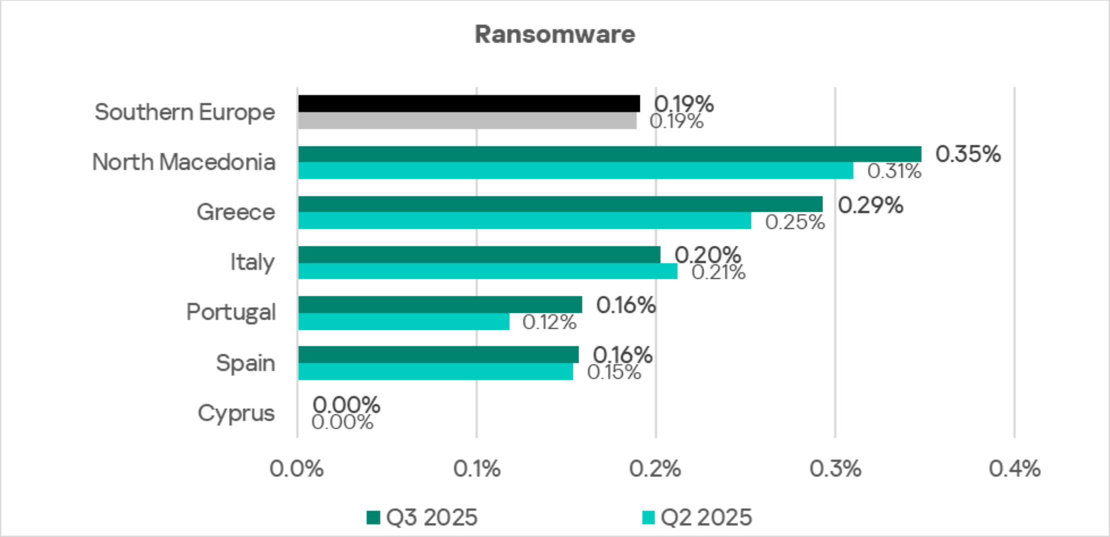
Ransomware

By the percentage of ICS computers on which ransomware was blocked, Southern Europe ranks fifth globally at 0.19%. This is 3.8 times higher than Northern Europe, which ranks last.

The indicator in the region fluctuates, but it did not change over the quarter.



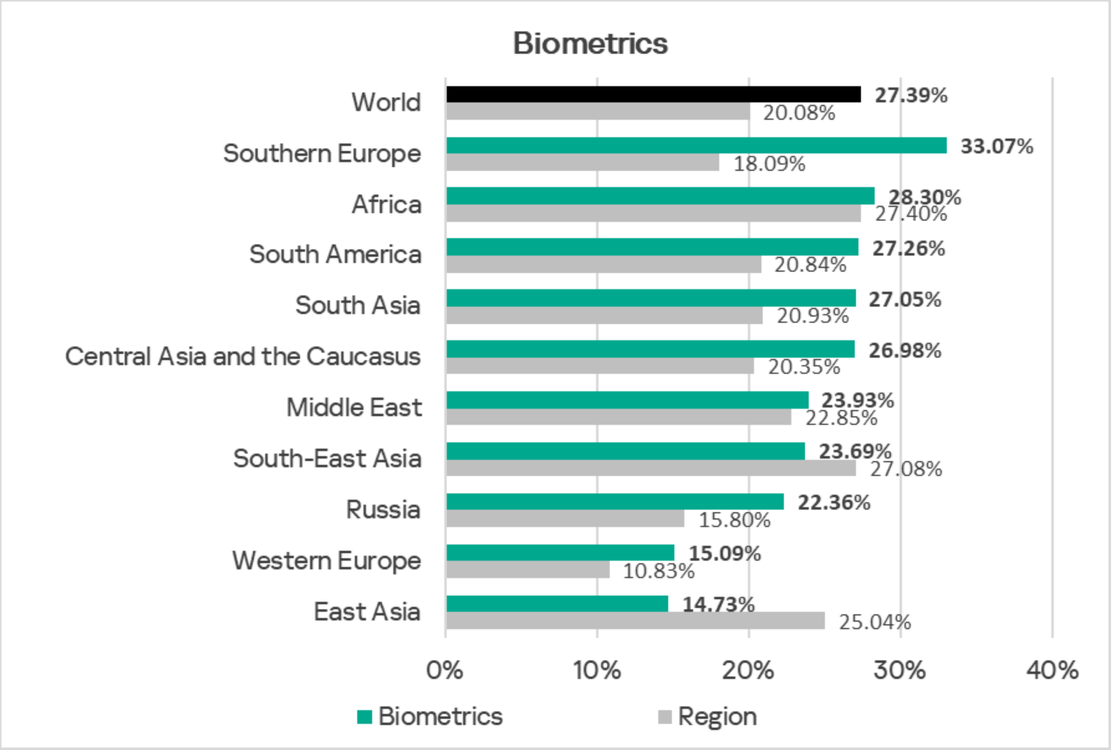
Among the region's countries, North Macedonia leads in the percentage of ICS computers on which ransomware is blocked with 0.35%. Over the quarter, the indicator increased in all countries except Italy.



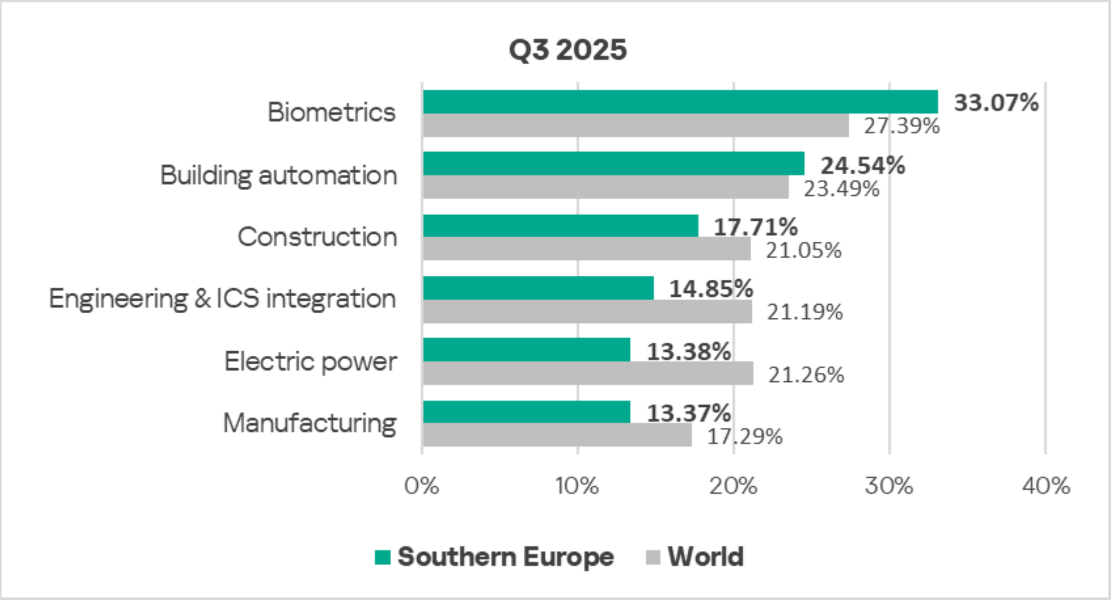
Industries

In Southern Europe, of all the industries and OT infrastructures covered in the report, malicious objects are most often blocked in biometric systems.

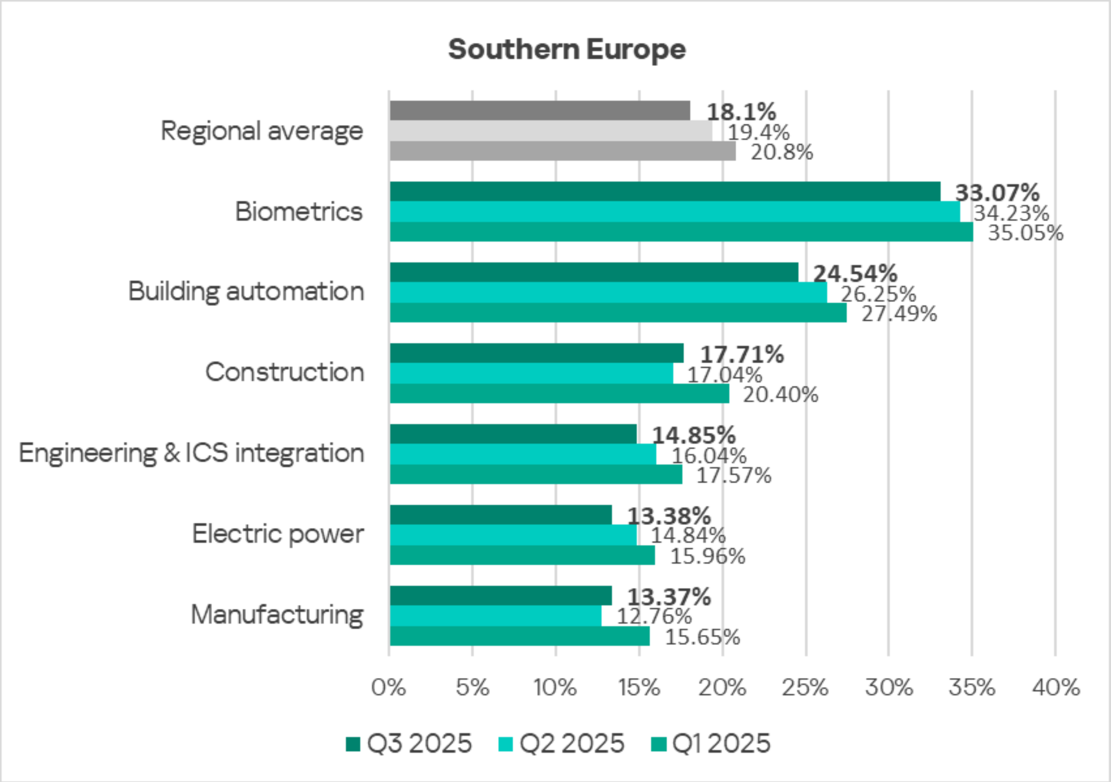
Southern Europe leads among regions in biometric systems.



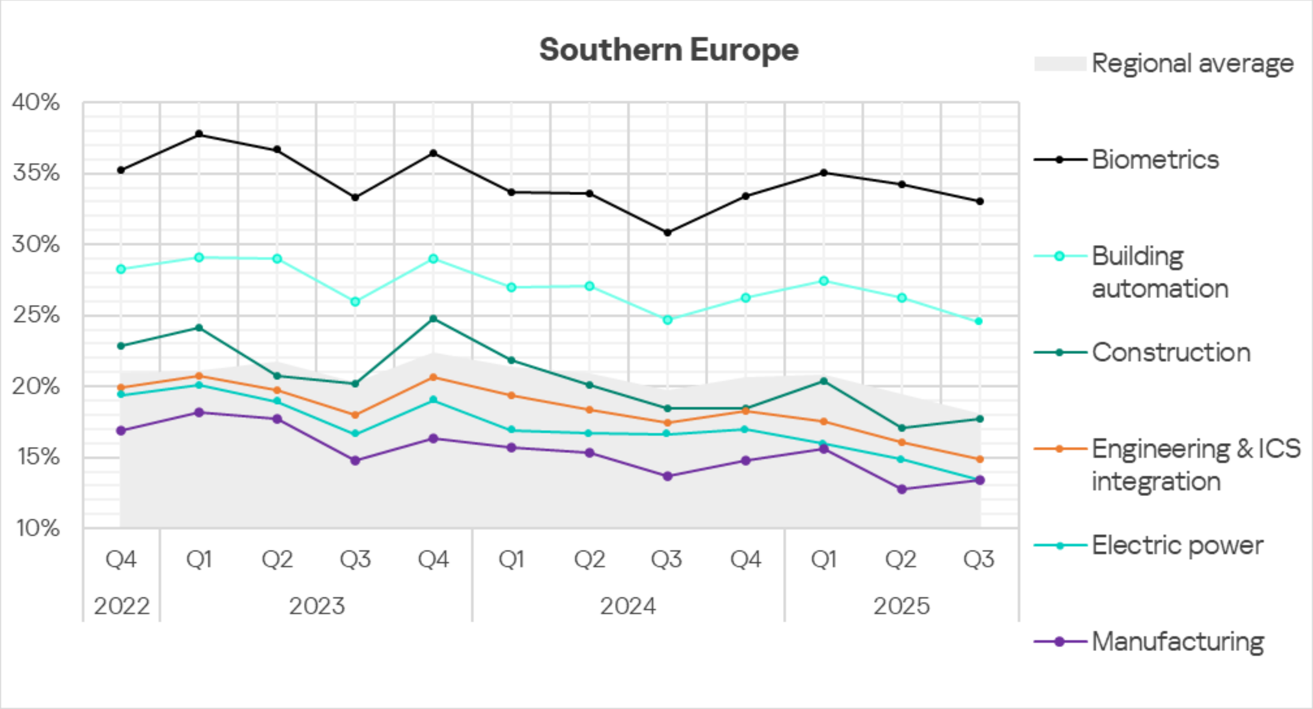
In Southern Europe, the percentage of ICS computers on which malicious objects were blocked is higher than the global averages in the OT infrastructure for biometric systems (by a factor of 1.2) and the building automation industry.



In Q3 2025, out of all the industries studied, the percentage of ICS computers on which malicious objects were blocked increased in the construction industry and in the manufacturing industry.



All studied industries demonstrate fluctuating trends in the percentage of ICS computers on which malicious objects were blocked. However, for biometric systems and building automation, the figures are significantly higher than the average for the region.



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 Southern Europe, Q3 2025

Industry / Threat source	Biometrics	Building automation	Electric power	Engineering & ICS integration	Construction	Manufacturing	Threat category total in the region
Internet	7.39%	7.28%	6.40%	6.59%	7.11%	4.43%	6.97%
Email clients	20.44%	12.71%	2.84%	4.18%	5.33%	3.34%	6.85%
Removable media	0.14%	0.09%	0.02%	0.07%	0.06%	0.11%	0.09%
Network folders	0.00%	0.02%	0.00%	0.01%	0.00%	0.00%	0.01%
Industry total in the region	33.07%	24.54%	13.38%	14.85%	17.71%	13.37%	

Threat category indicators for industries in Southern Europe, Q3 2025

Industry / Threat category	Biometrics	Building automation	Electric power	Engineering & ICS integration	Construction	Manufacturing	Threat category total in the region
Denylisted internet resources	2.48%	2.73%	2.65%	2.76%	3.28%	1.71%	2.85%
Malicious scripts and phishing pages (JS and HTML)	16.39%	13.14%	5.95%	6.94%	7.66%	4.87%	8.80%
Spy Trojans, backdoors and keyloggers	18.73%	11.07%	2.99%	3.69%	4.16%	3.85%	6.04%
Worms	2.09%	1.27%	0.66%	0.58%	0.44%	1.05%	0.82%
Miners in the form of executable files for Windows	0.27%	0.23%	0.24%	0.19%	0.11%	0.18%	0.20%
Malicious documents (MSOffice + PDF)	10.31%	7.71%	1.52%	2.23%	2.67%	2.11%	3.86%
Viruses	0.35%	0.46%	0.24%	0.18%	0.44%	0.15%	0.32%
Ransomware	0.51%	0.40%	0.09%	0.11%	0.00%	0.15%	0.19%
Web miners running in browsers	0.19%	0.16%	0.19%	0.14%	0.11%	0.11%	0.13%
Malware for AutoCAD	0.00%	0.03%	0.02%	0.02%	0.17%	0.00%	0.04%
Industry total in the region	33.07%	24.54%	13.38%	14.85%	17.71%	13.37%	

Southern Europe ranks first globally in the percentage of ICS computers on which threats were blocked in email clients. Email clients are a pertinent source of threats for all industries in the region.

In the percentage of ICS computers on which threats were blocked in email clients in different industries, Southern Europe has the following global rankings:

- First place in the OT infrastructure for biometric systems, the building automation industry, and the engineering and ICS integrators industry.
- Second place in the construction industry and manufacturing industry.
- Fourth place in the electrical energy industry.

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

The risk of targeted attacks is relevant for all industries of the region, to a lesser extent for the electrical energy industry and to a greater extent for biometric systems and building automation systems. Attacks on computers in these industrial automation sectors significantly raise the risk of supply-chain attacks on other industries.

In the percentage of ICS computers on which malicious documents are blocked in different industries, Southern Europe has the following global rankings:

- First place in the OT infrastructure for biometric systems and the building automation industry.
- Third place in the following three industries: construction, engineering and ICS integrators, and manufacturing.

In the percentage of ICS computers on which spyware is blocked in different industries, Southern Europe has the following global rankings:

- First place in the OT infrastructure for biometric systems and the building automation industry.
- Fourth place in the construction industry and manufacturing industry.

Based on the percentage of ICS computers on which ransomware is blocked in OT infrastructure for biometric systems and in the building automation industry, Southern Europe ranks fourth globally.

Biometric systems

Southern Europe ranks first among regions in the percentage of ICS computers on which malicious objects were blocked in the OT infrastructure for biometric systems.

Globally across all industries in all regions, the OT infrastructure for biometric systems in Southern Europe has the following rankings:

- First place in email client threats.
- First place in the percentage of computers where the following threat categories were blocked: malicious scripts and phishing pages, and malicious documents.

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

- First place in the percentage of ICS computers on which internet threats and email client threats are blocked.
- First place in the percentage of ICS computers on which the following threat categories are blocked: malicious documents, malicious scripts and phishing pages, and spyware.
- Third place in ransomware.

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

- First place in the percentage of ICS computers on which threats from the internet, email clients, and removable media were blocked.
- First place in the following threat categories: malicious scripts and phishing pages, spyware, malicious documents, worms, both types of miners, and ransomware.
- Third place in viruses.

Building automation

Southern Europe is in fifth place among regions based on the percentage of ICS computers on which malicious objects were blocked in the building automation industry.

Globally across all industries in all regions, the building automation industry in Southern Europe has the following rankings:

- Second place in email client threats.
- Second place in the percentage of computers where malicious scripts and phishing pages were blocked.

Based on industry indicators among regions, Southern Europe has the following rankings:

- First by percentage of ICS computers on which threats from email clients were blocked.
- First place in the percentage of ICS computers on which the following threat categories are blocked: malicious documents, malicious scripts and phishing pages, and spyware.

- Third place in ransomware.

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

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

Construction

Southern Europe is seventh among regions in the percentage of ICS computers on which malicious objects were blocked in the construction industry.

Based on industry indicators among regions, Southern Europe has the following rankings:

- Second 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 documents were blocked.
- Fourth place for spyware.

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

- 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 denylisted internet resources and malware for AutoCAD were blocked.
- Second place for viruses.
- Third place in the following threat categories: malicious scripts and phishing pages, spyware, and malicious documents.

Engineering and ICS integrators

Southern Europe is 10th among regions in the percentage of ICS computers on which malicious objects were blocked in the engineering and ICS integrators industry.

Based on the engineering and ICS integrators industry indicators among regions, Southern Europe has the following rankings:

- First by percentage of ICS computers on which threats from email clients were blocked.
- Third place in the percentage of ICS computers on which malicious documents were blocked.
- Fourth place in miners in the form of executable files for Windows.

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

- Second place in the percentage of ICS computers on which threats in network folders were blocked.
- Second place in denylisted internet resources.
- Third in terms of malware for AutoCAD.

Electrical power

Southern Europe is 10th 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, Southern Europe has the following rankings:

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

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

- Second for miners from both categories.

Manufacturing

Southern Europe is 11th among regions in the percentage of ICS computers on which malicious objects were blocked in the manufacturing industry.

Based on industry indicators among regions, Southern Europe has the following rankings:

- Second 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 documents were blocked.
- Fourth place for spyware.

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

- Second place in the percentage of ICS computers on which threats were blocked when connecting removable media.
- Third place in the percentage of ICS computers on which worms and ransomware were blocked.

Western Europe

Key cybersecurity issues in the region

Western Europe is one of the safest regions in terms of cybersecurity.

In Q3 2025, it ranked 13th globally by the percentage of ICS computers on which malicious objects were blocked.

In Western Europe, threat categories that showed any growth in Q3 2025 often represented key elements of a broader kill chain, particularly in targeted attacks. These included malicious scripts and phishing pages, spyware, and ransomware.

- Attackers employ malicious scripts for a wide range of purposes, including data collection and tracking, redirecting users to malicious web resources, and downloading additional malware — such as spyware — onto the system or browser.
- Spyware is used by attackers to steal confidential data, including information required to deliver other types of malware, such as ransomware.

Biometric systems (data collection, processing, and storage) in Western Europe led all industries across all regions in terms of the percentage of computers where ransomware was blocked.

Self-propagating malware (worms and viruses) rates increased in Western Europe, as did malware for AutoCAD — capable of active propagation by infecting all AutoCAD projects accessible on the computer.

Indicators for removable media and network folders increased accordingly, as these were the main sources through which worms, viruses, and malware for AutoCAD spread.

By the percentage of ICS computers on which network folder threats were blocked, Western Europe ranked fourth globally in two industries: electric power, and engineering and ICS integration.

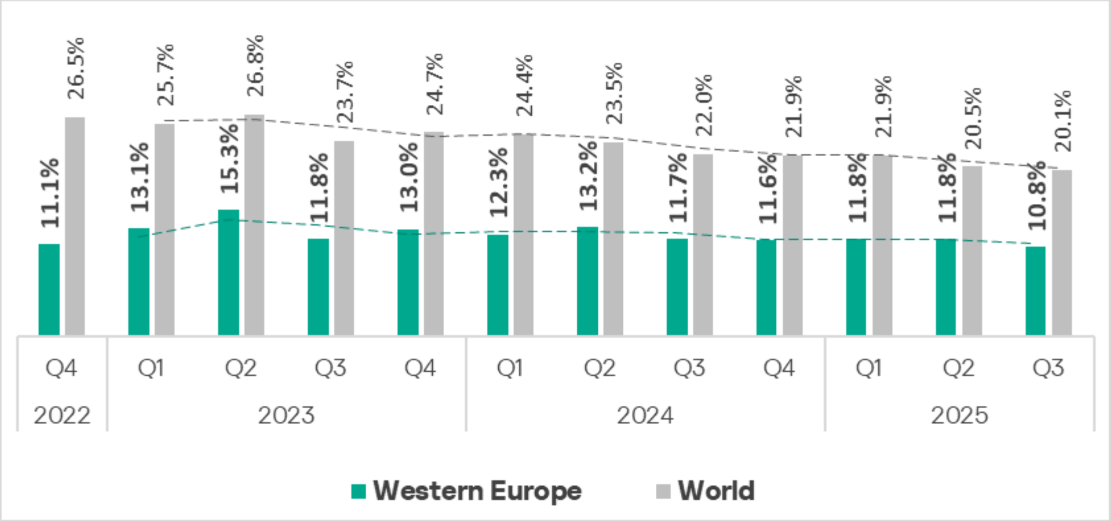
The percentage of ICS computers on which threats from email clients were blocked also increased in the region. Email is one of the channels used to distribute malicious scripts and the primary channel for spreading spyware.

Western Europe was 10th in the global rankings for threats originating from email clients, eighth for network folder threats; and ninth for the percentage of ICS computers on which denylisted internet resources were blocked.

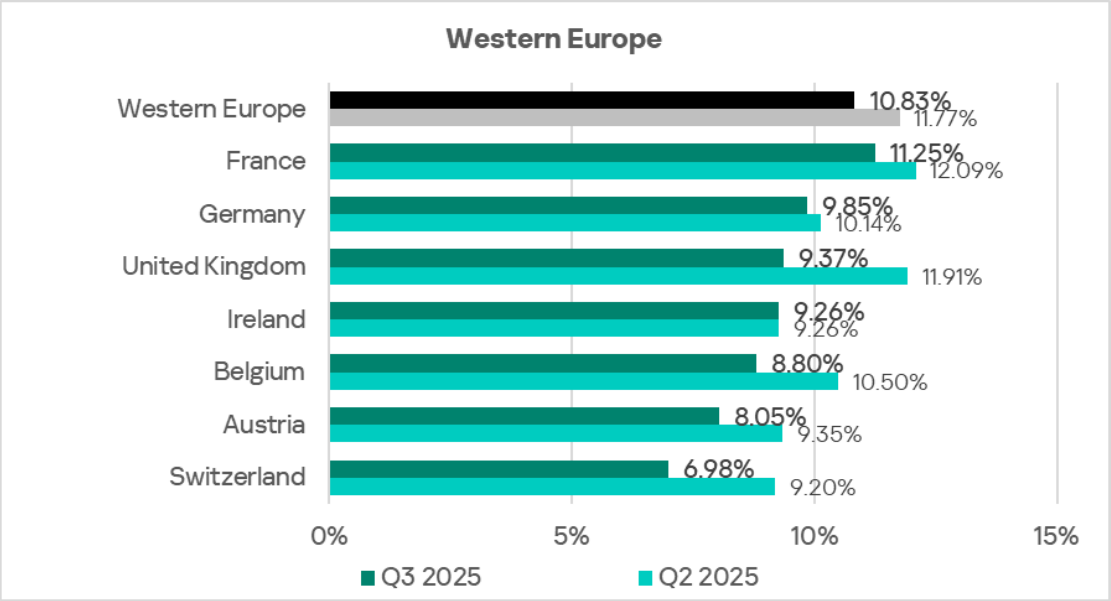
Across all other metrics — whether analyzed by source or by threat category — Western Europe ranked no higher than 11th place.

Statistics across all threats

In Q3 2025, it ranked 13th globally by the percentage of ICS computers on which malicious objects were blocked. This figure decreased from 11.8% to 10.8%. This is significantly below the global average but still 1.2 times higher than Northern Europe, the region with the lowest rate.

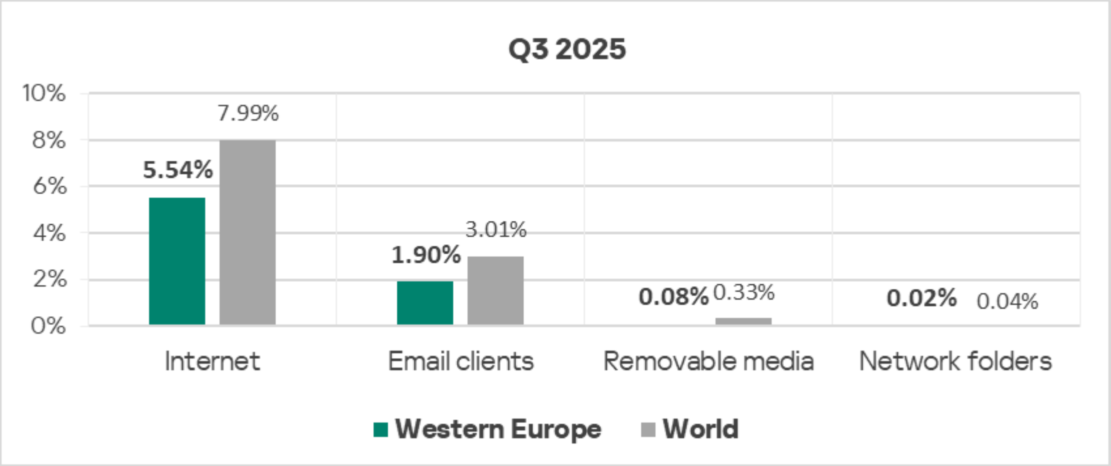


Among the region's countries, France leads in the percentage of ICS computers with blocked malicious objects, at 11.25%. Switzerland had the lowest figure at 6.98%.



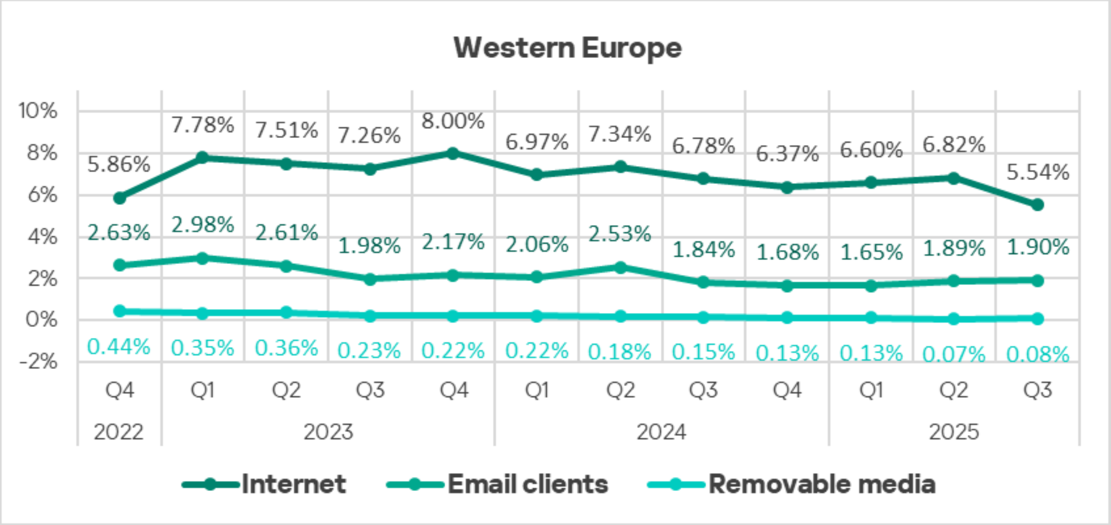
Threat sources

All threat source rates in Western Europe are below the global average.



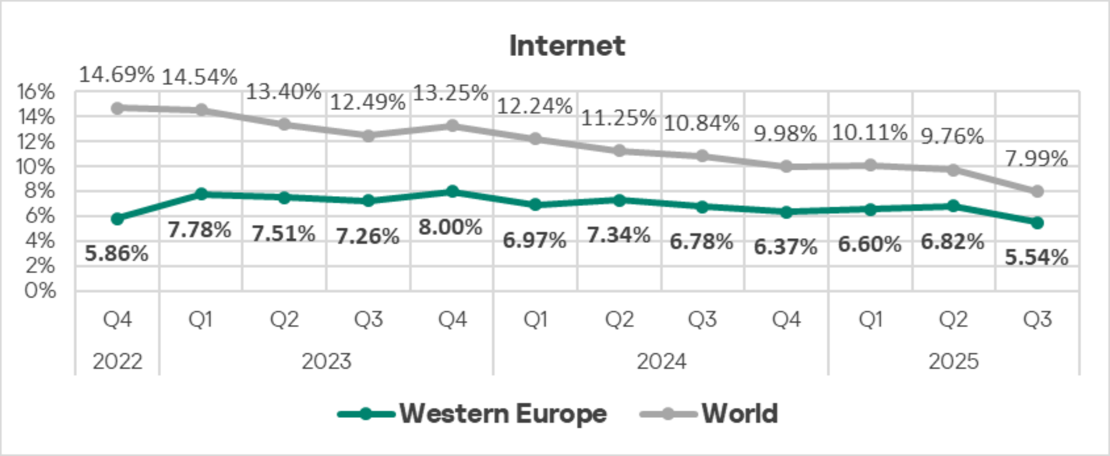
Malicious objects in the region spread primarily via the internet and email.

In Q3 2025, the percentage of ICS computers on which malicious objects were blocked in the region increased slightly for all sources of threats except the internet.

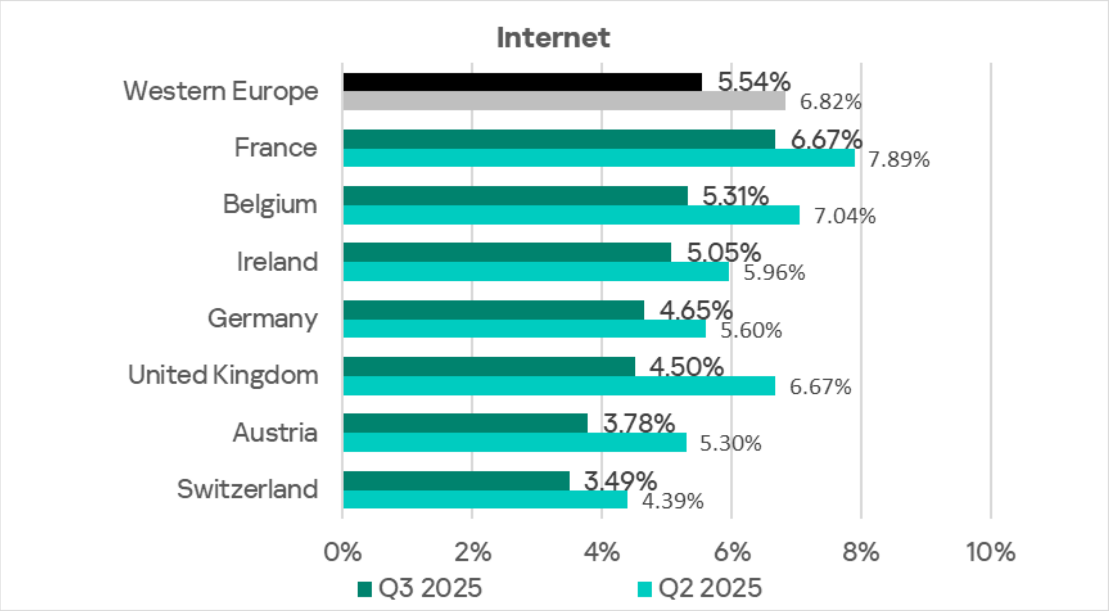


Internet

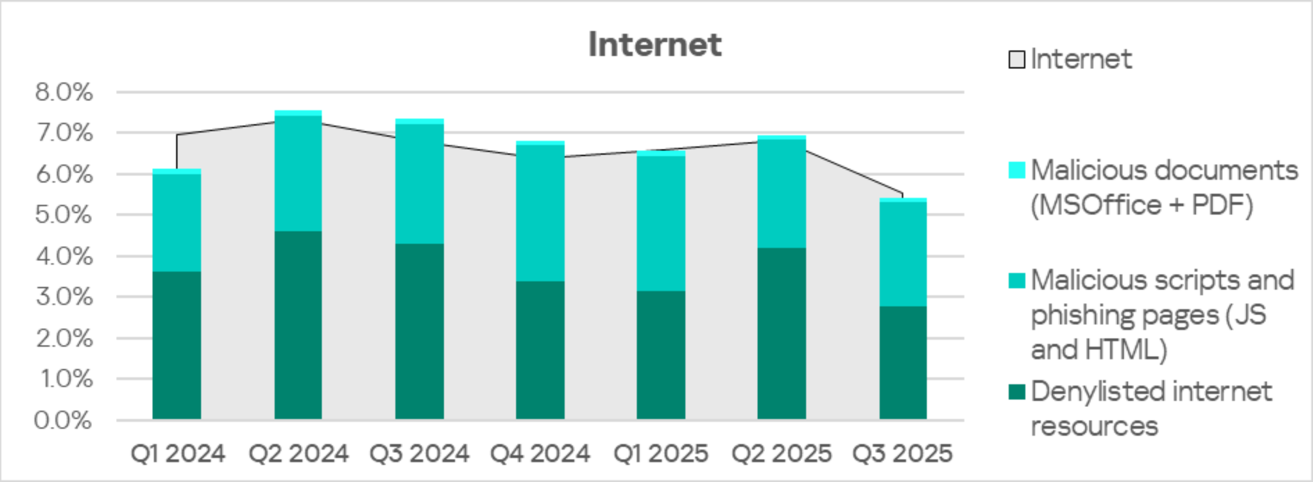
By the percentage of ICS computers on which internet threats were blocked, Western Europe ranks 13th globally, with a rate of 5.54%. This is 1.2 times higher than the lowest figure, recorded in Northern Europe.



Country-level rates range from 3.49% in Switzerland to 6.67% in France. The percentage of ICS computers on which internet threats were blocked during the quarter decreased in every country in the region.



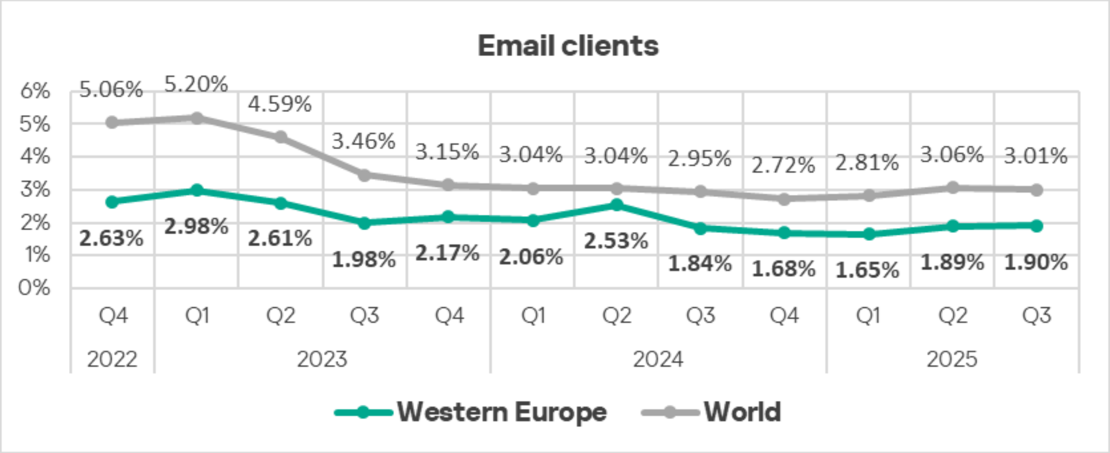
The main categories of internet threats blocked on ICS computers in the region are denylisted internet resources, malicious scripts and phishing pages.



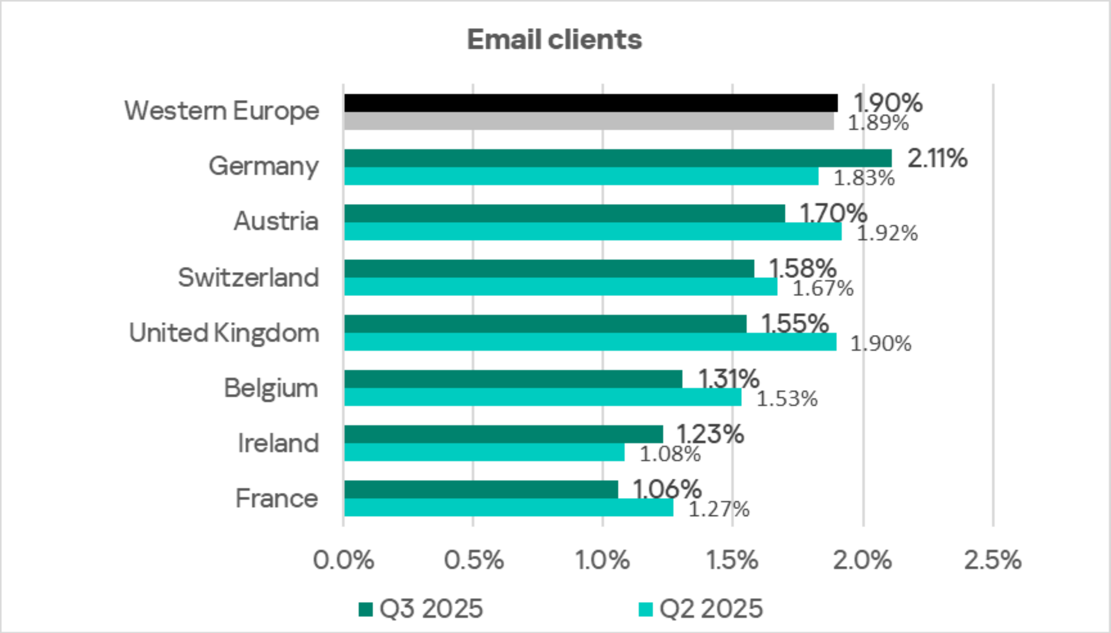
France led the region in terms of denylisted internet resources, as well as malicious scripts and phishing pages.

Email clients

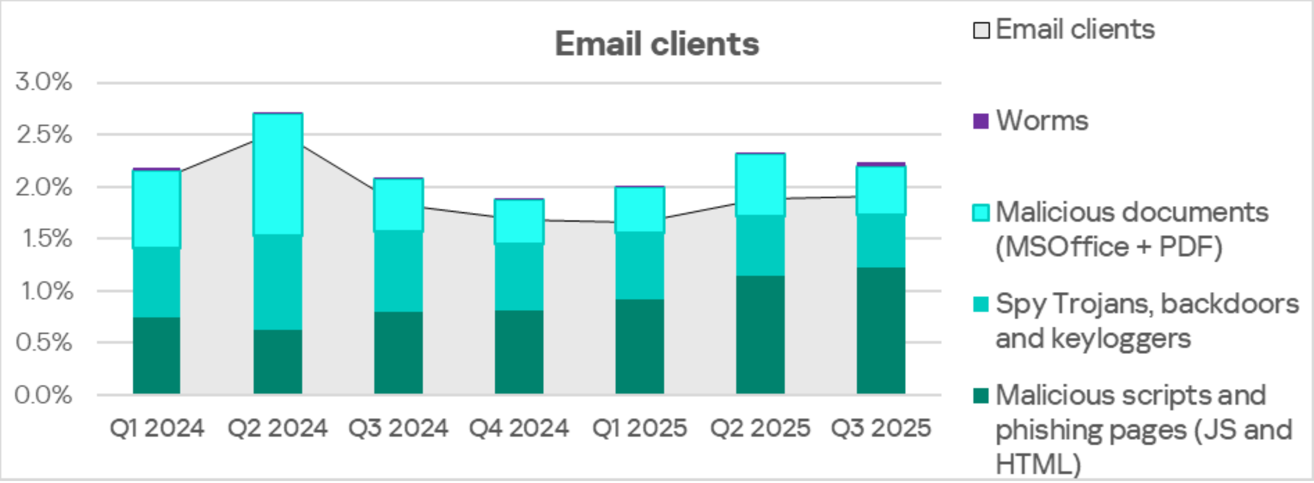
By the percentage of ICS computers on which threats from email clients were blocked, Western Europe ranked 10th in Q3 2025, with a rate of 1.90%. This is 2.4 times higher than in Russia, which ranks last.



Among countries in the region, Germany leads in this metric with 2.11%. France had the lowest figure (1.06%). Germany and Ireland saw an increase in Q3.



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



Spyware in the region spread mainly via email. Germany also led the region in spyware rates.

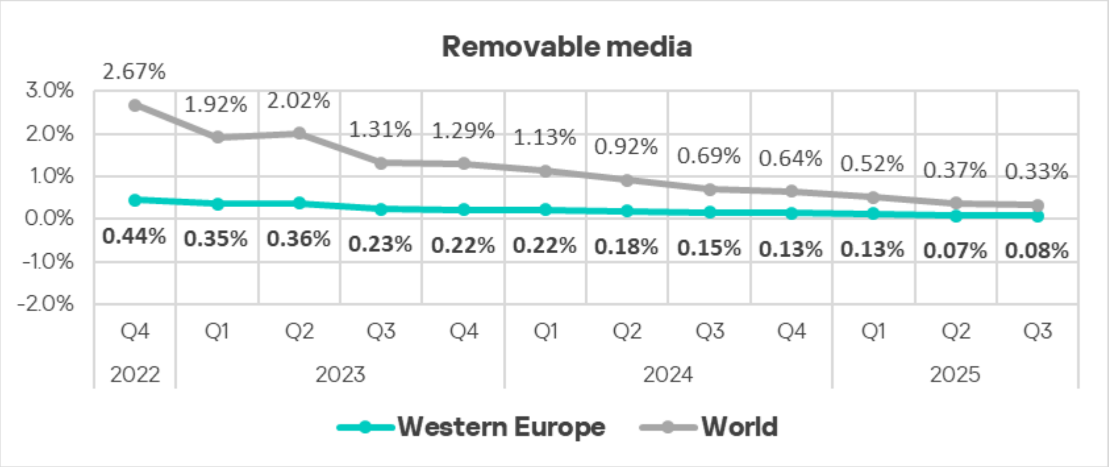
Notably, in Q3 2025, worms spread more frequently through email than through any other threat source.

Removable media

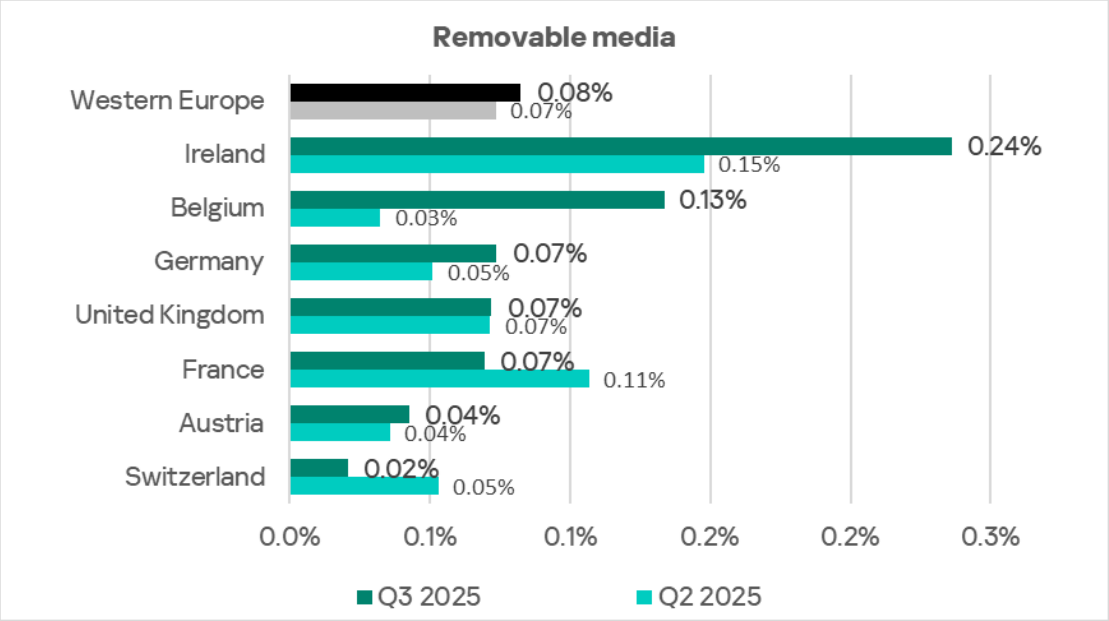
In terms of ICS computers where threats were blocked when connecting removable media, Western Europe ranked 11th globally in Q3 2025, with a rate of

0.08%. This figure is 1.6 times higher than in the Australia and New Zealand region, which ranks last.

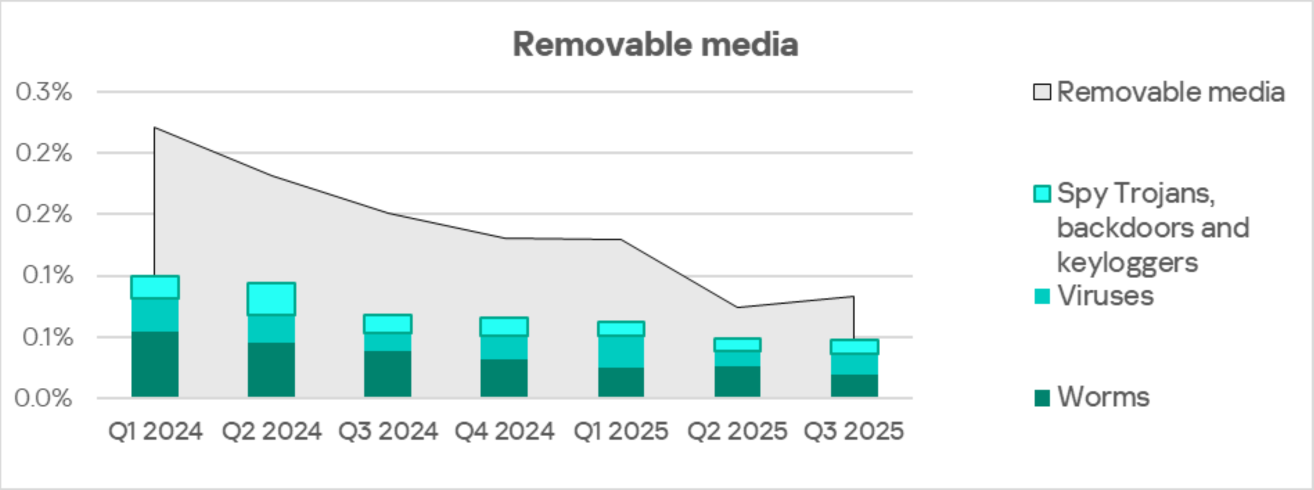
In Q3 2025, the percentage of ICS computers on which threats were blocked when connecting removable media increased slightly for the first time since Q2 2023.



Country-specific rates ranged from 0.02% in Switzerland to 0.24% in Ireland. The metric decreased in only two countries this quarter: Switzerland and France. Meanwhile, we observed a sharp increase in Belgium and Ireland.



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



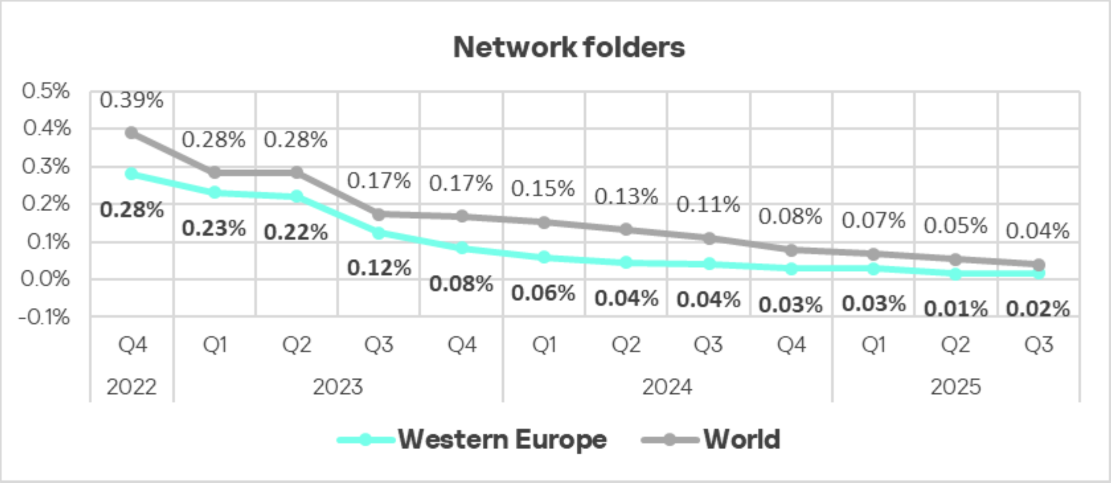
In Western Europe, viruses and worms spread through every threat source in Q3 2025. Viruses were mostly blocked on removable media.

Ireland, which led the rankings for threats blocked on removable media, also led in viruses and worms.

Network folders

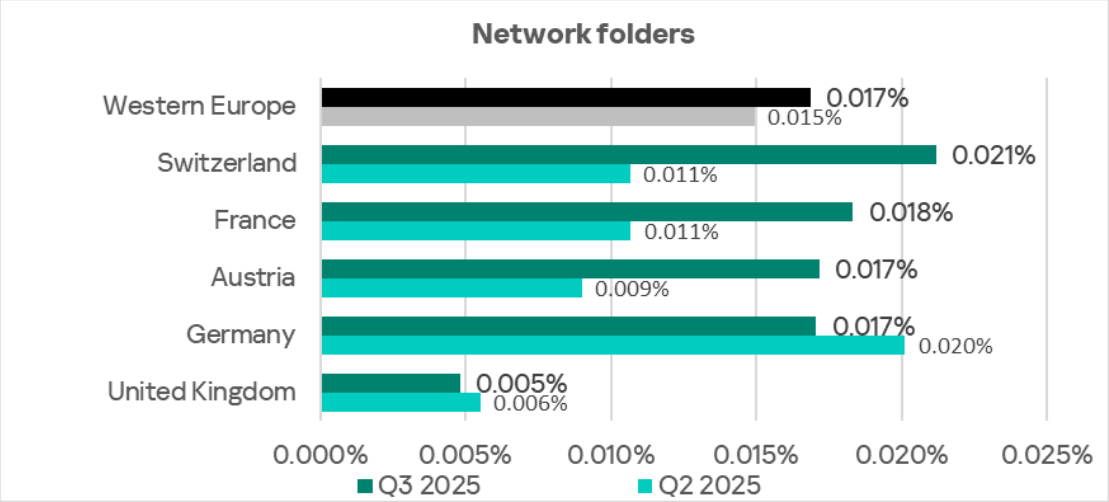
Western Europe was one of four regions globally in Q3 2025 which saw an increase in the percentage of ICS computers on which network folder threats were blocked. The region ranked eighth globally for this metric in Q3. This is the region's highest position in the global rankings — both in threat sources and categories.

The region's percentage of ICS computers on which network folder threats were blocked increased from 0.015% to 0.017%. This is 2.8 times higher than Northern Europe, which ranks last.

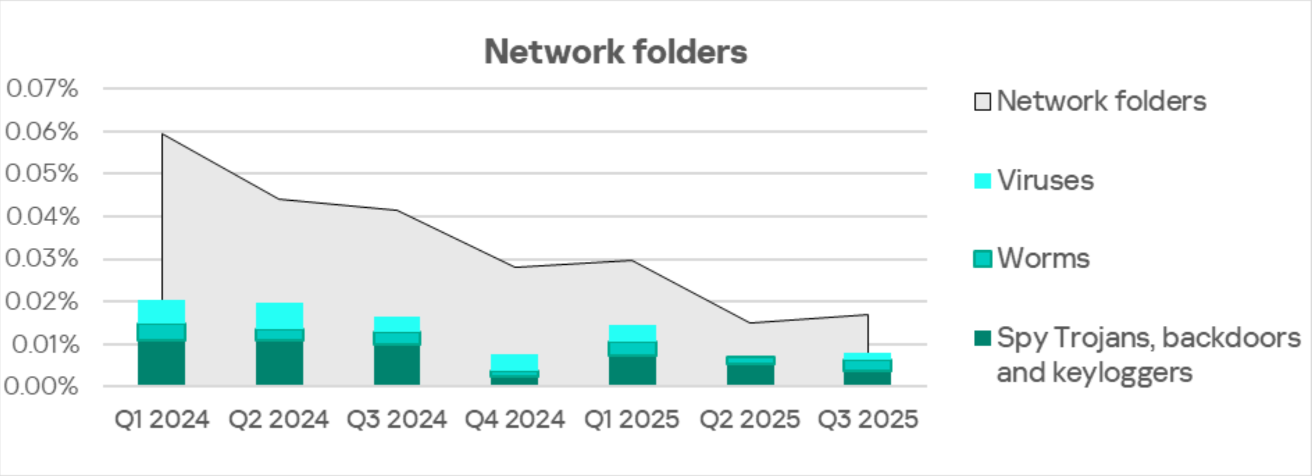


Among countries in the region, Switzerland leads with 0.021%. In Belgium and Ireland, these threats were virtually non-existent.

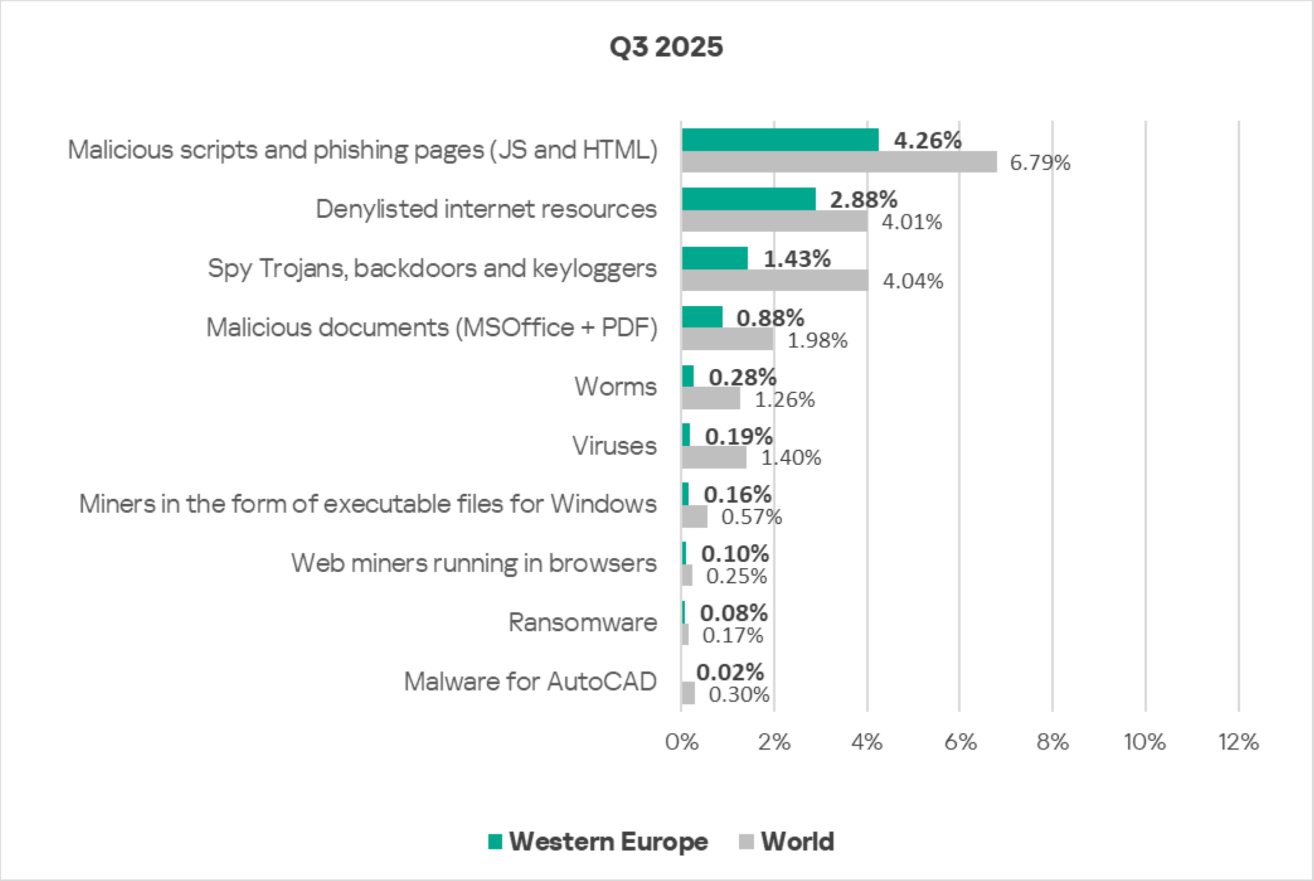
The metric increased noticeably in Switzerland, France, and Austria.

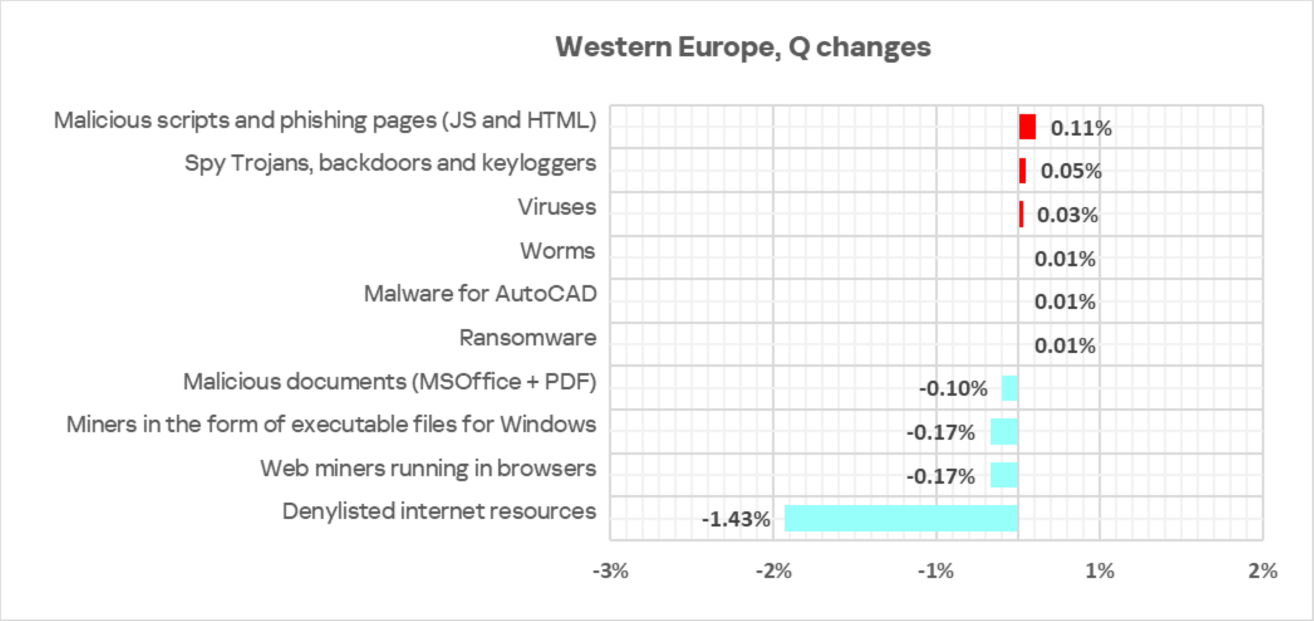


The main categories of network folder threats blocked were spyware, worms, and viruses.



Threat categories





For all threat categories, Northern Europe's figures remain below global averages.

Western Europe's highest ranking globally across all threat categories blocked on ICS computers was for denylisted internet resources. The region ranked 10th for this metric. In Q3 2025, this threat category decreased noticeably across all regions globally.

The rates for both types of miners — which increased in Q2 2025 — fell in Q3, returning to its previous position in the rankings.

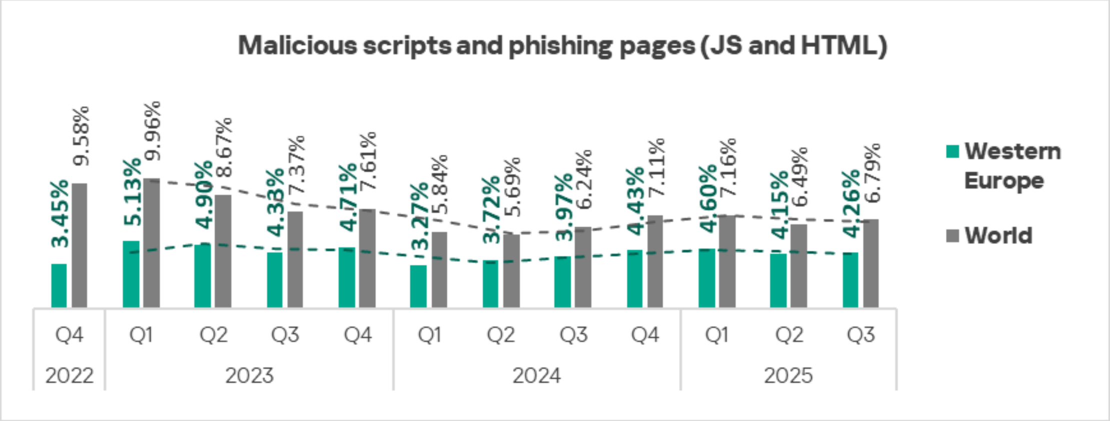
However, quarterly growth was recorded in the percentage of ICS computers on which the following categories of malicious objects were blocked:

- Malicious scripts and phishing pages.
- Spyware.
- Ransomware: 1.1 times higher.
- Worms.
- Viruses: 1.2 times higher.
- Malware for AutoCAD: 2.0 times higher.

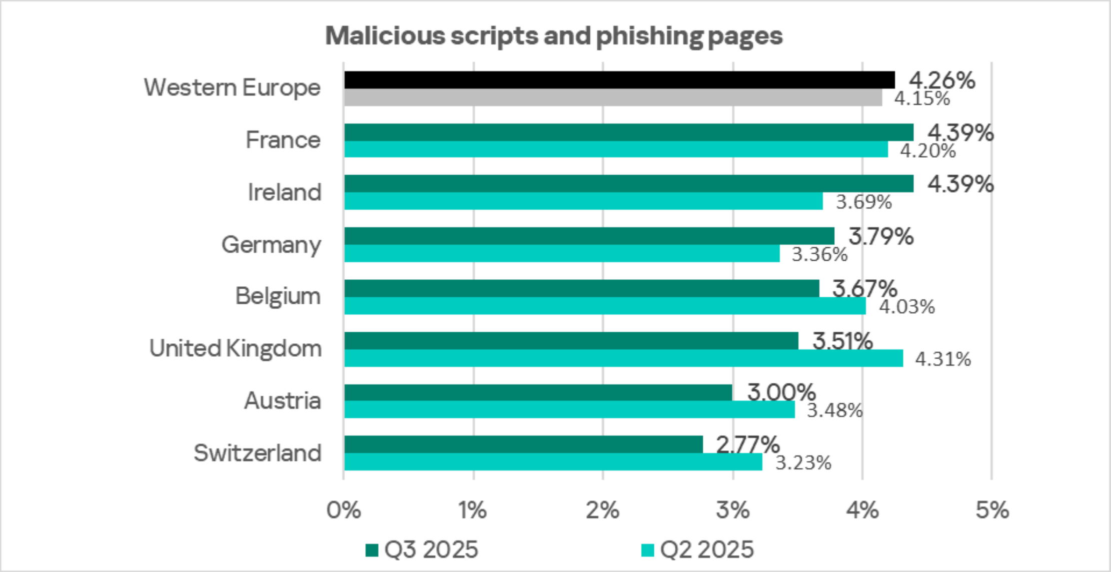
Malicious scripts and phishing pages

Western Europe ranked 12th among regions by the percentage of ICS computers on which malicious scripts and phishing pages were blocked, at 4.26%. This figure is 1.7 times higher than in Northern Europe, which has the lowest rate.

This metric typically fluctuates in the region; in Q3 2025, it increased.



Among countries in the region, France led in the percentage of ICS computers on which malicious scripts and phishing pages were blocked, with 4.39%. This metric increased in three countries in Q3: France, Ireland and Germany.

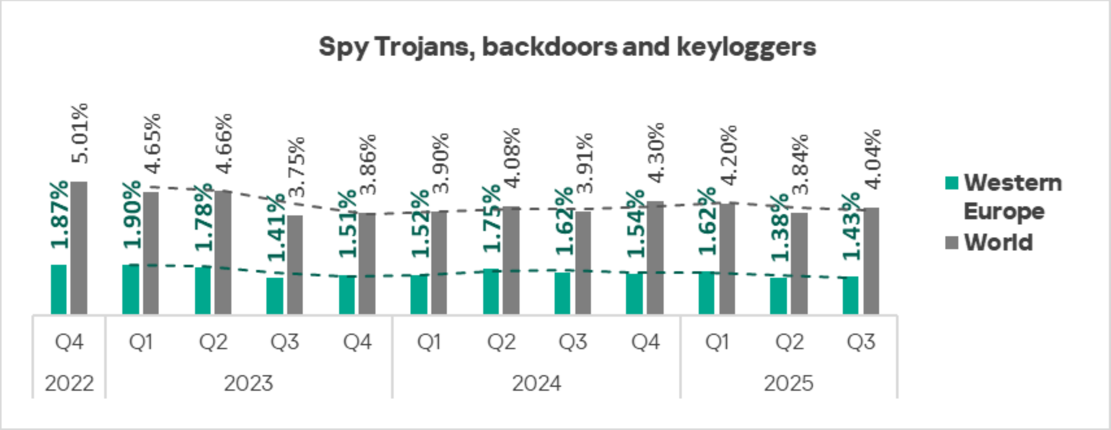


The main sources of malicious scripts and phishing pages were the internet and email. France led the region in internet threats.

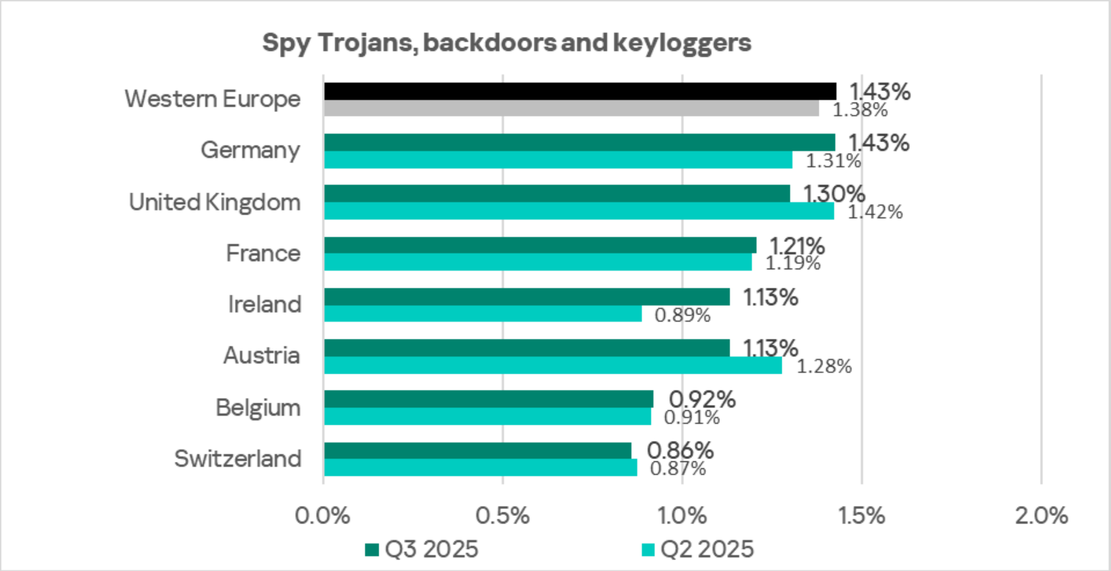
Spyware

By the percentage of ICS computers on which spyware was blocked, Western Europe ranked 13th (second-to-last) with 1.43%.

This metric typically fluctuates in the region; in Q3 2025, it increased.



Among the region's countries, Germany led with 1.43% in the percentage of ICS computers on which spyware was blocked. In Q3 2025, the indicator increased in Germany, France, Ireland and Belgium.

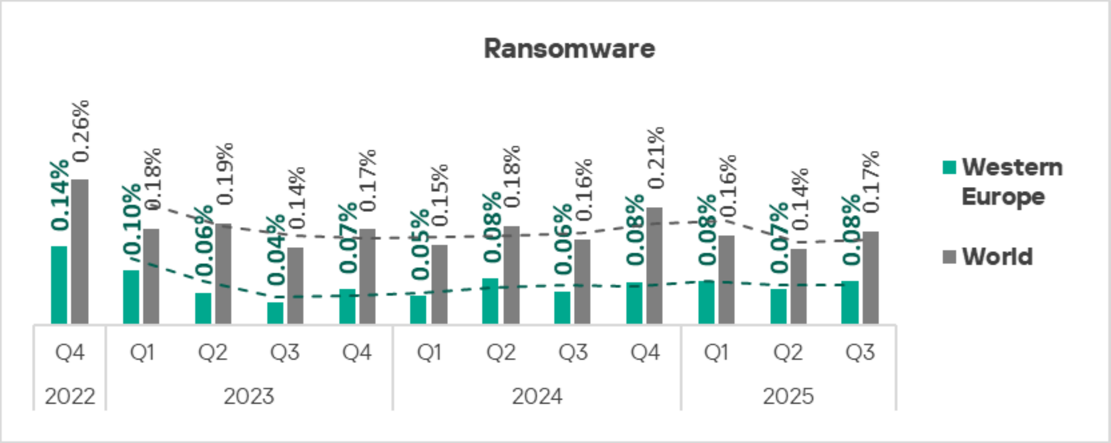


The main channel through which spyware spread in the region was email. Germany also led in email client threats.

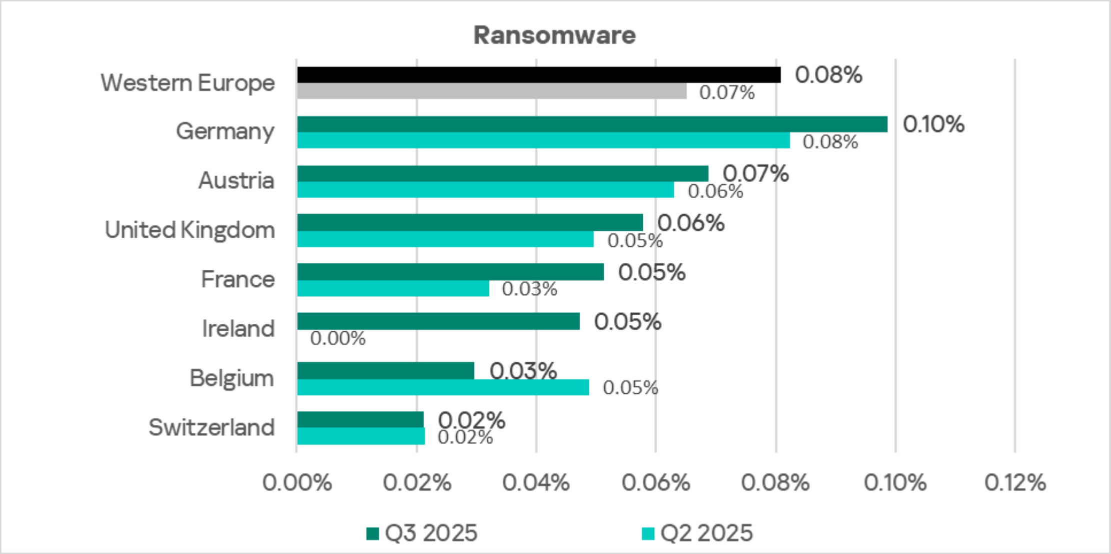
Ransomware

By the percentage of ICS computers on which ransomware was blocked, Western Europe ranked 11th globally with 0.08%. This is 1.6 times higher than Northern Europe, which has the lowest rate.

This metric typically fluctuates in the region; in Q3 2025, it increased slightly.



Among the region's countries, Germany led with 0.10% in the percentage of ICS computers on which ransomware was blocked. This metric increased in all countries in the region, with the exception of Belgium and Switzerland.

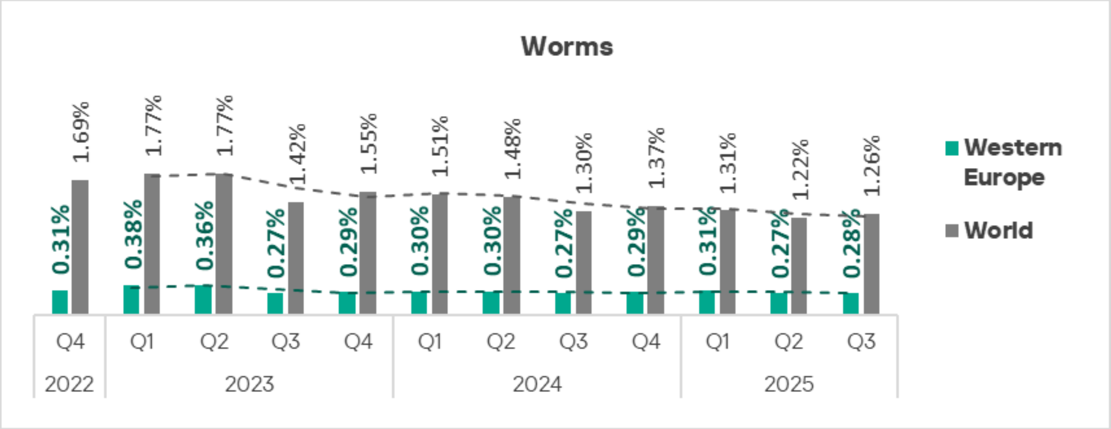


Once again, Germany led the region in spyware rates.

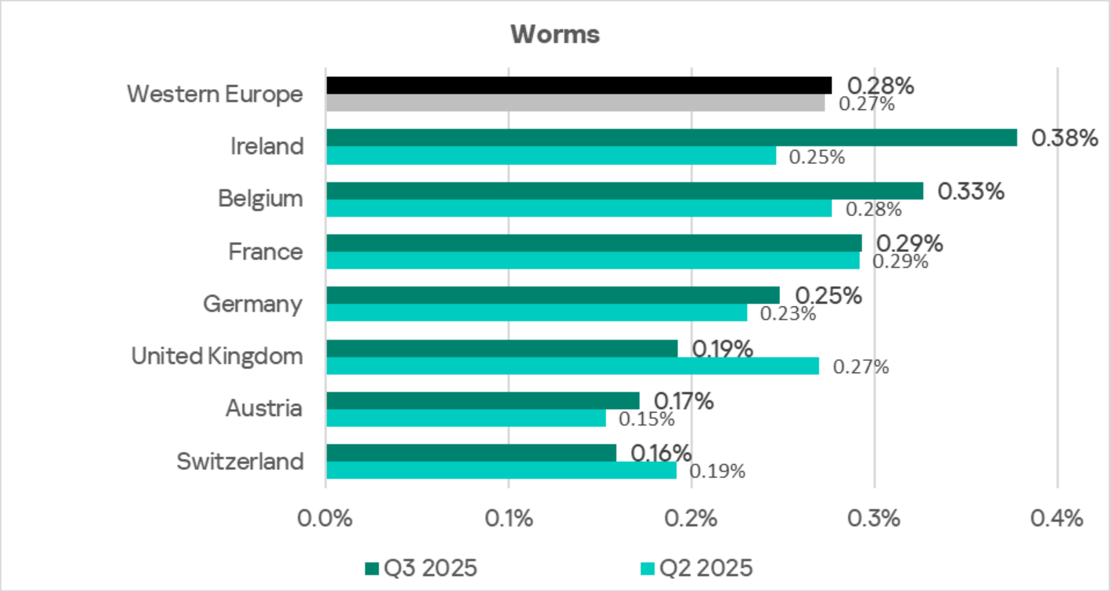
Worms

In terms of the percentage of ICS computers on which worms were blocked, Western Europe ranked 13th with 0.28%. This figure is 1.3 times higher than in Northern Europe, which boasts the lowest percentage among all regions.

In Q3 2025, the metric increased in most regions globally, including Western Europe.



Among countries in the region, Ireland led with 0.38% in the percentage of ICS computers on which worms were blocked. In Q3, this indicator increased in only two countries: the UK and Switzerland.

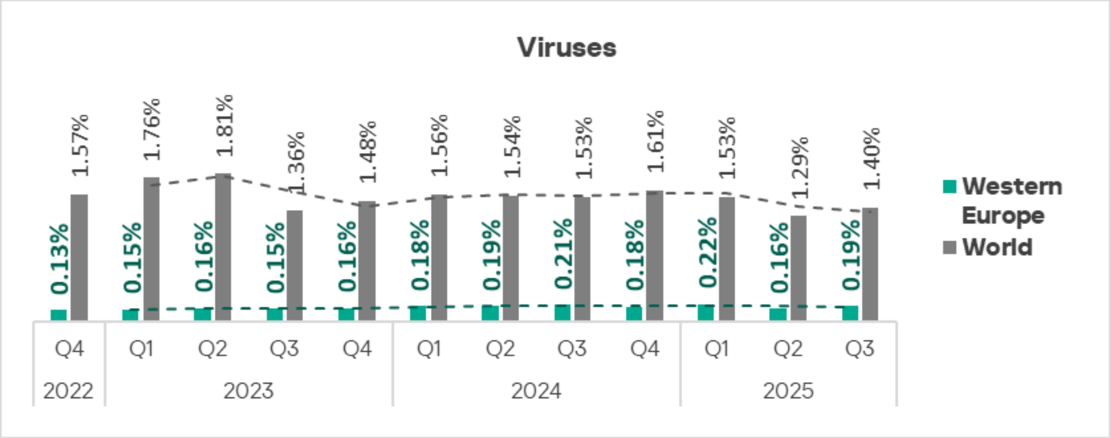


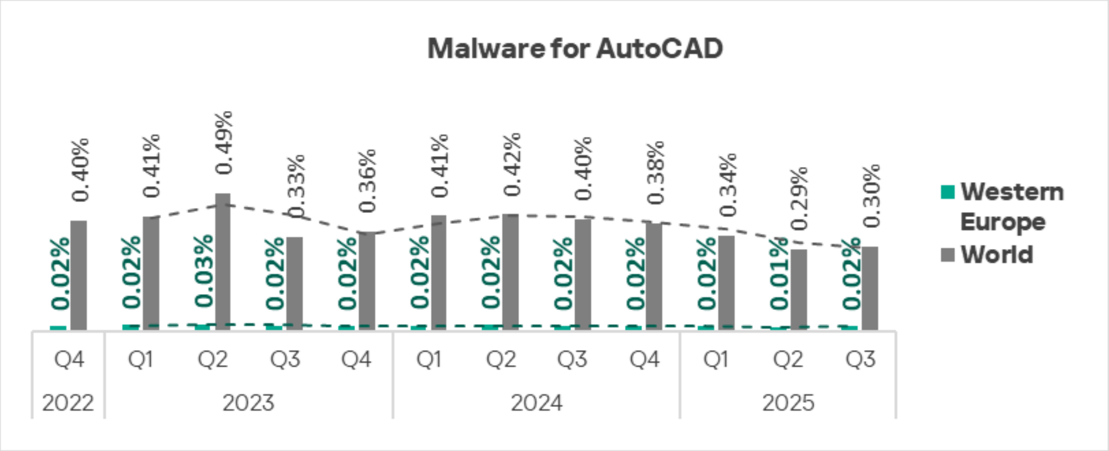
Ireland also led the region in the percentage of ICS computers on which threats were blocked when connecting removable media. Ireland also led in viruses.

Viruses and malware for AutoCAD

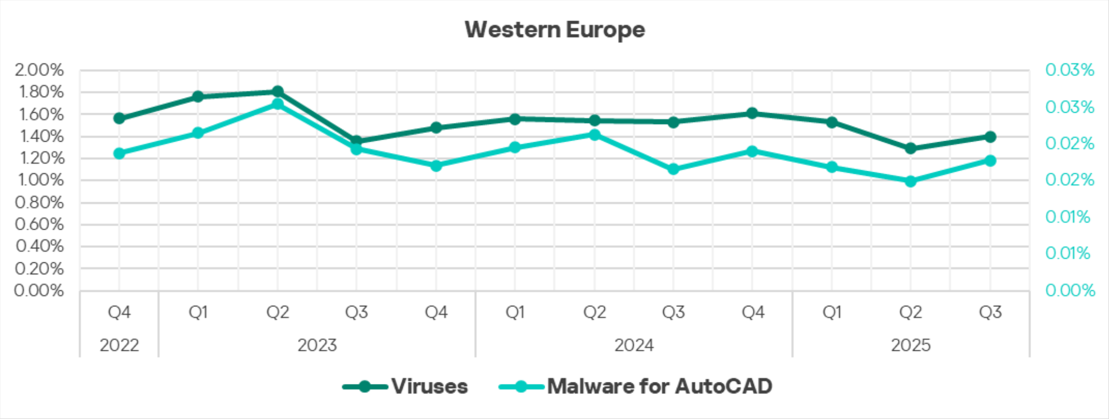
Western Europe ranked 12th globally in terms of the percentage of ICS computers on which viruses were blocked as well as for malware for AutoCAD.

Both categories increased over the quarter.

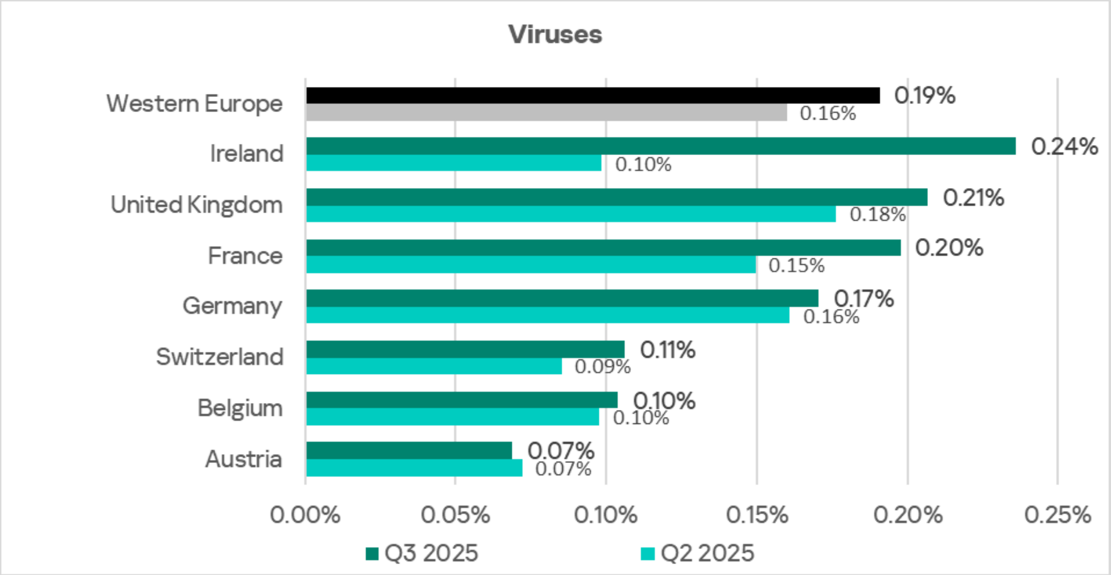




In the chart below, the second axis represents malware for AutoCAD, showing a clear similarity between the trends for both threat categories.

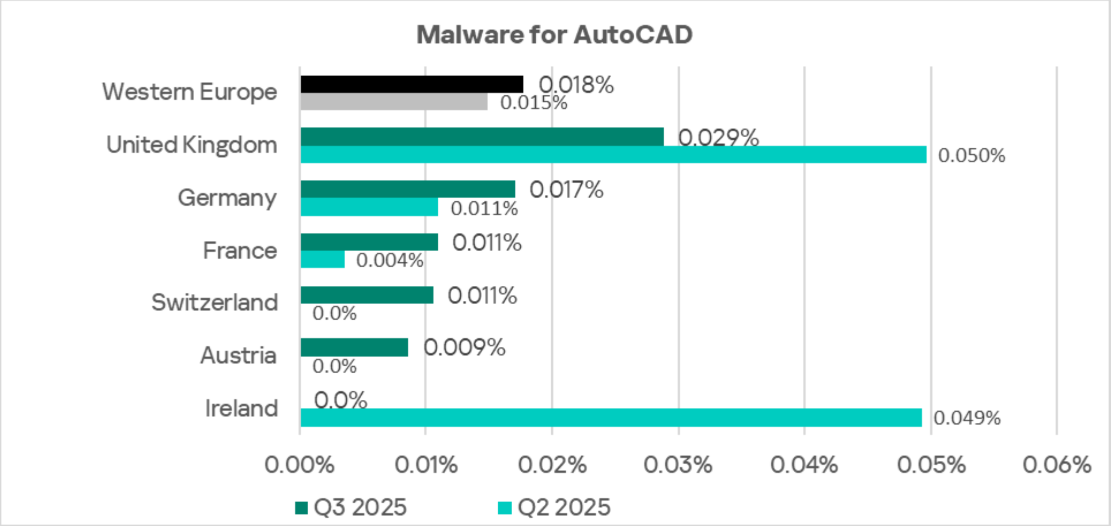


Among the region's countries, Ireland led in the percentage of ICS computers on which viruses were blocked, with the United Kingdom holding second place. In Q3, the figure increased in every country except Austria, with Ireland increasing by 2.4 times.



Viruses in the region spread through every threat source and were most commonly found on removable media.

The United Kingdom topped the rankings in terms of malware for AutoCAD.

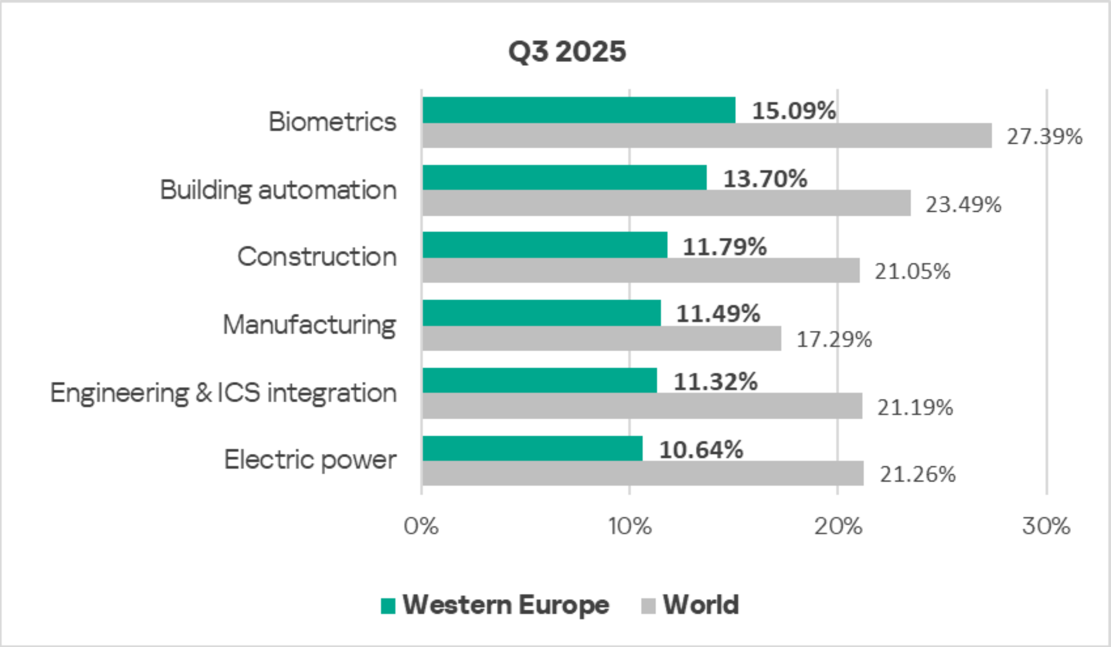


The main source of malware for AutoCAD is network folders,

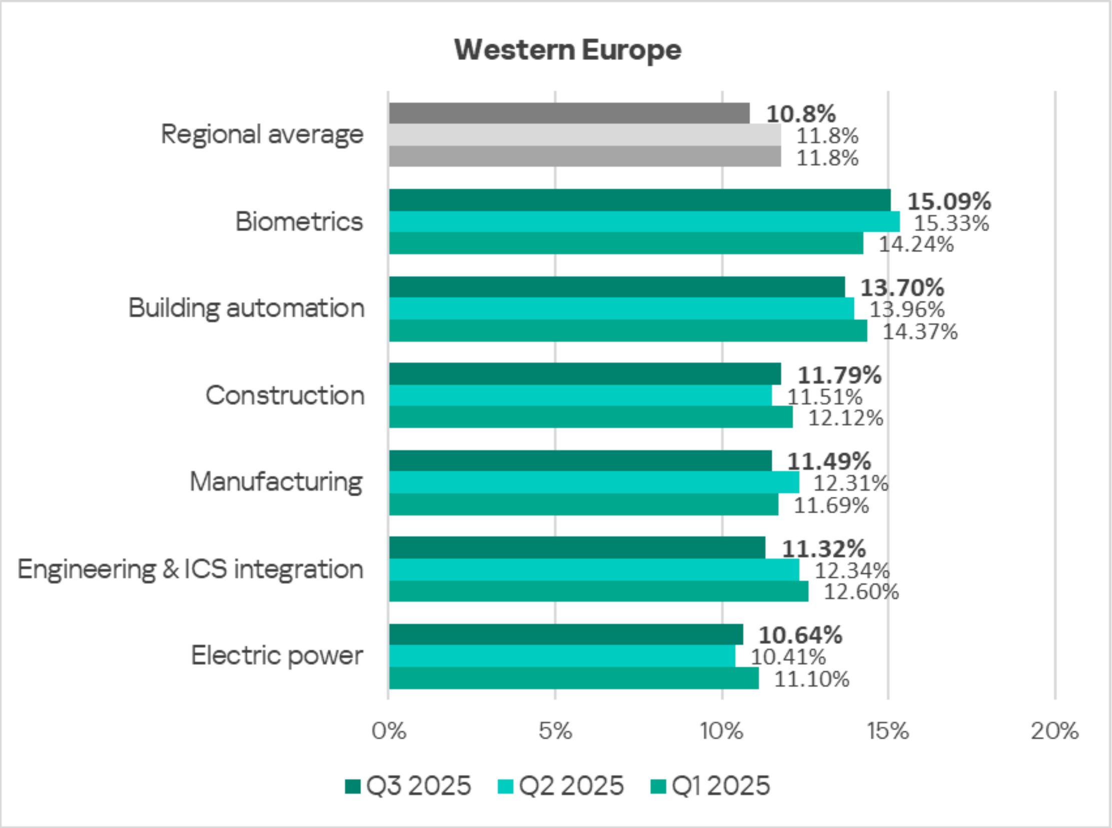
Industries

Among the industries reviewed in the report, the percentage of ICS computers on which malicious objects were blocked was highest in biometric systems.

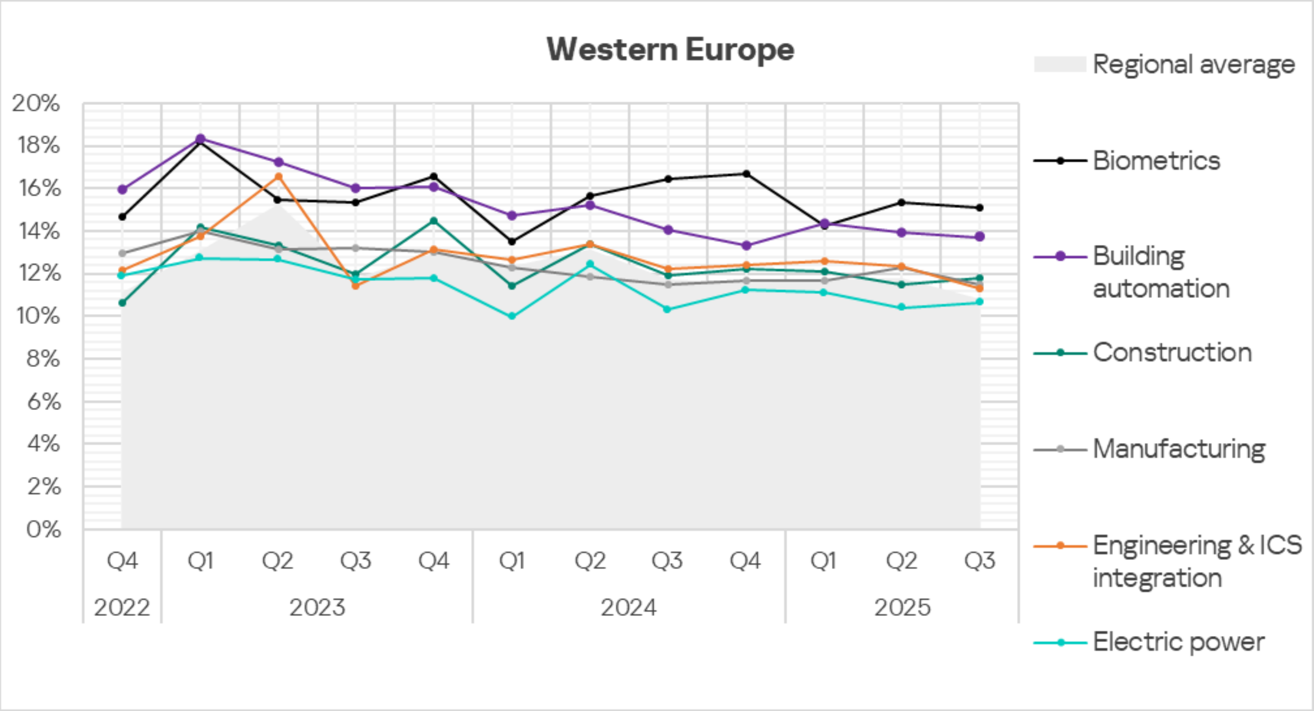
Figures for all industries in the region remain well below the global averages.



In Q3 2025, the rate increased in two of the industries reviewed in the region: construction and electric power.



Rates for ICS computers that blocked threats in building automation and the biometric systems OT infrastructure remained noticeably above the regional average.



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 Western Europe, Q3 2025

Industry / Threat source	Biometrics	Building automation	Electric power	Engineering & ICS integration	Oil & gas	Construction	Manufacturing	Threat category total in the region
Internet	5.61%	5.95%	5.47%	6.06%	6.96%	5.97%	5.29%	5.54%
Email clients	5.22%	3.90%	1.43%	1.75%	0.56%	2.15%	1.28%	1.90%
Removable media	0.19%	0.13%	0.14%	0.07%	0.00%	0.10%	0.32%	0.08%
Network folders	0.00%	0.03%	0.04%	0.02%	0.00%	0.05%	0.00%	0.02%
Industry total in the region	15.09%	13.70%	10.64%	11.32%	13.93%	11.79%	11.49%	

Threat category indicators for industries in Western Europe, Q3 2025

Industry / Threat category	Biometrics	Building automation	Electric power	Engineering & ICS integration	Oil & gas	Construction	Manufacturing	Threat category total in the region
Denylisted internet resources	3.45%	3.93%	3.86%	4.77%	4.91%	3.82%	3.76%	2.88%
Malicious scripts and phishing pages (JS and HTML)	6.70%	5.84%	3.05%	4.42%	3.76%	4.97%	3.89%	4.26%
Spy Trojans, backdoors and keyloggers	4.79%	2.51%	1.11%	1.43%	1.45%	1.03%	1.65%	1.43%
Worms	0.38%	0.45%	0.28%	0.27%	0.29%	0.17%	0.72%	0.28%
Miners in the form of executable files for Windows	0.19%	0.29%	0.33%	0.31%	0.58%	0.22%	0.25%	0.16%
Malicious documents (MSOffice + PDF)	3.64%	1.92%	0.78%	0.96%	0.58%	0.71%	0.85%	0.88%
Viruses	0.38%	0.26%	0.18%	0.16%	0.58%	0.24%	0.25%	0.19%
Ransomware	0.19%	0.12%	0.04%	0.06%	0.00%	0.00%	0.04%	0.08%
Web miners running in browsers	0.19%	0.26%	0.28%	0.26%	0.58%	0.22%	0.30%	0.10%
Malware for AutoCAD	0.00%	0.00%	0.00%	0.01%	0.00%	0.10%	0.00%	0.02%
Industry total in the region	15.09%	13.70%	10.64%	11.32%	13.93%	11.79%	11.49%	

By the percentage of ICS computers on which malicious objects were blocked across various industries globally, Western Europe ranked no higher than 11th in Q3 2025, with one exception: in the biometric systems OT infrastructure, the region placed ninth. However, this industry is represented by only 10 regions in the report.

Overall, the situation seemed relatively favorable. That said, in Q3 2025, Western Europe saw increases in threats originating from network folders and in ransomware, among others. This affected the indicators across several industries.

Western Europe was the global leader in ransomware rates within the biometric systems infrastructure.

Western Europe ranked fourth globally by the percentage of ICS computers on which network folder threats were blocked in two industries: electric power, and engineering and ICS integration.

Biometric systems

Western Europe ranked ninth globally for the percentage of ICS computers on which malicious objects were blocked in the biometric systems OT infrastructure.

In the global rankings across all industries and regions, the biometric systems OT infrastructure in Western Europe placed:

- First for the percentage of computers where ransomware was blocked.

In the cross-regional rankings for this industry, Western Europe ranked:

- First by percentage of ICS computers on which ransomware was blocked.

Among the region's industries, the biometric systems OT infrastructure ranked:

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

Building automation

Western Europe ranked 12th among regions for the percentage of ICS computers on which malicious objects were blocked in the building automation sector.

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 were blocked.
- Third place in denylisted internet resources.
- First place in the percentage of ICS computers on which miners in the form of executable files for Windows are blocked.
- Second for malicious scripts and phishing pages, malicious documents, worms, viruses, and ransomware.
- Third in the region in terms of web miners.

Construction

Western Europe ranked 13th globally for the percentage of ICS computers on which malicious objects were blocked in the construction sector.

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

- First for the percentage of ICS computers on which network folder threats were blocked.
- Second place in internet threats.
- Third place in email clients.

- First for the percentage of ICS computers on which denylisted internet resources, viruses, and malware for AutoCAD were blocked.
- Third place in malicious scripts and phishing pages.

Manufacturing

Western Europe ranked 13th for the percentage of ICS computers on which malicious objects were blocked in manufacturing.

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

- First place in the percentage of ICS computers on which threats from removable media are blocked.
- First for the worm rate.
- Third place in viruses.

Engineering and ICS integrators

Western Europe ranked 13th regionally for the percentage of ICS computers on which malicious objects were blocked in engineering and ICS integration.

In the cross-regional rankings for this industry, Western Europe ranked:

- Fourth by percentage of ICS computers on which threats in network folders 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 for the percentage of ICS computers on which denylisted internet resources, web miners, and malware for AutoCAD were blocked.
- Third for malicious documents and miners in the form of executable files for Windows.

Electrical power

Western Europe ranked 11th regionally for the percentage of ICS computers on which malicious objects were blocked in the electric power industry.

In the cross-regional rankings for this industry, Western Europe ranked:

- Fourth by percentage of ICS computers on which threats in network folders were blocked.

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

- Second place in the percentage of ICS computers on which threats in network folders were blocked.
- Third place in removable media threats.
- First place in the percentage of ICS computers on which web miners are blocked.
- Second for miners in the form of executable files for Windows.
- Third for denylisted internet resources, spyware, and ransomware.

Northern Europe

Key cybersecurity issues in the region

Northern Europe is the safest region globally in terms of cybersecurity, typically ranking last (14th) in the percentage of ICS computers on which malicious objects are blocked.

The figures for all threat categories decreased in Northern Europe in Q3 2025.

In most rankings of regions based on the percentage of ICS computers on which various categories of malicious objects from various sources are blocked, Northern Europe occupies the last places (13th, and more frequently 14th place).

Highest positions of Northern Europe in the rankings by threat category:

- Ninth place in miners in the form of executable files for Windows.
- Eleventh place in denylisted internet resources.
- Twelfth place in web miners.

Miners are still a major problem for the region. This is mainly due to the waves of infections on vulnerable online resources, which were exploited to distribute both categories of miners, spyware, and ransomware.

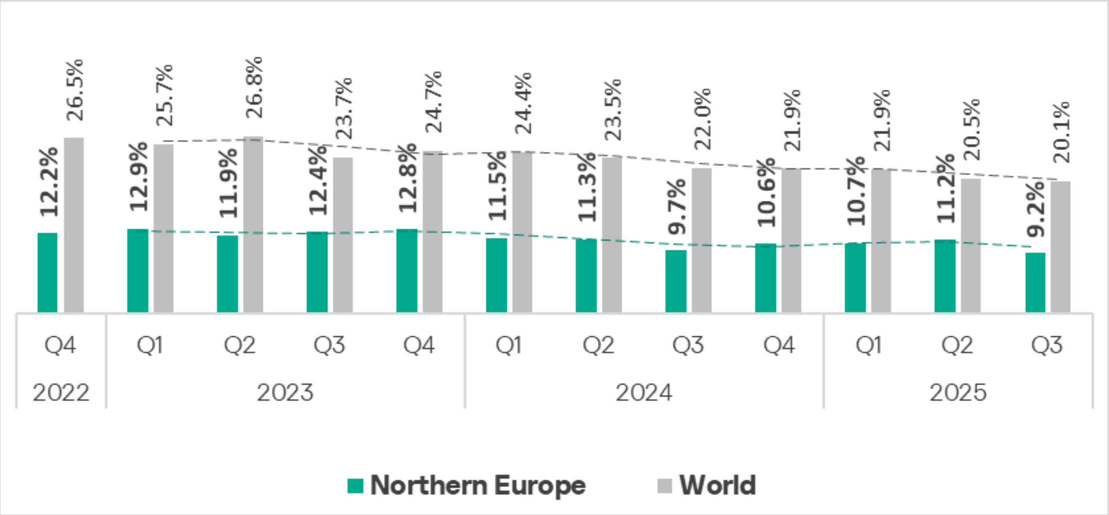
Among regions based on indicators in the manufacturing industry, Northern Europe ranks second in the percentage of industry ICS computers where miners in the form of executable files for Windows are blocked.

Statistics across all threats

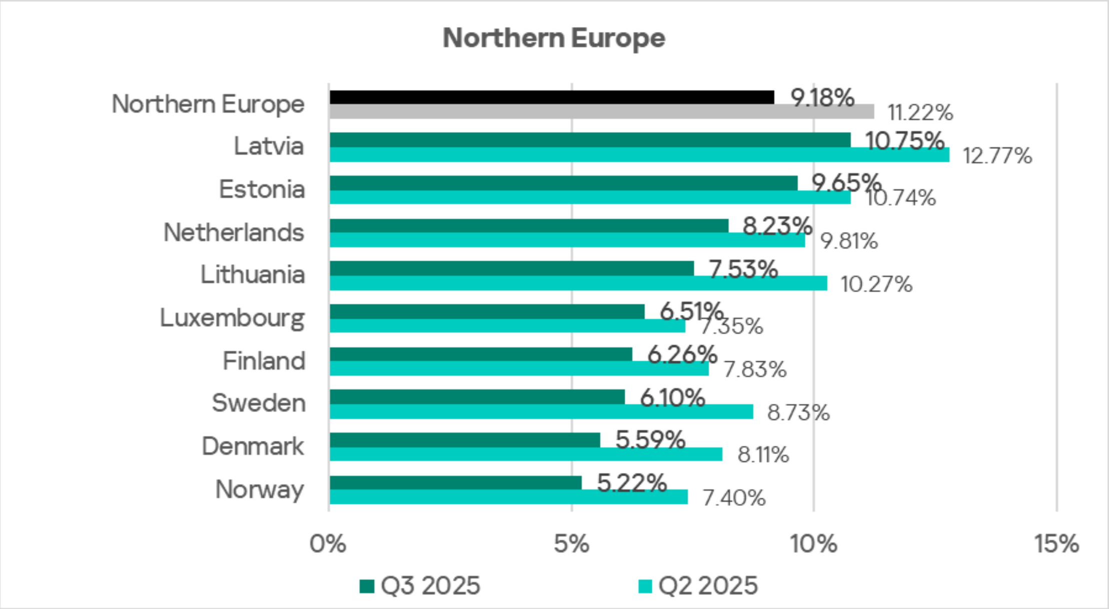
Northern Europe ranks 14th in the global ranking for the percentage of ICS computers on which malicious objects were blocked.

The region's figure is lower than in all other regions, and is significantly lower than the global average.

The percentage of ICS computers on which malicious objects were blocked in Q3 2025 in the region decreased from 11.2% to 9.2%.

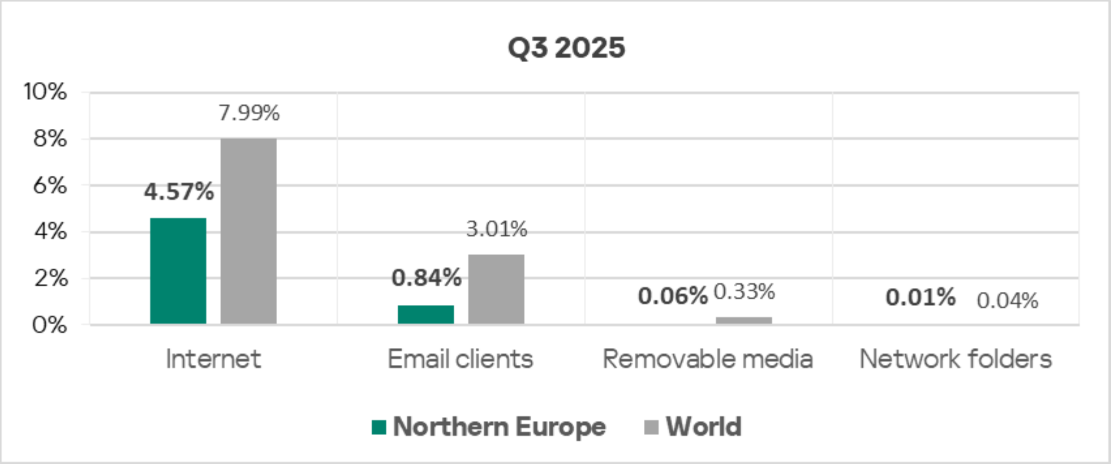


Among the region's countries, Latvia leads in the percentage of ICS computers with blocked malicious objects, at 10.75%. The lowest figure observed was in Norway at 5.22%. This indicator decreased in all countries over the quarter.

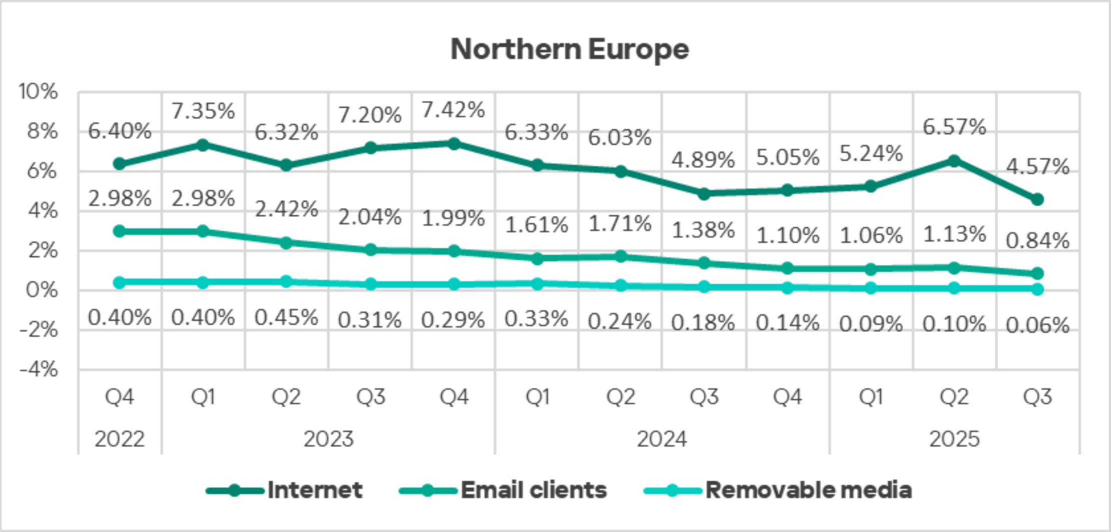


Threat sources

For all threat sources in Northern Europe, values are below global averages.



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

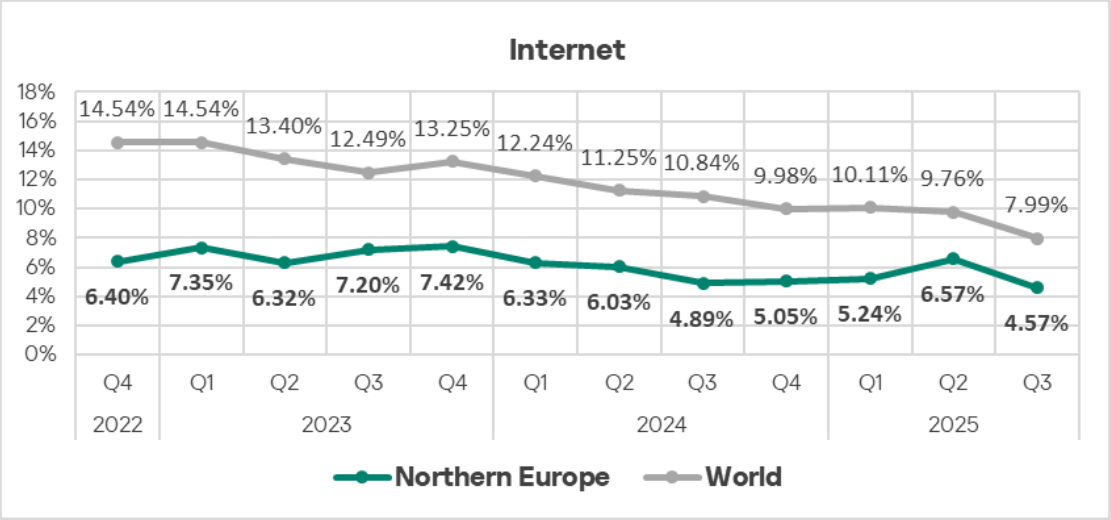


The dominant threat sources are the internet and email.

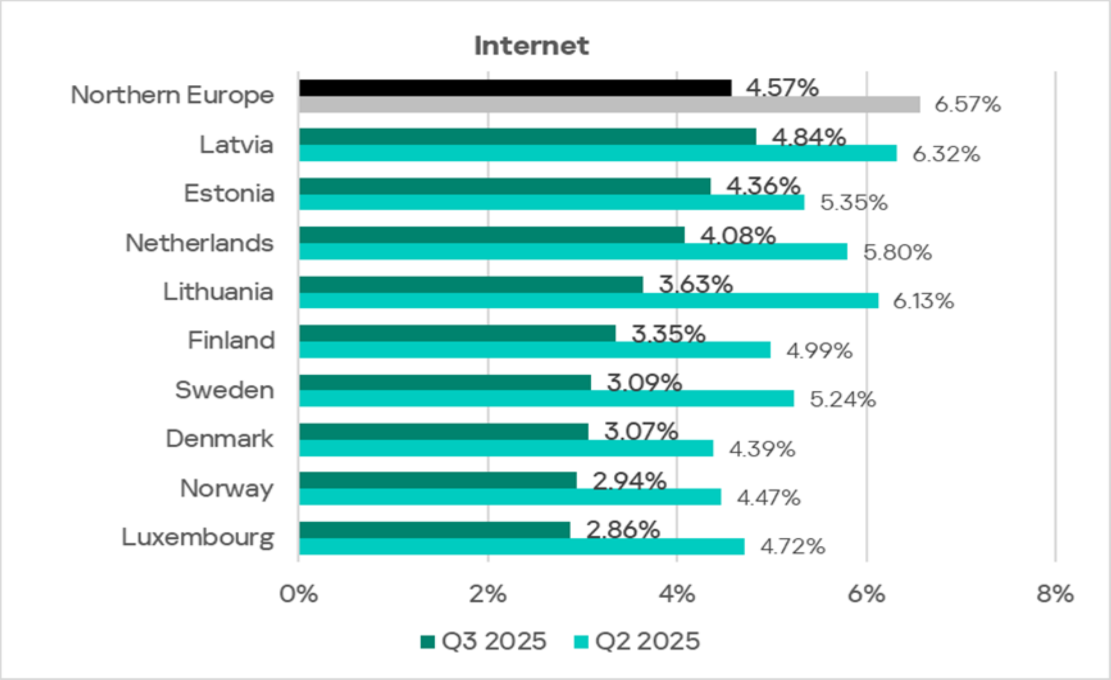
Internet

Based on the percentage of ICS computers on which internet threats were blocked, Northern Europe ranks last (14th) globally.

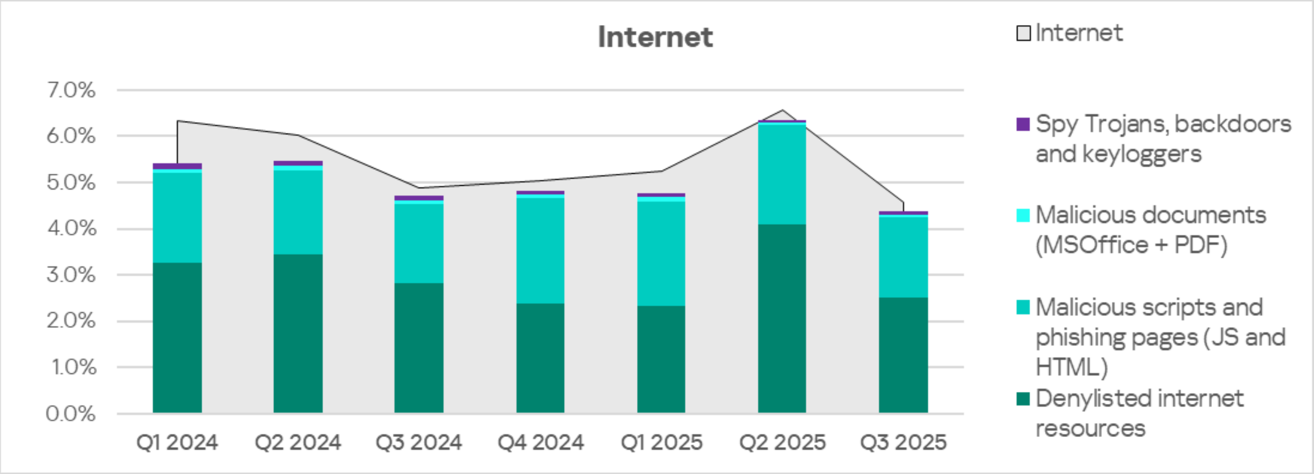
After this indicator grew over the course of three quarters, the value decreased to 4.57%, which is its minimum of the past three years. We should note that the percentage of ICS computers on which internet threats were blocked decreased in all regions.



Across the region, the percentage of ICS computers on which internet threats were blocked ranges from 2.86% in Luxemburg to 4.84% in Latvia. Over the quarter, this indicator decreased in all countries of the region.



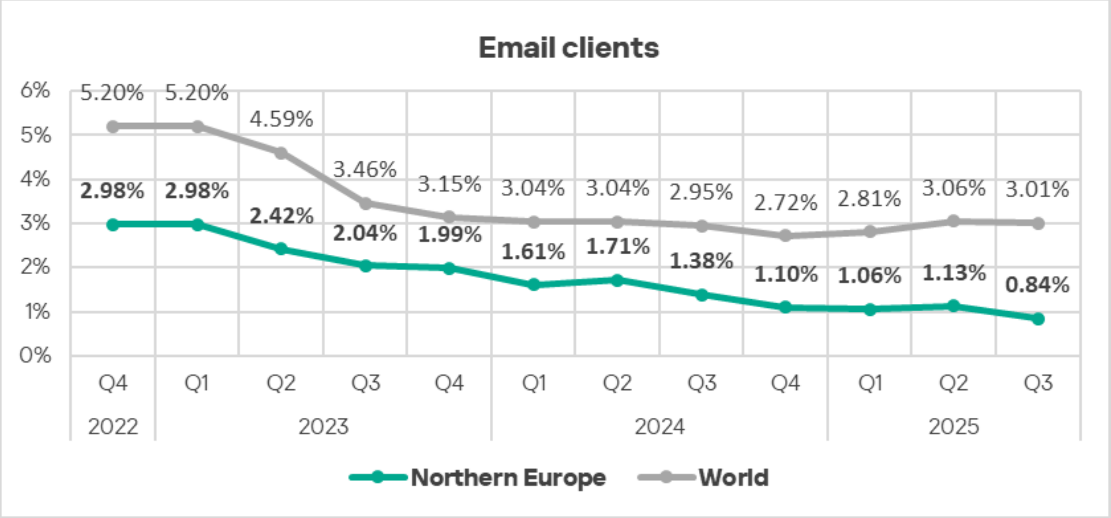
The main categories of internet threats blocked on ICS computers in the region are denylisted internet resources and malicious scripts and phishing pages.



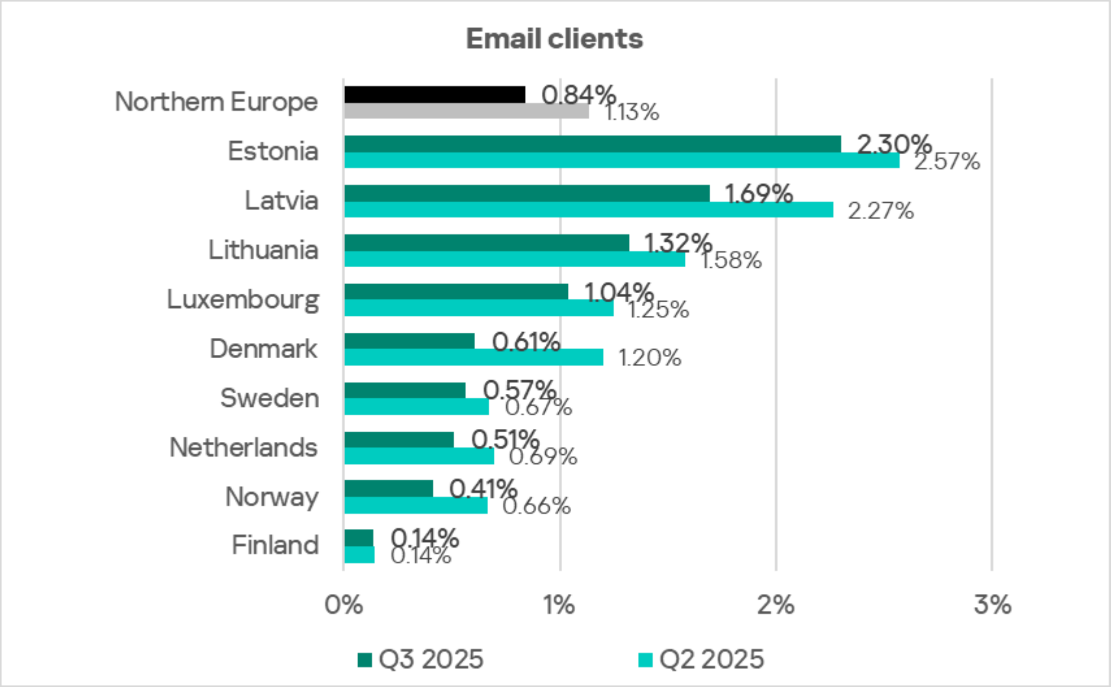
Email clients

Based on the percentage of ICS computers on which threats from email clients are blocked, Northern Europe ranked 13th among regions in Q3 2025.

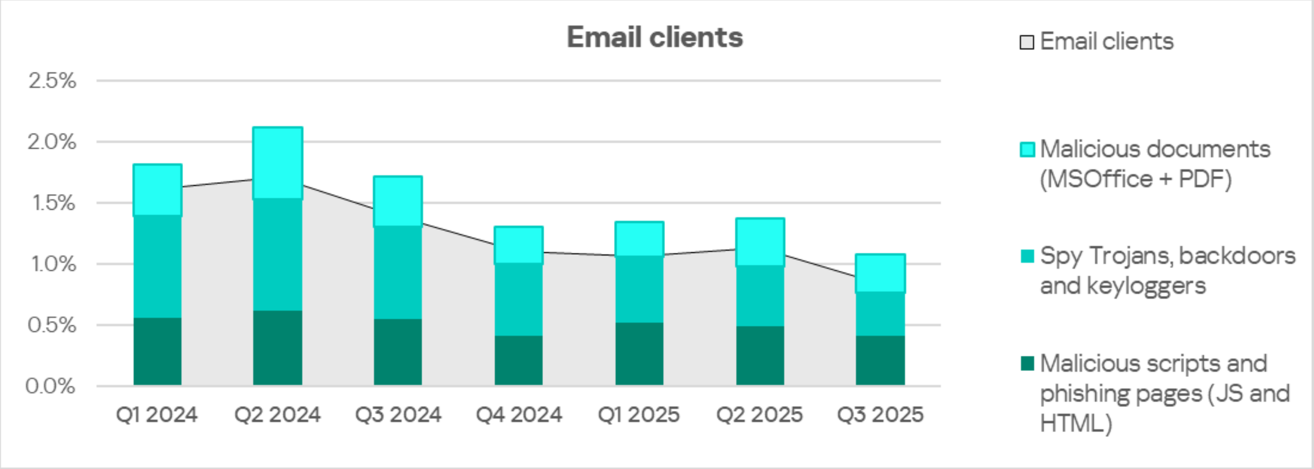
The figure decreased to 0.84% in the region over the quarter. Although this is its lowest value over three years, it is 1.1 times higher than in Russia, which ranks last.



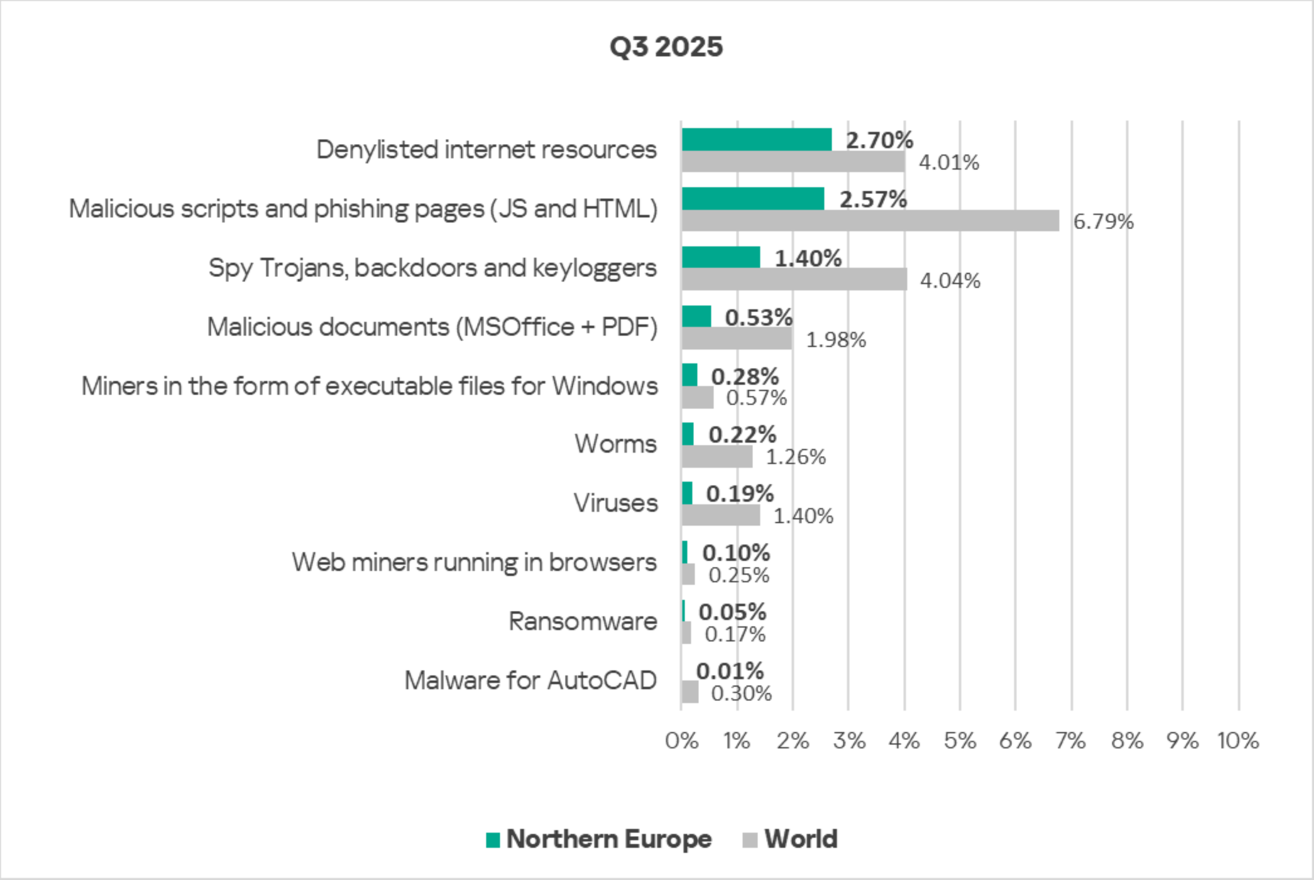
Among countries in the region, Estonia leads in this metric with 2.30%. The lowest figure observed was in Finland at 0.14%. Over the quarter, this indicator decreased in all countries except Finland.

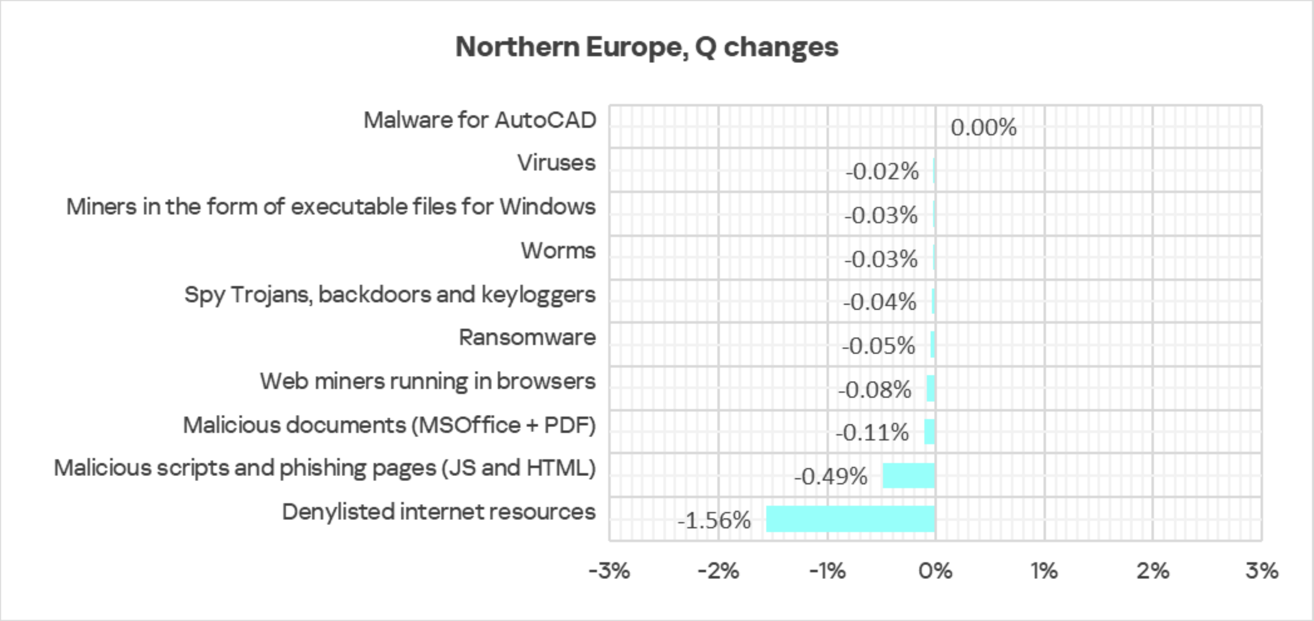


The main categories of email threats blocked on ICS computers are malicious scripts and phishing pages, spyware, and malicious documents.



Threat categories





For all threat categories, Northern Europe's figures remain below global averages.

The indicators over the quarter decreased for all threat categories.

In most rankings of regions based on the percentage of ICS computers on which various categories of malicious objects are blocked, Northern Europe occupies the last places (13th and 14th).

However, there are exceptions. Northern Europe has the following rankings in the following threat categories:

- Ninth place in miners in the form of executable files for Windows.
- Eleventh place in denylisted internet resources.
- Twelfth place in web miners.

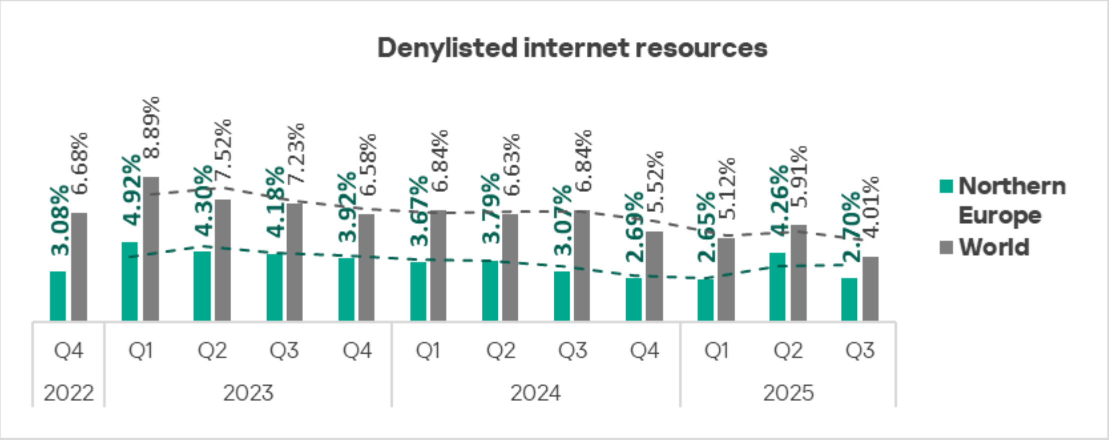
The highest position of Northern Europe in the rankings is for miners in the form of executable files for Windows.

Denylisted internet resources

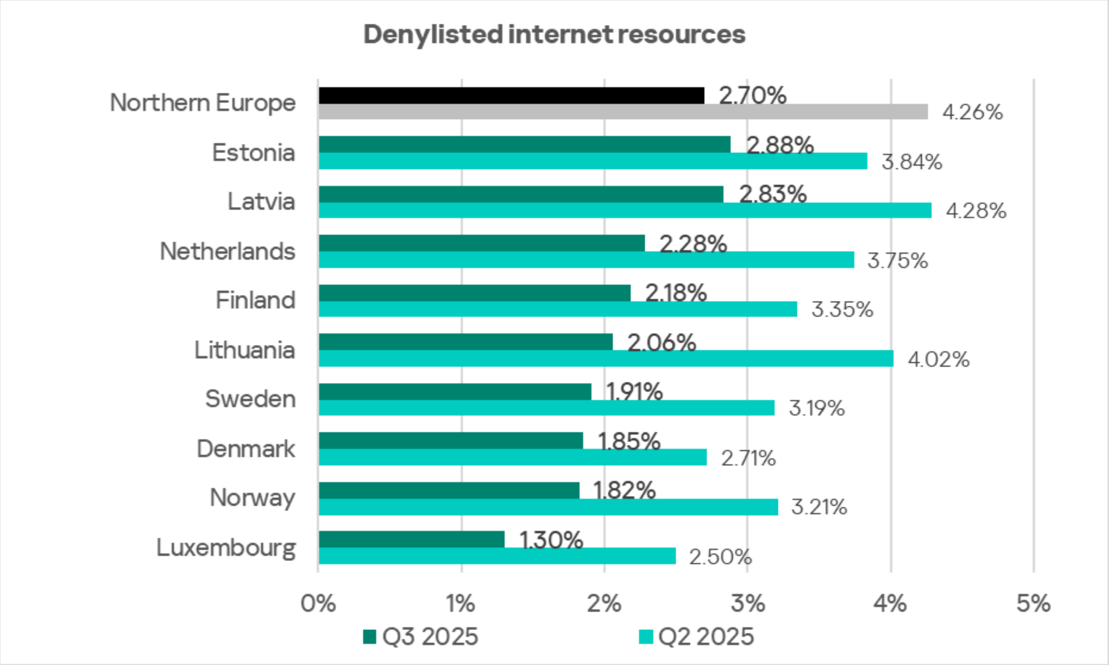
Denylisted internet resources are used by threat actors for initial infection. A significant portion of these resources is used to spread malicious scripts and phishing pages (HTML), which, in turn, can also be used to download cryptominers.

Based on the percentage of ICS computers on which denylisted internet resources are blocked, Northern Europe ranks 11th with a figure of 2.70%. This figure is 1.1 times higher than in Australia and New Zealand, which has the lowest rate.

In Q3 2025, just like in all regions, Northern Europe saw a decrease in the percentage of ICS computers on which denylisted internet resources were blocked.



Among countries of the region, Estonia leads with 2.88% in the percentage of ICS computers on which denylisted internet resources are blocked. Over the quarter, this indicator decreased in all countries of the region.

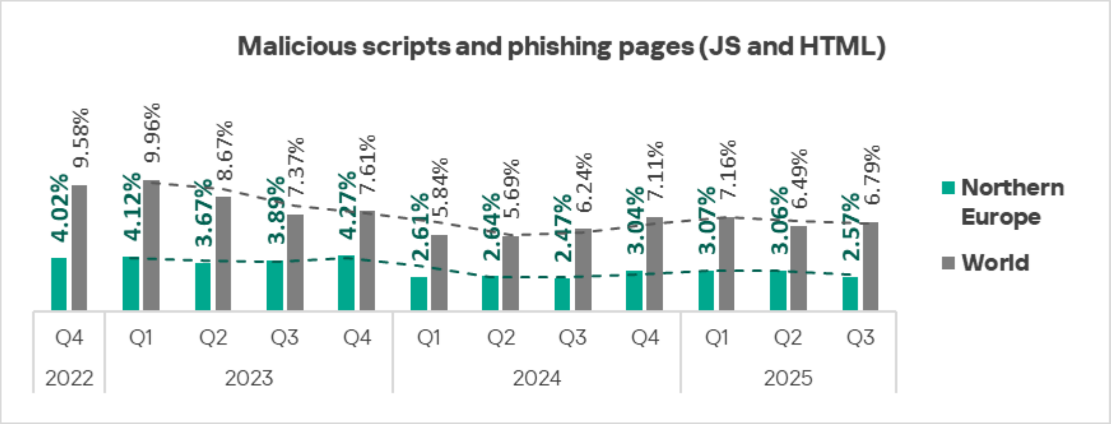


Malicious scripts and phishing pages

Malicious scripts are used by threat actors for a wide range of tasks including data collection, tracking, and redirecting the user's browser to malicious web resources, and downloading various malware into the system or browser (such as silent cryptomining). They are distributed both via the internet and through spam emails.

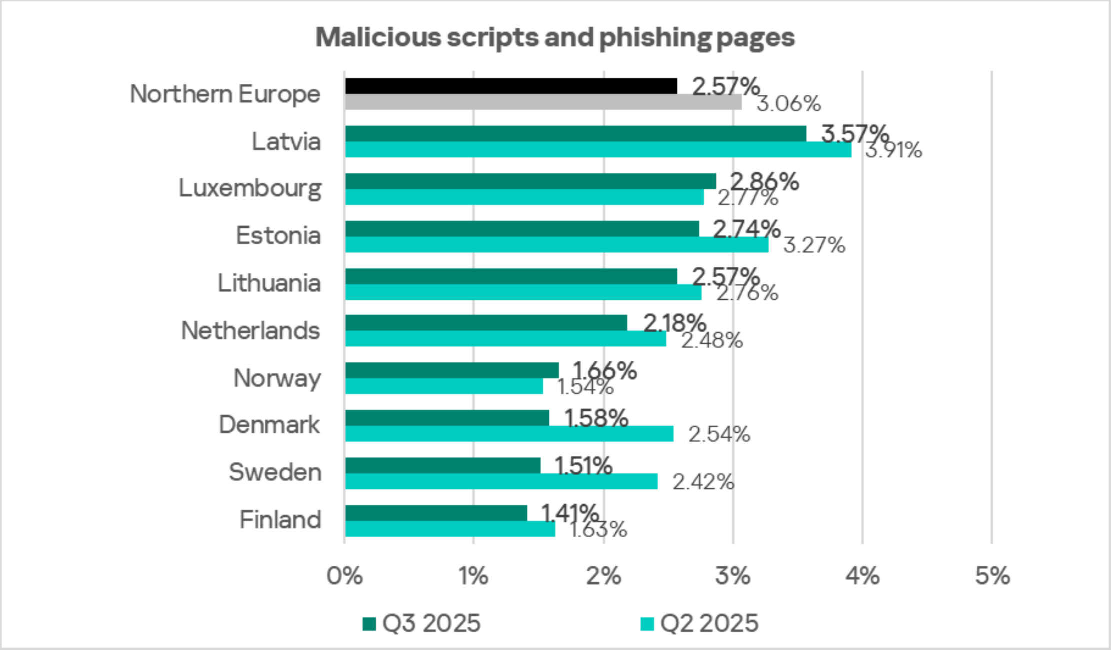
Based on the percentage of ICS computers on which malicious scripts and phishing pages are blocked, Northern Europe ranks 14th among regions with 2.57%.

The percentage of ICS computers on which malicious scripts and phishing pages are blocked fluctuates in the region. In Q3 2025, the indicator reached a three-year low.



Among countries in the region, Latvia leads with 3.57% in the percentage of ICS computers on which malicious scripts and phishing pages are blocked.

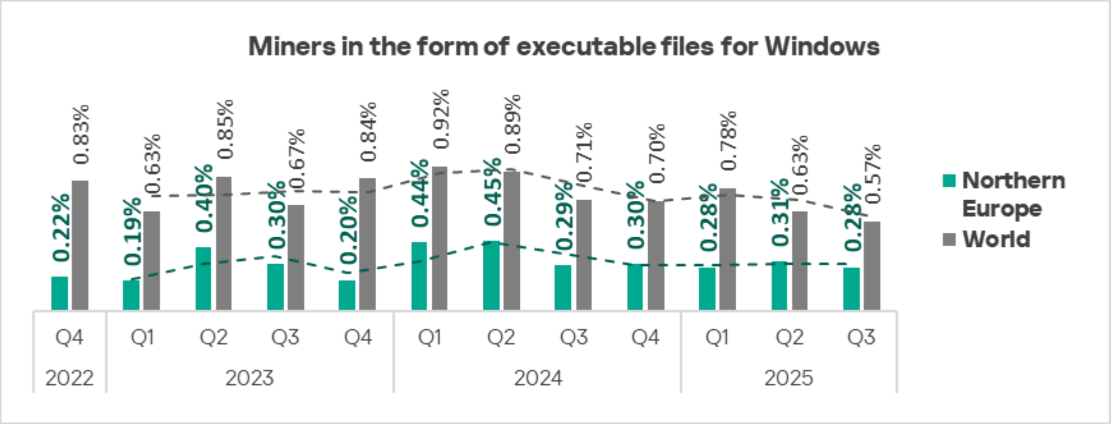
Over the quarter, this indicator decreased in all countries of the region except Luxembourg and Norway.



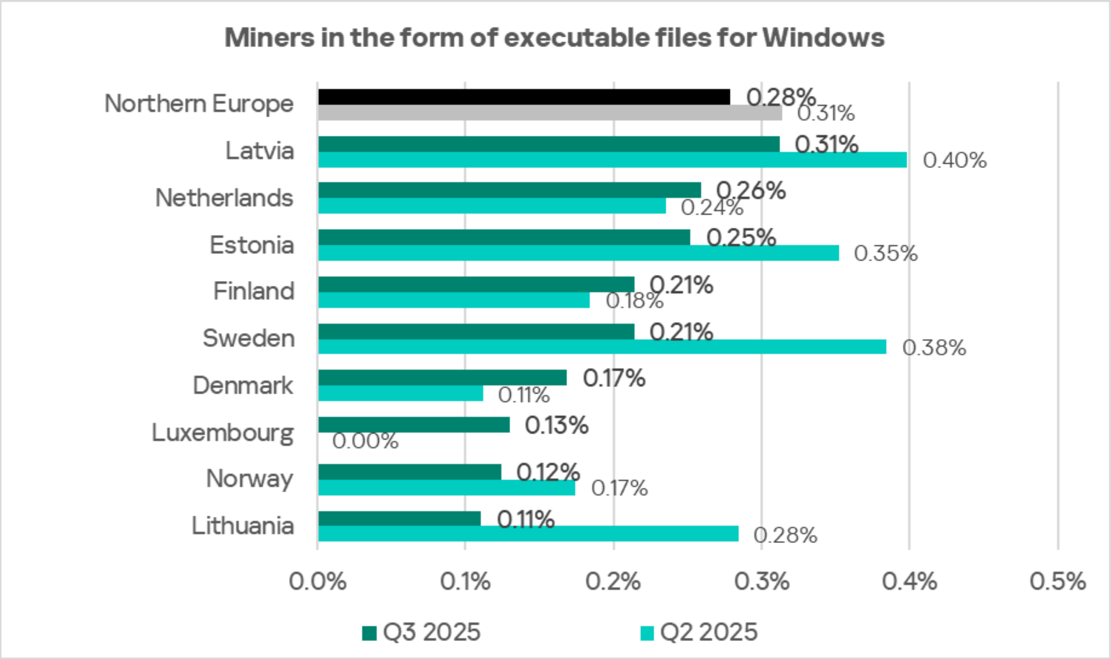
Miners in the form of executable files for Windows

Based on the percentage of ICS computers on which miners in the form of executable files for Windows are blocked, Northern Europe ranks ninth globally. This is the highest position of Northern Europe in the rankings, both by threat categories and by threat sources.

The indicator in the region fluctuates. In Q3 2025, it decreased to 0.28%. This indicator is 2.2 times higher than in the Australia and New Zealand region, which has the lowest figure among regions.



Among countries of the region, Latvia leads with 0.31% in the percentage of ICS computers on which miners in the form of executable files for Windows are blocked. Over the quarter, this indicator grew in the Netherlands, Finland, Denmark, and Luxembourg.

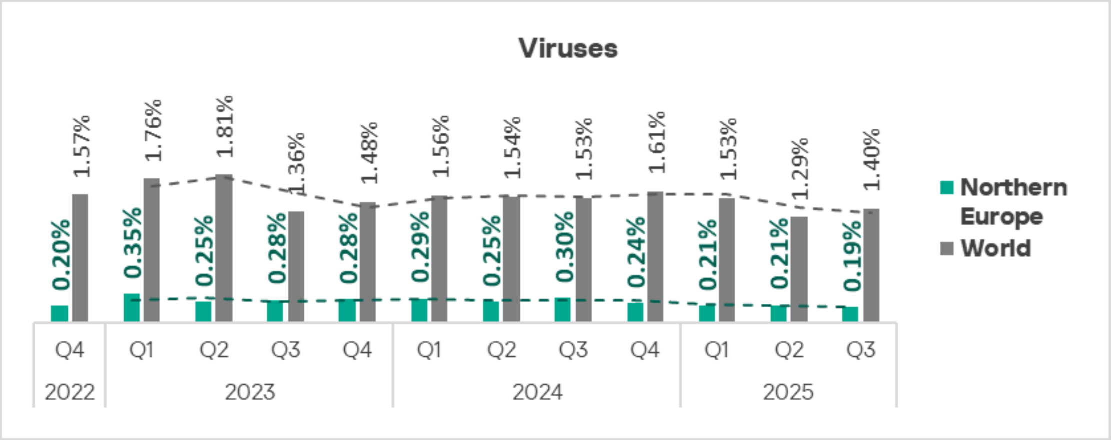


In Northern Europe, miners in the form of executable files for Windows spread primarily via the internet.

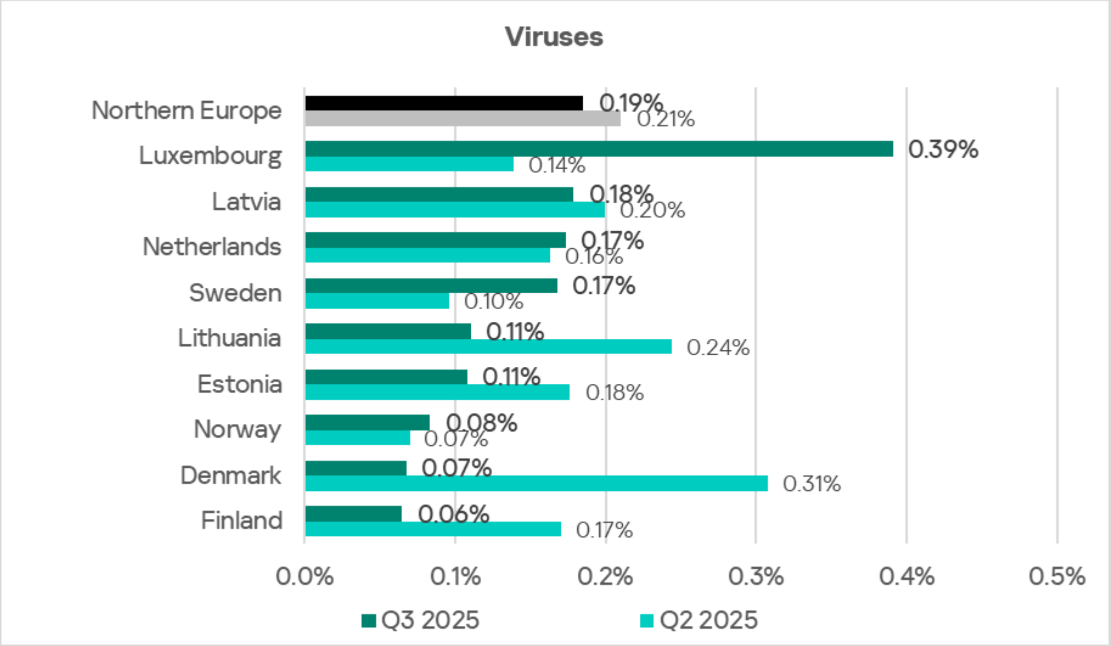
Viruses

Northern Europe ranks 13th among regions in the percentage of ICS computers on which viruses are blocked.

The figures over the quarter decreased to 0.19%. Although this is its lowest value over three years, this is still 1.2 times higher than in the Australia and New Zealand region, which sits at the bottom of this ranking.



Among countries of the region, based on the percentage of ICS computers on which viruses were blocked, Luxembourg leads with a wide margin after its indicator increased by a factor of 2.8 to 0.39% over the quarter. Latvia holds second place with 0.18%. In addition to Luxembourg, the indicator grew in Sweden, the Netherlands, and Norway.

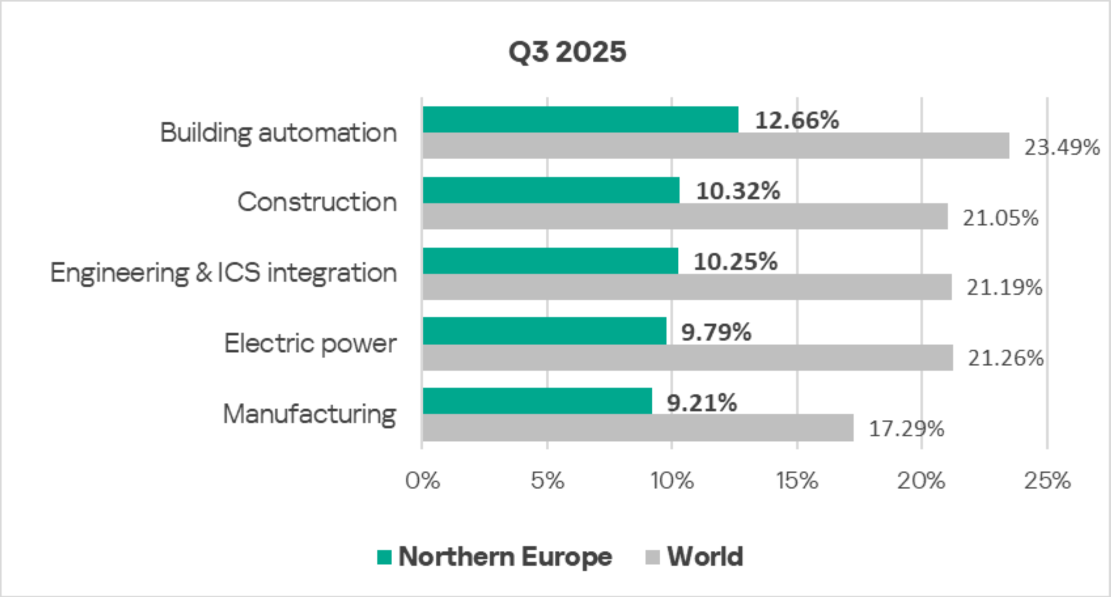


Viruses in the region spread through all threat sources, but mainly via email clients.

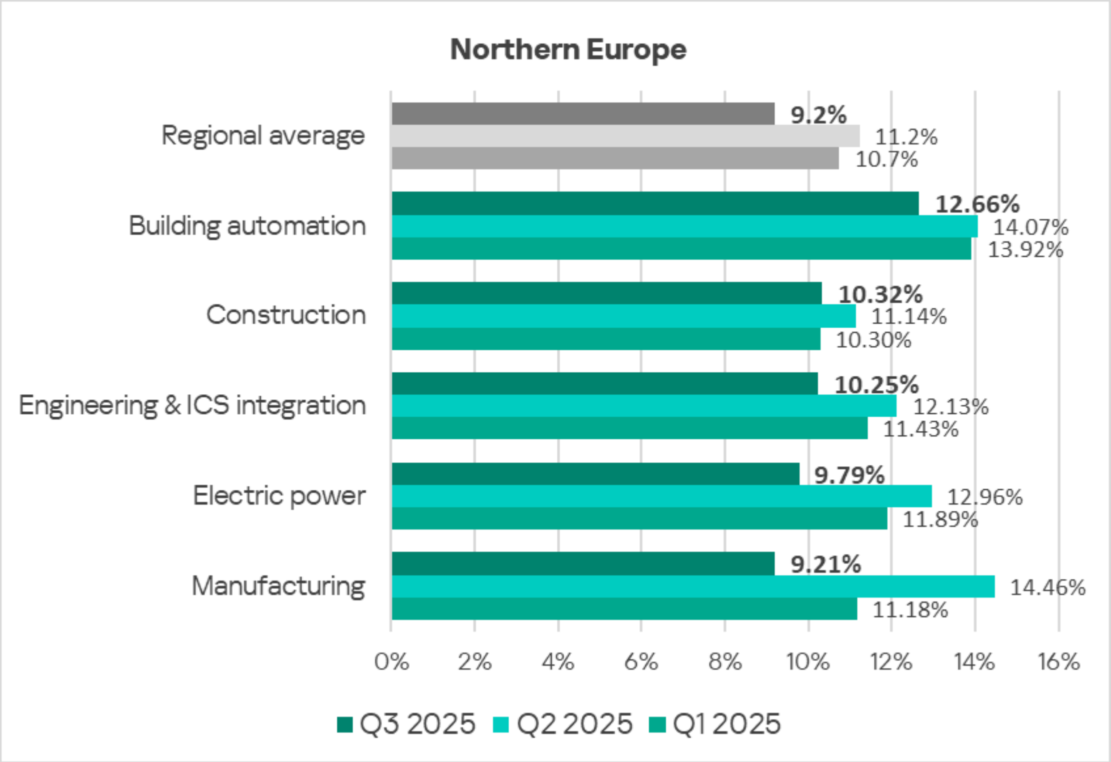
Industries

In Q3 2025, based on the percentage of ICS computers on which malicious objects were blocked, the building automation industry led the rankings of the studied industries and OT infrastructures in Northern Europe.

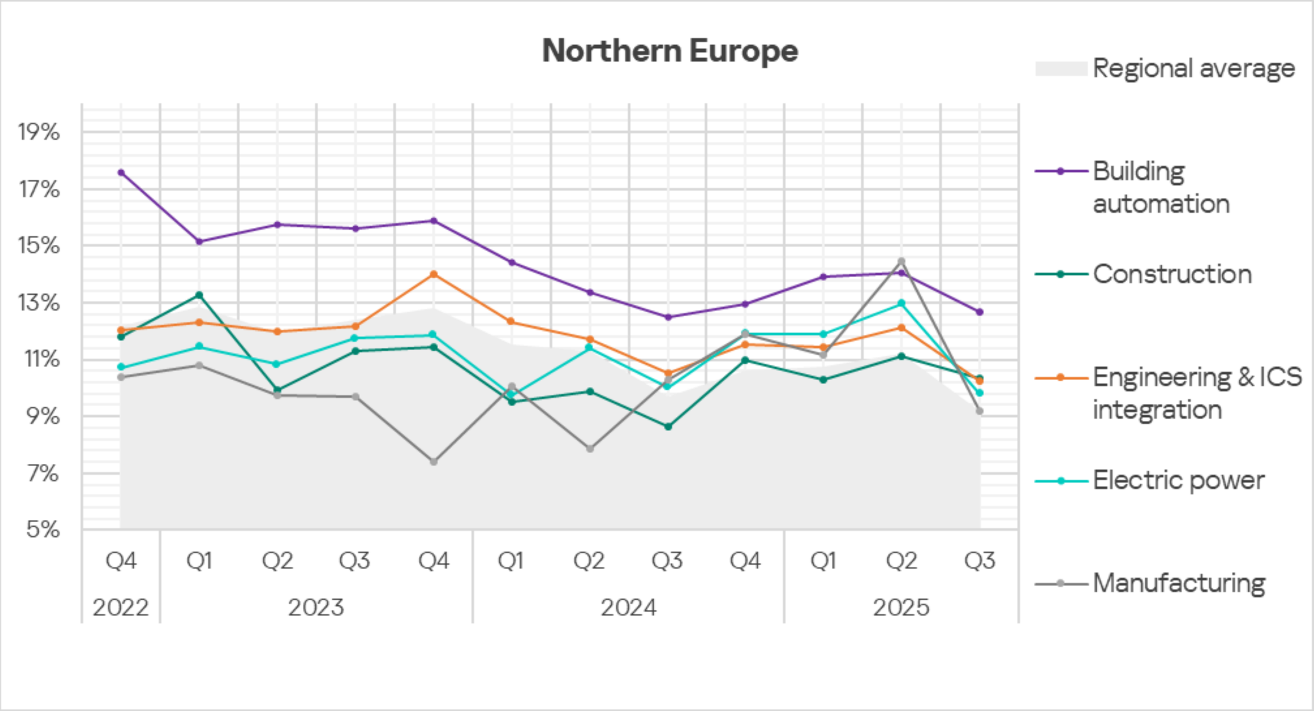
Rates across all industries in the region remain significantly below global averages.



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



The building automation trend continues to stand out well above the regional average.



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 Northern Europe, Q3 2025

Industry / Threat source	Building automation	Electric power	Engineering & ICS integration	Construction	Manufacturing	Threat category total in the region
Internet	5.60%	5.46%	5.64%	5.34%	5.34%	4.57%
Email clients	2.68%	0.45%	0.51%	0.85%	0.55%	0.84%
Removable media	0.12%	0.15%	0.05%	0.18%	0.18%	0.06%
Network folders	0.00%	0.00%	0.00%	0.00%	0.00%	0.01%
Industry total in the region	12.66%	9.79%	10.25%	10.32%	9.21%	

Threat category indicators for industries in Northern Europe, Q3 2025

Industry / Threat category	Building automation	Electric power	Engineering & ICS integration	Construction	Manufacturing	Threat category total in the region
Denylisted internet resources	3.37%	3.21%	3.46%	2.91%	3.68%	2.70%
Malicious scripts and phishing pages (JS and HTML)	4.14%	3.59%	2.90%	3.83%	2.76%	2.57%
Spy Trojans, backdoors and keyloggers	3.13%	2.09%	1.42%	1.82%	1.66%	1.40%
Worms	0.36%	0.52%	0.25%	0.43%	0.74%	0.22%
Miners in the form of executable files for Windows	0.42%	0.45%	0.25%	0.43%	0.92%	0.28%
Malicious documents (MSOffice + PDF)	1.70%	0.37%	0.33%	0.49%	0.37%	0.53%
Viruses	0.38%	0.52%	0.21%	0.43%	0.55%	0.19%
Ransomware	0.14%	0.22%	0.04%	0.00%	0.00%	0.05%
Web miners running in browsers	0.17%	0.07%	0.14%	0.06%	0.18%	0.10%
Malware for AutoCAD	0.00%	0.00%	0.02%	0.12%	0.00%	0.01%
Industry total in the region	12.66%	9.79%	10.25%	10.32%	9.21%	

In the rankings of regions based on the percentage of ICS computers on which malicious objects were blocked in various industries, Northern Europe occupies the last places (13th and 14th).

Miners of both categories pose a major threat for the region.

Among regions based on indicators in the manufacturing industry, Northern Europe ranks second in the percentage of ICS computers on which miners in the form of executable files for Windows are blocked.

Building automation

Northern Europe ranks 13th among regions based on the percentage of ICS computers on which malicious objects were blocked in the building automation industry.

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

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

- Second place in internet threats.
- First place in the percentage of ICS computers on which the following threat categories were blocked: malicious scripts and phishing pages, spyware, and malicious documents.
- Second place in web miners and ransomware.
- Third place in denylisted internet resources.

Construction

Northern Europe ranks 14th among regions in the percentage of ICS computers on which malicious objects were blocked in the construction industry.

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

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

Engineering and ICS integrators

Northern Europe ranks 14th among regions in the percentage of ICS computers on which malicious objects were blocked in the engineering and ICS integrators industry.

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

- First place based on the percentage of ICS computers on which internet threats were blocked.
- Second place in denylisted internet resources and malware for AutoCAD.
- Third place in web miners and ransomware.

Electrical power

Northern Europe ranks 13th among regions in the percentage of ICS computers on which malicious objects were blocked in the electrical energy industry.

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

- Third place in the percentage of ICS computers on which internet threats and removable media threats were blocked.
- First place in the percentage of ICS computers on which ransomware was blocked.

- Second place in the following threat categories: spyware, miners in the form of executable files for Windows, worms, and viruses.
- Third place in the following threat categories: malicious scripts and phishing pages, malicious documents.

Manufacturing

Northern Europe ranks 14th in the percentage of ICS computers on which malicious objects were blocked in the manufacturing industry.

Based on industry indicators among regions, Northern Europe has the following rankings:

- Second place in the percentage of ICS computers on which miners in the form of executable files for Windows are blocked.

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

- First place in the percentage of ICS computers on which threats from removable media are blocked.
- Third for threats from email clients.
- First place in the percentage of ICS computers on which the following threat categories are blocked: denylisted internet resources, both categories of miners, worms, and viruses.

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