Kaspersky ICS CERT

kaspersky

Threat landscape for industrial automation systems

Europe. Q2 2025

23.09.2025

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 were blocked exceeds the global average by 1.4 times.

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, the percentage of ICS computers on which malicious scripts and phishing pages were blocked is 1.1 times higher than the global average.

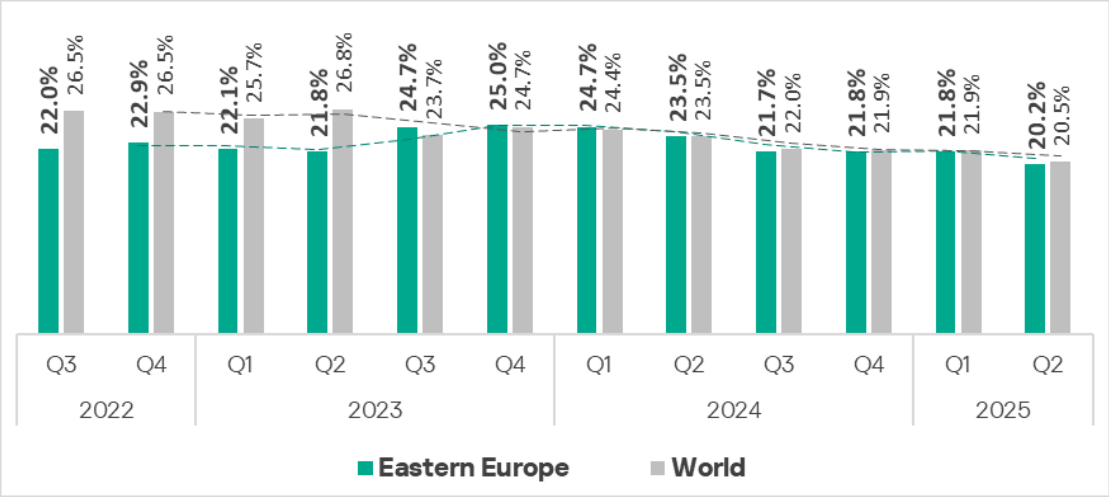
High rate of spyware

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.

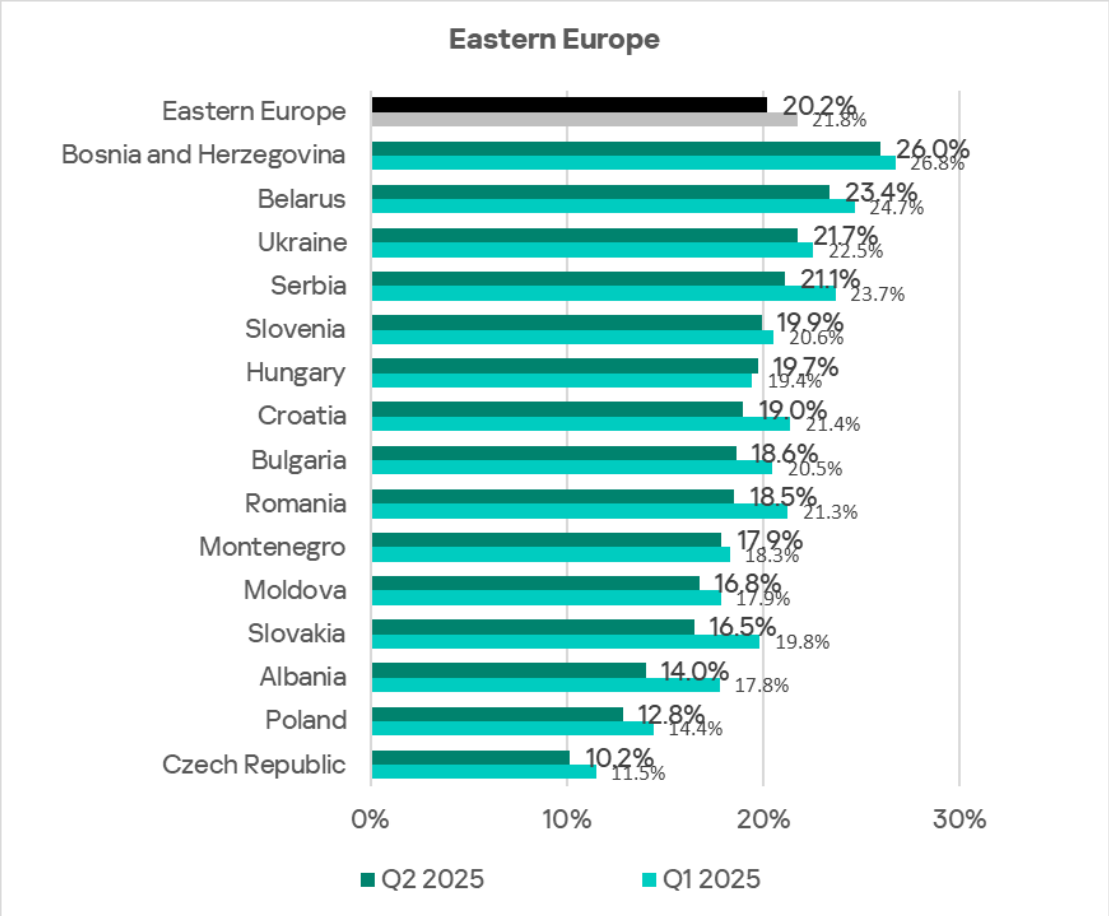
Statistics across all threats

In Q2 2025, Eastern Europe ranked sixth among all regions for the percentage of ICS computers on which malicious objects were blocked. This is the highest position of any European region. Before Q2 2023, the region never ranked higher than ninth.

In Q2 2025, this figure fell to 20.2% — slightly below the global average, but still 1.8 times higher than Northern Europe, the lowest-ranked region.

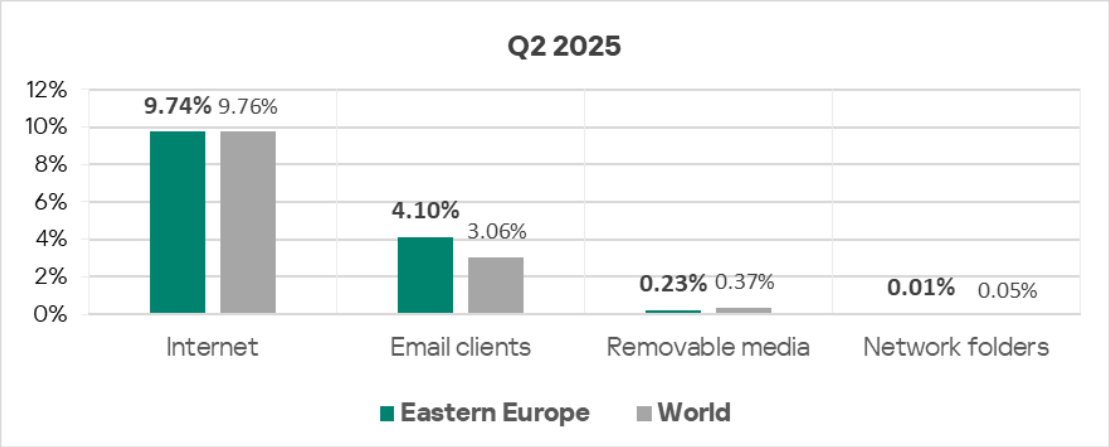


Among the region's countries, Bosnia and Herzegovina leads in this metric with 26.0%. The Czech Republic had the lowest figure at 10.2%.



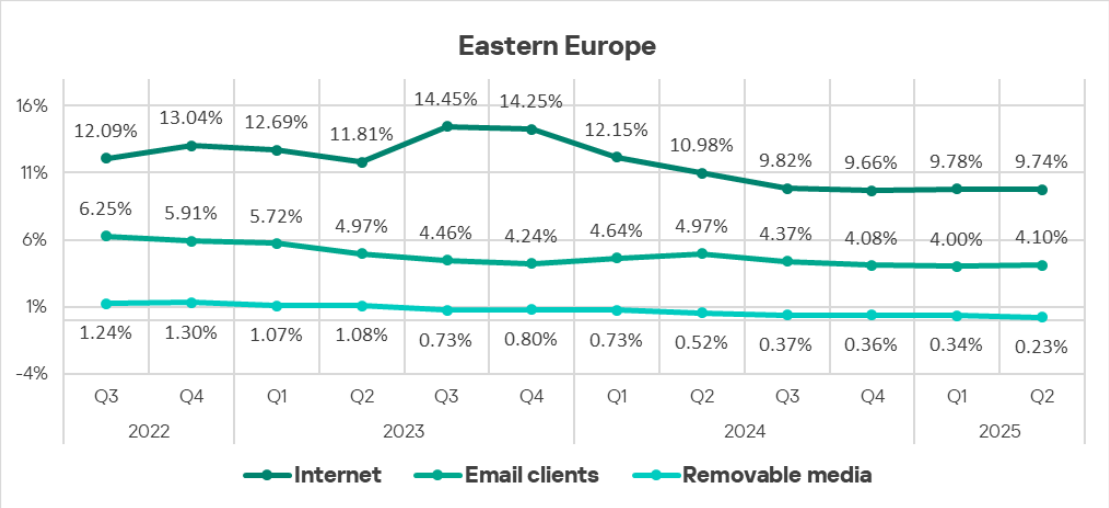
Threat sources

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 threats from email clients were blocked is 1.3 times higher than the global average.



Malicious objects in the region spread primarily via the internet and email. Eastern Europe ranked second-to-last among regions by the percentage of ICS computers on which threats from network folders were blocked.

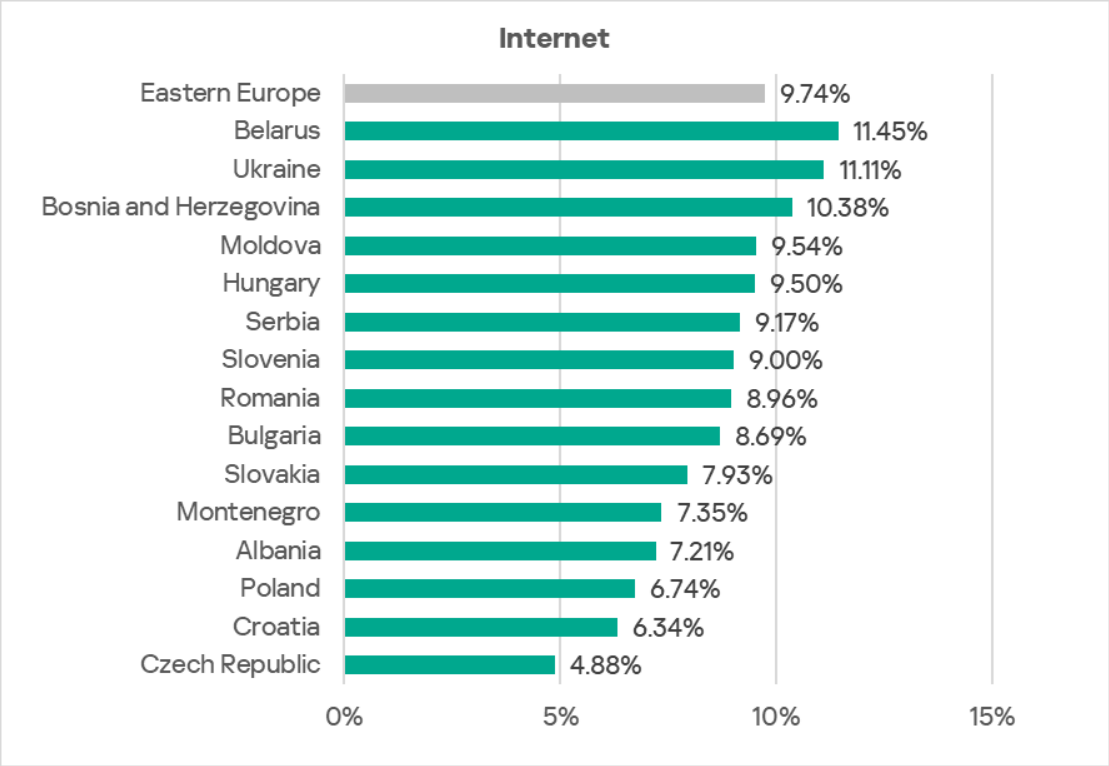
In Q2 2025, of all threat sources, only email clients showed a slight increase in the percentage of ICS computers with blocked malicious objects.



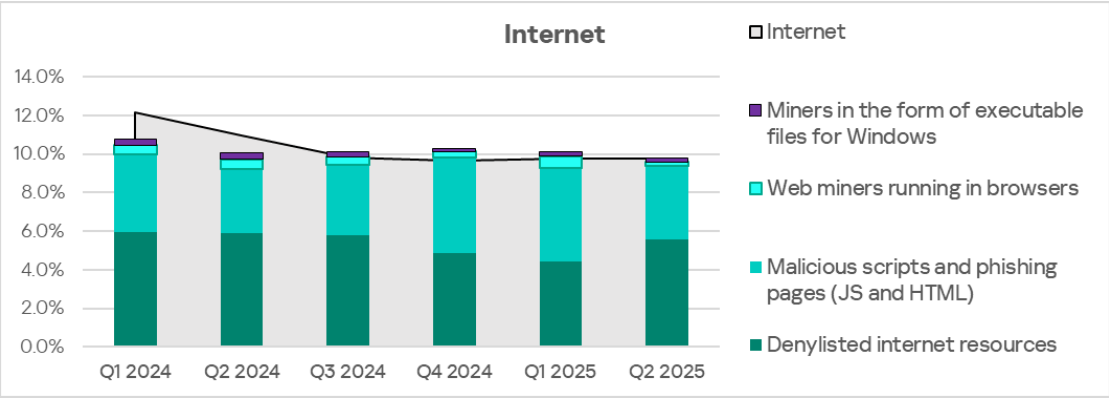
Internet

By percentage of ICS computers on which threats from the internet were blocked, Eastern Europe ranked fifth among regions at 9.74% — 1.5 times higher than the minimum (East Asia).

Country-level rates range from 4.88% in the Czech Republic to 11.45% in Belarus.



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

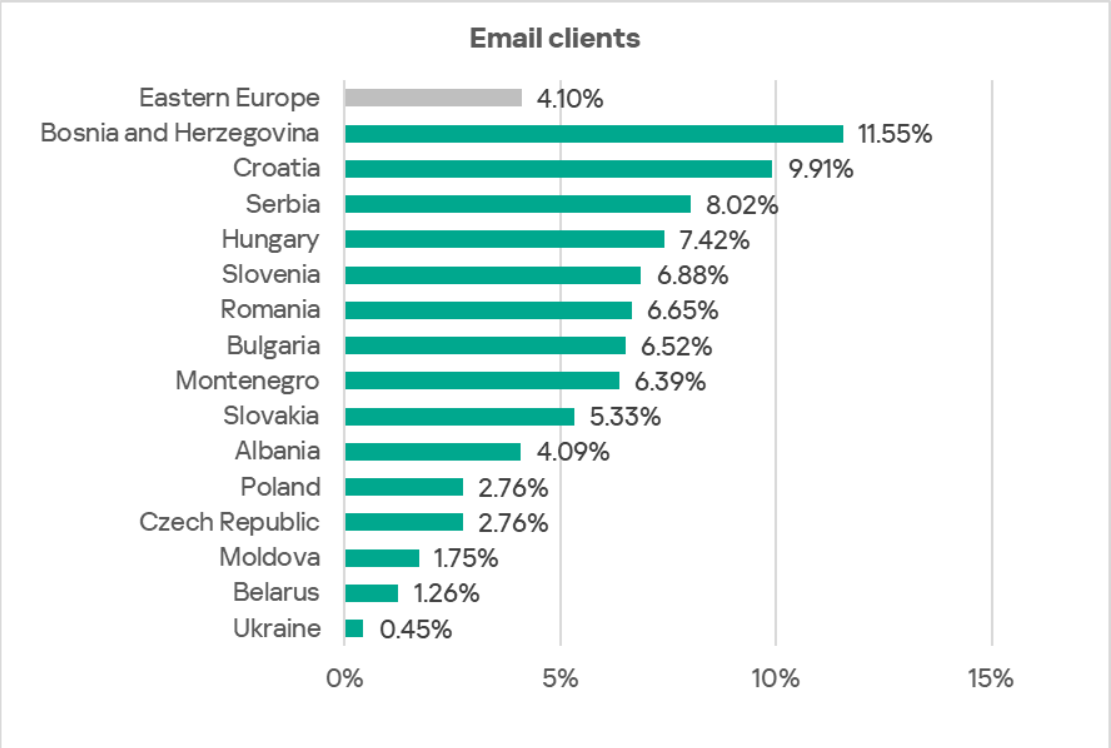


In terms of denylisted internet resources, Eastern Europe ranks third globally. In miners in the form of executable files, it ranks fourth.

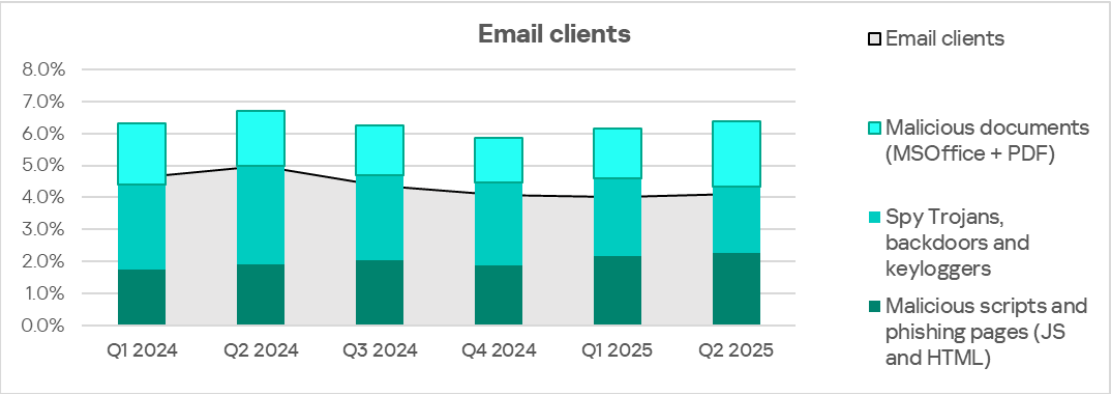
Email clients

By the percentage of ICS computers on which threats from email clients were blocked, Eastern Europe ranked sixth globally in Q2 2025, at 4.10%. This is 5.1 times higher than in Russia, which ranks last.

Among countries in the region, Bosnia and Herzegovina leads with 11.55%, while Ukraine ranks lowest at 0.45%.



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

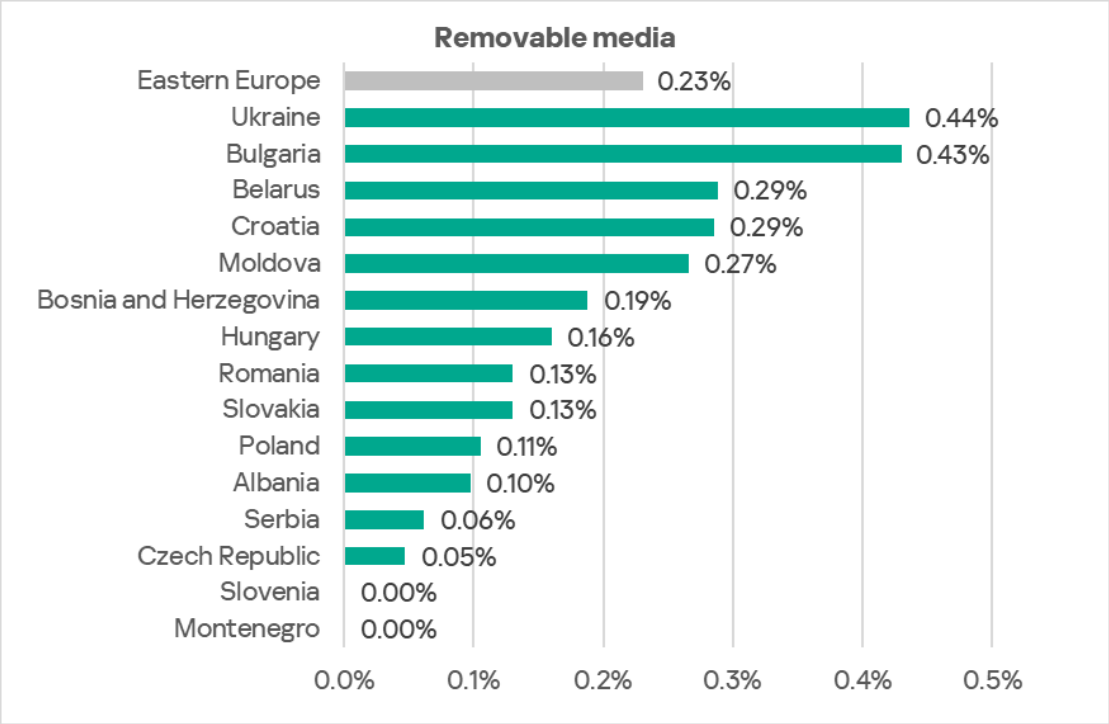


The top three countries by email client threats — Bosnia and Herzegovina, Croatia, and Serbia — also rank highest for malicious documents and spyware. In addition, Bosnia and Herzegovina and Serbia lead in the percentage of ICS computers on which malicious scripts and phishing pages were blocked.

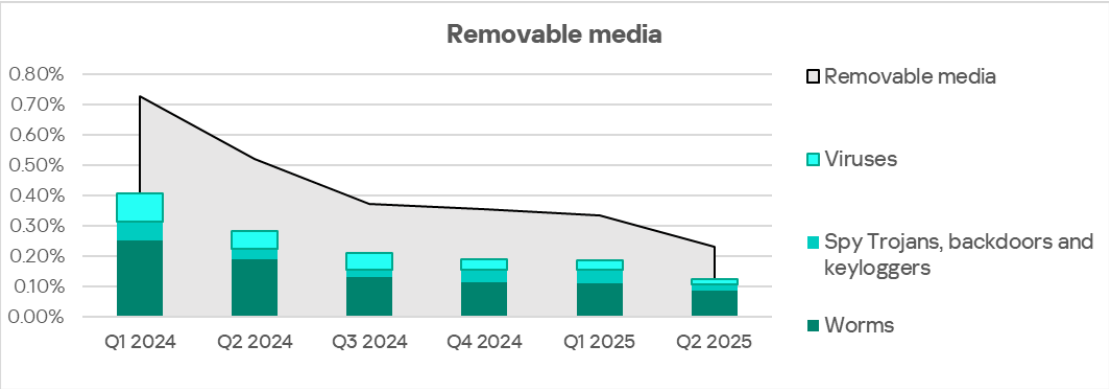
Removable media

In terms of ICS computers on which threats from removable media were blocked, Eastern Europe ranked seventh globally in Q2 2025, at 0.23%. Compared to North America (Canada), which ranks last, the rate is 8.6 times higher.

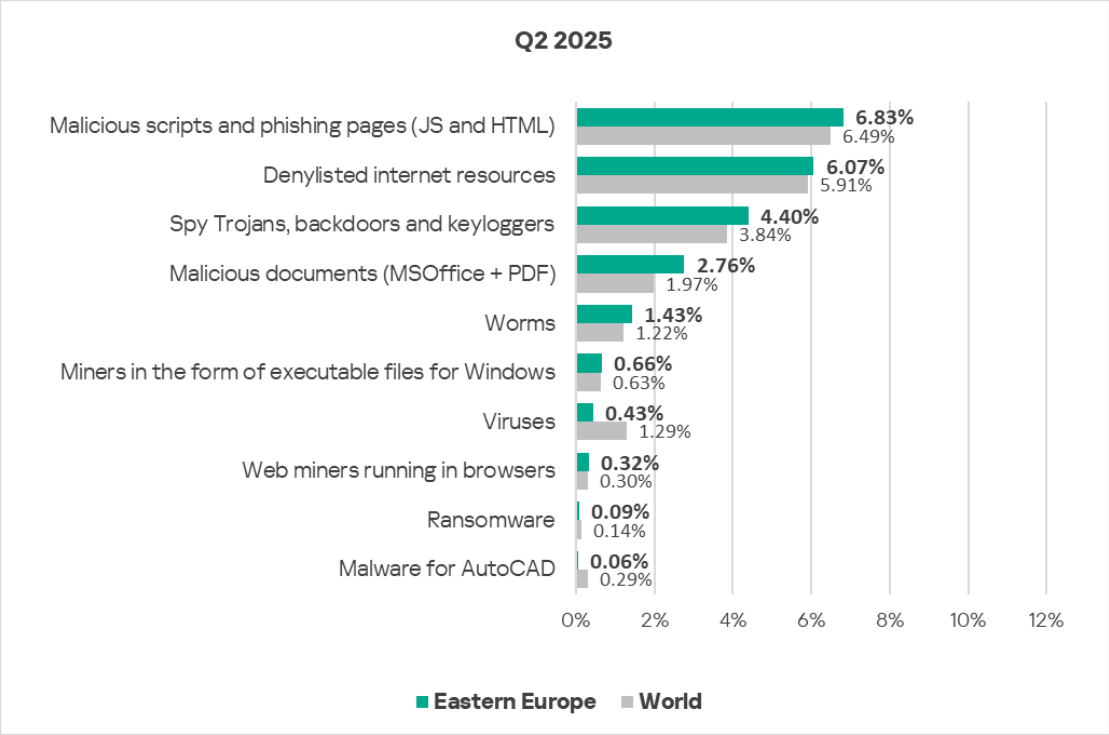
Among the countries in the region, Ukraine (0.44%) and Bulgaria (0.43%) lead by a wide margin in this metric.

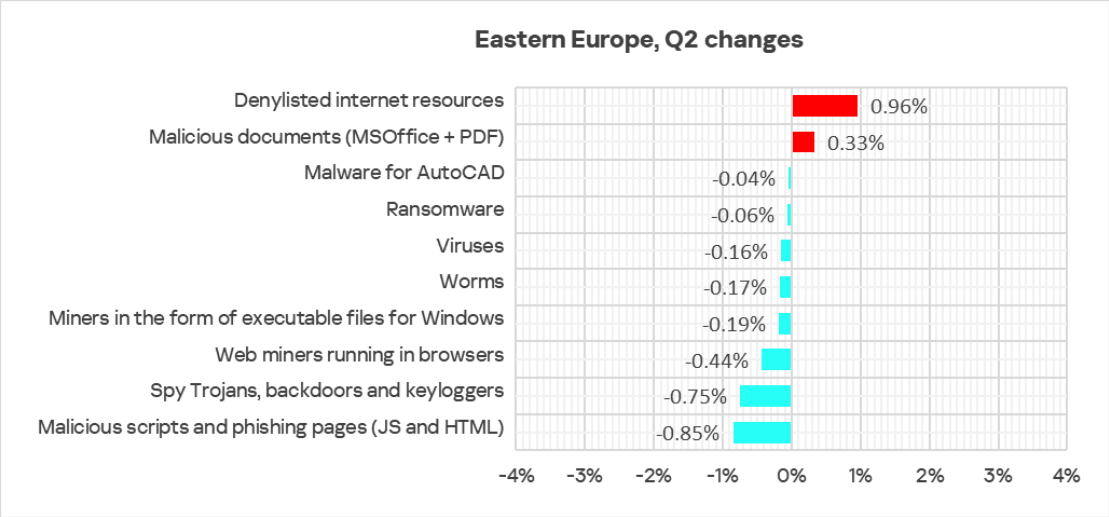


The main categories of threats blocked when connecting removable media to ICS computers are worms, spyware, and viruses.



Threat categories





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

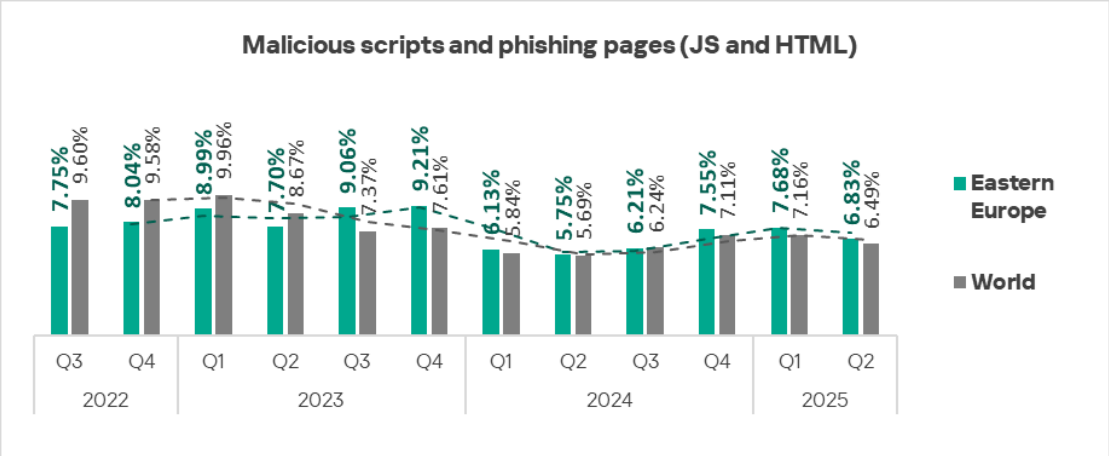
- Malicious documents: 1.4 times higher
- Malicious scripts and phishing pages: 1.1 times higher
- Spyware: 1.1 times higher
- Worms: 1.2 times higher
- Web miners: 1.1 times higher

Malicious scripts, phishing pages, and malicious documents are often used by attackers to deliver targeted malware — including spyware.

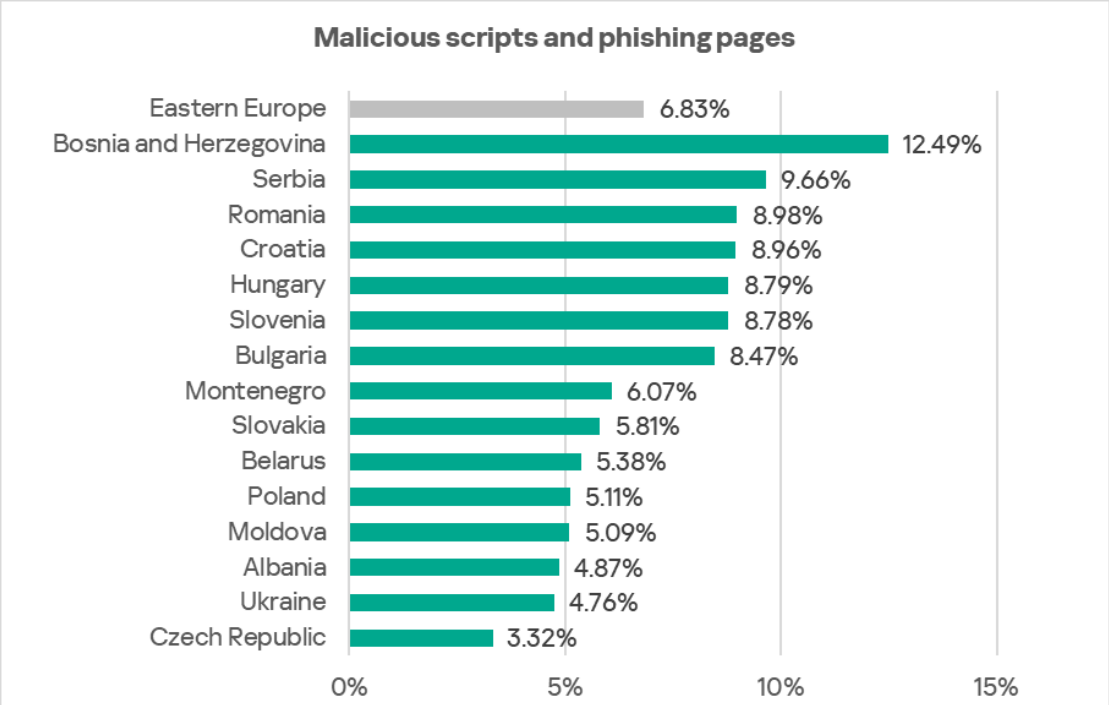
Bosnia and Herzegovina, Croatia, and Serbia rank in the top three for email client threats and for the percentage of ICS computers on which malicious documents and spyware were blocked. Bosnia and Herzegovina and Serbia also lead in malicious scripts and phishing pages.

Malicious scripts and phishing pages

Eastern Europe ranks seventh among regions by the percentage of ICS computers on which malicious scripts and phishing pages were blocked, at 6.83%. This figure is 2.2 times higher than in Northern Europe, which has the lowest rate.



Among countries in the region, Bosnia and Herzegovina leads in this metric with 12.49%.

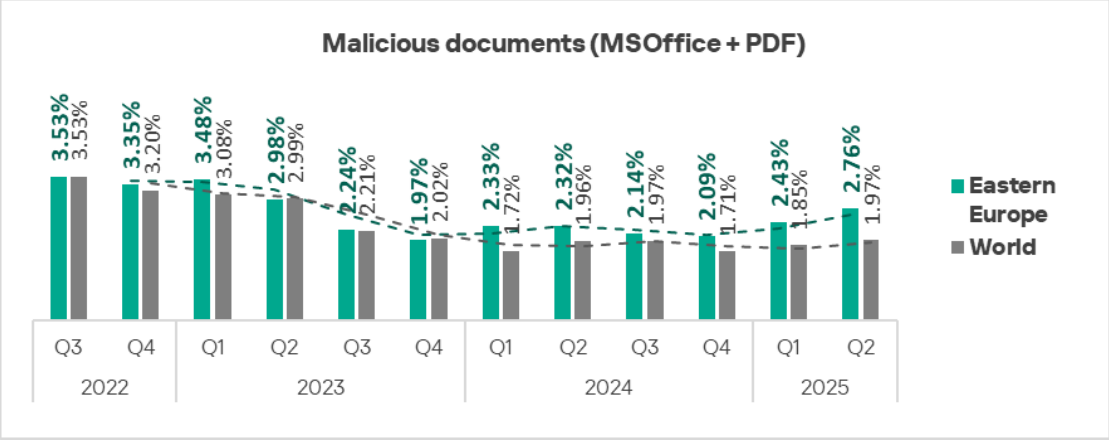


Malicious scripts and phishing pages spread both via the internet and through email.

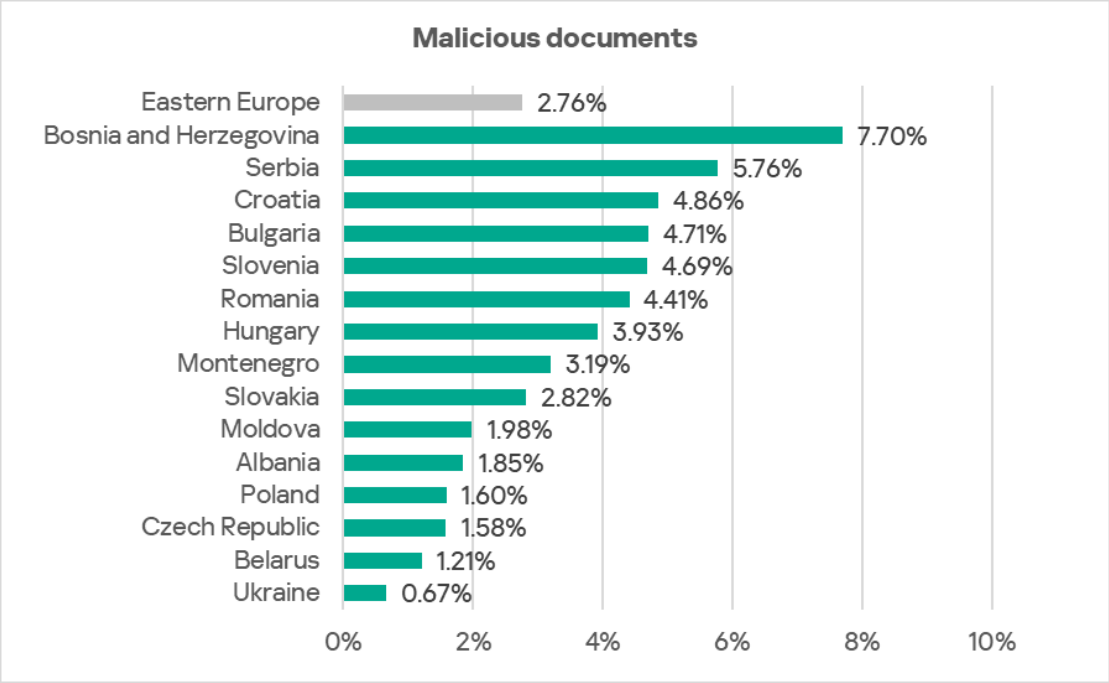
Malicious documents

Eastern Europe ranks fifth globally by the percentage of ICS computers on which malicious documents were blocked. The region's figure is 2.76%, 4.3 times higher than in Northern Europe, which ranks last.

The percentage of ICS computers on which malicious documents were blocked has been rising in the region for two consecutive quarters.



Among countries in the region, Bosnia and Herzegovina leads with 7.70%.

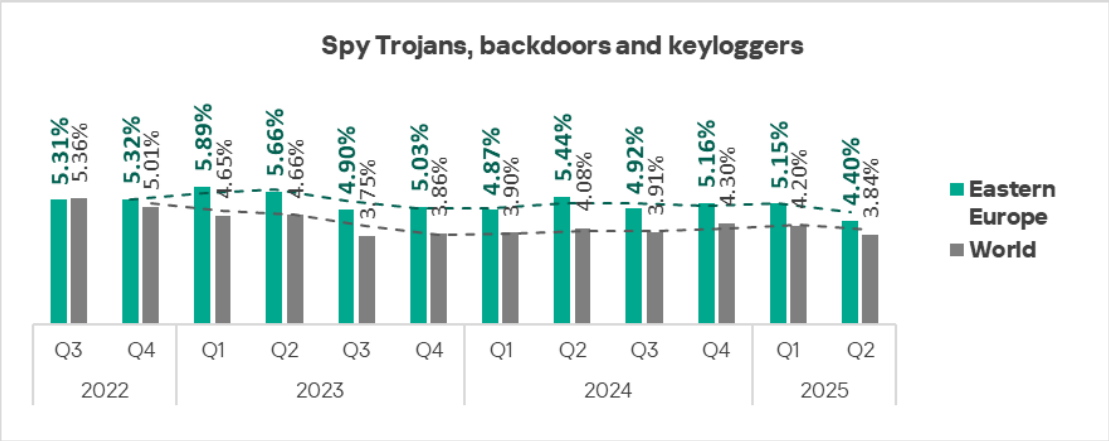


Malicious documents were distributed primarily via email.

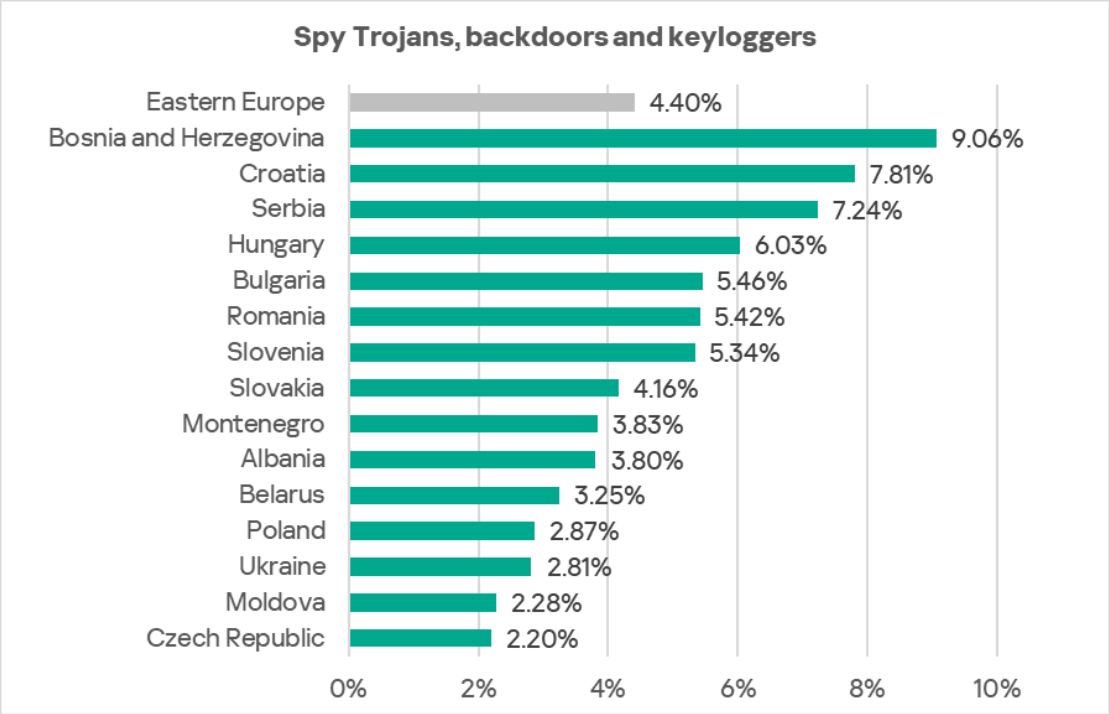
Spyware

By the percentage of ICS computers on which spyware was blocked, Eastern Europe ranks sixth globally with 4.40%. This is 3.2 times higher than in Western Europe, which has the lowest figure.

The percentage of ICS computers in Eastern Europe on which spyware was blocked fluctuates over time. In Q2 2025, it reached its lowest since Q3 2022.



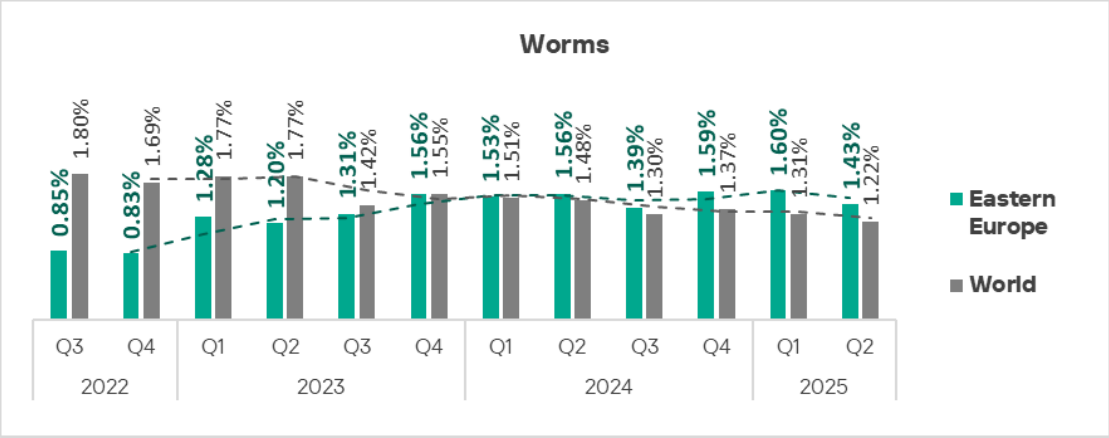
Among the region's countries and territories, Bosnia and Herzegovina leads with 9.06%, while the lowest rate is in the Czech Republic (2.20%).



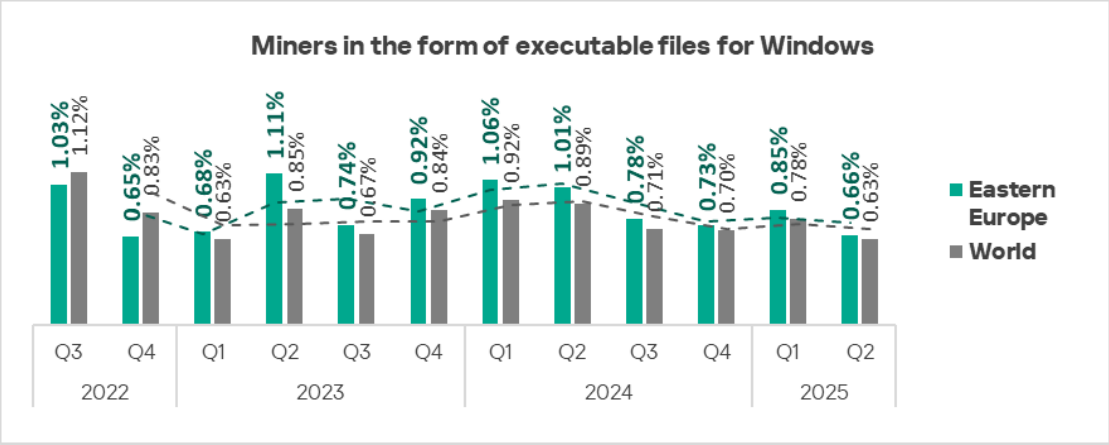
Spyware is blocked across all threat sources in the region but is most common in email clients.

Worms and miners in the form of executable files for Windows

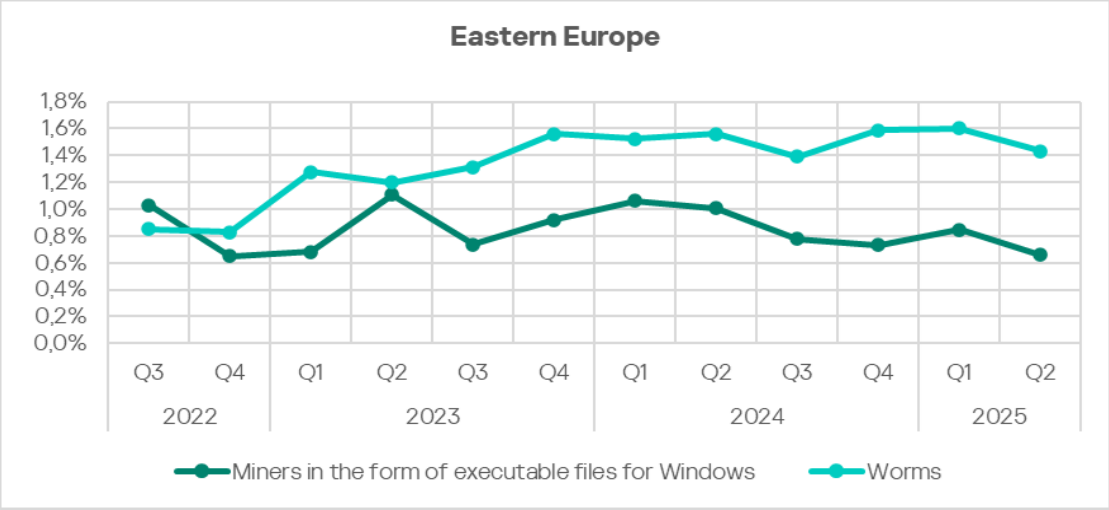
By the percentage of ICS computers with blocked worms, East Europe ranks fifth globally, with 1.43%. This figure is 6.5 times higher than in the Australia and New Zealand region, which ranks last.



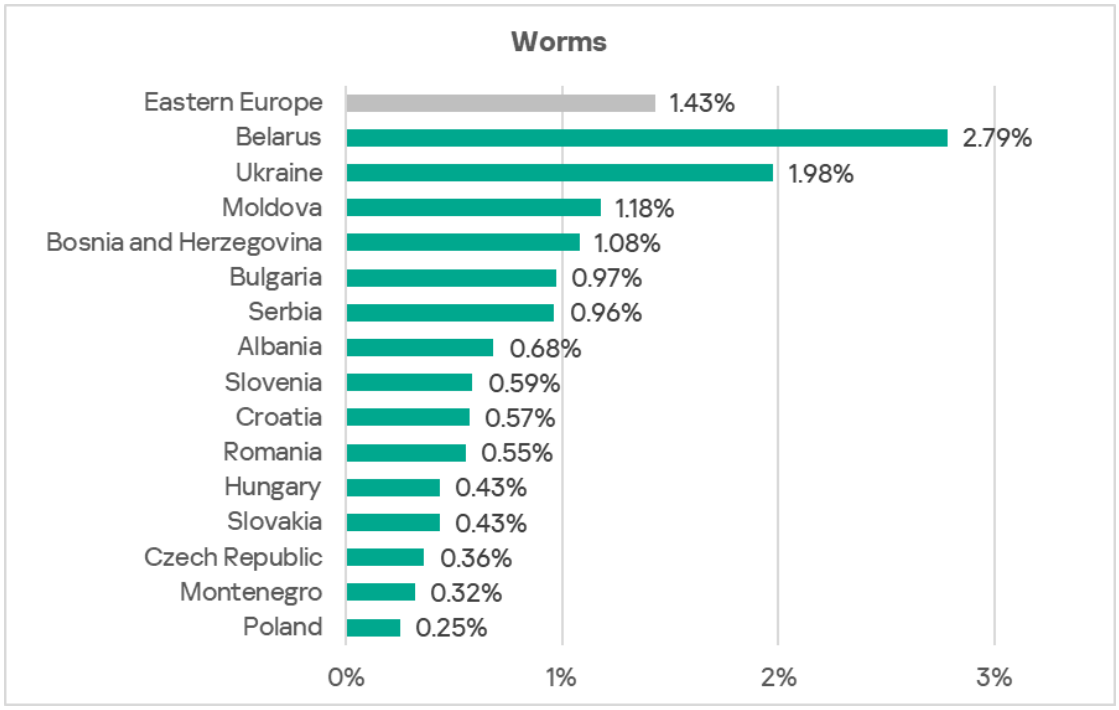
For miners in the form of executable files for Windows, the region ranks fourth, with 0.65%. This is 3.5 times higher than in East Asia, which has the lowest rate.

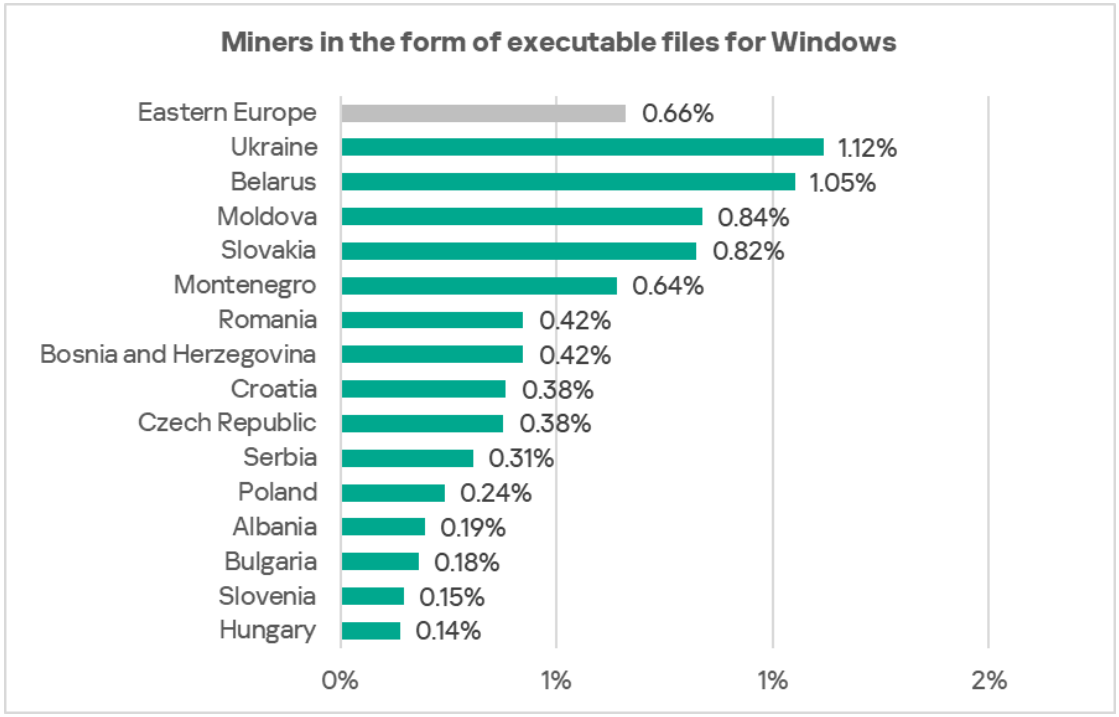


In Eastern Europe, the dynamics of these two categories are closely linked. This is because miners for Windows use modules and components that are essentially worms and serve to deliver the miner to other computers in the network (automated lateral movement). A similar situation is observed in Russia.



Among the region's countries, Belarus, Ukraine, and Moldova lead in the percentage of ICS computers with blocked worms. These three countries also lead in miners in the form of executable files for Windows.



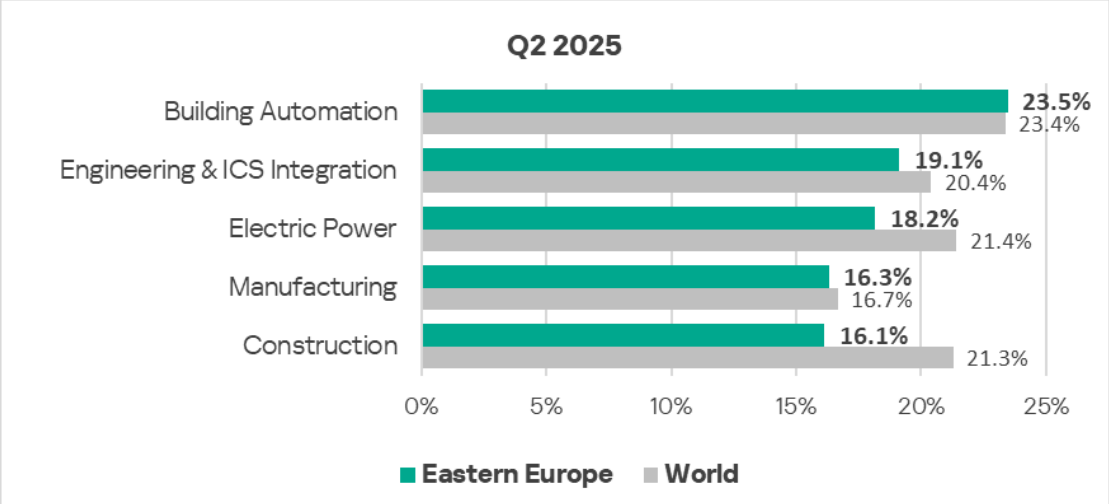


Ukraine and Belarus also rank in the top three for threats from removable media.

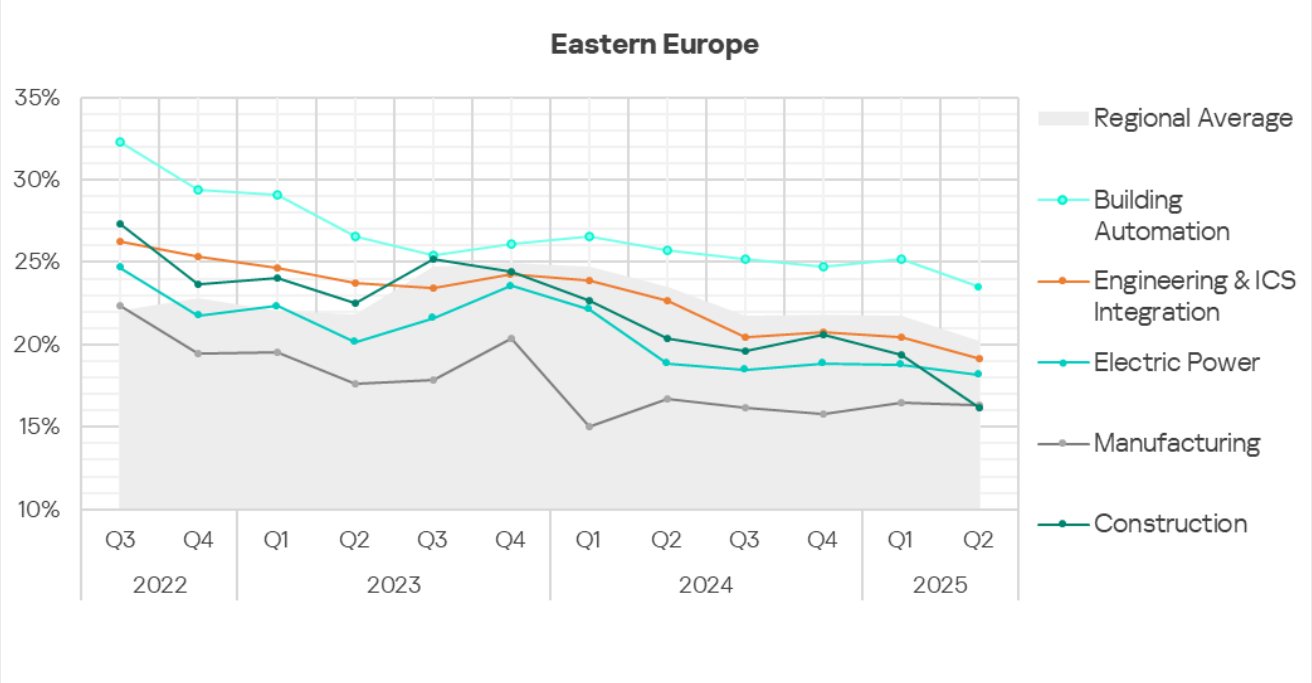
Industries

Of the region's industries considered in this report, building automation is the most frequently targeted. This is the only industry where the rate slightly

exceeds the global average. This is also the only one where the figure did not decline in Q2 2025.



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



Threat sources and malware categories in industries: hot spots

We use heat maps to assess threats facing industries. On these maps, cells are colored from red to green, where red indicates the maximum value for an industry in the region or a threat source or category across all regions and industries. In Eastern Europe, values closest to maximum are observed for the

aggregate score for building automation, as well as denylisted internet resources in the construction industry.

Threat source indicators for industries in Eastern Europe, Q2 2025

Industry / Threat source	Building Automation	Electric Power	Engineering & ICS Integration	Construction	Manufacturing	Threat category total in the region
Internet	9.85%	9.50%	10.28%	10.78%	9.70%	9.74%
Email clients	8.39%	3.25%	3.32%	2.08%	2.07%	4.10%
Removable media	0.32%	0.30%	0.20%	0.25%	0.13%	0.23%
Network folders	0.01%	0.05%	0.01%	0.00%	0.00%	0.01%
Industry total in the region	23.47%	18.17%	19.11%	16.13%	16.30%	

Threat category indicators for industries in Eastern Europe, Q2 2025

Industry / Threat category	Building Automation	Electric Power	Engineering & ICS Integration	Construction	Manufacturing	Threat category total in the region
Denylisted internet resources	5.65%	6.45%	6.69%	7.75%	6.86%	6.07%
Malicious scripts and phishing pages (JS and HTML)	10.01%	6.30%	6.45%	6.49%	5.30%	6.83%
Spy Trojans, backdoors and keyloggers	7.60%	3.69%	3.89%	2.52%	3.49%	4.40%
Worms	1.44%	1.67%	1.10%	0.57%	1.68%	1.43%
Miners in the form of executable files for Windows	0.66%	0.44%	0.72%	0.88%	0.65%	0.66%
Malicious documents (MSOffice + PDF)	5.59%	2.12%	2.06%	1.20%	1.55%	2.76%
Viruses	0.52%	0.59%	0.38%	0.63%	0.78%	0.78%
Ransomware	0.18%	0.10%	0.06%	0.06%	0.00%	0.00%
Web miners running in browsers	0.37%	0.34%	0.43%	0.44%	0.65%	0.32%
Malware for AutoCAD	0.01%	0.00%	0.08%	0.25%	0.00%	0.06%
Industry total in the region	23.47%	18.17%	19.11%	16.13%	16.30%	

Industry hot spots

Building automation

- Regional leader in the percentage of ICS computers on which threats from email clients and removable media were blocked.
- Regional leader in malicious scripts and phishing pages, spyware, malicious documents, and ransomware.

Engineering and ICS integrators

- Second place in the percentage of ICS computers on which threats from the internet and email clients were blocked.
- Second place regionally in miners in the form of executable files for Windows and malware for AutoCAD.

Electrical energy industry

- Regional leader in the percentage of ICS computers on which threats from network folders were blocked. Second place in removable media threats.
- Second place in malicious documents, worms, and ransomware.

Manufacturing

- Regional leader in worms, viruses, and web miners.
- Second place in denylisted internet resources.

Construction

- Regional leader by the percentage of ICS computers on which internet threats were blocked.
- Regional leader in denylisted internet resources and miners in the form of executable files for Windows.
- Second place in malicious scripts and phishing pages, viruses, and web miners.

Southern Europe

Key cybersecurity issues in the region

High risk of targeted attacks

In Q2 2025, industrial organizations in Southern European countries faced another wave of phishing campaigns, most notably targeting 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.

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

Southern Europe leads all regions in the percentage of ICS computers on which threats from email clients were blocked — 2.4 times higher than the global average.

It also ranks first globally in the percentage of ICS computers on which malicious documents were blocked — 2.2 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.

By the percentage of ICS computers on which malicious scripts and phishing pages were blocked, Southern Europe ranks second among regions globally, with a rate 1.4 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 spread both via the internet and through emails.

High rate of spyware

By the percentage of ICS computers on which spyware was blocked, Southern Europe ranks second, 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.

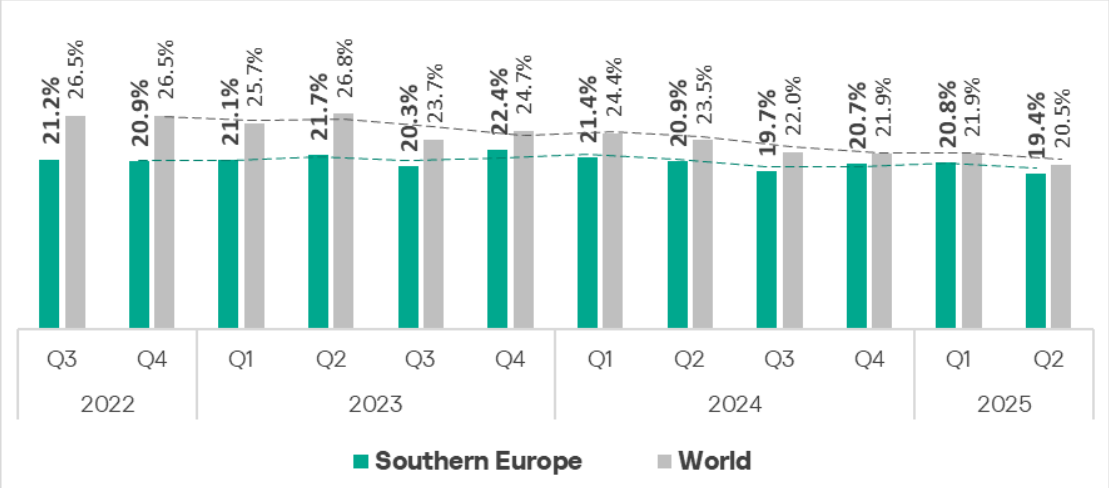
High ransomware rate

The region's percentage of ICS computers on which ransomware was blocked is 1.4 times higher than the global average.

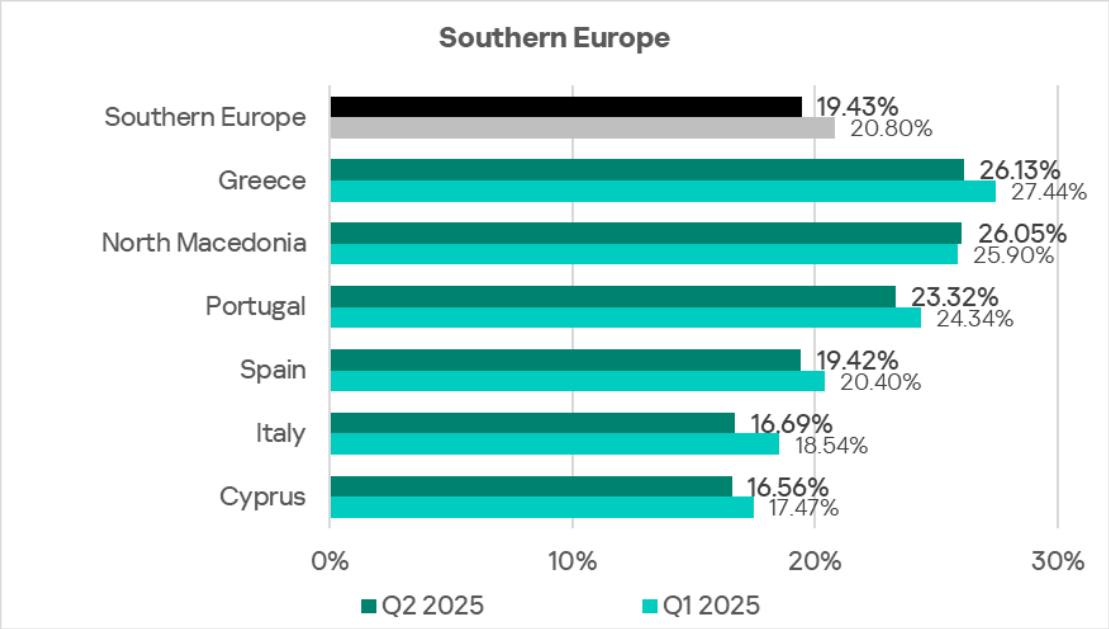
Statistics across all threats

In Q2 2025, Southern Europe ranked eighth globally in the percentage of ICS computers on which malicious objects were blocked.

The rate fell to its lowest since Q3 2022 — 19.4%. This is below the global average but still 1.7 times higher than in Northern Europe, the region with the lowest rate.



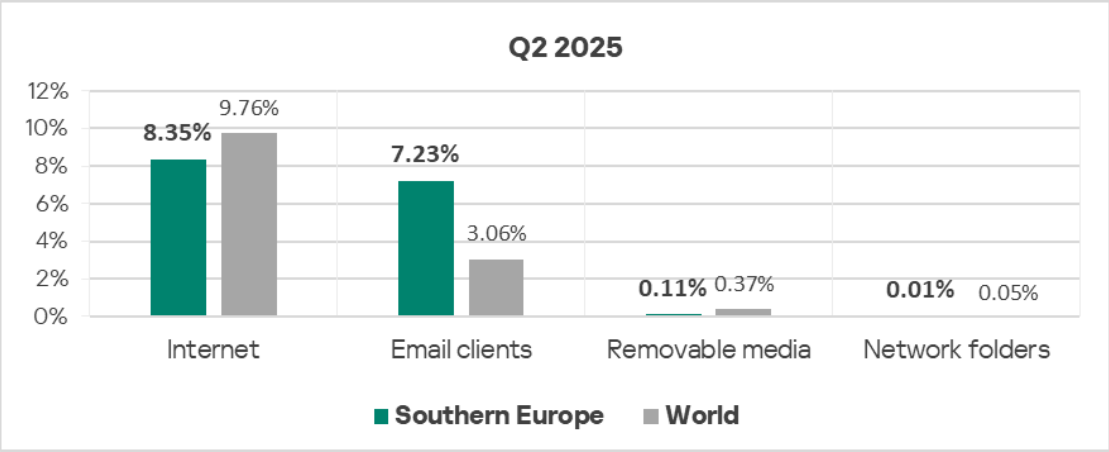
Among the countries of the region, Greece (26.13%) and North Macedonia (26.05%) recorded the highest percentages of ICS computers on which malicious objects were blocked. These two countries also lead most of the region's rankings by both sources and categories of threats.



Threat sources

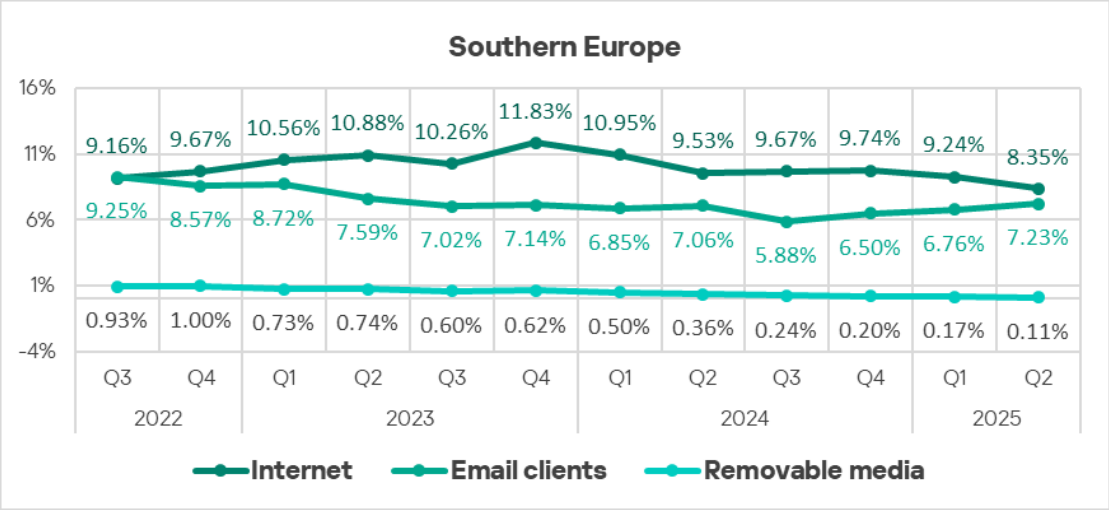
Southern Europe ranks first globally in the percentage of ICS computers on which threats from email clients were blocked. The rate for the region — 7.23% — is 2.4 times higher than the global average.

For all other sources of threats, Southern Europe scores below the global average.



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

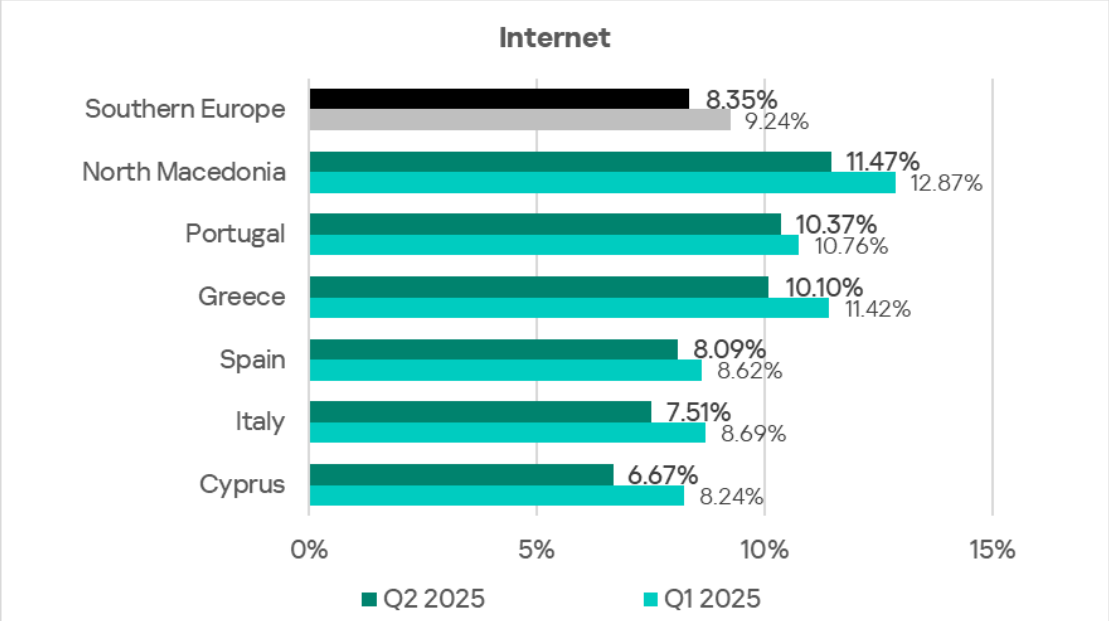
In Q2 2025, the percentage of ICS computers on which malicious objects were blocked fell across all threat sources except for mail clients.



Internet

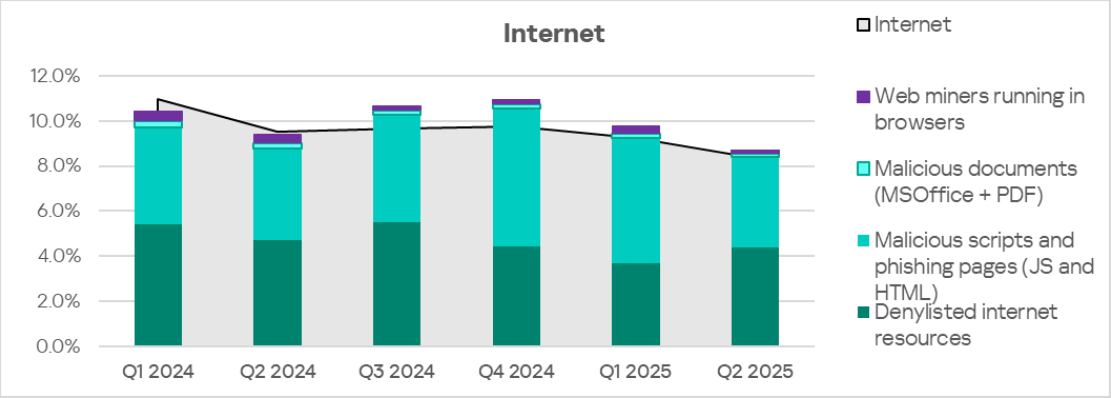
By the percentage of ICS computers on which threats from the internet were blocked, Southern Europe ranks ninth globally, at 8.35% — 1.3 times higher than the lowest figure (East Asia).

Country-level rates range from 6.67% in Cyprus to 11.47% in North Macedonia.



Portugal, which ranks second in this category, also holds second place for both types of miners and leads the region in blocked access to denylisted internet resources.

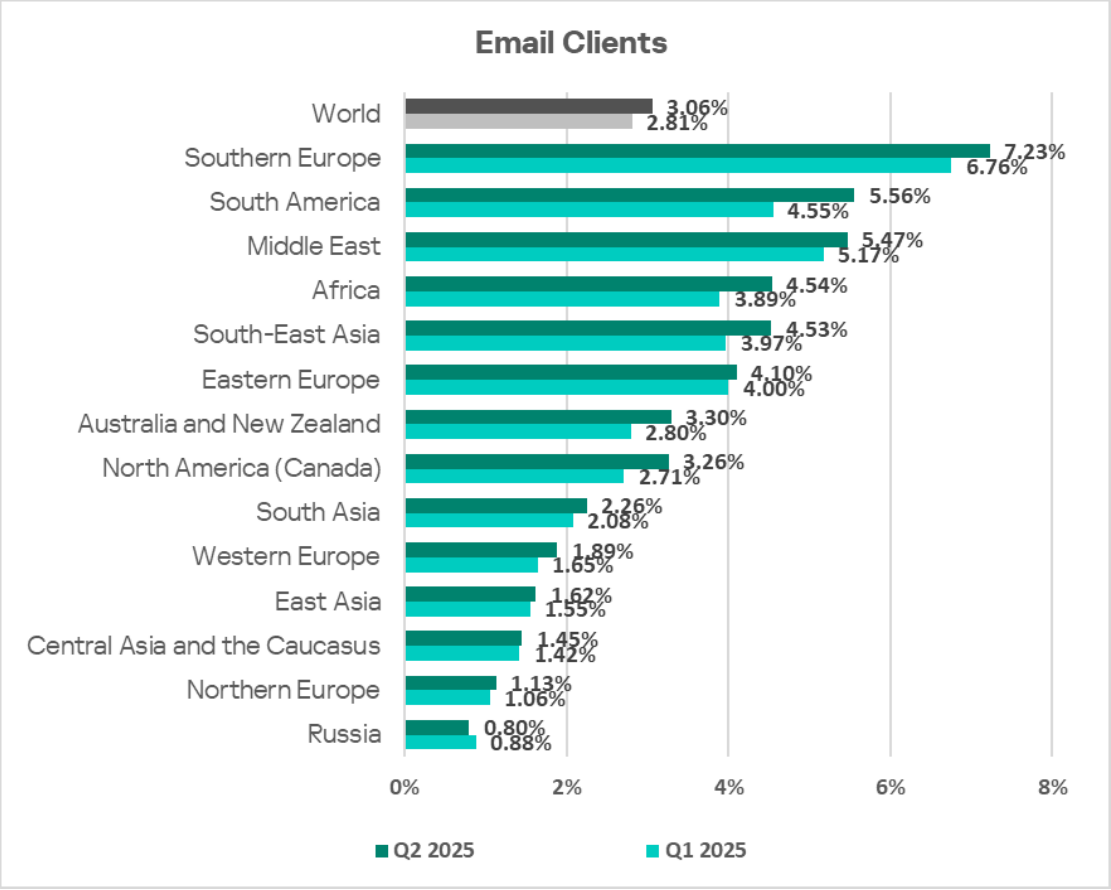
The main categories of internet threats blocked on ICS computers in the region are denylisted internet resources and malicious scripts and phishing pages.



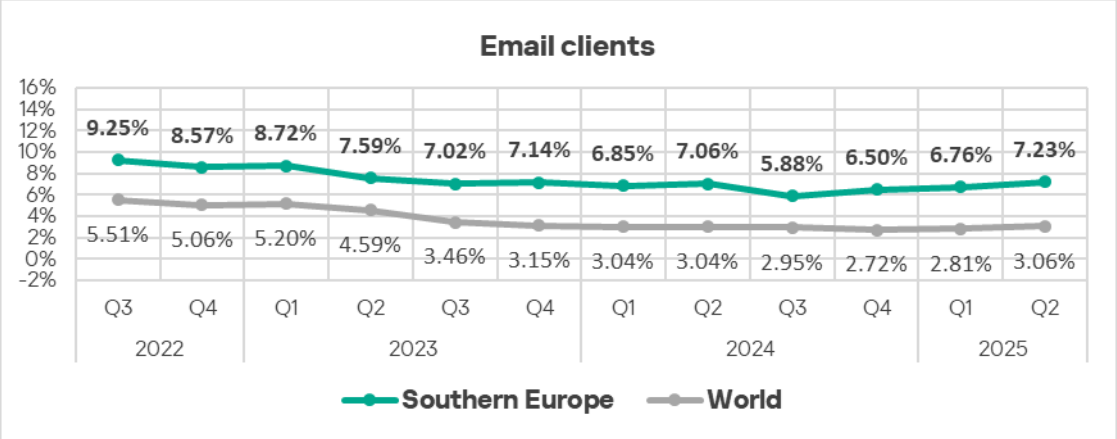
By the percentage of ICS computers on which malicious scripts and phishing pages were blocked, Southern Europe ranks second globally.

Email clients

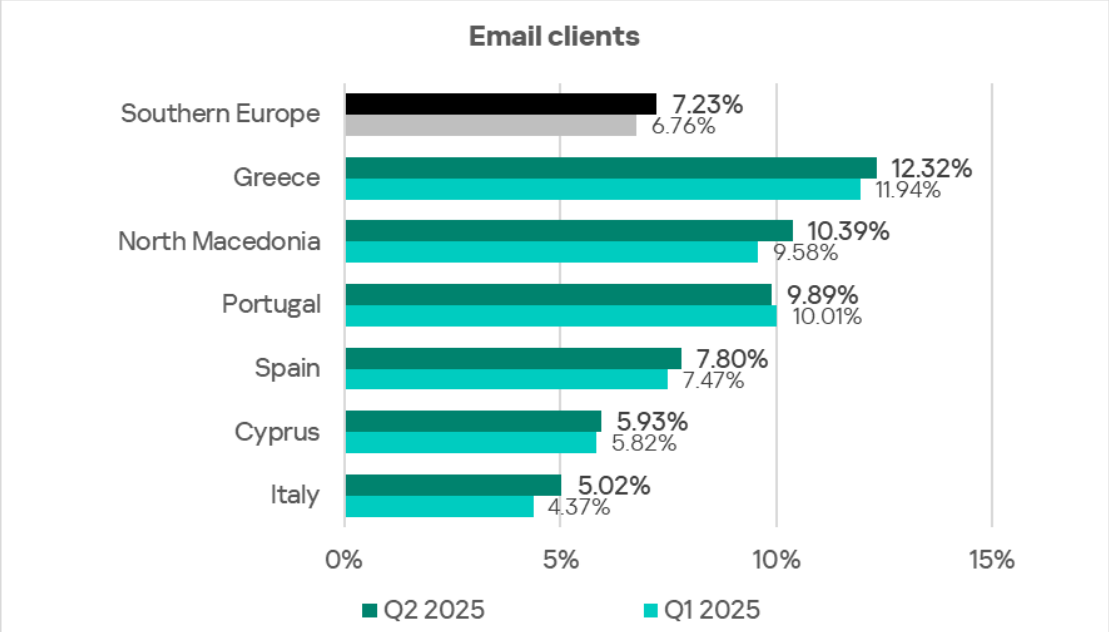
By the percentage of ICS computers on which threats from email clients were blocked, Southern Europe leads globally, with 7.23% in Q2 2025. This figure is nine times higher than in Russia, which ranks last.



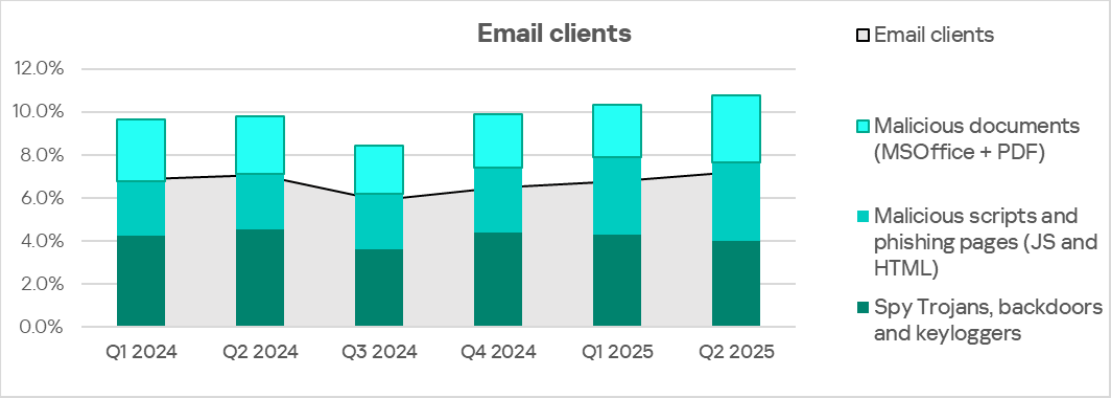
The percentage of ICS computers on which threats from email clients were blocked in Southern Europe rose for the third consecutive quarter.



Among the region's countries, Greece leads with 12.32%, while Italy recorded the lowest rate (5.02%).



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

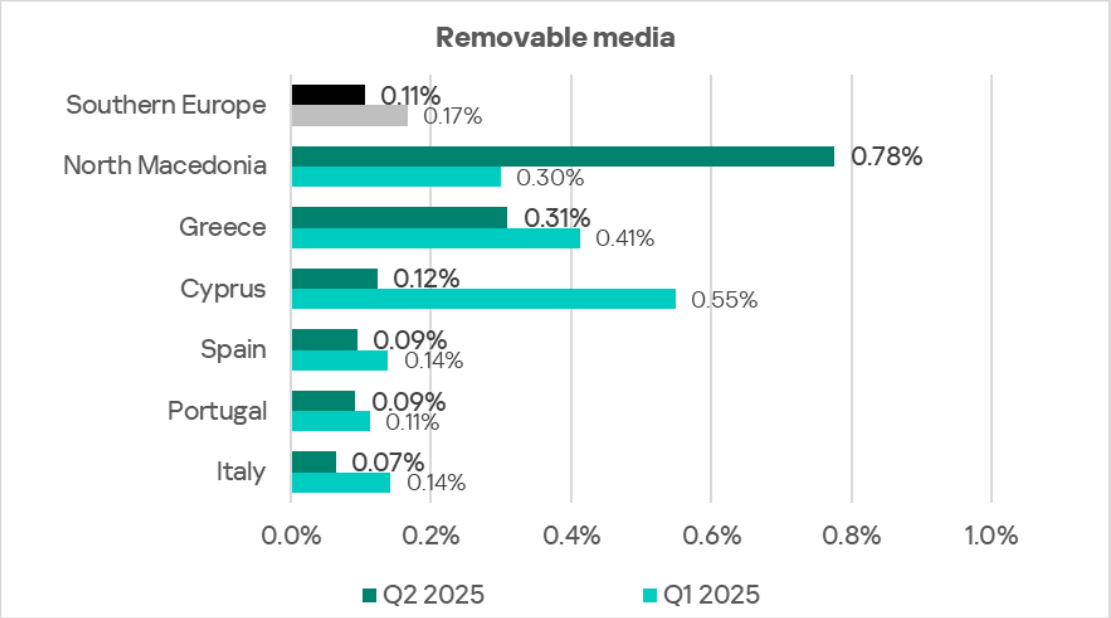


By the percentage of ICS computers on which malicious documents were blocked, Southern Europe ranks first globally.

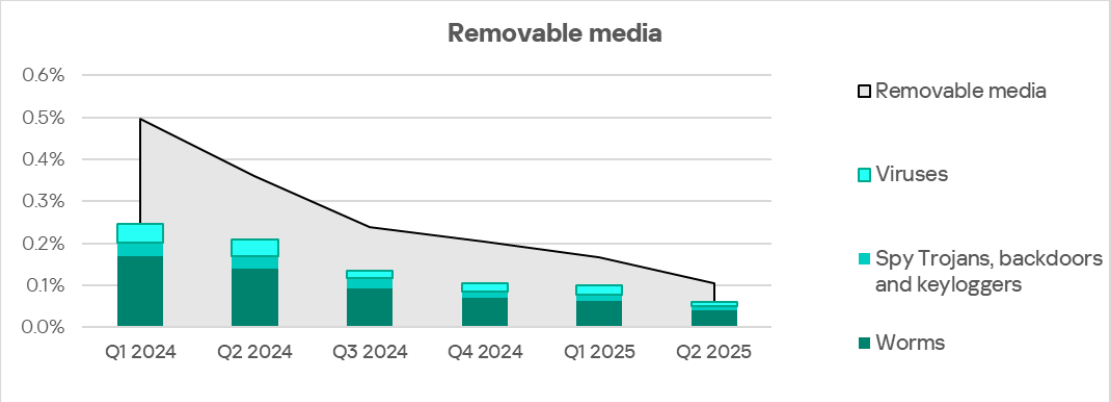
Removable media

By the percentage of ICS computers on which threats from removable media were blocked, Southern Europe ranks 10th among regions in Q2 2025. In North America (Canada), which ranks last, the figure is 3.9 times lower.

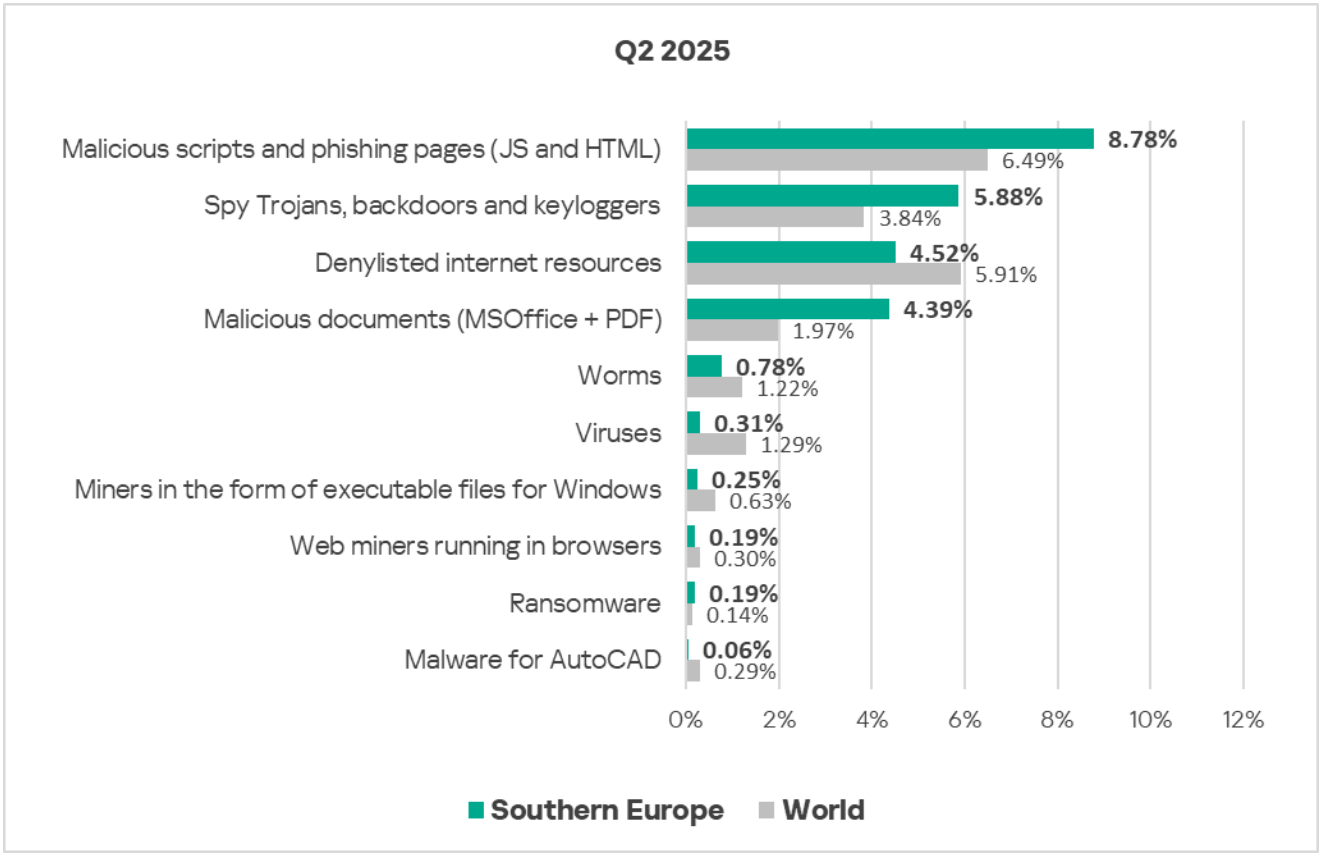
Within the region, North Macedonia is the leader with 0.78%.

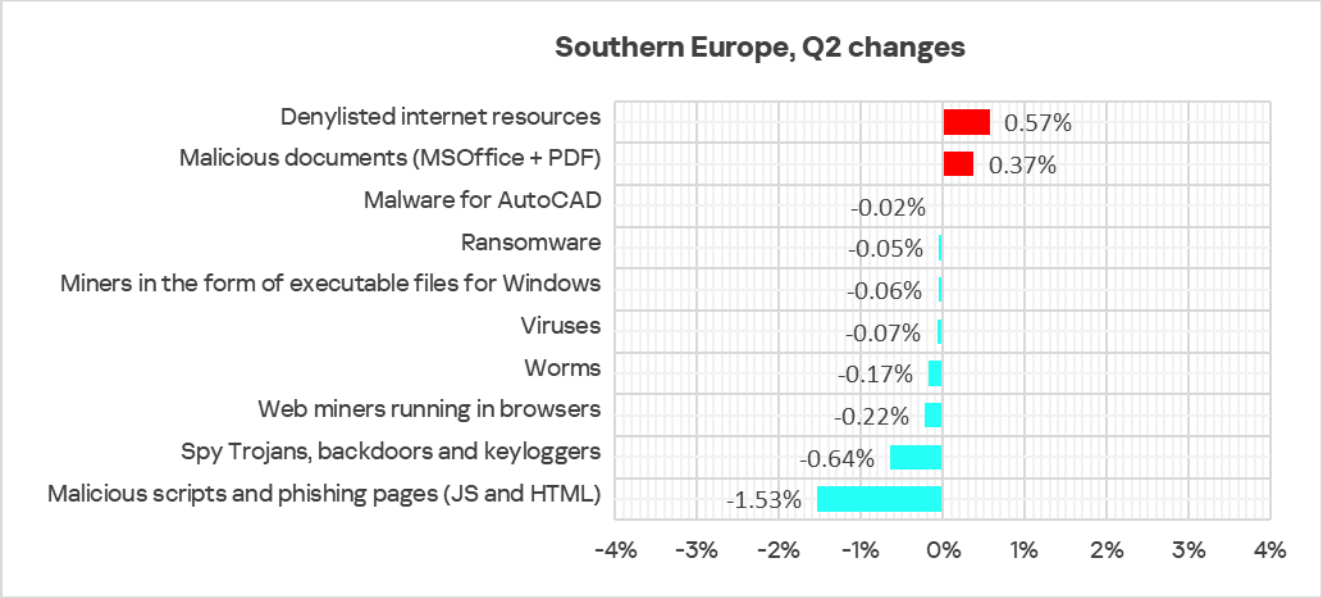


The main categories of threats blocked when connecting removable media to ICS computers are worms, spyware, and viruses.



Threat categories





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

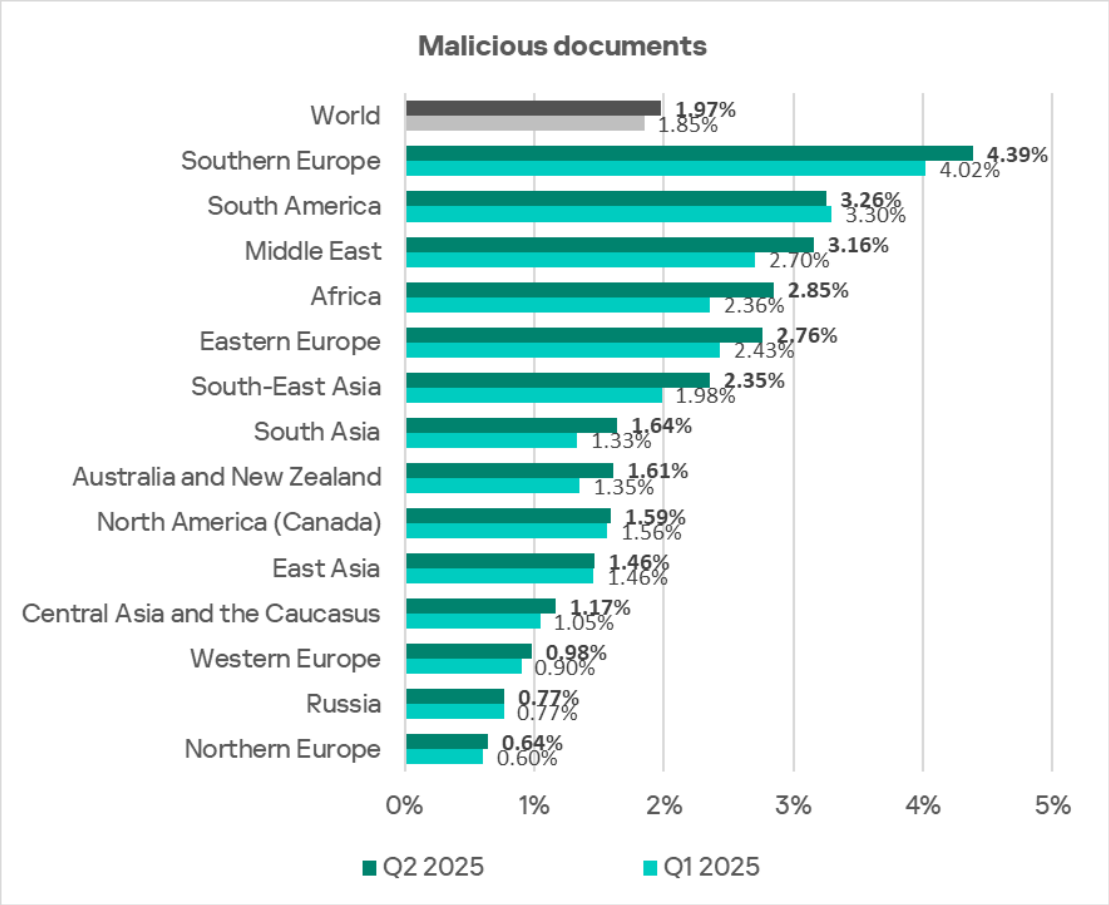
- Malicious documents: 2.2 times higher
- Spyware: 1.5 times higher
- Malicious scripts and phishing pages: 1.4 times higher
- Ransomware: 1.4 times higher

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

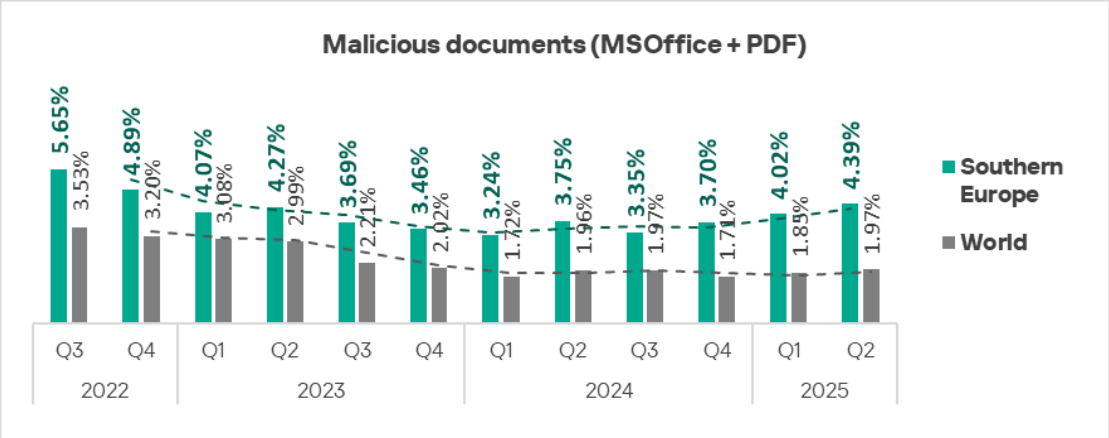
Greece and North Macedonia lead the rankings for these four categories. These two countries also top the regional list for the percentage of ICS computers on which threats from email clients were blocked.

Malicious documents

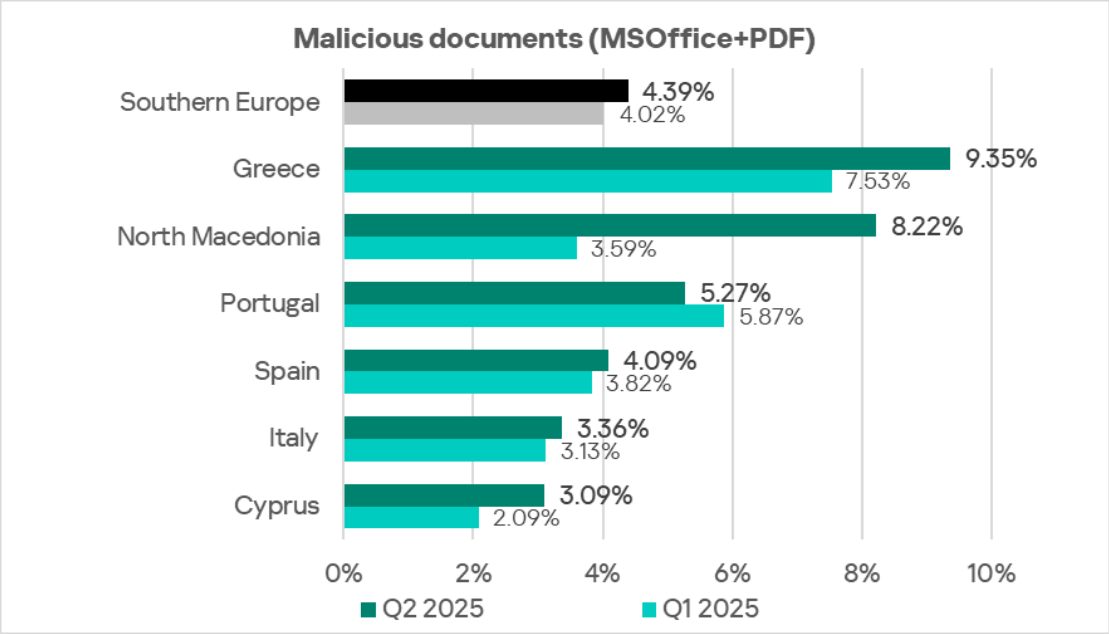
Southern Europe ranks first globally by the percentage of ICS computers on which malicious documents were blocked. In Q2 2025, the region's figure was 4.39%, which is 6.9 times higher than in Northern Europe, the lowest-ranked region.



The percentage of ICS computers on which malicious documents were blocked in the region has been rising for the third consecutive quarter. In Q2 2025, Southern Europe ranked third globally in growth in this category.



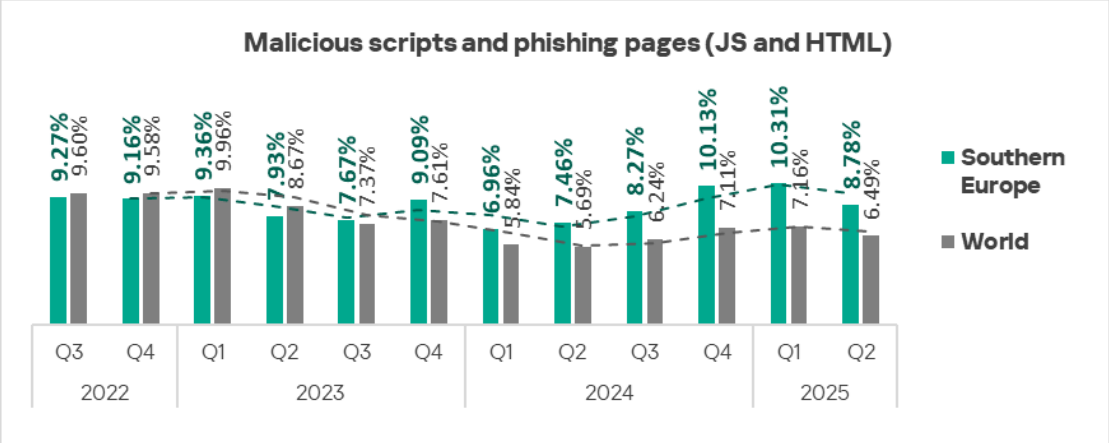
Among the region's countries, Greece leads with 9.35%. All countries in the region recorded an increase in this quarter, with the exception of Portugal.



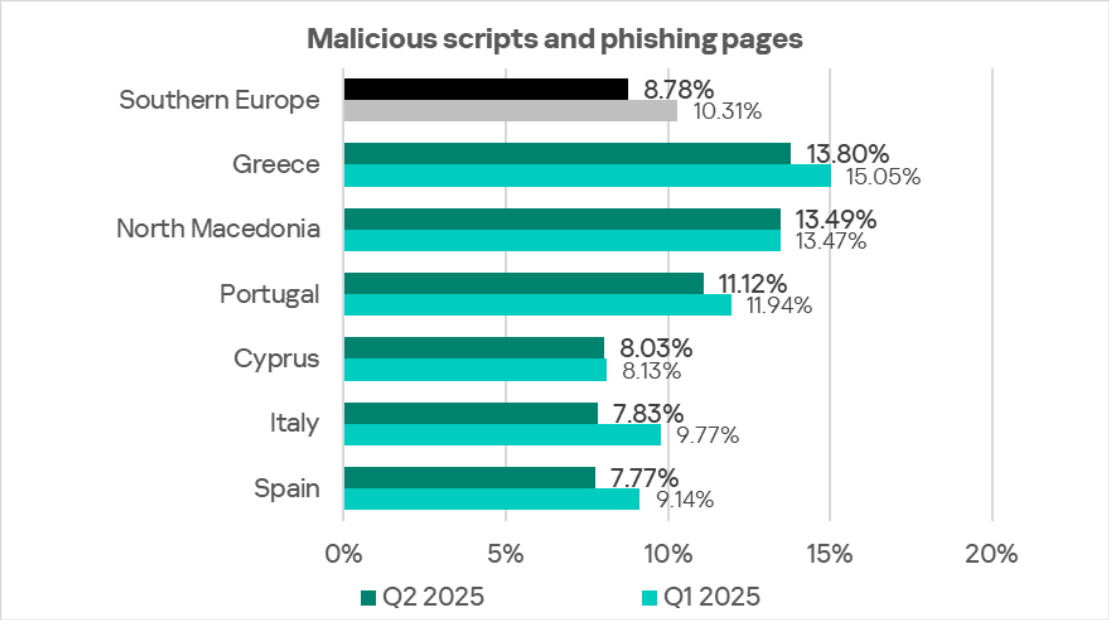
Malicious documents were distributed primarily via email.

Malicious scripts and phishing pages

In terms of ICS computers on which malicious scripts and phishing pages were blocked, Southern Europe ranks second in the global ranking with 8.78%. This is 2.9 times higher than Northern Europe, which has the lowest rate.



Among countries in the region, Greece leads in this metric with 13.80%.



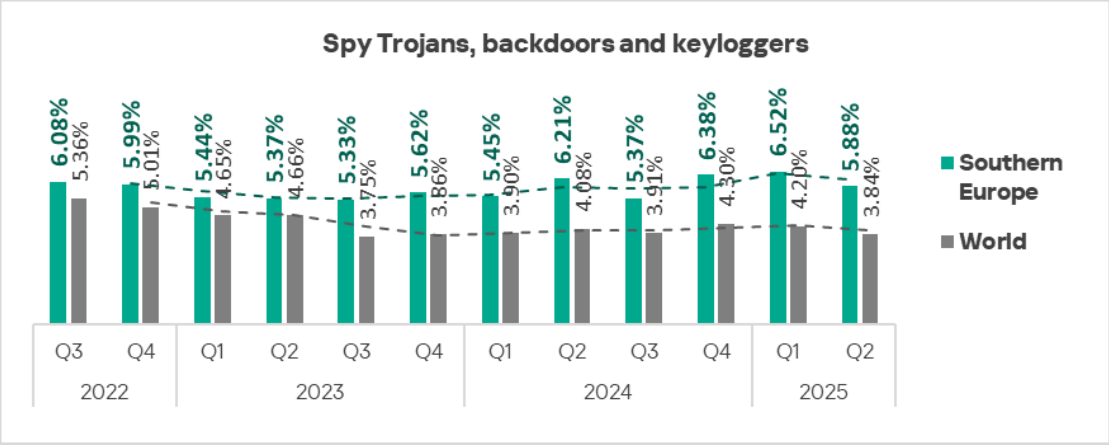
Malicious scripts and phishing pages spread both via the internet and through email.

Spyware

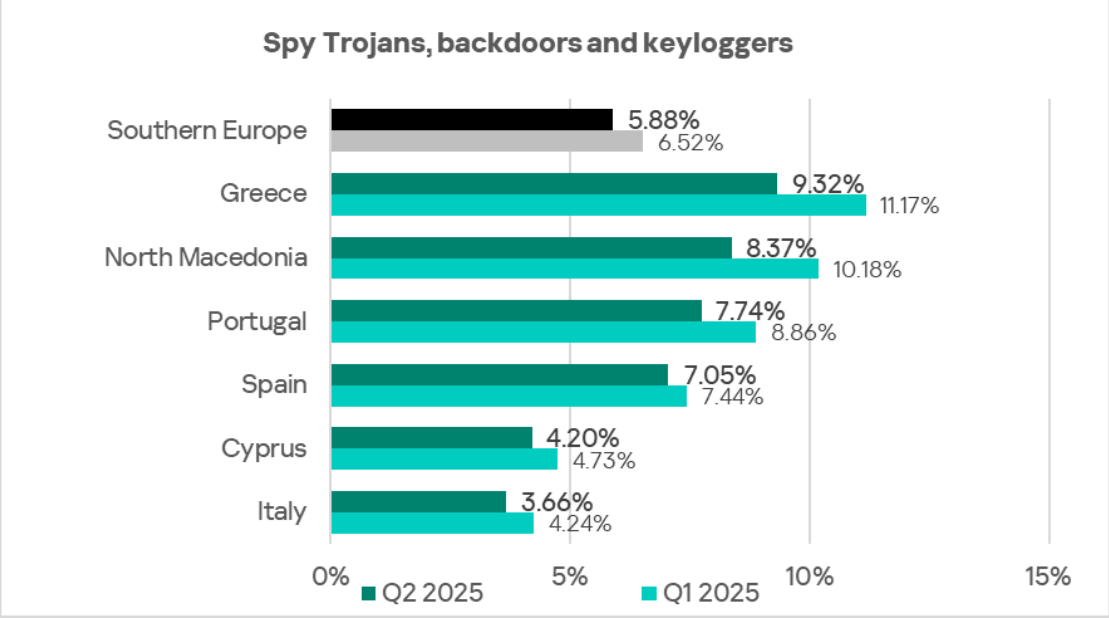
By the percentage of ICS computers on which spyware was blocked, Southern Europe ranks second globally, behind only Africa. The region's figure (5.88%) is 4.3 times higher than in Western Europe, which ranks lowest.

In the region's ranking of threat categories, spyware occupies second place. Besides Southern Europe, spyware also ranks second in two other regions — the Middle East and South America (in East Asia, it holds first place). These three regions — Southern Europe, South America, and the Middle East — also occupy the top positions globally for ICS computers on which threats from email clients were blocked.

The percentage of ICS computers in Southern Europe on which spyware was blocked fluctuates over time.



Among the region's countries and territories, Greece leads in the percentage of ICS computers with blocked spyware, at 9.32%.

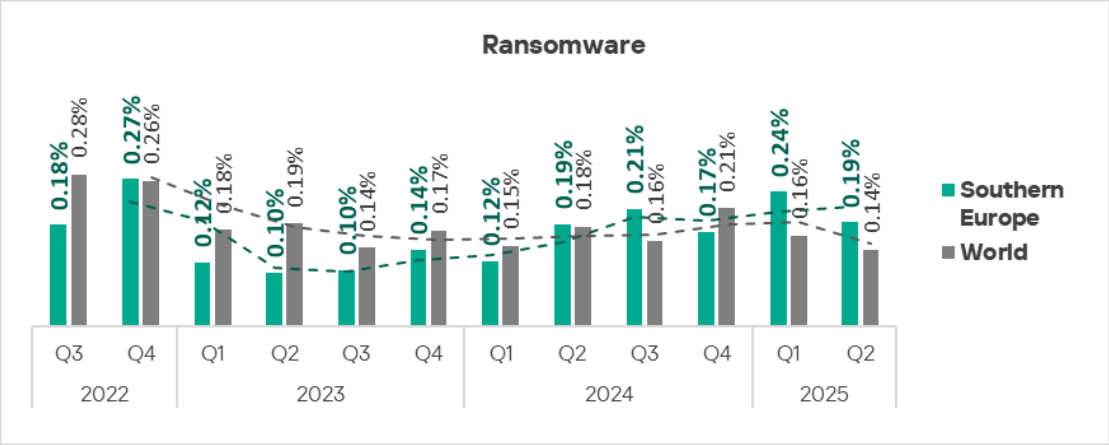


In the region, spyware was blocked mainly in email clients.

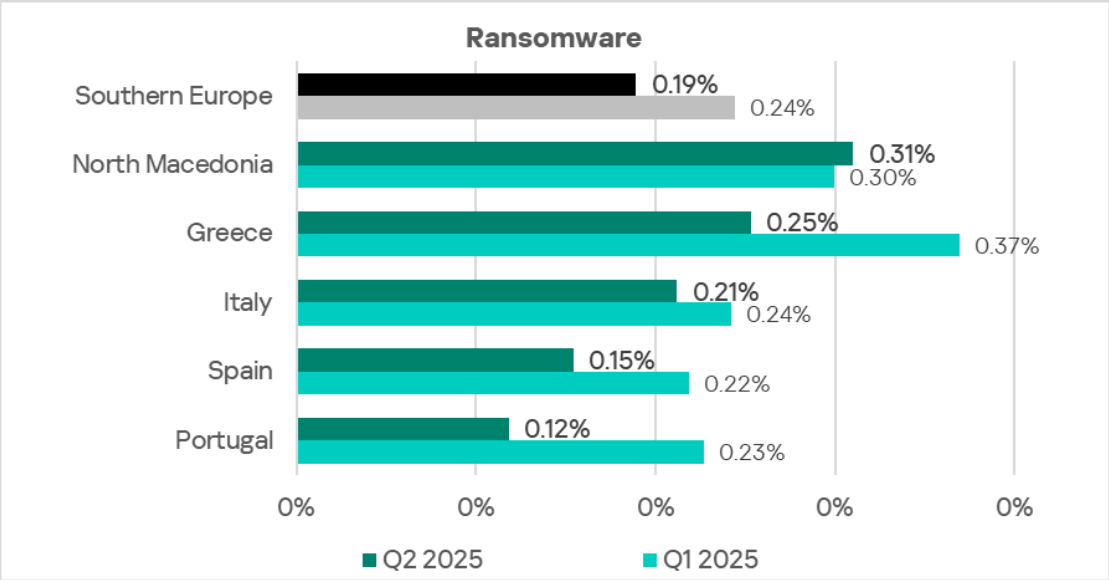
Ransomware

By the percentage of ICS computers on which ransomware was blocked, Southern Europe ranks fifth globally at 0.19%. This is 2.9 times higher than Western Europe, which ranks last.

This metric fluctuates in the region.



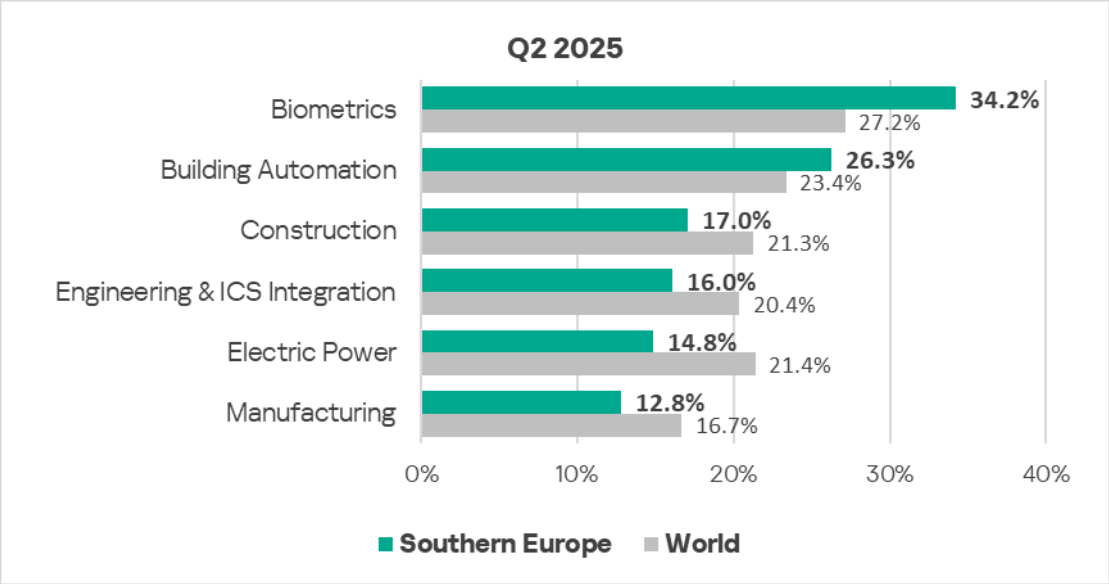
Among the region's countries, North Macedonia leads in this metric with 0.31%.



Industries

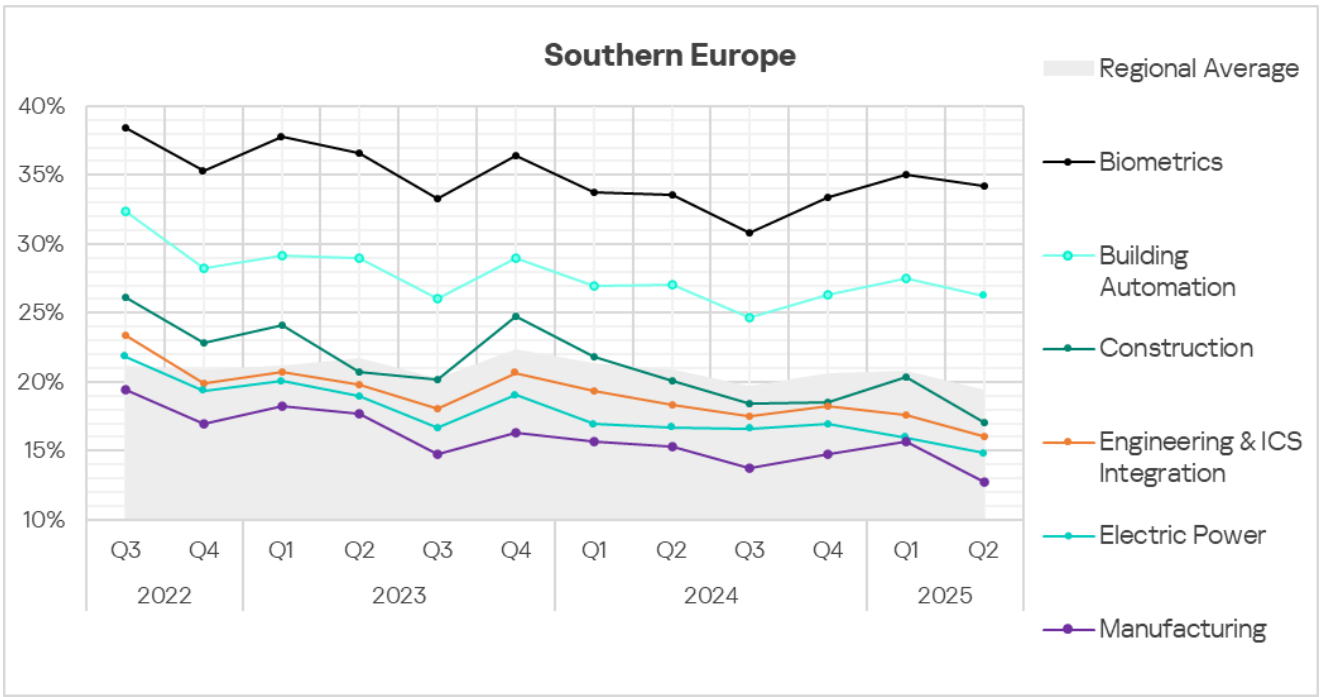
In Southern Europe, of all the industries and OT infrastructures covered in the report, malicious objects are most often blocked in biometric systems.

The percentage of ICS computers on which malicious objects were blocked exceeds the global average in biometric systems (1.2 times higher), as well as building automation (1.1 times higher). These were also the only two sectors where the percentage increased in Q2 2025.



For all other industries studied, the percentage of ICS computers on which malicious objects were blocked decreased in Q2 2025.

Overall, all industries in the region demonstrate fluctuating trends in the percentage of ICS computers on which malicious objects were blocked. However, for biometric systems and building automation, the figures remain significantly above the regional average.



Threat sources and malware categories in industries: hot spots

We use heat maps to assess threats facing industries. On these maps, cells are colored from red to green, where red indicates the maximum value for an industry in the region or a threat source or category across all regions and industries. In Southern Europe, the highest values are observed in biometric systems. The global maximum across all industries was recorded here for email clients and three threat categories: spyware Trojans, malicious scripts and phishing pages, and malicious documents. Moreover, the combined figure for biometric systems in the region is higher than in any other region.

Threat source indicators for industries in Southern Europe, Q2 2025

Industry / Threat source	Biometrics	Building Automation	Electric Power	Engineering & ICS Integration	Construction	Manufacturing	Threat category total in the region
Internet	8.97%	8.81%	7.63%	8.11%	8.02%	5.08%	8.35%
Email clients	20.38%	13.80%	3.19%	4.51%	5.20%	3.29%	7.23%
Removable media	0.06%	0.10%	0.16%	0.09%	0.06%	0.14%	0.11%
Network folders	0.00%	0.03%	0.02%	0.02%	0.00%	0.00%	0.01%
Industry total in the region	34.23%	26.25%	14.84%	16.04%	17.04%	12.76%	

Threat category indicators for industries in Southern Europe, Q2 2025

Industry / Threat category	Biometrics	Building Automation	Electric Power	Engineering & ICS Integration	Construction	Manufacturing	Threat category total in the region
Denylisted internet resources	4.37%	4.25%	4.48%	4.41%	4.70%	2.89%	4.52%
Malicious scripts and phishing pages (JS and HTML)	16.91%	13.95%	5.31%	6.77%	6.53%	5.00%	8.78%
Spy Trojans, backdoors and keyloggers	18.15%	10.61%	2.39%	3.60%	3.21%	2.93%	5.88%
Worms	1.84%	1.14%	0.69%	0.54%	0.39%	0.68%	0.78%
Miners in the form of executable files for Windows	0.41%	0.27%	0.27%	0.25%	0.22%	0.25%	0.25%
Malicious documents (MSOffice + PDF)	12.25%	9.00%	1.81%	2.45%	2.99%	1.82%	4.39%
Viruses	0.43%	0.43%	0.31%	0.21%	0.44%	0.14%	0.31%
Ransomware	0.60%	0.33%	0.05%	0.08%	0.00%	0.18%	0.19%
Web miners running in browsers	0.31%	0.20%	0.22%	0.20%	0.06%	0.07%	0.19%
Malware for AutoCAD	0.04%	0.07%	0.02%	0.04%	0.39%	0.04%	0.06%
Industry total in the region	34.23%	26.25%	14.84%	16.04%	17.04%	12.76%	

Industry hot spots

Biometric systems

- Global leader for email threats and in the following categories: spyware, malicious documents, and malicious scripts and phishing pages.
- Second place globally in ransomware.
- Regional leader in the percentage of ICS computers on which threats from the internet and email clients were blocked.
- First place in the region in the following categories: malicious scripts and phishing pages, spyware, malicious documents, worms, both types of miners, and ransomware.

Building automation

- Second place globally in email client threats, as well as malicious documents and spyware.
- Third place globally in malicious scripts and phishing pages.
- Regional leader in the percentage of ICS computers on which threats from network folders were blocked. Second place in the region in threats from the internet and email clients.

- Second place in the region for the following categories: malicious scripts and phishing pages, spyware, malicious documents, worms, viruses, ransomware, and malware for AutoCAD.

Construction

- Regional leader in blocked threats in the following categories: denylisted internet resources and miners in the form of executable files for Windows.
- Regional leader in blocked threats in the following categories: denylisted internet resources, viruses, and malware for AutoCAD.

Engineering and ICS integrators

- Third place in the region in the percentage of ICS computers on which threats from network folders were blocked.
- Third place in the region in the following categories: malicious scripts and phishing pages, spyware, denylisted internet resources, web miners, and malware for AutoCAD.

Electrical energy industry

- Regional leader in the percentage of ICS computers on which threats from removable media were blocked.
- Second place in the region in denylisted internet resources and both types of miners. Third place in web miners.

Manufacturing

- Second place in the region in the percentage of ICS computers on which threats from removable media were blocked.
- Third place in the region in ransomware.

Western Europe

Key cybersecurity issues in the region

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

In Q2 2025, it ranked second-to-last (13th) globally by the percentage of ICS computers on which malicious objects were blocked.

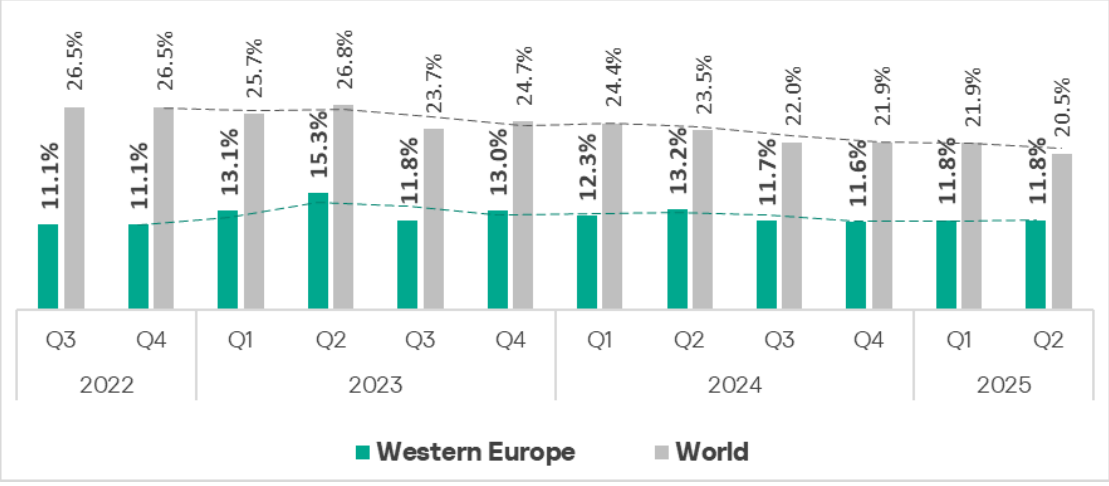
By the percentage of ICS computers on which web miners were blocked, Western Europe ranks eighth. Attacks involving web miners often coincide with large-scale campaigns to compromise vulnerable websites, which, once infected, are then used as C2 infrastructure.

Following another wave of infections from compromised sites, the regional average for web miners dropped back to 2024 levels. In the oil and gas sector, however, the percentage of ICS computers on which web miners were blocked remains very high.

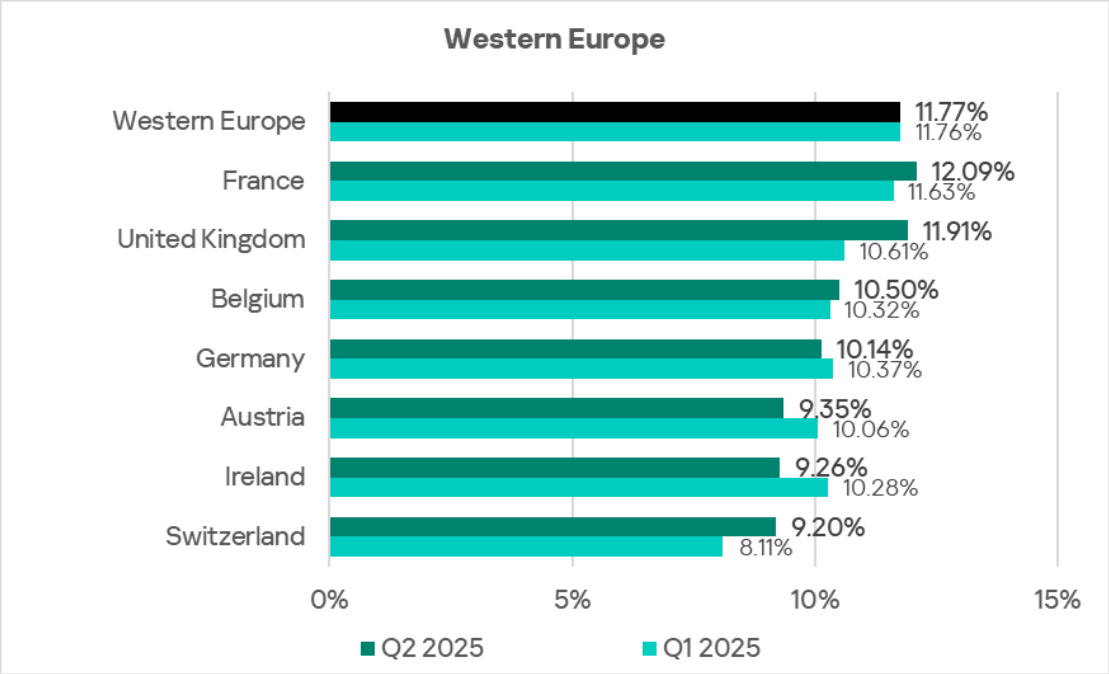
Across all other metrics — both by source and by category of threat — Western Europe does not rise above ninth place.

Statistics across all threats

In Q2 2025, it ranked second-to-last (13th) globally by the percentage of ICS computers on which malicious objects were blocked. The figure remained unchanged at 11.8%. This is well below the global average.

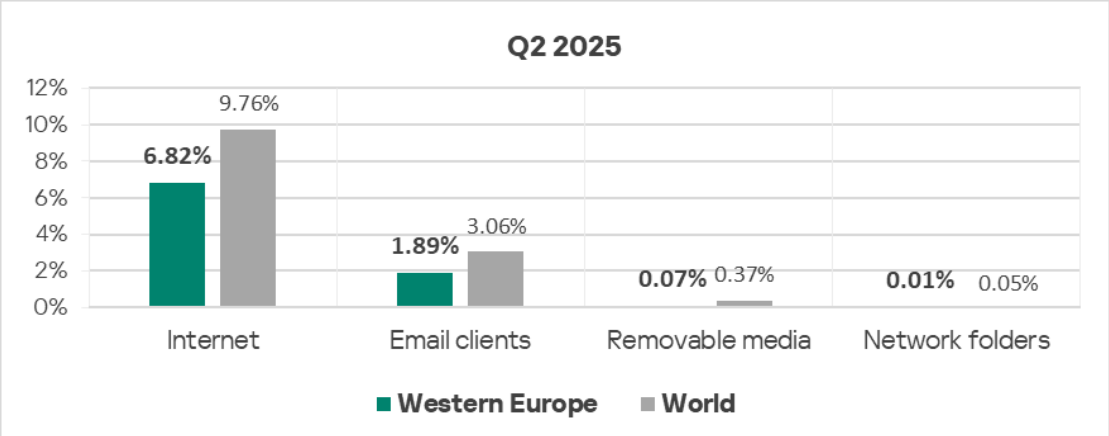


Among the region's countries, France leads in the percentage of ICS computers with blocked malicious objects, at 12.09%. The lowest figure is in Switzerland, at 9.20%.



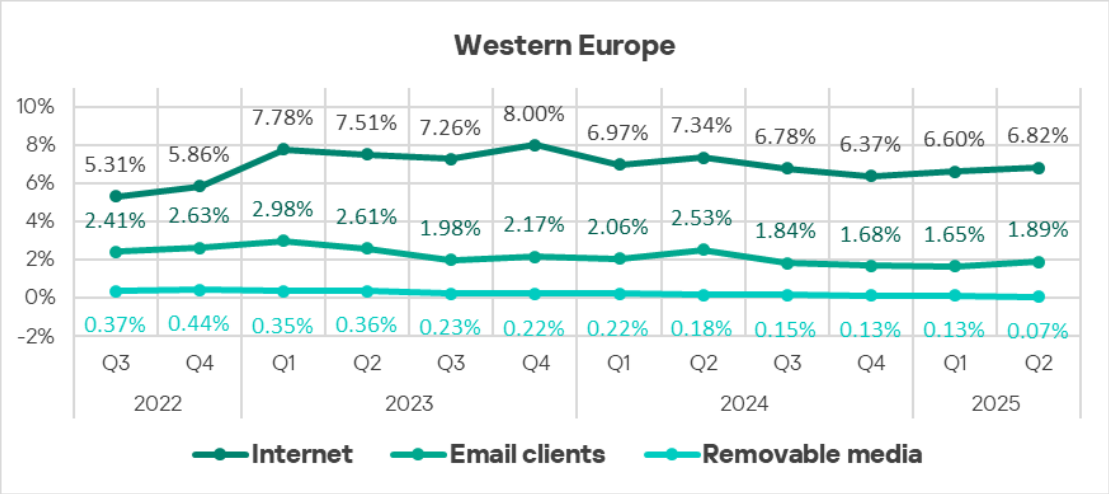
Threat sources

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



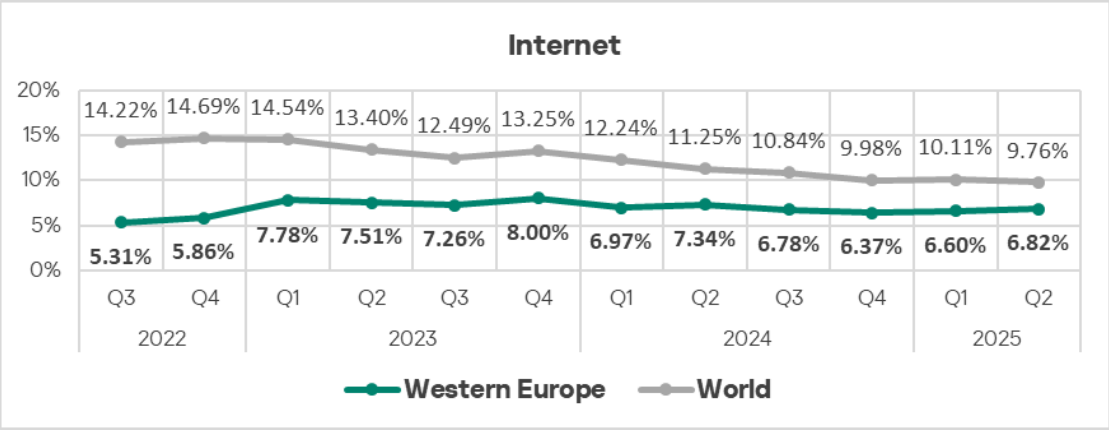
Malicious objects in the region spread primarily via the internet and email. By the percentage of ICS computers on which threats from removable media were blocked, Western Europe ranks third from the bottom.

In Q2 2025, the percentage of ICS computers on which malicious objects were blocked increased slightly for threats from both the internet and email clients.

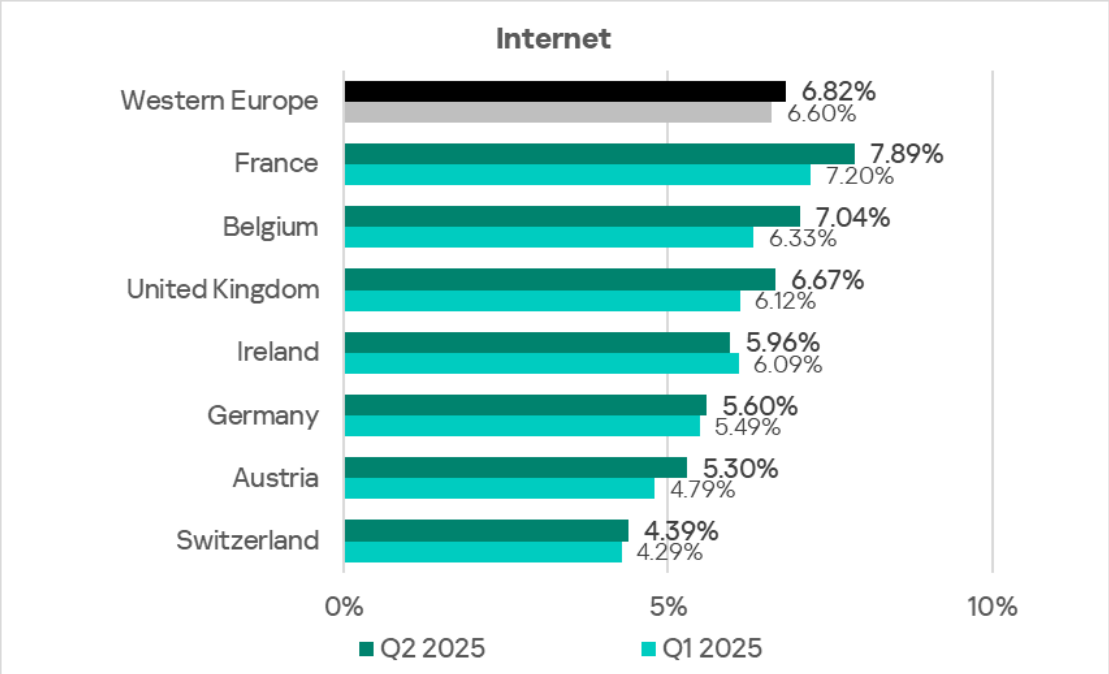


Internet

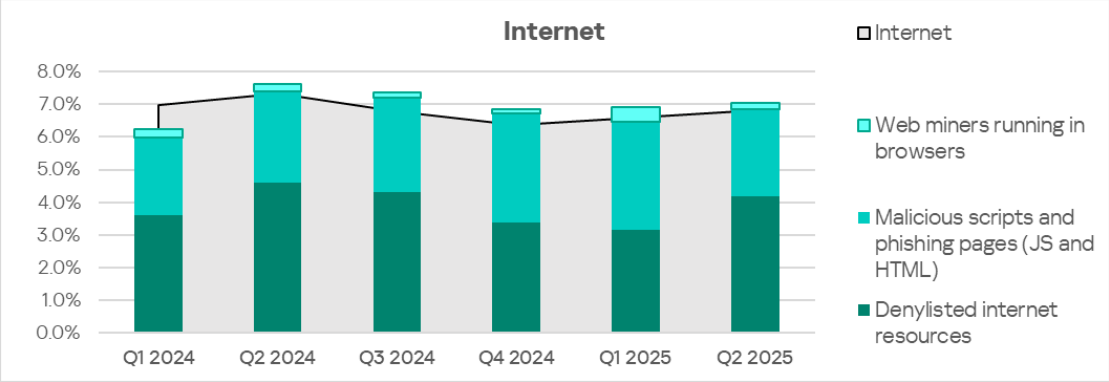
By the percentage of ICS computers on which threats from the internet were blocked, Western Europe ranks 12th globally, with a rate of 6.82%. This is 1.1 times higher than the lowest figure, recorded in East Asia.



Country-level rates range from 4.39% in Switzerland to 7.89% in France. The percentage of ICS computers on which threats from the internet were blocked increased in all countries of the region except Ireland.



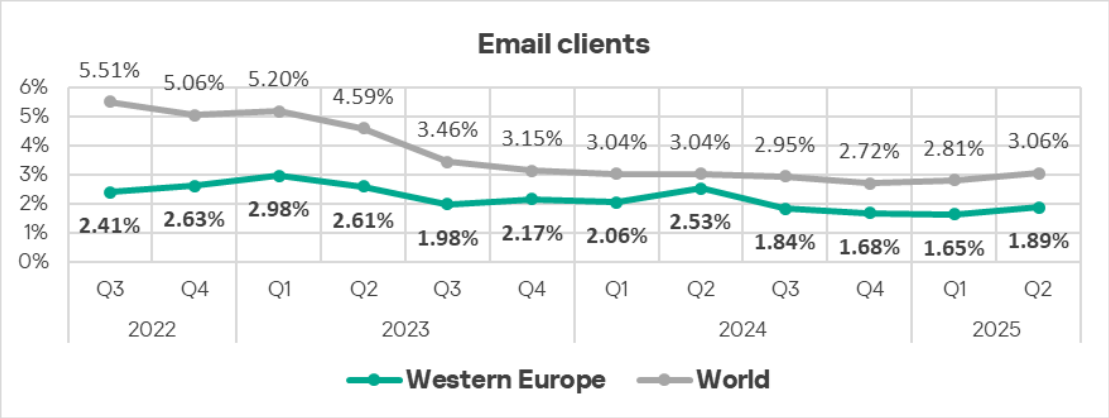
The main categories of internet threats blocked on ICS computers in the region are denylisted internet resources, malicious scripts and phishing pages, and web miners.



In terms of web miners, Western Europe ranks eighth globally.

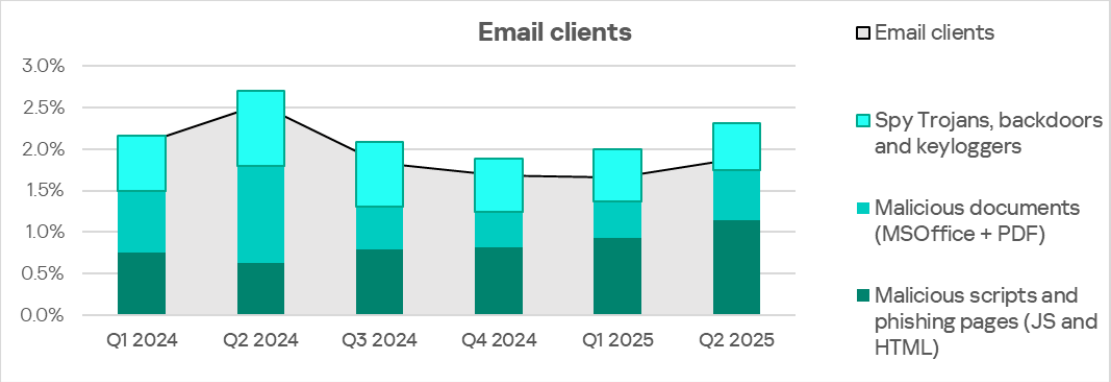
Email clients

By the percentage of ICS computers on which threats from email clients were blocked, Western Europe ranked 10th in Q2 2025, with a rate of 1.89%. This is 2.4 times higher than in Russia, which ranks last.



Among countries in the region, Austria leads in this metric with 1.92%. The lowest figure observed was in Ireland, at 1.08%. The rate increased across all countries of the region except Austria and Belgium.

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



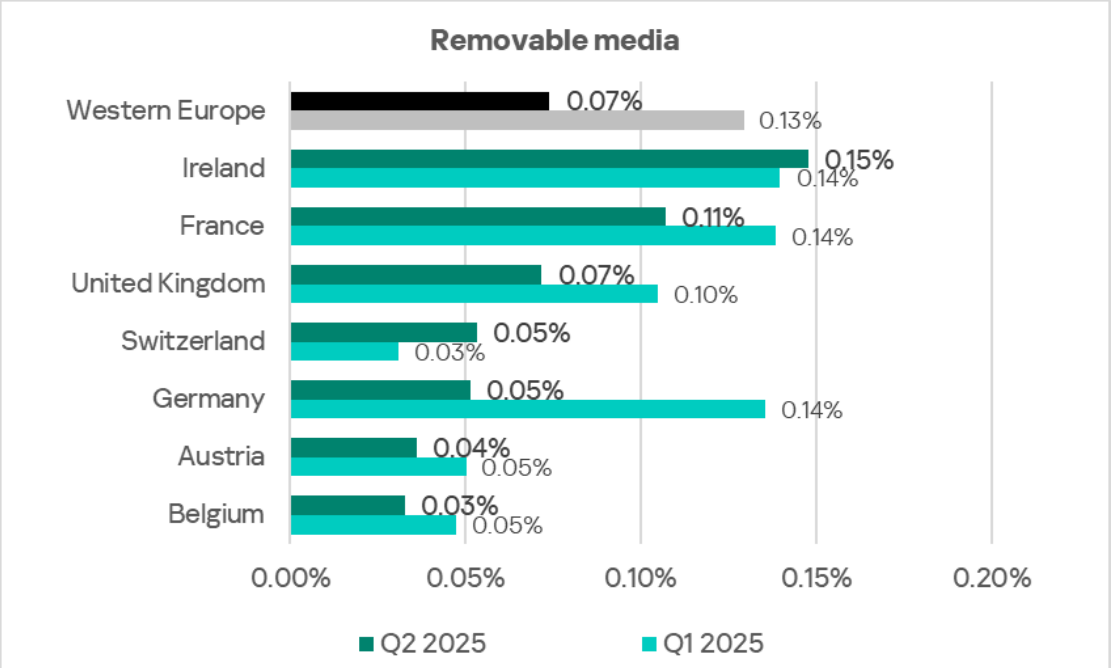
Spyware in the region is spread mainly via email.

The countries leading the email client rankings — Austria, the United Kingdom, and Germany — also rank highest for spyware infections.

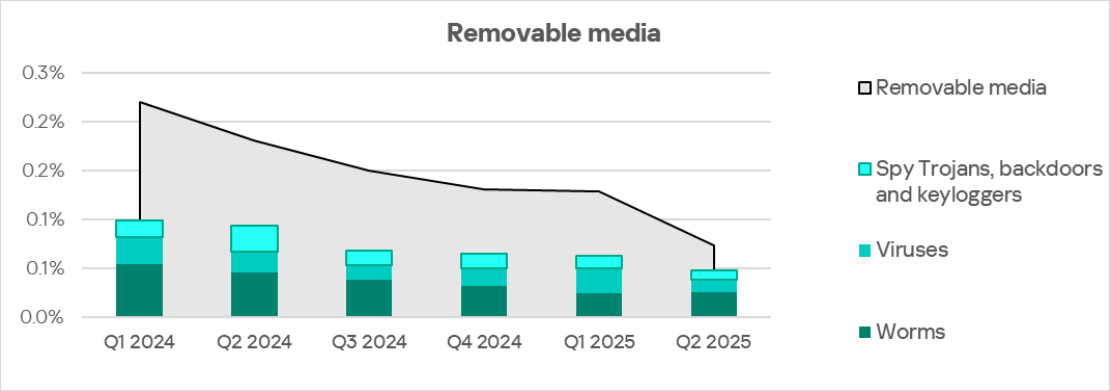
Removable media

In terms of ICS computers on which threats from removable media were blocked, Western Europe ranks 12th among regions in Q2 2025, with a rate of 0.07%. In North America (Canada), which ranks last, the figure is 2.8 times lower.

The rate in Western Europe ranges from 0.03% in Belgium to 0.15% in Ireland. Ireland and Switzerland are the only two countries in the region where this metric increased in Q2 2025.



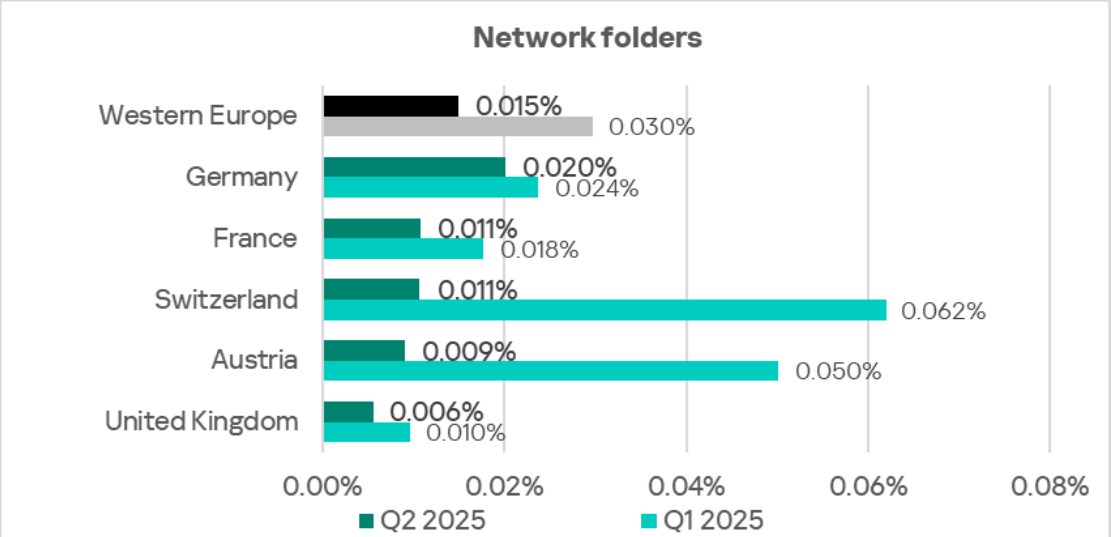
The main categories of removable media threats blocked on ICS computers in the region are worms, viruses, and spyware.



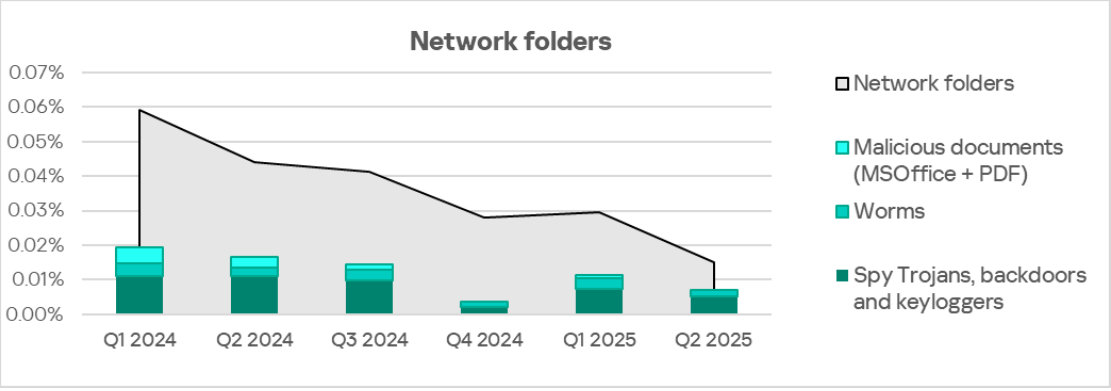
Network folders

By the percentage of ICS computers on which threats from network folders were blocked, Western Europe ranks 10th among regions in Q2 2025, with a rate of 0.015%. In Northern Europe, which ranks last, the figure is 1.5 times lower.

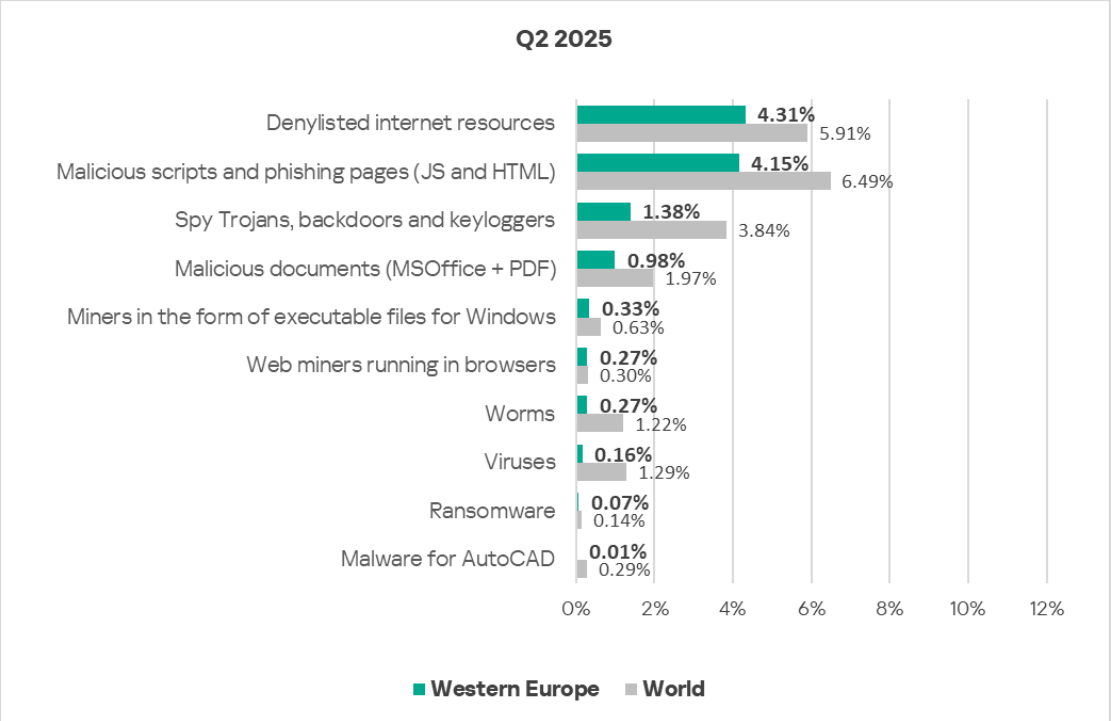
Among countries in the region, Germany leads with 0.02%.

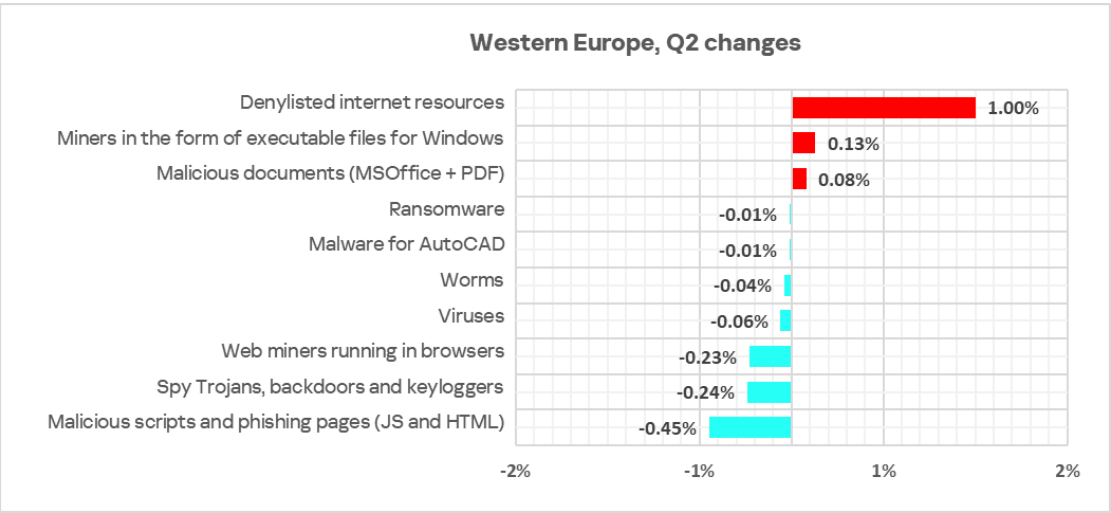


The main categories of network folder threats blocked are spyware and worms.



Threat categories





For all threat categories, the region's figures are lower than the global averages.

Western Europe's highest ranking across threat categories is in web miners, where it places eighth globally.

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

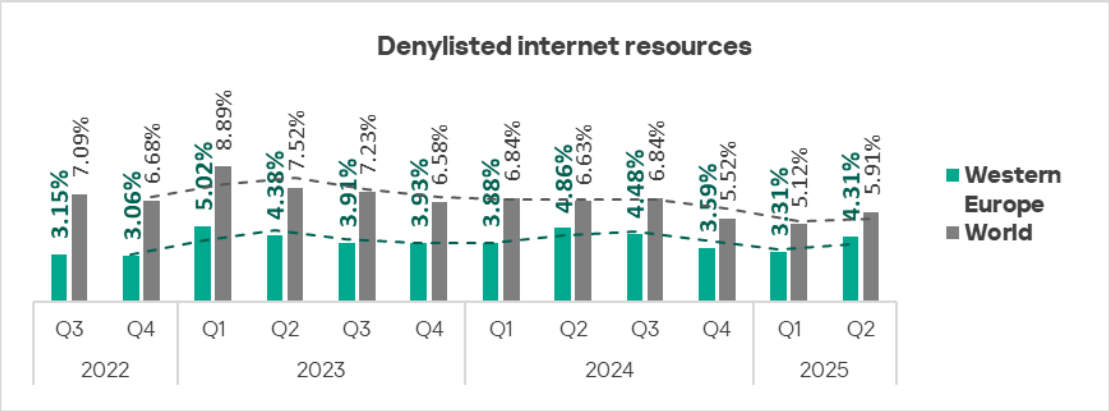
- Denylisted internet resources: 1.3 times increase, third place globally in growth

- Miners in the form of executable files for Windows: 1.7 times increase, global leader in growth
- Malicious documents: 1.1 times higher

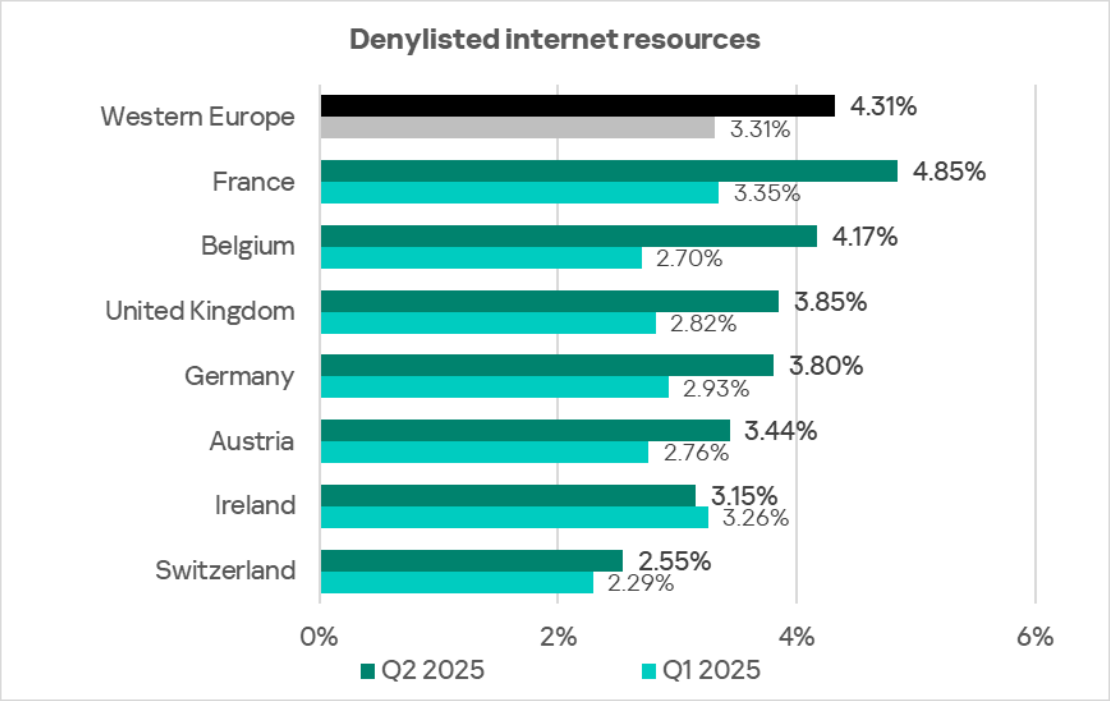
Denylisted internet resources

By the percentage of ICS computers on which denylisted internet resources were blocked, Western Europe ranks ninth globally, at 4.31%. This is 1.3 times higher than East Asia, where the rate is the lowest.

In Q2 2025, Western Europe ranked third globally in growth in the percentage of ICS computers were denylisted internet resources were blocked.



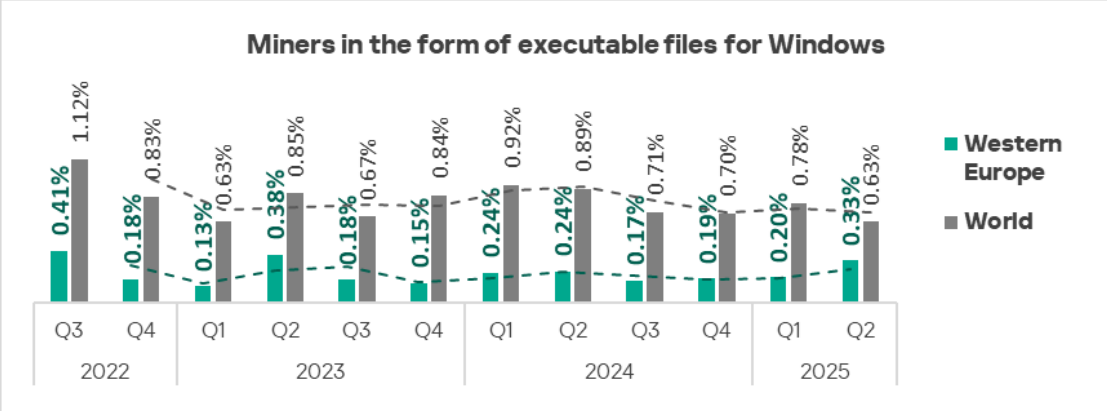
Among countries in the region, France leads at 4.85%. The percentage of ICS computers on which denylisted internet resources were blocked increased in all countries of the region except Ireland.



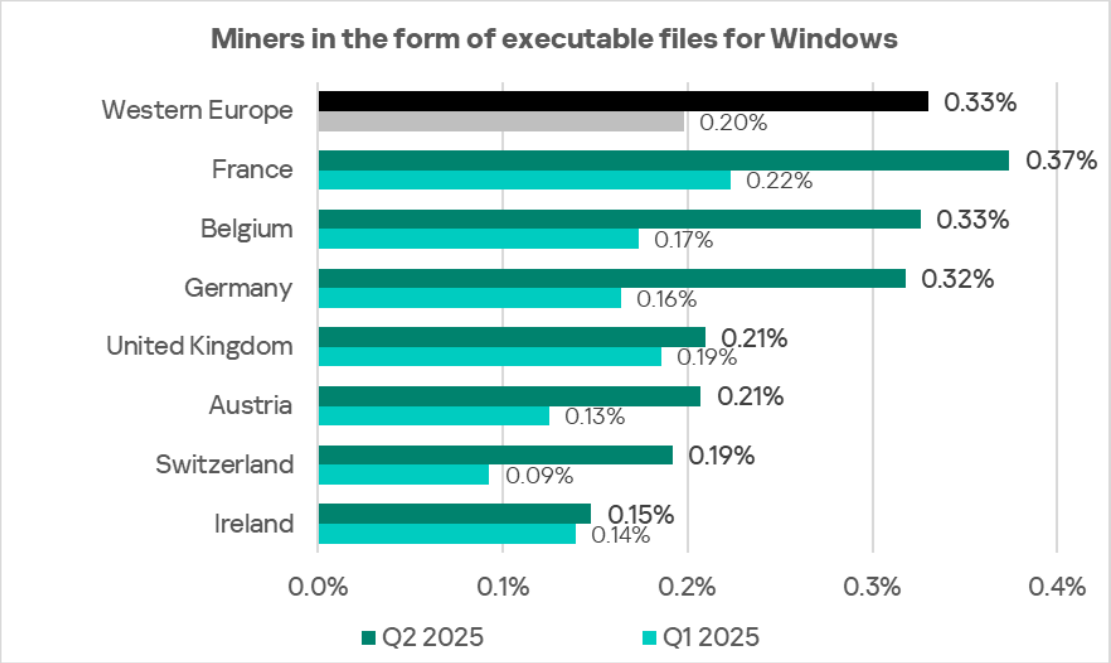
Miners in the form of executable files for Windows

By the percentage of ICS computers on which miners in the form of executable files for Windows were blocked, Western Europe ranks 10th at 0.33%. This is 1.8 times higher than East Asia, which has the lowest rate among all regions.

This metric has been growing in the region for three consecutive quarters. In Q2 2025, Western Europe ranked first globally in growth in this category.



Among the region's countries, France leads at 0.37%.



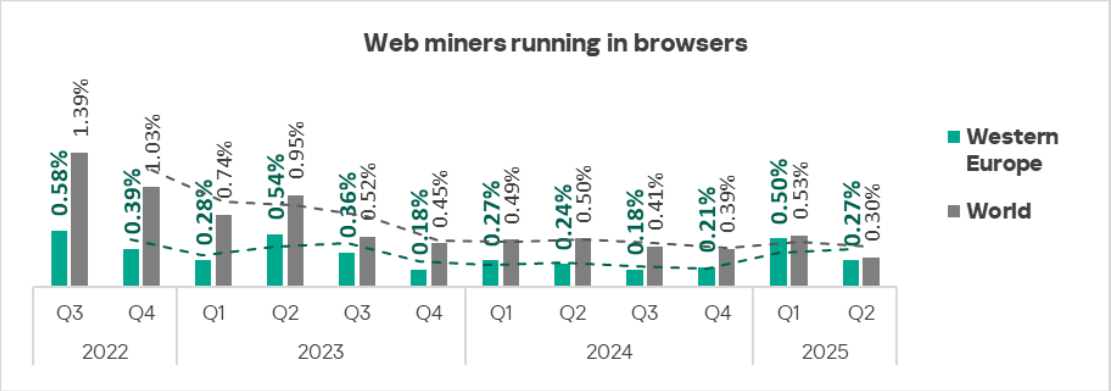
In Northern Europe, miners in the form of executable files for Windows spread primarily via the internet.

Notably, the countries at the top of this ranking — France, Belgium, and Germany — also lead in web miner rates.

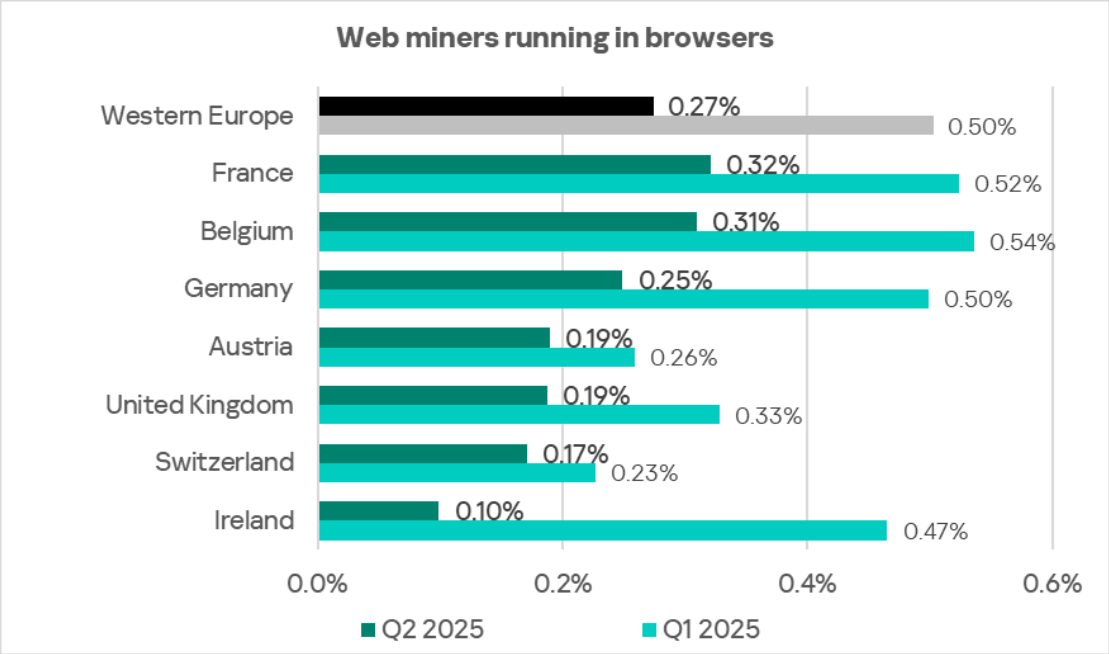
Web miners

Among the rankings by the percentage of ICS computers on which threats from various categories were blocked, Western Europe's highest position is in web miners — the region ranks eighth with 0.27%. This is 2.6 times higher than Eastern Asia, which has the lowest figure, and slightly below the global average.

After growth in the previous quarter, this metric declined across all regions, including Western Europe.



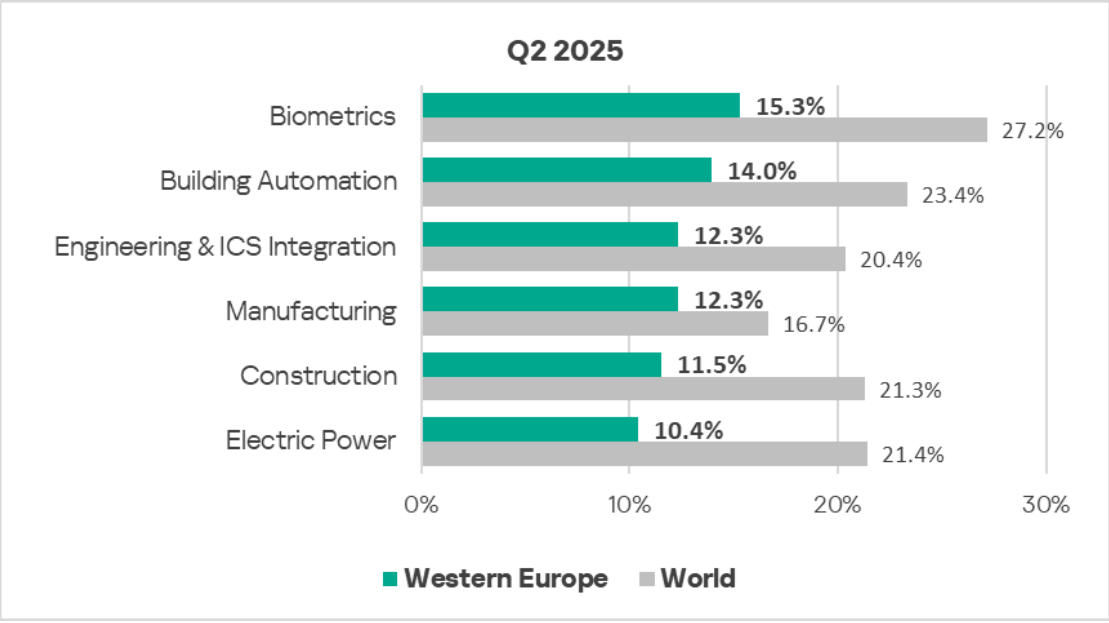
Among countries in the region, France leads at 0.32%.



Industries

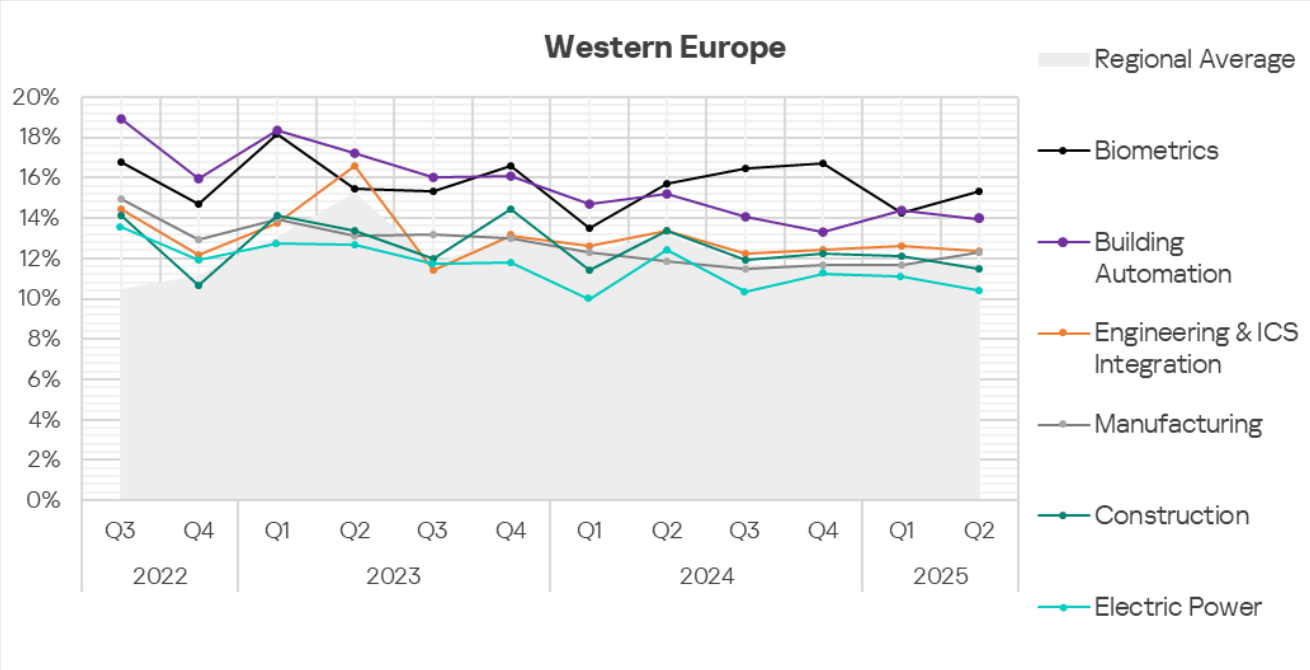
Among the industries reviewed in the report, the percentage of ICS computers on which malicious objects were blocked was highest in biometric systems.

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



In Q2 2025, out of the industries reviewed in the region, the rate increased in two sectors — biometric systems and manufacturing.

Rates for building automation and biometric systems remain noticeably higher than the regional average.



Threat sources and malware categories in industries: hot spots

We use heat maps to assess threats facing industries. On these maps, cells are colored from red to green, where red indicates the maximum value for an industry in the region or a threat source or category across all regions and industries. In Western Europe, the values closest to the maximum were observed for the combined figure in the building automation sector, as well as for the web miner category in the construction sector.

Threat source indicators for industries in Western Europe, Q2 2025

Industry / Threat source	Biometrics	Building Automation	Electric Power	Engineering & ICS Integration	Oil & Gas	Construction	Manufacturing	Threat category total in the region
Internet	5.75%	6.67%	5.73%	7.59%	7.51%	6.54%	6.39%	6.82%
Email clients	5.56%	4.18%	1.41%	1.73%	0.58%	2.11%	1.44%	1.89%
Removable media	0.00%	0.08%	0.17%	0.07%	0.29%	0.00%	0.25%	0.07%
Network folders	0.00%	0.01%	0.02%	0.02%	0.00%	0.00%	0.00%	0.01%
Industry total in the region	15.33%	13.96%	10.41%	12.34%	13.01%	11.51%	12.31%	

Threat category indicators for industries in Western Europe, Q2 2025

Industry / Threat category	Biometrics	Building Automation	Electric Power	Engineering & ICS Integration	Oil & Gas	Construction	Manufacturing	Threat category total in the region
Denylisted internet resources	3.45%	3.93%	3.86%	4.77%	4.91%	3.82%	3.76%	4.31%
Malicious scripts and phishing pages (JS and HTML)	6.70%	5.84%	3.05%	4.42%	3.76%	4.97%	3.89%	4.15%
Spy Trojans, backdoors and keyloggers	4.79%	2.51%	1.11%	1.43%	1.45%	1.03%	1.65%	1.38%
Worms	0.38%	0.45%	0.28%	0.27%	0.29%	0.17%	0.72%	0.27%
Miners in the form of executable files for Windows	0.19%	0.29%	0.33%	0.31%	0.58%	0.22%	0.25%	0.33%
Malicious documents (MSOffice + PDF)	3.64%	1.92%	0.78%	0.96%	0.58%	0.71%	0.85%	0.98%
Viruses	0.38%	0.26%	0.18%	0.16%	0.58%	0.24%	0.25%	0.16%
Ransomware	0.19%	0.12%	0.04%	0.06%	0.00%	0.00%	0.04%	0.07%
Web miners running in browsers	0.19%	0.26%	0.28%	0.26%	0.58%	0.22%	0.30%	0.27%
Malware for AutoCAD	0.00%	0.00%	0.00%	0.01%	0.00%	0.10%	0.00%	0.01%
Industry total in the region	15.33%	13.96%	10.41%	12.34%	13.01%	11.51%	12.31%	

Industry hot spots

Biometric systems

- Regional leader by the percentage of ICS computers on which threats from email clients were blocked.
- Regional leader in the percentage of ICS computers on which the following categories of threats were blocked: malicious scripts and phishing pages, spyware, malicious documents, and ransomware.
- Second place in the region in viruses.
- Third place regionally in worms and malware for AutoCAD.

Building automation

- Second place in the region for email client, removable media, and network folder threats. Third place in denylisted internet resources.
- Second place regionally in the following categories: malicious scripts and phishing pages, spyware, malicious documents, worms, ransomware.
- Third place regionally in denylisted internet resources and viruses.

Oil and gas

- Regional leader in the percentage of ICS computers on which threats from removable media were blocked. Second place in internet threats.

- Regional leader for denylisted internet resources, both types of miners, and viruses.

Engineering and ICS integrators

- Regional leader in the percentage of ICS computers on which threats from the internet and network folders were blocked.
- Second place regionally in denylisted internet resources and malware for AutoCAD.
- Third place regionally in malicious documents, miners in the form of executable files for Windows, and ransomware.

Manufacturing

- Second place in the region in the percentage of ICS computers on which threats from removable media were blocked.
- Regional leader in worms.
- Second place regionally in web miners.
- Third place regionally in spyware.

Construction

- Third place regionally in email client threats.
- Regional leader in malware for AutoCAD.
- Third place regionally in malicious scripts and phishing pages.

Electrical energy industry

- Second place regionally in network folder threats. Third place in removable media threats.
- Second place regionally in miners in the form of executable files for Windows.
- Third place regionally in web miners.

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.

At the same time, it is one of only two regions where this figure increased in Q2 2025.

In Northern Europe in Q2 2025, several threat categories grew, with the most significant increases in:

- Denylisted internet resources: 1.6 times higher, the highest growth globally for this metric
- Ransomware: 1.3 times higher, continuing a growth trend for the second consecutive quarter, with third place globally in growth in this category in Q2 2025
- Miners in the form of executable files for Windows: 1.1 times higher, the second-highest growth rate

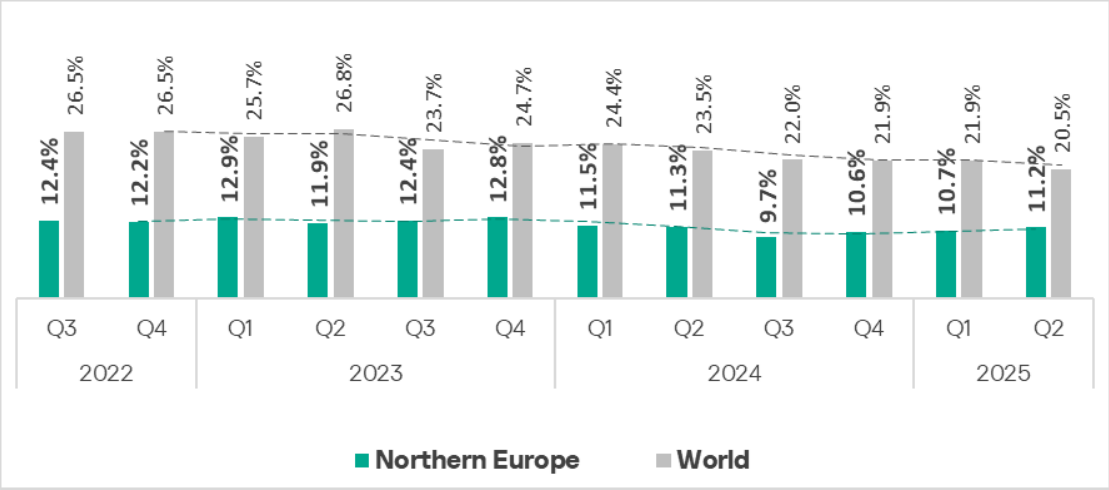
The main driver of this growth was waves of infections on vulnerable online resources, which were exploited to distribute both types of miners, spyware, and ransomware.

Statistics across all threats

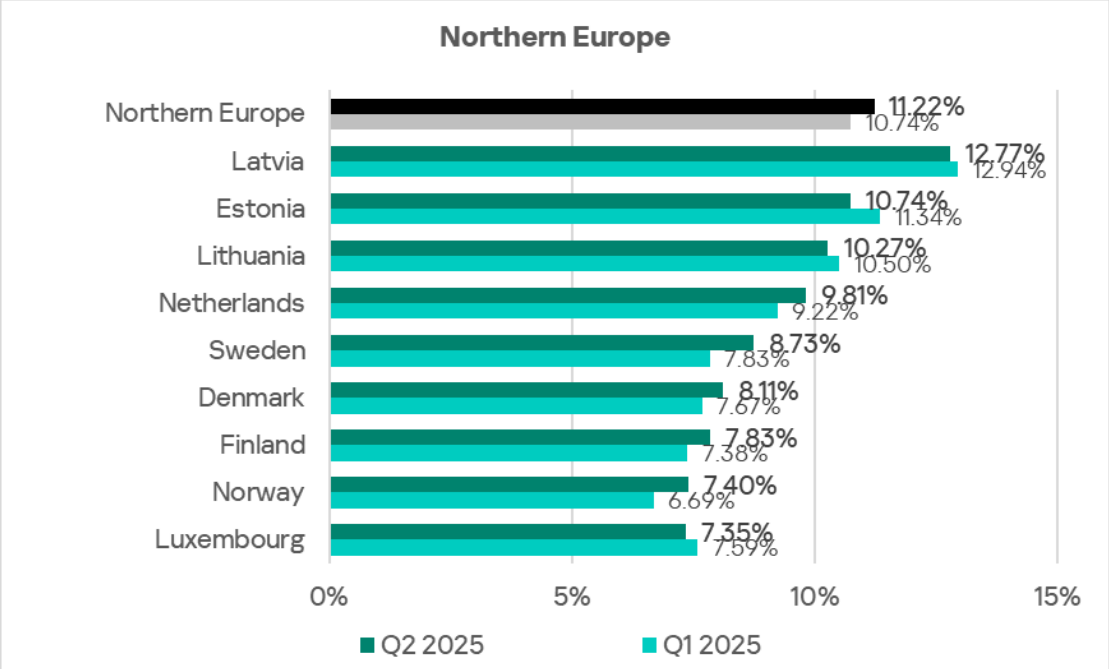
Northern Europe ranks 14th in the global ranking for the percentage of ICS computers on which malicious objects were blocked.

The region's figure is significantly lower than the global average.

It is one of only two regions to record an increase in this metric in Q2 2025. Nevertheless, the region's rate (11.2%) remains the lowest globally.

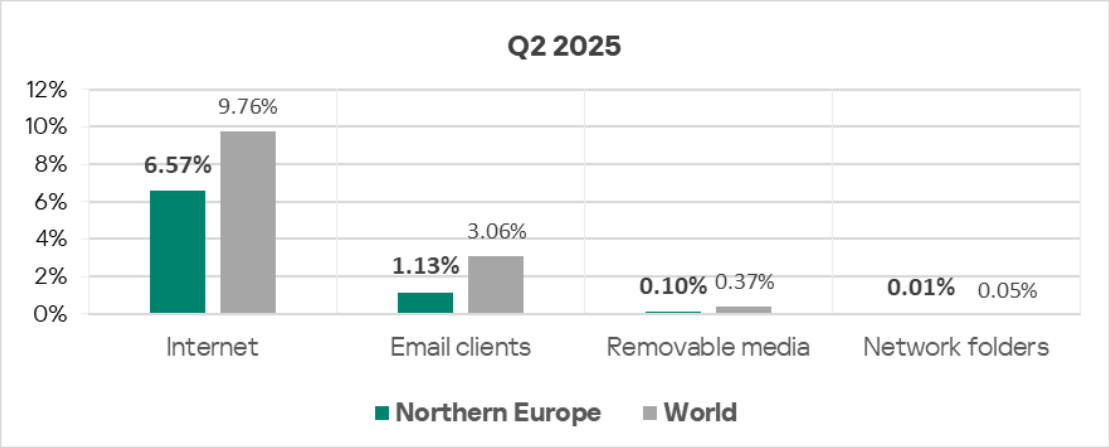


Among the countries in the region, Latvia leads with 12.77%, while Luxembourg has the lowest rate at 7.35%.



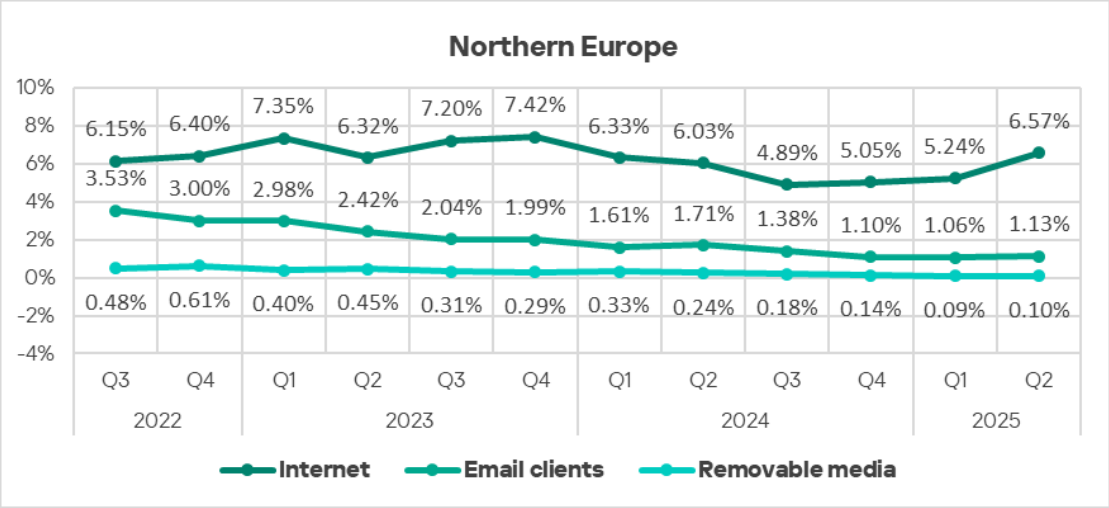
Threat sources

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



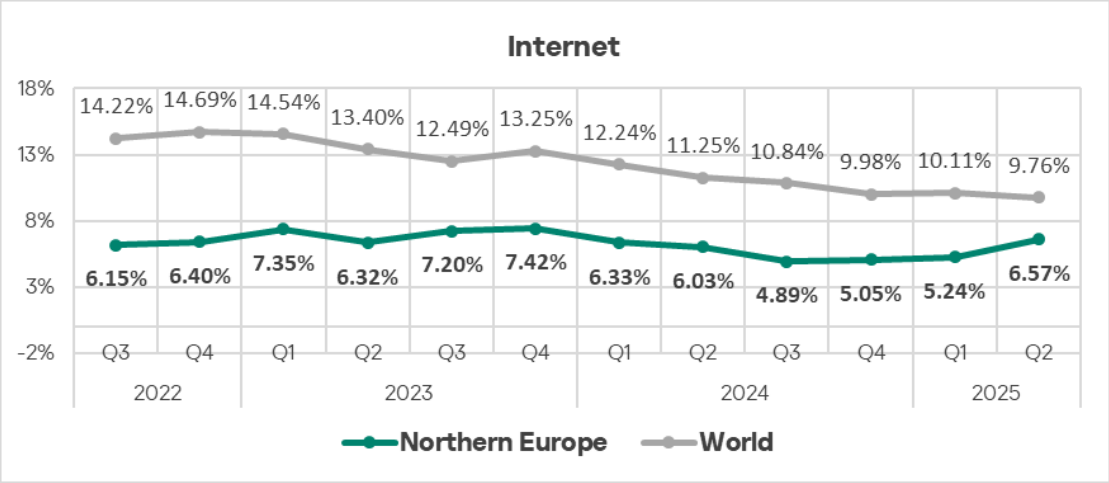
The dominant threat sources are the internet and email.

In Q2 2025, the percentage of ICS computers on which malicious objects were blocked increased across all threat sources. Northern Europe is the only region where the percentage of ICS computers on which threats from removable media were blocked did not decrease in Q2 2025.

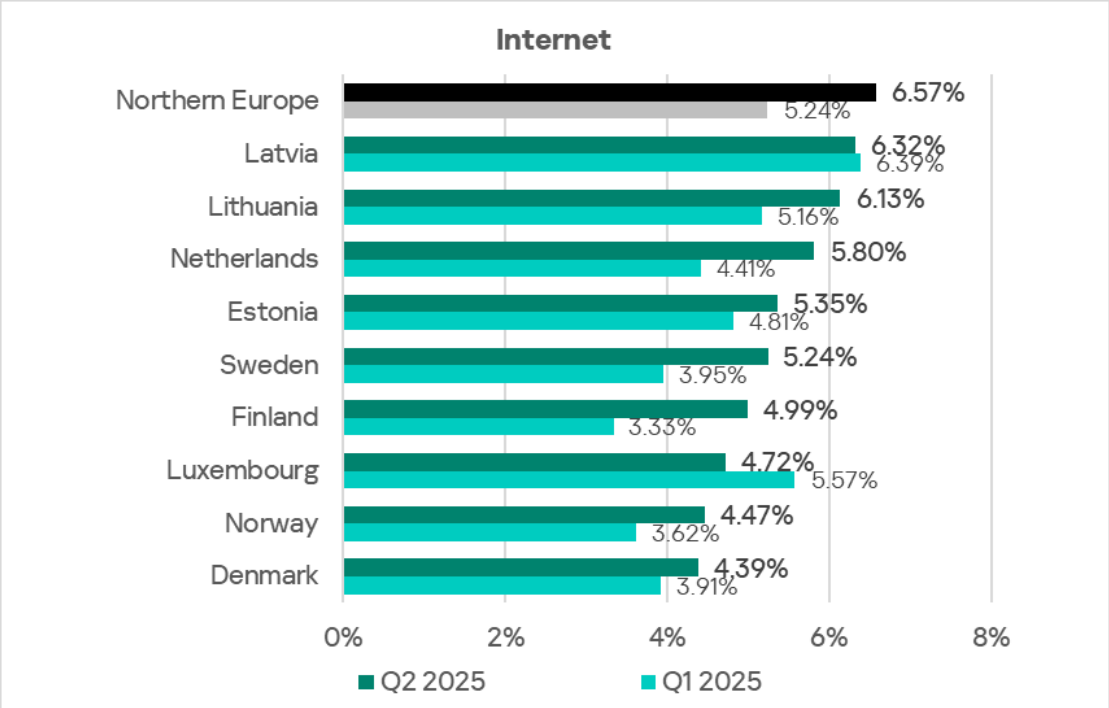


Internet

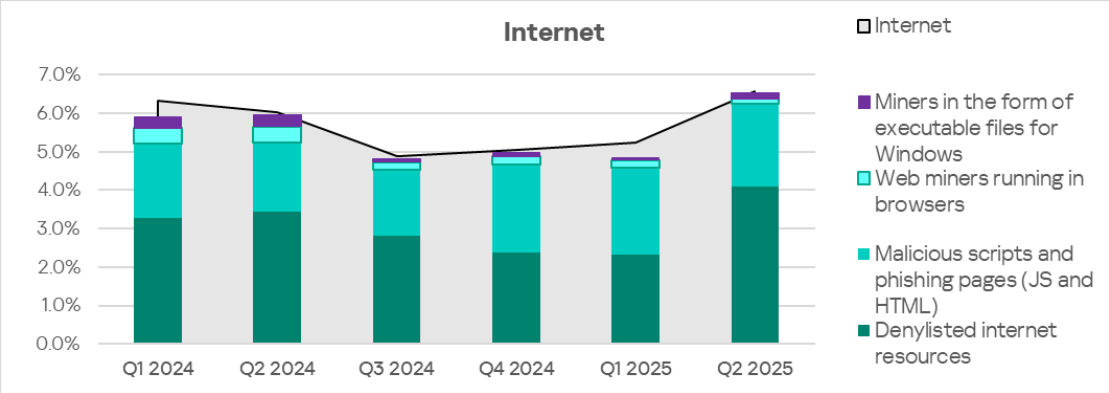
By percentage of ICS computers on which threats from the internet were blocked, Northern Europe ranks 13th globally at 6.57%. This figure has been growing for the third consecutive quarter. In Q2 2025, Northern Europe ranked first globally in growth in this category.



Across the region, the percentage of ICS computers on which threats from the internet were blocked ranges from 4.39% in Denmark to 6.32% in Latvia.

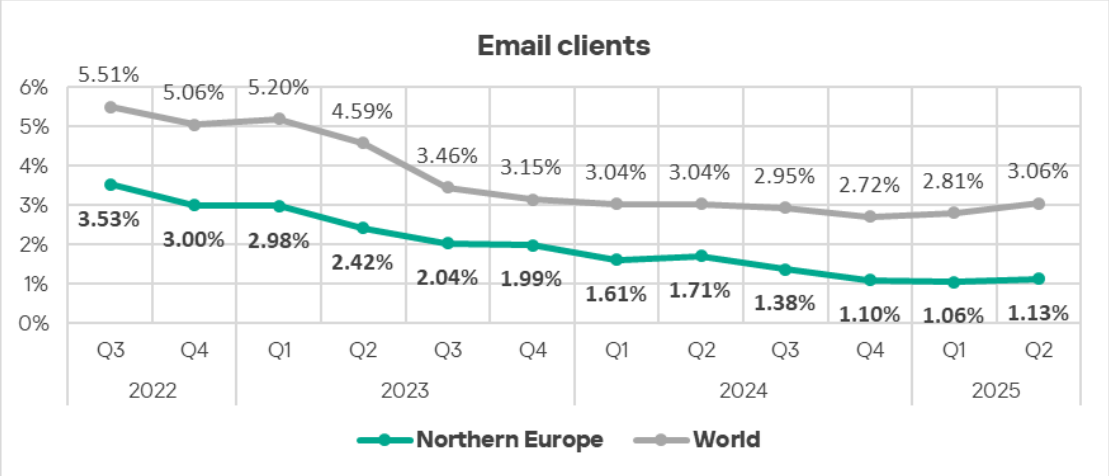


The main categories of internet threats blocked on ICS computers in the region are denylisted internet resources, malicious scripts and phishing pages, and both types of miners.

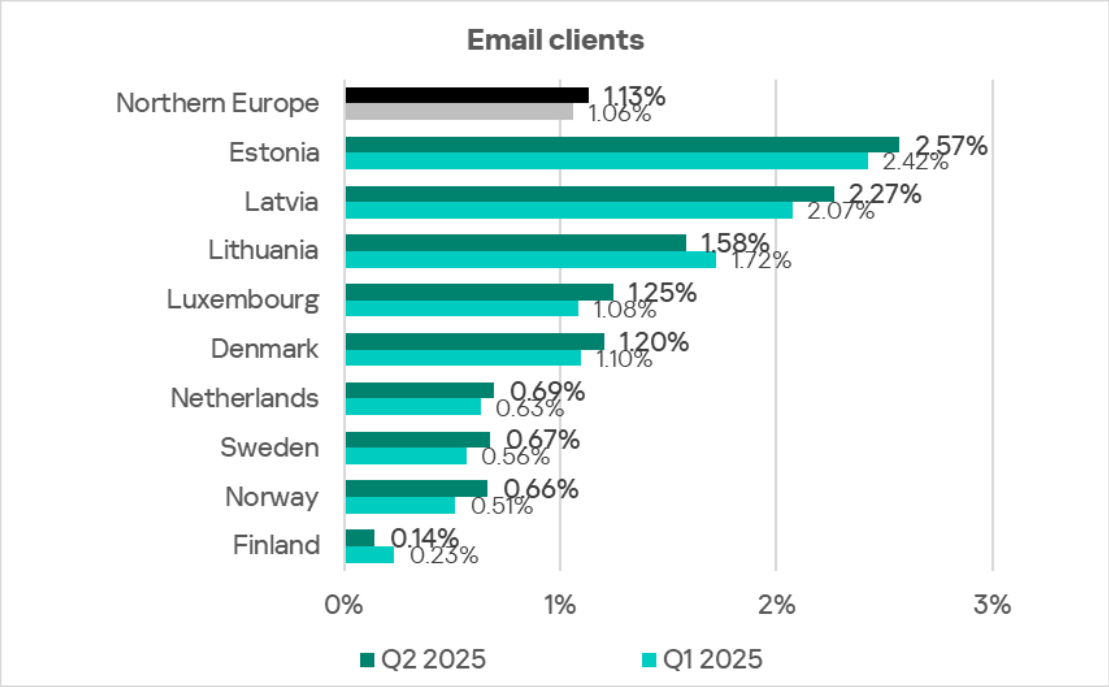


Email clients

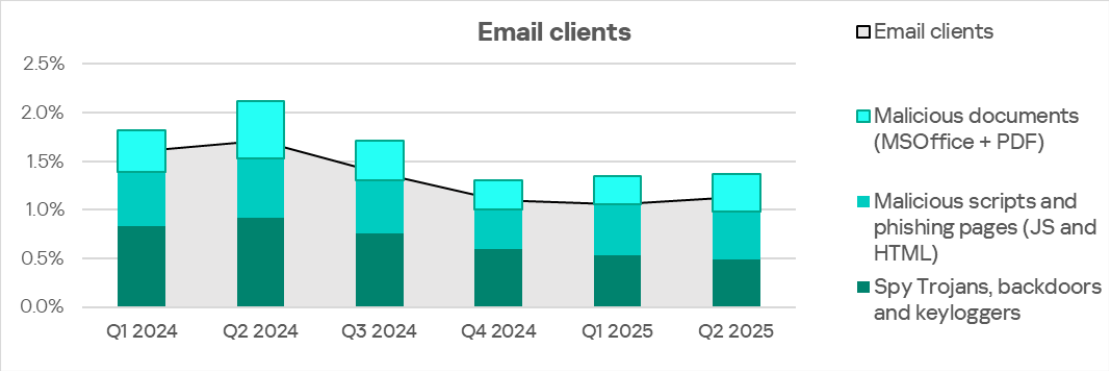
By the percentage of ICS computers on which threats from email clients were blocked, Northern Europe ranked 13th among regions in Q2 2025, with a rate of 1.13%. This is 1.4 times higher than Russia, which sits at the bottom of the ranking.



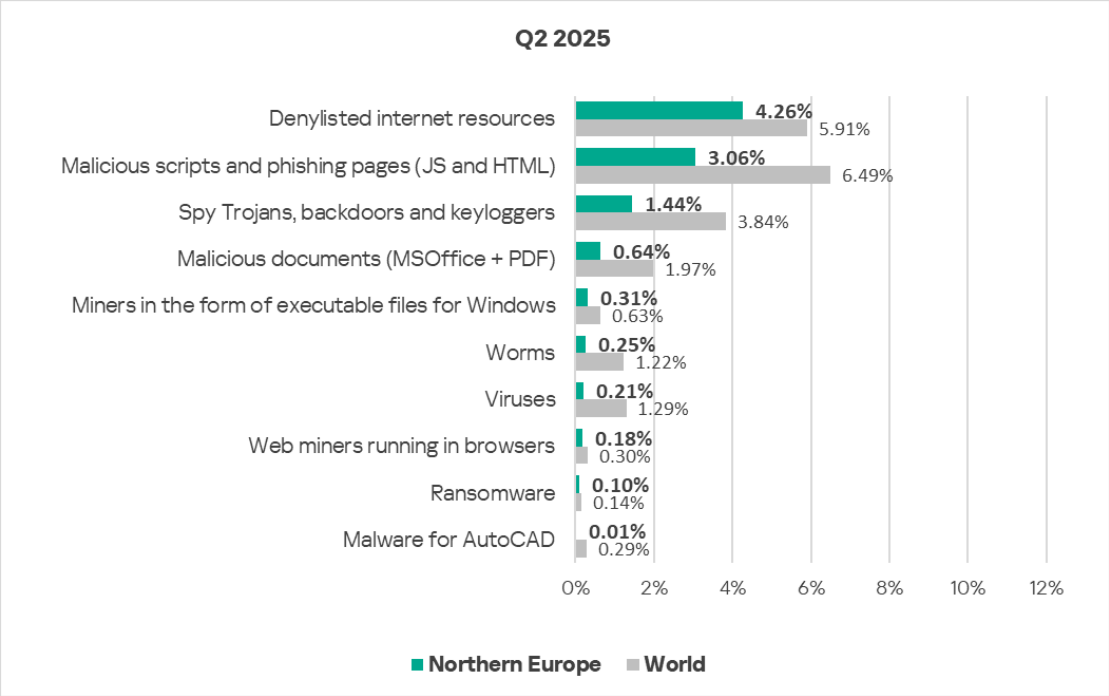
Among the region's countries, Estonia leads by this metric with 2.57%, while Finland has the lowest rate at 0.14%.

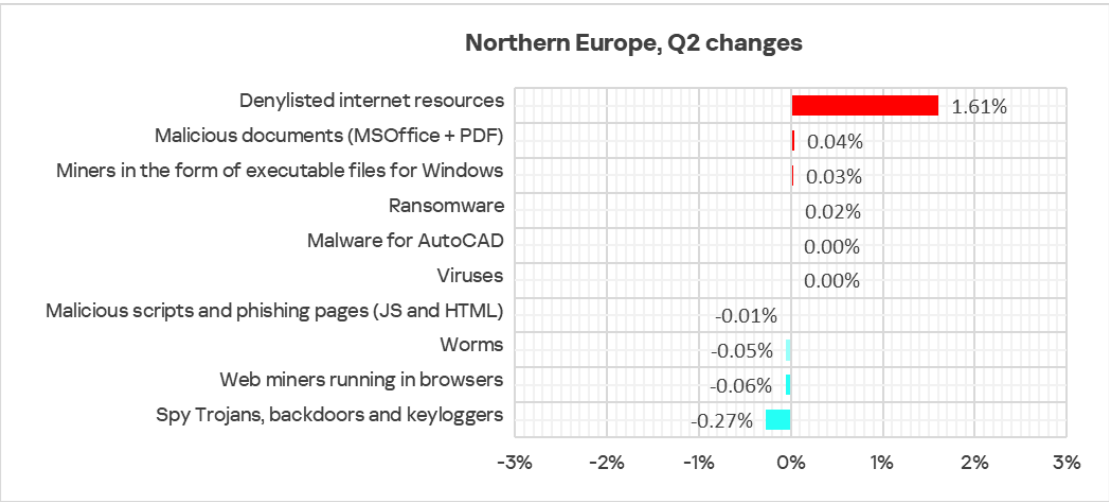


The main categories of email-borne threats blocked on ICS computers are spyware, malicious scripts and phishing pages, and malicious documents.



Threat categories





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

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

Denylisted internet resources: 1.6 times higher, the highest growth globally for this metric

Ransomware: 1.3 times higher, third globally in growth

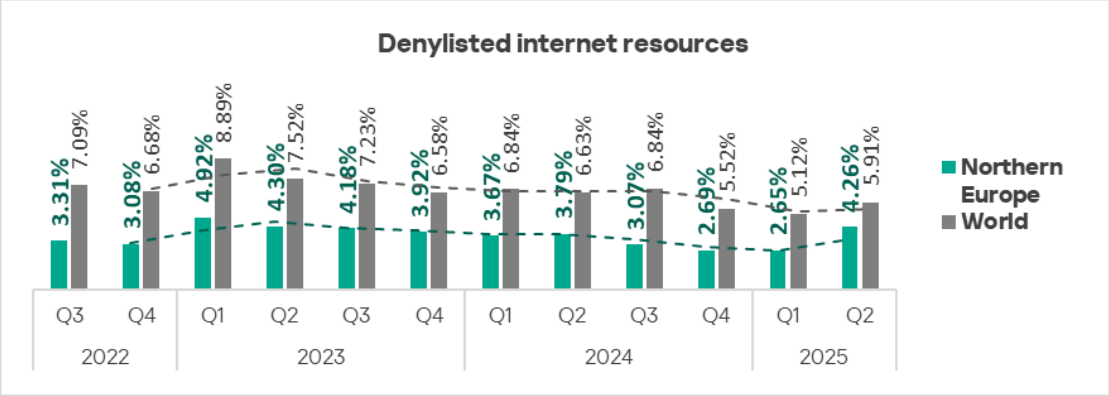
- Miners in the form of executable files for Windows: 1.1 times higher, second globally in growth
- Malicious documents: 1.1 times higher

Northern Europe is the only region where the percentage of ICS computers on which viruses were blocked did not decrease in Q2 2025.

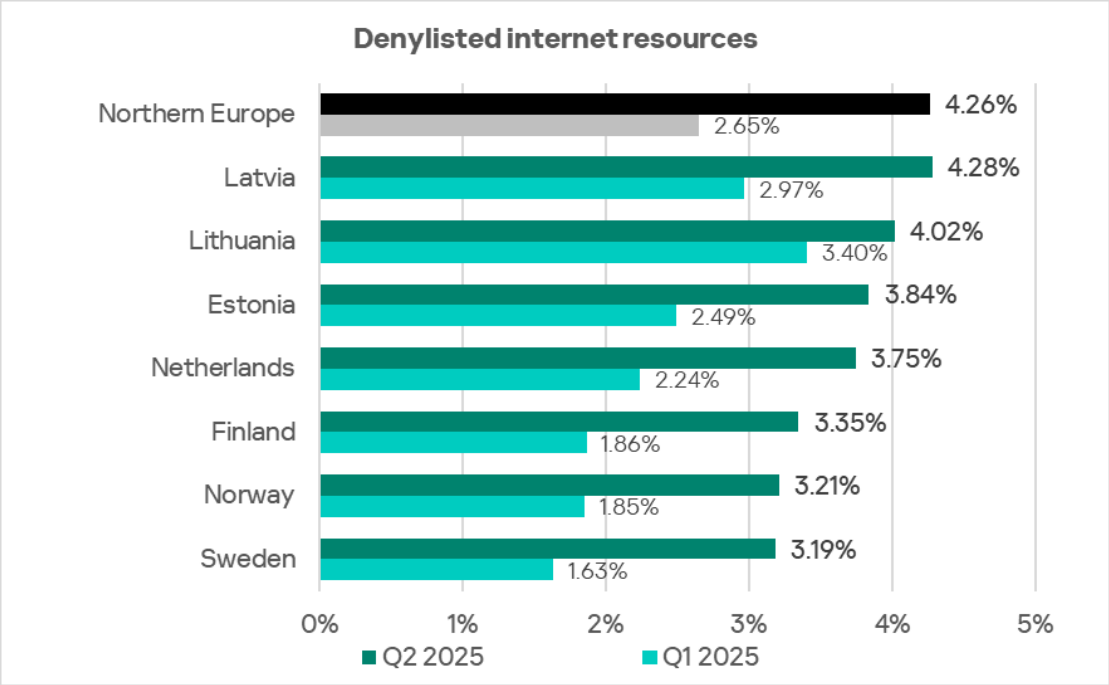
Denylisted internet resources

By the percentage of ICS computers on which denylisted internet resources were blocked, Northern Europe ranks 10th among regions, with a figure of 4.26%. This is 1.3 times higher than East Asia, where the rate is the lowest.

In Q2 2025, Northern Europe had the highest growth globally in this metric.



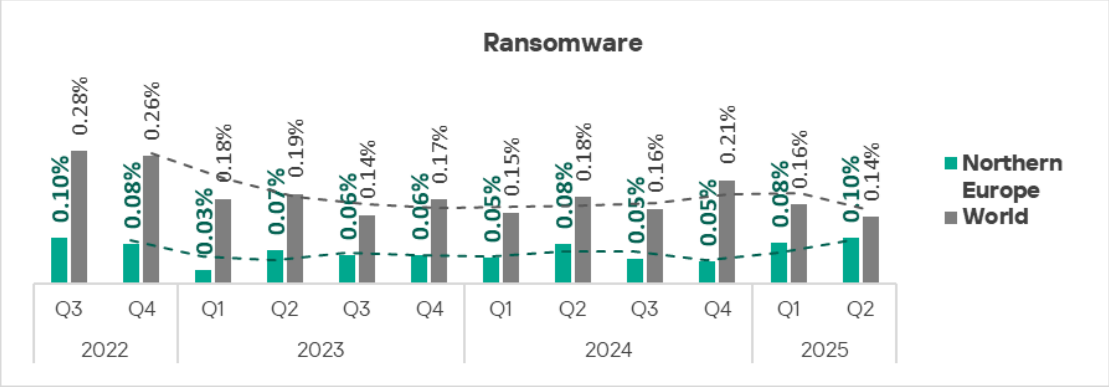
Within the region, Latvia leads with 4.28%. This quarter saw an increase in the rate across all countries in the region.



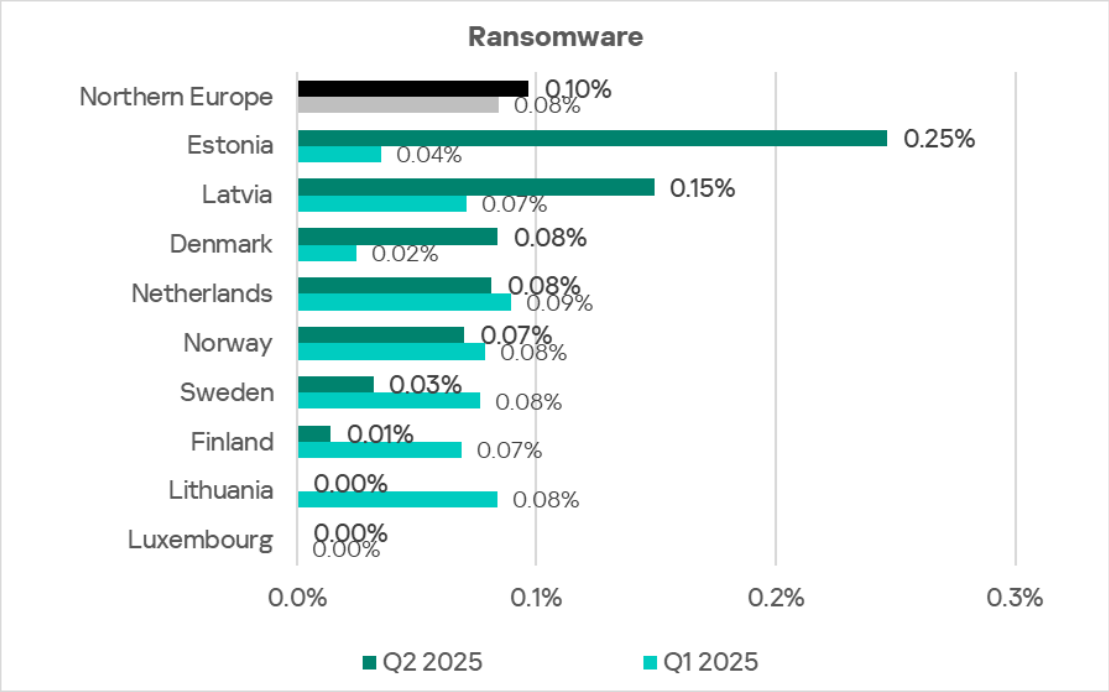
Ransomware

By the percentage of ICS computers on which ransomware was blocked, Northern Europe ranks 10th among regions, with 0.10%. This is 1.3 times higher than in Western Europe, which has the lowest figure.

The region's figure has been growing for the second consecutive quarter. In Q2 2025, Northern Europe ranked third globally for ransomware growth.



Within the region, Estonia leads, with the rate spiking to 0.25% in a single quarter.

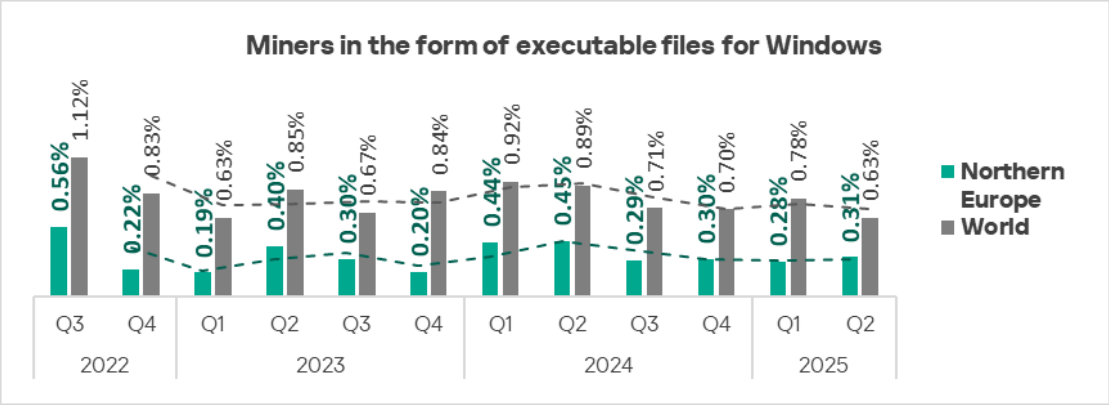


Ransomware is spread in the region via both the internet and email.

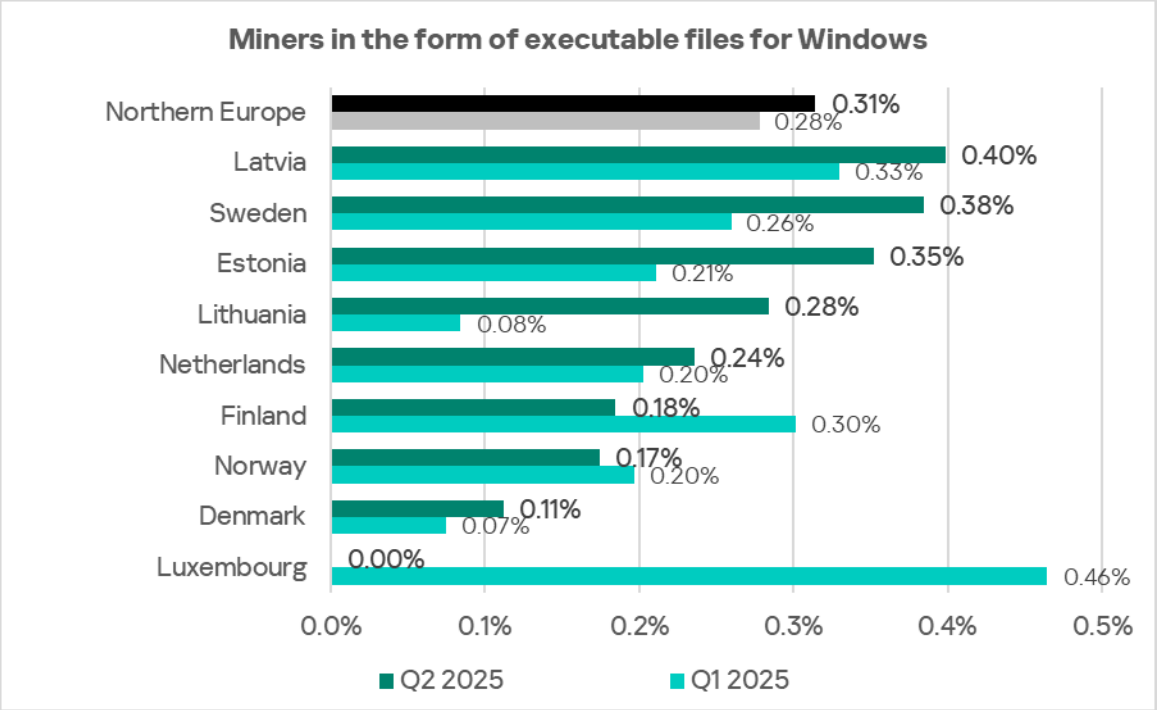
Miners in the form of executable files for Windows

By the percentage of ICS computers on which miners in the form of executable files for Windows were blocked, Northern Europe ranks 11th globally, with a rate of 0.31%. This is 1.7 times higher than East Asia, which has the lowest rate among all regions.

This metric fluctuates in the region. In terms of growth in Q2 2025, Northern Europe ranked second globally.



Within the region, Latvia leads with 0.40%.



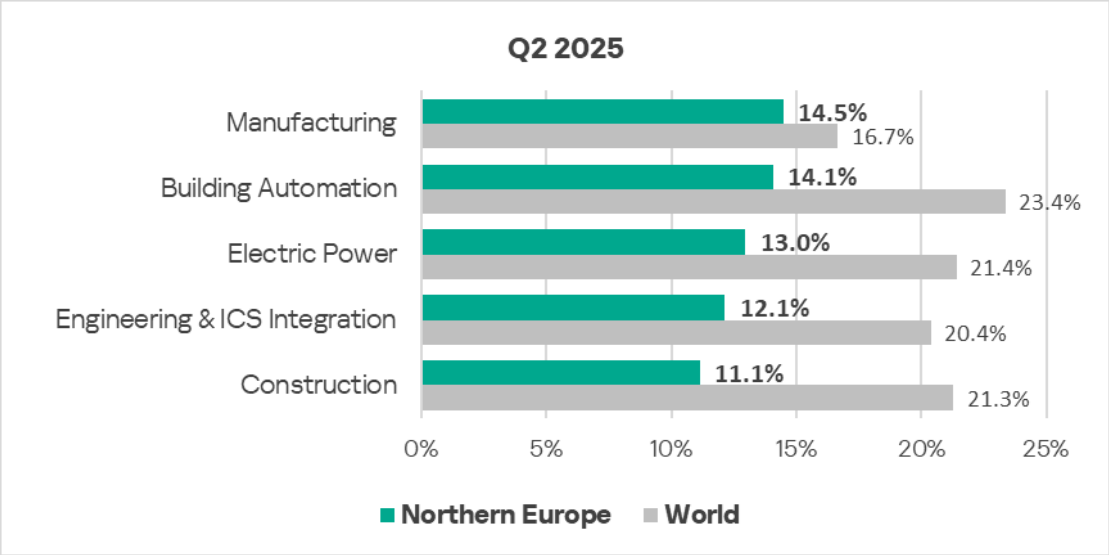
* Data for Luxembourg in Q2 2025 is not available.

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

Industries

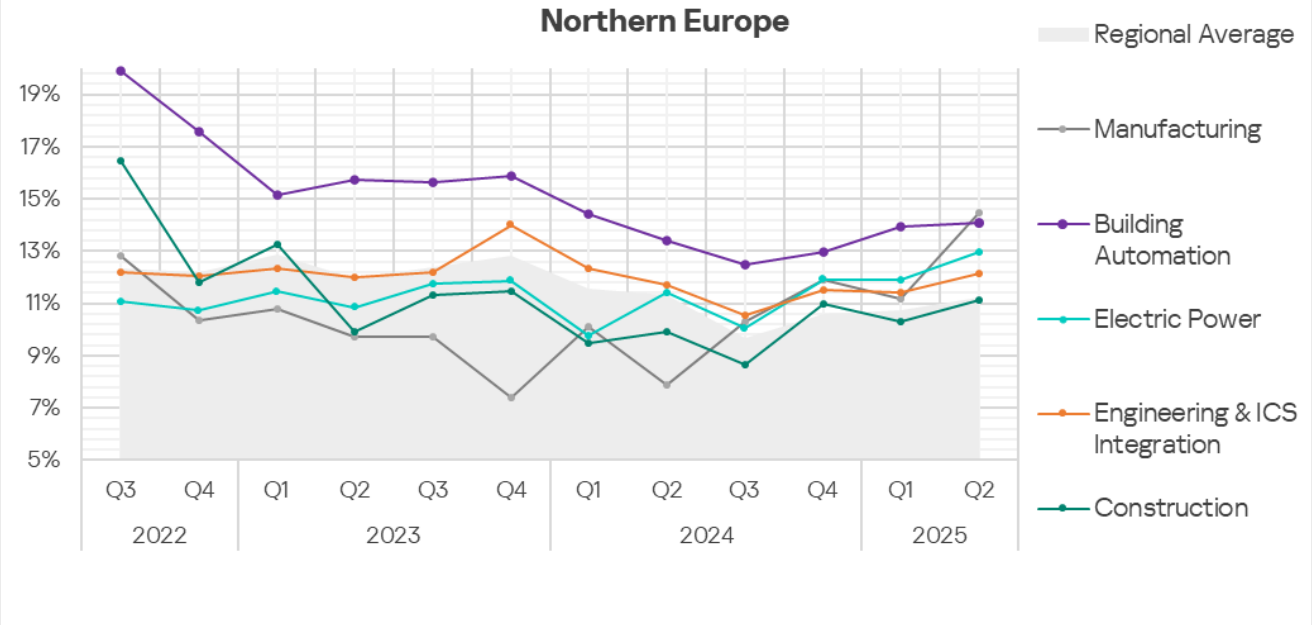
In Q2 2025, the percentage of ICS computers on which malicious objects were blocked was highest in the manufacturing sector compared to other industries under review. This figure increased by 1.3 times from the previous quarter, moving the industry up from third to first place in the regional ranking.

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



In Q2 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: hot spots

We use heat maps to assess threats facing industries. On these maps, cells are colored from red to green, where red indicates the maximum value for an industry in the region or a threat source or category across all regions and industries. In Northern Europe, most values are close to minimum levels. The

highest figure in the region is for denylisted internet resources blocked on computers in the electrical energy industry. Globally, this industry ranks 30th out of 98 for this threat category.

Threat source indicators for industries in Northern Europe, Q2 2025

Industry / Threat source	Building Automation	Electric Power	Engineering & ICS Integration	Construction	Manufacturing	Threat category total in the region
Internet	6.77%	8.09%	7.76%	6.86%	8.26%	6.57%
Email clients	3.36%	0.55%	0.72%	1.57%	1.24%	1.13%
Removable media	0.12%	0.16%	0.11%	0.31%	0.00%	0.10%
Network folders	0.00%	0.00%	0.01%	0.00%	0.00%	0.01%
Industry total in the region	14.07%	12.96%	12.13%	11.14%	14.46%	

Threat category indicators for industries in Northern Europe, Q2 2025

Industry / Threat category	Building Automation	Electric Power	Engineering & ICS Integration	Construction	Manufacturing	Threat category total in the region
Denylisted internet resources	4.53%	6.13%	4.96%	4.41%	5.58%	4.26%
Malicious scripts and phishing pages (JS and HTML)	4.20%	3.38%	3.65%	3.27%	5.58%	3.06%
Spy Trojans, backdoors and keyloggers	3.31%	1.41%	1.42%	1.51%	1.86%	1.44%
Worms	0.52%	0.55%	0.32%	0.38%	1.03%	0.25%
Miners in the form of executable files for Windows	0.30%	0.39%	0.35%	0.25%	0.41%	0.31%
Malicious documents (MSOffice + PDF)	1.69%	0.47%	0.48%	0.50%	0.83%	0.64%
Viruses	0.49%	0.47%	0.17%	0.38%	0.21%	0.21%
Ransomware	0.21%	0.31%	0.11%	0.19%	0.00%	0.10%
Web miners running in browsers	0.18%	0.31%	0.24%	0.19%	0.21%	0.18%
Malware for AutoCAD	0.00%	0.00%	0.00%	0.13%	0.00%	0.01%
Industry total in the region	14.07%	12.96%	12.13%	11.14%	14.46%	

Industry hot spots

Manufacturing

- Regional leader by the percentage of ICS computers on which threats from the internet were blocked.
- Regional leader in the following threat categories: malicious scripts and phishing pages, spyware, malicious documents, ransomware.
- Second place regionally in viruses and web miners.

Building automation

- Regional leader by the percentage of ICS computers on which threats from email clients were blocked.
- Regional leader in viruses.
- Second place regionally in the following categories: malicious scripts and phishing pages, spyware, malicious documents, worms, ransomware.

Electrical energy industry

- Second place regionally in threats from the internet and removable media.
- Regional leader in the following categories: denylisted internet resources, both categories of miners, and worms.

Engineering and ICS integrators

- Regional leader in network folder threats.
- Second place regionally in denylisted internet resources, miners in the form of executable files for Windows, and malware for AutoCAD.

Construction

- Regional leader in the percentage of ICS computers on which removable media threats were blocked. Third place in email client and network folder threats.
- Regional leader in malware for AutoCAD.

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