Kaspersky ICS CERT

kaspersky

# Threat landscape for industrial automation systems

## Europe. Q4 2025

28.04.2026

Version 1.0

Southern Europe 5
Key cybersecurity issues in the region 5
Statistics across all threats 6
Threat sources 8
Internet 9
Email clients 11
Removable media 13
Threat categories 15
Malicious documents 16
Malicious scripts and phishing pages 18
Spyware 19
Ransomware 21
Worms 22
Industries 24
Threat sources and malware categories in industries: 'hotspots' 28
Characteristics of the region 29
Eastern Europe 34
Key cybersecurity issues in the region 34
Statistics across all threats 35
Threat sources 37
Internet 38
Email clients 40
Removable media 42
Network folders 44
Threat categories 46
Malicious scripts and phishing pages 47
Spyware 48
Denylisted internet resources 50
Malicious documents 51
Worms 53
Miners in the form of executable files for Windows 54
Industries 56

Threat sources and malware categories in industries: 'hotspots' 58
Western Europe 63
Key cybersecurity issues in the region 63
Statistics across all threats 63
Threat sources 65
Internet 65
Email clients 67
Removable media 69
Network folders 71
Threat categories 73
Malicious scripts and phishing pages 74
Denylisted internet resources 76
Spyware 77
Malicious documents 79
Ransomware 80
Worms 82
Industries 83
Threat sources and malware categories in industries: 'hotspots' 86
Northern Europe 91
Key cybersecurity issues in the region 91
Statistics across all threats 92
Threat sources 93
Internet 94
Email clients 96
Threat categories 98
Malicious scripts and phishing pages 99
Denylisted internet resources 101
Spyware 103
Malicious documents 104
Miners in the form of executable files for Windows 106
Web miners 107
Viruses 109

Worms ..... 111
Industries ..... 113
Threat sources and malware categories in industries: 'hotspots' ..... 116
Methodology used to prepare statistics ..... 120

# 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 biometrics and building automation. Attacks on computers in these industrial automation sectors significantly raise the risk of supply-chain attacks on other industries.

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

It also led the ranking of regions 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.

### High rate of malicious scripts and phishing pages

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 percentage of ICS computers on which malicious scripts and phishing pages were blocked, Southern Europe ranked fourth 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 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 ranked third, with a rate 1.3 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**

In terms of the percentage of ICS computers on which ransomware was blocked, Southern Europe ranked third with a figure that was 1.8 times above the global average.

The percentage of ICS computers on which ransomware was blocked in the region increased by a factor of 1.47. During the quarter, this figure grew in five regions, with Southern Europe recording the most growth. This high position was driven by Greece, where the percentage of ICS computers on which ransomware was blocked increased by a factor of 3.6.

**Threat of the quarter**

In Q4 2025, email became a channel for spreading phishing messages during the latest wave of phishing campaigns known as Curriculum-vitae-catalina. These emails, disguised as a resume, contained a malicious executable file, the remote administration backdoor worm known as Backdoor.MSIL.XWorm. As a result, the figure for worms increased across all regions. Southern Europe led all other regions in terms of the growth in this metric.

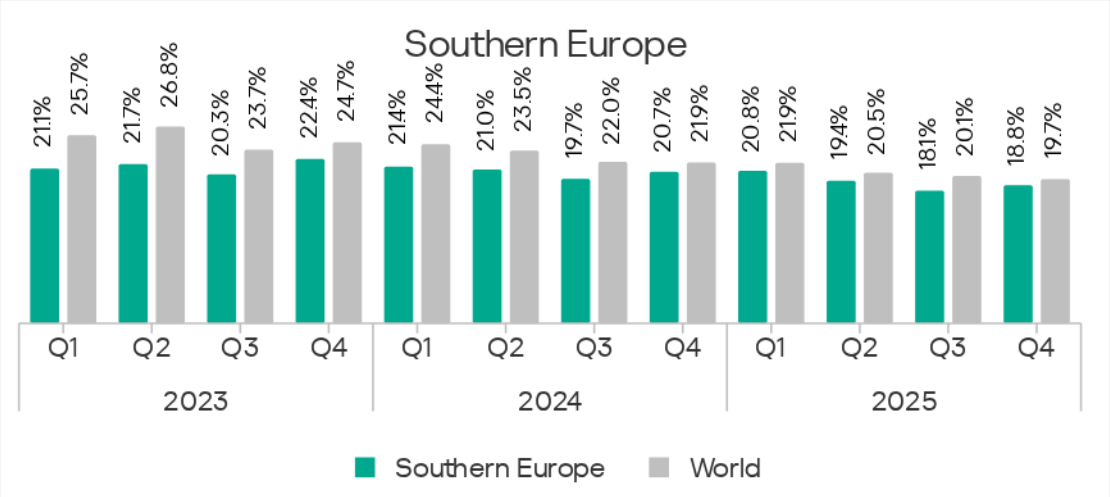
The figure for worms increased across all surveyed industries in the region, but most of all in the building automation industry (by a factor of 2.96) and the construction industry (by a factor of 2.60).

## Statistics across all threats

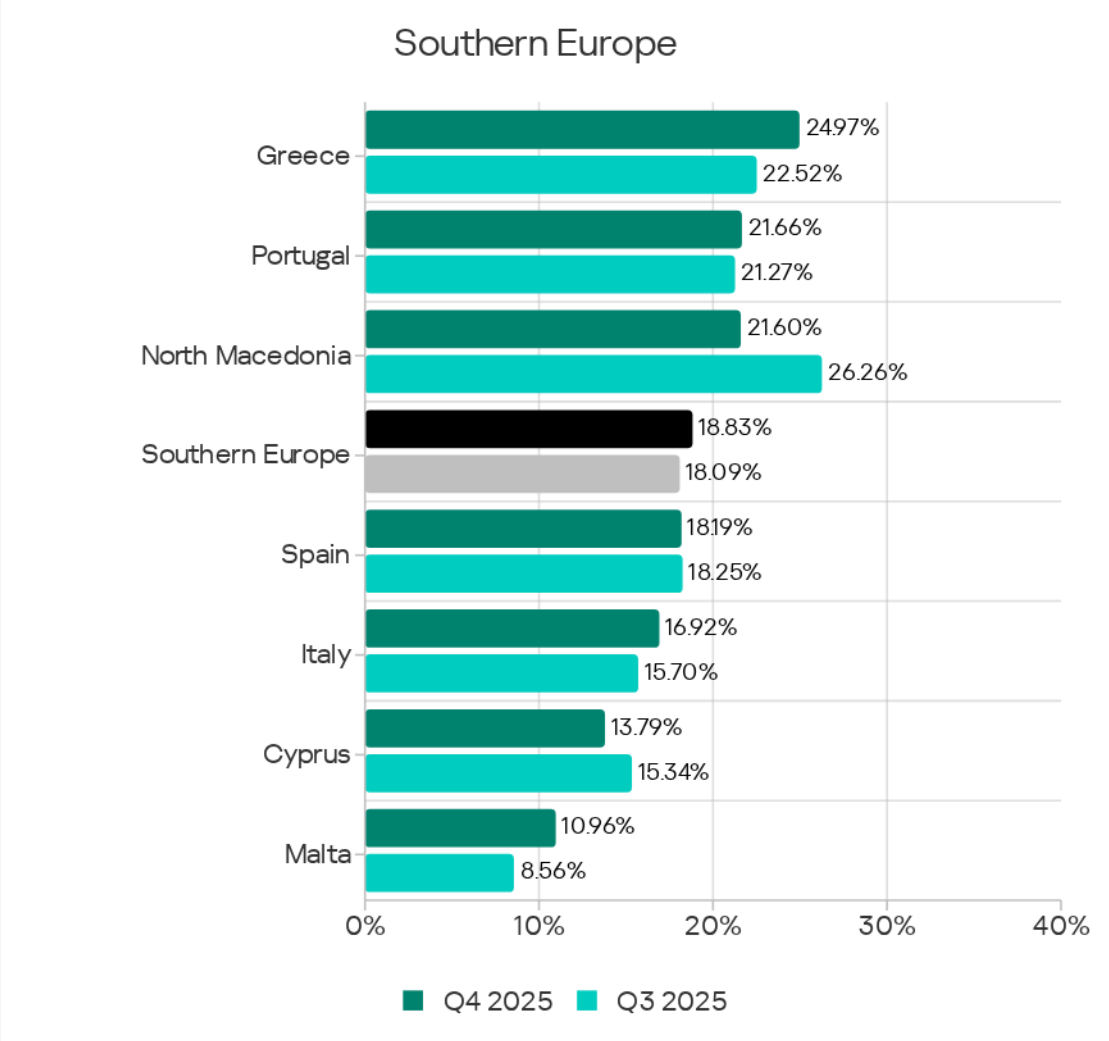
In Q4 2025, Southern Europe ranked eighth globally in the percentage of ICS computers on which malicious objects were blocked. The figure for Southern Europe was the highest among all regions in Europe.

This figure for the region increased to 18.8%. This was below the global average but still 2.2 times higher than in Northern Europe, the lowest-ranked region.

Southern Europe was one of four regions where the percentage of ICS computers on which malicious objects were blocked increased in Q4 2025. The region ranked first in terms of this increase.



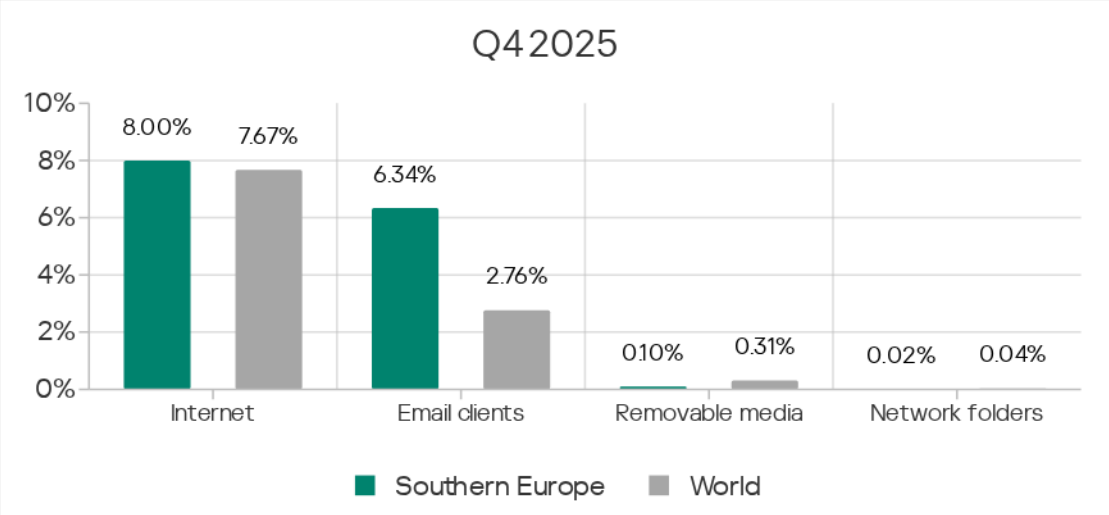

Among the region's countries, Greece led in the percentage of ICS computers on which malicious objects were blocked, at 24.97%. Malta had the lowest figure at 10.96%.



## Threat sources

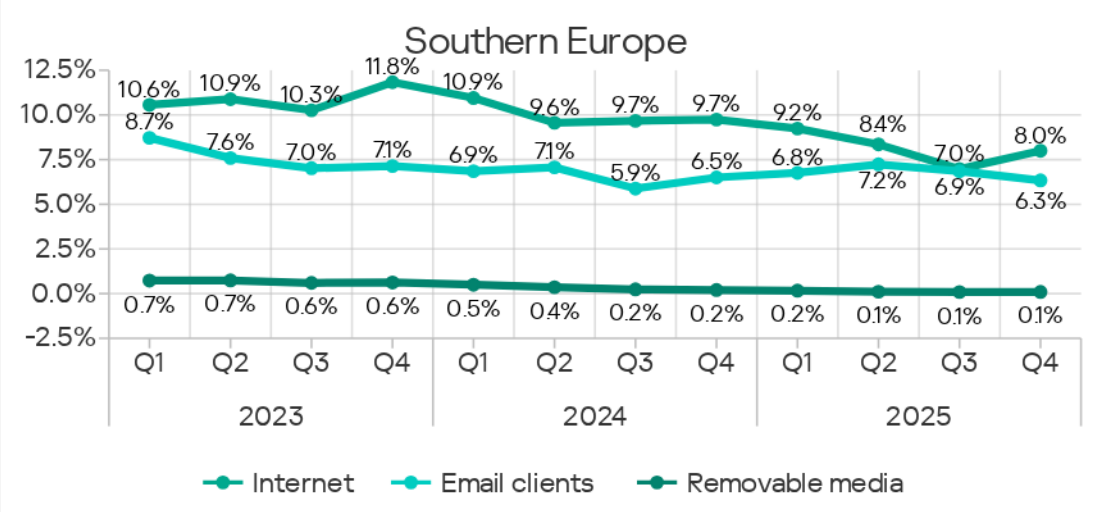
Southern Europe ranked first globally in the percentage of ICS computers on which threats form email clients were blocked. The rate for the region (6.34%) was 2.3 times higher than the global average.

The internet was another threat source that ranked above the global average. The figures for all other threat sources in Southern Europe were below the global averages.



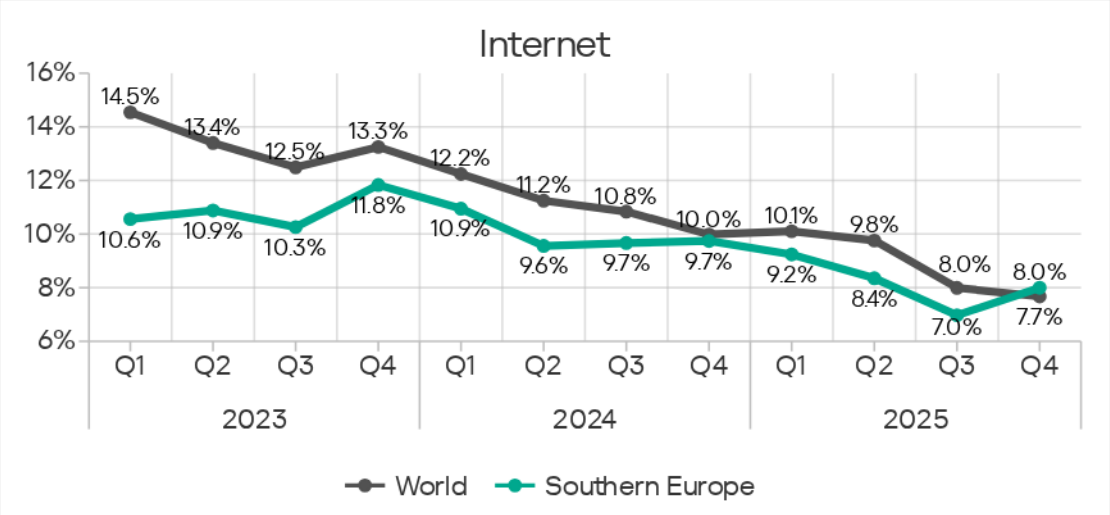

The main malware distribution channels in the region were the internet and email.

In Q4 2025, the region saw the figures for internet threats and removable drive threats increase.

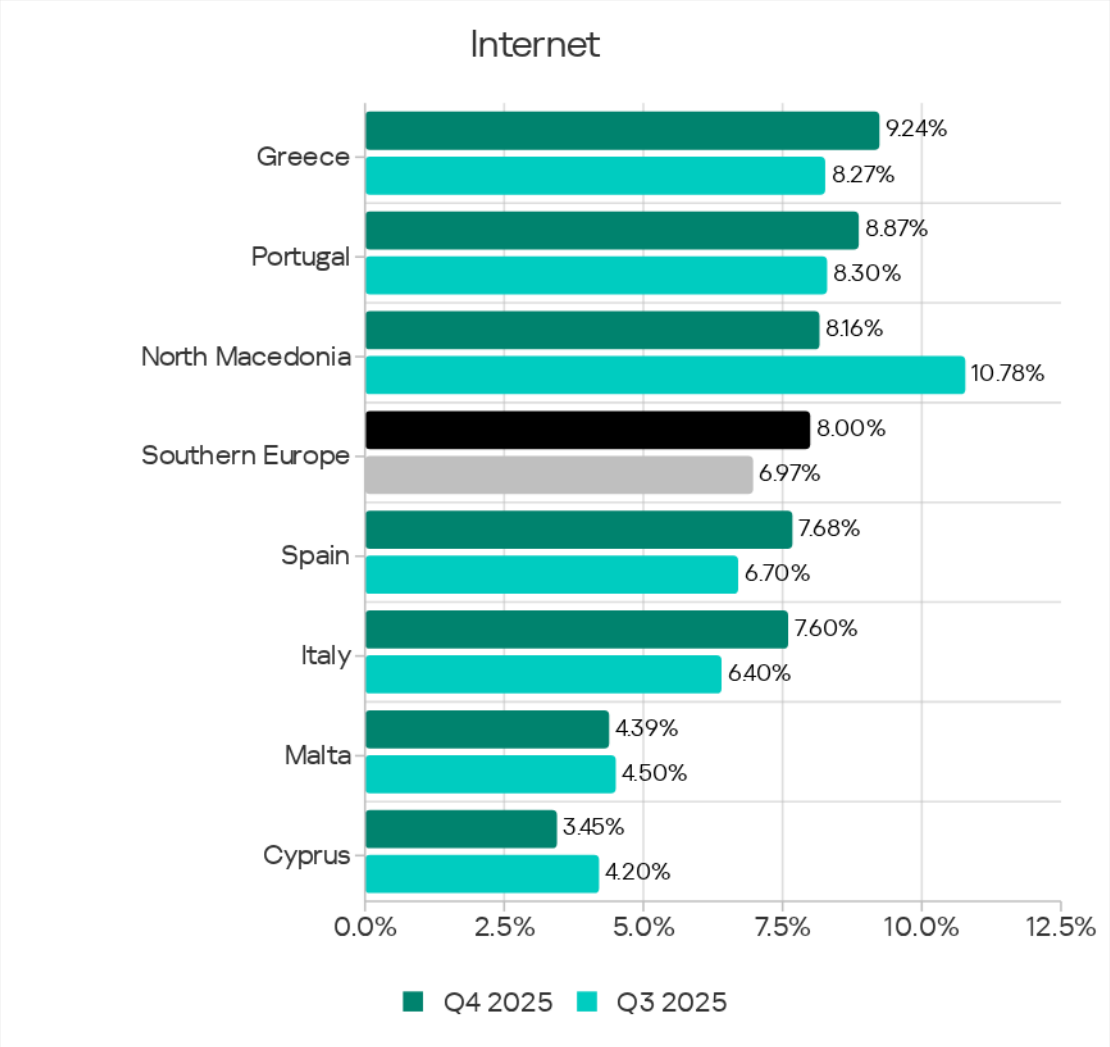


## Internet

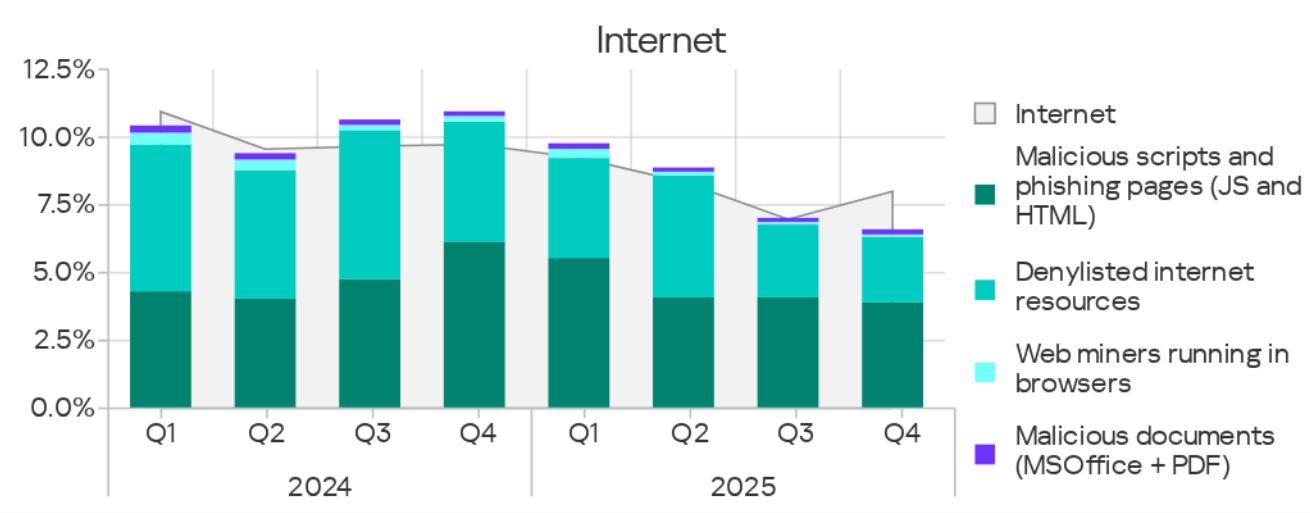
In terms of the percentage of ICS computers on which internet threats were blocked, Southern Europe rose from eighth to fifth place globally in Q4 2025. The figure for the region, at 8.00%, was twice as high as that for Northern Europe, which had the lowest figure among regions.




The figures increased across all countries in the region except for North Macedonia and Cyprus, ranging between 3.45% in Cyprus and 9.24% in Greece.

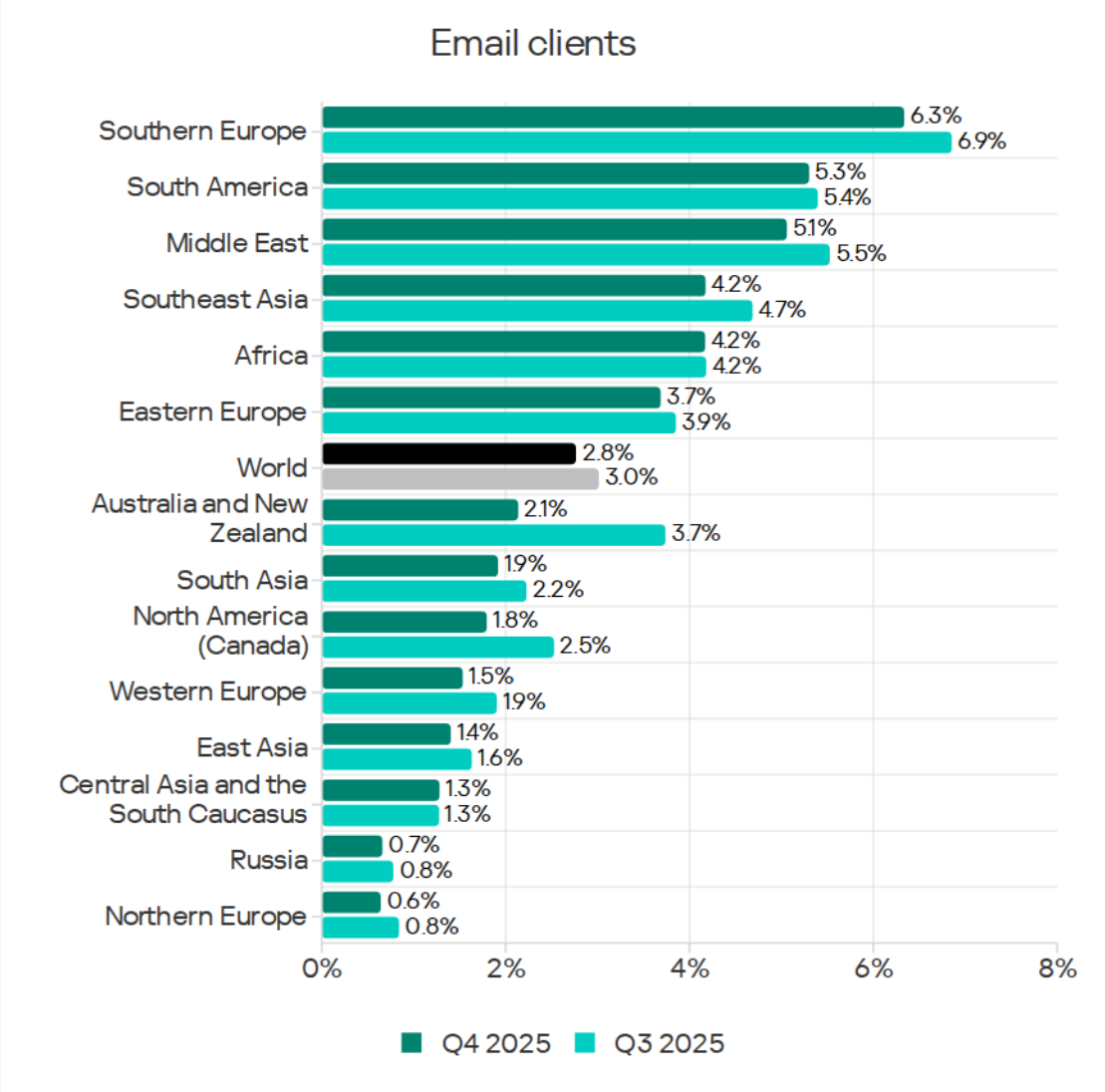



The main categories of internet threats blocked on ICS computers in the region were denylisted internet resources and malicious scripts and phishing pages.

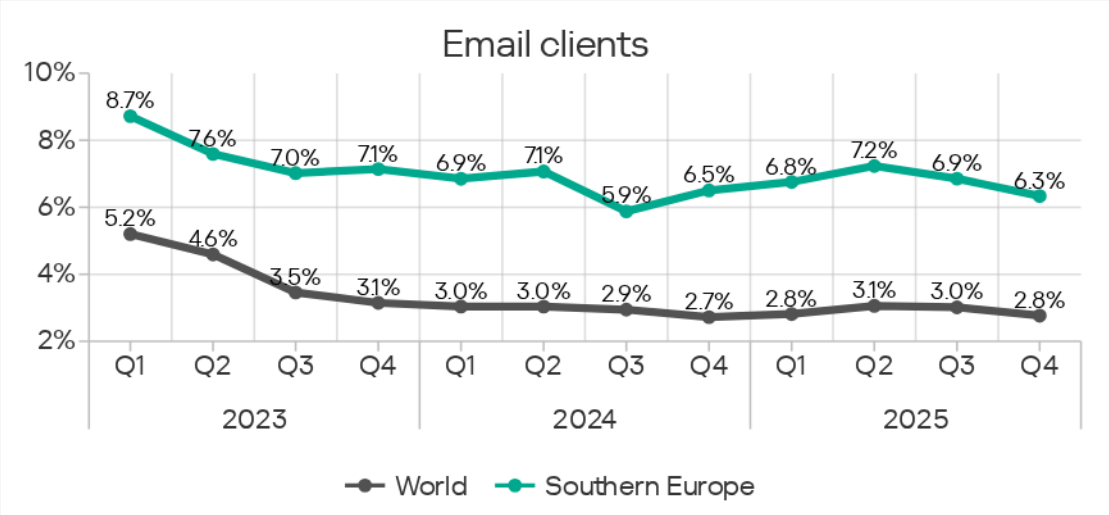


## Email clients

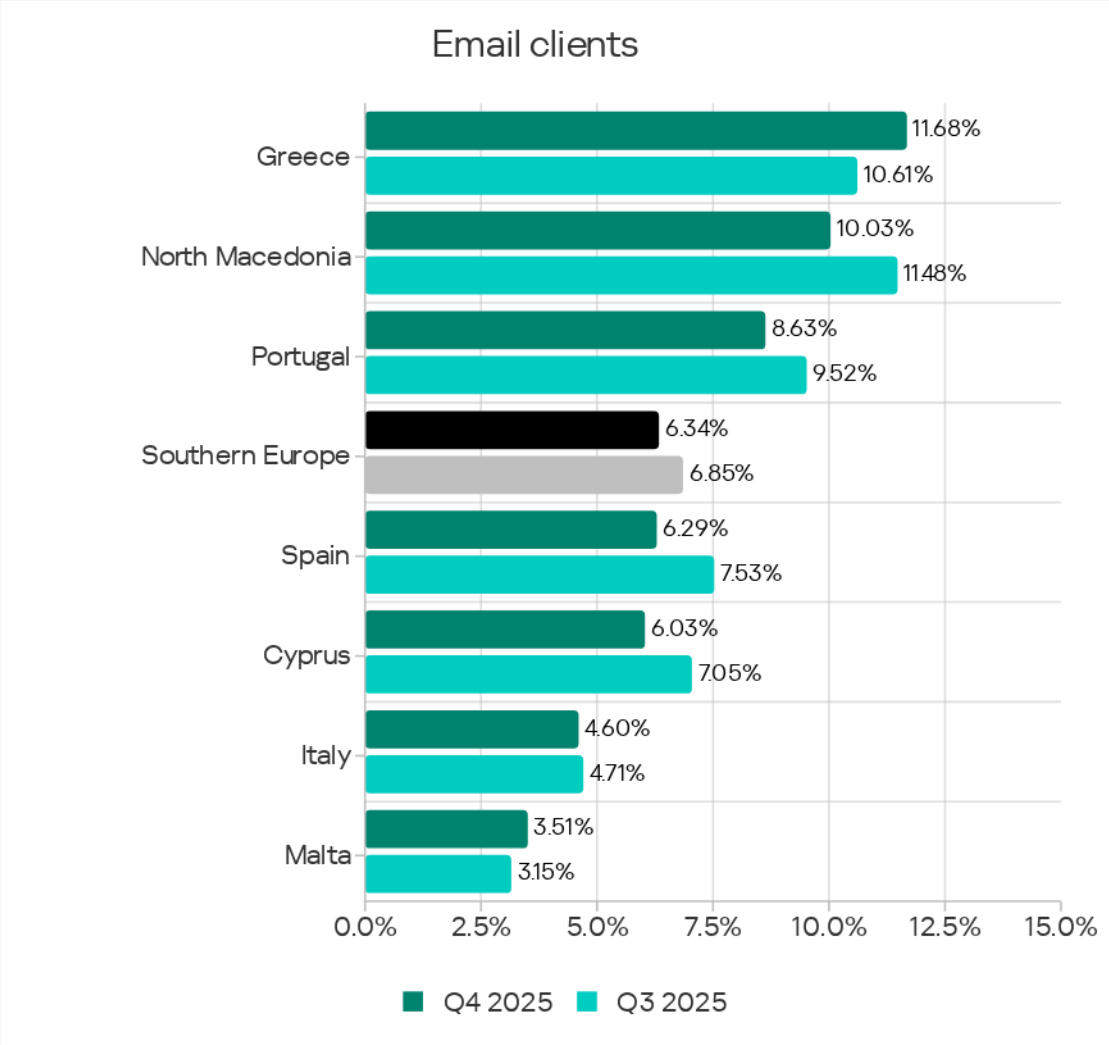
By percentage of ICS computers on which threats from email clients were blocked, Southern Europe led globally, with 6.34% in Q4 2025. This was 9.9 times higher than in Northern Europe, which ranked last.



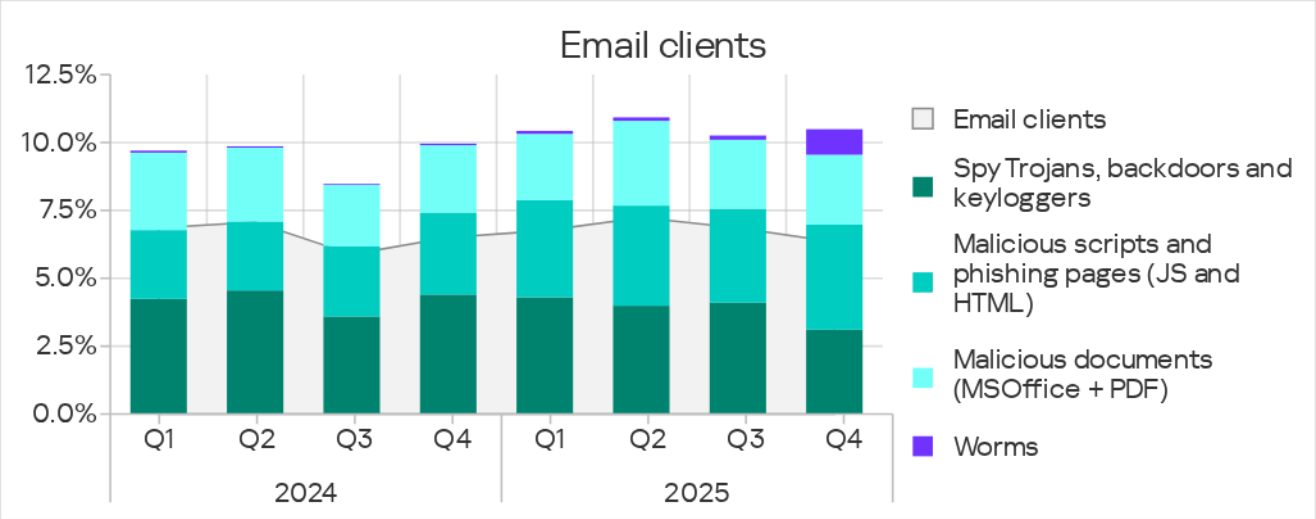

The percentage of ICS computers on which threats from email clients were blocked in Southern Europe has declined for two consecutive quarters.




Among countries in the region, Greece led with 11.68% in the percentage of ICS computers on which threats from email clients were blocked. The lowest figure observed was in Malta at 3.51%.



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




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

Q4 2025 saw a noticeable increase in the percentage of ICS computers on which worms from mail clients were blocked. This was connected associated with the latest wave of phishing campaigns known as Curriculum-vitae-catalina, which launched attacks across all regions of the world.

The attackers distributed phishing emails disguised as job applications. Disguised as a resume (Curriculum Vitae), these emails contained a malicious executable file, a remote administration backdoor worm known as Backdoor.MSIL.XWorm. Running that file caused system infection.

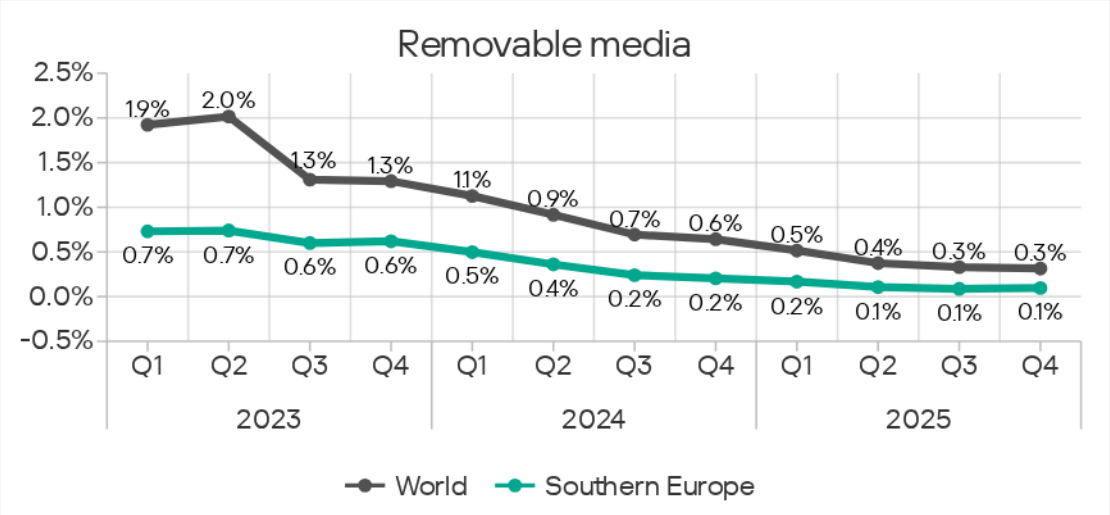
Normally, these campaigns are designed to deliver malware for data theft, spyware, or remote administration tools (RATs).

In Southern Europe, these attacks peaked in November. The figure for worms increased across all regions, with Southern Europe taking the top spot in terms of the growth for this metric.

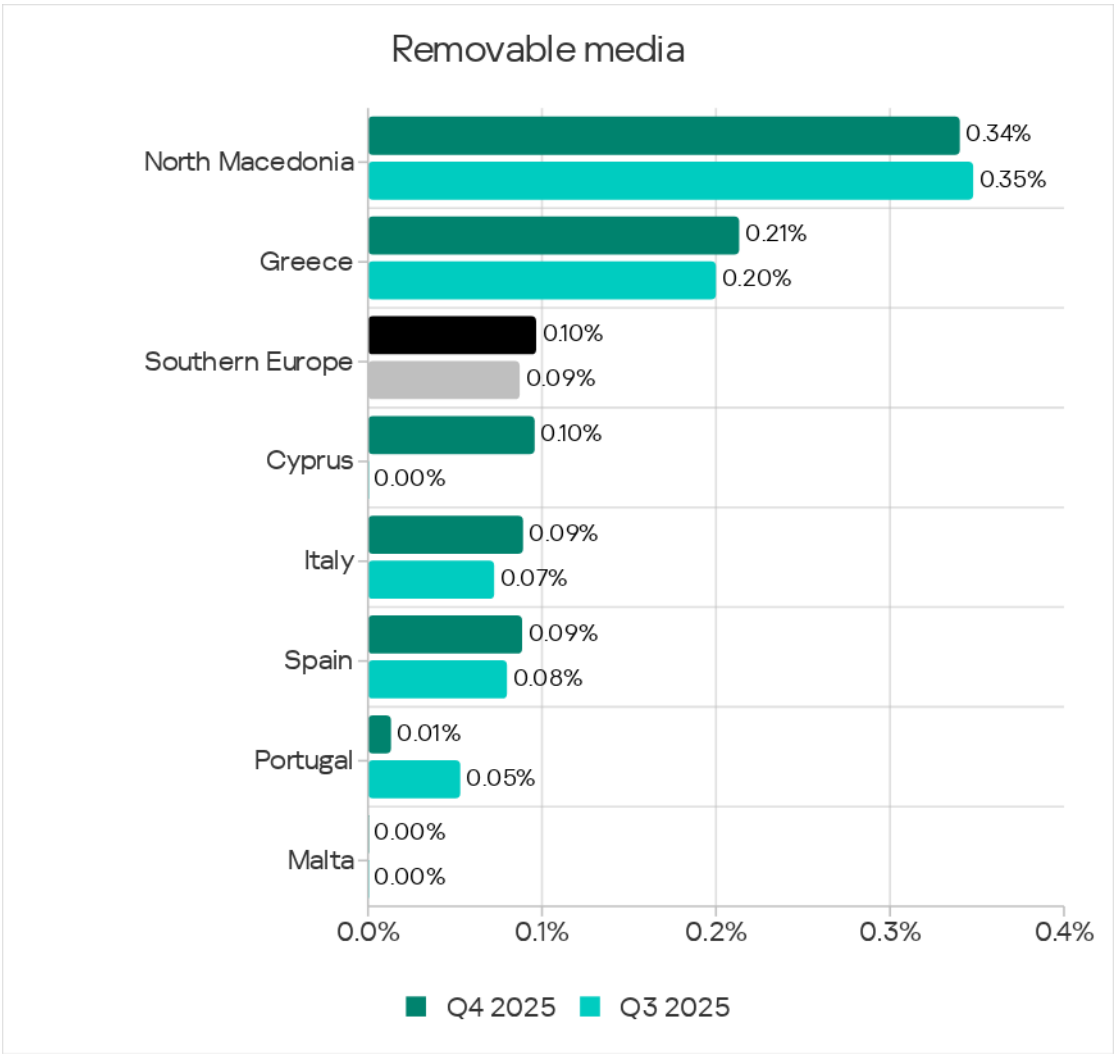
## Removable media

In terms of the percentage of ICS computers on which threats from removable media were blocked, Southern Europe ranked ninth among regions in Q4 2025 at 0.10%. This figure was 2.0 times higher than in the Australia and New Zealand region, which ranked last.

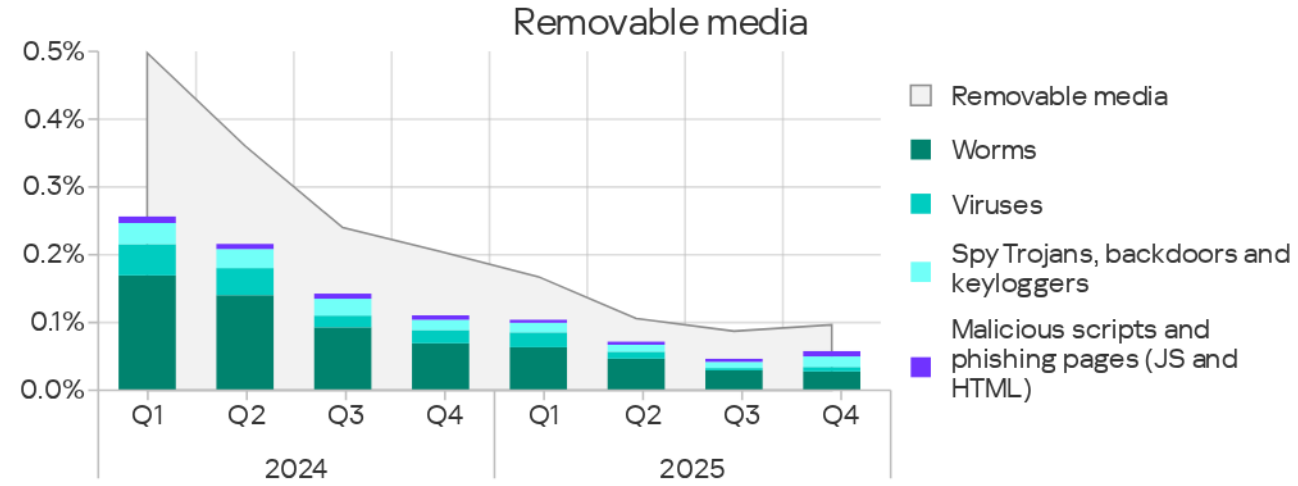
Southern Europe was one of three regions where the figure grew during the quarter.



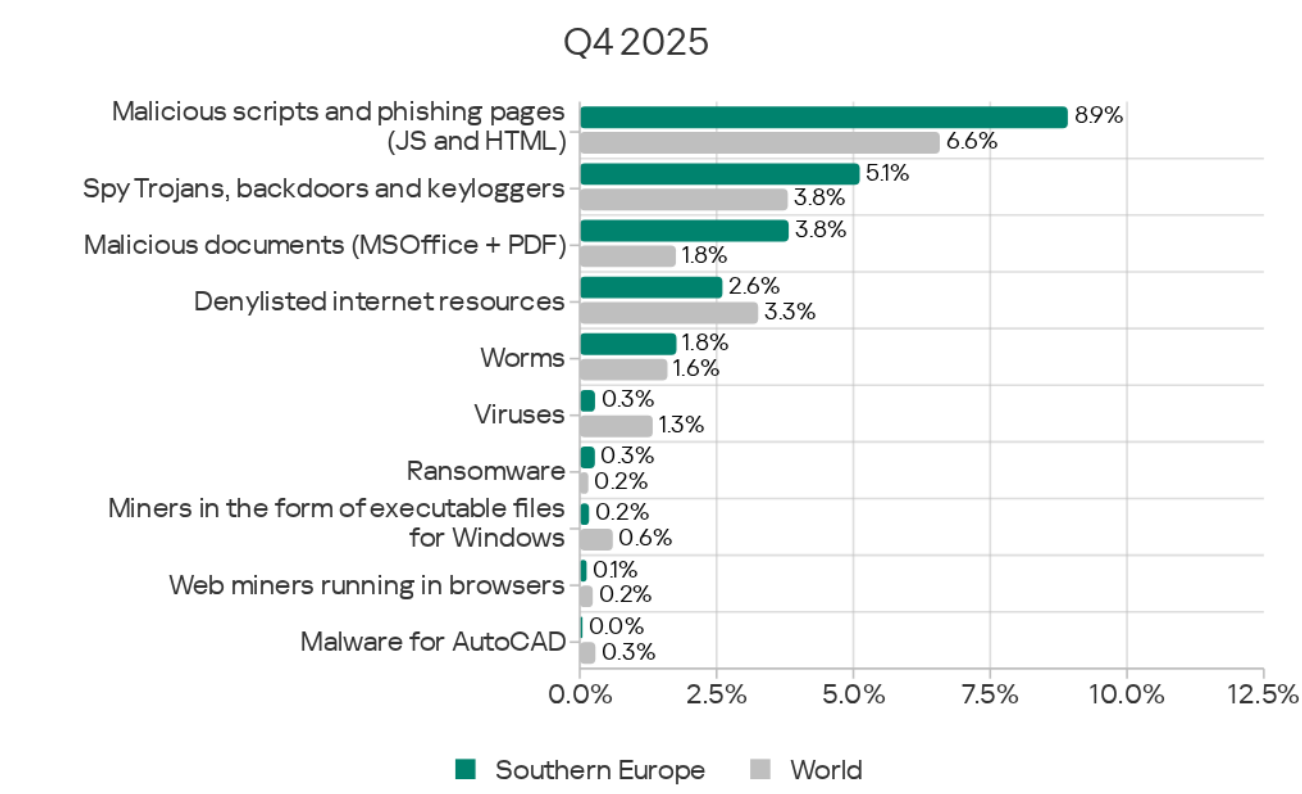

Within the region, North Macedonia was the leader with 0.34%.

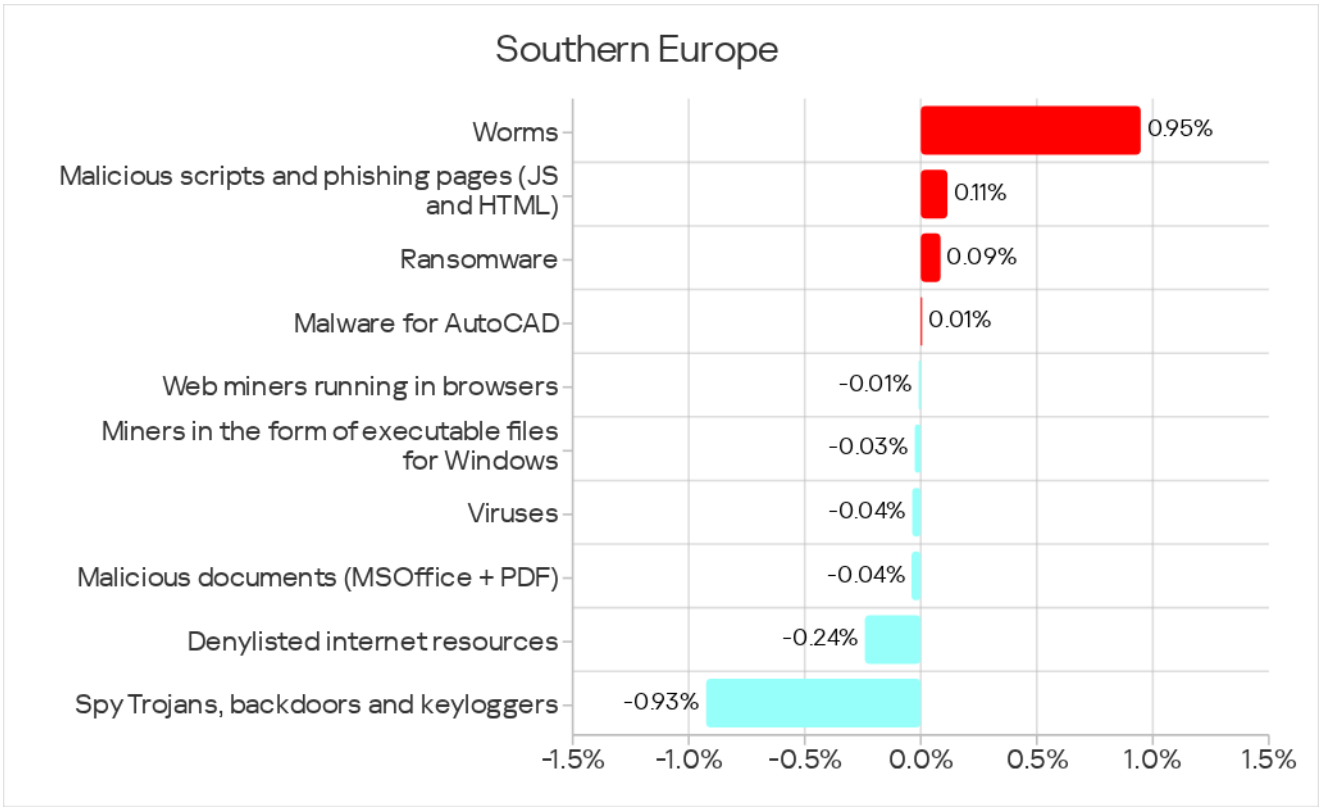


The main categories of threats that were blocked when connecting removable media to ICS computers were worms, spyware, malicious scripts and phishing pages, and viruses.




## Threat categories






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

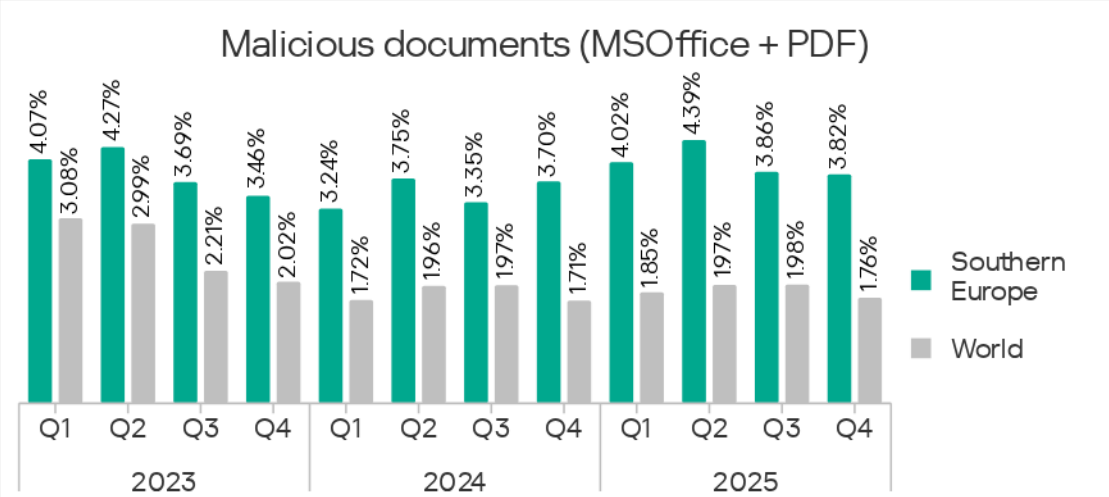
- Malicious documents: 2.2 times higher, or first among regions by the percentage of ICS computers on which this threat was blocked.
- Malicious scripts and phishing pages: 1.4 times higher.
- Spyware: 1.3 times higher, or third among regions by the percentage of ICS computers on which this threat was blocked.
- Ransomware: 1.8 times higher (third globally).
- Worms: 1.1 times higher.

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

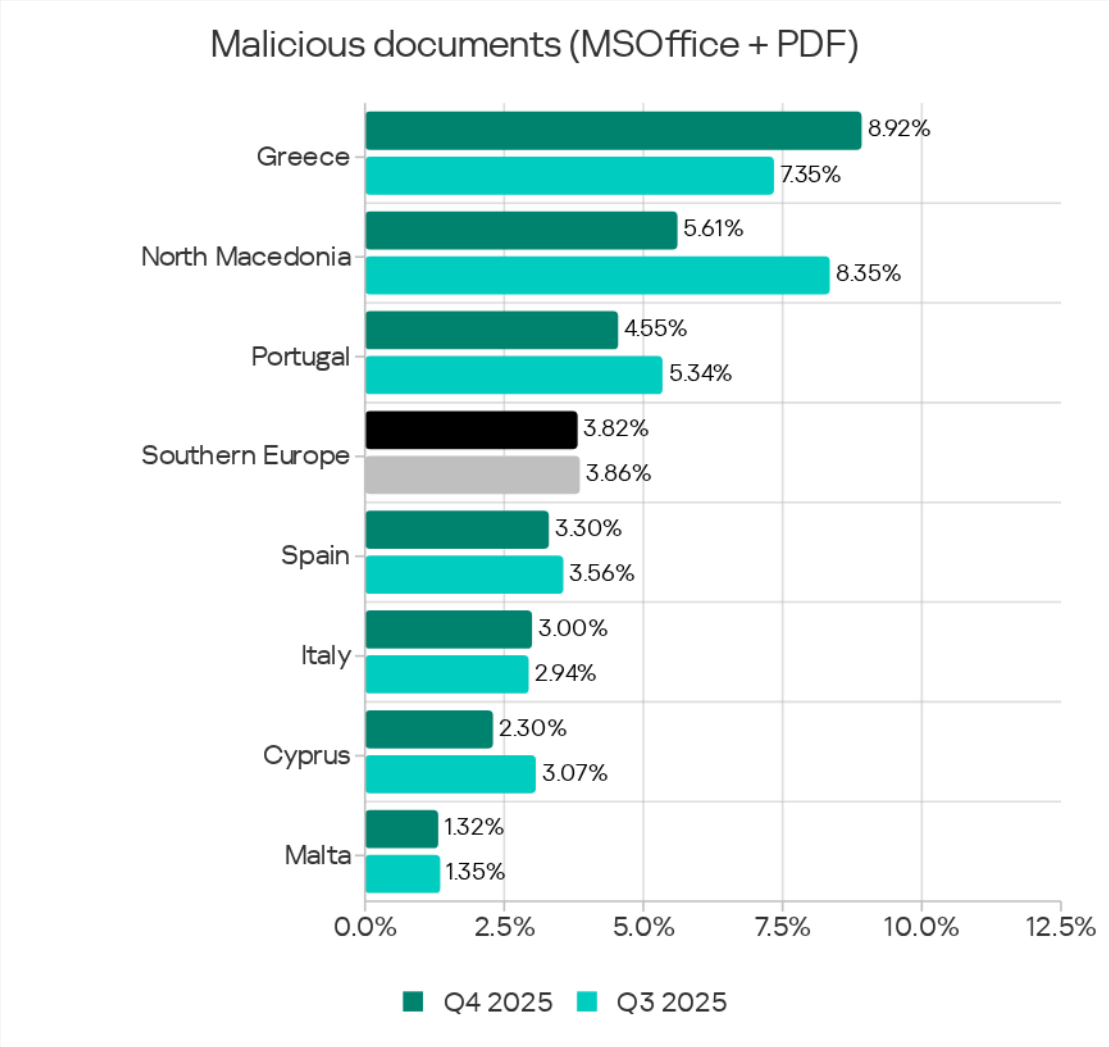
## Malicious documents

Southern Europe ranked first among regions by the percentage of ICS computers on which malicious documents were blocked, at 3.82%. This figure was 8.3 times above that for Northern Europe, which had the lowest percentage among all regions.

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



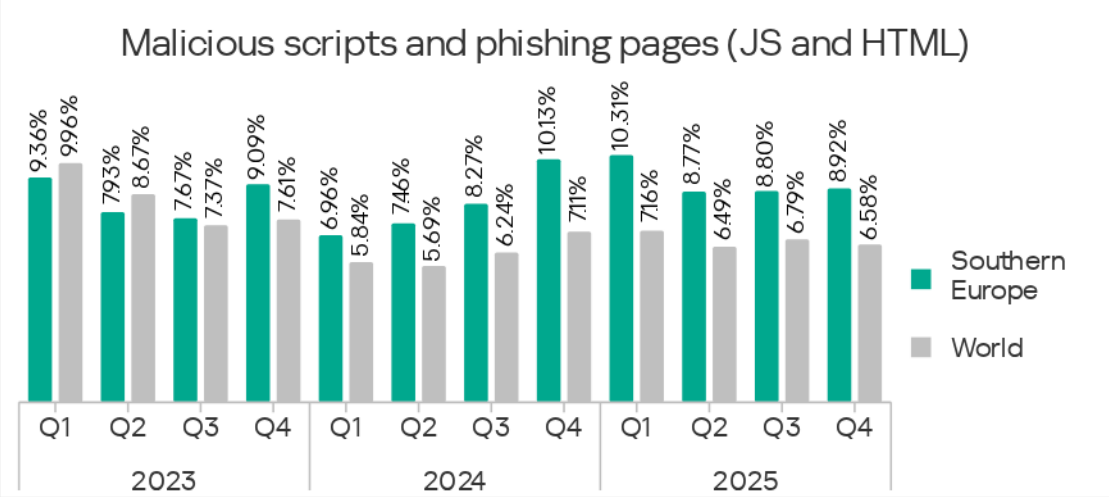

Among the region's countries, Greece led by the percentage of ICS computers on which malicious documents were blocked, at 8.92%.



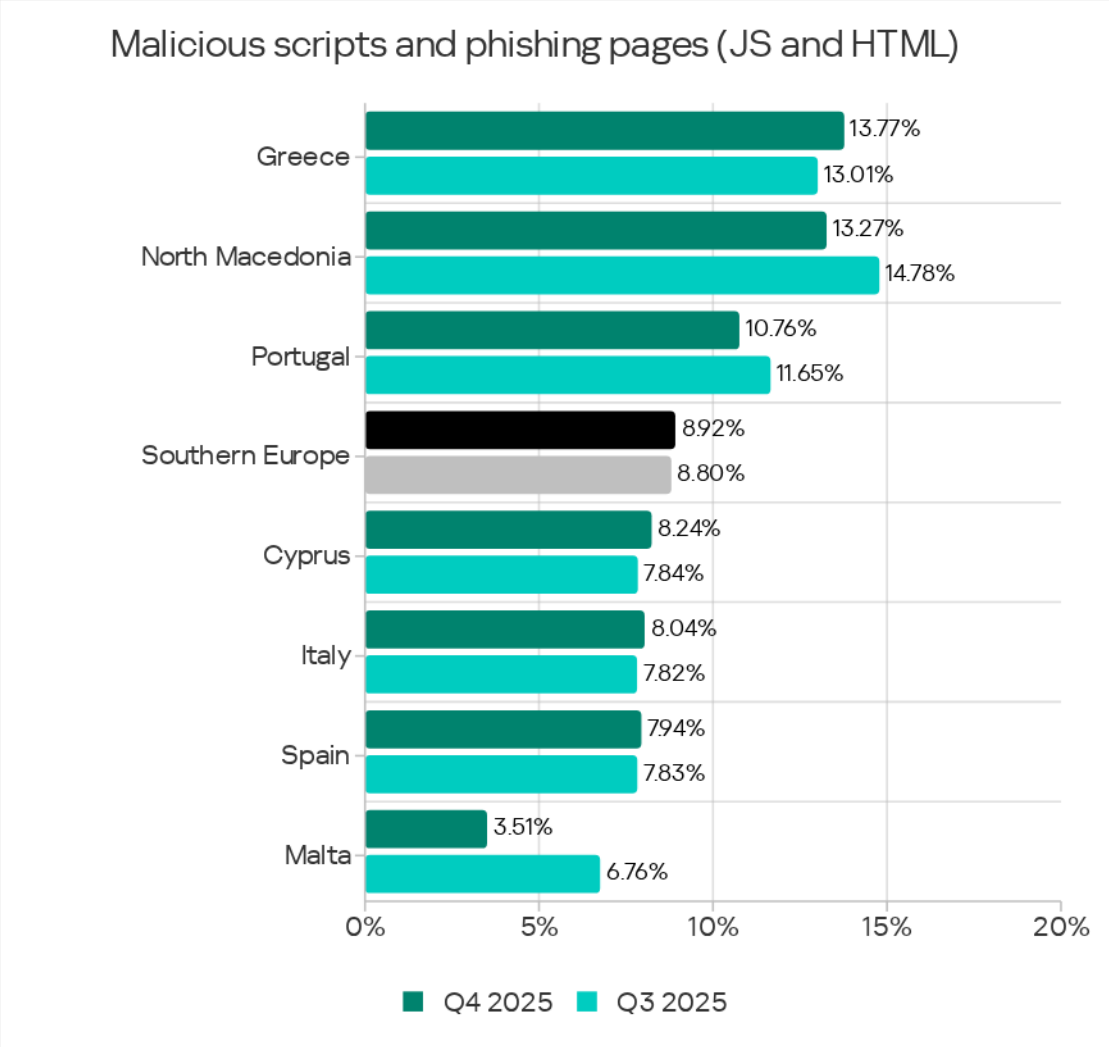

Malicious documents were distributed primarily via email.

## Malicious scripts and phishing pages

In terms of the percentage of ICS computers on which malicious scripts and phishing pages were blocked, Southern Europe ranked fourth, at 8.92%. This was 3.5 times above Northern Europe, which had the lowest figure.




Among the region's countries, Greece led by the percentage of ICS computers on which malicious scripts and phishing pages were blocked, at 13.77%.

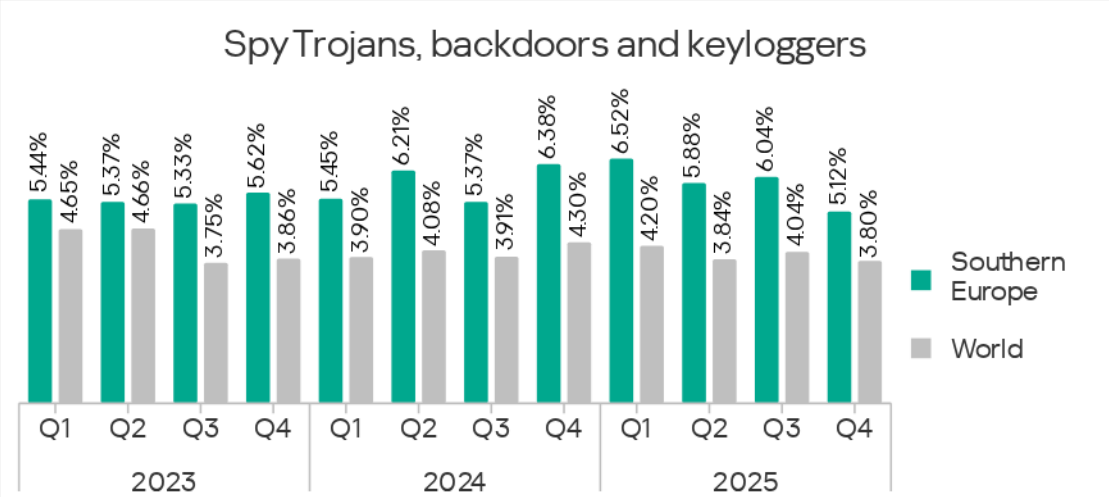



Malicious scripts and phishing pages spread both via the internet and through email.

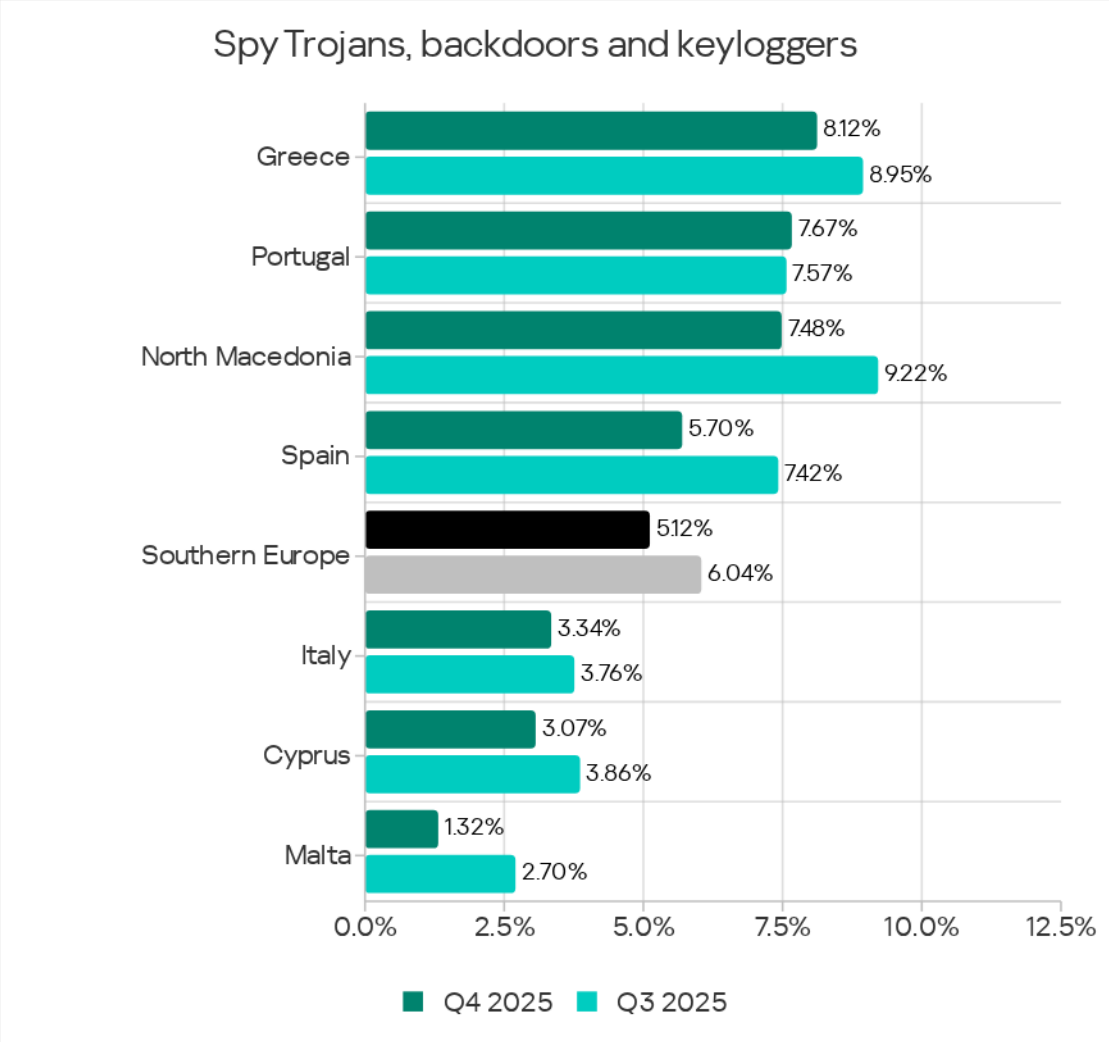
## Spyware

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

The percentage of ICS computers in Southern Europe where spyware was blocked fluctuates over time. In Q4 2025, it dropped to 5.12%. This was a three-year low for the region, but it was still 4.1 times above the figure for Northern Europe, which was last among regions.




Among the region's countries, Greece led by the percentage of ICS computers on which spyware was blocked, at 8.12%.



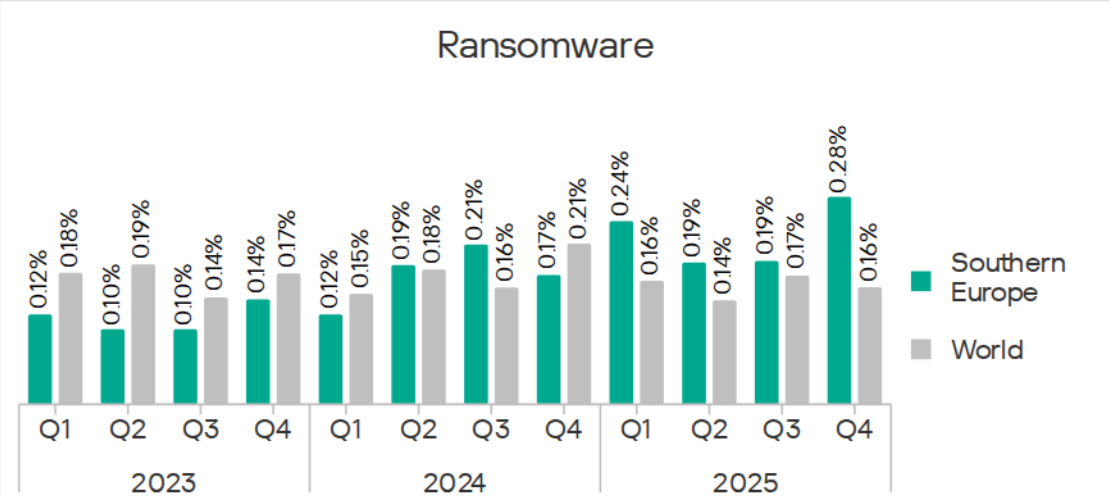
The main source of spyware in the region is email, though it is also encountered on the internet. You may recall that Southern Europe led the global ranking in the percentage of ICS computers on which threats from email clients were blocked.

## Ransomware

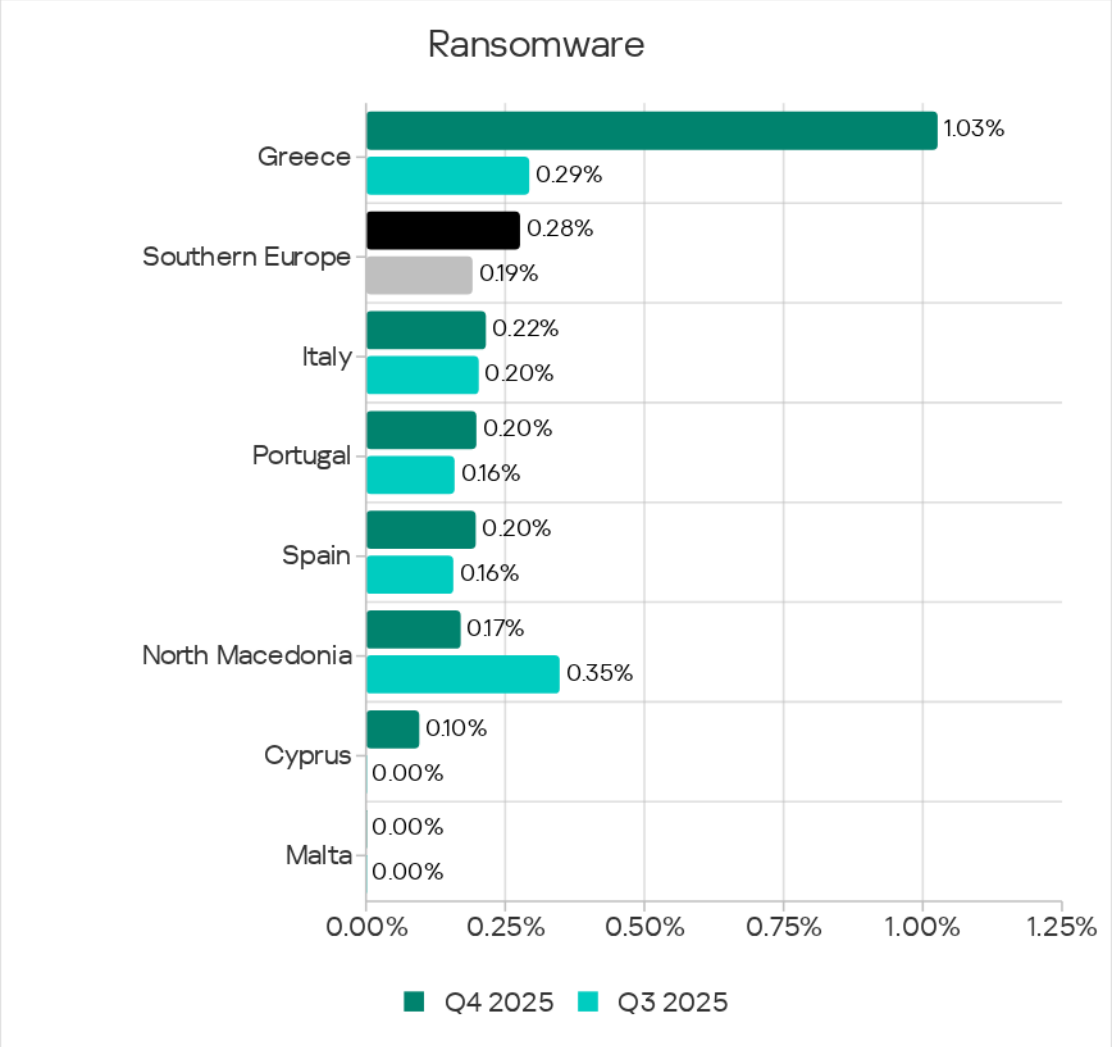
In terms of the percentage of ICS computers on which ransomware was blocked, Southern Europe rose from fifth to third place globally.

At 0.28%, the region's figure was 5.6 times above that for Northern Europe, which ranked last.

The percentage of ICS computers on which ransomware was blocked fluctuates in the region. It grew by a factor of 1.47 in Q4 2025; Southern Europe led all other regions in terms of the growth for this metric.




Among the region's countries, Greece, at 1.03%, led by a wide margin in terms of the percentage of ICS computers on which ransomware was blocked. In this country, the figure for the quarter increased by a factor of 3.6.

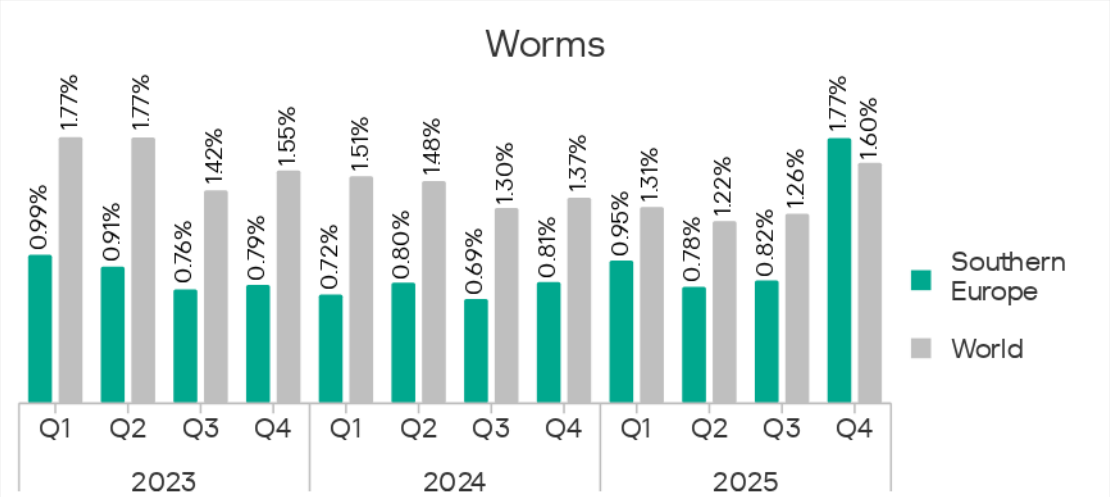



## Worms

In terms of the percentage of ICS computers on which worms were blocked, Southern Europe ranked sixth globally at 1.77%. This was 5.5 times above the figure for Northern Europe, which ranked last.

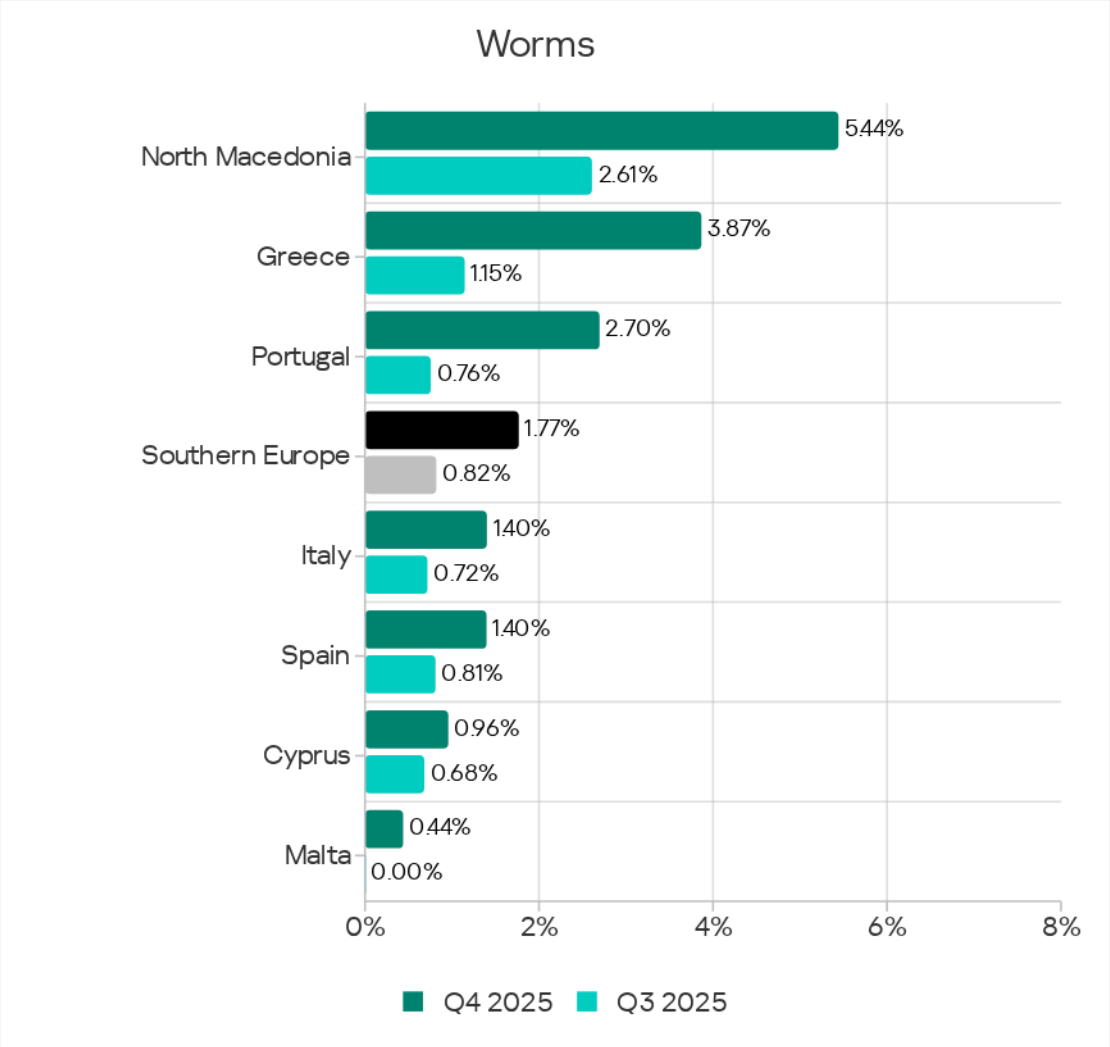
In Q4 2025, the worm metric grew across all regions due to the latest wave of phishing campaigns known as Curriculum-vitae-catalina which we described earlier.

In Southern Europe, the percentage of ICS computers on which worms were blocked increased by a factor of 2.16. As a result, the region was the leader in terms of worms.




The figure for worms increased across all surveyed industries in the region, but most of all in the building automation industry (by a factor of 2.96) and the construction industry (by a factor of 2.60).

The percentage of ICS computers on which worms were blocked during the quarter grew significantly across all countries in the region. North Macedonia led with 5.44%.

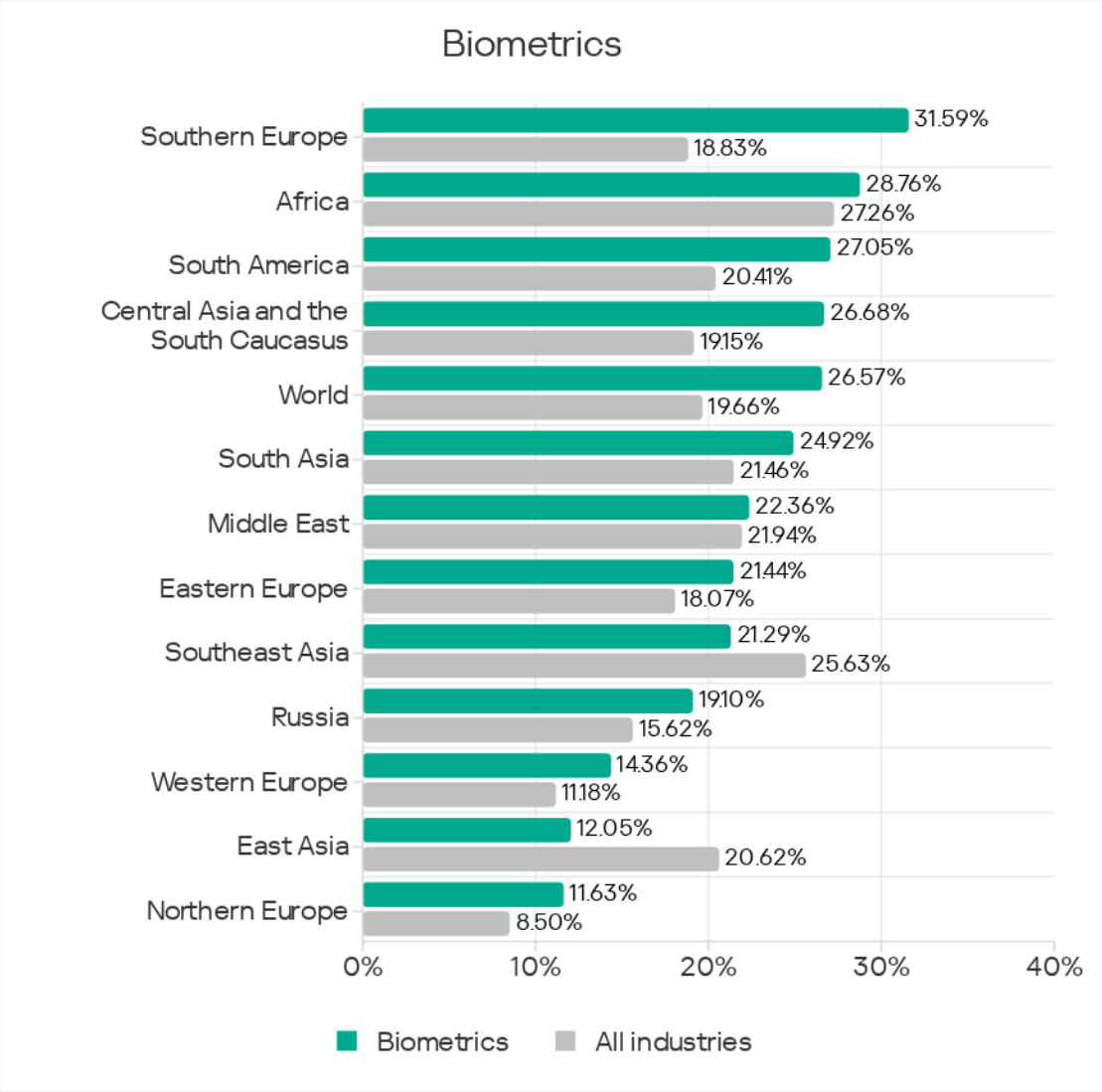



In Q4 2025, worms were spread over email during a phishing attack.

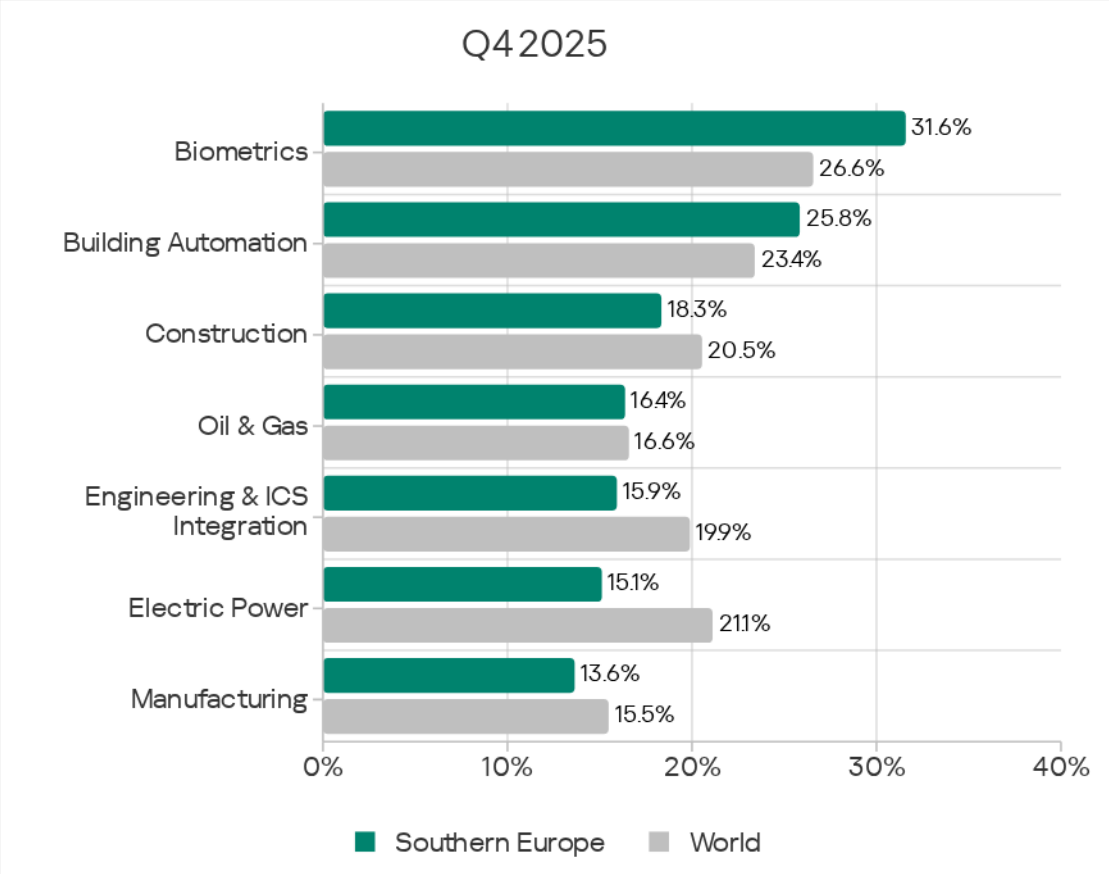
## Industries

In Southern Europe, of all the industries surveyed for the report, malicious objects were most often blocked in biometrics.

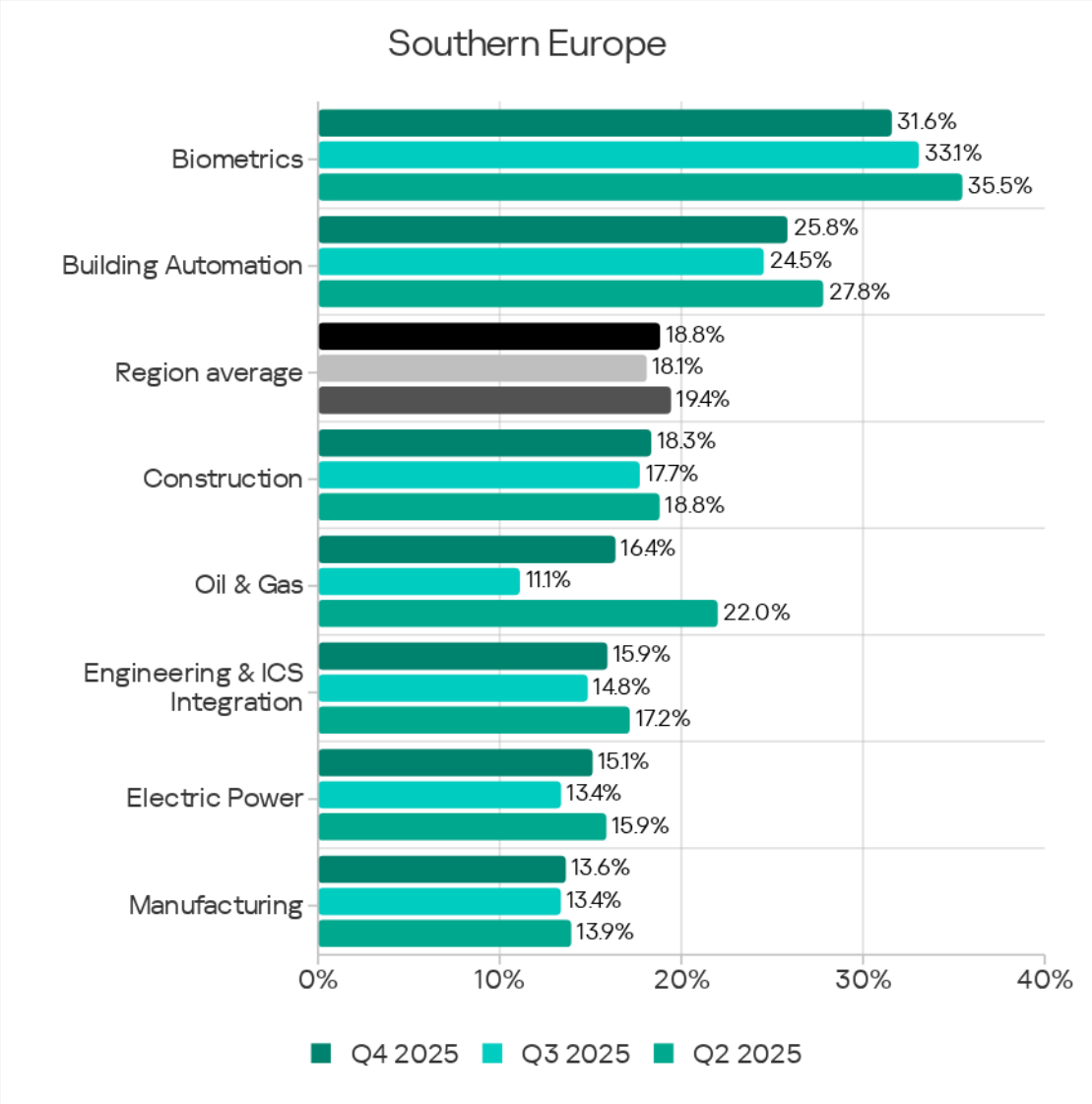
Southern Europe led among regions in terms of biometrics.



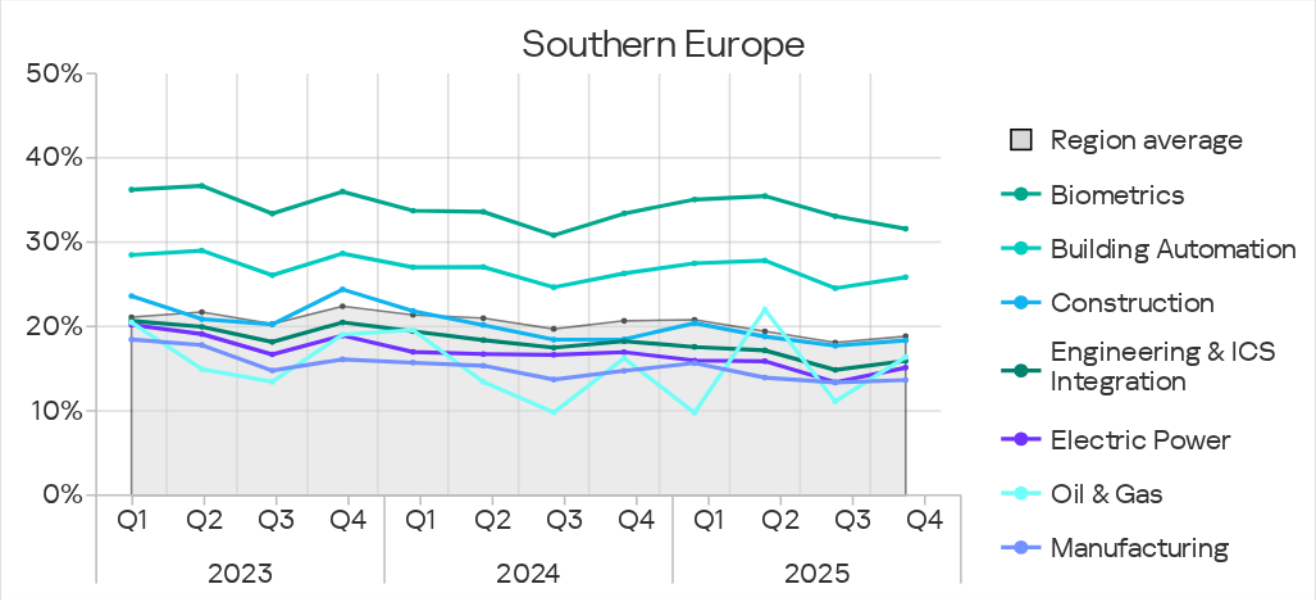

In Southern Europe, the percentage of ICS computers on which malicious objects were blocked was above the global average in biometrics (by a factor of 1.2) and in the building automation industry (by a factor of 1.1).




In Q4 2025, the percentage of ICS computers on which malicious objects were blocked increased across all of the surveyed industries except for biometrics.




The observed changes in the percentage of ICS computers on which malicious objects were blocked across all of the surveyed industries exhibited a tendency to fluctuate. The figures for biometrics and building automation significantly exceeded 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. Red signifies that the figure is close to the maximum.

**Threat source figures for industries in Southern Europe, Q4 2025**

| Industry / Threat source | Biometrics | Building Automation | Engineering & ICS Integration | Electric Power | Construction | Manufacturing | Category metric in region |
|---|---|---|---|---|---|---|---|
| Internet | 8.41% | 8.62% | 7.79% | 7.72% | 8.51% | 5.48% | 8.00% |
| Email clients | 17.97% | 12.52% | 3.89% | 2.70% | 5.22% | 2.79% | 6.34% |
| Removable media | 0.06% | 0.09% | 0.10% | 0.15% | 0.05% | 0.17% | 0.10% |
| Network folders | — | 0.02% | 0.01% | 0.02% | 0.11% | — | 0.02% |
| **Industry metric in region** | 31.59% | 25.84% | 15.93% | 15.12% | 18.34% | 13.64% | |

**Threat category figures for industries in Southern Europe, Q4 2025**

| Industry / Threat type | Biometrics | Building Automation | Engineering & ICS Integration | Electric Power | Construction | Manufacturing | Category metric in region |
|---|---|---|---|---|---|---|---|
| Denylisted internet resources | 2.95% | 2.95% | 2.36% | 2.76% | 2.91% | 1.83% | 2.61% |
| Malicious scripts and phishing pages (JS and HTML) | 17.17% | 14.31% | 6.95% | 5.91% | 7.80% | 5.20% | 8.92% |
| Malicious documents (MSOffice + PDF) | 9.99% | 8.08% | 2.18% | 1.72% | 2.42% | 1.86% | 3.82% |
| Spy Trojans, backdoors and keyloggers | 15.06% | 9.43% | 3.18% | 2.50% | 3.90% | 3.38% | 5.12% |
| Ransomware | 0.39% | 0.61% | 0.18% | 0.11% | 0.11% | 0.14% | 0.28% |
| Miners in the form of executable files for Windows | 0.22% | 0.17% | 0.17% | 0.18% | 0.33% | 0.03% | 0.17% |
| Web miners running in browsers | 0.16% | 0.12% | 0.13% | 0.15% | 0.27% | — | 0.13% |
| Malware for AutoCAD | 0.02% | 0.02% | 0.05% | 0.04% | 0.27% | 0.03% | 0.05% |
| Worms | 3.97% | 3.75% | 1.03% | 1.15% | 1.15% | 1.52% | 1.77% |
| Viruses | 0.53% | 0.34% | 0.21% | 0.24% | 0.60% | 0.21% | 0.28% |
| **Industry metric in region** | 31.59% | 25.84% | 15.93% | 15.12% | 18.34% | 13.64% | |

## Characteristics of the region

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

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

- First in biometrics, building automation, construction, and engineering and ICS integrators industry.

- Third in the manufacturing industry.
- Fourth place in the electrical energy industry.

The high figures for threats spread by email clients (phishing) and spyware clearly pointed to a significant exposure of the region's OT systems to advanced attackers.

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

In terms of the percentage of ICS computers on which malicious documents were blocked across various industries, Southern Europe ranked as follows:

- First in biometrics, building automation, and the engineering and ICS integrators industry.
- Second in the construction industry.
- Third in the manufacturing industry.

In terms of the percentage of ICS computers on which spyware was blocked across various industries, Southern Europe ranked as follows:

- First in biometrics and building automation.
- Fourth in the construction industry and manufacturing industry.

Southern Europe ranked third among regions in terms of the percentage of ICS computers on which ransomware was blocked. Southern Europe ranked as follows for this figure across various industries:

- First in the building automation industry.
- Third in the engineering and ICS integrators industry.

**Biometrics**

Southern Europe ranked first among regions in the percentage of ICS computers on which malicious objects were blocked in biometrics.

Based on indicators for biometrics among regions, Southern Europe had the following rankings:

- First by percentage of ICS computers on which threats from email clients were blocked.
- Third for internet threats.

- First for the percentage of ICS computers on which malicious documents, malicious scripts and phishing pages, and spyware were blocked.
- Second for worms.

The regional industry rankings for biometrics was as follows:

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

**Building automation**

Southern Europe was third among regions in terms of the percentage of ICS computers on which malicious objects were blocked in the building automation industry.

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

- First by percentage of ICS computers on which threats from email clients were blocked.
- Third for internet threats.
- First by the percentage of ICS computers on which the following categories of threats were blocked: malicious documents, malicious scripts and phishing pages, spyware, ransomware, and worms.

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

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

### Construction

Southern Europe was 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 had the following rankings:

- First by percentage of ICS computers on which threats from email clients were blocked.
- Third by the metric for network folders.
- Second place in the percentage of ICS computers on which malicious documents were blocked.

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

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

### Engineering and ICS integrators

Southern Europe was 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 had the following rankings:

- First by percentage of ICS computers on which threats from email clients were blocked.
- First in the percentage of ICS computers on which malicious documents were blocked.
- Third place in ransomware.

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

- Third by the percentage of ICS computers on which threats from removable media were blocked.
- Second in terms of malware for AutoCAD.

- Third place in ransomware.

**Electric power**

Southern Europe was 10th 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 ranked:

- Second in the percentage of ICS computers on which threats from removable media are blocked.
- Third by the metric for network folders.
- Third in both categories of miners and malware for AutoCAD.

**Manufacturing**

Southern Europe was seventh among regions by the percentage of ICS computers on which malicious objects were blocked in the manufacturing industry.

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

- Third by 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.

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

- First by the percentage of ICS computers on which threats were blocked when connecting removable media.
- Third by the percentage of ICS computers on which worms were blocked.

# Eastern Europe

## Key cybersecurity issues in the region

Eastern Europe ranked ninth globally by the percentage of ICS computers on which malicious objects were blocked. Eastern Europe ranked second for this metric among the European regions.

Eastern Europe had high rankings among all regions in the following threat categories:

- Third in malicious documents.
- Third in miners in the form of executable files for Windows.
- Fourth for worms.
- Fifth in denylisted internet resources.
- Sixth for spyware.
- Sixth in web miners.

Among the threat sources, email clients ranked the highest at sixth place.

**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 was 1.3 times higher than the global average.

The percentage of ICS computers on which malicious documents were blocked exceeded the global average by 1.5 times. Based on the metric for malicious documents, Eastern Europe came third among all the regions. This was the region's highest position in the rankings, both by source and by threat category.

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.

Based on the metrics for malicious documents in the building automation industry, Eastern Europe was second in the corresponding regional rankings, while it ranked third in the engineering and ICS integrators industry.

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 Q4 2025, the percentage of ICS computers on which malicious scripts and phishing pages were blocked was slightly below the global average.

**High rate of spyware**

The percentage of ICS computers on which spyware was blocked in Eastern Europe was relatively stable, slightly higher than the global average in Q4 2025. 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.

Based on the percentage of ICS computers on which spyware was blocked in the building automation industry, Eastern Europe ranked fourth globally.

**High figure for miners in the form of executable files for Windows**

In Q4 2025, Eastern Europe ranked third among regions based on the percentage of ICS computers on which miners in the form of executable files for Windows were blocked.

In Eastern Europe, miners in the form of executable files for Windows actively use modules and components that are essentially worms and deliver the miner to other computers in the network (automated lateral movement).

Eastern Europe ranked third among regions based on the metrics for executable miners in the building automation, construction and electric power industries, and fourth in the engineering and ICS integrators industry.

**Industries**

The threat of targeted attacks in the region is especially relevant for the building automation industry. Eastern Europe ranked second among regions based on the metrics for email client threats and malicious documents in this industry, and fourth for spyware.

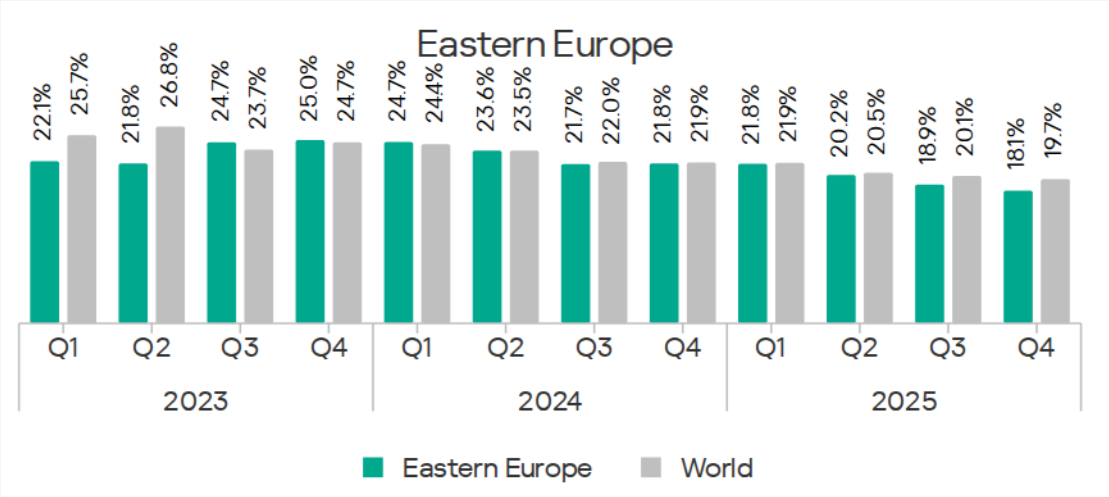
Among industries located in Eastern Europe, the building automation industry led in terms of the metrics for all threat sources, and for malicious scripts, malicious documents, and spyware.

Note the high figure for ransomware in the manufacturing industry. Based on the metric for ransomware in the manufacturing industry, Eastern Europe ranked third among all regions. Manufacturing topped the regional rankings of industries in terms of this metric.

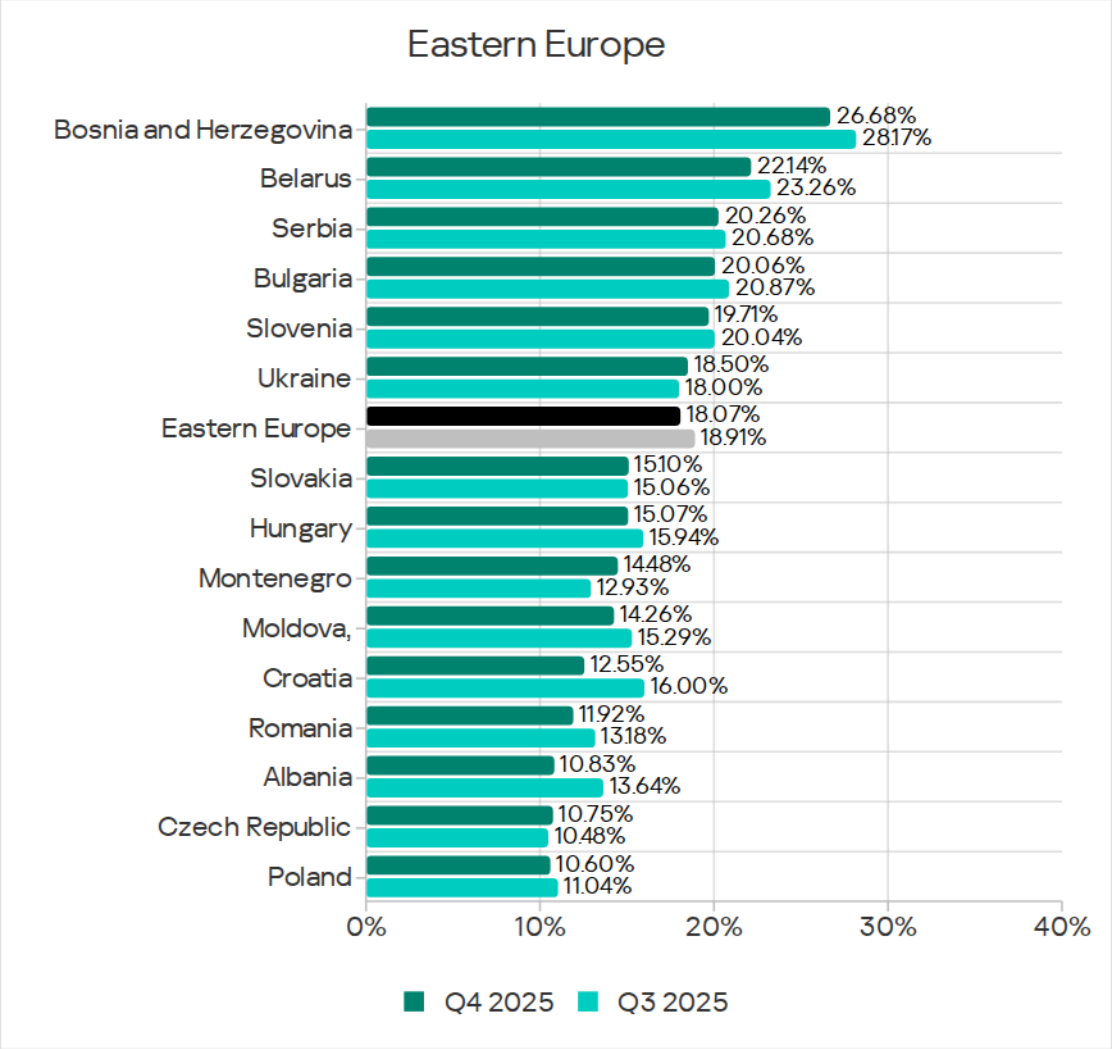
## Statistics across all threats

In Q4 2025, Eastern Europe ranked ninth globally in the percentage of ICS computers on which malicious objects were blocked.

The indicator in the region decreased to 18.1%, the lowest value for three years. It was slightly lower than the global average and 2.1 times higher than in Northern Europe, which had the lowest rate among all regions.



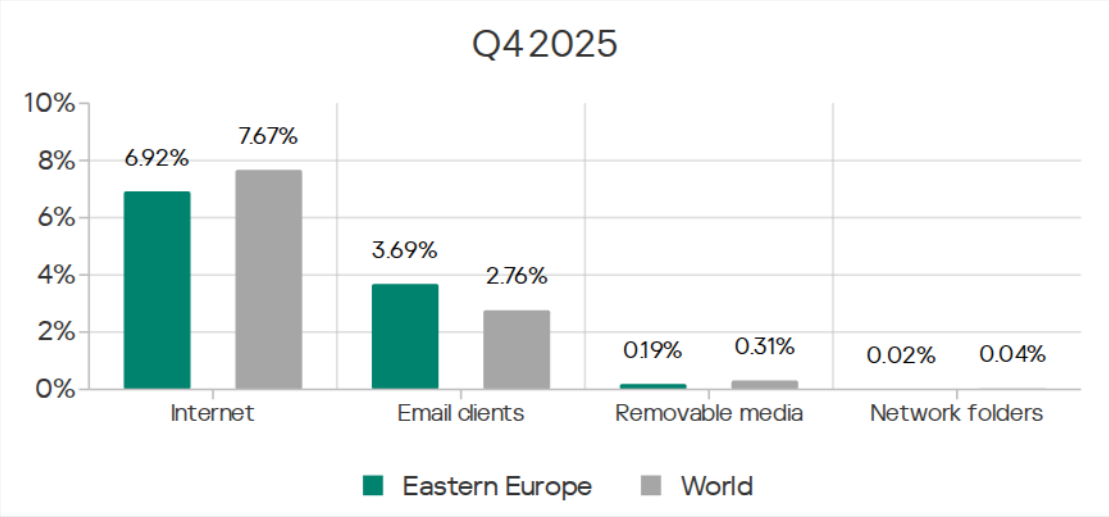

Among the region's countries, Bosnia and Herzegovina led in this metric with 26.68%. The lowest figure was in Poland – 10.60%. Over the quarter, the figure grew only in Ukraine, Montenegro, and Czechia.



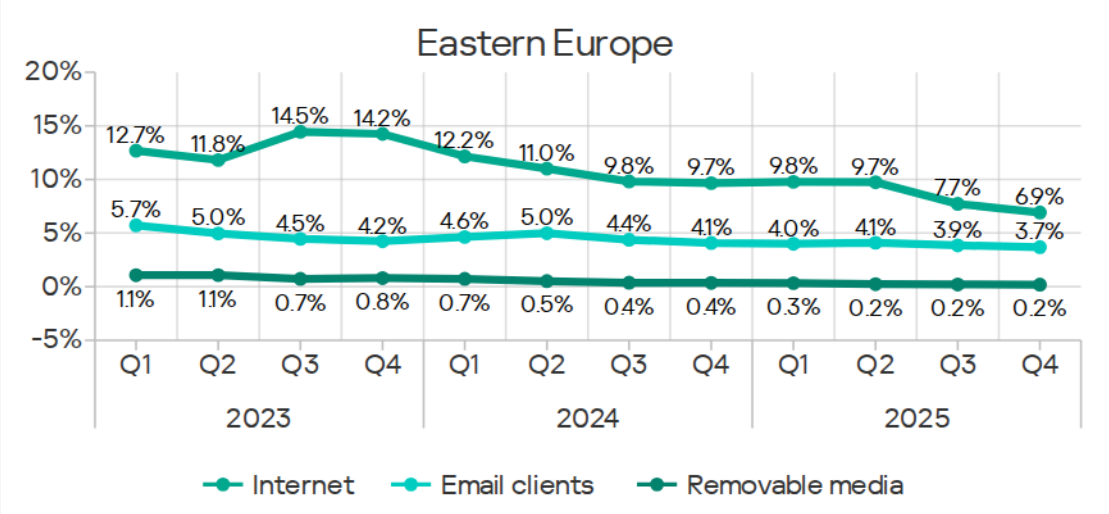

## Threat sources

With the exception of email clients, all threat source rates in Eastern Europe were below the global average.

The percentage of ICS computers on which threats from email clients were blocked was 1.3 times higher than the global average.

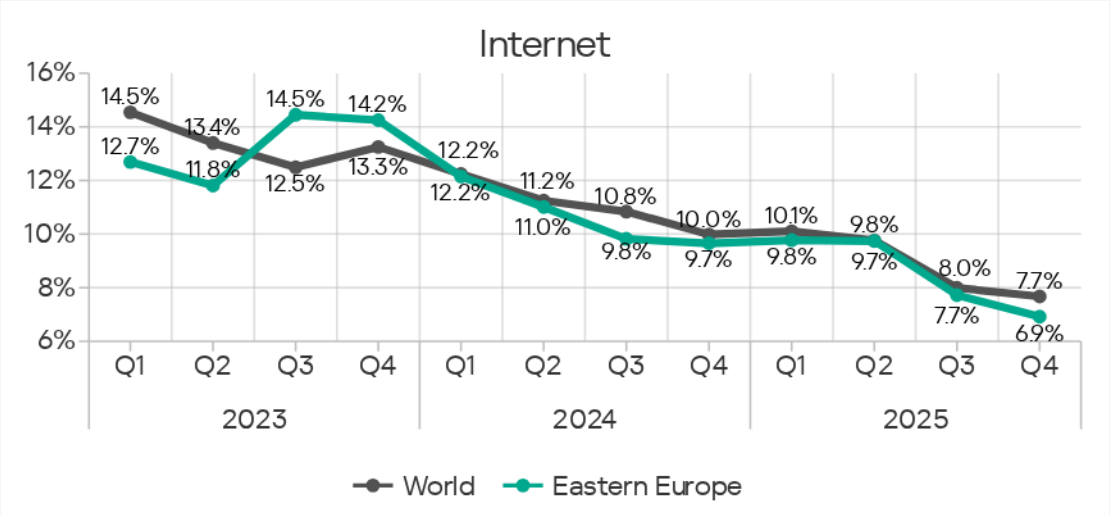



Malicious objects in the region spread primarily via the internet and email. The figures decreased for all threat sources across the region in Q4 2025.

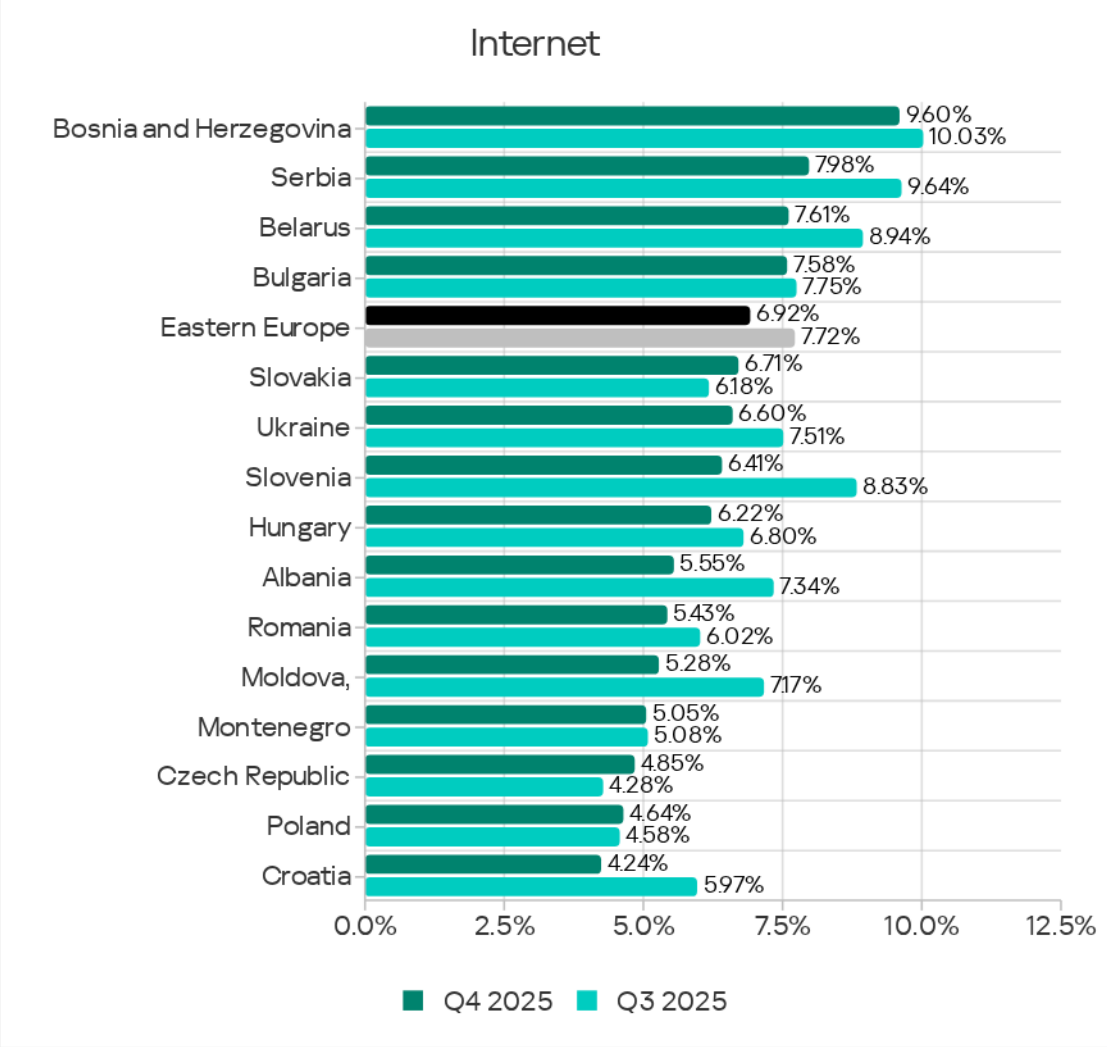



## Internet

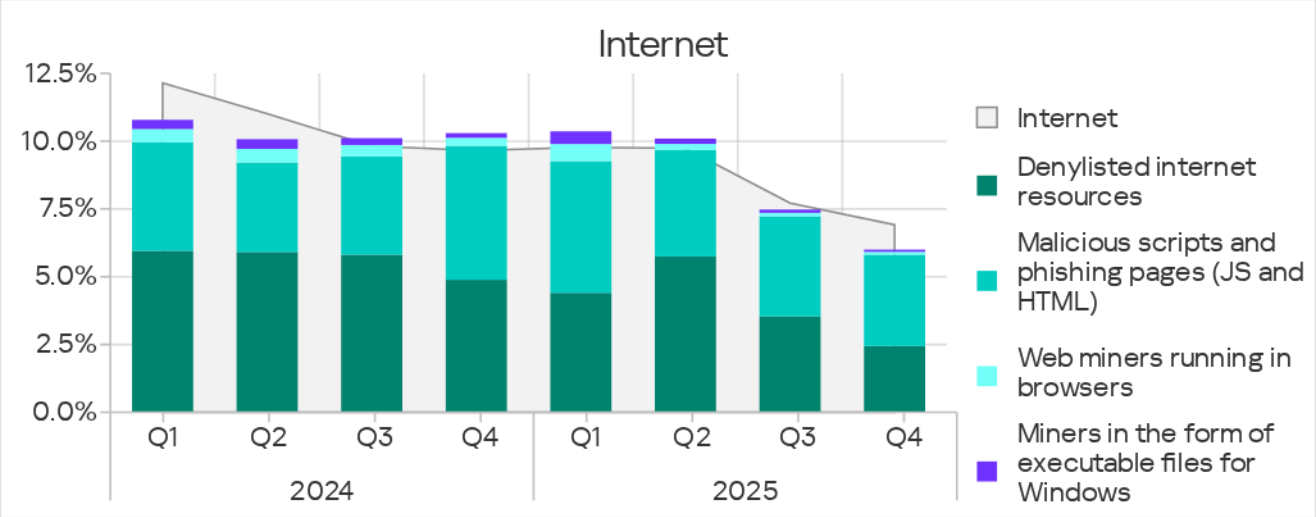
Based on the percentage of ICS computers on which internet threats were blocked, Eastern Europe ranked eighth globally at 6.92%, which was 1.7 times higher than the lowest figure (Northern Europe).




Country-level rates ranged from 4.24% in Croatia to 9.60% in Bosnia and Herzegovina.



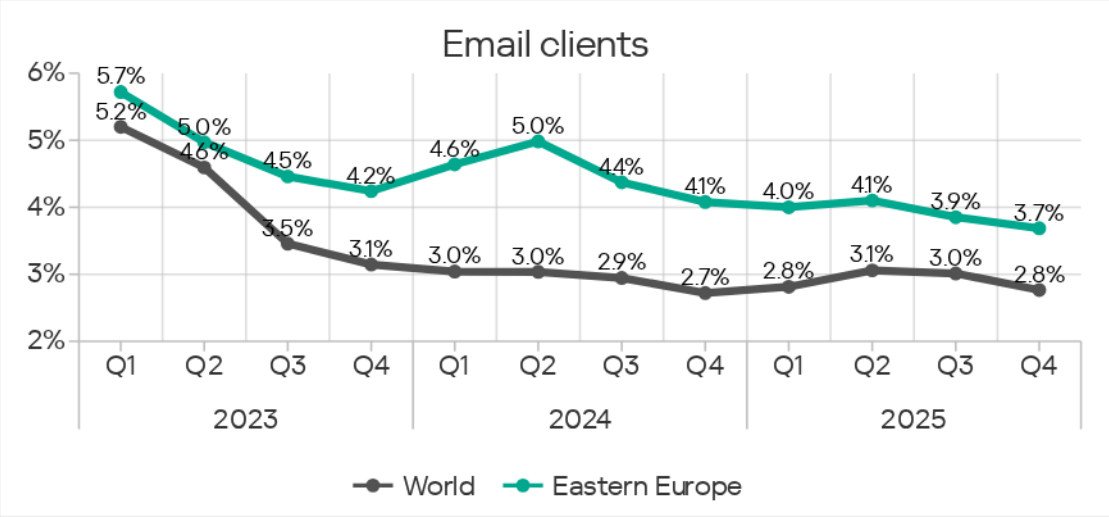
The main categories of internet threats that were blocked on ICS computers in the region included malicious scripts and phishing pages, as well as denylisted internet resources.



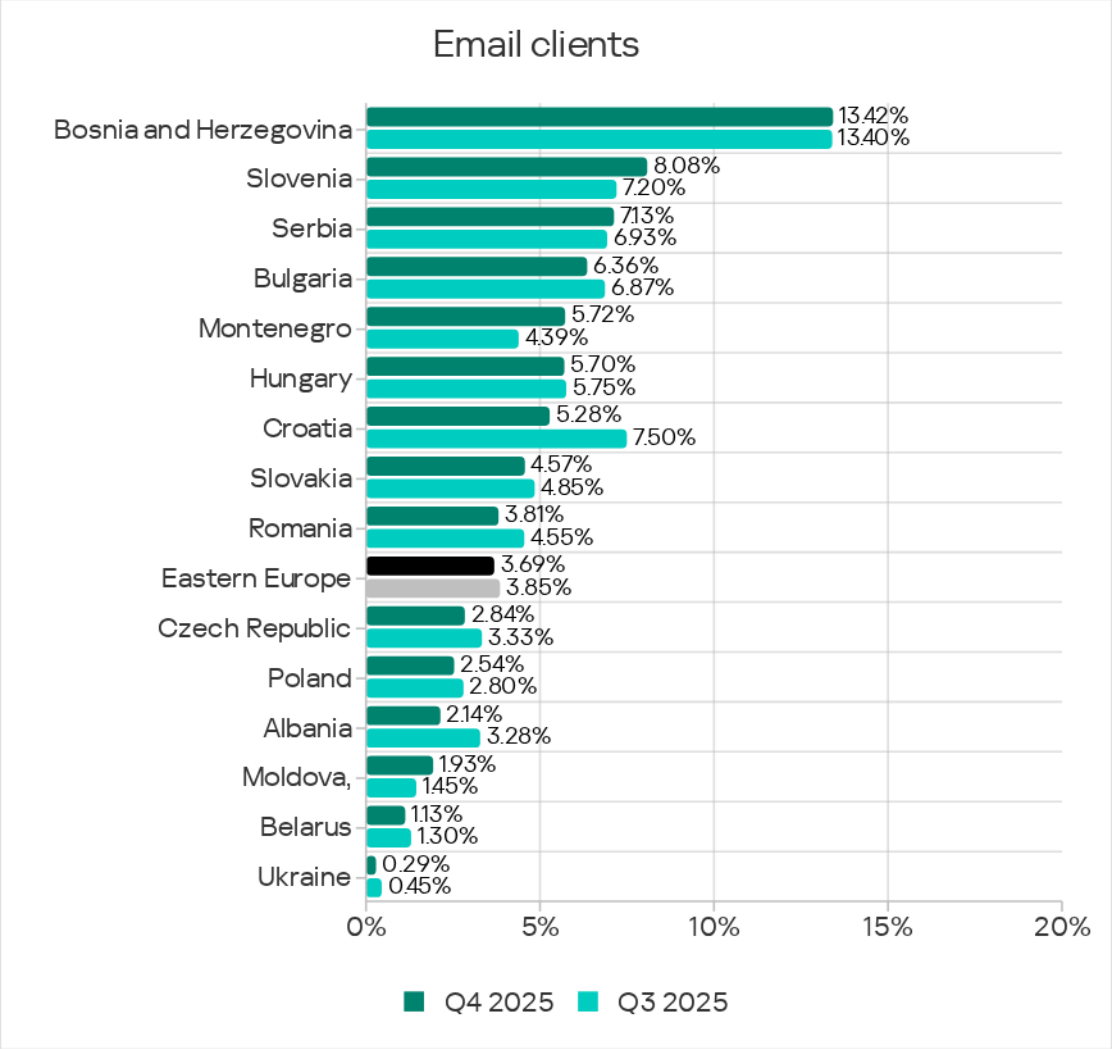

Based on the indicator for denylisted internet resources, Eastern Europe ranked fifth in the corresponding ranking of regions.

## Email clients

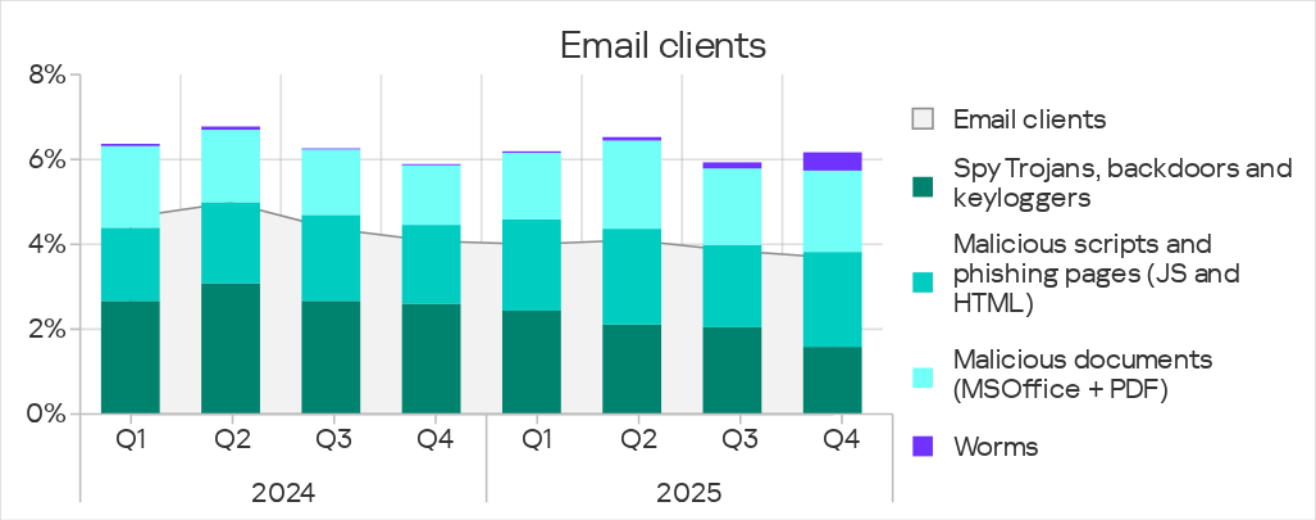
By percentage of ICS computers on which threats from email clients were blocked, Eastern Europe ranked sixth globally in Q4 2025, at 3.69%. This was 5.8 times higher than in Northern Europe, which ranked last.




Among countries in the region, Bosnia and Herzegovina (13.42%) led all other countries by a wide margin in the percentage of ICS computers on which threats from email clients were blocked. The lowest figure observed was in Ukraine at 0.29%.




The main categories of mail client threats that were blocked on ICS computers in the region were malicious scripts and phishing pages, malicious documents, and spyware.



Q4 2025 saw a noticeable increase in the percentage of ICS computers on which worms from email clients were blocked. This was connected with the latest wave of phishing campaigns known as Curriculum-vitae-catalina, which launched attacks across all regions of the world. In Eastern Europe, these attacks peaked in November.

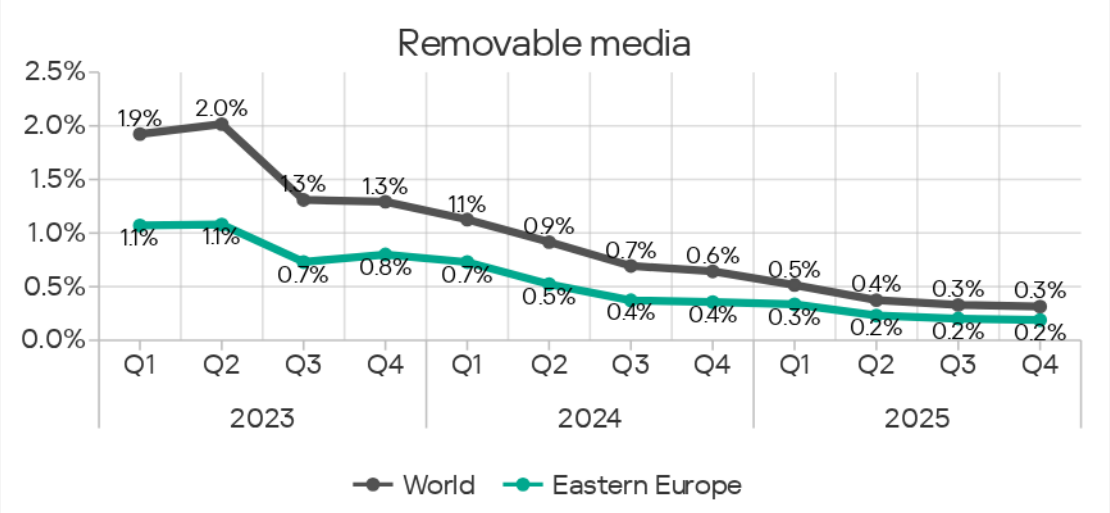
The hackers distributed phishing emails disguised as job applications. Disguised as a resume (Curriculum Vitae), these emails contained a malicious executable file, a remote administration backdoor worm known as Backdoor.MSIL.XWorm. Running that file caused system infection.

Normally, these campaigns are designed to deliver malware for data theft, spyware, or remote administration tools (RATs).

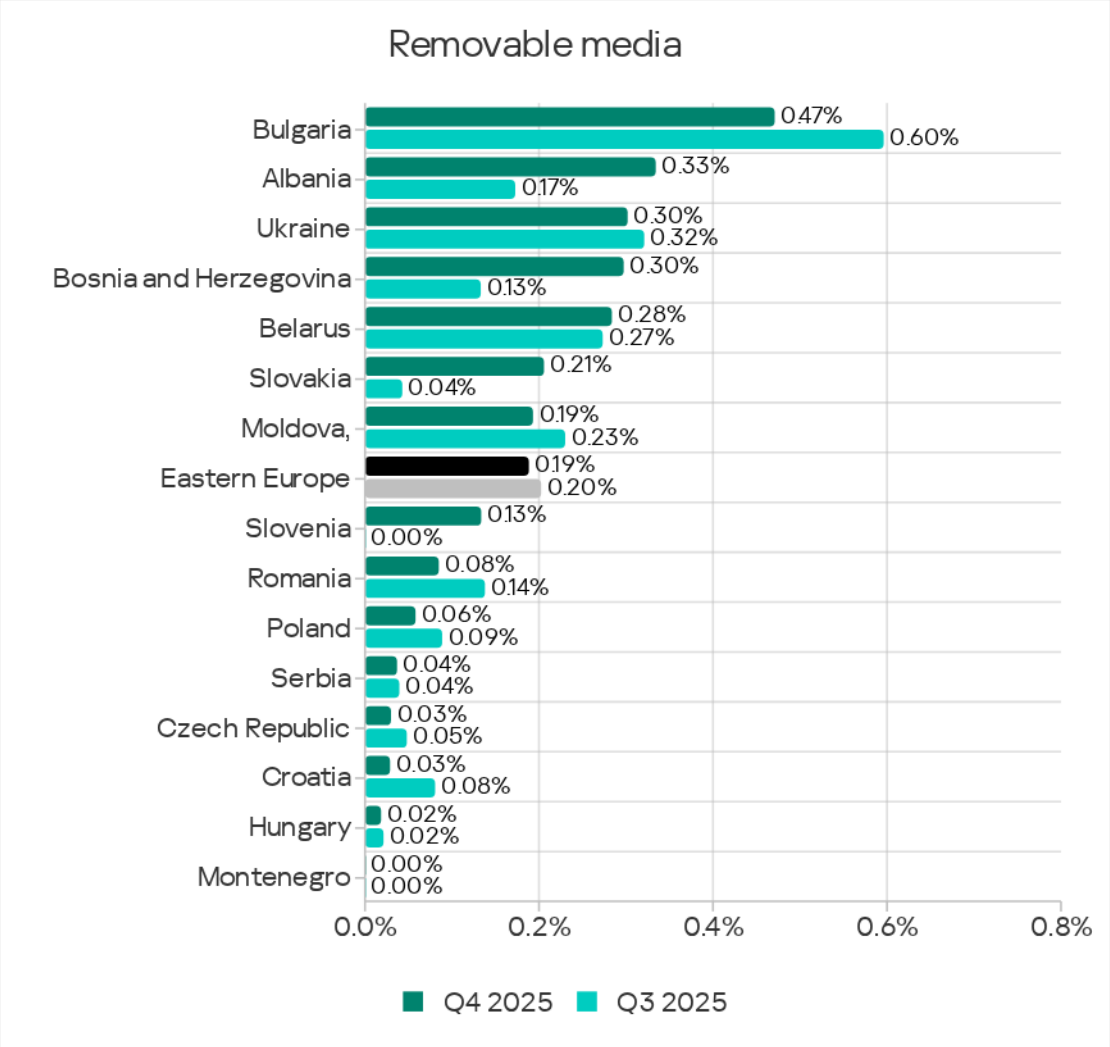
In terms of growth in the worm rate, the region was third.

## Removable media

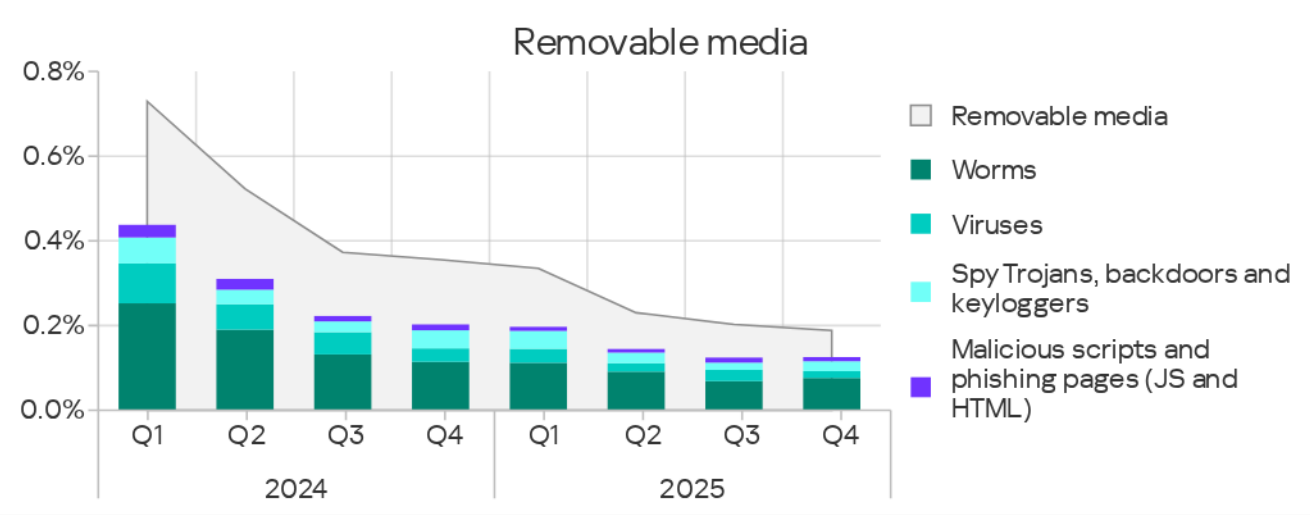
In terms of ICS computers on which threats were blocked when connecting removable media, Eastern Europe ranked seventh globally in Q4 2025, at 0.19%. This was 3.8 times higher than in the Australia and New Zealand region, which ranked last in the corresponding ranking.




Among the countries in the region, Bulgaria led in the percentage of ICS computers on which threats were blocked upon connecting removable media, with 0.47%.



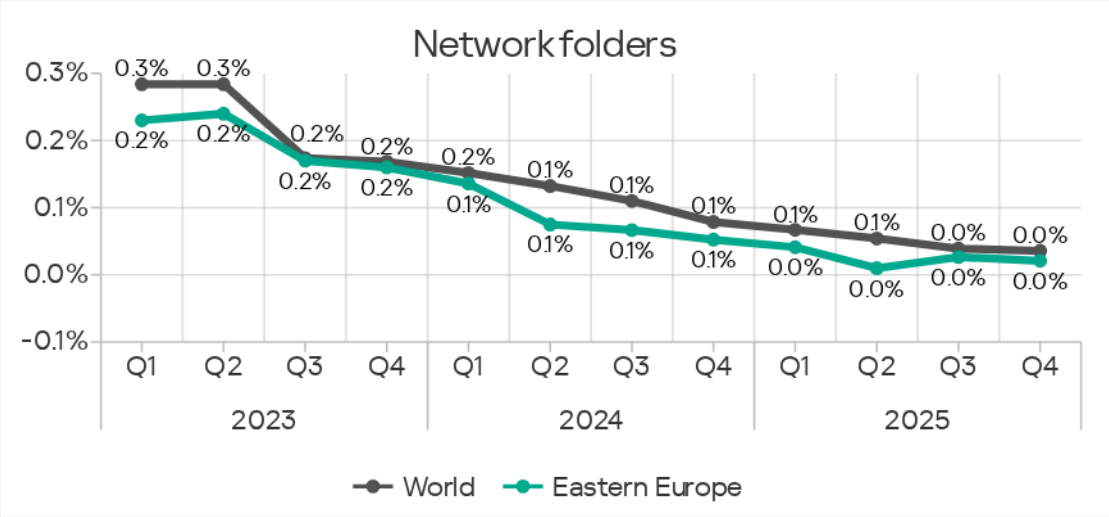

The main categories of removable media threats blocked on ICS computers in the region were worms, spyware, and viruses.



## Network folders

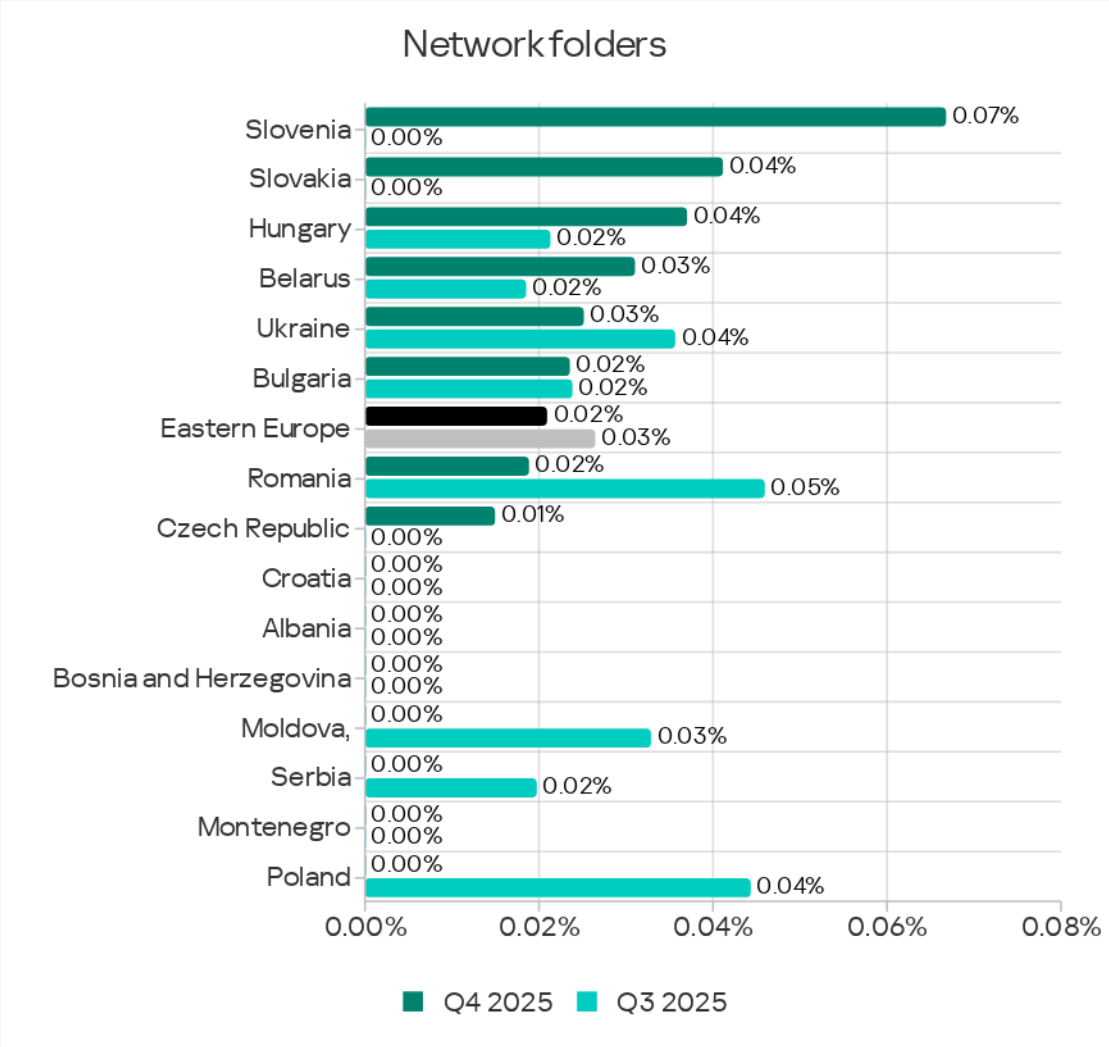
Eastern Europe fell from fifth to eighth place in the rankings of regions in the percentage of ICS computers on which threats from network folders were blocked.

After growing in the previous quarter, the figure for network folders across the region dropped to 0.02%. This was 3.1 times higher than in Northern Europe, which ranked last.



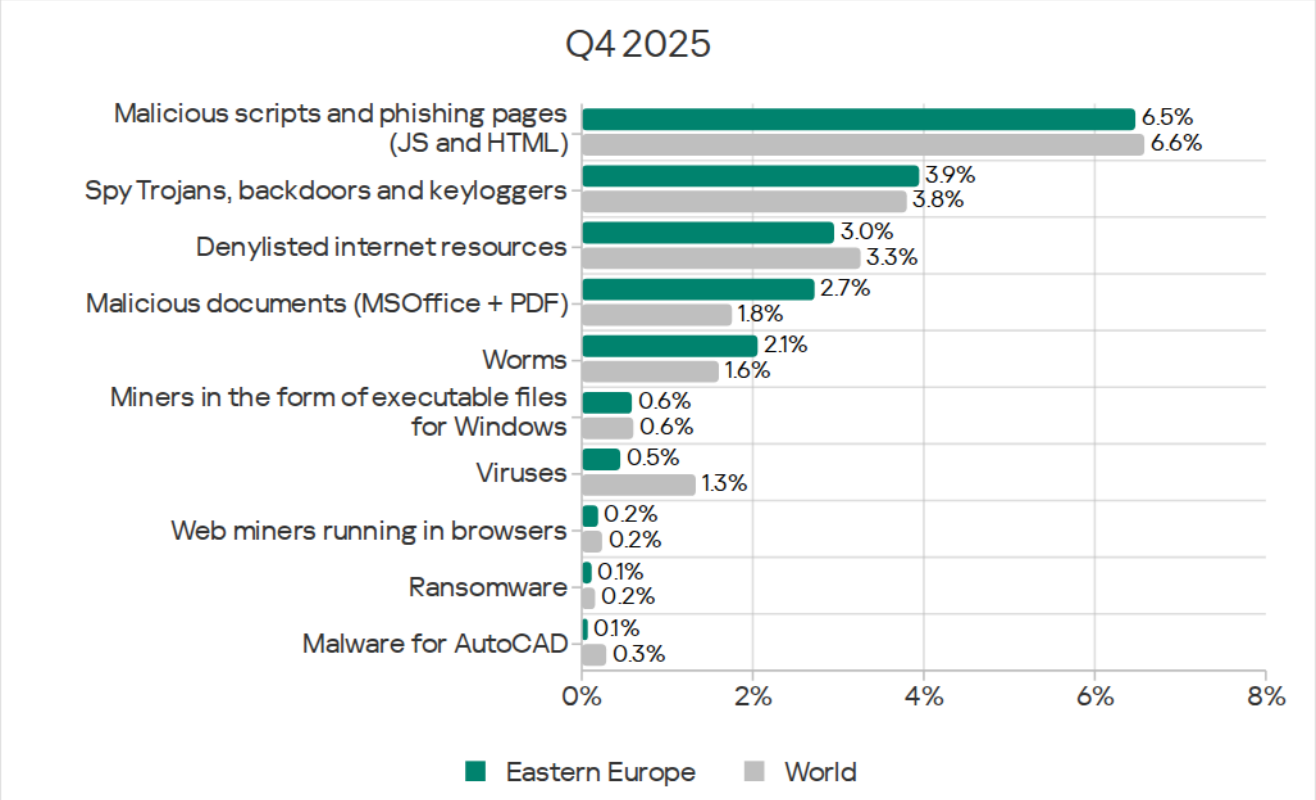

In a protected infrastructure, threats from network folders are encountered fairly rarely and not in all of the region's countries. The same is true for industries. Network folder threats were only detected in two industries: building automation, and engineering and ICS integrators.

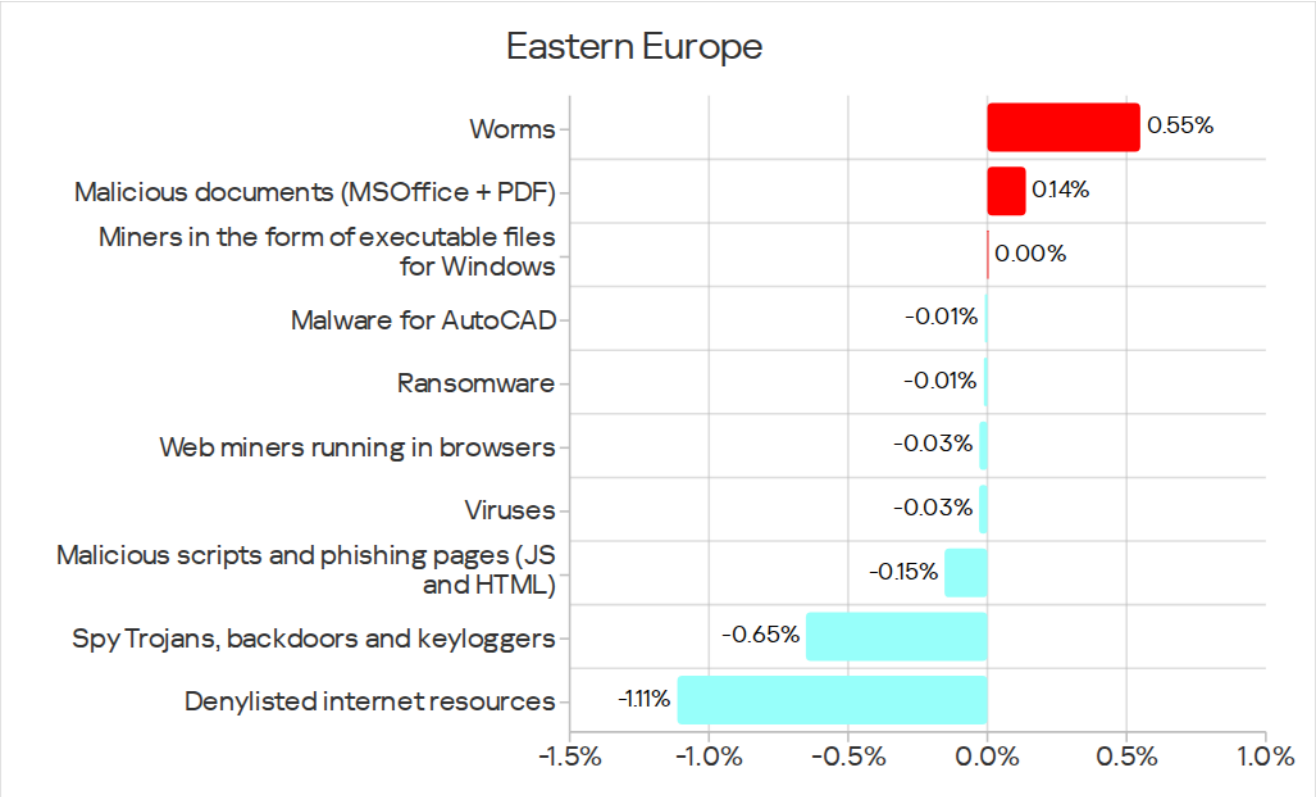
Among countries in the region, Slovenia led in the percentage of ICS computers on which threats from network folders were blocked with a figure of 0.07%.




In Q4 2025, the prevalent type of threat that spread through network folders was worms.

## Threat categories



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

- Malicious documents: 1.5 times higher (third among regions by the percentage of ICS computers on which the threat was blocked).
- Worms: 1.3 times higher (fourth globally).
- Spyware.

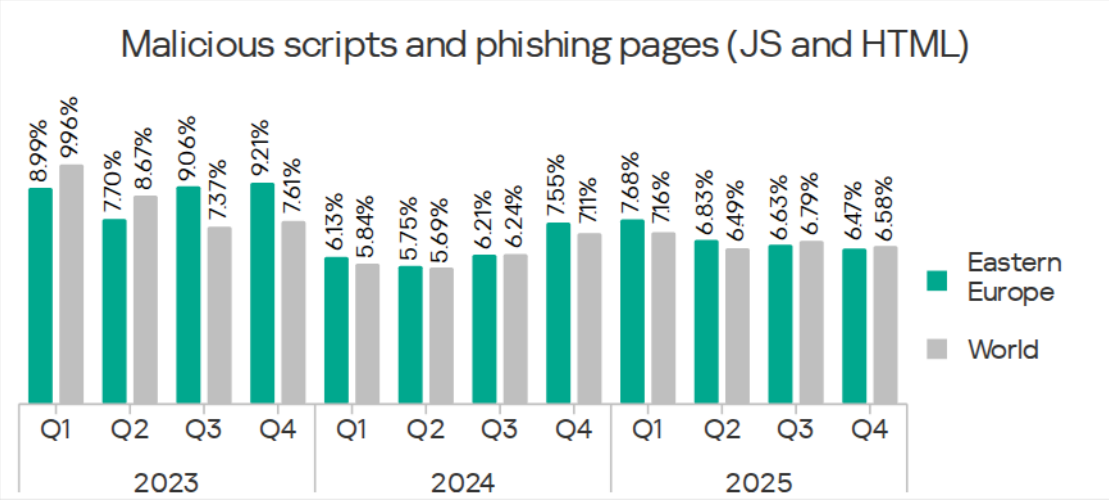
In terms of miners in the form of executable files, Eastern Europe ranked third among regions. The figure for the region was slightly below the global average.

In the region, the figures for all threat categories except worms, malicious documents, and executable miners decreased over the quarter. Eastern Europe led among regions in terms of the growth in malicious documents.

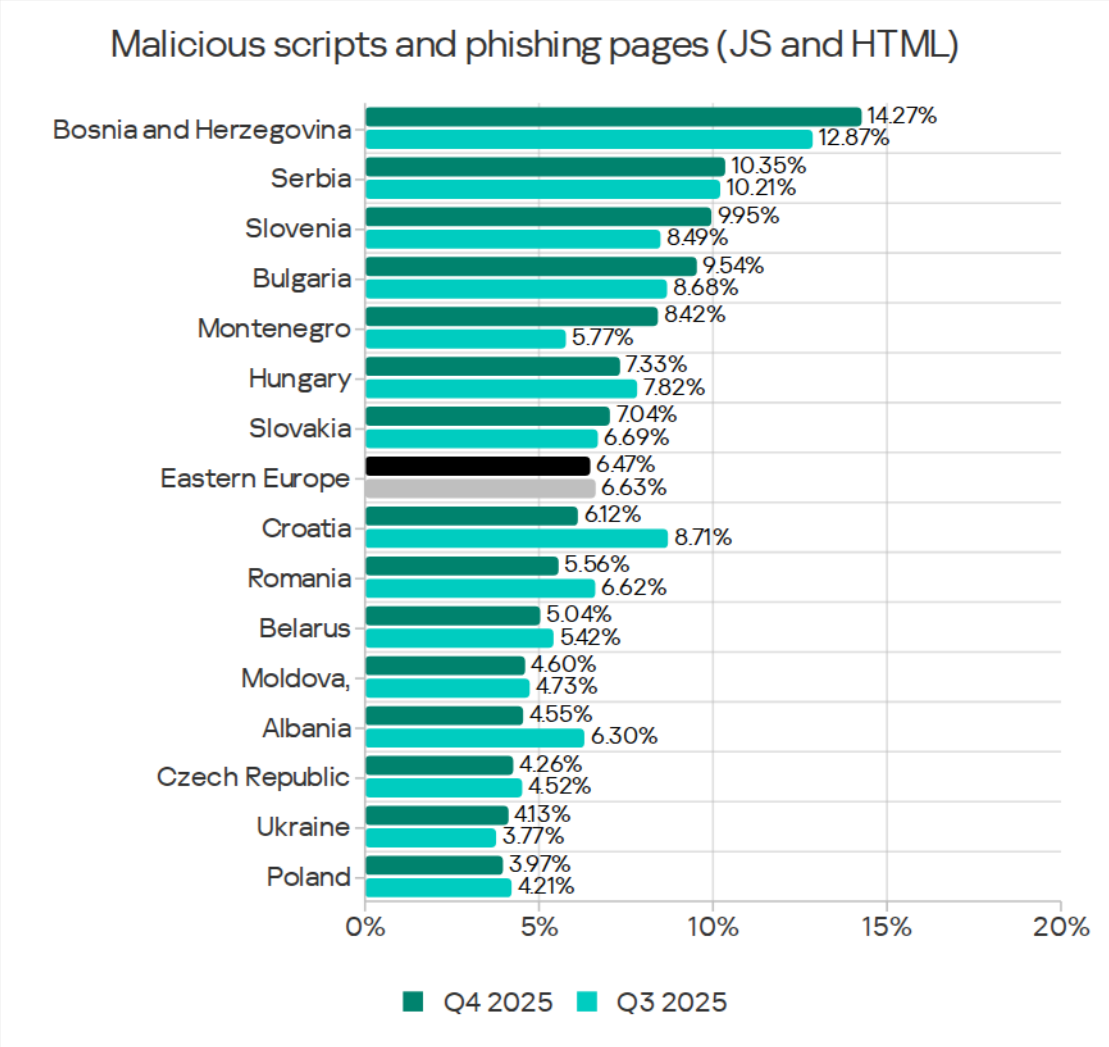
## Malicious scripts and phishing pages

Malicious scripts and phishing pages led the regional rankings for threat categories based on the percentage of ICS computers on which they were blocked.

Based on the percentage of ICS computers on which malicious scripts and phishing pages were blocked in Q4 2025, Eastern Europe ranked seventh globally with 6.47%. This was 2.6 times higher than Northern Europe, which had the lowest rate.




Among countries in the region, Bosnia and Herzegovina led in this metric with 14.27%. This was 2.2 times higher than the regional figure for this threat.

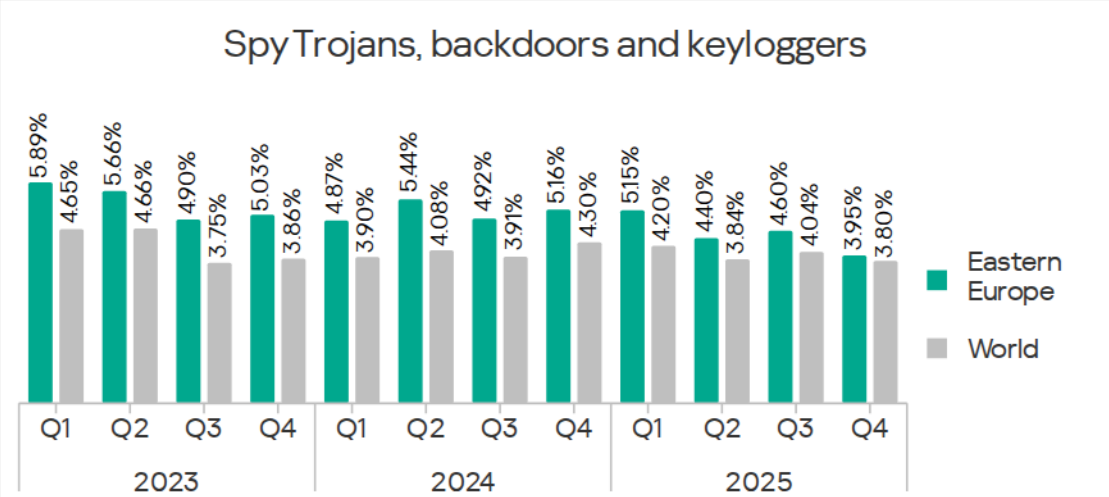



Malicious scripts and phishing pages spread both via the internet and through email.

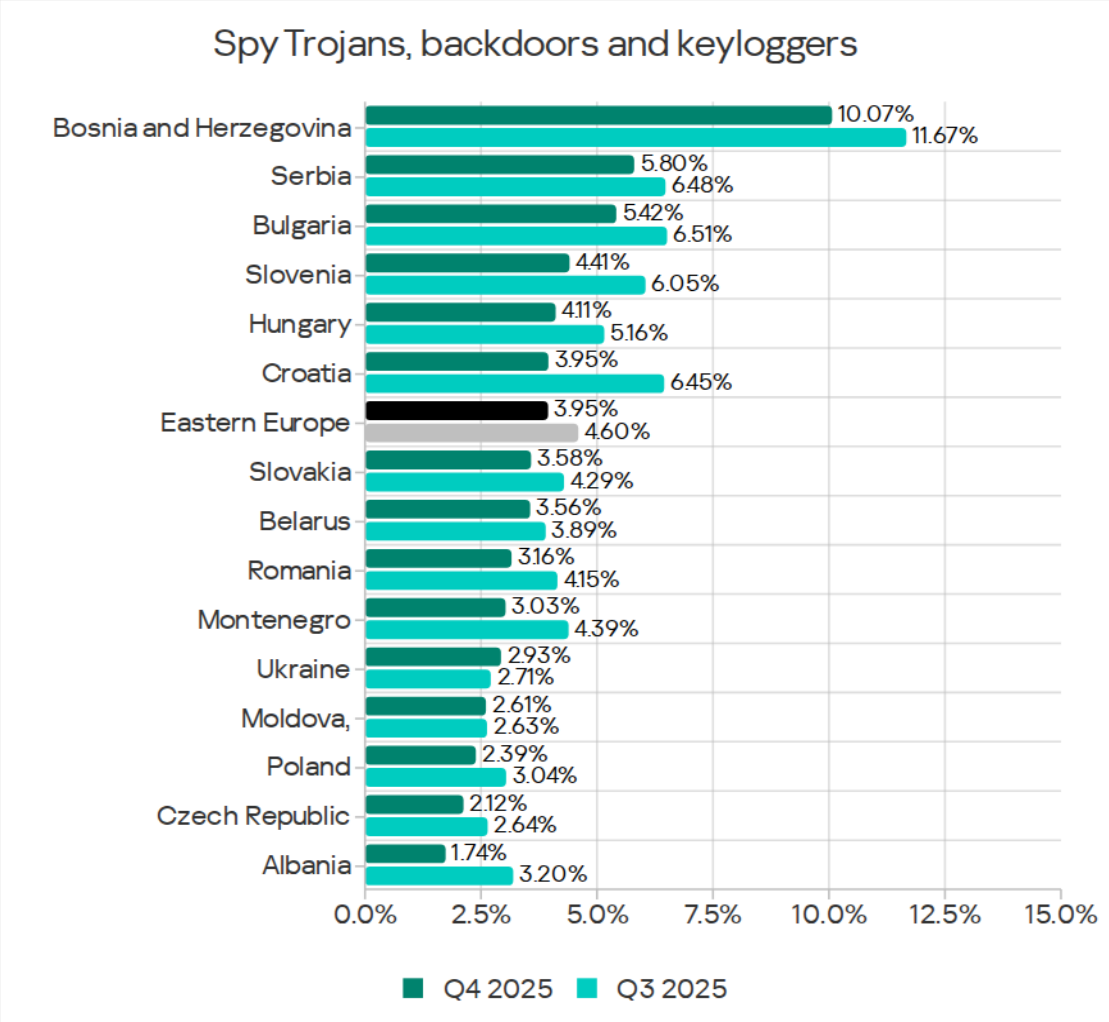
## Spyware

By the percentage of ICS computers on which spyware was blocked, Eastern Europe ranked sixth globally with 3.95%. This figure was 3.2 times higher than in Northern Europe, which had the lowest rate.

The percentage of ICS computers in Eastern Europe on which spyware was blocked fluctuates over time. In Q4 2025, this figure reached a three-year low.




Among the region's countries, Bosnia and Herzegovina led significantly in the percentage of ICS computers on which spyware was blocked, with 10.07%. The lowest figure was in Albania – 1.74%. The only country where the figure increased over the quarter was Ukraine.

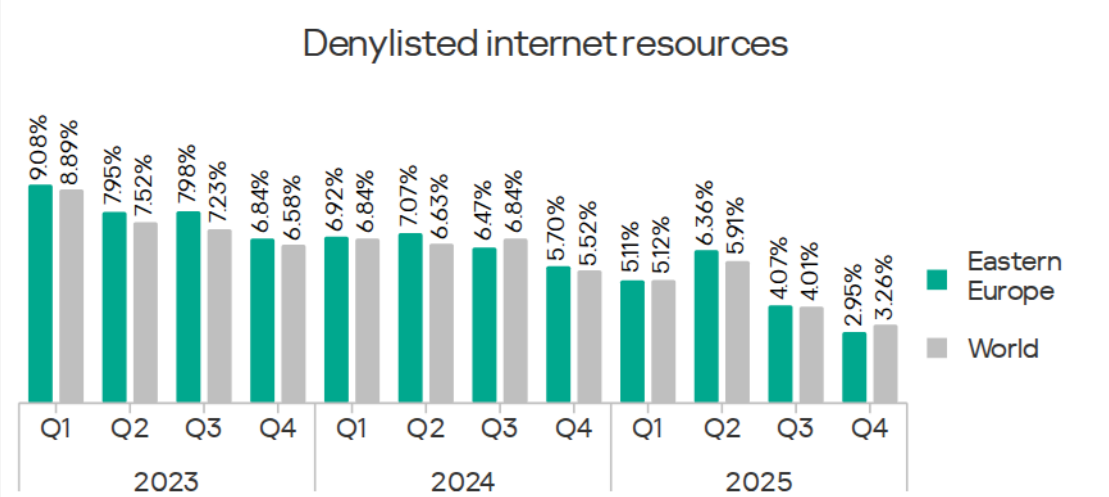


Spyware was blocked in the region across all threat sources, primarily in email clients.

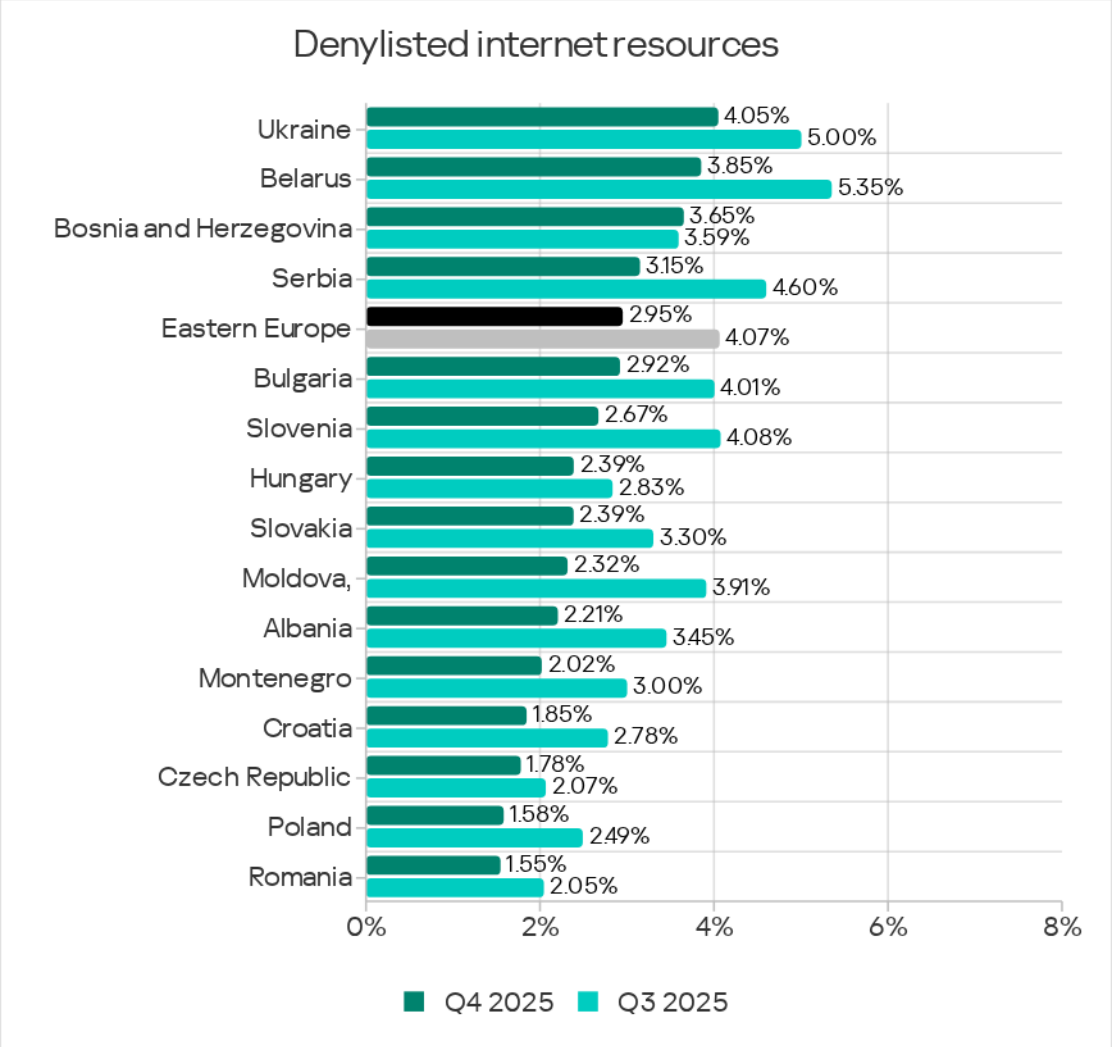
## Denylisted internet resources

By percentage of ICS computers on which denylisted internet resources were blocked, Eastern Europe ranked fifth globally with 2.95%. This figure was 1.7 times higher than in Northern Europe, which had the lowest rate.

The percentage of ICS computers on which denylisted internet resources were blocked is decreasing in Eastern Europe just as it is decreasing globally. Nevertheless, threats in this category ranked third in the regional rankings.




Among countries of the region, Ukraine led with 4.05% in the percentage of ICS computers on which denylisted internet resources were blocked. The lowest figure was in Romania – 1.55%. Over the quarter, this indicator decreased in all countries except Bosnia and Herzegovina.

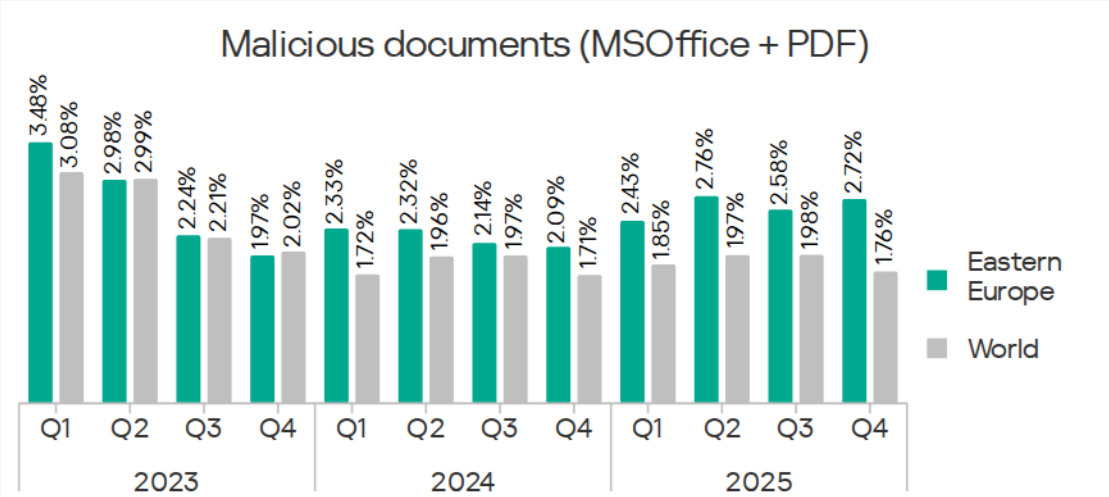



## Malicious documents

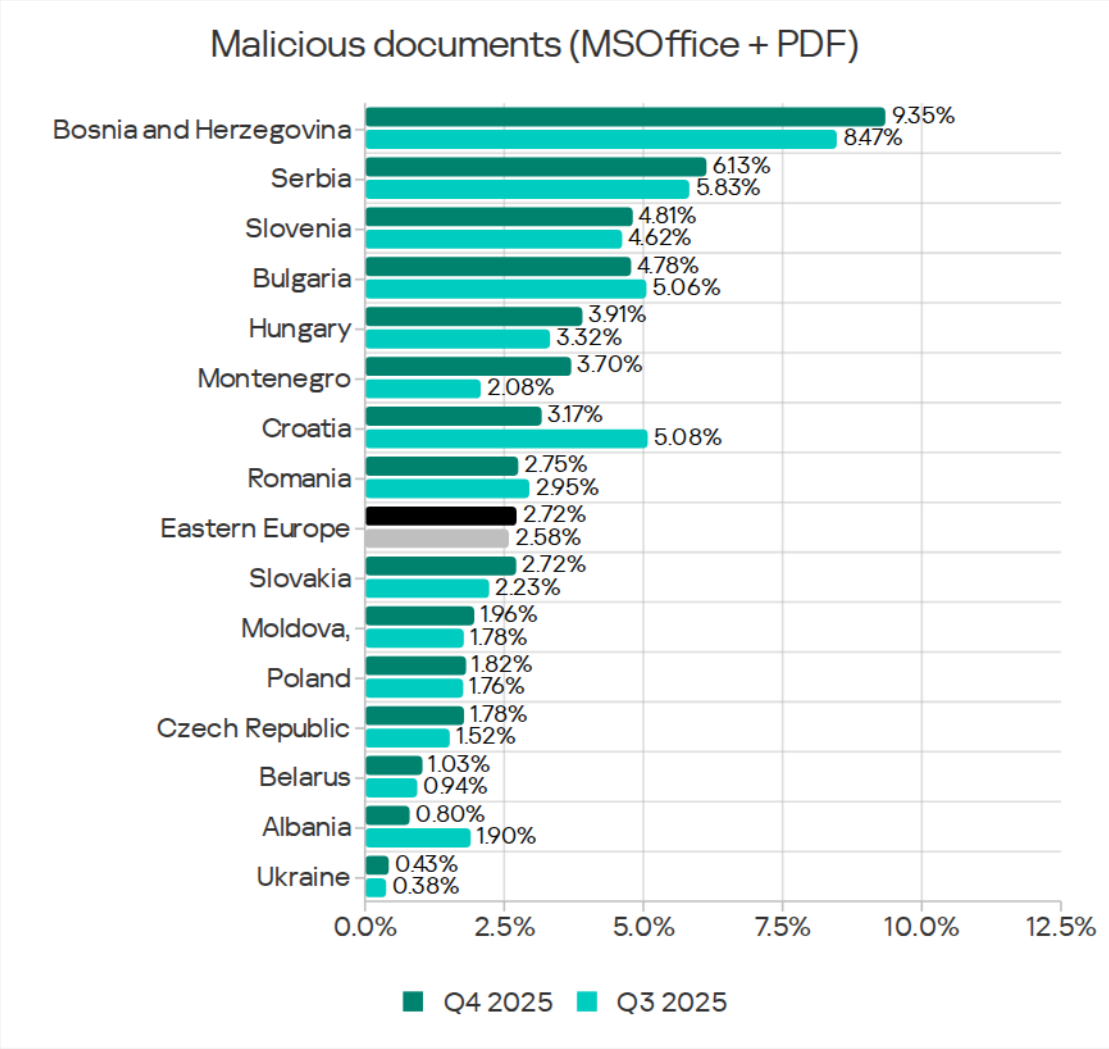
Based on the percentage of ICS computers on which malicious documents were blocked in Q4 2025, Eastern Europe rose from fifth to third place globally.

The rate increased by 2.72%, which was 5.9 times higher than in Northern Europe, which ranked last. Eastern Europe led among regions in terms of the growth in malicious documents.

Note that in 2025, the percentage of ICS computers on which malicious documents were blocked over the quarter in Eastern Europe was above the level of the previous 18 months.




Among countries in the region, Bosnia and Herzegovina led with 9.35%. Ukraine was last in the ranking with 0.43%.



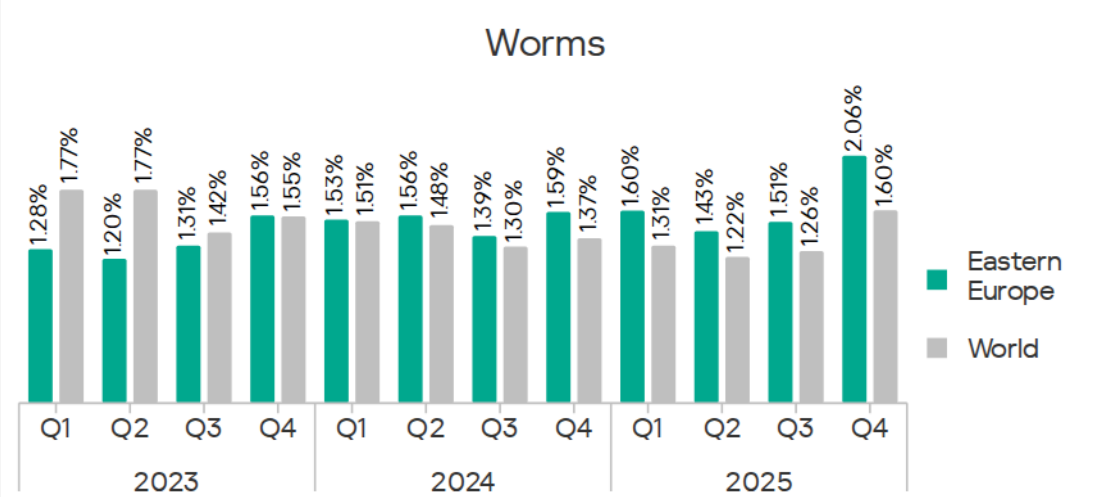

Malicious documents are distributed primarily via email.

Malicious documents are often used by attackers to deliver targeted malware – including spyware.

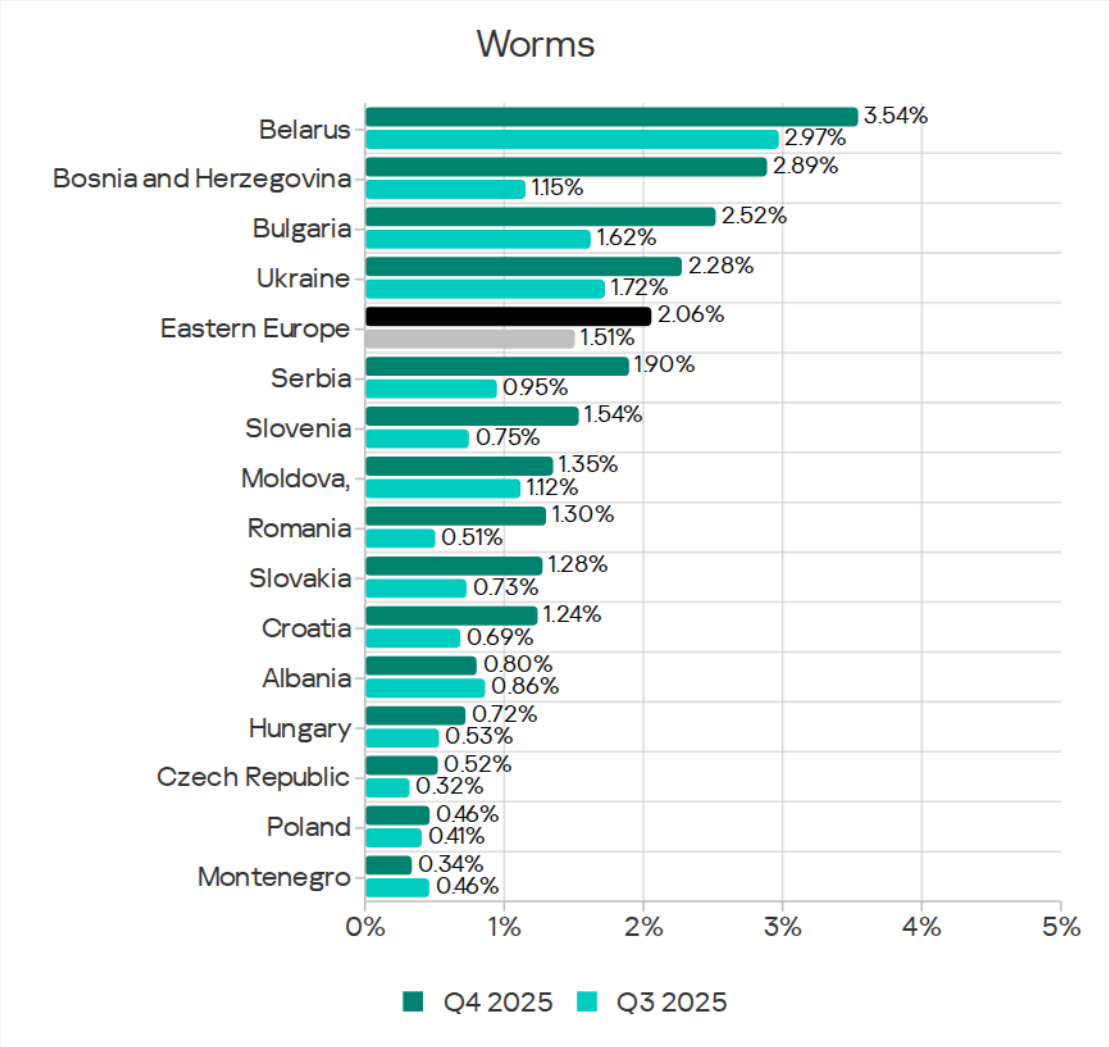
## Worms

By the percentage of ICS computers on which worms were blocked, Eastern Europe rose from sixth to fourth place globally, with 2.06%. The region's figure was 6.4 times higher than in Northern Europe, which ranked last.

In Q4 2025, the worm metric grew across all regions due to the global phishing campaign known as Curriculum-vitae-catalina which we described earlier. Eastern Europe ranked third among regions in terms of growth in this metric.



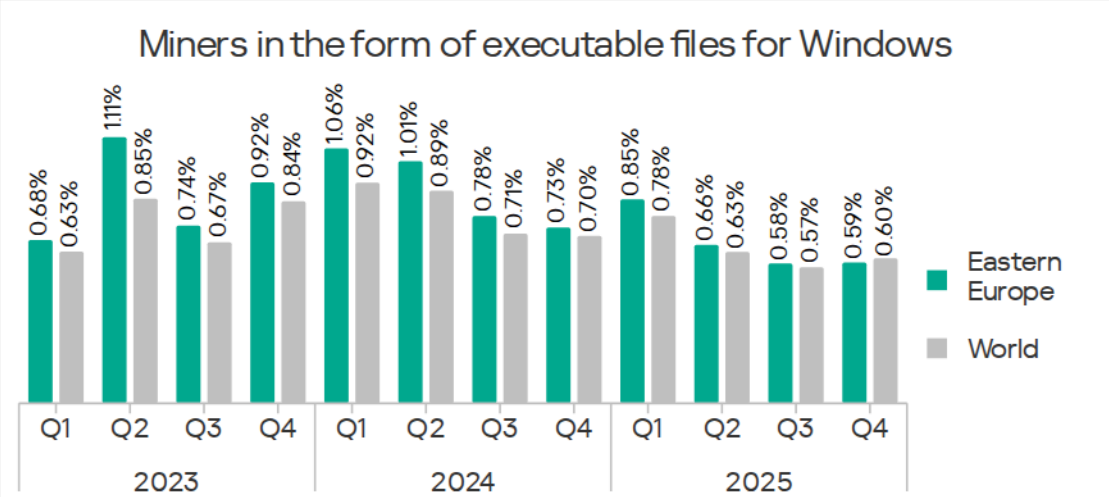

Among countries in the region, Belarus led with 3.54% in the percentage of ICS computers on which worms were blocked. This figure grew across all countries except Albania and Montenegro.



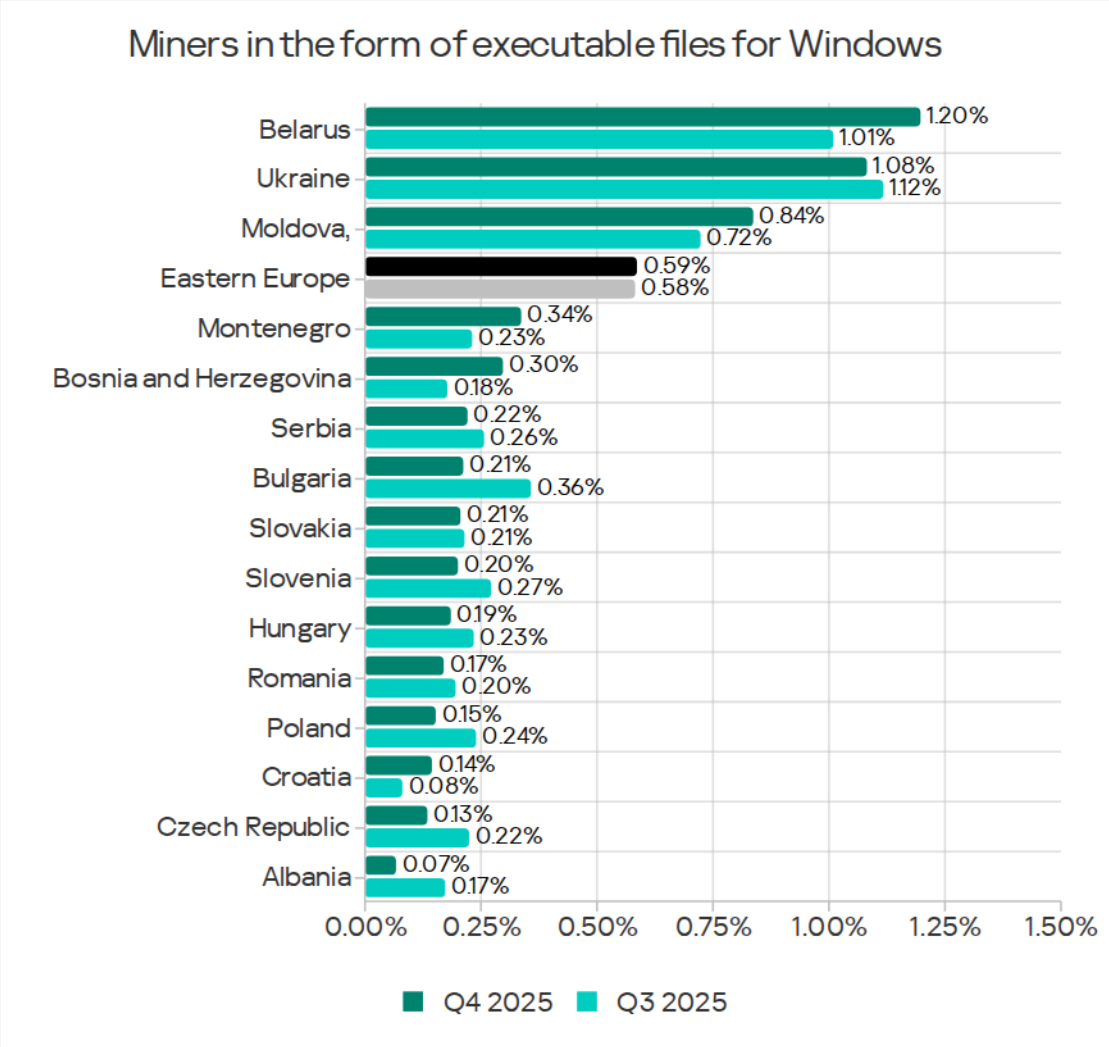

In Q4 2025, email became the main distribution channel for worms due to a phishing attack.

## Miners in the form of executable files for Windows

For miners in the form of executable files for Windows, the region ranked third, with 0.59%. This figure was slightly below the global average and 4.2 times higher than in North America (Canada), which had the lowest figure among regions.




Belarus and Ukraine also led among the region's countries in terms of miners in the form of executable files for Windows with 1.20% and 1.08%, respectively.



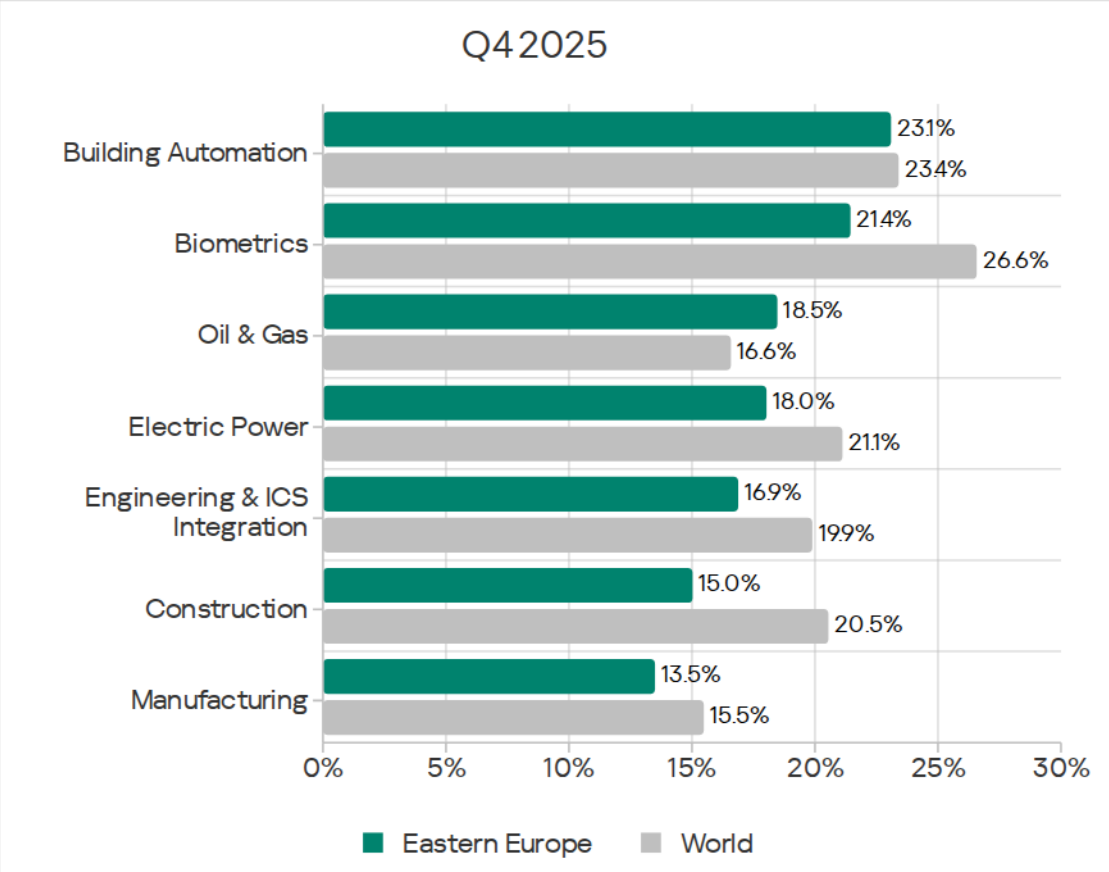
In Eastern Europe, miners in the form of executable files for Windows actively use modules and components that are essentially worms and deliver the miner to other computers in the network (automated lateral movement). A similar situation was observed in Russia.

Among industries in the region, this threat was especially relevant for the building automation and electric power sectors.

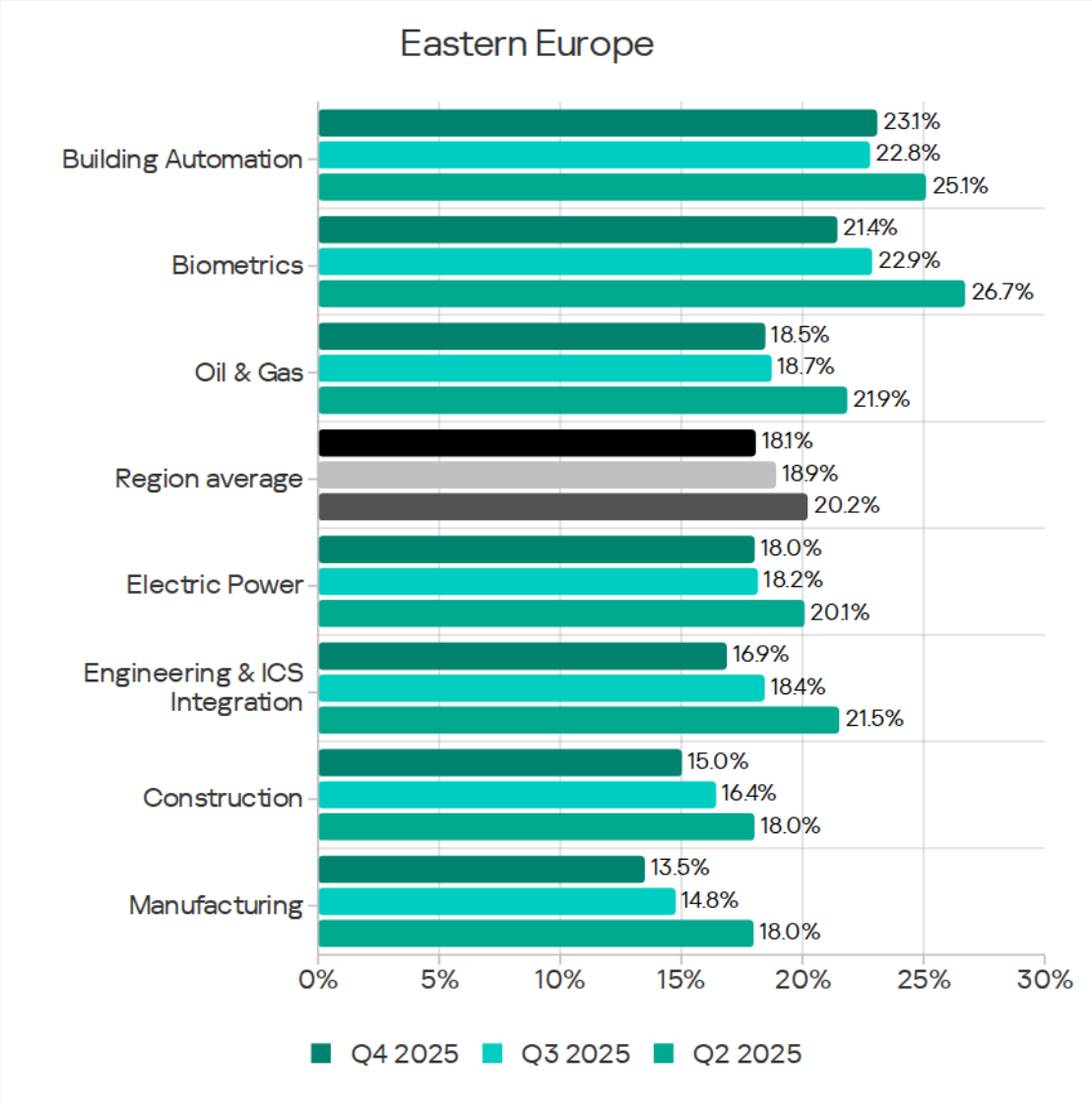
## Industries

Of the region's industries considered in this report, building automation was the most frequently targeted. Eastern Europe was one of three regions where the electric power industry came second in the regional rankings of industries. This industry ranked first only in East Asia, while its rankings in all other regions are lower.

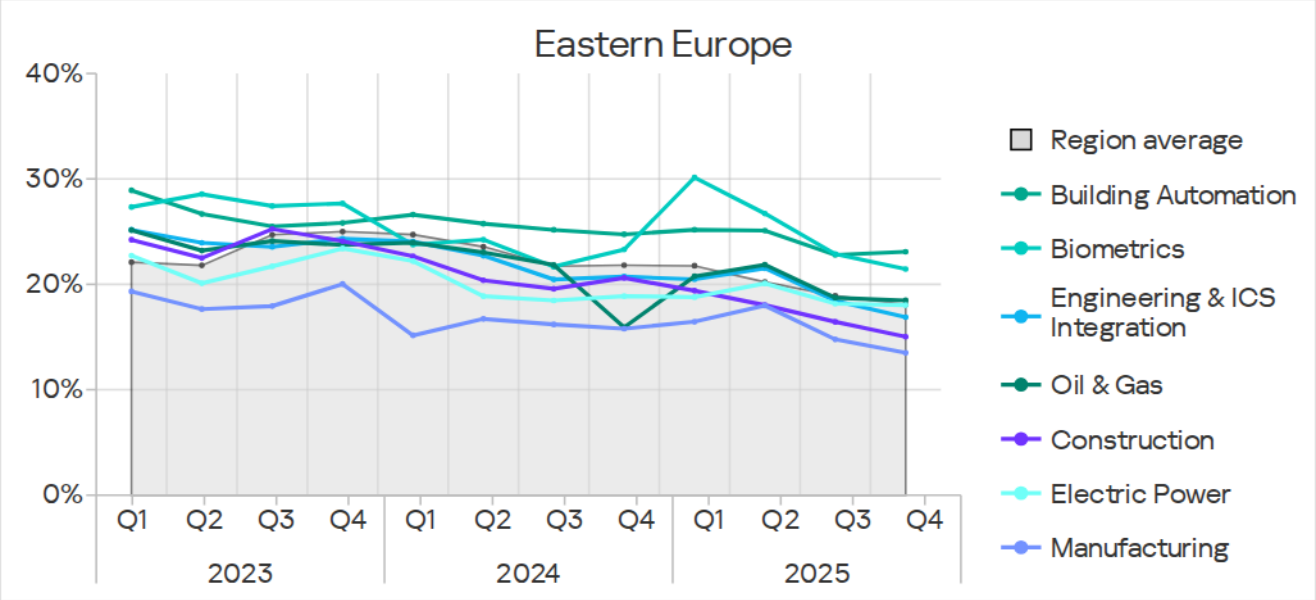
All industries showed indicators lower than the global averages.




The building automation industry was the only industry in the region where this indicator increased in Q4 2025.




The trends for the majority of industries under review suggest stabilization after significant growth in 2022. The figures for the construction industry and the engineering and ICS integrators industry are gradually decreasing.




## Threat sources and malware categories in industries: 'hotspots'

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

**Threat source indicators for industries in Eastern Europe, Q4 2025**

| Industry / Threat source | Biometrics | Building Automation | Engineering & ICS Integration | Electric Power | Oil & Gas | Construction | Manufacturing | Category metric in region |
|---|---|---|---|---|---|---|---|---|
| Internet | 6.79% | 8.17% | 7.28% | 7.78% | 9.55% | 8.16% | 5.83% | 6.92% |
| Email clients | 8.49% | 8.15% | 2.89% | 2.86% | 2.23% | 1.88% | 2.35% | 3.69% |
| Removable media | 0.64% | 0.26% | 0.14% | 0.22% | 1.59% | 0.23% | — | 0.19% |
| Network folders | — | 0.04% | 0.02% | — | — | — | — | 0.02% |
| **Industry metric in region** | 21.44% | 23.09% | 16.88% | 18.03% | 18.47% | 15.02% | 13.50% | |

**Threat category indicators for industries in Eastern Europe, Q4 2025**

| Industry / Threat type | Biometrics | Building Automation | Engineering & ICS Integration | Electric Power | Oil & Gas | Construction | Manufacturing | Category metric in region |
|---|---|---|---|---|---|---|---|---|
| Denylisted internet resources | 2.55% | 3.30% | 3.06% | 3.78% | 5.73% | 3.76% | 2.04% | 2.95% |
| Malicious scripts and phishing pages (JS and HTML) | 10.40% | 10.27% | 6.40% | 6.02% | 8.28% | 6.75% | 4.40% | 6.47% |
| Malicious documents (MSOffice + PDF) | 8.07% | 5.98% | 2.06% | 1.72% | 2.55% | 1.23% | 1.53% | 2.72% |
| Spy Trojans, backdoors and keyloggers | 8.49% | 7.10% | 3.39% | 4.00% | 3.50% | 3.11% | 2.86% | 3.95% |
| Ransomware | 0.21% | 0.20% | 0.10% | 0.04% | — | 0.06% | 0.20% | 0.12% |
| Miners in the form of executable files for Windows | — | 0.62% | 0.58% | 0.62% | 1.91% | 1.06% | 0.51% | 0.59% |
| Web miners running in browsers | — | 0.25% | 0.20% | 0.26% | 0.96% | 0.35% | 0.31% | 0.19% |
| Malware for AutoCAD | 0.21% | 0.02% | 0.06% | 0.09% | — | 0.41% | — | 0.07% |
| Worms | 2.34% | 3.17% | 1.40% | 2.46% | 4.14% | 1.76% | 2.45% | 2.06% |
| Viruses | 0.64% | 0.56% | 0.39% | 0.66% | 1.27% | 1.00% | 0.31% | 0.45% |
| **Industry metric in region** | 21.44% | 23.09% | 16.88% | 18.03% | 18.47% | 15.02% | 13.50% | |

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.

The building automation industry's indicators show all the signs of high exposure to advanced categories of threat actors. The figure for email client threats was also high in the construction industry.

Eastern Europe ranked second among regions based on the figure for email clients in both the building automation industry and the construction industry.

Based on the metric for ransomware in the manufacturing industry, Eastern Europe ranked third among all regions. Manufacturing topped the regional rankings of industries in terms of this metric.

Eastern Europe ranked third among regions in terms of executable miners in the building automation industry, construction industry, and electric power industry.

**Building automation**

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

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

- Second place in the percentage of ICS computers on which threats from email clients were blocked.
- Second place in the percentage of ICS computers on which malicious documents were blocked.
- Third place in miners in the form of executable files, as well as viruses.

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

- First by the percentage of ICS computers on which threats from all sources were blocked.
- First for malicious scripts and phishing pages, malicious documents, spyware, and worms.
- Second in miners in the form of executable files for Windows and ransomware.
- Third in denylisted internet resources and viruses.

**Electric power**

Eastern Europe ranked eighth 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 had the following rankings:

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

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

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

**Engineering and ICS integrators**

Eastern Europe ranked 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 had the following rankings:

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

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

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

**Construction**

Eastern Europe ranked ninth 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 had the following rankings:

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

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

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

- First in the following threat categories: both categories of miners, viruses, and malware for AutoCAD.
- Second place for denylisted internet resources and malicious scripts.

**Manufacturing**

Eastern Europe ranked 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 had the following rankings:

- First by percentage of ICS computers on which ransomware and worms were blocked.

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

- First in the percentage of ICS computers on which malware was blocked.
- Second in the percentage of ICS computers on which web miners were blocked.
- Third place in terms of worms.

# Western Europe

## Key cybersecurity issues in the region

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

In Q4 2025, it ranked 13th globally by the percentage of ICS computers on which malicious objects were blocked.

The percentage of ICS computers on which threats from the internet were blocked grew in Western Europe. Western Europe's highest ranking globally across all categories of threats blocked on ICS computers was for denylisted internet resources, in ninth place.

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

In Q4 2025, the figures for malicious documents and ransomware increased in Western Europe.

In terms of growth of the metrics in both of these threat categories, the engineering and ICS integrators industry ranked first among all industries of the region.

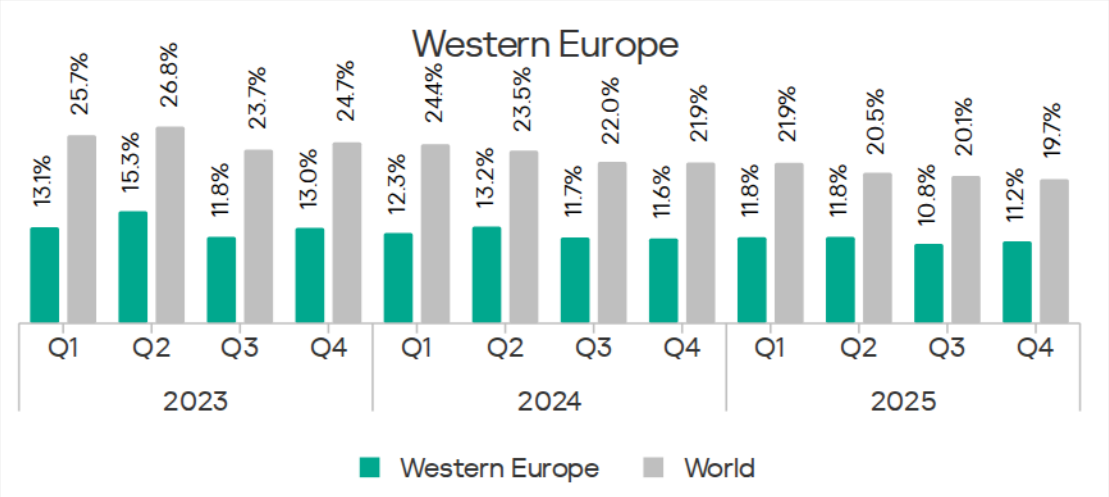
Among the countries of the region, Austria ranked first by growth of the percentage of ICS computers on which malicious documents and ransomware were blocked. In this country, the indicator for ransomware grew by a factor of 2.71 and the indicator for malicious documents grew by a factor of 1.49 in Q4 2025.

Austria also showed an increase in the indicators for malicious scripts and phishing pages by a factor of 1.35.

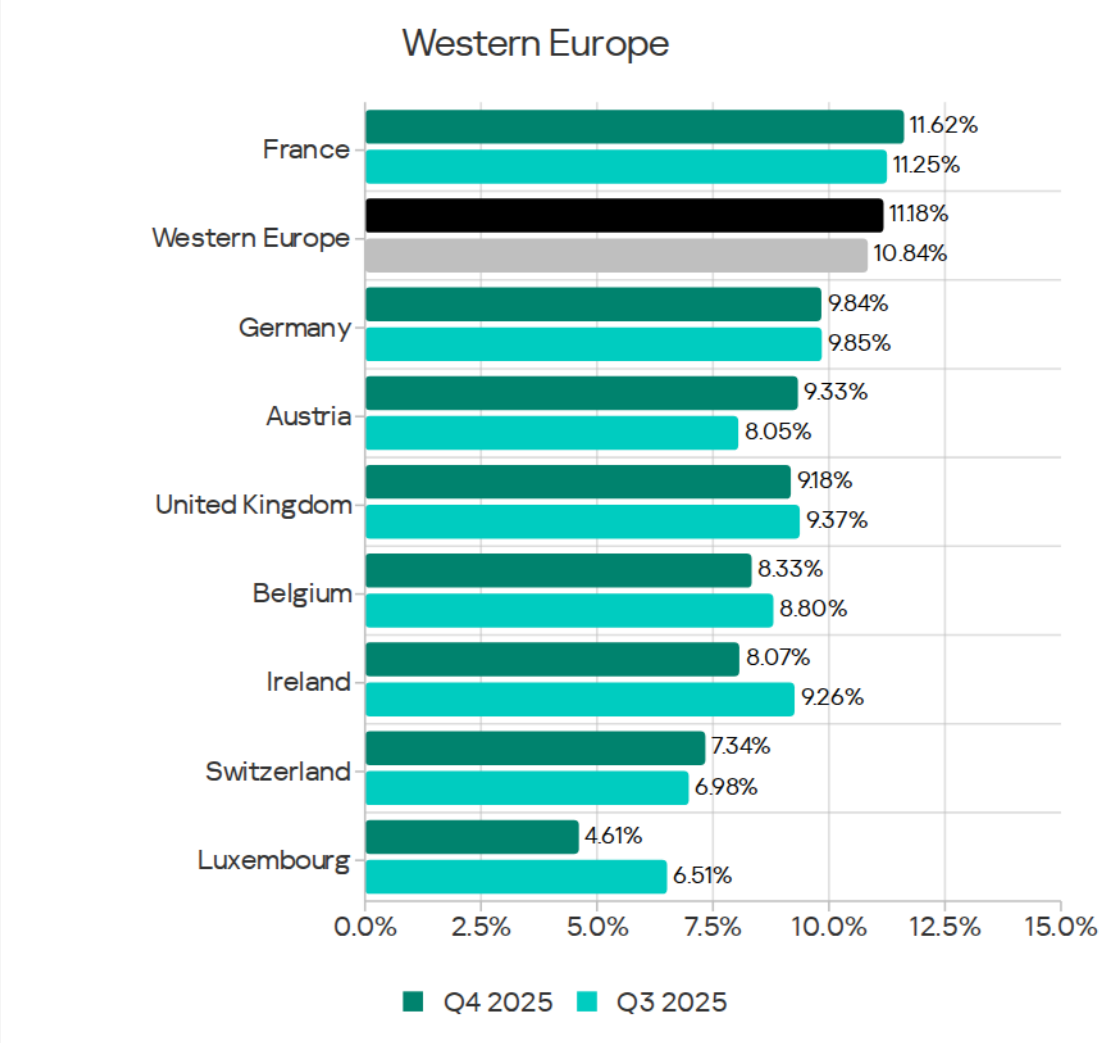
Based on the percentage of ICS computers on which threats from email clients were blocked, Austria led all other countries of the region with a figure that grew by a factor of 1.34.

## Statistics across all threats

In Q4 2025, Western Europe ranked 13th globally by percentage of ICS computers on which malicious objects were blocked. The figure in the region increased to 11.2%. This was significantly below the global average but still 1.3 times higher than in Northern Europe, the region with the lowest rate.

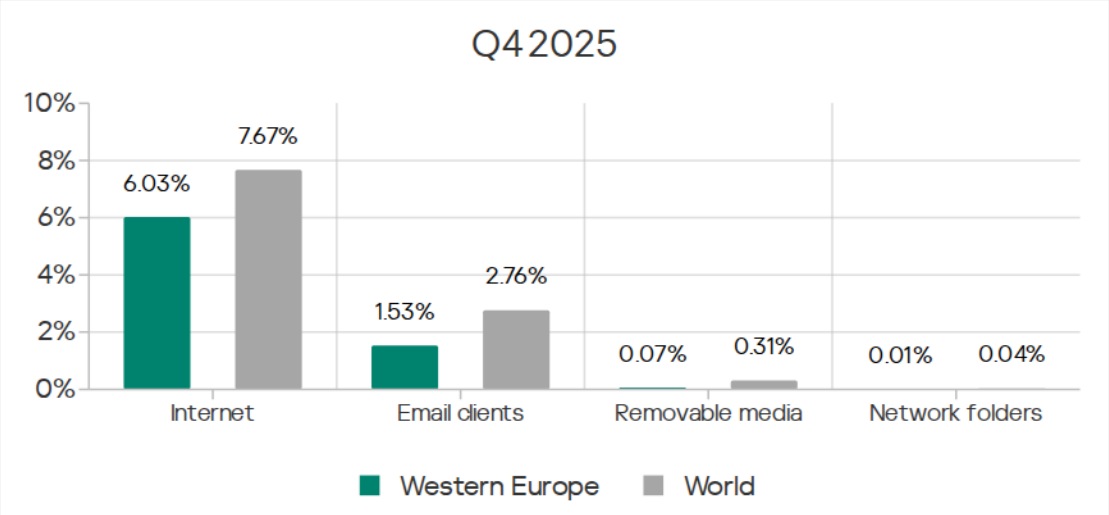



Among the region's countries, France led in the percentage of ICS computers with blocked malicious objects, at 11.62%. The lowest figure was in Luxembourg, at 4.61%.



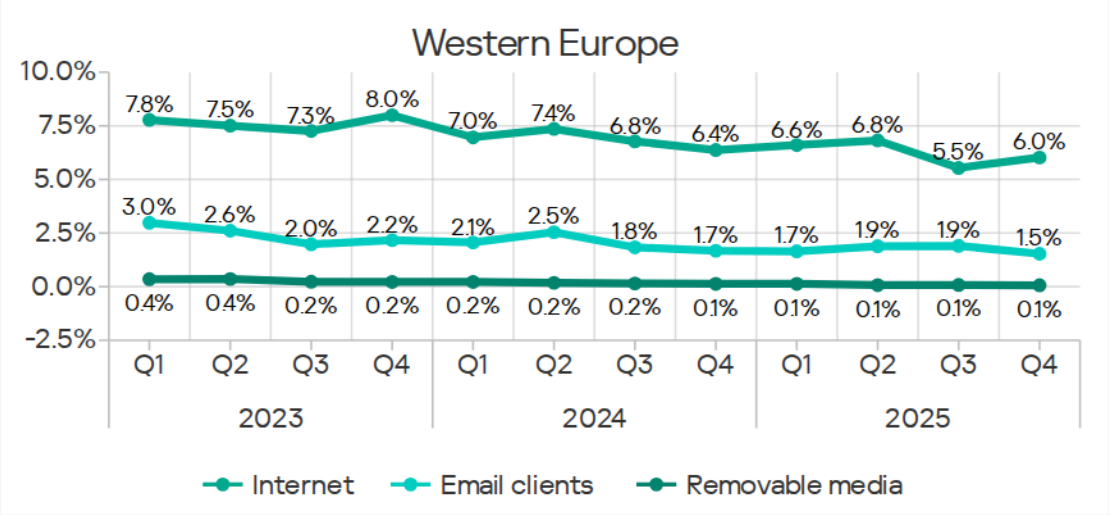
## Threat sources

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




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

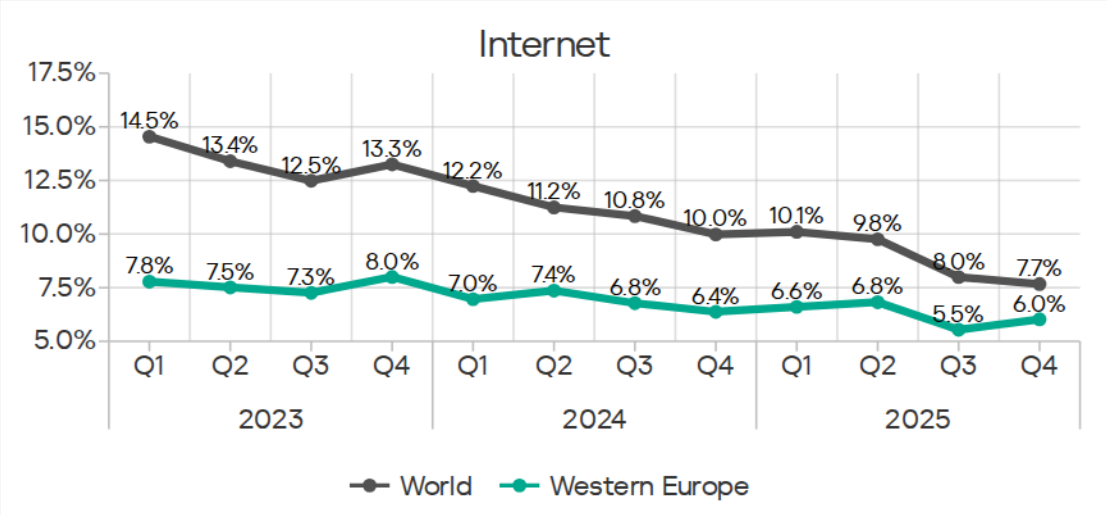
In Q4 2025, the percentage of ICS computers on which malicious objects were blocked in the region increased slightly for threats from the internet.



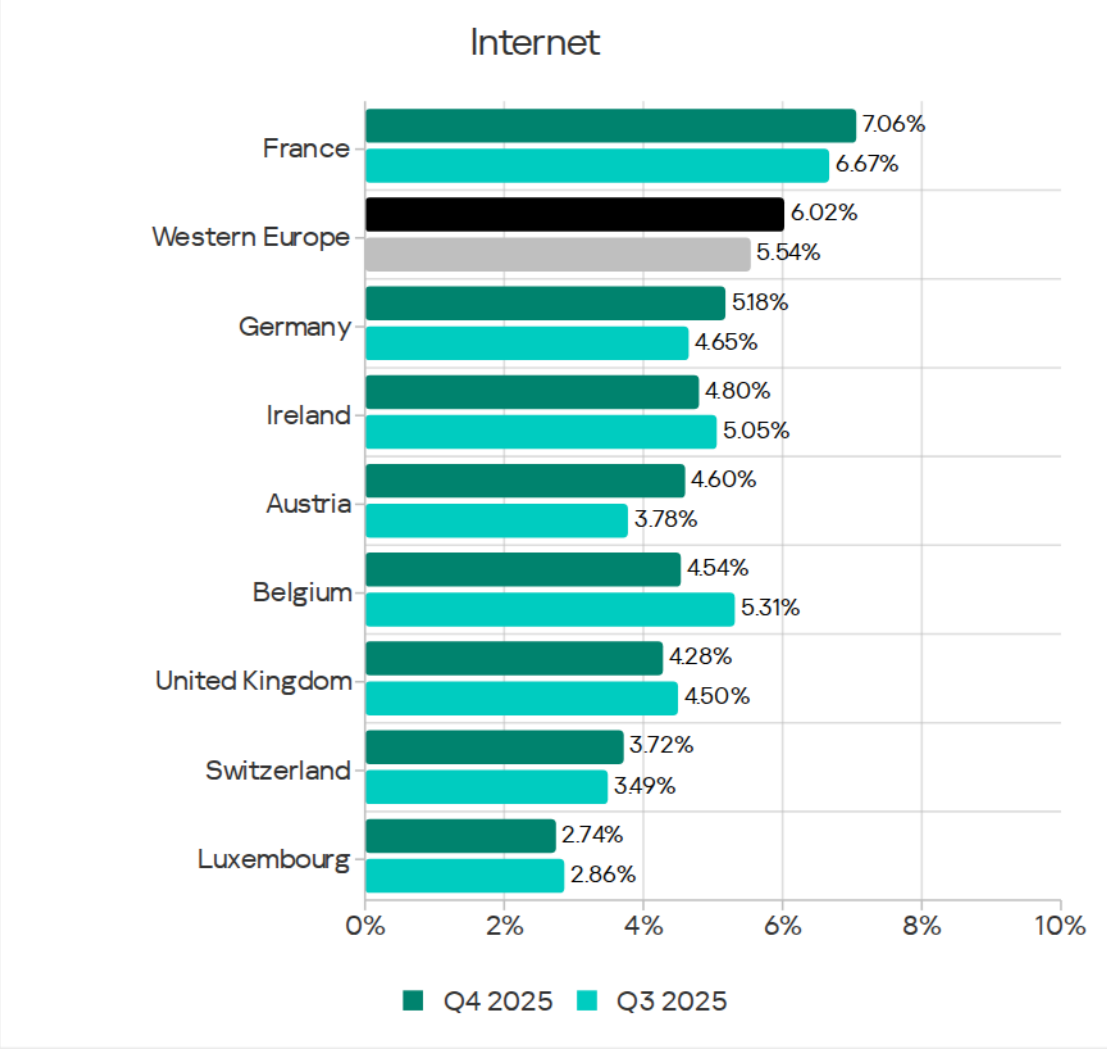

### Internet

By percentage of ICS computers on which internet threats were blocked, Western Europe ranked 11th globally, with a rate of 6.03%. This was 1.5 times higher than in Northern Europe, which recorded the lowest figure of all regions.

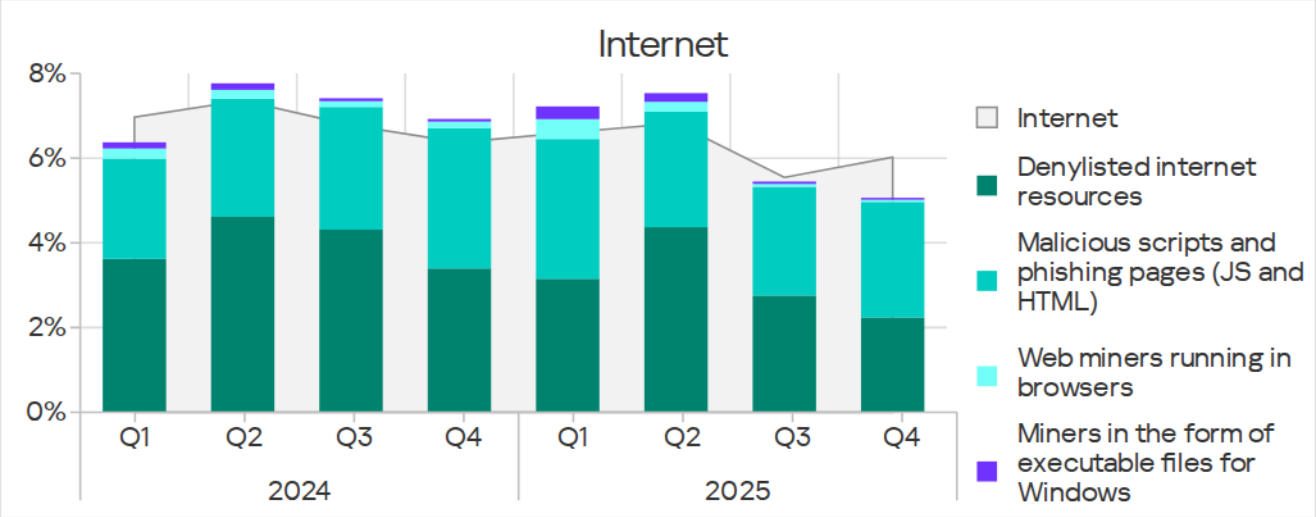
Western Europe was one of five regions in which the figure for threats from the internet increased in Q4 2025.




Country-level rates ranged from 2.74% in Luxembourg to 7.06% in France.



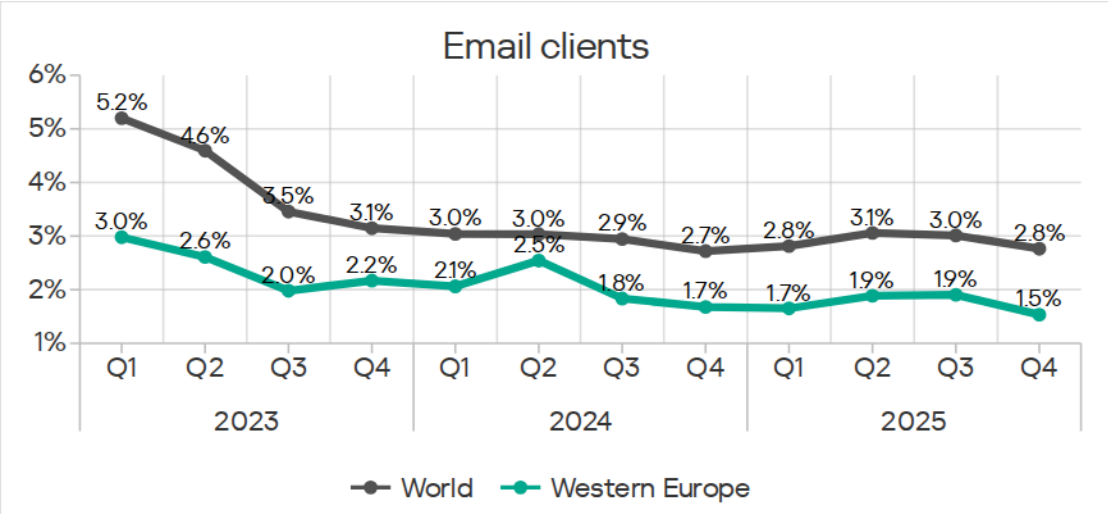
The main categories of internet threats blocked on ICS computers in the region include malicious scripts and phishing pages, as well as denylisted internet resources.



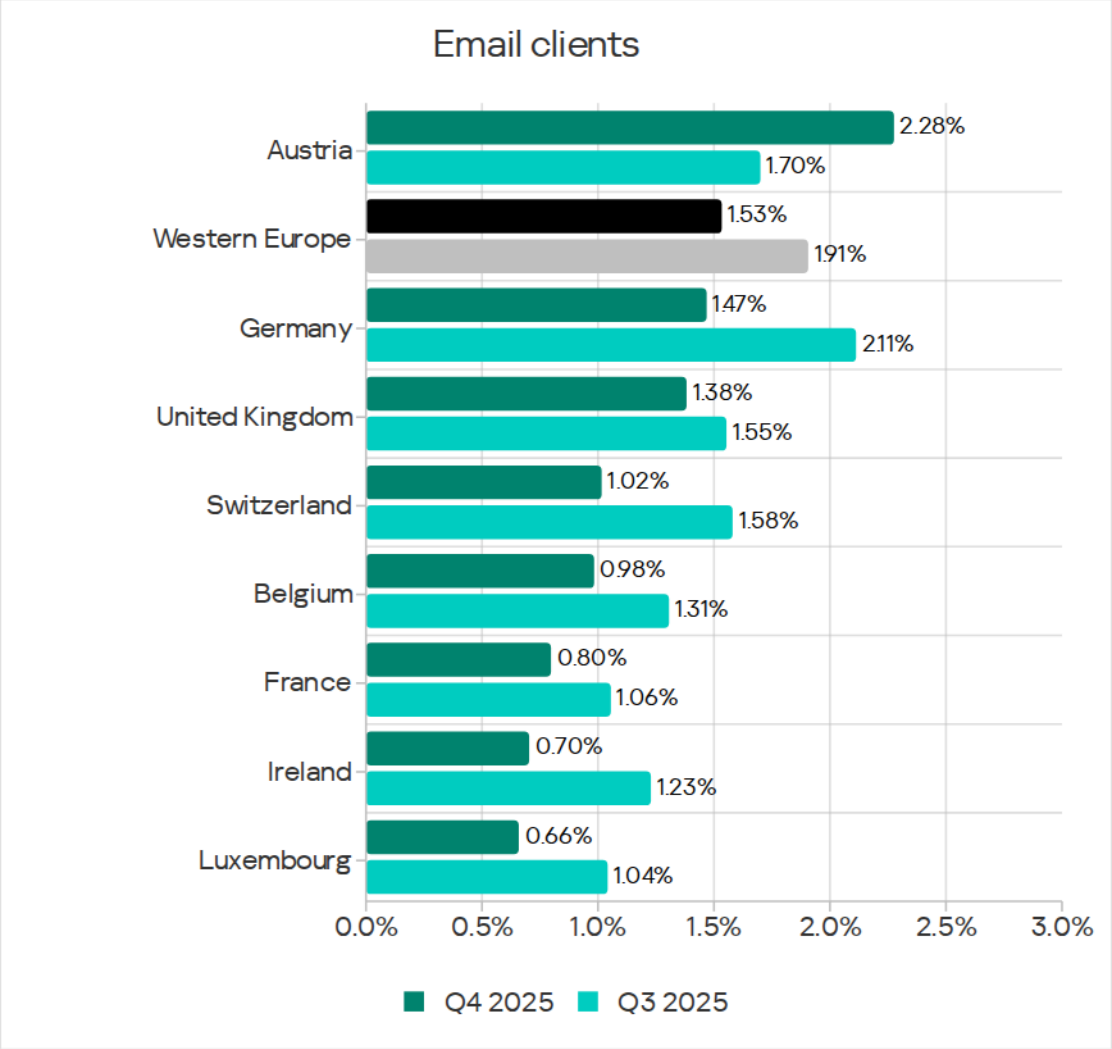

France led the region in terms of denylisted internet resources, as well as malicious scripts and phishing pages.

## Email clients

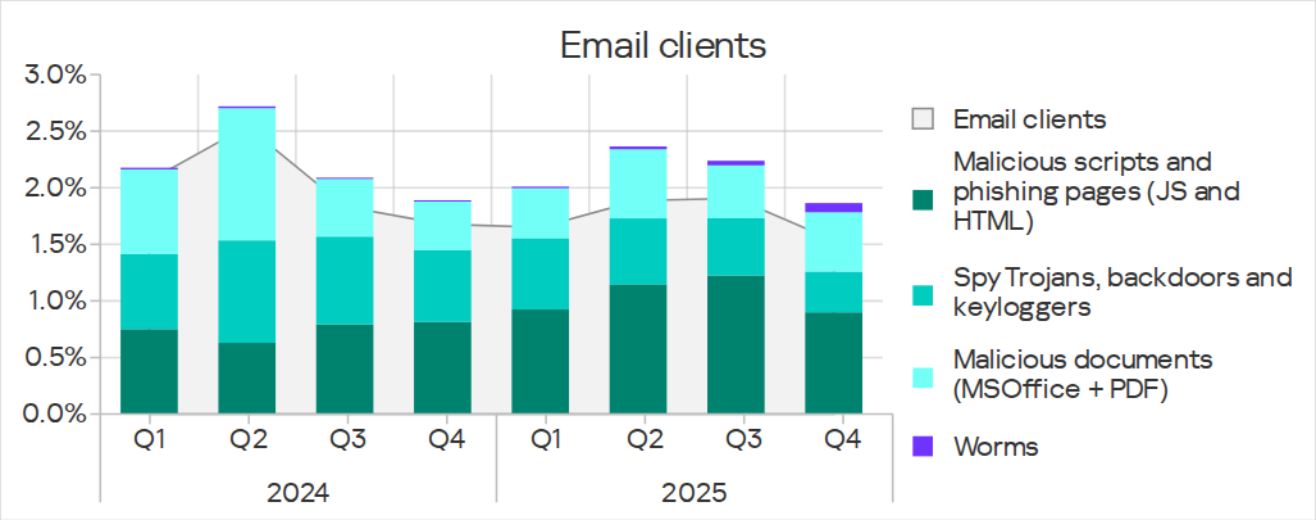
By percentage of ICS computers on which threats from email clients were blocked, Western Europe ranked 10th in Q4 2025, with a rate of 1.53%. This was 2.4 times higher than in Northern Europe, which ranked last.




Among countries in the region, Austria led in this metric with 2.28%. This is the only country where this metric grew over the quarter. In fact, it grew substantially by a factor of 1.34.




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



Spyware in the region spread mainly via email.

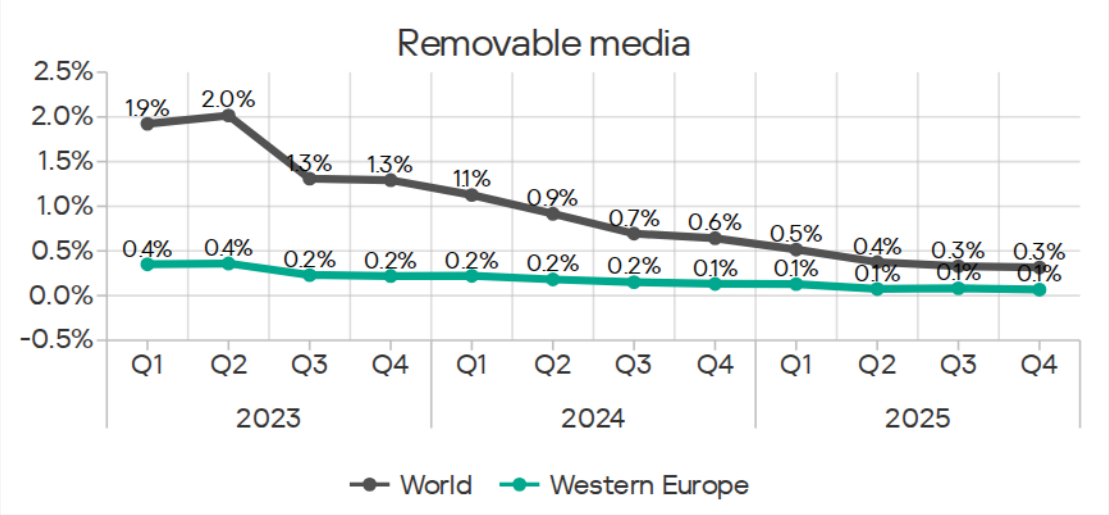
Q4 2025 saw an increase across all regions in the percentage of ICS computers on which worms from email clients were blocked. This was connected with the latest wave of phishing campaigns known as Curriculum-vitae-catalina. In Western Europe, these attacks peaked in October.

The indicator for worms increased in all regions of the world. Western Europe was one of the top three regions with the lowest growth in the worm metric over the quarter.

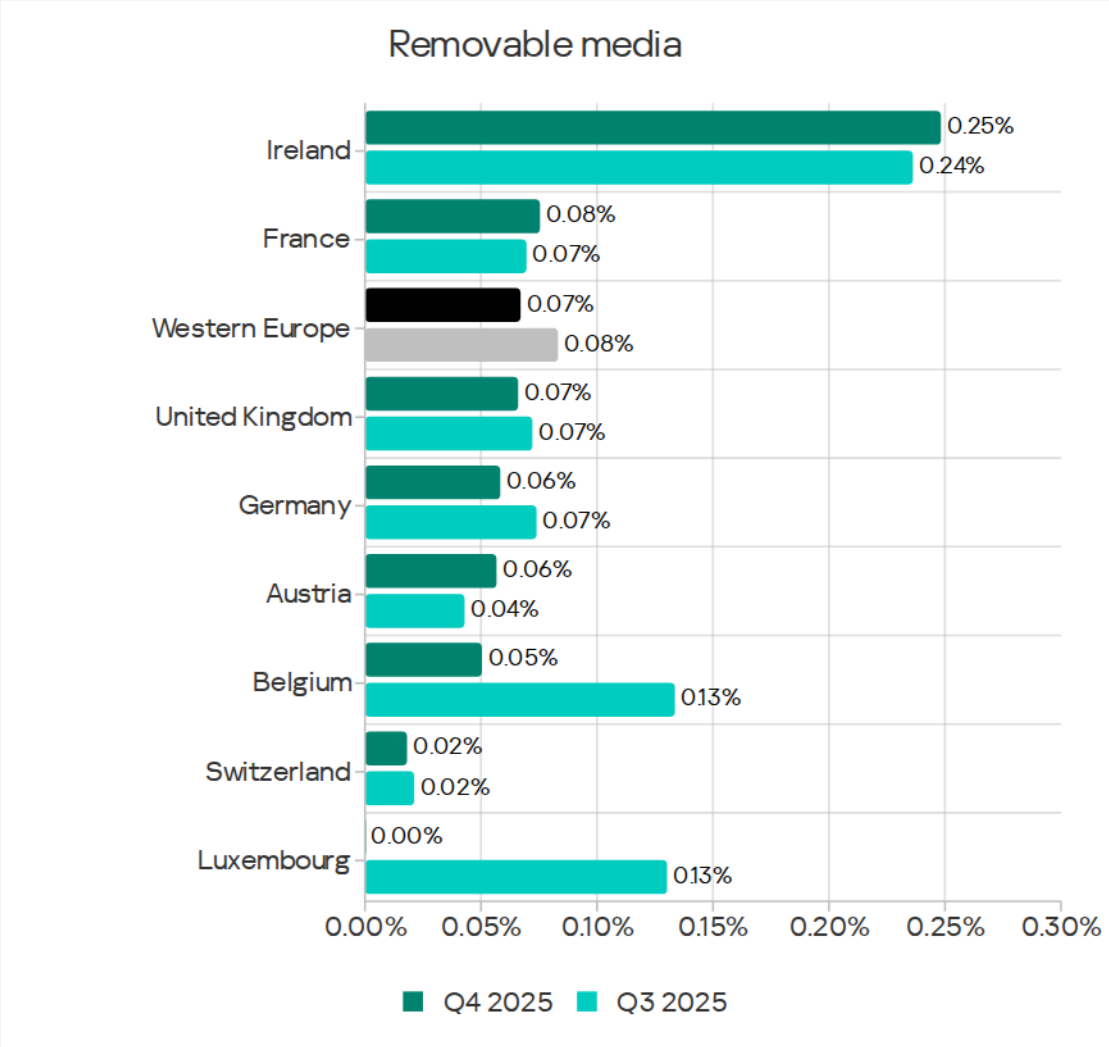
## Removable media

In terms of ICS computers on which threats from removable media were blocked, Western Europe ranked 12th globally in Q4 2025, with a rate of 0.07%. This figure was 1.4 times higher than in the Australia and New Zealand region, which ranked 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. In Q4 2025, this indicator dropped back to its Q2 2025 value.

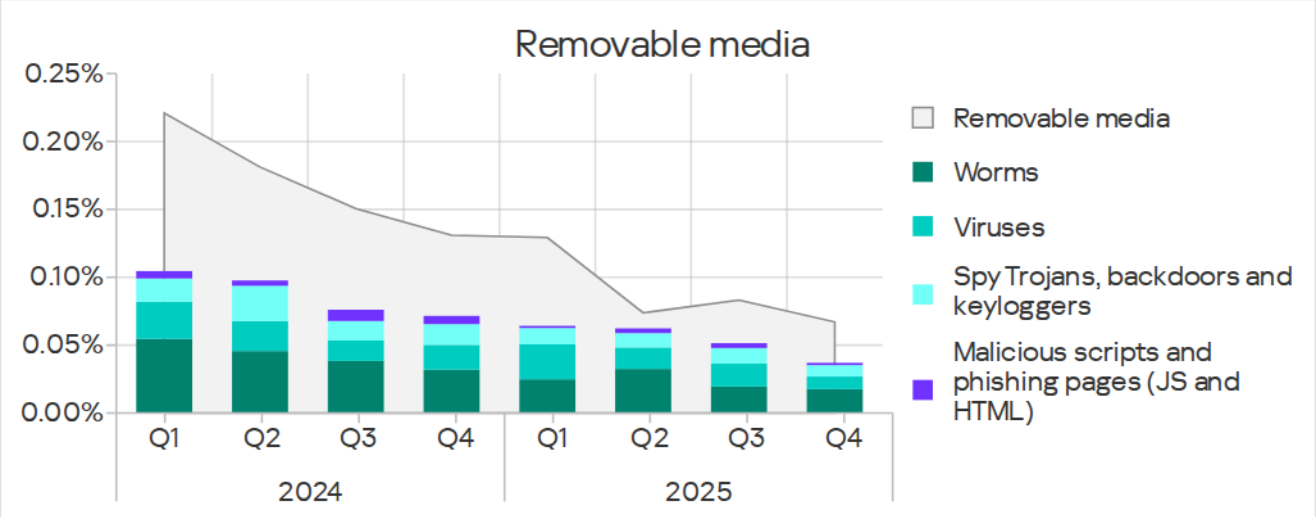



With 0.25%, Ireland led all other countries of the region by a wide margin.



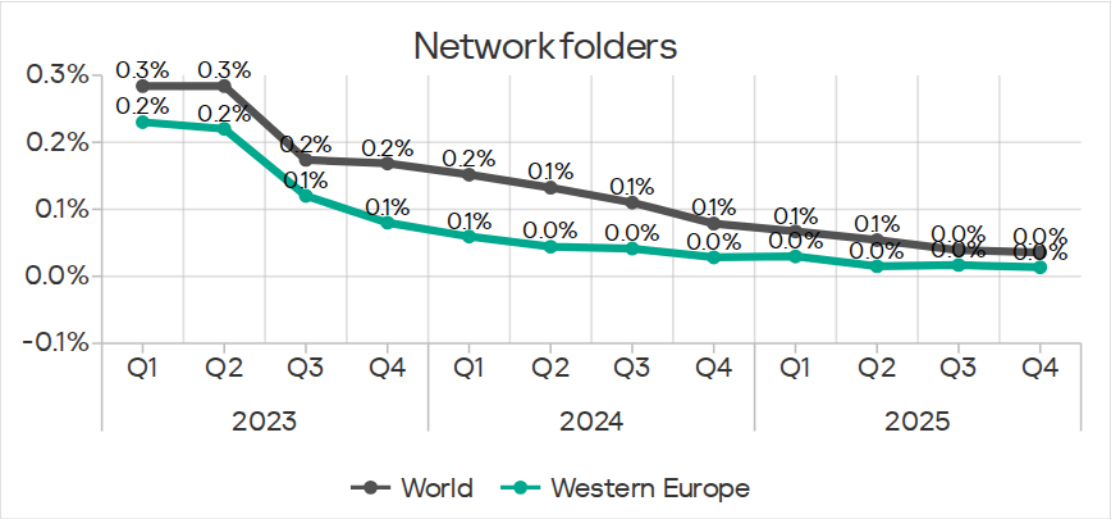

Q3 2025 saw a sharp increase in this indicator in Belgium (by a factor of 4.3) and in Ireland (by a factor of 1.6). In Q4 2025, the figure in Belgium returned to its normal values while the growth in Ireland continued, albeit not so dramatically.

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



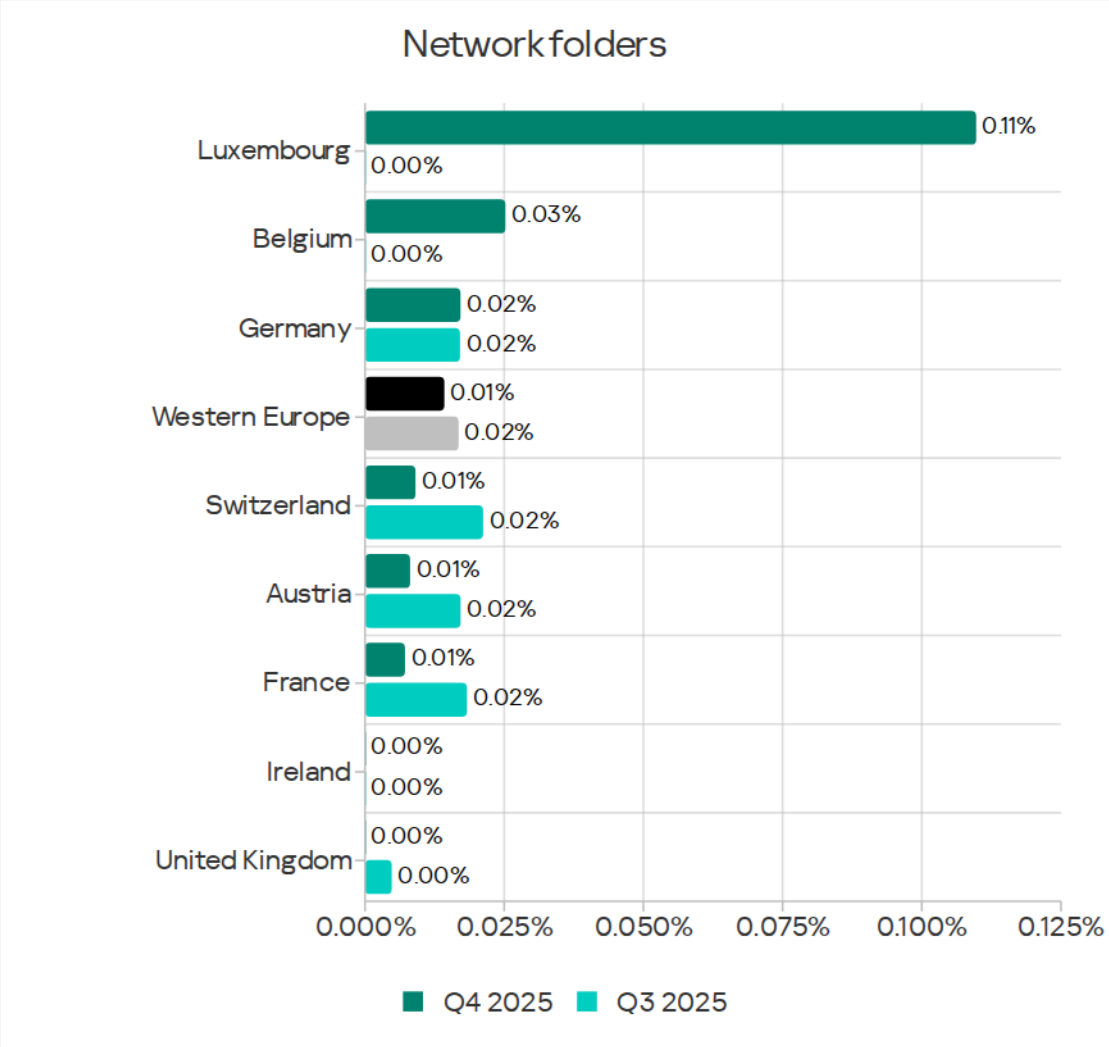

## Network folders

By percentage of ICS computers on which threats from network folders were blocked, Western Europe ranked 12th among regions in Q4 2025, with a rate of 0.014%. This was two times higher than in Northern Europe, which ranked last.



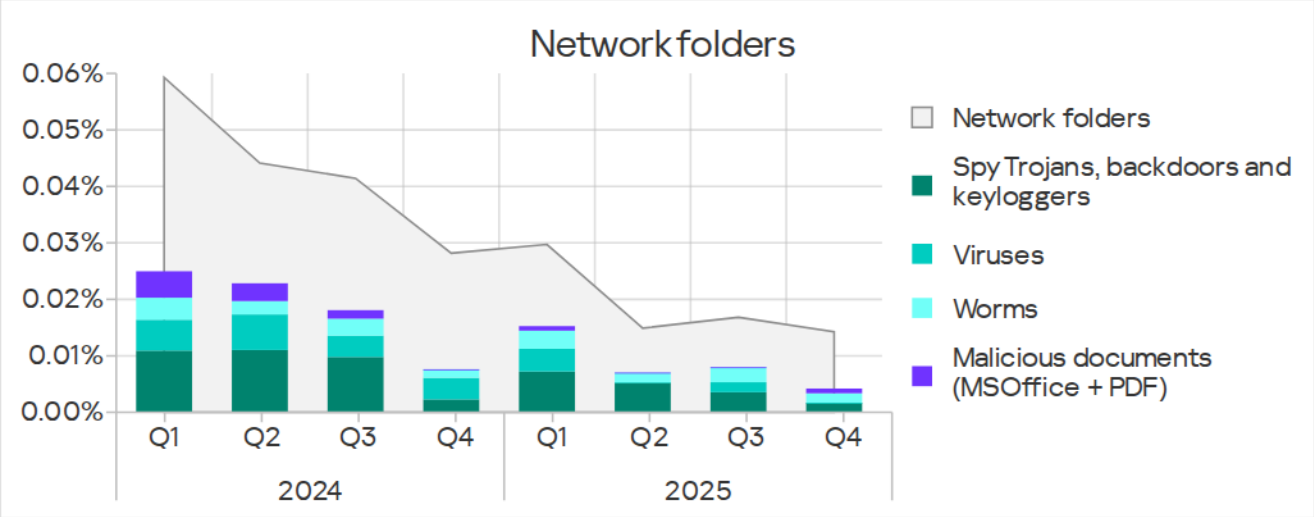

In a protected infrastructure, threats in network folders are encountered fairly rarely and not in all countries and industries of the region.

Among countries in the region, Luxembourg led with 0.11%.

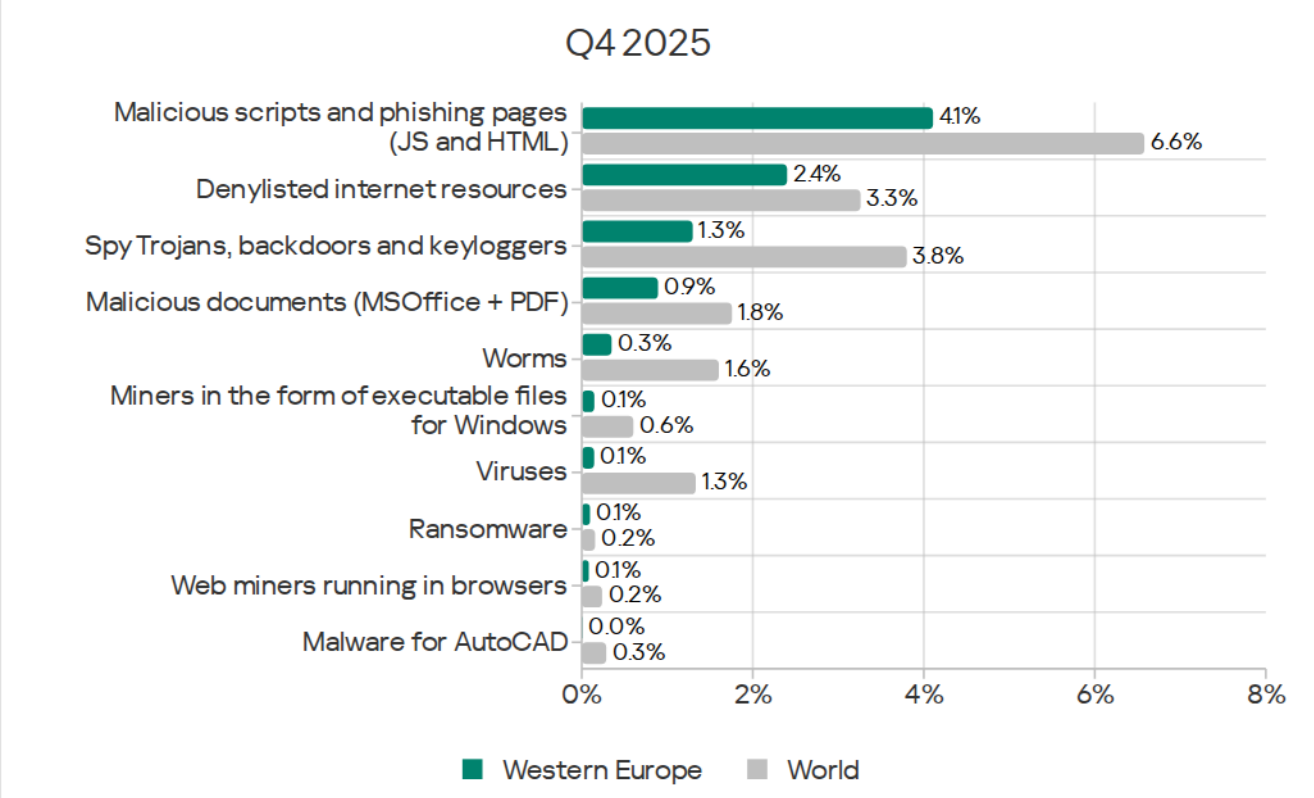


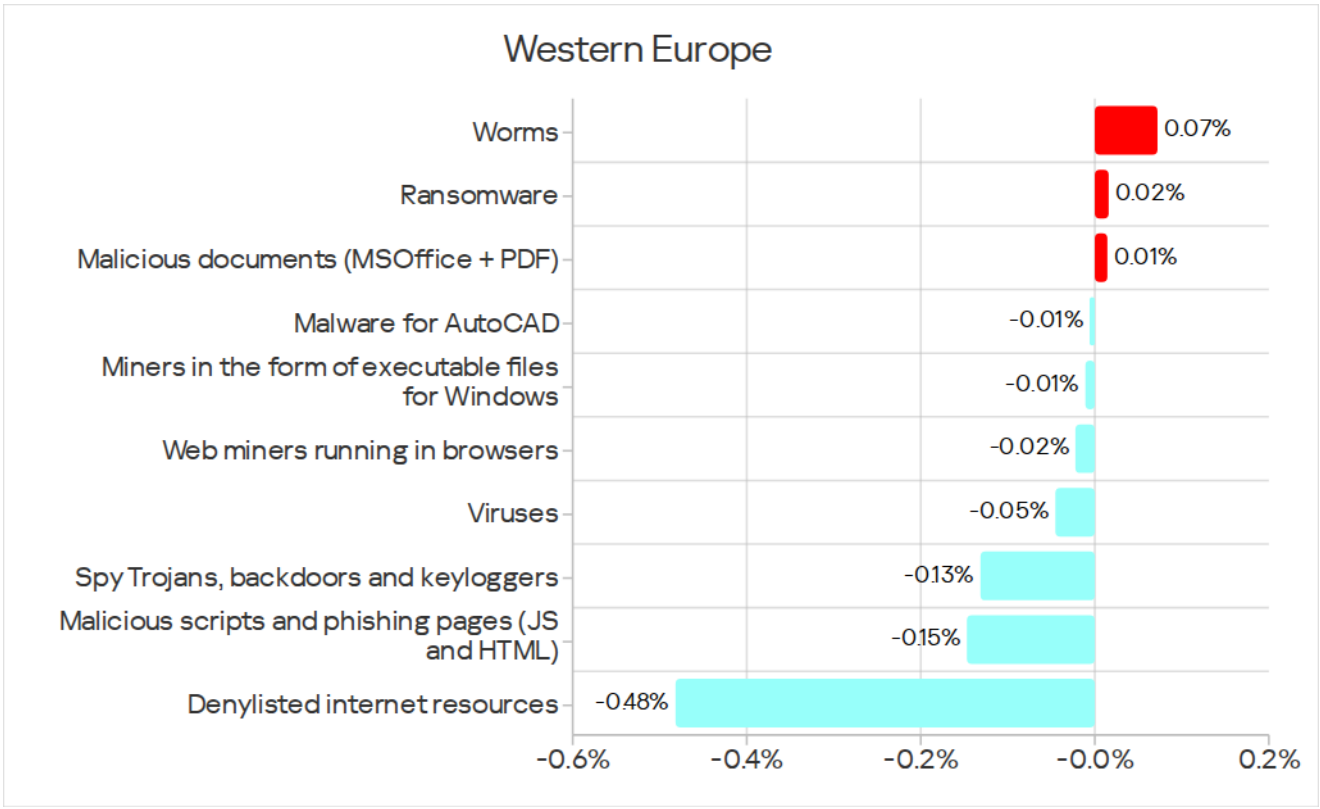

The manufacturing industry led all other industries for this indicator. This source of threats is also relevant for electric power and the engineering and ICS integrators industry.

The main categories of threats that were blocked in network folders in the region were spyware, worms, and malicious documents.




## Threat categories






For all threat categories, the region's figures remained below global averages.

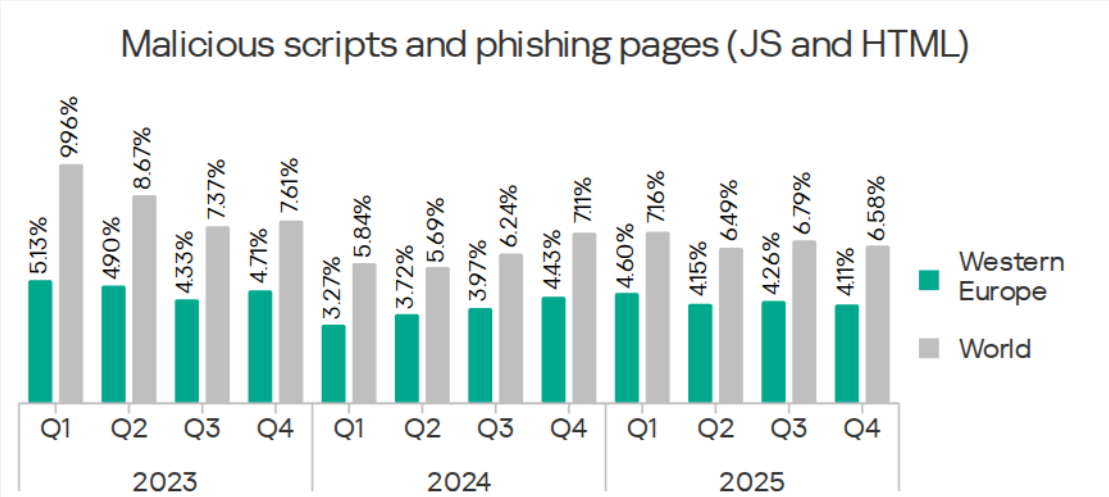
The figures decreased for all categories of threats except worms, ransomware, and malicious documents.

Western Europe's highest ranking globally across all categories of threats that were blocked on ICS computers was for denylisted internet resources, at 9th place. Based on the metrics for malicious documents, and malicious scripts and phishing pages, the region ranked 11th.

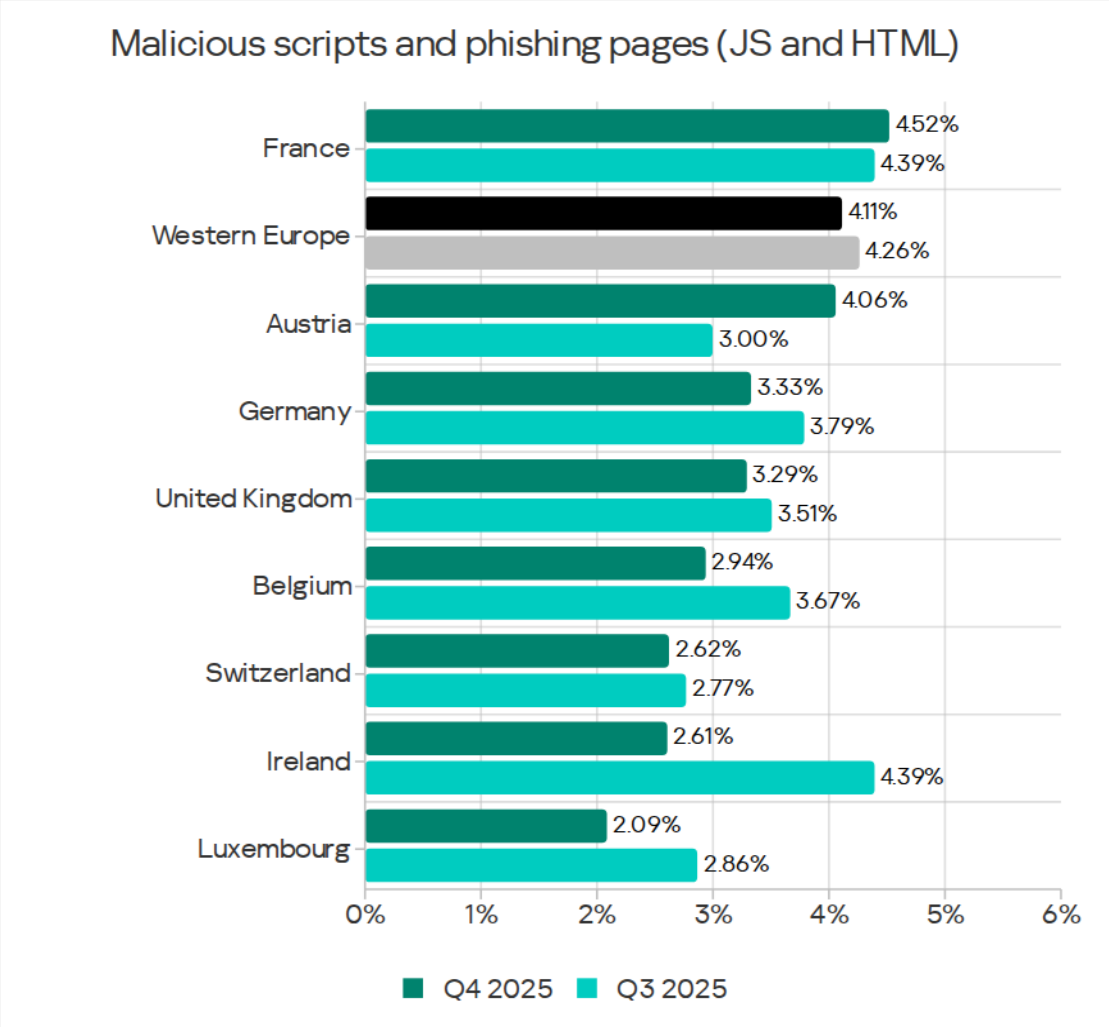
## Malicious scripts and phishing pages

Western Europe ranked 11th among regions by the percentage of ICS computers on which malicious scripts and phishing pages were blocked, at 4.11%. This figure was 1.6 times higher than in Northern Europe, which had the lowest rate.

This metric typically fluctuates across the region; it decreased in Q4 2025.




Among countries in the region, France led in the percentage of ICS computers on which malicious scripts and phishing pages were blocked, with 4.52%. This metric increased in the following two countries over the quarter: France and Austria (by a factor of 1.35 in Austria).

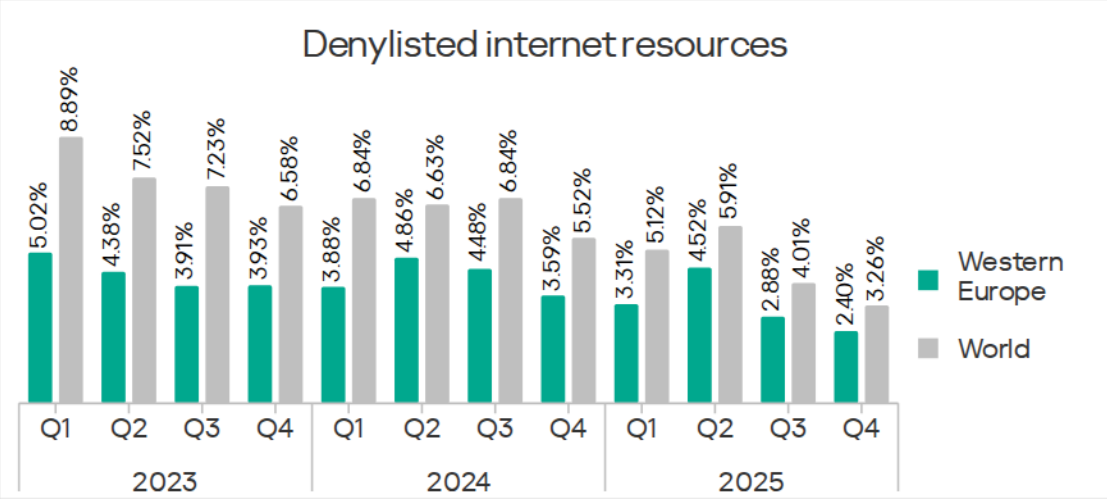


The main sources of malicious scripts and phishing pages were the internet and email.

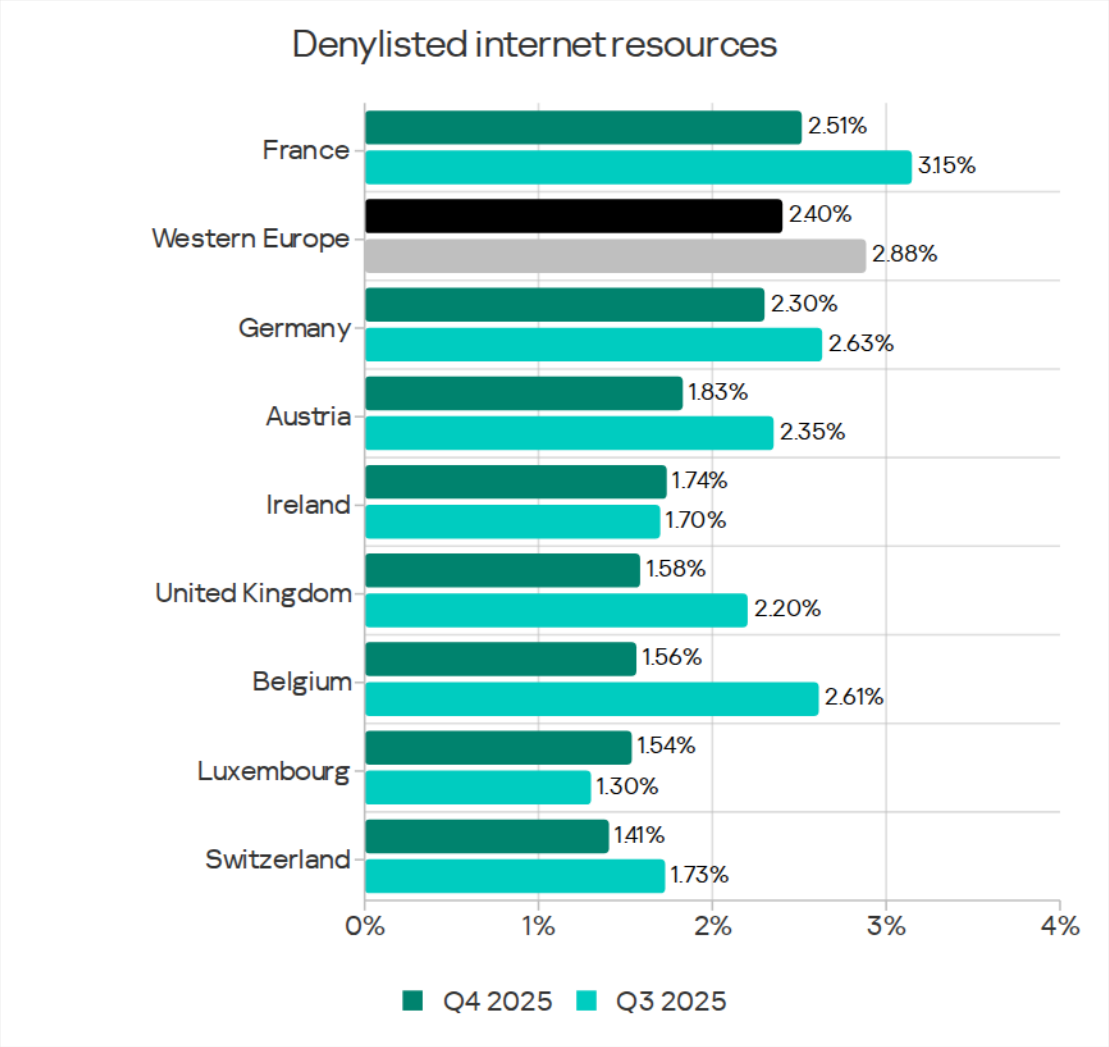
## Denylisted internet resources

By percentage of ICS computers on which denylisted internet resources were blocked, Western Europe ranked ninth globally. This was the region's highest position in the global rankings – in terms of both threat sources and categories.

The metric in the region fluctuates. In Q4 2025, the figure decreased to 2.4%, which was 1.4 times higher than in Northern Europe, which had the lowest figure.




Among countries of the region, France led with 2.51% in the percentage of ICS computers on which denylisted internet resources were blocked. Over the quarter, this figure increased only in Ireland and Luxembourg.

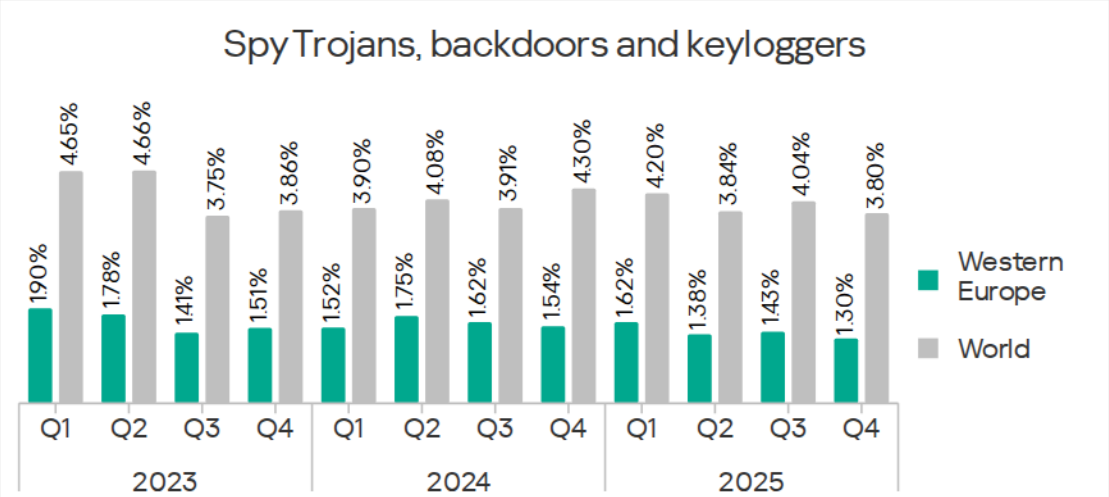



The main sources of malicious scripts and phishing pages were the internet and email. France led the region in internet threats.

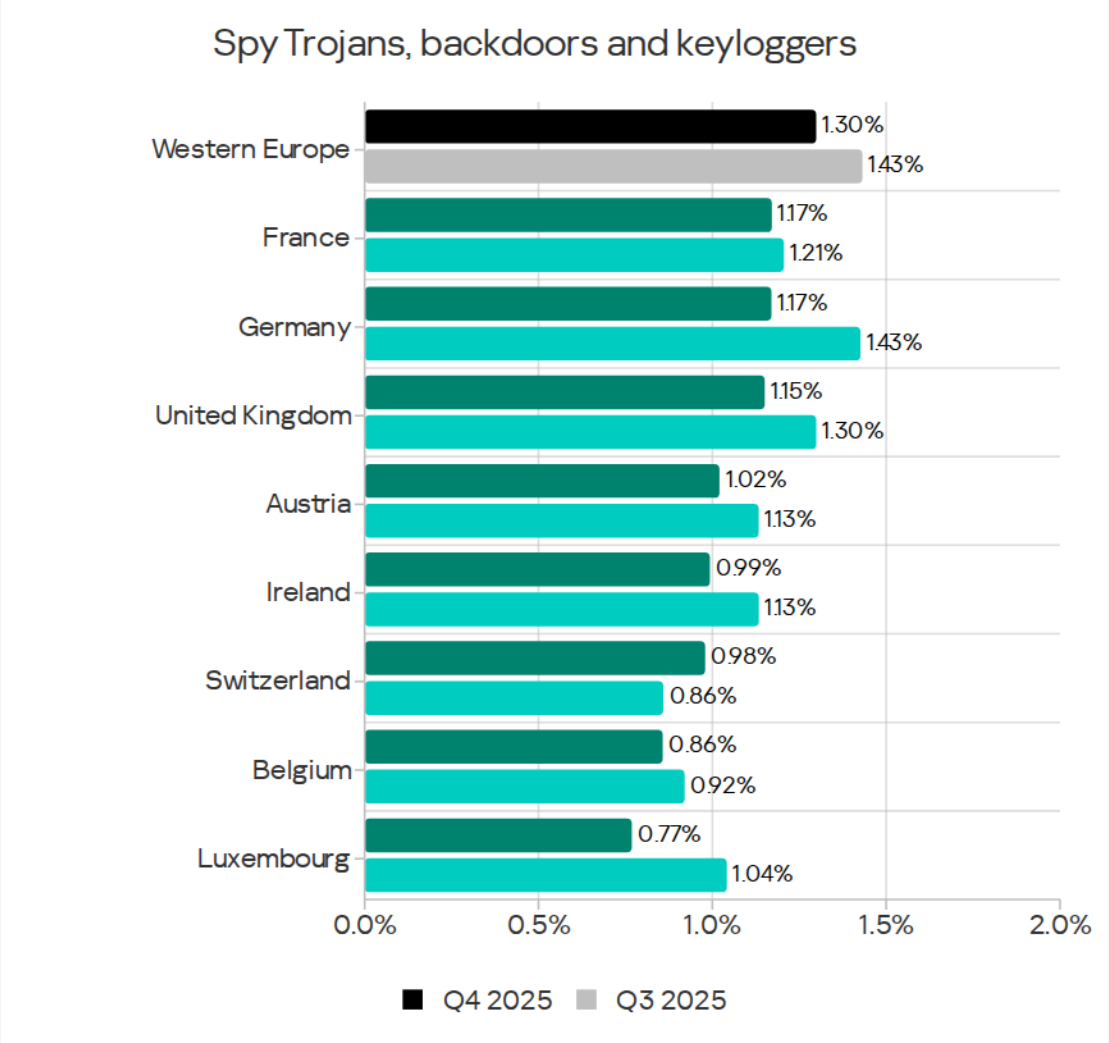
## Spyware

By the percentage of ICS computers on which spyware was blocked, Western Europe ranked 13th (second-to-last) with 1.30%. This was slightly higher than the figure in Northern Europe, which ranked last for this indicator.

This metric typically fluctuates across the region; it decreased in Q4 2025.




Among the region's countries, France and Germany both led with 1.17% in the percentage of ICS computers on which spyware was blocked. Over the quarter, this figure increased only in Switzerland.

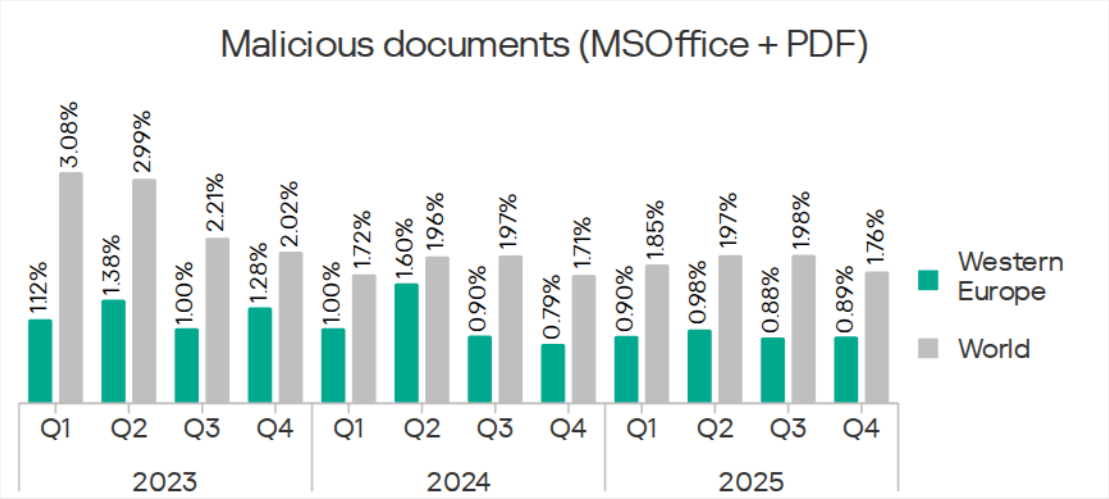


The main channel through which spyware spread in the region was email.

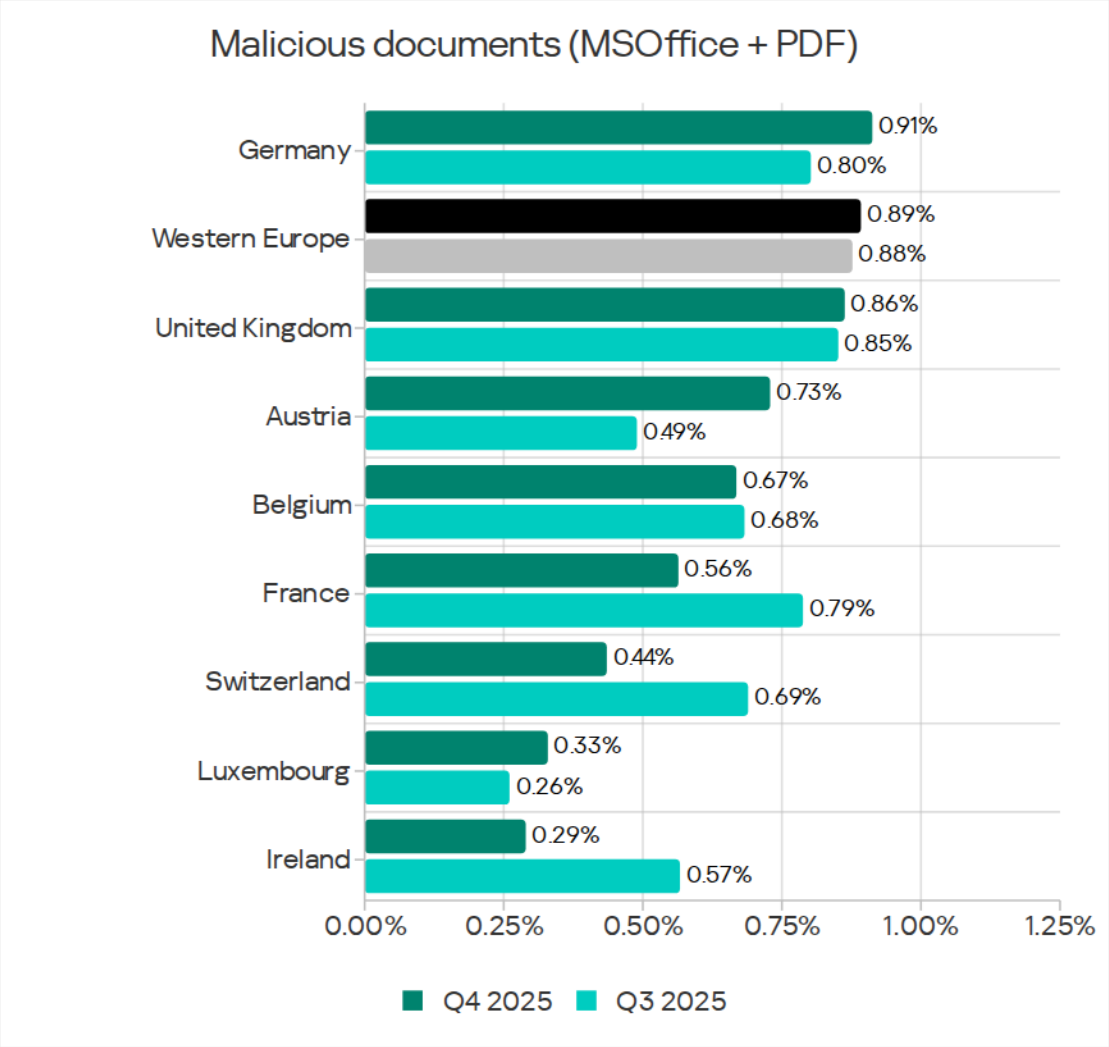
## Malicious documents

By the percentage of ICS computers on which malicious documents were blocked, Western Europe ranked 11th globally with 0.89%. This was 1.9 times higher than in Northern Europe, which had the lowest percentage value.

This metric typically fluctuates in the region; in Q4 2025, it increased.




Among the region's countries, Germany led with 0.91% in the percentage of ICS computers on which malicious documents were blocked. Over the quarter, this figure increased in Germany, the United Kingdom, Luxembourg, and Austria. In Austria, the figure increased by a factor of 1.49.

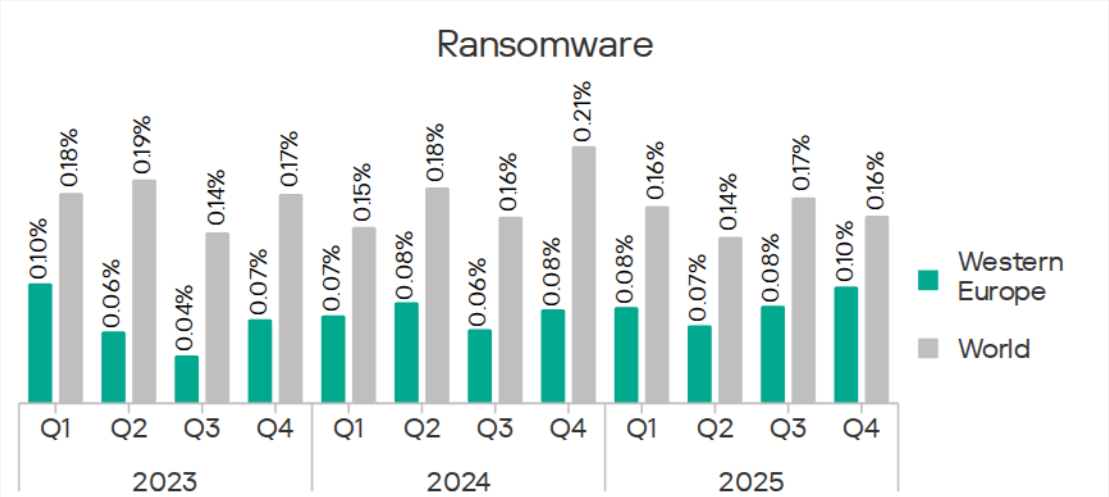



The main channel through which malicious documents were spread in the region was email.

## Ransomware

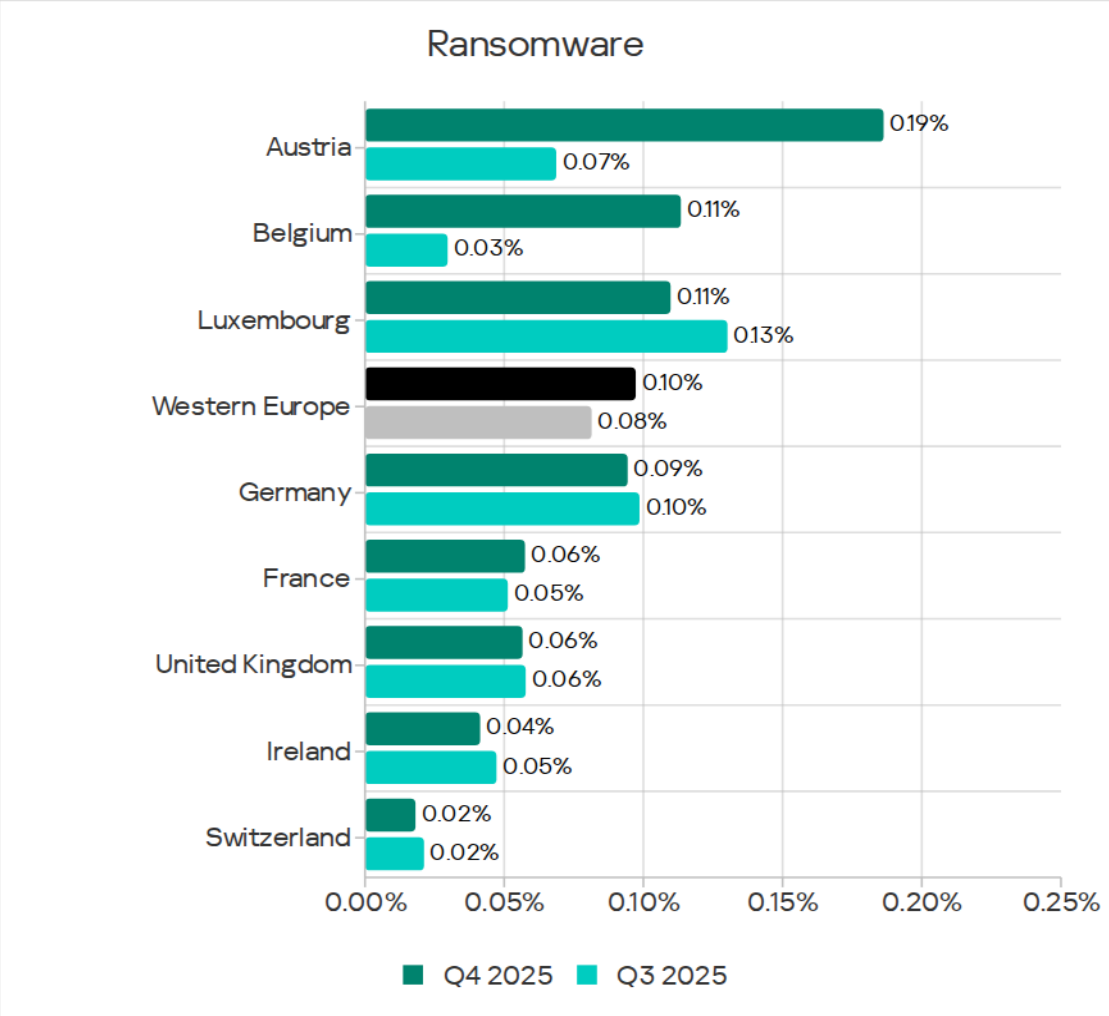
By the percentage of ICS computers on which ransomware was blocked, Western Europe ranked 12th globally with 0.10%. This was two times higher than in Northern Europe, which had the lowest rate.

This metric typically fluctuates in the region; in Q4 2025, it increased slightly.




Among the region's countries, Austria led with 0.19% in the percentage of ICS computers on which ransomware was blocked. In this country, the indicator grew by a factor of 2.71.

Belgium ranked second with 0.11%; the figure increased by a factor of 3.67.

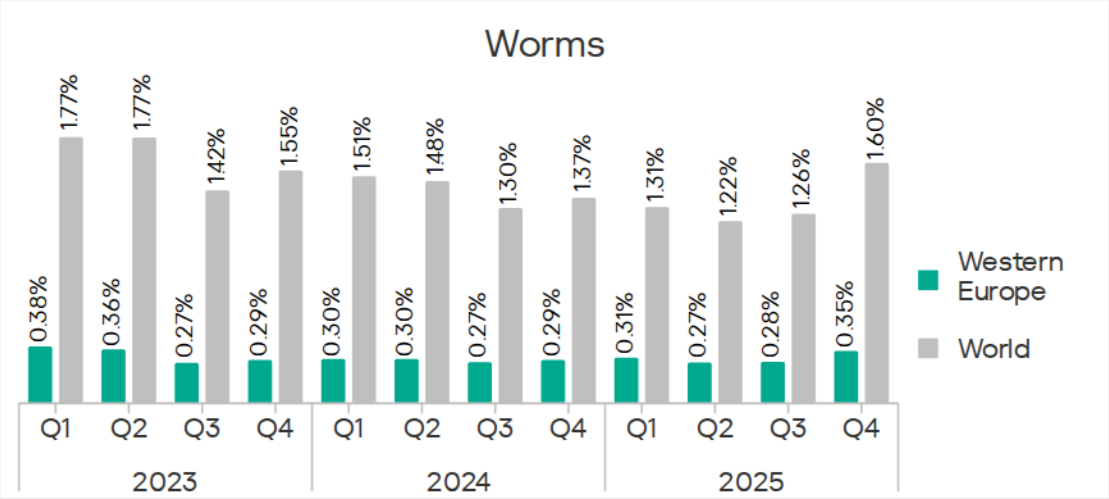


You will recall that Austria also led all other countries of the region in terms of threats from email clients in Q4 2025. This country also showed sharp growth in the indicators for malicious scripts and phishing pages, and malicious documents.

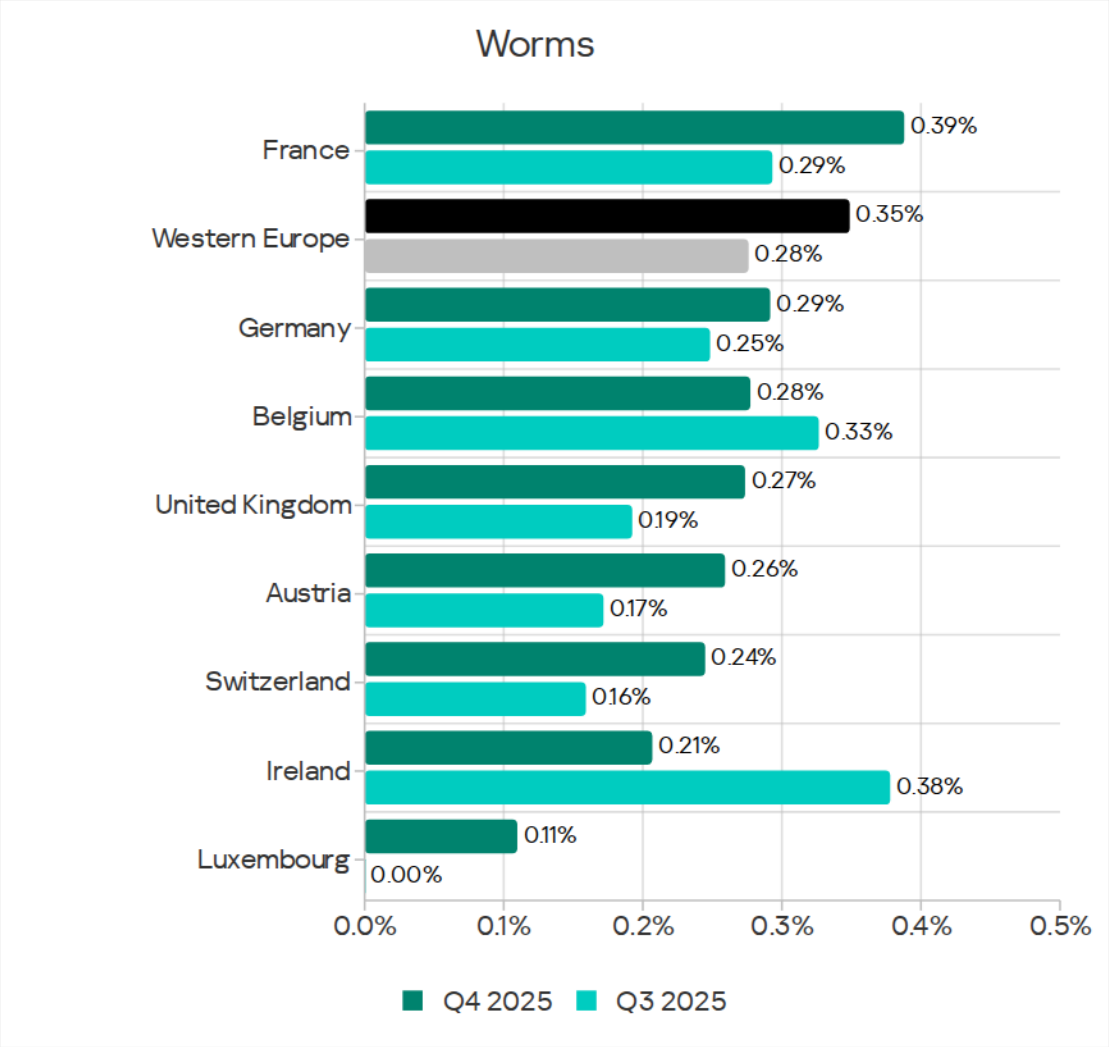
## Worms

In terms of the percentage of ICS computers on which worms were blocked, Western Europe ranked 13th with 0.35%. This figure was 1.1 times higher than in Northern Europe, which had the lowest percentage among all regions.

In Q4 2025, the worm metric grew across all regions due to the latest wave of phishing campaigns known as Curriculum-vitae-catalina which we described earlier. Western Europe ranks next to last among all regions based on the growth of this indicator.




Among countries in the region, France led with 0.39% in the percentage of ICS computers on which worms were blocked. Over the quarter, the figure increased in all countries except Belgium and Ireland.

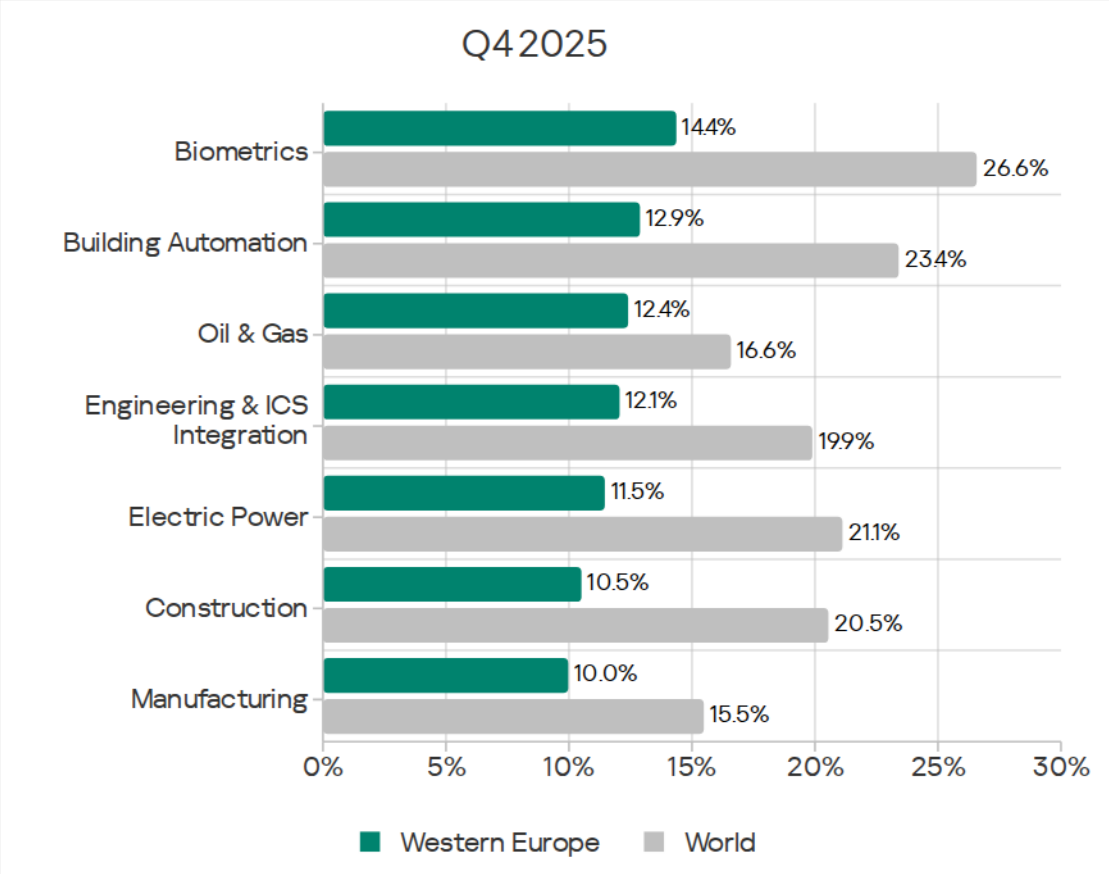



Worms in the region were spread over the internet, email, and on removable media. In Q4 2025, worms were spread predominately over email due to a phishing attack.

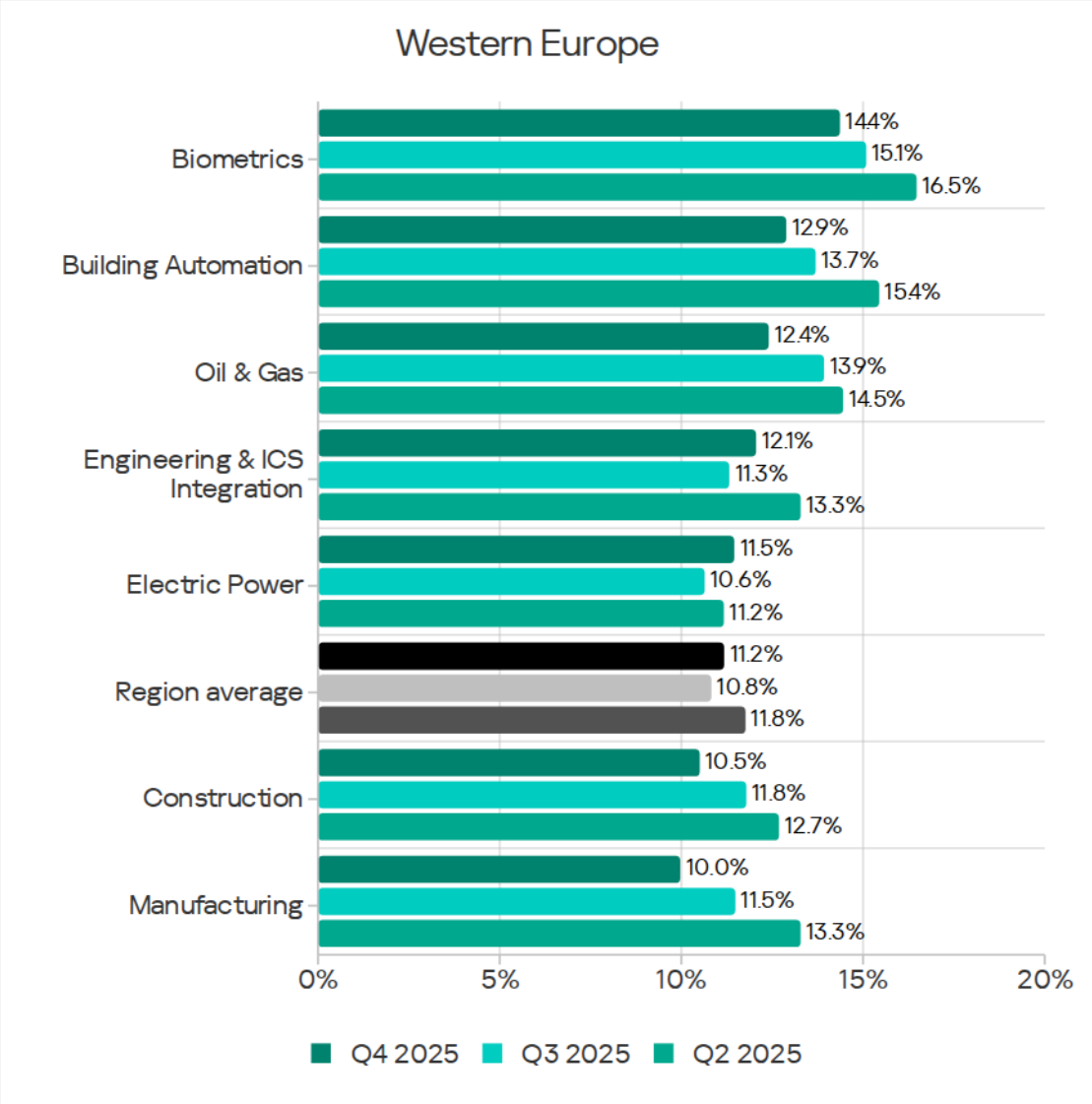
## Industries

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

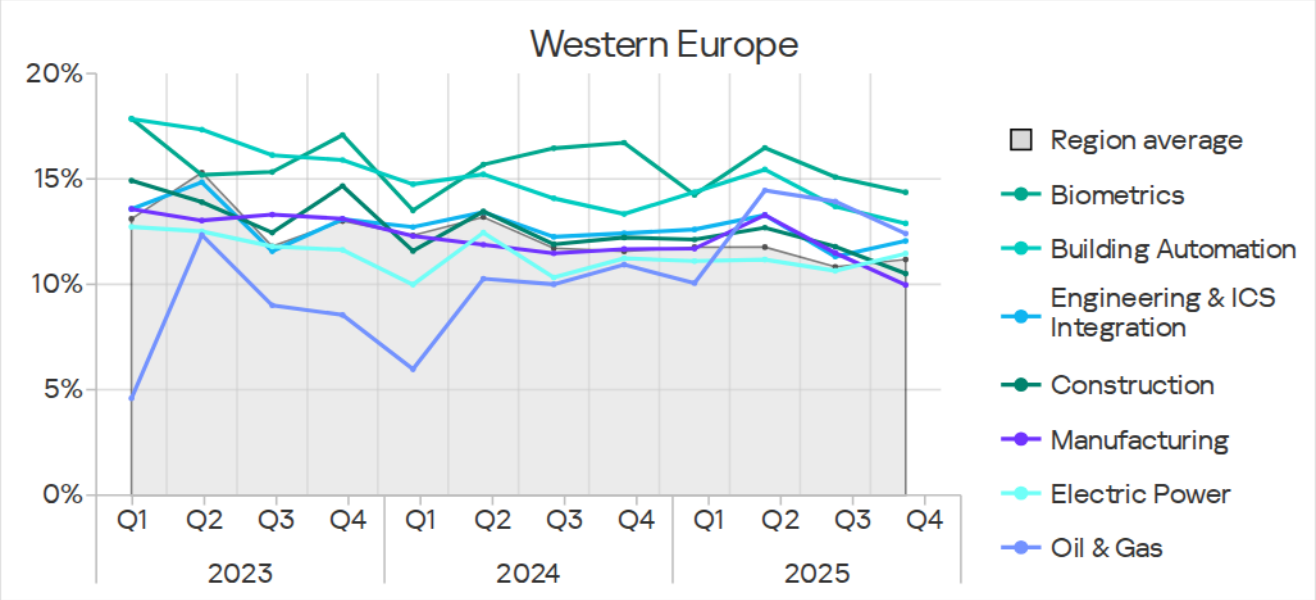
Figures for all industries in the region remained well below the global averages.




In Q4 2025, the indicator increased in two of the industries reviewed in the region: engineering and ICS integrators, 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. Red signifies that the figure is close to the maximum.

**Threat source indicators for industries in Western Europe, Q4 2025**

| Industry / Threat source | Biometrics | Building Automation | Engineering & ICS Integration | Electric Power | Oil & Gas | Construction | Manufacturing | Category metric in region |
|---|---|---|---|---|---|---|---|---|
| Internet | 4.97% | 5.64% | 6.81% | 6.19% | 7.09% | 5.76% | 5.35% | 6.02% |
| Email clients | 4.42% | 3.42% | 1.53% | 1.03% | 0.51% | 1.23% | 0.64% | 1.53% |
| Removable media | 0.18% | 0.09% | 0.06% | 0.12% | — | 0.14% | 0.09% | 0.07% |
| Network folders | — | — | 0.02% | 0.02% | — | — | 0.04% | 0.01% |
| **Industry metric in region** | 14.34% | 12.87% | 12.05% | 11.44% | 12.37% | 10.53% | 9.99% | |

**Threat category indicators for industries in Western Europe, Q4 2025**

| Industry / Threat type | Biometrics | Building Automation | Engineering & ICS Integration | Electric Power | Oil & Gas | Construction | Manufacturing | Category metric in region |
|---|---|---|---|---|---|---|---|---|
| Denylisted internet resources | 1.66% | 2.24% | 2.54% | 2.51% | 3.80% | 2.10% | 1.93% | 2.40% |
| Malicious scripts and phishing pages (JS and HTML) | 6.08% | 5.22% | 4.60% | 3.90% | 5.06% | 4.05% | 3.12% | 4.11% |
| Malicious documents (MSOffice + PDF) | 2.03% | 1.79% | 1.01% | 0.63% | 0.51% | 0.77% | 0.39% | 0.89% |
| Spy Trojans, backdoors and keyloggers | 2.21% | 2.27% | 1.36% | 1.39% | 2.53% | 1.23% | 1.33% | 1.30% |
| Ransomware | 0.18% | 0.16% | 0.13% | 0.06% | — | 0.07% | 0.04% | 0.10% |
| Miners in the form of executable files for Windows | 0.18% | 0.20% | 0.15% | 0.12% | 0.25% | 0.19% | 0.13% | 0.15% |
| Web miners running in browsers | 0.18% | 0.12% | 0.10% | 0.06% | 0.25% | 0.19% | 0.09% | 0.08% |
| Malware for AutoCAD | — | — | 0.02% | — | — | 0.17% | — | 0.01% |
| Worms | 0.37% | 0.74% | 0.33% | 0.46% | 1.01% | 0.29% | 0.47% | 0.35% |
| Viruses | 0.74% | 0.25% | 0.16% | 0.32% | 0.51% | 0.22% | 0.26% | 0.15% |
| **Industry metric in region** | 14.34% | 12.87% | 12.05% | 11.44% | 12.37% | 10.53% | 9.99% | |

In Q4 2025, global ranking by percentage of ICS computers on which malicious objects were blocked in various industries, Western Europe was one of the top three regions with the lowest figures in all industries except electric power.

The indicators for malicious documents and ransomware increased in Western Europe. Based on the figures for both categories — ransomware and malicious documents — engineering and ICS integrators ranked first among all industries.

The engineering and ICS integrators industry ranked third in the percentage of attacked ICS computers and led all other industries in the region based on the indicators for threats from the internet and denylisted internet resources. The electric power industry ranked second for these indicators. These high rankings

of industries suggest that there are weak restrictions governing outbound network traffic from OT networks to external networks.

The manufacturing industry ranked last in the percentage of attacked computers but led all other industries in terms of threats in network folders. This industry ranked second in worms and third in viruses.

**Biometrics**

Western Europe ranked 10th globally for the percentage of ICS computers on which malicious objects were blocked in biometrics.

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

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

**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 occupied the following positions:

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

**Engineering and ICS integrators**

Western Europe ranked 12th regionally for the percentage of ICS computers on which malicious objects were blocked in engineering and ICS integration.

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

- First place in the percentage of ICS computers on which internet threats were blocked.
- Third place in threats from email clients and network folders.
- First place in the percentage of ICS computers on which denylisted internet resources were blocked.
- Second in malware for AutoCAD.
- Third for malicious scripts and phishing pages, malicious documents, and ransomware.

**Electric 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 regional cross-industry rankings, the electrical energy industry ranked:

- Second place in the percentage of ICS computers on which threats from the internet and network folders were blocked.
- Third place in removable media threats.
- Second in the percentage of ICS computers on which denylisted internet resources and viruses were blocked.
- Third in spyware and worms.

**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 ranked:

- Second in the percentage of ICS computers on which threats from removable media were blocked.
- Third for internet threats.
- First in the percentage of ICS computers on which web miners and malware for AutoCAD were blocked.
- Second for miners in the form of executable files.

**Manufacturing**

Western Europe ranked last among all regions in the percentage of ICS computers on which malicious objects were blocked in the manufacturing industry.

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

- First in the percentage of ICS computers on which threats from network folders were blocked.

- Second for worms.
- Third in terms of viruses.

# 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 were blocked.

Northern Europe was also last (14th) in most rankings of regions based on the percentage of ICS computers on which various categories of malicious objects from various sources were blocked.

Northern Europe occupied higher spots in the rankings for the following threat categories:

- Ninth in miners in the form of executable files for Windows.
- Eleventh in web miners.
- Twelfth in viruses.

Northern Europe ranked 13th in terms of threats that were blocked on ICS computers when connecting removable media.

Northern Europe's highest position in the rankings both by source and by threat category was for miners in the form of executable files for Windows.

Based on the figures for the manufacturing industry, Northern Europe ranked second among regions by the percentage of ICS computers on which miners in the form of Windows executable files were blocked, and third for 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.

In Q4 2025, of all the threat categories in the region, a slight increase in the metrics for the quarter was seen only for worms, viruses, and web miners.

The figure for worms in Q4 grew across all regions due to the latest wave of phishing campaigns known as Curriculum-vitae-catalina. Northern Europe ranked 11th in terms of the growth in this metric. The percentage of ICS computers on which worms were blocked increased across all surveyed industries in the region except for the construction industry. Among the region's countries, the only country where the figure for worms increased over the quarter was Finland, which saw a twofold increase.

The figure for viruses over the quarter increased in only one of the surveyed industries in the region: the engineering and ICS integrators industry. Among

the region's countries, the percentage of ICS computers on which viruses were blocked increased the most in Finland, which saw a threefold increase.

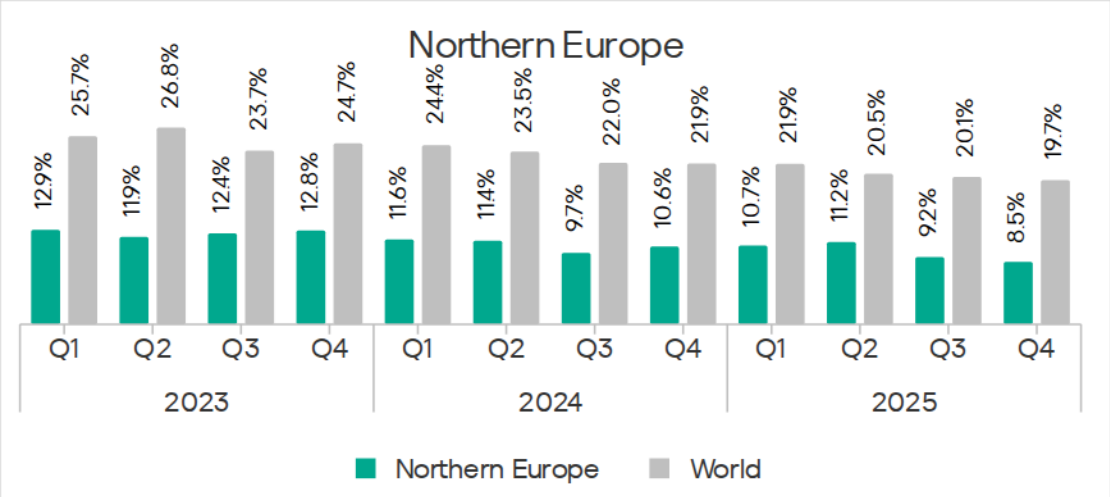
The figures for web miners over the quarter grew across all surveyed industries in the region. The most growth was seen in the manufacturing industry, which saw an increase by a factor of 3.3. Among the region's countries, the percentage of ICS computers on which web miners were blocked grew the most in Finland, which saw an increase by a factor of 3.5.

## Statistics across all threats

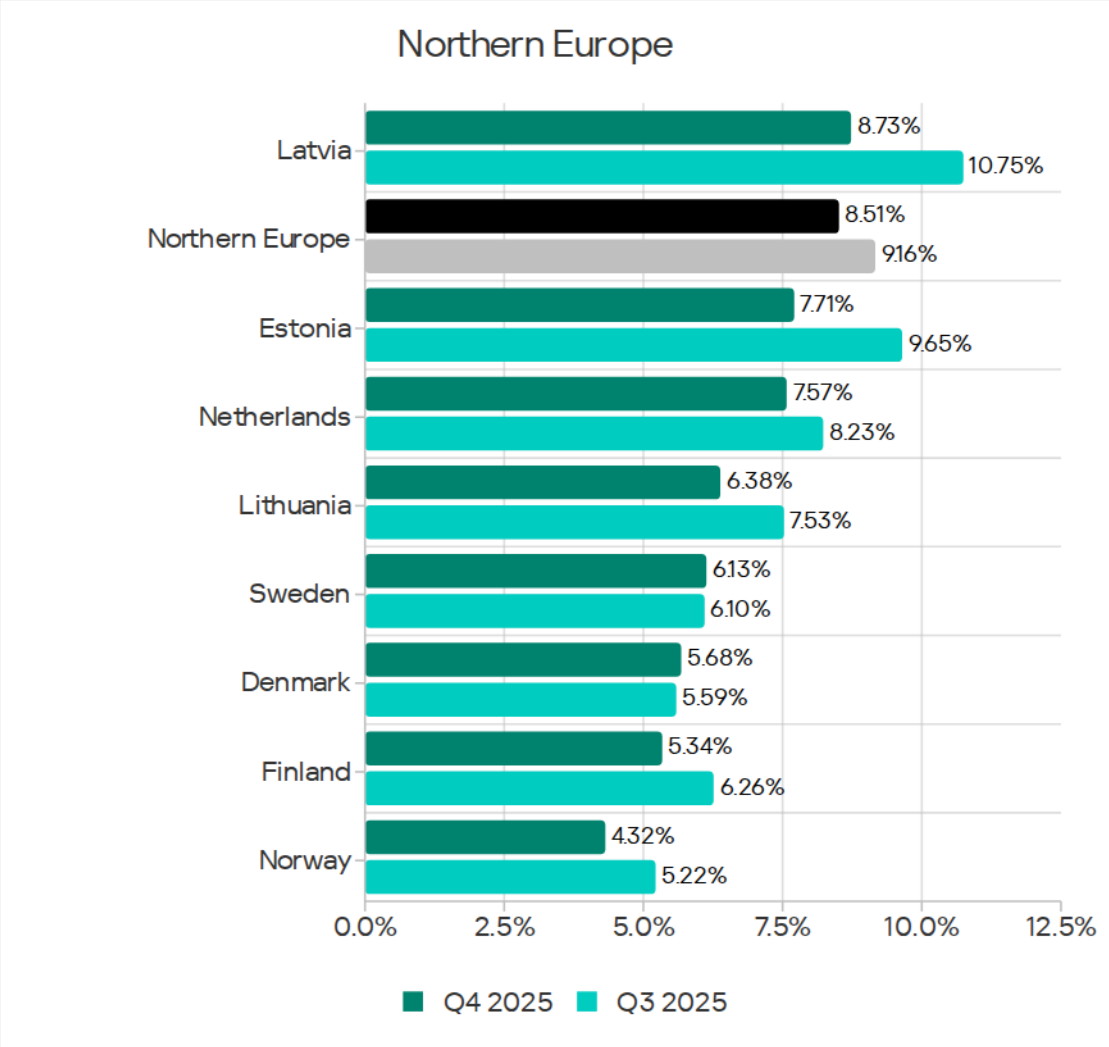
Northern Europe ranked 14th in the global ranking for the percentage of ICS computers on which malicious objects were blocked.

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

The percentage of ICS computers on which malicious objects were blocked in Q4 2025 in the region decreased from 9.2% to 8.5%.

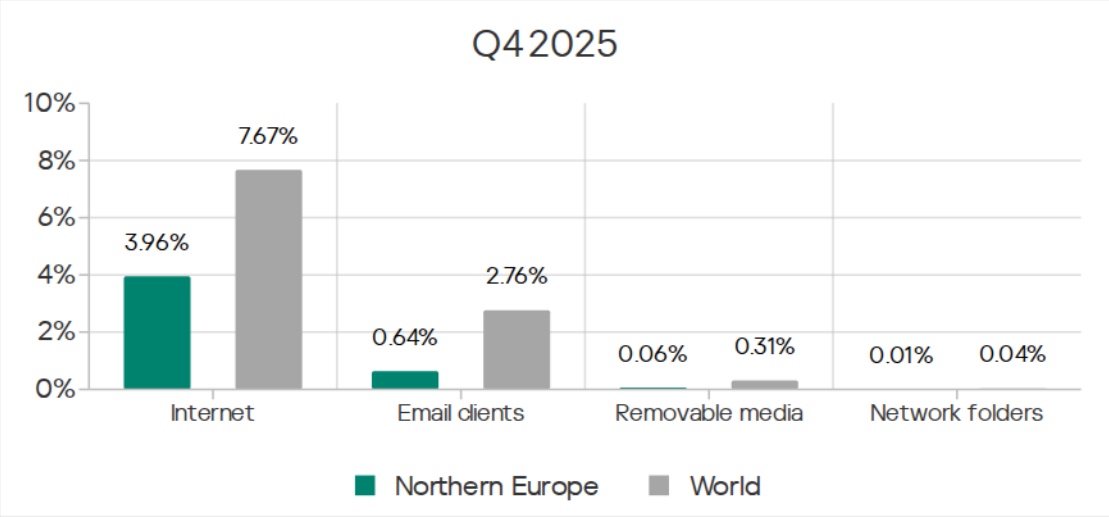



Among the region's countries, Latvia leads in the percentage of ICS computers on which malicious objects were blocked, at 8.73%. The lowest figure observed was in Norway at 4.32%. Over the quarter, this figure decreased across all countries with the exception of Sweden and Denmark.

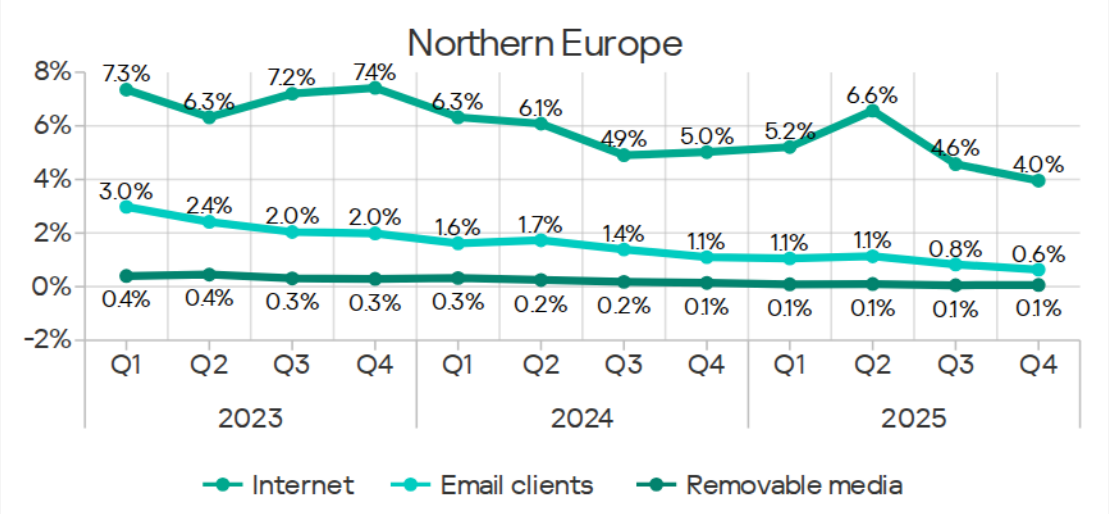



## Threat sources

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




In Q4 2025 in Northern Europe, the percentage of ICS computers on which malicious objects were blocked decreased for internet threats and email client threats. The figures for removable media and network folders remained unchanged.

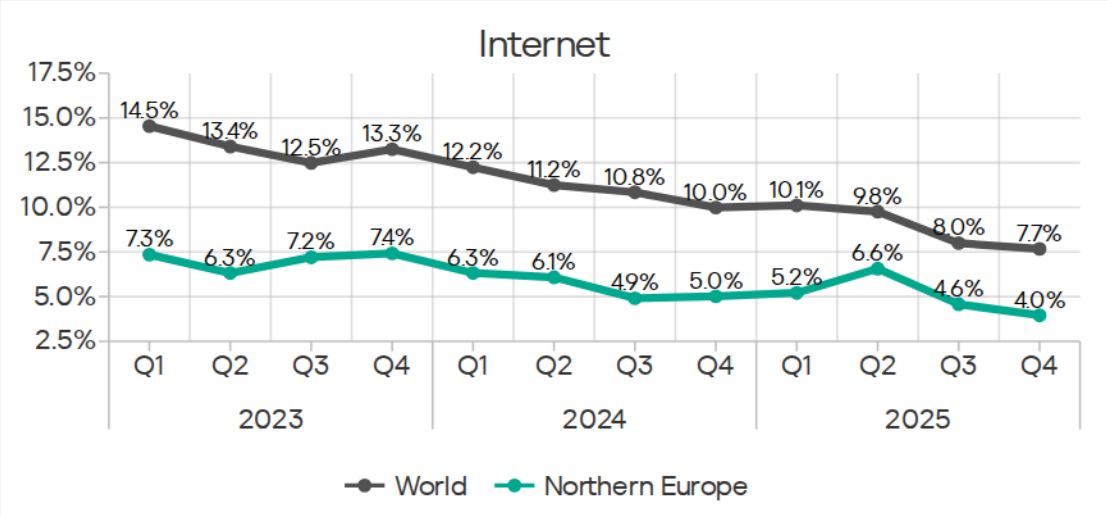



The dominant threat sources are the internet and email.

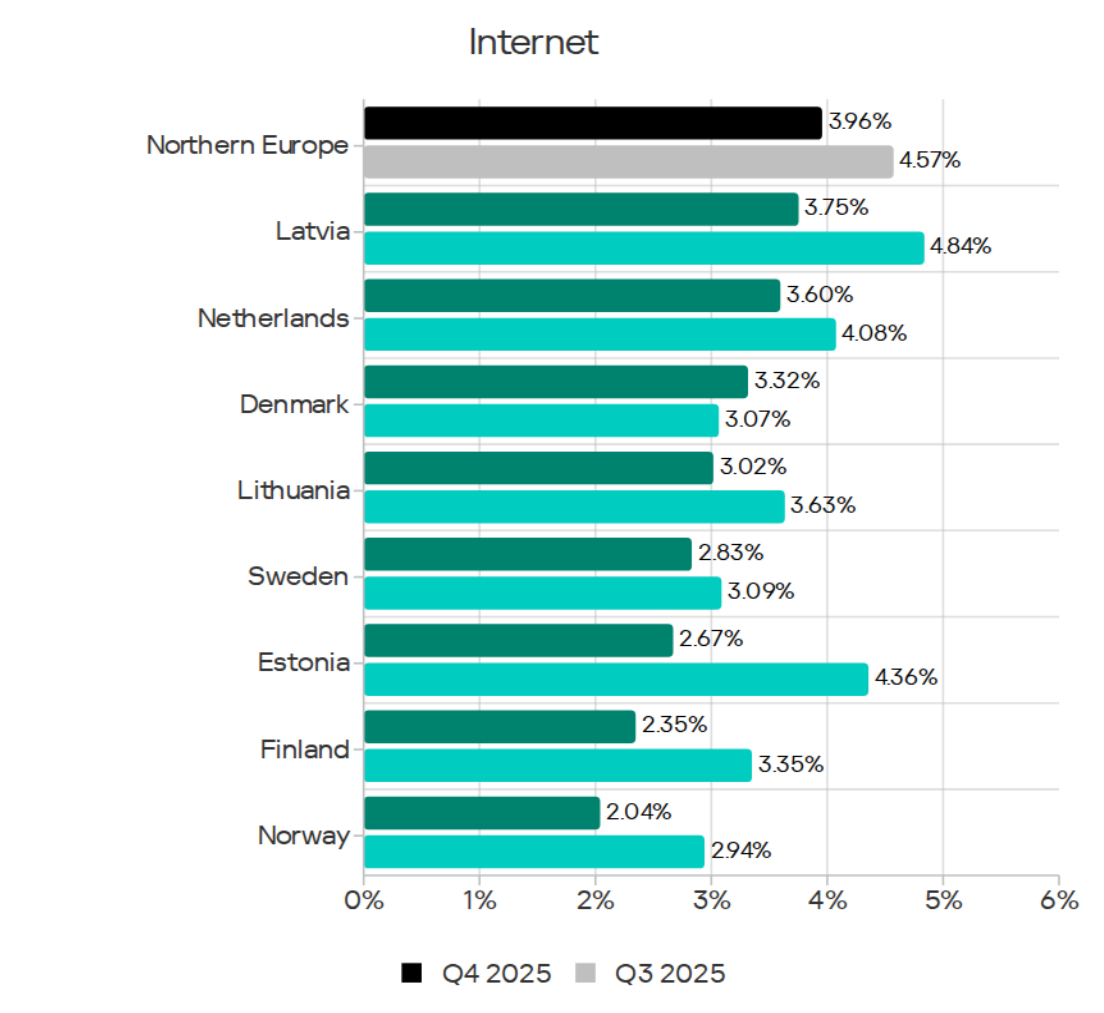
## Internet

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

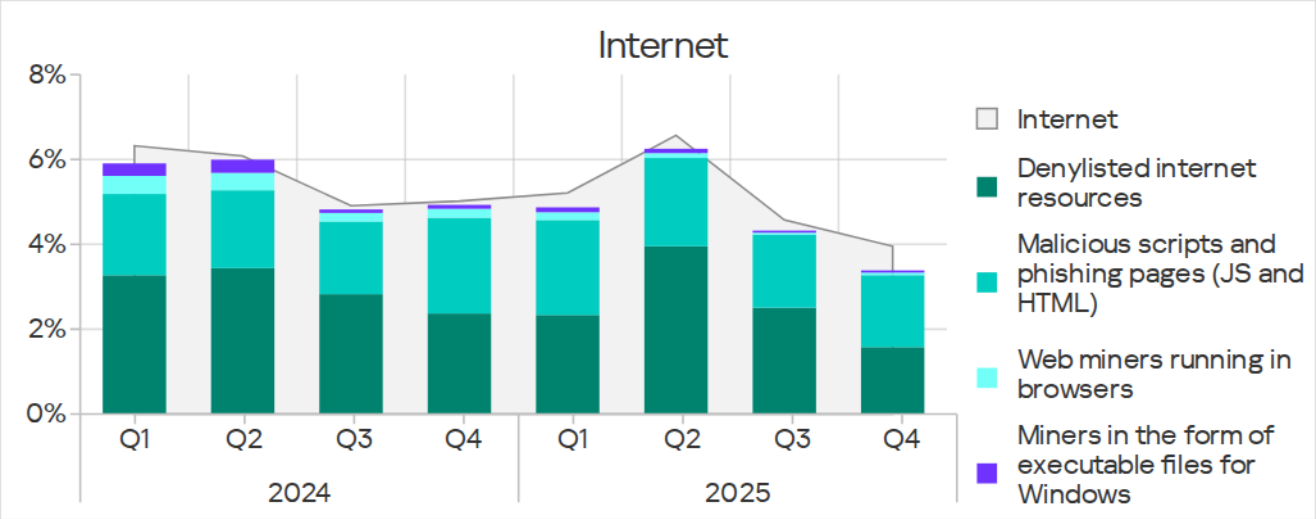
The region's figure declined for two consecutive quarters, dropping to its lowest level during the surveyed period at 3.96% in Q4 2025. We should note that the percentage of ICS computers on which internet threats were blocked decreased in all regions.




Across the region, the percentage of ICS computers on which internet threats were blocked ranged from 2.04% in Norway to 3.75% in Latvia. Over the quarter, this figure decreased across all countries in the region except for Denmark.



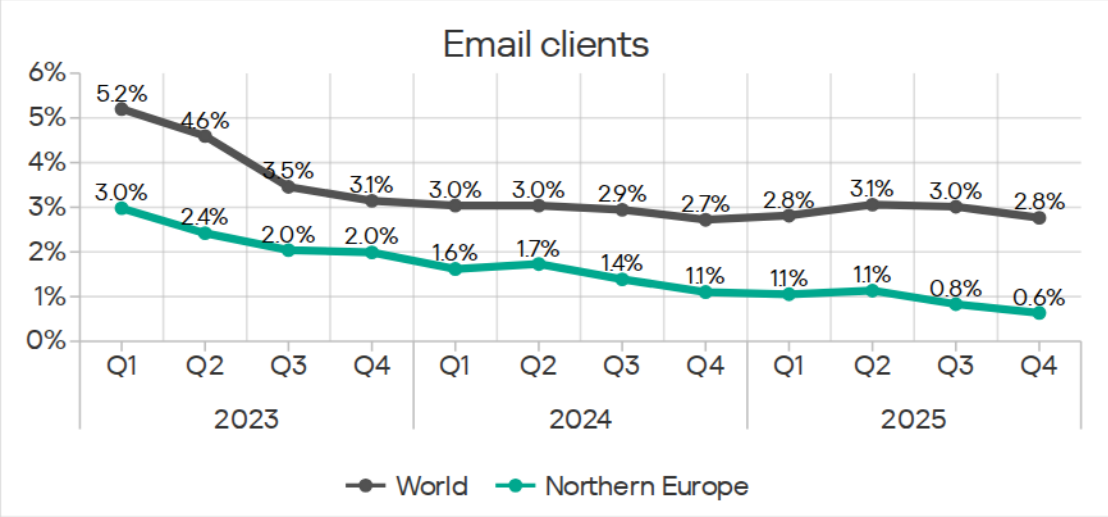
The main categories of internet threats blocked on ICS computers in the region were denylisted internet resources and malicious scripts and phishing pages.



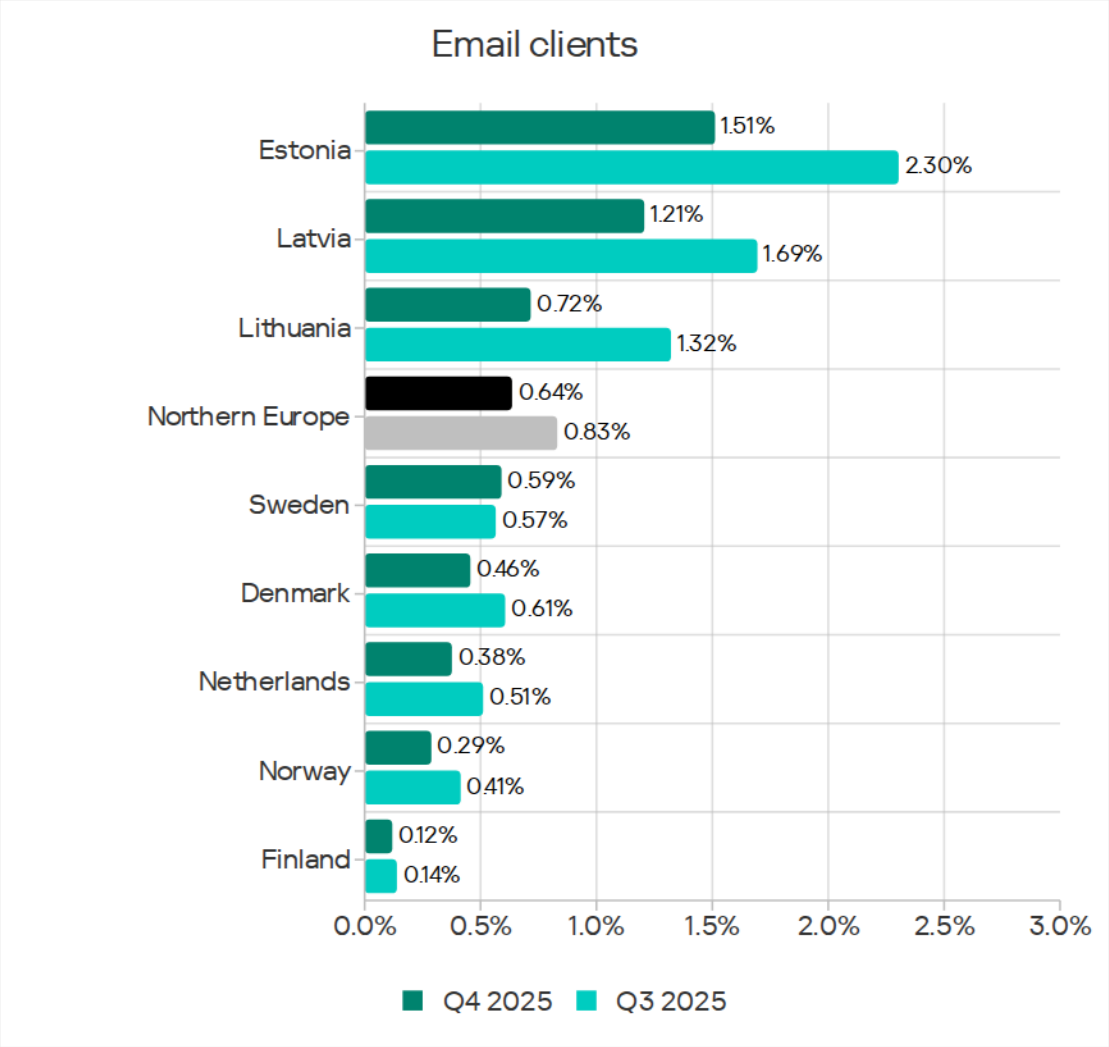

## Email clients

Based on the percentage of ICS computers on which threats from email clients were blocked, Northern Europe ranked 14th among all regions in Q4 2025.

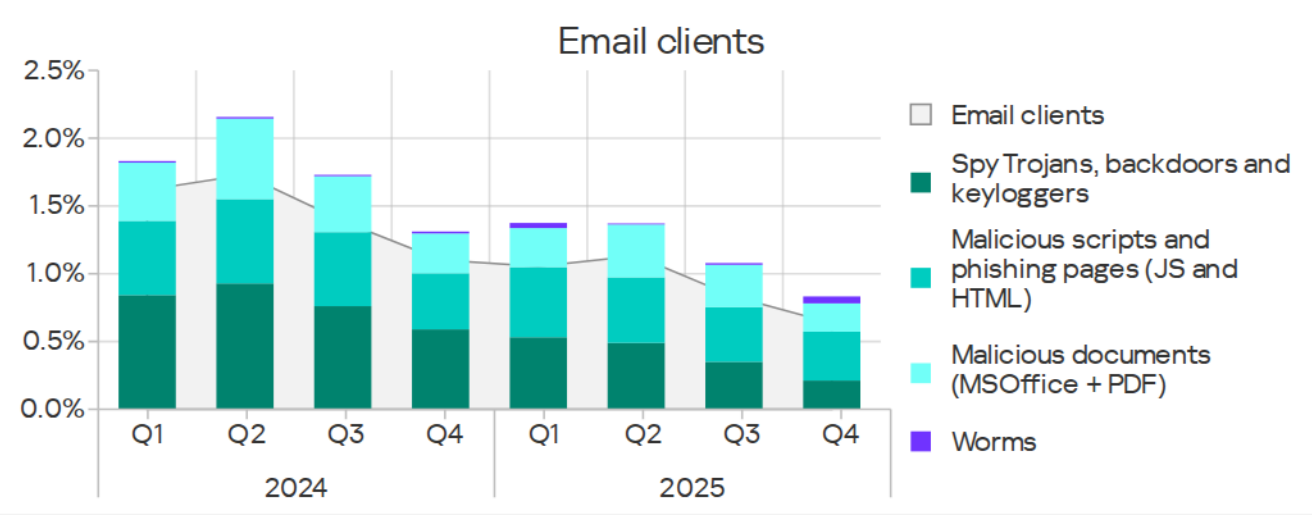
The figure decreased to 0.64% in the region over the quarter. This was the lowest figure seen during the surveyed period.




Among countries in the region, Estonia led in this metric with 1.51%. The lowest figure observed was in Finland at 0.12%. The figure for the quarter decreased across all countries in the region except for Sweden.



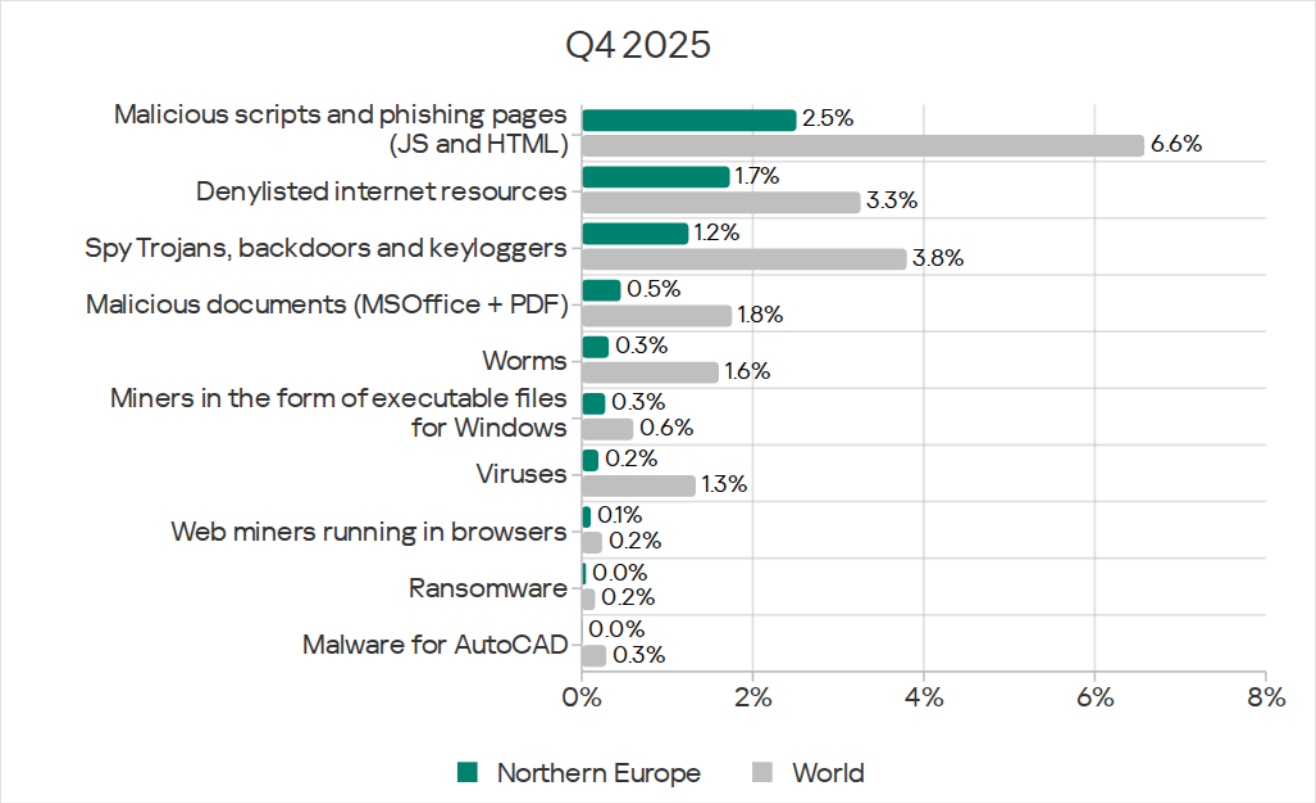

The main categories of email client threats blocked on ICS computers were malicious scripts and phishing pages, spyware, and malicious documents.

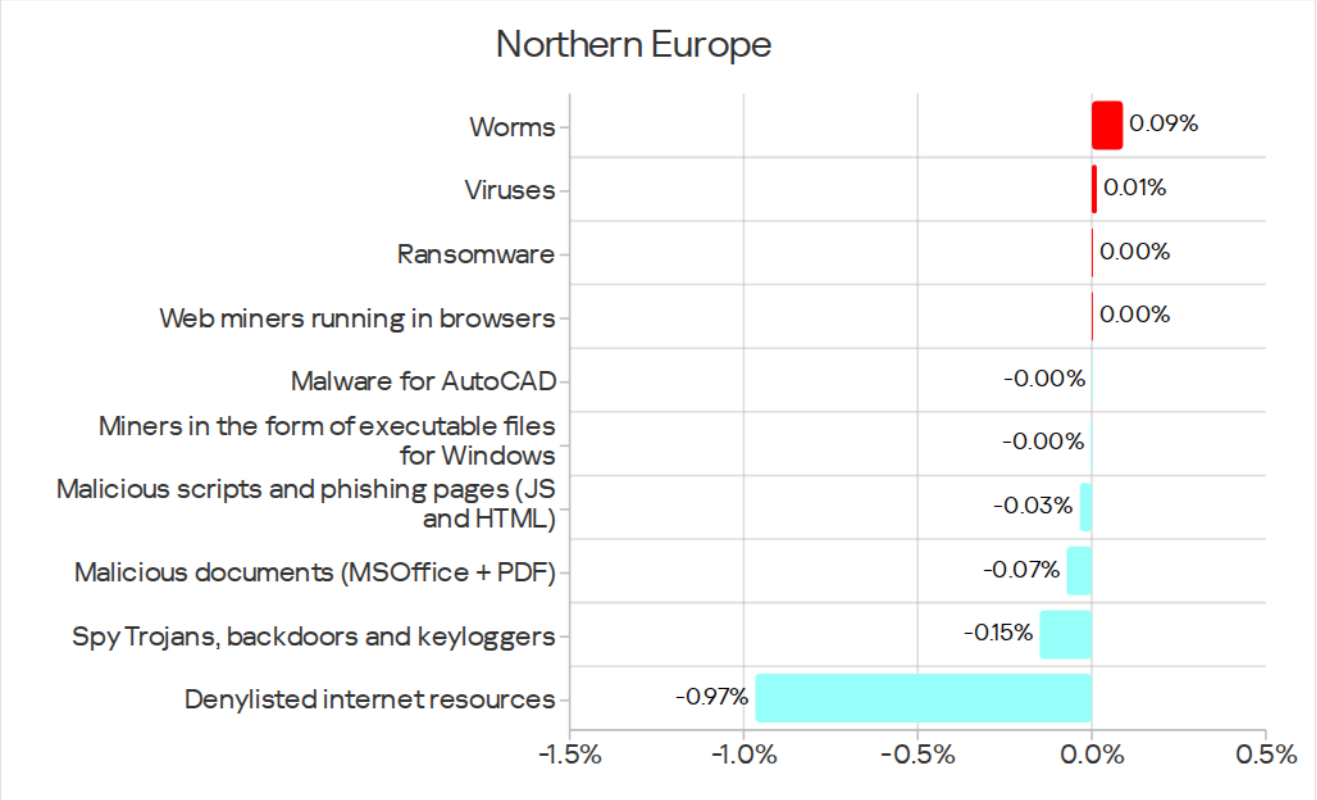


Q4 2025 saw an increase across all regions in the percentage of ICS computers on which worms from mail clients were blocked. This was connected with the latest wave of phishing campaigns known as Curriculum-vitae-catalina. In Northern Europe, these attacks peaked in November.

The hackers distributed phishing emails disguised as job applications. Disguised as a resume (Curriculum Vitae), these emails contained a malicious executable file, a remote administration backdoor worm known as Backdoor.MSIL.XWorm. Running that file caused system infection.

## Threat categories






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

Of all the threat categories, a slight increase in the figures over the quarter was seen for worms, viruses, ransomware, and web miners.

In most rankings of regions based on the percentage of ICS computers on which various categories of malicious objects were blocked, Northern Europe ranked 14th.

Northern Europe occupied higher positions in the rankings for the following threat categories:

- Ninth in miners in the form of executable files for Windows.
- Eleventh in web miners.
- Twelfth in viruses.

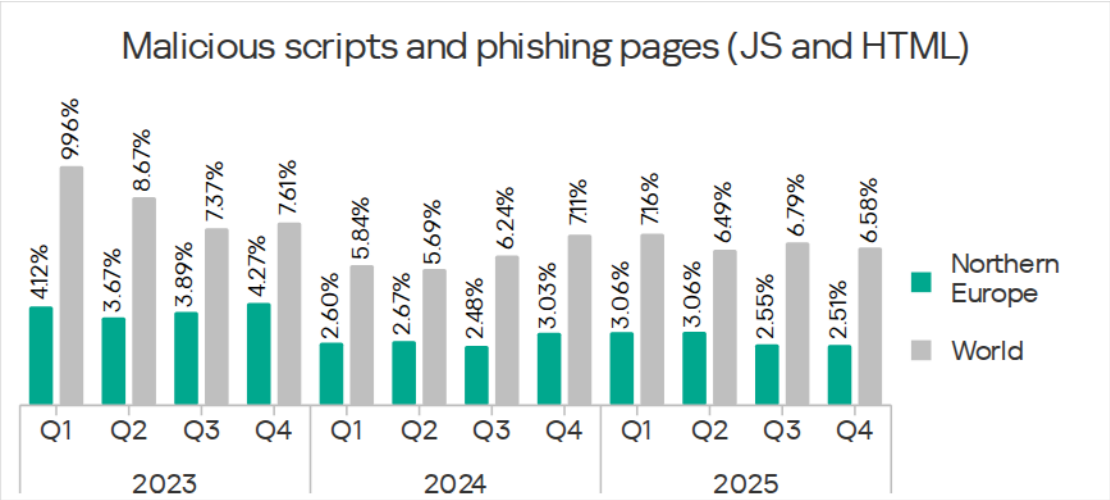
## Malicious scripts and phishing pages

The regional ranking of threat categories based on the percentage of ICS computers on which threats were blocked in Q4 2025 was led by malicious scripts and phishing pages, which knocked denylisted internet resources off the top spot.

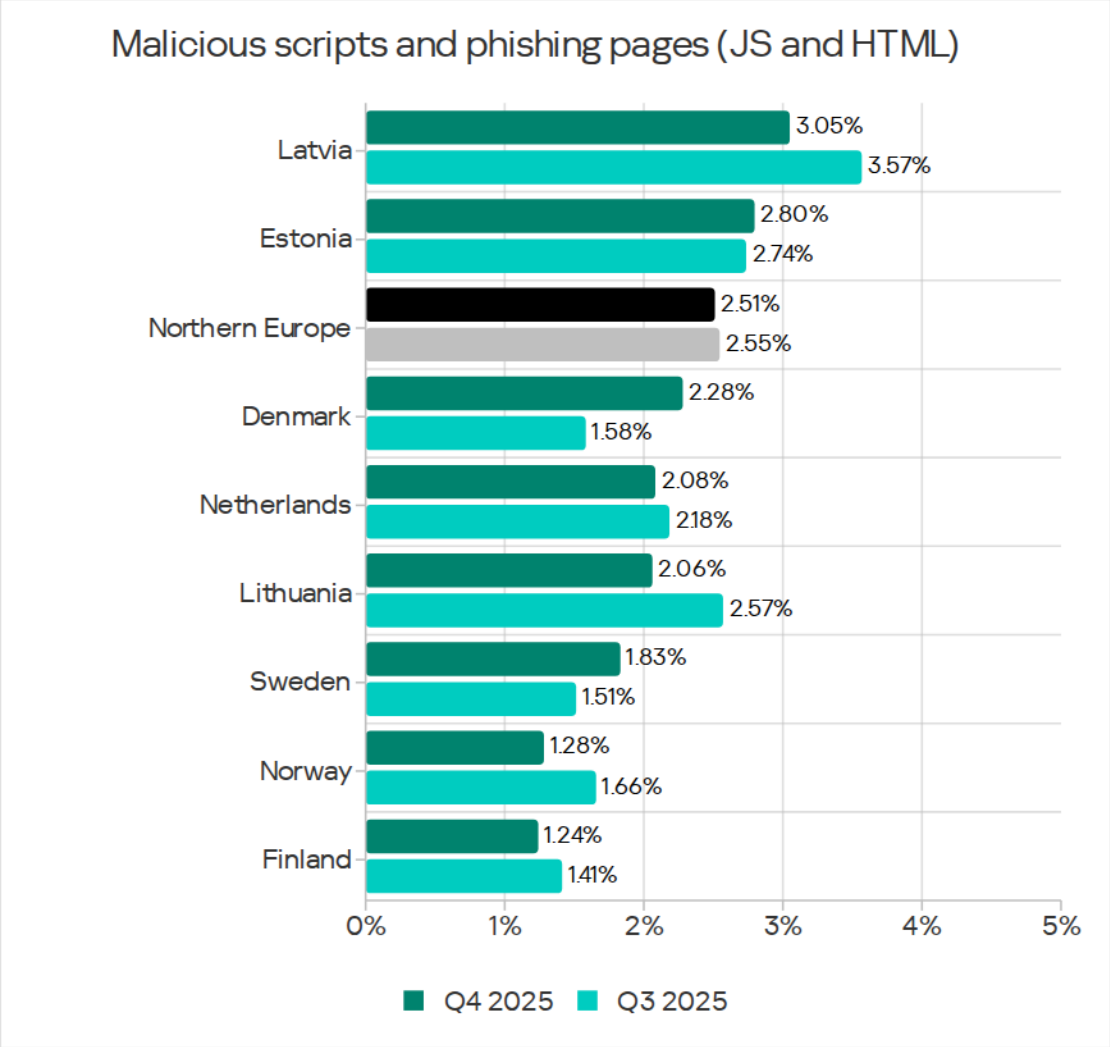
Malicious scripts are used by threat actors for a wide range of tasks including data collection, tracking, and redirecting the user's browser to malicious web resources, and downloading various malware into the system or browser (such as silent cryptomining). They are distributed both via the internet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

Based on the percentage of ICS computers on which malicious scripts and phishing pages were blocked, Northern Europe ranked 14th among regions.

This metric fluctuates in the region. It saw its lowest figure over the surveyed period in Q4 2025 at 2.51%.




Among countries in the region, Latvia led with 3.05% in the percentage of ICS computers on which malicious scripts and phishing pages were blocked. The figure over the quarter increased in Estonia, Denmark, and Sweden.

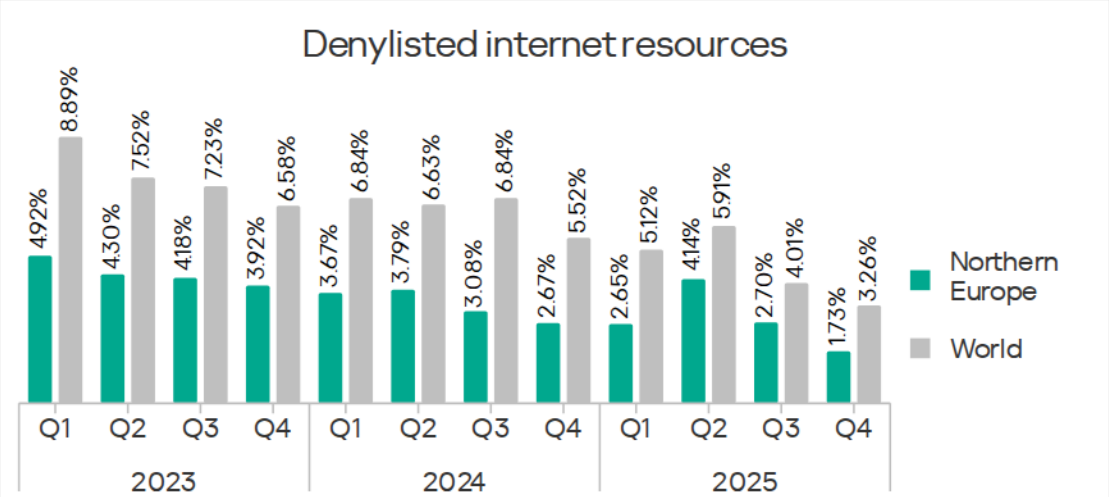



## Denylisted internet resources

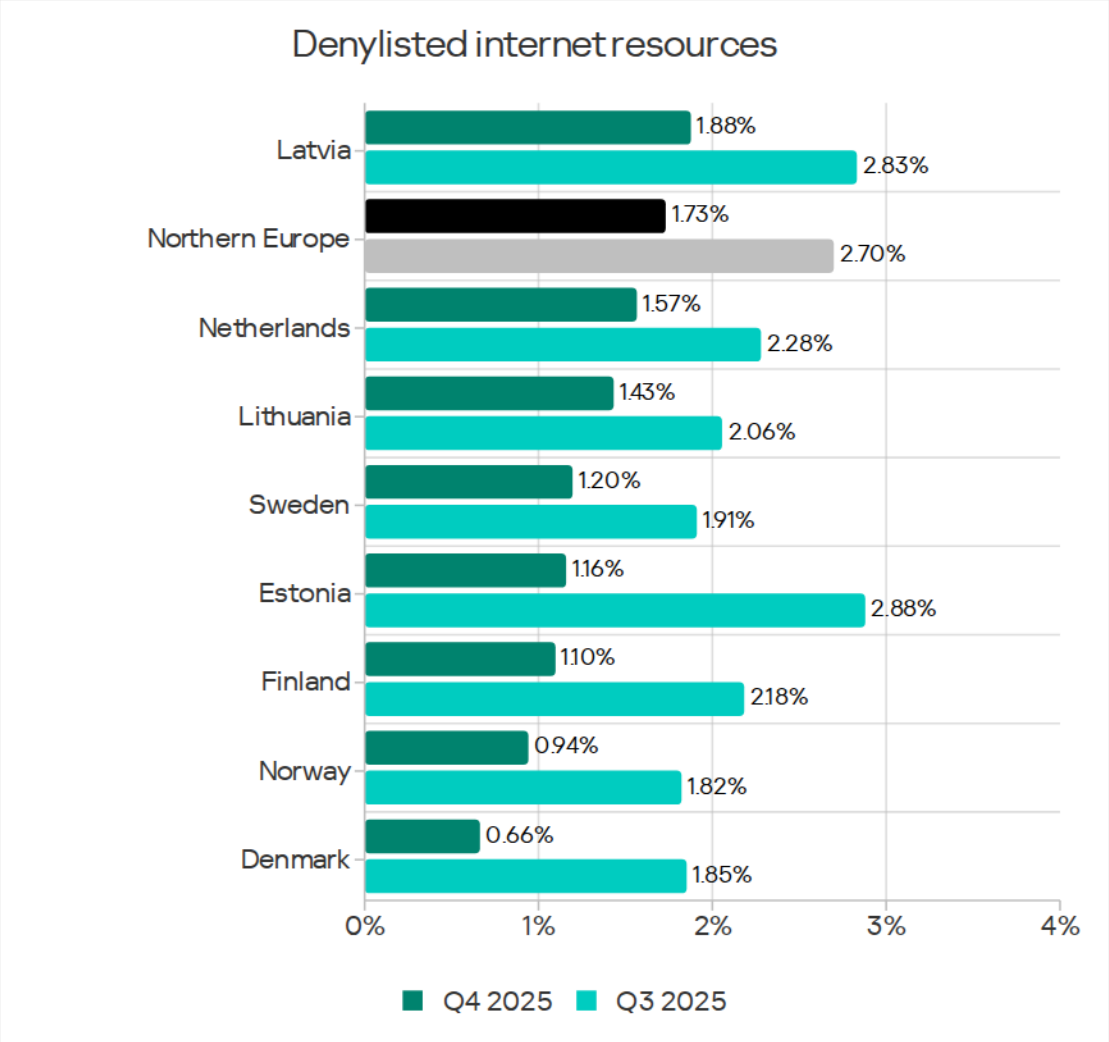
Denylisted internet resources are used by threat actors for initial infection. A significant portion of these resources is used to spread malicious scripts and phishing pages (HTML), which, in turn, can also be used to download cryptominers.

Based on the percentage of ICS computers on which denylisted internet resources were blocked, Northern Europe ranked last (14th) among regions, at 1.73%.

In Q4 2025, just like in all regions, Northern Europe saw a decrease in the percentage of ICS computers on which denylisted internet resources were blocked. The figure for this region turned out to be the lowest for the surveyed period.



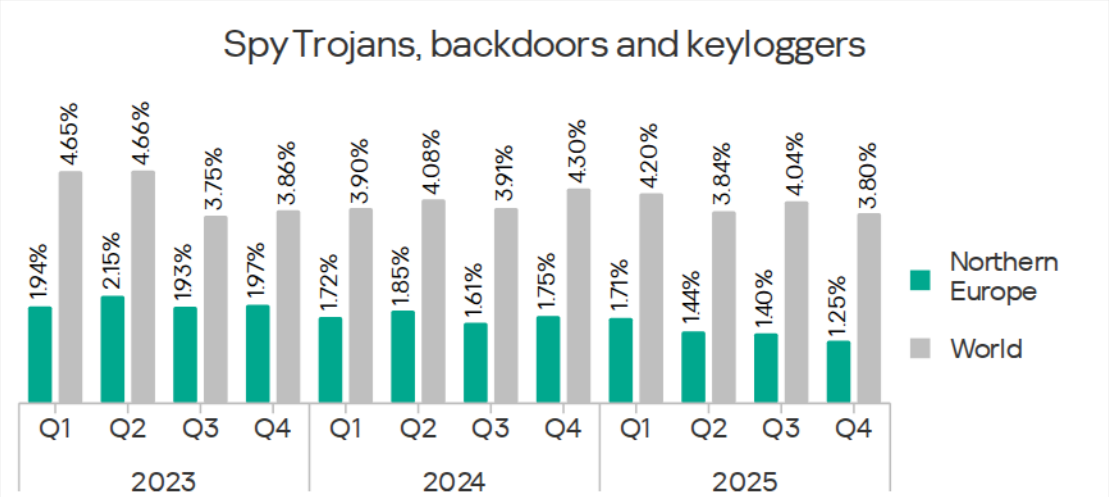

Within the region, Latvia led with 1.88%. Over the quarter, this figure decreased across all countries in the region.



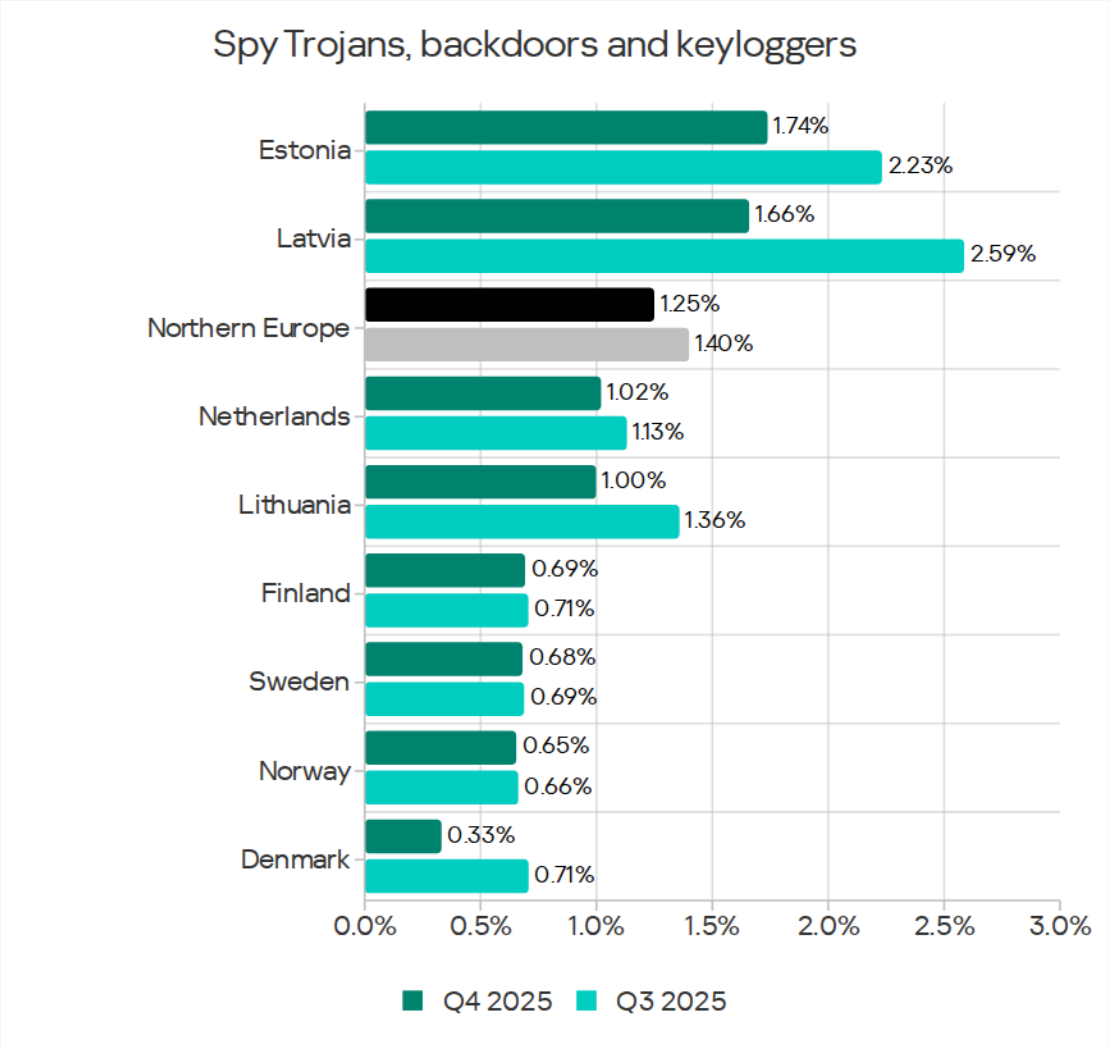
## Spyware

Based on the percentage of ICS computers on which spyware was blocked, Northern Europe ranked last (14th) among regions at 1.25%. This threat ranked third in the regional ranking of categories.

The region's figure declined for four consecutive quarters, dropping to its lowest level during the surveyed period in Q4 2025.




Among the region's countries, Estonia led with 1.74% in the percentage of ICS computers on which spyware was blocked. The metric decreased over the quarter across all countries.

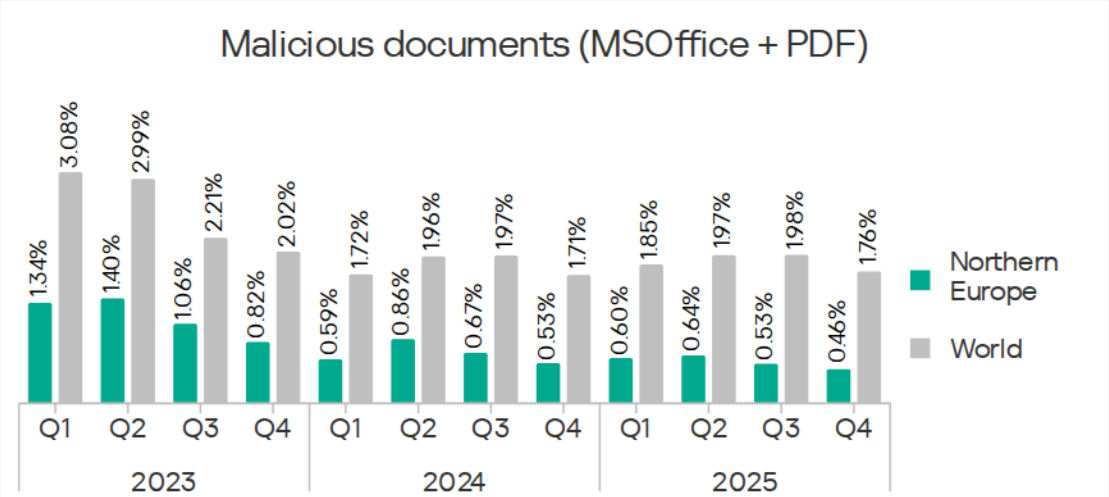



The main channel through which spyware spread in the region was email.

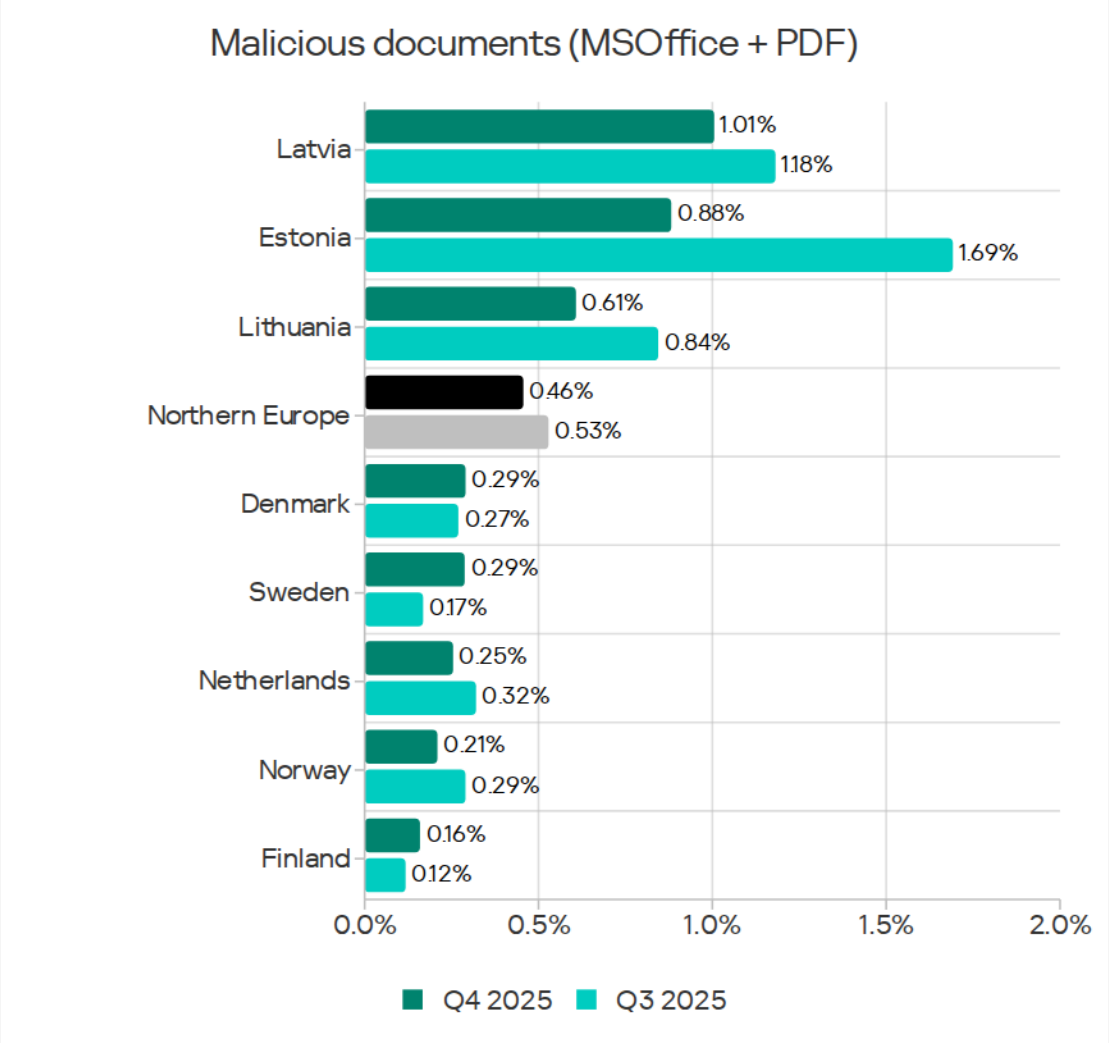
## Malicious documents

Based on the percentage of ICS computers on which malicious documents were blocked, Northern Europe ranked last (14th) globally at 0.46%.

This metric typically fluctuates across the region; it increased in Q4 2025.




Among the region's countries, Latvia led with 1.01% the ranking for the percentage of ICS computes on which malicious documents were blocked. Over the quarter, this figure increased in Denmark, Sweden, and Finland.

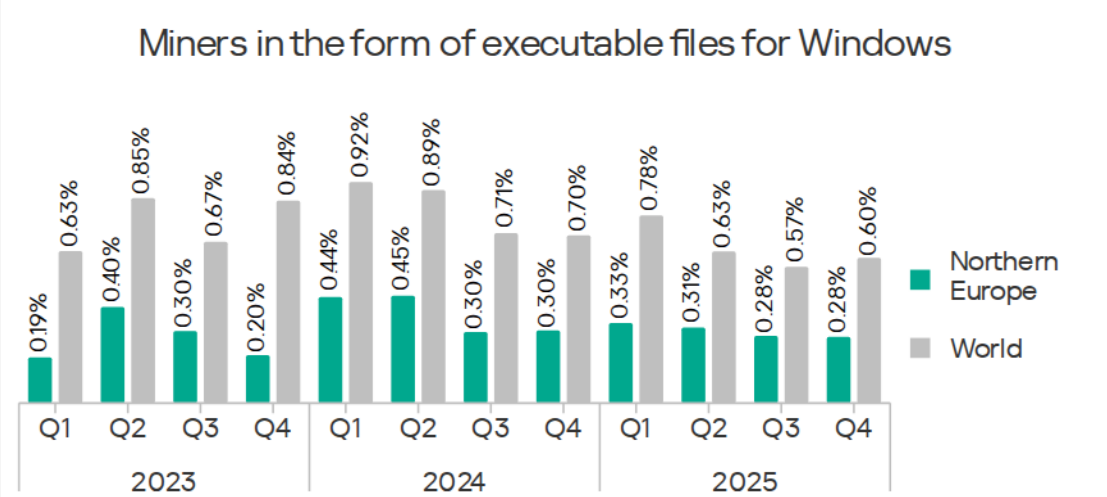


The main source of malicious documents was email.

## Miners in the form of executable files for Windows

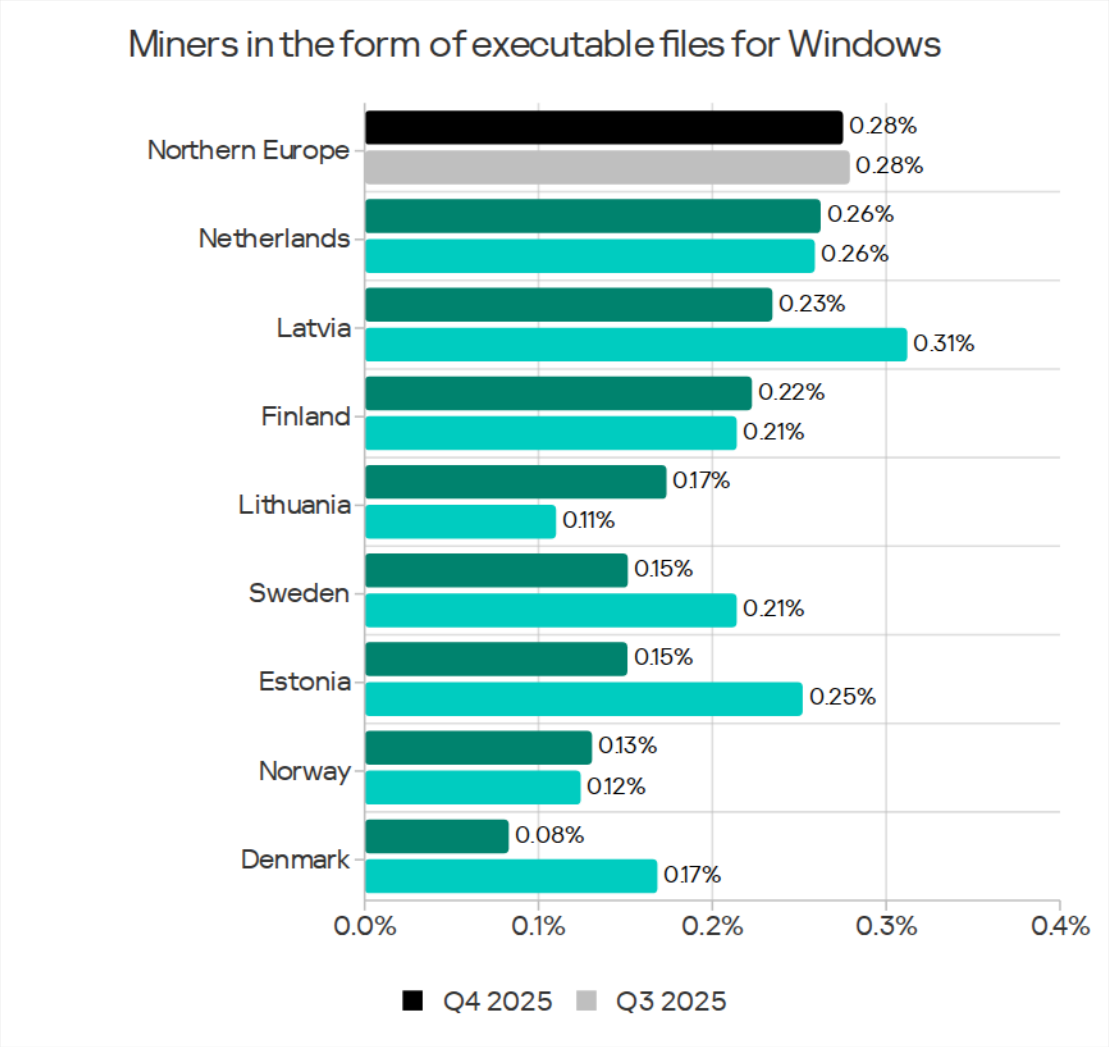
Based on the percentage of ICS computers on which miners in the form of executable files for Windows were blocked, Northern Europe ranked ninth among regions. This is the highest position of Northern Europe in the rankings, both by threat categories and by threat sources.

The indicator in the region fluctuates. In Q4 2025, it decreased to 0.28%. This figure was 1.9 times below North America (Canada), which had the lowest percentage among all regions.



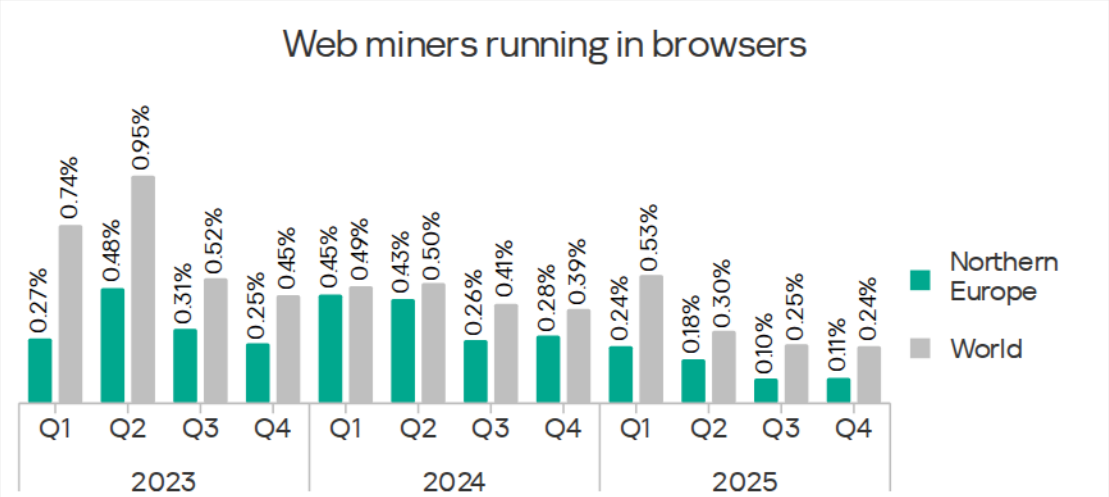

The region's figure for miners in the form of executable files increased in three of the surveyed industries: construction, engineering and ICS integrators, and building automation.

Among countries of the region, the Netherlands led with 0.26% in the percentage of ICS computers on which miners in the form of executable files for Windows were blocked. Over the quarter, this figure grew in the Netherlands, Finland, Lithuania, and Norway.



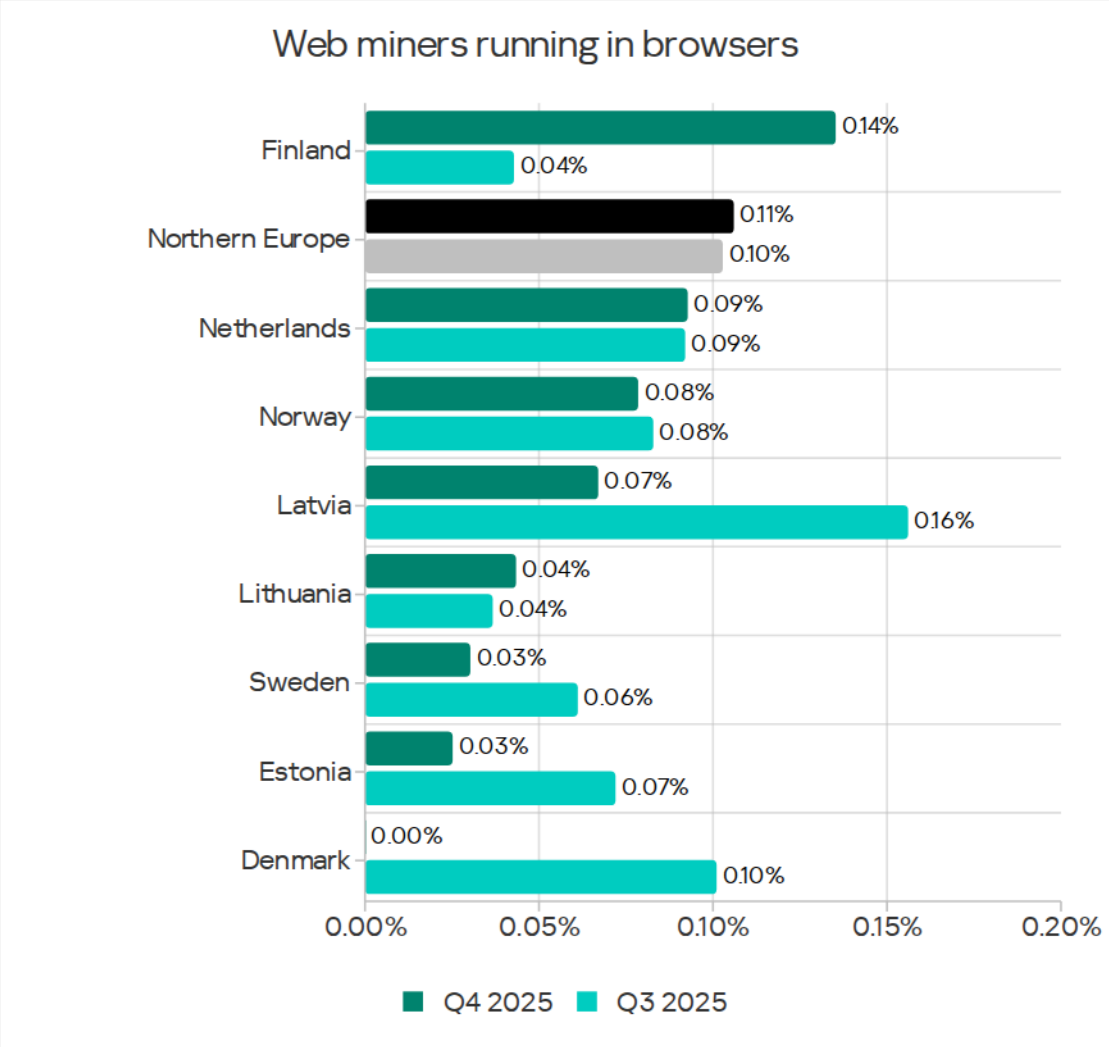

## Web miners

Based on the percentage of ICS computers on which web miners were blocked, Northern Europe ranked 11th globally at 0.11%. This was 1.8 times higher than in East Asia, which had the lowest figure.



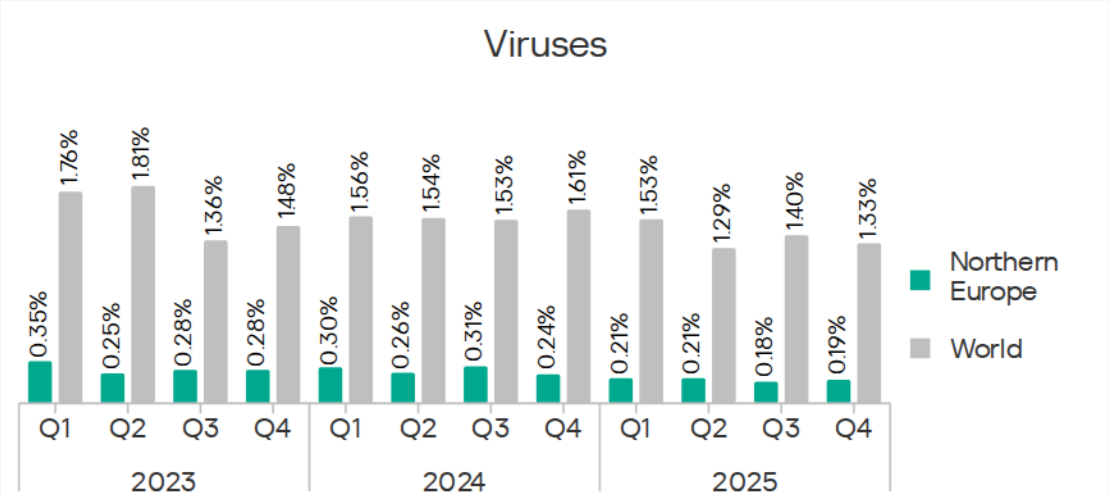

Web miners were one of three threats whose figure grew over the quarter. The figure for web miners increased across all surveyed industries in the region. The most growth was in the manufacturing industry, which saw an increase by a factor of 3.3.

Among countries in the region, Finland led at 0.14%. In this country, the figure over the quarter grew by a factor of 3.5. Aside from Finland, the figure also grew in Lithuania.



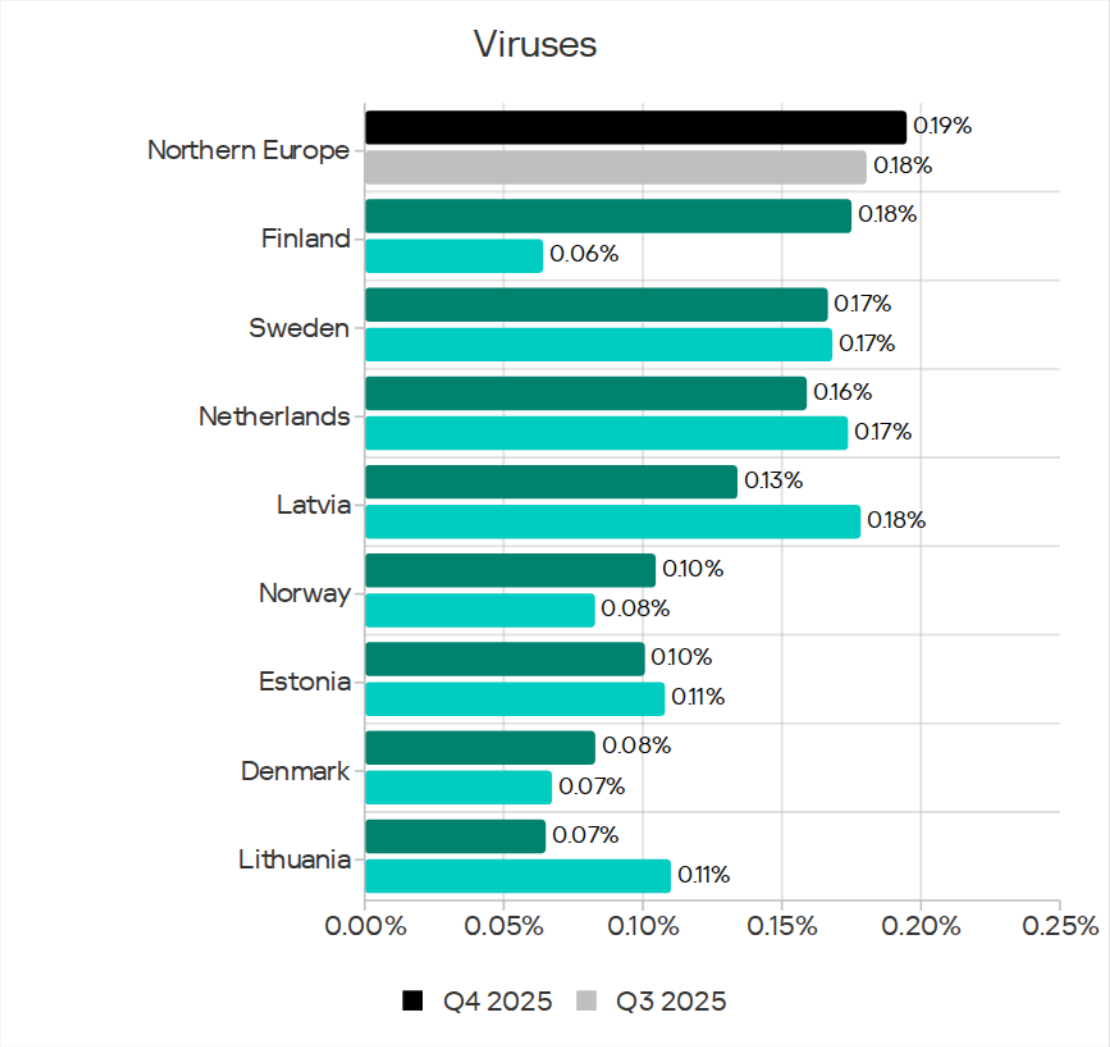

## Viruses

Northern Europe ranked 12th among regions in the percentage of ICS computers on which viruses were blocked, at 0.19%. This was 1.3 times higher than Western Europe, which ranked last in this category.




Viruses were among the three threats whose figure grew over the quarter. The figure for viruses increased in only one of the surveyed industries in the region: the engineering and ICS integrators industry.

Among the region's countries, Finland led in the percentage of ICS computers on which viruses were blocked, at 0.18%. The figure for the quarter increased in Norway, Denmark, and most noticeably in Finland, which saw a threefold increase.

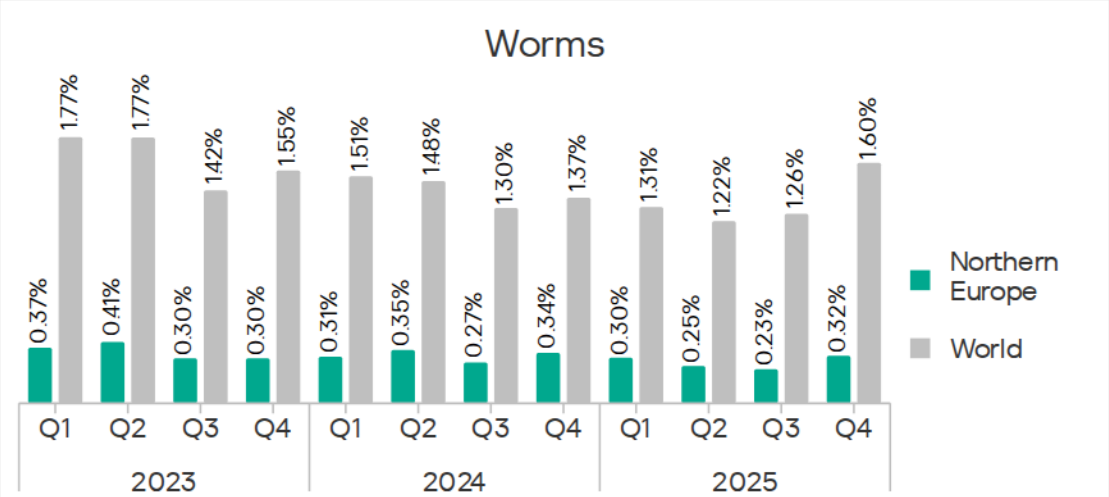



Viruses in the region spread through all threat sources, but mainly via email clients.

## Worms

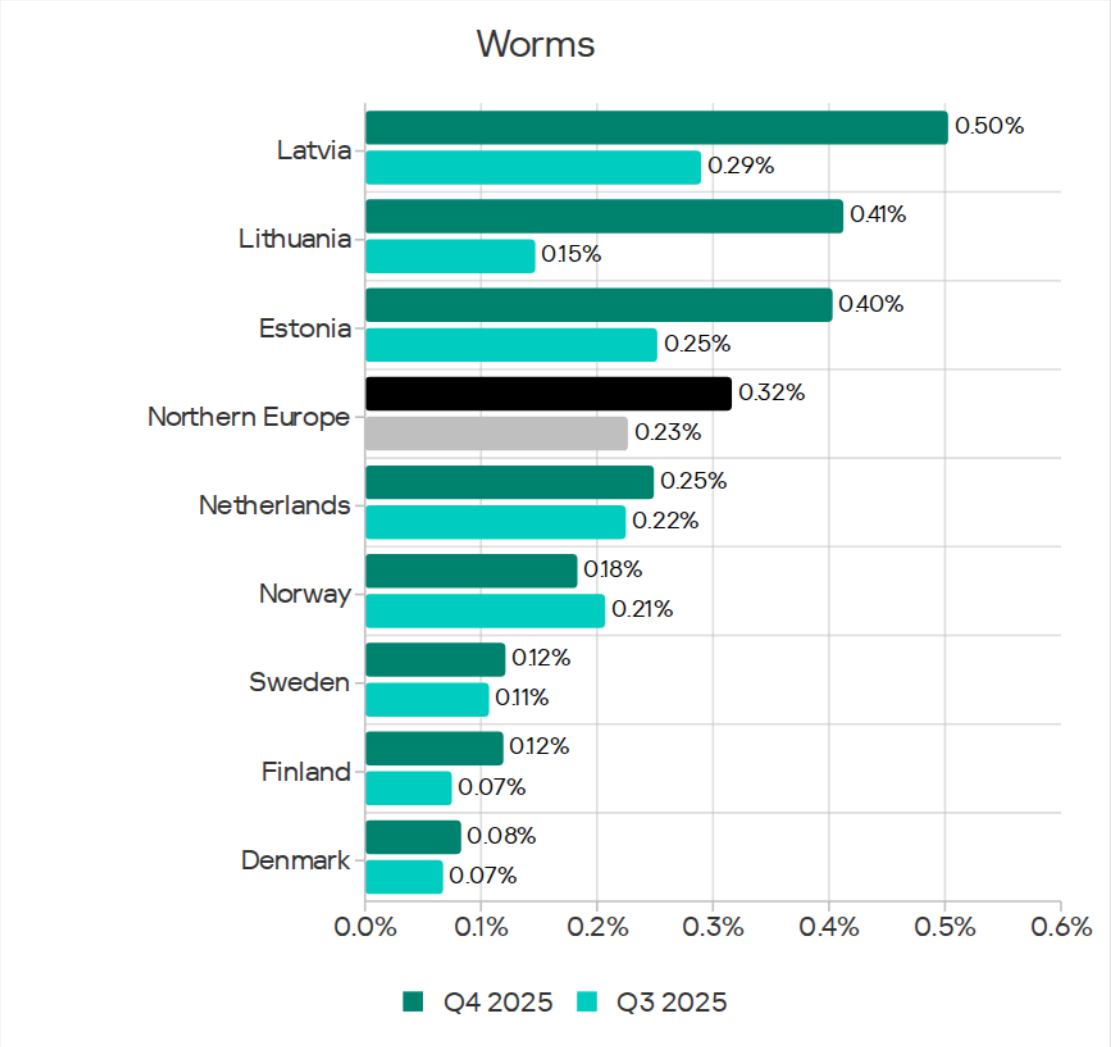
In terms of the percentage of ICS computers on which worms were blocked, Northern Europe ranked 14th with 0.32%.

In Q4 2025, the worm metric grew across all regions due to the latest wave of phishing campaigns known as Curriculum-vitae-catalina which we described earlier. Northern Europe ranked 11th among regions based on the growth in this figure.




The percentage of ICS computers on which worms were blocked increased across all surveyed industries in the region except the construction industry.

Among countries in the region, Latvia led with 0.50% in the percentage of ICS computers on which worms were blocked. The figure increased in all countries of the region, except Norway, and in Lithuania – by a factor of 2.7, and in Latvia – by a factor of 1.7.

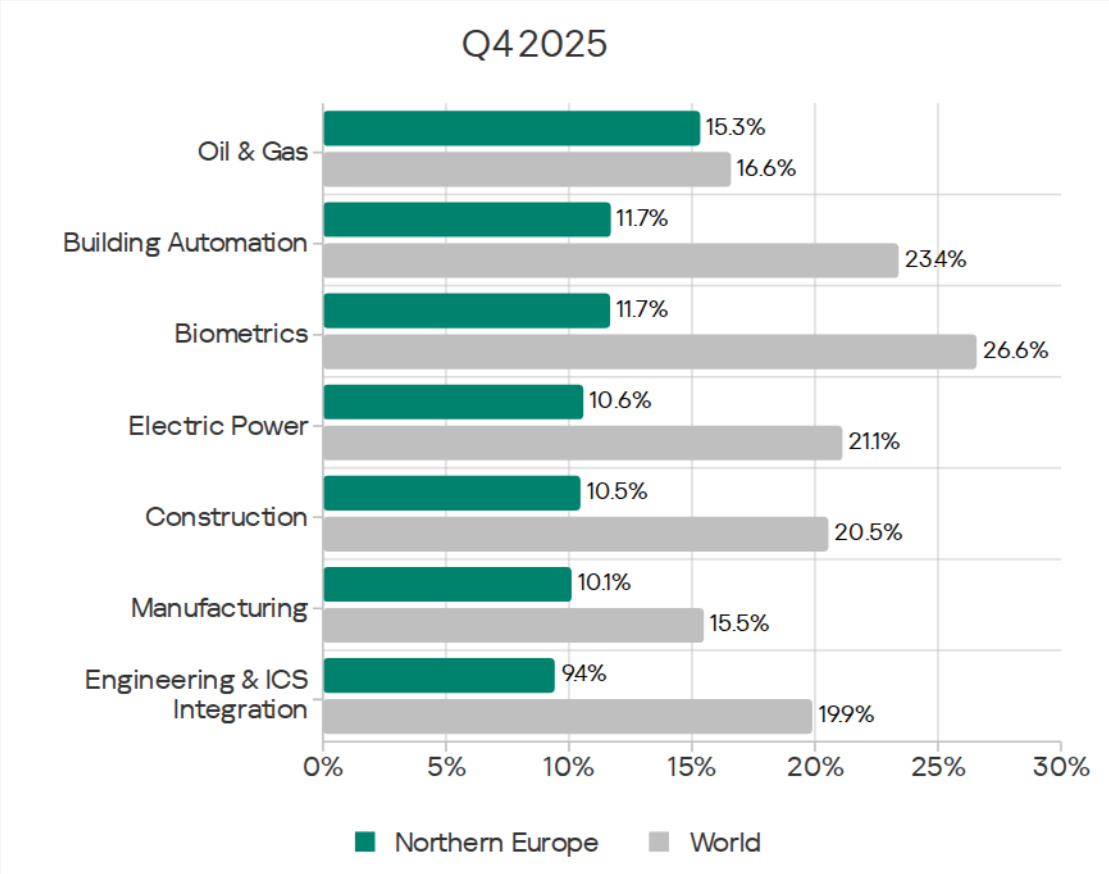



In Q4 2025, worms were spread predominately over email due to a phishing attack.

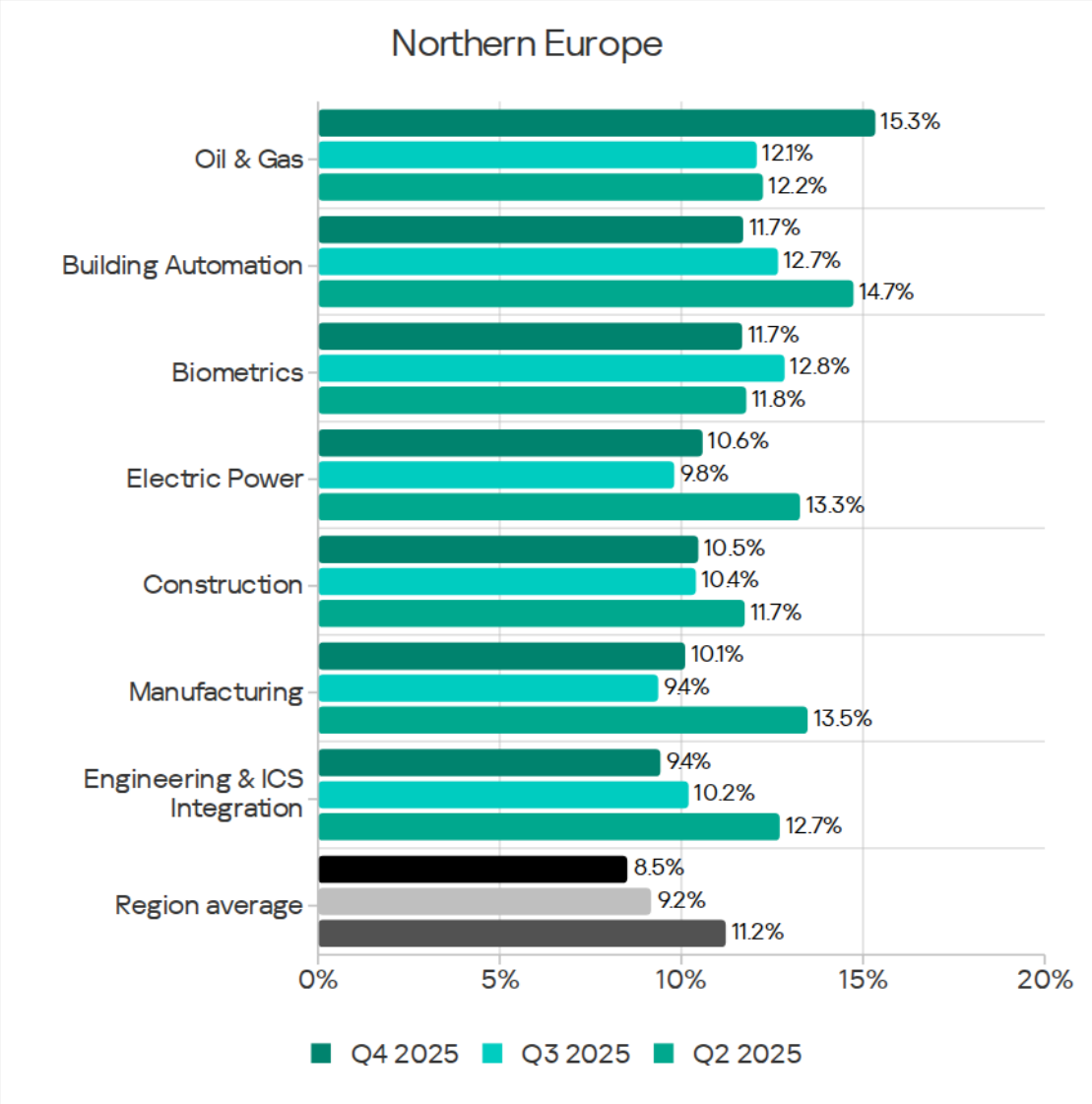
## Industries

In Q4 2025, based on the percentage of ICS computers on which malicious objects were blocked, the oil and gas industry led the rankings of the studied industries and OT infrastructures in Northern Europe.

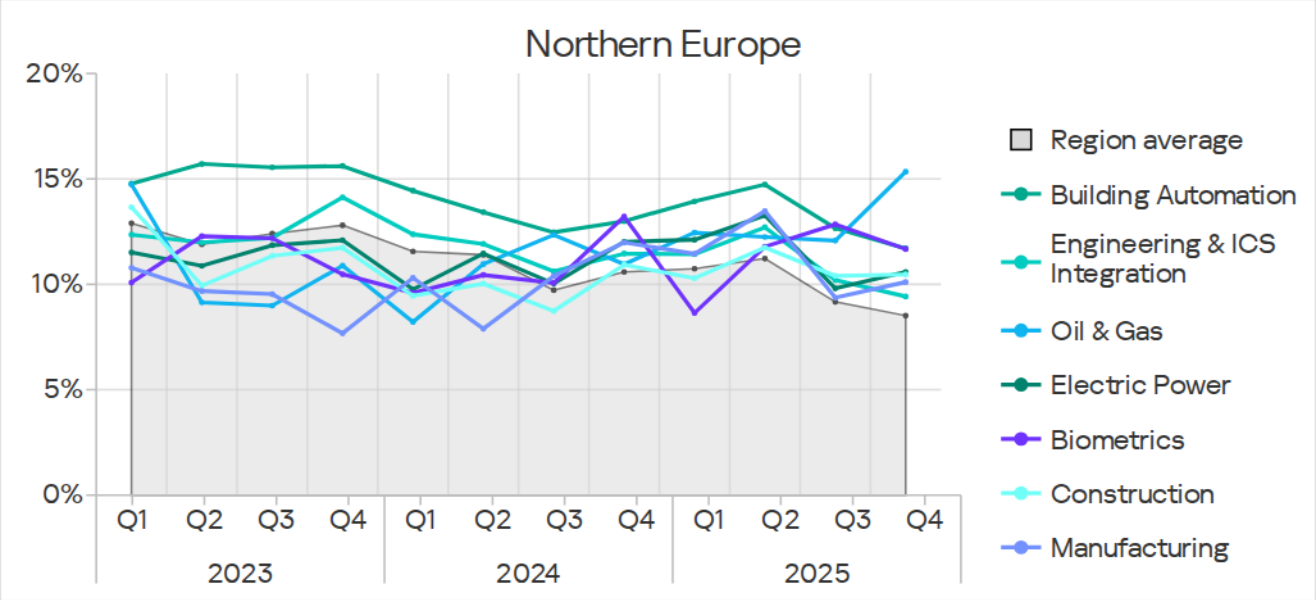
Figures almost for all industries in the region remained well below the global averages.




In Q4 2025, the percentage of ICS computers on which malicious objects were blocked increased in following industries: oil and gas, electric power, construction, and manufacturing.




The oil and gas industry figure is well above the regional averages.




## Threat sources and malware categories in industries: 'hotspots'

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

**Threat source indicators for industries in Northern Europe, Q4 2025**

| Industry / Threat source | Biometrics | Building Automation | Engineering & ICS Integration | Electric Power | Oil & Gas | Construction | Manufacturing | Category metric in region |
|---|---|---|---|---|---|---|---|---|
| Internet | 4.67% | 4.62% | 5.06% | 5.13% | 8.59% | 5.50% | 5.28% | 3.96% |
| Email clients | 1.56% | 2.16% | 0.36% | 0.67% | 0.31% | 1.36% | 0.90% | 0.64% |
| Removable media | — | 0.07% | 0.10% | 0.40% | — | 0.18% | 0.15% | 0.06% |
| Network folders | — | 0.01% | 0.01% | — | — | — | — | 0.01% |
| **Industry metric in region** | 11.67% | 11.70% | 9.42% | 10.59% | 15.34% | 10.47% | 10.11% | |

**Threat category indicators for industries in Northern Europe, Q4 2025**

| Industry / Threat type | Biometrics | Building Automation | Engineering & ICS Integration | Electric Power | Oil & Gas | Construction | Manufacturing | Category metric in region |
|---|---|---|---|---|---|---|---|---|
| Denylisted internet resources | 3.11% | 2.26% | 2.20% | 2.53% | 3.68% | 2.42% | 2.11% | 1.73% |
| Malicious scripts and phishing pages (JS and HTML) | 4.28% | 4.06% | 2.98% | 3.53% | 6.75% | 4.38% | 3.17% | 2.51% |
| Malicious documents (MSOffice + PDF) | 0.39% | 1.47% | 0.30% | 0.60% | 0.92% | 0.47% | 0.90% | 0.46% |
| Spy Trojans, backdoors and keyloggers | 1.95% | 2.82% | 1.26% | 2.00% | 1.84% | 1.18% | 2.11% | 1.25% |
| Ransomware | — | 0.13% | 0.05% | 0.13% | — | — | — | 0.05% |
| Miners in the form of executable files for Windows | 0.39% | 0.43% | 0.32% | 0.40% | 0.61% | 0.53% | 0.90% | 0.28% |
| Web miners running in browsers | — | 0.20% | 0.14% | 0.27% | 0.61% | 0.35% | 0.60% | 0.11% |
| Malware for AutoCAD | — | — | 0.01% | — | — | 0.12% | — | 0.01% |
| Worms | 0.78% | 0.74% | 0.32% | 0.80% | 0.92% | 0.24% | 1.21% | 0.32% |
| Viruses | 0.39% | 0.32% | 0.24% | 0.40% | 0.92% | 0.30% | 0.30% | 0.19% |
| **Industry metric in region** | 11.67% | 11.70% | 9.42% | 10.59% | 15.34% | 10.47% | 10.11% | |

Northern Europe came last (14th) in most rankings of regions based on the percentage of ICS computers on which malicious objects were blocked across various industries. The only rankings where Northern Europe was one spot above that were those for the electric power industry and the manufacturing industry.

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

In Q4 2025, the figure for miners in the form of executable files increased in three of the surveyed industries: construction, engineering and ICS integrators, and building automation.

The figure for web miners over the quarter increased across all surveyed industries in the region. The most growth was recorded in the manufacturing industry, which saw an increase by a factor of 3.3.

Based on the figures for the manufacturing industry, Northern Europe ranked second among regions by the percentage of ICS computers on which miners in the form of Windows executable files were blocked, and ranked third for web miners.

In Q4 2025, the figure for viruses slightly increased across the region. Of all the surveyed industries, the percentage of ICS computes on which viruses were blocked increased only in the engineering and ICS integrators industry.

Due to a wave of phishing campaigns known as Curriculum-vitae-catalina that spread a backdoor worm, the figure for worms increased across all industries except for the construction industry.

**Building automation**

Northern Europe ranked 14th 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 occupied the following positions:

- First place in the percentage of ICS computers on which threats from email clients were blocked.
- First for network folder threats (these threats were encountered in only two industries in the region).
- First for the percentage of ICS computers on which malicious documents and spyware were blocked.
- Second in threats of the following categories: malicious scripts and phishing pages, viruses, and ransomware.
- Third for denylisted internet resources, worms, and miners in the form of executable files for Windows.

**Electric power**

Northern Europe ranked 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 ranked:

- First by the percentage of ICS computers on which threats from removable media were blocked.

- Third for internet threats.
- First by the percentage of ICS computers on which denylisted internet resources, viruses and ransomware were blocked.
- Second for worms.
- Third for malicious scripts and phishing pages, malicious documents, spyware, and web miners.

**Construction**

Northern Europe ranked 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 ranked:

- First based on the percentage of ICS computers on which internet threats were blocked.
- Second by the percentage of ICS computers on which threats from email clients and removable media were blocked.
- First for malicious scripts and phishing pages, and malware for AutoCAD.
- Second in denylisted internet resources and both types of miners.

**Manufacturing**

Northern Europe ranked 12th in the percentage of ICS computers on which malicious objects were blocked in the manufacturing industry.

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

- Second by the percentage of ICS computers on which miners in the form of executable files for Windows were blocked.
- Third in the region in terms of web miners.

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

- Second in the percentage of ICS computers on which internet threats were blocked.
- Third for threats from email clients and removable media.
- First in the percentage of ICS computers on which worms and miners of both categories were blocked.
- Second for malicious documents and spyware.
- Third place in viruses.

### Engineering and ICS integrators

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

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

- Second for the percentage of ICS computers on which threats from network folders were blocked – these threats were encountered only in two of the region's industries.
- Second place in malware for AutoCAD.
- Third place in ransomware.

## 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

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

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

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

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

Kaspersky ICS CERT ics-cert@kaspersky.com