Kaspersky ICS CERT

kaspersky

Threat landscape for industrial automation systems

Middle East. Q4 2025

24.04.2026

Version 1.0

Middle East

Key cybersecurity issues in the region

High risk of targeted attacks

In the Middle East, the percentage of ICS computers on which threats from email clients were blocked was 1.8 times higher than the global average.

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

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 at stealing authentication data for corporate services.

Insufficient network segmentation

In the Middle East, the percentage of ICS computers on which threats from removable media were blocked was 1.8 times higher than the global average.

Relatively high levels of self-propagating malware point to large parts of the infrastructure remaining unprotected and insufficiently segmented.

The virus rate in the region was 1.4 times higher than the global average, and the worm rate was 1.6 times higher.

High rate of spyware

The region's percentage of ICS computers on which spyware was blocked was 1.3 times higher than the global average, and the rate for malicious documents was 1.5 times higher.

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

High ransomware rate

The ransomware rate in the region remains consistently high, nearly twice the global average.

In Q4 2025, the Middle East still ranked first among all regions by percentage of ICS computers on which ransomware was blocked.

The Middle East ranked no lower than fifth in the ransomware rankings for all industries except manufacturing. In the oil and gas sector, the Middle East was the leader for this indicator.

Striking country-level differences

In the Middle East, there are countries with very different industrial cybersecurity situations. Yemen ranked second in the world by percentage of ICS computers on which malicious objects were blocked, while Israel was one of the 10 safest countries.

Yemen led many of the region's rankings, and by a wide margin when it came to miners of both categories, worms, viruses and ransomware. The exception was email threats and categories of threats that spread primarily via email.

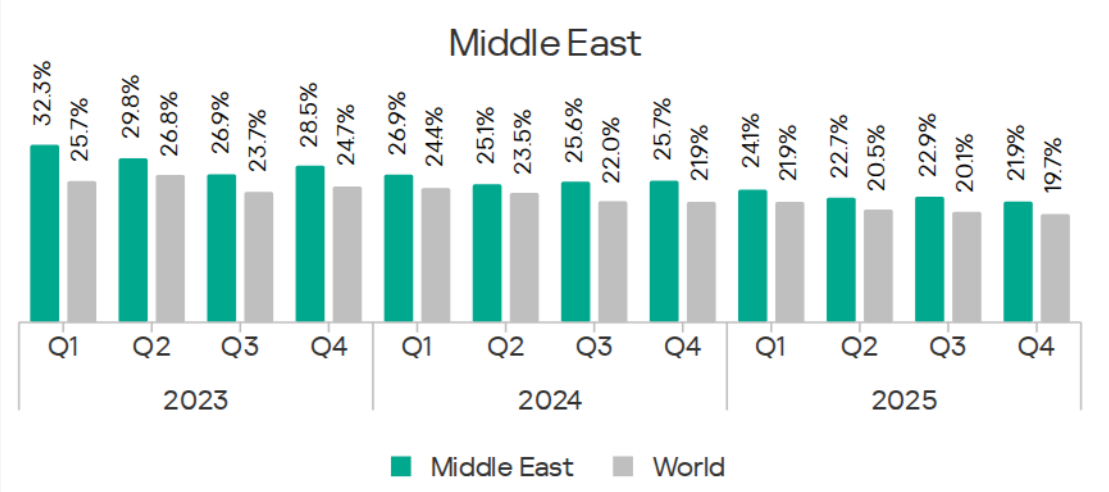
For threats from email clients, the UAE and Qatar held the top positions. These two countries also ranked first in malicious documents, and malicious scripts and phishing pages, and are among the top three countries for spyware.

Israel, by contrast, consistently has the lowest figures in most rankings, often by a significant margin.

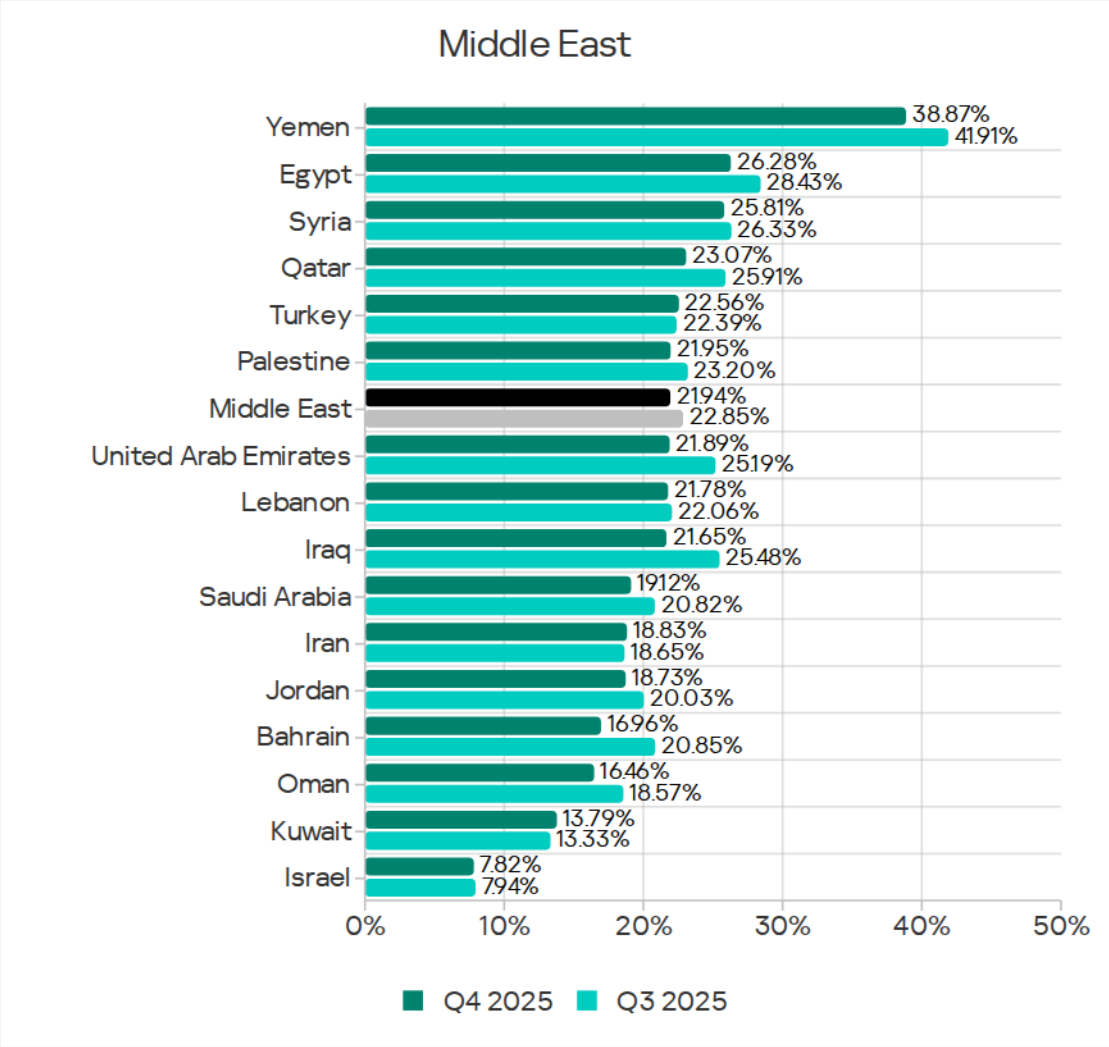
Statistics across all threats

In Q4 2025, the Middle East ranked third globally by percentage of ICS computers on which malicious objects were blocked. The region consistently exceeds the global average in this metric by 1.1 times.

The percentage decreased to 22.9%, which was 2.6 times higher than in Northern Europe, where the rate was the lowest.



Rates within the region vary from 7.82% in Israel to 38.87% in Yemen. These two countries are relative outliers, with the region's other countries ranging between 13% and 27%.



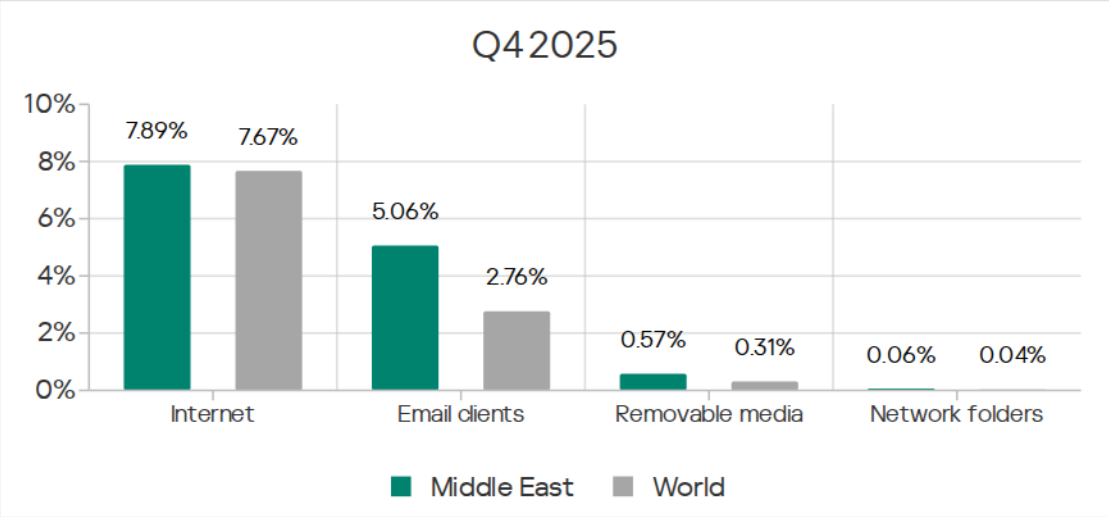
Yemen leads many of the region's rankings for both sources and categories of malware. In terms of email threats, as well as malicious documents, malicious scripts and phishing pages, and malware for AutoCAD categories, the UAE holds top spot.

Israel consistently comes bottom in most of the region's rankings.

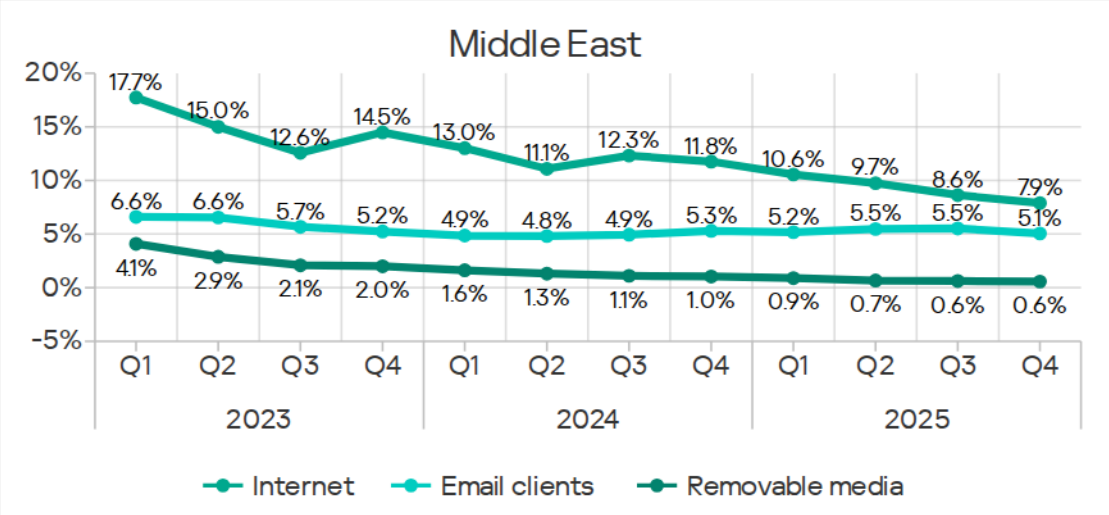
Threat sources

The percentage of ICS computers on which threats were blocked from various sources was higher in the Middle East than the global average for all sources. The region significantly exceeded the global average by percentage of ICS computers on which the following were blocked:

- Email client threats: 1.8 times higher.
- Removable media threats: 1.8 times higher.
- Network folder threats: 1.5 times higher.



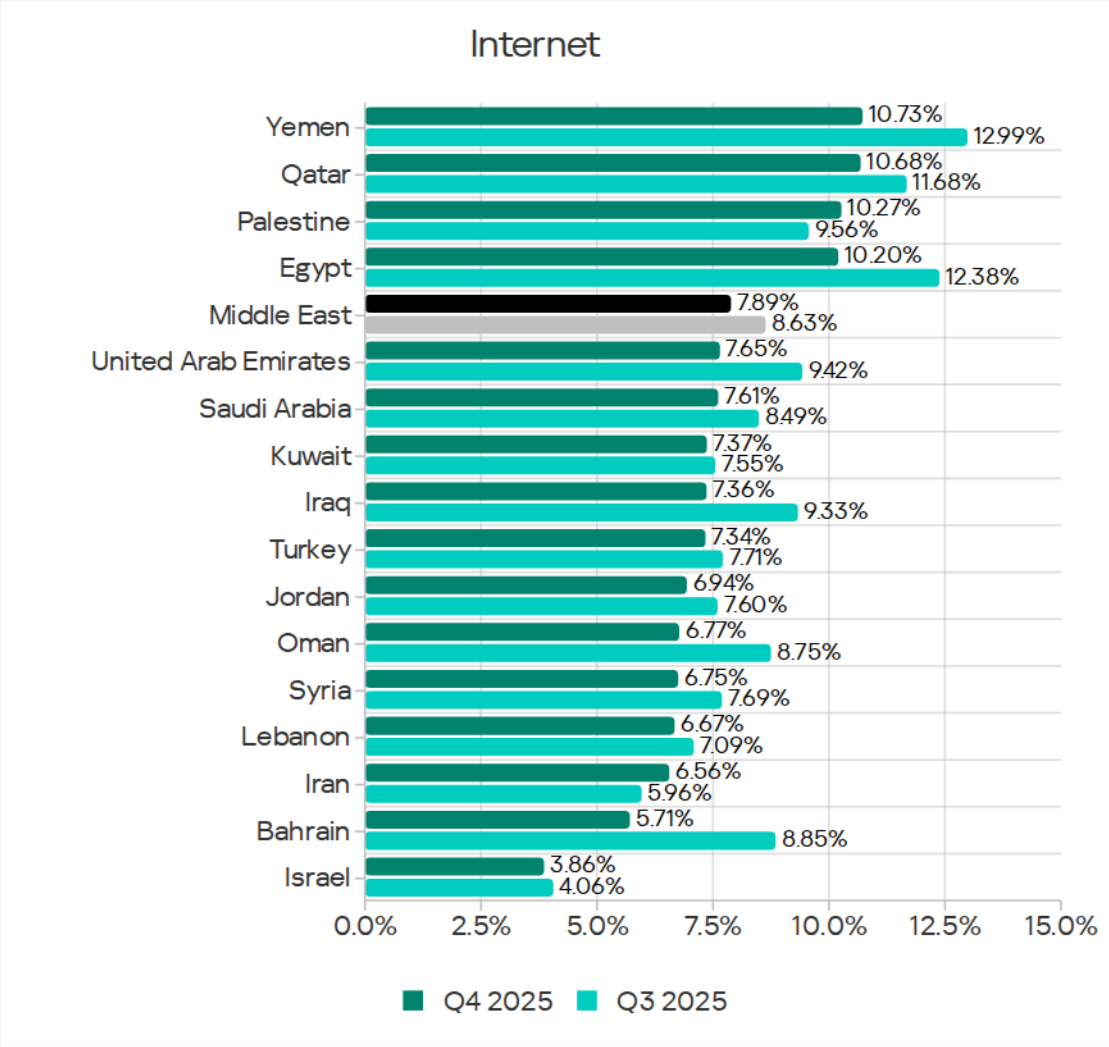
In Q4 2025, the percentage of attacked ICS computers decreased for all threat sources.



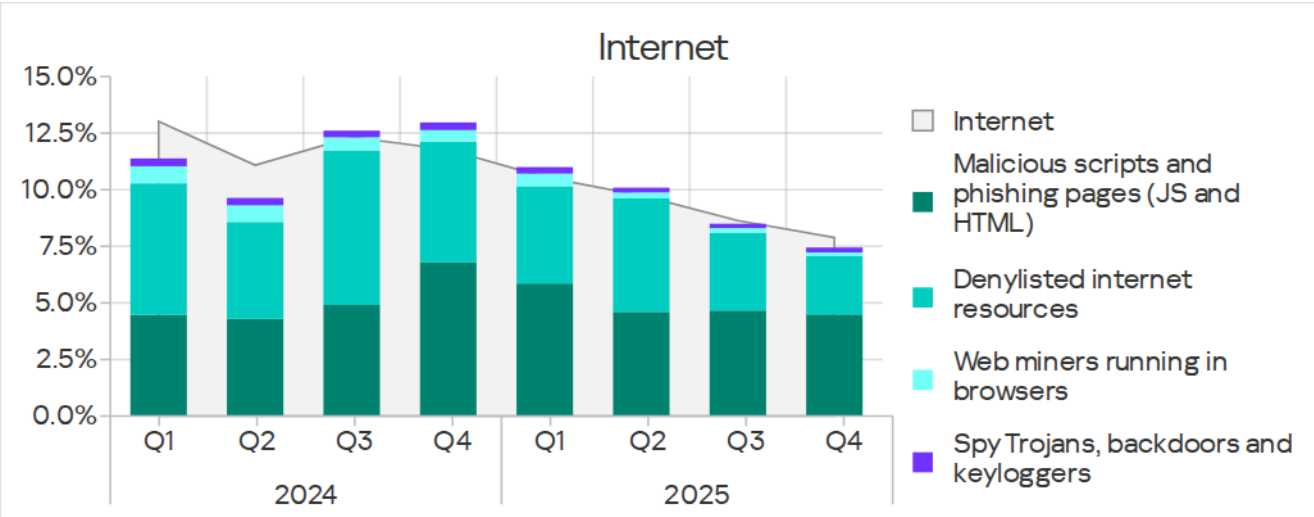
Internet

By percentage of ICS computers on which internet threats were blocked, the Middle East ranked sixth in the regional rankings with 7.89%. This was two times higher than the lowest rate recorded in Northern Europe.

Country-level rates ranged from 3.86% in Israel to 10.73% in Yemen.

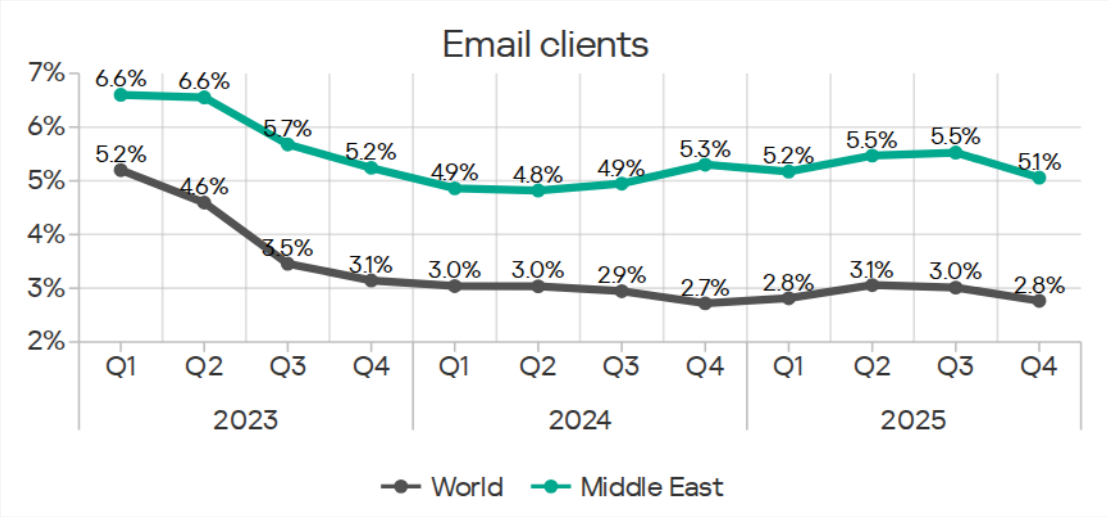


The main categories of internet threats that were blocked on ICS computers in the region included malicious scripts and phishing pages, as well as denylisted internet resources.

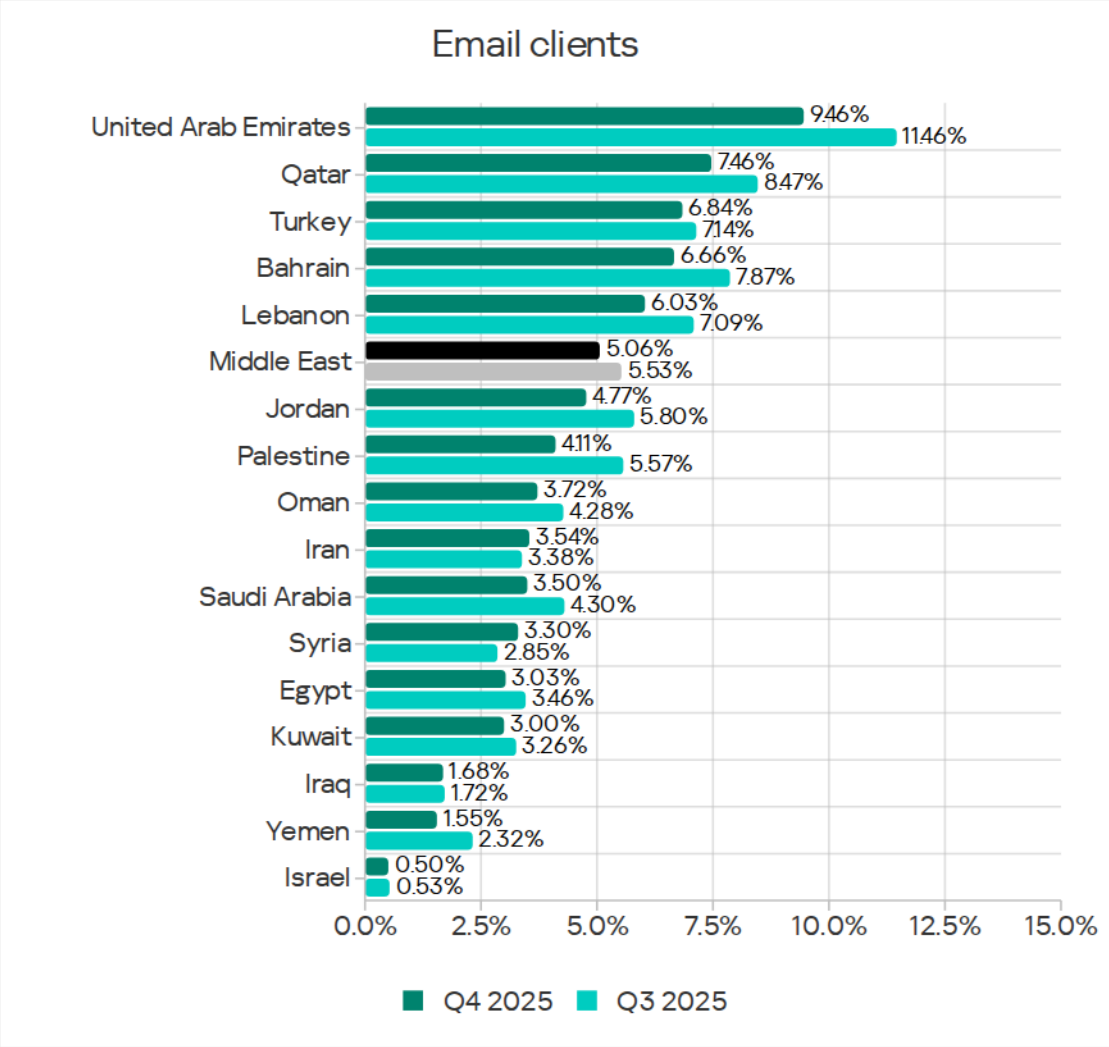


Email clients

In Q4 2025, the Middle East dropped from second to third place in the ranking of regions by the percentage of ICS computers on which threats from email clients were blocked. The percentage decreased to 5.06%, which was 7.9 times higher than in Northern Europe, which ranked last.

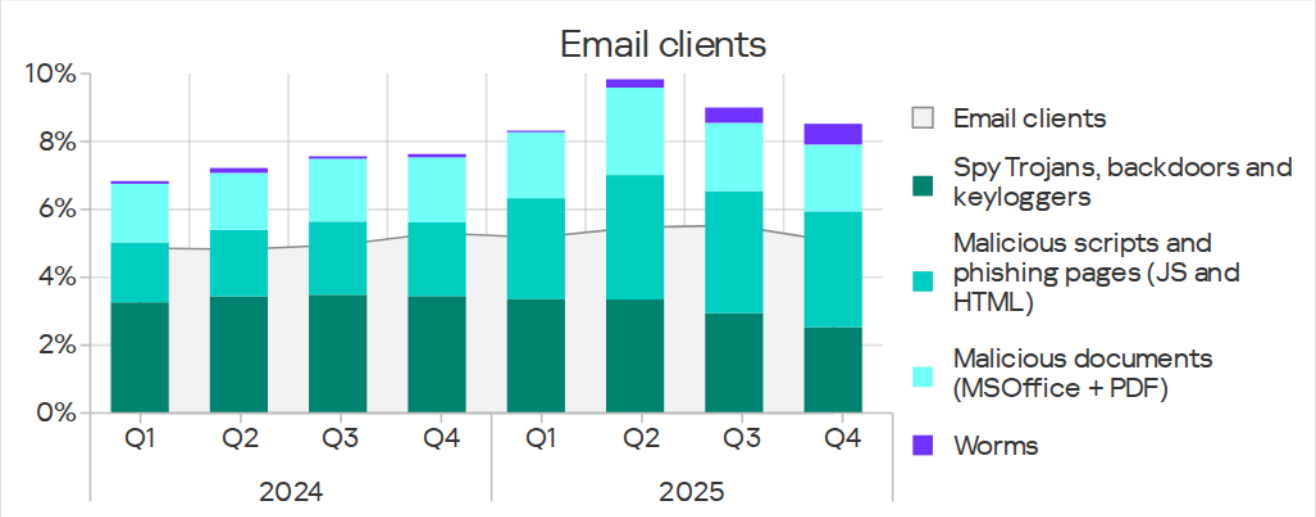


Within the region, the UAE consistently leads – in Q4 2025, it had a percentage of 9.46%. Israel had the lowest figure (0.50%). Yemen, which led in most other sources, ranked second to last.



The two leading countries in this ranking (the UAE and Qatar) also placed highly in terms of malicious documents, and malicious scripts and phishing pages. In the ranking for spyware, they came second and third respectively.

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



In Q4 2025, the percentage of ICS computers on which worms from email clients were blocked increased significantly. This is due to another wave of phishing attacks, known as Curriculum-vitae-catalina, affecting all regions of the world. In the Middle East, the attack peaked in November.

During the attack, the actor sent phishing emails disguised as job postings. The emails contained a malicious file (backdoor worm for remote management Backdoor.MSIL.XWorm) that masqueraded as a resume (Curriculum Vitae). When the file was executed, the system was infected.

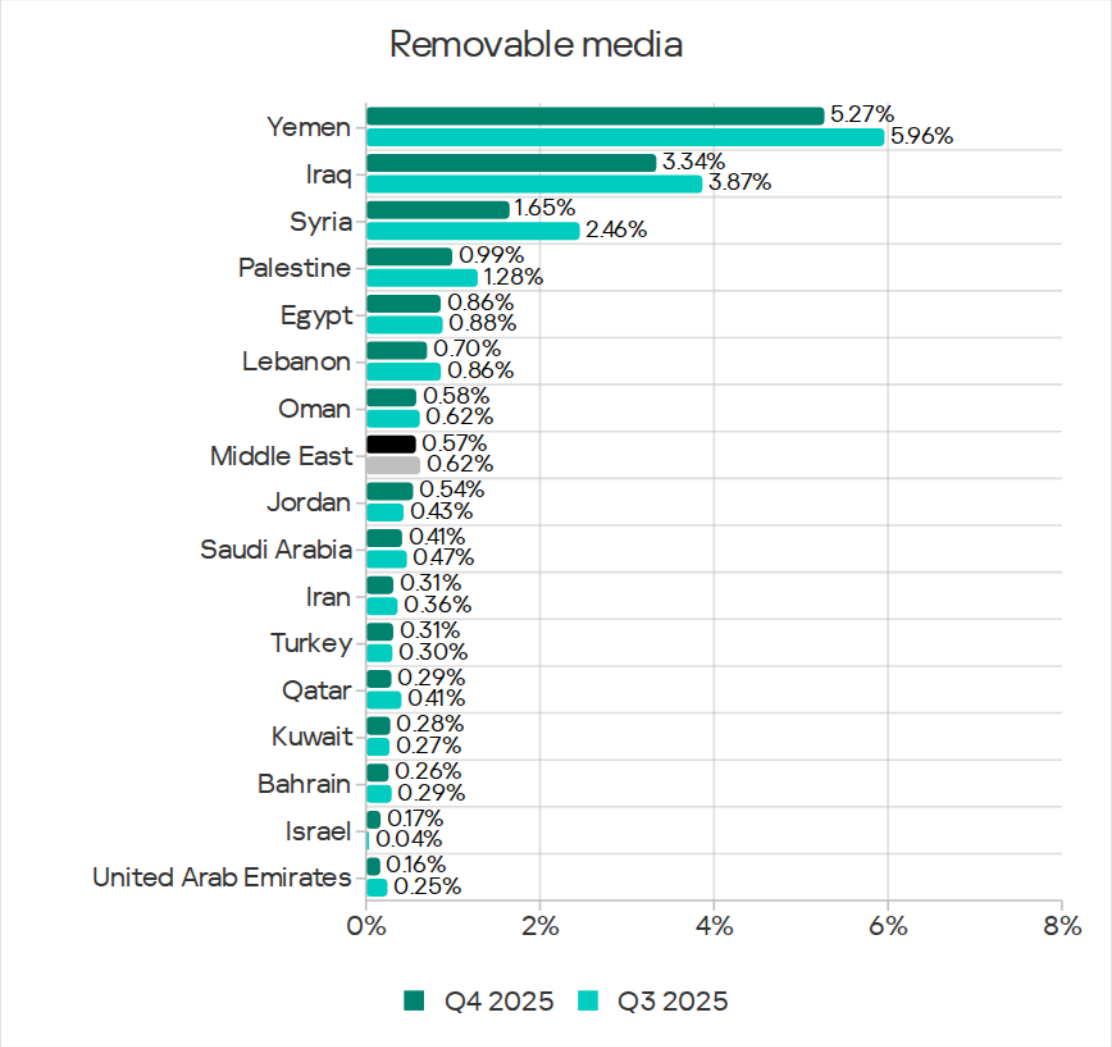
Typically, such campaigns are aimed at delivering malware for data theft, spyware, or remote management tools (RAT).

Backdoor.MSIL.XWorm was blocked most frequently on ICS computers in regions where threats from email clients are traditionally blocked most often — Southern Europe, South America and the Middle East.

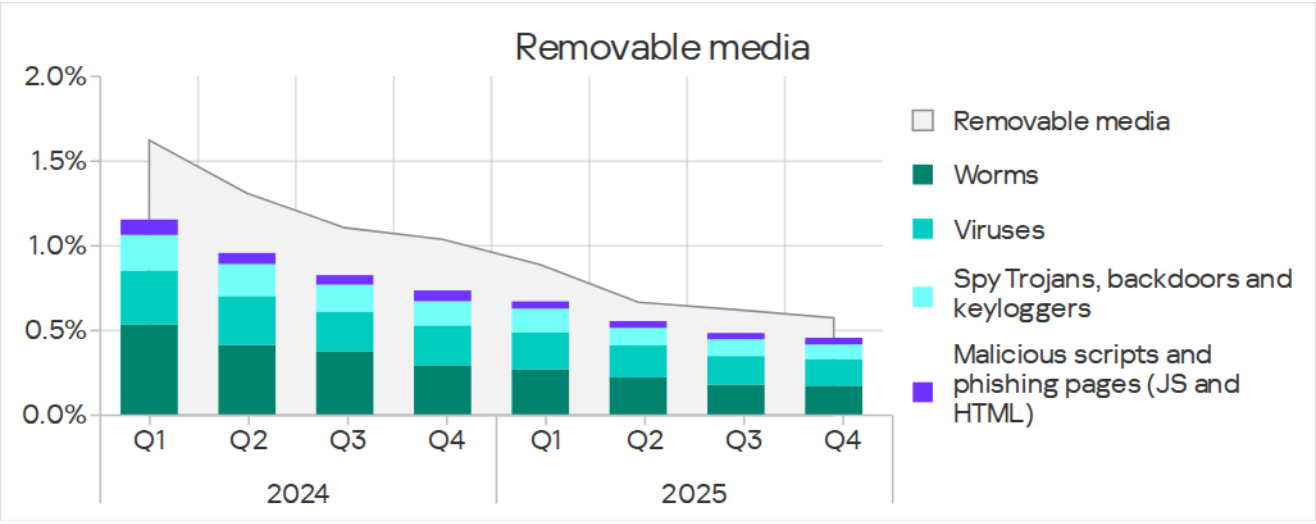
Removable media

In Q4 2025, the Middle East ranked third among regions by percentage of ICS computers on which threats from removable media were blocked, with 0.57%. This was 11.4 times higher than the figure for the Australia and New Zealand region, which ranked last.

Yemen led the region with 5.27%, followed by Iraq with 3.34%, in terms of the percentage of ICS computers on which threats from removable media were blocked. The other countries ranged from 0.16% in the UAE to 1.65% in Syria.



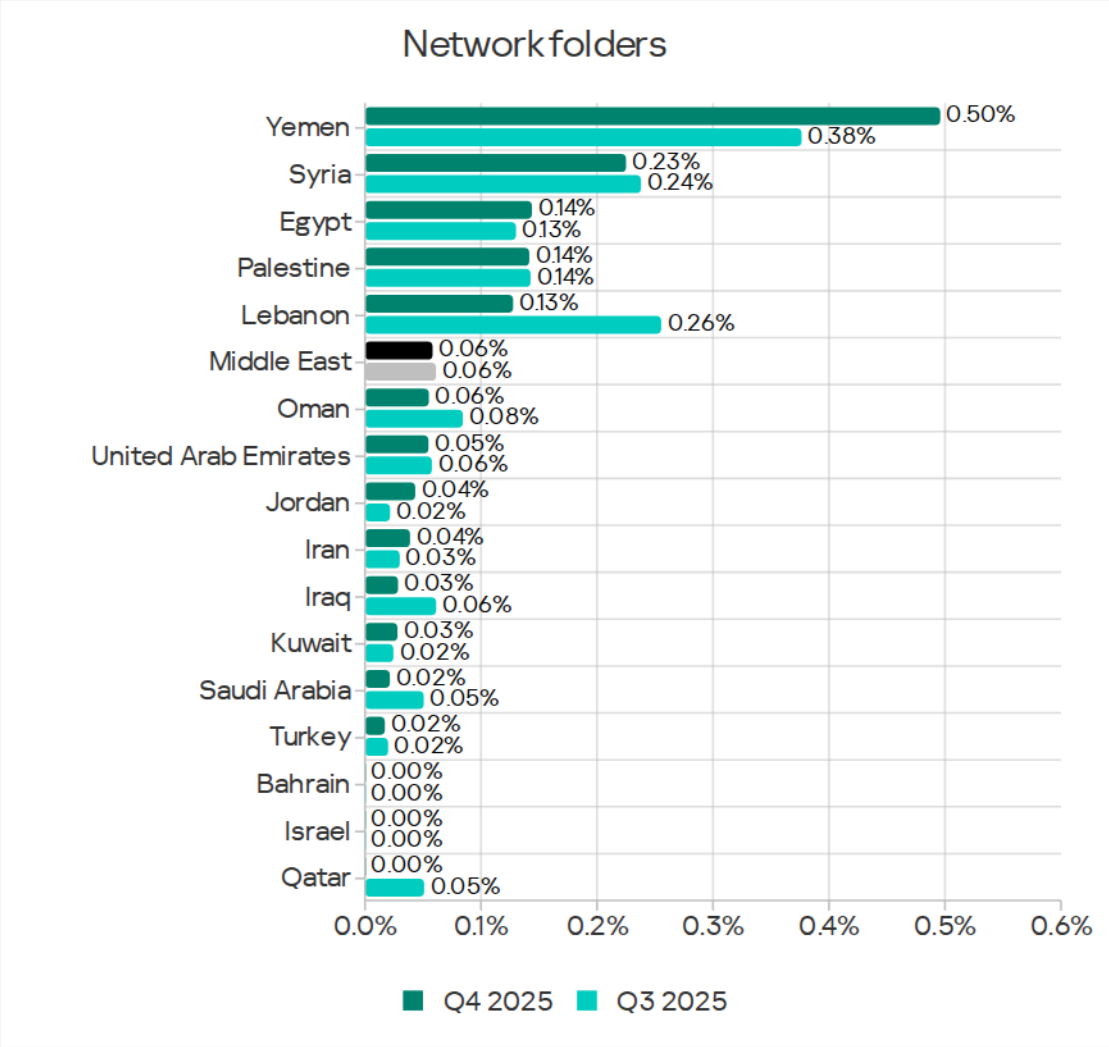
The main categories of removable media threats blocked on ICS computers in the region were worms, viruses, and spyware. The Middle East ranked second globally by percentage of ICS computers on which worms were blocked.



Network folders

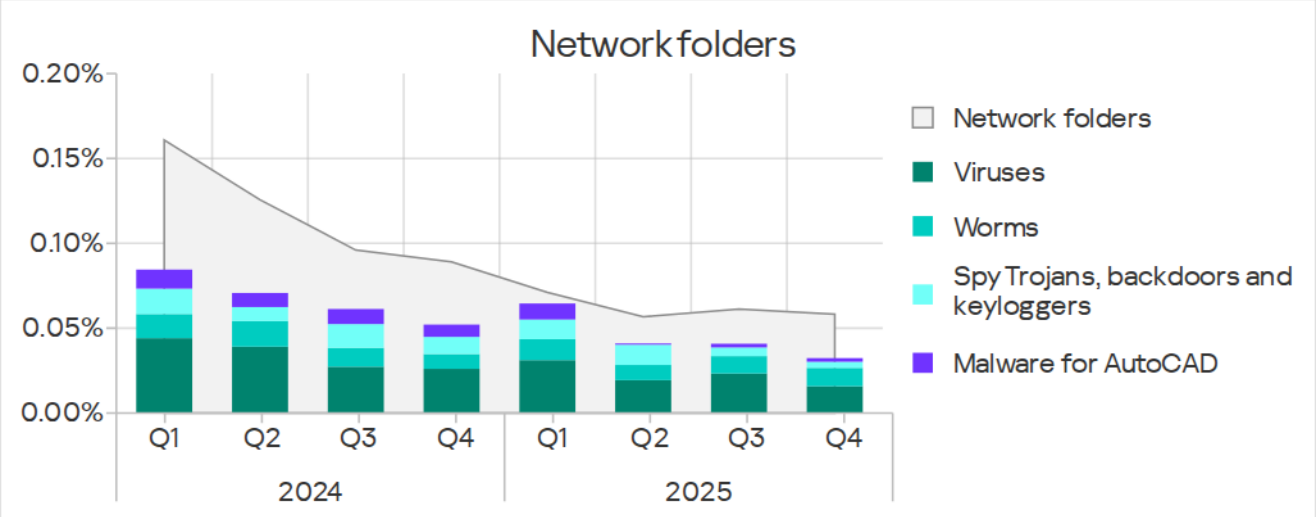
In Q4 2025, the ranked third among regions by percentage of ICS computers on which threats from network folders were blocked, with 0.06%. This was 8.3 times higher than in Northern Europe, which ranked last.

Yemen led the Middle East region by a wide margin with 0.50%.



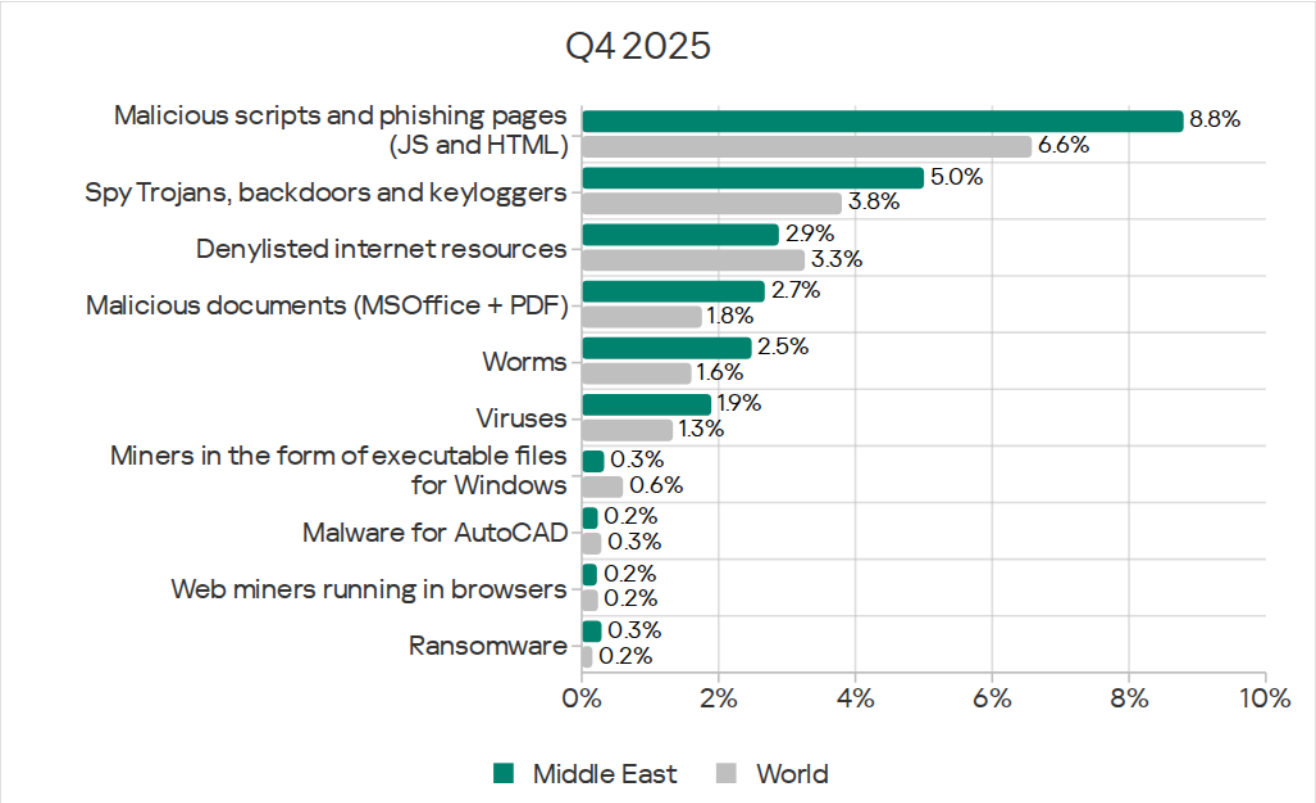
Note that threats from network folders were not blocked in all countries in the region.

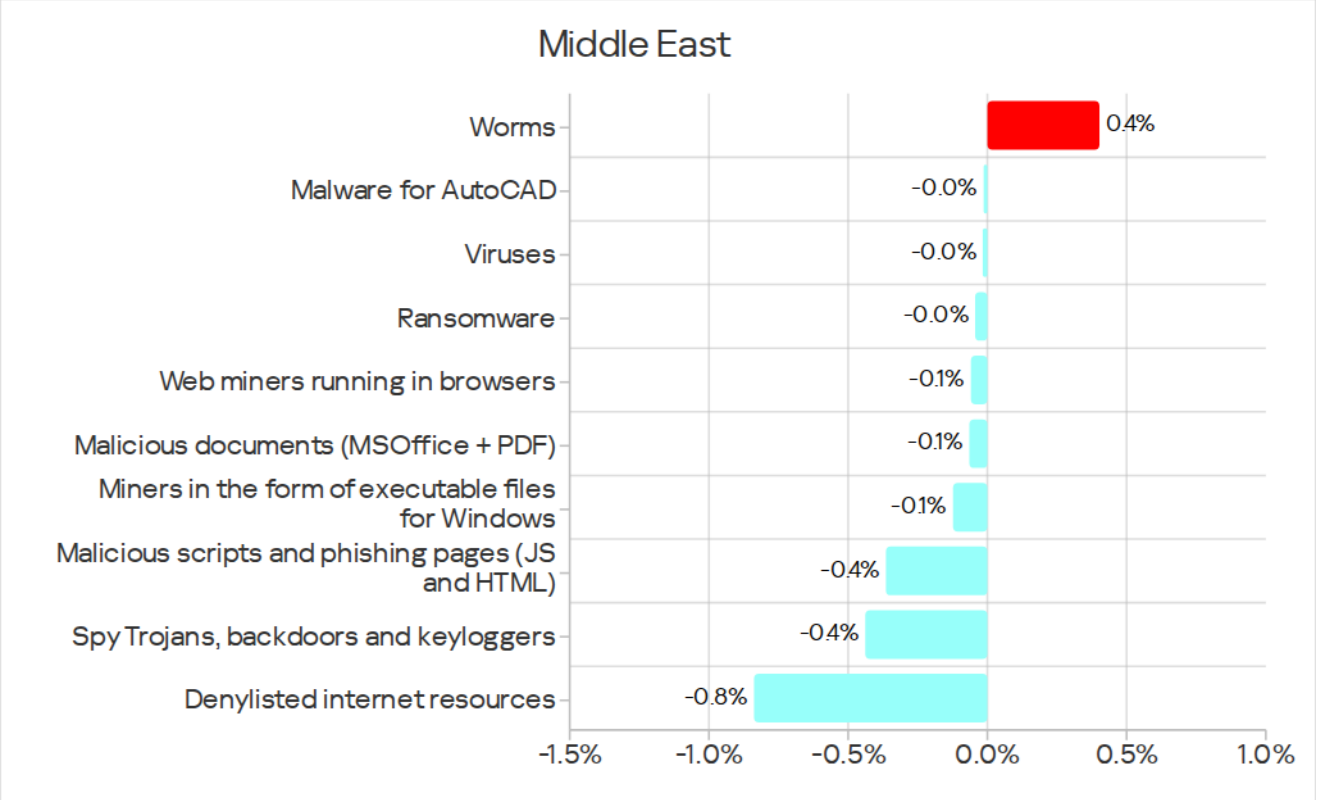
The main categories of threats from network folders were viruses, worms, and spyware.



Threat categories

In the Middle East, the percentage of ICS computers on which malicious objects were blocked was higher than the global average across all categories, except for denylisted internet resources, miners in the form of executable files for Windows, and malware for AutoCAD.





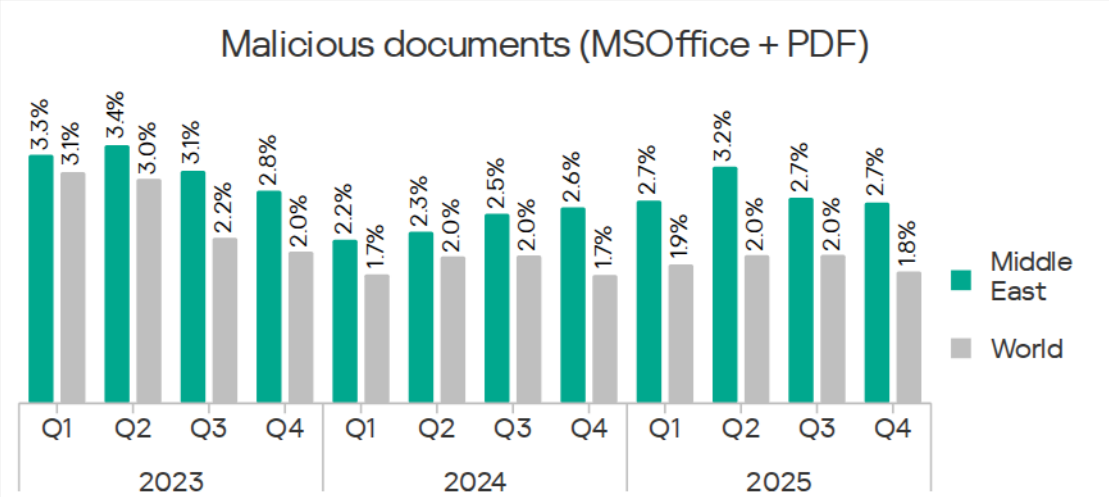
The largest differences compared with global averages were in the following threat categories:

- Ransomware: 1.8 times higher (first globally).
- Worms: 1.6 times higher (second globally).
- Malicious documents: 1.5 times higher (fourth globally).
- Viruses: 1.4 times higher (fourth globally).
- Spyware: 1.3 times higher (fourth globally).
- Malicious scripts and phishing pages: 1.3 times higher (fifth globally).

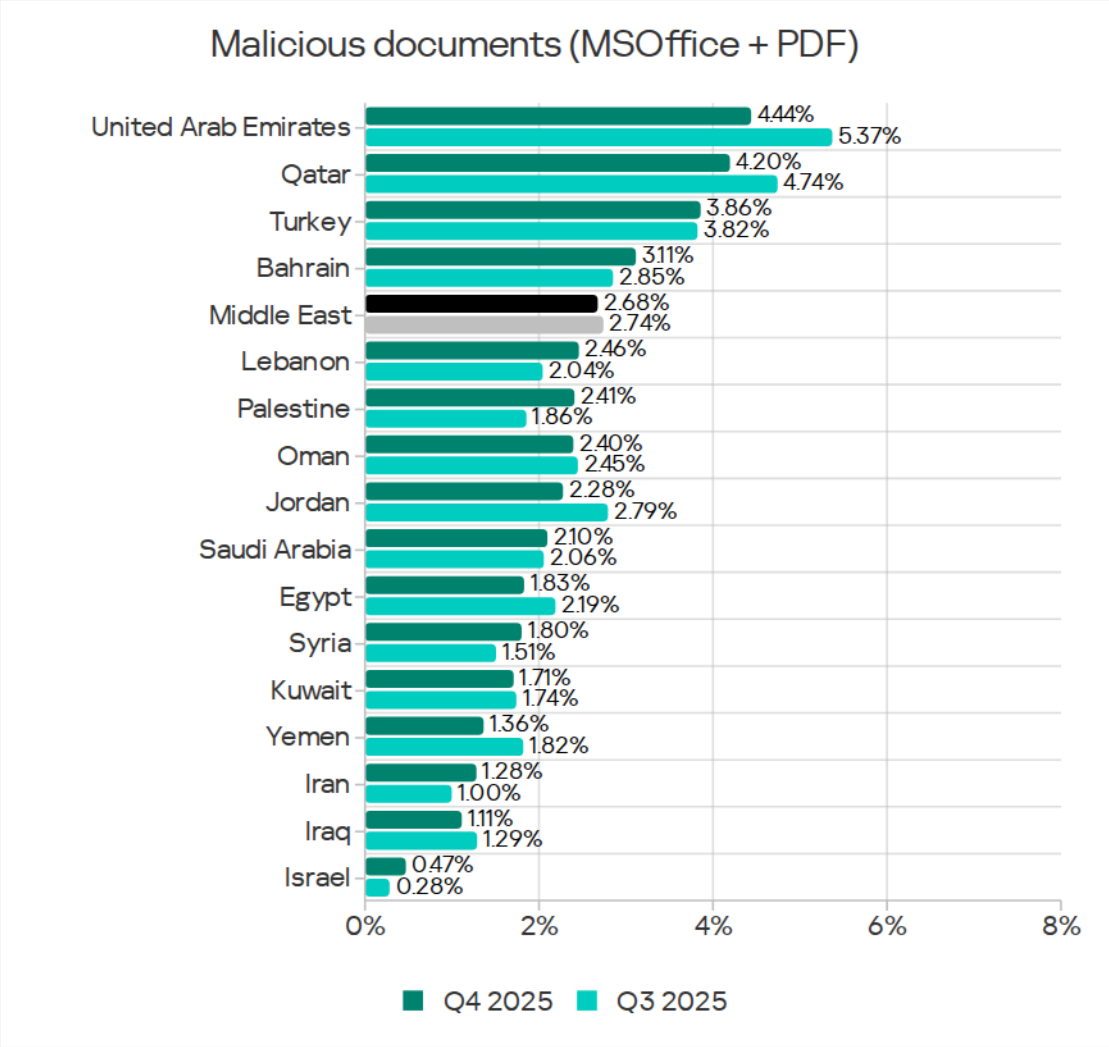
Malicious documents

In Q4 2025, the Middle East ranked fourth in terms of percentage of ICS computers on which malicious documents were blocked, with 2.68%. This was 5.8 times higher than in Northern Europe, which ranked last in this category.

This percentage had been on the rise since Q2 2024, but decreased over the past two quarters.



Among the region's countries and territories, the UAE led this ranking with 4.44%. Israel came last with 0.47%.

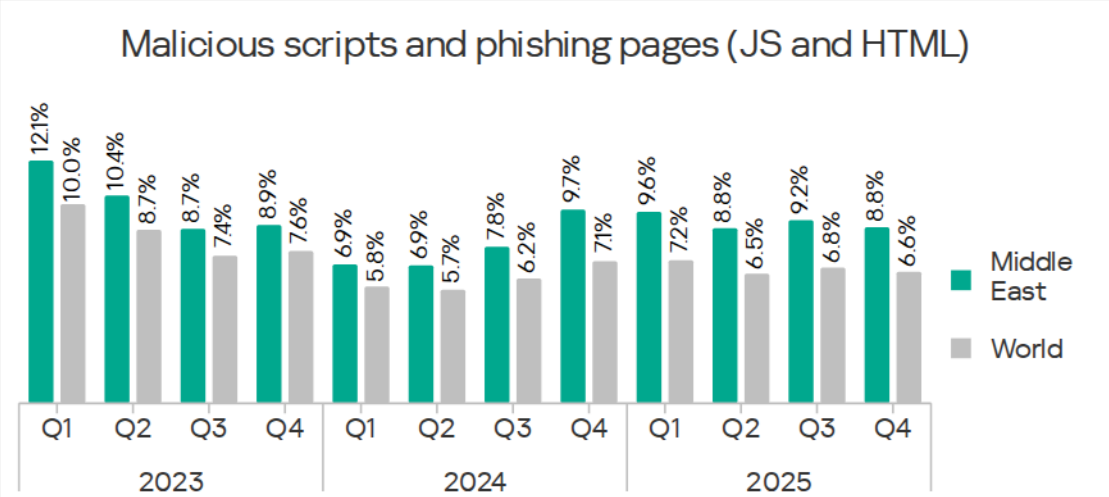


Malicious documents spread mainly via email.

Two countries in this ranking (the UAE and Qatar) also led the rankings for malicious scripts and phishing pages, malicious documents, as well as email client threats. They were also among the top three countries by percentage of ICS computers on which spyware was blocked.

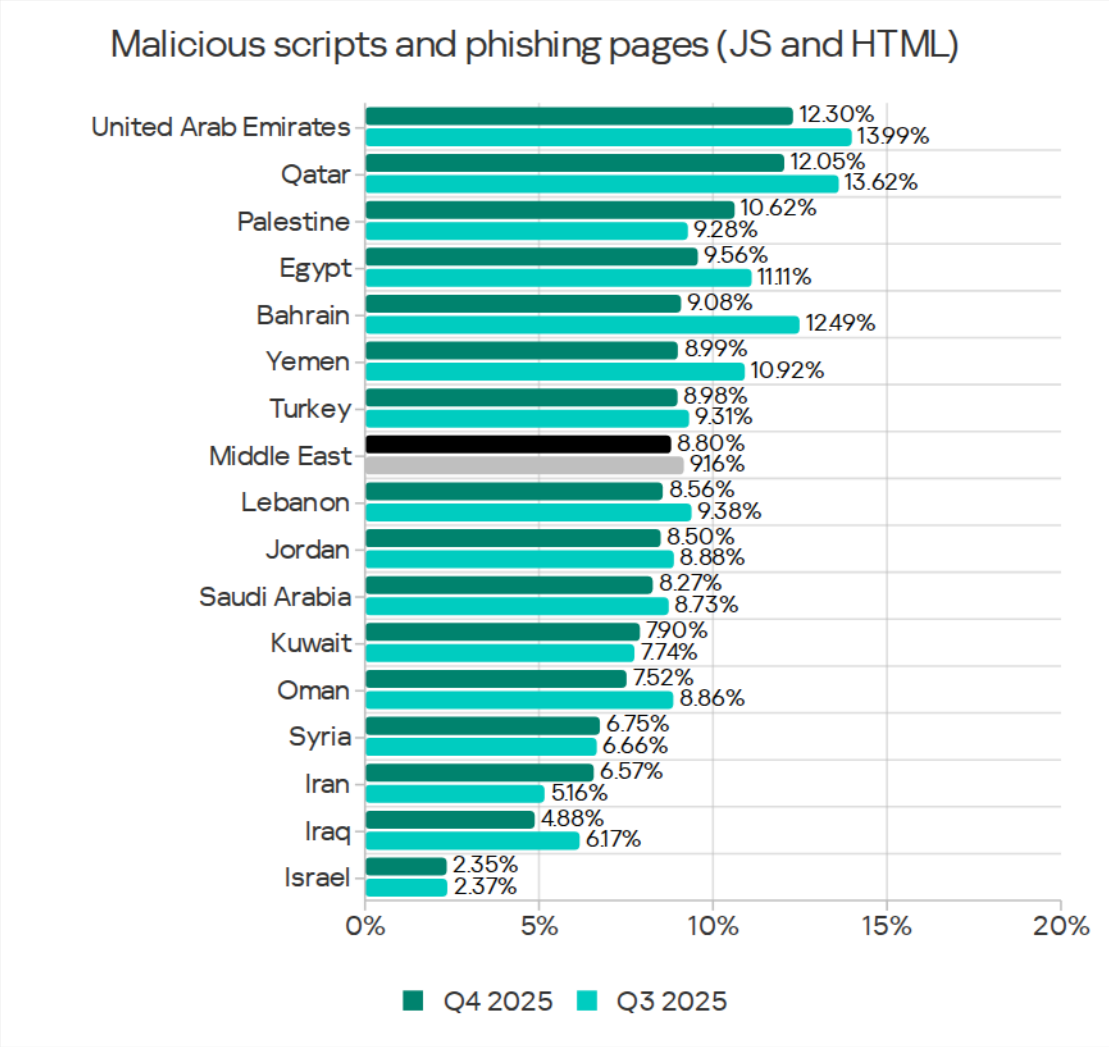
Malicious scripts and phishing pages

In terms of ICS computers on which malicious scripts and phishing pages were blocked, the Middle East ranked fifth globally with 8.80%. This was 3.5 times higher than in Northern Europe, which had the lowest figure.



These threats spread both from internet and via email.

Among the region's countries and territories, the UAE led in terms of percentage of ICS computers on which malicious scripts and phishing pages were blocked with 12.30%. Israel had the lowest figure (2.35%).

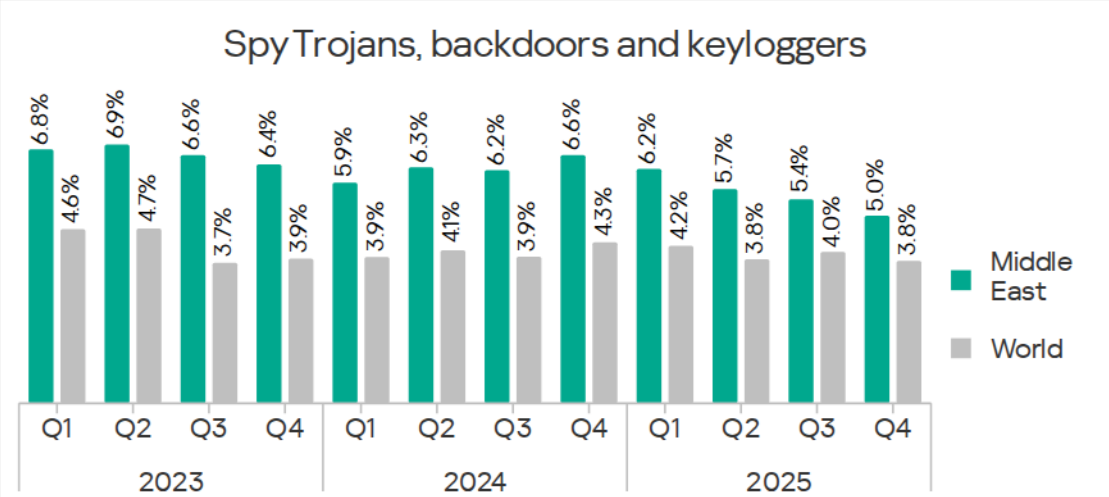


The two leading countries in this ranking (the UAE and Qatar) also topped the ranking for malicious documents and the regional ranking by percentage of ICS computers on which threats from email clients were blocked. They were also among the top three countries in the spyware ranking (topped by Yemen).

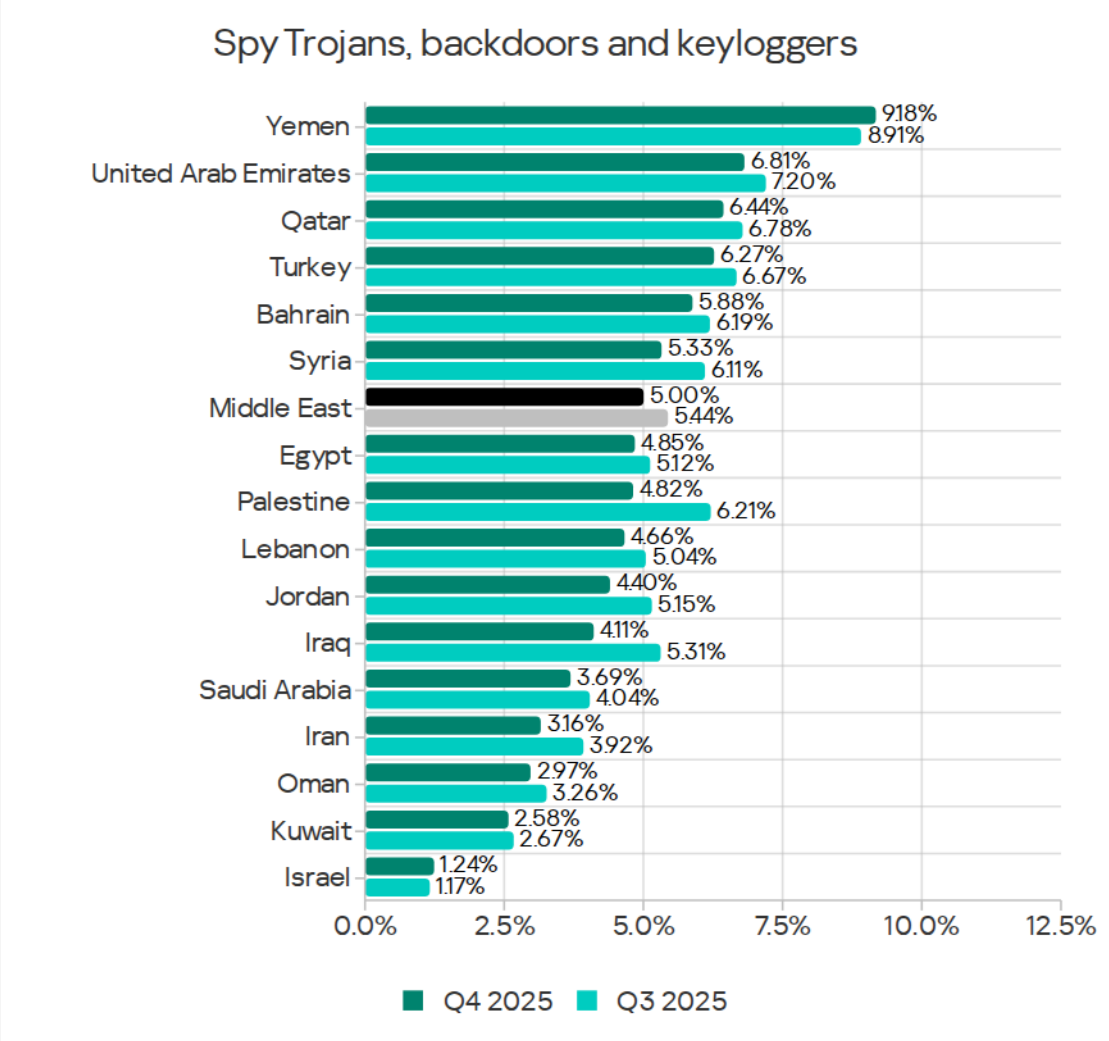
Spyware

By percentage of ICS computers on which spyware was blocked, the Middle East ranked fourth with 5.00%. This figure was four times higher than in Northern Europe, which had the lowest rate.

The percentage for this threat decreased throughout 2025 in the Middle East, reaching its lowest level over the past three years in Q4.



In Q4 2025, among the countries and territories in the region, Yemen led by percentage of ICS computers on which spyware was blocked, with 9.18%. Israel had the lowest figure (1.24%).



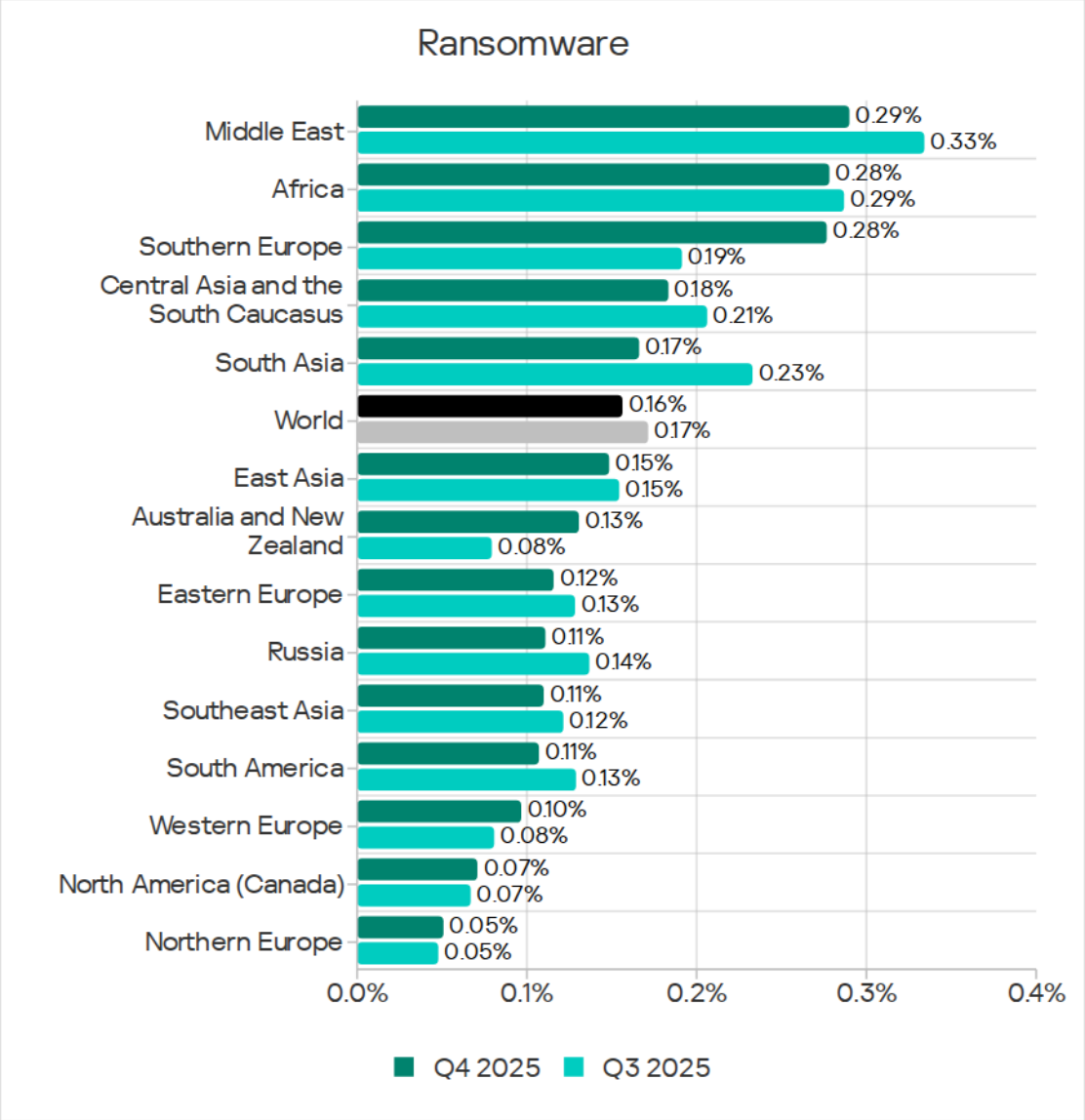
Although spyware in the region was blocked from all threat sources, this threat most often spreads via email clients.

Two of the top three countries in the spyware ranking (the UAE and Qatar) also ranked first in terms of email client threats. And they lead the region by percentage of ICS computers on which malicious documents, and malicious scripts and phishing pages were blocked.

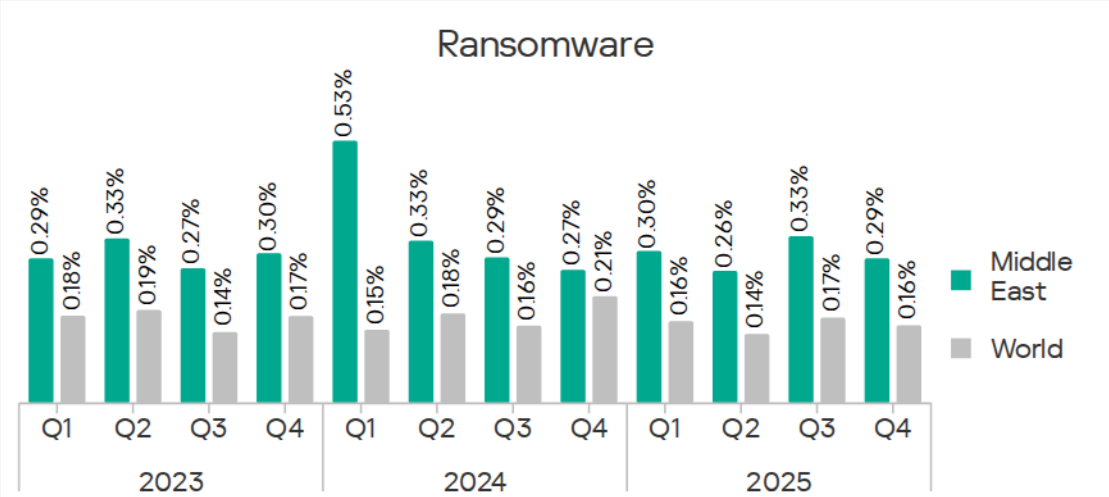
Spyware is used by attackers to steal confidential data and, in the case of targeted attacks, to spread throughout an organization's network and download the final payload. In some cases, spyware infections result in the installation of ransomware.

Ransomware

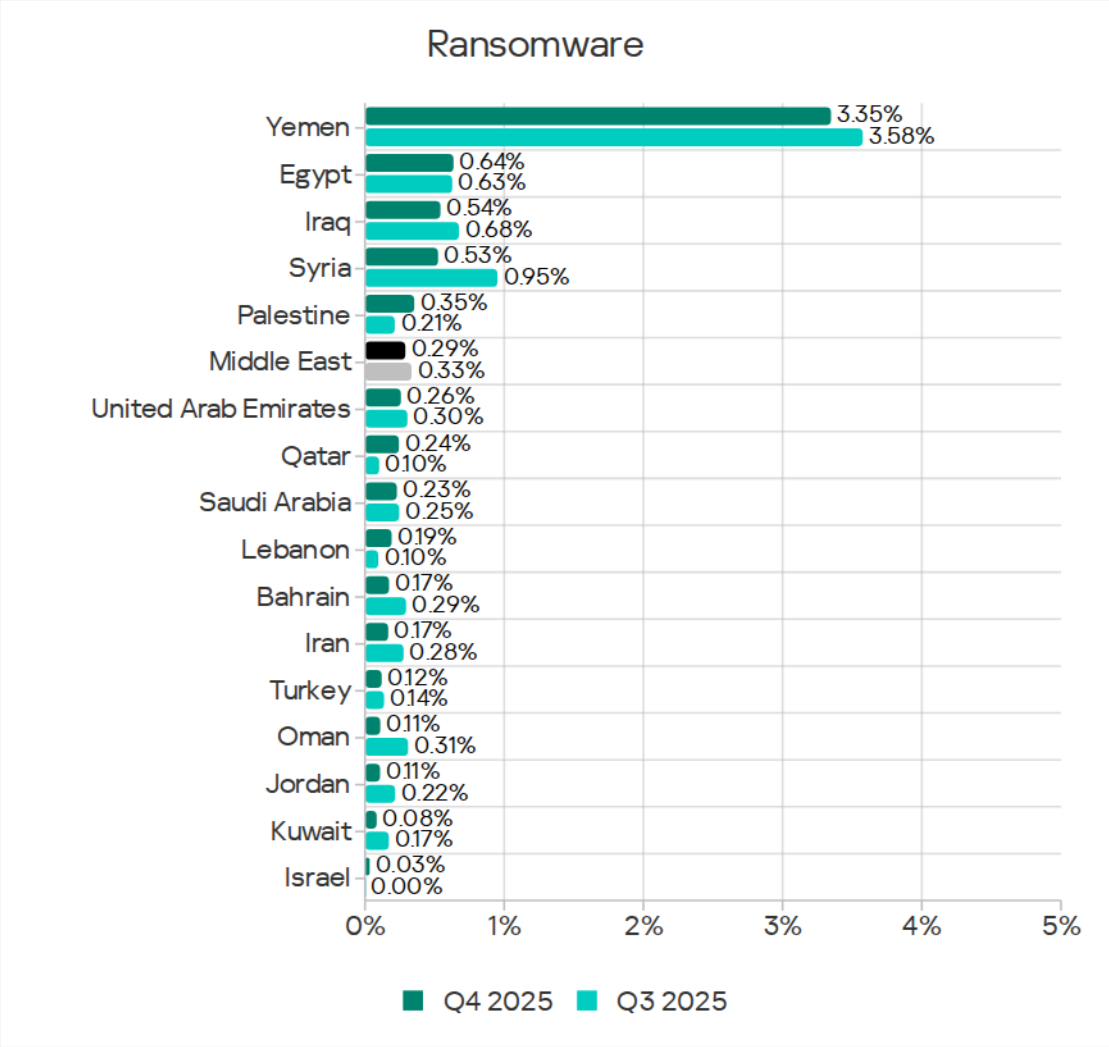
In Q4 2025, the Middle East remained in first place among the regions in terms of the percentage of ICS computers on which ransomware was blocked.



Since 2023, the indicator in the region has ranged from 0.26% to 0.33%. In Q4 2025, it decreased to 0.29%. This was 5.8 times more than Northern Europe in last place.



Yemen led the region by a huge margin in terms of the percentage of ICS computers on which ransomware was blocked, with a substantial figure of 3.35% for this category of threat. In other countries, the rates ranged from 0.64% in Egypt to 0.03% in Israel.



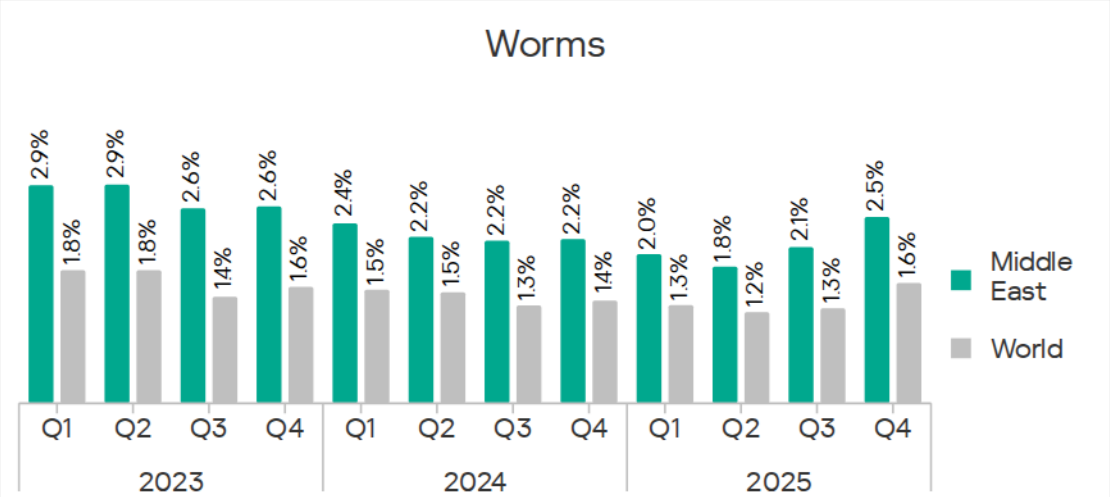
In the Middle East, this threat is most often spread via email clients and from removable media.

Worms

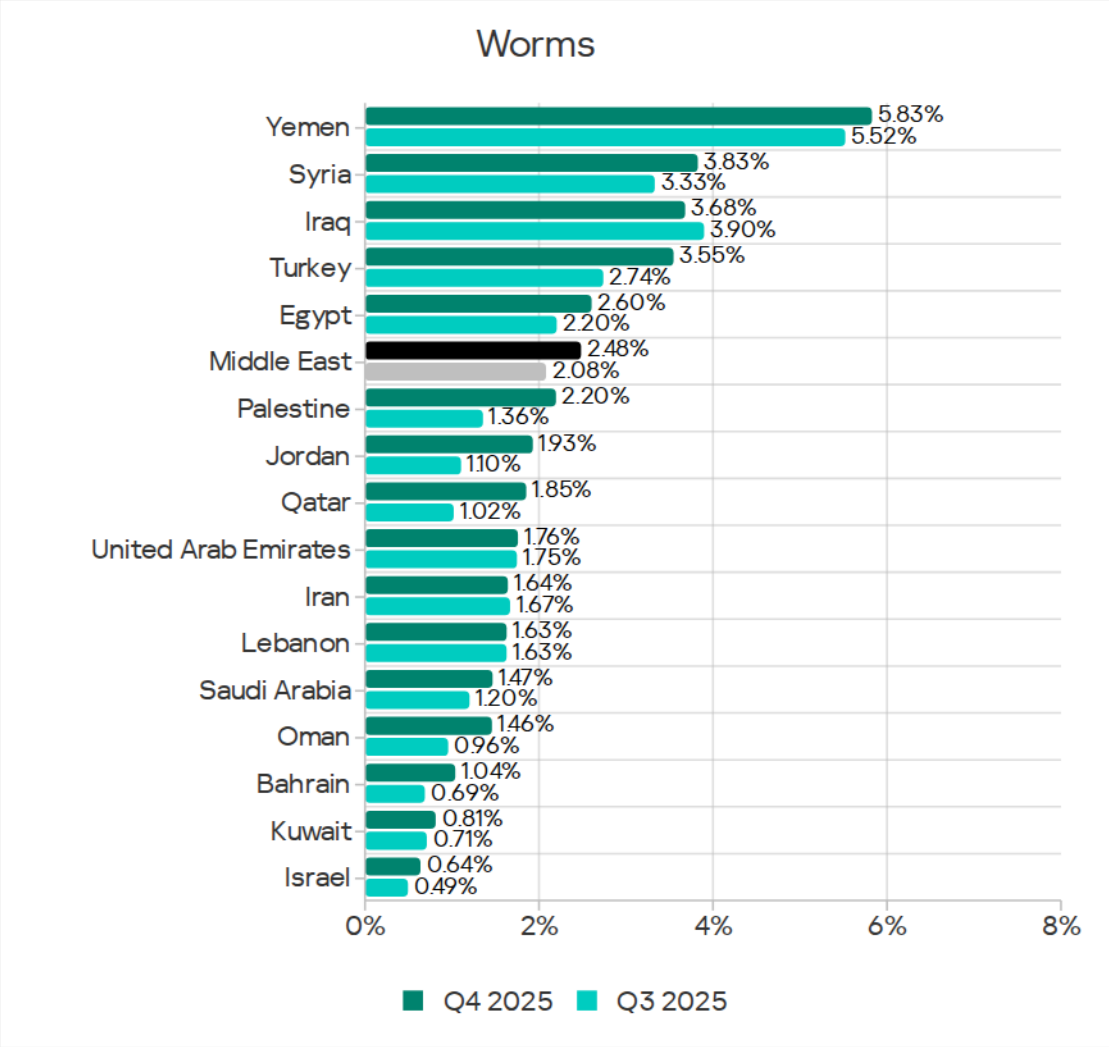
In Q4 2025, the Middle East ranked second in the regional ranking for the percentage of ICS computers on which worms were blocked, at 2.48%. This was 7.8 times higher than the lowest rate in Northern Europe.

During the quarter, phishing campaigns spread the backdoor worm Backdoor.MSIL.XWorm, resulting in an increased percentage of ICS computers on which worms were blocked in all regions.

Worms were the only threat category in the region that increased in Q4 of 2025. Based on this growth, the Middle East ranked fourth among the regions.

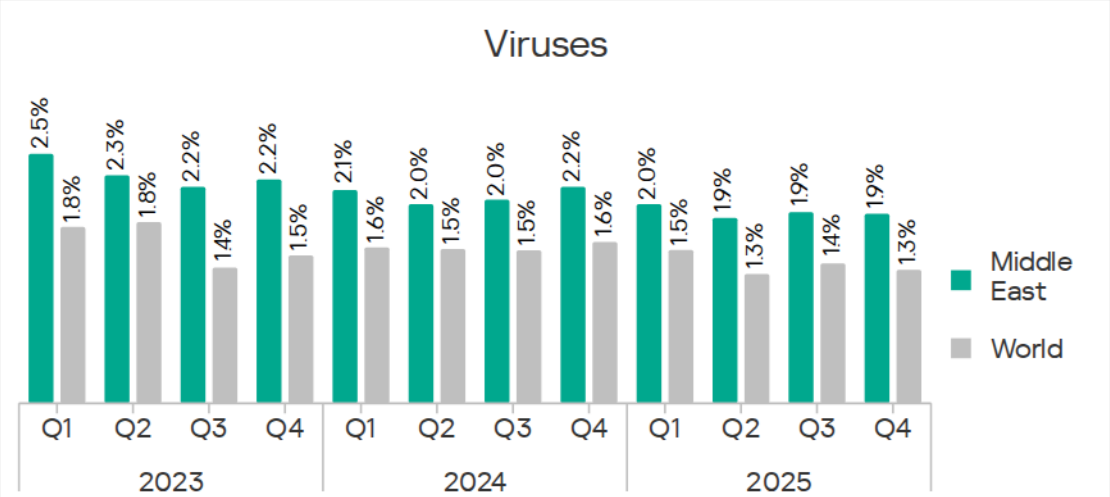


Yemen led the region by a wide margin in terms of the percentage of ICS computers on which worms were blocked, at 5.83%. It should be noted that the indicator increased in all countries during the quarter, with a few exceptions: it remained unchanged in Lebanon, while it decreased in Iran and Iraq.

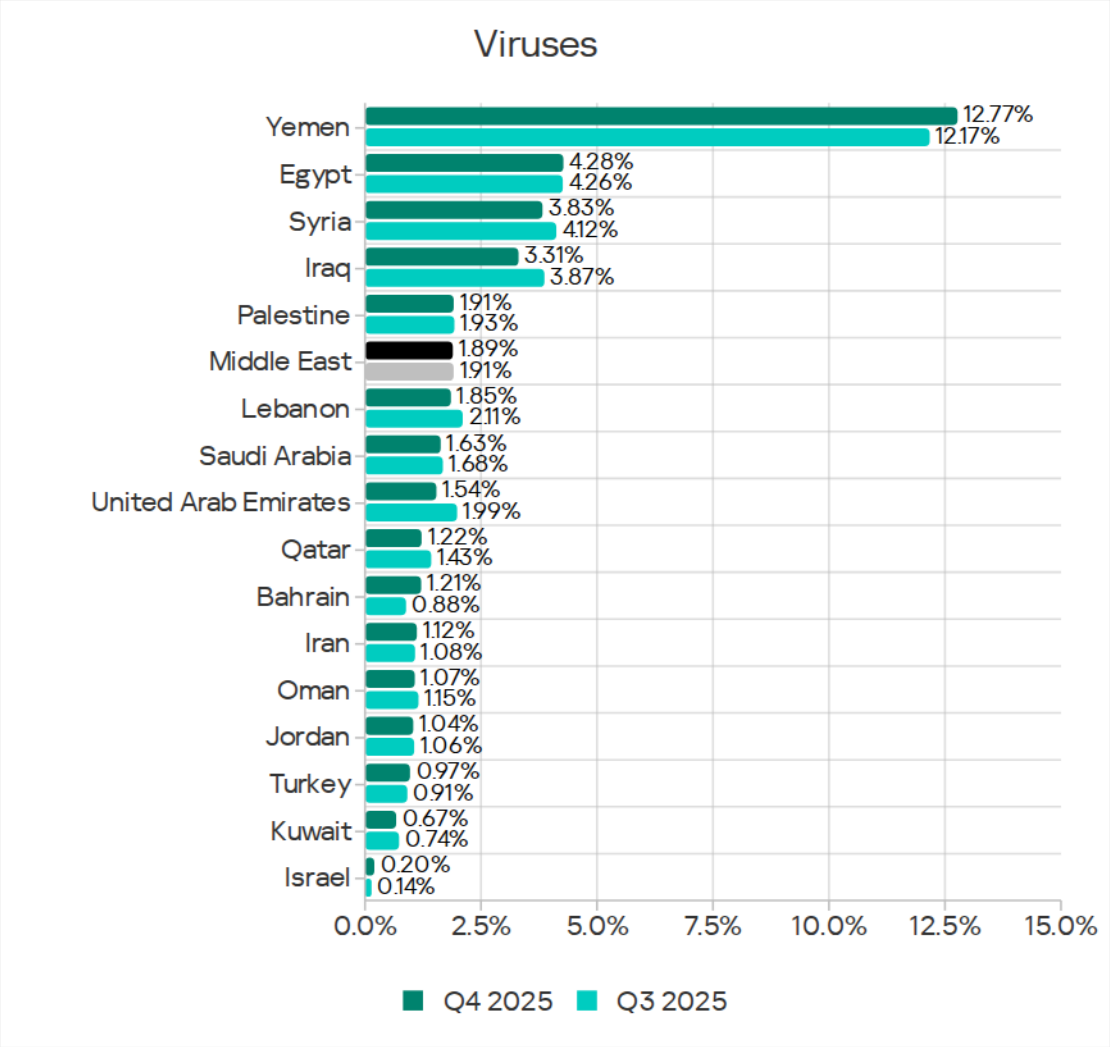


Viruses

The Middle East ranked fourth in terms of the percentage of ICS computers on which viruses were blocked. The figure decreased slightly to 1.89%. This was 12.6 times higher than in Western Europe, which had the lowest rate among all regions.



Yemen led the region by a wide margin in terms of the percentage of ICS computers on which viruses were blocked, at 12.77%. This figure was three times higher than that of Egypt, the next country in the ranking. Compared to Israel, which came bottom of the ranking, Yemen's rate was 63.9 times higher.

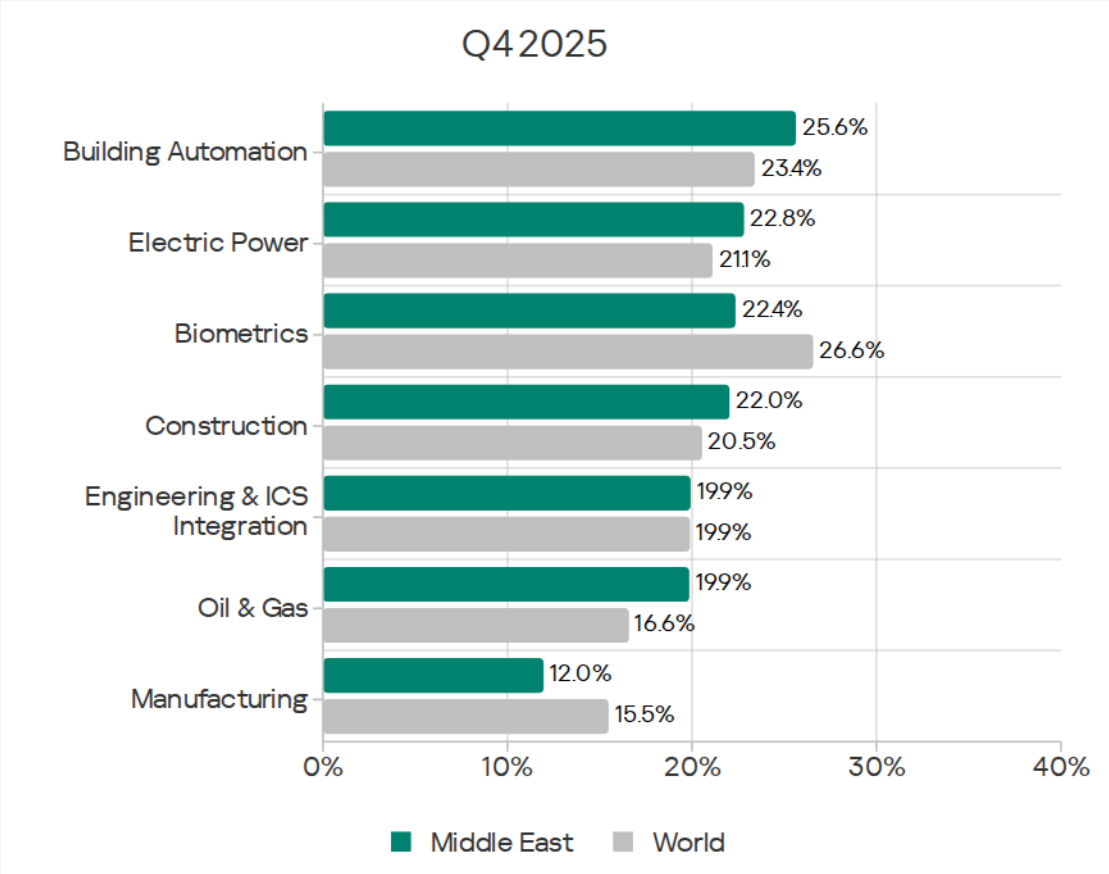


Industries

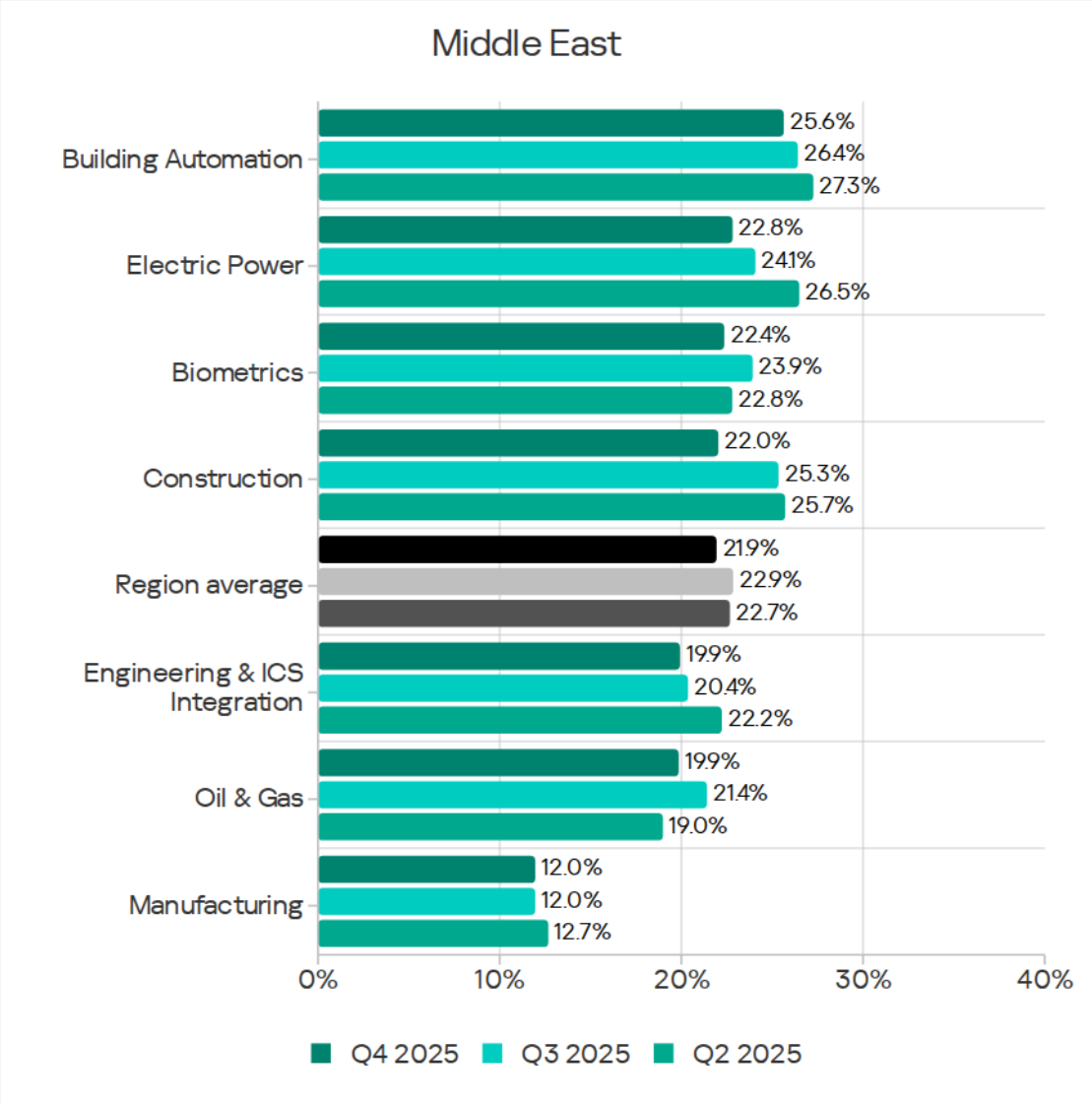
Among the industries covered in this report, the most frequently targeted in the Middle East was building automation.

The percentage of ICS computers on which malicious objects were blocked exceeded the global average in the following industries:

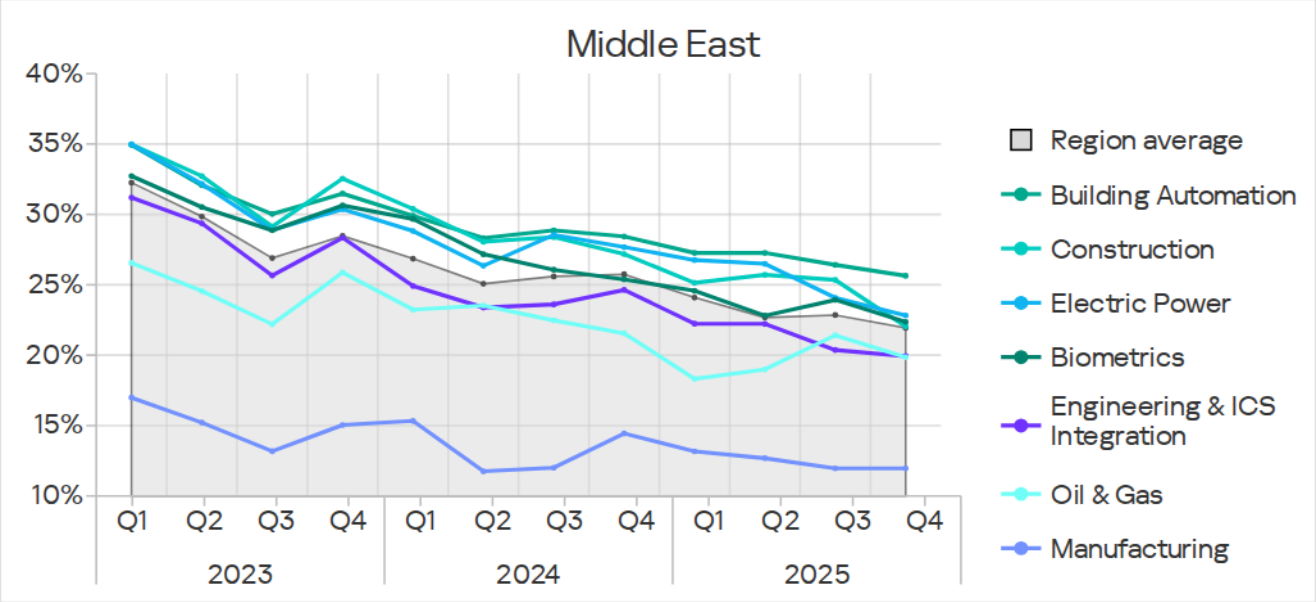
- Building automation: 1.1 times higher.
- Electrical energy: 1.1 times higher.
- Construction: 1.1 times higher.
- Oil and gas: 1.2 times higher.



In Q4 2025, the percentage of ICS computers on which malicious objects were blocked decreased in all industries except manufacturing, where the indicator was unchanged.



Despite periodic fluctuations, long-term trends show a generally positive dynamic (declining values).



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 the Middle East, Q4 2025

Industry / Threat source	Biometrics	Building Automation	Engineering & ICS Integration	Electric Power	Oil & Gas	Construction	Manufacturing	Category metric in region
Internet	7.49%	8.55%	7.86%	8.71%	6.94%	8.88%	4.67%	7.89%
Email clients	4.60%	7.57%	3.57%	3.71%	2.03%	4.48%	1.92%	5.06%
Removable media	1.21%	0.66%	0.42%	0.55%	0.39%	0.41%	0.35%	0.57%
Network folders	0.13%	0.08%	0.04%	0.04%	—	0.06%	—	0.06%
Industry metric in region	22.36%	25.64%	19.93%	22.82%	19.85%	22.03%	11.96%	

Threat category indicators for industries in the Middle East, Q4 2025

Industry / Threat type	Biometrics	Building Automation	Engineering & ICS Integration	Electric Power	Oil & Gas	Construction	Manufacturing	Category metric in region
Denylisted internet resources	3.05%	3.10%	2.94%	3.05%	2.93%	2.69%	1.92%	2.88%
Malicious scripts and phishing pages (JS and HTML)	8.41%	11.43%	7.28%	7.80%	5.53%	8.88%	4.29%	8.80%
Malicious documents (MSOffice + PDF)	3.23%	4.18%	1.70%	2.25%	1.02%	1.83%	0.92%	2.68%
Spy Trojans, backdoors and keyloggers	5.75%	7.26%	3.60%	4.36%	1.97%	3.60%	2.05%	5.00%
Ransomware	0.53%	0.45%	0.15%	0.34%	0.17%	0.21%	0.06%	0.29%
Miners in the form of executable files for Windows	0.32%	0.36%	0.40%	0.34%	0.28%	0.43%	0.19%	0.33%
Web miners running in browsers	0.29%	0.20%	0.28%	0.25%	0.34%	0.40%	0.13%	0.22%
Malware for AutoCAD	0.18%	0.20%	0.23%	0.13%	0.17%	1.02%	0.16%	0.23%
Worms	2.44%	3.46%	1.98%	2.46%	1.35%	1.39%	1.48%	2.48%
Viruses	2.84%	2.55%	1.23%	1.97%	1.97%	1.81%	1.04%	1.89%
Industry metric in region	22.36%	25.64%	19.93%	22.82%	19.85%	22.03%	11.96%	

The main problems in the region's industries

A high rate of ransomware. The Middle East ranked first in the ranking of regions in terms of the percentage of ICS computers on which ransomware were blocked. The region ranked no lower than fifth in the regional rankings across all industries except manufacturing.

High level of threats from email clients. This problem is relevant for several industries. In terms of the percentage of ICS computers on which threats from

email clients in various industries were blocked, the Middle East ranked among the regions as follows:

- First in the electric power industry (the region also ranked second in this industry for malicious documents).
- Second in the oil and gas and construction industries.
- Third in building automation and the engineering and ICS integrators industries.

The relevance of removable media as a threat source to IT infrastructure biometrics, as well as engineering and ICS integrators and oil and gas industries. In terms of threats from removable media in these industries, the Middle East ranked third among all the regions. In terms of worms in the engineering and ICS integrators industry, the region ranked second.

Building automation

The Middle East ranked fourth by percentage of ICS computers on which malicious objects were blocked in the building automation industry.

Among all regions by industry indicators, the Middle East ranked:

- Second in the percentage of ICS computers on which threats from network folders were blocked.
- Third for threats from email clients.
- Second by percentage of ICS computers on which ransomware was blocked.
- Third in terms of malicious documents, spyware, and malware for AutoCAD.

Among industries in the region, building automation ranked:

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

Electric power

The Middle East ranked fourth by percentage of ICS computers on which malicious objects were blocked in the electric power industry.

Among all regions by industry indicators, the Middle East ranked:

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

In the regional cross-industry rankings, the electric power industry ranked:

- Second in the percentage of ICS computers on which threats from the internet were blocked.
- Third for threats from removable media.
- Second by percentage of ICS computers on which denylisted internet resources, and worms were blocked.
- Third in terms of malicious documents, spyware, and ransomware.

Biometrics

The Middle East ranked sixth in the regional ranking by percentage of ICS computers on which malicious objects were blocked in biometric systems.

In the regional ranking by percentage of ICS computers on which threats in biometric systems were blocked, the Middle East ranked:

- First in the percentage of ICS computers on which threats from network folders were blocked.
- Third in threats from removable media.
- Third in the percentage of ICS computers on which viruses, and malware for AutoCAD were blocked.

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

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

Construction

The Middle East ranked fifth among all regions by percentage of ICS computers on which malicious objects were blocked in the construction industry.

Among all regions by industry indicators, the Middle East ranked:

- Second in the percentage of ICS computers on which threats from email clients were blocked.
- Third in the percentage of ICS computers on which malicious scripts and phishing pages, and web miners were blocked.

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

- First in the percentage of ICS computers on which threats from the internet were blocked.
- Third in terms of threats from email clients, and network folders.
- First in the percentage of ICS computers on which miners from both categories as well as malware for AutoCAD were blocked.
- Second in terms of malicious scripts and phishing pages.

Engineering and ICS integrators

The Middle East ranked fifth among regions by percentage of ICS computers on which malicious objects were blocked in the engineering and ICS integrators industry.

Among all regions by industry indicators, the Middle East ranked:

- Second in the percentage of ICS computers on which threats from network folders were blocked.
- Third in threats from email clients, and removable media.
- Second in the percentage of ICS computers on which worms were blocked.

Among the industries in the region, engineering and ICS integrators ranked second in terms of miners in the form of executable files for Windows, and malware for AutoCAD

Oil and gas

The Middle East ranked second among the five regions represented in the oil and gas industry by percentage of ICS computers on which malicious objects were blocked.

Among the regions by industry indicators, the Middle East ranked:

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

In the regional cross-industry rankings, oil and gas was:

- Second in the percentage of ICS computers on which web miners were blocked.
- Third in terms of viruses.

Manufacturing

The Middle East ranked 10th by percentage of ICS computers on which malicious objects were blocked.

Methodology used to prepare statistics

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

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

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

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

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

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

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

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

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

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

Kaspersky ICS CERT ics-cert@kaspersky.com