Kaspersky ICS CERT

Threat landscape for industrial automation systems

Middle East. Q3 2025

24.12.2025

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 1.9 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 is 1.4 times higher than the global average, and the worm rate is 1.7 times higher.

High rate of spyware

The region's percentage of ICS computers on which spyware was blocked is 1.3 times higher than the global average, and the rate for malicious documents is 1.4 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 2024, the Middle East ranked first among regions by percentage of ICS computers on which ransomware was blocked; in Q1 and Q2 2025, it ranked second. In Q3 2025, the Middle East again led the region in ransomwara.

The Middle East ranks no lower than fourth across all regions' ransomware rankings in all industries except manufacturing.

Striking country-level differences

Yemen leads many of the region's rankings, often by a wide margin. The exception is email threats.

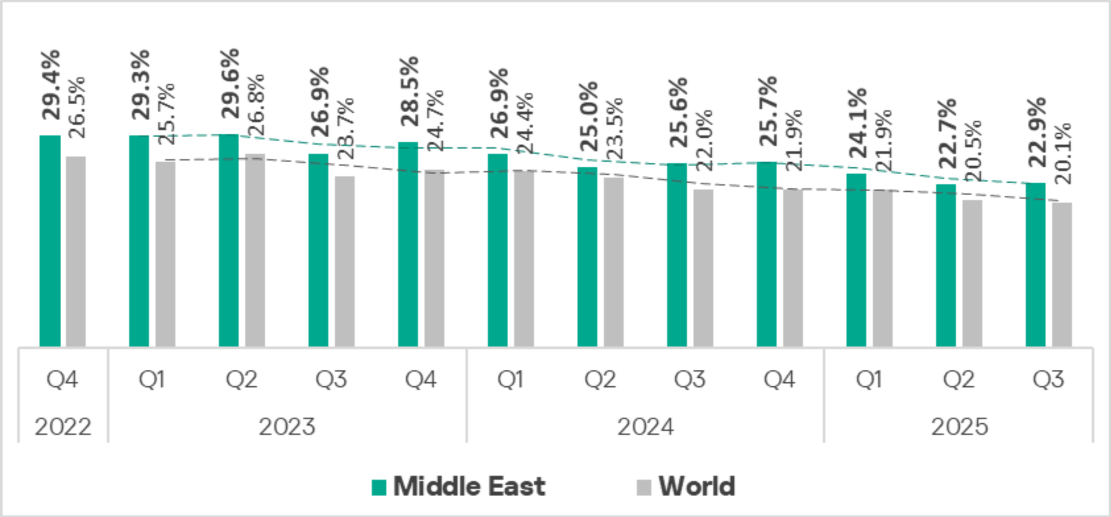
For threats from email clients, the UAE and Qatar hold the top positions. These same countries also rank among the leaders in malicious scripts and phishing pages, malicious documents, and spyware.

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

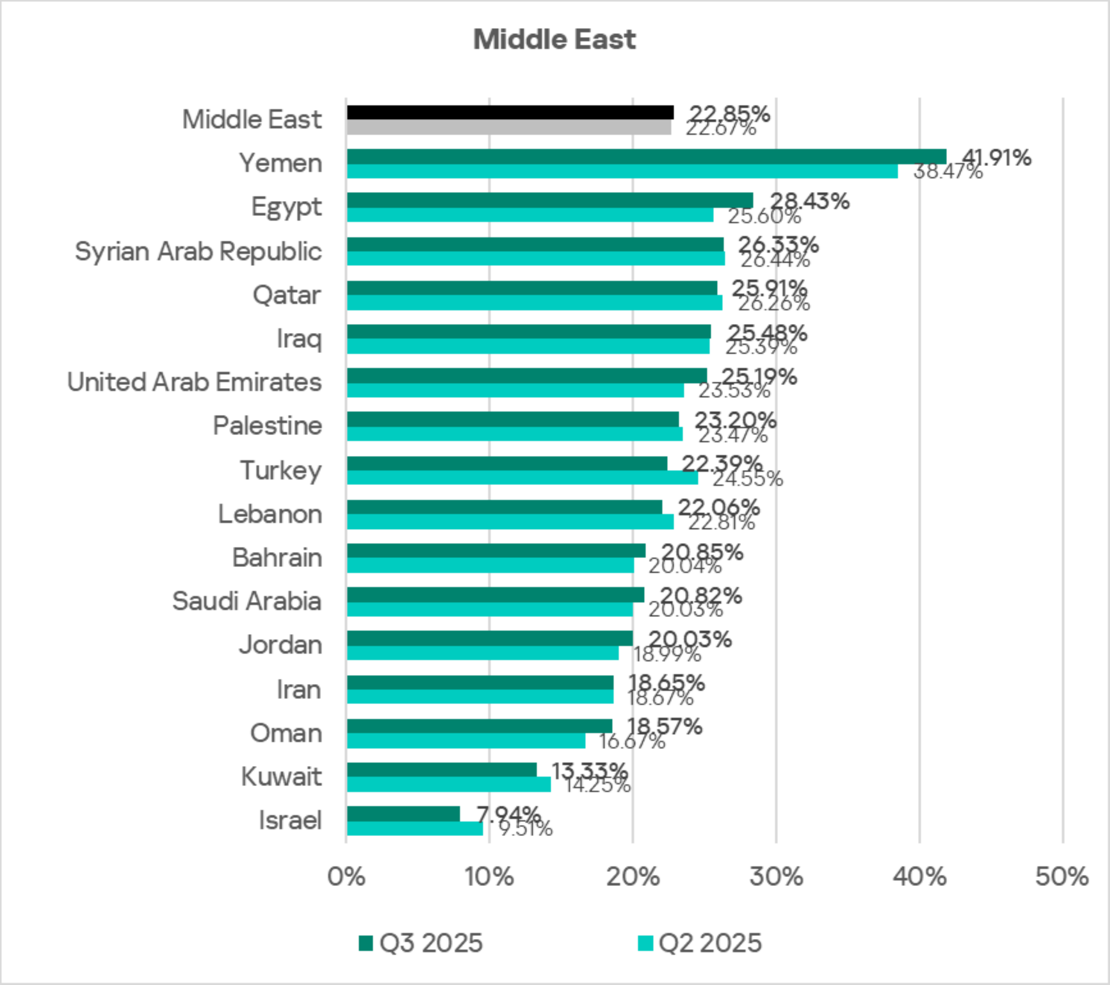
Statistics across all threats

In Q3 2025, the Middle East ranked fourth globally by percentage of ICS computers on which malicious objects were blocked. The region consistently exceeds the global average in this metric — in Q3 2025, by 1.1 times.

The percentage of ICS computers on which malicious objects were blocked in the Middle East rose slightly during the quarter, to 22.9%. This figure is 2.5 times higher than in Northern Europe, where the rate is minimal.



Within the region, rates vary from 7.54% in Israel to 41.91% in Yemen. These two countries are relative outliers, with the region's other countries ranging between 13% and 29%.



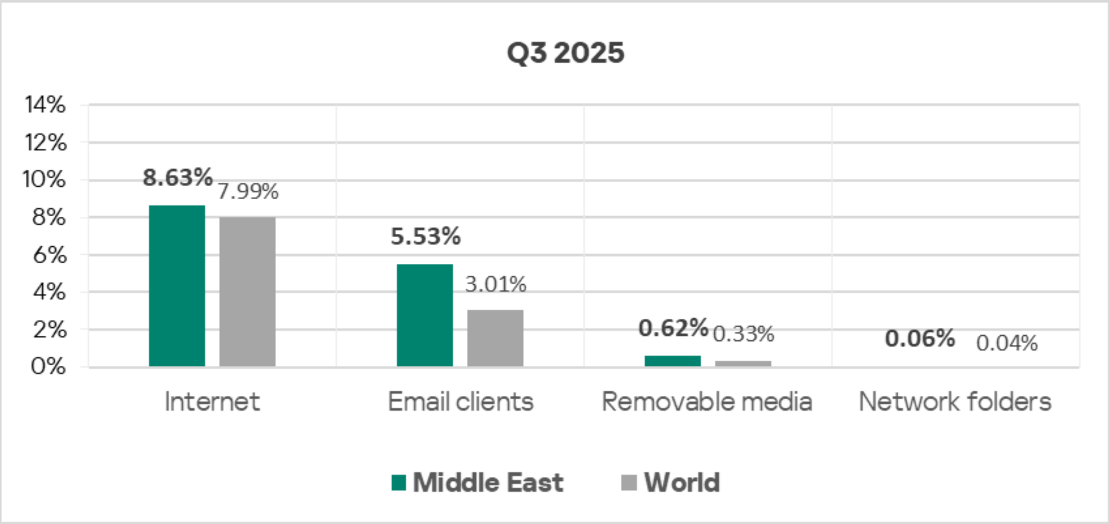
Yemen leads many regional rankings for both sources and categories of malware. In terms of email threats, as well as the malicious documents, malicious scripts and phishing pages, and malware for AutoCAD categories, the UAE holds top spot. Syria does likewise by percentage of ICS computers on which ransomware was blocked.

Israel consistently places at the bottom of most regional rankings.

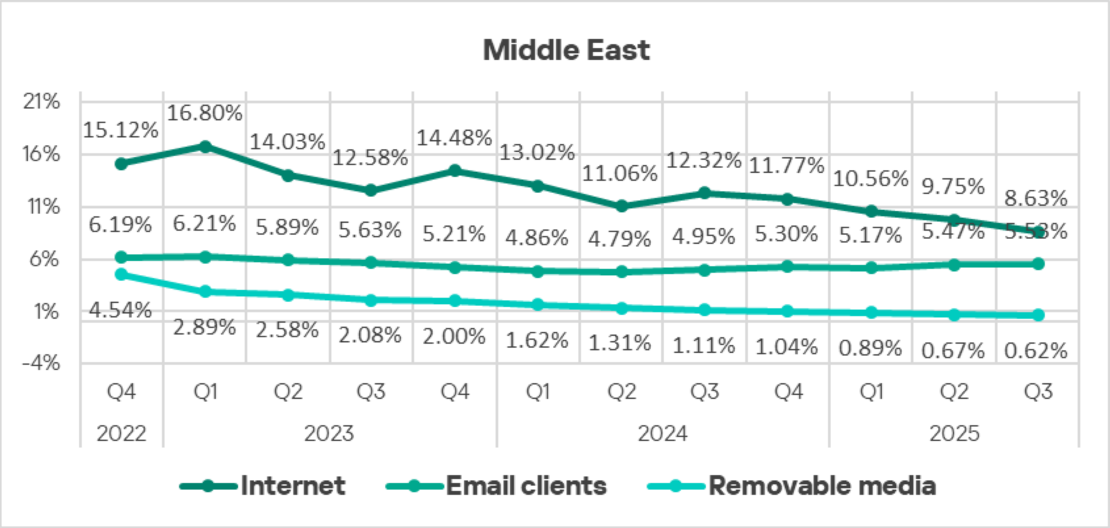
Threat sources

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

- Email client threats: 1.8 times higher.
- Removable media threats: 1.9 times higher.



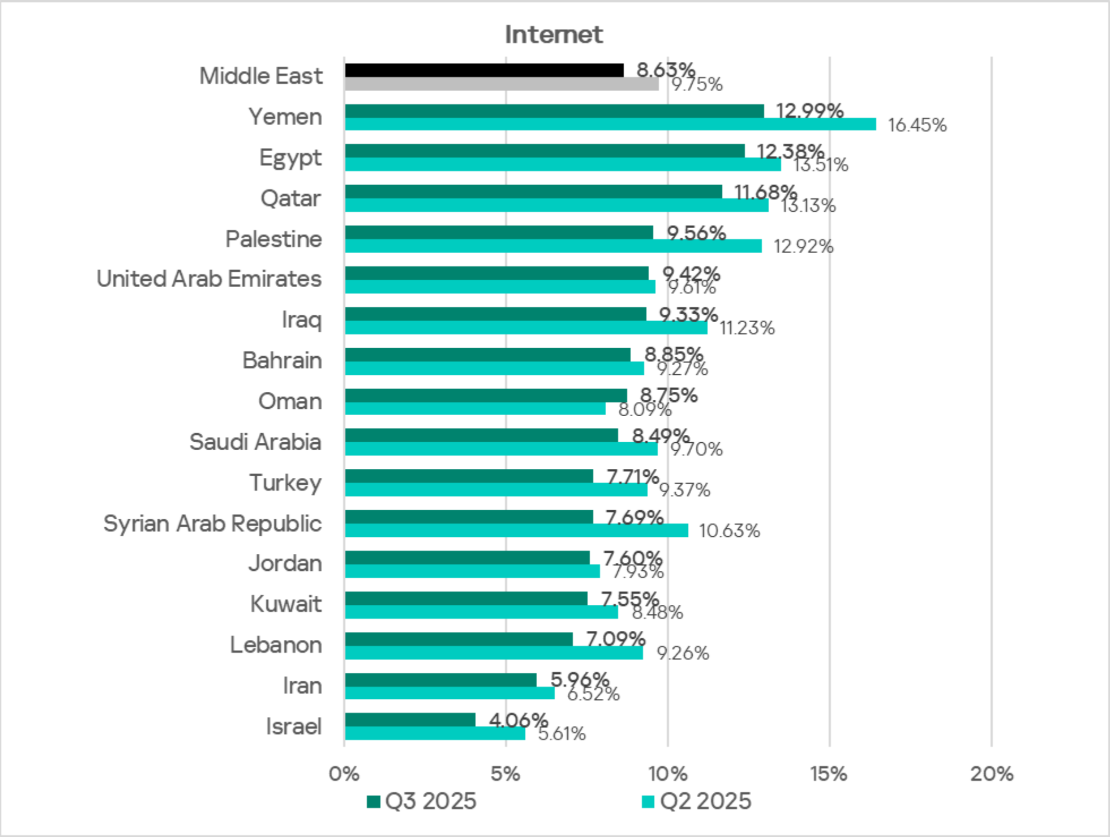
The percentage of attacked ICS computers is increasing only for email clients. All the other threat sources are trending downward.



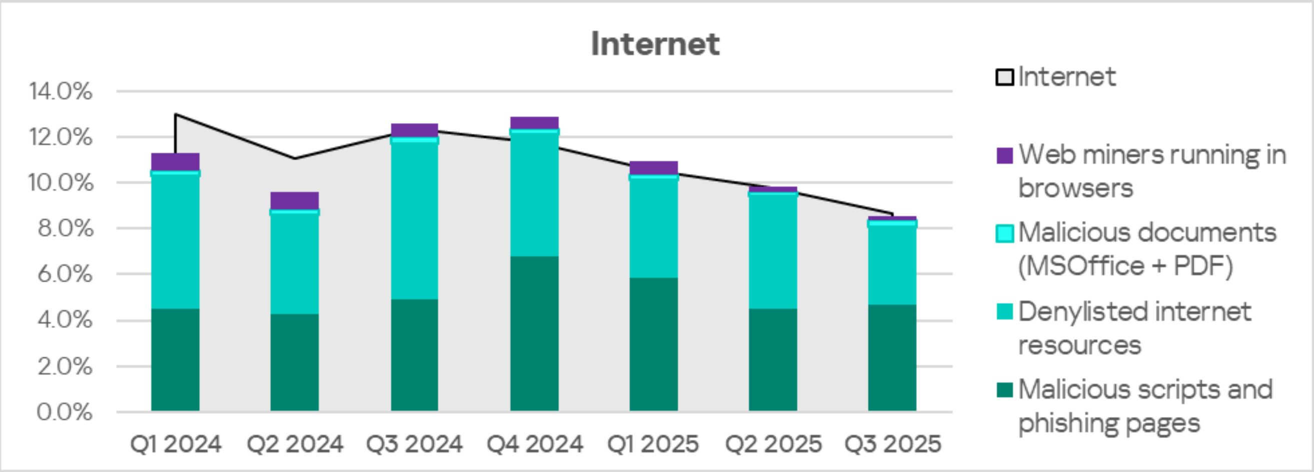
Internet

By percentage of ICS computers on which internet threats were blocked, the Middle East ranks fifth in the regional rankings with 8.63%, which is 1.9 times higher than the lowest score in Northern Europe.

Country-level rates range from 4.06% in Israel to 12.99% in Yemen.

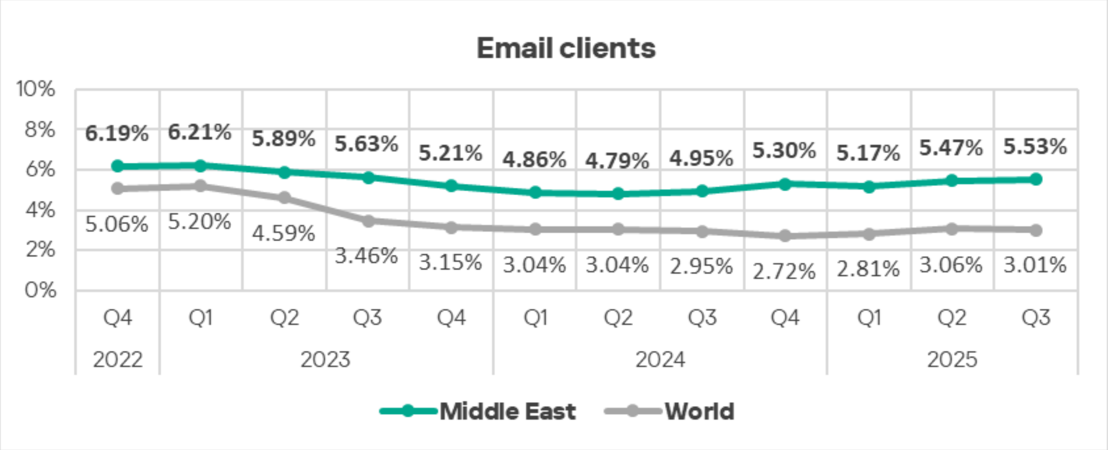


The main categories of internet threats that are blocked on ICS computers in the region include malicious scripts and phishing pages, as well as denylisted internet resources.

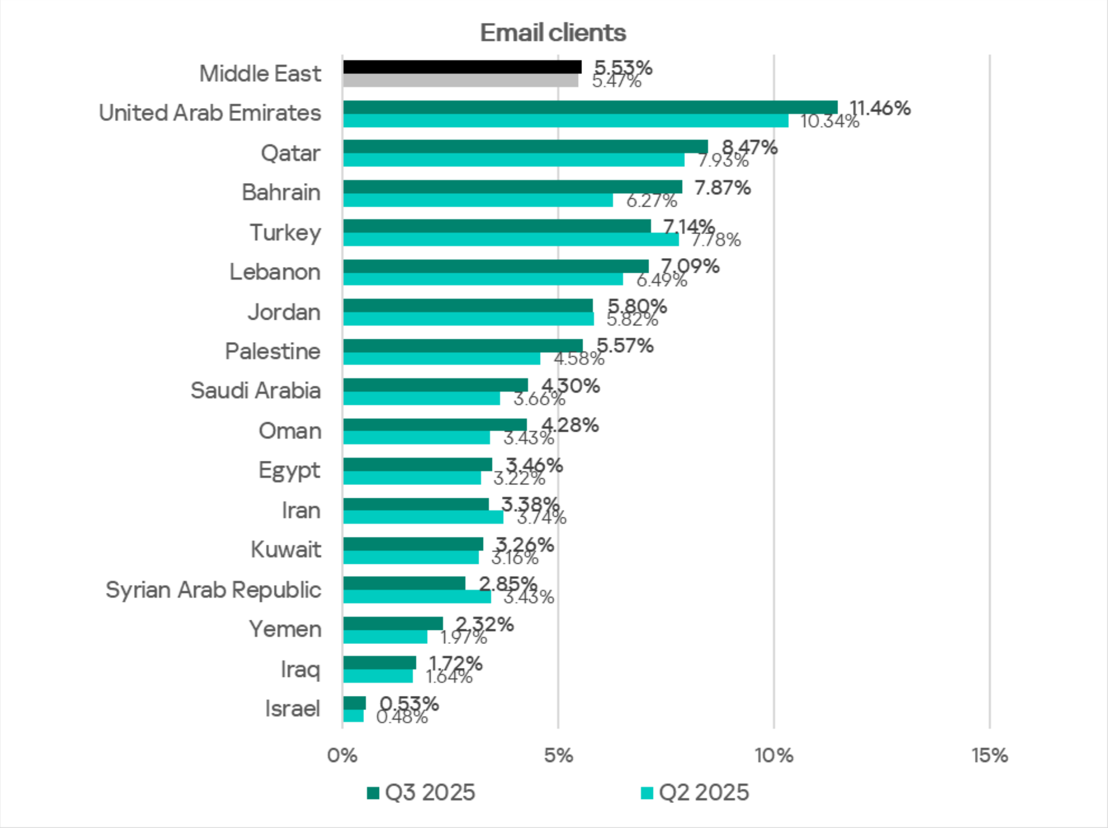


Email clients

Email clients have shown a rising trend as a threat source in the region since Q3 2024. In Q3 2025, the Middle East ranked second globally by percentage of ICS computers on which threats from email clients were blocked. This is 7.1 times higher than in Russia, which ranks last.

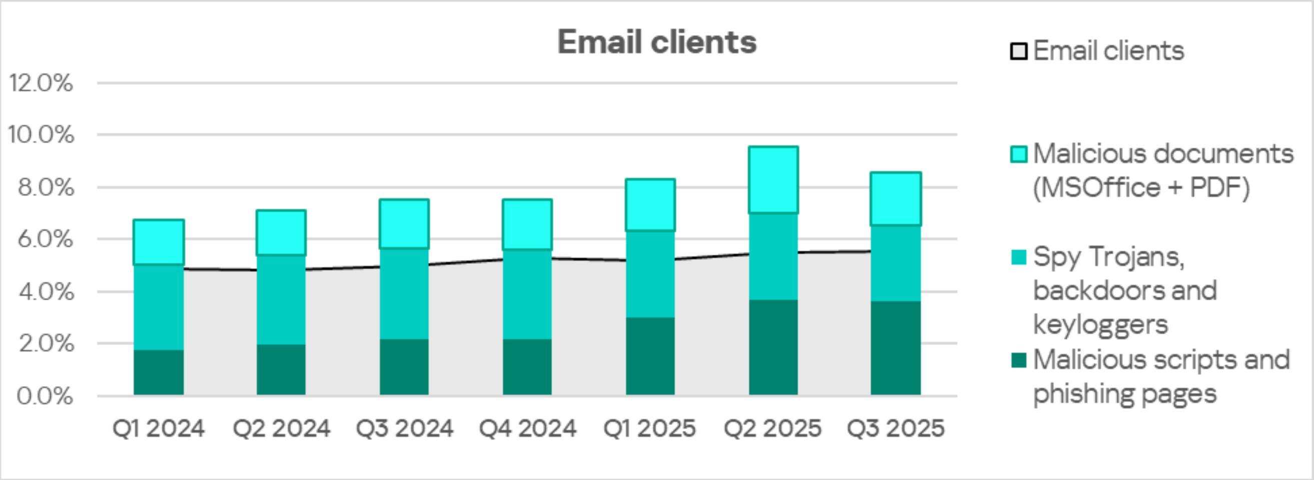


Within the region, the UAE leads with 11.46%. The lowest figure is in Israel (0.53%). Yemen, which leads in most other sources, ranks near the bottom here.



The top three countries in this ranking (the UAE, Qatar, Bahrain) also place highly in terms of malicious scripts and phishing pages.

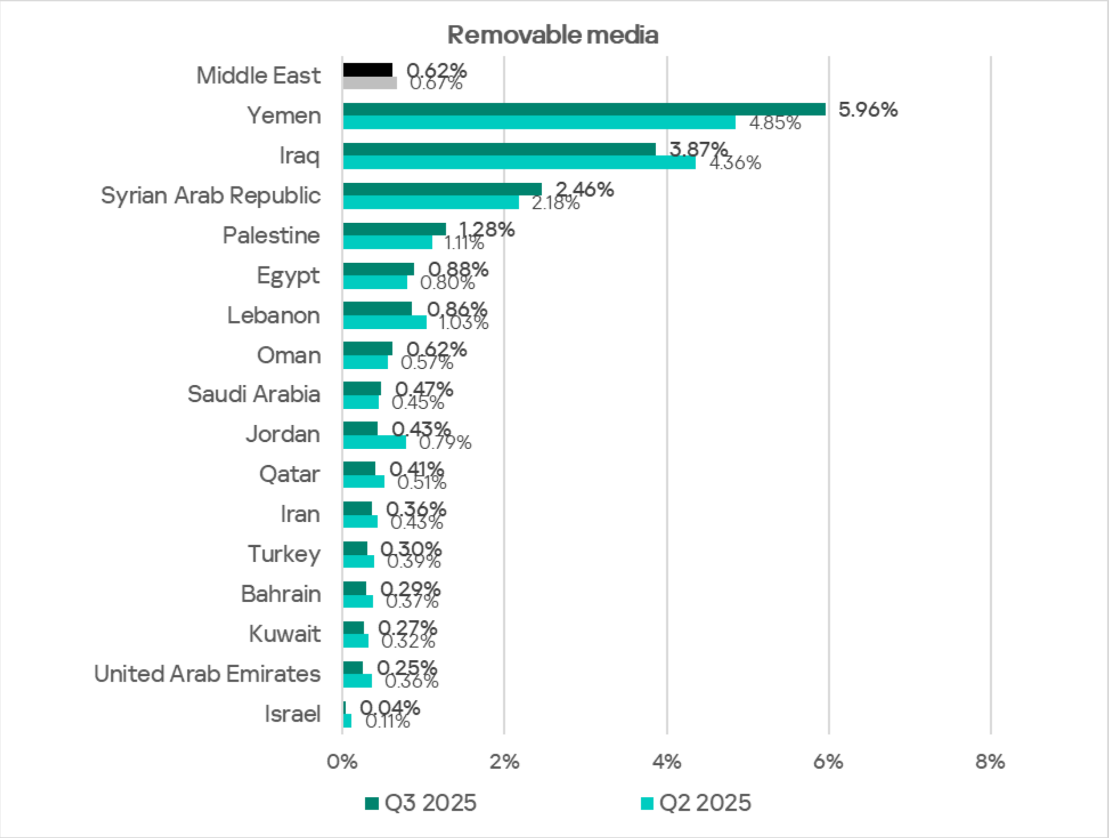
The main categories of email-borne threats blocked on ICS computers are malicious documents, spyware, malicious scripts, and phishing pages.



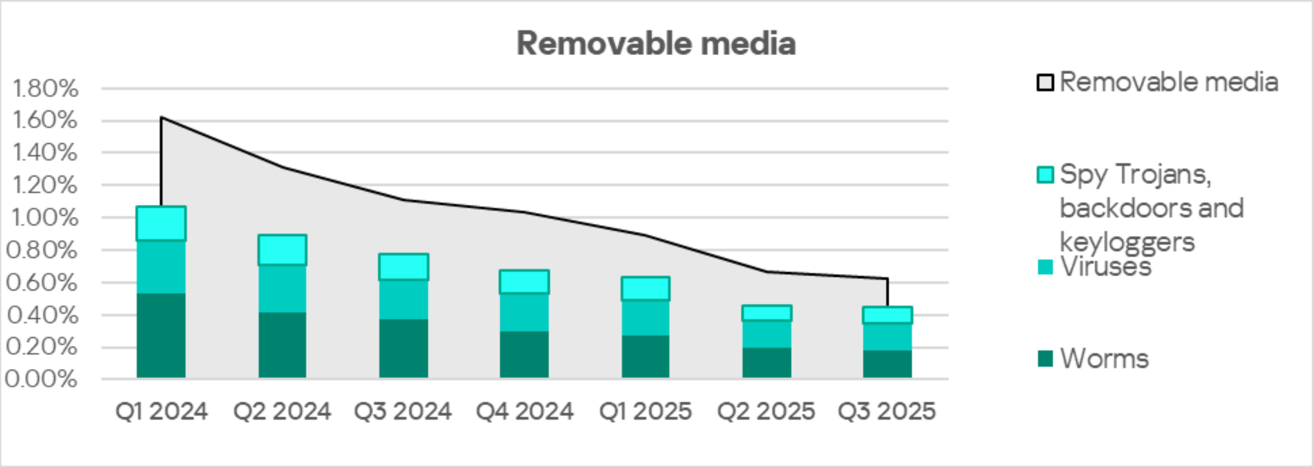
Removable media

By percentage of ICS computers on which threats were blocked when connecting to removable media, the Middle East ranked fourth among regions in Q3 2025, with 0.62%. This is 12.4 times higher than the Australia and New Zealand region, which ranks last in the corresponding ranking.

Among the countries and territories in the region, Yemen leads with 5.96% and Iraq with 3.87% by percentage of ICS computers on which threats were blocked when connecting to removable media. Other countries ranged from 0.04% in Israel to 2.46% in Syria.



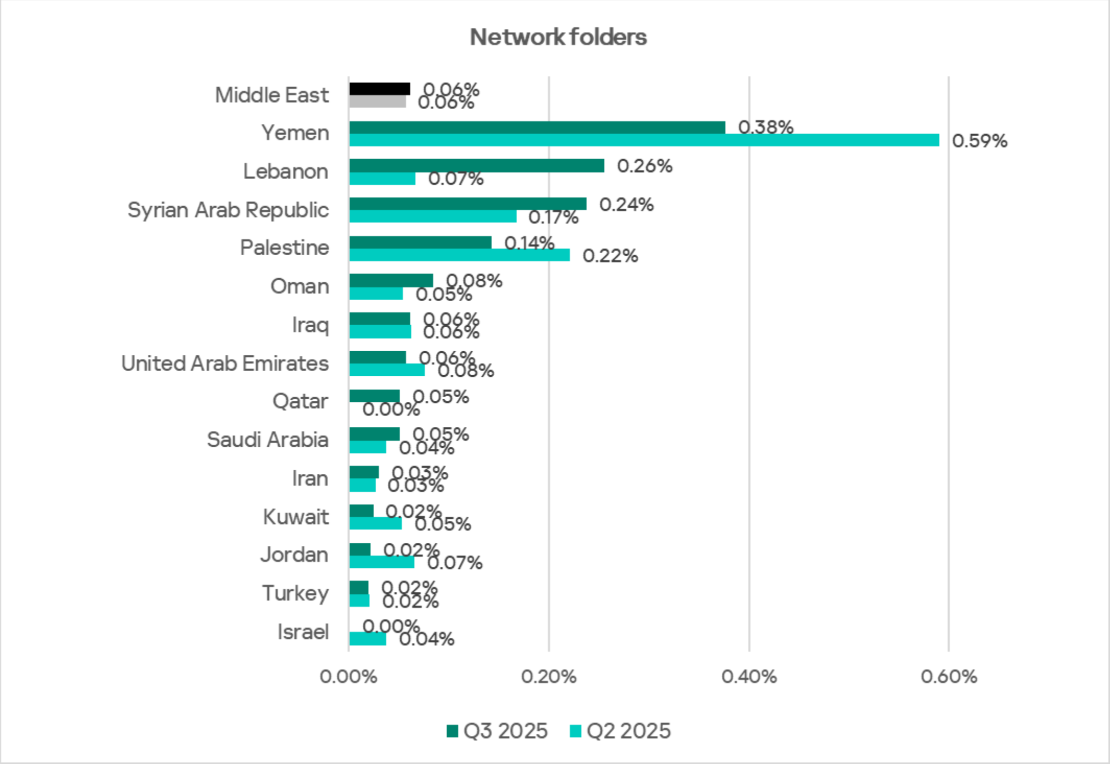
The main categories of removable media threats blocked on ICS computers in the region are worms, spyware, and viruses. By the percentage of ICS computers on which worms were blocked, the Middle East ranked third globally.



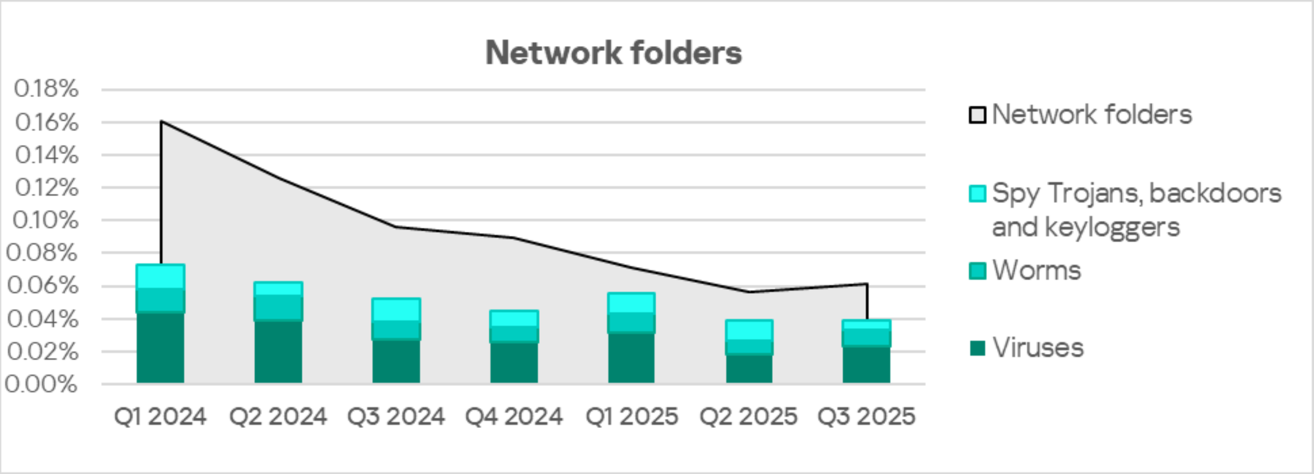
Network folders

By percentage of ICS computers on which threats were blocked in network folders, the Middle East ranked third among regions in Q3 2025, with 0.06%. This is 10.2 times higher than Northern Europe, which posted the lowest score.

Within the region, Yemen leads by a wide margin with 0.38%.

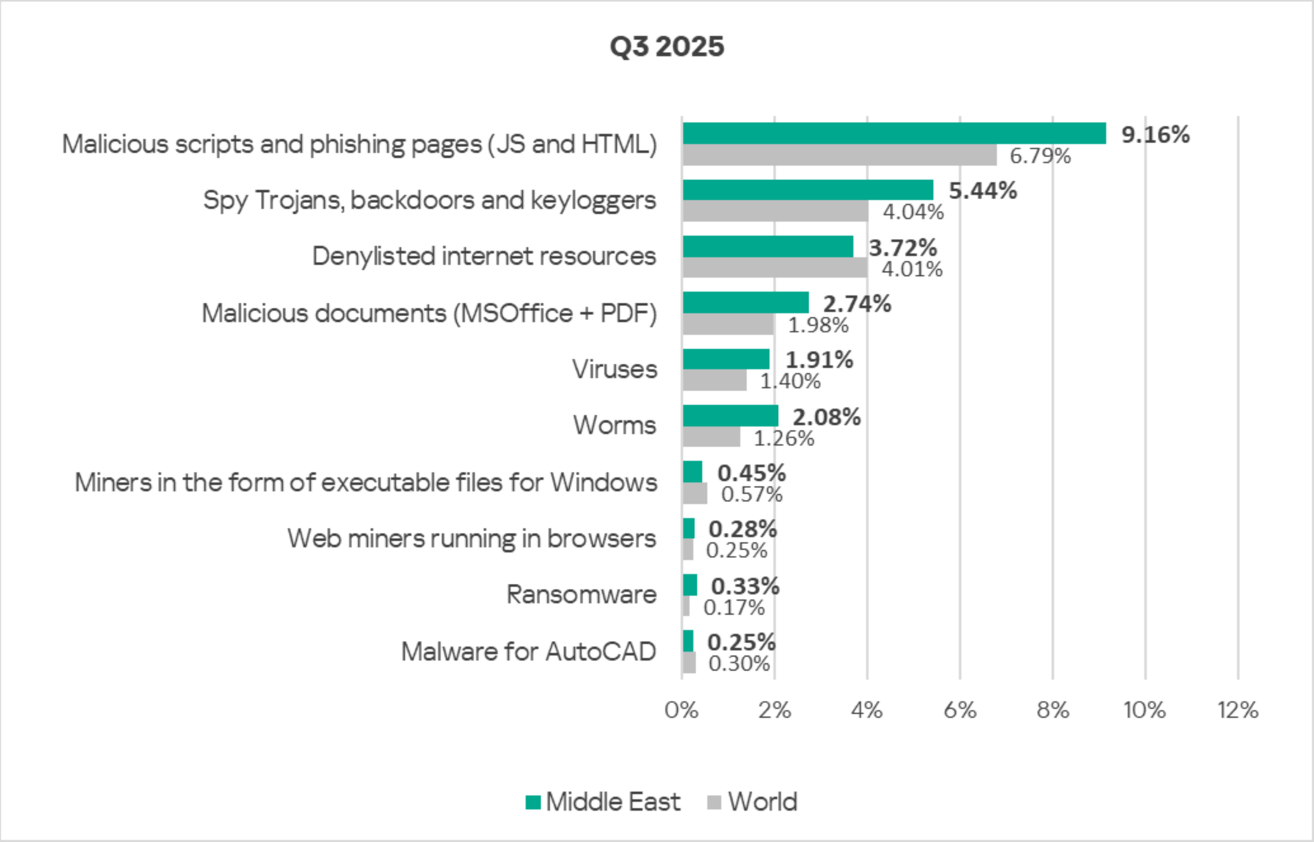


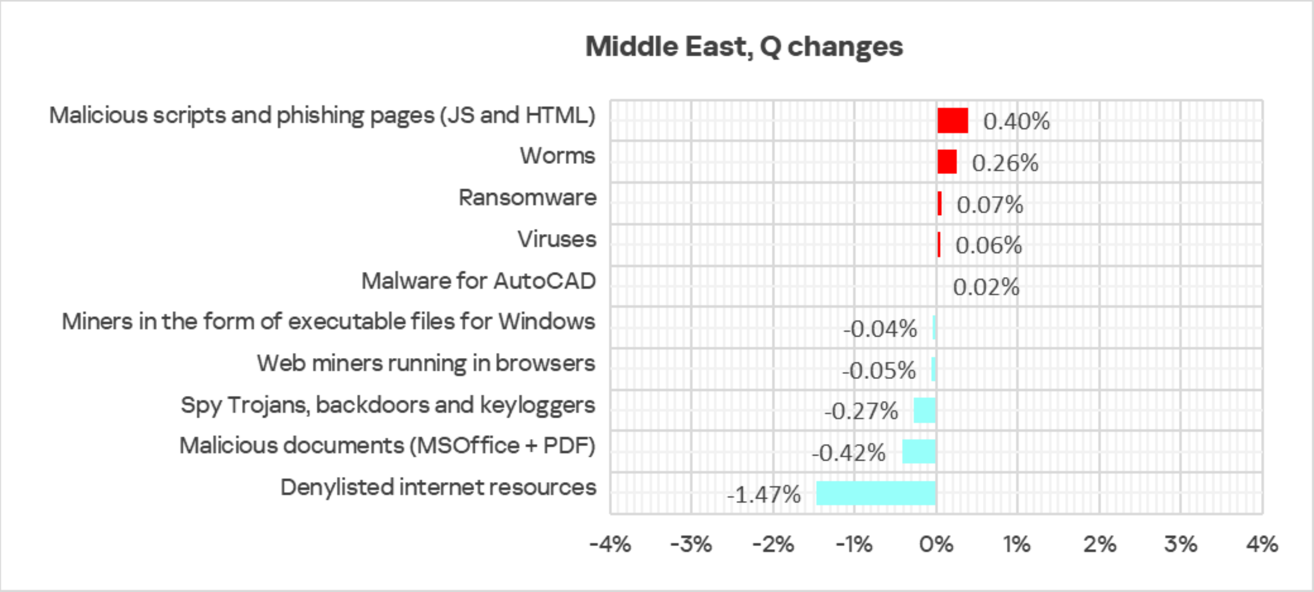
The main categories of threats that spread through network folders are viruses, worms, and spyware.



Threat categories

In the region, 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 are in the following threat categories:

- Malicious documents: 1.4 times higher (third globally).
- Malicious scripts and phishing pages: 1.3 times higher (fourth globally).
- Spyware: 1.3 times higher (fourth globally).

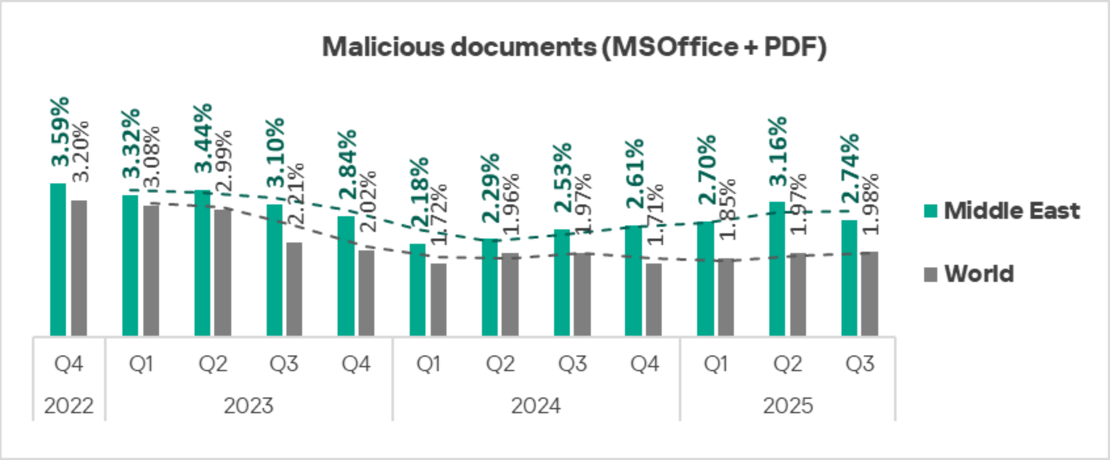
- Viruses: 1.4 times higher (fourth globally).
- Worms: 1.7 times higher (third globally).
- Ransomware: 1.9 times higher (first globally).

The Middle East ranks third among regions for web miners.

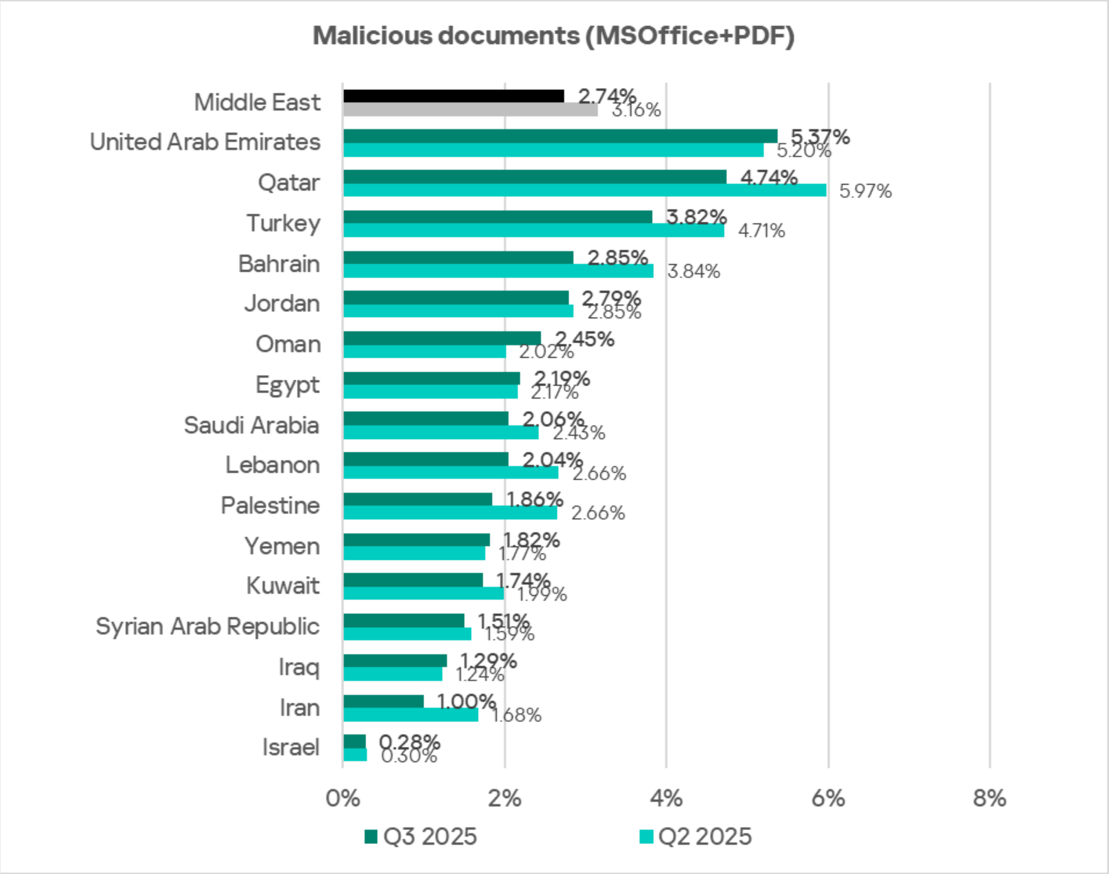
Malicious documents

In Q3 2025, the Middle East ranked third in terms of malicious documents, with 2.74%. This is 5.2 times higher than in Northern Europe, which ranks last in this category.

The percentage of ICS computers on which malicious documents were blocked was on the rise since Q2 2024, but decreased quarter-on-quarter in Q3 2025.



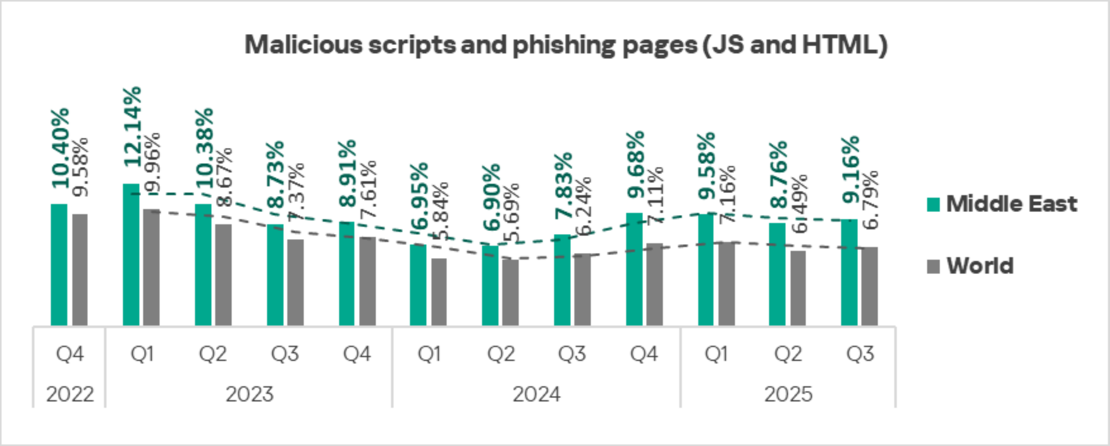
Among the region's countries and territories, the UAE leads in this metric with 5.37%. Israel ranks last with 0.28%, 3.6 times less than Iran, one place above.



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

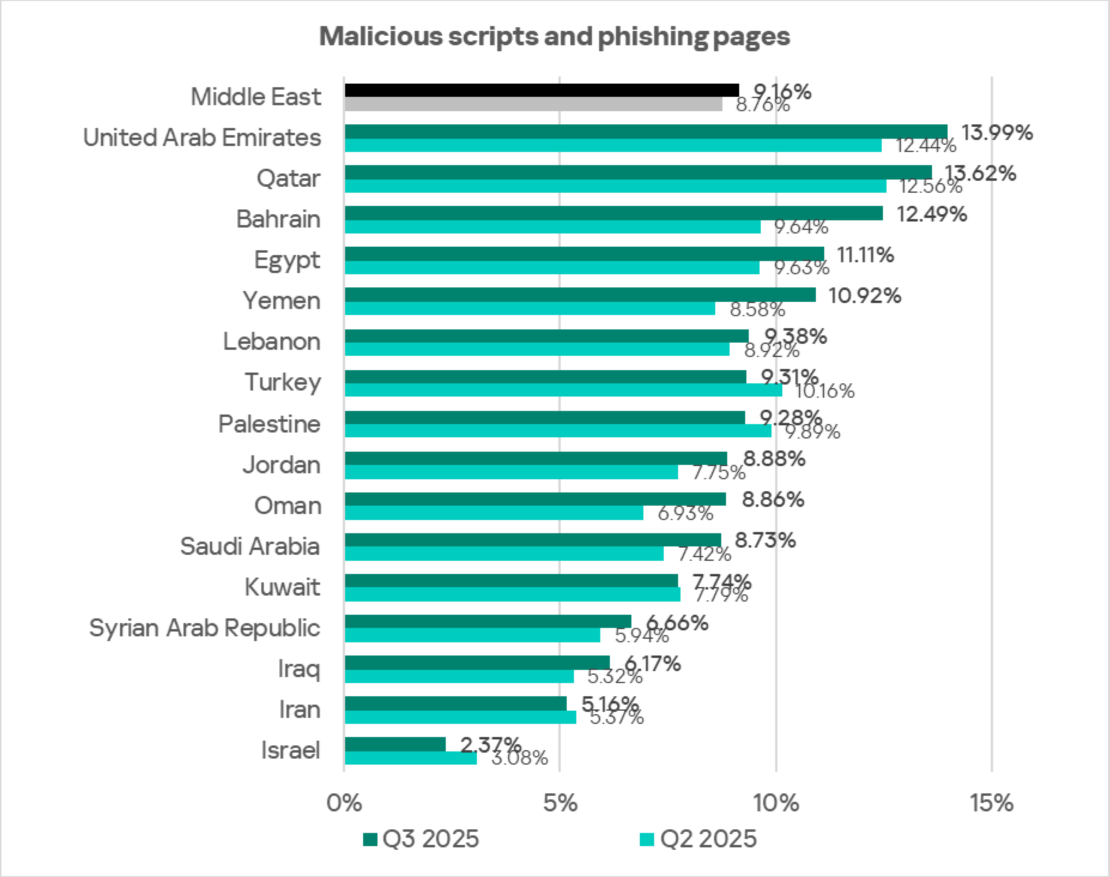
Malicious scripts and phishing pages

In terms of ICS computers where malicious scripts and phishing pages were blocked, the Middle East ranked fourth globally with 9.16%. This is 3.6 times higher than in Northern Europe, which had the lowest figure.



These threats spread both online and via email.

Among the region's countries and territories, the UAE leads in this metric with 13.99%. Israel scores the lowest (2.37%), 2.1 times less than Iran, one place above.

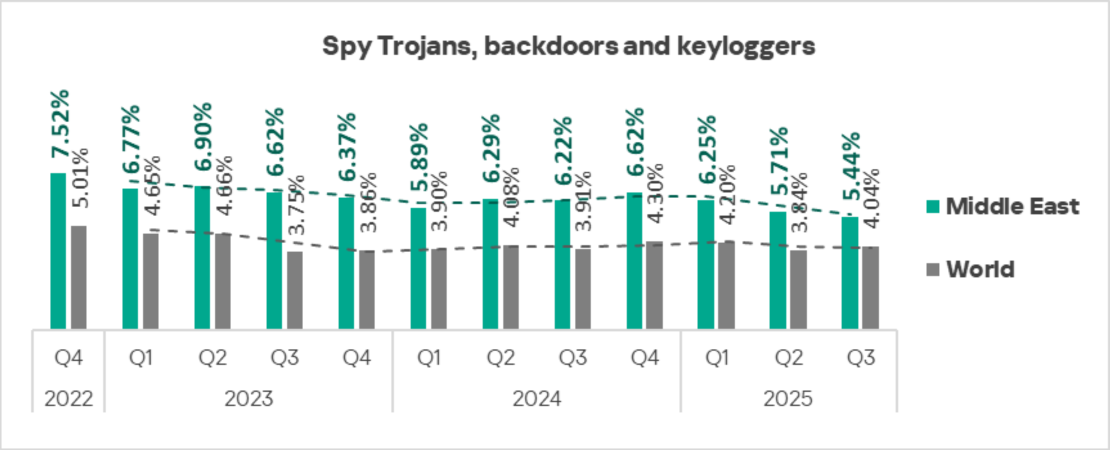


The two leading countries in this ranking (the UAE and Qatar) also top the ranking for malicious documents and the regional ranking by percentage of ICS computers on which threats were blocked in email clients. They are also among the top three countries in the spyware ranking (topped by Yemen).

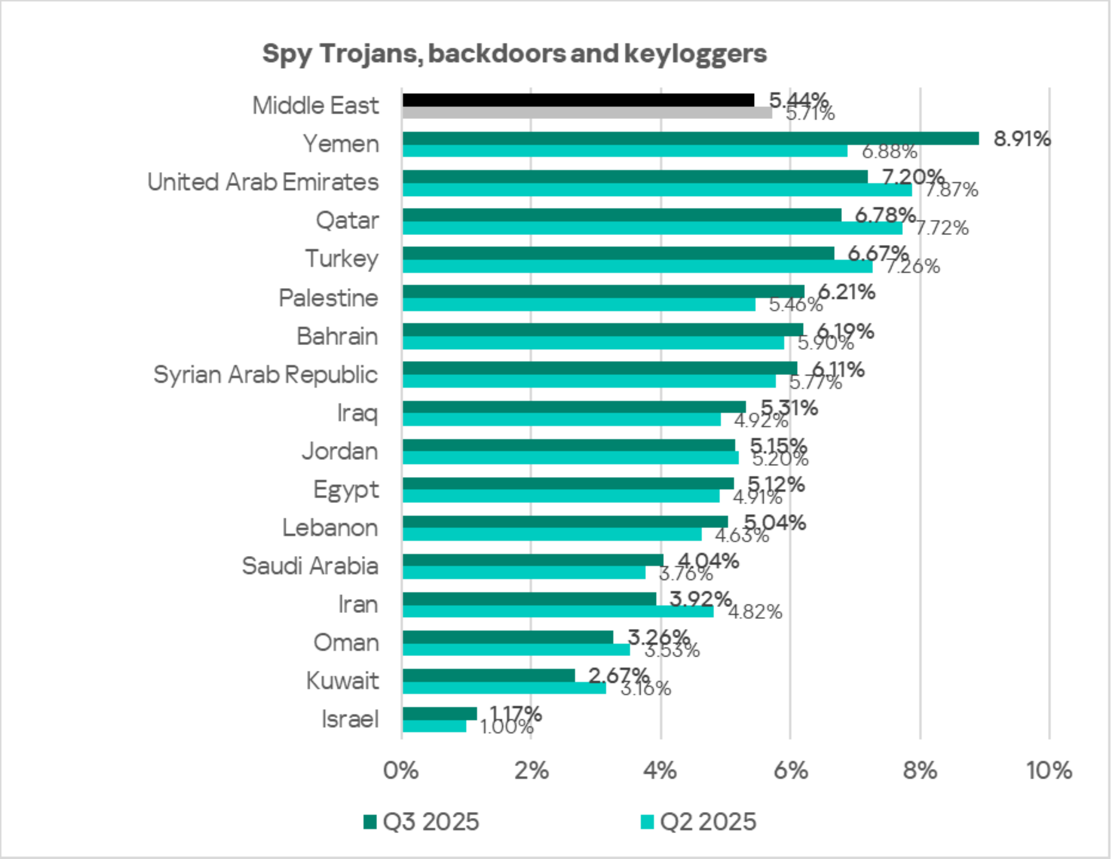
Spyware

By percentage of ICS computers on which spyware was blocked, the Middle East ranks fourth with 5.44%. This figure is 3.9 times higher than in Northern Europe, which has the lowest rate.

In the Middle East, the percentage of ICS computers on which spyware was blocked fell for the third consecutive quarter, hitting a three-year low in Q3 2025.



Among the countries and territories in the region, Yemen leads by percentage of ICS computers on which spyware was blocked in Q3 2025, with 8.91%. This country's score increased by 1.3 times over the quarter. Israel scored the lowest, 2.3 times less than Kuwait, which ranked one place higher.



Spyware in the region was blocked across all threat sources, but most often this threat spreads through email clients.

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

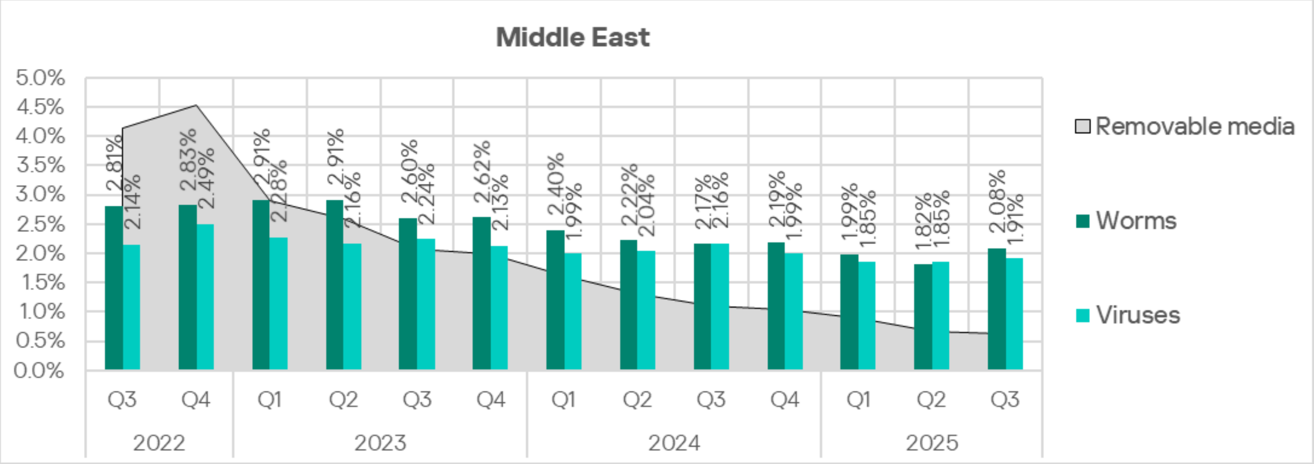
Self-propagating malware: worms and viruses

Worms and viruses are the main threat categories blocked when connecting removable media to ICS computers. The Middle East ranks fourth among regions by the percentage of ICS computers on which threats are blocked from removable media. The region also ranks third in worms and fourth in terms of viruses.

The percentage of ICS computers on which worms were blocked is 2.08%. This is 9.5 times higher than in Northern Europe, which scored the lowest.

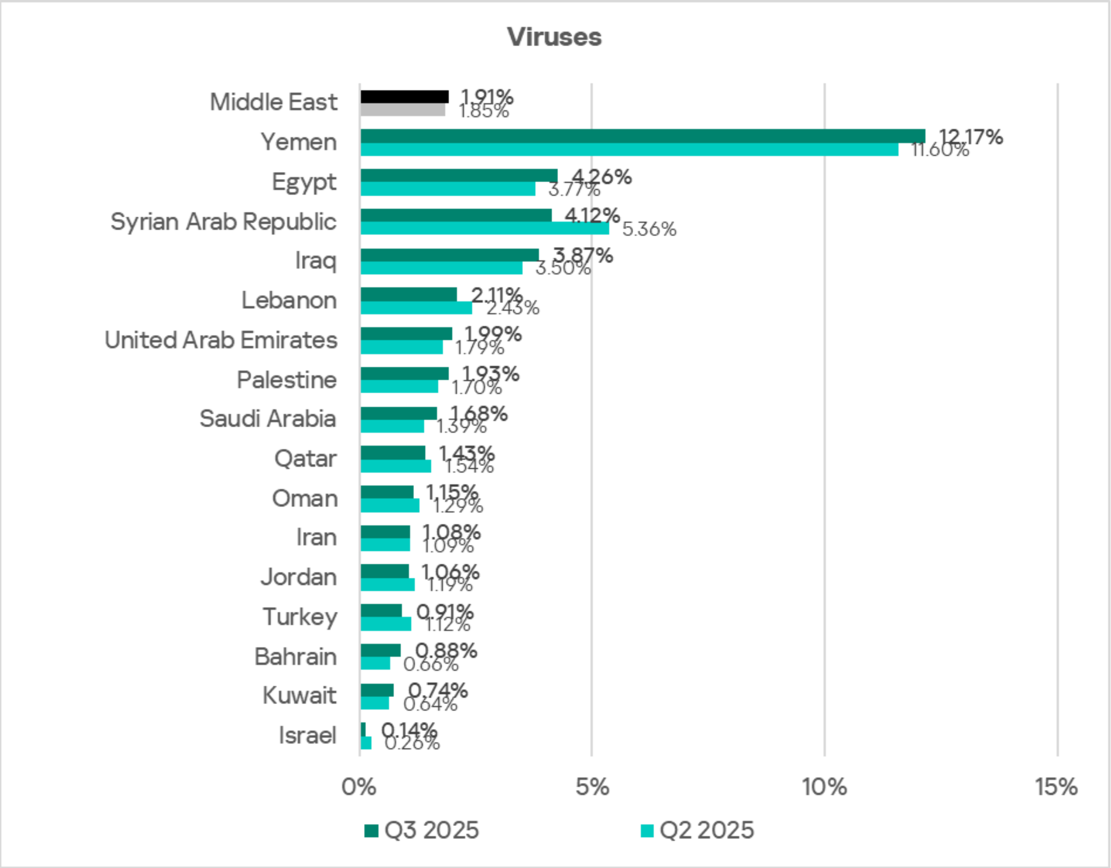
The percentage of ICS computers on which viruses were blocked is 1.91%. This is 11.9 times higher than Australia and New Zealand in last place.

The worm and virus rate, like the overall percentage of removable media threats, is gradually declining, with some fluctuations, although it lags behind the figures for removable media. In Q3 2025, both threat categories saw an increase.

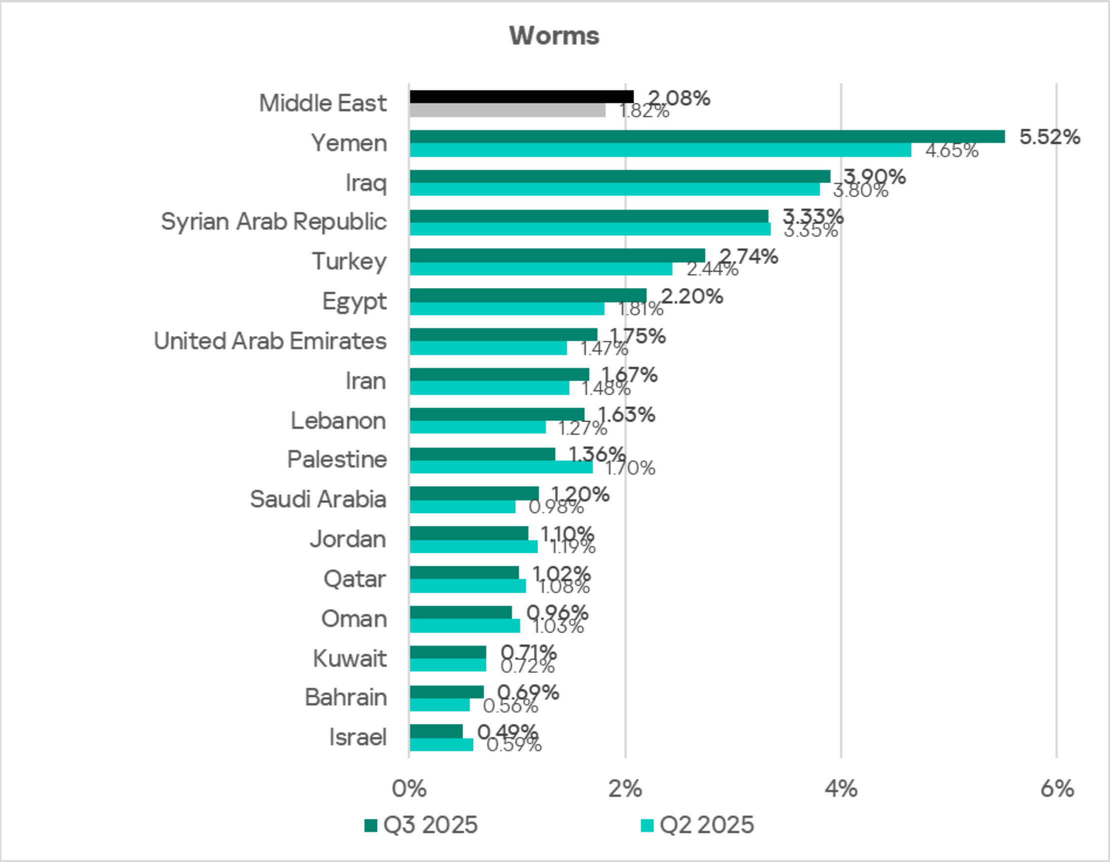


Among the countries and territories in the region, Yemen leads by a wide margin by percentage of ICS computers on which both worms and viruses were blocked.

In terms of viruses, Yemen's score (12.17%) is 2.9 times higher than that of Egypt, which ranks second in this ranking. Compared to Israel, which ranks last, Yemen's score is 86.9 times higher.



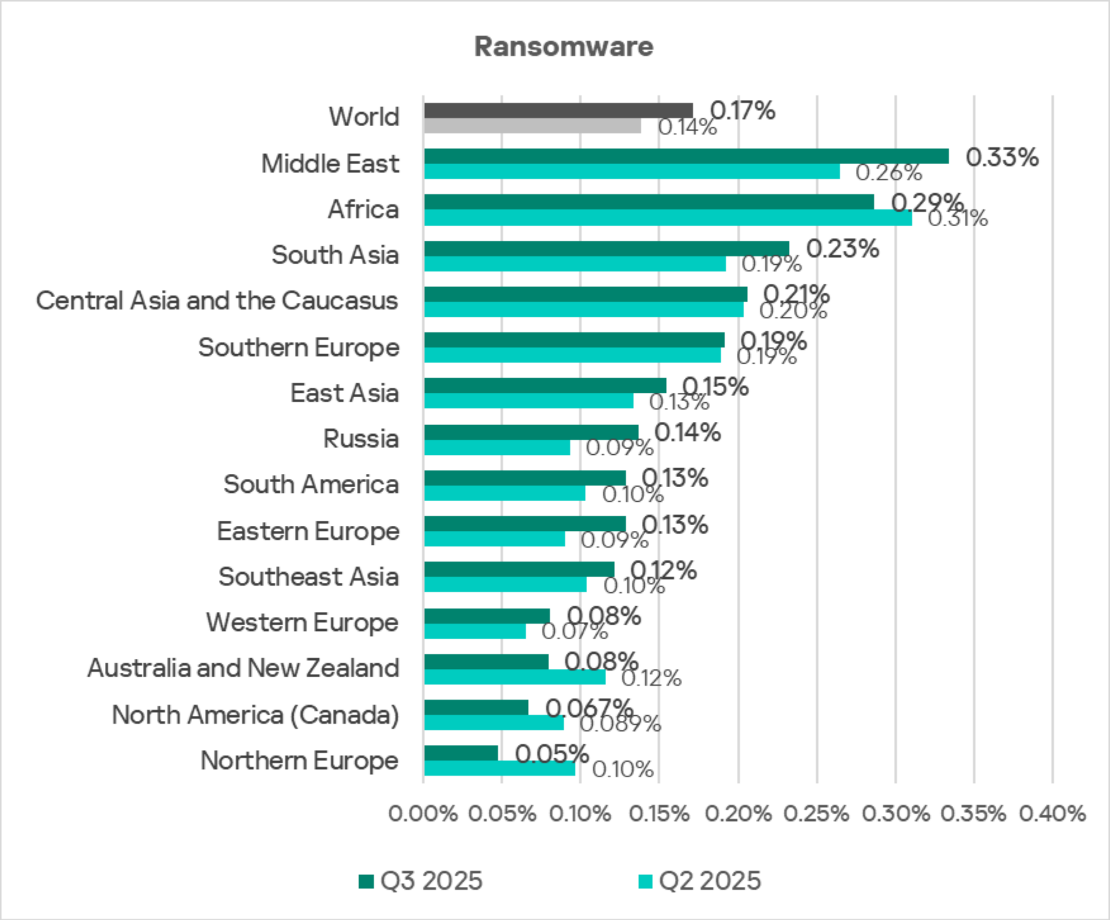
The difference between the worm rate in Yemen (5.52%) and in other countries is noticeable, but less significant.



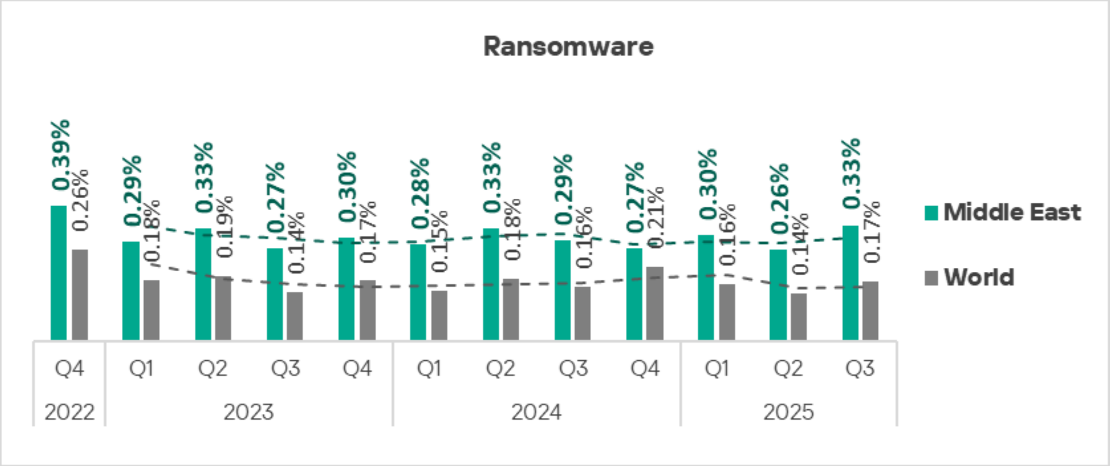
Ransomware

In the Middle East, the percentage of ICS computers on which ransomware was blocked is consistently high — almost double the global average. The region led this indicator in 2024, but was second in the first two quarters of 2025.

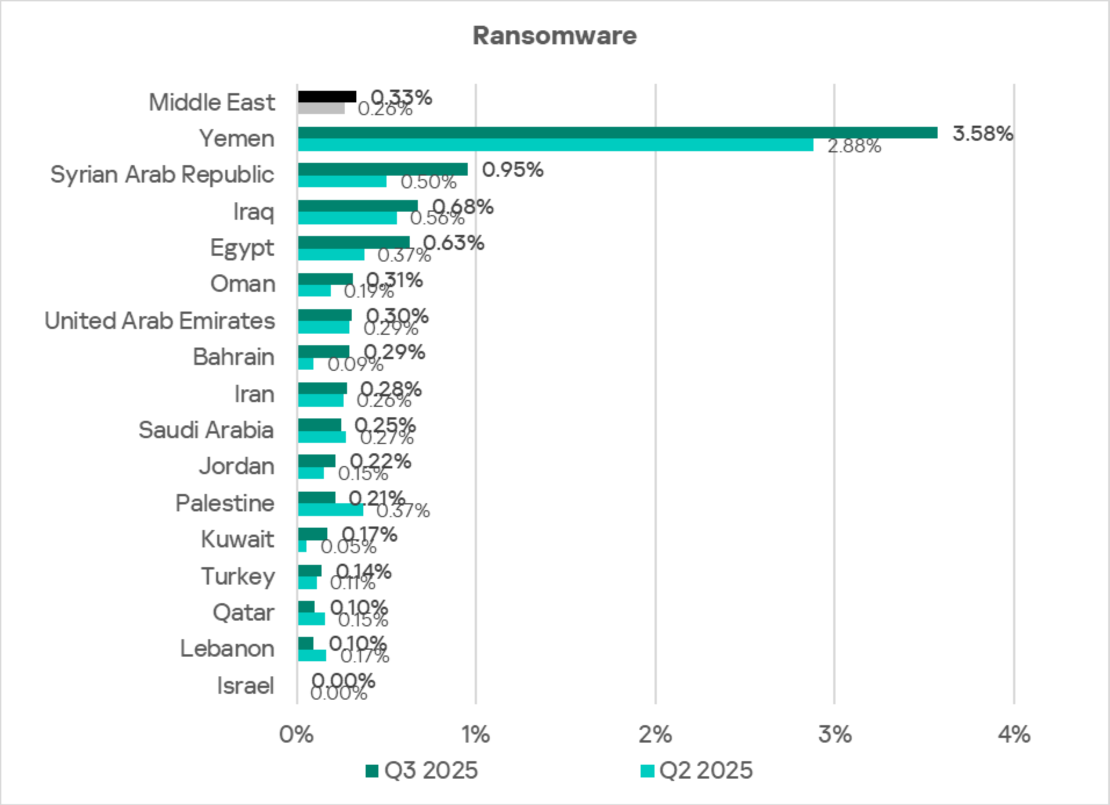
In Q3 2025, the Middle East regained its lead among regions by percentage of ICS computers on which ransomware was blocked.



Since 2023, the regional indicator has fluctuated between 0.26% and 0.33%. In Q3 2025, it rose to 0.33%. This figure is 6.6 times higher than in Northern Europe, which has the lowest rate.



Among the countries and territories in the region, Yemen leads comfortably by percentage of ICS computers on which ransomware was blocked, with what for this threat category is a gigantic 3.58%. Yemen's score is 3.8 times higher than second-place Syria.



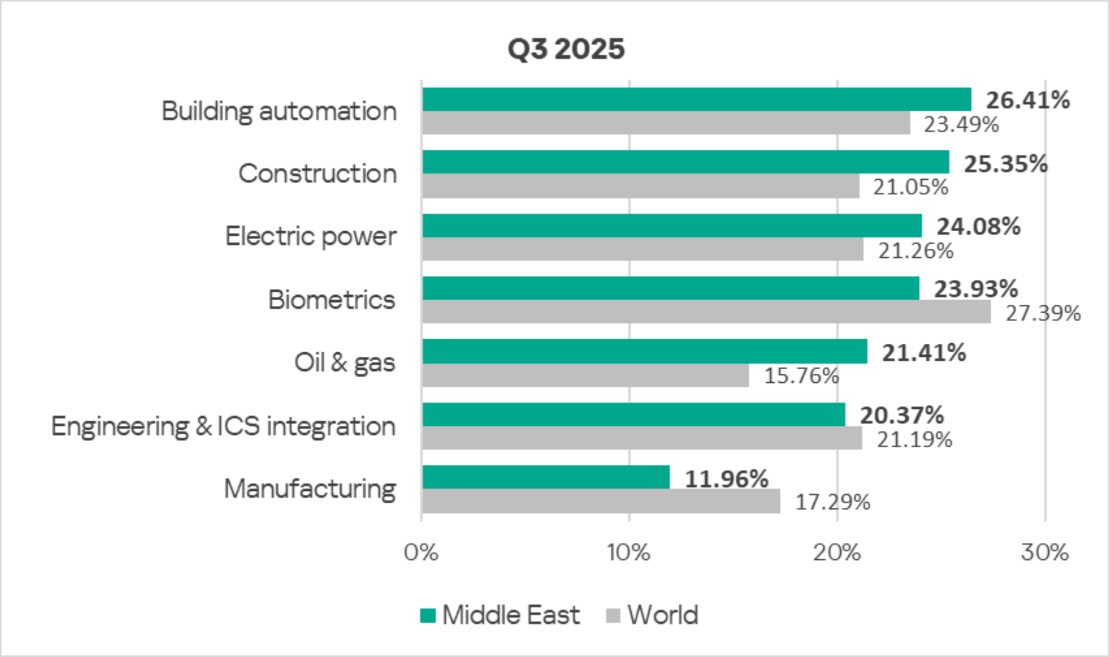
In the region, this threat most often spreads through email clients and removable media.

Industries

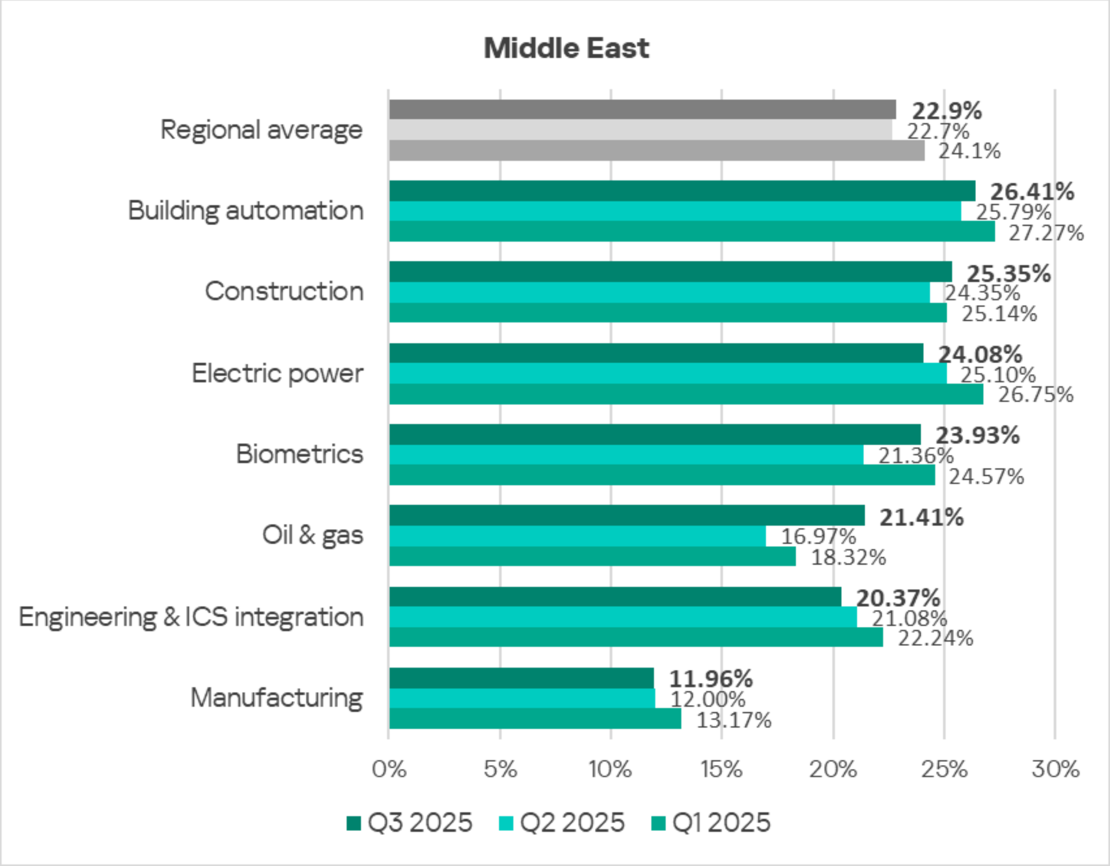
Among industries covered in the report, the most frequently targeted in the Middle East is building automation.

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

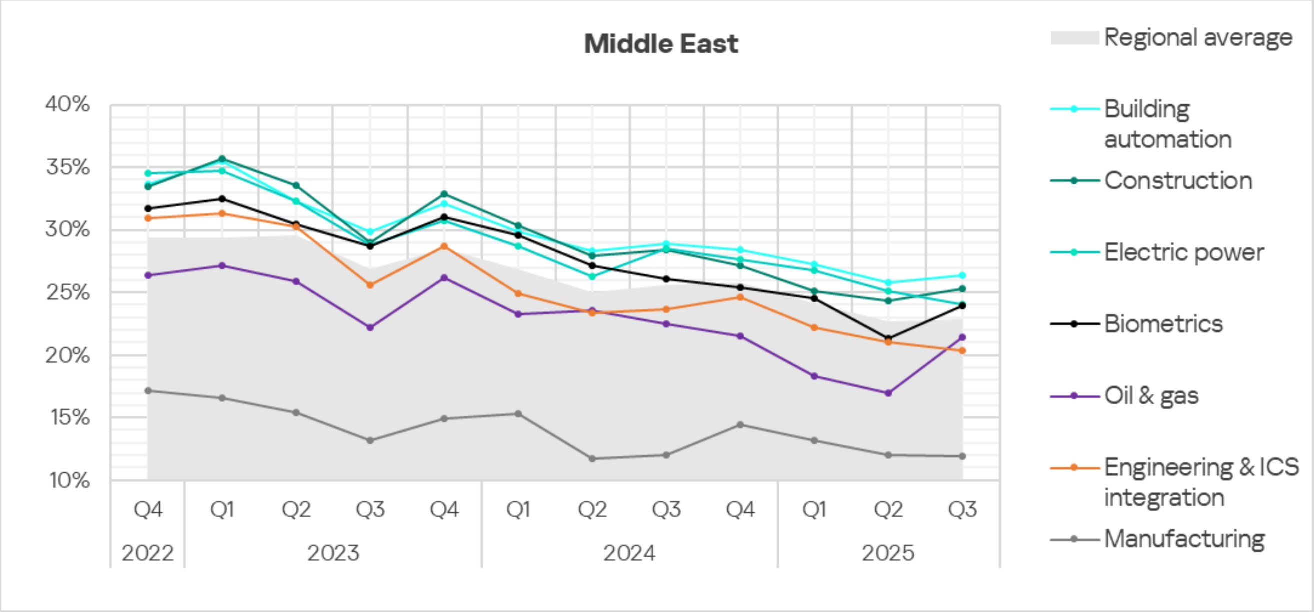
- Building automation: 1.1 times higher.
- Electrical energy: 1.1 times higher.
- Construction: 1.2 times higher.
- Oil and gas: 1.4 times higher.



In Q1 2025, the percentage of ICS computers on which malicious objects were blocked increased in all industries which had indicators above the global average.



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. The color red signifies that the figure approaches the maximum.

Threat source indicators for industries in the Middle East, Q3 2025

Industry / Threat source	Biometrics	Building automation	Electric power	Engineering & ICS integration	Oil & gas	Construction	Manufacturing	Threat category total in the region
Internet	8.48%	9.25%	10.30%	8.31%	7.57%	10.07%	4.86%	8.63%
Email clients	5.23%	8.28%	4.36%	3.65%	1.86%	5.49%	1.80%	5.53%
Removable media	1.16%	0.68%	0.66%	0.46%	0.79%	0.55%	0.38%	0.62%
Network folders	0.05%	0.10%	0.06%	0.03%	0.11%	0.12%	0.06%	0.06%
Industry total in the region	23.93%	26.41%	24.08%	20.37%	21.41%	25.35%	11.96%	

Threat category indicators for industries in the Middle East, Q3 2025

Industry / Threat category	Biometrics	Building automation	Electric power	Engineering & ICS integration	Oil & gas	Construction	Manufacturing	Threat category total in the region
Denylisted internet resources	3.62%	3.93%	4.50%	3.67%	3.79%	4.02%	2.29%	3.72%
Malicious scripts and phishing pages (JS and HTML)	9.75%	11.96%	9.07%	7.15%	6.44%	9.44%	4.20%	9.16%
Spy Trojans, backdoors and keyloggers	5.52%	7.87%	4.90%	3.89%	3.50%	4.07%	2.23%	5.44%
Worms	2.43%	2.68%	2.28%	1.69%	1.69%	1.44%	1.24%	2.08%
Miners in the form of executable files for Windows	0.48%	0.46%	0.50%	0.51%	0.73%	0.97%	0.26%	0.45%
Malicious documents (MSOffice + PDF)	2.72%	4.23%	2.14%	1.73%	1.07%	2.07%	0.90%	2.74%
Viruses	3.25%	2.62%	2.10%	1.12%	1.53%	2.36%	1.19%	1.91%
Ransomware	0.48%	0.48%	0.33%	0.21%	0.28%	0.23%	0.09%	0.33%
Web miners running in browsers	0.26%	0.27%	0.29%	0.32%	0.40%	0.68%	0.17%	0.28%
Malware for AutoCAD	0.26%	0.19%	0.15%	0.19%	0.28%	1.24%	0.29%	0.25%
Industry total in the region	23.93%	26.41%	24.08%	20.37%	21.41%	25.35%	11.96%	

In all industries, the main source of threats is the internet. Therefore, the most relevant threat categories include denylisted links, malicious scripts, and phishing pages (spread both online and via email).

Most industries across the region have a high percentage of ICS computers on which malicious scripts and phishing pages were blocked. The Middle East ranks second in the regional rankings for this indicator in the following industries:

- Building automation.
- Construction.
- Electrical energy.
- Oil and gas.

The Middle East ranks no lower than fourth in the regional ransomware rankings across all industries except manufacturing:

- Oil and gas: first.
- Building automation: second.
- Construction: third.
- Engineering and ICS integrators: third.
- Electrical energy: fourth.
- Biometric systems: fourth.

The Middle East ranks fourth or higher in the regional ransomware rankings for self-propagating malware (worms and viruses) and malware for AutoCAD. These categories of malicious objects ranked in the top four individually or collectively across all industries except electrical energy.

The Middle East leads all the regions in terms of malware for AutoCAD in OT infrastructure for biometric systems.

Building automation

The Middle East ranks third among regions by percentage of ICS computers on which malicious objects were blocked in the building automation industry.

In the global industry ranking across all regions, building automation in the Middle East ranks:

- Fifth in terms of threats delivered through email clients.
- Fifth by percentage of ICS computers on which malicious scripts and phishing pages were blocked.

Among regions by industry indicators, the Middle East ranks:

- Second by percentage of ICS computers on which threats from email clients and network folders were blocked.
- Fourth in terms of threats from the internet and removable media.
- Second by percentage of ICS computers on which malicious scripts, phishing pages, and ransomware were blocked.
- Third in terms of worms, viruses, and malware for AutoCAD.
- Fourth in terms of spyware.

Among industries in the region, building automation is:

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

Construction

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

In the global ranking by industry across all regions, the Middle East industry ranks:

- Fifth by percentage of ICS computers on which web miners were blocked.

Among regions by industry indicators, the Middle East ranks:

- First by percentage of ICS computers on which threats from email clients were blocked.
- Third for threats in network folders.
- Fourth for removable media.
- Second by percentage of ICS computers on which malicious scripts and phishing pages were blocked.
- Third for miners from both categories, worms and ransomware.
- Fourth for viruses and malware for AutoCAD.

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

- First for threats in network folders.
- Second for threats from the internet and email clients.
- First for miners from both categories and malware for AutoCAD.
- Second among industries in the region for denylisted internet resources.
- Third in the region for the following categories: malicious scripts, phishing pages, and viruses.

Electrical energy industry

The Middle East ranks fourth among regions by percentage of ICS computers on which malicious objects were blocked in the electrical energy industry.

Among regions by industry indicators, the Middle East ranks:

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

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

- First for internet threats.
- First for denylisted internet resources.
- Third for the following threat categories: malicious documents, spyware, worms, and ransomware.

Biometric systems

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

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

- Third by percentage of ICS computers on which threats were blocked on removable media and in network folders.
- Fourth for internet threats.
- First place in the percentage of ICS computers on which malware for AutoCAD is blocked.
- Third for viruses.
- Fourth for worms and ransomware.

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

- First for threats on removable media.
- Third for threats from email clients.
- First for viruses.
- Second for the following threat categories: malicious scripts and phishing pages, spyware, malicious documents, worms, and ransomware.

Oil and gas

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

Among regions by industry indicators, the Middle East ranks:

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

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

- Second for threats on removable media and in network folders.

- Second place in both types of miners.
- /Third for malware for AutoCAD.

Engineering and ICS integrators

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

Among regions by industry indicators, the Middle East ranks:

- Third by percentage of ICS computers on which threats from email clients, removable media, and network folders were blocked.
- Second by percentage of ICS computers on which worms were blocked.
- Third for ransomware, fourth for spyware.

Among industries in the region, engineering and ICS integrators ranks third for miners from both categories.

Manufacturing

The Middle East ranks 12th by percentage of ICS computers on which malicious objects were blocked.

Among regions by industry indicators, the Middle East ranks:

- Second place in the percentage of ICS computers on which threats in network folders are blocked.
- Fourth by percentage of ICS computers on which malware for AutoCAD was blocked.
- Among industries in the region, manufacturing ranks second in terms of malware for AutoCAD.

Methodology used to prepare statistics

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

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

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

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

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

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

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

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

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

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

Kaspersky ICS CERT ics-cert@kaspersky.com