Kaspersky ICS CERT

Threat landscape for industrial automation systems

Middle East. Q2 2025

22.09.2025

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 directly at stealing authentication data.

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.

High rate of spyware

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

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 Q1 and Q2 2025, the Middle East ranked second globally by the percentage of ICS computers on which ransomware was blocked (in 2024, the region topped this ranking).

Striking country-level differences

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

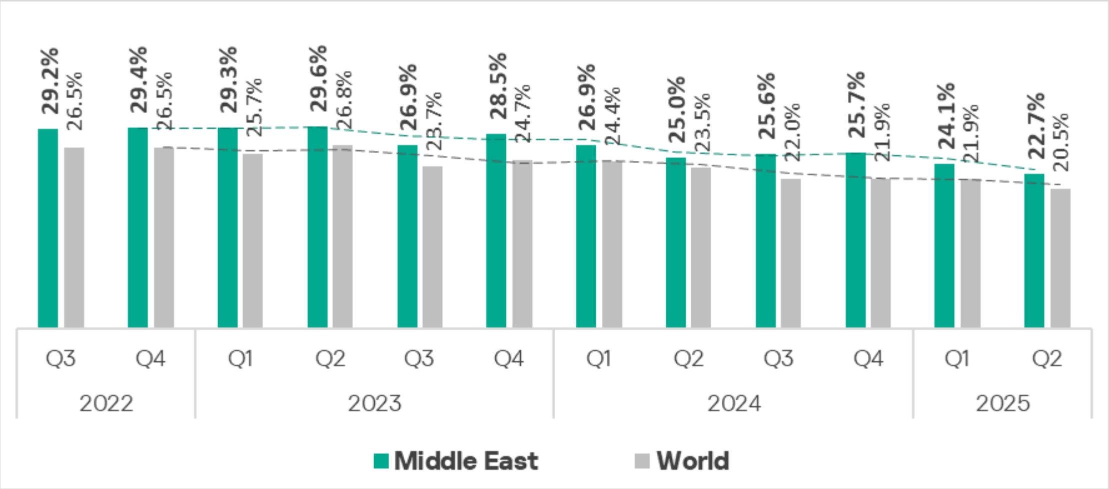
For threats from email clients, the UAE, Qatar, and Turkey hold the top positions. These same countries also rank among the leaders in malicious scripts and phishing pages, malicious documents, and spyware.

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

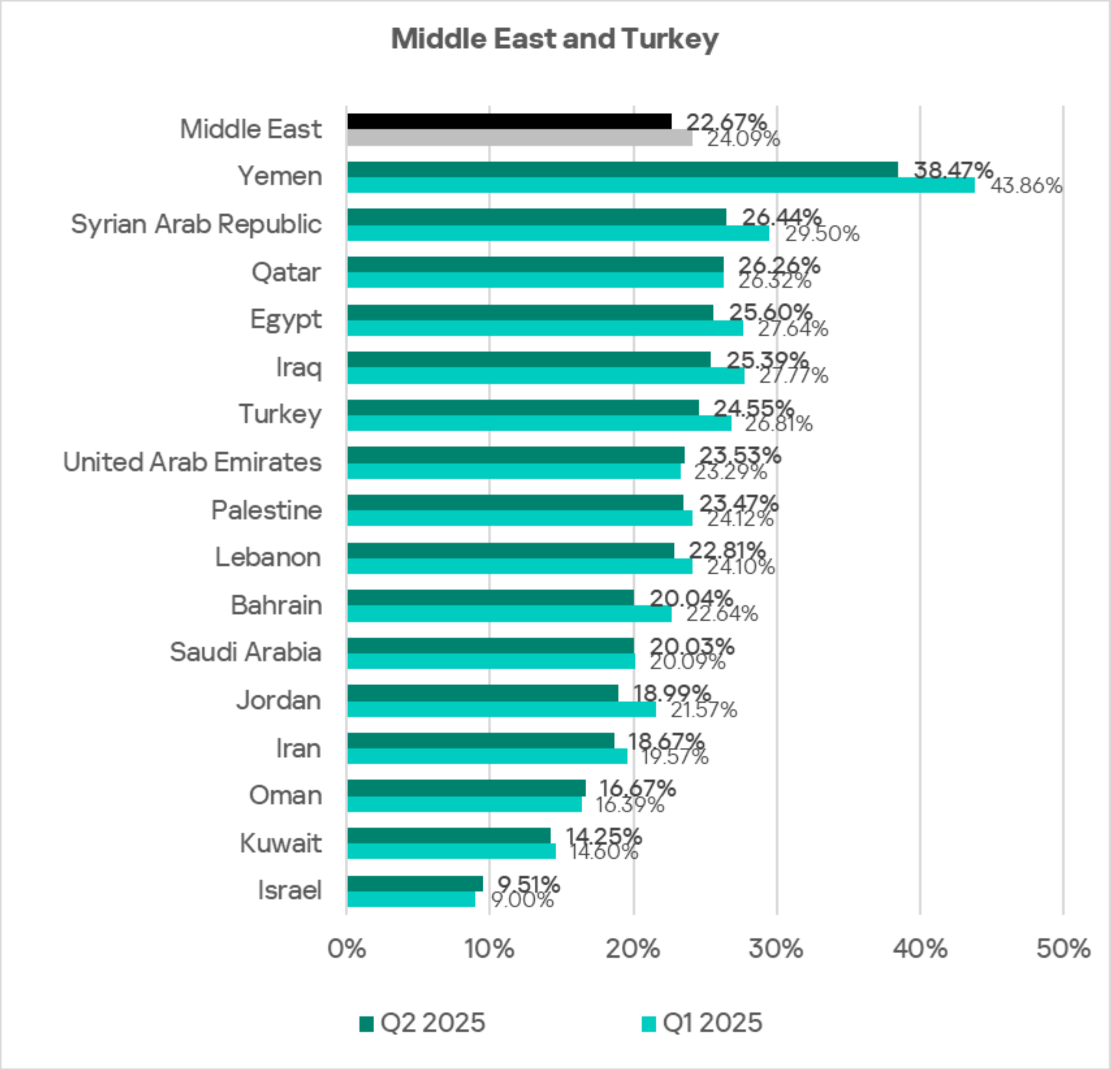
Statistics across all threats

In Q2 2025, the Middle East ranked third globally by the percentage of ICS computers on which malicious objects were blocked, with 22.7%. The region consistently exceeds the global average in this metric — in Q2 2025, by 1.1 times. This is twice as high as the lowest-ranking region, Northern Europe.

This figure has been declining for two consecutive quarters, falling by 1.4% over the reporting period.



Within the region, rates vary from 9.51% in Israel to 38.47% in Yemen. These two countries are relative outliers, with the region's other countries ranging between 14% and 27%.



Yemen dominates most of the region's rankings, with the exception of email threats. For threats from email clients, the UAE, Qatar, and Turkey hold the top positions. These countries also rank highly in malicious scripts and phishing pages, malicious documents, and spyware.

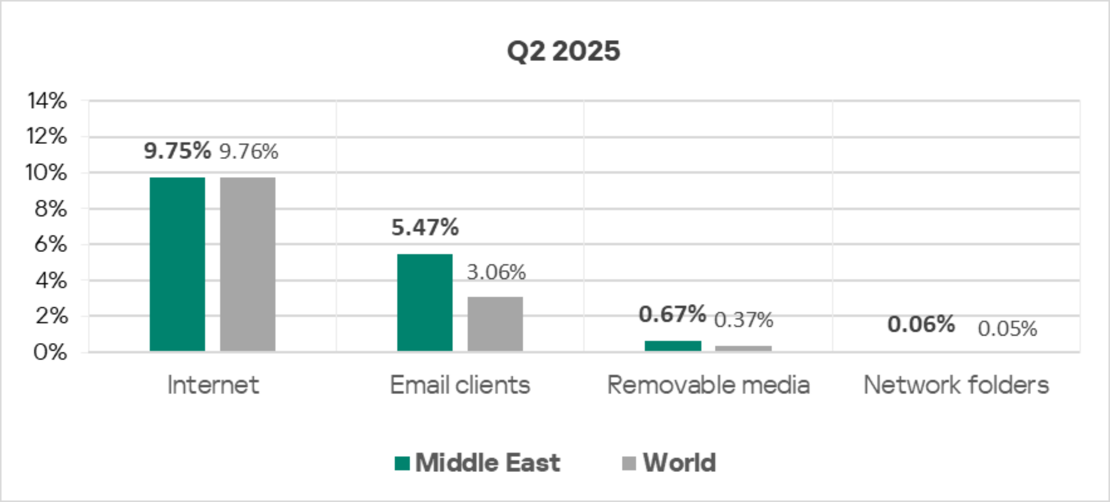
Israel consistently places at the bottom of most regional rankings.

Threat sources

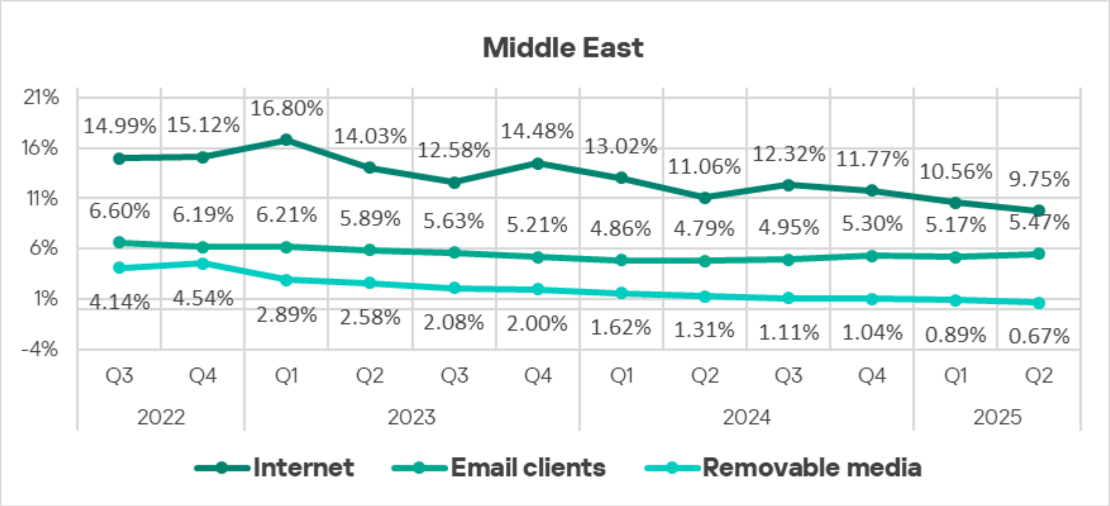
The percentage of ICS computers on which threats were blocked in the Middle East is higher than the global average across almost all sources. The exception is the internet, where it is roughly equal.

For two sources, the percentage is significantly higher than the global average:

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



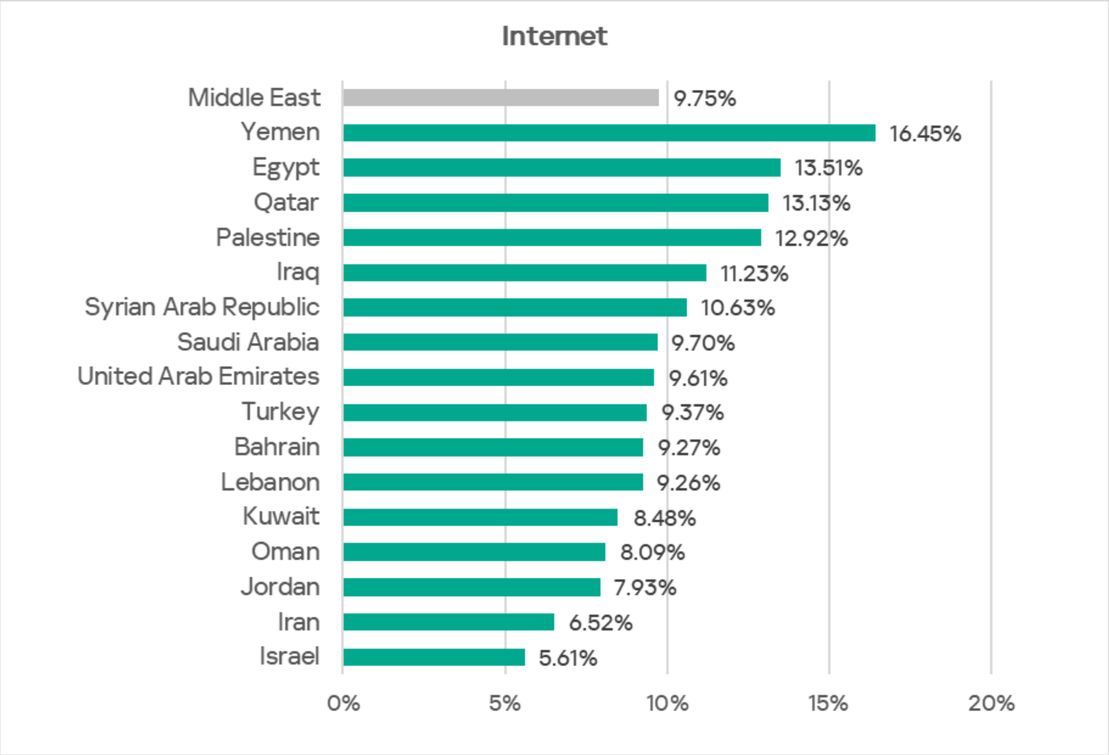
The percentage of attacked ICS computers is increasing only for email clients. All the other threat sources are trending downward.



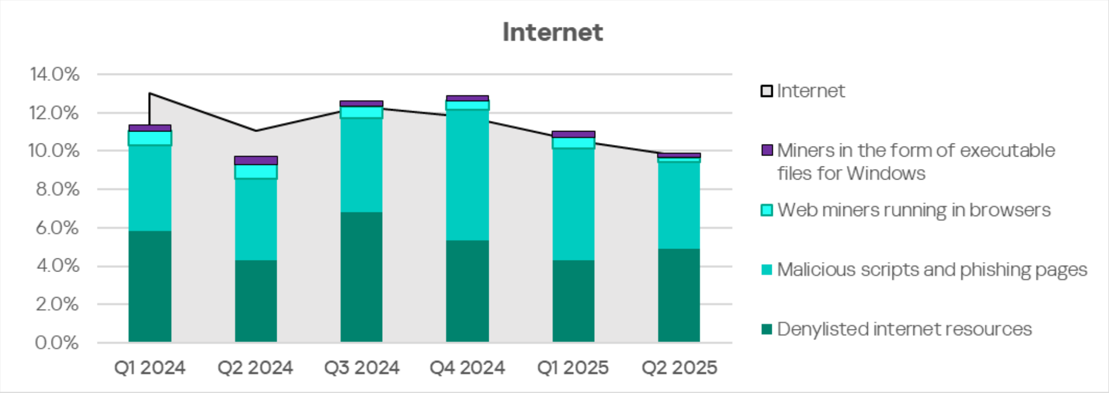
Internet

For ICS computers on which threats from the internet were blocked, the Middle East ranked fourth globally, with a rate 1.5 times higher than the lowest (East Asia).

Country-level rates range from 5.61% in Israel to 16.45% in Yemen.

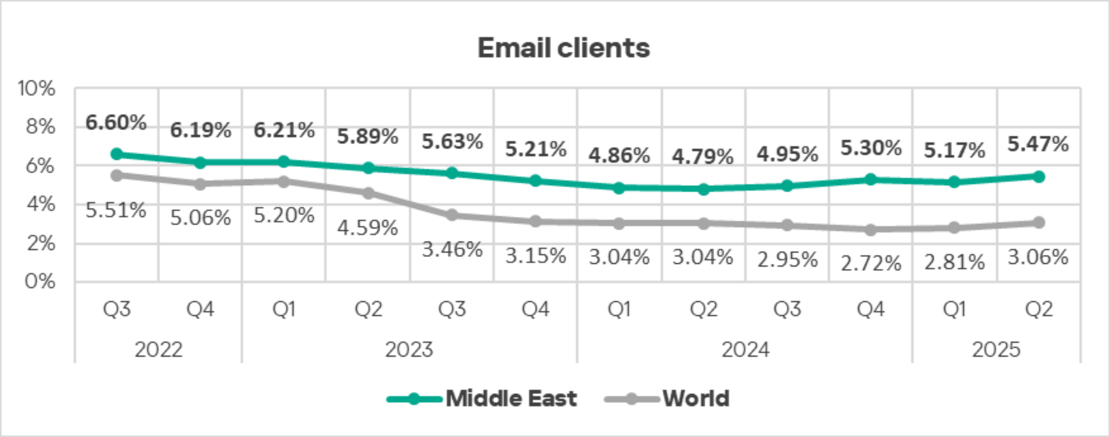


The main categories of internet threats blocked on ICS computers in the region are denylisted internet resources, malicious scripts and phishing pages, and miners.

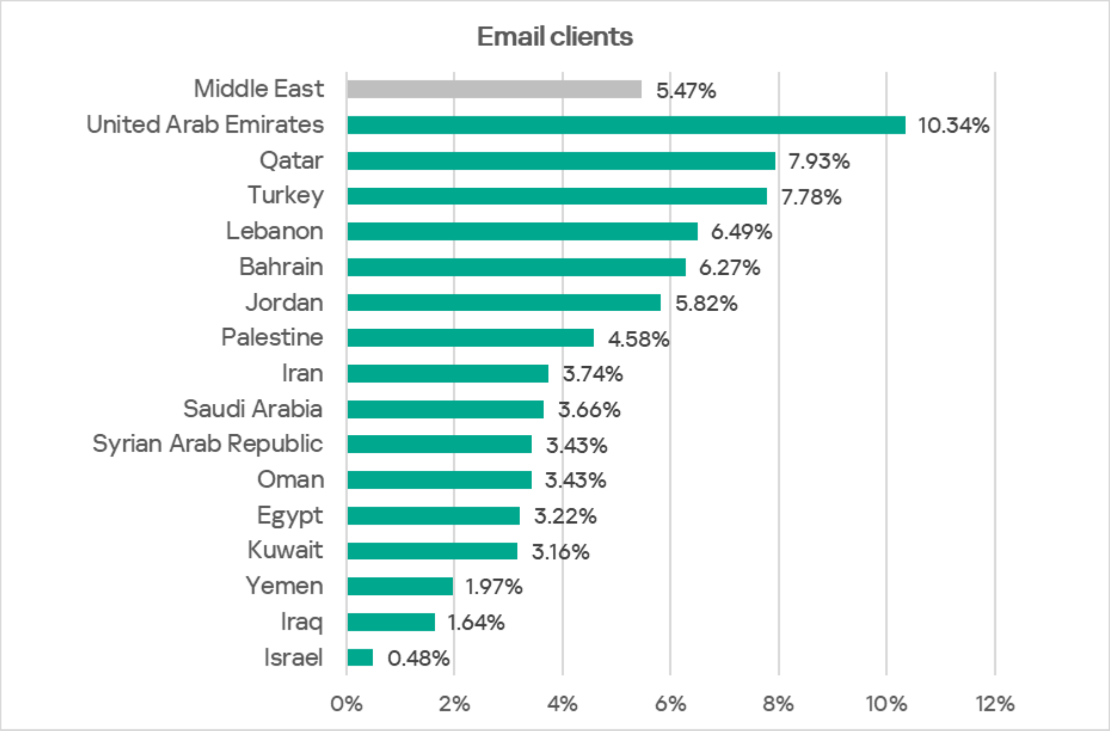


Email clients

Email clients have shown a rising trend as a threat source in the region since Q3 2024. In Q2 2025, the Middle East ranked third globally by the percentage of ICS computers on which threats from email clients were blocked. The region's figure is 6.8 times higher than Russia's, which ranks last.

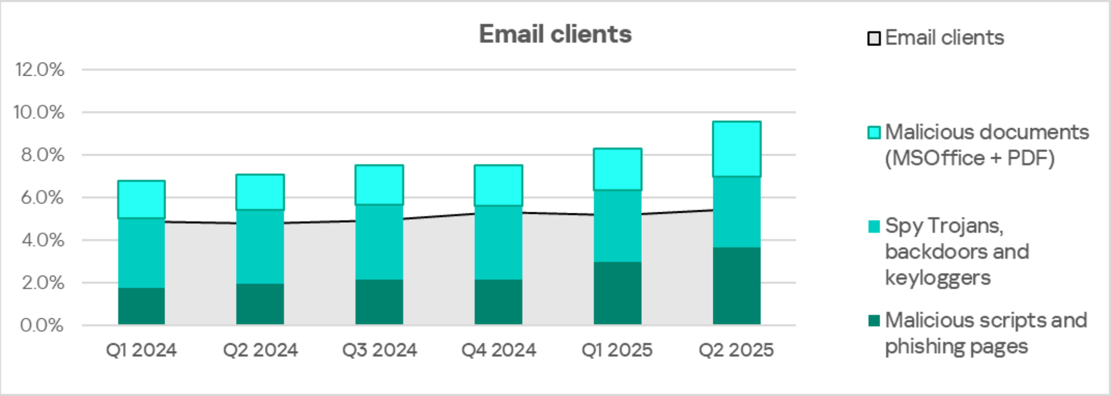


Within the region, the UAE leads with 10.34%. The lowest figure is in Israel (0.48%). Yemen, which leads in most other sources, ranks near the bottom here.



The top three countries in this ranking — the UAE, Qatar, and Turkey—are also among the leaders in malicious scripts and phishing pages, malicious documents, and spyware.

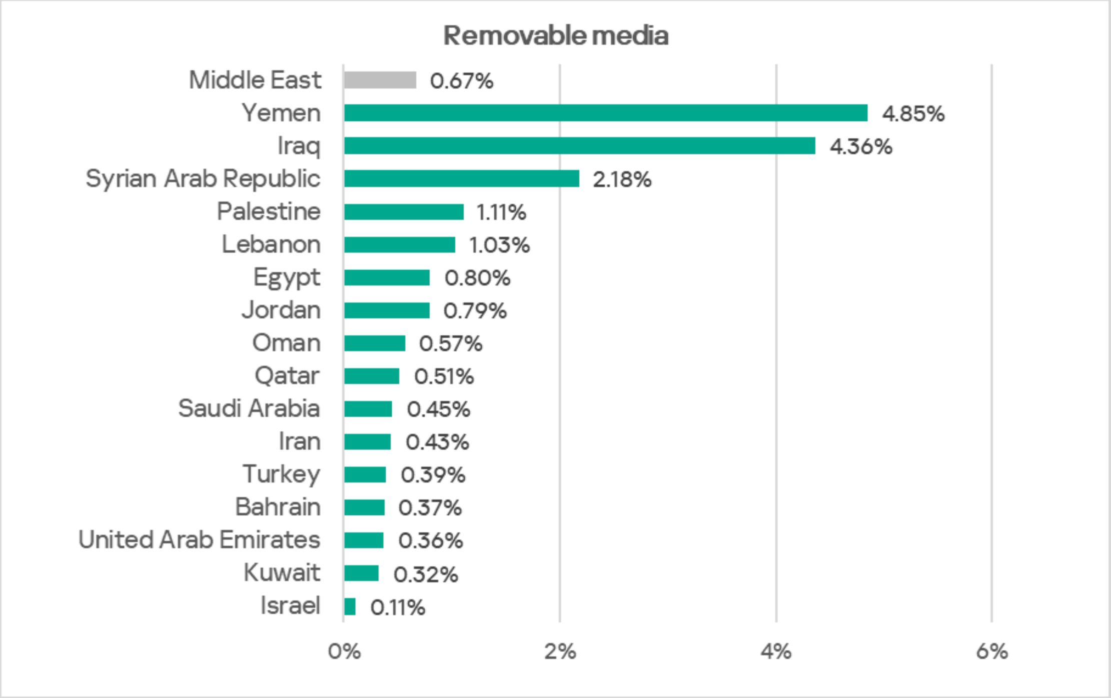
The main categories of email-borne threats blocked on ICS computers are malicious documents, malicious scripts and phishing pages, and spyware.



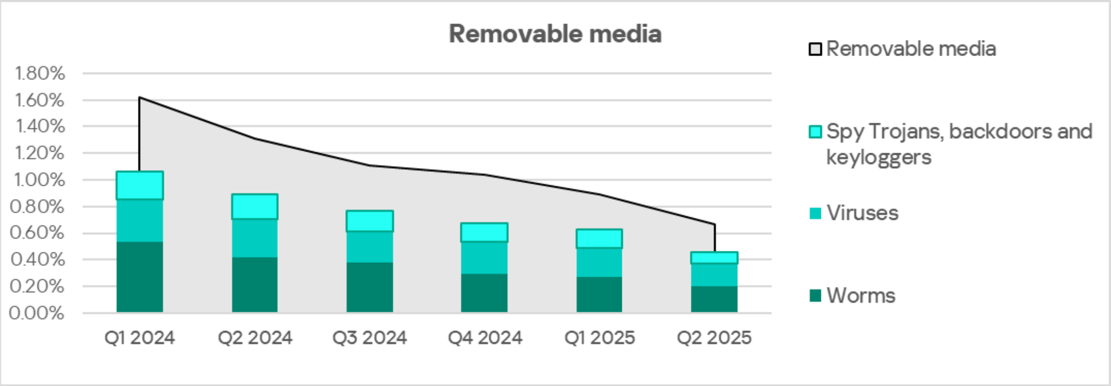
Removable media

In terms of ICS computers on which threats were blocked when connecting removable media, the Middle East ranked third globally in Q2 2025. Compared to North America (Canada), which ranks last, the rate is 25 times higher.

Within the region, there are two clear leaders in this metric: Yemen (4.85%) and Iraq (4.36%). Other countries ranged from 0.11% in Israel to 2.18% in Syria.



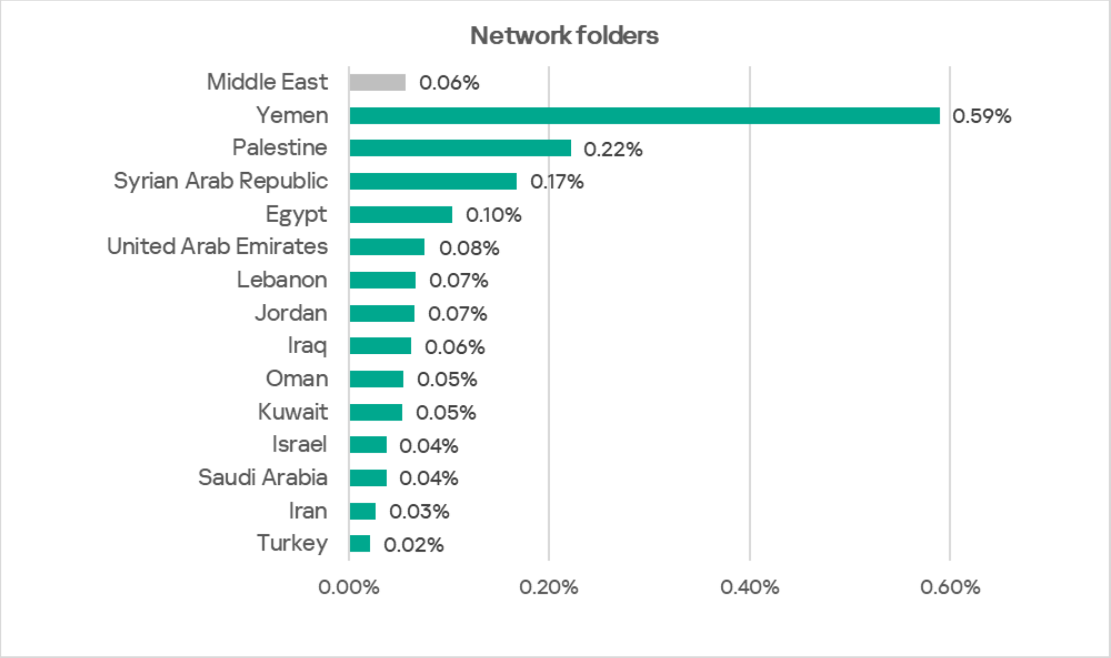
The main categories of removable media threats blocked on ICS computers in the region are worms, spyware, and viruses. By the percentage of ICS computers on which worms were blocked, the Middle East ranked third globally.



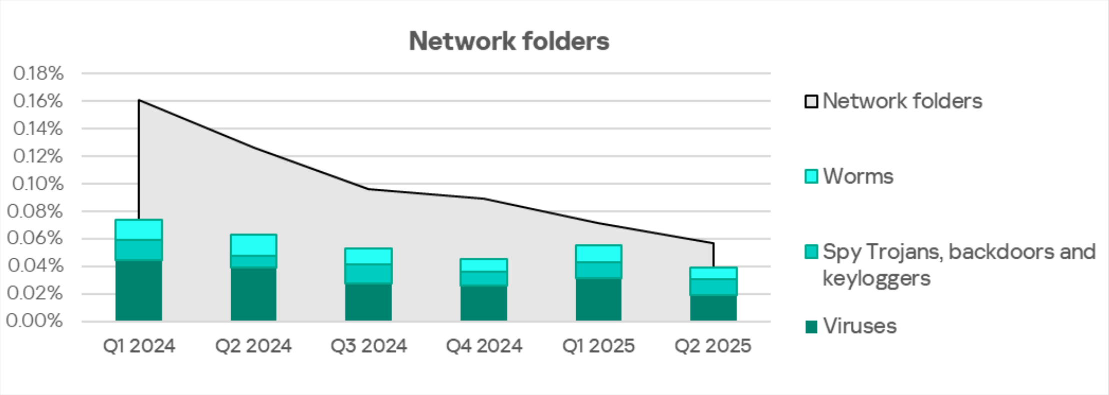
Network folders

In terms of ICS computers on which threats from network folders were blocked, the Middle East ranked fourth globally, with 0.06%. This is 5.9 times higher than Northern Europe, which had the lowest figure.

Within the region, Yemen leads by a wide margin with 0.59%.

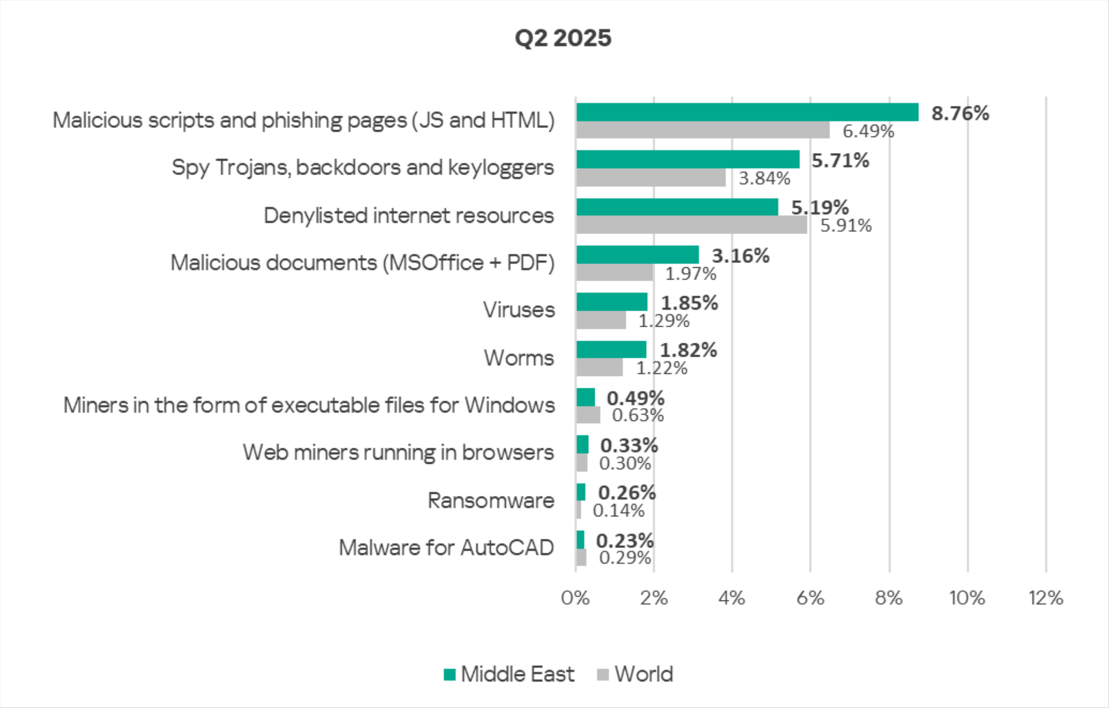


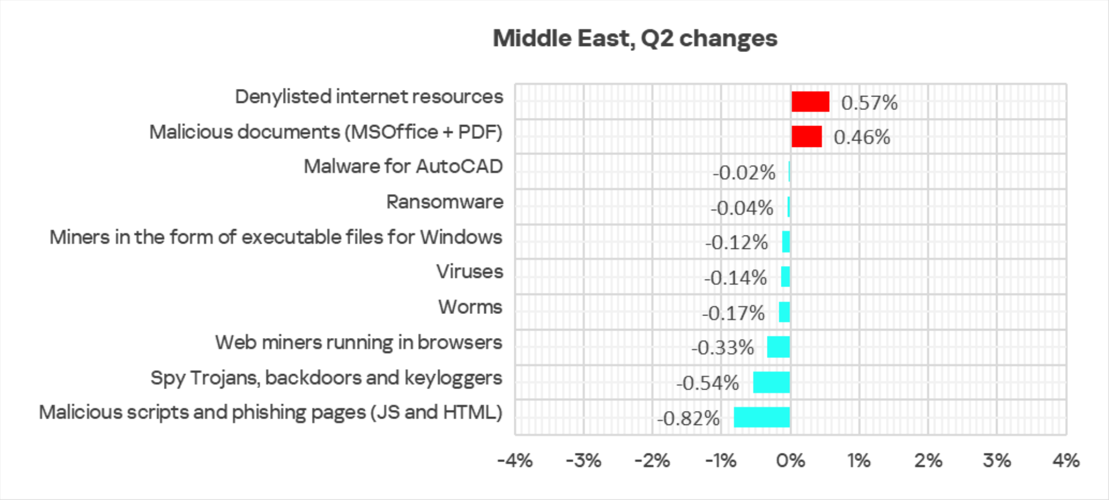
The main categories of threats spreading through network folders in the region are worms, viruses, and spyware.



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.



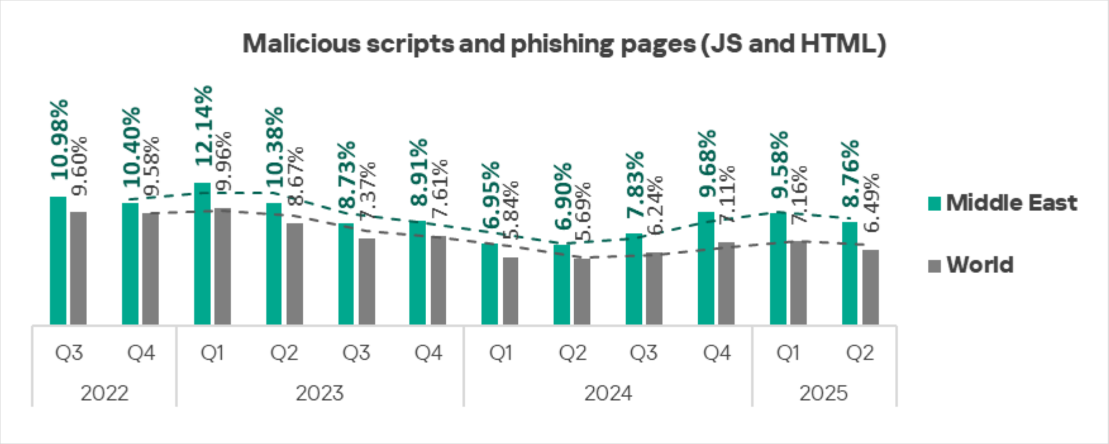


The largest differences compared with global averages are in the following threat categories:

- Ransomware: 1.9 times higher (second globally)
- Malicious documents: 1.5 times higher (third globally)
- Spyware: 1.5 times higher (fourth globally)
- Malicious scripts and phishing pages: 1.3 times higher (third globally)
- Worms: 1.5 times higher (third globally)
- Viruses: 1.4 times higher (fourth globally)

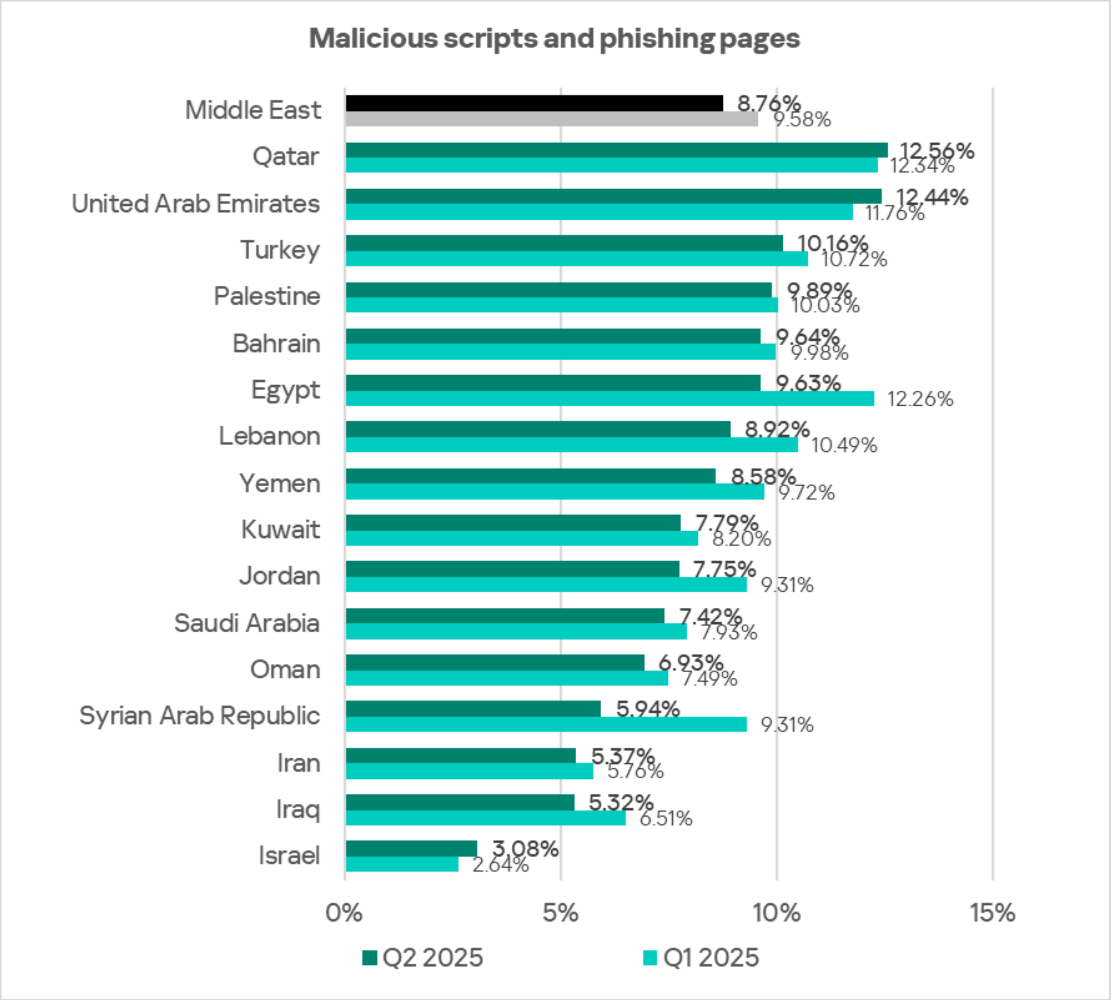
Malicious scripts and phishing pages

In terms of ICS computers on which malicious scripts and phishing pages were blocked, the Middle East ranked third globally with 8.76%. This is 2.9 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, Qatar leads in this metric with 12.56%. Israel has the lowest percentage, 1.7 times smaller than the next country, Iraq.

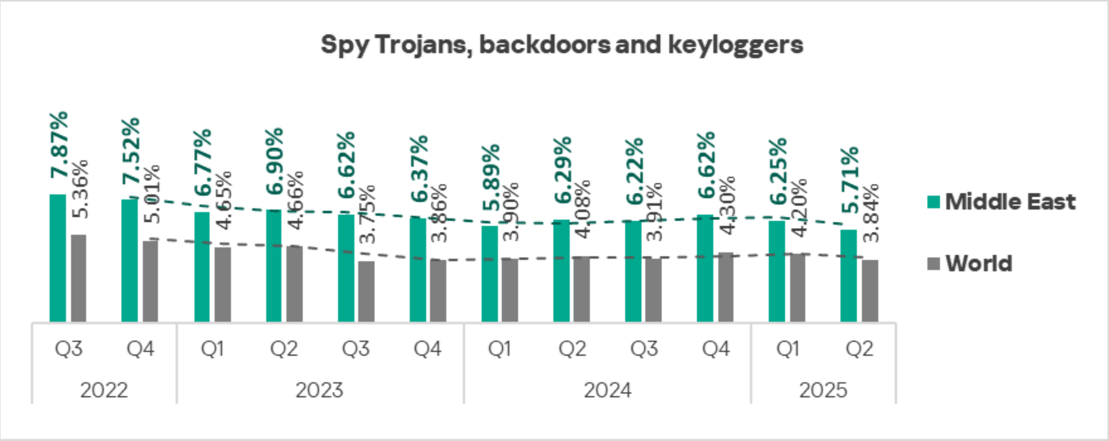


The top 3 countries in this rating — Qatar, the UAE, and Turkey — also lead the ranking in malicious documents, spyware, and the percentage of ICS computers on which threats were blocked from email clients.

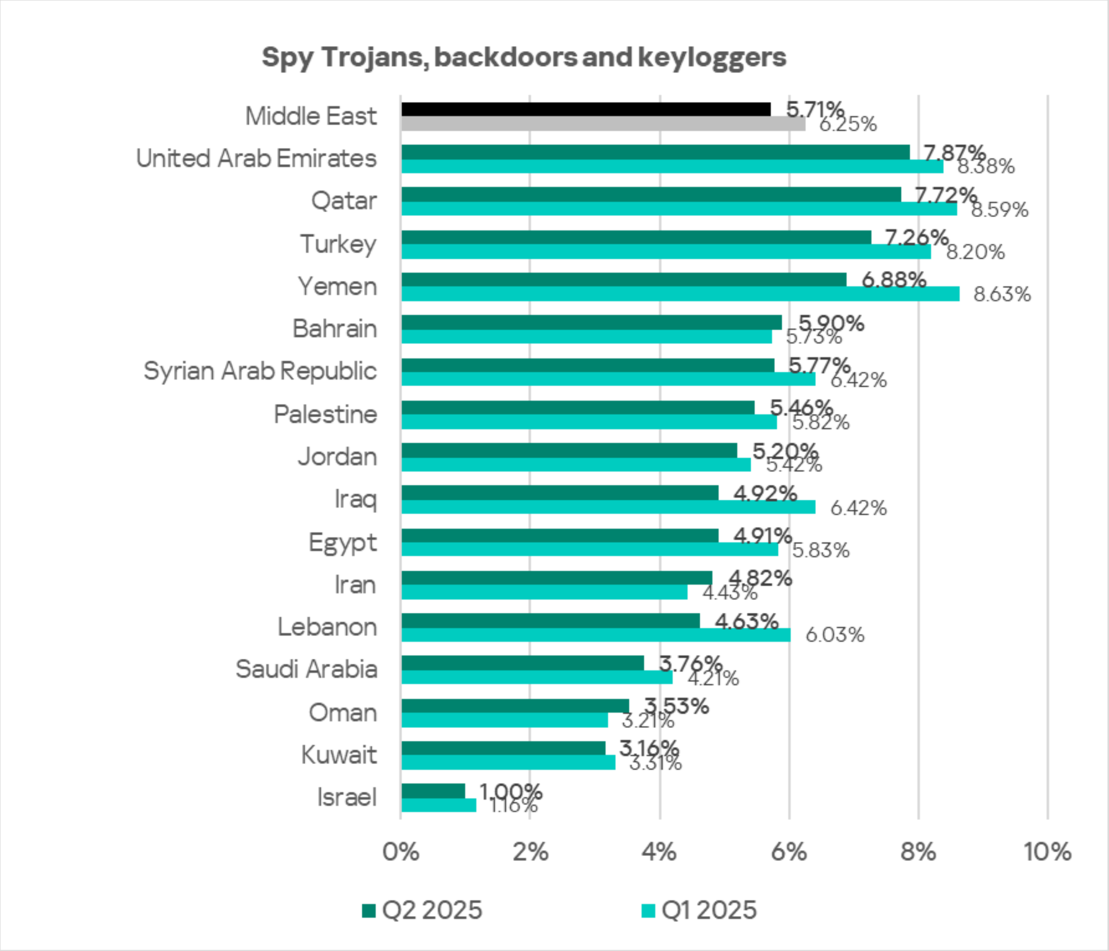
Spyware

By the percentage of ICS computers on which spyware was blocked, the Middle East ranks fourth globally with 5.71%. This is 4.1 times higher than in Western Europe, which has the lowest figure.

Since Q3 2023, the spyware rate in the Middle East has fluctuated between 5.71% and 6.62%. In Q2 2025, it reached its lowest level since Q3 2022.



Among the region's countries and territories, the UAE leads in the percentage of ICS computers on which spyware was blocked, at 7.87%. Israel has the lowest percentage, 3.2 times smaller than the preceding country, Kuwait.



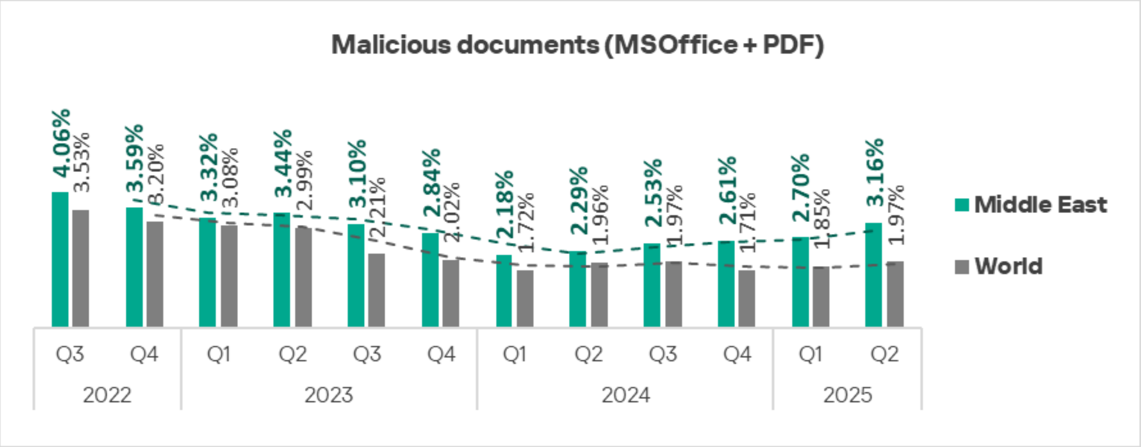
Spyware is blocked across all threat sources in the region, but most often spreads via email clients.

The top three countries in spyware also lead the rankings in email client threats, as well as blocked malicious documents, malicious scripts, and phishing pages.

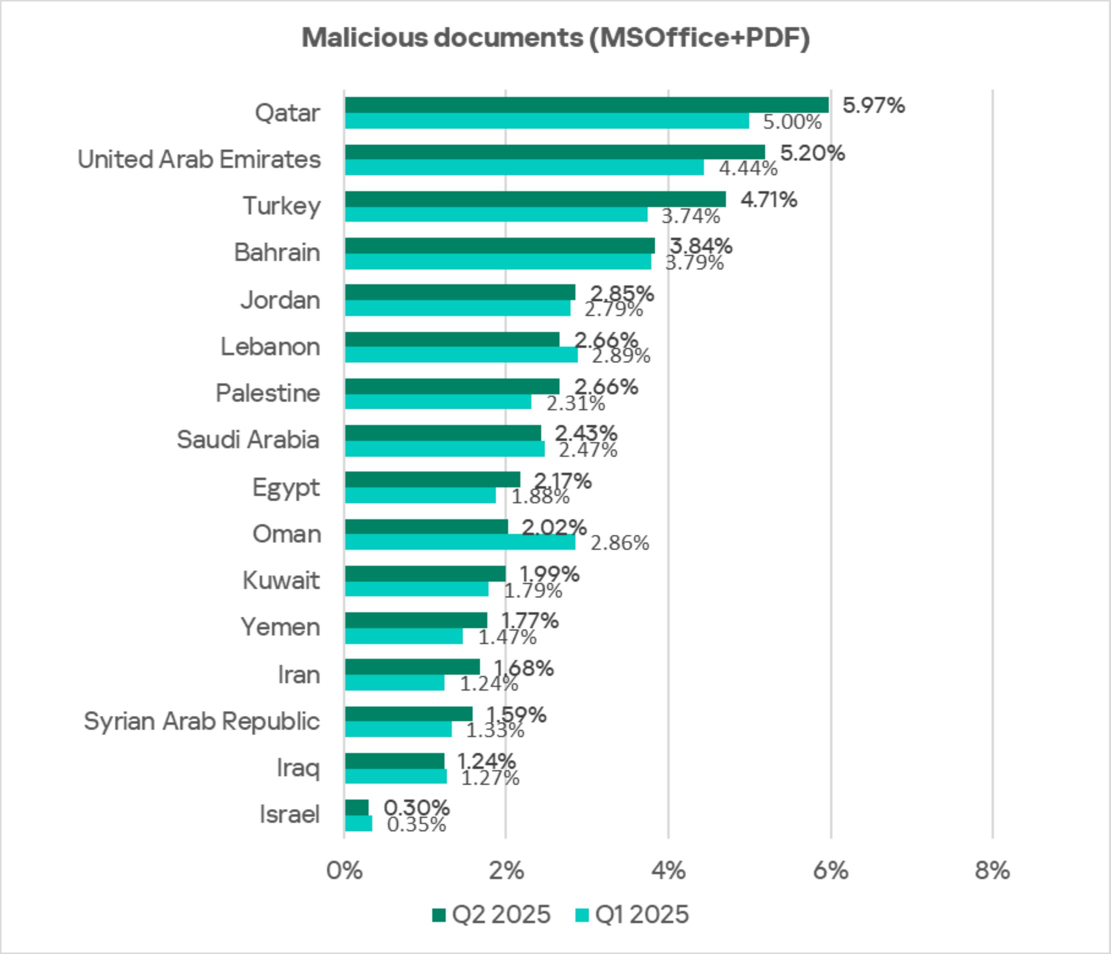
Malicious documents

Malicious documents are spread primarily via email. The Middle East ranks third globally both in email client threats and malicious documents. The malicious document rate in the region is 3.16%, 4.9 times higher than Northern Europe, which had the lowest figure.

The percentage of ICS computers on which malicious documents were blocked has been rising since Q2 2024.



Among the region's countries and territories, Qatar leads in this metric with 5.97%. Israel is last with 0.30%, 4.2 times lower than the preceding country, Iraq.



The top three countries in this ranking — Qatar, the UAE, and Turkey — also lead in malicious scripts and phishing pages, spyware, as well as the percentage of ICS computers on which threats from email clients were blocked.

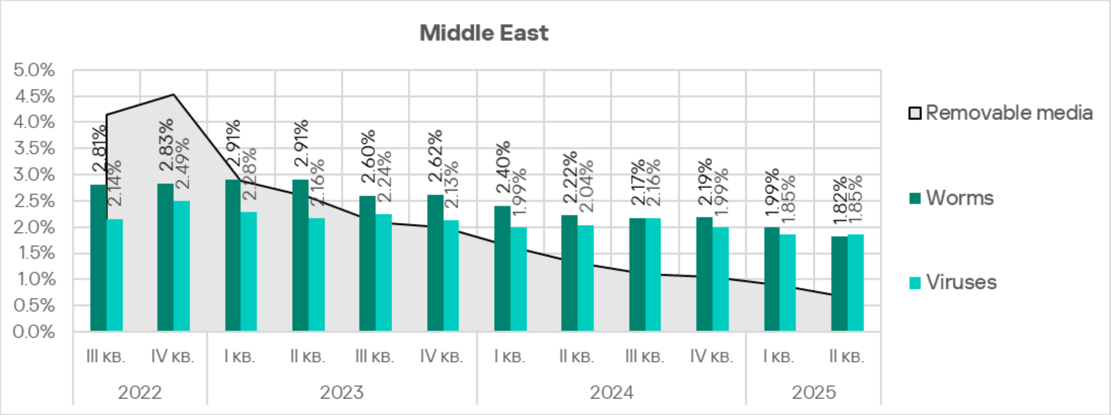
Self-propagating malware: worms and viruses

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

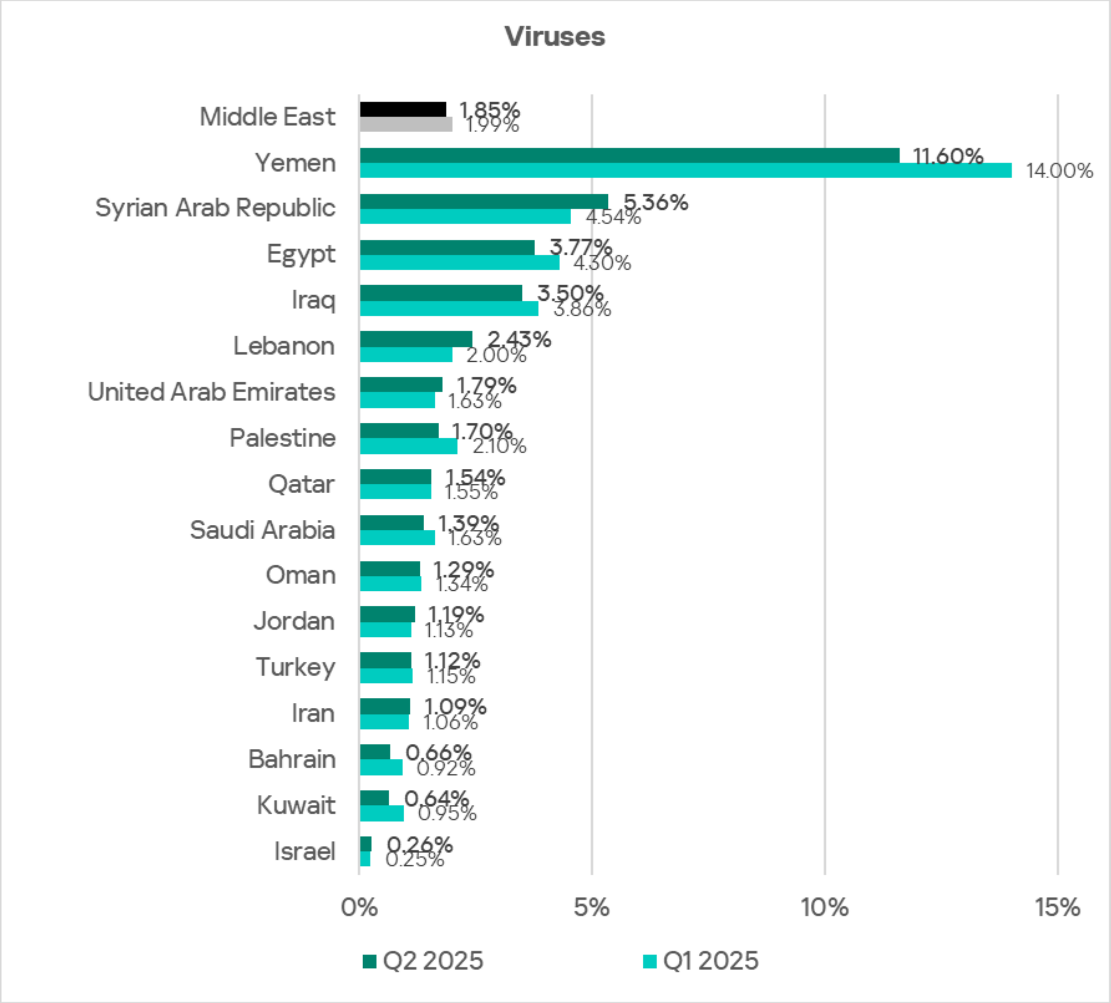
The percentage of ICS computers on which worms were blocked is 1.82%. This is 8.2 times higher than the lowest region, Australia and New Zealand.

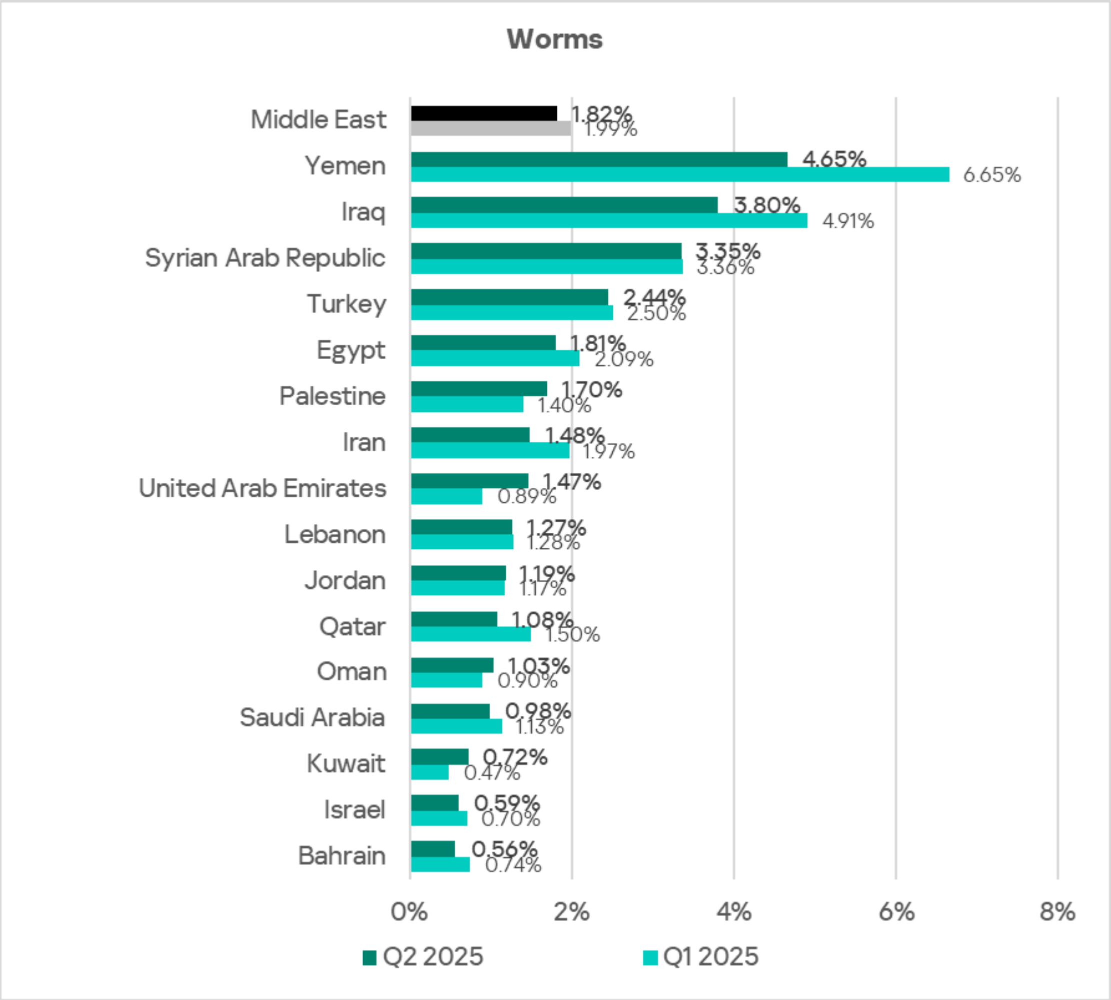
The percentage of ICS computers on which viruses were blocked is 1.85%, 14.7 times higher than Australia and New Zealand (again in last place).

The worm rate, similar to the overall percentage of threats from removable media, is gradually decreasing. Viruses display a more complex trend.



Among the region's countries and territories, Yemen leads in both worms and viruses, with a particularly wide margin in the case of viruses.



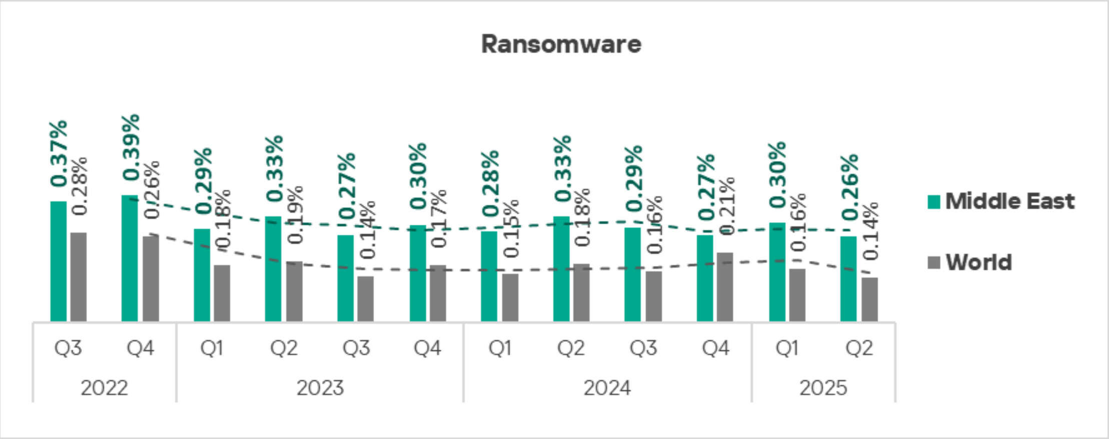


Ransomware

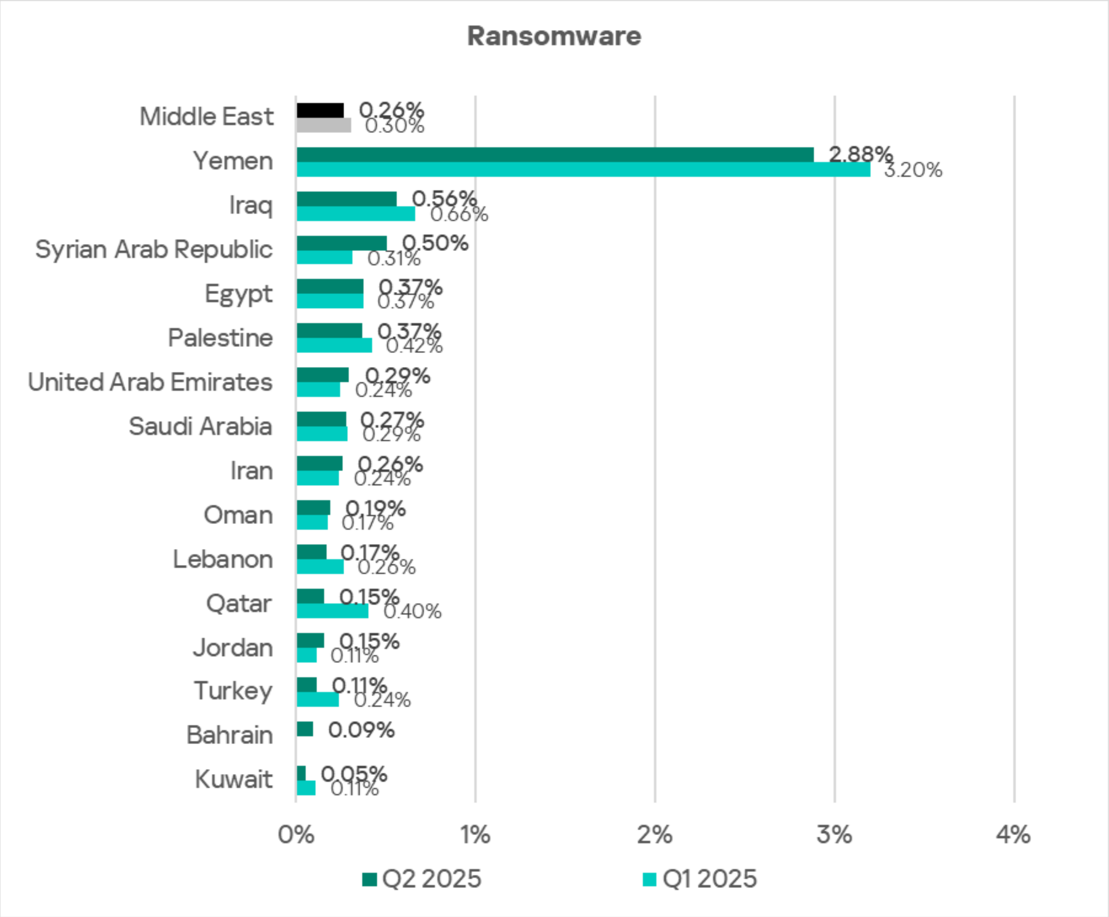
In the Middle East, the percentage of ICS computers on which ransomware was blocked is consistently high — almost double the global average. In 2024, the region led the global ranking. In Q1 and Q2 2025, it ranked second globally with 0.26%.

Compared with Western Europe, which had the lowest rate, the Middle East scored 4.1 times higher.

Since 2023, this metric has ranged between 0.26% and 0.33%. In Q2 2025, it reached its lowest since Q3 2022.



Once again, Yemen dominates in the percentage on which ransomware was blocked with a rate 5.2 times higher than Iraq, the second-ranked country.

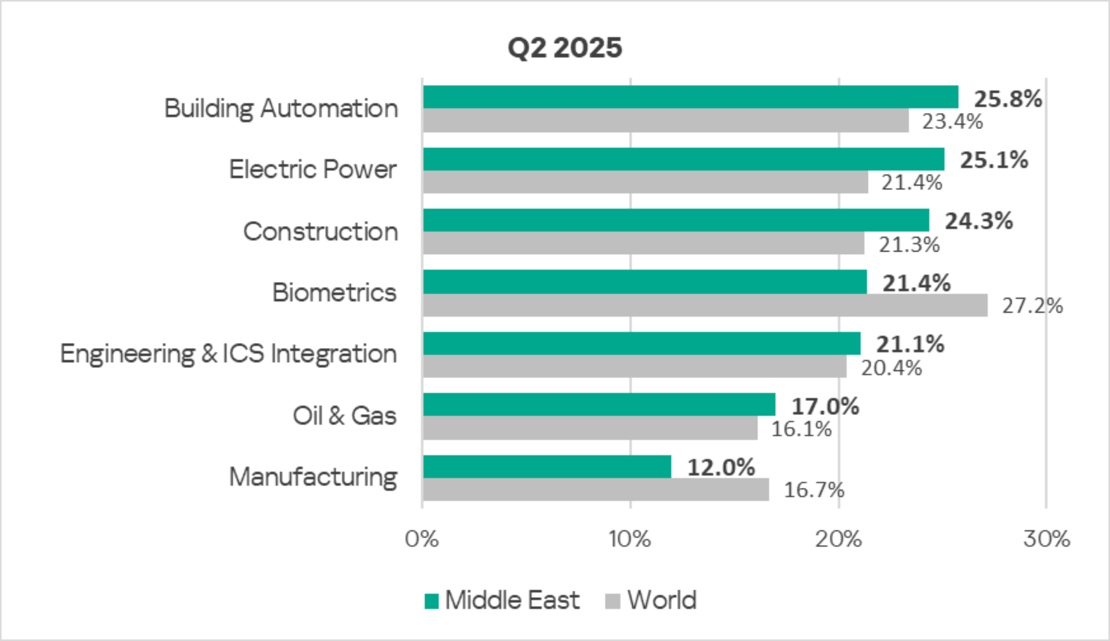


Industries

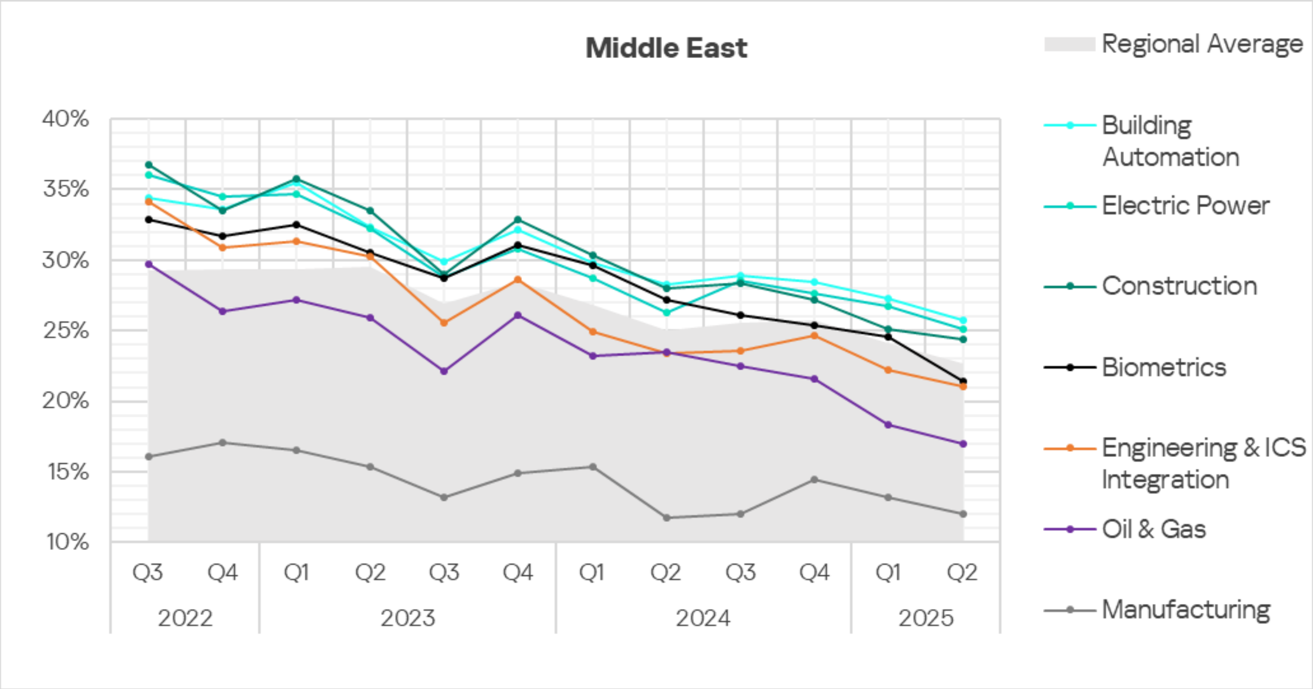
Among industries covered in the report, the most frequently targeted in the Middle East is building automation.

Compared to global averages, the percentage of ICS computers on which malicious objects were blocked is higher in the following industries:

- Electrical energy: 1.2 times higher
- Construction: 1.1 times higher
- Building automation: 1.1 times higher



In Q1 2025, the percentage of affected ICS computers decreased across all the studied industries. Despite periodic fluctuations, long-term trends show a generally positive dynamic (declining values).



Threat sources and malware categories in industries: hot spots

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

The heatmaps highlight industry hot spots — malware sources or categories with values higher than expected given the regional ranking of the industry or threat.

Threat source indicators for industries in the Middle East, Q2 2025

Industry / Threat source	Biometrics	Building Automation	Electric Power	Engineering & ICS Integration	Oil & Gas	Construction	Manufacturing	Threat category total in the region
Internet	8.50%	10.26%	11.17%	9.65%	7.23%	11.37%	5.27%	9.75%
Email clients	4.77%	8.27%	4.34%	3.93%	2.26%	4.68%	2.04%	5.47%
Removable media	1.39%	0.75%	0.61%	0.46%	0.39%	0.39%	0.65%	0.67%
Network folders	0.08%	0.09%	0.06%	0.02%	0.05%	0.03%	0.03%	0.06%
Industry total in the region	21.36%	25.79%	25.10%	21.08%	16.97%	24.35%	16.78%	

Threat category indicators for industries in the Middle East, Q2 2025

Industry / Threat category	Biometrics	Building Automation	Electric Power	Engineering & ICS Integration	Oil & Gas	Construction	Manufacturing	Threat category total in the region
Denylisted internet resources	5.09%	5.34%	6.46%	5.20%	4.03%	5.47%	2.64%	5.19%
Malicious scripts and phishing pages (JS and HTML)	7.67%	11.47%	8.10%	7.23%	6.64%	8.51%	4.50%	8.76%
Spy Trojans, backdoors and keyloggers	5.46%	8.08%	5.16%	4.56%	3.44%	4.30%	2.31%	5.71%
Worms	1.76%	2.35%	2.10%	1.49%	1.52%	1.18%	1.27%	1.82%
Miners in the form of executable files for Windows	0.45%	0.48%	0.61%	0.54%	0.44%	1.14%	0.15%	0.49%
Malicious documents (MSOffice + PDF)	2.64%	5.01%	2.69%	2.08%	1.43%	2.12%	1.04%	3.16%
Viruses	2.90%	2.53%	2.16%	1.17%	1.62%	2.21%	1.42%	1.85%
Ransomware	0.53%	0.42%	0.31%	0.15%	0.15%	0.18%	0.03%	0.26%
Web miners running in browsers	0.43%	0.31%	0.47%	0.33%	0.44%	0.92%	0.09%	0.33%
Malware for AutoCAD	0.29%	0.17%	0.29%	0.15%	0.34%	1.32%	0.36%	0.23%
Industry total in the region	21.36%	25.79%	25.10%	21.08%	16.97%	24.35%	12.00%	

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).

Industry hot spots

Building automation

- Highest percentage among industries in the region in ICS computers on which threats were blocked in email clients and network folders.
- Regional leader in malicious scripts and phishing pages, spyware, malicious documents, and worms.
- Second place regionally in viruses and ransomware.
- Third place regionally in denylisted internet resources.
- Fifth among all industries globally in malicious scripts and phishing pages.

Electrical energy industry

- Second in the region in terms of internet threats, third in terms of network folder threats.
- Regional leader in denylisted internet resources.
- Second place regionally in malicious documents, both categories of miners, and worms.
- Third place regionally in malicious scripts and phishing pages, spyware, and ransomware.

Construction

- First place regionally in internet threats; third in email client threats.
- Regional leader in both types of miners and malware for AutoCAD.
- Second place regionally in denylisted internet resources, malicious scripts, and phishing pages.
- Third place regionally in viruses.
- Fourth place globally in web miners.

Biometric systems

- Regional leader in threats from removable media. Second place in threats from email clients and network folders.
- Regional leader in viruses and ransomware.
- Second place regionally in spyware.
- Third place regionally in malicious documents and worms.

Engineering and ICS integrators

- Fourth place regionally in internet threats.

- Third place regionally in miners in the form of executable files for Windows.
- Fourth place regionally in spyware and denylisted internet resources.

Oil and gas industry

- Fourth place regionally in network-folder threats.
- Third place regionally in web miners and malware for AutoCAD.
- Fourth place regionally in worms.

Manufacturing

- Third place in the region in threats from removable media.
- Second place regionally in malware for AutoCAD.

Methodology used to prepare statistics

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

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

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

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

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

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

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

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

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

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

Kaspersky ICS CERT

ics-cert@kaspersky.com