Kaspersky ICS CERT

kaspersky

Threat landscape for industrial automation systems

Regions, Q2 2024

21.11.2024

Version 1.3

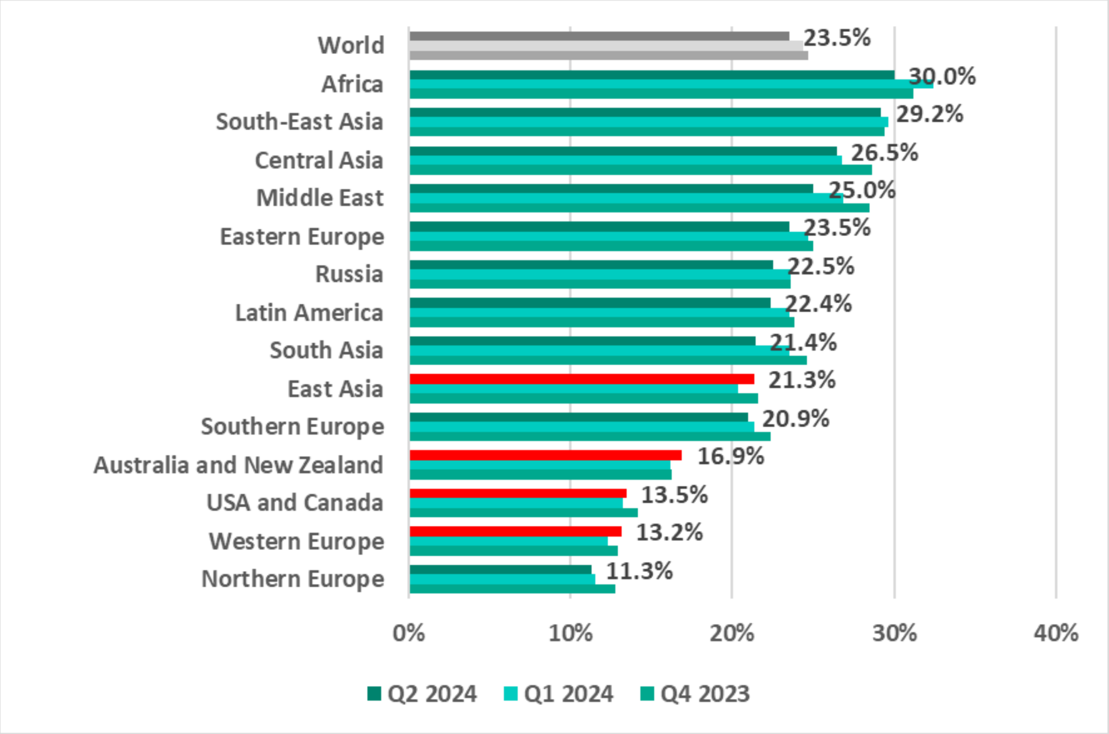
Q2 overview

Percentage of ICS computers

In the second quarter of 2024, the global percentage of ICS computers on which malicious objects were blocked decreased by 0.9 pp from the previous quarter to 23.5%.

Regionally, the percentage of ICS computers that blocked malicious objects during the quarter ranged from 11.3% in Northern Europe to 30% in Africa.

Regions ranked by percentage of ICS computers on which malicious objects were blocked, Q2 2024



All regions ranked by percentage of ICS computers on which malicious objects were blocked in the second quarter can be divided into three groups:

Over 25%

- Africa – 30.0%
- South-East Asia – 29.2%
- Central Asia – 26.5%

In the regions within this group, OT computers are generally overexposed to cyberthreats. There is underinvestment in cybersecurity, both in terms of tools and measures, as well as in addressing the shortage of experts, fostering a strong cybersecurity culture, and raising awareness.

20–25%

- Middle East – 25.0%
- Eastern Europe – 23.5%
- Russia – 22.5%
- Latin America – 22.4%
- South Asia – 21.4%
- East Asia – 21.3%
- Southern Europe – 20.9%

The regions within this group may face specific challenges in isolating their OT infrastructure from potential cyberthreats.

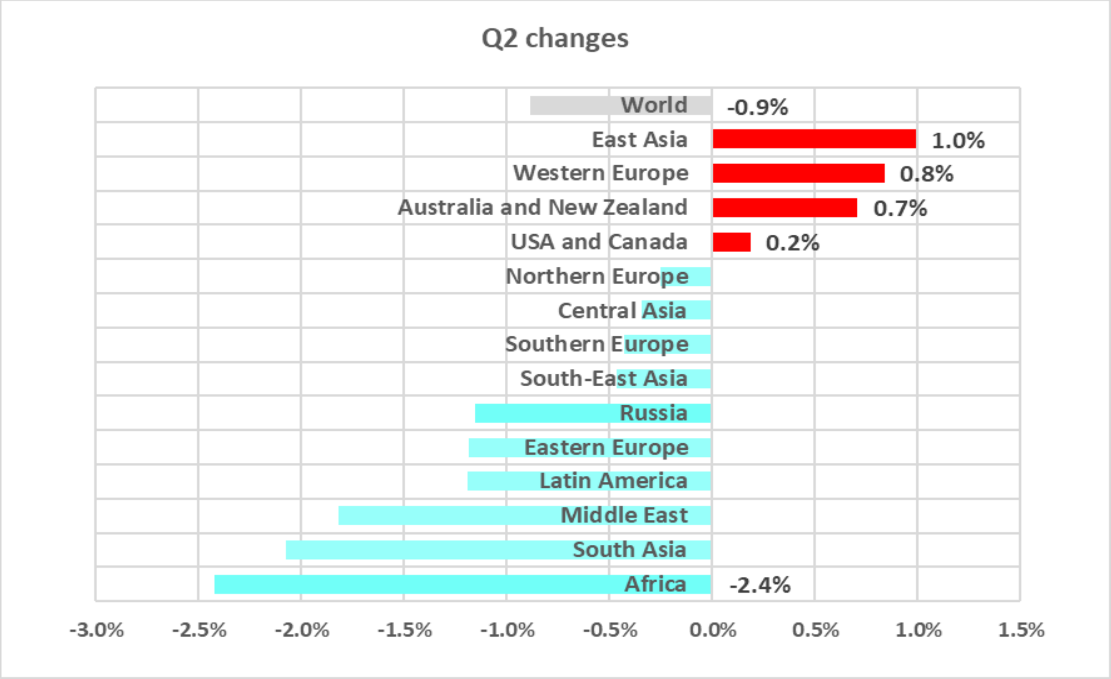
Up to 20%

- Australia and New Zealand – 16.9%
- US and Canada – 13.5%
- Western Europe – 13.2%
- Northern Europe – 11.3%

The third group consists of regions that are the safest in terms of keeping their OT infrastructure isolated from cyberthreats

Compared to the first quarter, the percentage of ICS computers on which malicious objects were blocked during the second quarter has increased in four regions.

Regions and world. Changes in the percentage of attacked ICS computers in Q2 2024



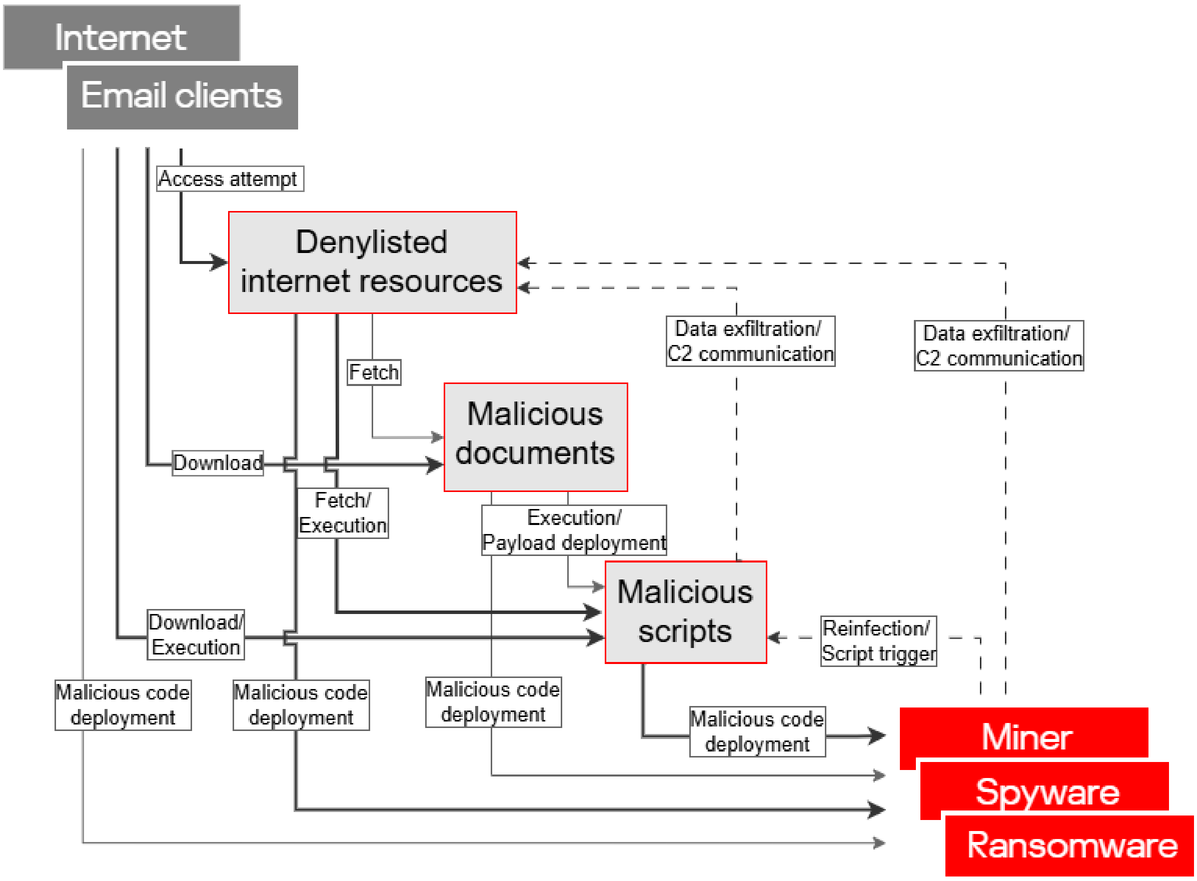
Malicious object categories

Malicious objects used for initial infection

Malicious objects that are used for initial infection of ICS computers include dangerous internet resources that are added to denylists, malicious scripts and phishing pages, and malicious documents.

By the logic of cybercriminals, these malicious objects can spread easily. As a result, they are blocked by security solutions more often than anything else. This is reflected in our statistics.

> Typical attacks blocked within an OT network are a multi-stage process, where each subsequent step of the attackers is aimed at increasing privileges and gaining access to other systems by exploiting vulnerabilities in OT systems and networks.
>
> It is worth noting that during the attack, intruders often repeat the same steps (TTP), particularly, when they use malicious scripts and established communication channels with the management and control infrastructure (C2) to move horizontally within the network and advance the attack.


Internet
Email clients
Access attempt
Denylisted internet resources
Data exfiltration/ C2 communication
Data exfiltration/ C2 communication
Fetch
Malicious documents
Download
Fetch/ Execution
Execution/ Payload deployment
Malicious scripts
Download/ Execution
Reinfection/ Script trigger
Malicious code deployment
Malicious code deployment
Malicious code deployment
Malicious code deployment
Miner
Spyware
Ransomware

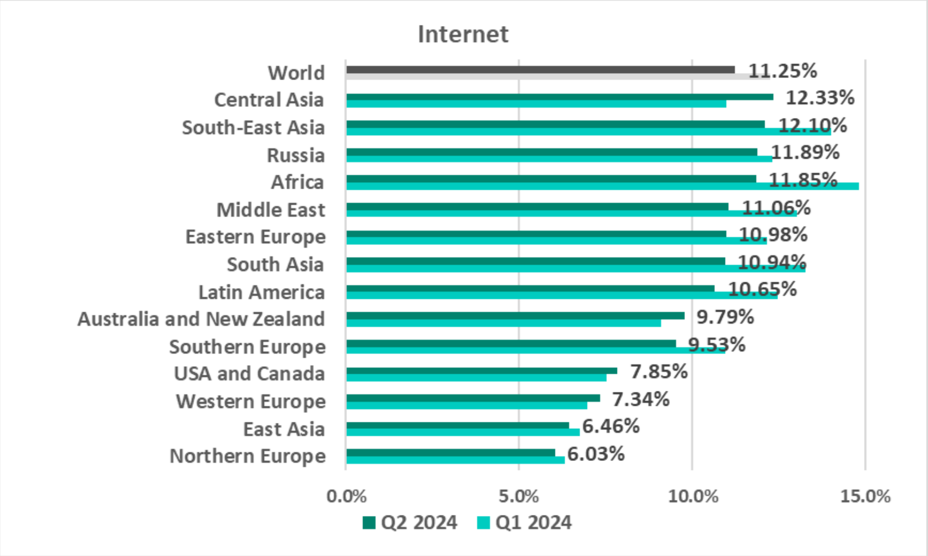
Kill chain examples: from initial infection to next-stage malware

Globally and in almost all regions, denylisted internet resources and malicious scripts and phishing pages are the top malware categories in terms of the percentage of ICS computers on which this malware was blocked.

The sources of the majority of malicious objects used for initial infection are the internet and email.

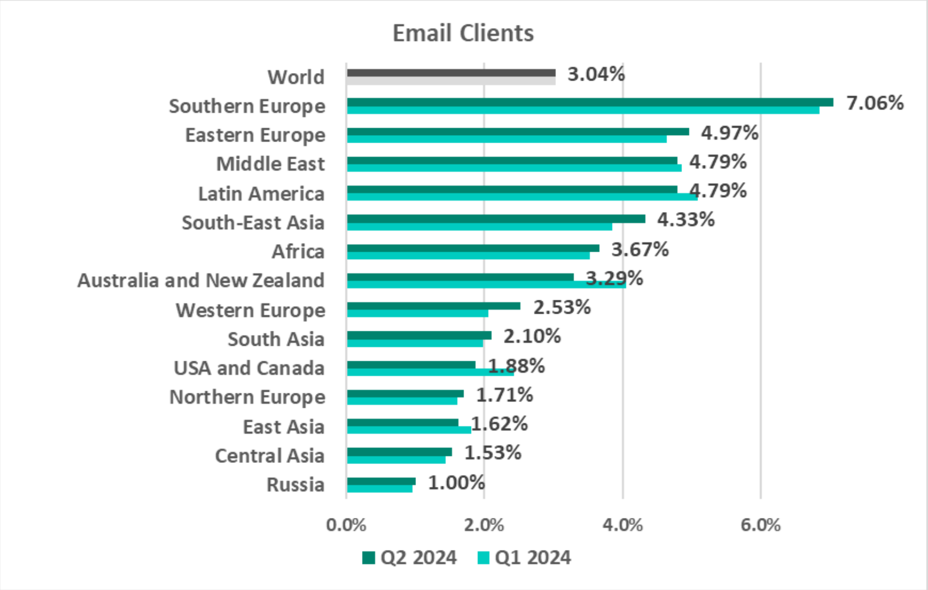
In Q2 2024, the regions with **internet** threats above the global average of 11.25% were **Central Asia**, **South-East Asia**, **Russia**, and **Africa**.

Regions ranked by percentage of ICS computers on which threats from the internet were blocked, Q2 2024



The regions with **email threats** above the global average of 3.04% were **Southern Europe**, **Eastern Europe**, **the Middle East**, **Latin America**, **South-East Asia**, **Africa**, **Australia and New Zealand**.

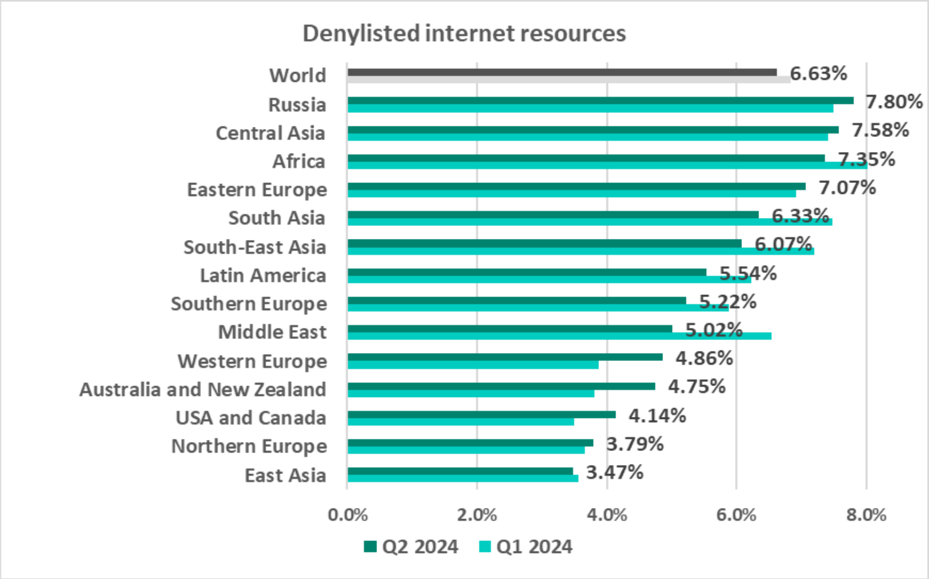
Regions ranked by percentage of ICS computers on which threats from email clients were blocked, Q2 2024



Denylisted internet resources

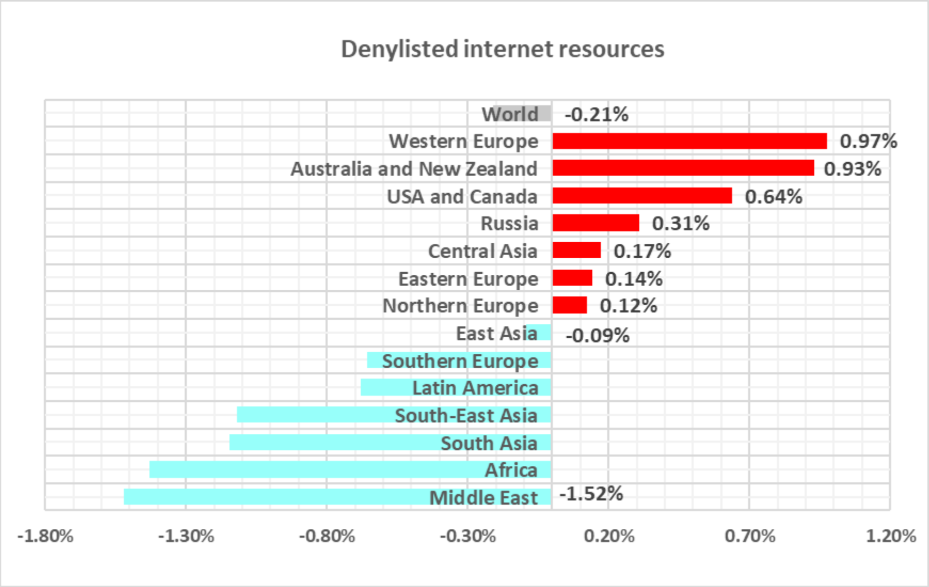
The leading regions by percentage of ICS computers on which denylisted internet resources were blocked (above the global average of 6.63%) were **Russia**, **Central Asia**, **Africa**, and **Eastern Europe**.

Regions ranked by percentage of ICS computers on which denylisted internet rersources were blocked, Q2 2024



The top three regions in terms of **growth** in the percentage of ICS computers on which denylisted internet resources were blocked were Western Europe, Australia and New Zealand, and USA and Canada.

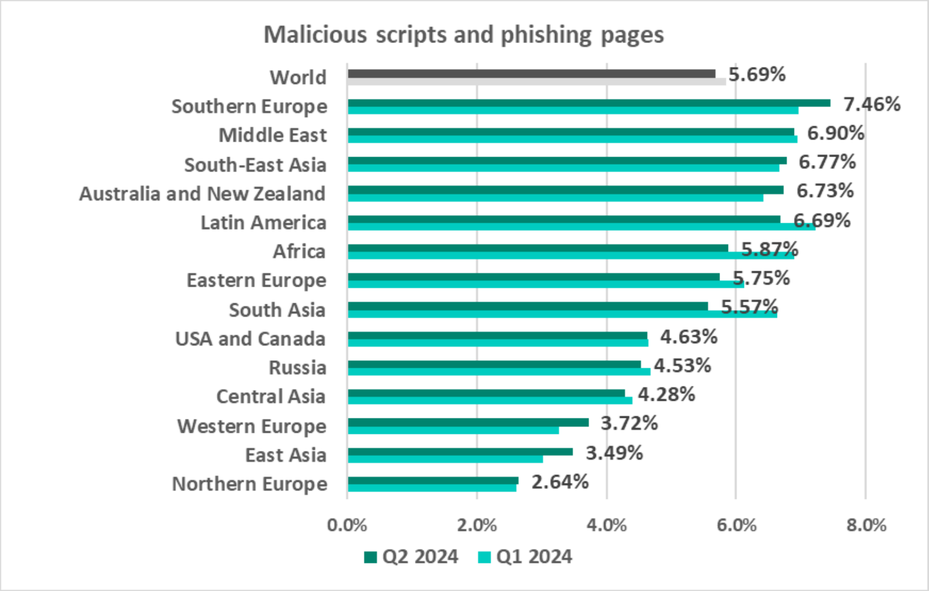
Changes in the percentage of ICS computers on which denylisted internet resources were blocked, Q2 2024



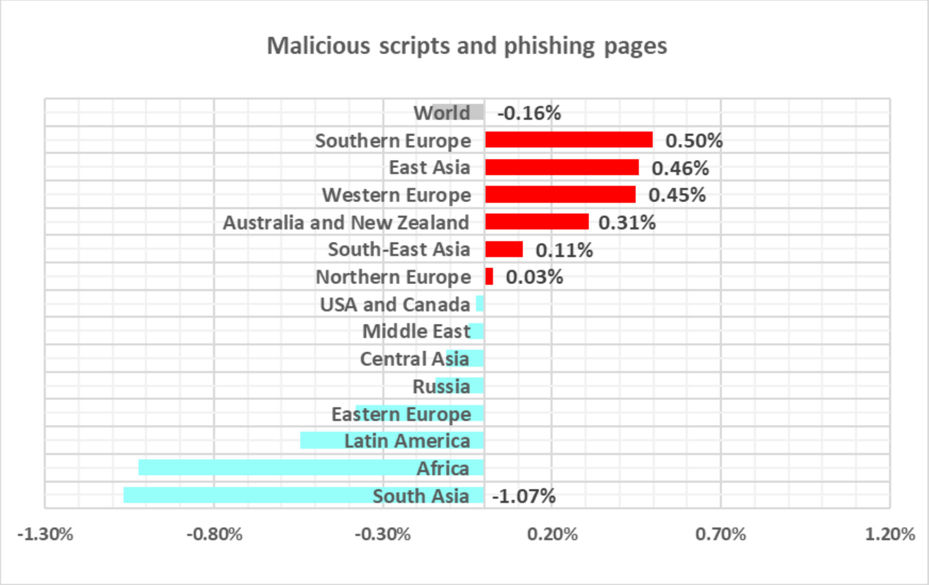
Malicious scripts and phishing pages

The leading regions by percentage of ICS computers on which malicious scripts and phishing pages were blocked (above the global average of 5.69%) were **Southern Europe**, **the Middle East**, **South-East Asia**, **Australia and New Zealand**, **Latin America**, **Africa**, and **Eastern Europe**.

Regions ranked by percentage of ICS computers on which malicious scripts and phishing pages were blocked, Q2 2024



Changes in he percentage of ICS computers on which malicious scripts and phishing pages were blocked, Q2 2024

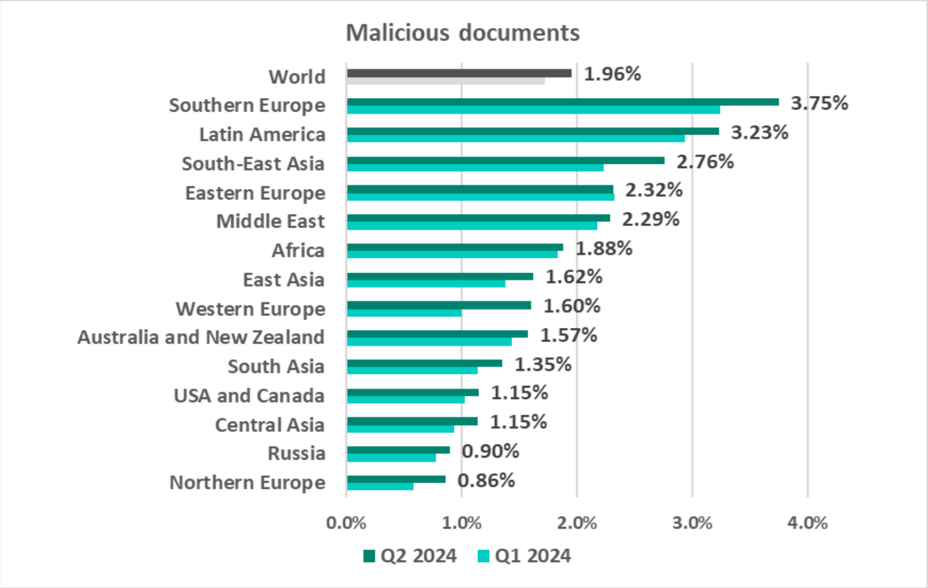


The top three regions in terms of **growth** in the percentage of ICS computers on which malicious scripts and phishing pages were blocked were Southern Europe, East Asia, and Western Europe.

Malicious documents

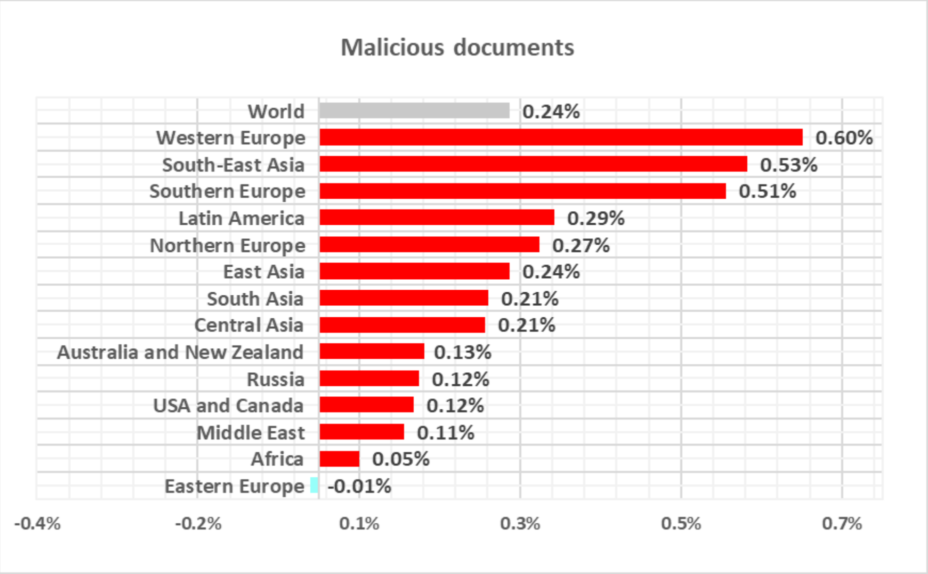
The leading regions by percentage of ICS computers on which malicious documents were blocked (above the global average of 1.96%) were **Southern Europe**, **Latin America**, **South-East Asia**, **Eastern Europe**, and **the Middle East**.

Regions ranked by percentage of ICS computers on which malicious documents were blocked, Q2 2024



The top three regions in terms of **growth** in the percentage of ICS computers on which malicious documents were blocked were Western Europe, South-East Asia, and Southern Europe.

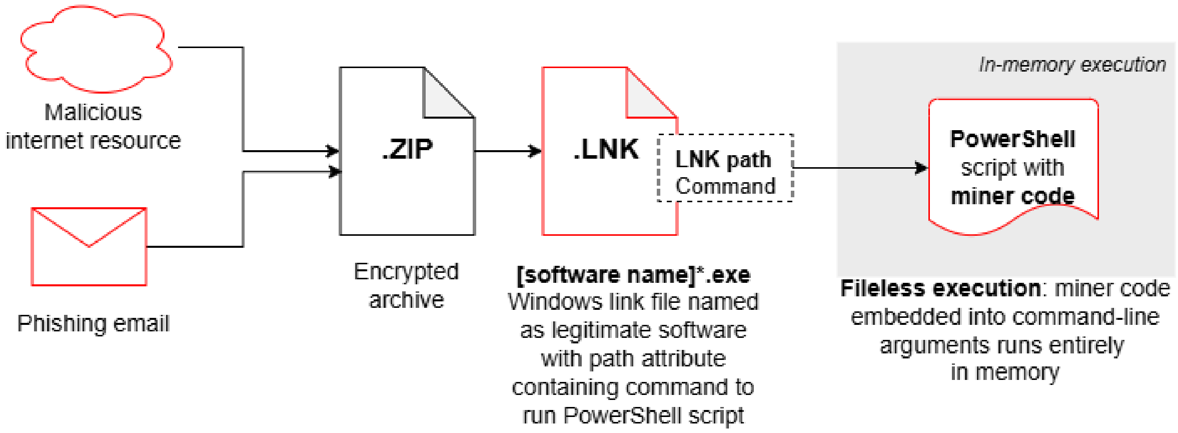
Changes in the percentage of ICS computers on which malicious documents were blocked, Q2 2024



Next-stage malware

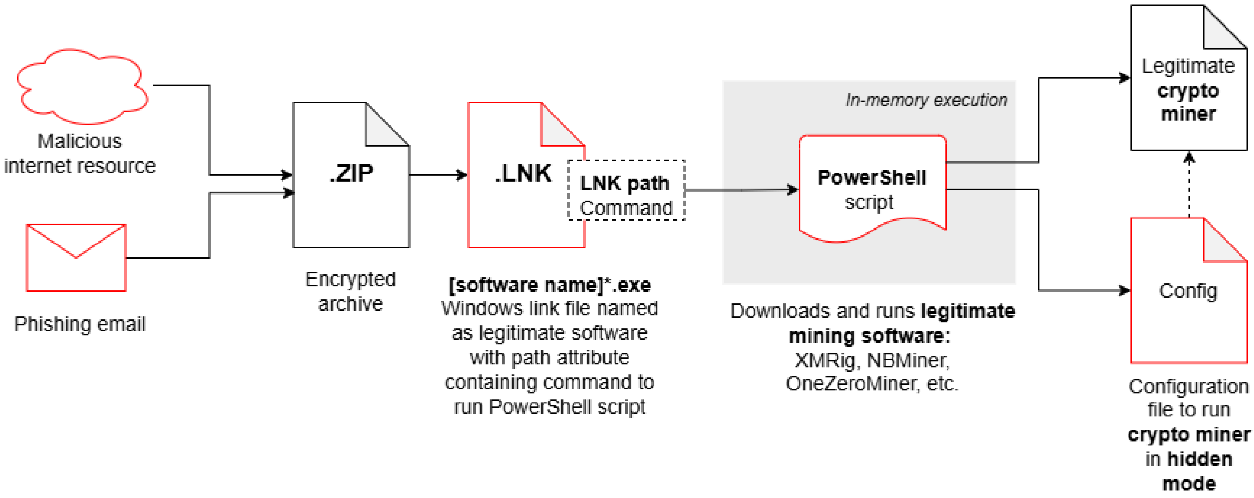
Malicious objects used to initially infect computers deliver next-stage malware – spyware, ransomware, and miners – to victims' computers.

In the second quarter of 2024, a significant portion of Windows miners found on ICS computers consisted of archives with names mimicking legitimate software. These archives did not contain actual software but included a Windows LNK file, commonly known as a shortcut. However, the target (or path) that the LNK file points to is not a regular application, but rather a command capable of executing malicious code, such as a PowerShell script. Nowadays, threat actors are increasingly using PowerShell to execute malware, including cryptominers, by embedding malicious code directly into command-line arguments. This code runs entirely in memory, enabling fileless execution and minimizing detection.


Malicious internet resource
Phishing email
.ZIP
Encrypted archive
.LNK
LNK path
Command
[software name]*.exe Windows link file named as legitimate software with path attribute containing command to run PowerShell script
In-memory execution
PowerShell script with miner code
Fileless execution: miner code embedded into command-line arguments runs entirely in memory

Kill chain example: fileless execution in cryptomining attacks

Another common method of deploying miners on ICS computers involves using legitimate cryptocurrency mining software such as XMRig, NBMiner, OneZeroMiner, and others. While these miners are not inherently malicious, they are classified as RiskTools by security systems. Attackers exploit these miners by combining them with customized configuration files that enable the miner's activity to be concealed from the user's view.


Malicious internet resource
Phishing email
.ZIP
Encrypted archive
.LNK
LNK path Command
[software name]*.exe Windows link file named as legitimate software with path attribute containing command to run PowerShell script
In-memory execution
PowerShell script
Downloads and runs legitimate mining software: XMRig, NBMiner, OneZeroMiner, etc.
Legitimate crypto miner
Config
Configuration file to run crypto miner in hidden mode

Kill chain example: use of legitimate mining tools in cryptomining attacks

Spyware

As a rule, the higher the percentage of ICS computers on which the initial infection malware is blocked, the higher the percentage for next-stage malware.

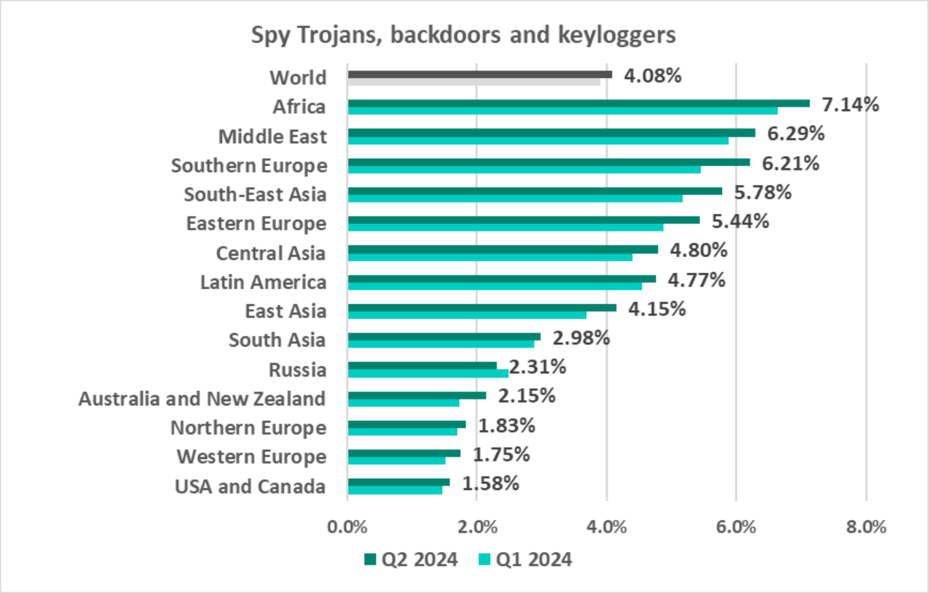
Spyware (including Trojans, backdoors, and keyloggers) is typically the most frequently detected type of next-stage malware. It is either used as a toolset for intermediate steps in the kill chain (such as reconnaissance and lateral movement) or as a final-stage tool for stealing and exfiltrating confidential data.

When spyware is detected on an OT computer, it usually indicates that the initial infection vector was not prevented – whether through a user clicking on a malicious link, opening an attachment from a phishing email, or plugging in an infected USB drive. This suggests that OT perimeter protection measures (such as network security and enforcement of removable device policies) were either absent or ineffective.

As expected, the regions leading in the percentage of ICS computers on which spyware was blocked were also the leading regions for initial infection threats (with the exception of Russia, which does not show high rates of spyware).

In Q2 2024, the regions with spyware above the global average of 4.08% were **Africa**, **the Middle East**, **Southern Europe**, **South-East Asia**, **Eastern Europe**, **Central Asia**, **Latin America**, **East Asia**.

Regions ranked by percentage of ICS computers on which spyware was blocked, Q2 2024

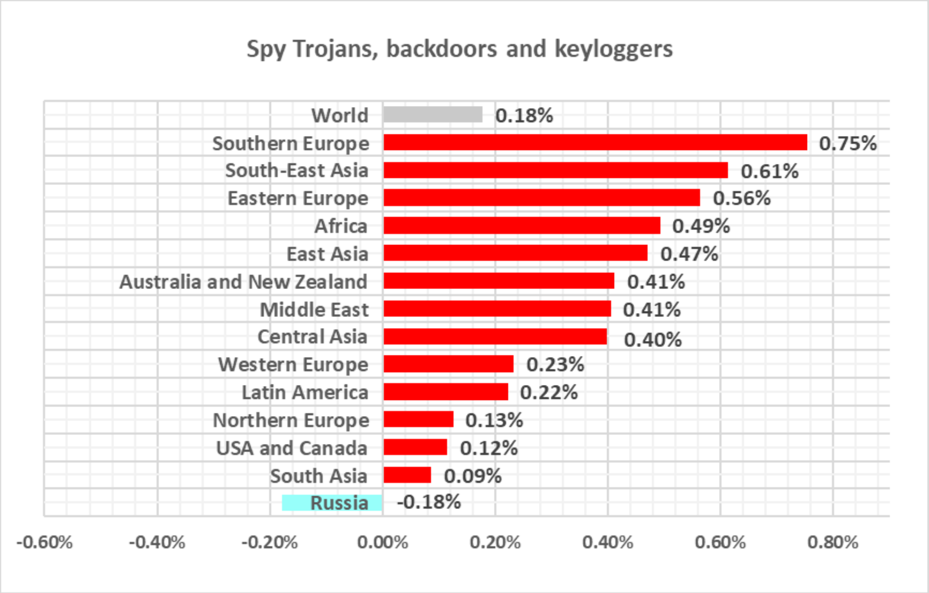


In almost all regions, spyware does not rank higher than third in the threat category rankings by percentage of ICS computers on which it was blocked, except in the following regions:

- **East Asia**: in this region, spyware is the **number one malware category** in terms of the percentage of ICS computers on which it was blocked (4.15%).
- **Central Asia, Africa, the Middle East, and Southern Europe**: spyware is the **second most prevalent** threat in these regions.

The top three regions in terms of **growth** in the percentage of ICS computers on which spyware was blocked were Southern Europe, South-East Asia, and Eastern Europe.

Changes in the percentage of ICS computers on which spyware was blocked, Q2 2024

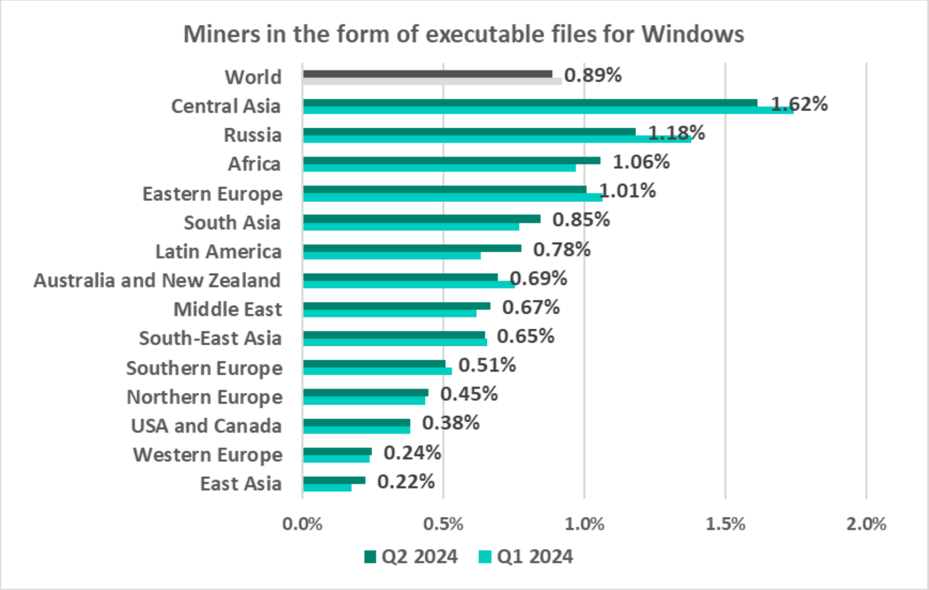


Covert crypto-mining programs

Miners in the form of executable files for Windows

The leading regions by percentage of ICS computers on which miners in the form of executable files for Windows were blocked (above the global average of 0.89%) were **Central Asia**, **Russia**, **Africa**, and **Eastern Europe**.

Regions ranked by percentage of ICS computers on which miners in the form of executable files for Windows were blocked, Q2 2024



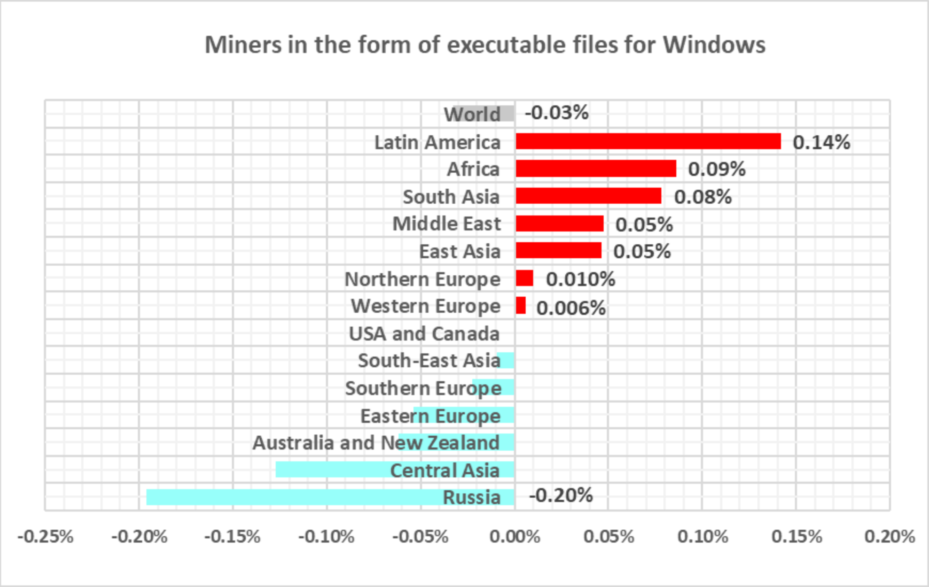
In the global ranking of threat categories by percentage of ICS computers on which they were blocked, miners in the form of Windows executable files are ranked seventh.

- In the corresponding ranking in Russia, they are in fourth place.

- In Central Asia, Australia and New Zealand, Northern Europe they came fifth.

The top three regions in terms of **growth** in the percentage of ICS computers on which miners in the form of Windows executable files were blocked were Latin America, Africa, and South Asia.

Changes in the percentage of ICS computers on which miners in the form of executable files for Windows were blocked, Q2 2024

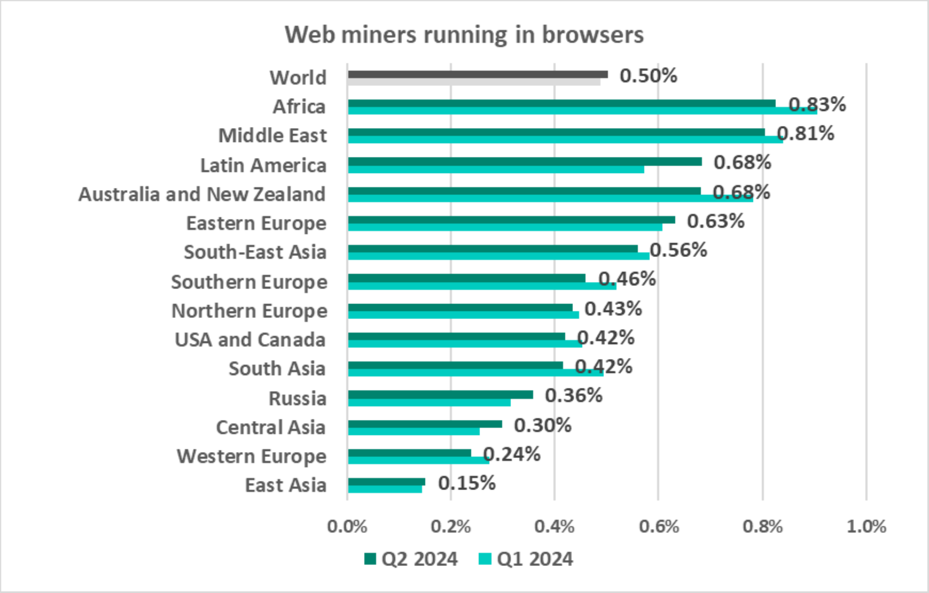


Covert crypto-mining programs

Web miners running in browsers

The leading regions by percentage of ICS computers on which web miners running in browsers were blocked (above the global average of 0.50%) were: **Africa**, **Middle East**, **Latin America**, **Australia and New Zealand**, **Eastern Europe**, and **South-East Asia**.

Regions ranked by percentage of ICS computers on which web miners were blocked, Q2 2024

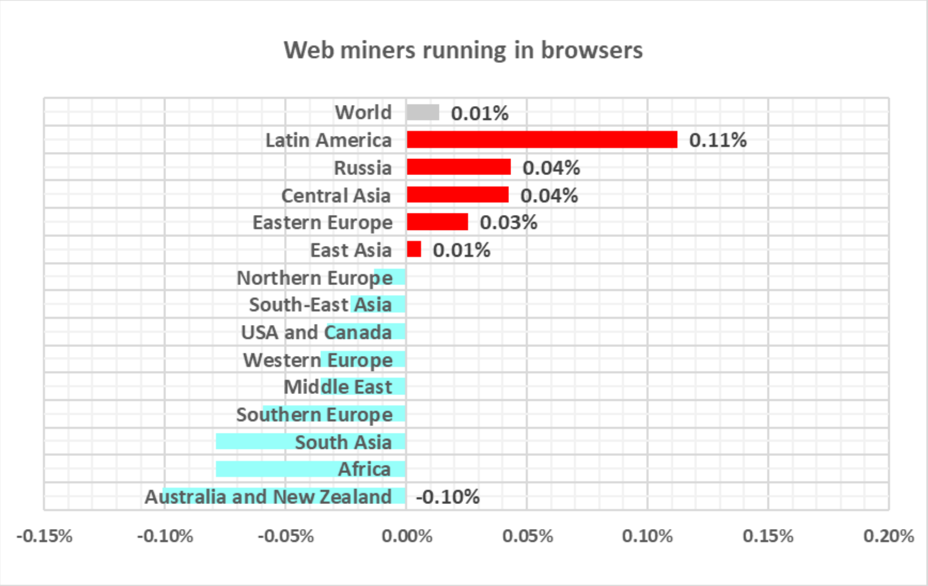


In the regional rankings of threat categories by percentage of ICS computers on which they were blocked, web miners ended up higher regionally (eighth place globally) in:

- US and Canada – fifth place in the regional ranking
- Northern Europe, Australia and New Zealand – sixth place in the respective regional ranking
- Eastern, Western, Southern Europe, Middle East – seventh place in the respective regional ranking

The top three regions in terms of **growth** in the percentage of ICS computers on which web miners were blocked were Latin America, Russia, and Central Asia.

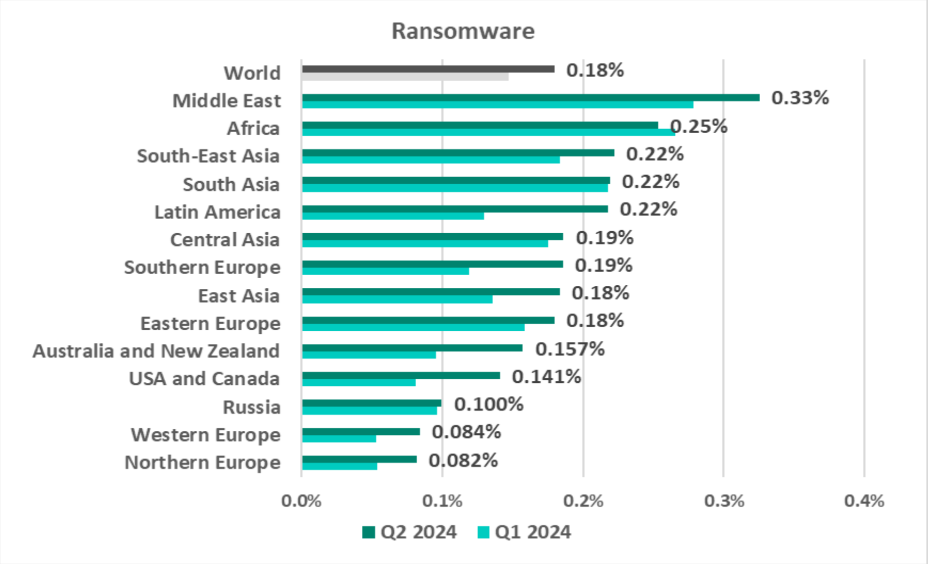
Changes in the percentage of ICS computers on which web miners were blocked, Q2 2024



Ransomware

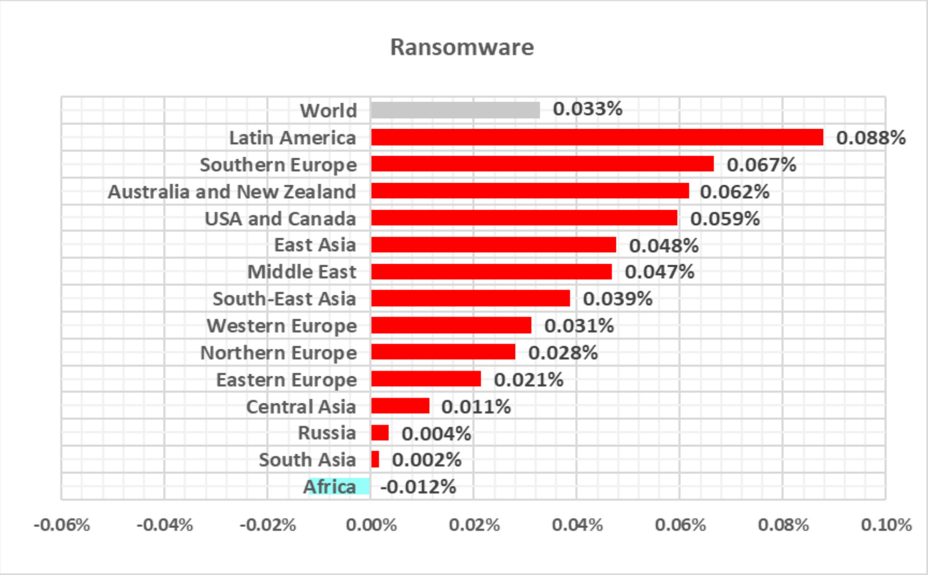
The regions where the highest percentage of ICS computers on which ransomware was blocked (above the global average of 0.18%) were **the Middle East**, **Africa**, **South-East Asia**, **South Asia**, **Latin America**, **Central Asia**, **Southern Europe**, and **East Asia**.

Regions ranked by percentage of ICS computers on which ransomware was blocked, Q2 2024



The top three regions in terms of **growth** in the percentage of ICS computers on which ransomware was blocked were Latin America, Southern Europe, and Australia and New Zealand.

Changes in the percentage of ICS computers on which ransomware was blocked, Q2 2024



Self-propagating malware. Worms and viruses

Worms and virus-infected files were originally used for initial infection, but as botnet functionality evolved, they took on next-stage characteristics.

To spread across ICS networks, viruses and worms rely on removable media, network folders, infected files including backups, and network attacks on outdated software.

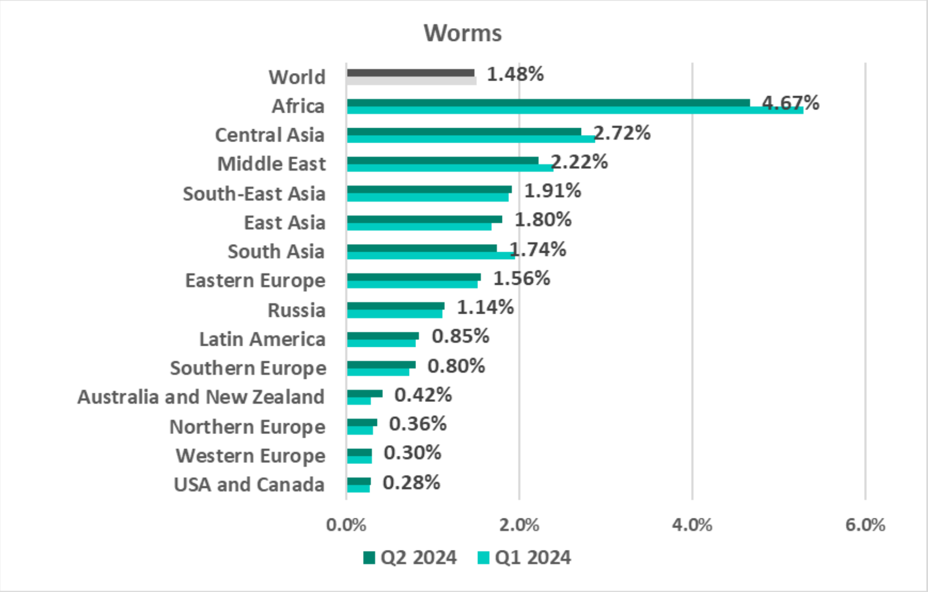
> High rates of self-propagating malware and malware spreading via network folders at the industry, country, or regional level likely indicate the presence of unprotected OT infrastructure that lacks even basic endpoint protection.

Worms

The leading regions by percentage of ICS computers on which worms were blocked (above the global average of 1.48%) were **Africa**, **Central Asia**,

the Middle East, **South-East Asia**, **East Asia**, **South Asia**, and **Eastern Europe**.

Regions ranked by percentage of ICS computers on which worms were blocked, Q2 2024

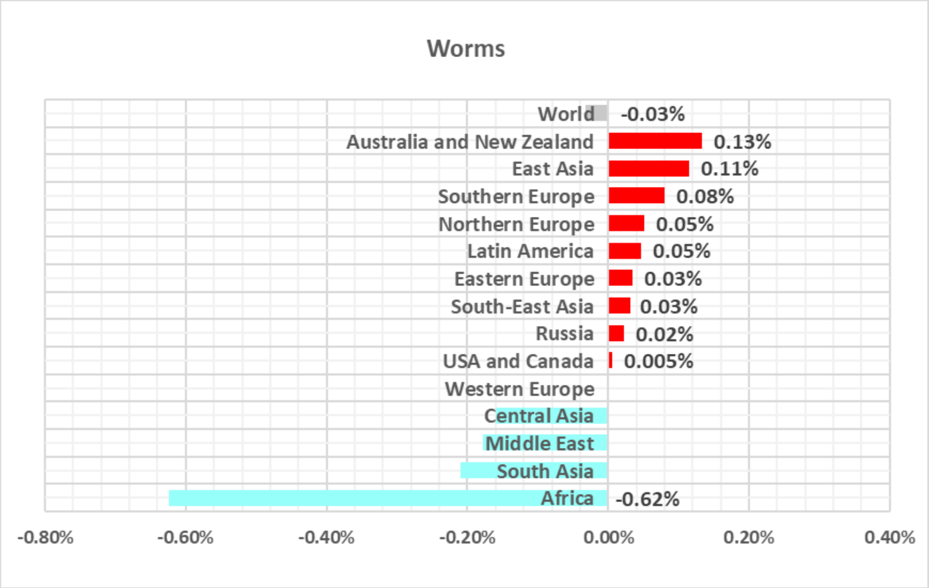


Globally, worms are in sixth place in the threat category ranking by percentage of ICS computers on which they were blocked. In similar regional rankings, **worms rank higher** in the following regions:

- Africa, Central Asia, South Asia – fourth place in the respective regional ranking
- East Asia, the Middle East, Latin America, Russia, Eastern Europe, Western Europe, Southern Europe – fifth place in the respective regional ranking

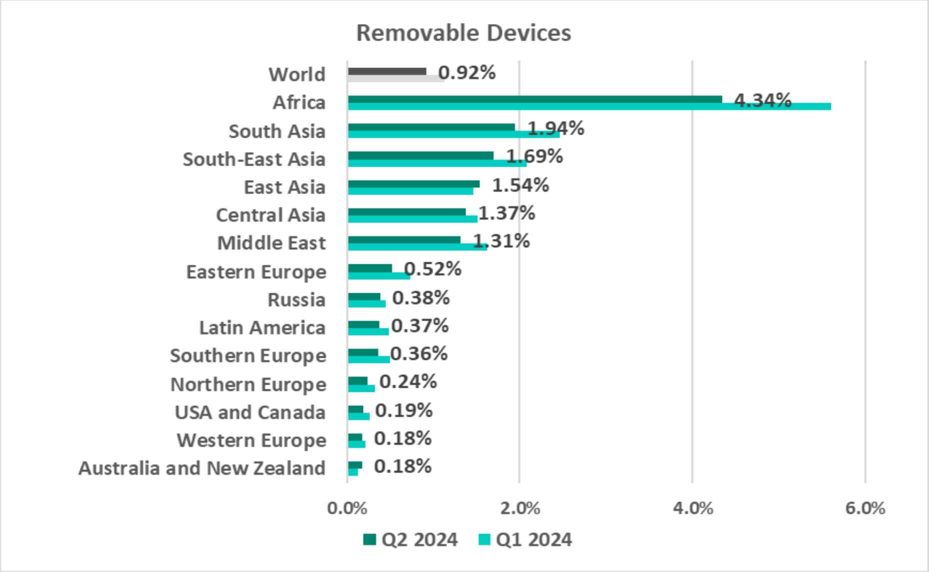
The top three regions in terms of **growth** in the percentage of ICS computers on which worms were blocked were Australia and New Zealand, East Asia, and Southern Europe.

Changes in the percentage of ICS computers on which worms were blocked, Q2 2024



The top regions for worms were also the leading regions by percentage of ICS computers on which threats were blocked when connecting **removable media**: Africa, South Asia, South-East Asia, East Asia, Central Asia, Middle East.

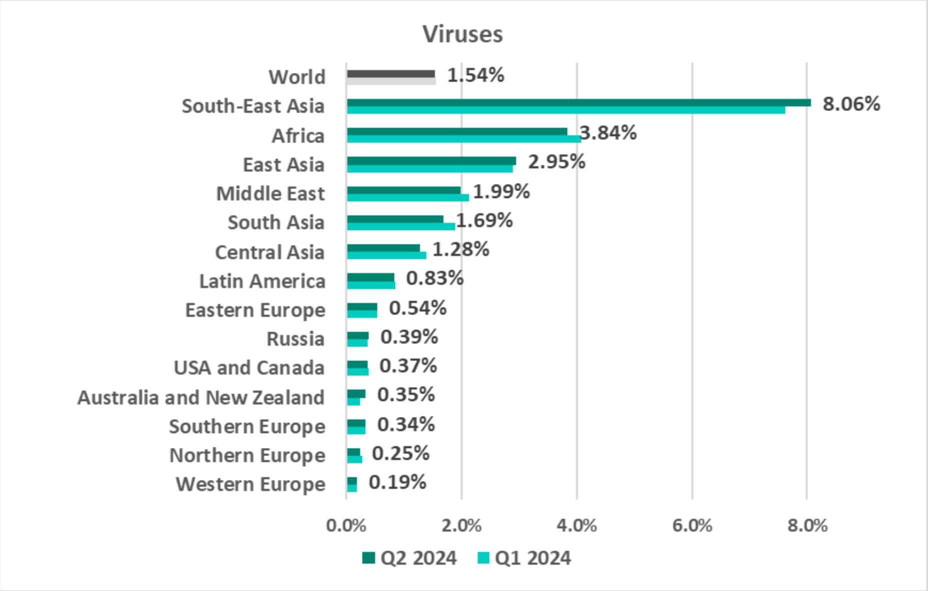
Regions ranked by percentage of ICS computers on which threats from removable devices were blocked, Q2 2024



Viruses

The leading regions by percentage of ICS computers on which viruses were blocked (above the global average of 1.54%) were **South-East Asia**, **Africa**, **East Asia**, **the Middle East**, **South Asia**.

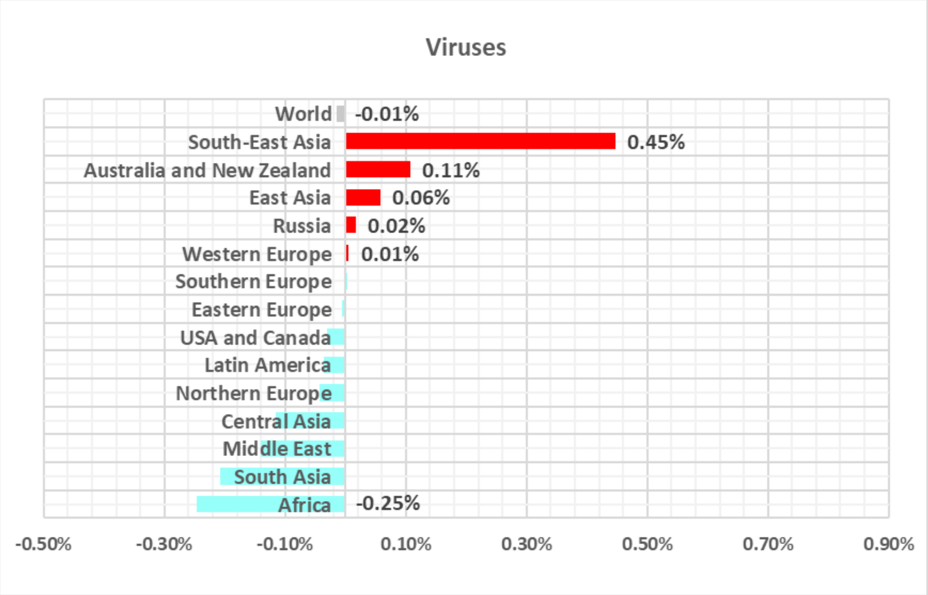
Regions ranked by percentage of ICS computers on which viruses were blocked, Q2 2024



In South-East Asia, viruses are in first place (!) in the threat category ranking by percentage of ICS computers on which they were blocked.

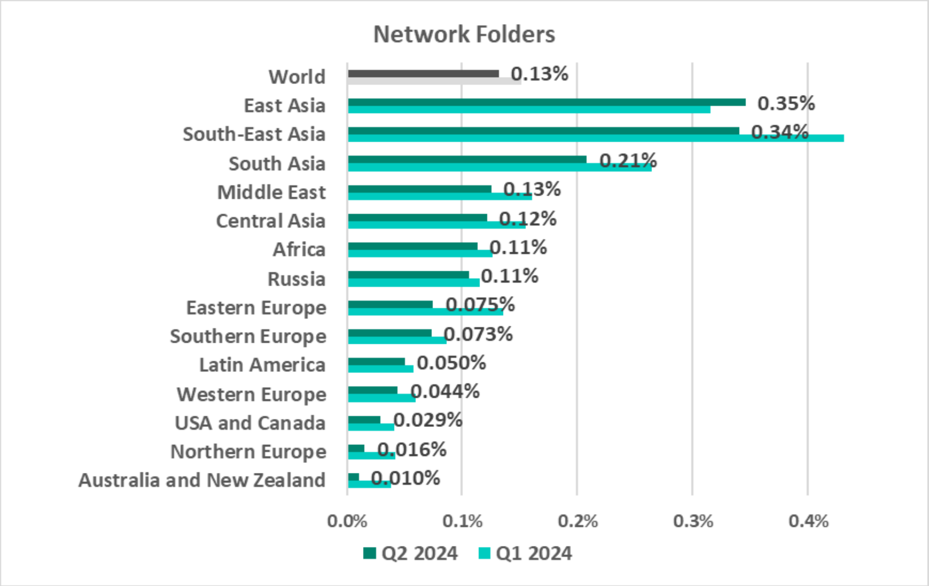
The top three regions in terms of **growth** in the percentage of ICS computers on which viruses were blocked were South-East Asia, Australia and New Zealand, and East Asia.

Changes in the percentage of ICS computers on which viruses were blocked, Q2 2024



Note that four of the top regions are also leaders by percentage of ICS computers on which **network folder threats** were blocked: East Asia, South-East Asia, South Asia, Middle East.

Regions ranked by percentage of ICS computers on which threats from network folderswere blocked, Q2 2024

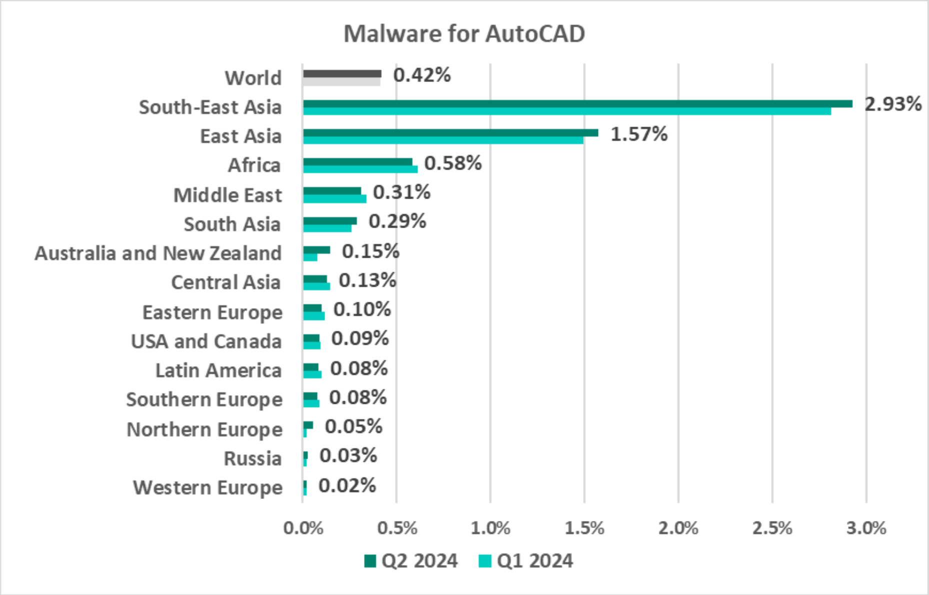


AutoCAD malware

This category of malware can spread in a variety of ways, so it does not belong to a specific group.

The same regions that lead in the virus ranking are also the leaders by percentage of ICS computers on which AutoCAD malware was blocked (above the global average of 0.42%): **South-East Asia**, **East Asia**, and **Africa**.

Regions ranked by percentage of ICS computers on which malware for AutoCAD was blocked, Q2 2024

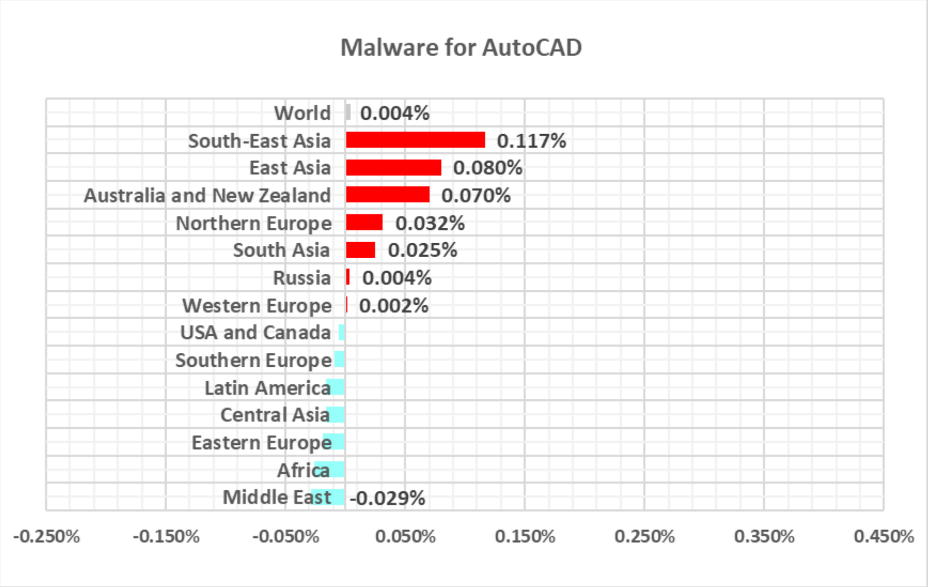


Normally, AutoCAD malware is a minor threat and usually comes bottom of the malware category rankings by percentage of ICS computers on which it was blocked.

However, in Q2 2024, this category ranked higher than the corresponding global ranking (ninth place) in the following regions:

- South-East Asia – fifth place in the regional ranking
- East Asia – seventh place in the regional ranking

The top three regions in terms of **growth** in the percentage of ICS computers on which malware for AutoCAD was blocked were South-East Asia, East Asia, and Australia and New Zealand.



Changes in the percentage of ICS computers on which malware for AutoCAD was blocked, Q2 2024

Regions. Special considerations

To see the specific distinctions of regions, you can compare them to other regions and to the global average statistics.

In most regions as well as globally, first place in the rankings by percentage of ICS computers on which specific threat categories were blocked are occupied by spyware and by the malicious objects used for the initial infection of computers. The internet leads the ranking of top threat sources in all regions.

Some of the regional rankings have their own peculiarities and distinctions, which are noted below.

Africa

Current threats

-1-

Denylisted internet resources

7.35%

▼ decrease in Q2
1.1x above global average
3rd in the world

-2-

Spyware

7.14%

▲ **1.1x** increase in Q2
1.8x above global average
1st in the world

-3-

Malicious scripts and phishing pages

5.87%

▼ decrease in Q2
slightly above global average

Worms

4.67%

▼ decrease in Q2
3.2x above global average
1st in the world

Viruses

3.84%

▼ decrease in Q2
2.5x above global average
2nd in the world

Executable miners

1.06%

▲ **1.1x** increase in Q2
1.2x above global average
3rd in the world
2nd in the world in terms of growth

Web miners

0.83%

▼ decrease in Q2
1.7x above global average
1st in the world

Ransomware

0.25%

▼ decrease in Q2
1.4x above global average
2nd in the world

Threats from
Internet

11.85%
▼ decrease in Q2

1.1x above global average
4th in the world

Threats from
Removable devices

4.34%
▼ decrease in Q2

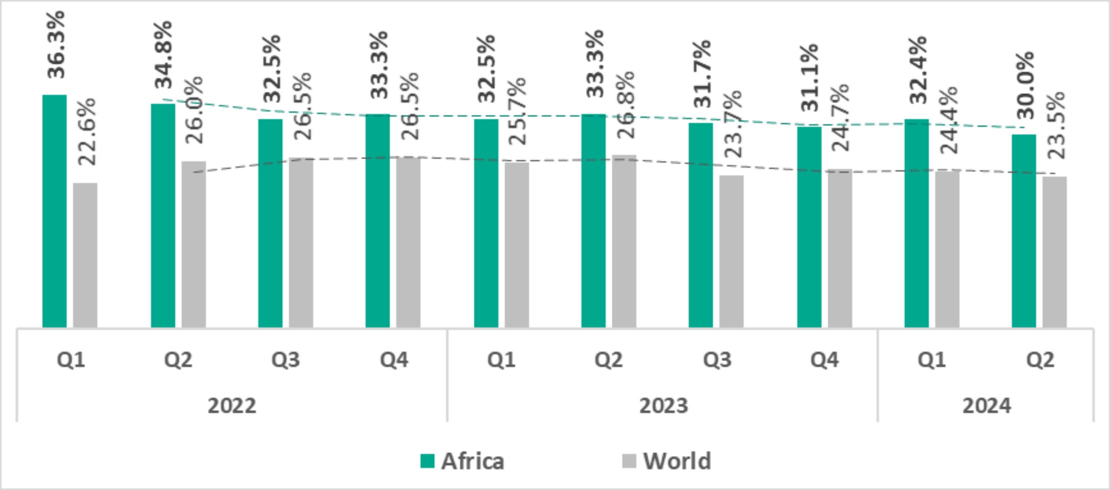
4.7x above global average
above **email threats**
1st in the world

Overall

First place in the global ranking by percentage of ICS computers on which malicious objects were blocked.

Of all regions, Africa traditionally has the highest percentage of ICS computers on which malicious objects were blocked. Therefore, it is not surprising that Africa leads in many rankings, in some cases by a huge margin.

The percentage of ICS computers on which malicious objects were blocked is higher than the global average. The region exhibits a slight downward trend with fluctuations.



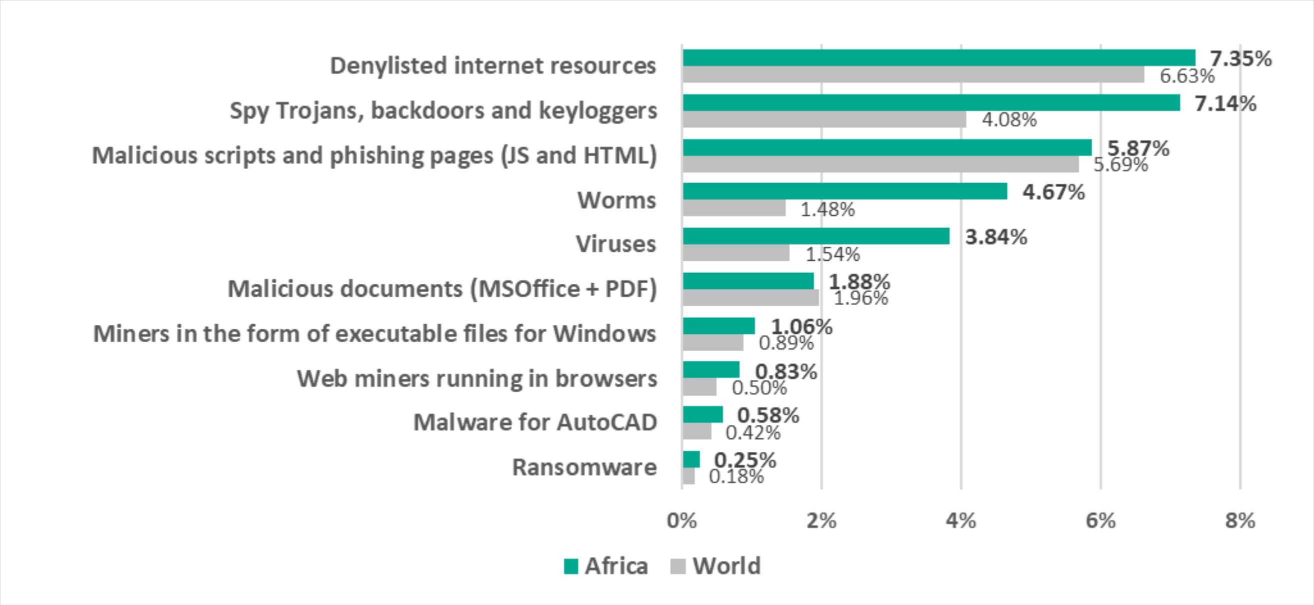
Comparative analysis

Africa occupies **leading positions** among regions by percentage of ICS computers on which the following were blocked:

- First place: spyware, web miners, worms, threats from removable media
- Second place: ransomware, viruses
- Third place: denylisted internet resources, miners in the form of executable files for Windows, malware for AutoCAD

Threat categories

- **Compared to global figures**, the region has a higher percentage of ICS computers on which threats were blocked across all threat categories except for malicious documents.



- The region has a significantly higher percentage than the respective global average percentages of ICS computers on which the following were blocked:
  - Worms, 3.2 times higher
  - Viruses, 2.5 times higher

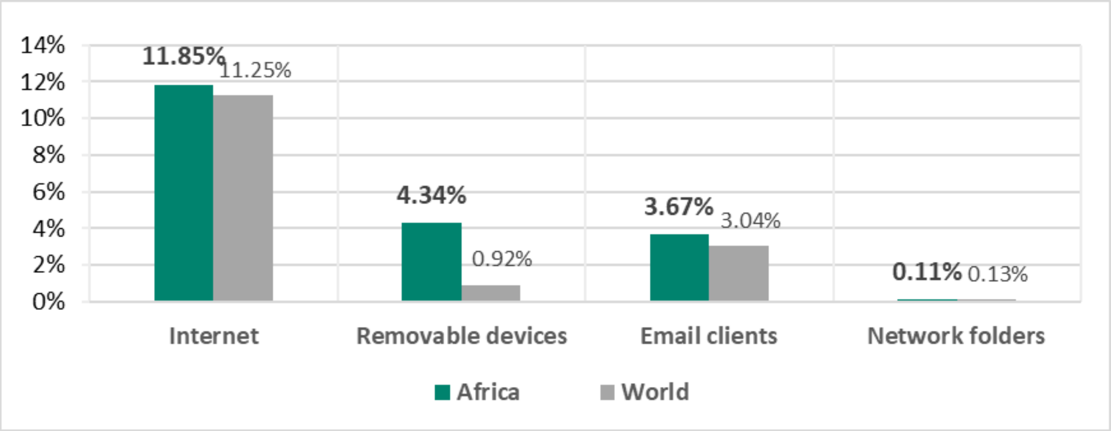
  Worms and viruses outpace malicious documents in the threat category ranking by percentage of ICS computers on which they were blocked. Worms are in fourth place (sixth place globally). As noted earlier, high rates of self-propagating malware on a large scale indicate that a significant portion of the OT infrastructure lacks even basic endpoint protection, making it a source of malware infection attempts.

  - Spyware, 1.7 times higher
  - Web miners, 1.7 times higher
  - Malware for AutoCAD, 1.4 times higher
  - Ransomware, 1.4 times higher

Threat sources

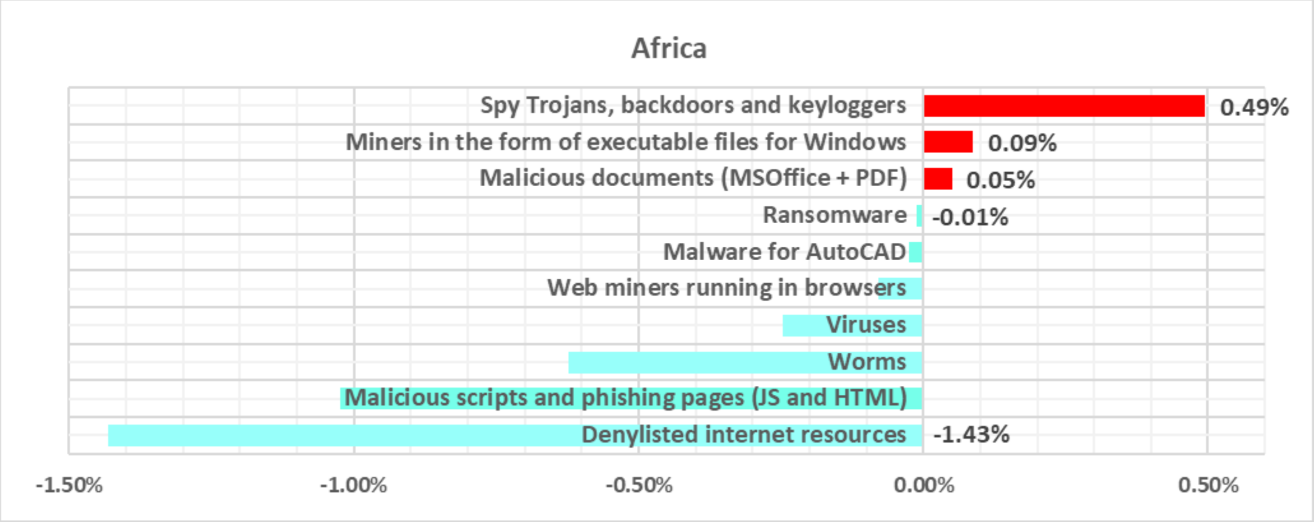
Removable drives occupy second place in the regional ranking of threat sources by percentage of ICS computers on which malicious objects from different sources were blocked (third place globally).

Africa is the only region this quarter where a higher percentage of ICS computers had threats blocked from removable media than from email threats. This appears to be a long-term trend. We assume this might indicate that OT systems in the region are generally not frequently connected to corporate resources, including email services. Instead, removable media is often used for information exchange in OT infrastructure.



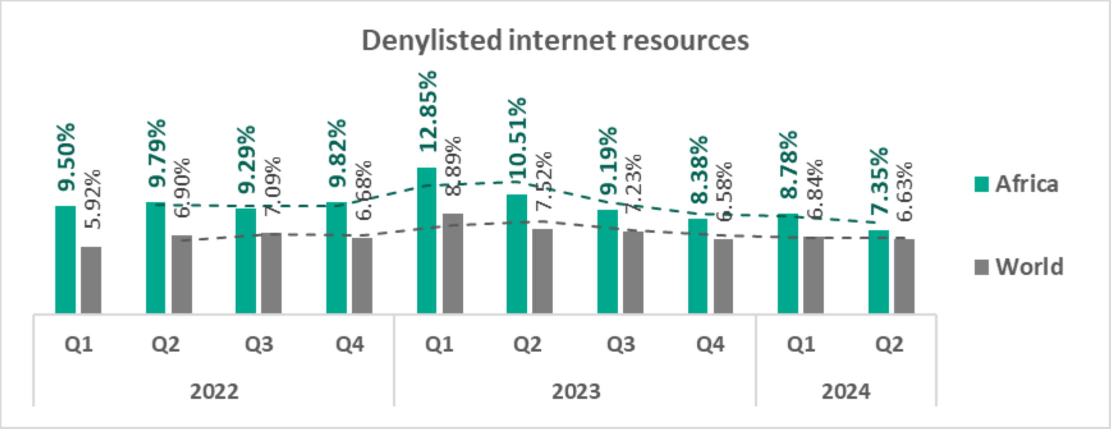
Quarterly changes and trends

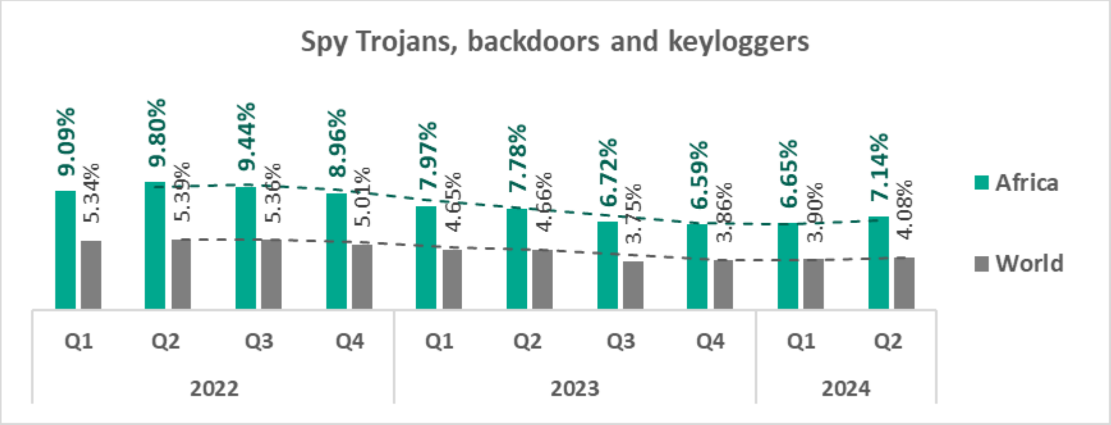
Threat categories

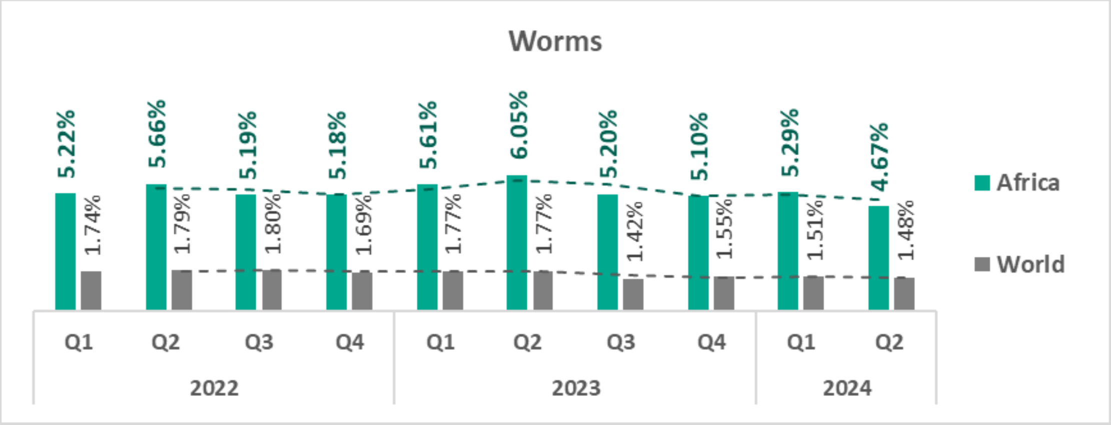


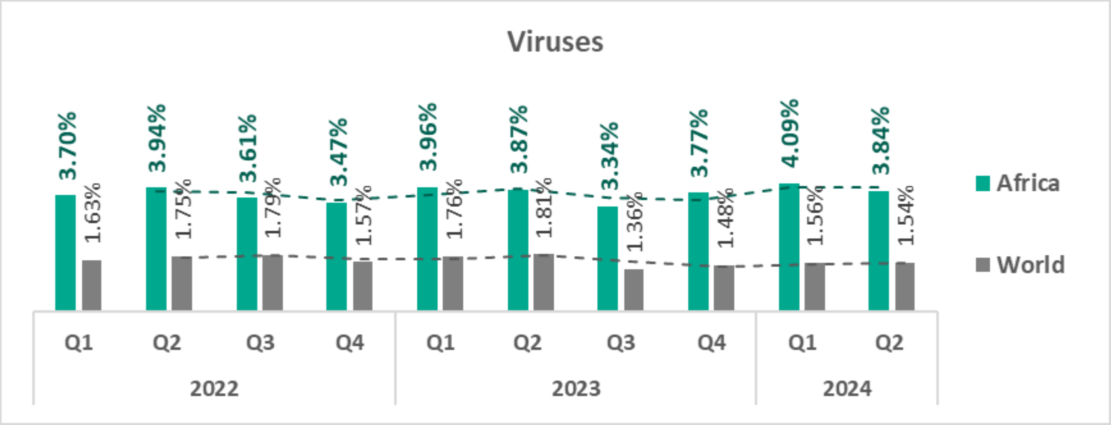
- The **largest proportional quarterly increase** in Q2 2024 was in the percentage of ICS computers on which the following were blocked:
  - ➢ Spyware – by 1.1 times, rising to second place in the region from third
  - ➢ Miners in the form of executable files for Windows – by 1.1 times

- The **top threat** categories exhibit various quarterly dynamics:

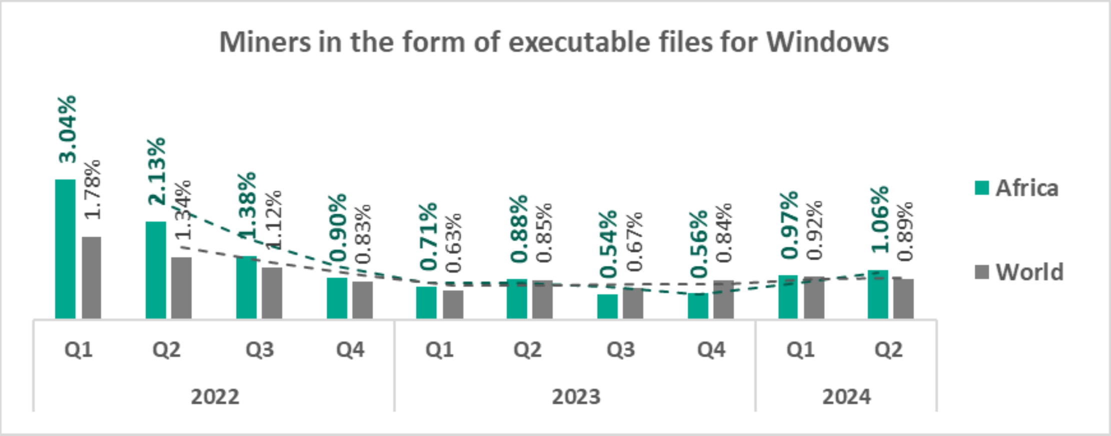




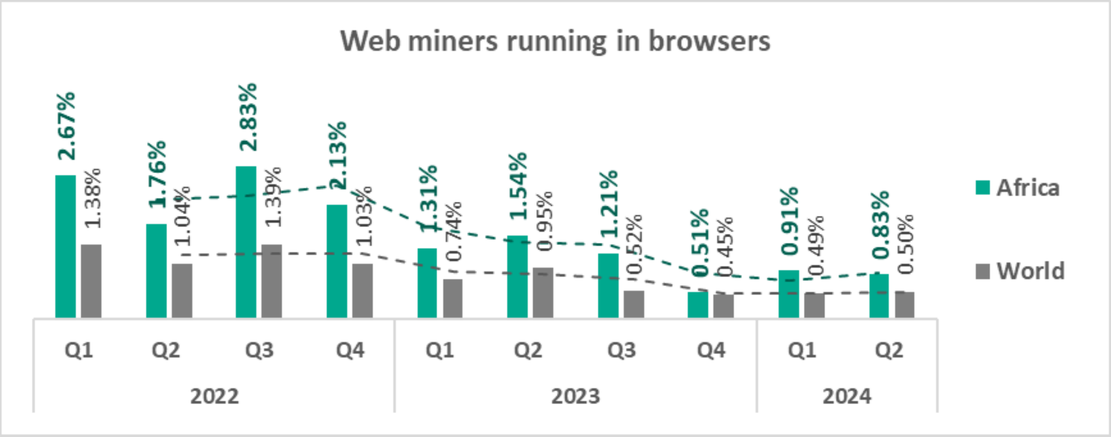




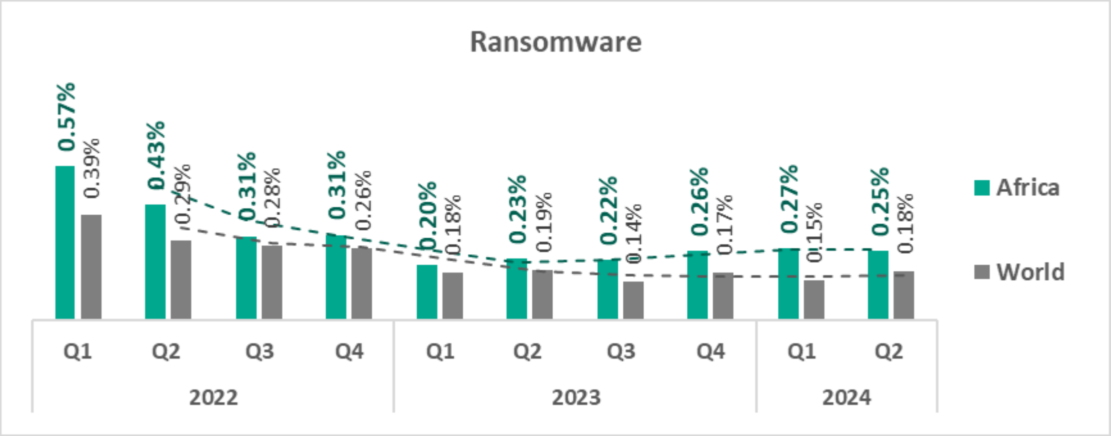
Viruses



Miners in the form of executable files for Windows



Web miners running in browsers

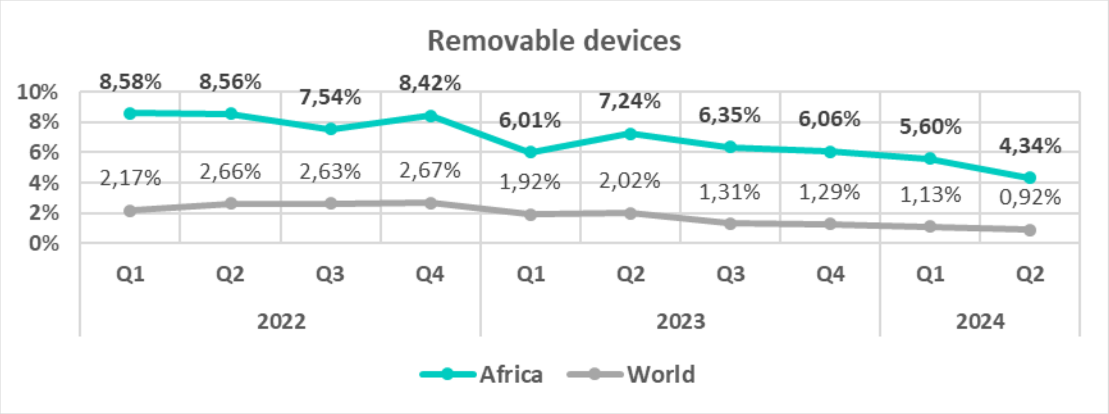


- The heatmap below illustrates changes in the ranking of threat categories in the region over a period of 2.5 years. **Denylisted internet resources** have been the leading threat category in the region since early 2023. **Spyware** moved up from third to second place in Q2 2024, while **malicious scripts and phishing** gradually dropped from first place in 2022 to third in Q2 2024.

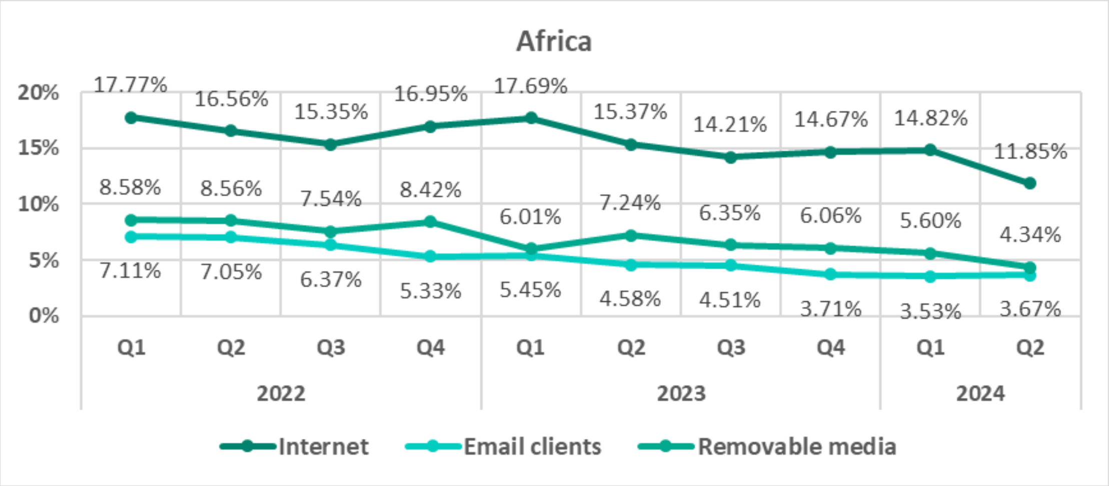
Africa	2022				2023				2024	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Denylisted internet resources	2	3	3	2	1	1	1	1	1	1
Spy Trojans, backdoors and keyloggers	3	2	2	3	3	3	3	3	3	2
Malicious scripts and phishing pages (JS and HTML)	1	1	1	1	2	2	2	2	2	3
Worms	4	5	4	4	4	4	4	4	4	4
Viruses	6	6	6	6	5	5	5	5	5	5
Malicious documents (MSOffice + PDF)	5	4	5	5	6	6	6	6	6	6
Miners in the form of executable files for Windows	7	7	8	8	8	8	8	7	7	7
Web miners running in browsers	8	8	7	7	7	7	7	8	8	8
Malware for AutoCAD	10	9	9	9	9	9	9	9	9	9
Ransomware	9	10	10	10	10	10	10	10	10	10

Threat sources

- **Removable devices** have been above the global average by a wide margin since Q2 2022 and exhibit a downward trend closely following the global trend.



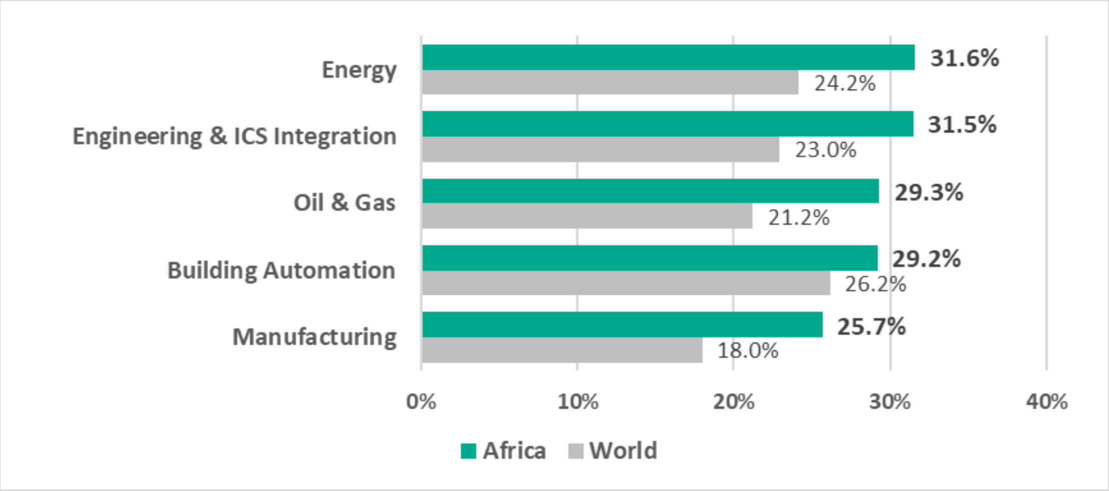
- In terms of **quarterly changes**, all threat sources exhibit mostly downward trends.



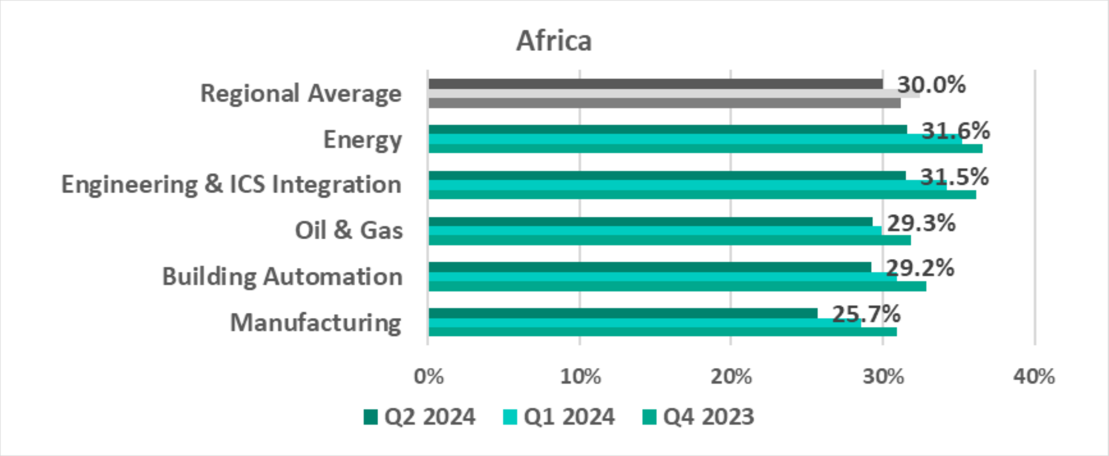
Industries

- The **most affected** industries in the region, as selected for this report, are:
  - ➢ Energy
  - ➢ Engineering and ICS Integration

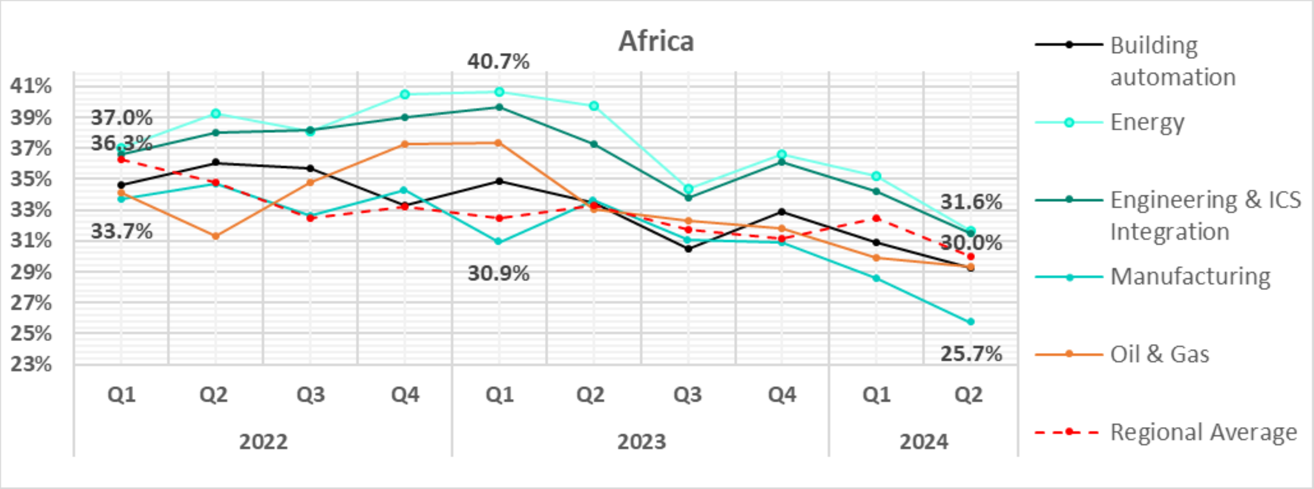
- Compared to the **global averages**, the following industries had a significantly higher percentage of ICS computers with blocked malicious objects compared to the respective global averages:
  - Manufacturing – 1.4 times higher
  - Engineering and ICS Integration – 1.4 times higher
  - Oil & Gas – 1.4 times higher
  - Energy – 1.3 times higher



- In **Q2 2024**, all selected sectors in the region exhibited a decrease in the percentage of ICS computers on which malicious objects were blocked.



- The selected sectors show positive dynamics in their **long-term trends**:



South-East Asia

Current threats

-1-

Viruses
8.06%

▲ **1.1x** increase in Q2
5.2x above global average
1st in the world

-2-

Malicious scripts and phishing pages
6.77%

▲ slight increase in Q2
1.2x above global average
3rd in the world

-3-

Denylisted internet resources
6.07%

▼ decrease in Q2

Spyware
5.78%

▲**1.1x** increase in Q2
1.4x above global average

Malware for AutoCAD
2.93%

▲ slight increase in Q2
7x above global average
1st in the world

Malicious documents
2.76%

▲ **1.2x** increase in Q2
1.4x above global average
3rd in the world

Ransomware
0.25%

▼ decrease in Q2
1.2x above global average
3rd in the world

Threats from
Internet
12.10%

▼ decrease in Q2
1.1x above global average
2nd in the world

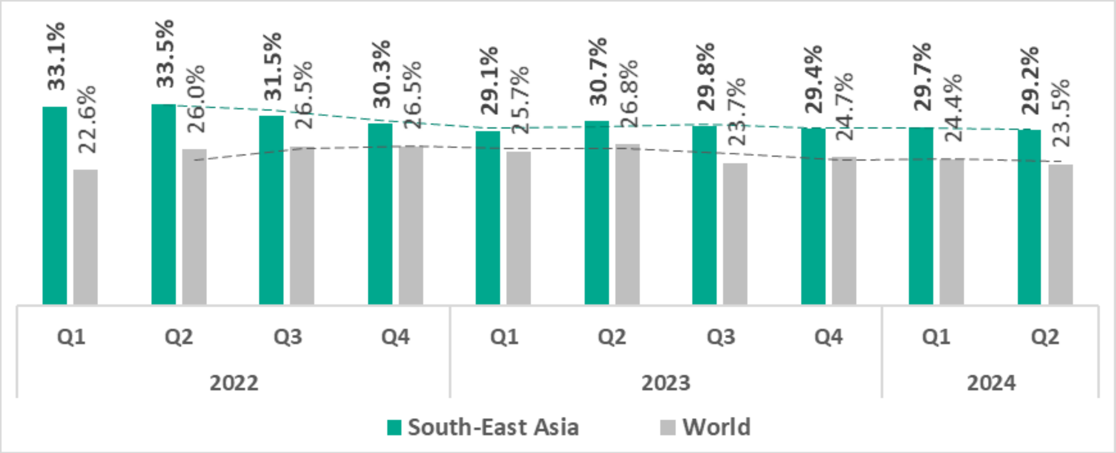
Threats from
Network folders
0.34%

▼ decrease in Q2
2.6x above global average
2nd in the world

Overall

Second place in the global ranking by percentage of ICS computers on which malicious objects were blocked.

The percentage of ICS computers where malicious objects were blocked remains consistently higher than the global average, reflecting a long-term trend. While the region shows a slight downward trend, this pattern includes periodic fluctuations.



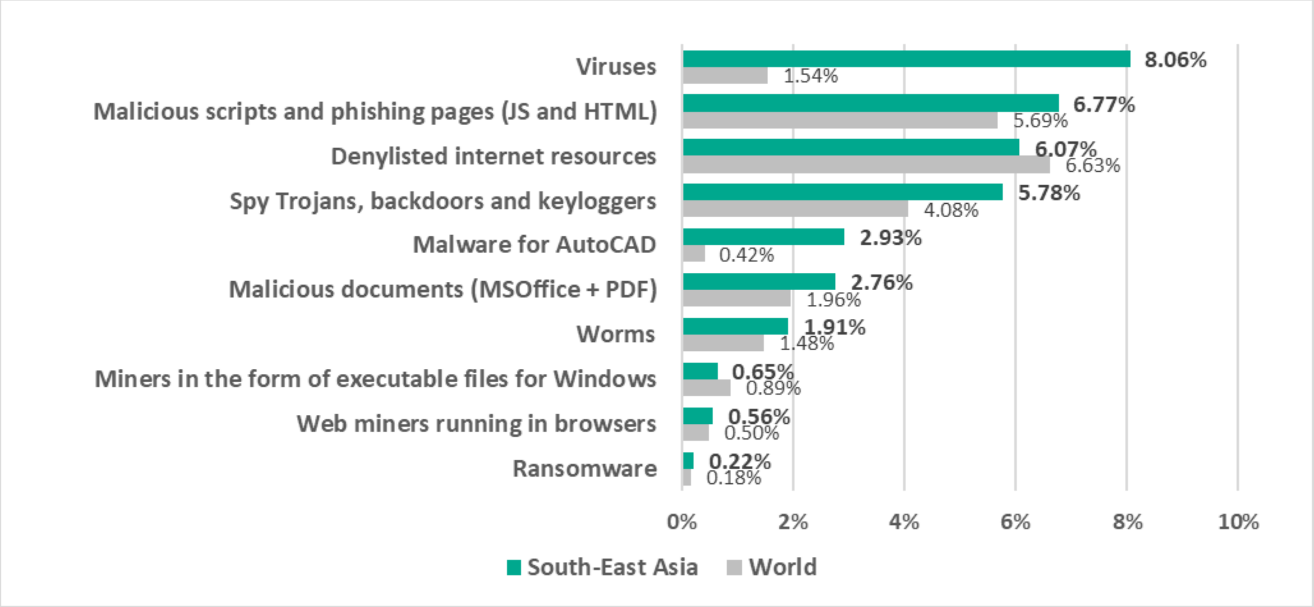
Comparative analysis

South-East Asia occupies **leading positions** among regions by percentage of ICS computers on which the following were blocked:

- First place: viruses, malware for AutoCAD
- Second place: threats from the internet, threats from network folders
- Third place: malicious scripts and phishing pages, malicious documents, ransomware

Threat categories

Viruses came first in the ranking of malware categories by percentage of ICS computers on which they were blocked. In South-East Asia, this percentage is 5.2 times higher than the global average.



AutoCAD malware is in fifth place in this ranking (the global percentage of ICS computers on which this malware was blocked is one of the lowest among all categories).

Compared to the global figures, the region has a significantly higher percentage of ICS computers on which the following were blocked:

- AutoCAD malware, 7 times higher
- Viruses, 5.2 times higher
- Spyware, 1.4 times higher
- Malicious documents, 1.4 times higher
- Worms, 1.3 times higher
- Ransomware, 1.2 times higher
- Malicious scripts and phishing pages, 1.2 times higher

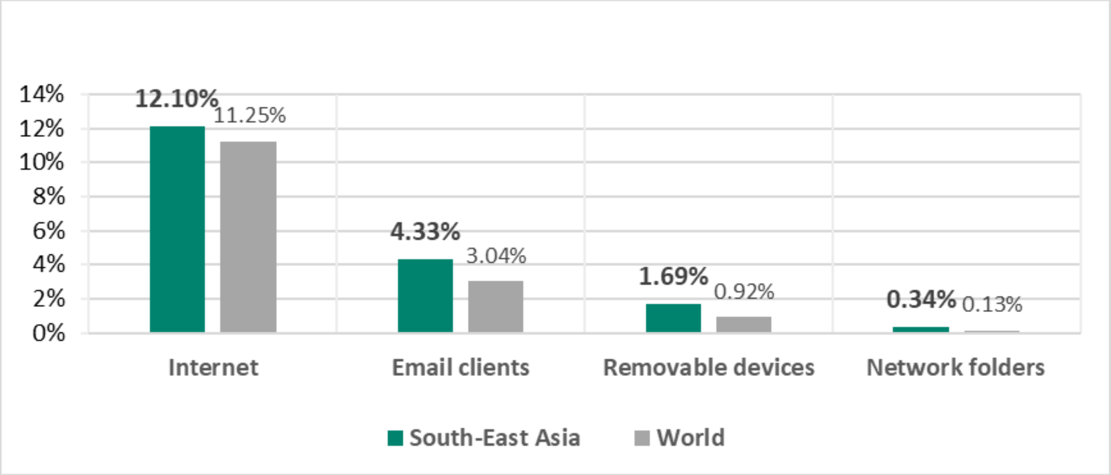
Threat sources

The region ranked first in the world by percentage of ICS computers on which threats from **network folders** were blocked, exceeding the global average by 2.6 times.

With regard to threats from the **internet**, the region ranked second in the world, slightly exceeding the global average.

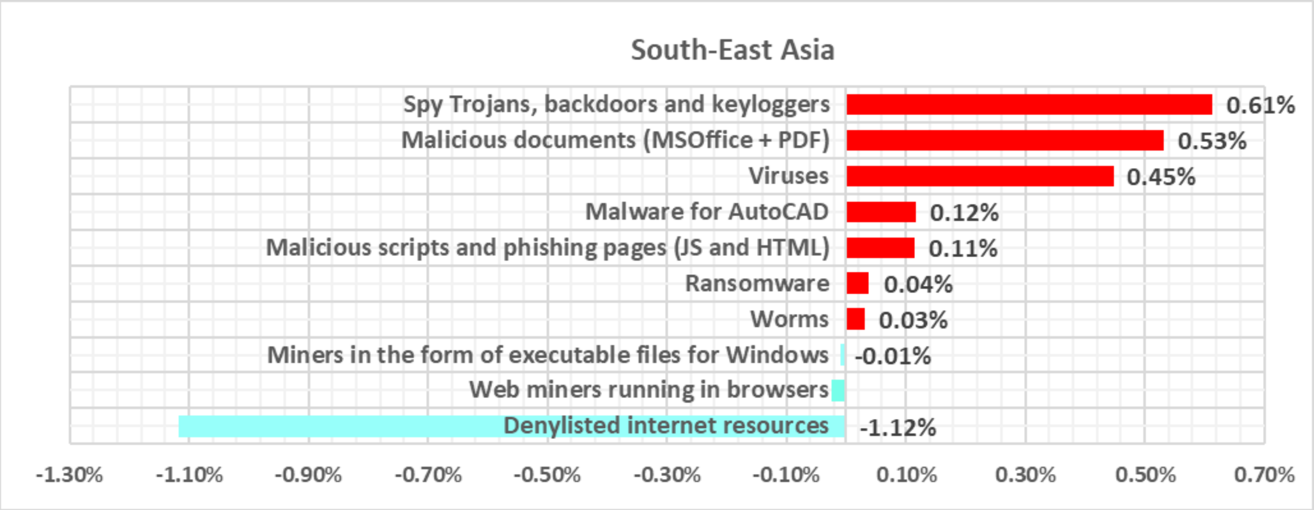
The region ranked third in the world by percentage of ICS computers on which malicious threats from **removable devices** were blocked, exceeding the global average by 1.8 times.

The percentage of computers on which threats from **email clients** were blocked exceeded the global average by 1.4 times in Q2 2024.



Quarterly changes and trends

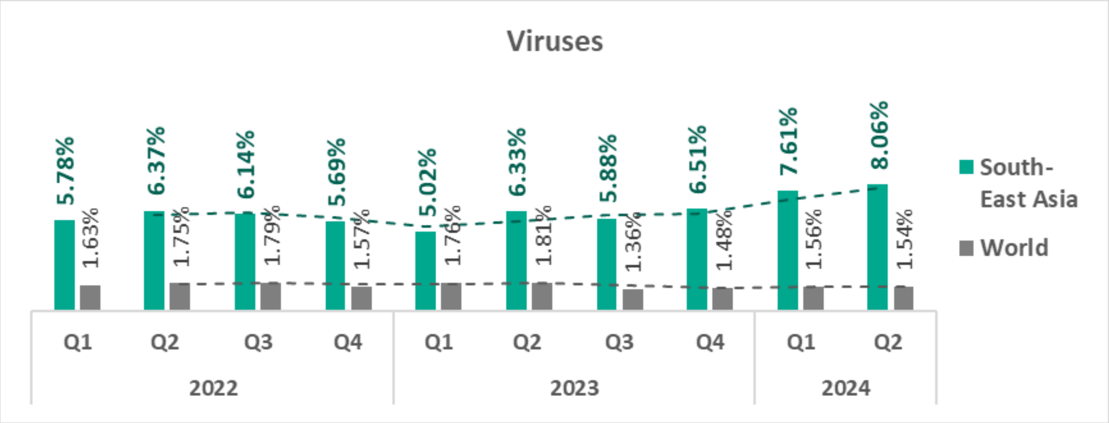
Threat categories

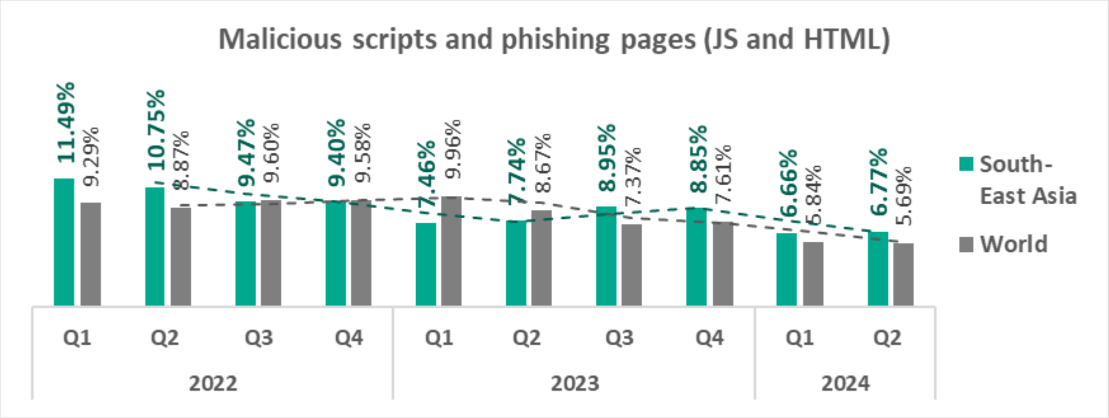


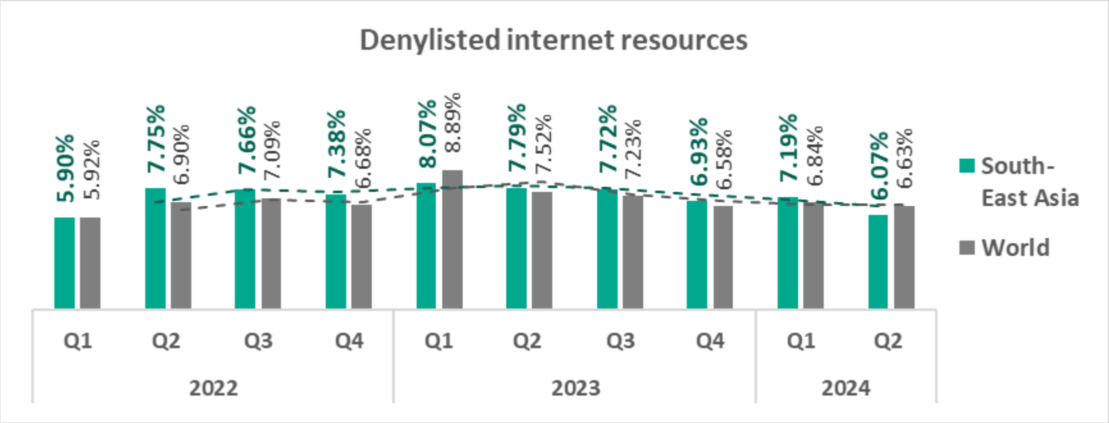
The **largest quarterly increase** was in the percentage of ICS computers on which the following were blocked:

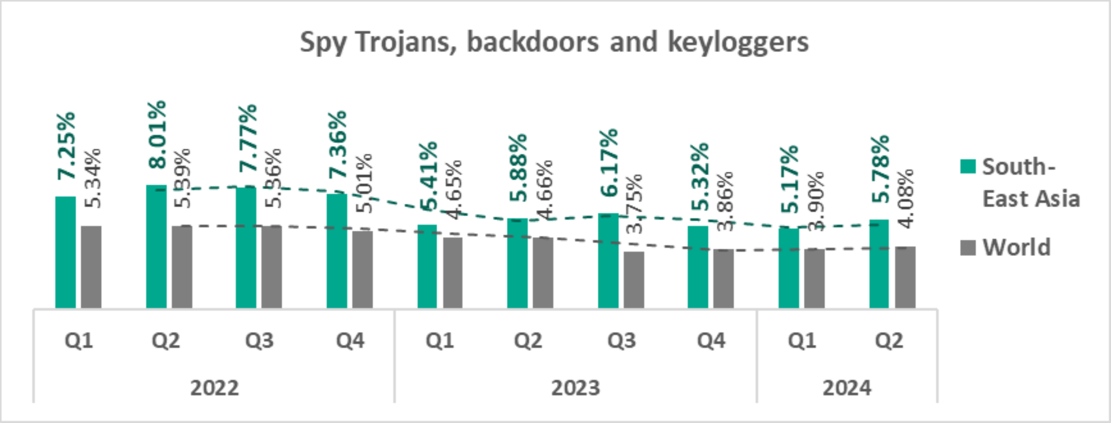
- Malicious documents – by 1.2 times
- Ransomware – by 1.2 times

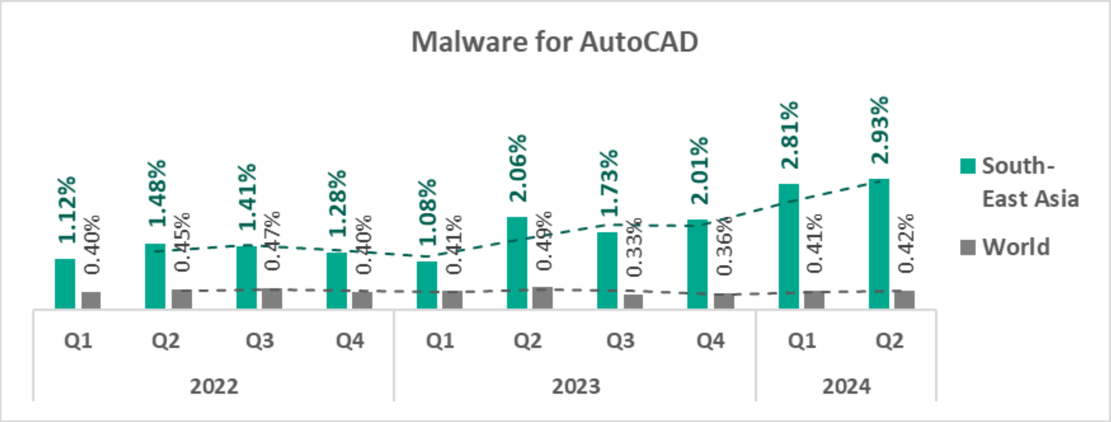
- The **top threat** categories exhibit various quarterly dynamics:

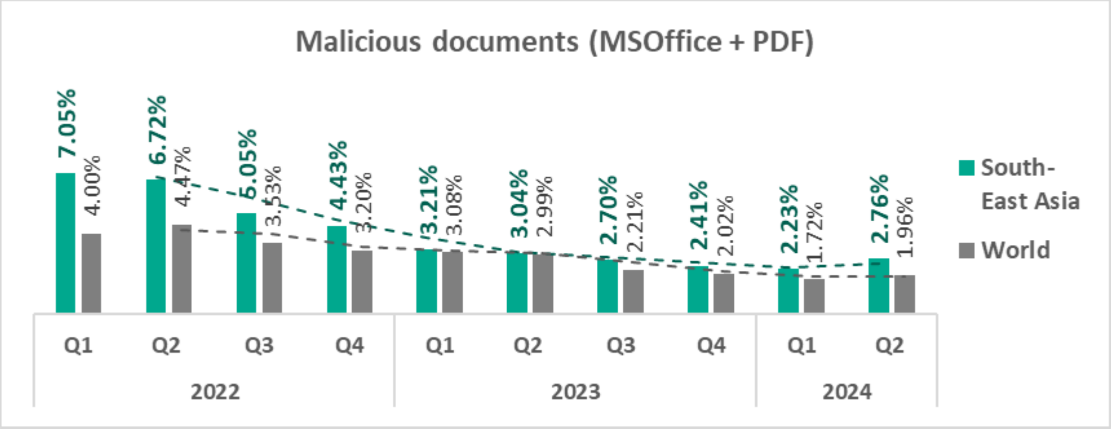


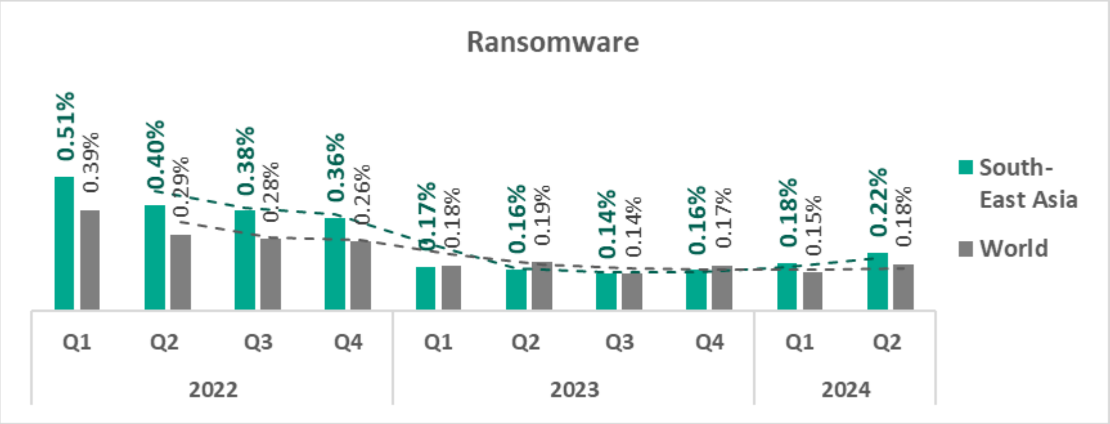





Spy Trojans, backdoors and keyloggers
7.25%
5.34%
8.01%
5.39%
7.77%
5.36%
7.36%
5.01%
5.41%
4.65%
5.88%
4.66%
6.17%
3.75%
5.32%
3.86%
5.17%
3.90%
5.78%
4.08%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
South-East Asia
World


Malware for AutoCAD
1.12%
0.40%
1.48%
0.45%
1.41%
0.47%
1.28%
0.40%
1.08%
0.41%
2.06%
0.49%
1.73%
0.33%
2.01%
0.36%
2.81%
0.41%
2.93%
0.42%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
South-East Asia
World


Malicious documents (MSOffice + PDF)
7.05%
4.00%
6.72%
4.47%
6.05%
3.53%
4.43%
3.20%
3.21%
3.08%
3.04%
2.99%
2.70%
2.21%
2.41%
2.02%
2.23%
1.72%
2.76%
1.96%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
South-East Asia
World

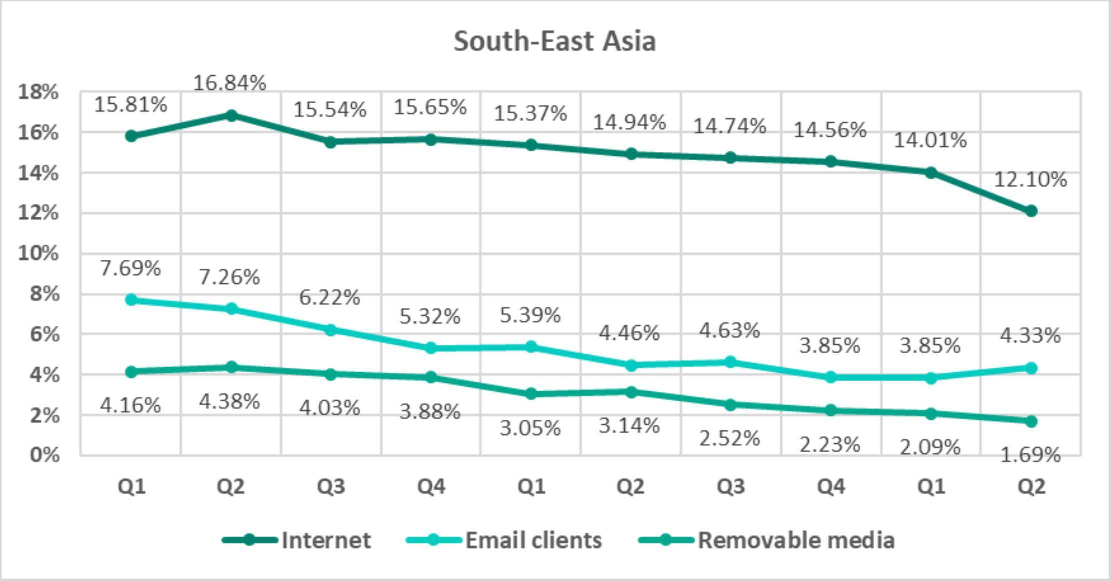


- The heatmap below illustrates changes in the rankings of threat categories in the region over a period of 2.5 years. **Viruses** have been the leading threat category in the region since Q1 2024. **Malicious scripts and phishing** moved up from third to second place in Q2 2024, while **denylisted internet resources** dropped from first place in the first half of 2023 to third in Q2 2024.

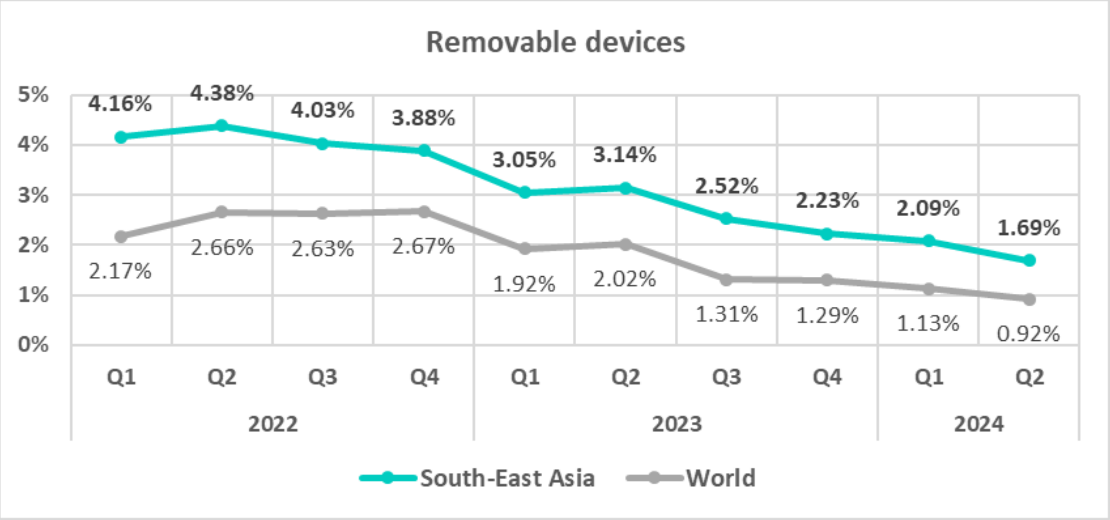
South-East Asia	2022				2023				2024	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Viruses	5	5	4	4	4	3	4	3	1	1
Malicious scripts and phishing pages (JS and HTML)	1	1	1	1	2	2	1	1	3	2
Denylisted internet resources	4	3	3	2	1	1	2	2	2	3
Spy Trojans, backdoors and keyloggers	2	2	2	3	3	4	3	4	4	4
Malware for AutoCAD	9	9	9	9	7	6	7	6	5	5
Malicious documents (MSOffice + PDF)	3	4	5	5	5	5	5	5	6	6
Worms	7	7	6	6	6	7	6	7	7	7
Miners in the form of executable files for Windows	6	6	8	8	9	9	9	9	8	8
Web miners running in browsers	8	8	7	7	8	8	8	8	9	9
Ransomware	10	10	10	10	10	10	10	10	10	10

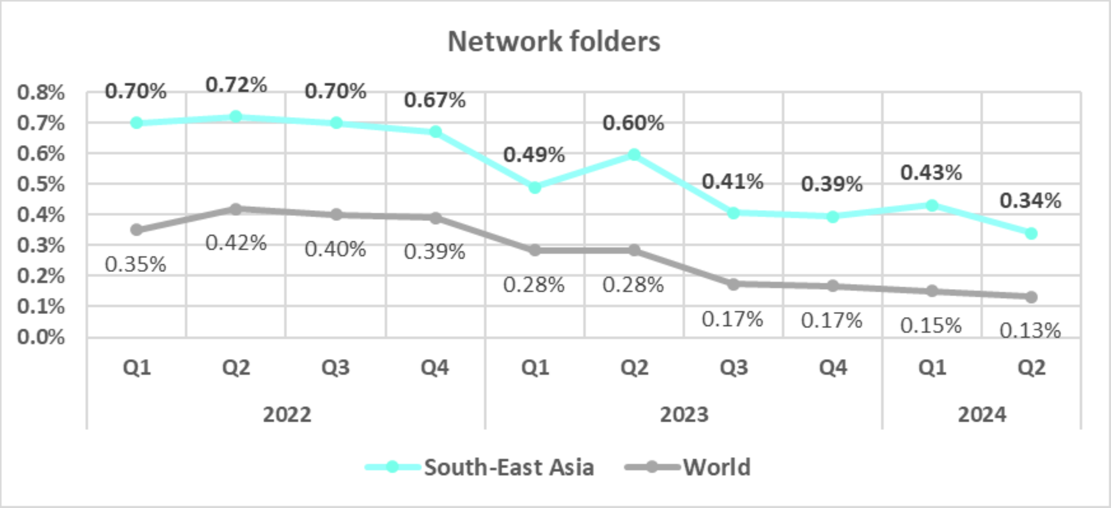
Threat sources

- Almost all threat sources except for email clients exhibited a decrease in terms of the percentage of ICS computers on which they were blocked. Threats from email clients increased by a factor of 1.1. In terms of **quarterly changes**, the major threat sources have shown mostly downward long-term trends.



Threats from **removable devices** and **network folders** are significantly above the respective global averages.



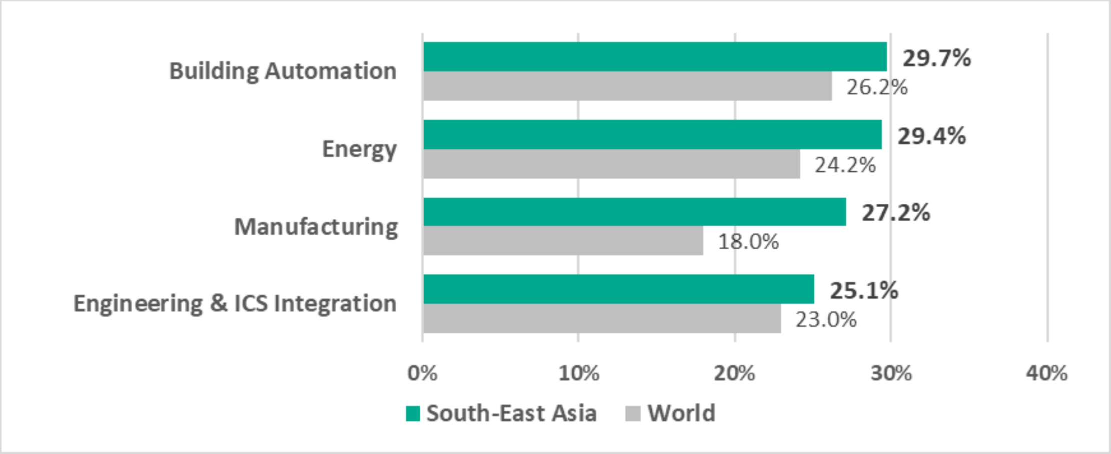


Industries

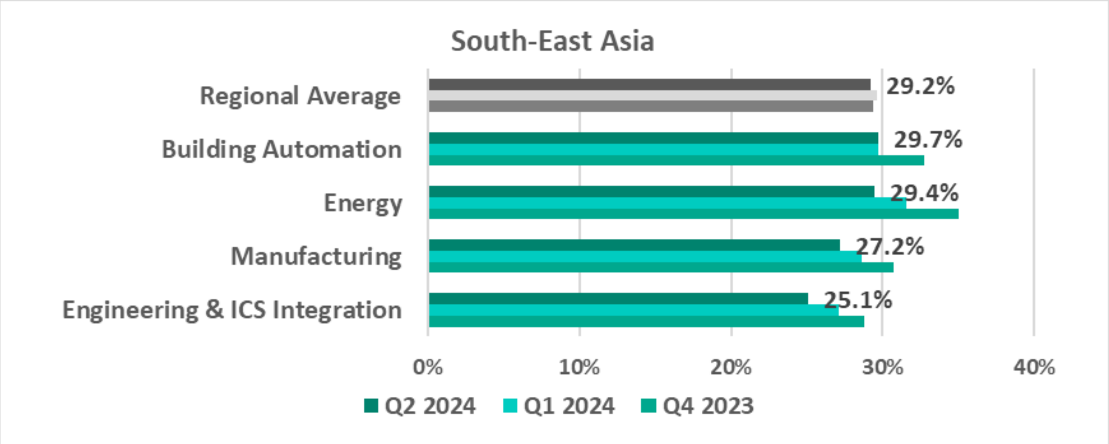
The **most affected** industries in the region, as selected for this report, are:

- Building automation
- Energy

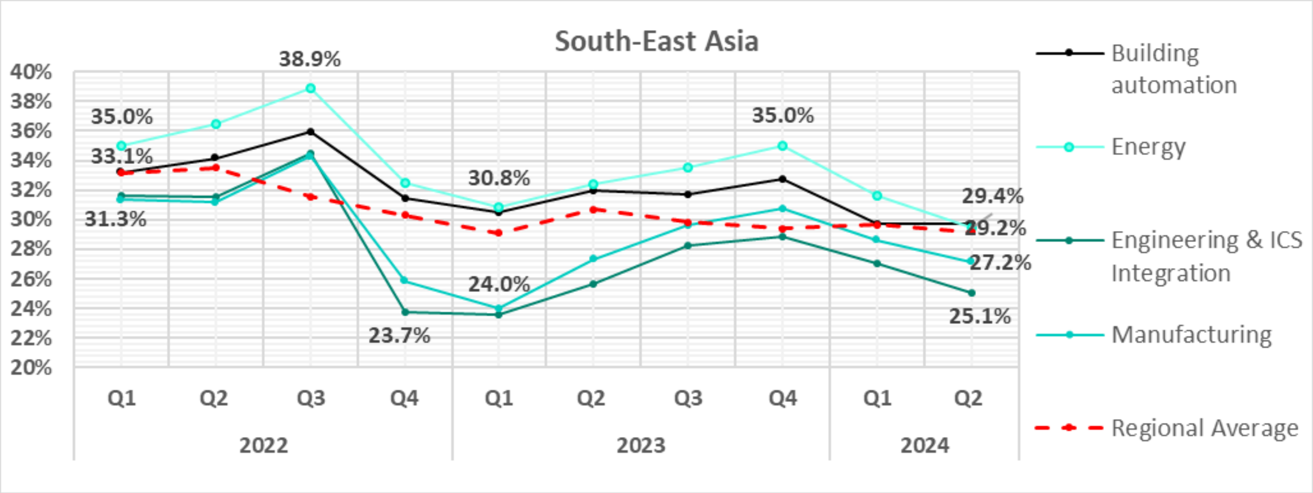
- **Compared to the global averages**, the following industries had a significantly higher percentage of ICS computers on which malicious objects were blocked:
  - Manufacturing – 1.5 times higher
  - Energy – 1.2 times higher



- In **Q2 2024**, all selected sectors experienced a decrease in the percentage of ICS computers where malicious objects were blocked, with the exception of building automation, which remained unchanged.



- The **trends** in the selected sectors demonstrate overall positive dynamics, though they are marked by steep jumps and extended periods of slow increases and declines.



Central Asia

Current threats

-1-

Denylisted internet resources
7.58%

▲ slight increase in Q2
1.1x above global average
2nd in the world

-2-

Spyware
4.80%

▲ **1.1x** increase in Q2
1.2x above global average

-3-

Malicious scripts and phishing pages
4.28%

▼ decrease in Q2

Worms
2.72%

▼ decrease in Q2
1.8x above global average
2nd in the world

Executable miners
1.62%

▼ decrease in Q2
1.8x above global average
1st in the world

Ransomware
0.19%

▲ **1.1x** increase in Q2
above global average

Threats from
Internet
12.33%

▲ **1.1x** increase in Q2
1.1x above global average
1st in the world
1st in the world **in terms of growth**

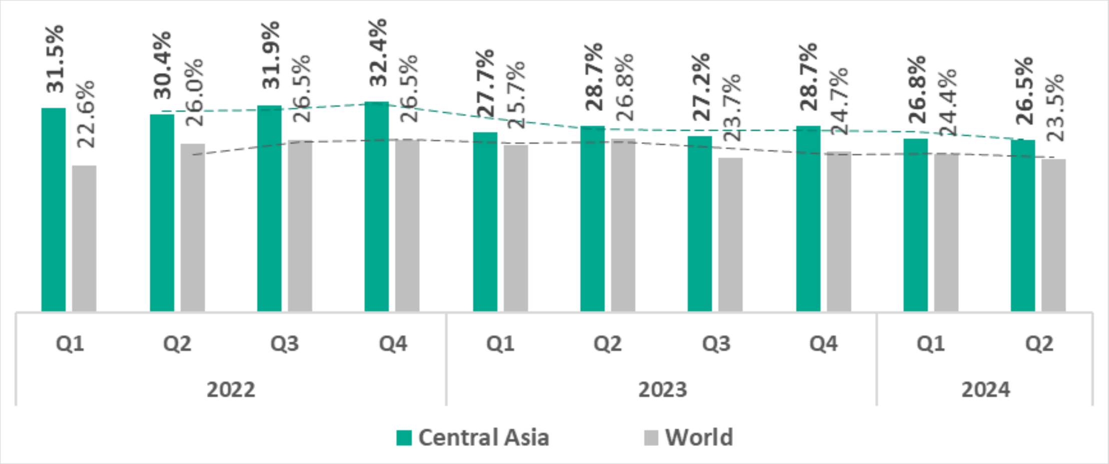
Threats from
Removable devices
1.37%

▼ decrease in Q2
1.5x above global average

Overall

Third place in the global ranking by percentage of ICS computers on which malicious objects were blocked.

The percentage of ICS computers where malicious objects were blocked remains higher than the global average, although the gap has tended to narrow since Q1 2023.

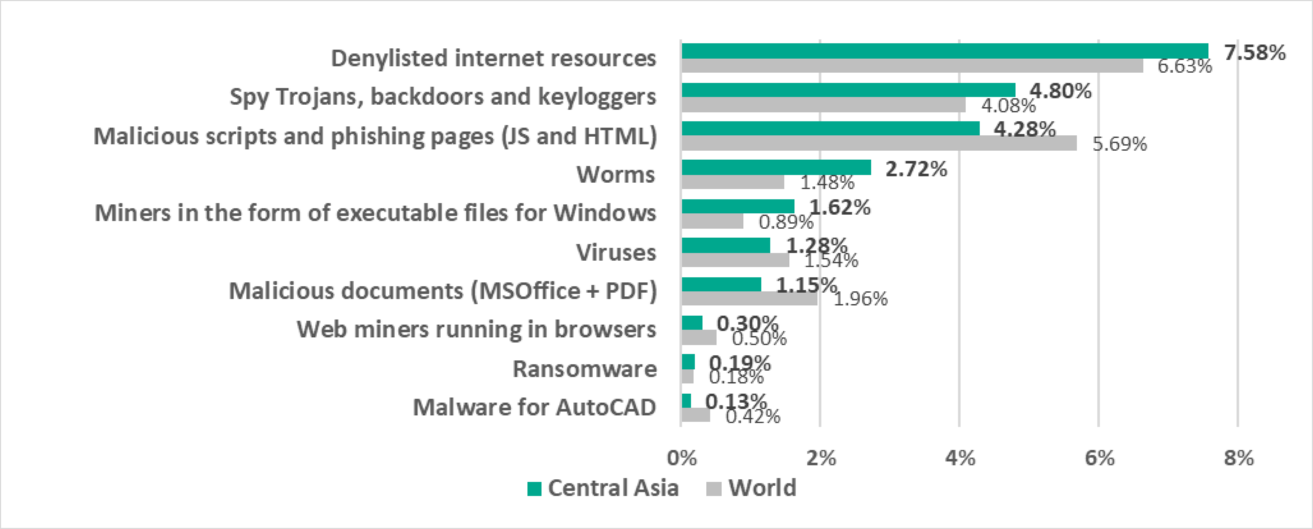


Comparative analysis

Central Asia occupies **leading positions** among regions by percentage of ICS computers on which the following were blocked:

- First place: threats from the internet, miner executable files for Windows
- Second place: denylisted internet resources, worms

Threat categories



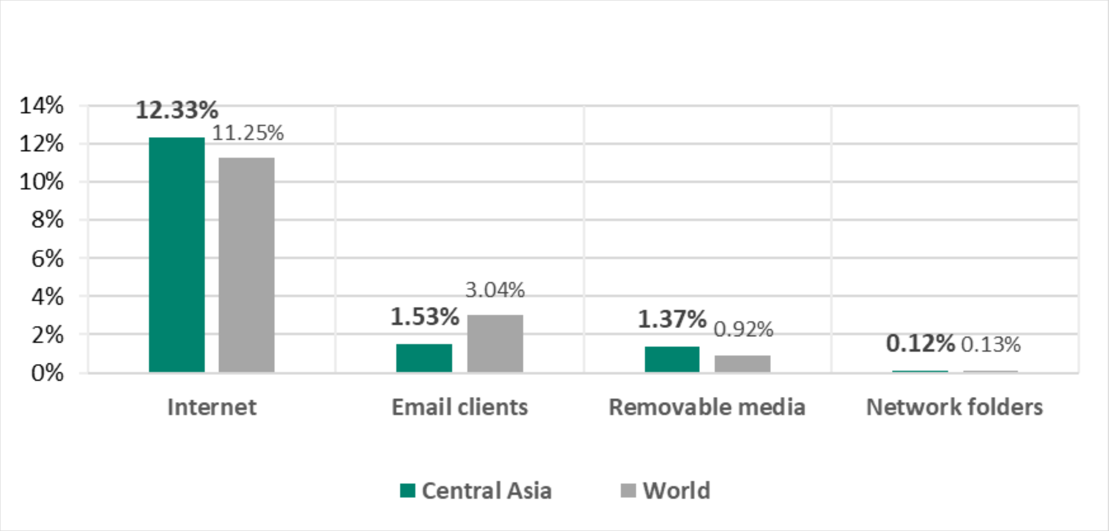
Compared to the global average, the region has a higher percentage of ICS computers on which the following were blocked:

- Worms, 1.8 times higher
- Miners in the form of executable files for Windows, 1.8 times higher. This threat category ranks fifth (seventh place globally).
- Spyware, 1.2 times higher
- Denylisted internet resources, 1.1 times higher

Threat sources

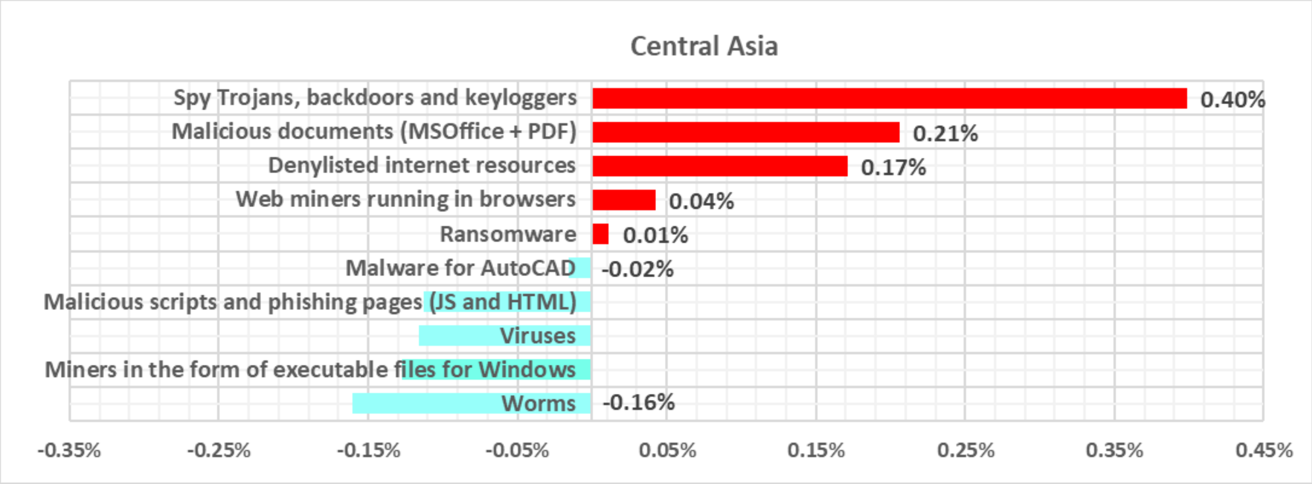
The region ranked first in the world by percentage of ICS computers on which threats from the **internet** were blocked, exceeding the global average by a factor of 1.1.

The percentage of ICS computers on which threats from **removable devices** were blocked exceeded the global average by 1.5 times in Q2 2024.



Quarterly changes and trends

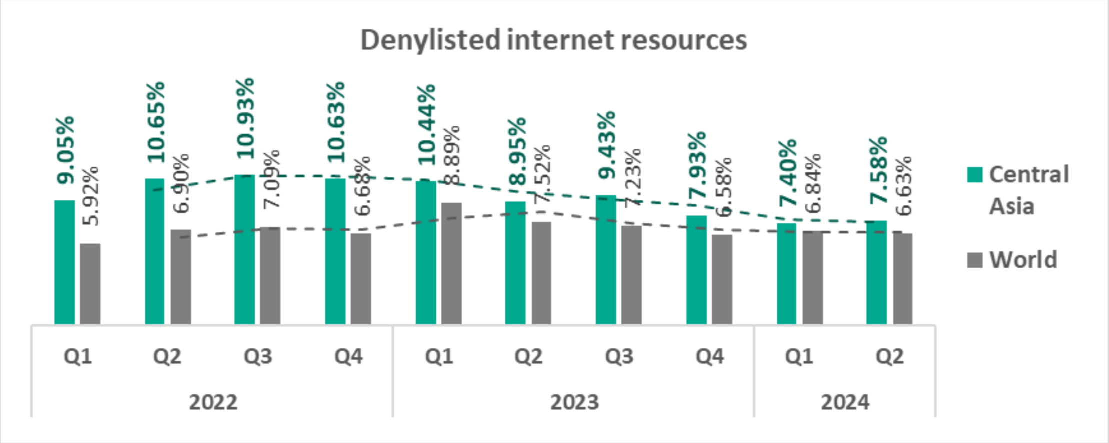
Threat categories

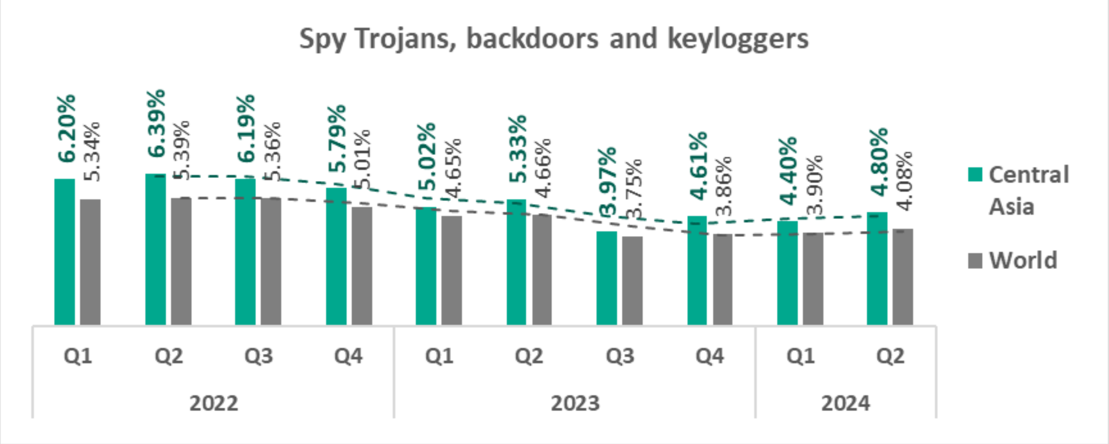


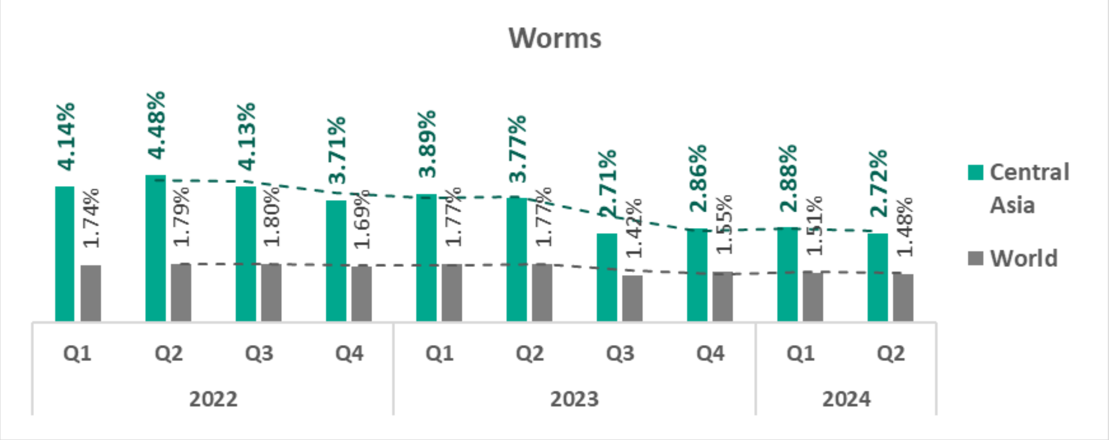
The **largest quarterly increase** was in the percentage of ICS computers on which the following were blocked:

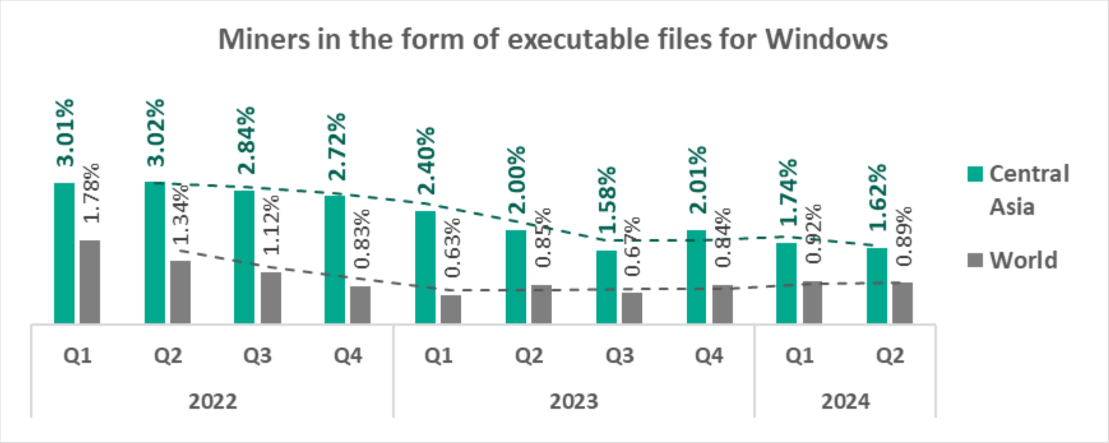
- Malicious documents – by 1.2 times
- Web miners – by 1.2 times
- Spyware – by 1.1 times
- Ransomware – by 1.1 times

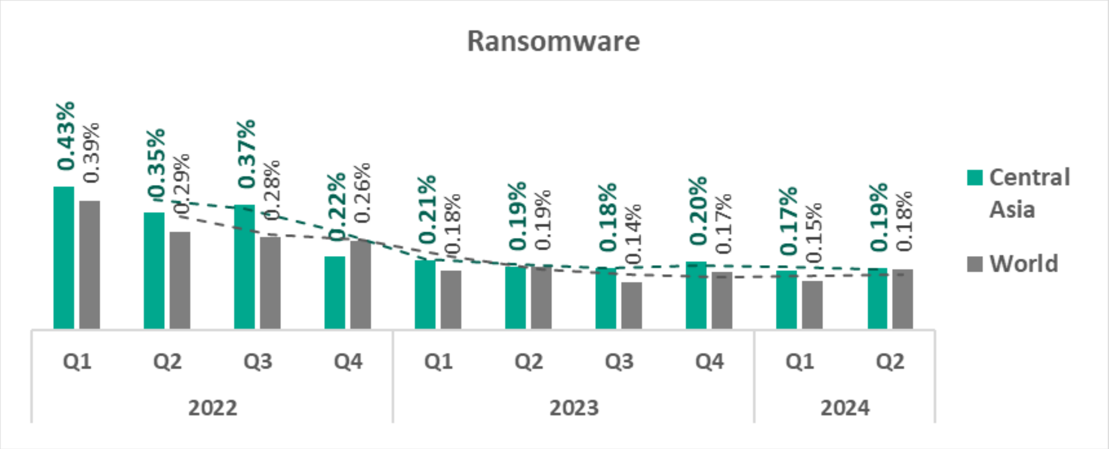
- The **top threat** categories exhibit various quarterly dynamics:








Miners in the form of executable files for Windows
3.01%
1.78%
3.02%
1.34%
2.84%
1.12%
2.72%
0.83%
2.40%
0.63%
2.00%
0.85%
1.58%
0.67%
2.01%
0.84%
1.74%
0.92%
1.62%
0.89%
Q1
Q2
Q3
Q4
2022
Q1
Q2
Q3
Q4
2023
Q1
Q2
2024
Central Asia
World

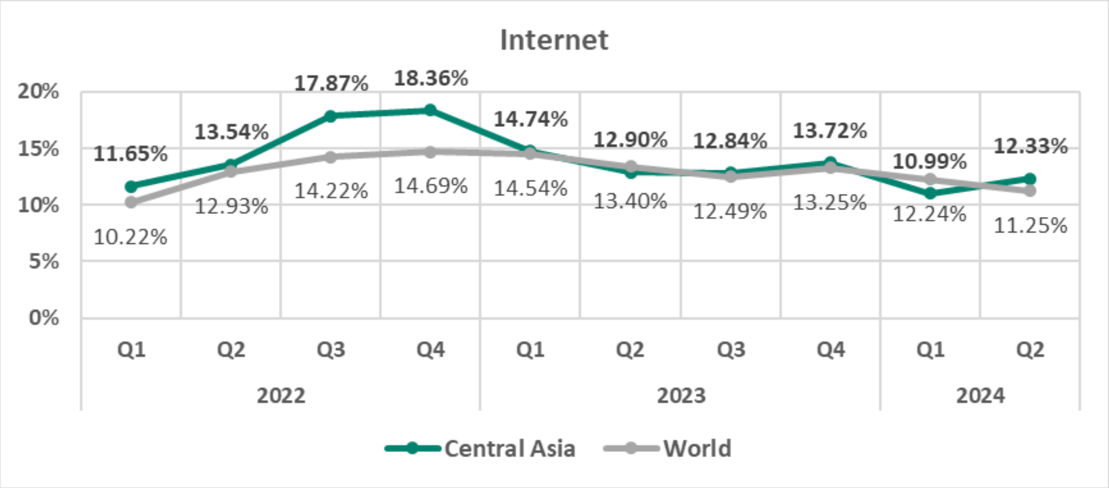

Ransomware
0.43%
0.39%
0.35%
0.29%
0.37%
0.28%
0.22%
0.26%
0.21%
0.18%
0.19%
0.19%
0.18%
0.14%
0.20%
0.17%
0.17%
0.15%
0.19%
0.18%
Q1
Q2
Q3
Q4
2022
Q1
Q2
Q3
Q4
2023
Q1
Q2
2024
Central Asia
World

- The heatmap below illustrates changes in the rankings of threat categories in the region over a period of 2.5 years. **Denylisted internet resources** have been the leading threat category in the region since Q1 2022, with the exception of Q4 2022 and Q4 2023. **Spyware** moved from third to second place in Q1 2024.

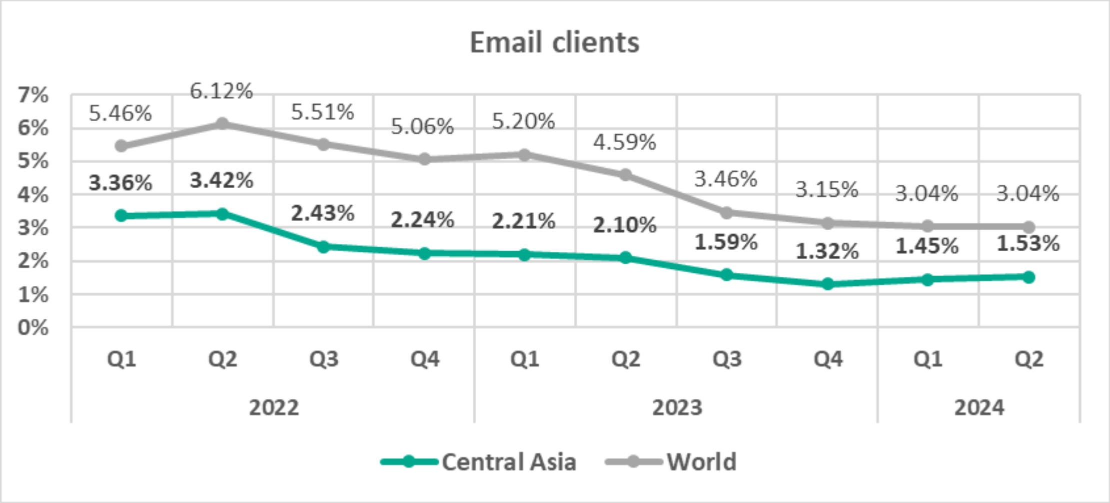
Central Asia	2022				2023				2024	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Denylisted internet resources	1	1	1	2	1	1	1	2	1	1
Spy Trojans, backdoors and keyloggers	2	2	3	3	3	3	3	3	2	2
Malicious scripts and phishing pages (JS and HTML)	3	3	2	1	2	2	2	1	3	3
Worms	4	4	4	4	4	4	4	4	4	4
Miners in the form of executable files for Windows	5	5	5	5	5	5	5	5	5	5
Viruses	7	7	7	7	7	7	6	6	6	6
Malicious documents (MSOffice + PDF)	6	6	6	6	6	6	7	7	7	7
Web miners running in browsers	8	8	8	8	8	8	8	8	8	8
Ransomware	9	9	9	9	9	9	9	9	9	9
Malware for AutoCAD	10	10	10	10	10	10	10	10	10	10

Threat sources

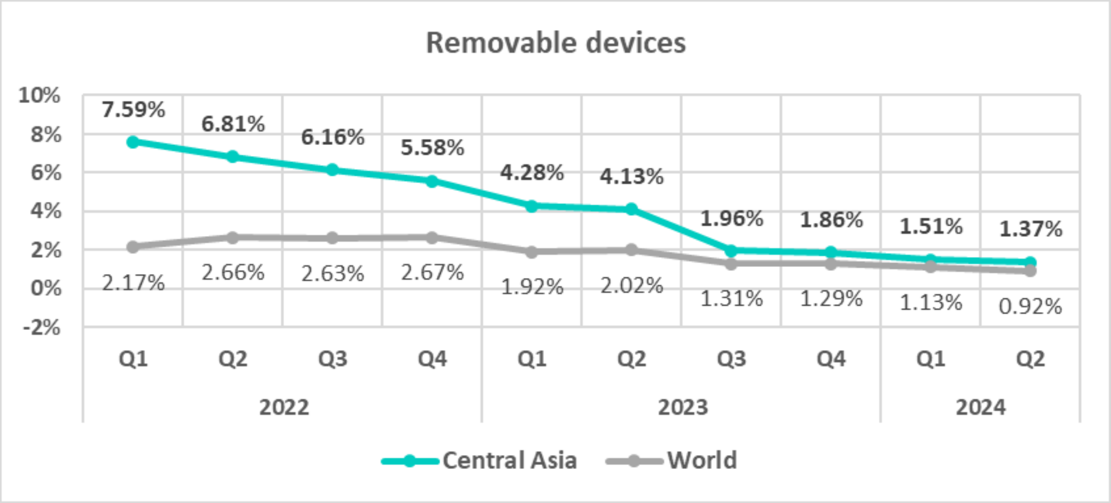
In Q2 2024, the region exhibited an increase in the percentage of ICS computers on which threats from the **internet** were blocked, exceeding the global average by a factor of 1.1.



Threats from **email clients** also saw a slight increase in Q2 2024.

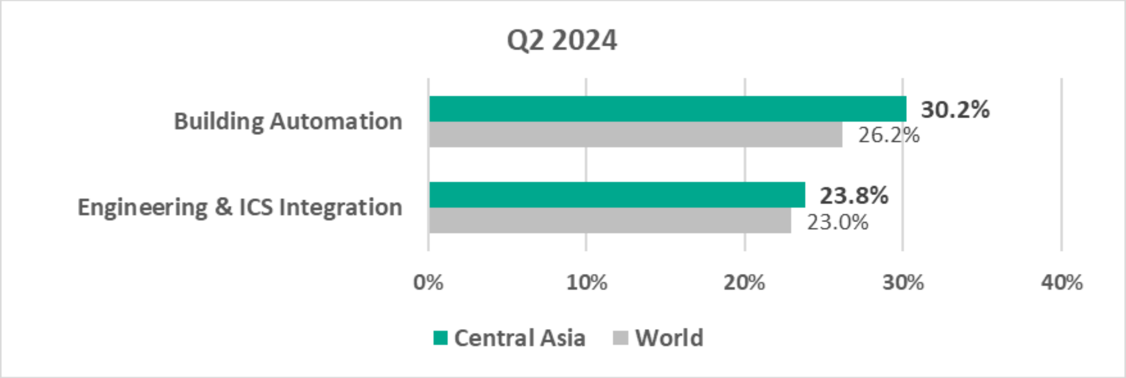


Threats from **removable devices** have been above the global average since Q1 2022, although the gap significantly narrowed by Q3 2023 compared to early 2022, and has remained steady since.

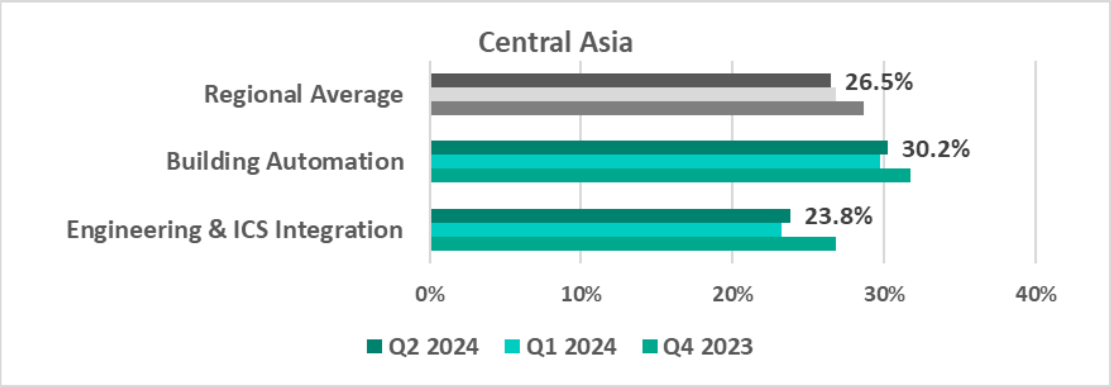


Industries

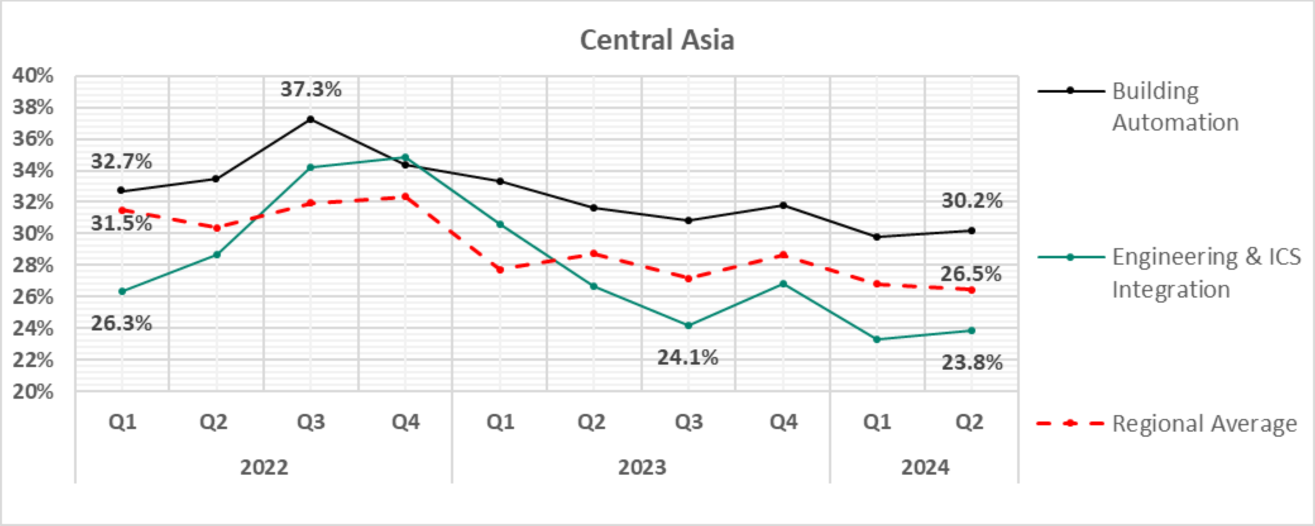
- The **most affected** industry in the region, as selected for this report, was **building automation.**
- From a **global perspective**, the percentage of ICS computers on which malicious objects were blocked in the building automation sector was 1.2 times higher than the global average for the industry:



- In **Q2 2024**, building automation, and engineering & ICS integration saw a slight increase in the percentage of ICS computers on which malicious objects were blocked.



- The **trends** in the selected sectors demonstrate overall positive dynamics.



Middle East

Current threats

-1-

Malicious scripts and phishing pages

6.90%

▼ decrease in Q2
1.2x above global average
2nd in the world

-2-

Spyware

6.29%

▲ **1.1x** increase in Q2
1.5x above global average
2nd in the world

-3-

Denylisted internet resources

5.02%

▼ decrease in Q2

Malicious documents

2.29%

▲ slight increase in Q2
1.2x above global average

Worms

2.22%

▼ decrease in Q2
1.5x above global average
3rd in the world

Viruses

1.99%

▼ decrease in Q2
1.3x above global average

Web miners

0.81%

▼ decrease in Q2
1.6x above global average
2nd in the world

Ransomware

0.33%

▲ **1.2x** increase
1.8x above global average
1st in the world

Threats from
Internet

11.06%

▼ decrease

Threats from
Email clients

4.79%

▼ decrease
1.6x above global average
3rd in the world

Threats from
Removable devices

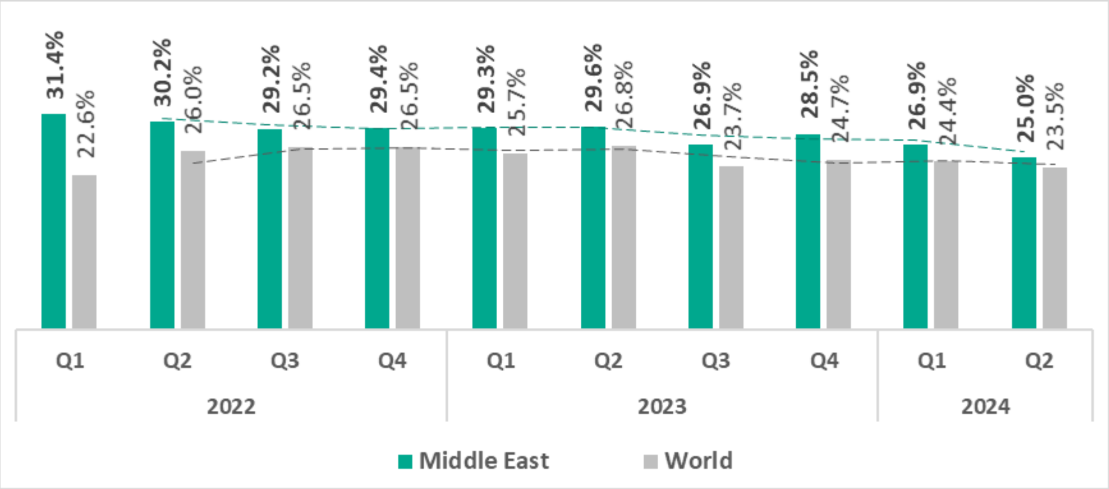
1.31%

▼ decrease
1.4x above global average

Overall

Fourth place in the global ranking by percentage of ICS computers on which malicious objects were blocked.

The percentage of ICS computers where malicious objects were blocked has remained higher than the global average since Q1 2022.



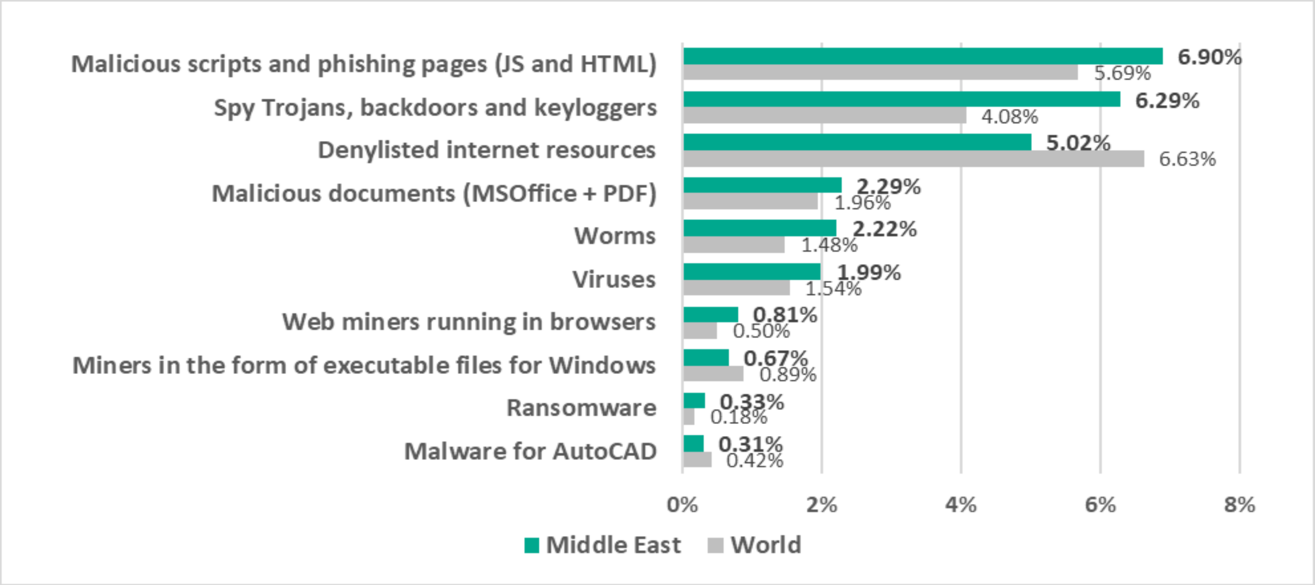
Comparative analysis

The Middle East occupies **leading positions** among regions by percentage of ICS computers on which the following were blocked:

- First place: ransomware
- Second place: spyware, malicious scripts and phishing pages, web miners
- Third place: worms, threats from email clients

Threat categories

- **Compared to the global figures**, the region has a higher percentage of ICS computers on which all categories of threats were blocked, except for denylisted internet resources, executable miners, and malware for AutoCAD.



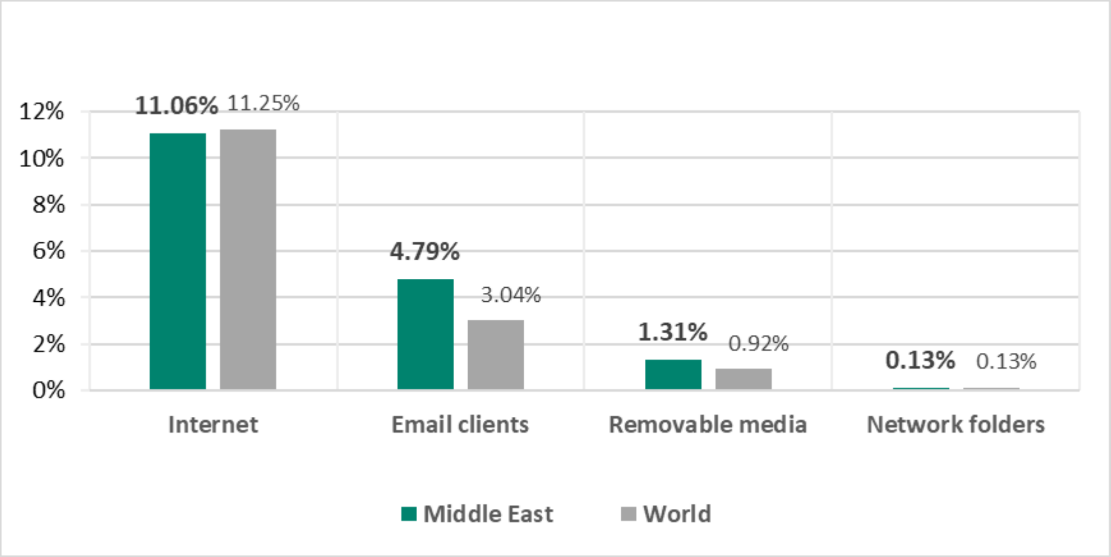
Specifically, the following threat categories showed significantly higher values:

- Ransomware, 1.8 times higher
- Web miners, 1.6 times higher
- Spyware, 1.5 times higher
- Worms, 1.5 times higher
- Visruses, 1.3 times higher
- Malicious scripts and phishing pages, 1.2 times higher
- Malicious documents, 1.2 times higher

Threat sources

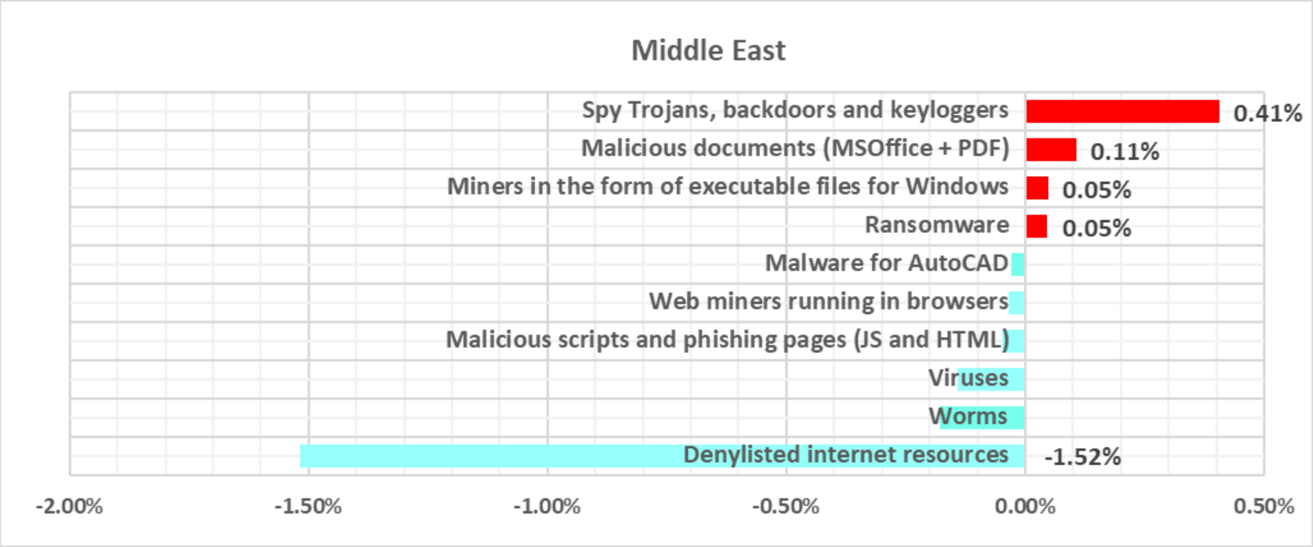
The region ranked **third in the world** by percentage of ICS computers on which threats from **email clients** were blocked, exceeding the global average by a factor of 1.6.

The percentage of computers on which threats from **removable devices** were blocked exceeded the global average by 1.4 times in Q2 2024.



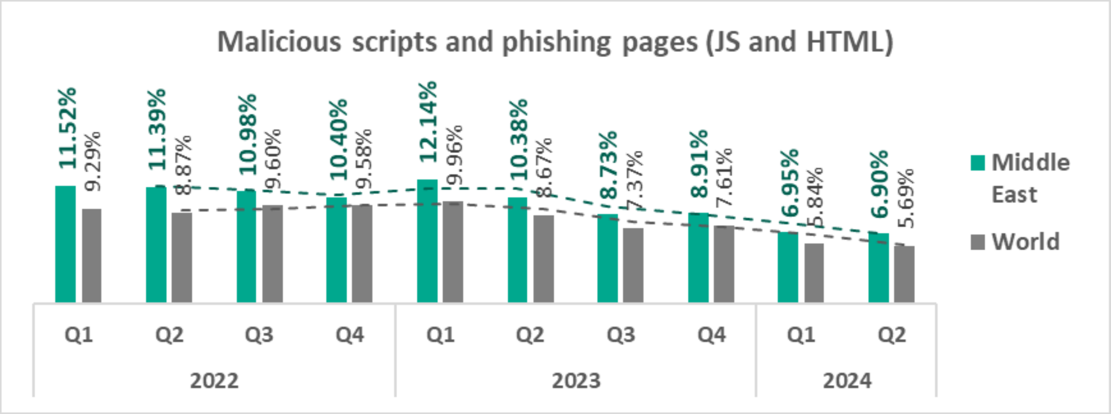
Quarterly changes and trends

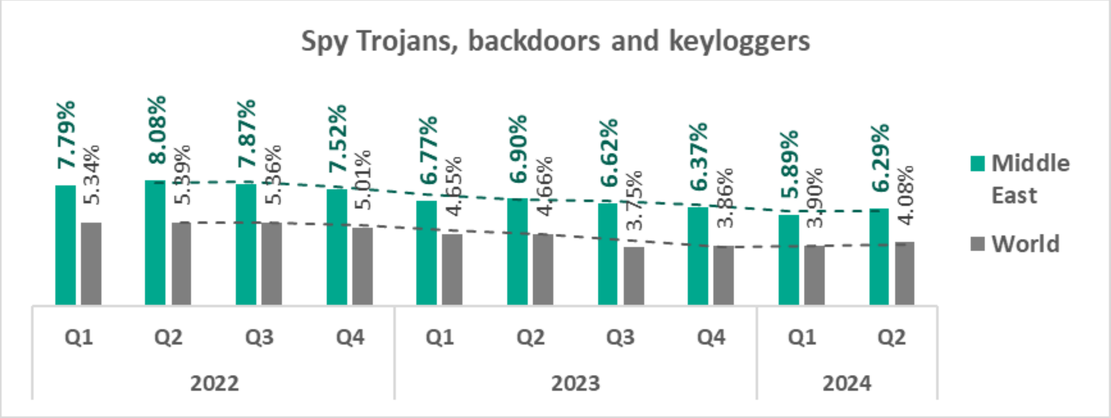
Threat categories

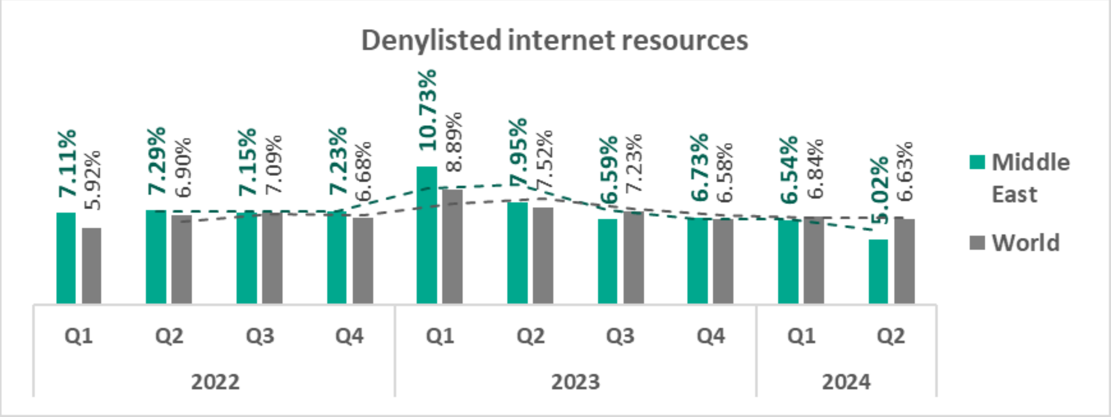


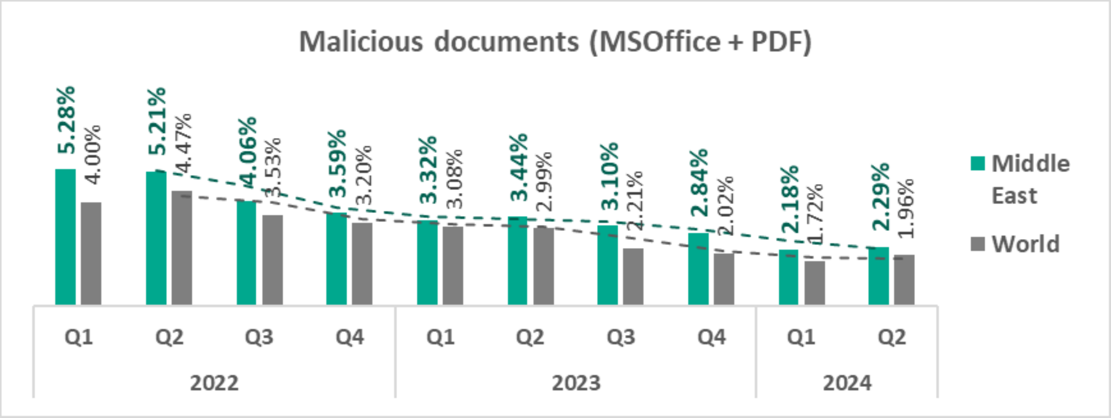
- The **largest quarterly increase** was in the percentage of ICS computers on which the following were blocked:
    - Ransomware – by 1.2 times
    - Miners in the form of executable files – by 1.1 times
    - Spyware – by 1.1 times

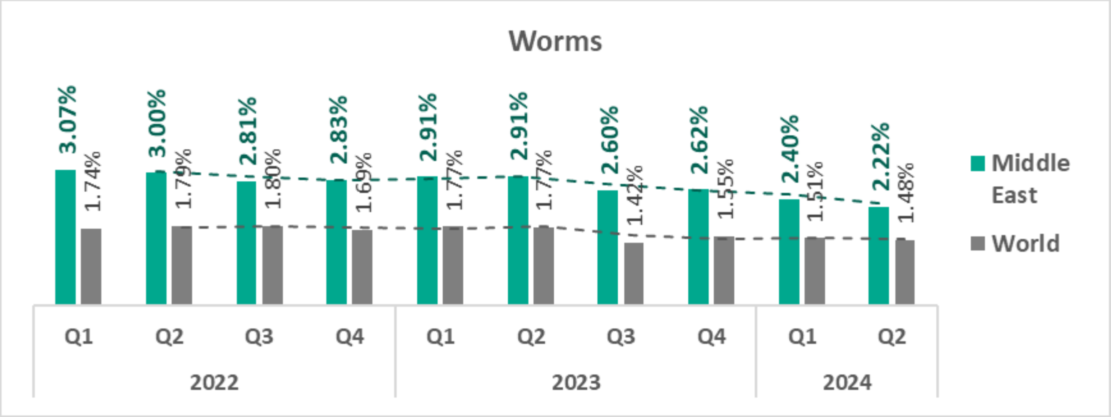
- The **top threat** categories exhibit various quarterly dynamics:

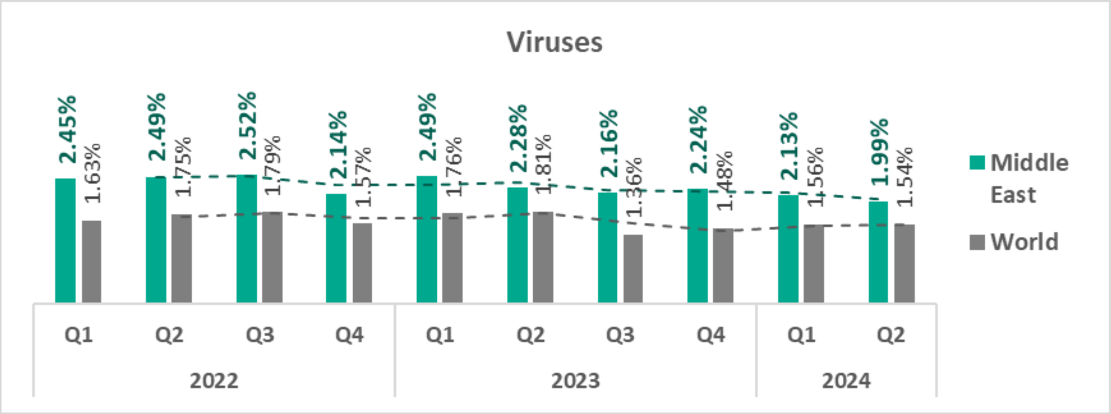


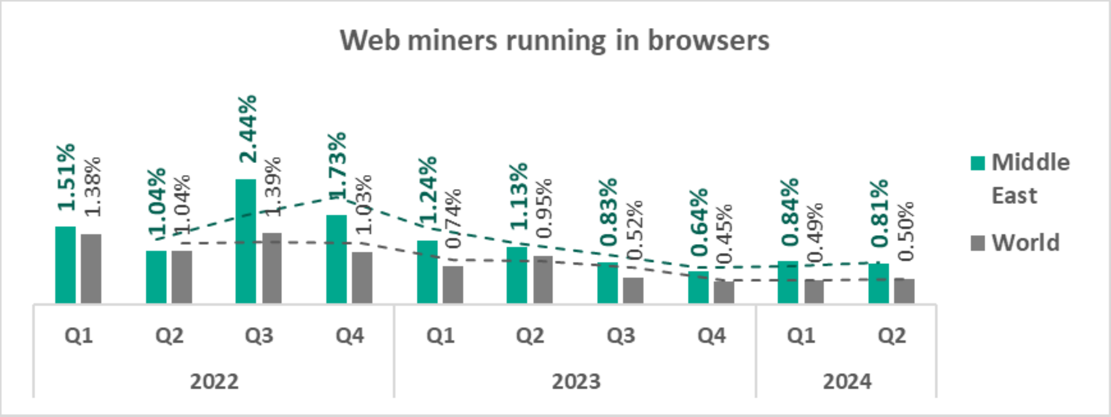


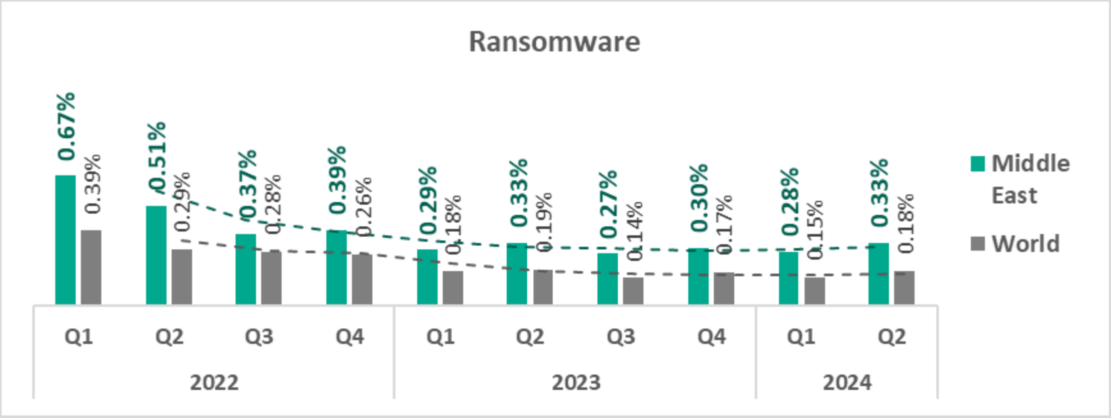



Malicious documents (MSOffice + PDF)
5.28%
4.00%
5.21%
4.47%
4.06%
3.53%
3.59%
3.20%
3.32%
3.08%
3.44%
2.99%
3.10%
2.21%
2.84%
2.02%
2.18%
1.72%
2.29%
1.96%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
Middle East
World

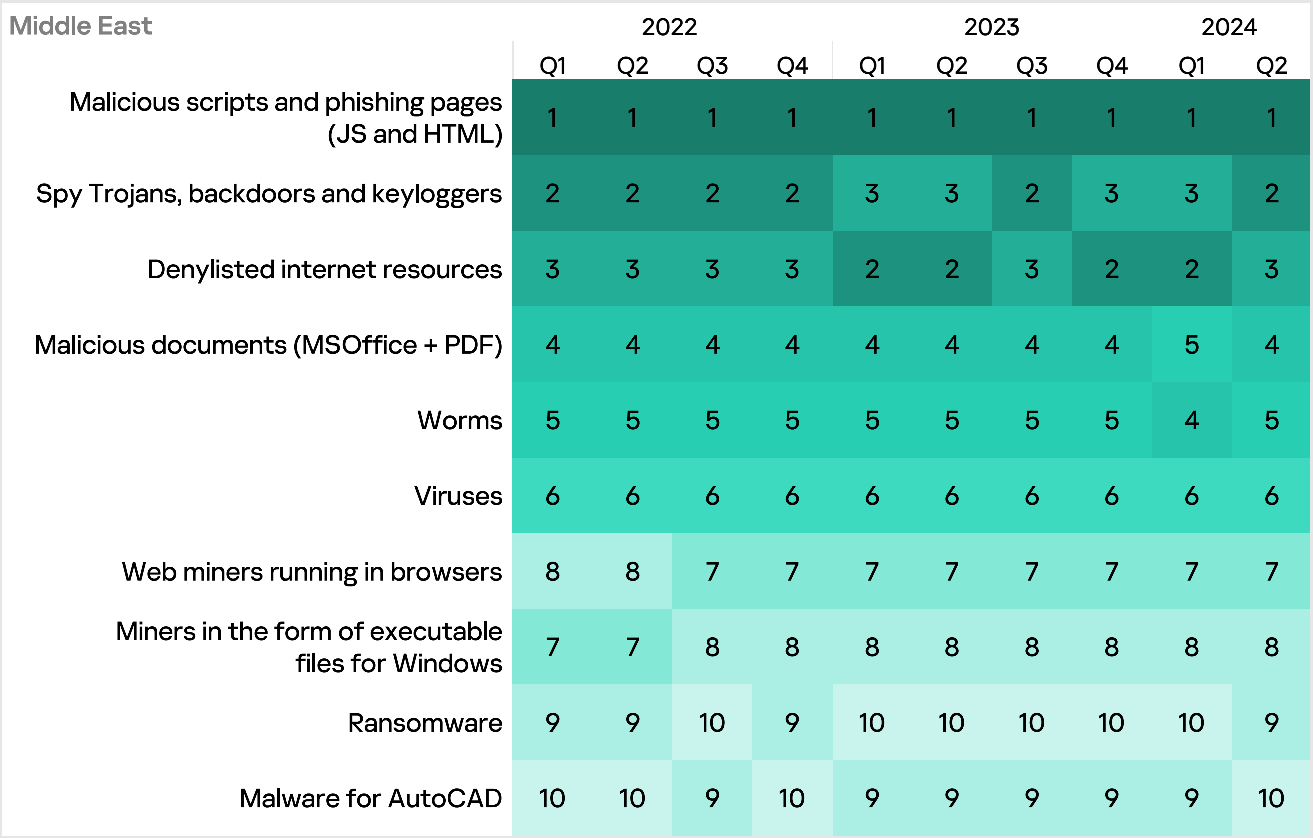

Worms
3.07%
1.74%
3.00%
1.79%
2.81%
1.80%
2.83%
1.69%
2.91%
1.77%
2.91%
1.77%
2.60%
1.42%
2.62%
1.55%
2.40%
1.51%
2.22%
1.48%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
Middle East
World


Viruses
2.45%
1.63%
2.49%
1.75%
2.52%
1.79%
2.14%
1.57%
2.49%
1.76%
2.28%
1.81%
2.16%
1.36%
2.24%
1.48%
2.13%
1.56%
1.99%
1.54%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
Middle East
World


Web miners running in browsers
1.51%
1.38%
1.04%
1.04%
2.44%
1.39%
1.73%
1.03%
1.24%
0.74%
1.13%
0.95%
0.83%
0.52%
0.64%
0.45%
0.84%
0.49%
0.81%
0.50%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
Middle East
World

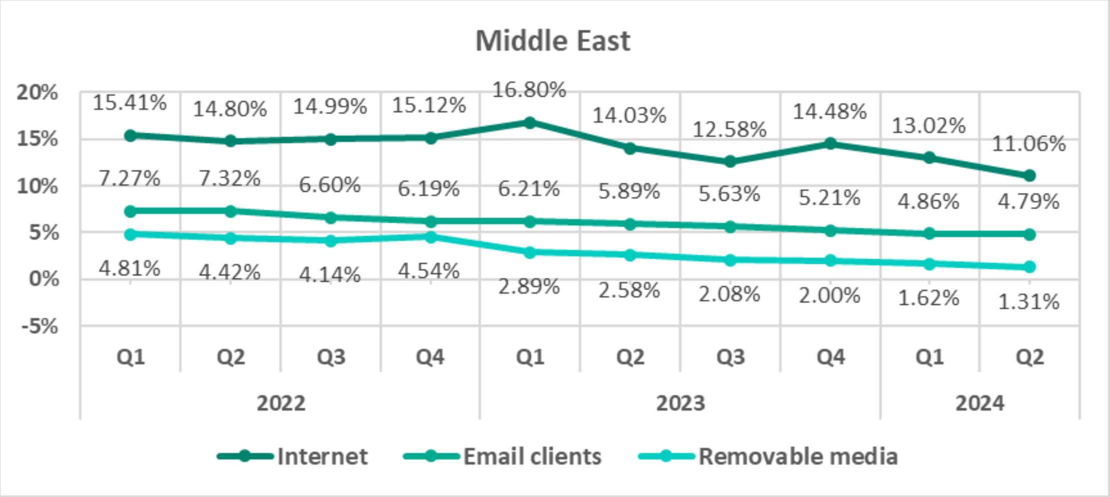

Ransomware
0.67%
0.39%
0.51%
0.29%
0.37%
0.28%
0.39%
0.26%
0.29%
0.18%
0.33%
0.19%
0.27%
0.14%
0.30%
0.17%
0.28%
0.15%
0.33%
0.18%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
Middle East
World

- The heatmap below illustrates changes in the rankings of threat categories in the region over a period of 2.5 years. **Malicious scripts and phishing pages** have been the leading threat category in the region since Q1 2022. **Spyware** moved up from third to second place in Q2 2024.

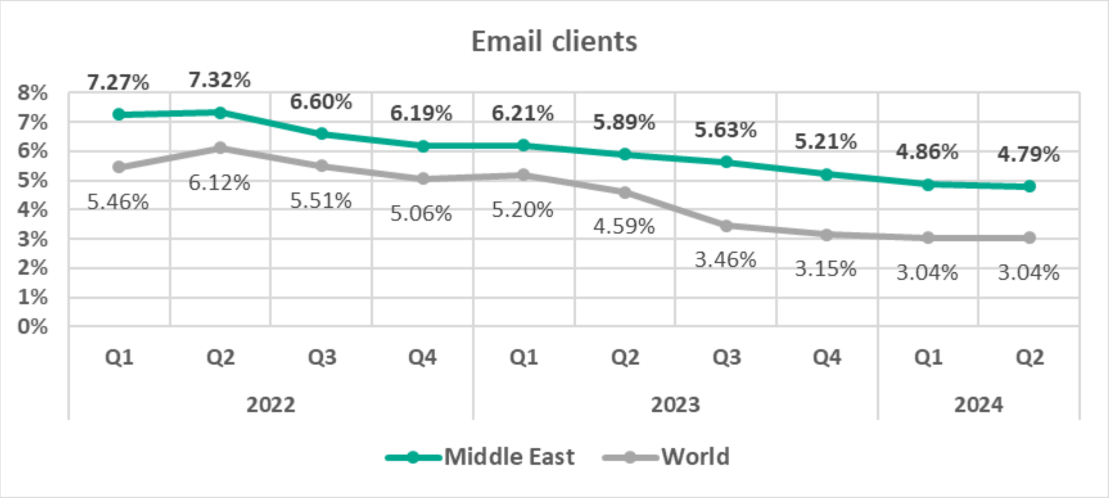


Middle East	2022				2023				2024	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Malicious scripts and phishing pages (JS and HTML)	1	1	1	1	1	1	1	1	1	1
Spy Trojans, backdoors and keyloggers	2	2	2	2	3	3	2	3	3	2
Denylisted internet resources	3	3	3	3	2	2	3	2	2	3
Malicious documents (MSOffice + PDF)	4	4	4	4	4	4	4	4	5	4
Worms	5	5	5	5	5	5	5	5	4	5
Viruses	6	6	6	6	6	6	6	6	6	6
Web miners running in browsers	8	8	7	7	7	7	7	7	7	7
Miners in the form of executable files for Windows	7	7	8	8	8	8	8	8	8	8
Ransomware	9	9	10	9	10	10	10	10	10	9
Malware for AutoCAD	10	10	9	10	9	9	9	9	9	10

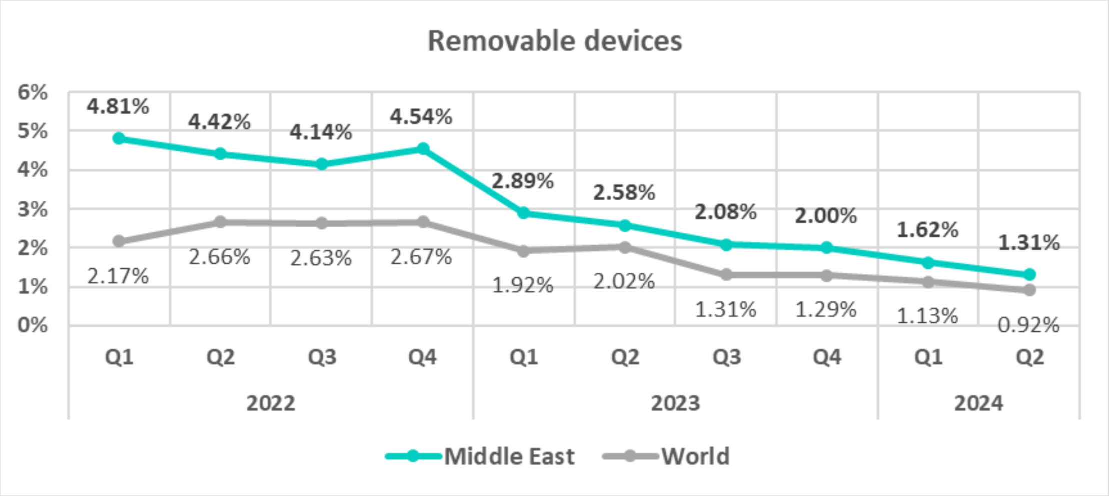
Threat sources



The trend for threats from **email clients** has been above the global average since Q1 2022. The gap widened in Q3 2023 and has remained mostly steady since.



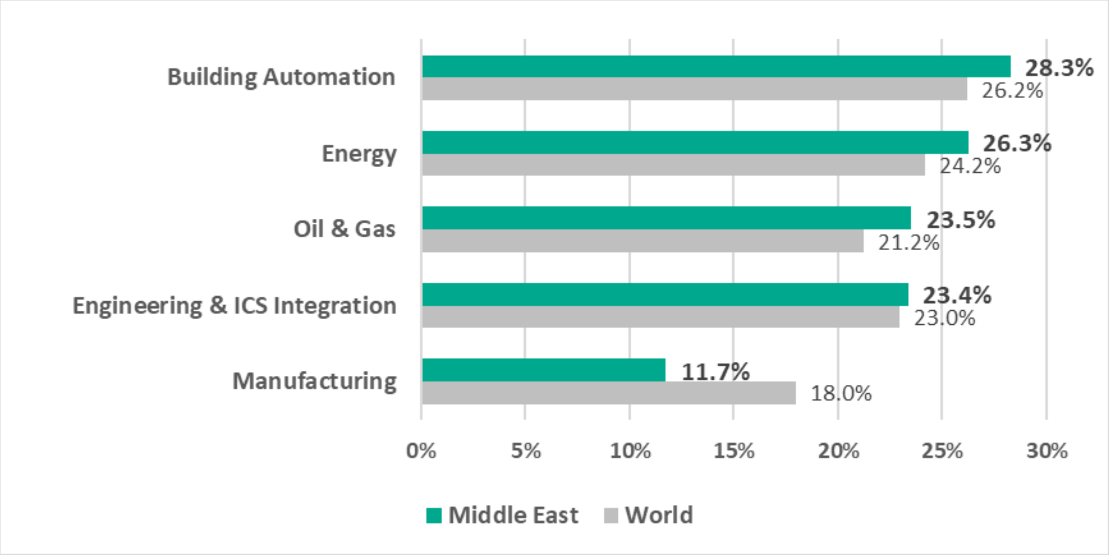
Threats from **removable devices** have been above the global average since Q1 2022. The gap had significantly narrowed by Q2 2023 compared to early 2022, and has remained steady since.



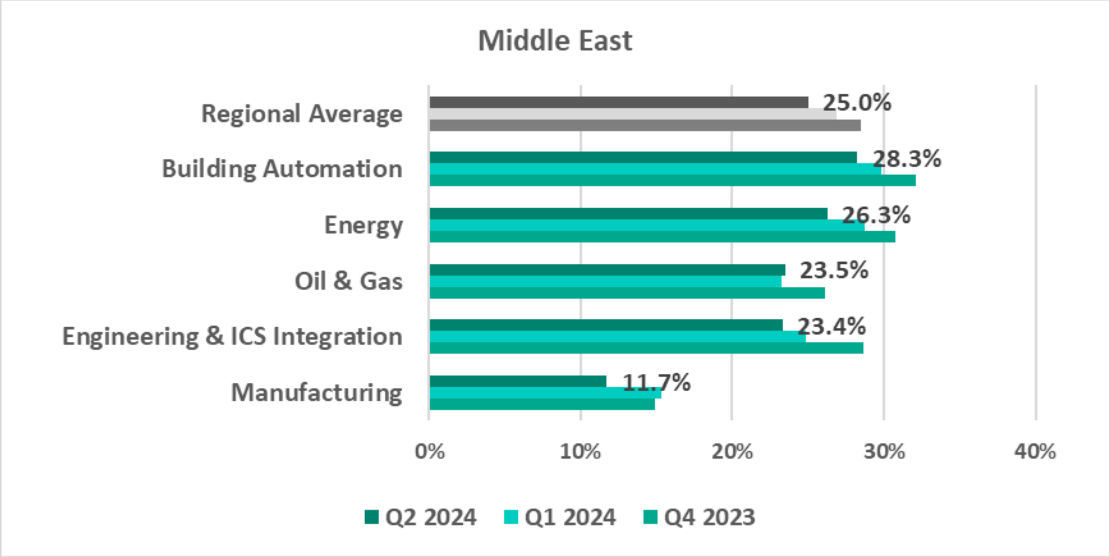
Industries

- The **most affected** industry in the region, as selected for this report, was **building automation**.

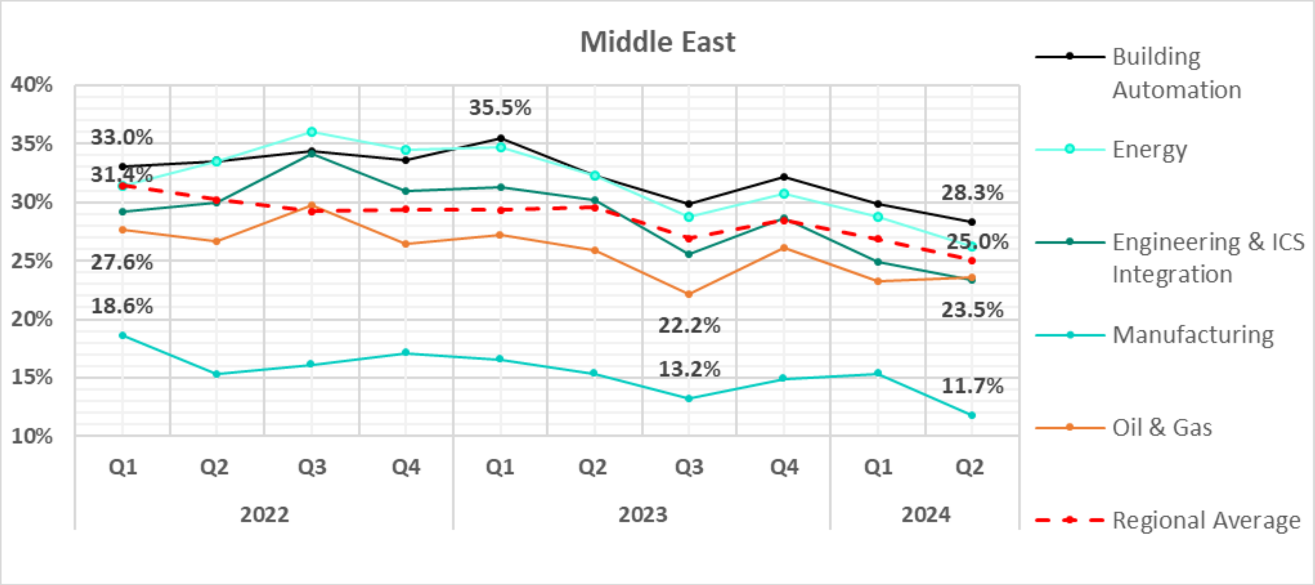
- From a **global perspective**, the following industries saw a higher percentage of ICS computers on which malicious objects were blocked:
  - Building automation – 1.1 times higher
  - Energy – 1.1 times higher
  - Oil and gas – 1.1 times higher respectively



- In **Q2 2024**, the **oil and gas** sector exhibited a slight increase in the percentage of ICS computers on which malicious objects were blocked, while the other sectors saw a decrease.



- The **trends** in the selected sectors demonstrate overall positive dynamics.



Eastern Europe

Current threats

-1-

Denylisted internet resources

7.07%

▲ slight increase in Q2
1.1x above global average
4th in the world

-2-

Malicious scripts and phishing pages

5.75%

▼ decrease in Q2
slightly above global average

-3-

Spyware

5.44%

▲ **1.1x** increase in Q2
1.3x above global average
3rd in the world **in terms of growth**

Malicious documents

2.32%

▼ decrease in Q2
1.2x above global average
4th in the world

Worms

1.56%

▲ slight increase in Q2
1.1x above global average

Executable miners

1.01%

▼ decrease in Q2
1.1x above global average
4th in the world

Web miners

0.63%

▲ slight increase in Q2
1.3x above global average
4th in the world

Ransomware

0.18%

▲ **1.1x** increase in Q2

Threats from
Internet

10.98%

▼ decrease in Q2

Threats from
Email clients

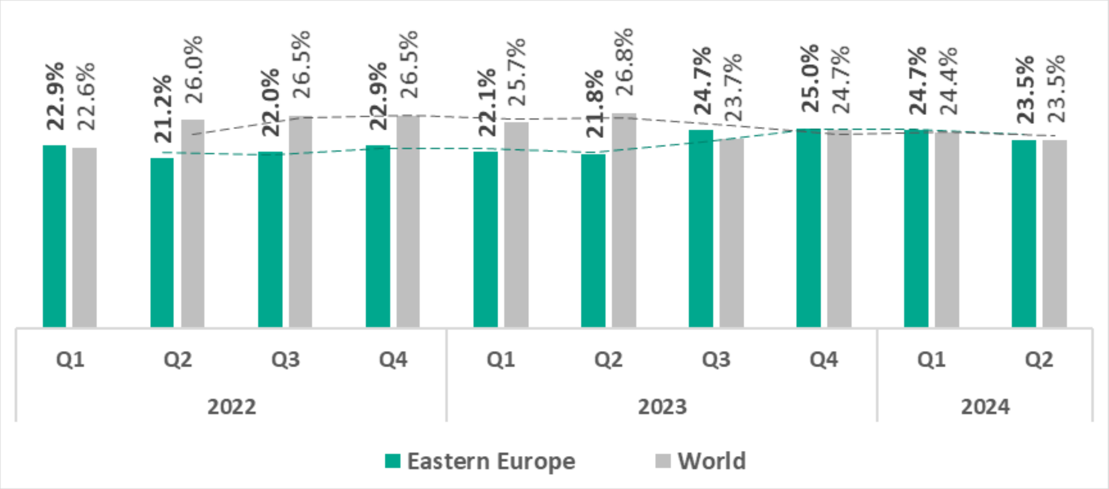
4.97%

▲ **1.1x** increase in Q2
1.6x above global average
2nd in the world
3rd globally **in terms of growth**

Overall

Fifth place in the global ranking by percentage of ICS computers on which malicious objects were blocked. Before Q2 2023, the region did not rank higher than ninth place.

In Q2 2024, the percentage of ICS computers on which malicious objects were blocked was the same as the global average.

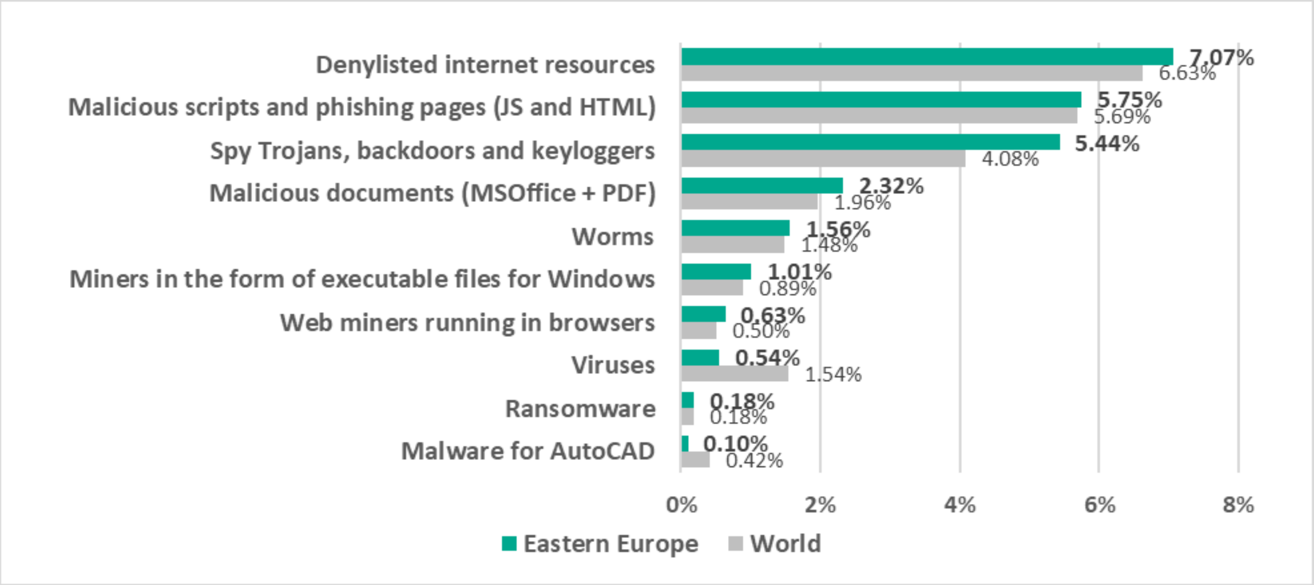


Comparative analysis

Eastern Europe ranked **second** among regions by percentage of ICS computers on which threats from email clients were blocked.

Threat categories

Compared to the global figures, the region has a higher percentage of ICS computers on which all categories of threats were blocked, except for viruses and malware for AutoCAD.

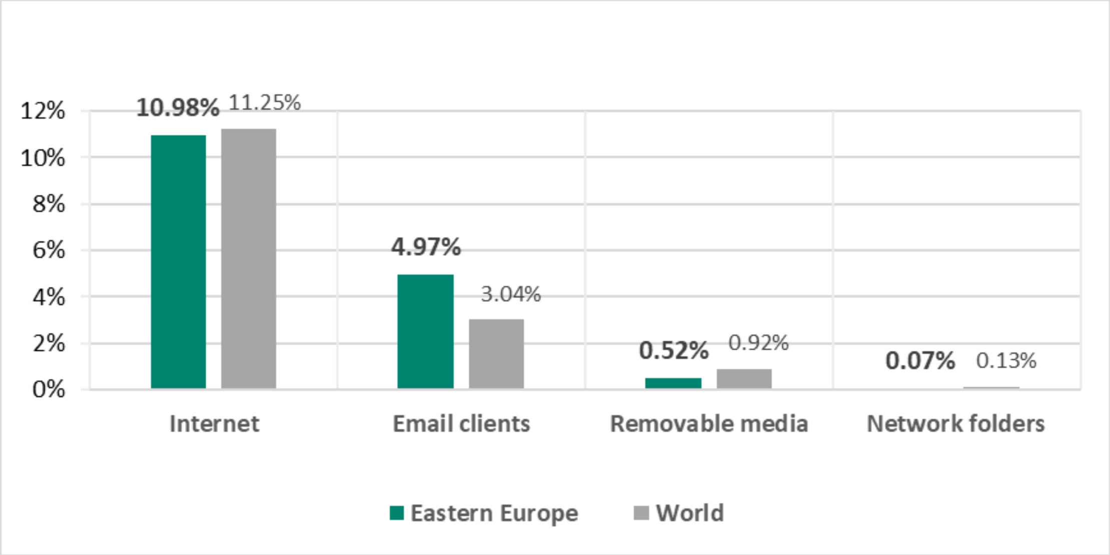


Specifically, the following threat categories showed significantly higher values compared to the global average:

- Spyware, 1.3 times higher
- Web miners, 1.3 times higher
- Malicious documents, 1.2 times higher

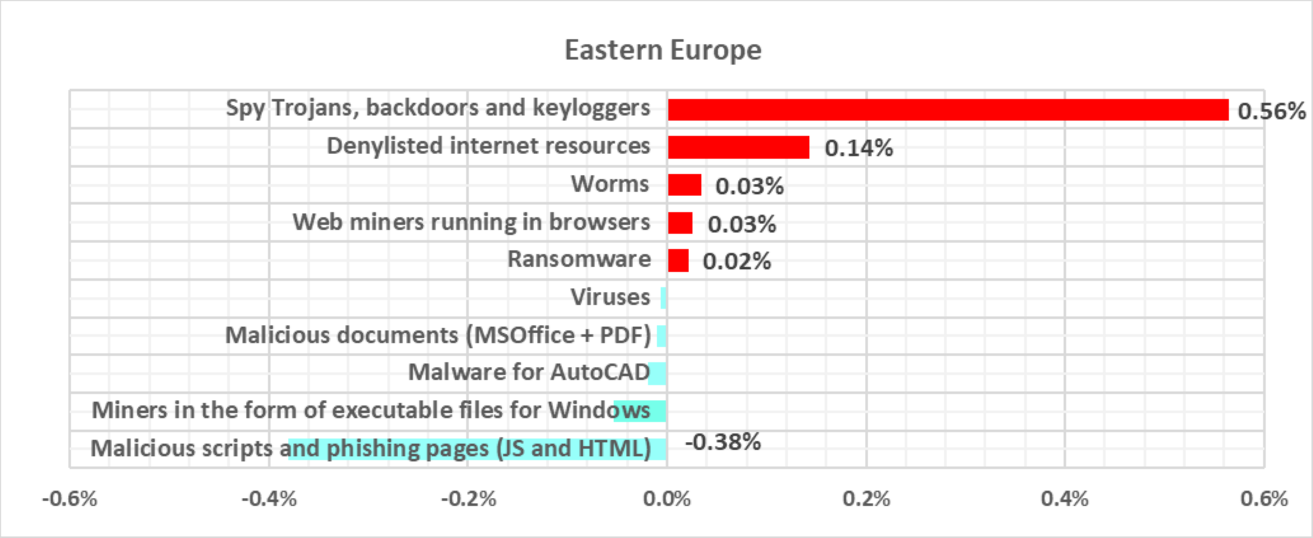
Threat sources

The region ranked second in the world by percentage of ICS computers on which threats from **email clients** were blocked, exceeding the global average by 1.6 times.

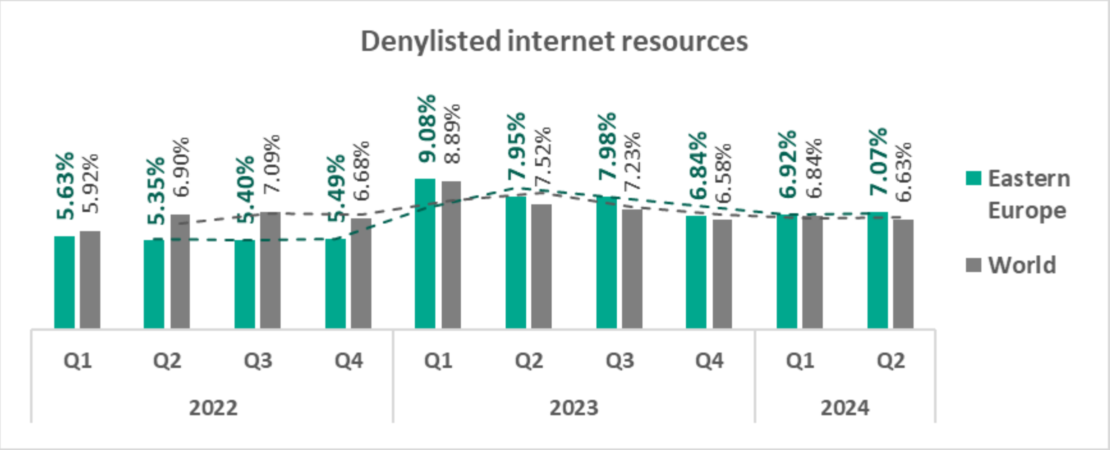


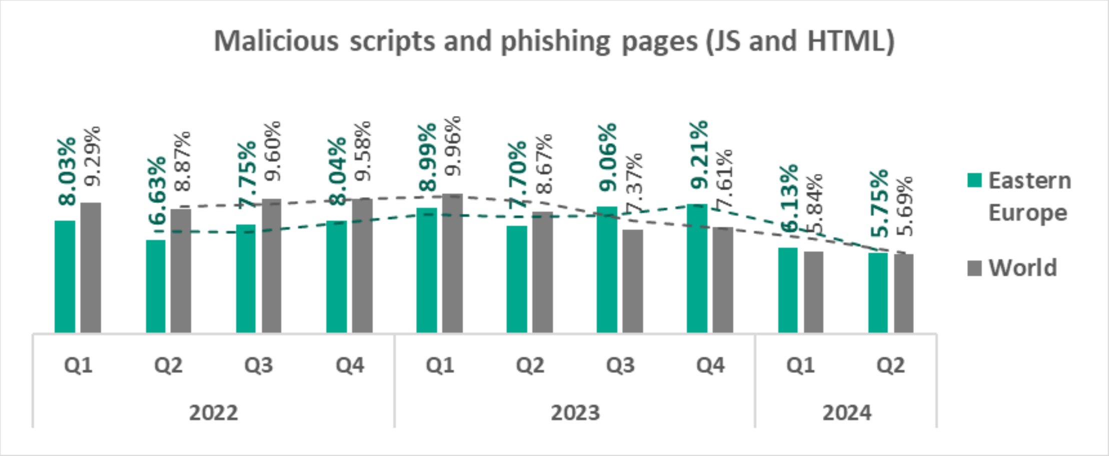
Quarterly changes and trends

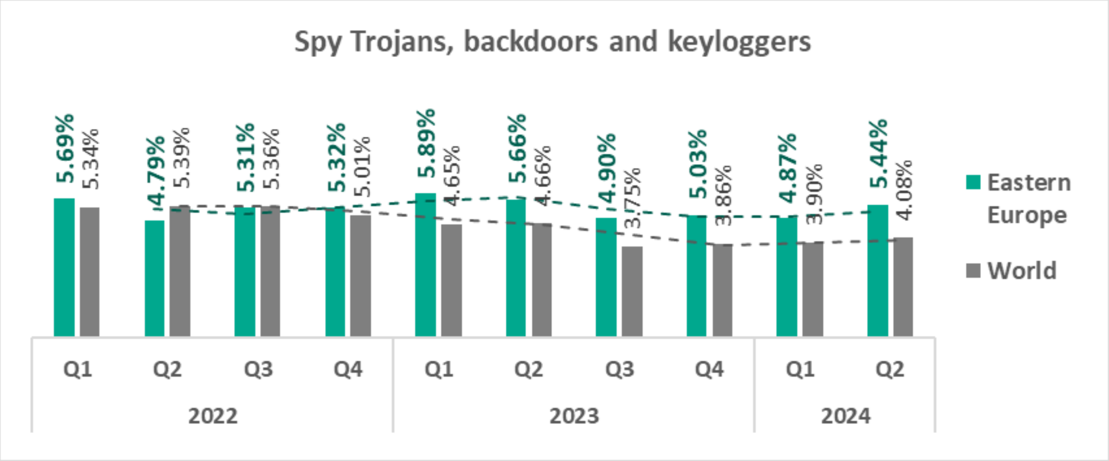
Threat categories

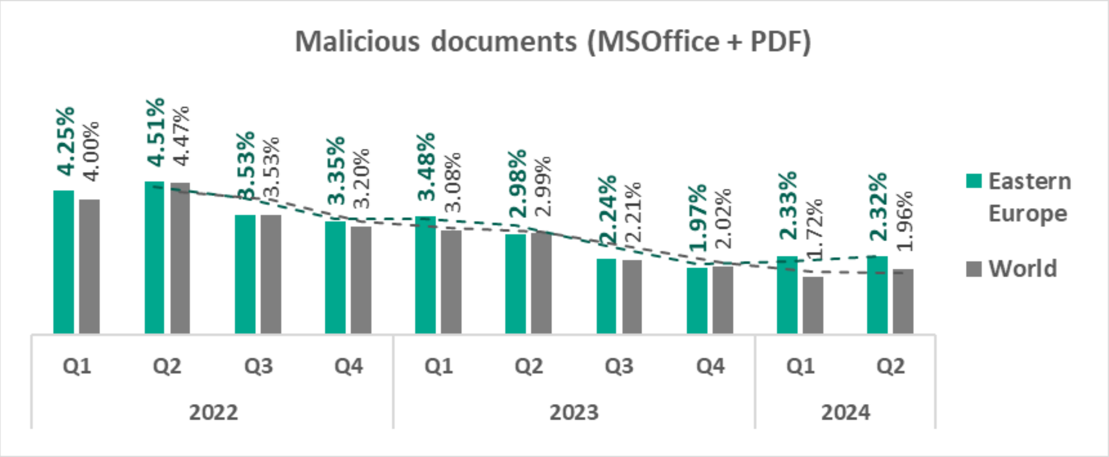


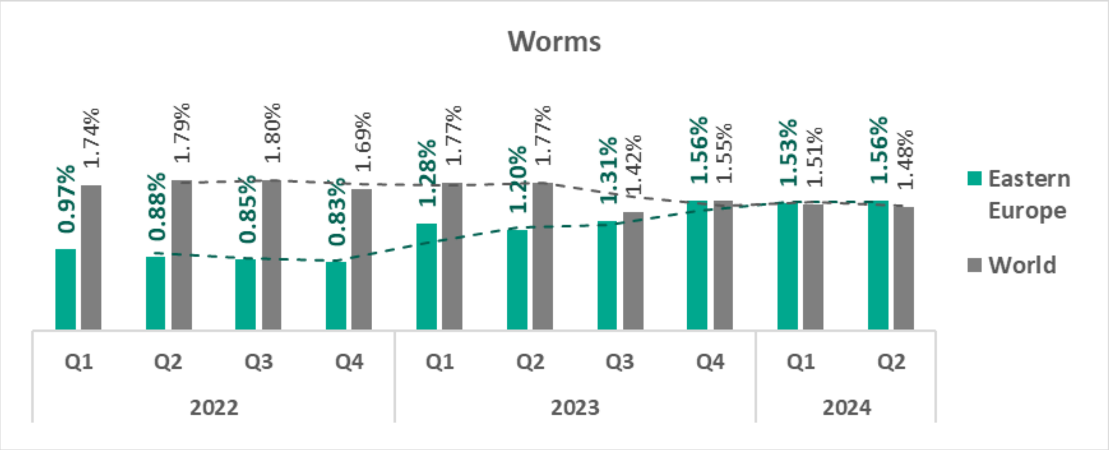
- The **largest quarterly increase** was in the percentage of ICS computers on which the following were blocked:
  - Spyware, by 1.1 times. Ranked third in the world in terms of growth
  - Ransomware, by 1.1 times.
- The **top threat** categories exhibit various quarterly dynamics:

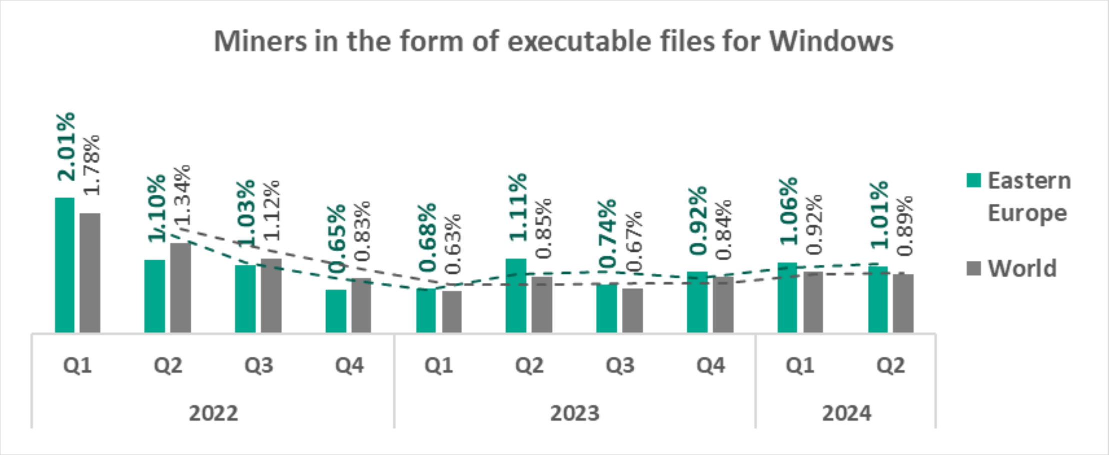


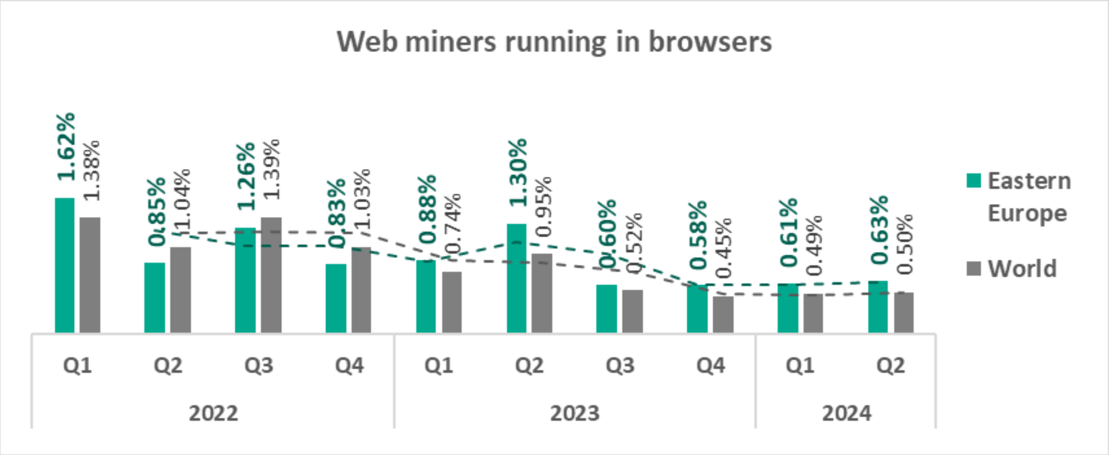

Malicious scripts and phishing pages (JS and HTML)
8.03%
9.29%
6.63%
8.87%
7.75%
9.60%
8.04%
9.58%
8.99%
9.96%
7.70%
8.67%
9.06%
7.37%
9.21%
7.61%
6.13%
5.84%
5.75%
5.69%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
Eastern Europe
World

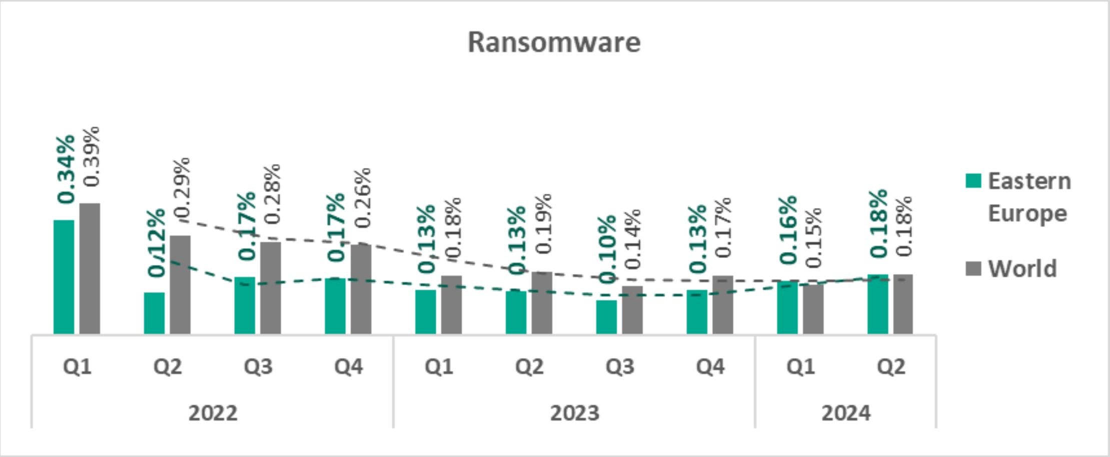

Spy Trojans, backdoors and keyloggers
5.69%
5.34%
4.79%
5.39%
5.31%
5.36%
5.32%
5.01%
5.89%
4.65%
5.66%
4.66%
4.90%
3.75%
5.03%
3.86%
4.87%
3.90%
5.44%
4.08%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
Eastern Europe
World


Malicious documents (MSOffice + PDF)
4.25%
4.00%
4.51%
4.47%
3.53%
3.53%
3.35%
3.20%
3.48%
3.08%
2.98%
2.99%
2.24%
2.21%
1.97%
2.02%
2.33%
1.72%
2.32%
1.96%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
Eastern Europe
World


Worms
0.97%
1.74%
0.88%
1.79%
0.85%
1.80%
0.83%
1.69%
1.28%
1.77%
1.20%
1.77%
1.31%
1.42%
1.56%
1.55%
1.53%
1.51%
1.56%
1.48%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
🟩 Eastern Europe
■ World


Miners in the form of executable files for Windows
2.01%
1.78%
1.10%
1.34%
1.03%
1.12%
0.65%
0.83%
0.68%
0.63%
1.11%
0.85%
0.74%
0.67%
0.92%
0.84%
1.06%
0.92%
1.01%
0.89%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
🟩 Eastern Europe
■ World


Web miners running in browsers
1.62%
1.38%
0.85%
1.04%
1.26%
1.39%
0.83%
1.03%
0.88%
0.74%
1.30%
0.95%
0.60%
0.52%
0.58%
0.45%
0.61%
0.49%
0.63%
0.50%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
🟩 Eastern Europe
■ World

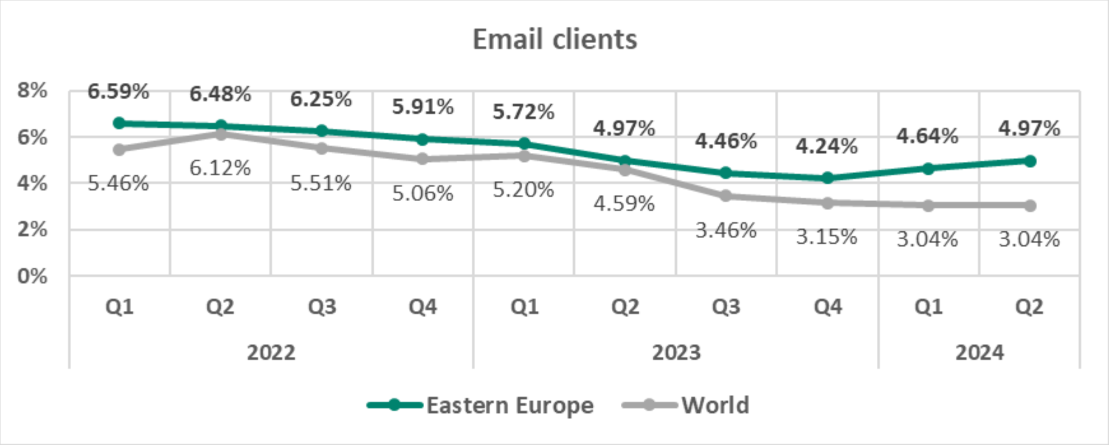


- The heatmap below illustrates changes in the rankings of threat categories in the region over a period of 2.5 years. **Denylisted internet resources** has been the leading threat category in the region since Q1 2024. **Malicious scripts and phishing pages** fell from first to second place in Q1 2024.

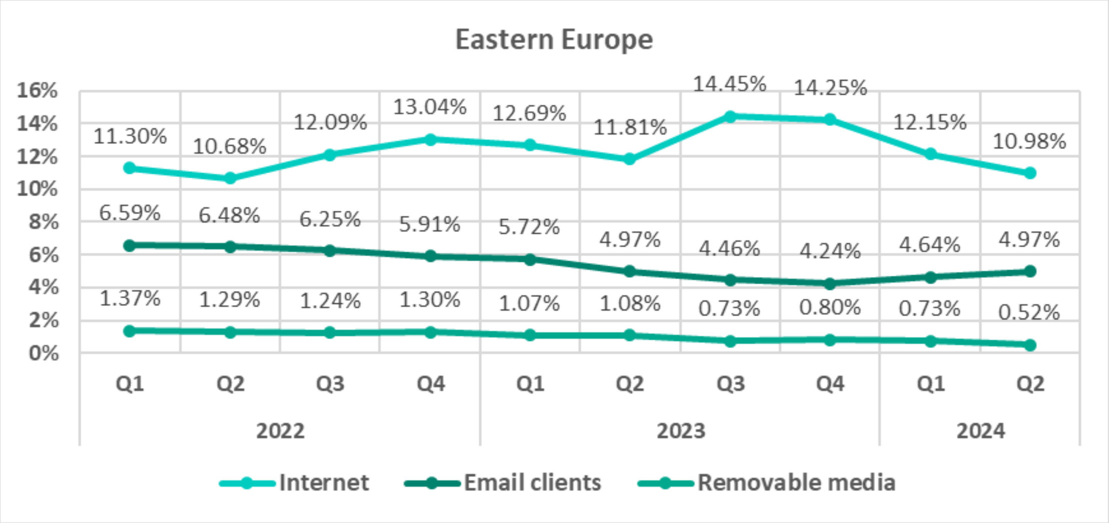
Eastern Europe	2022				2023				2024	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Denylisted internet resources	3	2	2	2	1	1	2	2	1	1
Malicious scripts and phishing pages (JS and HTML)	1	1	1	1	2	2	1	1	2	2
Spy Trojans, backdoors and keyloggers	2	3	3	3	3	3	3	3	3	3
Malicious documents (MSOffice + PDF)	4	4	4	4	4	4	4	4	4	4
Worms	7	6	7	6	5	6	5	5	5	5
Miners in the form of executable files for Windows	5	5	6	7	7	7	6	6	6	6
Web miners running in browsers	6	7	5	5	6	5	7	7	7	7
Viruses	8	8	8	8	8	8	8	8	8	8
Ransomware	9	9	9	9	9	9	9	9	9	9
Malware for AutoCAD	10	10	10	10	10	10	10	10	10	10

Threat sources

In Q2 2024, threats from **email clients** in Eastern Europe ranked third in the world in terms of growth. The trend has been above the global average throughout the observed period. The gap began to widen noticeably in Q2 2023 and reached its maximum in Q2 2024.



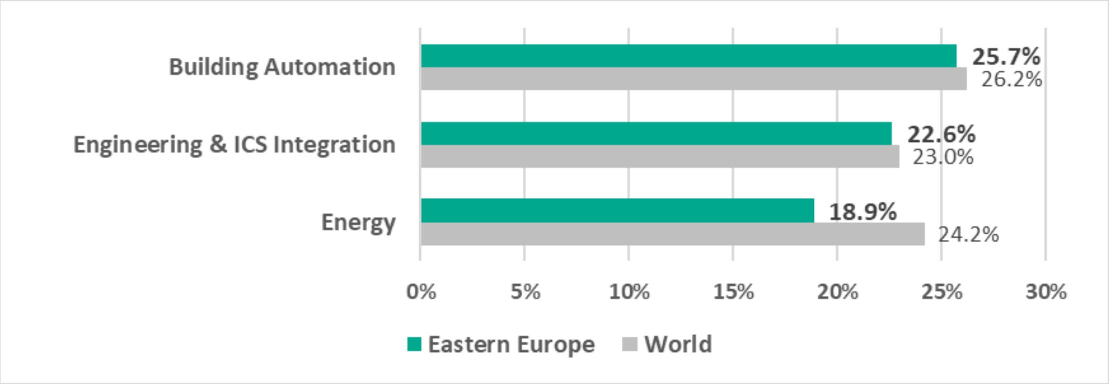
Threats from the **internet** and **removable devices** have exhibited a downward trend over the past three quarters.



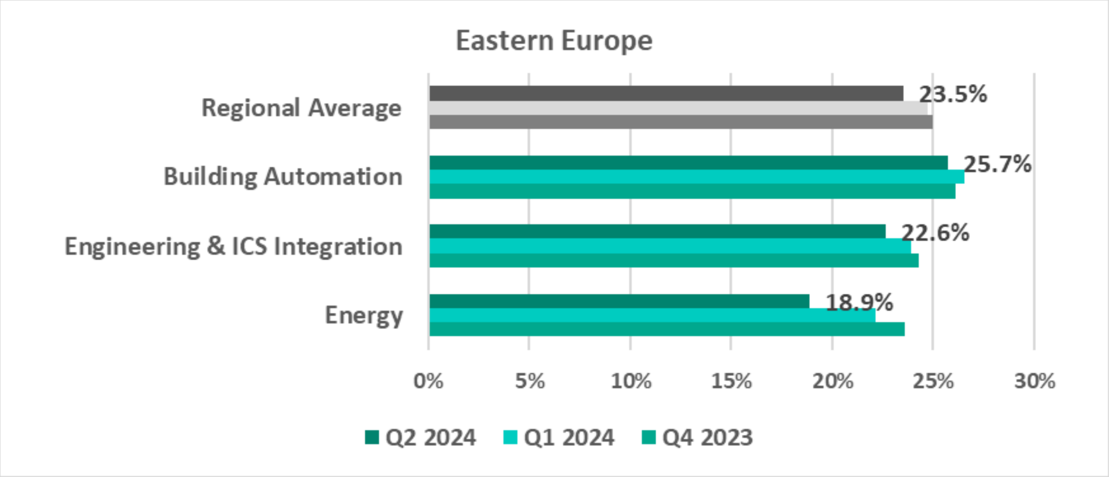
Industries

- The **most affected** industry in the region, as selected for this report, was **building automation**.

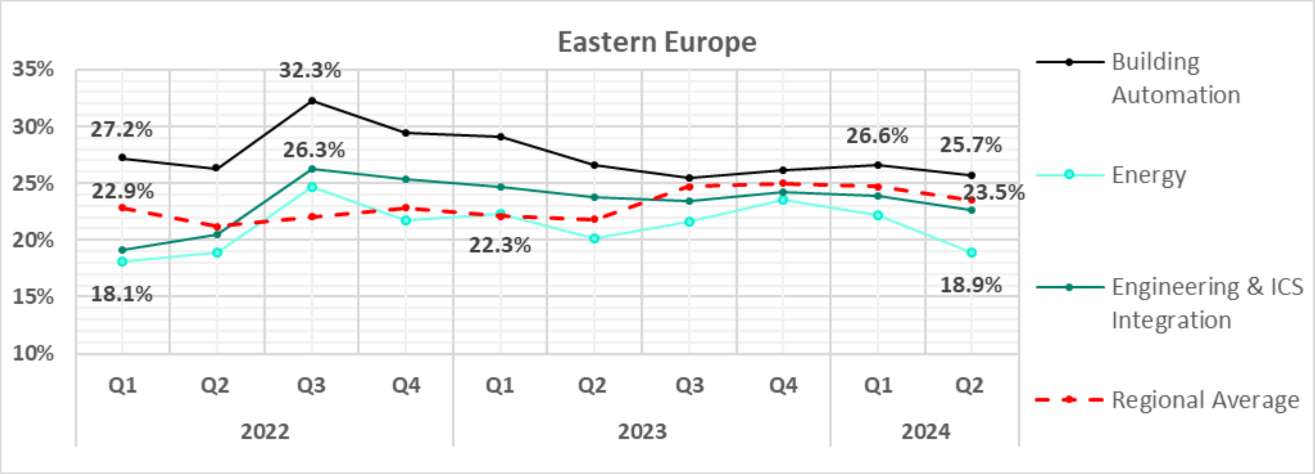
  Compared to the respective **global averages**, all selected industries demonstrated lower percentages of ICS computers on which malicious objects were blocked.



- In **Q2 2024**, all sectors under observation saw a decrease in the percentage of ICS computers on which malicious objects were blocked.



- The **trends** in the selected sectors demonstrate a general stabilization after a notable rise in 2022.



Russia

Current threats

-1-

Denylisted internet resources

7.8%

▲ slight increase in Q2
1.2x above global average
1st in the world

-2-

Malicious scripts and phishing pages

4.53%

▼ decrease in Q2

-3-

Spyware

2.31%

▼ decrease in Q2

Executable miners

1.18%

▼ decrease in Q2
1.3x above global average
2nd in the world

Malicious documents

0.90%

▲ **1.2x** increase in Q2

Threats from
Internet

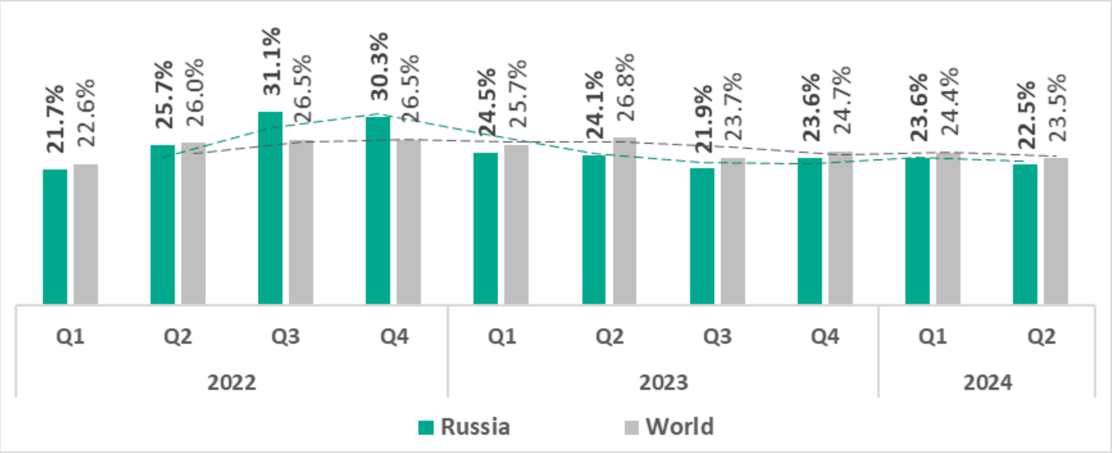
11.89%

▼ decrease in Q2
1.2x above global average
3rd in the world

Overall

Sixth in the global ranking by percentage of ICS computers on which malicious objects were blocked.

With the exception of Q3 and Q4 2022, the percentage of ICS computers on which malicious objects were blocked in the region is slightly lower than the global average.



Comparative analysis

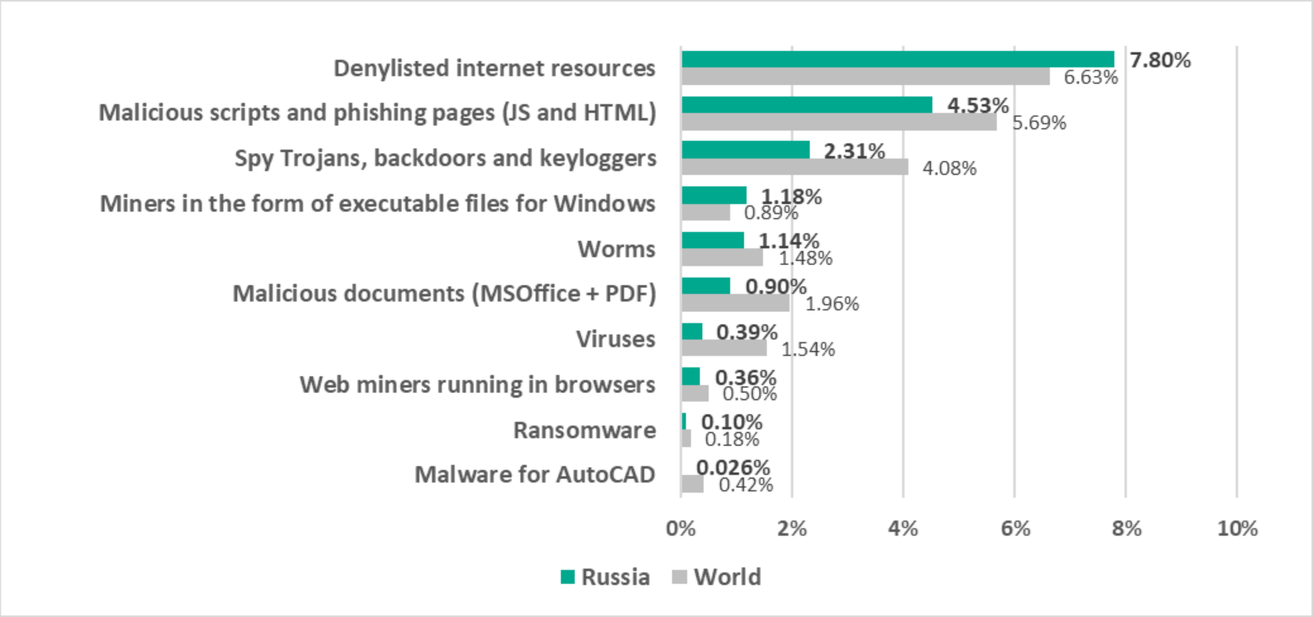
Russia occupies **leading positions** among regions by percentage of ICS computers on which the following were blocked:

- First place – denylisted internet resources
- Second place – miners in the form of executable files for Windows
- Third place – threats from the internet

Threat categories

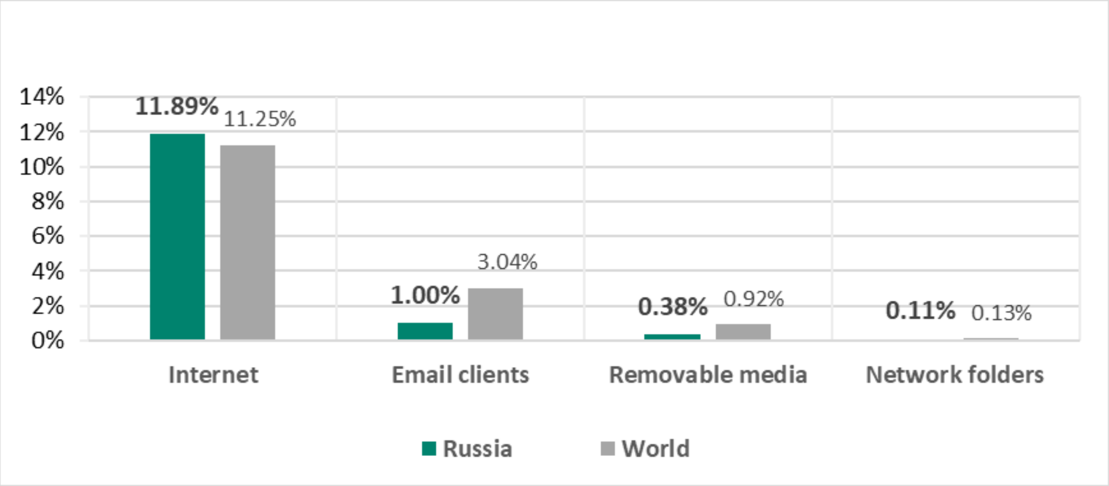
Compared to global figures, the region has a higher percentage of ICS computers on which the following threat categories were blocked:

- Miners in the form of executable files for Windows, 1.3 times higher
- Denylisted internet resources, 1.2 times higher



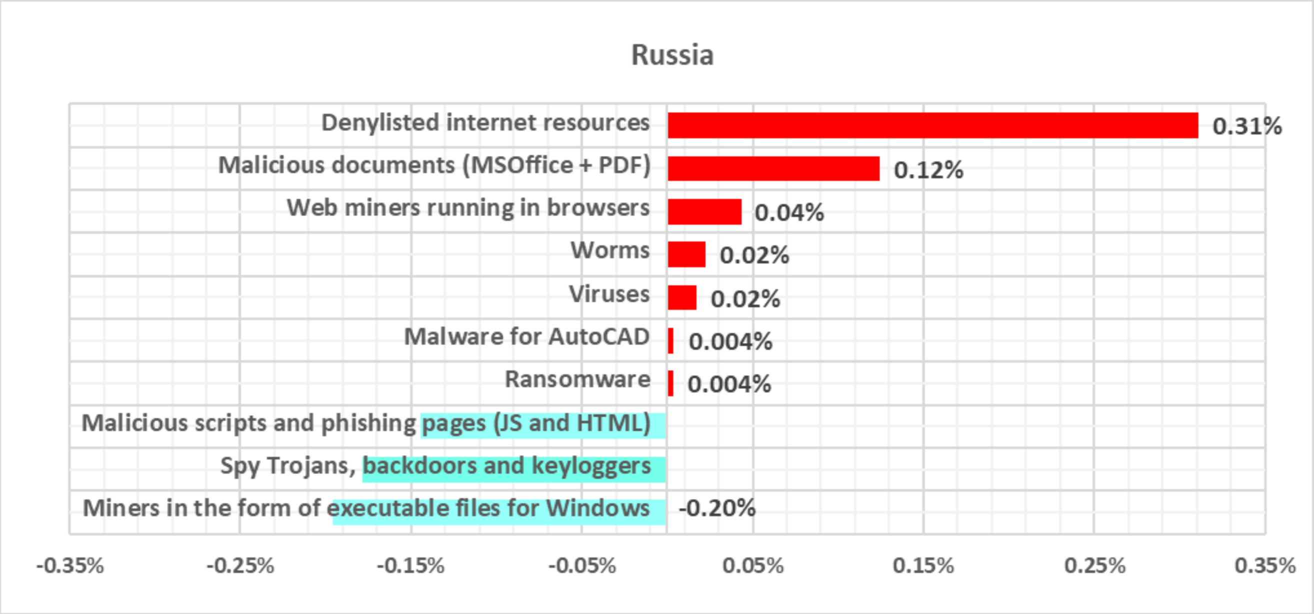
Threat sources

The region ranked **third in the world** by percentage of ICS computers on which malicious threats from the **internet** were blocked.

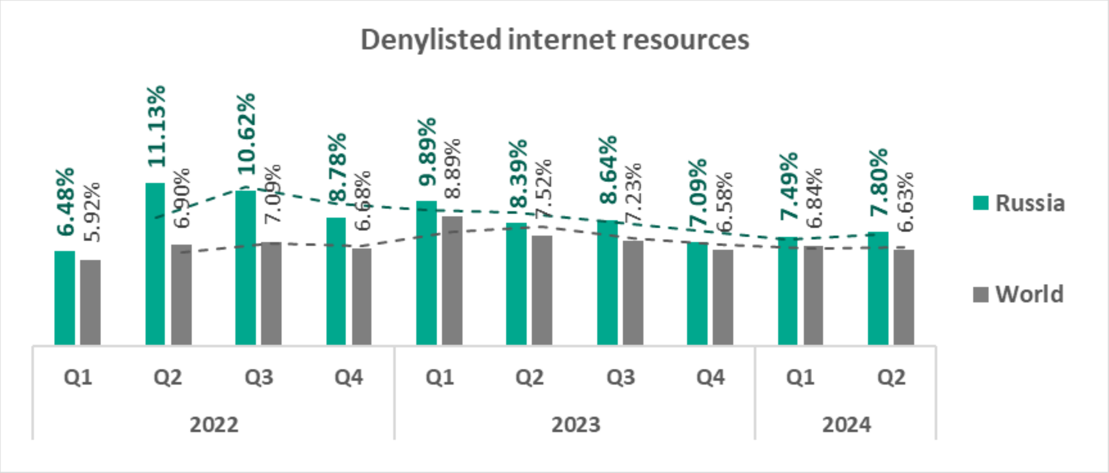


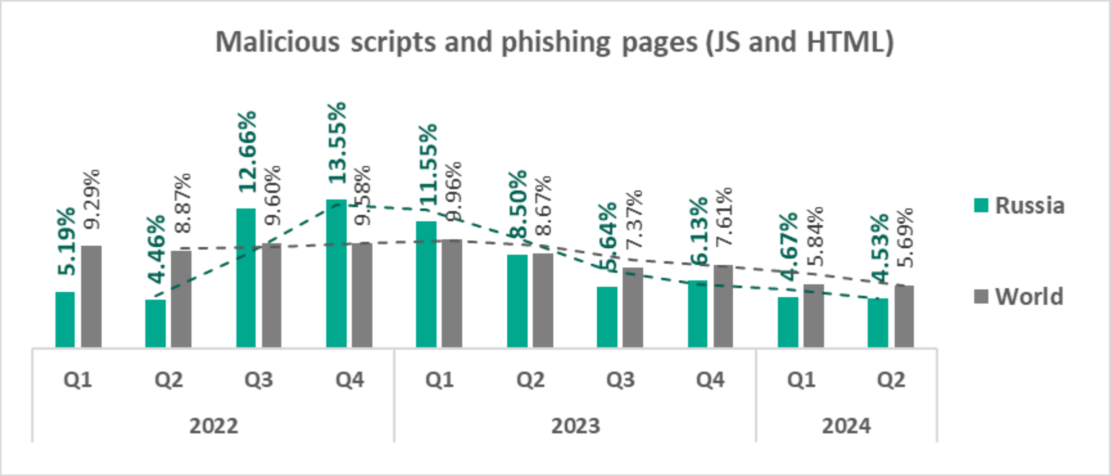
Quarterly changes and trends

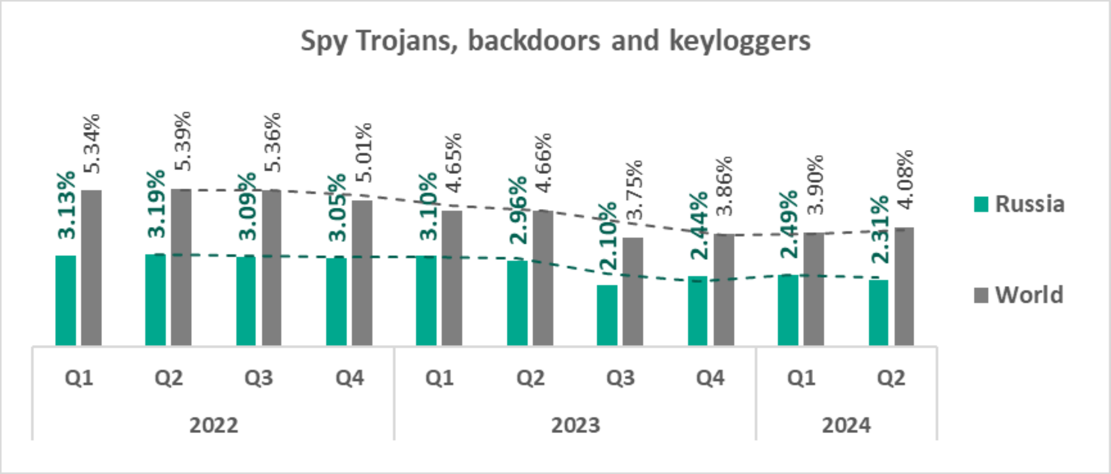
Threat categories

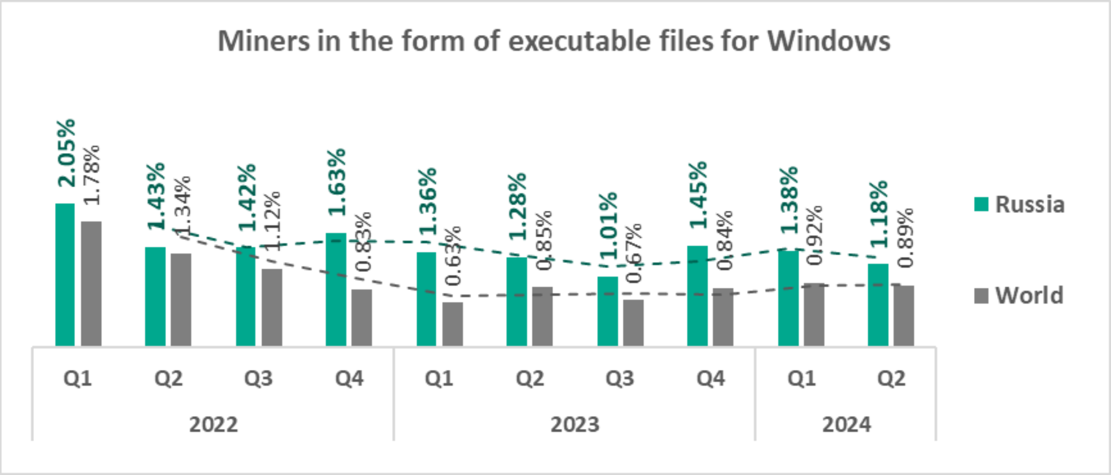


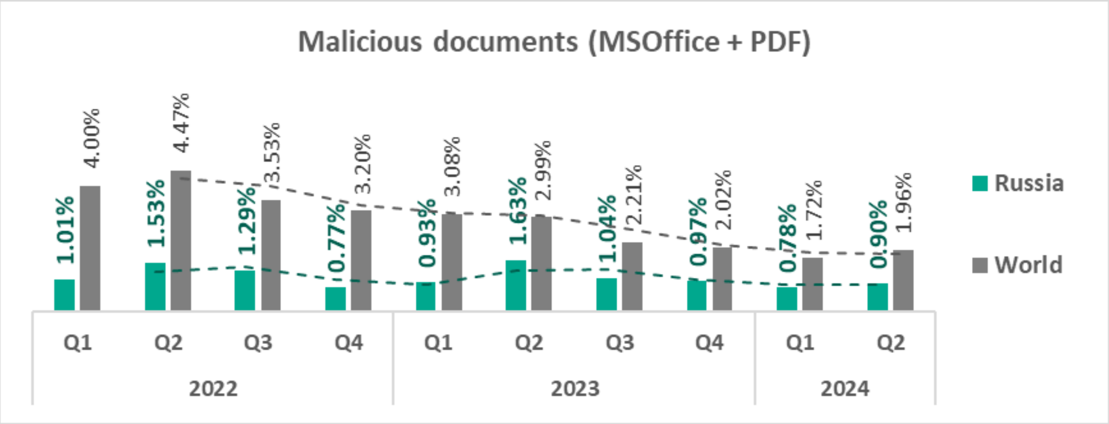
- The **largest proportional quarterly increase** in Q2 2024 was in the percentage of ICS computers on which the following were blocked:
  - Malicious documents, by 1.2 times.
  - Malware for AutoCAD, by 1.2 times.
- The **top threat** categories exhibit various quarterly dynamics:




Malicious scripts and phishing pages (JS and HTML)


Spy Trojans, backdoors and keyloggers


Miners in the form of executable files for Windows

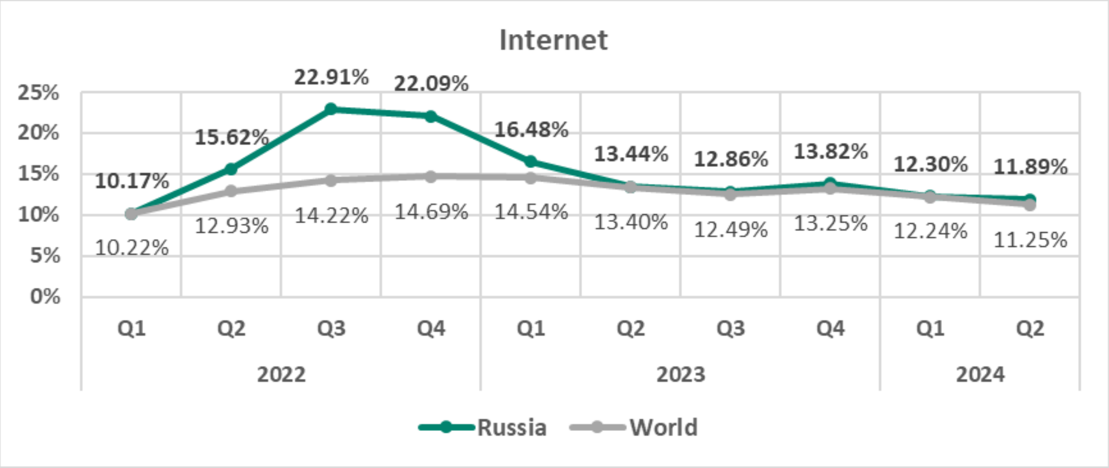


- The heatmap below illustrates changes in the rankings of threat categories in the region over a period of 2.5 years. **Denylisted internet resources** have been the leading threat category in the region since Q3 2023.

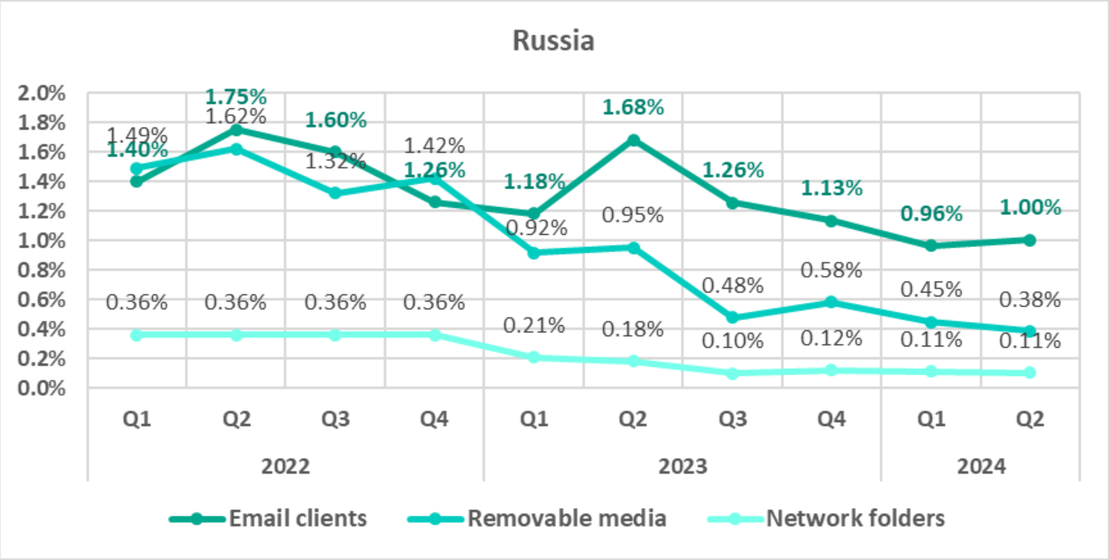
Russia	2022				2023				2024	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Denylisted internet resources	1	1	2	2	2	2	1	1	1	1
Malicious scripts and phishing pages (JS and HTML)	2	2	1	1	1	1	2	2	2	2
Spy Trojans, backdoors and keyloggers	3	3	3	3	3	3	3	3	3	3
Miners in the form of executable files for Windows	4	5	4	4	4	5	5	4	4	4
Worms	5	6	6	5	5	7	6	5	5	5
Malicious documents (MSOffice + PDF)	7	4	5	7	7	4	4	6	6	6
Viruses	8	8	8	8	8	8	8	8	7	7
Web miners running in browsers	6	7	7	6	6	6	7	7	8	8
Ransomware	9	9	9	9	9	9	9	9	9	9
Malware for AutoCAD	10	10	10	10	10	10	10	10	10	10

Threat sources

- Threats from the **internet** (by percentage of ICS computers where they were blocked) have exhibited a slightly oscillating downward trend since Q4 2022 and have remained very close to the global average since Q2 2023.

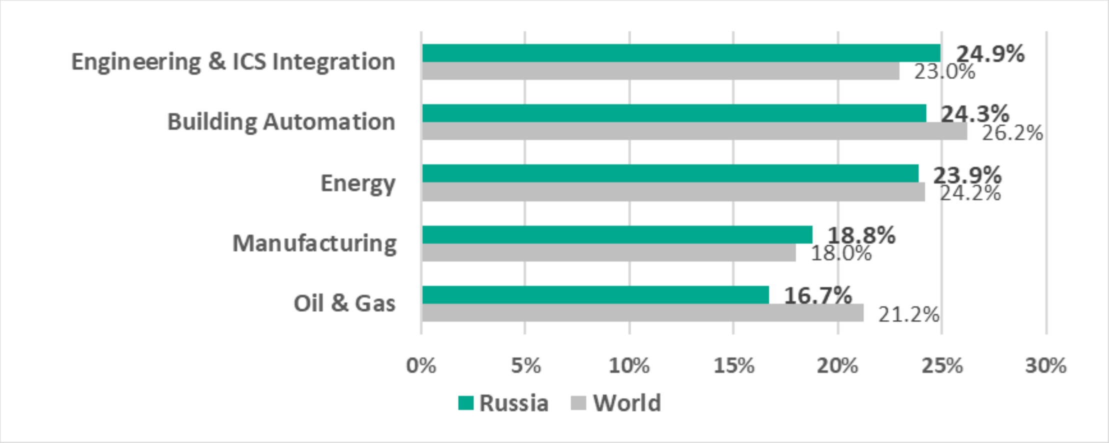


- Other threat sources also exhibit predominantly downward trends.

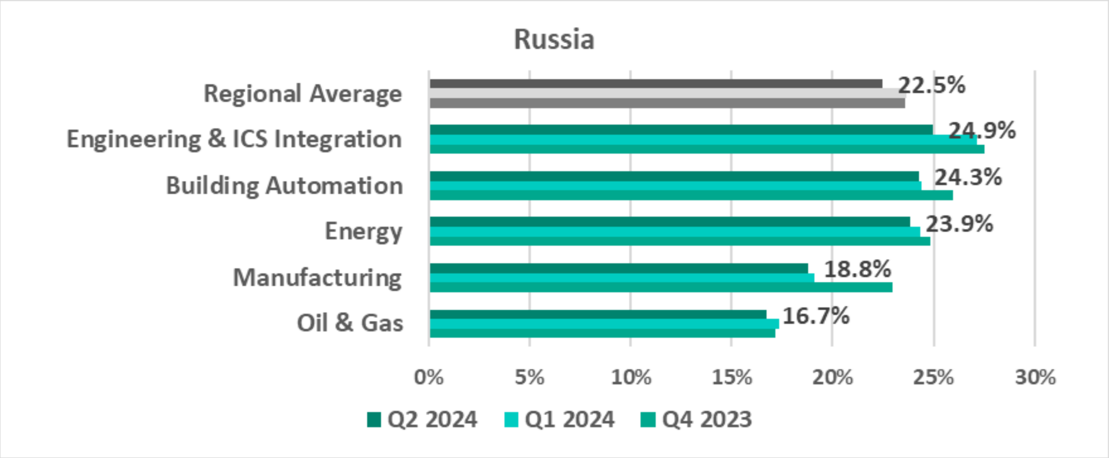


Industries

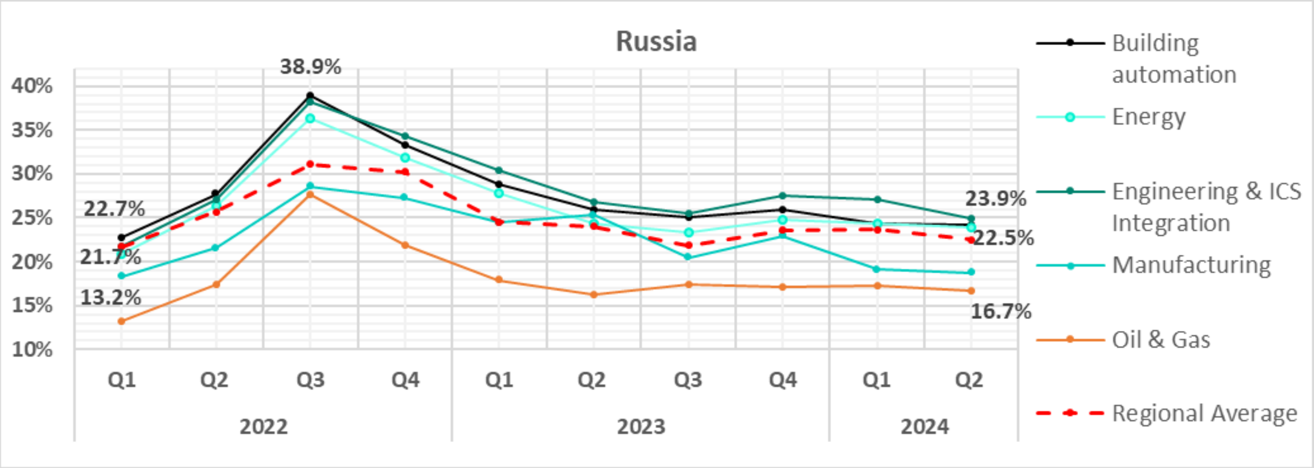
- The most **affected industries** in the region, as selected for this report, are:
  - ➢ Engineering and ICS integration
  - ➢ Building automation
  - ➢ Energy
- Compared to the **global averages**, the following industries had a higher percentage of ICS computers on which malicious objects were blocked:
  - ➢ Engineering and ICS Integration, 1.1 times higher
  - ➢ Manufacturing, slightly higher



- In **Q2 2024**, all the selected industries in the region exhibited a decrease in the percentage of ICS computers on which malicious objects were blocked.



- The selected sectors have shown mostly positive dynamics in their long-term **trends** since Q4 2022:



Latin America

Current threats

-1-

Malicious scripts and phishing pages

6.69%

▼ decrease in Q2

1.2x above global average

-2-

Denylisted internet resources

5.54%

▼ decrease in Q2

-3-

Spyware

4.77%

▲ slight increase in Q2

1.2x above global average

Malicious documents

3.23%

▲ **1.1x** increase in Q2

1.7x above global average

2nd in the world

Web miners

0.68%

▲ **1.2x** increase in Q2

1.4x above global average

3rd in the world

1st in the world **in terms of growth**

Ransomware

0.22%

▲**1.7x** increase in Q2

1.2x above global average

3rd in the world

1st in the world **in terms of growth**

Threats from

Internet

10.56%

▼ decrease in Q2

Threats from

Email clients

4.79%

▼ decrease in Q2

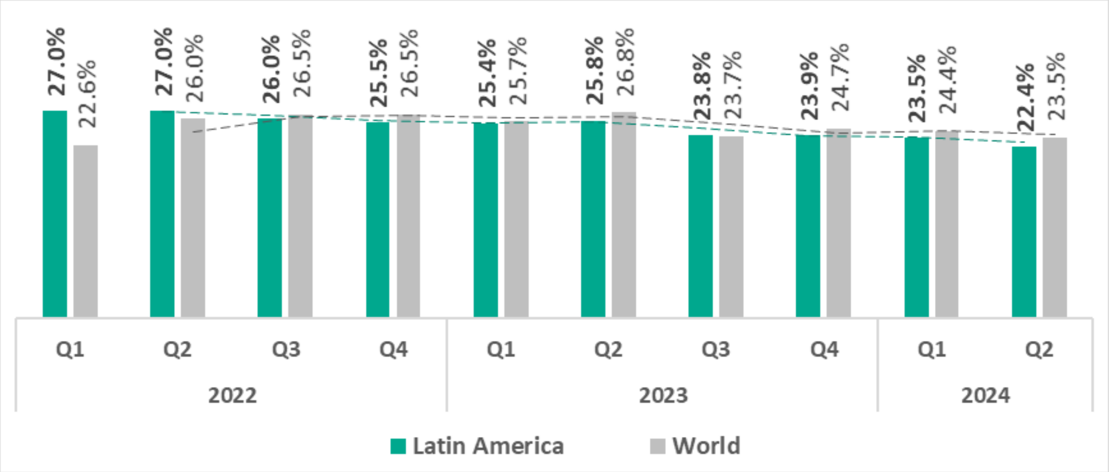
1.6x above global average

3rd in the world

Overall

Seventh place in the global ranking by percentage of ICS computers on which malicious objects were blocked. The region demonstrates a downward trend.

The percentage of ICS computers on which malicious objects were blocked has been slightly below the global average throughout the observed period, except at the beginning of 2022.



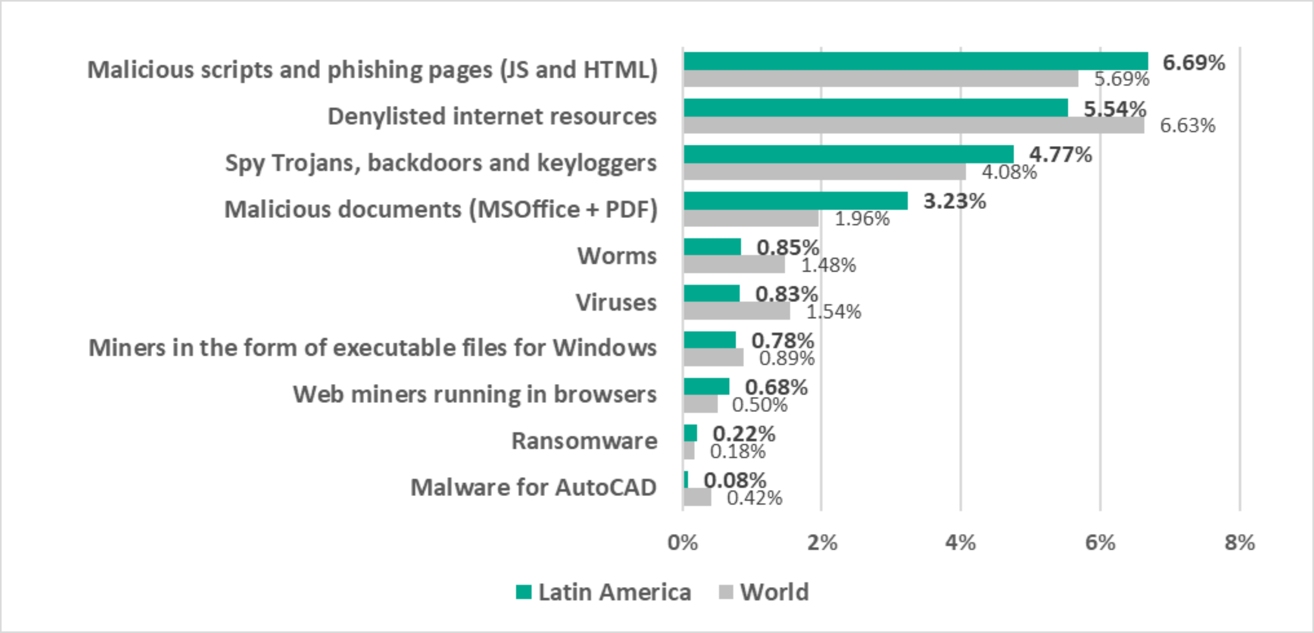
Comparative analysis

- Latin America occupies **leading positions** among regions by percentage of ICS computers on which the following were blocked:
  - Second place – malicious documents
  - Third place – web miners, ransomware, threats from email clients

Threat categories

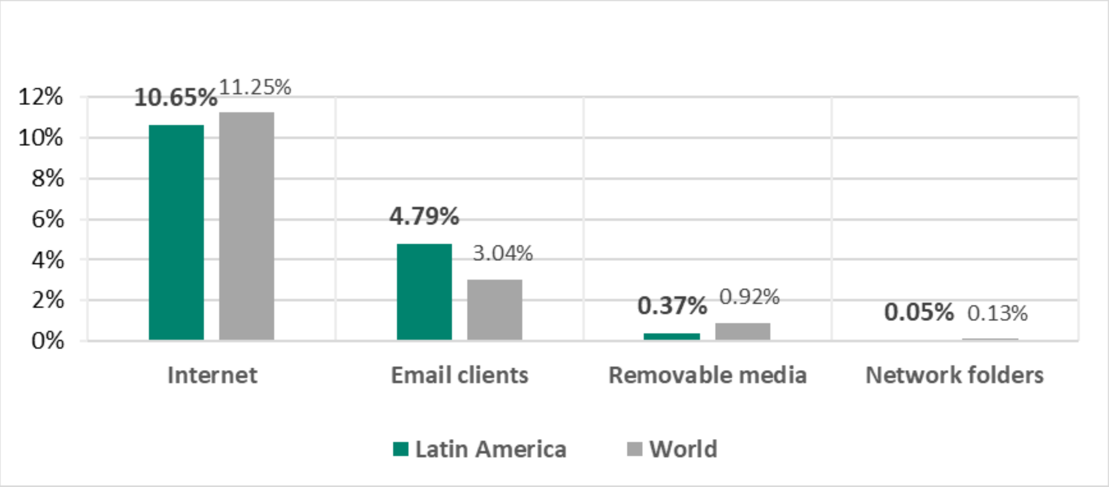
Compared to global figures, the region has a higher percentage of ICS computers on which the following threat categories were blocked:

- Malicious documents, 1.7 times higher
- Web miners, 1.4 times higher
- Malicious scripts and phishing pages, 1.2 times higher
- Spyware, 1.2 times higher
- Ransomware, 1.2 times higher



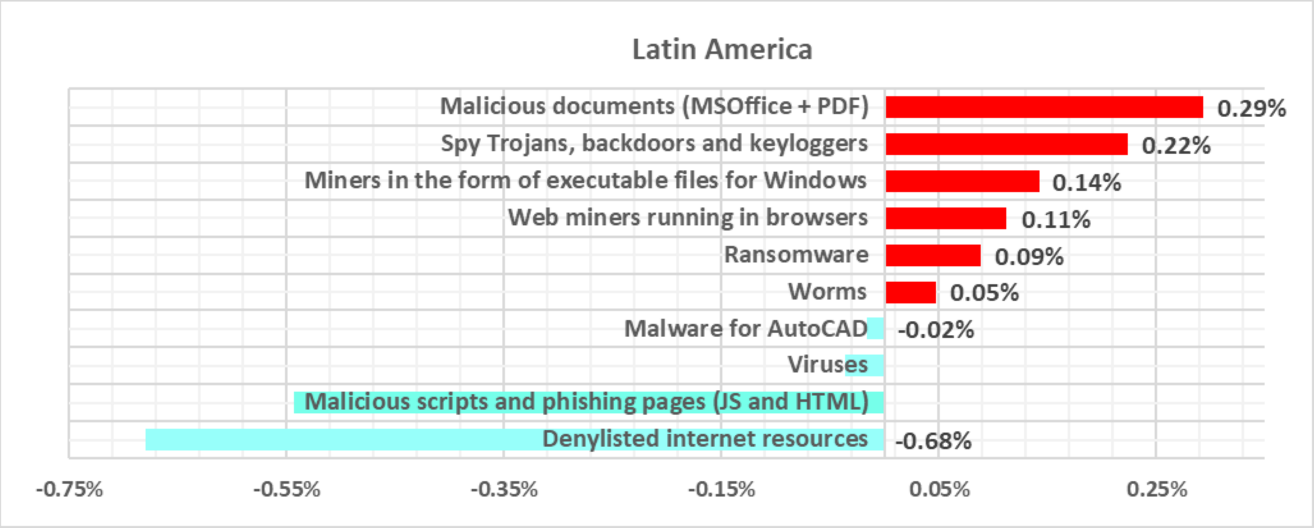
Threat sources

The region ranked **third in the world** by percentage of ICS computers on which malicious threats from **email clients** were blocked, exceeding the global average by 1.6 times.

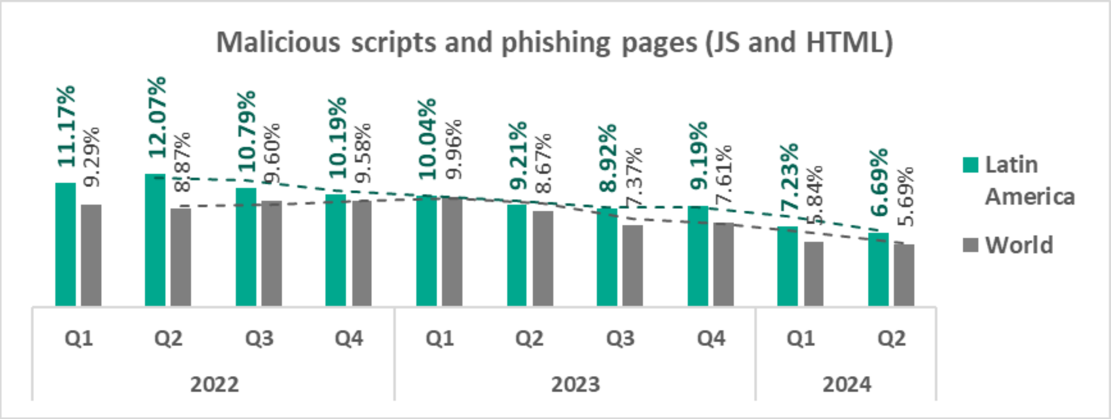


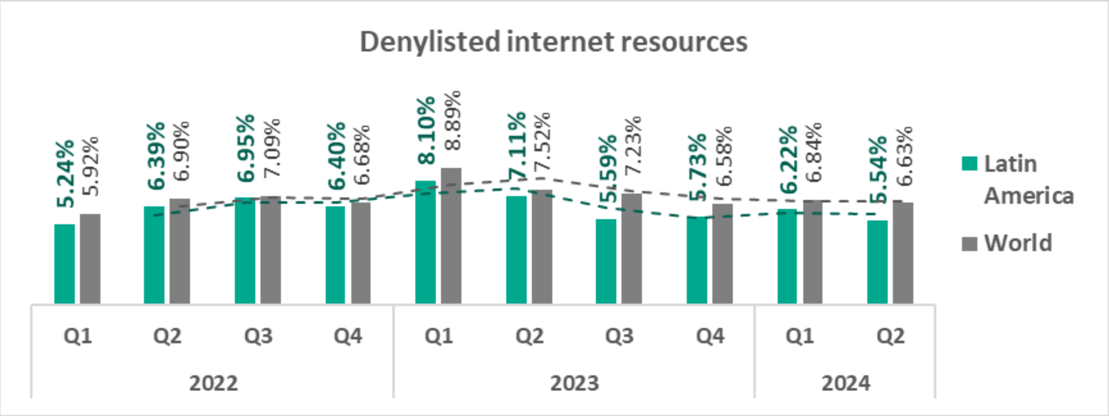
Quarterly changes and trends

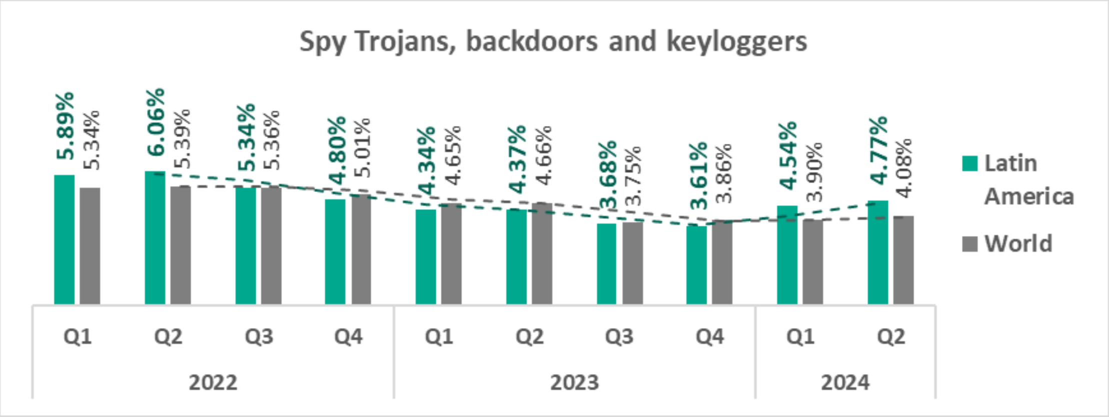
Threat categories

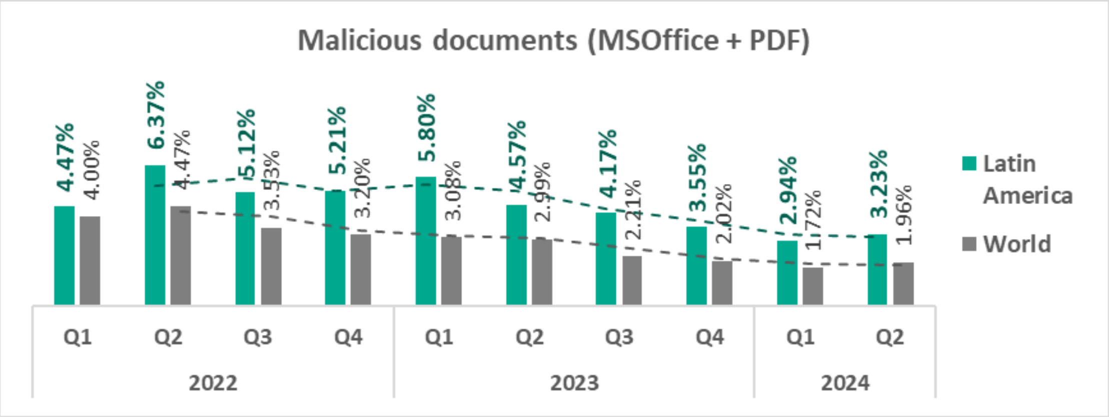


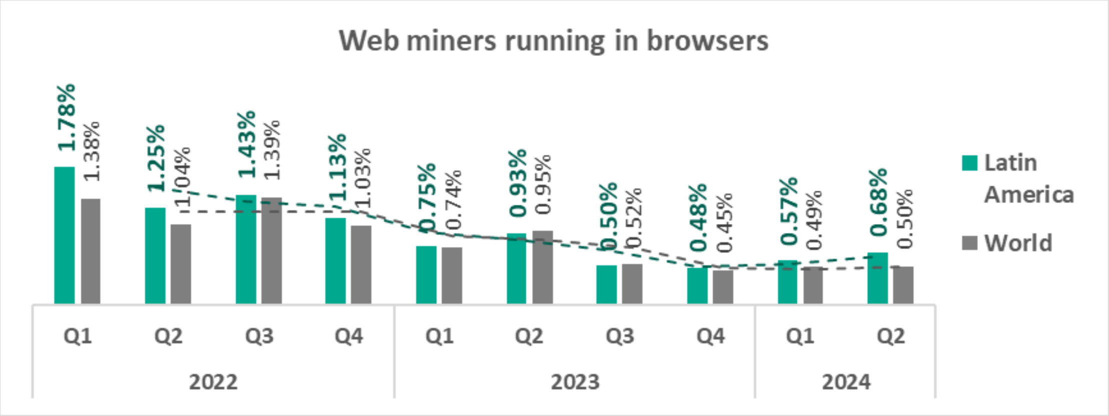
- The **largest quarterly increase** was in the percentage of ICS computers on which the following were blocked:
  - ➢ Ransomware – by 1.7 times
  - ➢ Web miners running in browsers – by 1.2 times
  - ➢ Miners in the form of executable files for Windows – by 1.2 times.
- The **top threat** categories exhibit various quarterly dynamics:

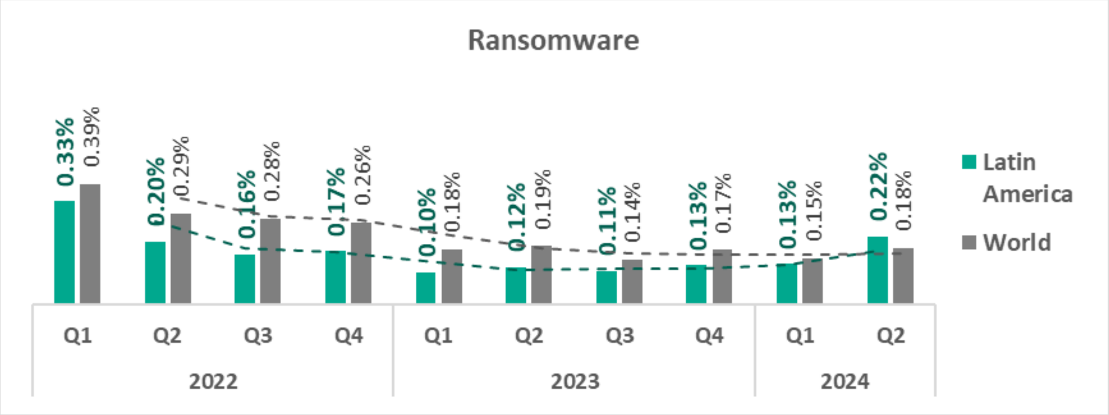



Denylisted internet resources
5.24%
5.92%
6.39%
6.90%
6.95%
7.09%
6.40%
6.68%
8.10%
8.89%
7.11%
7.52%
5.59%
7.23%
5.73%
6.58%
6.22%
6.84%
5.54%
6.63%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
Latin America
World


Spy Trojans, backdoors and keyloggers
5.89%
5.34%
6.06%
5.39%
5.34%
5.36%
4.80%
5.01%
4.34%
4.65%
4.37%
4.66%
3.68%
3.75%
3.61%
3.86%
4.54%
3.90%
4.77%
4.08%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
Latin America
World


Malicious documents (MSOffice + PDF)
4.47%
4.00%
6.37%
4.47%
5.12%
3.53%
5.21%
3.20%
5.80%
3.08%
4.57%
2.99%
4.17%
2.21%
3.55%
2.02%
2.94%
1.72%
3.23%
1.96%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
Latin America
World


Web miners running in browsers
1.78%
1.38%
1.25%
1.04%
1.43%
1.39%
1.13%
1.03%
0.75%
0.74%
0.93%
0.95%
0.50%
0.52%
0.48%
0.45%
0.57%
0.49%
0.68%
0.50%
Q1
Q2
Q3
Q4
2022
Q1
Q2
Q3
Q4
2023
Q1
Q2
2024
Latin America
World

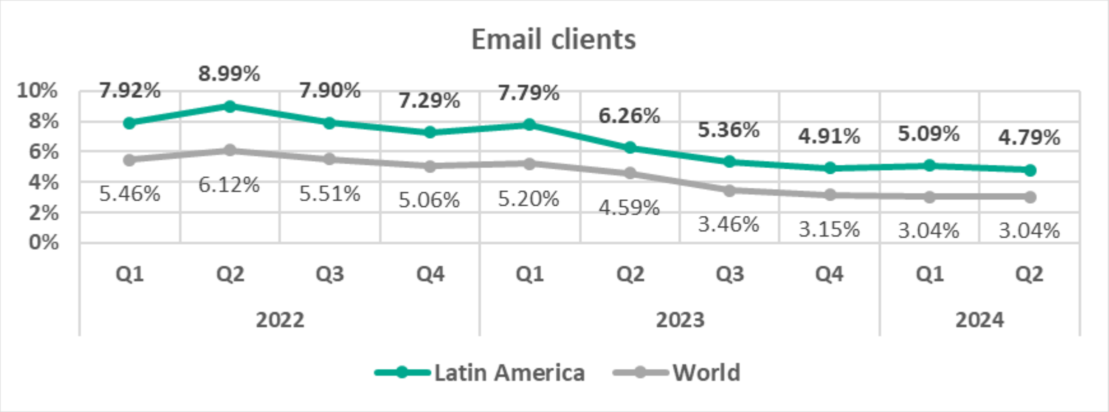

Ransomware
0.33%
0.39%
0.20%
0.29%
0.16%
0.28%
0.17%
0.26%
0.10%
0.18%
0.12%
0.19%
0.11%
0.14%
0.13%
0.17%
0.13%
0.15%
0.22%
0.18%
Q1
Q2
Q3
Q4
2022
Q1
Q2
Q3
Q4
2023
Q1
Q2
2024
Latin America
World

- The heatmap below illustrates changes in the rankings of threat categories in the region over a period of 2.5 years. **Malicious scripts and phishing pages** have been the leading threat category in the region throughout the observed period. **Spyware** moved up from fourth to third place in Q4 2023 and has held that position since.

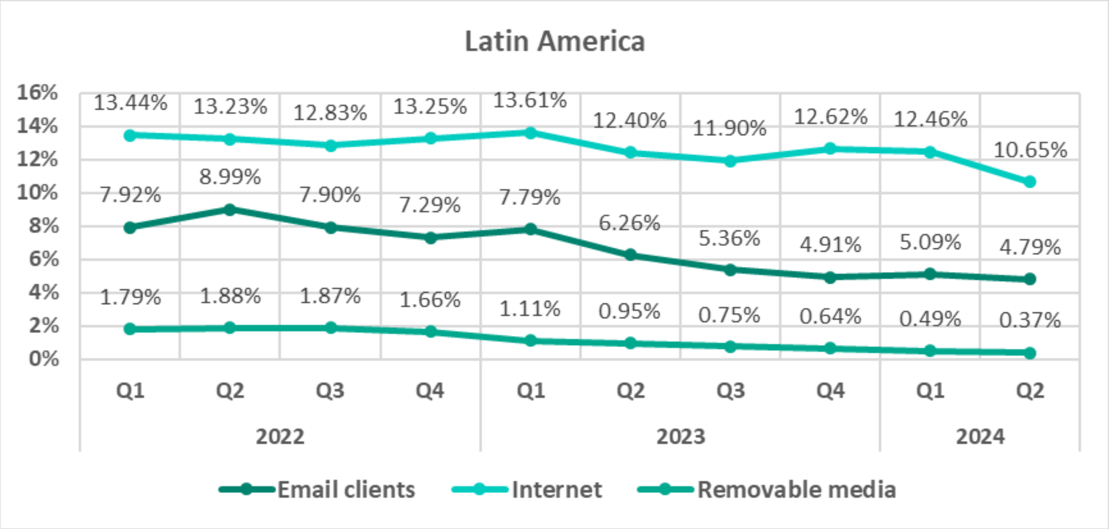
Latin America	2022				2023				2024	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Malicious scripts and phishing pages (JS and HTML)	1	1	1	1	1	1	1	1	1	1
Denylisted internet resources	3	2	2	2	2	2	2	2	2	2
Spy Trojans, backdoors and keyloggers	2	4	3	4	4	4	4	3	3	3
Malicious documents (MSOffice + PDF)	4	3	4	3	3	3	3	4	4	4
Worms	7	6	6	6	5	5	5	5	6	5
Viruses	8	8	8	7	6	6	6	6	5	6
Miners in the form of executable files for Windows	5	5	7	8	8	8	8	7	7	7
Web miners running in browsers	6	7	5	5	7	7	7	8	8	8
Ransomware	9	9	9	9	9	9	9	9	9	9
Malware for AutoCAD	10	10	10	10	10	10	10	10	10	10

Threat sources

- Threats from **email clients** (in terms of percentage of ICS computers where they were blocked) exhibit a downward trend consistent with the global trend, but noticeably above the global average.

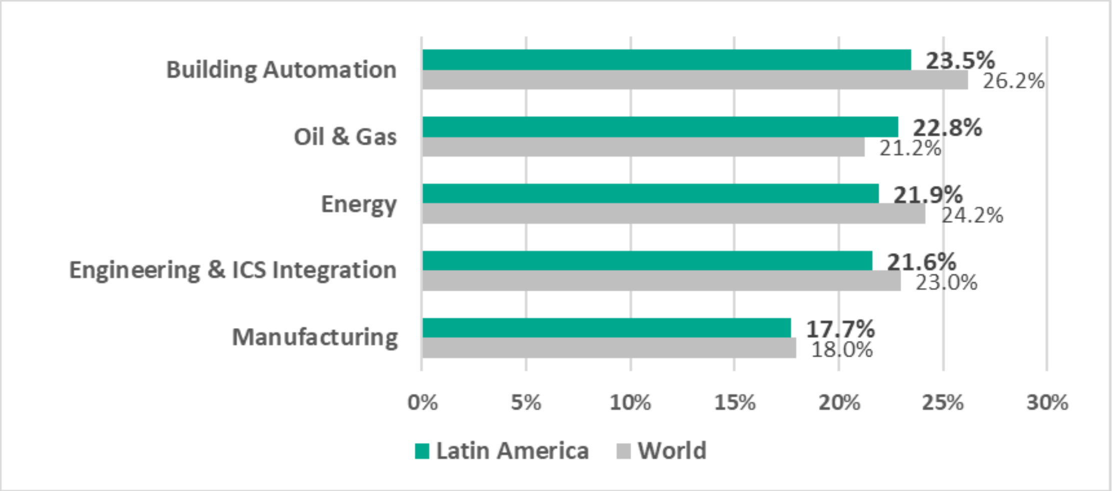


- Overall, all major sources exhibit downward trends.

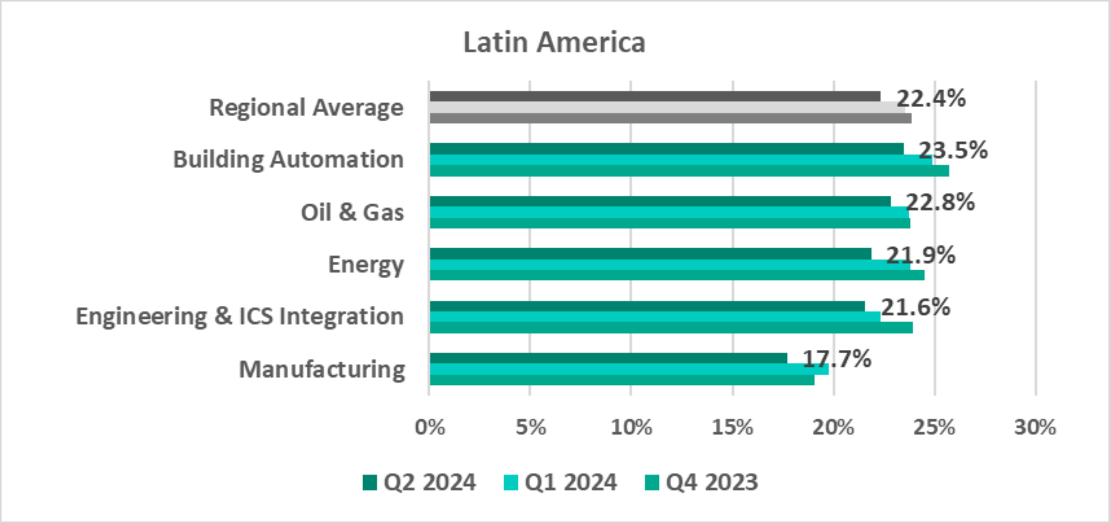


Industries

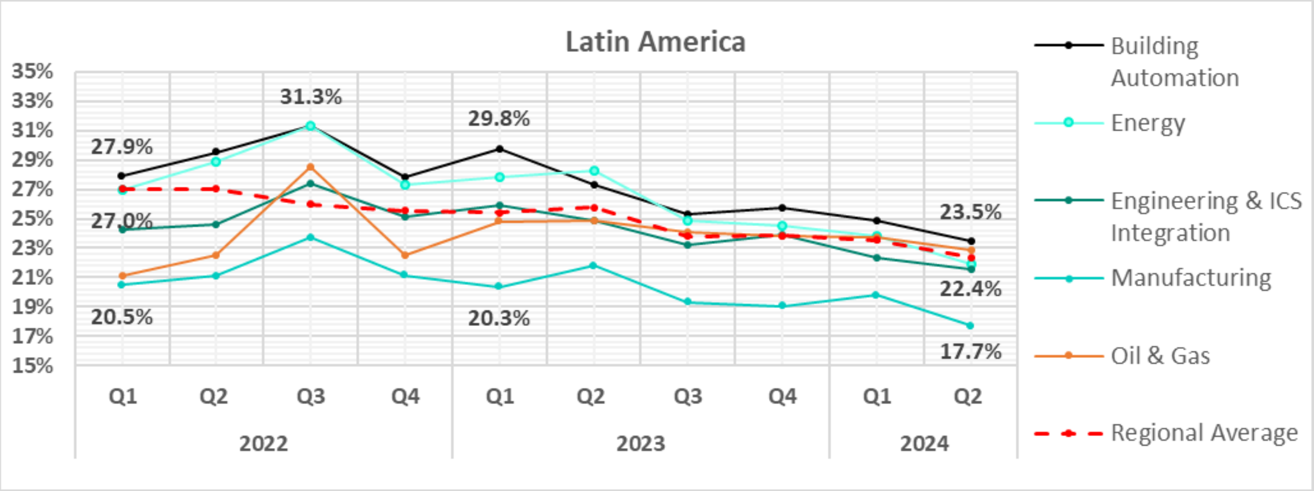
- The most **affected industry** in the region, as selected for this report, was **building automation.**
- From a **global perspective**, the percentage of ICS computers on which malicious objects were blocked in the oil and gas industry was 1.1 times higher than the sector's global average.



- In **Q2 2024**, all selected sectors in the region exhibited a decrease in the percentage of ICS computers on which malicious objects were blocked.



- The selected sectors have shown mostly positive dynamics in their long-term **trends** since Q1 2023:



South Asia

Current threats

-1-

Denylisted internet resources

6.33%

▼ decrease in Q2

-2-

Malicious scripts and phishing pages

5.57%

▼ decrease in Q2

-3-

Spyware

2.98%

▲ slight increase in Q2

Worms

1.74%

▼ decrease in Q2
1.2x above global average

Viruses

1.69%

▼ decrease in Q2
1.1x above global average

Ransomware

0.22%

▼ decrease in Q2
1.6x above global average
3rd in the world

Threats from
Internet

10.94%

▼ decrease in Q2

Threats from
Removable devices

1.94%

▼ decrease in Q2
2.1x above global average
2nd in the world

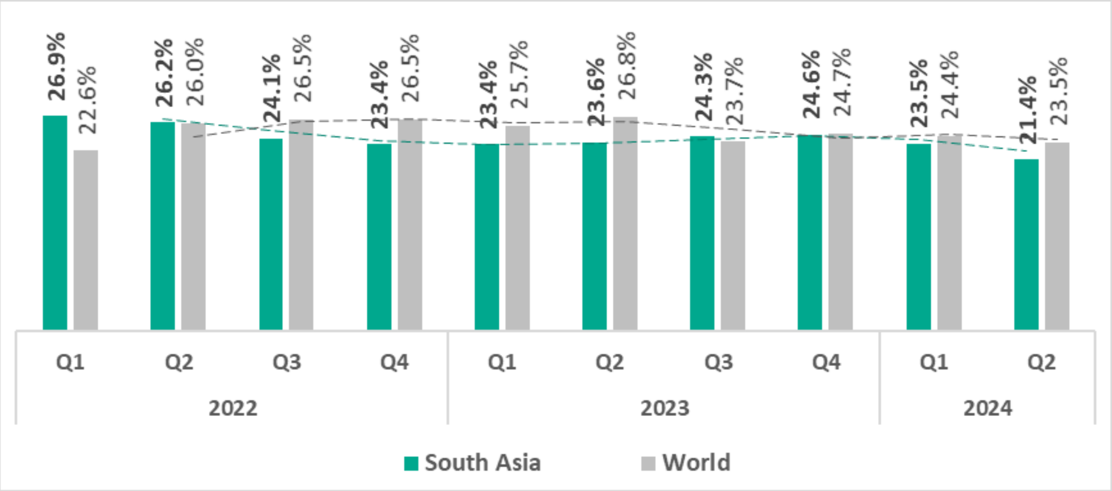
Threats from
Network folders

0.21%

▼ decrease in Q2
1.6x above global average
3rd in the world

Overall

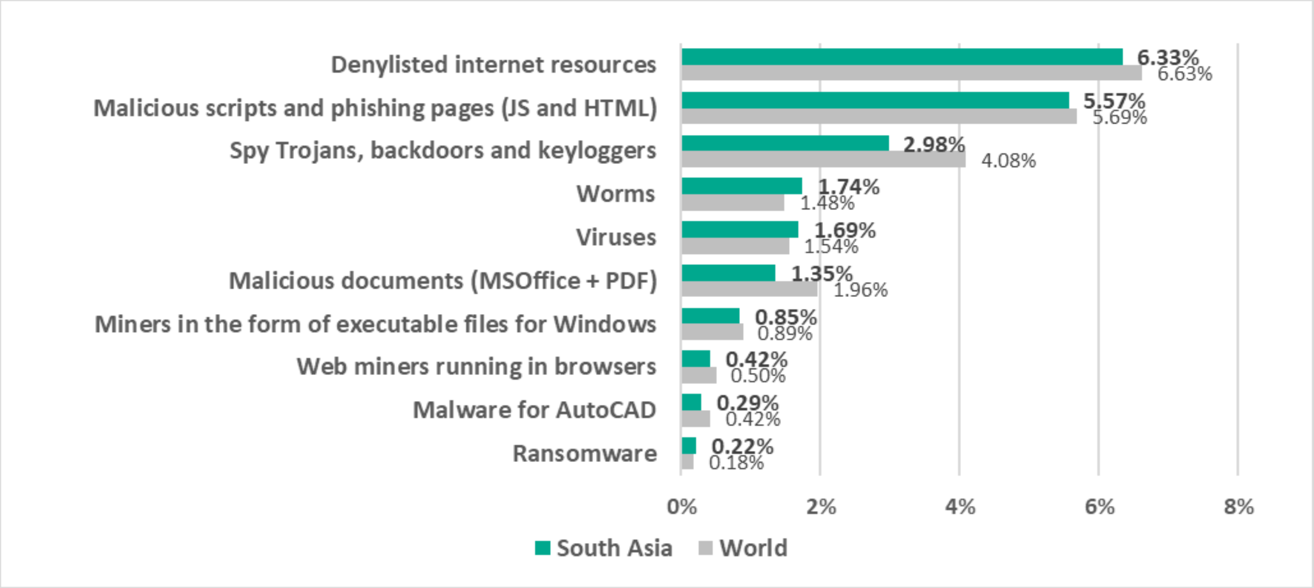
Eighth place in the global ranking by percentage of ICS computers on which malicious objects were blocked. The region demonstrates a slow downward trend with some fluctuations. The percentage of ICS computers on which malicious objects were blocked has been below the global average since Q4 2023.



Comparative analysis

- South Asia occupies **leading positions** among regions by percentage of ICS computers on which the following were blocked:
  - ➢ Second place – threats from removable devices
  - ➢ Third place – ransomware, threats from network folders

Threat categories

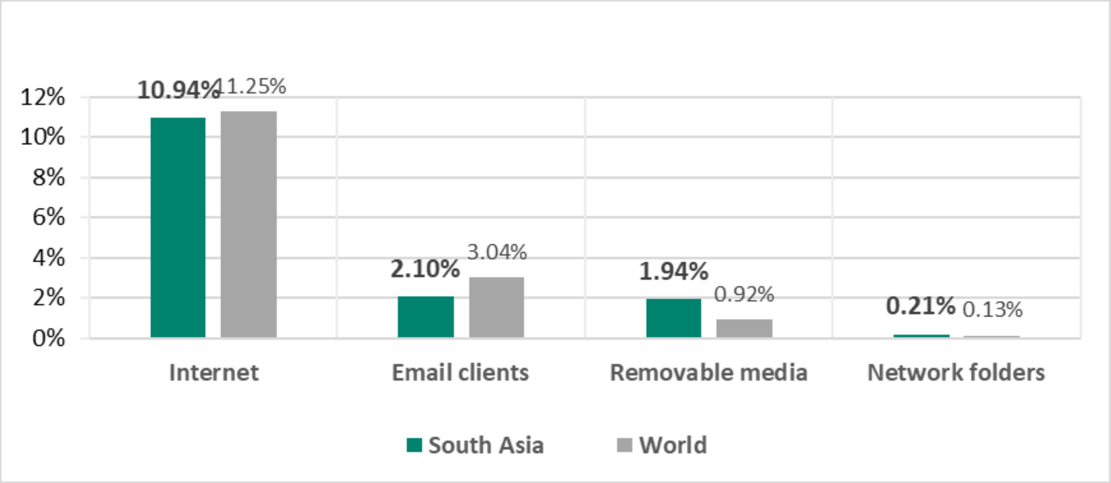


- **Compared to the global average**, the region has a noticeably higher percentage of ICS computers on which the following were blocked:
  - Ransomware, 1.2 times higher
  - Worms, 1.2 times higher. Worms ranked fourth in the regional ranking of threat categories by percentage of ICS computers on which they were blocked (sixth globally)
  - Viruses, 1.1 times higher

Threat sources

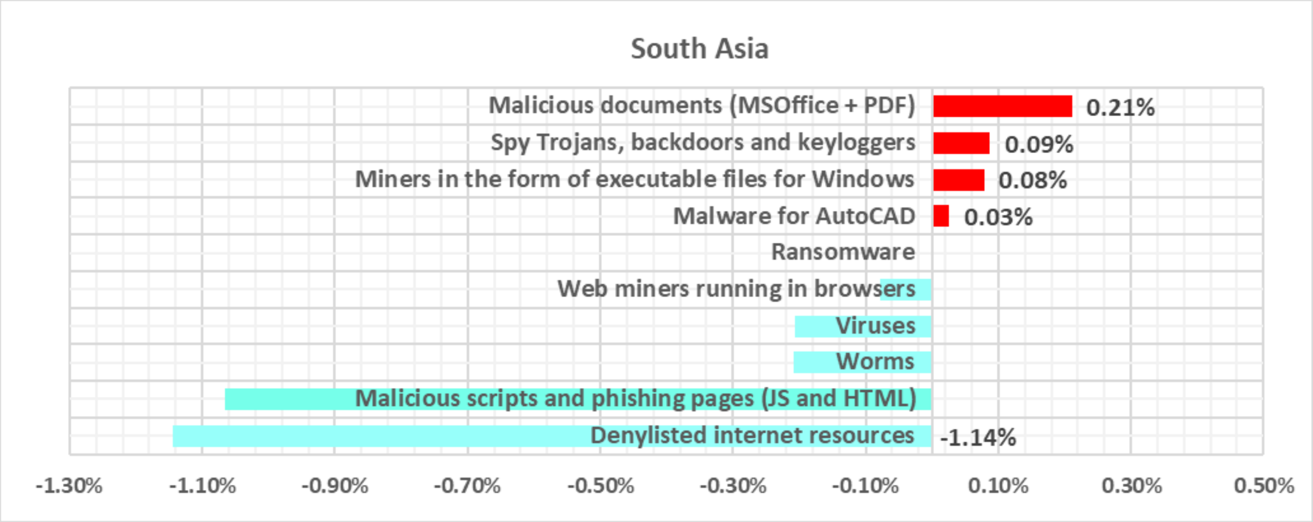
South Asia ranks **second globally** by percentage of ICS computers on which malicious threats from **removable devices** were blocked, surpassing the global average by 2.1 times.

Additionally, the region is **third** in the global ranking for the percentage of ICS computers on which malicious threats from **network folders** were blocked, exceeding the global average by a factor of 1.6.



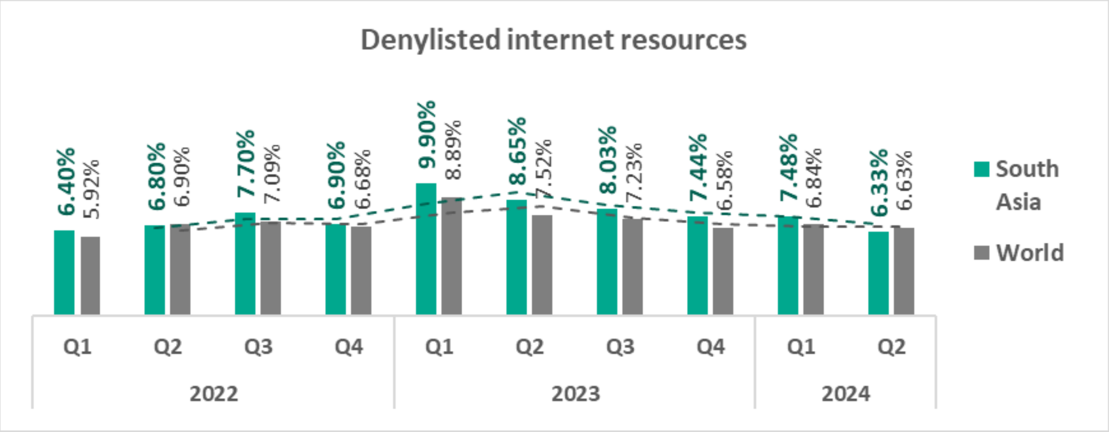
Quarterly changes and trends

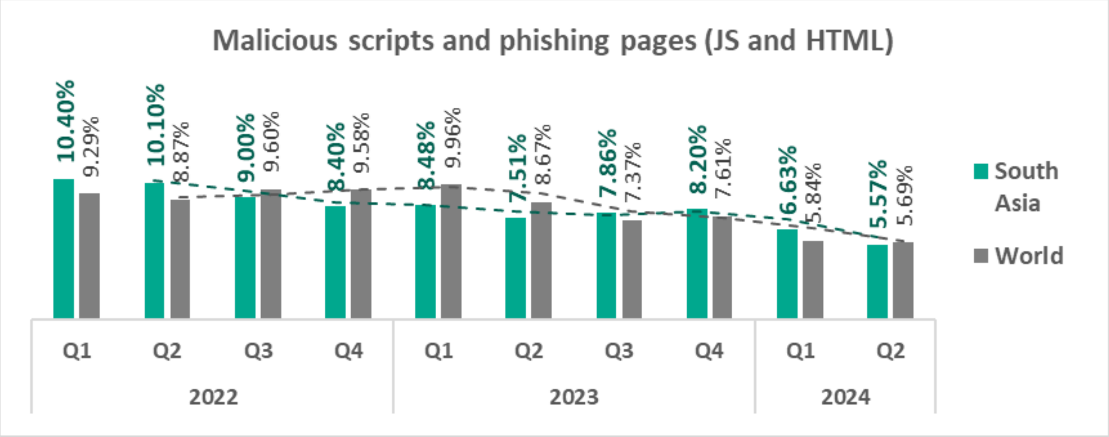
Threat categories

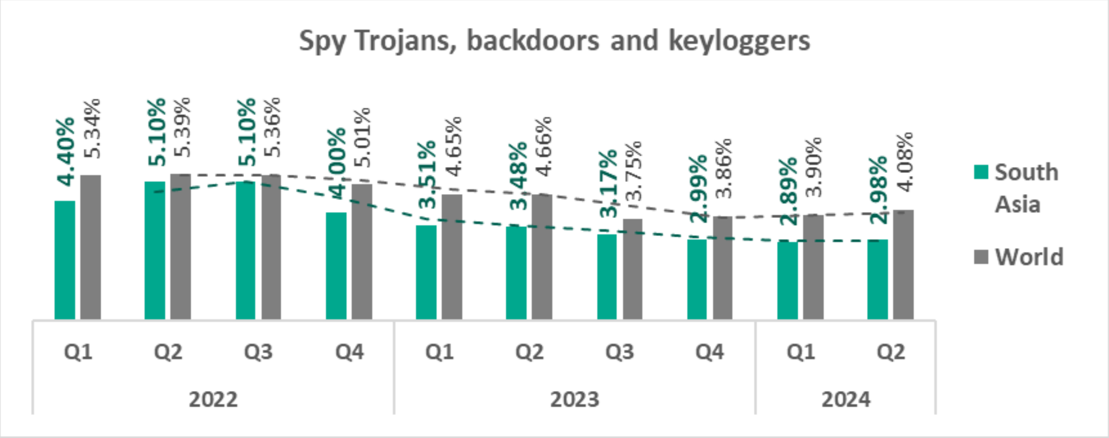


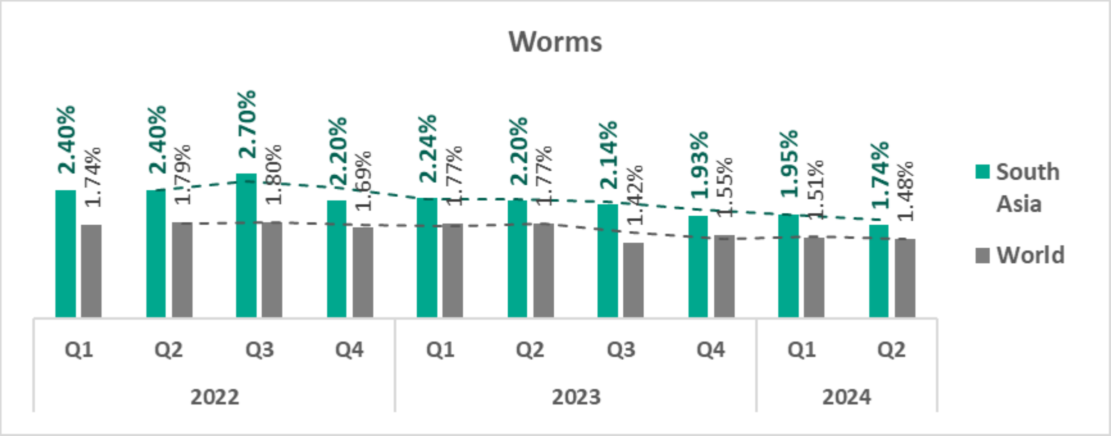
- The **largest quarterly increase** was in the percentage of ICS computers on which the following were blocked:
  - Malicious documents, by 1.2 times
  - Miners in the form of executable files for Windows, by 1.1 times
  - Malware for AutoCAD, by 1.1 times

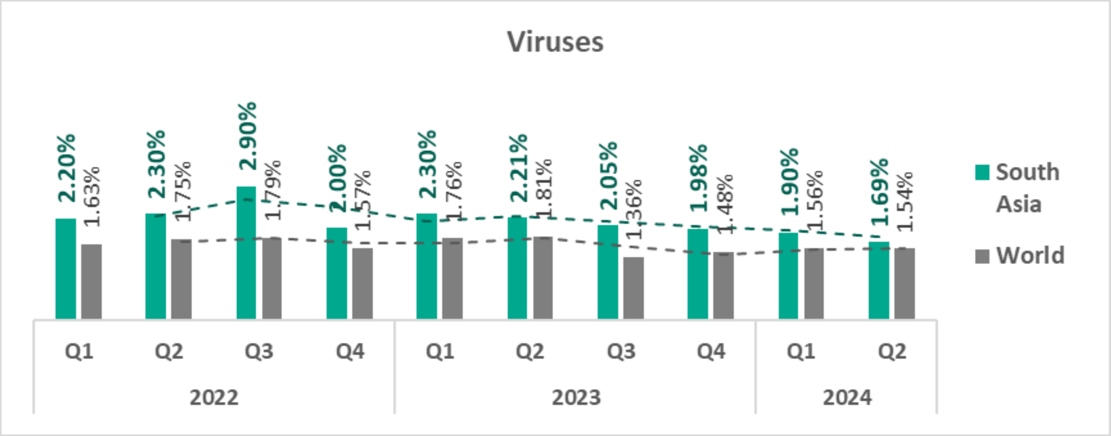
- **The top threat** categories exhibit various quarterly dynamics:

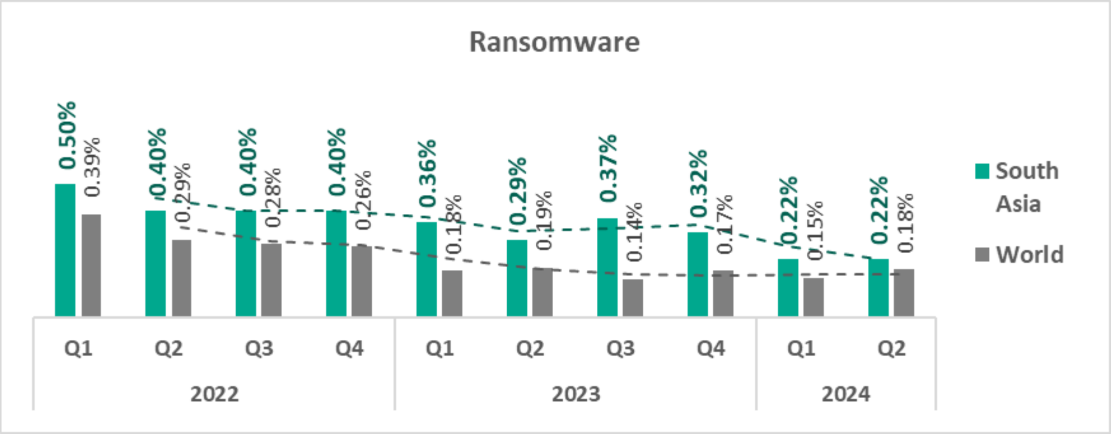

Denylisted internet resources


Malicious scripts and phishing pages (JS and HTML)


Spy Trojans, backdoors and keyloggers


Worms
2.40%
1.74%
2.40%
1.79%
2.70%
1.80%
2.20%
1.69%
2.24%
1.77%
2.20%
1.77%
2.14%
1.42%
1.93%
1.55%
1.95%
1.51%
1.74%
1.48%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
🟩 South Asia
■ World


Viruses
2.20%
1.63%
2.30%
1.75%
2.90%
1.79%
2.00%
1.57%
2.30%
1.76%
2.21%
1.81%
2.05%
1.36%
1.98%
1.48%
1.90%
1.56%
1.69%
1.54%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
🟩 South Asia
■ World


Ransomware
0.50%
0.39%
0.40%
0.29%
0.40%
0.28%
0.40%
0.26%
0.36%
0.18%
0.29%
0.19%
0.37%
0.14%
0.32%
0.17%
0.22%
0.15%
0.22%
0.18%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
🟩 South Asia
■ World

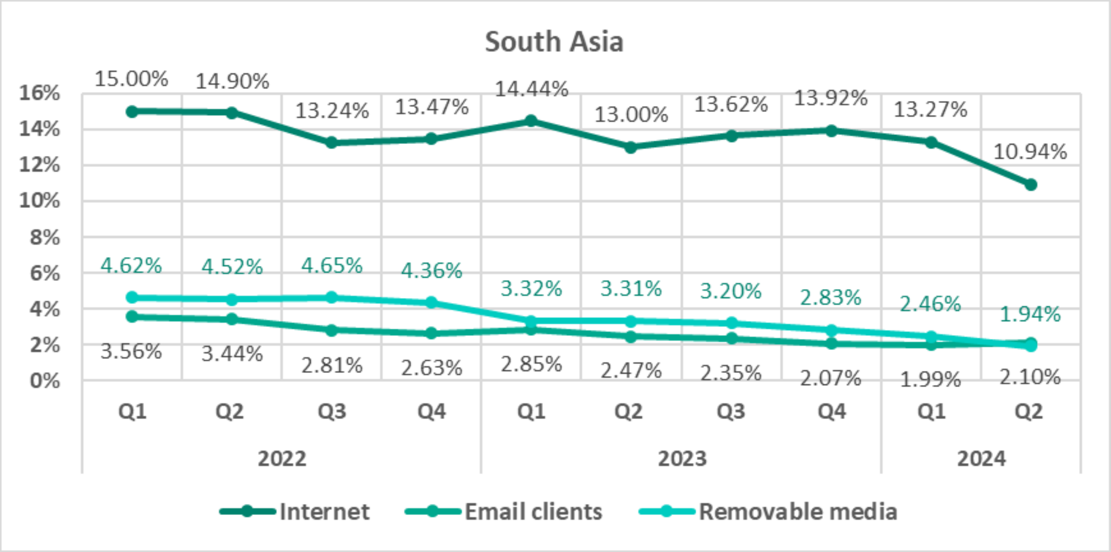
- The heat map below illustrates changes in the rankings of threat categories in the region over a period of 2.5 years. **Denylisted internet resources** have been the leading threat category in the region since Q1 2023, with the exception of Q4 2023. **Malicious scripts and phishing pages** have ranked second since Q1 2023 with the exception of Q4 2023 when they were in first place. **Viruses** and **worms** have consistently ranked high throughout the observed period, mostly alternating between fourth and fifth place.

South Asia	2022				2023				2024	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Denylisted internet resources	2	2	2	2	1	1	1	2	1	1
Malicious scripts and phishing pages (JS and HTML)	1	1	1	1	2	2	2	1	2	2
Spy Trojans, backdoors and keyloggers	3	3	3	3	3	3	3	3	3	3
Worms	5	5	5	4	5	5	4	5	4	4
Viruses	6	6	4	6	4	4	5	4	5	5
Malicious documents (MSOffice + PDF)	4	4	5	5	6	6	6	6	6	6
Miners in the form of executable files for Windows	7	7	8	7	7	7	7	7	7	7
Web miners running in browsers	8	8	7	7	9	8	8	8	8	8
Malware for AutoCAD	10	9	9	9	8	9	10	10	9	9
Ransomware	9	9	10	9	10	10	9	9	10	10

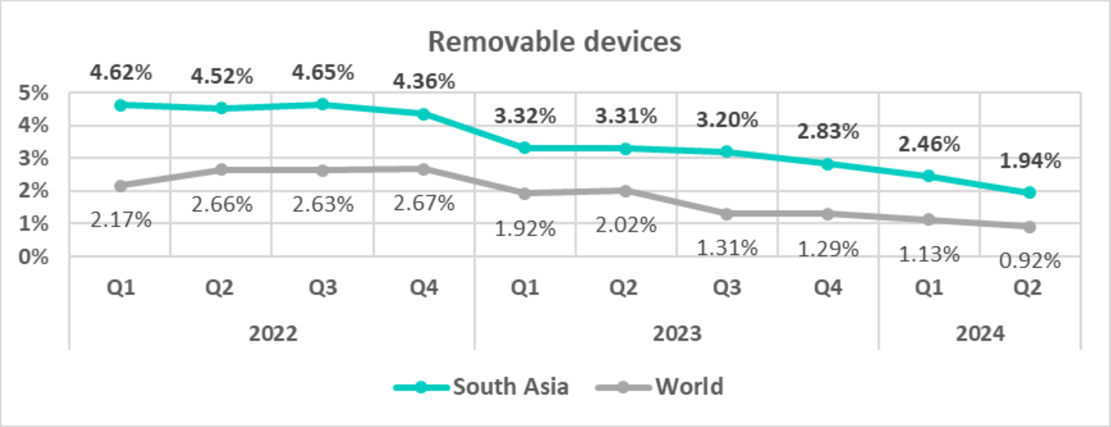
Threat sources

In Q2 2024, the percentage of ICS computers on which threats from **email clients** were blocked increased 1.1 times compared to the previous quarter, making it the second biggest threat source in the region (this source was third in Q1 2024).

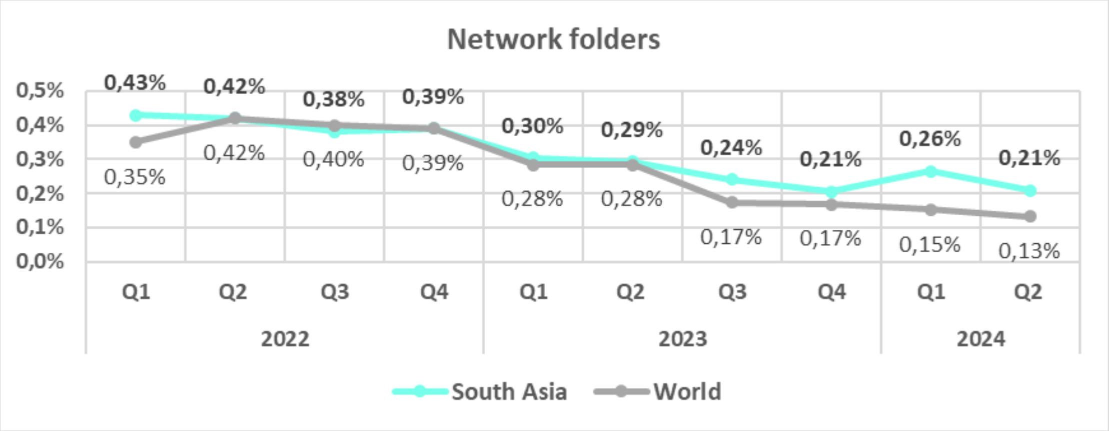
Since Q1 2022, threats from **removable drives** in South Asia had consistently placed second in the regional ranking by percentage of ICS computers on which malicious objects from various sources were blocked. However, in Q2 2024, the threat level from removable devices dropped, falling below that of email clients.



From a global perspective, the percentage of ICS computers on which threats from **removable devices** were blocked in South Asia closely followed the global trend, staying well above the global average. However, the gap between these trends has mostly become narrower since Q4 2022.



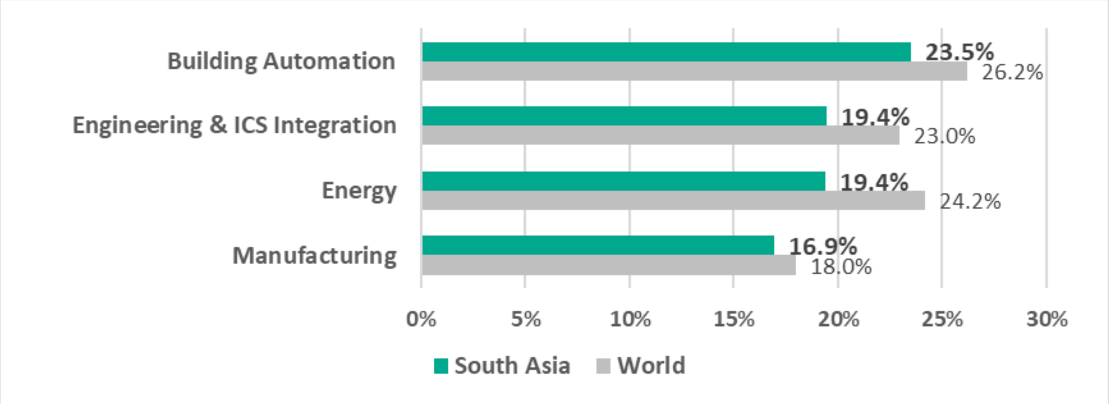
The percentage of ICS computers where threats from **network folders** were blocked follows the global trend. However, in Q3 2023, the regional trend diverged from the global one, rising noticeably above the global average.



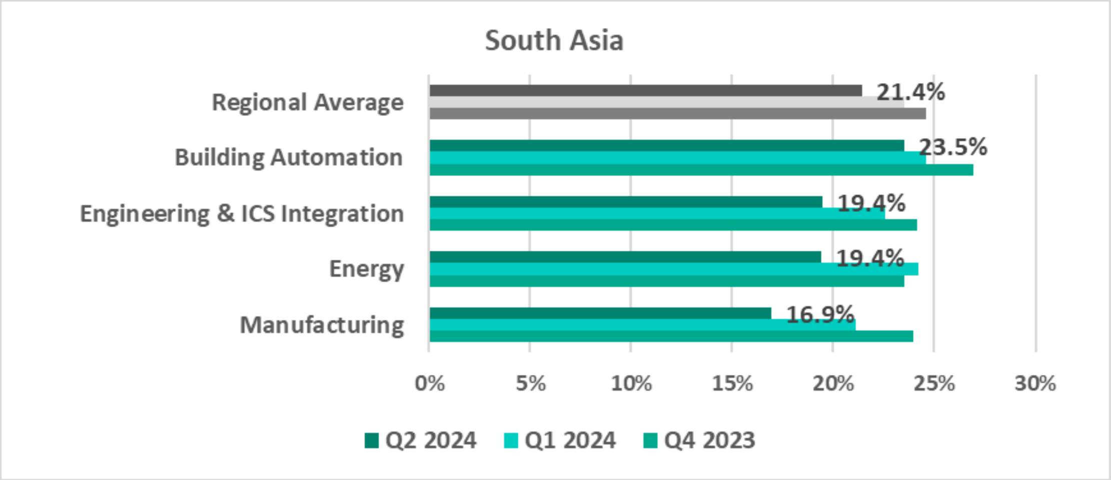
Industries

- **The most affected industry** in the region, as selected for this report, was **building automation.**

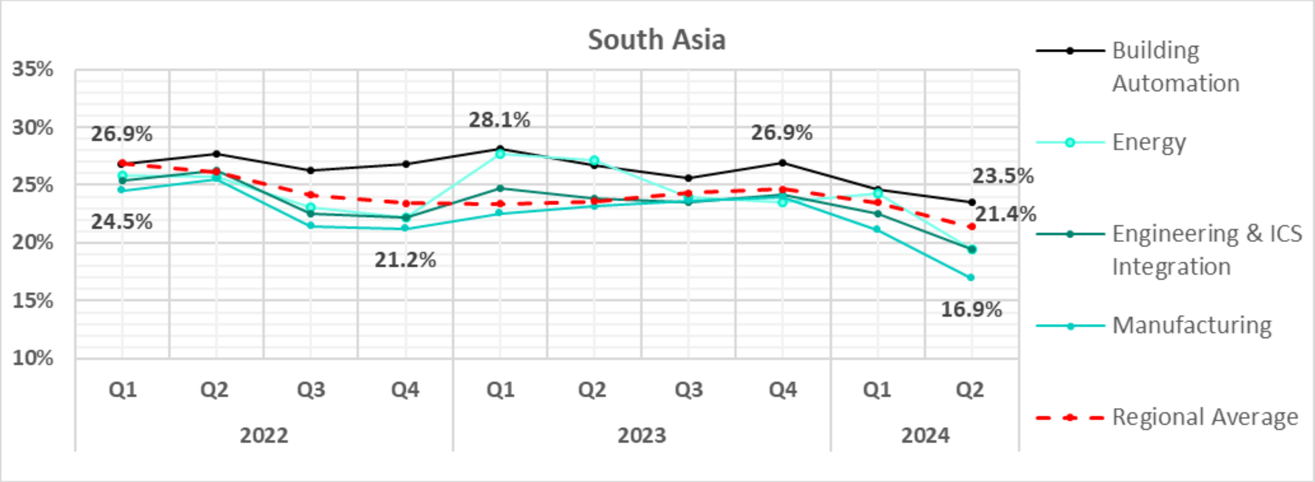
  From a **global perspective**, all sectors under consideration exhibited a lower percentage of ICS computers on which malicious objects were blocked than the respective global averages.



- In **Q2 2024**, all selected sectors in the region exhibited a decrease in the percentage of ICS computers on which malicious objects were blocked.



- The selected sectors show mostly positive dynamics in their long-term **trends** since Q1 2024:



East Asia

Current threats

-1-

Spyware

4.15%

▲ **1.1x** increase in Q2
above global average

-2-

Malicious scripts and phishing pages

3.49%

▲ **1.2x** increase in Q2
2nd in the world **in terms of growth**

-3-

Denylisted internet resources

3.47%

▼ decrease in Q2

Viruses

2.95%

▲ slight increase in Q2
1.9x above global average
3rd in the world
3rd in the world **in terms of growth**

Worms

1.80%

▲ **1.1x** increase in Q2
1.2x above global average
2nd in the world **in terms of growth**

Malware for AutoCAD

1.57%

▲ **1.1x** increase in Q2
1.6x above global average
3rd in the world
2nd in the world **in terms of growth**

Malicious documents

1.62%

▲ **1.2x** increase in Q2

Ransomware

0.18%

▲ **1.3x** increase in Q2

Threats from
Internet

6.46%

▼ decrease in Q2

Threats from
Removable devices

1.54%

▲ slight increase in Q2
1.7x above global average
1st in the world **in terms of growth**

Threats from
Network folders

0.35%

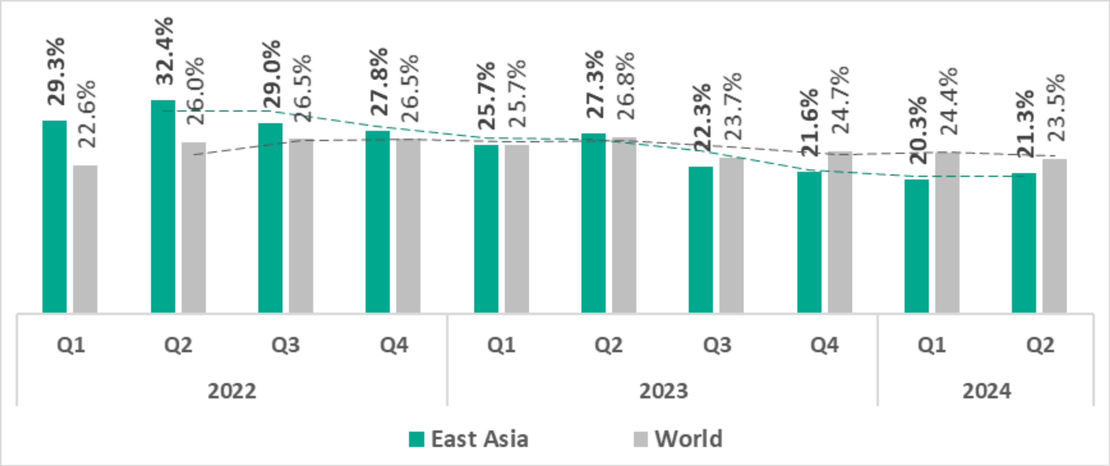
▲ **1.1x** increase in Q2
2.6x above global average
1st in the world
1st in the world **in terms of growth**

Overall

Ninth place in the global ranking by percentage of ICS computers on which malicious objects were blocked.

One of four regions that saw an increase in the percentage of ICS computers on which malicious objects were blocked.

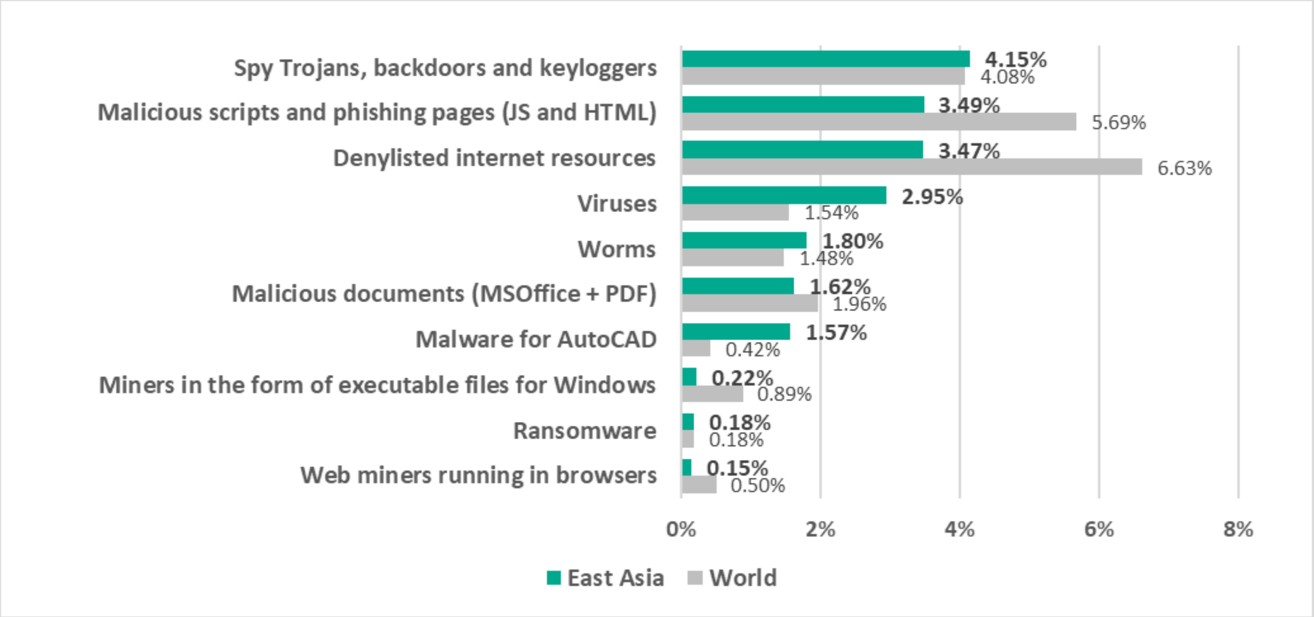
East Asia demonstrates a slow downtrend with fluctuations. The percentage of ICS computers on which malicious objects were blocked has been below the global average since Q3 2023.



Comparative analysis

- East Asia occupies **leading positions** among regions by percentage of ICS computers on which the following were blocked:
  - First place – threats from network folders
  - Second place – malware for AutoCAD
  - Third place – viruses
- **The only region in which spyware topped the malware category ranking** in terms of the percentage of ICS computers on which it was blocked.

Threat categories

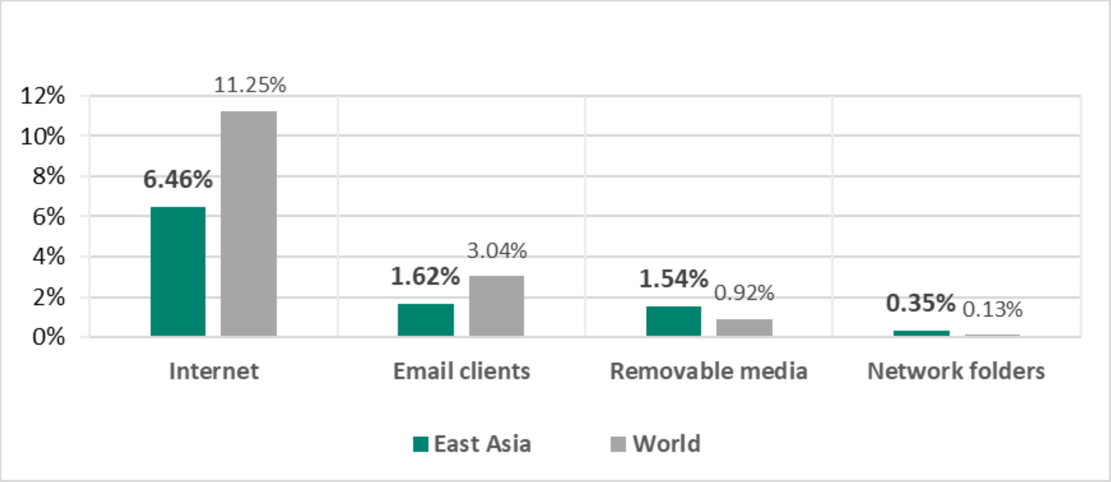


- **Compared to the global average**, the region has a noticeably higher percentage of ICS computers on which the following were blocked:
  - ➢ Malware for AutoCAD, 3.7 times higher
  - ➢ Viruses, 1.9 times higher
  - ➢ Worms, 1.2 times higher

Threat sources

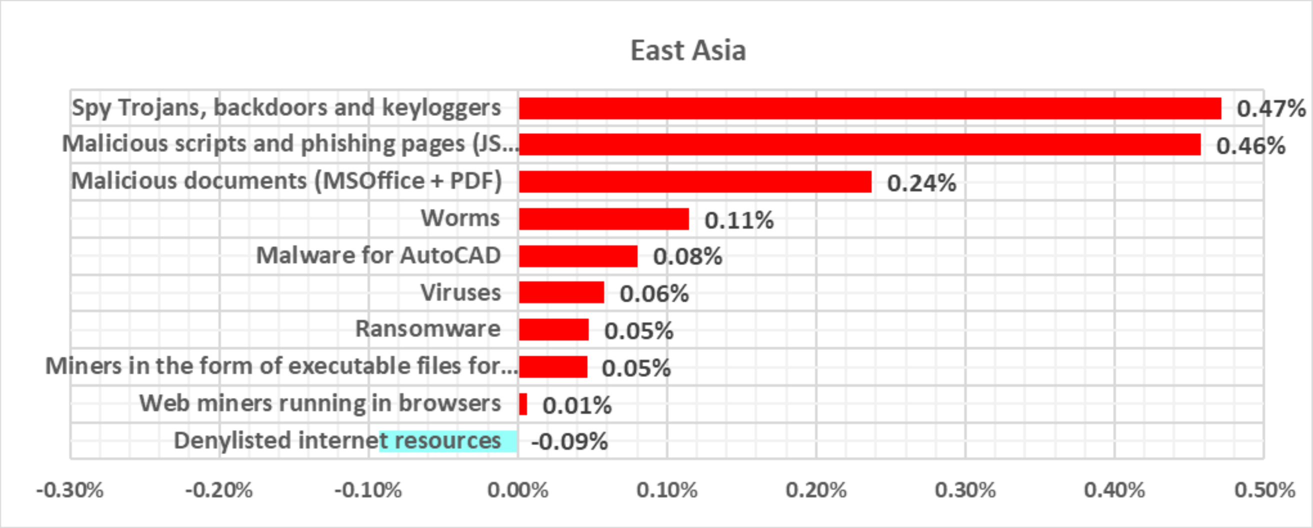
East Asia ranked **first** among the regions by percentage of ICS computers where malicious threats from **network folders** were blocked, surpassing the global average by 2.7 times.

The percentage of ICS computers on which threats from **removable devices** were blocked in the region was **1.7 times higher** than the global average.



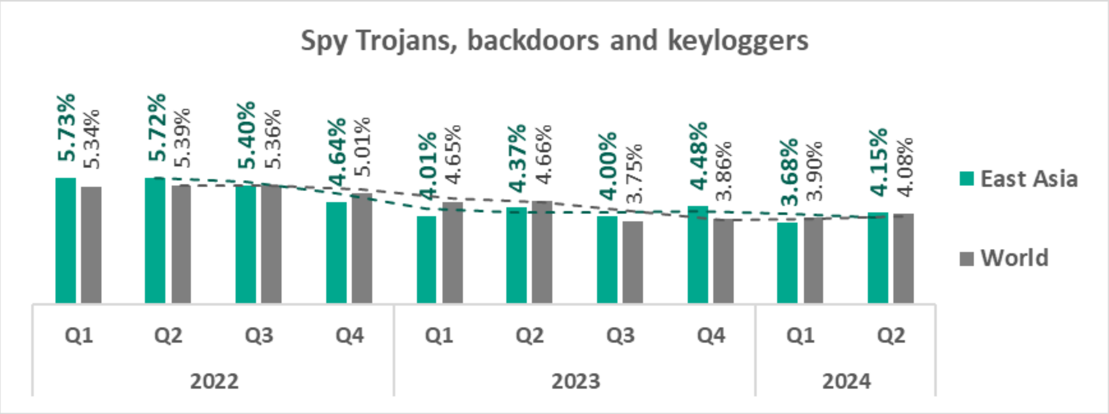
Quarterly changes and trends

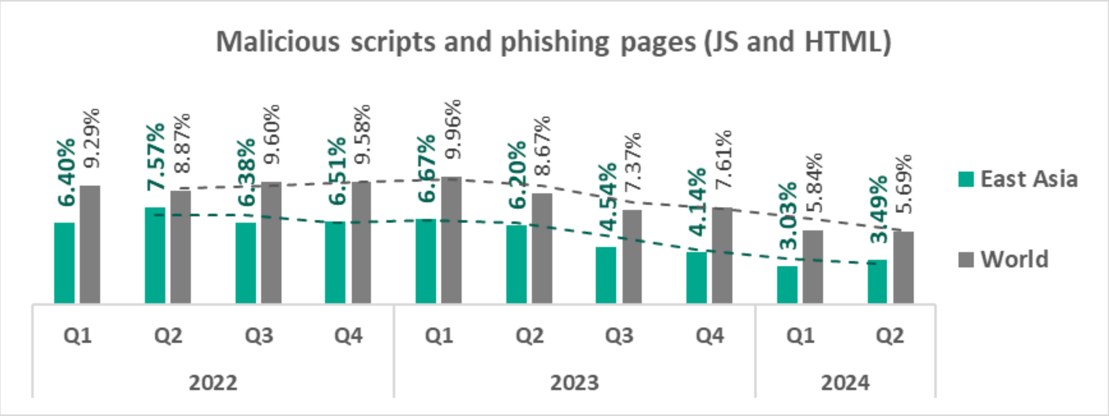
Threat categories

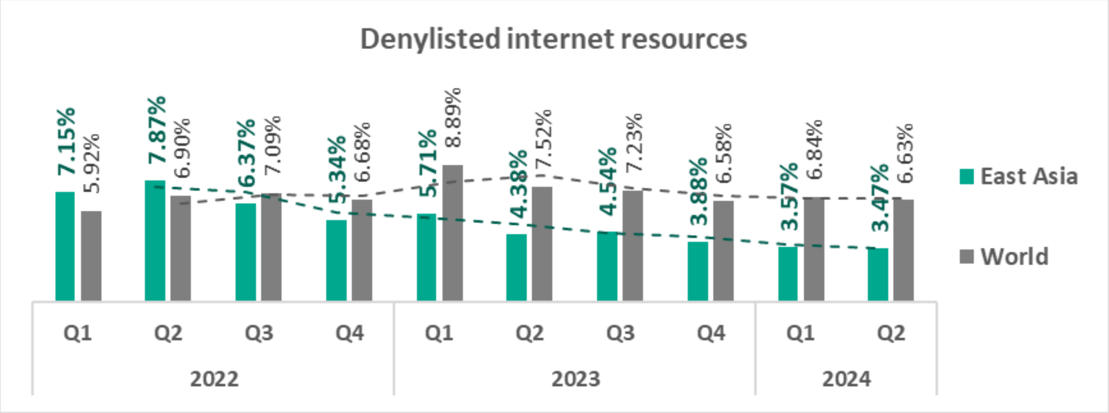


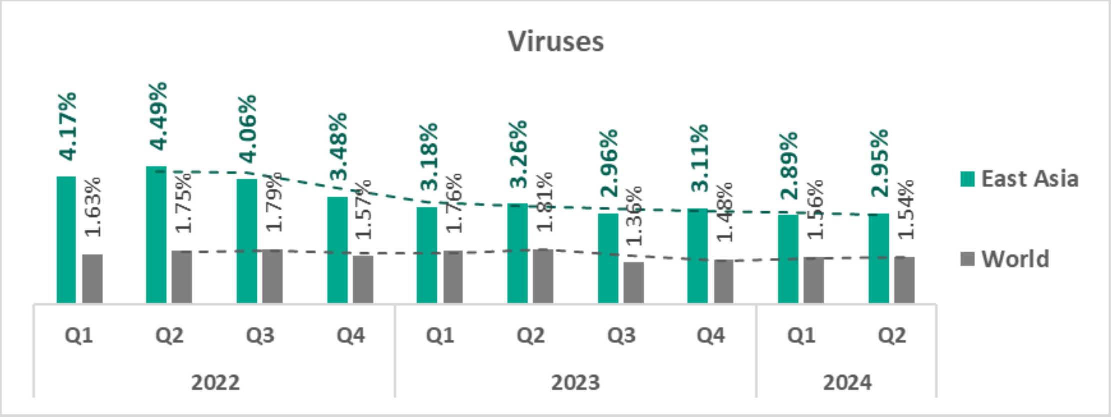
- All threat categories except for denylisted internet resources saw growth in Q2 2024.
- The **largest quarterly increase** was in the percentage of ICS computers on which the following were blocked:
  - Ransomware – by 1.3 times
  - Miners in the form of executable files for Windows – by 1.3 times
  - Malicious documents – by 1.2 times
  - Malicious scripts and phishing pages – by 1.2 times

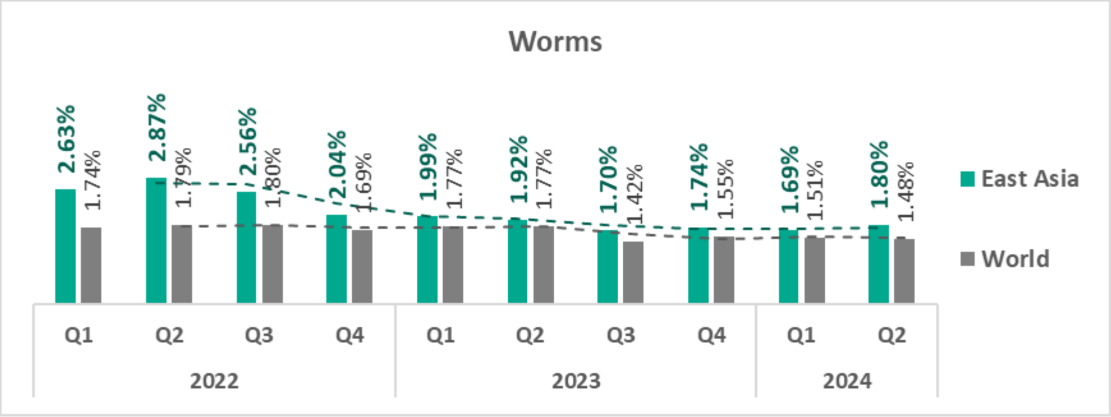
- The **top threat** categories exhibit various quarterly dynamics:

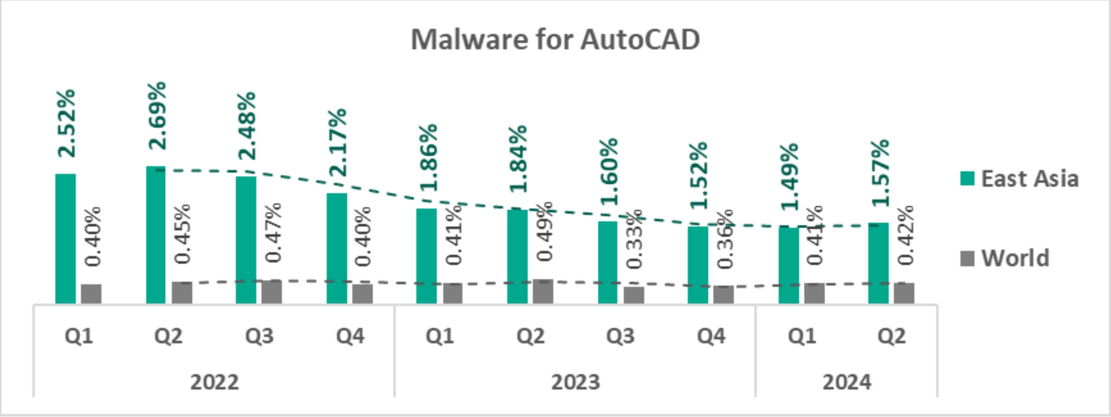


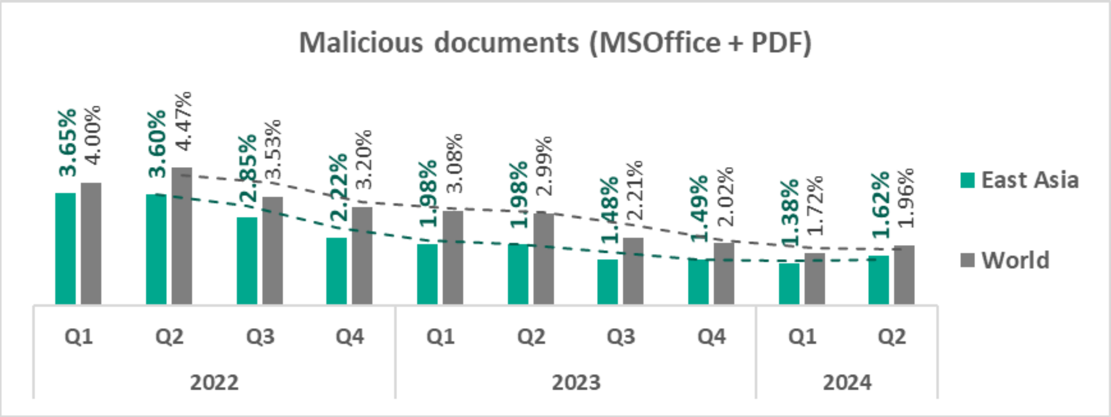


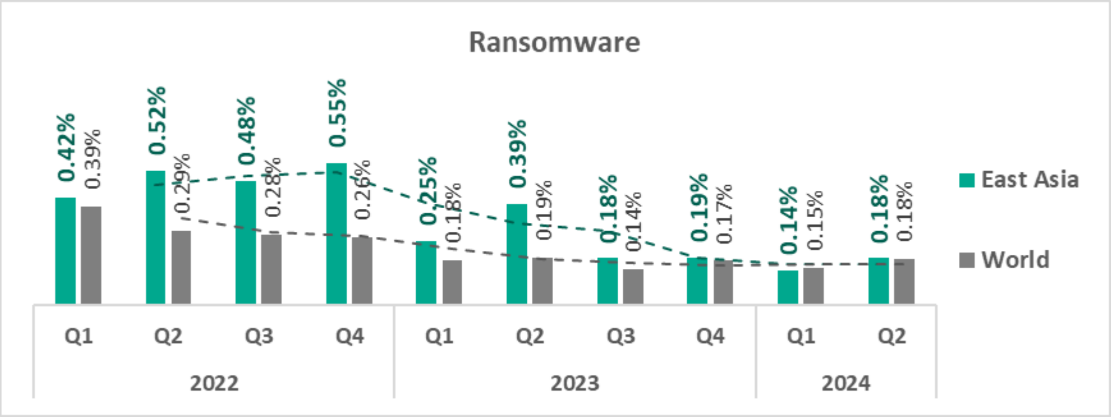



Viruses
4.17%
1.63%
4.49%
1.75%
4.06%
1.79%
3.48%
1.57%
3.18%
1.76%
3.26%
1.81%
2.96%
1.36%
3.11%
1.48%
2.89%
1.56%
2.95%
1.54%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
East Asia
World

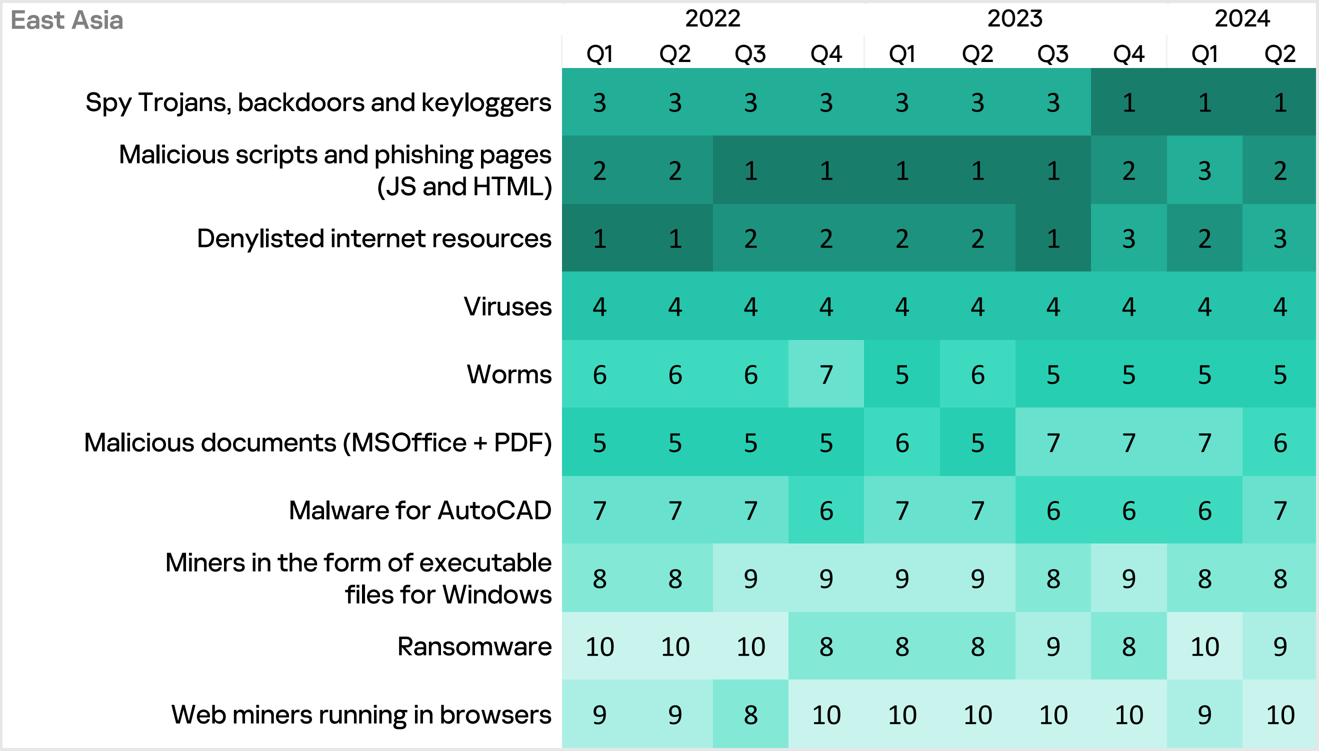

Worms
2.63%
1.74%
2.87%
1.79%
2.56%
1.80%
2.04%
1.69%
1.99%
1.77%
1.92%
1.77%
1.70%
1.42%
1.74%
1.55%
1.69%
1.51%
1.80%
1.48%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
East Asia
World


Malware for AutoCAD
2.52%
0.40%
2.69%
0.45%
2.48%
0.47%
2.17%
0.40%
1.86%
0.41%
1.84%
0.49%
1.60%
0.33%
1.52%
0.36%
1.49%
0.41%
1.57%
0.42%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
East Asia
World


Malicious documents (MSOffice + PDF)
3.65%
4.00%
3.60%
4.47%
2.85%
3.53%
2.22%
3.20%
1.98%
3.08%
1.98%
2.99%
1.48%
2.21%
1.49%
2.02%
1.38%
1.72%
1.62%
1.96%
Q1
Q2
Q3
Q4
2022
Q1
Q2
Q3
Q4
2023
Q1
Q2
2024
East Asia
World


Ransomware
0.42%
0.39%
0.52%
0.29%
0.48%
0.28%
0.55%
0.26%
0.25%
0.18%
0.39%
0.19%
0.18%
0.14%
0.19%
0.17%
0.14%
0.15%
0.18%
0.18%
Q1
Q2
Q3
Q4
2022
Q1
Q2
Q3
Q4
2023
Q1
Q2
2024
East Asia
World

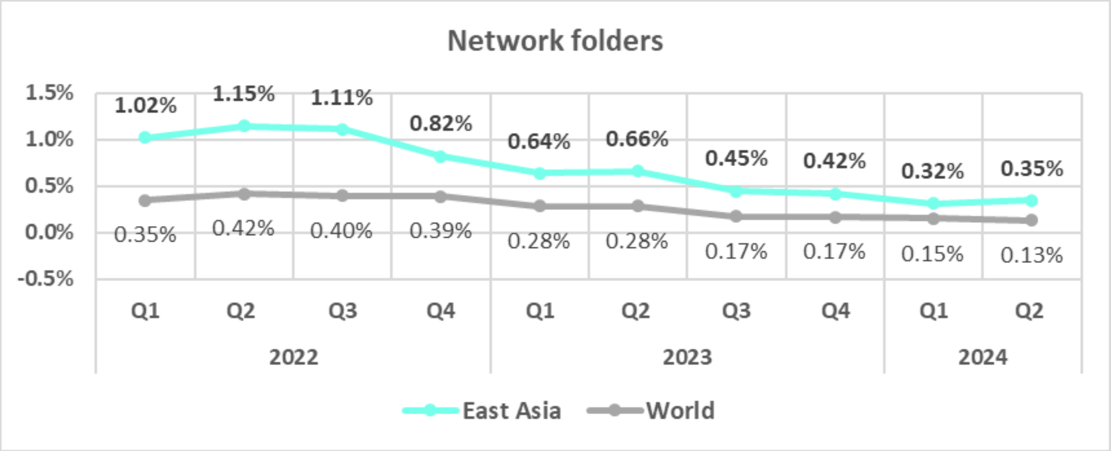
- The heatmap below illustrates changes in the rankings of threat categories in the region over a period of 2.5 years. **Spyware** has been the leading threat category in the region since Q4 2023, jumping from third to first place and replacing **malicious scripts and phishing pages**.



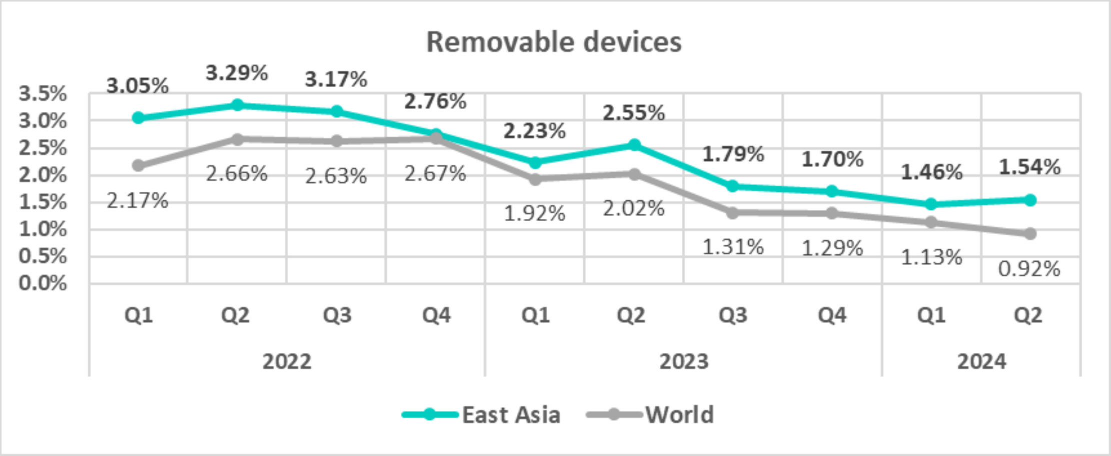
East Asia	2022				2023				2024	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Spy Trojans, backdoors and keyloggers	3	3	3	3	3	3	3	1	1	1
Malicious scripts and phishing pages (JS and HTML)	2	2	1	1	1	1	1	2	3	2
Denylisted internet resources	1	1	2	2	2	2	1	3	2	3
Viruses	4	4	4	4	4	4	4	4	4	4
Worms	6	6	6	7	5	6	5	5	5	5
Malicious documents (MSOffice + PDF)	5	5	5	5	6	5	7	7	7	6
Malware for AutoCAD	7	7	7	6	7	7	6	6	6	7
Miners in the form of executable files for Windows	8	8	9	9	9	9	8	9	8	8
Ransomware	10	10	10	8	8	8	9	8	10	9
Web miners running in browsers	9	9	8	10	10	10	10	10	9	10

Threat sources

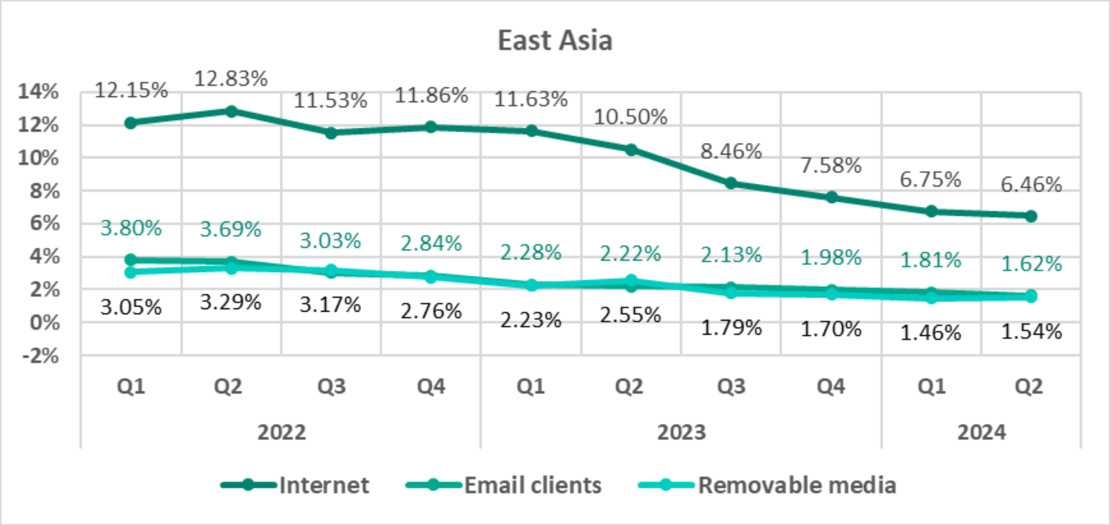
- **Network folder** threats which were blocked on ICS computers in East Asia showed a declining trend from the second half of 2022 to Q1 2024 but stayed consistently higher than the global average. While the global rate remained relatively stable at lower levels, the gap between East Asia and the global average gradually narrowed up to Q1 2024, with only a slight rise observed in East Asia in Q2 2024.



- In Q2 2024, the region exhibited an increase in threats distributed via **removable devices,** in contrast to the global average.

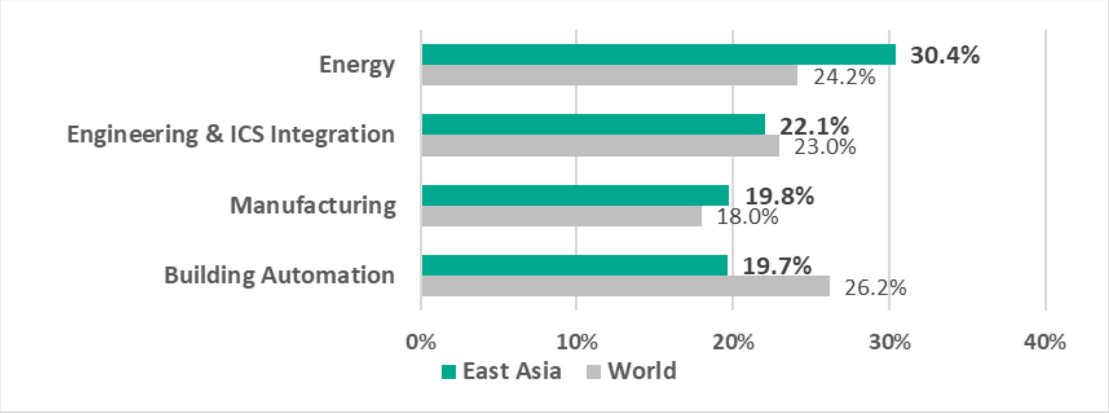


- Overall, all major sources exhibit downward trends.

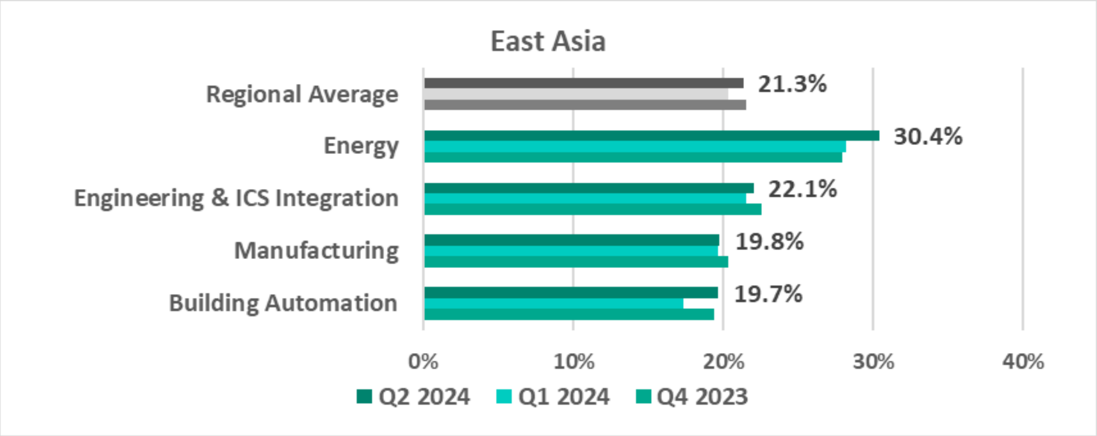


Industries

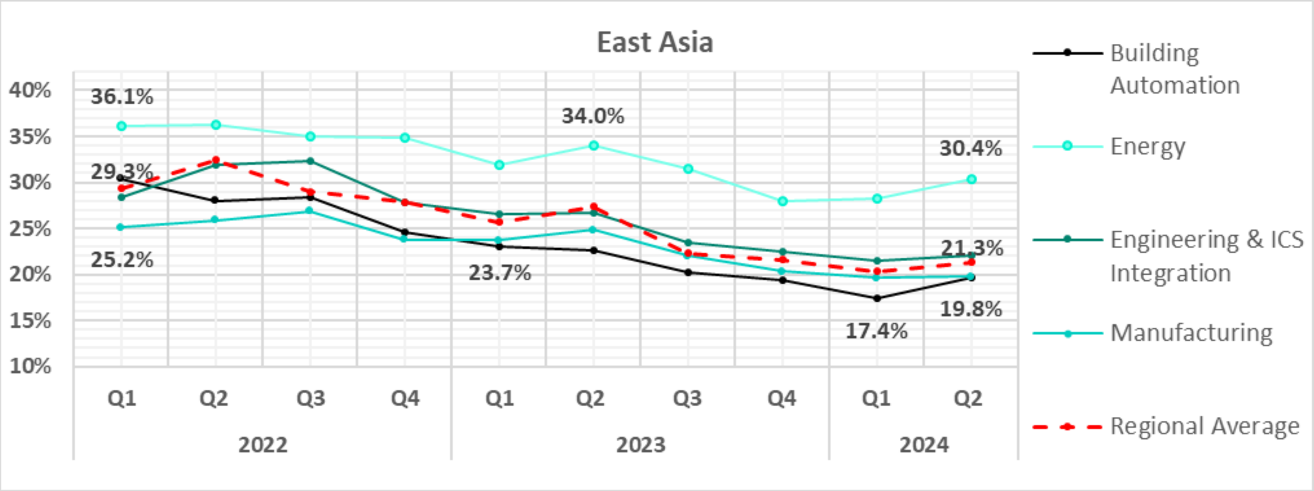
- The most **affected industry** in the region, as selected for this report, was **energy.**
- Compared to the respective **global averages**, the following sectors in the region saw a higher percentage of ICS computers on which malicious objects were blocked:
  - ➢ Energy, 1.3 times higher
  - ➢ Manufacturing, 1.1 times higher



- In **Q2 2024**, all sectors exhibited an increase in the percentage of ICS computers on which malicious objects were blocked. The following sectors saw noticeably higher values compared to the previous quarter:
  - ➢ Energy, 1.1 times higher
  - ➢ Building automation, 1.1 times higher



- The **energy** sector consistently exhibited the highest rate of blocked malicious objects on ICS computers throughout the period, significantly above the regional average. In contrast, other sectors experienced a downward trend from 2022 until Q1 2024, followed by an increase in Q2 2024:



Southern Europe

Current threats

-1-

Malicious scripts and phishing pages

7.46%

▲ **1.1x** increase in Q2
1.3x above global average
1st in the world
1st in the world **in terms of growth**

-2-

Spyware

6.21%

▲ **1.1x** increase in Q2
1.5x above global average
3rd in the world
1st in the world **in terms of growth**

-3-

Denylisted internet resources

5.22%

▼ decrease in Q2

Malicious documents

3.75%

▲ **1.2x** increase in Q2
1.9x above global average
1st in the world
3rd in the world **in terms of growth**

Ransomware

0.19%

▲ **1.6x** increase in Q2
above global average
2nd in the world **in terms of growth**

Threats from
Internet

9.53%

▼ decrease in Q2

Threats from
Email clients

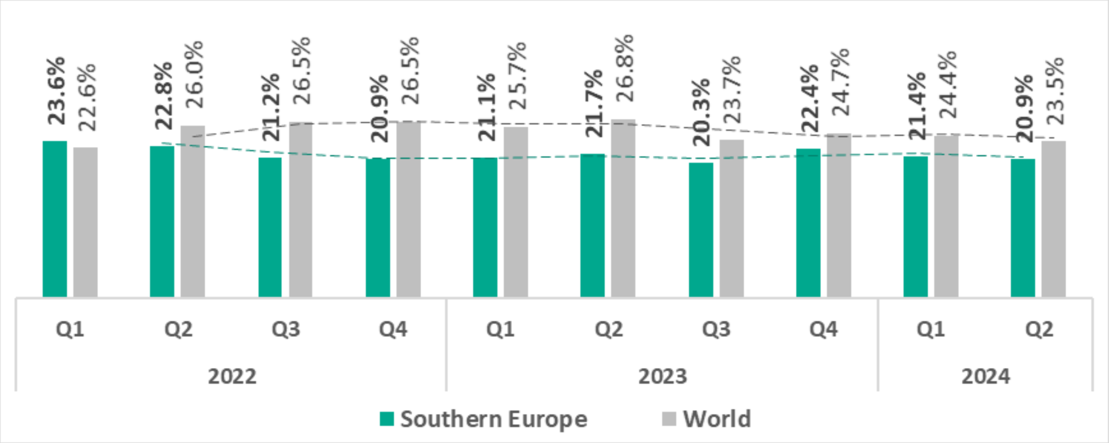
7.06%

▲ slight increase in Q2
2.3x above global average
1st in the world

Overall

Tenth place in the regional ranking.

In Southern Europe, the percentage of ICS computers on which malicious objects were blocked is normally below the global average.

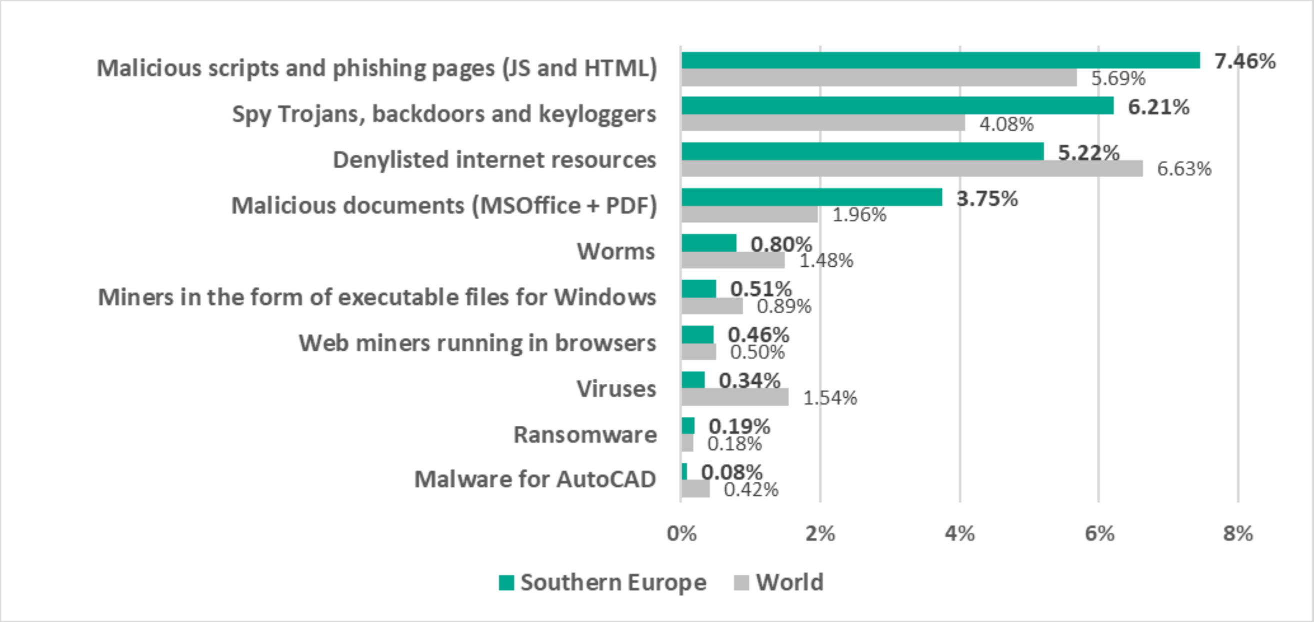


Comparative analysis

Southern Europe occupies **leading positions** among regions by percentage of ICS computers on which the following were blocked:

- First place – threats from email clients, malicious scripts and phishing pages, malicious documents.
- Third place – spyware.

Threat categories

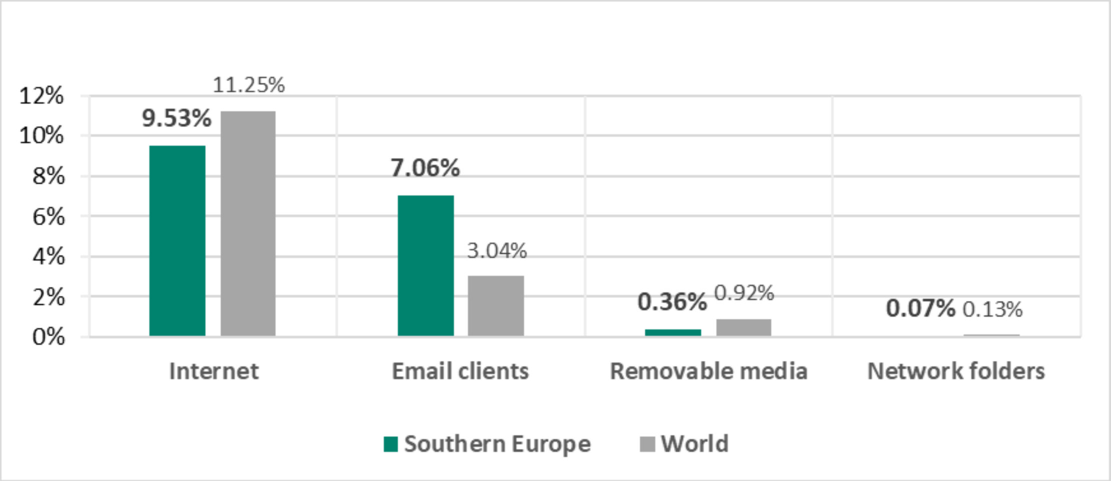


- **Compared to the global average**, the region has a higher percentage of ICS computers on which the following were blocked:
  - Malicious documents, 1.9 times higher
  - Spyware, 1.5 times higher
  - Malicious scripts and phishing pages, 1.3 times higher

Threat sources

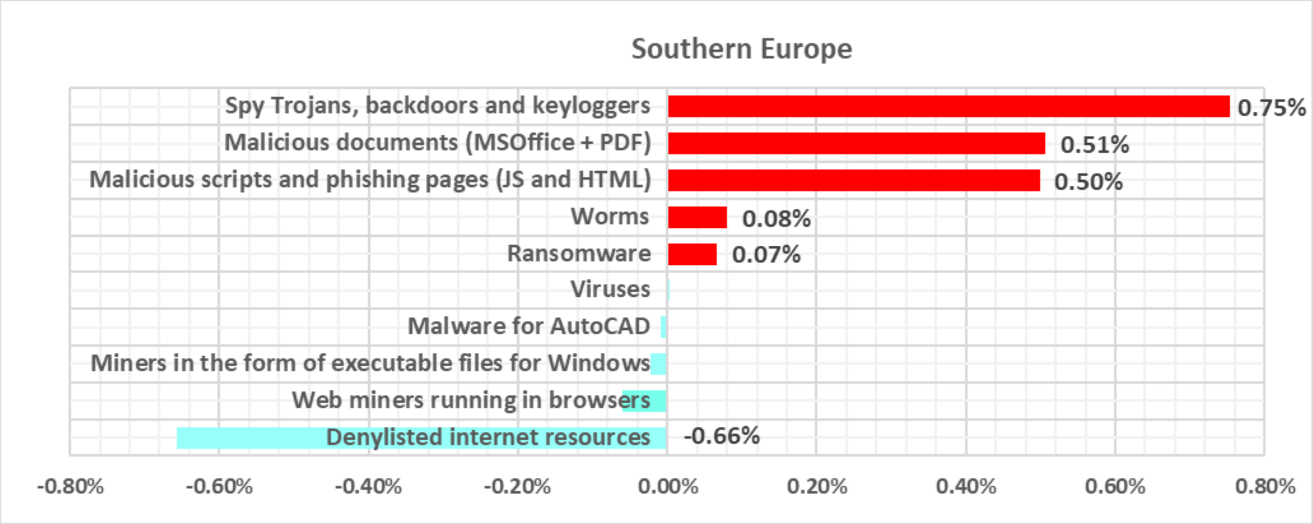
Southern Europe ranked **first in the world** by percentage of ICS computers where malicious threats from **email clients** were blocked, surpassing the global average by 2.3 times.

Other threat sources remained below their respective global averages.



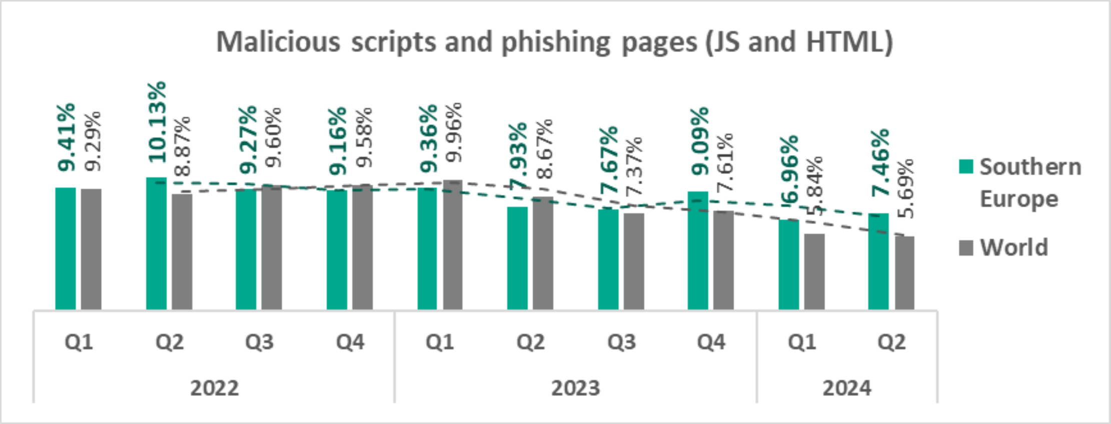
Quarterly changes and trends

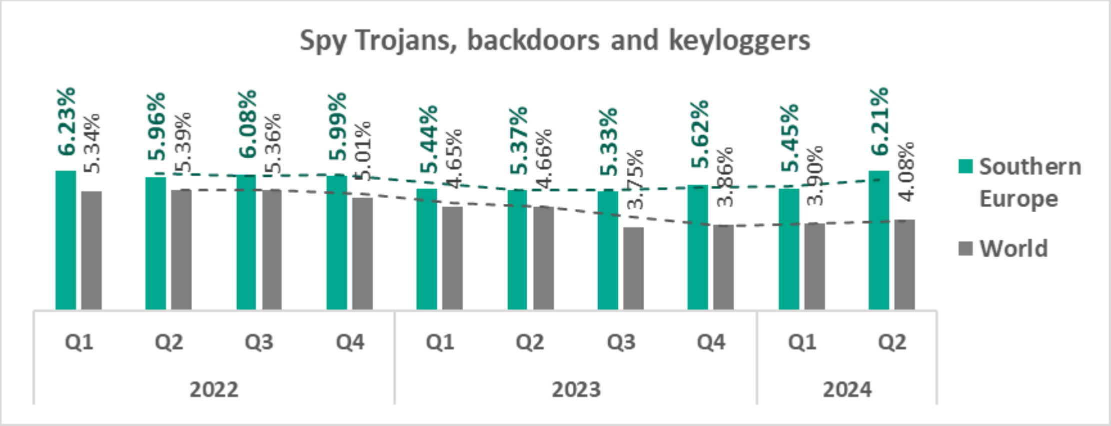
Threat categories

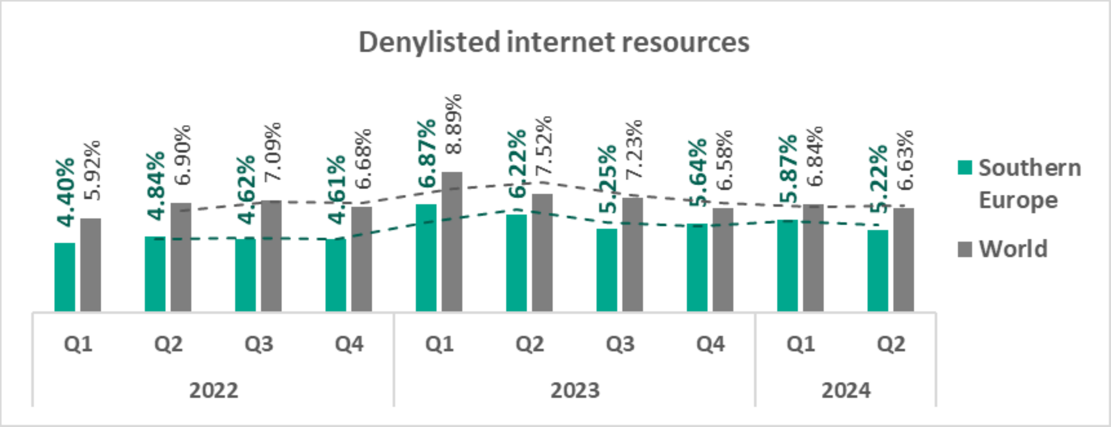


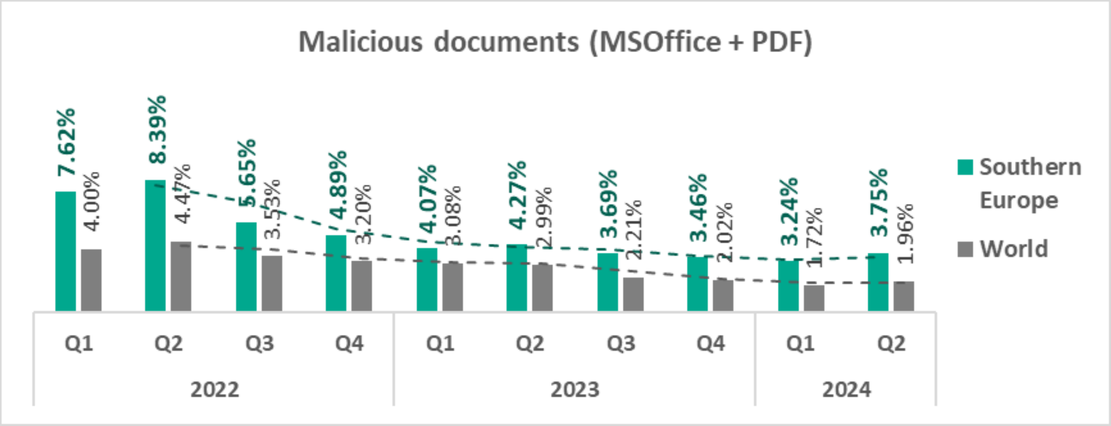
- The **largest quarterly increase** in absolute terms was in the percentage of ICS computers on which spyware was blocked. In terms of proportional increases, the following threat categories showed significant changes:
  - Ransomware, by 1.6 times
  - Malicious documents, by 1.2 times

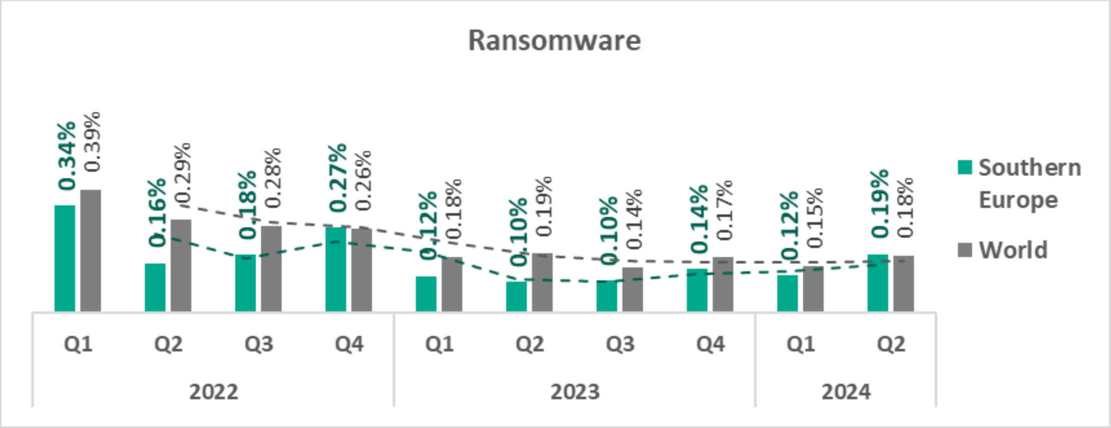
The **top threat** categories exhibit various quarterly dynamics:


Malicious scripts and phishing pages (JS and HTML)


Spy Trojans, backdoors and keyloggers


Denylisted internet resources


Malicious documents (MSOffice + PDF)
7.62%
4.00%
8.39%
4.47%
5.65%
3.53%
4.89%
3.20%
4.07%
3.08%
4.27%
2.99%
3.69%
2.21%
3.46%
2.02%
3.24%
1.72%
3.75%
1.96%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
Southern Europe
World

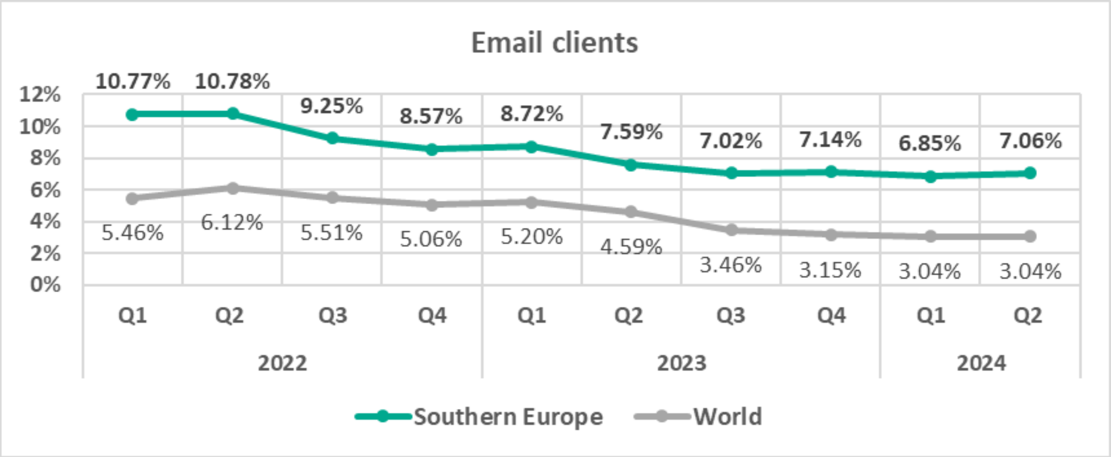

Ransomware
0.34%
0.39%
0.16%
0.29%
0.18%
0.28%
0.27%
0.26%
0.12%
0.18%
0.10%
0.19%
0.10%
0.14%
0.14%
0.17%
0.12%
0.15%
0.19%
0.18%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
Southern Europe
World

- The heatmap below illustrates changes in the rankings of threat categories in the region over a period of 2.5 years. **Malicious scripts and phishing pages** have been the leading threat category in the region throughout the observed period. **Spyware** moved from third to second place in Q2 2024. It alternated between second and third place throughout the observed period.

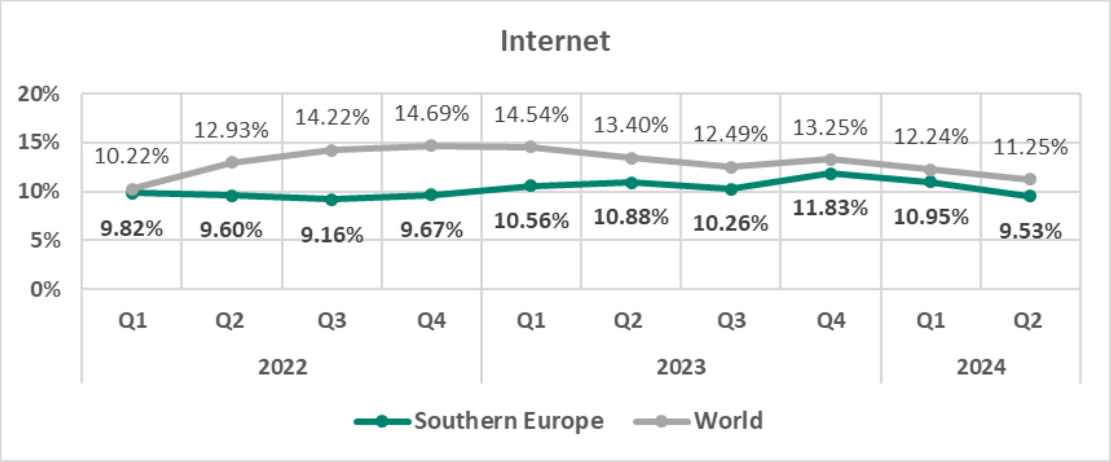
Southern Europe	2022				2023				2024	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Malicious scripts and phishing pages (JS and HTML)	1	1	1	1	1	1	1	1	1	1
Spy Trojans, backdoors and keyloggers	3	3	2	2	3	3	2	3	3	2
Denylisted internet resources	4	4	4	4	2	2	3	2	2	3
Malicious documents (MSOffice + PDF)	2	2	3	3	4	4	4	4	4	4
Worms	7	7	6	5	5	5	5	5	5	5
Miners in the form of executable files for Windows	5	5	7	7	8	7	6	7	6	6
Web miners running in browsers	6	6	5	6	7	6	7	8	7	7
Viruses	8	8	8	8	6	8	8	6	8	8
Ransomware	9	9	9	9	9	10	9	9	9	9
Malware for AutoCAD	10	10	10	10	10	9	10	10	10	10

Threat sources

In Q2 2024, the percentage of ICS computers on which threats from **email clients** were blocked increased compared to the previous quarter. The long-term trends, both local and global, for email client threats remained mostly consistent with each other until Q3 2023. However, since Q4 2023, the trends have started to diverge.

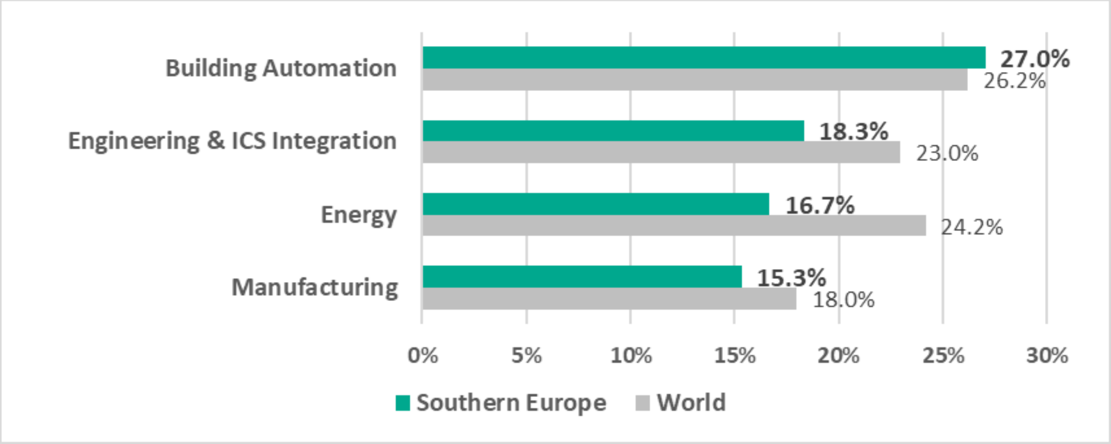


The local and global long-term trends for threats from the internet have been mostly consistent with each other since Q3 2023. Both trends have been declining since Q1 2024.

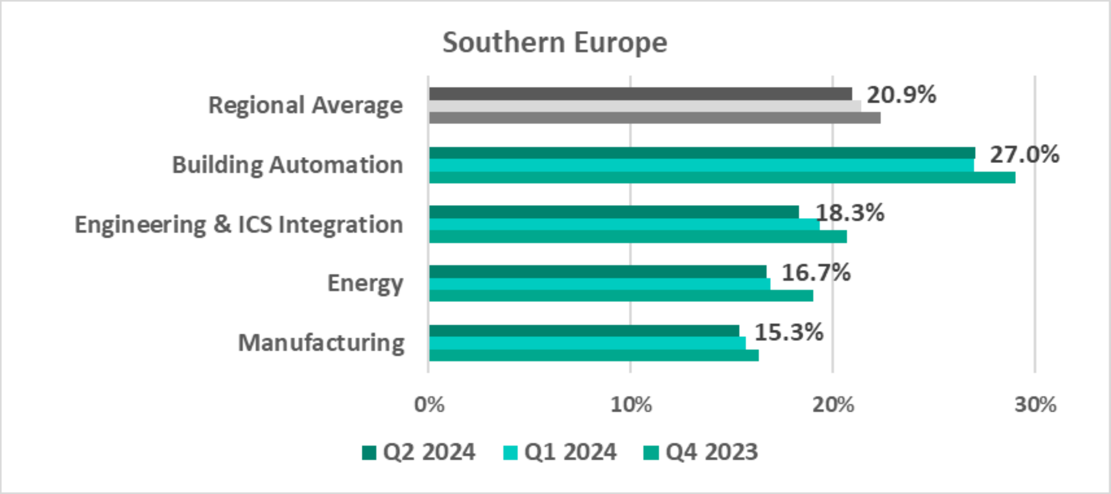


Industries

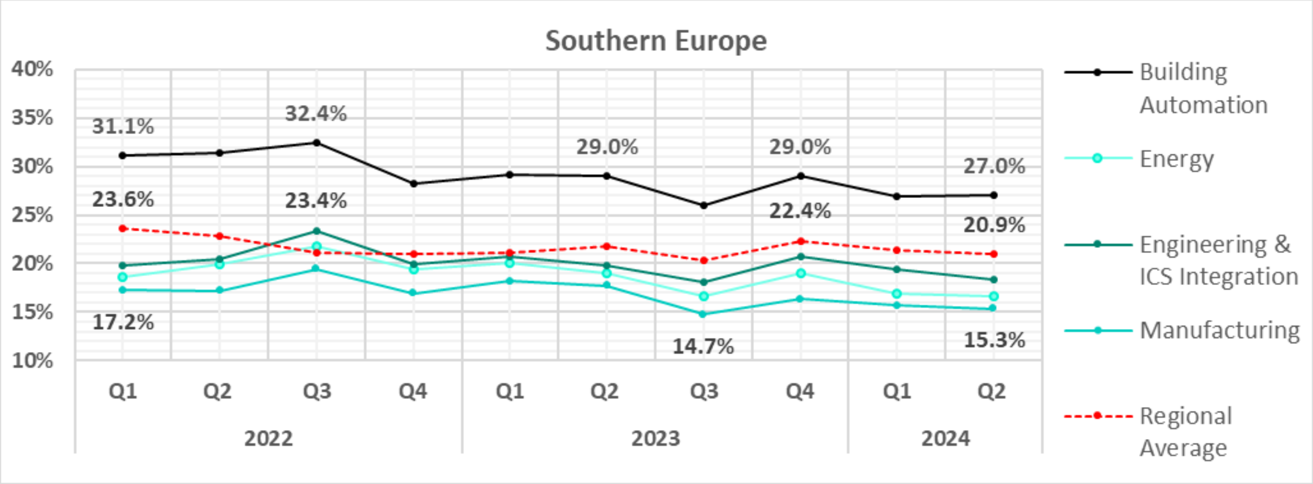
- The most **affected industry** in the region, as selected for this report, was **building automation.**
- Compared to the respective **global averages**, the building automation sector saw a higher percentage of ICS computers on which malicious objects were blocked.



- In **Q2 2024**, building automation was the only sector under observation that exhibited an increase in the percentage of ICS computers on which malicious objects were blocked.



- All selected sectors exhibit fluctuating **trends** in terms of percentage of ICS computers on which malicious objects were blocked. The rate in the **building automation** sector remains consistently higher than the regional average. Meanwhile, the other sectors have maintained steady, lower percentages since Q2 2023 with modest fluctuations throughout the period.



Australia and New Zealand

Current threats

-1-

Malicious scripts and phishing pages
6.73%

▲ slight increase in Q2
1.2x above global average
4th in the world

-2-

Denylisted internet resources
4.75%

▲ **1.2x** increase in Q2
2nd in the world **in terms of growth**

-3-

Spyware
2.15%

▲ **1.2x** increase in Q2

Web miners
0.68%

▼ decrease in Q2
1.4x above global average
6th in the region (8th in the global threat ranking)
3rd in the world

Worms
0.42%

▲ **1.5x** increase in Q2
1st in the world **in terms of growth**

Viruses
0.35%

▲ **1.5x** increase in Q2
2nd in the world **in terms of growth**

Ransomware
0.16%

▲ **1.6x** increase in Q2
close to global average
3rd in the world **in terms of growth**

Threats from
Internet
9.79%

▲ **1.1x** increase in Q2
2nd in the world **in terms of growth**

Threats from
Email clients
3.29%

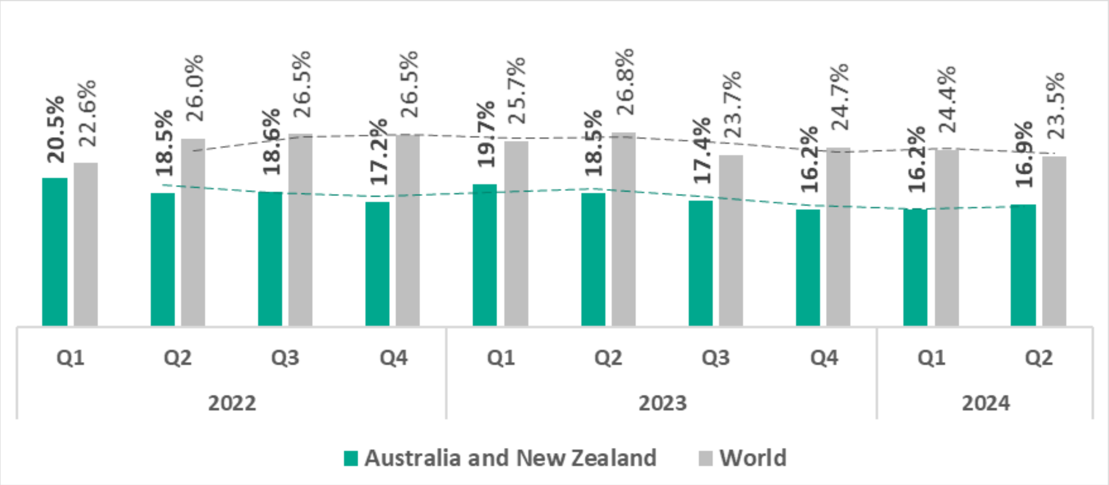
▼ decrease in Q2
1.2x above global average

Overall

Eleventh place in the regional ranking.

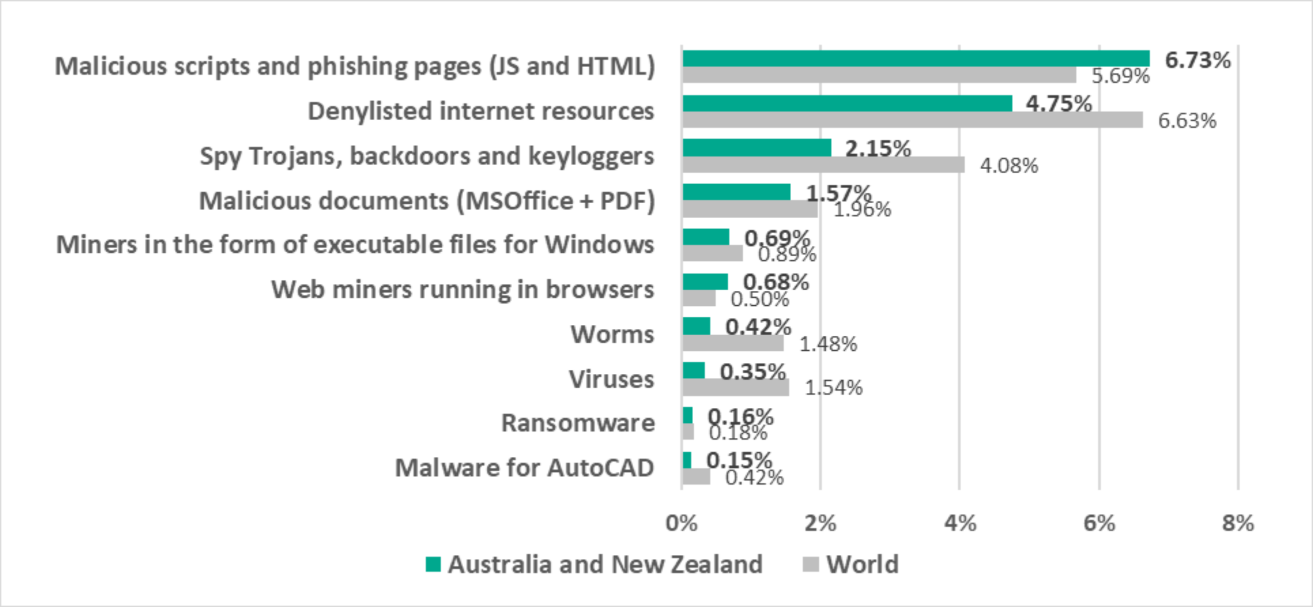
One of four regions that saw an increase in the percentage of ICS computers on which malicious objects were blocked.

The percentage of ICS computers on which malicious objects were blocked in the region is less than the global figure.



Comparative analysis

Threat categories



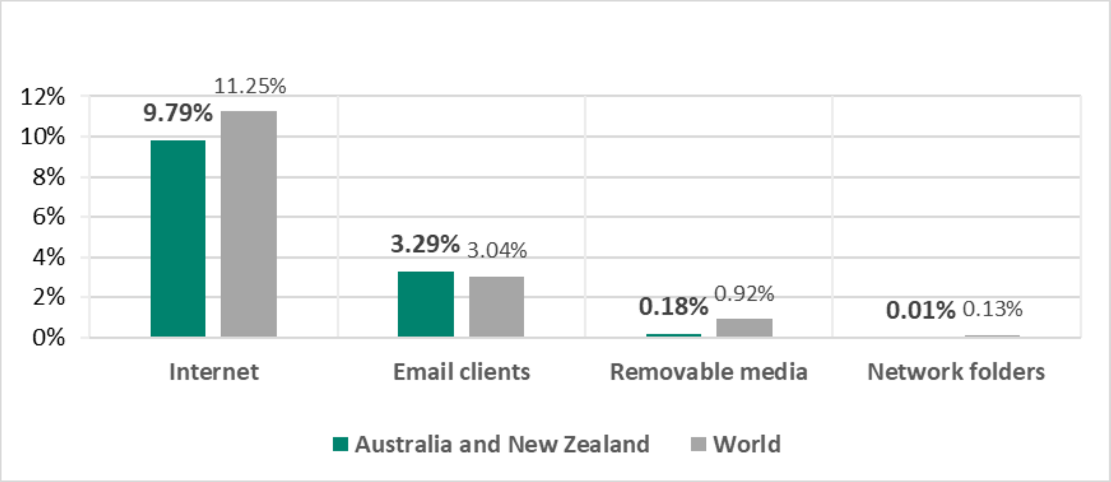
Compared to the global average, the region has a higher percentage of ICS computers on which the following were blocked:

- Web miners – 1.4 times higher
- Malicious scripts and phishing pages – 1.2 times higher

Threat sources

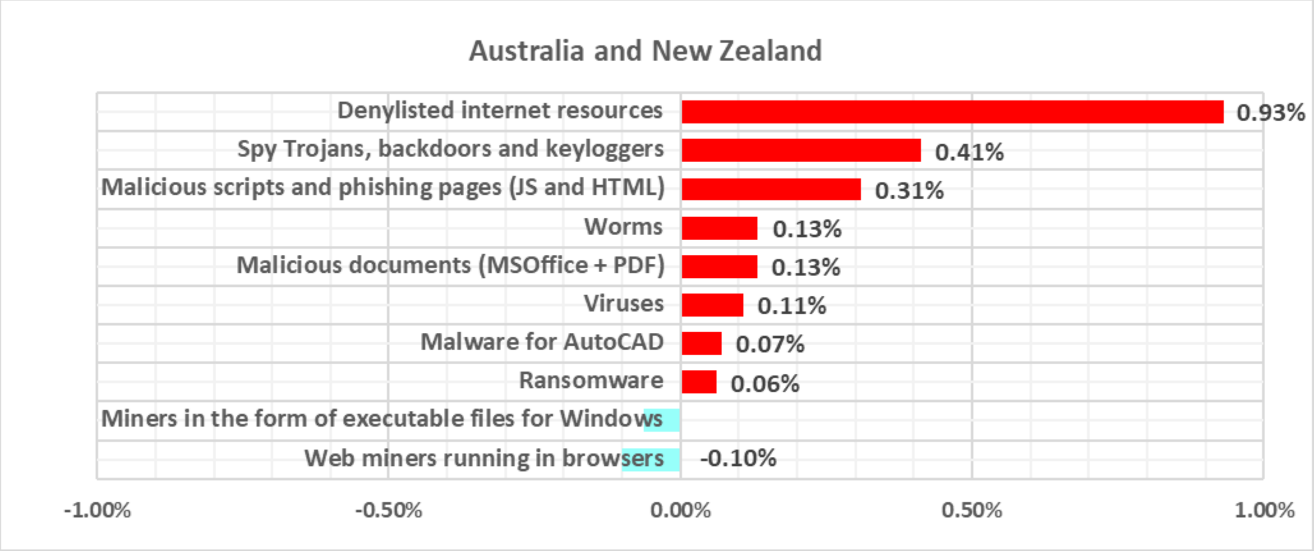
The percentage of ICS computers on which threats from **email clients** were blocked surpassed the global average by a factor of 1.1.

Other threat sources remained below their respective global averages.

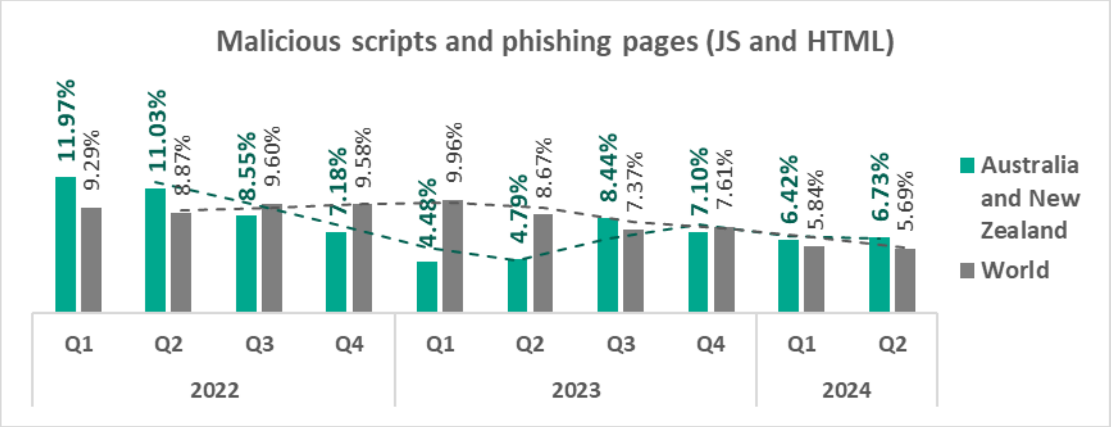


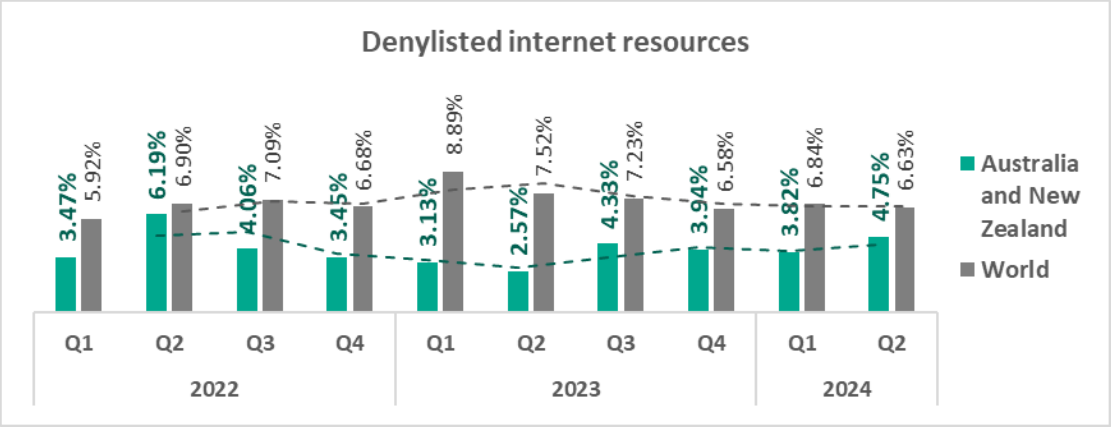
Quarterly changes and trends

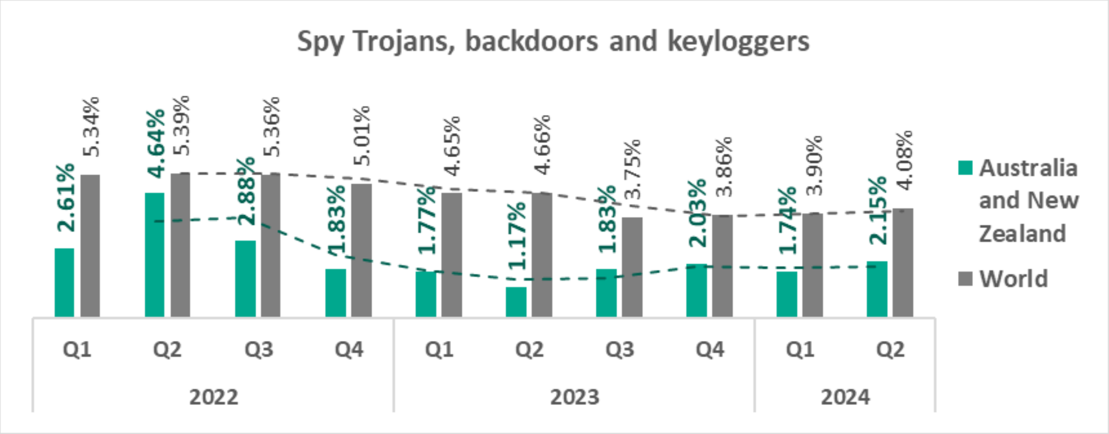
Threat categories



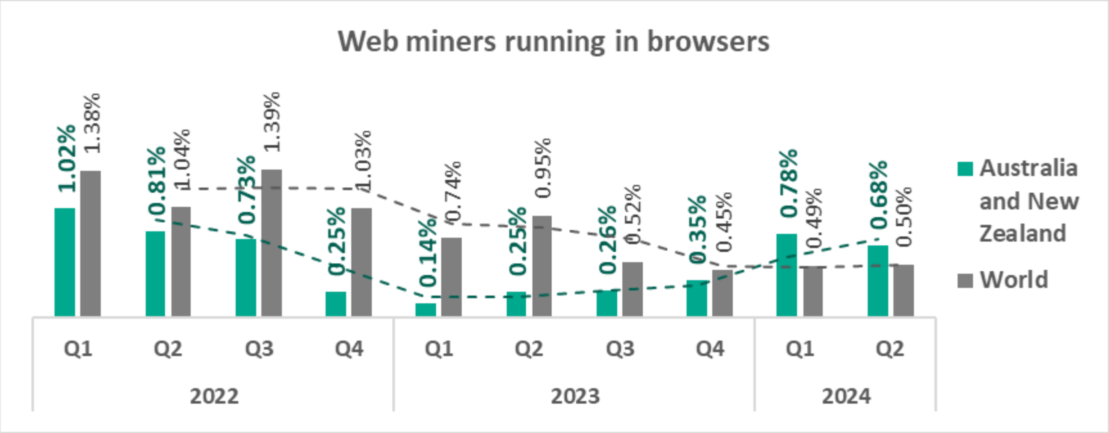
- Compared to the previous quarter, the **largest proportional increase** was in the percentage of ICS computers on which the following were blocked:
    - Malware for AutoCAD – by 1.9 times
    - Ransomware – by 1.6 times
    - Worms – by 1.5 times
    - Viruses – by 1.5 times
    - Spyware – by 1.2 times
    - Denylisted internet resources – by 1.2times
- The **top threat** categories exhibit various quarterly dynamics:



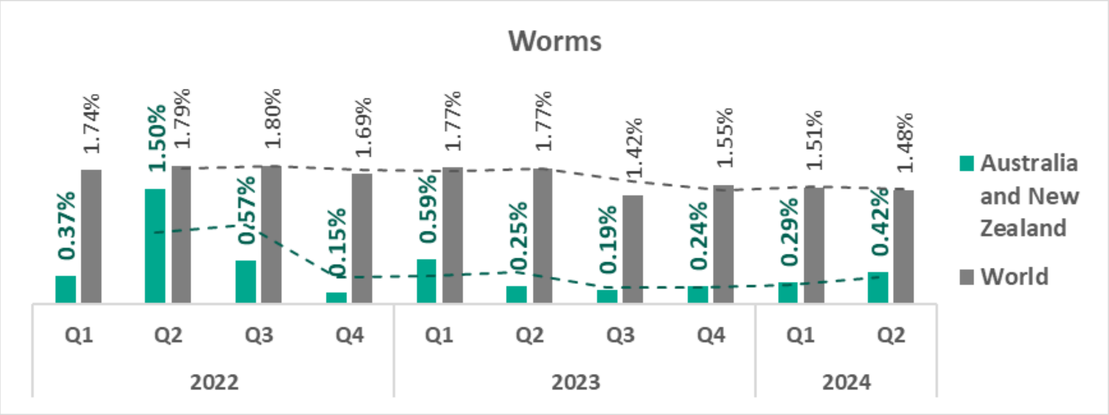




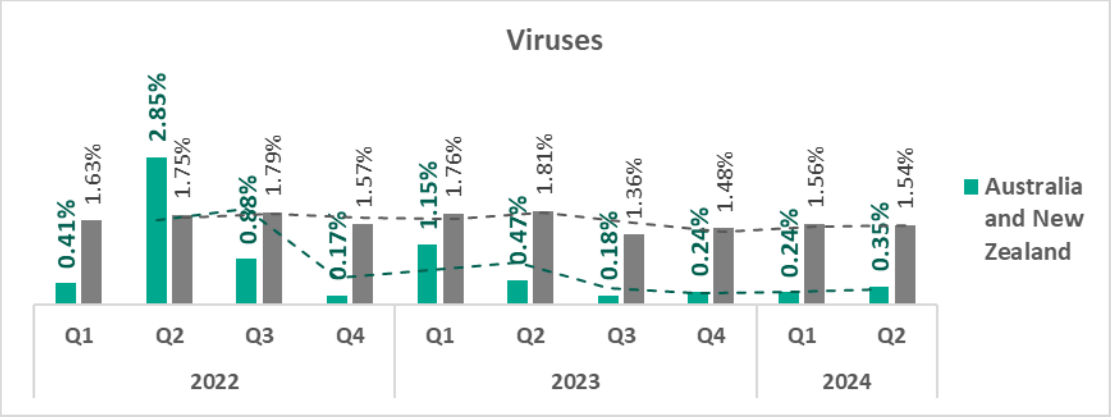
Spy Trojans, backdoors and keyloggers

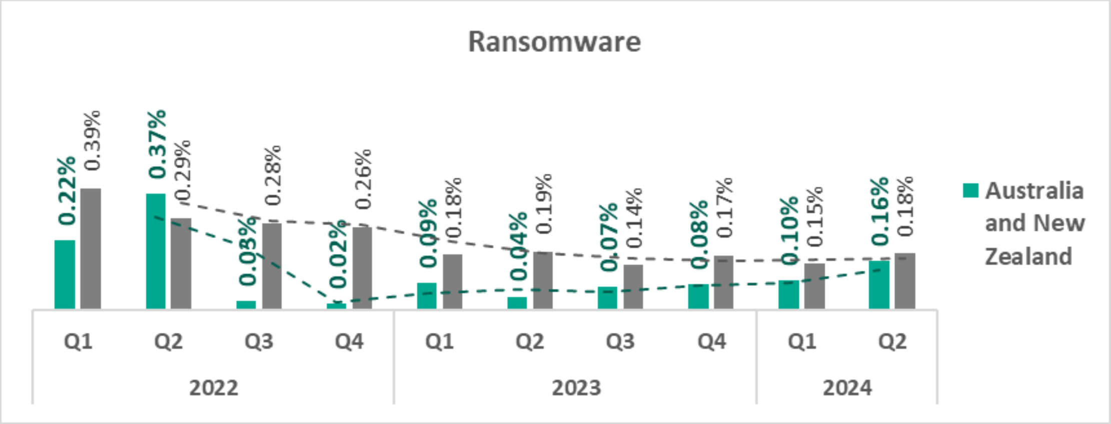


Web miners running in browsers



Worms


Viruses
0.41%
1.63%
2.85%
1.75%
0.88%
1.79%
0.17%
1.57%
1.15%
1.76%
0.47%
1.81%
0.18%
1.36%
0.24%
1.48%
0.24%
1.56%
0.35%
1.54%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
Australia and New Zealand

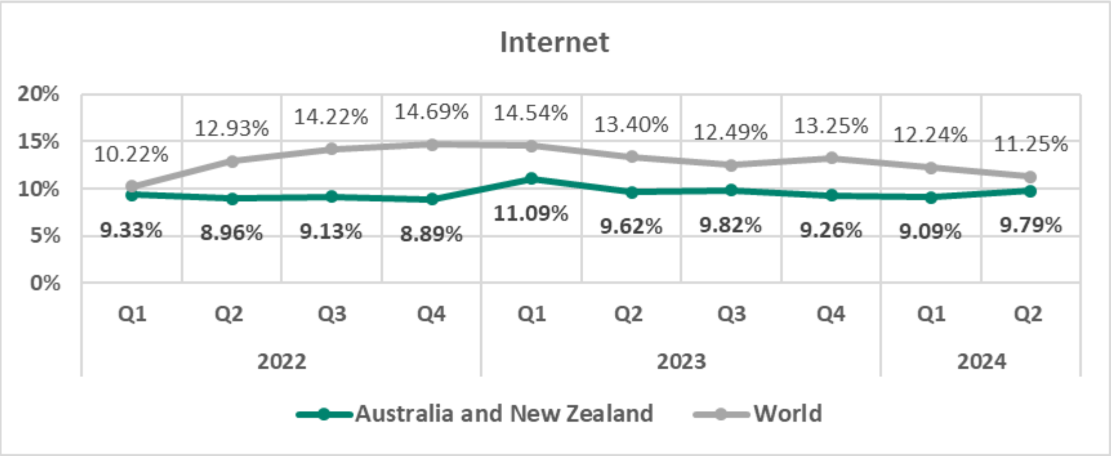

Ransomware
0.22%
0.39%
0.37%
0.29%
0.03%
0.28%
0.02%
0.26%
0.09%
0.18%
0.04%
0.19%
0.07%
0.14%
0.08%
0.17%
0.10%
0.15%
0.16%
0.18%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
Australia and New Zealand

- The heatmap below illustrates changes in the rankings of threat categories in the region over a period of 2.5 years. **Malicious scripts and phishing pages** have been the leading threat category in the region throughout the observed period, while **denylisted internet resources** have consistently ranked second.

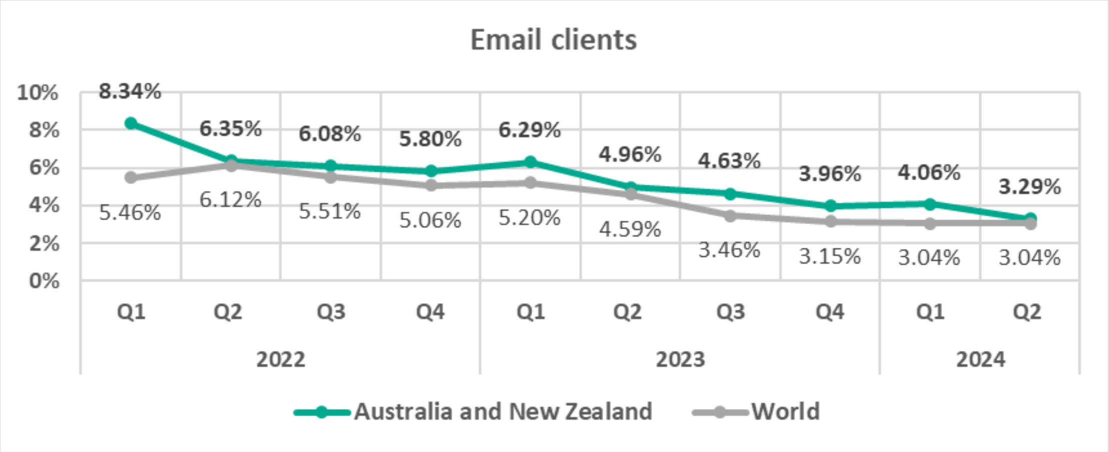
Australia and New Zealand	2022				2023				2024	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Malicious scripts and phishing pages (JS and HTML)	1	1	1	1	1	1	1	1	1	1
Denylisted internet resources	2	2	2	2	2	2	2	2	2	2
Spy Trojans, backdoors and keyloggers	3	3	3	4	3	3	4	4	3	3
Malicious documents (MSOffice + PDF)	4	4	4	3	5	4	3	3	4	4
Miners in the form of executable files for Windows	5	7	7	6	8	8	6	6	6	5
Web miners running in browsers	6	8	6	5	7	6	5	5	5	6
Worms	8	6	8	8	6	6	7	8	7	7
Viruses	7	5	5	7	4	5	8	7	8	8
Ransomware	9	9	9	9	9	9	9	9	9	9
Malware for AutoCAD	10	7	9	9	7	9	10	10	10	10

Threat sources

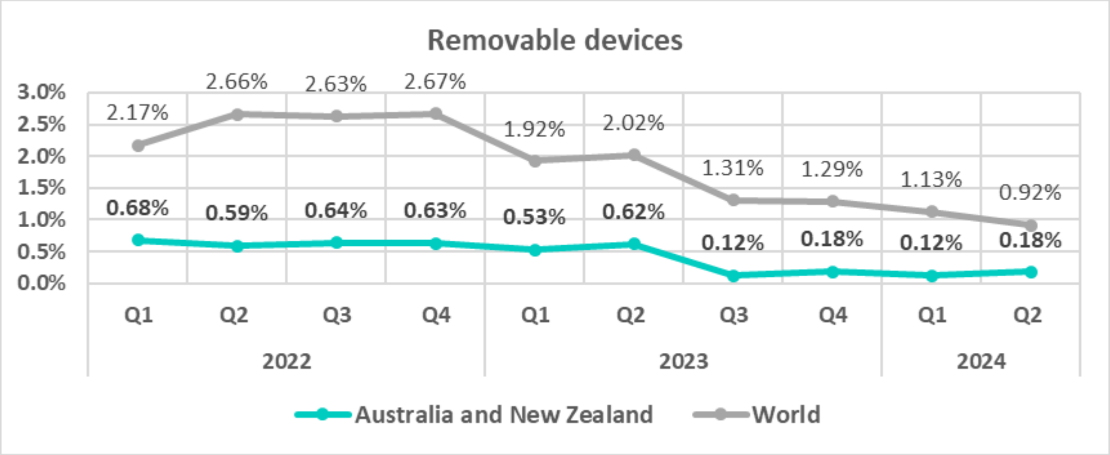
In Q2 2024, the percentage of ICS computers on which threats from the **internet** were blocked increased compared to the previous quarter by a factor of 1.1. The long-term local and global trends had been diverging but the gap between them has generally narrowed in recent quarters.



The long-term trend for **email client** threats shows mostly downward movement, while remaining above the global average throughout the observed period. However, in Q2 2024, the gap narrowed significantly.

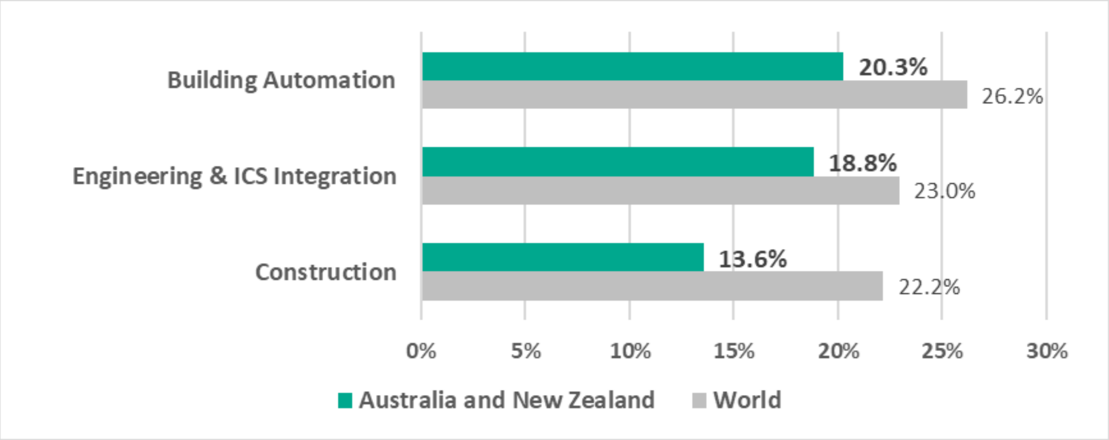


The long-term trend for threats from **removable devices** has been significantly below the global average throughout the observed period. After a noticeable drop in Q3 2023, the rate remained low with some fluctuations, followed by an increase in Q2 2024.

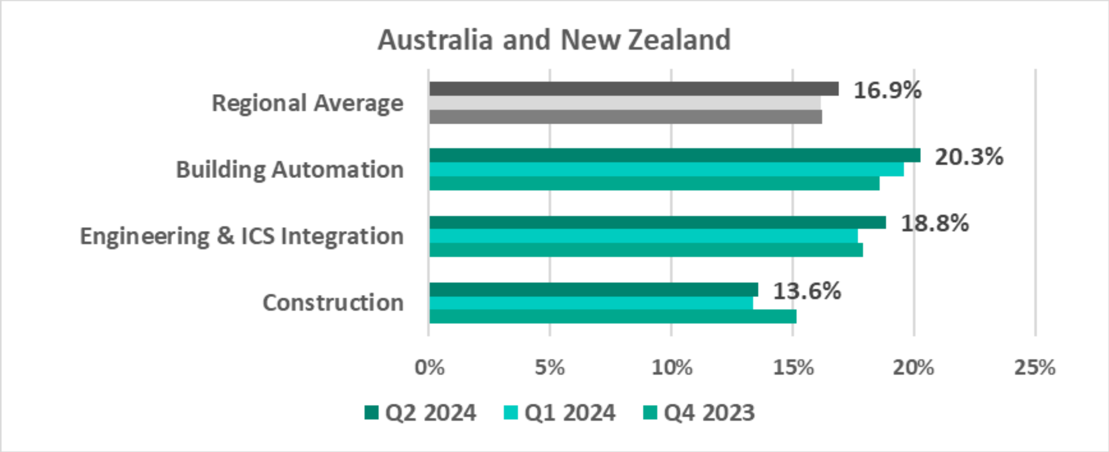


Industries

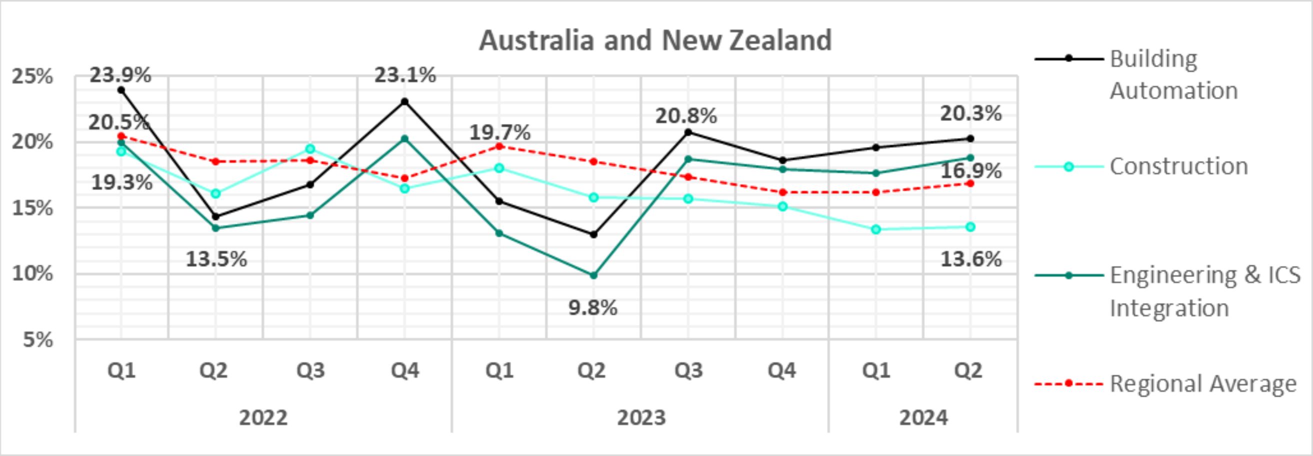
- The most **affected industry** in the region, as selected for this report, was **building automation.**
- Compared to the respective **global averages**, all sectors under study saw a lower percentage of ICS computers on which malicious objects were blocked.



- In **Q2 2024**, all sectors under study exhibited an increase in the percentage of ICS computers on which malicious objects were blocked compared to the previous quarter. The largest increase was in engineering and ICS integration – 1.1 times more.



- The **building automation** and **engineering & ICS integration** sectors exhibit highly fluctuating **trends**, oscillating around the regional average until Q3 2023 in terms of the percentage of ICS computers on which malicious objects were blocked. Both trends have stabilized above the regional average since Q4 2023. Meanwhile, the **construction** sector has shown a mostly downward trend, remaining below the regional average since Q4 2022.



USA and Canada

Current threats

-1-

Malicious scripts and phishing pages

4.63%

▲ **1.1x** increase in Q2

-2-

Denylisted internet resources

4.14%

▲ **1.2x** increase in Q2
3rd in the world **in terms of growth**

-3-

Spyware

1.58%

▲ **1.1x** increase in Q2

Malicious documents

1.15%

▲ **1.1x** increase in Q2

Web miners

0.42%

close to global average
5th threat in the region
vs. 8th in the world

Ransomware

0.14%

▲ **1.7x** increase in Q2
4th in the world **in terms of growth**

Threats from
Internet

7.85%

▲ slight increase in Q2
4th in the world **in terms of growth**

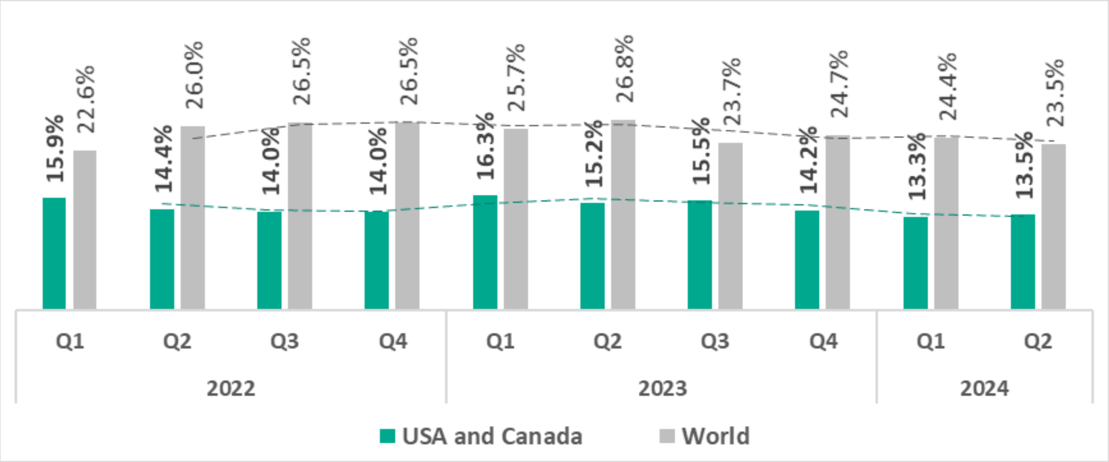
Overall

Twelfth place in the regional ranking.

One of the four regions that saw an increase in the percentage of ICS computers on which malicious objects were blocked, ranking fourth globally for the extent of the increase.

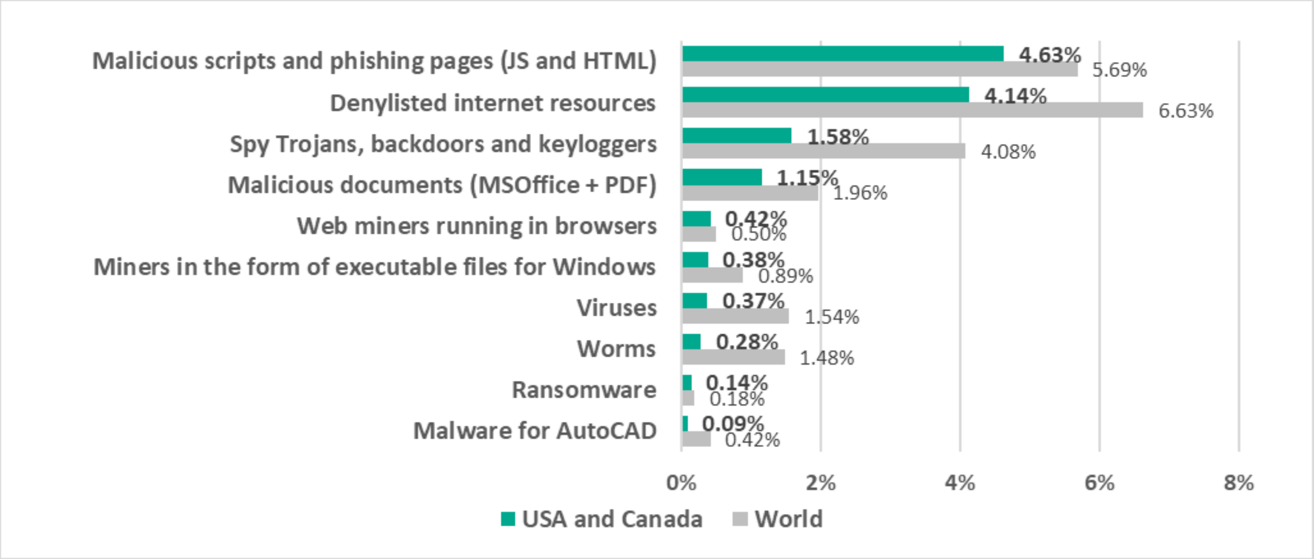
In general, this is one of the safest regions, with one of the lowest percentages of ICS computers on which malicious objects were blocked.

The percentage of ICS computers on which malicious objects were blocked in the region is lower than the global average.



Comparative analysis

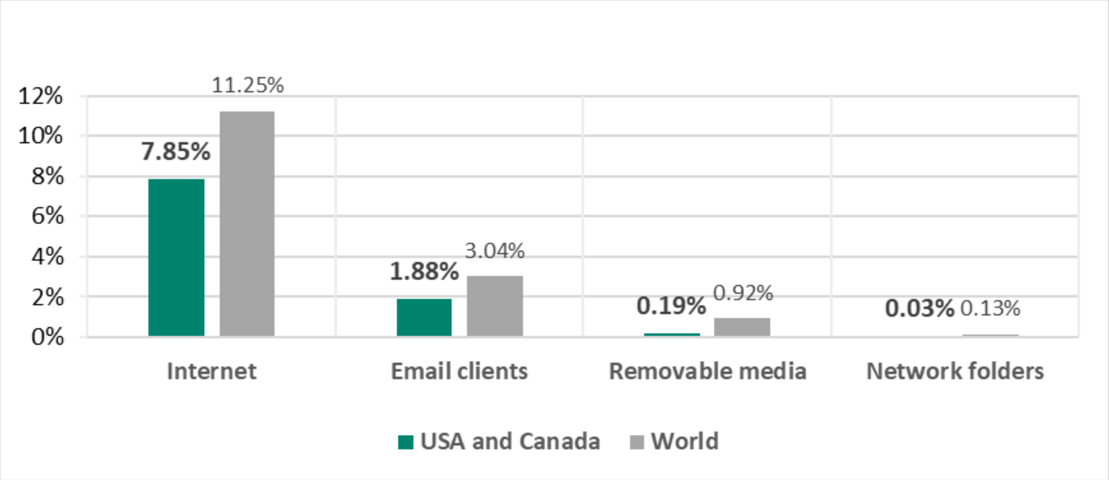
Threat categories



- **Compared to the global average**, the percentage of ICS computers in the region on which each threat type was blocked was lower across all threat types.
- **Web miners were fifth** in the ranking of malware categories by percentage of ICS computers on which they were blocked (eighth globally). Since the beginning of 2024, the percentage of ICS computers on which threats from this category were blocked in the region is close to the global average.

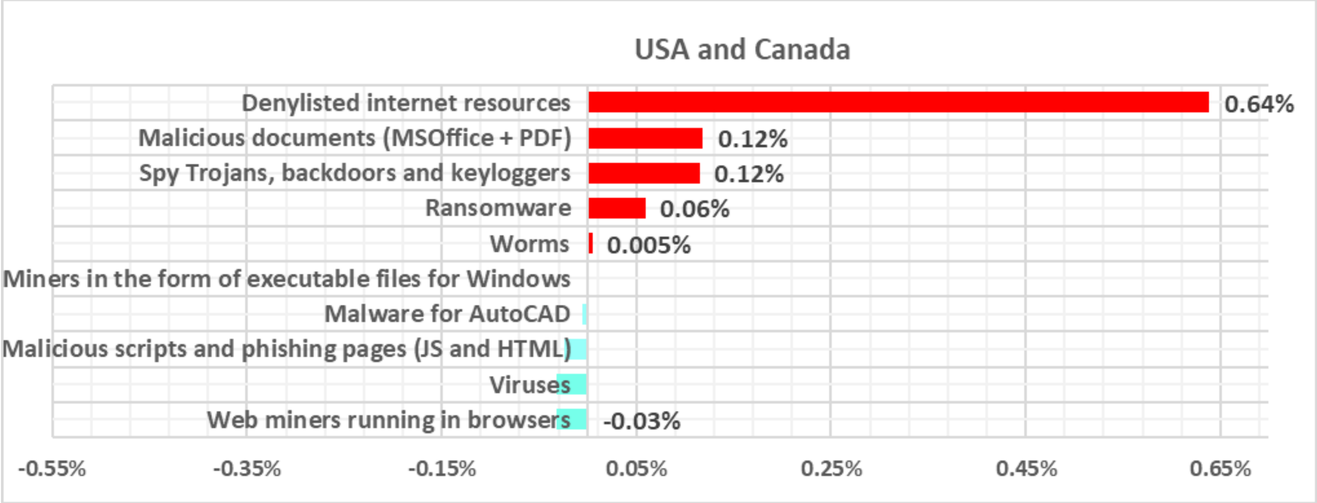
Threat sources

All threat sources showed values noticeably below their respective global averages.

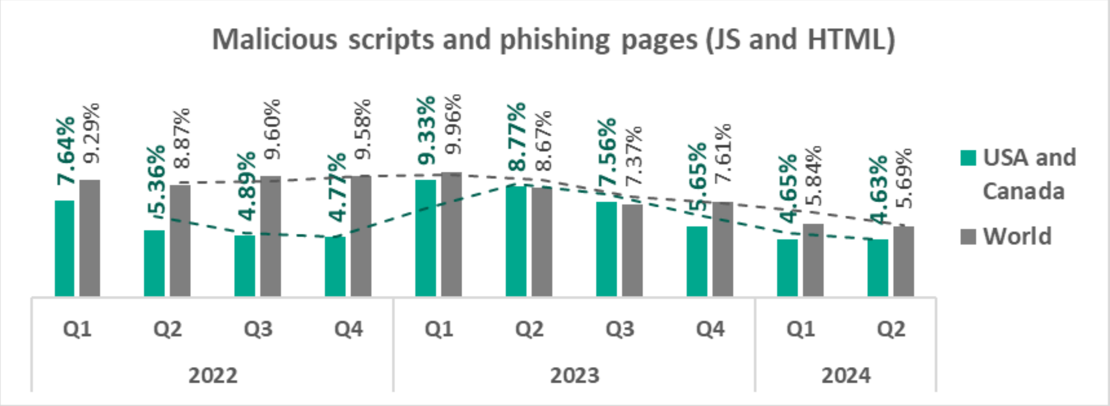


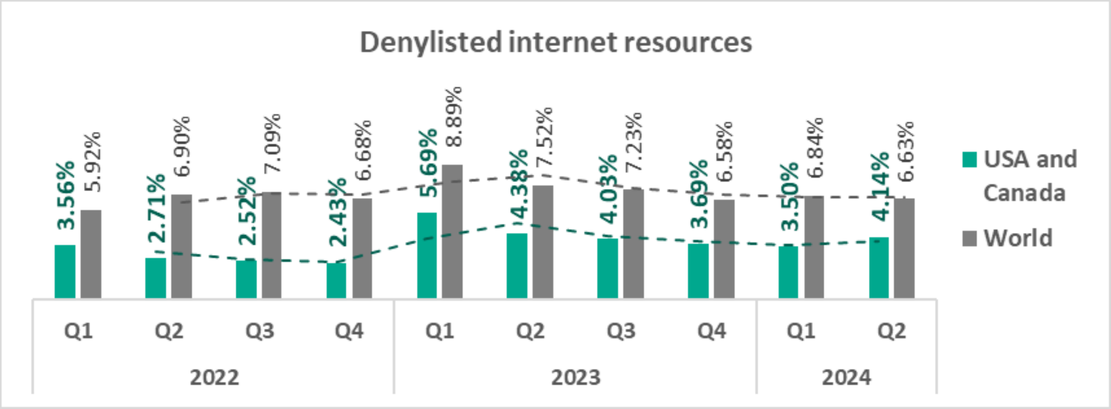
Quarterly changes and trends

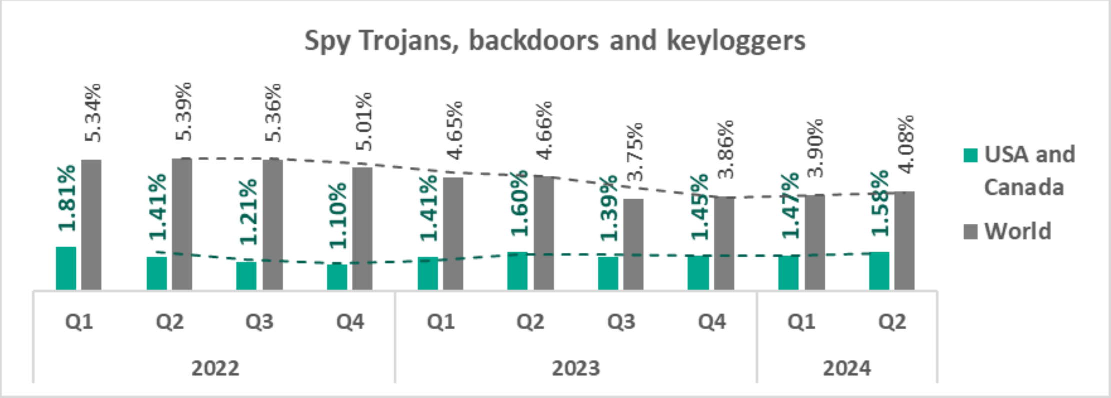
Threat categories

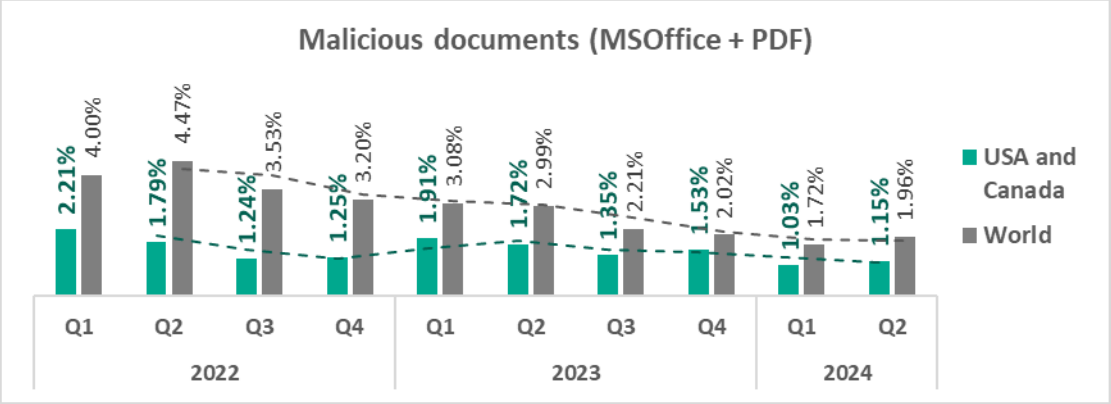


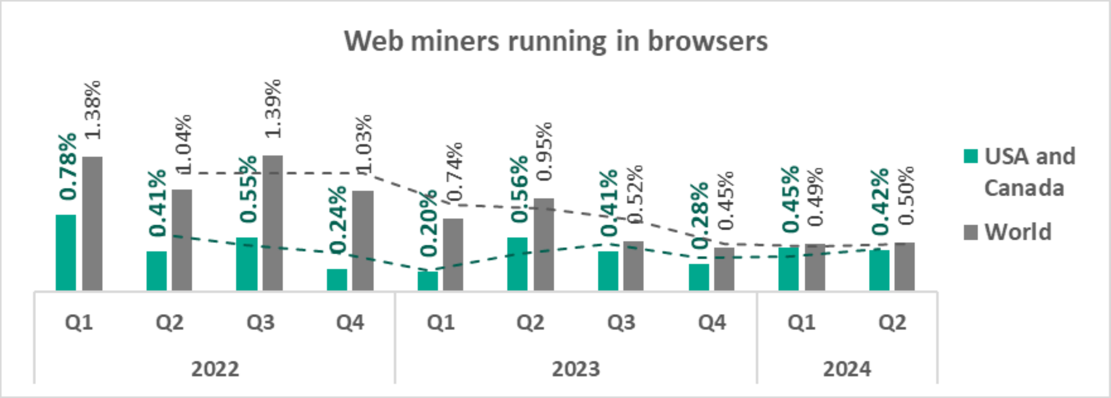
- The **largest quarterly increase** was in the percentage of ICS computers on which the following were blocked:
  - ➢ Ransomware – 1.8 times higher, ranking third globally by the size of the increase. As a result, the percentage for ransomware in the region was close to the global figure
  - ➢ Denylisted internet resources – 1.2 times higher, ranking third globally by the size of the increase
  - ➢ Spyware – 1.1 times higher
  - ➢ Malicious documents – 1.1 times higher
- The **top threat** categories exhibit various quarterly dynamics:

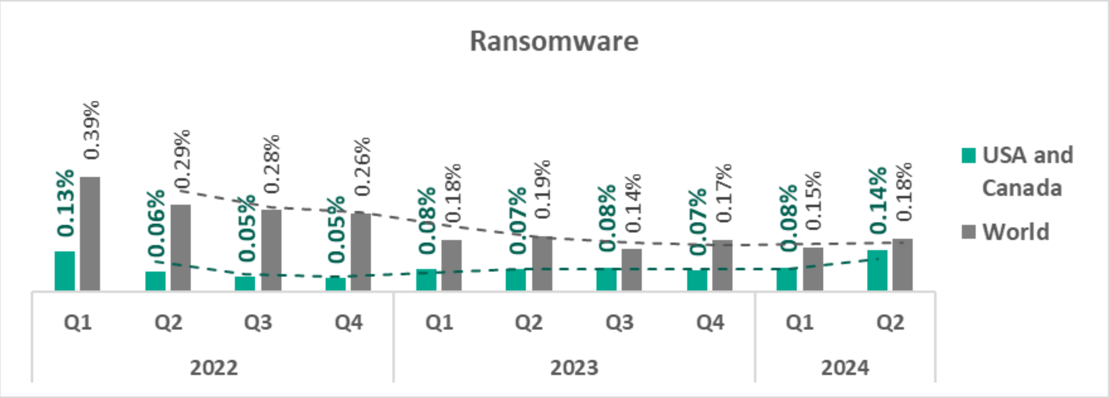



Denylisted internet resources
3.56%
5.92%
2.71%
6.90%
2.52%
7.09%
2.43%
6.68%
5.69%
8.89%
4.38%
7.52%
4.03%
7.23%
3.69%
6.58%
3.50%
6.84%
4.14%
6.63%
Q1
Q2
Q3
Q4
2022
Q1
Q2
Q3
Q4
2023
Q1
Q2
2024
USA and Canada
World


Spy Trojans, backdoors and keyloggers
1.81%
5.34%
1.41%
5.39%
1.21%
5.36%
1.10%
5.01%
1.41%
4.65%
1.60%
4.66%
1.39%
3.75%
1.45%
3.86%
1.47%
3.90%
1.58%
4.08%
Q1
Q2
Q3
Q4
2022
Q1
Q2
Q3
Q4
2023
Q1
Q2
2024
USA and Canada
World


Malicious documents (MSOffice + PDF)
2.21%
4.00%
1.79%
4.47%
1.24%
3.53%
1.25%
3.20%
1.91%
3.08%
1.72%
2.99%
1.35%
2.21%
1.53%
2.02%
1.03%
1.72%
1.15%
1.96%
Q1
Q2
Q3
Q4
2022
Q1
Q2
Q3
Q4
2023
Q1
Q2
2024
USA and Canada
World


Web miners running in browsers
0.78%
1.38%
0.41%
1.04%
0.55%
1.39%
0.24%
1.03%
0.20%
0.74%
0.56%
0.95%
0.41%
0.52%
0.28%
0.45%
0.45%
0.49%
0.42%
0.50%
Q1
Q2
Q3
Q4
2022
Q1
Q2
Q3
Q4
2023
Q1
Q2
2024
USA and Canada
World



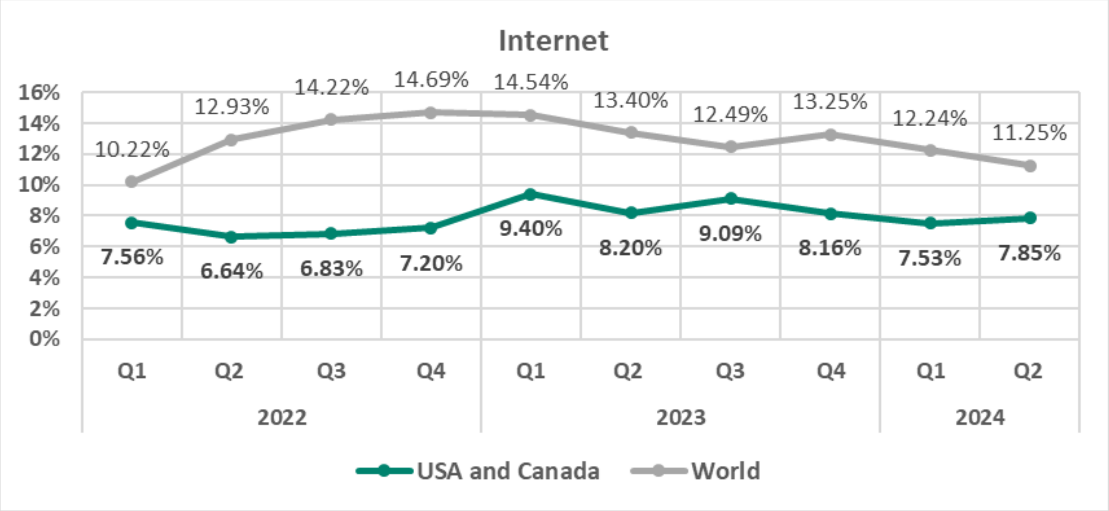
- The heatmap below illustrates changes in the rankings of threat categories in the region over a period of 2.5 years. **Malicious scripts and phishing pages** have been the leading threat category in the region throughout the observed period, while **denylisted internet resources** have consistently ranked second. **Spyware** has ranked third for two quarters in a row.

USA and Canada	2022				2023				2024	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Malicious scripts and phishing pages (JS and HTML)	1	1	1	1	1	1	1	1	1	1
Denylisted internet resources	2	2	2	2	2	2	2	2	2	2
Spy Trojans, backdoors and keyloggers	4	4	4	4	4	4	3	4	3	3
Malicious documents (MSOffice + PDF)	3	3	3	3	3	3	4	3	4	4
Web miners running in browsers	6	6	5	5	7	5	5	7	5	5
Miners in the form of executable files for Windows	5	5	6	6	8	6	6	8	7	6
Viruses	8	8	8	7	6	7	7	5	6	7
Worms	7	7	7	8	5	8	8	6	8	8
Ransomware	9	9	9	9	10	10	9	9	10	9
Malware for AutoCAD	10	10	10	10	9	9	10	10	9	10

Threat sources

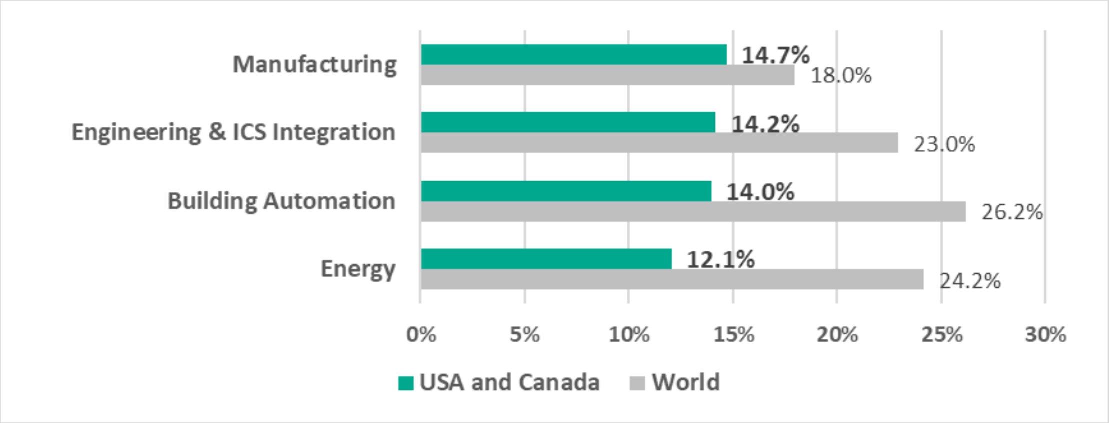
In Q2 2024, the percentage of ICS computers on which threats from the **internet** were blocked increased compared to the previous quarter – by 1.1 times. USA and Canada is one of the four regions that saw an increase, ranking **fourth globally** by the size of the increase.

The local and global trends for threats from the internet initially diverged, but the gap between them has gradually narrowed since Q1 2023.

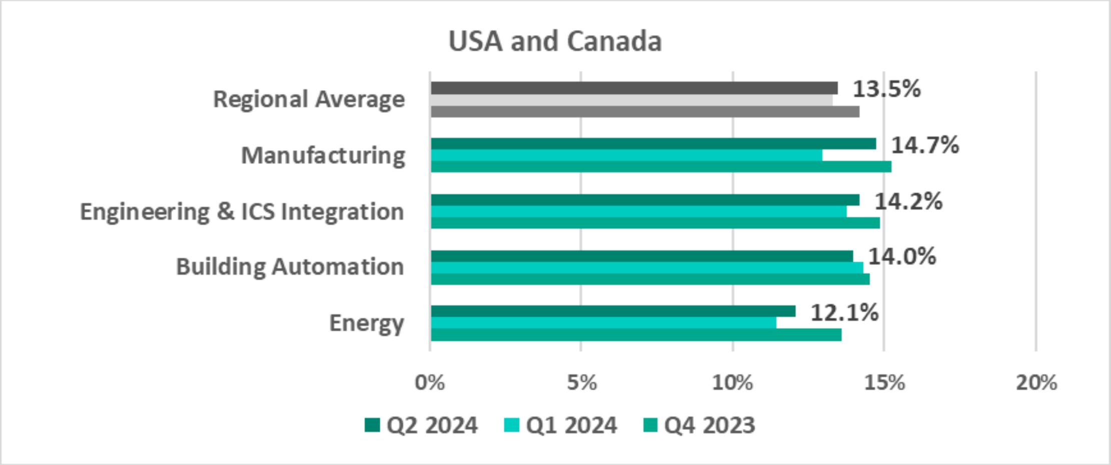


Industries

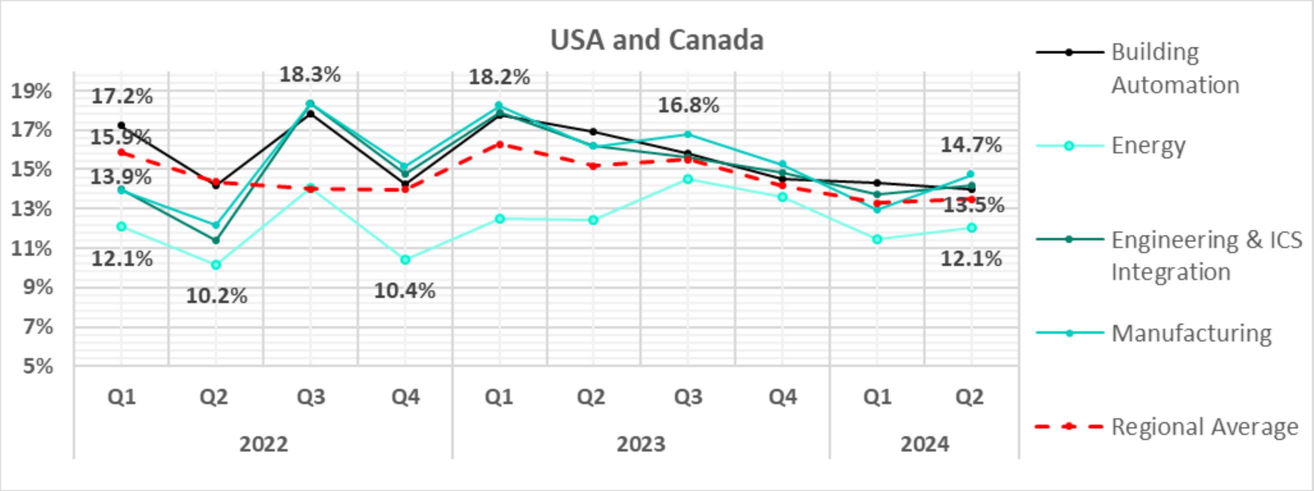
- The most **affected** industry in the region, as highlighted in this report, was **manufacturing**. It ranked fifth in the global ranking for the sector.
- From a **global perspective**, all sectors in the region remained significantly below the respective global averages.



- In **Q2 2024**, all sectors except for building automation exhibited an increase in the percentage of ICS computers on which malicious objects were blocked. The largest increase was in the following sectors:
  - Manufacturing, 1.1 times higher
  - Energy, 1.1 times higher



- All sectors under study exhibited highly fluctuating **trends** in the percentage of ICS computers on which malicious objects were blocked until Q1 2023. Since Q3 2023, the trends have stabilized around the regional average, which has shown a mostly downward trend since then.



Western Europe

Current threats

-1-

Denylisted internet resources

4.86%

▲ **1.3x** increase in Q2
1st in the world **in terms of growth**

-2-

Malicious scripts and phishing pages

3.72%

▲ **1.1x** increase in Q2
3rd in the world **in terms of growth**

-3-

Spyware

1.75%

▲ **1.2x** increase in Q2

Malicious documents

1.60%

▲ **1.6x** increase in Q2
1st in the world **in terms of growth**

Ransomware

0.08%

▲ **1.6x** increase in Q2

Threats from
Internet

7.34%

▲ **1.1x** increase in Q2
3rd in the world **in terms of growth**

Threats from
Email clients

2.53%

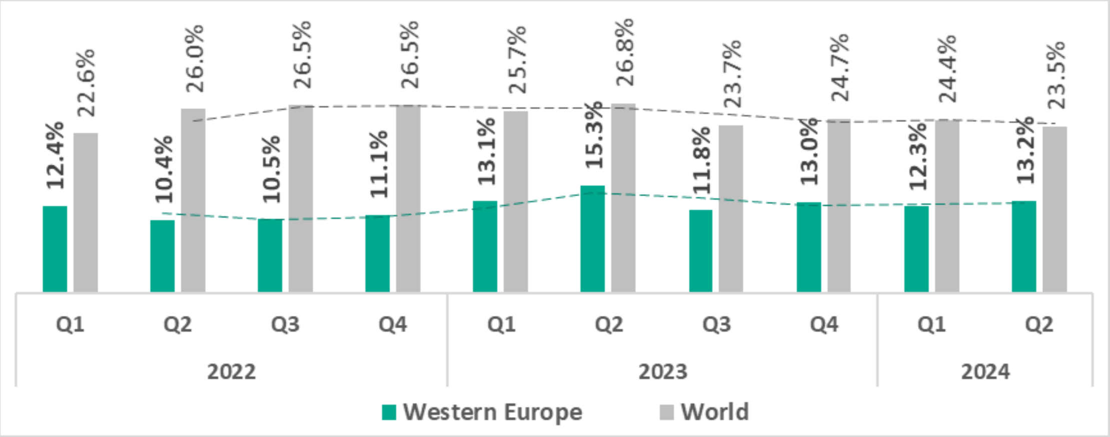
▲ **1.2x** increase in Q2
2nd in the world **in terms of growth**

Overall

Thirteenth place in the regional ranking.

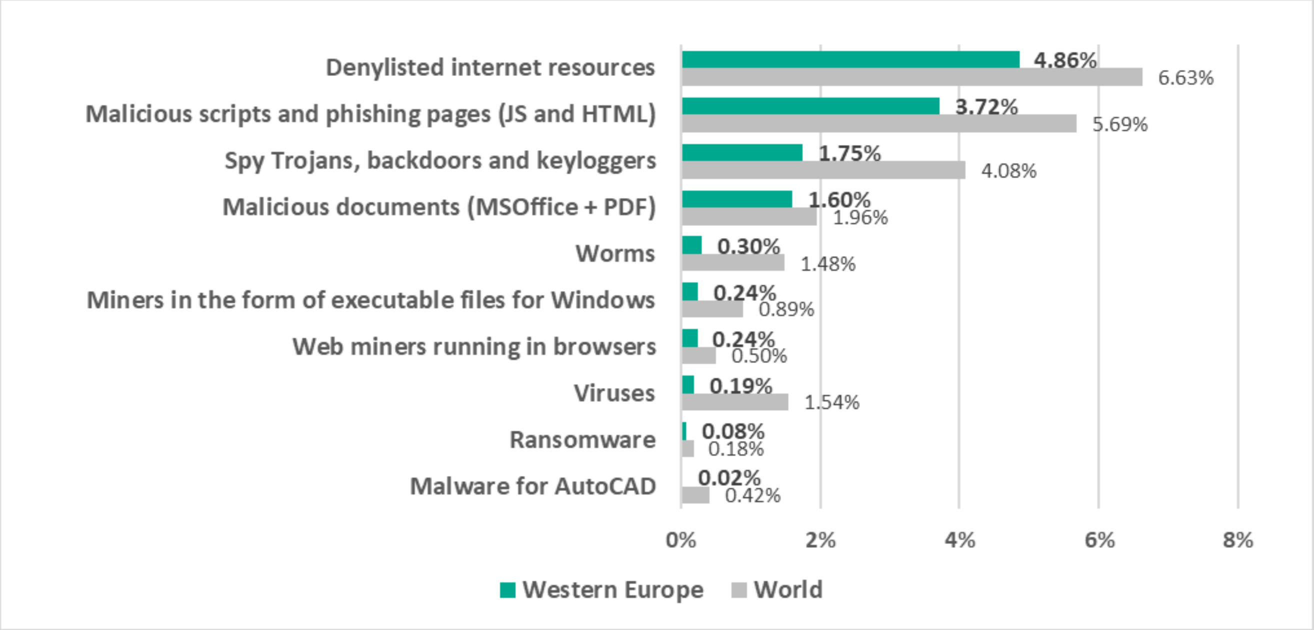
Western Europe is one of the four regions that saw an increase in the percentage of ICS computers on which malicious objects were blocked – by 1.1 times. The region ranked second in the world by the size of the increase.

In general, this is one of the safest regions, with one of the lowest percentages of ICS computers on which malicious objects were blocked. The percentage in this region is noticeably lower than the global average.



Comparative analysis

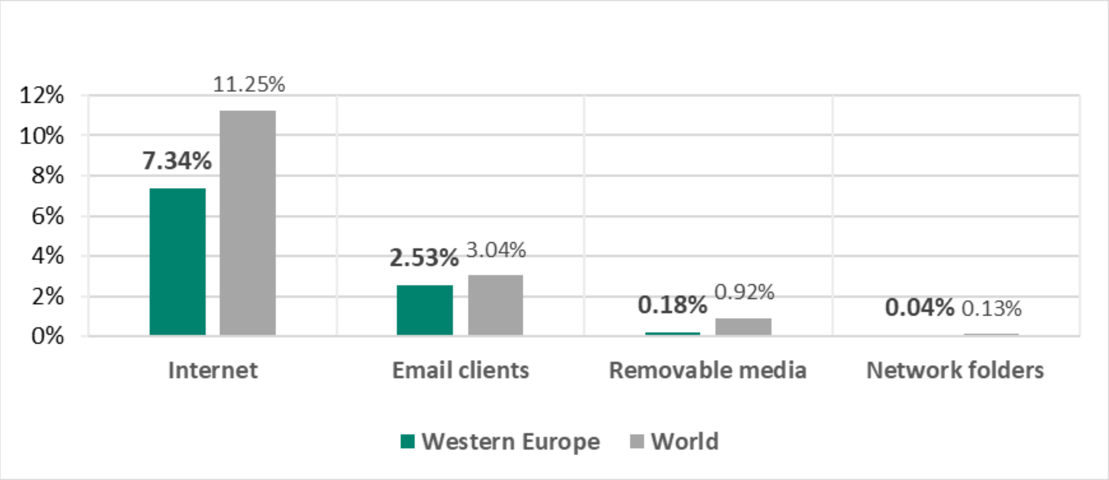
Threat categories



Compared to the global average, the percentage of ICS computers in the region on which each threat type was blocked was noticeably lower across all threat types.

Threat sources

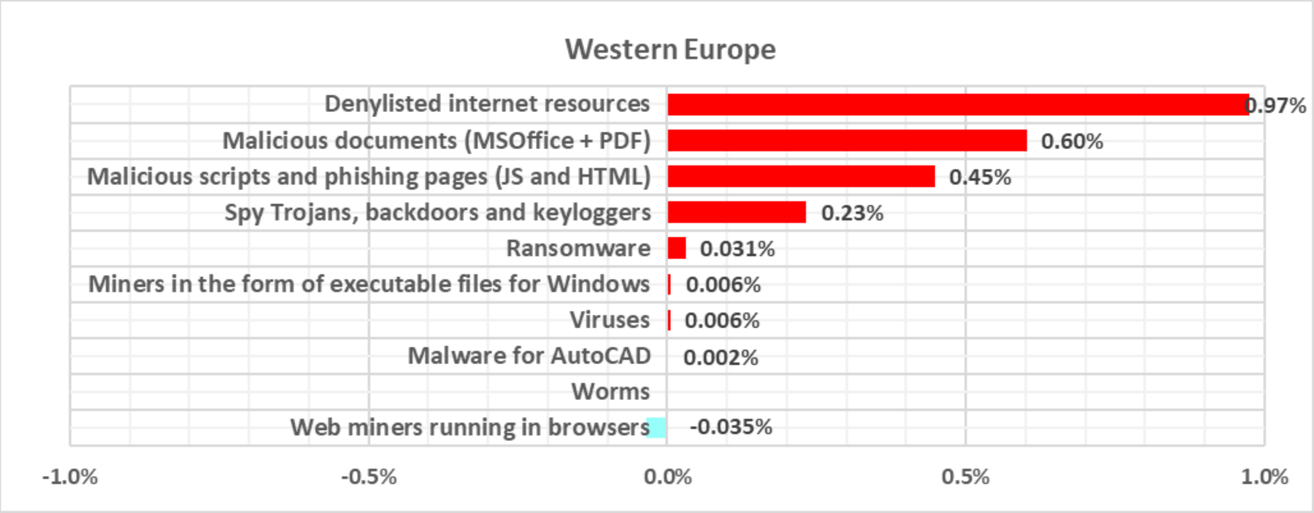
All threat sources showed values noticeably below their respective global averages.



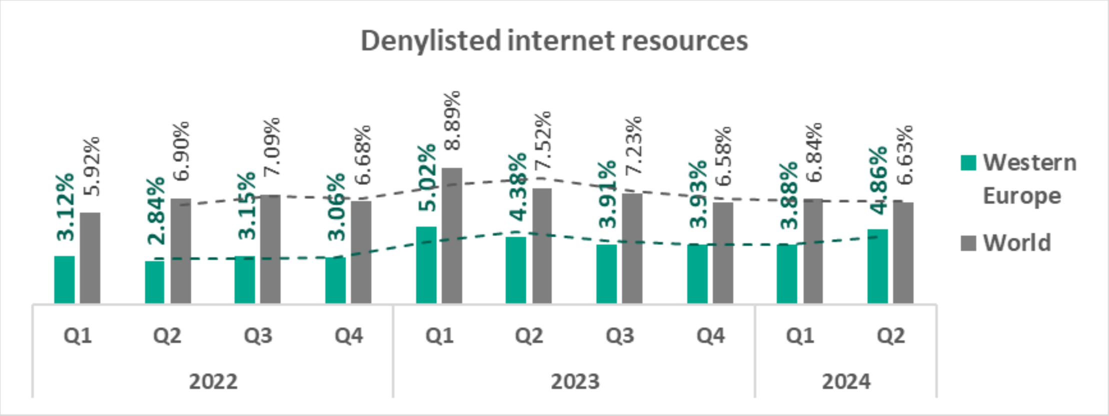
Quarterly changes and trends

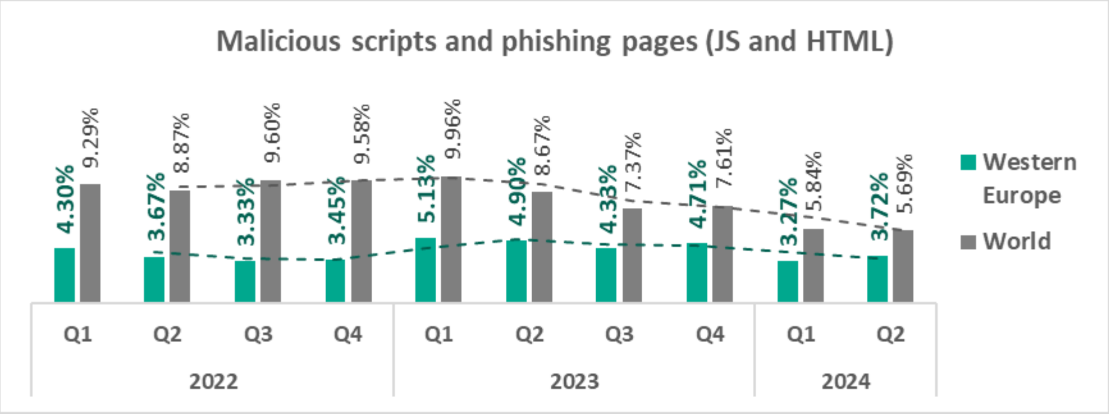
Threat categories

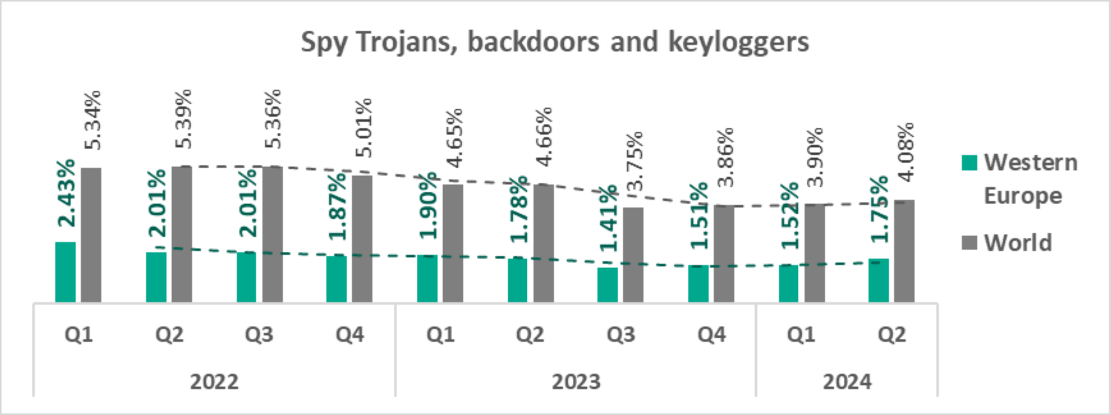
The majority of threat categories exhibited an increase in the percentage of ICS computers on which malicious objects were blocked.

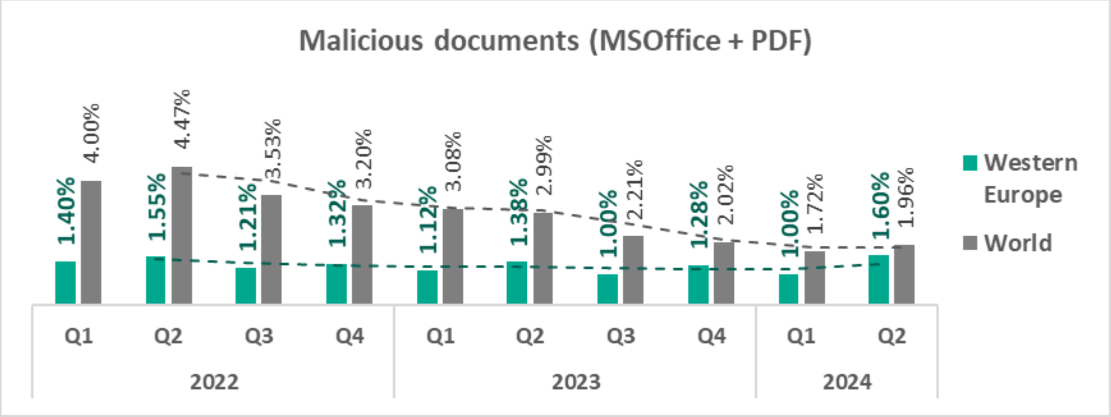


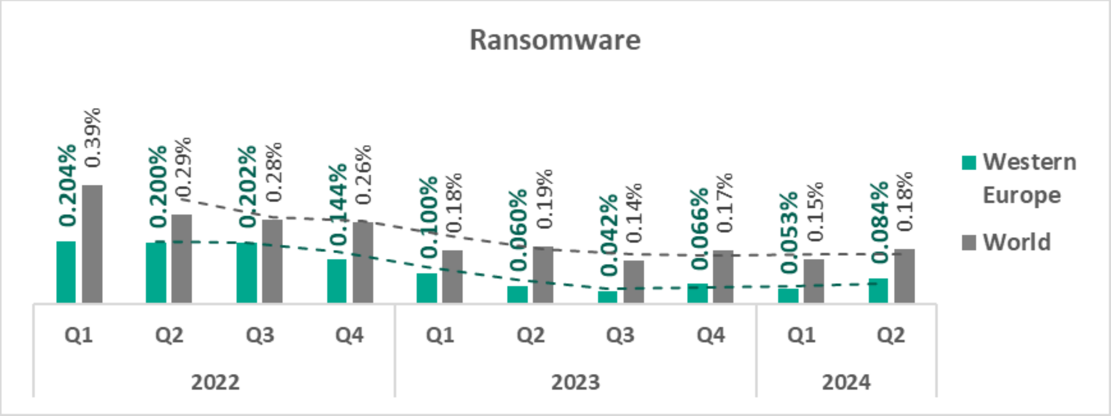
- The **largest quarterly increase** was in the percentage of ICS computers on which the following were blocked:
  - Malicious documents – 1.6 times higher, ranking first globally by the size of the increase
  - Ransomware – 1.6 times higher
  - Denylisted internet resources – 1.3 times higher, ranking first globally by the size of the increase
  - Spyware – 1.1 times higher
  - Malicious scripts and phishing pages – 1.1 times higher, ranking third globally by the size of the increase
  - Malware for AutoCAD – 1.1 times higher
- The **top threat** categories exhibit various quarterly dynamics:






Spy Trojans, backdoors and keyloggers
2.43%
5.34%
2.01%
5.39%
2.01%
5.36%
1.87%
5.01%
1.90%
4.65%
1.78%
4.66%
1.41%
3.75%
1.51%
3.86%
1.52%
3.90%
1.75%
4.08%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
Western Europe
World


Malicious documents (MSOffice + PDF)
1.40%
4.00%
1.55%
4.47%
1.21%
3.53%
1.32%
3.20%
1.12%
3.08%
1.38%
2.99%
1.00%
2.21%
1.28%
2.02%
1.00%
1.72%
1.60%
1.96%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
Western Europe
World


Ransomware
0.204%
0.39%
0.200%
0.29%
0.202%
0.28%
0.144%
0.26%
0.100%
0.18%
0.060%
0.19%
0.042%
0.14%
0.066%
0.17%
0.053%
0.15%
0.084%
0.18%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
Western Europe
World

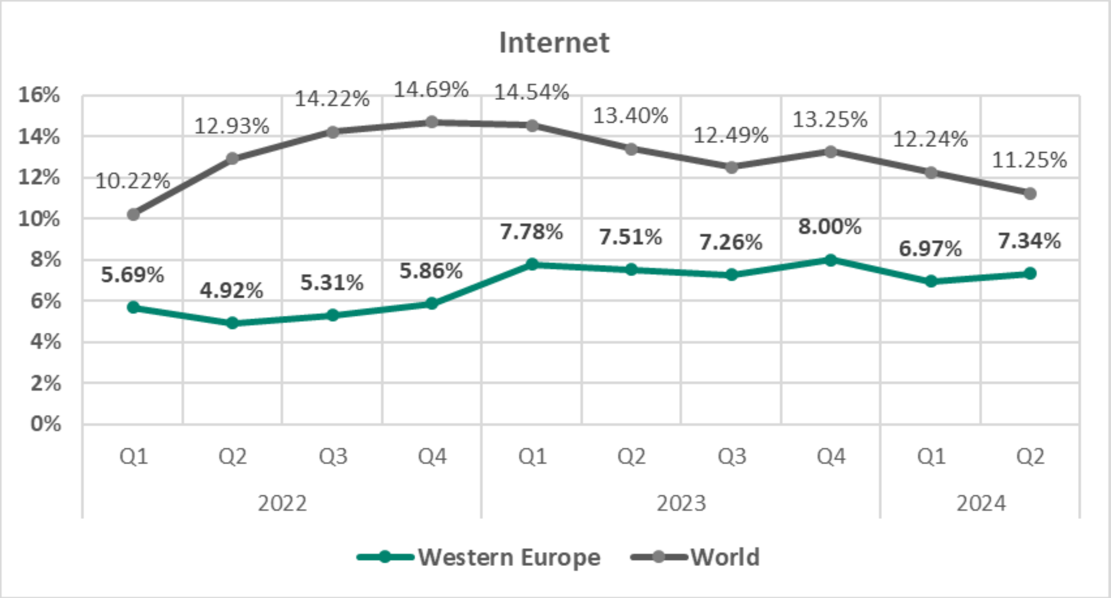
- The heatmap below illustrates changes in the rankings of threat categories in the region over a period of 2.5 years. Usually ranked second, **denylisted internet resources** moved up to first place in Q1 2024, pushing **malicious scripts and phishing pages** down to second. **Worms** have climbed from seventh in Q1 2022 to fifth in Q2 2024.

Western Europe	2022				2023				2024	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Denylisted internet resources	2	2	2	2	2	2	2	2	1	1
Malicious scripts and phishing pages (JS and HTML)	1	1	1	1	1	1	1	1	2	2
Spy Trojans, backdoors and keyloggers	3	3	3	3	3	3	3	3	3	3
Malicious documents (MSOffice + PDF)	4	4	4	4	4	4	4	4	4	4
Worms	7	7	7	6	5	7	6	5	5	5
Miners in the form of executable files for Windows	5	5	6	7	8	6	7	8	7	6
Web miners running in browsers	6	6	5	5	6	5	5	6	6	7
Viruses	9	9	9	9	7	8	8	7	8	8
Ransomware	8	8	8	8	9	9	9	9	9	9
Malware for AutoCAD	10	10	10	10	10	10	10	10	10	10

Threat sources

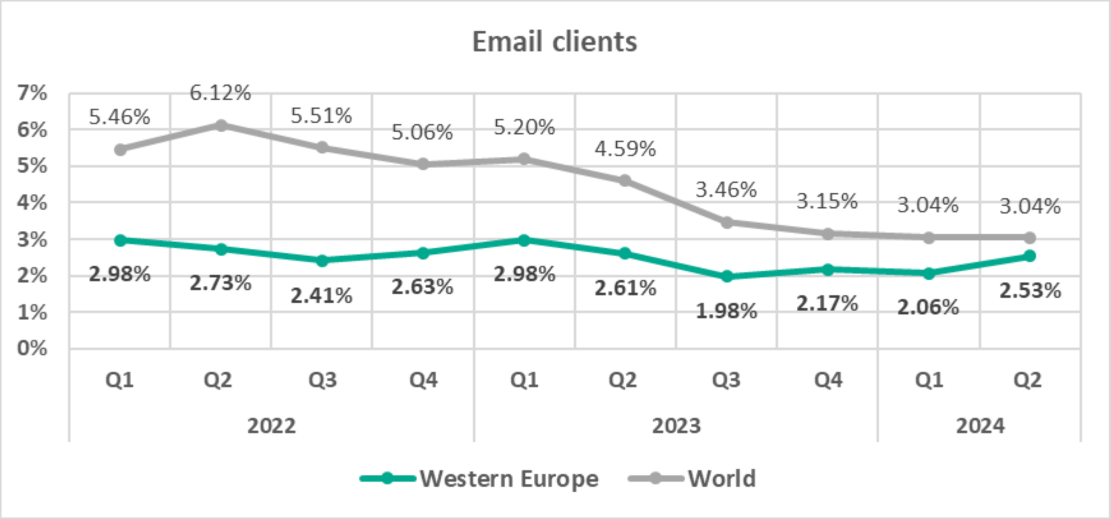
- Western Europe was among the only three regions that exhibited growth in the percentage of ICS computers on which threats from the **internet** were blocked.

  The local and global trends for threats from the **internet** initially diverged, but the gap between the two has been gradually narrowing since Q1 2023.



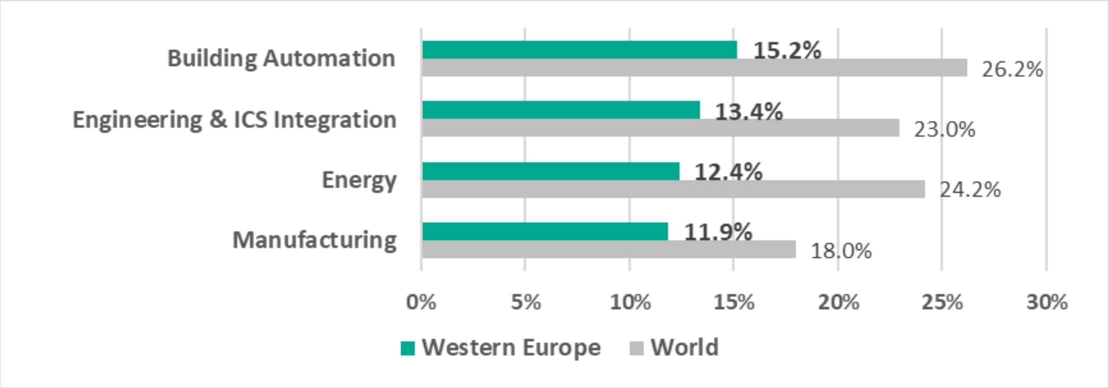
- The region also ranked **second in the world** in terms of the growth in the percentage of ICS computers on which threats distributed via **email clients** were blocked.

In Q2 2024, the gap between the long-term global and regional trends for threats from email clients narrowed to its smallest value during the observed period.

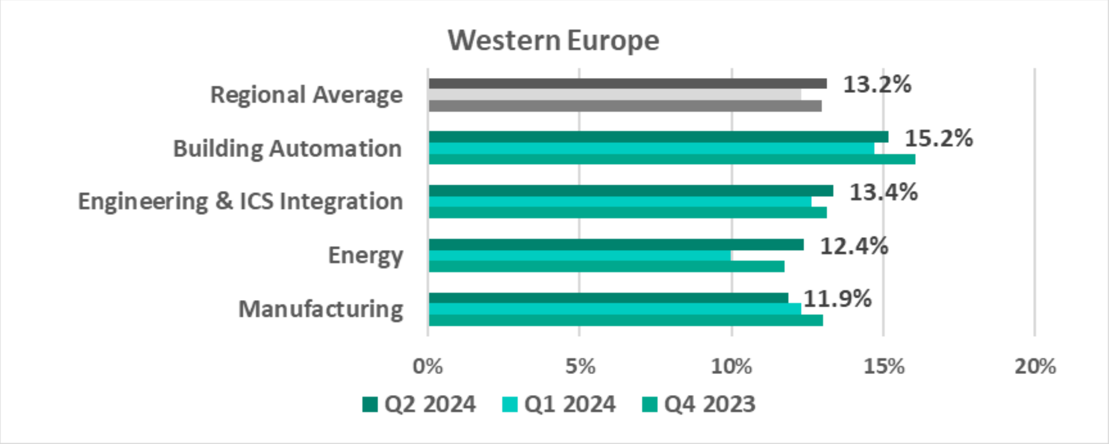


Industries

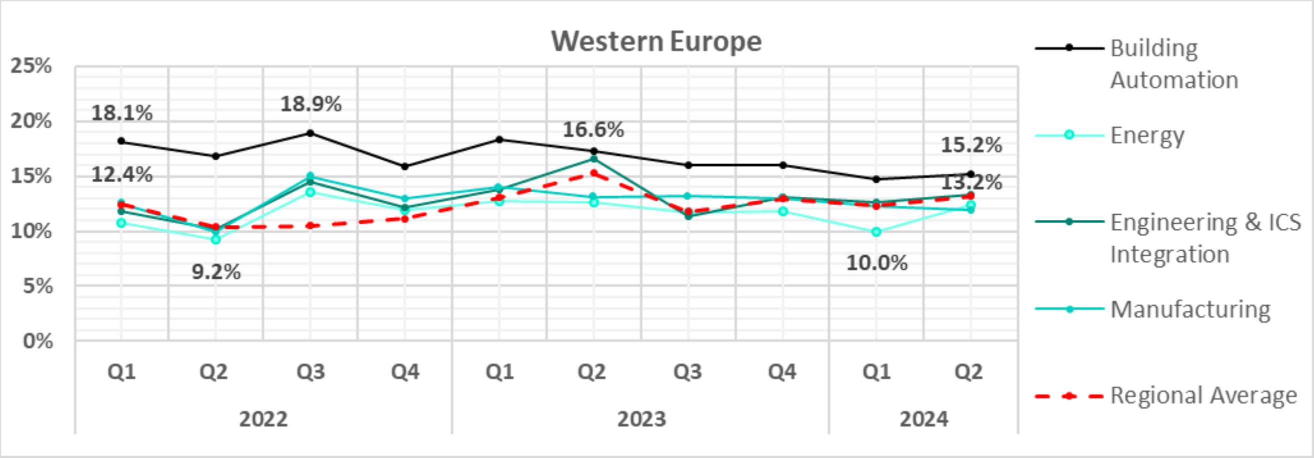
- The most **affected** industry in the region, as featured in this report, was **building automation**.
- From a **global perspective**, all sectors in the region remained significantly below the respective global averages.



- In **Q2 2024**, all sectors except for manufacturing exhibited an increase in the percentage of ICS computers on which malicious objects were blocked. The largest increase was in the following sectors:
  - ➢ Energy – 1.2 times higher
  - ➢ Engineering and ICS integration – 1.1 times higher



- All sectors under study exhibited fluctuating **trends** in the percentage of ICS computers on which malicious objects were blocked. Building automation exhibits a gradual downward trend.



Northern Europe

Current threats

-1-

Denylisted internet resources

3.79%

▲ slight increase in Q2

-2-

Malicious scripts and phishing pages

2.64%

▲ slight increase in Q2

-3-

Spyware

1.83%

▲ **1.1x** increase in Q2

Malicious documents

0.86%

▲ **1.5x** increase in Q2

Executable miners

0.45%

▲ **1.6x** increase in Q2
– 6th threat in the region
vs. 8th in the world

Ransomware

0.08%

▲ **1.5x** increase in Q2

Threats from
Internet

6.03%

▼ decrease in Q2

Threats from
Email clients

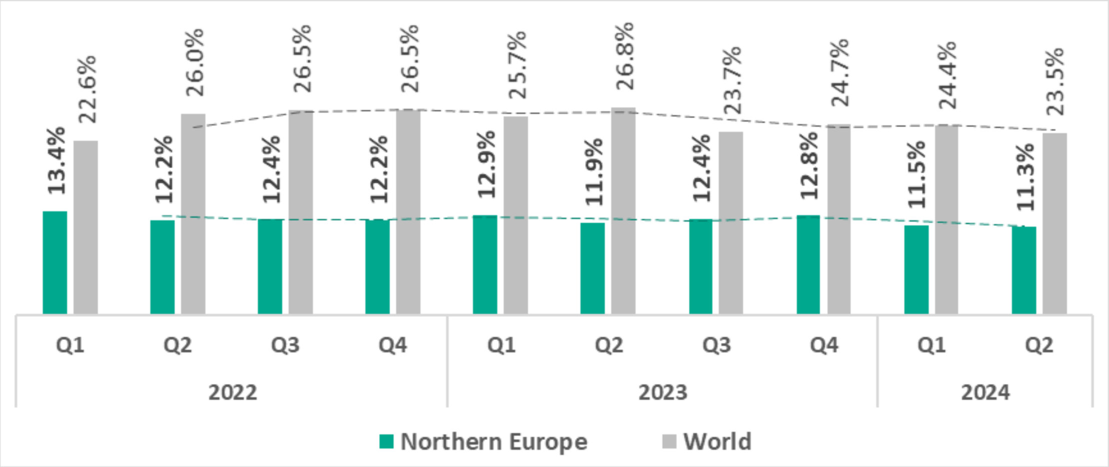
1.71%

▲ **1.1x** increase in Q2

Overall

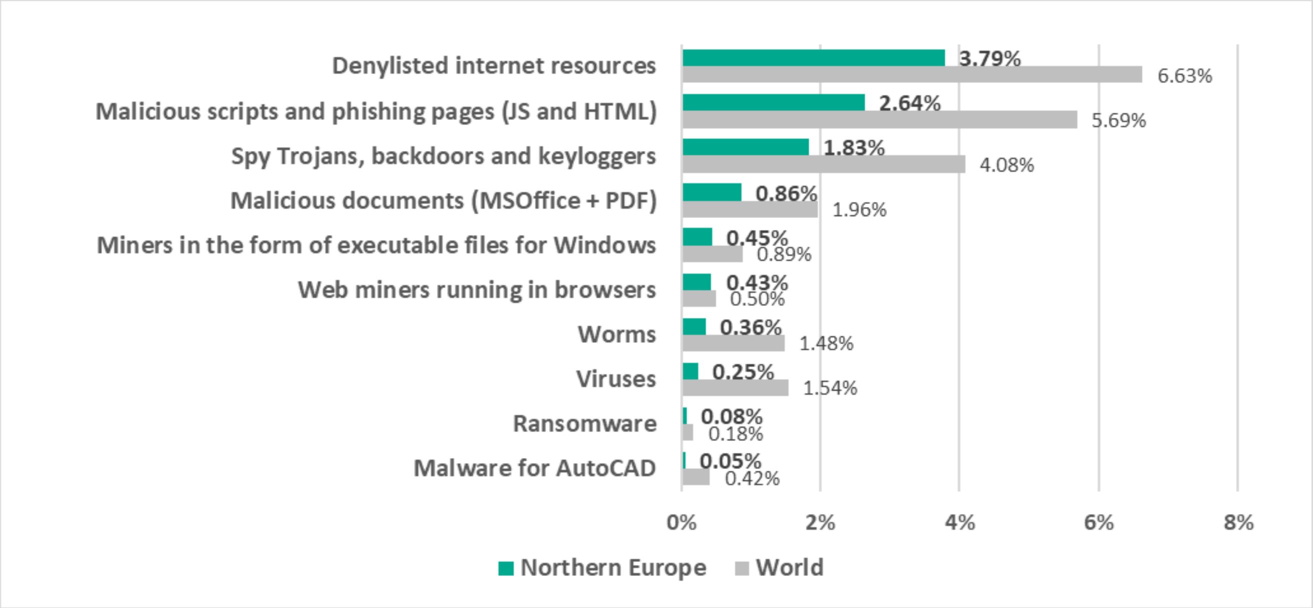
Fourteenth place in the regional ranking.

Traditionally the region has the lowest percentage of ICS computers on which malicious objects were blocked. The percentage is noticeably below the global average.



Comparative analysis

Threat categories

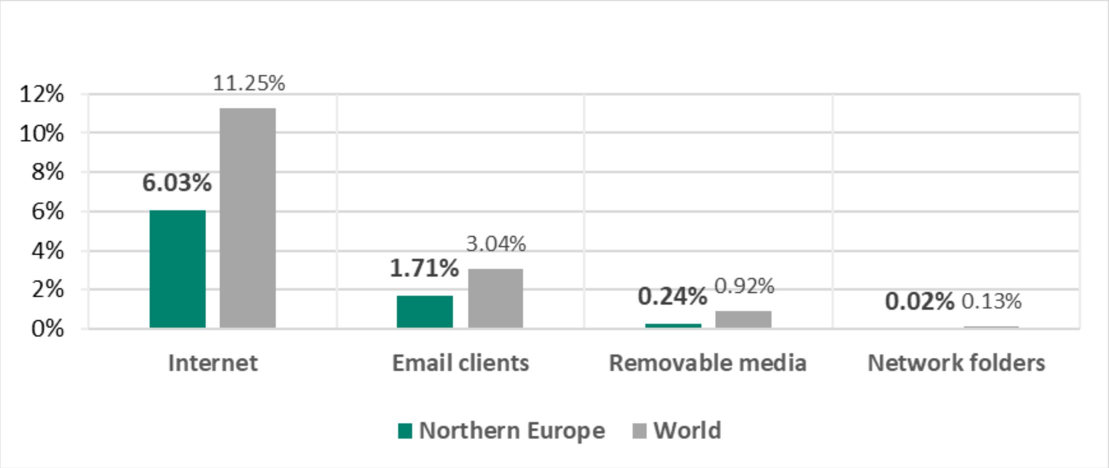


For all threat types, the percentage of ICS computers in the region on which each was blocked was noticeably lower than the corresponding global average.

- **Miners in the form of executable files for Windows were fifth** in the ranking of threat categories by percentage of ICS computers on which they were blocked (seventh globally). The percentage has been growing since Q1 2024.
- **Web miners were sixth** in the ranking of threat categories by percentage of ICS computers on which they were blocked (eighth globally). The percentage is close to the global average.

Threat sources

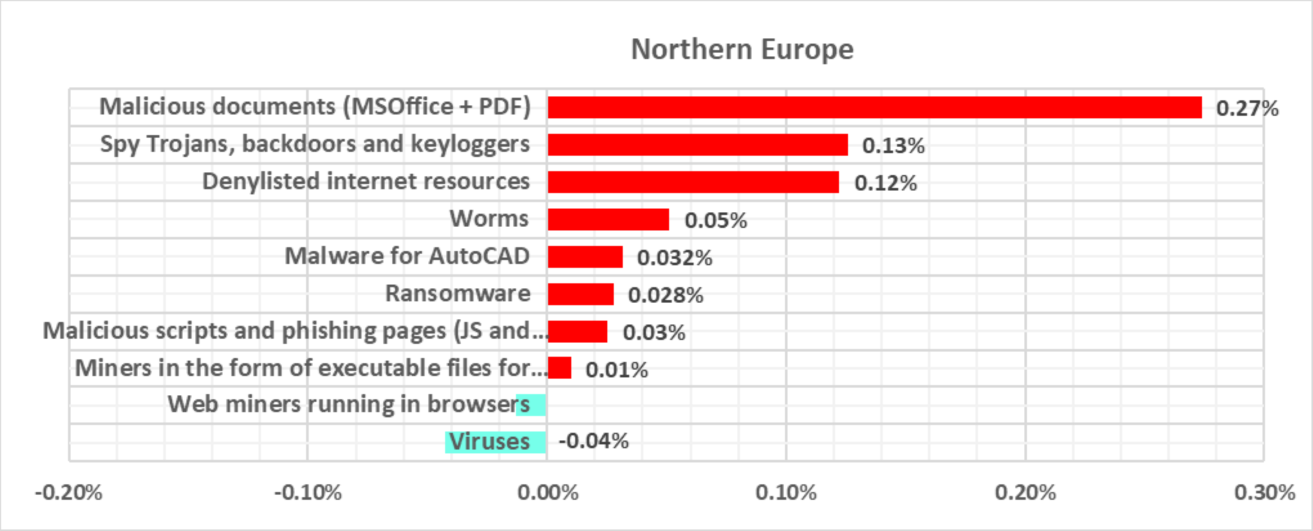
All threat sources showed values noticeably below their respective global averages.



Quarterly changes and trends

Threat categories

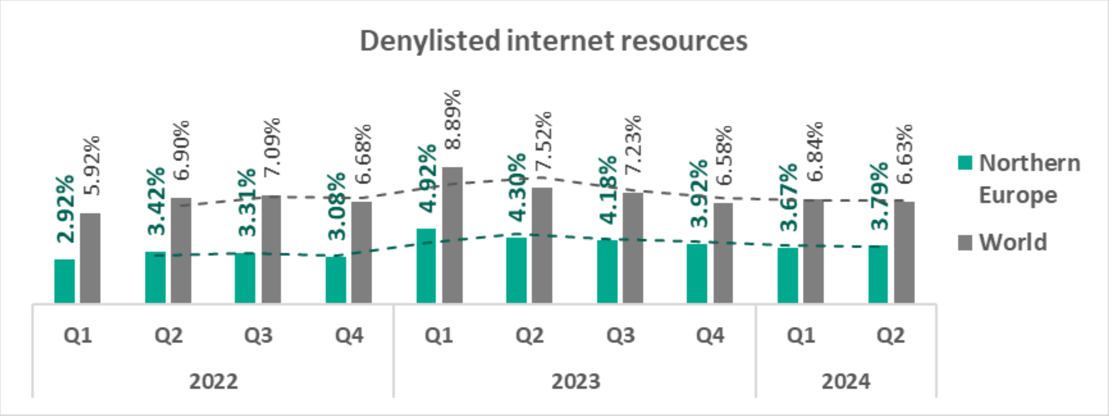
The majority of threat categories exhibited an increase in the percentage of ICS computers on which malicious objects were blocked.

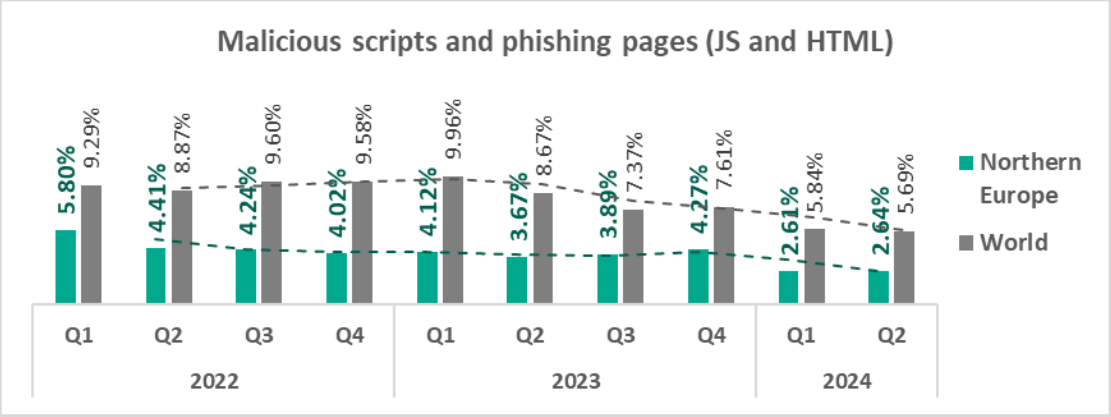


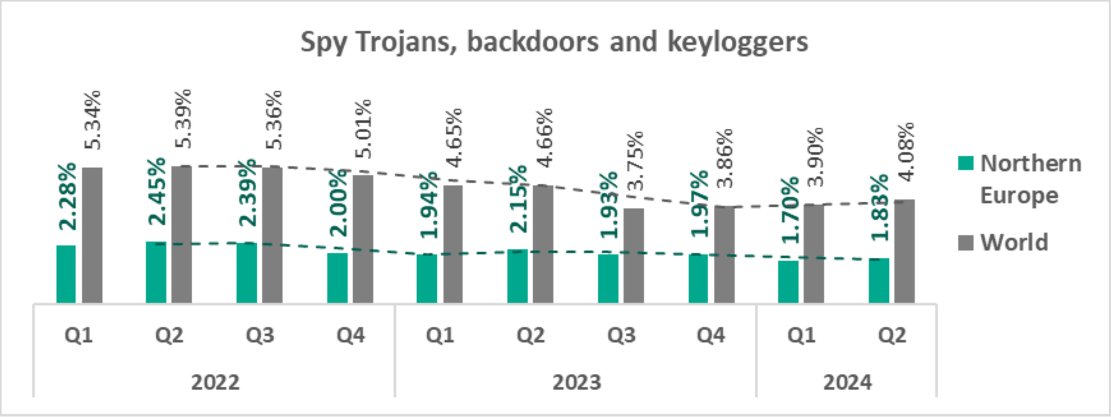
The **largest quarterly increase** was in the percentage of ICS computers on which the following were blocked:

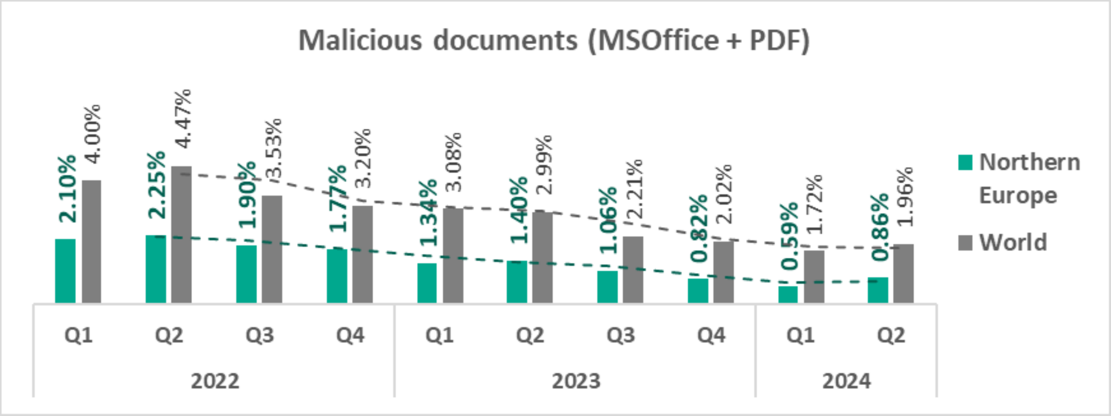
- Malware for AutoCAD, 2.4 times higher
- Malicious documents, 1.5 times higher
- Ransomware, 1.5 times higher
- Worms, 1.2 times higher

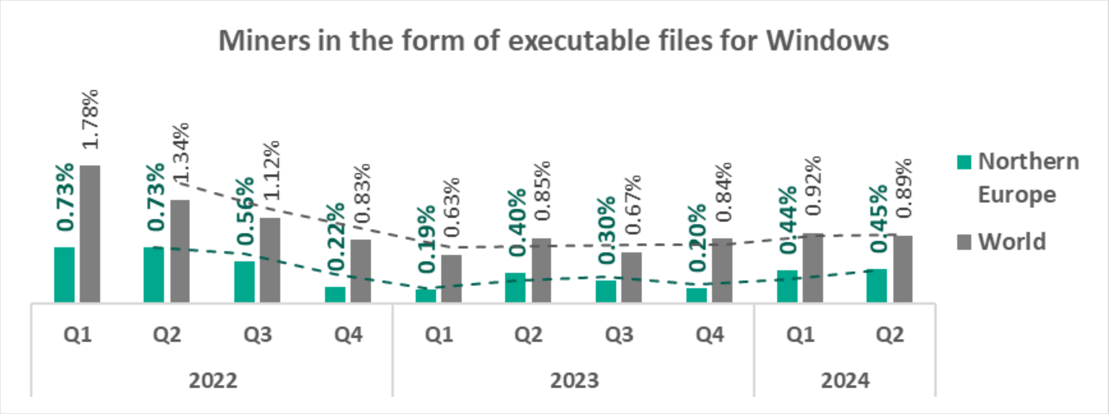
- The **top threat** categories exhibit various quarterly dynamics:



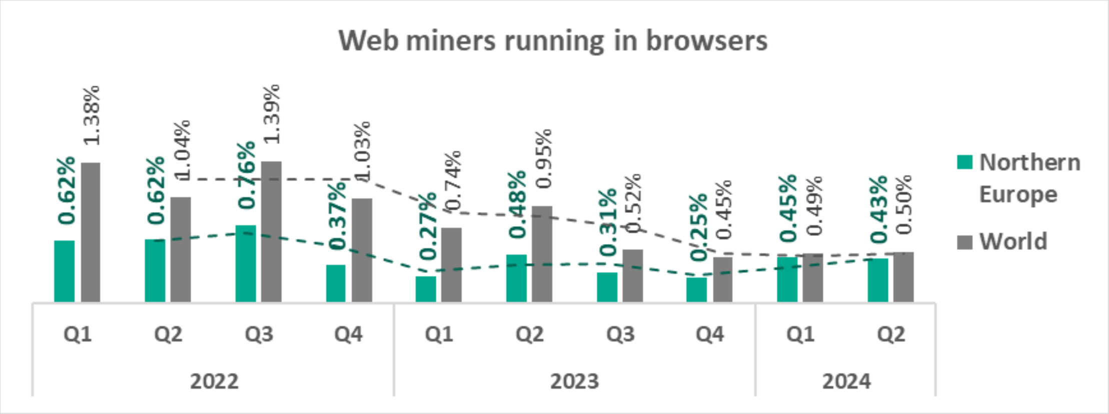

Malicious scripts and phishing pages (JS and HTML)
5.80%
9.29%
4.41%
8.87%
4.24%
9.60%
4.02%
9.58%
4.12%
9.96%
3.67%
8.67%
3.89%
7.37%
4.27%
7.61%
2.61%
5.84%
2.64%
5.69%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
Northern Europe
World


Spy Trojans, backdoors and keyloggers
2.28%
5.34%
2.45%
5.39%
2.39%
5.36%
2.00%
5.01%
1.94%
4.65%
2.15%
4.66%
1.93%
3.75%
1.97%
3.86%
1.70%
3.90%
1.83%
4.08%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
Northern Europe
World

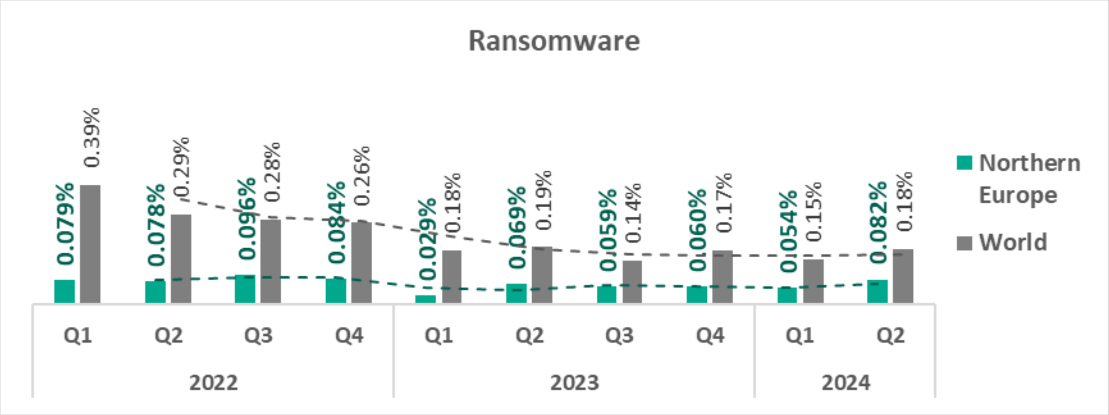

Malicious documents (MSOffice + PDF)
2.10%
4.00%
2.25%
4.47%
1.90%
3.53%
1.77%
3.20%
1.34%
3.08%
1.40%
2.99%
1.06%
2.21%
0.82%
2.02%
0.59%
1.72%
0.86%
1.96%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2022
2023
2024
Northern Europe
World



Miners in the form of executable files for Windows



Web miners running in browsers



Ransomware

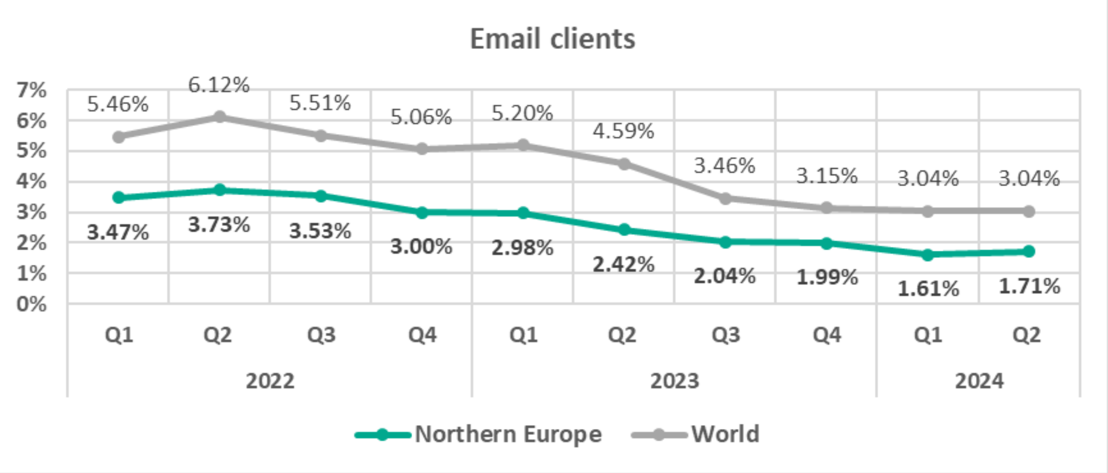
- The heatmap below illustrates changes in the rankings of threat categories in the region over a period of 2.5 years. **Denylisted internet resources** moved back to first place in Q1 2024, a position they previously held from Q1 2023 to Q3 2023, alternating with **malicious scripts and phishing pages**.

Northern Europe	2022				2023				2024	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Denylisted internet resources	2	2	2	2	1	1	1	2	1	1
Malicious scripts and phishing pages (JS and HTML)	1	1	1	1	2	2	2	1	2	2
Spy Trojans, backdoors and keyloggers	3	3	3	3	3	3	3	3	3	3
Malicious documents (MSOffice + PDF)	4	4	4	4	4	4	4	4	4	4
Miners in the form of executable files for Windows	5	5	6	7	8	7	6	8	6	5
Web miners running in browsers	6	6	5	5	7	5	5	7	5	6
Worms	7	7	7	6	5	6	6	5	7	7
Viruses	8	8	8	8	6	8	8	6	8	8
Ransomware	9	9	9	9	10	9	9	9	9	9
Malware for AutoCAD	10	10	10	10	9	10	10	10	10	10

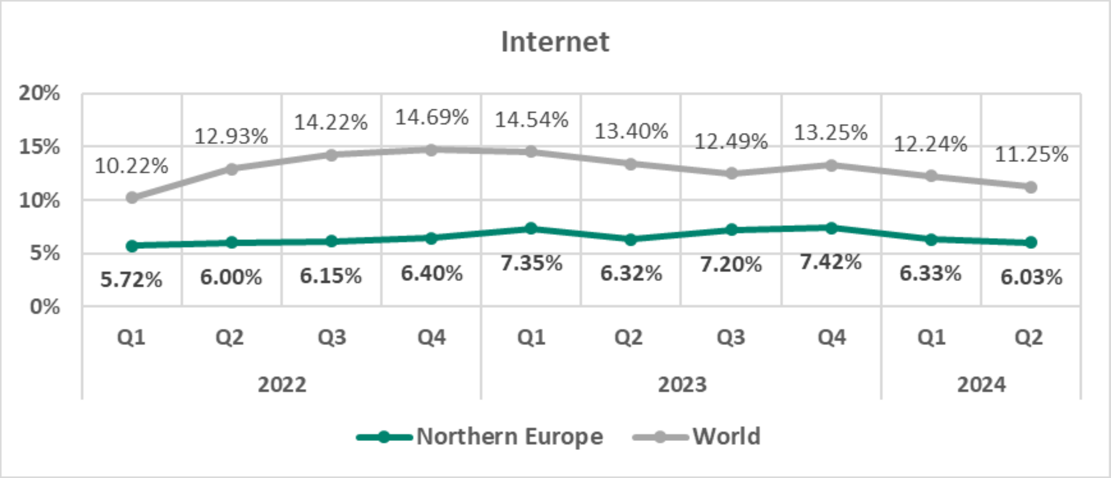
Threat sources

- The region saw an increase in the percentage of ICS computers on which threats distributed via **email clients** were blocked.

  Overall, the trend for email client threats is predominantly downward.

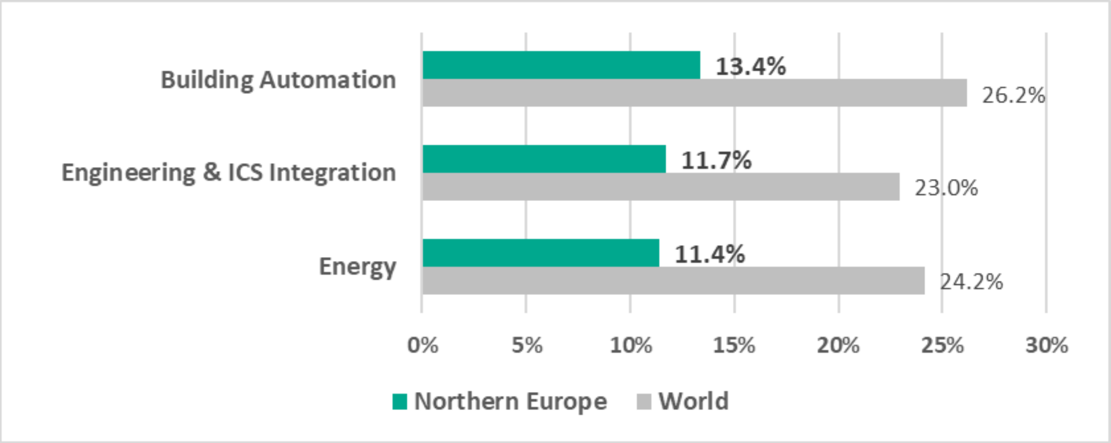


- The trend for threats from the internet generally demonstrated a gradual increase until Q4 2023, followed by a decline from Q1 2024.

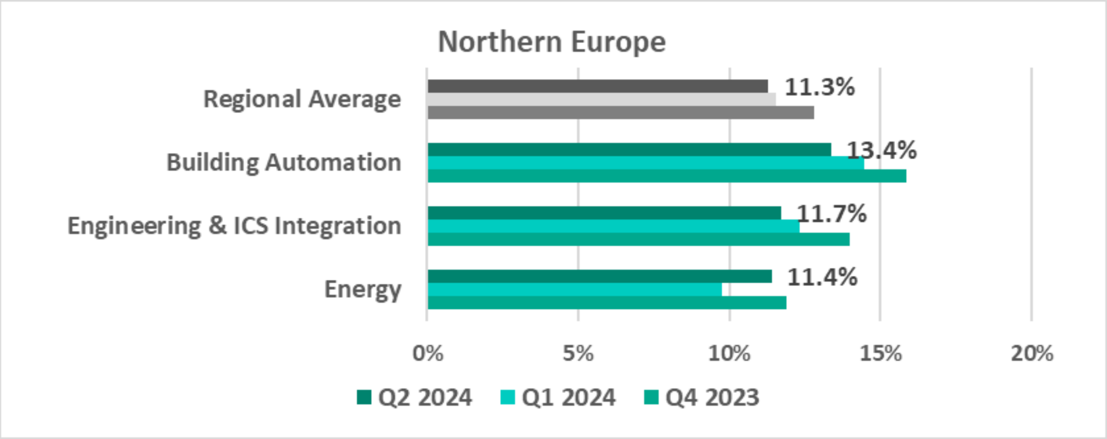


Industries

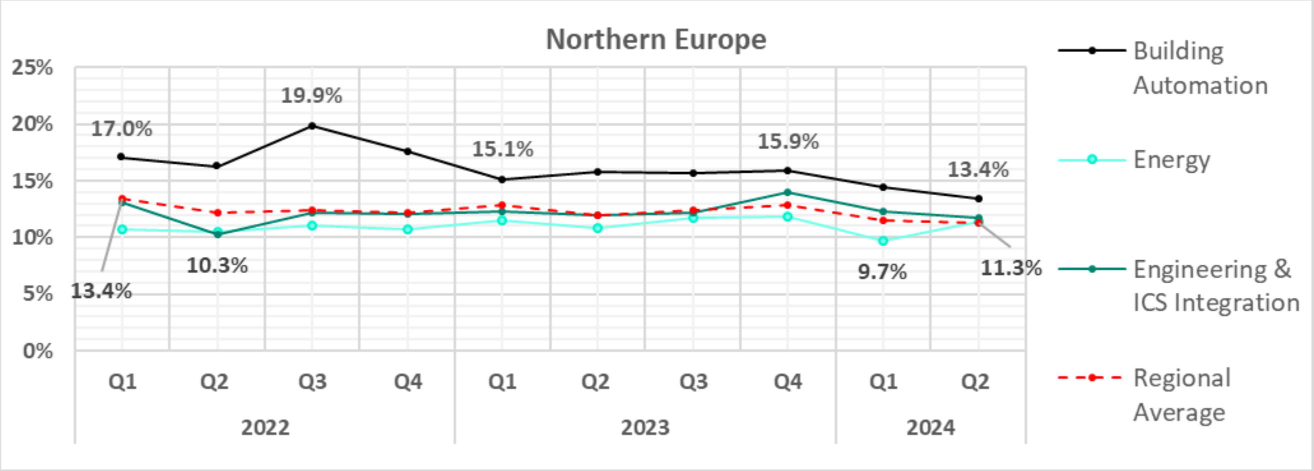
- The most **affected** industry in the region, as highlighted in this report, was **building automation**. It ranked fifth in the global ranking of the selected sectors.
- From a **global perspective**, all sectors under study in the region remained significantly below the respective global averages.



- In **Q2 2024**, the energy sector exhibited an increase in the percentage of ICS computers on which malicious objects were blocked – by 1.2 times.



- All sectors under study exhibited fluctuating **trends** in the percentage of ICS computers on which malicious objects were blocked. The building automation trend shows gradual decline, while energy, and engineering & ICS integration exhibit fluctuating long-term trends.



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

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

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 as attacked if a Kaspersky security solution blocked one or more threats on that computer during the period in 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 in 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