Kaspersky ICS CERT

Threat landscape for industrial automation systems

Regions, Q1 2024

27.05.2024 Version 1.0

Q1 in numbers

Percentage of ICS computers

Globally, in the first quarter of 2024, the percentage of ICS computers on which malicious objects were blocked decreased by 0.3 pp from the previous quarter to 21.4%.

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

Over 25%

- Africa – 32.4%
- South-East Asia – 29.7%
- Middle East – 26.9%
- Central Asia – 26.8%

In the regions of this group, ICS cybersecurity requires close attention and improvement.

20–25%

- Eastern Europe – 24.7%
- Russia – 23.6%
- Latin America – 23.5%
- South Asia – 23.5%
- Southern Europe – 21.4%
- East Asia – 20.3%

Up to 20%

- Australia and New Zealand – 16.2%
- US and Canada – 13.3%
- Western Europe – 12.3%
- Northern Europe – 11.5%

The third group contains the regions that are the safest in terms of cybersecurity.

The percentage of ICS computers on which malicious objects were blocked during the quarter has increased only in the top two regions: Africa (by 1.2 pp) and South-East Asia (by 0.2 pp).

Malware categories

Malicious objects used for initial infection

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

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

Globally and in almost all regions, denylisted internet resources and malicious scripts and phishing pages occupy first place in the rankings of malware categories by 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. The leading regions by percentage of ICS computers on which threats from these sources were blocked are the following:

Internet threats

- Africa – 14.82%
- South-East Asia – 14.01%

Email threats

- Southern Europe – 6.85%
- Latin America – 5.09%

Denylisted internet resources

The leading regions by percentage of ICS computers on which denylisted internet resources were blocked were:

- Africa – 8.78%
- Russia – 7.49%
- South Asia – 7.48%

Malicious scripts and phishing pages

The leading regions by percentage of ICS computers on which malicious scripts and phishing pages were blocked were:

- Latin America – 7.23%
- Southern Europe – 6.96%
- Middle East – 6.95%

Malicious documents

The leading regions by percentage of ICS computers on which malicious documents were blocked were:

- Southern Europe – 3.24%
- Latin America – 2.94%
- Eastern Europe – 2.33%

Next-stage malware

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

Among the miners designed to run on Windows, some of the most common are those distributed by attackers in the form of NSIS installer files with legitimate software.

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.

The three leading regions by percentage of ICS computers on which spyware was blocked were also the leading regions for malware from the first mentioned group:

- Africa – 6.65%
- Middle East – 5.89%
- Southern Europe – 5.45%

In almost all regions, in the threat category rankings by percentage of ICS computers on which it was blocked, spyware does not rank higher than third place, except for two 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, at 3.68%.
- **Central Asia**: in this region, in the corresponding ranking, spyware sits **at second place** with 4.40%.

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 were:

- Central Asia – 1.78%
- Russia – 1.38%
- Eastern Europe – 1.06%

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

- In the corresponding ranking in Russia, they are in fourth place.
- In Central Asia they came in fifth place.

We should note that during Q1 2024, the percentage of ICS computers on which miners in the form of Windows executable files were blocked increased in all regions except Russia and Central Asia.

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 were:

- Africa – 0.91%
- Middle East – 0.84%
- Australia and New Zealand – 0.78%

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

- Australia and New Zealand – 0.78%
- US and Canada – 0.45%
- Northern Europe – 0.27%

In Q1 2024, the percentage of ICS computers on which web miners running in browsers were blocked increased in all regions except Russia and Central Asia.

Ransomware

The regions where the highest percentage of ICS computers on which ransomware was blocked were:

- Middle East – 0.28%
- Africa – 0.27%
- South Asia – 0.22%

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.

In three regions, the percentage of ICS computers on which threats were blocked **when connecting removable media is higher than** the percentage of ICS computers on which **mail threats** were blocked (although it was lower in all others):

- Africa – 5.6% (leads this ranking)
- South Asia – 2.46%
- Central Asia – 1.51%

Worms

The leading regions by percentage of ICS computers on which worms were blocked were:

- Africa – 5.29%
- Central Asia – 2.88%
- Middle East – 2.40%

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 are in fourth place in four regions**:

- Africa – 5.29%
- Central Asia – 2.88%
- Middle East – 2.40%
- South Asia – 1.95%

The top regions for worms were the leading regions by percentage of ICS computers on which threats were blocked when connecting **removable media**:

- Africa – 5.60%
- South Asia – 2.46%

Viruses

The leading regions by percentage of ICS computers on which viruses were blocked were:

- South-East Asia – 7.61%
- Africa – 4.09%
- East Asia – 2.89%

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

Note that two of the three top regions are also leaders by percentage of ICS computers on which **network folder threats** were blocked.

- South-East Asia – 0.43%
- East Asia – 0.32%

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:

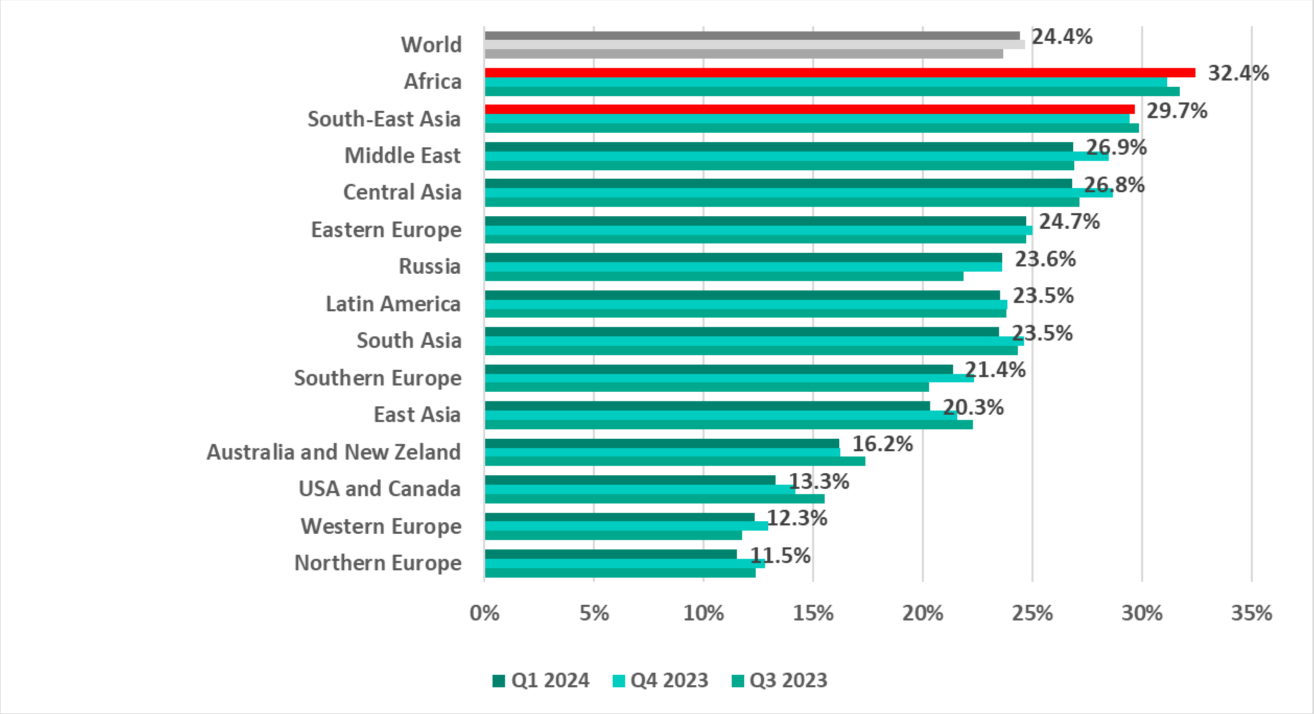
- South-East Asia – 2.81%
- East Asia – 1.49%
- Africa – 0.61%

Normally, AutoCAD malware is a minor threat that usually comes in last place in the malware category rankings by percentage of ICS computers on which they were blocked. In **South-East Asia** in Q1 2024, this category came in **fifth place**.

Regions. Rankings

Percentage of attacked ICS computers

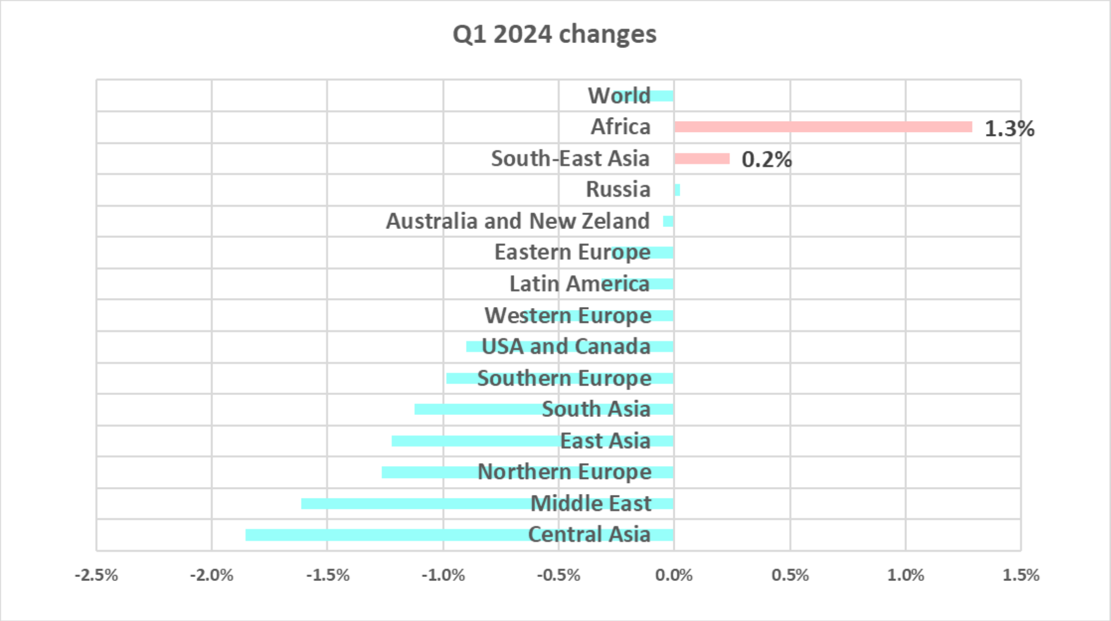
The percentage of ICS computers on which malicious objects were blocked during the quarter varied regionally from 34.2% in Africa to 11.5% in Northern Europe.



Regions ranked by percentage of ICS computers on which malicious objects were blocked, Q1 2024

The two regions with the highest percentage of attacked ICS computers, Africa and South-East Asia, saw their percentages increase from the previous quarter.

Regions and world. Changes in the percentage of attacked ICS computers in Q1 2024



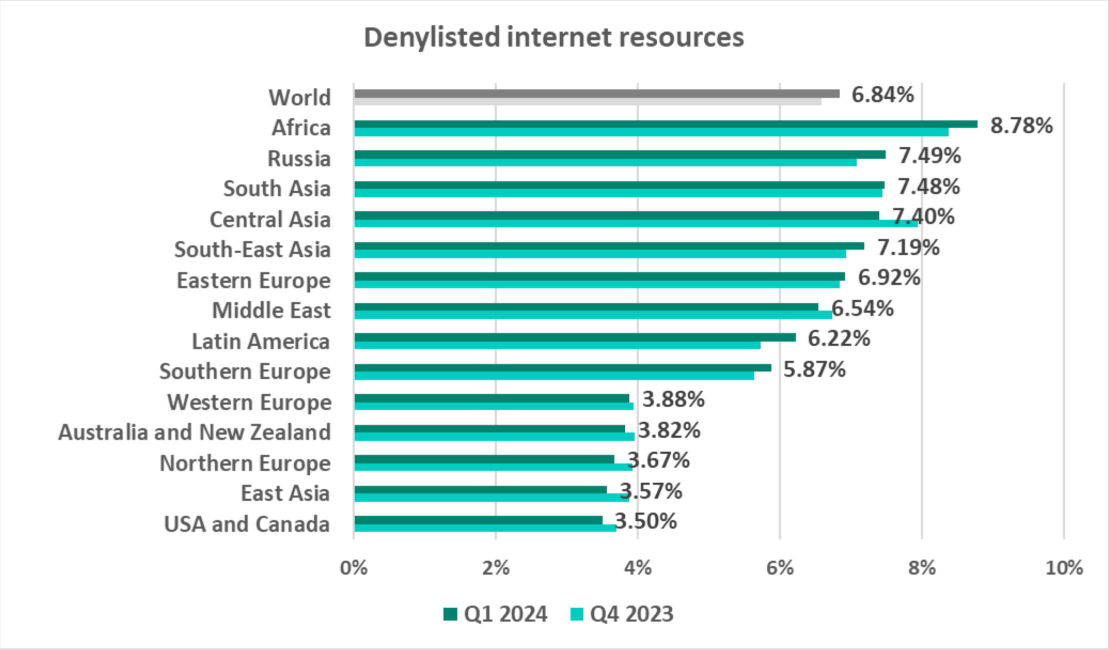
Malicious object categories

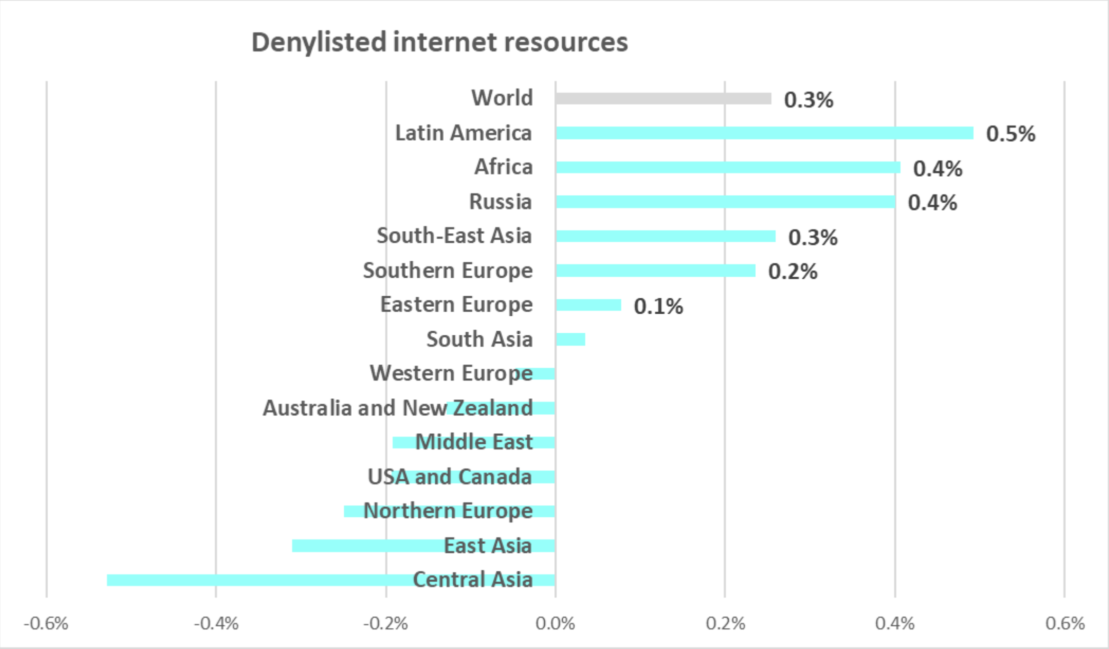
The percentage of ICS computers on which malware from different categories is blocked differs in various regions. The positions of regions in these rankings do not always match their positions in the ranking by percentage of ICS computers on which all threats were blocked.

The diagrams below show the rankings of regions by percentage of ICS computers on which malware of a specific category was blocked in Q1 2024.

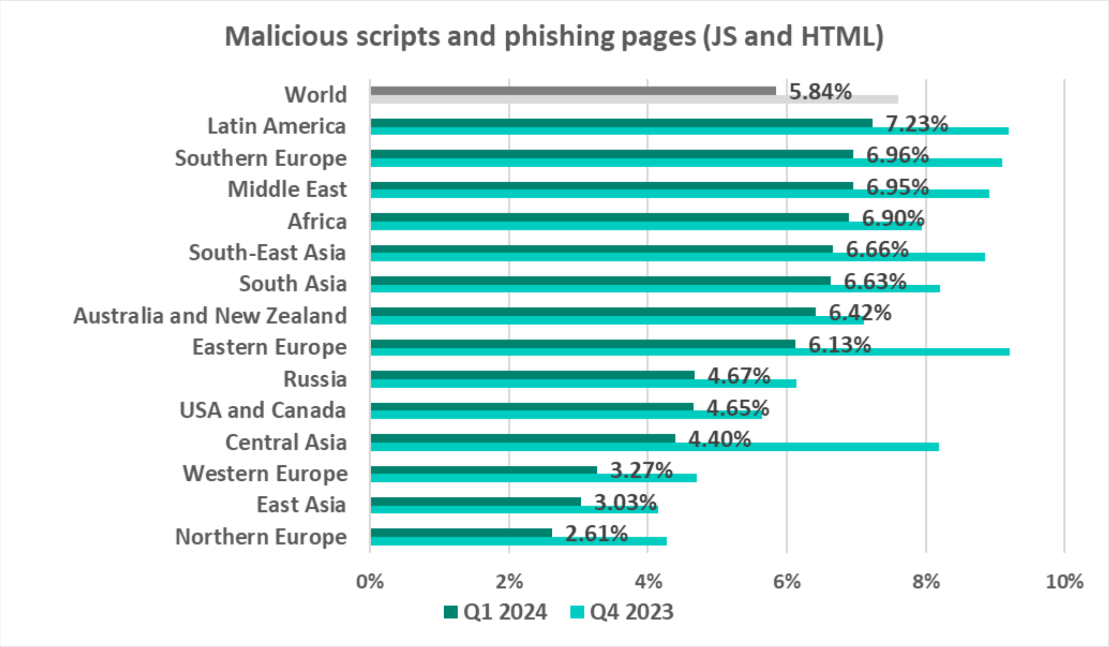
Malicious objects used for initial infection

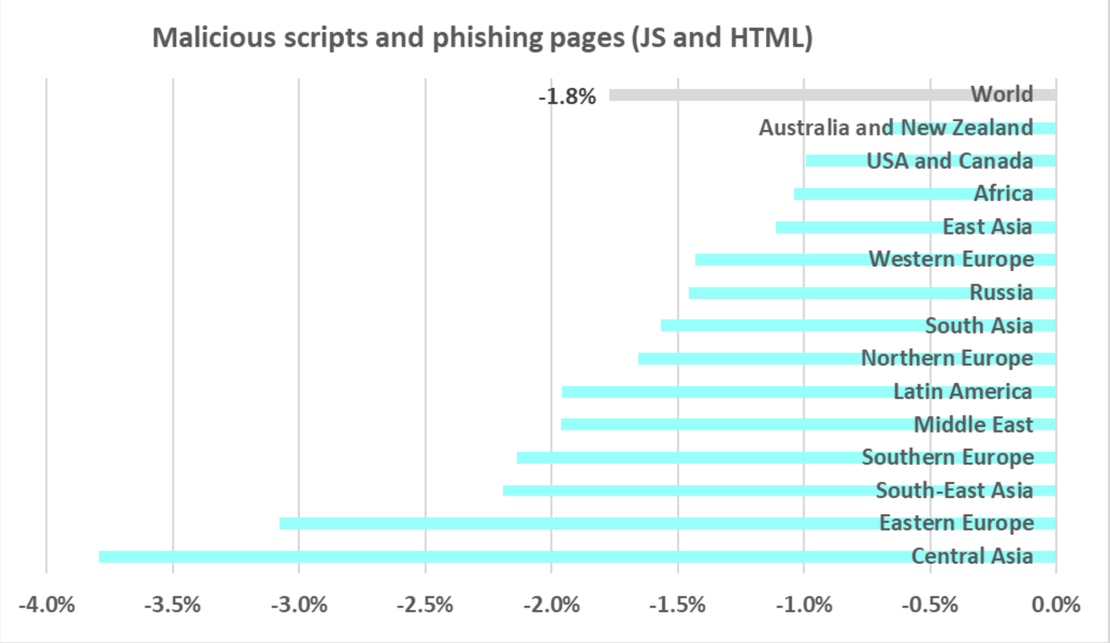
Denylisted internet resources



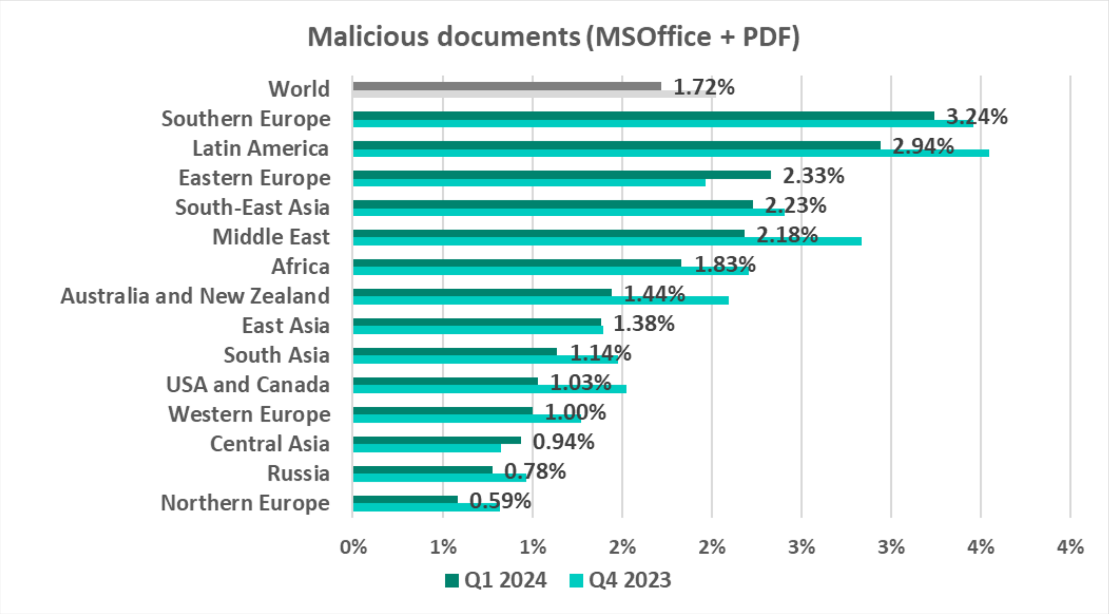


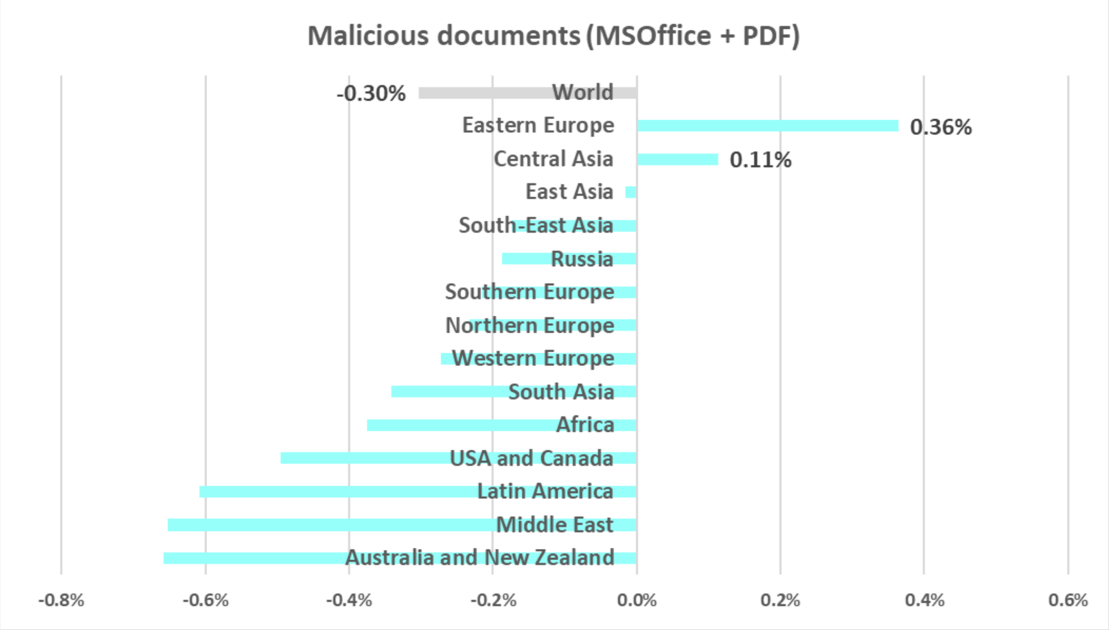
Malicious scripts and phishing pages (JS and HTML)





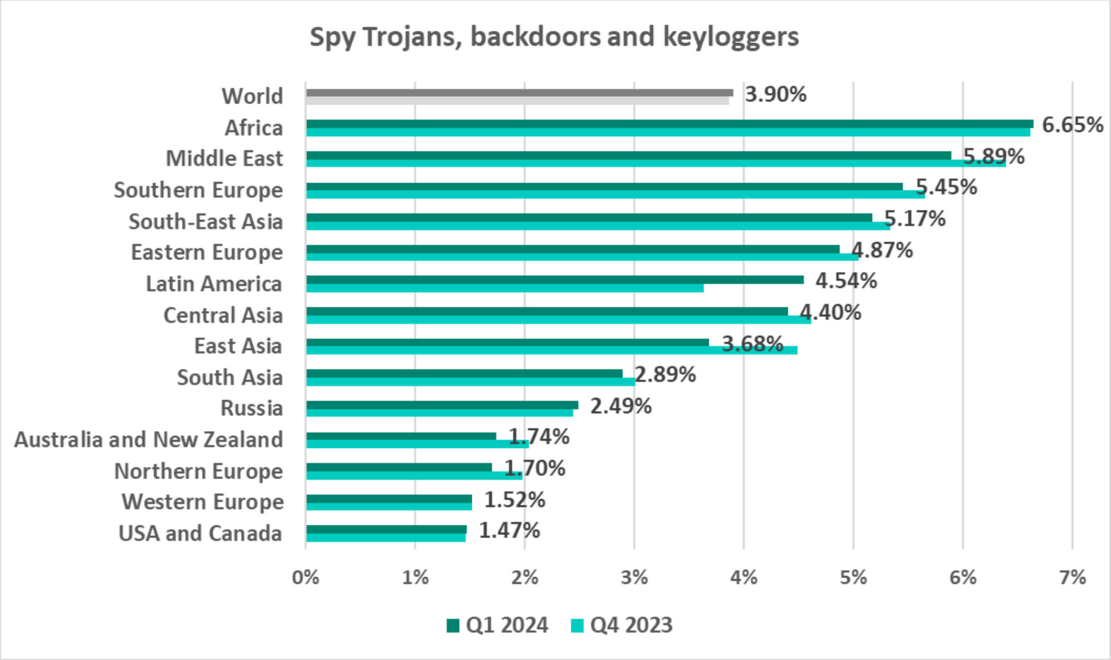
Malicious documents (MSOffice+PDF)

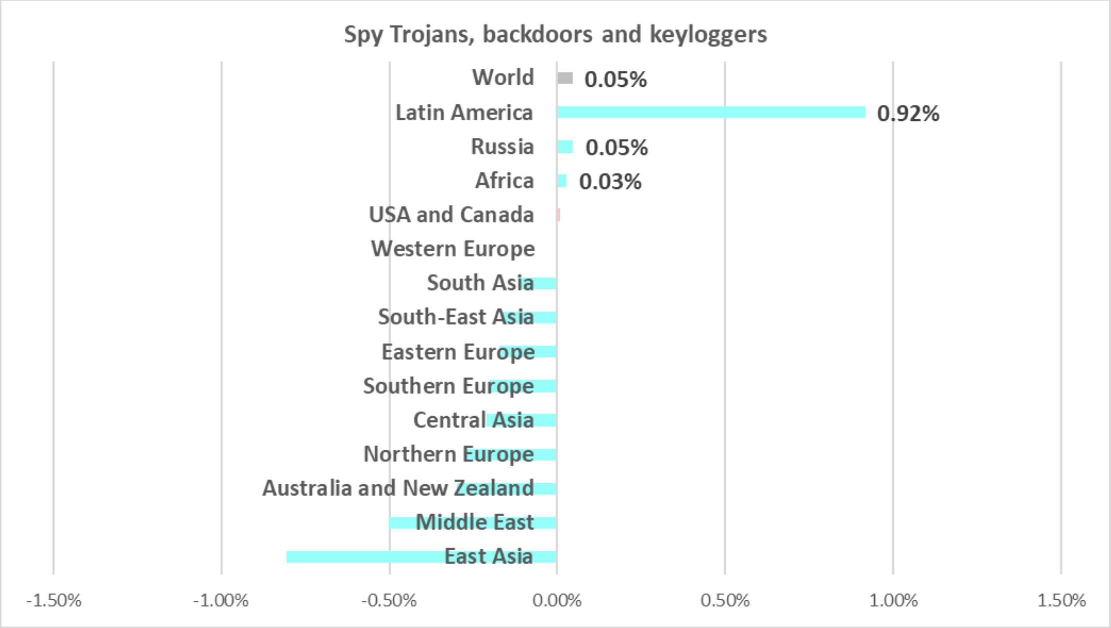




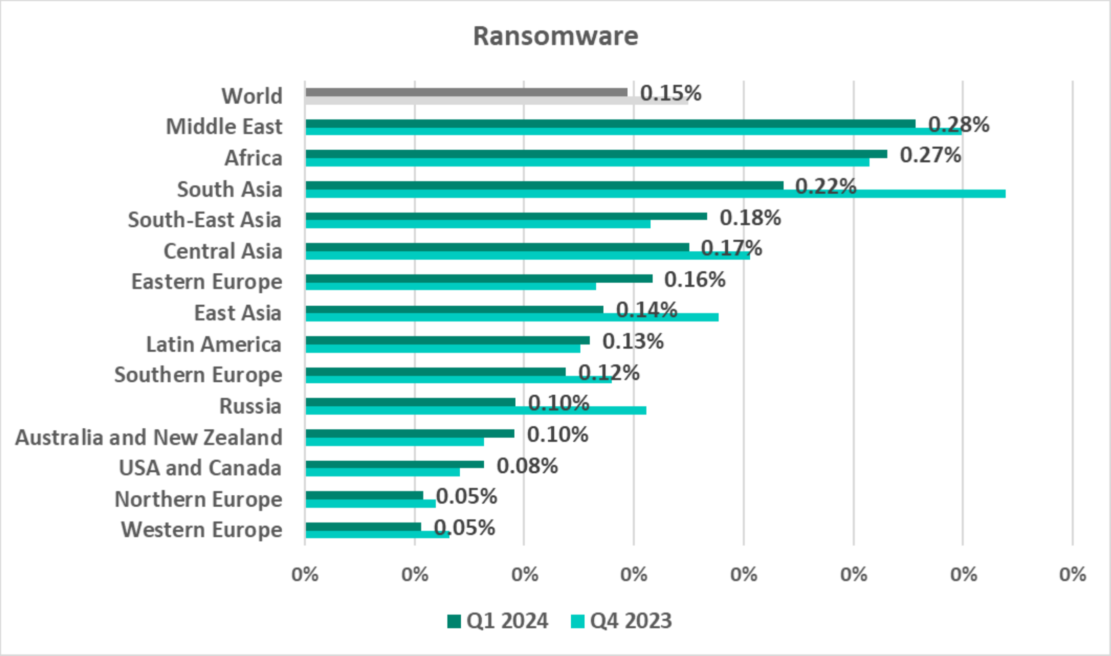
Next-stage malware

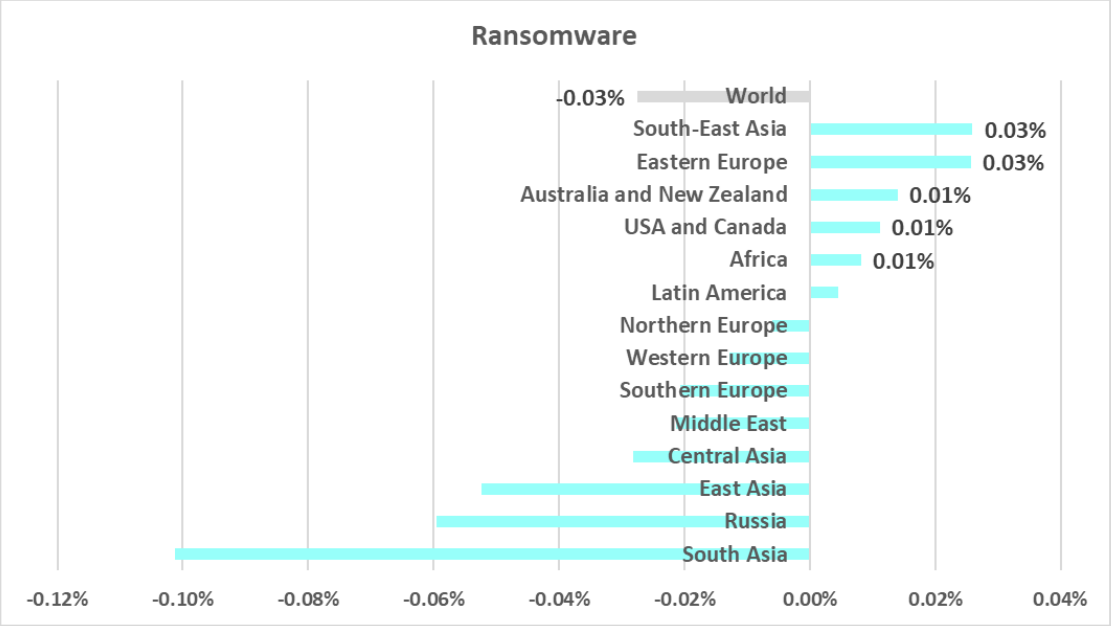
Spyware





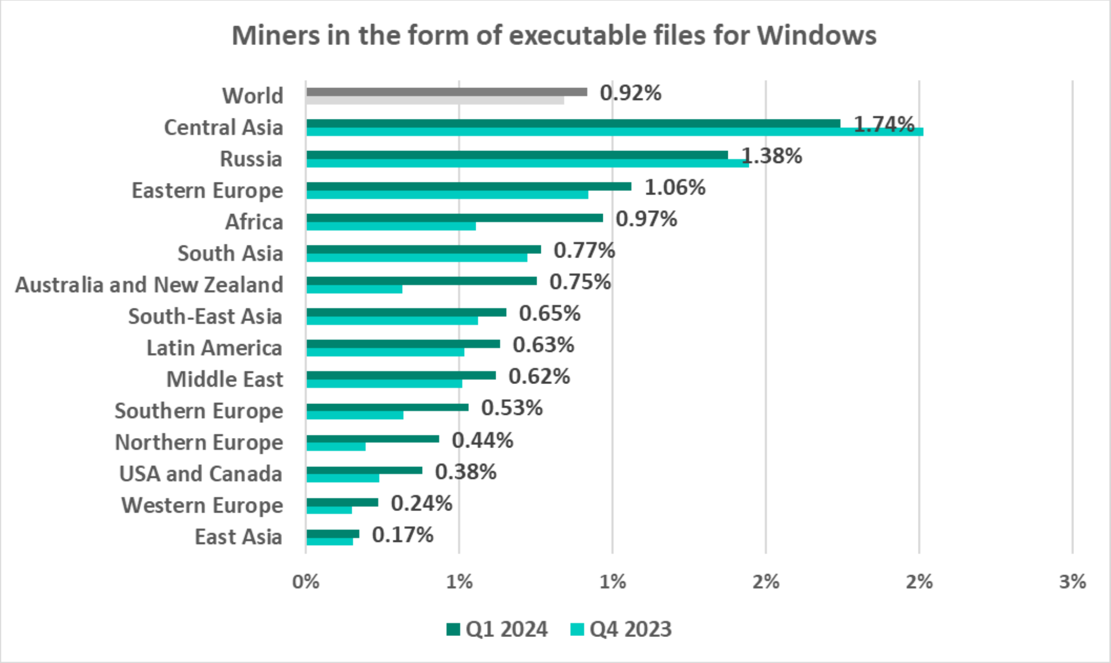
Ransomware

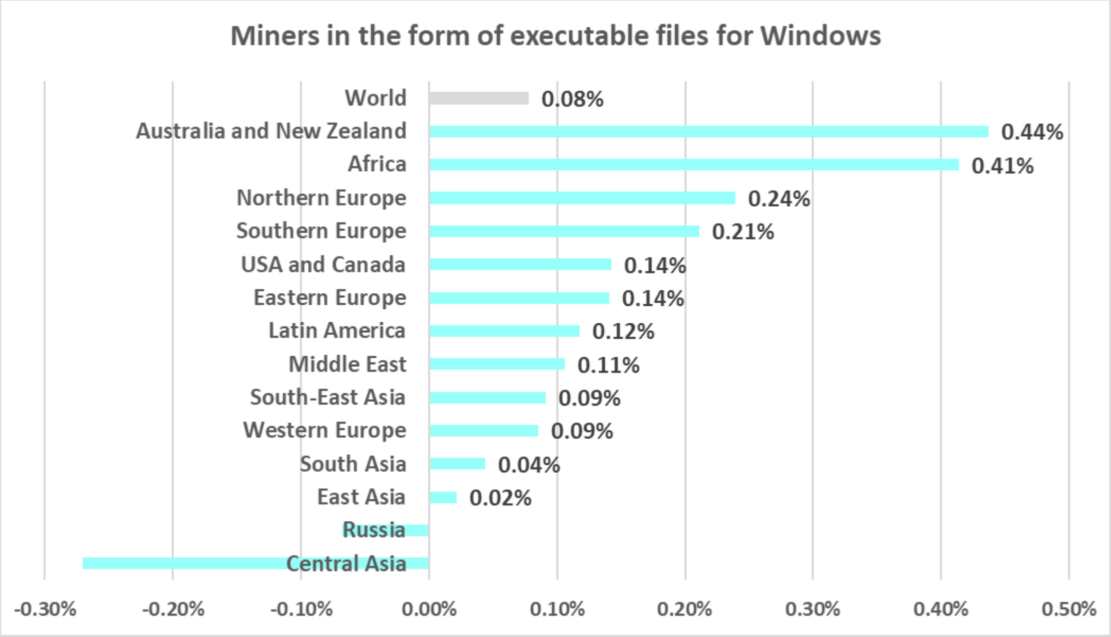

Ransomware
World 0.15%
Middle East 0.28%
Africa 0.27%
South Asia 0.22%
South-East Asia 0.18%
Central Asia 0.17%
Eastern Europe 0.16%
East Asia 0.14%
Latin America 0.13%
Southern Europe 0.12%
Russia 0.10%
Australia and New Zealand 0.10%
USA and Canada 0.08%
Northern Europe 0.05%
Western Europe 0.05%
0% 0% 0% 0% 0% 0% 0% 0%
■ Q1 2024 ■ Q4 2023


Ransomware
World -0.03%
South-East Asia 0.03%
Eastern Europe 0.03%
Australia and New Zealand 0.01%
USA and Canada 0.01%
Africa 0.01%
Latin America
Northern Europe
Western Europe
Southern Europe
Middle East
Central Asia
East Asia
Russia
South Asia
-0.12% -0.10% -0.08% -0.06% -0.04% -0.02% 0.00% 0.02% 0.04%

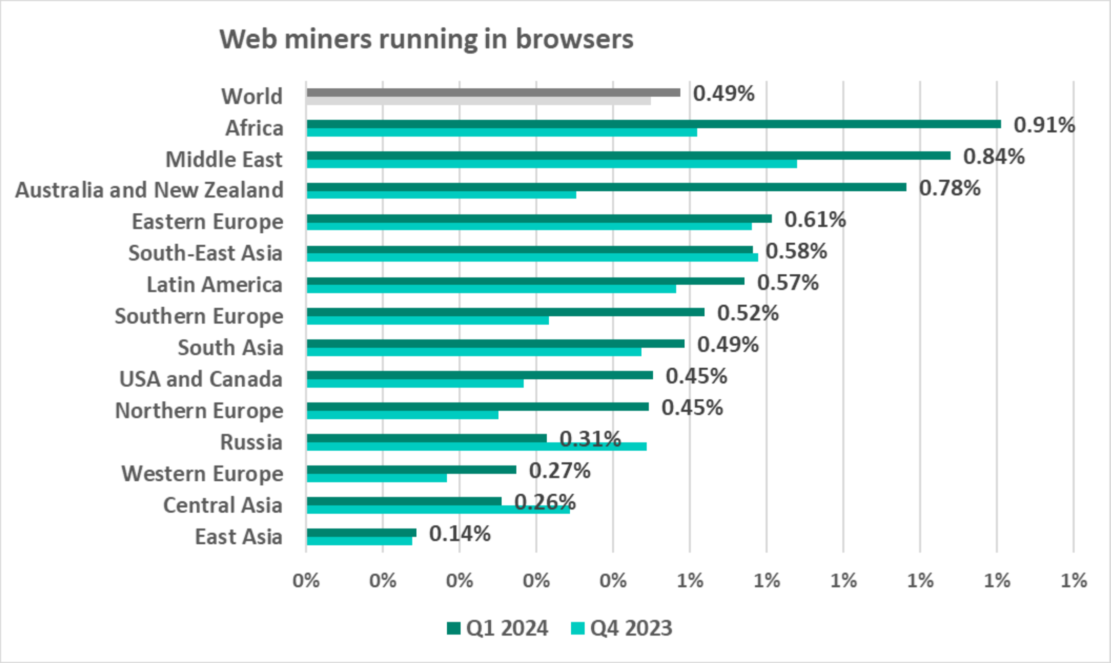
Covert crypto-mining malware

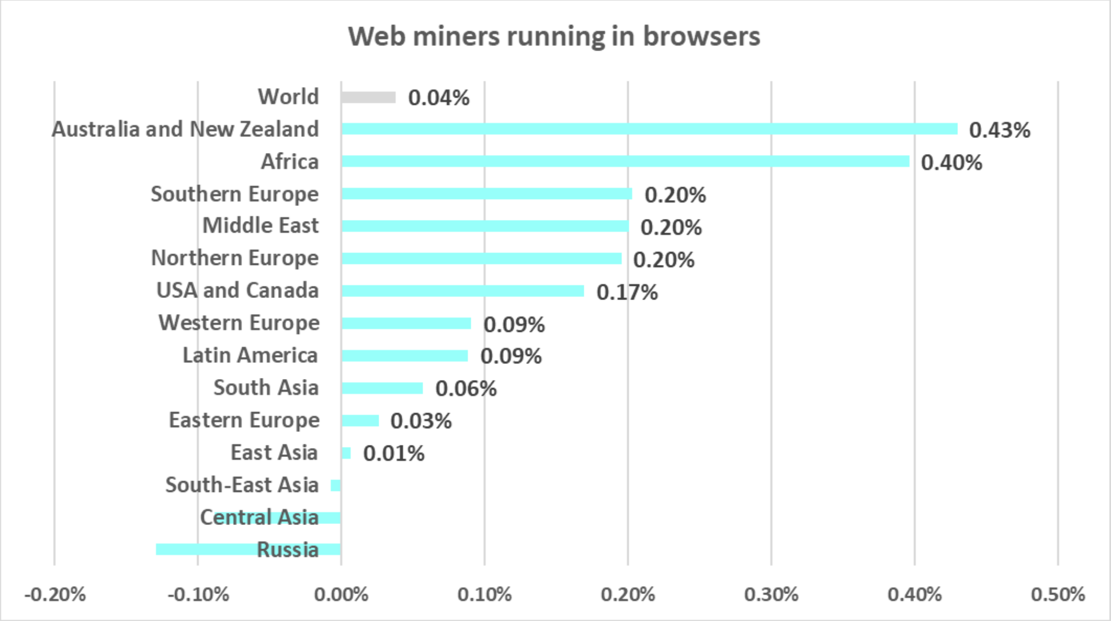
Miners in the form of executable files for Windows





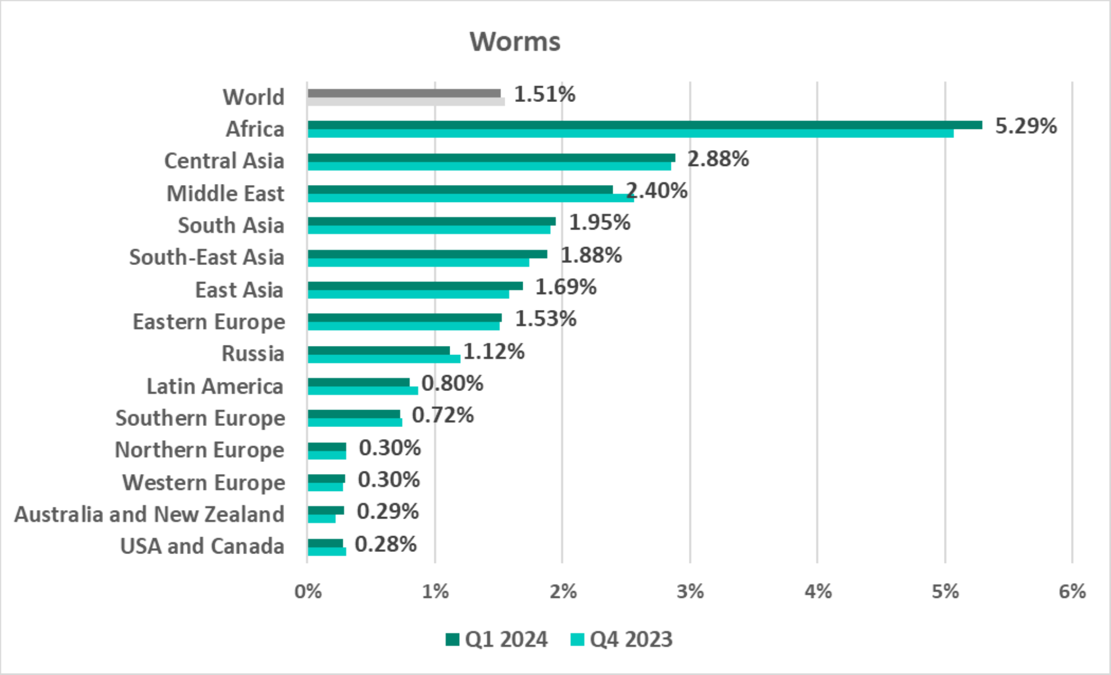
Web miners

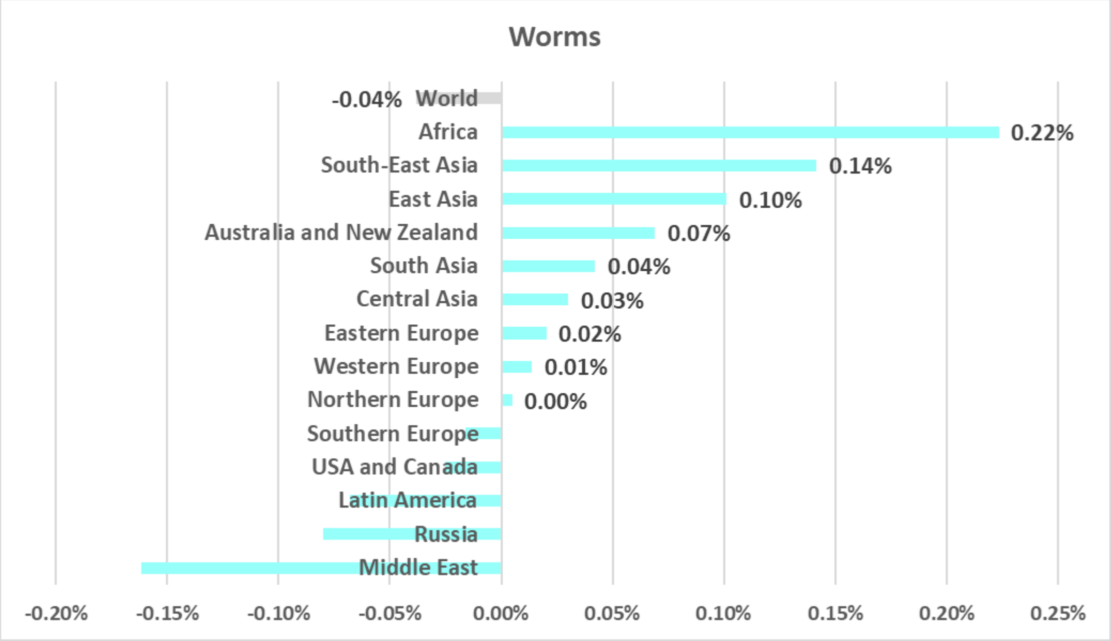

Web miners running in browsers
World 0.49%
Africa 0.91%
Middle East 0.84%
Australia and New Zealand 0.78%
Eastern Europe 0.61%
South-East Asia 0.58%
Latin America 0.57%
Southern Europe 0.52%
South Asia 0.49%
USA and Canada 0.45%
Northern Europe 0.45%
Russia 0.31%
Western Europe 0.27%
Central Asia 0.26%
East Asia 0.14%
0% 0% 0% 0% 0% 1% 1% 1% 1% 1% 1%
Q1 2024
Q4 2023


Web miners running in browsers
World 0.04%
Australia and New Zealand 0.43%
Africa 0.40%
Southern Europe 0.20%
Middle East 0.20%
Northern Europe 0.20%
USA and Canada 0.17%
Western Europe 0.09%
Latin America 0.09%
South Asia 0.06%
Eastern Europe 0.03%
East Asia 0.01%
South-East Asia
Central Asia
Russia
-0.20% -0.10% 0.00% 0.10% 0.20% 0.30% 0.40% 0.50%

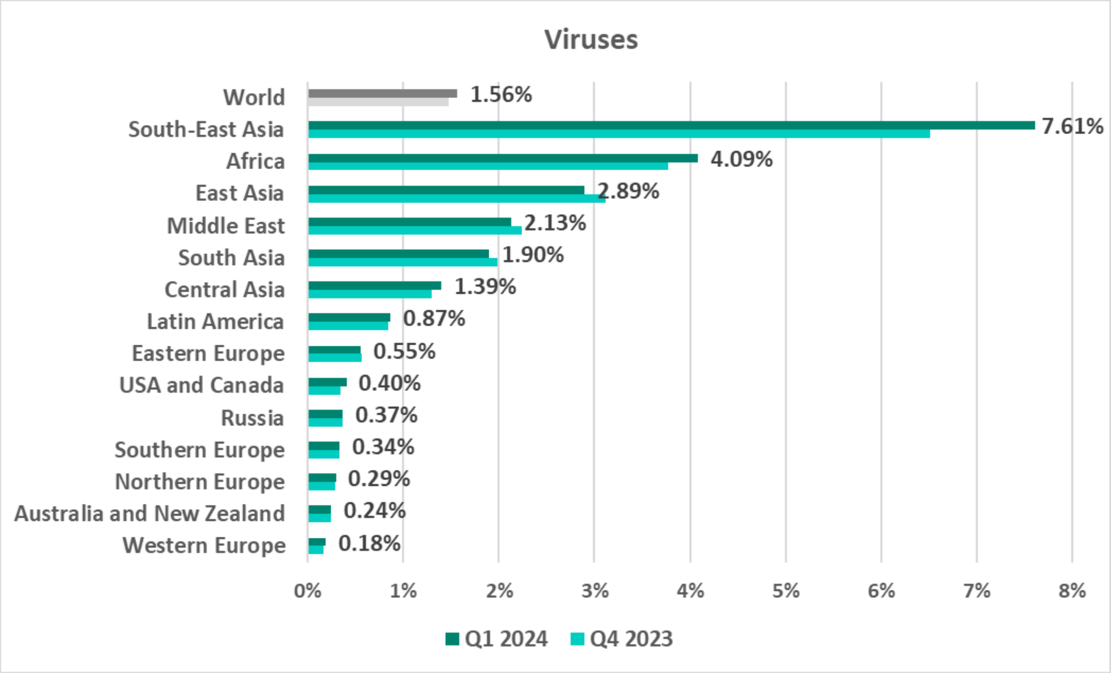
Self-propagating malware. Viruses and worms

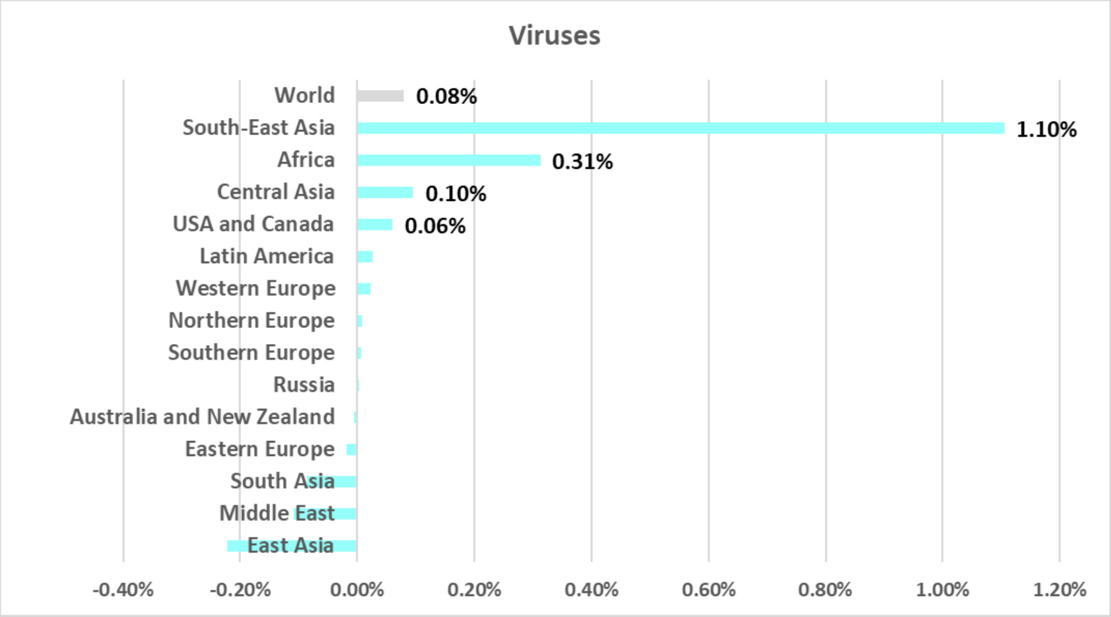
Worms



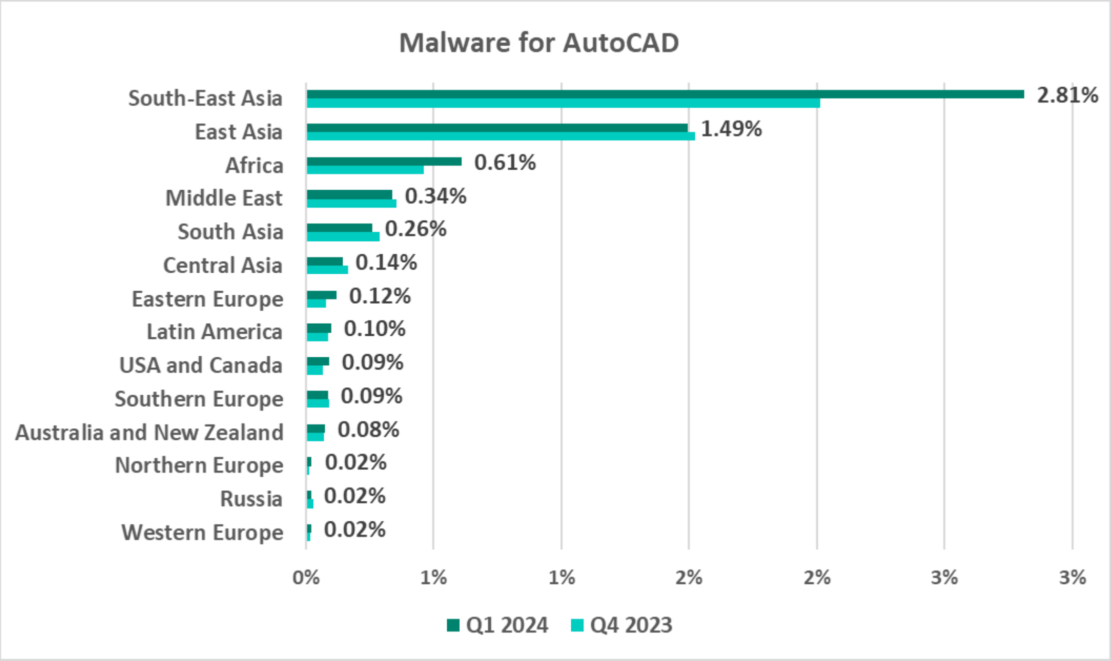


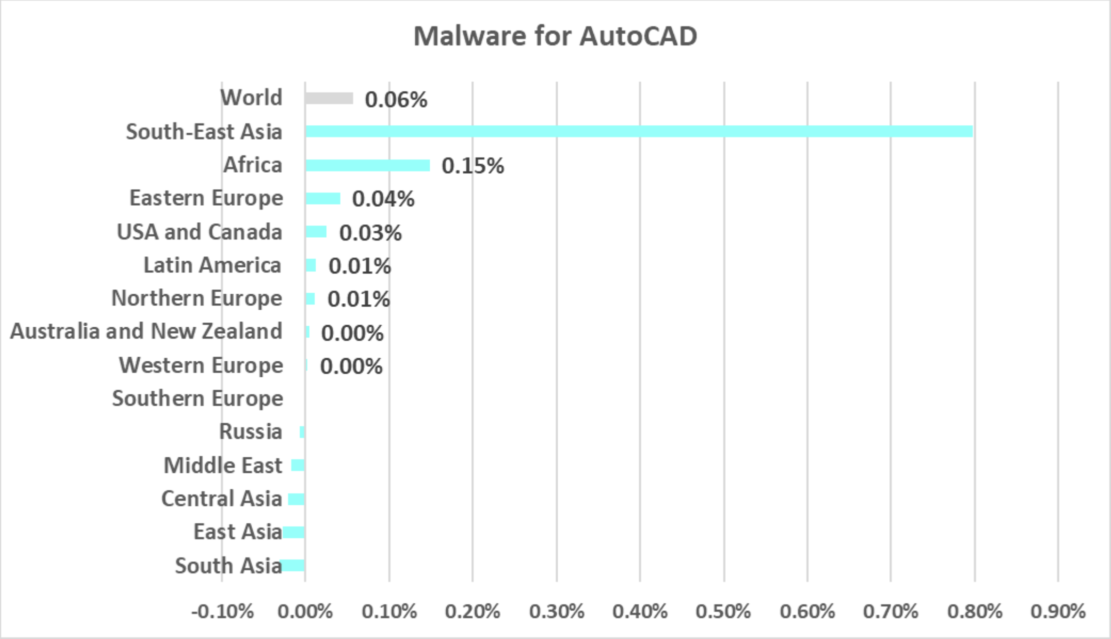
Viruses


Viruses
World 1.56%
South-East Asia 7.61%
Africa 4.09%
East Asia 2.89%
Middle East 2.13%
South Asia 1.90%
Central Asia 1.39%
Latin America 0.87%
Eastern Europe 0.55%
USA and Canada 0.40%
Russia 0.37%
Southern Europe 0.34%
Northern Europe 0.29%
Australia and New Zealand 0.24%
Western Europe 0.18%
0% 1% 2% 3% 4% 5% 6% 7% 8%
🟩 Q1 2024 🟩 Q4 2023


Viruses
World 0.08%
South-East Asia 1.10%
Africa 0.31%
Central Asia 0.10%
USA and Canada 0.06%
Latin America
Western Europe
Northern Europe
Southern Europe
Russia
Australia and New Zealand
Eastern Europe
South Asia
Middle East
East Asia
-0.40% -0.20% 0.00% 0.20% 0.40% 0.60% 0.80% 1.00% 1.20%

AutoCAD malware





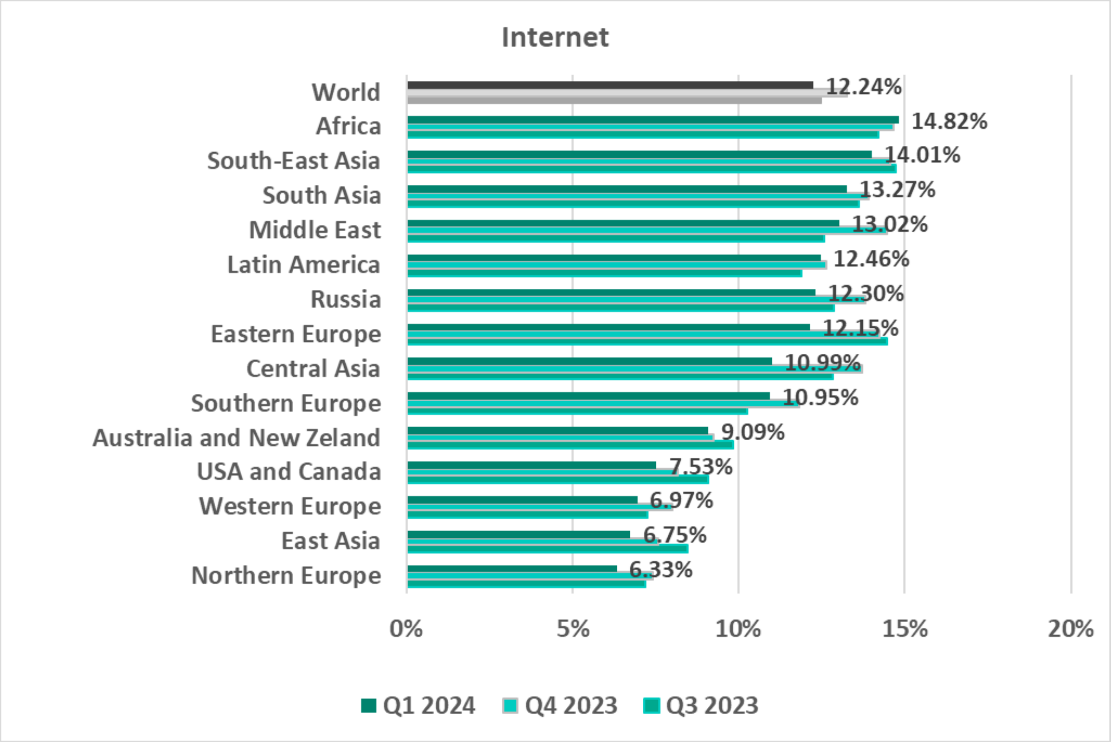
Threat sources

The **percentage of ICS computers on which threats from various sources were blocked** differs in the regions just like for malware from different categories.

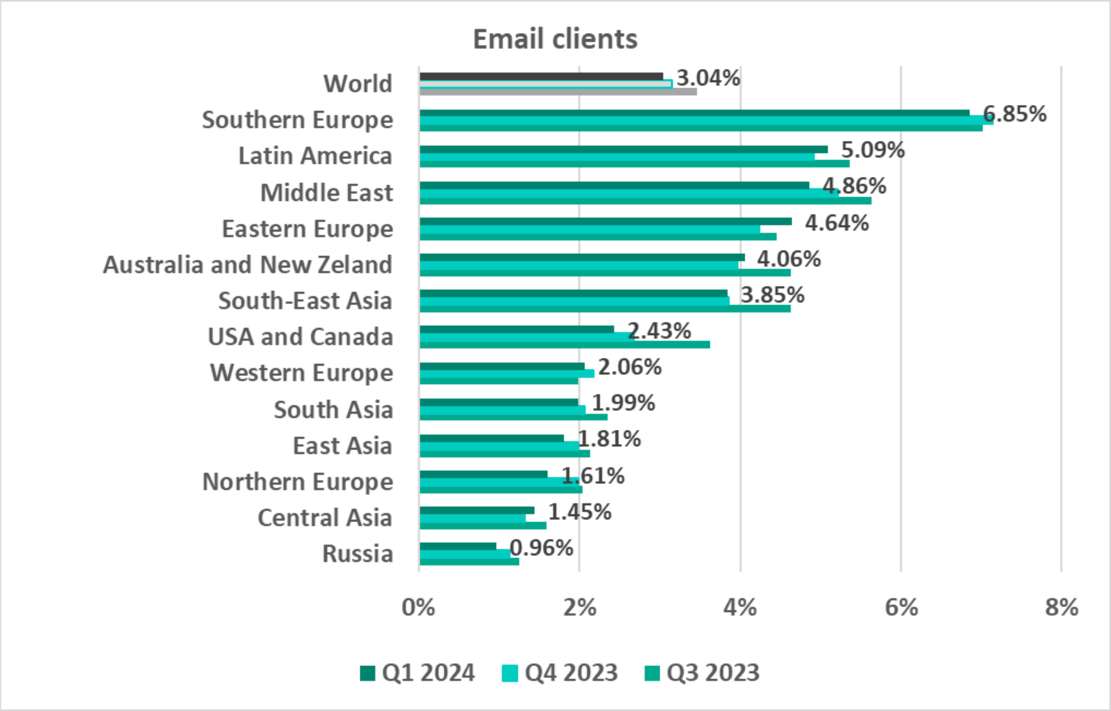
The diagrams below show **the rankings of regions by percentage of ICS computers on which malware from a specific source was blocked in Q1 2024.**

Please note that we were not able to define the source of malware in all cases.

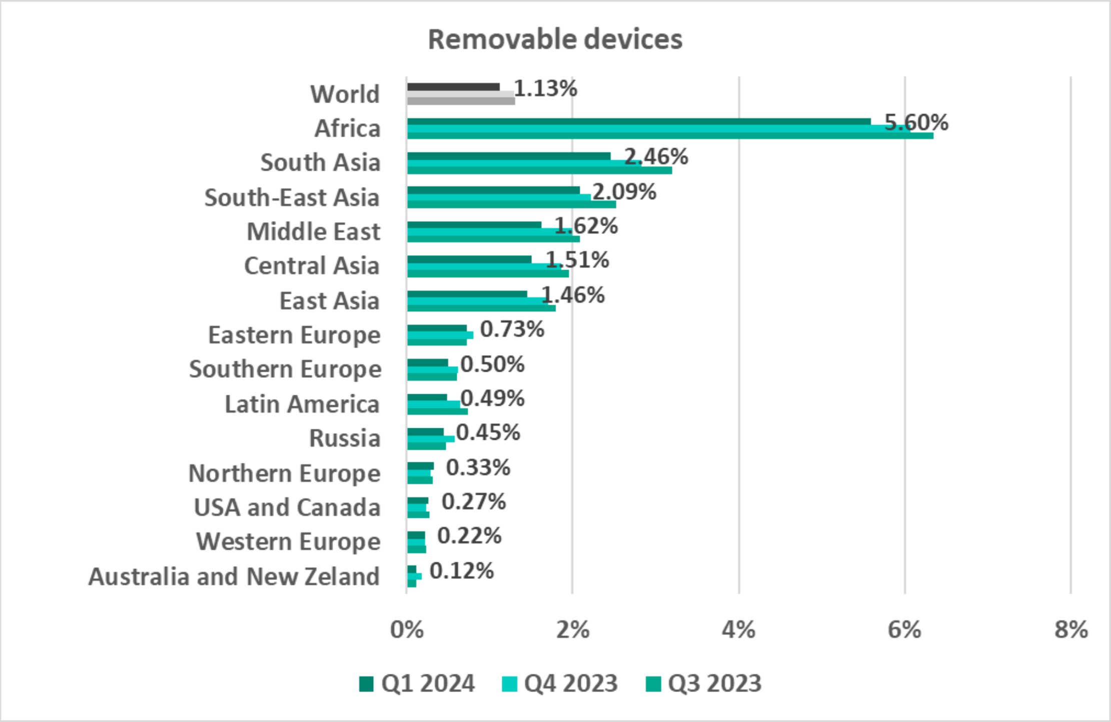
Internet



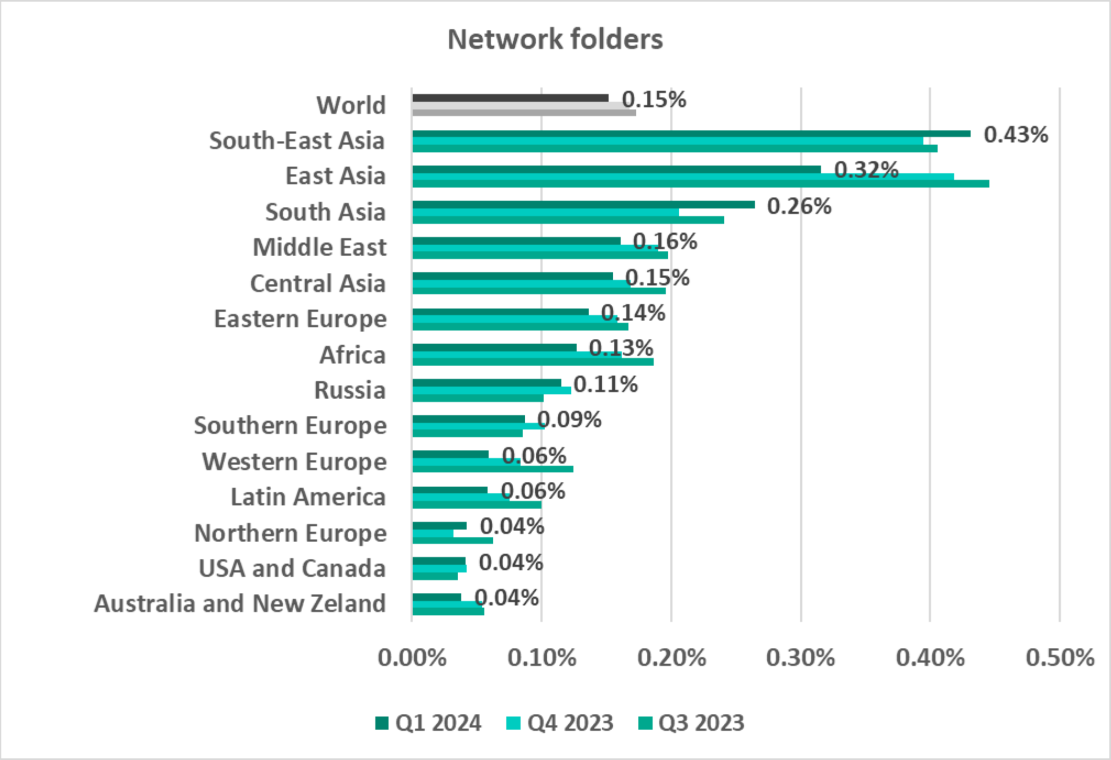
Email clients



Removable media



Network folders



Regions. Special considerations

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

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

Some of the rankings in regions have their own specifics and distinctions that we note below.

Africa

In comparison to other regions

First place in the regional ranking. One of two regions where the percentage of attacked ICS computers grew during the quarter.

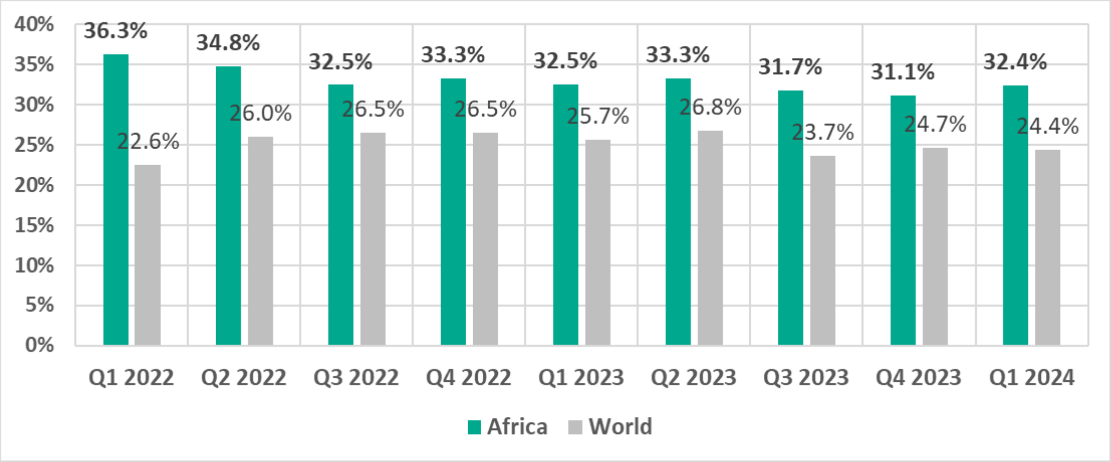
Of all regions, Africa traditionally has the highest percentage of ICS computers on which malicious objects were blocked. Therefore, it is not surprising that Africa leads in many rankings, in some cases by a huge margin.

Among regions, Africa leads in the following:

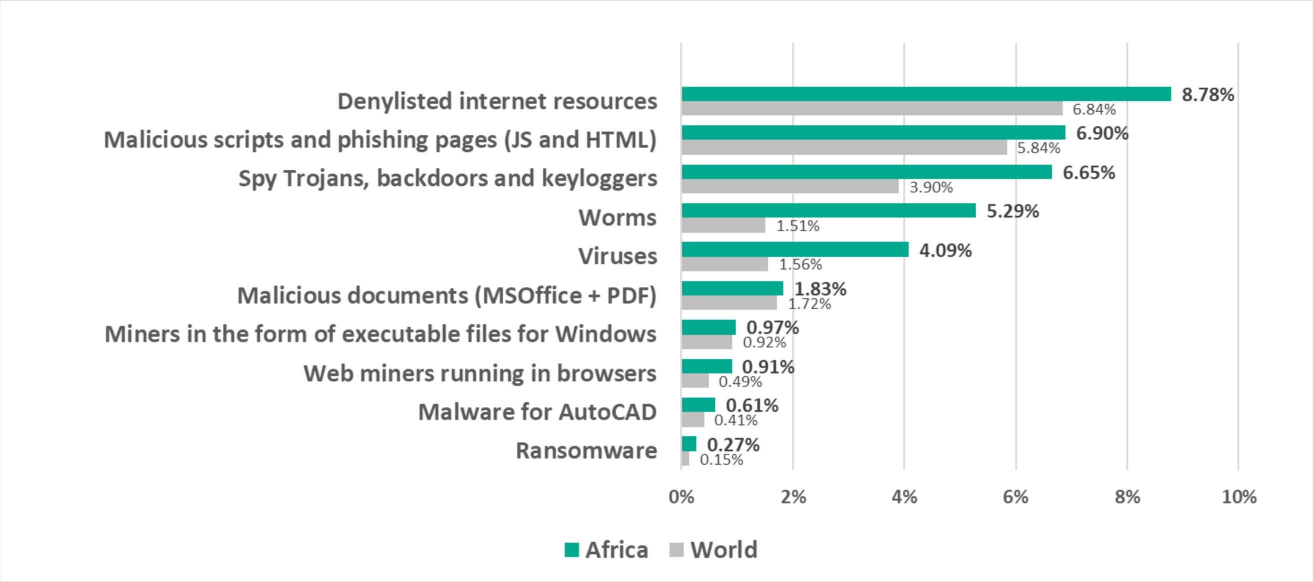
- By percentage of ICS computers on which **denylisted internet resources** were blocked.
- By percentage of ICS computers on which **spyware** was blocked.
- By percentage of ICS computers on which **web miners** were blocked.
- By percentage of ICS computers on which **worms** were detected (by a wide margin).
- By percentage of ICS computers on which **internet** threats were blocked
- By percentage of ICS computers on which **removable media** threats were blocked (by a wide margin).

In comparison to the world

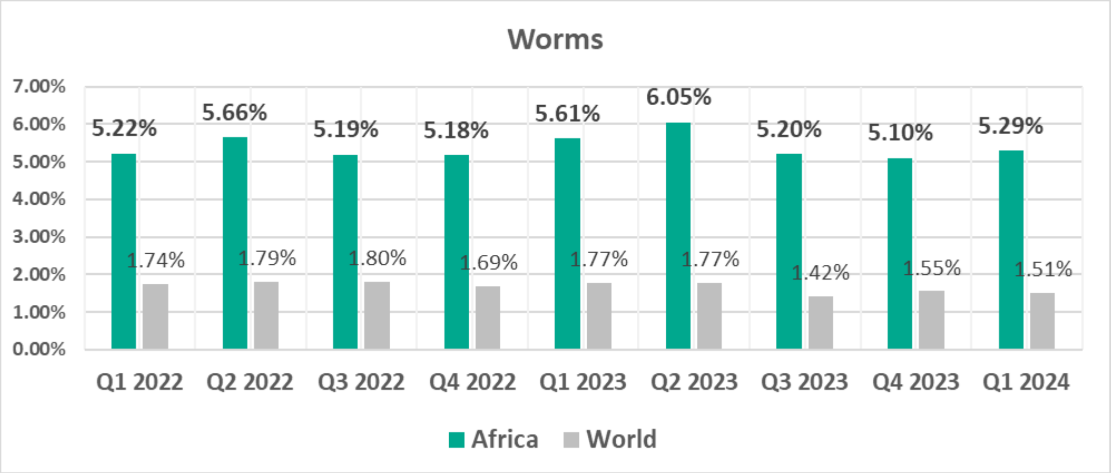
- Percentage of ICS computers on which malicious objects were blocked is higher than the global average.



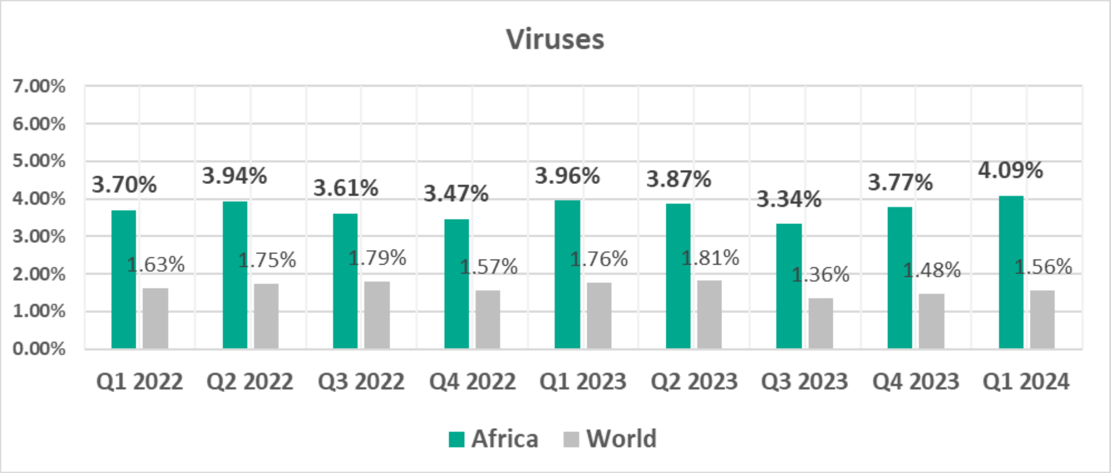
- Compared to global figures, the region has a higher percentage of ICS computers on which all categories of threats were blocked.



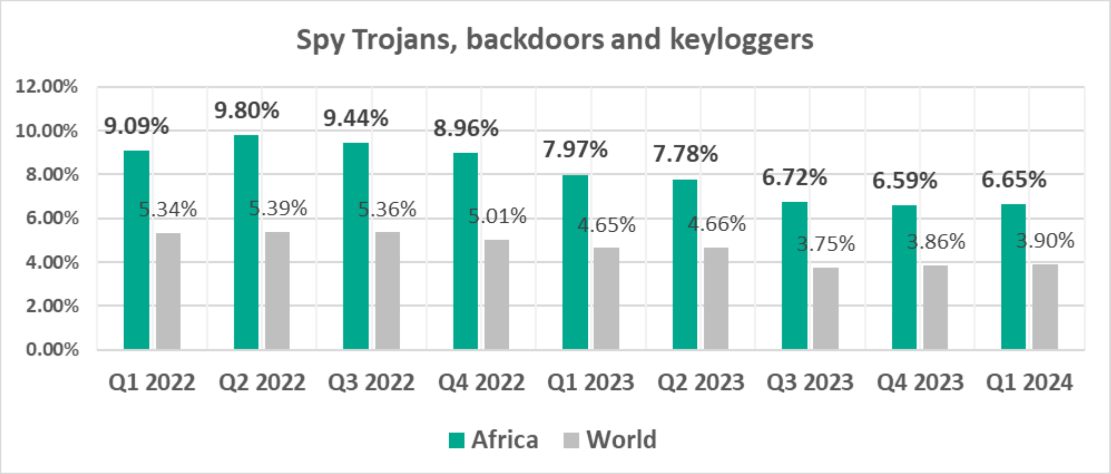
- From a global perspective, it has a significantly higher percentage of ICS computers on which the following was blocked:
  - Worms, by 3.5 times



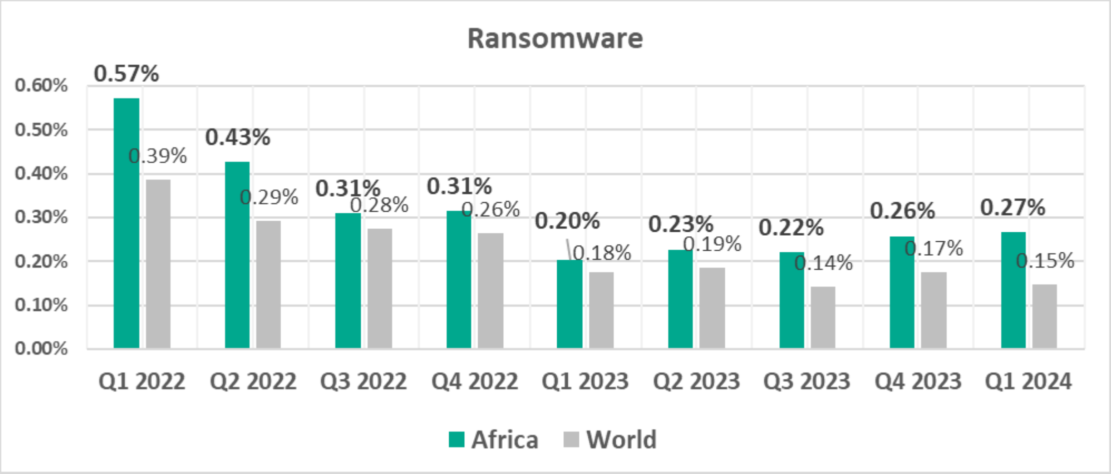
- Viruses, by 2.6 times



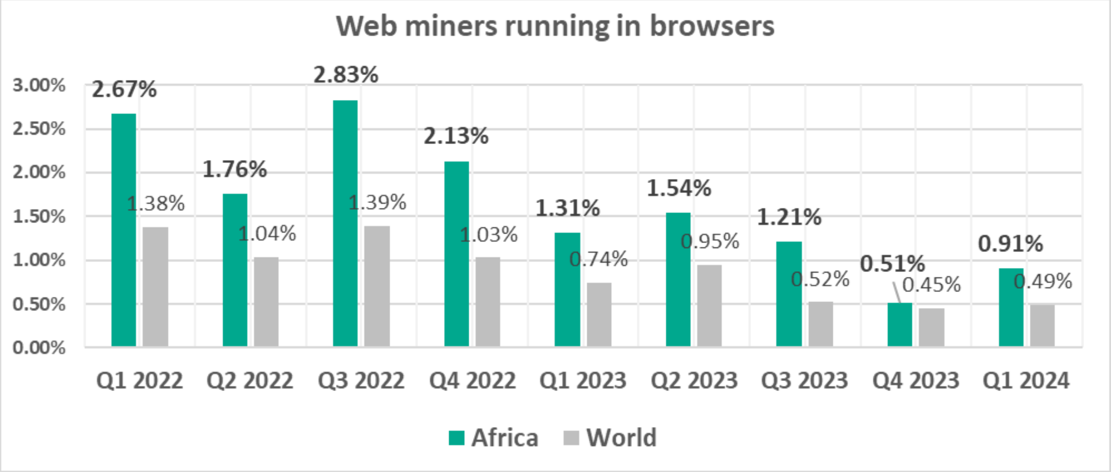
- Spyware, by 1.7 times



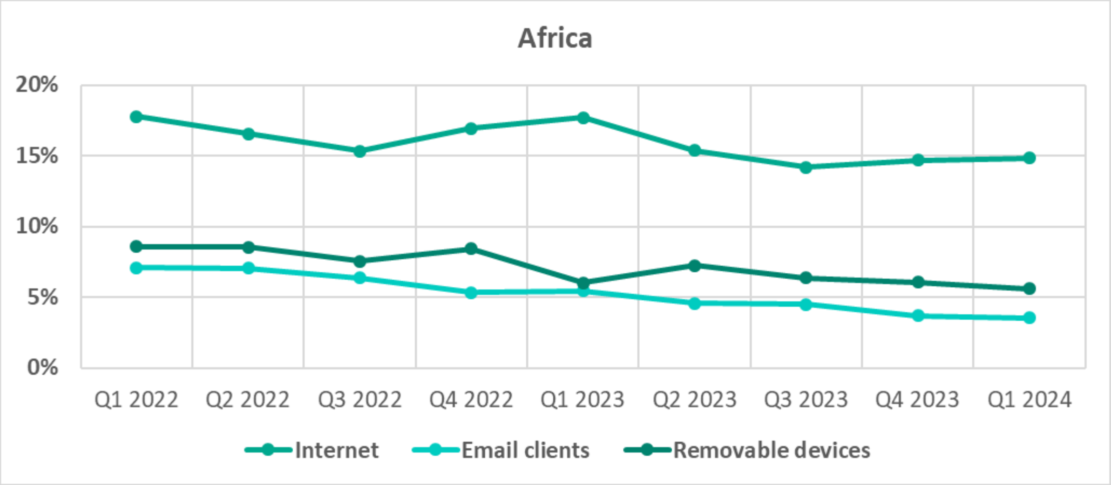
- Ransomware, by 1.8 times



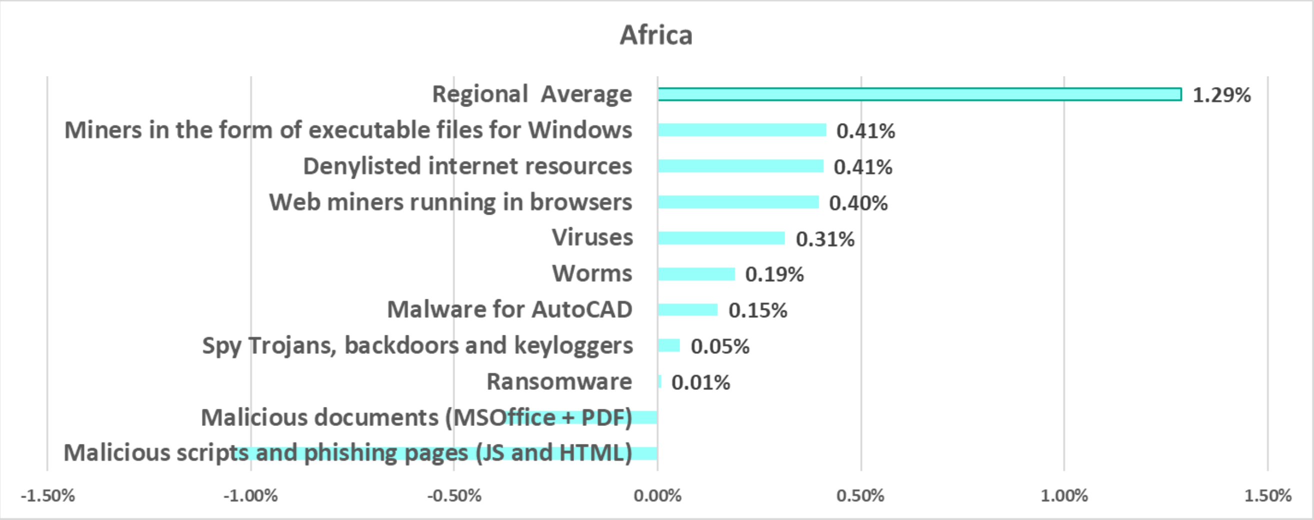
- Web miners, by 1.8 times



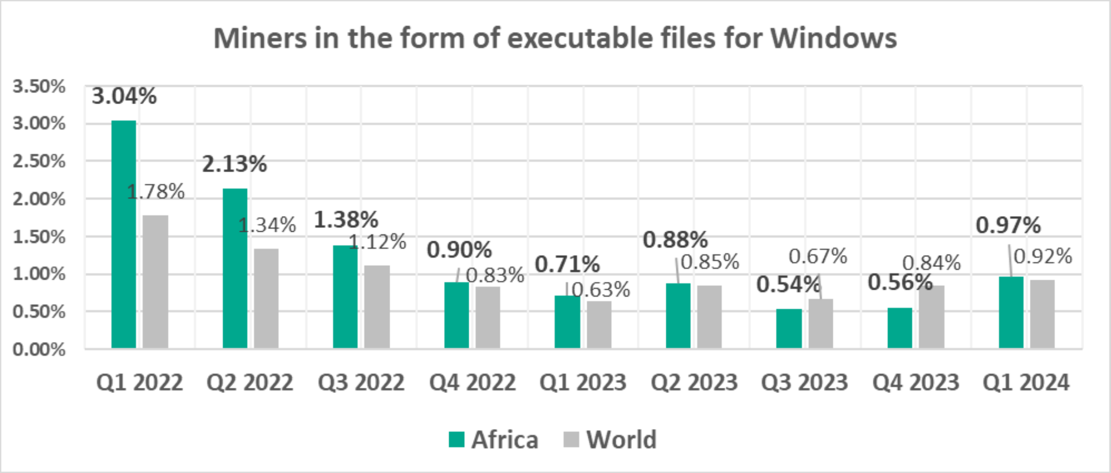
- **Worms and viruses** outpaced malicious documents in the threat category ranking by percentage of ICS computers on which they were blocked. Worms are in fourth place (sixth place globally).
- **Removable drives** occupy second place in the ranking of threat sources by percentage of ICS computers on which malicious objects from different sources were blocked (third place globally). Africa is one of three regions in which the percentage of ICS computers on which threats were blocked during connection of removable media exceeded the percentage of ICS computers on which email threats were blocked.



Quarterly changes



- The largest quarterly increase was in the percentage of ICS computers on which miners were blocked:
  - ➢ Web miners, by 1.8 times
  - ➢ Miners in the form of executable files for Windows, by 1.7 times



Current threats

- ➢ Threats spread over the internet
- ➢ Spyware
- ➢ Covert crypto-mining malware
- ➢ Worms
- ➢ Viruses
- ➢ Threats spread on removable media

In Africa, the percentage of ICS computers on which malicious objects were blocked was the highest among all regions.

In Q1 2024, we see a sharp increase in the percentage of ICS computers on which the following was blocked:

- ➢ Malicious miners

South-East Asia

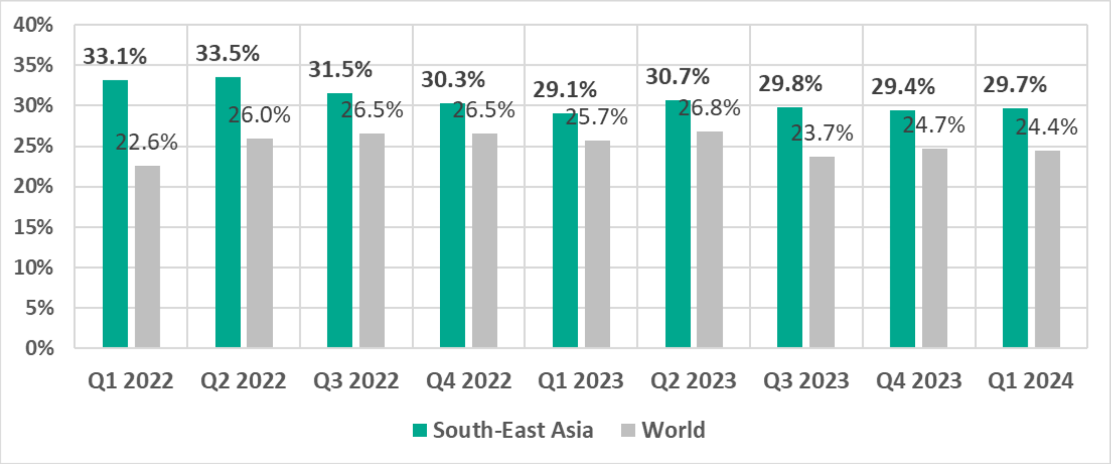
In comparison to other regions

Second place in the regional ranking.

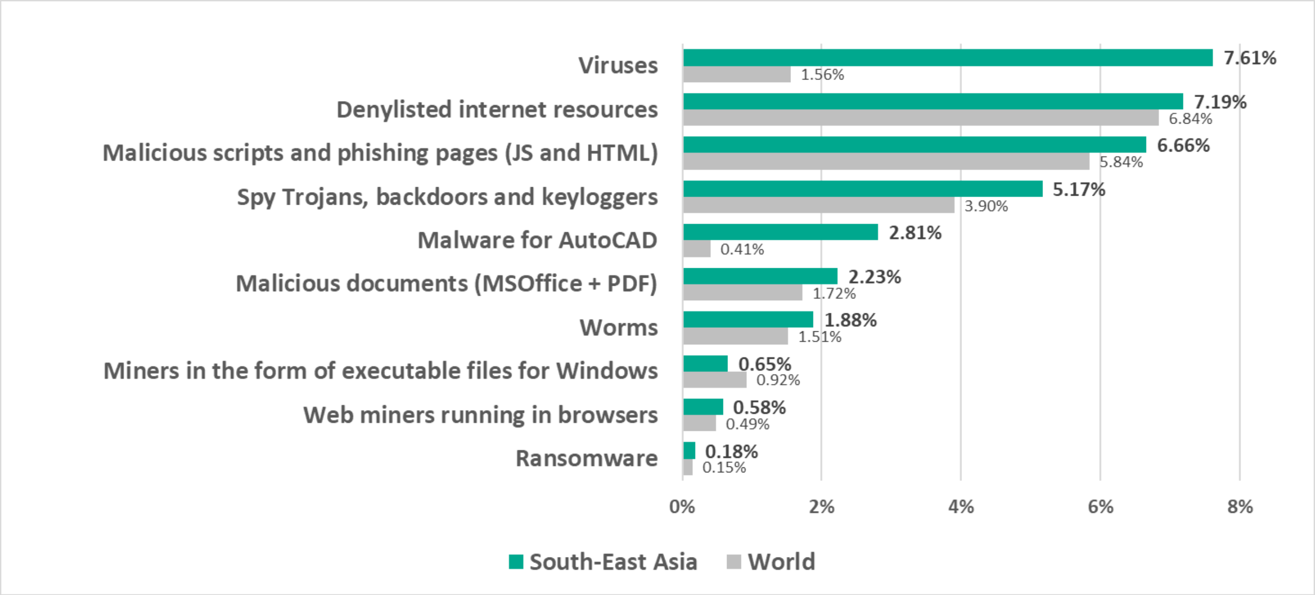
- **Leader** by percentage of ICS computers on which **viruses** were blocked (by a wide margin).
- In this region, the most significant growth during the quarter was in the percentage of ICS computers on which viruses were blocked (+1.1 pp).
- **Leader** by percentage of ICS computers on which **malware for AutoCAD** was blocked. In South-East Asia, Q1 2024 showed the highest growth of this figure among all regions (by 0.8 pp).
- **Leader** by percentage of ICS computers on which malware was blocked **in network folders**.
- **Second** among the regions by percentage of ICS computers on which **internet threats** were blocked.
- **Third** regionally by percentage of ICS computers on which malware was blocked when connecting **removable media**.

In comparison to the world

- Percentage of ICS computers on which malicious objects were blocked is higher than the global average.

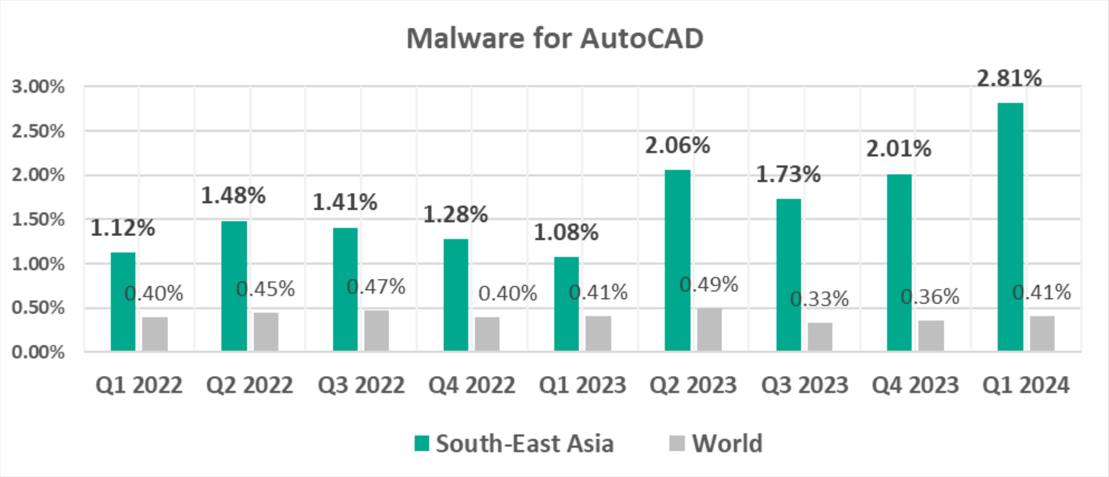


- **Viruses were first (!)** in the ranking of malware categories by percentage of ICS computers on which they were blocked. In South-East Asia, this percentage is 5 times higher than the global average.

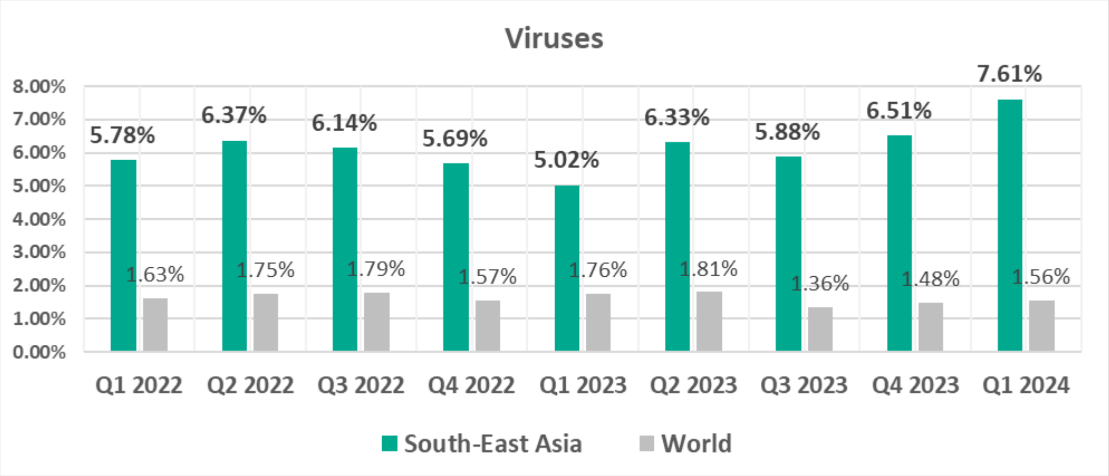


- **AutoCAD malware** took fifth place in this ranking (the global percentage of ICS computers on which this malware was blocked is the lowest among all categories).

- Compared to the global figures, the region has a significantly higher percentage of ICS computers on which the following was blocked:
    - AutoCAD malware, by 6.8 times

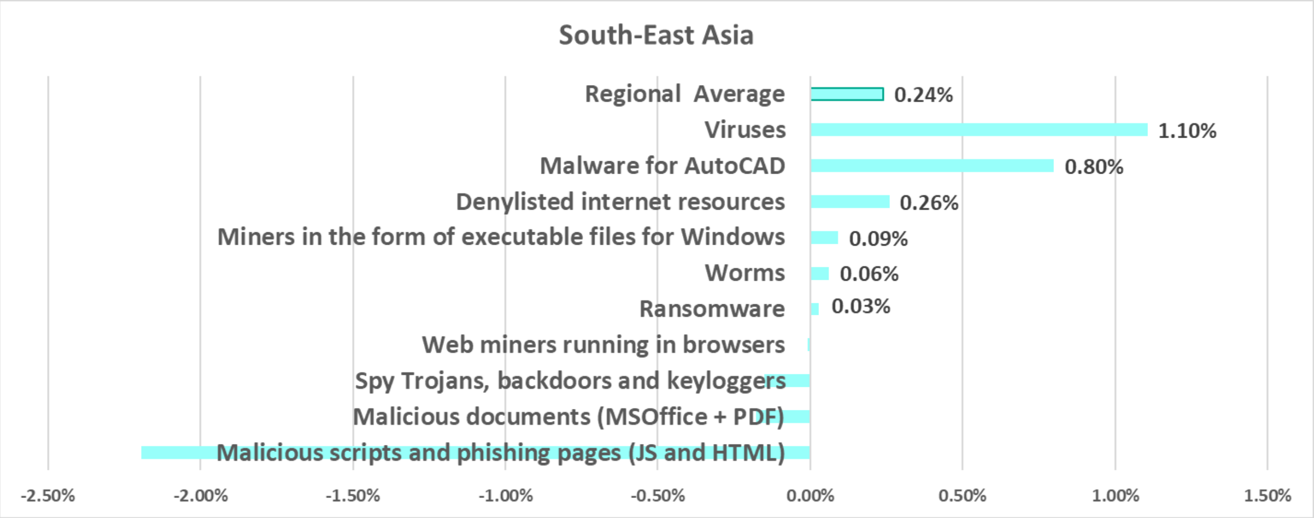


- Viruses, by 4 times



- Spyware, by 1.3 times
- Malicious documents, by 1.3 times
- Ransomware, by 1.2 times

Quarterly changes



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

- AutoCAD malware – by 1.4 times
- Viruses, by 1.2 times

Current threats

- **Viruses. Leading threat category by percentage of attacked ICS computers.** Globally, this category is in fifth place while in other regions it does not get any higher than fourth place (East Asia).
- Spyware
- Ransomware
- AutoCAD malware
- Threats spread on removable media

Industrial organizations in the region need to ensure better protection of their industrial network with at least the minimum set of security measures and tools.

Middle East

In comparison to other regions

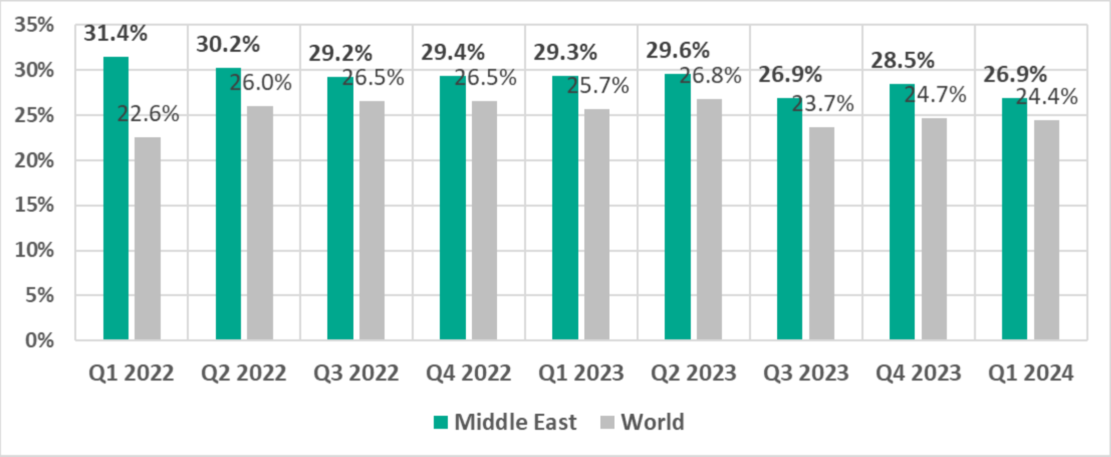
Third place in the regional ranking.

- **Leader** by percentage of ICS computers on which **ransomware** was blocked.

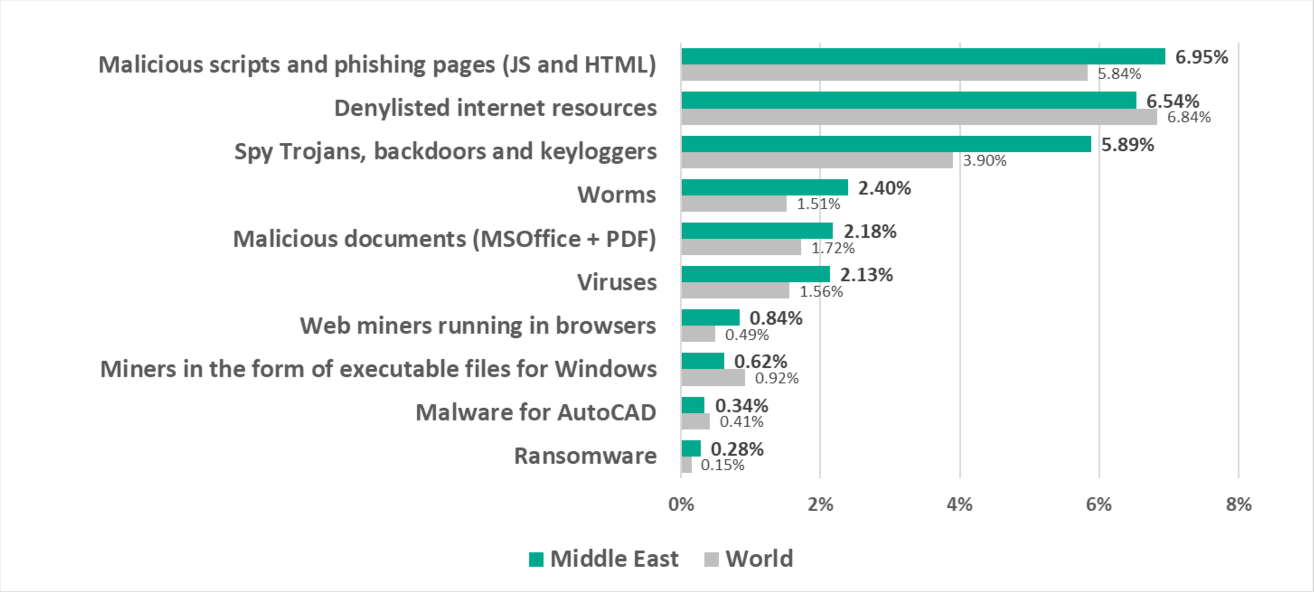
- **Second** by percentage of ICS computers on which **spyware** was blocked.
- **Second** by percentage of ICS computers on which **web miners** were blocked.
- **Third** by percentage of ICS computers on which **worms** were blocked.
- **Third** by percentage of ICS computers on which **malicious scripts and phishing pages were blocked**.
- **Third** by percentage of ICS computers on which **email threats** were blocked.

In comparison to the world

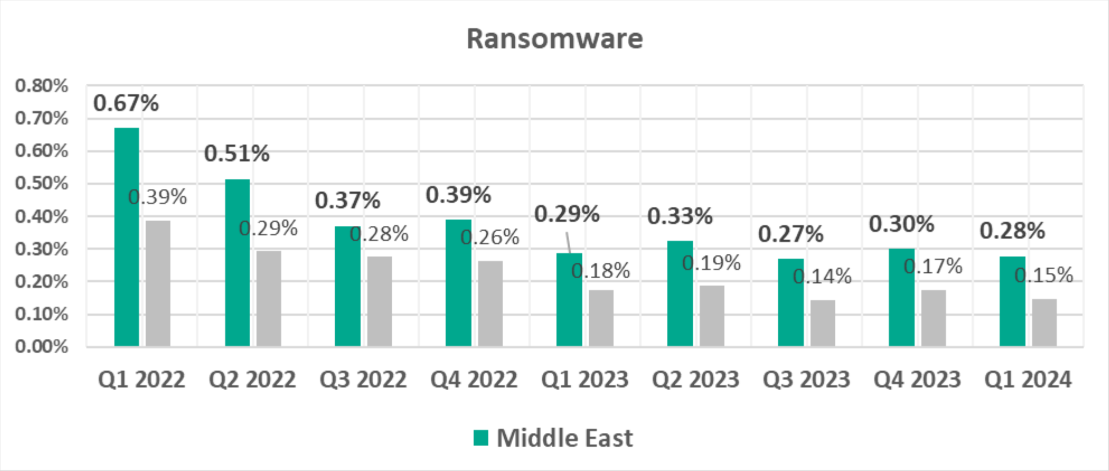
- Percentage of ICS computers on which malicious objects were blocked is higher than the global average.



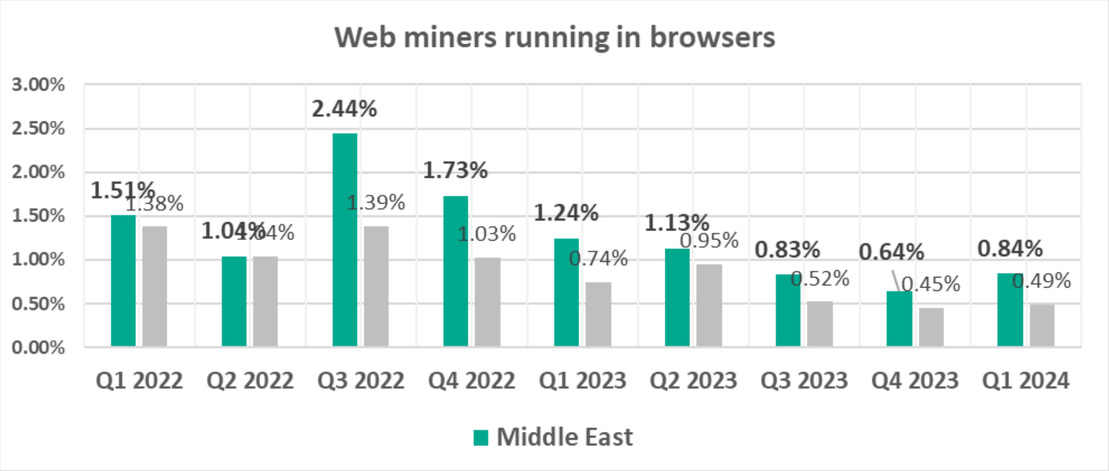
- Compared to the global figures, the region has a higher percentage of ICS computers on which all categories of threats were blocked, except denylisted internet resources.



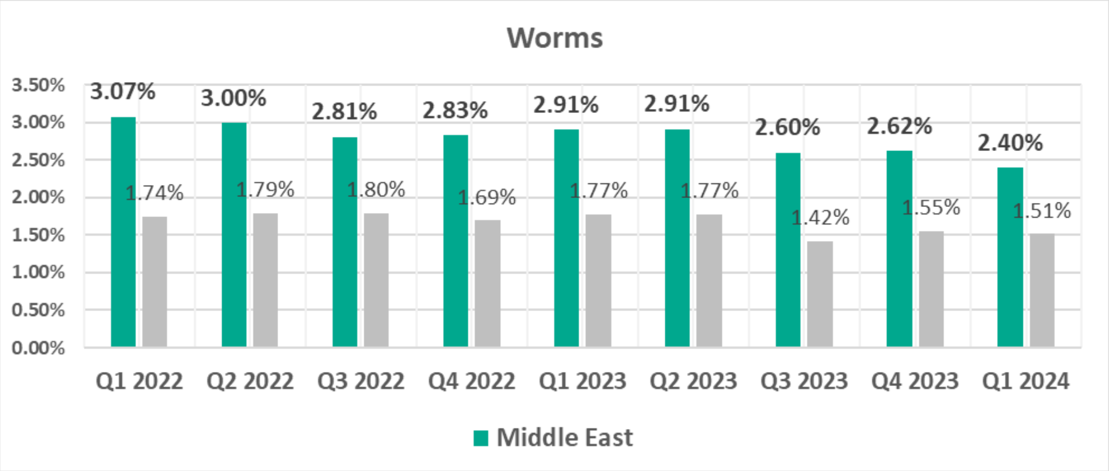
- Compared to the global average, the region has a noticeably higher percentage of ICS computers on which the following was blocked:
  - ➢ Ransomware, by 1.9 times



- Web miners, by 1.7 times

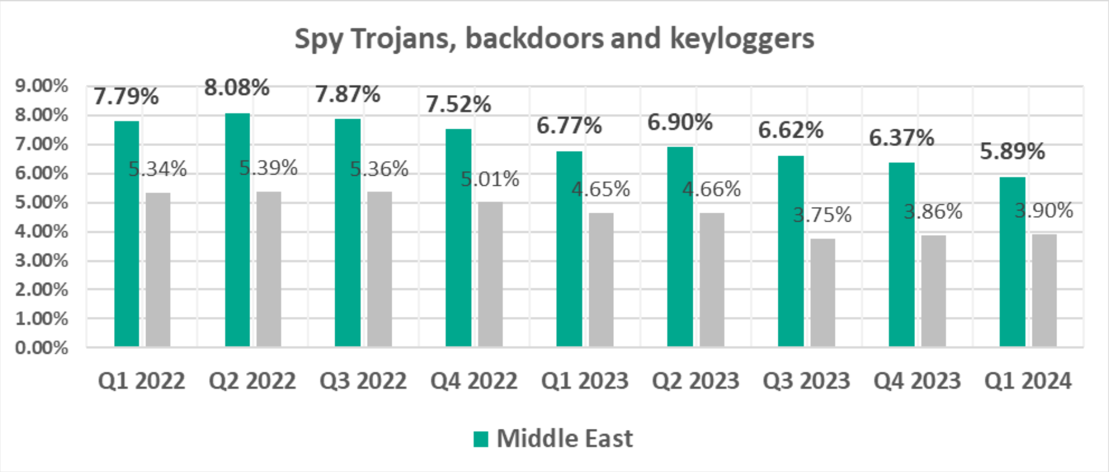


- Worms, by 1.6 times

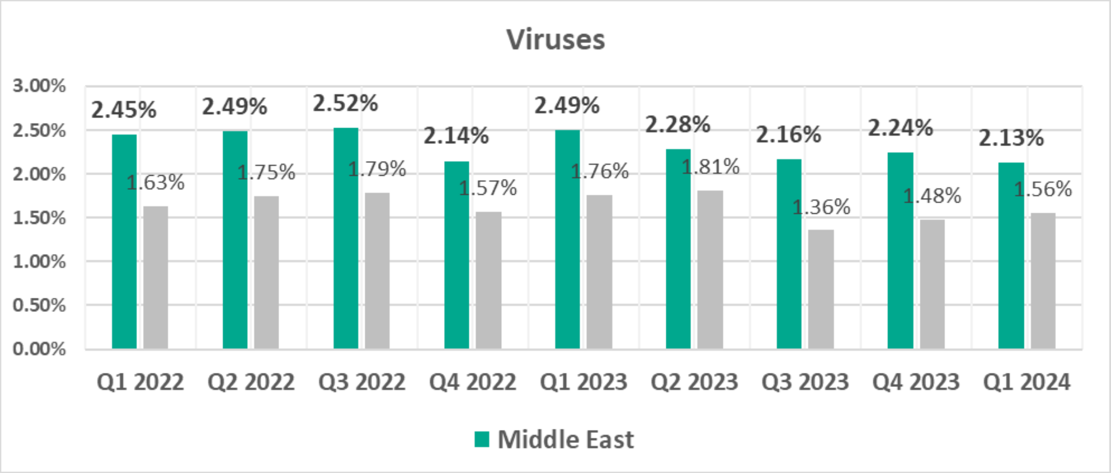


Worms were fourth in the ranking of malware categories by percentage of ICS computers on which they were blocked (sixth globally).

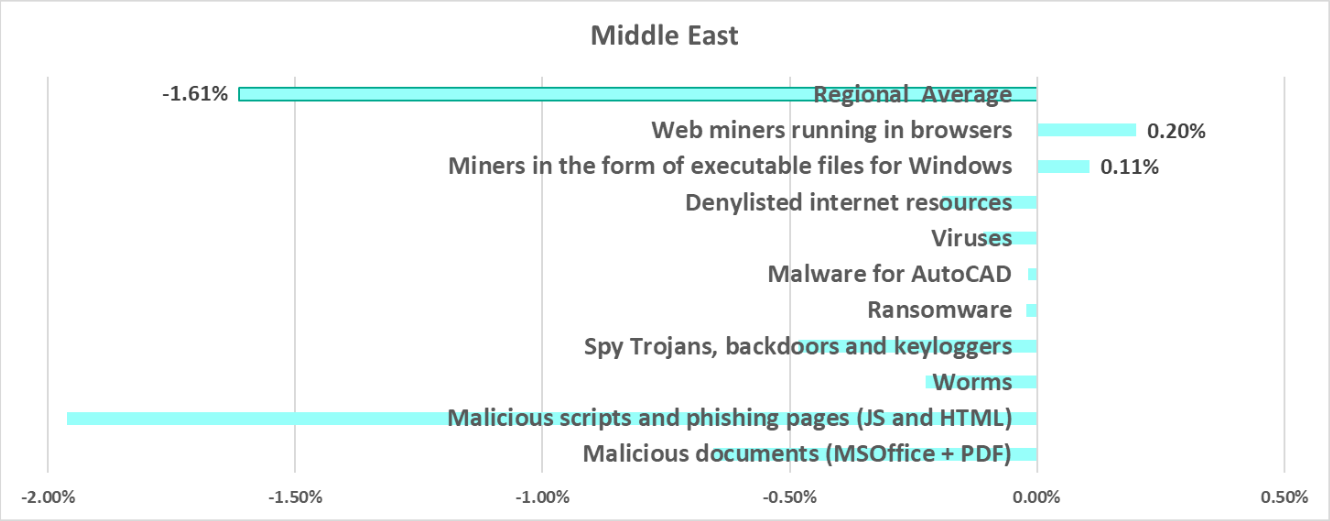
- Spyware, by 1.5 times



- Viruses, by 1.5 times



Quarterly changes



The largest quarterly increase was in the percentage of ICS computers on which covert crypto-mining malware was blocked:

- Web miners, by 1.3 times
- Miners in the form of executable files for Windows, by 1.2 times

Current threats

- **Ransomware**
  From Q4 2022 through Q3 2023, the Middle East held second place in the regional ranking for this threat category. It has been the leader since Q4 2023.
- Spyware
- Worms and viruses
- Malicious miners
- Email threats

Central Asia

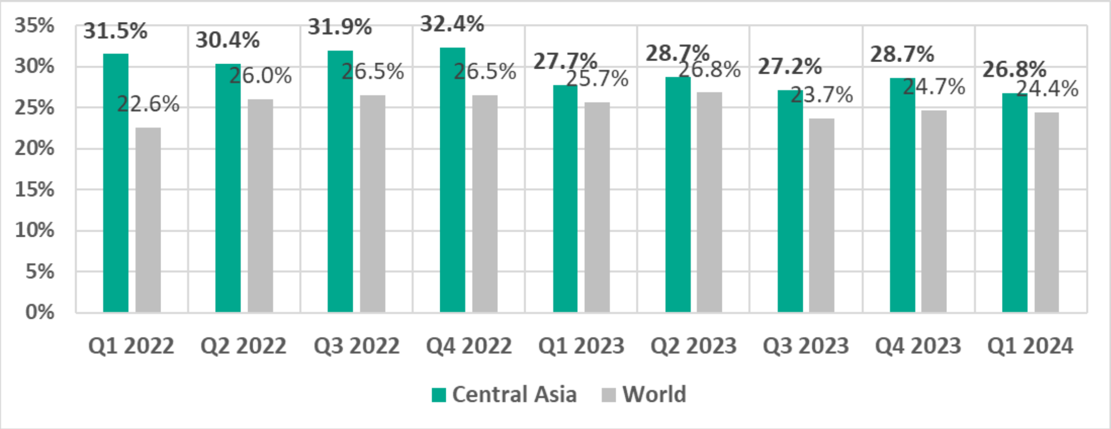
In comparison to other regions

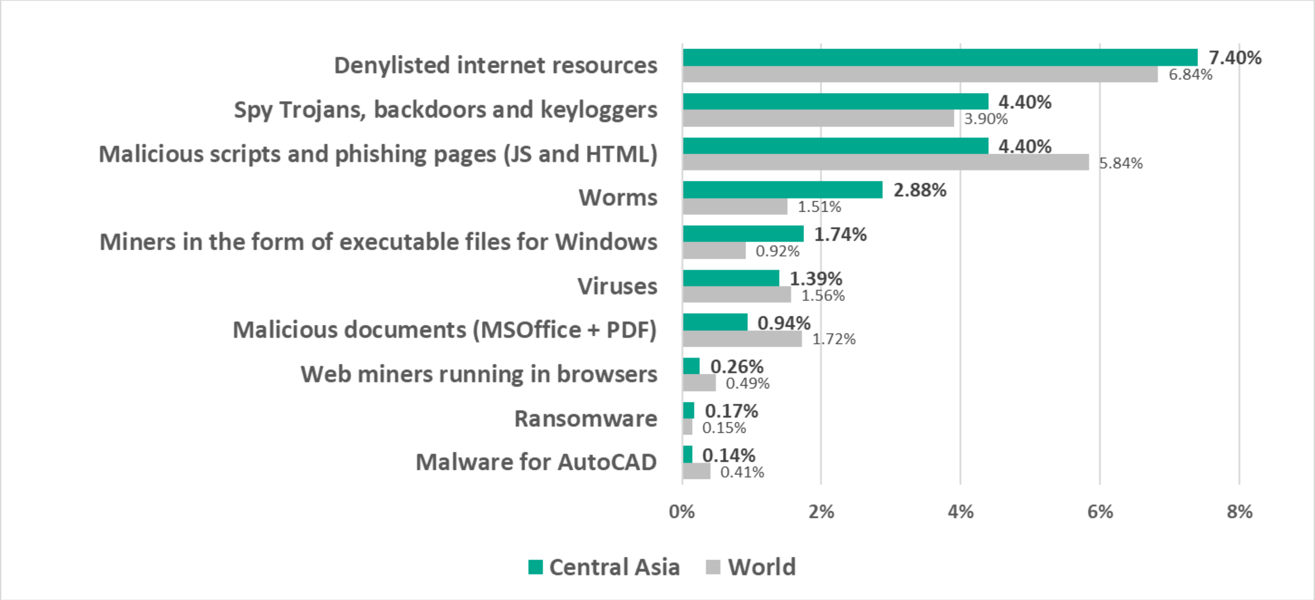
Fourth place in the regional ranking.

- **Leads** by percentage of ICS computers on which **miner executable files for Windows** were blocked.
- **Second** by percentage of ICS computers on which **worms** were blocked.

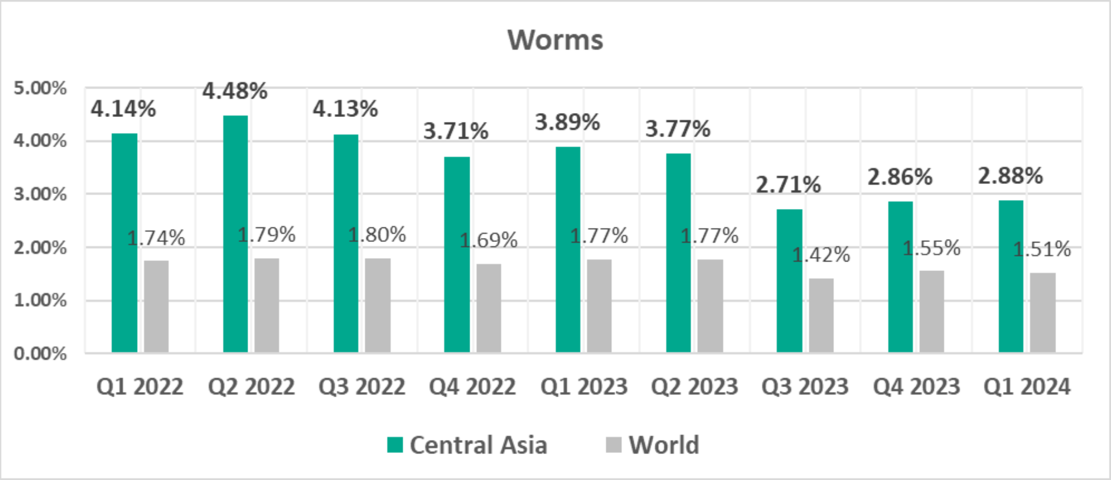
In comparison to the world

- Percentage of ICS computers on which malicious objects were blocked is higher than the global average.

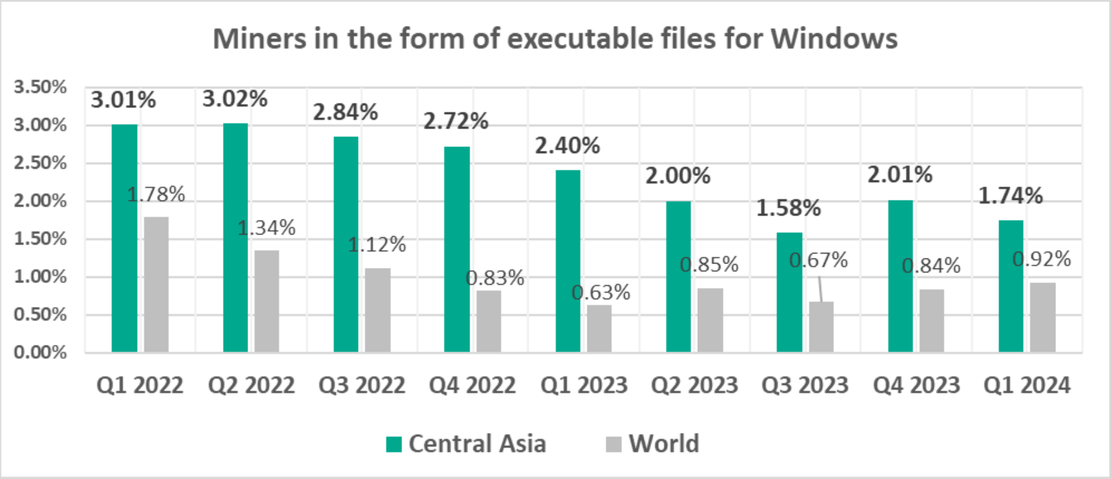




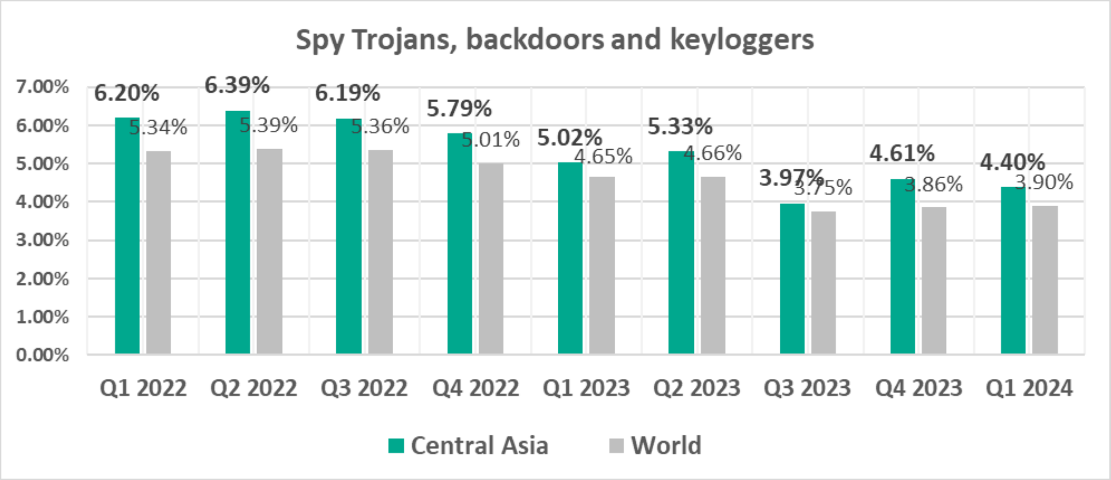
- Compared to the global average, the region has a higher percentage of ICS computers on which the following was blocked:
  - ➢ Worms, by 1.9 times. Worms rank in fourth place (sixth place globally).



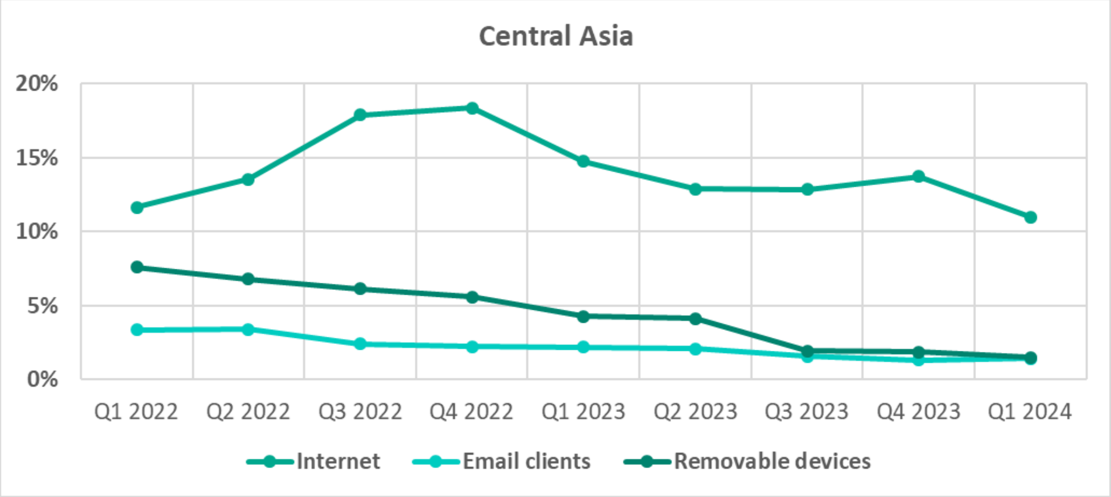
  - ➢ Miners in the form of executable files for Windows, by 1.9 times. This threat category ranks in fifth place (seventh place globally).



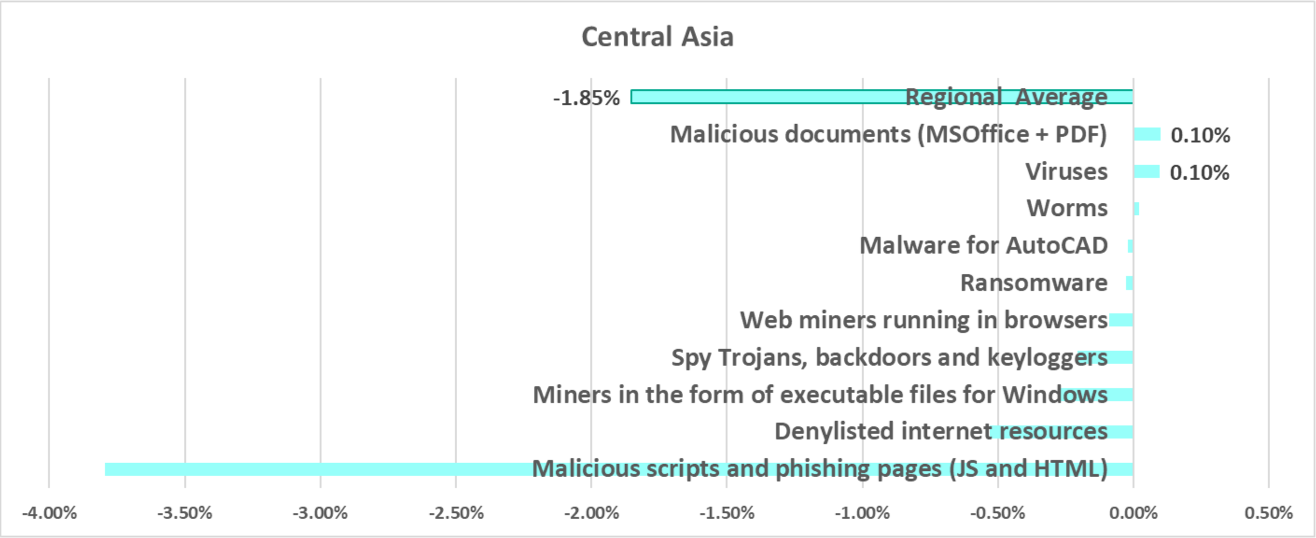
- **Spyware was second** in the ranking of malware categories by percentage of ICS computers on which it was blocked.



- In the region, **removable media** category occupies second place in the ranking of threat sources by percentage of ICS computers on which malicious objects from different sources were blocked. One of three regions in which the percentage of ICS computers on which threats were blocked when connecting removable media exceeded the percentage of ICS computers on which email threats were blocked.



Quarterly changes



Current threats

- Spyware
- Miners in the form of executable files for Windows
- Worms
- Threats spread on removable media

Eastern Europe

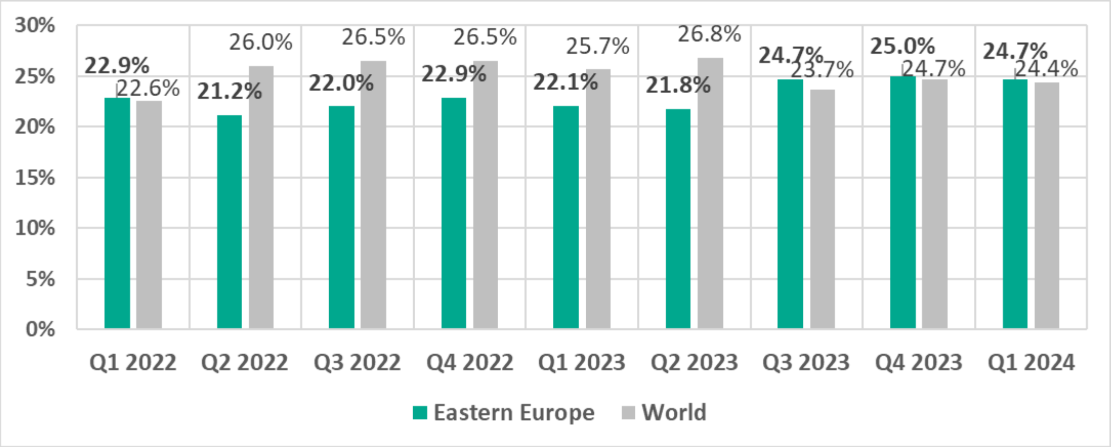
In comparison to other regions

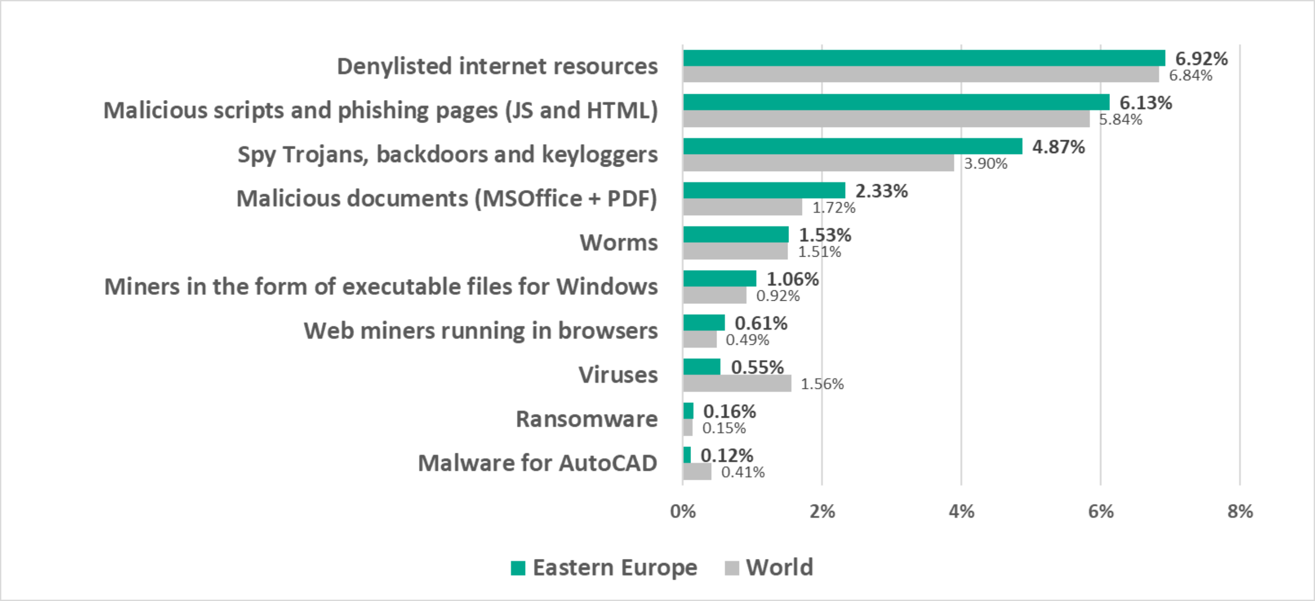
Fifth place in the regional ranking. Before Q2 2023, the region did not rank higher than ninth place.

- **Third** by percentage of ICS computers on which **malicious documents** were blocked. One of two regions where this figure grew during the quarter (by the 0.36 pp, which is the maximum growth rate).
- **Third** by percentage of ICS computers on which **miner executable files for Windows** were blocked.
- **Fourth** by percentage of ICS computers on which **email threats** were blocked.
- **Only region in the world** that shows growth in the vulnerability of OT computers to cyberthreats since the beginning of 2022.

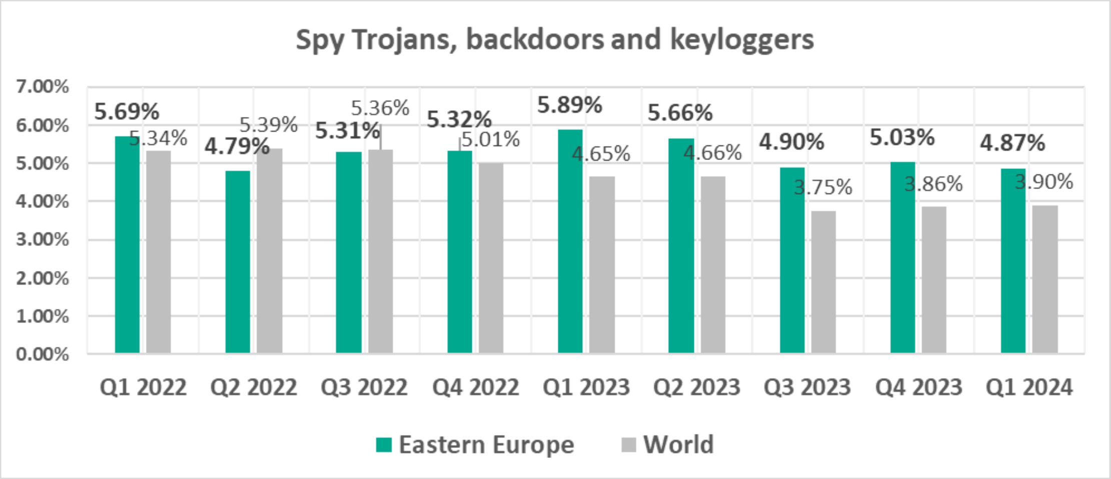
In comparison to the world

- The percentage of ICS computers on which malicious objects were blocked since Q3 2023 is slightly higher than the global average.

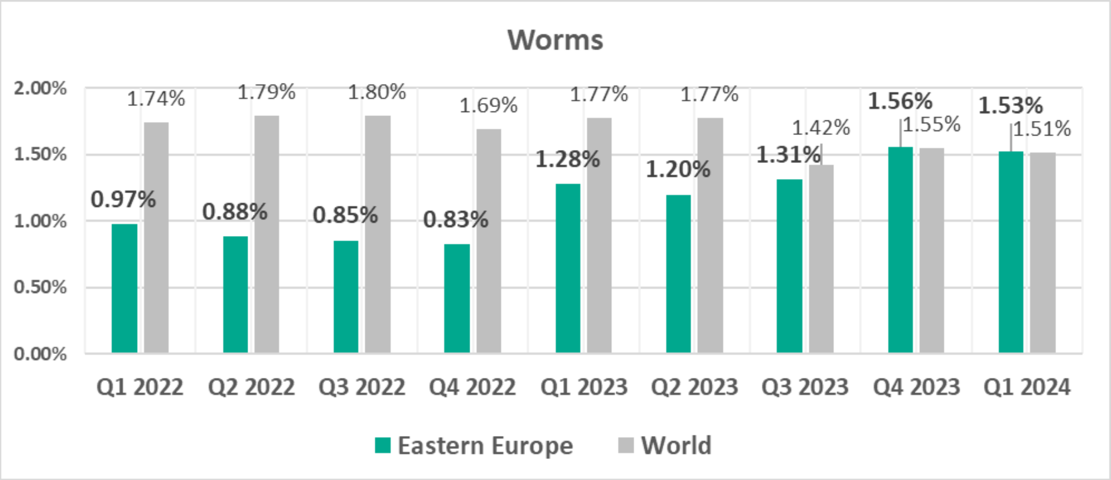




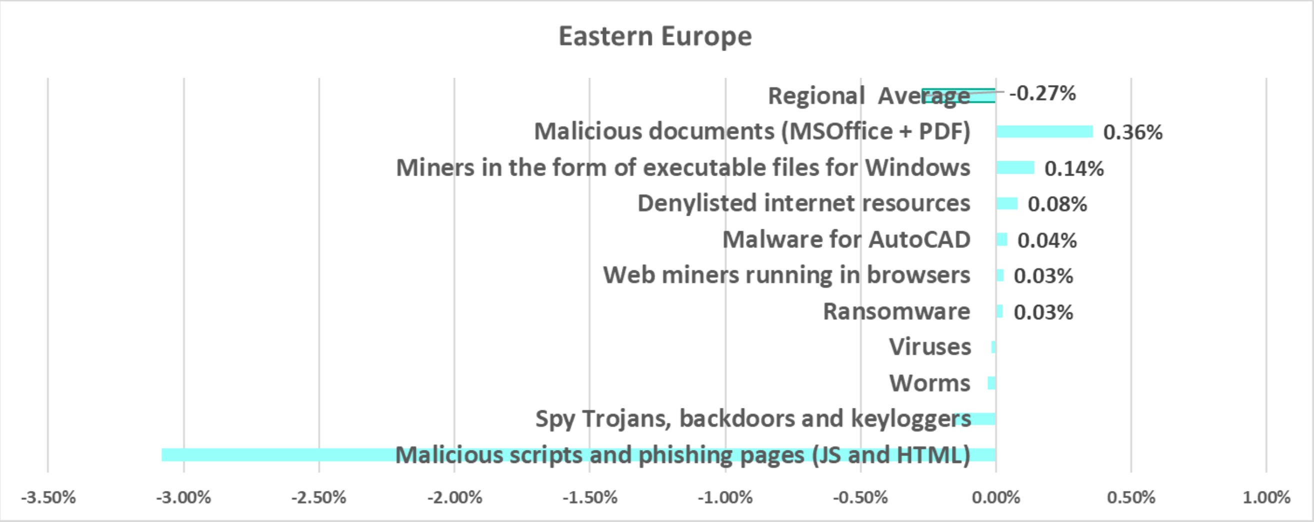
- Compared to the global average, the region has a noticeably higher percentage of ICS computers on which the following was blocked:
  - Spyware, by 1.2 times



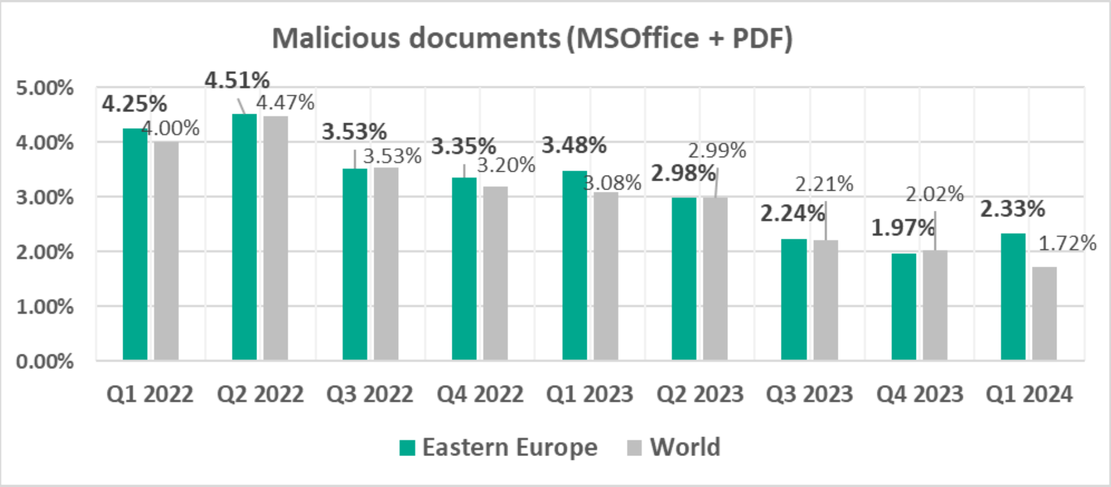
- Since the beginning of 2023, the percentage of ICS computers on which worms were blocked has grown in the region.



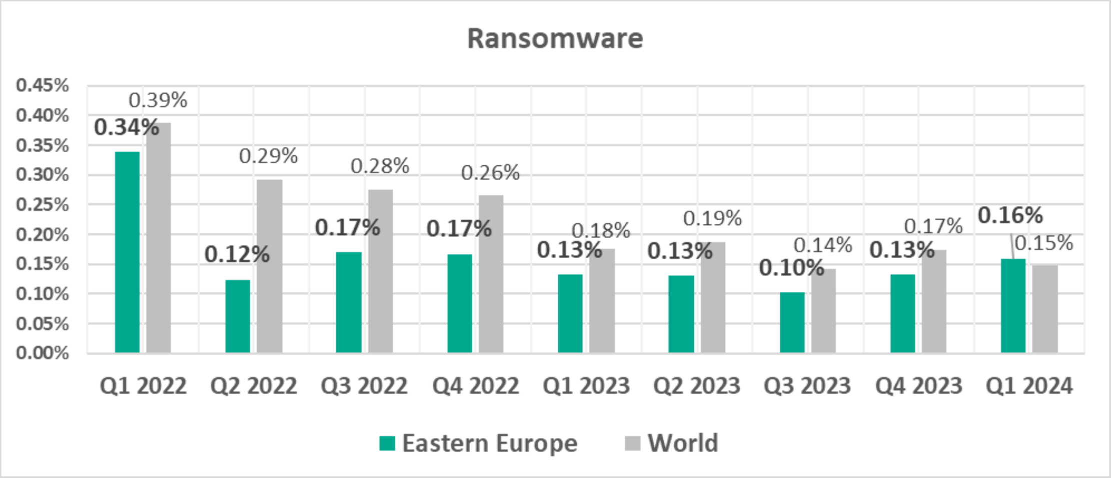
Quarterly changes



- The largest quarterly increase was in the percentage of ICS computers on which the following was blocked:
  - Malicious documents, by 1.2 times. As a result of this growth, the percentage for malicious documents in the region exceeded the corresponding global indicator by 1.4 times.



- Ransomware, by 1.2 times. The percentage is growing for the second quarter in a row and already caught up with the global average.



Current threats

- Malicious documents
- Spyware
- Ransomware
- Email threats
- Worms
- Miners in the form of executable files for Windows

The vulnerability of OT systems to various types of threats is apparently due to the region's general deficiency of cybersecurity financing for industrial facilities. In particular, the increased percentage of ICS computers on which worms were detected signifies that the OT infrastructure is not sufficiently covered by endpoint security tools. The increased risk of compromise of industrial infrastructures via phishing is also evident by the high indicators for threats spread by email and by the high percentage of computers on which malicious documents were blocked.

Russia

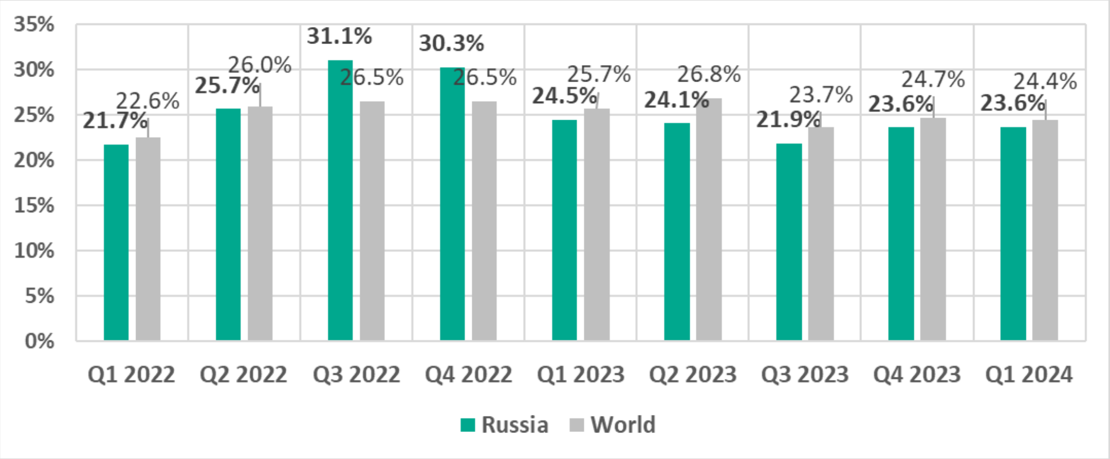
In comparison to other regions

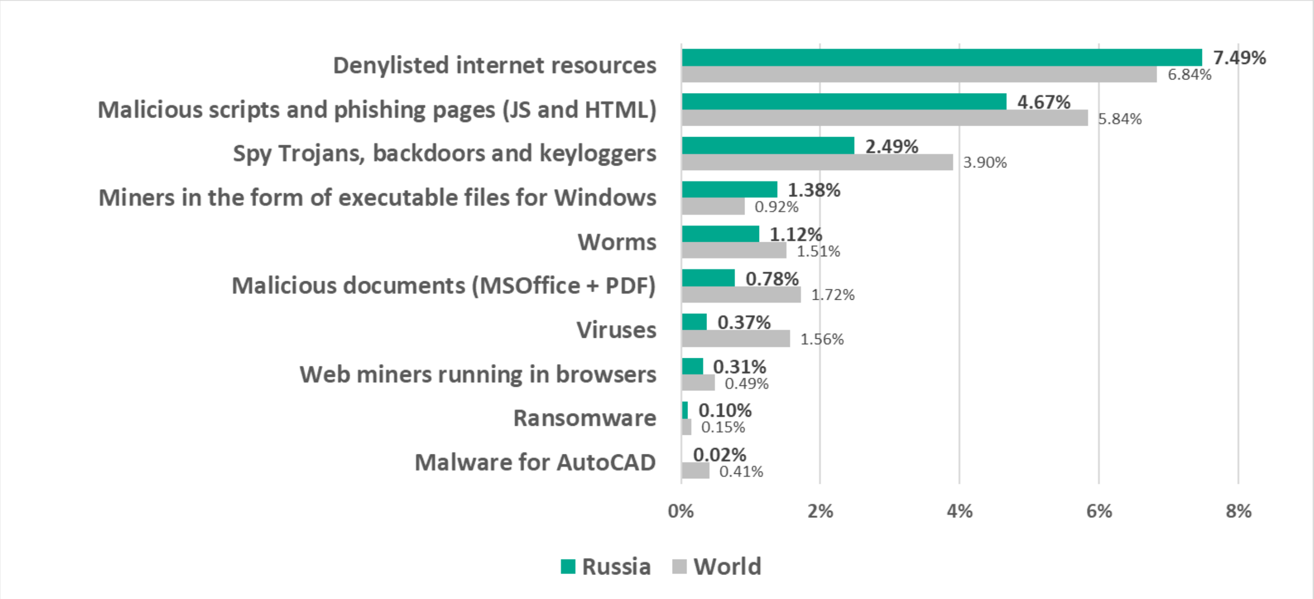
Sixth place in the regional ranking.

- **Second** by percentage of ICS computers on which **denylisted internet resources** were blocked.
- **Second** by percentage of ICS computers on which **miner executable files for Windows** were blocked.

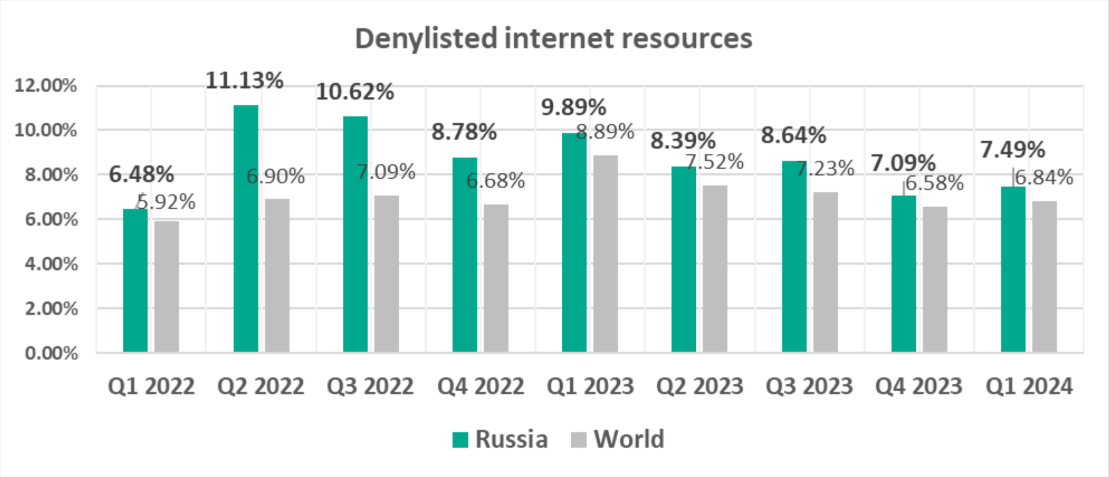
In comparison to the world

- 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.

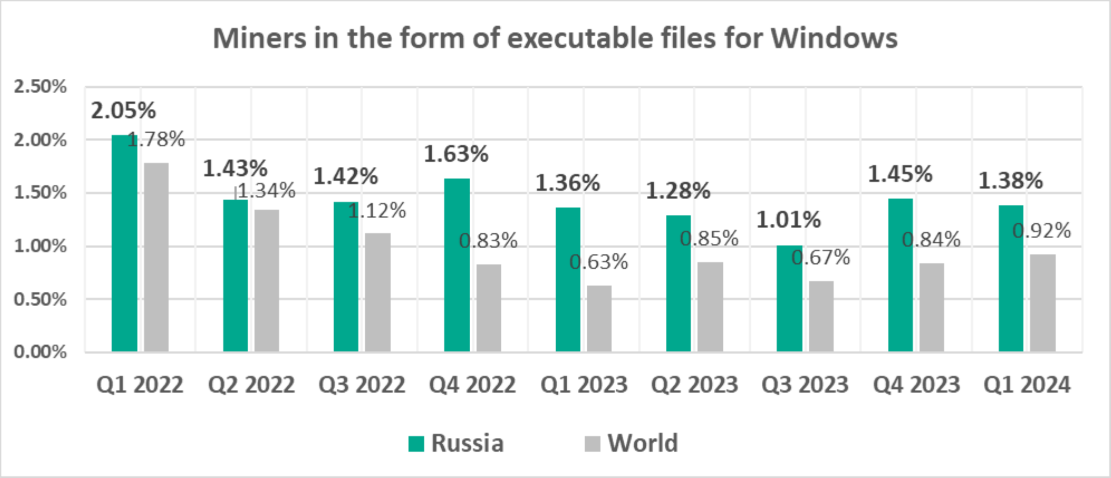




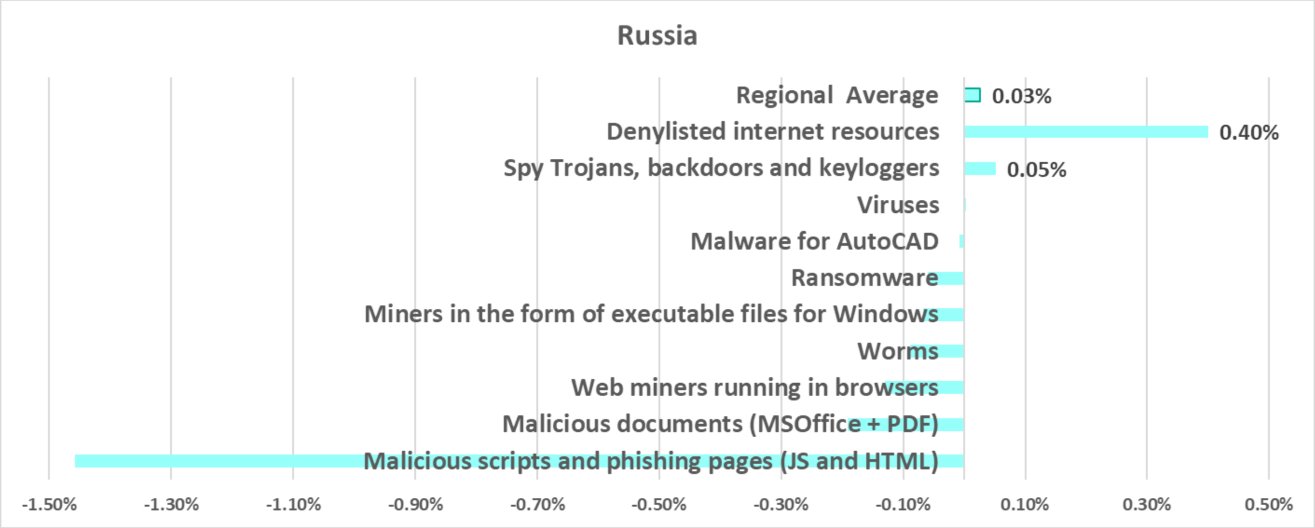
- Compared to the global average, the region has a higher percentage of ICS computers on which the following was blocked:
  - Denylisted internet resources



- Miners in the form of executable files for Windows, by 1.5 times. Such miners were fourth in the region by percentage of ICS computers on which they were blocked (by a wide margin).



Quarterly changes



Current threats

- Internet threats
- Miners in the form of executable files for Windows

Industrial organizations in Russia should seriously try to reduce internet access on ICS computers and train their employees how to securely work with internet resources when access to them is really required. Right now, the high risk of infection is directly linked to internet access that goes far beyond the pale of reason.

Latin America

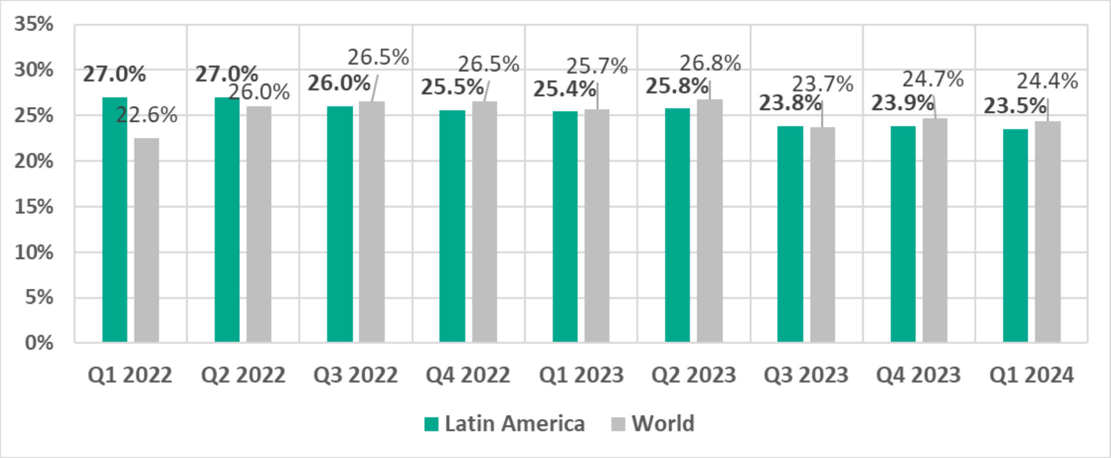
In comparison to other regions

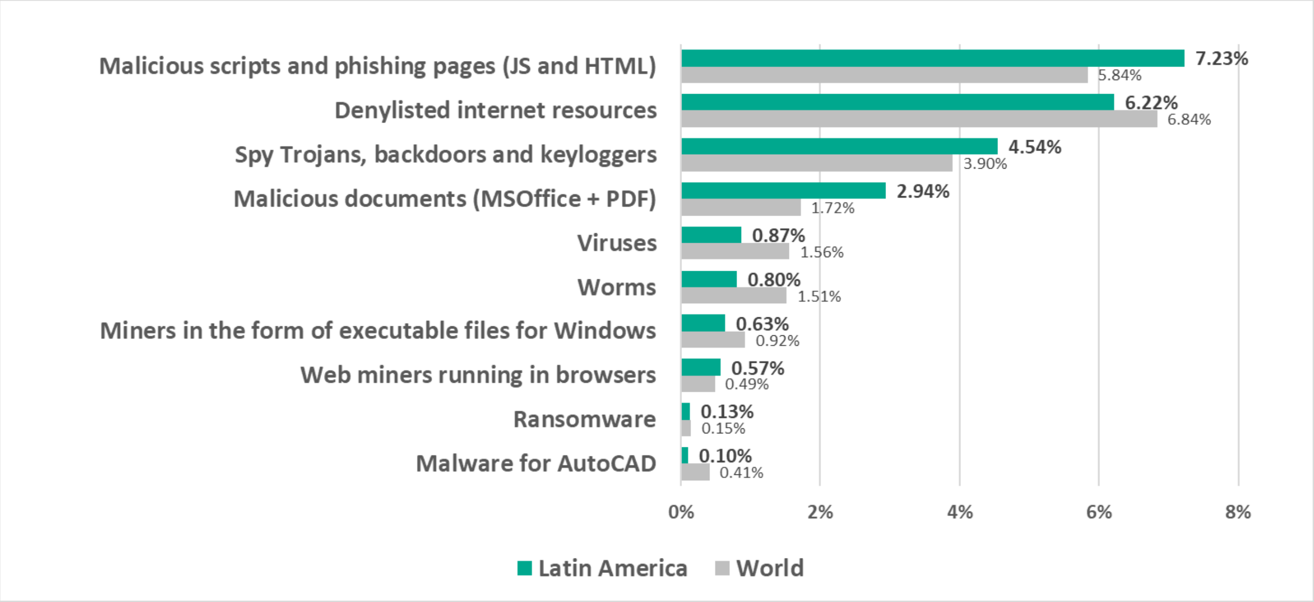
Seventh place in the regional ranking.

- **Leads** by percentage of ICS computers on which **malicious scripts and phishing pages** were blocked.
- **Second** by percentage of ICS computers on which **malicious documents** were blocked.
- **Second** by percentage of ICS computers on which **email threats** – malicious email attachments and phishing links – were blocked.
- The percentage of ICS computers on which **spyware** was blocked during the quarter grew by 0.92 pp, which was the maximum among regions.

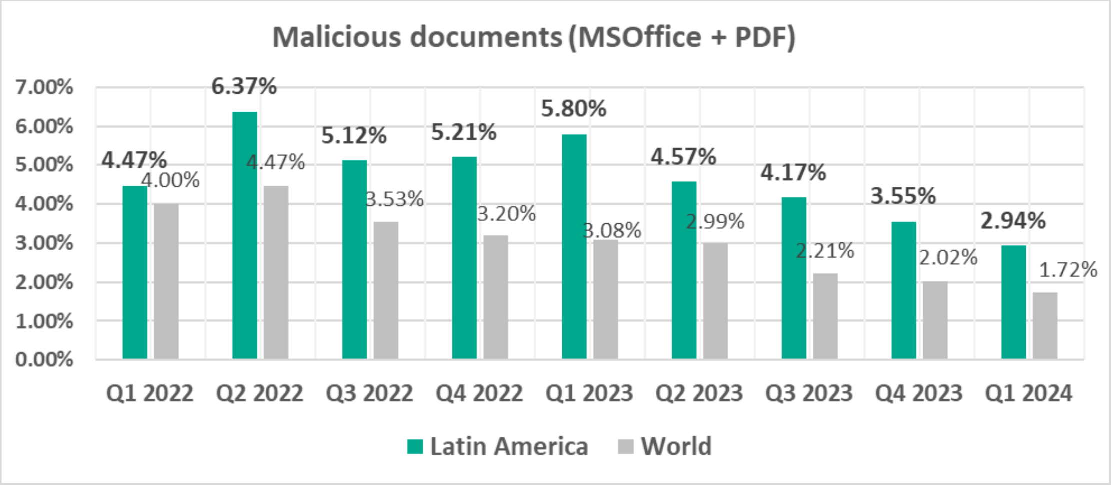
In comparison to the world

- Percentage of ICS computers on which malicious objects were blocked is close to the global average.

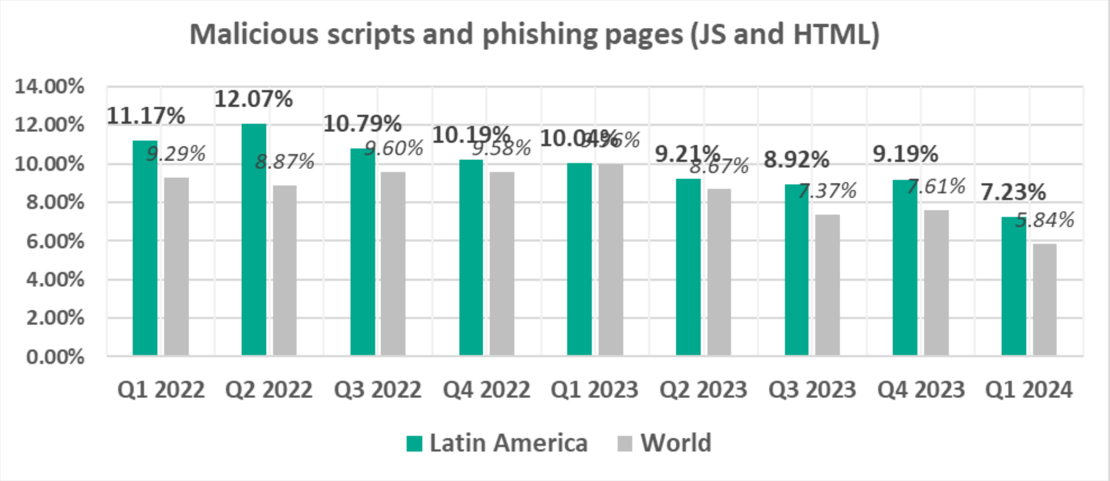




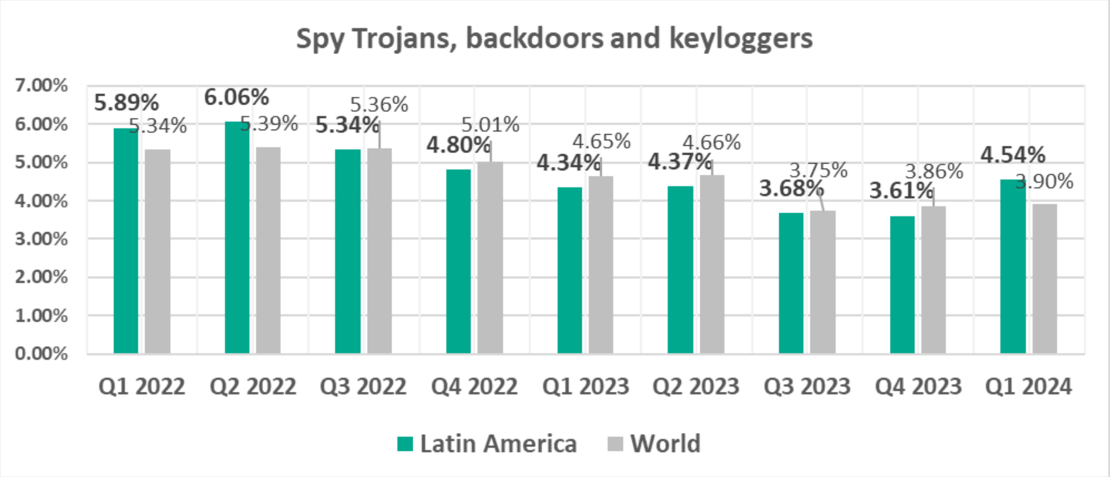
- Compared to the global average, the region has a higher percentage of ICS computers on which the following was blocked:
  - Malicious documents, by 1.7 times



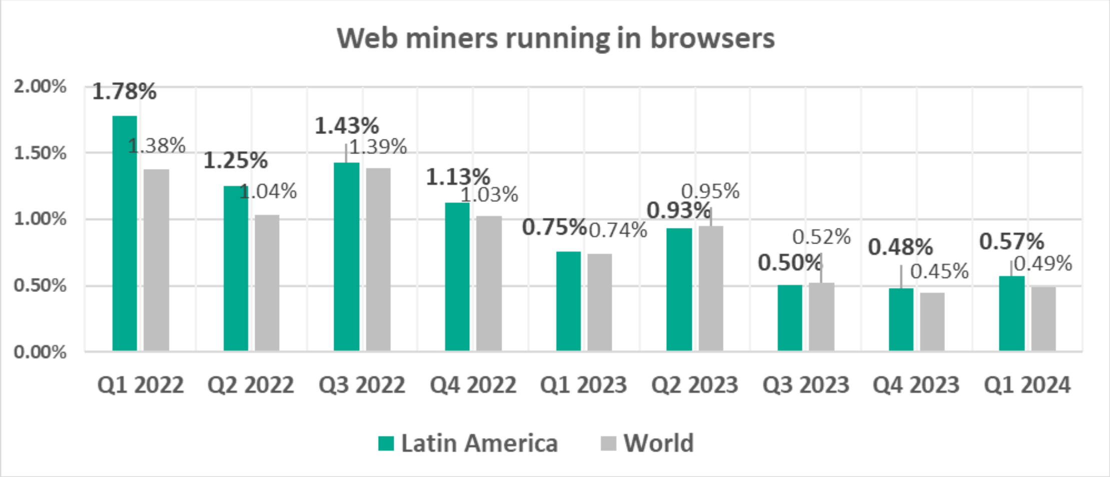
- Malicious scripts and phishing pages, by 1.2 times



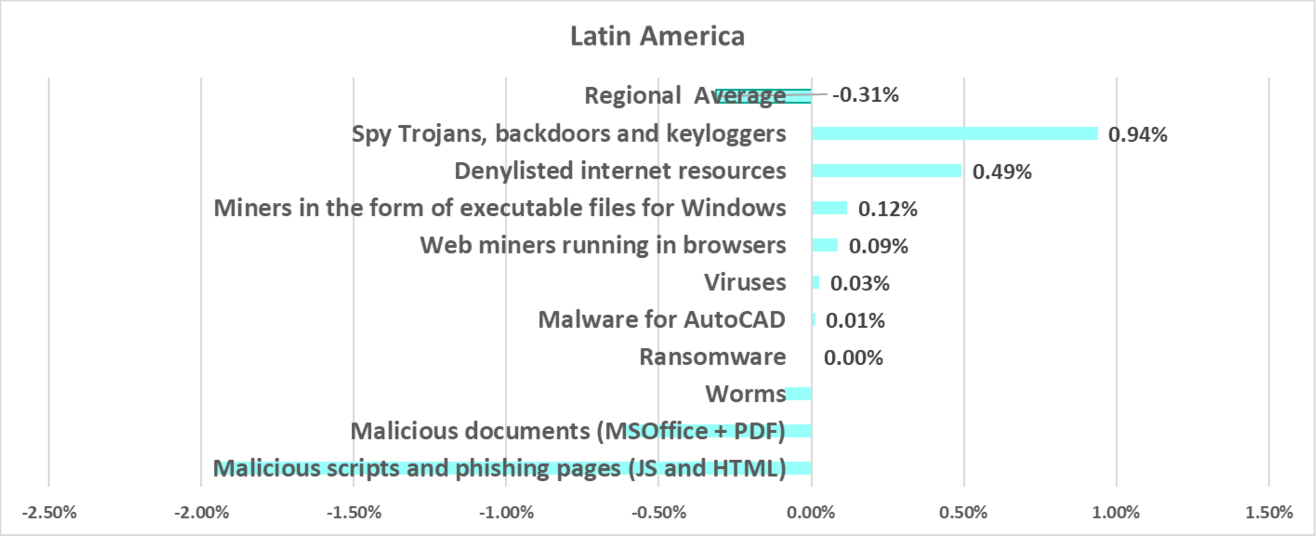
- Spyware, by 1.2 times



- Web miners

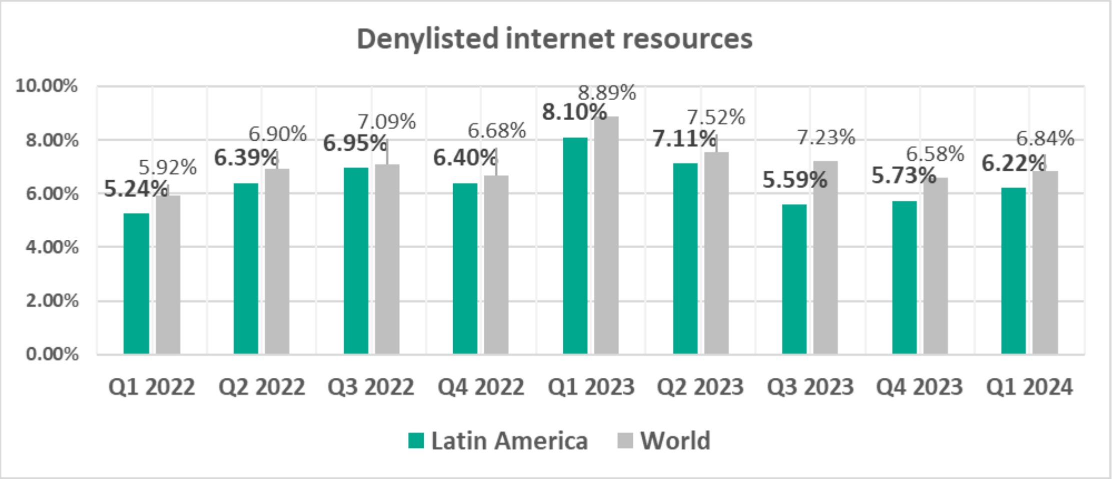


Quarterly changes



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

- Spyware, by 1.3 times
- Denylisted internet resources are slowly growing for the second quarter in a row.



Current threats

- Malicious scripts and phishing pages
- Malicious documents
- Spyware
- Email threats

Everything indicates that the industrial systems in the region are extremely vulnerable to phishing attacks.

Industrial organizations in the region should pay more attention to this threat. They must consider the use of automated anti-phishing tools and employee training. In the current situation, they should recognize the high risk of targeted attacks conducted directly against industrial network segments.

South Asia

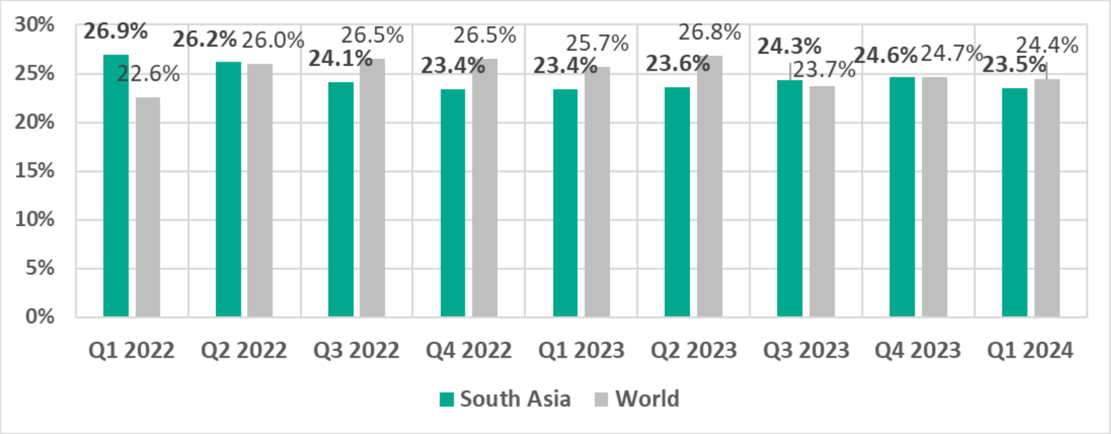
In comparison to other regions

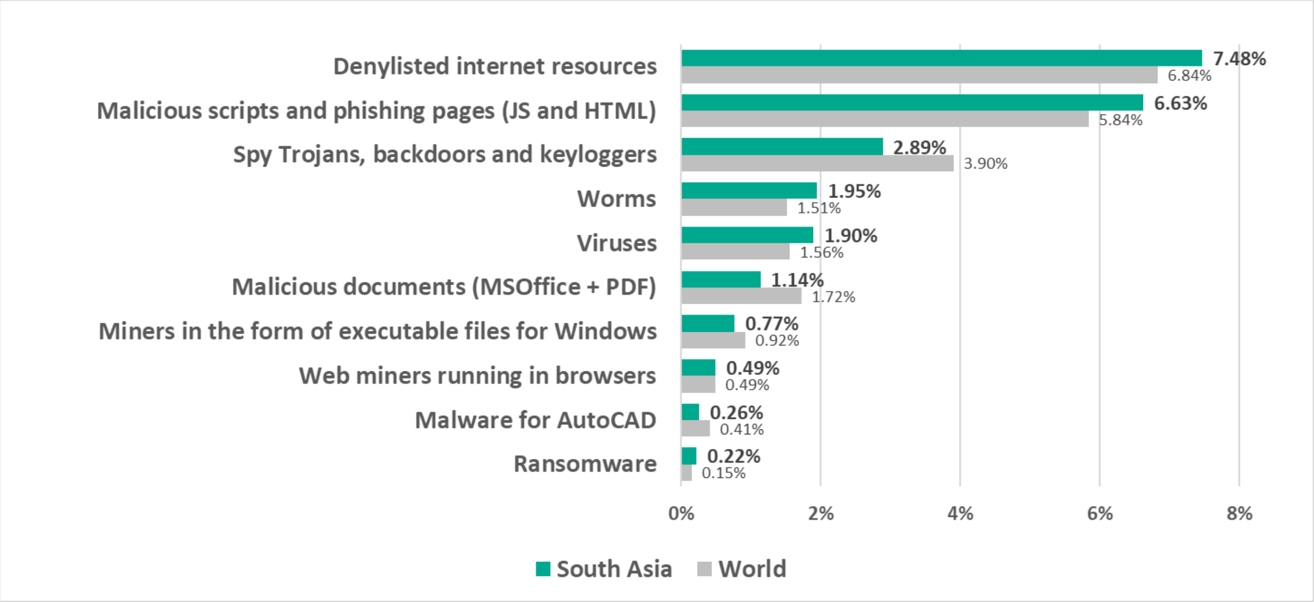
Eighth place in the regional ranking.

- **Second** by percentage of ICS computers on which **removable media** were blocked.
- **Third** by percentage of ICS computers on which **network folder threats** were blocked.
- **Third** by percentage of ICS computers on which **internet threats** were blocked.
- **Third** by percentage of ICS computers on which **denylisted internet resources** were blocked.
- **Third** by percentage of ICS computers on which **ransomware** was blocked.

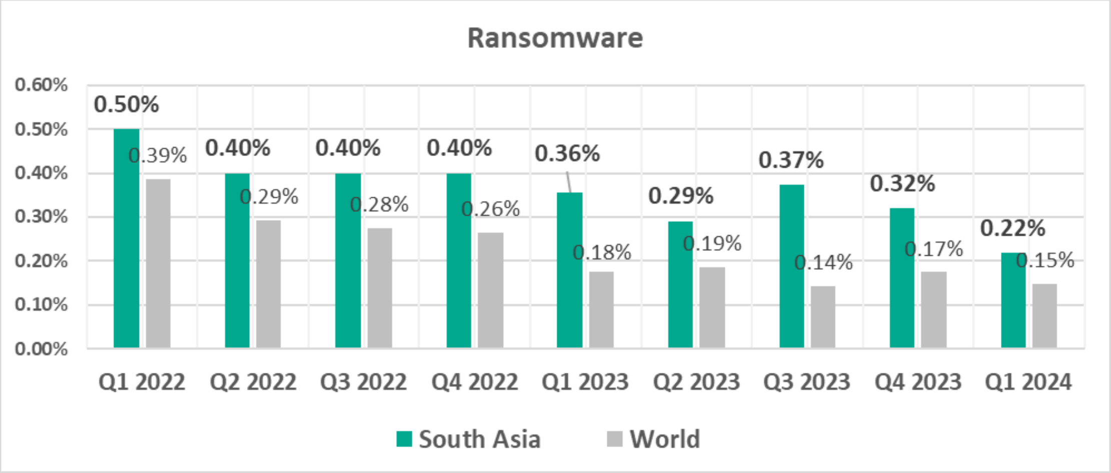
In comparison to the world

- Since Q3 2023, the percentage of ICS computers on which malicious objects were blocked in the region is close to the global average figures.

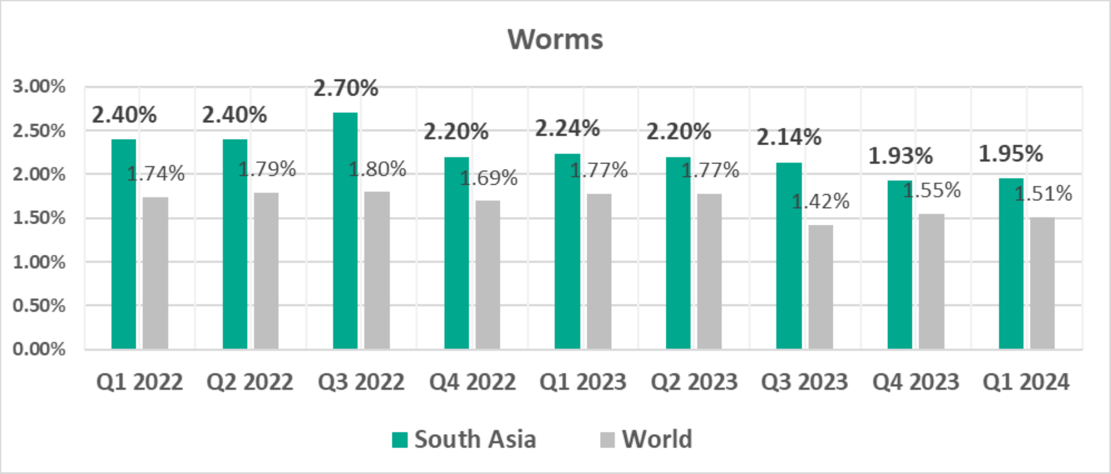




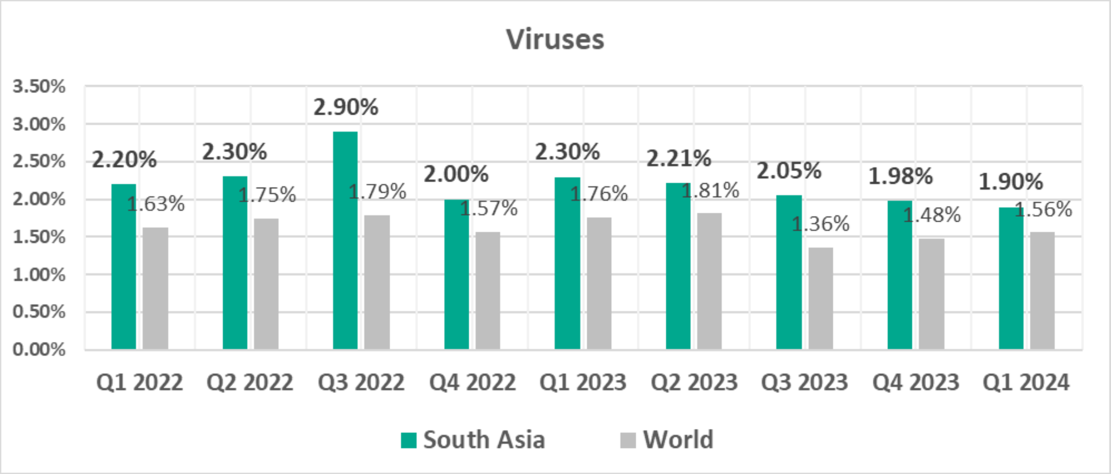
- Compared to the global average, the region has a noticeably higher percentage of ICS computers on which the following was blocked:
  - ➢ Ransomware, by 1.5 times



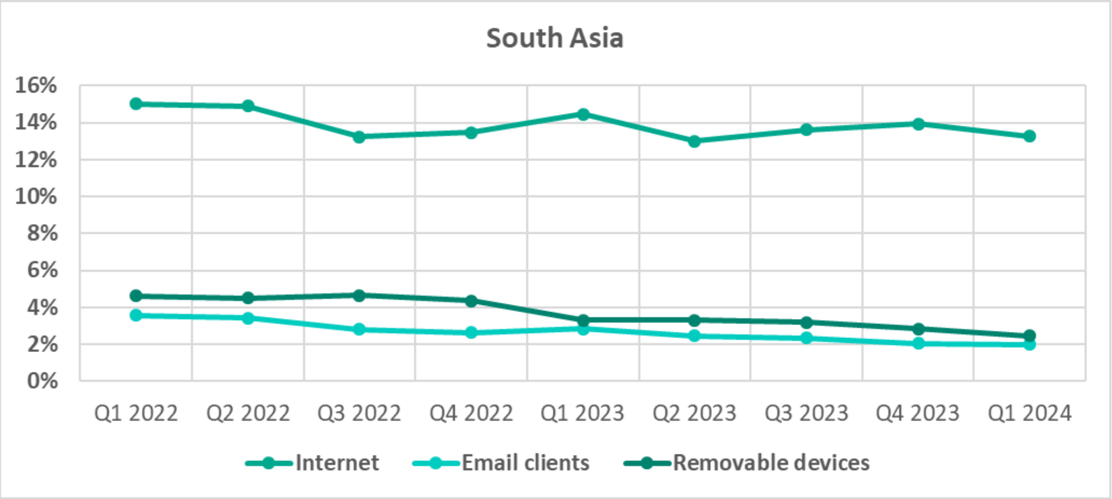
- Worms, by 1.3 times. **Worms were fourth** in the ranking of malware categories by percentage of ICS computers on which they were blocked (sixth globally).



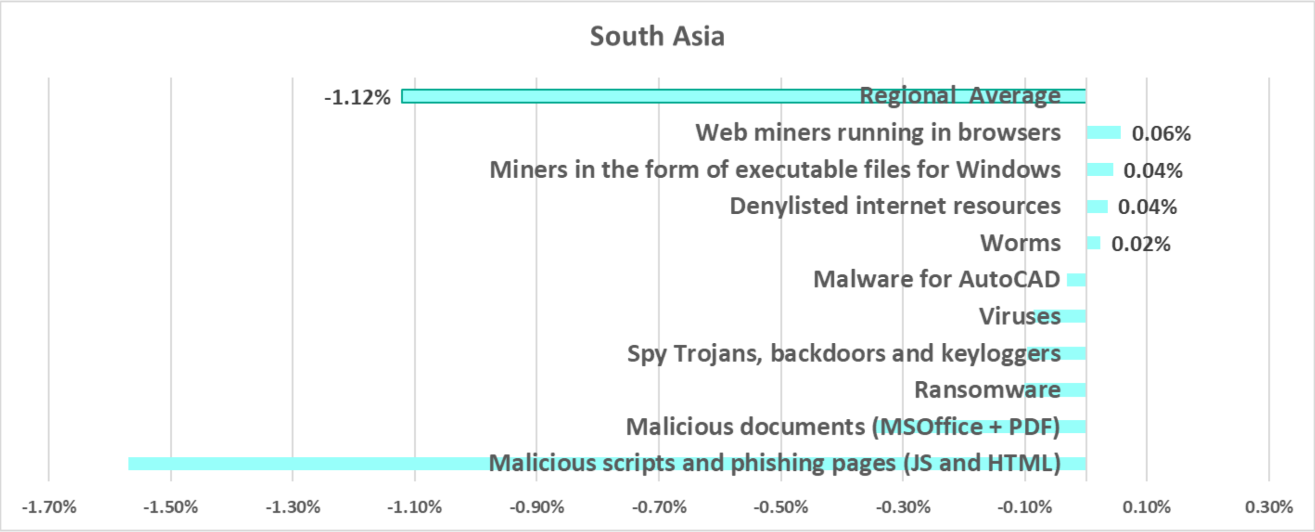
- Viruses, by 1.2 times



- **Removable drives** in South Asia occupy second place in the ranking of threat sources by percentage of ICS computers on which malicious objects from different sources were blocked. One of three regions in which the percentage of ICS computers on which threats were blocked when connecting removable media exceeded the percentage of ICS computers on which email threats were blocked.



Quarterly changes



Current threats

- Compromised and malicious internet resources
- Ransomware
- Worms
- Viruses
- Threats spread on removable media
- Network folder threats

The high percentage of computers that encountered threats spread through network folders and removable media and the high figures for self-propagating malware tell us that a significant portion of the industrial infrastructure in the region is not secured. Industrial organizations in the region should also focus more attention on teaching their employees safe cybersecurity behaviors.

Southern Europe

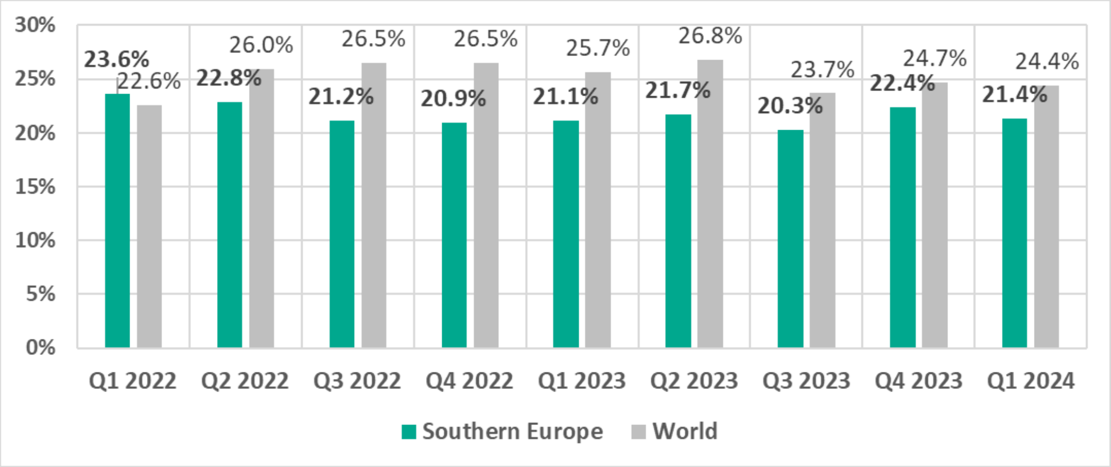
In comparison to other regions

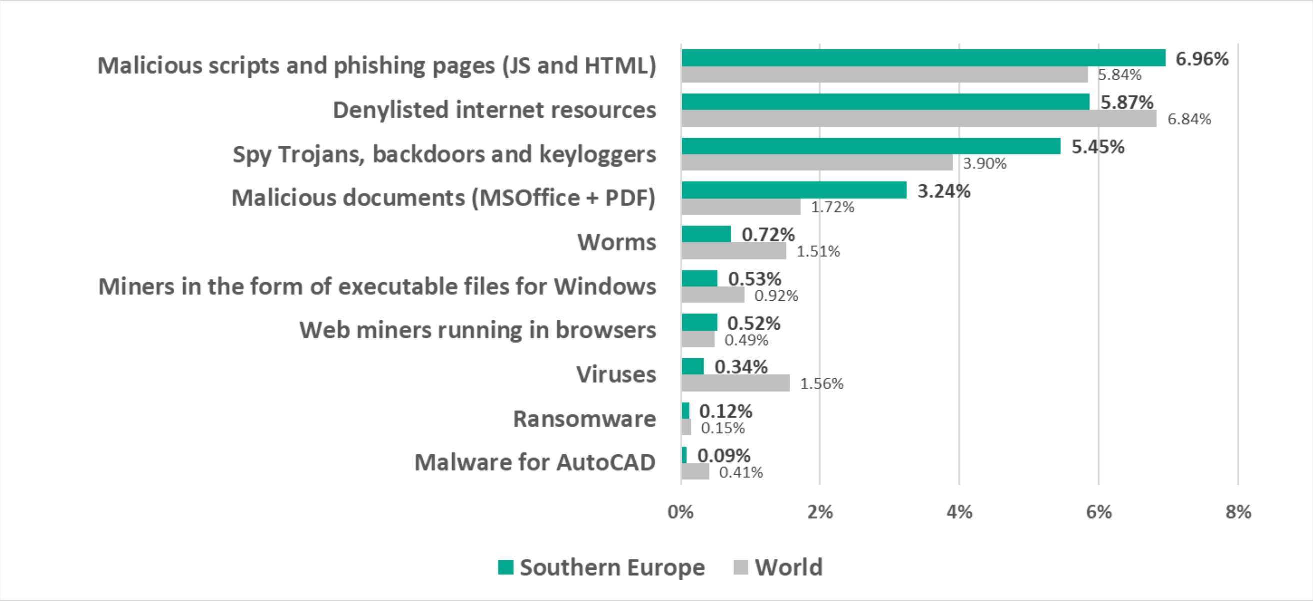
Ninth place in the regional ranking.

- **Leader** by percentage of ICS computers on which **malicious documents** were blocked.
- **Leader** by percentage of ICS computers on which **email threats** were blocked.
- **Second** among the regions by percentage of ICS computers on which **malicious scripts and phishing pages were blocked**.
- **Third** by percentage of ICS computers on which **spyware** was blocked.

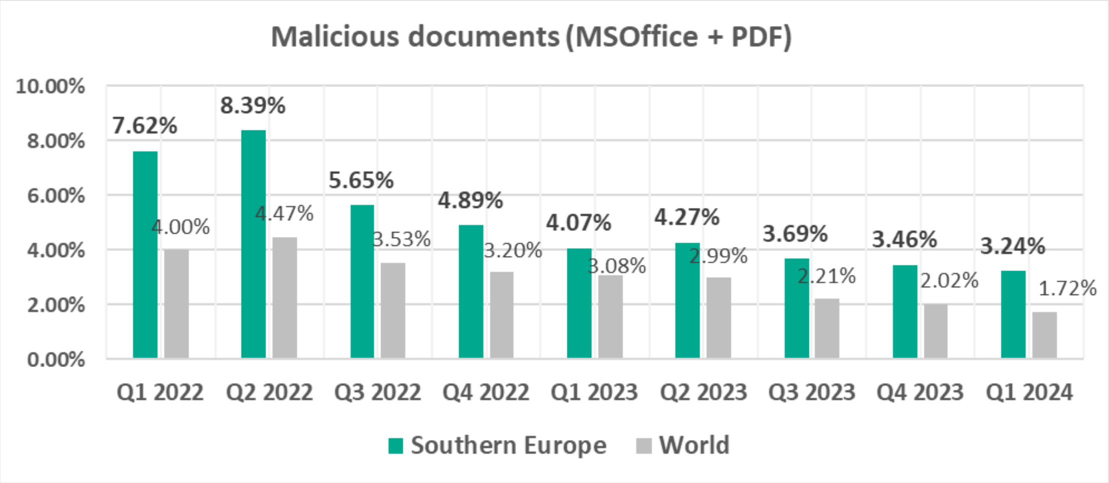
In comparison to the world

- In this region, the percentage of ICS computers on which malicious objects were blocked is less than the global average.

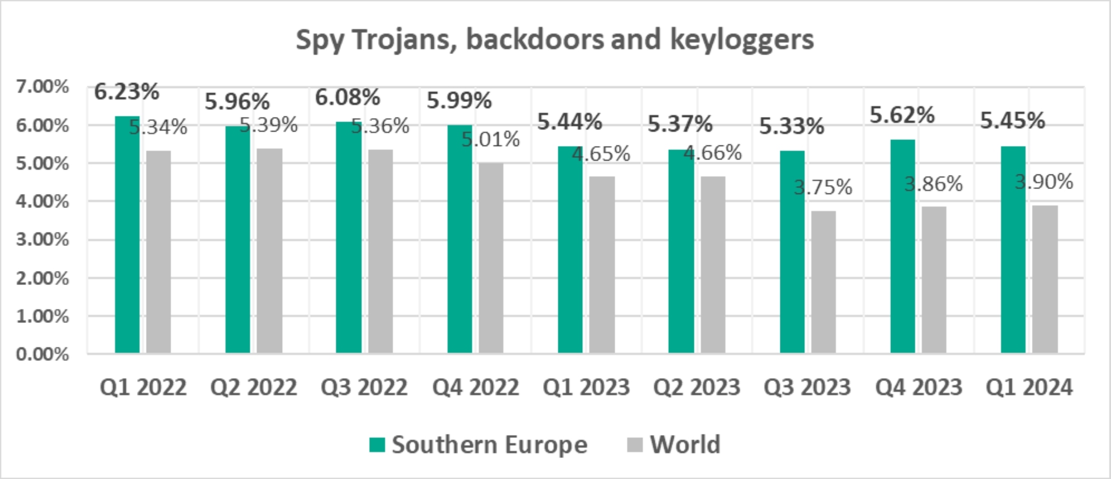




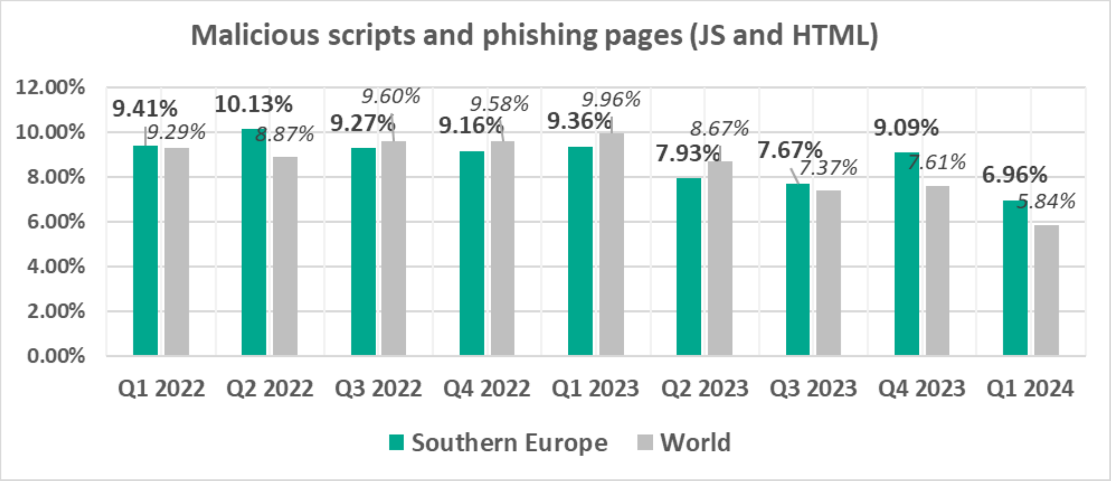
- Compared to the global average, the region has a higher percentage of ICS computers on which the following was blocked:
  - ➢ Malicious documents, by 1.9 times



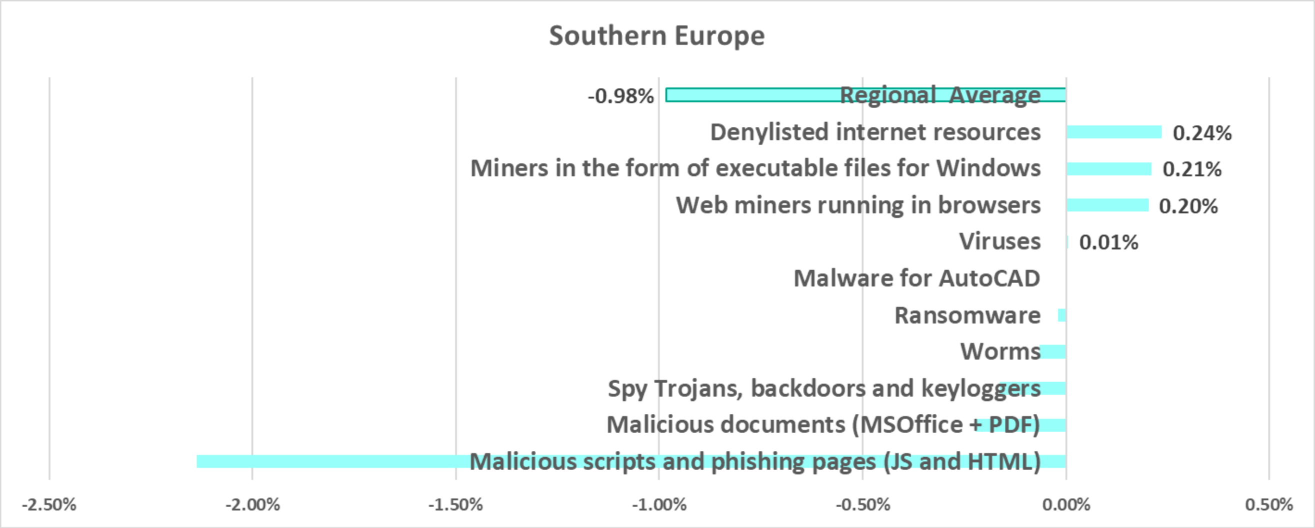
- Spyware, by 1.4 times



- Malicious scripts and phishing pages, by 1.2 times

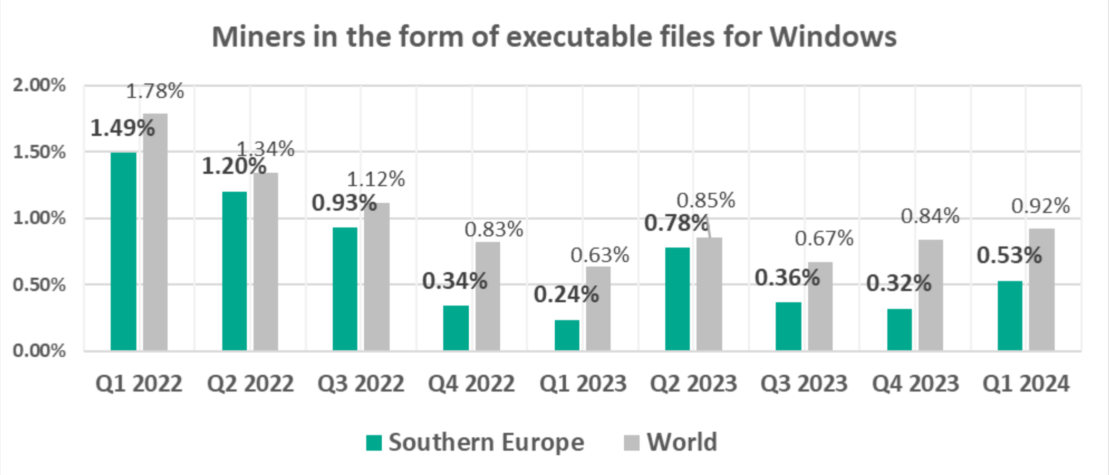


Quarterly changes

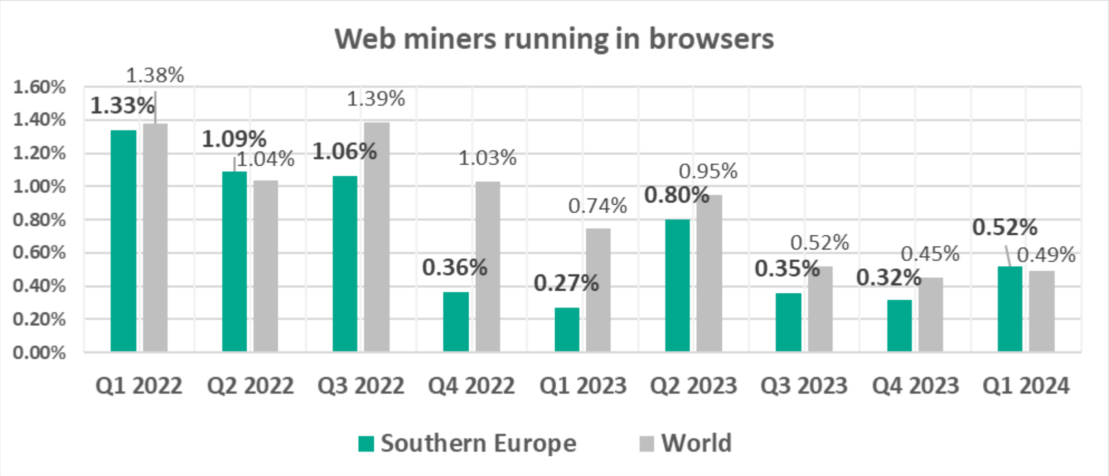


The largest quarterly increase was in the percentage of ICS computers on which covert crypto-mining malware was blocked:

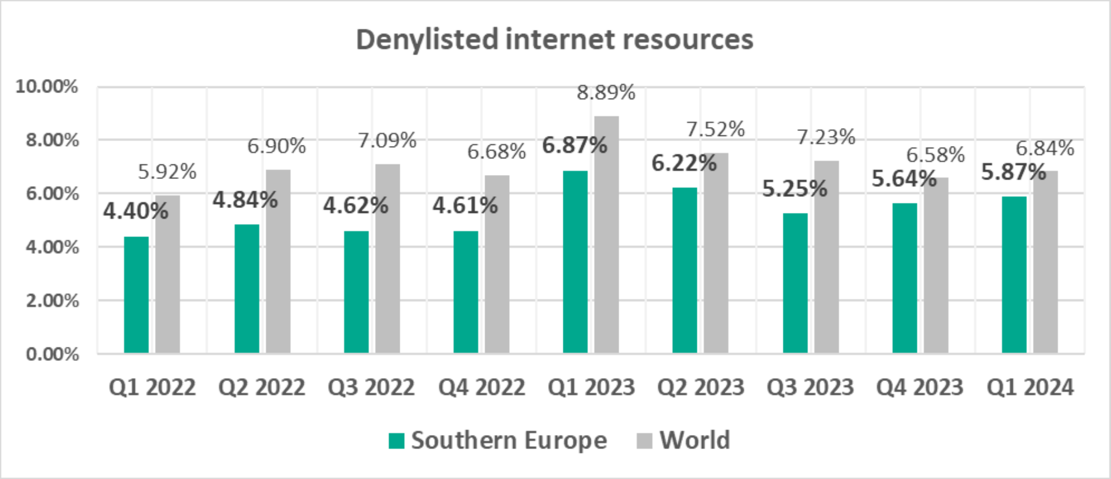
- Miners in the form of executable files for Windows, by 1.7 times



- Web miners, by 1.6 times. As a result, the percentage in the region exceeded the global figure.



- ➢ Percentage of ICS computers on which blocked internet resources from the denylist are slowly growing in Southern Europe for the second quarter in a row.



Current threats

- ➢ Malicious documents
- ➢ Spyware
- ➢ Malicious scripts and phishing pages
- ➢ Email threats

Everything indicates a high threat of phishing attacks on the industrial infrastructure in the region. Phishing is one of the preferred initial compromise methods for cybercriminals specializing in targeted attacks such as APT, ransomware attacks, BEC attacks, and hacktivist attacks.

East Asia

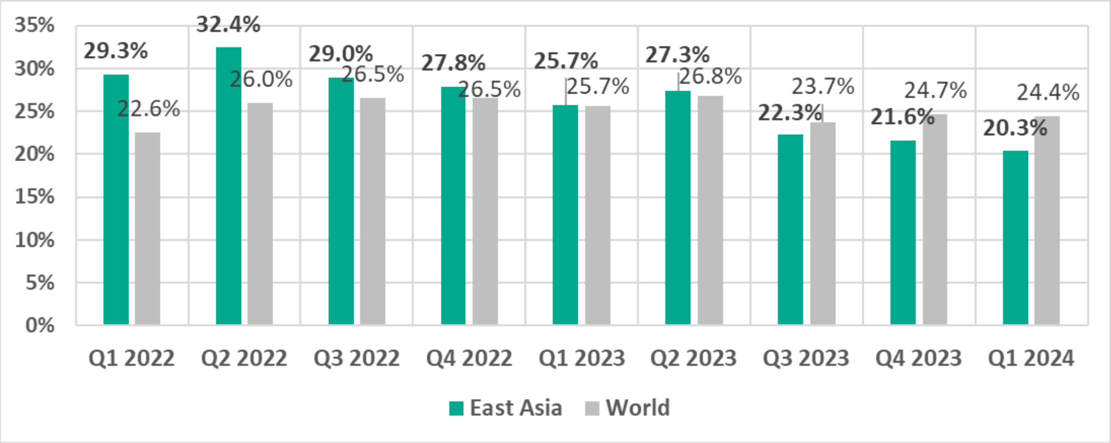
In comparison to other regions

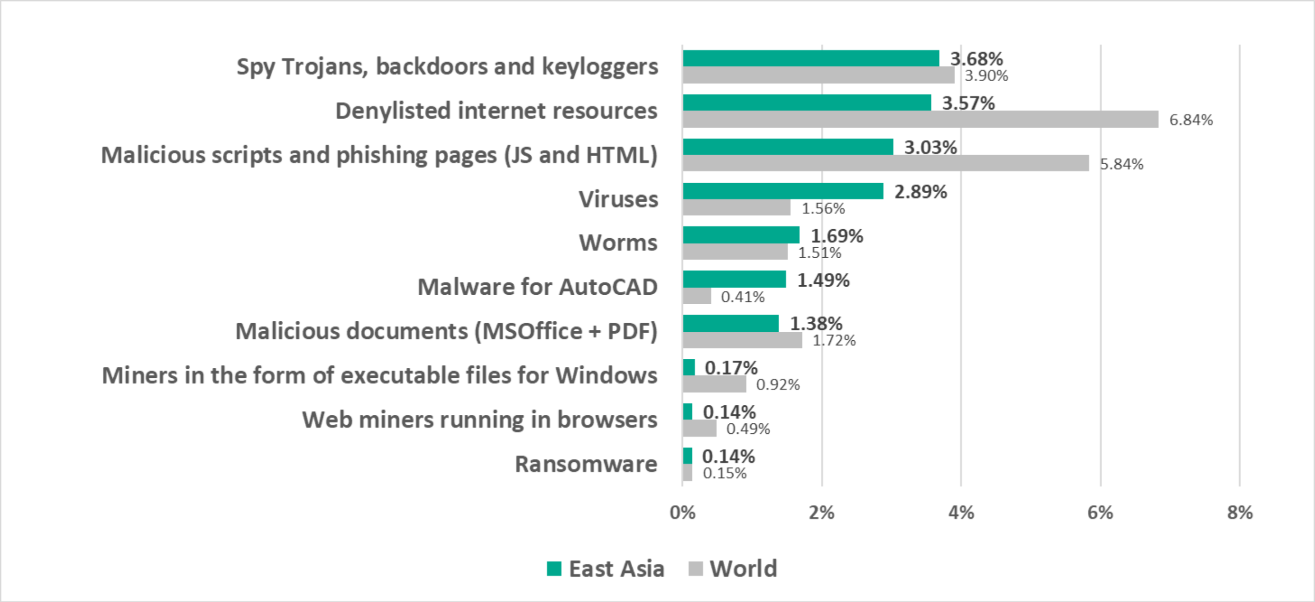
Tenth place in the regional ranking.

- **Second** by percentage of ICS computers on which **malware for AutoCAD** was blocked.
- **Third** by percentage of ICS computers on which **viruses** were blocked.
- **The only region in which spyware topped the malware category ranking** in terms of the percentage of ICS computers on which it was blocked.

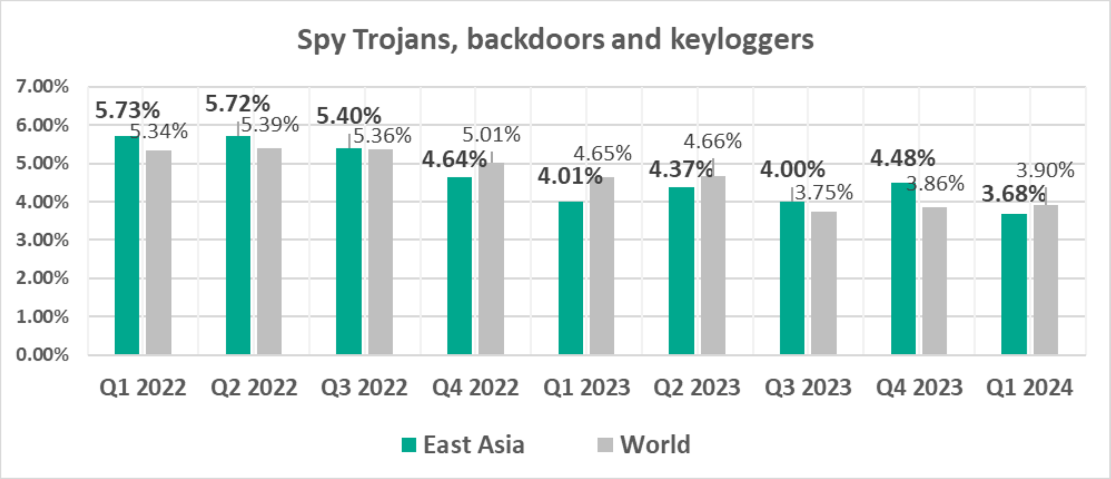
In comparison to the world

- Since Q3 2023, the percentage of ICS computers on which malicious objects were blocked in the region is lower than the corresponding global figure.



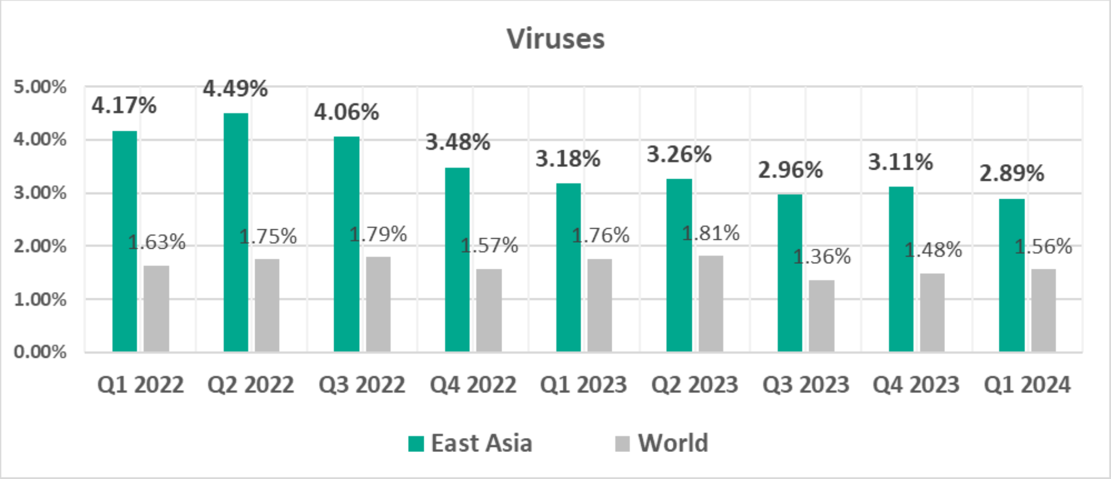


- **Spyware was first** in the ranking of malware categories by percentage of ICS computers on which it was blocked (third globally).

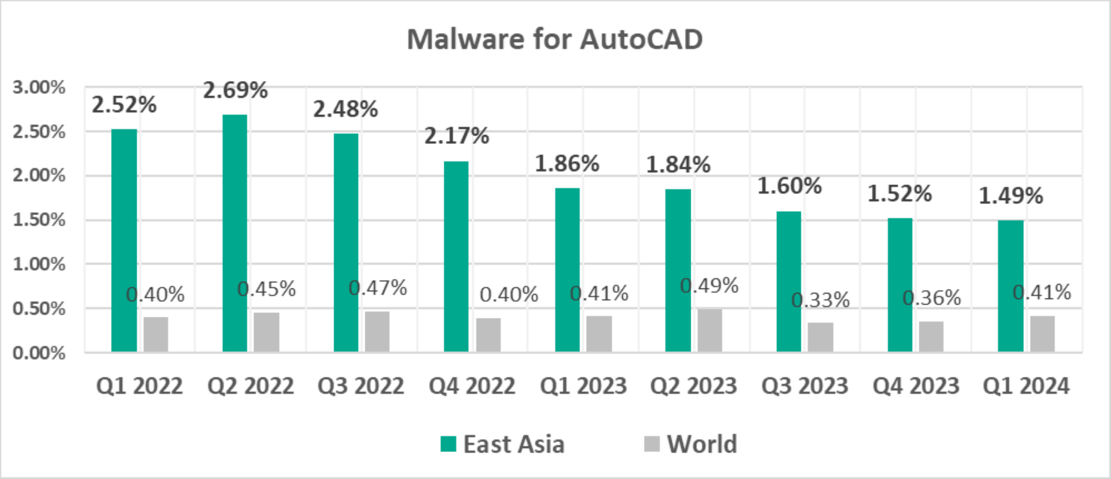


- Compared to the global average, the region has a noticeably higher percentage of ICS computers on which the following was blocked:

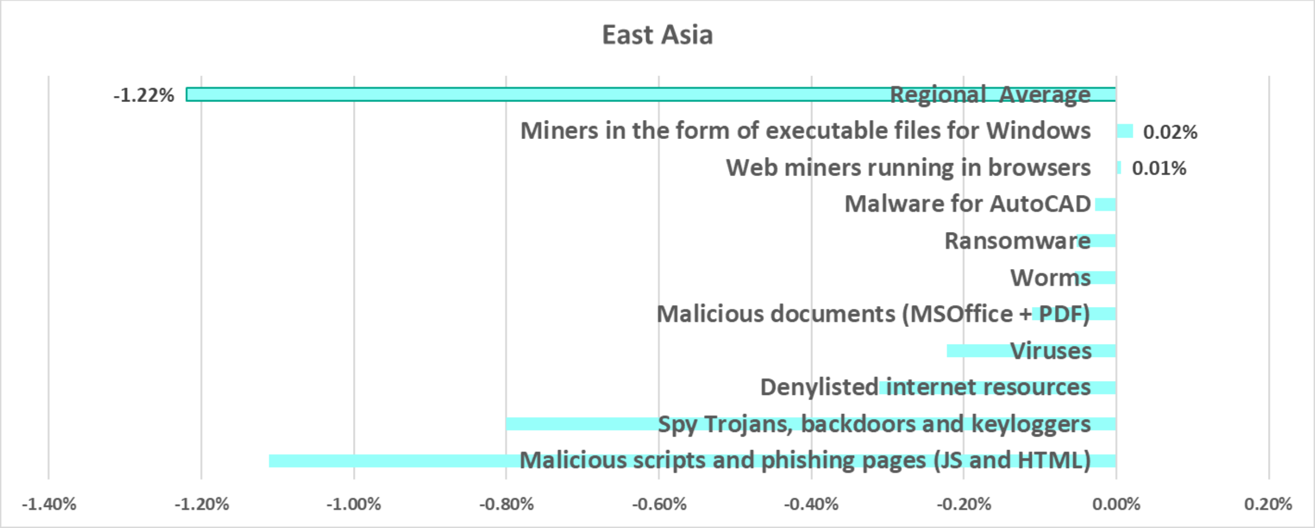
  ➢ Viruses, by 1.9 times



- AutoCAD malware, by 3.6 times



Quarterly changes



Current threats

- Spyware
- Viruses
- AutoCAD malware

It is likely that the active use of spyware by cybercriminals leads to a high percentage of compromised authentication data in industrial enterprise systems, which significantly increases the risks of subsequent targeted attacks.

Australia and New Zealand

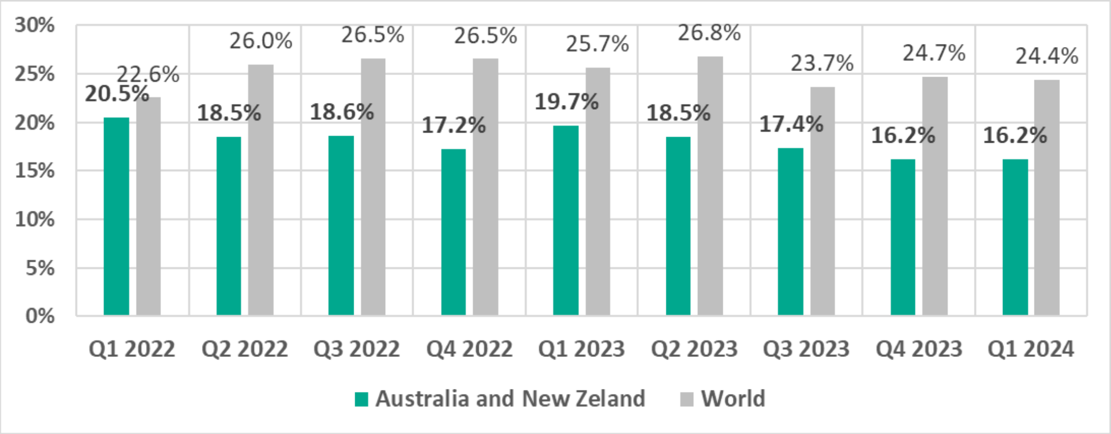
In comparison to other regions

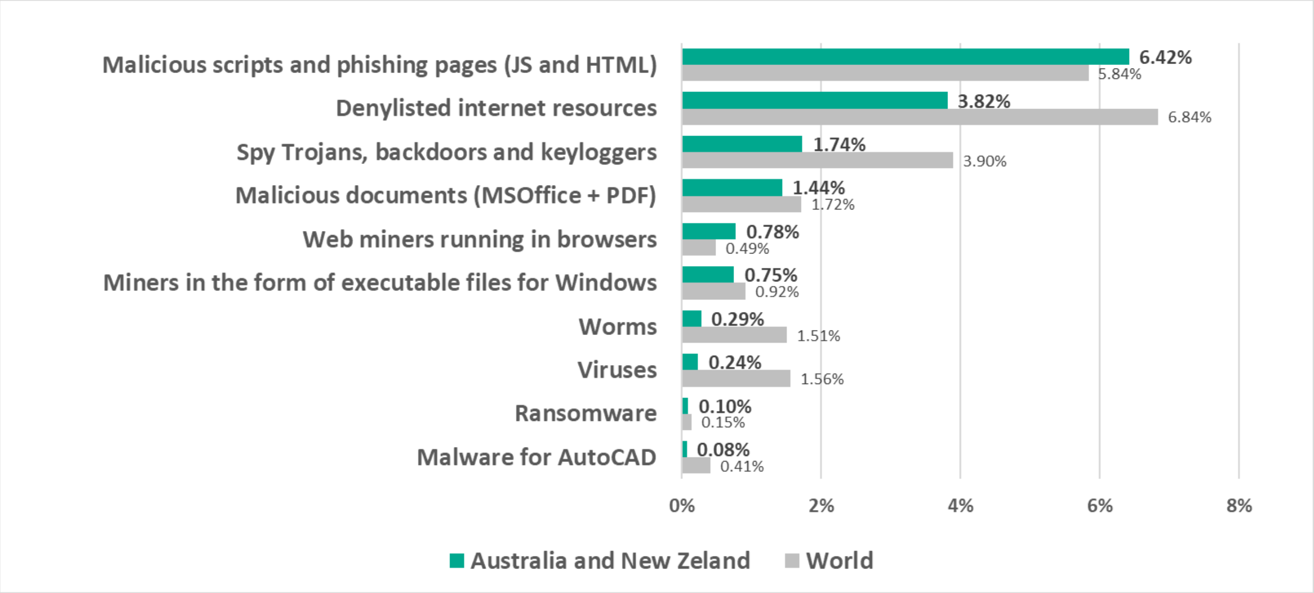
Eleventh place in the regional ranking.

- Third by percentage of ICS computers on which **web miners** were blocked.
- One of the three regions where **web miners were fifth in the ranking** of malware categories by percentage of ICS computers on which they were blocked (miners rank lower in all other regions, eighth globally).
- The percentage of ICS computers on which web miners were blocked in Australia and New Zealand grew by 0.43 pp, which was the maximum among regions.
- The percentage of ICS computers on which miners in the form of Windows executable files were blocked in Australia and New Zealand grew by 0.44 pp, which was the maximum among regions.

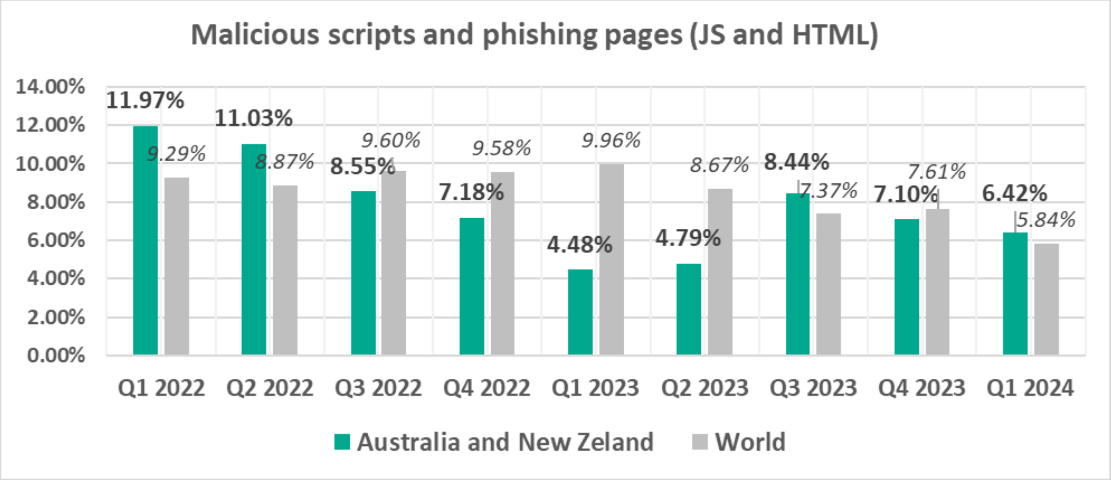
In comparison to the world

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

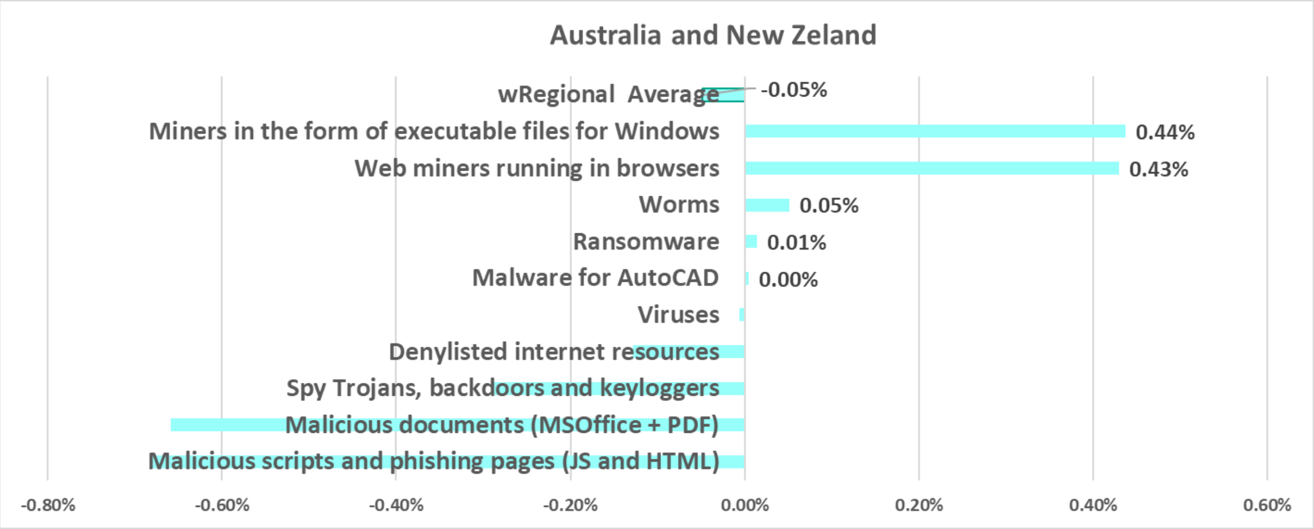




- Compared to the global average, the region has a higher percentage of ICS computers on which the following was blocked:
  - Web miners, by 1.6 times. Web miners were fifth in the ranking of malware categories by percentage of ICS computers on which they were blocked (eighth globally).
  - Malicious scripts and phishing pages

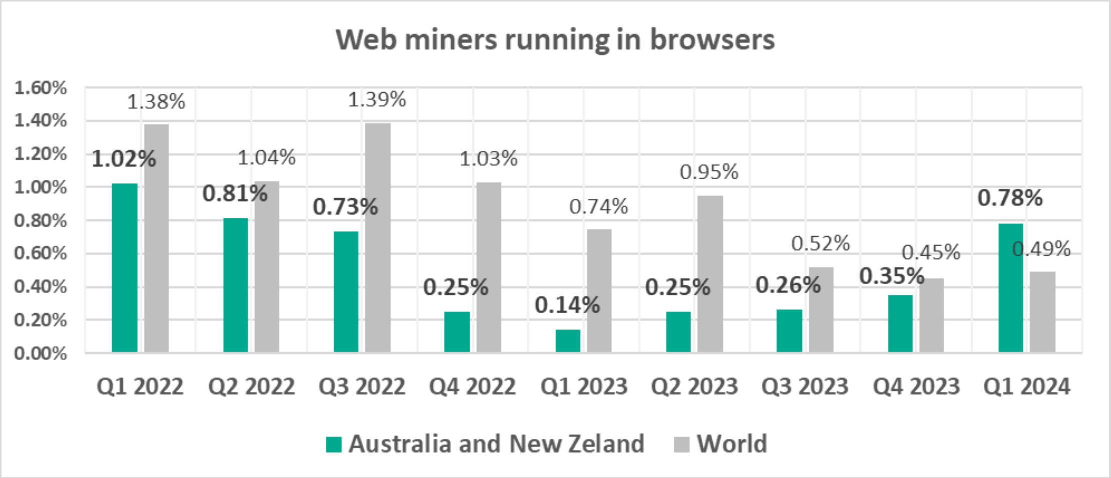


Quarterly changes

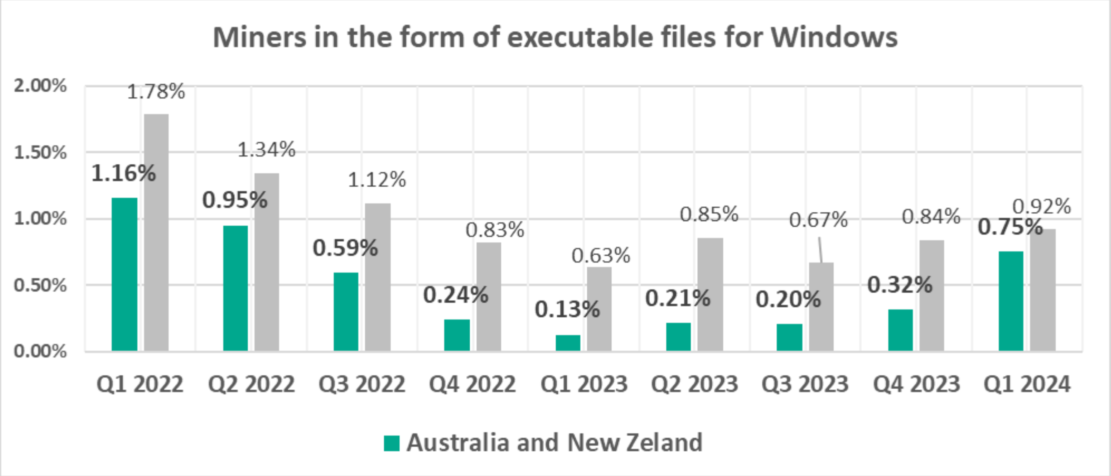


The largest quarterly increase was in the percentage of ICS computers on which the following was blocked:

- Web miners, by 2.2 times. As a result, the percentage in the region exceeded the global figure.

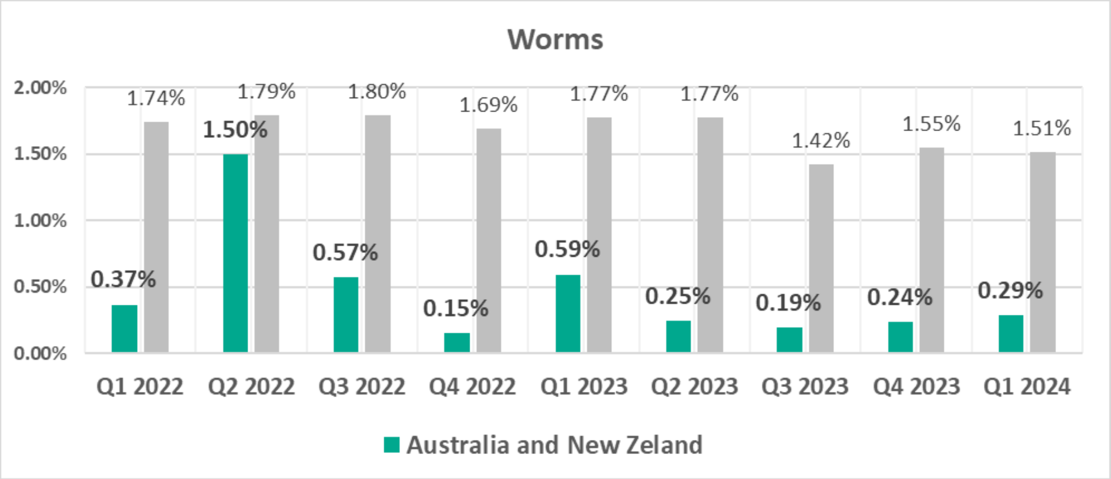


- ➢ Miners in the form of executable files for Windows, by 2.4 times



The percentage of ICS computers on which malicious miners were blocked is growing for both categories since Q2 2023.

- ➢ Worms, by 1.2 times. The percentage for this category is growing for the second quarter in a row.



Current threats

- ➢ Web miners
- ➢ Miners in the form of executable files for Windows
- ➢ Malicious scripts and phishing pages

US and Canada

In comparison to other regions

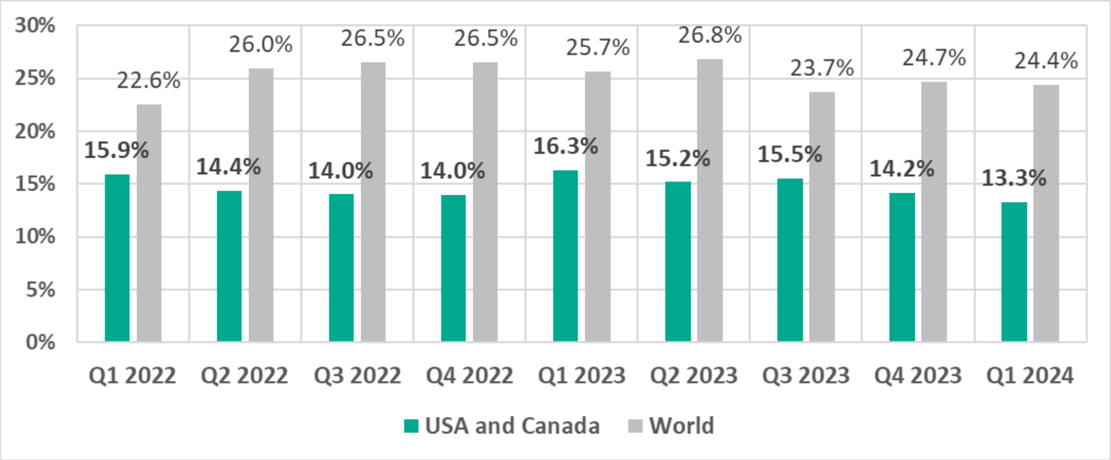
Twelfth place in the regional ranking.

One of three safest regions with the lowest percentage of ICS computers on which malicious objects were blocked.

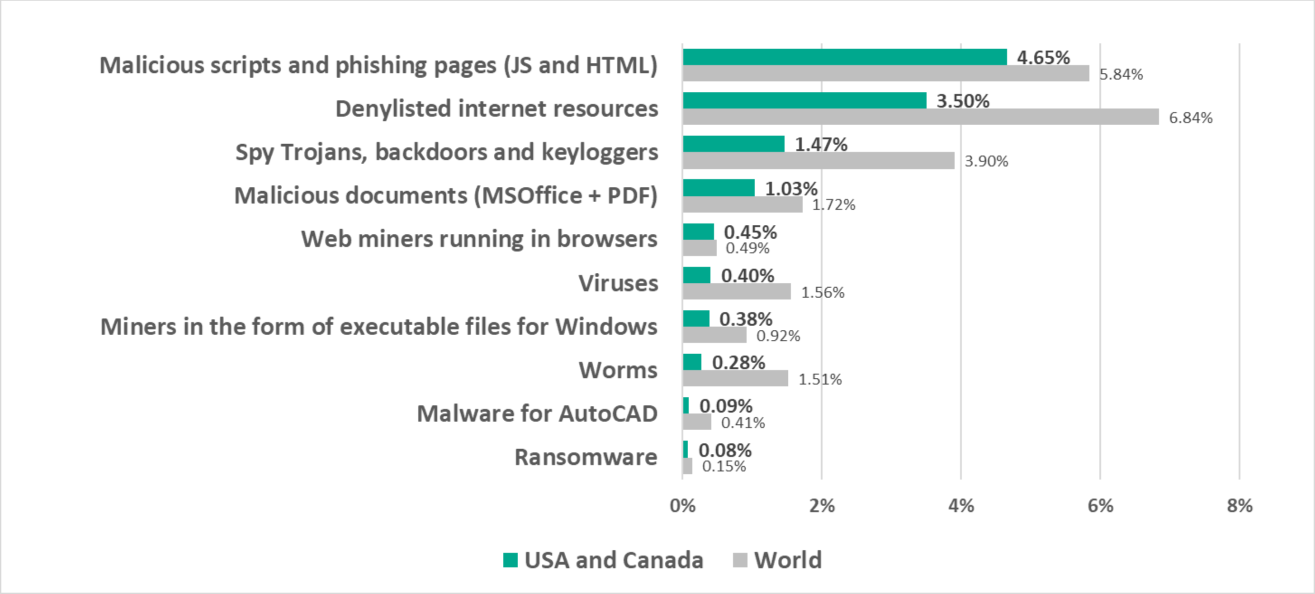
- One of the three regions where **web miners were fifth in the ranking** of malware categories by percentage of ICS computers on which they were blocked (miners rank lower in all other regions, eighth globally).

In comparison to the world

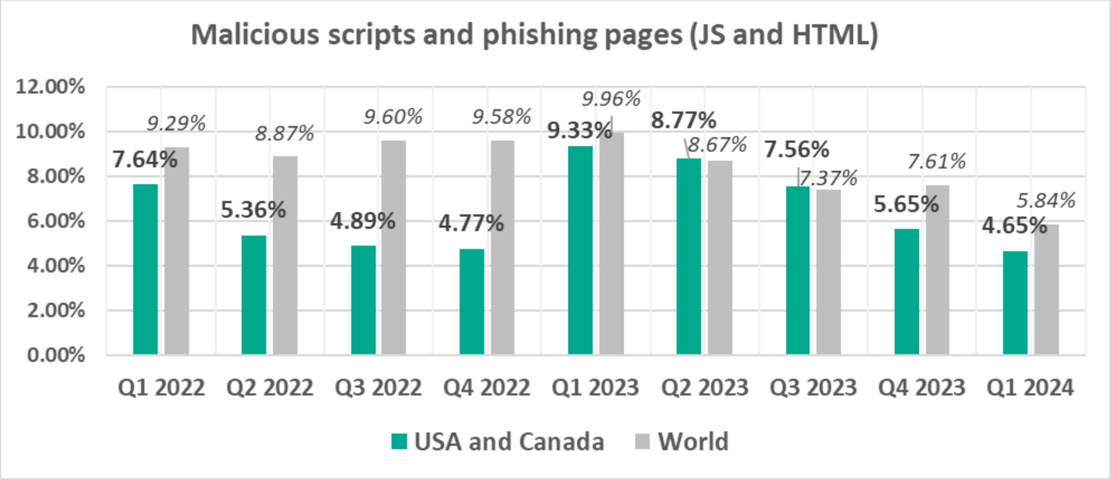
- The percentage of ICS computers on which malicious objects were blocked in the region is noticeably less than the corresponding global figure.



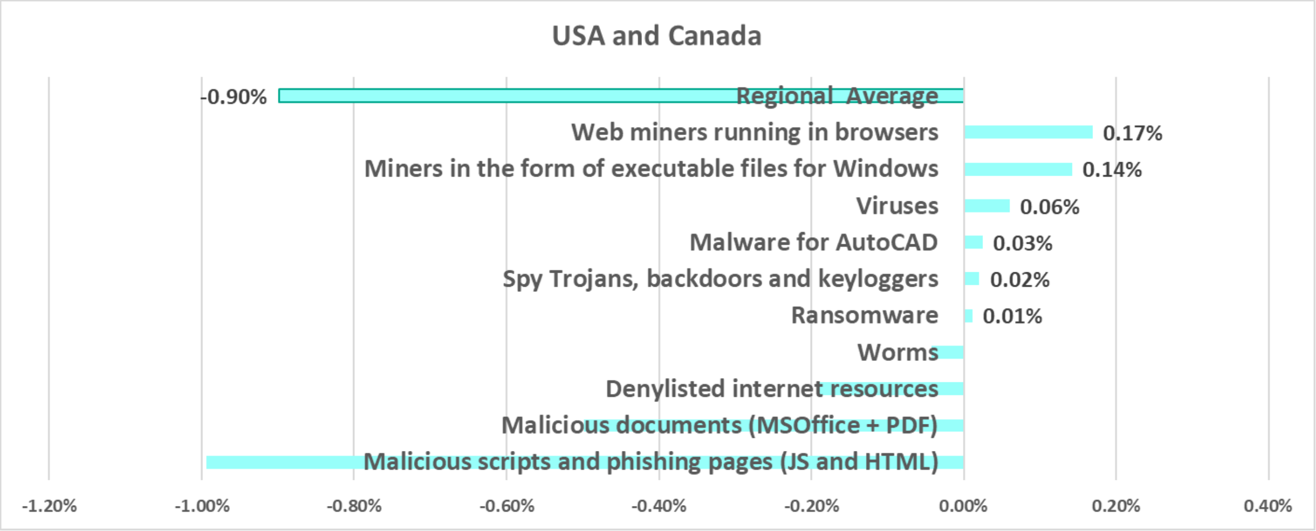
- The percentage of ICS computers on which malicious objects from various categories were blocked in the region is less than the global average for all categories.



- **Web miners were fifth** in the ranking of malware categories by percentage of ICS computers on which they were blocked (eighth globally).
- Since 2023, the percentage of ICS computers on which malicious scripts and phishing pages were blocked in the region is close to the global average.

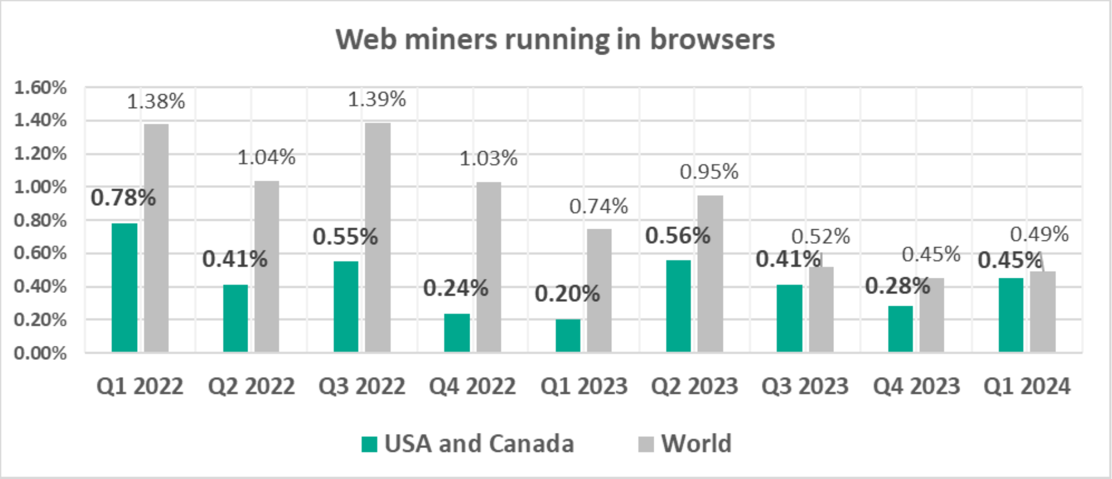


Quarterly changes

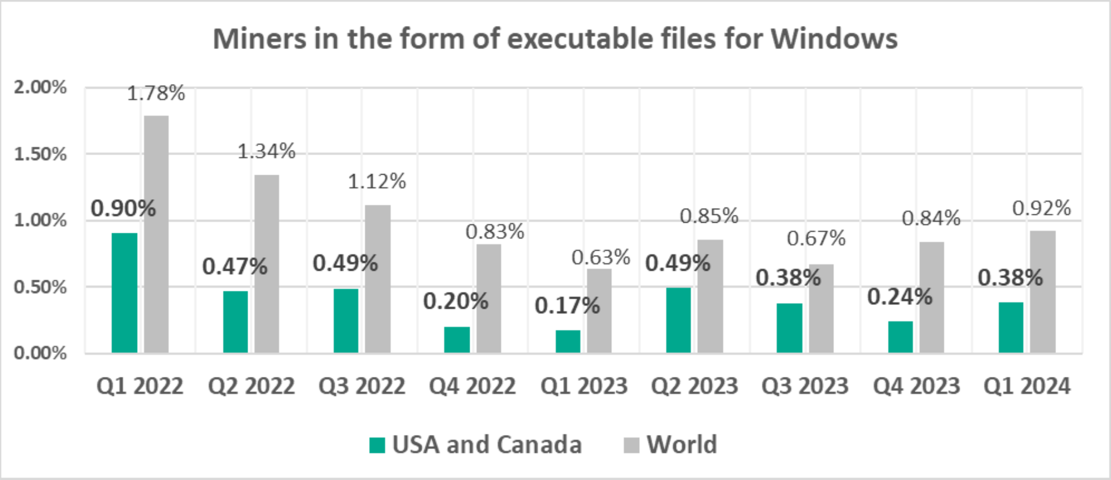


The largest quarterly increase was in the percentage of ICS computers on which the following was blocked:

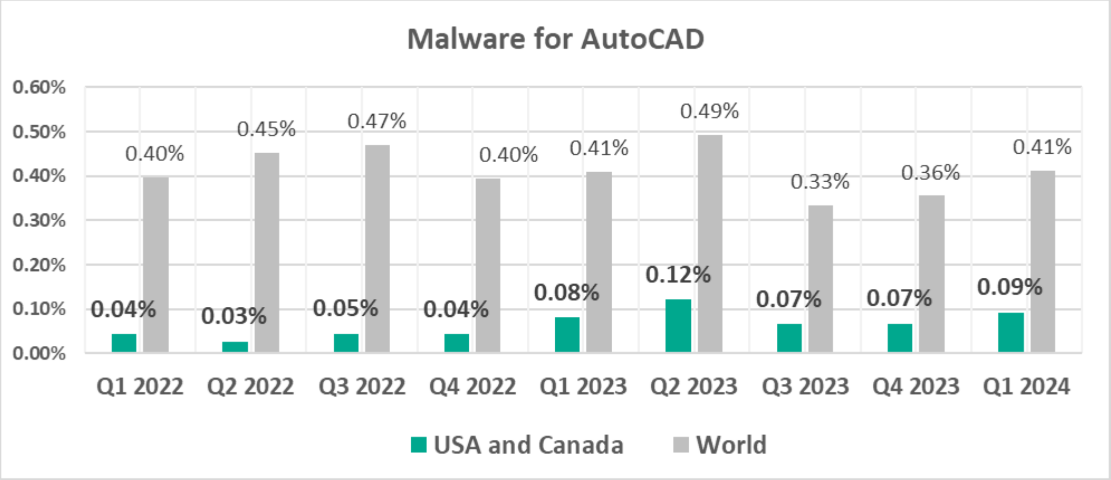
- Web miners, by 1.6 times. As a result, the percentage for web miners in the region was close to the global figure.



- Miners in the form of executable files for Windows, by 1.6 times



- AutoCAD malware – by 1.4 times



Current threats

- Malicious scripts and phishing pages

Q1 2024 saw an increase in the percentage of ICS computers on which the following threats were blocked:

- Web miners
- Miners in the form of executable files for Windows
- AutoCAD malware

Based on the combination of indicators, the region is safe overall.

Western Europe

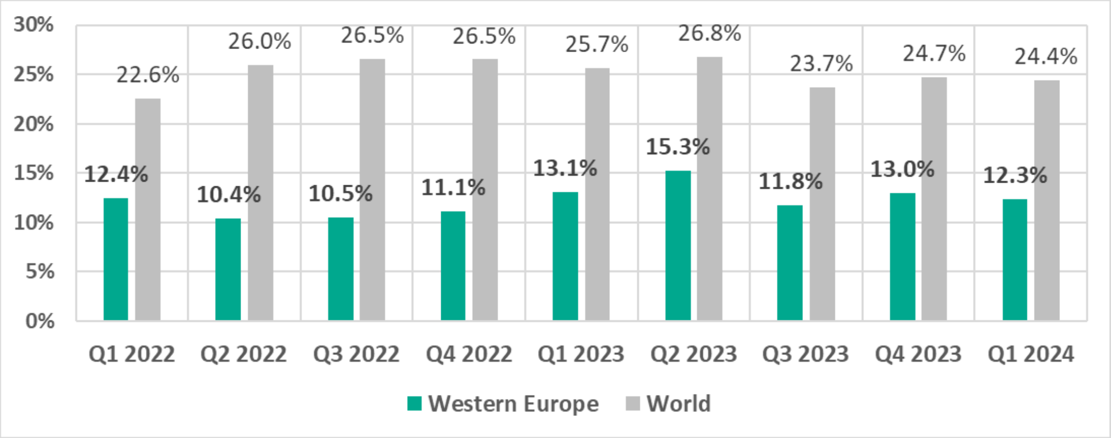
In comparison to other regions

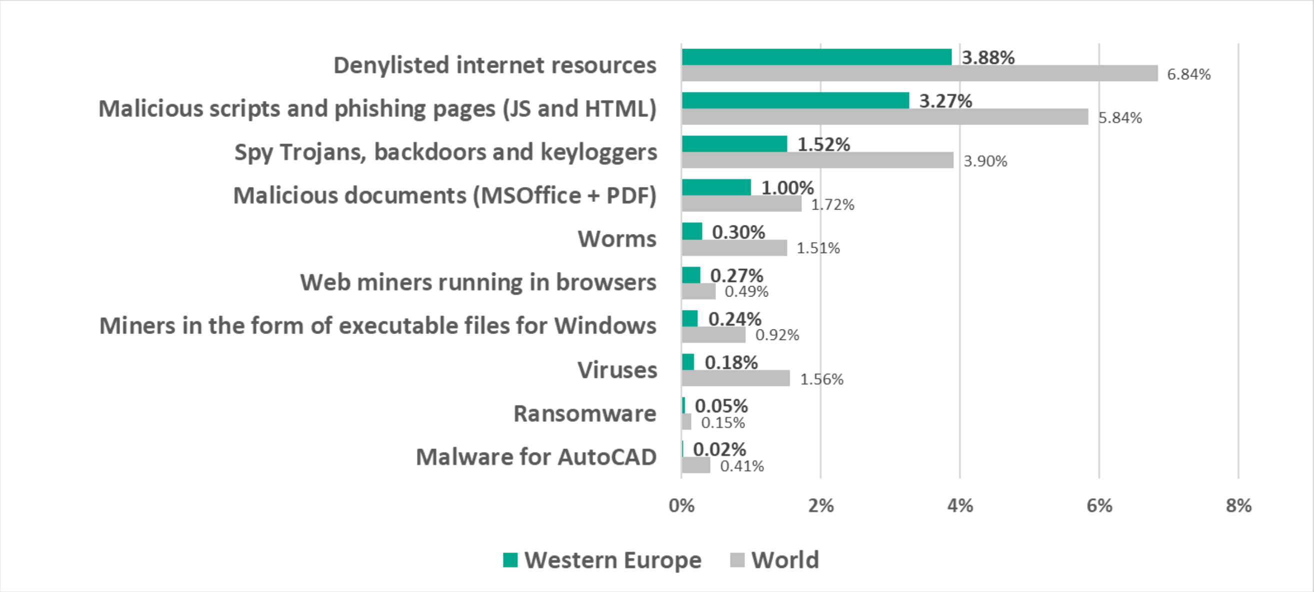
Thirteenth place in the regional ranking.

One of three safest regions with the lowest percentage of ICS computers on which malicious objects were blocked.

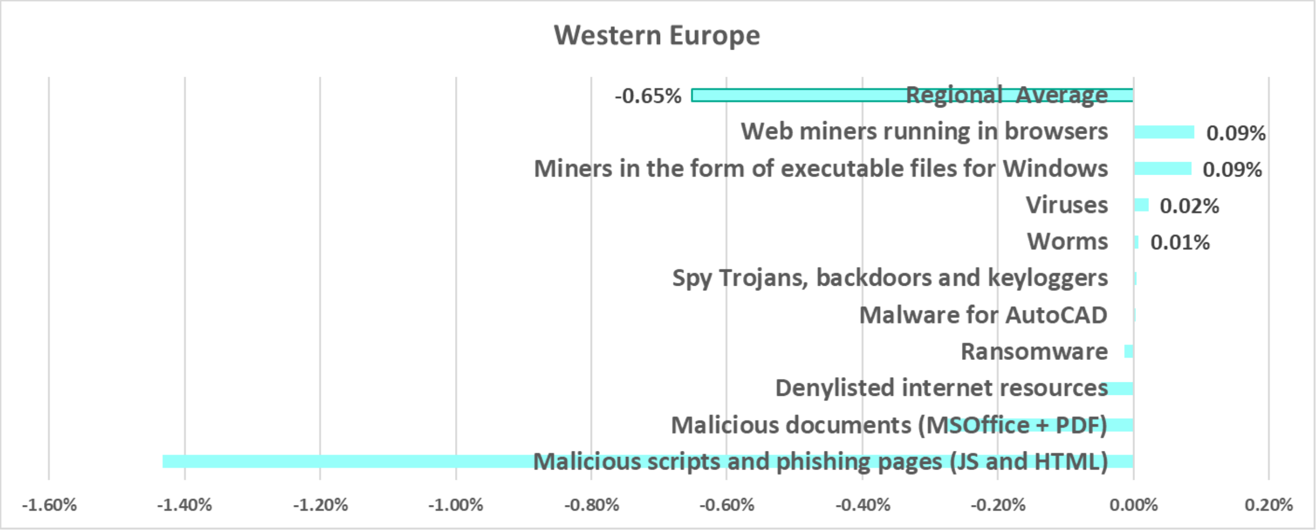
In comparison to the world

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



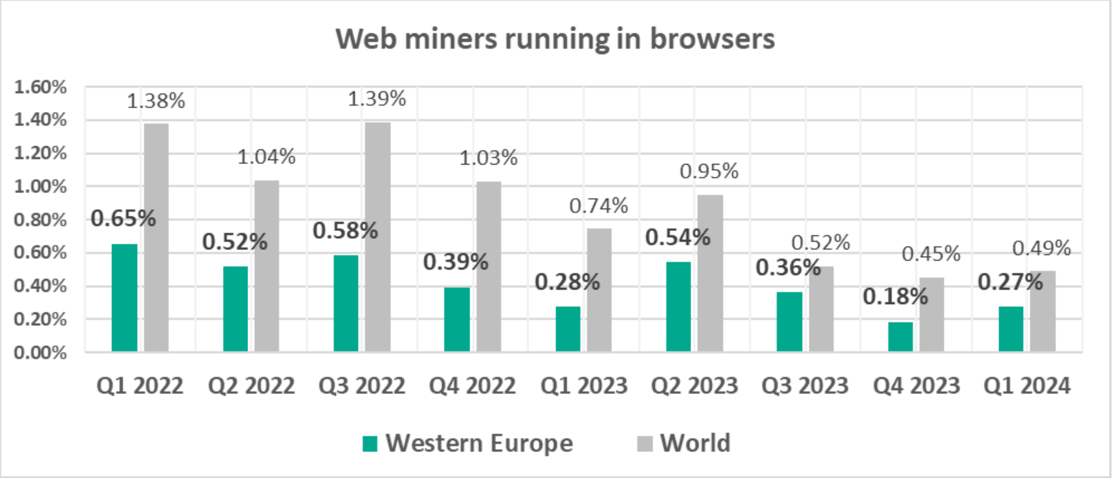


Quarterly changes

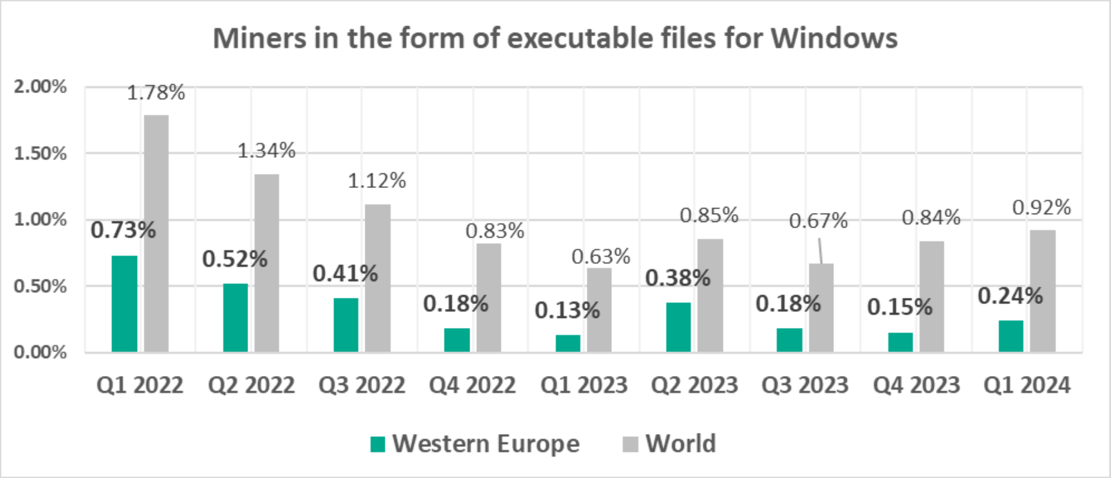


The largest quarterly increase was in the percentage of ICS computers on which the following was blocked:

- Web miners, by 1.5 times



- Miners in the form of executable files for Windows, by 1.5 times



Current threats

Q1 2024 saw an increase in the percentage of ICS computers on which the following threats were blocked:

- Miners in the form of executable files for Windows
- Web miners

The region is safe overall.

Northern Europe

In comparison to other regions

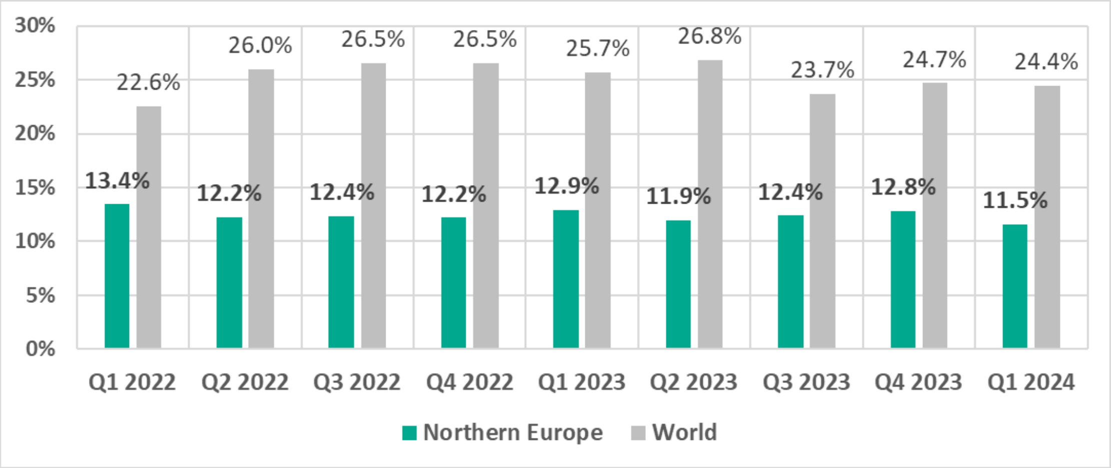
Fourteenth place in the regional ranking.

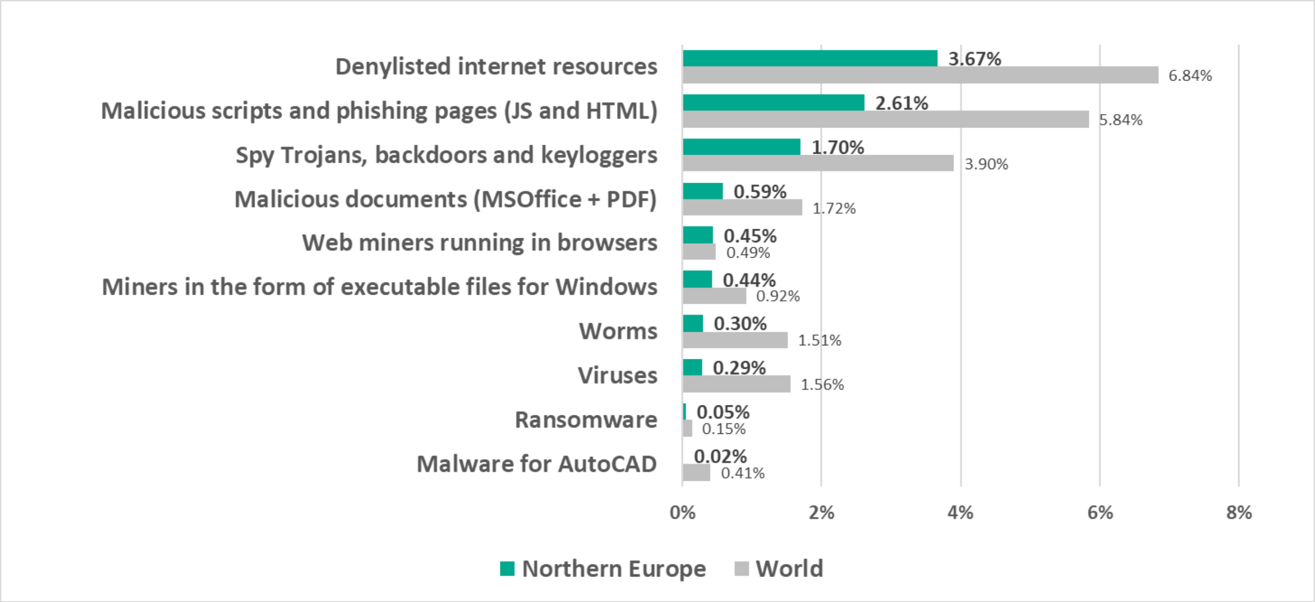
Traditionally the region has the lowest percentage of ICS computers on which malicious objects were blocked.

- One of three regions where **web miners were fifth** in the ranking of malware categories by percentage of ICS computers on which they were blocked (eighth globally).

In comparison to the world

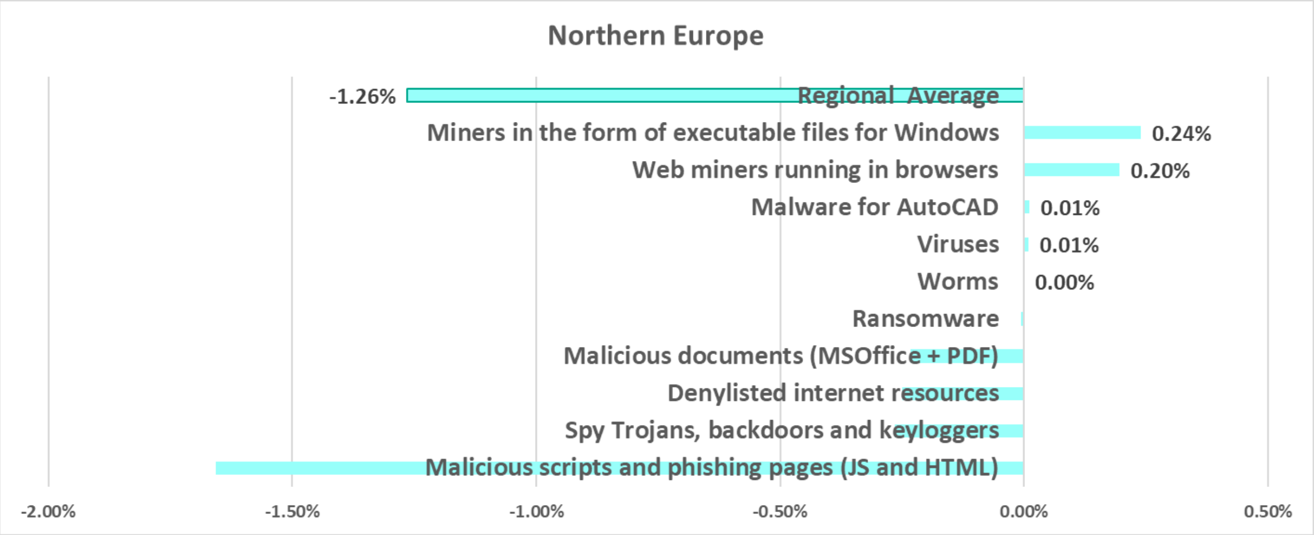
- The percentage of ICS computers on which malicious objects were blocked in the region is noticeably less than the corresponding global figure.





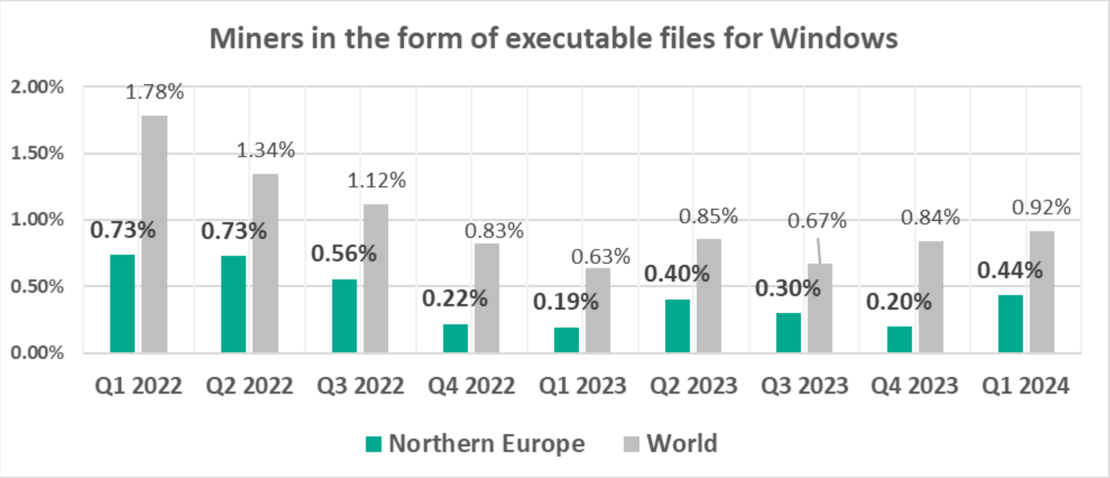
- **Web miners were fifth** in the ranking of malware categories by percentage of ICS computers on which they were blocked (eighth globally).

Quarterly changes

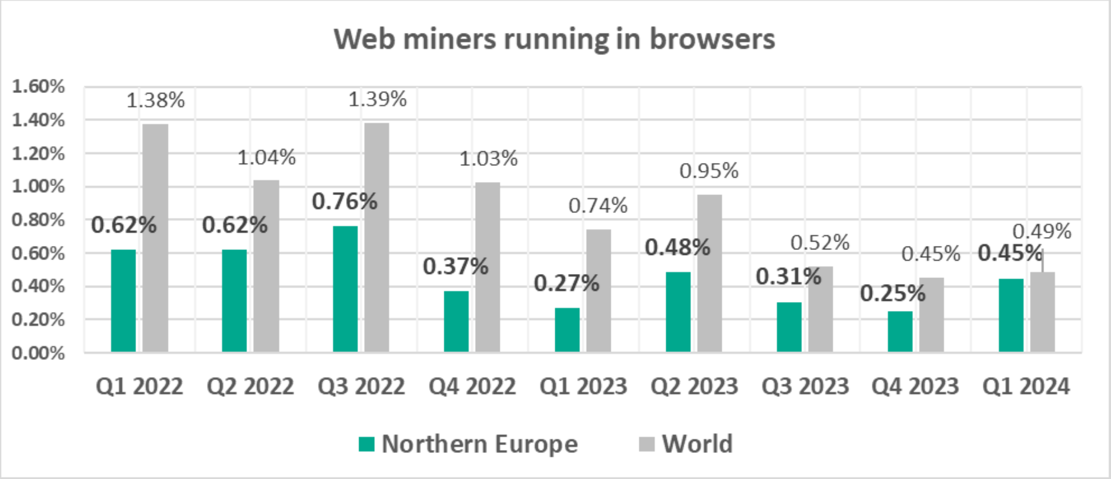


The largest quarterly increase was in the percentage of ICS computers on which the following was blocked:

- Miners in the form of executable files for Windows, by 2.2 times. Q1 percentage is the highest since the end of 2022.



- Web miners, by 1.8 times. As a result, the percentage for web miners in the region was close to the global figure.



Current threats

Region with the lowest percentage of attacked ICS computers.

Q1 2024 saw an increase in the percentage of ICS computers on which the following threats were blocked:

- Miners in the form of executable files for Windows
- Web miners

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