

Threat landscape for industrial automation systems

Regions, Q3 2024

Q3 overview	3
Percentage of ICS computers	3
Malicious object categories.....	5
Regions. Special considerations	21
Africa.....	22
South-East Asia	33
Middle East.....	43
Central Asia.....	54
Latin America	63
South Asia	73
Eastern Europe	83
East Asia	94
Southern Europe.....	105
Russia	114
Australia and New Zealand.....	122
Western Europe	131
USA and Canada.....	138
Northern Europe	145
Methodology used to prepare statistics	153

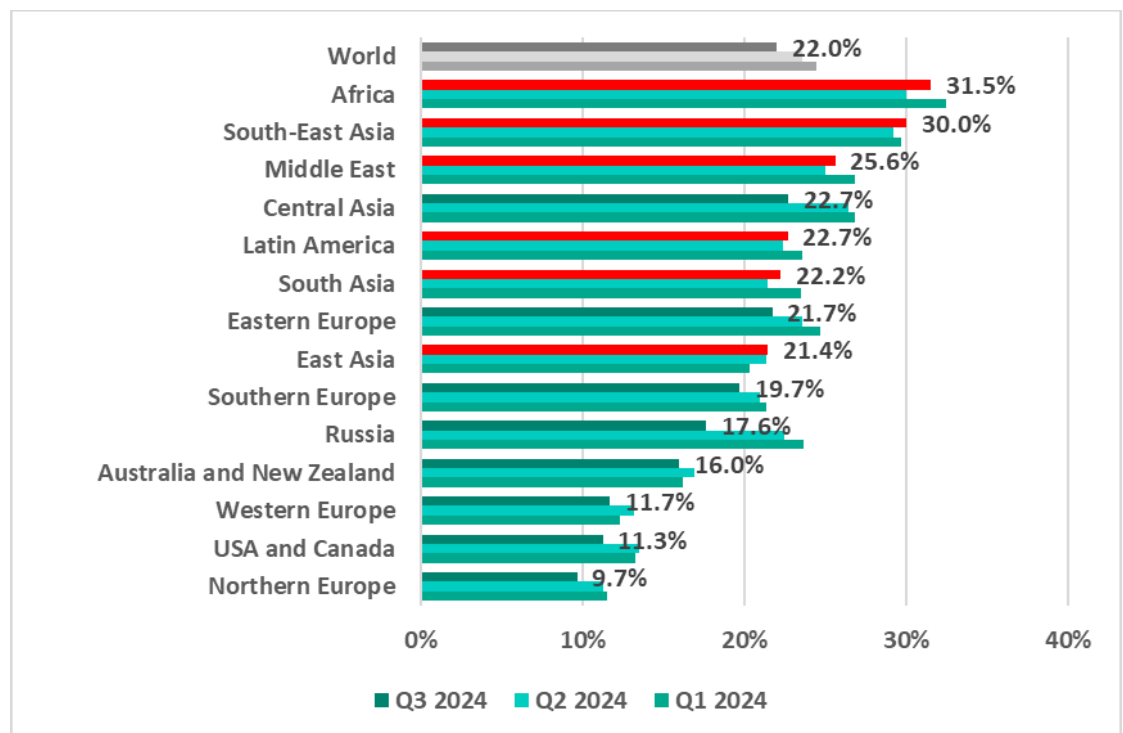
Q3 overview

Percentage of ICS computers

In the third quarter of 2024, the global percentage of ICS computers on which malicious objects were blocked decreased by 1.5 pp from the previous quarter to 22%.

Regionally¹, the percentage of ICS computers that blocked malicious objects during the quarter ranged from 9.7% in Northern Europe to 31.5% in Africa.

Regions ranked by percentage of ICS computers on which malicious objects were blocked, Q3 2024



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

Over 25%

- Africa – 31.5%
- South-East Asia – 30%
- Middle East – 25.6%

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.

¹ The report takes into account statistics for the USA received before September 29, 2024.

20–25%

- Central Asia – 22.7%
- Latin America – 22.7%
- South Asia – 22.2%
- Eastern Europe – 21.7%
- East Asia – 21.4%

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

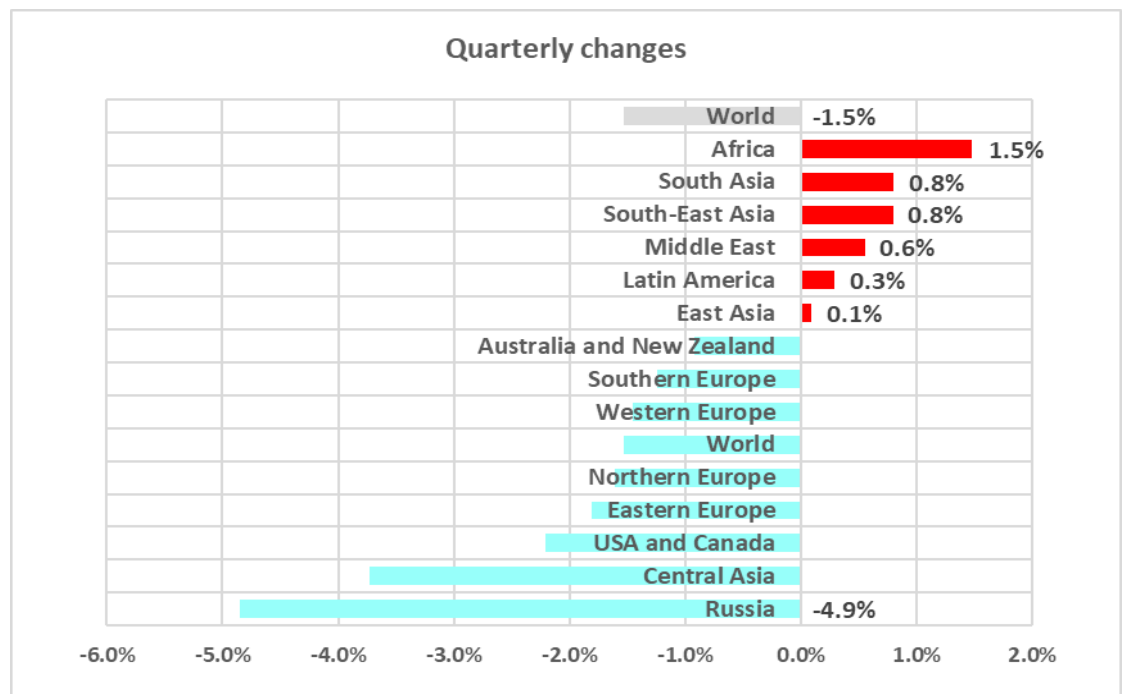
Up to 20%

- Southern Europe – 19.7%
- Russia – 17.6%
- Australia and New Zealand – 16%
- US and Canada – 11.3%
- Western Europe – 11.7%
- Northern Europe – 9.7%

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

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

Regions and world. Changes in the percentage of attacked ICS computers in Q3 2024



Malicious object categories

Malicious objects used for initial infection

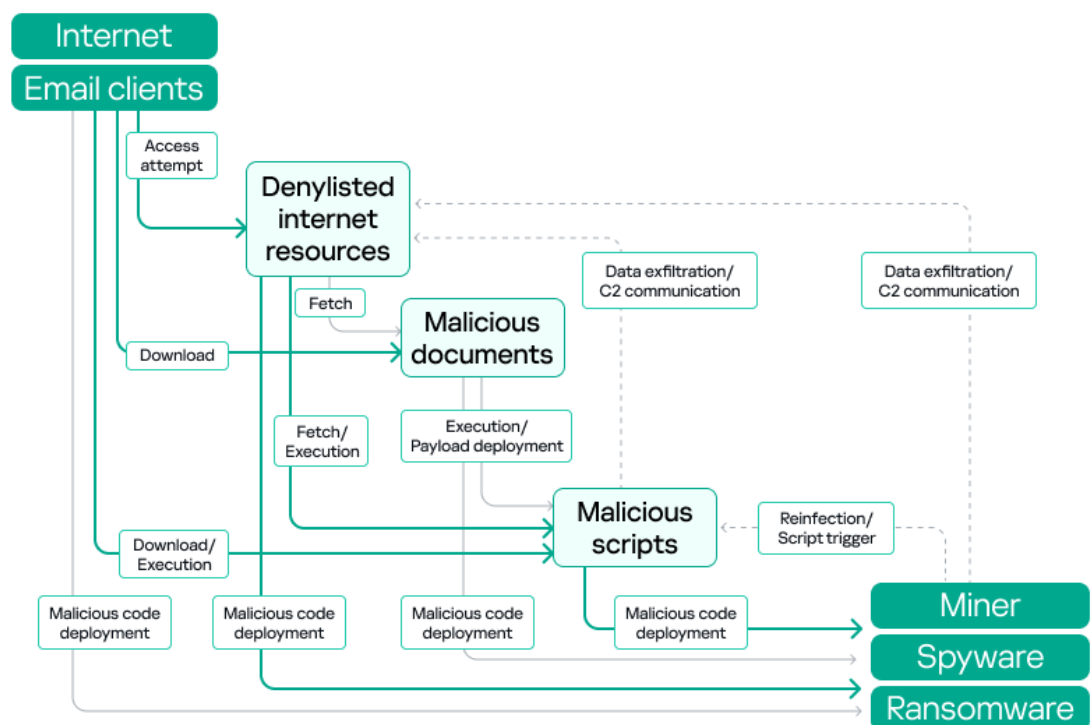
Malicious objects that are used for initial infection of ICS computers include dangerous internet resources that are added to denylists, malicious scripts and phishing pages, and malicious documents.

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), especially 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.

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

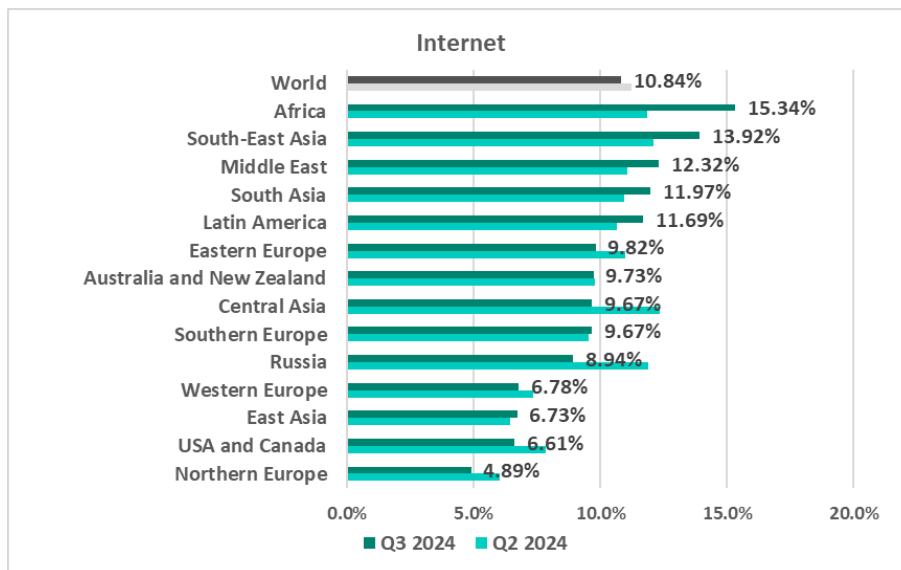


Globally and in almost all regions, denylisted internet resources and malicious scripts and phishing pages are the top categories of malicious objects in terms of the percentage of ICS computers on which these objects were blocked.

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

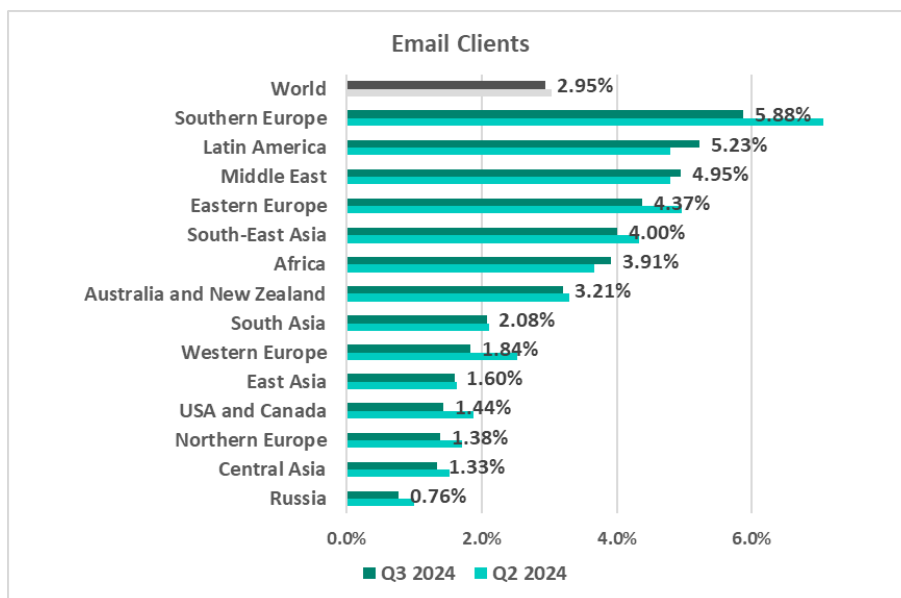
In Q3 2024, **Africa**, **South-East Asia**, and the **Middle East** ranked as the **top three** regions by the percentage of ICS computers on which threats from **internet** were blocked.

Regions ranked by percentage of ICS computers on which threats from the internet were blocked, Q3 2024



The **top three** regions with the highest **email threats** rates were **Southern Europe**, **Latin America**, and the **Middle East**.

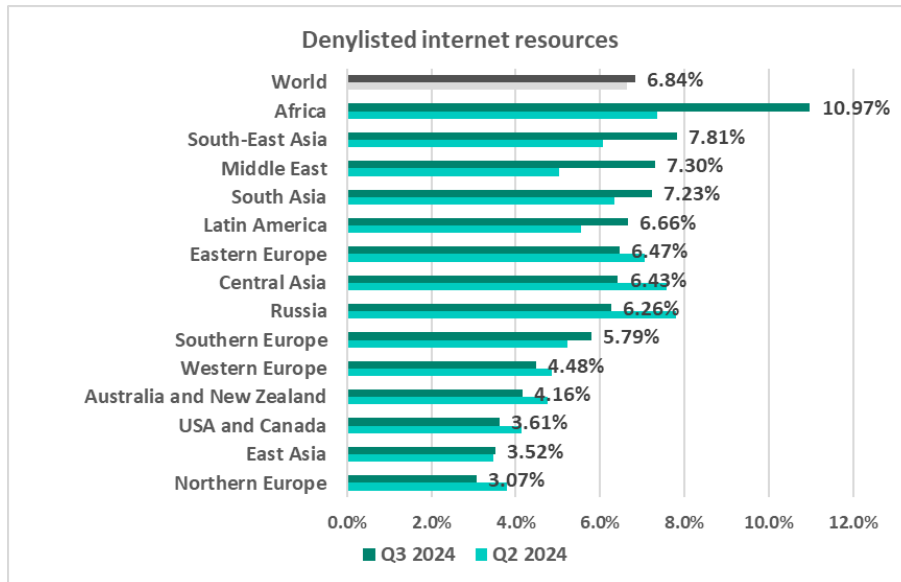
Regions ranked by percentage of ICS computers on which threats from email clients were blocked, Q3 2024



Denylisted internet resources

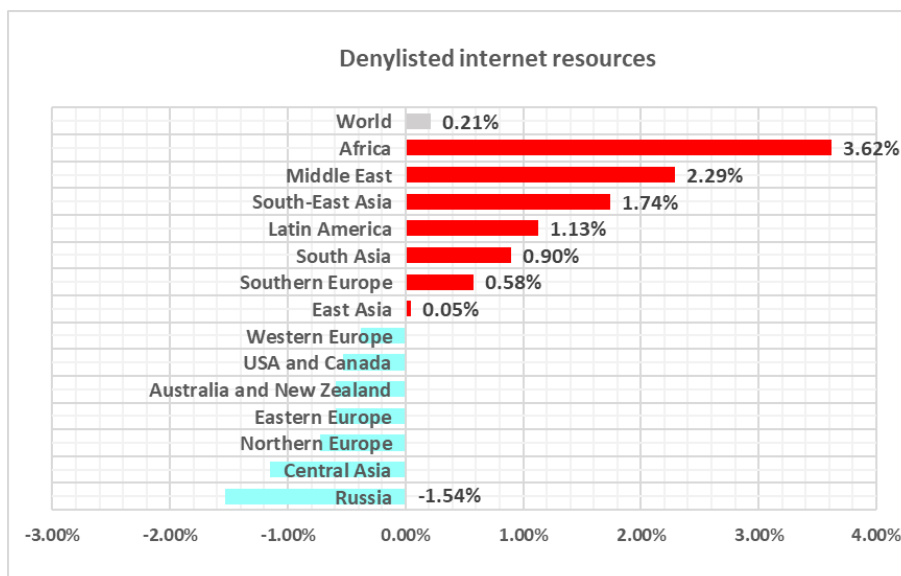
Africa, South-East Asia, and the Middle East ranked as the **top three** regions by the percentage of ICS computers on which denylisted internet resources were blocked.

Regions ranked by percentage of ICS computers on which denylisted internet resources were blocked, Q3 2024



The top three regions in terms of **growth** in the percentage of ICS computers on which denylisted internet resources were blocked were **Africa, the Middle East, and South-East Asia.**

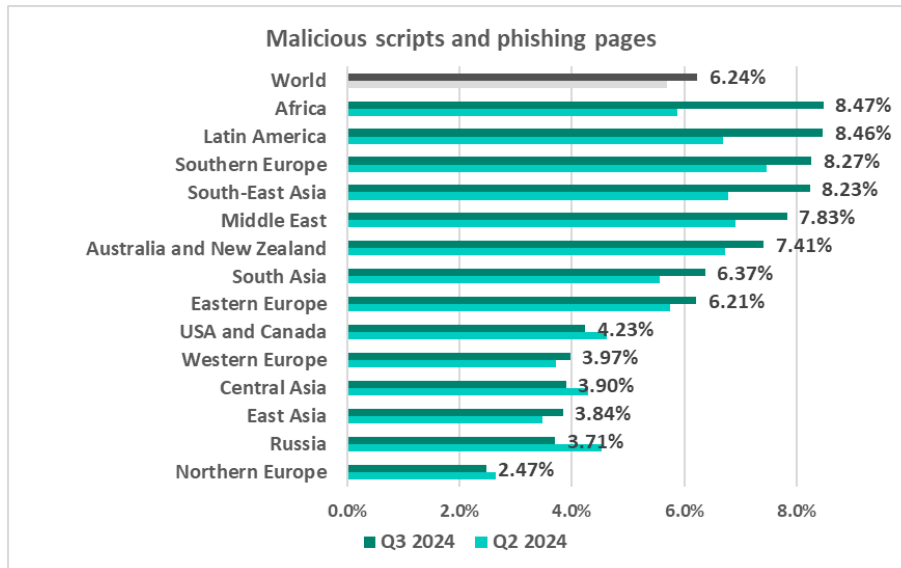
Changes in the percentage of ICS computers on which denylisted internet resources were blocked, Q3 2024



Malicious scripts and phishing pages

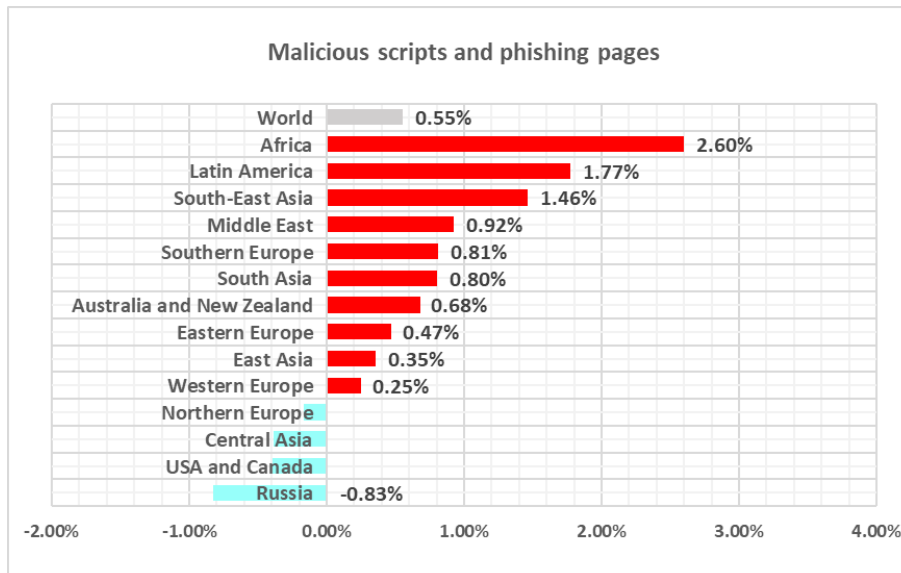
The **top three** regions by percentage of ICS computers on which malicious scripts and phishing pages were blocked were **Africa, Latin America, and Southern Europe**.

Regions ranked by percentage of ICS computers on which malicious scripts and phishing pages were blocked, Q3 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 **Africa, Latin America, and South-East Asia**.

Changes in the percentage of ICS computers on which malicious scripts and phishing pages were blocked, Q3 2024



A significant increase in the percentage of malicious scripts and phishing pages in the majority of regions was driven by a series of widespread phishing attacks in August and September of 2024. In these attacks, threat actors used malicious scripts that execute in the browser, mimicking various windows with CAPTCHA-

like interfaces, browser error messages, and similar pop-ups. These scripts are designed to trick users into following simple instructions on their computers, which ultimately trigger the download of next-stage malware – either the Lumma stealer or the Amadey Trojan.

The phishing lures were distributed through various channels, including phishing emails (e.g. fake vulnerability notifications claiming to be from GitHub), malicious links, and malvertising networks found on various resources (e.g. file sharing services). The instructions provided by the phishing scripts tricked users into executing malicious PowerShell commands to download additional spyware.

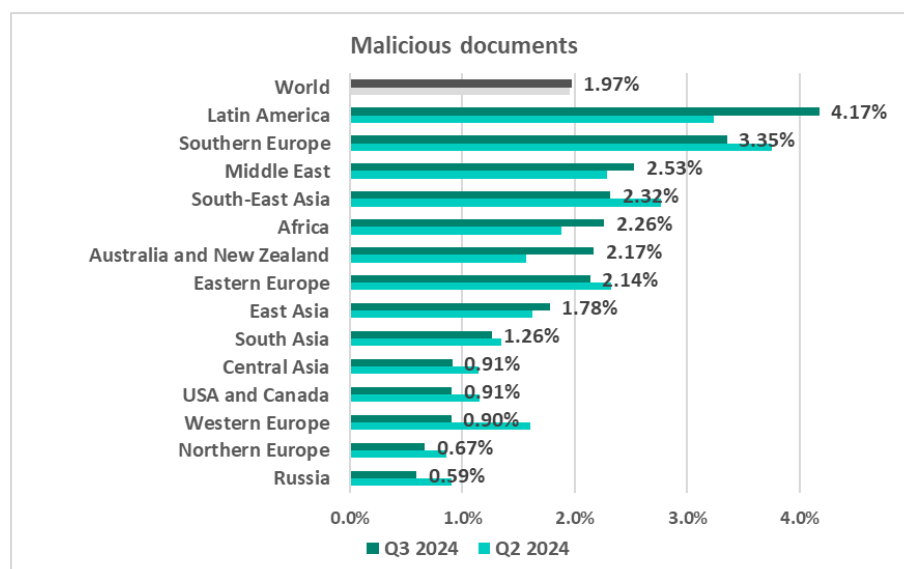
It's important to note that both Lumma and Amadey are designed to steal credentials from browsers and password managers. In addition, Amadey has been observed using modules to steal credentials from various Virtual Network Computing (VNC) systems².

The exposure of these credentials significantly increases the risk of subsequent attacks, such as ransomware, as threat actors can use the stolen data to access sensitive systems and escalate their attacks.

Malicious documents

Latin America, Southern Europe, and the Middle East ranked as the **top three** regions by the percentage of ICS computers on which malicious documents were blocked.

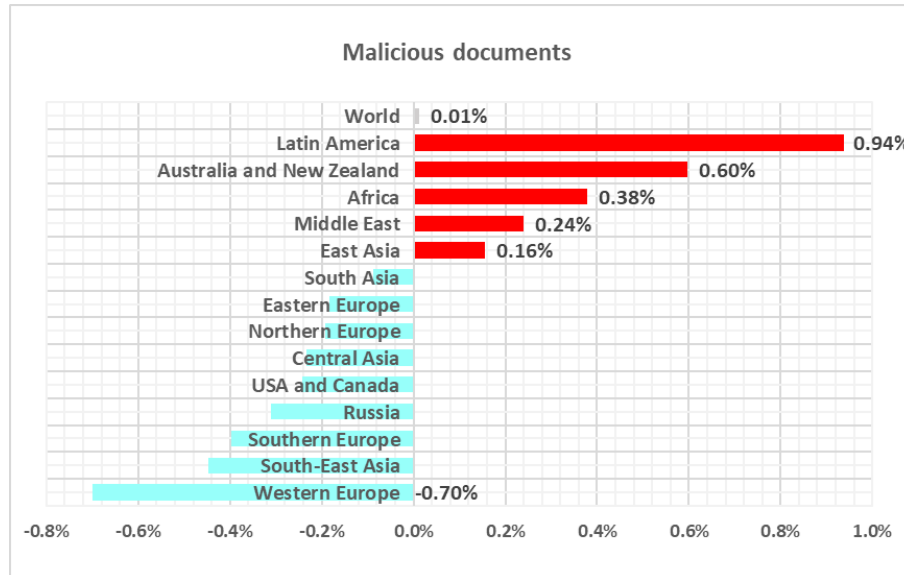
Regions ranked by percentage of ICS computers on which malicious documents were blocked, Q3 2024



² Read more about these attacks here: [Malicious CAPTCHA delivers Lumma and Amadey Trojans](#)

The top three regions in terms of **growth** in the percentage of ICS computers on which malicious documents were blocked were **Latin America, Australia and New Zealand, and Africa**.

Changes in the percentage of ICS computers on which malicious documents were blocked, Q3 2024



Next-stage malware

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

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

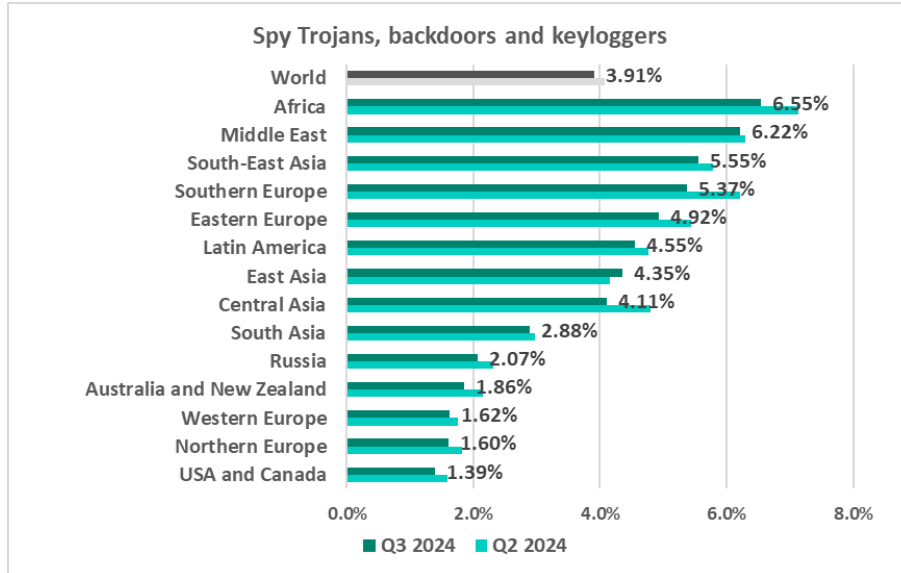
Spyware (including Trojans, backdoors, and keyloggers) is typically the most frequently detected type of next-stage malware. It is either used as a toolset for intermediate steps in the kill chain (such as reconnaissance and lateral movement) or as a final-stage tool for stealing and exfiltrating confidential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

In Q3 2024, **Africa**, the **Middle East**, and **South-East Asia** ranked as the **top three** regions by the percentage of ICS computers on which spyware was blocked.

As expected, these regions also ranked among the highest for one or more types of initial infection threats.

Regions ranked by percentage of ICS computers on which spyware was blocked, Q3 2024

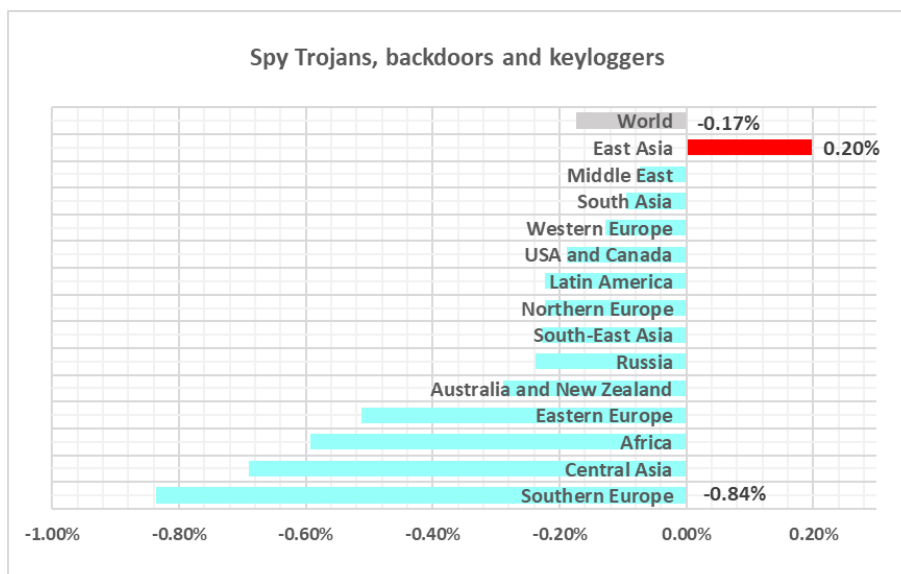


In almost all regions, spyware does not rank higher than third in the threat category rankings by percentage of ICS computers on which it was blocked, except in the following regions:

- **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.
- **Central Asia:** spyware is the **second most prevalent** threat in this region.

East Asia is also the only region in Q3 2024 in which spyware showed **growth** in terms of the percentage of ICS computers on which it was blocked.

Changes in the percentage of ICS computers on which spyware was blocked, Q3 2024

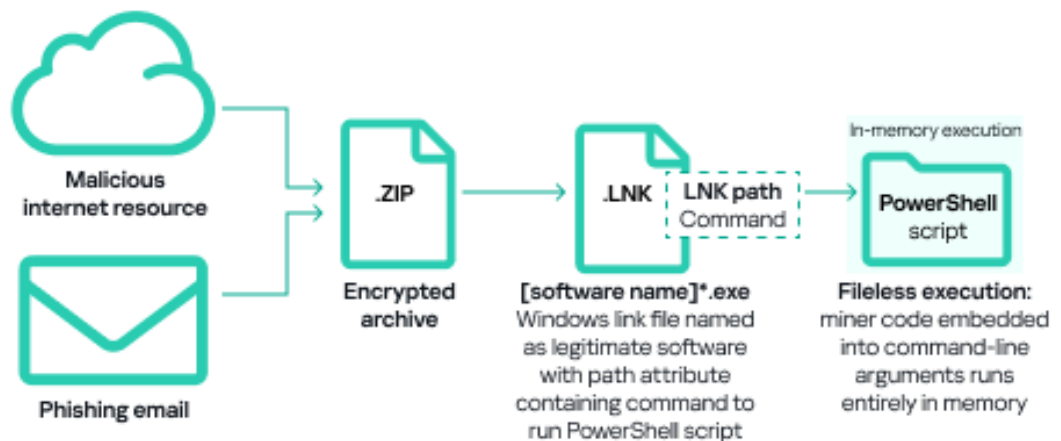


Covert crypto-mining programs

Miners in the form of executable files for Windows

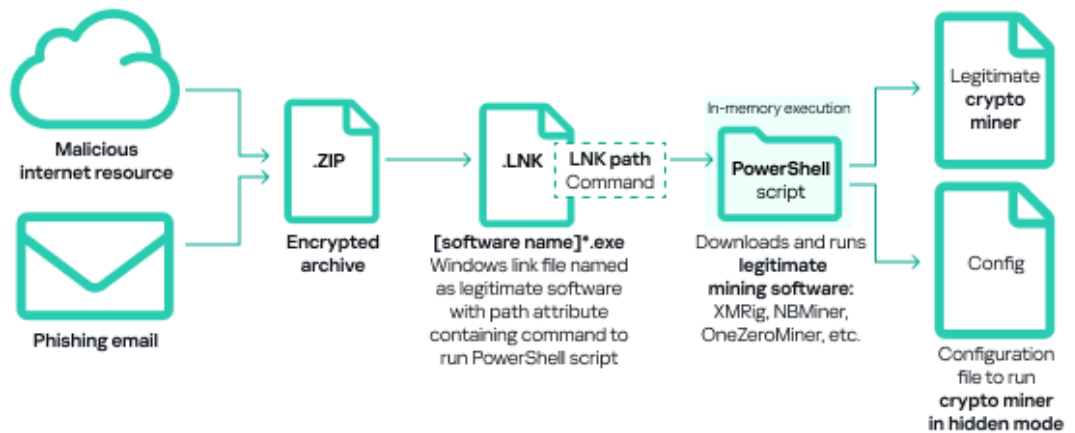
In the third quarter of 2024, similar to the previous quarter, a significant portion of Windows miners found on ICS computers consisted of archives with names mimicking legitimate software. These archives did not contain actual software but included a Windows LNK file, commonly known as a shortcut. However, 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.

Kill chain example:
fileless execution
in cryptomining attacks



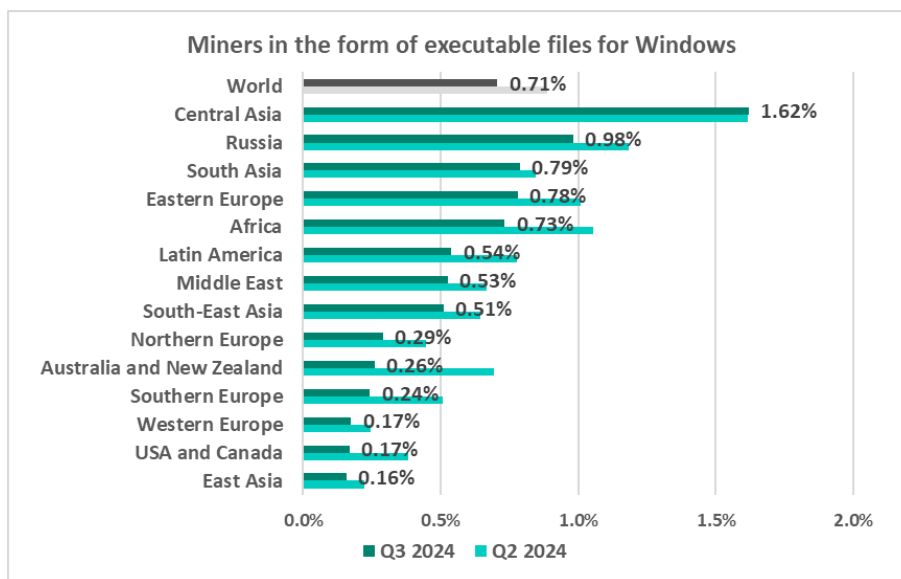
Another common method of deploying miners on ICS computers involves using legitimate cryptocurrency mining software such as XMRig, NBMiner, OneZeroMiner, and others. While these miners are not inherently malicious, they are classified as [RiskTools](#) by security systems. Attackers exploit these miners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

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



The **top three** regions by percentage of ICS computers on which miners in the form of executable files for Windows were blocked were **Central Asia**, **Russia**, and **South Asia**.

Regions ranked by percentage of ICS computers on which miners in the form of executable files for Windows were blocked, Q3 2024

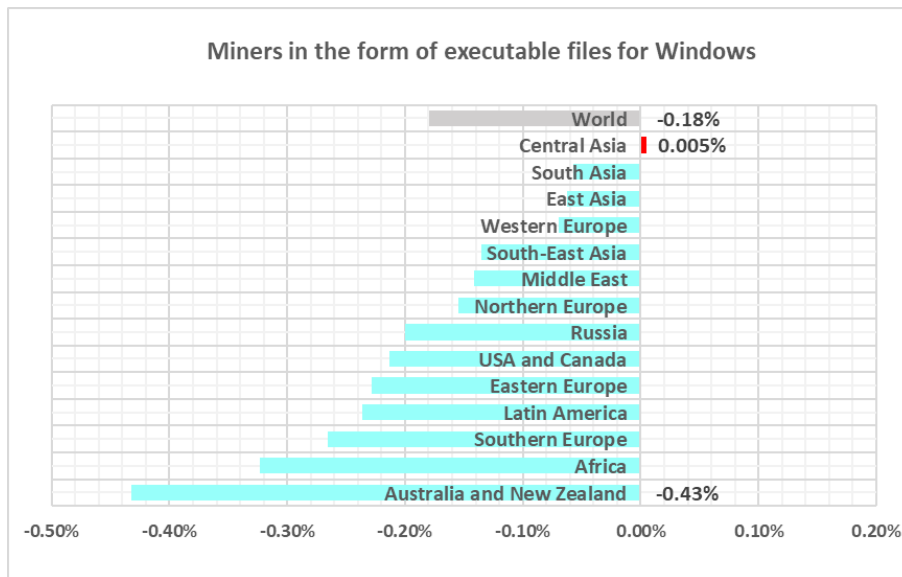


In the global ranking of threat categories by percentage of ICS computers on which they were blocked, miners in the form of Windows executable files are normally ranked seventh.

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

Central Asia was also the only region in Q3 2024 that showed **growth** in the percentage of ICS computers on which executable miners were blocked.

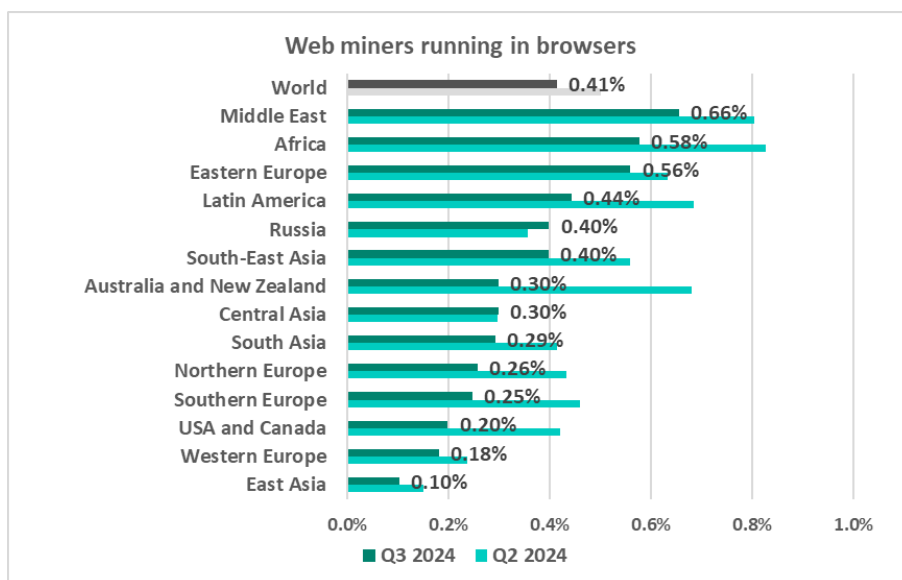
Changes in the percentage of ICS computers on which miners in the form of executable files for Windows were blocked, Q3 2024



Covert crypto-mining programs Web miners running in browsers

The three leading regions by percentage of ICS computers on which web miners running in browsers were blocked were: **Middle East, Africa, and Eastern Europe.**

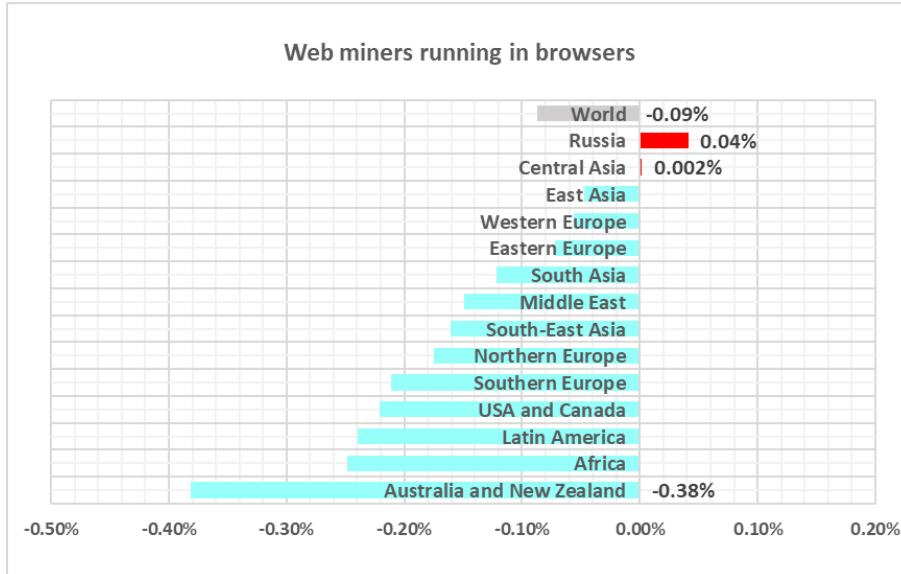
Regions ranked by percentage of ICS computers on which web miners were blocked, Q3 2024



In the regional rankings of threat categories by percentage of ICS computers on which they were blocked, web miners ended up much higher regionally (eighth place globally) in **Australia and New Zealand** – fifth place in the regional ranking.

Russia and **Central Asia** were the only regions that experienced **growth** in the percentage of ICS computers on which web miners were blocked.

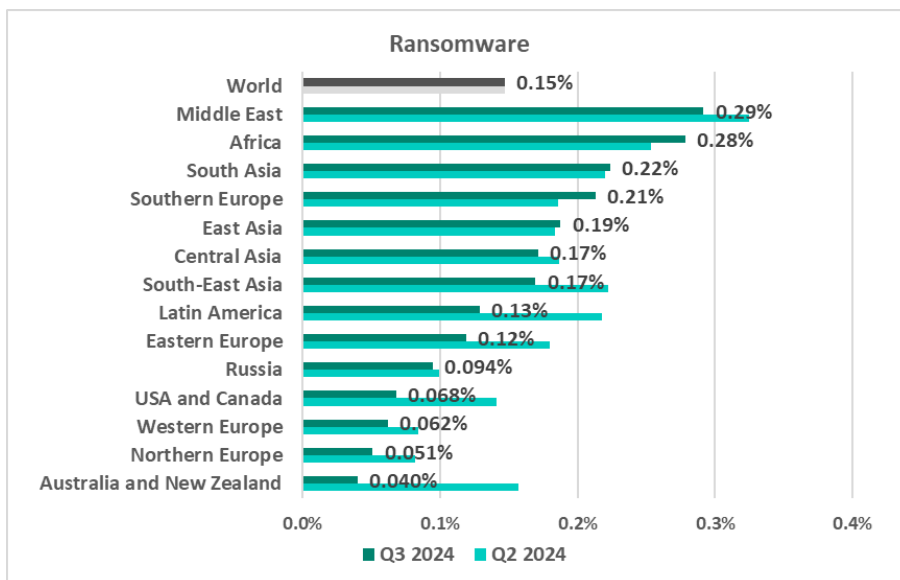
Changes in the percentage of ICS computers on which web miners were blocked, Q3 2024



Ransomware

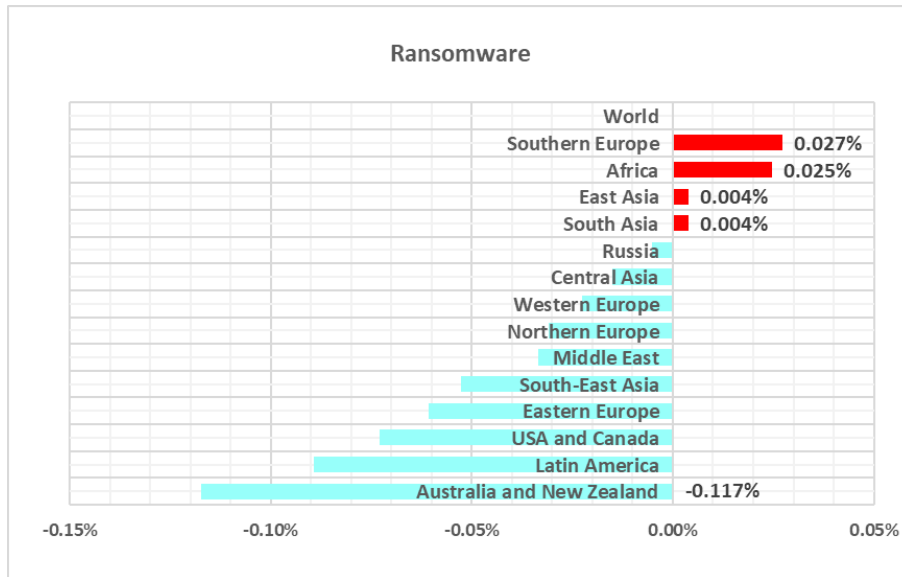
The **top three** regions with the highest percentage of ICS computers on which ransomware was blocked were the **Middle East, Africa,** and **South Asia.**

Regions ranked by percentage of ICS computers on which ransomware was blocked, Q3 2024



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

Changes in the percentage of ICS computers on which ransomware was blocked, Q3 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.

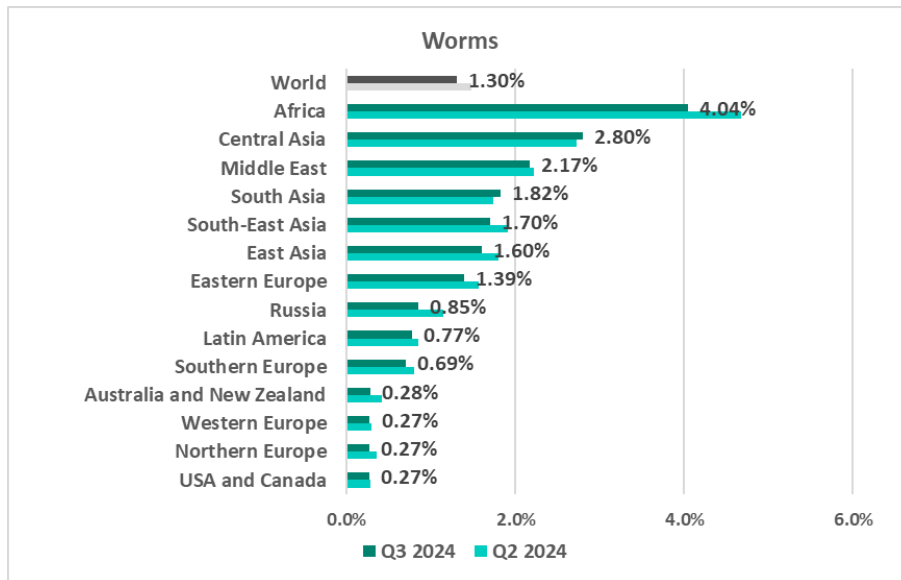
To spread across ICS networks, viruses and worms rely on removable media, network folders, infected files including backups, and network attacks on outdated software.

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 **top three** regions by percentage of ICS computers on which worms were blocked were **Africa, Central Asia, the Middle East**.

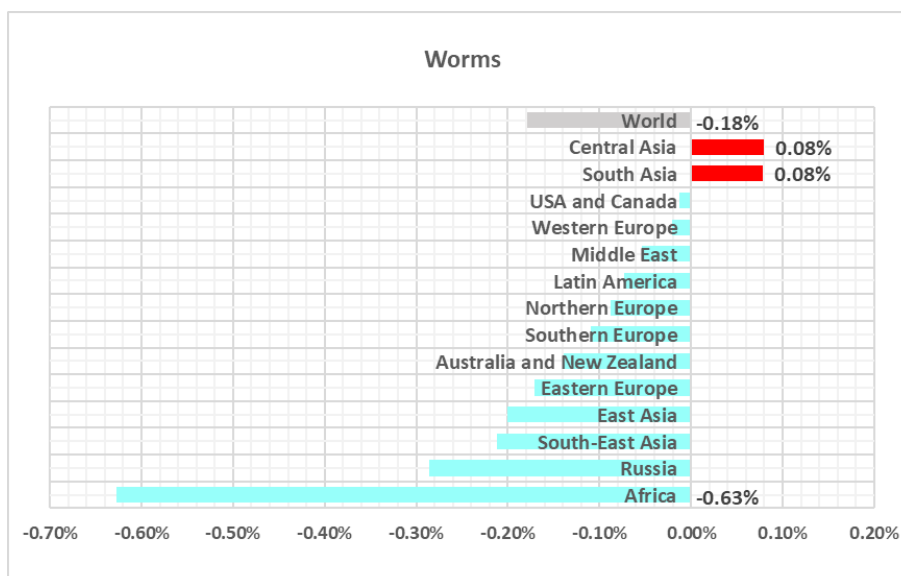
Regions ranked by percentage of ICS computers on which worms were blocked, Q3 2024



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 much higher** in the following regions: Africa, Central Asia, South Asia – fourth place in the respective regional ranking.

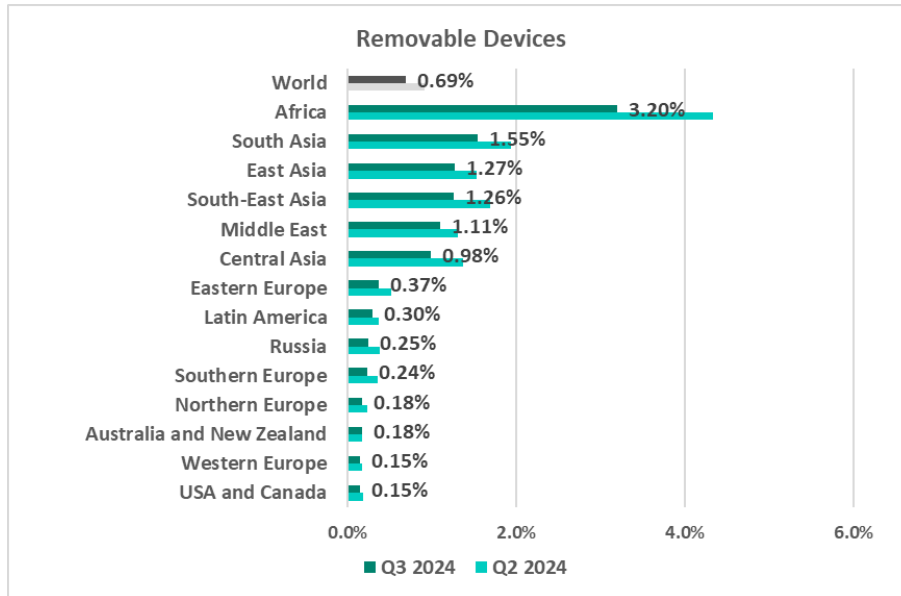
South and **Central Asia** were the only regions in terms of **growth** in the percentage of ICS computers on which worms were blocked.

Changes in the percentage of ICS computers on which worms were blocked, Q3 2024



Africa and **South Asia** were also among the leading regions by percentage of ICS computers on which threats were blocked when connecting **removable media**.

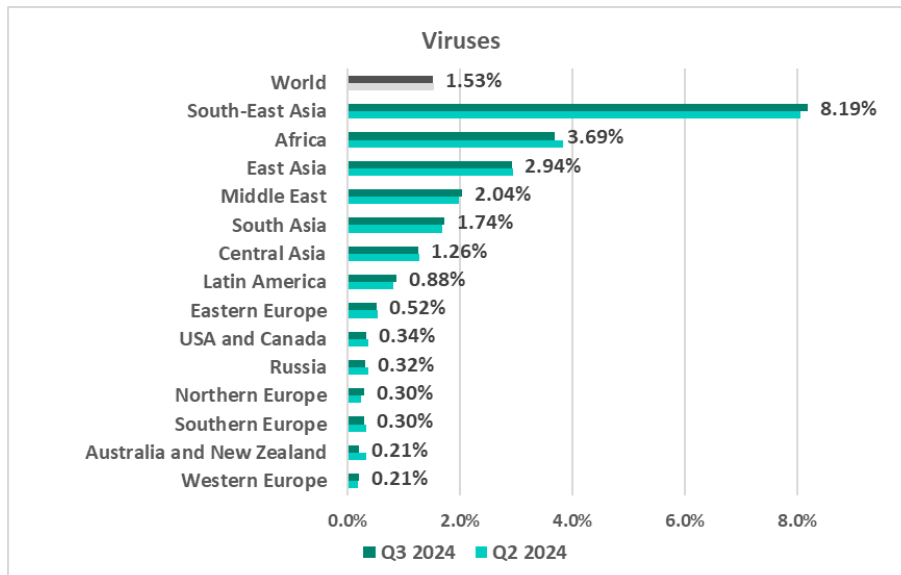
Regions ranked by percentage of ICS computers on which threats from removable devices were blocked, Q3 2024



Viruses

The **top three** regions by percentage of ICS computers on which viruses were blocked were **South-East Asia, Africa, and East Asia**.

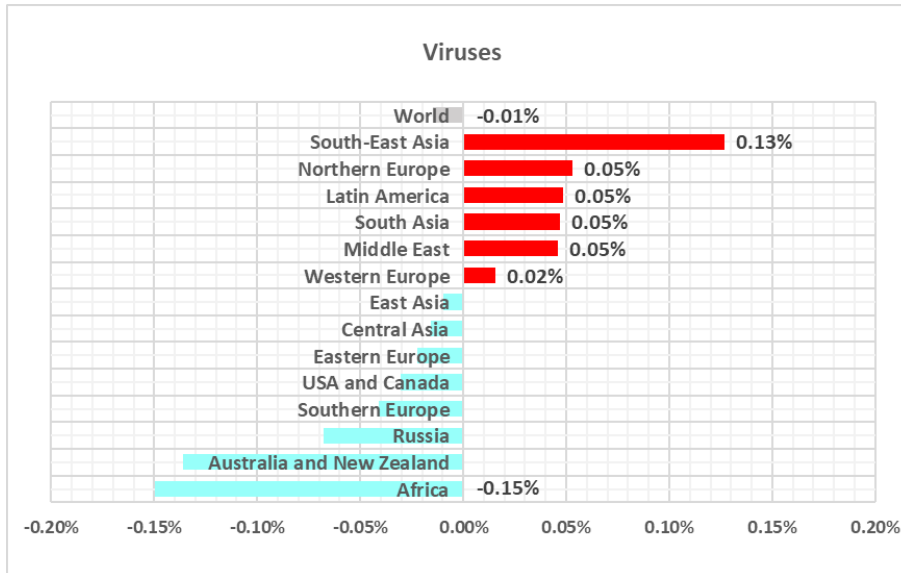
Regions ranked by percentage of ICS computers on which viruses were blocked, Q3 2024



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

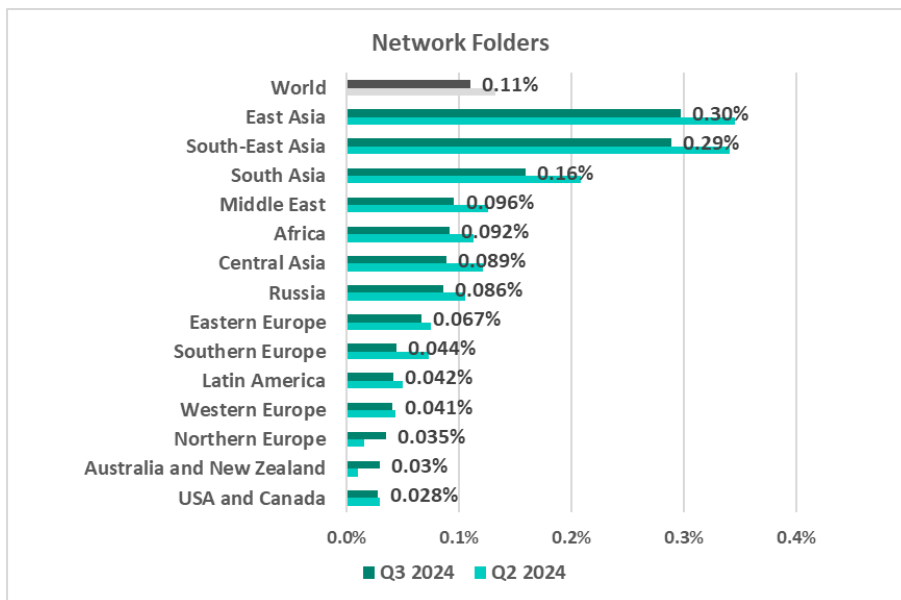
The top three regions in terms of **growth** in the percentage of ICS computers on which viruses were blocked were **South-East Asia, Northern Europe, and Latin America**.

Changes in the percentage of ICS computers on which viruses were blocked, Q3 2024



Note that there is an overlap between the leading regions in viruses and leaders by percentage of ICS computers on which **network folder threats** were blocked.

Regions ranked by percentage of ICS computers on which threats from network folders were blocked, Q3 2024

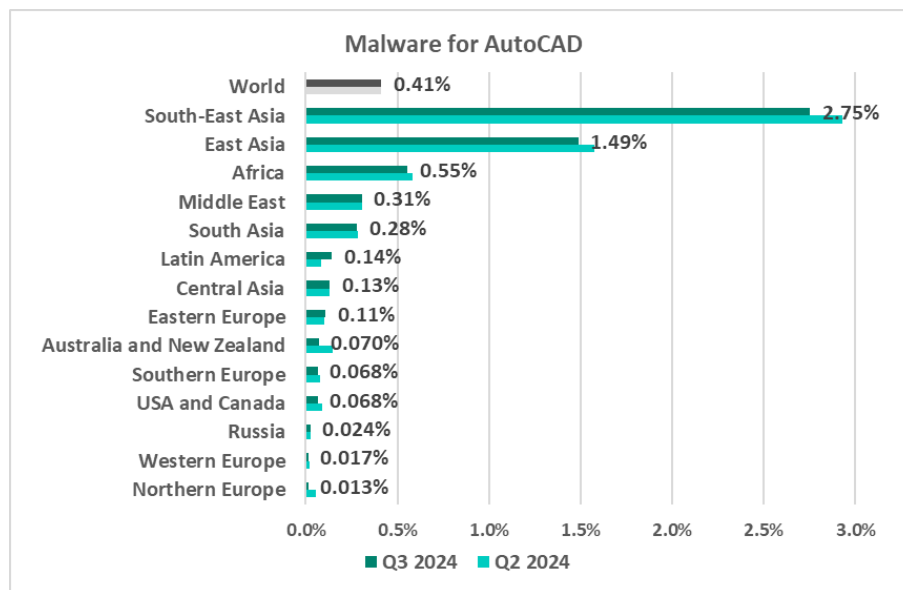


AutoCAD malware

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: **South-East Asia, East Asia, and Africa.**

Regions ranked by percentage of ICS computers on which malware for AutoCAD was blocked, Q3 2024



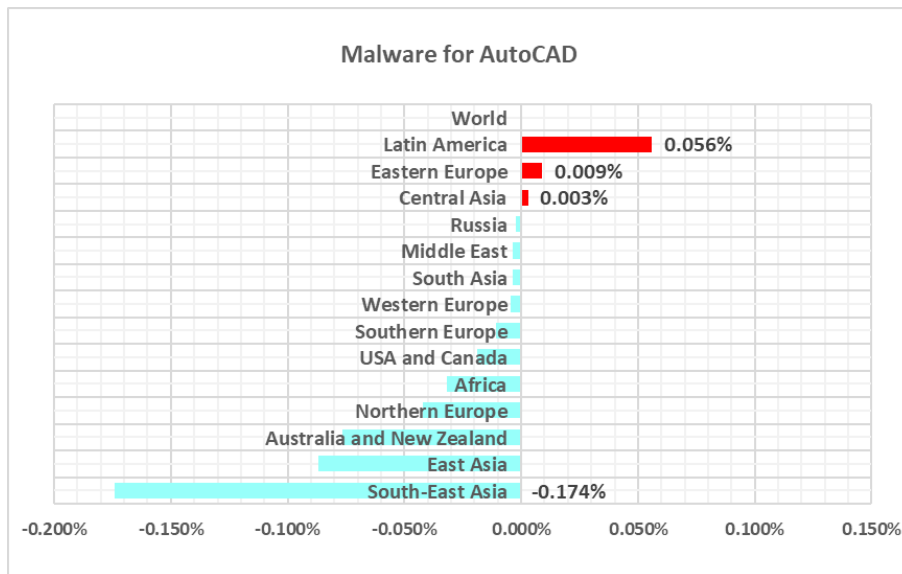
Normally, AutoCAD malware is a minor threat and usually comes bottom of the malware category rankings by percentage of ICS computers on which it was blocked.

However, in Q3 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 **Latin America, Eastern Europe, and Central Asia.**

Changes in the percentage of ICS computers on which malware for AutoCAD was blocked, Q3 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

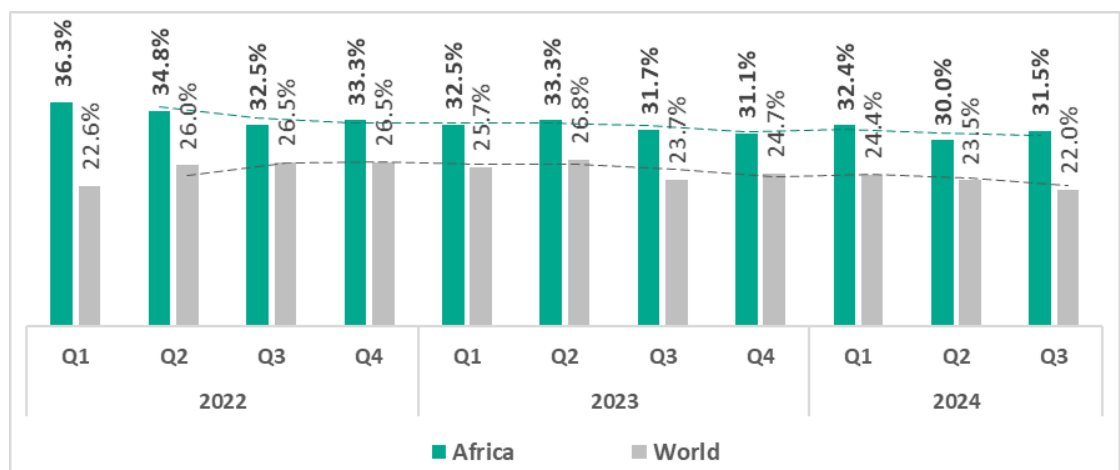
<p>N.1 IN THE REGION</p> <p>DENYLISTED INTERNET RESOURCES</p> <p>10.97%</p> <p> 1.5x increase in Q3 1st globally in growth</p> <p> 1.6x above global average 1st in the world</p>	<p>N.2 IN THE REGION</p> <p>MALICIOUS SCRIPTS & PHISHING PAGES</p> <p>8.47%</p> <p> 1.4x increase in Q3 1st globally in growth</p> <p> 1.4x above global average 1st in the world</p>	<p>N.3 IN THE REGION</p> <p>SPYWARE</p> <p>6.55%</p> <p> decrease in Q3</p> <p> 1.7x above global average 1st in the world</p>
<p>WORMS</p> <p>4.04%</p> <p> decrease in Q3</p> <p> 3.1x above global average 1st in the world</p>	<p>VIRUSES</p> <p>3.69%</p> <p> decrease in Q3</p> <p> 2.4x above global average 2nd in the world</p>	<p>MALICIOUS DOCUMENTS</p> <p>2.26%</p> <p> 1.2x increase in Q3 3rd globally in growth</p> <p> 1.1x above global average</p>
<p>WEB MINERS</p> <p>0.58%</p> <p> decrease in Q3</p> <p> 1.4x above global average 2nd in the world</p>	<p>MALWARE FOR AUTOCAD</p> <p>0.55%</p> <p> decrease in Q3</p> <p> 1.4x above global average 3rd in the world</p>	<p>RANSOMWARE</p> <p>0.28%</p> <p> 1.1x increase in Q3 2nd globally in growth</p> <p> 1.8x above global average 2nd in the world</p>
<p>THREATS FROM INTERNET</p> <p>15.34%</p> <p> 1.3x increase in Q3</p> <p> 1.4x above global average 1st in the world</p>	<p>THREATS FROM EMAIL CLIENTS</p> <p>3.91%</p> <p> 1.1x increase in Q3 2nd globally in growth</p> <p> 1.3x above global average</p>	<p>THREATS FROM REMOVABLE DEVICES</p> <p>3.20%</p> <p> decrease in Q3</p> <p> 4.6x above global average 1st in the world</p>

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. However, in Q3 2024, the region showed an increase in the percentage of ICS computers on which malicious objects were blocked.



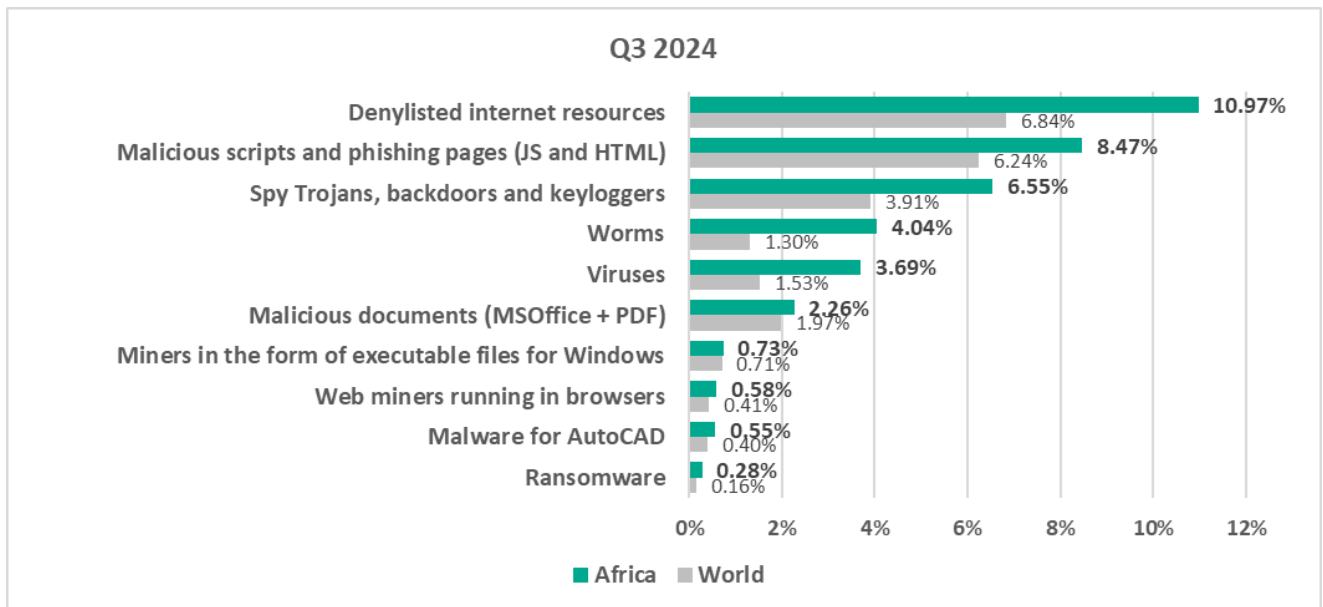
Comparative analysis

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

- First place: denylisted internet resources, malicious scripts and phishing pages, spyware, worms, threats from internet and removable devices
- Second place: web miners, ransomware, viruses

Threat categories

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



- The region has a significantly **higher** percentage **than the respective global average** percentages of ICS computers on which the following were blocked:

- Worms, 3.1 times higher
- Viruses, 2.4 times higher

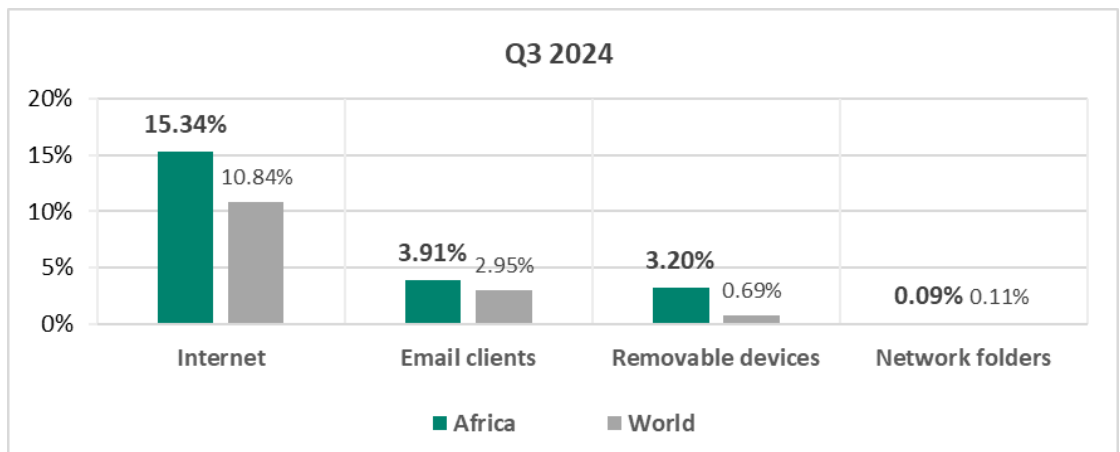
Worms and viruses outpace malicious documents in the threat category ranking by percentage of ICS computers on which they were blocked. Worms are in fourth place (sixth place globally). As noted earlier, high rates of self-propagating malware on a large scale indicate that a significant portion of the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

- Ransomware, 1.8 times higher
- Spyware, 1.7 times higher
- Denylisted internet resources, 1.6 times higher

- Web miners, 1.4 times higher
- Malicious scripts and phishing pages, 1.4 times higher
- Malware for AutoCAD, 1.4 times higher

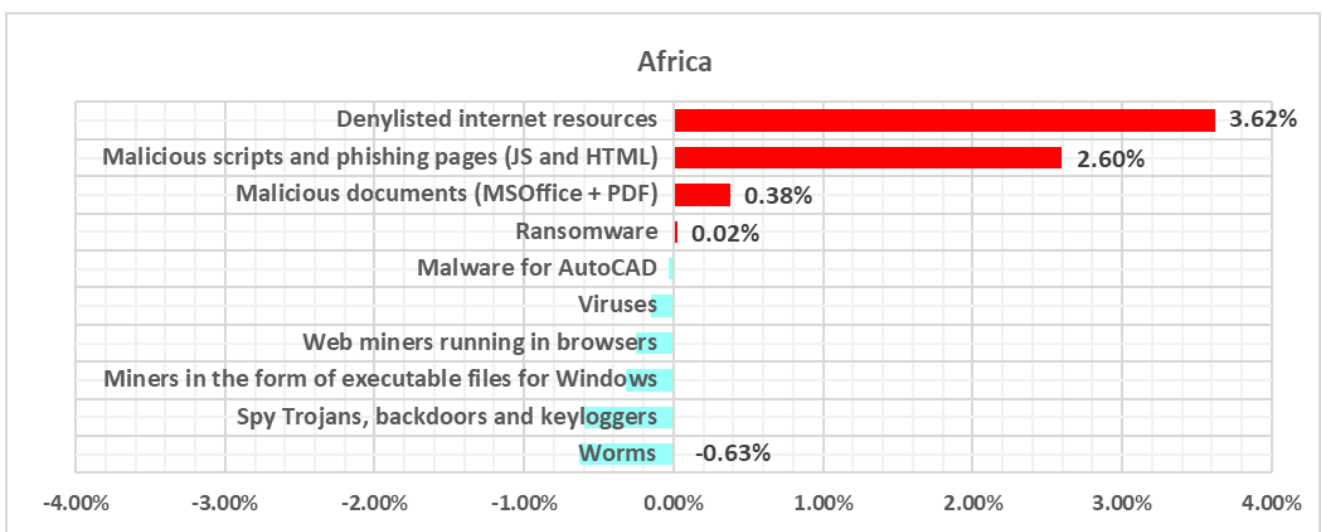
Threat sources

- The region ranked **first in the world** both by percentage of ICS computers on which threats from **internet** and **removable devices** were blocked, exceeding the global average by 1.4 times and 4.6 times respectively.
- With regard to threats from the **email clients**, the region ranked **second in the world**, exceeding the global average by 1.3 times.

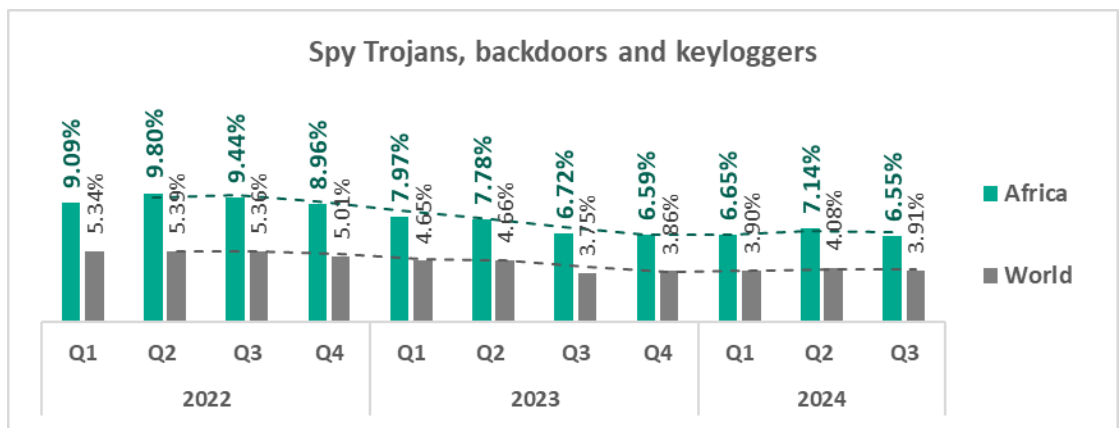
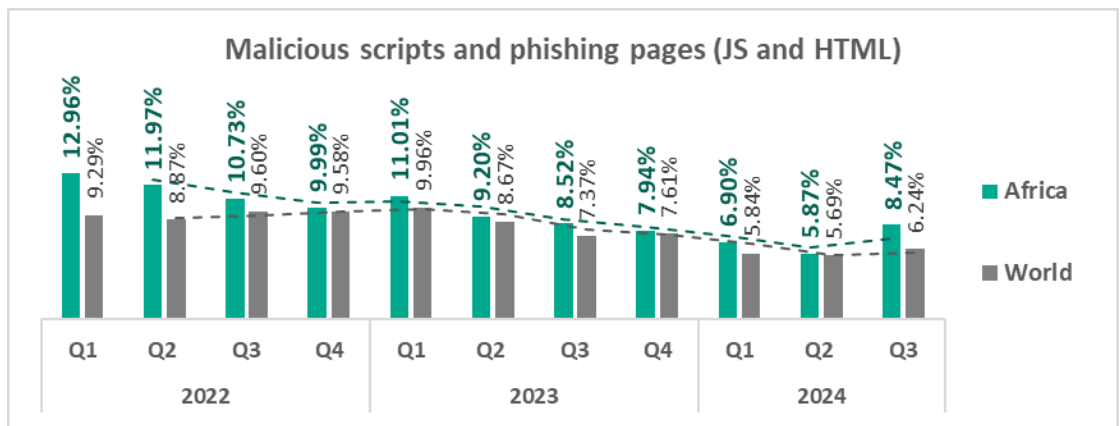
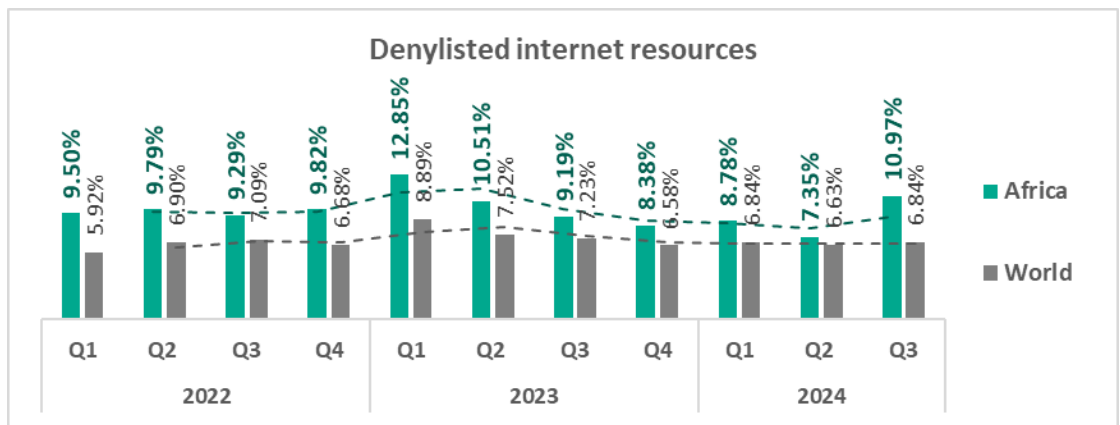


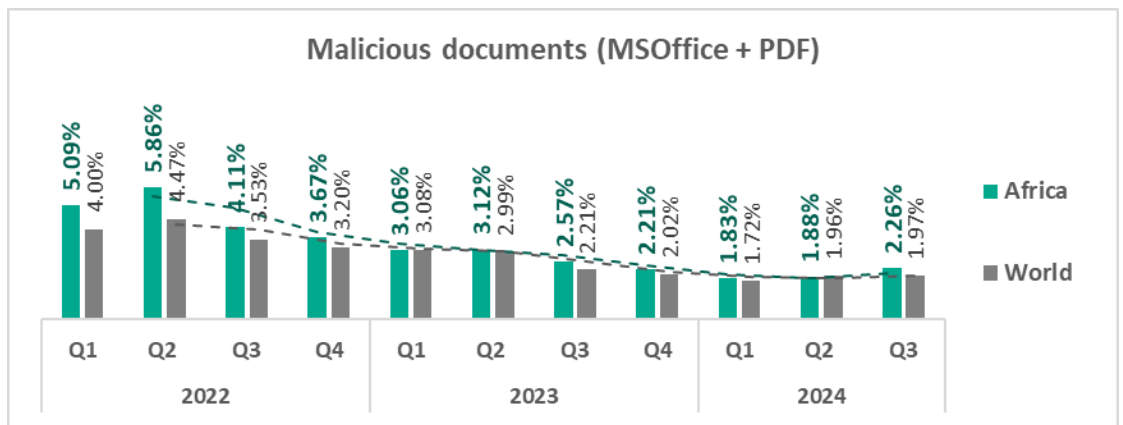
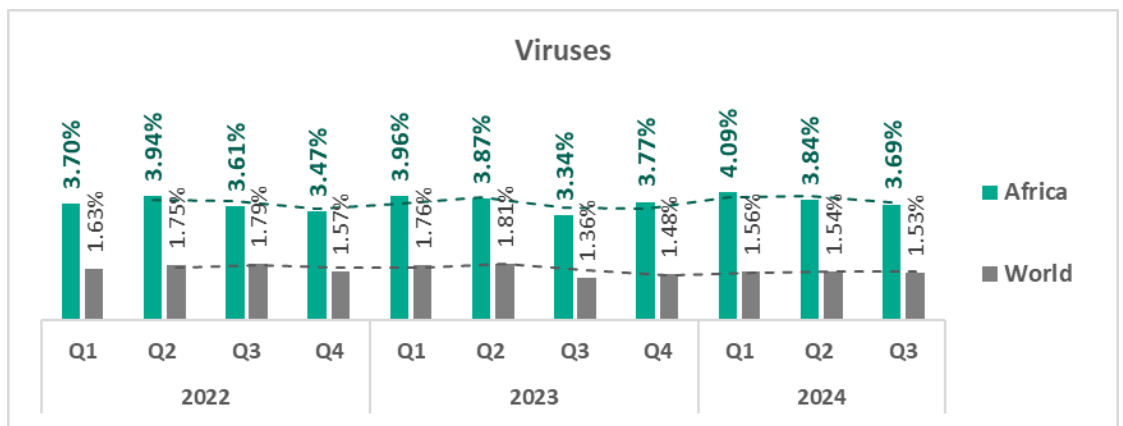
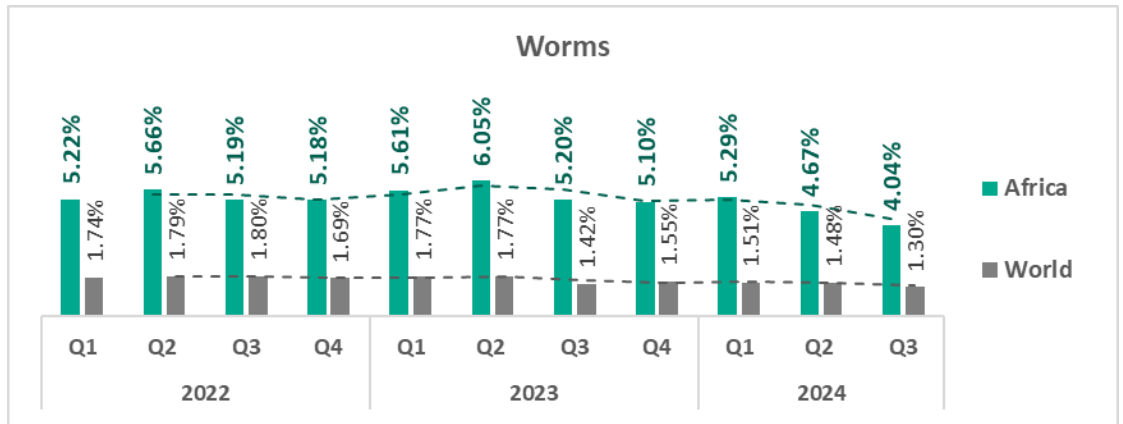
Quarterly changes and trends

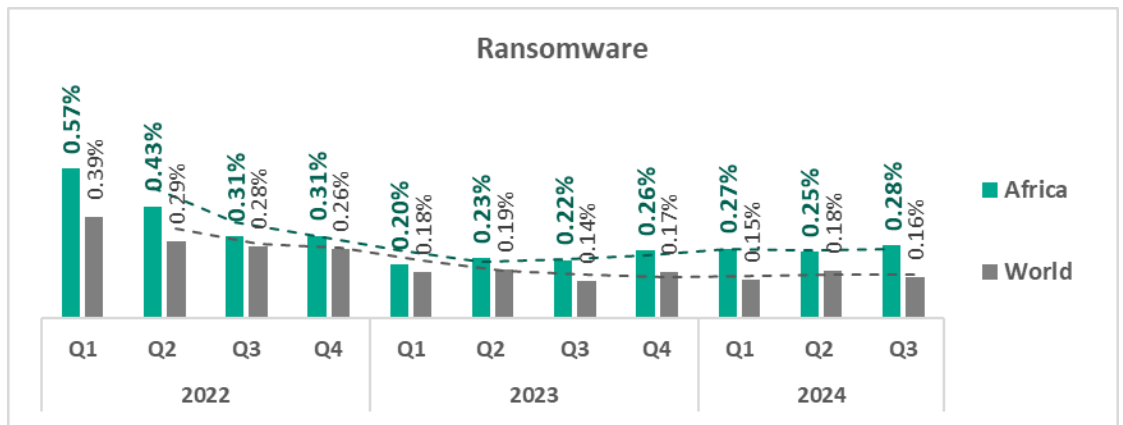
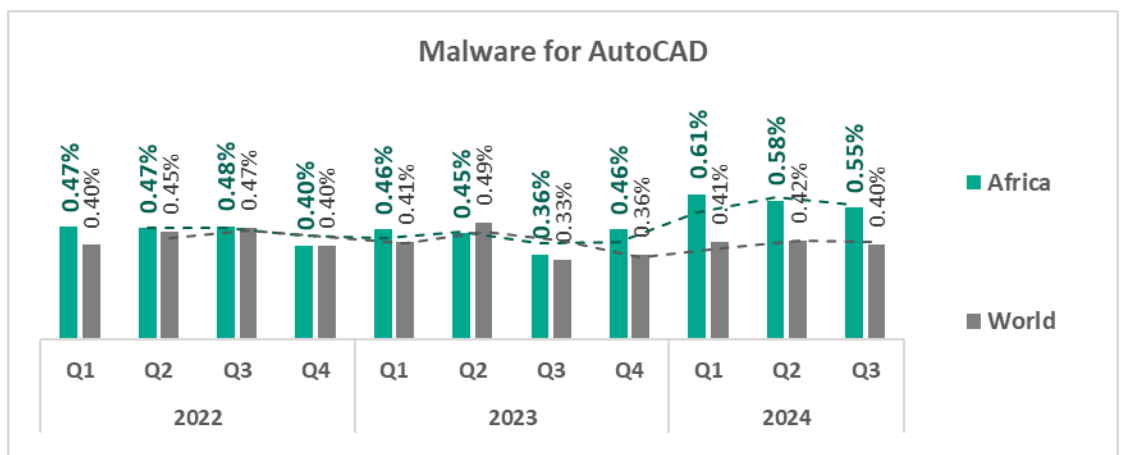
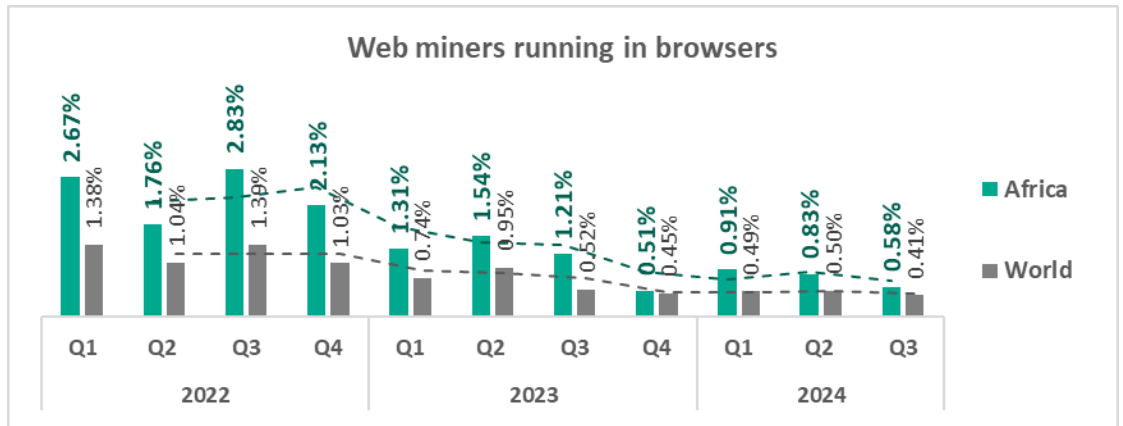
Threat categories



- The **largest proportional increase** in Q3 2024 was in the percentage of ICS computers on which the following were blocked:
 - Denylisted internet resources – by 1.5 times
 - Malicious scripts and phishing pages – by 1.4 times
 - Malicious documents – by 1.2 times
 - Ransomware – by 1.1 times
- The **top threat** categories exhibit various quarterly dynamics:





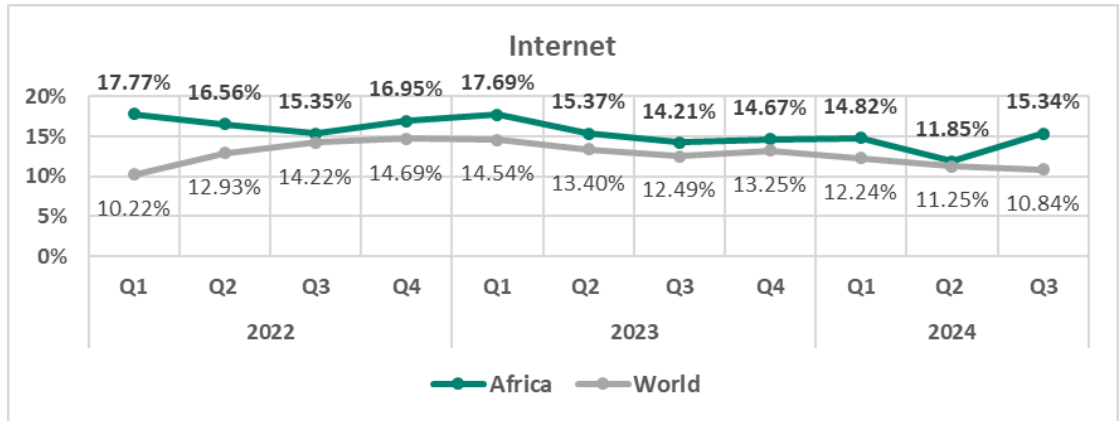


- The heatmap below illustrates changes in the ranking of threat categories in the region since the beginning of 2022. **Denylisted internet resources** have been the leading threat category in the region since early 2023. **Malicious scripts and phishing** moved back from third to second place in Q3 2024, while **spyware** dropped back to the third place.

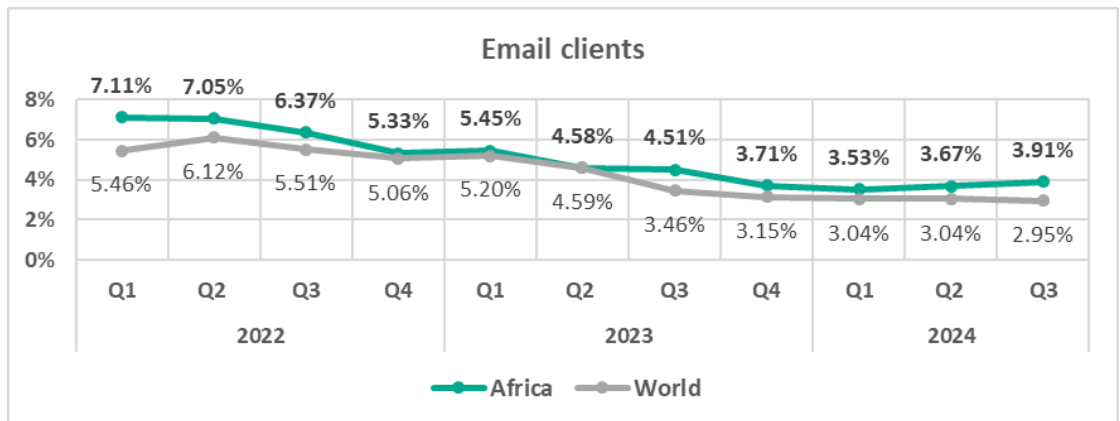
Africa	2022				2023				2024		
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3
Denylisted internet resources	2	3	3	2	1	1	1	1	1	1	1
Malicious scripts and phishing pages (JS and HTML)	1	1	1	1	2	2	2	2	2	3	2
Spy Trojans, backdoors and keyloggers	3	2	2	3	3	3	3	3	3	2	3
Worms	4	5	4	4	4	4	4	4	4	4	4
Viruses	6	6	6	6	5	5	5	5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

Threat sources

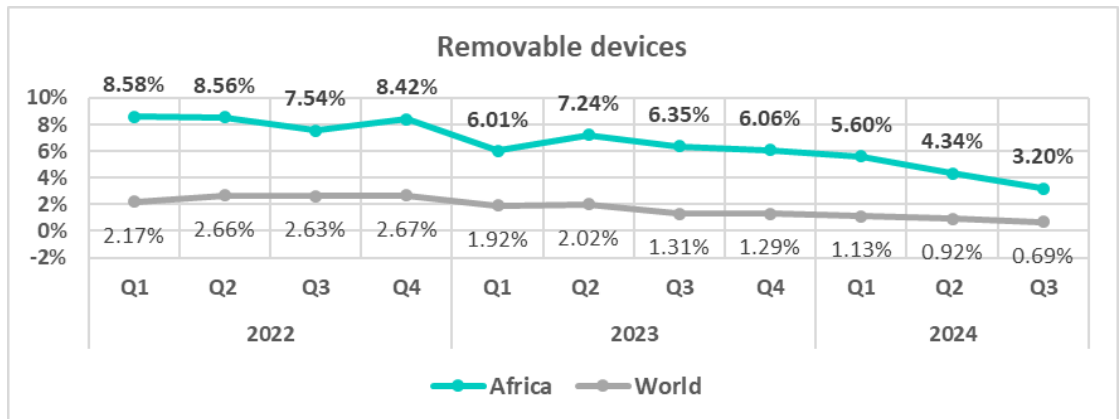
- In Q3 2024, the **internet** as a threat source exhibited a **steep increase**, in contrast to the global trend.



- Email client** threats **continued to increase** in Africa in Q3 2024, while the global trend showed a decline.

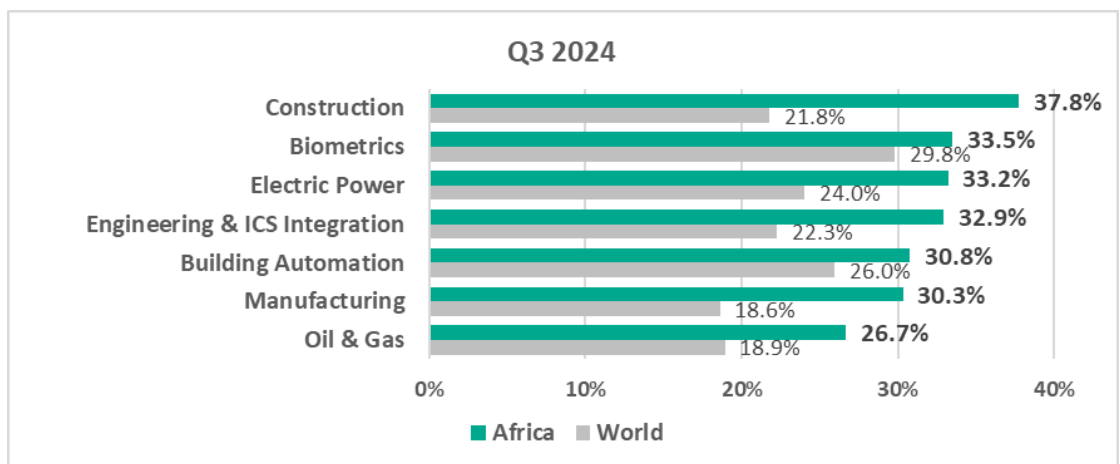


- Threats from **removable devices** continued to decrease which corresponds to the global trend. In Q3 2024, the rate of ICS computers on which threats from removable devices were blocked finally became lower than the rate of threats from email clients.

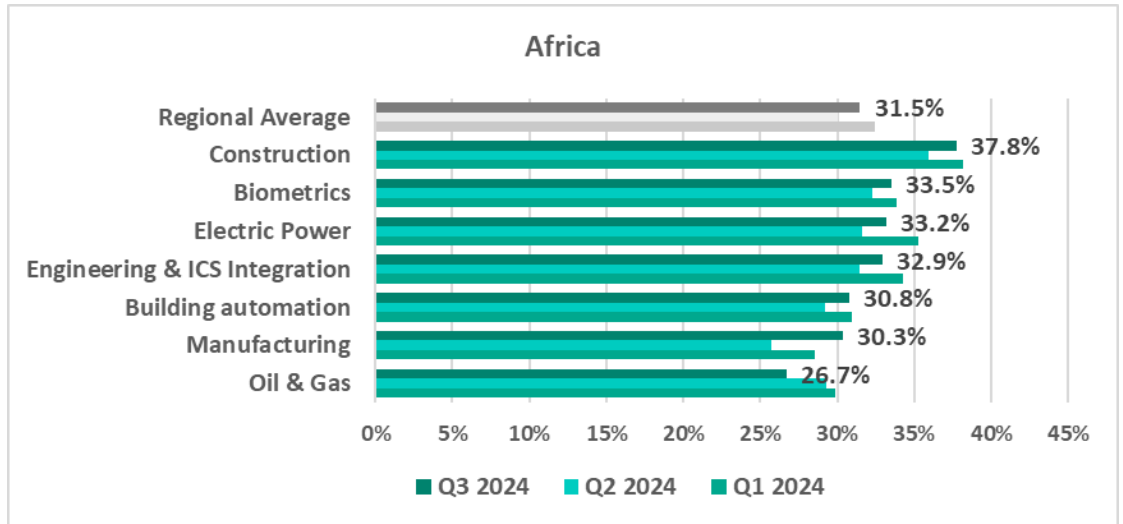


Industries

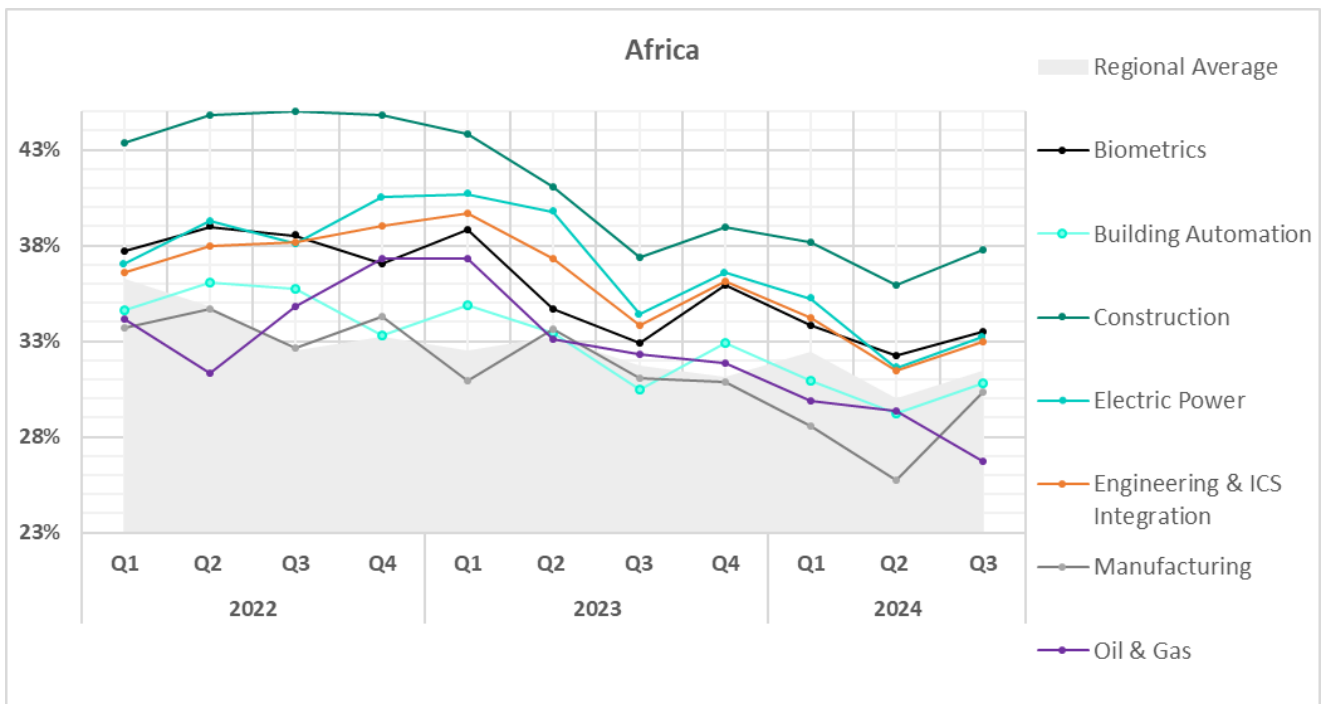
- The **most affected** industry in the region, as selected for this report, is **construction**.
- **Compared to the global averages**, the following industries had a significantly higher percentage of ICS computers with blocked malicious objects compared to the respective global averages:
 - Construction – 1.7 times higher
 - Manufacturing – 1.6 times higher
 - Engineering & ICS Integration – 1.5 times higher
 - Oil & Gas – 1.4 times higher
 - Electric Power – 1.4 times higher



- In **Q3 2024**, all selected sectors in the region, except oil & gas, exhibited an **increase** in the percentage of ICS computers on which malicious objects were blocked.





















- The selected sectors show positive dynamics in their **long-term trends** with occasional major fluctuations:



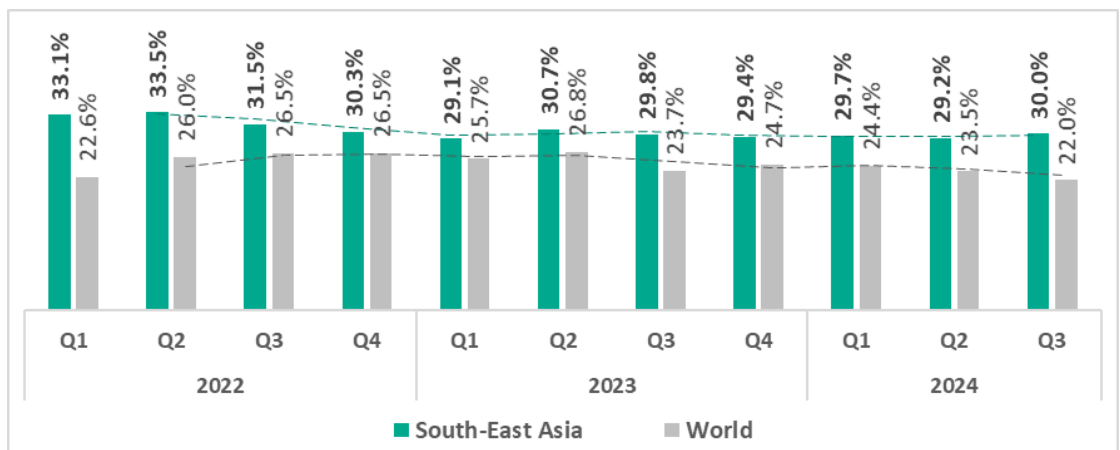
South-East Asia

Current threats

<p>N.1 IN THE REGION</p> <p>MALICIOUS SCRIPTS & PHISHING PAGES</p> <p>8.23%</p> <p> 1.2x increase in Q3 3rd globally in growth</p> <p> 1.3x above global average</p>	<p>N.2 IN THE REGION</p> <p>VIRUSES</p> <p>8.19%</p> <p> slight increase in Q3 2nd globally in growth</p> <p> 5.4x above global average 1st in the world</p>	<p>N.3 IN THE REGION</p> <p>DENYLISHED INTERNET RESOURCES</p> <p>7.81%</p> <p> 1.3x increase in Q3 3rd globally in growth</p> <p> 1.1x above global average 2nd in the world</p>
<p>SPYWARE</p> <p>5.55%</p> <p> decrease in Q3</p> <p> 1.4x above global average 3rd in the world</p>	<p>MALWARE FOR AUTOCAD</p> <p>2.93%</p> <p> decrease in Q3</p> <p> 6.9x above global average 1st in the world</p>	<p>MALICIOUS DOCUMENTS</p> <p>2.32%</p> <p> decrease in Q3</p> <p> 1.2x above global average</p>
<p>WORMS</p> <p>1.70 %</p> <p> decrease in Q3</p> <p> 1.3x above global average</p>	<p>THREATS FROM INTERNET</p> <p>13.92%</p> <p> 1.3x increase in Q3</p> <p> 1.4x above global average 1st in the world</p>	<p>THREATS FROM NETWROK FOLDERS</p> <p>0.29%</p> <p> decrease in Q3</p> <p> 2.6x above global average 2nd in the world</p>

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.
- In **Q3 2024**, the region showed an **increase** in the percentage of ICS computers on which malicious objects were blocked, compared to the previous quarter.



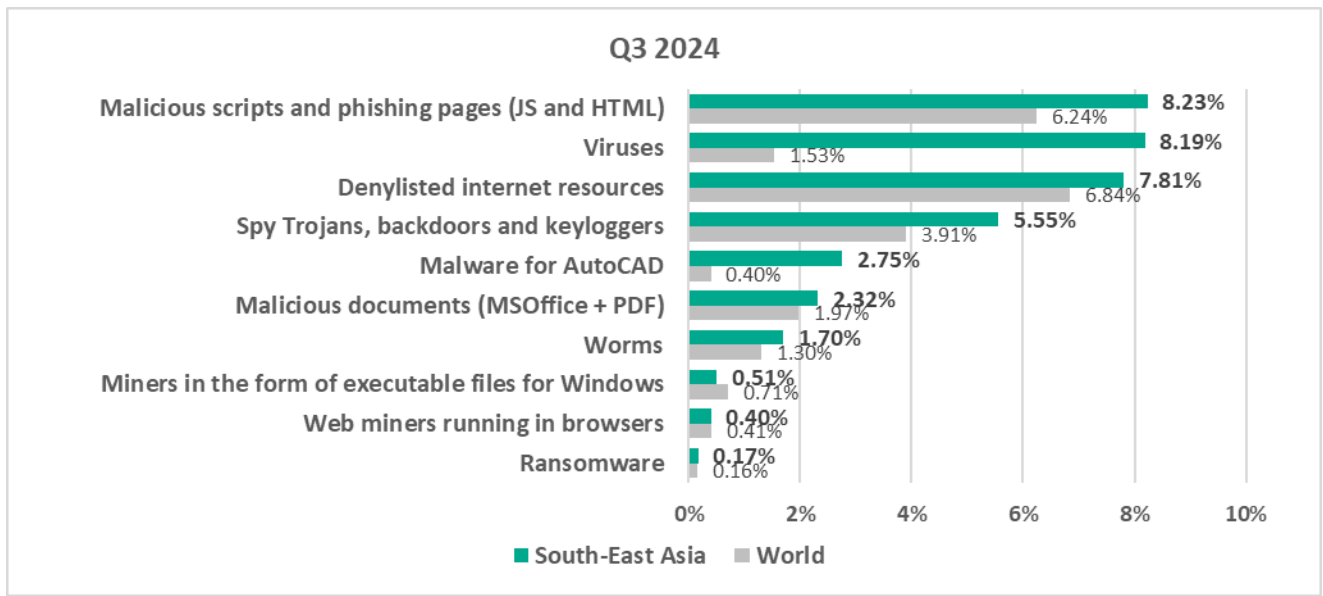
Comparative analysis

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: denylisted internet resources, threats from the internet, threats from network folders
- Third place: malicious spyware

Threat categories

- **Viruses came second** in the ranking of malware categories by percentage of ICS computers on which they were blocked. In South-East Asia, this percentage is 5.4 times higher than the global average.

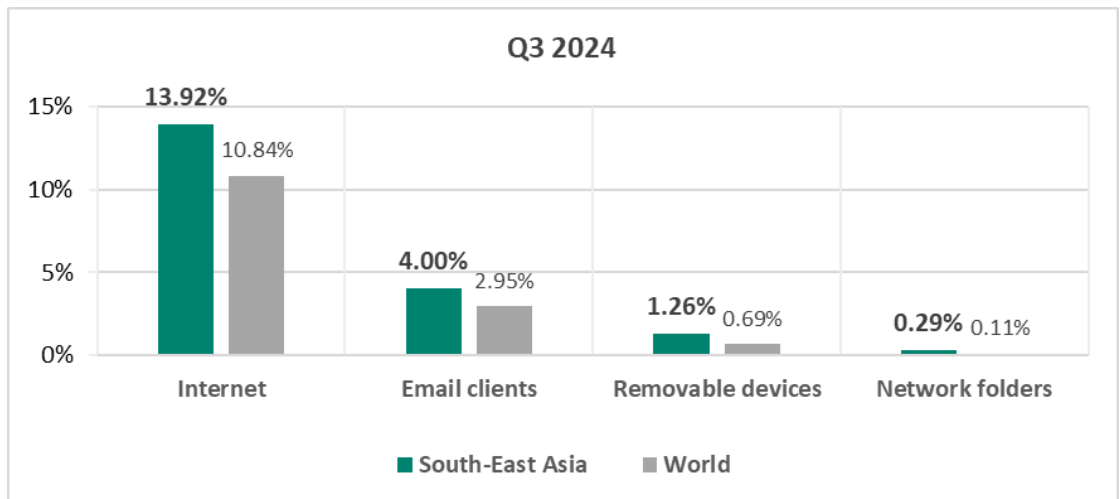


- **AutoCAD malware** is in **fifth place** in this ranking (the global percentage of ICS computers on which this malware was blocked is one of the lowest among all categories).
- **Compared to the global figures**, the region has a significantly **higher percentage** of ICS computers on which the following were blocked:
 - AutoCAD malware, 6.9 times higher
 - Viruses, 5.4 times higher
 - Spyware, 1.4 times higher
 - Malicious scripts and phishing pages, 1.3 times higher
 - Worms, 1.3 times higher
 - Malicious documents, 1.2 times higher

Threat sources

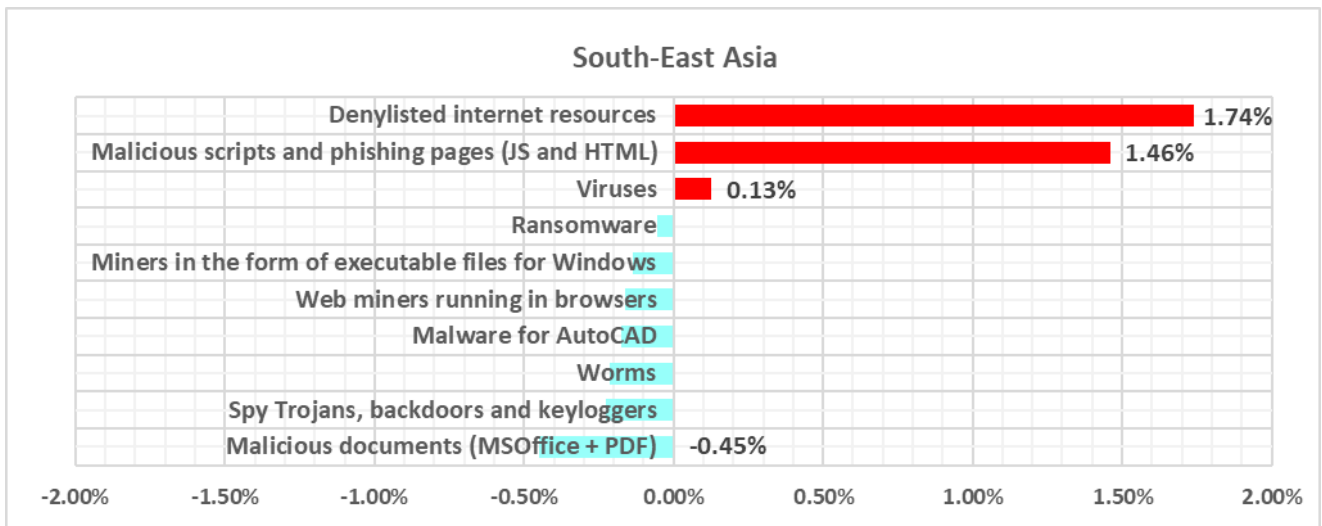
- The region ranked **second in the world** by percentage of ICS computers on which threats from **network folders** were blocked, exceeding the global average by 2.6 times.
- With regard to threats from the **internet**, the region ranked **second in the world**, exceeding the global average by 1.3 times.

- 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 Q3 2024.



Quarterly changes and trends

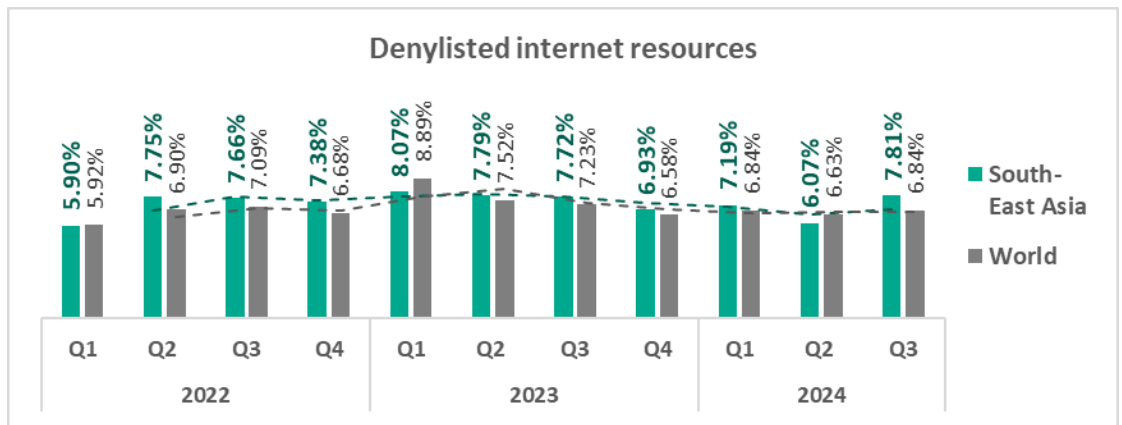
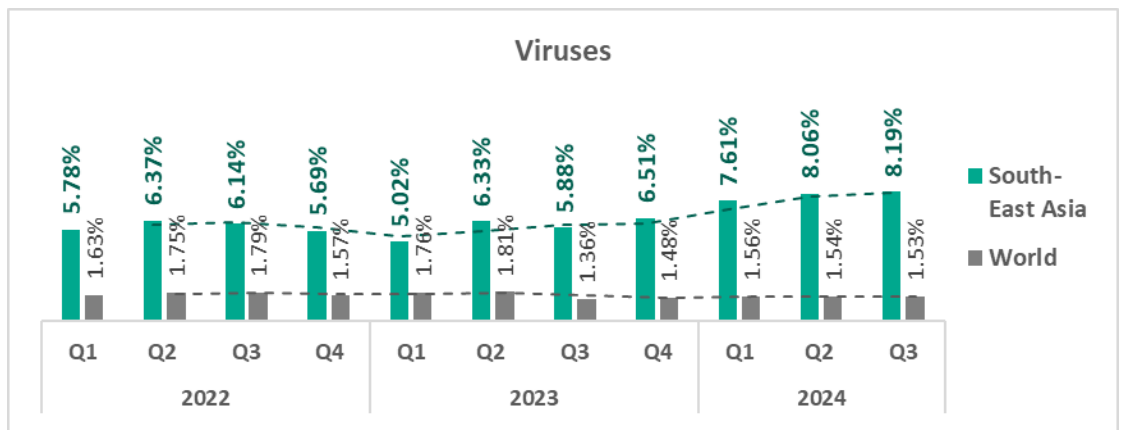
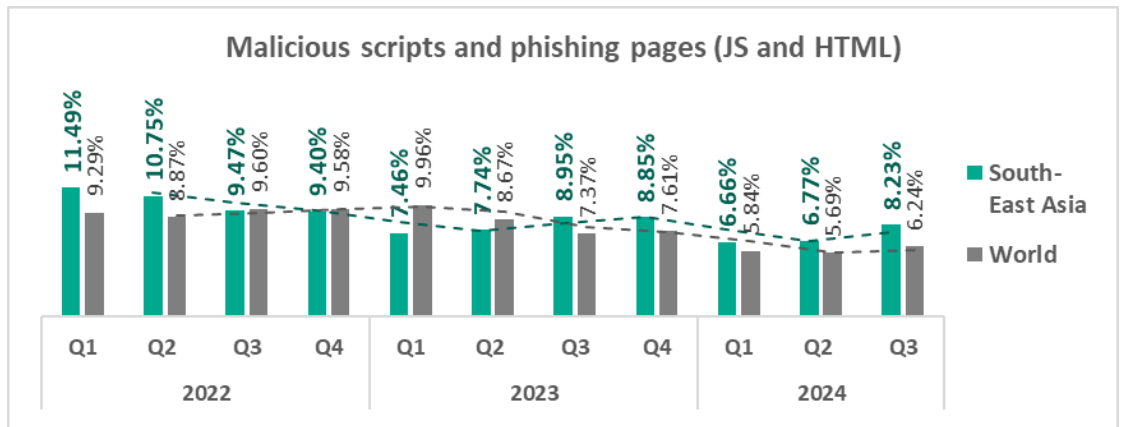
Threat categories

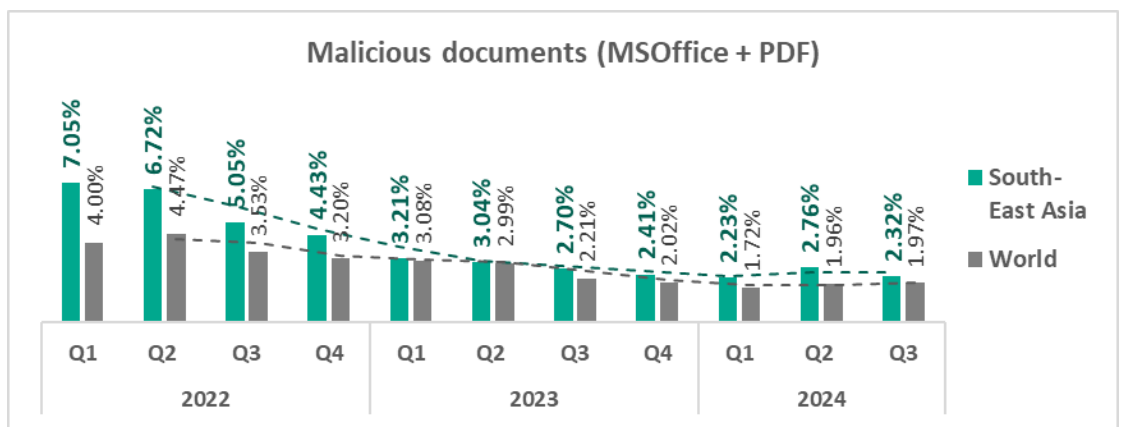
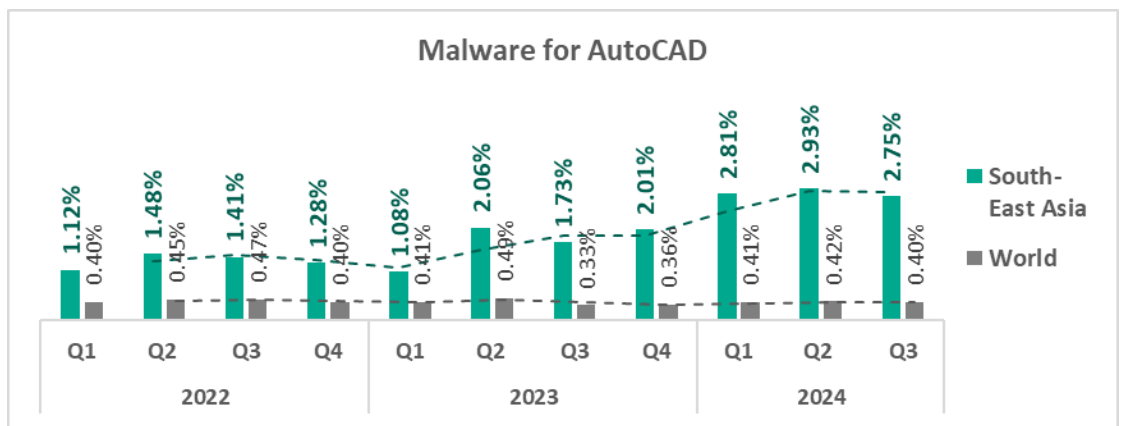
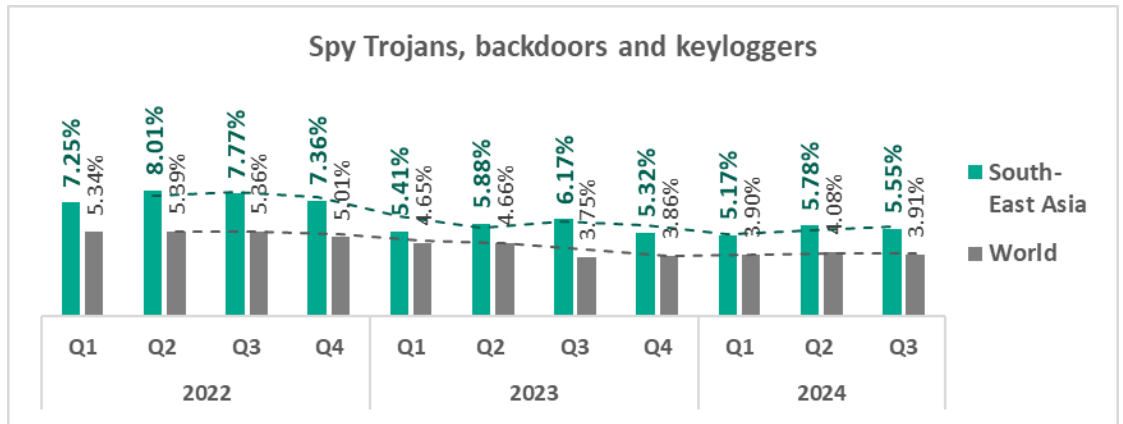


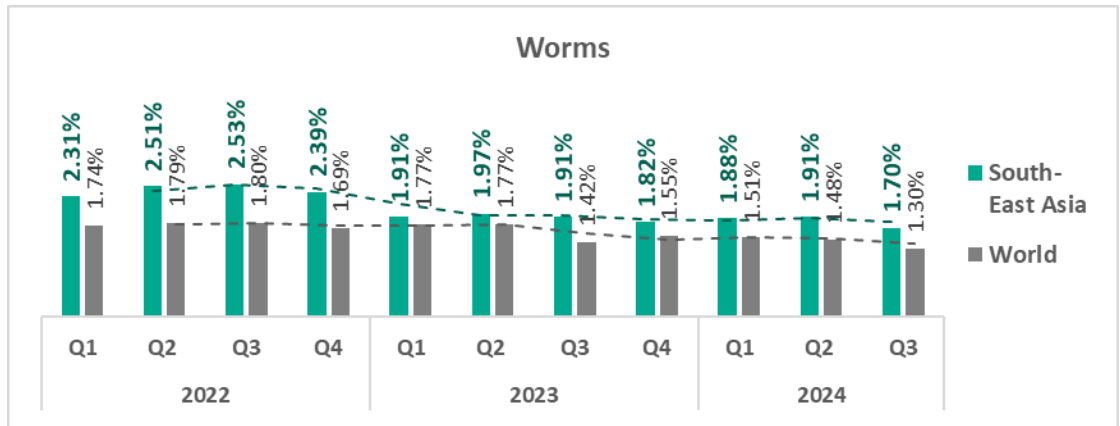
The **largest proportional increase** in Q3 2024 was in the percentage of ICS computers on which the following were blocked:

- Denylisted internet resources – by 1.3 times
- Malicious scripts and phishing pages – by 1.2 times

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





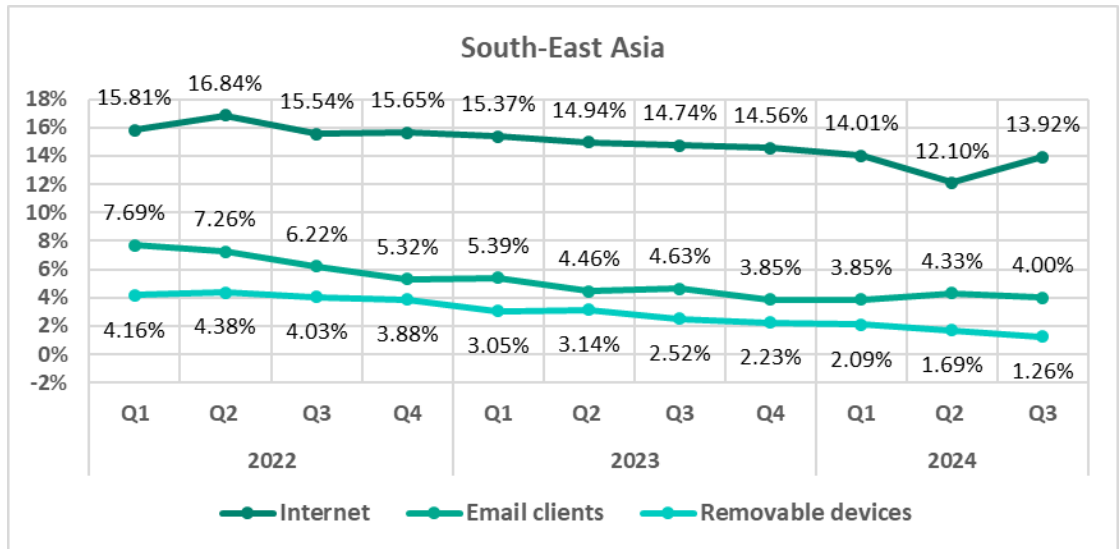


- The heatmap below illustrates changes in the ranking of threat categories in the region since the beginning of 2022. **Malicious scripts and phishing** moved up from second to first place in Q3 2024, while **viruses** dropped from first place to second.

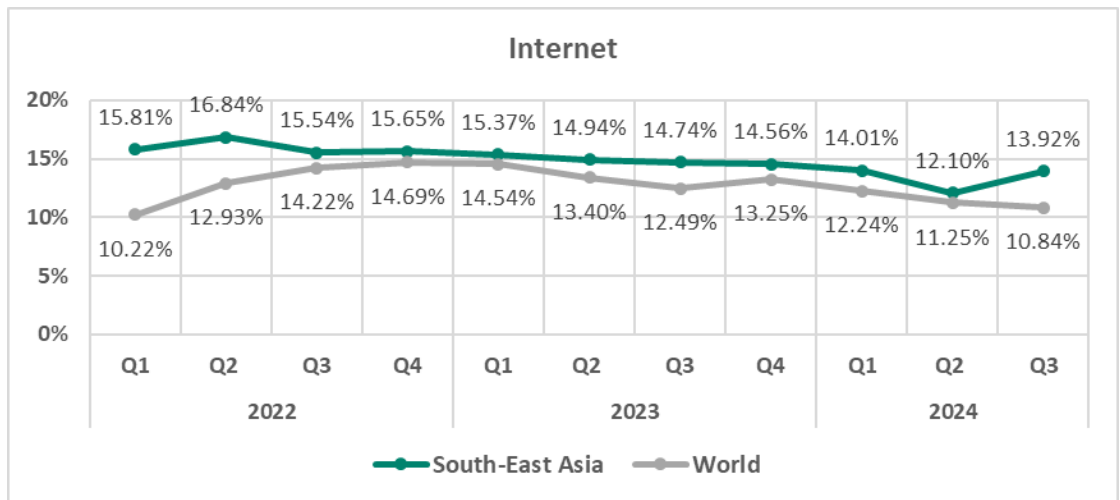
South-East Asia	2022				2023				2024		
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3
Malicious scripts and phishing pages (JS and HTML)	1	1	1	1	2	2	1	1	3	2	1
Viruses	5	5	4	4	4	3	4	3	1	1	2
Denylisted internet resources	4	3	3	2	1	1	2	2	2	3	3
Spy Trojans, backdoors and keyloggers	2	2	2	3	3	4	3	4	4	4	4
Malware for AutoCAD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

Threat sources

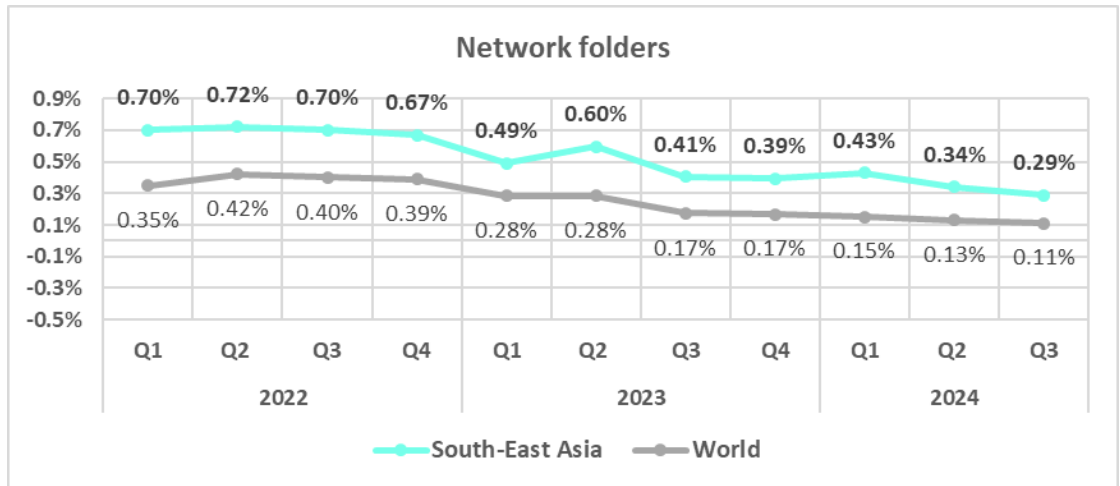
- In terms of **quarterly changes**, the all threat sources, except internet, showed a **decrease** in percentage of ICS computers on which malicious objects were blocked.



- Threats from the **internet increased** 1.3 times, in contrast to the global average trend.

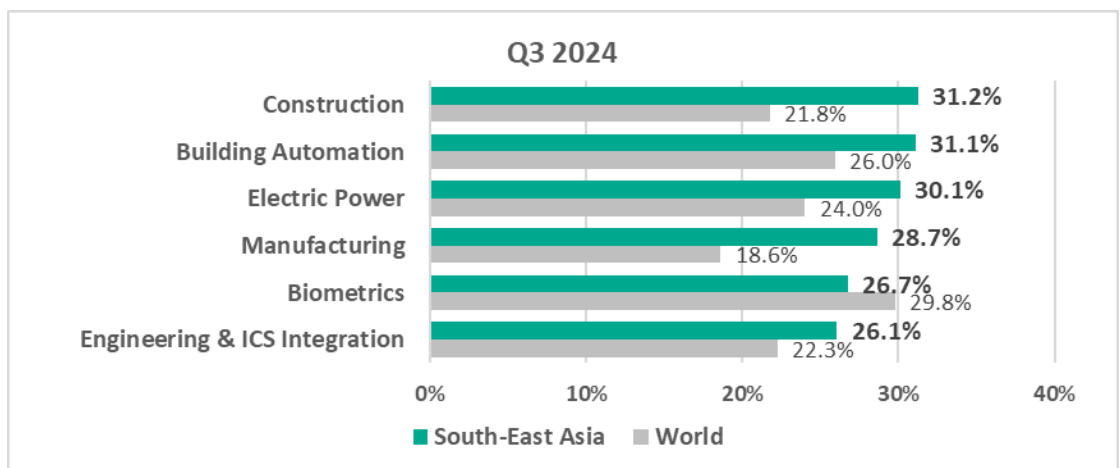


- The trend for threats from **network folders** has been on average **twice as high as the global average** throughout the observed period.

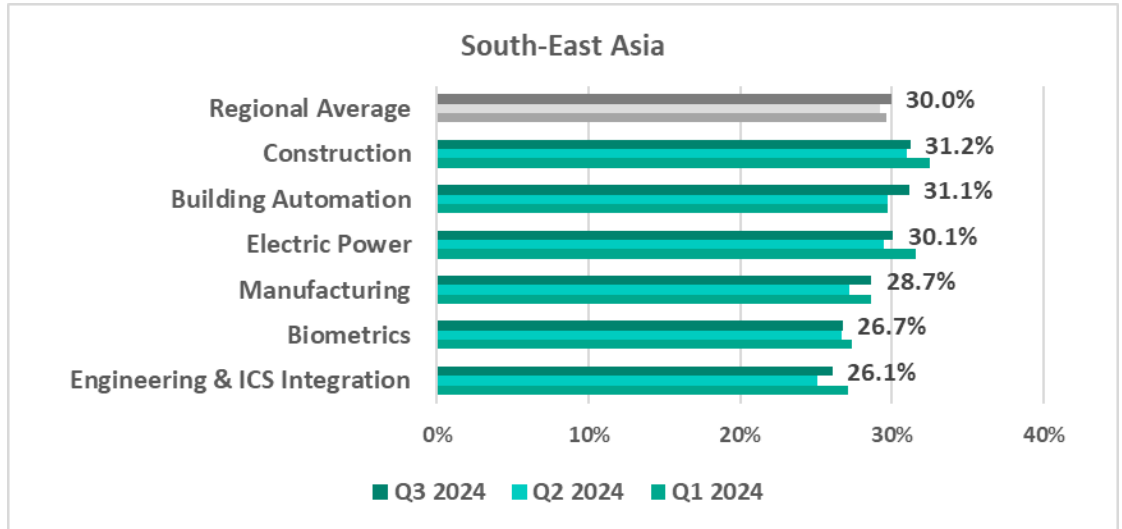


Industries

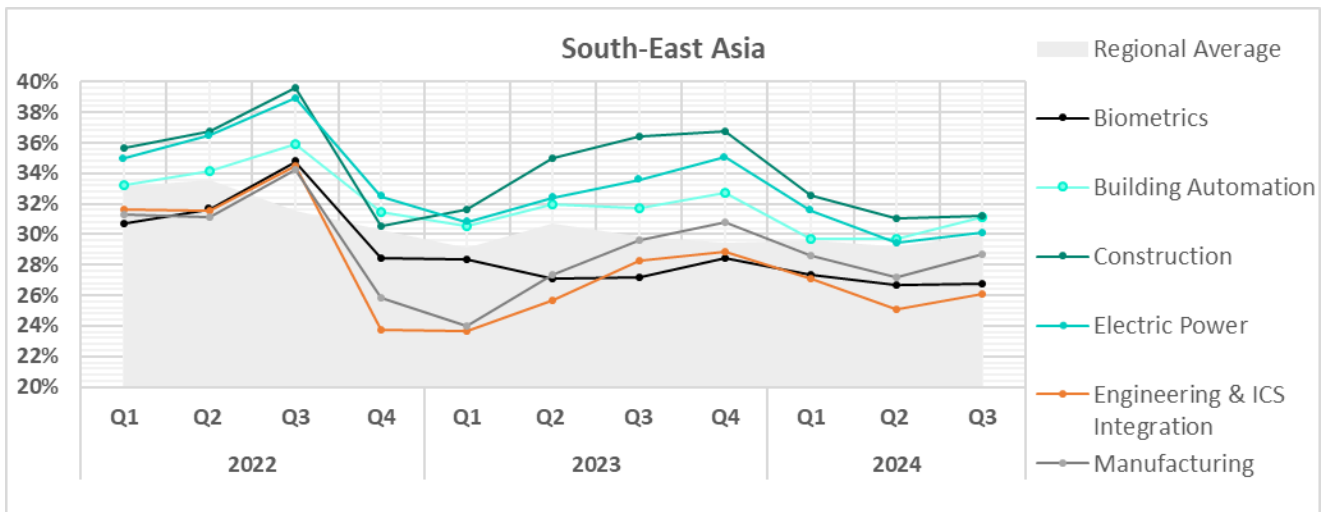
- The **most affected** industries in the region, as selected for this report, are:
 - Construction
 - Building automation
- **Compared to the global averages**, the following industries had a significantly **higher percentage** of ICS computers on which malicious objects were blocked:
 - Manufacturing – 1.5 times higher
 - Construction – 1.4 times
 - Electric power – 1.3 times
 - Building automation – 1.2 times higher
 - Engineering and ICS integration – 1.2 times



- In **Q3 2024**, all selected sectors experienced an **increase** in the percentage of ICS computers where malicious objects were blocked.

























- 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.



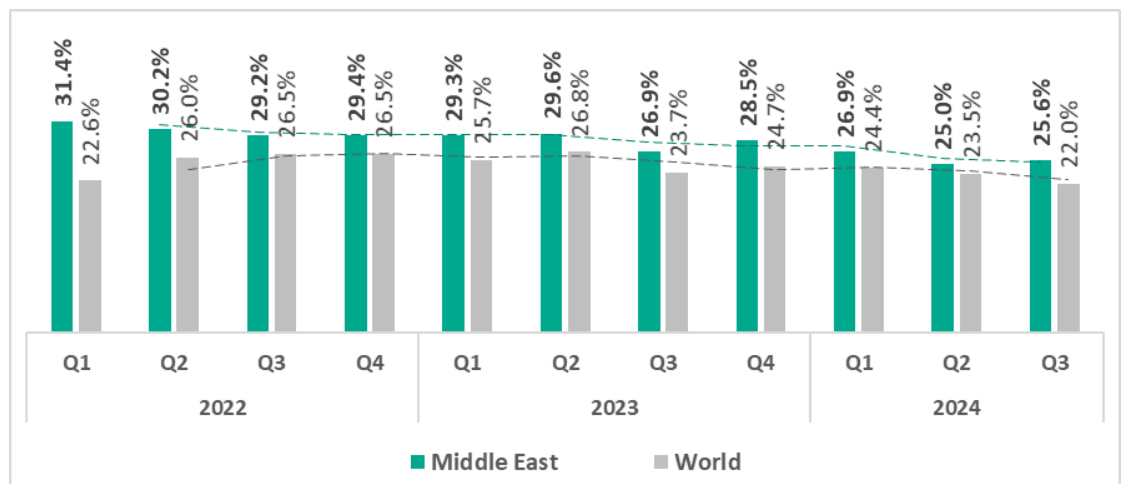
Middle East

Current threats

<p>N.1 IN THE REGION</p> <p>MALICIOUS SCRIPTS & PHISHING PAGES</p> <p>7.83%</p> <p> 1.1x increase in Q3</p> <p> 1.3x above global average</p>	<p>N.2 IN THE REGION</p> <p>DENYLISHED INTERNET RESOURCES</p> <p>7.30%</p> <p> 1.5x increase in Q3</p> <p>2nd globally in growth</p> <p> 1.1x above global average</p> <p>3rd in the world</p>	<p>N.3 IN THE REGION</p> <p>SPYWARE</p> <p>6.22%</p> <p> decrease in Q3</p> <p> 1.6x above global average</p> <p>2nd in the world</p>
<p>MALICIOUS DOCUMENTS</p> <p>2.53%</p> <p> 1.1x increase in Q3</p> <p>3rd globally in growth</p> <p> 1.3x above global average</p> <p>3rd in the world</p>	<p>WORMS</p> <p>2.17%</p> <p> decrease in Q3</p> <p> 1.7x above global average</p> <p>3rd in the world</p>	<p>VIRUSES</p> <p>2.04%</p> <p> slight increase in Q3</p> <p> 1.3x above global average</p>
<p>WEB MINERS</p> <p>0.66%</p> <p> decrease in Q3</p> <p> 1.6x above global average</p> <p>1st in the world</p>	<p>RANSOMWARE</p> <p>0.29%</p> <p> decrease in Q3</p> <p> 1.8x above global average</p> <p>1st in the world</p>	
<p>THREATS FROM</p> <p>INTERNET</p> <p>12.32%</p> <p> 1.1x increase in Q3</p> <p>3rd globally in growth</p> <p> 1.1x above global average</p> <p>3rd in the world</p>	<p>THREATS FROM</p> <p>EMAIL CLIENTS</p> <p>4.95%</p> <p> slight increase in Q3</p> <p>3rd globally in growth</p> <p> 1.7x above global average</p> <p>3rd in the world</p>	<p>THREATS FROM</p> <p>REMOVABLE DEVICES</p> <p>1.11%</p> <p> decrease in Q3</p> <p> 1.6x above global average</p>

Overall

- **Third** place in the global ranking by percentage of ICS computers on which malicious objects were blocked in Q3 2024.
- The percentage of ICS computers where malicious objects were blocked remains **higher than the global average** throughout the observed period.
- In **Q3 2024**, the region showed an **increase** in the percentage of ICS computers on which malicious objects were blocked compared to the previous quarter.



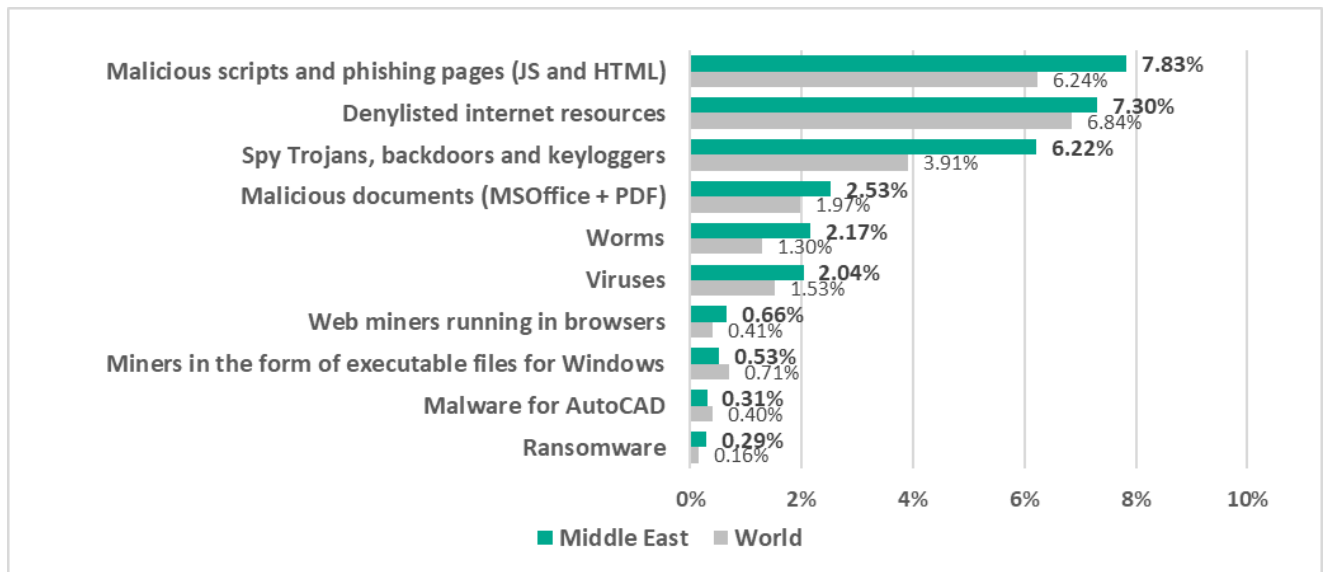
Comparative analysis

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

- First place: web miners, ransomware
- Second place: spyware
- Third place: denylisted internet resources, malicious documents, worms, threats from email clients and internet.

Threat categories

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

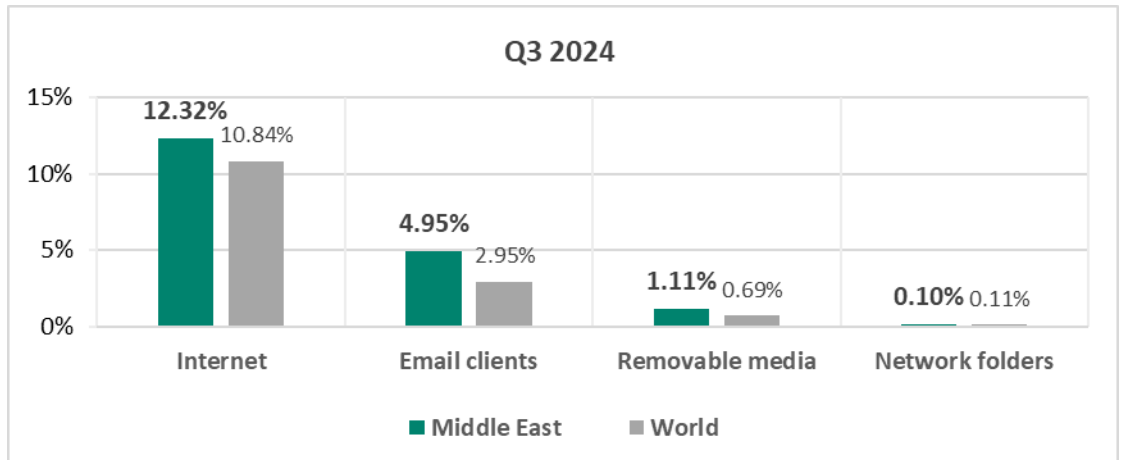


Specifically, the following threat categories showed **significantly higher** values:

- Ransomware, 1.8 times higher
- Worms, 1.7 times higher
- Spyware, 1.6 times higher
- Web miners, 1.6 times higher
- Viruses, 1.3 times higher
- Malicious scripts and phishing pages, 1.3 times higher
- Malicious documents, 1.3 times higher

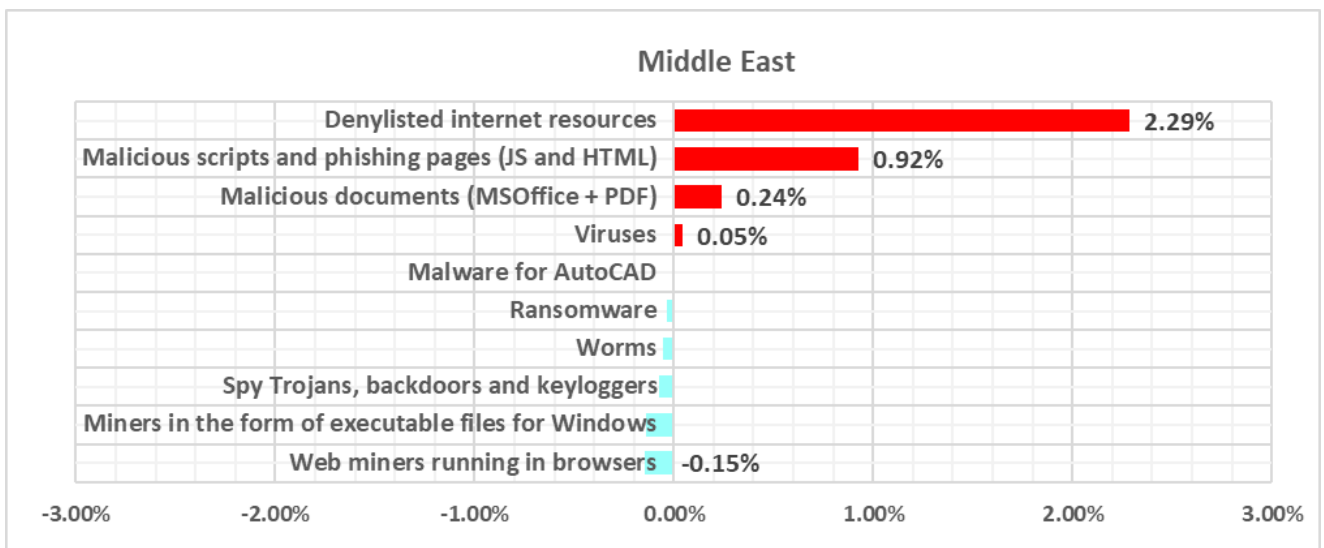
Threat sources

- The region ranked **third in the world** by percentage of ICS computers on which threats from **internet** and **email clients** were blocked, exceeding the global average by a factor of 1.1 and 1.7 respectively.
- The percentage of computers on which threats from **removable devices** were blocked **exceeded the global average** by 1.6 times in Q3 2024.



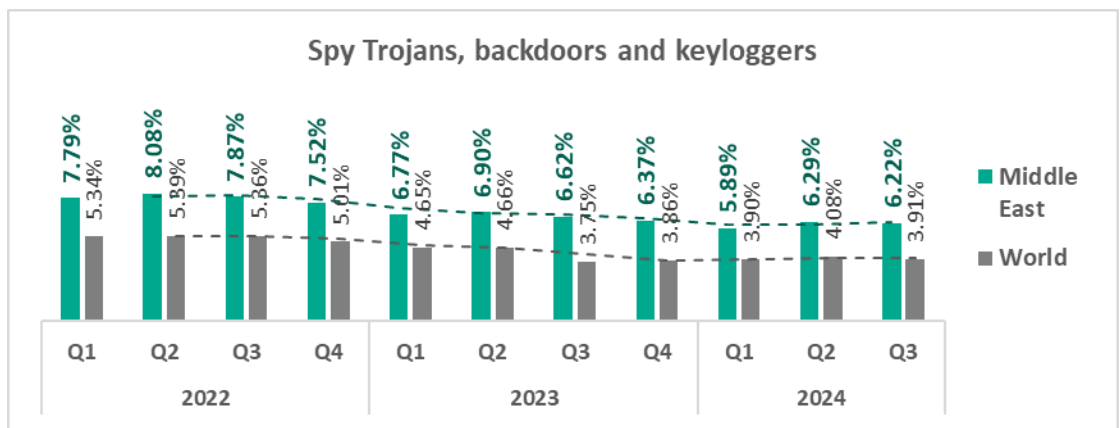
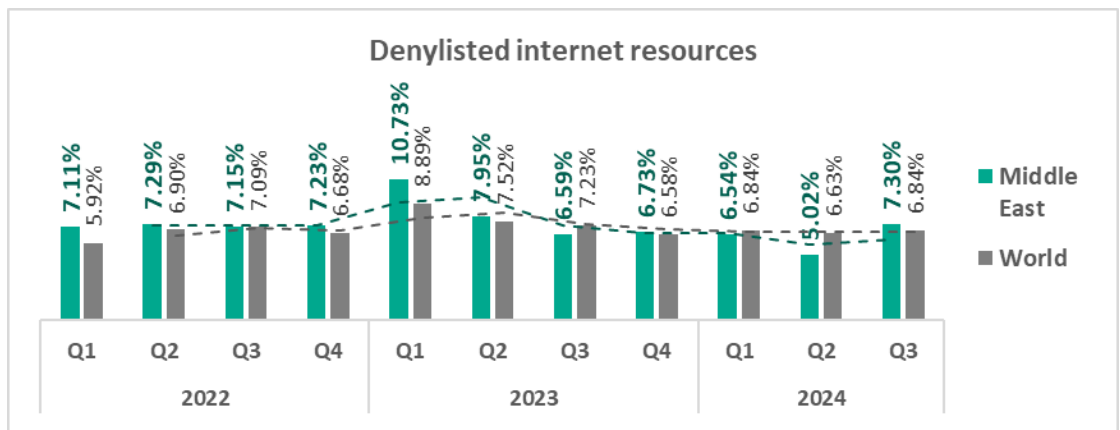
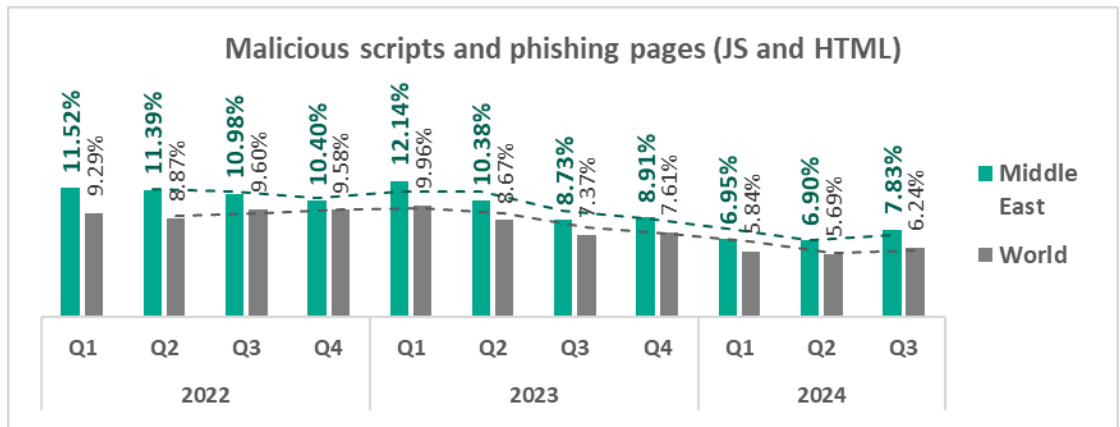
Quarterly changes and trends

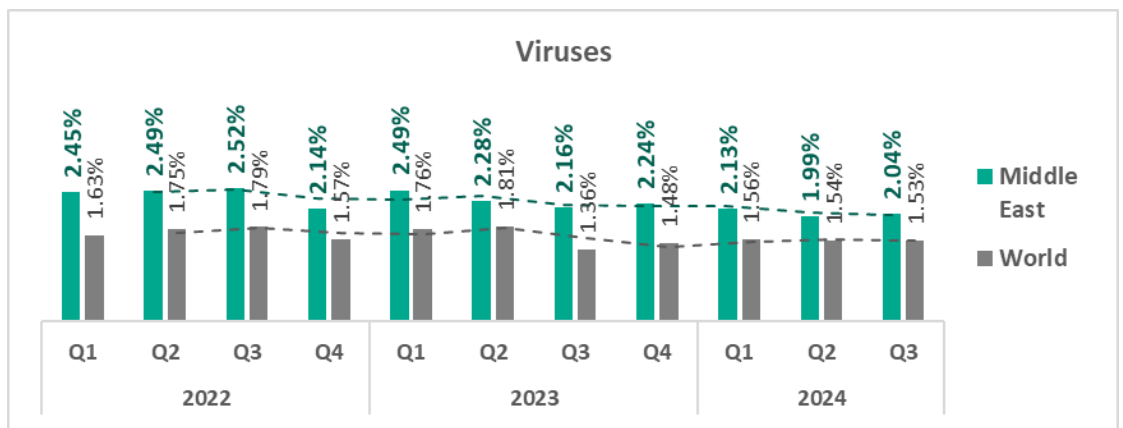
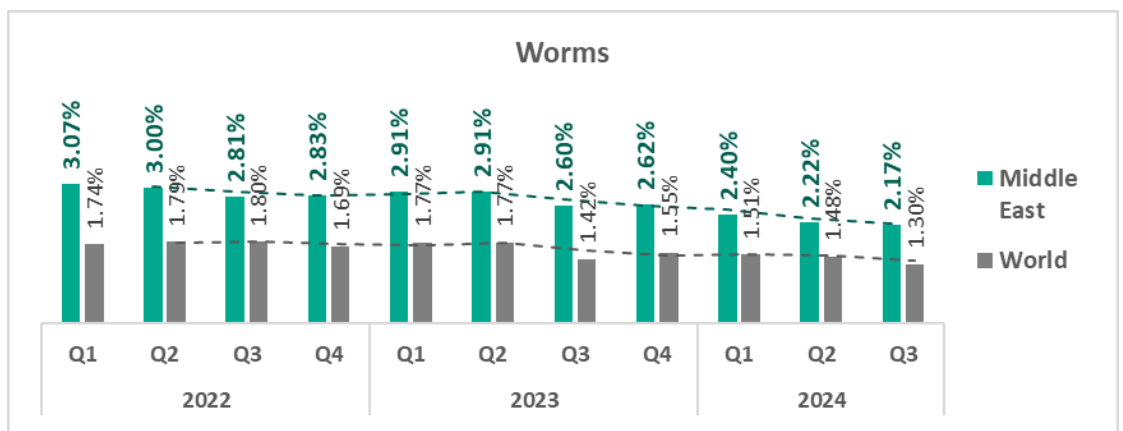
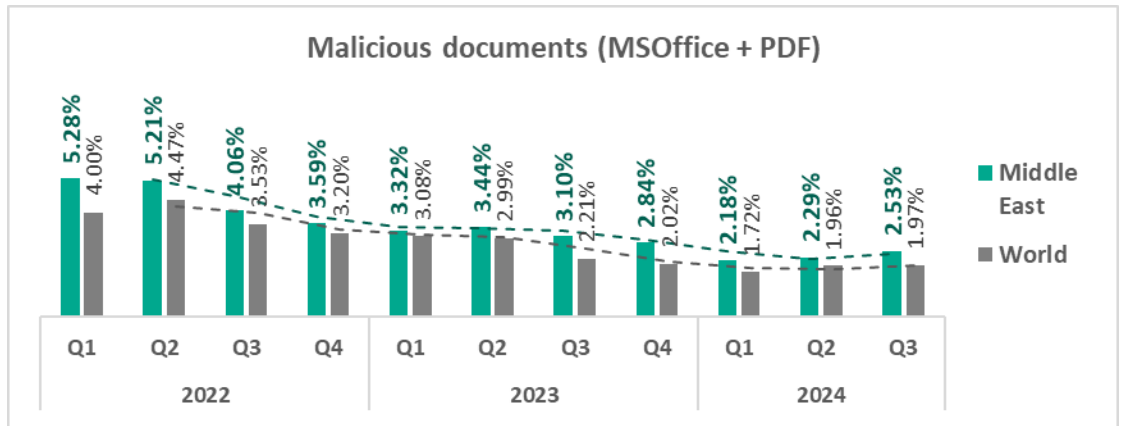
Threat categories

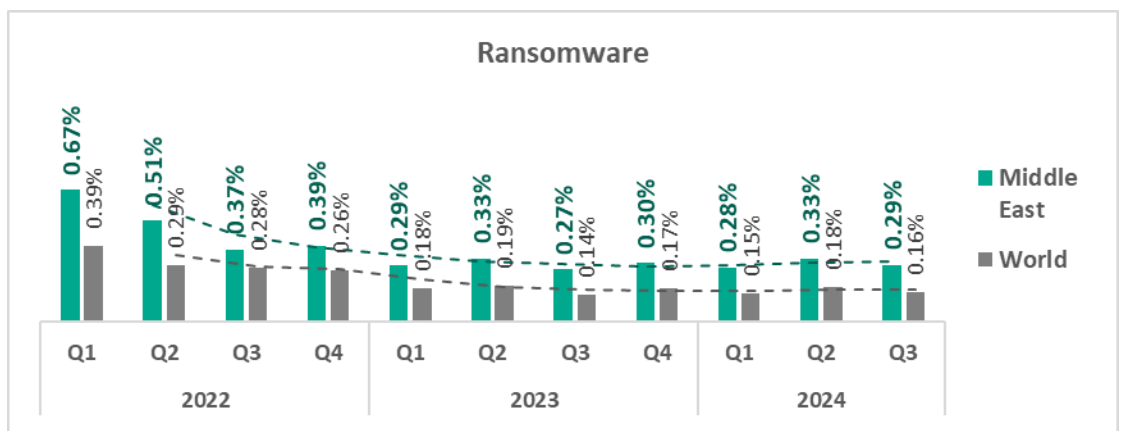
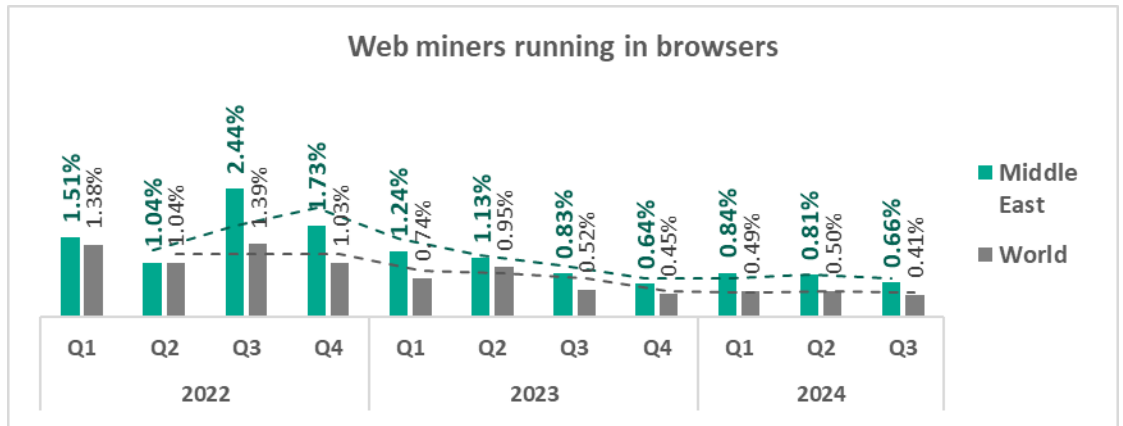


- The **largest proportional increase** in Q3 2024 was in the percentage of ICS computers on which the following were blocked:
 - Denylisted internet resources – by 1.5 times
 - Malicious scripts and phishing pages – by 1.1 times
 - Malicious documents – by 1.1 times

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



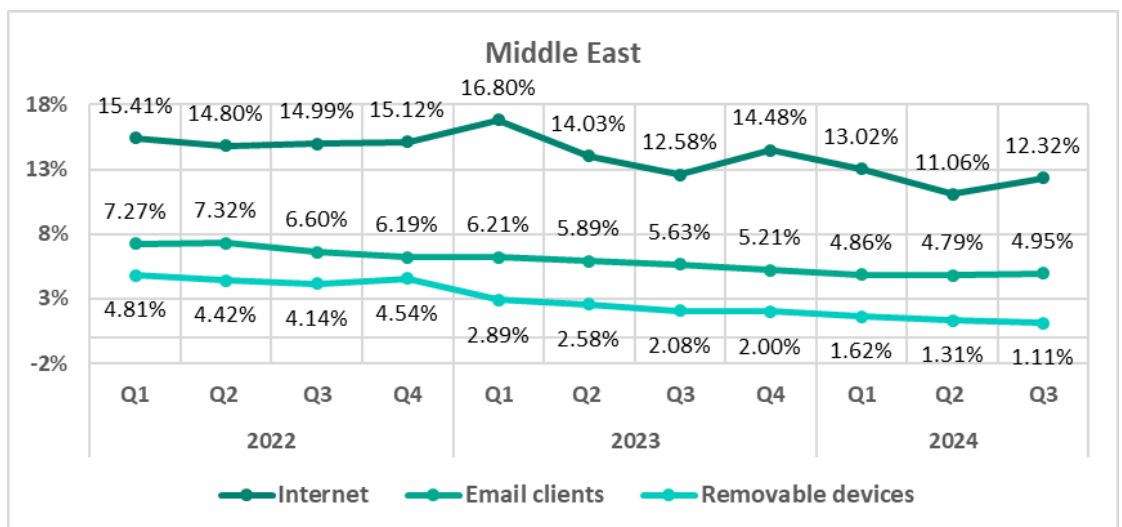




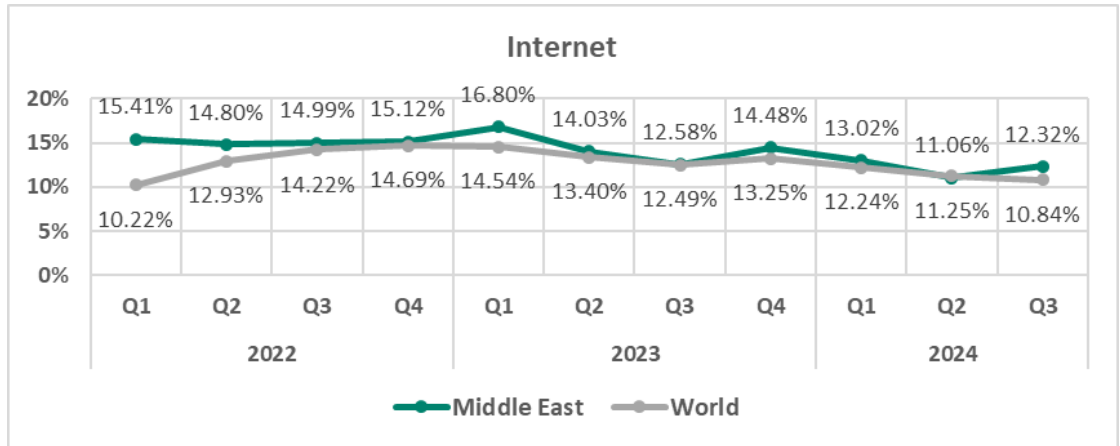
- The heatmap below illustrates changes in the rankings of threat categories in the region since the beginning of 2022. **Malicious scripts and phishing pages** have been the leading threat category throughout the observed period. **Denylisted internet resources** returned from third to second place in Q3 2024.

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

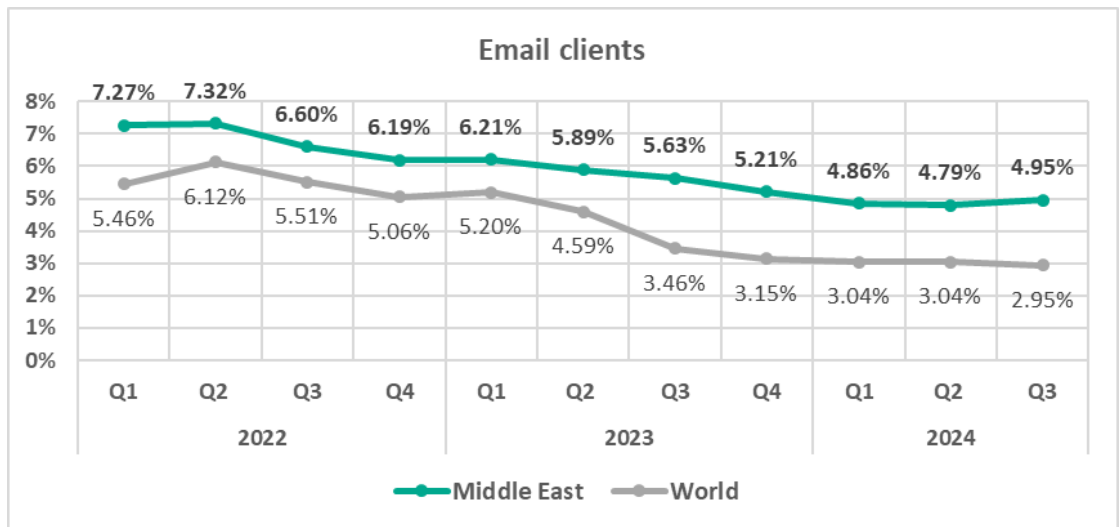
Threat sources



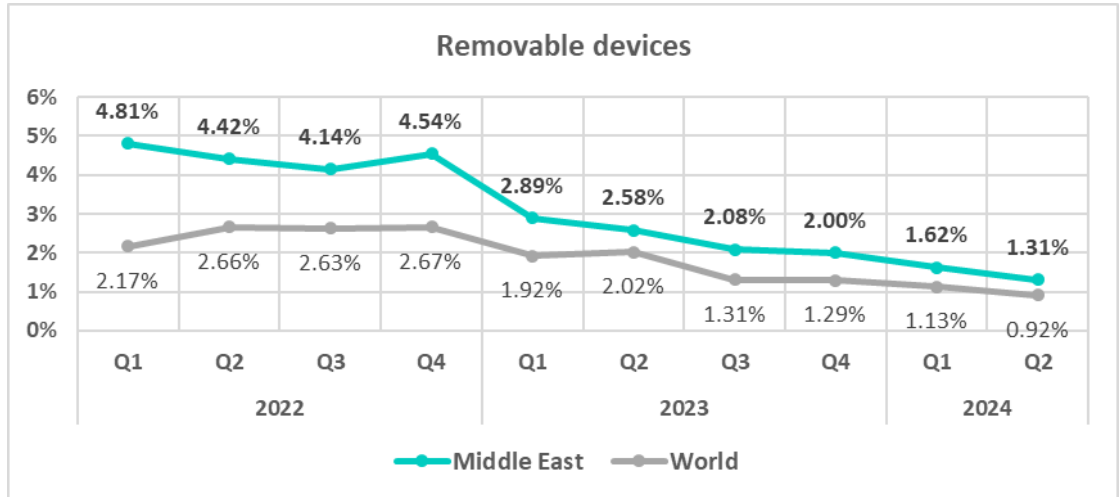
- Threats from the **internet** remained slightly **above the global average** throughout the observed period, except in Q2 2024. The trend **increased in Q3 2024** following a decline in the previous two quarters.



- The trend for threats from **email clients** has been **above the global average** throughout the observed period. The **gap widened** in Q3 2024.

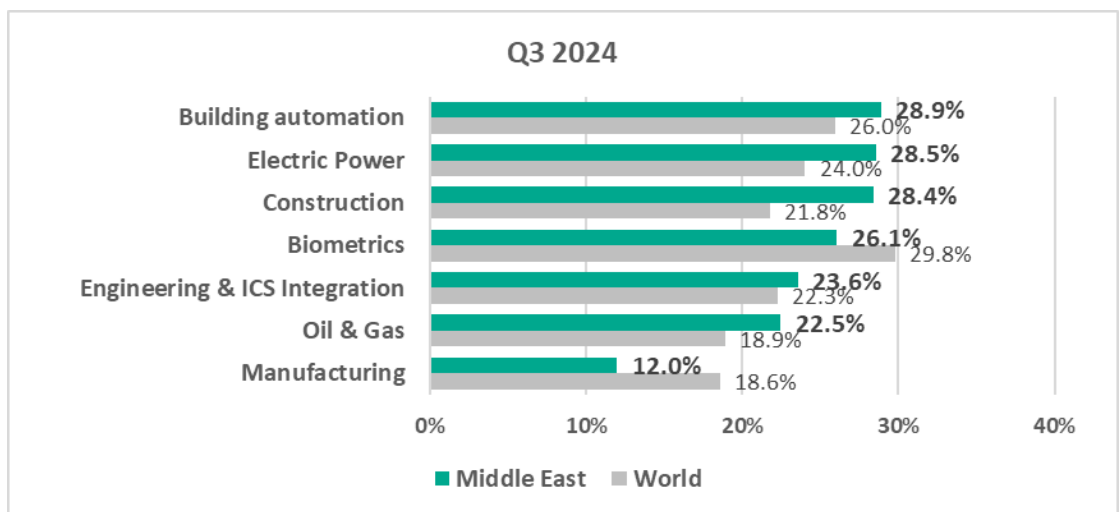


- Threats from **removable devices** have been **above the global average** throughout the observed period.

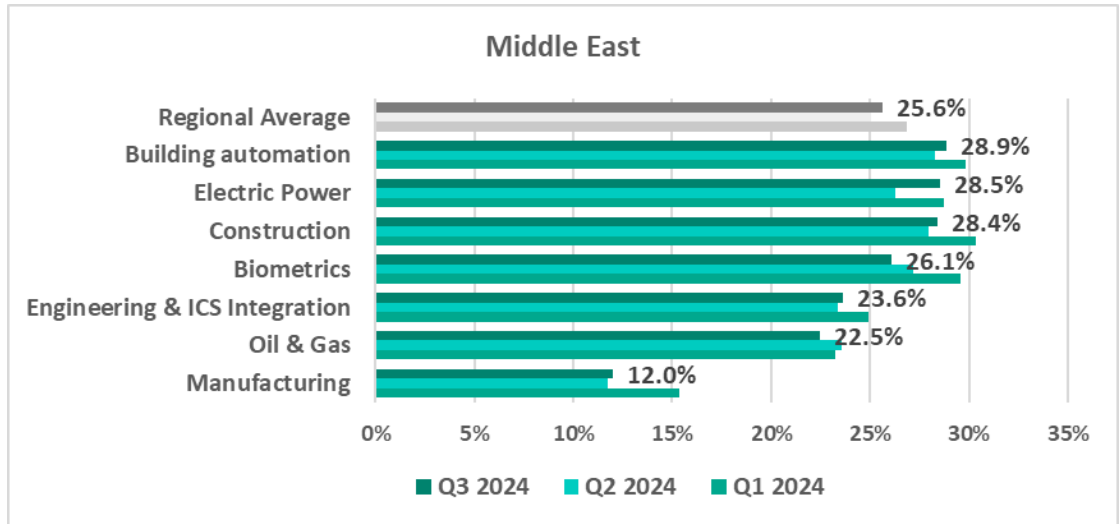


Industries

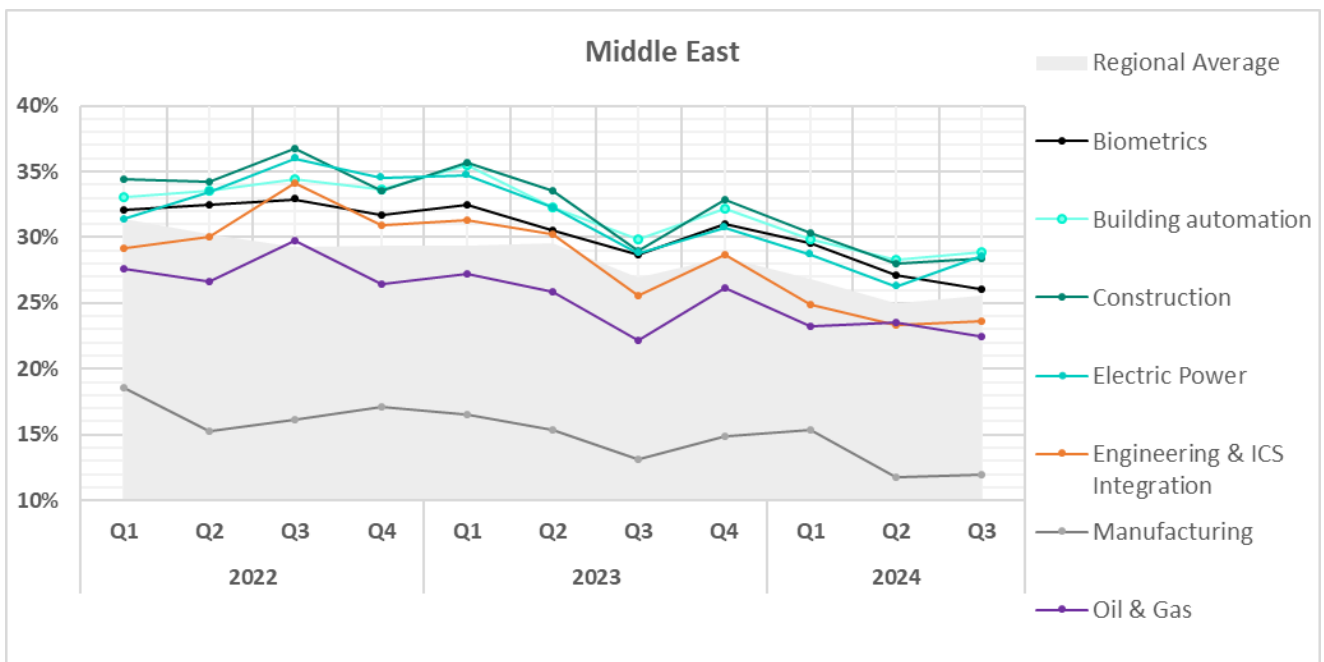
- The **most affected** industry in the region, as selected for this report, was **building automation**.
- **From a global perspective**, the following industries saw a **higher percentage** of ICS computers on which malicious objects were blocked:
 - Construction – 1.3 times higher
 - Electric power – 1.2 times higher
 - Oil and gas – 1.2 times higher
 - Building automation – 1.1 times higher
 - Engineering & ICS Integration – 1.1 times higher



- In **Q3 2024**, the **electric power** sector exhibited the **most noticeable increase** (by a factor of 1.1) in the percentage of ICS computers on which malicious objects were blocked, compared to the previous quarter.
















- Despite occasional fluctuations, the **trends** in the selected sectors show overall **positive dynamics**.



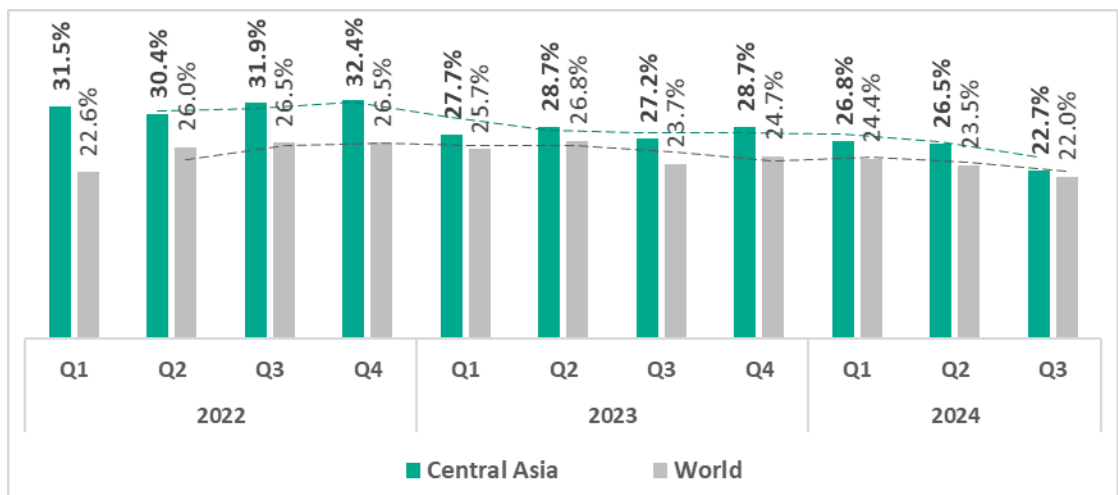
Central Asia

Current threats

<p>N.1 IN THE REGION</p> <p>DENYLISTED INTERNET RESOURCES</p> <p>6.43%</p> <p> decrease in Q3</p>	<p>N.2 IN THE REGION</p> <p>SPYWARE</p> <p>4.11%</p> <p> decrease in Q3</p> <p> 1.2x above global average</p>	<p>N.3 IN THE REGION</p> <p>MALICIOUS SCRIPTS & PHISHING PAGES</p> <p>3.90%</p> <p> decrease in Q3</p>
<p>WORMS</p> <p>2.80%</p> <p> slight increase in Q3</p> <p> 2.2x above global average 2nd in the world</p>	<p>EXECUTABLE MINERS</p> <p>1.62%</p> <p> slight increase in Q3</p> <p> 2.3x above global average 1st in the world</p>	<p>RANSOMWARE</p> <p>0.17%</p> <p> decrease in Q3</p> <p> 1.1x above global average</p>
<p>THREATS FROM INTERNET</p> <p>9.67%</p> <p> decrease in Q3</p>	<p>THREATS FROM REMOVABLE DEVICES</p> <p>1.37%</p> <p> decrease in Q3</p> <p> 1.4x above global average</p>	

Overall

- **Fourth** place in the global ranking by percentage of ICS computers on which malicious objects were blocked.
- In **Q3 2024**, the region showed significant **decline** (by 1.2 times) in the percentage of ICS computers on which malicious objects were blocked compared to the previous quarter.
- The indicator remains **higher than the global average**, although in **Q3 2024**, the **gap was the smallest** throughout the observed period.

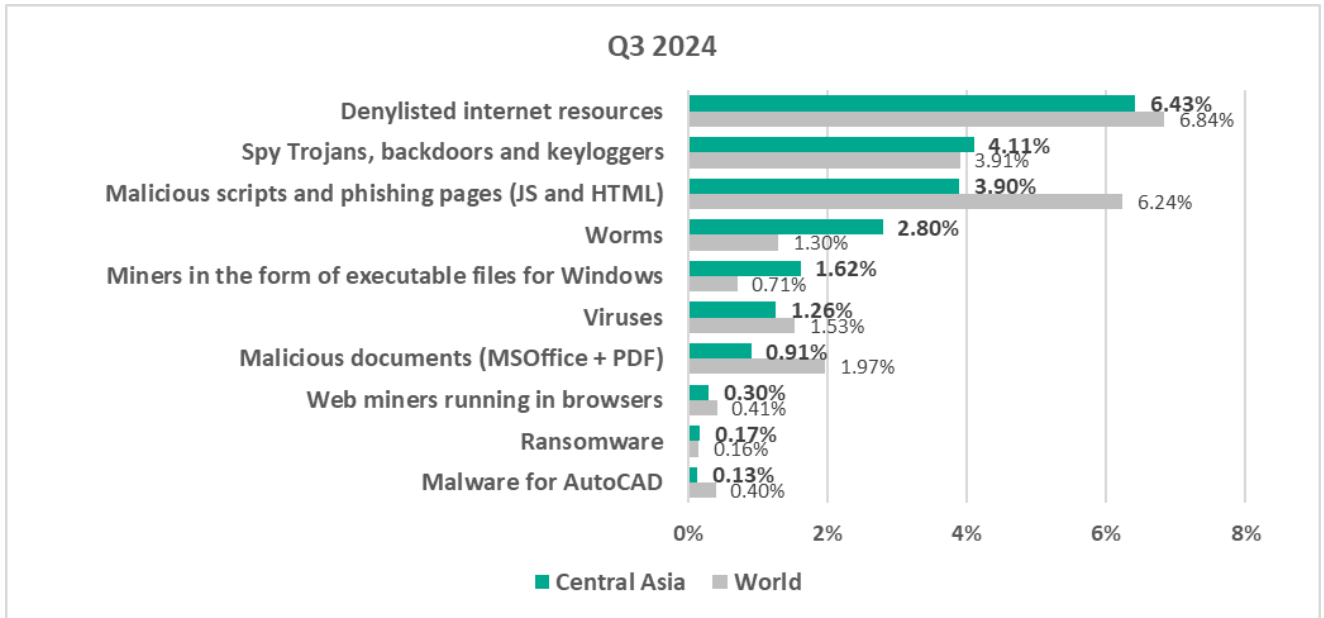


Comparative analysis

In Q3 2024, Central Asia occupied **leading positions** among regions by percentage of ICS computers on which the following were blocked:

- First place: miner executable files for Windows
- Second place: worms

Threat categories

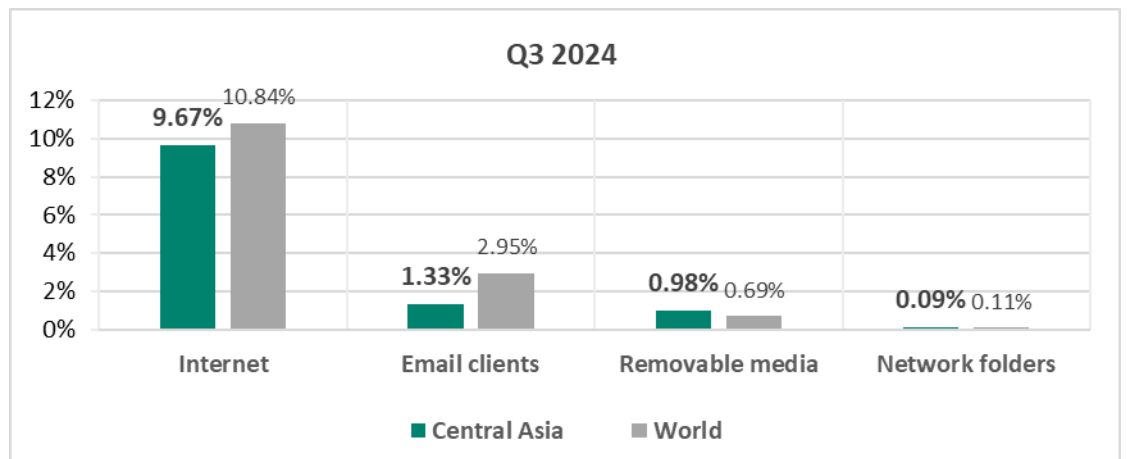


Compared to the global average, the region has a higher percentage of ICS computers on which the following were blocked:

- Miners in the form of executable files for Windows, 2.3 times higher
- Worms, 2.2 times higher
- Ransomware, 1.1 times higher
- Spyware, 1.1 times higher

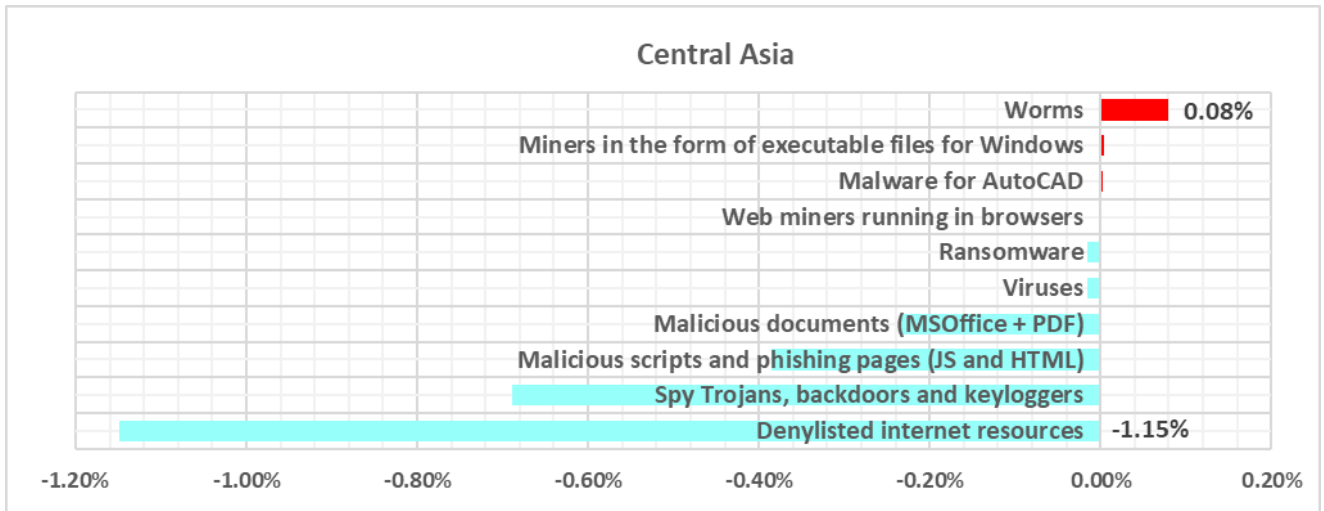
Threat sources

- The percentage of ICS computers on which threats from **removable devices** were blocked **exceeded the global average** by 1.4 times in Q3 2024.

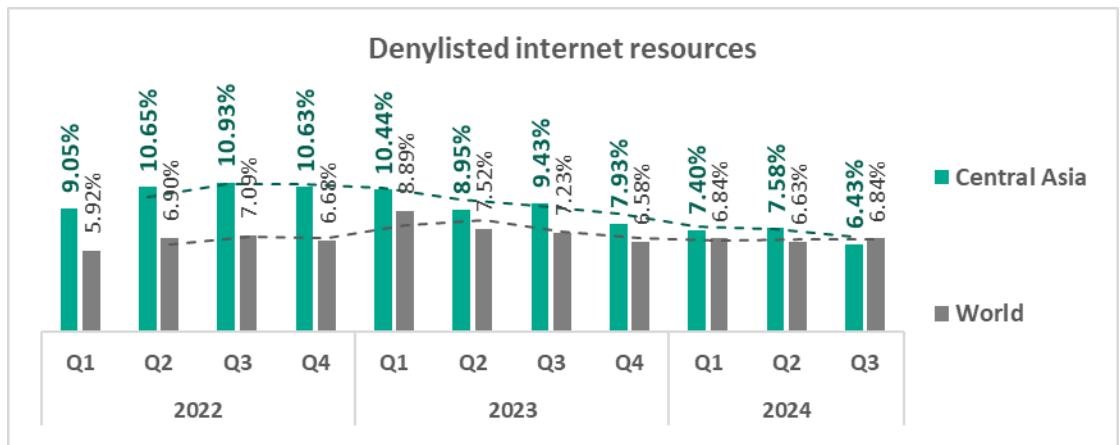


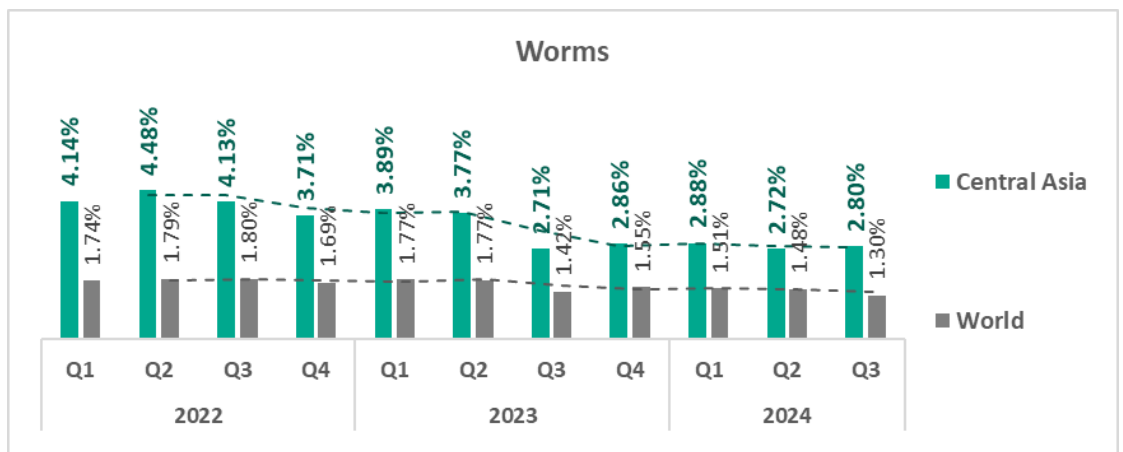
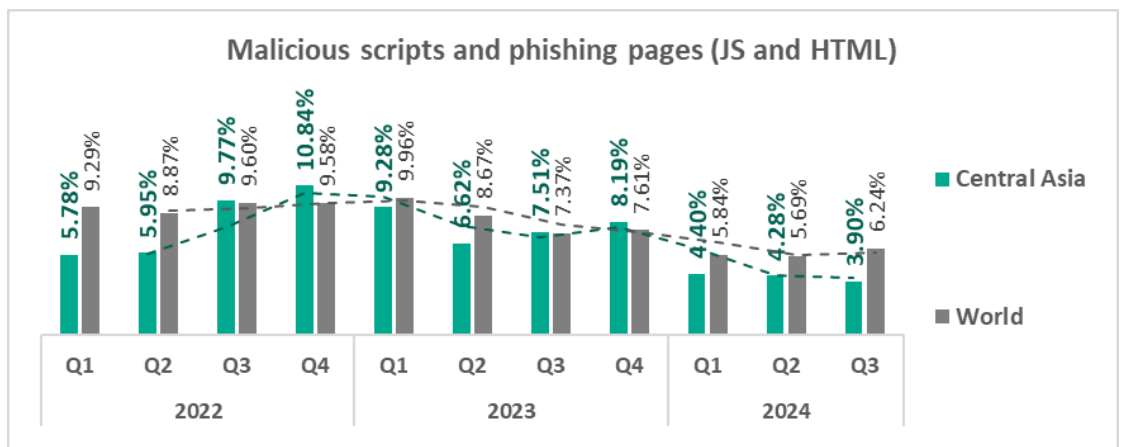
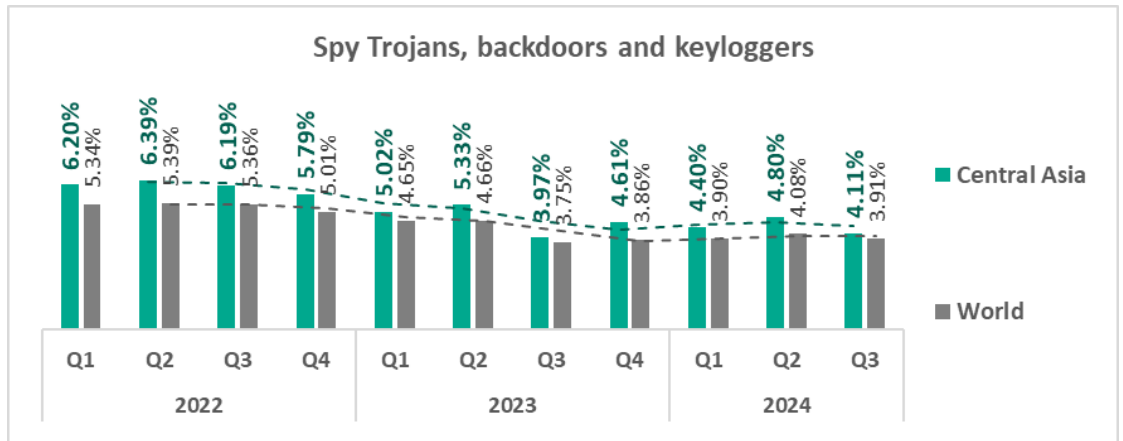
Quarterly changes and trends

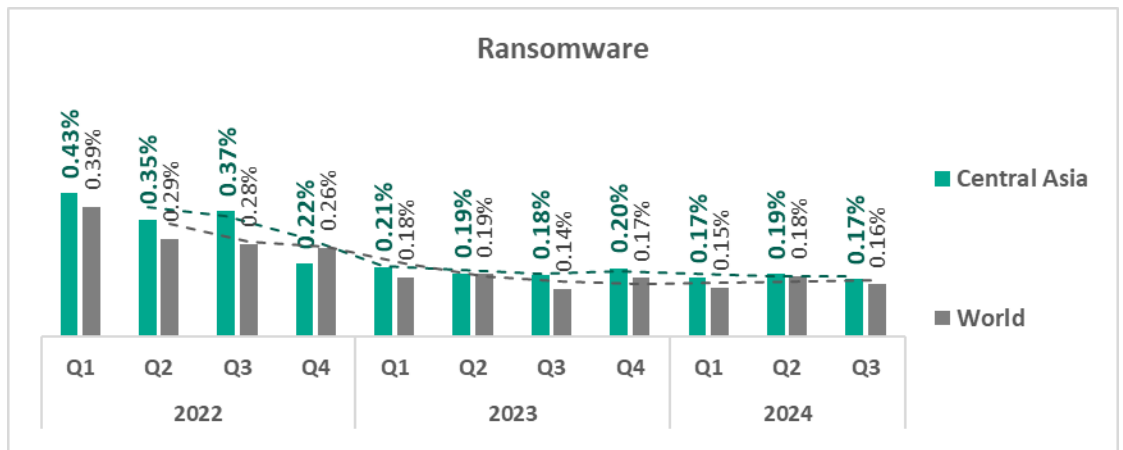
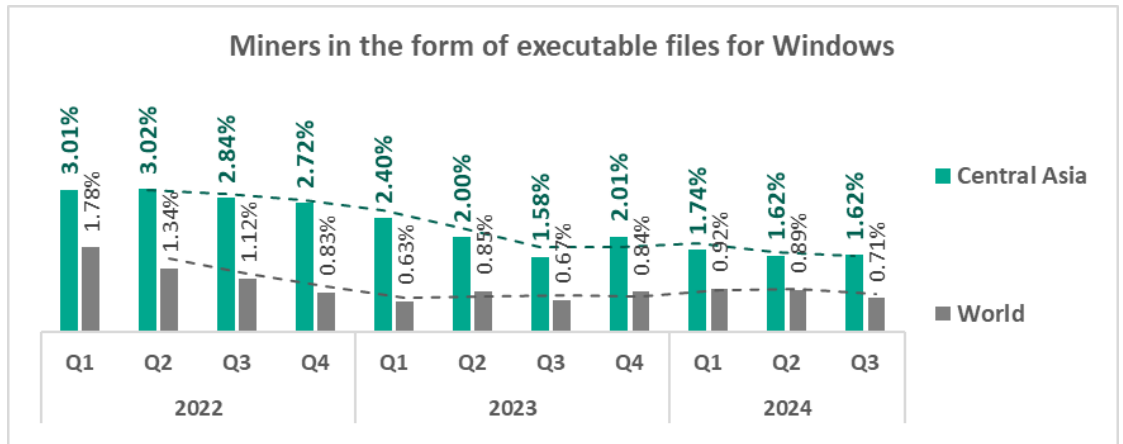
Threat categories



- Worms, executable miners, malware for AutoCAD, and web miners were the only threat categories that saw an **increase in Q3 2024** compared to the previous quarter.
- The **top threat** categories exhibit various quarterly dynamics:





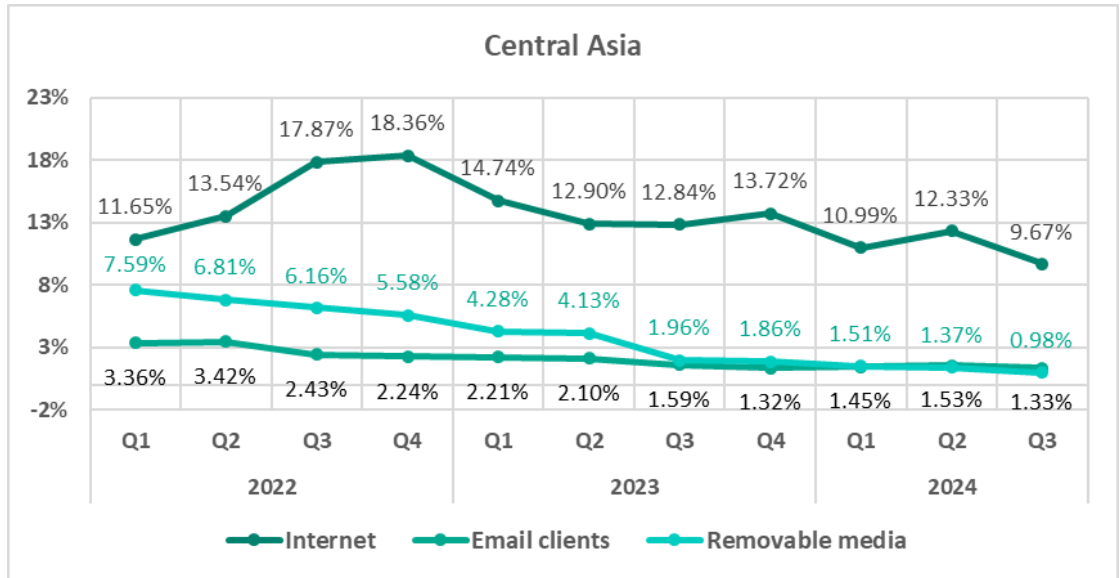


- The heatmap below illustrates changes in the rankings of threat categories in the region since the beginning of 2022. **Denylisted internet resources** have been the leading threat category in the region since Q1 2022, with the exception of Q4 2022 and Q4 2023. **Spyware** moved from third to second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

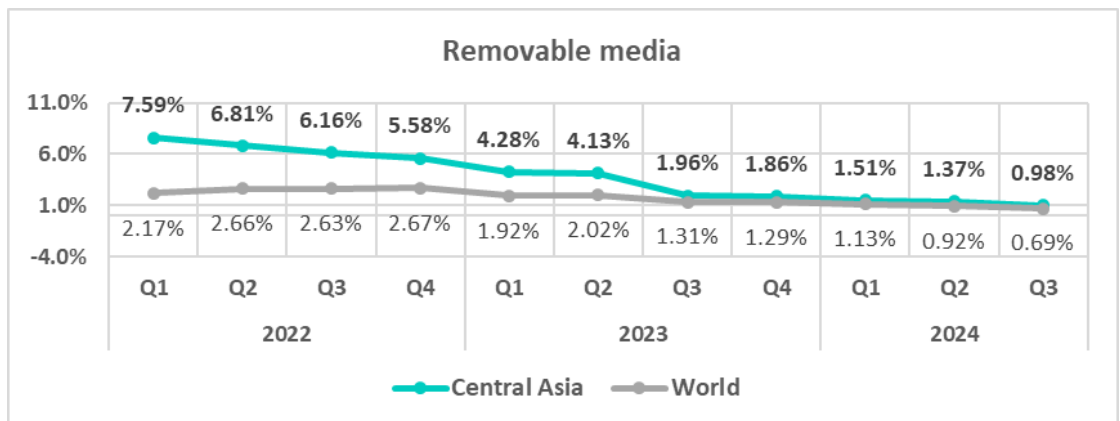
Central Asia	2022				2023				2024		
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3
Denylisted internet resources	1	1	1	2	1	1	1	2	1	1	1
Spy Trojans, backdoors and keyloggers	2	2	3	3	3	3	3	3	2	2	2
Malicious scripts and phishing pages (JS and HTML)	3	3	2	1	2	2	2	1	3	3	3
Worms	4	4	4	4	4	4	4	4	4	4	4
Miners in the form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

Threat sources

- In Q3 2024, all **sources of threats** in the region exhibited a **decrease** in the percentage of ICS computers on which they were blocked.

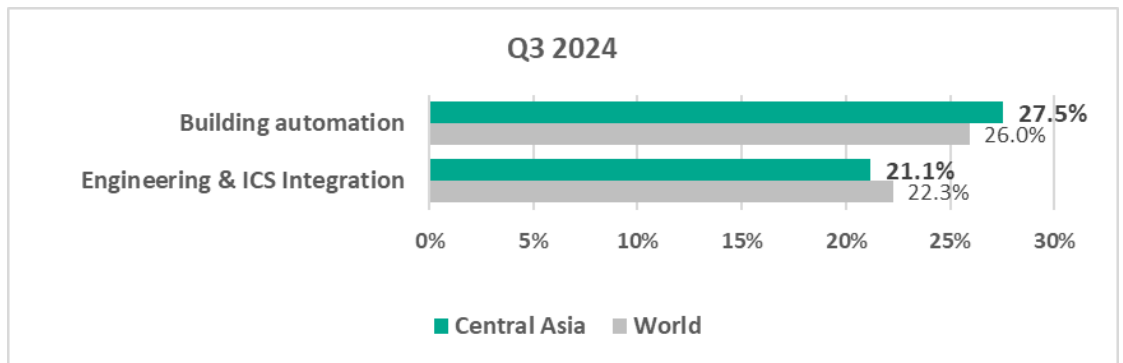


- Threats from **removable devices** have been above the **global average** throughout the observed period, although the **gap significantly narrowed** by Q3 2024 compared to early 2022.

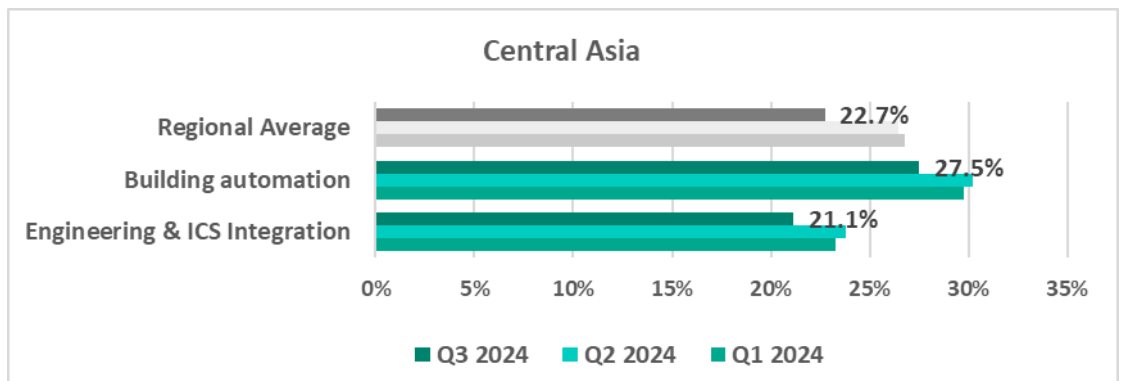


Industries

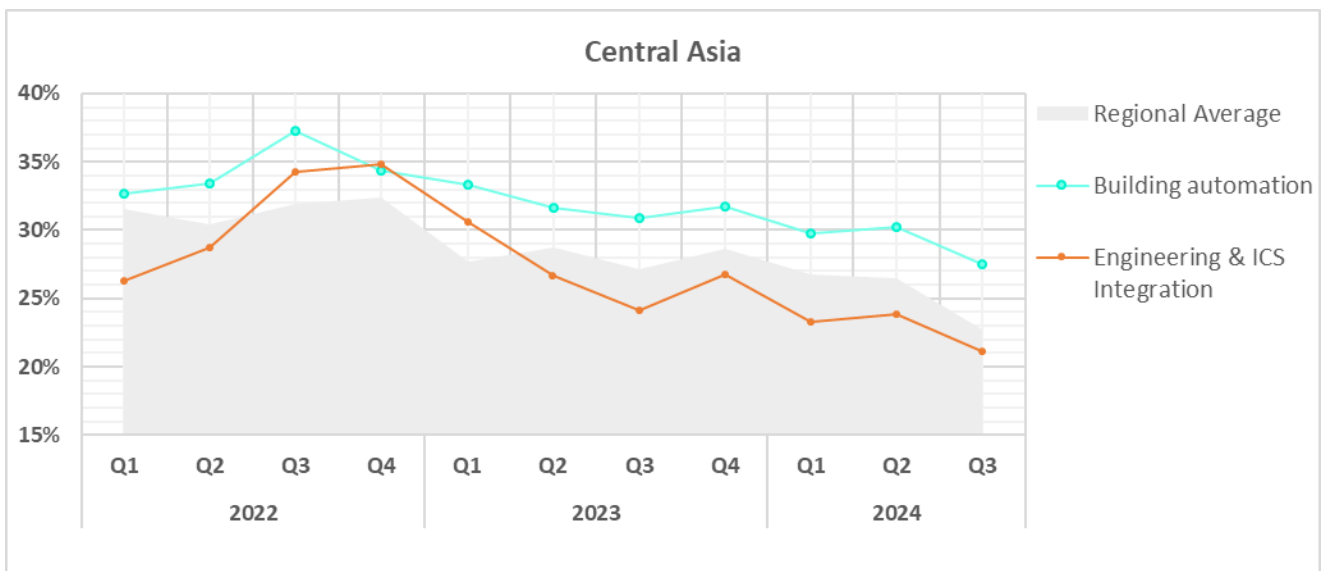
- The **most affected** industry in the region, as selected for this report, was **building automation**.
- From a global perspective, the percentage of ICS computers on which malicious objects were blocked in the **building automation** sector was 1.1 times **higher than the global average** for the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



- In **Q3 2024**, the sectors under study saw a **decrease** in the percentage of ICS computers on which malicious objects were blocked.

















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



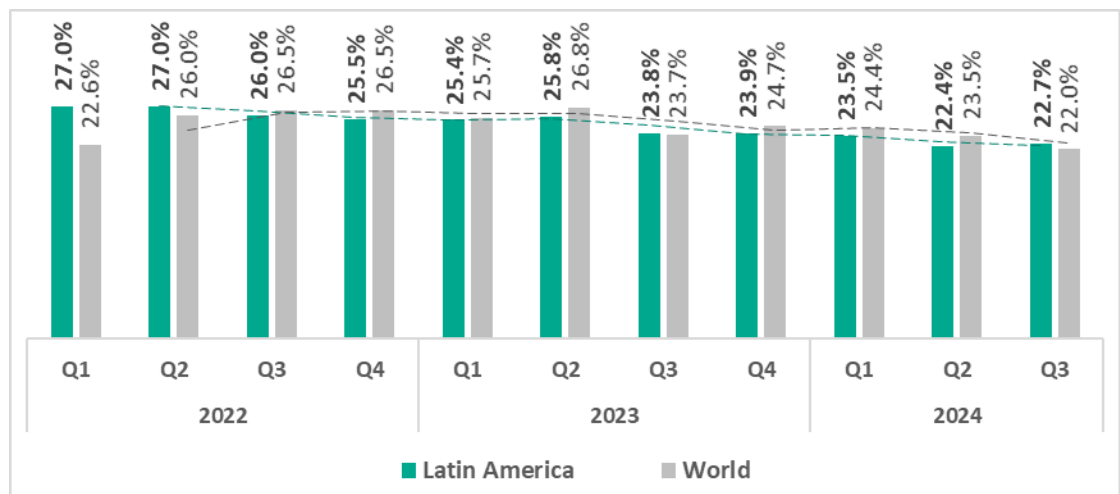
Latin America

Current threats

<p>N.1 IN THE REGION</p> <p>MALICIOUS SCRIPTS & PHISHING PAGES</p> <p>8.46%</p> <p> 1.3x increase in Q3 2nd globally in growth</p> <p> 1.4x above global average 2nd in the world</p>	<p>N.2 IN THE REGION</p> <p>DENYLISHED INTERNET RESOURCES</p> <p>6.66%</p> <p> 1.2x increase in Q3</p>	<p>N.3 IN THE REGION</p> <p>SPYWARE</p> <p>4.55%</p> <p> decrease in Q3</p> <p> 1.2x above global average</p>
<p>MALICIOUS DOCUMENTS</p> <p>4.17%</p> <p> 1.3x increase in Q3 1st globally in growth</p> <p> 2.1x above global average 1st in the world</p>	<p>WEB MINERS</p> <p>0.44%</p> <p> decrease in Q3</p> <p> 1.1x above global average</p>	<p>MALWARE FOR AUTOCAD</p> <p>0.14%</p> <p> 1.7x increase in Q3 1st globally in growth</p>
<p>THREATS FROM INTERNET</p> <p>11.69%</p> <p> 1.1x increase in Q3</p> <p> 1.1x above global average</p>	<p>THREATS FROM EMAIL CLIENTS</p> <p>4.79%</p> <p> 1.1x increase in Q3 1st globally in growth</p> <p> 1.8x above global average 2nd in the world</p>	

Overall

- **Fifth** place in the global ranking by percentage of ICS computers on which malicious objects were blocked.
- Overall, the region demonstrates a **downward trend**.
- However, in **Q3 2024**, the percentage of ICS computers on which malicious objects were blocked **increased**, slightly exceeding the global average.



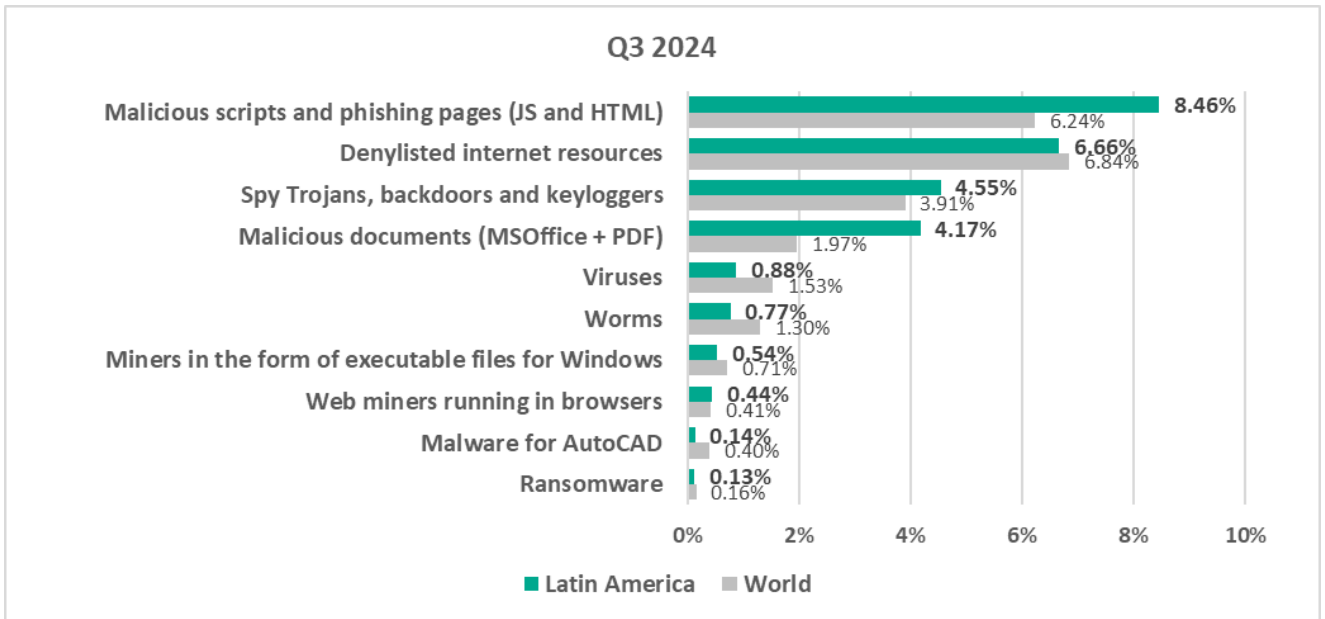
Comparative analysis

- Latin America occupies **leading positions** among regions by percentage of ICS computers on which the following were blocked:
 - First place – malicious documents
 - Second place – malicious scripts and phishing pages, threats from email clients

Threat categories

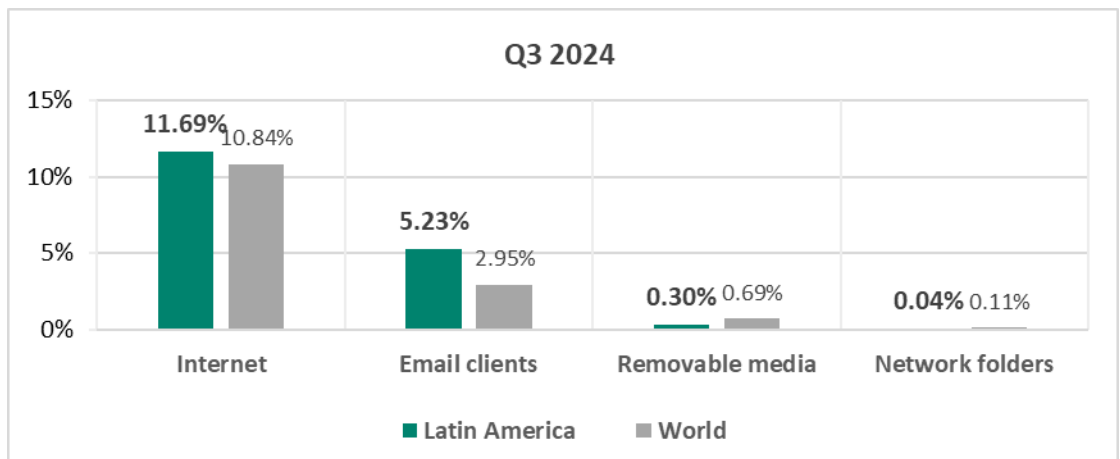
Compared to global figures, the region has a **higher percentage** of ICS computers on which the following threat categories were blocked:

- Malicious documents, 2.1 times higher
- Malicious scripts and phishing pages, 1.4 times higher
- Spyware, 1.2 times higher
- Web miners, 1.1 times higher



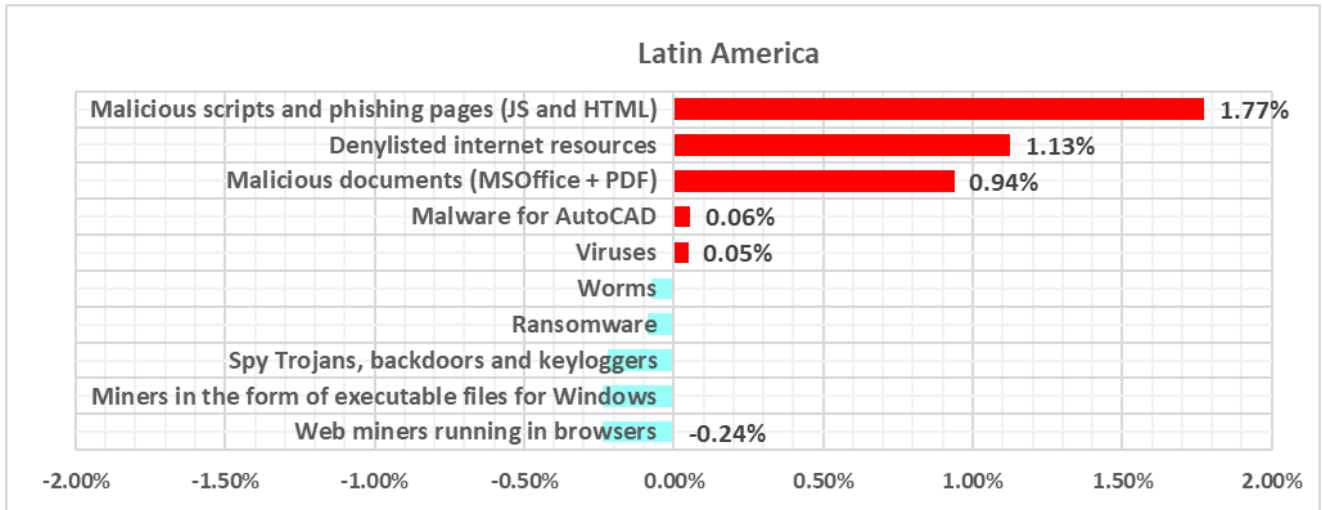
Threat sources

- The region ranked **second in the world** by percentage of ICS computers on which malicious threats from **email clients** were blocked, exceeding the global average by 1.8 times.

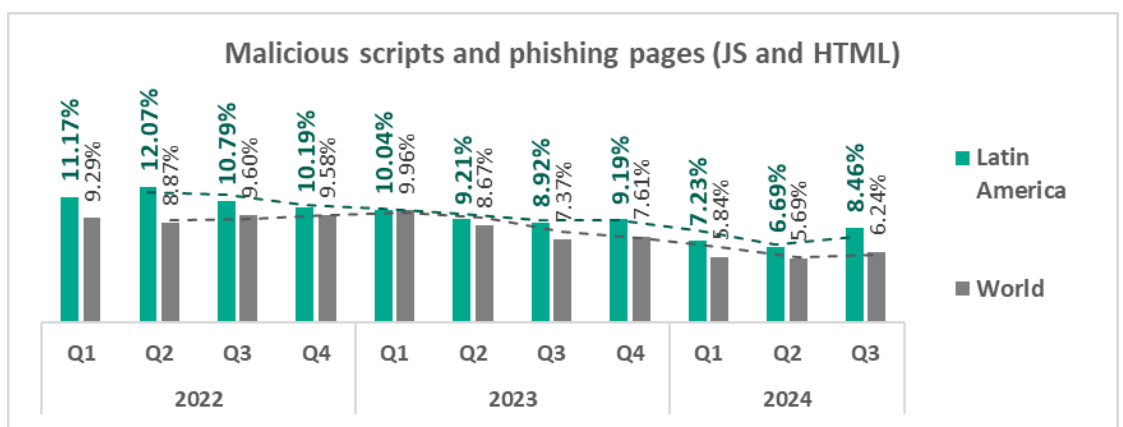


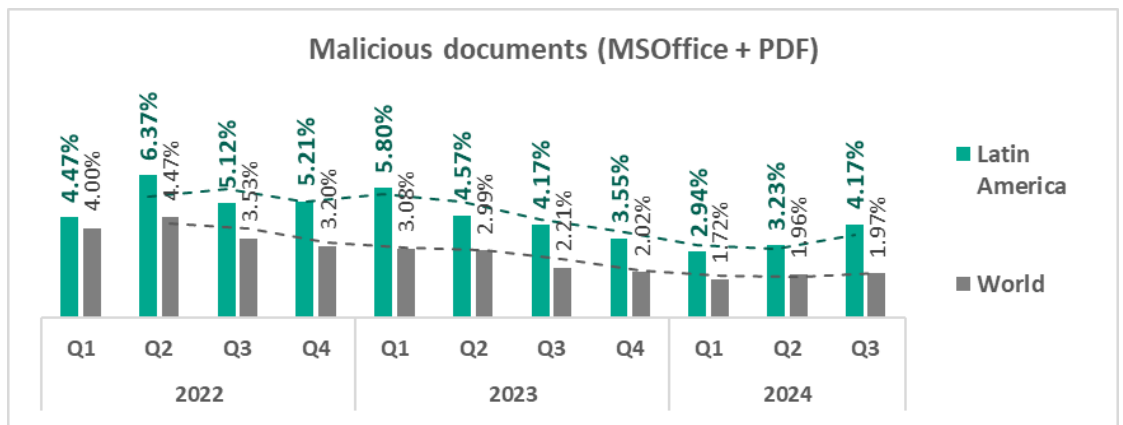
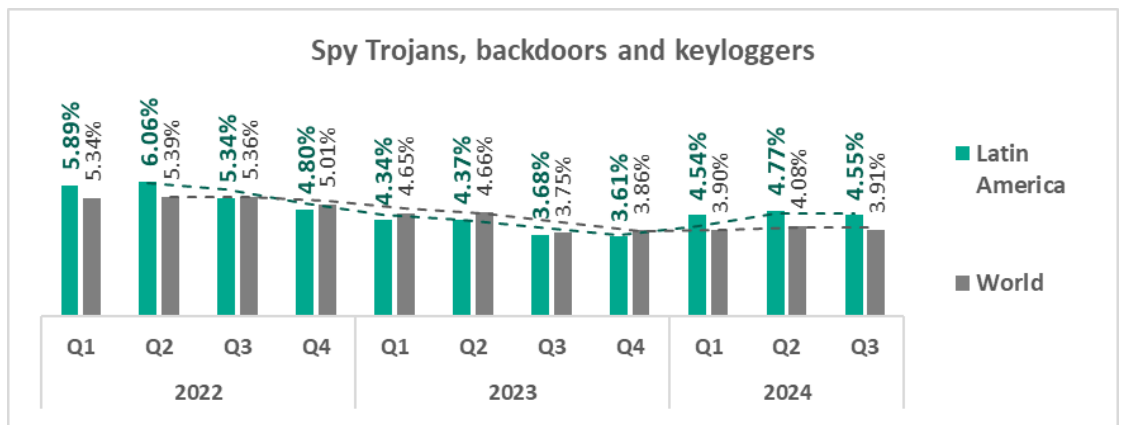
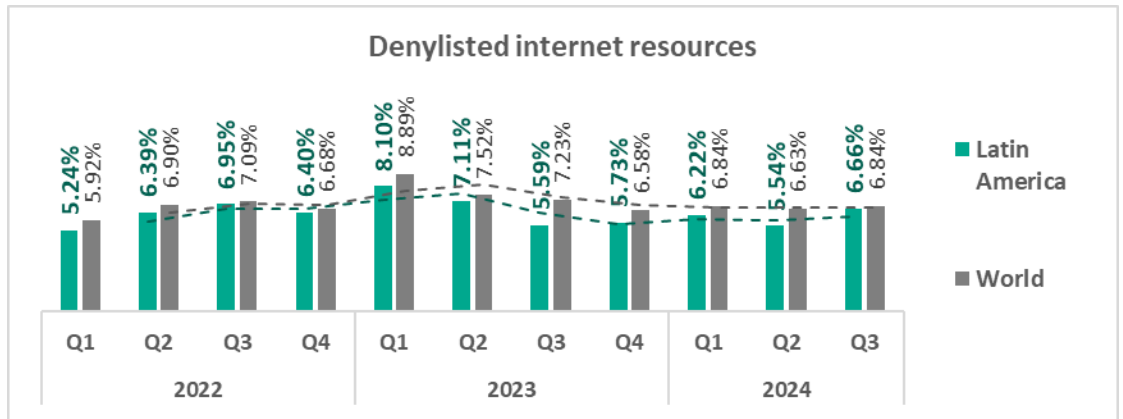
Quarterly changes and trends

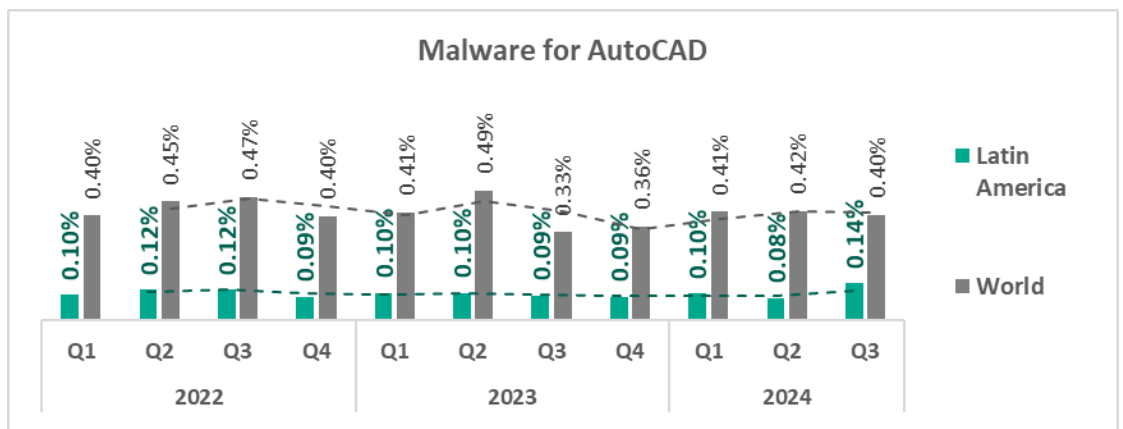
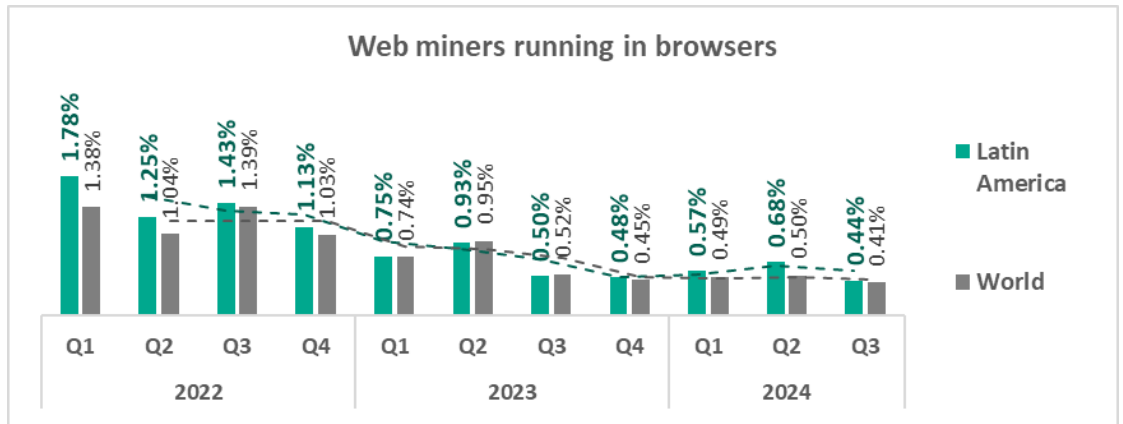
Threat categories



- The **largest proportional increase** in Q3 2024 was in the percentage of ICS computers on which the following were blocked:
 - Malware for AutoCAD – by 1.8 times
 - Malicious documents – by 1.3 times
 - Malicious scripts and phishing pages – by 1.3 times
 - Denylisted internet resources – by 1.2 times
 - Viruses – by 1.1 times.
- The **top threat** categories exhibit various quarterly dynamics:







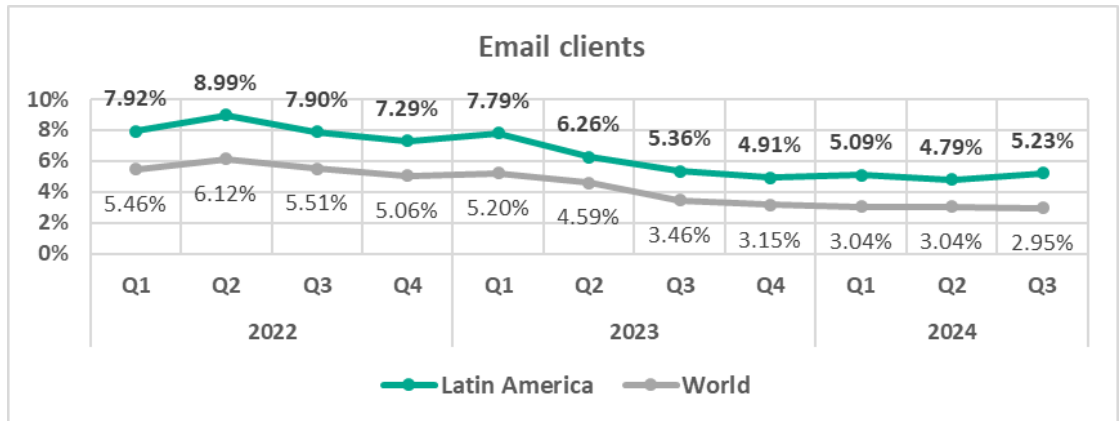
- The heatmap below illustrates changes in the rankings of threat categories in the region since the beginning of 2022. **Malicious scripts and phishing pages** have been the leading threat category in the region throughout the observed period. **Spyware** moved up from fourth to third place in Q4 2023 and has held that position since. In Q3 2024, **viruses** and **malware for AutoCAD** moved one position up.

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

Threat sources

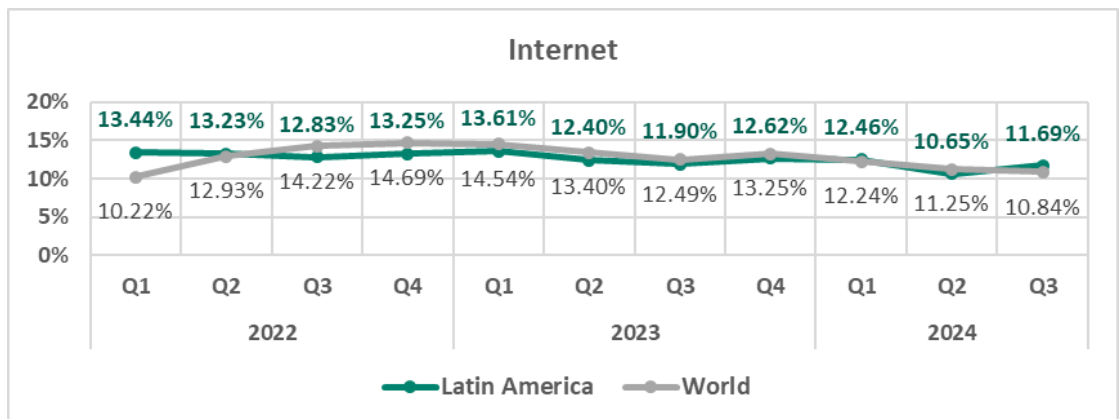
- Threats from **email clients** (in terms of percentage of ICS computers where they were blocked) exhibit a gradual **downward trend** mostly consistent with the global trend, but noticeably above the global average.

In **Q3 2024**, there was a significant **increase** by 1.1 times compared to the previous quarter.



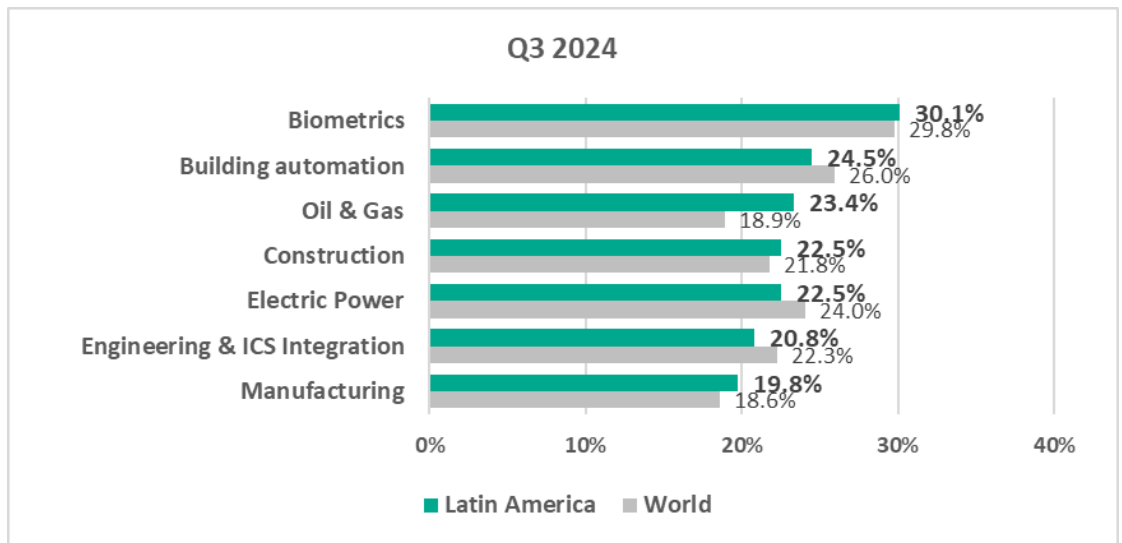
- Threats from **internet** exhibit a slow **downward** trend with fluctuations mostly consistent with the global trend.

In **Q3 2024**, there also was a **noticeable increase** by 1.1 times compared to the previous quarter, slightly exceeding the global average.

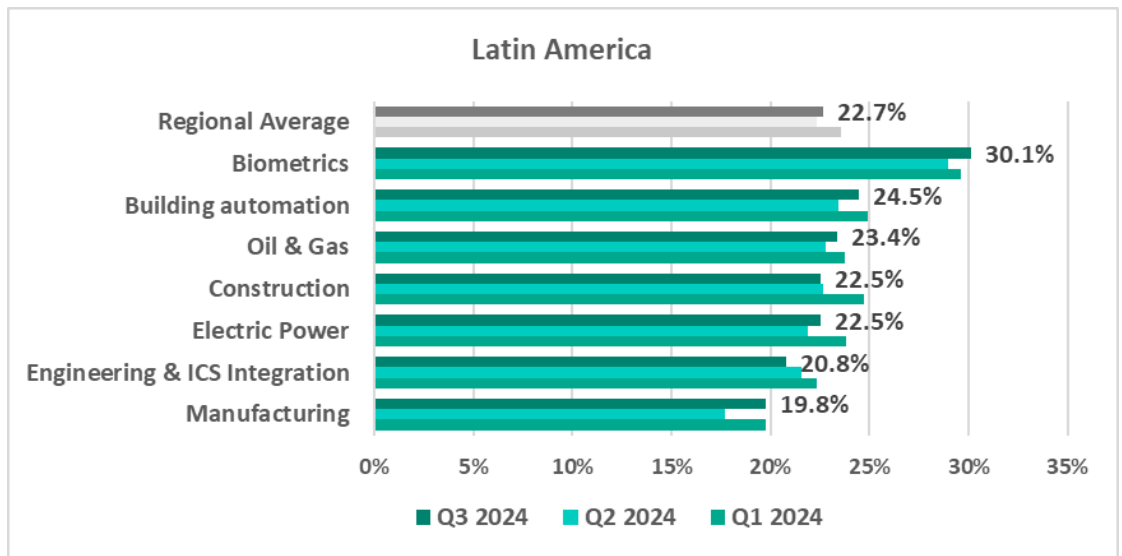


Industries

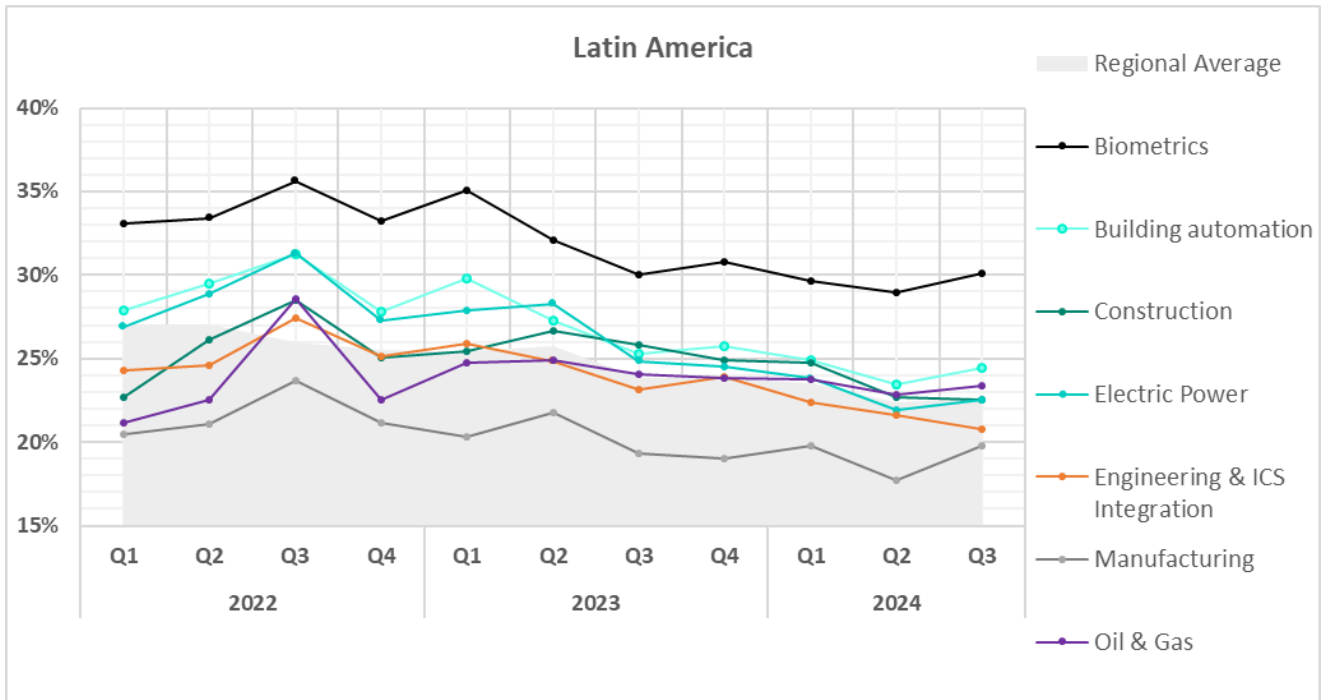
- The most **affected industry** in the region, as selected for this report, was **biometrics**.
- From a **global perspective**, the percentage of ICS computers on which malicious objects were blocked in the **oil and gas** industry was **1.2 times higher than the sector's global average**.



- In **Q3 2024**, the majority of the selected sectors in the region exhibited an **increase** in the percentage of ICS computers on which malicious objects were blocked. The most noticeable increase was in **manufacturing** – by 1.1 times compared to the previous quarter.




















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



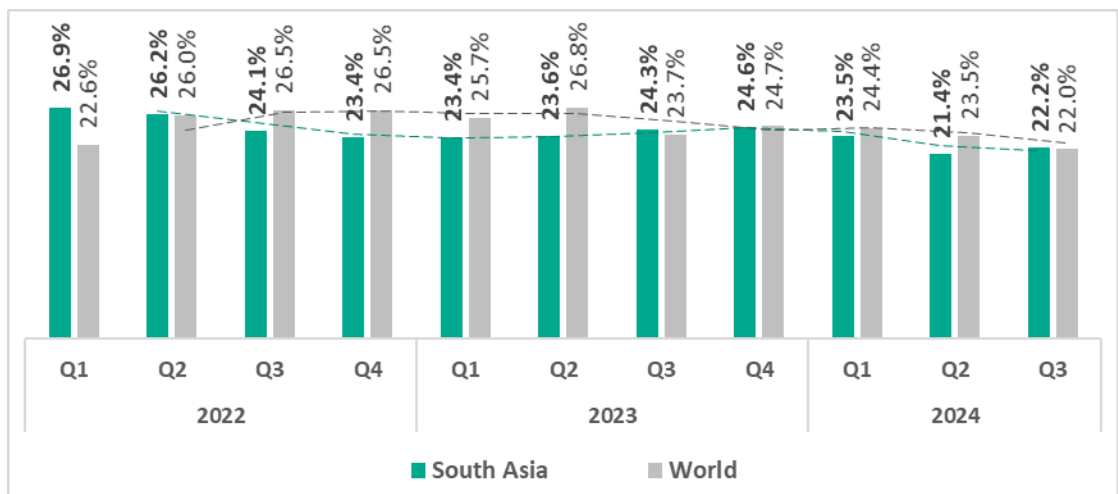
South Asia

Current threats

<p>N.1 IN THE REGION</p> <p>DENYLISTED INTERNET RESOURCES</p> <p>7.23%</p> <p> 1.1x increase in Q3</p> <p> 1.1x above global average</p>	<p>N.2 IN THE REGION</p> <p>MALICIOUS SCRIPTS & PHISHING PAGES</p> <p>6.37%</p> <p> 1.1x increase in Q3</p>	<p>N.3 IN THE REGION</p> <p>SPYWARE</p> <p>2.88%</p> <p> decrease in Q3</p>
<p>WORMS</p> <p>1.82%</p> <p> slight increase in Q3 2nd globally in growth</p> <p> 1.4x above global average</p>	<p>VIRUSES</p> <p>1.74%</p> <p> slight increase in Q3</p> <p> 1.1x above global average</p>	<p>EXECUTABLE MINERS</p> <p>0.79%</p> <p> decrease in Q3</p> <p> 1.1x above global average 3rd in the world</p>
<p>RANSOMWARE</p> <p>0.22%</p> <p> 1.4x above global average 3rd in the world</p>		
<p>THREATS FROM INTERNET</p> <p>11.97%</p> <p> 1.1x increase in Q3</p> <p> 1.1x above global average</p>	<p>THREATS FROM REMOVABLE DEVICES</p> <p>4.79%</p> <p> decrease in Q3</p> <p> 2.2x above global average 2nd in the world</p>	<p>THREATS FROM NETWORK FOLDERS</p> <p>0.21%</p> <p> decrease in Q3</p> <p> 1.5x above global average 3rd in the world</p>

Overall

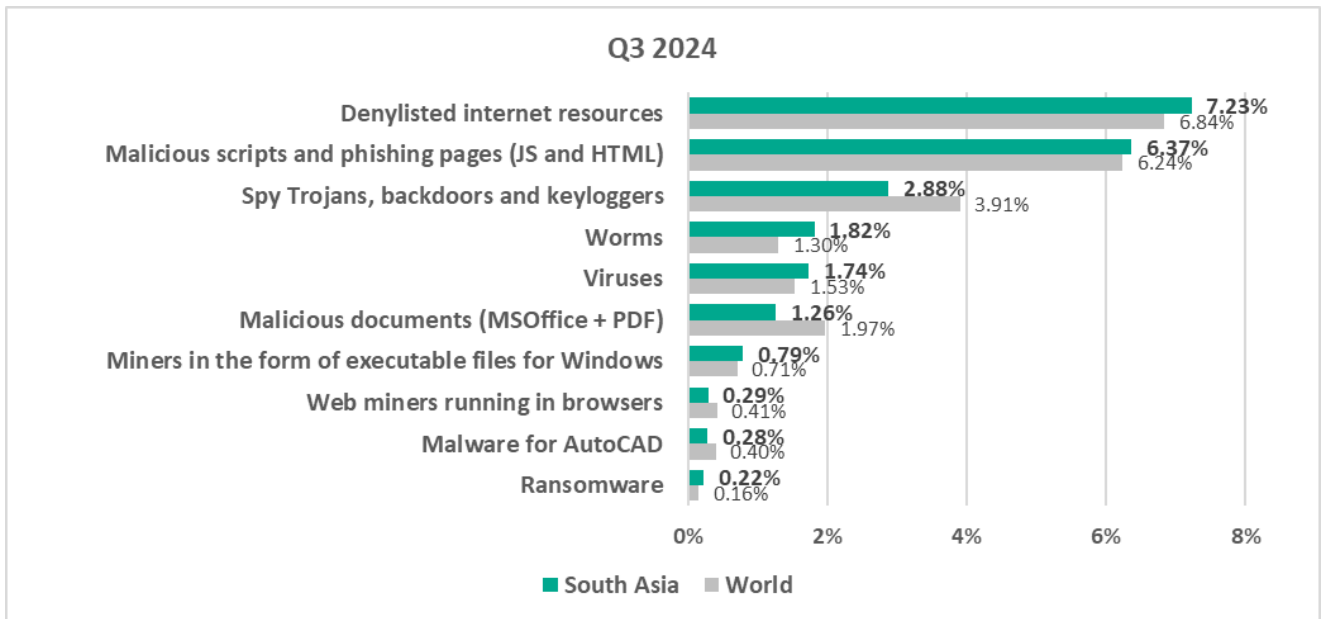
- **Sixth** place in the global ranking by percentage of ICS computers on which malicious objects were blocked.
- The region demonstrates a slow **downward** trend with some fluctuations.
- In **Q3 2024**, the percentage of ICS computers on which malicious objects were blocked **increased**, slightly exceeding the global average.



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 – miners in the form of executable files for Windows, ransomware, threats from network folders

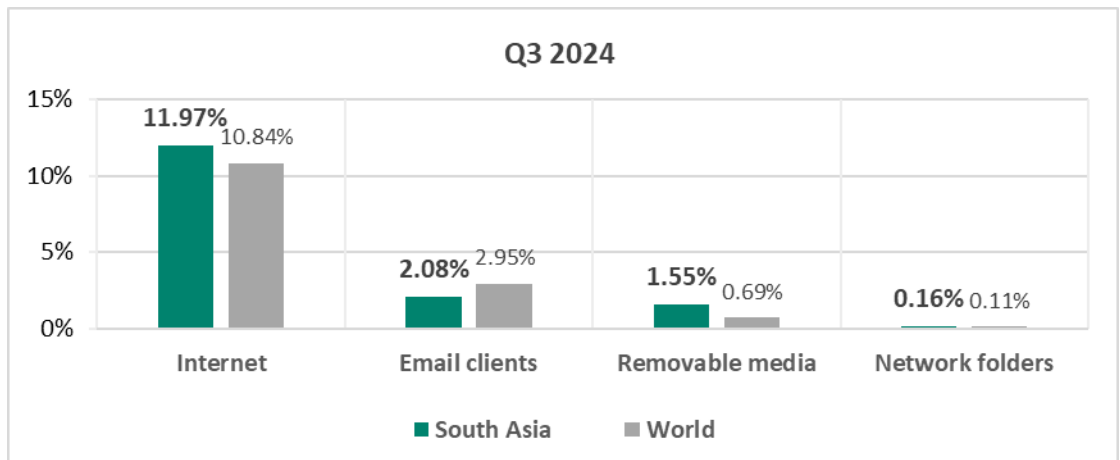
Threat categories



- Compared to the global average, the region has a noticeably higher percentage of ICS computers on which the following were blocked:
 - Worms, 1.4 times higher. Worms ranked fourth in the regional ranking of threat categories by percentage of ICS computers on which they were blocked (sixth globally)
 - Ransomware, 1.4 times higher
 - Viruses, 1.1 times higher
 - Miners in the form of executable files for Windows, 1.1 times higher.

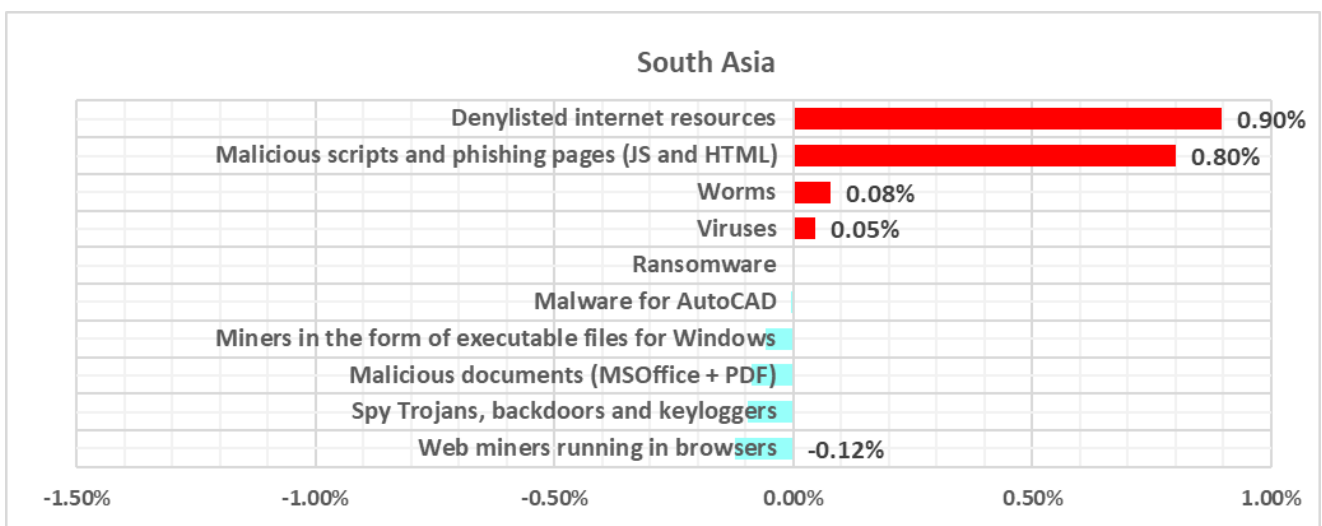
Threat sources

- South Asia ranks **second globally** by percentage of ICS computers on which malicious threats from **removable devices** were blocked, surpassing the global average by 2.2 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 1.5.



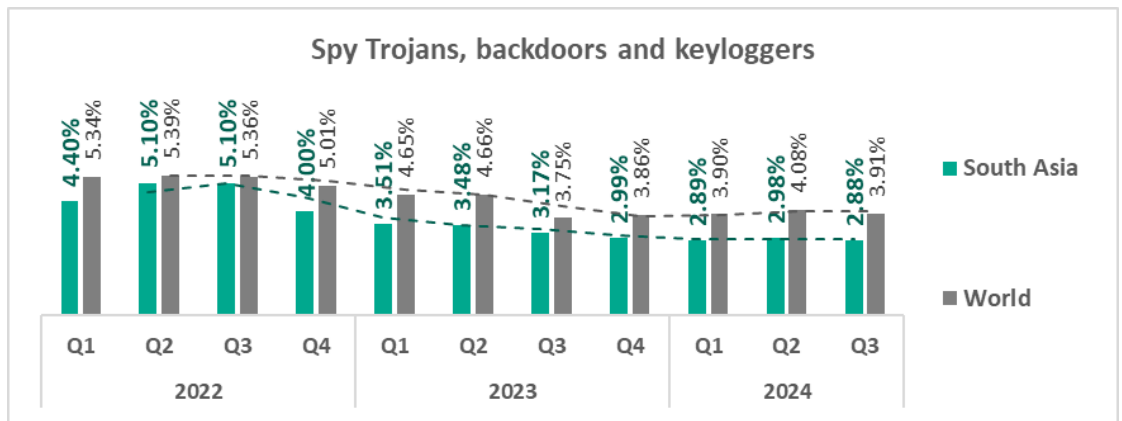
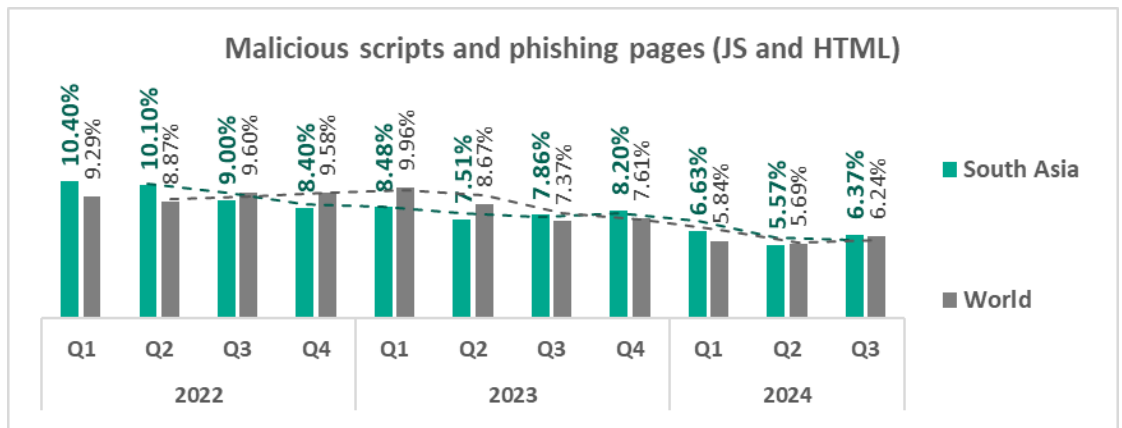
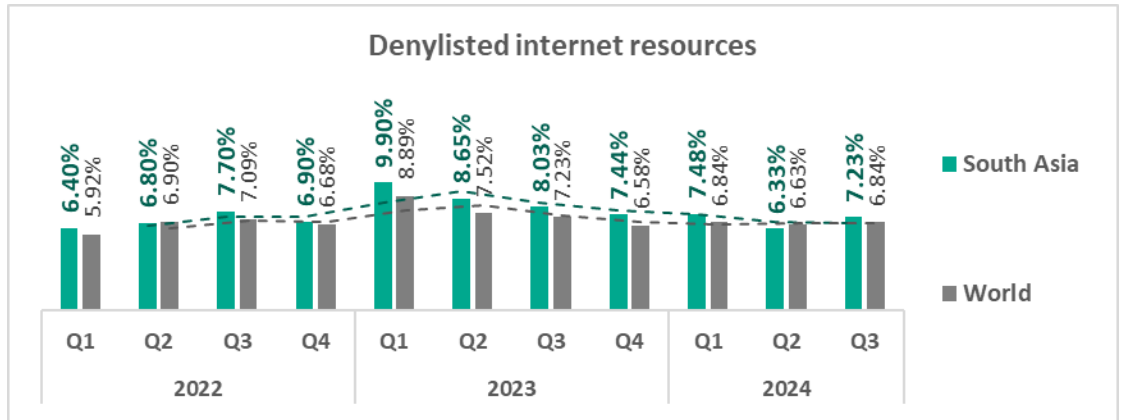
Quarterly changes and trends

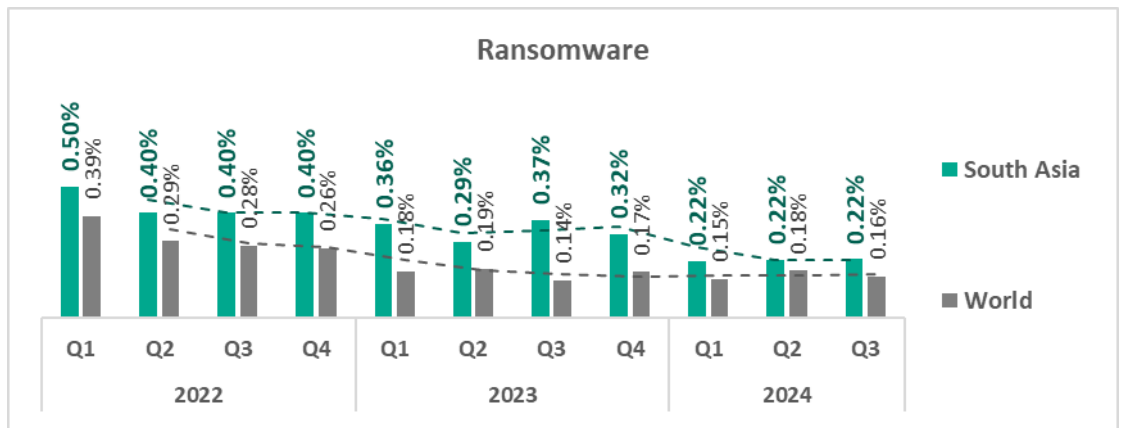
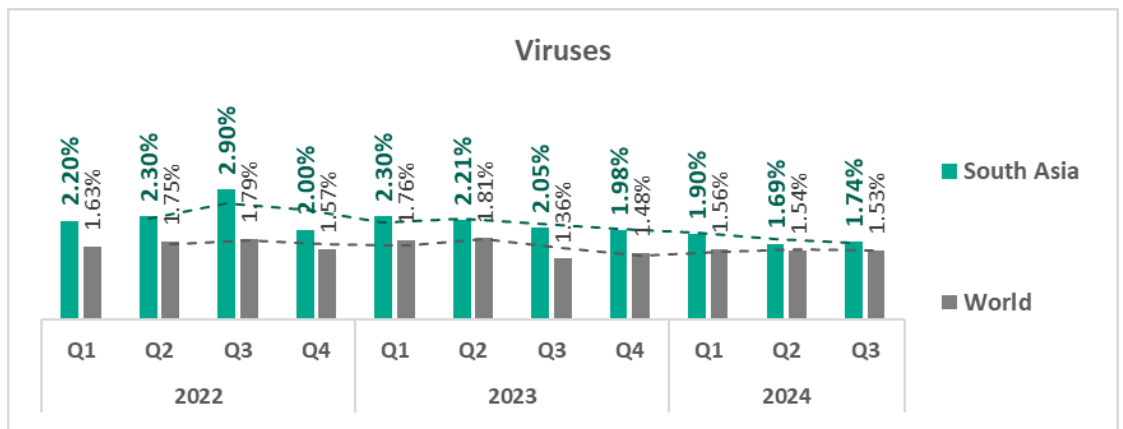
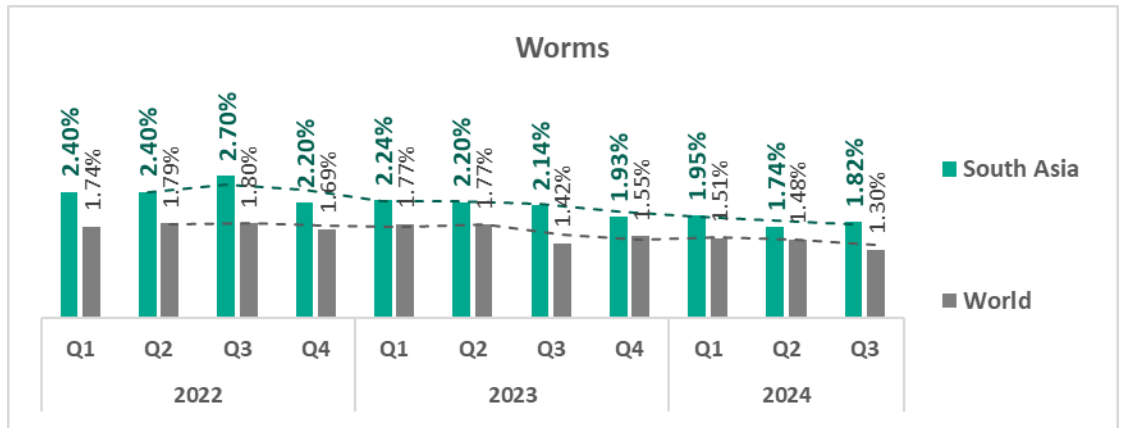
Threat categories



- The **largest proportional increase** in Q3 2024 was in the percentage of ICS computers on which the following were blocked:
 - Malicious scripts and phishing pages, by 1.1 times
 - Denylisted internet resources, by 1.1 times

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



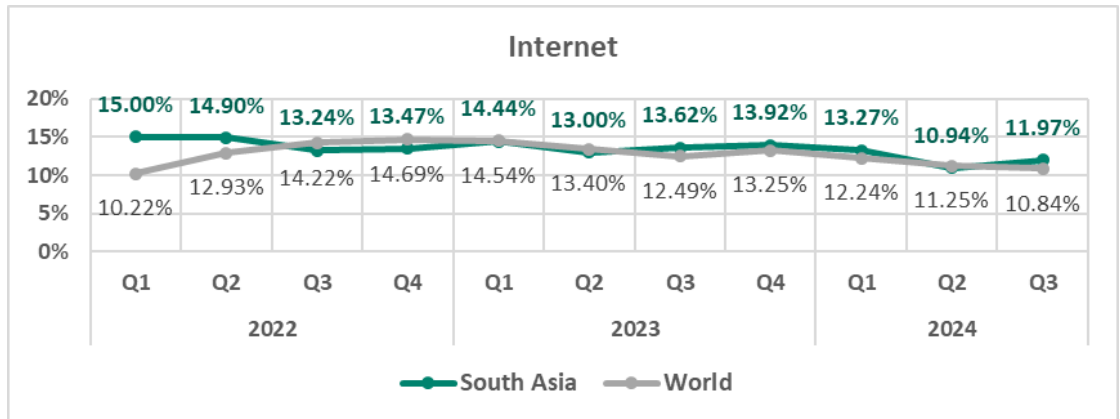


- The heat map below illustrates changes in the rankings of threat categories in the region since the beginning of 2022. **Denylisted internet resources** have been the leading threat category in the region since Q1 2023, with the exception of Q4 2023. **Malicious scripts and phishing pages** have ranked 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.

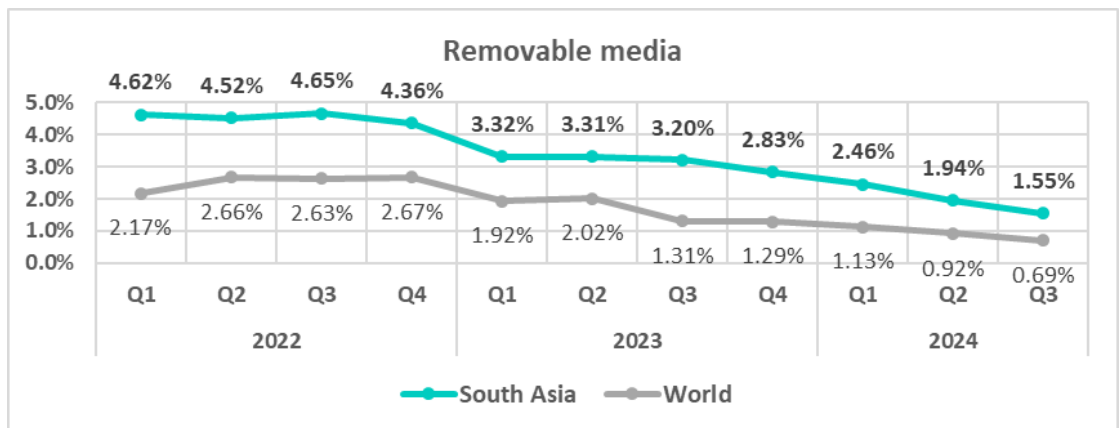
South Asia	2022				2023				2024		
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3
Denylisted internet resources	2	2	2	2	1	1	1	2	1	1	1
Malicious scripts and phishing pages (JS and HTML)	1	1	1	1	2	2	2	1	2	2	2
Spy Trojans, backdoors and keyloggers	3	3	3	3	3	3	3	3	3	3	3
Worms	5	5	5	4	5	5	4	5	4	4	4
Viruses	6	6	4	6	4	4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

Threat sources

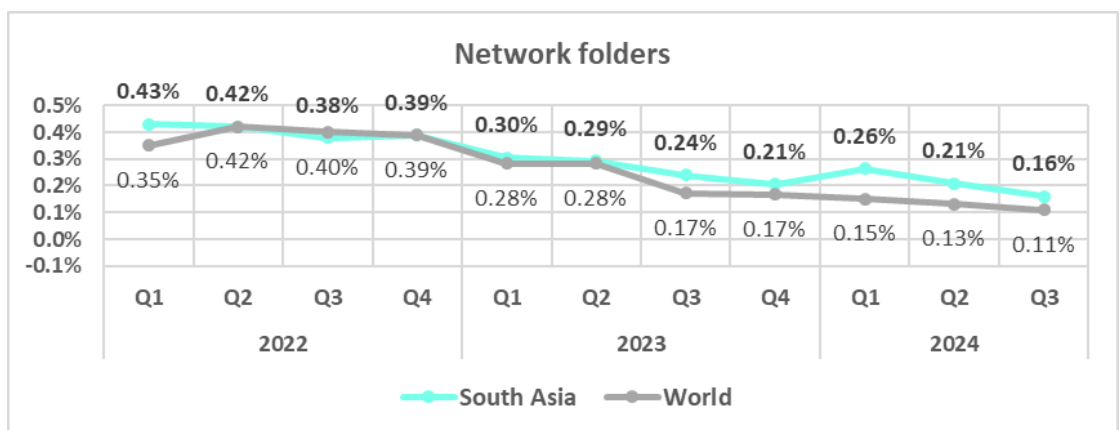
- In **Q3 2024**, the percentage of ICS computers on which threats **internet** were blocked **increased** 1.1 times compared to the previous quarter.



- Threats from **removable drives** demonstrate a **downward trend** in South Asia, however, significantly above the respective global trend.



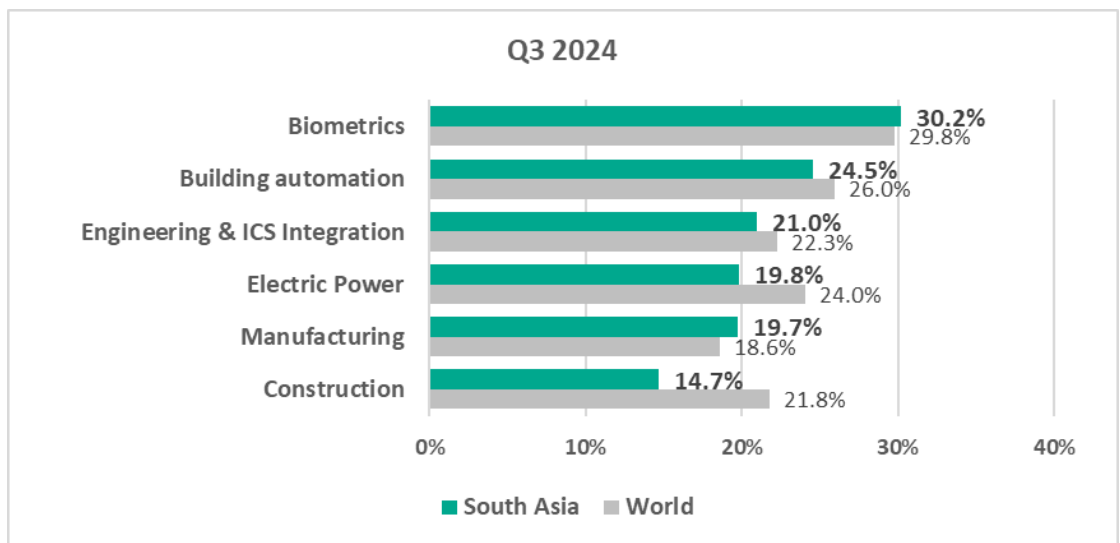
- Threats from **network folders** after a spike in Q1 2024 have been demonstrating a **downward trend**, staying well above the global average.



Industries

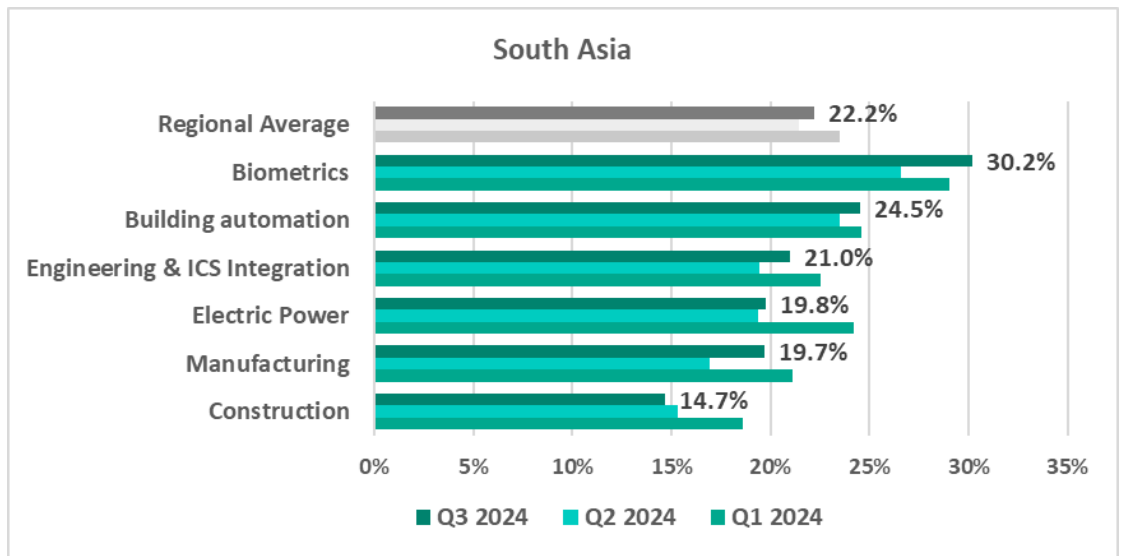
- **The most affected industry** in the region, as selected for this report, was **biometrics**.

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

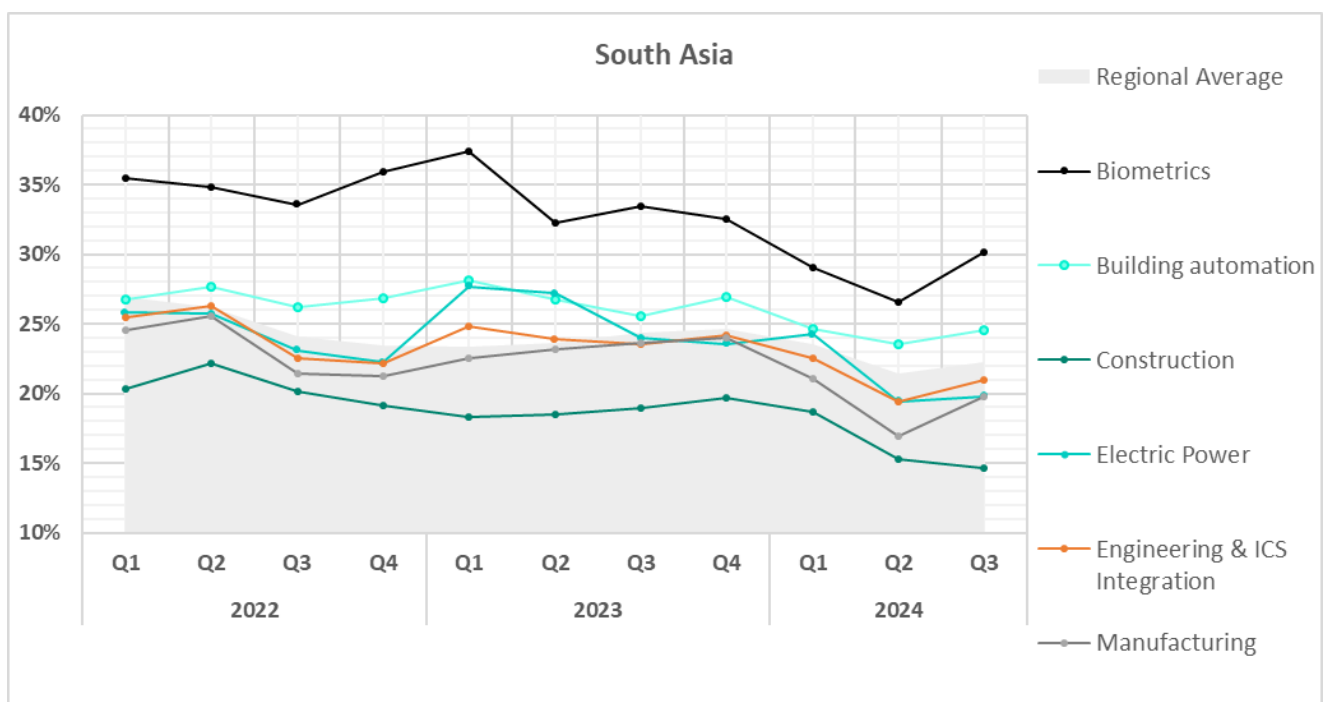


- In **Q3 2024**, all selected sectors in the region, except construction, exhibited an **increase** in the percentage of ICS computers on which malicious objects were blocked.

The most noticeable increase was in **manufacturing** – by 1.2 times, and **biometrics** – by 1.1 times, compared to the previous quarter.



















- The selected sectors for the most part show slow **positive dynamics** with noticeable fluctuations in their long-term **trends**.



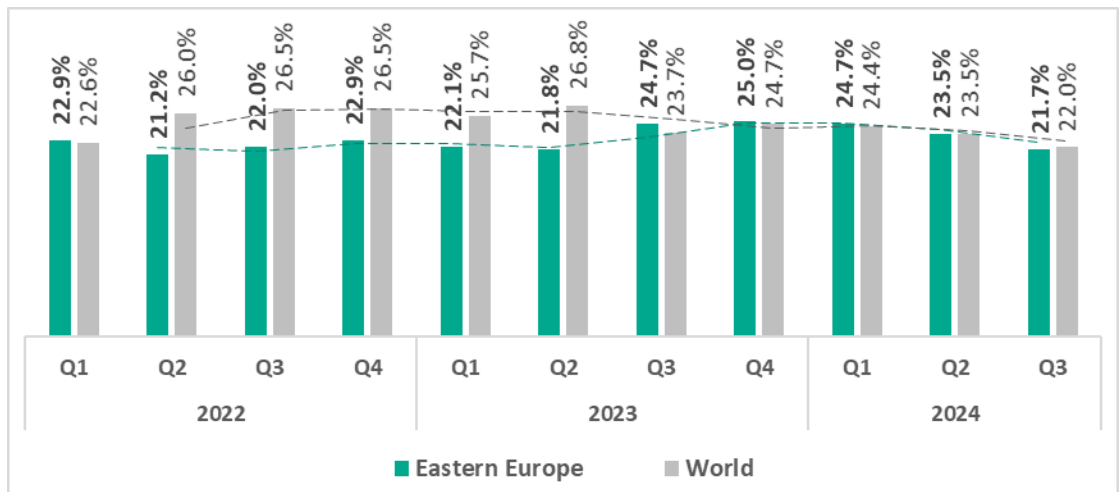
Eastern Europe

Current threats

<p>N.1 IN THE REGION</p> <p>DENYLISTED INTERNET RESOURCES</p> <p>6.47%</p> <p> decrease in Q3</p>	<p>N.2 IN THE REGION</p> <p>MALICIOUS SCRIPTS & PHISHING PAGES</p> <p>6.21%</p> <p> 1.1x increase in Q3</p>	<p>N.3 IN THE REGION</p> <p>SPYWARE</p> <p>4.92%</p> <p> decrease in Q3</p> <p> 1.3x above global average</p>
<p>MALICIOUS DOCUMENTS</p> <p>2.14%</p> <p> decrease in Q3</p> <p> 1.1x above global average</p>	<p>WORMS</p> <p>1.39%</p> <p> decrease in Q3</p> <p> 1.1x above global average</p>	<p>EXECUTABLE MINERS</p> <p>0.78%</p> <p> decrease in Q3</p> <p> 1.1x above global average</p>
<p>WEB MINERS</p> <p>0.56%</p> <p> decrease in Q3</p> <p> 1.4x above global average 3rd in the world</p>	<p>MALWARE FOR AUTOCAD</p> <p>0.11%</p> <p> 1.1x increase in Q3 2nd globally in growth</p>	
<p>THREATS FROM INTERNET</p> <p>9.82%</p> <p> decrease in Q3</p>	<p>THREATS FROM EMAIL CLIENTS</p> <p>4.79%</p> <p> decrease in Q3</p> <p> 1.5x above global average</p>	

Overall

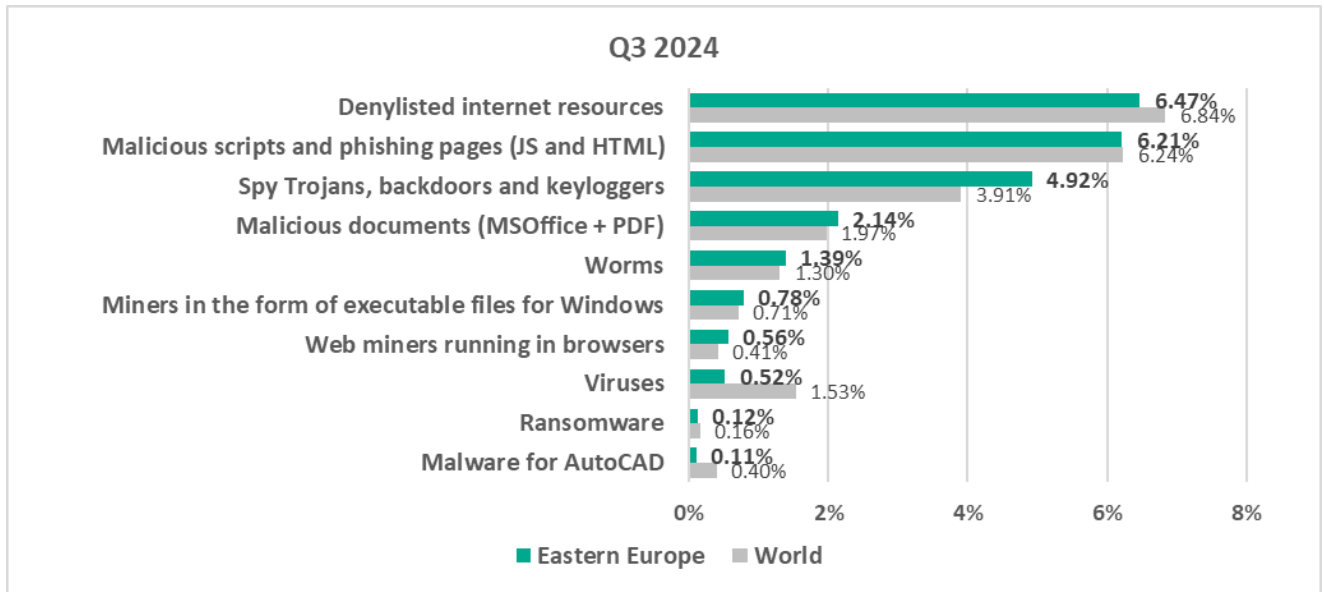
- **Seventh** place in the global ranking by percentage of ICS computers on which malicious objects were blocked. Before Q2 2023, the region did not rank higher than ninth place.
- In **Q3 2024**, the region showed a **decline** by a factor of 1.1 in the percentage of ICS computers on which malicious objects were blocked compared to the previous quarter. The indicator was **below the global average**.



Comparative analysis

Eastern Europe ranked **third** among regions by percentage of ICS computers on which web miners were blocked.

Threat categories

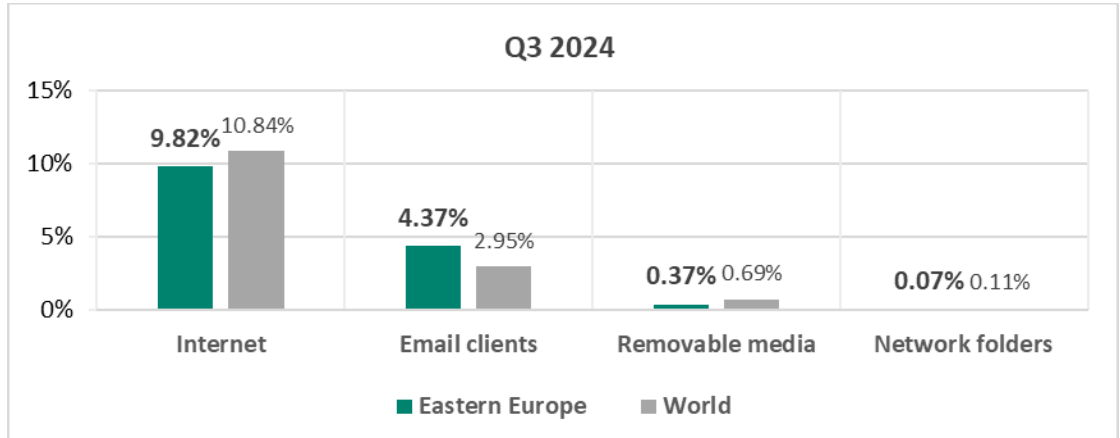


Compared to the global figures, the region has a **higher percentage** of ICS computers on which the following were blocked:

- Web miners, 1.4 times higher
- Spyware, 1.3 times higher
- Miners in the form of executable files for Windows, 1.1 times higher
- Malicious documents, 1.1 times higher
- Worms, 1.1 times higher

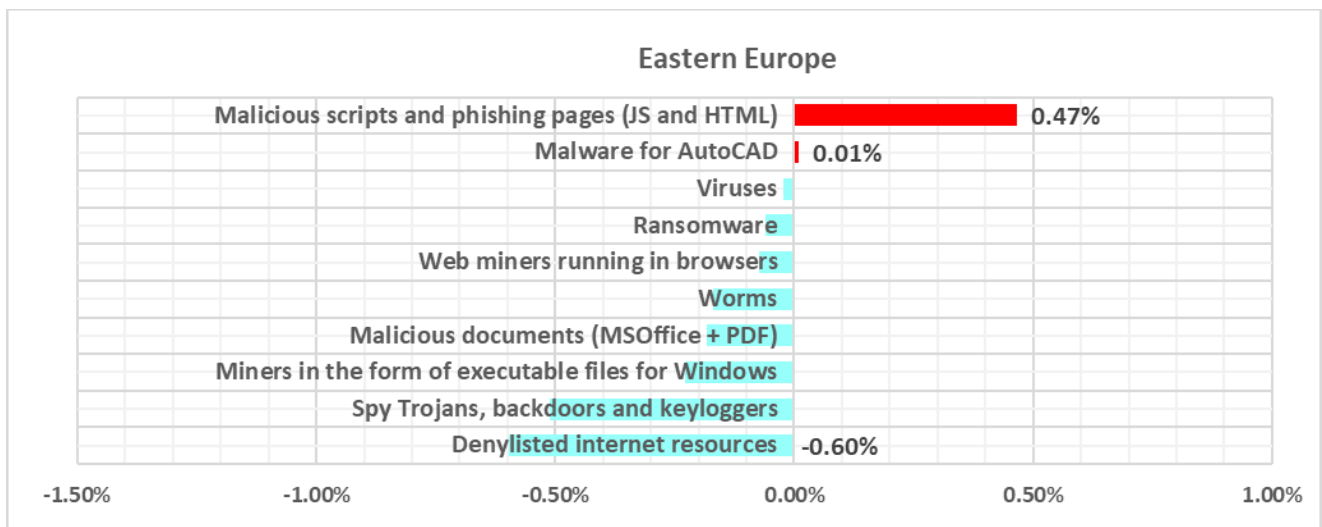
Threat sources

- Threats from **email clients** exceeded the global average by 1.5 times.



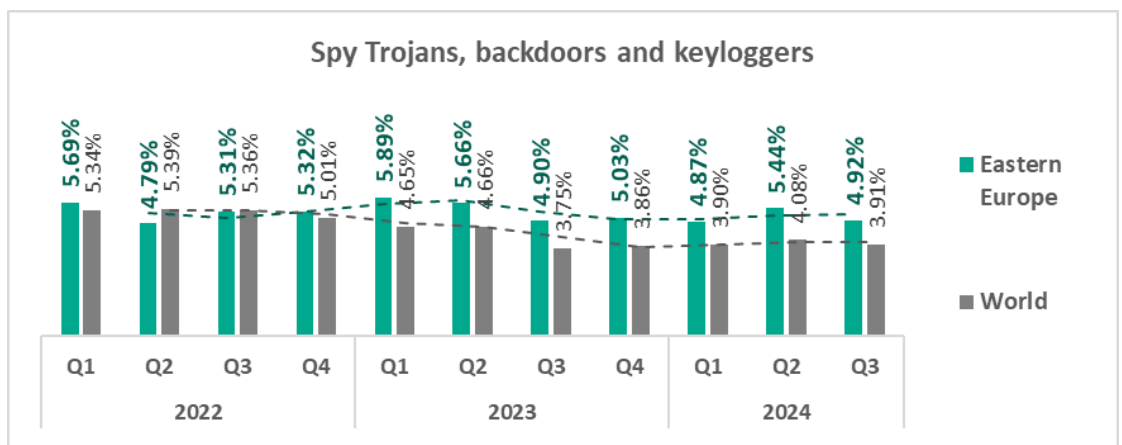
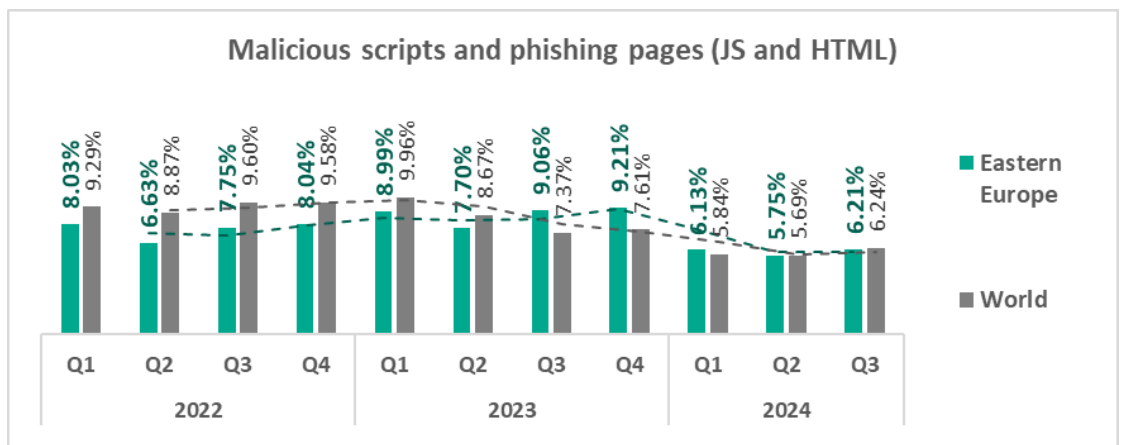
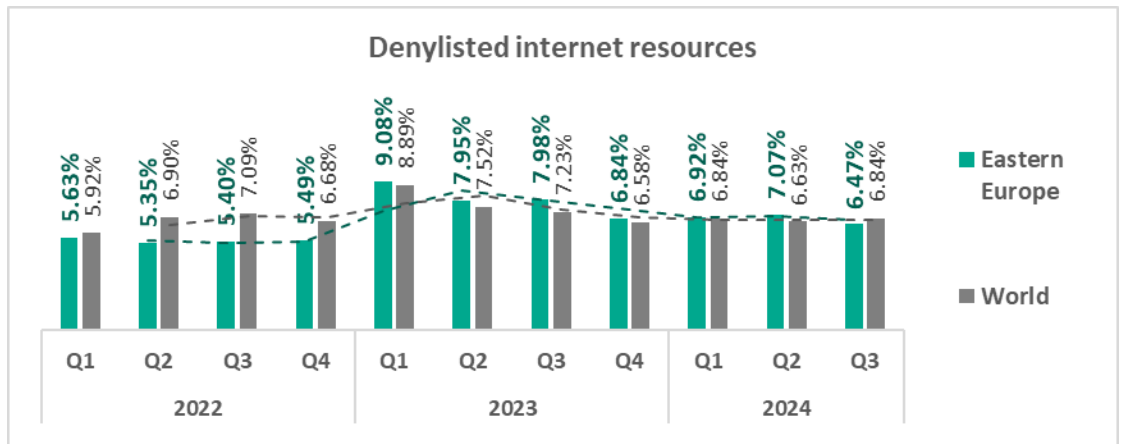
Quarterly changes and trends

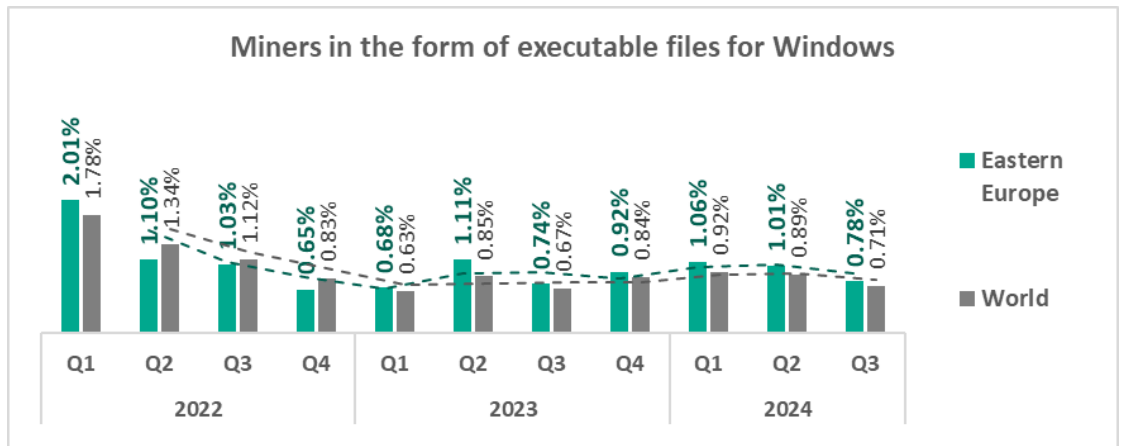
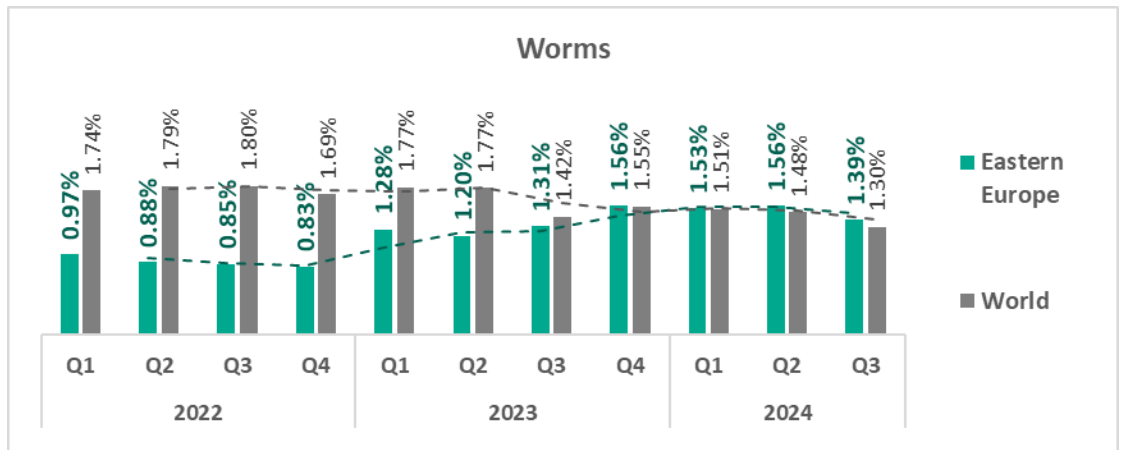
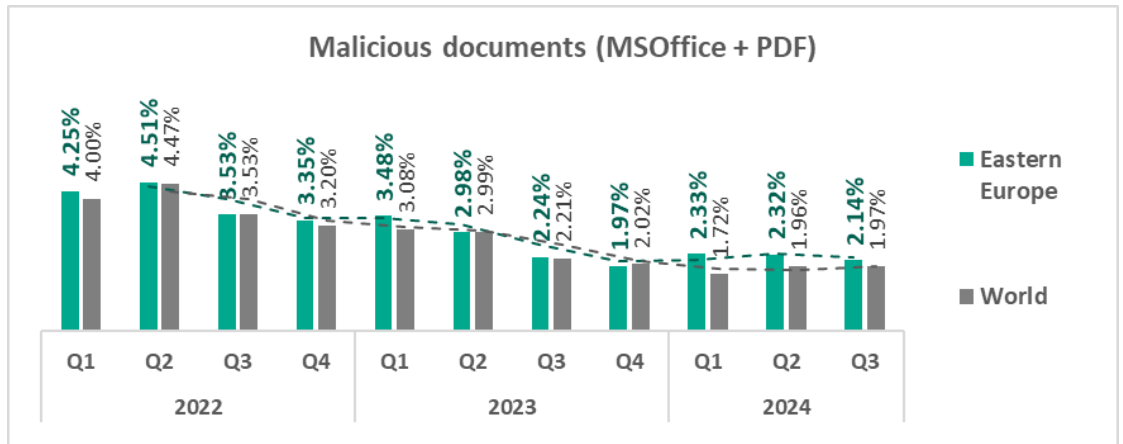
Threat categories

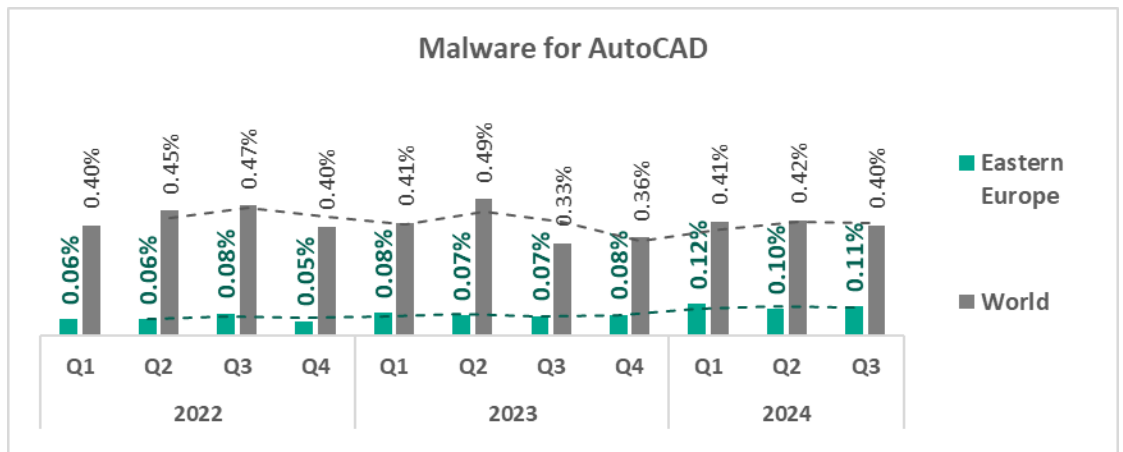
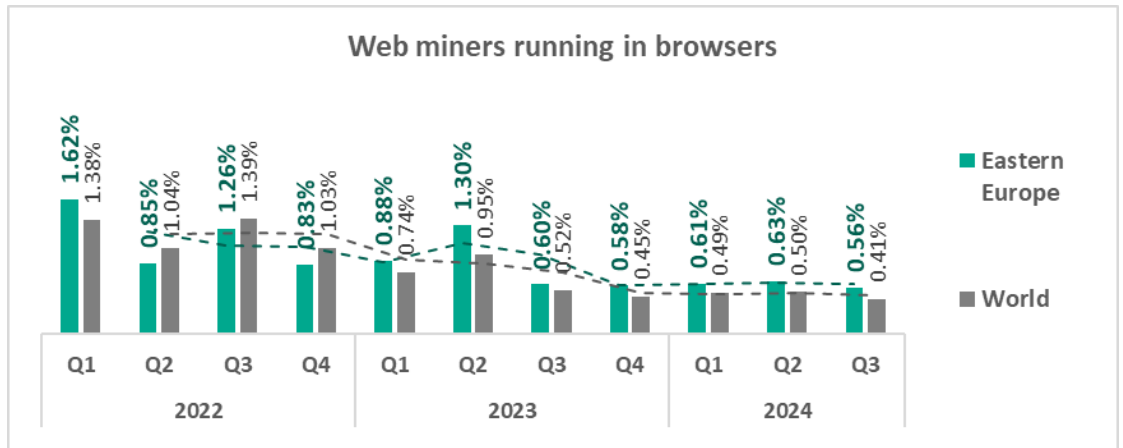


- The **largest quarterly increase** was in the percentage of ICS computers on which the following were blocked:
 - Malicious scripts and phishing pages, by 1.1 times.
 - Malware for AutoCAD, by 1.1 times. Ranked second in the world in terms of growth

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





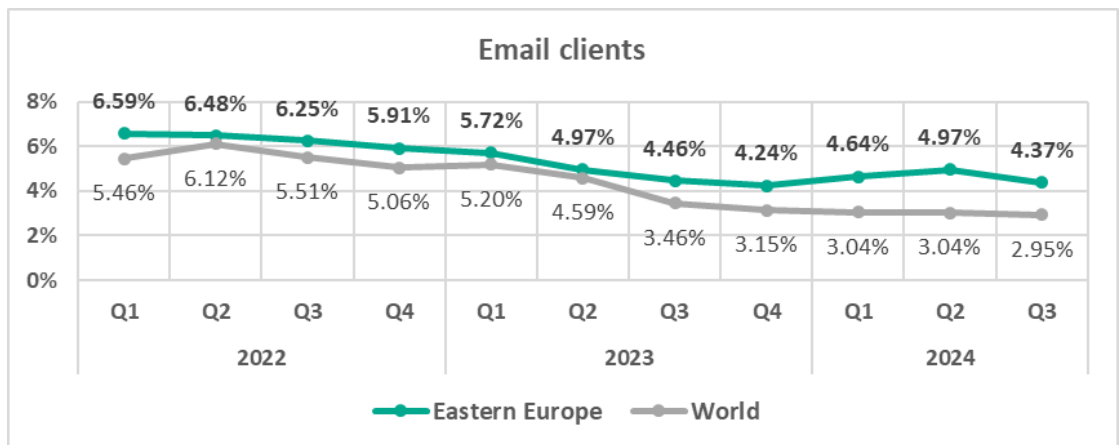
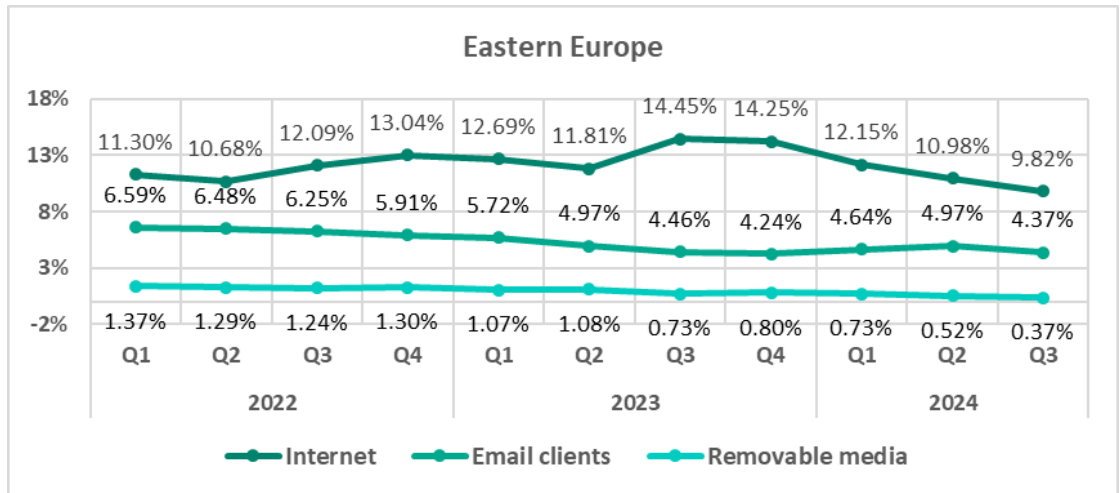


- The heatmap below illustrates changes in the rankings of threat categories in the region since the beginning of 2022. **Denylisted internet resources** has been the leading threat category in the region since Q1 2024. **Malicious scripts and phishing pages** fell from first to second place in Q1 2024.

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

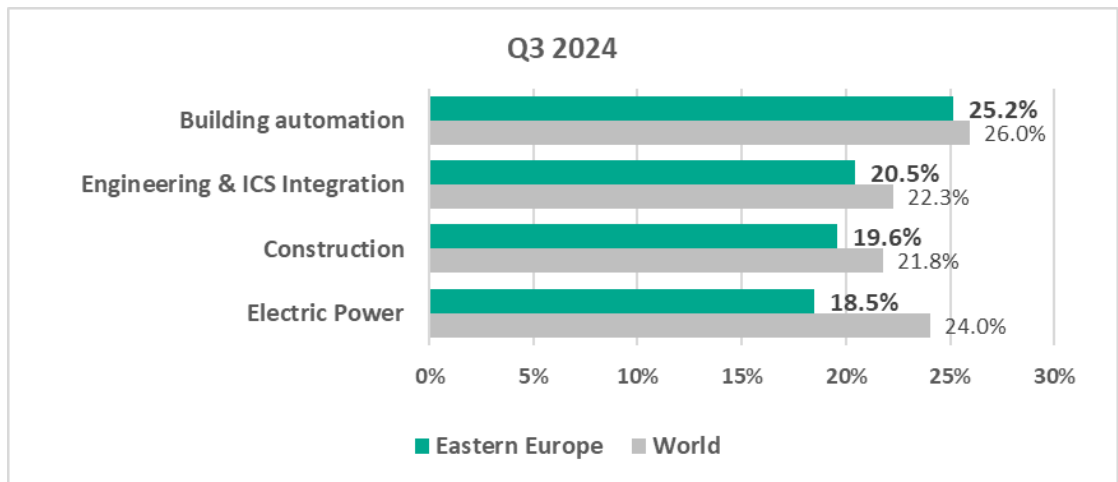
Threat sources

- In **Q3 2024**, all threats sources in Eastern Europe exhibited a **decrease** of the percentage of ICS computers on which they were blocked.

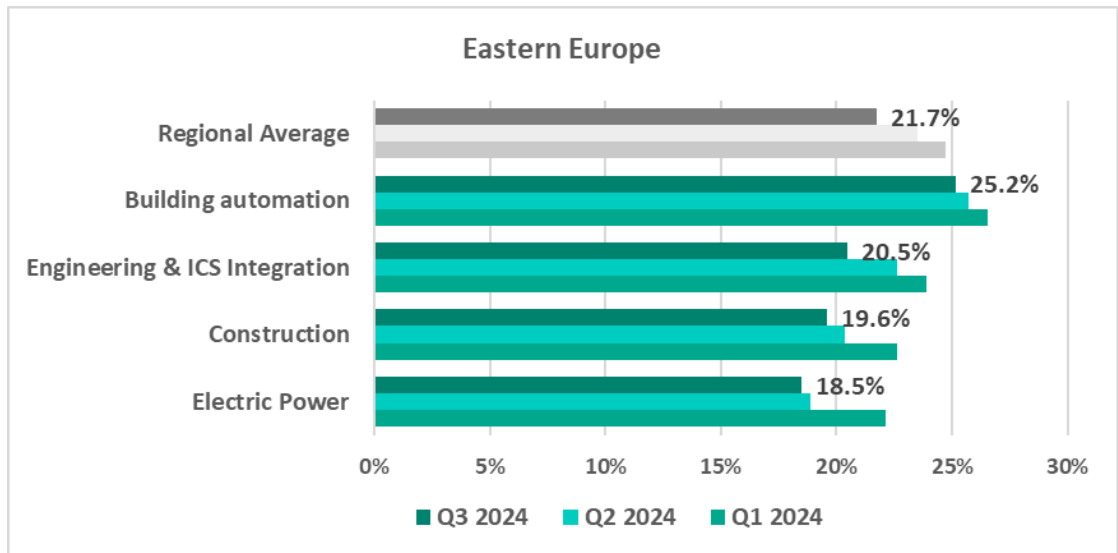


Industries

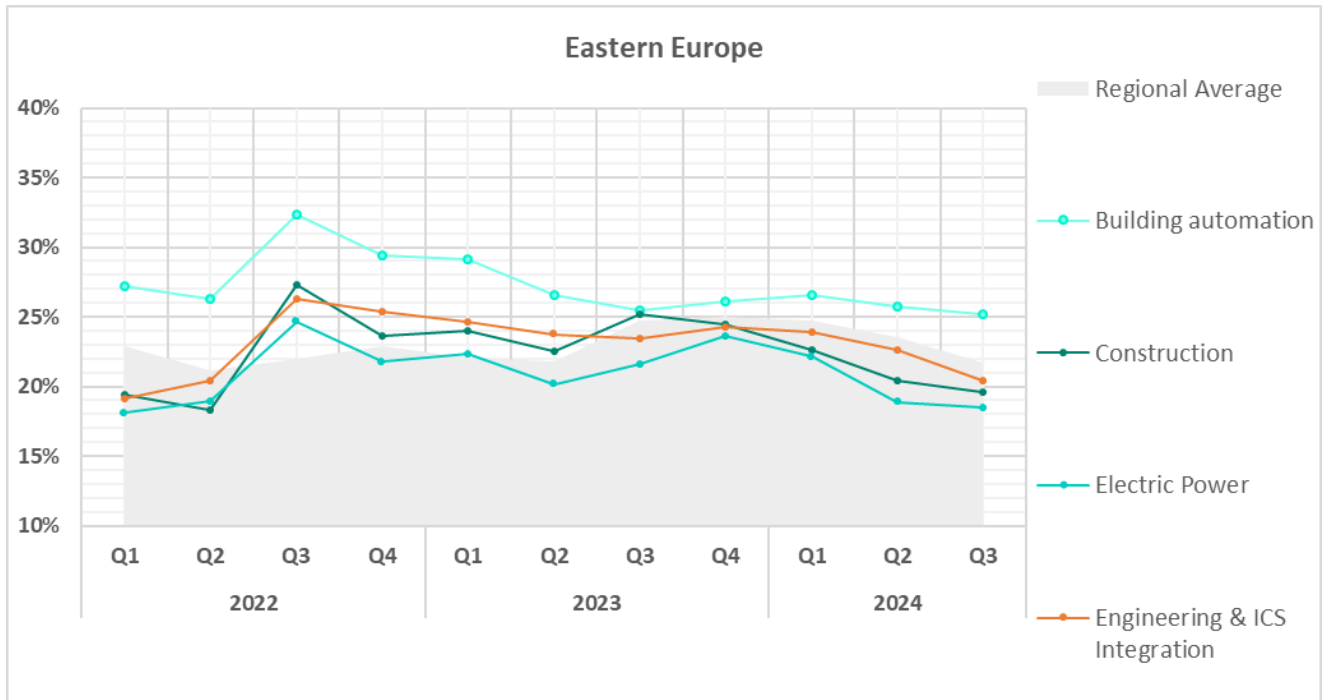
- The **most affected** industry in the region, as selected for this report, was **building automation**.
- Compared to the respective **global averages**, all selected industries demonstrated **lower percentages** of ICS computers on which malicious objects were blocked.



- In **Q3 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 still demonstrate a **general stabilization** after a notable rise in 2022.



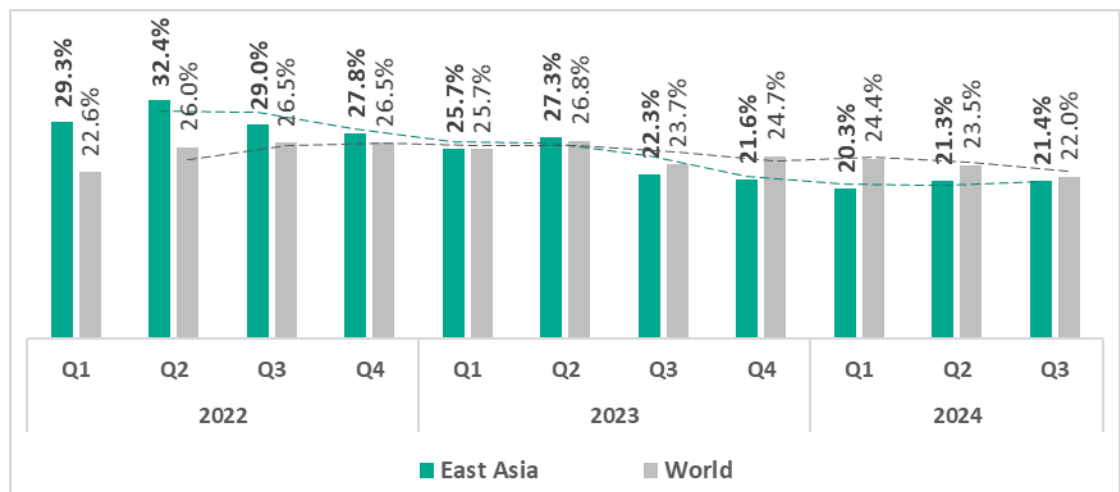
East Asia

Current threats

<p>N.1 IN THE REGION</p> <p>SPYWARE 4.35%</p> <p> slight increase in Q3 1st globally in growth</p> <p> 1.1x above global average</p>	<p>N.2 IN THE REGION</p> <p>MALICIOUS SCRIPTS & PHISHING PAGES 3.84%</p> <p> 1.1x increase in Q3</p>	<p>N.3 IN THE REGION</p> <p>DENYLISTED INTERNET RESOURCES 3.52%</p> <p> slight increase in Q3</p>
<p>VIRUSES 2.94%</p> <p> decrease in Q3</p> <p> 1.9x above global average 3rd in the world</p>	<p>MALICIOUS DOCUMENTS 1.39%</p> <p> 1.1x increase in Q3</p>	<p>WORMS 1.60%</p> <p> decrease in Q3</p> <p> 1.2x above global average</p>
<p>MALWARE FOR AUTOCAD 1.49%</p> <p> decrease in Q3</p> <p> 3.7x above global average 2nd in the world</p>	<p>RAMSOMWARE 0.19%</p> <p> 1.1x increase in Q3 3rd globally in growth</p> <p> 1.2x above global average</p>	
<p>THREATS FROM INTERNET 6.73%</p> <p> slight increase in Q3</p>	<p>THREATS FROM REMOVABLE DEVICES 1.27%</p> <p> decrease in Q3</p> <p> 1.8x above global average 3rd in the world</p>	<p>THREATS FROM NETWORK FOLDERS 0.30%</p> <p> decrease in Q3</p> <p> 2.7x above global average 1st in the world</p>

Overall

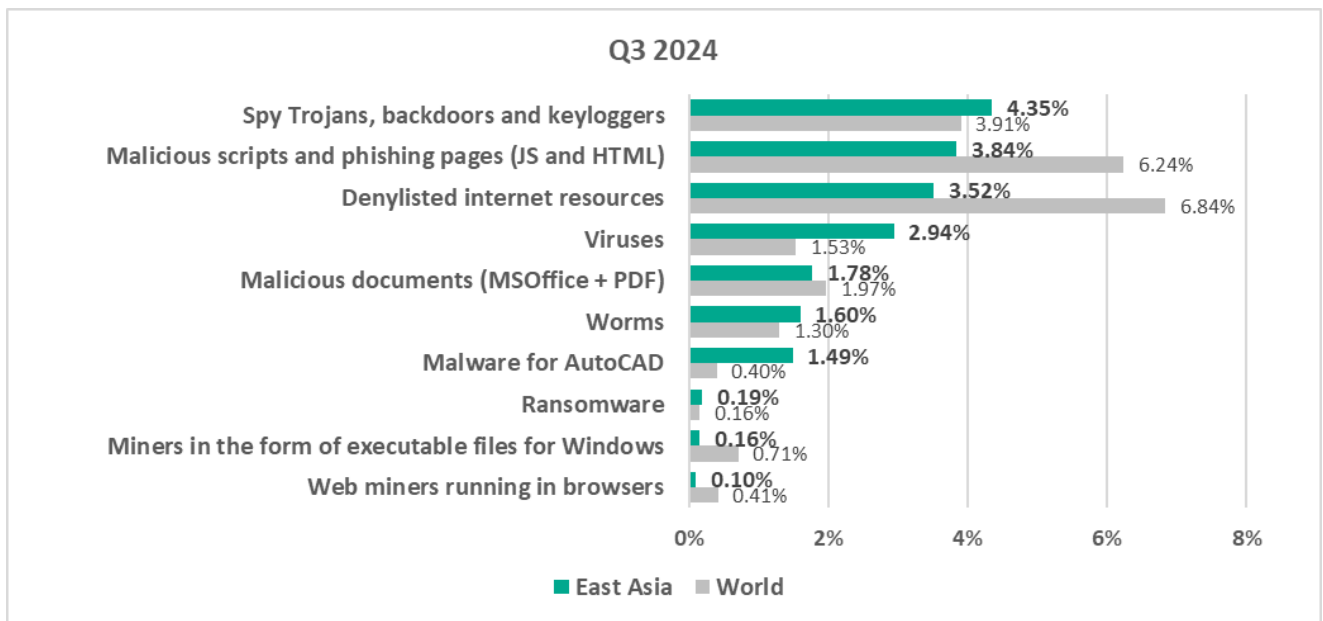
- **Eighth** place in the global ranking by percentage of ICS computers on which malicious objects were blocked.
- East Asia demonstrates a **downtrend** with fluctuations.
- The percentage of ICS computers on which malicious objects were blocked has been **below the global average** since Q3 2023.
- In **Q3 2024**, the region showed a slight **increase** in the percentage of ICS computers on which malicious objects were blocked compared to the previous quarter.



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, threats from removable devices
- **The only region in which spyware topped the malware category ranking** in terms of the percentage of ICS computers on which it was blocked.

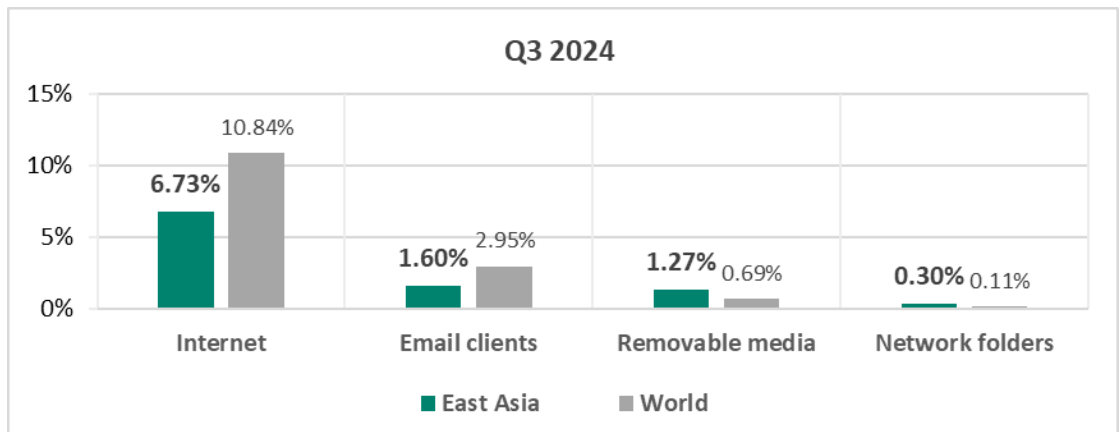
Threat categories



- **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
 - Ransomware, 1.2 times higher
 - Spyware, 1.1 times higher

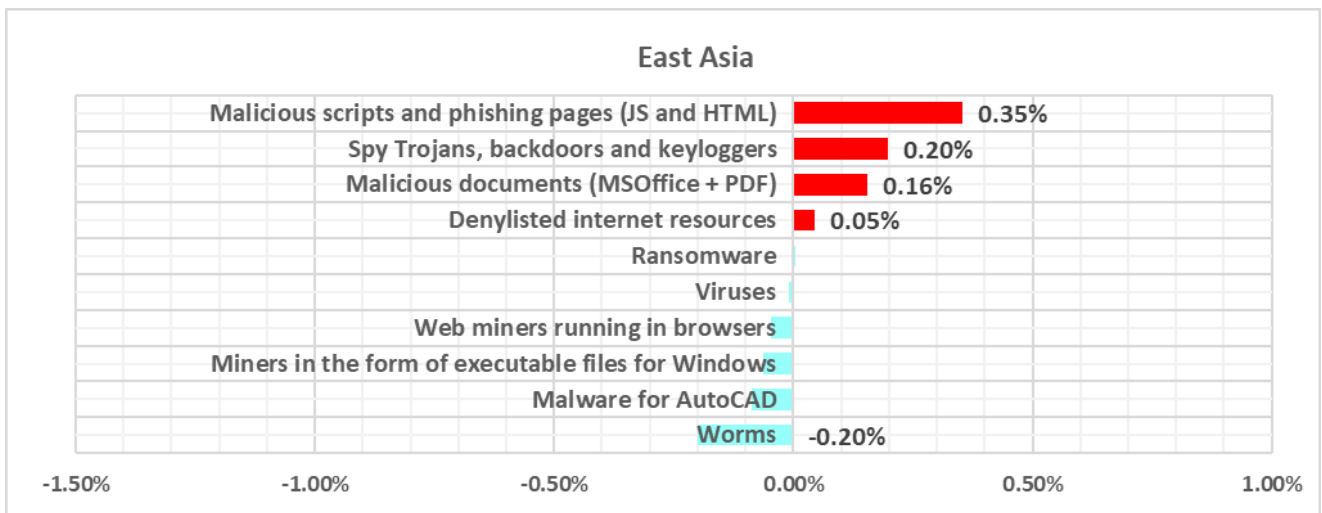
Threat sources

- In Q3 2024, East Asia ranked **first** again **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 1.8 times **higher than the global average**.

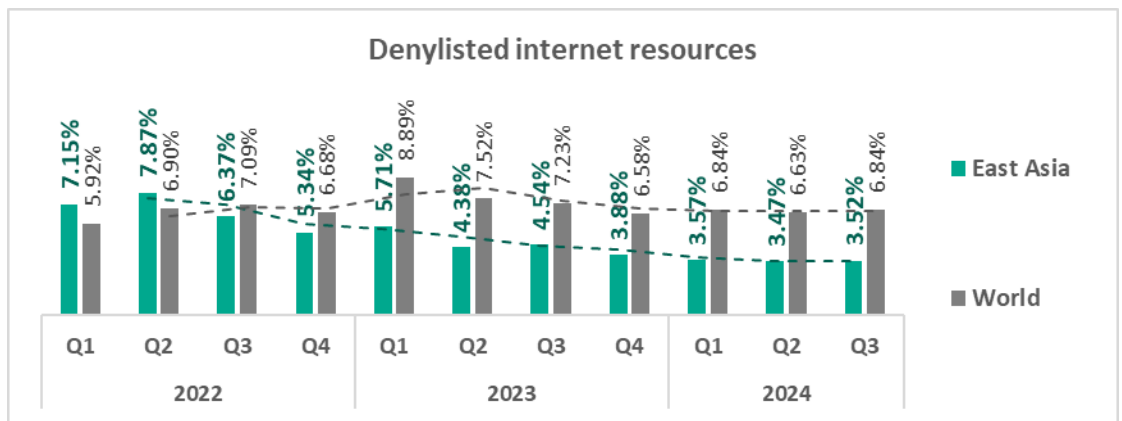
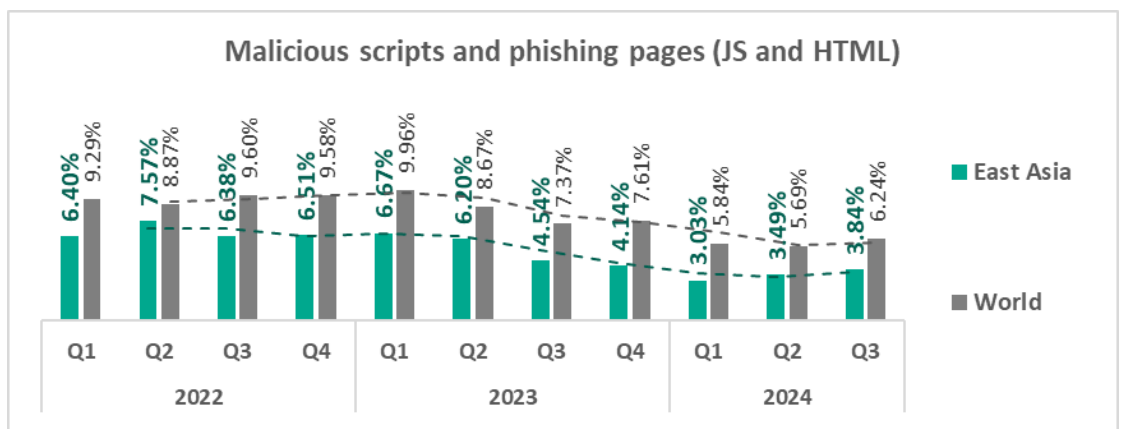
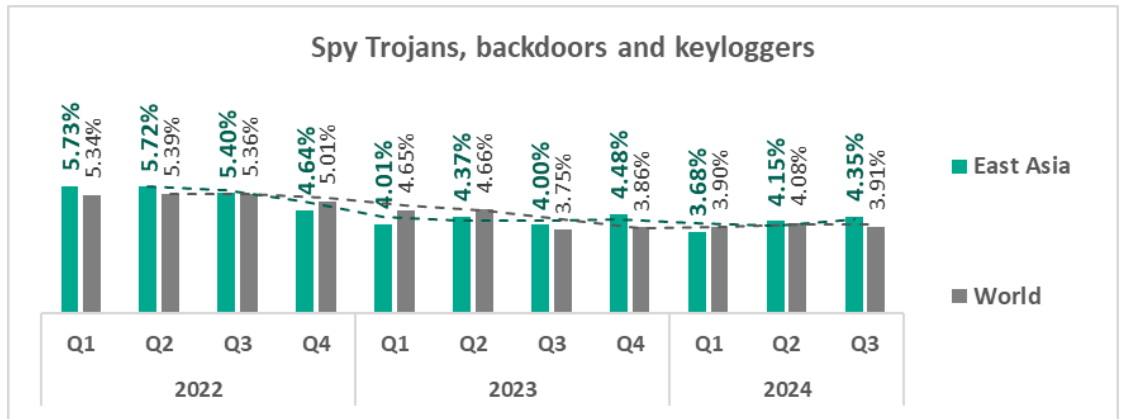


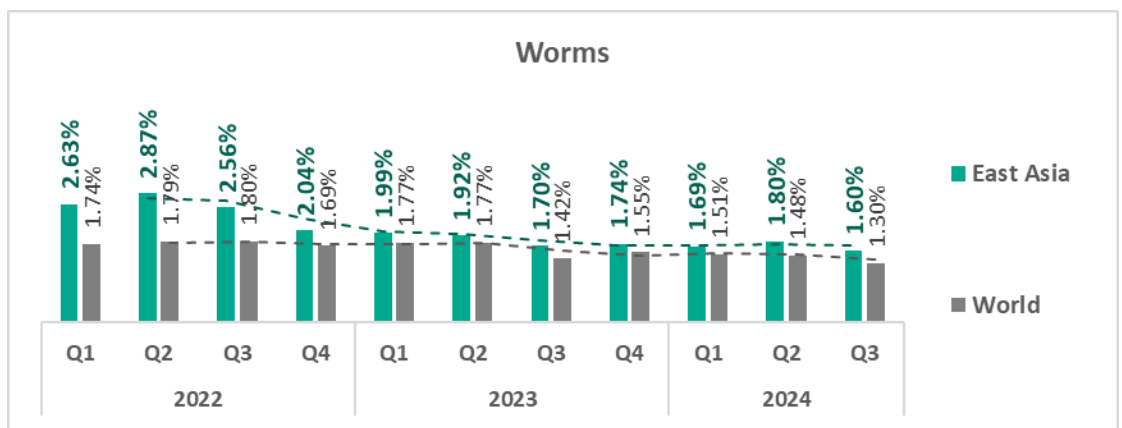
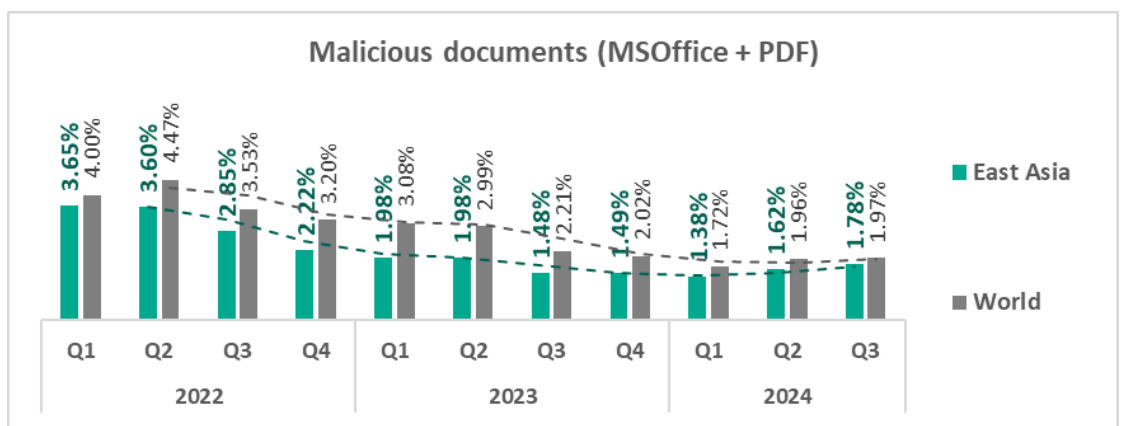
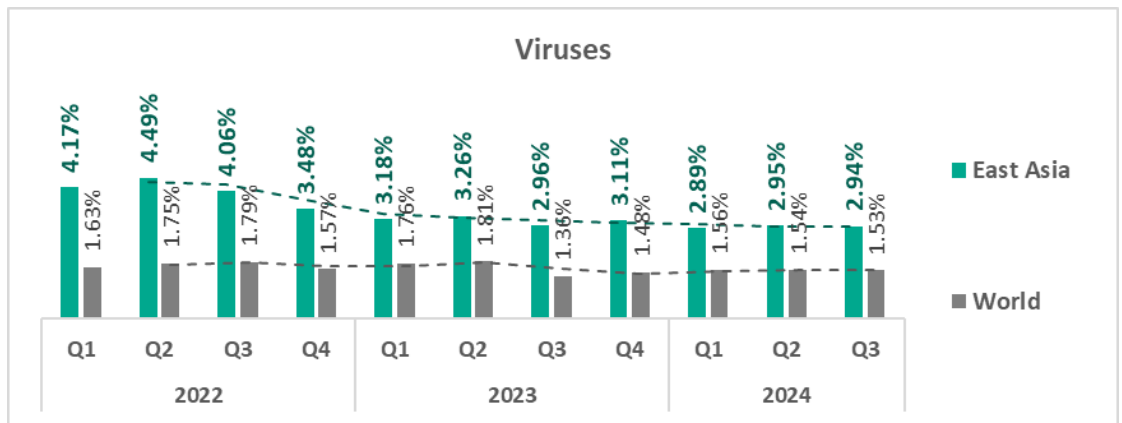
Quarterly changes and trends

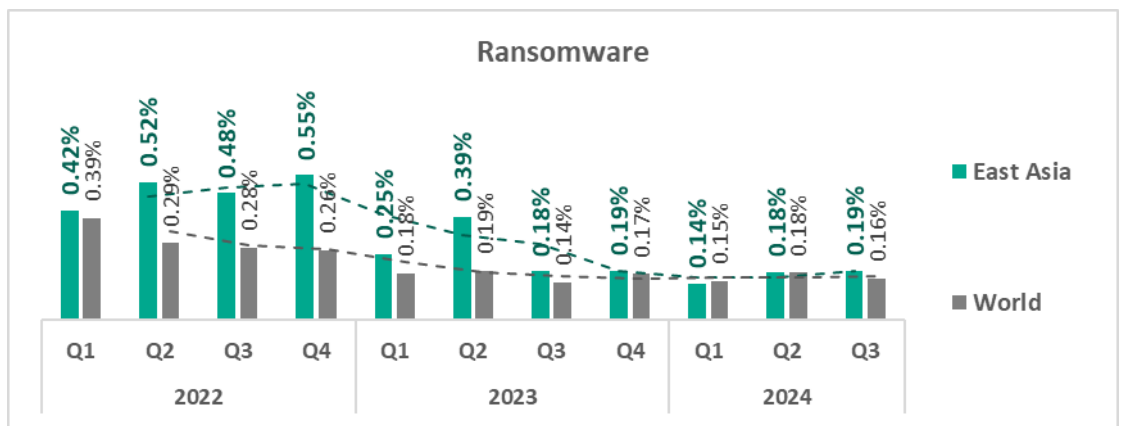
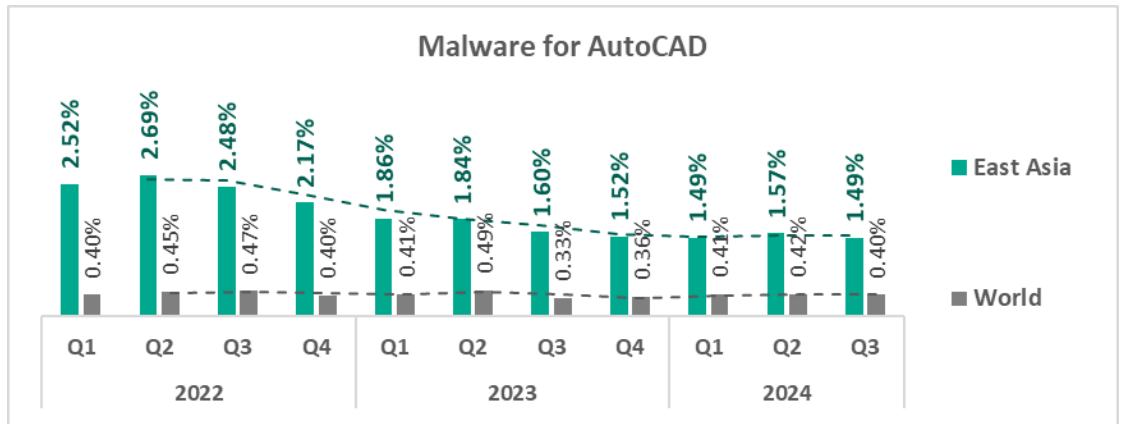
Threat categories



- The **largest proportional increase** in Q3 2024 was in the percentage of ICS computers on which the following were blocked:
 - Malicious scripts and phishing pages – by 1.1 times
 - Malicious documents – by 1.1 times
 - Ransomware – by 1.1 times
 - Spyware – by 1.1 times
- The **top threat** categories exhibit various quarterly dynamics:





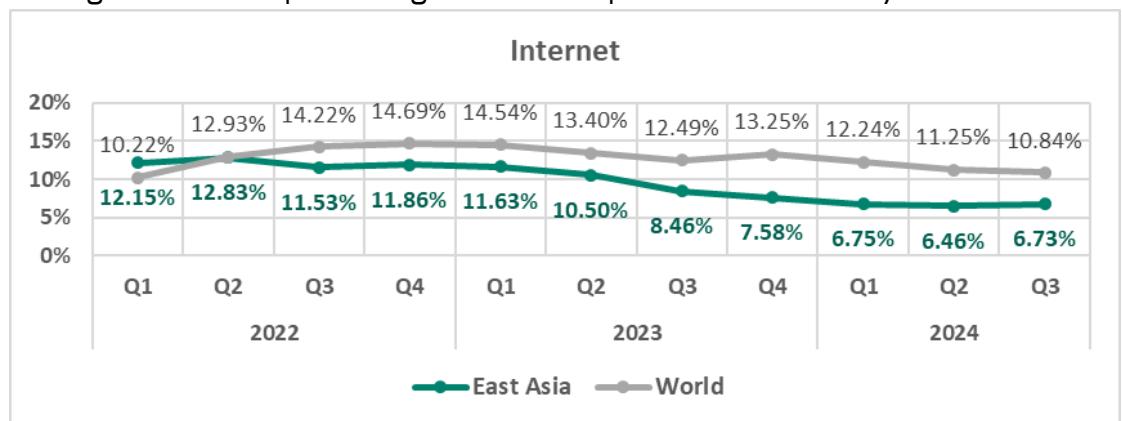


- The heatmap below illustrates changes in the rankings of threat categories in the region since the beginning of 2022. **Spyware** has been the leading threat category in the region since Q4 2023, jumping from third to first place and replacing **malicious scripts and phishing pages**. **Malicious documents** and **ransomware** moved up one position to fifth and eighth place, respectively.

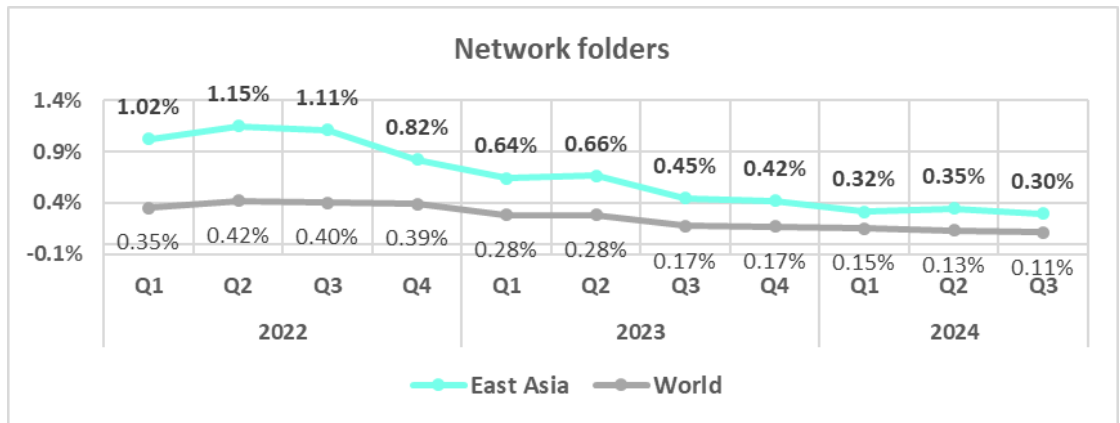
East Asia	2022				2023				2024			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	
Spy Trojans, backdoors and keyloggers	3	3	3	3	3	3	3	1	1	1	1	
Malicious scripts and phishing pages (JS and HTML)	2	2	1	1	1	1	1	2	3	2	2	
Denylisted internet resources	1	1	2	2	2	2	1	3	2	3	3	
Viruses	4	4	4	4	4	4	4	4	4	4	4	
Malicious documents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

Threat sources

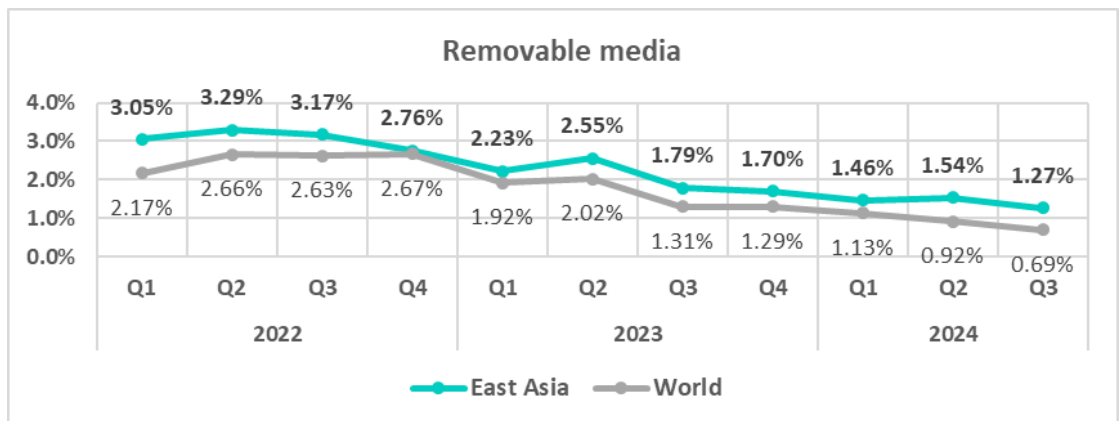
- Internet** threats exhibited an **increase in Q3 2024**, in contrast to the global average in terms of percentage of ICS computers on which they were blocked.



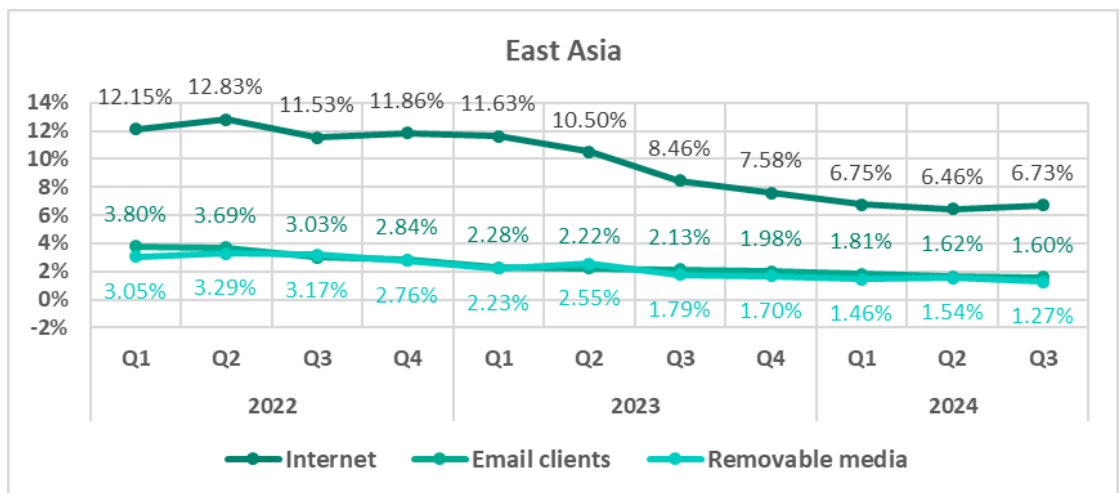
- **Network folder** threats which were blocked on ICS computers in East Asia continued to show a mostly **declining trend** started in the second half of 2022, staying significantly above the global average.



- The region exhibited a **decrease** in threats distributed via **removable devices**.

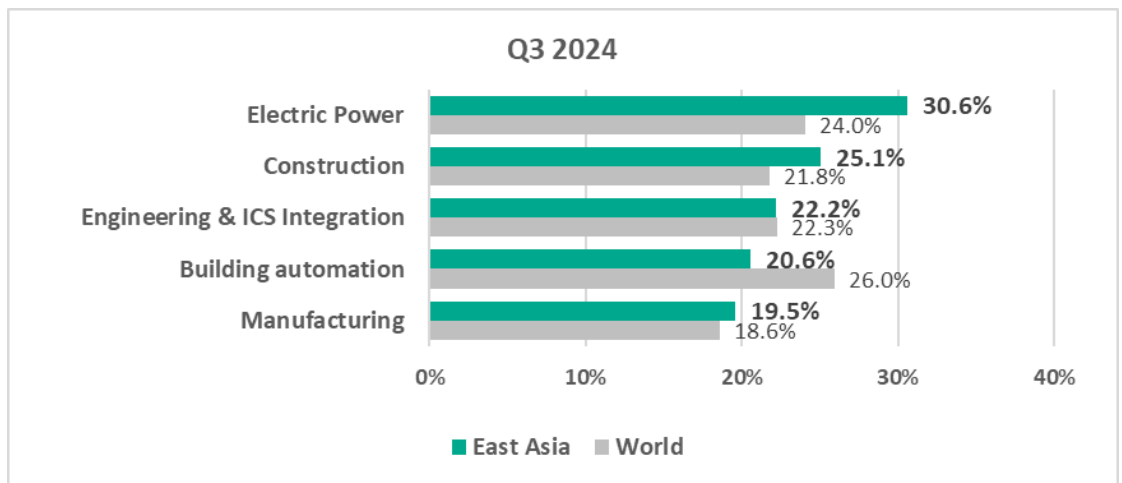


- Overall, all major sources exhibit **downward long-term trends**.

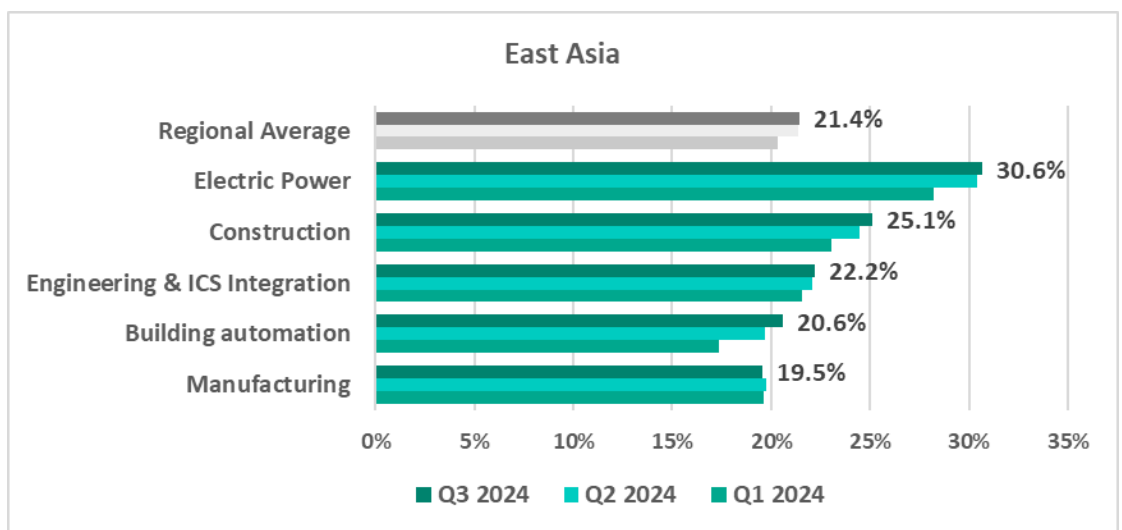


Industries

- The most **affected industry** in the region, as selected for this report, was **electric power**.
- 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:
 - Electric power, 1.3 times higher
 - Construction, 1.2 times higher

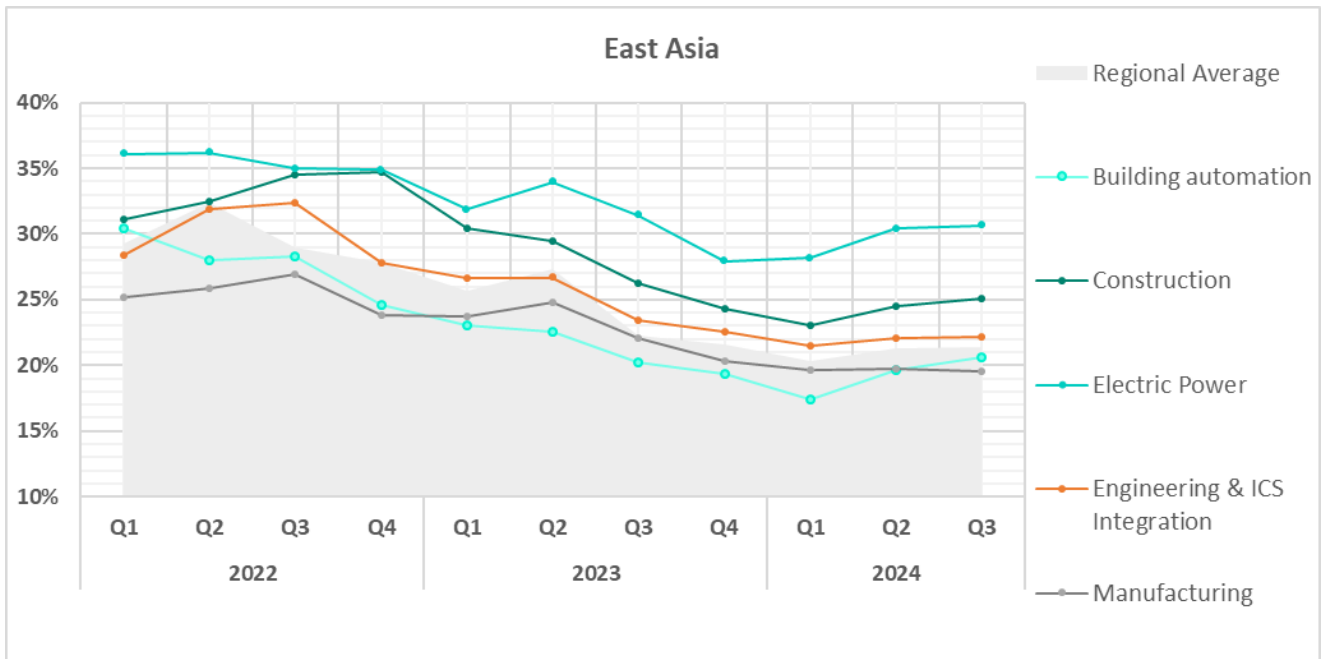


- In **Q3 2024**, all sectors, except for manufacturing, exhibited an **increase** in the percentage of ICS computers on which malicious objects were blocked.















- The **electric power** sector consistently exhibited the **highest rate of blocked malicious objects** on ICS computers throughout the period, significantly above the regional average.

All sectors, except manufacturing, showed an **upward trend starting in Q2 2024**.



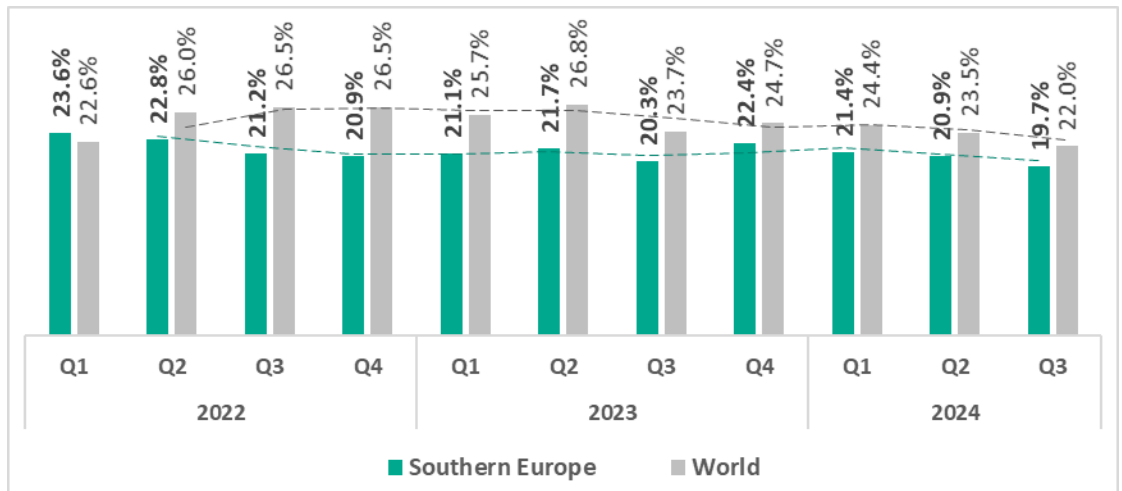
Southern Europe

Current threats

<p>N.1 IN THE REGION</p> <p>MALICIOUS SCRIPTS & PHISHING PAGES</p> <p>8.27%</p> <p> 1.1x increase in Q3</p> <p> 1.1x above global average 3rd in the world</p>	<p>N.2 IN THE REGION</p> <p>DENYLISTED INTERNET RESOURCES</p> <p>5.79%</p> <p> 1.1x increase in Q3</p>	<p>N.3 IN THE REGION</p> <p>SPYWARE</p> <p>5.37%</p> <p> decrease in Q3</p> <p> 1.4x above global average</p>
<p>MALICIOUS DOCUMENTS</p> <p>3.35%</p> <p> decrease in Q3</p> <p> 1.7x above global average 2nd in the world</p>	<p>RANSOMWARE</p> <p>0.21%</p> <p> 1.1x increase in Q3 1st globally in growth</p> <p> 1.3x above global average</p>	
<p>THREATS FROM INTERNET</p> <p>9.67%</p> <p> slight increase in Q3</p>	<p>THREATS FROM EMAIL CLIENTS</p> <p>5.88%</p> <p> decrease in Q3</p> <p> 2x above global average 1st in the world</p>	

Overall

- **Ninth** 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**.
- In **Q3 2024**, the region saw a 1.1-fold **decrease** in the percentage of ICS computers on which malicious objects were blocked.

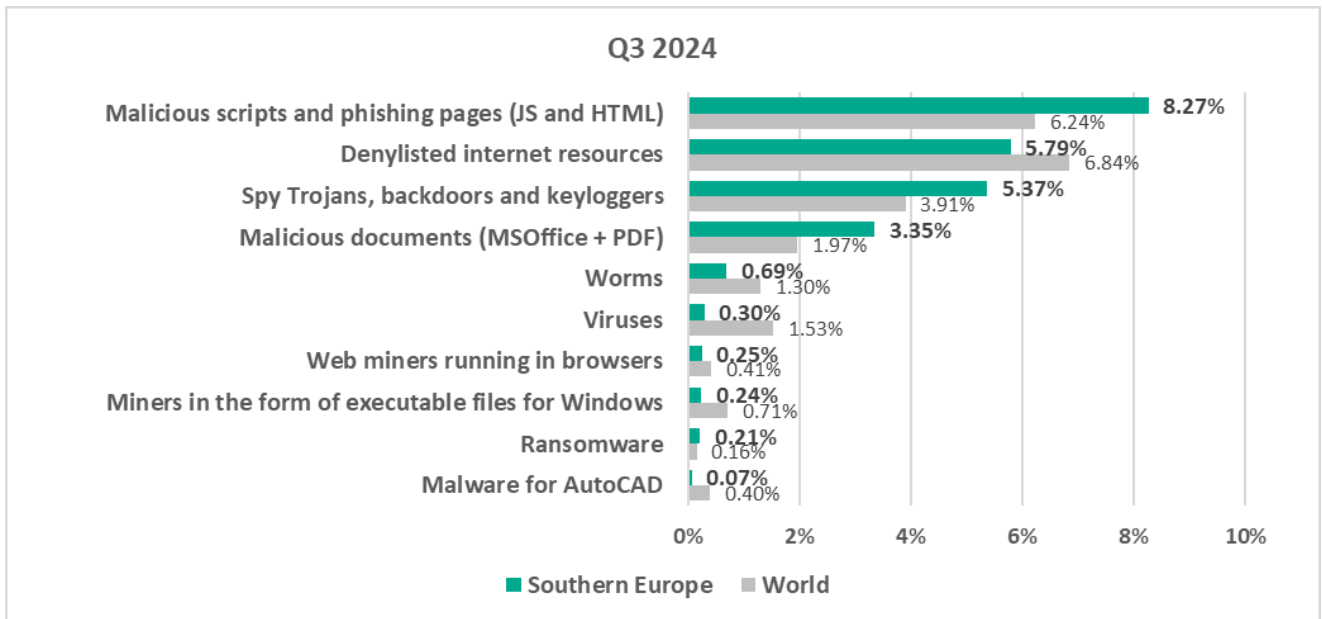


Comparative analysis

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

- First place – threats from email clients
- Second place – malicious documents
- Third place – malicious scripts and phishing pages

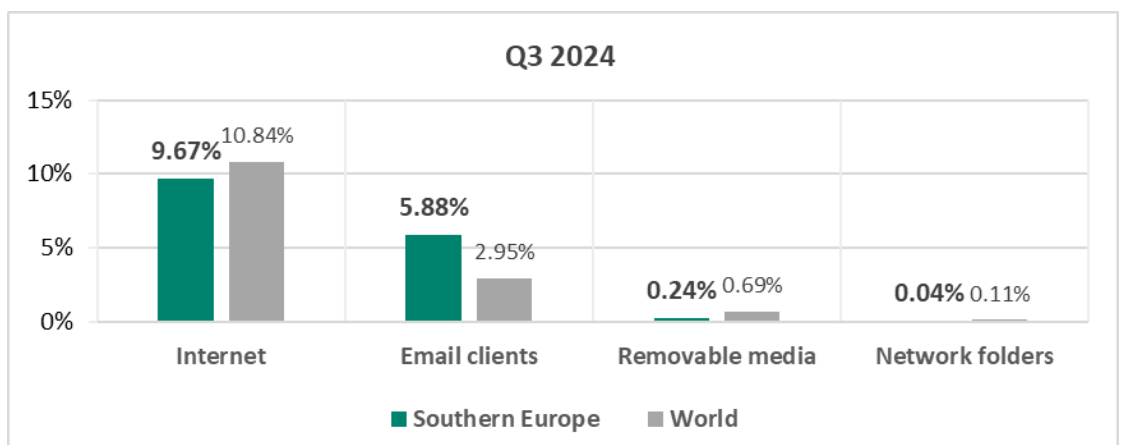
Threat categories



- **Compared to the global average**, the region has a higher percentage of ICS computers on which the following were blocked:
 - Malicious documents, 1.7 times higher
 - Spyware, 1.4 times higher
 - Malicious scripts and phishing pages, 1.3 times higher
 - Ransomware, 1.3 times higher

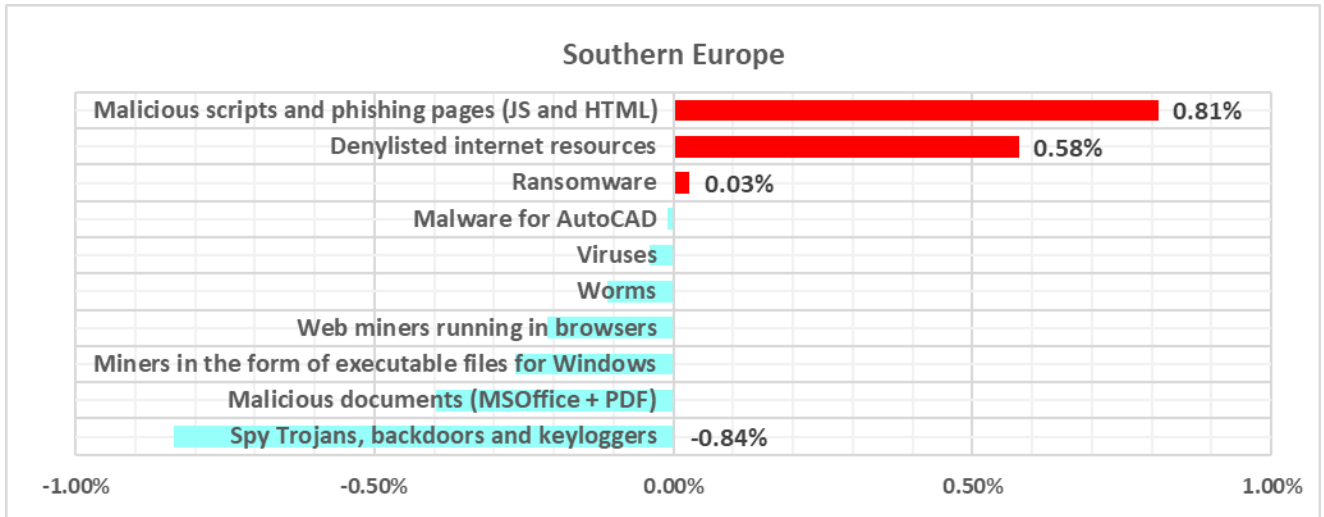
Threat sources

- 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 times.

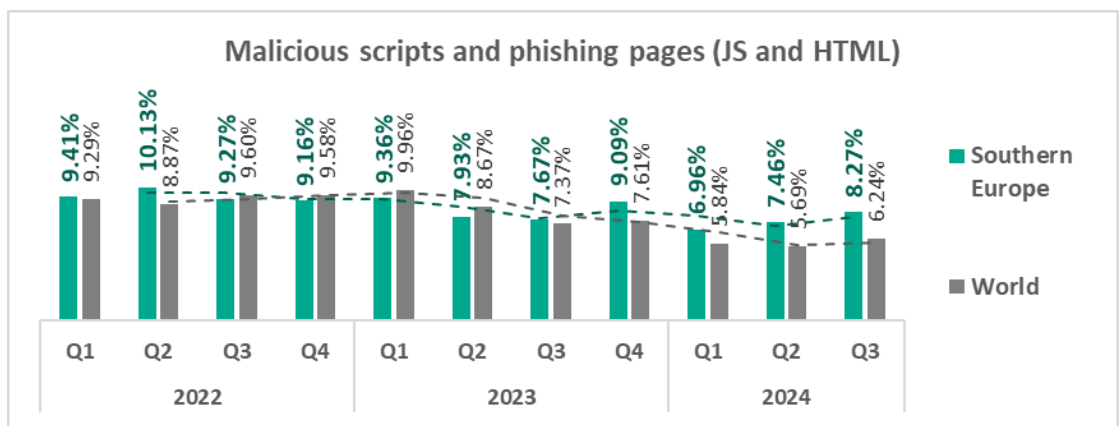


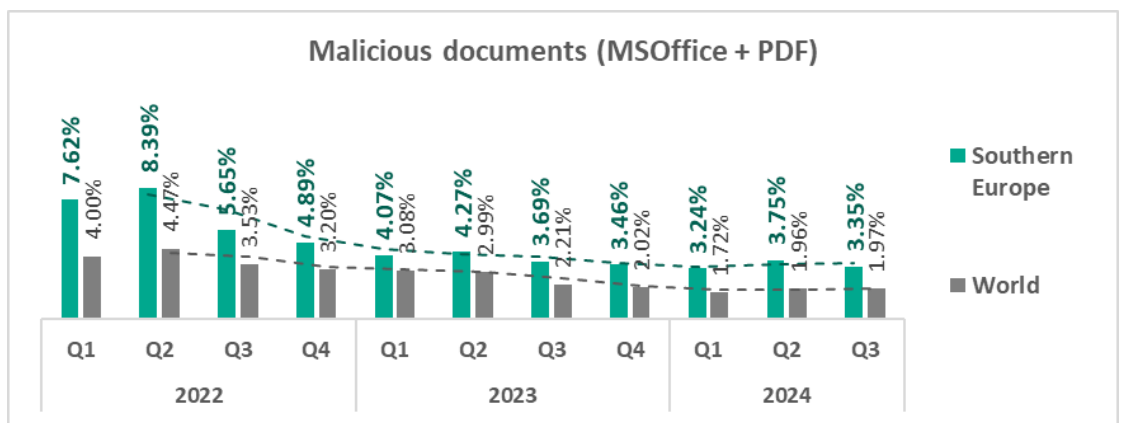
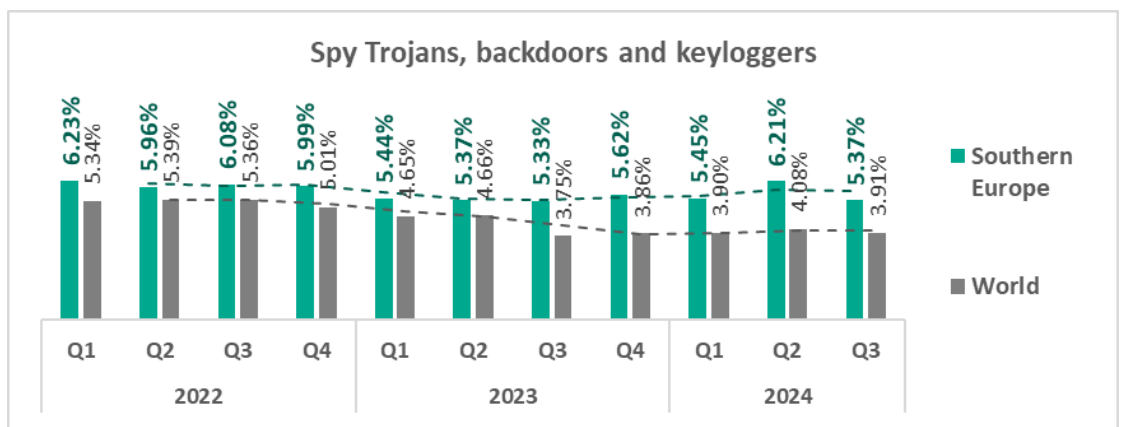
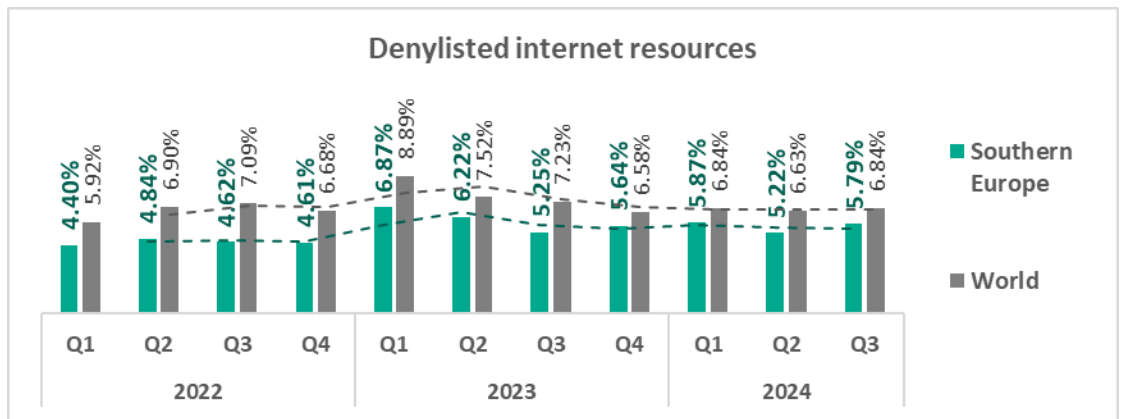
Quarterly changes and trends

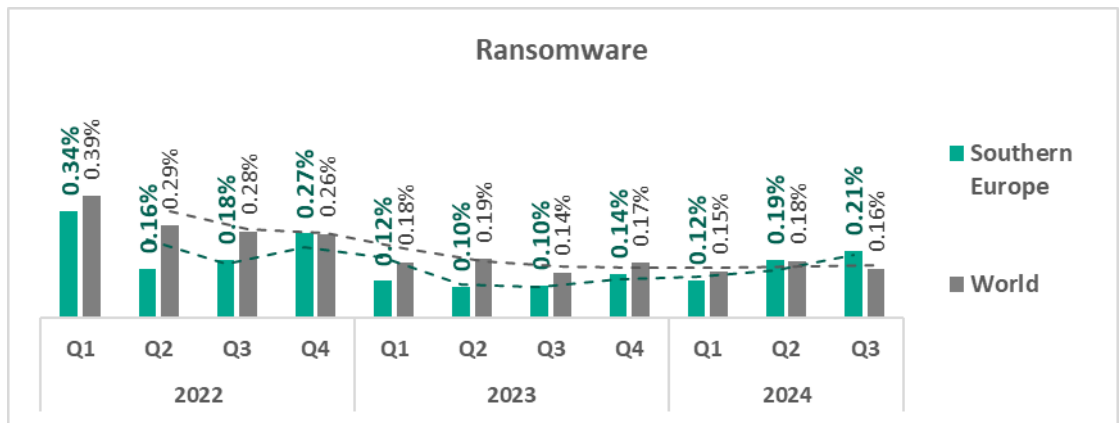
Threat categories



- The **largest proportional increase** in Q3 2024 was in the percentage of ICS computers on which the following were blocked:
 - Ransomware, by 1.1 times
 - Malicious scripts and phishing pages, by 1.1 times
 - Denylisted internet resources, by 1.1 times
- The **top threat** categories exhibit various quarterly dynamics:





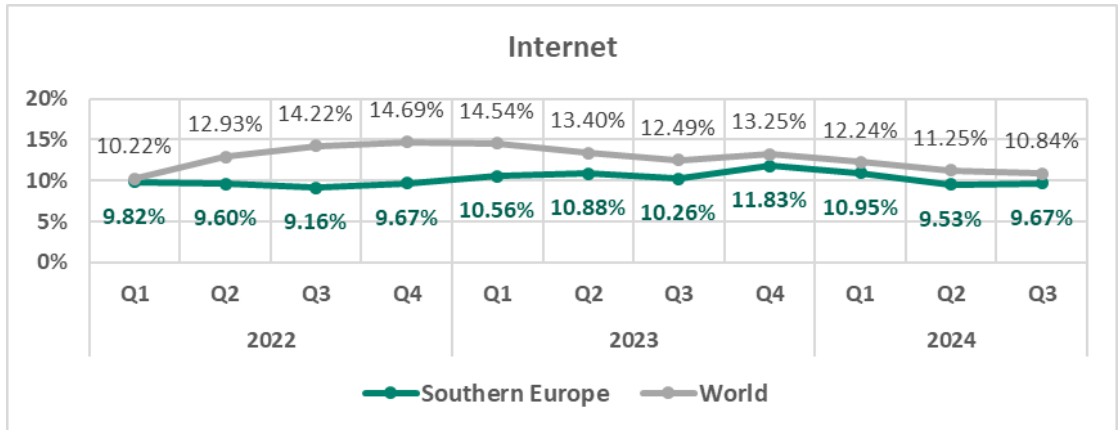


- The heatmap below illustrates changes in the rankings of threat categories in the region since the beginning of 2022. **Malicious scripts and phishing pages** have been the leading threat category in the region throughout the observed period. **Denylisted internet resources** moved back to second from third place in Q3 2024. **Viruses** jumped from eighth to sixth place due to a substantial decrease in threats from both categories of miners.

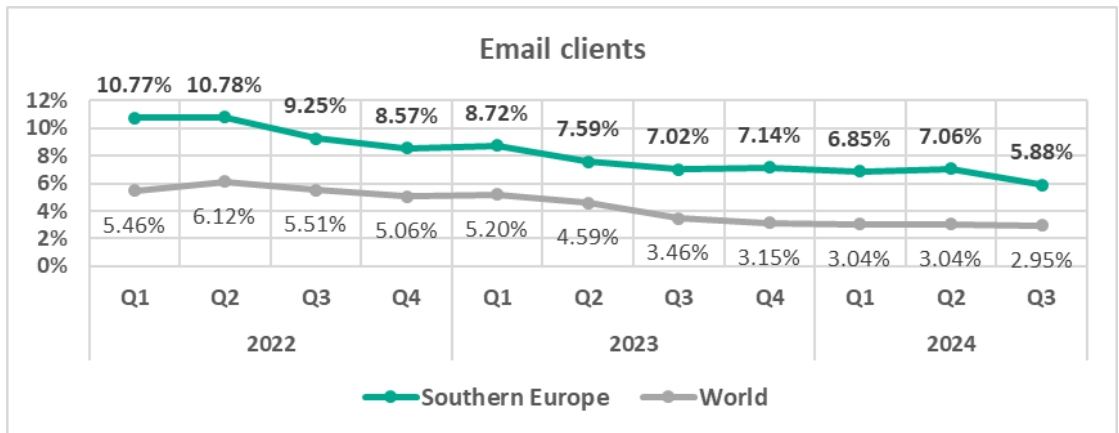
Southern Europe	2022				2023				2024		
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3
Malicious scripts and phishing pages (JS and HTML)	1	1	1	1	1	1	1	1	1	1	1
Denylisted internet resources	4	4	4	4	2	2	3	2	2	3	2
Spy Trojans, backdoors and keyloggers	3	3	2	2	3	3	2	3	3	2	3
Malicious documents (MSOffice + PDF)	2	2	3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

Threat sources

- In **Q3 2024**, the percentage of ICS computers on which threats from **internet** were blocked **increased** compared to the previous quarter, in contrast to the global trend.

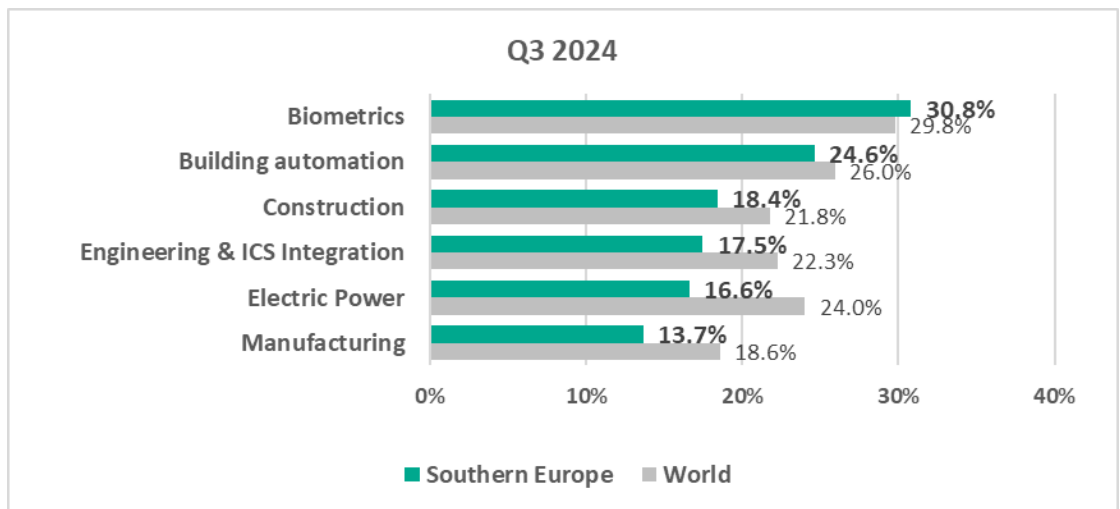


- Threats from **email clients** showed a **decrease** in percentage of ICS computers on which they were blocked, compared to the previous quarter.

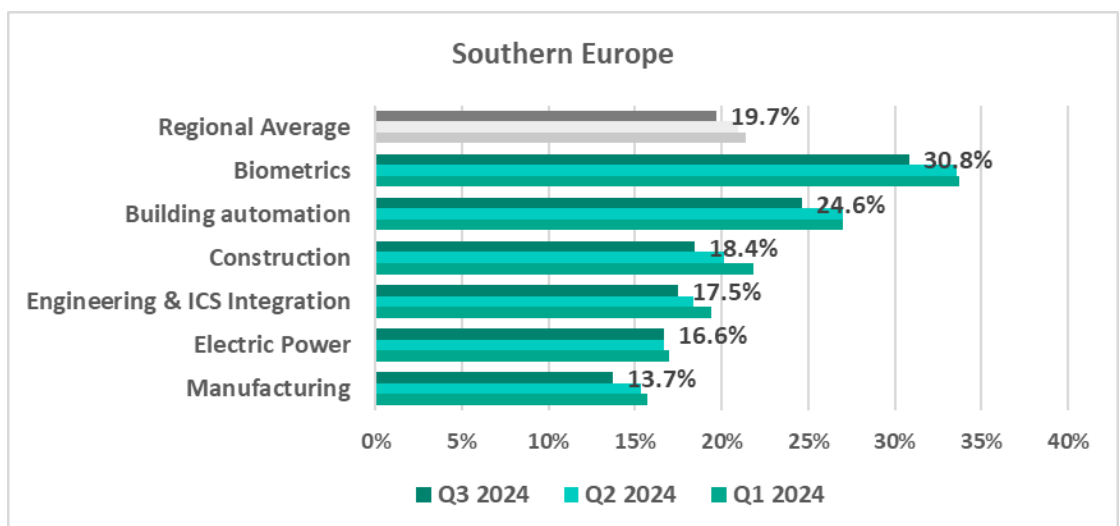


Industries

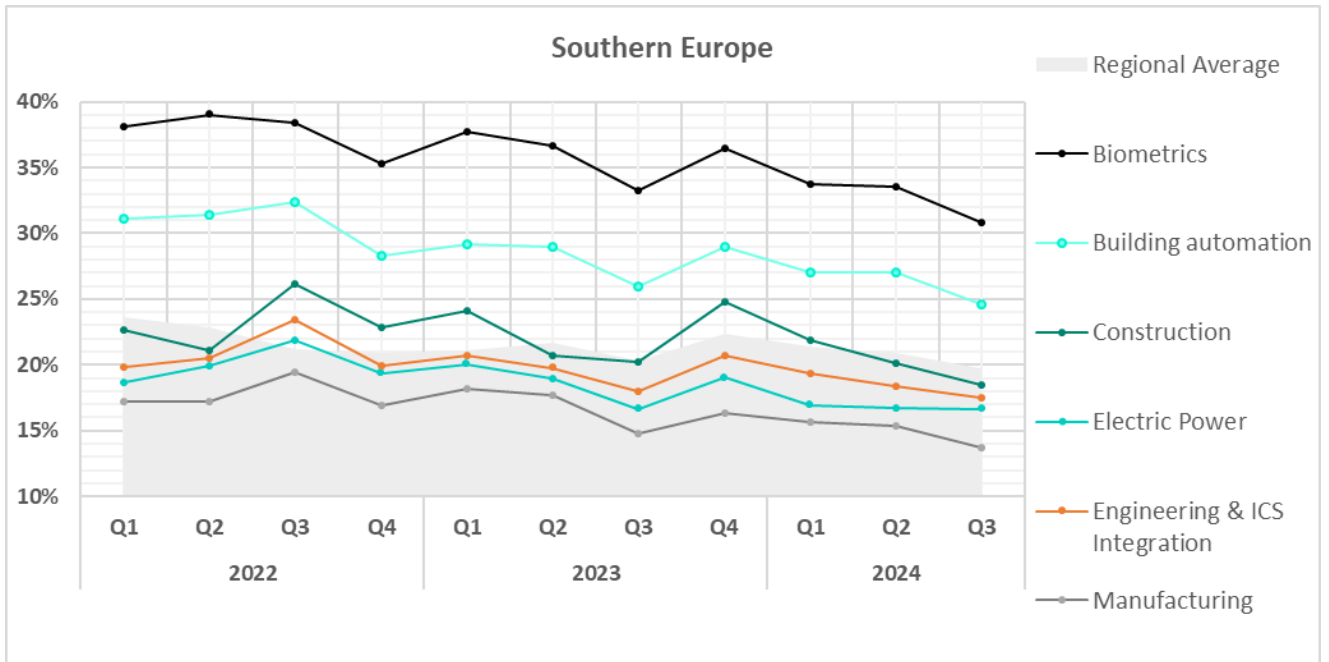
- The most **affected industry** in the region, as selected for this report, was **biometrics**.
- Compared to the respective **global averages**, the **biometrics** sector saw a **higher percentage** of ICS computers on which malicious objects were blocked in Q3 2024.



- In **Q3 2024**, all sectors under observation in the region exhibited a **decrease** in the percentage of ICS computers on which malicious objects were blocked.



- All selected sectors exhibit **fluctuating long-term trends** in terms of percentage of ICS computers on which malicious objects were blocked. The rates in the **biometrics** and **building automation** sectors remain significantly **higher than the regional average**.



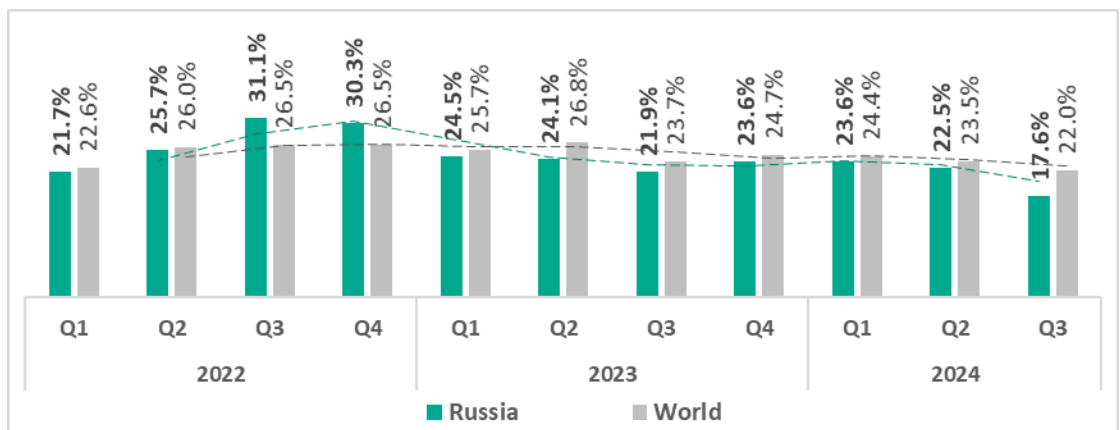
Russia

Current threats

<p>N.1 IN THE REGION</p> <p>DENYLISTED INTERNET RESOURCES</p> <p>6.26%</p> <p>decrease in Q3</p>	<p>N.2 IN THE REGION</p> <p>MALICIOUS SCRIPTS & PHISHING PAGES</p> <p>3.71%</p> <p>decrease in Q3</p>	<p>N.3 IN THE REGION</p> <p>SPYWARE</p> <p>2.07%</p> <p>decrease in Q3</p>
<p>EXECUTABLE MINERS</p> <p>0.98%</p> <p>decrease in Q3</p> <p>1.4x above global average 2nd in the world</p>	<p>WEB MINERS</p> <p>0.40%</p> <p>1.1x increase in Q3 1st globally in growth</p>	<p>THREATS FROM INTERNET</p> <p>8.94%</p> <p>decrease in Q3</p>

Overall

- **Tenth** in the global ranking by percentage of ICS computers on which malicious objects were blocked.
- In **Q3 2024**, the region saw a significant **decrease** (by a factor of 1.3) in threats that were blocked on ICS computers.

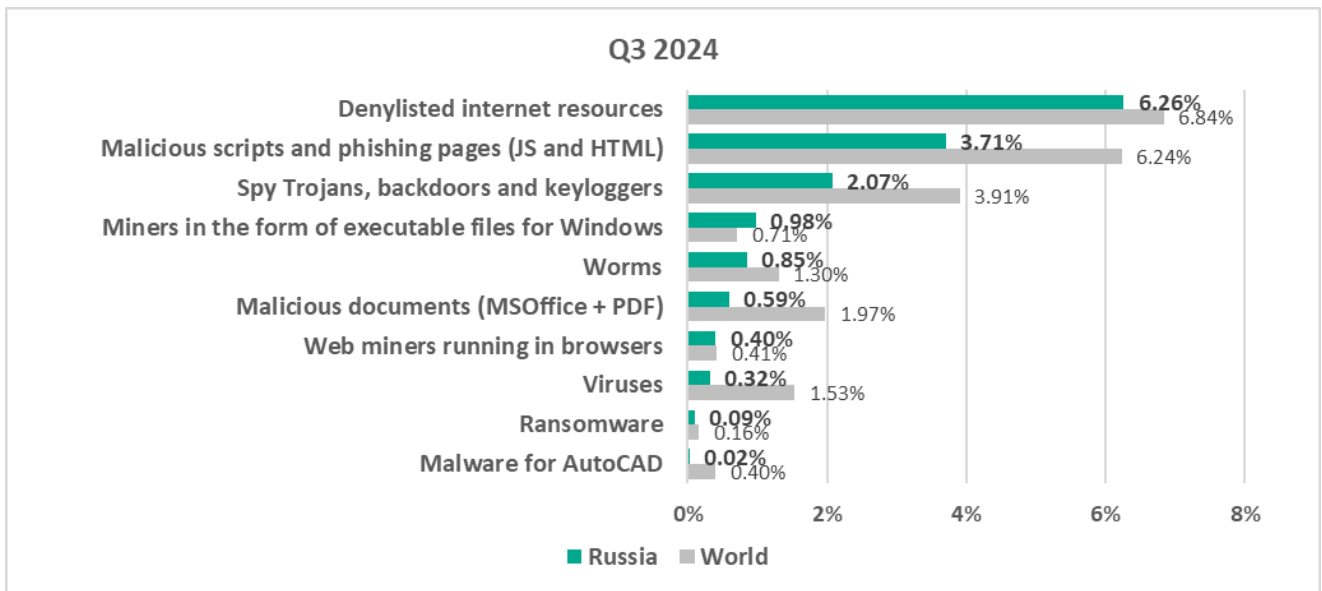


Comparative analysis

In Q3 2024, Russia occupied **second place** among regions by percentage of ICS computers on which **miners in the form of executable files for Windows** were blocked.

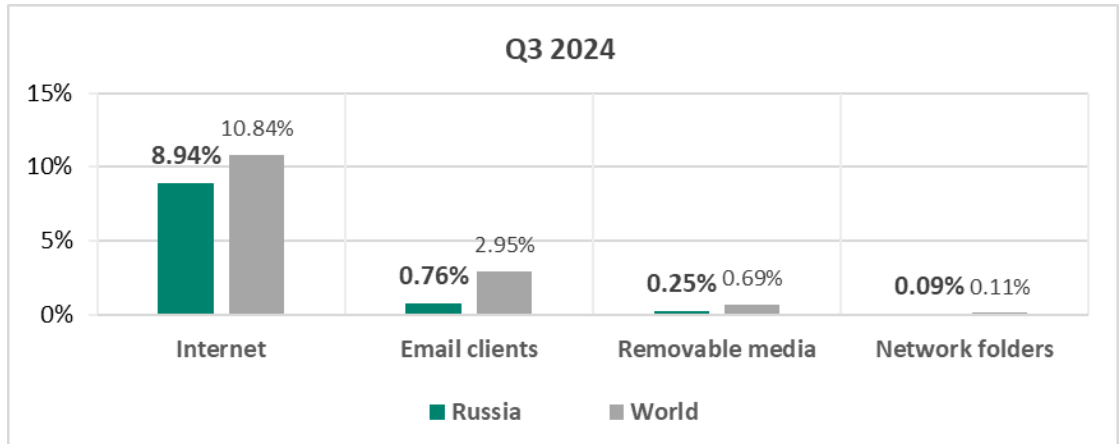
Threat categories

- **Compared to global figures**, the region has a **higher percentage** of ICS computers on which miners in the form of executable files for Windows – 1.4 times higher.



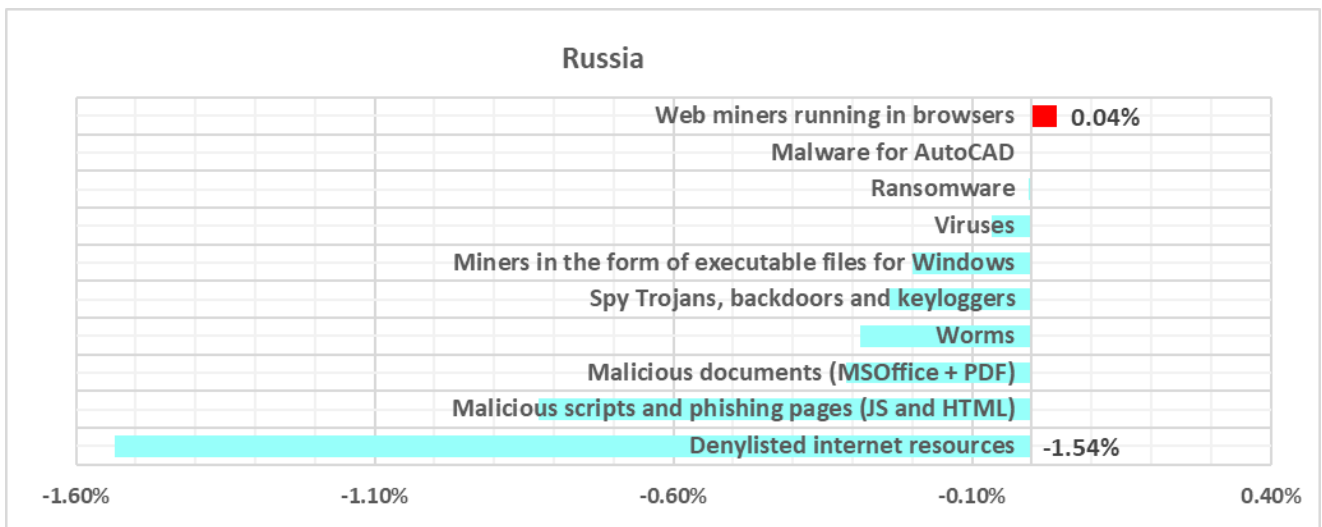
Threat sources

The region showed **lower rates** for all threat sources compared to the **respective global averages** for these sources.



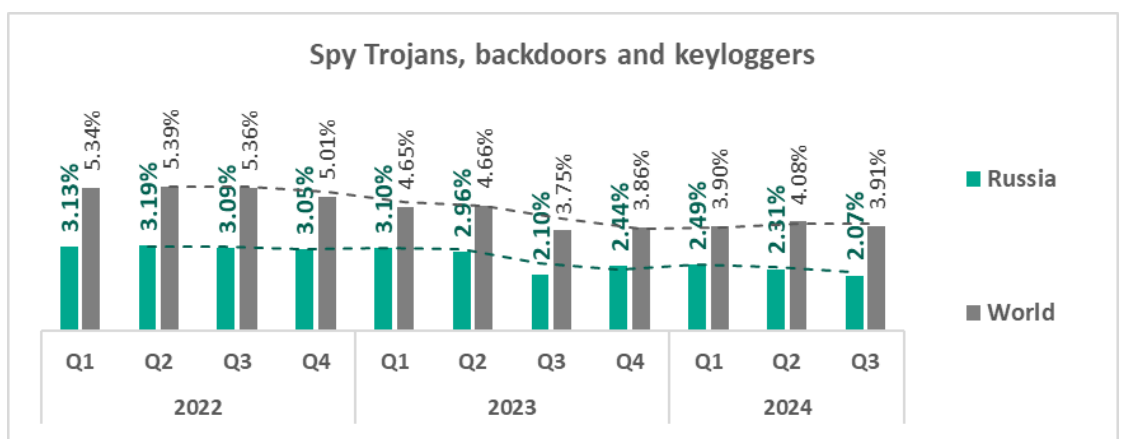
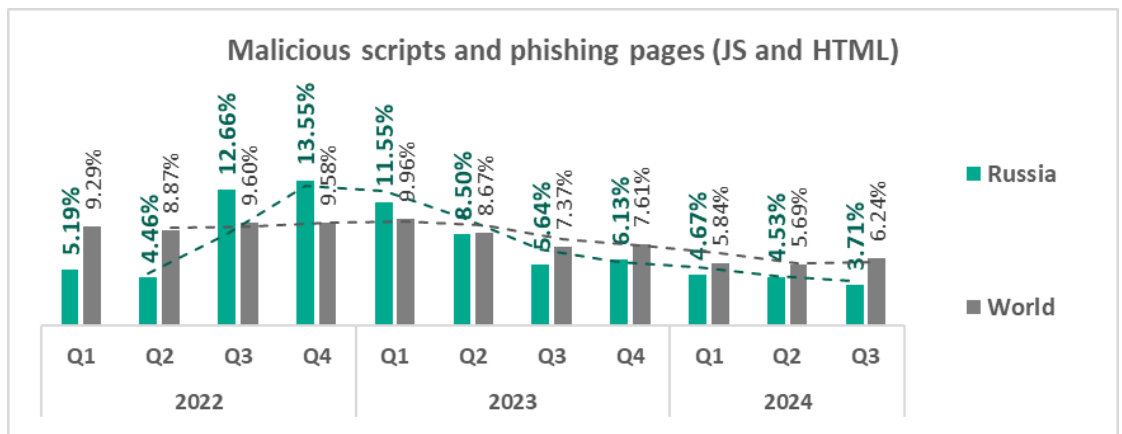
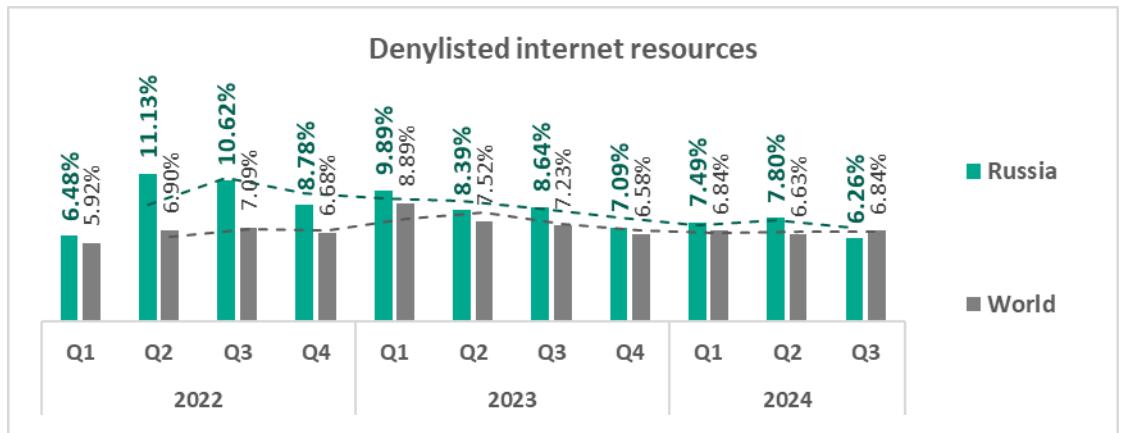
Quarterly changes and trends

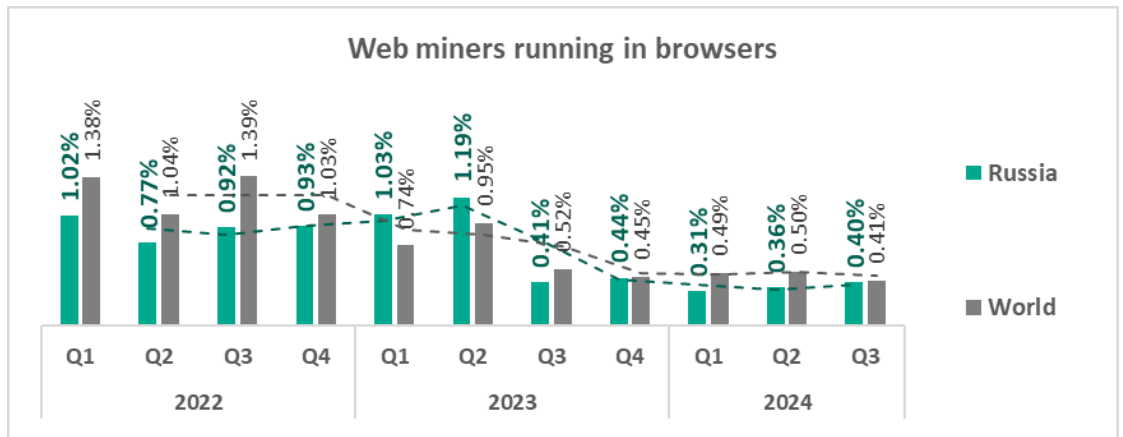
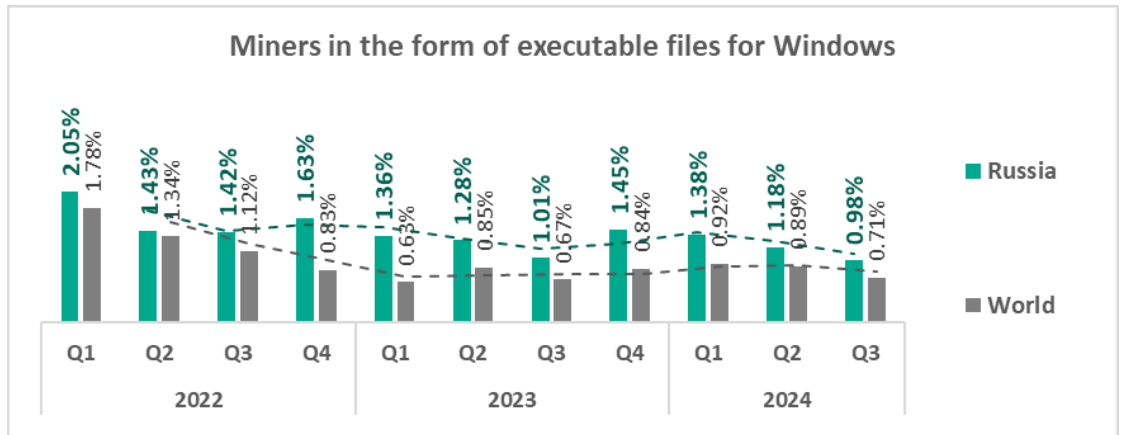
Threat categories



- The **only increase** in Q3 2024 was in the percentage of ICS computers on which the web miners were blocked – by a factor of 1.1.

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



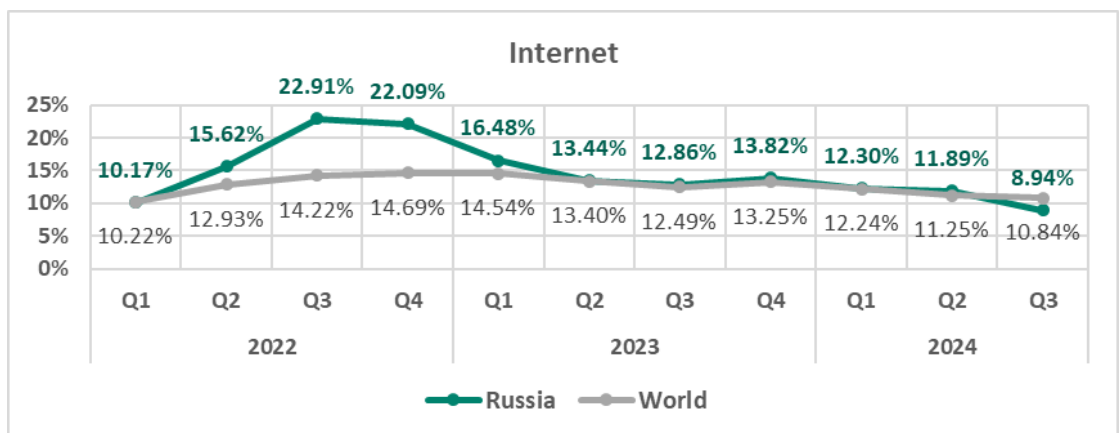


- The heatmap below illustrates changes in the rankings of threat categories in the region since the beginning of 2022. **Denylisted internet resources** have been the leading threat category in the region since Q3 2023. **Web miners** moved one position up in Q3 2024 – from eight to seventh.

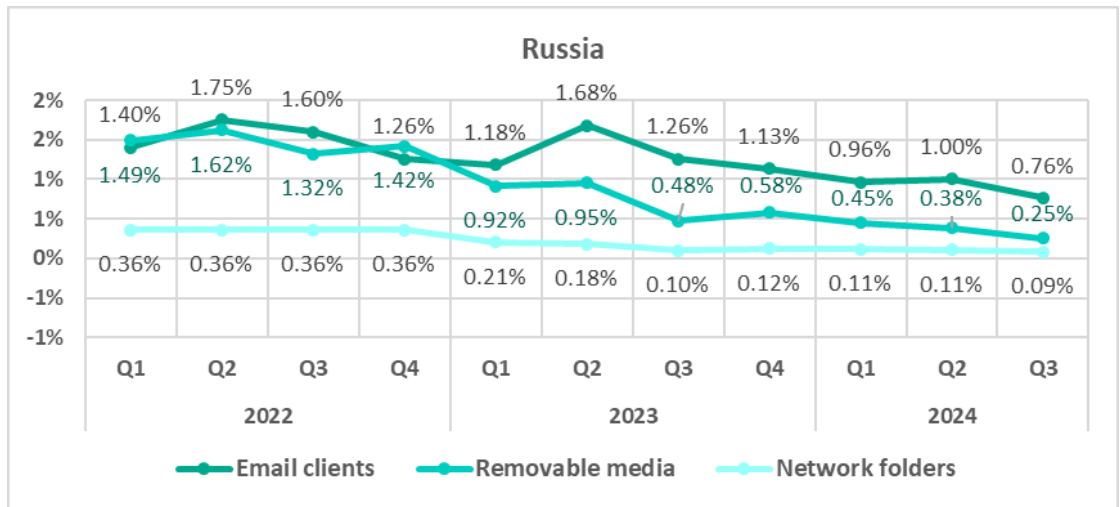
Russia	2022				2023				2024		
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3
Denylisted internet resources	1	1	2	2	2	2	1	1	1	1	1
Malicious scripts and phishing pages (JS and HTML)	2	2	1	1	1	1	2	2	2	2	2
Spy Trojans, backdoors and keyloggers	3	3	3	3	3	3	3	3	3	3	3
Miners in the form of executable files for Windows	4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

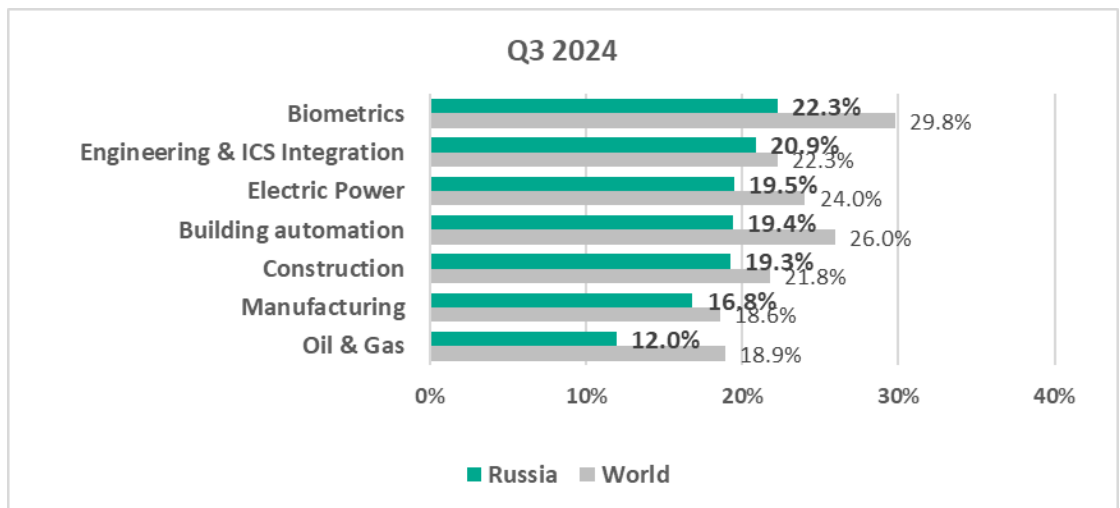


- Other threat sources exhibit predominantly **downward trends**.

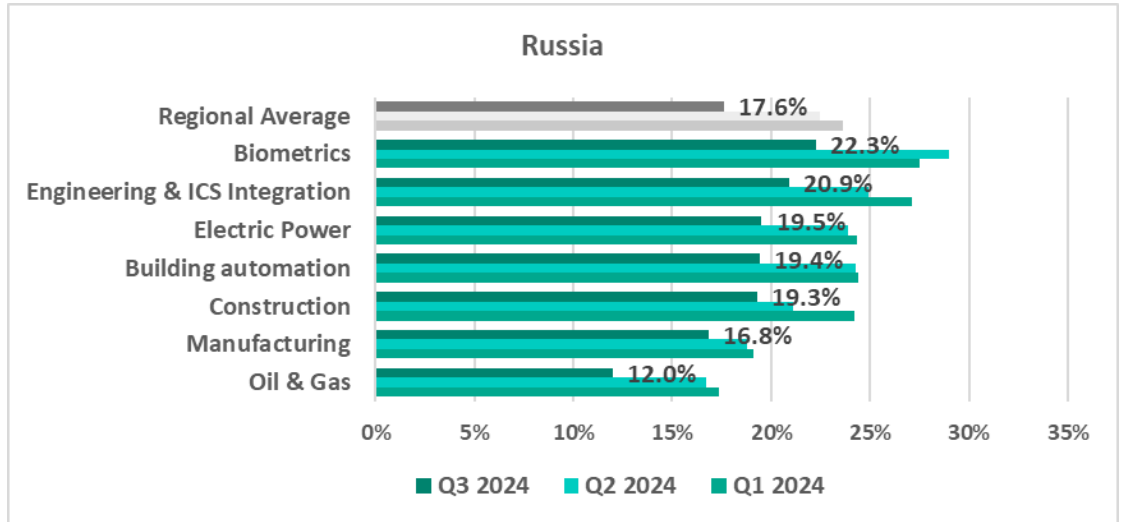


Industries

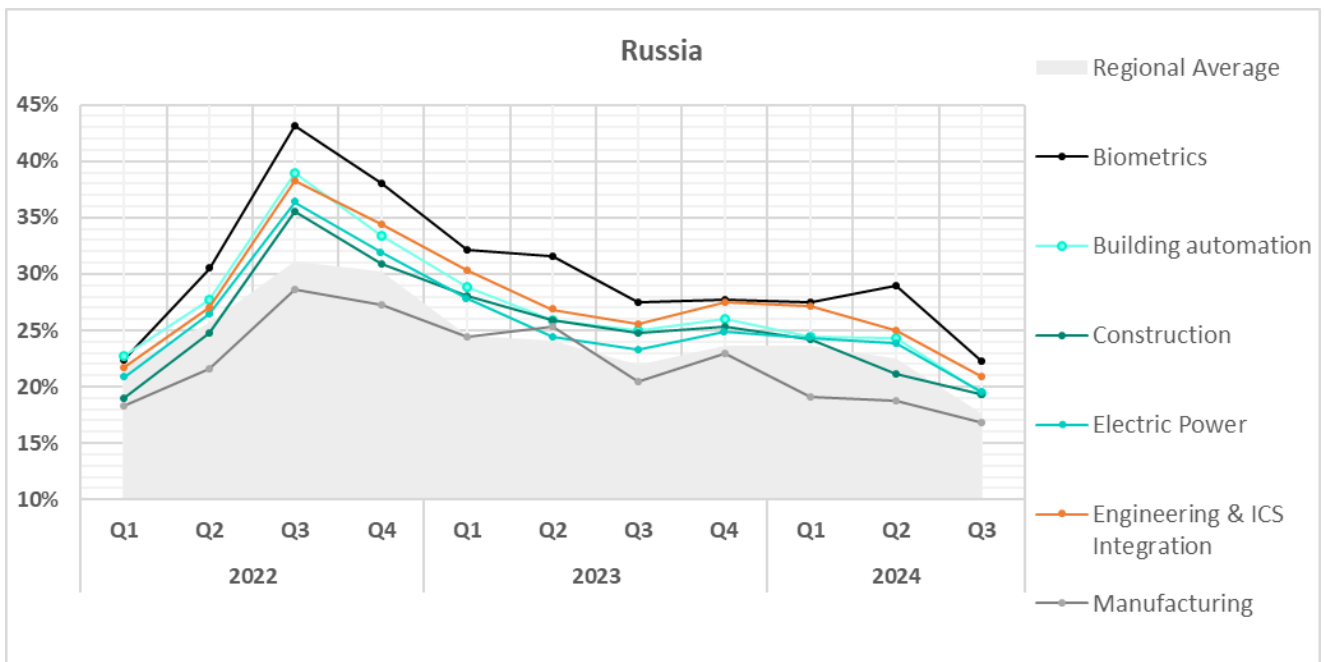
- The most **affected industry** in the region, as selected for this report, was **biometrics**.
- Compared to the **global averages**, all sectors under study saw a **lower percentage** of ICS computers on which malicious objects were blocked.



- In **Q3 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.



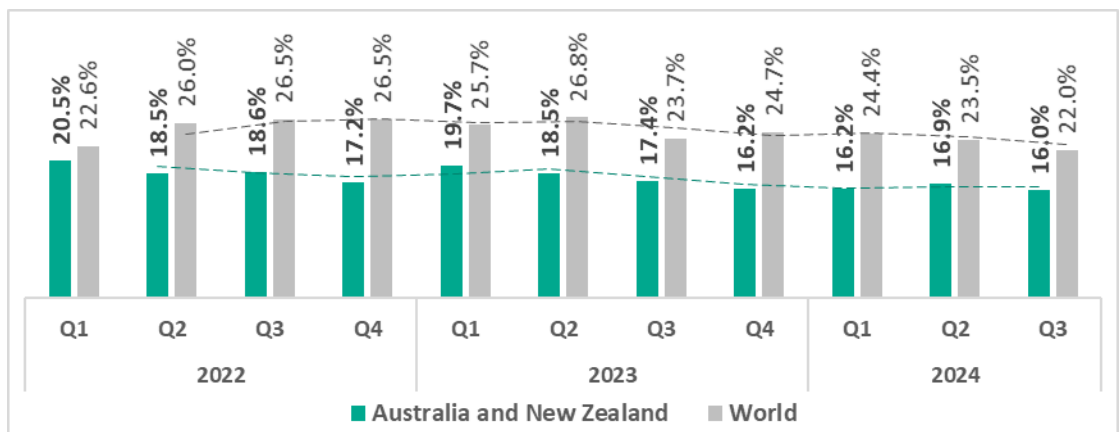
Australia and New Zealand

Current threats

<p>N.1 IN THE REGION</p> <p>MALICIOUS SCRIPTS & PHISHING PAGES</p> <p>7.41%</p> <p> 1.1x increase in Q3</p> <p> 1.2x above global average</p>	<p>N.2 IN THE REGION</p> <p>DENYLISTED INTERNET RESOURCES</p> <p>4.16%</p> <p> decrease in Q3</p>	<p>N.3 IN THE REGION</p> <p>MALICIOUS DOCUMENTS</p> <p>2.17%</p> <p> 1.4x increase in Q3</p> <p>2nd globally in growth</p> <p> 1.1x above global average</p>
<p>SPYWARE</p> <p>1.86%</p> <p> decrease in Q3</p>	<p>THREATS FROM INTERNET</p> <p>9.73%</p> <p> decrease in Q3</p>	<p>THREATS FROM EMAIL CLIENTS</p> <p>3.21%</p> <p> decrease in Q3</p> <p> 1.1x above global average</p>

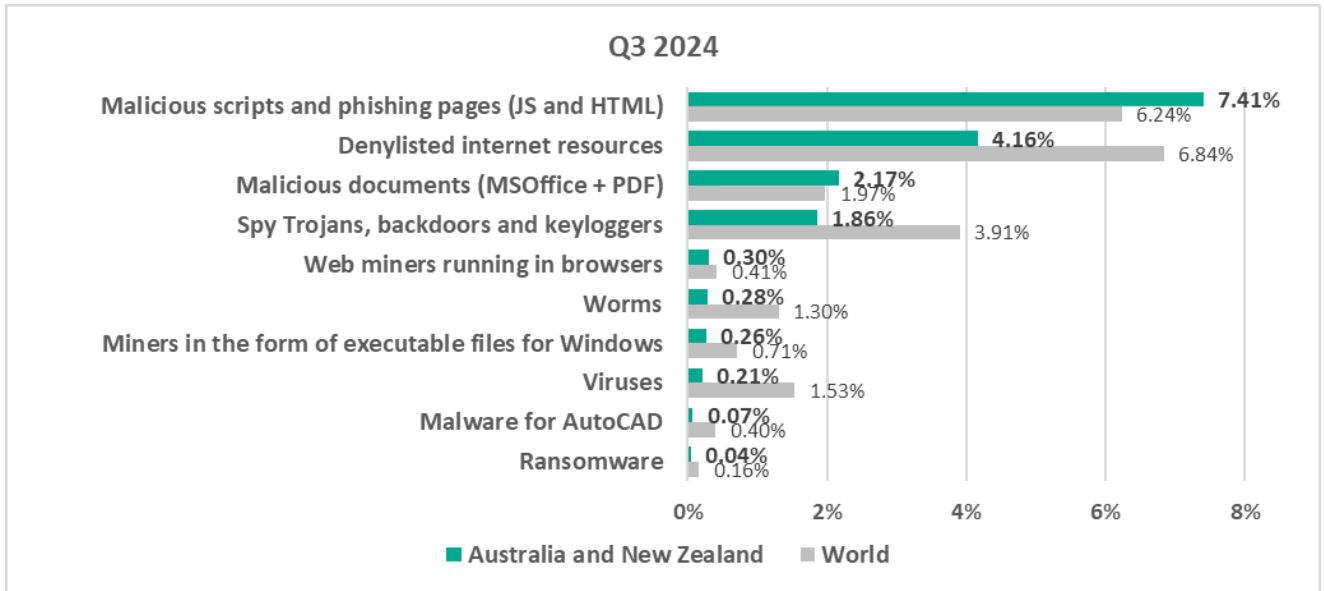
Overall

- **Eleventh** place in the global ranking.
- In **Q3 2024**, the region saw a **decrease** in threats that were blocked on ICS computers.
- The percentage of ICS computers on which malicious objects were blocked in the region is noticeably **less than the global figure**.



Comparative analysis

Threat categories

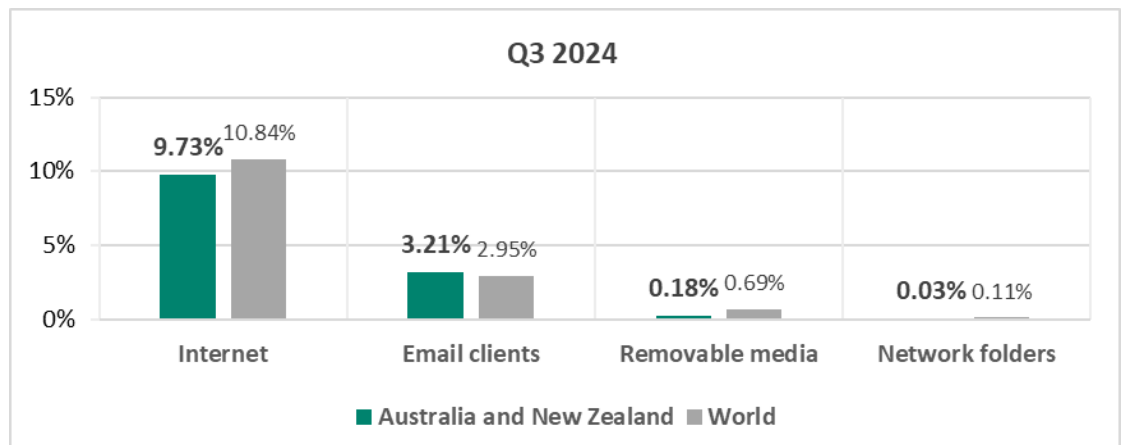


- **Compared to the global average**, the region has a noticeably **higher percentage** of ICS computers on which the following were blocked:
 - Malicious scripts and phishing pages – 1.2 times higher
 - Malicious documents – 1.1 times higher

Threat sources

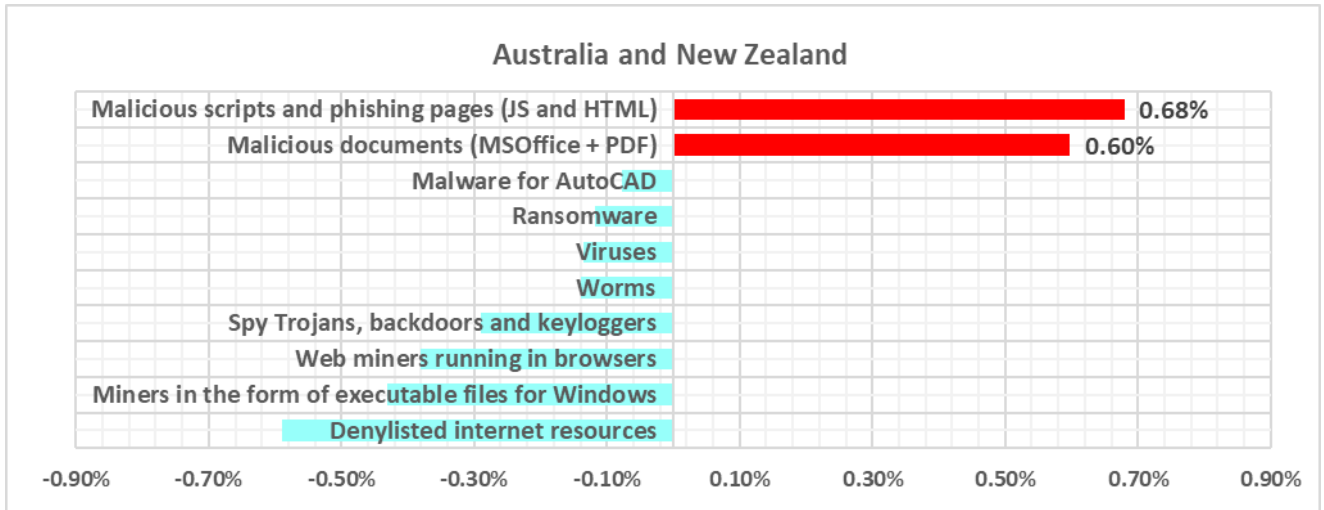
The percentage of ICS computers on which threats from **email clients** were blocked **surpassed the global average** by a factor of 1.1.

Other threat sources remained below their respective global averages.

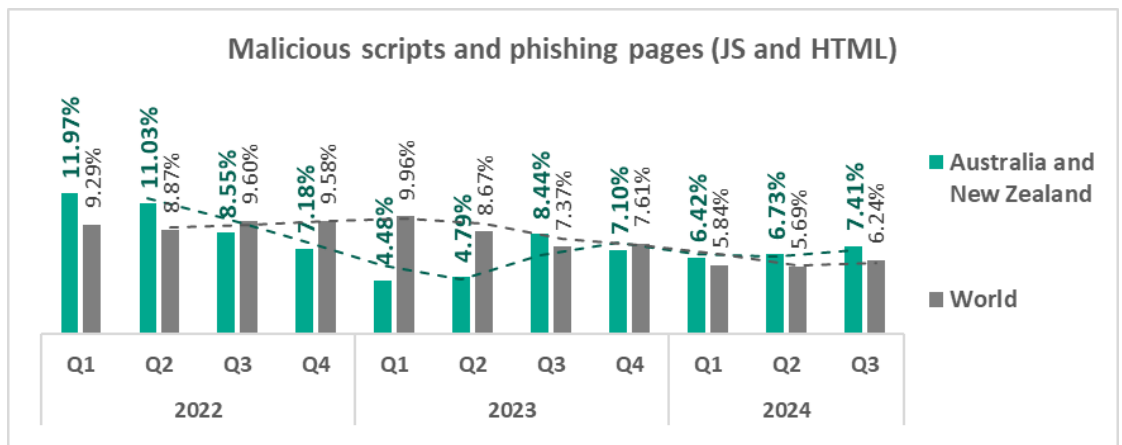


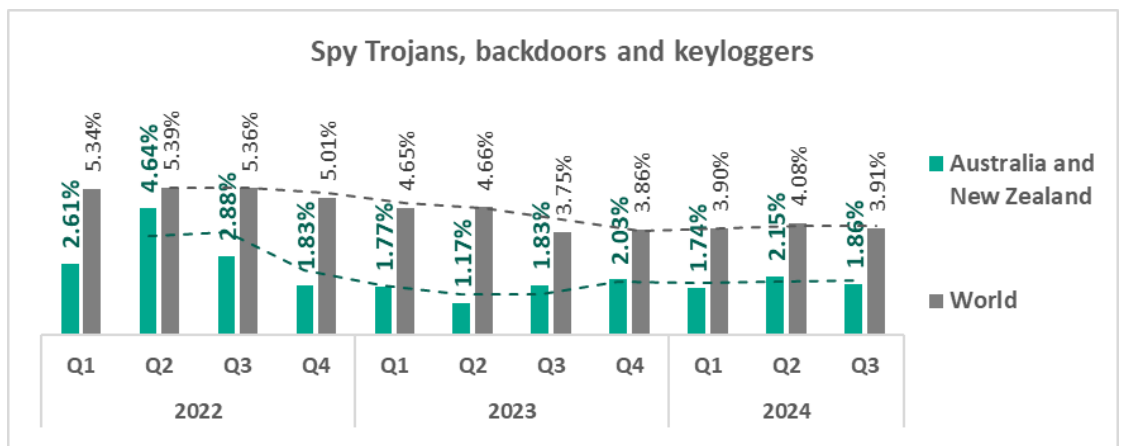
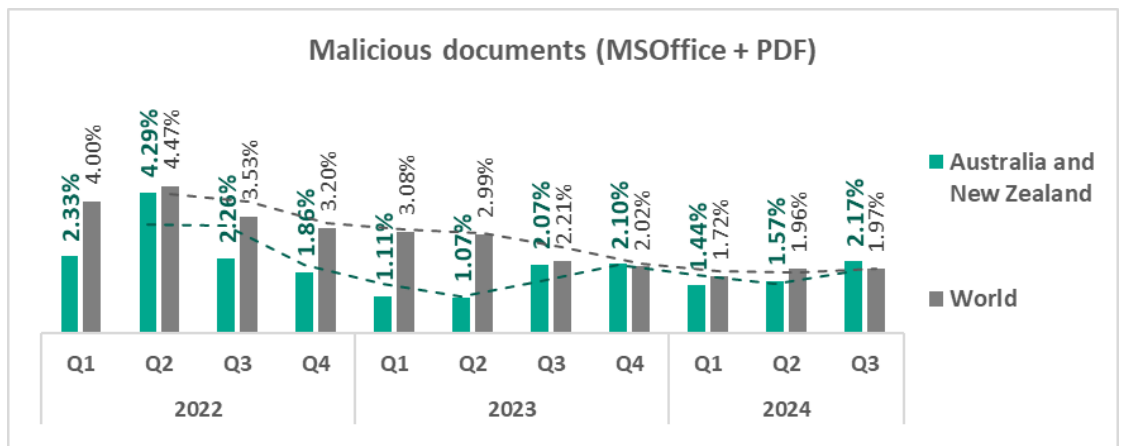
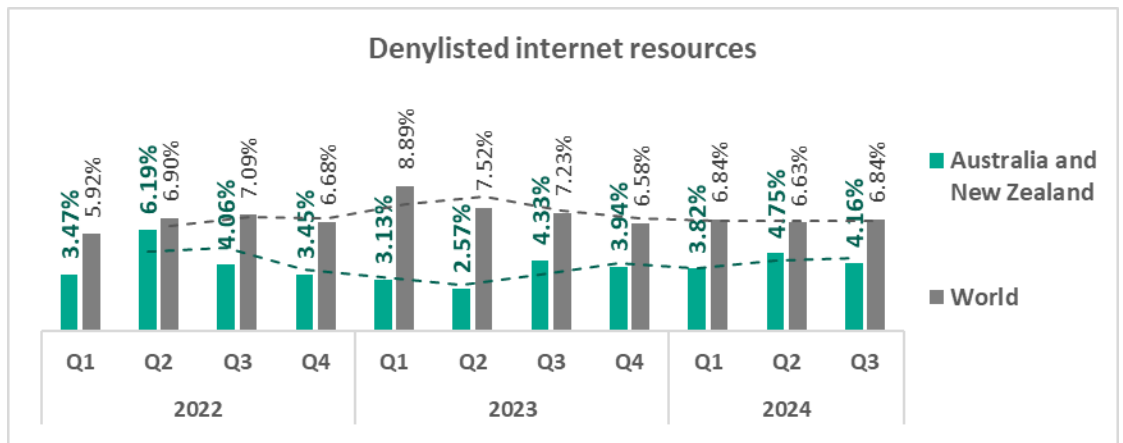
Quarterly changes and trends

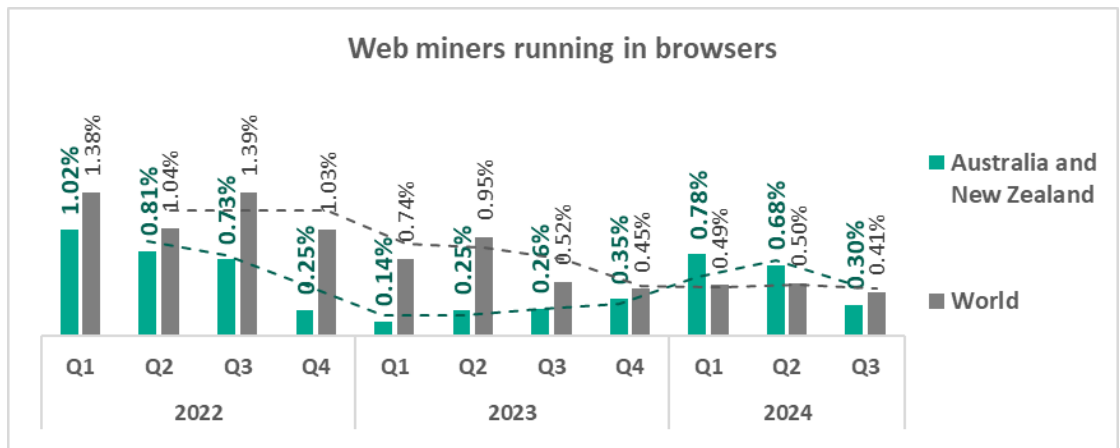
Threat categories



- Compared to the previous quarter, the **largest proportional increase** was in the percentage of ICS computers on which the following were blocked:
 - Malicious documents – 1.4 times higher
 - Malicious scripts and phishing pages – 1.1 times higher
- The **top threat** categories exhibit various quarterly dynamics:





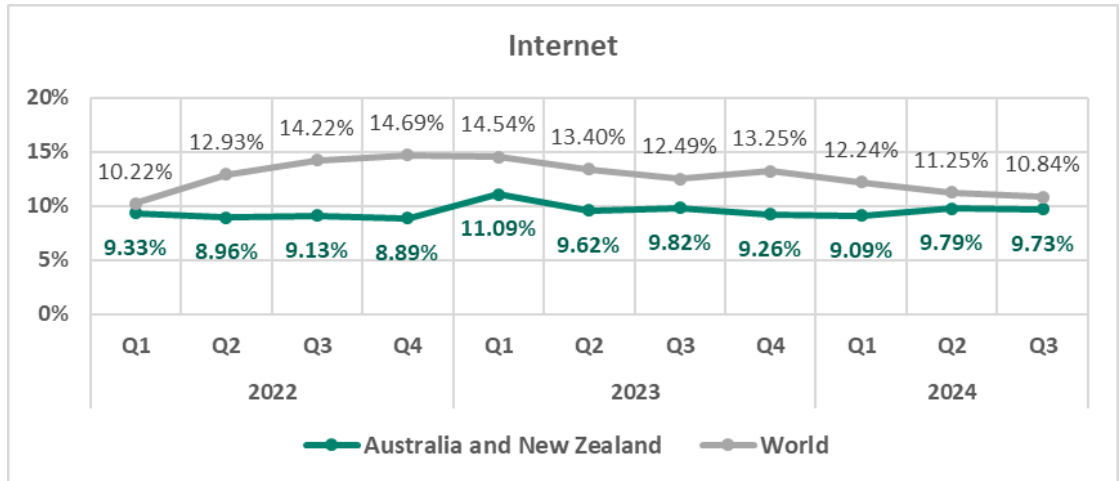


- The heatmap below illustrates changes in the rankings of threat categories in the region since the beginning of 2022. **Malicious scripts and phishing pages** have been the leading threat category in the region throughout the observed period, while **denylisted internet resources** have consistently ranked second. In Q3 2024, **malicious documents** moved to third place, surpassing spyware. **Executable miners** dropped from fifth to seventh place in the regional rating.

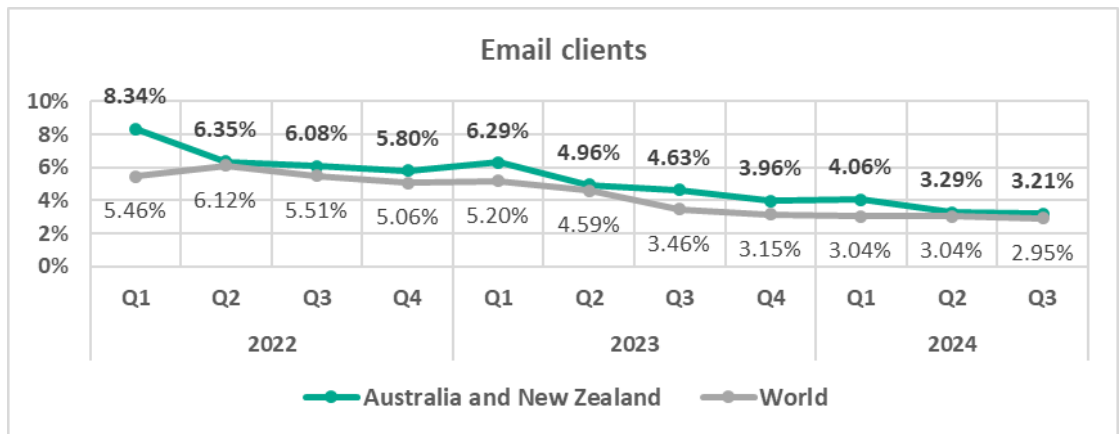
Australia and New Zealand	2022				2023				2024		
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3
Malicious scripts and phishing pages (JS and HTML)	1	1	1	1	1	1	1	1	1	1	1
Denylisted internet resources	2	2	2	2	2	2	2	2	2	2	2
Malicious documents (MSOffice + PDF)	4	4	4	3	5	4	3	3	4	4	3
Spy Trojans, backdoors and keyloggers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

Threat sources

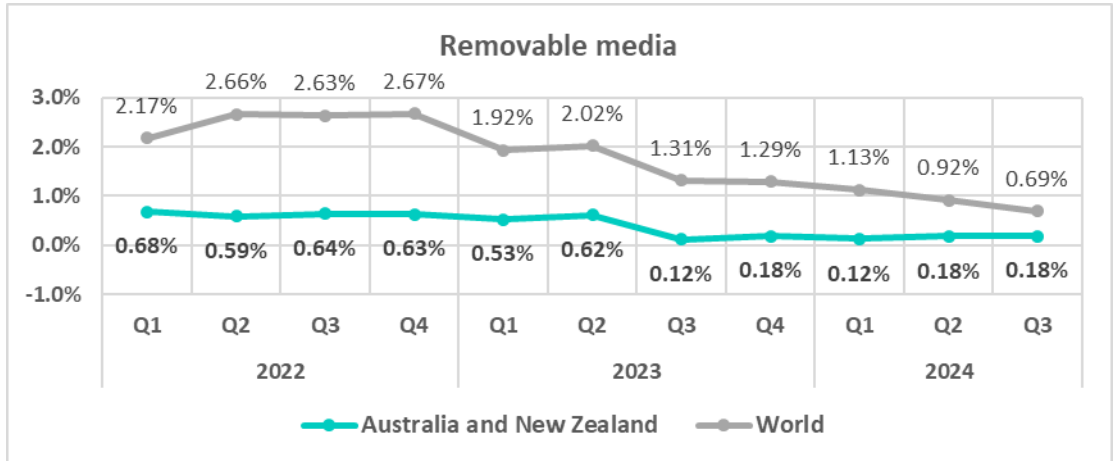
- Threats from the **internet** (measured by percentage of ICS computers where they were blocked) have shown a mostly flat trend **nearing the global average in Q3 2024**.



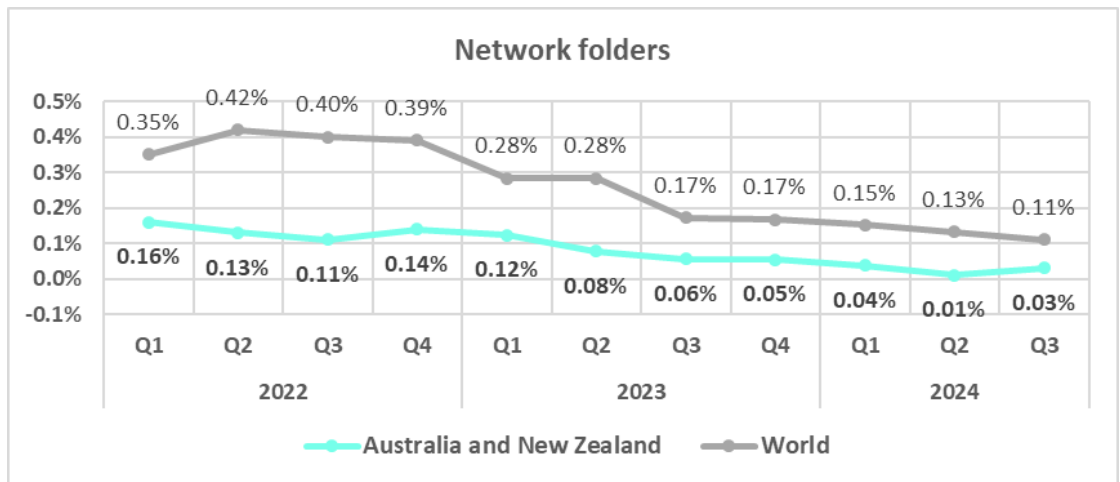
- The trend for **email client** threats continues to show **mostly downward** movement, while remaining **above the global average** throughout the observed period.



- The **long-term trend** for threats from **removable devices** has been significantly **below the global average** throughout the observed period. In Q3 2024, the rate remains low.



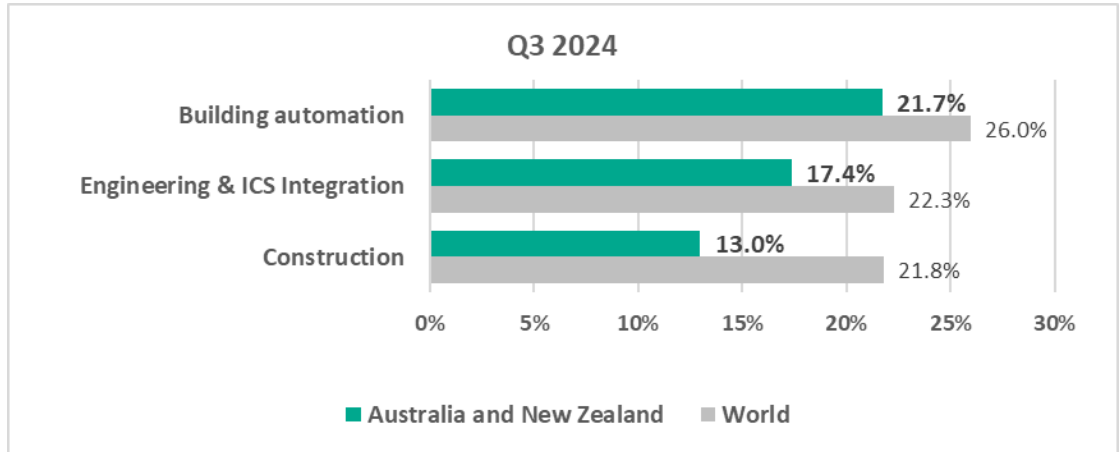
- The **long-term trend** for threats from **network folders** has been also significantly **below the global average** throughout the observed period. After a drop in Q2 2024, the rate **went up in Q3 2024**.



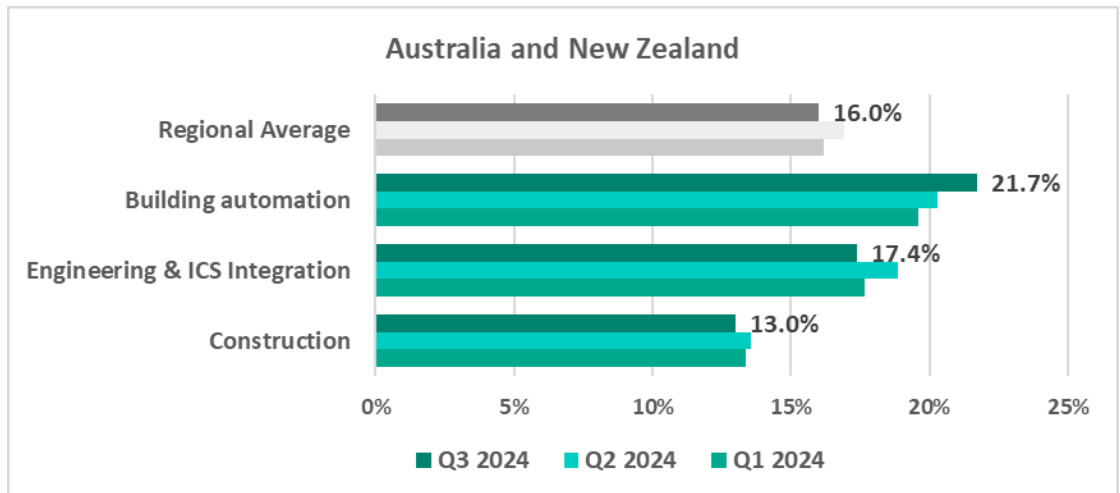
Industries

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

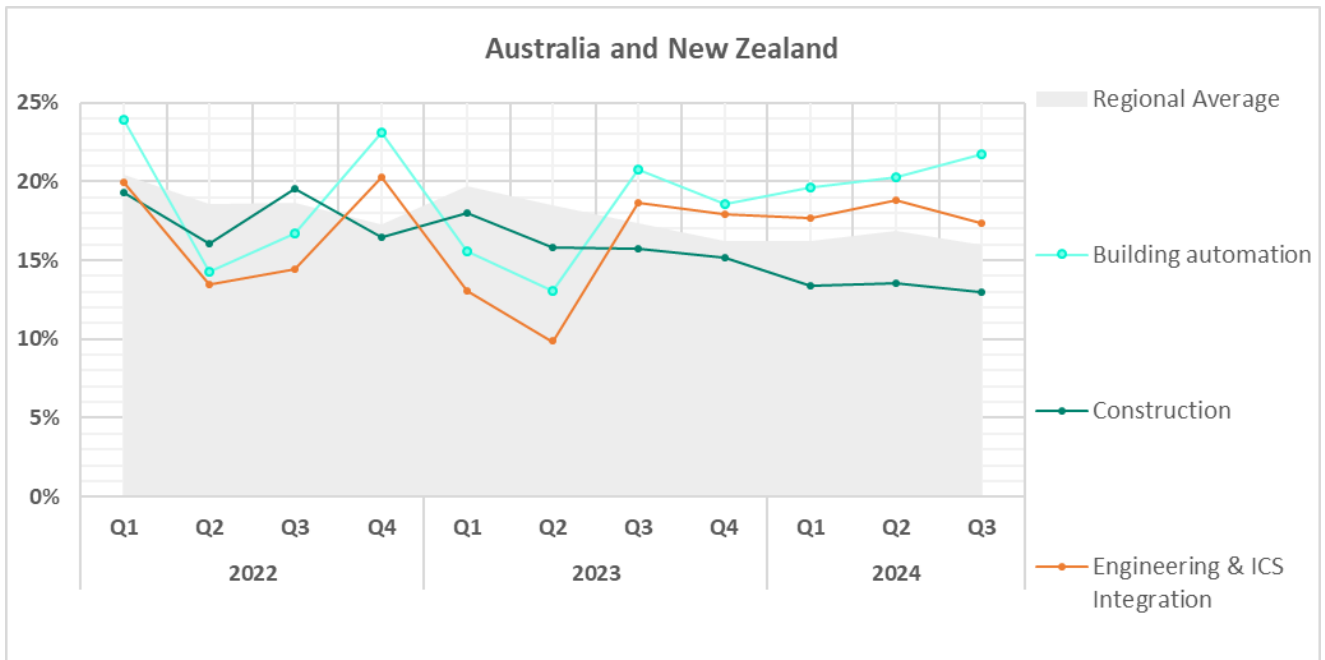
- Compared to the respective **global averages**, all sectors under study saw a **lower percentage** of ICS computers on which malicious objects were blocked.



- In **Q3 2024**, the **building automation** sector exhibited an **increase** in the percentage of ICS computers on which malicious objects were blocked compared to the previous quarter – by 1.1 times.



- 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 keeps showing a **mostly downward trend**, remaining below the regional average since Q4 2022.



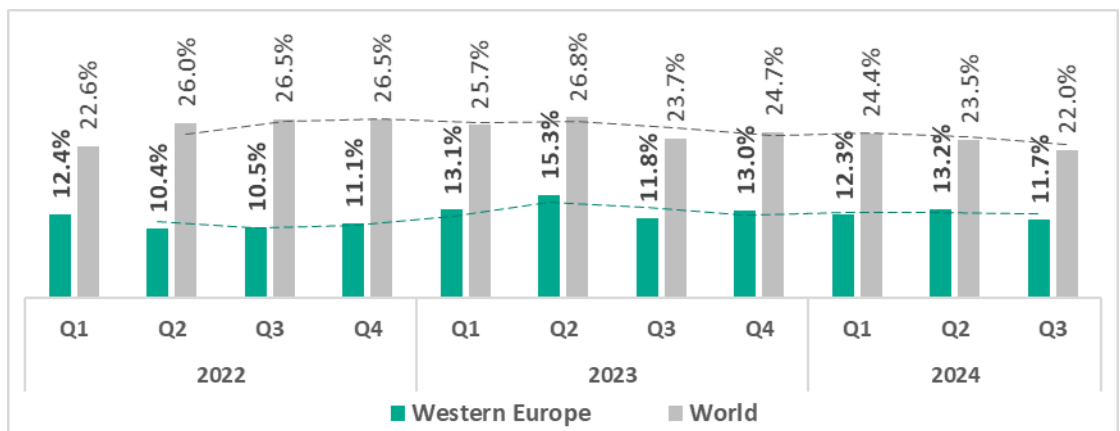
Western Europe

Current threats

<p>N.1 IN THE REGION</p> <p>DENYLISTED INTERNET RESOURCES</p> <p>4.48%</p> <p>decrease in Q3</p>	<p>N.2 IN THE REGION</p> <p>MALICIOUS SCRIPTS & PHISHING PAGES</p> <p>3.97%</p> <p>1.1x increase in Q3</p>	<p>N.3 IN THE REGION</p> <p>SPYWARE</p> <p>1.62%</p> <p>decrease in Q3</p>
<p>VIRUSES</p> <p>0.21%</p> <p>1.1x increase in Q3</p>	<p>THREATS FROM INTERNET</p> <p>6.78%</p> <p>decrease in Q3</p>	

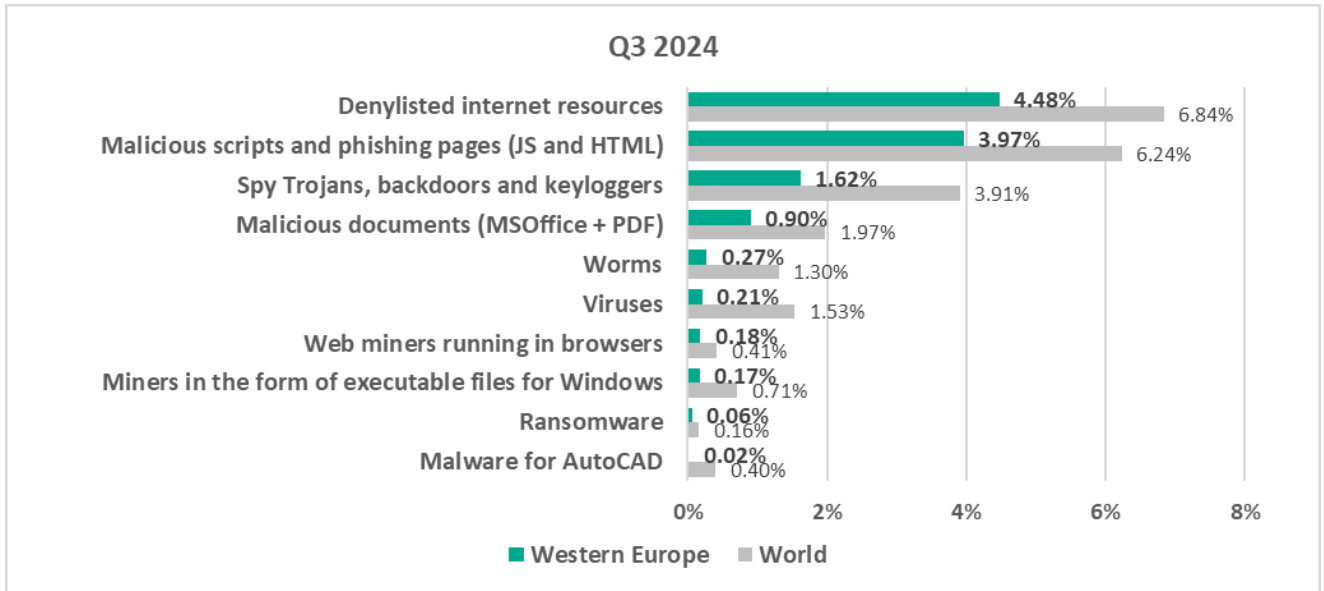
Overall

- **Twelfth** place in the global ranking.
- In general, this region has **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**.
- In **Q3 2024**, the region showed a **decrease** in threats that were blocked on ICS computers.



Comparative analysis

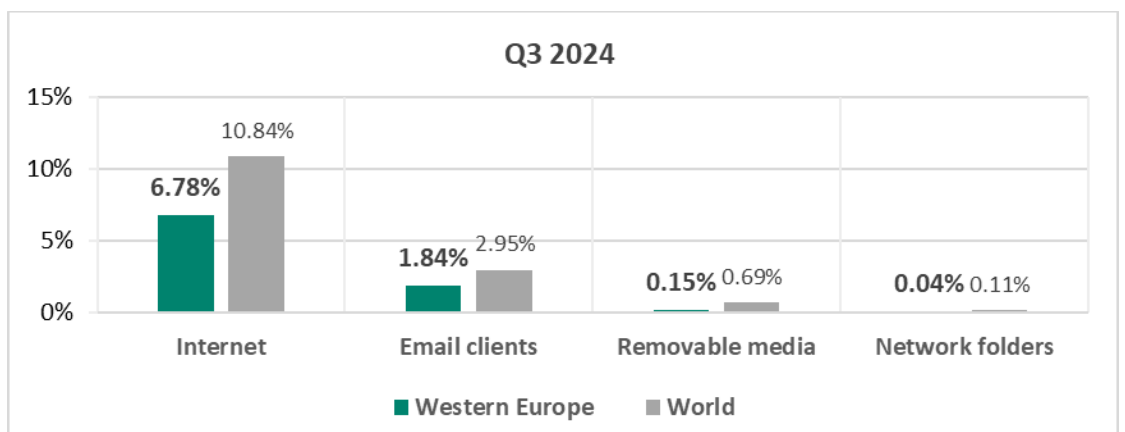
Threat categories



- **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.

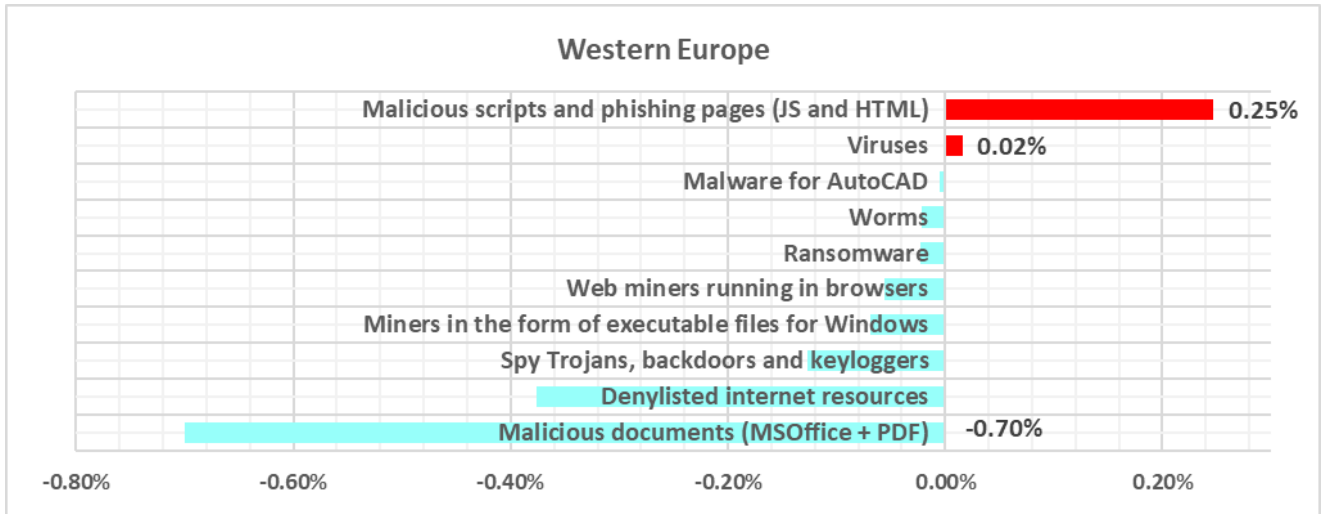
Threat sources

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

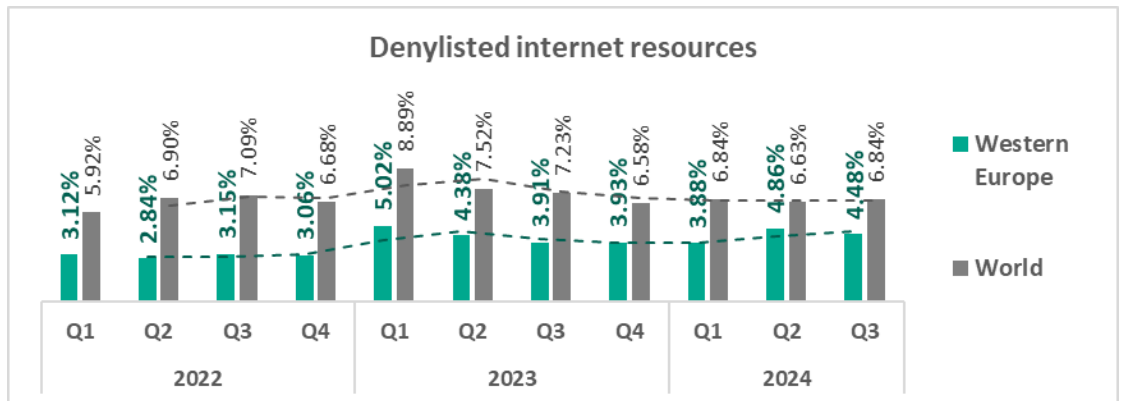


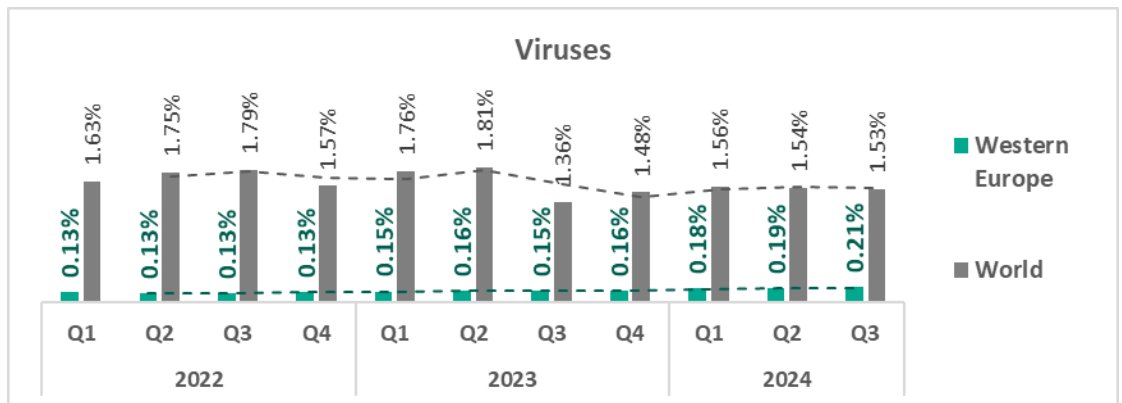
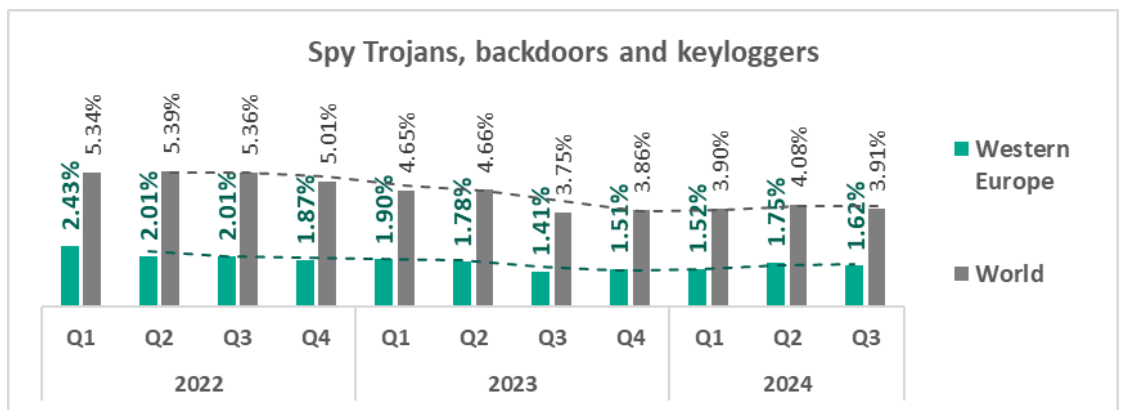
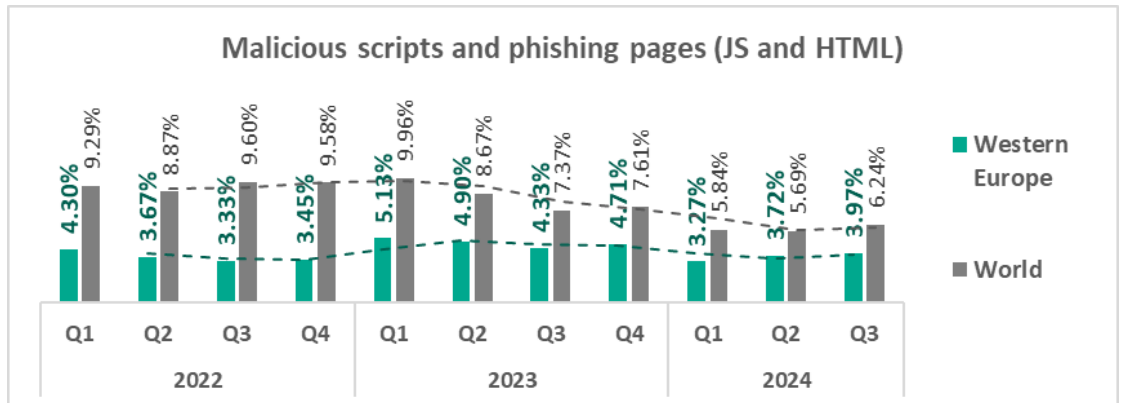
Quarterly changes and trends

Threat categories



- The **largest proportional increase** in **Q3 2024** was in the percentage of ICS computers on which the following were blocked:
 - Malicious scripts and phishing pages – 1.1 times higher
 - Viruses – 1.1 times higher
- The **top threat** categories exhibit various quarterly dynamics:



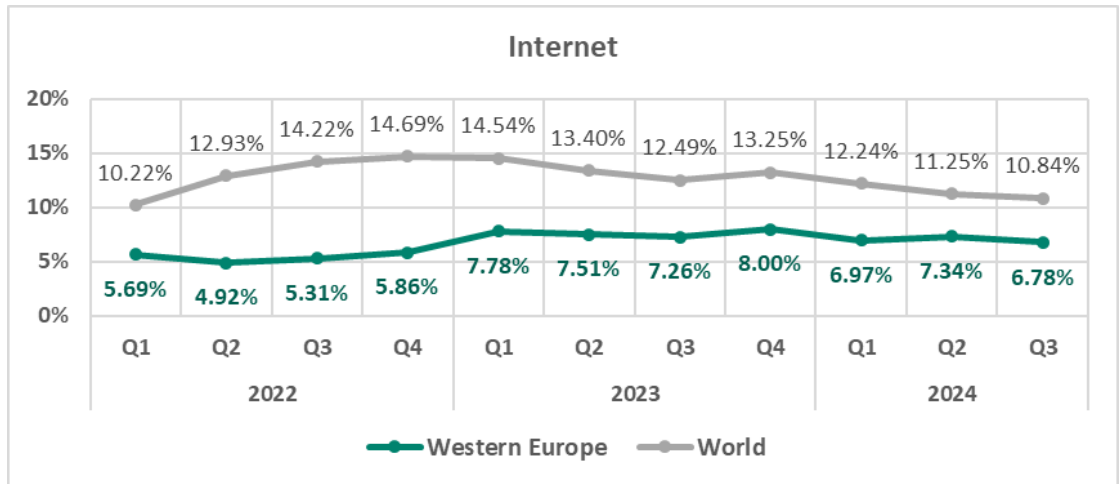


- The heatmap below illustrates changes in the rankings of threat categories in the region since the beginning of 2022. **Denylisted internet resources** have been the leading threat category in the region since Q1 2024. In Q3 2024, **viruses** moved up to sixth place from eighth in the regional threat category ranking, while **executable miners** dropped from sixth to eighth place.

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

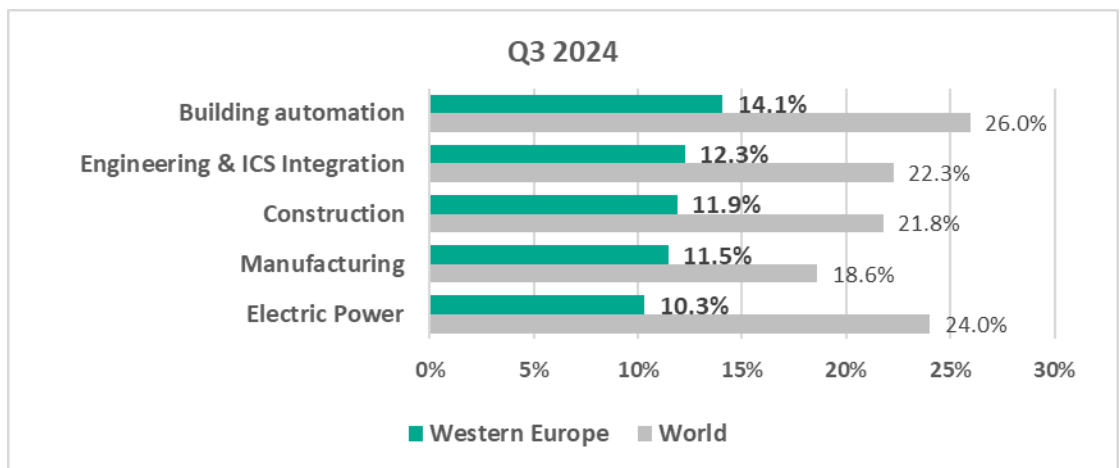
Threat sources

- Threats from the **internet** have shown a mostly **flat trend with minor fluctuations** since Q2 2023.

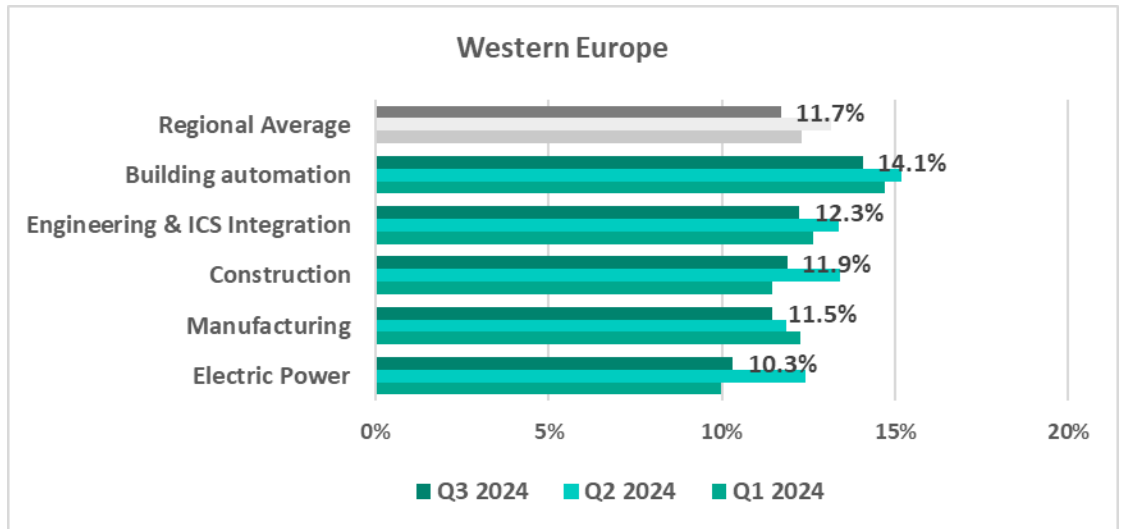


Industries

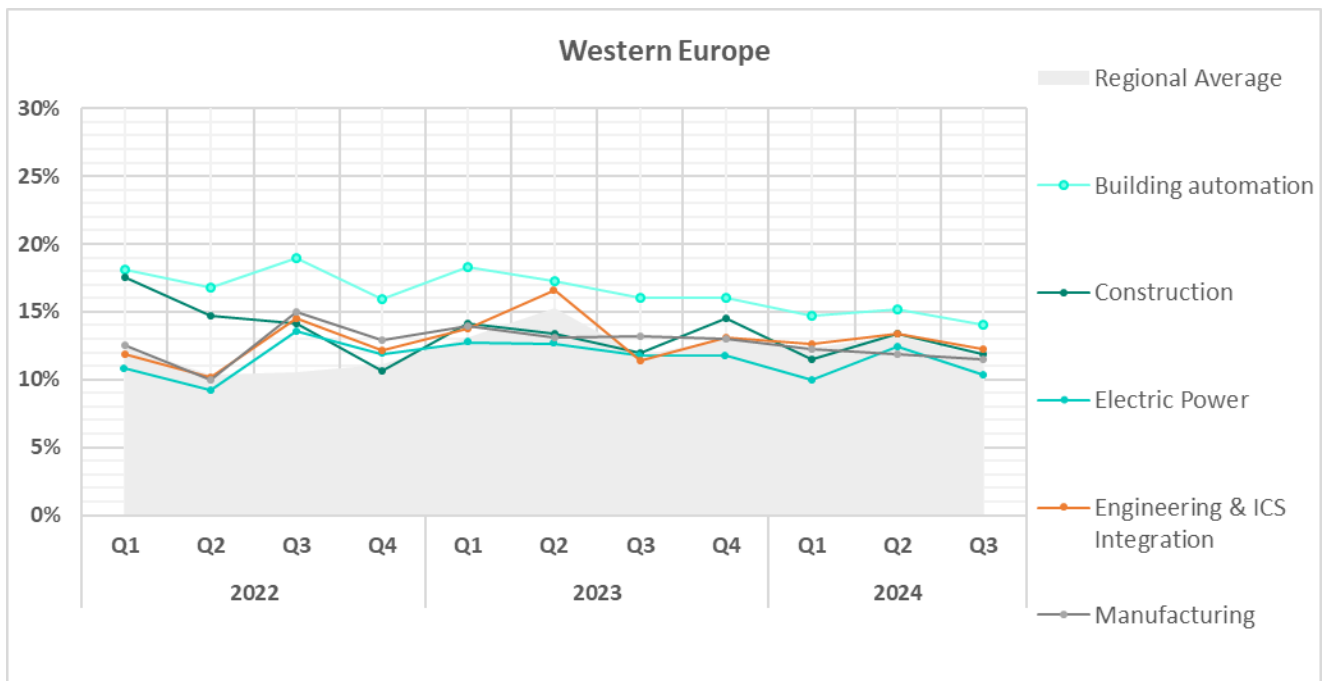
- The most **affected** industry in the region, as featured in this report, was **building automation**
- From a **global perspective**, all sectors in the region remained **significantly below** the respective global averages.



- In **Q3 2024**, all sectors exhibited a **decrease** in the percentage of ICS computers on which malicious objects were blocked.







- The **long-term trend** in the **building automation** sector remains significantly **above the regional average**.



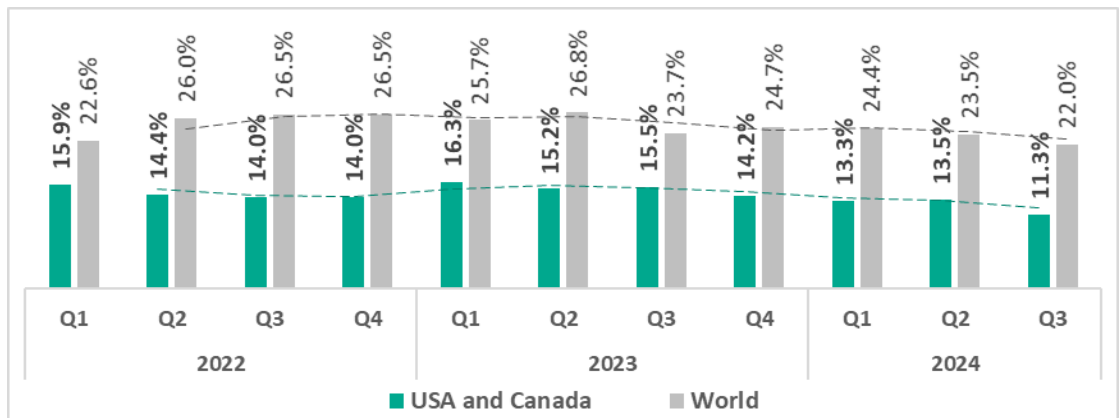
USA and Canada

Current threats

<p>N.1 IN THE REGION</p> <p>MALICIOUS SCRIPTS & PHISHING PAGES</p> <p>4.23%</p> <p> decrease in Q3</p>	<p>N.2 IN THE REGION</p> <p>DENYLISTED INTERNET RESOURCES</p> <p>3.61%</p> <p> decrease in Q3</p>	<p>N.3 IN THE REGION</p> <p>SPYWARE</p> <p>1.39%</p> <p> decrease in Q3</p>
<p>THREATS FROM INTERNET</p> <p>6.61%</p> <p> decrease in Q3</p>		

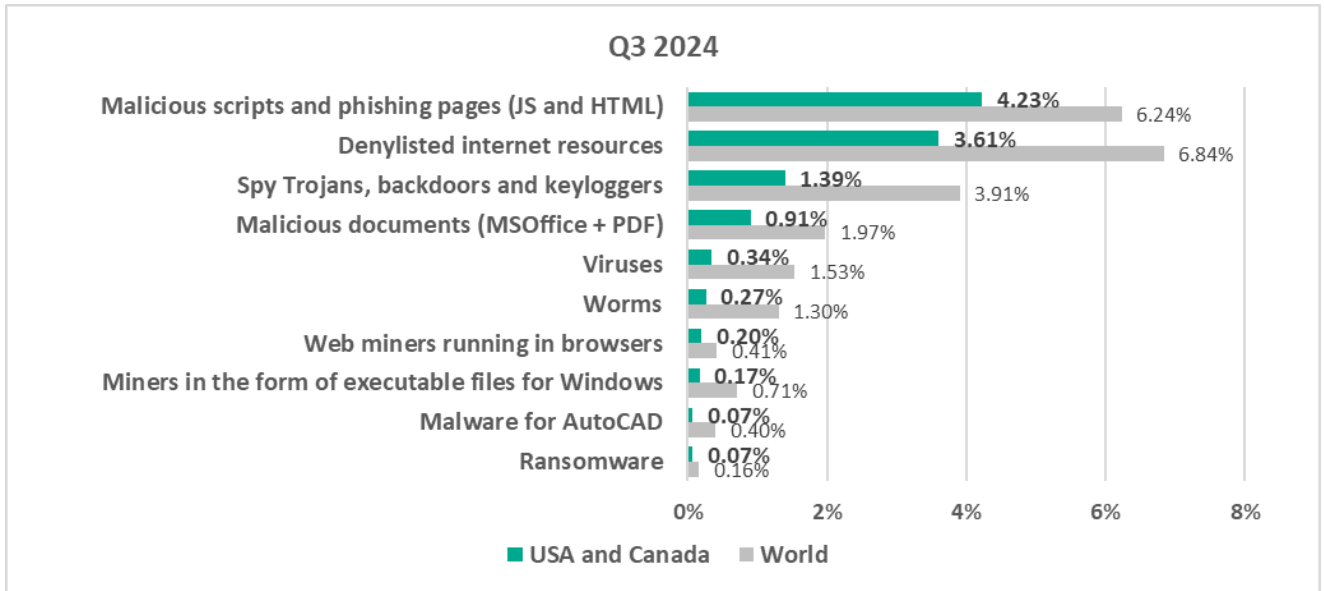
Overall

- **Thirteenth** place in the regional ranking.
- In general, this region has **one of the lowest percentages** of ICS computers on which malicious objects were blocked.
- In **Q3 2024**, the region showed a **decrease** by a factor of 1.2 in threats that were blocked on ICS computers.



Comparative analysis

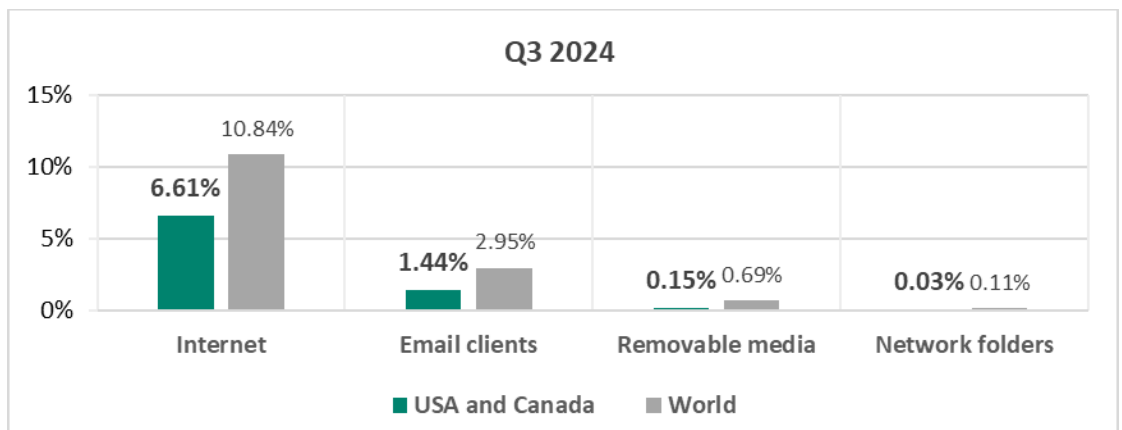
Threat categories



- **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**.

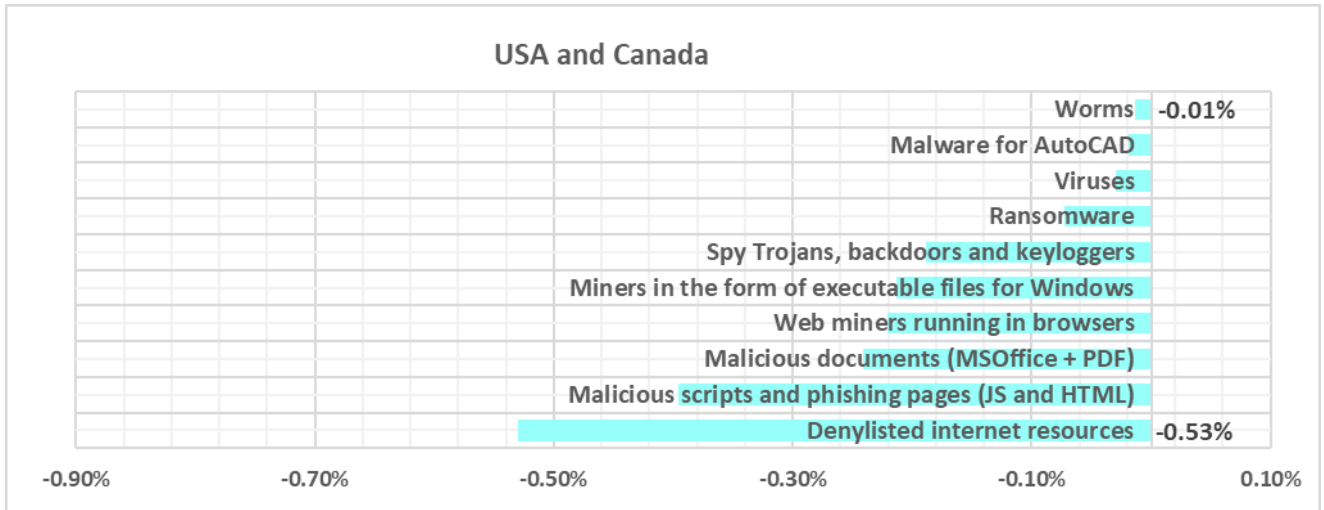
Threat sources

- All threat sources keep showing values **noticeably below** their respective **global averages**.

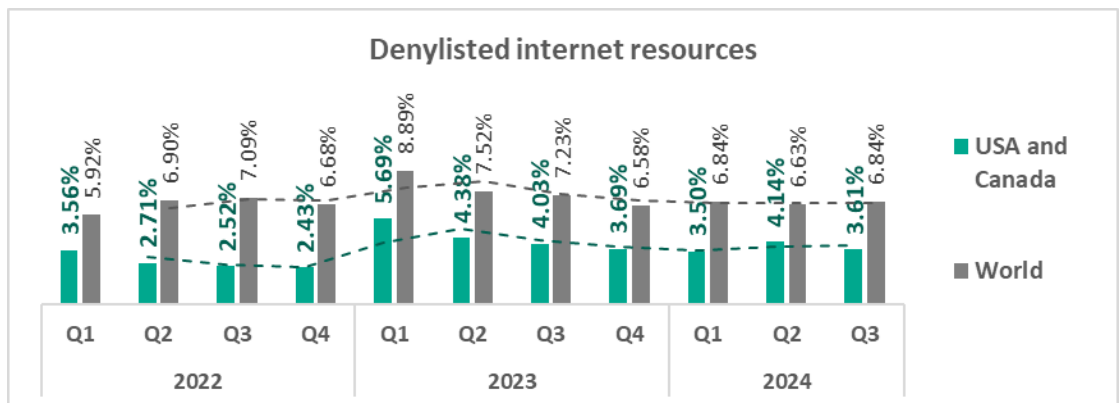
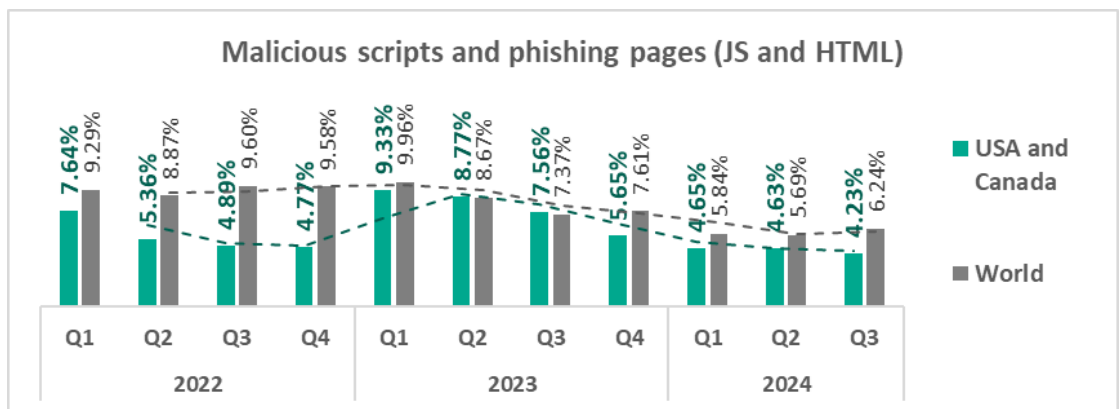


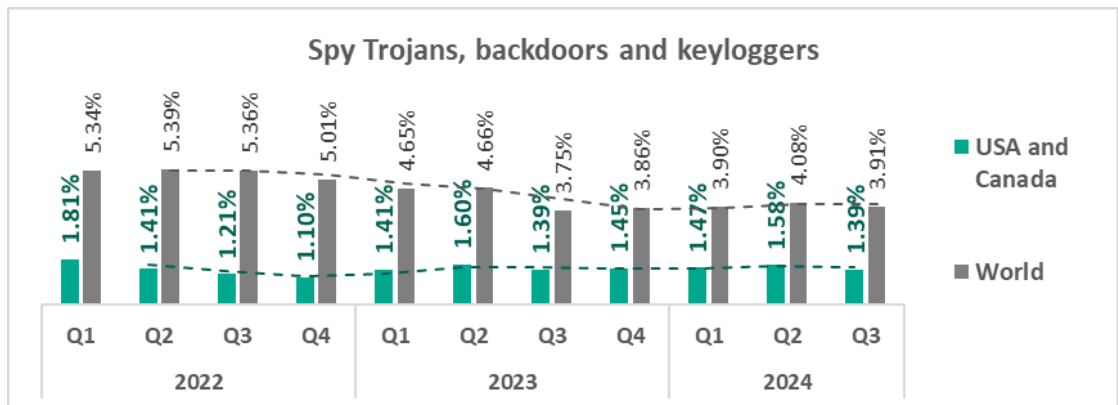
Quarterly changes and trends

Threat categories



- In **Q3 2024**, all threat categories exhibited a **decrease** in values.
- The **top threat** categories exhibit various quarterly dynamics:



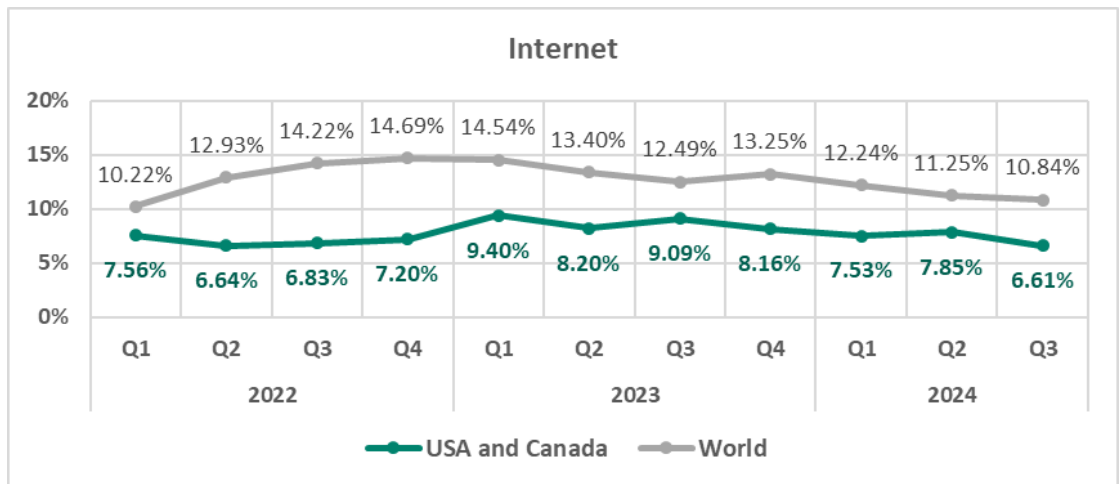


- The heatmap below illustrates changes in the rankings of threat categories in the region since the beginning of 2022. **Malicious scripts and phishing pages** have been the leading threat category in the region throughout the observed period, while **denylisted internet resources** have consistently ranked second. **Spyware** has ranked third for three quarters in a row. **Web miners** dropped from fifth to seventh place in Q3 2024. **Ransomware** and **malware for AutoCAD** showed equally small values and ranked last in the regional rating.

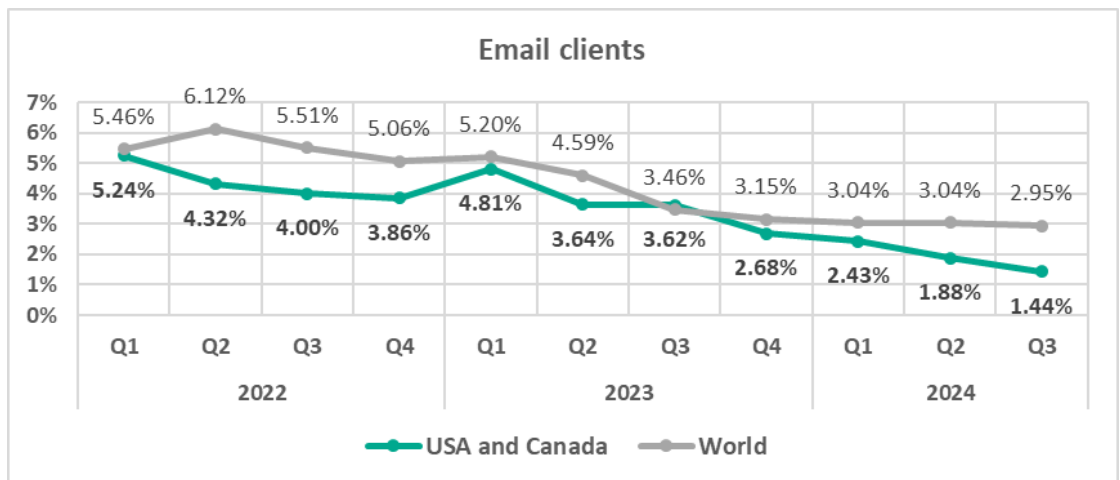
USA and Canada	2022				2023				2024		
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3
Malicious scripts and phishing pages (JS and HTML)	1	1	1	1	1	1	1	1	1	1	1
Denylisted internet resources	2	2	2	2	2	2	2	2	2	2	2
Spy Trojans, backdoors and keyloggers	4	4	4	4	4	4	3	4	3	3	3
Malicious documents (MSOffice + PDF)	3	3	3	3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

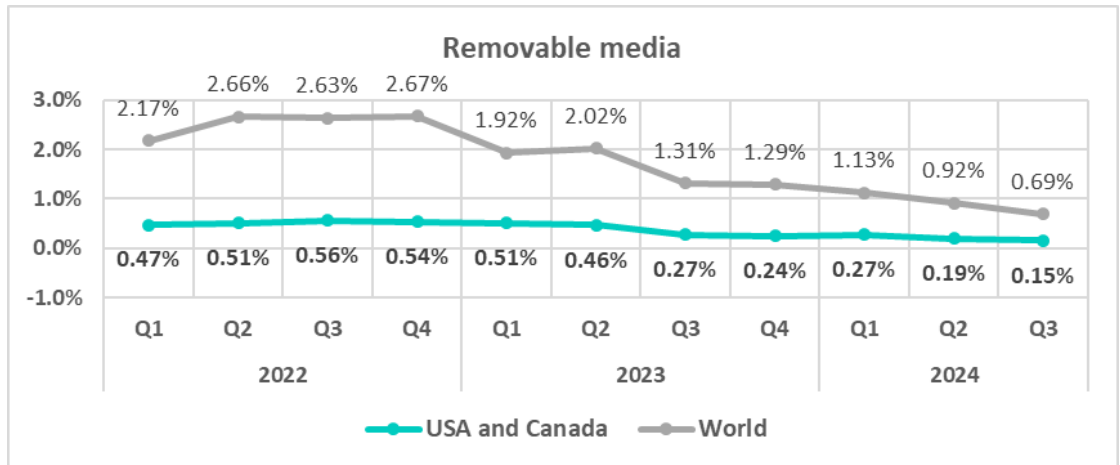
Threat sources

- In **Q3 2024**, the percentage of ICS computers on which threats from the **internet** were blocked **decreased** compared to the previous quarter, reaching its **lowest value** since the beginning of 2022.



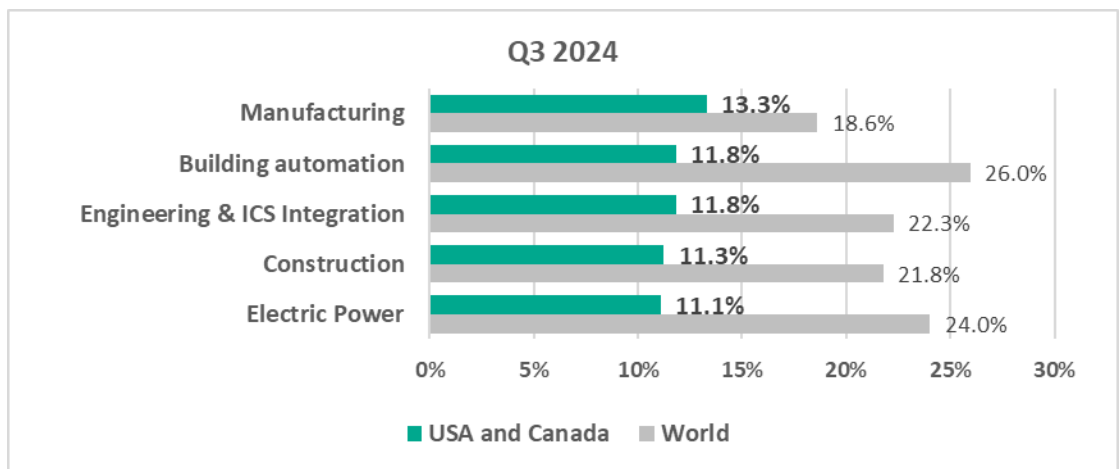
- Threats from **email clients** and **removable devices** demonstrate **downward trends**.



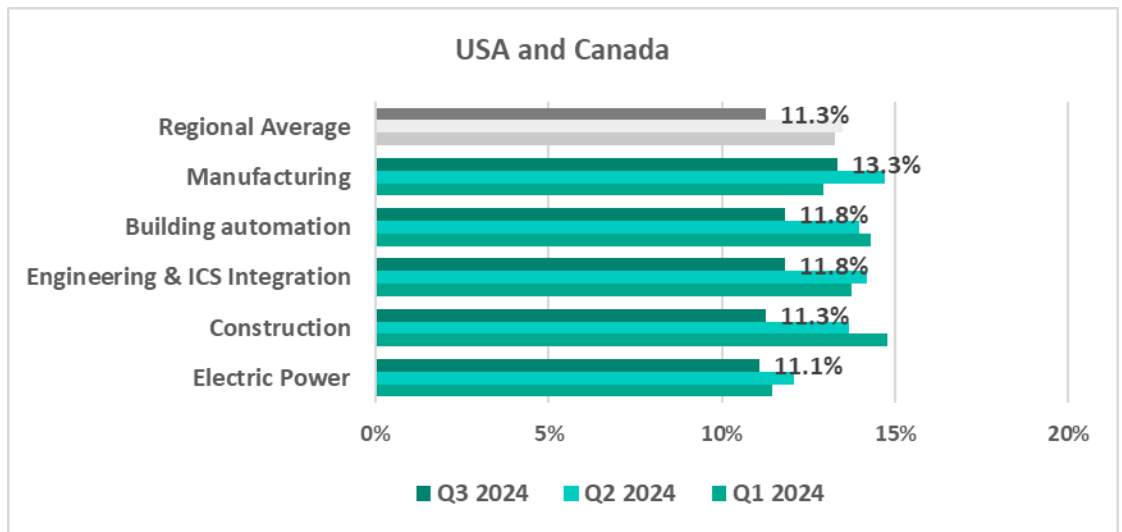


Industries

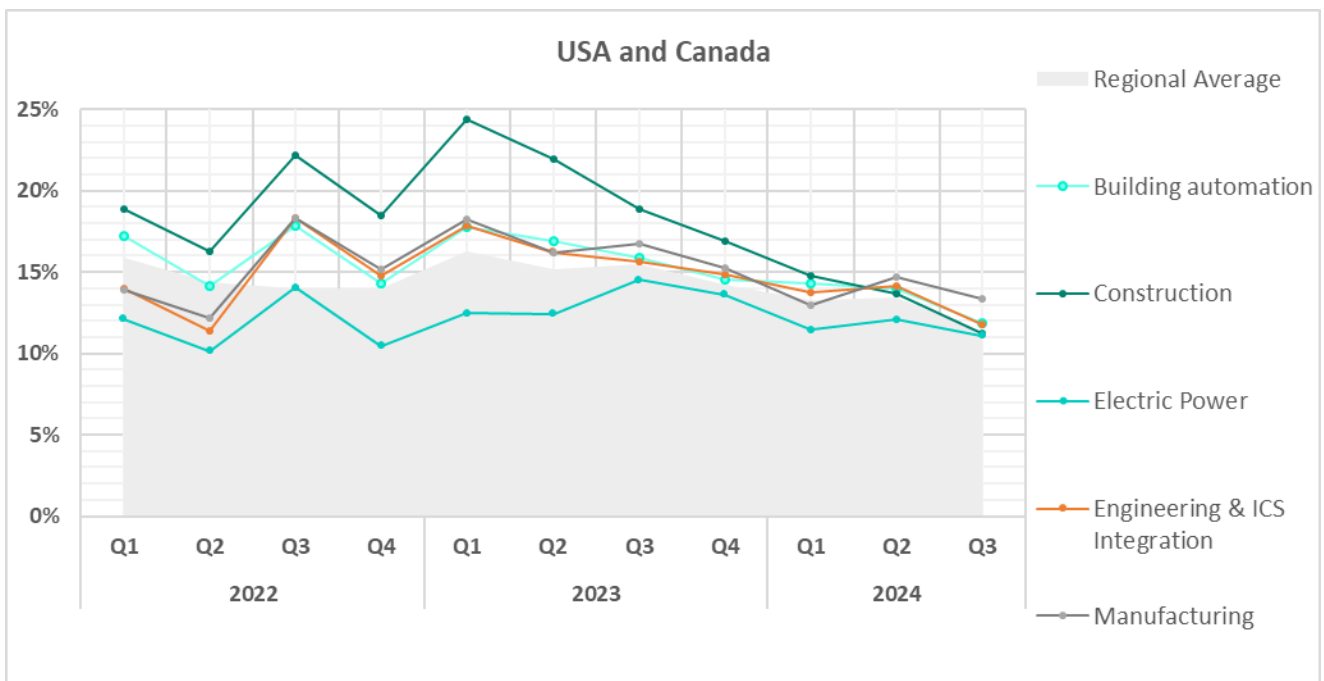
- The most **affected** industry in the region, as highlighted in this report, was **manufacturing**. It ranked fifth in the global ranking for the sector.
- From a **global perspective**, all sectors in the region remained significantly **below** the respective **global averages**.



- In **Q3 2024**, all sectors exhibited a **decrease** in the percentage of ICS computers on which malicious objects were blocked.



- Since Q3 2023, all sectors under study exhibited mostly **downward trends** in the percentage of ICS computers on which malicious objects were blocked.



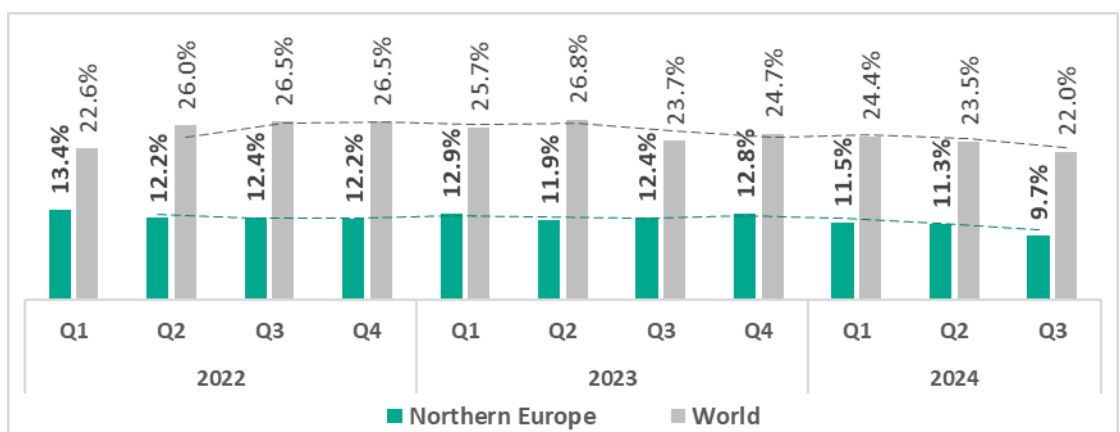
Northern Europe

Current threats

<p>N.1 IN THE REGION</p> <p>DENYLISHED INTERNET RESOURCES</p> <p>3.07%</p> <p>decrease in Q3</p>	<p>N.2 IN THE REGION</p> <p>MALICIOUS SCRIPTS & PHISHING PAGES</p> <p>2.47%</p> <p>decrease in Q3</p>	<p>N.3 IN THE REGION</p> <p>SPYWARE</p> <p>1.60%</p> <p>decrease in Q3</p>
<p>VIRUSES</p> <p>0.21%</p> <p>1.2x increase in Q3 2nd globally in growth</p>	<p>THREATS FROM INTERNET</p> <p>4.89%</p> <p>decrease in Q3</p>	

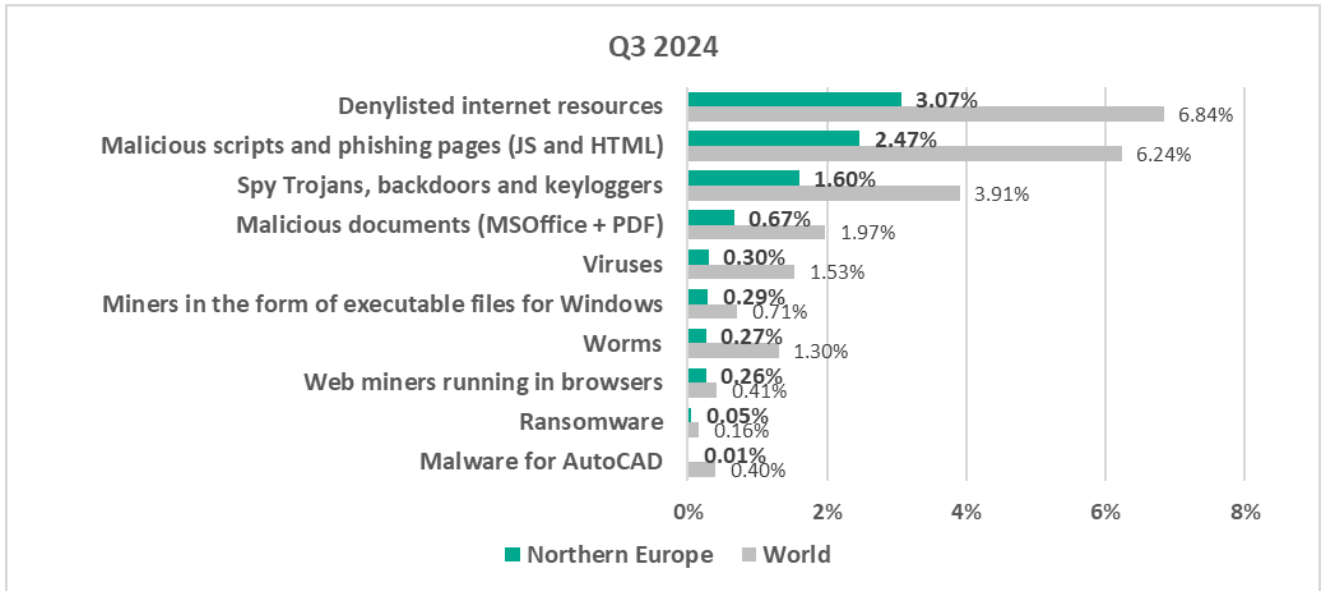
Overall

- **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 **significantly below the global average**.



Comparative analysis

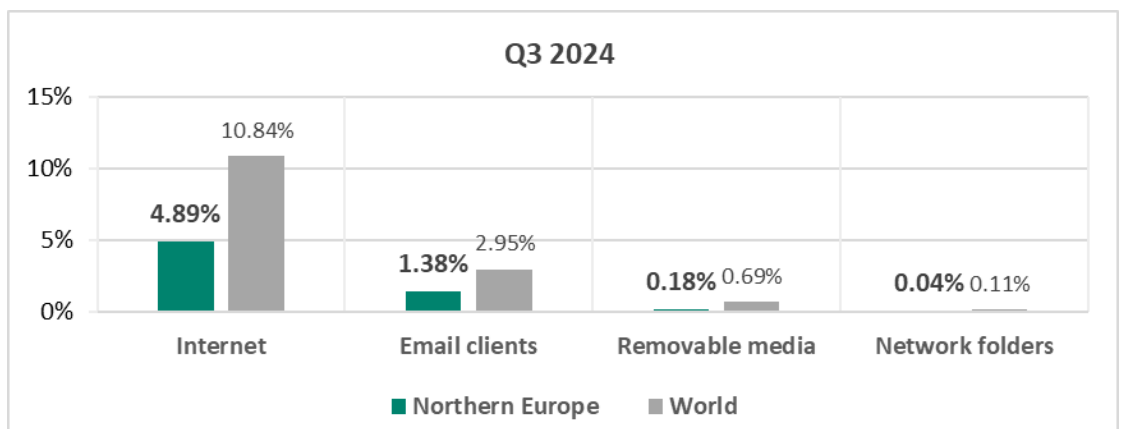
Threat categories



- 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**.

Threat sources

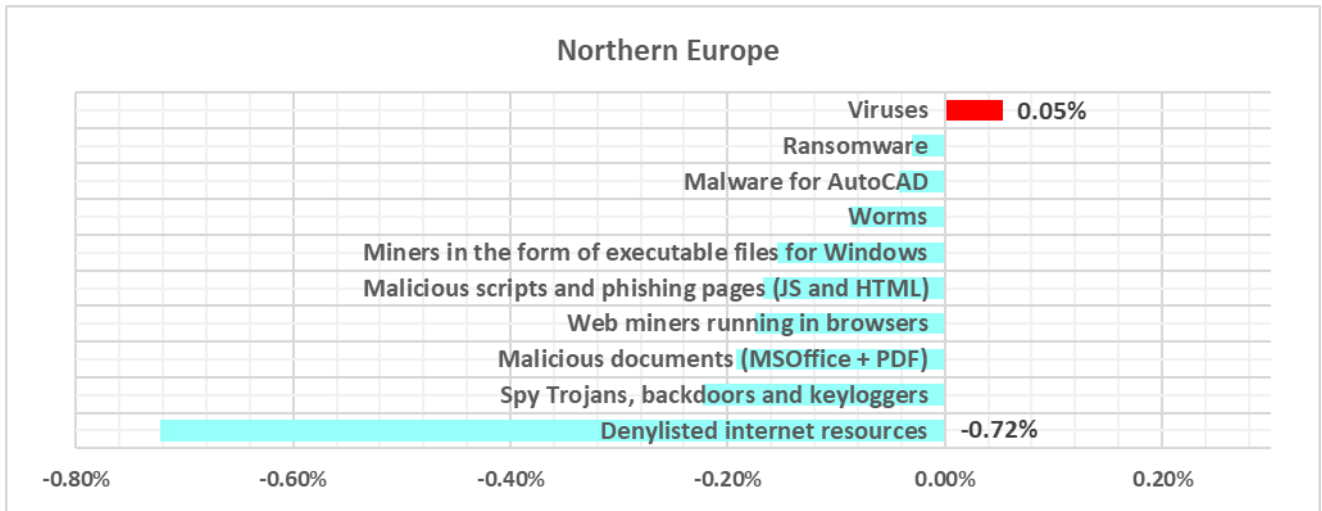
- All **threat sources** showed values noticeably **below** their respective **global averages**.



Quarterly changes and trends

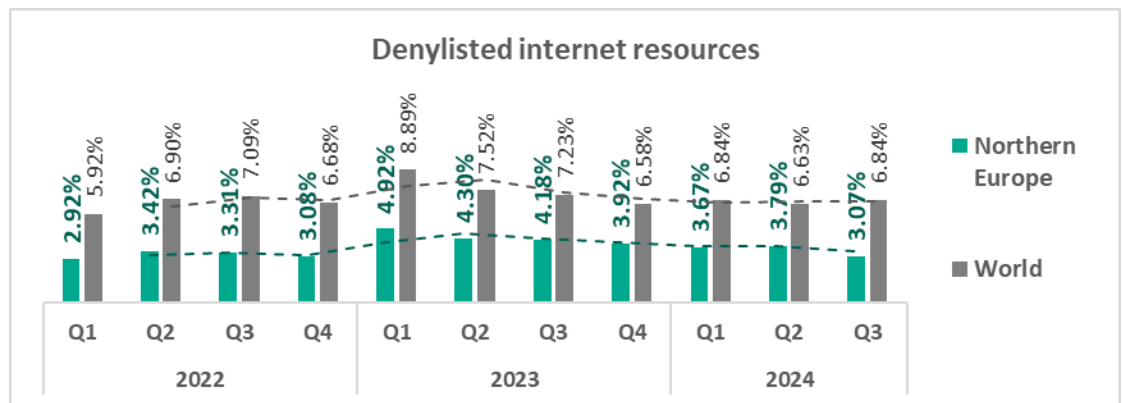
Threat categories

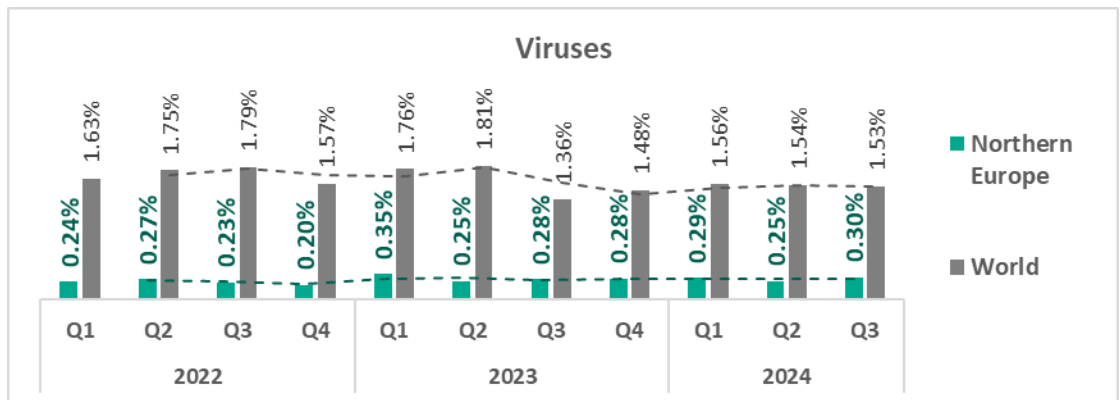
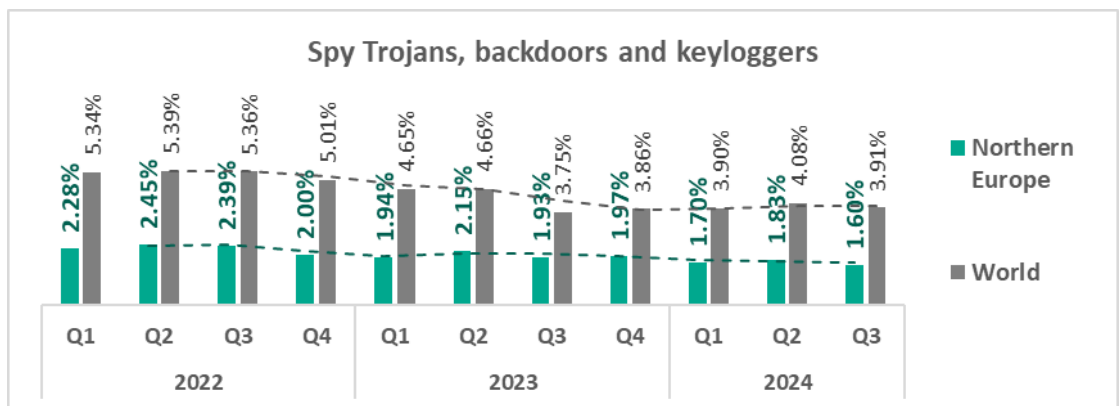
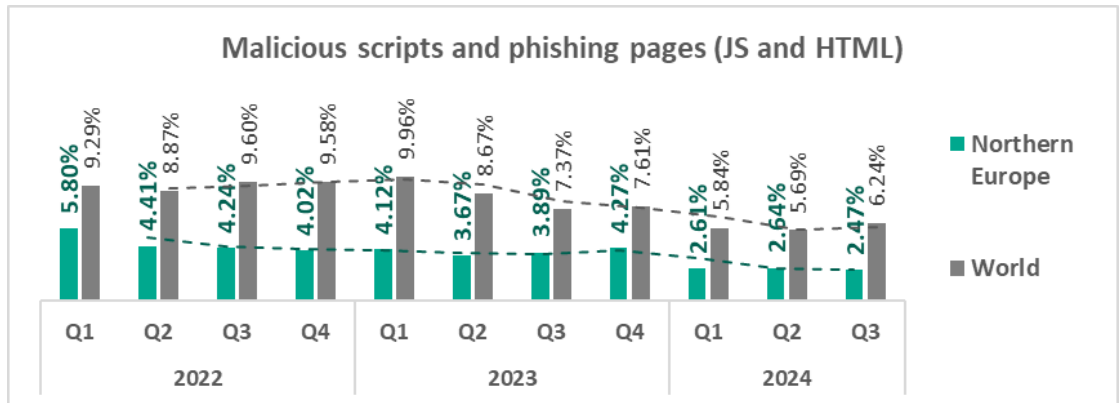
- The majority of threat categories exhibited a **decrease** in the percentage of ICS computers on which malicious objects were blocked, compared to the previous quarter.



The only **quarterly increase** was in the percentage of ICS computers on which **viruses** were blocked – **by 1.2 times**.

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



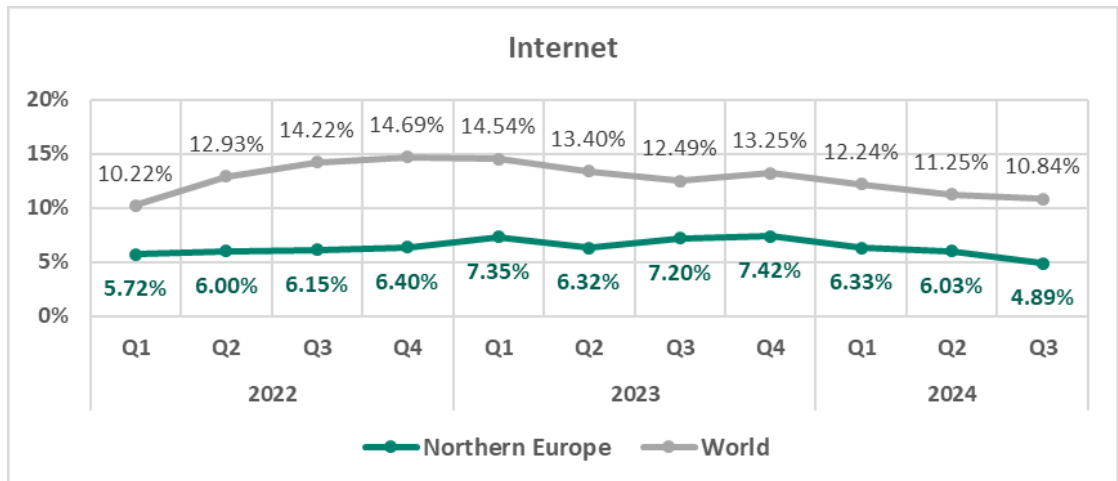


- The heatmap below illustrates changes in the rankings of threat categories in the region since the beginning of 2022. **Denylisted internet resources** have remained at the top of the ranking for three consecutive quarters. **Viruses** moved from eighth to fifth place in Q3 2024, while **web miners** dropped from sixth to eighth place.

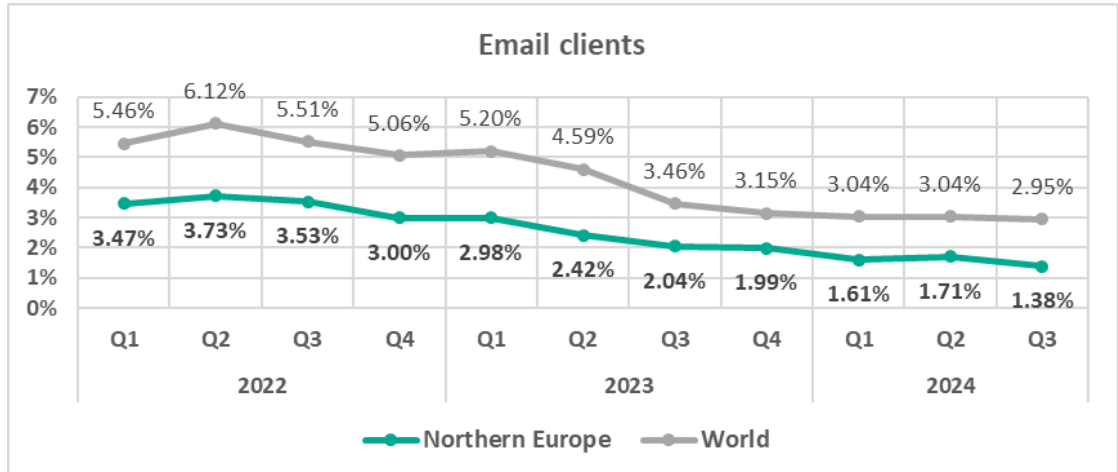
Northern Europe	2022				2023				2024		
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3
Denylisted internet resources	2	2	2	2	1	1	1	2	1	1	1
Malicious scripts and phishing pages (JS and HTML)	1	1	1	1	2	2	2	1	2	2	2
Spy Trojans, backdoors and keyloggers	3	3	3	3	3	3	3	3	3	3	3
Malicious documents (MSOffice + PDF)	4	4	4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

Threat sources

- In **Q3 2024**, the **downward trend** for threats from the internet persisted, reaching its **lowest value** since the beginning of 2022 in terms of percentage of ICS computers on which such threats were blocked.

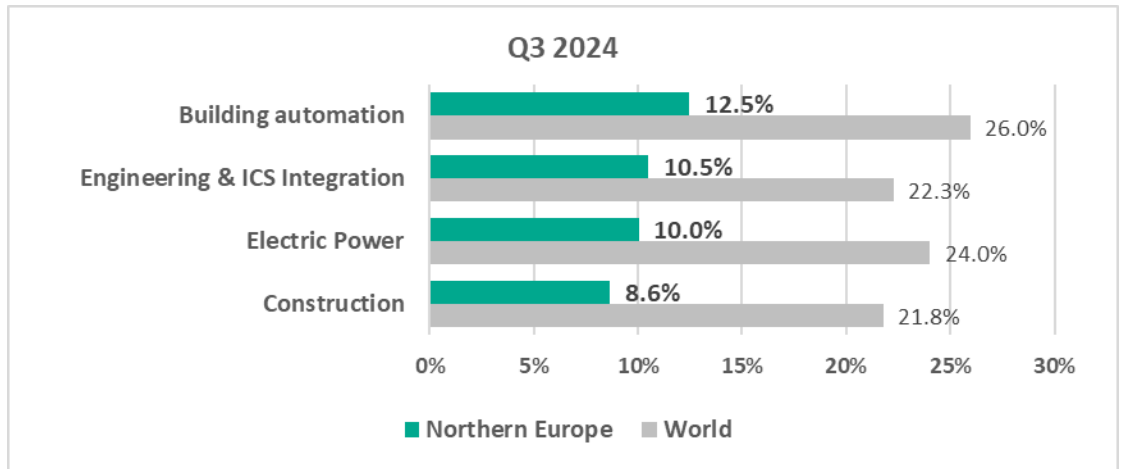


- The trend for threats from **email client** demonstrated similar dynamics to the internet threats, reaching its **lowest point** during the observed period.

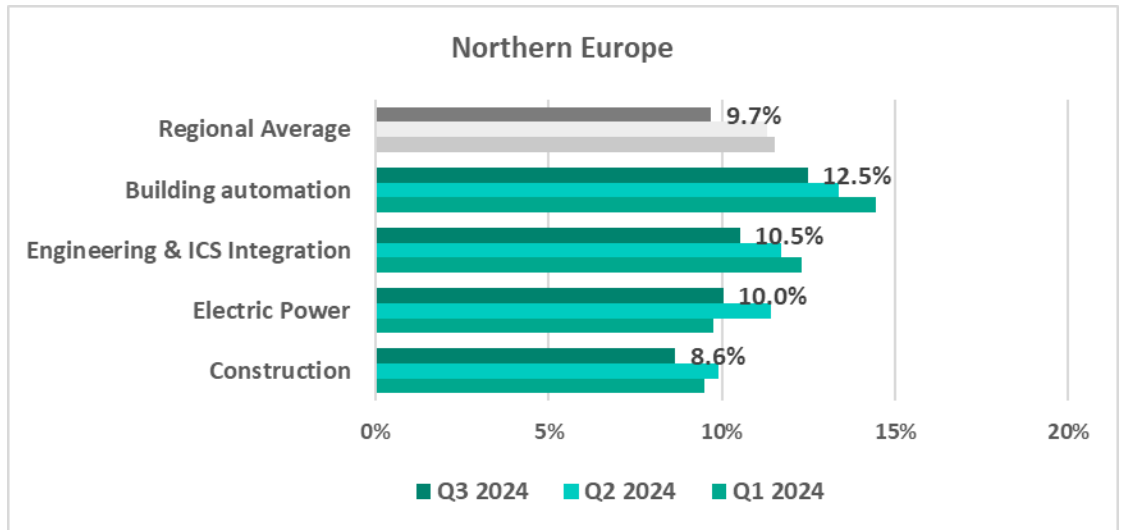


Industries

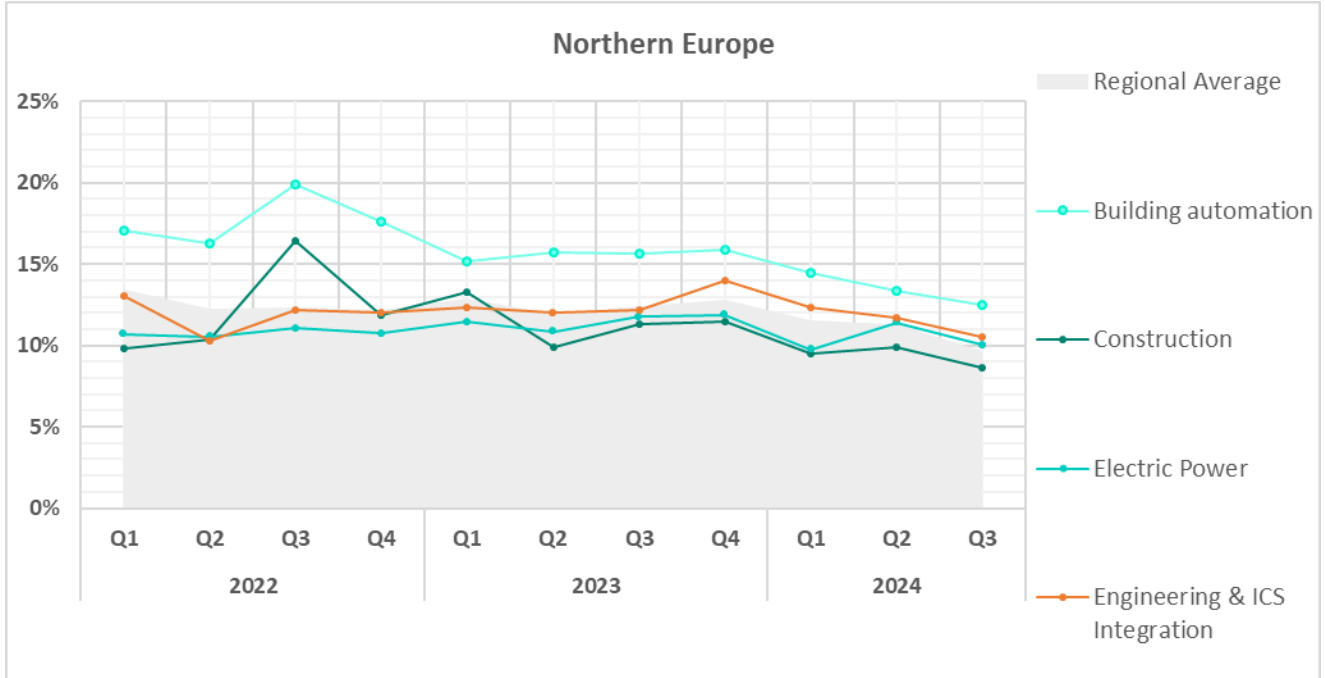
- The most **affected** industry in the region, as highlighted in this report, was **building automation**. It ranked fifth in the global ranking of the selected sectors.
- From a **global perspective**, all sectors under study in the region remained significantly **below** the respective **global averages**.



- In **Q3 2024**, all sectors exhibited a **decrease** in the percentage of ICS computers on which malicious objects were blocked.



- The **building automation** trend remains well **above the regional average** trend, while exhibiting a gradual decline.



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 APTs³.

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

³ 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