Kaspersky ICS CERT

Threat landscape for industrial automation systems

Q4 2024

17.03.2025

Version 1.0

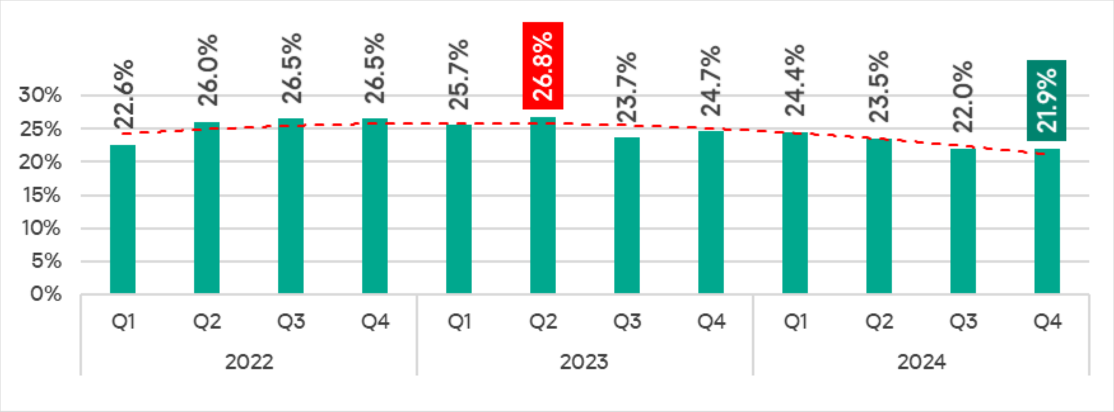
Q4 in numbers

Parameter	Q3 2024	Q4 2024	Quarterly changes
Global percentage of attacked ICS computers	22.0%	21.9%	▼ 0.1 pp
Percentage of ICS computers on which malicious objects from different categories were blocked			
Malicious scripts and phishing pages (JS and HTML)	6.24%	7.11%	▲ 0.87 pp
Denylisted internet resources	6.84%	5.52%	▼ 1.32 pp
Spy Trojans, backdoors and keyloggers	3.91%	4.30%	▲ 0.39 pp
Malicious documents (MSOffice + PDF)	1.97%	1.71%	▼ 0.26 pp
Viruses	1.53%	1.61%	▲ 0.08 pp
Worms	1.30%	1.37%	▲ 0.07 pp
Miners in the form of executable files for Windows	0.71%	0.70%	▼ 0.01 pp
Web miners running in browsers	0.41%	0.39%	▼ 0.02 pp
Malware for AutoCAD	0.40%	0.38%	▼ 0.02 pp
Ransomware	0.16%	0.21%	▲ 0.05 pp
Main threat sources			
Internet	10.84%	9.98%	▼ 0.86 pp
Email clients	2.95%	2.72%	▼ 0.23 pp
Removable media	0.69%	0.64%	▼ 0.05 pp
Network folders	0.11%	0.08%	▼ 0.03 pp

Statistics across all threats

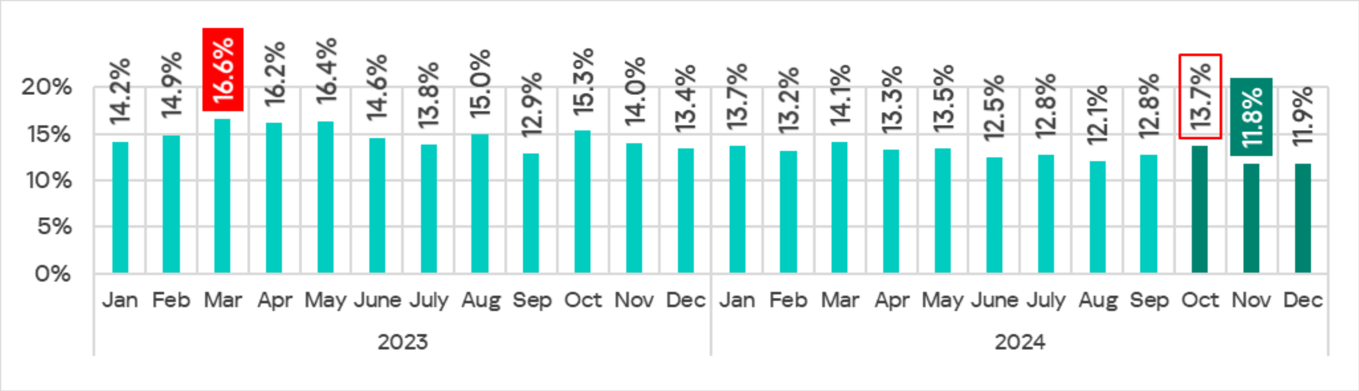
In the fourth quarter of 2024, the percentage of ICS computers on which malicious objects were blocked decreased by 0.1 pp from the previous quarter to 21.9%.

Percentage of ICS computers on which malicious objects were blocked, by quarter, 2022-2024



Compared to the fourth quarter of 2023, the percentage decreased by 2.5 pp.

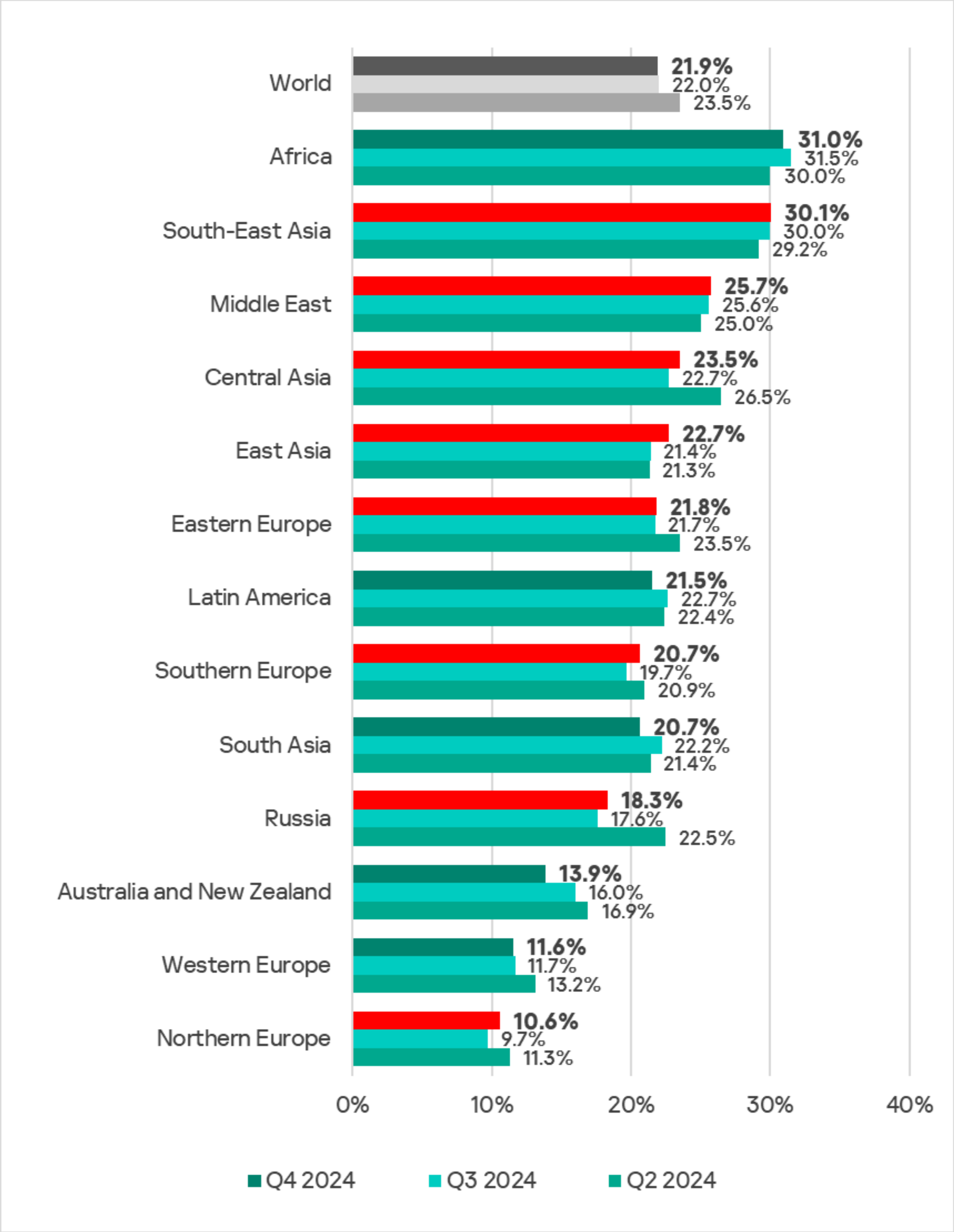
The percentage of ICS computers on which malicious objects were blocked during the fourth quarter of 2024 was highest in October and lowest in November. In fact, the percentage in November 2024 was the lowest of any month in two years.



Percentage of ICS computers on which malicious objects were blocked, Jan 2023–Dec 2024

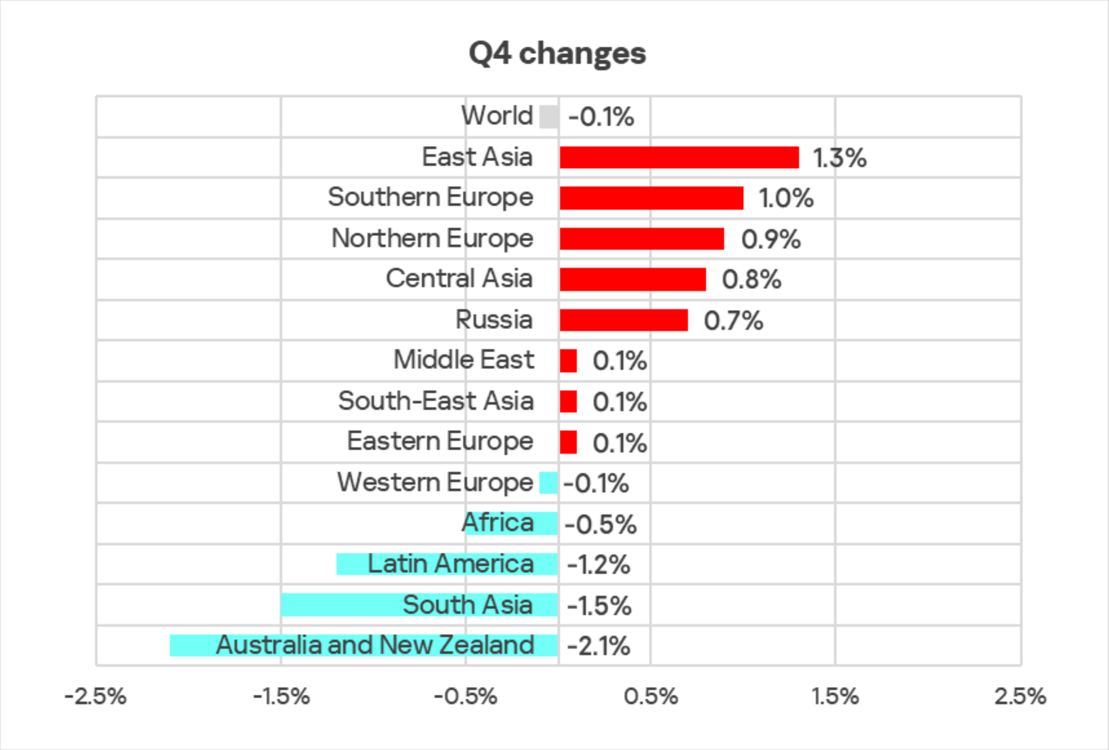
Regionally, the percentage of ICS computers that blocked malicious objects during the quarter ranged from 10.6% in Northern Europe to 31% in Africa.

Regions ranked by percentage of ICS computers where malicious objects were blocked, Q4 2024



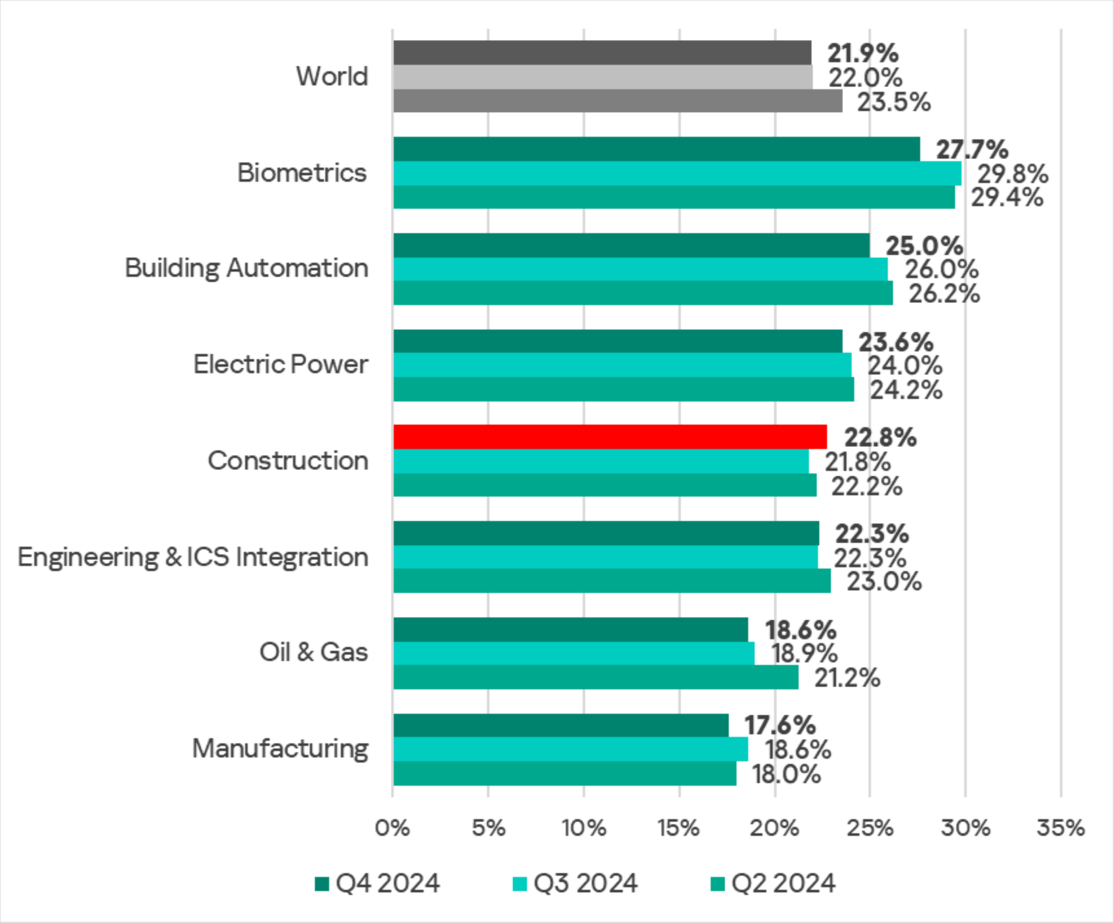
Eight of 13 regions saw their percentages increase from the previous quarter.

Regions and world. Changes in the percentage of attacked ICS computers in Q4 2024

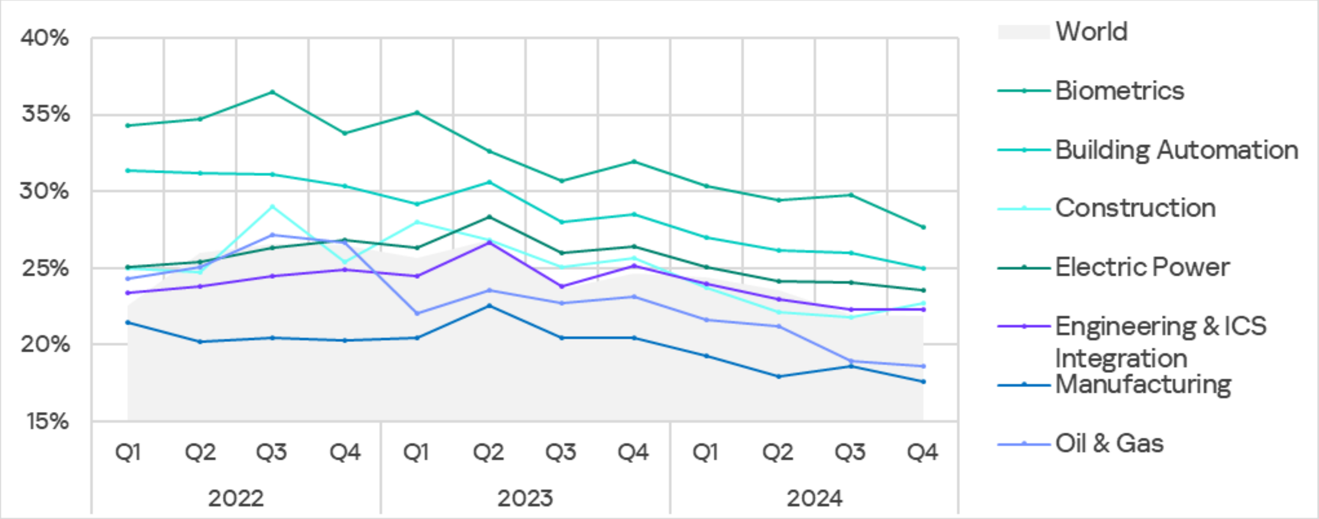


Selected industries

The biometrics sector led the surveyed industries in terms of the percentage of ICS computers on which malicious objects were blocked.



In the fourth quarter of 2024, the percentage of ICS computers on which malicious objects were blocked decreased across most industries, with the exception of the construction sector.



Percentage of ICS computers on which malicious objects were blocked in selected industries

Diversity of detected malicious objects

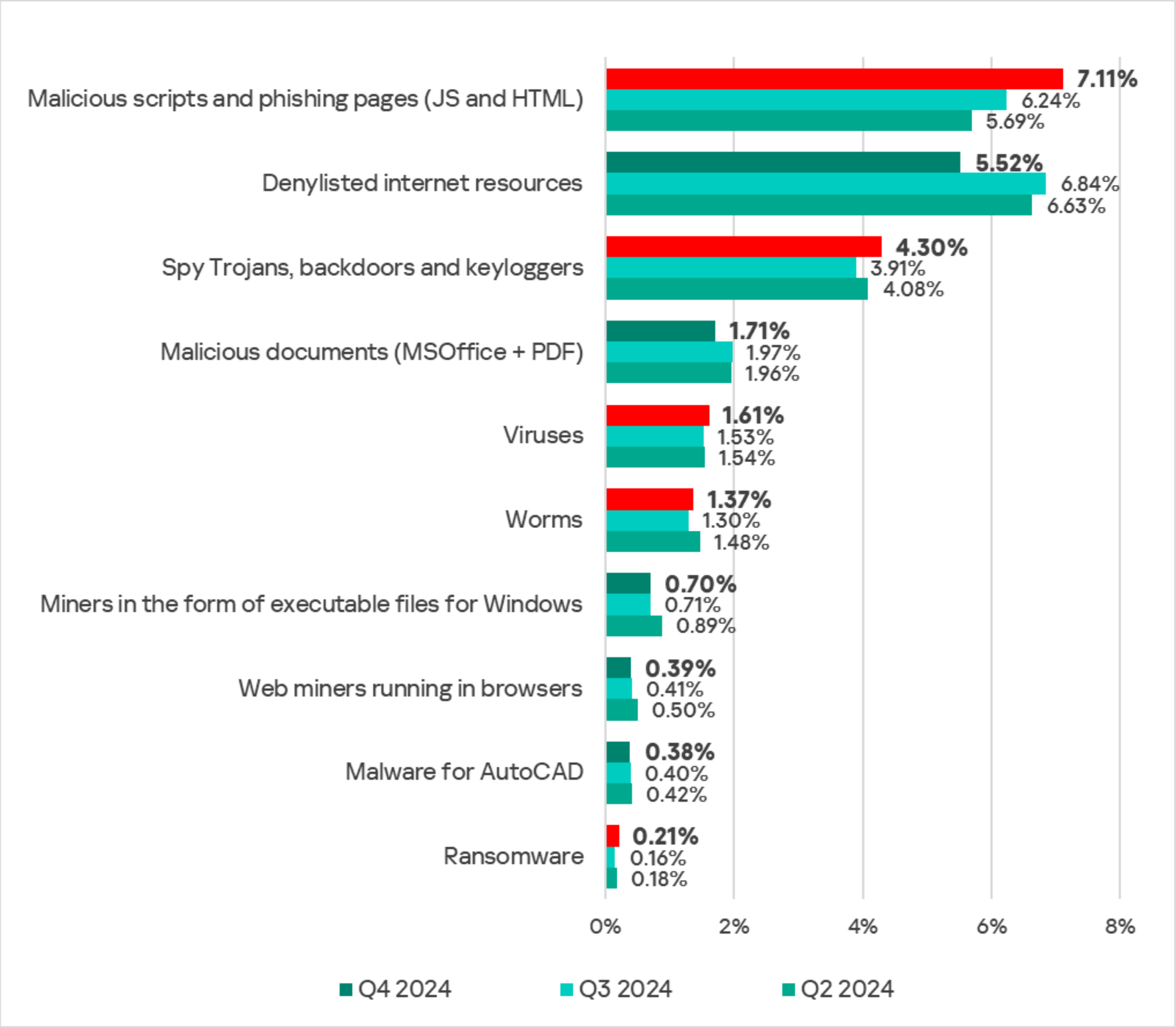
Malicious objects of various categories, which Kaspersky products block on ICS computers, can be divided into three groups according to their distribution method and purpose.

1. Malicious objects used for initial infection.
   This category includes denylisted internet resources, malicious scripts and phishing pages, and malicious documents.
2. Next-stage malware.
   This category includes spyware, ransomware, miners in the form of executable files for Windows, and web miners.
3. Self-propagating malware.
   This category includes worms and viruses.

Malware for AutoCAD does not belong to a specific group, as it can spread in a variety of ways.

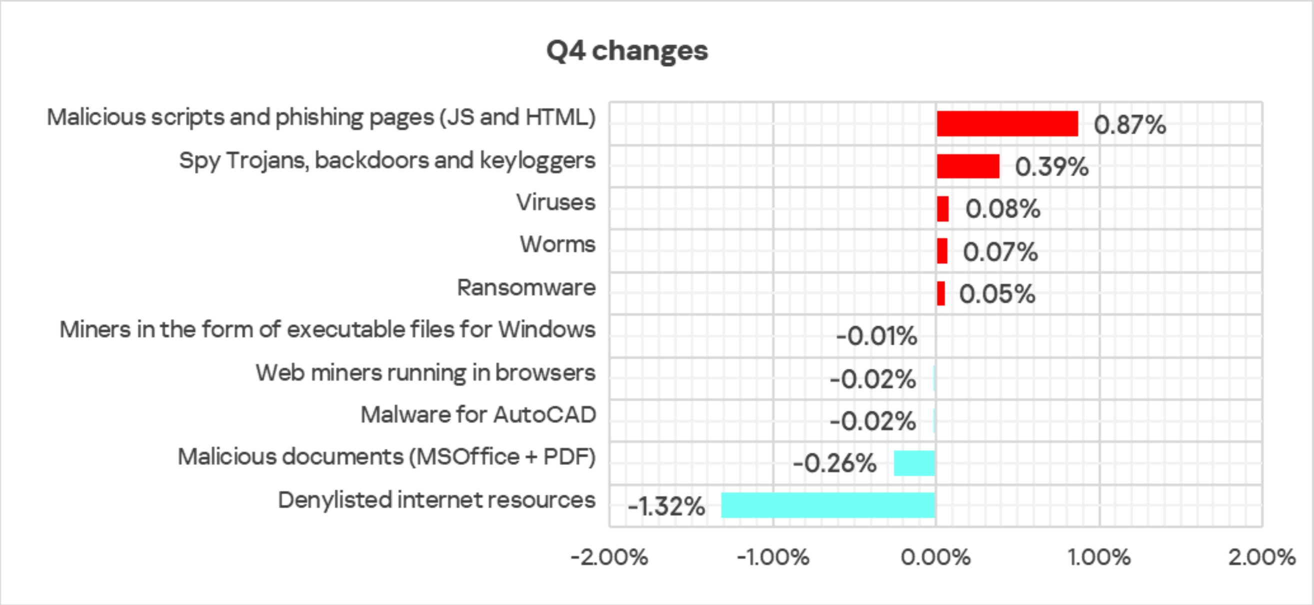
In the fourth quarter of 2024, Kaspersky's protection solutions blocked malware from 11,065 different malware families of various categories on industrial automation systems.

Malicious objects categorized as initial infection threats typically rank highest among threat categories in terms of the percentage of ICS computers on which threats were blocked.



Percentage of ICS[1] computers on which the activity of malicious objects from various categories was blocked

[1] Note that it would not be appropriate to add up the percentages because in many cases more than one threat type could be blocked on a computer during the period under review.



Changes in the percentage of ICS computers on which malicious objects from different categories were blocked in Q4 2024 compared to Q3 2024.

The largest proportional growth during this period was in the percentage of ICS computers on which **ransomware** was blocked, which increased 1.3 times.

Another notable proportional increase was in the percentage of ICS computers on which **malicious scripts and phishing pages, spyware, worms, and viruses** were blocked, each growing 1.1 times.

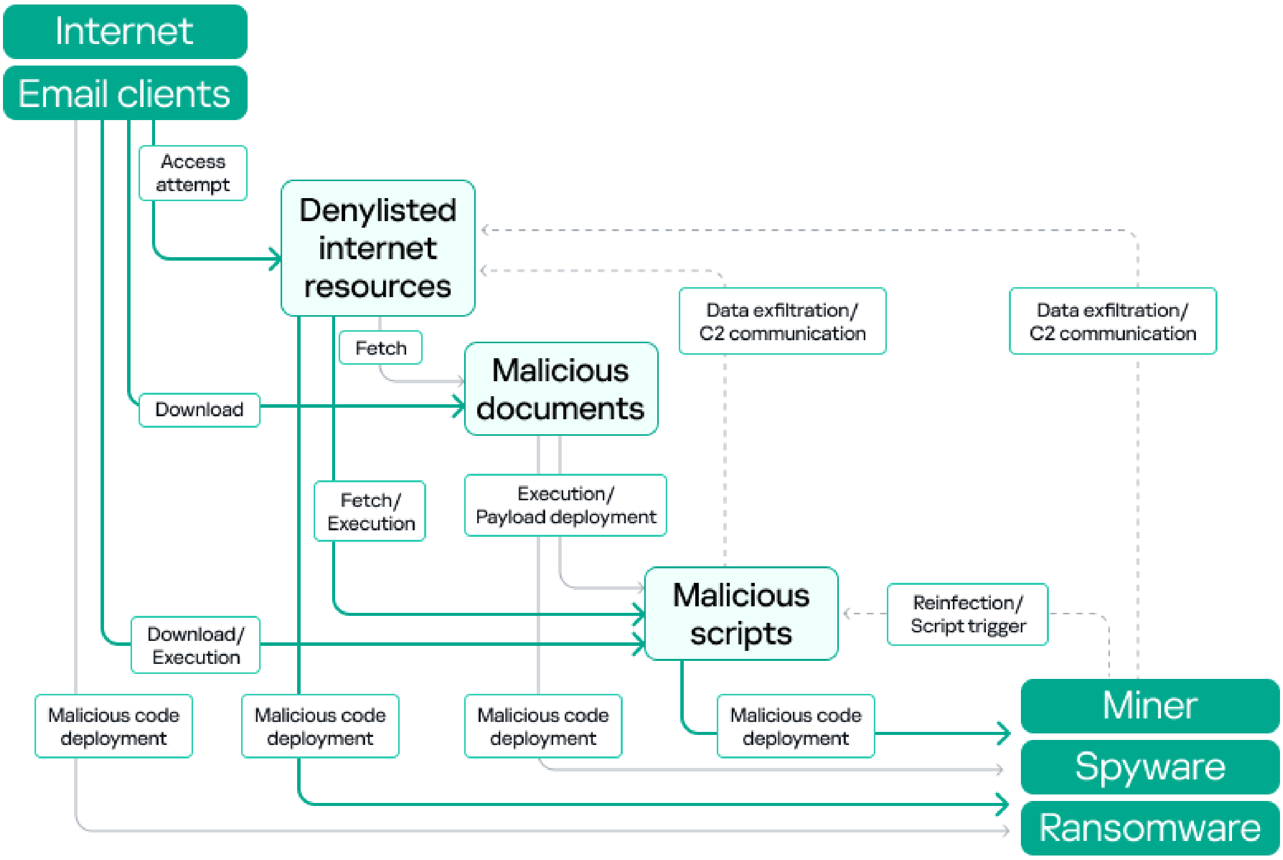
The most notable proportional decrease was in the percentage of ICS computers on which **denylisted internet resources** and **malicious documents** were blocked, both of which decreased 1.2 times.

Malicious objects used for initial infection

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

The logic of cybercriminals is that 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.

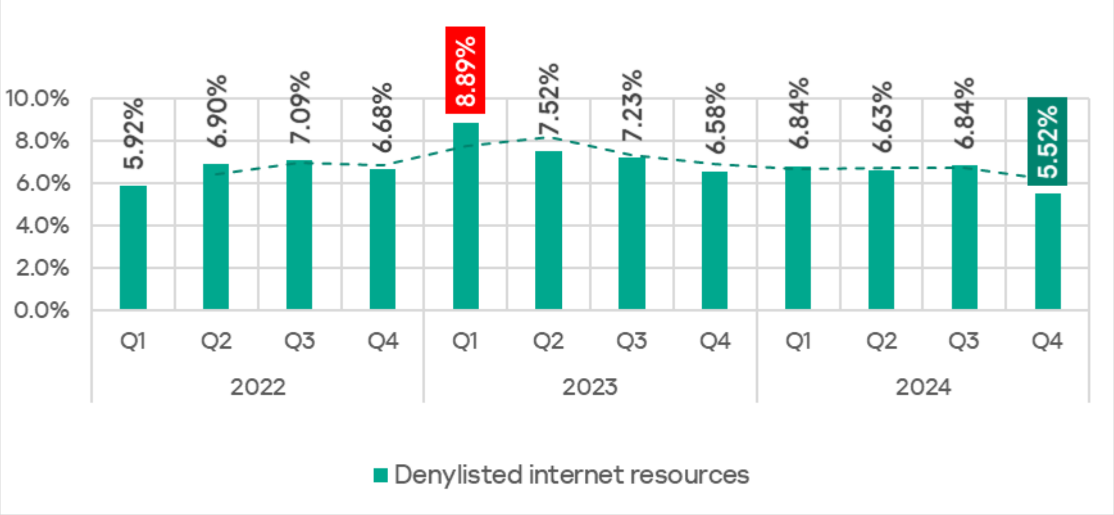

Internet
Email clients
Access attempt
Denylisted internet resources
Fetch
Download
Malicious documents
Data exfiltration/ C2 communication
Data exfiltration/ C2 communication
Fetch/ Execution
Execution/ Payload deployment
Malicious scripts
Reinfection/ Script trigger
Download/ Execution
Malicious code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

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

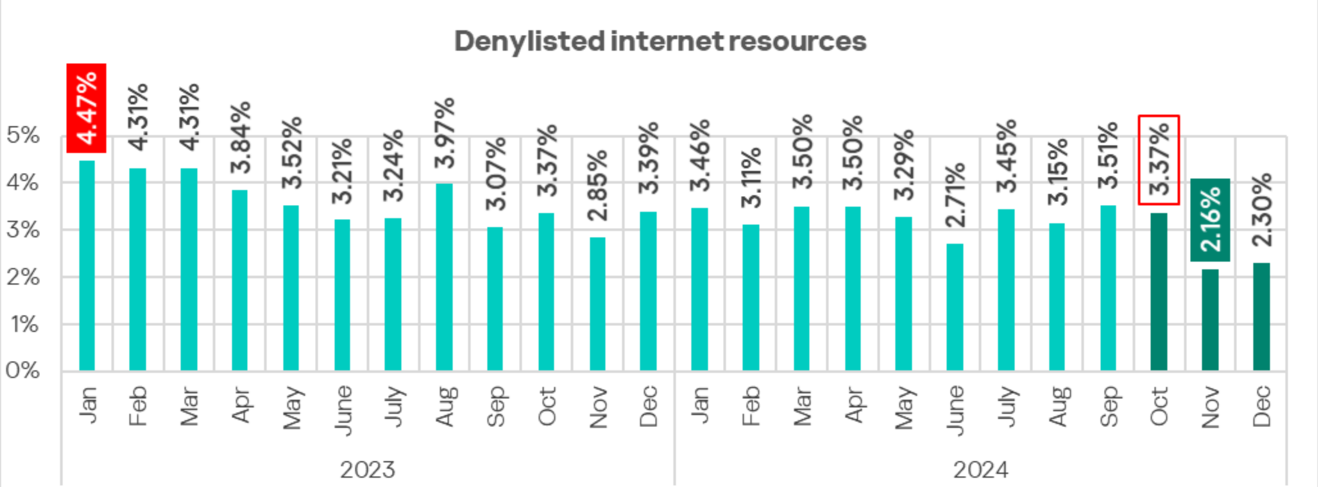
Denylisted internet resources

Denylisted internet resources are associated with malware spread or control. A significant percentage of these resources is used for spreading malicious scripts and phishing pages (HTML).

In the fourth quarter of 2024, the percentage of ICS computers on which denylisted internet resources were blocked decreased, reaching its lowest value in the observed period.



The rate of denylisted internet resources fluctuated throughout the months of the fourth quarter, reaching its highest point in October and its lowest in November 2024, which also marked the lowest monthly rate in the past two years.



As previously noted in the Q3 2024 report, the increase in blocked denylisted internet resources was primarily driven by an increase in the number of newly created domain names and IP addresses used by cybercriminals as command and control (C2) infrastructure for distributing malware and phishing attacks.

The decline in the percentage of denylisted internet resources in November-December 2024 was likely influenced not only by proactive threat mitigation measures at various levels – from resource owners and hosting providers to ISPs and law enforcement agencies. Another contributing factor was the tendency of attackers to frequently change domains and IP addresses to evade detection in the initial stages, based on lists of known malicious resources.

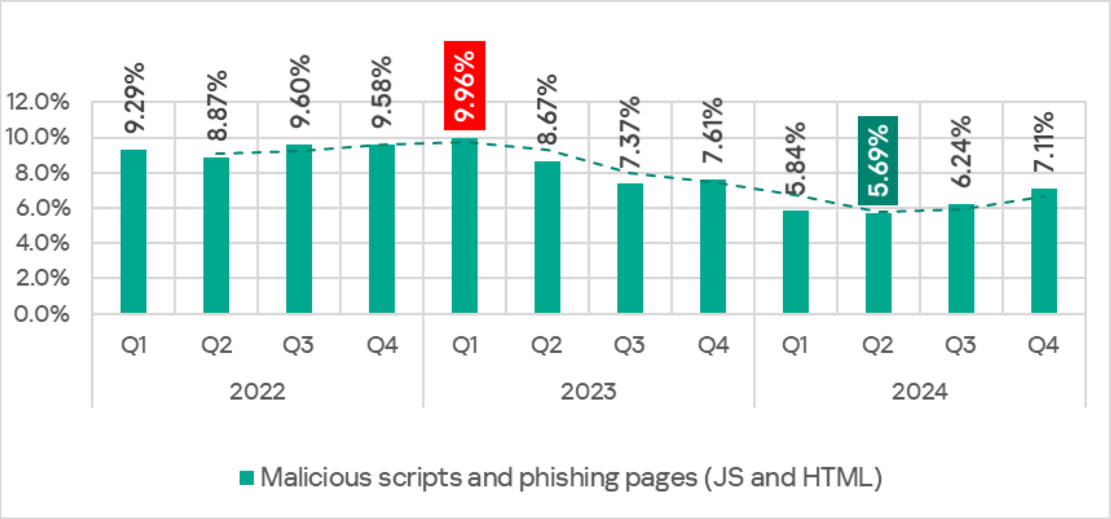
In practice, this means that until a malicious web resource is identified and added to a denylist, it may not immediately appear in threat statistics, leading to an apparent decrease in the percentage of ICS computers on which such resources were blocked.

However, in Q4, we also saw a rise in the percentage of the next steps in the attack chain – malicious scripts and phishing pages, spyware, and ransomware.

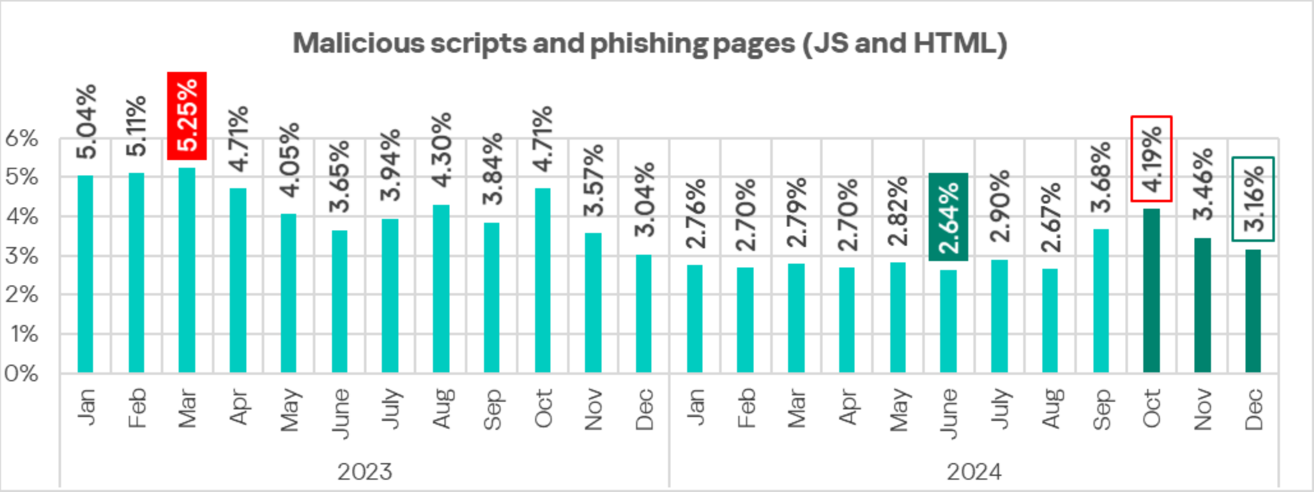
Malicious scripts and phishing pages (JS and HTML)

Malicious actors use scripts for a wide range of objectives: collecting information, tracking, redirecting the browser to a malicious site, and uploading various types of malware (spyware and/or silent crypto mining tools) to the user's system or browser. These spread via the internet and email.

In the fourth quarter of 2024, the percentage of ICS computers on which malicious scripts and phishing pages were blocked continued to increase.



The monthly rate of malicious scripts and phishing pages spiked in October, reaching its highest monthly value in 2024, before gradually decreasing throughout the rest of the fourth quarter, as shown below.



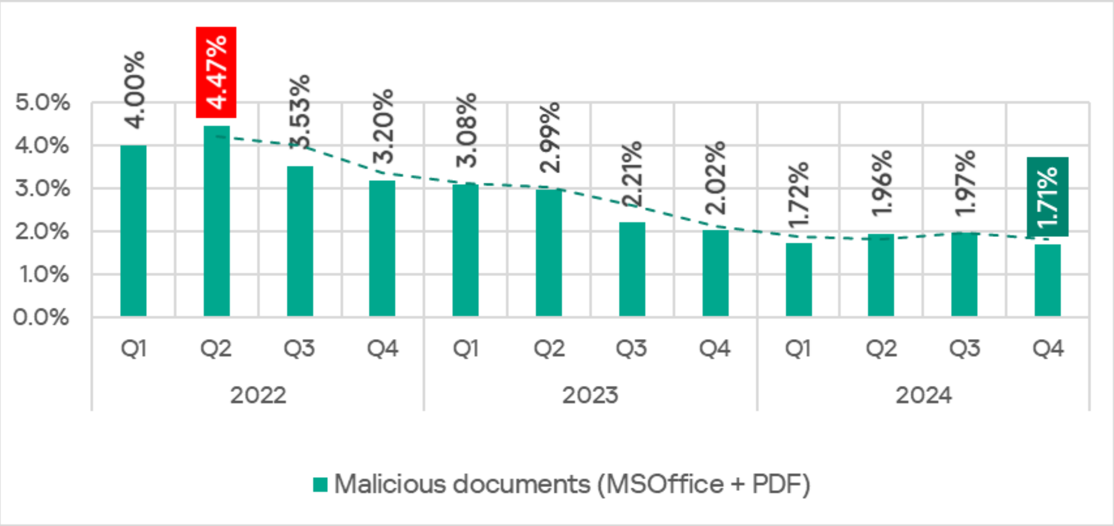
A significant increase in the percentage of malicious scripts and phishing pages in October was driven by a series of widespread phishing attacks in late summer and early autumn 2024, as mentioned in the Q3 2024 report. Threat actors used malicious scripts that executed in the browser, mimicking various windows with CAPTCHA-like interfaces, browser error messages, and similar pop-ups to trigger the download of next-stage malware – either the Lumma stealer or the Amadey Trojan.

Malicious documents (MSOffice+PDF)

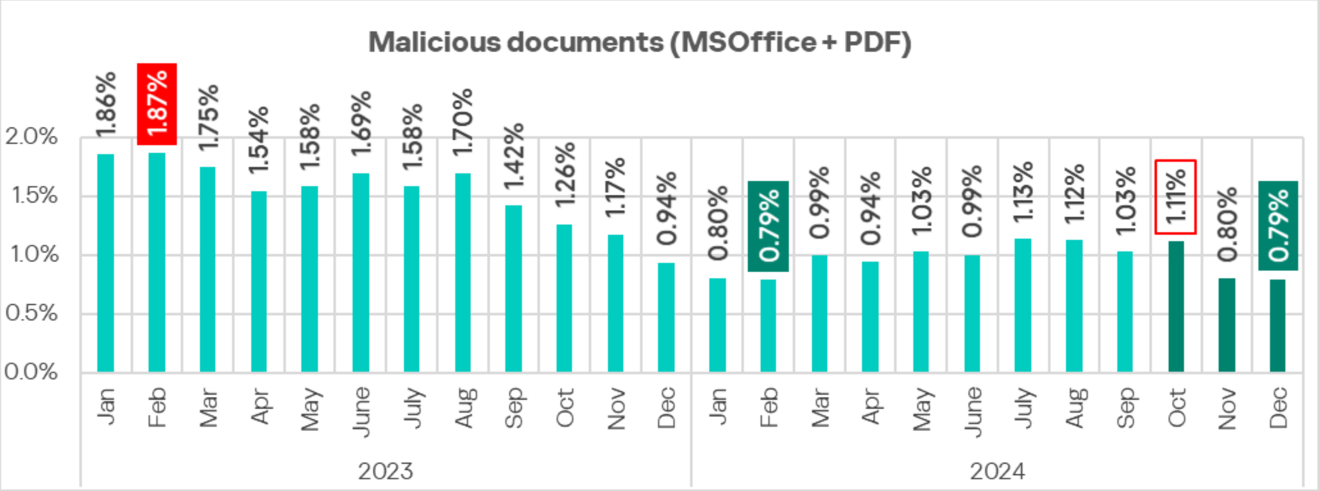
Attackers send malicious documents attached to phishing messages and use them in attacks aimed at initial infection of computers. Malicious documents typically contain exploits, malicious macros, and malware links.

In Q4 2024, the percentage of ICS computers with malicious documents on them was the lowest it has been in the last three years.

.



As shown below, the monthly rate of malicious documents in December 2024 was the lowest recorded in the past two years, matching the rate in February 2024.



Next-stage malware

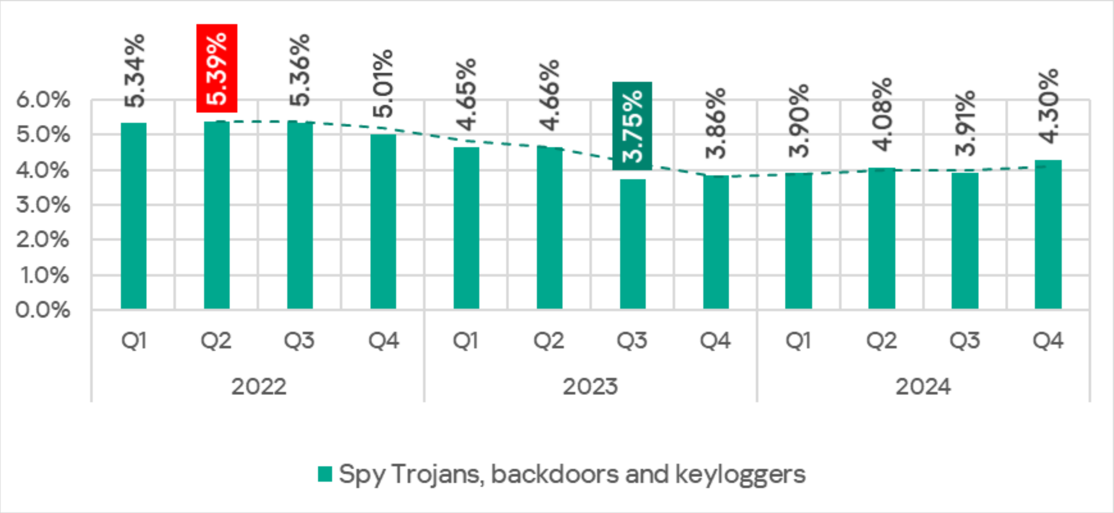
Malicious objects used to initially infect computers deliver next-stage malware – spyware, ransomware, and miners – to victims' computers. As a rule, the higher the percentage of ICS computers on which the initial infection malware is blocked, the higher the percentage for next-stage malware.

Spyware

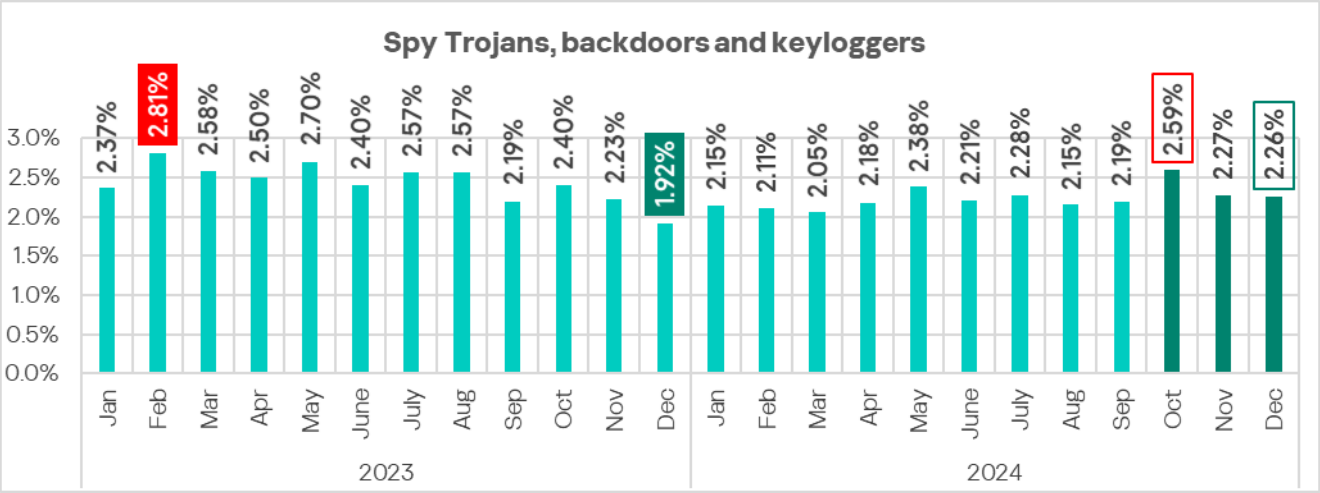
Spyware (spy Trojans, backdoors, and keyloggers) can be found in lots of phishing emails sent to industrial organizations. Spyware is used for unauthorized remote access and confidential data theft. The ultimate goal of most spyware attacks is stealing money, but spyware is also used in targeted attacks, for cyberespionage.

Spyware is also used to steal the information needed to deliver other types of malware, such as ransomware and silent miners, as well as to prepare for targeted attacks.

In Q4 2024, the percentage of ICS computers on which spyware was blocked increased.

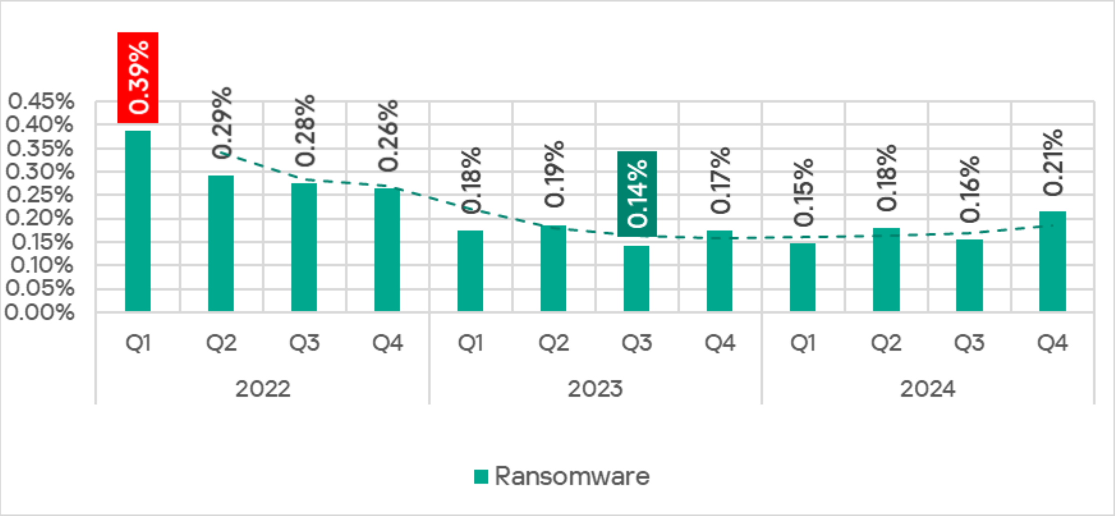


As shown below, the monthly rate of spyware spiked in October 2024 reaching its highest monthly value in 2024.

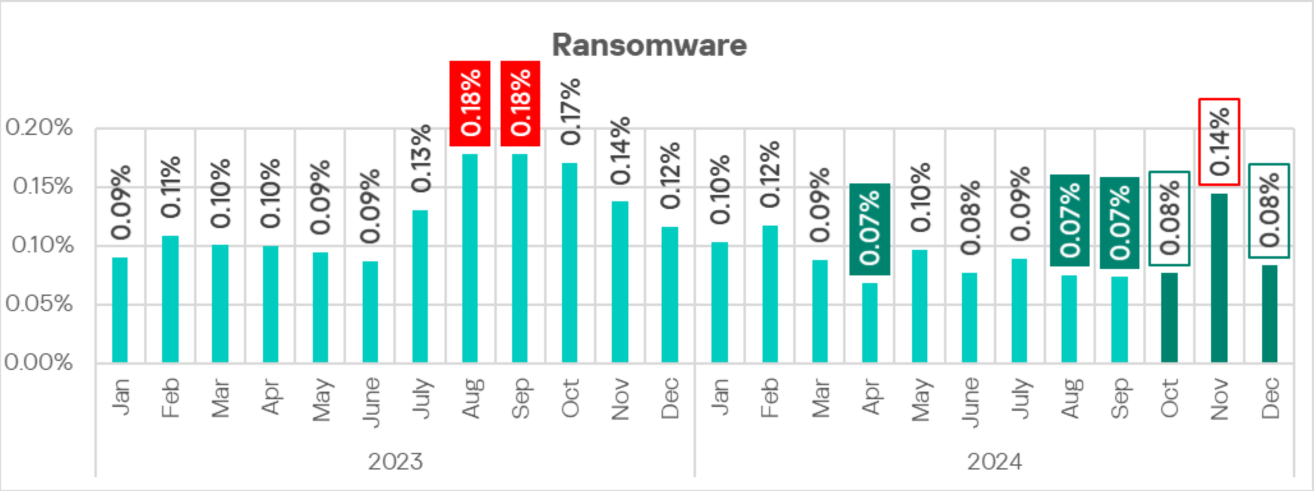

Spy Trojans, backdoors and keyloggers
3.0%
2.5%
2.0%
1.5%
1.0%
0.5%
0.0%
2.37%
2.81%
2.58%
2.50%
2.70%
2.40%
2.57%
2.57%
2.19%
2.40%
2.23%
1.92%
2.15%
2.11%
2.05%
2.18%
2.38%
2.21%
2.28%
2.15%
2.19%
2.59%
2.27%
2.26%
Jan
Feb
Mar
Apr
May
June
July
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
June
July
Aug
Sep
Oct
Nov
Dec
2023
2024

Ransomware

The percentage of ICS computers on which ransomware was blocked increased by a factor of 1.3 in Q4 2024 compared to the previous quarter, reaching its highest value in two years.



The increase was driven by a spike in November, which marked the highest monthly rate for ransomware in 2024.



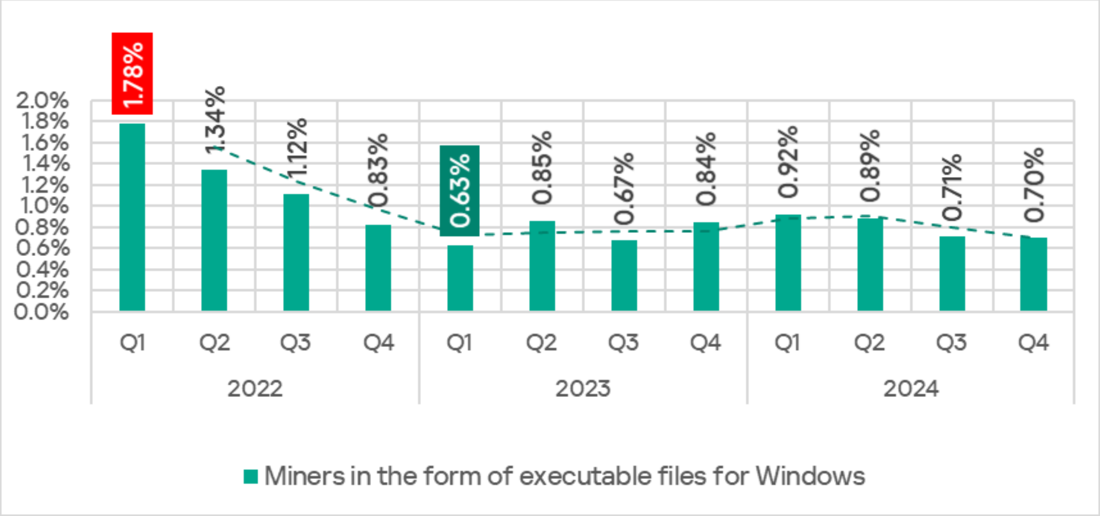
Miners in the form of executable files for Windows

In addition to “classic” miners – applications written in .Net, C++, or Python and designed for hidden crypto mining – new forms are emerging. Popular “fileless” execution techniques continue to be adopted by various threat actors, including those implanting crypto miners on OT machines.

In the fourth quarter of 2024, similar to the previous quarter, a significant portion of Windows miners found on ICS computers consisted of archives with names that mimicked legitimate software. These archives did not contain actual software, but did include 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 crypto miners, by embedding malicious code directly into command line arguments. This code runs entirely in memory, enabling fileless execution and minimizing detection.

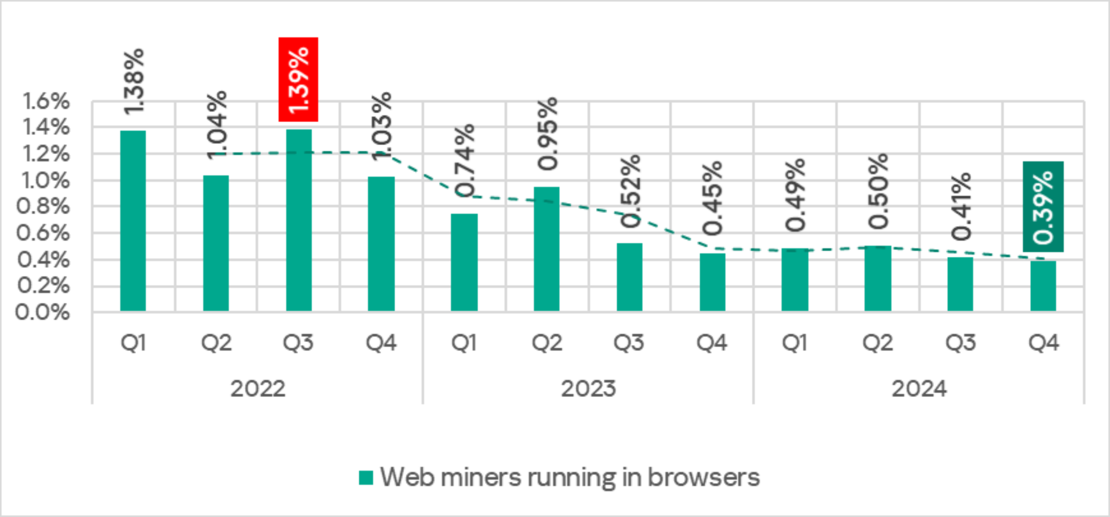
Another common method of deploying miners on ICS computers involves using legitimate cryptocurrency mining software such as XMRig, NBMiner, OneZeroMiner, and others. While these miners are not inherently malicious, they are classified as RiskTools by security systems. Attackers exploit these miners by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

In Q4 2024, the percentage of ICS computers on which miners in the form of executable files for Windows were blocked continued to decrease, reaching its lowest value in 2024.



Web miners

The percentage of ICS computers on which web miners were blocked also continued to fall in the fourth quarter of 2024, reaching its lowest value in the observed period.



Self-propagating malware. Worms and viruses

Self-propagating malware (worms and viruses) is a category unto itself. Worms and virus-infected files were originally used for initial infection, but as botnet functionality evolved, they took on next-stage characteristics.

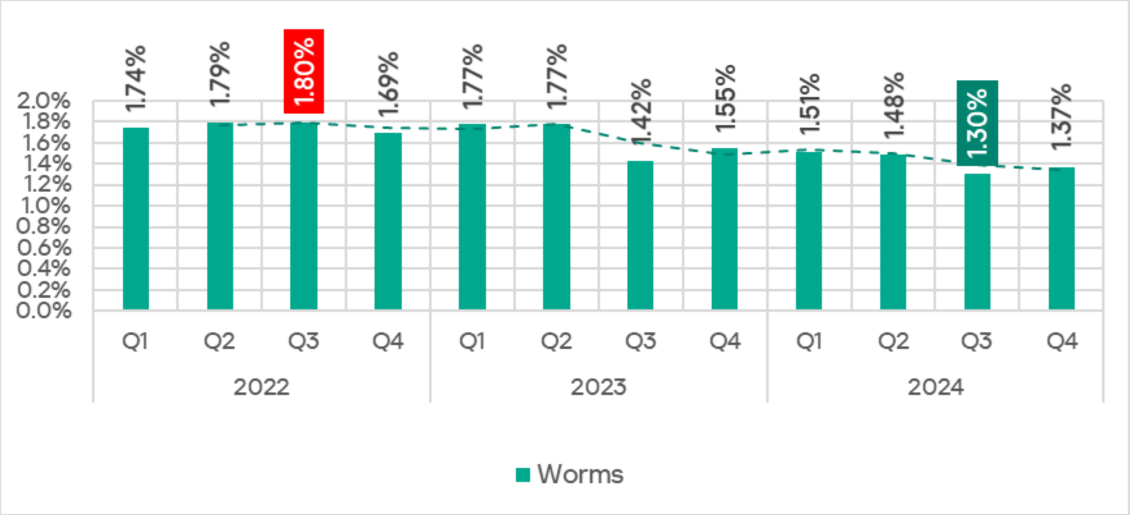
To spread across ICS networks, **viruses and worms** rely on removable media, network folders, infected files including backups, and network attacks on outdated software such as Radmin2.

A lot of those still spreading are legacy viruses and worms whose command and control servers have been shut down. However, these types of malware can compromise infected systems by opening network ports or changing configurations, cause software failures, denial of service, and so on.

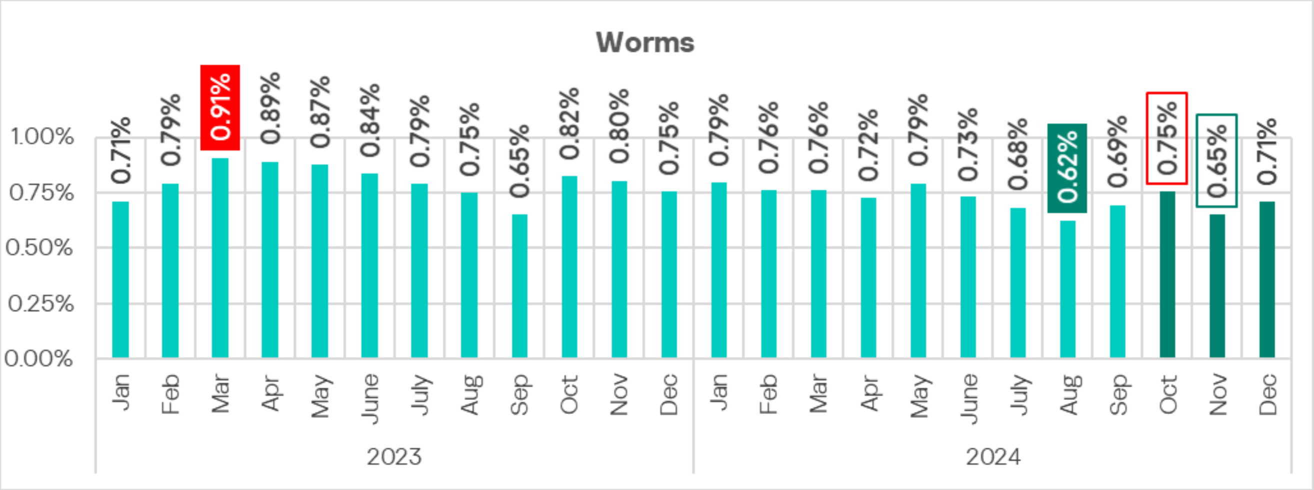
Worms

New worm versions used by malicious actors to spread spyware, ransomware, and miners can also be found on ICS networks. In most cases, they rely on network service (e.g., SMB or RDP) exploits that have been addressed by the vendors but still persist on OT networks, previously stolen credentials, or password brute-forcing.

After hitting its lowest point in Q3 2024, the percentage of ICS computers on which worms were blocked increased in the last quarter of 2024.

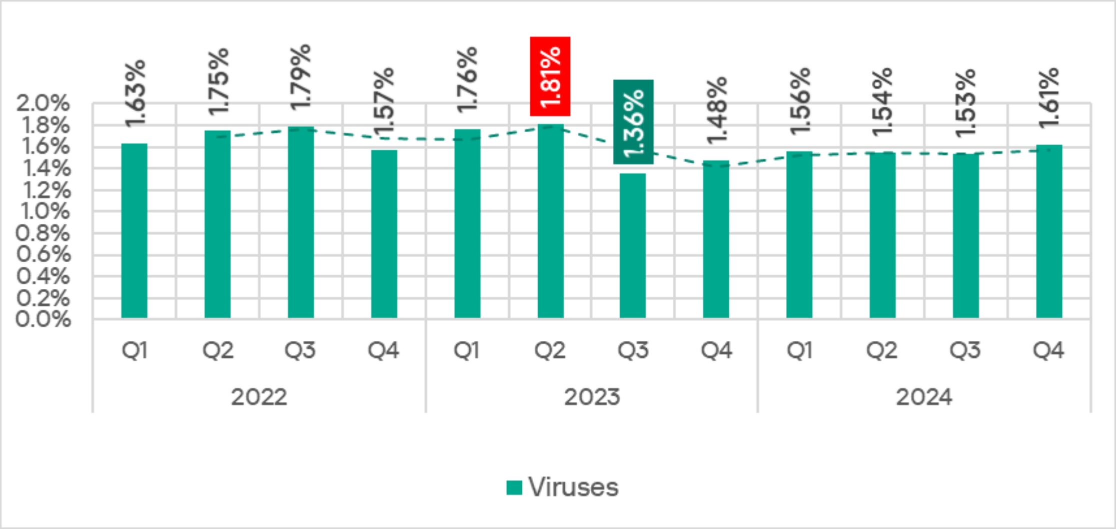


The increase was driven by a spike in October.

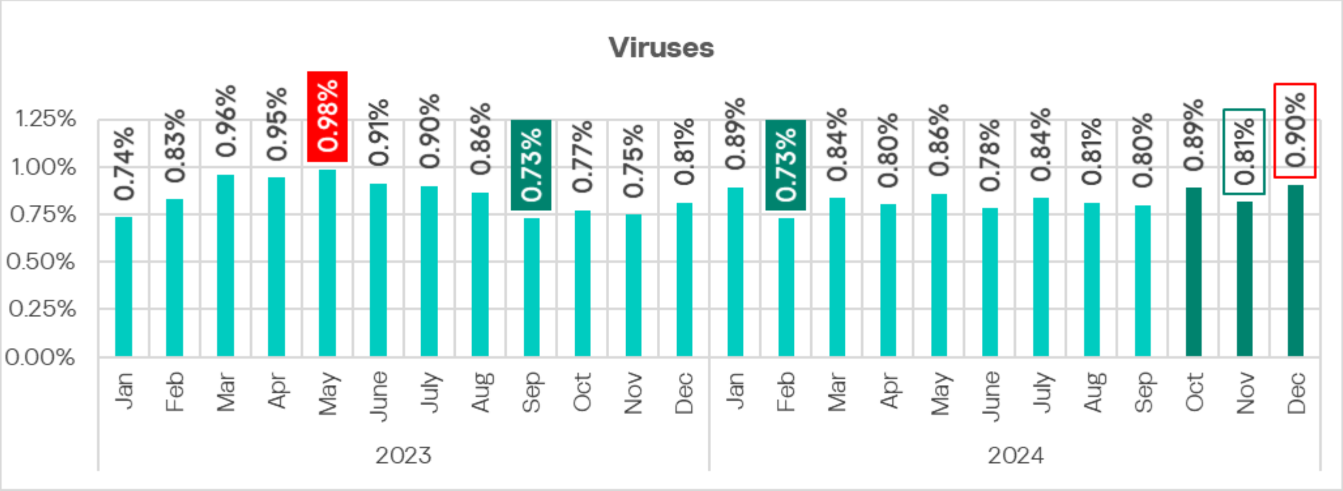


Viruses

The percentage of ICS computers on which viruses were blocked increased in the last quarter of 2024.



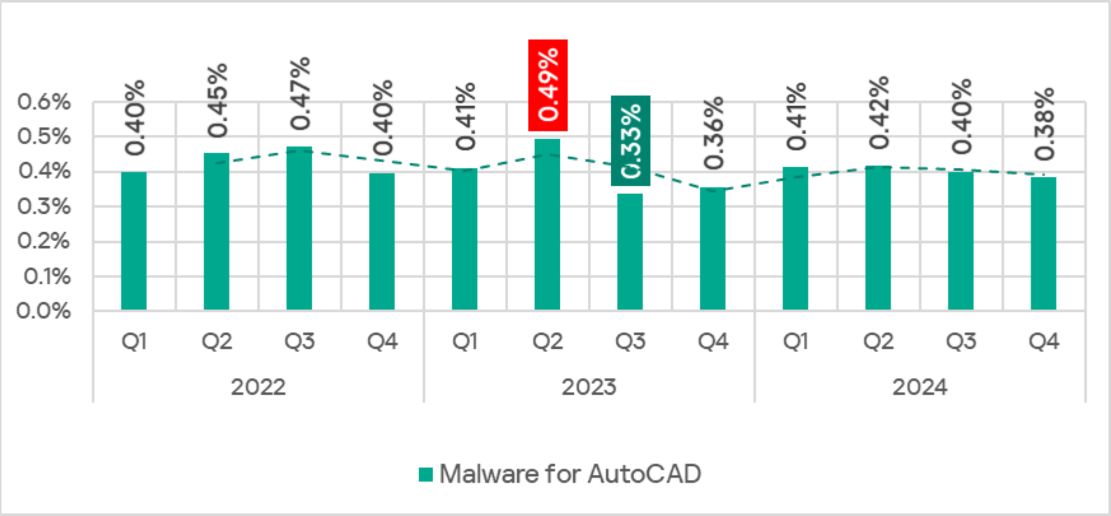
The virus rate fluctuated throughout the months of the fourth quarter, peaking in December 2024, which also marked the highest monthly rate in 2024.



AutoCAD malware

AutoCAD malware is typically a low-level threat, coming last in the malware category rankings in terms of the percentage of ICS computers on which it was blocked.

In the fourth quarter of 2024, the percentage of ICS computers on which AutoCAD malware was blocked continued to decrease.

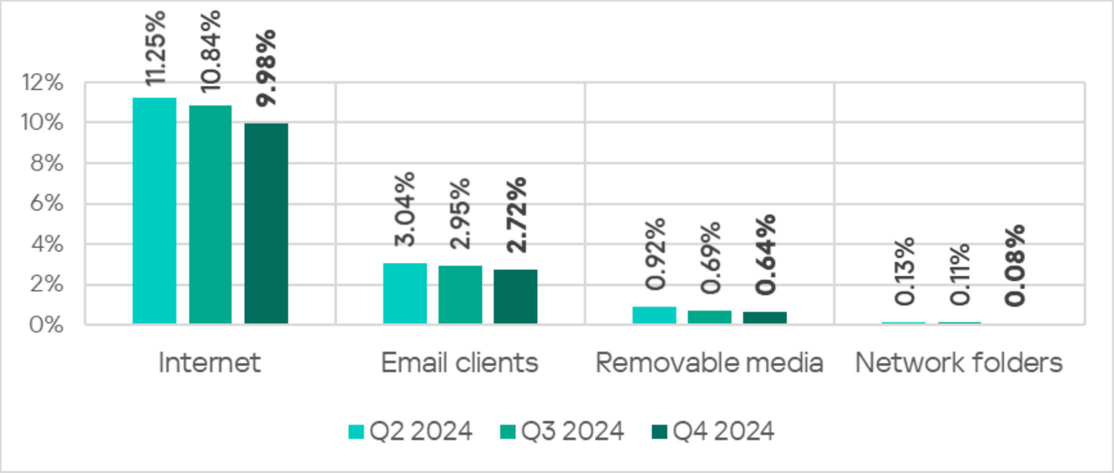


Main threat sources

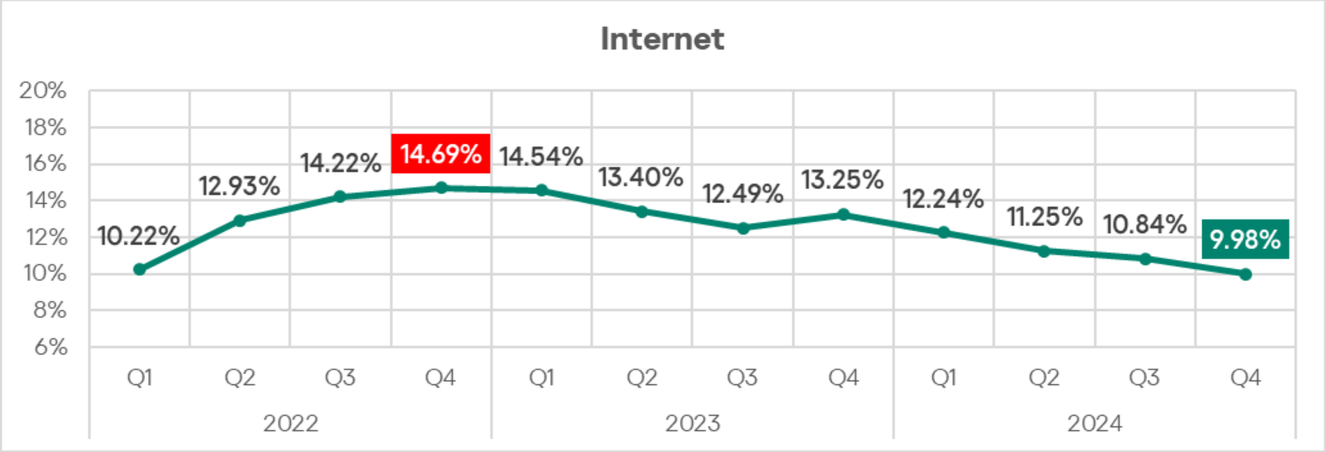
The internet, email clients, and removable storage devices remain the primary sources of threats to computers in an organization's technology infrastructure. Note that the sources of blocked threats cannot be reliably identified in all cases.

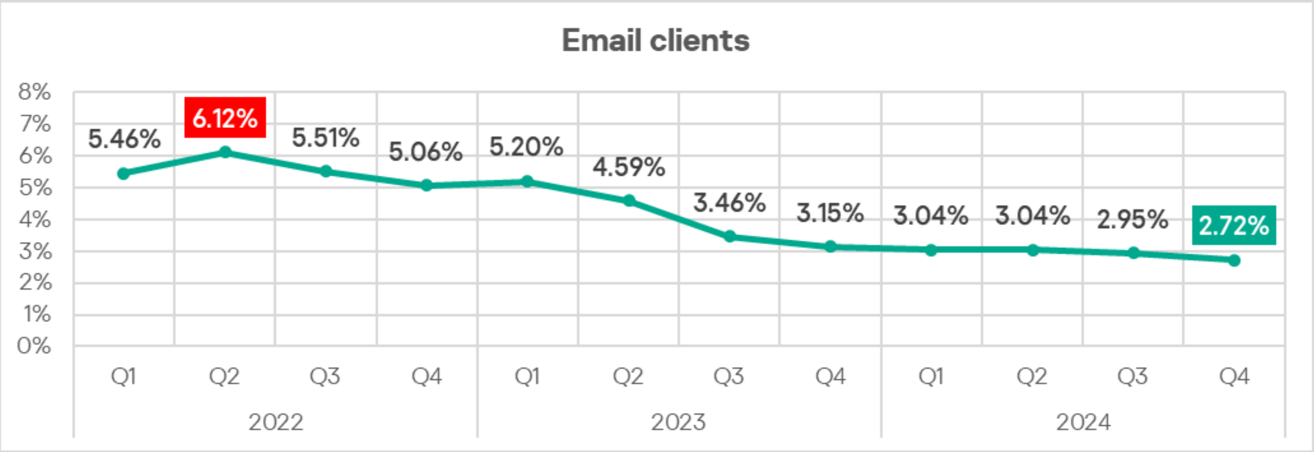
In the fourth quarter of 2024, the percentage of ICS computers on which threats from various sources were blocked decreased for all threat sources described in this report.

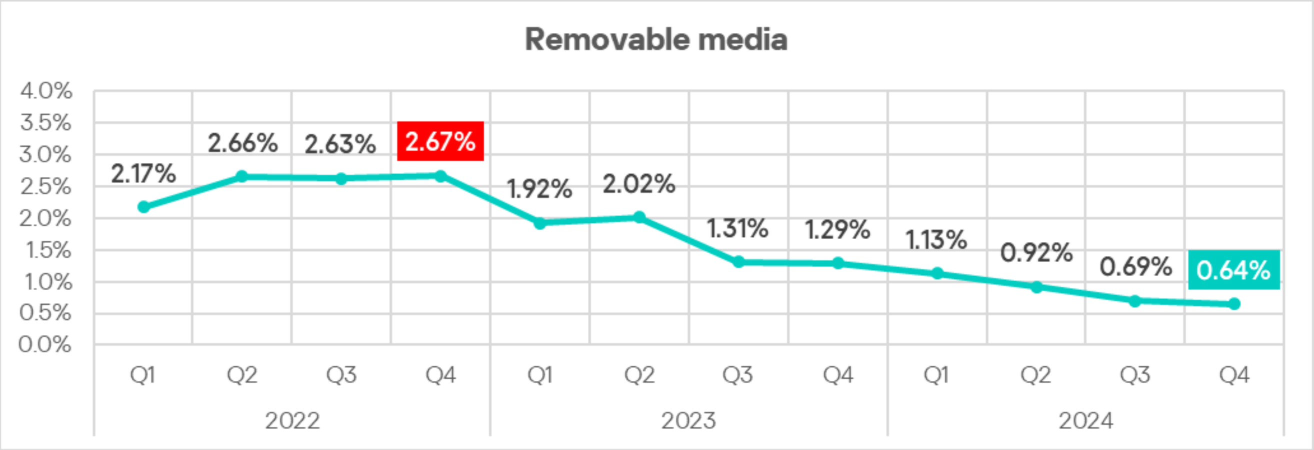
Percentage of ICS computers on which malicious objects from various sources were blocked

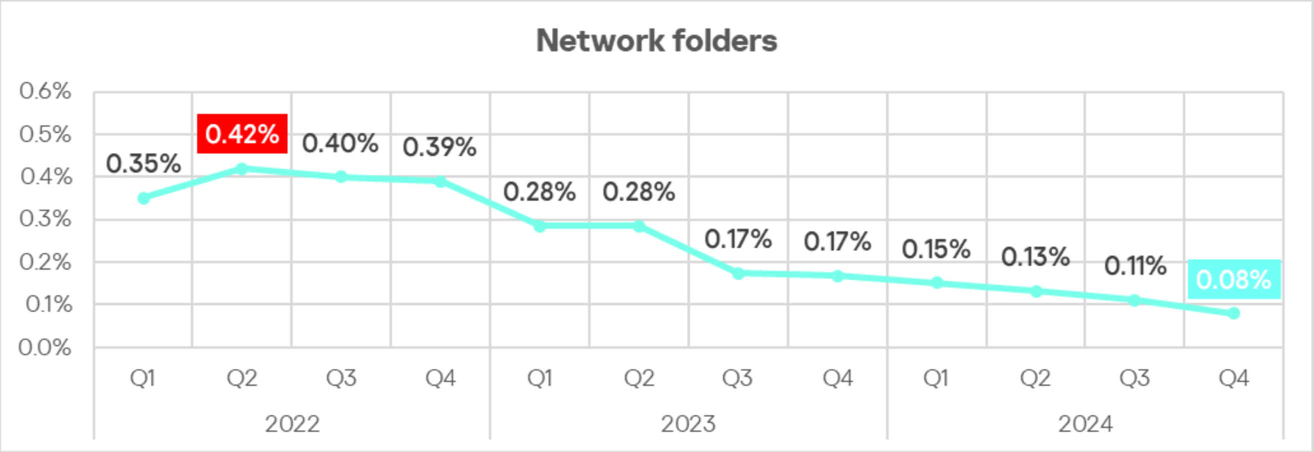


All threat sources recorded their lowest values for the observed period.




Email clients
8%
7%
6%
5%
4%
3%
2%
1%
0%
5.46%
6.12%
5.51%
5.06%
5.20%
4.59%
3.46%
3.15%
3.04%
3.04%
2.95%
2.72%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
2022
2023
2024


Removable media
4.0%
3.5%
3.0%
2.5%
2.0%
1.5%
1.0%
0.5%
0.0%
2.17%
2.66%
2.63%
2.67%
1.92%
2.02%
1.31%
1.29%
1.13%
0.92%
0.69%
0.64%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
2022
2023
2024


Network folders
0.6%
0.5%
0.4%
0.3%
0.2%
0.1%
0.0%
0.35%
0.42%
0.40%
0.39%
0.28%
0.28%
0.17%
0.17%
0.15%
0.13%
0.11%
0.08%
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
2022
2023
2024

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 those KSN users who consented to its anonymous sharing and processing for the purpose described in the KSN Agreement for the Kaspersky product installed on their computer.

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

Data shared by the user contains only the data types and categories described in the appropriate KSN Agreement. This data helps to a significant extent in analyzing the threat landscape and serves as a prerequisite for detecting new threats including targeted attacks and APTs[2]*.*

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

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

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

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

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