Kaspersky ICS CERT

kaspersky

Threat landscape for industrial automation systems

Q1 2024

27.05.2024

Version 1.1

Q1 in numbers

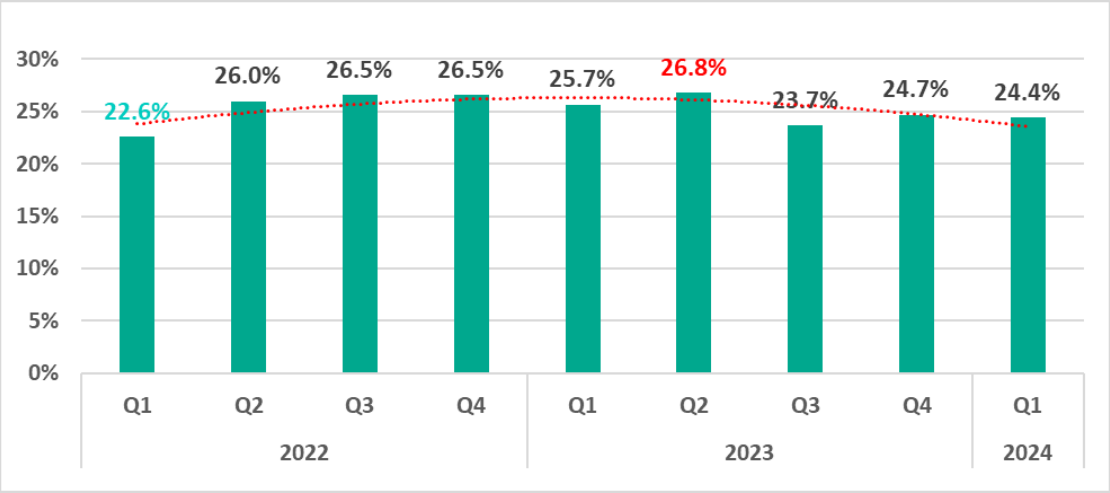
Parameter	Q4 2023	Q1 2024	Quarterly changes
Global percentage of attacked ICS computers	24.7%	24.4%	-0.3 pp
Percentage of ICS computers on which malicious objects from different categories were blocked			
Denylisted internet resources	6.58%	6.84%	0.26 pp
Malicious scripts and phishing pages (JS and HTML)	7.61%	5.84%	-1.77 pp
Spy Trojans, backdoors and keyloggers	3.86%	3.90%	0.04 pp
Malicious documents (MSOffice + PDF)	2.02%	1.72%	-0.30 pp
Viruses	1.48%	1.56%	0.08 pp
Worms	1.55%	1.51%	-0.04 pp
Miners in the form of executable files for Windows	0.84%	0.92%	0.08 pp
Web miners running in browsers	0.45%	0.49%	0.04 pp
Malware for AutoCAD	0.36%	0.41%	0.05 pp
Ransomware	0.17%	0.15%	-0.02 pp
Main threat sources			
Internet	13.25%	12.24%	-1.01 pp
Email clients	3.15%	3.04%	-0.11 pp
Removable media	1.29%	1.13%	-0.16 pp
Network folders	0.17%	0.15%	-0.02 pp

Statistics across all threats

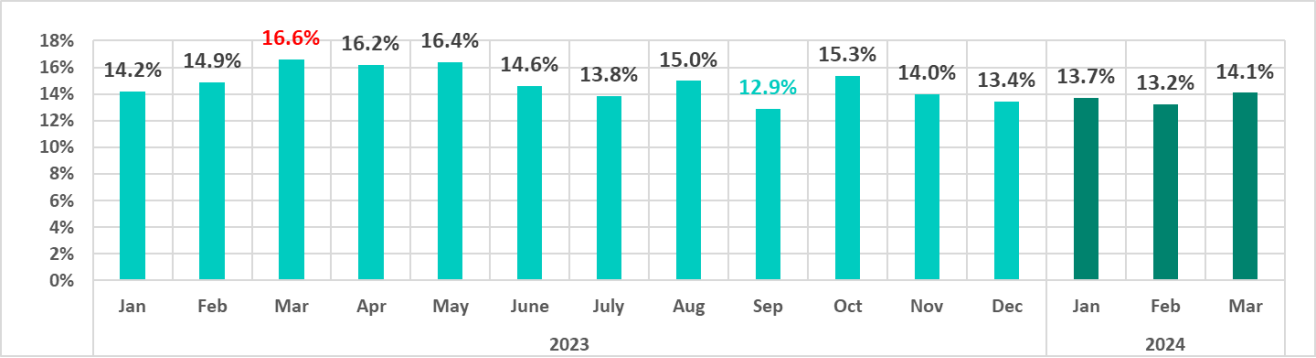
In the first quarter of 2024, the percentage of ICS computers on which malicious objects were blocked decreased by 0.3 pp from the previous quarter to 24.4%.

Compared to the first quarter of 2023, the percentage decreased by 1.3 pp.

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

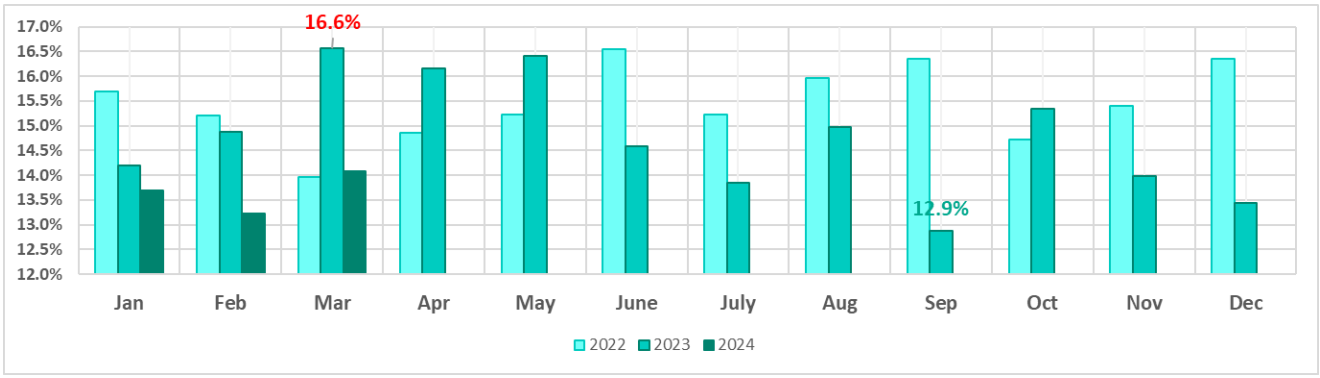


The percentage of ICS computers on which malicious objects were blocked in the first quarter of 2024 was highest in March and lowest in February.



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

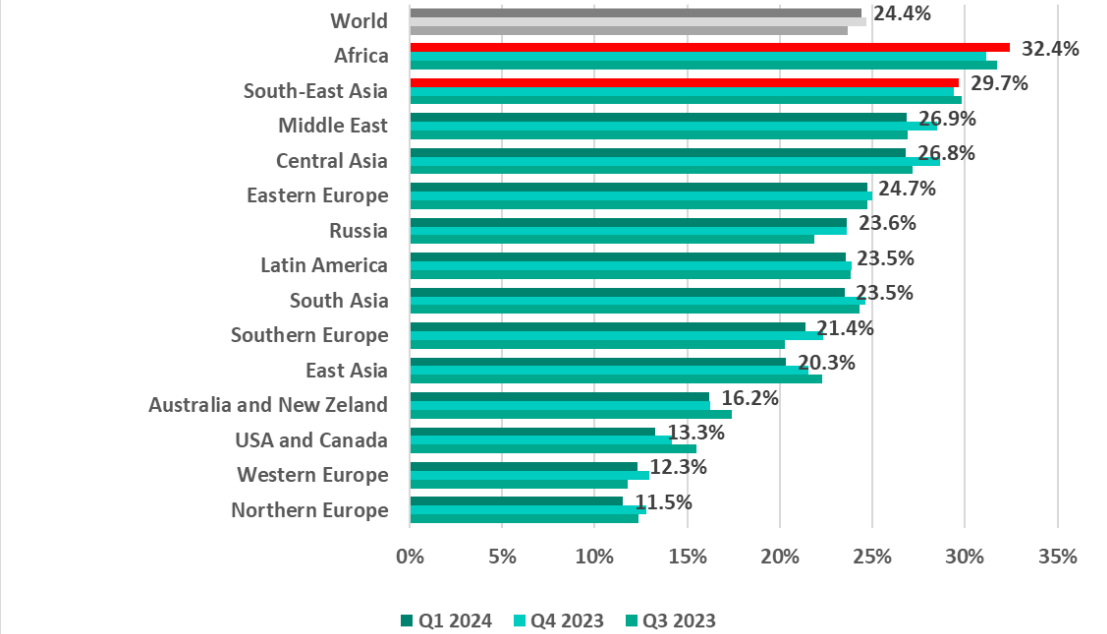
The percentages for the first three months of 2024 are significantly lower than those for the first three months of the previous year (2023).



Percentage of ICS computers on which malicious objects were blocked, by month, 2021–2024

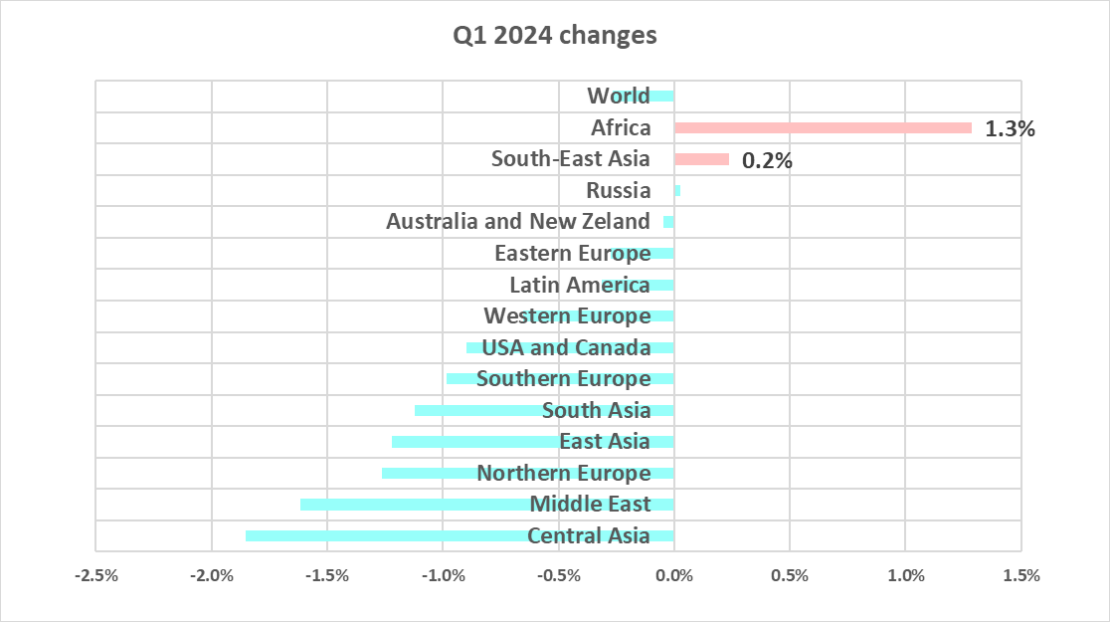
Regionally, the percentage of ICS computers that blocked malicious objects during the quarter ranged from 32.4% in Africa to 11.5% in Northern Europe.

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



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

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

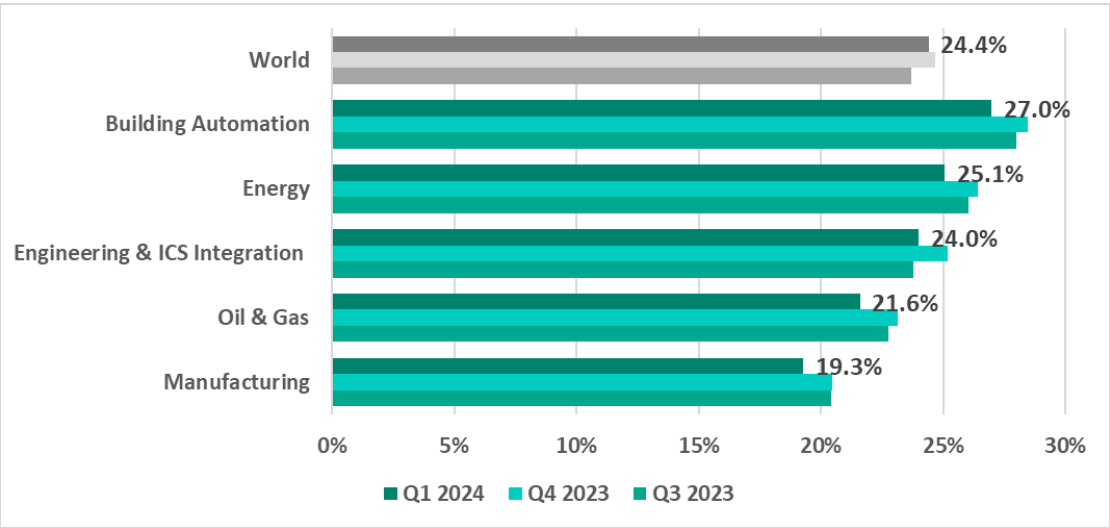


We discuss regional statistics in more detail in our regional report.

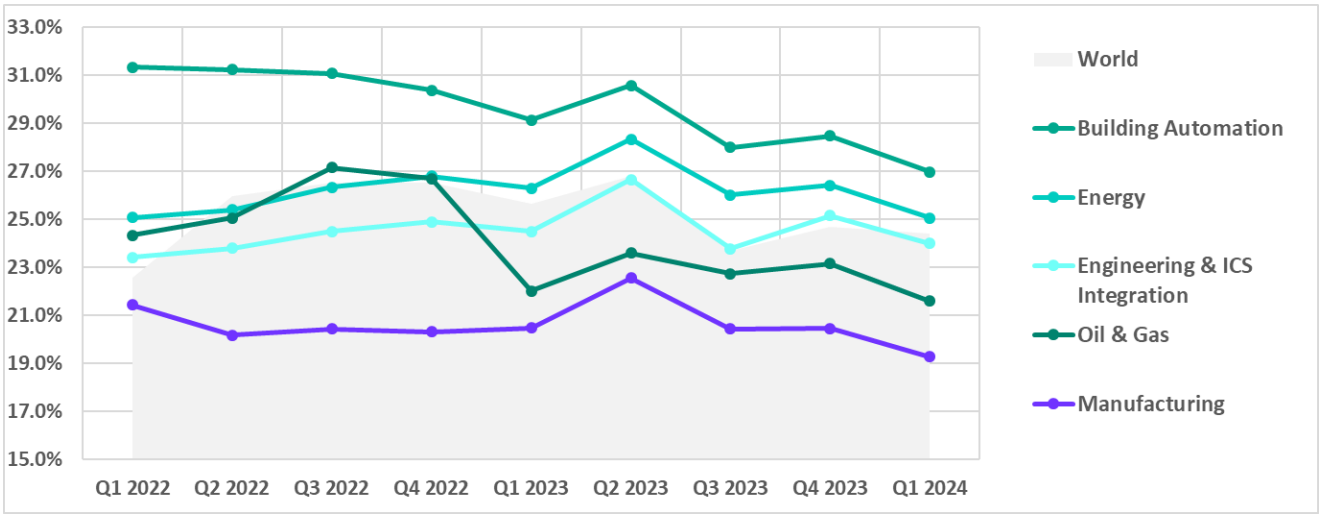
Selected industries

Building automation has traditionally led the surveyed industries in terms of the percentage of ICS computers on which malicious objects were blocked.

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



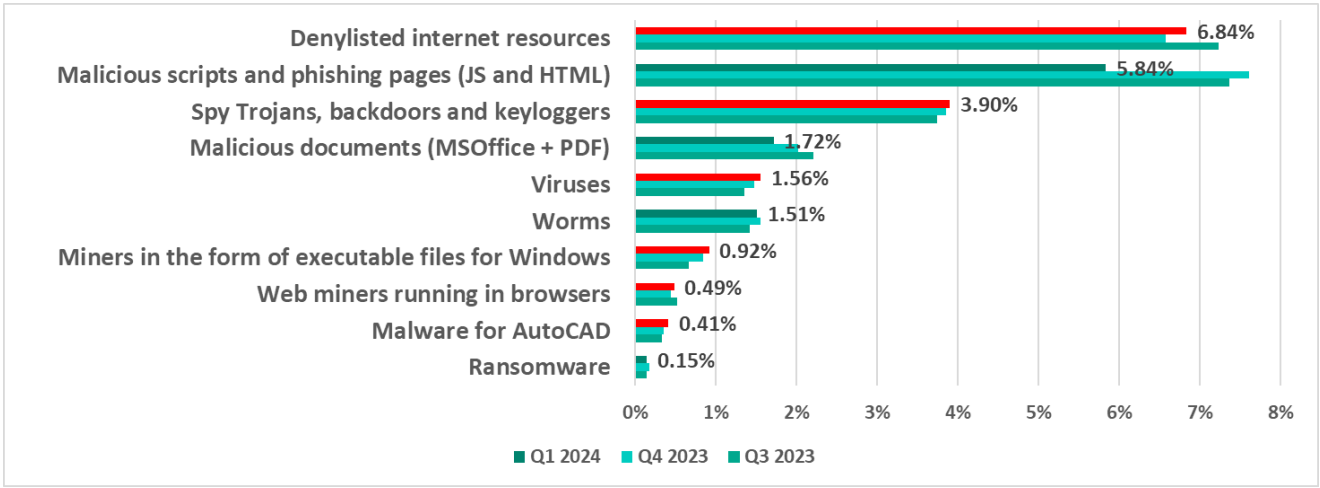
In the first quarter of 2024, the percentage of ICS machines that blocked malicious objects decreased across all industries.



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

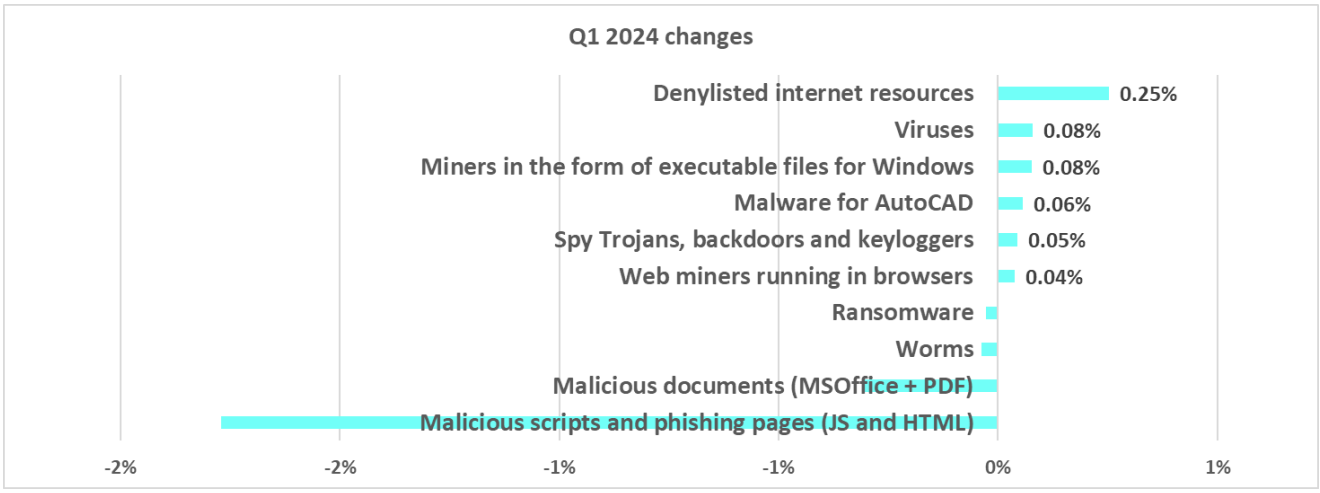
Diversity of detected malware

In the first quarter of 2024, Kaspersky's protection solutions blocked malware from 10,865 different malware families of various categories on industrial automation systems.



Percentage of ICS* computers on which the activity of malicious objects of various categories was prevented

*Note that it would not be appropriate to sum up the percentages, as in many cases, more than one threat type could be blocked on one computer in the period under review.



Change in percentage of ICS computers blocked by various categories of malicious objects in Q1 2024

Compared to the previous quarter, in the first quarter of 2024, the most significant increase in the percentage of ICS computers on which malicious objects of various categories were blocked was as follows:

- AutoCAD malware – by 1.16 times.

Malicious object categories

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
2. Next-stage malware
3. Self-propagating malware

Malicious objects used for initial infection

Malicious objects used for initial infection include dangerous web resources, malicious scripts, and malicious documents.

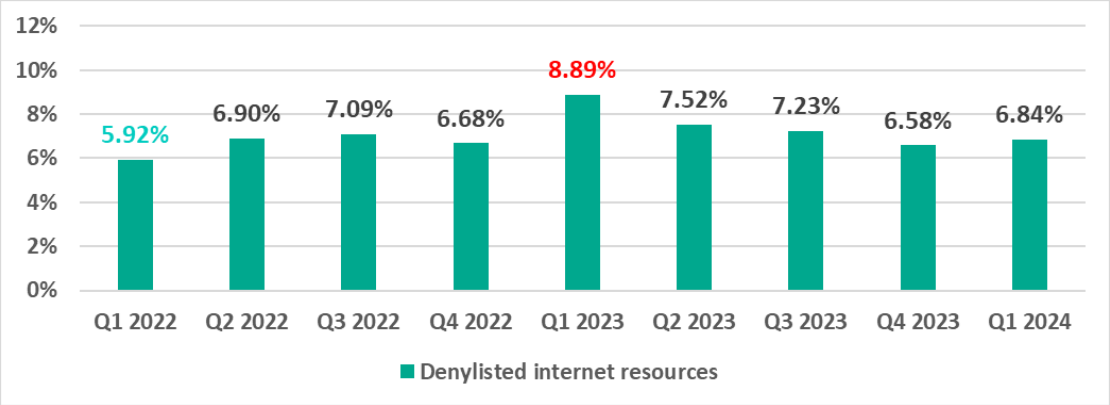
Dangerous web resources (denylisted internet resources) are associated with malware spread or control. A significant percentage of these resources is used for spreading malicious scripts and phishing pages (HTML).

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.

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.

Denylisted internet resources

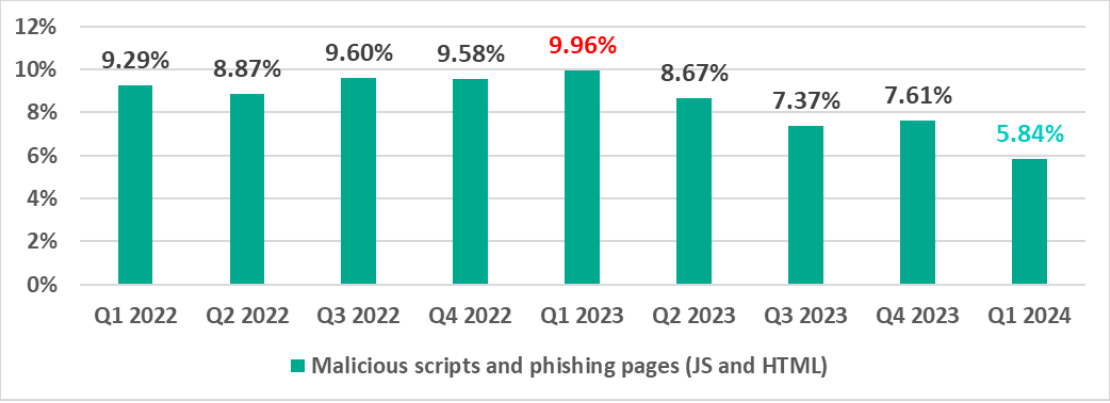
Denylisted internet resources are associated with malware spread or control. A significant percentage of these resources is used for spreading malicious scripts and phishing pages (HTML).



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.

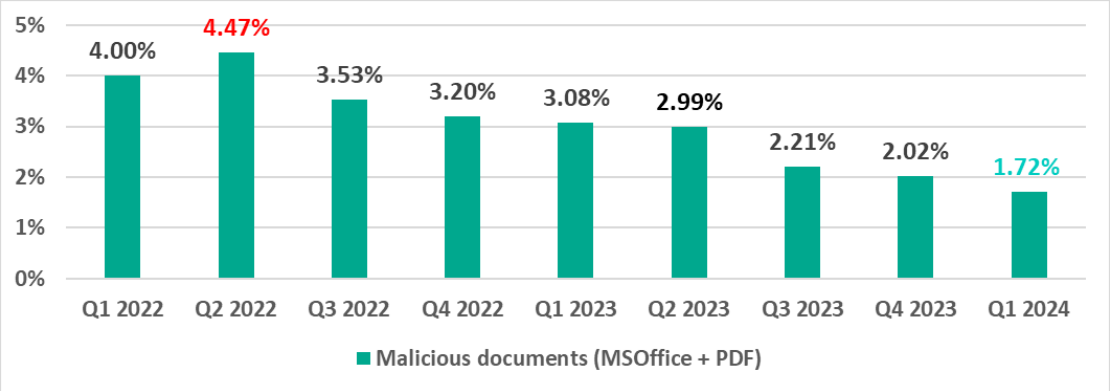
In the first quarter of 2024, the percentage of ICS computers on which malicious scripts and phishing sites were blocked was the lowest since 2022.



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.

The percentage of ICS computers with malicious documents on them peaked in the second quarter of 2022 and has been declining since then.



Next-stage malware

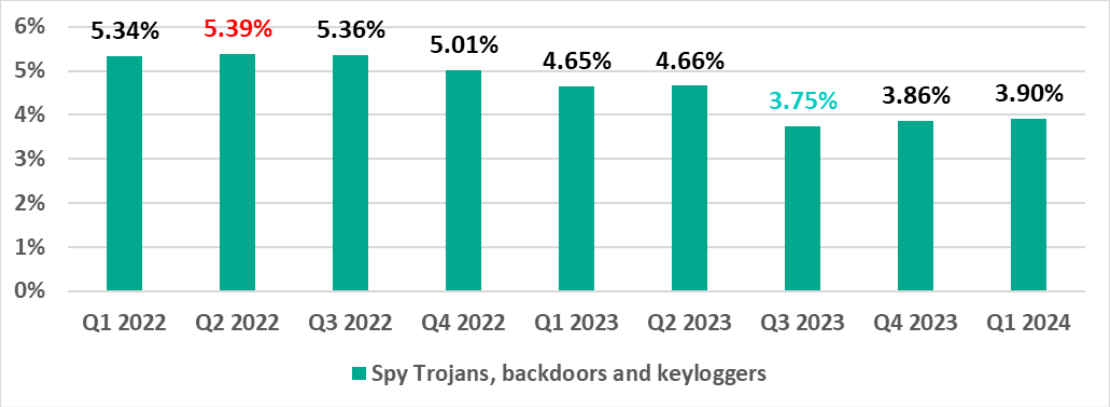
Malicious objects used to initially infect computers deliver next-stage malware – spyware, ransomware, and miners – to victims' computers. As a rule, the higher the percentage of ICS computers on which the initial infection malware is blocked, the higher the percentage for next-stage malware.

Spyware

Spyware (spy Trojans, backdoors, and keyloggers) can be found in lots of phishing email 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.

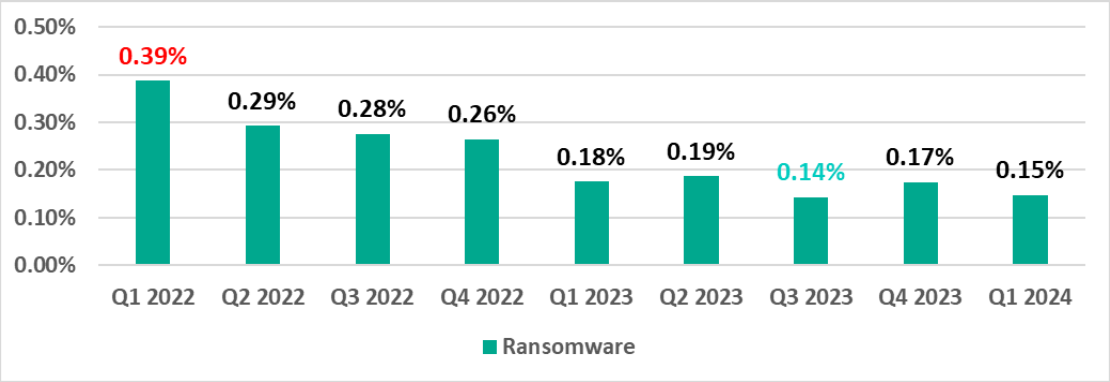
Spyware is also used to steal the information needed to deliver other types of malware, such as ransomware and silent miners, as well as to prepare for targeted attacks.

The percentage of ICS computers on which spyware was blocked was lowest in the third quarter of 2023, and has increased slightly over the past two quarters.

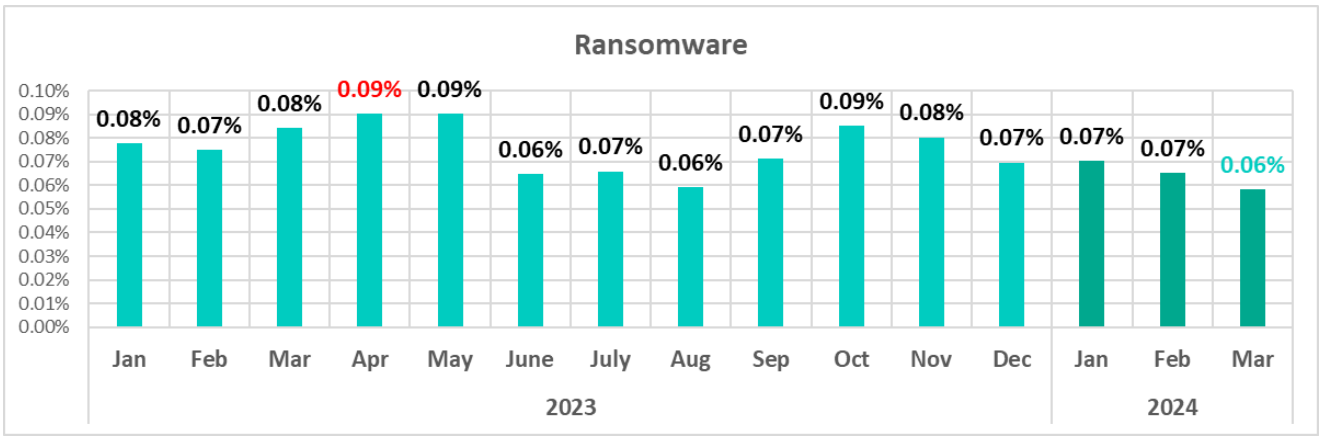


Ransomware

The percentage of ICS computers on which ransomware was blocked varies from quarter to quarter within 0.3 pp.



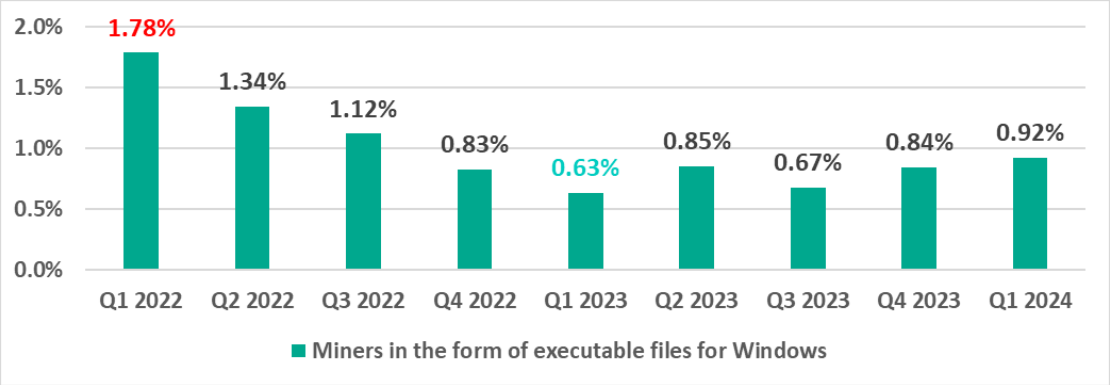
As the graph below shows, the ransomware rate has been declining since November 2023.



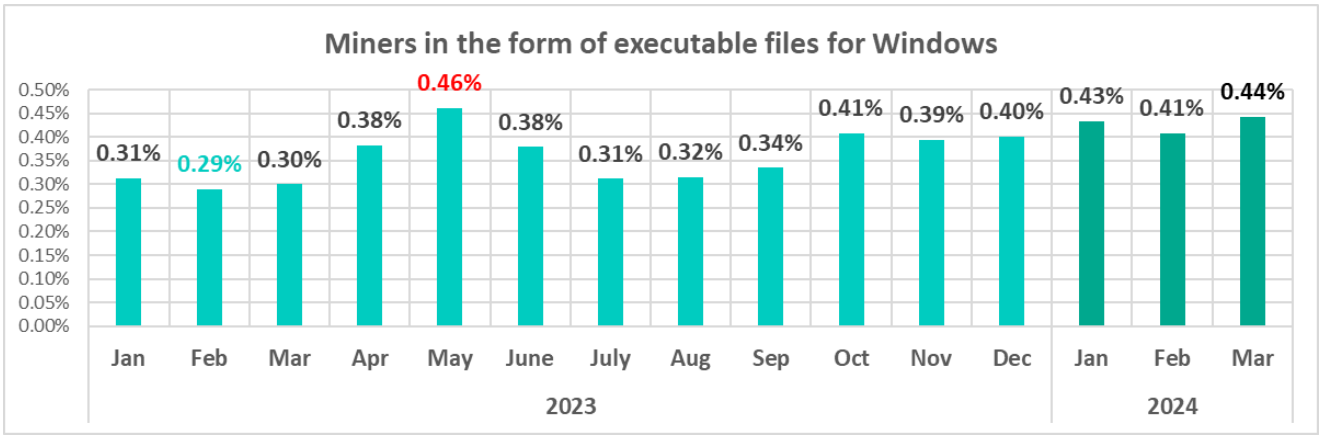
Miners in the form of executable files for Windows

The percentage of ICS computers on which miners in the form of executable files for Windows are blocked was at a minimum in the first quarter of 2023. It has been increasing since the second quarter of 2023, and compared to the first quarter of 2023, it has increased 1.5 times.

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

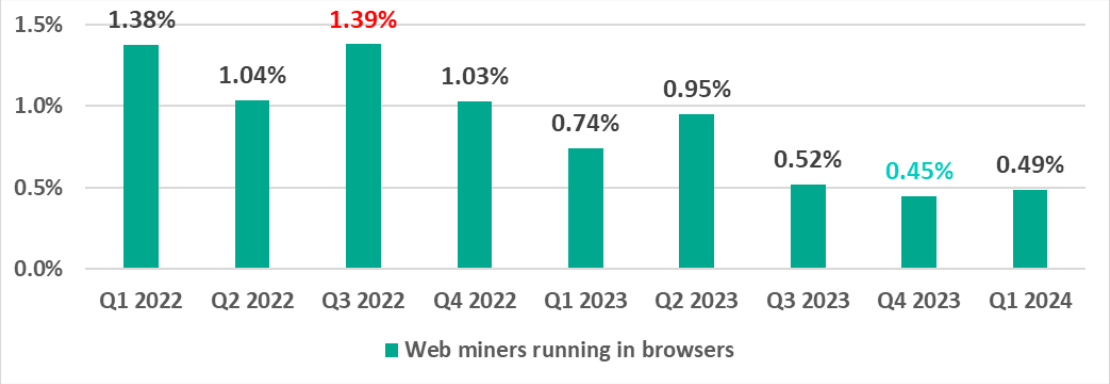


Since October 2023, the percentage of ICS computers on which miners in the form of executable files for Windows have been blocked has been higher than any other month of 2023 except May.



Web miners

The percentage of ICS computers on which web miners were blocked was lowest in the last quarter of 2023 and increased slightly in the first quarter of 2024.



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.

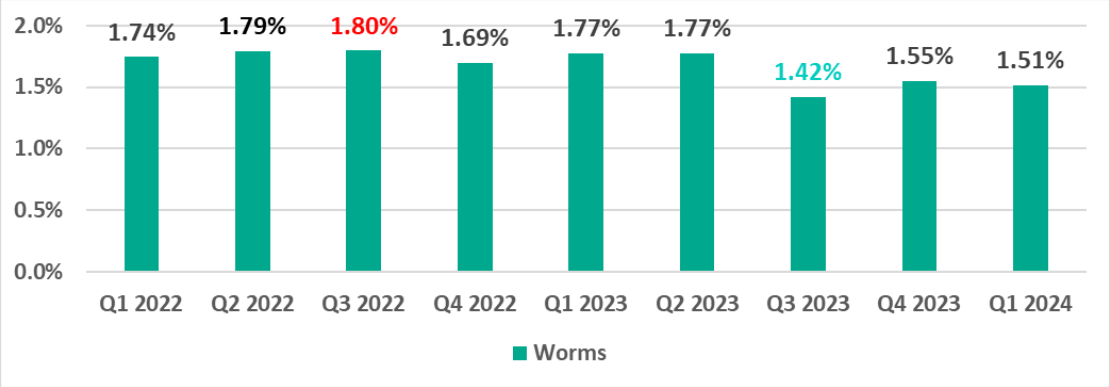
To spread across ICS networks, **viruses and worms** rely on removable media, network folders, infected files including backups, and network attacks on outdated software, such as Radmin2.

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.

New worm versions used by malicious actors for spreading spyware, ransomware, and miners can be found on ICS networks as well. More often than not, 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 boot-forcing.

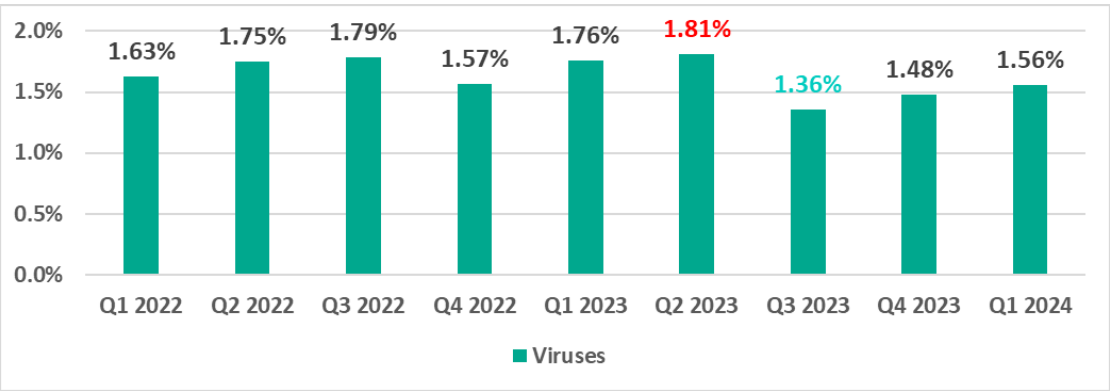
Globally, the percentage of ICS computers on which viruses and worms were blocked has slowly increased from a low in the third quarter of 2023.

Worms



Viruses

The percentage of ICS computers on which viruses were blocked is increasing after a low point in the third quarter of 2023, but has not yet exceeded the levels seen in 2022 and the first two quarters of 2023.

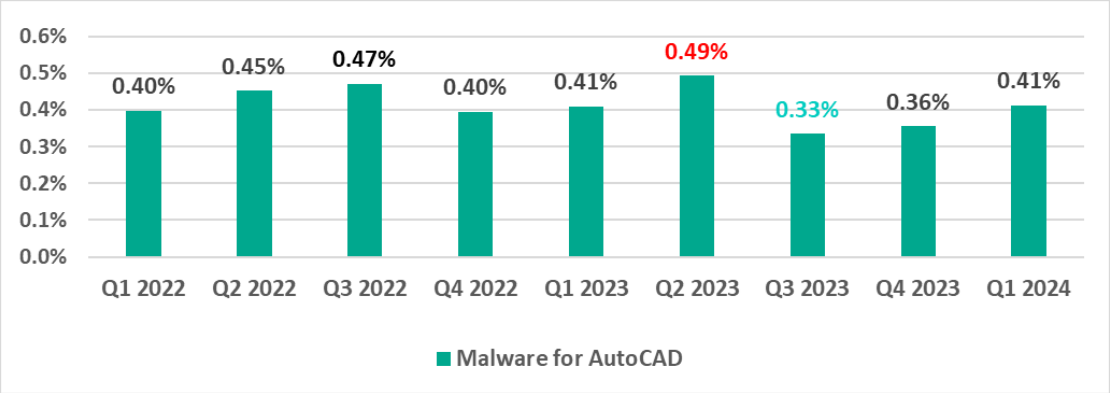


AutoCAD malware

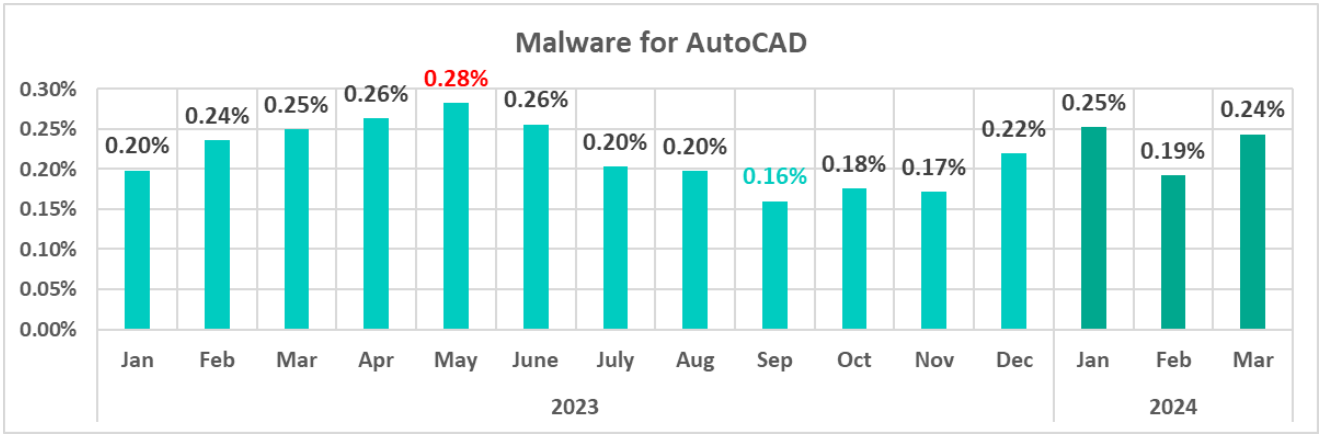
This category of malware can spread in a variety of ways, so it does not belong to a specific group.

It 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 first quarter of 2024, the percentage of ICS computers on which AutoCAD malware was blocked increased by a factor of 1.16.



In the first three months of 2024, the percentage of miners was close to its mid-2023 peak.

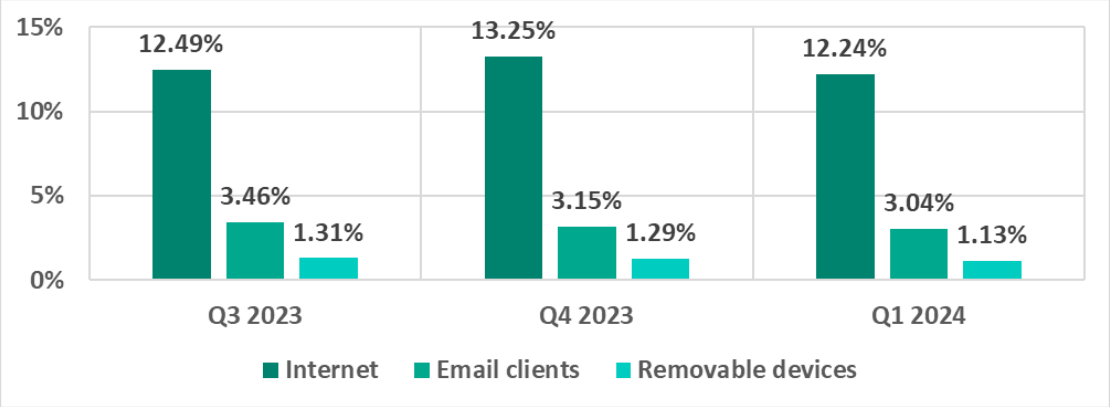


Main threat sources

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.)

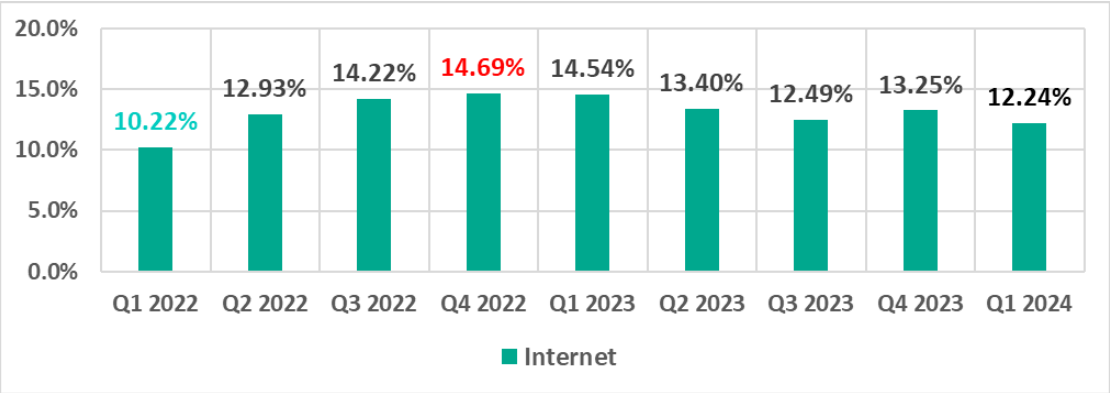
In the first quarter of 2024, the percentage of ICS computers on which threats from various sources were blocked decreased for all major threat sources.

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

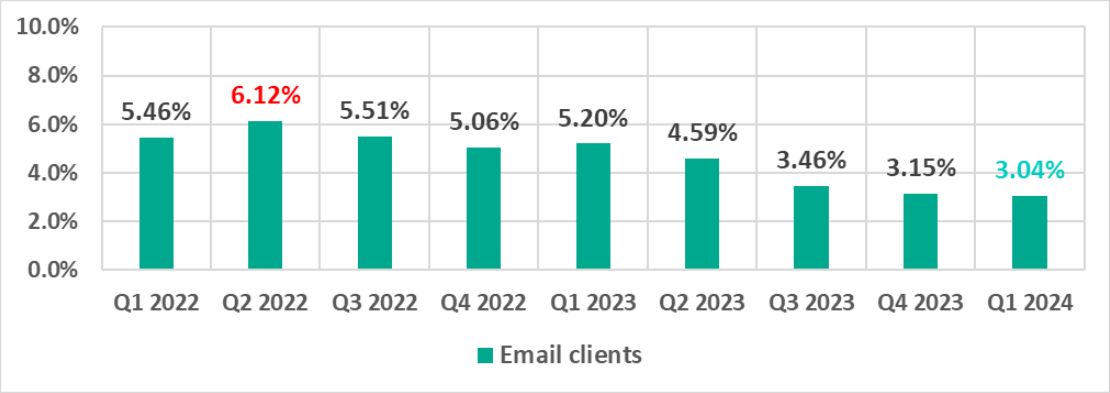


The first quarter of 2024 saw the lowest quarterly percentage since 2022 for threats from email and threats distributed on removable media. The last time the percentage was lower for the internet was two years ago, in the first quarter of 2022.

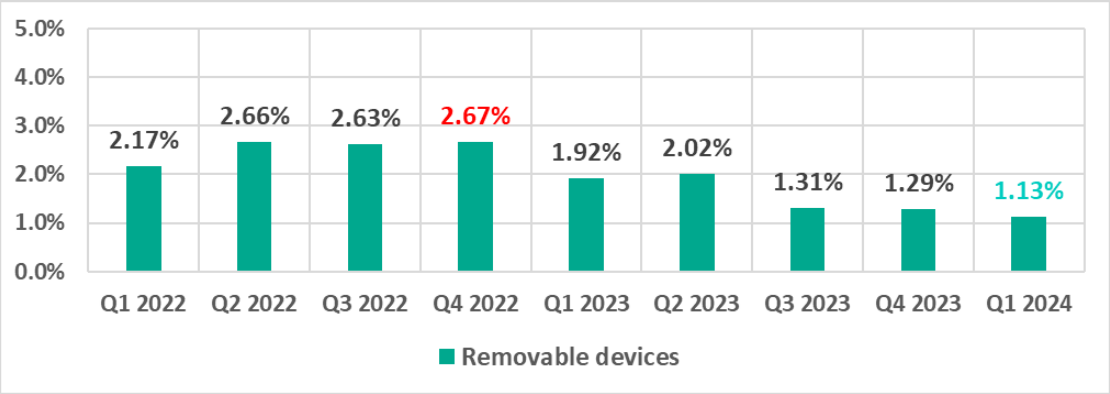
Internet



Email clients

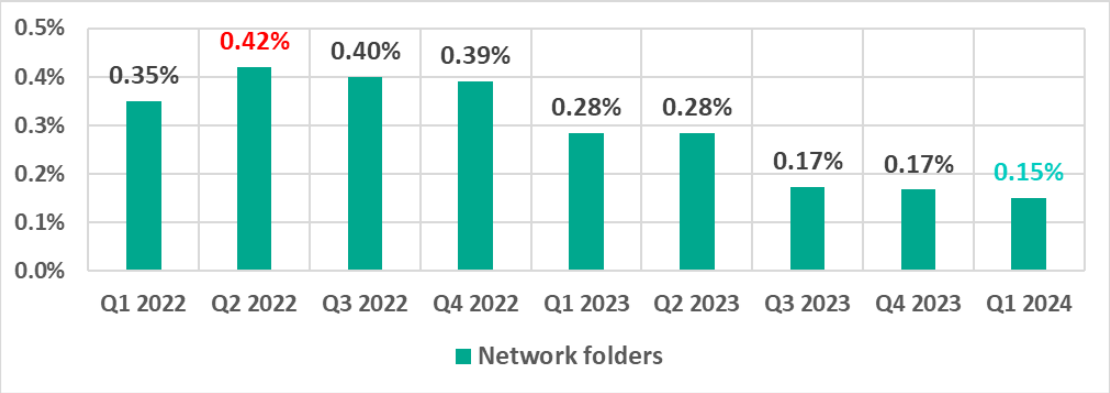


Removable media



Network folders

Network folders are a minor source of threats. The percentage of ICS computers on which network folder threats were blocked was also the lowest since 2022.



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 had 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[1].

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

- Supervisory control and data acquisition (SCADA) servers
- Data storage (Historian) servers
- Data gateways (OPC)
- Stationary workstations of engineers and operators
- Mobile workstations of engineers and operators
- Human machine interface (HMI)
- OT network administration computers
- ICS software development computers

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.

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

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