Kaspersky ICS CERT

Threat landscape for industrial automation systems

Q2 2024

26.09.2024

Version 1.0

Q2 in numbers

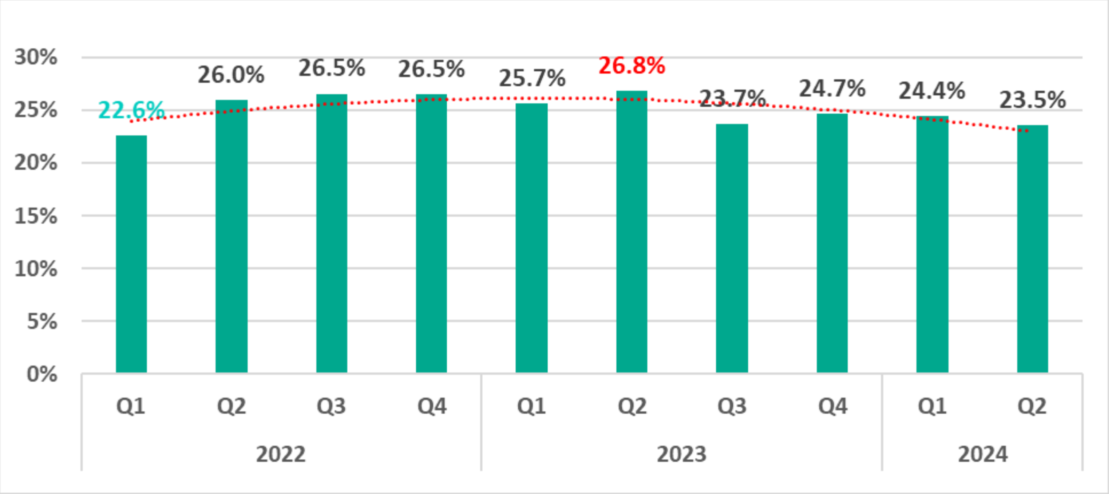
Parameter	Q1 2024	Q2 2024	Quarterly changes
Global percentage of attacked ICS computers	24.4%	23.5%	-0.9 pp
Percentage of ICS computers on which malicious objects from different categories were blocked			
Denylisted internet resources	6.84%	6.63%	-0.21 pp
Malicious scripts and phishing pages (JS and HTML)	5.84%	5.69%	-0.15 pp
Spy Trojans, backdoors and keyloggers	3.90%	4.08%	0.18 pp
Malicious documents (MSOffice + PDF)	1.72%	1.96%	0.24 pp
Viruses	1.56%	1.54%	-0.02 pp
Worms	1.51%	1.48%	-0.03 pp
Miners in the form of executable files for Windows	0.92%	0.89%	-0.03 pp
Web miners running in browsers	0.49%	0.50%	0.01 pp
Malware for AutoCAD	0.41%	0.42%	0.01 pp
Ransomware	0.15%	0.18%	0.03 pp
Main threat sources			
Internet	12.24%	11.25%	-0.99 pp
Email clients	3.04%	3.04%	0 pp
Removable media	1.13%	0.92%	-0.21 pp
Network folders	0.15%	0.13%	-0.02 pp

Statistics across all threats

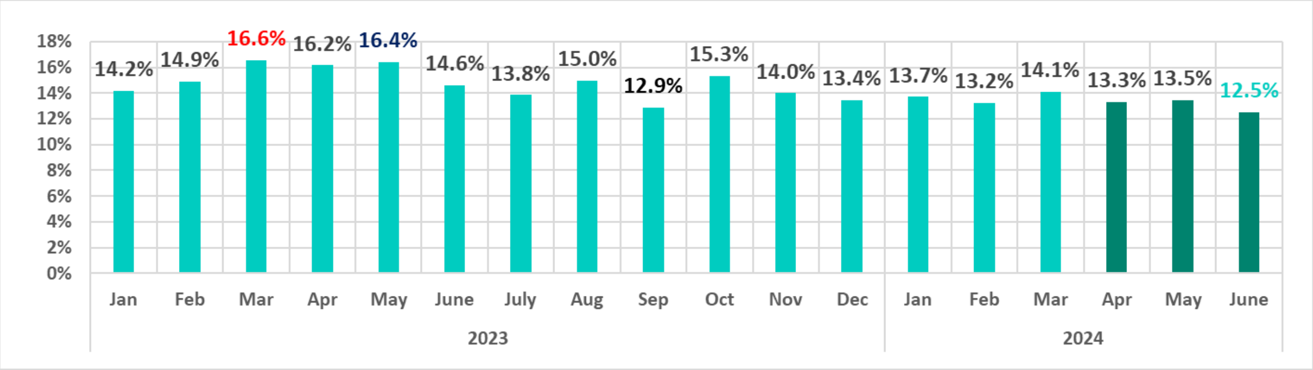
In the second quarter of 2024, the percentage of ICS computers on which malicious objects were blocked decreased by 0.9 pp from the previous quarter to 23.5%.

Compared to the second quarter of 2023, the percentage decreased by 3.3 pp.

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



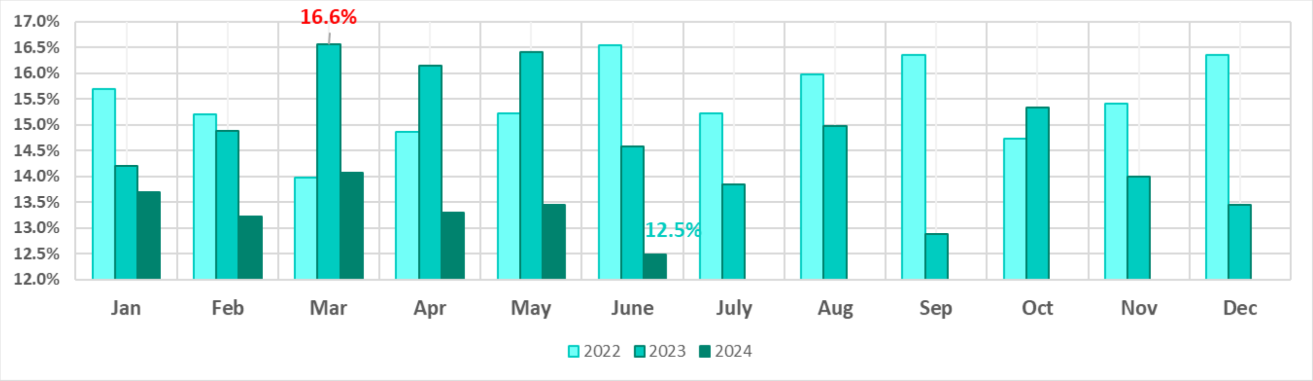
The percentage of ICS computers on which malicious objects were blocked in the second quarter of 2024 was highest in May and lowest in June.



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

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

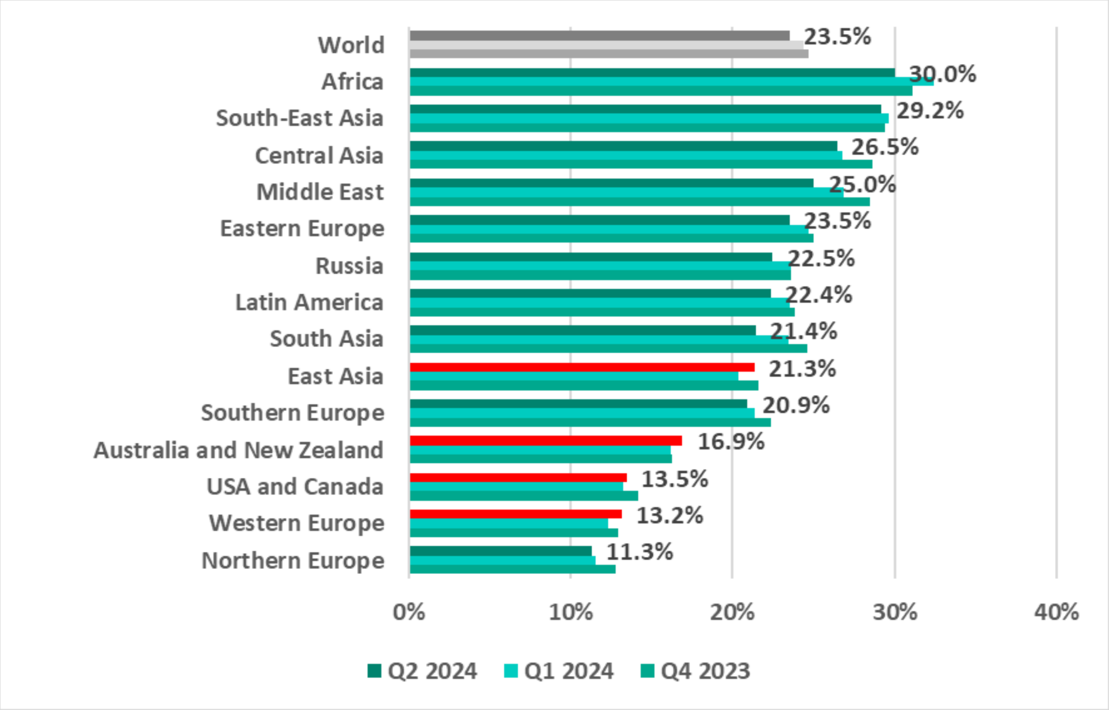
In fact, the percentage in June 2024 was the lowest for the period from 2022 to the end of the first half of 2024.



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

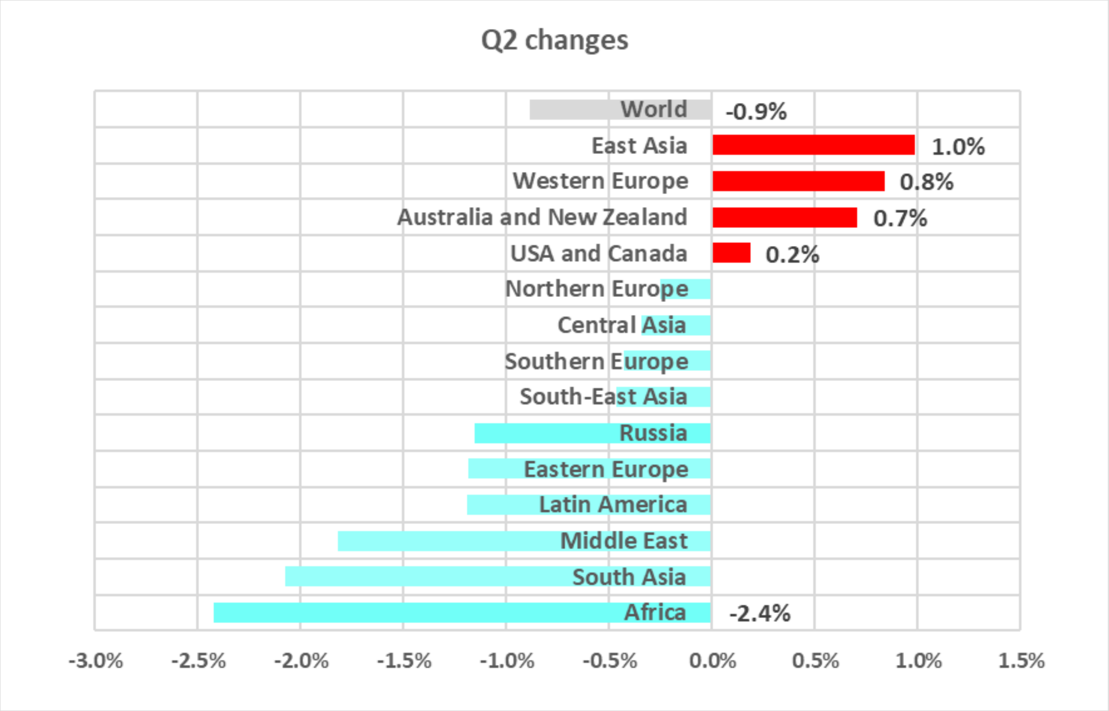
Regionally, the percentage of ICS computers that blocked malicious objects during the quarter ranged from 11.3% in Northern Europe to 30% in Africa.

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



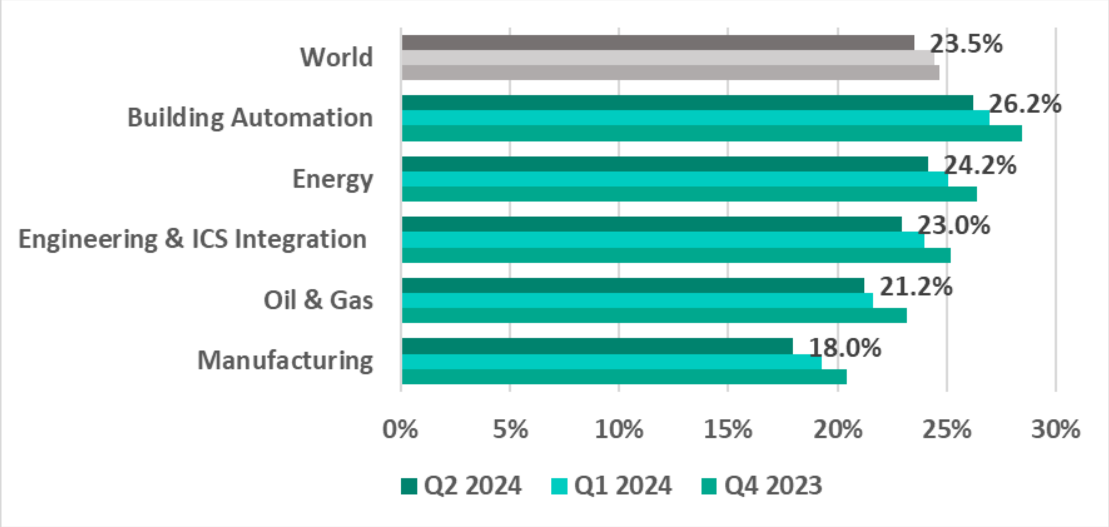
Four regions – East Asia; USA and Canada; Australia and New Zealand; and Western Europe – saw their percentages increase from the previous quarter.

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

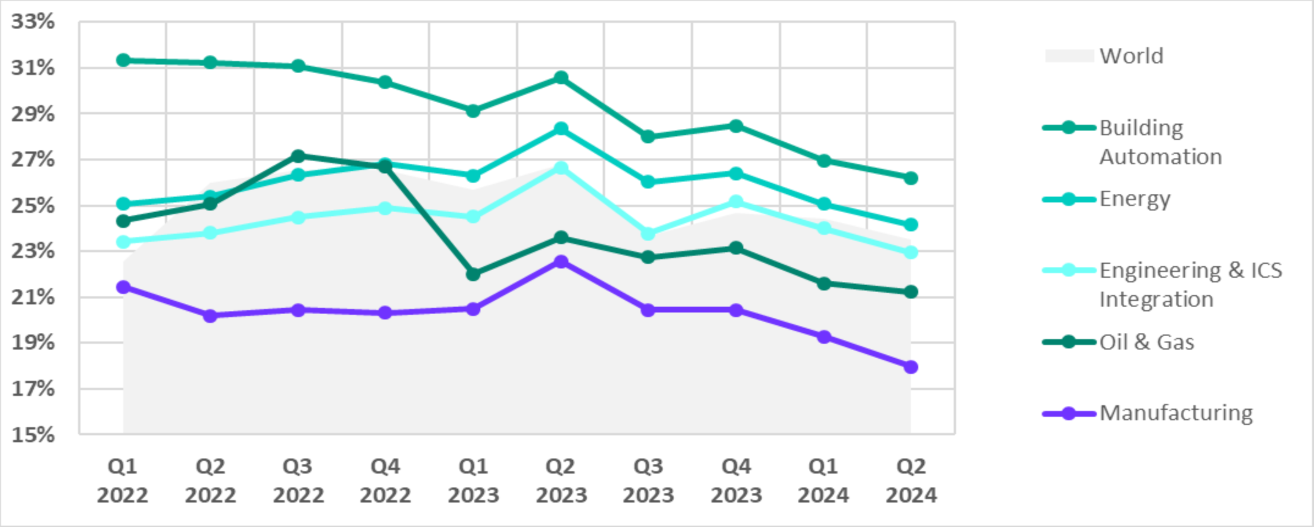


Selected industries

The building automation sector continued to lead the surveyed industries in terms of the percentage of ICS computers on which malicious objects were blocked.



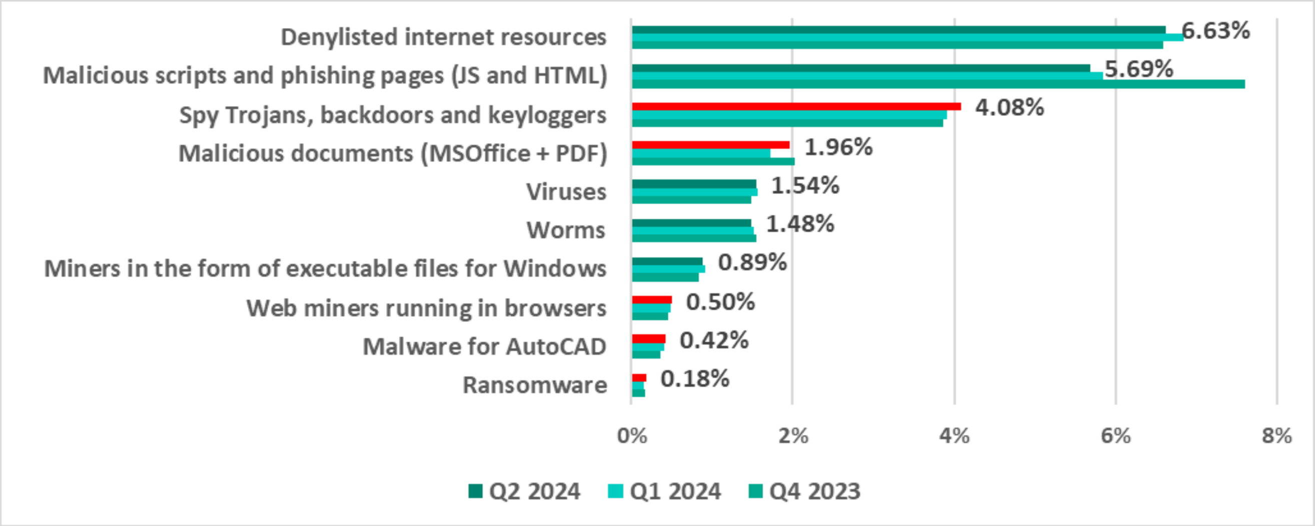
In the second quarter of 2024, the percentage of ICS computers on which malicious objects were blocked decreased across all industries.



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

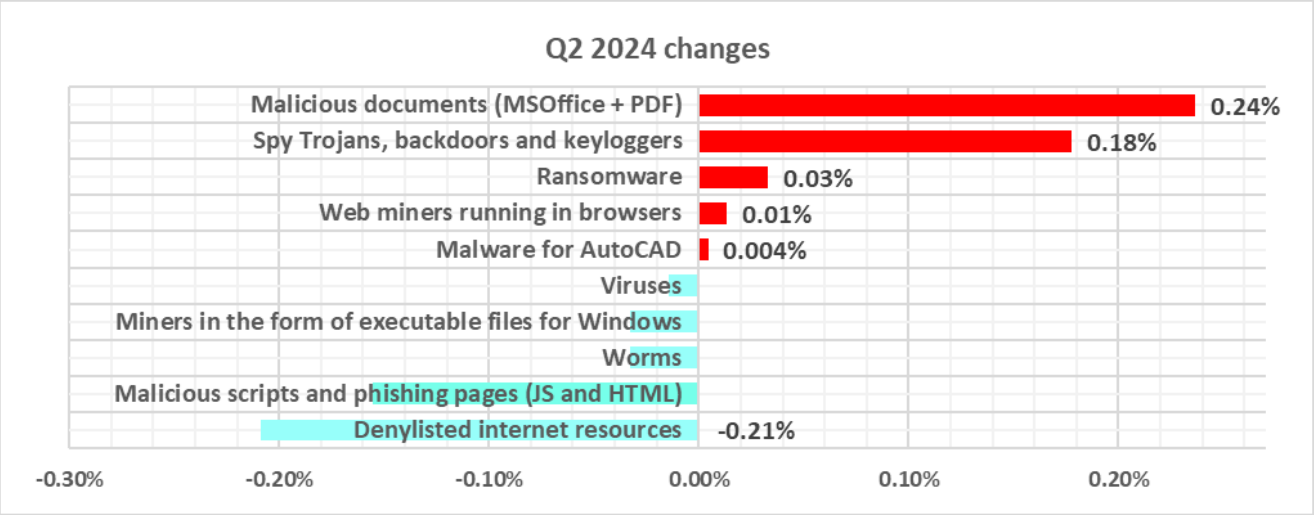
Diversity of detected malware

In the second quarter of 2024, Kaspersky's protection solutions blocked malware from 11,349 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 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 Q2 2024, compared to Q1 2024.

Compared to the previous quarter, the most noticeable proportional increase in the second quarter of 2024 was in the percentage of ICS computers on which **ransomware** was blocked – a 1.2-fold increase.

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:

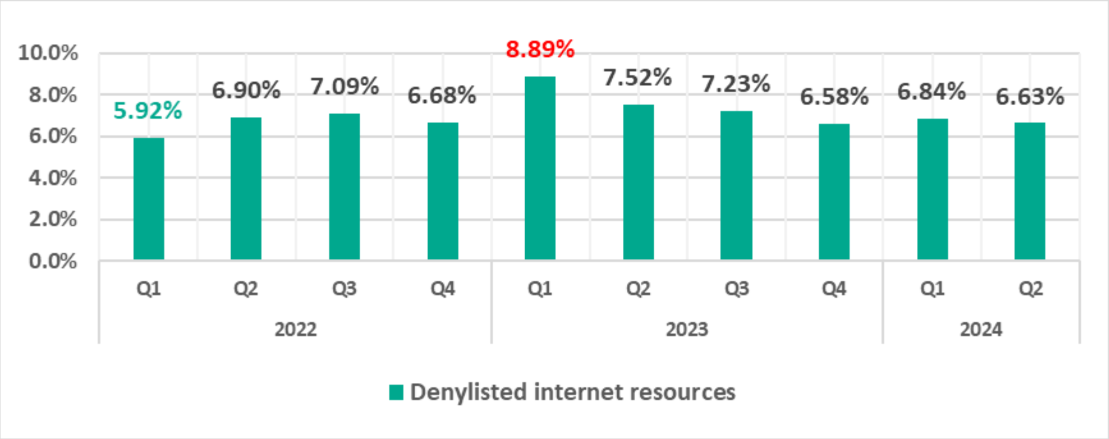
1. Malicious objects used for initial infection
2. Next-stage malware
3. Self-propagating malware

Malicious objects used for initial infection

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

Denylisted internet resources

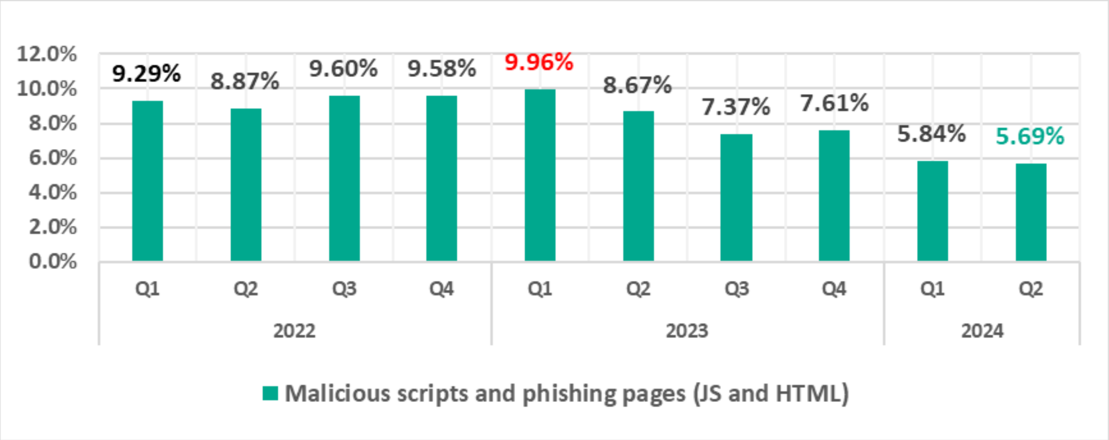
Denylisted internet resources are associated with malware spread or control. A significant percentage of these resources is used for spreading malicious scripts and phishing pages (HTML).



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.

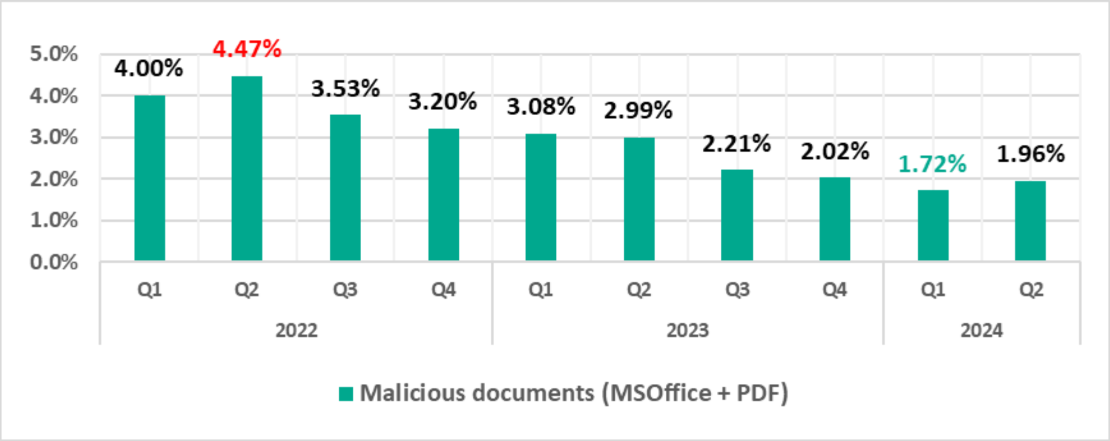
In the second quarter of 2024, the percentage of ICS computers on which malicious scripts and phishing sites were blocked continued to decrease and was the lowest since 2022.



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 then steadily declined until an increase in the second quarter of 2024.



Next-stage malware

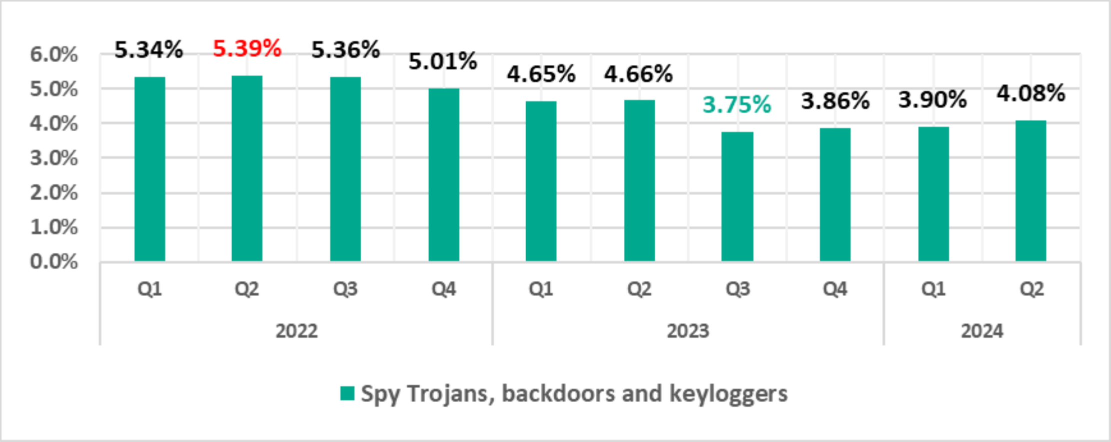
Malicious objects used to initially infect computers deliver next-stage malware – spyware, ransomware, and miners – to victims' computers. As a rule, the higher the percentage of ICS computers on which the initial infection malware is blocked, the higher the percentage for next-stage malware.

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.

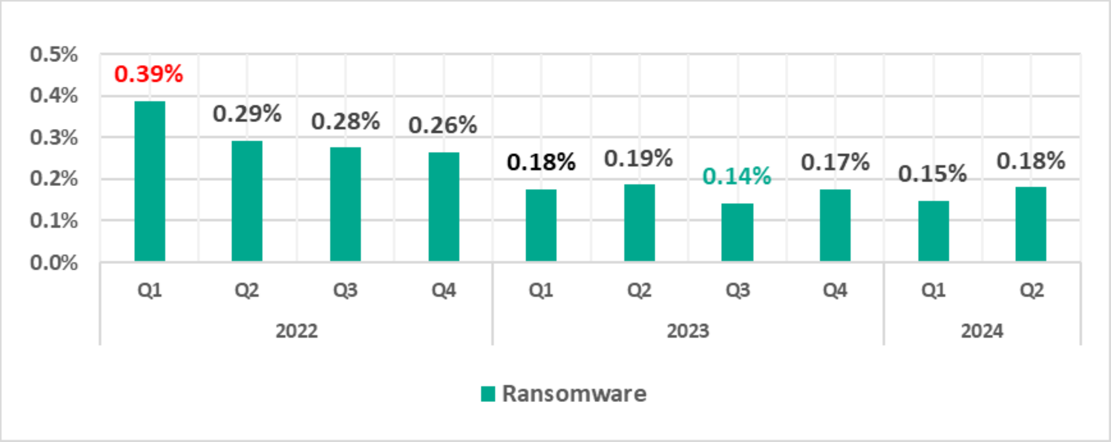
Spyware is also used to steal the information needed to deliver other types of malware, such as ransomware and silent miners, as well as to prepare for targeted attacks.

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 three quarters.

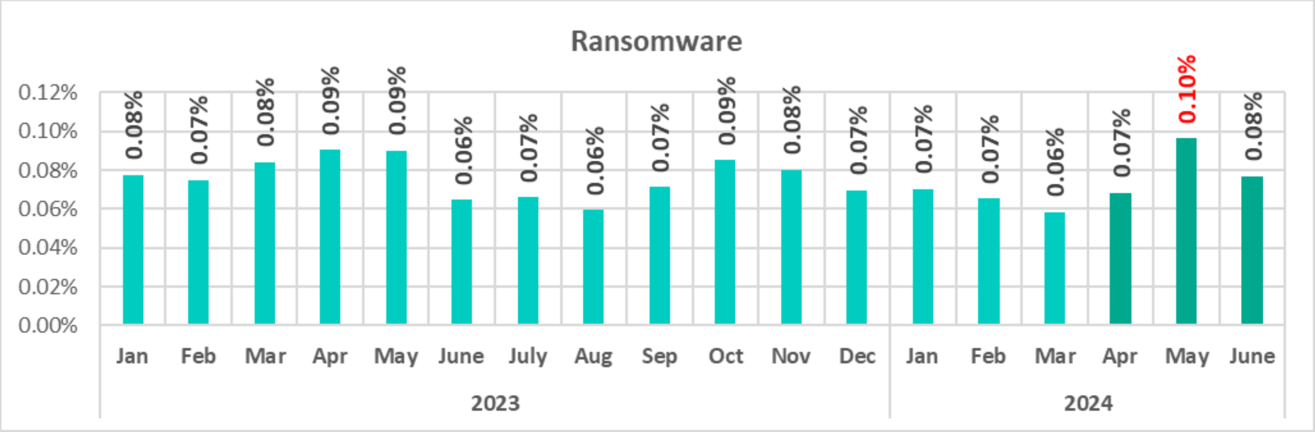


Ransomware

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



As the graph below shows, the ransomware rate alternated significantly during the months of the second quarter, reaching its highest value since early 2023 in May 2024.



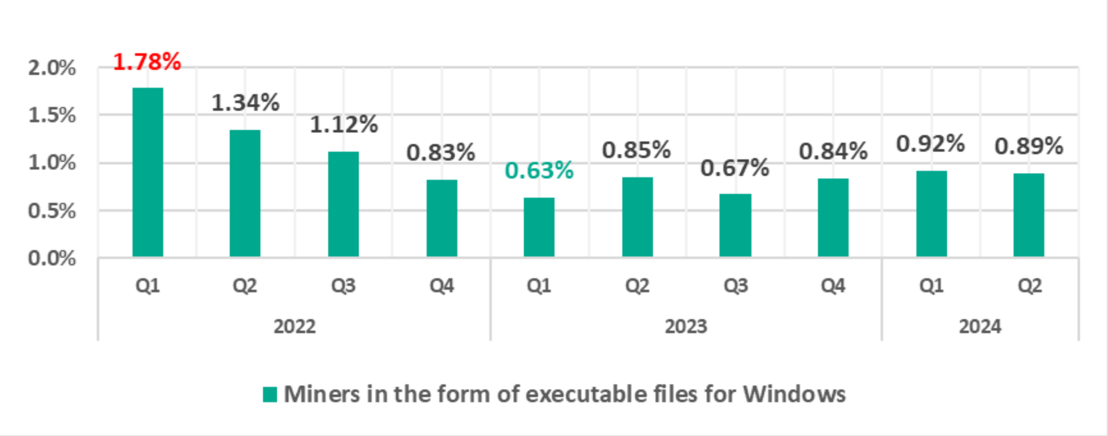
Miners in the form of executable files for Windows

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.

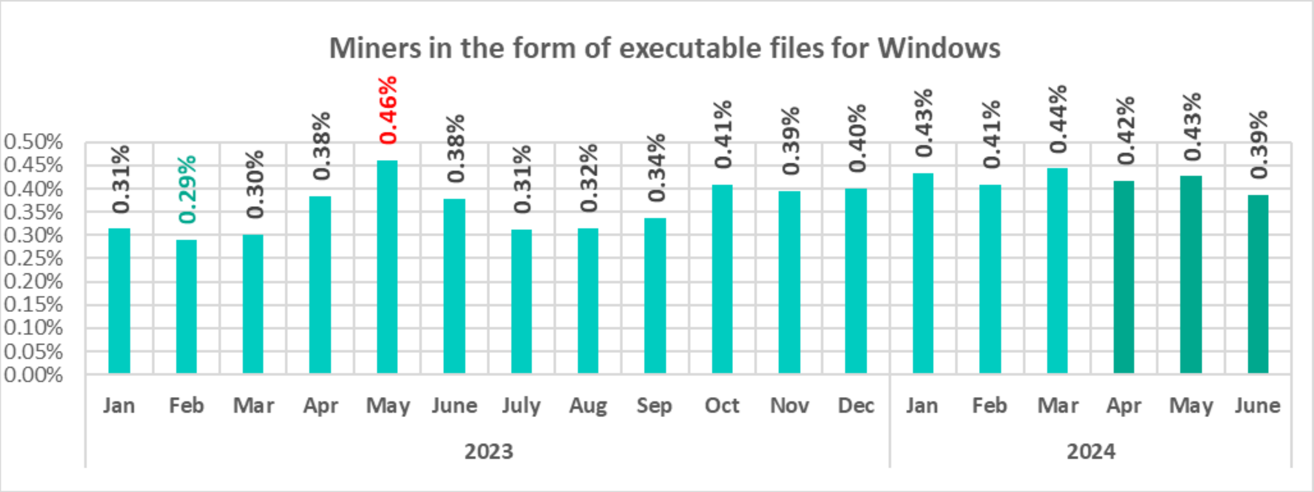
In addition to “classic” miners – applications written in .Net, C++, or Python and designed for hidden crypto mining – new forms are emerging. Popular "fileless" execution techniques continue to be adopted by various threat actors, including those implanting crypto miners on OT machines.

In the second quarter of 2024, 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 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.

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.

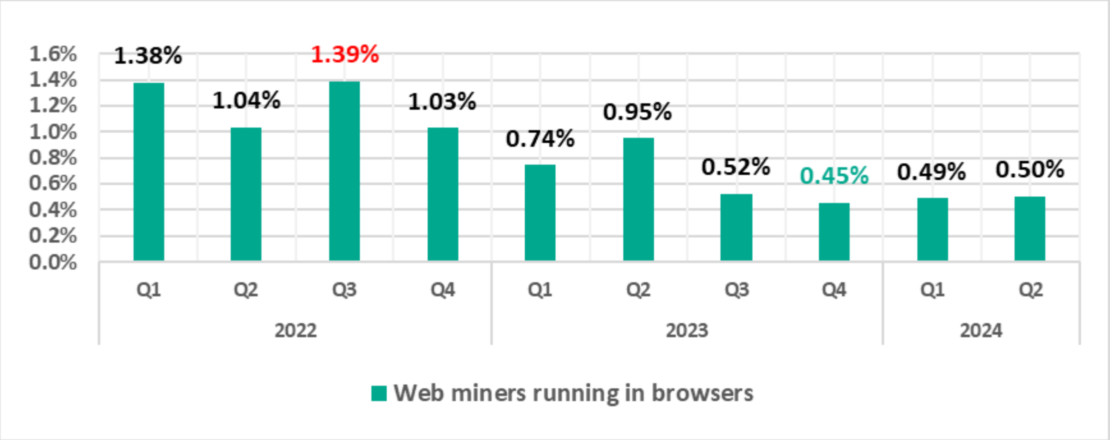


Since October 2023, the percentage of ICS computers on which miners in the form of executable files for Windows have been blocked remains higher than any other month in 2023 except May.



Web miners

The percentage of ICS computers on which web miners were blocked continued to increase slightly in the second 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.

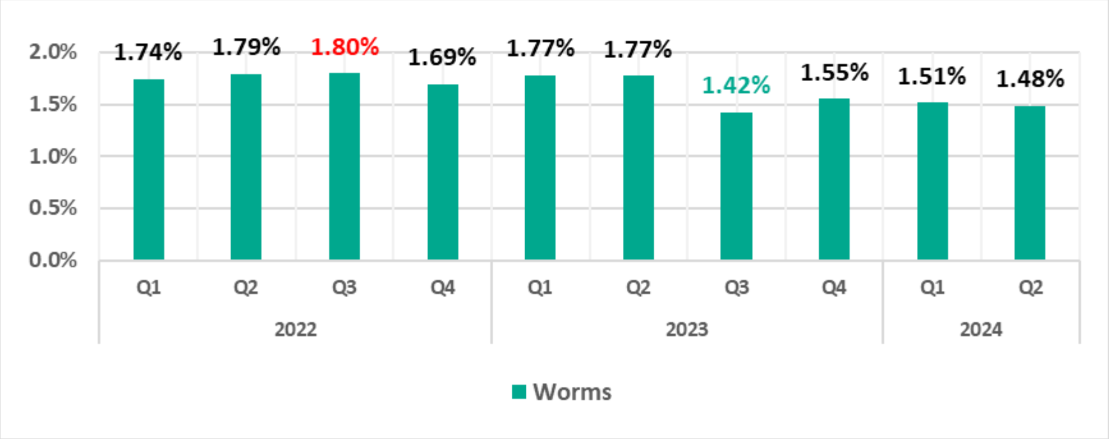
A lot of those still spreading are legacy viruses and worms whose command-and-control servers have been shut down. However, these types of malware can compromise infected systems by opening network ports or changing configurations, cause software failures, denial of service, and so on.

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

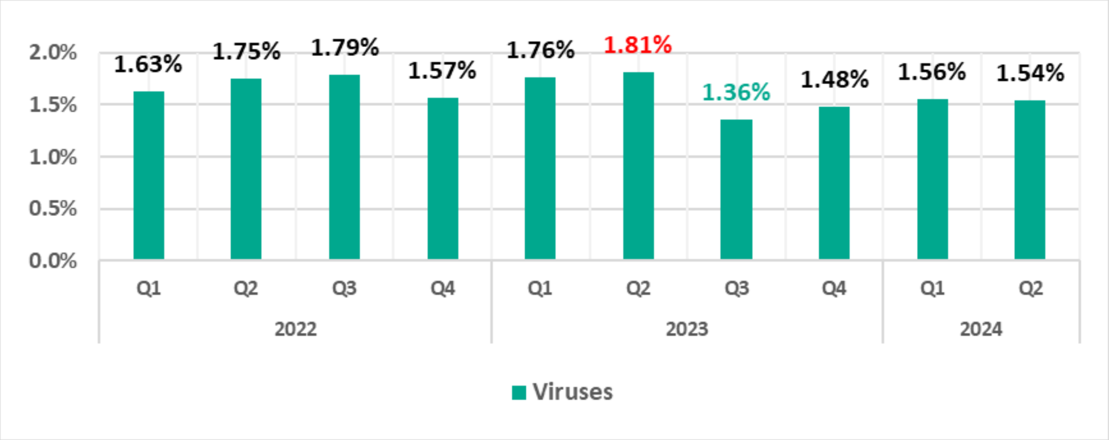
New worm versions used by malicious actors to spread spyware, ransomware, and miners can also be found on ICS networks. In most cases, they rely on network service (e.g., SMB or RDP) exploits that have been addressed by the vendors but still persist on OT networks, previously stolen credentials, or password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

The percentage of ICS computers on which worms were blocked continued to decrease in the second quarter of 2024.



Viruses

The percentage of ICS computers on which viruses were blocked decreased slightly in the second quarter of 2024.

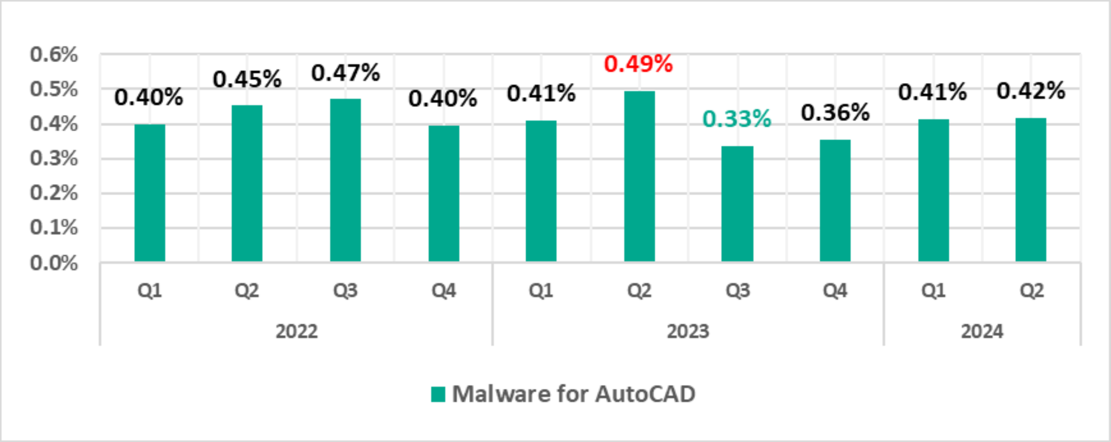


AutoCAD malware

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 second quarter of 2024, the percentage of ICS computers on which AutoCAD malware was blocked showed a slight increase.

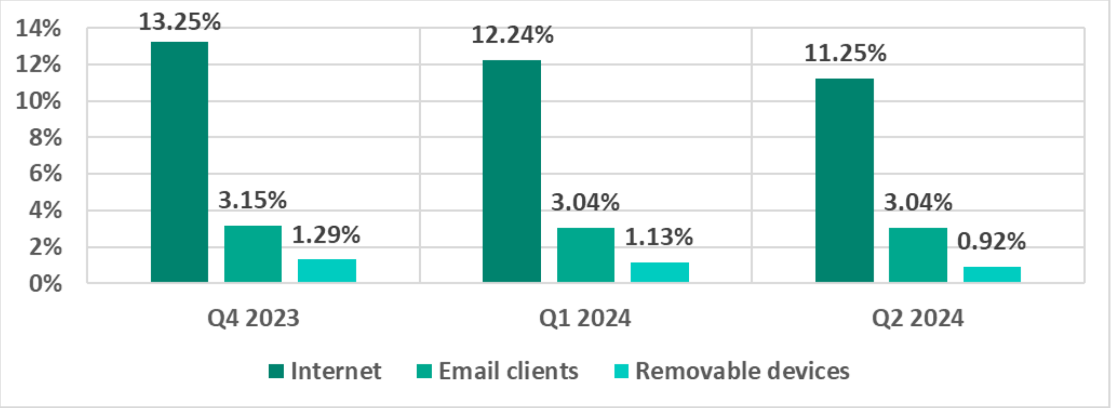


Main threat sources

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.)

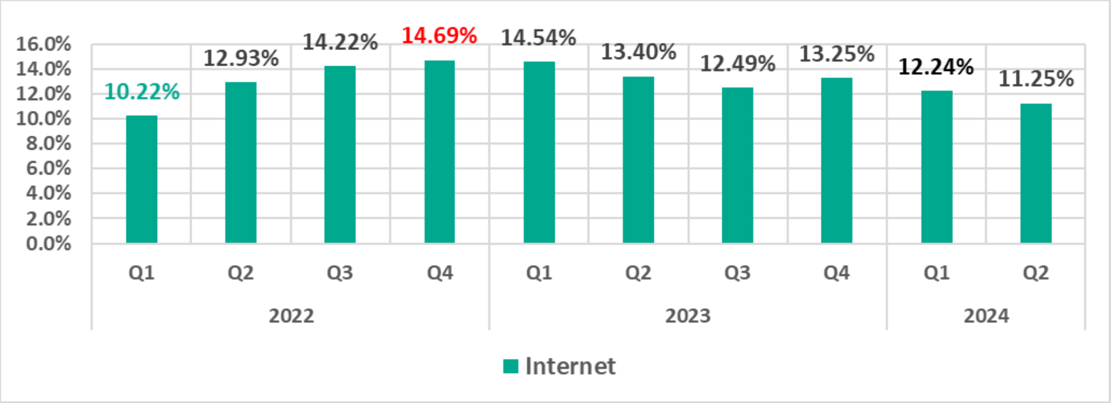
In the second quarter of 2024, the percentage of ICS computers on which threats from various sources were blocked decreased for the internet and removable devices.

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

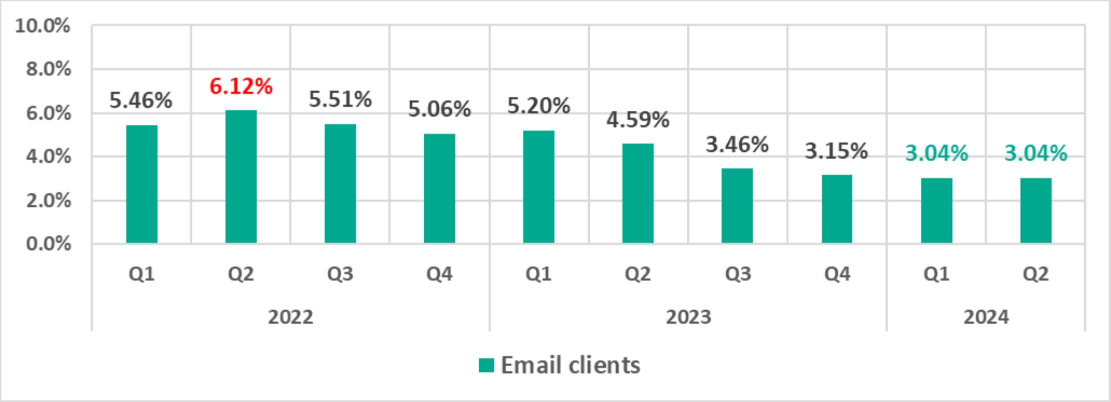


The second quarter of 2024, similar to the first quarter, saw the lowest quarterly percentage of threats from email and threats distributed on removable media since 2022. The last time the percentage was lower for the internet was two years ago, in the first quarter of 2022.

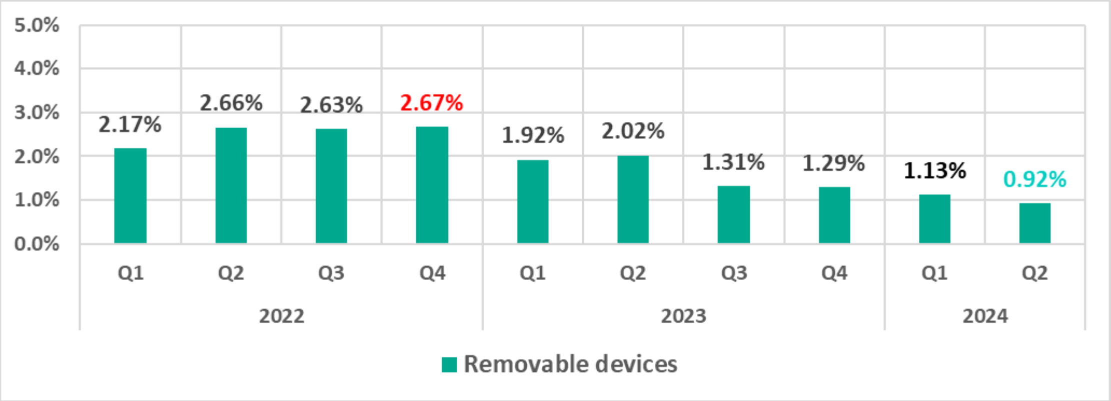
Internet



Email clients

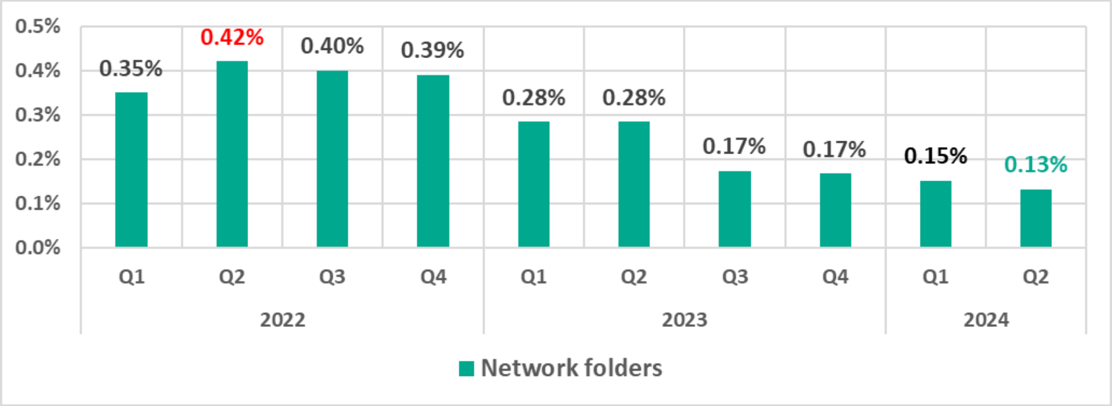


Removable media



Network folders

Network folders are a minor source of threats. The percentage of ICS computers on which network folder threats were blocked in the second quarter was 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 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:

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

- 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 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