Kaspersky ICS CERT

kaspersky

Threat landscape for industrial automation systems

Q3 2024

25.12.2024

Version 1.1

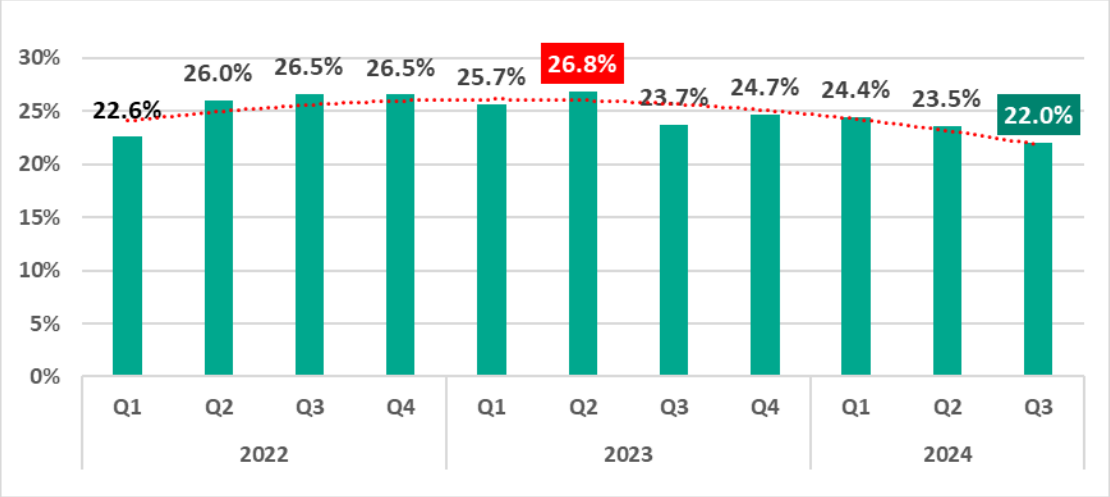
Q3 in numbers

Parameter	Q2 2024	Q3 2024	Quarterly changes
Global percentage of attacked ICS computers	23.5%	22.0%	-1.5 pp
Percentage of ICS computers on which malicious objects from different categories were blocked			
Denylisted internet resources	6.63%	6.84%	0.21 pp
Malicious scripts and phishing pages (JS and HTML)	5.69%	6.24%	0.55 pp
Spy Trojans, backdoors and keyloggers	4.08%	3.91%	-0.17 pp
Malicious documents (MSOffice + PDF)	1.96%	1.97%	0.01 pp
Viruses	1.54%	1.53%	-0.01 pp
Worms	1.48%	1.30%	-0.18 pp
Miners in the form of executable files for Windows	0.89%	0.71%	-0.18 pp
Web miners running in browsers	0.50%	0.41%	-0.09 pp
Malware for AutoCAD	0.42%	0.40%	-0.02 pp
Ransomware	0.18%	0.16%	-0.02 pp
Main threat sources			
Internet	11.25%	10.84%	-0.41 pp
Email clients	3.04%	2.95%	-0.09 pp
Removable media	0.92%	0.69%	-0.23 pp
Network folders	0.13%	0.11%	-0.02 pp

Statistics across all threats

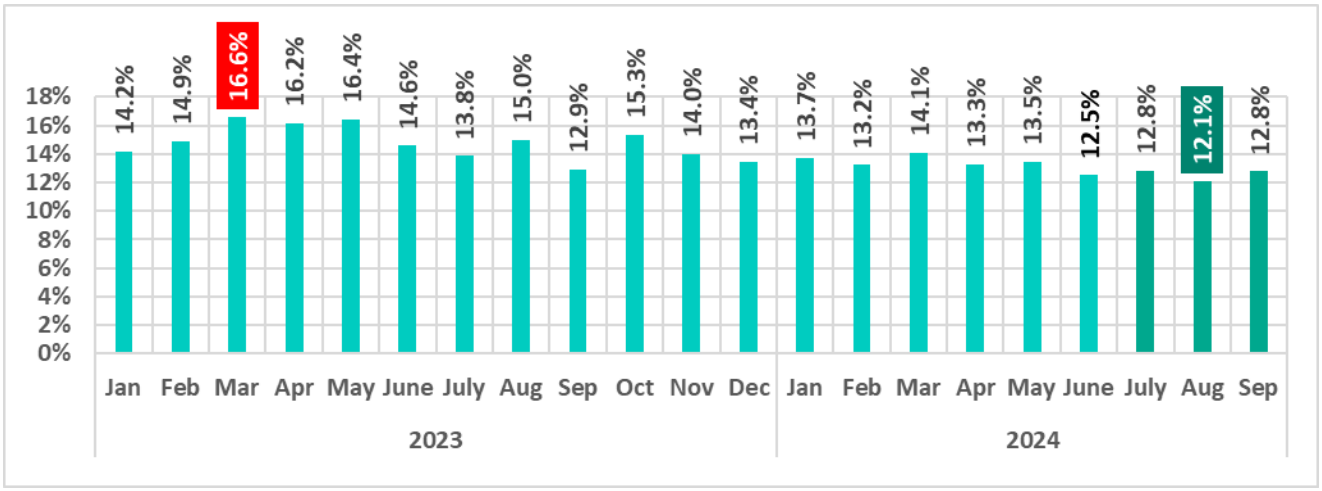
In the third quarter of 2024, the percentage of ICS computers on which malicious objects were blocked decreased by 1.5 pp from the previous quarter to 22%.

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



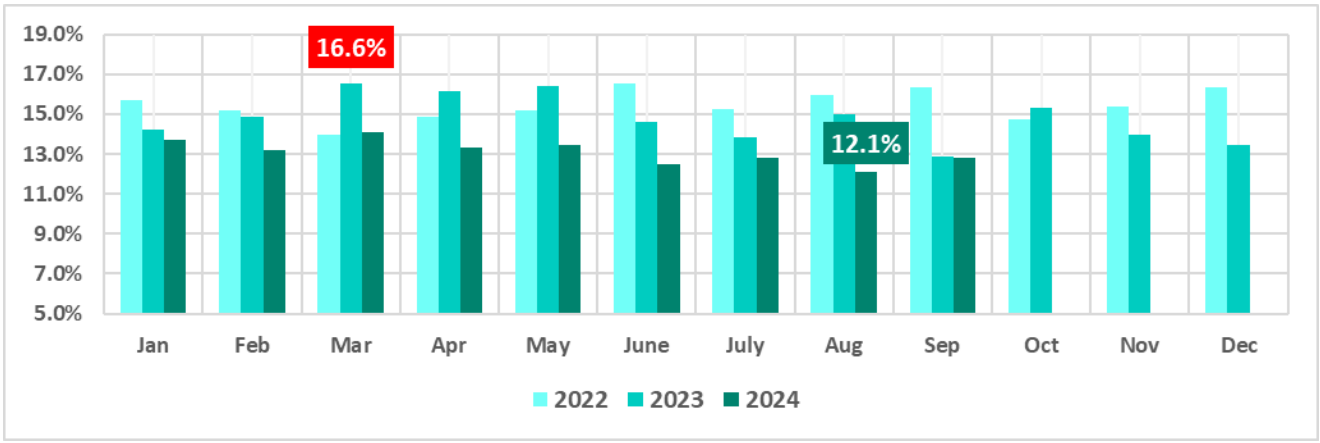
Compared to the third quarter of 2023, the percentage decreased by 1.7 pp.

The percentage of ICS computers on which malicious objects were blocked during the third quarter of 2024 was highest in July and September, and lowest in August. In fact, the percentage in August 2024 was the lowest of any month in the observed period.



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

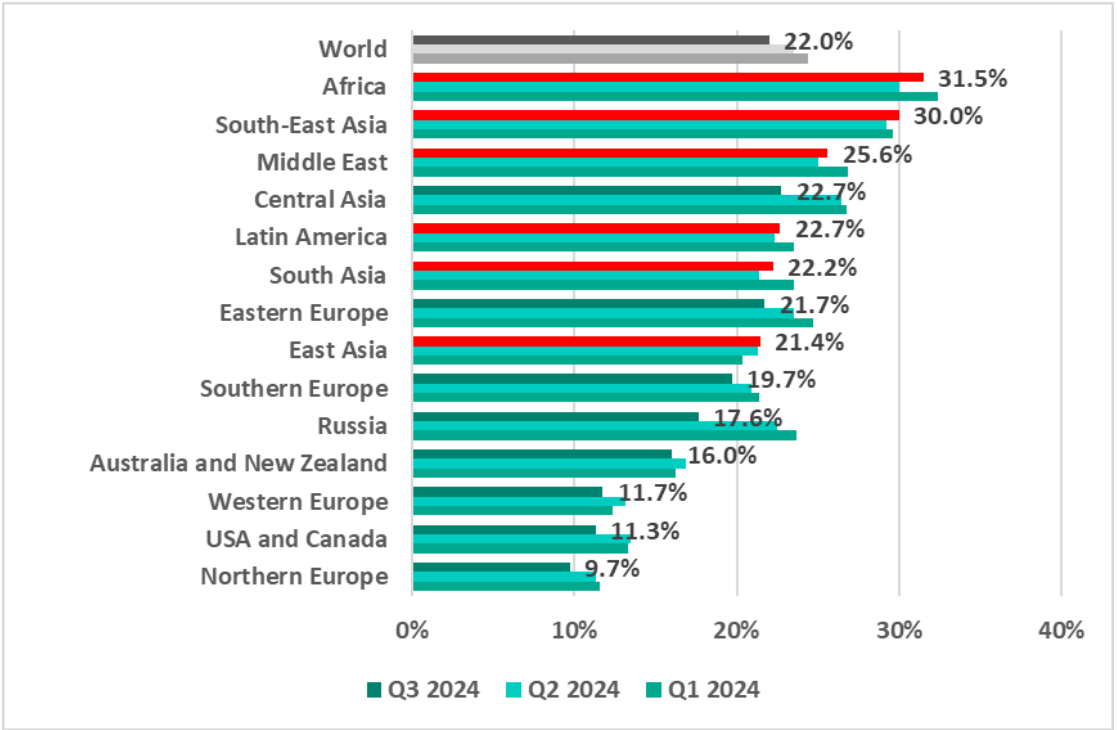
The percentages for the three months of the third quarter of 2024 are significantly lower than those for the same months of the previous year (2023).



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

Regionally[1], the percentage of ICS computers that blocked malicious objects during the quarter ranged from 9.7% in Northern Europe to 31.5% in Africa.

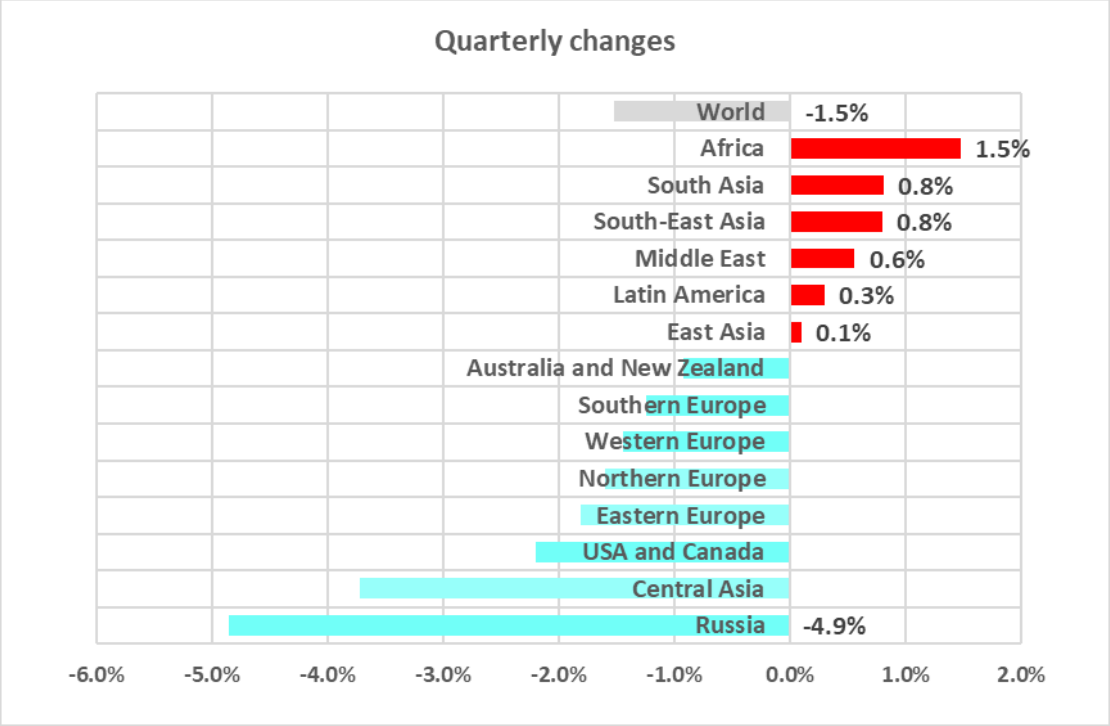
Regions ranked by percentage of ICS computers where malicious objects were blocked, Q3 2024



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

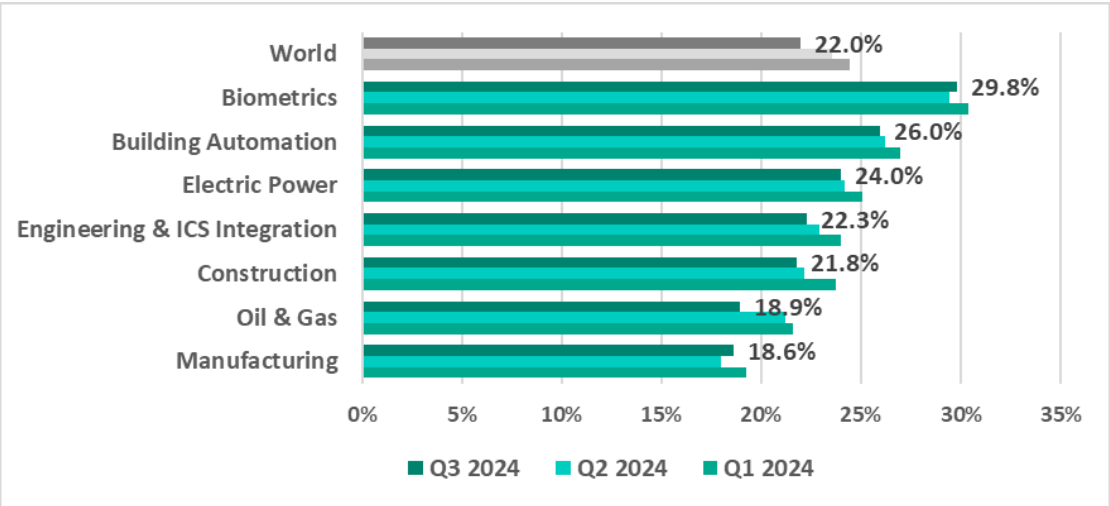
Six regions – Africa, South Asia, South-East Asia, the Middle East, Latin America, and East Asia – saw their percentages increase from the previous quarter.

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

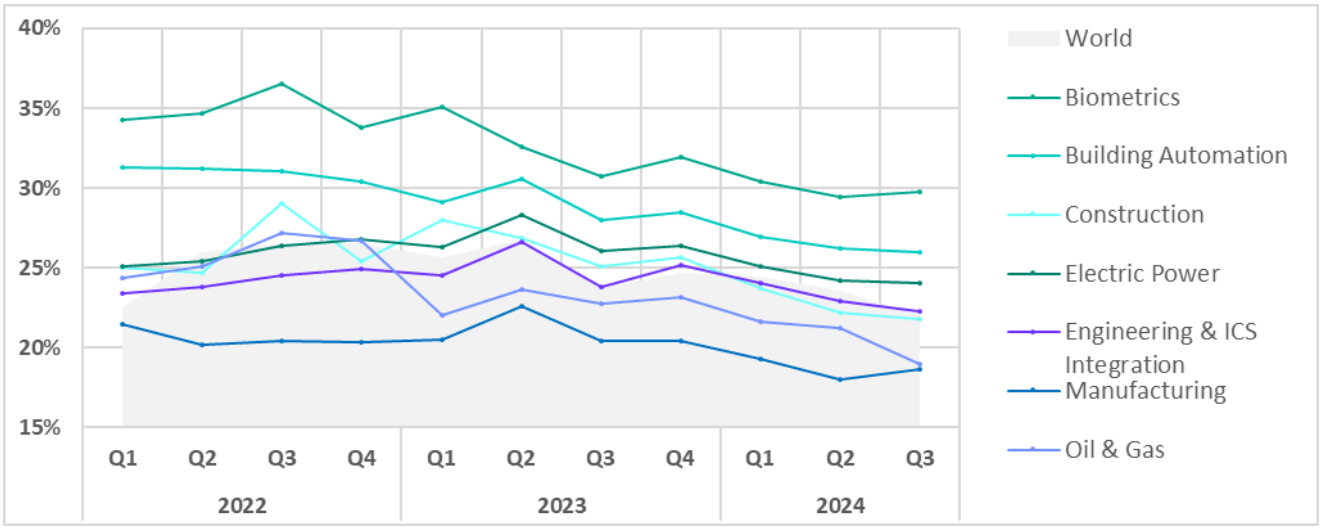


Selected industries

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



In the third quarter of 2024, the percentage of ICS computers on which malicious objects were blocked decreased across most industries, with the exception of the Biometrics and Manufacturing sectors.



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

Diversity of detected malicious objects

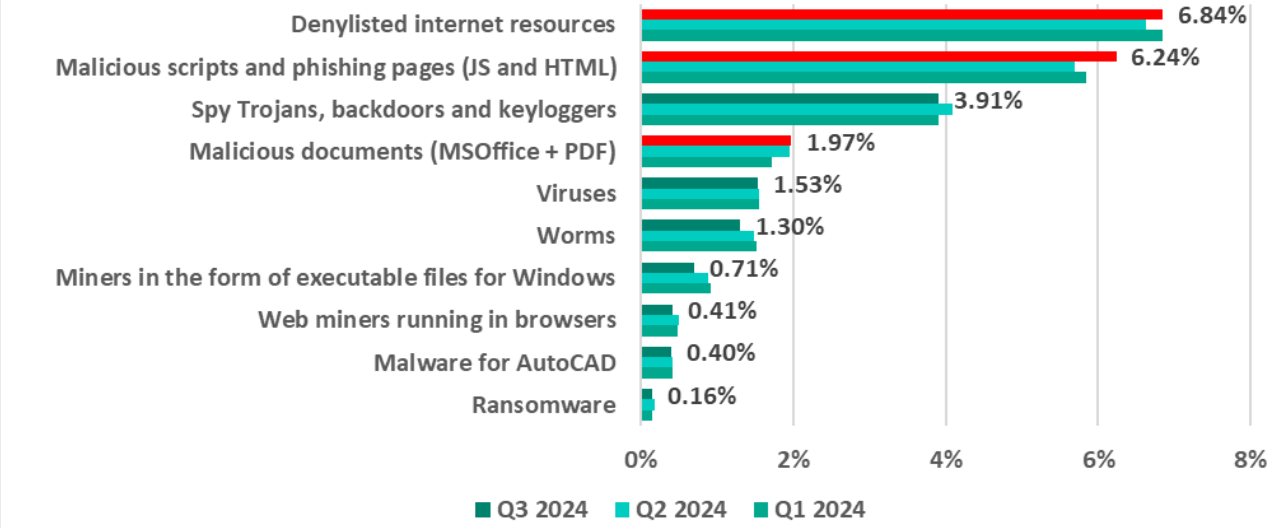
Malicious objects of various categories, which Kaspersky products block on ICS computers, can be divided into three groups according to their distribution method and purpose.

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.

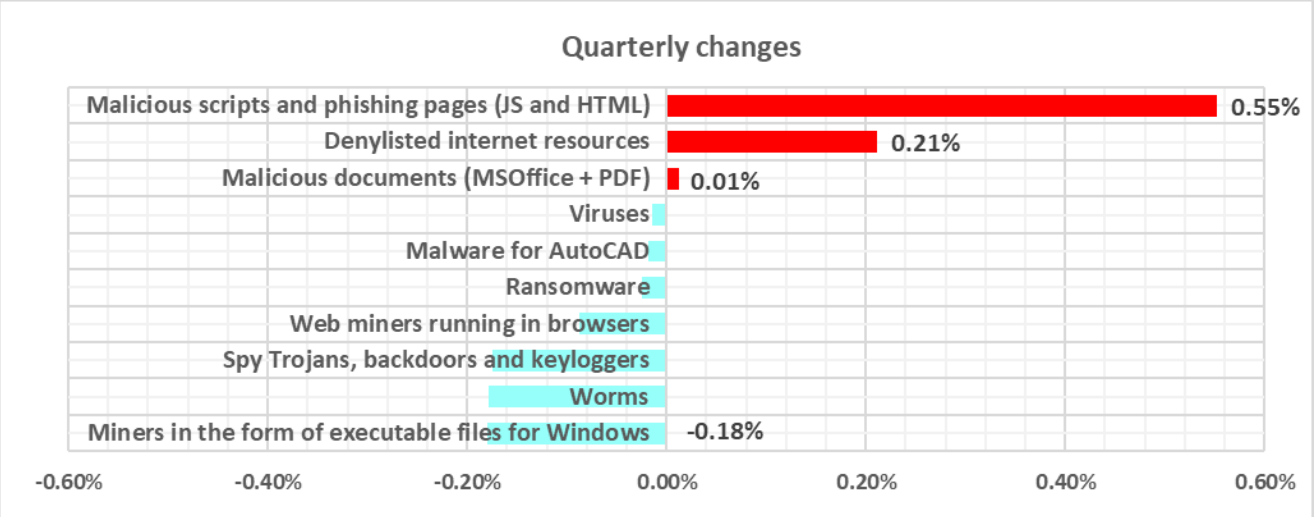
Malware for AutoCAD does not belong to a specific group, as it can spread in a variety of ways.

In the third quarter of 2024, Kaspersky's protection solutions blocked malware from 11,882 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 percentage of ICS computers on which threats were blocked.



Percentage of ICS[2] computers on which the activity of malicious objects of various categories was prevented



Changes in the percentage of ICS computers on which malicious objects from different categories were blocked in Q3 2024, compared to Q2 2024.

As shown in the chart above, initial infection threats increased in Q3 2024 compared to the previous quarter.

The most notable proportional growth during this period was in the percentage of ICS computers on which **malicious scripts and phishing pages** were blocked, representing an increase of 1.1 times.

[2] 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.

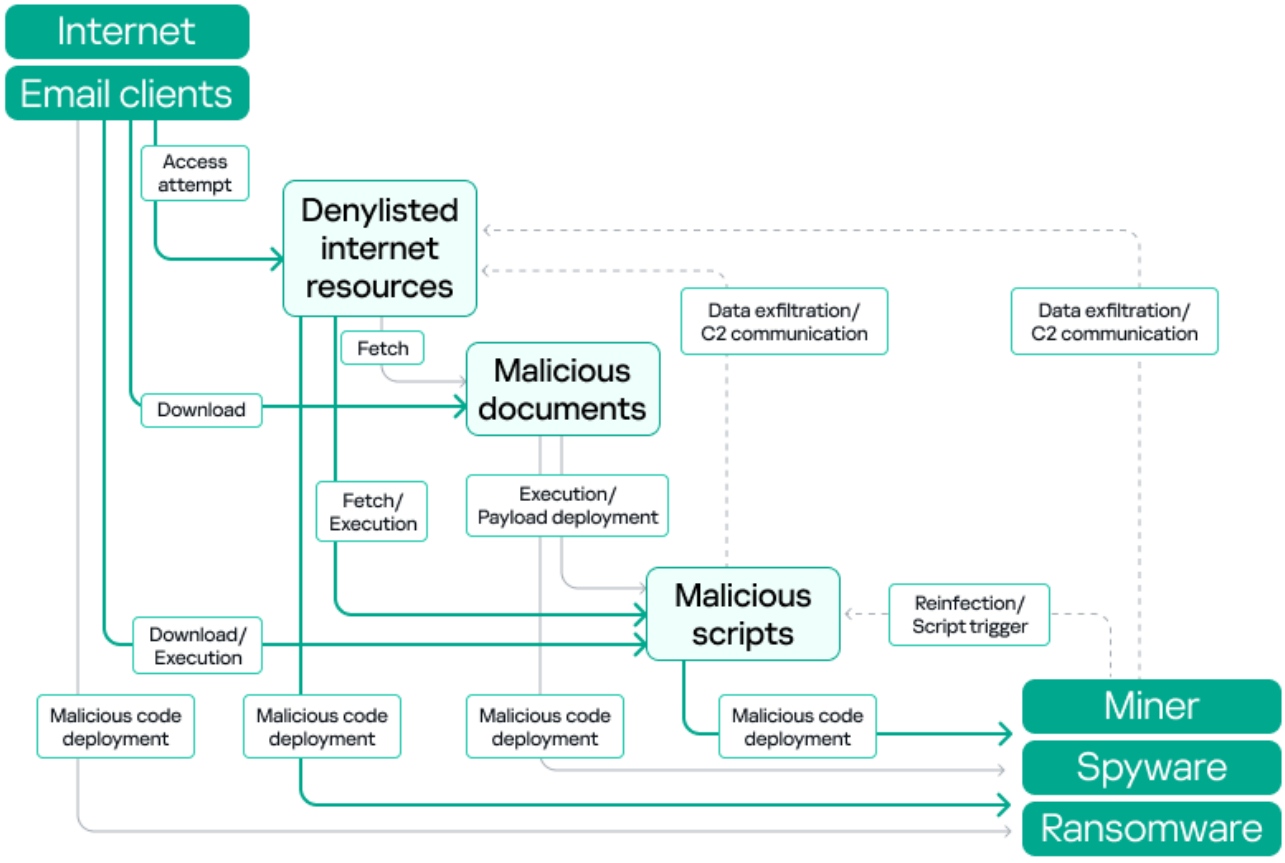
Malicious objects used for initial infection

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.

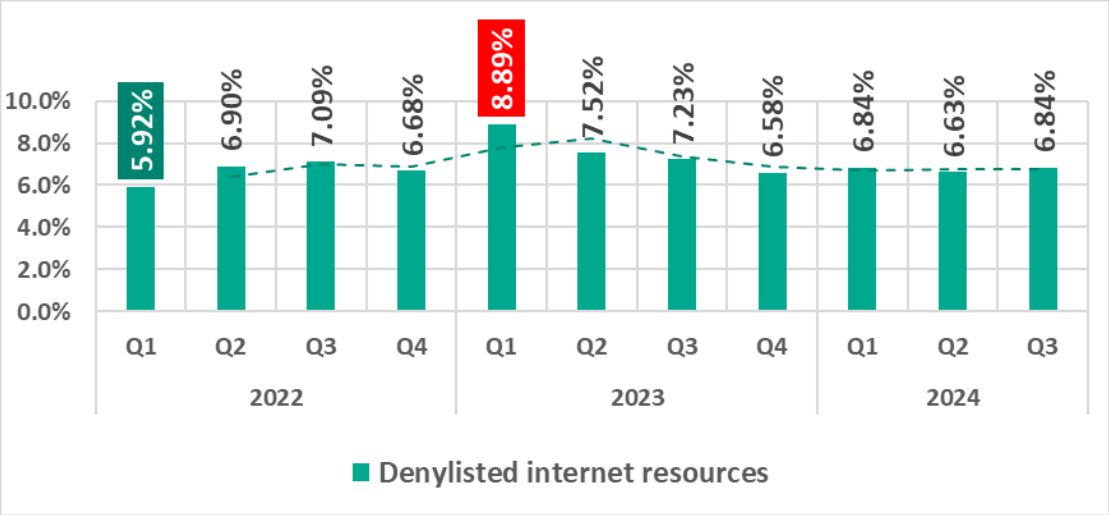


Kill chain examples: from initial infection to next-stage malware

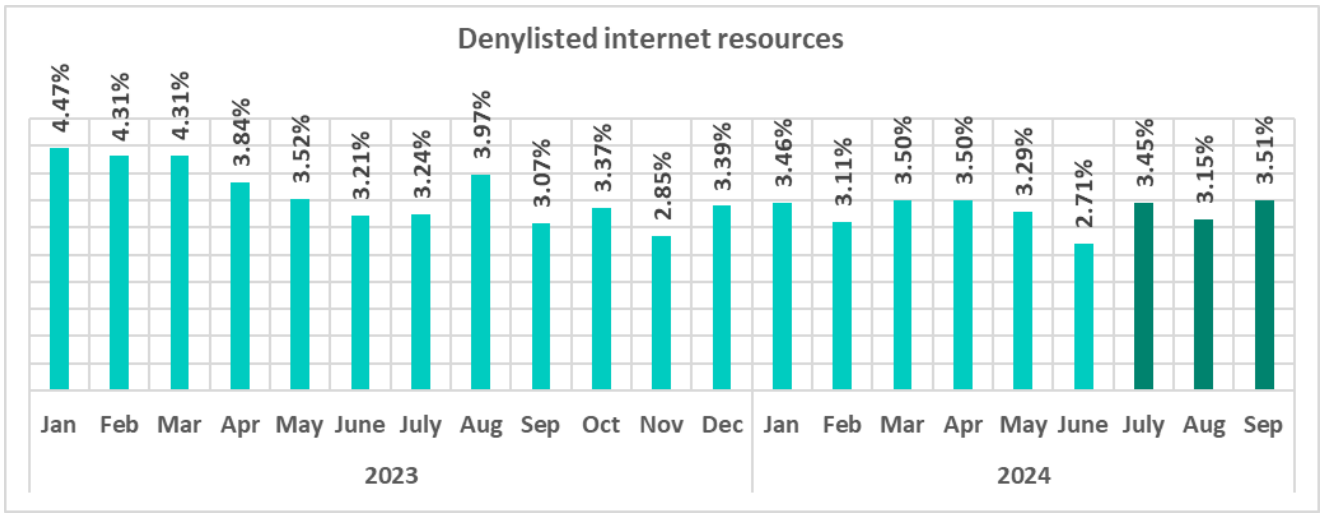
Denylisted internet resources

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 third quarter of 2024, the percentage of ICS computers on which denylisted internet resources were blocked increased slightly, but the overall trend in 2024 is steady and flat.



As the graph below shows, the rate of denylisted internet resources fluctuated throughout the months of the third quarter, reaching its highest value since September 2023 in September 2024.

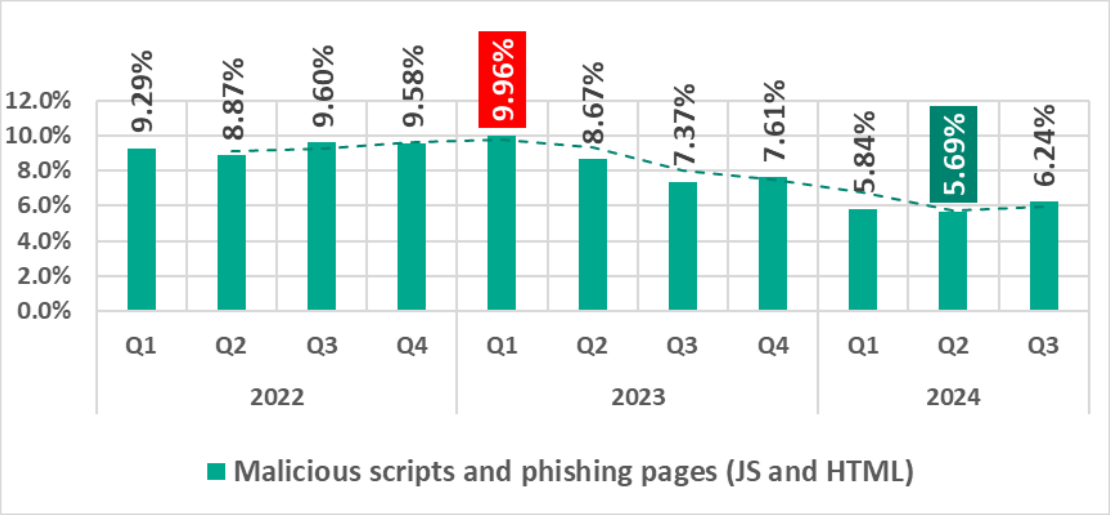


The significantly higher rate of blocked denylisted internet resources in July was primarily driven by an increase in the number of newly created malicious domain names and IP addresses used by cybercriminals as command and control (C2) infrastructure for distributing malware and phishing attacks.

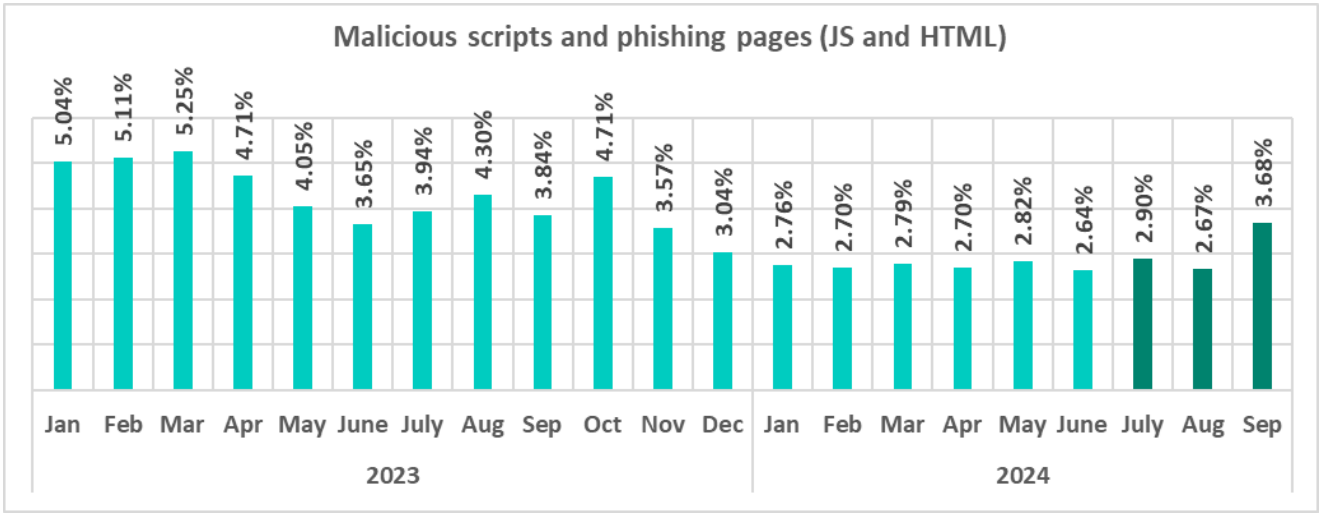
Malicious scripts and phishing pages (JS and HTML)

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 third quarter of 2024, the percentage of ICS computers on which malicious scripts and phishing pages were blocked increased, rebounding from its lowest point in the observed period, recorded in Q2 2024.



The monthly rate of malicious scripts and phishing pages fluctuated throughout the third quarter, as shown below, reaching its highest value since November 2023 in September 2024.



A significant increase in the percentage of malicious scripts and phishing pages was driven by a recent series of widespread phishing attacks in August and September. 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 adult sites, file sharing services, betting platforms, anime resources, and web apps that monetize through traffic. 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) systems[3].

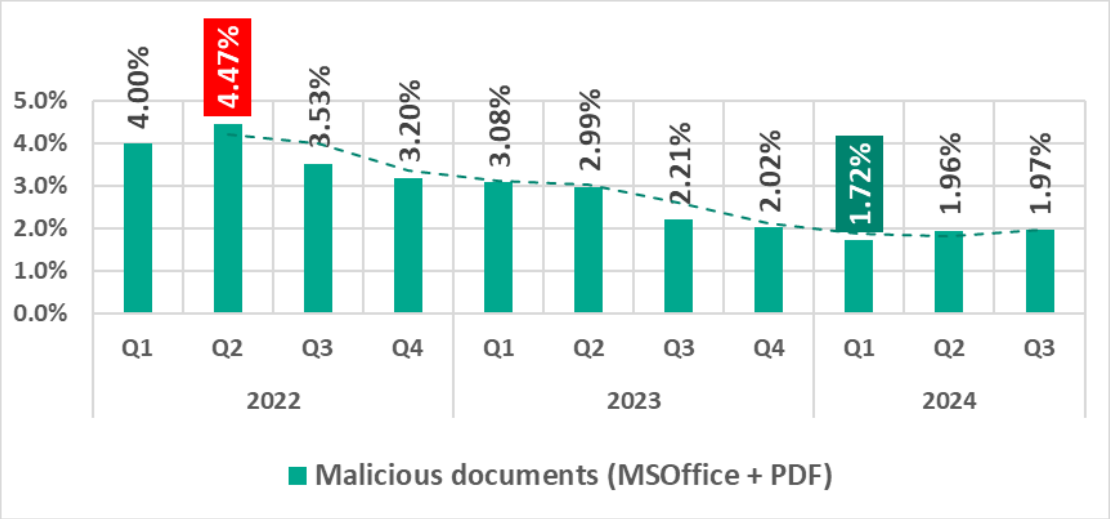
The exposure of these credentials significantly increases the risk of subsequent attacks, such as ransomware, as threat actors can use the stolen data to access sensitive systems and escalate their attacks.

Malicious documents (MSOffice+PDF)

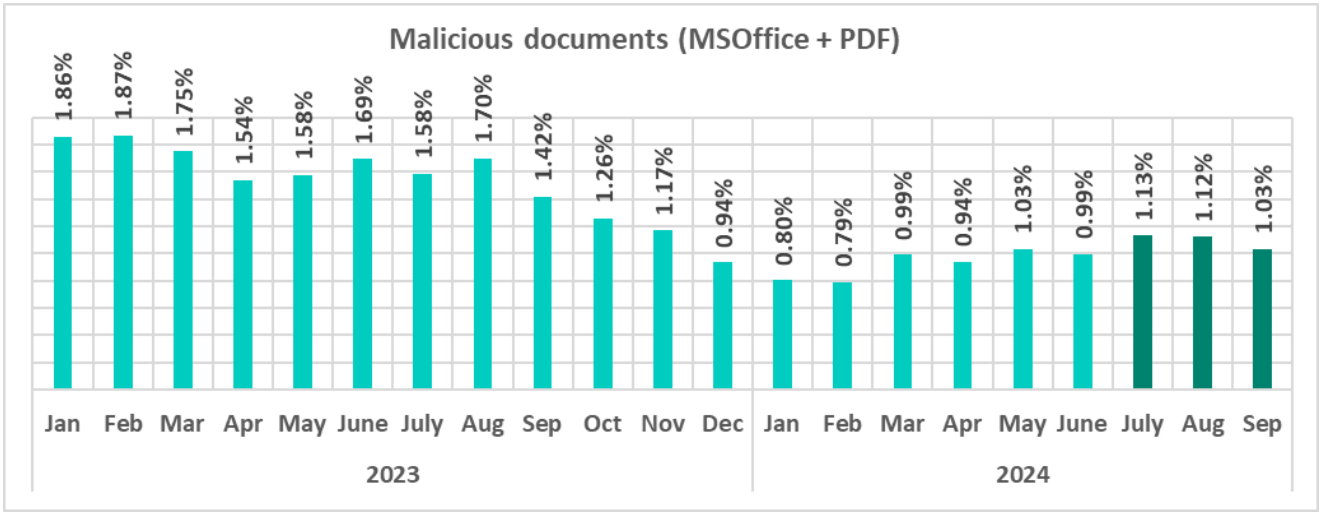
Attackers send malicious documents attached to phishing messages and use them in attacks aimed at initial infection of computers. Malicious documents typically contain exploits, malicious macros, and malware links.

The percentage of ICS computers with malicious documents on them peaked in the second quarter of 2022 and steadily declined until an increase in the second quarter of 2024, which continued into Q3 2024.

[3] Read more about these attacks here: Malicious CAPTCHA delivers Lumma and Amadey Trojans



As shown below, the monthly rate of malicious documents in the third quarter of 2024 peaked in July and then declined. The July 2024 rate was also the highest recorded since December 2023.



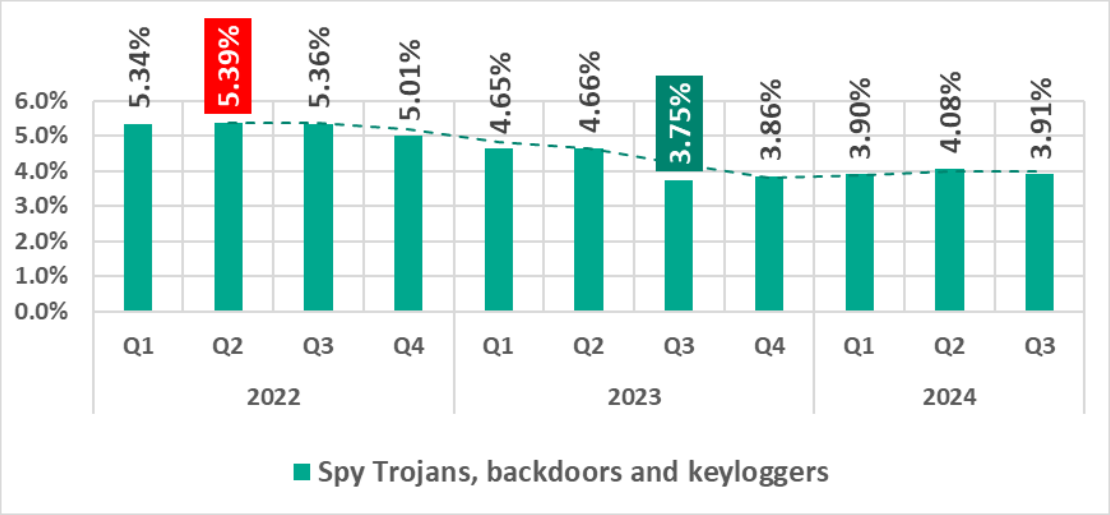
Next-stage malware

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

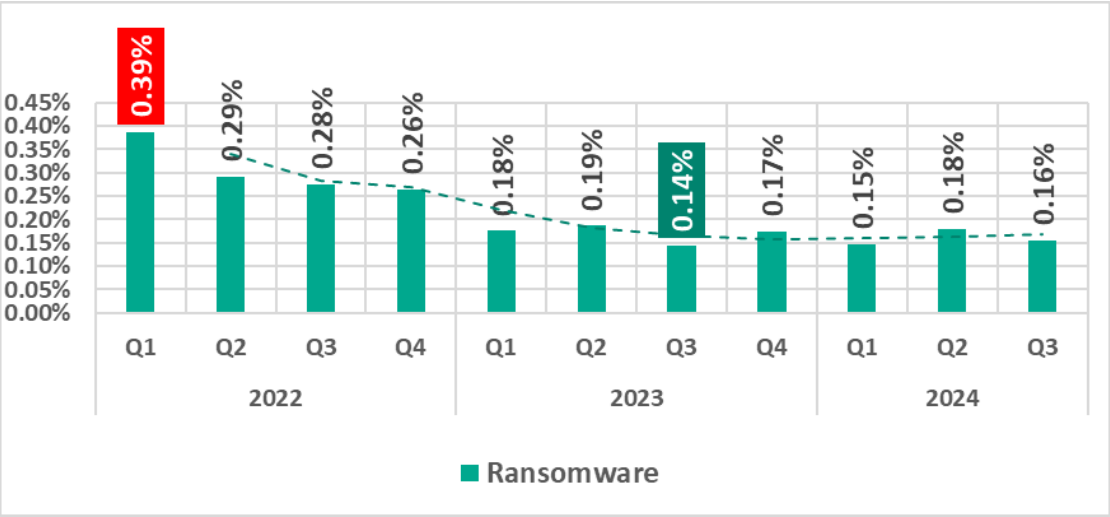
Spyware (spy Trojans, backdoors, and keyloggers) can be found in lots of phishing emails sent to industrial organizations. Spyware is used for unauthorized remote access and confidential data theft. The ultimate goal of most spyware attacks is stealing money, but spyware is also used in targeted attacks,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



Ransomware

The percentage of ICS computers on which ransomware was blocked continued to vary from quarter to quarter within 0.03 p.p.



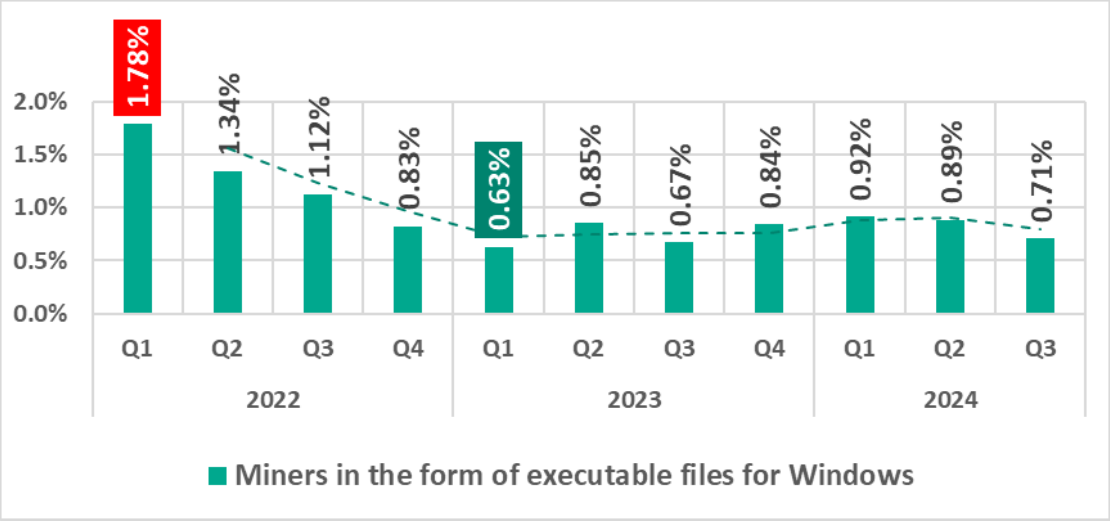
Miners in the form of executable files for Windows

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.

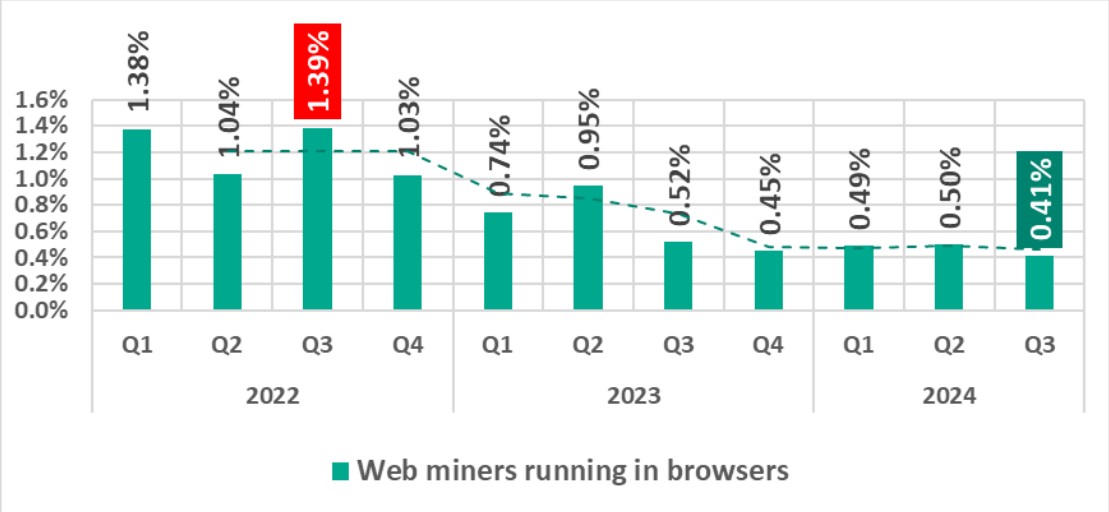
In the third quarter of 2024, similar to the previous quarter, a significant portion of Windows miners found on ICS computers consisted of archives with names that mimicked legitimate software. These archives did not contain actual software, but did include a Windows LNK file, commonly known as a shortcut.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



Web miners

The percentage of ICS computers on which web miners were blocked decreased in the third 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.

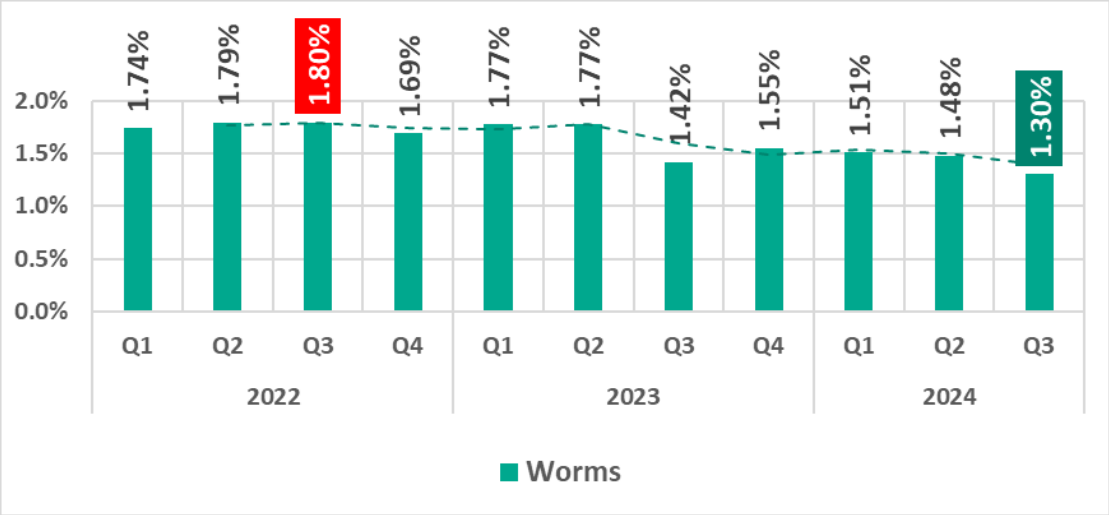
A lot of those still spreading are legacy viruses and worms whose command-and-control servers have been shut down. However, these types of malware can compromise infected systems by opening network ports or changing configurations, cause software failures, denial of service, and so on.

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

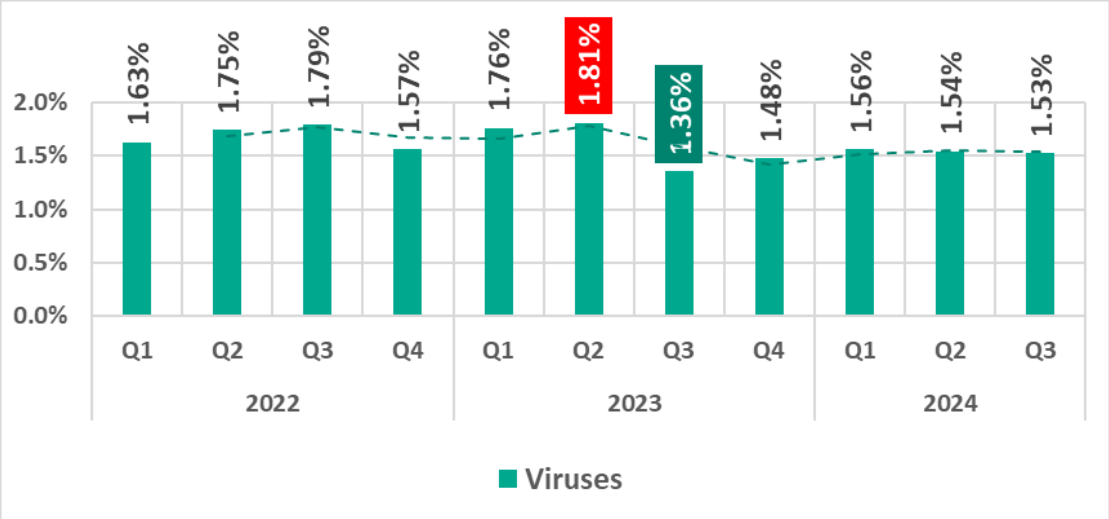
New worm versions used by malicious actors to spread spyware, ransomware, and miners can also be found on ICS networks. In most cases, they rely on network service (e.g., SMB or RDP) exploits that have been addressed by the vendors but still persist on OT networks, previously stolen credentials, or password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

The percentage of ICS computers on which worms were blocked continued to decrease in the third quarter of 2024, reaching its lowest point in the observed period.



Viruses

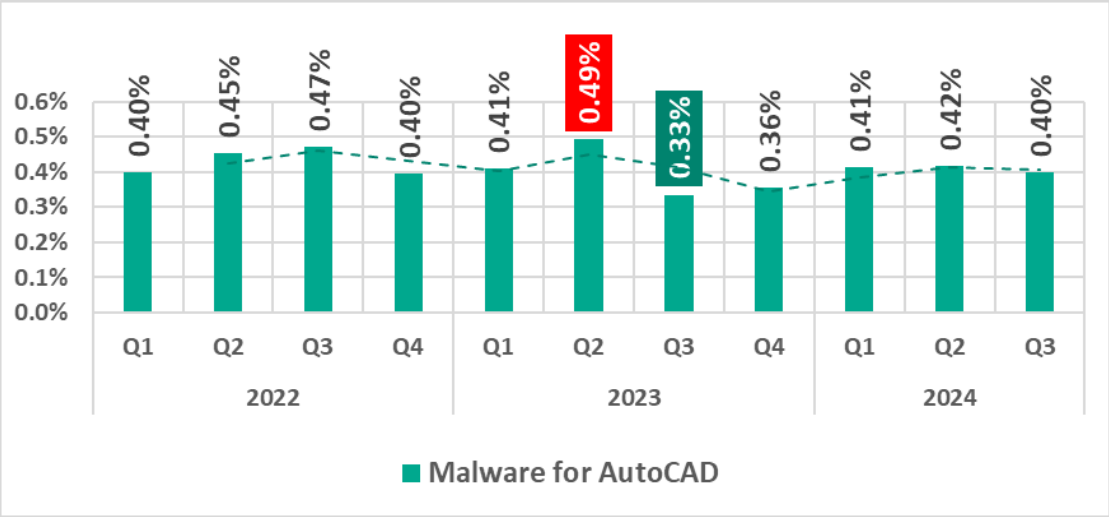
The percentage of ICS computers on which viruses were blocked decreased slightly in the third quarter of 2024.



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

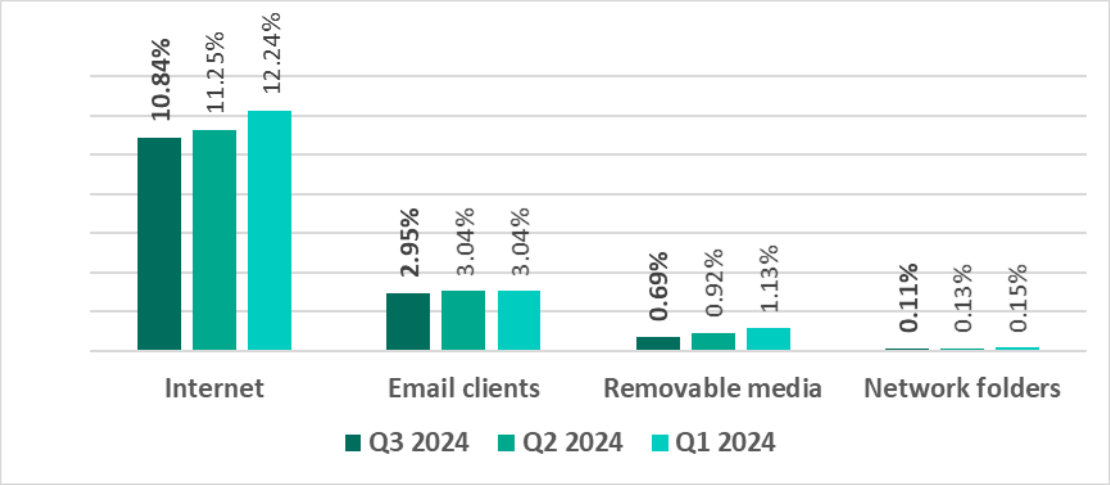


Main threat sources

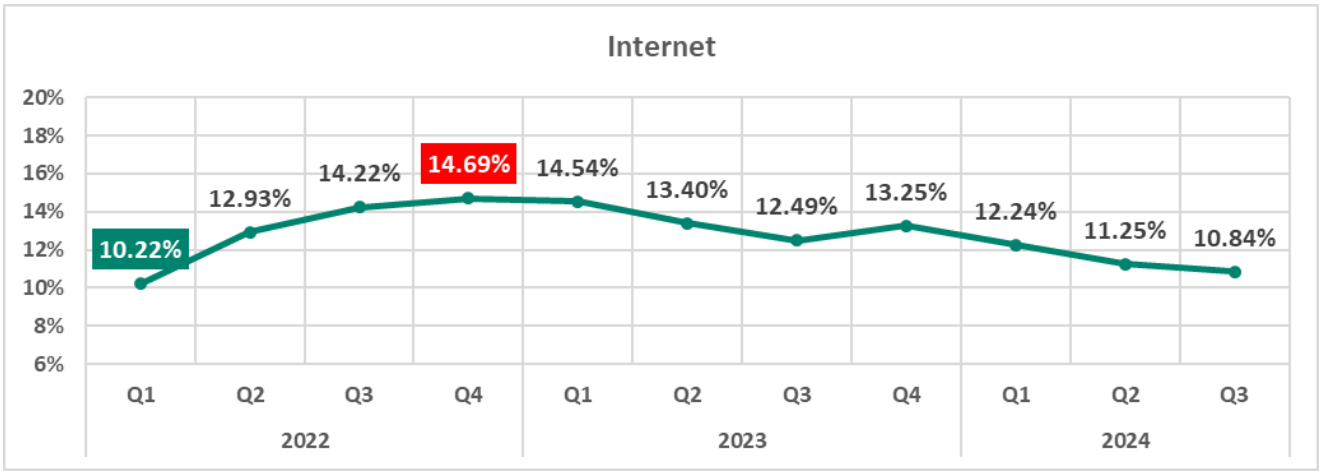
The internet, email clients, and removable storage devices remain the primary sources of threats to computers in an organization's technology infrastructure. (Note that the sources of blocked threats cannot be reliably identified in all cases.)

In the third 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

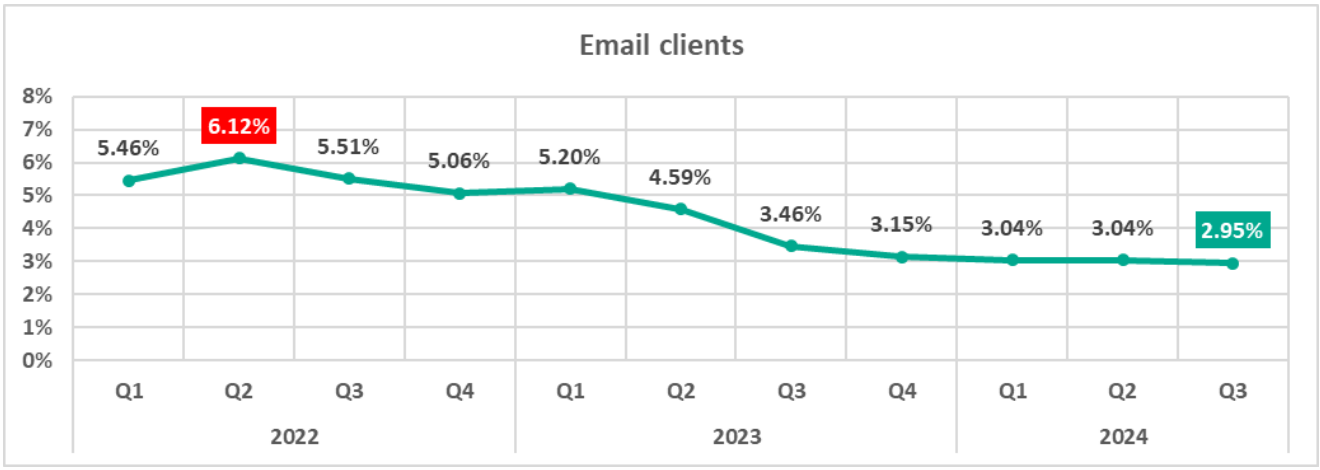


Internet



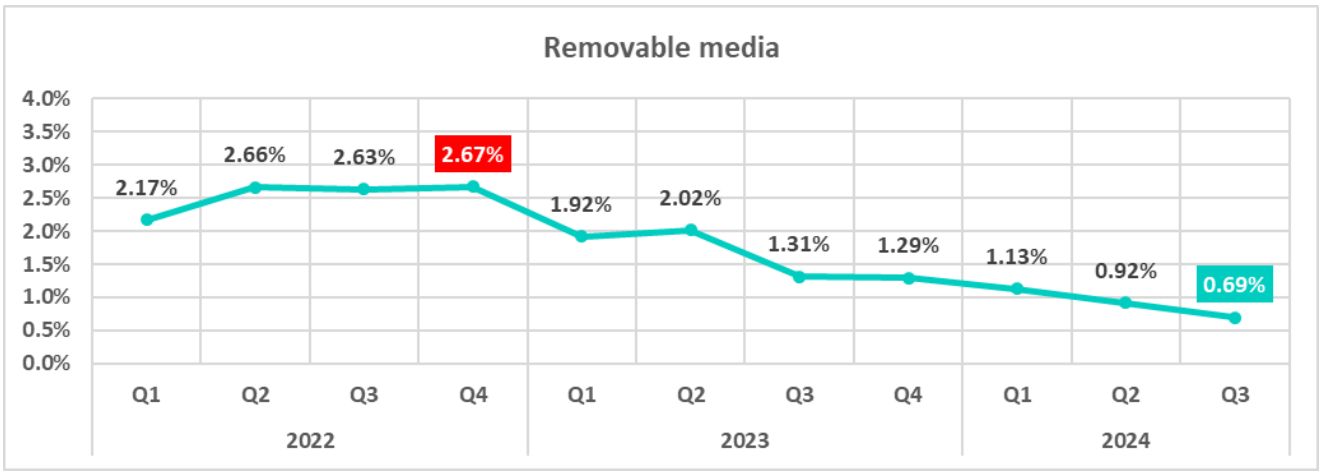
Email clients

The percentage of ICS computers on which threats from email clients were blocked in the third quarter was the lowest in the observed period.



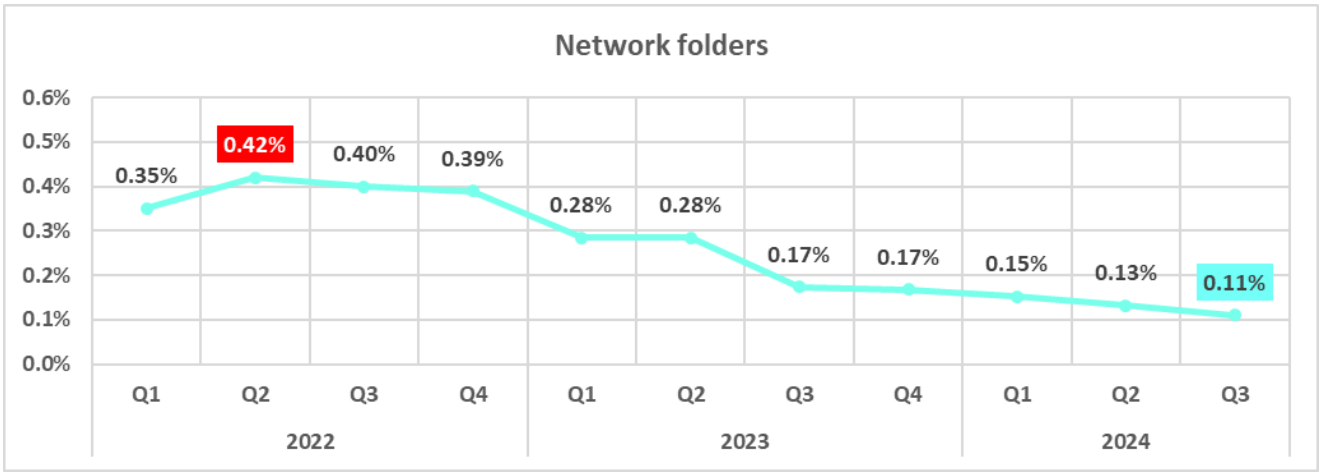
Removable media

The percentage of ICS computers on which threats distributed on removable devices were blocked in the third quarter was the lowest in the observed period.



Network folders

Network folders are a minor source of threats. The percentage of ICS computers on which network folder threats were blocked in the third quarter was the lowest in the observed period.



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[4].

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

[4] 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