Kaspersky ICS CERT

kaspersky

Threat landscape for industrial automation systems

Russia. Q4 2025

23.04.2026

Version 1.0

Russia 3
Current threats 3
Statistics across all threats 5
Threat sources 5
Internet 6
Email clients 7
Removable media 9
Network folders 10
Threat categories 11
Denylisted internet resources 12
Spy Trojans, backdoors, and keyloggers 13
Worms 14
Miners in the form of executable files for Windows 15
Web miners 17
Malicious documents 17
Viruses 18
Ransomware 19
Industries 19
Threat sources and malware categories in industries: 'hotspots' 22
Methodology used to prepare statistics 28

Russia

Current threats

Russia ranked 10th among regions by percentage of ICS computers on which malicious objects were blocked. At the same time, the region held higher positions in the rankings based on threat figures in the following categories:

- Miners in the form of executable files for Windows – second place.
- Denylisted internet resources – third place.
- Web miners – fourth place.
- Spyware, viruses and ransomware – ninth place.

Removable media stand out among threat sources: Russia ranked eighth among regions by the percentage of ICS computers on which threats were blocked when removable media were connected.

The internet is the main source of threats in Russia

The main categories of internet threats blocked on ICS computers are: denylisted internet resources, malicious scripts and phishing pages, and miners.

Denylisted internet resources

The list of denylisted internet resources is used to prevent initial infection attempts. The following threats are primarily blocked on ICS computers using the list:

- Known malicious URLs and IP addresses used by attackers to host malicious payloads and configurations.
- Suspicious (untrustworthy) web resources with entertaining and gaming content that are often used to deliver unwanted software, cryptominers, and malicious scripts.
- CDN nodes used by attackers to distribute malicious scripts on popular websites.
- File and data sharing services, including repositories, which are often used by attackers to host payloads and next-stage configurations.

Cybercriminals use denylisted internet resources primarily for malware distribution, for phishing attacks, and as command-and-control (C2) infrastructure. A significant percentage of such resources is used to distribute malicious scripts and phishing pages (HTML).

High values of this parameter typically point to:

- Poor enforcement of information security policies (ICS computers have internet access in one way or another).
- Failings in the information security culture (employees access unsafe internet resources).

By percentage of ICS computers on which denylisted internet resources were blocked in the industries covered in this report, Russia ranks among regions as follows:

- First place for the building automation industry.
- Second place for the biometric systems.
- Third place for the electric power industry.

Miners in the form of executable files for Windows, and worms

Since late 2022, Russia has consistently ranked second among regions (behind Central Asia and the South Caucasus) by percentage of ICS computers on which miners in the form of executable files for Windows were blocked.

In Q4 2025, worms ranked fourth among threat categories in Russia. Besides Russia, this threat category holds such high positions only in regional rankings for Africa, South Asia, and Central Asia and the South Caucasus.

These two threat categories show very similar dynamics in Russia. This is because miners for Windows extensively use modules and components that are essentially worms, designed to deliver the miner to other computers on the network as part of automated lateral movement.

Miners in various industries

The miner threat is relevant to all industries in the region: Russia ranked fourth or higher in the regional rankings based on miner percentage figures for both miner categories across all industries except manufacturing. In the manufacturing industry, Russia ranked third in terms of miners in the form of executable files and fourth in terms of web miners.

Ransomware

Russia ranked ninth among regions by percentage of ICS computers on which ransomware was blocked.

The threat is relevant to all industries. Russia ranked sixth or higher in the regional rankings by percentage of ICS computers on which ransomware was blocked in the industries covered.

In Q4 2025, Russia ranked second in the regional ranking by percentage of attacked computers in biometric systems and third in the rankings based on this percentage in the electric power and oil and gas industries.

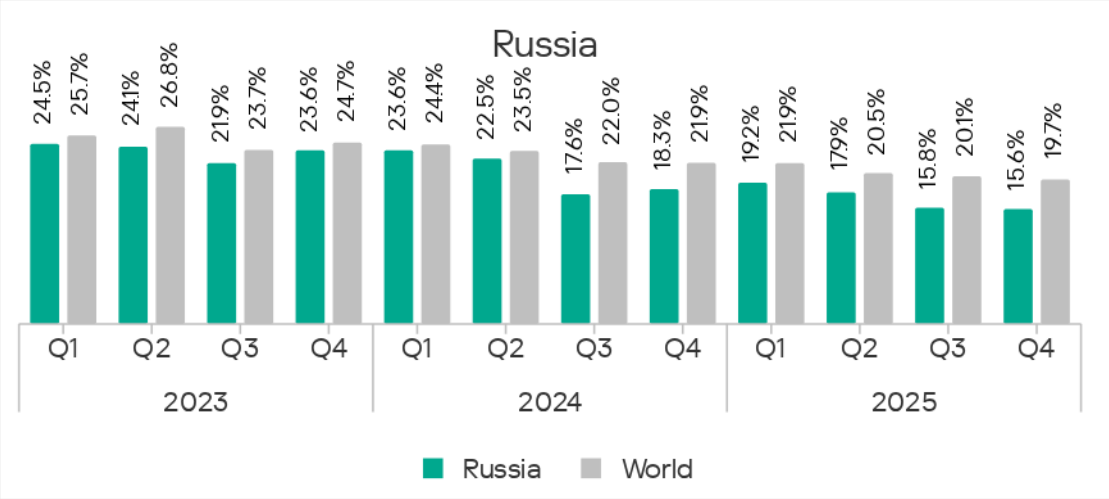
Threats on removable media

Russia ranked eighth among regions by percentage of ICS computers on which threats were blocked when removable media were connected.

Statistics across all threats

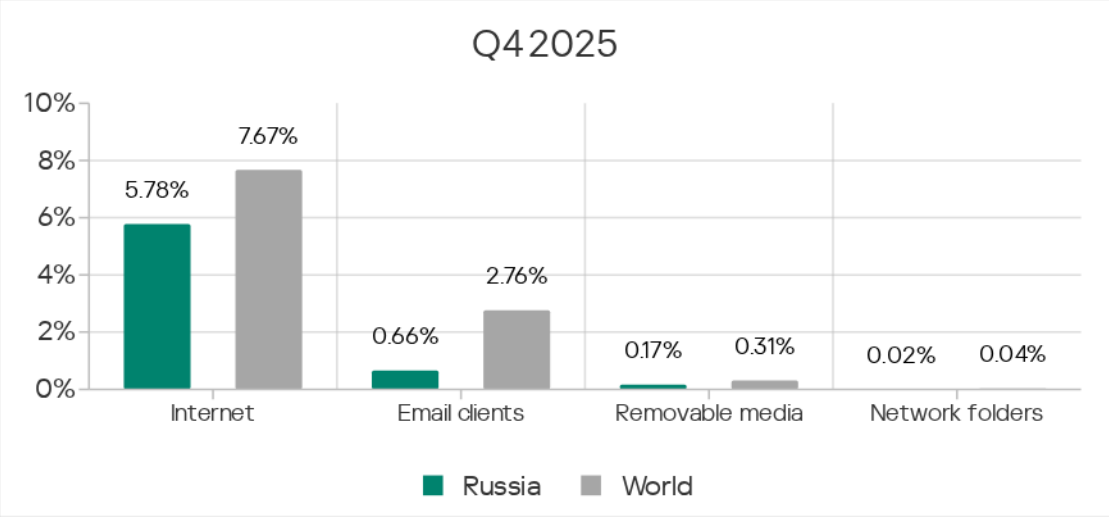
Russia ranked 10th among regions by the percentage of ICS computers on which malicious objects were blocked.

The region's percentage figure was below the global average and has been decreasing for the third consecutive quarter. In Q4 2025, it reached the lowest value for the period under review – 15.6%. This was 1.8 times higher than in Northern Europe, which ranked last among all regions.

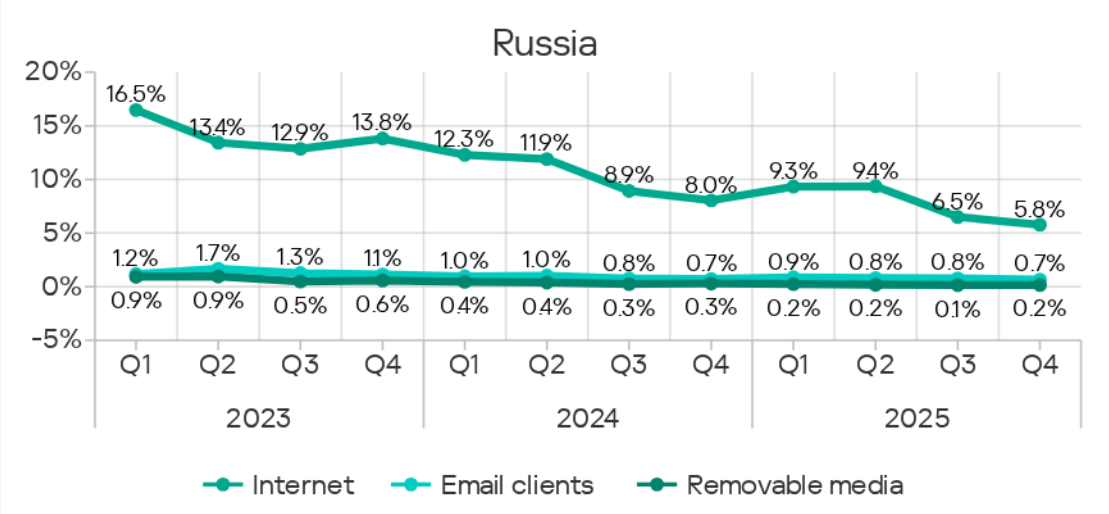


Threat sources

In Russia, the percentages of ICS computers on which threats from various sources were blocked were lower than the global averages for all threat sources.



Among all threat sources, only the percentage figure for removable media increased over the quarter.

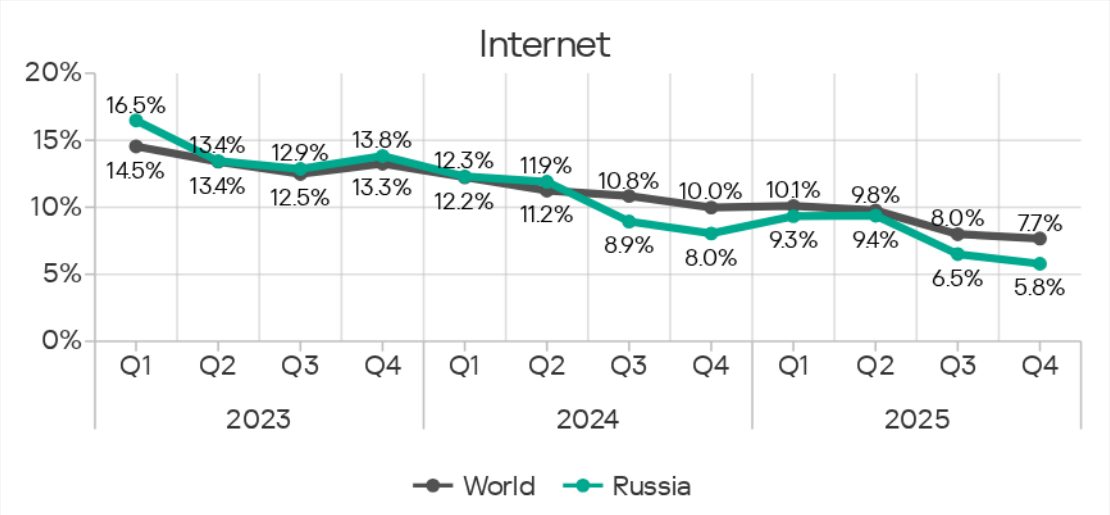


Russia's highest position in the rankings by percentage of ICS computers on which threats from various sources were blocked is for removable media – the region ranked eighth.

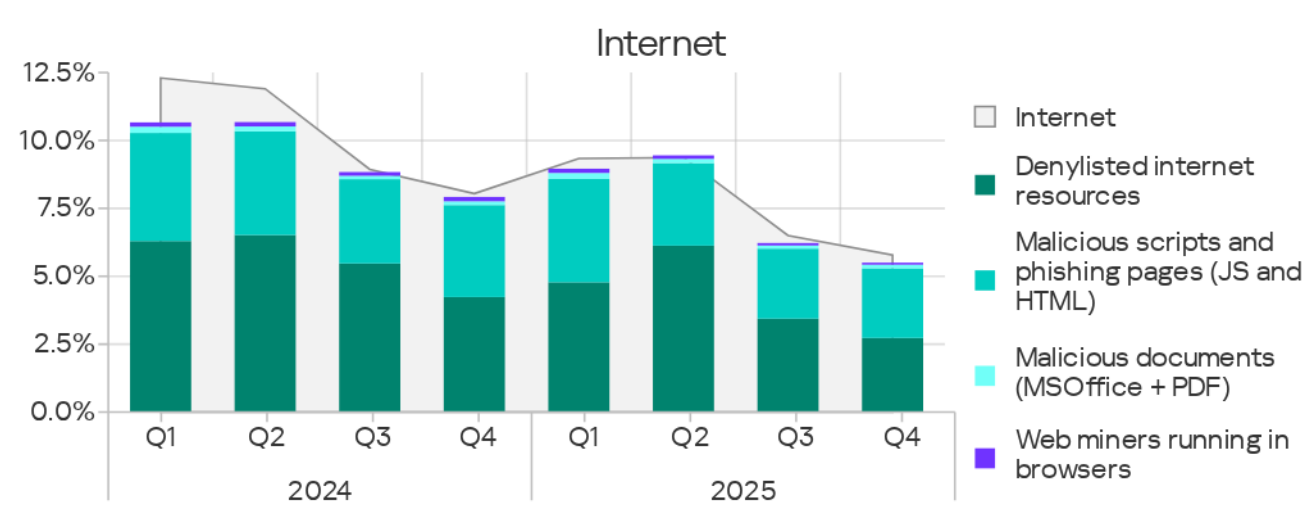
Internet

Russia ranked 12th with 5.78% in the ranking of regions by percentage of ICS computers on which internet threats were blocked. Compared with Northern Europe, which ranked last, Russia's figure was 1.5 times higher.

The percentage of ICS computers on which internet threats were blocked in Russia increased during the first two quarters of 2025 and decreased in Q3 and Q4. In Q4, the figure reached its lowest value for the period under review.



The main categories of internet threats blocked on ICS computers were denylisted internet resources, and malicious scripts and phishing pages.



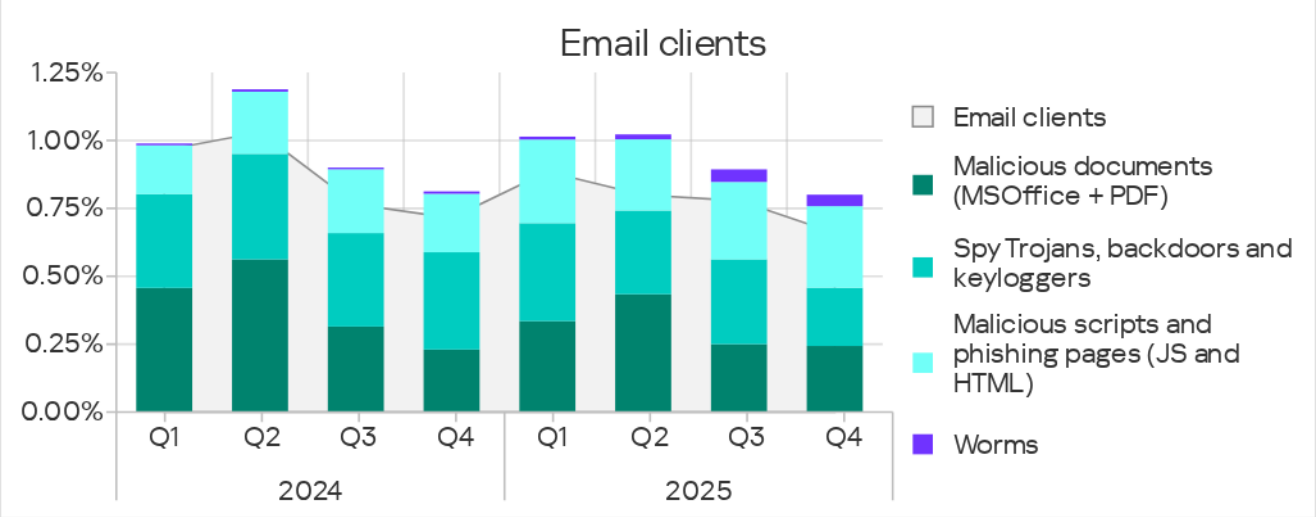
Russia ranked third in the regional ranking by percentage of ICS computers on which denylisted internet resources were blocked.

Malicious scripts and phishing pages are distributed both online and via email. In Russia in Q4 2025, they were distributed primarily online.

Email clients

In Q4 2025, Russia ranked 13th (second-lowest), with 0.66% of ICS computers on which threats from email clients were blocked. This value was slightly higher than in Northern Europe, which had the lowest figure among all regions.

The main categories of email threats blocked on ICS computers were malicious scripts and phishing pages, malicious documents, and spyware.



Email is the main distribution channel for malicious documents and spyware. Malicious scripts are distributed both via email and online. In Q4 2025, the internet was the main source of this threat.

In Q4 2025, the percentage of ICS computers on which worms from email clients were blocked increased. This was due to a new wave of a phishing campaign known as Curriculum-vitae-catalina, which targeted organizations in all regions of the world. In Russia, the attack peaked in October.

The attackers sent phishing emails disguised as job applications. These emails contained a malicious executable file (Backdoor.MSIL.XWorm, a worm-backdoor used for remote administration) masquerading as a CV (Curriculum Vitae). If the file was launched, the system became infected.

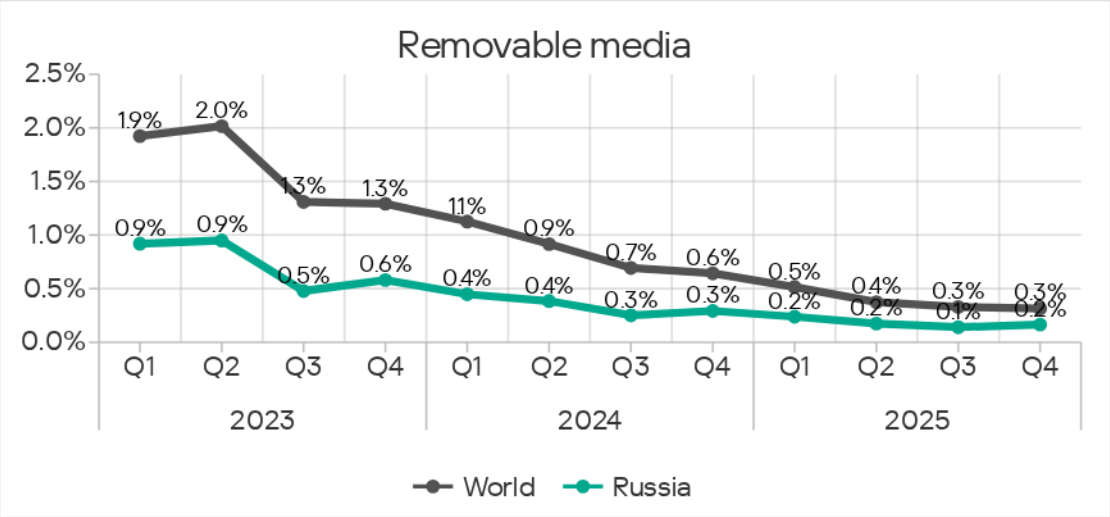
Such campaigns are typically aimed at delivering malware for data theft, spyware, or remote administration tools (RATs).

The percentage of ICS computers on which worms were blocked increased across all regions, with Russia ranking eighth based on the rate of increase. In Russia, unlike other regions, removable media remained the main source of worms in Q4, although the occurrence of this threat in email also increased noticeably.

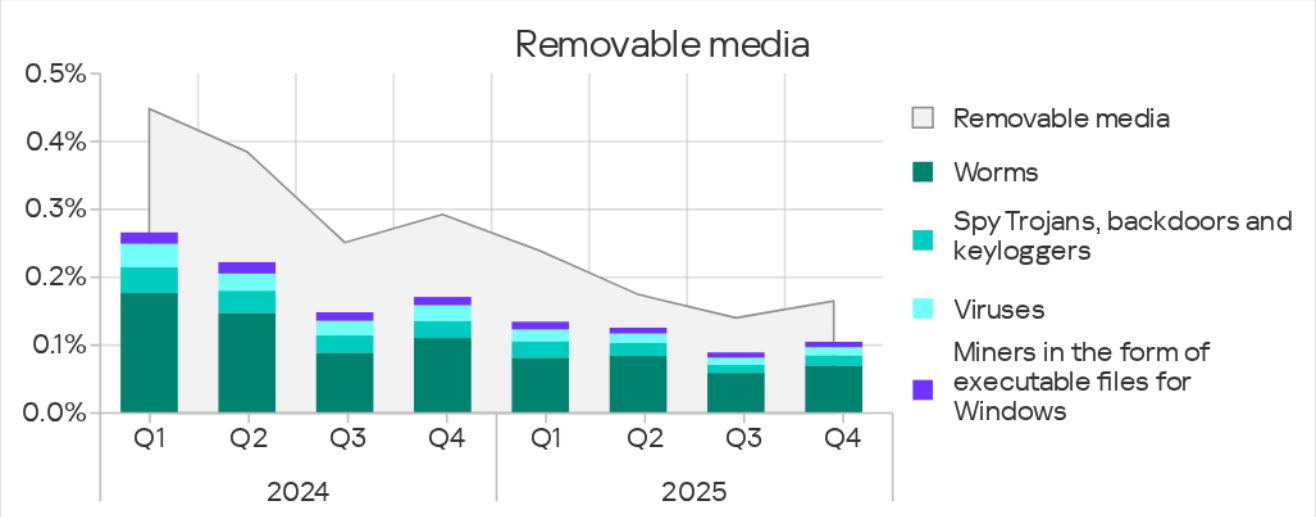
Removable media

Russia ranked eighth in the regional ranking by percentage of ICS computers on which threats were blocked when removable media were connected. This is the region's highest ranking for various threat sources.

In Q4 2025, the percentage figure for Russia rose to 0.17%. This was 3.4 times higher than in the Australia and New Zealand region, which ranked lowest.



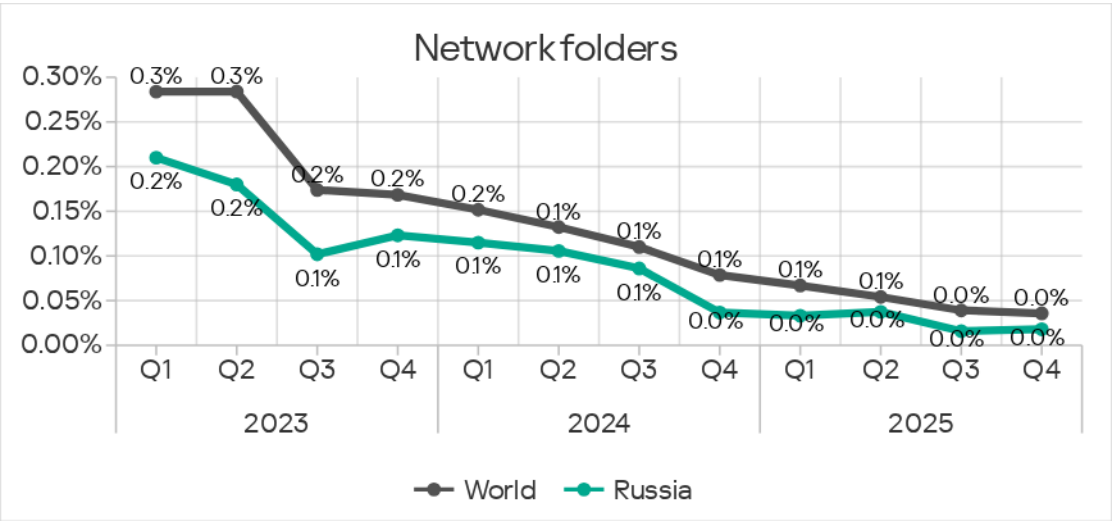
The main categories of threats blocked in the region when removable devices were connected to ICS computers were worms, spyware, viruses, and miners in the form of executable files for Windows.



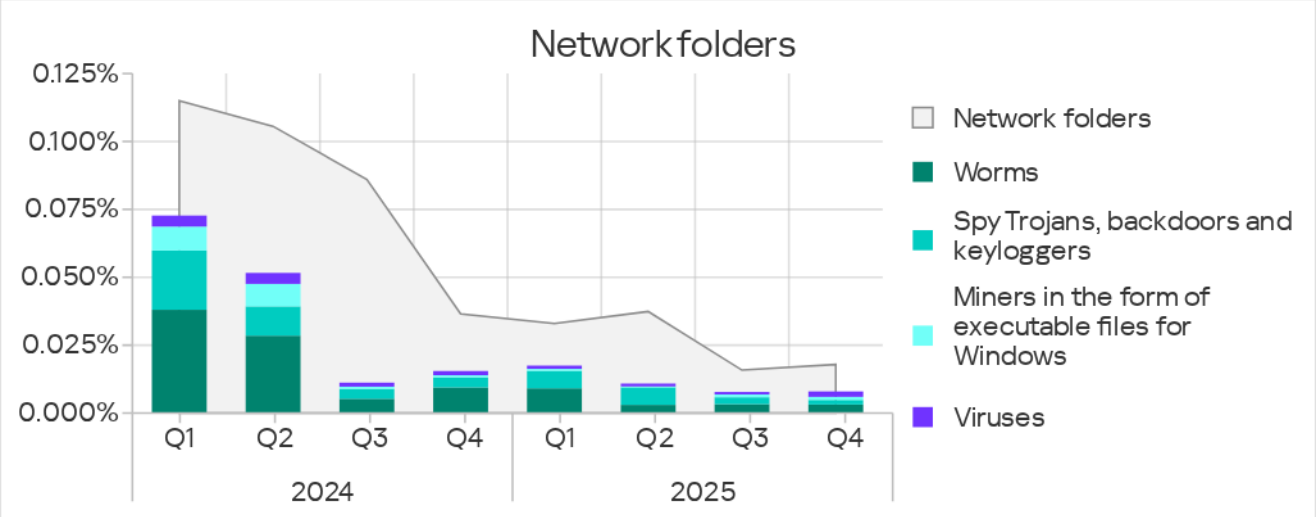
Removable media are the main distribution channel for worms. Unlike other regions, where, due to the phishing campaign, more worms were blocked on ICS computers in email than on removable media, removable media remained the main source of worms in Russia.

Network folders

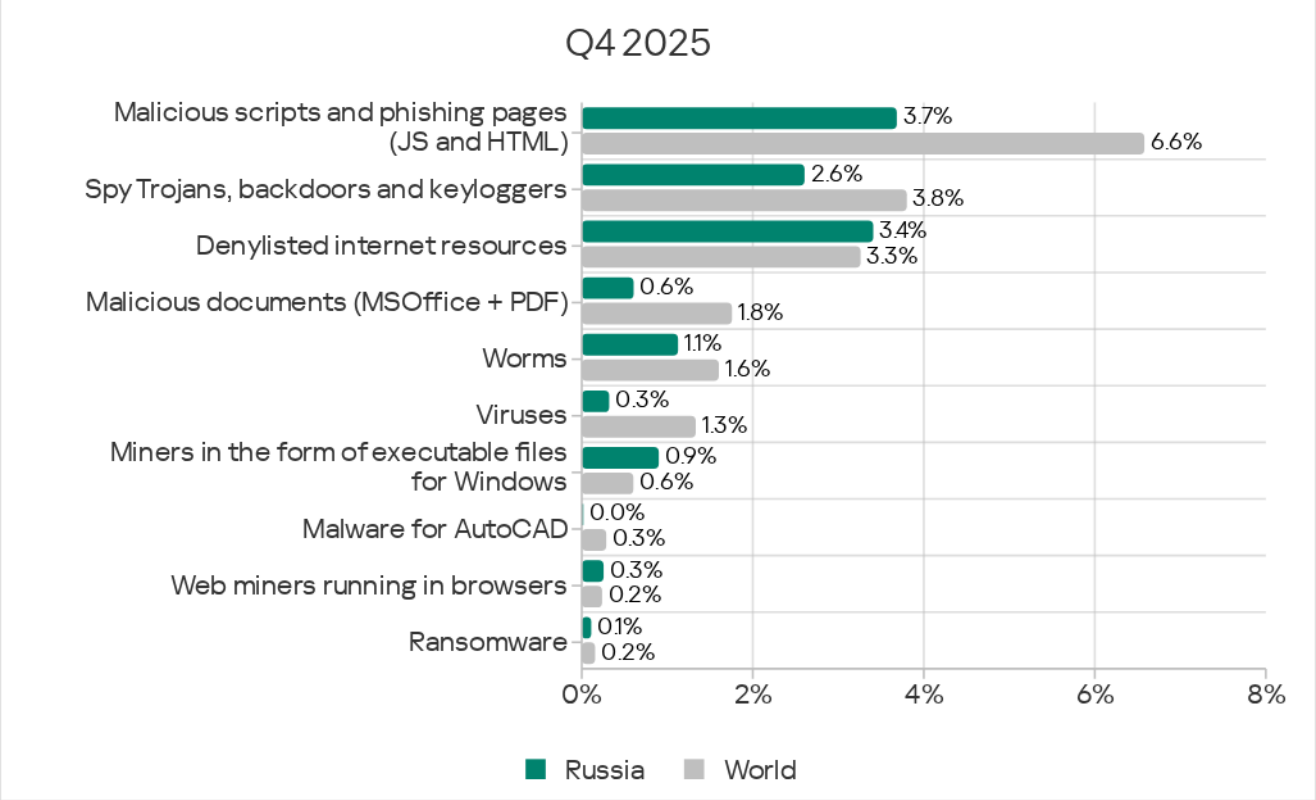
Russia ranked 11th, with 0.018%, in the regional ranking by percentage of ICS computers on which threats were blocked in network folders. This figure was 2.6 times higher than in Northern Europe, which had the lowest value among all regions.

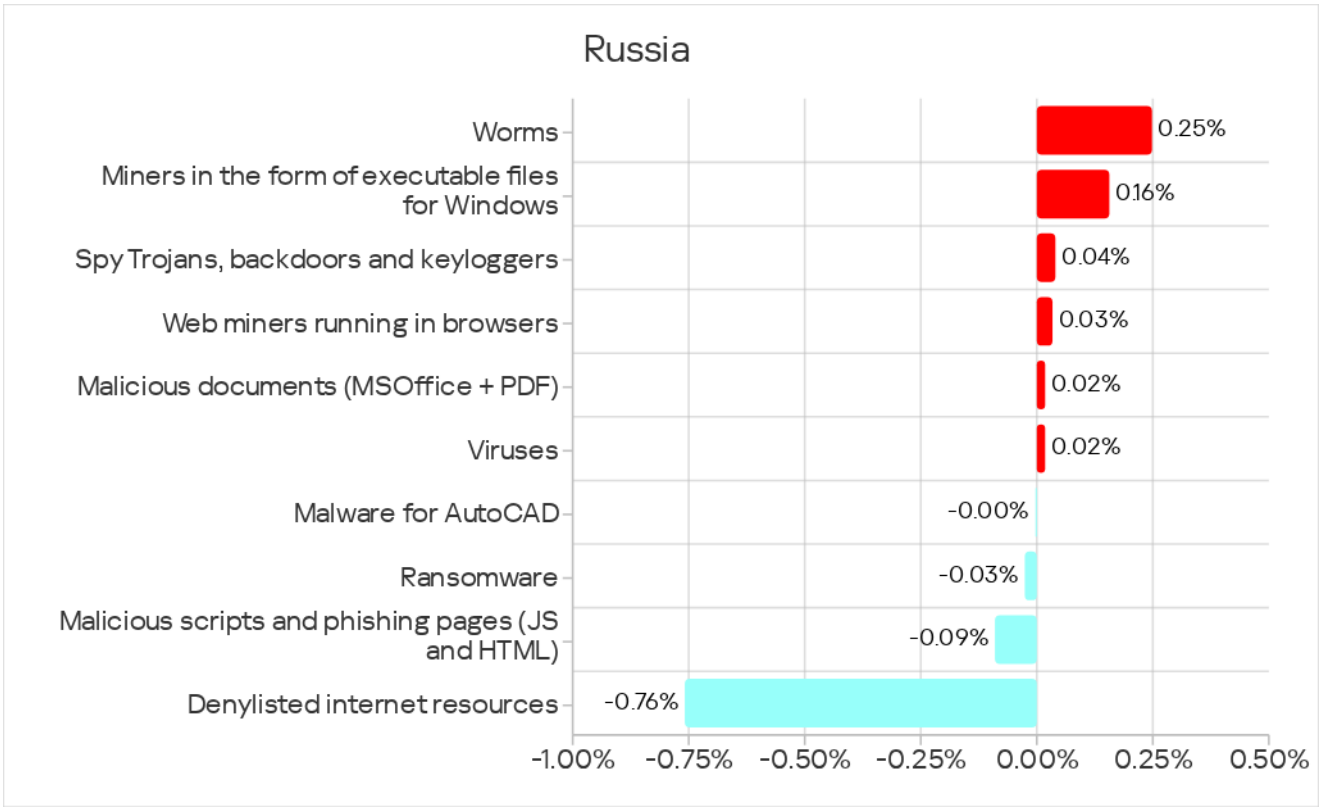


The main categories of threats blocked in network folders in Q4 2025 were worms, viruses, spyware, and miners in the form of executable files for Windows.



Threat categories





In Russia, the percentage of ICS computers on which malicious objects were blocked exceeds the global average for three threat categories:

- Denylisted internet resources – third place among regions by percentage of ICS computers on which this threat was blocked.
- Miners in the form of executable files for Windows – 1.5 times higher, second place among regions based on this parameter.
- Web miners – 1.1 times higher, fourth place among regions based on this parameter.

Over the quarter, the percentage increased for worms, both miner categories, spyware, malicious documents, and viruses.

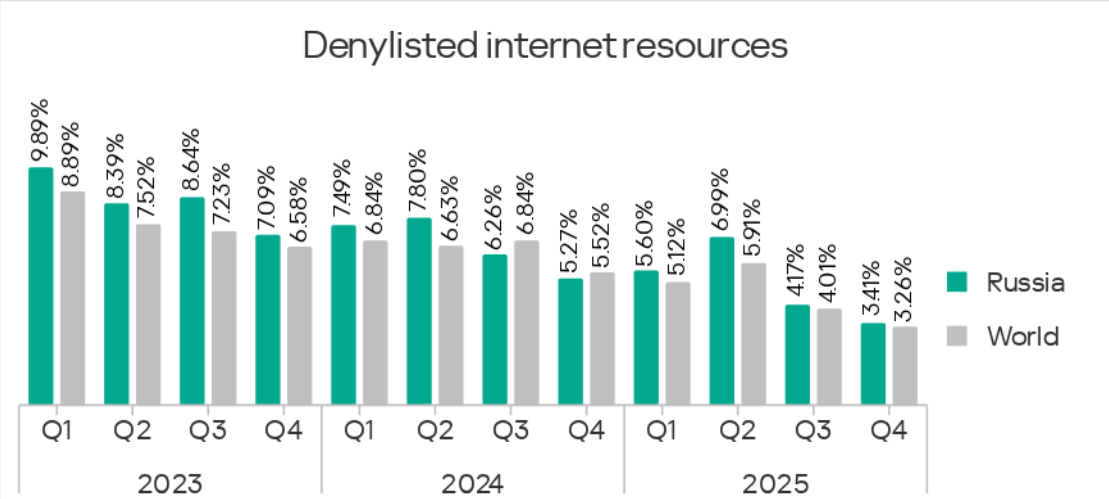
Russia ranked first among regions based on the increase in the percentage figure for miners in the form of executable files.

Denylisted internet resources

In Q4 2025, Russia rose from fourth to third place in the ranking of regions by percentage of ICS computers on which denylisted internet resources were blocked.

At the same time, denylisted internet resources ceded first place to malicious scripts and phishing pages in the regional threat category rankings, even though Russia ranked 13th in the regional ranking for scripts.

The percentage of ICS computers on which denylisted internet resources were blocked is gradually decreasing in Russia, as it is in all regions of the world. In Q4, Russia's figure was 3.41%, 2.0 times higher than Northern Europe's, which ranked last among all regions.



Among the industries under review in the region, the highest percentage for the denylisted internet resources category was in the electrical energy industry.

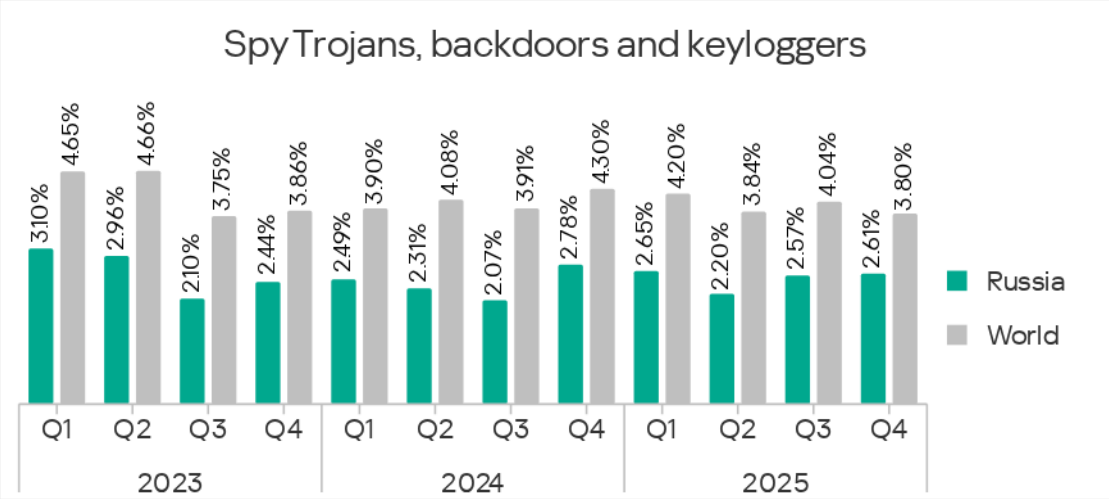
By percentage of ICS computers on which denylisted internet resources were blocked in various industries, Russia ranked among regions as follows:

- First place based on the percentage in building automation;
- Second place based on the percentage in biometric systems;
- Third place based on the percentage in the electric power industry.

Spy Trojans, backdoors, and keyloggers

In Q4 2025, Russia ranked ninth among regions by percentage of ICS computers on which spyware is blocked.

The percentage of ICS computers on which spyware was blocked in Russia increased to 2.61%. This was 2.1 times higher than in Northern Europe, which had the lowest value among regions.



Spyware is distributed through all threat sources. Most often – via email and the internet.

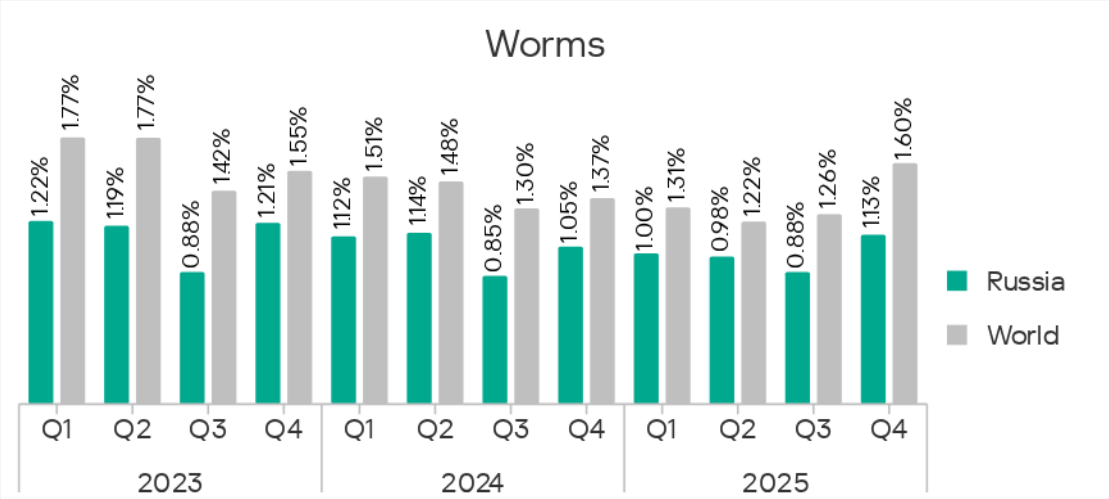
Russia was one of the two regions where the percentage figures for spyware increased over the quarter.

The percentage of ICS computers on which spyware was blocked increased in four of the industries under review in the region: oil and gas, construction, electric power, and engineering and ICS integrators. The oil and gas industry ranked first in terms of the increase in this percentage.

Worms

In Russia, worms ranked fourth in the regional threat category ranking. Apart from Russia, worms were in such a high position in the regional rankings only in Africa, South Asia, and Central Asia and the South Caucasus.

Russia ranked 10th among regions by percentage of ICS computers on which worms were blocked. The figure for Russia, 1.13%, was 3.5 times than in Northern Europe, which had the lowest value among regions.



For worms, removable media are the main distribution channel.

In Q4 2025, the percentage figures for worms increased across all regions due to a global phishing campaign known as Curriculum-vitae-catalina, as mentioned above. Unlike other regions, where the phishing campaign led to higher percentages of worms being blocked on ICS computers in email than on removable media, removable media remained the main source of worms in Russia.

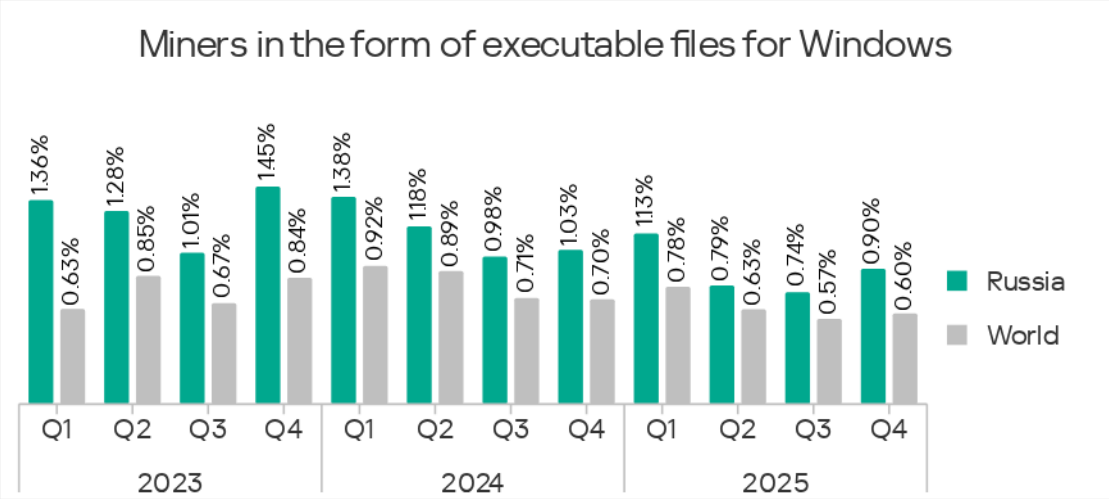
The percentage of ICS computers on which worms were blocked increased in all industries under review in the region except manufacturing and biometric systems. Building automation saw the highest increase in this percentage.

Miners in the form of executable files for Windows

Russia ranked second among regions by percentage of ICS computers on which miners in the form of executable files for Windows were blocked, behind only Central Asia and the South Caucasus.

Russia was one of the four regions that saw an increase in the percentage of ICS computers on which miners of this category were blocked. In fact, Russia ranked first by the increase in this percentage.

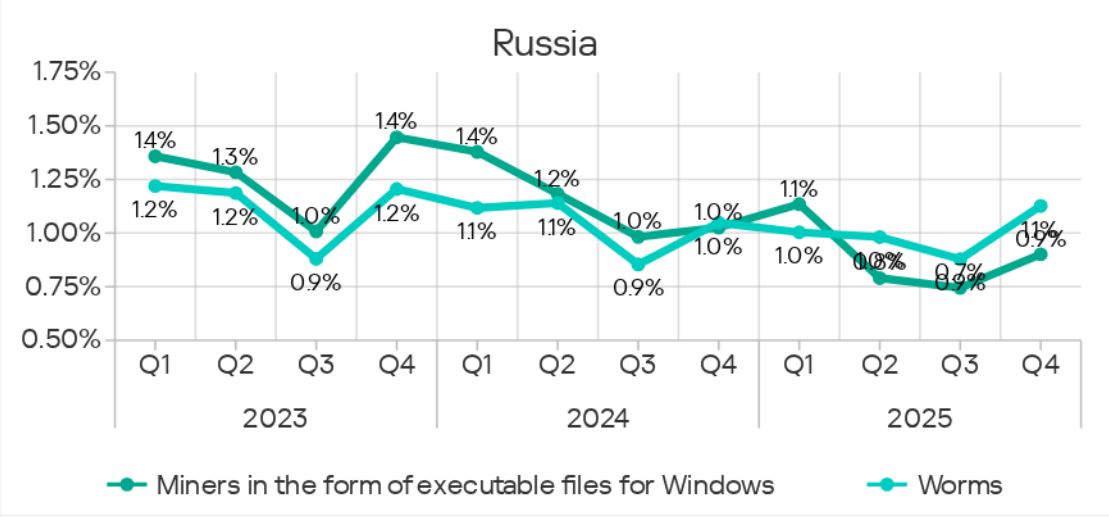
In Q4 2025, the percentage figures for miners in the form of executable files for Windows in Russia increased to 0.90%. This value was 6.4 times higher than in North America (Canada), which had the lowest value among regions.



The percentage of ICS computers on which miners in the form of executable files were blocked increased across all industries under review in the region. Manufacturing and electric power lead in terms of the increase in this percentage.

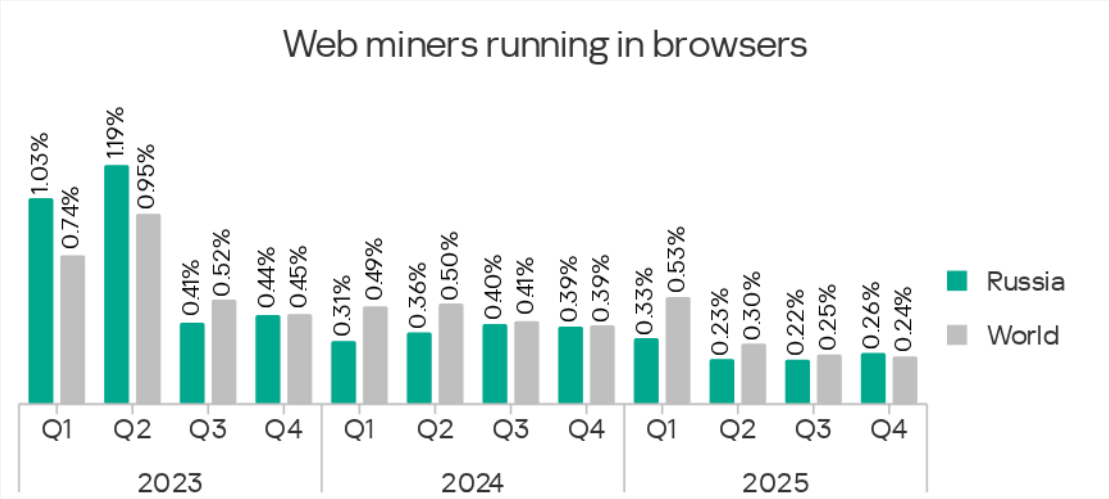
In Russia, miners for Windows extensively use modules and components that are essentially worms, designed to deliver the miner to other computers on the network as part of automated lateral movement.

Miners in the form of executable files for Windows are distributed primarily online, and also via removable media and network folders, leveraging worm functionality. That is why miners in the form of executable files and worms in Russia show similar dynamics.



Web miners

Russia ranked fourth among regions by percentage of ICS computers on which web miners were blocked, at 0.26%. This was 4.3 times higher than in East Asia, which ranked lowest.

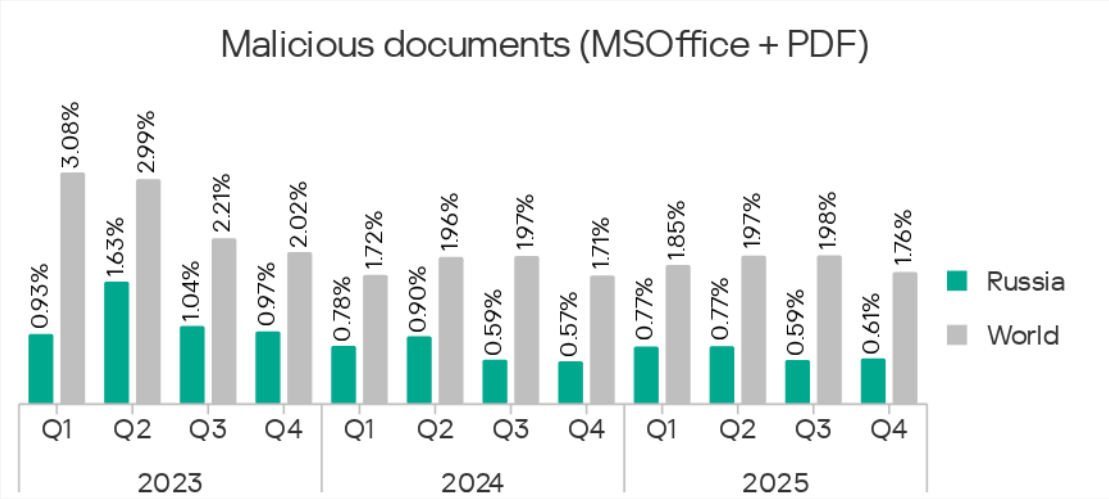


Russia was one of three regions where the percentage of ICS computers on which web miners were blocked increased in Q4 2025.

This threat's percentage figures increased in four of the industries under review in the region: manufacturing, oil and gas, building automation, and biometric systems. Manufacturing ranked highest in terms of the growth of this percentage.

Malicious documents

Russia ranked 13th among regions by percentage of ICS computers on which malicious documents were blocked, at 0.61%. This was 1.3 times higher than in Northern Europe, which ranked last.



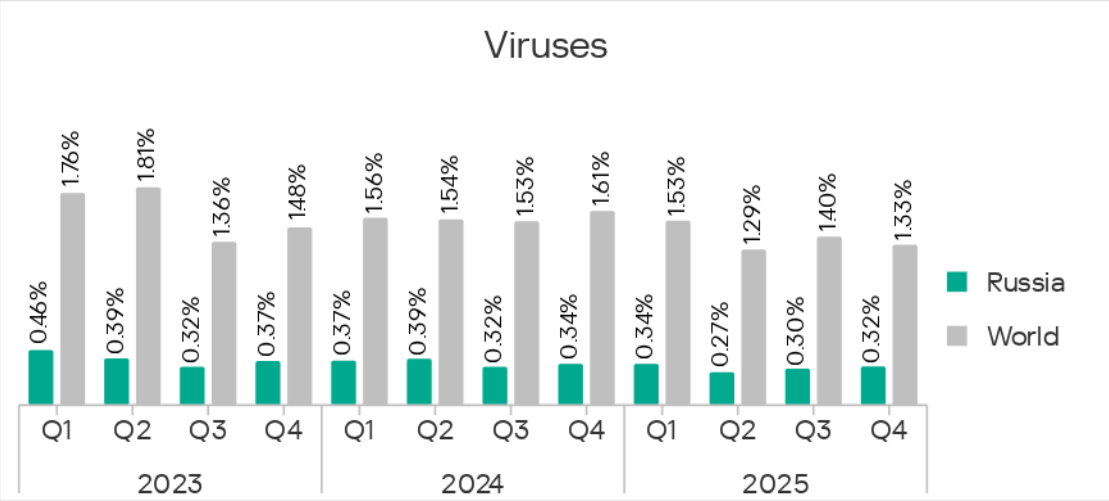
Russia was one of three regions where the percentage of ICS computers on which malicious documents were blocked increased over the quarter.

The percentage increased in two of the industries under review in the region – oil and gas, and electric power.

The main sources of malicious documents were email clients (primarily) and the internet.

Viruses

Russia ranked ninth among regions by percentage of ICS computers on which viruses were blocked, with 0.14%. This was 2.1 times higher than in Western Europe, which had the lowest percentage of all regions.



Russia was one of four regions where the percentage of ICS computers on which viruses were blocked increased in Q4 2025.

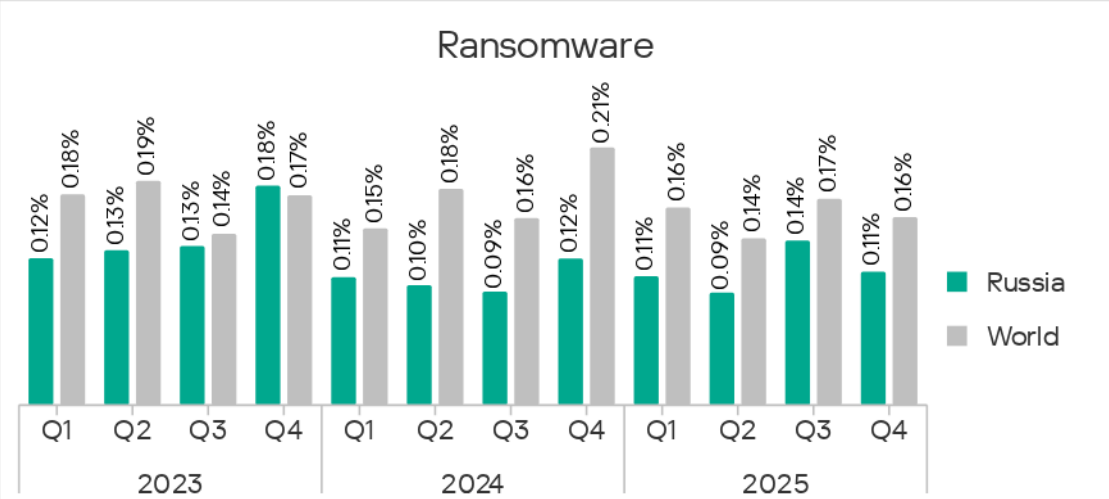
The percentage figures for viruses increased in all industries under review in the region except construction and manufacturing. Biometric systems lead in terms of the increase in this percentage.

In Q4 2025, viruses were distributed via all sources in Russia, most often via the internet.

Ransomware

Russia ranked ninth among regions by percentage of ICS computers on which ransomware was blocked, with 0.11%. This was 2.2 times higher than in Northern Europe, which ranked lowest.

The percentage figure for the region fluctuates. After increasing in Q3 2025, it decreased in Q4.



Russia ranked sixth or higher in the regional rankings by percentage of ICS computers on which ransomware was blocked in the industries under review. Russia ranked second for biometric systems and third for the electric power and oil and gas industries.

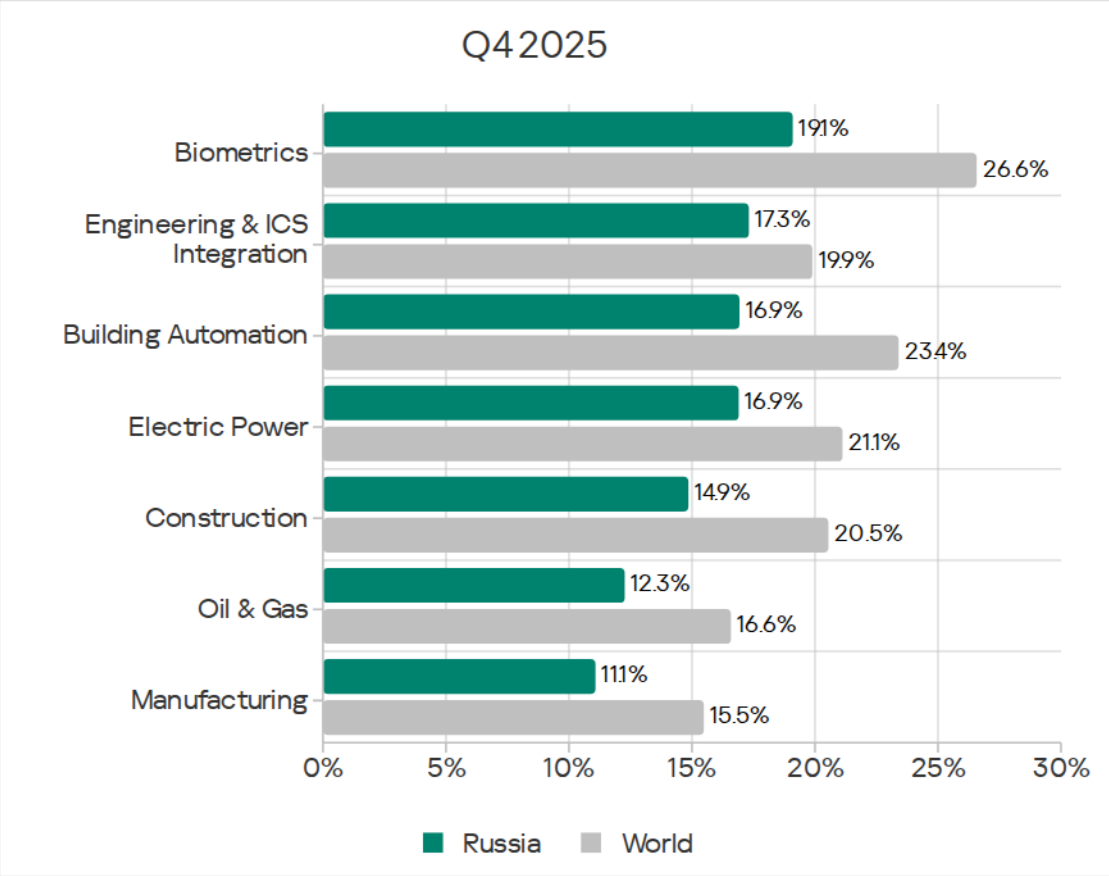
Despite a decrease in the average value for Russia in Q4, the percentage of ICS computers on which ransomware was blocked increased in all industries under review in the region except construction and building automation. Biometric systems lead the ranking by the increase in this indicator.

In Q4 2025, ransomware in Russia was distributed via the internet and email.

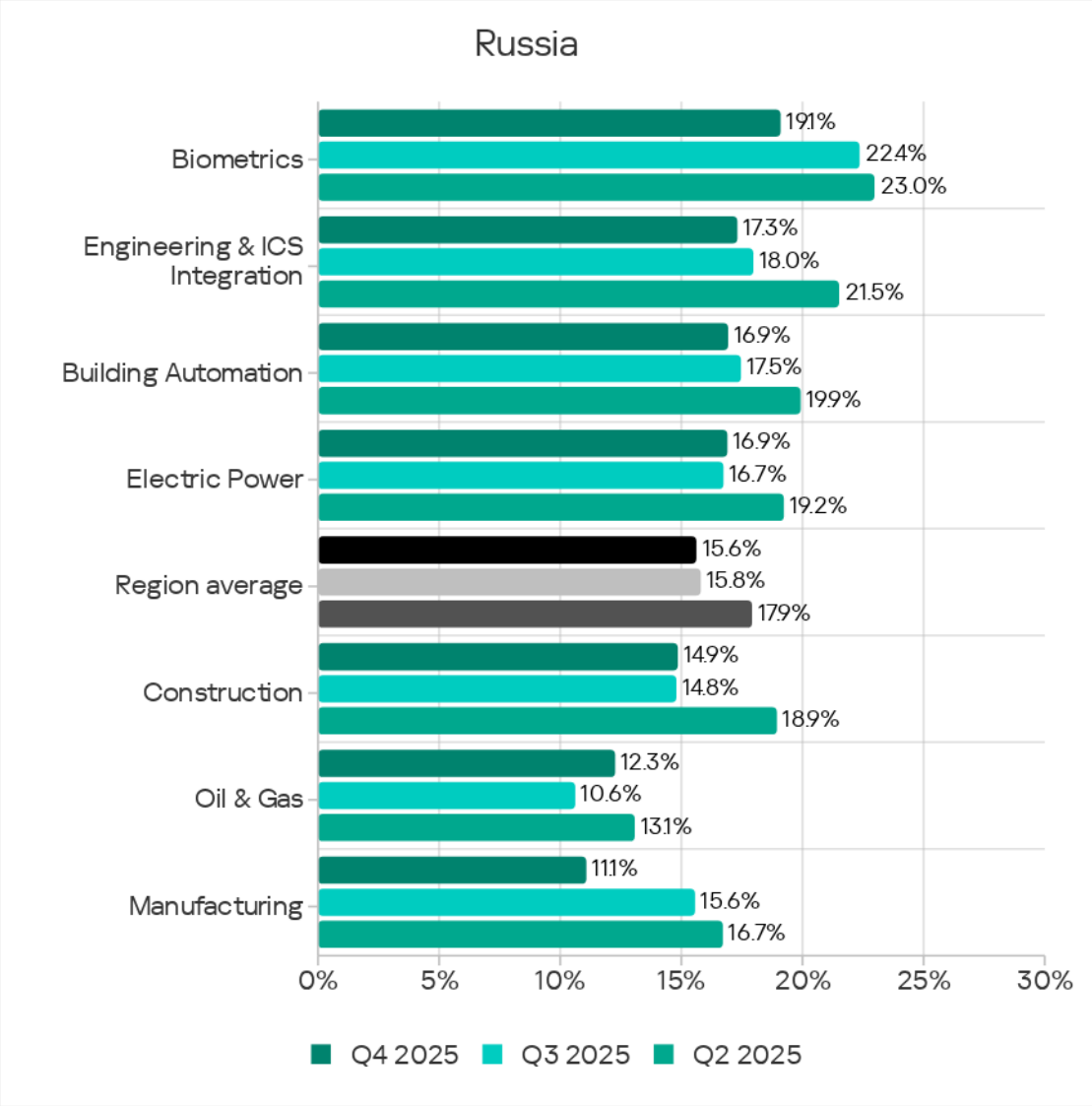
Industries

In Russia, of all the industries covered in this report, malicious objects were most often blocked in biometric systems.

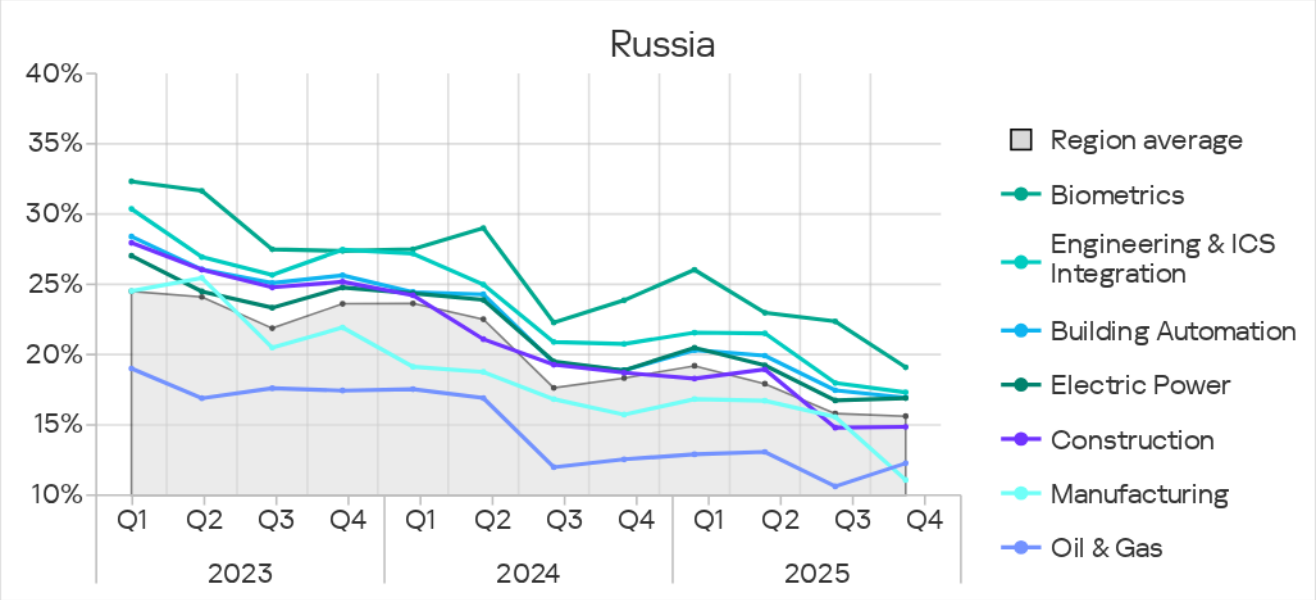
In all industries in the region, the percentage of ICS computers on which malicious objects were blocked was below the corresponding global averages.



In Q4 2025, among all industries under review in the region, the percentage of ICS computers on which malicious objects were blocked increased in the electrical energy, construction, and oil and gas industries.



Across all industries under review, the percentage figures are gradually decreasing, with periodic fluctuations.



Threat sources and malware categories in industries: 'hotspots'

We use heat maps when assessing threats to industries in the regions. The color on the heatmap indicates the position in the global industry rankings across regions for each individual threat category or source. Red signifies that the figure is close to the maximum.

Threat source indicators for industries in Russia, Q4 2025

Industry / Threat source	Biometrics	Building Automation	Engineering & ICS Integration	Electric Power	Oil & Gas	Construction	Manufacturing	Category metric in region
Internet	5.92%	6.24%	6.55%	6.77%	4.28%	6.37%	3.62%	5.78%
Email clients	2.57%	1.54%	0.73%	1.14%	0.94%	0.74%	0.49%	0.66%
Removable media	0.55%	0.23%	0.21%	0.39%	0.25%	0.36%	0.23%	0.17%
Network folders	0.08%	0.04%	0.01%	0.03%	0.06%	0.03%	—	0.02%
Industry metric in region	19.10%	16.93%	17.31%	16.90%	12.27%	14.85%	11.08%	

Threat category indicators for industries in Russia, Q4 2025

Industry / Threat type	Biometrics	Building Automation	Engineering & ICS Integration	Electric Power	Oil & Gas	Construction	Manufacturing	Category metric in region
Denylisted internet resources	4.21%	3.94%	3.77%	4.61%	2.92%	4.06%	2.66%	3.41%
Malicious scripts and phishing pages (JS and HTML)	5.38%	4.33%	4.15%	4.40%	3.00%	4.41%	2.36%	3.68%
Malicious documents (MSOffice + PDF)	1.56%	1.23%	0.77%	1.42%	1.19%	0.67%	0.68%	0.61%
Spy Trojans, backdoors and keyloggers	3.82%	3.47%	2.80%	3.16%	2.10%	2.61%	1.83%	2.61%
Ransomware	0.78%	0.32%	0.14%	0.34%	0.29%	0.21%	0.13%	0.11%
Miners in the form of executable files for Windows	1.09%	1.06%	1.11%	1.58%	0.78%	1.21%	0.89%	0.90%
Web miners running in browsers	0.55%	0.39%	0.34%	0.61%	0.38%	0.62%	0.45%	0.26%
Malware for AutoCAD	0.08%	0.02%	0.04%	0.03%	0.12%	0.10%	0.08%	0.02%
Worms	1.56%	1.57%	1.04%	1.69%	1.32%	1.24%	1.15%	1.13%
Viruses	0.94%	0.50%	0.50%	1.03%	0.59%	0.59%	0.49%	0.32%
Industry metric in region	19.10%	16.93%	17.31%	16.90%	12.27%	14.85%	11.08%	

The internet is the main source of threats for all industries. As a consequence, the relevant threat categories include links to denylisted internet resources, malicious scripts and phishing pages, and spyware, which are all distributed via this threat source.

By percentage of ICS computers on which **denylisted internet resources** were blocked in various industries, Russia ranked among regions as follows:

- First place in the building automation industry based on this percentage.
- Second place in biometric systems.
- Third place in the electric power industry.

High percentage figures for miners. Russia ranked third or higher in regional rankings based on percentage figures for both miner categories across all industries except manufacturing.

In the manufacturing industry, Russia ranked third based on the percentage figures for miners in the form of executable files for Windows and fourth based on the percentage figures for web miners.

The percentage of ICS computers on which miners in the form of executable files were blocked increased over the quarter across all industries under review in the region, with the greatest increase observed in the manufacturing industry.

High percentage figures for ransomware. By percentage of ICS computers on which ransomware was blocked, Russia ranked among regions as follows:

- Second place in biometric systems.
- Third place in the electrical energy and oil and gas industries.
- Fourth place in the building automation and construction industries.
- Fifth place in the engineering and ICS integrators industry.

Russia ranked sixth based on its percentage figure for ransomware in the manufacturing industry.

The percentage of ICS computers on which ransomware was blocked increased over the quarter in all industries under review in the region except construction and building automation.

Biometrics

Russia ranked ninth in the regional rankings by percentage of ICS computers on which malicious objects were blocked in biometric systems.

Based on the percentage figures for biometric systems, Russia ranked as follows among regions:

- Second place based on the percentage of ICS computers on which threats of the following categories were blocked: denylisted internet resources, both miner categories, and ransomware.

Among industries in the region, biometric systems ranked as follows:

- First place based on percentage figures for all threat sources except the internet.
- First place by percentage of ICS computers on which the following threat categories were blocked: malicious scripts and phishing pages, malicious documents, spyware, and ransomware.

- Second place based on percentage figures for denylisted internet resources and viruses.
- Third place based on percentage figures for worms, web miners, and malware for AutoCAD.

Engineering and ICS integrators

Russia ranked eighth among regions by percentage of ICS computers on which malicious objects were blocked in the engineering and ICS integrators industry.

Based on percentage figures for this industry, Russia ranked among regions as follows:

- First place by percentage of ICS computers on which miners in the form of executable files for Windows were blocked.
- Second place based on percentage figures for web miners.

The engineering and ICS integrators industry ranked among industries in the region as follows:

- Second place for internet threats.
- Third place by percentage of ICS computers on which miners in the form of executable files for Windows were blocked.

Building automation

Russia ranked 10th among regions by percentage of ICS computers on which malicious objects were blocked in the building automation industry.

Based on percentage figures for this industry, Russia ranked among regions as follows:

- First place by percentage of ICS computers on which denylisted internet resources and web miners were blocked.
- Second place by percentage of ICS computers on which miners in the form of executable files for Windows were blocked.

Building automation ranked among industries in the region as follows:

- Second place for email threats.
- Third place for threats in network folders.
- Second place by percentage of ICS computers on which malicious documents and ransomware were blocked.
- Third place based on percentage figures for malicious documents and ransomware.

Electric power

Russia ranked ninth among regions by percentage of ICS computers on which malicious objects were blocked in the electric power industry.

Based on percentage figures for this industry, Russia ranked among regions as follows:

- Second place by percentage of ICS computers on which both miner categories were blocked.
- Third place by percentage of ICS computers on which denylisted internet resources and ransomware were blocked.

The electrical energy industry ranked among industries in the region as follows:

- First place by percentage of ICS computers on which internet threats were blocked.
- Second place based on the percentage figures for removable media;
- Third place for threats from email clients.
- First place by the percentage of ICS computers on which malicious documents, web miners, and ransomware were blocked.
- Second place based on percentage figures for the following threat categories: malicious documents, web miners, and ransomware.
- Third place based on percentage figures for malicious scripts and phishing pages, as well as spyware.

Construction

Russia ranked 10th among regions by percentage of ICS computers on which malicious objects were blocked in the construction industry.

Based on percentage figures for this industry, Russia ranked among regions as follows:

- Second place by percentage of ICS computers on which both miner categories were blocked.

Construction ranked among industries in the region as follows:

- Third place by percentage of ICS computers on which threats from the internet and from removable media were blocked.
- First place by percentage of ICS computers on which web miners were blocked.
- Second place based on percentage figures for the following threat categories: malicious scripts and phishing pages, miners in the form of executable files, and malware for AutoCAD.

- Third place based on percentage figures for denylisted internet resources and viruses.

Oil and gas

Russia ranked fifth among the five regions that have an oil and gas industry, in terms of the percentage of ICS computers on which malicious objects were blocked in this industry.

Based on percentage figures for this industry, Russia ranked among regions as follows:

- First place based on percentage figures for threats in network folders – this is the only region where such threats were blocked on ICS computers in the oil and gas industry.
- Second place by percentage of ICS computers on which malicious documents and both miner categories were blocked.
- Third place by percentage of ICS computers on which ransomware was blocked.

The oil and gas industry ranked among industries in the region as follows:

- Second place by percentage of ICS computers on which threats in network folders were blocked.
- First place by percentage of ICS computers on which malware for AutoCAD was blocked.

Manufacturing

Russia ranked 11th by percentage of ICS computers on which malicious objects were blocked in the manufacturing industry.

Based on percentage figures for this industry, Russia ranked among regions as follows:

- Third place by percentage of ICS computers on which miners in the form of executable files for Windows were blocked, and fourth place by the percentage for web miners.

Methodology used to prepare statistics

This report presents the results of analyzing statistics obtained with the help of Kaspersky Security Network (KSN). The data was received from KSN users who consented to its anonymous sharing and processing for the purposes described in the KSN Agreement for the Kaspersky product installed on their computer.

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

Data shared by the user contains only the data types and categories described in the appropriate KSN Agreement. This data helps to a significant extent in analyzing the threat landscape and serves as a prerequisite for detecting new threats including targeted attacks and 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
- 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, the food industry, light industry, pharmaceuticals. This also includes systems from engineering and integration firms that work with enterprises in a variety of industries,

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

as well as building management systems, physical security, and biometric data processing.

We consider a computer to have been attacked if a Kaspersky security solution blocked one or more threats on that computer during the review period: 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 review period 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