Kaspersky ICS CERT

Threat landscape for industrial automation systems

Russia. Q3 2025

22.12.2025 Version 1.0

Russia

Current threats

The main source of threats in Russia is the internet

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

The list of denylisted internet resources is used to prevent initial infection attempts. In particular, the following threats on ICS computers are blocked with the aid of this list:

- Known malicious URLs and IP addresses used by attackers to host malicious payloads and configurations;
- Suspicious (untrustworthy) web resources with entertaining or gaming content, 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, 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 these resources is used for spreading malicious scripts and phishing pages (HTML).

High values of the indicator typically point to:

- Weak control over the implementation of information security policies (ICS computers are internet-facing in some capacity);
- Failings in the information security culture (employees access unsafe internet resources).

Miners in the form of executable files for Windows and worms

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

In Q3 2025, worms were fourth in the threat category rankings for Russia. Besides Russia, only the Central Asia and South Caucasus region has such a high position for this threat category.

The dynamics of these two threat categories in Russia are strikingly similar. This is because miners for Windows actively use modules and components that are essentially worms and serve to deliver the miner to other computers in the network (automated lateral movement).

Miners threaten every industry in the region: Russia consistently ranks no lower than fourth in regional rankings for both types of miners across all industries.

Ransomware

In terms of ICS computers where ransomware is blocked, Russia ranks seventh globally.

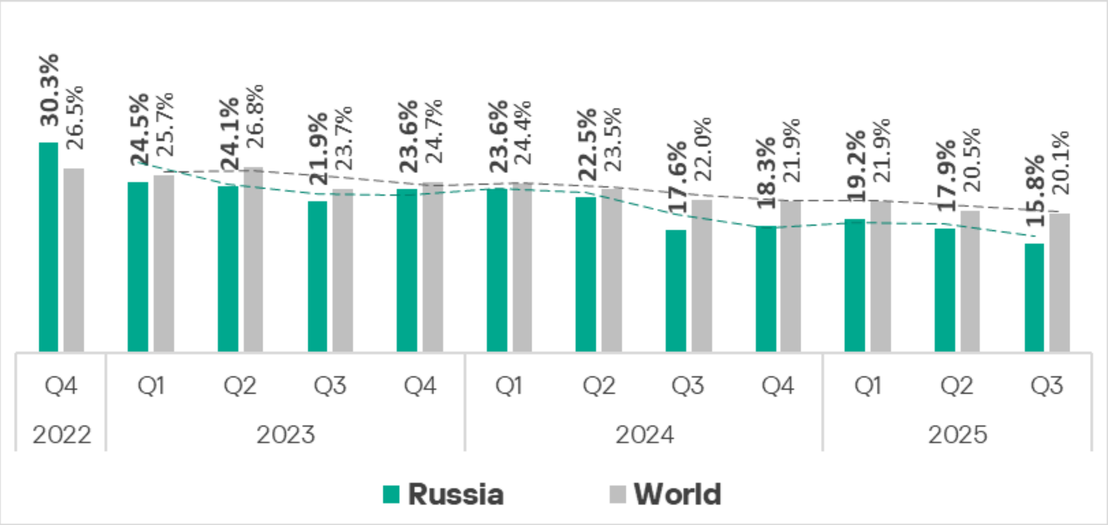
In Q3 2025, the prevalence of this threat in the region increased significantly, with Russia recording the second-highest growth rate globally.

The threat is relevant to building automation, oil and gas, and construction. Russia leads the regional cross-industry rankings for ransomware incidents in building automation, and holds second place in oil and gas industry and construction.

Statistics across all threats

Russia ranks 10th in the global ranking for the percentage of ICS computers on which malicious objects were blocked.

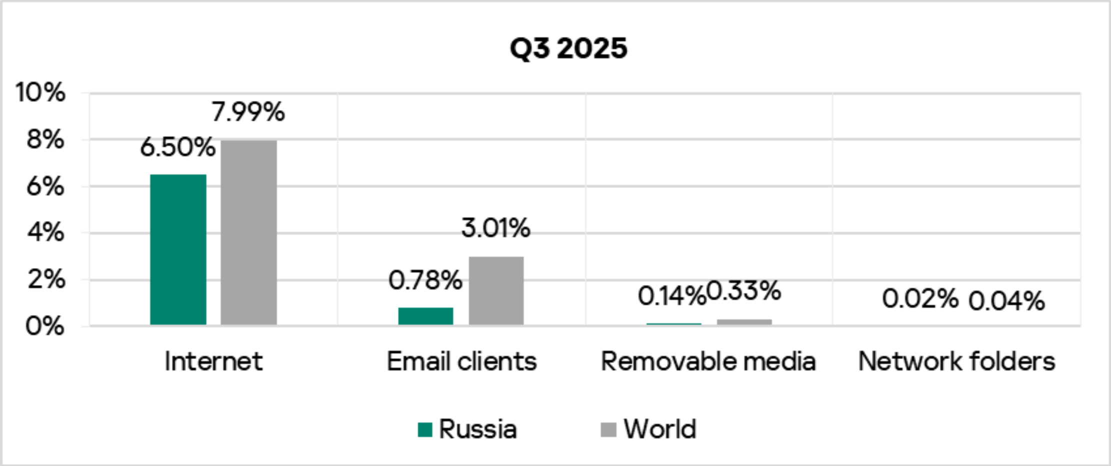
The region's figure has declined for two consecutive quarters. In Q3 2025, it reached a three-year low of 15.8%. This is 1.7 times higher than in Northern Europe, which is last in this ranking of regions.



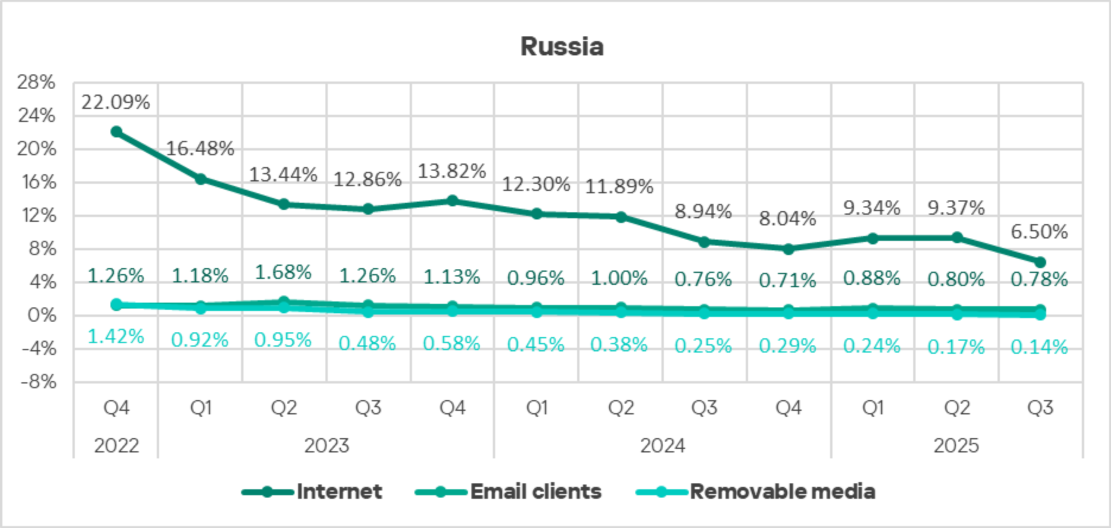
This indicator for the region has remained below the global average since the beginning of 2023.

Threat sources

The percentages of ICS computers in Russia on which threats from various sources are blocked, are lower than the global average.



The indicator decreased across all threat sources for the quarter.



Internet

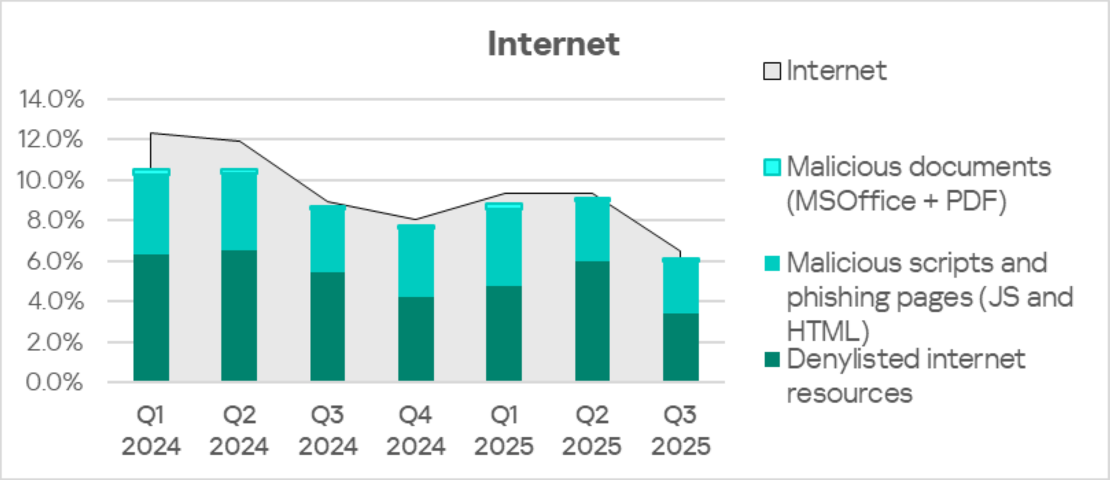
In the ranking of regions by percentage of ICS computers on which internet threats were blocked, Russia is in 10th place with 6.50%. Compared to the region that rounds off this ranking — Northern Europe — Russia scores 1.4 times higher.

In Russia, the percentage of ICS computers on which online threats were blocked increased during the first two quarters of 2025. In the third quarter, the figure declined by 2.87 p.p., to a three-year low.

It is notable that in Q3 2025, the percentage of ICS computers with blocked internet threats decreased across all regions, yet Russia experienced the largest change.

The main categories of internet threats blocked on ICS computers include denylisted internet resources, malicious scripts and phishing pages, as well as malicious documents.

Malicious scripts and phishing pages, as well as malicious documents are distributed both online and via email. Unlike malicious emails, however, malicious scripts and phishing pages in Russia during Q3 2025 were primarily distributed online.

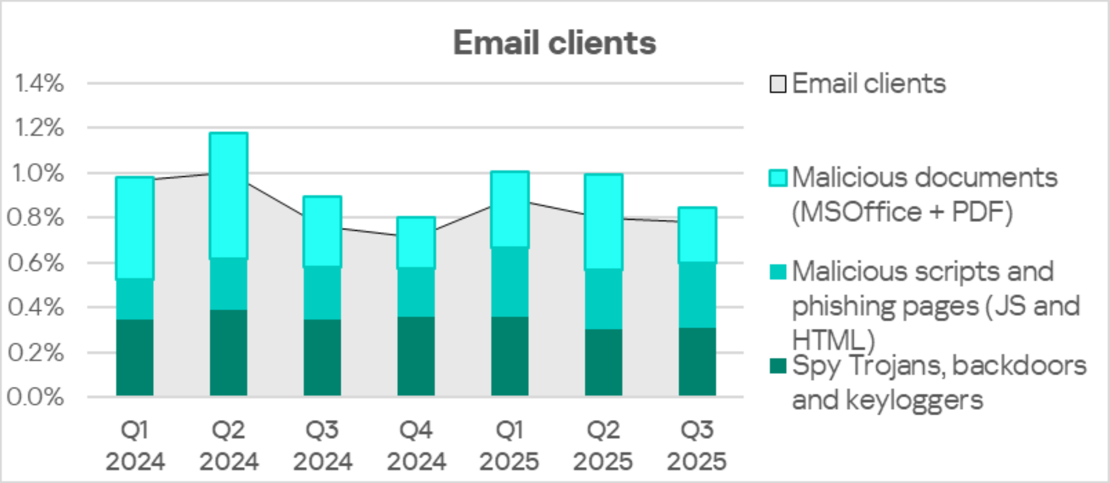


Email clients

The percentage of ICS computers on which email client threats were blocked in Q3 2025 was the lowest in Russia among all regions, 0.78%.

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

The main distribution channel for malicious documents and spyware is email. Malicious scripts are distributed both via email and online. In Q3 2025, the internet was the primary source of this threat.

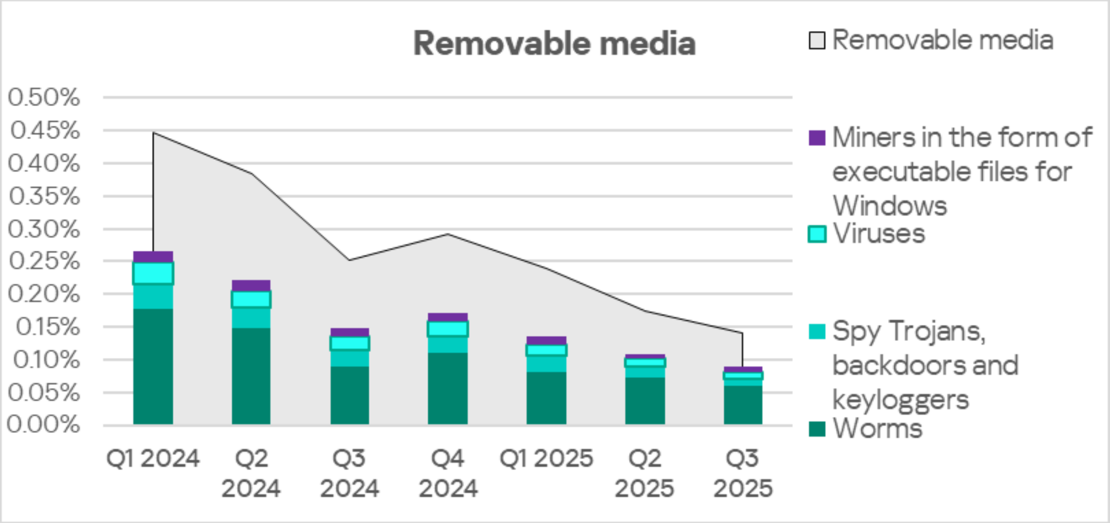


Removable media

By percentage of ICS computers on which removable media threats were blocked, Russia places eighth in the corresponding regional ranking with 0.14%. This figure is 2.8 times higher than in the Australia and New Zealand region, which props up the ranking.

The main categories of removable media threats blocked on ICS computers in the region are worms, spyware, viruses, and miners in the form of executable files for Windows.

The main distribution channel for worms is removable media.

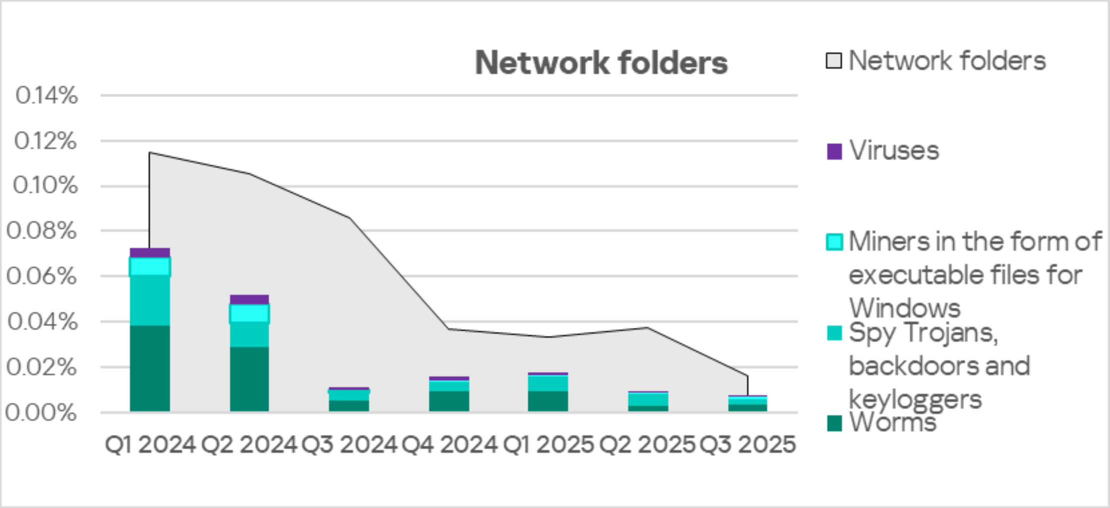


Network folders

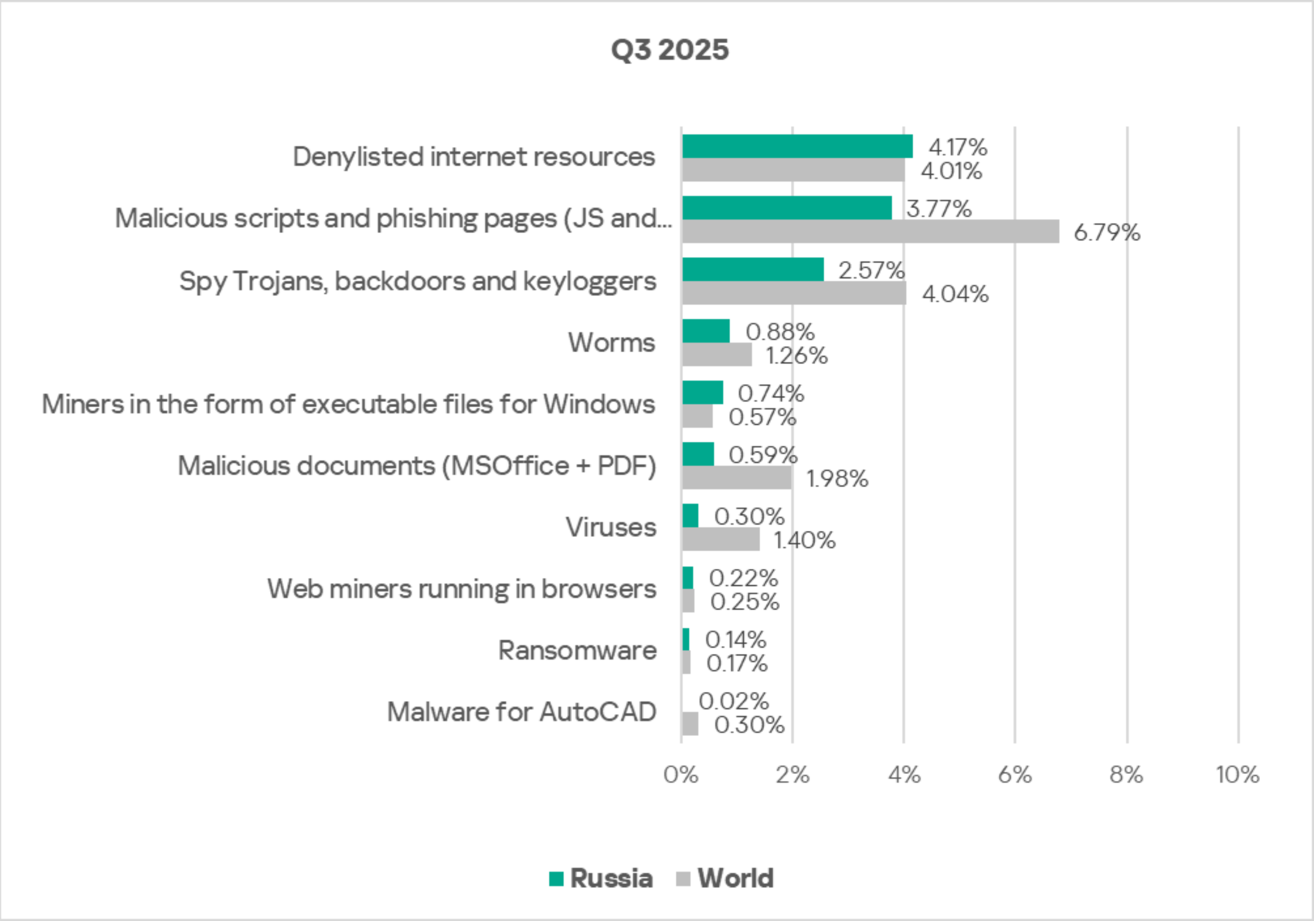
By percentage of ICS computers on which network folder threats were blocked, Russia is in 10th place in the corresponding regional ranking with 0.016%. This is

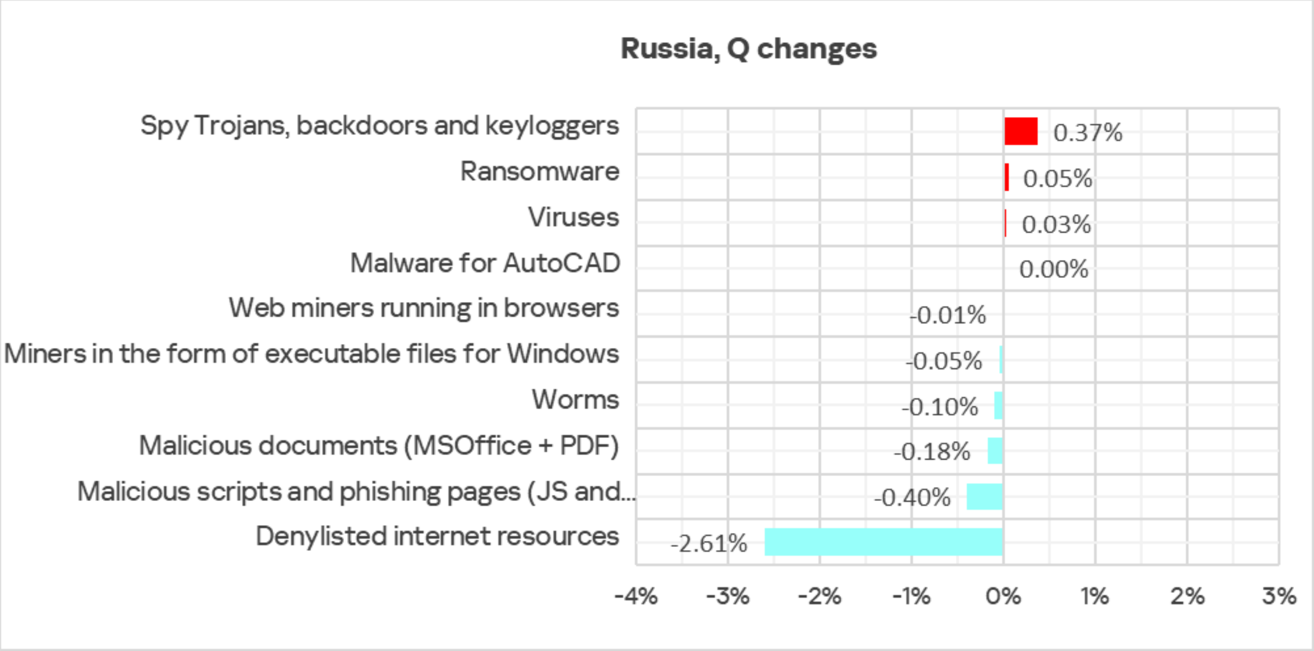
2.7 times more than in Northern Europe, which boasts the lowest percentage among all regions.

The main threat categories blocked within network folders during Q3 2025 were worms, spyware, viruses, and miners in the form of executable files for Windows.



Threat categories





In Russia, two threat categories show a higher percentage of ICS computers on which malicious objects were blocked than the global average: denylisted internet resources and miners in the form of executable files for Windows.

The figure for the first category is comparable to the global average. The percentage of ICS computers on which miners in the form of executable files for Windows are blocked exceeds the global average by a factor of 1.3. Russia is second in the regional rankings for this indicator.

During the quarter, three threat categories registered an increase in this indicator: spyware, ransomware, and viruses.

Russia ranked second in the respective regional rankings for the growth in spyware and ransomware in Q3 2025.

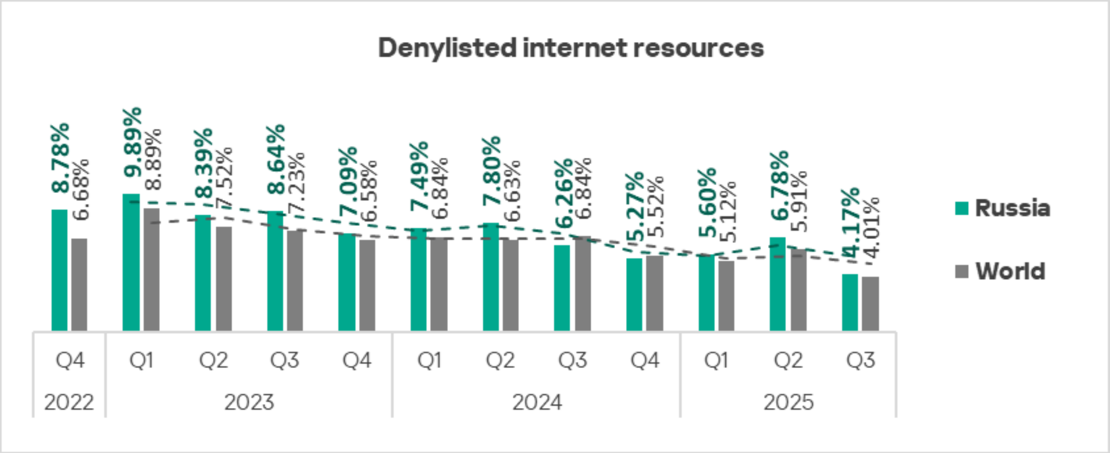
The largest quarterly decrease was observed for denylisted internet resources. Similar to online threats, Russia led all regions in the magnitude of change (decrease), even though the percentage of ICS computers blocking denylisted internet resources declined across all regions.

Despite this decrease, Russia ranks fourth in the regional standings in the percentage of ICS computers on which denylisted internet resources were blocked. This threat category retained its leading position within the region's threat category rankings.

Denylisted internet resources

In the regional rankings in the percentage of ICS computers on which denylisted internet resources are blocked, Russia dropped from second to fourth place.

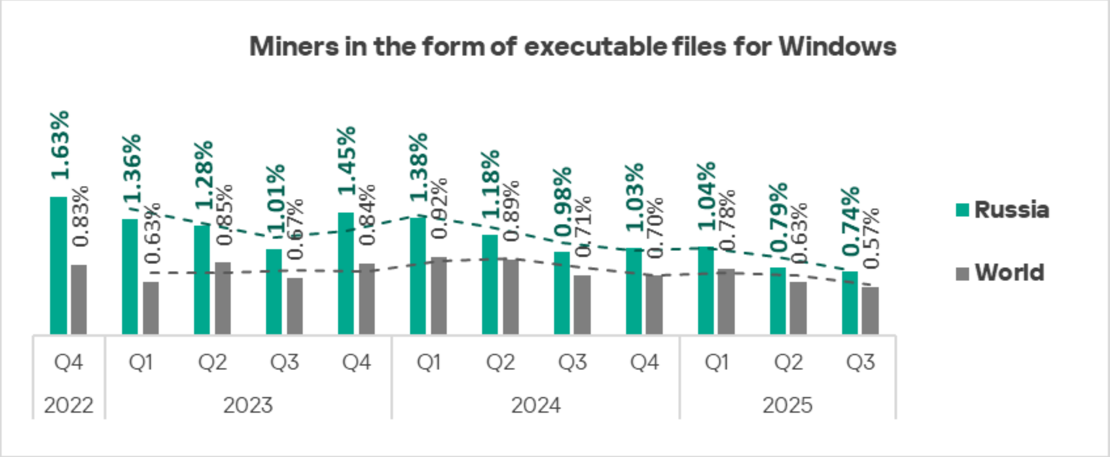
Denylisted internet resources maintained their position as the leading threat category within the region, despite a significant decrease to 4.17% in Q3 2025. The figure for Russia is 1.8 times higher than that for the Australia and New Zealand region, which ranks last in this category.



Miners in the form of executable files for Windows and worms

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

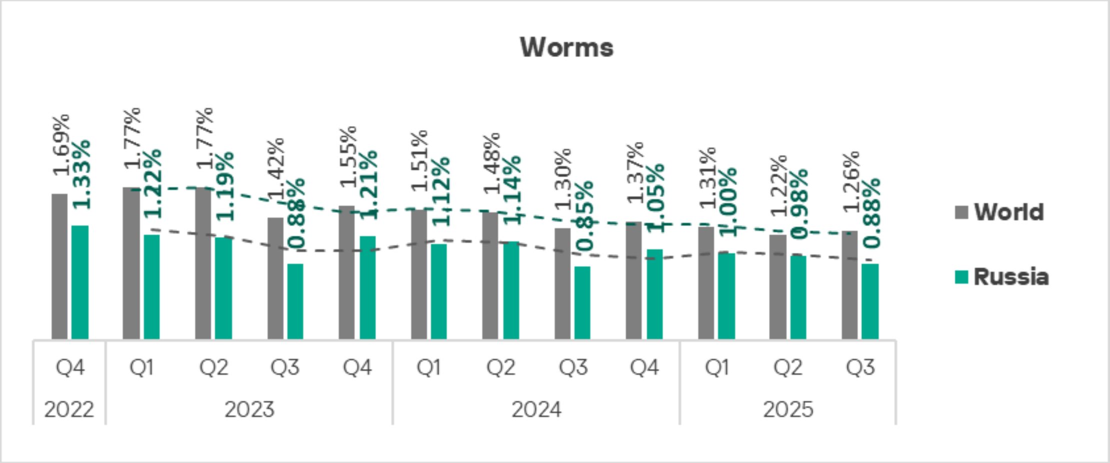
The figure for miners in the form of executable files for Windows decreased in Russia, as it did across all regions, in Q3 2025 The figure for Russia reached a three-year low of 0.74% This figure is 5.7 times higher than in the Australia and New Zealand region, which ranks last.



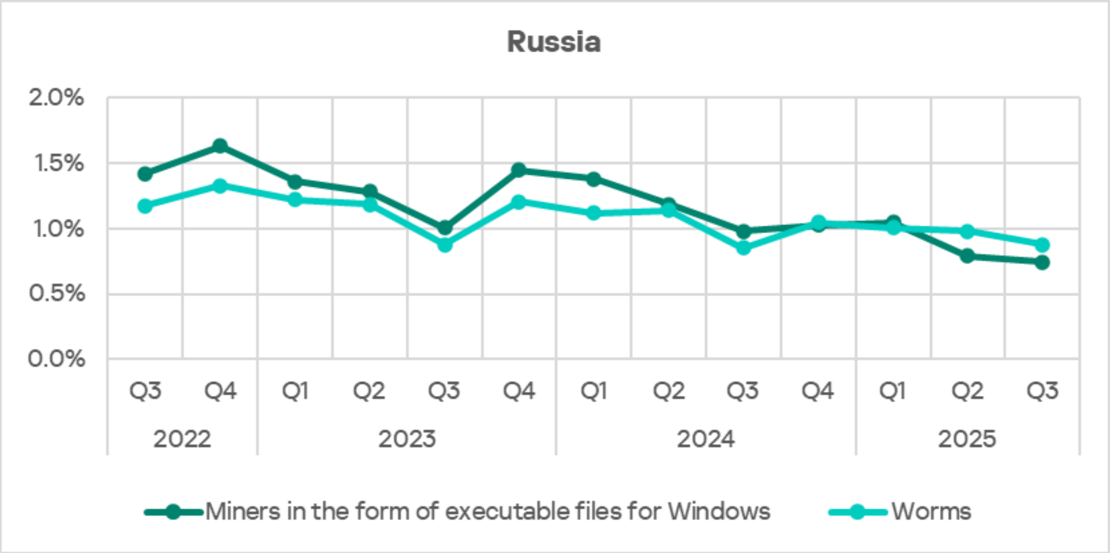
Miners in the form of executable files for Windows actively use modules and components that are essentially worms and serve to deliver the miner to other computers in the network (automated lateral movement).

In Q3 2025, worms were fourth in the threat category rankings for Russia. Apart from Russia, only in Central Asia and South Caucasus is this threat category in such a high position in the regional ranking. Russia holds eighth place in the regional rankings.

The figure for worms in Russia decreased to 0.88% during the quarter. This figure is four times higher than in Northern Europe, which has the lowest rate.



Miners in the form of executable files for Windows are distributed primarily online and through removable media and network folders, often leveraging worm functionality. That's why the indicators for miners in the form of executable files and for worms show similar dynamics in Russia.

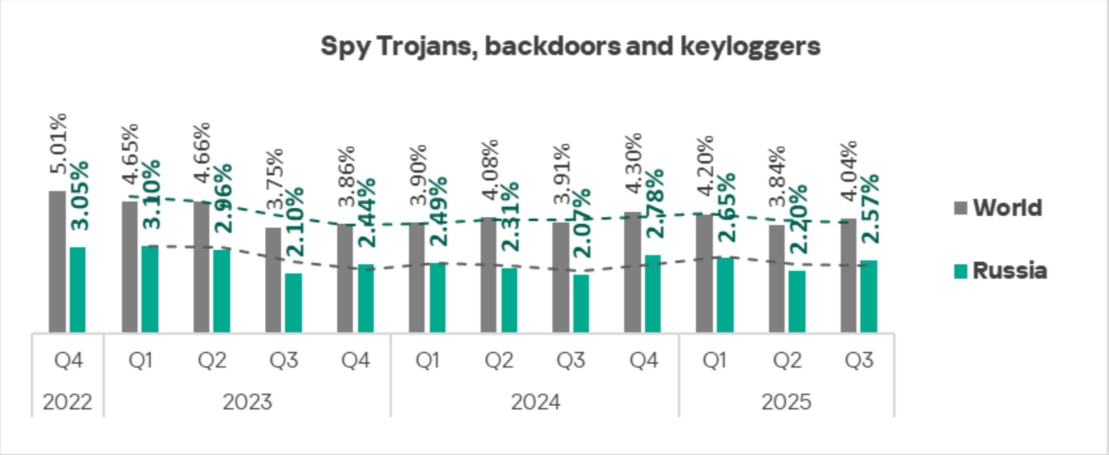


Spy Trojans, backdoors and keyloggers

In Q3 2025, Russia ranked tenth among regions for the percentage of ICS computers on which spyware is blocked.

Spyware is one of three threat categories in the region whose prevalence increased during the quarter. Russia ranked second globally for the growth rate of this indicator.

In Russia, the percentage of ICS computers blocking spyware (2.57%) is 1.8 times greater than in Northern Europe, which has the lowest figure among all regions.



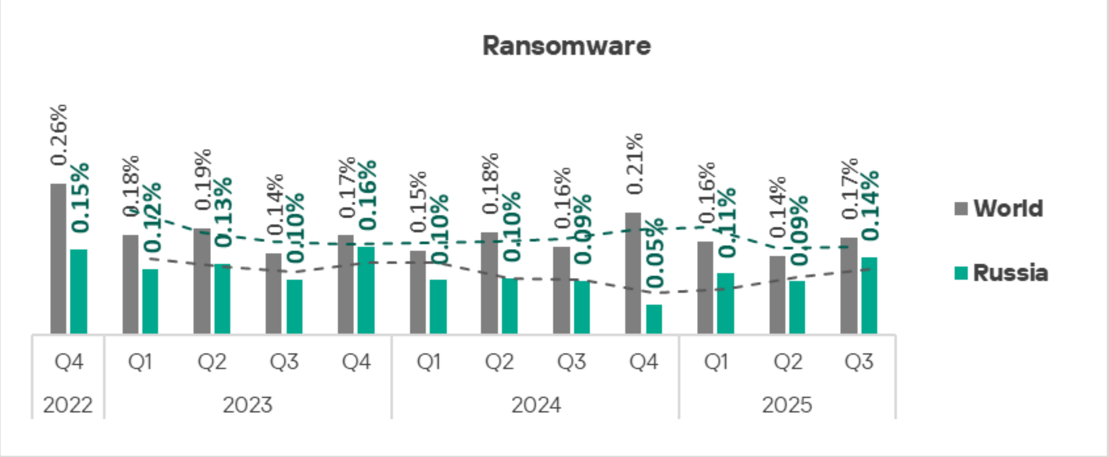
Spyware is distributed through all threat sources, most commonly via email and online.

Ransomware

In terms of ICS computers on which ransomware is blocked, Russia ranks seventh globally.

In Q3 2025, the prevalence of this threat in the region increased significantly, reaching 0.14% Russia ranked second among regions for its growth rate.

The percentage of ICS computers blocking ransomware in Russia is 2.8 times higher than in Northern Europe, which ranks last in this category.

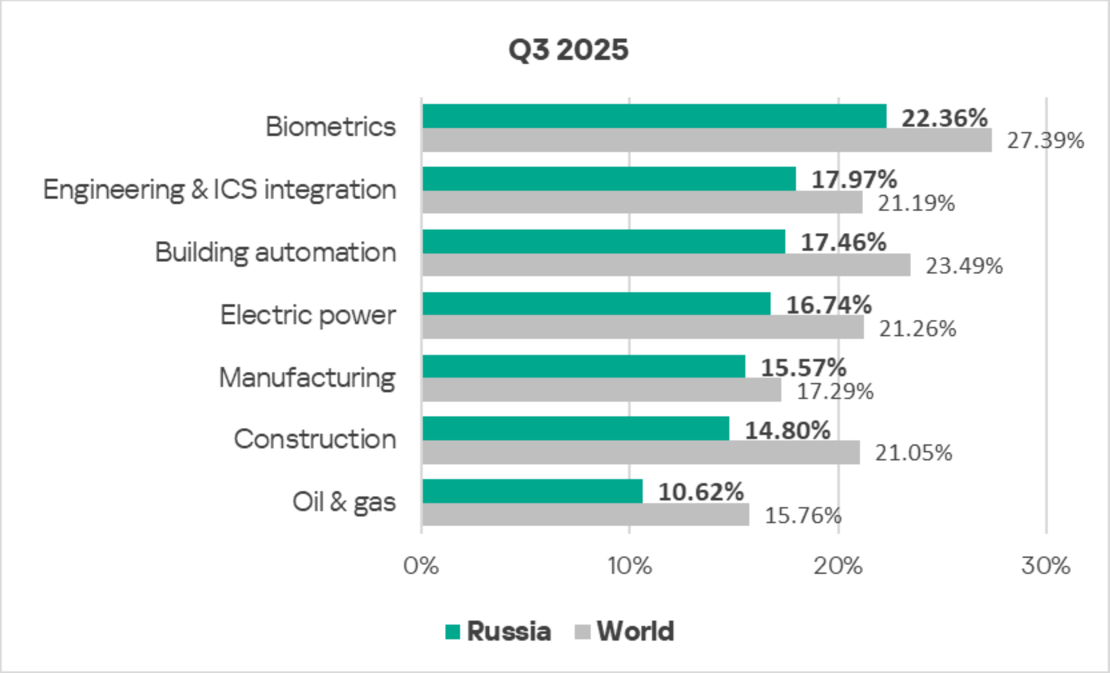


In Q3 2025, ransomware in Russia was distributed online and via email However, these threats are blocked twice as often in email clients compared to online sources.

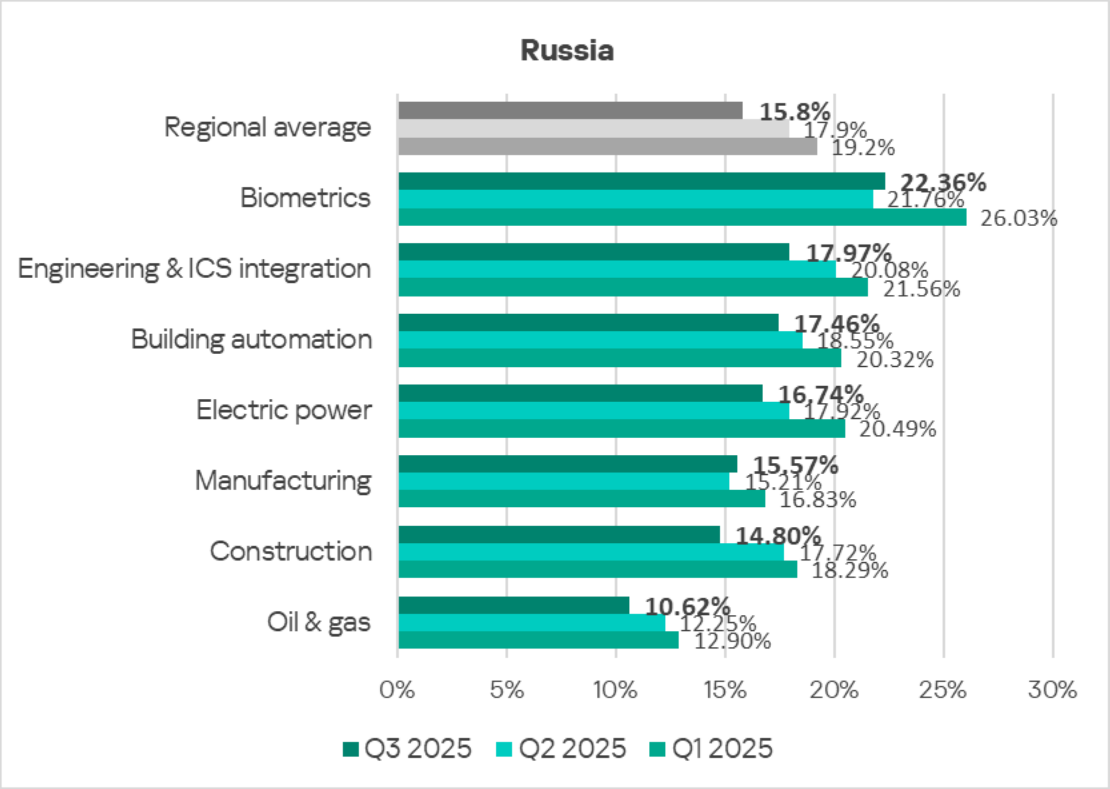
Industries

In Russia, of all the industries and OT infrastructures covered in the report, malicious objects are most often blocked in biometric systems.

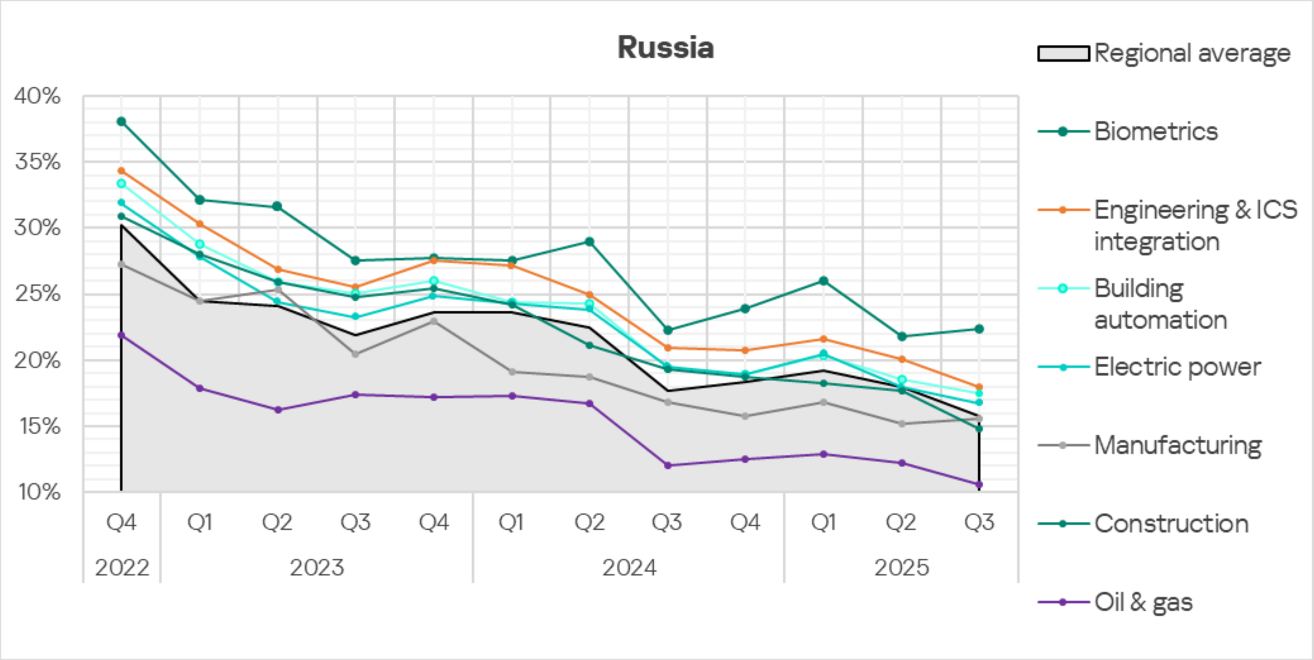
In all industries in the region, the percentage of ICS computers on which malicious objects were blocked is lower than the corresponding global average.



In Q3 2025, the percentage of ICS computers on which malicious objects were blocked fell in all industries covered in the region with the exception of the biometric systems and manufacturing OT infrastructure.



In all the industries covered, the indicators 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. The color red signifies that the figure approaches the maximum.

Threat source indicators for industries in Russia, Q3 2025

Industry / Threat source	Biometrics	Building automation	Electric power	Engineering & ICS integration	Oil & gas	Construction	Manufacturing	Threat category total in the region
Internet	8.10%	6.76%	7.64%	7.91%	4.06%	7.05%	5.24%	6.50%
Email clients	2.70%	1.84%	1.18%	0.88%	0.88%	0.66%	0.69%	0.78%
Removable media	0.31%	0.21%	0.38%	0.19%	0.20%	0.43%	0.28%	0.14%
Network folders	0.08%	0.03%	0.05%	0.02%	0.05%	0.04%	0.05%	0.02%
Industry total in the region	22.36%	17.46%	16.74%	17.97%	10.62%	14.80%	15.57%	

Threat category indicators for industries in Russia, Q3 2025

Industry / Threat category	Biometrics	Building automation	Electric power	Engineering & ICS integration	Oil & gas	Construction	Manufacturing	Threat category total in the region
Denylisted internet resources	5.01%	4.49%	5.66%	5.03%	3.08%	4.75%	3.48%	4.17%
Malicious scripts and phishing pages (JS and HTML)	5.78%	4.41%	4.27%	4.39%	2.72%	4.08%	3.15%	3.77%
Spy Trojans, backdoors and keyloggers	5.86%	3.89%	3.02%	2.76%	1.69%	2.32%	3.06%	2.57%
Worms	2.24%	1.21%	1.49%	0.93%	1.23%	1.01%	1.21%	0.88%
Miners in the form of executable files for Windows	0.93%	0.92%	1.38%	0.99%	0.64%	1.18%	0.59%	0.74%
Malicious documents (MSOffice + PDF)	2.08%	1.27%	1.11%	0.78%	0.81%	0.78%	0.90%	0.59%
Viruses	0.69%	0.46%	0.88%	0.48%	0.58%	0.68%	0.95%	0.30%
Ransomware	0.39%	0.57%	0.14%	0.12%	0.14%	0.24%	0.12%	0.14%
Web miners running in browsers	0.46%	0.37%	0.74%	0.36%	0.26%	0.63%	0.28%	0.22%
Malware for AutoCAD	0.00%	0.03%	0.08%	0.05%	0.11%	0.26%	0.19%	0.02%
Industry total in the region	22.36%	17.46%	16.74%	17.97%	10.62%	14.80%	15.57%	

In all industries, the main source of threats is the internet. Therefore, the current threat categories include denylisted links, malicious scripts and phishing pages, and spyware distributed through this threat source.

Miners threaten every industry: Russia consistently ranks no lower than fourth in regional rankings for both types of miners across all industries.

Building automation, oil and gas, and construction show high ransomware prevalence. For this indicator, Russia leads in the building automation sector and holds second place in the oil and gas and construction sectors in their respective regional rankings.

Biometric systems

Russia ranks eighth among regions in the percentage of ICS computers on which malicious objects were blocked in the OT infrastructure for biometric systems.

In the regional rankings for OT infrastructure for biometric systems, Russia has the following positions:

- First place in the percentage of ICS computers on which threats in network folders are blocked.
- Second place in the percentage of ICS computers on which denylisted internet resources and both types of miners are blocked.

The regional industry rankings for OT infrastructure for biometric systems is as follows:

- First place in all threat sources except for removable media.
- Third place for removable media threats.
- First place in malicious scripts and phishing pages, malicious documents, spyware, and worms.
- Second place in ransomware.
- Third place in denylisted internet resources, viruses, and web miners.

Engineering and ICS integrators

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

In the cross-regional rankings for this industry, Russia holds the following positions for each indicator:

- Second place in the percentage of ICS computers on which denylisted internet resources are blocked.
- Third place in the percentage of ICS computers on which miners in the form of executable files for Windows are blocked.
- Fifth in the region in terms of web miners.

In the regional cross-industry rankings, engineering and ICS integrators has the following positions:

- Second place for internet threats.
- Second place in the percentage of ICS computers on which denylisted internet resources are blocked.
- Third place in metrics in the following categories: malicious scripts and phishing pages, and miners in the form of executable files for Windows.

Building automation

Russia ranks tenth among regions in the percentage of ICS computers on which malicious objects were blocked in the building automation industry.

In the global cross-regional industry ranking, Russia's building automation sector holds:

- Second place in the percentage of ICS computers on which ransomware was blocked.

In the cross-regional rankings for this industry, Russia holds the following positions for each indicator:

- First place in the percentage of ICS computers on which denylisted internet resources and ransomware are blocked.
- Second place in the percentage of ICS computers on which miners in the form of executable files for Windows are blocked.
- Third in the region in terms of web miners.

In the regional cross-industry rankings, building automation has the following positions:

- Second place in email threats.
- First place in the percentage of ICS computers on which malware is blocked.
- Second place in malicious scripts and phishing pages, spyware, and malicious documents.

Electrical energy industry

Russia ranks ninth among regions in the percentage of ICS computers on which malicious objects were blocked in the electrical energy industry.

In the global cross-regional industry rankings, Russia's electrical energy industry holds:

- Third place in ICS computers where web miners were blocked.

In the cross-regional rankings for this industry, Russia holds the following positions for each indicator:

- Third place in the percentage of ICS computers on which threats in network folders are blocked.
- Second place in the percentage of ICS computers on which both types of miners are blocked.
- Fourth place in the percentage of ICS computers on which denylisted internet resources are blocked.

In the regional cross-industry rankings, the electrical energy industry ranks:

- Second place in the percentage of ICS computers on which threats from removable media are blocked.
- Third place in online threats and threats from email clients and network folders.
- First place in the percentage of ICS computers on which denylisted internet resources and both types of miners are blocked.
- Second place in worms and viruses.
- Third place for removable malicious documents.

Manufacturing

Russia ranks seventh in the percentage of ICS computers on which malicious objects were blocked in manufacturing.

In the cross-regional rankings for this industry, Russia holds the following positions for each indicator:

- Third place in the percentage of ICS computers on which threats in network folders are blocked.
- Third place in the percentage of ICS computers on which both types of miners are blocked.

In the regional cross-industry rankings, the manufacturing sector ranks:

- Second place in the percentage of ICS computers on which threats in network folders are blocked.
- First place in the percentage of ICS computers on which viruses are blocked.
- Second place in malware for AutoCAD.
- Third place for spyware.

Construction

Russia ranks tenth among regions in the percentage of ICS computers on which malicious objects were blocked in the construction sector.

In the cross-regional rankings for this industry, Russia holds the following positions for each indicator:

- Second place in the percentage of ICS computers on which miners in the form of executable files for Windows and ransomware are blocked.
- Fourth place in the percentage of ICS computers on which web miners are blocked.

In the regional cross-industry rankings, the construction sector ranks:

- First place in the percentage of ICS computers on which threats from removable media are blocked.
- First place in the percentage of ICS computers on which malware for AutoCAD is blocked.
- Second place in both types of miners.
- Third place in ransomware.

Oil and gas

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

In the cross-regional rankings for this industry, Russia holds the following positions for each indicator:

- Second place in the percentage of ICS computers on which threats in network folders are blocked.
- Third place in email clients.
- Second place in the percentage of ICS computers on which ransomware is blocked.
- Fourth place in malicious documents, both types of miners, worms, and malware for AutoCAD.

In the regional cross-industry rankings, oil and gas is:

- Third place in the percentage of ICS computers on which worms and malware for AutoCAD are blocked.

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 as 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 under review 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