Kaspersky ICS CERT

kaspersky

Threat landscape for industrial automation systems

Africa. Q3 2025

25.12.2025

Version 1.0

Africa

Key cybersecurity issues in the region

Low cybersecurity maturity of industrial companies

High threat detection rates point to low cybersecurity maturity across industrial companies on the continent: the availability of internet access on OT computers, weak phishing protection, large portions of unprotected infrastructure, and still relatively poor employee cyberhygiene.

In Africa, the percentage of ICS computers on which all categories of threats were blocked is higher than the global average***.***

Unprotected OT infrastructure and weak network segmentation

In Africa, the percentage of ICS computers blocking self-propagating malware (worms and viruses) is significantly higher than the global average. By the percentage of ICS computers on which worms were blocked, Africa leads all other regions by a wide margin; in terms of viruses, it ranks second.

High detection rates of self-propagating malware and malware spread via network folders at the industry, country, or regional level likely indicate unprotected OT infrastructures lacking even basic endpoint protection. Such unprotected computers become sources of further malware spread.

Weak enterprise network segmentation and lack of control over removable media further exacerbate the situation.

Absence or ineffectiveness of perimeter defenses for OT networks

The rate of spyware detections in the region far exceeds the global average: it was 1.6 times higher in Q3 2025.

Finding spyware on ICS computers usually indicates that the initial infection vector — whether a malicious link, an attachment from a phishing email, or an infected USB device — has already succeeded. This points to the lack or ineffectiveness of OT network perimeter defenses, such as monitoring network communications and enforcing removable media usage policies.

By the percentage of ICS computers on which spyware is blocked, Africa consistently ranks first among all regions.

Lack of control over the use of removable media

In Q3 2025, the percentage of ICS computers on which threats were blocked when connecting removable media was 4.3 times higher than the global average. In this indicator, Africa leads the world by a wide margin.

Frequent attempts to infect protected systems via USB drives may indicate:

- A low level of enterprise digitalization (lack of secure internal file storage and transfer systems);
- The existence of significant unprotected enterprise infrastructure acting as a source of USB infections;
- A poor overall information security culture.

Cybersecurity adoption lags behind the pace of rapidly developing industries

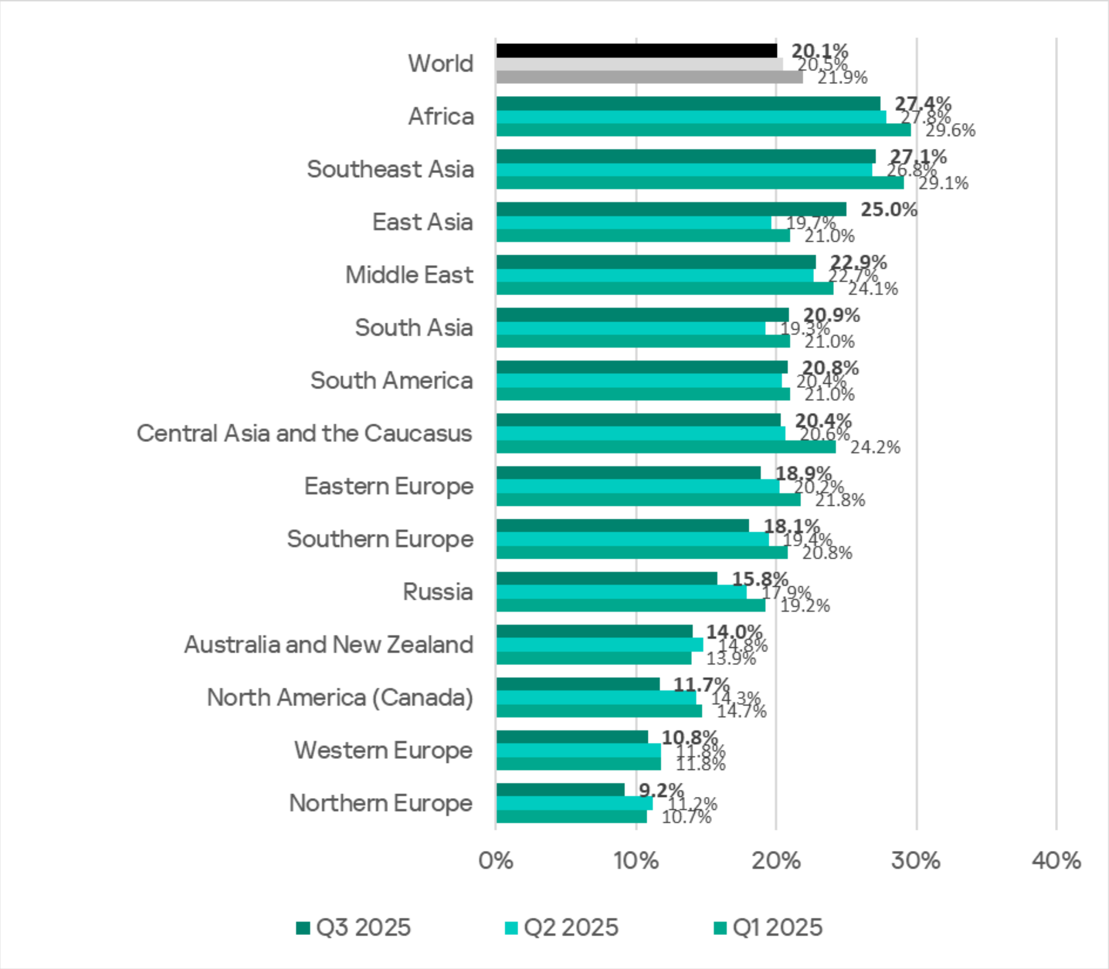
One broad conclusion we can draw from years of monitoring OT infrastructure exposure to threats is that the implementation of cybersecurity measures and tools almost always lags behind industry growth. When facilities are commissioned, cybersecurity is often an afterthought. Protections are insufficient, staff is poorly trained, and compliance with security policies is half-hearted.

This trend is clearly visible in statistics on African industries and infrastructure types (see below). Rapidly developing sectors include oil and gas, energy, manufacturing, and construction. Engineering is developing alongside these.

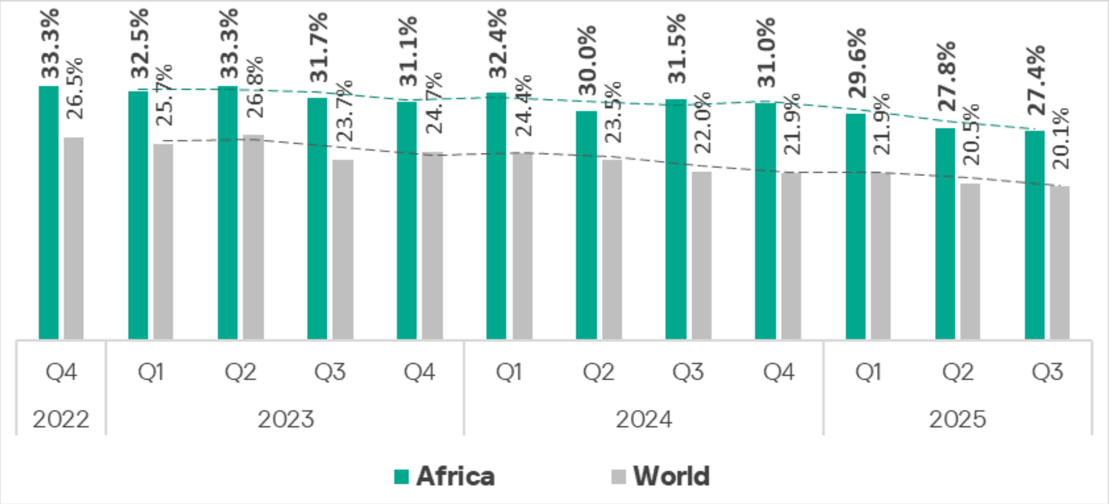
Statistics across all threats

In Q3 2025, Africa remained the leading region by the percentage of ICS computers on which malicious objects were blocked. However, Southeast Asia is only 0.3 p.p. behind in second place.

In Q3 2025, the percentage of ICS computers in Africa where malicious objects were blocked dropped a bit further — to 27.4%. Nevertheless, this figure is still 1.4 times higher than the global average. Moreover, compared to Northern Europe (which ranks last), Africa's rate is now 3 times higher (up from 2.5).

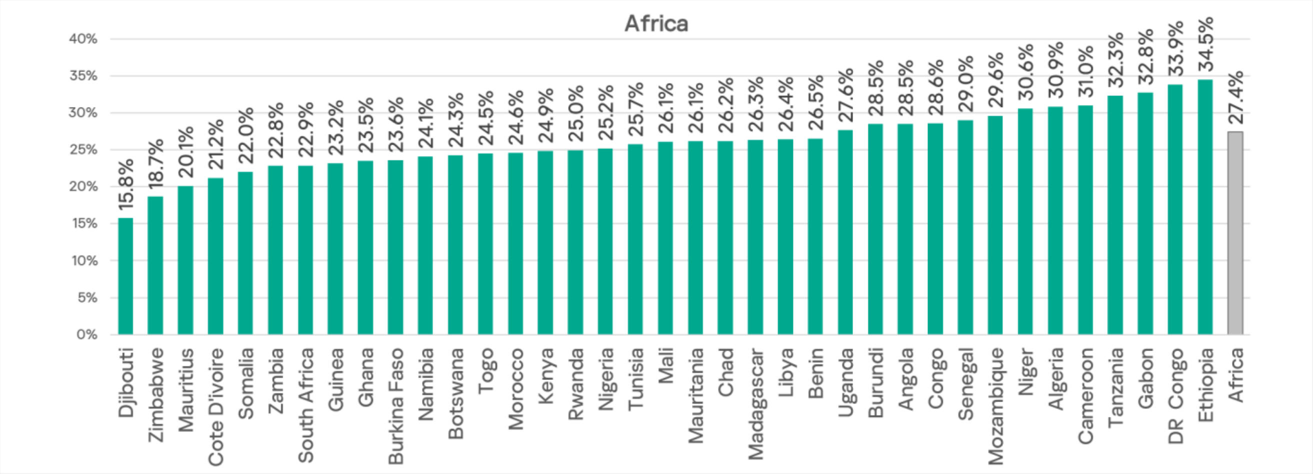


This indicator has been declining in the region for four consecutive quarters.



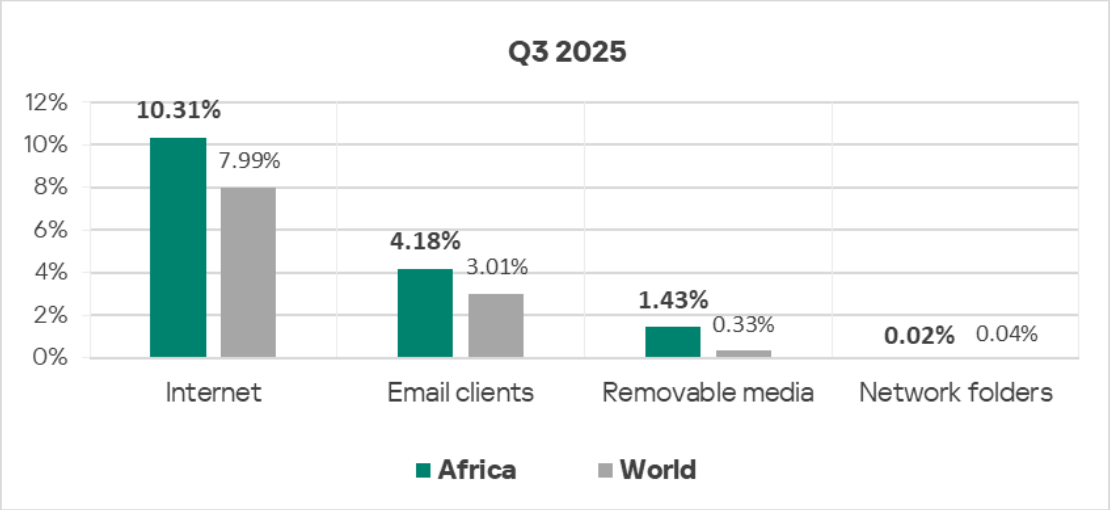
Across African countries, the percentage of ICS computers on which malicious objects were blocked ranges from 15.8% in Djibouti to 34.5% in Ethiopia.

The rate falls below 20% in only two countries: Zimbabwe and Djibouti. In Niger, Algeria, Cameroon, Tanzania, Gabon, the DRC, and Ethiopia, it's over 30%.

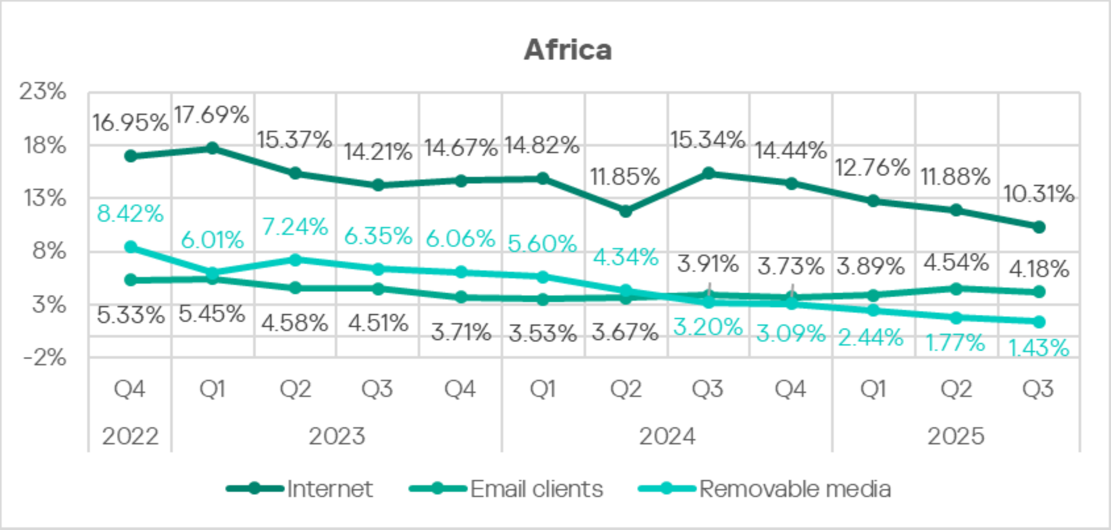


Threat sources

In Q3 2025, Africa's rate was higher than the global average for all threat sources with the exception of network folders. The rate for removable media threats was particularly high: 4.3 times higher.

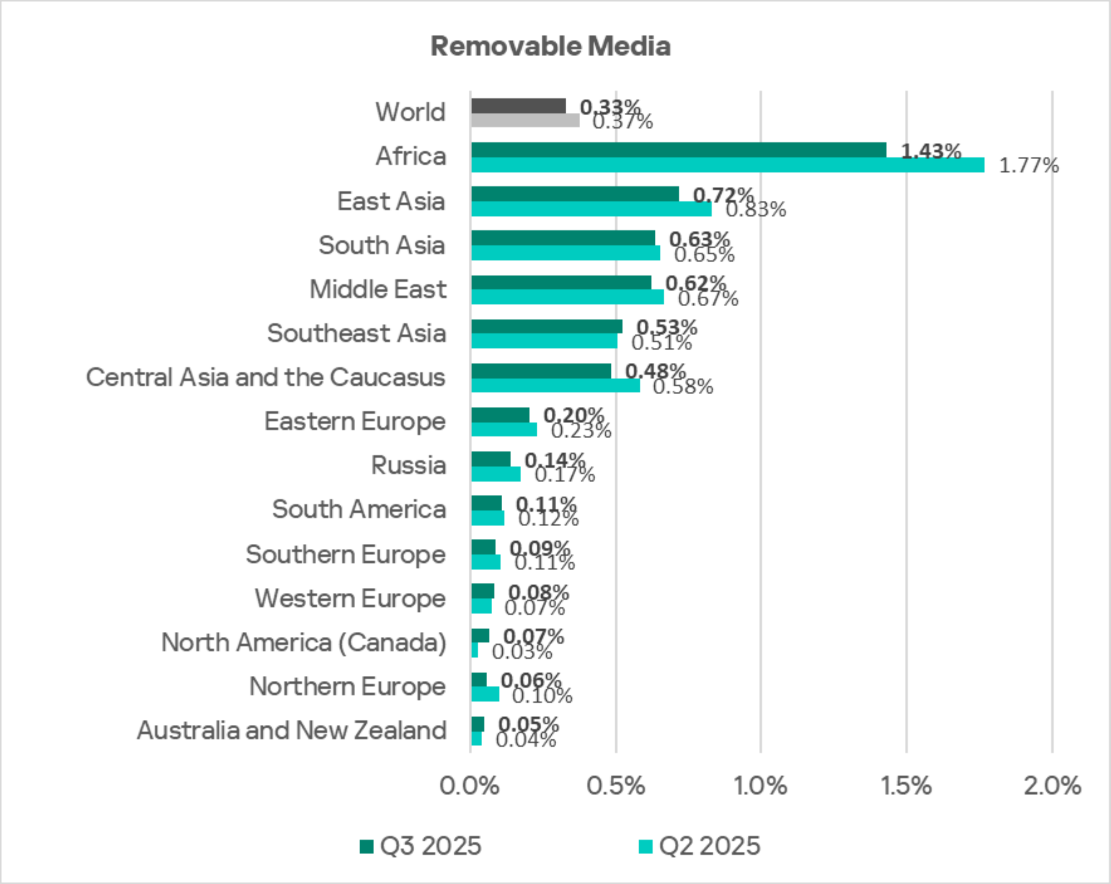


Nevertheless, the rate for all threat sources decreased this quarter.

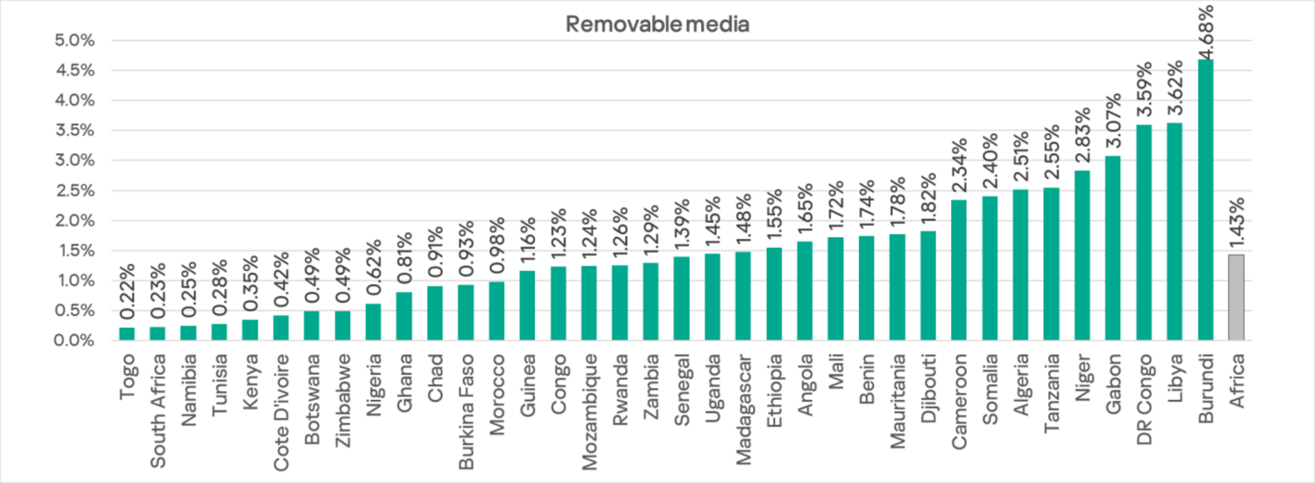


Removable media

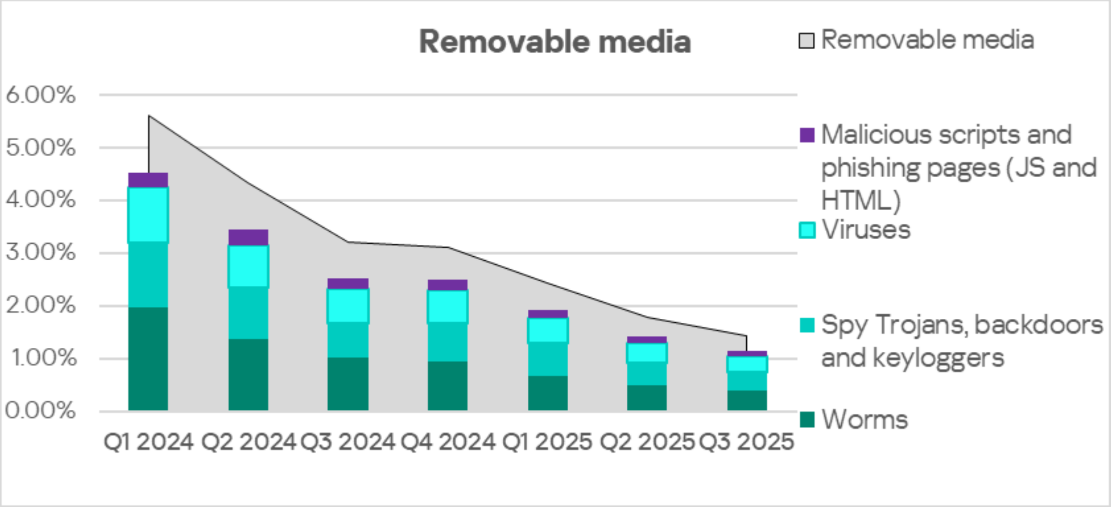
Despite a steady decline in the percentage of ICS computers on which removable media threats were blocked, Africa continues to lead the world by a large margin in this indicator. Africa's figure (1.43%) is 28.6 times higher than that of Australia and New Zealand, which has the lowest rate.



Among the countries in the region, Burundi leads significantly in the percentage of ICS computers on which threats were blocked upon connecting removable media, with 4.68%. The other countries range from 0.22% in Togo to 3.62% in Libya.

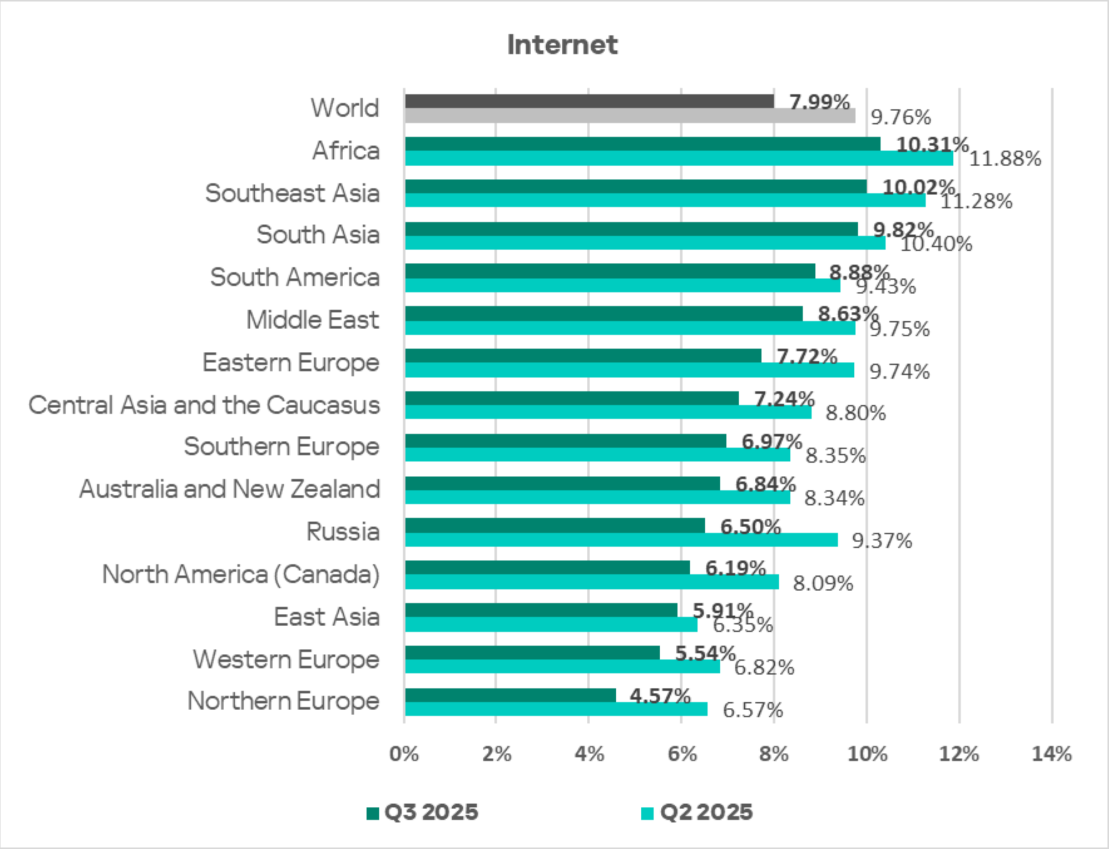


The main threat categories blocked on ICS computers from removable media in Q3 2025 were worms, spyware, viruses, and malicious scripts. By the percentage of ICS computers on which these categories were blocked, Africa also leads the world (in viruses, it ranks second).

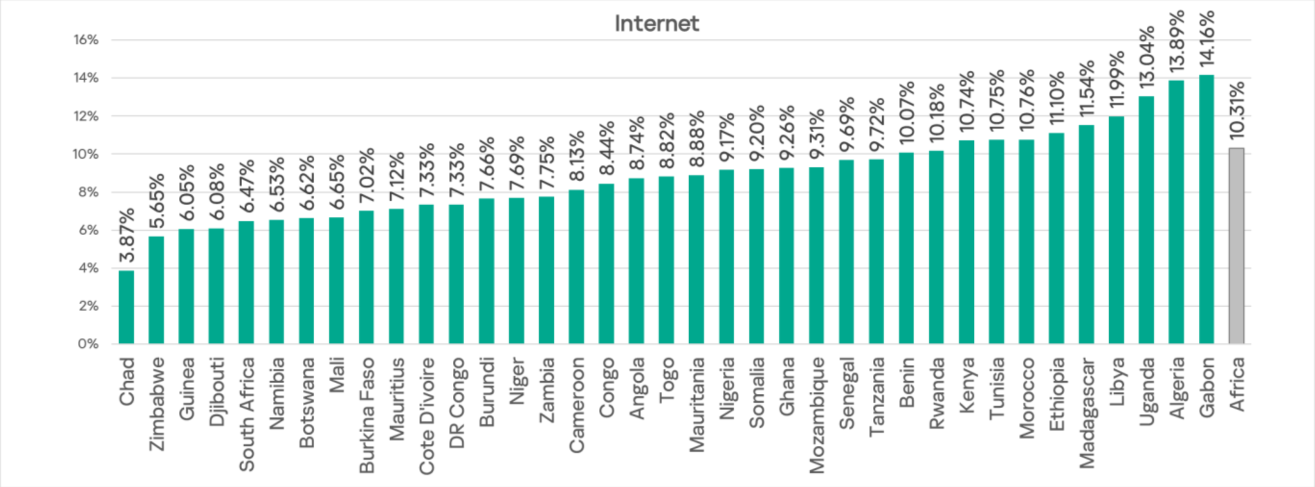


Internet

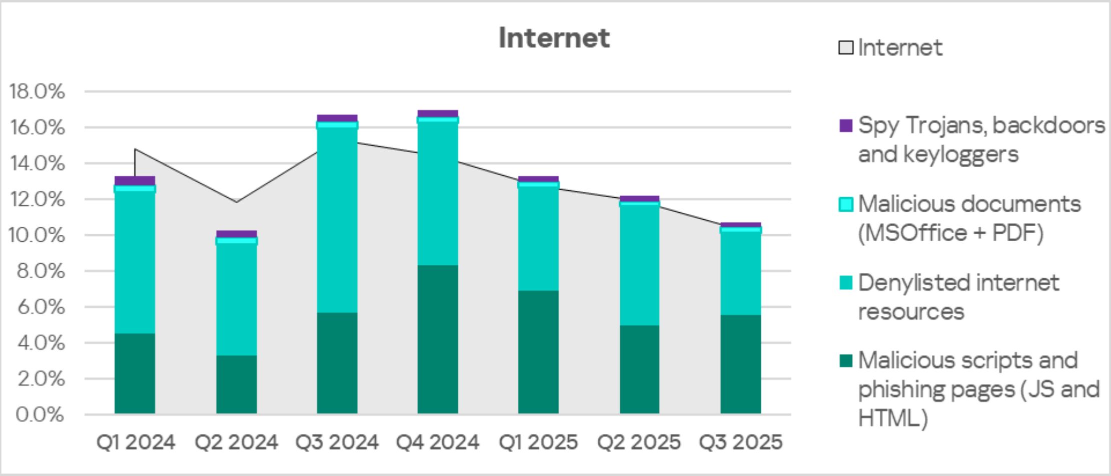
Another threat source where Africa leads is the internet. In Q3 2025, Africa's percentage of ICS computers on which internet threats were blocked (10.31%) exceeded that of Northern Europe (lowest ranking) by 2.3 times.



Among countries in the region, Gabon leads with 14.16%. Chad has a noticeably smaller percentage of ICS computers with blocked internet threats (3.87%).

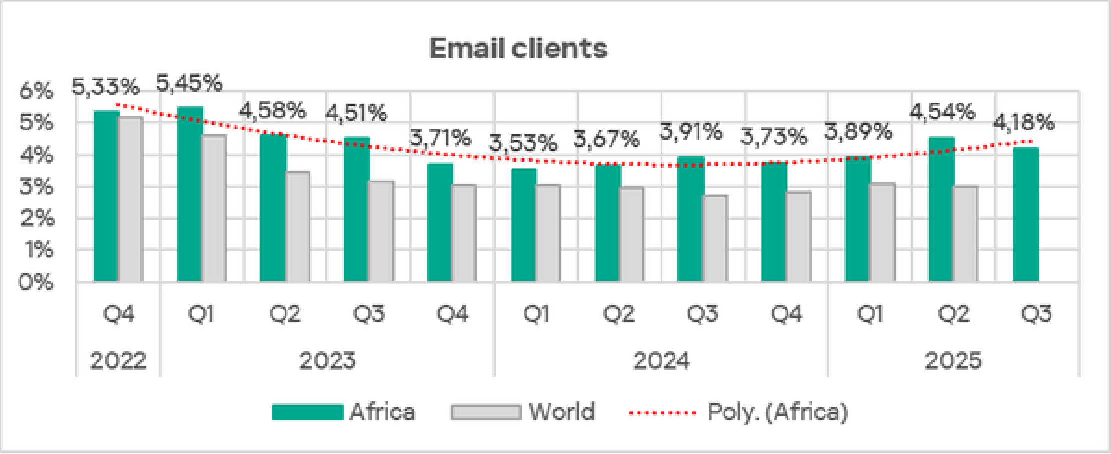


The primary internet threat categories blocked on ICS computers in Q3 2025 were malicious scripts and phishing pages, denylisted internet resources, malicious documents, and spyware.

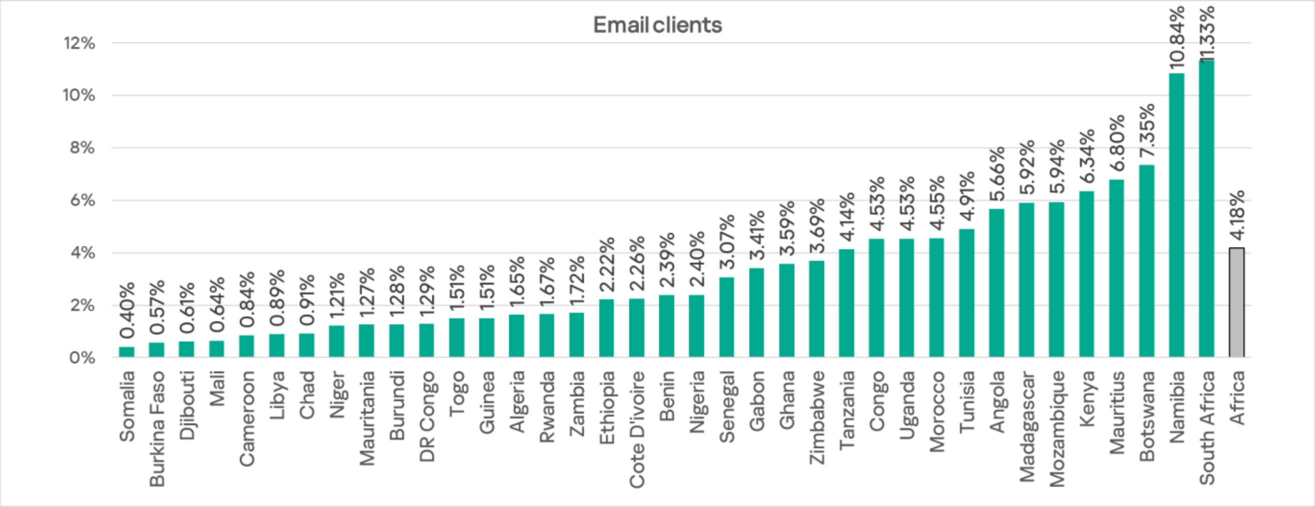


Email clients

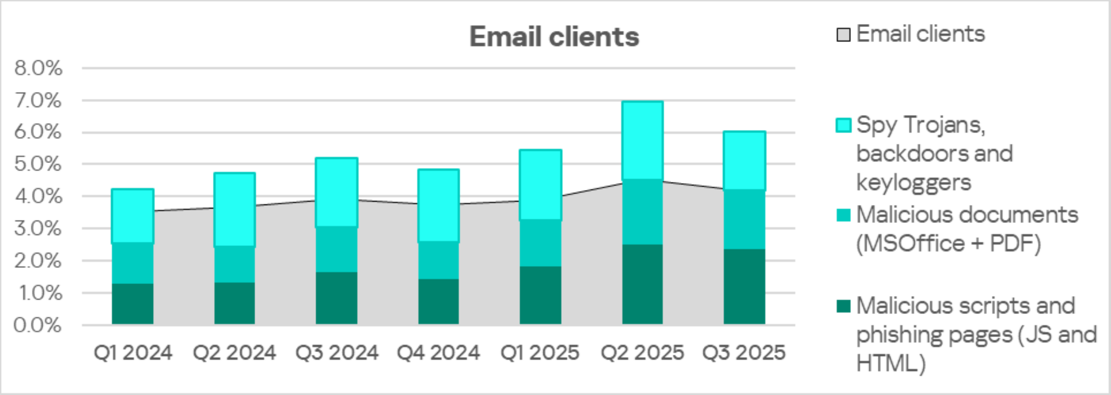
After increasing during the first two quarters of 2025, the percentage of ICS computers in Africa where email client threats were blocked decreased. Globally, Africa ranks fifth among regions with 4.18%. This is 5.4 times higher than in Russia, which has the lowest figure globally.



South Africa and Namibia clearly lead the region in the percentage of ICS computers on which threats were blocked in mail clients, with 11.33% and 10.84%, respectively. Somalia has the lowest rate at 0.4%.

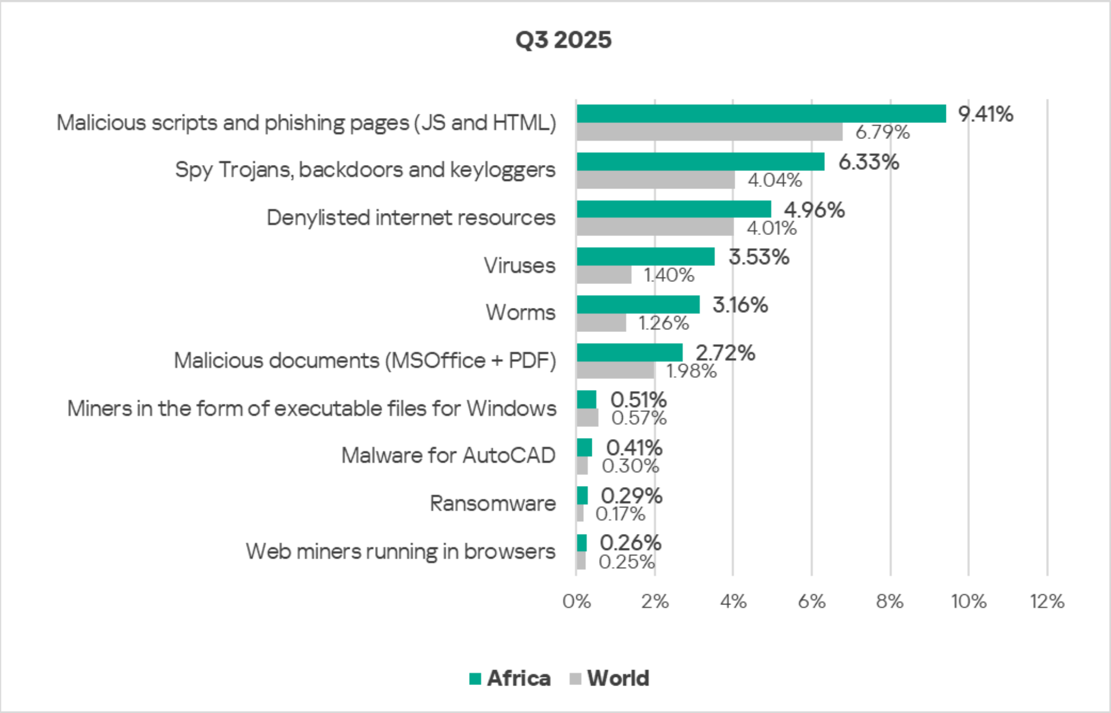


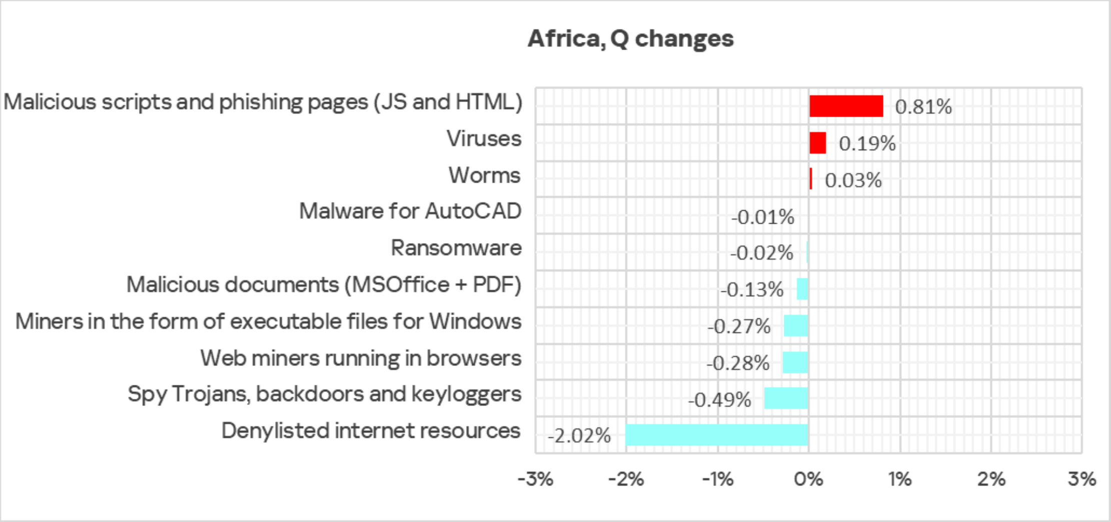
The main email client threat categories blocked on ICS computers in Q3 2025 were malicious scripts and phishing pages, malicious documents, and spyware.



Threat categories

In Africa, the percentage of ICS computers on which malicious objects were blocked exceeds the global average in every threat category except miners in the form of executable files for Windows.





The most significant differences with global averages are seen in the following categories:

- Viruses: Africa's rate is 2.5 times higher
- Worms: 2.5 times higher
- Spyware: 1.6 times higher

In Q3 2025, Africa leads the rankings in the percentage of ICS computers on which the following were blocked:

- Malicious scripts and phishing pages (JS and HTML) — Africa jumped up from fourth to first place

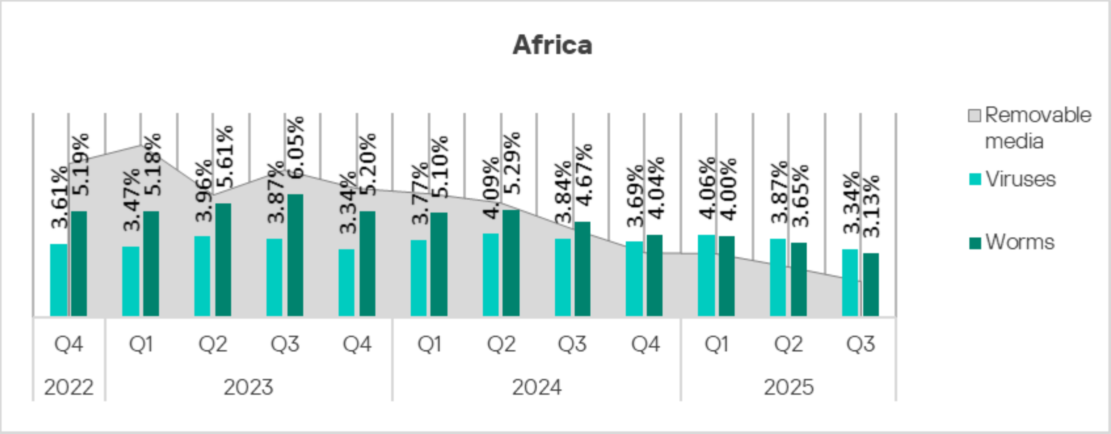
- Denylisted internet resources
- Spyware
- Worms

Africa ranks second in viruses and ransomware.

Self-propagating malware: worms and viruses

Worms and viruses are the main threat categories blocked when connecting removable media to ICS computers. Given Africa's consistent top ranking for this threat source, it's unsurprising that worms and viruses spread faster there than in other regions.

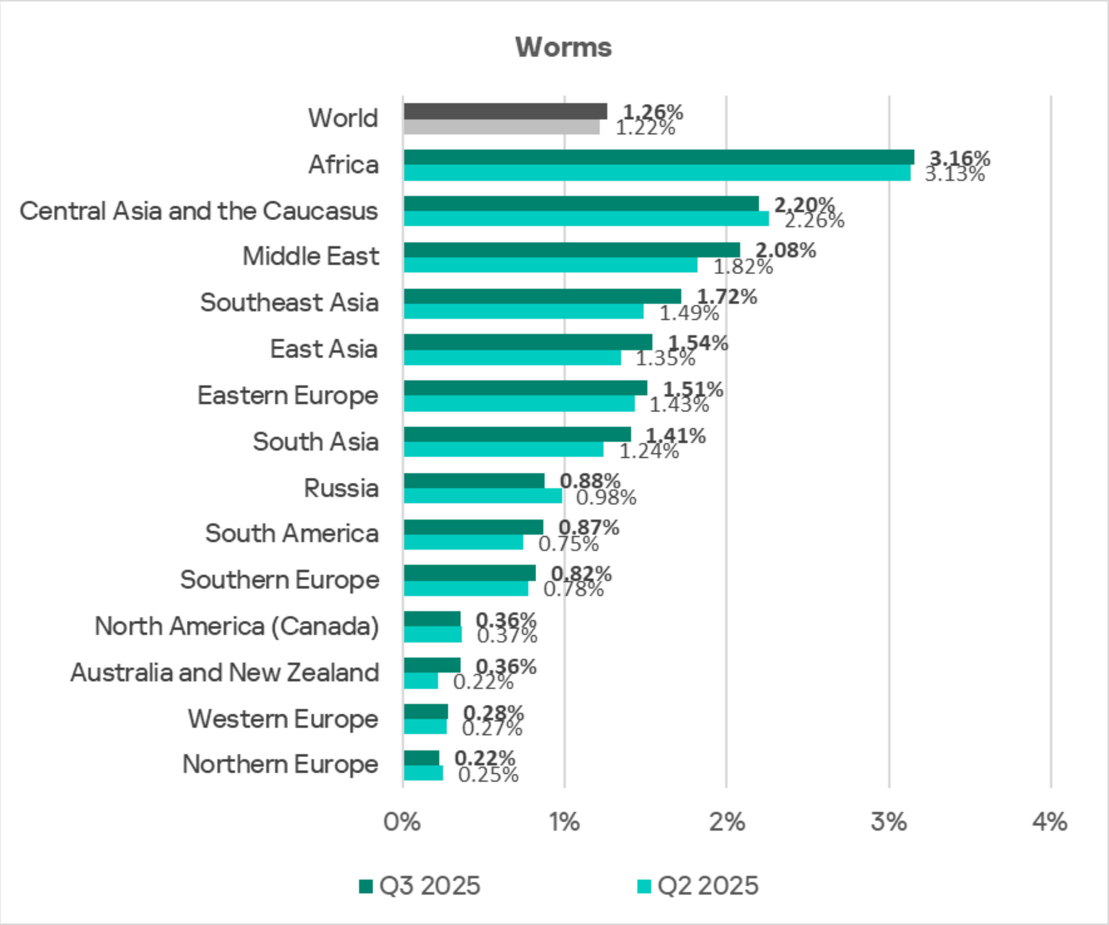
The worm rate, similar to the overall percentage of threats from removable media, is gradually decreasing. Virus dynamics are more complex, but we've also seen a decline here over the last two quarters.



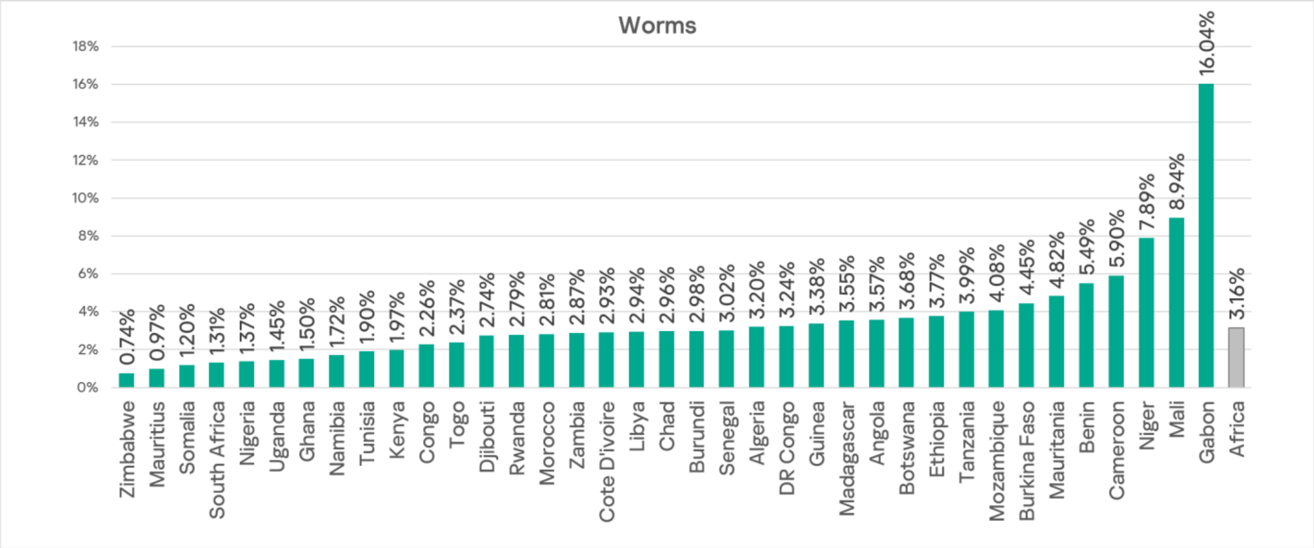
Worms

Africa remains the consistent leader among regions in the percentage of ICS computers on which worms are blocked. Although the figure is gradually declining, it is still significantly higher in Africa than anywhere else.

In Q3 2025, the percentage of ICS computers on which worms were blocked in Africa increased slightly to 3.16%. This is 14.4 times higher than in Northern Europe, which ranks last.



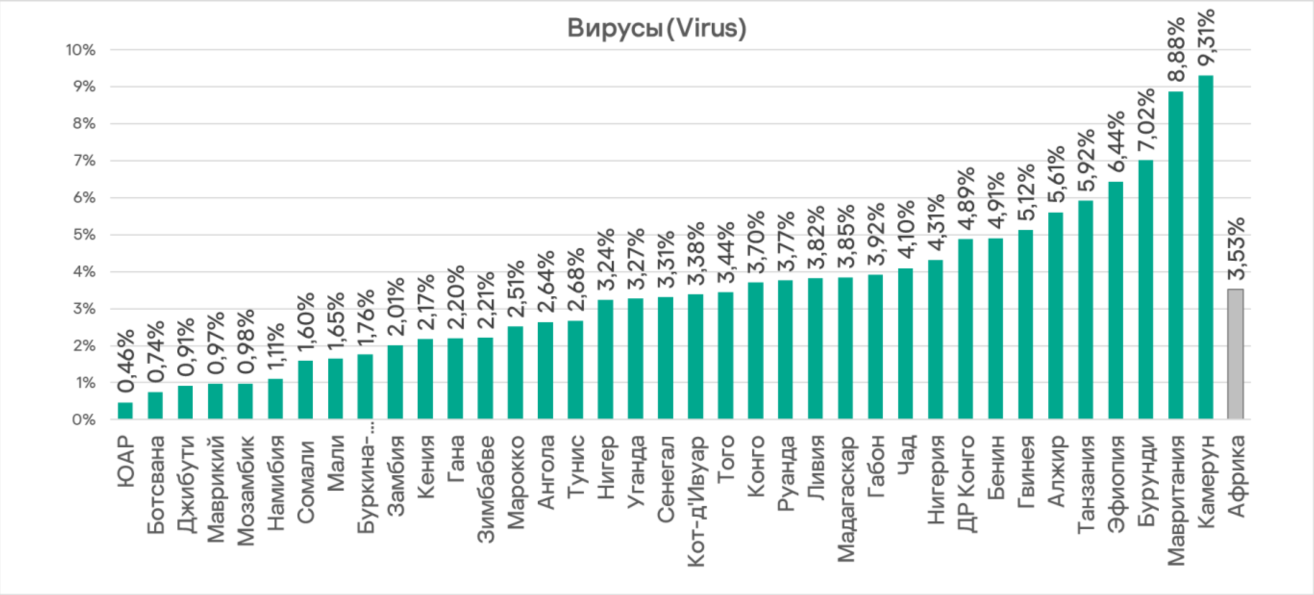
Among the region's countries Gabon leads this metric by a large margin with an anomalously high 16.04%. This is 1.8 times higher than the next country, Mali (8.94%). The lowest figure is in Zimbabwe — 0.74%.



Viruses

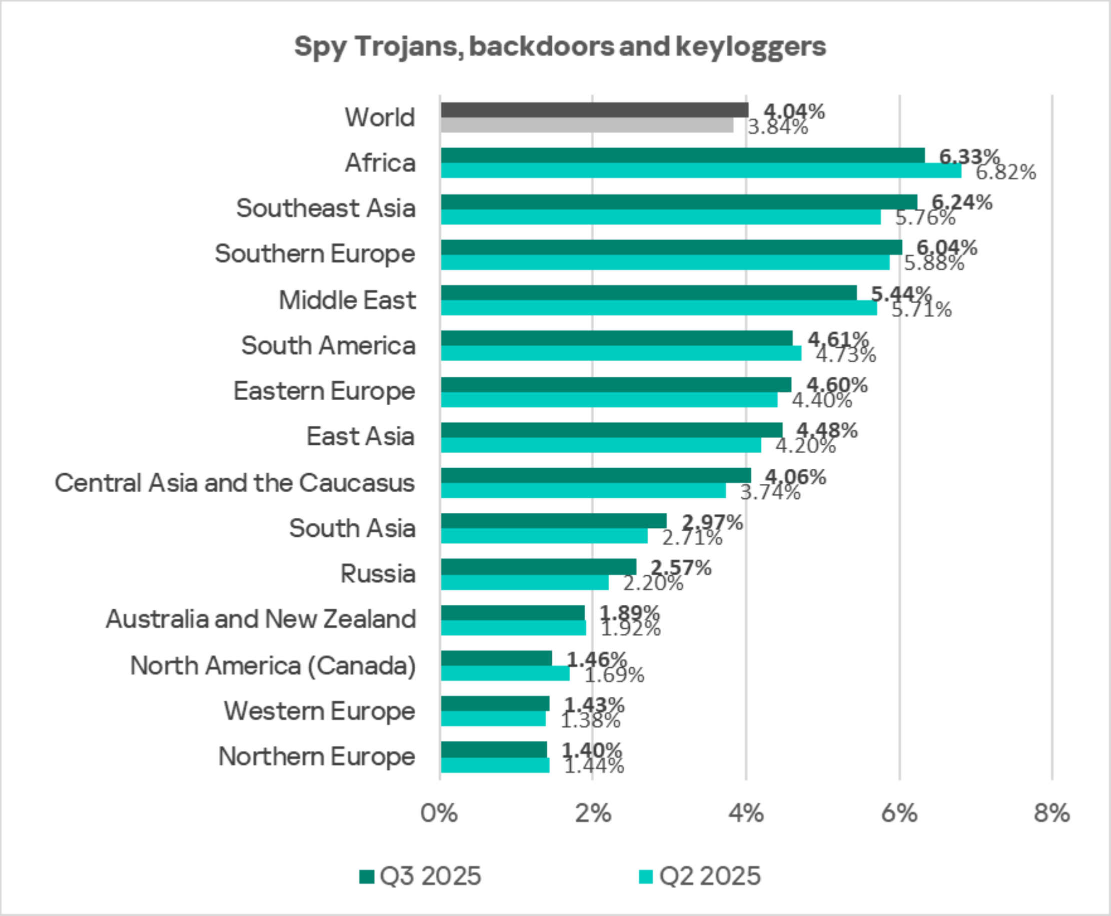
In terms of ICS computers where viruses are blocked, Africa ranks second globally with 3.53%. This is 22.1 times higher than Australia and New Zealand, which is last.

Cameroon (9.31%) and Mauritania (8.88%) lead the region in the percentage of ICS computers on which viruses are being blocked. The lowest figure is in South Africa — 0.46%.

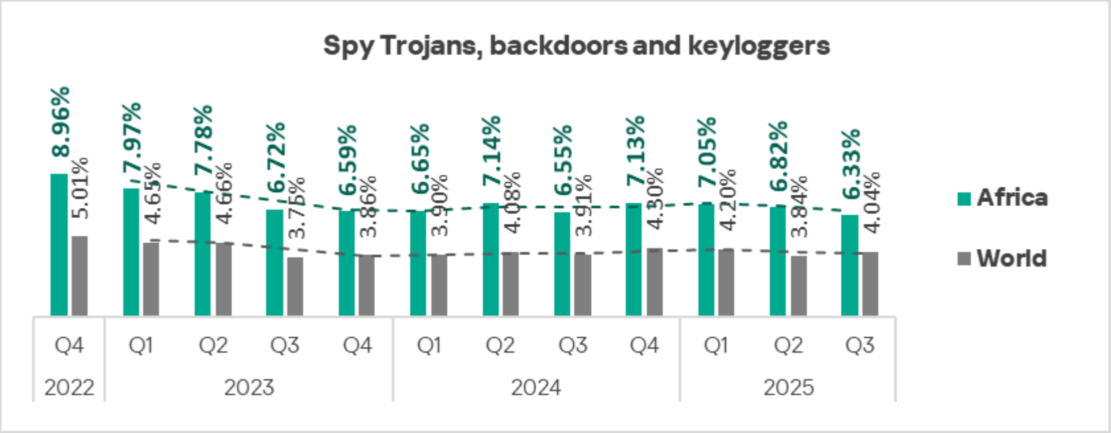


Spyware

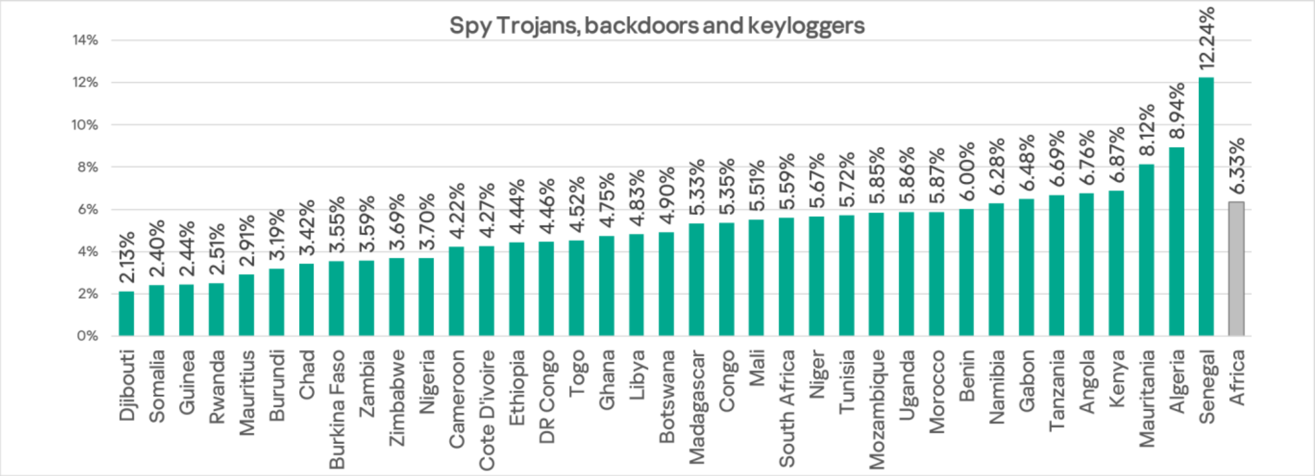
Africa consistently leads regions in the percentage of ICS computers on which spyware was blocked. In Q3 2025, this figure in Africa dropped to 6.33% — still 4.5 times higher than in Northern Europe, which has the lowest percentage of ICS computers on which spyware is being blocked.



This metric has been declining in the region for three consecutive quarters.



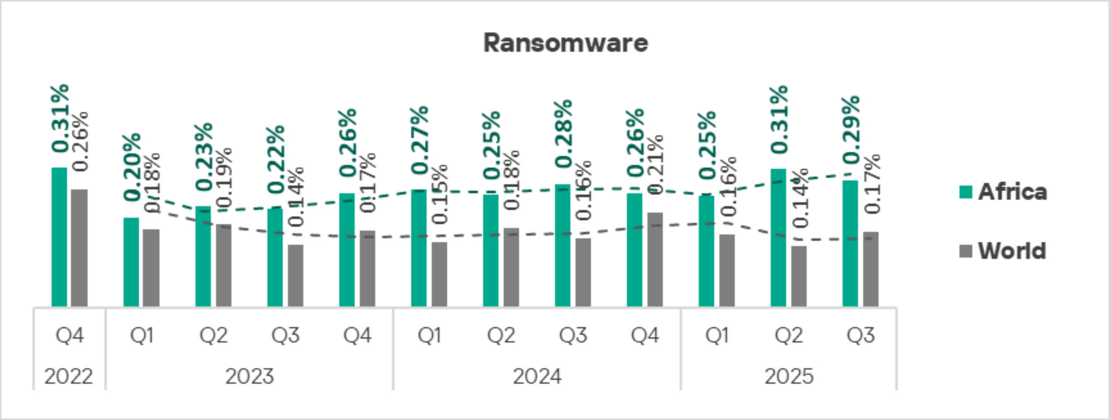
Senegal leads the region by a wide margin in the percentage of ICS computers on which spyware was blocked, with 12.24%.



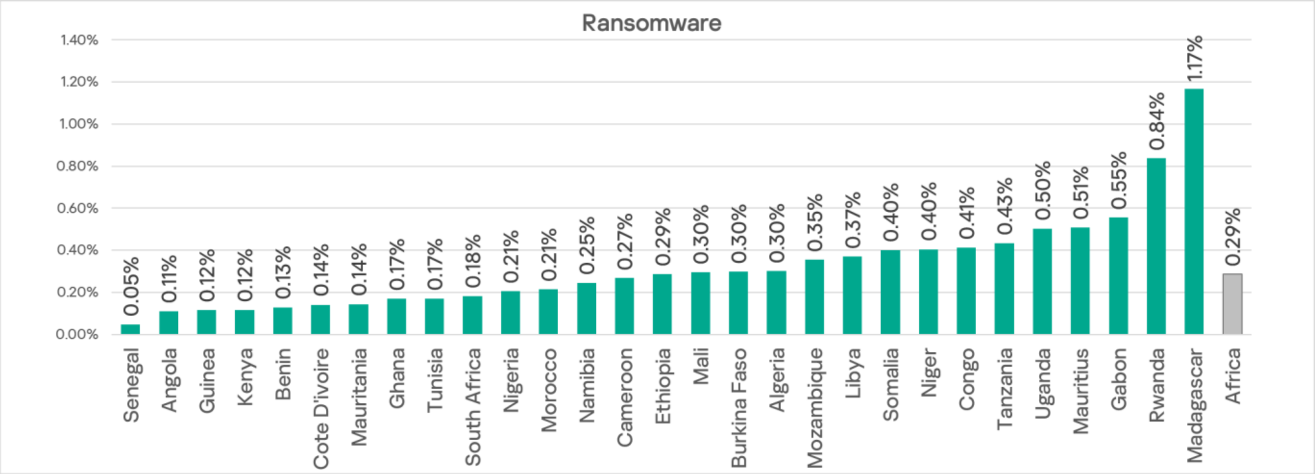
Ransomware

In Q3 2025, Africa ranks second globally in the percentage of ICS computers on which ransomware was blocked, with 0.29%. This is 5.8 times higher than Northern Europe, which has the lowest rate.

In Q2, Africa was the leader in this metric. In Q3, the percentage of ICS computers on which ransomware was blocked decreased slightly, and the region dropped to second place in the ranking.



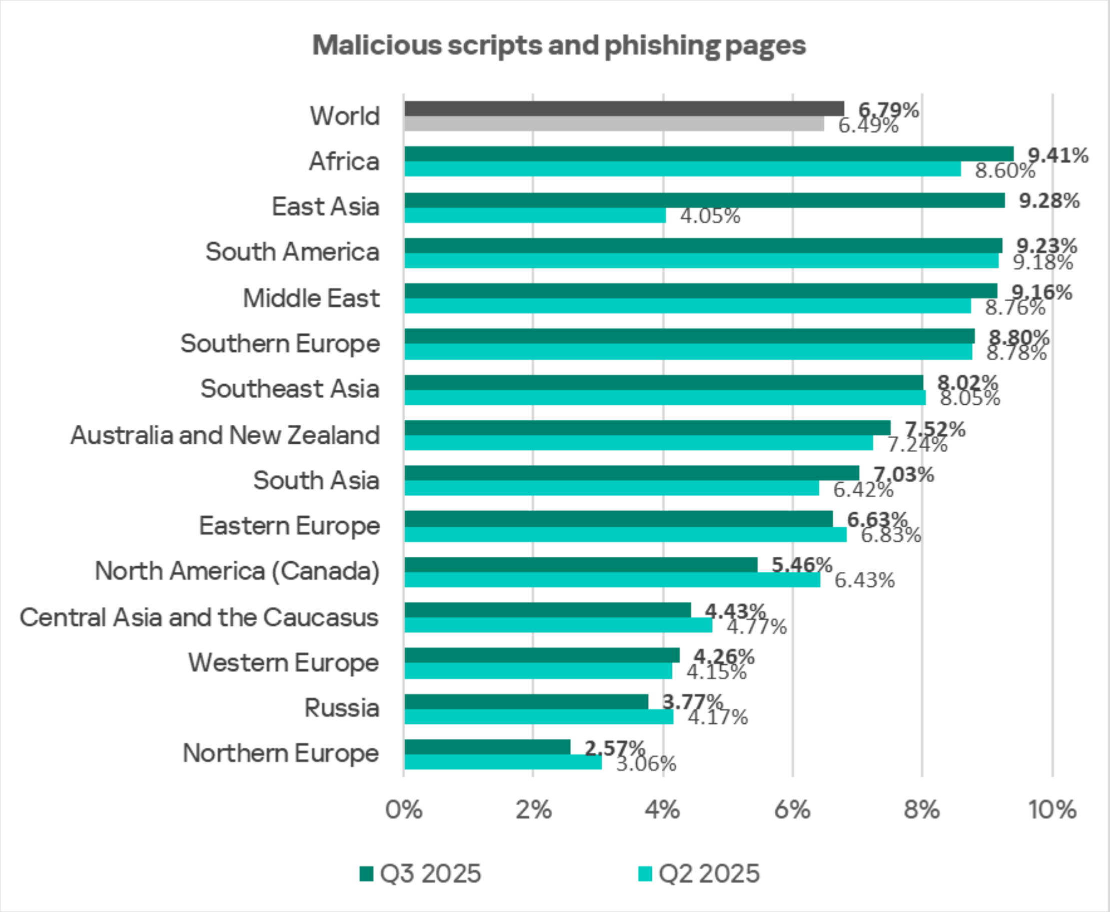
Among the countries of the region, Madagascar (1.17%) and Rwanda (0.84%) recorded the highest percentages of ICS computers where ransomware was blocked.



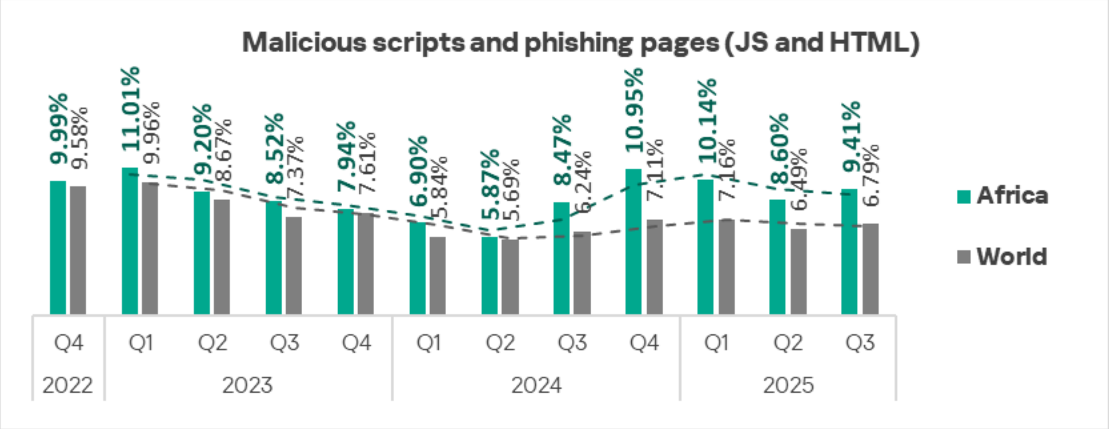
Notably, the threat was not detected in every country in the region in Q3 2025.

Malicious scripts and phishing pages

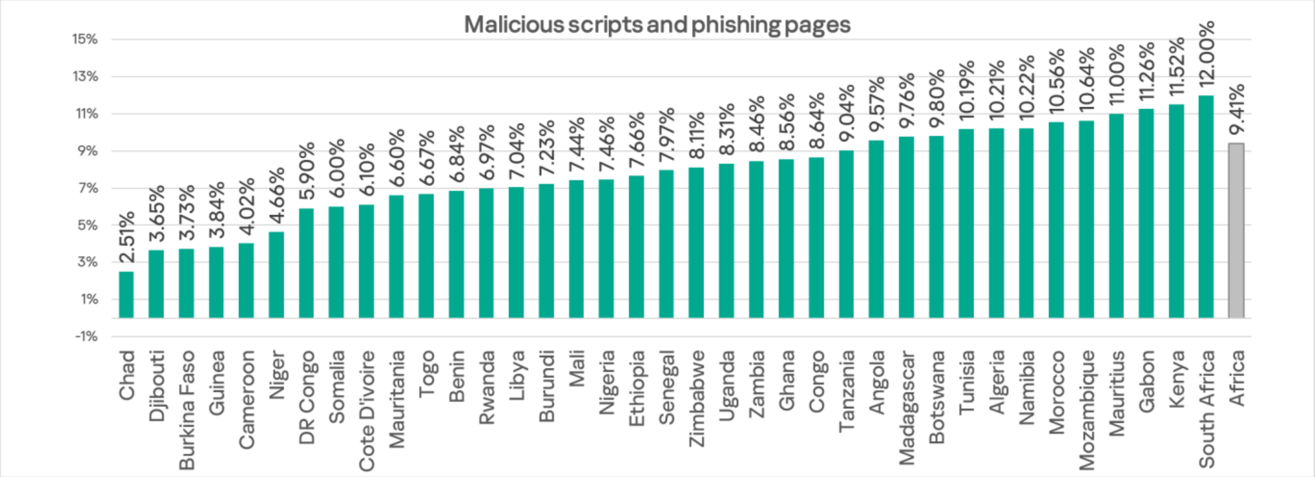
In Q3, Africa rose from fourth to first place globally in the percentage of ICS computers on which malicious scripts and phishing pages are blocked. The figure increased to 9.41% in this quarter. This figure is 3.7 times higher than in Northern Europe, which has the lowest percentage value.



Despite this sharp rise in ranking, the value for this quarter is not the highest seen in the last three years. Notably, during this period Africa also topped the percentage of ICS computers on which malicious scripts and phishing pages were blocked twice more — in Q3 and Q4 2024.

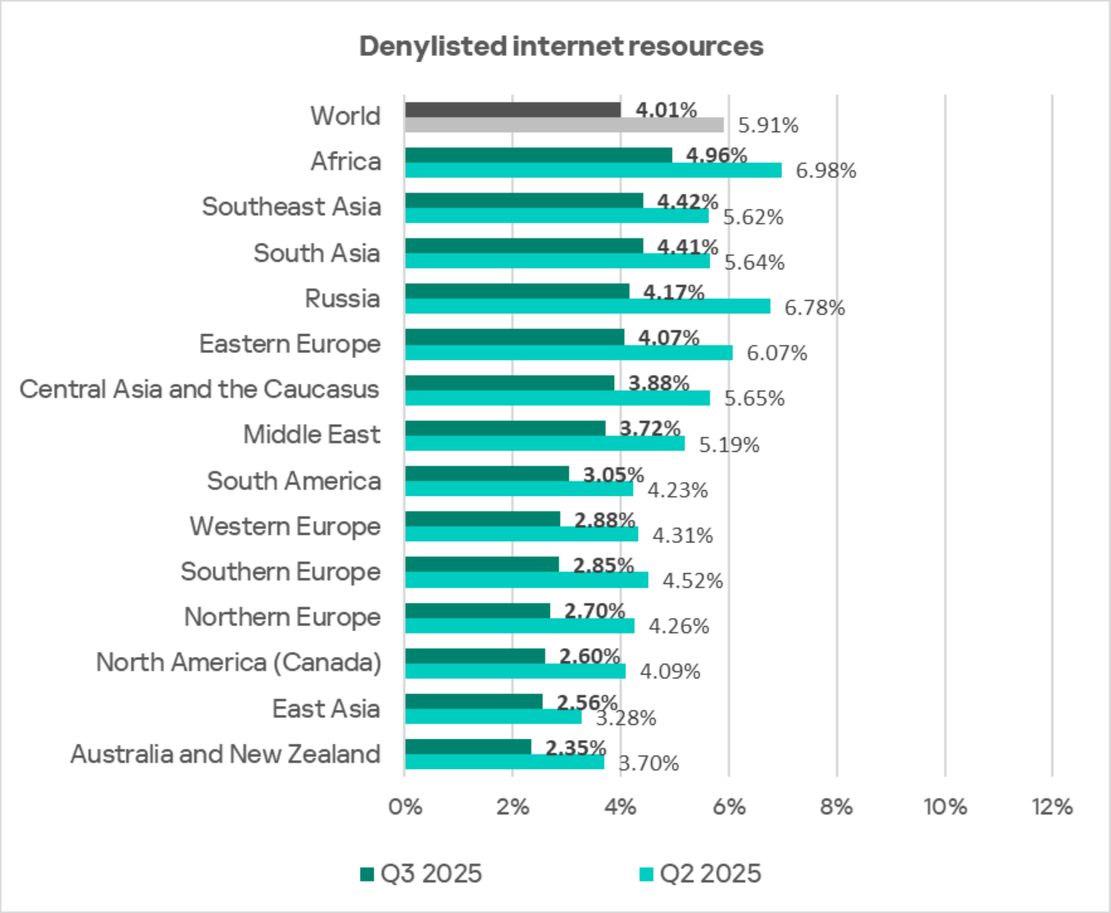


Among countries in the region, South Africa leads in this metric with 12.0%. South Africa also leads the ranking for email client threats. Chad had the lowest figure at 2.51%.

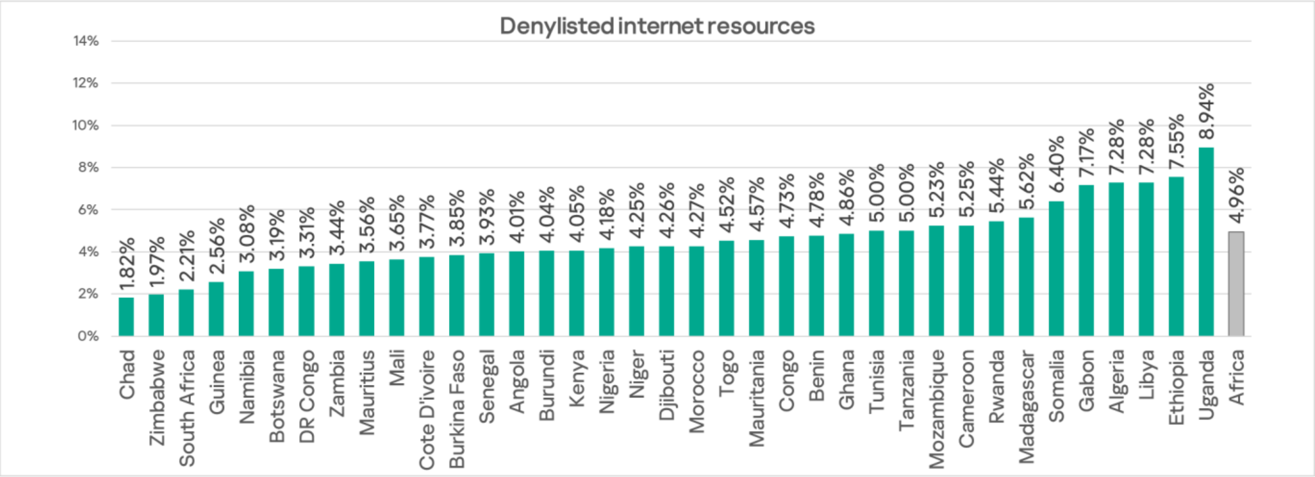


Denylisted internet resources

In Q3 2025, the percentage of ICS computers on which access to denylisted internet resources was blocked decreased across all regions. Africa remained the leader in this metric with 4.96%. This figure is 2.1 times higher than in Australia and New Zealand, which ranks last.

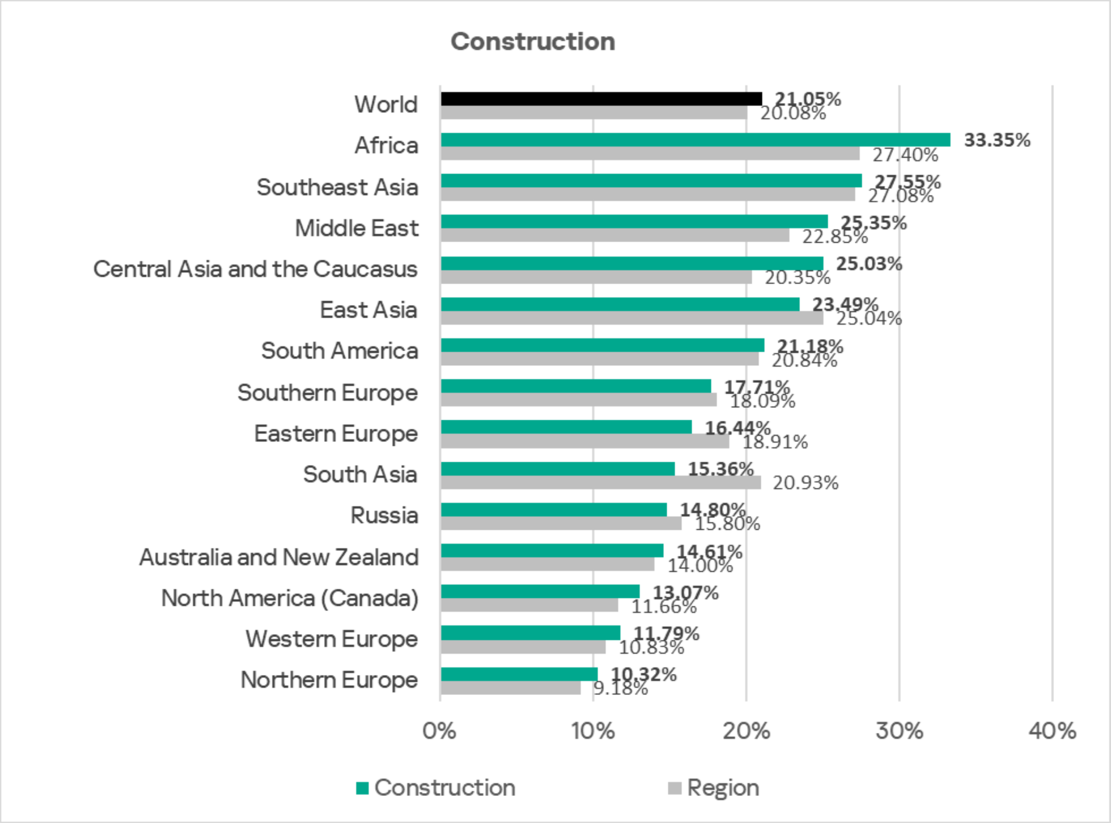


Uganda leads the region in the percentage of ICS computers on which denylisted internet resources are being restricted, with 8.94%. This country is also among the top 3 in the region for the percentage of ICS computers on which internet threats are blocked. Chad had the lowest figure at 1.82%.

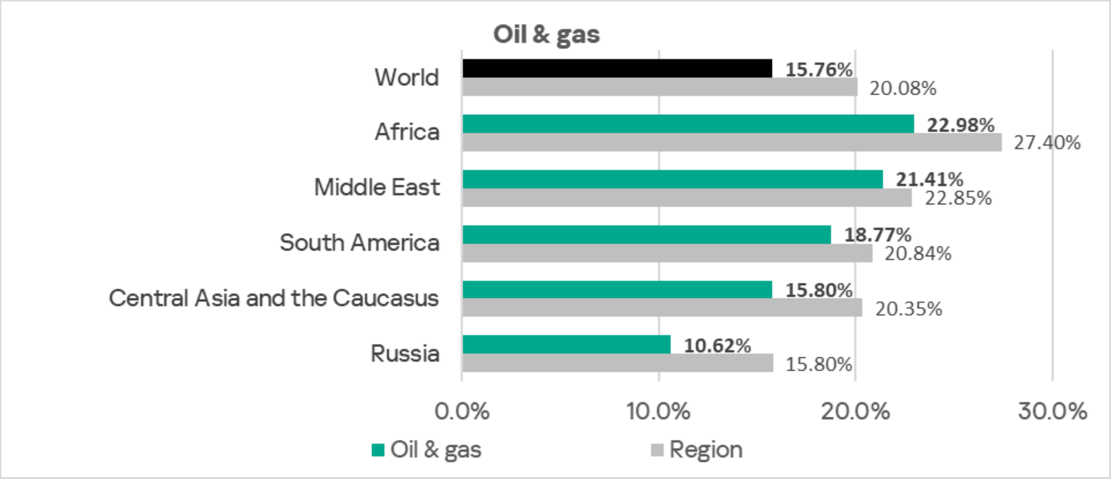


Industries

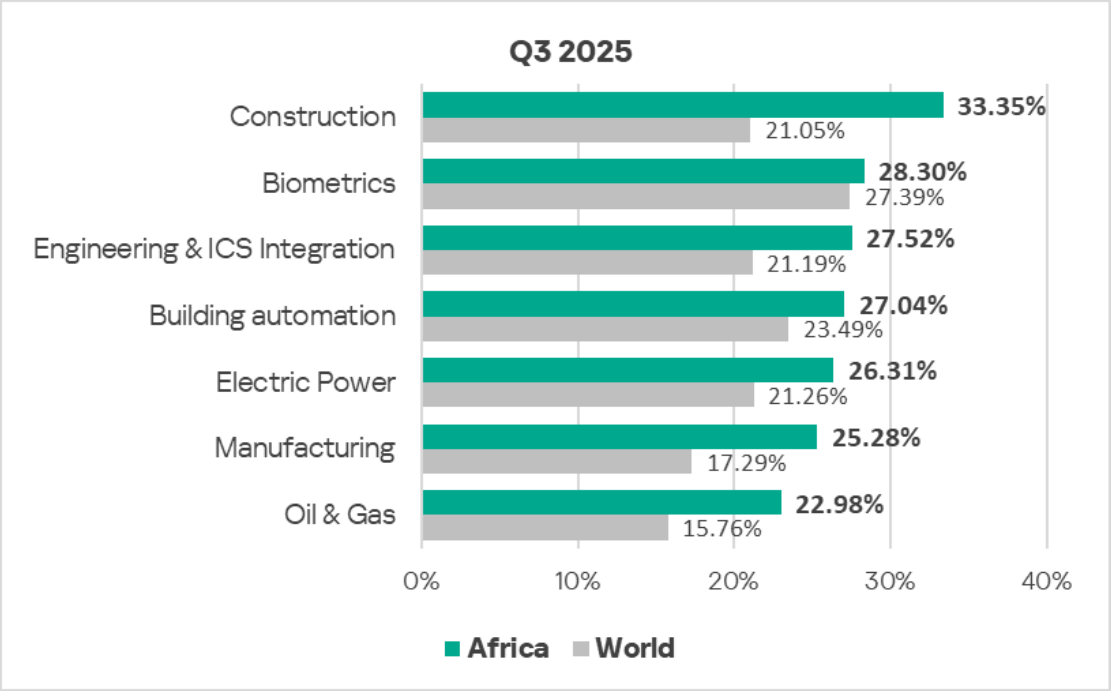
In Africa, construction remains the most frequently threatened industry among those covered in this report. Africa leads globally in the percentage of ICS computers in this industry where malicious objects were blocked.



Africa also leads in the oil and gas sector.

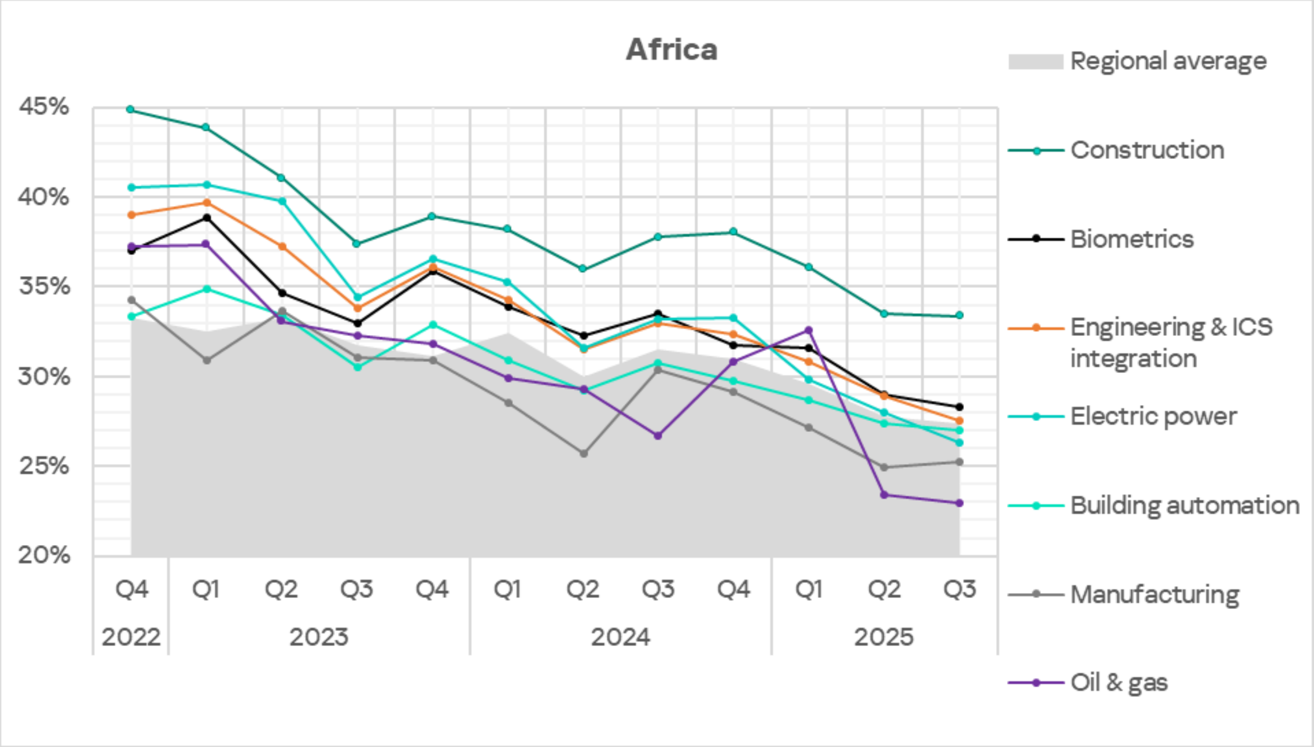


All the region's industries exceed the respective global averages. The largest differences are in construction (1.6 times), manufacturing, and oil and gas (both 1.5 times).



This figure decreased in all industries except manufacturing this quarter.

All the industries covered show positive long-term trends (decreasing values) with significant 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 Africa, Q3 2025

Industry / Threat source	Biometrics	Building automation	Electric power	Engineering & ICS integration	Oil & gas	Construction	Manufacturing	Threat category total in the region
Internet	10.07%	9.60%	11.69%	11.96%	9.59%	12.06%	11.32%	10.31%
Email clients	6.08%	7.18%	2.74%	2.49%	0.85%	3.46%	2.83%	4.18%
Removable media	1.60%	1.11%	1.15%	1.46%	1.33%	1.94%	0.09%	1.43%
Network folders	0.02%	0.02%	0.00%	0.01%	0.00%	0.00%	0.00%	0.02%
Industry total in the region	28.30%	27.04%	26.31%	27.52%	22.98%	33.35%	25.28%	

Threat category indicators for industries in Africa, 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	4.58%	4.25%	6.23%	6.15%	6.48%	6.32%	5.60%	4.96%
Malicious scripts and phishing pages (JS and HTML)	10.69%	11.06%	8.83%	9.44%	9.90%	8.77%	7.22%	9.41%
Spy Trojans, backdoors and keyloggers	8.42%	7.16%	5.62%	5.65%	7.50%	3.58%	4.18%	6.33%
Worms	3.87%	2.84%	3.05%	2.71%	3.46%	2.55%	2.28%	3.16%
Miners in the form of executable files for Windows	0.67%	0.47%	0.50%	0.68%	0.83%	0.28%	0.47%	0.51%
Malicious documents (MSOffice + PDF)	3.69%	4.55%	1.79%	1.69%	2.19%	2.08%	1.04%	2.72%
Viruses	3.65%	2.95%	3.89%	3.33%	6.02%	1.98%	3.61%	3.53%
Ransomware	0.44%	0.33%	0.36%	0.27%	0.31%	0.38%	0.09%	0.29%
Web miners running in browsers	0.30%	0.28%	0.11%	0.37%	0.28%	0.19%	0.19%	0.26%
Malware for AutoCAD	0.12%	0.10%	0.36%	0.38%	1.88%	0.28%	0.47%	0.41%
Industry total in the region	28.30%	27.04%	26.31%	27.52%	22.98%	33.35%	25.28%	

Construction

Among all industries across all regions, Africa's construction sector ranks:

- First place in the percentage of computers where threats were blocked on removable media.

- Second place in the percentage of computers where worms were blocked.

Across regions, Africa ranks:

- First in ICS computers blocking threats when connecting to removable media, and second in internet threats.
- First in ICS computers where threats in the following categories are blocked: denylisted internet resources, malicious scripts and phishing pages, spyware, ransomware, worms.

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

- First place in both the internet threat metric and the percentage of ICS computers on which threats are blocked when connecting removable media.
- First place across several categories at once: denylisted internet resources, viruses, miners in the form of executable files for Windows and malware for AutoCAD. Construction also ranks second in spyware and worms among all industries.

Biometric systems

Among all industries and regions globally, Africa's biometric systems sector ranks:

- First place in the percentage of computers where worms were blocked.

Across regions, Africa ranks:

- Second in ICS computers where threats were blocked when connecting to removable media.
- First in ICS computers where worms were blocked, and second in viruses.

Within Africa's industries, OT infrastructure for biometric systems ranks:

- First in threats from network folders, and second in the percentage of ICS computers on which threats are blocked in email clients and on connected to removable media.
- First in ICS computers where spyware, worms, and ransomware are blocked.
- Second place in malicious scripts and phishing pages, malicious documents, and web miners.

Engineering and ICS integrators

Across regions, Africa ranks:

- First place in the percentage of ICS computers on which internet threats and threats on connected removable media were blocked.
- First place in the percentage of ICS computers on which denylisted internet resources, spyware, and worms are blocked, as well as second place in the following categories: malicious scripts and phishing pages, and ransomware.

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

- Second place in the percentage of ICS computers on which internet threats are blocked, and third place in threats from removable media and network folders.
- First place in the percentage of ICS computers on which web miners are blocked.
- Second place in the percentage of ICS computers on which miners in the form of executable files for Windows are blocked, and third place in malware for AutoCAD.

Building automation

Across regions, Africa ranks:

- First place in ICS computers in the industry where threats on connected removable media are blocked, and third in internet threats.
- Second in the percentage of ICS computers in the industry where in worms and viruses are blocked.
- Third in malicious scripts and phishing pages.

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

- First in email client threats and third in threats from network folders.
- First place in the percentage of ICS computers on which malicious documents, as well as malicious scripts and phishing pages, are blocked.
- Third place in the percentage of ICS computers on which spyware and web miners are blocked.

Electrical energy industry

Across regions, Africa ranks:

- First place in the percentage of ICS computers on which internet threats are blocked, and second place in threats from removable media.

- First place in the percentage of ICS computers on which denylisted internet resources are blocked, second place in worms, and third place in malicious scripts.

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

- Third in the percentage of ICS computers on which internet threats were blocked.
- Second in viruses.
- Third in the following categories: denylisted internet resources, worms, and ransomware.

Manufacturing

Across regions, Africa ranks:

- First place in the percentage of ICS computers on which internet threats are blocked, and third place in email client threats.
- First place in the percentage of ICS computers on which denylisted internet resources and ransomware are blocked. The region is also in second place in malicious scripts and phishing pages, and third place in worms.

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

- Fourth in internet threats and email client threats.
- Second in denylisted internet resources and ransomware.

Oil and gas industry

Across regions, Africa ranks:

- First place in the percentage of ICS computers on which internet threats are blocked, and third place in email client threats.
- First in the percentage of ICS computers on which threats from the following categories are blocked: denylisted internet resources, malicious scripts and phishing pages, spyware, viruses, worms, and malware for AutoCAD.

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

- Second in malware for AutoCAD.

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