kaspersky

Threat landscape for industrial automation systems

Statistics for H2 2021

Kaspersky ICS CERT

03.03.2022 Version 1.0

2021 in numbers

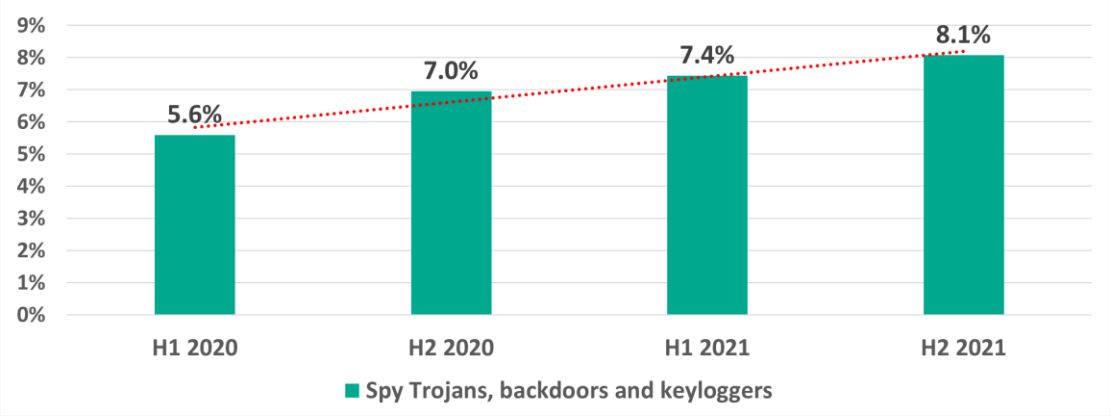
Indicator	H1 2021	H2 2021	2021
Percentage of attacked ICS computers in the world	33.8%	31.4%	39.6%
Percentage of attacked ICS computers by region			
Northern Europe	11.1%	10.4%	12.1%
United States and Canada	16.5%	17.2%	19.7%
Western Europe	15.3%	15.8%	20.2%
Australia and New Zealand	23.7%	21.4%	26.5%
Eastern Europe	29.5%	28.4%	32.4%
Southern Europe	29.4%	25.1%	33.0%
Latin America	32.8%	32.5%	38.7%
South Asia	35.2%	35.6%	41.0%
Middle East	37.3%	34.3%	42.0%
Russia	39.4%	30.0%	42.3%
Central Asia	42.0%	37.9%	44.7%
East Asia	43.2%	40.5%	48.1%
Africa	46.1%	43.4%	50.9%
Southeast Asia	44.2%	47.6%	51.2%
Main threat sources globally			
Internet	18.3%	16.5%	22.2%
Removable devices	5.2%	4.8%	6.7%
Email clients	3.5%	3.7%	4.2%
Network folders	0.52%	0.57%	0.75%

Trends

Since H1 2020, we have seen increases in the percentages of ICS computers on which the following types of objects were blocked:

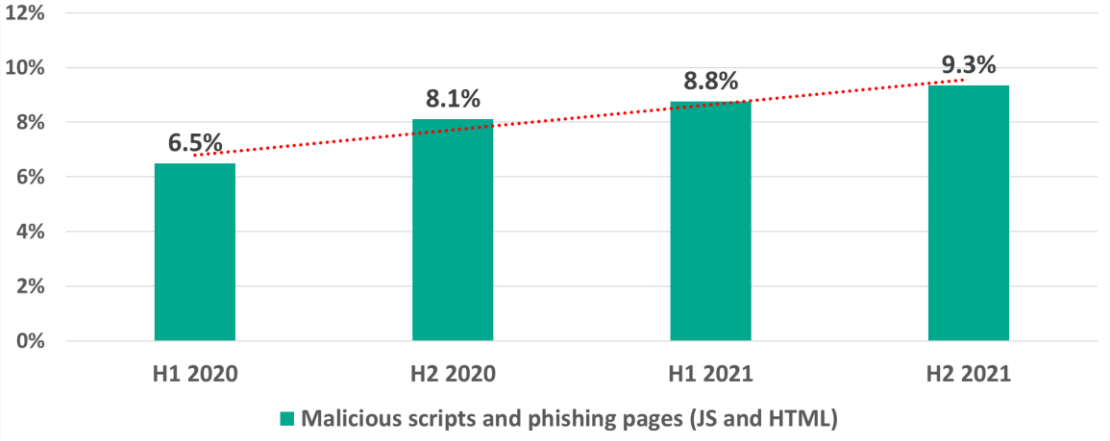
- **Spyware** – by a factor of 1.4 — from 5.6% to 8.1%.

Percentage of ICS computers on which spyware was blocked



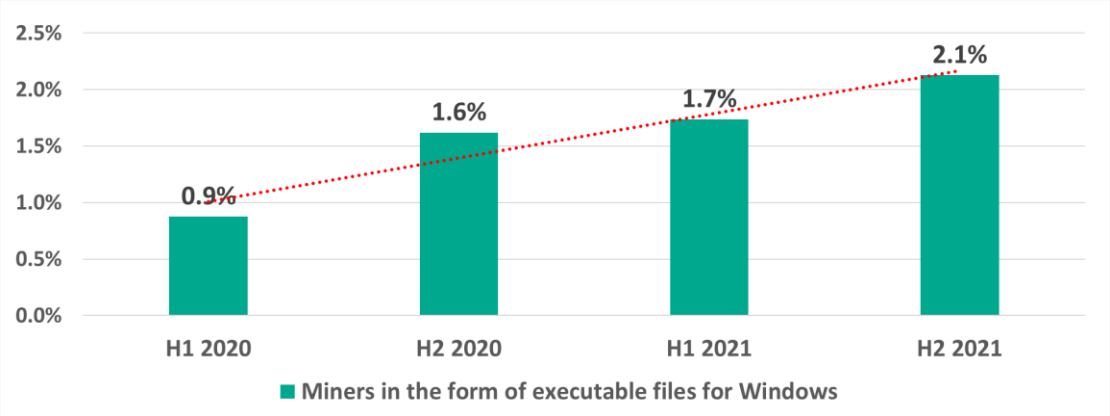
- **Malicious scripts and phishing pages** – by a factor of 1.4 – from 6.5% to 9.3%.

Percentage of ICS computers on which malicious scripts and phishing pages (JS and HTML) were blocked



- **Cryptocurrency miners (Windows executable files)** – more than doubled – from 0.9% to 2.1%.

Percentage of ICS computers on which cryptocurrency miners were blocked



Global statistics

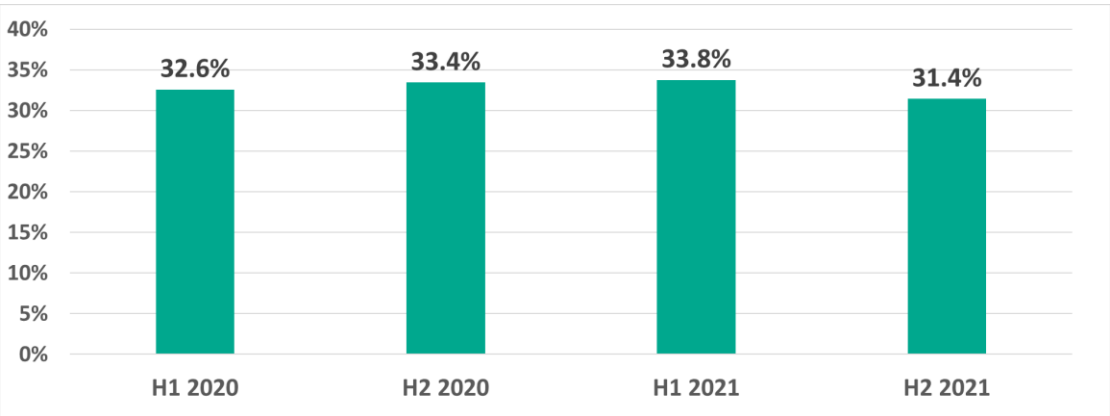
2021 is the second year we have spent living and working in the pandemic. By 2021 everyone got used to pandemic limitations – industrial organization employees and IT security professionals and threat actors. If we compare the numbers from 2020 and 2021, we see that 2021 looks more stable, particularly in H2.

Percentage of ICS computers on which malicious objects were blocked

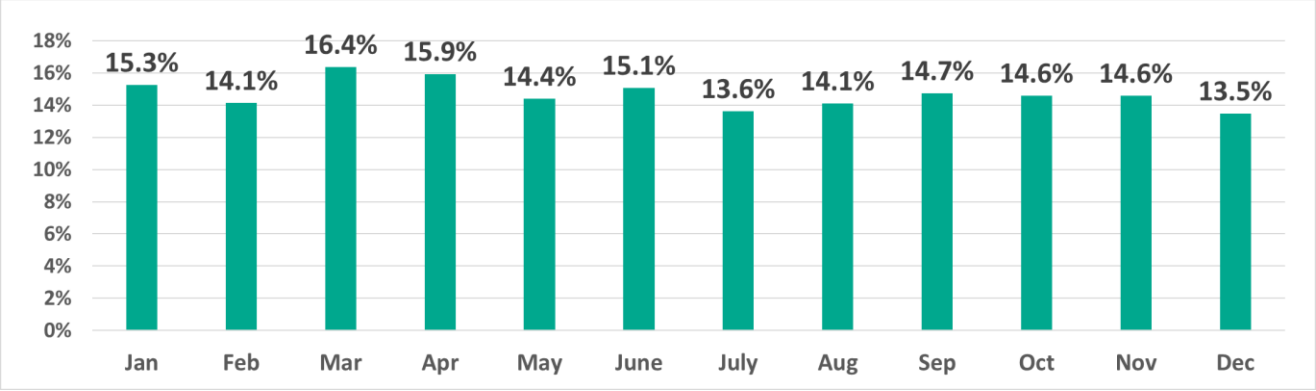
The percentage of ICS computers on which malicious objects were blocked in 2021 increased by 1 percentage point from 2020 – from 38.6% to 39.6%.

However, if the situation is examined by each 6 month period things look better: in H2 2021 this percentage decreased by 1.4 p.p. for the first time in 1.5 years.

Percentage of ICS computers on which malicious objects were blocked



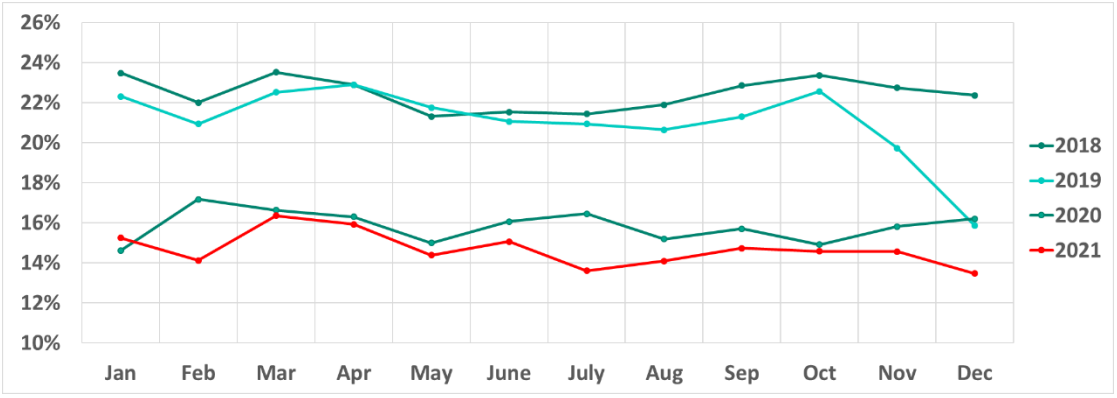
As we can see from the graph depicting the monthly dynamics of the percentage of attacked ICS computers, the numbers in H2 2021 were more stable than in H1 – the numbers were lower and there were no sharp fluctuations.



Percentage of ICS computers on which malicious objects were blocked, January – December 2021

It is also worth noting that in 2021 the vectors of monthly fluctuations (increases and decreases) are the same as those in 2019 and, particularly, in 2018 more often than in 2020. Specifically, we can see decreases in July and August that we believe are due to the traditional vacation periods. However, compared to 2018 and 2019, the summer decrease in the percentage of ICS computers on which malicious objects were blocked was less pronounced in 2021.

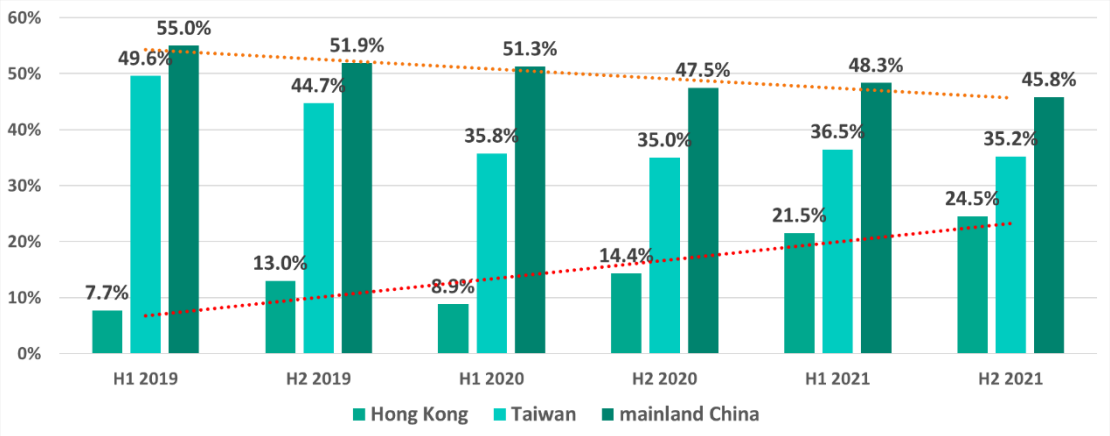
Percentage of ICS computers on which malicious objects were blocked, January – December 2018 – 2021



The situation in different countries varies greatly. Specifically, the percentage of ICS computers on which malicious objects were blocked in H2 2021 ranges from 8.5% in Luxemburg to 54.9% in Vietnam.

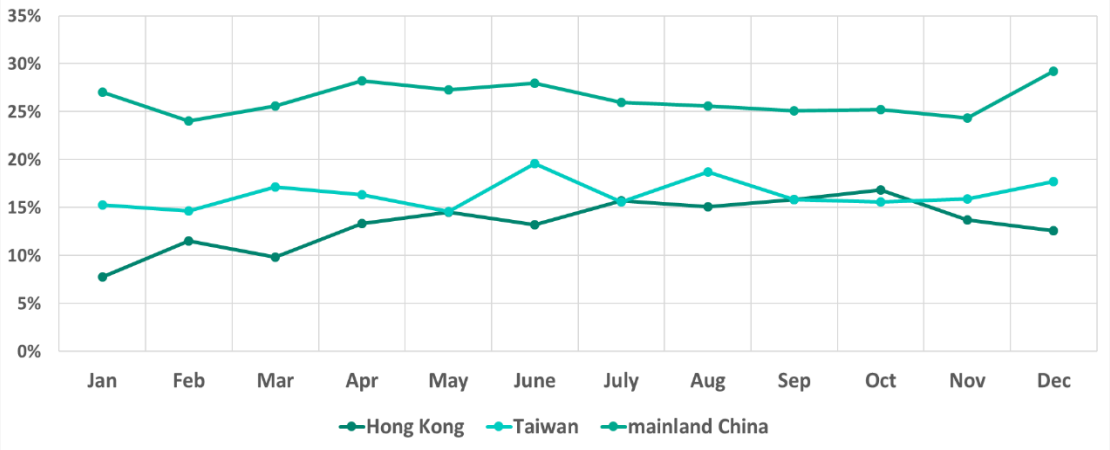
Moreover, the dynamics of this indicator vary significantly in different countries and territories. For example, we saw this number continue to grow in Hong Kong, but at the same time the percentage of ICS computers on which malicious objects were blocked is gradually decreasing in Taiwan and, even more noticeably, in continental China.

Hong Kong, Taiwan, and continental China – percentage of ICS computers on which malicious objects were blocked



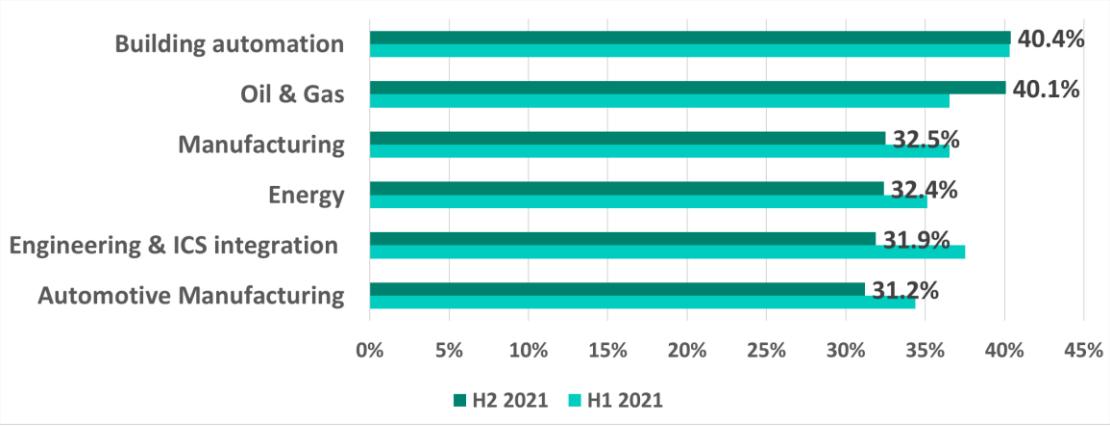
Curiously, monthly changes in the percentage of ICS computers attacked in Taiwan and Hong Kong in 2021 showed reverse dynamics: the indicator moved in opposite directions in these two territories, decreasing in Taiwan as it grew in Hong Kong and vice versa.

Hong Kong, Taiwan and contrinental China – percentage of ICS computers on which malicious objects were blocked, January – December 2021



Selected industries

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



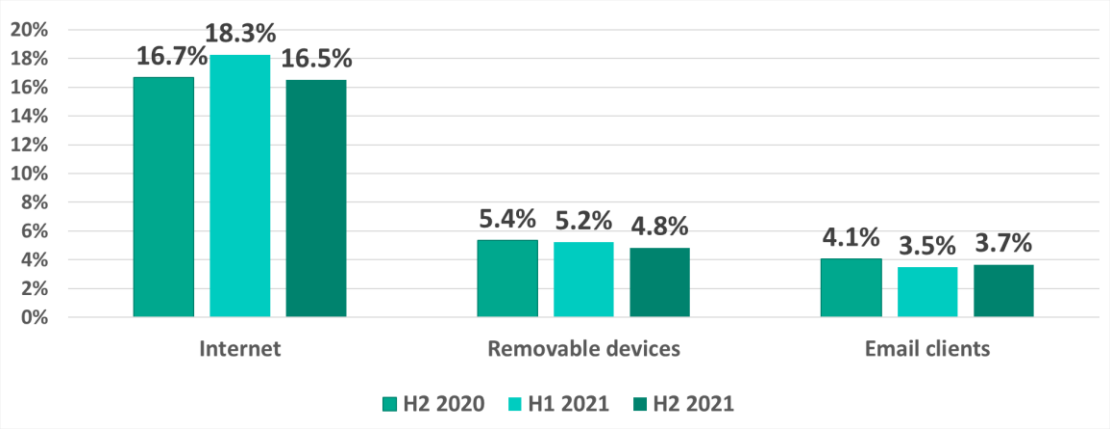
In H2 2021 oil and gas was the only industry where the percentage of ICS computers on which malicious objects were blocked rose (+3.5 p.p.). Interestingly,

in H1 2021 we saw percentages fall across all industries, with the greatest drop in the oil and gas sector (-7.5 p.p.).

Main threat sources

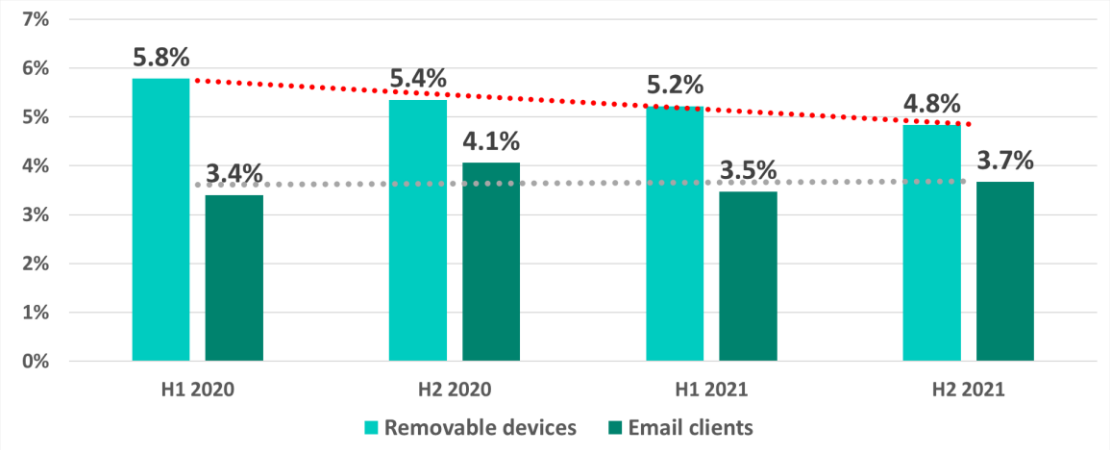
The internet, removable devices and email continue to be the main sources of threats for computers in the OT infrastructures of companies and organizations. It should be noted that in some cases reliably identifying the source of blocked threats is not possible.

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



The Internet remains the main source as usual, with removable devices coming in second and email clients third. However, we are seeing the gap between last two sources gradually closing. The number for **removable devices** has been dropping every half year.

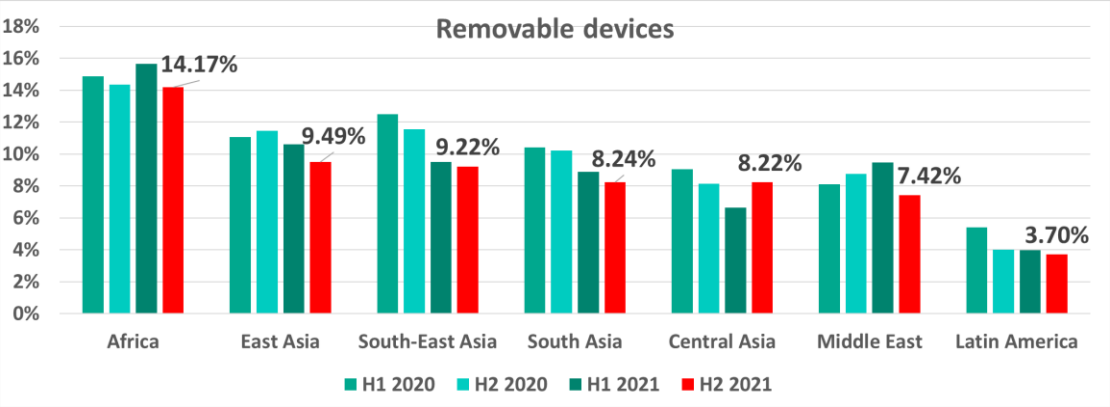
Percentage of ICS computers on which malicious objects were blocked by threat source – removable devices versus email clients



We believe that the decrease in the percentage of ICS computers on which malware was blocked when removable devices were connected to them shows that enterprises are constantly working to increase their minimum levels of security: the number of unprotected systems connected to the network that serve as internal sources of malware infections via removable devices (mostly worms) is falling.

Africa and Asia are the largest contributors to the global percentage of ICS computers on which malicious objects were blocked when removable devices were connected. Africa, whose percentage has not fallen significantly over the past two years, tops the global ranking. In Southeast, South and East Asia, the percentages have been decreasing over a few 6 month periods, which is reflected in the worldwide averages.

Percentage of ICS computers on which malicious objects were blocked when removable devices were connected, selected regions

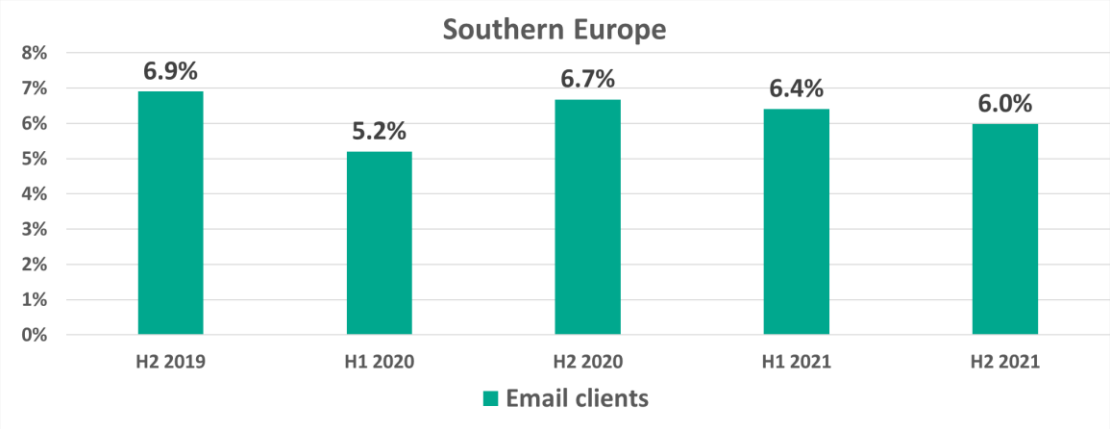


We see that in Central Asia the percentage of ICS computers on which threats were blocked when removable devices were connected is also decreasing every 6 month period except for H2 2021 when it rose again. Interestingly, we see the opposite in the Middle East where the percentage grew over every 6 month period until H2 2021 when it dropped noticeably.

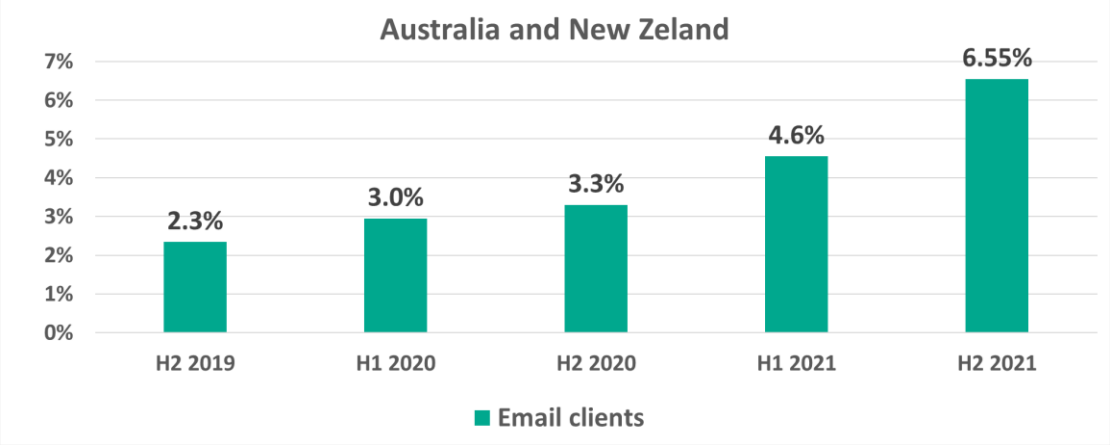
Despite the positive dynamics in the worldwide statistics, the percentage of ICS computers where malicious objects were blocked when removable devices were connected is still alarmingly high. In H2 2021 Algeria led with 19.7%. At the same time in Japan and Denmark there was almost no malware detected on removable devices when they were connected to ICS computers.

In H2 2021, Australia, New Zealand and Southern Europe led the ranking of regions by the percentage of ICS computers on which malicious objects were blocked in **email attachments**. While this percentage is traditionally high in Southern Europe, it has nearly tripled in Australia and New Zealand in the past two years.

Southern Europe – percentage of ICS computers on which malicious objects were blocked in email attachments

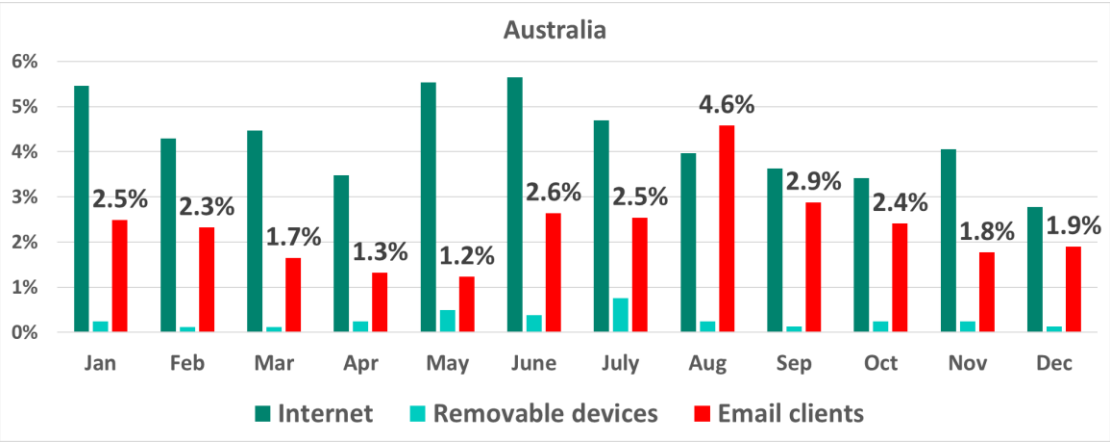


Australia and New Zealand – percentage of ICS computers on which malicious objects in email attachments were blocked



In these regions, email makes a significant contribution to the stream of threats. For example, in August 2021 the percentage of ICS computers on which malicious email attachments were blocked was higher in Australia than the percentages for other sources of threats, including the internet.

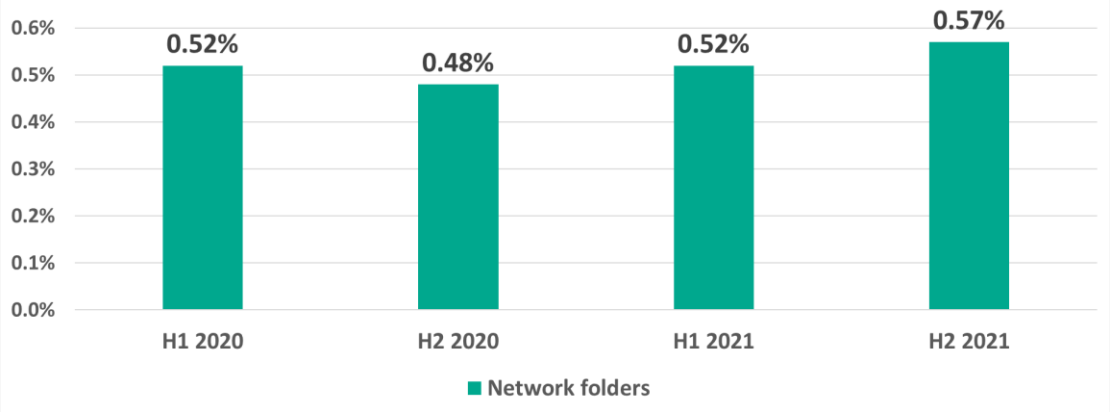
Australia – percentage of ICS computers on which malicious objects from various sources were blocked, January – December 2021



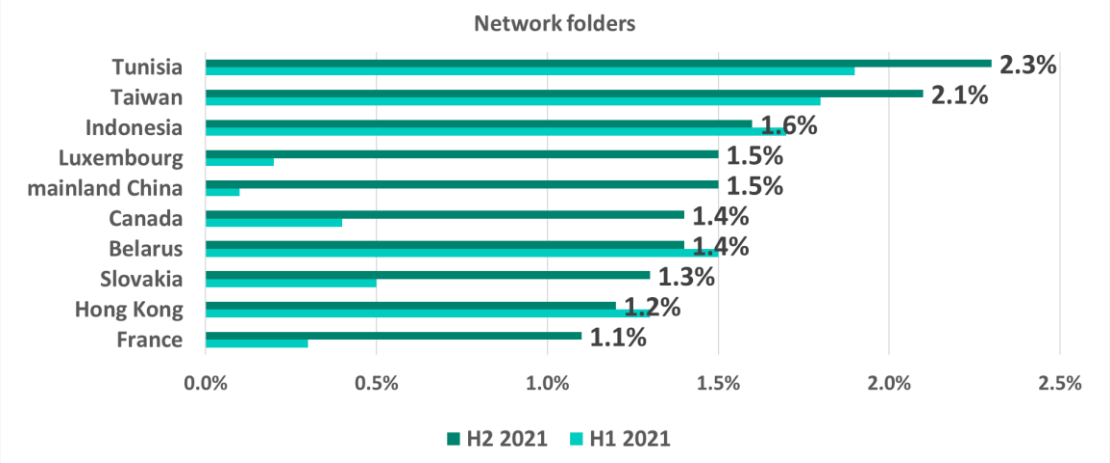
We recommend that security professionals in these regions pay special attention to protecting employees from phishing scams.

Shared network folders are one of the minor threat sources. Only on 0.57% of attacked ICS computers malicious objects were blocked in network shares in H2 2021. However, this percentage is slowly growing and is over 1% in a few countries and territories.

Percentage of ICS computers on which malicious objects were blocked in shared network folders



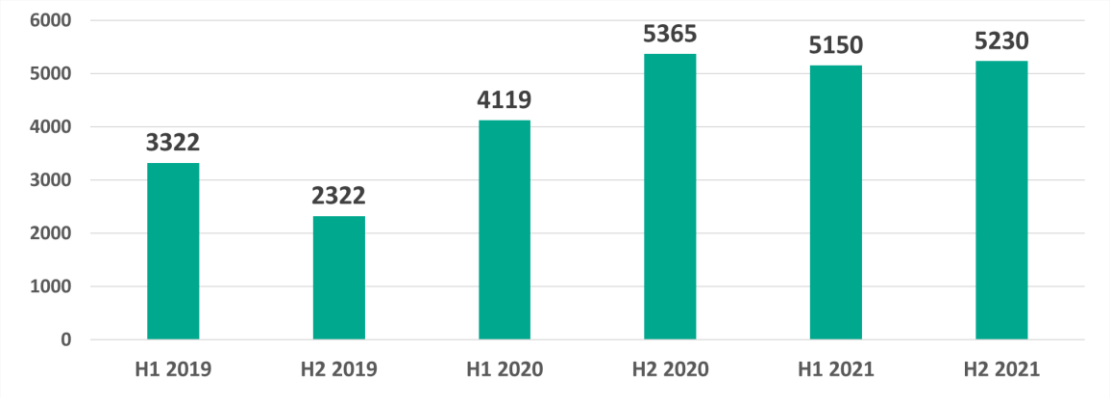
Countries and territories with the largest percentage of ICS computers on which malicious objects were blocked in shared network folders in H2 2021



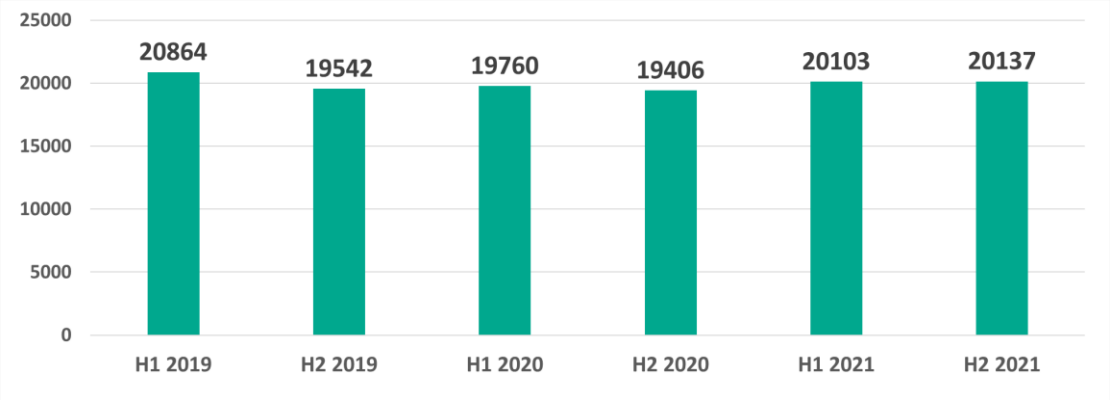
Variety of detected malware

In H2 2021 Kaspersky security solutions blocked over 20,000 malware variants from 5,230 families on ICS computers.

Number of malware families blocked on ICS computers



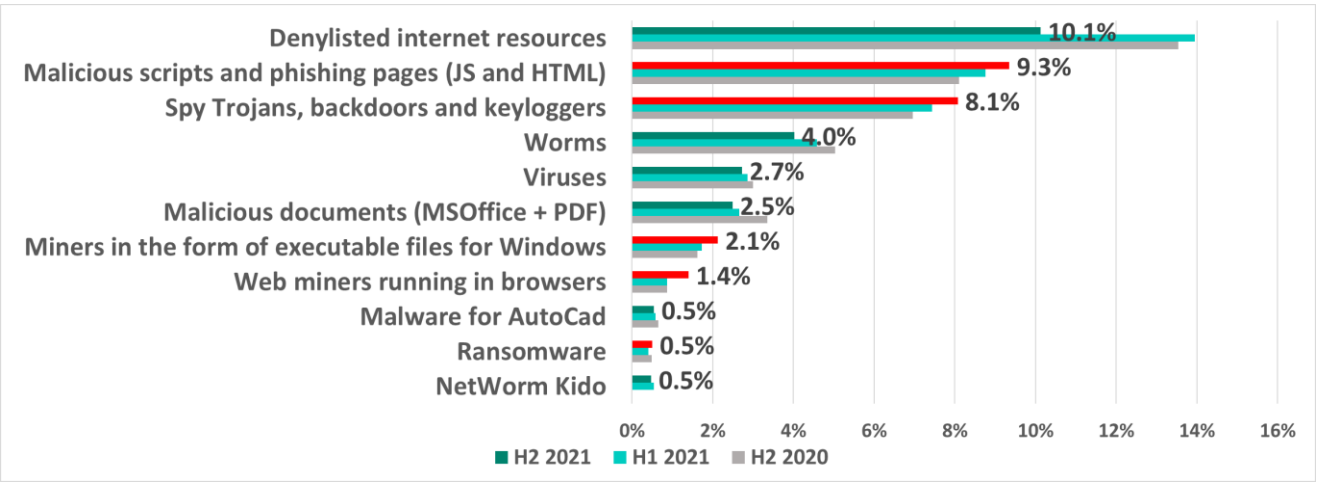
Number of malware variants blocked on ICS computers



Malware categories

Malicious objects blocked by Kaspersky products on ICS computers fall into many categories. You can find a brief description of each category in a separate document.

The results of our analysis revealed the following estimated percentages of ICS computers on which the activity of malicious objects from different categories had been prevented:



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

*Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period.

Denylisted internet resources

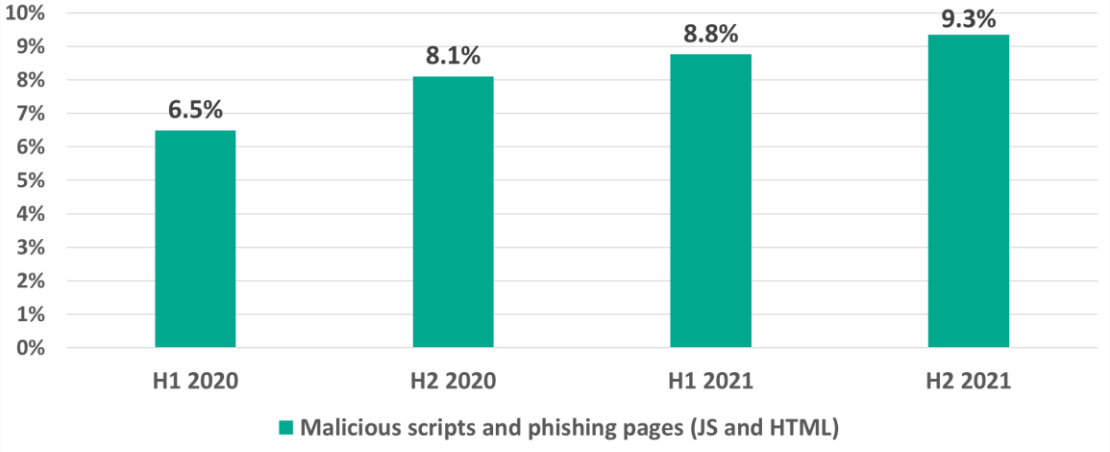
Based on the percentages of attacked ICS computers, we see that the leader continues to be denylisted internet resources, a significant part of which is used to distribute malicious scripts and phishing pages (HTML). The most noticeable change in H2 was the -3.9 p.p. decrease in the share of this threat category.

To a great degree, the lower figures for blocked denylisted web resources were caused by proactively blocking malicious scripts built into browser extensions, as well as deleting malicious script loaders from numerous legitimate sites (including untrustworthy or insecure ad modules). Many such web resources and related malicious scripts were spread mostly in Russia and former Soviet republics.

Malicious scripts and phishing pages (JS and HTML)

In second place we have malicious scripts and phishing pages (JS and HTML), distributed both via the internet and phishing emails (including office documents and/or archives). The percentage of ICS computers on which malicious scripts and phishing pages were blocked is rising steadily year to year – it has increased 1.4 times from the beginning of 2020.

Percentage of ICS computers on which malicious scripts and phishing pages (JS and HTML) were blocked

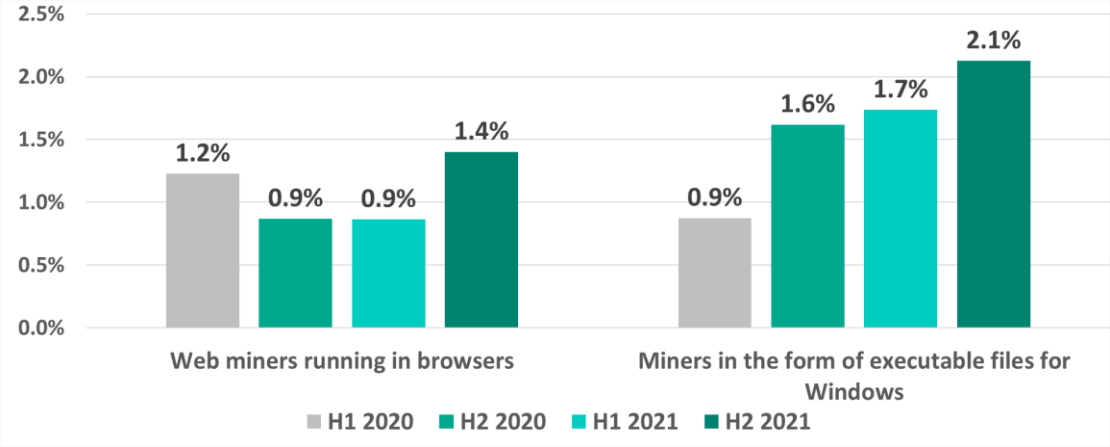


Malicious scripts are used by threat actors to achieve very different goals ranging from data collection, tracking and re-directing user browsers to malicious web resources to loading various malware (such as spyware or cryptocurrency miners) onto user systems or into browsers.

Miners

Significantly, as threat actors use scripts more and more, they are also using cryptocurrency miners increasingly. The percentage of ICS computers on which miners (executable Windows files) were blocked has more than doubled from H1 2020. In H2 2021 we see the percentage of web miners growing as well.

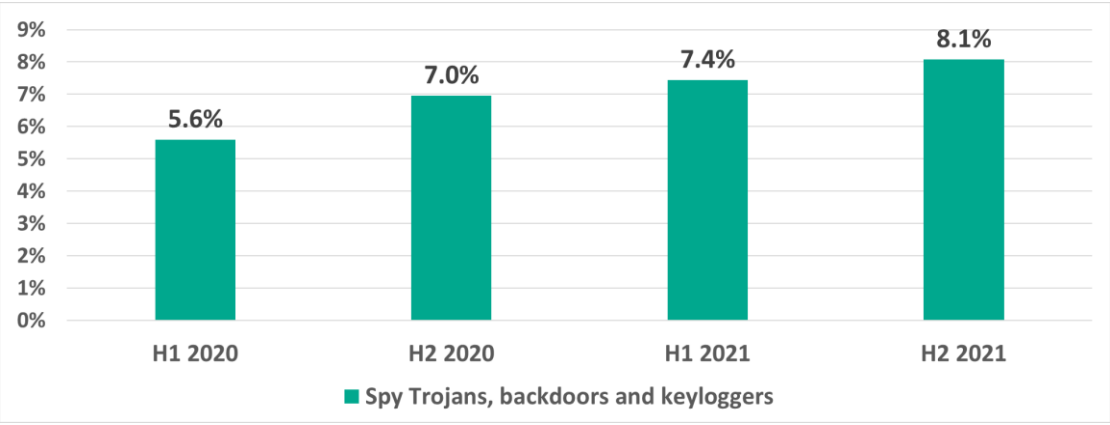
Percentage of ICS computers on which cryptocurrency miners were blocked



Spyware

Spyware (Trojan-Spy, backdoors and keyloggers) is in third place. These threats are designed to provide attackers with hidden remote access to the infected system and/or to steal data, including authentication credentials. The percentage of ICS computers on which spyware was blocked has grown by a factor of 1.4 since H1 2020.

Percentage of ICS computers on which spyware was blocked



In 2021 Kaspersky ICS CERT experts spotted numerous attacks on ICS computers using spyware. About 20% of all spyware samples blocked on ICS computers worldwide were used in limited-scope attacks with short malware lifespans. The spyware samples used in these campaigns were quite conventional, i.e., from the arsenal used often by threat actors in larger-scale attacks. In many cases the malware was sent from organization to organization in phishing emails disguised as normal correspondence between the victim organizations.

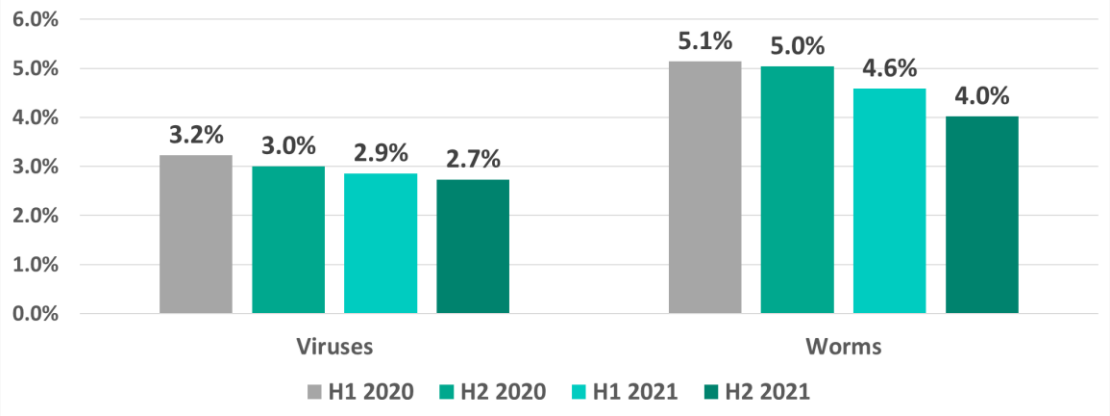
Kaspersky has recently released a report where we provided an analysis of the TTPs of these attacks and a large part of the malicious ecosystem – from the MaaS platforms and testing and debugging infrastructure to user forums and

online marketplaces where threat actors buy and sell authentication credentials for hidden remote access to computers of various industrial organizations.

Viruses and worms

As usual, viruses and worms are in fourth and fifth place, respectively. The good news is that the percentage of ICS computers on which these types of malware are blocked is slowly, but steadily decreasing.

Percentage of ICS computers on which viruses and worms were blocked



Viruses and worms continue to live out their lifespans in ICS networks, where they spread via network shares, removable devices, infected files (including backups) and network attacks on hopelessly out-of-date software such as Radmin2. We are seeing that old viruses, such as Virut and Sality, and old worms, such as Kido/Conficker are not really active since their command-and-control servers were taken down long ago.

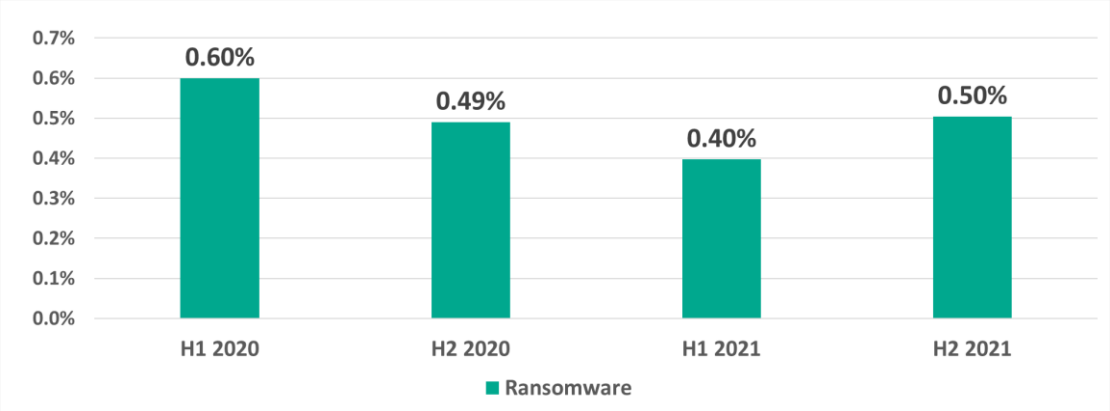
However, they not only still weaken the defenses of infected systems by opening network ports and changing settings, but can also cause software crashes and denial-of-service conditions.

At the same time, new versions of worms do appear in ICS networks. These are used by threat actors to distribute spyware, ransomware and miners across networks. These worms usually spread by using exploits for vulnerabilities in network services (such as SMB or RDP) for which vendors have released fixes but which remain unpatched on industrial networks, or authentication credentials stolen previously or even good old password brute-forcing.

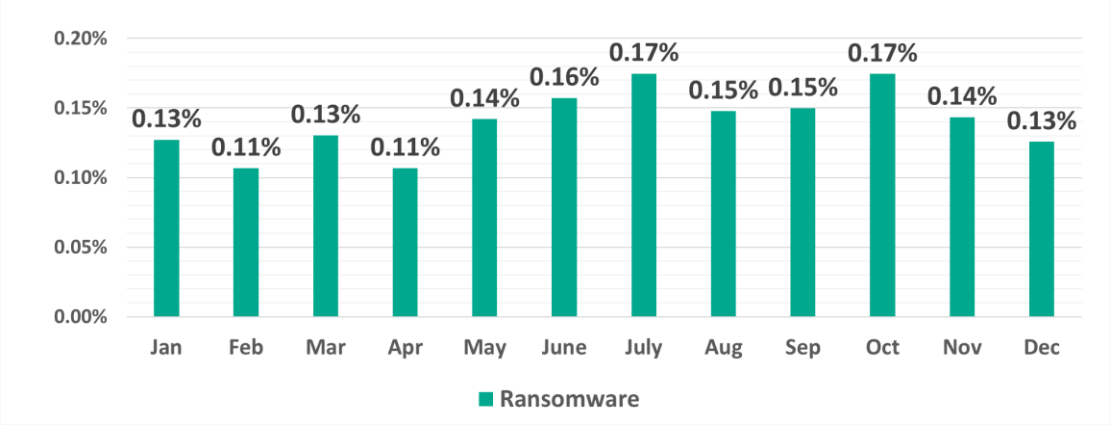
Ransomware

In H2 2021 ransomware was blocked on 0.50% of ICS computers. The highest percentage of ICS computers on which ransomware was blocked in 2021 was recorded in July and October (0.17%) and the lowest in February and April (0.11%).

Percentage of ICS computers on which ransomware was blocked

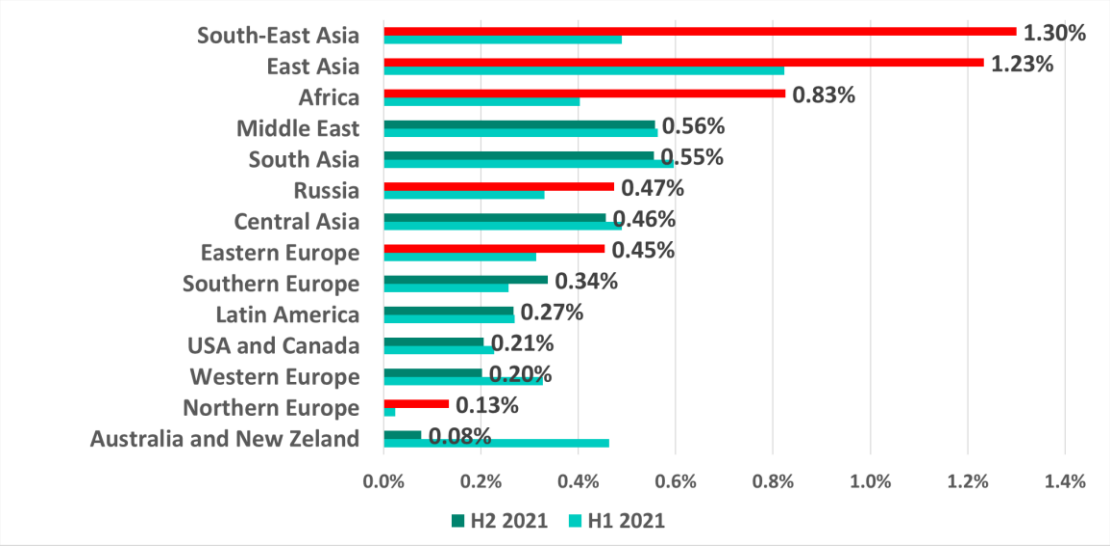


Percentage of ICS computers on which ransomware was blocked, January – December 2021



In H2 2021 the percentage of ICS computers attacked by ransomware increased in half of the world's regions. The most significant increases were recorded in Southeast Asia, East Asia and Africa, which are thus the leaders in this ranking.

Regions ranked by percentage of ICS computers on which ransomware was blocked, H2 2021

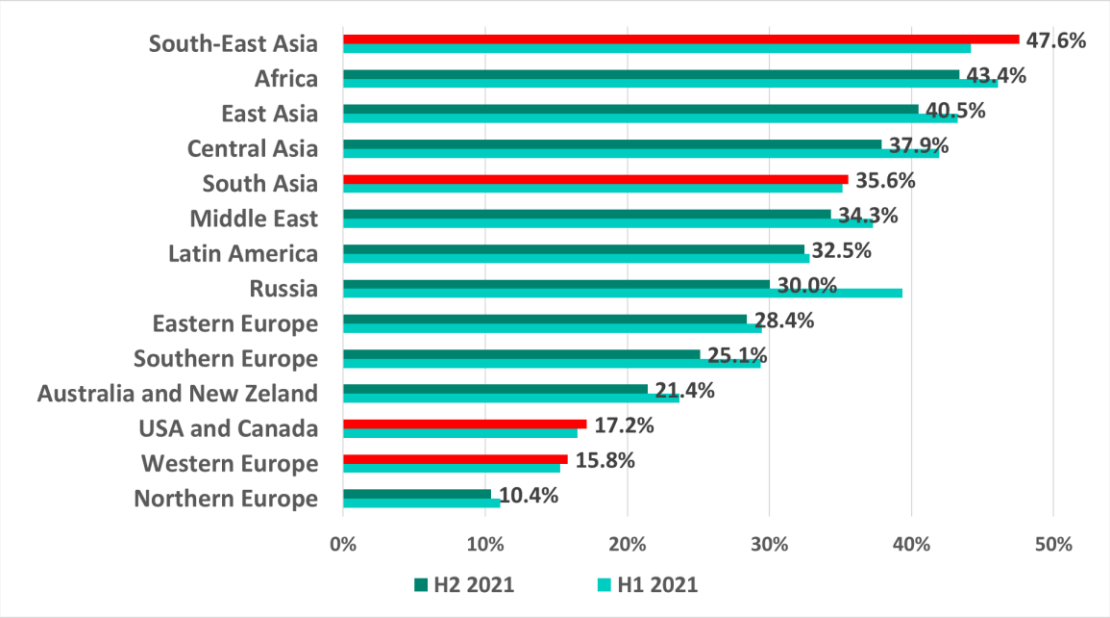


Geographical distribution

Percentage of ICS computers on which malicious objects were blocked: geography

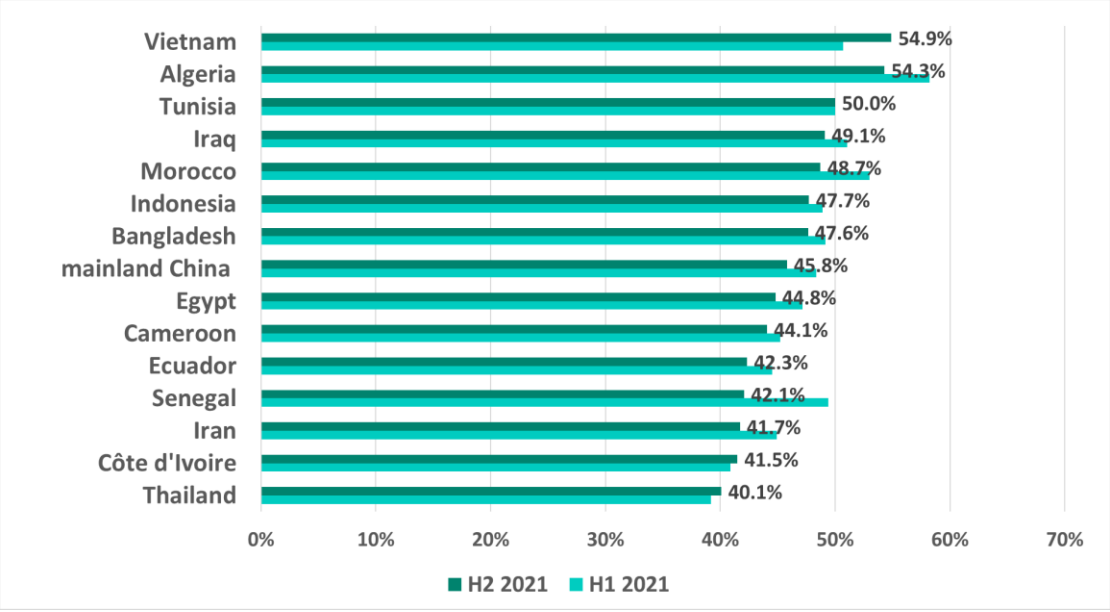
Southeast Asia, Africa, East Asia and Central Asia lead in the ranking of global regions based on the percentage of ICS computers on which malicious activity was prevented.

Regions ranked according to percentage of ICS computers on which malicious objects were blocked in H2 2021



The largest increase (+3.4 p.p.) in the percentage of ICS computers on which malicious objects were blocked was recorded in Southeast Asia.

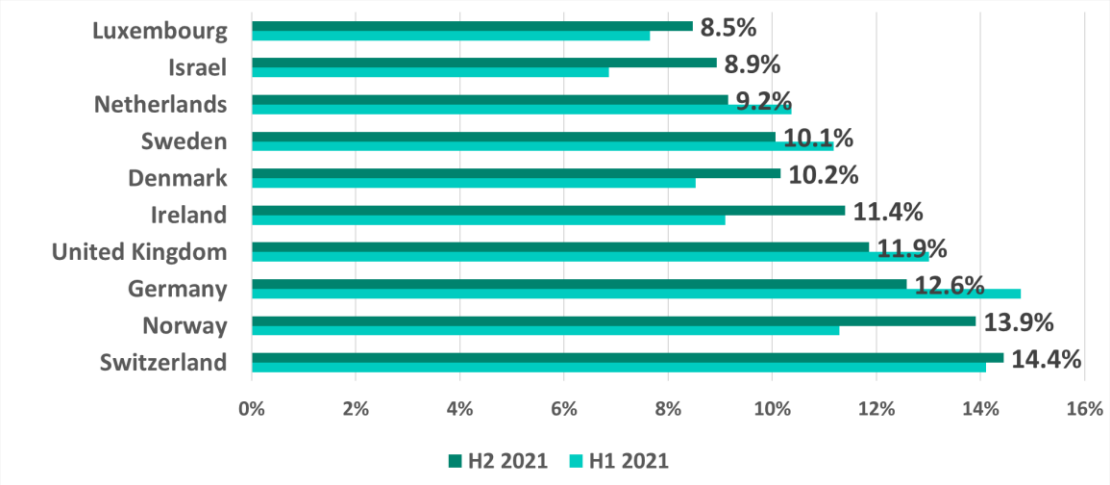
Top 15 countries and territories with the largest percentages of ICS computers on which malicious objects were blocked in H2 2021



The most significant increase in the percentage of ICS computers on which malicious objects were blocked was recorded in the Philippines (+5.1 p.p.), in Peru (+5.0 p.p.) and in Argentina (+4.9 p.p.).

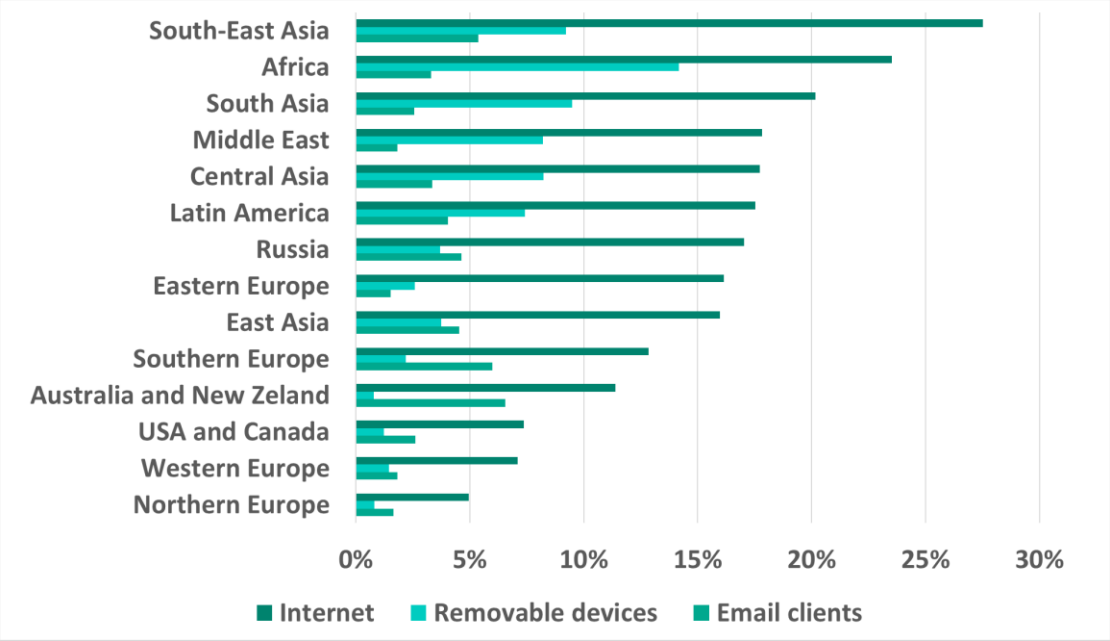
The lowest percentage in H2 2021 was recorded in Luxemburg.

10 countries and regions with the smallest percentage of ICS computers where malicious objects were blocked in H2 2021



Main threat sources: regional and country data

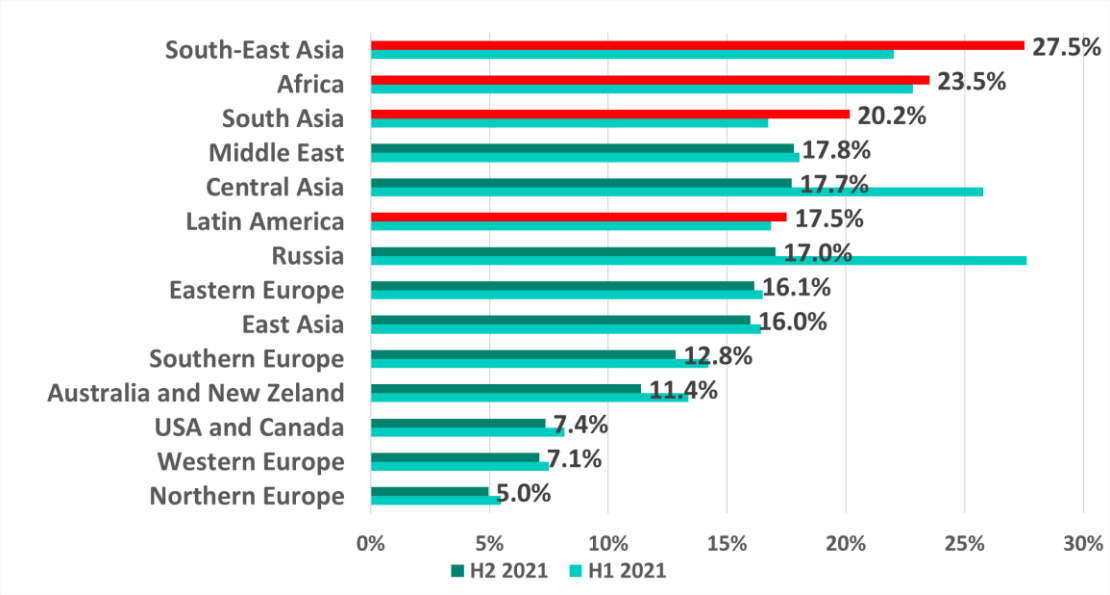
Main sources of threats blocked on ICS computers, by regions of the world, H2 2021



Internet

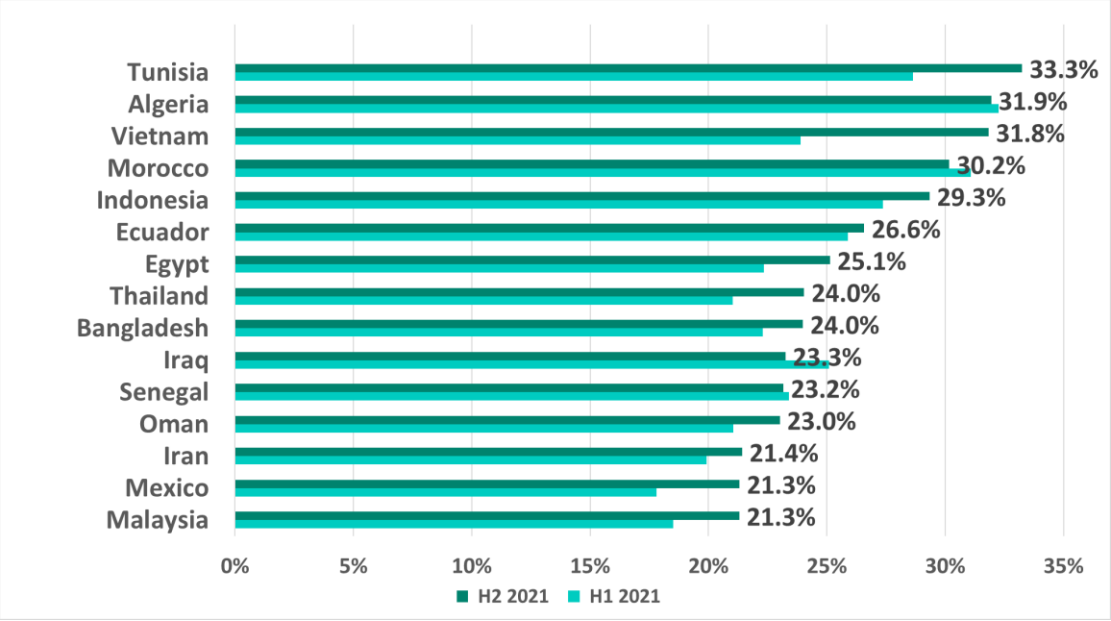
The percentage of ICS computers on which internet threats were blocked in H2 2021 grew in 4 regions in the world, most noticeably in Southeast Asia (+5.6 p.p.) and South Asia (+3.3 p.p.).

Regions ranked according to percentage of ICS computers on which internet threats were blocked, H2 2021



Among countries and territories, the leaders are in Asia, Africa and the Middle East. Only one country from Latin America made it into the Top 15 – Mexico.

TOP 15 countries and territories with the highest percentage of ICS computers on which internet threats were blocked in H2 2021

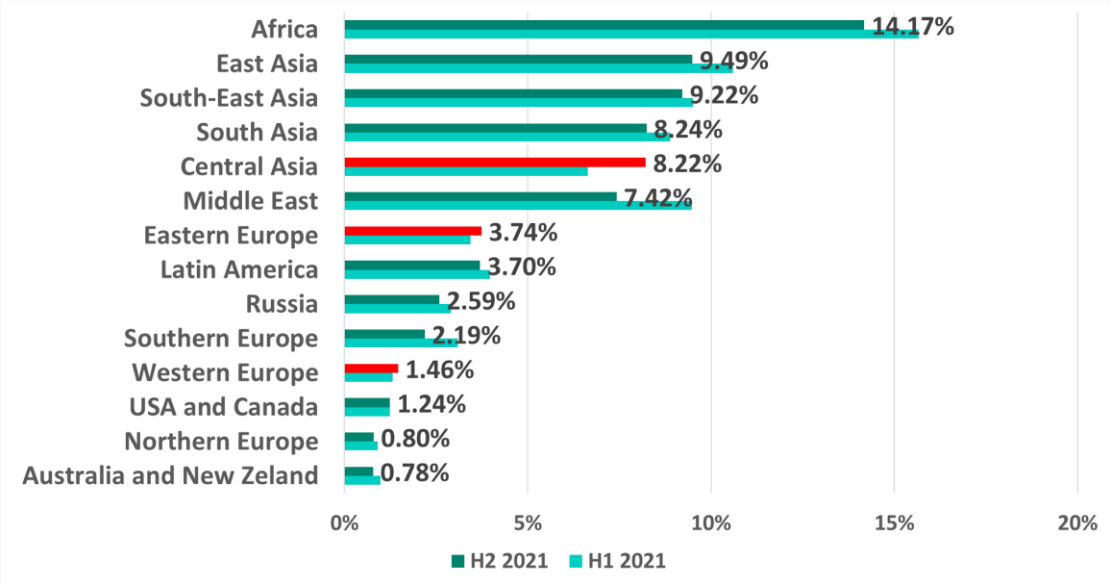


The biggest increase in the percentage of ICS computers on which malicious objects from the internet were blocked in H2 2021 was recorded in Vietnam (+7.9 p.p.).

Removable devices

As usual, Africa, some Asian regions and the Middle East led in our rankings by the percentage of ICS computers on which malware was blocked when removable devices were attached.

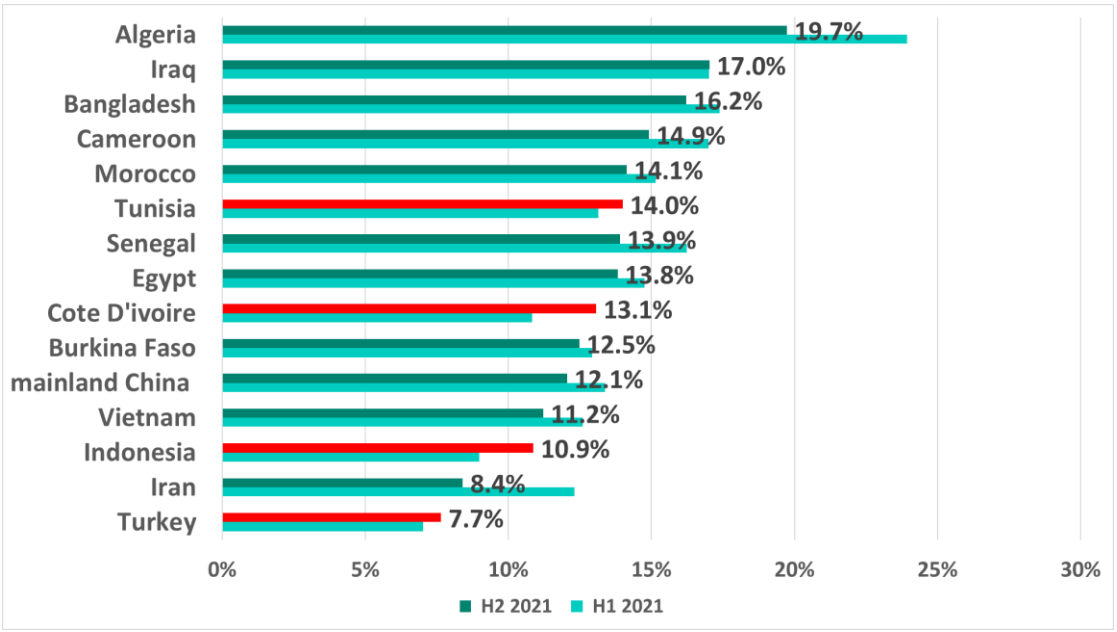
Regions ranked according to percentage of ICS computers on which malware was blocked when removable devices were connected, H2 2021



In H2 2021 this percentage decreased in all regions except for Central Asia, Eastern Europe and Western Europe.

In H2 2021 amongst the 15 countries and regions ranked by percentage of ICS computers on which malware was blocked when removable devices were connected the percentage grew in only 4 countries.

TOP 15 countries and territories ranked by percentage of ICS computers on which malware was blocked when removable devices were attached, H2 2021

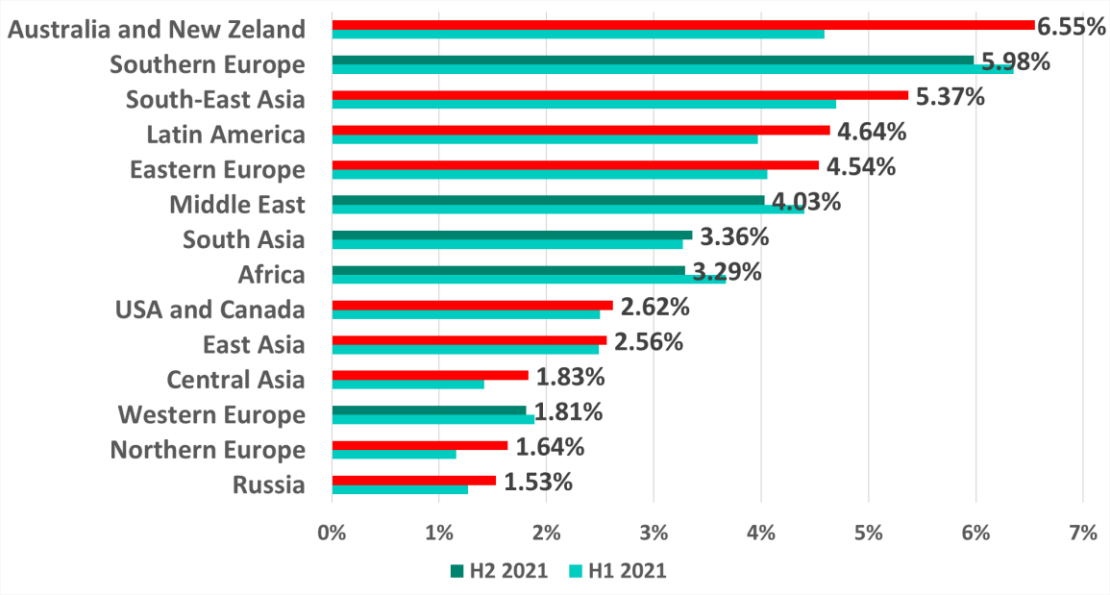


Email clients

Surprisingly, Australia and New Zealand led in the ranking of regions based on the percentage of ICS computers on which malicious email attachments were blocked in H2 2021 with an increase from 4.55% to 6.55%.

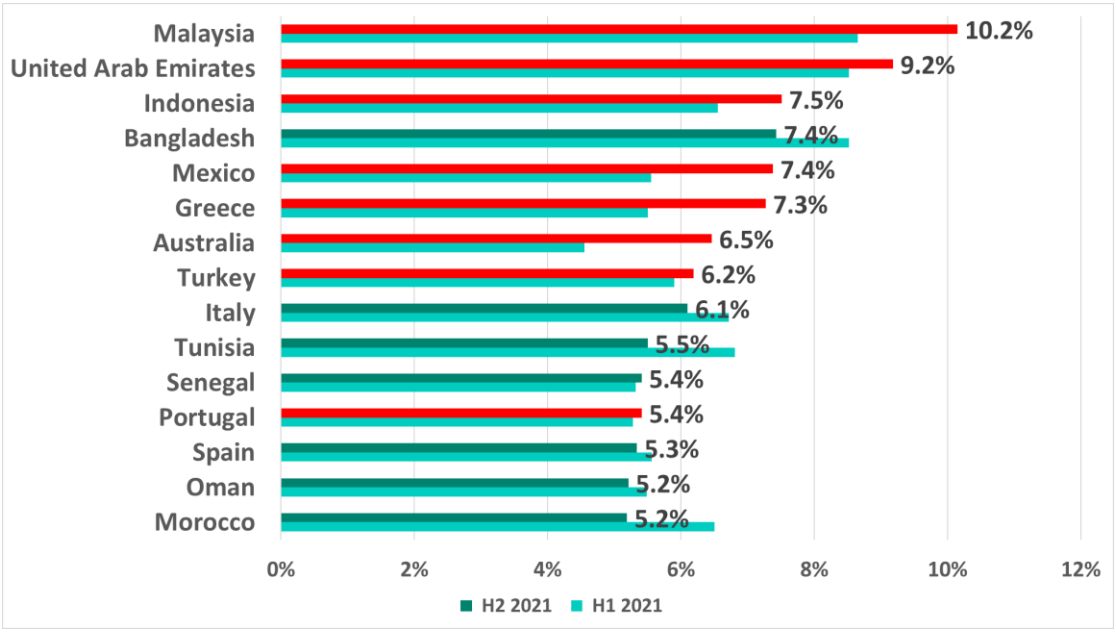
Notice that in H1 2021 Australia and New Zealand was the only region where this percentage increased (+1.3 p.p.). In H2 2021 we saw this percentage increase in 10 out of 14 regions worldwide.

Regions ranked by percentage of ICS computers on which malicious email attachments were blocked, H2 2021



Australia is in 7th place (6.5%) among countries and territories with the largest percentages of ICS computers on which malicious email attachments were blocked. Malaysia led with a record breaking 10.2%.

TOP 15 countries and territories ranked by the percentage of ICS computers on which malicious email attachments were blocked, H2 2021



Just as in H1 2021, we see the following European countries in this ranking – Greece, Italy, Portugal, and Spain.

Methodology used to prepare statistics

This report presents the findings of an analysis of statistical data obtained using the distributed antivirus network known as Kaspersky Security Network (KSN). The data was received from those KSN users who gave their voluntary consent to have data anonymously transferred from their computers and processed for the purpose described in the KSN Agreement for the Kaspersky product installed on their computer.

Connecting to the KSN network enables our customers to reduce the time it takes the security solutions installed on their systems to respond to previously unknown threats and to improve the overall detection quality provided by the security products through querying the cloud infrastructure in which malicious object data is stored. That data is technically impossible to transfer entirely to the client side due to its large size and resource consumption.

The telemetry data transferred by the user includes only those types and categories of information that are described in the relevant KSN Agreement. This data is not only significantly helpful in analyzing the threat landscape, but it is also necessary for identifying new threats, including targeted attacks and advanced persistent threats (APT)[1].

The statistical data presented in the report was received from ICS computers protected by Kaspersky products that Kaspersky ICS CERT categorizes as part of the industrial infrastructure at organizations. This group includes Windows computers that perform one or several of the following functions:

- Supervisory control and data acquisition (SCADA) servers;
- Data storage servers (Historian);
- Data gateways (OPC);
- Stationary workstations of engineers and operators;
- Mobile workstations of engineers and operators;
- Human Machine Interface (HMI);
- Computers used for industrial network administration;
- Computers used to develop software for industrial automation.

For the purposes of this report, "attacked computers" are those on which Kaspersky security solutions blocked one or more threats during the reporting period. When determining the percentages of machines on which malware infections were prevented, we use the ratio of the number of computers attacked during the reporting period to the total number of computers in our sample from which we received depersonalized information during the reporting period.

[1] We recommend that organizations which have any restrictions in place with respect to transferring data outside the organization's perimeter should consider using the Kaspersky Private Security Network service.

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global project of Kaspersky 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