kaspersky

Threat landscape for industrial automation systems

Statistics for H1 2021

Kaspersky ICS CERT

09.09.2021 Version 1.0

H1 2021 Report at a glance

Percentage of ICS computers attacked

1. During the first half of 2021 (H1 2021) the **percentage of attacked ICS computers** was **33.8%**, which was 0.4 percentage points (p.p.) higher than in H2 2020.

   Per country the number varied from 58.4% in Algeria to 6.8% in Israel.

   If we look at regional numbers, Africa led with 46.1%, followed by Southeast Asia at 44.1%, East Asia at 43.1% and Central Asia at 42.1%.

2. **The largest increases in the percentage of attacked ICS computers** during H1 2021 were as follows:

   - Over 10 p.p. in Belarus (50.4%) and Ukraine (33.1%);
   - 7.4 p.p. in the Czech Republic (20.2%) and Slovakia (24.3%);
   - 6.5 p.p. in Hong Kong (20.8%);
   - 6 p.p. in Australia (23%) and Cameroon (45.2%).

   The internet was the main source of threats causing these increases.

3. The percentage of ICS computers on which threats were blocked decreased **in all monitored industries**. This was especially noticeable in the oil and gas (36.5%) and building automation (40.3%) sectors (-7.5 p.p. and -6.3 p.p., respectively).

Main threat sources

The internet, removable media and email continue to be the main sources of threats to computers in ICS environments.

1. **Threats from the internet** were blocked on 18.2% of ICS computers (+1.5 p.p.).

   In H1 2021, the largest increases of this indicator were observed in Belarus (+12.2 p.p.), Ukraine (+8 p.p.) and Russia (+6.7 p.p.)

   Russia headed this rating among regions with 27.6% and Belarus among individual countries with 32.8%.

2. **Threats arriving via removable media connections** were blocked on 5.2% of ICS computers (-0.2 p.p.), which continues a downward trend beginning in H2 2019.

   Africa leads noticeably amidst regional rankings with 15.6%, and Algeria leads among individual countries with 24%.

In H1 2021 the percentage of ICS computers on which threats were blocked when removable media were connected to them decreased in Asian regions.

3. **Malicious email attachments** were blocked on 3.4% of ICS computers (-0.6 p.p.).

   Southern Europe was the highest ranked region for this indicator with 6.4%, while Bangladesh led among individual countries with 8.8%.

   The only region where the percentage increased was Australia and New Zealand (+1.3 p.p.)

The variety of malware detected

In H1 2021 Kaspersky security solutions blocked over 20.1 thousand malware variants from 5,150 families in ICS environments.

1. **Denylisted internet resources** were the main threat source and were blocked on 14% of ICS computers.

   Threat actors use malicious scripts on various media resources and sites hosting pirated content. These scripts redirect users to websites that spread spyware and/or cryptocurrency miners. The percentage of computers where such threats have been blocked has been growing since 2020.

2. **Malicious scripts and redirects (JS and HTML)** were blocked on 8.8% of ICS computers (+0.7 p,p,).

   Australia and New Zealand (+3.8 p.p.), as well as Russia (+4.4 p.p.) saw a noticeable growth in the percentage of computers where malicious downloader scripts used for downloading spyware were blocked.

3. **Spyware (backdoors, Trojan spies and keyloggers)** were blocked on 7.4% of ICS computers (+0.4 p.p.).

   This indicator was highest in East Asia (14.3%), Africa (13.4%) and Southeast Asia (11.2%).

4. **Ransomware** was blocked on 0.40% of ICS computers (-0.1 p.p.)

   This indicator is highest in East Asia with 0.82%.

   In the Middle East we saw an increase in the percentage of computers on which worms (+0.4 p.p.) and ransomware (+0.3 p.p.) were blocked.

Global statistics

This section of the 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].

Methodology used to prepare statistics

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 systems.

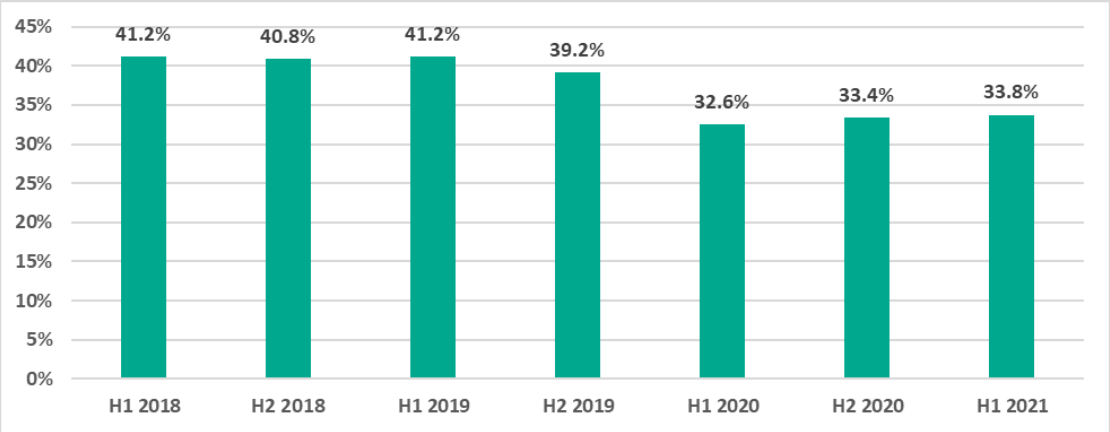
[1] We recommend that organizations which have any restrictions in place with respect to transferring data outside the organization's perimeter should consider using the Kaspersky Private Security Network service.

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.

Percentage of ICS computers on which malicious objects were blocked

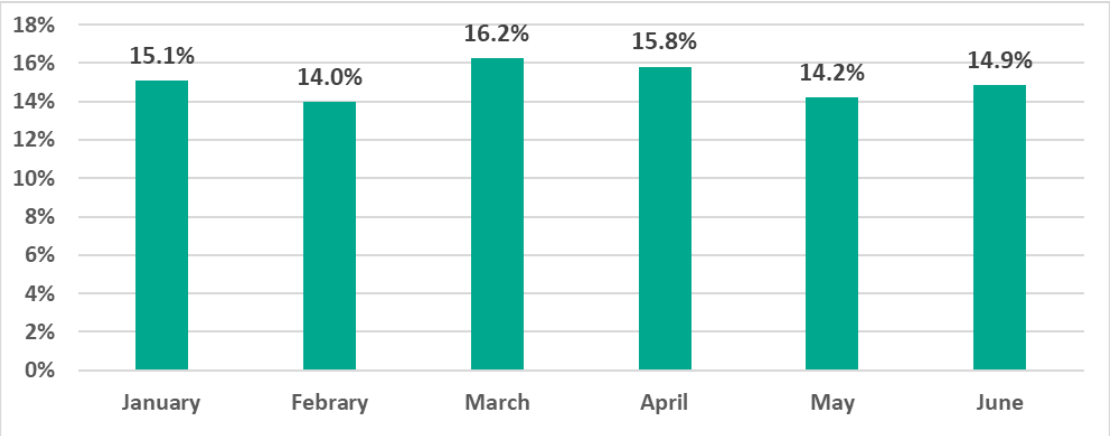
In H1 2021, the percentage of ICS computers on which malicious objects were blocked was 33.8%, which was 0.4 p.p. more than in H2 2020.

Percentage of ICS computers on which malicious objects were blocked



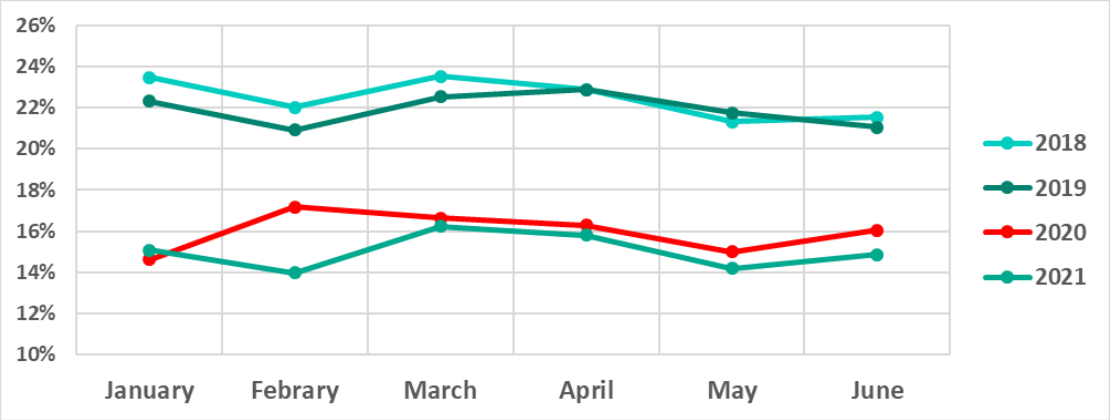
The lowest percentage of ICS computers on which malicious objects were blocked was recorded in February and the highest percentage was recorded in March.

Percentage of ICS computers on which malicious objects were blocked by month, H1 2021



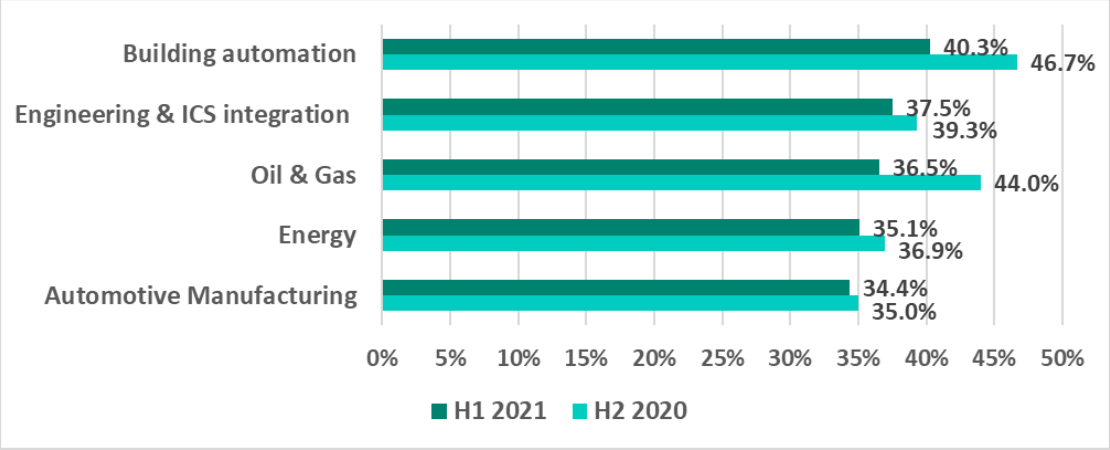
Note that the monthly dynamics of the indicator during H1 2021 resembled 2020 except for February. In February 2020 we saw an unusual growth in the percentage of attacked ICS computers that we did not see in previous years.

Percentage of ICS computers on which malicious objects were blocked, by months of the first half of the year, 2018 - 2021



Selected industries

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



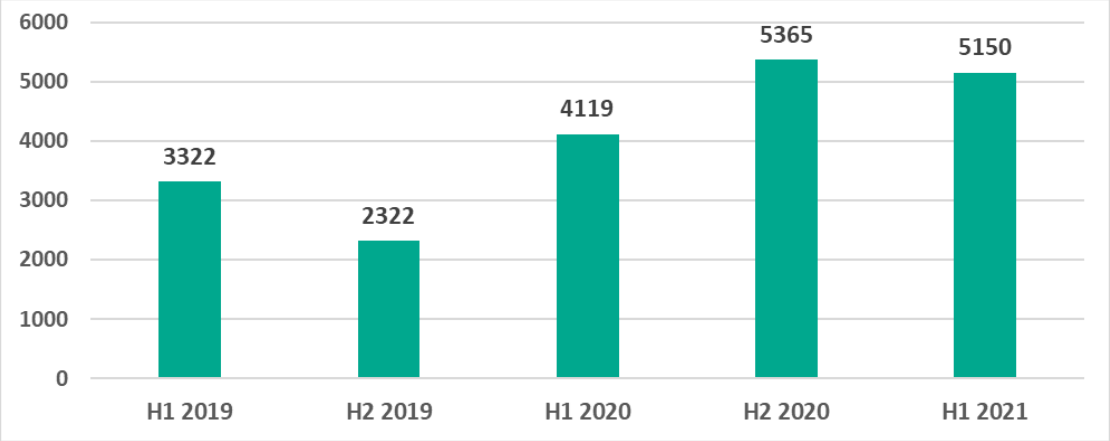
In H1 2021 the indicators in all selected industries decreased, particularly noticeably in oil and gas (-7.5 p.p.) and building automation (-6.4 p.p.).

Computers used in building automation systems often have the same attack surface as ordinary corporate systems, which is broader than the attack surface of ICS computers. Such computers can be connected to the corporate network and have access to various services, such as the internet, corporate email, the domain controller, etc. Building automation systems often belong to contractor organizations and are not always controlled by the corporate information security service, even when they have access to the company's corporate network.

Variety of detected malware

In H1 2021 Kaspersky security solutions blocked over 20,000 malware variants from 5,150 families on ICS computers.

Number of malware families blocked on ICS computers

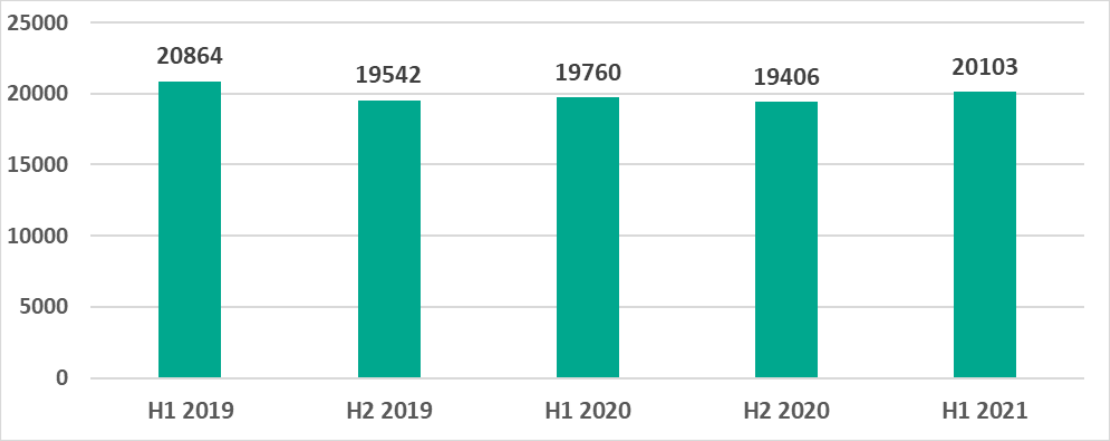


The number of malware families has slightly decreased in H1 2021 versus H2 2020 but remains higher than the numbers recorded in the previous eighteen months.

This, as well as an analysis of malware samples, clearly points to an established practice whereby threat actors offer popular malware (particularly spyware) families using the MaaS (malware-as-a-service) model. Rather than create 'their own' unique malware, attackers use ready-made malware that is often customized to meet their needs, which does not require them to have any software development skills.

The increase in the number of unique malware samples is also due to threat actors using malware obfuscation services on a massive scale to prevent the malware from being detected.

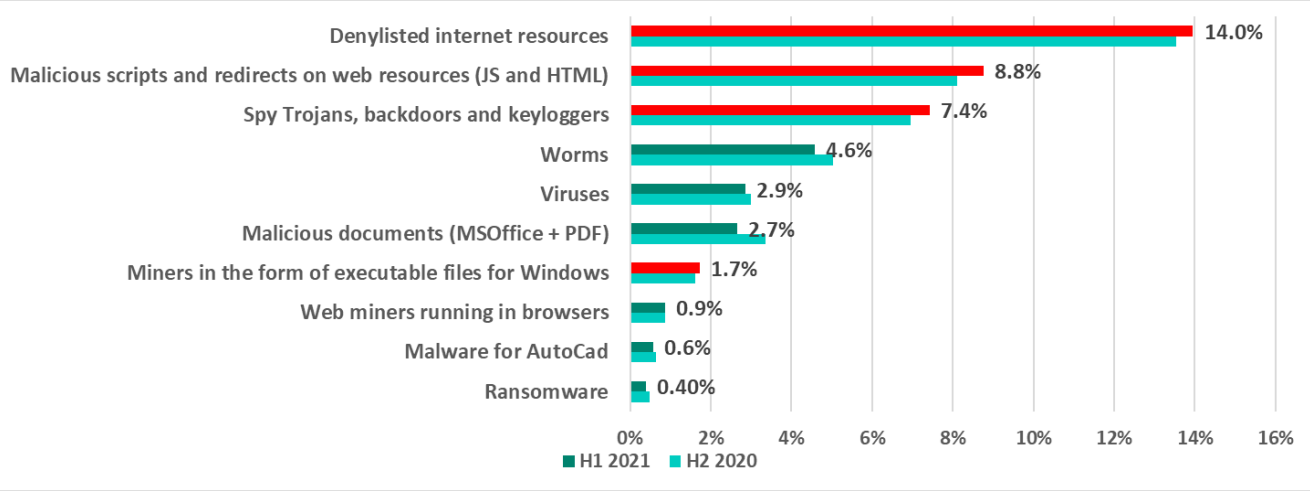
Number of mlaware variants blocked on ICS computers



Categories of malicious objects

Malicious objects blocked by Kaspersky products on ICS computers fall into many categories. To give a better idea of the types of threats blocked by Kaspersky products, we conducted a detailed classification.

The results of our detailed 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.

A brief description of each threat type is available in a separate document.

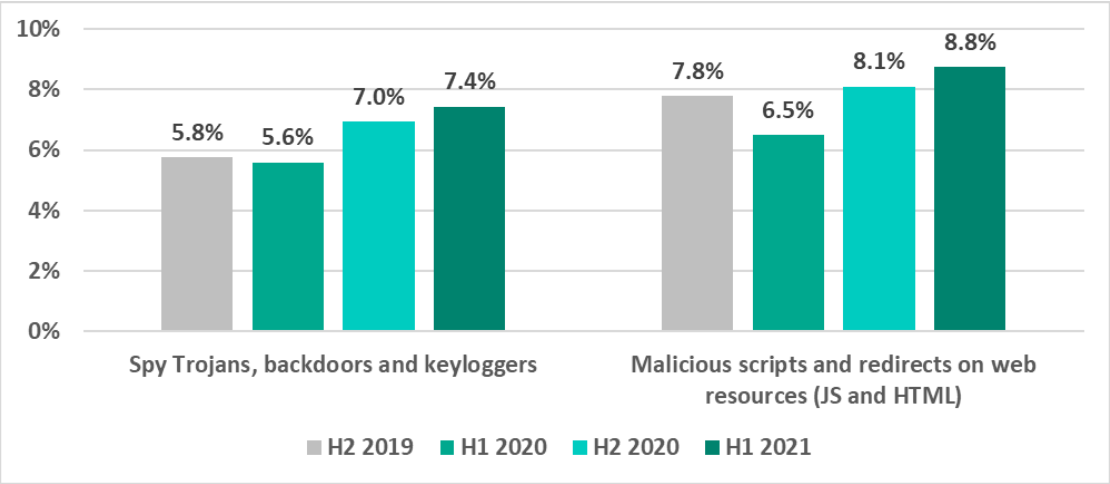
H1 2021 saw an increase in the percentage of ICS computers on which the following categories of threats were blocked:

- **Internet threats** – denylisted web resources involved in the distribution or management of malware – up by 0.5 p.p.;
- **Malicious scripts and redirects on web resources** (JS and HTML) up by 0.7 p.p.;
- **Spyware** – Trojan-Spy malware, backdoors and keyloggers – up by 0.4 p.p.;
- **Cryptocurrency miners** – executable files for Windows – up by 0.12 p.p.

Malicious scripts are used by threat actors on various media resources and websites hosting pirated content to redirect users to sites which distribute spyware and/or malwre designed to mine cryptocurrency without the user's knowledge.

Note that the percentages for spyware and malicious scripts and redirects are growing for the second six-month period now.

Percentage of ICS computers on which malicious objects were blocked

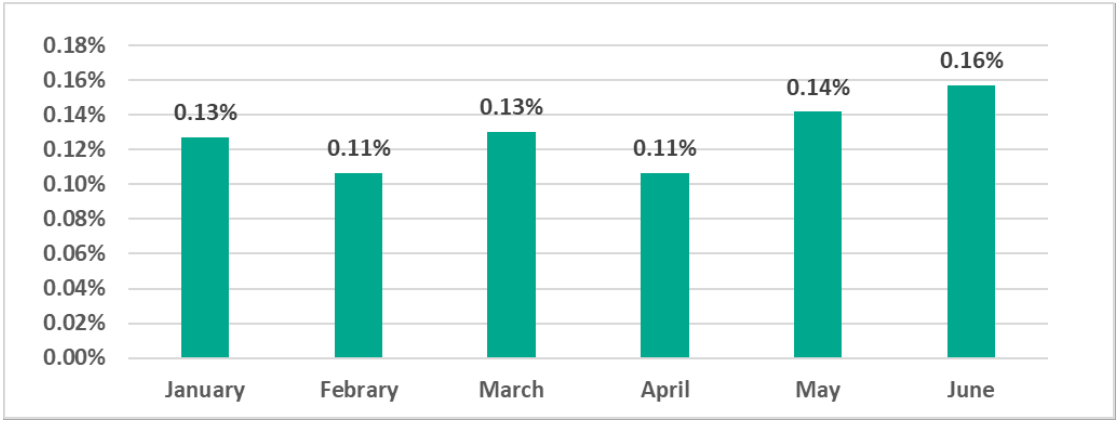


Ransomware

Ransomware infection attempts were blocked on 0.40% of ICS computers in H1 2021, which is 0.09 p.p. lower than during the previous six-month period.

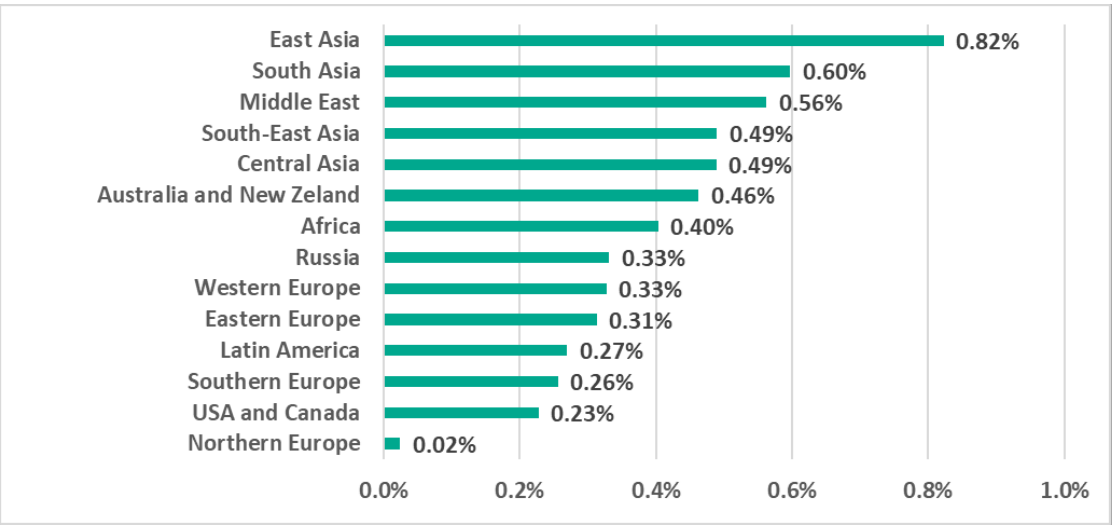
The largest percentage of ICS computers on which ransomware was blocked occurred in June (0.16%) and the smallest in February and April (0.11%).

Percentage of ICS computers on which ransomware was blocked by month, H1 2021



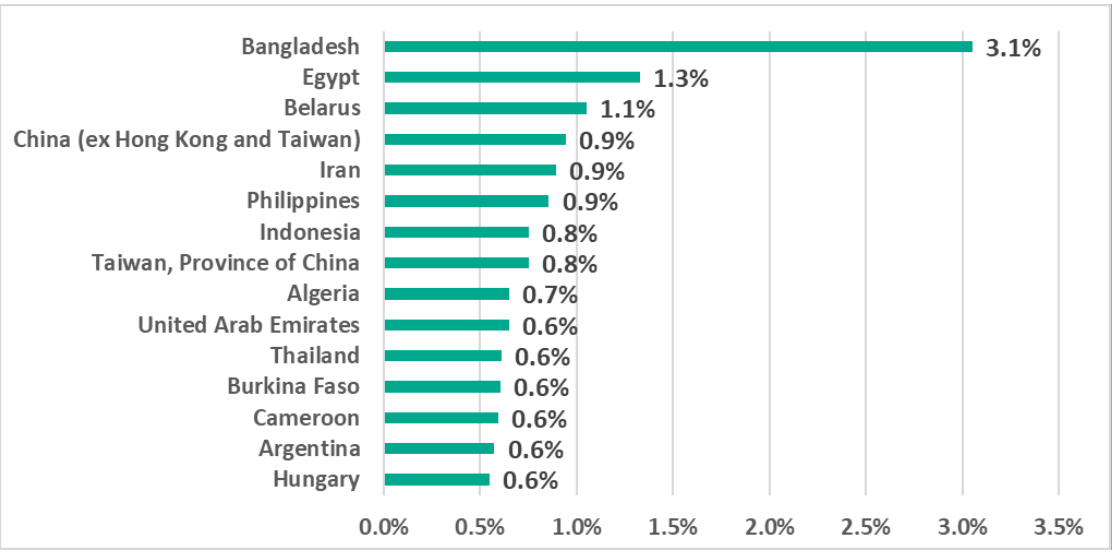
Asia and the Middle East led in the regional ranking by percentage of ICS computers attacked by ransomware.

Regions ranked by percentage of ICS computers on which ransomware was blocked in H1 2021



Only two European countries, Belarus and Hungary, appear on the TOP 15 list of countries and territories with the largest percentages of ICS computers on which ransomware was blocked.

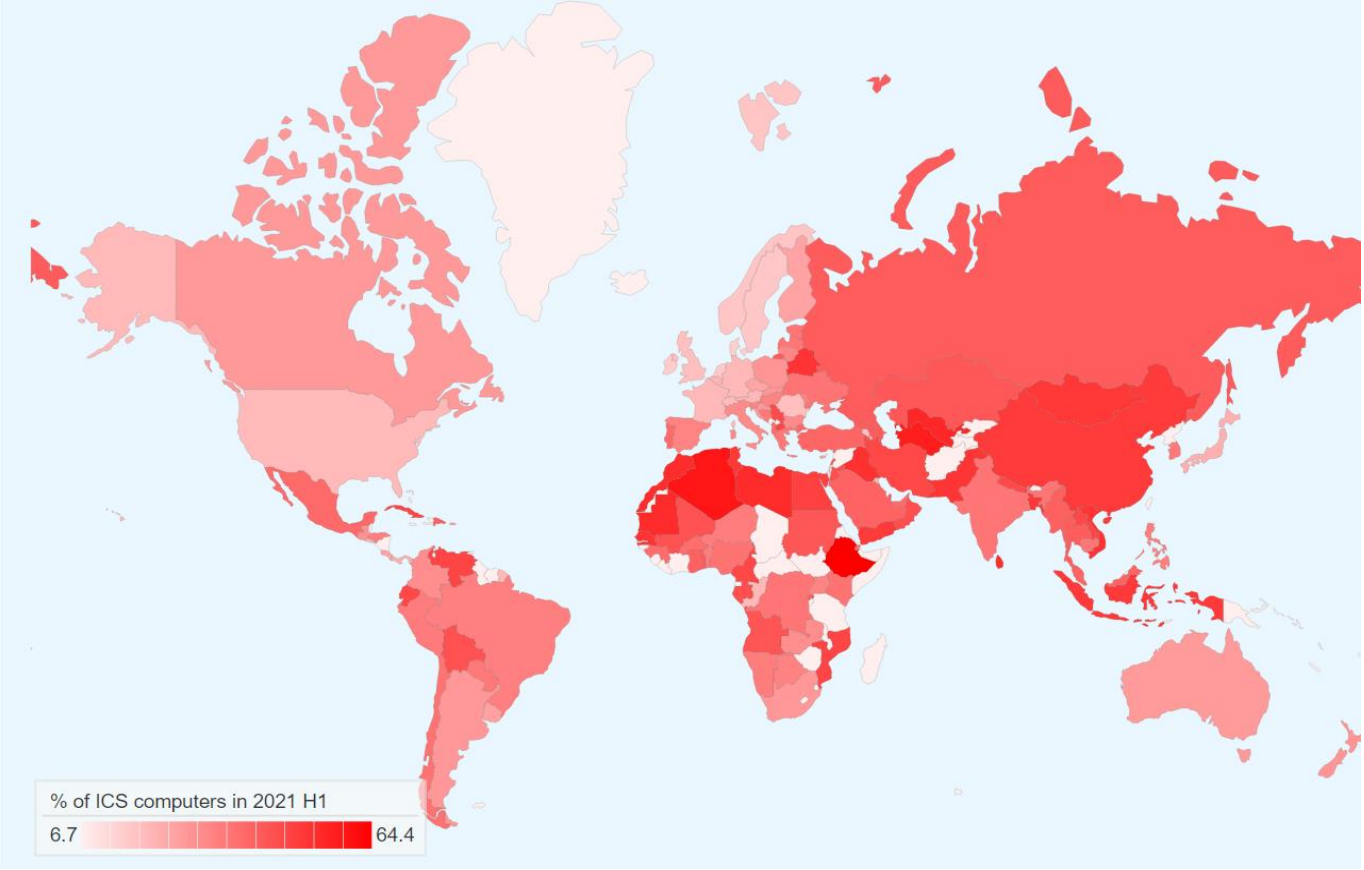
TOP 15 countries and territories ranked by percentage of ICS computers on which ransomware was blocked in H1 2021



In Russia, the percentage of ICS computers on which ransomware was blocked remained at 0.33%.

Geographical distribution

The map below depicts the percentage of ICS computers on which malicious objects were blocked relative to the number of such systems in each country.

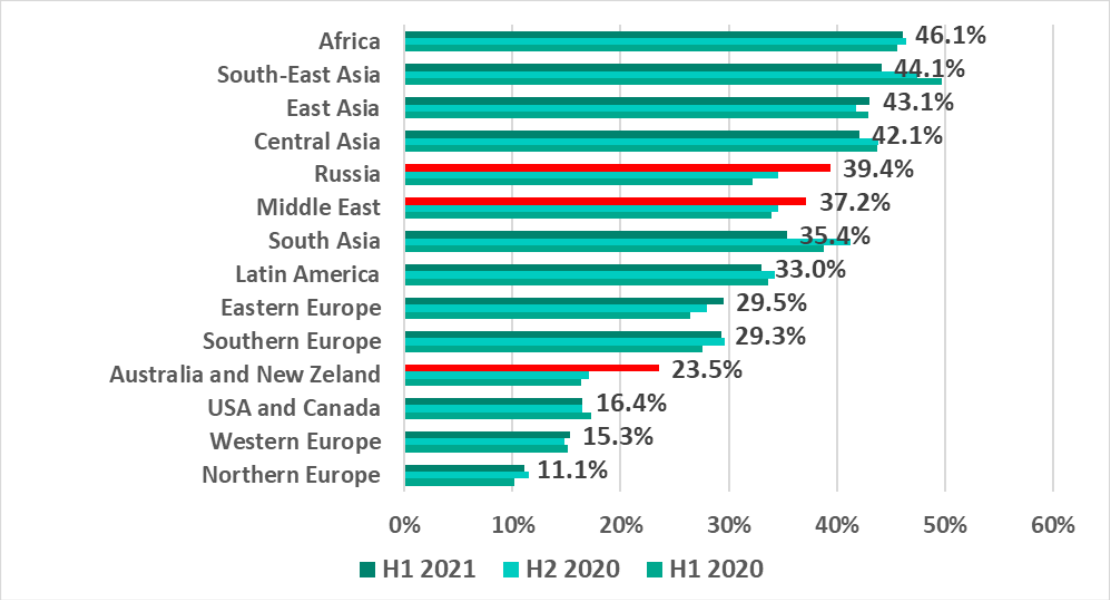


Geographical distribution of attacks* on industrial automation systems in H1 2021
** percentage of ICS computers on which maliciouis objects were blocked*

Regions

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

Percentage of ICS computers on which malicious objects were blocked by global region



The largest increases in the percentages of ICS computers on which malicious objects were blocked were as follows:

1. **By 6.5 p.p. in Australia and New Zealand;**
2. **By 4.8 p.p. in Russia** – Russia has risen in the ranking from 8th to 5th place over a year;
3. **By 2.6 p.p. in the Middle East.**

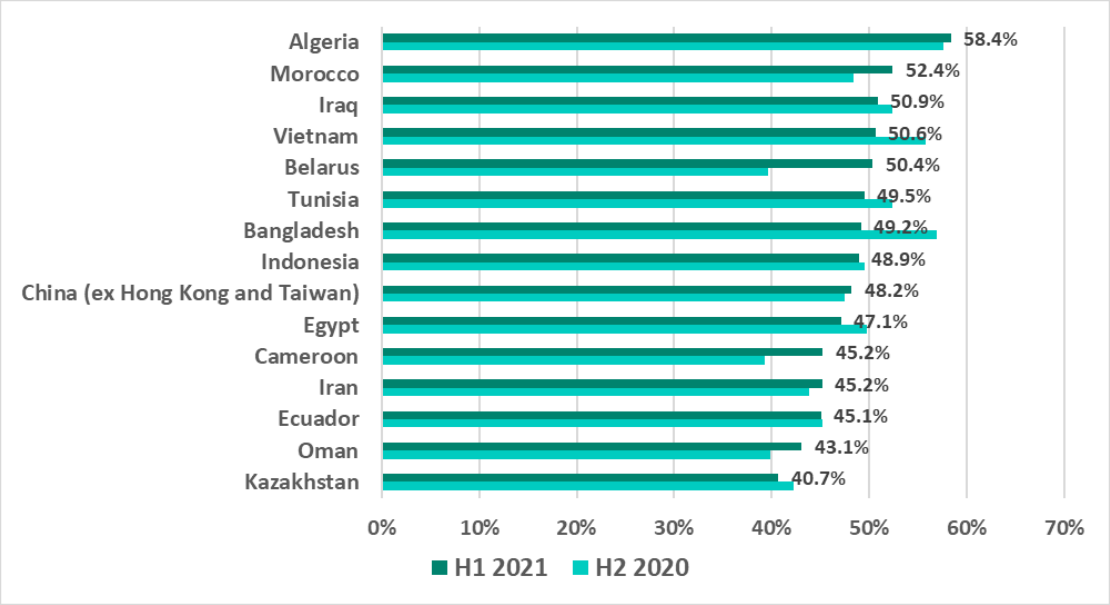
Such a significant growth in the percentages **in Australia and New Zealand** has to do with changes in the main method used to spread spyware in the region. In previous periods, spyware was mainly distributed via phishing emails with malicious attachments containing spyware or its downloader. In H1 2021 we saw malicious downloader scripts, which are mostly spread via the internet, used more often to distribute spyware. The percentage of ICS computers on which such malicious objects were blocked grew in Australia and New Zealand by 3.8 p.p.

In **Russia** we see a similar trend with a growth of 4.4 p.p.

We see a different trend in **the Middle East**, where we recorded a growth in the percentage of ICS computers where the malware blocked included worms (+0.4 p.p.) and ransomware (+0.3 p.p.), whilst the percentages for malicious downloader scripts that were blocked went down (-0.3 p.p.).

Countries

Top 15 countries and territories with the largest percentages of ICS computers on which malicious objects were blocked in H1 2021

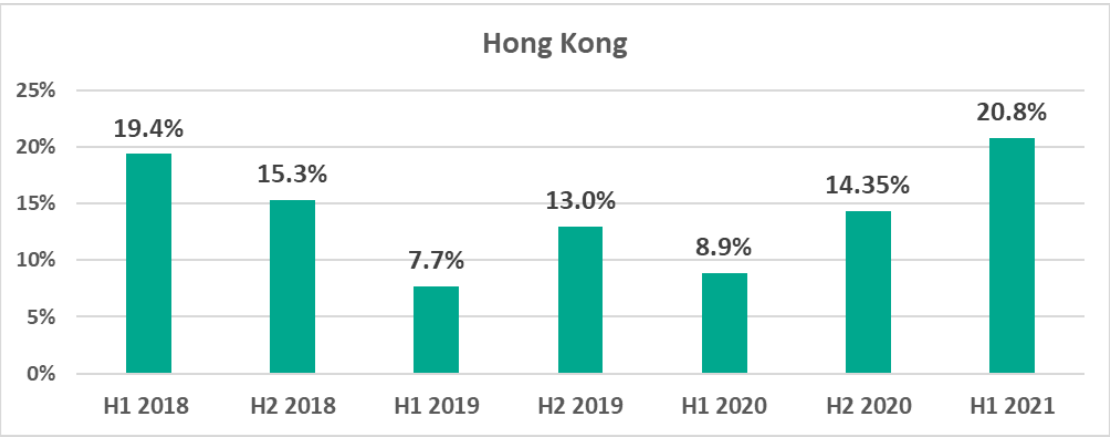


We recorded the greatest increases in percentages of ICS computers that have been attacked as follows:

1. More than **10 p.p. – in Belarus and Ukraine**. Belarus now ranks fifth in the country ratings.
2. By 7.4 p.p. in the Czech Republic and Slovakia. The Czech Republic is no longer on the list of the safest countries.
3. By **6.5 p.p. in Hong Kong and by 6 p.p. in Australia**. These countries are no longer in the top 10 of the safest countries.
4. By **6 p.p. – in Cameroon**. Cameroon is now in the TOP 15 based on the percentage of ICS computers that have been attacked.

It is worth noting that the percentage of ICS computers on which malicious objects were blocked in Hong Kong is higher than it has been over the past 3 years.

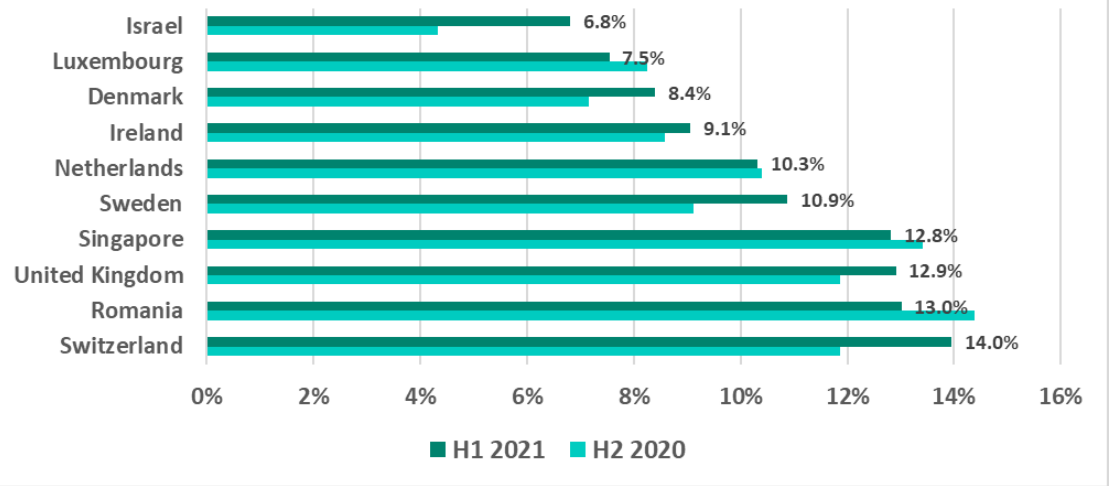
Percentage of ICS computers on which malicious objects were blocked in Hong Kong



The most noticeable decreases in the percentages of ICS computers on which malicious objects were blocked occurred as follows:

1. over 10 p.p. – in the Philippines;
2. by 8.4 p.p. in Bangladesh;
3. over 7 p.p. in Saudi Arabia, Argentina and Sri Lanka.

TOP 10 countries and territories with the lowest percentages of ICS computers on which malicious objects were blocked in H1 2021

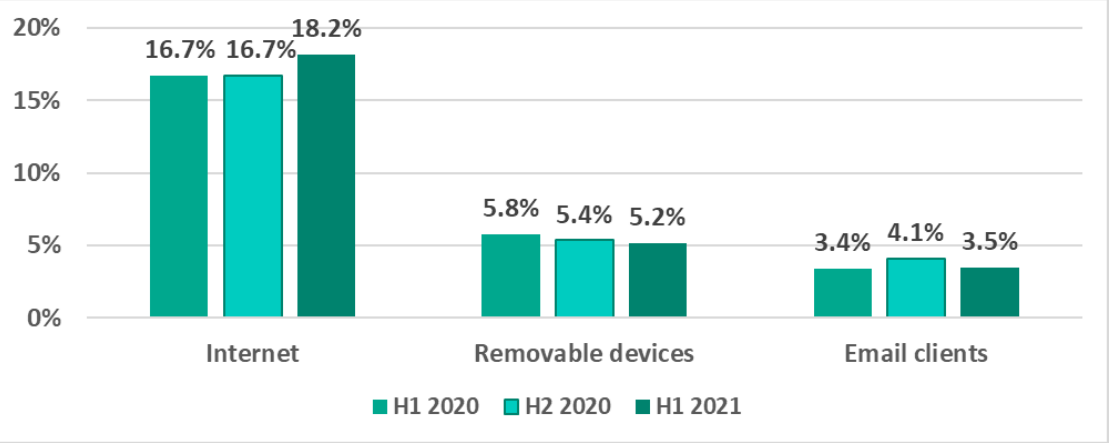


Threat sources

The internet, removable media and email are the main sources of threats for computers in the industrial infrastructure of organizations.

Main sources of threats blocked on ICS computers*

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



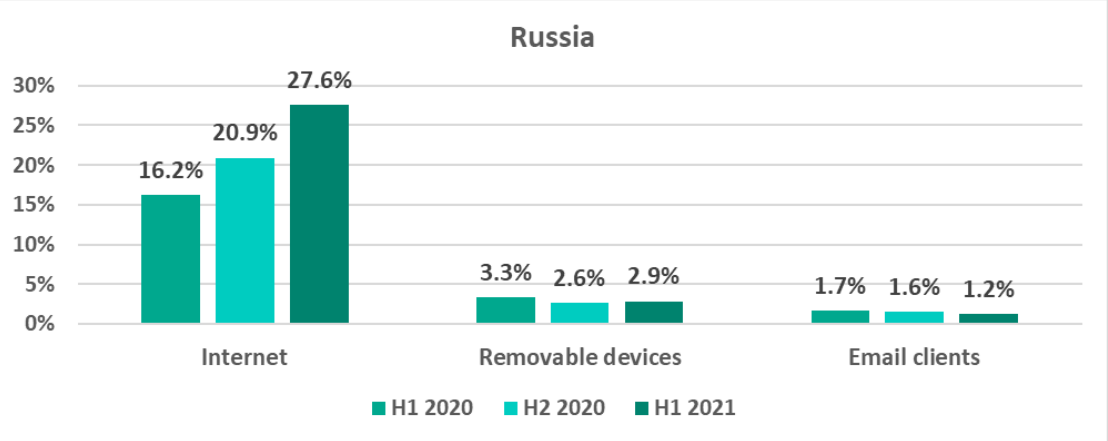
In the first half of 2021, percentages of ICS computers on which different threats were blocked changed as follows:

1 Internet threats – increased by 1.5 p.p.;
2 Threats blocked when removable media was connected have been decreasing throughout the past year; in H1 2021 their percentage decreased by 0.2 p.p.;
3 Threats blocked in email attachments decreased by 0.6 p.p.

In Russia, the percentage of ICS computers on which threats from the internet were blocked, increased significantly – by 6.7 p.p.

Russia. Main sources of threats blocked on ICS computers*

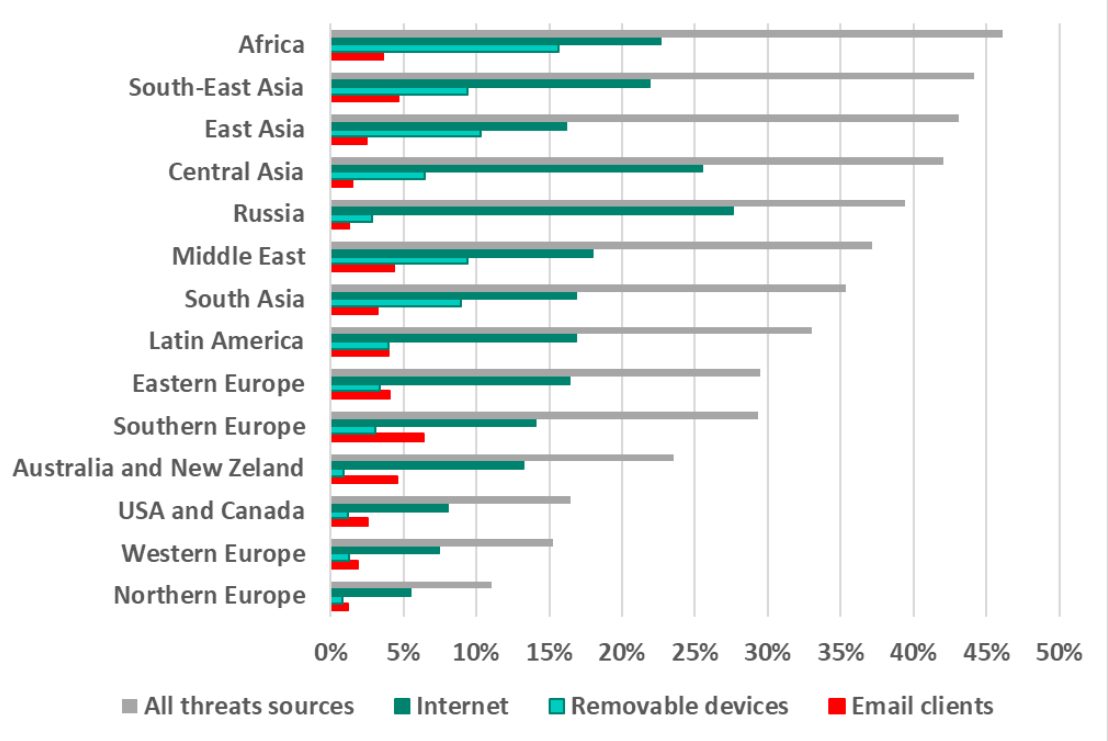
** percentage of ICS computers on which malicious objects from different sources were blocked*



Main threat sources: geographical distribution

Main sources of threats blocked on ICS computers* by region in H1 2021

** In some cases, the percentage of ICS computers on which malicious objects from different sources were blocked cannot be established*

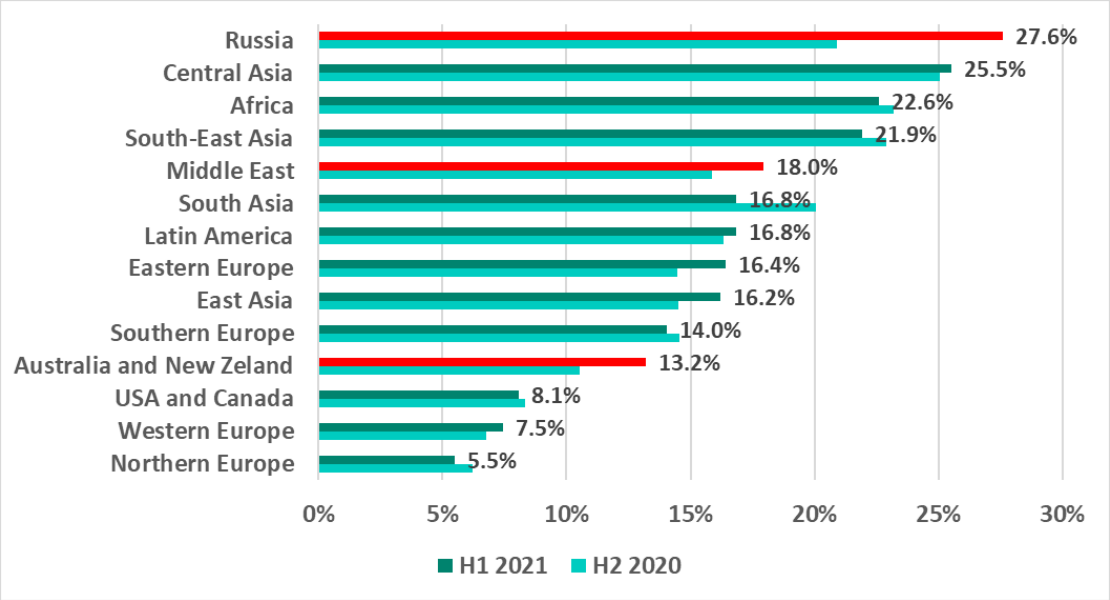


As in previous periods, in the safer regions – Europe, USA and Canada, and Australia and New Zealand – the percentage figures for malicious email attachments are higher than those for removable media.

Internet

The internet is the main source for threats blocked on ICS computers. All regions can be divided into three main groups based on the percentages of ICS computers on which malicious objects were blocked. The first group includes the regions with percentages ranging from 20% to 28%; the second group includes the regions with percentages from 13% to 18%. The final group, the safest, includes regions with percentages of 9% or lower.

Percentage of ICS computers on which malicious objects from the internet were blocked by global region

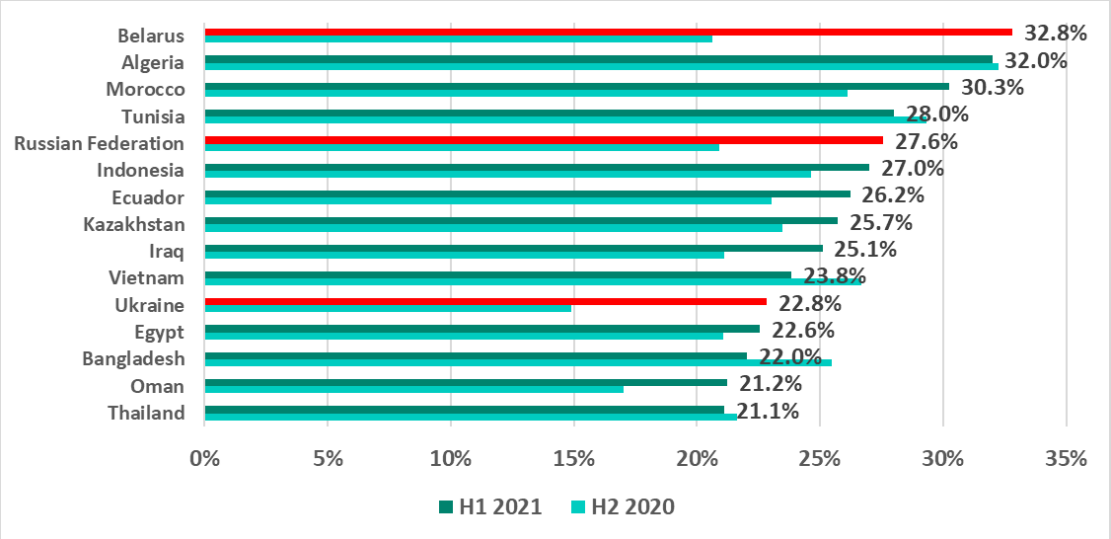


In H1 2021 the percentage of ICS computers on which internet threats were blocked rose most significantly:

1. **By 6.7 p.p. in Russia**, which unexpectedly took first place among all regions with 27.6%;
2. **By 2.7 p.p. in Australia and New Zealand**, placing this region into the second group with 13.2%;
3. **By 2.1 p.p. in the Middle East**.

The most noticeable decrease in this percentage was recorded in South Asia at minus 3.2 p.p.

TOP15 countries and territories with the highest percentages of ICS computers on which internet threats were blocked in H1 2021



The largest increases in this percentage in H1 2021 were recorded as follows:

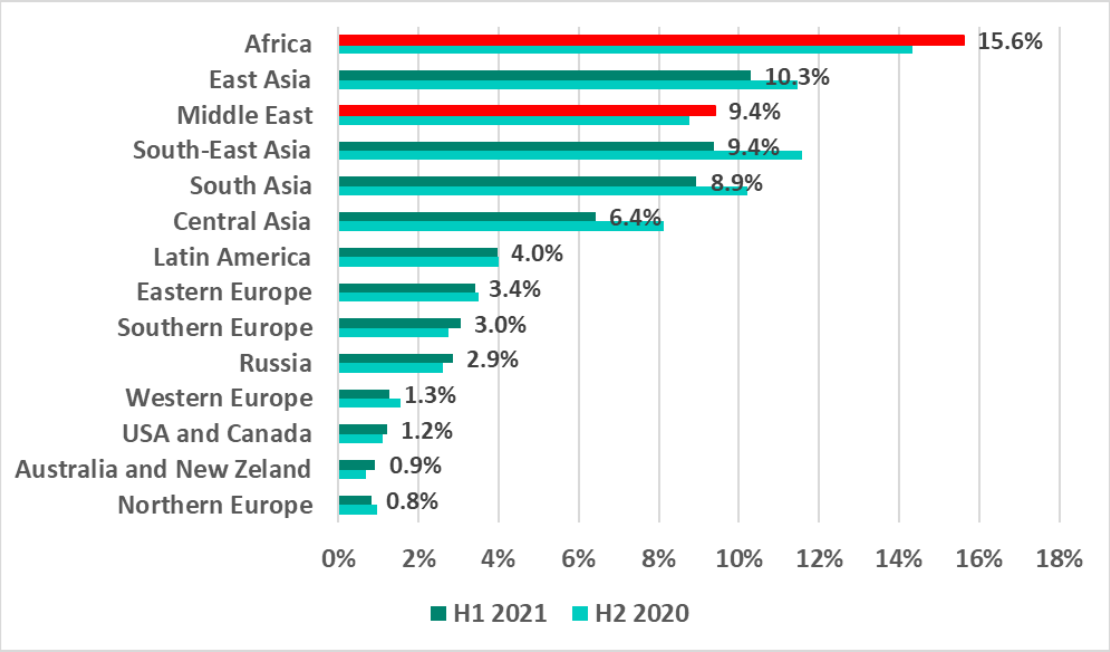
1. **A record of 12.2 p.p. in Belarus**, which took the country to the top place;
2. **By 8 p.p. in Ukraine;**
3. **And 6.7 p.p. in Russia.**

Finally, there are no other European countries in the TOP 15.

Removable media

The rating of regions based on the percentage of ICS computers on which malware was blocked when removable media was connected to them is, as usual, headed by Africa, regions of Asia, and the Middle East.

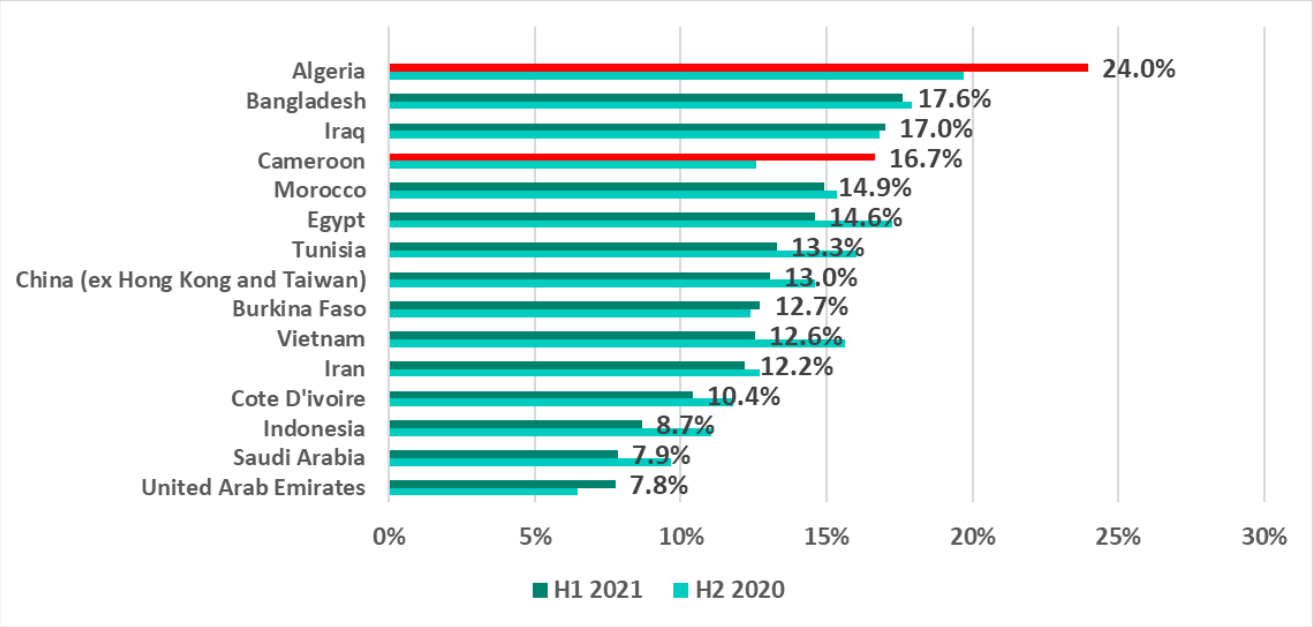
Regions ranked by percentage of ICS computers on which malware was blocked when removable media was connected in H1 2021



The largest increase in the percentage – by 1.3 p.p. – was recorded in Africa.

In all Asian regions the percentages decreased by 1.2 – 2.2 p.p., whereas in the Middle East the percentage increased slightly (by 0.6 p.p.). As a result, the Middle East has gone up from fifth to third place in the ranking.

In H1 2021, as usual, no countries from Europe, North America or Australia made the TOP 15 in the ranking based on the percentage of ICS computers on which malware was blocked when removable media was connected to them.



15 countries and territories with the largest percentage of ICS computers on which malware was blocked when removable media was connected to them in H1 2021

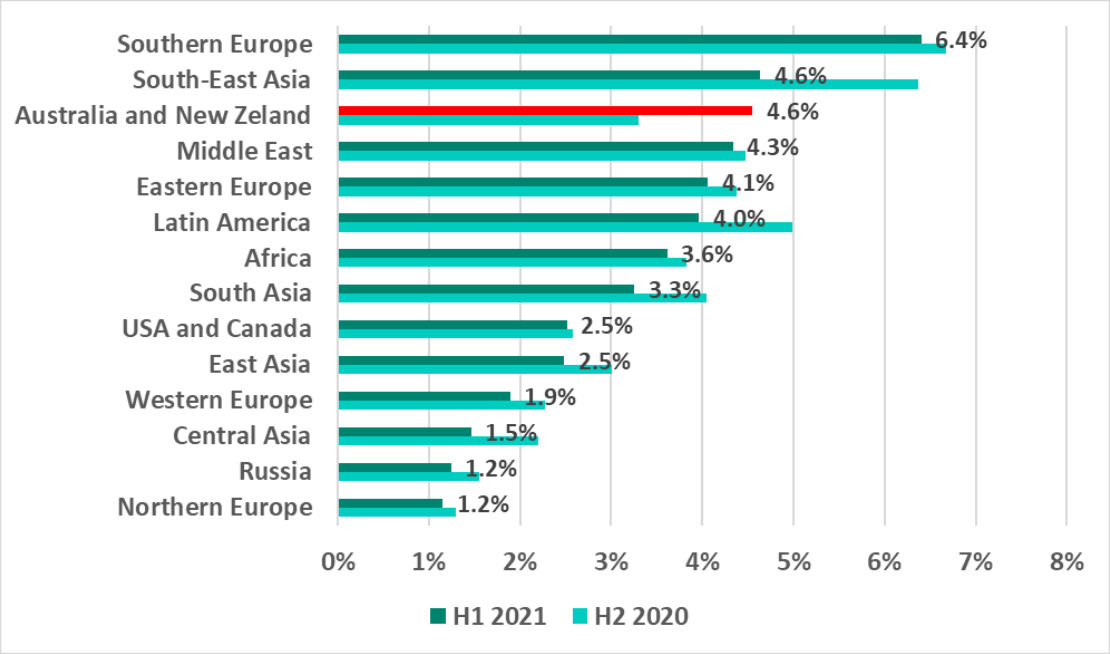
The largest increases of these percentages were recorded in Algeria and Cameroon – by 4.3 and 4.1 p.p. respectively.

Email clients

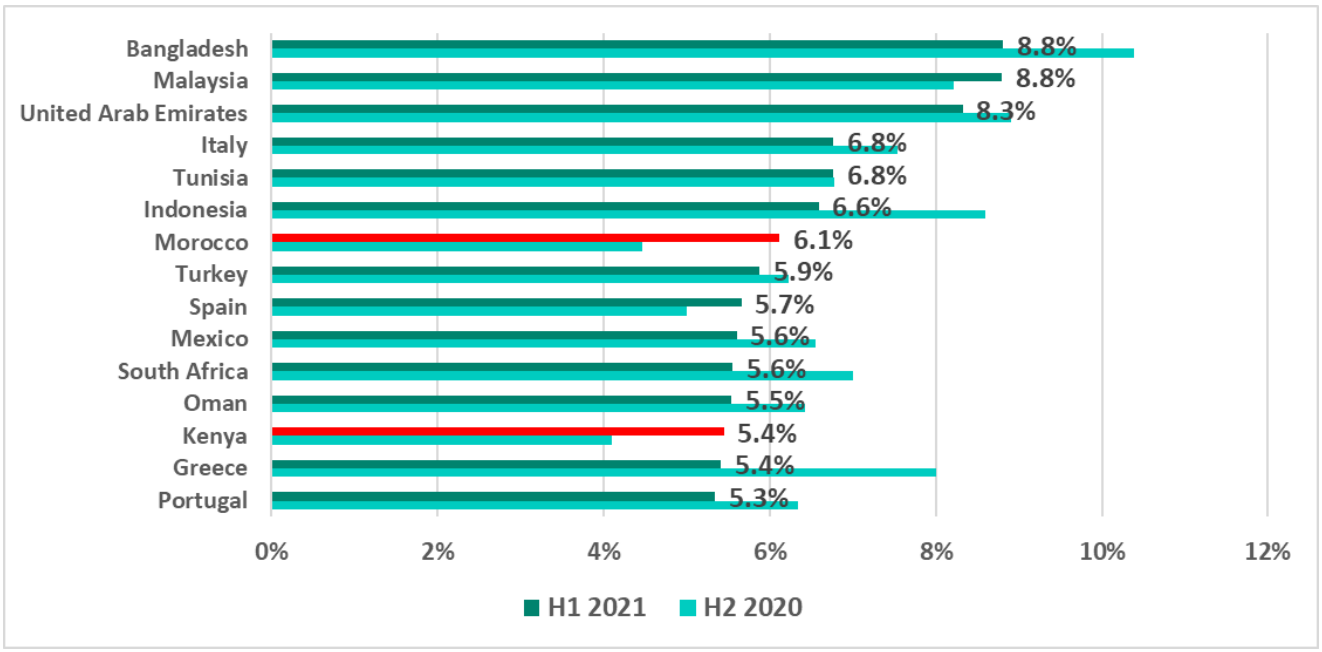
Just as in H2 2020, Southern Europe and Southeast Asia continue to head the ranking of regions by the percentage of ICS computers on which malicious email attachments were blocked.

The percentage rose in most regions during H2 2020. In H1 2021 the growth continued only in one region – Australia and New Zealand (+1.3 p.p.). It is worth noting that the percentage of ICS computers on which malicious email attachments were blocked has been rising in this region since H1 2020.

Regions ranked by percentage of ICS computers on which malicious email attachments were blocked in H1 2021



Southern European countries, including Italy, Spain, Greece and Portugal are among the TOP 15 countries by percentage of ICS computers on which malicious email attachments were blocked.



TOP 15 countries with the highest percentages of ICS computers on which malicious email attachments were blocked in H1 2021

The most significant increases in this indicator, by 1.7 and 1.3 p.p. respectively, were recorded in Morocco and Kenya.

In Greece we saw a decrease of 2.6 p.p., which resulted in the country moving down from 5th to 14th place.

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