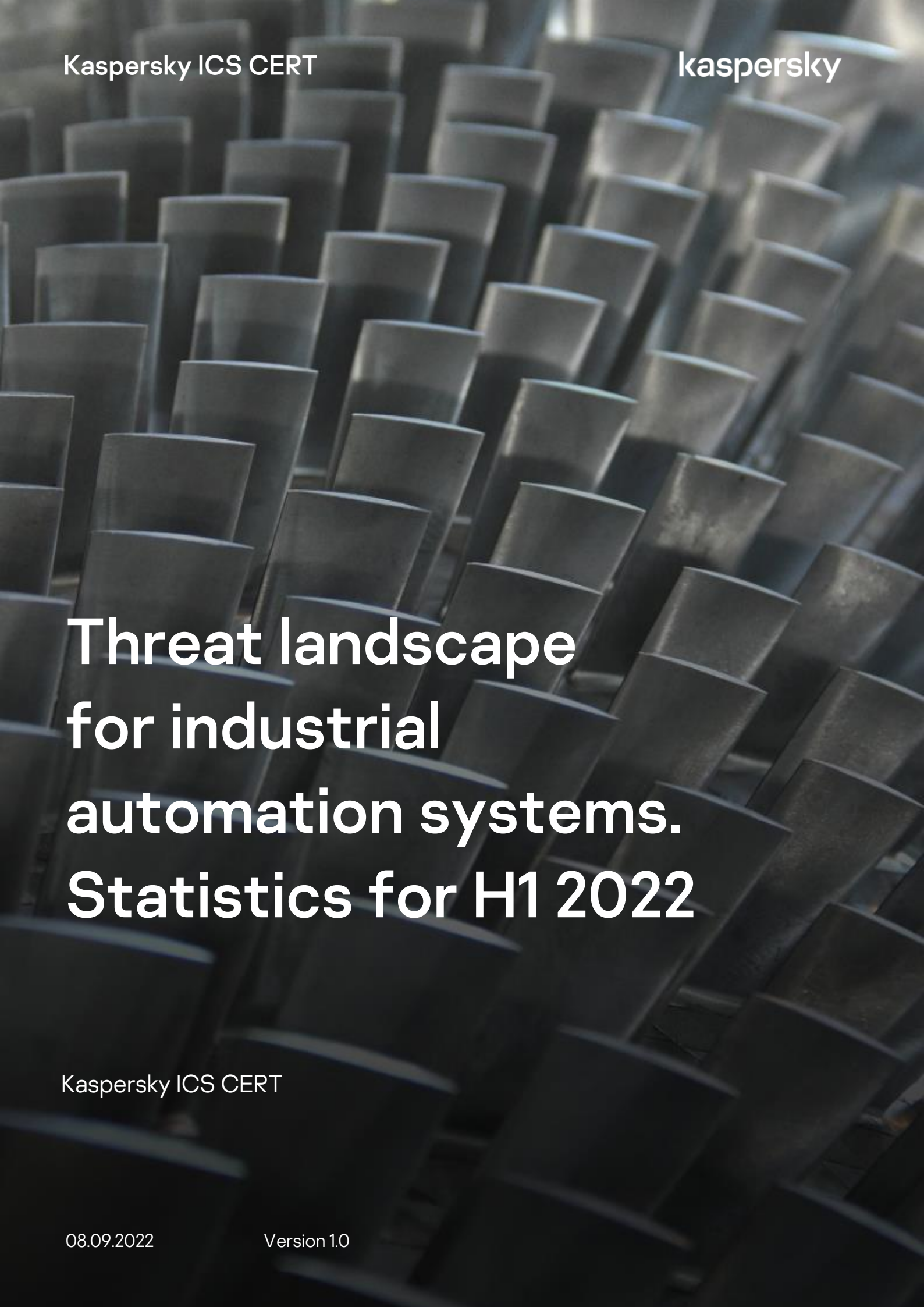
kaspersky



Threat landscape for industrial automation systems. Statistics for H1 2022

Kaspersky ICS CERT

08.09.2022 Version 1.0

This report is based on an analysis of statistical data collected through the Kaspersky Security Network (KSN), a distributed antivirus network. The data was received from those KSN users who have given 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 provides an opportunity for our clients to improve the reaction speed of our security solution to new and unknown threats. It also improves the detection quality of the solution due to the access to the cloud infrastructure where data on malicious objects is stored. This data is only accessible via the cloud due to the size of the database and the resources required to store it locally.

The information transferred by the user includes only the types and categories of data described in the relevant KSN Agreement. This information not only assists in analyzing the threat landscape, but is also needed to detect new threats, including targeted attacks and APTs.[1]

H1 2022 in numbers

Percentage of ICS computers on which malicious objects were blocked:

- 31.8% – the percentage of ICS computers around the world on which malicious objects were blocked in H1 2022 at least once.
- 1.7 p.p. – the decrease in the percentage between January and March. For the first time in five years of observations, the lowest percentage in the first half of the year was observed in March.
- 41.5% – Africa. The highest percentage throughout the regions in H1 2022.
- 12.8% – Northern Europe. The lowest percentage throughout the regions worldwide in H1 2022. But, also the highest percentage for this region in any six-month period from H1 2020 to H1 2022
- 43.2% – Taiwan in H1 2022. After an unexpected increase of 8 p.p. in H1 2022, Taiwan is now ahead of mainland China (41.4%).
- 6.8% – Luxembourg in H1 2022. The lowest percentage among countries around the world.

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

Malware varieties:

- 7219 – how many malware families were blocked on ICS computers.
- 8.6% – the percentage of ICS computers on which spyware was blocked. Building Automation was the industry attacked most by spyware in H1 2022 – 12.9%.
- 2.8% – the percentage of ISC computers on which cryptocurrency miners (Windows executable files) were blocked in the Manufacturing sector.

Percentage of ICS computers on which ransomware was blocked:

- 0.65% – around the world during H1 2022, the highest percentage for any half-year reporting period from H1 2020 to H1 2022.
- 0.27% – February 2022. The highest percentage for any month during the period from January 2020 to June 2022 around the world.
- 1% – percentage for the Building Automation industry in H1 2022, the highest percentage among all industries of ICS computers attacked by ransomware.
- 0.95% – percentage for East Asia in H1 2022. This is the highest percentage of ICS computers attacked by ransomware among all regions.
- 0.89 % – Middle East in H1 2022. The Middle East is in second place in the ransomware-based ranking of regions. The percentage of ICS computers on which ransomware was blocked during a six-month reporting period grew 2.5 times in this region from 2020.
- 9 out of 14 – the number of regions where the percentage of ICS computers on which ransomware was blocked increased in H1 2022.

Threat sources:

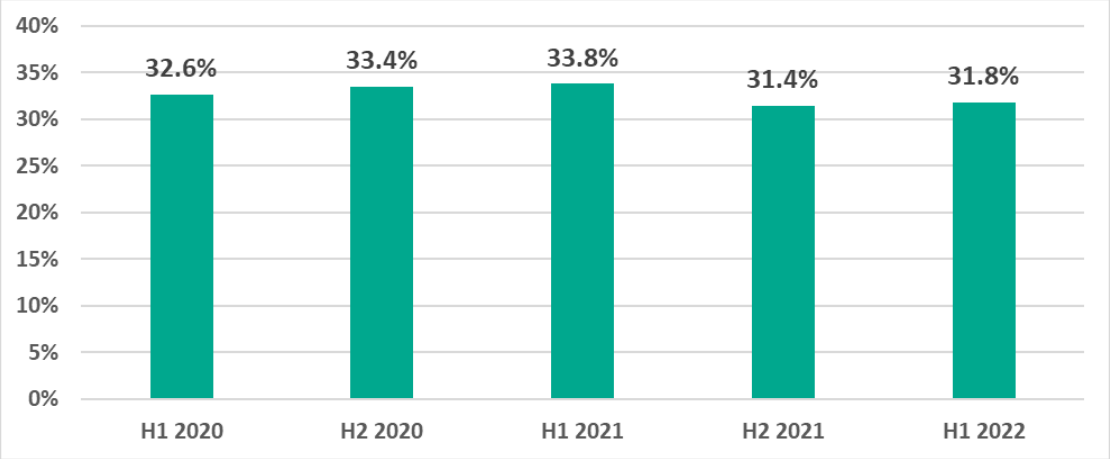
- 14.4% – the percentage of ICS computers on which malicious email attachments and phishing links were blocked in the Building Automation sector. This is twice more than the worldwide average of 7%. Professionals in the Building Automation sector actively use internet resources and email and can be used by attackers as 'entry points' into the target organization's infrastructure.
- 10.4 % – the percentage of ICS computers on which threats were blocked when removable media was attached in the Oil and Gas sector, which was 3 times more than the average worldwide of 3.5%.
- 1.2% – the percentage of ICS computers in the Oil and Gas industry on which malware in network folders was blocked, which is 2 times more than the worldwide average of 0.6%.

Global statistics

Percentage of ICS computers on which malicious objects were blocked

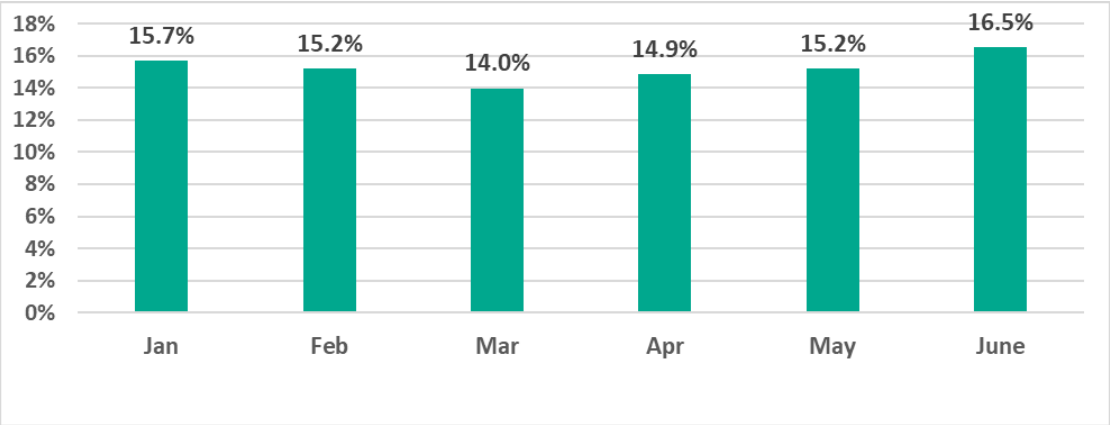
In H1 2022 malicious objects were blocked on 31.8% of ICS computers.

Percentage of ICS computers on which malicious objects were blocked



During H1 2022 we see the largest percentage of ICS computers on which malicious objects were blocked in June and the smallest in March.

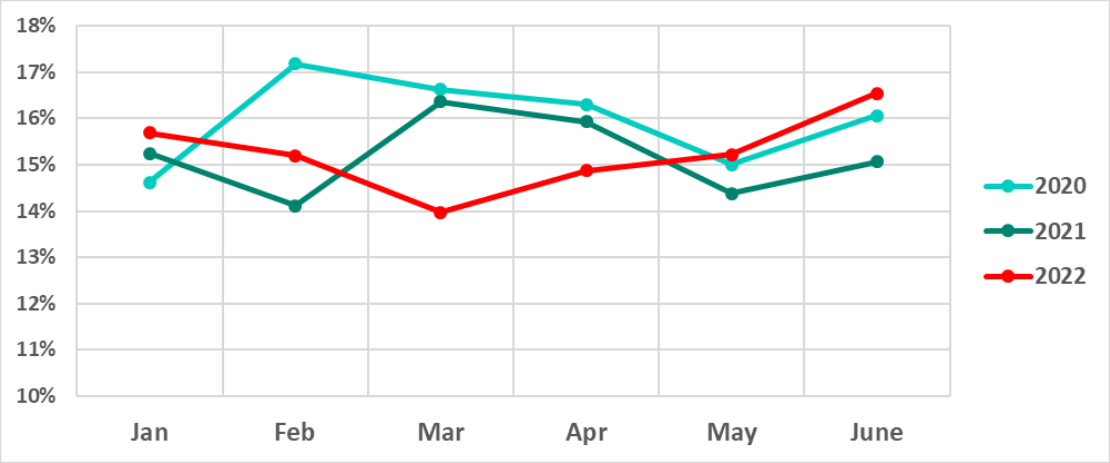
Percentage of ICS computers on which malicious objects were blocked, Jan – June 2022



Notably, in H1 2022, for the first time in five years, the lowest percentage was observed in March. The lows in monthly statistics are usually associated with vacation and holiday periods, such as the summer months, as well as December and January. This is likely to be due to lower user activity and, as a consequence, lower proportions of computers on which malware was blocked.

We believe that the unusually low percentage observed in March 2022 was also associated with a decrease in user activity, which this time was probably due to disrupted supply chains and spikes in COVID infections in January and March 2022.

Percentage of ICS computers on which malicious objects were blocked, January – June 2020, 2021, and 2022

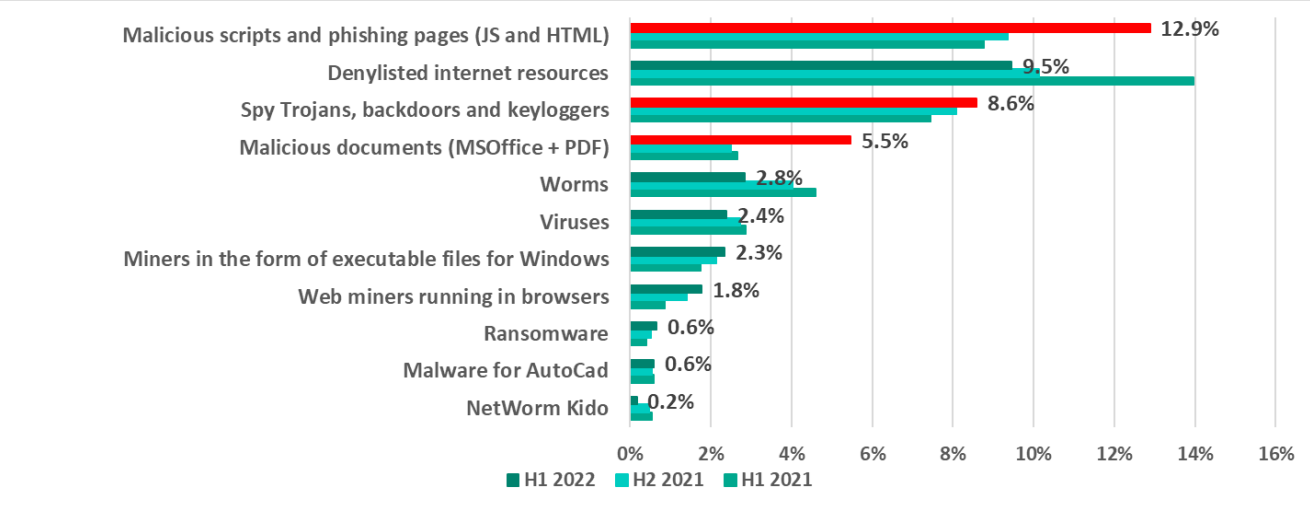


Variety of the malware detected

In H1 2022 Kaspersky security solutions blocked over 102,000 malware variants from 7,219 families in industrial automation systems.

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.



Percentage of ICS computers* on which the activity of malicious objects from different categories was prevented

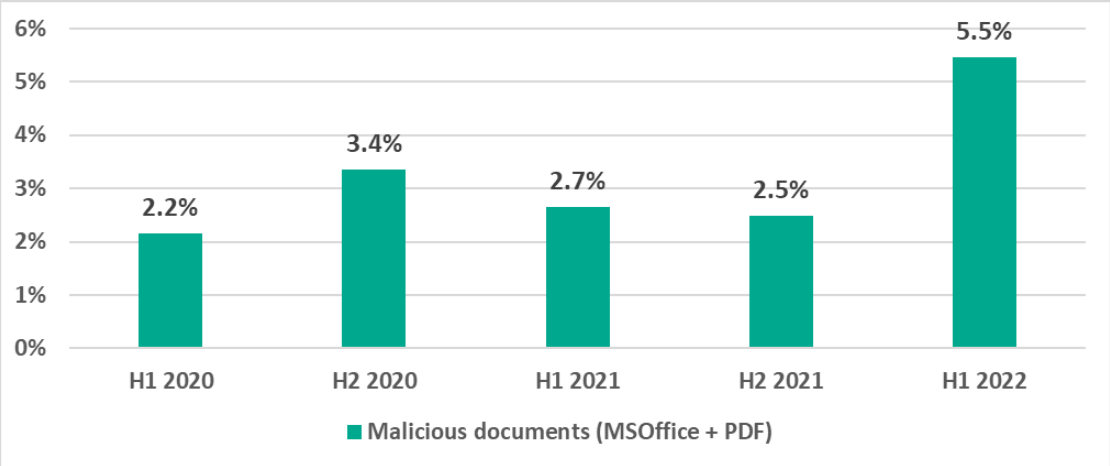
**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period.*

In H1 2022 the largest increases were observed in the percentages of ICS computers on which the following malware was blocked:

- **Malicious scripts and phishing pages** (JS and HTML) – by 3.5 p.p.
- **Malicious documents** – by 3.0 p.p.
- **Spyware** – Trojan spies, backdoors and keyloggers – by 0.5 p.p.

Malicious scripts and phishing pages are distributed via both the internet and email messages. Threat actors often send **malicious documents** in phishing emails. All of these methods are actively used for initial infections.

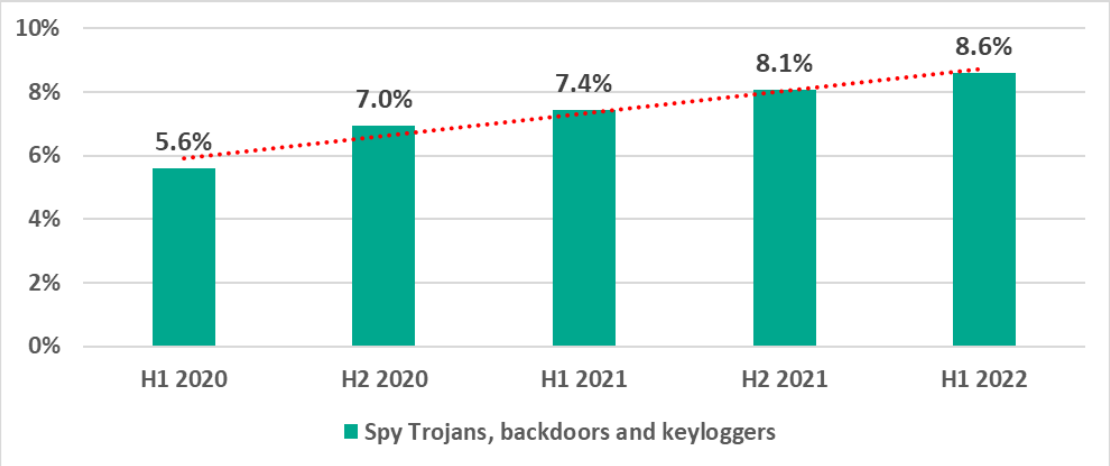
Percentage of ICS computers on which malicious documents (MSOffice + PDF) were blocked



The next stage in most cases entails the attackers downloading **spyware**, which is used to steal confidential information, to gain remote access to infected machines, and to download targeted malware, including **ransomware** (we will talk about it in more detail – see below).

We are seeing the percentage of ICS computers on which spyware has been blocked grow steadily since 2020.

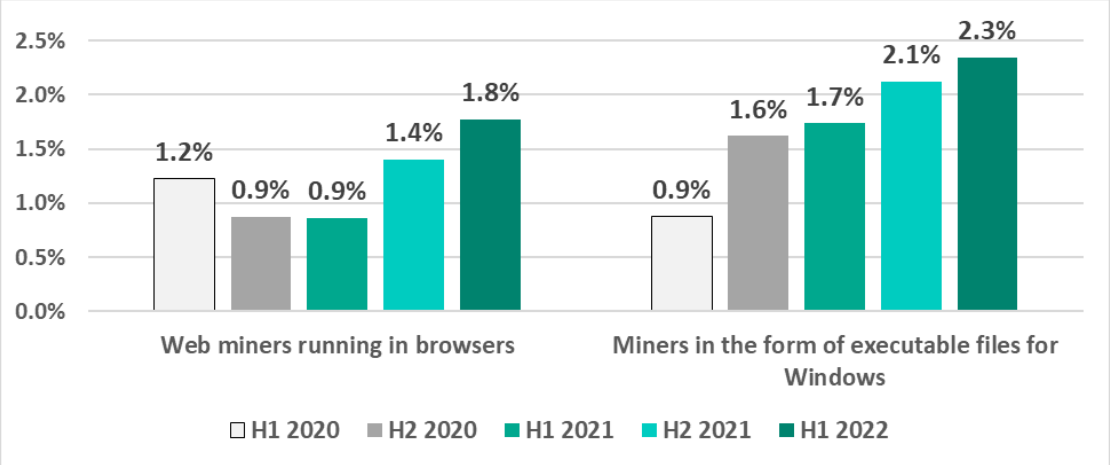
Percentage of ICS computers on which spyware was blocked



We are also seeing a slow but steady increase in the percentage of ICS computers on which malware for covert cryptocurrency mining is blocked:

- **Web miners, which are executed in browsers** – by 0.4 p.p.
- **Miners implemented as Windows executable files** – by 0.2 p.p.

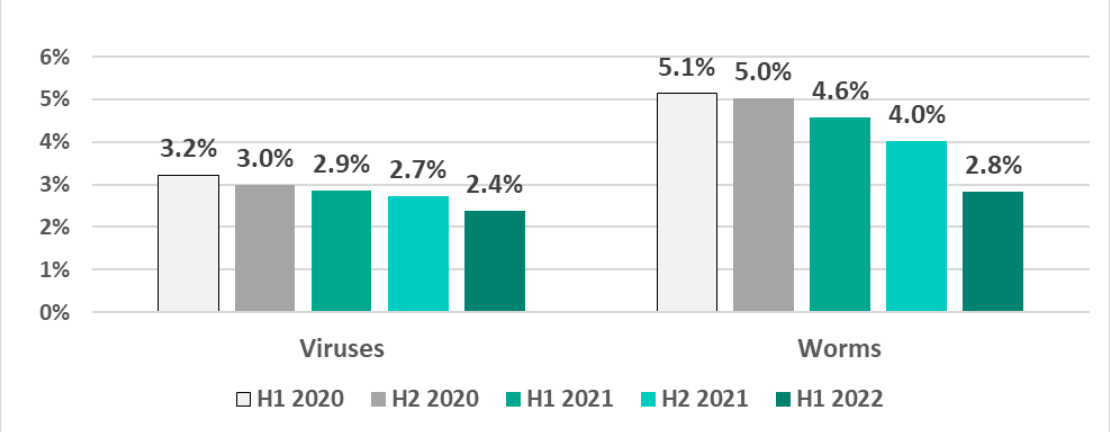
Percentage of ICS computers on which malware for covert cryptocurrency mining was blocked



Miners are often distributed via websites to which users have been redirected by malicious scripts. These are placed by threat actors on media resources and sites providing pirated content.

In the meantime, we are seeing a steady decrease in the percentage of ICS computers on which viruses and worms have been blocked. We believe that this could be a side effect of increasing security rollouts in OT environments, which eliminates infection hotspots and helps prevent self-propagating malware from spreading.

Percentage of ICS computers on which viruses and worms were blocked



Viruses and worms spread in ICS networks via removable media, network folders, infected files (including backups) and network attacks on outdated software, such as Radmin2.

There is a number of relatively old viruses and worms which are still spreading, such as Kido/Conficker. Despite having their command-and-control servers shut down, these older worms and viruses pose two threats: one, they undermine the security of the infected systems, for instance they open network ports and change settings, and, two, they can potentially cause software crashes or denial-of-service conditions.

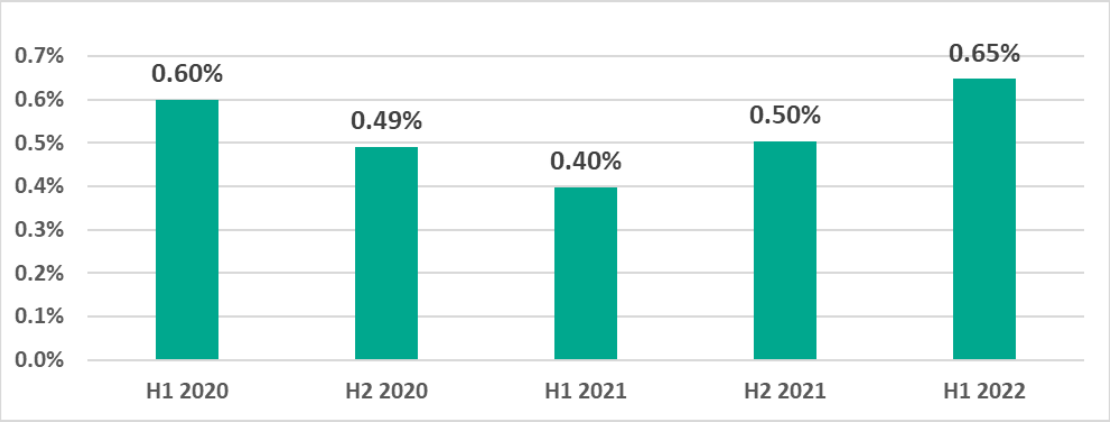
However, new versions of worms, used by threat actors to spread spyware, ransomware and miners in infected networks, are also being seen in ICS networks. Usually, these worms spread by exploiting vulnerabilities in network services, such as SMB or RDP, which have been fixed by vendors but still exist in OT environments or by using authentication data stolen earlier, or even by brute forcing passwords.

The decrease of the percentage of ICS computers on which such malware is blocked is due to, among other things, more careful scanning of removable media. In fact, the percentage of ICS computers on which malware was blocked when removable media was attached has been decreasing over several six-month reporting periods in a row.

Ransomware

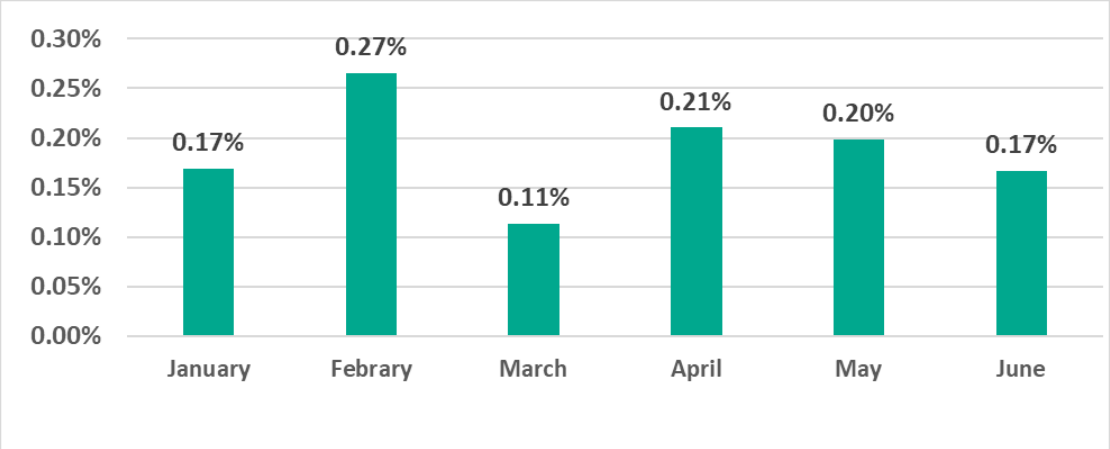
During H1 2022 ransomware was blocked on 0.65% of ICS computers. This is the highest half-year percentage since H1 2020.

Percentage of ICS computers on which ransomware was blocked



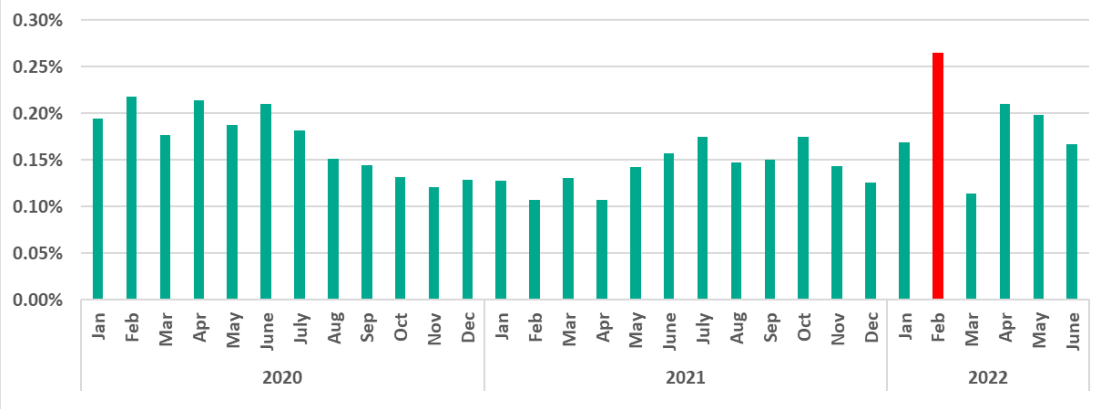
The largest percentage of ICS computers on which ransomware was blocked was recorded in February and the smallest in March.

Percentage of ICS computers on which ransomware was blocked, January – June 2022



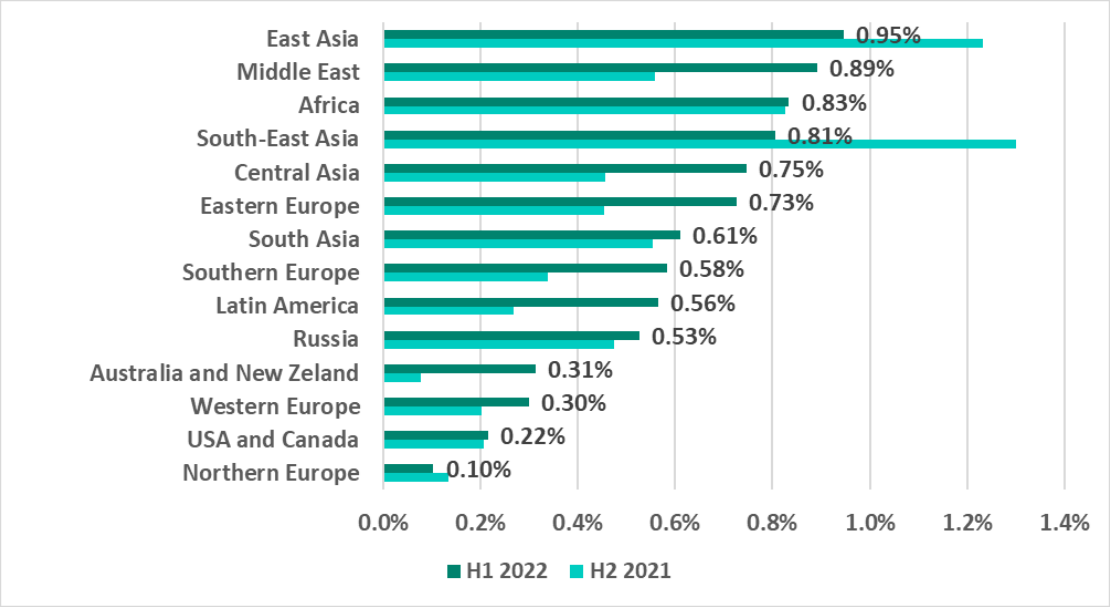
Notably, the February figure broke all records over two and a half years of observation.

Percentage of ICS computers on which ransomware was blocked, January 2020 – June 2022



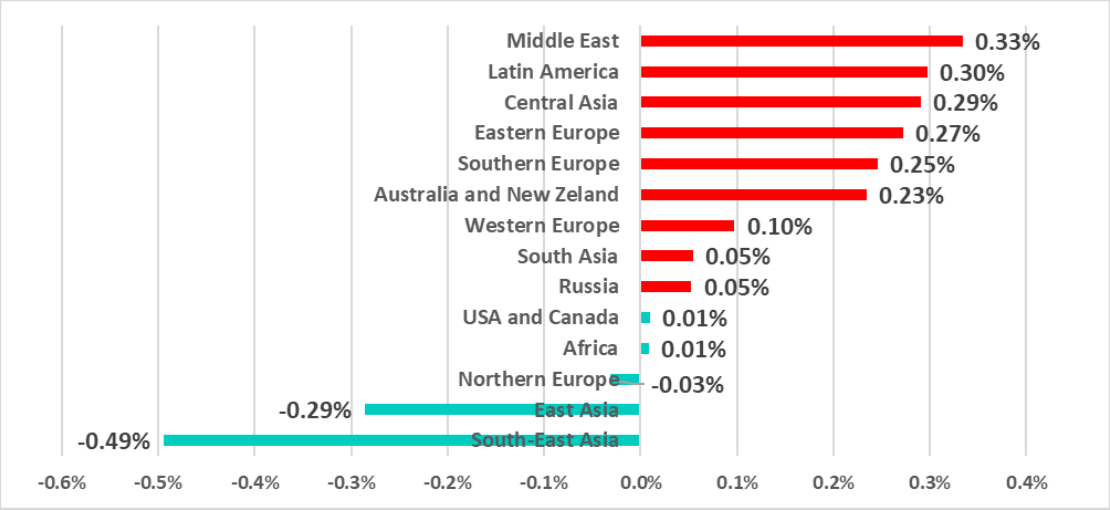
In H1 2022 the percentage of ICS computers attacked by ransomware increased in nine regions of the world.

Regions ranked by percentage of ICS computers on which ransomware was blocked in H1 2022



The growth in the Middle East and Latin America is particularly worth noting.

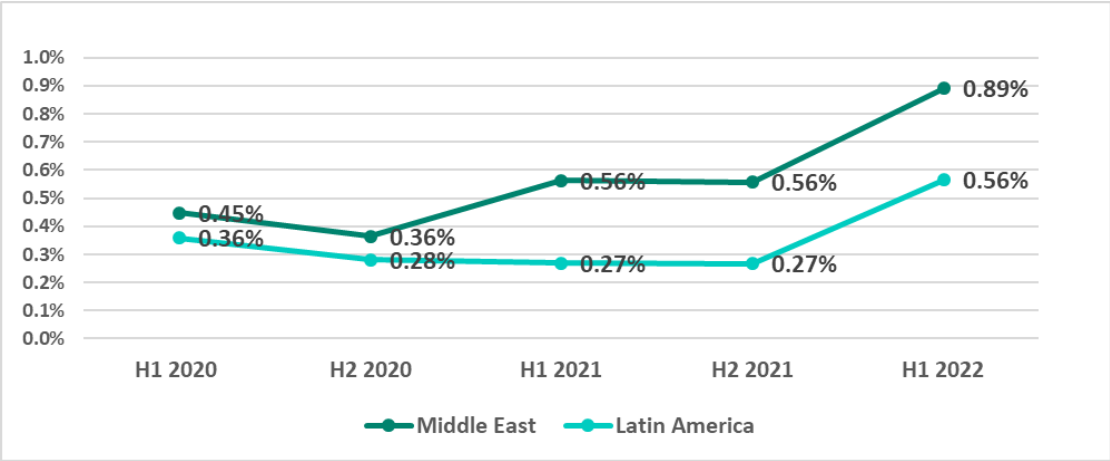
Changes throughout regions worldwide in the percentage of ICS computers on which ransomware was blocked



Since 2020 the percentage of ICS computers on which ransomware was blocked in the Middle East has increased slowly by a factor of 2.5.

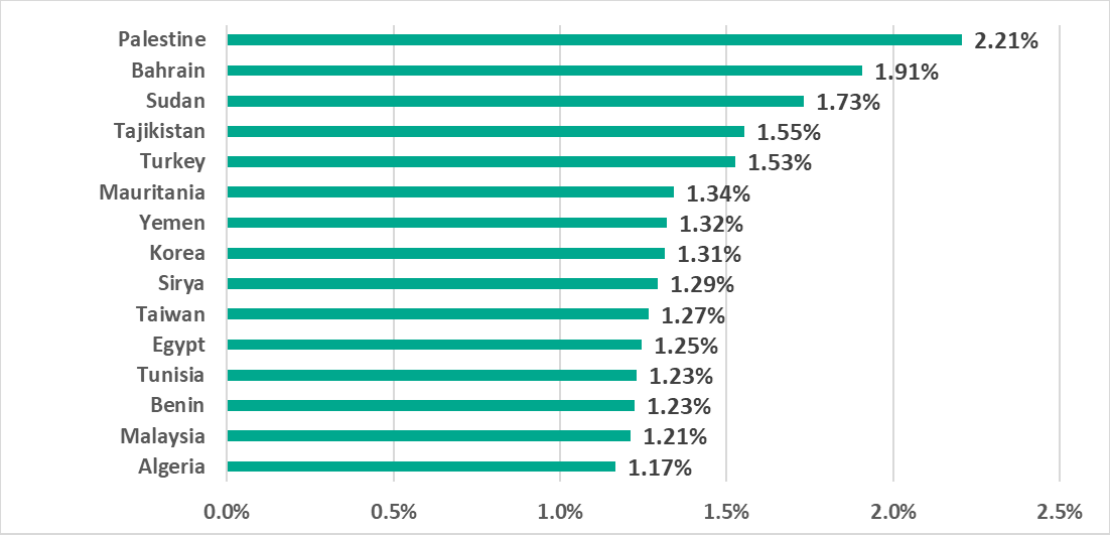
In Latin America the number was decreasing through the end of 2021, but in H1 2022 the number suddenly doubled versus the number in H2 2021.

Percentage of ICS computers on which ransomware was blocked in the Middle East versus Latin America



Palestine currently leads the ranking of countries and territories with the highest percentage of ICS computers on which ransomware was blocked.

Top 15 countries and territories with the highest percentage of ICS computers on which ransomware was blocked, H1 2022

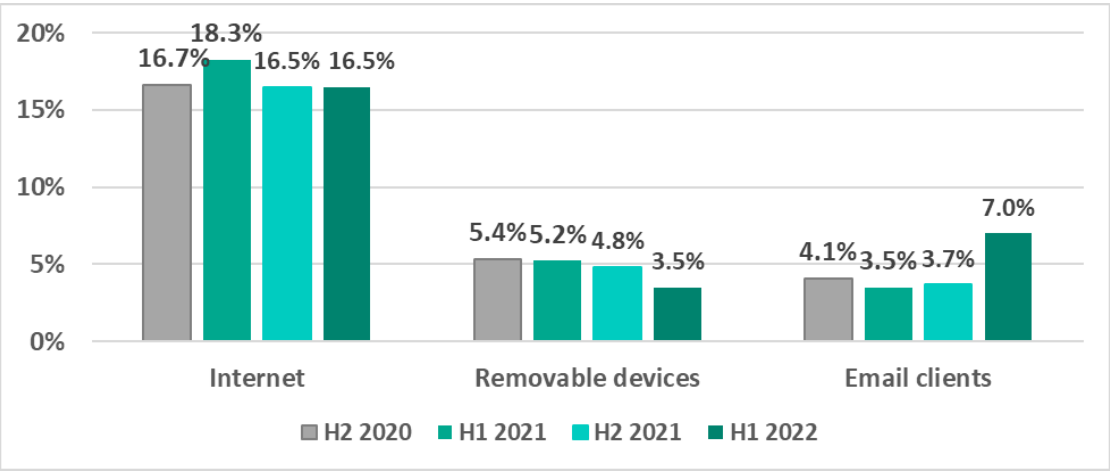


This ranking is updated every six-month period and in H1 2022 only 3 countries from H2 2021 remain – Algeria, Egypt and Turkey.

Threat sources

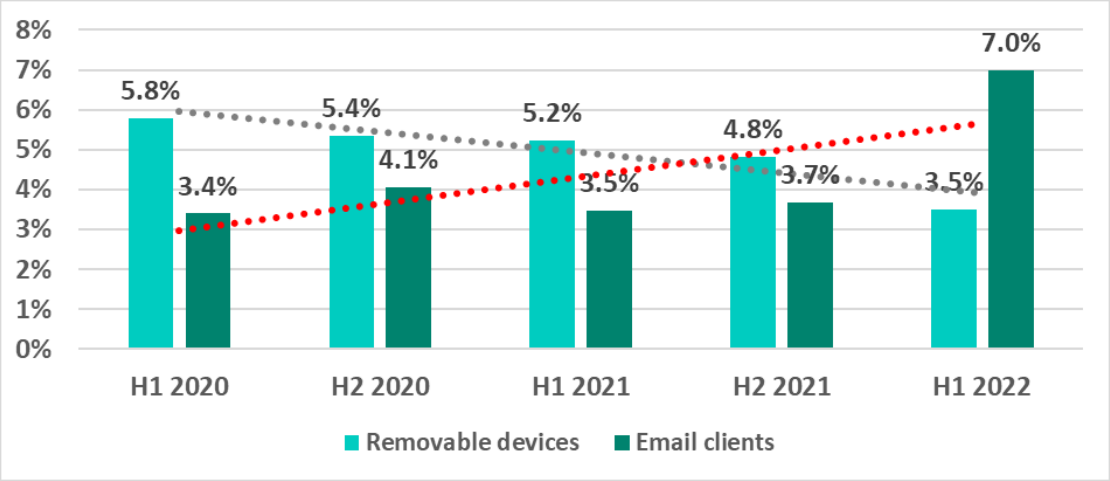
The main threat sources for computers in the operational technology infrastructure of organizations continue to be the internet, removable media and email.

Percentage of ICS computers on which threats from various sources have been blocked



In H1 2022 we see a continuing decrease in the percentage of ICS computers on which malware was blocked when removable media was attached.

Percentage of ICS computers on which malware was blocked when removable media was attached versus malicious email attachments and phishing links



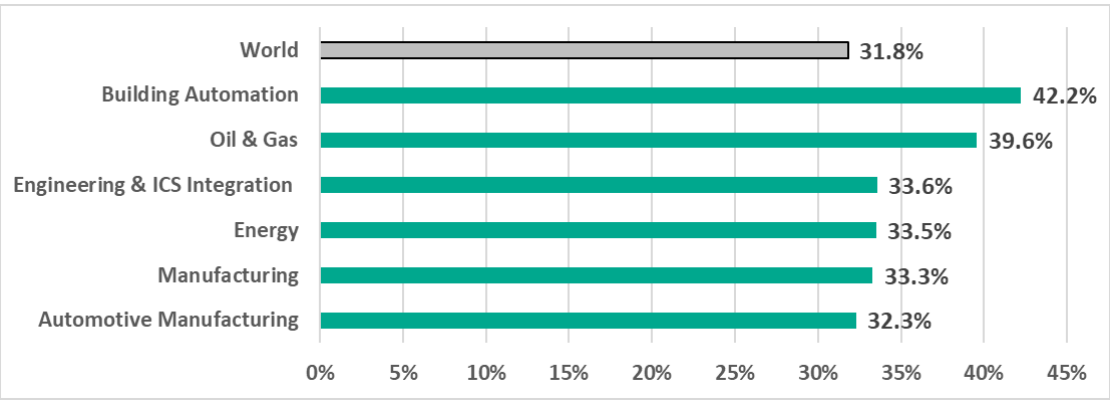
At the same time, we see a stable growth in the percentage of ICS computers on which malicious email attachments and phishing links have been blocked. A marked difference between H2 2021 and H1 2022 is due in part to the larger number of ICS machines that supply anonymized statistics to us. A large proportion of the 'new' machines are computers of ICS engineers and building automation systems, on which email clients are used extensively (see statistics by industry below). The contribution of such machines to the overall percentage of ICS computers on which malicious email attachments and/or phishing links were blocked was 2 – 2.5 p.p., while the remaining ICS computers accounted for a growth of about 1% p.p.

Selected industries

We have taken a look at several industries to see how the situation changes from sector to sector.

The percentage of ICS computers on which malicious objects were blocked in all our chosen industries was greater than the global average.

Percentage of ICS computers where malicious objects were blocked in selected industries in H1 2022

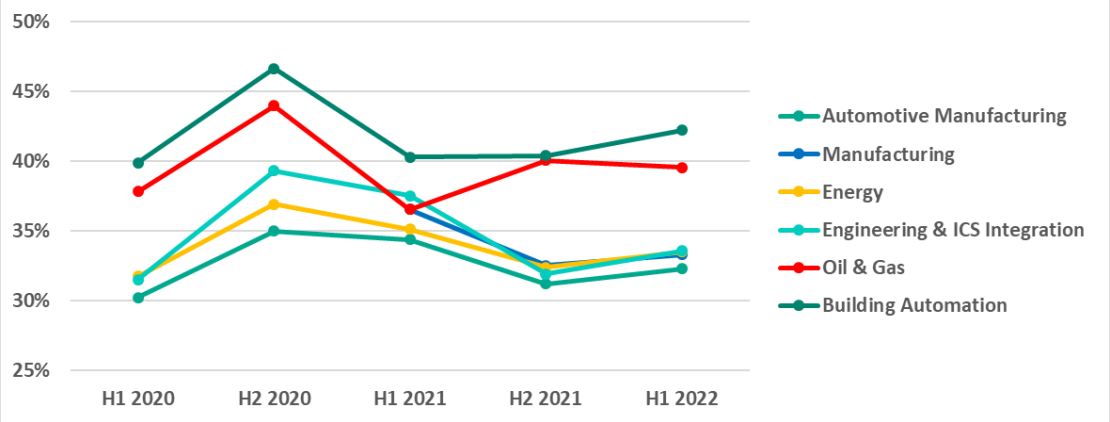


Two sectors, Building Automation and Oil and Gas, lead the rest by 8.6 p.p. and 6 p.p. respectively.

The Engineering and ICS integrators, Energy, and Manufacturing sectors are within 0.1 p.p. from each other.

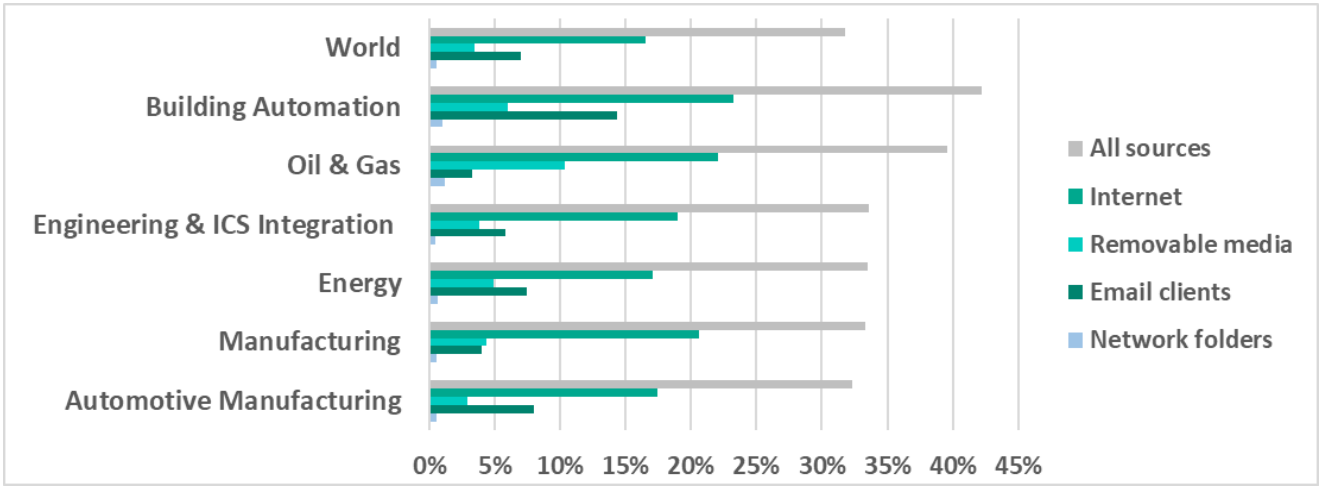
In 2021, the percentage of ICS computers on which malicious objects were blocked decreased in all sectors we investigated. The only exception was Oil and Gas, where the percentage grew in H2 2021. However, Oil and Gas was the only sector in H1 2022 where the percentage decreased – the percentage increased slightly in all other sectors.

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



Despite the increase in the percentage of attacked ICS computers in H1 2022, all of the percentages are less than in H2 2020.

The main threat sources in all sectors were the internet, email and removable media.



Percentage of ICS computers on which malware from various sources were blocked in selected industries in H1 2022

Building Automation

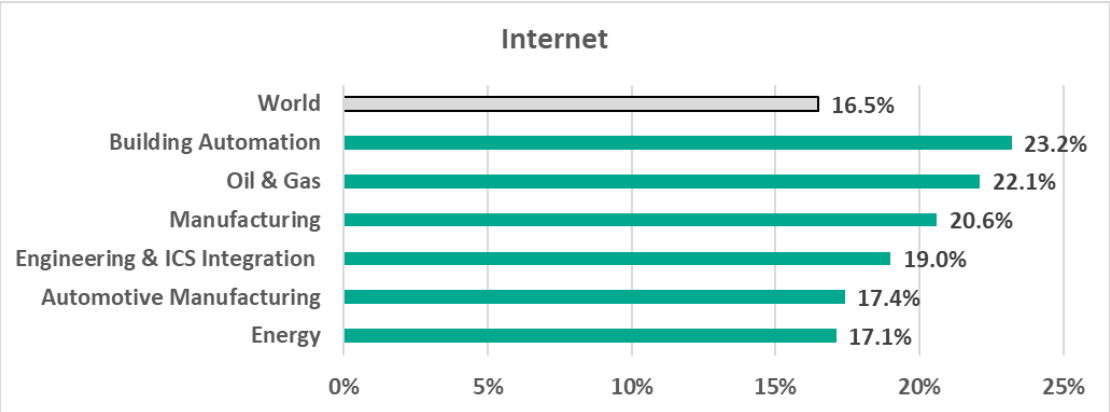
Building Automation is in first place in the rating of selected industries ranked by percentage of ICS computers on which malicious objects were blocked with 42.2%.

This was the most "restless" industry – it led in most industry ratings by different types of malware and also by some threat sources.

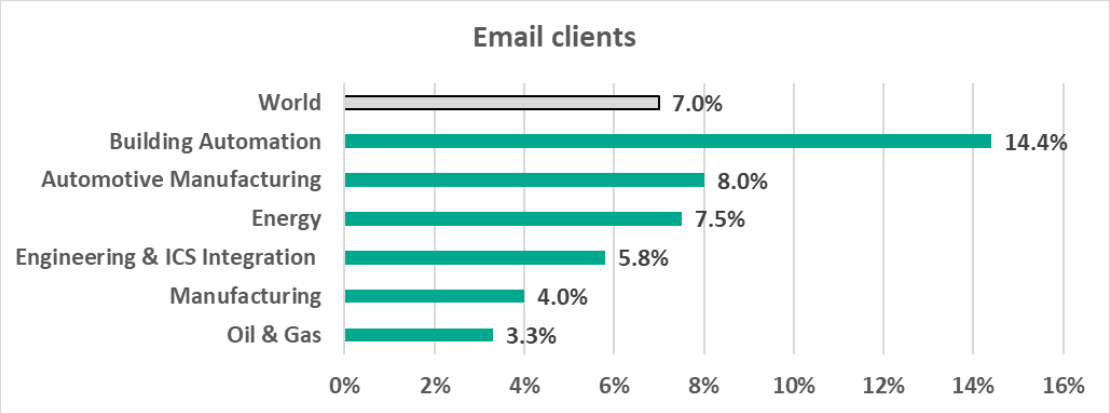
It can be seen in the diagrams below that professionals in the Building Automation industry use internet resources and email more actively than those in other industries. As a result, they can prove a more accessible 'entry point' into the target organization's infrastructure for attackers. Given that the building automation system monitoring and control function is often taken out of an enterprise's organization structure and is provided, for example, as a third-party service, a compromised workstation of a building automation system engineer or operator can easily provide attackers with access to many organizations at the same time.

Building Automation leads in ratings based on the percentage of ICS computers on which the following types of threats have been blocked:

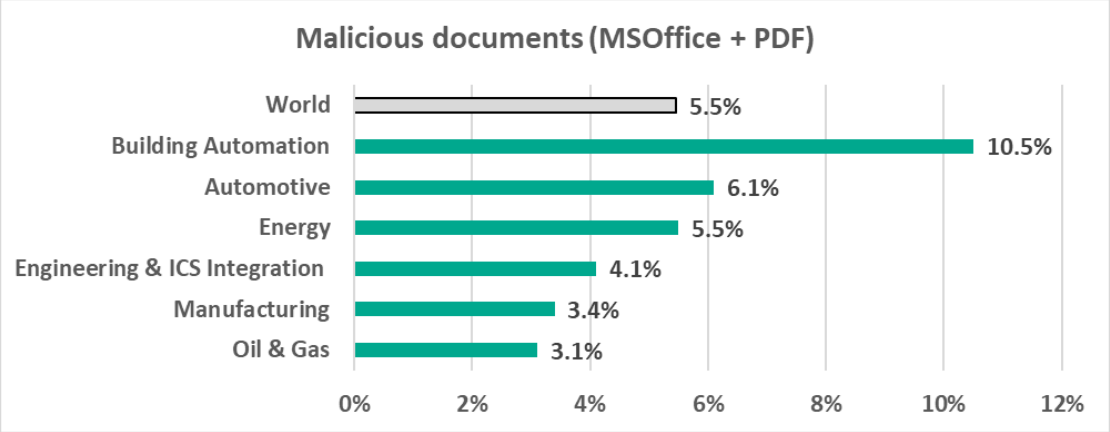
- Malicious objects from the internet



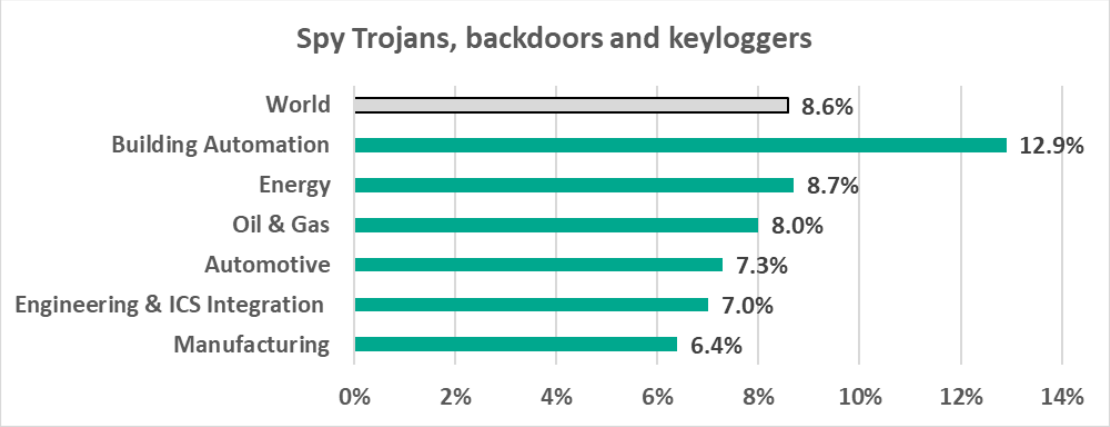
- Threats distributed via the internet:
  - denylisted internet resources – 11.5%,
  - malicious scripts and phishing pages – 17.7%.
- Malicious email attachments and phishing links. As we can see in the diagram below, Building Automation leads with a significant margin, and, moreover, the percentage for this sector is twice as much as the average worldwide.



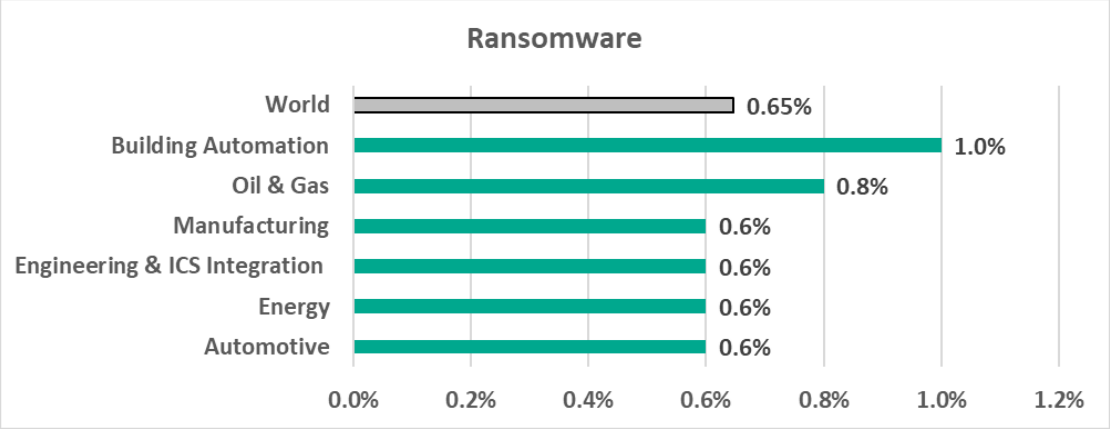
- Malicious office documents, which are usually distributed via phishing emails. In this category the Building Automation percentage is predictably almost twice the average worldwide.



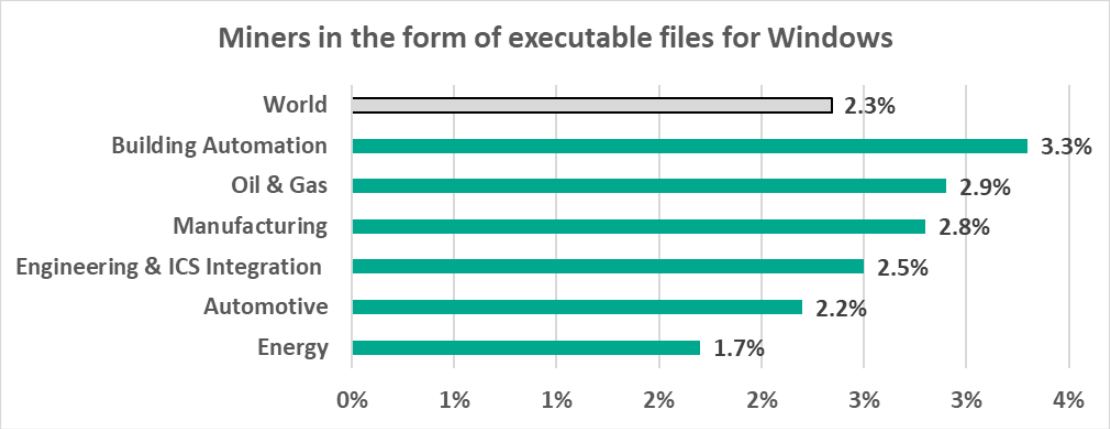
- Spyware, which is the most common payload of phishing emails, is also found on a larger percentage of computers than in other industries.

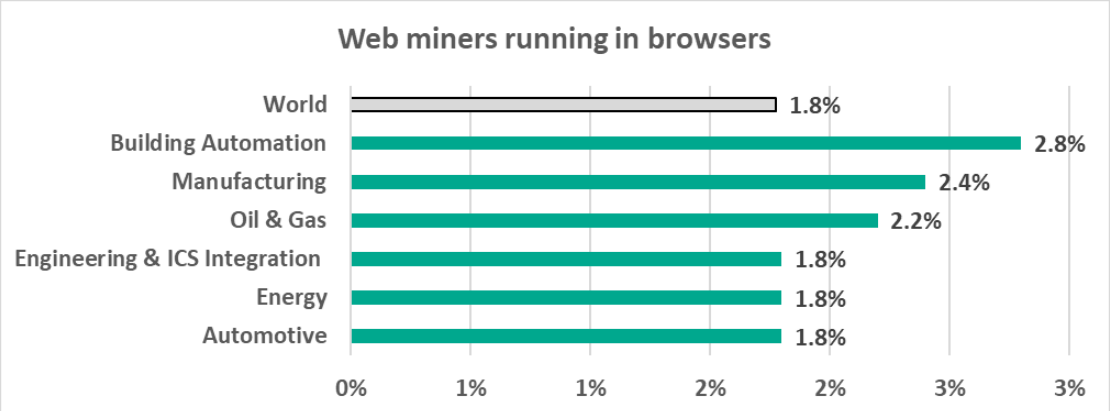


- Ransomware



- Malware for covert cryptocurrency mining





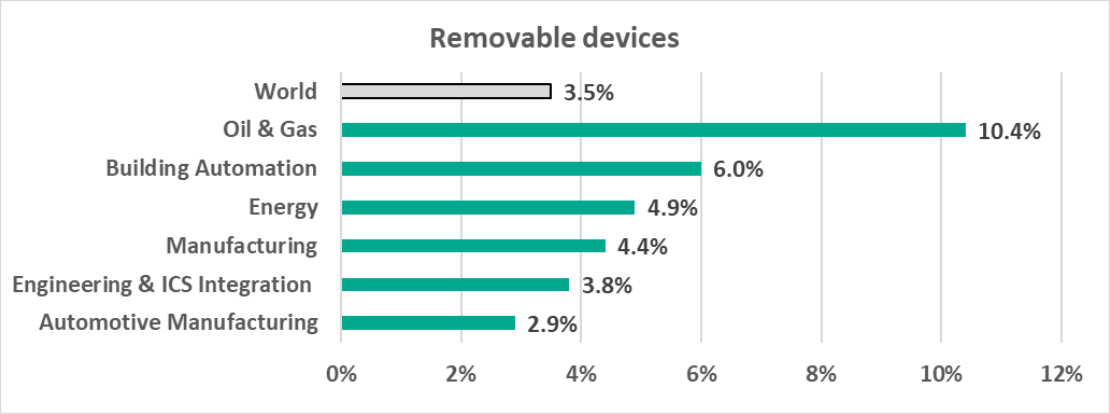
Oil and Gas

Oil and Gas is in **second place** among selected industries based on percentages of ICS computers on which the following malicious objects were blocked:

- all malicious objects (39.6%),
- ransomware (0.8%),
- cryptocurrency miners – Windows executable files (2.9%) (see the diagrams above).

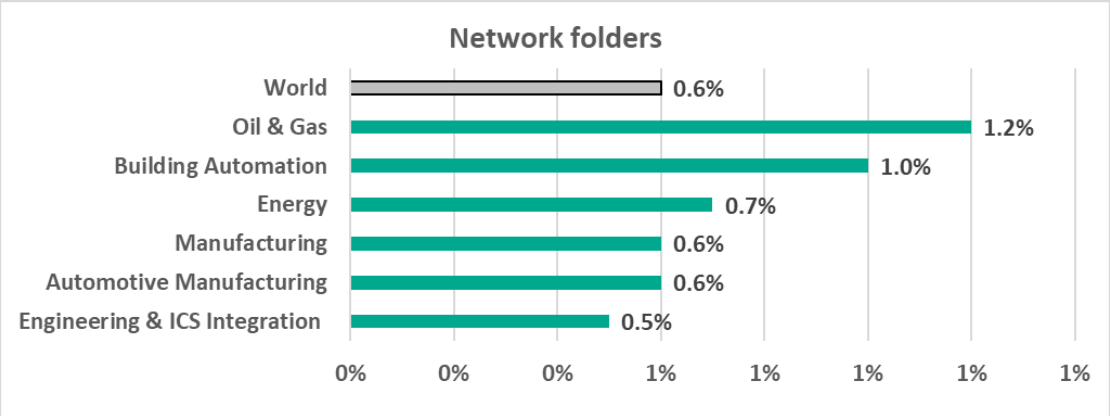
In its turn, Oil and Gas leads industries in the following rankings by percentage of ICS computers on which malware was blocked:

- When removable media was attached.

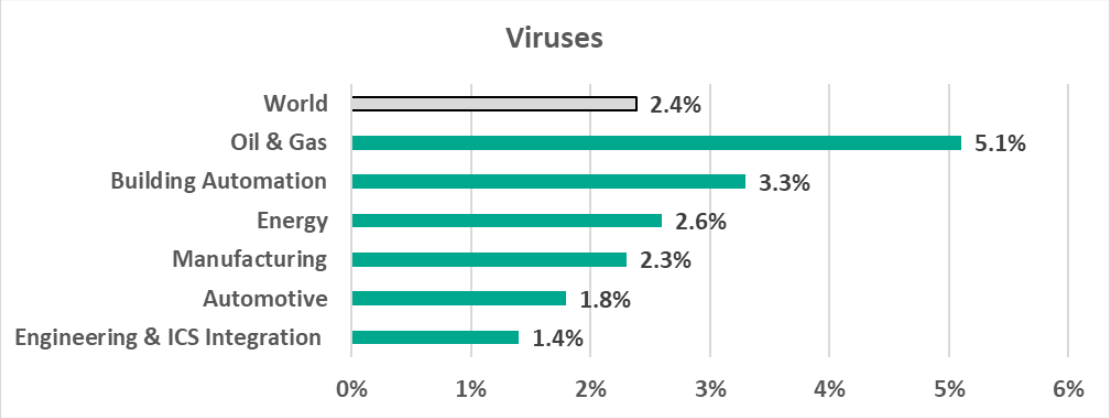


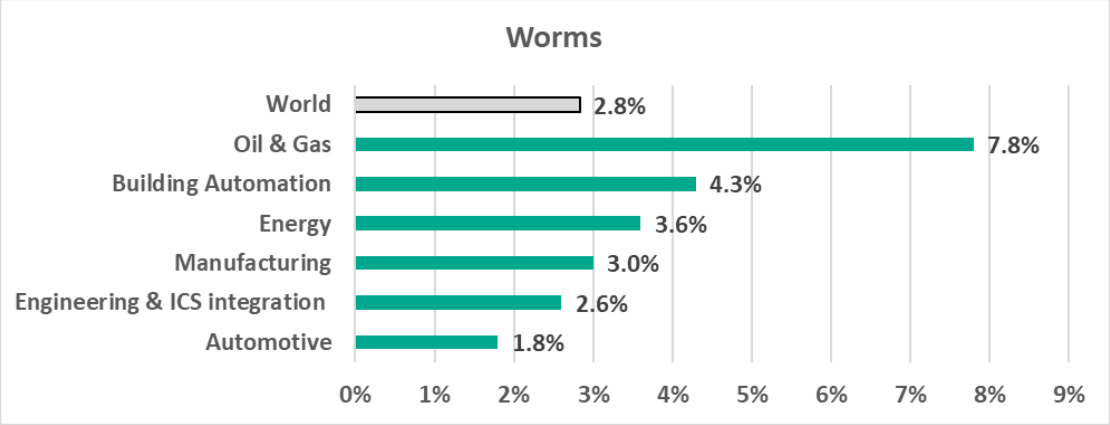
We believe that such a high percentage of computers on which malware is blocked when removable media is connected can be due primarily to the way this industry operates. A large number of geographically distributed enterprises, often with poor communication channels connecting remote systems and sites, means that removable media has to be used more extensively when performing maintenance tasks, compared with other industries.

- In network folders.



- Viruses and worms.





Unsurprisingly, since Oil and Gas leads in the removable media and network folder categories, it leads here, since viruses and worms mostly spread through networks via removable media and network folders.

Manufacturing

The Manufacturing industry is in **third place** in rankings of selected industries by percentage of ICS computers on which the following threats were blocked.

- internet threats (20.6%),
- cryptocurrency miners – Windows executable files (2.8%).

The industry is also in **second place** when ranked by web miners, which are executed in browsers (2.4%, see the diagrams above).

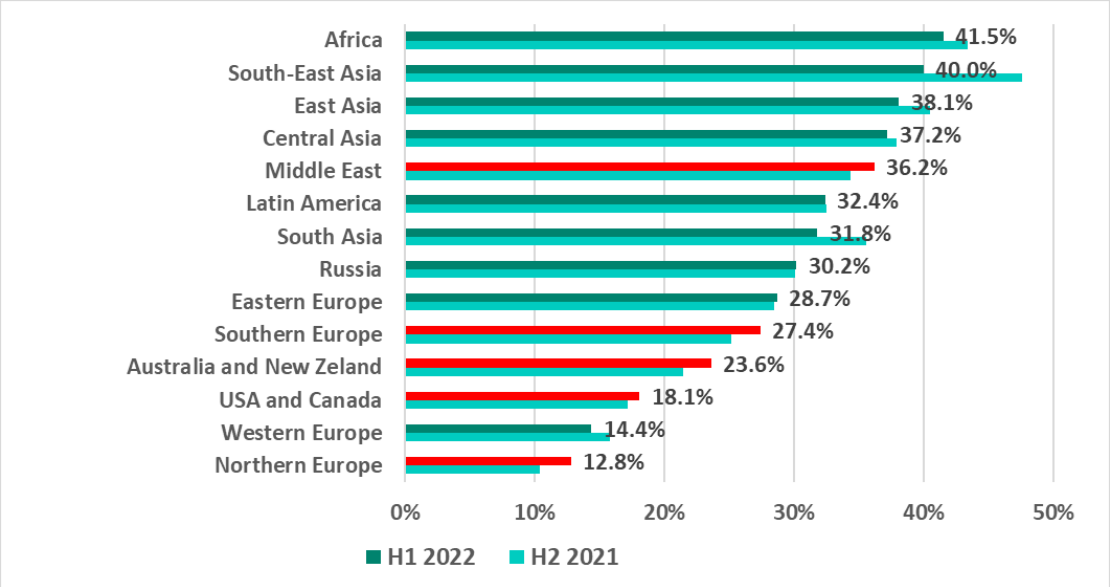
Regions and countries

The map below shows the percentage of ICS computers on which malicious objects were blocked in each country, relative to overall number of ICS computers in each country.

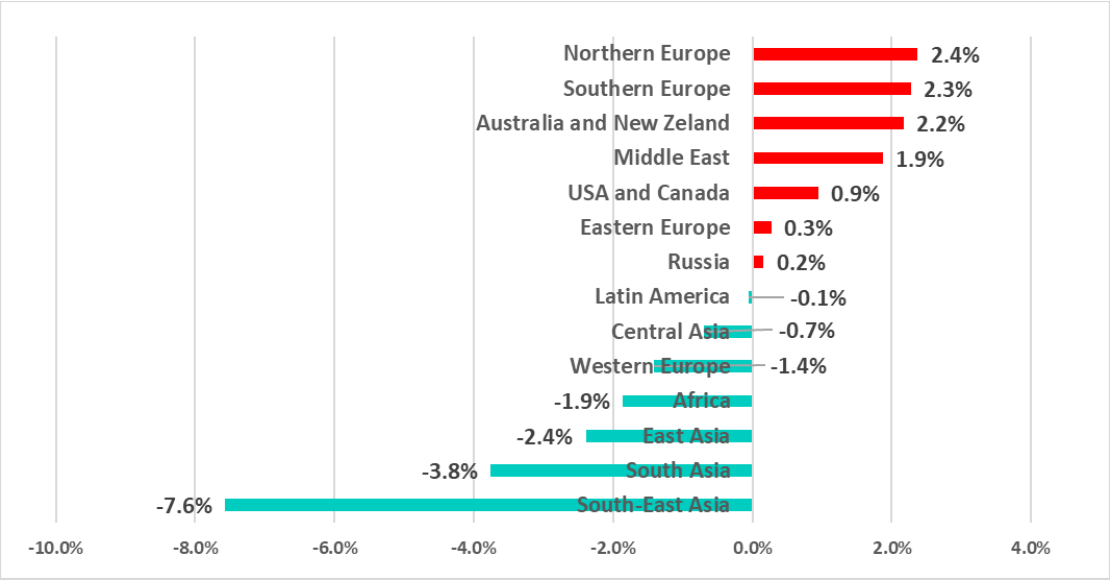
Regions

Africa, Southeast Asia, 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.

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



Changes in H1 2022 in the percentage of ICS computers on which malicious objects were blocked in regions around the world

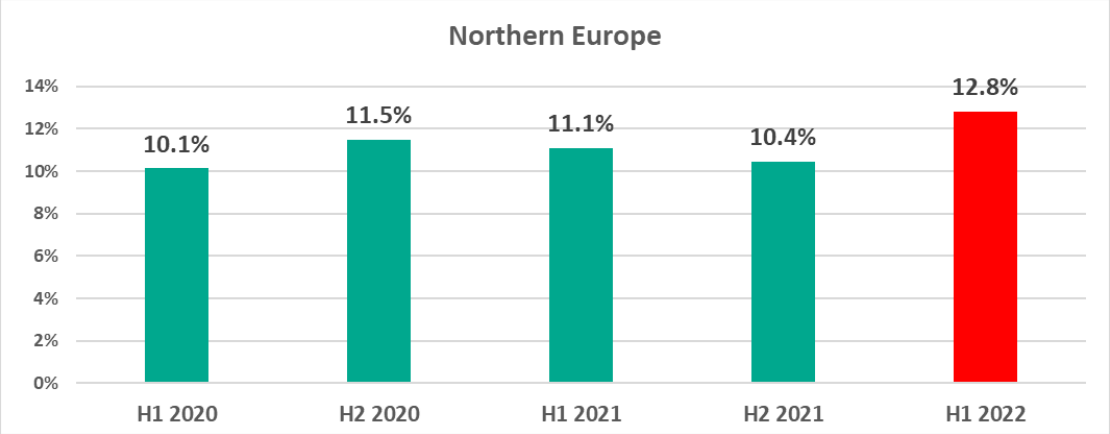


As the graphs demonstrate, in H1 2022 the percentage of ICS computers on which malicious objects were blocked increased in 7 out 14 global regions. All of them, except for the Middle East, are in the lower part of the ratings, i.e., among the more secure ones in this category. The only secure region in which the percentage decreased was Western Europe.

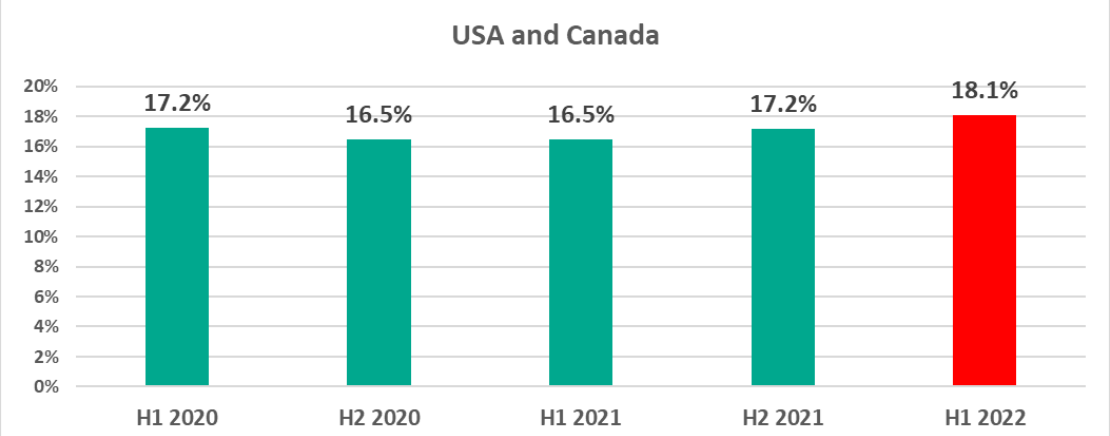
At the same time, the percentage has decreased in H1 2022 in the top 7 positions (aka the less secure ones) in the regional ratings by percentage of ICS computers on which malicious objects were blocked. The only exception was the Middle East, as mentioned above.

In the USA and Canada, as well as Northern Europe we see the largest percentage of ICS computers on which malicious objects were blocked that we have seen in 2.5 years.

Percentage of ICS computers on which malicious objects were blocked in Northern Europe

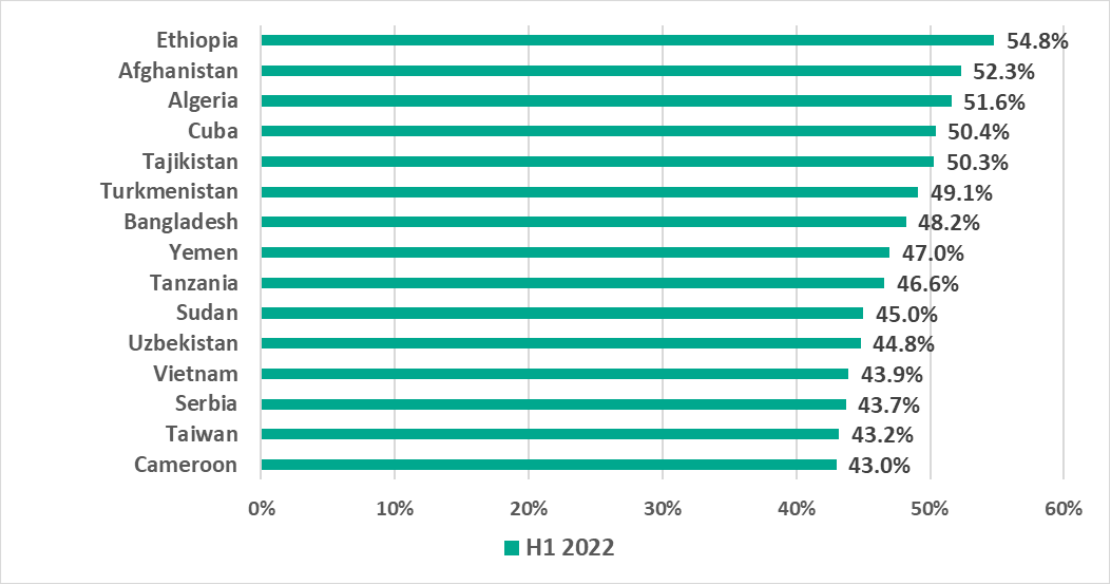


Percentage of ICS computers on which malicious objects were blocked in the USA and Canada



Countries

Top 15 countries and territories with the largest percentages of ICS computers on which malicious objects were blocked, H1 2022

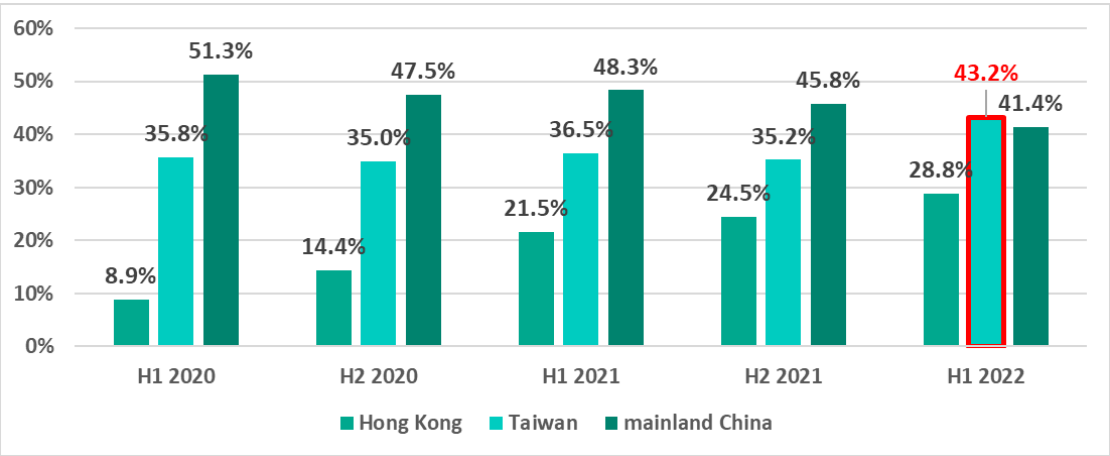


Three of the countries and territories, South Africa (+11.5 p.p.), Denmark (+9.4 p.p.) and Taiwan (+8.0 p.p.), demonstrated the most significant increases in the percentage of ICS computers on which malicious objects were blocked. In all three we also see the largest percentage in H1 2022 during the period from H1 2020 through H1 2022.

In 2021 we noted that the percentage of attacked ICS computers was relatively stable in Taiwan, was gradually increasing in Hong Kong and decreasing in mainland China.

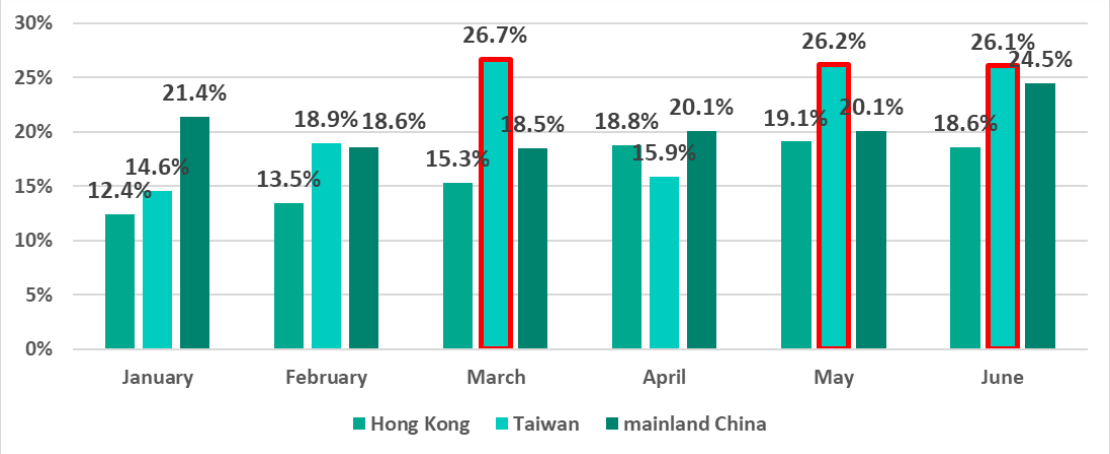
In H1 2022 we see these trends continuing in Hong Kong and mainland China, however the percentage has increased so much in Taiwan, that it is greater than in mainland China.

Percentage of ICS computers on which malicious objects were blocked in Hong Kong, Taiwan and mainland China



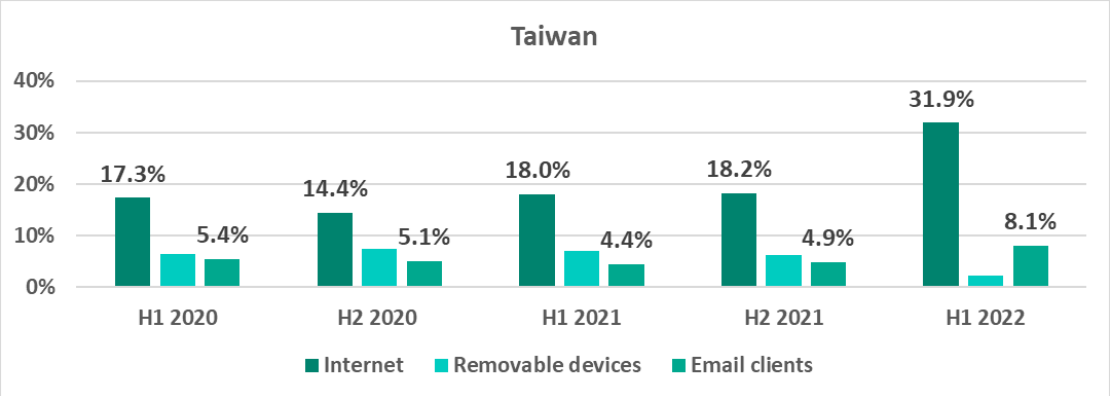
The largest percentages of ICS computers on which malicious objects were blocked in Taiwan were recorded in March, May and June.

Percentage of ICS computers on which malicious objects were blocked in Hong Kong, Taiwan and mainland China by month, January – June 2022



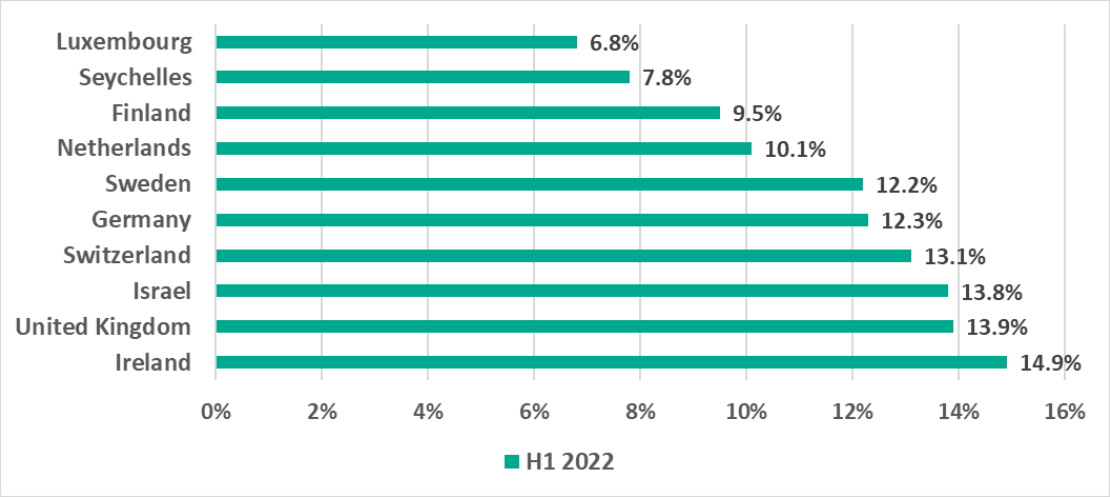
At the same time, in H1 2022, the percentage of ICS computers on which threats from the internet were blocked increased in Taiwan (Taiwan even ranked top among countries and territories based on this indicator). This growth is largely due to an aggressive advertising campaign in Taiwan during this period, in which users were redirected to phishing resources).

Percentage of ICS computers on which malicious objects were blocked by threat source



Similar to H2 2021, the smallest percentage of ICS computers on which malicious objects were blocked in H1 2022 was recorded in Luxembourg.

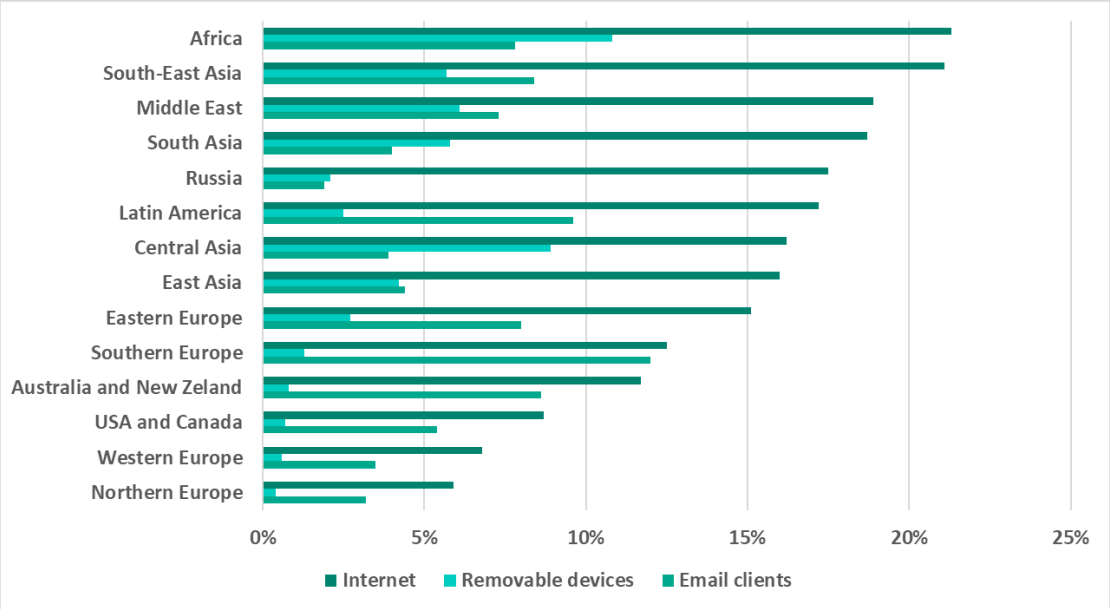
10 countries and territories with the smallest percentages of ICS computers on which malicious objects were blocked, H1 2022



The most significant decreases in the percentage of ICS computers on which malicious objects were blocked were observed in Vietnam (-11.0 p.p.), Iraq (-9.7 p.p.) and in Tunisia (-8.5 p.p.).

Main threat sources: geography

Main sources of threats blocked on ICS computers, in global regions, H1 2022

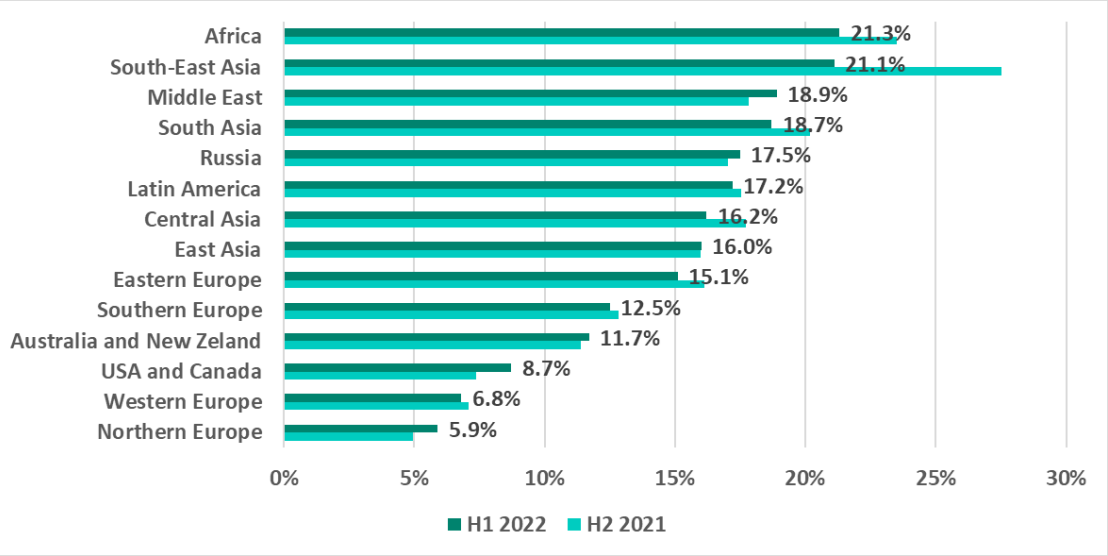


It is worth remembering that it is not always possible to ascertain the exact source when calculating the percentage of ICS computers on which malicious objects from various sources were blocked.

Internet

The percentage of ICS computers on which threats from the internet were blocked in H1 2022 increased in the Middle East (+1.1 p.p.), in Russia (+0.5 p.p.), in North America (+1.3 p.p.) and Northern Europe (+0.9 p.p.).

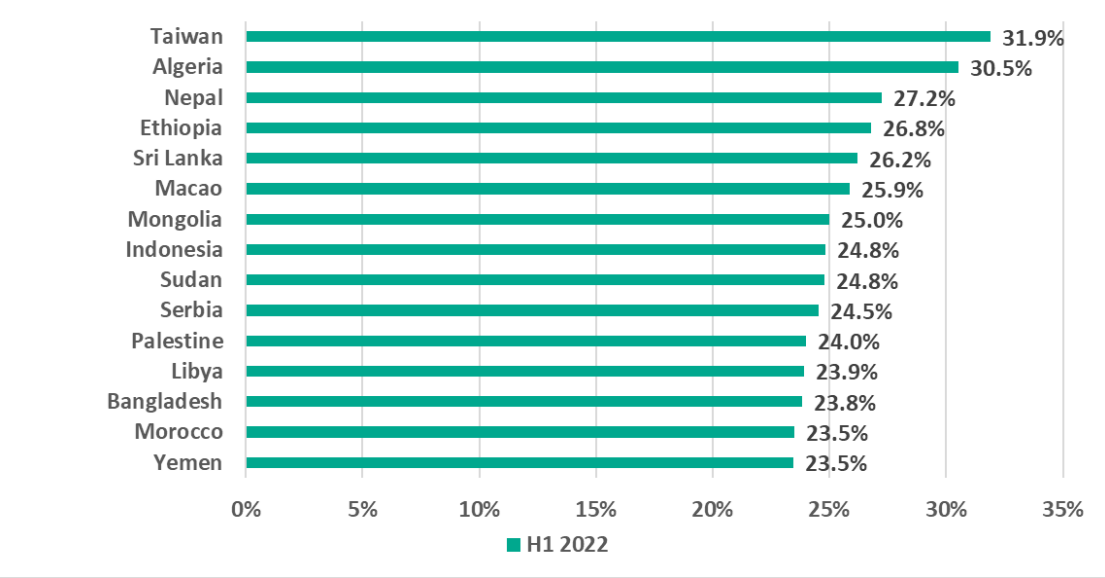
Percentage of ICS computers on which threats from the internet were blocked, by global regions



A noticeable decrease in the percentage was recorded in Southeast Asia (-6.4 p.p.).

Taiwan leads among all countries and territories. We already noted above, that in H1 2022 Taiwan unexpectedly experienced a growth of +8 p.p. in the percentage of ICS computers on which malicious objects were blocked. It is clear that threats from the internet were the main contributors to this growth.

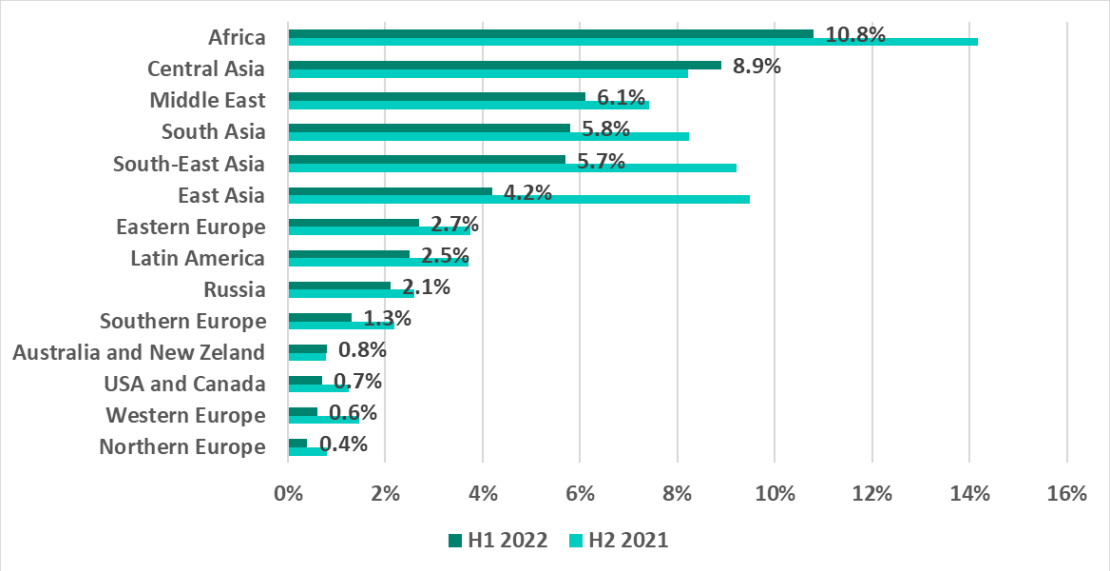
TOP 15 countries and territories with the highest percentage of ICS computers on which internet threats were blocked, H1 2022



Removable media

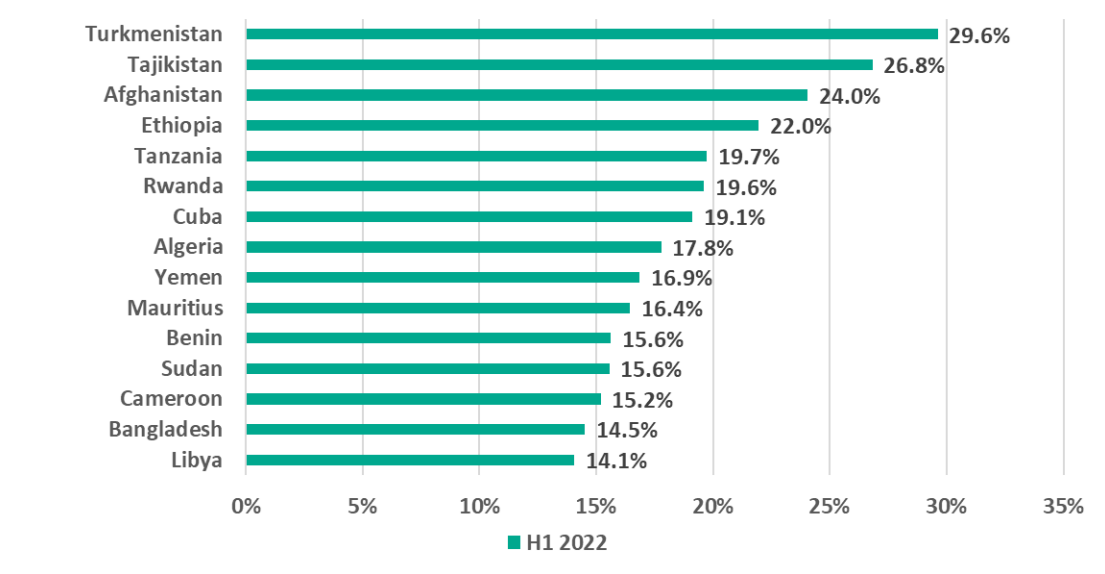
The percentage of ICS computers on which malware was blocked when removable media was attached decreased in all regions except Central Asia and Australia and New Zealand.

Regions ranked according to percentage of ICS computers on which malware was blocked when removable media was connected, H1 2022



Central and Southeast Asian countries led the ranking of countries and territories based on percentage of ICS computers on which malware was blocked when removable media was attached.

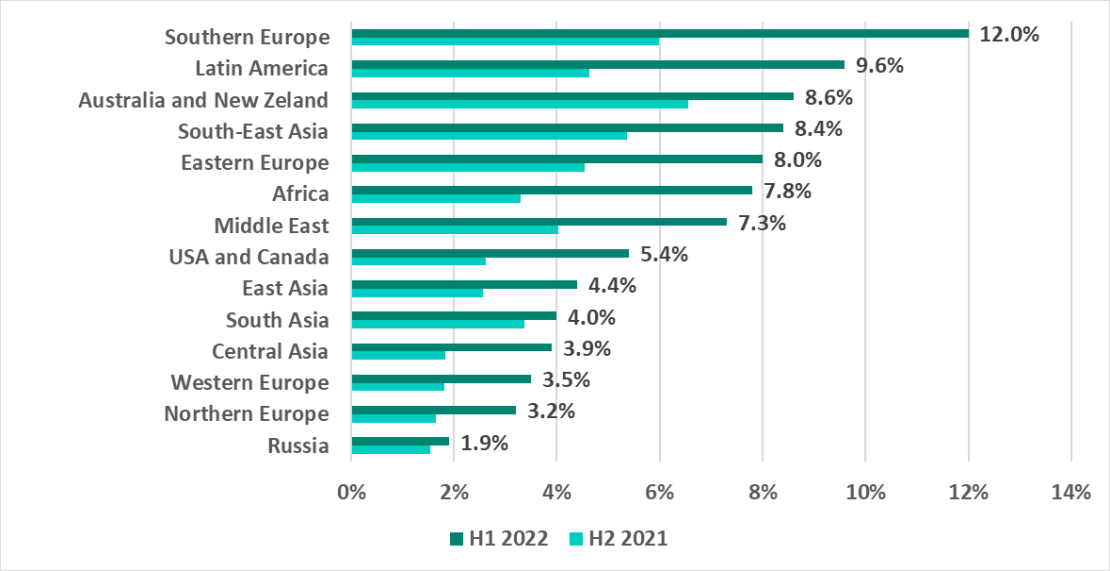
TOP 15 countries and territories ranked by percentage of ICS computers on which malware was blocked when removable media was attached, H1 2022



Email clients

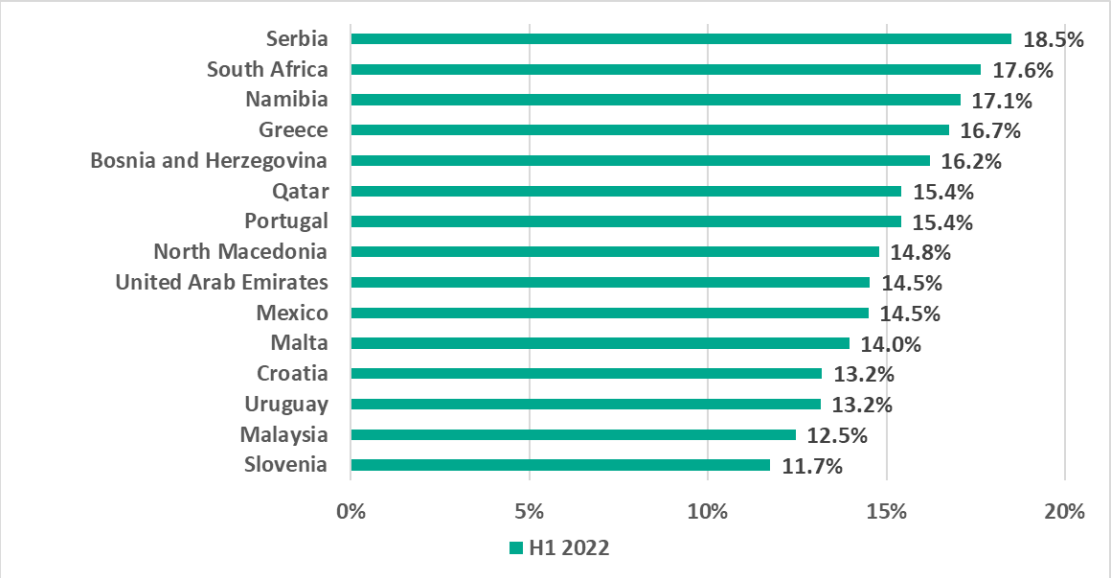
In H1 2022 the percentage of ICS computers on which malicious email attachments and phishing links were blocked increased in all regions. The largest increase was recorded in Southern Europe (+6.0 p.p.), which also led the ranking based on this parameter.

Regions ranked by the percentage of ICS computers on which malicious email attachments and phishing links were blocked, H1 2022



Countries and territories from various regions ended up in the TOP 15 ranking by percentage of ICS computers on which malicious email attachments and phishing links were blocked.

TOP 15 countries and territories with the largest percentages of ICS computers on which malicious email attachments and phishing links were blocked, H1 2022



Most of the countries on this list are from Eastern and Southern Europe.

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.

For the purposes of this report, "attacked computers" are those on which Kaspersky security solutions blocked one or more threats during the reporting period (in the diagrams below, a reporting period can be a month, a six-month period or a year, depending on the context). 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.

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