Kaspersky Lab ICS CERT

KASPERSKY lab

Threat Landscape for Industrial Automation Systems

H1 2018

06.09.2018 Version 1.1

Contents

For many years, Kaspersky Lab experts have been uncovering and researching cyberthreats that target a variety of information systems – those of commercial and government organizations, banks, telecoms operators, industrial enterprises, and individual users. In this report, Kaspersky Lab Industrial Control Systems Cyber Emergency Response Team (Kaspersky Lab ICS CERT) publishes the findings of its research on the threat landscape for industrial automation systems conducted during the first half of 2018.

The main objective of these publications is to provide information support to global and local incident response teams, enterprise information security staff and researchers in the area of industrial facility security.

H1 2018 – Key events

Spectre and Meltdown vulnerabilities in industrial solutions

In early 2018, vulnerabilities that allow unauthorized access to virtual memory content were discovered in Intel, ARM64 and AMD processors. The attacks exploiting these vulnerabilities were given the names Meltdown and Spectre.

The issue is related to three vulnerabilities:

- bounds check bypass (CVE-2017-5753/Spectre);
- branch target injection (CVE-2017-5715/Spectre);
- rogue data cache load (CVE-2017-5754/Meltdown).

While both Spectre and Meltdown attacks allow user applications to obtain other programs' data, Meltdown attacks also allow kernel memory to be read.

This problem has affected many computers, servers and mobile devices running Windows, macOS, Linux, Android, iOS and Chrome OS that use vulnerable microprocessors. Industrial equipment – SCADA servers, industrial computers and network devices with vulnerable processors – also proved vulnerable to Meltdown and Spectre.

One of the first companies to report about the vulnerabilities in their products was Cisco. Affected devices include Cisco 800 Industrial Integrated Services Routers and Industrial Ethernet 4000 switches.

Other industry vendors then published notifications about the impact of the Meltdown and Spectre vulnerabilities on their products.

PHOENIX CONTACT informed customers that dozens of its products, including control systems, industrial computers and HMI were vulnerable to Meltdown and Spectre.

Meltdown and Spectre also affected Siemens industrial equipment: RUGGEDCOM APE and RX1400 VPE devices, SIMATIC HMI Comfort panels, SIMATIC IPC industrial computers, SIMATIC S7-1500 Software Controller PLC, and others.

As well as the information on Meltdown and Spectre, Siemens reported its solutions being affected by two more vulnerabilities from a class of vulnerabilities referred to as Spectre Next Generation (Spectre-NG) discovered later in May 2018.

Other vendors, including Schneider Electric, ABB and OSIsoft, also published information about the use of vulnerable processors in their products.

Energetic Bear/Crouching Yeti: attacks on servers

In February, Kaspersky Lab ICS CERT published a report on an investigation into the initial infection tactics used by the notorious APT group Energetic Bear/Crouching Yeti, as well as the results of an analysis of several web servers compromised by the group in 2016 and early 2017, using information provided by the server owners.

Energetic Bear/Crouching Yeti has been active since at least 2010, attacking companies and individuals in various countries. The specialists at CrowdStrike initially noted a strong focus on the energy and industrial sectors, which may explain the name Energetic Bear. Later, when the diversity of the group's attacks became clearer, the researchers at Kaspersky Lab named it Crouching Yeti. The targets of the attacks are mainly concentrated in Europe and the US.

Recently, the number of attacks on companies in Turkey increased significantly. According to US-CERT and the UK National Cyber Security Centre, the Energetic Bear/Crouching Yeti APT group is linked to the Russian government.

The initial infection tactics used by the group is a multi-step process that begins with phishing emails being sent out with malicious documents and infecting various servers. Some infected servers are used by the group as auxiliaries – used only for hosting various tools. Others are infected so they can be used in watering hole attacks, with some servers hosting an SMB link that leads to other servers that steal the authentication data of potential victims.

With some rare exceptions, the Energetic Bear/Crouching Yeti group uses publicly available tools to carry out their attacks. All the utilities discovered by the Kaspersky Lab ICS CERT experts have open source code that is freely available on GitHub. This makes the task of attack attribution very difficult without additional group "markers".

In most cases observed by Kaspersky Lab ICS CERT, the attackers performed tasks to identify vulnerabilities, gain persistence on different nodes and steal authentication data in order to develop the attack further.

An analysis of the compromised servers and the attacks on them showed that for Energetic Bear/Crouching Yeti, almost any vulnerable server on the internet is seen as a potential foothold from which to develop targeted attacks.

The investigation into the initial, intermediate and subsequent targets of these attacks also revealed a diverse geography. The largest number of victims and targets was in Russia, followed by Turkey and Ukraine. Under half of the systems attacked were related to industry, agricultural services and utilities.

Cryptominers in industrial networks

In February 2018, several media reports claimed industrial enterprises were infected with malware containing cryptocurrency mining functionality.

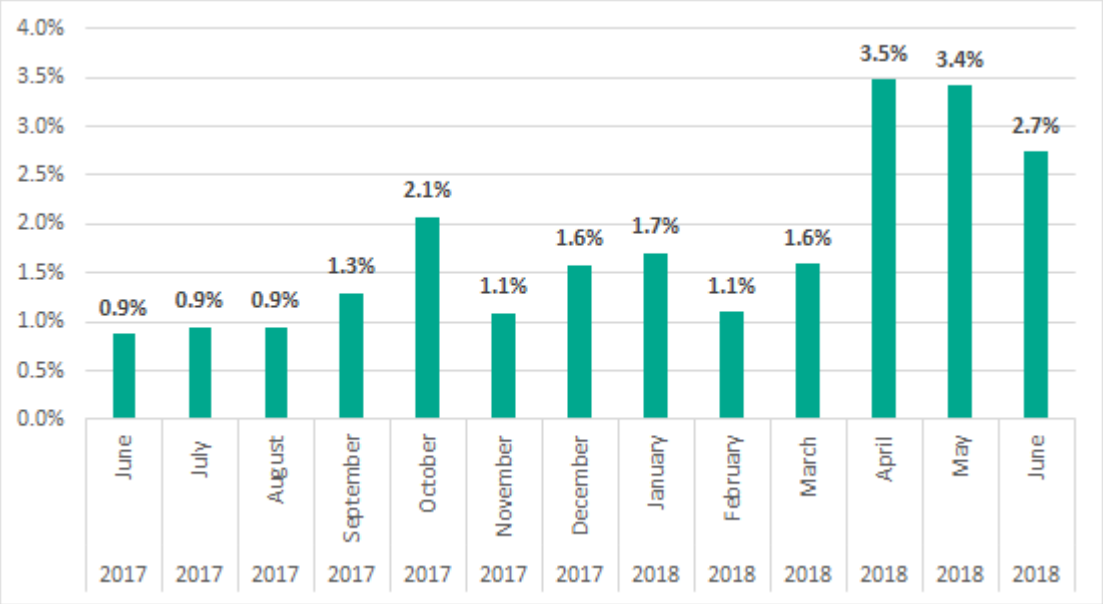
At one wastewater treatment plant in Europe four servers running Windows XP and CIMPLICITY SCADA software from GE Digital were compromised. The malware slowed down the HMI and SCADA servers used for monitoring industrial processes.

Tesla's cloud servers were also breached and their computing resources utilized to mine the Monero cryptocurrency. Cybercriminals attacked the Kubernetes framework used in the electric vehicle manufacturer's infrastructure and embedded malware to generate cryptocurrency.

According to Kaspersky Lab ICS CERT, these widely publicized incidents are far from being unique and reflect a worrying overall trend.

Since April 2018, Kaspersky Lab has been using more accurate verdicts to collect statistics about miners. They now include miners that were previously detected as Trojans.
As a consequence, our statistics show that the percentage of ICS computers attacked by malicious programs designed for mining cryptocurrencies has grown sharply since April and in the first half of 2018 reached 6% – 4.2 percentage points more than the previous six months.

Share of ICS computers attacked by cryptocurrency mining malware



The main problem caused by mining malware is the increased load on industrial information systems. This is likely to be inadmissible for many industrial automation systems as it could affect the stability of their operations and reduce the level of control over the industrial process at the enterprise.

Large-scale attacks on Cisco switches affect critical infrastructure objects

On April 6, attacks targeting Cisco IOS switches were detected around the world, affecting the operations of internet providers, data centers and websites.

The attackers exploited the CVE-2018-0171 vulnerability in the Cisco Smart Install Client software. According to the Cisco Talos team, more than 168,000 devices worldwide are potentially exposed.

The attack utilized a special bot that detects vulnerable devices, replaces the Cisco IOS image on the switches and modifies the configuration file. The switch then becomes unavailable.

The attacks had an obvious focus on organizations in Russia and Iran. According to Cisco Talos, the targeted companies included critical infrastructure facilities.

New VPNFilter malware with SCADA monitoring function

In May 2018, the new VPNFilter malicious software was discovered. It infected at least 500,000 routers and network-attached storage devices (NAS) in 54 countries.

VPNFilter has a complex modular architecture whose components implement various functions, including collecting network traffic and data, executing commands and controlling the device, intercepting packets, monitoring Modbus protocols, and communicating with the command server via the Tor network.

The malware exploits a variety of known vulnerabilities to infect devices, but the infection vector is not yet clear. During infection, a component is installed that persists through a reboot and is capable of downloading additional malicious modules.

That is why VPNFilter requires the close attention of the information security community, as this malware can be used to steal credentials, detect industrial SCADA equipment, and perform various attacks using infected devices together in a botnet.

Attack on satellite systems

In June 2018, a massive cyberattack originating from computers in China was detected. It targeted telecom operators, a satellite communications operator, as well as defense contractors in the United States and countries in South-East Asia.

During the attack, cybercriminals compromised computers used to control communication satellites and collect geolocation data. Expert opinion suggests the motives behind the cyberattacks were to spy and intercept data from civil and military communication channels. However, an attack like this could potentially lead to an unauthorized change to the location of satellites in orbit and disrupt communications.

The malware detected included the Rikamanu and Syndicasec Trojans, the Catchamas program for stealing data, the keylogger Mycicil and the backdoor Spedear.

The attackers used the legitimate software and administration tools PsExec, Mimikatz, WinSCP and LogMeIn to carry out the infection. These kinds of tools allow cybercriminals to conceal their activity and go unnoticed.

Key research: details on Triton malware

At the end of H1 2018, details appeared about the malicious TRITON software that caused a malfunction in the emergency protection system at an enterprise last December.

Triton was created specifically to interfere with the operation of Triconex Safety Instrumented System (SIS) from Schneider Electric. It is known that the closed TriStation network protocol is used for remote interaction with Triconex via the TriStation 1131 programming environment.

Malware analysis showed a strong match between specific strings found in the malicious program and in the TriStation program file tr1com40.dll, such as mnemonic names for the TriStation protocol's commands. The researchers concluded that to implement network communication with Triconex, the Triton developers had, by all appearances, reverse engineered executable files included in TriStation 1131.

IoT botnet activity

Since the beginning of the year, the number of new botnets made up of IoT devices has grown, confirming expert forecasts about a significant increase in the number of IoT zombie networks in 2018.

The most significant events in terms of IoT security were the appearance of the new Hide 'N Seek (HNS) botnet, as well as the detection of new Mirai modifications OMG and WICKED.

The botnets are still mainly composed of unprotected IP cameras and routers. However, the attackers have started using other types of 'smart' devices. For example, in April 2018,

a botnet consisting, among other things, of internet-connected TVs was discovered. It was used to implement DDoS attacks on financial organizations.

With such rapid development of malware targeting the IoT, news about the appearance of a public tool that automatically searches for and hacks vulnerable IoT devices is particularly significant. Publication of such programs in the public domain can dramatically increase the number of cybercriminals using IoT devices to attack computer systems and networks.

Ransomware attacks

Despite the global decrease in the number of users attacked by ransomware, the percentage of ICS computers on which ransomware attacks were blocked grew from 1.2% to 1.6%. Although this may not seem very significant, the danger posed by these programs to industrial enterprises can hardly be underestimated after the Wannacry and ExPetr campaigns.

In the first half of the year, extortionists were responsible for a dangerous incident at a medical institution involving a ransomware infection. According to media reports, an attack on the Federal Center for Neurosurgery in the city of Tyumen, Russia, resulted in cybercriminals gaining access to servers hosting components of the MEDIALOG medical information system used as a database for medical images, test results and other information needed to treat patients.

The MEDIALOG system turned out to be unavailable just when it was necessary for emergency brain surgery on a 13-year-old girl. It was later learned that the files needed for the operation had been encrypted by a malicious program. Fortunately, the surgeons managed to perform the operation despite not having access to important medical results.

The Neurosurgery Center in Tyumen was not the only victim in this series of attacks. Cybercriminals deliberately targeted medical institutions and only encrypted files hosted on servers that were critical for the work of that organization. This indicates that they intended to cause as much damage as possible to the working processes of the medical institutions.

This series of attacks is a vivid example of how cybercriminals can not only disable the computer systems of medical institutions but also have a direct impact on the treatment of patients.

Attacks on industrial enterprises using RATs

RMS and TeamViewer-based phishing attacks

Kaspersky Lab ICS CERT reported on yet another wave of phishing emails containing malicious attachments aimed primarily at industrial enterprises in Russia. The malicious program used in the attacks installs legitimate software for remote administration – TeamViewer or Remote Manipulator System/Remote Utilities (RMS) – that allows attackers to gain remote control over the targeted systems. Various techniques are used to mask the presence and activity of the unauthorized software.

When they need to move further within a compromised network, the attackers can download an additional set of malicious programs, which is specifically tailored to the attack on each individual victim. This set of malware may contain spyware, additional remote administration tools, software to exploit vulnerabilities in the operating system and application software, as well as the Mimikatz utility, which makes it possible to obtain account data for Windows accounts.

Phishing emails imitate legitimate commercial offers, with the content of each email reflecting the activity of the organization under attack and the type of work performed by the employee to whom the email is sent. The available information suggests the main purpose of the attackers is to steal money from the target organization's accounts. Obviously, in addition to financial losses, these attacks result in confidential data leaks.

The Kaspersky Lab ICS CERT report was published in early August, but this series of attacks dates back to November 2017.

Attacks using RATs in a company's industrial network

Kaspersky Lab products blocked multiple attacks on the industrial network of an automobile manufacturer and service company, in particular, on computers designed to diagnose the engines and onboard systems of trucks and heavy-duty vehicles.

A RAT was installed and intermittently used on at least one of the computers in the company's industrial network. Over a period of several months, numerous attempts to launch various malicious programs using the RAT were blocked on the computer. The blocked programs included modifications of the malware detected by Kaspersky Lab products as Net-Worm.Win32.Agent.pm. When launched this worm immediately begins to proliferate on the local network using exploits for the MS17-010 vulnerabilities – the same ones that were published by ShadowBrokers in the spring of 2017 and were used in attacks by the infamous WannaCry and ExPetr cryptors.

The Trojan-Downloader.Nymaim malware family was also blocked. Representatives of this family are often used to download modifications of the Necus family botnet agent which in turn is used to infect computers with ransomware from the Locky family.

Based on the frequency of attempts to run malware via the RAT and other data, we believe the RAT authentication data was compromised and used by cybercriminals to attack computers belonging to this organization from the internet.

The installation of RAT programs on ICS computers is sometimes a necessity, but they become very dangerous if used or controlled by cybercriminals. We have conducted a special investigation into this problem and will publish the results in the near future.

Threat statistics

All statistical data used in this report was collected using the Kaspersky Security Network (KSN), a distributed antivirus network. The data was received from those KSN users who gave their consent to have data anonymously transferred from their computers. We do not identify the specific companies/organizations sending statistics to KSN, due to the product limitations and regulatory restrictions.

Methodology

The data was received from ICS computers protected by Kaspersky Lab products that Kaspersky Lab 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).

The statistics analyzed also include data received from computers of industrial control network administrators and software developers who develop software for industrial automation systems.

For the purposes of this report, attacked computers are those on which our security solutions have been triggered at least once during the reporting period. When determining percentages of machines attacked, we use the ratio of *unique* computers attacked to all computers in our sample from which we received anonymized information during the reporting period.

ICS servers and stationary workstations of engineers and operators often do not have full-time direct internet access due to restrictions specific to industrial networks. Internet access may be provided to such computers, for example, during maintenance periods.

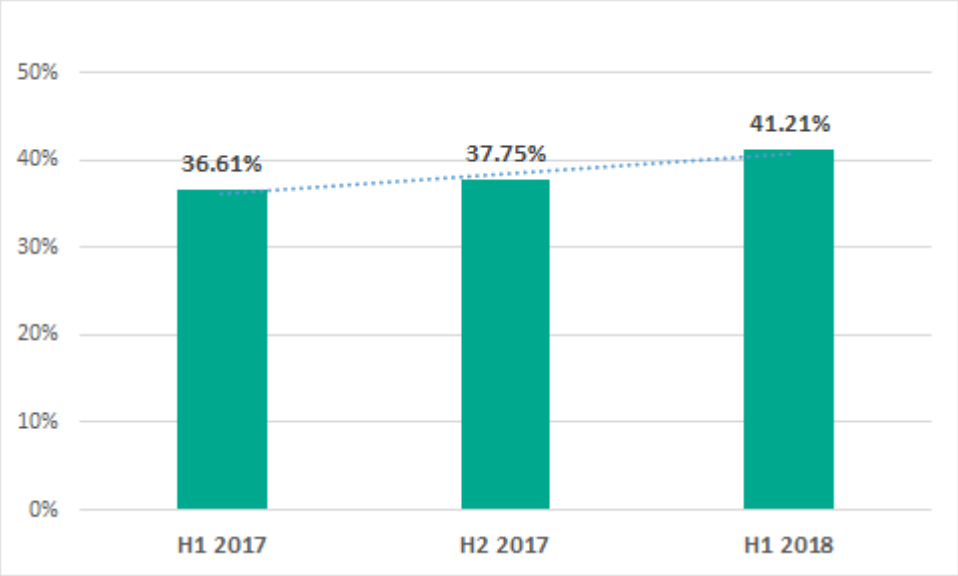
Workstations of system/network administrators, engineers, developers and integrators of industrial automation systems may have frequent or even full-time internet connections.

As a result, in our sample of computers categorized by Kaspersky Lab ICS CERT as part of the industrial infrastructure of organizations, about 42% of all machines had regular or full-time internet connections in H1 2018. The remaining machines connected to the Internet no more than once a month, many much less frequently than that.

Percentage of ICS computers attacked

The percentage of ICS computers attacked in H1 2018 increased by 3.5 p.p. compared with H2 2017 and reached **41.2%.** The year-over-year increase was 4.6 p.p.

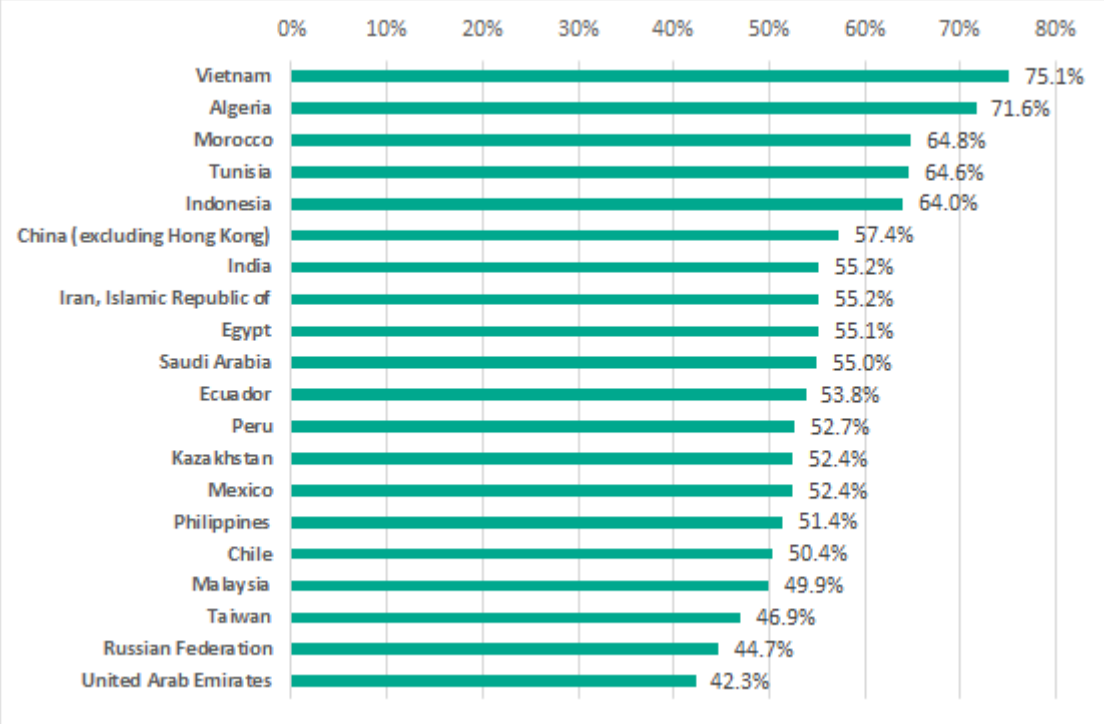
Percentage of ICS computers attacked



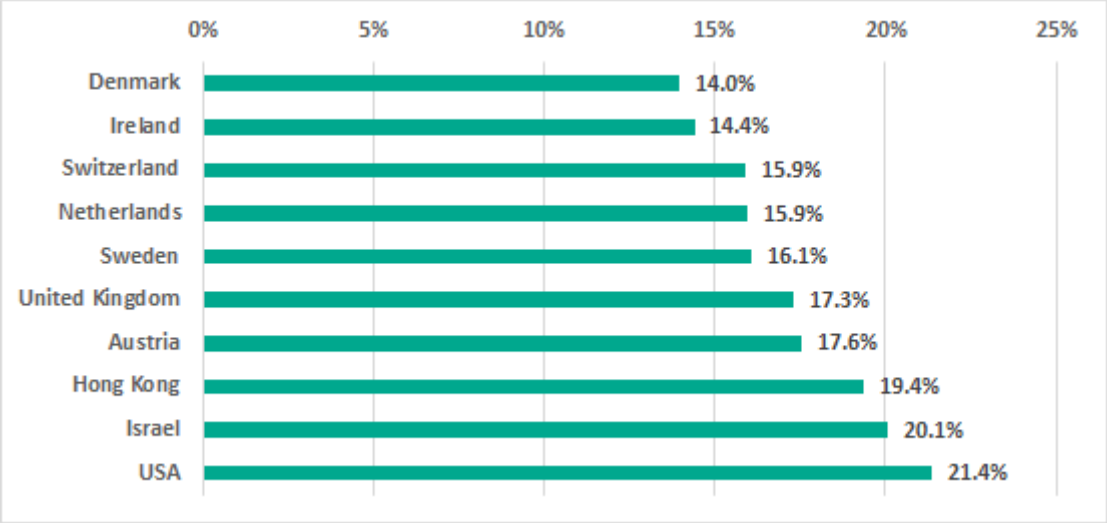
The increase in the percentage of ICS computers attacked was due primarily to the overall increase in malicious activity.

Geographical distribution

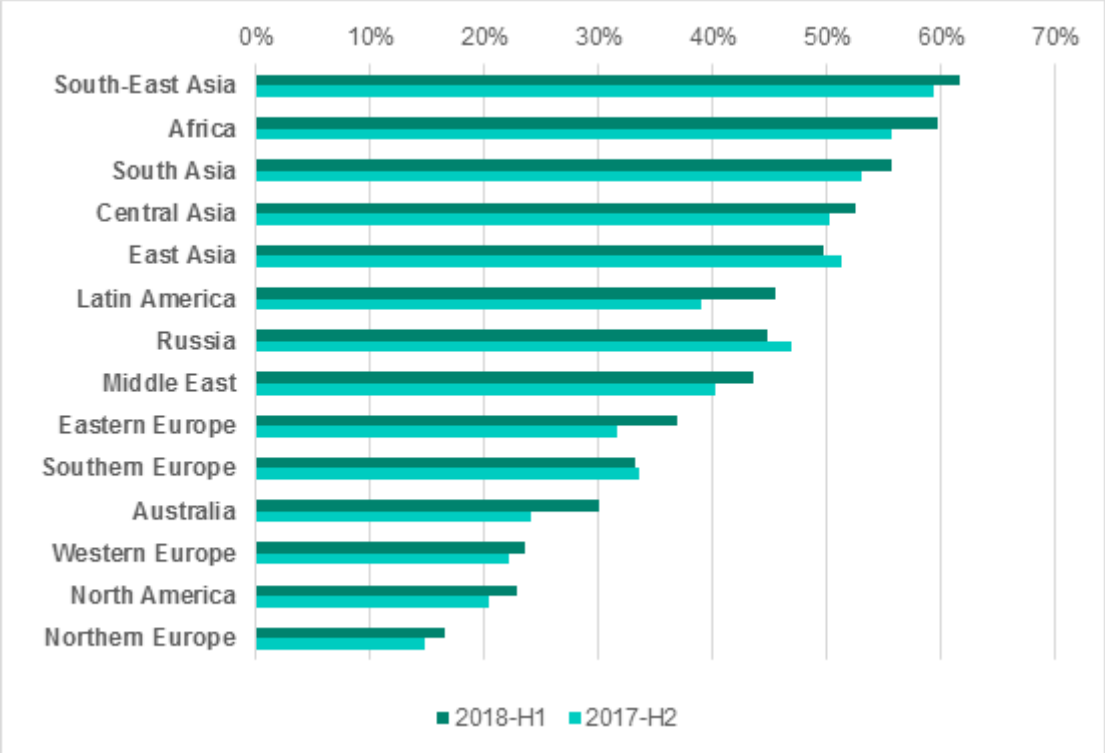
TOP 20 countries by percentage of ICS computers attacked, H1 2018



10 countries with the lowest percentages of ICS computers attacked, H1 2018



Percentage of ICS systems attacked in regions of the world, H1 2018 vs H2 2017



A comparison between different regions of the world shows that:

- countries in Africa, Asia and Latin America are significantly worse off in terms of the percentage of ICS computers attacked than countries in Europe, North America and Australia;
- the figures for Eastern Europe are considerably greater than those for Western Europe;
- the percentage of ICS computers attacked in Southern Europe is higher than that in Northern and Western Europe.

Presumably, this situation could be due to the amounts of funds invested by organizations in infrastructure protection solutions. According to IDC, from a geographic perspective, the US and Western Europe were the largest markets for information security products in 2017.

Within geographical regions, the figures can vary significantly between different countries. For example, the situation in South Africa is the most favorable compared to most African countries, and Israel and Kuwait are noticeably better off than other countries in the Middle East.

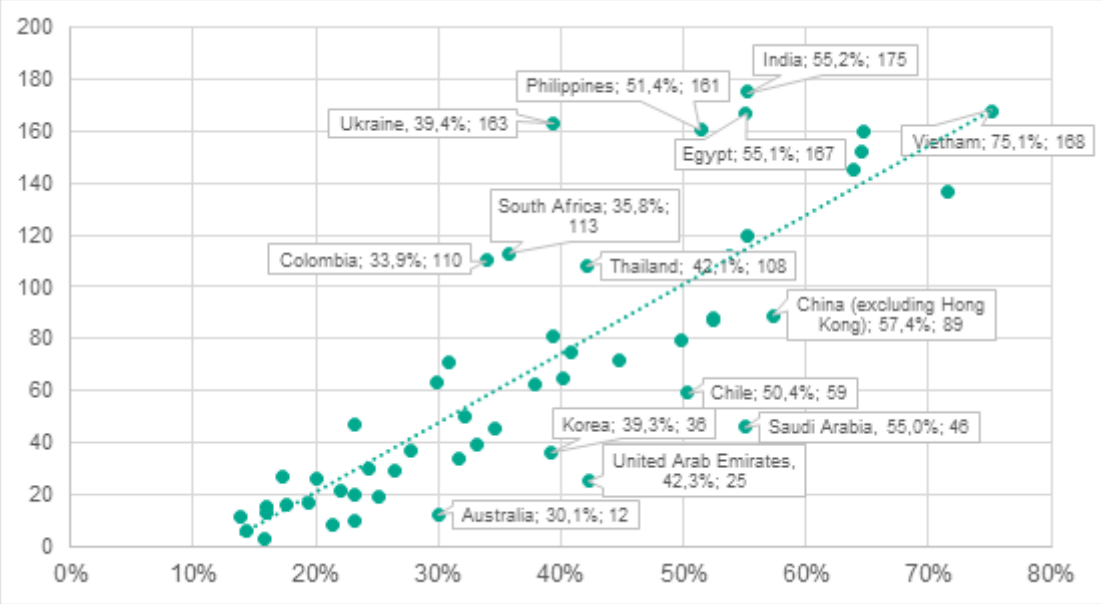
Factors affecting the cybersecurity of ICS computers

As we can see, there are significant variations between different countries of the world – from 14 to 75 percent of ICS computers attacked. We believe that such substantial differences could be explained by the overall level of development in different countries and differences in the cybersecurity levels, as well as the levels of malicious activity in different countries.

Notably, all countries that, based on our data, had minimal percentages of ICS computers attacked, were classified by the International Monetary Fund as advanced economies. In addition, six of the ten countries that had the lowest percentage of ICS computers attacked – the US, the UK, the Netherlands, Sweden, Switzerland, and Israel – were among the TOP 20 countries according to Global Cybersecurity Index 2017 developed by the International Telecommunication Union (ITU).

An analysis which matched the percentage of ICS computers attacked in each country to that country's position in the per capita GDP ranking demonstrated that there is a high positive correlation between these two parameters (multiple correlation coefficient R=0.84 and significance coefficient P<0.001). With some exceptions, countries with high per capita GDP levels (i.e., those in high positions in the ranking) had a lower percentage of ICS computers attacked than countries with low per capita GDP levels.

Percentage of ICS computers attacked in each country (axis X) vs the country's position in the per capita GDP ranking (axis Y)



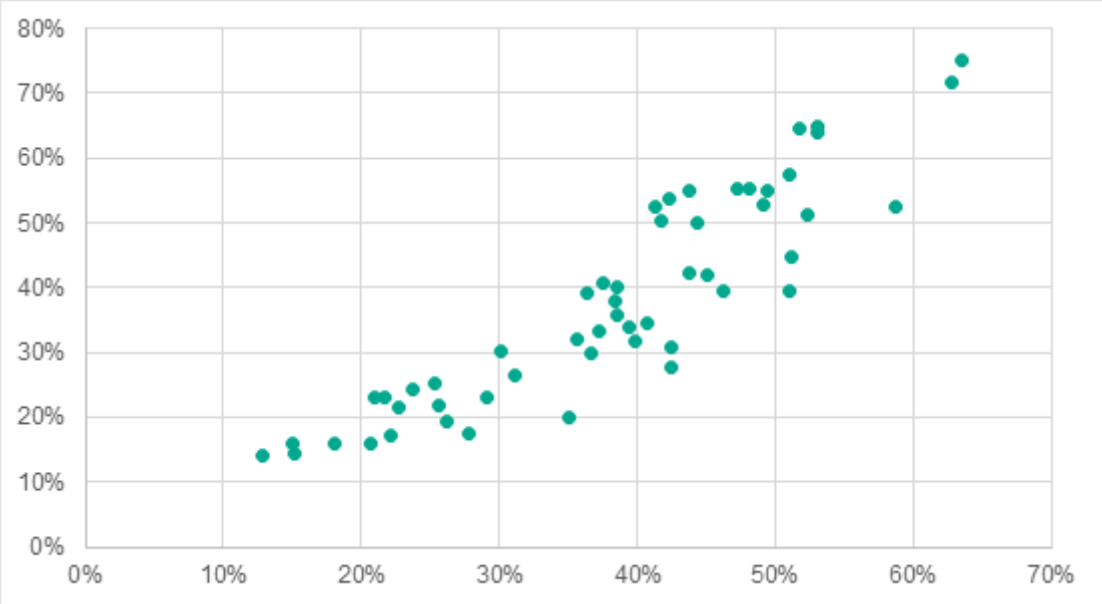
Seven of the ten countries with the highest percentage of ICS computers attacked in 2017 were not among the top 100 countries by per capita GDP levels.

The high percentages of ICS computers attacked in developing countries could have to do with these countries having had industrial sectors for a relatively short time only. It is well known that, when designing and commissioning industrial facilities, the main focus is often on the economic aspects of their operation and the physical safety of the industrial process, while information security is much lower on the list of priorities.

The few examples picked out on the graph possibly show some of the countries which spend available resources more (above the dotted line) or less (below the dotted line) efficiently than others to protect their industrial assets from cyberattacks.

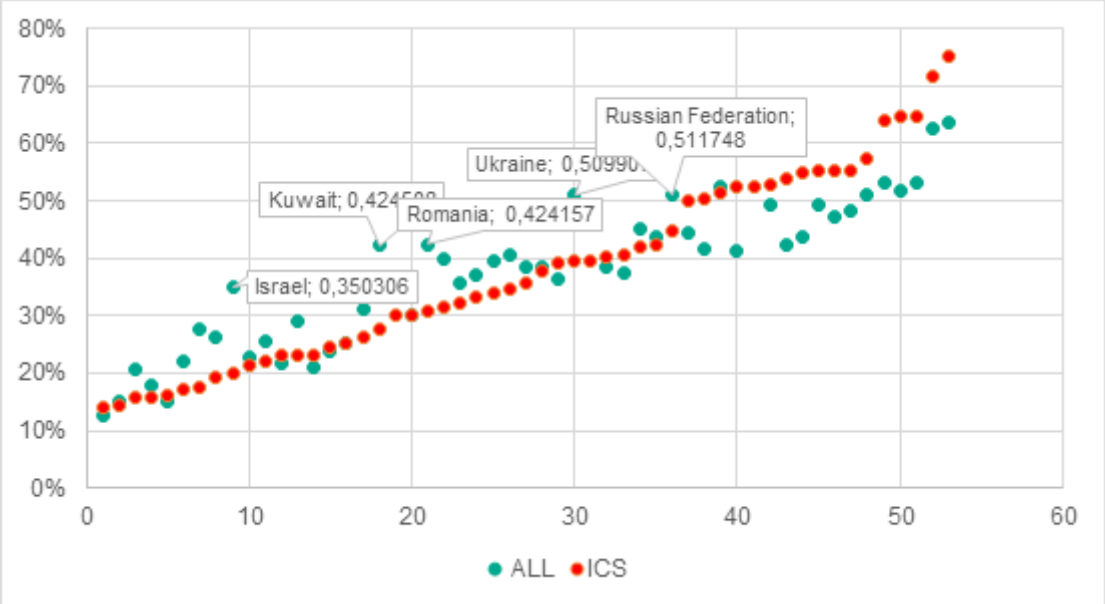
To evaluate the levels of malicious activity in different countries, we calculated the percentage of all computers (home, corporate and ICS computers) attacked in each country. We found that there was a high positive correlation (with multiple correlation coefficient R = 0.89 and significance coefficient P < 0.001) between the percentage of ICS computers attacked in a country and malware activity in that country (measured as the percentage of all computers attacked).

Percentage of all computers attacked in each country (axis X) vs percentage of ICS computers attacked (axis Y), H1 2018



This data is consistent with the assumption that computers in the industrial network infrastructure that are connected to the corporate network and/or connect to the internet, even occasionally, are in most cases affected by malware attacks to the same extent as such traditional cyberattack targets as office computers of organizations and individuals in the same country.

Percentage of all computers attacked in each country and percentage of ICS computers attacked in each country, H1 2018



It should be noted that in nearly all of the countries where at least one half of all ICS computers were attacked during the six months (the TOP 20 of our ranking), the percentage of machines attacked in the industrial network infrastructure was higher than the overall percentage of computers attacked in these countries. This situation is particularly disturbing, given that, according to World Bank and Organization for Economic Co-operation and Development data, eight countries from this list – Indonesia, China, India, Iran, Saudi Arabia, Mexico, the Philippines and Malaysia – were also among the TOP 30 countries by industrial output in 2017.

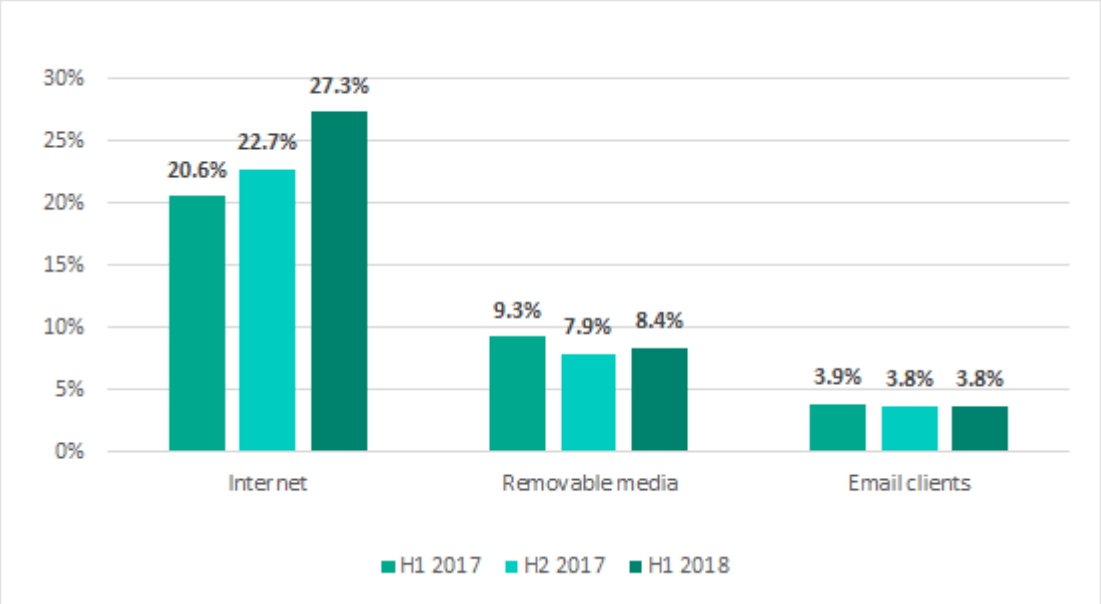
Main sources of infection

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

In the past years the internet became the main source of infection for computers on organizations' industrial networks. Moreover, we have observed increases in the percentage of ICS computers on which phishing emails and malicious attachments opened in online email services using the browser, as well as attempts to download malware from the internet and to access known malicious and phishing web resources, were detected.

While a year ago, in H1 2017, the internet was the source of threats blocked on 20.6% of ICS computers from which we receive anonymized statistics, in H1 2018 the figure was as high as 27.3%.

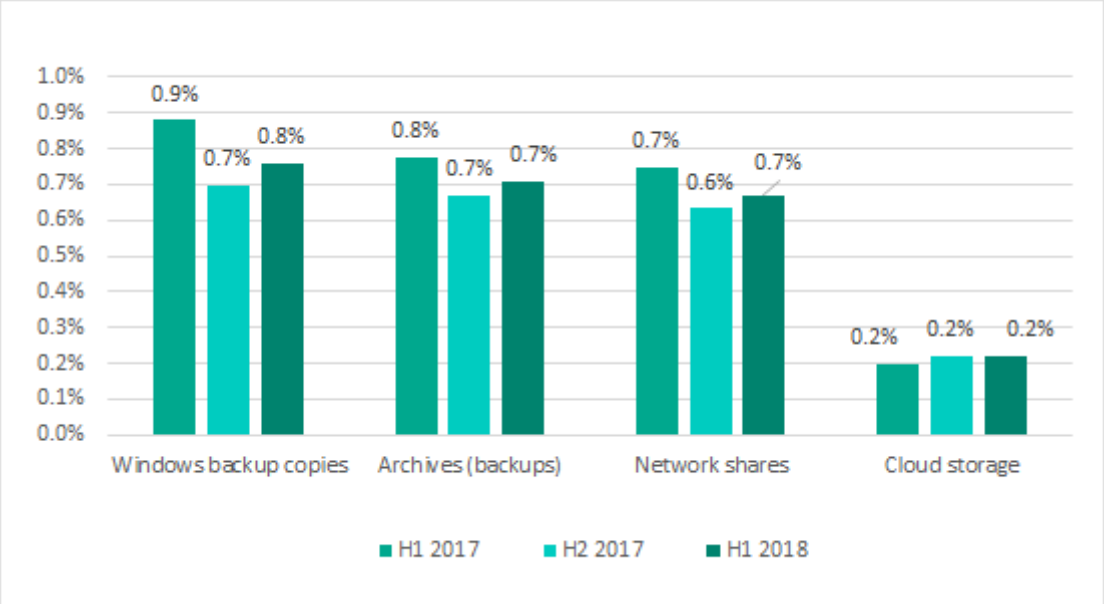
Main sources of threats blocked on ICS computers (percentage of computers attacked during half-year periods)



This pattern seems logical: modern industrial networks can hardly be considered isolated from external systems. Today, an interface between the industrial network and the corporate network is needed both to control industrial processes and to provide administration for industrial networks and systems. The ability to access the internet from the industrial network can be a forced necessity – it could be required, for example, by employees of contractor organizations to provide maintenance and technical support for industrial automation systems. The computers of contractors, developers, integrators, and system/network administrators, who connect to the industrial network of a customer enterprise from the outside (directly or remotely) and often have unrestricted access to the internet, can also be one of the channels used by malware to infect an industrial network. Another such channel can be created by connecting computers on the industrial network to the internet via mobile phone operators' networks (using mobile phones, USB modems and/or Wi-Fi routers with 3G/LTE support). The second and third most common sources of industrial network infection were removable media and email clients, respectively. The figures for these sources of infection did not change significantly during H1 2018.

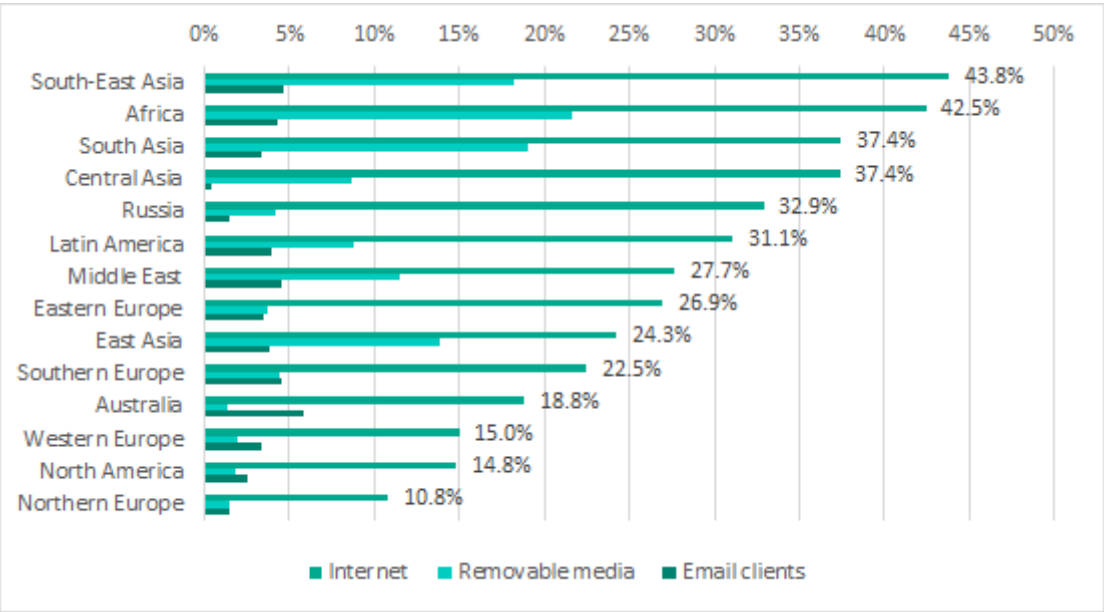
The contribution of other sources of infection did not exceed 1% for any of the sources and remained at the levels demonstrated in the previous six months.

Minor sources of threats blocked on ICS computers (percentage of all ICS computers attacked during six-month periods)



Main sources of ICS computer infections by region

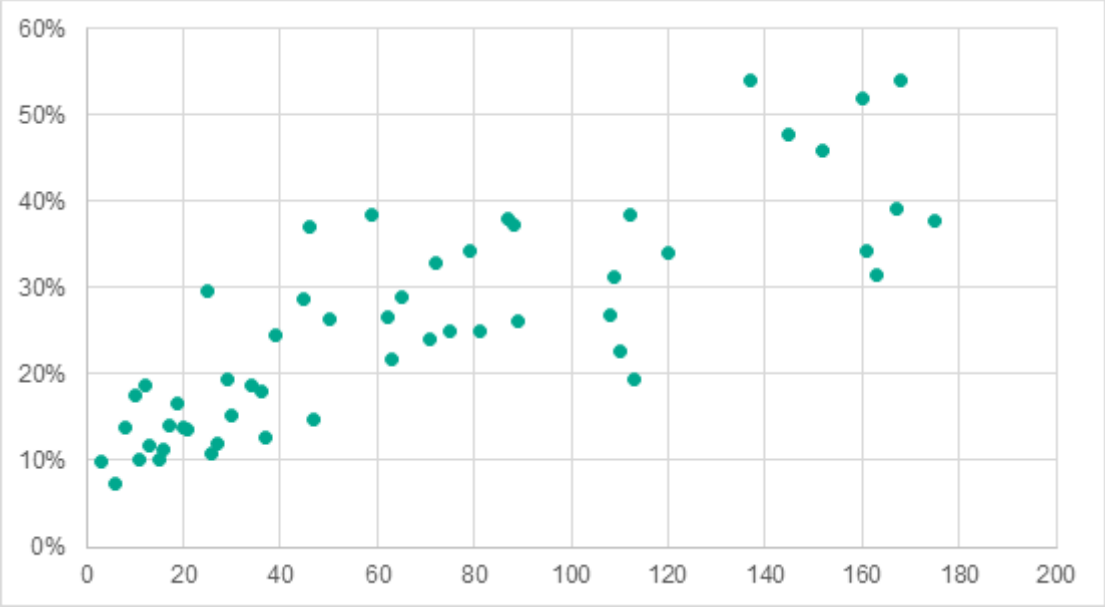
Main sources of threats blocked on ICS computers by region, H1 2018



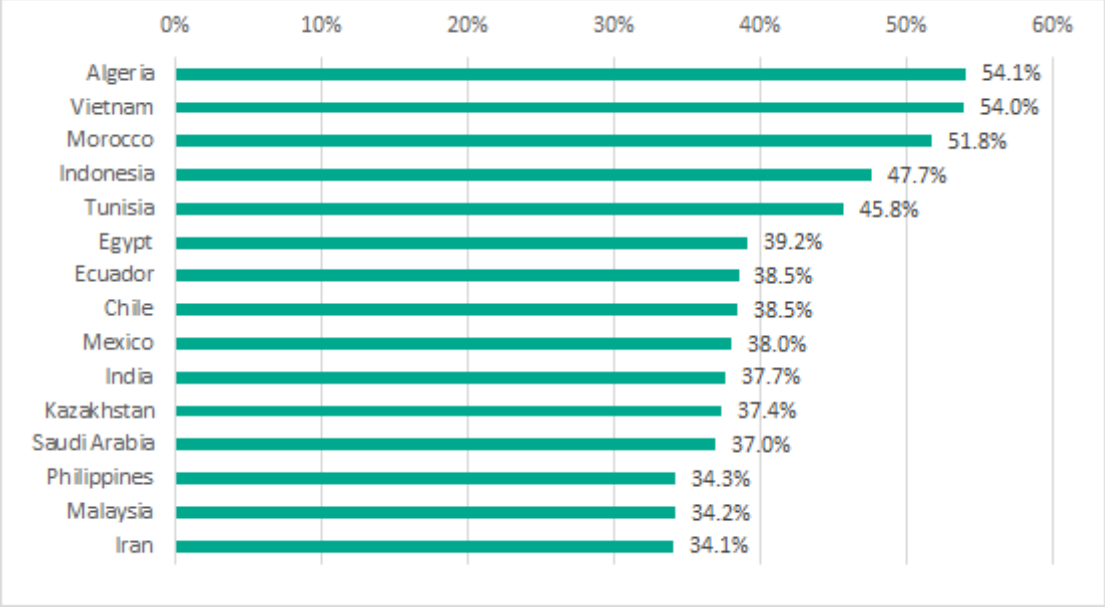
Internet

Since the internet is the main source of attacks on ICS computers, it stands to reason that, as in the case of all ICS computers attacked, there is a correlation between the per capita GDP level and the percentage of ICS computers on which internet-borne threats were blocked in different countries (multiple correlation coefficient R = 0.82, significance coefficient P<0.001).

Positions of different counties in the per capita GDP ranking (axis X) vs percentages of ICS computers attacked by internet threats in these countries (axis Y)



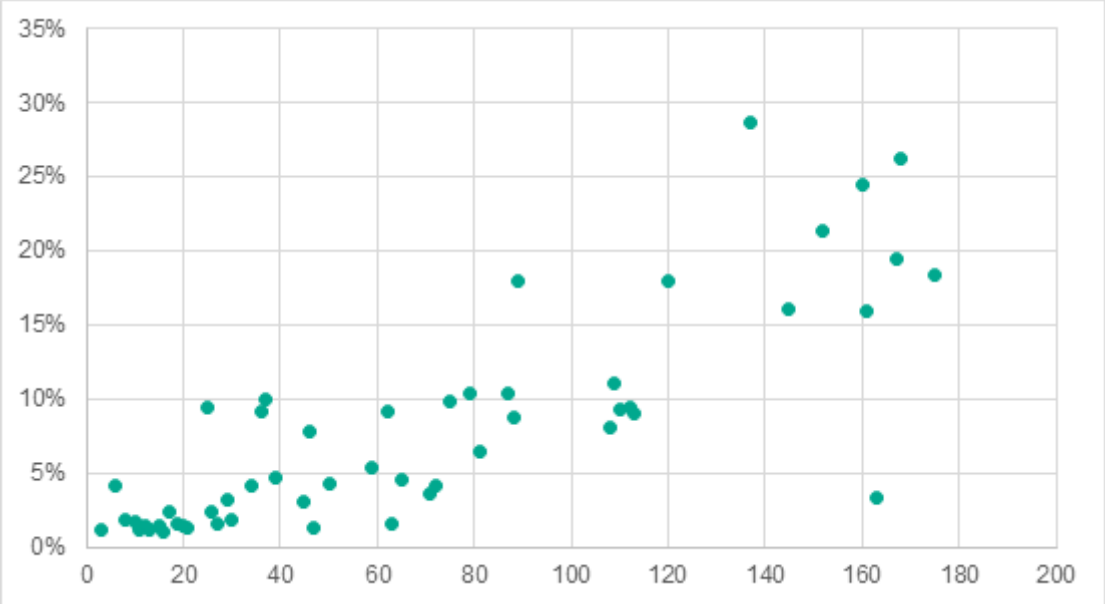
TOP 15 countries based on the percentage of ICS computers on which internet threats were blocked, H1 2018



Removable media

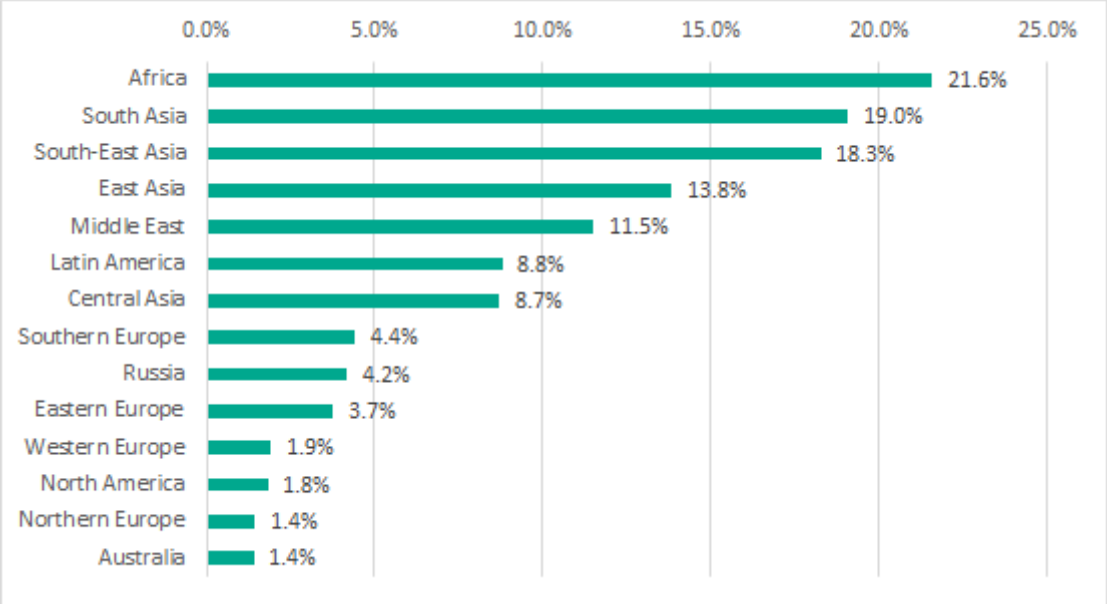
In the case of threats that spread via removable media, the situation is similar, with some exceptions, to internet threats: in countries with low per capita GDP levels, the percentage of ICS computers attacked from removable media was higher (multiple correlation coefficient R=0.82, significance coefficient P< 0.001).

Positions of countries in the per capita GDP ranking (axis X) vs percentage of ICS computers in these countries attacked by threats from removable media (axis Y)



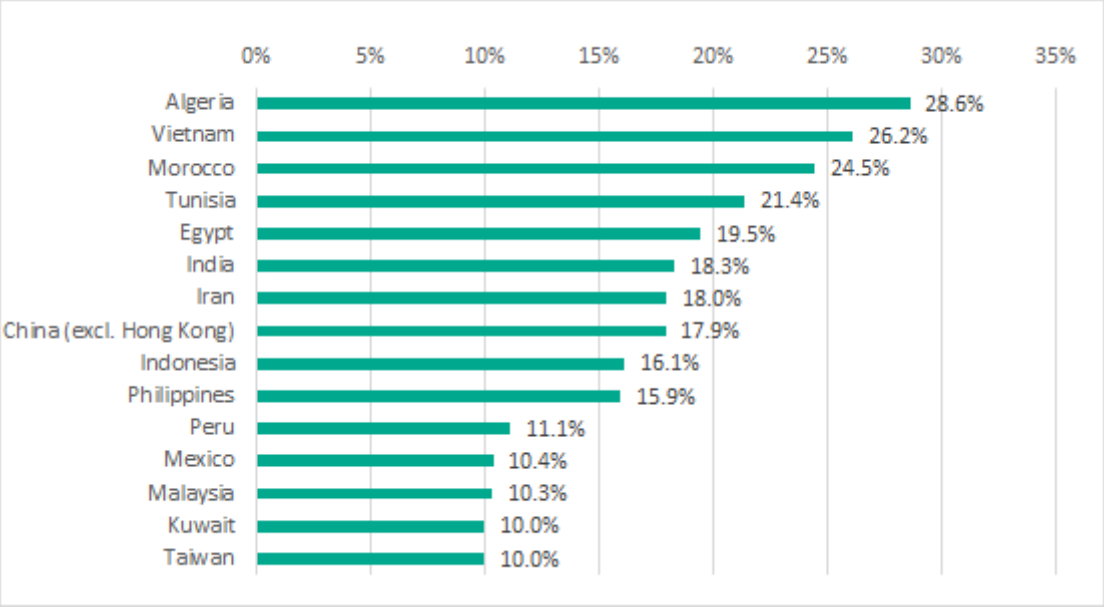
This largely defined the ranking of regions by percentage of computers attacked from removable media.

Ranking of regions by percentage of ICS computers attacked via removable media, H1 2018



The highest percentage of ICS computers attacked via removable media was recorded in Africa, the Middle East and South-East Asia. This could indicate that removable media are widely used in these regions to transfer information between ICS computers, which, in combination with the relatively low overall level of cyberthreats, determined the high percentage of ICS computers attacked. On the other side of the spectrum, this percentage was lowest in Western Europe and North America. We believe that this could be due to the higher overall level of security measures, as well as the less extensive use of removable media.

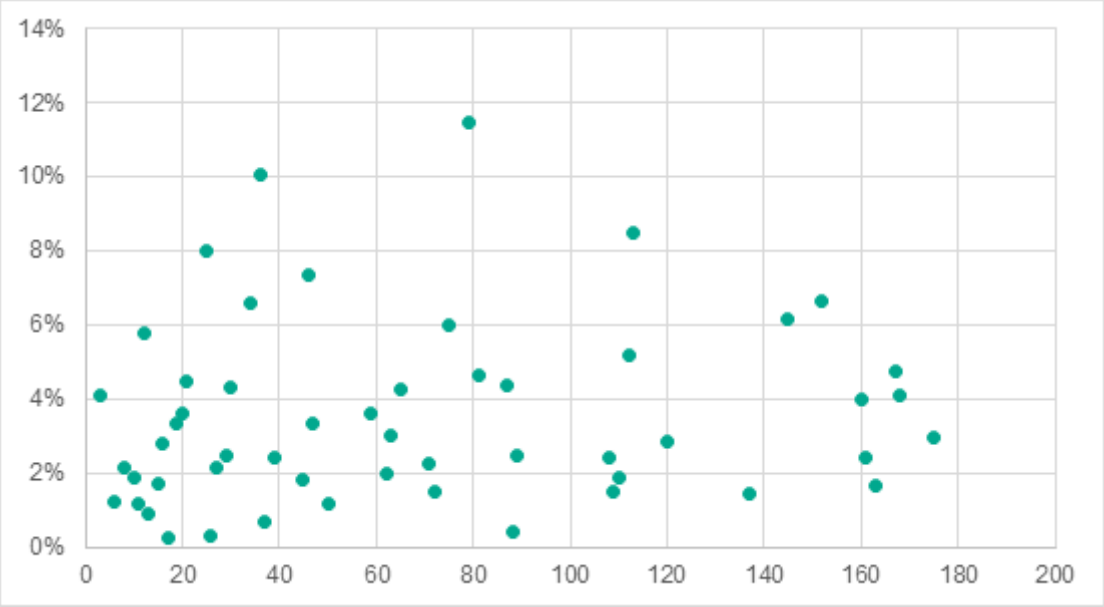
TOP 15 countries by percentage of ICS computers attacked through removable media, H1 2018



Email clients

Curiously, the situation with email-borne threats is different: there is no correlation between the percentage of ICS computers attacked through email clients and the per capita GDP level.

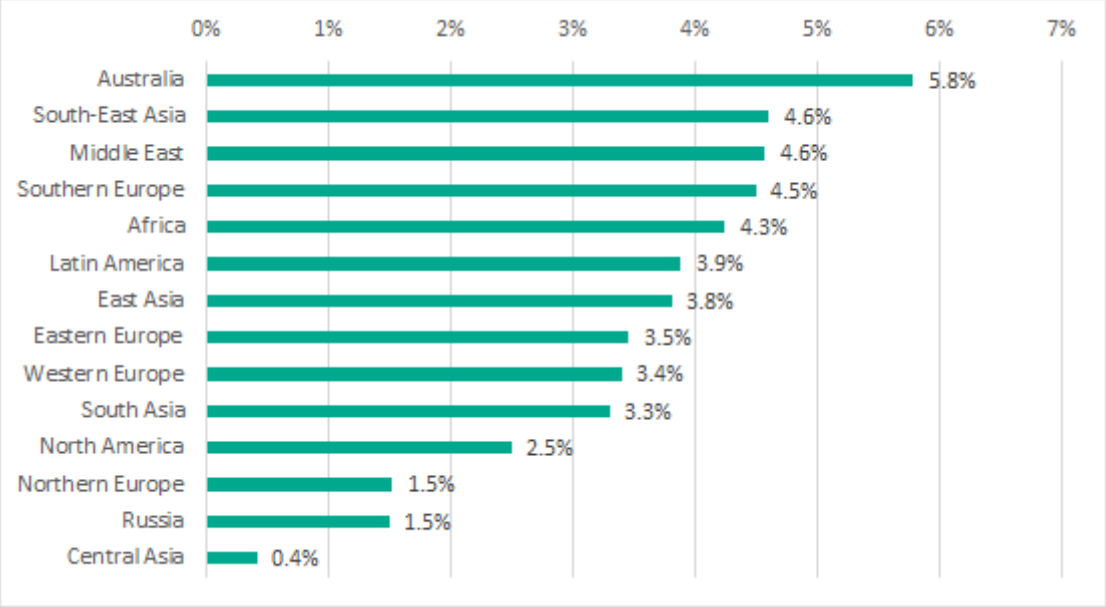
Position of each country in the per capita GDP ranking (axis X) vs percentage of ICS computers in the country attacked through email clients (axis Y)



This means that, if the assumption that a high overall level of information security is characteristic of countries with high per capita GDP levels, this does not help to combat email-borne attacks. That is, the information security level has virtually no effect on the number of phishing emails and malicious email attachments that get through protection at the network perimeter and reach ICS computers. A possible explanation is that, irrespective of the overall level of cybersecurity at an enterprise, effective tools designed to protect from email-borne attacks are either not used on the network perimeter or not properly configured.

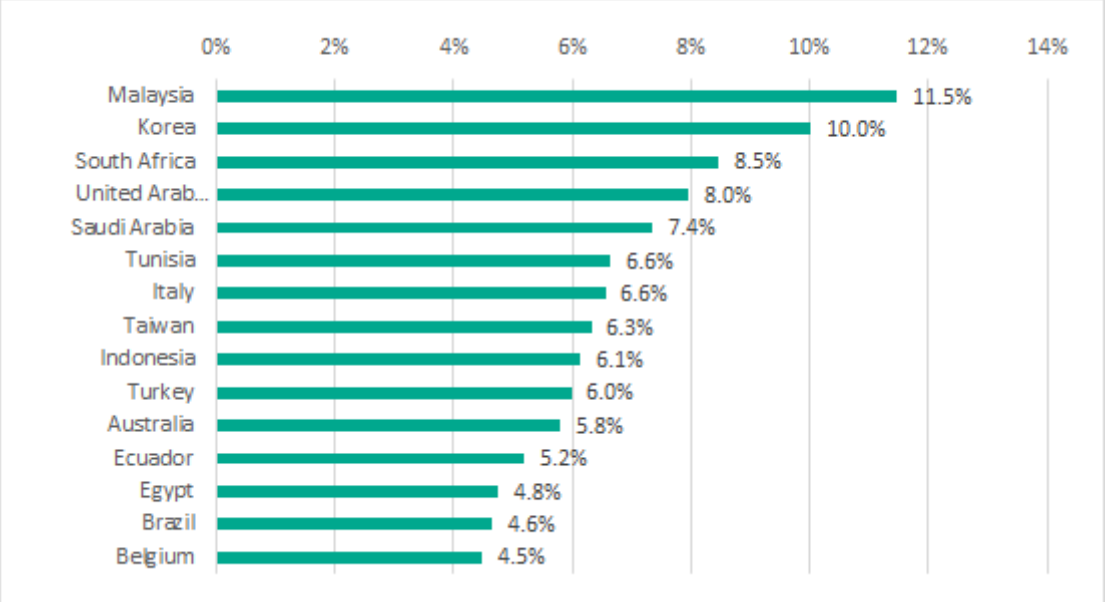
The ranking of regions by percentage of ICS computers attacked through email clients does not show a wide range of values. Australia, which does relatively well in other respects, is at the top of the ranking, while the figures for most other regions are in the range from 2.5 to 4.6 percent.

Ranking of regions by percentage of ICS computers attacked through email clients, H1 2018



It should be noted that Australia is only in 11th place in the ranking of *countries* by percentage of ICS computers attacked through email clients. Curiously, the 15 countries with the worst situation in terms of email-borne attacks include Belgium, which does well based on other criteria, as well as Italy and South Africa, which are also relatively well off in other respects.

TOP 15 countries by percentage of ICS computers attacked through email clients, H1 2018



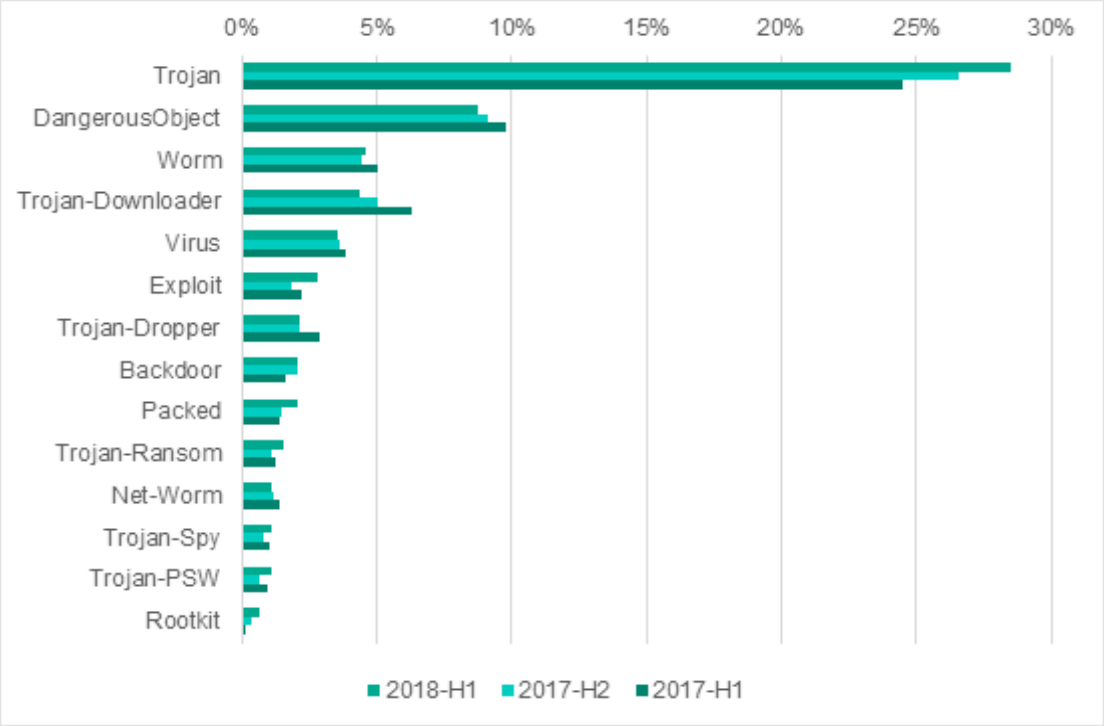
We believe that these observations should be treated with particular care, because emails are often used in targeted attacks on industrial enterprises. We wrote about some such campaigns here and here.

Malware on industrial automation systems

In H1 2018, Kaspersky Lab security solutions installed on industrial automation systems detected over 19.4 thousand malware modifications from 2.8 thousand different malware families.

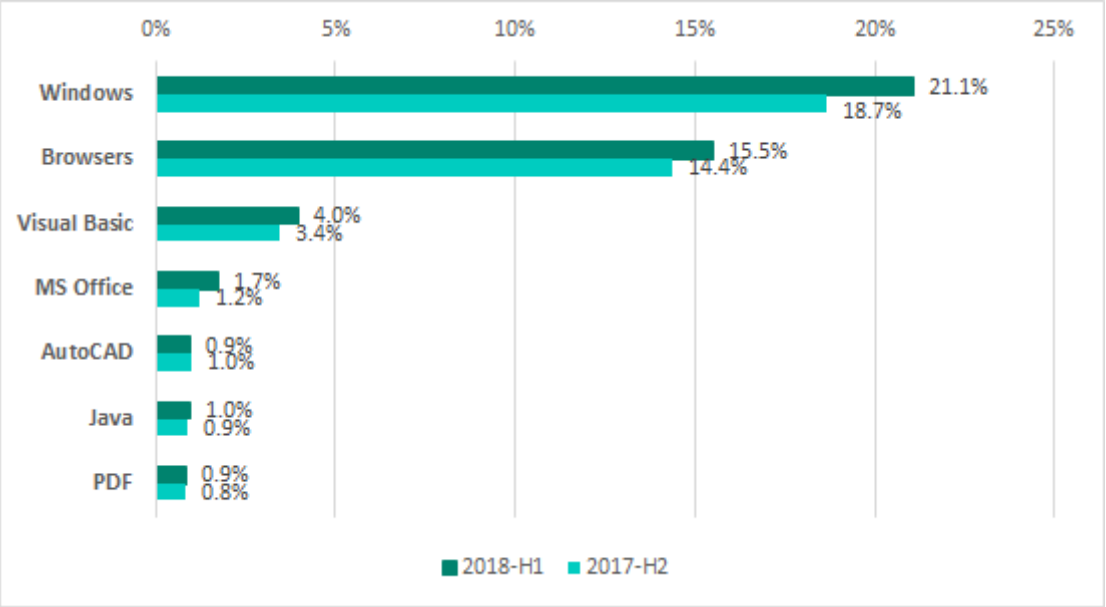
As before, attempts to infect ICS computers were, in most cases, random attacks rather than parts of targeted attacks.

Malware classes, percentage of ICS computers attacked, H1 2018



Platforms used by malware

Main platforms used by malware, percentage of ICS computers attacked, H1 2018 vs H2 2017



In the diagram above:

- the Windows platform includes all threats for x86 and x64;
- the Browsers platform includes all threats that attack browsers, as well as malicious HTML pages;
- the Microsoft Office platform includes all threats that target the relevant software (Word, Excel, PowerPoint, Visio, etc.).

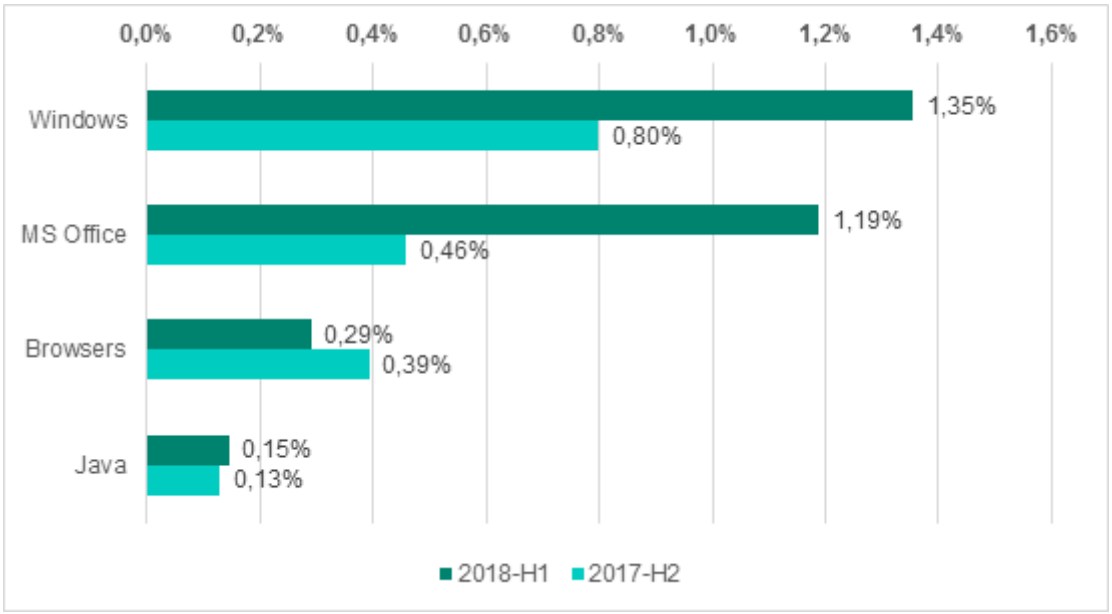
In H1 2018, threat actors continued to attack legitimate websites that had vulnerabilities in their web applications in order to host malware components on these websites. Notably, the increase in the percentage of ICS computers attacked through browsers in H1 2018 was due to the increase in the number of attacks that involved JavaScript cryptocurrency miners.

At the same time, the increase in the number of ICS computers attacked using Microsoft Office documents (Word, Excel, RTF, PowerPoint, Visio, etc.) was associated with waves of phishing emails. In most cases, malicious Microsoft Office documents attached to such emails contain exploits designed to infect computers with various spyware. Users who are unaware of the threat often forward infected office documents to their colleagues, transfer such documents via removable drives and shared folders, helping the malware to spread. This is why it is extremely desirable to restrict the use of office software Microsoft Office, PDF, etc.) on ICS computers.

Exploits

The percentage of ICS computers on which attempts to use exploits were blocked grew by 1 p.p., reaching 2.8%.

Types of applications attacked by exploits, percentage of ICS computers attacked



It should be noted that attackers often use downloaders written in Visual Basic Script as exploit payload or embed them directly into office documents. Such scripts can only be executed if the Windows Script Host (WSH) is installed on the system. It is usually installed by default during the installation of Windows. This means that to protect the system from malware written in Visual Basic Script, WSH should be disabled in the Windows Registry, unless it is required for the industrial control system's operation. This also applies to malicious code

written in Java: if Java Runtime is not required for the industrial control system's operation, it is recommended to refrain from using it in order to reduce the risk of infection.

The ShadowBrokers exploits that were leaked in March 2017 and were used in attacks of WannaCry and ExPetr encryption malware, were also utilized in H1 2018 as part of various malicious programs. An increase in the number of attacks involving these exploits was the reason behind the increase in the percentage of ICS computers attacked using malware and exploits for Windows x86 and x64.

Spyware

The percentage of ICS computers attacked by spyware (Trojan Spy and Trojan PSW), grew by 0.4 p.p.

Spyware is often distributed via phishing emails. One prominent example is South Korea, which ranked highest based on the percentage of ICS computers on which spyware was blocked. The figure for Korea was 6%. Most spyware in that country was distributed in phishing emails targeting specifically users in the Asia-Pacific region.

Notably, most such phishing emails are very similar to each other (they use similar headings/message text/file names) in different regions of the world, with the exception of Asia, where phishing emails have a more pronounced "Asian" flavor: all industrial companies mentioned in emails targeting Asian users are located in Asia.

It should also be noted that Korea is in third place based on backdoor attacks, which were blocked on 6.4% of ICS computers. The top position in that ranking is taken by Vietnam with an impressive 9.8%.

Our recommendations

We recommend taking a range of information security measures to address the threats described in this report.

The proposed security measures are listed in the diminishing order of importance to implementation difficulty ratio, based on the experience of our experts.

This list is not meant to be exhaustive. We developed it with a view to addressing the industrial enterprise and industrial automation system information security issues that we identified and analyzed as part of our research conducted during the reporting period.

Specifically, these recommendations do not include such measures as configuring the firewall to block connections from outside the industrial network over protocols that are used to automate the industrial process or blocking direct connections to hosts on the industrial network from the internet. This is because, based on the results of industrial network audits and penetration tests that we have conducted at industrial enterprises, we believe that the vast majority of organizations already have such measures in place.

Measures that require no organizational changes, additional personnel, adjustments to business or industrial processes, or significant changes to information systems

We believe that these measures can help to make the first step towards securing the enterprise's industrial facilities. We also believe that they are applicable to most organizations, regardless of the maturity level of their information security processes.

1. Use antivirus protection to protect all hosts on the industrial network from malware attacks.
   - Check that all the main protection components are enabled and running.
   - Avoid excluding folders containing ICS software, OS system folders or user profiles from protection scope.
   - If possible, avoid using any exclusions from scanning at all.
   - Ensure that antivirus databases are updated at least once every 24 hours. If possible, the databases should be updated in accordance with the recommendations provided by the security solution's vendor.
   - Check that the security solution is configured to scan removable media automatically when they are connected to the host.
   - If possible, configure up-to-date verdicts to be received from the vendor's antimalware cloud without delay.

2. Configure rules on firewalls installed on the industrial network's boundary.
   - Block requests to services that provide remote access to file system objects, such as SMB/CIFS and/or NFS (applicable to attacks on systems that run Linux).
   - Configure rules to control the use of remote administration tools. Create a whitelist of addresses from which access to systems on the industrial network is allowed. Ensure that the whitelist includes only the addresses of trusted resources and excludes administration tool vendors' cloud infrastructures and other untrusted and unknown addresses.
   - Block external email services from being used inside the industrial network.
   - Block external HTTP/HTTPS email services.
   - Block social networks.
   - Block cloud-based file storage services.
   - Block torrents.

3. Configure protection from spam and phishing emails inside the corporate network and on its boundary.
   - Ensure that antispam and anti-phishing protection is updated with the frequency recommended by the vendor.
   - If possible, configure a connection to the vendor's cloud service that serves verdicts without delay.
4. Configure antivirus protection on the organization's network perimeter and control of connections to malicious and potentially unwanted online resources.
5. Audit the use of email on the industrial network.
   - Use antivirus protection to block external email services on computers that are part of the industrial network.
   - To the extent possible, block corporate email on the industrial network, remove any email clients installed or use application startup control tools to block them from running.
   - Disable the "mailto" service.
6. Audit the use of network shared folders on the industrial network.
   - Disconnect all network shared folders, unless they are required by the industrial process.
   - Disconnect services that provide remote access to the file system, including SMB/CIFS and NFS, where they are not required by the industrial process.
7. Audit the use of third party remote administration tools on the industrial network, such as VNC, RDP, TeamViewer RMS/Remote Utilities. Remove all remote administration tools that are not required by the industrial process.
8. Disable remote administration tools supplied as part of the ICS software (for detailed instructions, consult the documentation for the relevant software), unless they are required by the industrial process.
9. Audit the use of other software on the industrial network that significantly increases the ICS attack surface. Uninstall any such software, provided that it is not required by the industrial process. A special emphasis should be made on the following types of software:
   - Web browsers
   - Social networking clients
   - Email clients
   - Microsoft Office software
   - Adobe software
   - Java Runtime
   - Media players
   - Script interpreters such as Perl, Python, PHP
   - Unlicenced "cracked" software – such software often includes backdoors or is infected with malware
10. Disable the Windows Script Host, provided that it is not required for the industrial control system's operation and is not otherwise required by the industrial process.
11. If possible, use Windows domain group policies to restrict the use of SeDebugPrivilege privileges by local administrators of systems on the industrial network (such privileges may be required by some software products, such as the Microsoft SQL Server – consult the documentation provided by vendors of the respective systems).

Measures designed for organizations with a high level of information security maturity

Applying these measures in insufficiently mature organizations could require spending significant amounts of time or resources, organizing new cybersecurity processes, making staffing changes, and could involve other complications.

1. Establish the process of training the enterprise's staff in cyber-hygiene.
   - Organize cybersecurity training courses for employees to increase their awareness of modern threats, including their targets, techniques, scenarios of attacks on industrial organizations, the dangers posed by attacks to business and industrial processes, methods of protection against attacks and incident prevention.
   - Organize regular training on cyberthreats and methods of protection against them with an emphasis on changes in the threat landscape, as well as training for new employees. Consider using training platforms (online or deployed at the enterprise), webinars, and recorded versions of earlier training sessions to make training more accessible to the enterprise's employees.
   - Implement the practice of holding short staff briefings on protection against cyberthreats.
   - Provide employees of the enterprise with information materials reminding them about the need for protection against cyberthreats, including posters, brochures, etc.
   - Organize regular cybersecurity drills and employee knowledge reviews in this area.
2. Set up an industrial information security and cyberdefence service.
   - Appoint an officer responsible for the cyberprotection of information systems on the industrial network.
   - Make protection of the industrial network an integral part of the overall information security assurance process at the enterprise.
   - Organize the work of various horizontal and vertical divisions and services in the organization, including engineers, operators, IT, and IS, to provide effective protection from cyberattacks.
   - Establish effective communications on cybersecurity issues with vendors of automation systems and security solutions.
   - Establish an information security incident response procedure on the industrial network.
3. Introduce the practice of regularly auditing the information security status of information systems on the industrial network.
   - Take an inventory of running network services on all hosts of the industrial network; where possible, stop (or, preferably, disable / remove) vulnerable network services (unless this will jeopardize the continuity of the industrial process) and other services that are not directly required for the operation of the automation system. Special emphasis should be made on the following services: SMB/CIFS, NBNS, LLMNR.
   - Audit privilege separation for ICS components, trying to achieve maximum access granularity.
   - Audit the network activity in the industrial network and on its boundaries. Eliminate any network connections with external and other adjacent information networks that are not required by the industrial process.
   - Audit the security of remote access to the industrial network; place a special emphasis on whether demilitarized zones are set up in compliance with IT security requirements.

- Audit policies and practices related to using removable media and portable devices. Block devices that provide illegitimate access to external networks and the internet from connecting to industrial network hosts. Wherever possible, disable the relevant ports or control access to them using properly configured specialized tools.
- Audit accounts and the password policy. User and service accounts should have only those privileges which are required for the proper operation of the facility. The number of user accounts with administrative privileges should be as limited as possible. Strong passwords should be used (at least 9 characters long, both upper and lower case, combined with digits and special characters; passwords should not include dictionary words), with regular password changing enforced by the domain policy, for example, every 90 days. Wherever possible, insecure authentication algorithms, such as NTLM, should be replaced with the more secure NTLMv2 and Kerberos.

4. Establish a procedure for fixing any security vulnerabilities in systems that are part of the industrial network in a timely manner.
   - Gain access to sources of information on vulnerabilities identified in ICS products, network devices and common components, set up a procedure for processing and analyzing such information.
   - Implement a procedure for regularly scanning systems deployed on the industrial network and on its perimeter for vulnerabilities. Consider deploying dedicated tools designed to detect vulnerabilities in systems that are part of the industrial network.
   - Regularly update the operating systems, application software and security solutions on systems that are part of the industrial network.
   - Install firmware updates on devices used in industrial automation systems and safety instrumented systems in a timely manner.

5. Use specialized technologies listed below to implement automatic protection. As a rule, this requires fine-tuning, careful testing and highly developed information security incident monitoring and response procedures:
   - Configure application startup control in whitelisting mode (usually this functionality is included in antimalware solutions for industrial network hosts). Where this is impossible, configure application startup control in monitoring mode, with notifications sent to the employee responsible for information security.
   - Deploy dedicated tools (they can be part of solutions that provide antivirus protection for industrial network hosts) for ensuring the integrity of computers, including critical areas and the configuration of the operating system and application software, particularly ICS software. Where this is not possible, configure integrity control in monitoring mode with notifications sent to the employee responsible for information security.
   - Configure external device connection control (for USB drives, mobile phones, etc.).
   - Enable the Host-based Intrusion Prevention System (HIPS) components included in the antivirus solution.
   - Deploy automatic tools to take the inventory of devices connected to the industrial network and control new device connections. This requires engaging highly qualified specialists to monitor and respond to any incidents detected.
   - Deploy dedicated network traffic monitoring and network anomaly and cyberattack detection tools for industrial networks. In most cases, using such tools do not require making any changes to the structure or configuration of ICS systems and can be deployed without shutting these systems down. However, dedicated and highly qualified staff, integration with other anomaly detection tools and highly developed information security procedures on the industrial and corporate networks will probably be required to use such tools effectively.

6. Deploy dedicated tools for registering information security incidents on the industrial network and automating procedures for handling such incidents.
7. Establish a procedure for obtaining and processing information on relevant threats to ensure proper and timely responses to new attacks and prevent any incidents:
   - Specialized intelligence reports on newly identified attacks and malicious campaigns that target industrial enterprises.
   - Reports on studies of the tactics, techniques and procedures (TTP) used by known threat actors in attacks on industrial organizations.
   - Intelligence reports on the analysis of the landscape of threats that affect industrial enterprises.
   - Indicators of compromise for industrial network hosts.

Measures that require major changes to the industrial network's configuration and topology and involve other significant modifications to the enterprise's information systems

1. Keeping in mind that it is usually impossible to completely isolate the industrial network from adjacent networks, we recommend implementing the following measures to provide more secure remote access to automation systems and transfer of data between the industrial network and other networks that have different trust levels:
   - Isolate systems that have full-time or regular connections to external networks (mobile devices, VPN concentrators, terminal servers, etc.) into a separate segment of the industrial network – the demilitarized zone (DMZ).
   - Divide systems in the demilitarized zone into subnets or virtual subnets (VLAN), with restricted access between subnets (only the communications that are required should be allowed).
   - Perform all the necessary communication between the industrial network and the outside world (including the enterprise's office network) via the DMZ only.
   - If necessary, deploy terminal servers that support reverse connection methods (from the industrial network to the DMZ) in the DMZ.
   - Wherever possible, use thin clients to access the industrial network from the outside (using reverse connection methods).
   - Block access from the demilitarized zone to the industrial network.
   - Restrict network traffic on ports and protocols used on the edge routers between the organization's network and those of other companies (if information is transferred from one company's industrial network to another company).
   - If the enterprise's business processes are compatible with one-way data communication (from the industrial network to the corporate network), we recommend that you consider using data diodes.
2. Before deploying and launching new ICS systems and components, we recommend testing them for compliance with security requirements, including scanning them for known and new (previously unknown) vulnerabilities, as part of the new ICS component appraisal process. This will help to achieve a significant reduction of costs associated with ensuring the information security of systems after their deployment.
3. All other things being equal, we recommend giving preference to products developed by vendors with security in mind, e.g., using an approach based on proper separation of security domains and implementation of MILS (Multiple Independent Layers of Security) principles.

4. To provide protection against Man-in-the-Middle attacks, we recommend that the enterprise should consider implementing strong encryption of traffic both inside the industrial network and on its boundary – at least where this is supported by the equipment used and by the enterprise's business and industrial processes.
5. In some cases, encryption of traffic between components of the industrial network can be configured, even if this functionality is not supported by the existing equipment – in that case, additional tools can be used. We recommend consulting the vendor of your automation systems.
6. It is a good idea to use two-factor authentication for employees who need to access systems on the industrial network.
7. We recommend deploying the PKI infrastructure to simplify support for authentication and encryption procedures and processes.
8. To reduce risks associated with supply-chain attacks (i.e., attacks conducted via a chain of suppliers and contractors), consider implementing a policy, mechanisms and procedures to control the connection of devices, (e.g., contractors' and engineers' laptops) to the industrial network.

Kaspersky Lab Industrial Control Systems Cyber Emergency Response Team (Kaspersky Lab ICS CERT) is a global project of Kaspersky Lab aimed to coordinate the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky Lab ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the Industrial Internet of Things.

Kaspersky Lab ICS CERT **Ics-cert@kaspersky.com**