KASPERSKY lab

Threat Landscape for Industrial Automation Systems in H1 2017

Kaspersky Lab ICS CERT

Contents

For many years, Kaspersky Lab experts have detected and analyzed cyberthreats that target various information systems – those of commercial and government organizations, banks, telecoms operators, industrial enterprises, and individuals. Here, Kaspersky Lab Industrial Control Systems Cyber Emergency Response Team (Kaspersky Lab ICS CERT) publishes the results of its research on the threat landscape for industrial automation systems for the first six months of 2017.

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

Main Events of the 6 Months

New Cyberweapons

In June 2017, the results of research into the CrashOverride/Industroyer malware were published. Experts from ESET and Dragos Inc., as well as a number of independent researchers, came to the conclusion that the malware was designed to disrupt the operation of industrial control systems (ICS), particularly electrical substations. CrashOverride/Industroyer is capable of directly controlling switches and circuit breakers in electrical substation circuits.

The malware works with four industrial protocols that are widely used in the power sector, transport management, water supply and other types of critical infrastructure: IEC 60870-5-101 (aka IEC 101), IEC 60870-5-104 (aka IEC 104), IEC 61850, OLE for Process Control Data Access (OPC DA). The developers of CrashOverride/Industroyer can reconfigure the program to attack any industrial environment where target communication protocols are used. In all likelihood, they designed CrashOverride/Industroyer so it could be scaled for attacks against a variety of systems, rather than for a specific attack type.

Another significant feature of CrashOverride/Industroyer, according to the ESET report, is that it includes an additional tool that exploits vulnerabilities in the Siemens SIPROTEC family of protection relays. Devices can be made to stop responding by sending them a specially crafted data packet. To re-enable a device, it has to be manually rebooted.

If the malware uses the tool, in the event of a critical situation in an electrical network, the damage may not be limited to a power failure; the attack could damage equipment due to relay protection and control systems failing to work properly. If overloads are planned in a certain way, an attack in one place can result in cascading power shutdowns at several substations.

ESET experts believe that CrashOverride/Industroyer may have been connected with the December 2016 blackout in Kiev, when a Ukrenergo substation serving the north of Kiev malfunctioned. According to Ukrenergo representatives, the failure at the substation was due to an external impact on its SCADA systems.

Reasons for believing the failure may have been caused by CrashOverride/Industroyer include the malware having adequate functionality to carry out such attacks and the activation timestamp – 17 December 2016, which was the date of the blackout. Nevertheless, at this time there is no direct proof that this malware has been involved in any known attacks against power sector facilities. It should also be noted that ESET experts, who were able to analyze the largest number of CrashOverride/Industroyer modules, emphasize the lack of any clues as to the malware writers' origins.

The capabilities of CrashOverride/Industroyer are testament to its developers' skills and their thorough knowledge of the way industrial control systems work in electric power sector facilities. It is unlikely that this kind of malware could be developed without access to the hardware used in such facilities.

All of this means that CrashOverride/Industroyer is a true cyberweapon targeting industrial systems. It is perhaps the most serious known threat to industrial control systems since Stuxnet.

Hacker Attacks on Safety Systems

Disrupting Washington DC Police Closed-Circuit Camera Network

In mid-January, eight days before Donald Trump's inauguration, the video surveillance system used by the DC police department was brought down. Of the 187 data storage devices used to record video from cameras installed in public areas, 123 were infected with encryption ransomware.

According to The Washington Post, in spite of the forthcoming presidential inauguration in the US capital, the city paid no ransom. To restore the affected devices to normal operation, they were taken offline and all the software on them was reinstalled.

By the time of the presidential inauguration, the surveillance system was restored to normal operation. Later, at the request of US authorities, UK law enforcement agencies arrested a British man and a Swedish woman in London for their possible involvement in the incident.

Dallas Emergency Alert System Hack

In April 2017, residents of Dallas in the US experienced at first hand the consequences of a cyberattack on safety systems when all the city's emergency sirens were set off as a result of a hack. In the space of 90 minutes, the 156 sirens, which are normally used to warn of tornadoes, went through 15 90-second activation cycles. Engineers only managed to stop the sirens late at night, after manually shutting down their radio system and repeaters.

Without disclosing any details, the city authorities stated that the attack had been carried out via a radio signal. Experts from Bastille, a security firm, believe that it is most likely that somebody carried out a "radio replay" attack: the attacker recorded the control center's commands transmitted over an emergency radio frequency during a monthly test of the emergency alert system and then played them back later.

It took two days to restore the system to normal operation. If a tornado had hit during those two days, city residents would not have been alerted.

Persirai IoT Botnet

In April 2017, a researcher named Pierre Kim published the results of his work, in which he stated that over 1000 IP camera models from 354 different vendors had a dangerous vulnerability in the built-in web server. In addition to a detailed description of the problem, Kim published code fragments and information that over 185,000 vulnerable cameras could be detected via Shodan (he also included the relevant link). According to the researcher, his objective in publishing this information was to draw the attention of the many camera manufacturers to the vulnerability. However, malicious actors were the quickest to react to the publication, as is often the case.

As early as May 2017, Trend Micro experts uncovered a new IoT botnet made up of vulnerable cameras, which they dubbed Persirai. According to Trend Micro, cybercriminals use the botnet primarily for DDoS attacks.

Business Email Compromise Attacks on Industrial Companies

Kaspersky Lab ICS CERT experts reported on Business Email Compromise (BEC) attacks carried out by Nigerian threat actors that were primarily targeting industrial and large transportation and logistics companies. In the attacks analyzed by Kaspersky Lab, industrial companies account for over 80% of potential victims. All in all, over 500 attacked companies were discovered in more than 50 countries.

In the first stage, fraudsters send emails with malicious attachments to corporate addresses. The malware used in these attacks is designed to steal confidential data and, in some cases, to install stealthy remote administration tools on infected systems. After infecting a corporate computer, the attackers make screenshots of the employee's correspondence using malware or set up hidden redirection of messages from the attacked computer's mailbox to their own mailbox. This enables them to track which transactions are being prepared in the company.

After selecting the most promising transaction among those in the pipeline, the attackers register domain names that are very similar to the names of the seller companies. Using the newly registered domains, the cybercriminals are able to carry out a man-in-the-middle attack: they intercept the email with the seller's invoice and forward it to the buyer from a mailbox in a phishing domain after replacing the seller's account details with the details of an account belonging to the attackers. Alternatively, they can send a request on behalf of the seller for an urgent change of bank details in addition to the seller's legitimate email containing the invoice.

Another option for the cybercriminals is to gain access to the legitimate mailbox of one of the attacked company's employees using Trojan Spy and/or Backdoor malware and then send fraudulent emails from that mailbox. Phishers can also send emails on behalf of the seller with spoofed email headers pointing to the seller's legitimate mailbox as a sender.

In any event the chances of the recipient never suspecting anything and the criminals getting the money are very high.

Such attacks are dangerous for industrial companies. In the event of a successful attack, the company making a purchase not only loses money but also fails to receive the goods they need on time. This can be critical for an industrial company: if the goods are raw materials used in manufacturing or spare parts needed to repair equipment, their non-delivery can result in downtime or failure to perform scheduled maintenance or commissioning and start-up work.

However, there are other possible consequences, as well. The spyware programs used by phishers send a variety of data from infected machines to their command-and-control servers, including information on industrial companies' operations and main assets, such as information on contracts and projects. Screenshots made on workstations of operators, engineers, designers and architects have been found on some of the command-and-control servers used by cybercriminals.

So far, experts have not seen any cases of information stolen by the attackers being sold on the black market. However, it is clear that, for the companies being attacked, in addition to the direct financial loss on specific transactions a BEC attack poses other, possibly more serious, threats.

It should be noted that BEC attacks on industrial companies continue in the second half of 2017.

Dangerous Publications

WikiLeaks: the CIA Archive

An important development in the first six months of 2017 was the leak of an archive from a special unit of the US Central Intelligence Agency. The archive included information on CIA hacking tools: malware, including zero-day exploits, malicious remote access tools and related documentation. Part of the archive was published on WikiLeaks.

The dump obtained by WikiLeaks is known as Vault 7. Since March 2017, about 9,000 documents have been disclosed in a series of publications. These documents detail CIA capabilities related to surreptitiously compromising various electronic devices, from mobile phones and smart TVs to corporate systems. CIA malware targets software for Windows, MacOS, Linux, iPhone, Android, SmartTV television sets, and routers.

Documents published by WikiLeaks list numerous vulnerabilities. In particular, after the Vault 7 publication, Cisco warned its customers of a critical vulnerability that could allow an attacker to execute arbitrary code and gain full control of more than 300 different models of its switches and routers (the vulnerability was closed in May).

According to experts, most of the vulnerabilities on the list were closed by vendors before the WikiLeaks publication. WikiLeaks did not disclose any information on hacking tools or exploits. However, even the part that was published can help cybercriminals develop their own malicious arsenal. It is very likely that in the future we will see mass attacks and the consequences of surreptitious penetrations based on the information published in Vault 7.

Shadow Brokers: the NSA Archive

In April, the Shadow Brokers hacker group opened access to a National Security Agency (NSA) archive containing exploits and attack tools.

At first, Shadow Brokers tried to sell their archive. Later, most of it was published. The data that was made public included exploits for network equipment and routers, for banking systems, for UNIX-like systems and for various versions of Windows. Some of the vulnerabilities published were previously unknown zero-day vulnerabilities.

Microsoft announced that most of the published vulnerabilities from the archive had been fixed or were irrelevant for Windows 7 and higher. Microsoft closed three of the vulnerabilities one month prior to the Shadow Brokers publication – in the MS17-10 patch.

The patch also closed a vulnerability in SMBv1, which was targeted, among others, by NSA exploits EternalBlue and EternalRomance. Just a month and a half after the Shadow Brokers publication, variants of these exploits were used to distribute the now infamous encryption ransomware programs WannaCry and ExPetr (Petya).

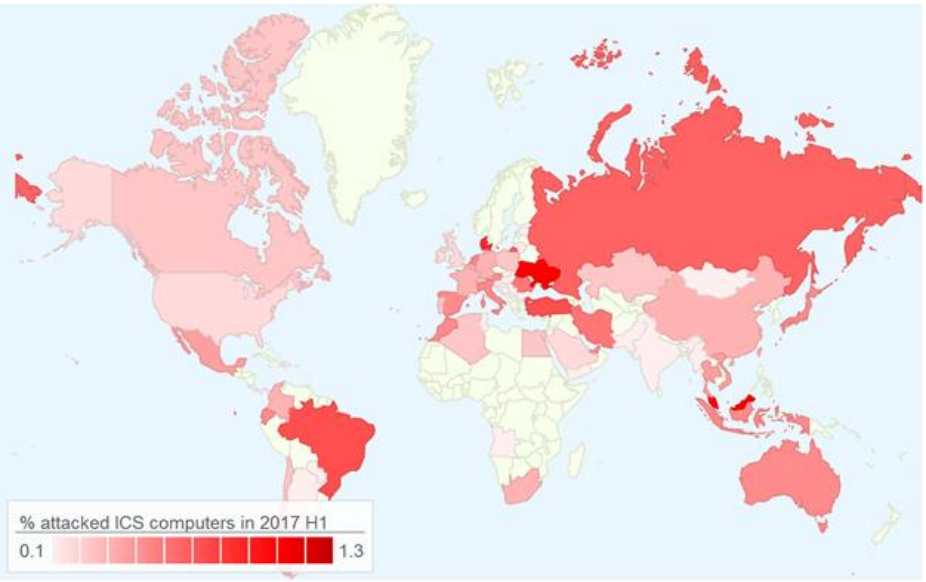
Ransomware Attacks

The first half of 2017 will be remembered – and not just by security experts – for encryption ransomware attacks. The WannaCry outbreak and ExPetr attacks ensured this problem got widespread public attention.

Ransomware has become a significant threat for companies, including industrial enterprises. It is particularly dangerous for enterprises that have critical infrastructure facilities, since malware activity can disrupt industrial processes.

Kaspersky Lab products have blocked numerous encryption ransomware attacks on ICS computers in 63 countries across the globe. The map below shows the percentage of industrial automation systems attacked by encryption ransomware to the total number of such systems in each country.

According to our data, **0.5%** of computers in the industrial infrastructure of organizations were attacked by encryption ransomware at least once in the first half of 2017.



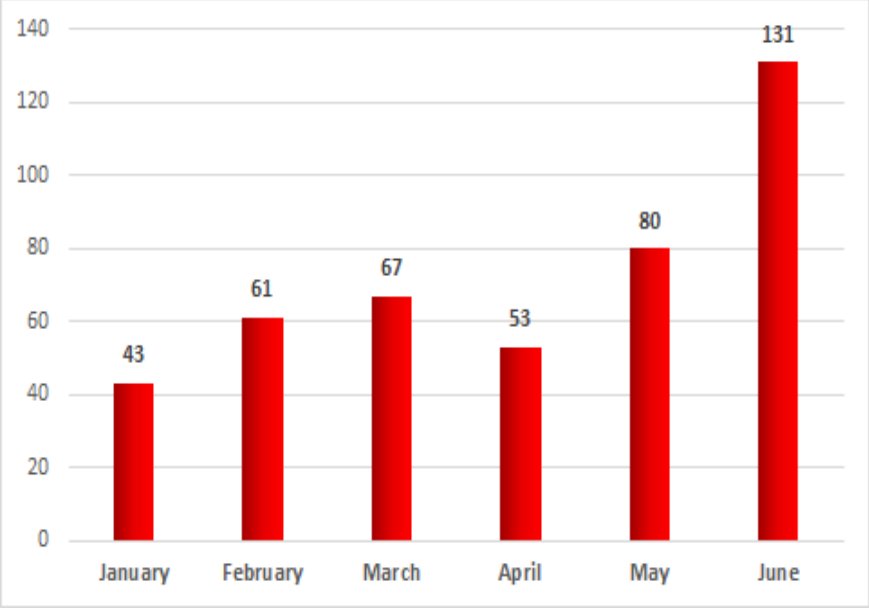
Geographical distribution of encryption Trojan attacks on industrial systems (percentage of ICS computers attacked in each country)

Top 10 countries based on the percentage of ICS computers attacked by encryption malware:

	Country*	% of systems attacked
1	Ukraine	1.33%
2	Malaysia	1.31%
3	Denmark	1.12%
4	Republic of Korea	1.06%
5	Turkey	0.88%
6	Brazil	0.85%
7	Russia	0.80%
8	Romania	0.67%
9	Iran	0.65%
10	Austria	0.65%

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

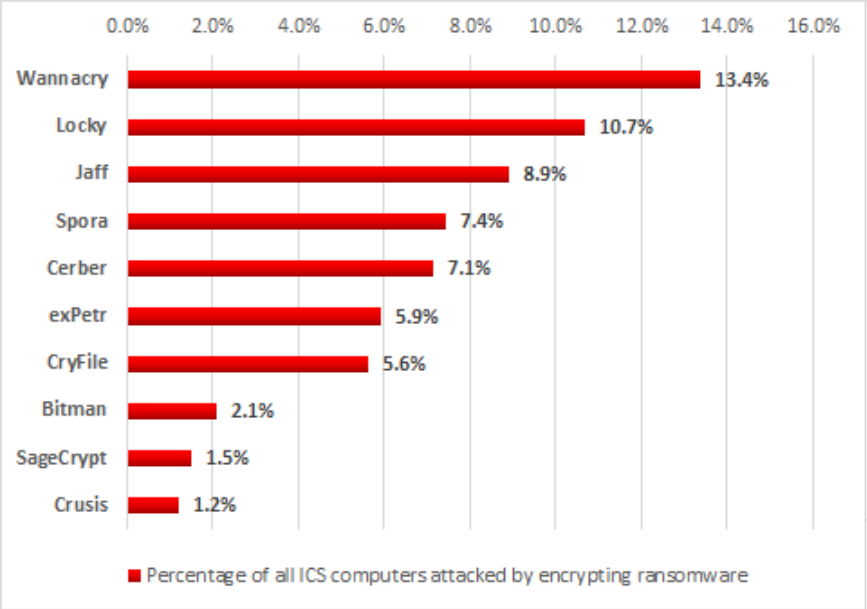
In the first six months of 2017, we observed the largest number of ICS computers attacked during the WannaCry epidemic.



Number of unique ICS computers attacked by encryption Trojans, H1 2017

During the first six months of 2017, attacks by encryption ransomware belonging to 33 different families were blocked on ICS computers. Fortunately, we did not find any dedicated programs designed specifically to block industrial automation software among the malware samples detected.

Based on the number of machines attacked, WannaCry ranked highest in the first half of 2017 – it accounted for 13.4% of all computers in industrial infrastructure attacked by encryption ransomware.



TOP 10 most widespread encryption Trojan families, H1 2017

Note that second and fifth positions in our ranking are occupied by two families, Locky and Cerber, which, according to Google experts and researchers from New York University Tandom School of Engineering, earned the highest profits for cybercriminals in the past two years ($7.8 million and $6.9 million respectively).

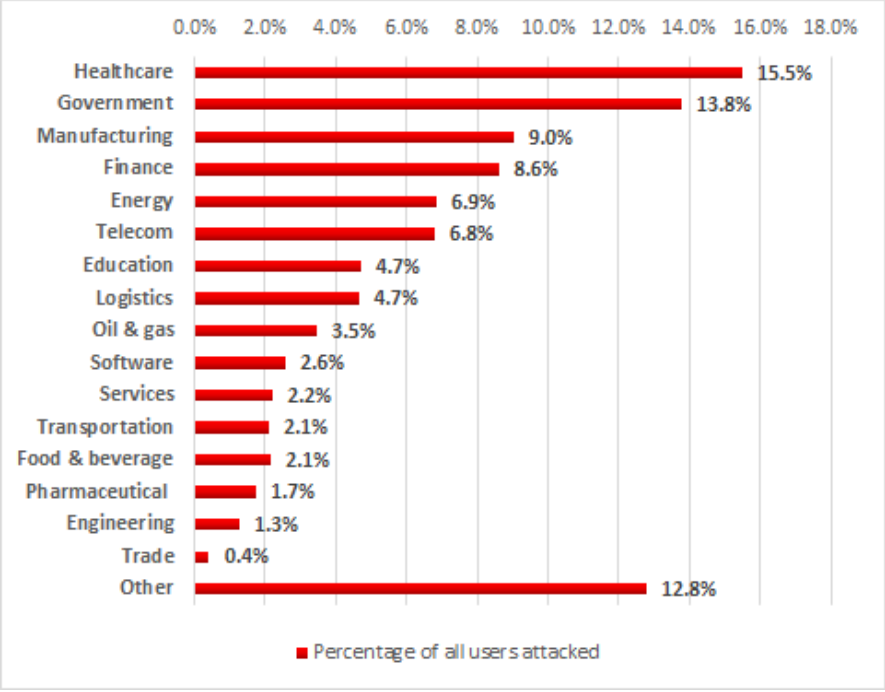
Most of the TOP 10 encryption Trojans are distributed through spam emails disguised as business communication. The emails are sent with malicious downloaders attached to them or with links to encryption malware downloaders in message bodies.

There are two exceptions – WannaCry and ExPetr were the most notorious encryption ransomware programs of the first half of 2017. The rate at which they spread and the effectiveness with which they infected computers were unprecedented for this class of malware. This was in large measure due to their use of National Security Agency (NSA) exploits that were made publicly available by the Shadow Brokers hacker group in April 2017 (see above).

The WannaCry Outbreak

The rapid proliferation of WannaCry began on 12 May and quickly turned into an epidemic that affected computers in 150 countries across the globe.

Companies attacked by WannaCry included those involved in different types of manufacturing, oil refineries, urban infrastructure and electricity distribution network facilities. According to Kaspersky Security Network data, at the beginning of June the distribution, by industry, of companies attacked was as follows:



Distribution of companies attacked by WannaCry by industry, May – June 2017

There are several known cases of WannaCry infections that resulted in downtime of industrial and social infrastructure facilities.

Renault was forced to suspend the operation of several of its factories; a Nissan production line was affected in at least one case; production was halted at a Honda plant in Sayama, Japan.

The Spanish newspaper El Mundo confirmed that Spanish industrial companies had been affected by WannaCry infections, including Gas Natural (a natural gas supplier) and Iberdrola, an electric power company.

Social infrastructure facilities affected included healthcare institutions. Specifically, it has been reported that many hospitals were unable to access patients' medical records, as a result of which some operations had to be canceled.

It turned out later that the software installed on some medical devices also had the CVE-2017-0143 (MS17-010) vulnerability, which was exploited by EternalBlue. In the middle of May, Siemens issued a security bulletin and advisories for magnetic resonance imaging systems and multi-purpose diagnostic workstations that could have been affected by the WannaCry attack.

Many incidents were not publicly reported.

As mentioned above, the attackers used a National Security Agency (NSA) exploit – a modified variant of EternalBlue, which exploits the CVE-2017-0143 vulnerability in components of the Windows SMBv1 service. Although Microsoft released a patch for the vulnerability back in March (Security Bulletin MS17-010), over 200,000 computers were affected by the ransomware epidemic, according to a Europol estimate.

To exploit the vulnerability, it is necessary to establish a connection with the remote machine on TCP ports 139 and 445. The malware identified machines with TCP port 445 available for connection. If the vulnerability was successfully exploited, the malware achieved persistence on the system and began to encrypt files. After infecting a computer, WannaCry spread across the local network, using the same EternalBlue exploit for a vulnerability in SMBv1 service components.

As a rule, industrial systems inside the control network perimeter are either not directly connected to the Internet or their Internet access is provided via the corporate network using NAT, a firewall and a corporate proxy server, which should rule out any infection of these systems through the Internet. However, according to our data, at least several dozen computers that were part of industrial enterprise control systems were attacked by the WannaCry encryption worm. In cases where computers were not properly protected they were infected and files on these computers were encrypted. This could result in failure or disruption of the operation of industrial control systems at these enterprises and in disruption of their production cycles. So how was the network worm able to penetrate the control network?

WannaCry infections were possible because of typical industrial network configuration errors. We analyzed all infection pathways and came to the conclusion that in most cases industrial automation systems had been attacked by WannaCry malware from the local corporate network and through VPN connections.

The ExPetr (Petya) Attack

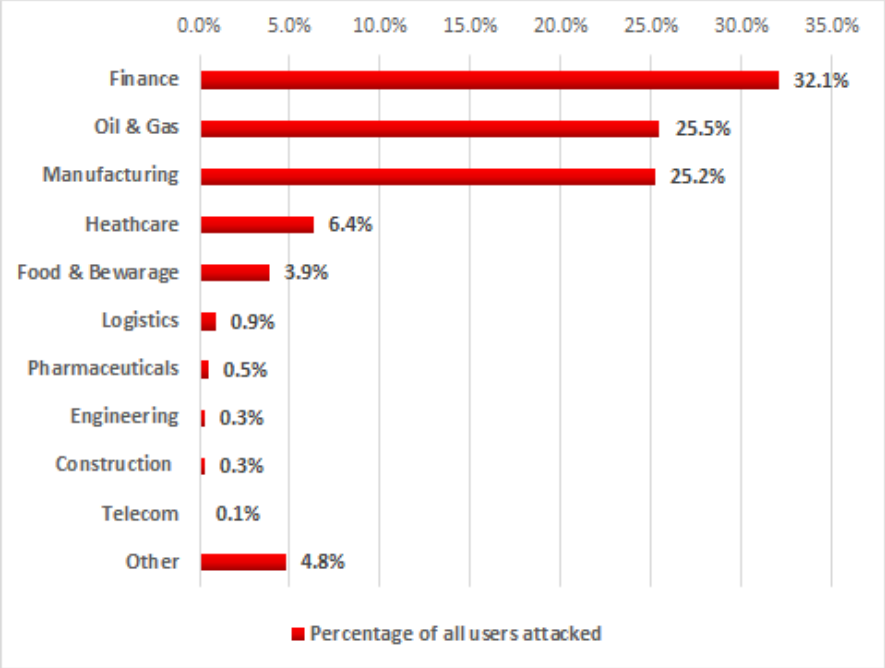
The ExPetr attack, which started on the morning of June 27 in Russia and Ukraine and then spread to Europe, affected some important industries and services.

In Ukraine, victims included power sector companies, Ukrainian banks, the Kiev Metro, Borispol Kiev airport, Kharkov airport, and the Chernobyl radiation monitoring station. In Russia, reports started appearing at about the same time that servers at Rosneft Corporation had been hit by a "powerful hacker attack". It was subsequently revealed that other industrial companies, including the giant steel maker Evraz, HMS Group, which includes such companies as Sibneftemash, HMS Neftemash and Giprotyumenneftegaz, were affected by attacks of the encryption malware.

Later, reports of infections started coming in from other European countries. Victims included the pharmaceutical giant Merck and Co., the Danish logistics giant Maersk and dozens of other companies, including SaintGobain, a large industrial organization in France.

The system that controls the loading and unloading of containers at one of the terminals of Jawaharlal Nehru Port Trust, which is India's largest container port and is operated by A.P. Moller-Maersk, was disrupted by the attack – the system could no longer identify which shipment belonged to whom.

We analyzed the industry distribution of ExPetr (Petya) attack targets. According to Kaspersky Security Network data, as of 28 June, at least 50% of the companies attacked were from manufacturing, and oil and gas industries.



Industry distribution of ExPetr attack targets

To infect computers and launch the malware on them, cybercriminals used the updating mechanism of a third-party Ukrainian electronic workflow program called M.E.Doc. In addition, it has been established that at least one legitimate website was infected and used to redirect requests to a malicious file (a so-called watering hole attack). It can be inferred from this that the initial attack vector was sufficiently

narrow, but the lateral movement mechanism enabled the encryption malware to "go out into the world". For lateral movement, ExPetr used NSA exploits – EternalBlue and EternalRomance. The use of this mechanism resulted, among other things, in the infection of computers that connected to an infected local network via VPN.

In addition, the malware launched itself on a local network's remote computers using PsExec and WMI tools, with the credentials of the current user stolen using a dedicated program such as Mimikatz, which was stored in the malware's resources.

In addition to encrypting data, ExPetr overwrote the infected machine's MBR.

Extortion or Sabotage?

Both WannaCry and ExPetr are categorized as encryption ransomware. The groups behind these malicious programs are completely different. However, both groups seemed poised to make enormous amounts of money from successful ransomware attacks, but failed to do so – for different reasons.

Strictly speaking, ExPetr is not ransomware. Researchers very soon found out that, due to errors in its code, even the attackers themselves could not decrypt victims' files. This means that the Trojan actually belongs to the class of malware that destroys information, i.e., Wiper. It is likely that the real objective of ExPetr attacks was not to extort ransom payments – the ransom demands may have been a mask for acts of sabotage.

Some experts believe that in the case of WannaCry money was not the main aim of the malicious actor either. Given the enormous number of infected computers, the attackers' takings were meager. Notably, compared to others in the cybercriminal business centered around ransomware, the WannaCry owners did not demonstrate a particular interest in improving the situation.

Kaspersky Lab experts believe that the active distribution of encryption malware is set to continue. The authors of these Trojans are increasingly distributing their products using the SaaS (Software as a Service) model. This enables those cybercriminals who lack the skills, resources or motivation to develop their own malware to make money from cyber extortion. There are more and more players of varying caliber in this field.

Industrial companies are targeted by encryption malware attacks alongside other organizations. So far, there have been no credible instances of targeted ransomware attacks against industrial companies that have a ransom as their primary objective – so far, such attacks have mostly been carried out against financial organizations. In the wild, we have not seen any encryption malware specifically designed to block industrial automation software. So far, all known cases of computers in the industrial network infrastructure being infected with encryption malware have fallen into the category of accidental, rather than targeted, infections.

Unfortunately, even an accidental infection of computers on an industrial network by encryption malware can result in downtime or a malfunction of the enterprise's industrial automation systems, leading to the disruption of the enterprise's production cycles.

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.

Methodology

The data was received from 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).

This group also includes computers of employees at contractor organizations and 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.

Note that Internet access restrictions can be significantly different for computers inside an industrial network and computers that make up the infrastructure of that industrial network.

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.

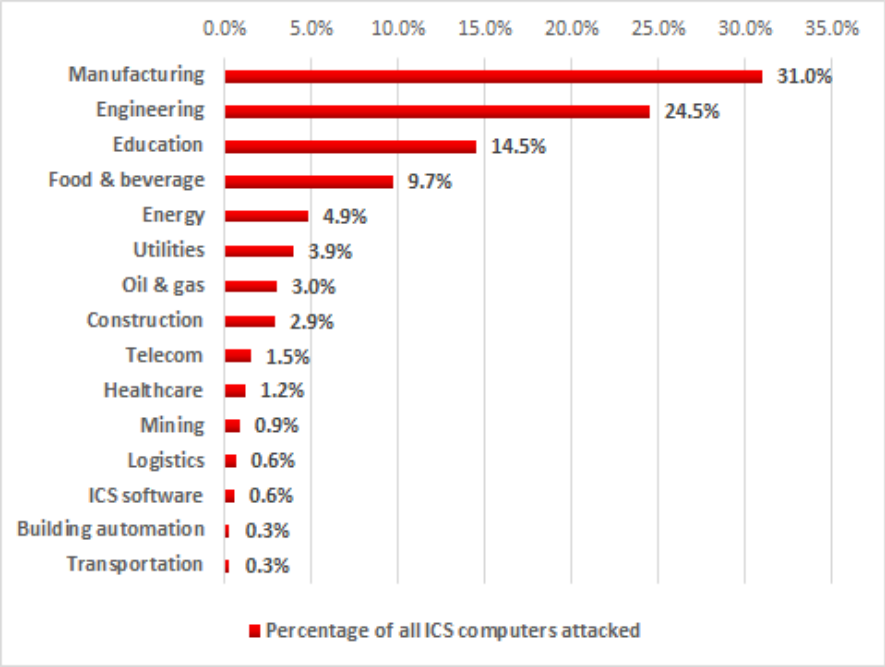
Workstations of system/network administrators, developers and integrators of industrial automation systems, as well as computers of contractors that connect to the industrial network (e.g., to provide monitoring and technical support) may have frequent or even full-time Internet connections.

As a result, in our sample of computers categorized by Kaspersky Lab ICS CERT as part of an organization's industrial control infrastructure, 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

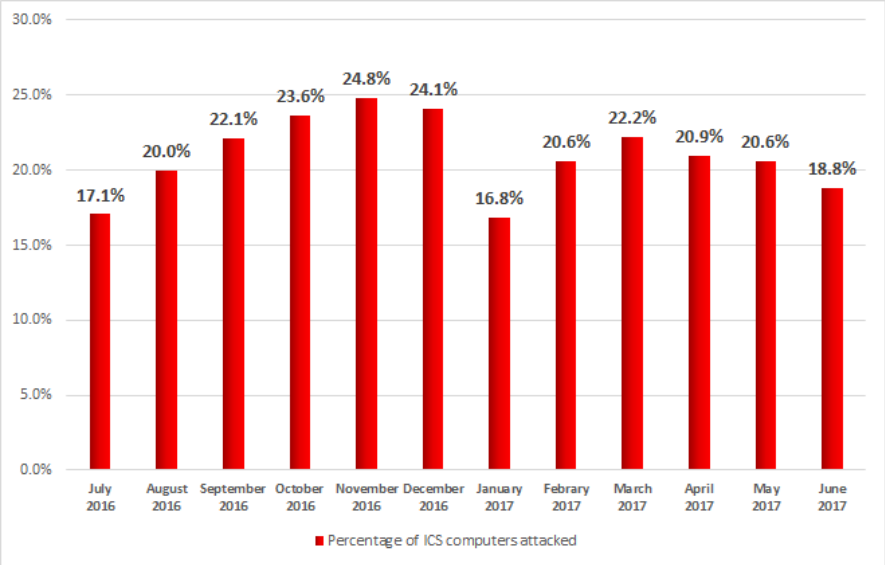
In the first half of 2017, Kaspersky Lab products blocked attack attempts on **37.6%** of ICS computers protected by them globally, which is 1.6 percentage points less than in the second half of 2016.

ICS computers in manufacturing companies that produce various materials, equipment and goods accounted for about one third of all attacks.



Distribution of ICS computers attacked by industry, H1 2017

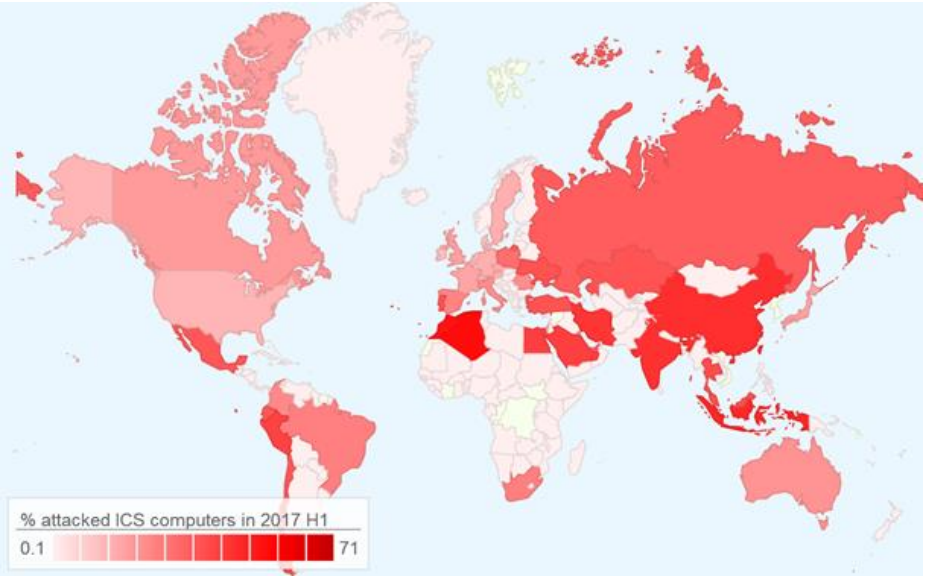
While the proportion of machines attacked grew from one month to the next in the second half of 2016, the dynamics were somewhat different in the first six months of 2017. We saw attacker activity fall in January, then the proportion of computers attacked rose back to its former level in February and March and then it gradually declined again from April to June.



Percentage of ICS computers attacked globally by month, July 2016 – June 2017

Geographical Distribution of Attacks on Industrial Automation Systems

The map below shows percentages of industrial automation systems attacked to the total number of such systems in each country. The least affected countries are Ireland (13.8%), Denmark (14.1%), the Netherlands (15.5%), the US (17.1%), and Switzerland (17.4%).



Geographical distribution of attacks on industrial automation systems, H1 2017

TOP 15 countries by percentage of ICS computers attacked:

	Country*	% of systems attacked
1	Vietnam	71.0%
2	Algeria	67.1%
3	Morocco	65.4%
4	Indonesia	58.7%
5	China	57.1%
6	India	56.0%
7	Iran	55.3%
8	Saudi Arabia	51.8%
9	Egypt	51.6%
10	Peru	50.8%
11	Thailand	47.8%
12	Malaysia	47.2%
13	Ukraine	46.3%
14	Portugal	46.1%
15	Kazakhstan	45.9%

* 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.

Malware in Industrial Automation Systems

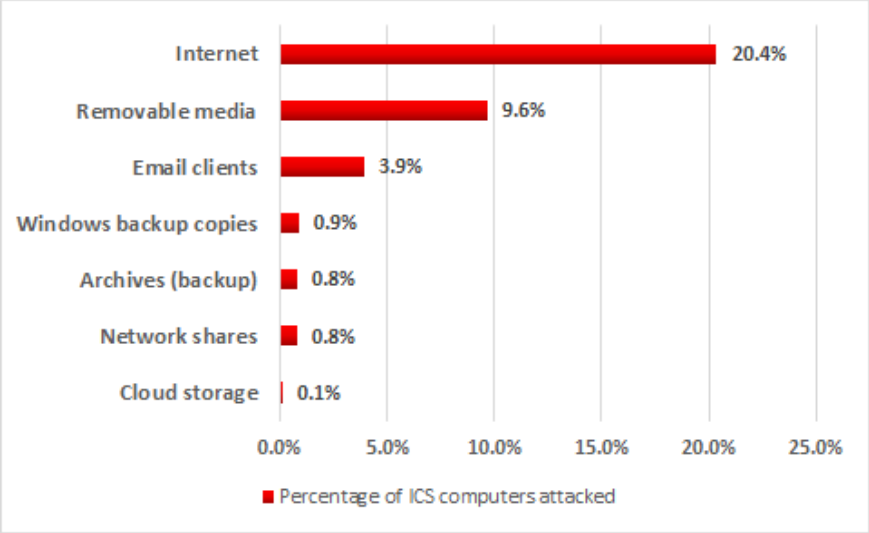
In terms of the use cases and the technologies used, industrial networks are becoming increasingly similar to corporate networks. Consequently, the threat landscape for industrial systems is becoming similar to the threat landscape for corporate systems.

About 18,000 different modifications of malware belonging to more than 2,500 different families were detected on industrial automation systems in the first half of 2017.

In the vast majority of cases, attempts to infect ICS computers were accidental and malware functionality was not specifically designed for industrial automation systems.

The same categories of malware that attack corporate computers are also relevant for ICS computers, including spyware (Trojan-Spy and Trojan-PSW), ransomware (Trojan-Ransom), backdoors and Wiper-type programs (KillDisk), which render the computer unusable and wipe data from the hard drive. Such programs pose a particularly serious threat to ICS computers, since infection with such malware can result in a loss of control or disruption of industrial processes.

Sources of Industrial Automation System Infection



Main sources of threats blocked on ICS computers, H1 2017

In the first half of 2017, attempts to download malware from the Internet or access known malicious or phishing web resources were blocked on 20.4% of ICS computers.

For computers that are part of 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 operators' networks (using mobile phones, USB modems and/or Wi-Fi routers with 3G/LTE support). As for contractors, developers, integrators and system/network administrators that connect to the control network externally (directly or remotely), they often have unrestricted Internet access. Their computers are in the highest-risk group and can be used by malware as a channel for

penetrating into the industrial networks of enterprises served by them. As we mentioned above, about 40% of computers in our sample connect to the Internet on a regular basis.

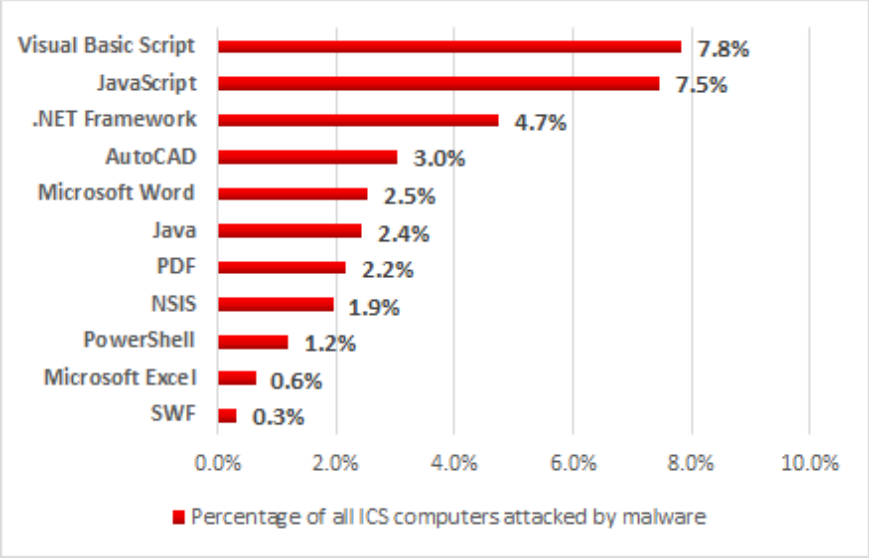
Malware was detected on 9.6% of ICS computers when removable media were connected to them. Malware that spreads via removable media and network folders often infects legitimate files or uses names similar to those of legitimate files (this behavior is characteristic of many viruses and worms). Malicious files with names that are the same as those of legitimate files can be included into secure data archives created by users (we detected such archives on 0.8% of computers) and file system backups created by the operating system (also 0.8%).

Malicious email attachments and malicious scripts built into email message bodies were blocked on 3.9% of ICS computers. In our ranking, email clients are in third place. In most cases, attackers distribute emails with malicious attachments in office document formats, such as MS Office and PDF.

On 0.1% of ICS computers, malware was found in local folders of cloud storage services, which automatically synchronize with the cloud when the computer connects to the Internet. This synchronization results in the following situation: malicious files are automatically delivered to all devices connected to a cloud storage if the cloud storage is infected (via any of the computers that have access to it).

Platforms Used by Malware

Malware in the form of Windows (Win32/Win 64) executable files was blocked on more than 50% of all computers attacked. Instead of developing an executable file, threat actors often implement malicious functionality using a script language, which is executed by interpreters that are already installed on the computer of a would-be victim. A ranking of the main platforms used by malware apart from Windows is provided below.



Platforms used by malware, H1 2017

Note that attackers often use small loaders written in JavaScript, Visual Basic Script or Powershell, which are launched using command-line parameters for the relevant interpreters.

Our Recommendations

To prevent such accidental infections in the future and to provide protection from targeted attacks against industrial networks, we recommend taking a set of measures designed to ensure the security of the industrial network's internal and external perimeters.

First of all, to provide secure remote management of automation systems and the transfer of data between the industrial network and other networks, access should be restricted to the greatest extent possible between systems which are parts of different networks or which have different trust levels:

- Systems that constantly or regularly communicate 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 communications that are necessary should be allowed);
- All required information exchange between the industrial network and the outside world should be carried out via the DMZ;
- If necessary, terminal servers can be deployed in the DMZ to enable reverse connection methods (from the industrial network to the DMZ).
- Thin clients should be used whenever possible to access the industrial network (using reverse connection methods);
- Where possible, 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.

It should be kept in mind that the threat landscape for industrial automation systems is continually changing, with new vulnerabilities found both in application software and in industrial software.

To provide protection against unknown threats, including targeted threats, we recommend:

1. Taking an inventory of running network services; 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 that exploit vulnerabilities in Linux).
2. Auditing ICS component access isolation; 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).

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 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. 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 hosts on the industrial network. Wherever possible, disabling the relevant ports or controlling access to these ports using properly configured specialized tools.
7. 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 stopping their operation.

Of course, completely isolating the industrial network from adjacent networks is 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**