ICS CERT

Threat Landscape for Industrial Automation Systems in the second half of 2016

Kaspersky Lab ICS CERT

Contents

For many years, Kaspersky Lab experts have been detecting and analyzing cyberthreats that target various information systems – those of commercial and governmental organizations, banks, telecoms operators, industrial enterprises and individuals. The Kaspersky Lab Industrial Control Systems Cyber Emergency Response Team (Kaspersky Lab ICS CERT) is starting a series of regular publications about our research devoted to the threat landscape for industrial organizations.

The main goal of these publications is to provide well rounded data intelligence on modern cyber security threats in the critical infrastructure and industrial space, as well as to share incident details with CERT teams and security researches working in the field of industrial security.

ICS IT security challenges

Cyber security challenges in industrial control networks are the result of rapidly increasing functional requirements and exponentially growing use of information technology in manufacturing/industrial environments. For decades, the evolution of process automation systems has been closely connected with that of traditional IT systems. An important requirement for industrial control systems is to ensure the greatest possible availability of industrial processes. To meet this requirement, industrial control systems must support functions that are not typical of traditional IT systems.

Upgrading industrial control systems takes much longer than upgrading traditional IT systems. Over time, industrial organizations have developed high-level information control systems based on traditional IT technologies. However, to integrate these new information systems into existing industrial control processes, these organizations had to create additional communication and information exchange paths, mostly unverified ad-hock solutions, some of which connect information systems with lower levels of existing SCADA systems. This new approach puts the entire Confidentiality-Integrity-Availability (CIA) concept, as well as the safety of individual processes and related hardware, at risk. In response to this problem, we can see growing demand for information control technologies designed for low-level (field-level) SCADA automation. Most Industrial organizations believe that field-level information technologies will help to satisfy CIA requirements and provide the communication capabilities required by existing high-level information control systems and related IT systems (finance, supply-demand, SAP/ERP systems, management, etc.).

The rapid adoption of information systems by organizations gives rise to other challenges, such as the need for regular system updates, patch and change management, upgrades for all lower and middle level hardware used by information systems. This can include the following types of hardware:

- Stationary and portable systems (mostly computers) for operating and engineering staff,
- SCADA monitoring servers, virtual servers,
- Industrial routers and network routing devices,
- Network switches,
- Programmable Logic Controllers (PLC),
- Field devices of various levels of complexity and autonomy with digital or analog input/output.

This introduces additional cyber security challenges, including the following:

1. Increased complexity of integrated information systems, hardware devices and component software produced by different vendors with minimal attention to security. This increases the risk of known and unknown vulnerabilities being exploited.
2. Measures designed to ensure compliance with CIA requirements and device compatibility in newly-designed information systems often put security requirements aside, leaving these systems in weak or highly vulnerable configurations.
3. The safety configuration in a typical SCADA deployment, including field-level devices, is not designed to perform well in the event of direct tampering with the control process (e.g. by remote intruders) or malicious use of existing access rights by the enterprise's staff. Analysis shows that in most such cases safety systems cannot perform their functions properly. As a result, a disrupted

industrial process can cause significant damage (killing people, damaging hardware, causing environmentally harmful spills or leaks, etc.).

4. An air gap between the industrial network and other networks was an easy-to-implement requirement 10 or 15 years ago. However, the ever-growing reliance of modern finance, supply and planning processes on connectivity and business analytics renders air-gaps impracticable, with very little chance of that simple solution being used in the future.

Modern industrial networks features

Providing integration of network segments

Today, **integration of the industrial network with the corporate network is required both for controlling manufacturing and for industrial network and system administration.**

Production management systems, such as MES, ERP, which run on the corporate network, are used to control the enterprise's entire production and resource management process. These systems are used not only to get performance data but also to influence the operation of individual industrial automation objects (workshops, lines etc.). As a rule, the uninterrupted operation of production management systems and all related systems is maintained by a section of the company's IT staff – system administrators and software developers – whose computers are usually also part of the corporate network.

Although integration of corporate and industrial networks is becoming a necessity, sometimes it is implemented without regard for many IT security risks.

Setting up secure access between the corporate and industrial networks usually comes down to one of the following solutions:

- restricting IP access on the firewall separating the industrial network from the corporate network ('lazy' DMZ),
- using VPN tunnels between computers on the corporate and industrial networks,
- using jump servers with local or domain authorization,
- using authorization on a corporate domain (on an ActiveDirectory server) to determine a user's access level to objects on the industrial network.

In reality, none of these solutions alone can currently provide the necessary level of protection. An optimal level of protection for an industrial network should not only protect the network against external threats but also provide secure remote management of industrial systems. This level can only be achieved using a combination of multiple solutions.

Access to external systems and networks

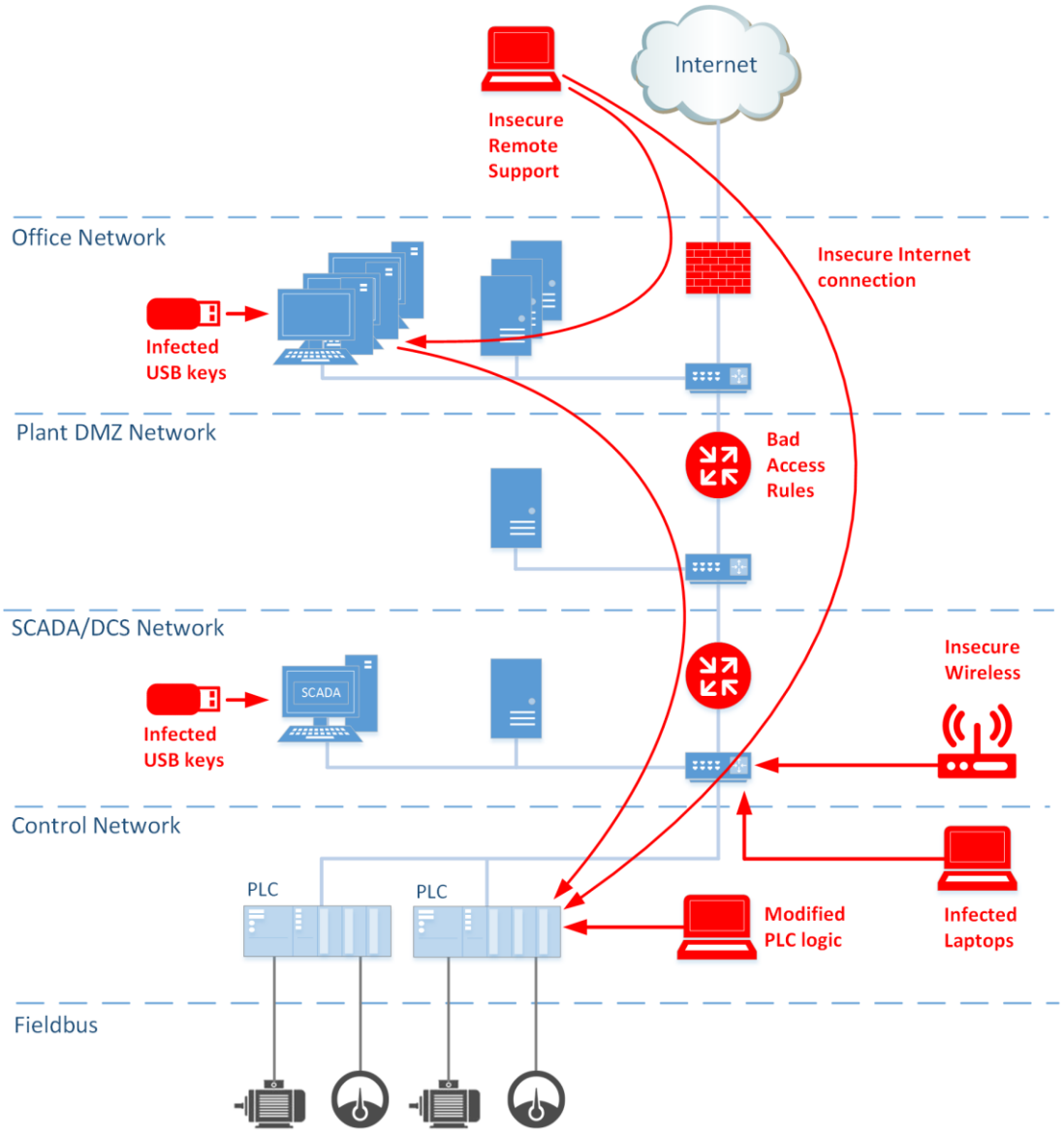
Internet access from an industrial control network is not necessarily the result of weak restrictions – it can be a forced necessity. Physically separate parts of an ICS can be situated in locations that are not inhabited by people. Such objects do not require permanent service staff: their maintenance is provided remotely via mobile Internet channels. A repair crew only visits these facilities for scheduled inspections or in an emergency.

It is important to note that maintenance and technical support of industrial control systems is often provided by employees of contractor organizations. This work is usually performed using remote access to the customer's industrial network from the corporate network of the contractor organization. Depending on the limitations and circumstances of each particular situation, an employee from the contractor organization can connect to the customer's industrial network (directly or via the contractor organization's corporate network) while away from the office using any available network for Internet access.

A user connecting from outside the industrial network (a contractor, developer or administrator) usually has high access rights at the local system level (local administrator) or at the entire network level. If the division into levels is organized as a flat network or as several virtual subnetworks (VLANs) with a common network core and without sufficient access control between different VLANs, this sort of user can accidentally or intentionally infect computers on the industrial network. In practice, the multilevel hierarchical structure of an industrial network is organized as several VLANs, with access between them not always limited to operational needs.

A changing threat landscape

Corporate and industrial networks, which form a multilevel hierarchical infrastructure in modern industrial companies, are increasingly being integrated. New technologies are being used that improve process transparency and efficiency at the enterprise level, as well as providing flexibility and fault tolerance of the functions performed at medium and lower industrial automation levels. This requires a greater freedom of communication and integration of systems at all levels. At the same time, functions related to the administration of new systems, including those on the industrial network, are the responsibility of the company's IT department. The upshot of all this is that the industrial network is increasingly similar to the corporate network – both in terms of usage scenarios and in terms of technologies used.



Cyberattack vectors

Naturally, the threat landscape of modern industrial information systems is becoming similar to the threat landscape of corporate ('office') IT systems. We see evidence of this in our research. Below we provide some of the results obtained during the second half of 2016, i.e., since Kaspersky Lab ICS CERT was created.

Vulnerabilities in ICS software

As a result of the relatively independent (from 'traditional' IT) evolution of industrial automation systems, vendors of industrial solutions for many years developed ICS software and hardware with virtually no regard for IT security requirements. At the same time, a transition to developing solutions that are more secure is often a long and painful process that is further complicated by certification and production control requirements.

Exploitation of software vulnerabilities in enterprise industrial networks, particularly critical infrastructure objects, can lead to disastrous consequences. Finding and eliminating these vulnerabilities, in addition to developing more advanced industrial solutions and specialized security tools, is a top-priority task for security experts.

The following type of vulnerabilities are critical:

- remote code execution,
- remote damage to hardware or software or DDoS capability,
- crypto attacks to network communication resources of data transferred via the networks,
- remote access to process configuration, control data for stealing, altering, duplicating, etc,
- manipulation with access credentials including local and remote users.

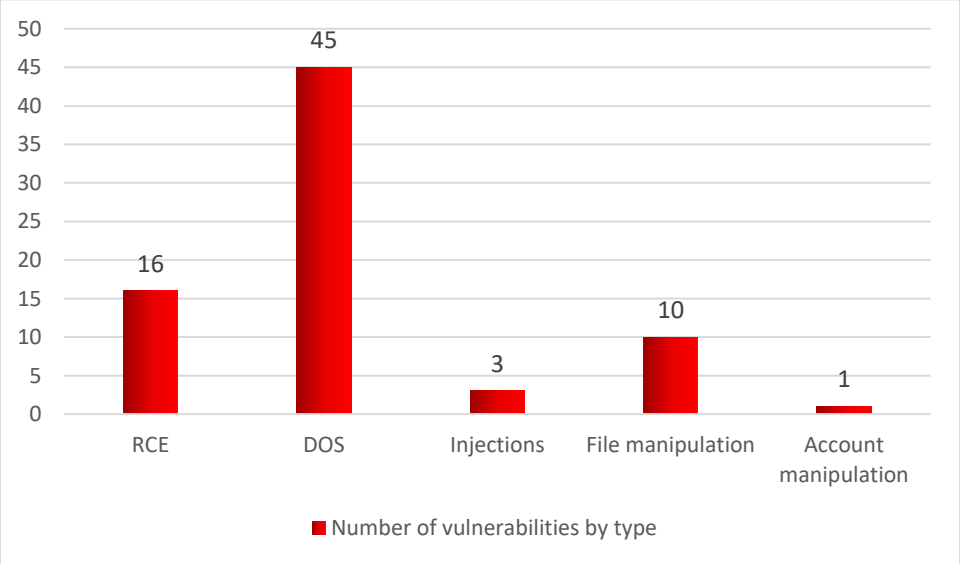
Need to mention another type of insecure behavior when the access credential are hardcoded in the application code, e.g. SCADA default access credentials or manufacturing zone home written applications with hardcoded admin credentials created to simplify access to various components and systems, e.g change and patch management or data gathering feeders.

With each passing year the number of vulnerabilities identified grows compared to the number of problems eliminated. For example, according to US ICS-CERT, in 2016 that organization registered 187 vulnerability notifications. During the same period, 139 reports of closed vulnerabilities were published.

Vulnerabilities detected by Kaspersky Lab

In 2016, Kaspersky Lab evaluated the current state of IT security components in the industrial control systems of different vendors. As a result of this research, 75 vulnerabilities were identified in ICS components.

The diagram below groups the vulnerabilities discovered based on the capabilities that exploiting these vulnerabilities provide to attackers.



Distribution of vulnerabilities uncovered by Kaspersky Lab in 2016 according to the ways in which they can be used

Brief descriptions of each vulnerability type:

- RCE (remote code execution) — vulnerabilities that enable arbitrary code to be remotely executed in a target system.
- DOS (denial of service) – vulnerabilities enabling a denial-of-service attack to be carried out remotely. In the event of a successful attack, the target software or hardware stops responding to legitimate requests, requiring the software, operating system or hardware to be restarted.
- Code Injections – a group which includes vulnerabilities enabling SQL injections and XML injections to be performed. Vulnerabilities in this group can be exploited to fulfil requests and read data on target systems without authorization. Under certain conditions, these vulnerabilities enable RCE attacks to be carried out.
- File manipulations – a group of vulnerabilities that enable various file operations (create, delete, move) to be performed remotely. Under certain conditions, these vulnerabilities also enable RCE attacks to be carried out.
- User access account manipulation – a group of vulnerabilities that enable attacks on legitimate user data to be carried out (create a new user, remove or block an existing user).

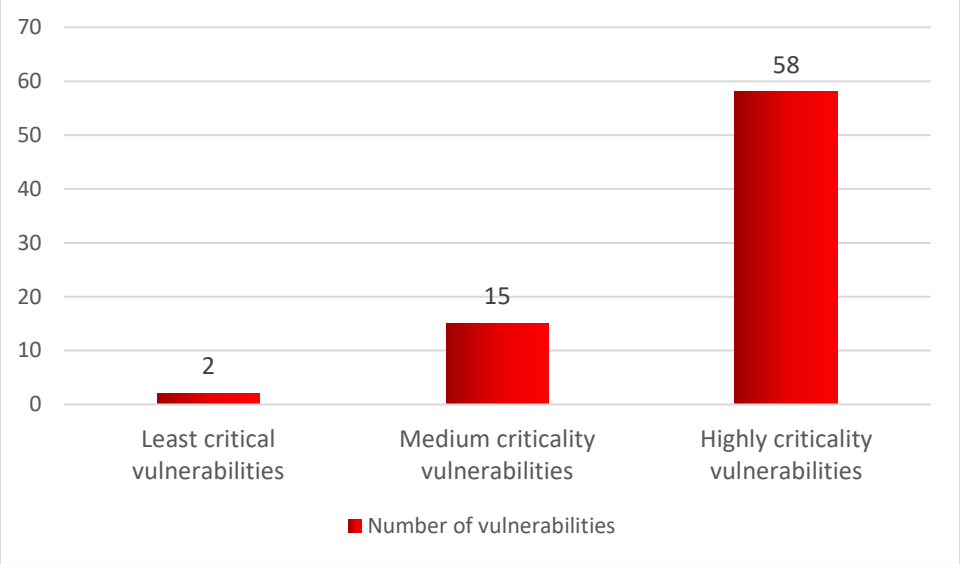
Severity levels of the vulnerabilities identified

We also analyzed the severity of the vulnerabilities found for vulnerable systems. We used the CVSS v3.0 metric as the basis of this analysis.

CVSS (Common Vulnerability Scoring System) is an open standard for assessing the severity of software vulnerabilities. CVSS assigns severity scores to vulnerabilities. Scores, which range from 0 (least severe) to 10 (most severe), are calculated based on a formula that depends on several metrics, including ease of exploiting a vulnerability and exploit impact. The third version of the CVSS standard supports better evaluation of cyber-physical systems, such as industrial networks and their components.

It should be noted that, although the accepted vulnerability classification used for IT is also valid for industrial components, risks associated with the same vulnerabilities can be different for systems on corporate networks and for those on industrial networks. CVSS 3.0 offers a qualitative gradation of severity levels that is mainly applicable to vulnerabilities in traditional IT environments. We do not apply this classification to industrial systems; instead we regard all vulnerabilities in ICS components as critical, based on the following levels:

- least critical: CVSS v3.0 severity score 5.0 or lower
- medium criticality: CVSS v3.0 severity score from 5.1 to 6.9 (inclusive) CVSS v3.0
- most critical: CVSS v3.0 severity score 7.0 or higher.



Distribution of vulnerabilities identified by Kaspersky Lab in 2016 by severity scores

There are numerous legitimate companies that offer anyone who is interested the opportunity to buy a ready-made proof-of-concept exploit kit (without malicious payload) for a variety of industrial software or to order an analysis of specific industrial software.

We consider this practice to be inadmissible, since there is a significant danger of the code falling into the wrong hands. Kaspersky Lab follows the principle of responsible disclosure of information about newly discovered vulnerabilities, despite the less-than-responsible attitude of some software vendors towards closing these vulnerabilities.

Problems related to closing vulnerabilities

Of the 75 vulnerabilities identified by the middle of March 2017 by Kaspersky Lab, industrial software vendors closed 30. A vendor refused to close 1 vulnerability (account manipulations), arguing that the company does not regard the relevant functionality as a vulnerability.

Our experience of working with some industrial software and hardware vendors shows that a vendor sometimes needs over 18 months to close critical vulnerabilities. This indicates that the approach to addressing vulnerabilities as part of the software development cycle has not yet been sufficiently refined.

- Vendors do not prioritize the closing of identified vulnerabilities based on their severity.
- Vendors prefer to fix vulnerabilities in the next release of their product rather than releasing a fix or patch that is critical from an IT security viewpoint.
- Some vendors prefer not to disclose information on some of the vulnerabilities that had been identified and closed on the grounds that the vulnerable solutions are used by a “limited number” of enterprises.

We do our best to ensure that industrial software and hardware vendors eliminate vulnerabilities within the shortest possible time.

Another issue that is not directly connected with industrial component manufacturers is the installation of updates and security patches at enterprises. Losses due to equipment downtime associated with updating the software can be significant even in comparison with the risks posed by vulnerabilities.

Even if a vendor has released a patch that fixes some vulnerabilities, the chances of it being promptly installed in the industrial infrastructure are not very high. In 2016, the Kaspersky Lab ICS CERT team analyzed existing and publicly known vulnerabilities found in Rockwell Automation solutions in 2014-2016. According to the findings of the study, the proportion of the vendor's software with unpatched vulnerabilities in the systems of Kaspersky Lab users could range between 17% and 93%. (The findings of our analysis of popular products by other major vendors will be published in 2017.)

Based on our research and ICS IT security audits, we believe that most organizations that have various ICS components currently do not have effective update management for their industrial components. The problem is that any changes to the hardware or software part of an ICS must first and foremost be tested for compatibility with the existing infrastructure. Sometimes such testing is carried out during periods of planned system downtime, but in today's industrial environment this is the exception rather than the rule. For ICS owners, the process of installing critical updates is either too labor-intensive or not a high-priority task in the system's overall lifecycle. As a result, at some enterprises critical updates of various industrial system components are not installed for years, making these enterprises vulnerable in the event of cyberattacks.

However, things in the world of industrial system vulnerabilities are not all bad. With each year, industrial enterprises are becoming more responsible when it comes to closing vulnerabilities. New methods of protecting an ICS at industrial enterprises are emerging, which include, among other things, detecting the exploitation of various vulnerabilities. Many ICS owners have already launched the process of upgrading their systems to more secure architectures and solutions. Now, cybersecurity requirements for the entire system are included when designing or upgrading the ICS, indicating a more mature and responsible approach to ICS design and development.

Threat statistics

All statistical data used in the report was obtained using Kaspersky Security Network (KSN), a distributed antivirus network. Data was received from those KSN users who consented to have their data collected anonymously.

Percentage of computers attacked

On average, in the second half of 2016 Kaspersky Lab products across the globe blocked attempted attacks on **39.2%** of protected computers that Kaspersky Lab ICS CERT classifies as being part of industrial enterprise technology infrastructure.

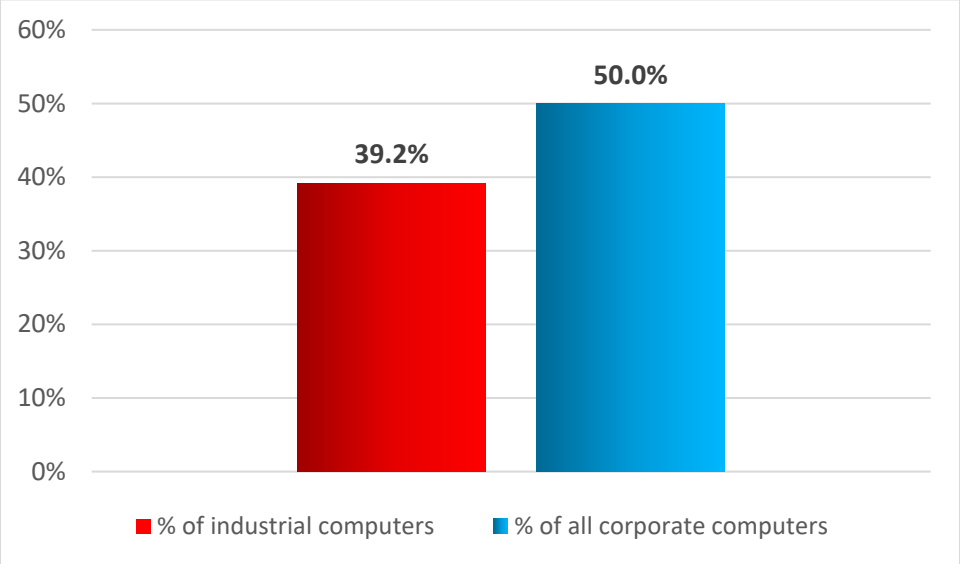
This group includes computers that run Windows and perform one or more of the following functions:

- Supervisory Control and Data Acquisition (SCADA) servers,
- Data storage servers (Historian),
- Data gateways (OPC),

- Stationary engineer and operator workstations,
- Mobile engineer and operator workstations,
- Human Machine Interface (HMI).

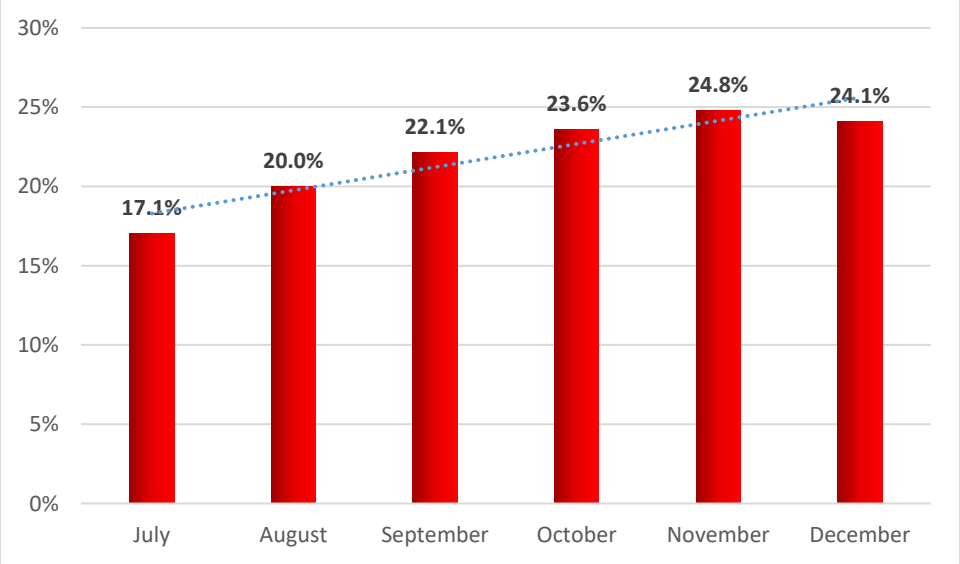
The group also includes computers of external 3-d party contractors, SCADA vendors and system integrators as well as internal SCADA administrators.

Note that the percentage of industrial computers attacked is lower than that of corporate computers as a whole.



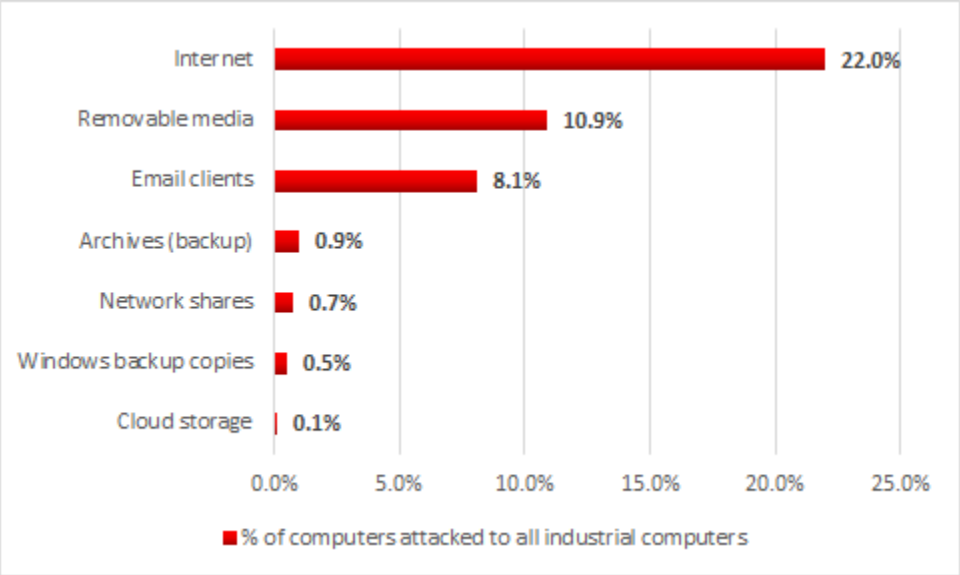
Percentage of industrial computers and all corporate computers attacked (second half of 2016)

Every month, an average of one industrial computer in five (20.1%) is attacked by malware.



Percentage of industrial computers attacked by month (second half of 2016)

Sources of industrial system infection



Sources of threats blocked on industrial computers (second half of 2016)

According to our data, in the second half of 2016 malware downloading and access to known malicious and phishing web resources was blocked on 22% of industrial computers. In other words, one industrial computer in five faced the risk of online infection at least once during that period.

Unlike corporate office networks, which have a stable Internet connection, the frequency with which industrial computers connect to the Internet can vary significantly. Some computers in our sample (about 50%) connect to the Internet on a regular or permanent basis. Others connect to the Internet no more than once a month. Consequently, these machines have a lower risk of infection: during the second half of 2016, only 6% of them encountered online threats. Note that this figure is lower than that for corporate users as a whole (18.2%).

It should be noted that Internet access restrictions can vary significantly for computers on the industrial network and computers that make up the industrial network's infrastructure. In most cases, ICS servers and the stationary workstations of engineers and operators do not have always-on direct Internet access, apparently due to limitations imposed by the industrial network in which they are located. Internet access can be provided during maintenance.

On the other hand, the computers of system/network administrators, developers and integrators of industrial automation systems, as well as those contractors who connect to the industrial network directly or remotely (e.g., to provide monitoring and technical support), are not just connected to the industrial network with its inherent limitations but can freely connect to the Internet.

In our view, these computers are in the highest risk group. This is confirmed by the numerous incidents related to attacks (targeted or accidental) on industrial enterprises that have taken place in recent years (for example, see this and this).

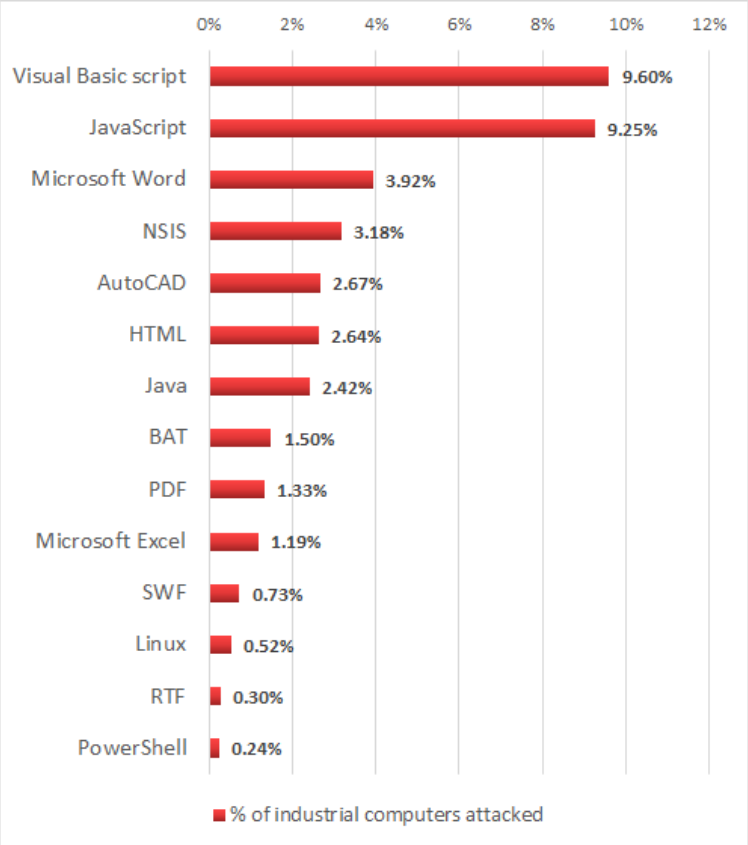
In practice, a network's limitations and specific features cannot always shield industrial computers and their users from external networks and systems. Computers from network with limited access to external resources can often connect to the Internet via mobile phone operators' networks using mobile phones, USB modems and/or Wi-Fi routers with 3G/LTE support.

It is worth noting that on 0.1% of industrial computers malware was detected in the local folders of cloud file storage services. Such folders are automatically synchronized with the cloud storage when the computer connects to the Internet. When a storage is infected from a computer that has access to it (e.g., the user's home computer), infected files will be automatically delivered to all the devices connected to the storage service.

Removable media are the second-biggest source of infection on an industrial network. In the second half of 2016, malware was detected on 10.9% of industrial computers when removable media were connected to them.

Importantly, in the ranking of malware detected on industrial computers, attacks on a high percentage of industrial computers were associated with malware of the following classes: Virus, Worm and Net-Worm (see below). Malware in these classes uses removable media and network folders as its main distribution channels. Since malware often hides its presence in the system by infecting existing files or using similar names – it may take the user a long time to realize that files are infected. (The same approach is used when distributing malware via network folders.) The user may create protected data archives containing these files. In addition, infected files can be saved in file system backup copies created by the operating system.

Malicious email attachments and malicious scripts embedded in message bodies were blocked on 8.1% of industrial computers. In most cases, attackers use ordinary phishing (emails that, as a rule, mimic messages from banks, delivery services, etc.) to catch the user's attention and hide malicious intent. Most commonly, malware is distributed in such malicious emails in office document formats – such as MS Office and PDF – rigged with malicious scripts and/or exploits for vulnerabilities in the relevant applications.



Platforms used by malware to mask itself and avoid detection (second half of 2016)

Note that to avoid detection, as well as masking malicious software and hiding all traces of infection, attackers also use small downloaders written in JavaScript, Visual Basic Script and Powershell that are launched using command line parameters for the relevant interpreters.

Geographic distribution of attacks on industrial systems

TOP 15 countries based on the percentage of industrial computers attacked:

	Country*	% of systems attacked
1	Vietnam	66.1
2	Algeria	65.6
3	Morocco	60.4
4	Tunisia	60.2
5	Indonesia	55.7
6	Bangladesh	54.2
7	Kazakhstan	54.1
8	Iran	53.9
9	China	53.3
10	Peru	53.1
11	Chile	52.8

12	India	52.5
13	Egypt	51.6
14	Mexico	49.6
15	Turkey	46.2

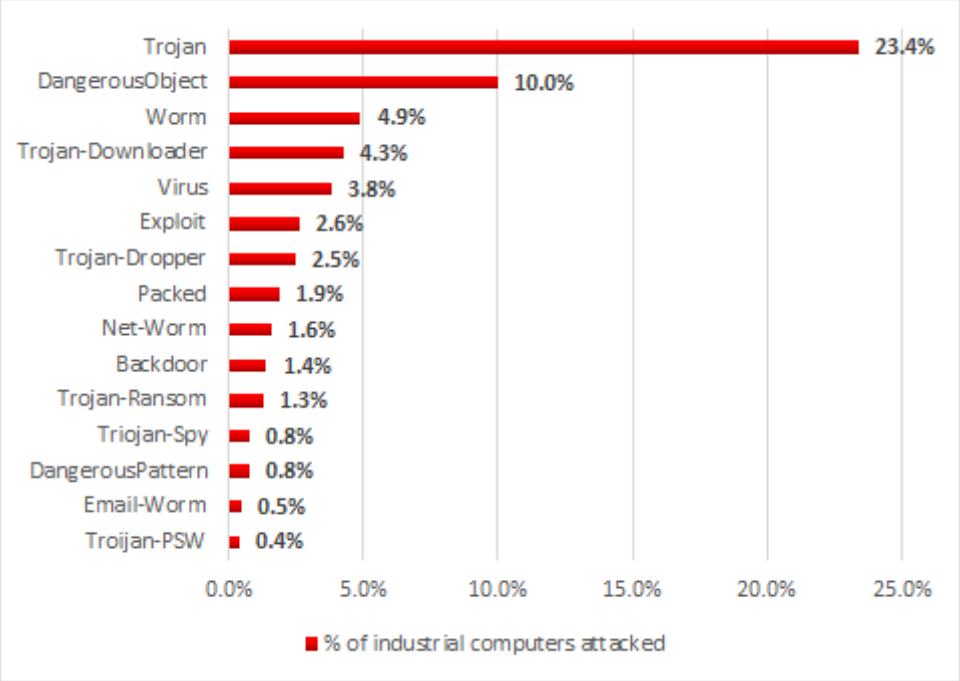
* The calculations exclude countries in which the number of industrial users is insufficient to obtain representative data.

Malware in industrial automation systems

In the second half of 2016, about 20 thousand different modifications of malware representing over two thousand different malware families were detected in total in industrial automation systems.

In most cases, industrial computer infection attempts are sporadic and the malicious functionality is not specific to attacks on industrial automation systems. This means that all the threats and malware categories that affect non-industrial companies across the globe are also relevant to industrial companies. These threats include Trojan spies, financial malware, ransomware (including encrypting ransomware), backdoors and Wiper (KillDisk) type programs that put the computer out of operation and wipe the data on the hard drive.

Remarkably, there is very little difference between the rankings of malware detected on industrial computers and those of malware detected on corporate computers. We believe that this demonstrates the absence of significant differences between computers on corporate networks and those on industrial networks in terms of the risk of chance infections. However, it is obvious that even a chance infection on an industrial network can lead to dangerous consequences.



Distribution of industrial computers attacked by classes of malware used in attacks (second half of 2016)

Malware representing the Backdoor, Trojan-Ransom, Trojan-Spy and Trojan-PSW classes poses a particular threat to computers on an industrial network.

Trojan-Ransom. One type of ransomware (Trojan-Ransom) blocks an infected computer and demands that money be transferred to the attacker's account to unblock the computer. Virtually any such program can completely deprive ICS engineers and operators of control over the automation system. At the same time, the ransomware program may have no information about the industrial control system it has blocked. Another Trojan-Ransom variety encrypts work-related documents and files, which, in the case of industrial automation systems, can also result in a loss of control over these systems. For example, San Francisco Municipal Transportation Agency was infected with ransomware in late November of 2016, resulting, among other things, in its turnstiles being blocked. The attackers demanded a ransom of 100 bitcoins (equivalent to about $73,000) to decrypt files and unlock the infected systems.

Backdoor, Trojan-Spy and Trojan-PSW. Malicious programs representing the Backdoor, Trojan-Spy and Trojan-PSW classes are in most cases agents of botnets controlled through the attackers' command-and control (C&C) servers. These programs not only collect information on infected computers, their users and systems connected to the network and send that information to the attackers but can also be used to carry out targeted attacks, because their functionality offers attackers a rich selection of remote control capabilities.

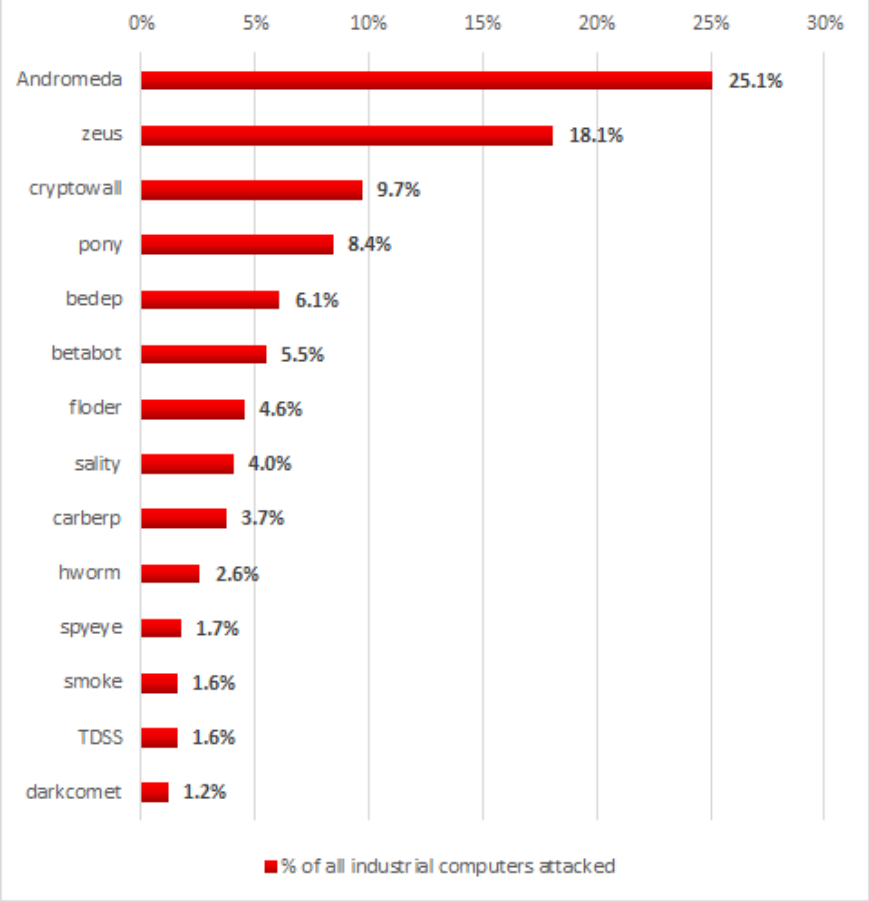
Botnet activity in industrial networks

According to our data, botnet agents (malware that can be remotely controlled via command-and-control servers) and/or traces of their activity were detected on 5% of all industrial computers attacked.

In most cases, botnet agents perform operations that are not specific to industrial systems, such as searching for and stealing financial information, stealing authentication data for various online resources and services, brute forcing passwords, distributing spam and carrying out attacks against specific Internet resources, including denial-of-service (DDoS) attacks.

Although the above operations are not specifically designed to disrupt the work of any industrial system, this use of system resources, as well as incompatibility and/or errors in the code of malicious programs and industrial software can disrupt the network's operation and cause denial of service (DoS) of the infected system and other devices on the network. We saw examples of this while analyzing the security of industrial enterprises in 2016. In addition, if the botnet agent attacks third-party Internet resources (we have seen instances of this, as well), this can create reputational risks for the company that owns the relevant IP addresses.

Most botnet agents are modular malicious programs that can dynamically change their functionality, including changes based on the data about the system sent to the attackers' command-and-control servers. At the same time, data collected by botnet agents by default is sufficient to identify the company that owns the system, as well as the type of system. In addition, access to machines infected by botnet agents is often offered for sale on specialized exchanges on the Darknet.



Distribution of industrial computers attacked by botnet agents by bot families

According to our data, **Andromeda** malware (Backdoor.Win32.Androm) was the most widespread botnet agent family in industrial networks (25.1% of all industrial computers attacked by bots) in the second half of 2016. Bots from this family are often used to distribute spam and to download data-encryption modules to infected computers in order to encrypt data on the hard drive and extort money in return for the decryption key.

Agents of the ZeuS (Trojan-Spy.Win32.Zbot) botnet are in second place (18.1%) based on the number of machines on industrial networks attacked by botnet agents. The main malicious function of programs in this family is theft of authentication data for accessing various online services. After the source code of a malicious program from the Zbot family was leaked in 2011, numerous modifications of malware from this family appeared. ZeuS/Zbot is usually distributed via phishing emails, infected websites that attack known vulnerabilities in browsers and plugins, as well as through other malware.

Malware that makes up the Cryptowall botnet (9.7% of machines attacked) is ransomware belonging to the Trojan-Ransom.Win32.Cryptodef family. Its main function is encrypting files on the hard drive in order to get money from the user in exchange for a decryption key. Malware from this family is mainly distributed through phishing sites and emails with malicious attachments written in JavaScript. After being launched, a script downloads a copy of Cryptodef malware to the infected machine, which encrypts files on the infected computer and blocks the operating system's welcome screen. On the blocked screen, the

malware displays a message demanding that money be sent to the attackers in exchange for a decryption key that will unblock the infected system.

Targeted attacks against industrial companies

According to our data, targeted attacks on companies in different industrial sectors are increasingly common. These are organized attacks that can target one enterprise, several enterprises, companies in one industrial sector or a broad range of industrial enterprises, as in the case of one phishing attack that we detected (see below).

Protecting against targeted attacks is usually a more complicated task than protecting against chance infections. With targeted attacks, in addition to known malware available on the cybercriminal market, attackers can use unique malicious programs developed for a specific purpose, including 0-day exploits. Malware can be launched using legitimate code interpreters (such as Perl, Python, PowerShell), which also makes detecting attacks at early stages more difficult. In addition, as our experience of the past several years shows, it is not uncommon for tools included in publicly available penetration testing frameworks to be used in APT-style attacks.

Targeted attacks nearly always start by attacking the weakest link in the security chain – that is, users. To increase the chances of infecting computers, attackers use watering hole-type attacks and refined social engineering methods. As a result, the employees themselves download and run malware on their organization's computers.

In addition to infecting machines on the corporate network, attackers have other methods of penetrating an isolated industrial network:

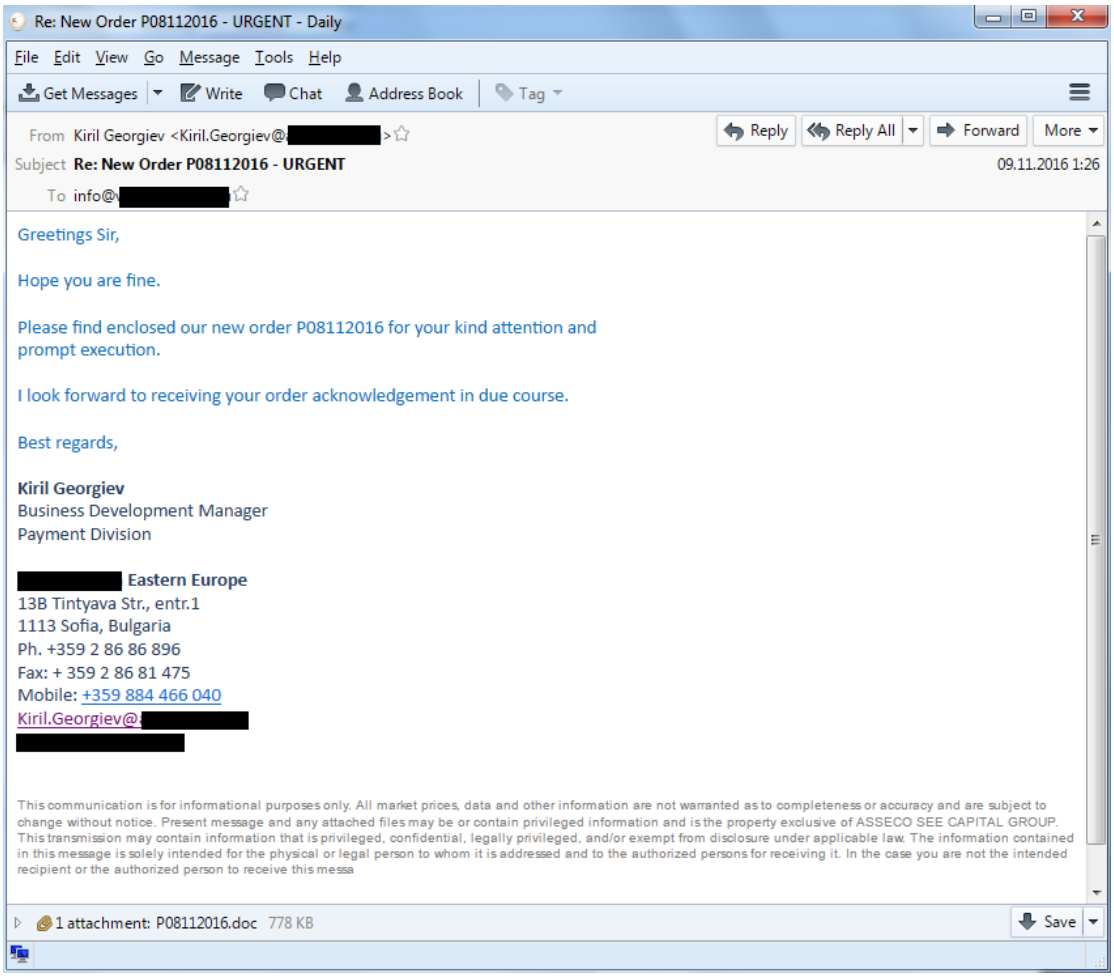
1. Targeted infection of USB media in order to distribute malicious program modules and transfer information between computers, bridging the “air gap”. There have been numerous implementations of this in the past, including attacks such as Stuxnet, Flame, Equation and ProjectSauron.
2. Compromising a local resource on the intranet that can be accessed from the industrial network, or compromising networking hardware. An advanced attacker has many options to choose from: hosting a watering hole script on an internal web resource, spoofing files on the file server or updates distributed by the update server. If necessary, attackers can use a local server as a command-and-control server to control an infected isolated computer. In the case of compromised routers, the attackers are able to “listen” to traffic in order to extract various credentials for subsequent access to computers and resources, as implemented in BlackEnergy2 attacks.
3. Infecting computers belonging to the contractors of industrial companies that connect their machines to the industrial network.

Spearphishing attack against industrial companies

The Kaspersky Lab Industrial Control Systems Cyber Emergency Response Team (Kaspersky Lab ICS CERT) detected a series of phishing attacks which began no later than June 2016 and which are still active. The

attacks target primarily industrial companies – metallurgical, electric power, construction, engineering and others. We estimate the number of companies attacked at over 500 in more than 50 countries around the world.

In all the cases that we have analyzed, phishing emails were sent on behalf of various supplier companies, customers, commercial organizations and delivery services, and contained offers to view updated pricelists, requests to check invoice information, review product prices, resend a supposedly damaged file or receive goods listed in a consignment note.



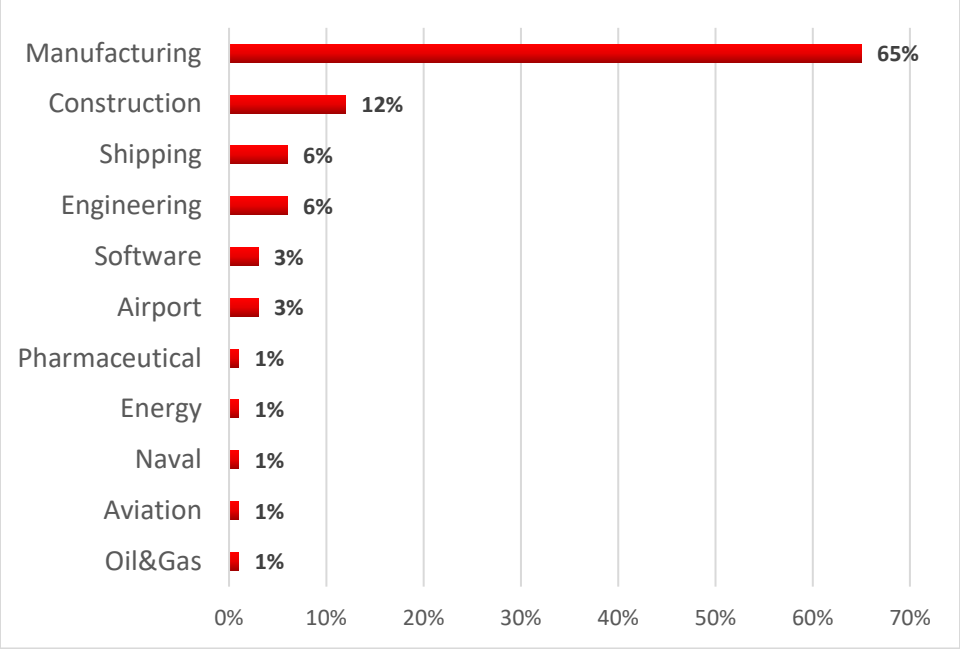
Phishing message sample

The documents attached to the emails were RTF files containing an exploit for the CVE-2015-1641 vulnerability, archives of different formats containing malicious executable files, or documents with macros and OLE objects designed to download malicious executables. The executable files embedded into documents or stored in archives are Trojan spies and backdoors from different families, such as ZeuS, Pony/FareIT, Luminosity RAT, NetWire RAT, HawkEye, and ISR Stealer.

An analysis of the message headers leads to the conclusion that many emails were sent from corporate mail servers that had been infected with spyware designed to steal email account credentials.

None of the malicious programs used in the attack are unique to this malicious campaign – they are all very popular among cybercriminals. However, these programs are packed with unique modifications of VB and MSIL packers that are used only in this attack.

The diagrams below show the distribution of the companies attacked according to industry. The largest number of attacks against industrial companies targeted various manufacturing companies, including makers of industrial equipment, materials and electronics. A significant proportion of the companies attacked are involved in the construction and design of industrial facilities and automation systems.



Distribution of the industrial companies attacked, by industry

Our experience of investigating targeted attacks shows that cyberespionage is often used to prepare subsequent attack stages. We have so far not been able to establish the attackers' goals and motivation with reasonable certainty. The investigation continues.

Note that one quarter of all targeted attacks uncovered by Kaspersky Lab in 2016 targeted, among others, different industries – machine building, energy, chemical, transport and others.

APT attacks

APT (Advanced Persistent Threat) attacks are the most dangerous type of cyberattacks. In many cases they are distinguished by the considerable skills displayed by the attackers, technical sophistication and duration: APT attacks can last for years. These attacks are meticulously thought out and organized and require vast resources. Victims of APT attacks include high-profile individuals, the intelligence services of various countries, governmental and military institutions, scientific organizations, mass media and industrial companies. The victims also include enterprises that are part of the critical infrastructure in different countries.

In the vast majority of cases, the goal of APT attacks is to steal valuable information (cyberespionage). However, there are known cases of attacks using malware designed for industrial sabotage – Stuxnet,

Black Energy, Shamoon Wiper (1, 2), StoneDrill. These attacks were intended to carry out sabotage at the enterprises being attacked and, as a consequence, at disrupting production and business processes.

Conclusions

The research carried out in the second half of 2016 by Kaspersky Lab ICS CERT experts clearly demonstrates a number of trends in the evolution of industrial enterprise security. A summary of these trends is provided below.

1. We have seen stable growth in the percentage of industrial computers attacked since the beginning of our observations, highlighting the importance of cybersecurity issues.
2. The IT threat landscape for industrial systems is increasingly similar to the threat landscape for corporate networks. This is promoted by the active integration of these two types of networks using a set of technologies and architectural solutions, as well as by the similarity of usage scenarios designed to optimize processes and improve manageability. This trend is not likely to change. Consequently, we can expect not only the emergence of new threats specifically designed for industrial enterprises but also the evolution of existing, traditional IT threats, which involves their adaptation for attacks against industrial enterprises and physical world objects.
3. Isolation of industrial networks can no longer be considered an effective protective measure. The proportion of malware infection attempts involving portable media, infection of backup copies, use of sophisticated schemes for transferring data from isolated networks in complex attacks – all of this demonstrates that risks cannot be avoided by simply disconnecting a system from the Internet.
4. The approach of industrial software vendors to closing vulnerabilities and the situation with fixing known vulnerabilities at enterprises is by no means reassuring. The vast majority of industrial enterprises remain vulnerable to computer attacks for years.
5. The emergence of large-scale malicious campaigns targeting industrial enterprises indicates that black hats see this area as promising. This is a serious challenge for the entire community of industrial automation system developers, owners and operators of such systems, and security vendors. We are still remarkably languid and slow-moving in most cases, which is fraught with dangers under the circumstances.

Kaspersky Lab Industrial Control Systems Cyber Emergency Response Team is a special Kaspersky Lab project that will offer the wide range of information services, starting from the intelligence on the latest threats and security incidents with mitigation strategies and all the way up to incident response and investigation consultancy and services. In addition to the latest intelligence about threats and vulnerabilities, Kaspersky Lab's Industrial CERT will share expertise on compliance. Being a non-commercial project, ICS CERT will share information and expertise to its members free of charge.

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