Security

CERT Orange Polska 2017 Report

Smile.
Together we will
be safer.

The report was developed in cooperation with Integrated Solutions, the supplier of modern ICT solutions

Table of Contents

1. Introduction

Billions of events processed per month, thousands of security incidents, multigigabytes DDoS attacks, spectacular vulnerabilities, more and more sophisticated phishing campaigns… In such publications as the report, you could indefinitely show numbers and information that increasingly keep hitting the news of top media outlets. Regardless of how often we do it though, they will still remain numbers and headlines. Something that is well read – but is it actual essence of IT security?

If Orange Polska customers do not see the notifications of the malicious software that concern them, it means that our job was done properly; that the majority of threats were stopped before they reached their computers or smartphones. If it is not the case, CyberShield still won't allow the threats to communicate with cybercriminals and send them sensitive data or encrypt the device, together with handing you the information how to get rid of the infection. While looking for fresh IT security news and information how to protect yourself, you will find the https://cert.orange.pl/ website to – contrary to the well-known proverb – be the wise Pole BEFORE the damage happens. Effective and transparent security are our constant aims.

IT security from Orange Polska's view is a continuous process, improving the existing solutions and looking for the new ones.

IT security is not sophisticated firewalls, antivirus software, it isn't even the CyberShield. Limiting the security to specific solutions is the first step to losing the war with cybercriminals. They do not waste time. Carelessness of individual internet users as well as small companies and enterprises translates to enormous money to be picked up, exceeding at least for the last few years the world's earnings from drug trafficking. IT security from Orange Polska's view is a continuous process, improving the existing solutions and looking for the new ones. It is the rising number of professional services we offer – quite often they are less expensive and more effective to take advantage of over 20 years of experience, than to invest one's money to build own security solutions from scratch. Last but not least, it is building awareness of various user groups, including children and teenagers. Entry level to digital world lowered a long time ago, so even the youngest ones have to be both protected and educated, so ”digital natives” could enter the adulthood aware not only of advantages, but also the risks of their „connected lives”.

What did the world of cyberthreats look like in 2017 from Orange Polska's point of view? It is time to immerse yourself in the 4th edition of our annual report.

Jean-François Fallacher
President of the Management Board
Orange Polska

2. Year 2017 – a summary

If we were to sum up the year 2017 in cyber-security in one word, it would be "ransomware", pronounced in many ways and many contexts. Relating to companies and individual users alike, not only on expert websites, but more and more often in mainstream media. Demanding ransom – another trend which has implicitly permeated from the offline world into our existence in the digital world.

Tens of thousands of screens around the world, many of them connected with public use: cash machines, information boards at train/bus stations and airports – in the middle of May, information appeared on all of them concerning… a necessity to pay a ransom. What has been seen by ordinary people, however, was only the tip of an iceberg. It was what could not be seen that was most dangerous. Attacked were car manufacturers, ministries, local authorities, telecommunications companies, railway in Germany and Russia, hospitals, banks, universities... On the one hand, we have financial losses and a real danger to people traveling by the rail or even hospital patients. On the other hand, we have to deal with surprise and fear, when we become aware that our ordinary daily routine can be disrupted by cyber-attacks. Let us not forget about imagination, which later can simulate even the most grievous scenarios.

Ransomware it's not only attacks on companies. For a regular internet user – until he sees the effects caused by WannaCry with his own eyes – ransomware concerns hard drive of his computer, and personal files. The idea behind ransomware has been best described at the Security Case Study conference by Mikko Hypponen, one of the most charismatic legends in the field of security.

– Once, a criminal thought: "All right, stealing data from businesses is one thing, surely it will be bought by the victim, or by the competition. But who will buy data stolen form an ordinary internet user? Hmm, himself actually!"

Pictures, family mementos, important documents that we are working on at home, diplomas, our own artwork – we all know how many files do we accumulate on the hard drives of our PC's. Despite the increasing popularity of cloud services, and the fact that the data from our computers can be uploaded to them automatically, many of us still keep it on the drive out of habit, oftentimes in one copy. The effect is then especially painful – if the files encrypted were e.g. pictures of our children, there will not be many who will hesitate to pay the ransom. Such occurrences can be confirmed by the fact, that the ransomware "business" earn this way over one billion dollars a year!

Somewhat in the background of the mainstream discussions on ransomware, the topic of cyber-weapons creeps along more and more often. Very popular, although impossible to definitely confirm, are theories that the goal of WannaCry and Petya/NotPetya was not financial gain at all. Why? The creators of the first one earned only around 200 thousand USD, whereas e.g. CryptoWall earned 325 million (!) USD. Their role was to cover the traces left after other, more serious cyber-attacks, financed by governmental institutions. What can be worse from the knowledge that we have been attacked, but we do not know by whom then? The fact... that we actually do not know what was stolen.

Why is all this possible at all? Because we still do not treat the internet serious enough. Many among us, who witnessed the birth of the global network, still cannot cultivate the awareness that the internet ceased to only be a tool of entertainment, and threats have moved, where a significant part of our lives has been moved. On the other hand, for a great part of the so-called "digital natives", the internet is a natural environment. Therefore, as we do not look everywhere in search of a thug while walking the streets, as in the web, we do not smell deceit everywhere. As a result, still a large percentage of internet users are fooled by the more and more sophisticated sociotechnical tricks, especially since the criminals are also constantly polishing their technique. An evil, hooded man breaking into the server room? Such things only happen in the minds of Hollywood screenwriters. Usually the offender prepares a clever piece of phishing, and sends it out to a specifically profiled group of people. If he wants to break into your company – he will always find someone on social media, who will be careless enough to get him profiled sufficiently and make him click on the maliciouse-mail. In addition, the offenders will hit the company with a DDoS attack, to hide its true aim in the resulting mess.

Still a large percentage of internet users are fooled by the more and more sophisticated social engineering tricks, especially since the criminals are also constantly polishing their technique.

This is why it is worth knowing what is going on in the world, being aware of the risks and our own weaknesses, and if all that fails – giving into the hands of experts.

Below, we present data relating to incidents processed by CERT Orange Polska in general, and divided into categories.

2.1 Incidents processed by CERT Orange Polska

Efficiency in detecting and processing computer incidents is the basic criterion in evaluation of reaction teams. In order to provide the quickest, and most effective, CERT Orange Polska constantly monitors events within the network which is the field of our activity, basing upon a well-organized telemetric base. Basing on its range, it may be assumed that the field of reaction of the security team includes networks and devices of the entire country.

In 2017, the number of system events registered monthly by the CERT Orange Polska team exceeded the threshold of 10 billion, which means over a billion more than in the previous year. The automated environment functioning within the borders of CERT OPL allows detection of security incidents, which deviate from the established norm (anomalies), and anticipated system and user activities. There were almost 148 thousand registered anomalies in 2017, a thousand of which were classified as incidents, and required managing by our experts. In total, CERT Orange Polska had processed 12 029 incidents in the year 2017 (17 199 incidents in 2016).

Monthly averages for 2017

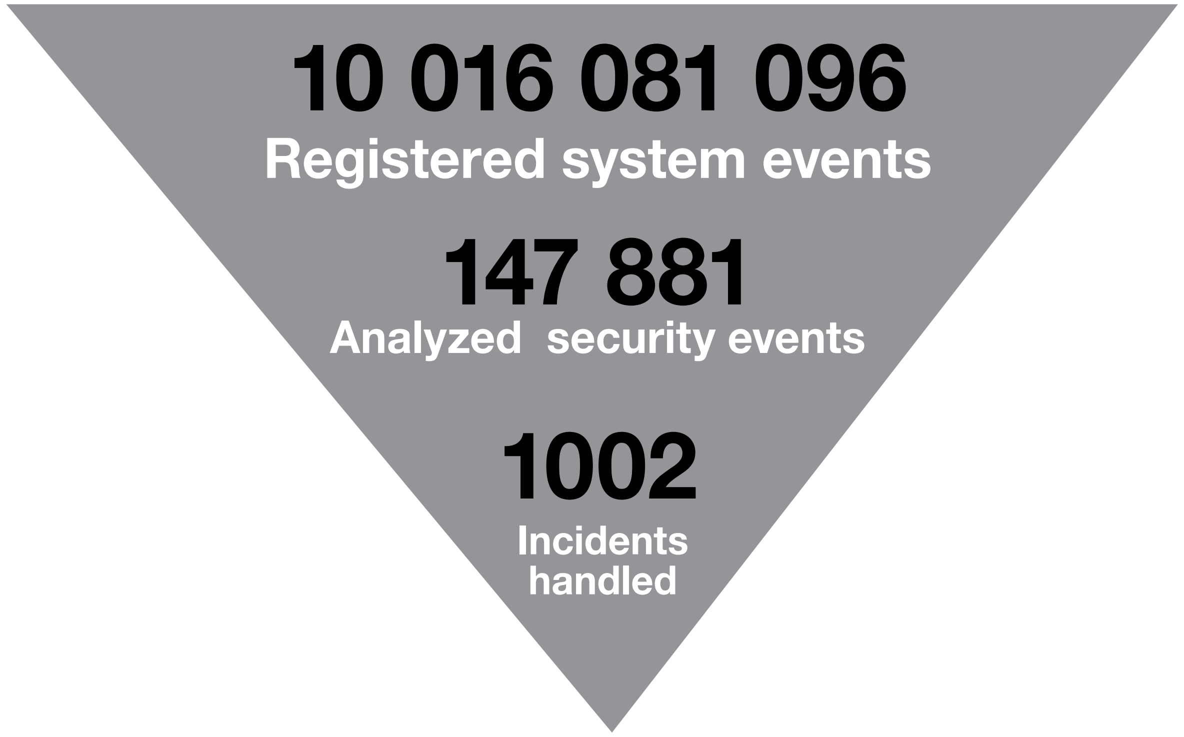


Figure 1 *Inverted pyramid of decomposition of events and incidents handled by CERT Orange Polska per month*

[1] System event should be understood as an event describing the functioning of the system.
[2] Security events are understood as those from among all events, which describe the status of an ICT system's security.

> **In 2017, the number of system events registered monthly by the CERT Orange Polska team exceeded the threshold of 10 billion – over a billion more than in the previous year.**

2.2 Incidents by category

In this chapter, we will present a percentage distribution of the incidents processed by us, divided into categories and in comparison with the previous year. Among the incidents observed, the ones from the abusive content had clear advantage, similarly to the previous year – combined, they constituted almost half (48,9%) of all incidents. They were followed by attacks on resource availability – 19,5% (20,3% in 2016), intrusion attempts - 14,7% (a decrease from 20,31% in 2016) and violations connected with gathering information - 6,9% (5 pp less than in 2016).
The categories of the least frequently occurring incidents were malicious code - 5,5% (6,73% in 2016), and online scam – 2,9 % (1,17% in 2016).

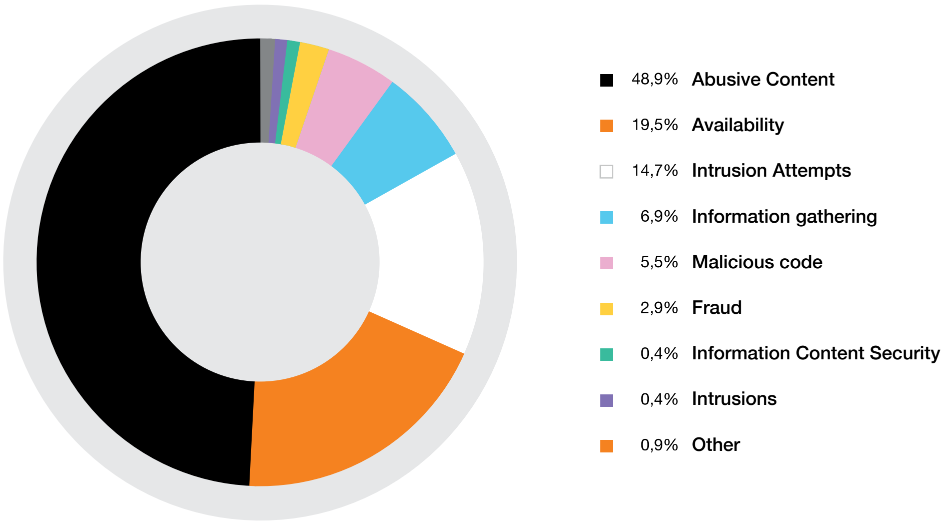


Figure 2 *Percentage distribution of incidents processed by CERT Orange Polska in the year 2017.*

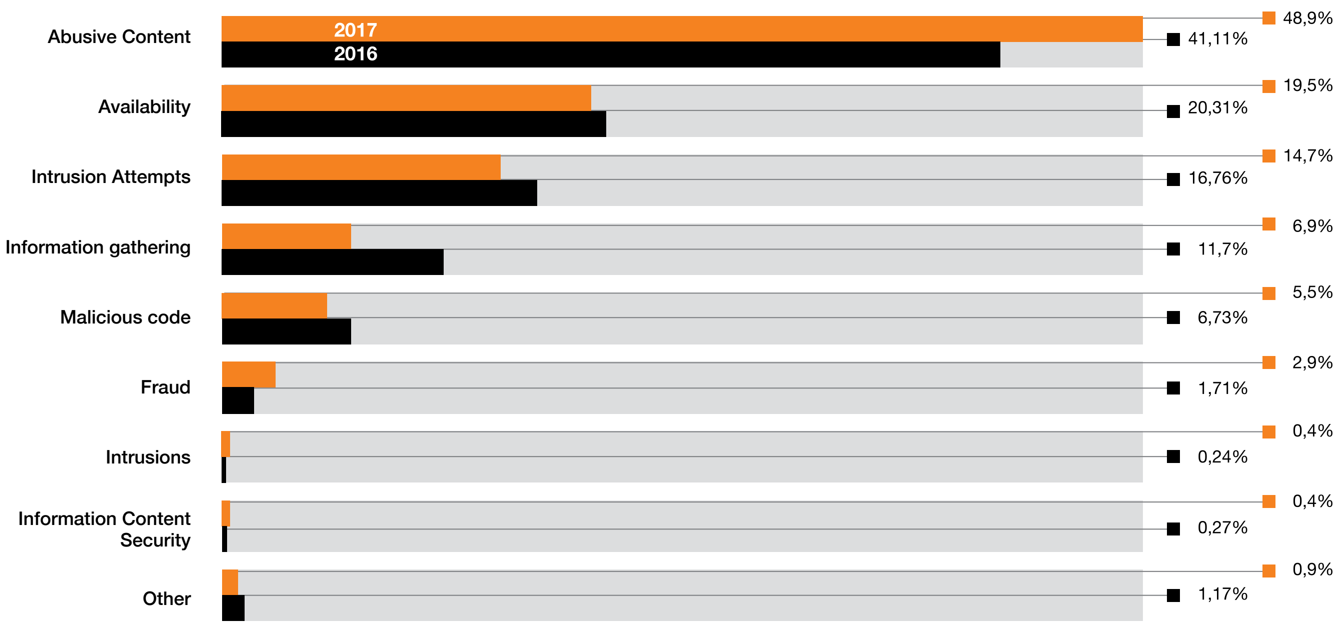


Figure 3 *Percentage distribution of incidents processed by CERT Orange Polska in 2017, and the comparison with the year 2016.*

According to the next graph, the time of incident occurrence distribution in 2017 is irregular, and differs from the previous year. Most of all, a decrease in the number of incidents between May and September can be noticed. Renewed increase in the number of processed incidents was observed in October.

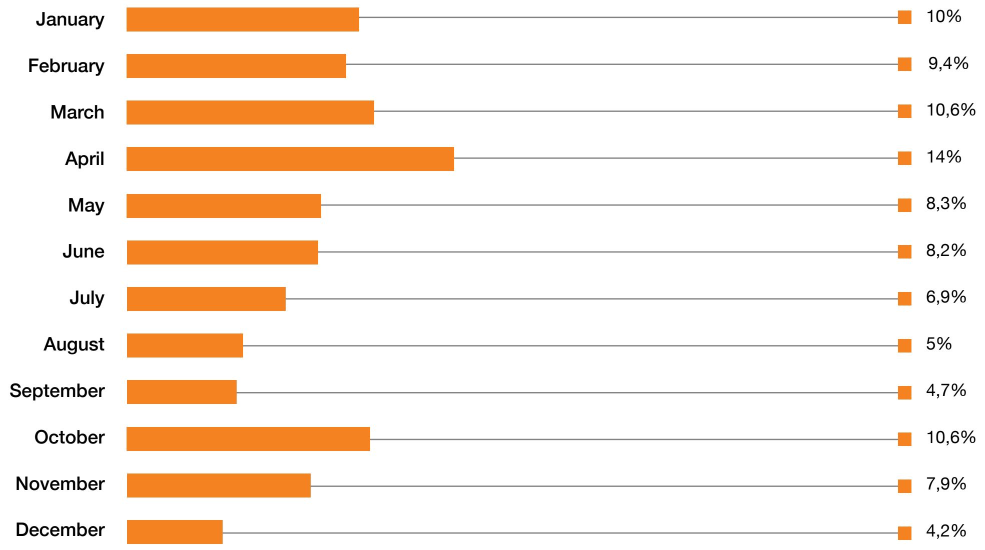


Figure 4 *Monthly distribution of incidents in the year 2017.*

2.2.1 Abusive content

Within this category, analysed are mostly incidents connected with distributing spam, copyright violations, (e.g. piracy), and dissemination of content forbidden by law (e.g. racist propaganda, child pornography, or ones promoting violence). Those cases belong into the largest class of incidents. In the year 2017 they constituted for 48, 9 % of all incidents. Particular intensification of incidents from this category was observed in April, while the lowest number of occurrences took place in October.

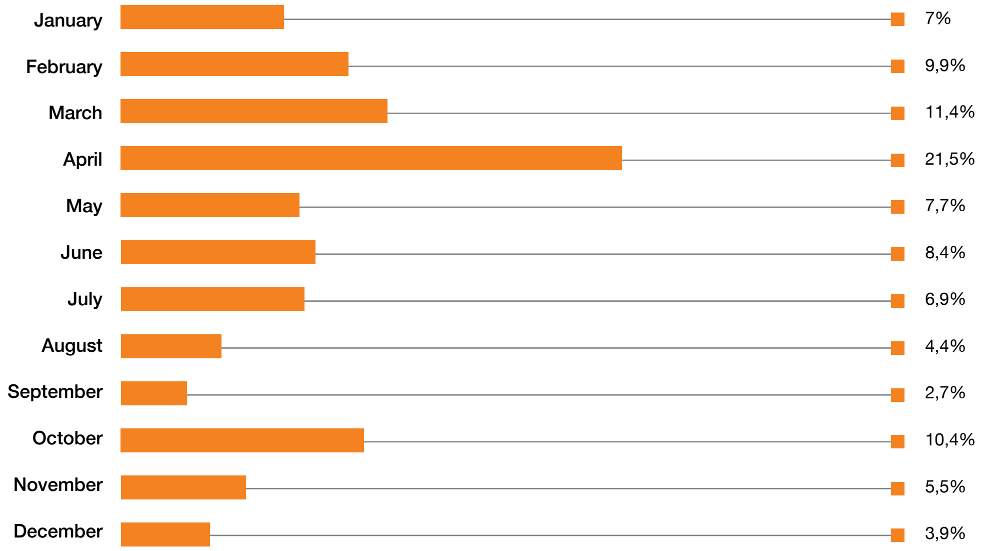


Figure 5 *Monthly distribution of incidents from abusive content category in the 2017.*

Security violations in the field of resource availability should be understood as a kind of incident connected with disruptions in functioning of systems or networks, aiming to lead to their malfunction or blockade (DDoS/DoS type attacks). Important here are also sabotage campaigns, the goal of which was dealing damage to data, disruption of a process, or destruction of an ICT system. In 2017, CERT Orange Polska classified 19,5 % incidents in this category. The largest number of attacks on resource availability was observed in October.

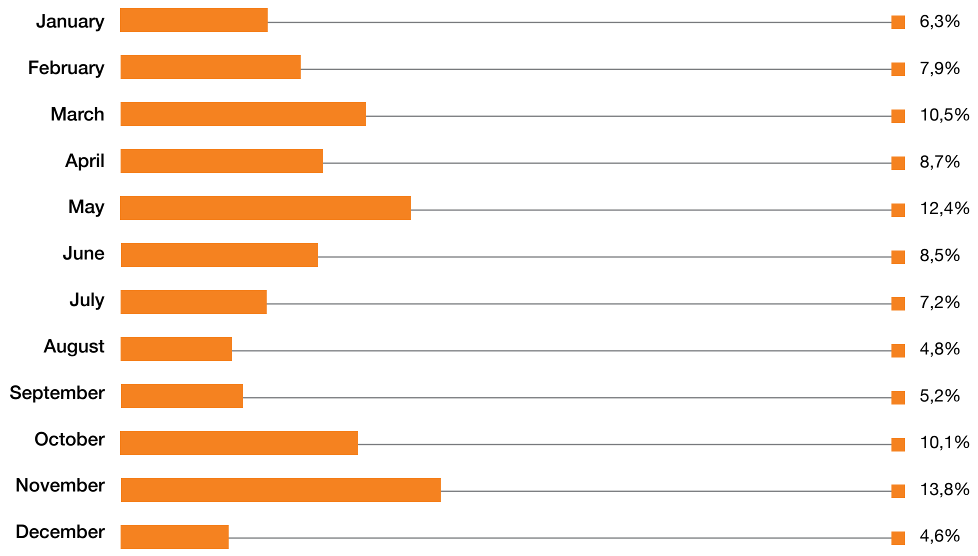


Figure 6 *Monthly distribution of incidents from the attack on resource availability category in 2017 .*

2.2.2 Intrusion Attempts

The security team of Orange Polska classifies intrusion attempts as incidents connected with exploitation of vulnerable stations' (work stations, components, networks) systems in order to gain access to them, or take over them. Intrusion attempts also include attempts to compromise a system by logging into it. In 2017, the largest number of cases from this category occurred in January (almost a quarter of all occurring that year), and in the further months, the percentage distribution remained rather regular, but not greater than 10 %.

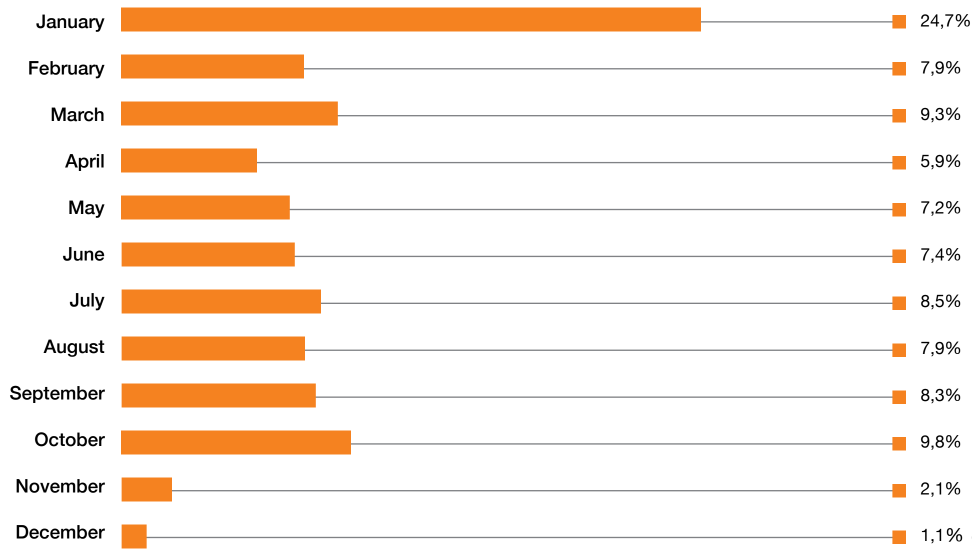


Figure 7 *Monthly distribution of incidents form the intrusion attempts category in 2017.*

2.2.3 Information Gathering

Those violations include events such as port scanning, unauthorized monitoring of a network, or attempts to gather information about a system and users through phishing campaigns. Orange Polska processed most of these incidents in the beginning of the year. The monthly distribution of that kind of violations was stable, and it did not exceed 10% per month.

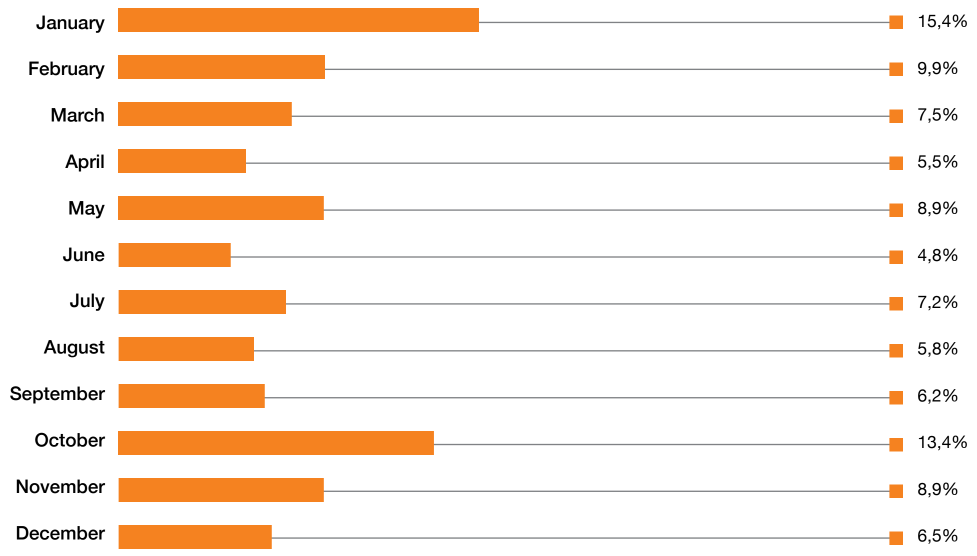


Figure 8 *Monthly distribution of incidents from the violations connected with gathering information category in 2017.*

2.2.4 Malicious code

According to CERT Orange Polska, incidents connected with malicious code include infections, threat distribution, and hosting of C&C servers. The security team processed most of the malware incidents in the fourth quarter of the year.

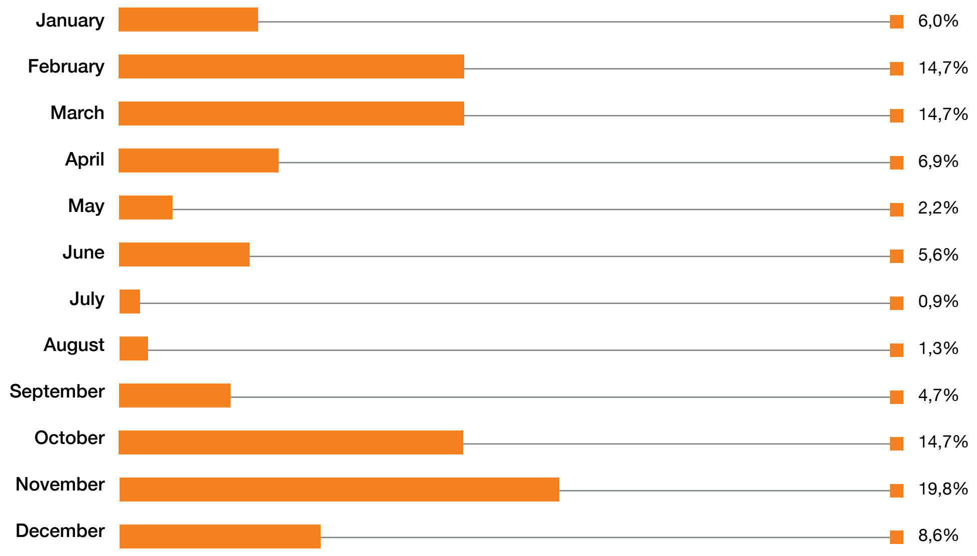


Figure 9 *Monthly distribution of incidents from malicious software category in 2017.*

3. The most important threats and events in Poland and worldwide in 2017 - an overview.

January

02.01

Forged profile of Media Expert on Facebook

During the Christmas season, a new kind of scam appeared on Facebook, in which the cyber-criminals pretended to represent a chain selling RTV. The users sharing the false profile were lured with a free shopping coupon. Links that were supposed to lead to website revealing the contest's winners were malformed in such a way, that the users opening them were redirected to their own profiles. The „winner" had only just to fill a prize receipt form, doing which required them to send two Premium-type SMS messages, for the total cost of over 50 PLN.

02.01

Disclosure of data of Orange customers

The operator attached a PDF file containing unremoved data of other users to an e-mail of appreciation to the customers. The data was only seemingly hidden, and possible to read if copied to a text editor. In the end, the scale of the incident was small, as the data of only four users was disclosed.

16.01

A successful method of attack on Gmail accounts

Gmail users received phishing messages from hacked e-mail accounts of their acquaintances. Clicking on a link or a picture attached in the message redirected the users to a counterfeit log-in site, confusingly similar to Google's site. This way, the attackers gathered authorization data, as well as expanded the list of their potential victims. To avoid this kind of scenario, verification of address bar in the browser was necessary. The campaign was highly effective, and the cyber-criminals were able to trick even technical specialists.

17.01

Impersonating CEIDG

Using the wrongly configured CEIDG (Central Registry and Information about Business Activities) domain, the cyber-criminals were sending out e-mails demanding payment from business owners.
The fraudsters took advantage of the fact that the governmental domain ceidg.gov.pl did not have the SPF (Sender Policy Framework) service field configured, so there were no obstacles to sending forged correspondence.

February

02.02

Phishing campaign targeting courier companies' customers under the guise of an undelivered parcel

The CERT Orange Polska team has identified two new phishing campaigns. In the first of them, the offenders impersonate the UPS courier company. An important notice is that the e-mails are written in flawless Polish language, which could make the recognition of the deception significantly harder. The attachment itself was not malicious, so running it did not cause detection by antivirus engines. The contents of the attachment, however, consisted of a link leading to a website where the user, after re-writing a displayed piece of code, could download a receipt. After downloading the alleged receipt and running the file, a malicious code (Ransomware.Matsnu aka Rannoh) has been executed, encrypting the user's data and displaying a payment demand.
The other campaign used counterfeit notifications about parcels undelivered by the DPD Company. The goal was to convince the user to click on a link leading to the supposed details concerning the parcel, which in reality caused downloading malicious software.

03.02

Hacking into Financial Supervision Activity

This time, the attackers used the watering hole mechanism. They took advantage of trust put in governmental institutions, as it was the Polish Financial Supervision Authority's website that has been infected. Traces left by the offenders in the software used, as well as analysis of network traffic suggested different countries of origin of the attacks.
It was known that a Cyrillic keyboard has been used among other things, however the hackers' "working hours" pointed towards the United States. The attack itself went on the following way: the offenders integrated basically undetectable malware into the Polish Financial Supervision Authority's website. The malicious software was a spyware, and was supposed to send user identification data of the people using this website.The spyware checked if the person using the PFSA's website was present on the previously prepared list of targets, and if they were, asked the offenders whether to attack, or not. The attacks did not happen automatically – the targets were carefully selected, and not every user visiting the PFSA's website was even suggested as a target. The data available indicates that strategic plans, marketing concepts and other data sensitive to the financial sector were stolen. At the same time, it is hard to determine what exactly has been leaked, because the data had been encrypted by the offenders prior to transfer.

04.02

Hacking of the largest hosting service in the Tor network and sharing the data

In the beginning of February, it has been announced that Freedom Hosting 2 (the successor of the well-known Freedom Hosting shut down by the authorities), the largest hosting service in the web, containing approx. 20% of all hidden websites, has been attacked by anonymous attackers, who disabled all the websites it contained, and publicized their database in the web. The database counts over 2 GB, including over 800 websites, also Polish ones. The website of the discredited hosting service has been replaced, and an instruction describing how did the intruders managed to gain access to the hosting's database was put onto it.

24.02

Security gaps in Cloudflare allowing leaks of sensitive data from websites using it

It was made public that the well-known security researcher from Google, Tavis Ormandy, revealed information about an enormous gap in Cloudflare (used by over 5,5 million websites) during his investigation. As a cause of that gap, sensitive user data has been leaking, including passwords, cookies, IP addresses, tokens, personal information, private messages, pictures, and encryption keys.

March

02.03

Malware campaigns under the guise of delivering a receipt from Orange Polska

CERT Orange Polska recorded an increase of phishing attacks connected with impersonating addresses form the „orange.pl" and „neostrada.pl" domains. The messages title suggested that the file attached, was a receipt for the allegedly ordered services. Not all messages contained text though, which could convince the victim with even more efficiency to open the Trojan-containing attachment.
After the installation, the Trojan downloaded subsequent elements of malicious software.

11.03

Malware campaign aimed at PayU users

A campaign impersonating an on-line payment service provider, characterized by its professionally handled socio-technical aspect. A counterfeit message, informing about the payment status for a cinema ticket included an attachment with malicious software "vjw0rm". The Trojan could install other threats without the user's knowledge. Businesses were the cyber-criminals primary targets.

March

15.03

Hacking Twitter accounts and using them for political actions

Political action on Twitter calling to boycott the Dutch government by Turkey was possible due to compromising the Twitter Count application – a service allowing tracking statistics connected with user accounts. This way, the hackers broke into many opinion-forming accounts, like, among others the one of the Forbes magazine, and of Graham Cluey, a journalist dealing with cyber-security. The intercepted accounts always shown the same propaganda message aimed against Holland.

23.03

Hacking of the jakdojade.pl website

Due to an unpatched vulnerability Apache Struts2 in the older version of the popular ”jakdojade.pl” service, the cyber-criminals gained an opportunity to replace the website. The break-in was committed by a hacking group from Pakistan. The situation was managed shortly after detecting the incident.

April

04.04

Website of the so-called Islamic State spreads malicious software

The Amaq, information agency which serves the Islamic State in spreading their propaganda, has been intercepted by hackers affiliated with the Anonymous group. They did not shut down the site itself, though. The hackers tampered with the website's code and implemented a malicious Flash plug-in update file, which then infected users visiting the site. Upon entering the Amaq website, a notification about an outdated version of the Adobe Flash Player plug-in was displayed. Installation would be downloaded immediately after the user clicked the OK button on the pop-up window. The file which was downloaded this way from the Amaq website was a so-called dropper, which downloaded malicious software onto the target's computer just upon being installed. It is estimated, basing upon unconfirmed data, that the malicious software has been downloaded by approximately 600 users.

07.04

Mailing campaign impersonating DHL under the guise of delivering a parcel

The CERT Orange Polska team informed about phishing attacks aimed towards customers of the DHL courier company. The counterfeit messages sent out by the offenders encouraged the user to click on a link and download a “delivery status report” file. That was the way “infostealer”, a kind of malware stealing information used for authorization in web applications such as social media, e-mail accounts, or banking services, found its way to the user's device. Apart from losing their data, the users affected by this phishing attack were also exposed to infections with ransomware.

10.04

Wonga customers' personal data leak

In the first decade of April we were informed about a “possible unauthorized access” to the data of Wonga.com loan service customers. There might have been as much as 25 thousand victims among the loan provider's customers in Poland. The Wonga.com company notified its clients via e-mail, that the unauthorized access might concern data like first and last name, address, phone number, social security number, and identity cars number. Wonga underlined that despite the attack, it was by no means confirmed that the data has been transferred. The company did not reveal any detailed information about the breach, saying only that all the errors have been fixed.

21.04

Mailing campaigns impersonating Delta Air Lines

In the announcement from the 21st of April, CERT Orange Polska team informed about another malware campaign with the use of phishing attacks on the Delta Air Lines customers. The counterfeit messages encouraged the victim to click on a link and download “flight ticket order status information”, which when opened, attacked the computer with malicious software. Upon clicking the link, the victim was redirected to a website, and a file with name structure: DELTA_ticket_username.doc was downloaded. Opening this document injected the malicious code ”hanictor” into the memory, under the name of the system process verclsid.exe. In the next step, the process referred to several domains from which it downloaded further instructions, including URLs, from which it was supposed to download the proper malware, the task of which was to steal authorization data to popular web services.

April

25.04

The hacking of HipChat and sensitive data leak

By the end of April, information was released about the hacking of an online chat service allowing to create private text, voice, and video chat channels as well as to store data - HipChat. The service was immensely popular and used for communication in various project teams. Among the data stolen from the users there were their usernames, e-mail addresses, and the hashes of their passwords. It was good luck within bad luck, that the passwords were stored using the bcrypt hash function, which causes process of encrypting them to be quite lengthy. Unfortunately, the offenders could have also gained access to the names of the channels, their topics, and conversation history of specific channels. The announcement of the company providing the HipChat service highlights that the error, which the criminals took advantage of, existed within an external library.

May

04.05

E-mail campaigns under the guise of scans from multifunction printers

An attack targeted at the users of multifunction printers with the function of sending e-mails with the printed files. Instead of downloading the file with the printed file, the user downloaded malicious software, which upon opening, infected the device and searched the workstations for passwords and Windows Mail files in browsers such as Mozilla, Chrome, IE, and in instant messengers.

08.05

Mailing campaigns impersonating PKO BP bank

Internet users were receiving e-mails containing no text, but containing a ”confirmation of payment” PDF attachment. The file possessed malicious functionality – by connecting to a counterfeit PKO BP server, it downloaded unwanted software to the user's work station.

10.05

Mailing campaigns impersonating Orange customers

A phishing campaign, in which cyber-criminals were sending out messages suggesting an alleged necessity of returning a certain sum of money.

14.05

Global attack of the WannaCry worm

This kind of malware quickly paralyzed ICT systems all around the world. WannaCry was taking advantage of a vulnerability in the SMBv1 protocol of Windows operating systems. The campaign's main tool was the Eternal Blue exploit, developed by the American NSA agency. The Exploit's existence has been made public due to activities of the Shadow Brokers group. Because of the breach, it was possible to execute malicious code on the user's workstation, and encrypt all his files. The campaign infected over 200 thousand computers in 150 countries in total. The WannaCry campaign has been put to an end thanks to blocking of one of the domains, with which the malicious program has been communicating in the process of propagation.

16.05

Increase in the activity of the Njw0rm Trojan

The CERT Orange Polska team noticed an increase in the activity of a dangerous trojan called ”Njw0rm”, allowing criminals to take full control over the infected computer, including theft of logins and passwords, executing any chosen system commands, as well as receiving further updates from the botmaster.

June

05.06

Phishing on iCloud

In the beginning of June, CERT Orange Polska noticed extraordinary activity concerning a phishing campaign aimed at iCloud service customers. In the e-mail messages the attackers suggested an unauthorized access attempt to the user's account, which was allegedly blocked for security reasons. There was a PDF file attached in the message, supposed to guarantee security during the re-verification of the user account. The link from the document led the victim to a website impersonating iCloud, which demanded verification data.

12.06

Sensitive data leak of several thousand patients of a Polish hospital

Data of 50 thousand patients has leaked from one of Polish hospitals. The data was available for download and usage for any internet user, who stumbled upon the server's address. There was no authorization system guarding the data, and it was located on publicly available servers (information that could be downloaded from them included social security numbers, address, blood typeand results of some tests, and in case of employees, also identity cards data and/or bank accounts). On the same server, there were also found music albums, pirate versions of popular programs, and crypto-currencies mining programs.

14.06

Leak of several thousand CV of Wroclaw University students

It turns out that Polish universities do not care for the ICT security of their students well enough. After a number of cases connected with authorization in library systems, where both username and password were the student's index number, around 11 thousand CVs and cover letters have leaked from the Wroclaw University. All those documents were stored on an unprotected server of the Wroclaw University Career Centre, and were accessible to anyone who would "look" in the right place.

26.06

Phishing attack impersonating GIODO

In June, a phishing attack aimed at legal community took place. E-mails were sent to law firms, allegedly coming from the Inspector General for Personal Data Protection, informing about an upcoming inspection in the institution. The message itself contained no text, and an attachment, which upon opening encrypted the victim's computer. It remains unknown how many people fall victim of those criminals.

28.06

Global attack of the Petya/NotPetya ransomware

In the beginning it was thought to be another ransomware, but after further research it turned out to be a wiper – malicious software supposed not to only encrypt data, but also to destroy it by overwriting it. The Ukrainian company M.E.Doc, specializing in accounting software, was the first to be attacked. Software update has been replaced on the company's servers, and all businesses making tax settlements in Ukraine have to use this software.

By updating software from that brand, other businesses were infected. Later on, the malicious software propagated on its own, taking advantage of a vulnerability in the SMB protocol, as well as thanks to tools from the Microsoft Corporation - PS exec, WMIC.

It was because of them that the malicious code could spread to other computers, including the ones with fully updated operational systems.

The malware activated with a few dozens of minutes of delay, and the infection occurred in two phases. The first of them replaced MBR and forced the machine's restart, and the second one carried out the proper encrypting. The attack has been observed all over the world, but its main target was Ukraine. Among the affected institutions there were banks, mobile network operators, national energy providers, as well as the power plant in Chernobyl and the aircraft manufacturer Antonov. Additionally, hundreds of private businesses fell victim to the attacks.

According to Microsoft, 12 500 computers were infected in Ukraine, and the traces of the malicious software were found in over 60 countries.

July

12.07

Phishing attack aimed at PKO Leasing customers under the guise of receipts

PKO Leasing customers were receiving messages with counterfeit receipts attached, compressed into ".rar" type files. The sender was hiding behind the leasing. efaktura@pkoleasing.pl address, taking advantage of errors in the domain's SPF settings. Opening the attached file resulted in infection of the user's work station.

19.07

Phishing campaign aimed at energy sector companies

Energy sector companies in the United States were targeted by a phishing campaign conducted by hackers from the Dragonfly group, also known as the Energetic Bear. The messages sent contained Microsoft Word files attachments, which were stealing authorization data from the work stations. The cyber-criminals also used the watering hole technique, carefully analyzing the data of the employees with the access to industrial control systems. According to the report from the American government, there were no significant violations of the critical infrastructure.

25.07

REDISBAD customers' personal data of the leak

Due to wrongly configured web application in the online store "redisbad.pl" there was a leak of the customers' personal information (first and last name, phone number, e-mail, address). According to the experts' estimations, over 200 thousand records could have been disclosed.

29.07

Discovery of the cyber-attack on Equifax

In July, employees of Equifax, an American consulting corporation monitoring credit reports have discovered that a serious data leak occurred in their company. Among the leaked information, there were social security numbers, birth dates, and driving license numbers. The range of the break-in could include even 143 million of American citizens. The cyber-criminals took advantage of a vulnerability in Apache Struts, which was supporting an Exuifax web application. The vulnerability has been known since March 2017. The event was widely publicized in the media, as well as initiated a series of significant changes in the structures of the company itself.

31.07

The Global Internet Forum to Counter Terrorism meeting

The key players of the social media industry – Twitter, Facebook, Microsoft and YouTube have met on the first workshop of the Global Internet Forum to Counter Terrorism. In the three-sided talks hosting state administration, businesses, and non-governmental organizations, it has been established that the Forum's competence, would include i.a. information exchange concerning traces left by terrorist organizations.

August

01.08

Attack aimed at HBO and the leak of popular TV series 'Game of Thrones'

The servers of the HBO company fell prey to a hacking attack. Among the stolen data, as stated the attackers were the script to the new season of 'Game of Thrones' series. The offenders responsible for the attack claimed that that are in possession of a huge amount of materials (around. 1, 5 TB of data). They threatened that more portions of it would be released to the web if the company would not pay the ransom they demanded.

04.08

RDP attacks targeting Polish companies

There has been noticeable increase in system login attempts via RDP services – a protocol allowing communication with graphic terminals in Microsoft Windows (Terminal Services). The service has been available in all Windows operating systems since version Windows 2000 through the program remote desktop connection. When someone successfully logged in, the data on the computer would be encrypted, and a request for ransom appeared. The number of users affected by this attack remains unknown.

August

16.08

Facebook scam exposing users to costs

A new kind of scam appeared on social media. The victim received a message from a friend, with a link to a picture which looked as if it has been made into a video. Depending on what kind of system the victim was using, either fake file hosting services were displayed, charging money for downloading the file, or a certain amount of money was charged by sending a premium-type SMS, after the victim attempted to play the video.

18.06

Cyber-attack attempts on the G20 group. Russian APT group suspected

Russian-language attack aimed at the participants of the G20 meeting. That kind of attack was based on the discovery of a new JavaScript dropper, a backdoor called KopiLuwak. Malicious software posing as a PDF file attachment was being propagated through a phishing e-mail message. Clicking on the attachment caused an actual PDF to open, but malware was being installed in the background. The document itself seemed to be a genuine invitation for signing up to a meeting of the G20 work group, and had been probably stolen from a person authorized to receive it. After the installation the malicious software allowed the attackers to gain full control over the system.

September

10.09

Error in the OLX service allowing anyone to download other people's receipts

Due to a simple error on the OLX website, popular online marketplace, any internet user had access to receipts of the service's customers. The receipts contained the customers' address data. The possibility to take advantage of the unwanted functionality has been promptly removed by the administrator.

15.09

Phishing campaign in LinkedIn

Accounts overtaken in the LinkedIn web service were used by the cyber-criminals to carry out a malicious phishing campaign. The messages were being sent out via "InMail", a build-in functionality of a popular website used for communication between its users. The content of the e-mail included a link to a counterfeit website reminiscent of some of Google's services (as well as of other digital suppliers). That way, the hackers gathered the victim's authorization data. The scale of the attack is unknown, but it has been revealed that one of the overtaken accounts had 500 contacts within its business.

20.09

Malware campaign aimed at mBank customers under the guise of confirmation of bank transfer

This time, a phishing campaign was aimed at mBank customers. The cyber-criminals were impersonating the bank, and sending out messages with infected attachments, which imitated bank transfer confirmations. After the user opened such an attachment, he was asked for permission to connect witha server, which then downloaded ransomware to his computer.

22.09

European Union's Cybersecurity Package

The European Commission publicized the project of the so-called cyber-security package, a proposition to regulate the matter of cyber-security on the European Union level. The package includes i.a. the Commission's directions concerning coordinated reaction to computer incidents in case of critical situations, as well as the matter of extending ENISA's (European Union Agency for Network and Information Security) mandate.

28.09

CERT Orange Polska observed a phishing campaign consisting of e-mails impersonating the DHL courier company.

The cyber-criminals used the spoofing technique to lure the users into clicking on a link which was allegedly leading to a parcel tracking website. Going to that page equaled running an installation of malicious software.

October

10.10

Phishing campaigns aimed at iOS users

German blogger working on cyber-security topics, Felix Krause detected a gap in the iOS system, due to which criminals can create basically undetectable phishing attack. iPhone users could have been affected by an attack in which they were asked for authorization data to the iCloud service. Users of those devices are often asked to perform this kind of authorization, so a request like this does not raise any doubts. Meanwhile, it turned out that with the use of certain vulnerabilities, a message like that can be made to display while attempting an attack. The problem was that in iOS any application can ask for password, not just the system applications. Password to iCloud grants access to basically everything that the user has sent to the cloud, as well as allows installation of applications and system updates. To verify who in fact was requesting a password from us, it was only needed to push the Home button. If the window was being displayed by the operating system, it remained visible. If by a malicious application, it would disappear.

Dismantling of a criminal group stealing personal information from telecoms

The Polish National Police Headquarters informed about the arresting of employees of a certain telecom, who were stealing i.a. customer personal data from their company. The offenders gained unauthorized access to the operator's database, and shared the data with a marketing company working for a rival operator. It should be noted that the security measures used for protection of the ICT systems were not compromised, and that monitoring devices running in the system have detected the activity – it was that the person authorized to access the systems has misused it. The criminal charges concern 700 thousand personal and IC data records. The information stolen included i.a. first and last name, phone number and address.

17.10

KRACK - the attack to which almost all Wi-Fi devices are vulnerable

The KRACK (Key Reinstallation AttaCKs) attack allowed the attacker eavesdropping on transmissions in WiFi networks, which prior to its publication were considered to be well-protected. That vulnerability was extraordinary, because it did not only relate to certain devices, but to the whole WPA2 protocol. The basic attack vector is aimed against the 4-Way Handshake sub-protocol, carried out during the user's connection to the network. The attacker gained the ability to re-use the victim's already used keys. Carrying out a successful attack required that the attacker remained within range of the victim's Wi-Fi, and only traffic not secured by higher-layer protocols could be eavesdropped on. The attack did not store the password to the device itself, so there was no need of changing it. The KRACK vulnerability has been repaired, but adequate patches should be installed on devices with Windows 10, and most of the ones running on Windows 7 and 8/8.x.

23.10

IoT Reaper – new Internet of Things exploit

A new IoT devices exploit has appeard. In October, a huge botnet was found, consisting of Internet of Things devices. Among the vulnerable devices were kitchen appliances, gadgets, and cameras, but also some industrial machines. Devices from brands such as GoAhead, D-Link, TP-Link, AVTECH, NETGEAR, MikroTik, Linksys, and Synology were identified as targets for the attacks. The number of devices intercepted by malicious software has been increasing regularly up until the end of October.

26.10

Global attack of the Bad Rabbit ransomware

New malicious software appeared which managed to paralyze some subjects of the media and transport sector, mainly in Russia, Ukraine, and Bulgaria, in relatively short time. The first reports suggested a threat similar to the Petya/NotPetya malware, but the similarity was restricted to the file encryption method. According to the reports, over 200 institutions were attacked, such as the subway in Kiev, the airport in Odessa and the Russian press agency Interfax. The ransomware was infecting computer systems through a fake Adobe Flash Player update. Most of the infected sources included websites in the ".ru" domain. The offenders demanded a ransom of 0,05 BTC for the decryption of the files. The situation has been mostly contained, mainly thanks to the creation of a so-called kill-switch, which prevented the application from running on the victim's device.

November

09.11

OVH servers' crash

The global crash of the French hosting provider OVH's servers caused paralysis of a significant number of websites and web services. Two independent incidents took place in w Strasburg and Roubaix. Due to this unfortunate coincidence, both locations have been down, which affected internet users all around the world, but mainly the ones from Europe. The datacenter in Strasburg experienced issues with electric power, and in Roubaix there was a problem with optical fiber network, which connected the datacenter to the nodes allowing further connection with networks located in Paris, Frankfurt, Amsterdam, London and Brussels. The problem stemmed from a software error on the network equipment, which caused loss of configuration and trouble with connection the works to restore the full functionality took several hours.

20.11

The Dotpay campaign

A Polish malware campaign consisting of e-mails impersonating the Dotpay payment operator has reached Polish internet users. The victims were receiving e-mails calling for payment of a relatively low amount. The messages had Flotera ransomware attached to them. The cost of getting the data back set by the offenders amounted to around 100 USD.

21.11

Data leak from Uber

The international transport company Uber reported a huge data leak, which took place in 2016. In October last year, unknown attackers hacked the company's servers and stole data of 57 million customers and employees. The data included surnames, e-mail addresses of 50 million passengers, and 7 million personal data records of drivers. Two cyber-criminals gained access to the GitHub repository used by Uber's programmers, from where they have stolen employees' authorization data. They used them to log into Amazon Web Services, from where they have stolen the data archive, and then demanded ransom, threating that the data would be disclosed. The company's former management decided to pay the ransom of 100 thousand USD.

24.11

The Scarab virus

Department of the National Police of Ukraine informed about the Scarab virus spreading through the largest spam botnet "Necurs". Experts from cyber-security field have found over 12,5 million e-mails containing files with the newest version of the ransomware. After a successful encryption of files and folders, the virus automatically created and opened a text file named "IF YOU WANT TO RECEIVE ALL YOUR FOLDERS BACK, PLEASE, READ IT.TXT". The IT.TXT file appears on the computer's desktop. The sum of the ransom for decrypting the files has not been revealed, but the attackers warned that any delay would result in its increase, until the victim made contact with them via e-mail or BitMessage.

28.11

Critical vulnerability in the MacOS system

A vulnerability in the MacOS X High Sierra system has been detected. The error may potentially compromise the user's personal data. A criminal having a physical (or remote) access to the machine, may access it and modify the files without possessing the administrator's credentials. The users exposed to the threat were the ones who have not enabled the access to guest account, and the ones who have not changed the root password. Apple released an appropriate patch.

December

05.12

Theft of wallet contents of Bitcoin owners

The online largest crypto-currency mining service, Nicehash, informed all users about a security breach. Unknown perpetrators have managed to compromise Nicehash and steal all bitcoins from the main wallets of the service. The incident has been detected after dozens of complaints from Nicehash's customers, concerning the loss of their bitcoins. Users whom the announcement concerned have reported, that their bitcoins were redirected to a wallet storing 4 736, 42 bitcoins. The Nicehash's website has been unavailable since 5th until 20th of December. It seems, however, that the funds have returned to their rightful owners.

07.12

Data leak of the AI.type application's database

Data of 31 million AI.type virtual keyboard users has leaked after the creators of the popular application have left the database server without any security measures. The problem affected users of smartphones running on the Android system. Information gathered by the application inclided i.a. first and last name, e-mail, user's location, and also their contact list, which expanded the range of damage. The free version of AI.type was gathering much more information, including device serial numbers, name of the ICT operator, IP addresses used when connected to a wireless network, and when the user of the faulty software used Google applications, especially detailed data from public profiles, including pictures.

09.12

Data leak

During a scan of the deep web for stolen data, IT security experts have discovered a single file containing a database of 1, 4 billion e-mail addresses and passwords. It was the biggest database leak written in plain text up to date. Among the data, 10,5 million addresses of Polish internet users were found. The analysis showed that the stolen passwords came also from governmental domains, such as: .gov.pl, .policja.gov.pl, .mon.gov.pl, .sejm.gov.pl, and .prezydent.pl. The database in question contained data from several hundred data leaks, the well-known and undiscovered ones alike.

18.12

HTTP servers' vulnerability in IoT

Researchers have discovered a vulnerability in the web code of the GoAhead servers, built into IoT devices. The vulnerability might have been potentially used to take over the gadgets. The NIST report states that the vulnerability marked as CVE-2017-17562, allows the attacker to inject his code to the vulnerable device, taking over it, and using it to spy on its user. The threat may concern from 700 thousand to 2 million devices.

”

The costs of cyber-attacks are still relatively low, whereas profits to achieve outnumber them by tens or hundreds of times.

4. Trends for 2018

We can be sure that the year 2018 will not change much in the field of phishing campaigns. It should be expected, that cyber-criminals will continue attempts to compromise ICT systems using social engineering, which becomes more and more elaborate, and the process itself has multiple stages. APT (Advanced Persistent Threat) type attacks will become especially dangerous for critical infrastructure subjects, with emphasis on the banking sector. As in many cases, also this time financial reasons are an inseparable factor.

As the year 2017 has proven, malicious campaigns aimed at this sector are simply profitable. Attacks are also being carried out with the use of social media services such as Facebook or LinkedIn with increased frequency. The threat, however is not only limited to scam, which lures us into sending costly premium-type SMS messages, but it also includes the possibility of user profiling in order to prepare a precise attack on e.g. an employer. The development of spying software for mobile devices will surely be a great support for this kind of operations.

As predicted in the last year’s analysis, incidents with the use of ransomware type of malware, were one of the main threats in the cyberspace, the best example of this being campaigns like WannaCry and Bad Rabbit. Unfortunately, everything seems to indicate that in the year 2018 this trend will persist. Businesses as well as individual users are still willing to pay ransom to the offenders. The destructive potential of malicious software cannot be underestimated, what could have been witnessed this year with the NotPetya campaign. The worm, which has been initially classified as ransomware, turned out to be a wiper after it had been established that the offenders are unable to restore the encrypted files.

It is quite possible that the Personal Data protection Regulation (RODO) entry into force will not prevent the increase in the number of incidents concerning data leaks.

Due to high fines that the watchdog body can impose on subjects, we may actually see an intensification of attacks on personal information databases. Such attacks may be connected with unfair competition, as well as attempts to threaten the subjects by the offenders with reporting the leaks to appropriate organs. There is a risk, that RODO will only make the practice of asking for ransom more common.

As predicted in the last year's analysis, incidents with the use of ransomware were one of the main threats in the cyberspace.

More and more data, both public and private is processed using cloud computing, which results in significant market demand for security services dedicated to such solutions Everything seems to indicate that in the year 2018 this field will be an important part of the cyber-security landscape. It is not difficult to imagine that incidents such as the OVH crash will increase in numbers, but will also be caused by deliberate actions. Consequences of such operations, as it could be seen with the French cloud service provider, may be very serious.

As in the previous year, further increase in attacks using Internet of Things is expected. Low security of "intelligent" devices, along with the possibility of using them in DDoS attacks reinforces the conviction, that the incoming months will not be an exception in this matter. It is worth mentioning, that campaigns of this kind can be very expensive, and relatively difficult to conduct on a greater scale. This is why they are expected to become more popular as a service in this specific field, especially due to the fact that they are becoming of greater interest to national bodies (the so-called state sponsored operations).

ICT threats will increasingly occur in correlation with threats stemming from manipulation of information. A hacking attack results in not only unauthorized access to resources, but also generates effects in the information environment. Many a time, publication of stolen correspondence is meant to introduce materials into the environment, where it becomes a tool for further manipulation. It should be assumed that the trend of interfering into both systems and information environment will pose a greater and greater threat to the personnel and security systems. The process of manipulating information has the potential to not only shape the results of an ICT attack, but it may also be used to create, and take advantage of a vulnerability in ICT systems, through initial shaping of an ICT environment.

It should also be concerned more and more popular way of making money at the expense of computing power of network and computer users. CERT Orange PL lately observed a new infection type – BitCoinMiner, malicious software which uses computer resources to generate cryptocurrencies for cyber criminals. Another way for mining bitcoins is to use scripts on webpages, which activate when user run the browser - of course without their knowledge and consent. So far, threat emer

Artificial Intelligence and cyber-security – a challenge of incoming years?

Rogue machines taking over the world are still science-fiction, but the Artificial Intelligence of machines, devices and systems plays an increasingly important role in the world around us, also in terms of cyber-security. According to the studies available, traffic generated by the internet network is caused by human activity in only 48, 2 %. The remaining part is generated by various kinds of bots substituting human activity. Almost one third of those programs are bots having a malicious influence on cyberspace. They lead disinformation campaigns, distribute so-called "fake news" and initiate DDoS attacks, as well as many other ones of criminal nature, in an automated way. It is worth emphasising, that hacking tools compose 2, 6 % of all network traffic.

The true risk of Artificial intelligence is the fact, that it may be difficult to predict what kind of abilities will it develop without its creator's assistance, and who will make use of this potential. AI may be used for good or ill, it may be responsible for e.g. detection and removal of vulnerabilities, or recognition of suspicious network activities, while filling staff shortages in the cyber-security market. AI's additional assets are its computing capabilities, which are way greater than the ones of any human. When facing dynamically spreading attacks, reaction time matters – an example of that was provided by the ransomware campaigns from 2017 – and Artificial Intelligence may be just the thing to ensure it.

The use of AI may also change the approach from reactive, which is still predominant in security teams, to proactive. Processing incidents on an ongoing basis, hoping that they can be repelled the next time is not enough. Criminals constantly change means and vectors of attack, which will be recognized by AI with much more efficiency. On the other hand, it is to be expected that it will be used for attacks by hackers just as much, e.g. for bypassing security systems or finding.

This means that most probably, the only chance of defence from Artificial Intelligence used for criminal purposes will be to use Artificial Intelligence in the field of security. Surely it will be a classic analogy to an arms race during the Cold War, and it will be difficult to predict who will win. There are scenarios stating, that using AI on a massive scale can lead to unprecedented consequences in the future.

No one is capable of creating feasible, long-term forecast of technological development of society – as for now we can only forecast it in a linear manner, without considering possible developmental leaps. Of one thing we can be almost sure - AI will be excellent at accomplishing goals, but if those goals will not be consistent with the ones of the security sector, we will face a great risk. To provide the basic security, legal regulations concerning responsibility of a creator of a certain solution will be necessary. This kind of approach will allow at least half a chance that creation of such algorithms will be accompanied by serious reflection. This of course, only applies when we assume that the use of AI will always be fully ethical and legal, which seems like quite a utopian option.

So far, threat emerging from BitCoinMiners still remains on a low level (slightly above 2% as CERT Orange Polska data states). However, great popularity of cryptocurrencies and the fact, that some of them gain strength (BitCoin even several times in the recent years) force cyber-security specialists to look deeper into the issue. CERT Orange Polska predicts that such incidents will only intensify in 2018 and become a great challenge for cyber-security experts. It is because the detection of a script digging up a cryptocurrency on a website is not easy for the average internet user.

Artificial Intelligence threats - commentary

dr inż. Paweł Tadejko
Once a programmer, later a designer/analyst, and finally a Software Architect. For over 10 years he has been gathering experience in large IT projects, working for the ComputerLand / Sygnity corporation, in projects created as dedicated solutions for businesses, but also for administration, i.a. the Ministry of Foreign Affairs, Health, and Finance. Designing IT system concepts resulted in the SOA and SaaS architectures ceasing to hold any secrets from him.

Meanwhile he has been working as a Data Scientist, before it became popular. In the year 2009 he got his doctorate from analysis and classification of arrhythmia in the signal of EKG. He used to want to analyse emotion recorded in electrocardiogram, but it ended more down-to-earth, with QRS classification, and anomaly detection using wavelet transform and chosen tools of machine learning. Currently an academic employee at the IT department of the Bialystok University of Technology. As the manager of post-graduate studies, he aims to proof that faculties can indeed be in tune with the market, and when developed with partners from that market, also more practical. A co-founder of a group of enthusiasts – and later an association - Magia Podlasia (pl. The Magic of Podlachia) His passion is photography.

AI has been present in the topics concerning security for a long time, but recently it seems somewhat more pronounced, and not just because of revelations about AI appearing in the media. What is interesting is that it is used on both “light” and “dark” side of the forces operating in the field of security. And as much as the challenges awaiting AI “in service” of security belong to a somewhat different class, the topic is surely is very promising, which we can witness. A confirmation of this is i.a. the fact, that the current fields of research funded by UE - Horizon 2020 – there appeared a category named „Artificial Intelligence & Decision Support” in the “SECURITY” section.

The history of using AI in the domain of security is very old – its roots reach the beginning of the previous century. As much as the first polymorphic viruses can be described as not very advanced, the heuristic methods of anti-virus scanning which appeared by the end of the 90’s, started using Artificial Neural Networks for analysing code of unknown viruses.

The intelligence of viruses, Trojans, and malware may consist in not only mutating of their code to make it harder to detect, but also in other activities connected with the attacks. These can be either mechanisms of bypassing AV, taking advantage of gaps, breaking operating system security, or other techniques meant to keep the malware running and conducting attacks. By the end of the 2000-2010 decade 4th generation of anti-virus systems, which has already been using Artificial Intelligence techniques to learn, and distinguish between “good” and “bad” software, also basing upon its behaviour in the operating system.

A separate category of AV tools are systems basing on anomaly analysis and detection of behaviours deviating from the norm, e.g. anomalies in the use of network protocols. That may be an area, where AI might have the most to offer. With the amount of data transferred in networks, manual analysis concerning detection of violations is impossible. Here come the machine learning tools, which are able to “catch” suspicious events and initially classify them as anomalies, and later eventually as threats. One such example of their implementation is e-mail spam and Intrusion Detection Systems - IDS. Thanks to the ability of learning, AI allows classification of attacks according to known algorithms, but also to new ones, of similar type. IDS of this class can also learn new user behaviours and new attacks. It is machine learning methods that allow them to function in this case without building complicated sets of rules and signatures.

I would not demonize the threats connected with AI just yet, because as much as it can beat the world champion at Go, or the best chess program at chess, it fails miserably at many down-to-earth” problems. Humans have the advantage when it comes to connecting facts, so oftentimes even things considered to be literally a “child’s play” cause AI significant trouble. Still, in the field of anomaly and suspicious behaviour analysis it is second to none. Unfortunately, here also the market abhors a vacuum. If one can teach AI to detect anomalies, maybe attacks could be conducted in such way, that the AI would learn wrong, and fail to recognize anomalies in time? This is how the so called “adversarial machine learning” branch has been born, which is about developing methods to weaken and confuse security algorithms using the AI engine.

Luckily for us, we have a hidden ally in the fight against dangerous systems based on the AI engine implemented in the same computer virus. A program like this requires enormous computing power, while computer viruses need to be agile pieces of code. It is way harder for them to conceal the use of high computing power. Of course an intelligent virus might be a botnet. In such case it can use the computing power of the entire network. And this is the moment when we get to the stage seen in the movies. Let us hope that for a long time, only in the science-fiction ones.

5. Social Media – initial attack vector?

Despite increasing awareness, many users still do not comprehend that the internet became an integral part of our life. Just as our online and offline activities dynamically intermingle, so do threats.

Even without looking at the statistics, it can be safely assumed that if we would remove all network traffic connected to social media services from the internet, it would appear that all network devices suddenly have huge reserves of storage. Since the first version of Facebook went online in February 2004, the number of Mark Zuckerberg's service users dynamically increased, to exceed 2 billion in the June of 2017, including 1, 3 million active users every day (!). The amount of data accumulated on Facebook's servers is approaching 1 exabyte (10^{18}). For many, Facebook is an important part of their lives, an information source, a place where they begin and sustain friendships. And if so – it is also a good "hunting ground" for cyber-criminals.

Despite increasing awareness, many users still do not comprehend that the internet became an integral part of our life. Just as our online and offline activities dynamically intermingle, so do threats. Actually, it is even worse – a thief in the streets can steal what we took with us, whereas the one online, in white gloves can rob us of the savings of our life. Moreover, taking advantage of our carelessness, he has the opportunity to attack our company or employer! Here, the potential range of costs and damage is practically unlimited. In the worst case scenario, it may end in the company's bankruptcy as a result of the amount of refunds paid, or clients resignation.

As for now, Facebook is a leader among the social media, thus most of the threats are related to it, threats of substantial and specific nature, meaning the ones connected with social engineering.
The specificity of social media services focused on interpersonal relations makes us easily cheated by this sort of frauds. Especially, that in a situation where the offenders do not have to create their own malicious software (the supply of ready solutions in the malware-as-a-service model greatly exceeds the demand) can focus on polishing their social engineering skills, that may lead to, specific, dedicated methods of manipulation.

The risk that we will become targets of manipulation using social media is significant. However, from the viewpoint of our employer, our carelessness may lead to far worse consequences, including infiltration of the company network by the cyber-criminals. Why? Knowing where we want to break-in, we search for company employees using e.g. LinkedIn. Next step would be finding their private social media accounts (this is made way easier if the employees put links to their social media profiles, or have a picture there). Then we familiarize ourselves with the victim's interests, and in case of extraordinary carelessness, we may find out where and when does the victim tends to attend. Lastly – in a Hollywood style – we steal his identifier/cryptographic token/phone number, or - avoiding our direct interference, we prepare a phishing attack specifically with the victim's interests or competences in mind, so that they have no chances of evading it.

How to minimize the potential risk? What serves us best is common sense, and being mindful when of browsing the internet. It should be remembered that what we upload to the network will probably remain there forever. It is important to adjust visibility settings – otherwise our activity will be available to view by the whole world. It is also worth considering to separate our public identity from the private one, to make the task much more difficult for the crook.
It is not worth rationalizing that "we are not that important", or "who would attack an ordinary employee", etc. In 2014, an American supermarket chain Target became an infamous figure in the media, after criminals installed malware on its checkout terminals.
The program managed to steal data from several million debit cards (!).

What was the vector of attack? It started form an air-conditioning company servicing several shops in this chain. Of course the story of how the offenders were able to get to the servers sending software to check-out terminals is a whole different one, nevertheless it all started from one ordinary employee...

It is also worth considering to separate our public identity from the private one, to make the task much more difficult for the crook.

Another example is a successful attack on the profile – or friends actually – of Admiral James Stavridis, the NATO Supreme Allied Commander in Europe in the year 2012. The attack consisted of creating a few fake profiles on Facebook, impersonating the Admiral, and then convincing his actual friends to add the offenders to the friend list. The "most important soldier in Europe" was never hiding his fascination with the internet, sharing information and his reflections on the activities of NATO on his public Facebook profile. Being aware of this, the crooks created several accounts impersonating the Admiral, counting in it that his friends, without giving it much thought will conclude that he simply changed his account! When one of them – probably also from the military – indeed automatically clicked "OK", he had instantly given the offenders access to his private data! And eventually, all this could serve as preparation – even after several/several dozen months – of a dedicated attack, not even necessarily at Admiral Stavridis.

[3] http://www.wirtualnemedia.pl/artykul/ilu-uzytkownikow-ma-facebook-dwa-miliardy

5.1 Threats to privacy, how to safeguard against them (FB, LI)

What can we do to feel secure in social networks?

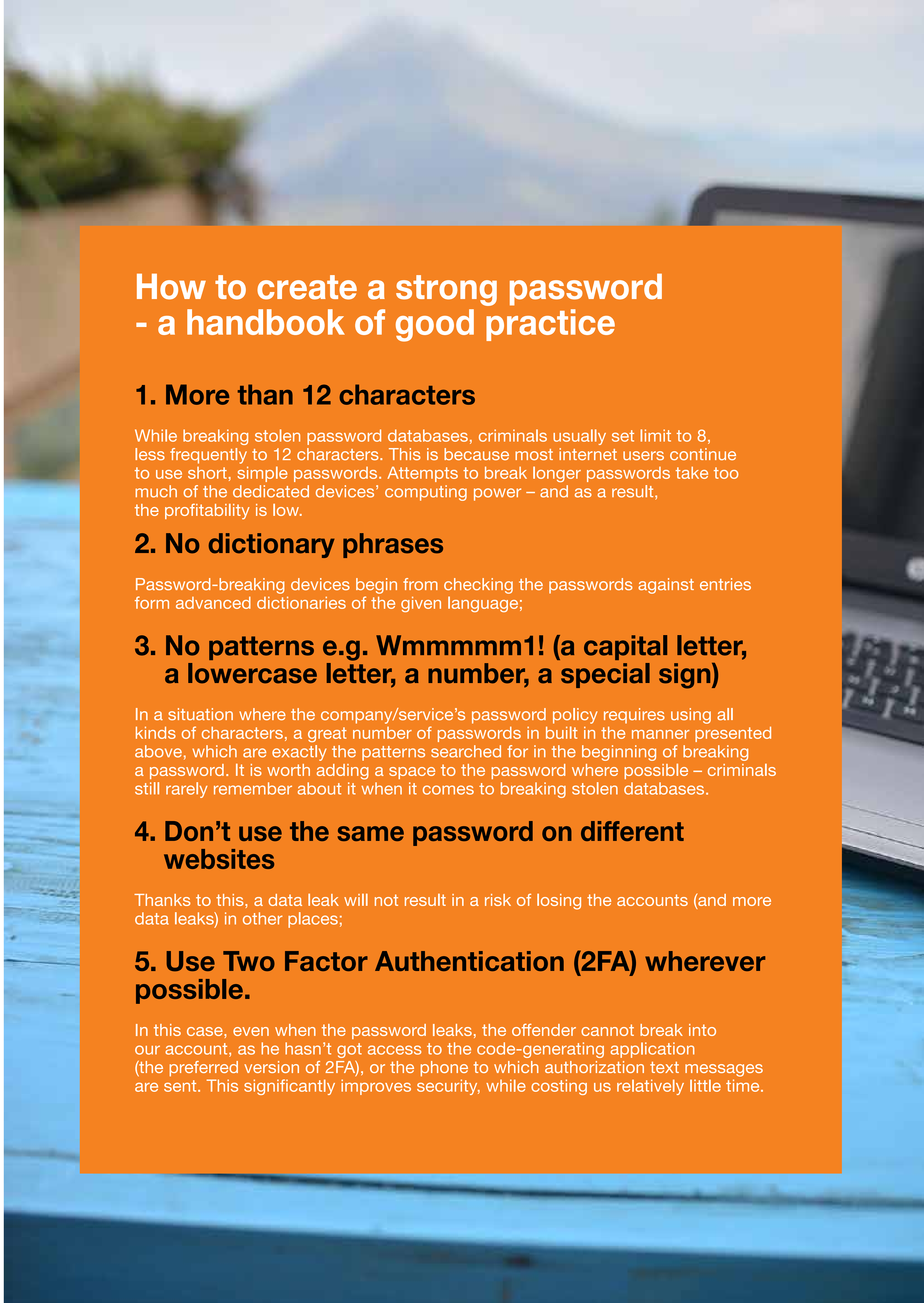
1. Each of the services offers options to modify privacy settings – they are worth using to increase the level of security of the data stored on the profiles.
2. Friend invitations should be approached with caution, as should involvement in social groups.
3. Geolocation data should be used with caution, or even better, completely disabled.
4. Personal information should not be published (birthdate, vacation plans, daily schedule, credit card number, etc.).
5. Suspicious links and posts should not be clicked.

Moreover, anytime and anywhere, we should:

a) Set strong passwords (12+ characters, capital and lowercase letters, special signs, numbers);
b) Keep your software updated
c) Use antivirus software
d) If we are customers of Orange Polska – regularly check your home network using the CyberShield (https://cert.orange.pl/cybertarcza).

5.2 How to create a strong password – a handbook of good practice

The good practices described here are one thing, but most of all we should remember about common sense. It is worth knowing how an ideal password should look like, but most of us, instead of obsessive care for every service we use (oftentimes there are hundreds of them), should start from a simple risk evaluation. A complex, impossible to break password? Definitely when it comes to bank services, systems connected to our job available online and last but not least - e-mail accounts and social media services. In the times of the 2.0 these two groups are also important, because this is where identity theft begins. In case of less important places in the net we can ease up a bit – but not too much.



How to create a strong password - a handbook of good practice

1. More than 12 characters

While breaking stolen password databases, criminals usually set limit to 8, less frequently to 12 characters. This is because most internet users continue to use short, simple passwords. Attempts to break longer passwords take too much of the dedicated devices' computing power – and as a result, the profitability is low.

2. No dictionary phrases

Password-breaking devices begin from checking the passwords against entries form advanced dictionaries of the given language;

3. No patterns e.g. Wmmmmm1! (a capital letter, a lowercase letter, a number, a special sign)

In a situation where the company/service's password policy requires using all kinds of characters, a great number of passwords in built in the manner presented above, which are exactly the patterns searched for in the beginning of breaking a password. It is worth adding a space to the password where possible – criminals still rarely remember about it when it comes to breaking stolen databases.

4. Don't use the same password on different websites

Thanks to this, a data leak will not result in a risk of losing the accounts (and more data leaks) in other places;

5. Use Two Factor Authentication (2FA) wherever possible.

In this case, even when the password leaks, the offender cannot break into our account, as he hasn't got access to the code-generating application (the preferred version of 2FA), or the phone to which authorization text messages are sent. This significantly improves security, while costing us relatively little time.

6. What do children look for on the web?

Almost 16 million attempts to access pornographic websites. Over 100 million blocked entries to websites connected with malicious software, spam, and phishing. Children not manage to enter paedophilia-themed websites. Now you know why it is important to take care of your children's safety in the web.

There was a time when a child's eyes brightened up when it was gifted a ball or a bicycle. Times have changed, though, and we could half-jokingly say that it has gotten easier nowadays. The problem ceased to exist – the most important gift most children expect is a smartphone. Parents' sole dilemma is not "if" but "when" to equip the young person with an "intelligent" phone. Meanwhile, many of us parents are still unaware of threats lurking in the web.

One of the ways to manage online threats concerning children is the "Safe Starter" service. For over three years this solution protects children's mobile devices in the simplest and effective way. All we need is a SIM card assigned to the service, and then automatically, with no need for any activity on the part of the parent, the child's access to dangerous content, e.g. pornography, malicious software, spam and phishing websites, extreme and disturbing content, or paedophilic websites is blocked. Safe Starter is based on URL categorization. Upon attempt to open a website assigned to a blocked category, Safe Starter user will see a blocking page instead. The same thing will happen if a website has not been categorized yet (which is important e.g. in case of rapidly growing number of pornographic websites). Access to most of encrypted websites is also blocked by default – the law forbids modification of https requests (i.a. because of the necessity to maintain the integrity of connection with banking websites). In this case, a so-called "whitelist", containing trusted websites is created, and in case of blocking an encrypted a website, the user may request unblocking it directly from the blockade screen. All this happens on the network level, without using the devices computing power, and at the same time not allowing uninstallation of the security measures, thus making bypassing them significantly more difficult.

In a certain analysed period, the infrastructure of Safe Starter registered over 10,5 billion requests, with the following distribution in relation to parts of importance (from among several dozen categories):

	Total	Social media	Games	Malicious websites and applications	Potentially unwanted software	Hazard	Pornography	Illegal software	Phishing	Spam
Requests	10,5 billion	1,84 billion	261million	88,8million	40,2 million	36,4 million	15,8 million	12,3 million	6,4 million	6,3 million
%	100%	7,4%	2,48%	0,84%	0,38%	0,35%	0,15%	0,12%	0,061%	0,059%

Nudity	Cartoon /video game	Sexual	Weaponry content	Spyware /keyloggers	Exploits	Drugs	Extreme content	Violence	Paedophilia
4,81 million	2,12million	784 thousand	754 thousand	414 thousand	268 thousand	51,2 thousand	28 thousand	19,2 thousand	1374
0,045%	0,02%	0,0074%	0,0071%	0,0039%	0,0025%	0,00049%	0,00027%	0,00018%	0,00001%

Conclusions drawn from the table above may seem optimistic, but it is worth paying attention to the distribution of the "bad" categories. Almost 17,5 % entries to social media services are further confirmation that for "digital natives", young people to whom the digital world is something natural, such services are a kind of a digital playground, where they spend time with their friends.

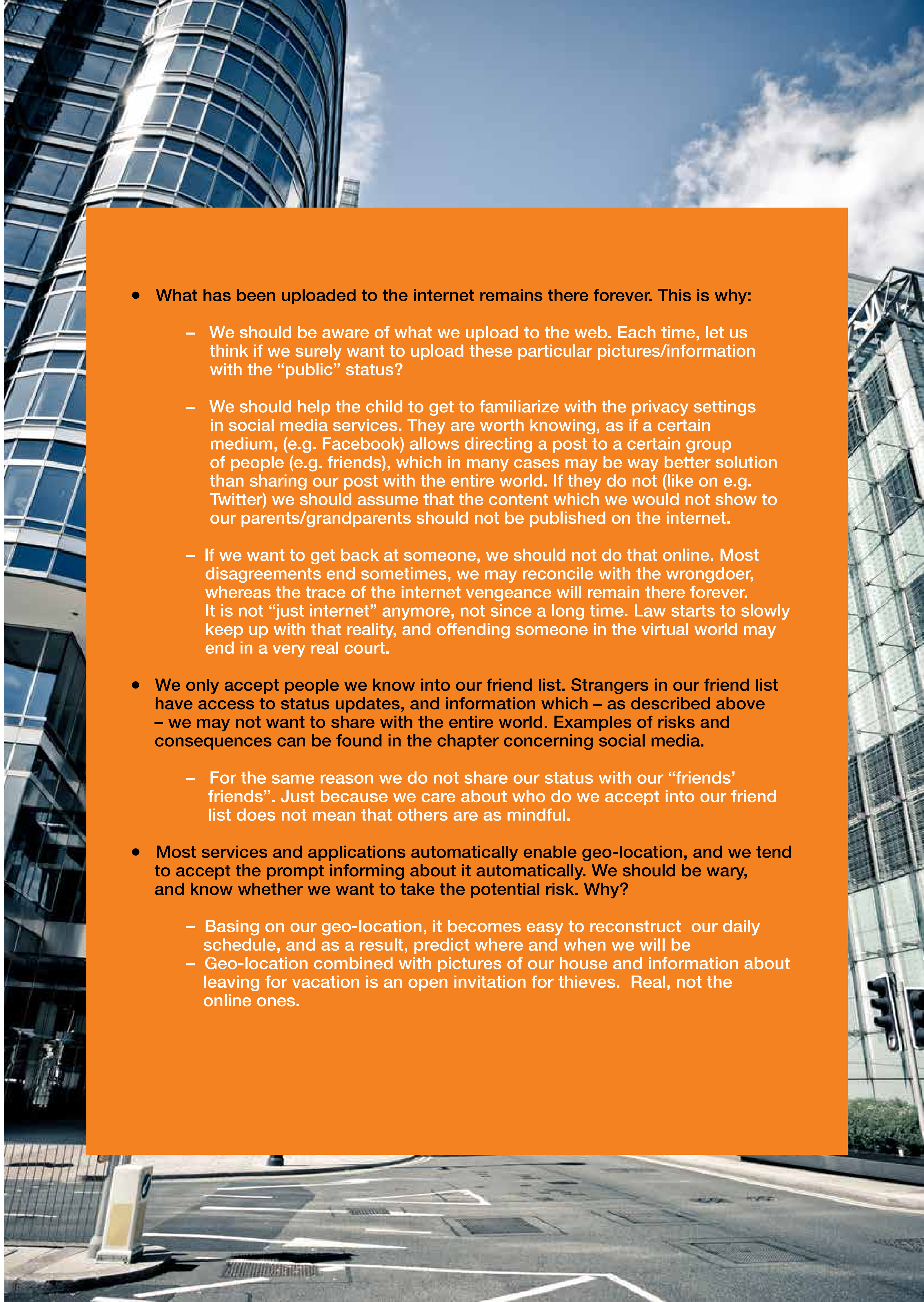
It gives plenty of room to manoeuvre for the parents, concerning simply... talking to children, and also – if they have not done that – familiarizing themselves with social media.

It is also worth noticing, that Safe Starter, which by default was supposed to protect the youngest of the internet users from pornography, became a sort of online antivirus. After combining the malicious websites and applications, phishing, spam, spyware/keyloggers and exploits categories, we will get almost 1% of traffic (which translates into over 102 million visits) of malicious nature, blocked before it get to smartphones or tablets of potential victims. This is almost 6,5 times more than attempts to access pornographic websites! It is without doubt good, that some the most serious categories – drugs, extreme content, violence and paedophilia combined– constituted not even 0,001% of website entry attempts in the period analysed. On one hand, this can be treated as a proof of education in this field, and the effectiveness of the solution itself as well. On the other hand, to treat this problem with due seriousness, we as parents cannot limit our approach to technological solutions only.

Here appears plenty of room to manoeuvre for the parents, concerning simply... talking to children, and also – if they have not done that – familiarizing themselves with social media. As the above statistics show, it is there, where our children spend a lot of their time, and because of this, it is there where people who might bear ill intentions towards them may find them. Limiting the surveillance over a child to technological solutions only, we may fall into the "two identities" trap – a situation in which our offspring officially (meaning where it can be observed by the parent) will display model behaviour, performing all worrisome activities in the invariably popular secret/closed social groups, or with the use of encrypted communicators. It is worth remembering that, also in the context of paedophilic websites mentioned before. As much as having protected 1374 young people from entering these extremely dangerous websites, it is known, that such content is not generally accessible, and that paedophiles find their victims through social networks in particular.

Data privacy threats in social media.

The 17% of entries to social network websites mentioned above using the Safe Starter is another proof of how important children's education is in the field of threats connected with social media. There is no way to sweep it under the carpet, or ignore it by rationalizing that children know more about these matters than the parents (although it is true in most cases). This is why instead of demonizing social media and desperately seeking alternatives, it is worth to, while highlighting the benefits, focus on the things children should be careful about, which is:



- What has been uploaded to the internet remains there forever. This is why:
  - We should be aware of what we upload to the web. Each time, let us think if we surely want to upload these particular pictures/information with the "public" status?
  - We should help the child to get to familiarize with the privacy settings in social media services. They are worth knowing, as if a certain medium, (e.g. Facebook) allows directing a post to a certain group of people (e.g. friends), which in many cases may be way better solution than sharing our post with the entire world. If they do not (like on e.g. Twitter) we should assume that the content which we would not show to our parents/grandparents should not be published on the internet.
  - If we want to get back at someone, we should not do that online. Most disagreements end sometimes, we may reconcile with the wrongdoer, whereas the trace of the internet vengeance will remain there forever. It is not "just internet" anymore, not since a long time. Law starts to slowly keep up with that reality, and offending someone in the virtual world may end in a very real court.
- We only accept people we know into our friend list. Strangers in our friend list have access to status updates, and information which – as described above – we may not want to share with the entire world. Examples of risks and consequences can be found in the chapter concerning social media.
  - For the same reason we do not share our status with our "friends' friends". Just because we care about who do we accept into our friend list does not mean that others are as mindful.
- Most services and applications automatically enable geo-location, and we tend to accept the prompt informing about it automatically. We should be wary, and know whether we want to take the potential risk. Why?
  - Basing on our geo-location, it becomes easy to reconstruct our daily schedule, and as a result, predict where and when we will be
  - Geo-location combined with pictures of our house and information about leaving for vacation is an open invitation for thieves. Real, not the online ones.

Partner's commentary

Martyna Różycka

Martyna Różycka is the leader of the Dyżurnet.pl team functioning within NASK. It is a place, where internet users can anonymously report illegal or harmful content published on the internet. Since the year 2007, she is a part of the Safer Internet project.

The best weapon against the dangers of the internet is knowledge, and if a threat occurs - an appropriate reaction. In the light of the NASK's research, and our daily observations, the internet initiation takes place earlier and earlier, and along with it, comes the responsibility of parents and teachers to pass this knowledge on, and to adjust it to current needs. While introducing the a child into the world of the internet, we have to pass on the rules that apply there, and to prepare the environment which the children use – to limit the influence of harmful content or dangerous behaviour as much as possible. The first moment is very important, as this is when we teach the child basic rules, but we should also remember about teenagers, and do not leave them to themselves. A child's needs change each year, and we constantly deal with new phenomena and threats.

In the last year, along with materials presenting sexual abuse of children, of course, internet users reported harmful content to Dyżurnet.pl. I conclude that by speaking about security on the internet, we should speak about security in general. Let videos about ingesting dangerous substances, e.g. household chemical products, or taking photos in dangerous situations be example of such approach. Some aspects connected with internet security go beyond the borders of the online world.

This does not depend only on parents and teachers – it is the responsibility of all mindful internet users, companies providing services, institutions working in the field of security. This is why co-creating the culture of safe and friendly internet is so important. What is also important, is the reaction in case of a threat – the work of teams such as CERT, or the Dyżurnet.pl, receiving reports about violations and threats is very much needed. Together, we help internet users, and intervene when necessary, working towards security on the internet.

> **While introducing the a child into the world of the internet, we have to pass on the rules that apply there, and to prepare the environment which the children use – to limit the influence of harmful content or dangerous behaviour as much as possible.**

7. Analysis of the most important cyber-threats in 2017

Malicious software activity in the year 2017 did not vary significantly from previous years. The main threats were still ransomware and botnets, from which i.a. DDoS attacks were generated. However, the previous year has shown that campaigns distributing malicious software can have deeply damaging impact on functioning of key business processes. That was made clear by the cases of i.a. WannaCry and NotPetya. Malware is still one of the basic tools negatively impacting Poland's security in the cyberspace.

7.1 Malicious software - the most dangerous activity of malware and ransomware

In the year 2017 (similarly to previous years) the highest activity was being shown by malicious software classified as Trojans, adware type of software, and PUP. Trojans are software allowing e.g. to trace the user's online activity, going off in case of detection of a certain action, e.g. logging into a service on the internet, in order to steal his passwords. Theft of funds from bank accounts – the so-called Banking Trojans were a significant source of offences with the use of malicious software.

Also in the headlines was extraordinarily "toxic" kind of ransomware, which blocked access to the user's data by encrypting his files in order to extort financial goods from him. Currently, a significant part of malicious software is propagated by phishing campaigns, in which the users, under a seemingly correctly constructed e-mail message, are encouraged to take actions, e.g. to click on an attachment, and by this, expose themselves to the consequences of cyber-criminals activities.

Such was the case of the Necurs botnet, which propagated using adequately prepared e-mail messages, installing ransomware on the computers of unaware users. Orange Polska noted almost 8 thousand queries relating to this botnet from DNS servers, which makes 6th place in the TOP10 general classification of botnet network activity in the Orange Polska network."

We invite you to familiarize yourself with the results of our observations in the field of malicious software. We have gathered quite large quantities of malicious code in the beginning phase of its distribution, the so-called „0 day" (we would like to say "thank you" for all incident report sent to cert.opl@orange.com). Part of the results can be found hare, the other one on the CERT Orange Polska website. The rest, e.g. samples of malicious code remains stored in our archives.

7.1.1 Detected events connected with activity of malicious software

CERT Orange Polska divides the identified events connected directly or indirectly with malware activity into three groups:

- **Malware object:** delivery of malicious software to terminal station
- **Web infection:** a real-time infection, and installation of malicious software on the victim's device
- **Malware callback:** confirmation of successful activation of malicious code by connecting network communication with a remote control server (in order to download further instructions, or redirecting stolen information).

Malware Object	Malware Callback	Web Infection
70 397	2 409 735	26 715

Figure 10 *The number of specific types of registered events connected with malicious software In the reference sample of network traffic.*

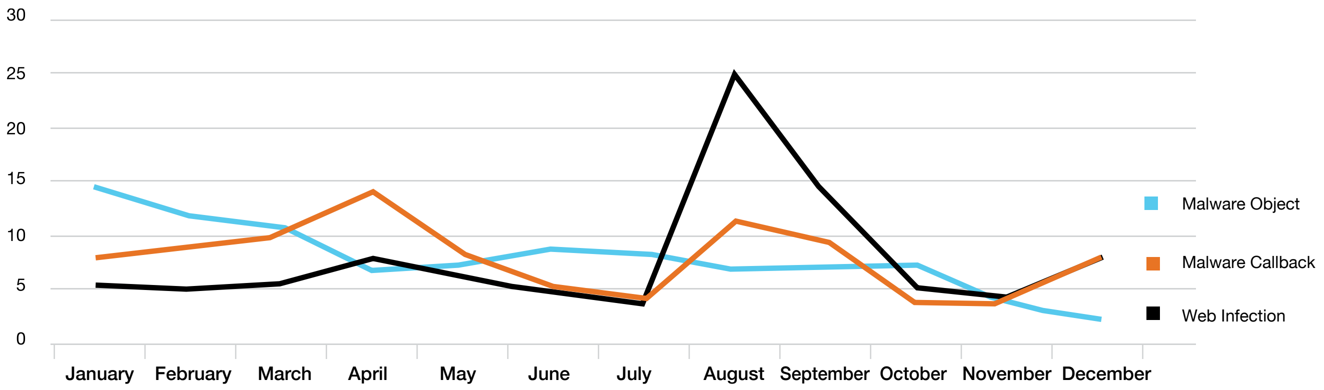


Figure 11 *Monthly percentage distribution of specific types of registered events connected with identified malicious software.*

Among all registered events, the vast majority of them are attempts of infected computers to communicate withthe C&C server (over 96%). This reflects well today's threats, as well as it says much about the number of infected devices. During this process, additional malicious components are being downloaded onto the user's computer. The computers intercepted this way may then become a part of the botnet, sending out spam, or conducting DDoS attacks.

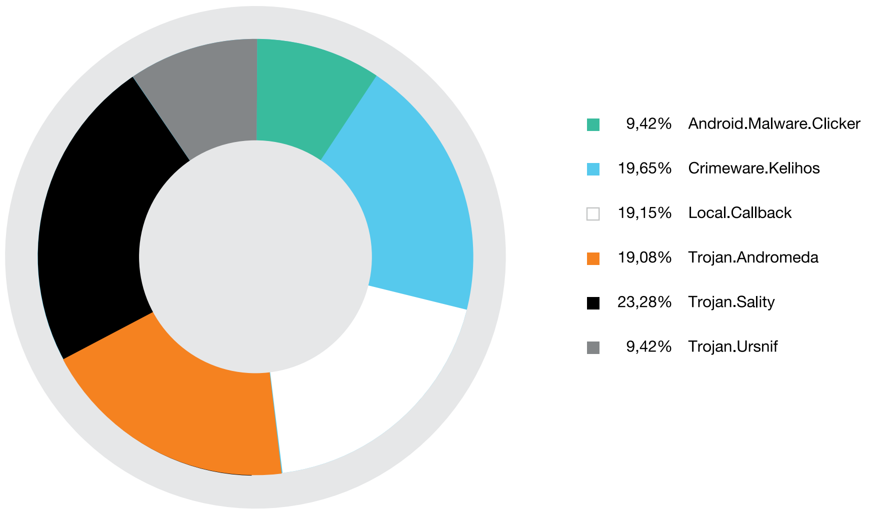


Figure 12 *The largest botnets - Percentage of all connections to botnets during the year.*

In the year 2017 most of the connections were directed towards a botnet distributing the **Trojan.Sality** software. This worm functioning in Windows environment is capable of e.g. transferring sensitive data about the user. The largest botnets also include **Crimeware.Kelihos**, which sends out spam, attacks crypto-currency wallets, as well as mines crypto-currencies using the resources of infected computers. Within active botnets, also a well-known threat **Trojan.Andromeda**. was found.

7.1.2. Threats using DNS service vulnerabilities

The largest number of events, which means as much as 73, 5 billion in total, in monitored network traffic, was generated by domains which were targets of PRSD (pseudo random subdomain) denial-of-service type of attacks. The highest accumulation of events of this type took place by the end of January 2017 r. Traditionally, DNS Traffic Amplification type of attacks (reflective amplification using open DNS servers) are a significant threat. The highest accumulation of events of this type took place in March and April of 2017. Also, over 1, 242 billion events connected with the activity of an unclassified botnet network and malicious software was detected. A similar event volume (1, 204 billion) was observed in relation to the Necurs threat, a botnet known mostly from distributing the Locky ransomware and Dridex bank Trojan. The highest accumulation of events of this type took place in February 2017. Over 981 million events were classified as the so-called malware call home, which means communication of the malware installed in a software system with the C&C.

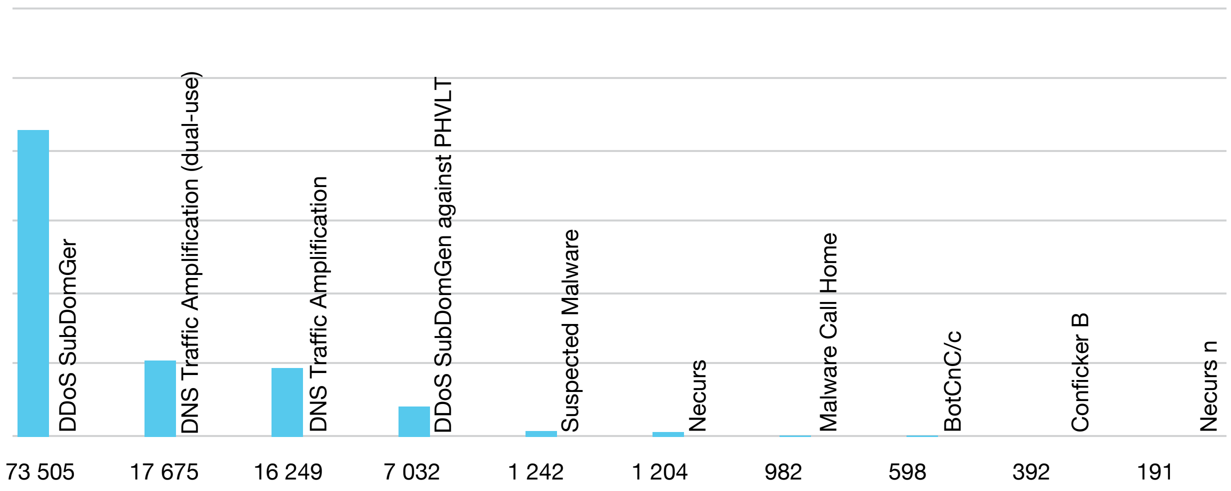


Figure 13 *10 most important security events in DNS traffic.*

7.1.3 Malicious software in fixed broadbands.

In the first quarter of 2017 the number of events of Neostrada service users was remained at around 90 thousand events per month. During the next months, less of such events has been observed, meaning up to 75 thousand events a month. Among customers using IDSL services, volume of observe incidents of that kind was half as small (around 43 thousand events a month). April was a ground-breaking month, when the number increased by 64% (up to 67 events). Then, rapid decrease and halt of the tendency was observed during the further months. This was caused by stopping of the spread of **Mirai/Hajime** malware in the Orange network.

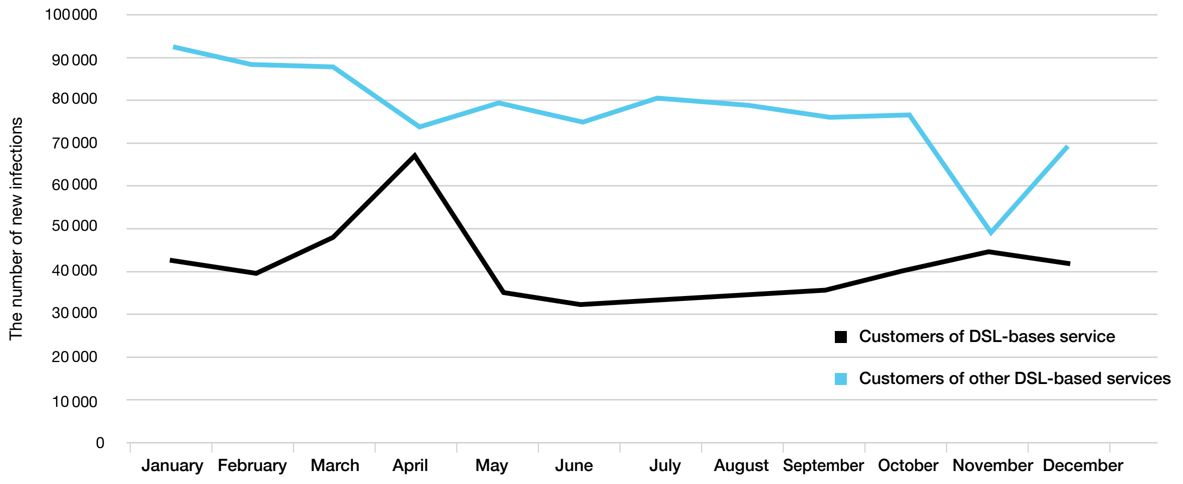


Figure 14 *Unique malware events registered in 2017.*

In the networks being the basis of fixed access to the internet, such as Neostrada and Internet DSL, the year 2017 was marked by the highest activity of malicious software from the **Trojan** family, **Backdoor** and **Riskware**.

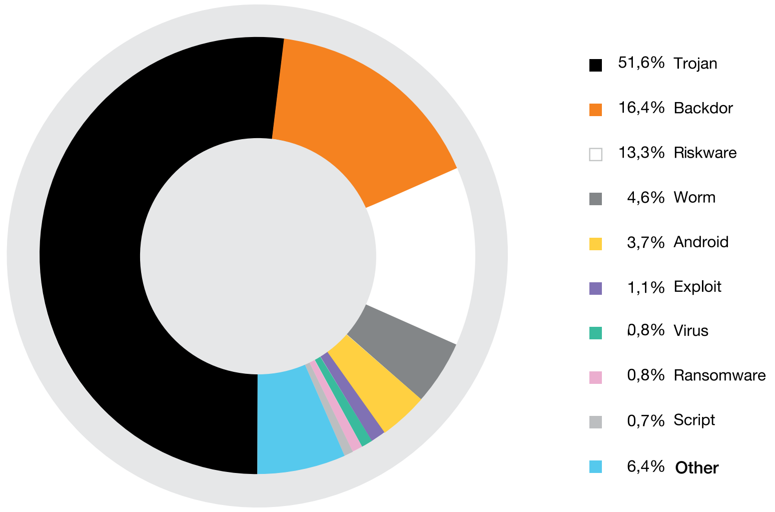


Figure 15 *Percentage distribution of registered malware events by category*

Category	Quantity
Trojan	1 293 416
Backdoor	409 732
Riskware	332 817
Worm	115 304
Android	93 790
Exploit	28 890
Virus	20 500
Ransomware	19 602
Script	16 854
CoinMiner	13 301
Inne	160 100

Figure 16 *Number of registered malware events divided into categories*

The most active Trojan software was **Trojan.Sality** (around 190 thousand unique infections) and **Trojan.Kelihos** (around 147 events instead of unique infections).

An interesting phenomenon that could be observed in the last quarter of 2017 was the appearance of internet services, which used the computing power of internet users for “mining” digital currency. In the Orange Polska network, we have noted 6578 unique events with **CoinMiner.Adylkuzz** malware by the end of the year.

7.1.4 Malicious software in mobile networks

Year by year, the percentage of threats for mobile devices is increasing. In 2017, CERT Orange Polska security team noted an increase in the percentage of mobile alerts by 25 %. (7 % in the year 2016).

Registered were also over 556 thousand events related to attempts of establishing a connection with C&C servers, and almost as much as 77 thousand cases of delivery of a malware sample, and over 42 thousand real time events. In the monthly distribution of events connected with mobile devices security, increased levels of malware activity ocurred in the period between August and November of 2017.

Malware Object	Malware Callback	Web Infection
76 990	556 152	42 488

Figure 17 *The number of specific types of registered events connected with malicious software for mobile devices divided into categories in the reference net traffic sample.*

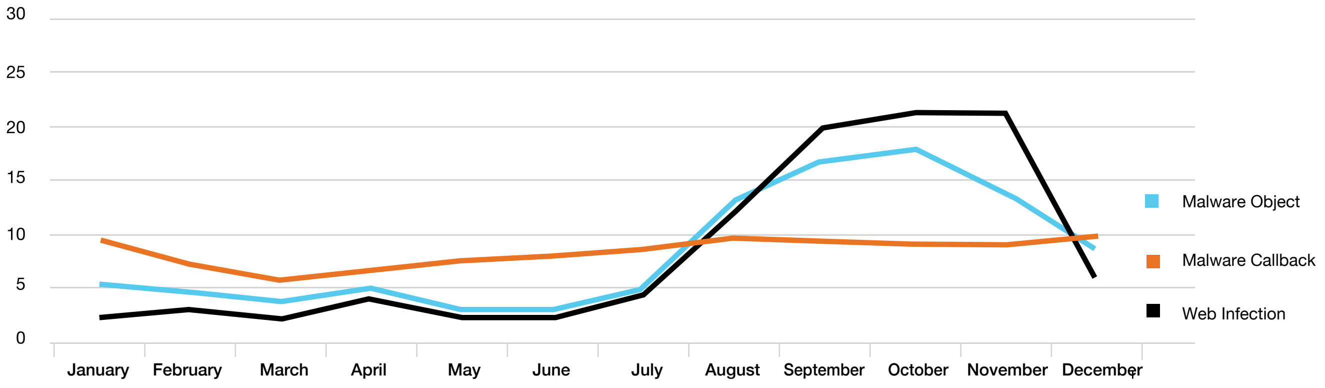


Figure 18 *The monthly percentage distribution of specific types of registered events connected with identified malicious software.*

When it comes to the number of detected connections with C&C servers and droppers, in the IPv6 mobile network, the tendency remained at the level of around 5 thousand new infections monthly, in the first half of the year. A significant increase in the number of users infected with malicious mobile software was noted in the summer months (June – August), counting even up to 18 thousand infections. This trend overlaps to a significant extend with the data relating to events connected with malicious software activity.

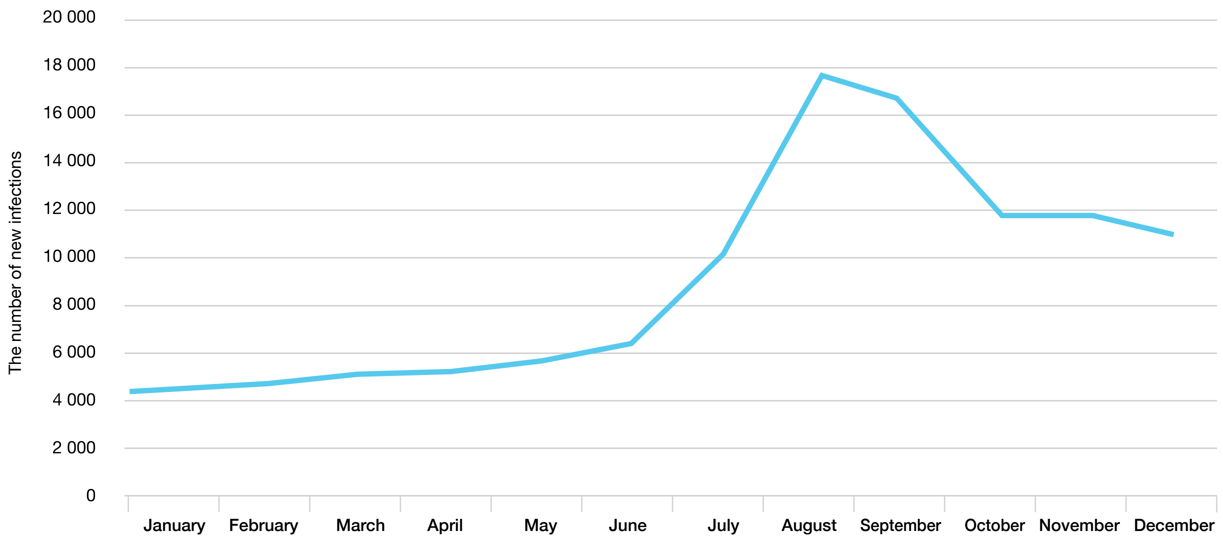


Figure 19 *Users infected with malicious software in the IPv6 mobile network*

Because mobile devices serve us for more and more kinds of services, including the ones that process sensitive personal data, or allow us to make online payments, there is still more and more malicious software aiming to take over those processes. Let us add, that ordinary users very often do not implement good practice concerning security, especially when it comes to updating their devices, which makes it easier for cyber-criminals to conduct a successful attack.

Particularly vulnerable to threats are devices running on the Android system, especially its older versions. W 2017r. The vulnerabilities of that system were used mostly **Clicker** which viewed ads from pornographic services in the background, and without the user’s knowledge, as well as **Triada**, the functionality of which was based on the ability to modify the network in social media services, and installing unwanted applications. HiddenAds on the other hand, is a typical adware type of software, displaying ads in an intrusive way in the web browser. The **MKero** worm was also featured on the list, as it was subscribing often expensive SMS Premium services without the user’s knowledge and control.

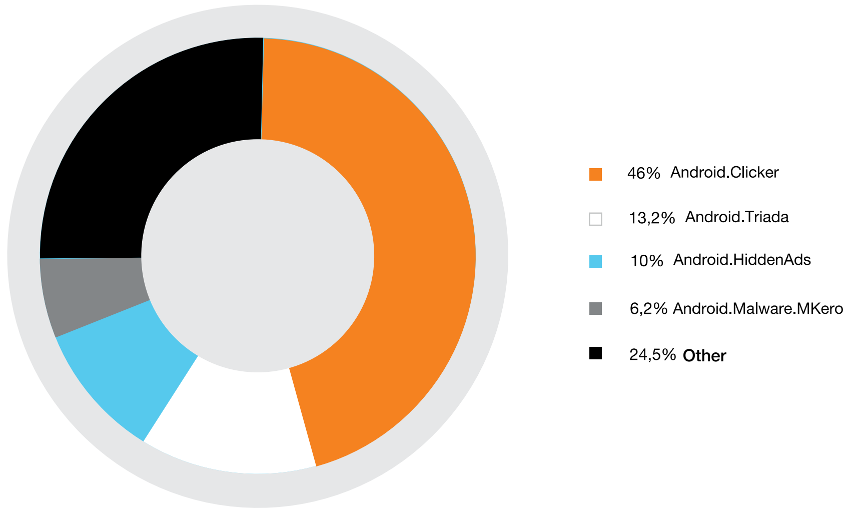


Figure 20 *The most important mobile threats in the year 2017 divided into categories.*

“To many people following news from this field, our annual summary of malicious software activity may be quite a surprise”. The spectacular waves of attacks of threats encrypting data and demanding considerable amounts of money for decrypting it might have suggested that it is malware of this type that dominated the battlefield of security application manufacturers and creators of malicious software. Thinking technology and quality-wise, that point of view can be considered correct, as new techniques of attack and some mechanisms of function of malicious software not encountered before, have forced laboratories and developer centres of antivirus creators to develop new protective functions. Also – as in case of threats using e.g. MS Office suite macros – renewal and modernization of mechanisms the importance of which significantly dropped in the last years. Effects of the activity of encrypting threats are also quite “spectacular”, loses caused by them significant, and for many organizations which had not secured themselves against them in time, often catastrophic.

However from the perspective of specific groups and families of malicious software, the past year did not drastically deviate from the previous ones. The top places on the list of detected and removed infections are invariably occupied by Trojan type of threats, and all kinds of spying applications, analysing the users’ behaviour, and oftentimes displaying advertisement content adjusted to the user’s analysed preferences in a very annoying manner (Adware, Spyware and PUP types of applications – potentially unwelcome/malicious programs, bordering on the verge of law and ethics). It is worth mentioning here, that technically, that kind of threats often pose a significant challenge for security applications, because many of them use advanced defence mechanisms, making their successful detection and removal from the infected system difficult – years of cyber-evolution in this field has done their work – modern adware and spyware are very sophisticated tools.

Ransomware’s low position on the list does not result directly form detections alone – it is worth to notice the detected Script, Office.Macro, Mail.Infected type of attacks – the goal of most of them was delivery of data-encrypting software to end-systems. Blocking them in an early stage did not allow installation of applications encrypting or damaging data in the system. In this context, they can be considered as a single group.

As each year, a group of “classic” viruses file infectors Win32.Virus has made it into the summary, and among them, especially Win32.Sality, Win32.Brontok and Win32.Virut. Their presence is considered the so-called “bottom drawer syndrome”, stemming from activities of users consisting in restoring old resources – CD drives, pen drives, archives – recorded a couple of years ago, containing programs and files infected with viruses that might have been undetectable by antivirus software back then.

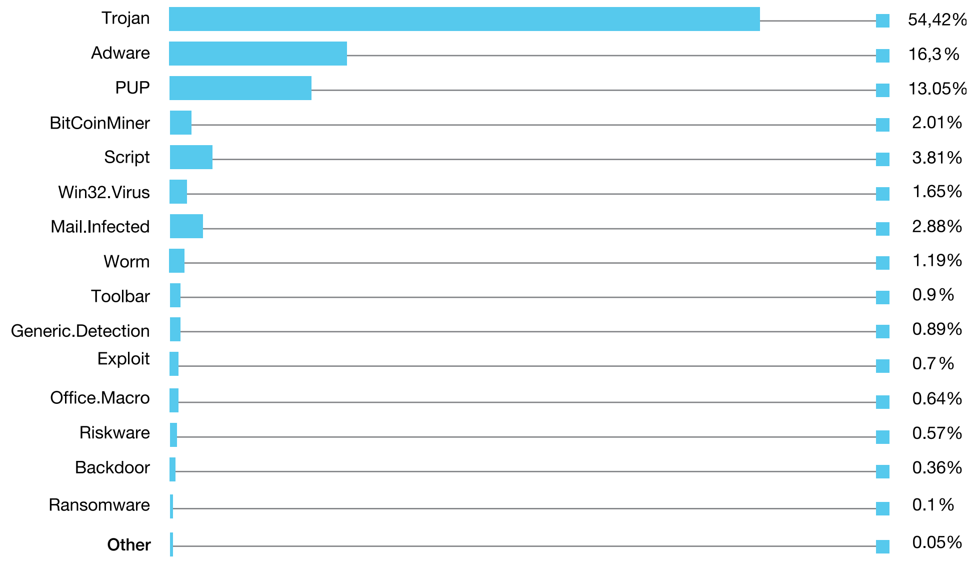
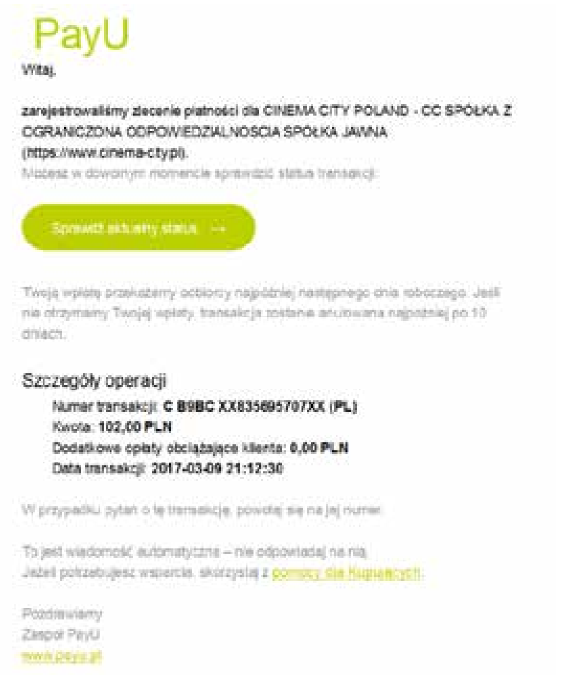


Figure 21 *Distribution of infections detected in the year 2017 (source: ArcaBit)*

An example of the framework analyzing the possibilities of “vjw0rm” malware in the PayU phishing campaign



PayU

Witaj,

zarejestrowaliśmy zlecenie płatności dla CINEMA CITY POLAND - CC SPÓŁKA Z OGRANICZONA ODPOWIEDZIALNOSCIA SPÓŁKA JAWNA (https://www.cinema-city.pl).

Możesz w dowolnym momencie sprawdzić status transakcji:

Sprawdź aktualny status →

Twoją wpłatę przekażemy odbiorcy najpóźniej następnego dnia roboczego. Jeśli nie otrzymamy Twojej wpłaty, transakcja zostanie anulowana najpóźniej po 10 dniach.

Szczegóły operacji

Numer transakcji: C B9BC XX835695707XX (PL)
Kwota: 102,00 PLN
Dodatkowe opłaty obciążające klienta: 0,00 PLN
Data transakcji: 2017-03-09 21:12:30

W przypadku pytań o tę transakcję, powołaj się na jej numer.

To jest wiadomość automatyczna – nie odpowiadaj na nią.
Jeżeli potrzebujesz wsparcia, skorzystaj z pomocy dla Kupujących.

Pozdrawiamy
Zespół PayU
www.payu.pl

In the first half of March 2017 phishing campaign impersonating PayU took place. Potential victims were receiving e-mails suggesting, that the sender is PayU. E-mails contained malicious attachement named “Potwierdzenie Platnosci – C B9BC XX835695707XX_PDF.js” (payment confirmation).

Looking more precisely on the attachement, we can observed that despite the “PDF” in the file name, the real extension is Java Script code. When executing the file, user installed malicious software named “vjw0rm”, which allowed to take full control over the workstation. After installation, virus added system registry key through which it could be launched everytime the operation system started.

Below we present the scheme of this particular malware. Detailed analysis carried out in the CERT Orange Polska laboratory can be downloaded from the CERT OPL website.

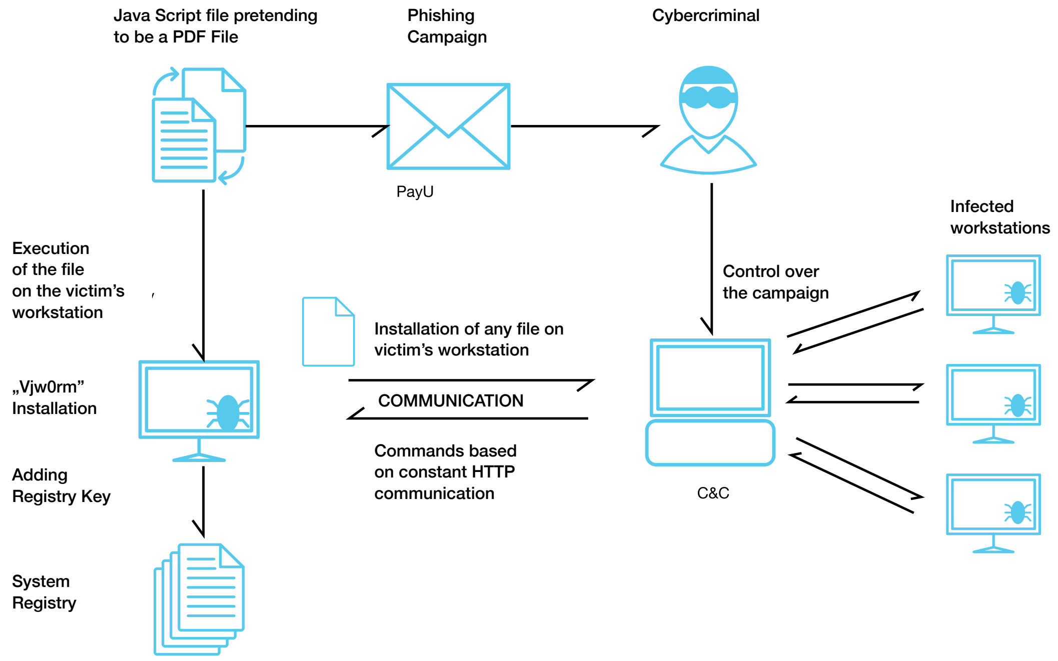

Java Script file pretending to be a PDF File
Phishing Campaign
Cybercriminal
PayU
Execution of the file on the victim’s workstation
Infected workstations
Control over the campaign
Installation of any file on victim’s workstation
„Vjw0rm” Installation
COMMUNICATION
Commands based on constant HTTP communication
Adding Registry Key
C&C
System Registry

Figure 22 *CERT Orange Polska malware laboratory*

How to protect ourselves?

There is no method guaranteeing complete security, and humans are still the weakest link. The rules for protecting ourselves against the effects of malicious software activity may seem trivial, but in most cases they significantly reduce the risk. It is important to protect ourselves on several levels, by e.g. raising awareness (our own, those closest to us, or colleagues) concerning the threats described in this report, use software securing mobile devices and systems processing sensitive data, never share personal information to people who would try to convince us to do so by using more and more interesting social engineering tricks (the grandson method, impersonating a bank or gas service official, a policeman, etc.).

It has been true for countless years, that far-reaching vigilance is the way. Messages received via e-mail, Messenger, or other applications should not be opened with complete trust. One can be never sure if the sender is actually someone we know, or just a name chosen to lure us into reading the messages contents or clicking on a link. We should beware of counterfeit messages. Vigilance is a very effective weapon, and oftentimes it gives us more than antivirus software we have installed, according to the rule that “prevention is better than cure”.

Individual users and small businesses should definitely use desktop software meant for protection from harmful malware activity. Nowadays the term “antivirus software” does not give justice to the advanced abilities of personal devices security solutions, and it limits threat awareness to one group of malicious software. The most effective protection in application form for users who cannot afford “enterprise” tier of solutions, should contain at least mechanisms protecting from malicious code, network security, protection of sensitive files from the destructive effects of ransomware, use the ‘sandbox’ mechanism, phishing protection for the e-mail client, as well as mechanisms allowing to verify the reputation of downloaded resources in less trusted environments.

Large businesses (corporations and institutions) possessing adequate financial means should protect themselves on all levels. Apart from regular staff training, they should ensure proper protection of their resources at the interface with less trusted environments. In this case, from technological point of view, a minimalistic approach would be to protect electronic mail exchange services with public networks, as well as filtering queries to external websites, along with analysis of resources downloaded from such networks. Some companies choose to completely block P2P communication beyond their infrastructure, but this depends on their internal regulations and decisions made by the management.

In every environment – no matter a company or home – we should ensure a functioning mechanism of installing security patches delivered by operating system and application manufacturers. This is very important (critical even) as applications with errors in them (vulnerabilities) may be a significant gap in the security of protected resources (data) – and as we know, the weakest link may compromise the entire structure. In the further section of this report, are detailed analyses of vulnerabilities worthy of notice that we have chosen from the last year.

Making backup copies of important data is a timeless rule, and as archaic as it may sound, definitely the most secure is the data stored on mediums accessible on read-only basis, such as non-rewritable drives, or memory cards with an appropriate LOCK switch, blocking the record function. Another solution is storing data in a place inaccessible physically as well as via network.

Software should be downloaded and installed only from trusted sources. If there is an option to install the software in trusted and separated environment beforehand – it is worth to use it. Inconveniences connected with organizing such an environment are disproportionally smaller in comparison with the consequences of losing data or the system crash, and the necessity to recover it.

It is also worth to familiarise ourselves with the rules of using mobile system distributors’ repositories such as Google Play Store – the creator of the most popular mobile device system named Android. The “Google Play Protect” software is an additional means of protection from suspicious applications available in Google Play Store – ones that suggest the user that they are e.g. games, actually serve to smuggle in malicious code, the goal of which is e.g. stalking the user of a certain device in the web. This software scans the device in specified intervals of time to verify whether any of the installed applications were not reported as compromised, and may jeopardize the security of the user’s data, or privacy regulations.

By downloading illegal software (or cracks), multimedia (films/music) using p2p services, or websites specialized in sharing illegal content, users take up the risk of compromising their devices by malicious software. Knowing about a large number of customers who do not want to pay for licenses, cyber-criminals “weave in” malicious code into the illegal materials. The code may serve to connect the unaware user’s computer to C&C servers (botnet), where compromised devices become one of the many “zombie” computers, executing orders given out by the botnet’s administrators. Is it worth to download such content and compromise our systems? Can we feel comfortable knowing that the device may be also used by “someone else”? These are the questions that we should answer before we make the first step, by reaching out for e.g. torrents. After the first time we cannot be sure of anything anymore.

If possible, we should use the NAT function (called this way for the sake of simplification) while accessing the internet. If a router of an operator providing this kind of access is installed in our home or office, there is a chance, that computers and other devices functioning within the internal network are not available directly from the internet. If a mobile device connects directly to the operator’s network, it also does not mean that it is not using this kind of protection. Some of the ICT operators use the NAT mechanism within their own network, and it is made transparent for common internet user. We should remember that a router bought separately should be configured by an expert, possess an active firewall, and disabled, or limited remote control interface.

More details concerning certain threats can be found in the chapters dedicated to specific threats.

Partner’s commentary

Grzegorz Michałek - owner and chairman of the management board of Arcabit Sp. z o.o. and mks_vir Sp. z o.o., graduate of Warsaw University of Technology’s faculty of Electronics and Information Technology, programmer from passion, and author of many books and publications on programming. Connected with the anti-virus branch since over 25 years. He has been cooperating with both domestic and foreign companies from the field of security. He gives seminars, and lectures on the matters of anti-virus protection and malware analysis. Supporter and exponent of new technologies, and unconventional solutions in the field of cyber-security.

Yet another annual analysis of trends in cyberspace confirms the general rule that governs the evolution of malicious software – attacks are directed where there is money, or resources which can generate money. One could say it is clichéd, but this seemingly obvious rule forces cyber-criminals to exercise constant creativity, and to seek new areas generating illegal profits.

Taking a look at lists of threats, we can see at the leading positions unmatched leaders of classification – Trojans, adware, spyware, unwanted applications – these are “safe bets”, which always, regardless of time, generate profits for their “operators”. The first half of the last year also was an area of operation for a wide spectrum of data-encrypting threats, and demanding ransom for the possibility of getting it back (often false one), however the development of mechanisms protecting from such activity (in operating systems, and security applications as well) has noticeably reduced the efficiency and profitability of this area of cyber-crime. The rapid growthn popularity of crypto-currencies and the vision of profits generated by them laid the groundwork for another family of malicious software – miners using computing power of millions of computers around the world. The concept itself was not new of course – one only needs to recall the SETI@home project popular at the time, in which users could support scientific research with the power of their own, private machines. Cyber-criminals are using the same model, the only difference being that the computing power is being utilized without the users’ knowledge, and the creators of malicious software use a wide variety of social-engineering mechanisms, as well as software and security gaps to launch the mining procedures on as many machines as possible.

The effects are visible in our TOP10 lists – the leading positions have been occupied since several months now by malware from the BitCoinMiner family. This tendency will surely persist throughout the next 10 – 12 months. Meanwhile, we are also going to observe recurring ransomware attacks, taking advantage of the users’ dulled vigilance.

7.2 Volumetric attacks on services and infrastructure - DDoS

DDoS, a type of distributed attack, consisting in sending mass amounts of requests to the chosen services in the infrastructure in order to disrupt its functioning. Managing incidents of this type is one of the priorities CERT Orange Polska.

7.2.1 DDoS Attacks – characteristics of the traffic

Below we present characteristics of traffic in case of specific port numbers on connections analysed by Orange Polska. Data presented on the diagrams is averaged.

Port 123 is used by the NTP service (Network Time Protocol), used for time synchronization in ICT and telecommunications. On the connection analysed by Orange Polska, the highest traffic on this port (over 25 Gbps) was observed in March and August.

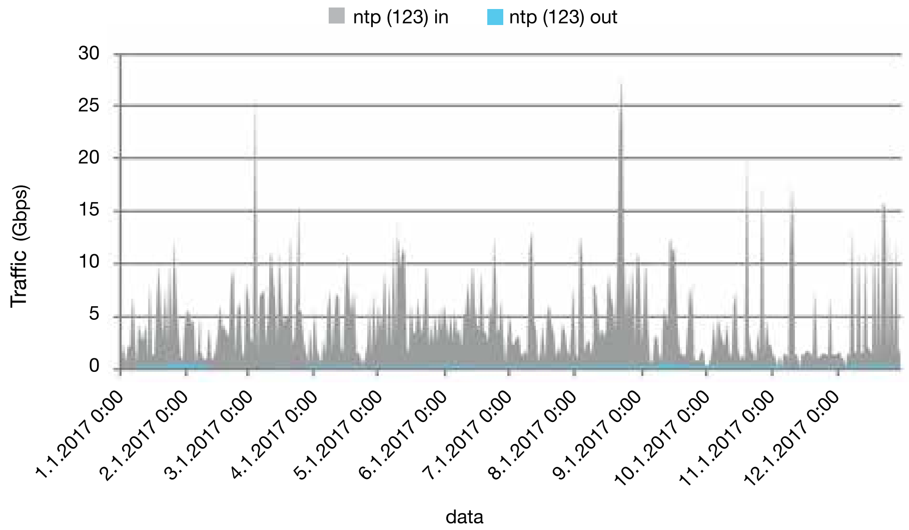


Figure 23 *Characteristics of traffic on port 123 on the connection analysed by Orange Polska in 2017*

Port 1900 is used by the SSDP protocol (Simple Service Discovery Protocol), which serves for UPnP device (Universal Plug and Play) detection, e.g. keyboards, printers, and routers. The highest traffic (over 10 Gbps) on this port was observed by the CERT Polska team in October.

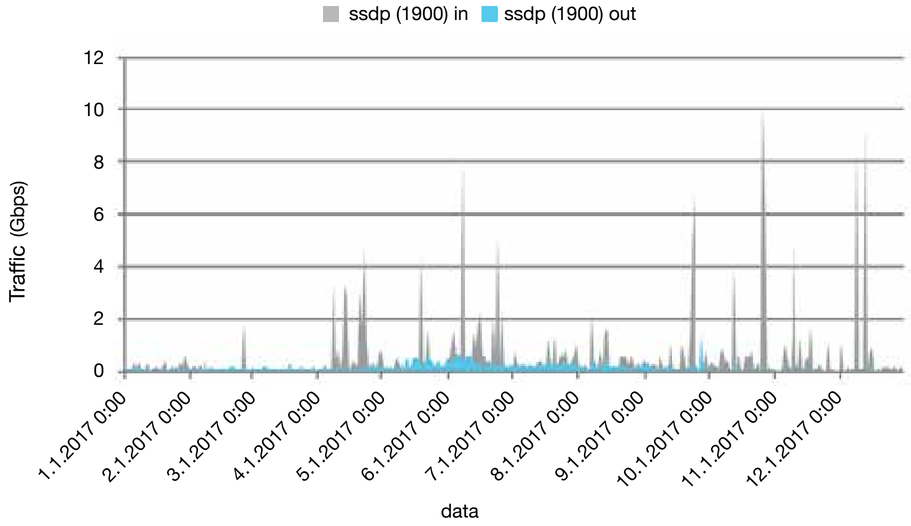


Figure 24 *Characteristics of traffic on port 1900 on the connection analysed by Orange Polska .*

The highest traffic on this port (over 17 Gbps) has been identified in September. Significant fluctuations reaching even 16 Gbps were also registered by the end of the year.

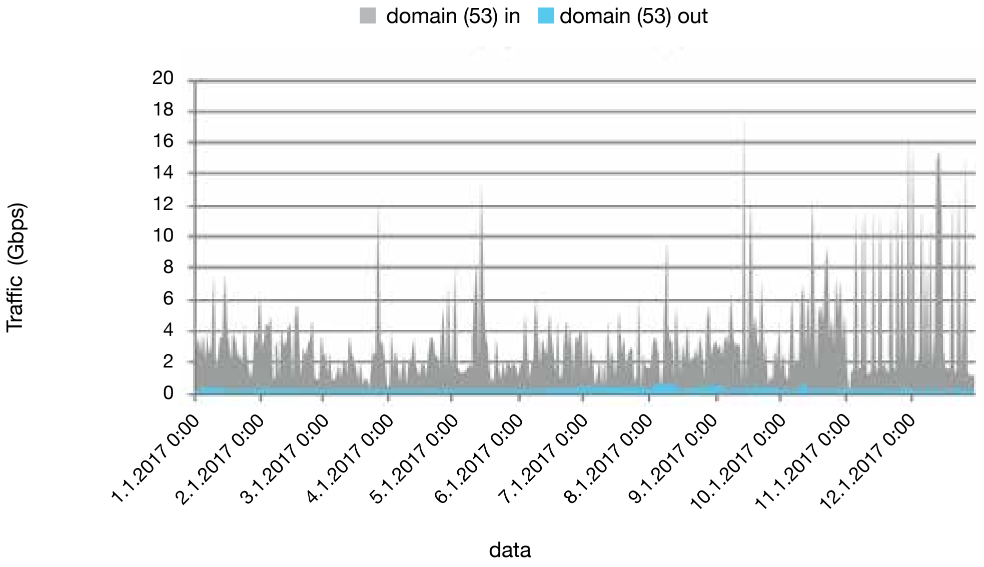


Figure 25 *Characteristics of traffic on port 53 on the connection analysed by Orange Polska.*

Port 19, used by the CharGen protocol (Character Generator Protocol), serves for generating characters for test purposes. The most significant traffic on this port (over 5 Gbps) has been registered in January.

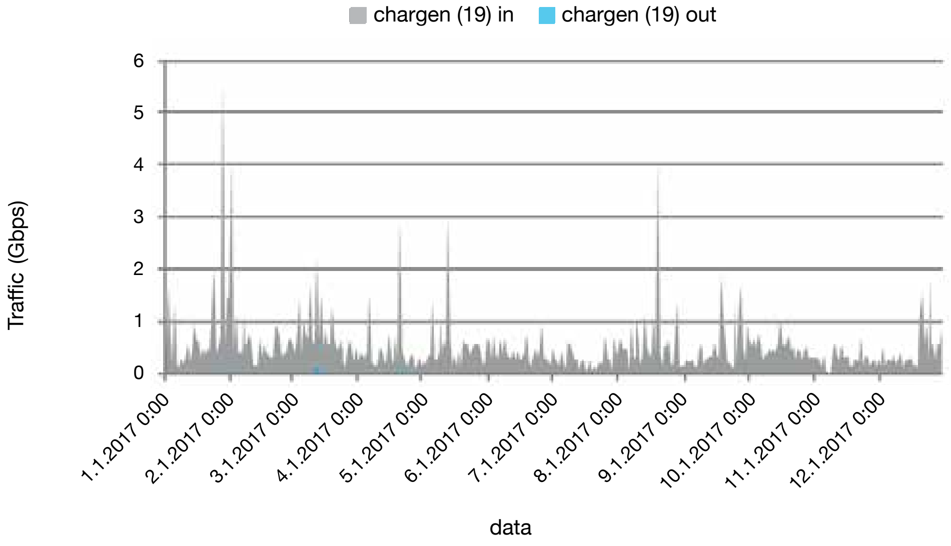


Figure 26 *Characteristics of traffic on port 19 on the connection analysed by Orange Polska.*

7.2.2 DDoS attack – types of attacks

The classification system for DDoS attacks used by CERT Orange Polska is based on three categories with different level of severity. The high level alert usually has significant impact on the availability of services, whereas the low and medium ones just limit it under certain circumstances. The most alerts with the highest level of severity took place on 22nd of October. When it comes to alerts with the low and medium level of severity, their noticeable increase took place in January, as well as in the period between September and December 2017.

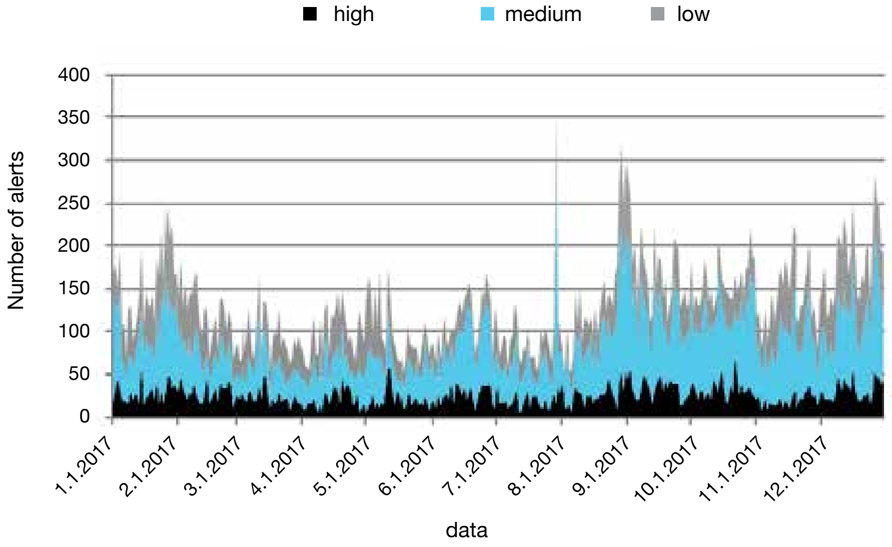


Figure 27 *Distribution of DDoS alerts based on their level of severity.*

In the percentage distribution of DDoS attacks we can observe that the percentage of medium level alerts is the highest (2). They constitute almost half of the registered events. In comparison with the year 2016 this distribution is almost identical. As in the previous years, the lowest percentage includes the attacks with the highest level of severity (1). It equalled 22% in the year 2016, and 20% in 2017.

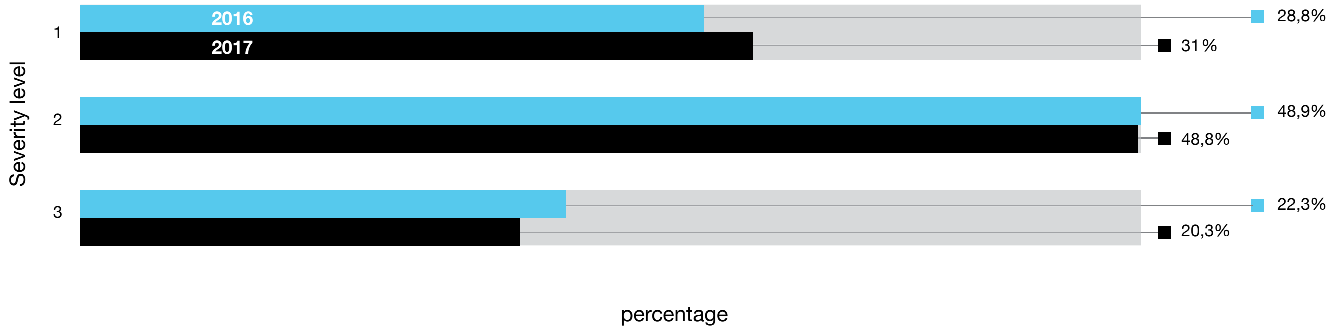


Figure 28 *Percentage distribution of the level of DDoS alert severity.*

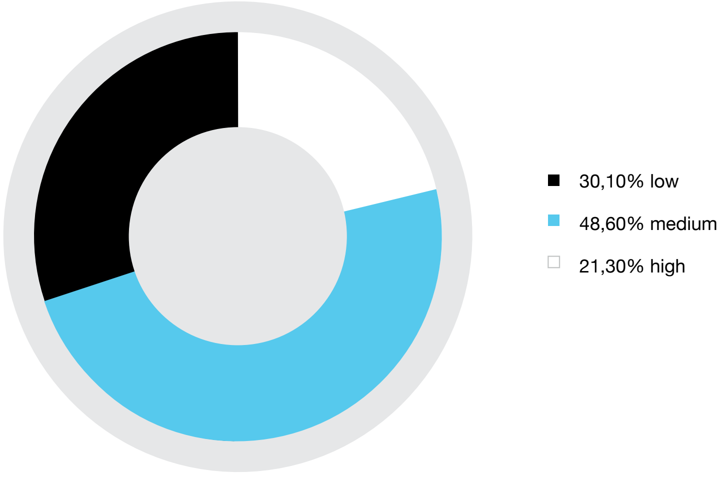


Figure 29 *Percentage distribution of the level of DDoS alert severity as a diagram.*

As in the previous year, in the distribution concerning the most common types of attacks, UDP Fragmentation type attacks were the most important ones in the year. This type of attack constituted over 55% of all attacks. The CERT Orange Polska team has also observed a small increase in the percentage of DNS Flood type of attacks – by almost 4 pp. in comparison to 2016.

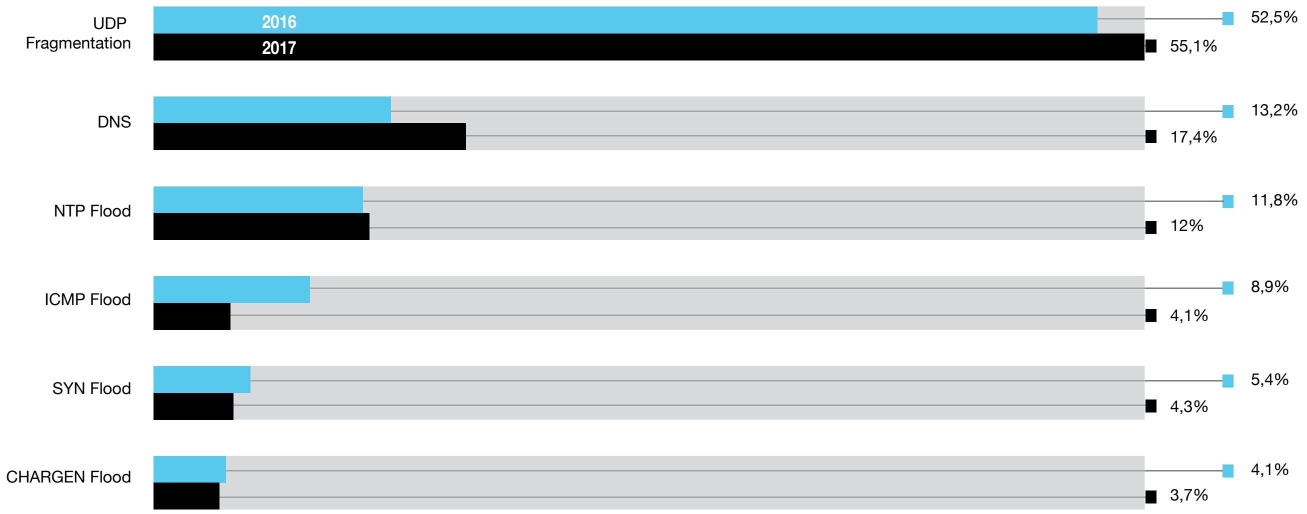


Figure 30 *The most common types of DDoS attacks*

UDP Fragmentation – an attack in which large UDP packages (over 1500 byte) are sent by the attacker. Bearing in mind the need to reconnect the defragmented packages on the receiving device, using additional resources of the processor becomes necessary, which stresses the computer's system.

Reflected DNS – also called a reflected attack, a method using vulnerabilities of network communication protocols. For the purpose of amplification, vulnerabilities of protocols such as UDP, DNS, SNMP, CHARGEN and NTP may be used.

ICMP Flood – a technique in which non-standard amounts of large ICMP packages are sent in order to "flood" the victims computer network. Usually a network of intercepted devices (bots) is used in this case. As a result of this kind of operation, bandwidth capacity is limited, and services are blocked.

SYN Flood – an attack basing on a vulnerability in the three-way handshake, a procedure of establishing connection used in the TCP protocol. The attacker sends a SYN flag, which serves for initiating connection between the source and target host, to the TCP ports. The attacked system responds with a SYN-ACK message, which opens the port, and awaits a confirmation of establishing a connection - an ACK flag from the attacker. The flag is never sent, so the connection is not established, but since the "victim" is waiting for conformation, the system's resources are being depleted.

7.2.3 Analysis of the largest volumetric attacks observed in

As in the previous years, a trend prevails suggesting the shorter and shorter duration of attacks. Just as in the year 2016, in 2017 the percentage of volumetric attacks lasting for more than 30 minutes constituted about over 6%. The only real change observed was the decrease in the percentage of attacks lasting between 10 and 15 minutes, by around 3 pp. The average duration time of all alerts was around 15 minutes (16 minutes 2016)

In 2017 the average volume at the peak intensity of a DDoS attack observed in the Orange Polska network reached 1,22 Gbps (1,15 Gbps in 2016). The highest traffic intensity value at the peak of an attack reached around 177 Gbps (82 Gbps in 2016).

> Gbps (gigabyte per second) in the context of DDoS attacks, means the intensity of the data stream directed at the service being attacked.

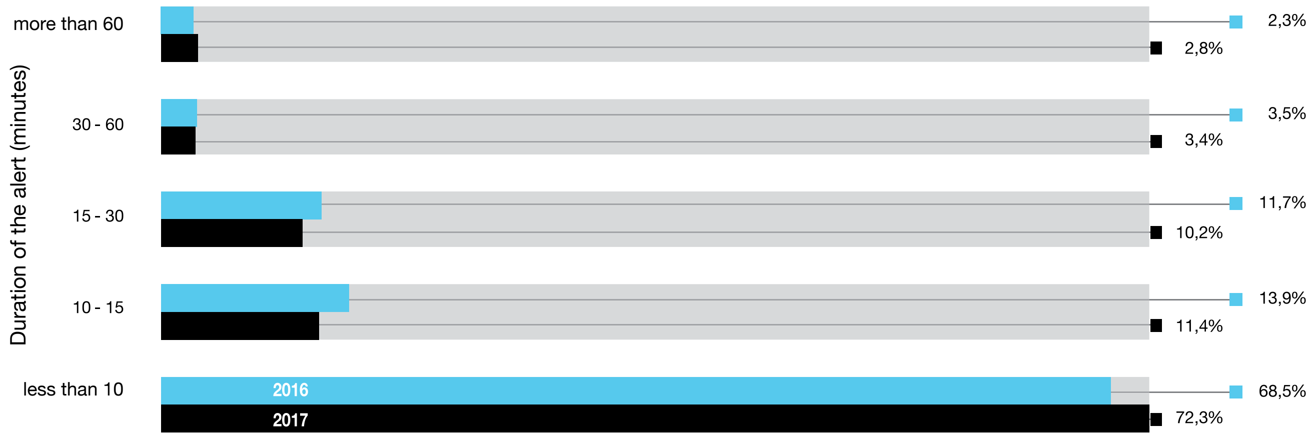


Figure 31 *Duration of DDoS attacks observed in the Orange Polska network in 2017*

In comparison with the year 2016 the CERT Orange team observed over 5 pp increase in the percentage of attacks not exceeding 0, 2 Gbps. The smallest change in comparison with the previous years concerned attacks of high intensity.

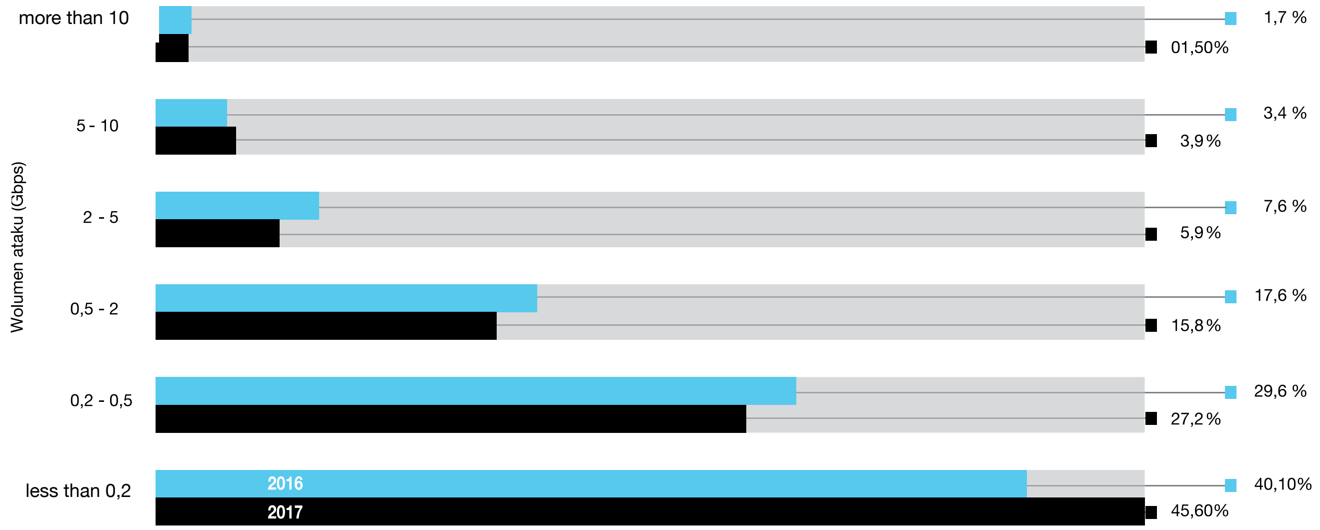


Figure 32 *Percentage distribution of DDoS attack volumes observed in the Orange Polska network in 2017.*

How to protect ourselves form the effects of DDoS attacks?

To protect ourselves form DDoS attacks efficiently, we should not wait for them to happen. It is our duty to prepare for them beforehand – we should assume that our resources will be attacked anyways.
Because of this, some of the actions should be performed in advance, to prepare us for an attack. Important tasks at this stage include:

1. Contacting our internet services provider, and finding out about the possibilities concerning support in case of DDoS attack, as well as familiarizing ourselves with the procedure for requesting this sort of support when such attack happens.
2. Identifying processes, services, and devices critical for the functioning of the organization.
3. Prepare detailed documentation of the network and IT infrastructure of the organization. Check the documentation of the IT infrastructure: business owners, IP addressing; prepare a topological diagram of network and a list of resources.
4. Prepare a detailed procedure in the event of an attack. We should remember about providing an alternate communications channel, e.g. with the ISP or MSSP. In case of an attack, the company (corporate, internet) e-mail and VoIP phone may not be working properly.
5. Optimize and improve the state of all the devices working within the IT infrastructure, the so-called hardening.
6. Prepare a "whitelist" of IP addresses, which in case of a necessity to limit the traffic, should have a priority of service (the largest customers, key investors).
7. Plan the way in which the company's customer's will be informed about the temporary impossibility to contact the organization the in the regular way (Twitter, FB)
8. Estimate potential losses in case of a DDoS attack.
9. It is also necessary to monitor the efficiency of the network infrastructure in order to detect the attack.

We should regularly test our infrastructure by performing so-called stress-tests. This allows to precisely determine the level of traffic volume, which the infrastructure can withstand, and to find weak points in its structure.

Upon detection of a DDoS attack, we should make contact with the teams administering the network infrastructure, the internet services provider, law enforcement, and CERT/CSIRT teams.

To address this kind of attacks, the first phase of action includes performing actions to analyse them:

1. Understanding the data flow in the attack, determining its source (and maybe its motive).
2. Identification of the infrastructure affected.
3. Analysis of server event registers, routers, firewalls, applications, and other resources which may be the target of the attack.
4. Finding out which aspects differ the traffic resulting from the attack from the normal traffic (source IP addresses, ports, TCP flags).
5. Using traffic analysing software (tcpdump, NetFlow, etc). Downloading and saving a sample of the attack may be useful in context of a future analysis.

After analysing the attack, and understanding its nature, we should move onto alleviating its effects, i.a. by (if our network allows it):

1. Limiting the traffic resulting from the attack as much as possible, by e.g. using BGP FlowSpec protocol, for which cooperation which the operator is required. If this is not possible, we should neutralize the points of interconnection with the external network (on routers, firewalls, load balancers, etc.)
2. Closing unwanted ports on firewalls
3. Switching to alternative networks, and blackholing the traffic to the original IP addresses.
4. Increasing the bandwidth through cache or CDN services in the Anycast technology.
5. Running the traffic through a service or a device protecting from DDoS attacks.
6. Configuring the filters so that they would block packages generated by the system in response to requests which are a part of the DDoS attack.

Partner's commentary

Mirosław Maj

More than 20 years of experience in ICT security. Founder and president of the Cybersecurity Foundation, CEO of the ComCERT company, a former leader of CERT Polska team. In 2017-2018 he was the adviser to the Minister of National Defence of Polska on planning cyberdefence capabilities and building organizational structures as well as establishing international cooperation on the field of cyberdefence. Initiator of Polish Civic Cyberdefence organization. He is the member of Trusted Introducer team being responsible for accreditation and certification of CERTs. European Network Information Security Agency expert and co-author of many ENISA publications including CERT exercises and papers on improvement the CERT coordination. He organized cyber exercises in Poland and Georgia for energy, banking and telecommunication sectors. Speaker on many international conferences including the FIRST conferences. He is also the orgniser of five editions of the cyber exercises Cyber-EXE Polska and SECURITY CASE STUDY conference.

I always watch statistical data prepared by CERT Orange Polska with curiosity. Possessing the largest operator network in Polska, this team has the highest chance and possibilities to depict phenomena connected with network traffic. This concerns particularly traffic resulting from DDoS attacks, the observing and combating of which CERT Orange Polska treats as a priority, as they say themselves.

The overview of data gathered on DDoS type attacks in 2017 most of all comes to conclusion, that there are no significant changes in what do we observe in this field. A year earlier, everyone experienced distinct sense of danger stemming from appearing DDoS attacks based on botnets built upon IoT devices. This time, there was nothing as shocking. This does not mean that there were no interesting phenomena that could be omitted. The most fundamental phenomenon was the recorded shorter time length of DDoS attacks. 85% of attacks in 2017 lasted less than 15 minutes. The shorter time length as accompanied by the decreasing average volume of attacks. Almost 75% reached level no higher than 0,5 Gbps. Both these values may indicate that DDoS attacks are more frequently used against small services, for immediate needs, and often also against individual users. After all, the phenomenon of attacks on online players is already commonly known. With commercialisation of the market of such games, this phenomenon can gain significant importance.

As for defence against attacks, practically nothing changes. As it is known, with attacks of large volume, (and they do occur, as the data from the report indicates), there is no solution apart from close cooperation with the operator. Regardless of the mention of shorter and smaller attacks, the danger associated with attacks of great volume should not be forgotten, as they can paralyze the entire organization, and above all, its key services. While looking at the data, it is worth taking a look at the types of attacks. They remain practically the same. Again, the most activities are associated with the NTP, UPnP, DNS and CharGEN services. That is the best evidence of how much is there to do in the matter of configuration of "Polish" internet. Wrongly configured services are regularly used for e.g. "amplification" type of attacks without much trouble. It would be for the best, if not only those supposed to protect themselves took a look at this data, but also the ones whose ambitious objective is to increase the level of cyber-security in Poland did it as well.

7.3 Attacks on end devices – modems, routers and IoT.

Analysis of the most dangerous attacks on end devices.

In the year 2017 we had several cases of incidents connected with the security of modems and IoT devices. The first of the challenges was dealing with the Mirai botnet, which was not easy.

Port 7547 has been preventively blocked, but at the same time, we have registered an increase in the number of damaged modems of our customers. The problem turned out to be accidentally disabling firewalling for port 30005 during administrative works (this port is used by some of our modems for remote control). Additionally, a gap which caused writing to the flash memory with every attempt to connect with the TR service, resulted in permanent, physical damage to the modem. The precedent however has been stopped at the last moment.

Just as in the previous year, in 2017 the trend connected with mass use of vulnerabilities in modems/IoT has been on the increase. Vulnerbilities that are the most useful to cyber-criminals are the ones which allow penetration of many kinds of devices/manufacturers. A good example of this is recently discovered code-execution vulnerability in the GoAhead webserver, on which many internet of things manufactures base. The only line of defence from this kind of attacks is not providing any services on the internet, and if necessary, using VPN.

In the years to come, due to the increasing number of IPv6 users, we can anticipate new kinds of attacks. Google Project Zero has conducted very interesting research in this field. The target was the popular DNS/DHCP dnsmasq server. Gaps hidden within its implementation of the IPv6 protocol allow constructing a functioning exploit, which could bypass today's ASLR/DEP security due to memory leakage. Dnsmasq in many different versions is installed on around a million devices all around the world.

Today's software if built from a huge amount of subcomponents. Because of this, its manufacturers are unable to provide 100% security. During the research and development works, CERT Orange Polska conducted tests of "Intelligent House" type of solutions from two manufacturers. In both cases, the devices possessed gaps allowing their penetration from a local network, and subsequently, using a gap in the servers, granted access to the users' data.

The main reasons for the poor level of security of this type of devices are:

- Either lack of or improper validation of SSL certificates.
- Lack of encryption.
- OWASP TOP 10 vulnerabilities.

How to protect ourselves?

Technical infrastructure using data transmission services (or one responsible for them) in many cases is very simple. Routers, modems, switches, industrial drivers, cameras – these are all uncomplicated devices, used to varying extent in offices, homes, and industrial facilities. There are countless devices in the internet network, which is perfectly illustrated by the depletion of the pool of IPv4 addresses. Vulnerabilities in software managing such devices may bear potentially dangerous consequences. If we add to this the fact, that each of such devices may control an intelligent house, a production line, or a power plant – it almost sets off the alarm bells for eventual effects of possible threats materializing.

We all remember events of the past, about measurement devices of the energy sector leaked to the internet, or about the crash in Deutsche Telekom, which caused paralysis of 900 thousand subscribers, preventing them from using the internet or television. It should be remembered that our security, safeguarding sensitive data, and continuity of business services consists in everything that participates in digital processing and transferring data. It is not enough to secure our personal computer with appropriate software detecting malicious code and blocking its activity, just as it is not enough to secure our mobile devices.

As shown in this report, the entire ICT infrastructure has to be properly secured. Modems, routers, intelligent houses consisting of dozens of components communicating with one another (and with the world), every one of which can be an independent network device (router, modem, temperature sensor, gates, windows, gas, etc.).

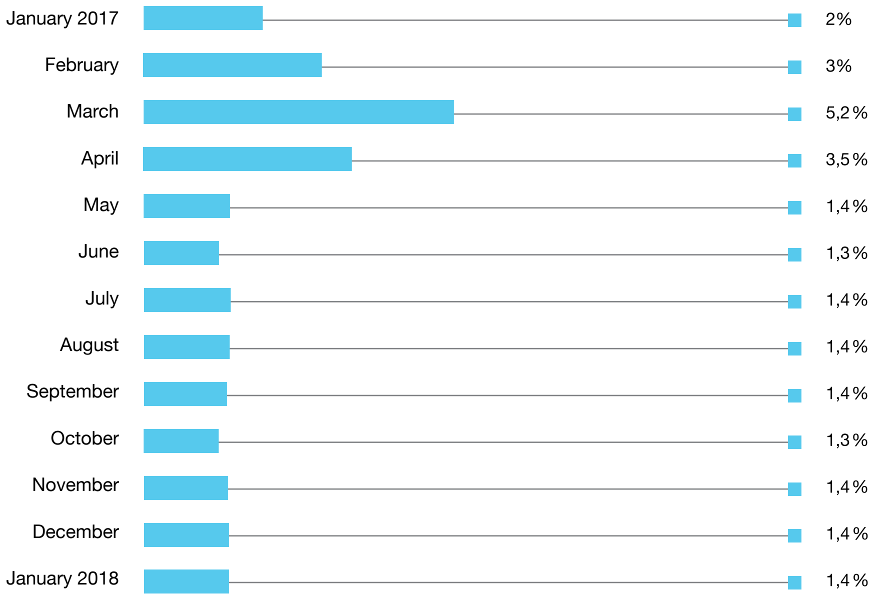


Figure 33 *Percentage of infected users in broadband networks.*

CERT Orange Polska recommends:

1. We should not use simple passwords. The default factory password should be replaced, and if possible, multi-factor authentication should be used, e.g. password and an additional token.

2. If WPS is operated, but we are not using that function – we should disable it.

3. If the UPnP function is not necessary, we recommend disabling it.

4. Device administration is best conducted from the internal network, after closing the VPN tunnel.

5. We should ensure regular monitoring, and (if a new version is available) updating software.

6. Using the "port forwarding" function is not recommended, unless it is a deliberate and thought-out action.

7. Access to a device interfacing with untrusted networks should be blocked from the side of WAN, unless we have ensured access on a high level of confidentiality, e.g. VPN.

8. For wireless devices, the strongest cryptographic algorithms are recommended, as well as strong passwords, using the RADIUS protocol, and filtering MAC addresses by setting the policy to "block others".

9. In case of registering solutions we should check (configure) the data storage method. Many operators offer uploading pictures and other kinds of data to cloud. It is a good practice to verify who manages such a cloud, whether the data is not disclosed to anyone, and in what way access to this data is secured.

10. Data transmission devices (both at home and in the office) that we use should allow managing them via appropriate interface. This rule applies to "intelligent" devices installed at points of interconnection of internal networks with public networks.

11. Cryptographic security measures should be applied in communication with services, or with accesses.

12. It is recommended to use alternative software (developing, supported) in case of lack of newer versions of the current software – especially when vulnerabilities appear

13. In case of businesses, regular scanning of the infrastructure is recommended.

14. In case of decommissioning a device, we should take care of data anonymization. Restoring the device to factory settings does not always cause removal of the configuration file from internal memory.

15. It is recommended to provide a "guest" area in the internal network for people unauthorized to use the trusted segment of the network. This kind of solution can be applied at home, as well as in the office, and lecture or conference rooms.

16. If possible, we should enable the option to log events which may indicate security breach attempts. A good solution would be to send such events to an external system monitoring this kind of events.

Partner's commentary

Michał Sajdak

Founder and consultant service Sekurak.pl d/s IT security Securitum. He has ten years of experience in issues related to technical IT security. He implements safety tests. The holder of the certificate: CISSP, CEH, CTT +.

In the context of IoT, year 2017 was, in my opinion, a little more peaceful then 2016 (when for example the Mirai botnet was being discussed). Does it mean that we have got the (in)security of the Internet of Things under control? Nothing could be further from truth – this looks like a clam before the storm. Initiatives such as bitnet IoT reaper (https://sekurak.pl/iot-reaper-nowy-botnet-uzbrojony-w-eksploity-na-urzadzenia/) are a proof of this – it is one of the rare cases where utilized are not only access passwords to devices, but also exploits – oftentimes for vulnerabilities, that have been just made public.

What is also worrying, are the new exploits allowing mass interception of devices. Here the CVE-2017-17562 vulnerability is certainly worth mentioning, (https://sekurak.pl/zaglada-iot-jednen-z-najpopularniejszych-serwerow-http-w-iot-podatny-na-zdalne-proste-wykonanie-kodu/) occurring in a popular webserver – GoAhead - used in IoT devices. The vulnerability allows to intercept a device remotely, without possessing the authentication data, and in most cases the attacker gains all privileges - root.

Using websites such as Shodan, one can easily locate almost a million devices using that websever. On one hand, there is no telling whether they are vulnerable, on the other – IoT manufacturers are not known for prompt patching, which is additionally passed onto users. Did the year 2017 lack in hot news from the world of IoT? Of course it did not. Here, the research of the Checkpoint company is worth bringing up, showing how one can intercept an intelligent vacuum cleaner – along with the feed from its camera (https://sekurak.pl/zhackowali-odkurzacz-mozliwosc-zdalnego-sterowania-dostep-do-feedu-video-ofiar/).

Another innovative idea (although carried out in laboratory conditions) was also the presentation of a worm attacking intelligent light bulbs, and propagating itself wirelessly. Here, with the adequate density of IoT devices, one could "intercept an entire city" (https://sekurak.pl/przygotowali-robaka-atakujacego-iot-bezprzewodowo-potrafi-przejmowac-cale-miasta/). It is also disheartening to see a simple administrator's password (5147), embedded permanently into the firmware of one of devices monitoring radiation in nuclear power plants (https://sekurak.pl/systemy-monitorujace-promieniowanie-w-elektrowniach-atomowych-haslo-admina-5147/)

In my view, the most spectacular attacks are still ahead – especially, that it is hard to see more professional approach to security in creators of the IoT world.

7.4 Social-engineering based attacks and the role of phishing

Who has never received a spam e-mail, cast the first stone. Year by year, the percentage of unwanted e-mails in comparison to the rest of the messages is becoming smaller, but still, in the past four years, 6 out of 10 e-mail messages are spam.

10 years ago, the first association with spam would be messages written in poor Polish, or e-mails offering gigantic amounts of money from inheritance of some stranger, which we would supposedly get in return for sending the scammer a fraction of this sum. And miracle cures for impotence of course. Today's times mean messages impersonating specific, well-known brands, which are more and more difficult to distinguish from genuine ones. The reason? It is no longer about buying "medicine" of unknown origin, or a direct scam. Now clicking in the wrong place ends with theft of our login and password at best, and in worse cases either in a break-in to our computer (or company network), or encryption of our files until we pay an expensive ransom.

Today a criminal does not have to be an expert in the field of malicious software – that is the least of his concerns, as supply of ready-to-use solutions available on the market greatly exceeds demand. The key is to convince the user to install the malicious software delivered to him, and here comes social engineering. The basic rules of manipulation were described best by the guru of social psychology Robert Cialdini:

- Reciprocity. We are "programmed" to return favours. Even if we received something that can be be easily found on the internet, in turn, we may automatically give back confidential information, or simply click on a link sent to us, without considering where it can lead.
- Commitment and consistence. Once we take a certain stance, or make a decision, it is very hard to back out from it, even if a cognitive dissonance occurs. If the offender will convince one person that he has the right to access confidential information, that person may lend credence to his version.
- Social proof of righteousness. If enough people view something as good/beneficial, somewhat automatically we see it similarly. On Facebook we oftentimes click the "like" button on profiles liked by a sufficient number of our friends without considering the credibility of such profiles.
- Fondness. As a rule, we will gladly help the people we know and like. We will to such an extent, that we may, from the force of habit, open an attachment from an e-mail received "from them", which may turn out to be a virus sent without their knowledge.
- Authority. The magnitude of the power of authority has been proved by scientific experiments, as well as by the fact of how many people still gets tricked by phishing e-mails. In short, if someone says that he is calling us from a serious-sounding organization, looks like a CEO of a corporation, or drives an expensive car, does not necessary make him credible. Just as a counterfeit antivirus program is not worth our trust, just because it bears a striking resemblance to a real one.
- Shortage. The knowledge that we may run short of something affects our assessment of the situation. This does not only concern commercial products (limited time offer), but also time. Most of us have encountered – or use – the "But I'm in a hurry!" argument. If someone is in a hurry, and we get convinced by him, it is very probable that we will forget about security.

In case of phishing campaigns, it is also worth to highlight the existence of something called a "call to action" in marketing. A call to action, expressed in an insistent way, often accompanied by a threat using words like "immediately", "important", "security", "consequences", "blockade" etc. – all this is meant to evoke anxiety in the victim, and as a result, provoke immediate reaction. And later, well – later it is all over.

[4] https://www.statista.com/statistics/420391/spam-email-traffic-share/

7.4.1. Analysis of phishing campaigns in the Orange Polska network

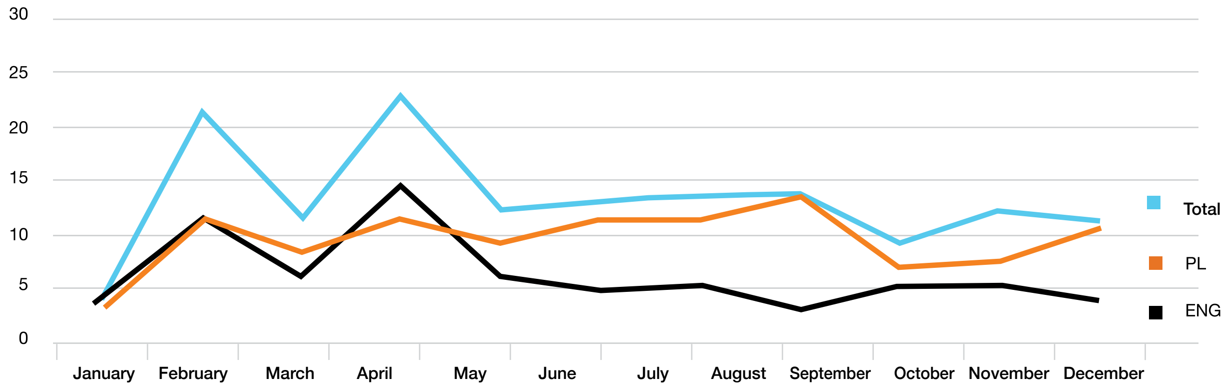


Figure 34 *Unique phishing campaigns detected in the Orange network in 2017.*

In the year 2017 CERT Orange Polska highlighted 146 specific phishing campaigns, detected in the Orange Polska corporate network. 94 of them (64%) were in English,
and the remaining 47 (32%) in Spanish and German.

The most popular topic of the analysed phishing (39 campaigns – 26,71%) were impersonating courier companies, which confirms the trend generally observed in this field. A significant percentage also included messages about a necessity to pay an outstanding invoice/receipt, or a return of a mistakenly sent bank transfer. The most interesting of e-mails which found its way into the CERT Orange Polska's researchers was… divorce papers from "the wife's lawyer". Here the offenders' artfulness may be something to envy – a great "call to action", very few men would not automatically open such an e-mail.

It is worth mentioning though, that none of the phishing campaigns conducted by Thomas - probably the most popular, and certainly the most "prolific" wrecker attacking Polish internet users with Vortex ransomware, has made it into the corporate network.

7.4.2. Internet service user awareness – how to protect ourselves from such threats.

It could seem that internet users know very well how to protect themselves from phishing – statistics however, suggest otherwise. Most of all, it is worth to repeat this advice ad nauseam, until it gets into our head, and we will automatically refrain from doing certain things. So, let us remember to:

How to protect yourself against phishing?

- Implement the rule of limited trust in relation to all messages in any way connected with the matter of finances, or our sensitive data.
- When using banking websites, or the ones of any service providers, get into the habit of checking the URL in the browser's address bar. In some cases, the addresses contain the name of the bank, but e.g. in the *.info.pl, or *.top domain.
- Carefully read the contents of every suspicious message; when in doubt, compare it with previous e-mails from that sender.
- Before clicking on any link, check where does it lead (by holding the cursor over it). If it is in any way suspicious – do not click.
- Analyse everything that the browser displays – e.g. security certificate error.
- Treat all „calls to action" evoking an emotional response in you as a red flag.
- If a link in an e-mail redirects you to a form which you are supposed to fill with your sensitive information, make sure if this is what was supposed to happen.
- Do not open invoices "out of curiosity" if you are not expecting them.
- **When in doubt – contact the alleged sender.**

Partner's commentary

Adam Haertle

Renowned speaker, trainer and lecturer. Since the year 2004 he regularly performs at all significant conferences dedicated to security in Poland, where he receives the highest ratings in participant surveys. Lecturer of two postgraduate courses at SGH and Bialystok University of Technology. In 2017 he gave over 70 lectures dedicated to the matters of security in the web, dangers of using electronic banking, privacy, and data protection in businesses, for open and closed audiences all across the country. In his lectures, he describes real threats awaiting businesses and users, using simple language and real-life examples. He deals with security professionally since over dozen of years, first in the Deloitte company, and later in UPC, where for 12 years he was responsible for all matters regarding data protection in the country and region. Since six years he runs the ZaufanaTrzeciaStrona.pl website, one of the largest Polish-speaking web pages dedicated to data security.

When I talk with the auditors of my raising user awareness lectures in companies all across the country, and when I read correspondence from the readers, I see that the era of attacks taking advantage of browser exploits is long gone. People used to say "don't go to any phony websites, you'll catch something". Today, thanks to increased level of security of browsers, and elimination of the most dangerous plug-ins, attacks through WWW sites have become a rarity. Most criminals have chosen an easier way to the users' computers, meaning electronic mail.

Over 90% of infections analysed by our team start this way. Flooded with hundreds of e-mails every day, employees do not have the time to analyse if the message just received is malicious, and whether they should click on a certain attachment, or to held back and call the helpdesk. We also cannot put all our trust in solutions filtering the mail – sure, the better ones filter out most of the threats, but even if we will set up three intelligent boxes one behind the other, there will be always a malicious message that will make it through those fences. It is also hard to 100% trust the antivirus, because although it is very useful, correctly identifying most malicious e-mails or their attachments after a couple of minutes, some people will click faster than the antivirus downloads new threat signatures.

Does that mean that we should come to terms with infections of our computers? Nothing could be further from truth. We should be ready for them, as at some point they will surely happen, but attacks on e-mail can be successfully fended off. The combined effect of filtering, and antivirus systems along with proper staff training makes it more and more difficult to access the victim's mailboxes and convince them to install malicious software. It is also worth remembering that just as signatures in antivirus programs, training should be updated in the employees' heads. It is no coincidence that the highest amount of messages saying „Thank you for a great lecture, we have managed to get the infection before it could get us thanks to it" I receive in the first weeks after the lecture, and later their number decreases – until the next lecture.

7.5 Attacks using telecommunications networks – SS7

Signalling System 7 (SS7) is a set of protocols used in telecommunications networks, introduced to the market in the year 1975. SS7 establishes and disconnects telephone calls, manages phone numbers, (number translation and portability services) tarification services, the SMS service, and many others. The SS7 system is the "cardiovascular system" of a telecommunications infrastructure. It allows communication between its key elements (digital networks based on 2G, 3G, 4G and intermediary standards) within one telecommunications operator, as well as between operators.

7.5.1 Threats connected with SS7

System SS7 possesses low level of security, because at the time of its implementation, meaning 40 years ago, the market of telecommunications services looked radically different. Most of all, operators were far less numerous, and their networks were treated as trusted. The situation has changed immeasurably with the introduction and development of the so-called added-value services, the realisation of which proceeds in cooperation with businesses unrelated to telephone networks. Today, cyber-criminals can buy access to a telephone network easily, and thanks to the introduction of the SS7 over IP, they only need a normal computer to conduct an attack, not specialized equipment.

The most critical threats connected with SS7:

Signal message category	Ð			1	2						3					
Threat \ SS7 signal message (MSISDN/IMSI Ð identifiable subscriber numbers)	fuzzed message	MAP_MT_FORWARD_SHORT_MESSAGE	MAP_PROVIDE_ROAMING_NUMBER	MAP_ANY_TIME_INTERROGATION(MSISDN)	MAP_PROVIDE_SUBSCRIBER_INFO(IMSI)	MAP_INSERT_SUBSCRIBER_DATA(IMSI)	MAP_DELETE_SUBSCRIBER_DATA(IMSI)	MAP_RESET	MAP_UNSTRUCTURED_SS_NOTIFY(MSISDN)	MAP_UNSTRUCTURED_SS_REQUEST(MSISDN)	MAP_PURGE_MS(IMSI)	MAP_UPDATE_LOCATION(IMSI)	MAP_REGISTER_SS(IMSI)	MAP_MO_FORWARD_SHORT_MESSAGE(MSISDN)	MAP_PROCESS_UNSTRUCTURED_SS_REQUEST(IMSI)	ISUP_IAM(MSISDN)
Location tracking (cell_id)				X	X											
MO call/SMS intercept						X										
MT call/SMS intercept						X						X				
DoS for targeted subscriber						X	X				X					
DoS of telco infrastructure	X							X								
Subscriber Account Fraud based on IRSF						X	X									
Call, SMS, USSD impersonation/spoofing														X	X	
Operator fraud (SMS Faking)		X														
USSD spam (usually not charged)									X							

SS7 message types:

Category 1	Not expected from interconnect
Category 2	Expected only for visitors from their home networks
Category 3	Expected only from subscribers in roaming

The most critical vulnerability of the SS7 protocol is connected with the Mobile Application Part layer (MAP) in the control plane dedicated to mobile networks and responsible for providing roaming services.

Almost all services can be provided using roaming, and because of this, the spectrum of possible attacks taking advantage of the SS7 protocol vulnerability is very wide. Unprotected networks (which used to be a common negligence a few years ago) are exposed to hazards such as e.g. determining location of the subscribers, intercepting SMS, eavesdropping on phone calls, and also attacks blocking access to services.

Thankfully, not all attacks can be successfully carried out in all networks. Operators have begun implementation of adequate solutions addressing the threats. Some attacks of this kind can be easily blocked, especially if they are based on signal messages not expected in the inter-connection traffic (category 1). If the attacks are based on signal messages occurring in the inter-connection traffic, more advanced methods of their filtration and analysis will be needed.

7.5.2. How to plan the development of a telecommunications infrastructure to minimize the effects of such attacks

The most effective method of securing an SS7 network is in-depth analysis and layer approach, as advanced attacks require gathering a certain amount of data, a process which cannot be conducted using a spoofed address. The attacker may be stopped during the following phases: acquiring access to the network, data gathering, and the actual attack.

How to stop the attack in its different phases:

1. Access to the network (in the control plane)

- Only allowing addresses associated with roaming partners
- Scanning addresses from the inter-connection traffic based on which addresses are expected on certain code points;
- Blocking our own addresses form the inter-connection traffic (in order to prevent bypassing any filters implemented in the internal network)

2. Gathering data from the networks and data of the users (data protection)

- Protecting the user's IMSI number and his location (information about the VLR he is using) using proxy for the type of the messages expected from the inter-connection traffic, such as SRI_for_SM (Send Routing Information for Short Message)

3. The actual attack (defence, or at least detection of the attack)

- Blocking signal messages not expected from the inter-connection traffic
- Blocking signal messages with inconsistences between the SCCP and MAP layers
- Blocking signal messages expected form the inter-connection traffic exclusively to guest-subscribers from their home networks, if they concern the home location
- Blocking signal messages expected from the the inter-connection traffic exclusively to guest-subscribers from their home networks, if a mismatch between the sender of the message, and the subscriber whom it concerns occurs (caution should be exercised, due to the potential risk of affecting internationally shared infrastructure)
- Blocking/detecting malicious network traffic on location data, and possible speed of the basing subscriber's movement (caution is advised due to GSM networks on ships).

[5] IMSI, International Mobile Subscriber Identity – a unique number assigned to each SIM card in telecommunications networks.
[6] VLR, Visitor Location Servicer – rejestr abonentów gości.

7.5.3 Directions from which malicious SS7 traffic comes to the OPL

Below we present a graph with the amount of malicious signal messages in December of 2017:

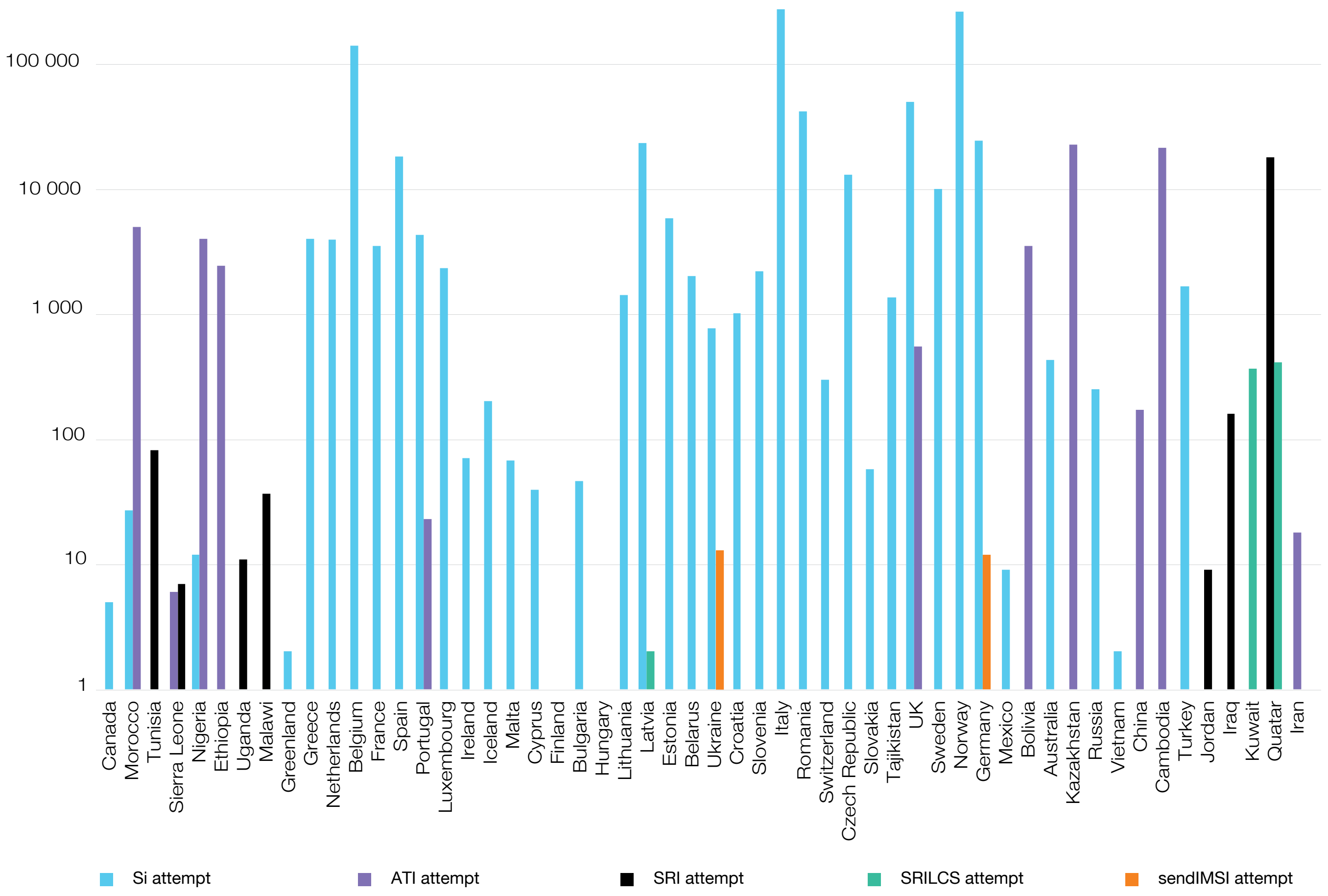


Figure 35 *Amount of malicious signal messages in December of 2017*

Partner's commentary

Philippe Langlois
Philippe Langlois is an Information Security worldwide expert in Network and Telecom with more than 20 years of experience in telecom and network security. He successfully founded several industry-leading companies in security including Qualys (US, NASDAQ: QLYS), INTRINsec (FR), WorldNet (FR), WaveSecurity (US), TSTF (EU) and P1 Security (FR). He conducted security missions such as audit, pentest, hardening, vulnerability analysis, risk analysis and threat intelligence in Telecom and Network domains. Philippe defined new methods and created appropriate tools to audit SS7, IMS and SIGTRAN networks through heavy R&D work. He led world-class pioneering work in vulnerability assessment product development such as in Qualys and INTRINsec. He also led the development of a number of complex system architectures in security products, ASP services and ISP/MSP infrastructures, and built and motivated international engineering teams, around security products and services.

In 2017, the SS7 signaling vulnerabilities still remain a significant threat directed towards the mobile operators and their core network infrastructures. This trend was identified all through the Year, as a vast number of the SS7 attacks were publicly known/revealed and several attack simulators were published on the Internet. The requirements, professional skills and knowledge needed by the attackers have significantly decreased over the past years and now the attacks can be conducted by a wide range of actors.

The main motivation for attacking SS7 signaling networks remains the same: mainly fraud, geolocation, SMS spam and call interception. The technical reason for this usage of SS7 is mostly because the VoLTE and SMS over LTE Signaling protocol deployment is progressing slowly. Voice and SMS services are still covered by legacy SS7 protocols and mobile phones are still served by 3G and 2G networks. This situation can both be expected in the near future and unfortunately also in the long term, because of the roaming scenarios.

Most of the mobile networks worldwide are under continuous signaling attacks or under probes which try to test the networks for vulnerabilities. The most common attacks are basic signaling attacks conducted through single messages, however we also detected multiple advanced attacks coming from specific network origins, indicating probable nation-state attacks. Monitoring solutions / Intrusion Detection Systems may help enable early discovery, prevention of attacks and continuous monitoring of the network for vulnerabilities. Regular and proactive vulnerability scanning of signalling networks could also help early detection of the network vulnerabilities.

From a legal/regulation perspective the situation got attention and is closely followed by Congress and Department of Homeland Security in the USA and by ENISA in the European Union. The telecom industry has recognised these security issues and is trying to take actions on its own. The largest mobile operators now closely collaborate and exchange the results of their research inside the GSMA Fraud and Security Group, where the work is also accelerated by private companies acting as associate GSMA members. Telecom operator groups most often follow the research, invest into their security and take preventive and proactive actions. However, there is still inadequate protection and a lack of knowledge and awareness inside the smaller operators and in some specific Regions of the World.

7.6 Social Media – the most important abuse

Examples of social-engineering based vectors of attack using social media

- **Giveaways**.
  "For free" is one of the keywords in today's world. Consumerism is on the increase, causing us to want every shiny gadget, so in a situation where someone wants to give us something free of charge, or even for filling a form – we get easily tricked. Phones without protective foil, gift cards, airplane tickets, Robert Lewandowski's car, these are just a few examples. The threat is not so great if we only have to like some page, and the aim is to later sell such a "like farm" to someone who needs the likes. It gets worse, if the authors of such scams require us to send an identity-confirming SMS – that may cost us from several, to several hundred PLN.

- **Who viewed my profile?**
  There is no way to determine who has been viewing our profile. Facebook does not give developers access to data necessary to create such tools. Their alleged installation may end in infecting the computer.

- **Hot first-hand news**
  Every time, when the world is shaken by some sensational news, it is worth to remain cautious before clicking on the "here exclusively" placed on fanpages unrelated to the media we know.

- **Shock and gore**
  "OMG", "Shocking!", "see DEFINITELY", "What have he/she done!?" – These types of simple slogans playing on primal emotions still incite interest. After clicking, it usually ends with a message, that the video material requires a (fake) Flash update, under the guise of which malicious software is installed.

- **Help me my friend, I have been robbed**
  This scam has recently gain popularity. The victims were receiving desperate messages from their Facebook friends, with a plea for quick financial support. The sender was supposed to be abroad, where he had been robbed of documents and money, having only his phone left, and asking for a transfer to the closest Western Union point. The friend was sitting at home or work at this time of course, when the offender had broken into his account (using e.g. one of the methods described here).

- **From the life of celebrities**
  Another sign of our times is popularity of people who are known for being well-known. Criminals are aware of that, thus regularly appearing fake information about accidents or deaths of famous people. Right after the clicking, e.g. in the background of the news piece in a frame invisible to the viewer, anything can be placed – from giving a like, through granting privileges to an external application, ending with installation of malicious software.

It is worth highlighting – which has been proven by examples many times described in the year 2017 – that social networks are a perfect place for spreading disinformation, the so-called "fake news" popularised by i.a. politicians. Certain groups invest plenty of time, money and human resources into distributing, mainly through Twitter and Facebook, information meant to sow doubt and anxiety, or antagonizing important social groups. This is worth remembering when we engage in discussion about serious, oftentimes political topics through social. We should consider how much of the content we read feels natural, and how much of it seems fabricated.

How to protect ourselves?

It is worth to pay attention if the website address is known to us, and is it a renowned informational website. Unfortunately, websites distributing fake news often encourage visiting them by advertising themselves as independent media, writing about things that others are "not allowed to", or simply claiming to base their information on truth. Bearing this in mind, we should pay special attention to websites, blogs, and social media groups promoting themselves with such slogans.

Distribution of propaganda, or speaking broader, elements of the process of manipulating informational environment is very similar to cyber-attacks. With the use of social engineering, the user is encouraged to interact witch such an object, and then packages of disinformation are sent to the "acquired" viewer among the informational noise created to lend credence to the false content.

Among other things, this is the reason why fake news is so successful and has this kind of range. On the internet we should most of all apply one rule: verify the source of information. We can also avoid becoming a recipient of manipulation by following notifications about identification of such processes in the informational environment of the cyberspace.

Partner's commentary

FUNDACJA bezpieczna cyberprzestrzeń

Cybersecurity Foundation

Social media offer more and more functionalities to their users. More interaction between websites and their users entails more risk connected with security. Greater amount of information shared using social media entails more risk connected with attacks using social engineering as a basis for exploiting user's weaknesses.

The basic threat comes from the vulnerability created by the constant access to the mass amounts of information published on the user's time list. Information habits, using materials sent by friends combined with information placed on the website as propositions by the website's algorithm result in the creation of informational noise, which in effect amplified the vulnerabilities.

The user becomes accustomed to the flood of information, loses his guard, and as a result it becomes easier to "smuggle in" infected material to him, or to influence him using selected information.

It is worth noticing, that the society gives into manipulation, which to some extent can affect worldview, and as a result the audience's decisions. Internet and media became an area of activity for governmental and non-governmental actors, for whom informational environment and attacks on ICT systems become an aspect of conducting military operations.

Fake news campaigns, disinformation, and mass distribution of propaganda expose internet users to oftentimes fabricated informational environment.
Paying attention to sources of information seems necessary, along with higher level of criticism towards the vociferous headlines and content created basing on insinuation, questions, or pure opinion.

Social media hide also other areas for manipulation. Opinion groups, forums and leaders do not always have to be real. Oftentimes popular user groups are in fact fabricated resources used to constantly shape the viewers.
Recommendations:

Partner's commentary

Piotr Konieczny

A security expert helping the largest Polish and foreign companies with safeguarding their networks and web services. A graduate of Glasgow Caledonian University. A winner of multiple awards for the best lectures at the biggest Polish conferences dedicated to IT security. The founder of Niebezpiecznik.pl, a counselling company consulting IT projects in the matter of security. In Niebezpiecznik.pl Piotr manages the audit team, and penetration tests of ICT systems, as well as conducts training for administrators and programmers, as well as for regular employees of Polish companies, who in certain aspects of their professional responsibilities use computers and the internet.

Although Mark Zuckerberg admitted that the number of Facebook users is decreasing for the first time, unfortunately this does not go in pair with the number of attacks registered by the editorial board of the Niebezpiecznik website among Polish Facebook users. There are still throngs of Polish internet users who lose money by subscribing to Premium SMS services, after it turns out that the fanpage they have just liked have just sent them a shopping voucher to spend at Biedronka (a chain of inexpensive supermarkets in Poland) or a discount coupon for clothes at H&M (see https://niebezpiecznik.pl/post/falszywy-profil-media-expert-na-facebooku-w-2-dni-oszukal-tysiace-osob/). The trick that most of fake fanpages base upon is quite clever. The list of winners published by the organizer of the fake contest consisted of links to the profiles of the "winners", and always on the second or third position there was link to the person currently logged in to Facebook. Everyone was the winner! However, to claim the reward, you had to fill a form, the downloading of which required providing your phone number, and then confirming that you are an adult by re-writing a four-digit PIN number sent to you in an SMS. Wait, what? Unfortunately some people were so blinded by the joy of winning, that the quite clear message in the SMS message saying "you will be receiving SMS messages with jokes three times a week, costing 21 PLN each" ceased to be visible for them.

But Facebook frauds are not only fake profiles impersonating popular brands, but also our very friends. And I do not mean the "Hey man, are these your pics?" questions well-worn over the years, leading to a file infection our computer with malicious software (see: https://niebezpiecznik.pl/post/ktos-wrzucil-tu-twoje-przerobione-zdjecia-z-facebooka-uwaga-na-nowy-atak/). Since some time, our friends on Facebook, being actually criminals who have intercepted their accounts, are using more and more advanced social engineering. They claim to have been robbed while travelling, and they need 100 PLN to buy a return ticket. Thankfully, their credit card was in a different pocket than the wallet, so they ask for a transfer to the account assigned to the card. They will use a cash machine. Of course they have no funds on this card, because it is the end of the month, and they have spent everything. Or the beginning of the month and their salary has not arrived yet. They send this kind of request to all friends of the victim whose account they had intercepted. Thanks to this, they receive 100 PLN not once, but up to several dozen times. That is quite a pay for a dozen minutes of talking with a dozen people. And let us get this clear, this does not require any kind of special hacking abilities. This is why we are going to see more such attacks with different vectors of attack. Recently, a request for help with paying for an order in an online store "because my bank doesn't work" became popular, or for help with investment into crypto-currencies.

Because of the "How not to get hacked" lectures given all across the country (see: https://niebezpiecznik.pl/jak-nie-dac-sie-zhackowac/), I had the opportunity to speak with many victims of such attacks in person. What shocks me most in the stance of the people who gave criminals access to their accounts, by falling for phishing earlier, are claims such as "I don't really care for my Facebook account, let them hack it, I don't keep anything important there ". You do, victim, you do. Your friends who trust you, and which – thanks to this trust – can be robbed by a criminal in your name. This is why if someone cares about keeping good relationships with their friends, not only of Facebook, he should safeguard the access to his accounts. Facebook (but also many other services) offers quite a lot in this matter. It is definitely worth to enable two factor authentication, best basing on U2F keys, as only then phishing will not be able affect us. If a criminal will extort our password, he will not do anything without a physical U2F key, which needs to be plugged into the computer during the login for a moment, or touché to our phone.

It is also worth to regularly skim through the list of applications which we have connected to our Facebook account, and if we have not been using some for a longer time, to uninstall it. Take a look at it now, and you may be surprised how many applications from external manufacturers, which you have forgotten about, and they still have access to your data tam.

And one more advice, which may prove useful not only in the context of attacks using social networks: block the Premium SMS service at your mobile operator (see: https://niebezpiecznik.pl/post/nie-daj-sie-naciagaczom-zablokuj-uslugi-premium-rate-radzimy-jak-to-zrobic/). In many attacks, not only the ones using Facebook, this is how victims are being robbed. Sometimes, you do not even have to click, you simply enter a perfectly normal website, and you automatically subscribe to such kind of thing (see: https://niebezpiecznik.pl/post/czy-to-ty-uwaga-na-nowy-scam-na-facebooku-ktory-moze-cie-drogo-kosztowac/).

7.7 The most important security vulnerabilties, and attackson applications

Cyber-criminals take advantage of vulnerabilities in software, protocols, and network services. Sometimes it happens, that there is no information concerning specific vulnerabilities, or that they remain undetected for years, which causes the exploit market to grow. Described here, are the most critical vulnerabilities of 2017 and ways to avoid.

7.7.1 Analysis of the most dangerous vulnerabilities of systems and applications

Eternal Blue (CVE-2017-0144):
It is commonly assumed, that this exploit was used by the American NSA. Information about it has leaked to the public as a result of theft by a group going by the name Shadow Brokers.

The vulnerability used by EternalBlue is located in the svr.sys driver in the Windows system family. The error consists in wrong configuration memory buffer size for the needs of the driver's operations.

The exploit using this vulnerability allows remote execution of code at the root level. In practice this means performing any operation in the infiltrated system, without restrictions connected with authorization, and very few little traces in the logs. According to the Common Vulnerability Scoring System CVSSv3 the vulnerability was rated 8.2/10.

The exploit has been used in a number of ransomware families, i.a.: WannaCry, NotPetya, and BadRabbit, in order to create an efficient mechanism of propagation. In the result of high severity of the vulnerability, epidemics of those families grew into incidents of international scale in a matter of a dozen hour. This happened despite the fact that – as say some researchers analysing those families – they were designed to propagate only within local networks.

Orange recommends:

To resolve this vulnerability in Windows systems, we recommend installing the MS17-010 security patch available from Microsoft. Regular software updates – is the first and most basic step to secure yourself from attacks. Disable the SMBv1 protocol. It is an out-dated file sharing protocol, counting around 30 years now, and it can be used by various kinds of malicious software. Threats can be avoided by disabling this protocol as the system's administrator. If a user wants to secure himself more efficiently, blocking ports responsible for SMBv1 may be the way. Those ports include the 445 TCP port, and ports from 137 to 139 UDP. They can be easily blocked using Firewall.

CVE-2017-0037 i CVE-2017-0059:
Both vulnerabilities are present in new versions of Internet Explorer and Edge software.

The CVE-2017-0059 vulnerability allows memory leak using a use-after-free type of error. CVE-2017-0037 vulnerability, on the other hand, uses an error connected with variable identification in html processing engine. In combination with the former vulnerability, it allows remote execution of code with privileges of the browser's user.

Both vulnerabilities have been adopted by the Disdain exploit pack (software allowing creation of websites automatically infecting the users who open them). Up until now the exploit pack has been used for installation of various kinds of malicious software – from bank Trojans to ransomware.

Orange recommends:

- Install Internet Explorer patches going by the numbers MS17-06 and MS17-07
- Install and update antivirus software
- Do not open suspicious websites

RSALib

In 2017 an error in the implementation of RSA encryption has been discovered in a popular library (RSALib), which is currently used in many products (i.a. Infineon Technologies chips) partaking in encryption, digital signature and authentication.

RSA is one of the most popular asymmetrical cryptographic algorithms with a public key. The name comes from the first letters of the algorithm's creators – Ron Rivest, Adi Shamir and Loeonard Adleman. Its security lays in the difficulty of factorization of large composite numbers.

Factorization of the public key consists in finding prime numbers p and q, thanks to which we gain the private key component. Familiarity with other components of this algorithm also makes the factorization easier and faster. The process is difficult and time consuming due to the use of large numbers, so the longer the key the more time it takes to factorize it – currently, the recommended minimum size of the key is 2048 bit.

Researchers have discovered, that during the creation of large prime numbers, the RSALib library uses two several-dozen-bit constituents, which radically lower the entropy of the prime numbers generated (a prime number counting 512 bit in this case has 99 bit entropy).

There exist two techniques relating to this vulnerability:

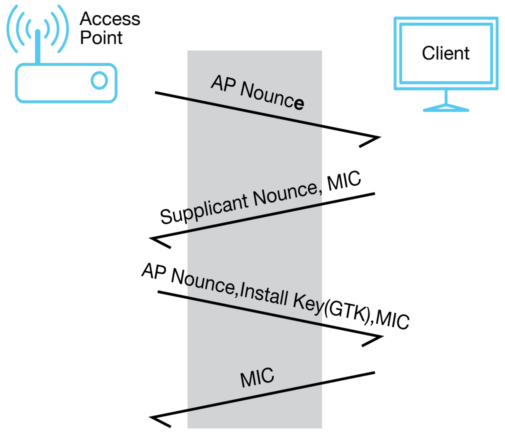
1. Fingerprinting – a technique allowing verifying if a given RSA key has been created using the RSALib library
2. Factorization – finding the p and q prime numbers

Orange recommends

- To protect ourselves against the use of vulnerability in the RSA encryption, we should install patches released by hardware and software manufacturers (i.a. Microsoft, Google, HP, Lenovo etc.)

KRACK

In October 2017 a vulnerability was detected in the WPA and WPA2 protocols. An attacked called KRACK (Key Reinstallation AtaCK) takes advantage of a vulnerability in the beginning stage of connecting a client to a WiFi device. The devices initiate encryption key negotiation (4 way handshake), the process looking as below (PSK):



1. Nouce is a value generated by the AP, unused before. In the first step it is sent to the client

2. The client generates its own value, and basing upon it, as well as on the AP nouce, and AP and the client's MAC address, it creates a PTK key, and sends back its own nounce value along with a MIC control sum (Message Integrity Code).

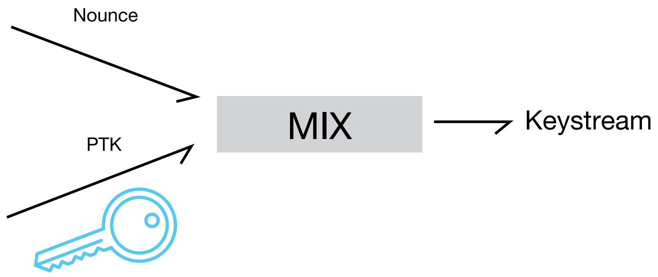
3. The AP verifies the data received, and generates a PTK key basing upon the client's nounce, and the MAC of them both, and sends back a GTK (Group Transient Key). The client then installs the key that was sent.

4. The client sends a confirmation with a control sum.

In this model, the PTK key is not sent by either party, but rather created basing on the nounce value, and the key previously established for both machines (PSK). In case the packages are lost (package 4 will not be delivered to the AP), the AP will send package 3 several times.

The vulnerability consists in the fact that subsequently receiving package 3 by the client causes the session key to reset, coming back to its original values. This significantly lowers the security of encryption, because in many protocols (CCMP, GCMP) it is required, that a certain key was only used once. If this does not happen, the attacker may be able to decrypt the traffic, inject packages, etc. To take advantage of this vulnerability, the attacker "barges into" the traffic between the client and (MitM) and adequately blocks the transfer of package 4, so that the AP will have to force re-installation of the key by sending the package 3 again.

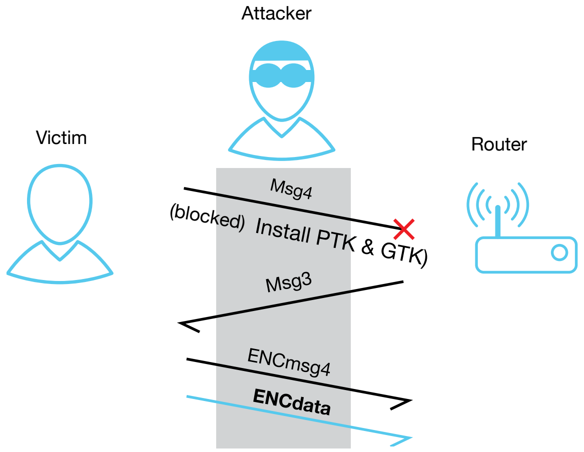
The key generating process comes to calculating a keystream basing upon nounce and PTK, thanks to which we encrypt the packages:



The attacker has an easier task when it comes to Android and Linux systems. It turns out that the system servicing a wireless connection after a subsequent reception of package 3, resets the serial key to null value, so in this case decrypting the traffic is easy.

The attacker places himself between the vulnerable client and the device (MitM) and passes the package between those two parties, with the difference being that he does not do that in case of package 4, so the router sends package 3 again to continue the transmission. The vulnerable device sends package 4 again, but it is already encrypted. Package 4 is almost the same before the re-transmission (it differs slightly), so the attacker knows the value of the encrypted package 4 and knows that the same key has been used for re-transmission. From there, decrypting the package is simple.

The whole process is presented below:



By operating (XOR) on encrypted and unencrypted msg4, the attacker is able to reconstruct the keystream used for encrypting msg4, which means he is able to encrypt the remaining data.

The attacker has an easier task when it comes to Android and Linux systems. It turns out that the system servicing a wireless connection after a subsequent reception of package 3, resets the serial key to null value (the attacker does not have to possess msg4 in an encrypted and decrypted form to recover the keystream) so decrypting the traffic is easy.

The example presented above concerns a vulnerability in a device connecting with AP. However, a protocol allowing reinstallation the key in AP - Fast BSS Transition (FT, 802.11) is also vulnerable, as are some routers working in client.

The least vulnerable systems are Windows and iOS, because the implementation of the 4 way handshake deviates from the standard. These systems are vulnerable to attack on the group key (GTK), though.

How can we protect ourselves?

- First, we should check for updates for the devices we are using. Similar to any case, installing them is necessary. When it comes to KRACK, basically all devices equipped with Wi-Fi are vulnerable.
- Preparation of adequate updates is time consuming, though, so many devices do not have them. In such case, we should pay special attention to the networks we are using, especially the public Wi-Fi networks, which we should generally avoid.
- If we are forced to use a public network, it is better not to exchange important information, or log into our accounts, especially the ones connected electronic banking – eventually, we can do this using a VPN, where the connection is made through a specially encrypted tunnel. Thanks to that, no one will be able see our authorization data.
- The recommended solution is owning a personal mobile internet connection, which greatly lowers the risk.

OWASP – a new classification of threats

In the year 2017, a threat update to OWASP Top 10 has been released. It is a document raising awareness of the people engaged in creating web applications, concerning the most common security vulnerabilities. The last update took place in the year 2013.

While comparing the two versions, some changes in the security of web applications landscape can be noticed. In the new version, risks connected with XXE, unsecured de-serialisation, or insufficient monitoring, and the points concerning CSRF threats and incorrect redirections have been removed. Presented below, is the comparison of the two versions from the year 2013 and 2017:

2013
A1. Injection
A2. Broken Authentication and Session Management
A3. Cross-Site Scripting (XSS)
A4. Insecure Direct Object References
A5. Security Misconfiguration
A6. Sensitive Data Exposure
A7. Missing Function Level Access Contr
A8. Cross-Site Request Forgery (CSRF)
A9. Using Components with Known Vulnerabilities
A10. Unvalidated Redirects and Forwards

2017
A1. Injection
A2. Broken Authentication
A3. Sensitive Data Exposure
A4. XML EXternal Entities (XXE)
A5. Broken Access Control
A6. Secuirity Misconfiguration
A7. Cross-Site Scripting (XSS)
A8. Insecure Deserialization
A9. Using Components with Known Vulnerabilities
A10. Insufficient Logging & Monitoring

Explanation concerning specific OWASP 2017 positions:

A1 Are various kinds of code injection on the side of the server: SQL, NoSQL, OS commands, LDAP

A2 Is wrongly implemented way of authorization, e.g.: of logging mechanism, session tokens or keys.

A3 Is lack of sensitive data protection, and allowing third party access to it, without additional means of protection (e.g. encryption)

A4 Is lack of correctly configured XML engines, which makes it possible to read files, execute a code remotely

A5 Is an extension in the privileges of an already logged user, making him able to modify data of other users, change access policies etc.

A6 Is lack of changes in default settings, leaving generic accounts/passwords, unconfigured HTTP header fields, or error reports containing sensitive data

A7 Is lack of data validation coming from the user, concerning e.g. execution of a Java Script code, which allows redirection, theft of cookies, session keys, and other sensitive.

A8 Is lack of validation of the data which was to be. Sometimes it allows for an execution of a code.

A9 Is using libraries and modules which contain errors

A10 Is insufficient logging of the user's activities. An attacker can use this to remain undetected (by e.g. taking unlogged actions).

Top ports scanned

1433	A standard Microsoft SQL Server port, often scanned by bots searching instances of databases protected by weak passwords or vulnerable to attacks
5060	The default port for the SIP protocol, dominating signalling protocol for VoIP
7547	A port responsible for remote management of the end user's devices.
2323	Used in communication with Internet of Things devices, intensely scanned by the Mirai botnet
137	One responsible for connecting IP addresses with the names of computers
8080	One used by many web proxy and application services, i.a. Syncthing GUI, M2MLogger and Apache Tomcat server
123	Port 123 is used by the NTP (Network Time Protocol) service, used for time sync in ICT and telecommunications systems
81	Port TCP is used for communication between hosts
3306	A port for MySQL – the most popular system for managing relational databases
1900	A port for the SSDP protocol, used for detecting UPnP (Universal Plug-and-Play) devices; a common target of DDoS attacks

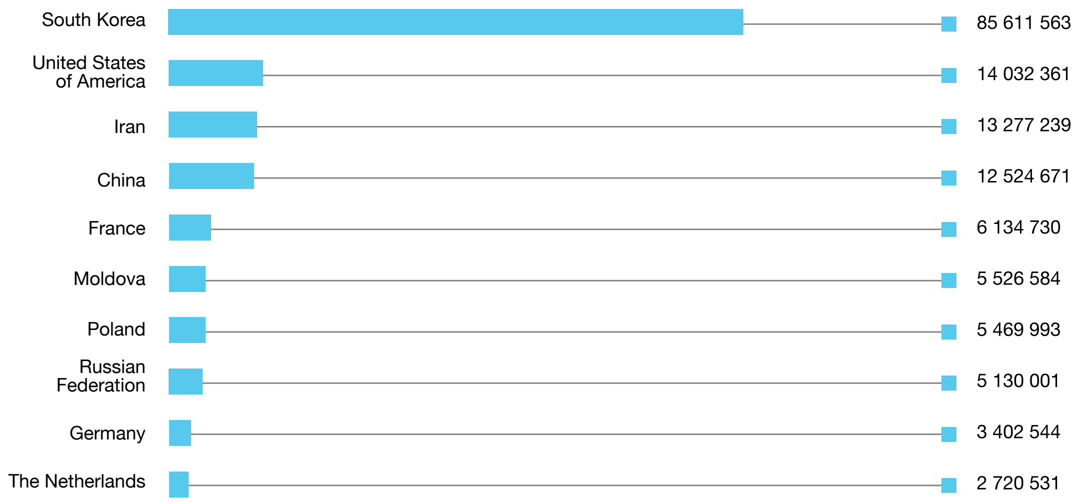


Figure 36 *The greatest number of scans.*

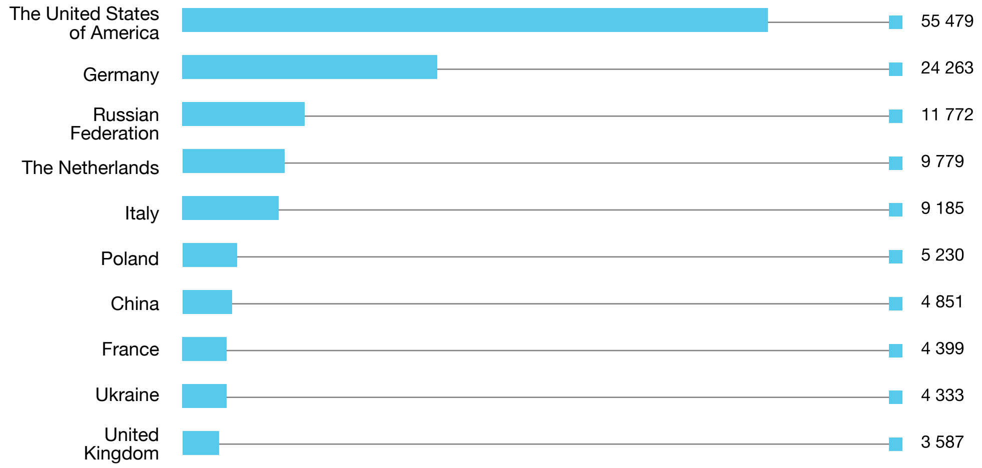


Figure 37 *The greatest number of scans with the greatest number of unique ports.*

How can we protect ourselves?

Vulnerabilities in software will always exist. There is no ideally written application, just as there is no absolute, guaranteed security. Application security should be understood in a wider context, by keeping track of the threats approaching. Every error in the code, every vulnerability, may cause an application we are using for business or private purposes to cease functioning properly, and as a result, services and data becoming compromised.

– At the development stage, it is recommended to perform regular inspections of the source code, and subject the subsequent versions of the finished application to security tests.

– If we are using a ready-made solution (no matter if dedicated one, or an open source one). We should remember about updating it. Of course, this also concerns operating systems. It is a necessary condition to eliminate vulnerabilities in applications, and to prevent known threats (exploits) from disrupting their proper function.

– In operator solution and large businesses, solutions such as WAF (Web Application Firewall), can be used. Their purpose is to block remote (network) attacks in the application layer, by using application errors (types of attacks for WEB applications are described in the “OWASP – new threat classification” section of this report.

– It is recommended to separate particular layers of business systems. They should be divided into as many OSI model layers as possible, meaning the presentation, application, and database layers.

– In case of network devices functioning in the L3 OSI layer, and e.g. being a part of architecture of intelligent houses w – in the first place we should find out whether appropriate updates are available for those devices. As I any other case, it is necessary to install them, or at least to contact the solution’s provider. When KRACK is in question, basically all devices equipped with Wi-Fi are vulnerable.

– If a vulnerable device has an “End of Life” or “End of Support” status, we should consider eliminating it, replacing its firmware with an alternative one, provided by the online society, or using it in a different segment of the network, one with a low security status.

Partner’s commentary

Borys Łącki

For more than 15 years associated with IT security. Author of dozens of lectures at professional conferences (Confidence, SECURE, Attack and Defense, Internet Security Banking, SecureCON, SEConference). Specialist in penetration testing in LogicalTrust (www.logicaltrust.net) – a company providing complex information security services. For over 7 years he has been tracking cybercriminals targeting unaware users and he has been publishing his observations and warnings on his blog http://bothunters.pl/”

Since over a dozen of years we observe a repeating pattern. Every year new, shocking security errors appear, but along with them, there also appear new, more and more interesting ways of bypassing security. Year 2017 was not an exception here.

By analysing the most sophisticated attacks we can see that despite the fact that the newest operating systems and applications have plenty of additional security measures, making it supposedly impossible to successfully apply unknown attacks, people with enough skill and motivation are still finding ways to bypass those solutions. And even though the costs of attack rise with every year, the increasing number of solutions being connected to the network (systems, applications, devices) present in our daily life, the constant need to support old systems, and the still insufficient testing of certain areas of IT, the forthcoming future seems to be abundant with new incidents and challenges.

The quickening race between those conducting attacks, and those trying to protect their resources, is a fact we have to face. As the year 2017 has shown, the role of the defender sill become especially difficult, as criminals more and more eagerly take advantage of vulnerabilities in extortion software (ransomware). As incidents in companies such as Maersk, Merck or TNT have shown, even a several-week of delay in delivery of security patches, today may result in hundreds of millions dollar losses. The beginning of 2018 and security errors in processors (the “Spectre” and “Meltdown” vulnerabilities) have shown that we can expect new vulnerabilities in even the most surprising elements of the infrastructure.

Companies wanting to better protect their resources should remember that in risk analysis, even the darkest scenarios should be taken into consideration. Basing upon over a dozen years of experience in security testing, I think that businesses should focus primarily on systematic approach to vulnerability management. Unfortunately, todays cyber-criminals only need several hours to adjust malicious software to newly discovered vulnerabilities present in our systems. This is why conscious shortening the time of presence of known vulnerabilities, as well as quick and dynamic reacting to new threats is so important.

8 CERT Orange Polska

CERT Orange Polska is a specialized unit functioning since over 20 years in the structures of Orange Polska, responsible for swift and professional analysis of threats appearing in the internal Orange Polska network, customer networks, and the Wide World Web.

The team's main task is taking necessary action in situations threating resources of Orange Polska's customers, as well as contributing to raising awareness concerning threats in all users of the internet, through publications on services hosted by the CERT OPL team.

CERT Orange Polska provides support for the Orange Polska network users in the field of reacting to security threats in their own ICT systems, and at the same time being a trusted point of contact for other users involved in the cases processed.

Structurally in the organization, CERT Orange Polska is located in the operating area of the ICT infrastructure and Cyber-security. In Orange, apart from autonomous operations of specific CERT teams in certain companies/countries, there exists a team in the parent company, Orange-CERT-CC, which can coordinate operations for the entire group, if such a need arises. This kind of cooperation is of huge value for the specific teams in terms of exchanging experiences.

CERT Orange Polska works in close cooperation with Security Operations Centre (SOC) OPL. The operators of the 1st line of SOC support work 24/7/365 monitoring the level of security of our network's users, accepting requests, reacting to identified incidents and taking threat-minimizing measures. Analyst and expert teams of further lines of support (including CERT OPL) support the daily work of the operating line in case of occurrence of more complex events, not covered in procedures of reaction to standard incidents.

CERT OPL analyses trends in the development of threats, as well as tests and analyses the consequences of their occurrence. The team communicates with internet users through publications posted on the CERT Orange Polska website, Orange's blog and through Twitter. Below are CERT Orange Polska website's visiting statistics. A significant increase in the number of visits in the main CERT OPL website follows every time threat to internet users occurs. We have observed a clear increase on 2nd of January, they day of launching an informational campaign in the CyberShield.

The category "the number of unique views of the StopPhishing websites" has been monitored since June 2017. The increase of the StopPhishing websites registered in July has been caused by the phishing campaigns impersonating morele.net and DotPay.

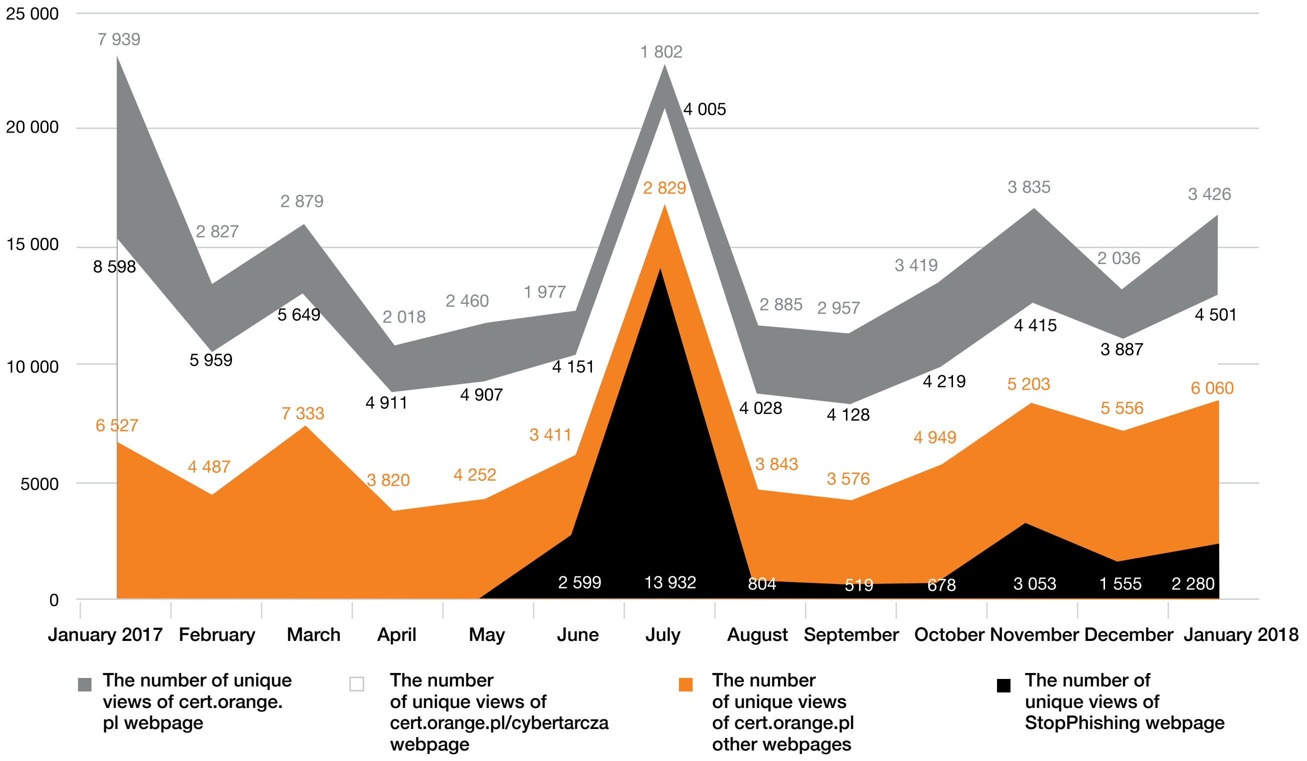


Figure 38 *The number of unique views of cert.orange.pl webpage*

8.1 Cooperation with other organizations and security teams

CERT Orange Polska participates in the operations of the largest organization associating CERT – FIRST (Forum of Incident Response and Security) teams in the world. Above all, this means a confirmation of the high level of competence of the CERT Orange Polska team by an independent organization, which proves the high level of effectiveness of analyses, elimination of security threats in the Orange Polska network, and ensuring continuity of services.

Within the framework of domestic cooperation CERT Orange Polska has founded, and takes part in the works of Abuse Forum – an informal organization associating representatives of the largest Polish telecommunications operators, internet services providers, social media, and also public administration bodies, including ministries and central governmental authorities. Quarterly meetings and mailing list serve the improvement of communication and strengthening cooperation, thanks to which we can be even more effective in preventing and reacting to threats appearing in the web. Aside from these operations, we collaborate with similar organizations within other subjects at the operational level, on a regular basis, in case of detecting threats that might affect them (i.a. counterfeit invoices with malicious software for the alleged services provided by third-party companies received by the customers of Orange Polska).

In 2017, Orange/CERT OPL team in association with CERT Polska - NASK became the organizers of an event in connection with TF-CSIRT. This will be the 54th assembly of the members of CSIRT/CERT.
The event will take place in Warsaw, in the second half of May 2018. The event will take place in Warsaw, in the second half of May 2018. The assembly's agenda, including lectures and workshops, is in preparation and will be made public under the following address: https://tf-csirt.org/tf-csirt/meetings/54th-meeting/

Last minute update:

Orange Polska as the only Polish telecommunications operator and the only European provider of Orange Group services, became a member of the global MANRS (Mutually Agreed Norms for Routing Security) initiative in February of 2018, created to prevent abuse in the field of routing security.

We have received certificates in four fields:

- Filtration: ensuring the validity of our own, and the customers' packages outbound to the neighbouring networks
- Anti-spoofing: allowing validation of the source address for our own customer networks, end users, and infrastructure
- Coordination: Maintaining globally available, up-to-date contact information
- Global validation: Publishing our own data in order to allow the other members to validate the routing information on a global scale

8.2 Orange Polska services taking advantage of the CERT team experiences

Orange Polska constantly improves the services connected with the security of its customers from threats coming from the Wide World Web. The matter concerns technological solutions supporting the Orange Polska services in the higher layers, e.g. the application layer.

- **CyberShield.** On the operator's network level, we protect Orange network users with mechanisms of the CyberShield, filtering out gloal network threats in a manner completely transparent to the user. The effectiveness of the protection provided by the CyberShield has been confirmed by the interest put into it by foreign operators collaborating with Orange Polska – they are planning to implement this solution in their own infrastructures.
- **Safe Starter.** Simple, transparent, uncluttered, not requiring installation, nor configuration parental control service. Just insert a dedicated SIM card into the mobile device to prevent the child from entering inappropriate websites (pornography, paedophilia, disturbing content, etc.)
- **Protect Children in the Web.** Expanded, paid version of the parental control with the feature of advanced configuration. The parent can determine the websites blocked for each child individually, black and white lists, and also assign permissions for each and every installed application, control the time spent in the internet, and while using certain applications. In the parent's panel, detailed reports concerning the use of the device appear.

CyberShield after another year of functioning has proven its effectiveness. Detailed data concerning malicious software can be found in chapter 7.1.

The CERT Orange Polska team constantly improves this solution, allowing effective filtration of traffic every day. This is achieved by perfecting threat detecting algorithms, developing Cyber Threat Intelligence, building and developing our own feed base, and supplying it with new data. In the year 2017 we have detected thousands of infection within the network, of which several thousand users have been effectively informed about the most significant threats.

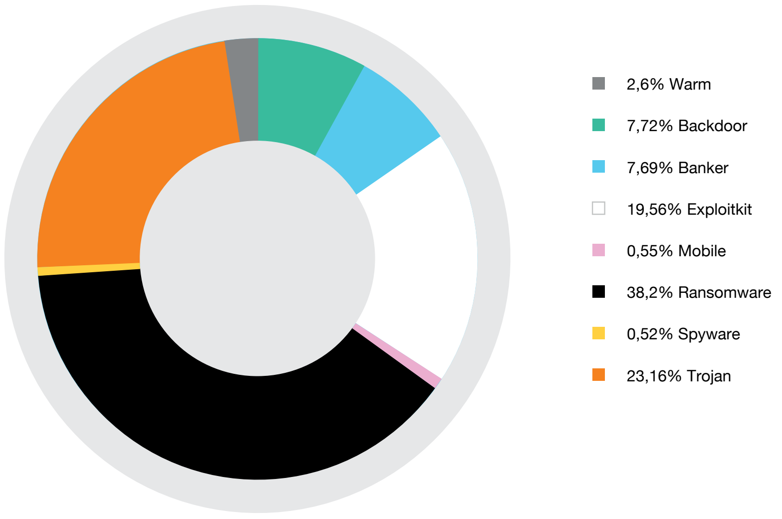


Figure 39 *Blocked events by CyberShield in 2017*

Safe Starter is a dedicated service for mobile devices. It works basing on the principle of classification of the resources viewed in the global internet network, and blocking suspicious services. Using the safe starter when registering a SIM card allows more efficient potection, as it is the adult (parent) who decides what SIM card will the child be using.

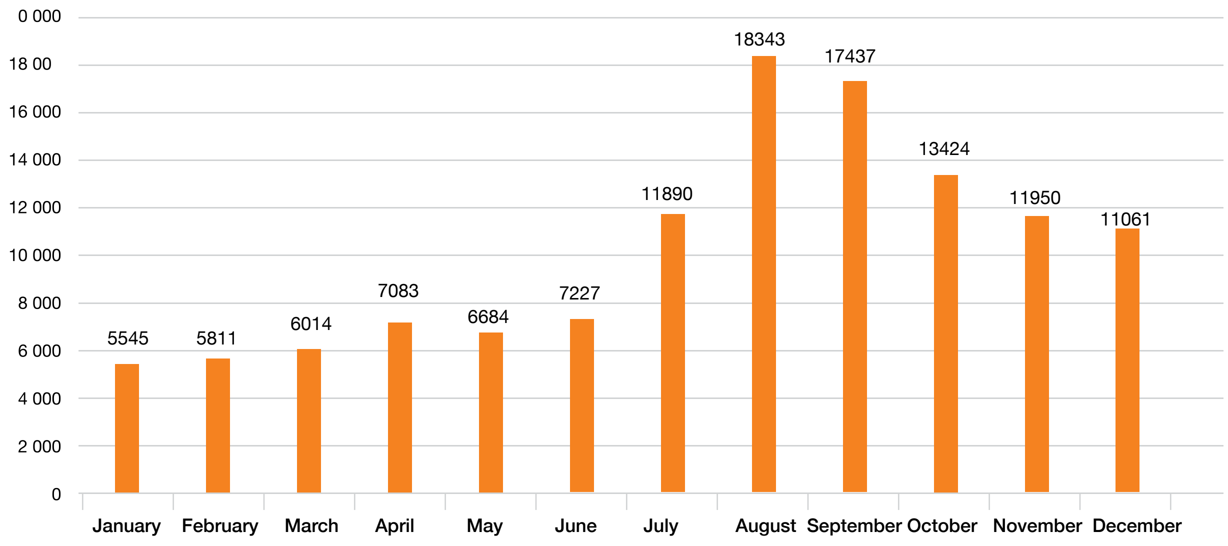


Figure 40 *Infections in Mobile Orange Polska network (IPv6)*

8.3 Contact wth CERT Orange Polska

CERT Orange Polska aims to reach internet users with a concise message that will be devoid of technical jargon and to the point, one that if regularly repeated, has a chance to get into the heads of the most susceptible victims of the attacks. The main source of education is the CERT Orange Polska website (https://cert.orange.pl/) and the operator's blog (https://blog.orange.pl/). The first of the websites gathers information on a number of topics concerning security, suitable for different kinds of viewers – starting with easy-to-understand topics for regular internet users, (security alerts, new threat descriptions, operation patterns of cyber-criminals, etc.), through information on vulnerabilities, and detailed malware analyses useful for people with expertise in the matters of networkand security. The blog on the other hand, describes threats in the context of particular events which took place in Polska and around the world, in a clear and comprehensible manner, updating every Thursday.

The best way to stay updated on the information from CERT Orange Polska jest following our account on Twitter. Under the address 🐦 https://twitter.com/cert_opl there can be found the newest information on phishing campaigns targeted at Orange Polska's customers, malicious software analysed by our experts, as well as notifications about the newest entries on the https://cert.orange.pl/ website, and if needed – an option to ask us a question.

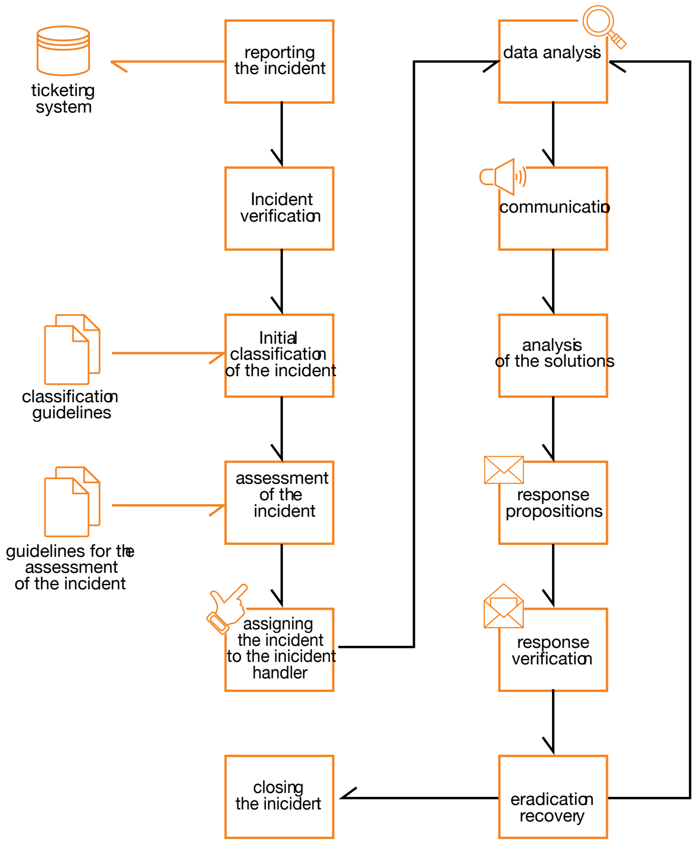

ticketing system
reporting the incident
Incident verification
classification guidelines
Initial classification of the incident
guidelines for the assessment of the incident
assessment of the incident
assigning the incident to the incident handler
closing the inicident
data analysis
communication
analysis of the solutions
response propositions
response verification
eradication recovery

Figure 41 *Computer security incident management workflow*

8.4 Procedure of reaction to a computer incident

Incident reaction procedure consists in an orderly arranged set of actions took by the members of the CERT OPL team, and by other cells engaged in conducting an effective analysis. The incident management process is composed of several steps:

1. Registration and verification of a report
2. Preliminary effect evaluation (triage)
3. Assigning the person responsible for handling the incident
4. Handling the incident
5. Closing the incident

Registration of the an incident report has two common sources: a user reports an improperly functioning device, service, application, etc. or the break-in detection systems (IPS, IDS, SIEM) indicate abnormal behaviour in the network.

During the registration of an incident report, the staff performs its verification in three aspects:

- Is the report of suspicion of incident occurrence in fact a security incident,
- Does the report concern the area of operation of the CERT OPL team (is it within its "constituency"),
- Does the report not concern an already registered incident.

The next step is performing a preliminary classification of the incident, and evaluation of its significance (how serious its effects may be). Basing on that, incidents and their management are assigned adequate priority.

The priority of incident management may depend on several factors:

- the type of the incident
- the incident's influence on the organization's business processes (customers')
- type of the data, the security of which has been compromised by the incident

the security of which has been compromised by the incident

- the possibility of restoring the systems affected by the incident (time and resources)
- the type of customer being serviced by CERT (indicated by the SLA agreements)
- the type of the subject reporting the incident (e.g. media or the government)

Assigning the right priorities to the incidents is particularly important in case of massive and complex ICT attacks, and it is the key to choosing the fastest incident reaction strategy.

Each of the incidents should have a staff member (incident handler) assigned, responsible for its handling.

Generally speaking, the person who has been appointed as fitting to react to the incident, should act according to the procedure presented below:

1. Data analysis
2. Communication
3. Solution analysis
4. Choice of strategy and proposals for action
5. Verification of actions
6. Liquidation of the incident's effects

It is worth taking notice that all the steps should be taken in several cycles, in which the subsequent steps should be as follows:

1. Limitation of the incident's effects (isolation of network segments, work stations, redirecting traffic, securing evidence)
2. Liquidation of the effects (removal of incident sources, system restoration))
3. Restoration of production services (testing them for correct operation)

The last step, often unappreciated, is closing the incident, meaning documentation of the team's actions, filling in the information about the incident, particularly: who and when has first noticed the indications of the incident, what was the incident's range, how were the incident's effects limited, what was the strategy for removal of the malicious software, and what was the procedure of restoration of the production services.

9. How to protect financial institutions or companies, both large and small – Orange Polska security services

The increasing use of ICT systems in all aspects of running a business causes an increase in value of information, and as a result, the necessity to efficiently protect it. Here reaction time to potential threats that could affect our business counts. Orange Polska offers services, thanks to which you can minimize the risk in case of many kinds of threats. There is something for everyone.

9.1 DDoS protection

What are DDoS (Distributed Denial of Service) attacks: A dispersed attack, meant to block access to resources, most commonly:

- attacks on the bandwidth necessary for providing a service, e.g. ICMP/UDP,
- attacks aiming to deplete systems resources e.g. TCP SYN,
- attacks on applications, e.g. attacks using the http, DNS, or VoIP applications protocols.

When to use: Unavailability of service

What it's about: Protection of the customer's online resources from volumetric denial of service attacks. Network traffic is monitored 24/7/365 for anomaly detection. In case of an actual attack, we filter out the suspicious packages, so only normal network traffic reaches the customer. Used as a support for the solution Flow Spec mechanisms introduced into Orange networks, allow interception and mitigation of volumetric attacks of very large scale.

How it works: It is a combination of three elements: SOC and CERT Orange Polska teams, Arbor Networks platform, and the use of operator mechanisms in domestic and international traffic (dnssinkholing, blackholing etc.).

For whom: For everyone using the World Wide Web network (WWW) and possessing their own infrastructure.

Benefits:

- Ensuring security of business processes and information
- Constant monitoring of traffic and identification of occurrence of potential threats
- Competences of Operational Security Centre experts available 24/7/365
- Immediate defence against attacks at the customer's infrastructure
- No need to invest in adequate infrastructure and flexible accounting model, thanks to cloud computing

9.2 Monitoring security incidents

What is it: A constant process of identifying incidents, and notifying people responsible for managing the infrastructure.

How it works: By searching information about suspicious events (incidents) in the logs of the systems monitored.

Available solutions applicable separately or in packages:

9.2.1 SIEM as a Service

When to use: If you want to be able to identify incidents in the whole infrastructure, keep data in a place and manage it efficiently

What it's about: Implementation or sharing the functionality of the SIEM system with the customer, in order to gather significant events from systems, applications, and their correlations, and search them for security incidents

How it works: A choice of an appropriate system for the customer's needs and budget, delivery of a complete solution, which means its installation, availability and monitoring 24/7/365, integration of log sources, formulation and implementation of security scenarios

For whom: For everyone responsible for infrastructure and data maintenance

Benefits:

- Constant monitoring and identification of security incidents
- Immediate notification of people responsible for the infrastructure and protected data about
- Flexible tailor-made model, i.e. option of running it at the customer's place, or in a cloud

9.2.2 SOC as a Service

When to use: If you want to centralize security operations to quickly react to potential threats.

What it's about: A pre-made incident monitoring process, using competences of the Security Operations Centre (SOC) Orange Polska team – cyber-security operators, analysers and experts monitoring the customer's systems and data through e.g. SIEM.

How it works: A process involving integrating data from the customer's systems (a console, SIEM system data and other) with a rapid incident response team.

For whom: For everyone responsible for infrastructure and data maintenance, as well as for people bound by the regulations concerning quick response to incidents (e.g. RODO, KNF)

Benefits:

- A pre-formulated process of incident processing
- An experienced team of experts ready for work
- Lower costs – no need for building a team of specialists and competences from scratch
- Immediate notification about incidents

9.3. Feed as a Service

What is it: A compendium of knowledge concerning threats identified by CERT Orange Polska in the cyberspace, especially in the Orange Polska network.

What it's about: Delivery of information about malicious activity observed on the internet, especially in the Orange Polska network (malware, C&C, other).

How it works: An automated process of information delivery as CSV text files, or API mechanisms in defined formats, containing data about so-called C&C servers, domains and IP addresses of web services infecting browsers with malicious software, IP addresses exhibiting malicious activity towards Orange Polska network (ports scanning, attack attempts etc.).

For whom: All organizations maintaining security systems.

Benefits: Reinforcing the systems possessed with unique data gathered by CERT Orange Polska.

9.4. Vulnerability tests

What is it: Detecting and classifying the customer's system's vulnerabilities, which may be used for taking over it, stealing sensitive data, and other actions leading to image and financial losses.

When to use: In order to check the system's vulnerability to potential threats.

What it's about: Using the knowledge and experience of CERT Orange Polska (White Hat Hacker), specialist software, which scans the customer's infrastructure, and generates a report with a list of detected vulnerabilities. Basing upon it, the CERT Orange Polska experts will prepare a list of the most important recommendations that should be implemented to avoid the use of the vulnerabilities by potential offenders.

For whom: Organizations possessing their own ICT infrastructure.

Benefits: Evaluation and quick identification of security gaps and expert recommendations concerning improvement of the customer's infrastructure's security

9.5 Penetration tests

What is it: Practical evaluation of the current security status, especially the presence of known vulnerabilities, and resistance to security breach attempts.

When to use: In order to test security mechanisms in the customer's infrastructure.

What it's about: An attempt to gain unauthorized access to the customer's chosen ICT system, using the white box/ black box method.

For whom: Organizations providing their infrastructure to other parties in the web.

Benefits:

- Evaluation and quick identification of security gaps and expert recommendations concerning improvement of the customer's infrastructure's security
- Objective and independent evaluation of factual level of the system's security.

9.6 Performance tests

What is it: A controlled DoS/ DDoS type attack at the chosen elements of the customer's ICT system (network link, servers, services, internet node) conducted in order to evaluate the resistance to DDoS type attacks.

What it's about: Analysis conducted from the viewpoint of a potential offender, using the team's competences, traffic generators, pre-formulated scenarios of network attacks, and the transport network of the Orange Polska infrastructure.

When to use: In order to test the security measures against DDoS type attacks

For whom: Organizations providing their infrastructure to other parties in the web

Benefits:

- Quick system security evaluation concerning DDoS type attacks
- Recommendations CERT Orange Polska concerning improvement of the system's security
- Objective and independent evaluation of factual level of the system's security.
- The option to define individual scenarios with the customer.

9.7 Malware Protection InLine

What is it: Protection of the customer's network resources by preventing and detecting malware infections attempting to permeate to the client's infrastructure from the internet.

What it's about: The customer's traffic at the Internet Point of Presence is monitored and analysed for the presence of malicious code in the files.

How it works: Malware is detected using techniques connected with detailed analysis of an attack. Suspicious network flows are reconstructed in virtual machines conducting advanced analyses of malware behaviour in an environment simulating the actual customer's environment (Sandbox). The process is based on behavioural analysis of code, which also allows identifying advanced (APT) attacks and zero-day malware. The customer's infrastructure's outgoing traffic is analysed for the connection of malware with the so-called C&C servers.

For whom: For everyone using the World Wide Web network and possessing their own infrastructure

Benefits:

- Quick identification and blockade of malicious software activity
- Protection from new-generation cyber-security threats of the APT and zero-day type
- No need of investing in service-protecting devices
- Protection from the customer's employees carelessness.

9.8 Malicious software analysis

What is it: An analysis of malicious software delivered by a CERT Orange Polska customer as a part of a service.

What it's about: Behaviour evaluation concerning the malicious activities observed, (i.a. establishing IP addresses of Command&Control servers, IP addresses of domains), of the code delivered by the customer, by running it in a series of strictly controlled virtual environments of Orange Polska.

How it works: The result of the Orange Polska's analysis is a report from works describing the detected threats of malware's malicious activity in the system, along with the description of methods of its propagation.

For whom: For customers who want to check their software for an eventual occurrence of maliciousness, and become aware of its influence over the infrastructure

Benefits:

- Availability of the CERT Orange Polska's expert team and laboratory
- A report concerning the identified maliciousness, and its influence over the customer's infrastructure
- Recommendations of CERT Orange Polska concerning threat minimization.

9.9 Secure DNS

What is it: Prevention of the consequences of a DDoS type attacks aimed at the customer's DNS infrastructure

What it's about: Geographical dispersion of the servers responsible for the customers' DNS. The queries always end up in the geographically (network-wise) closest server.

How it works: Orange Polska uses the "anycast" technology – tested and proven on the internet since many years. Worldwide networks providing the .com and .pl domains are functioning in this technology. Secure DNS consists of over 40 nodes, located in the Orange network, as well as other networks in Poland, and abroad, across five continents. The responses from the closest node will come with maximum speed, through shortest possible route, without delay.

For whom: For customers providing online services, internet domains owners

Benefits:

- Redirecting attacks from the customer's own infrastructure to DNS servers
- Increasing the availability of DNS services
- Zwiększenie dostępności usług DNS
- Quick and easy service configuration, as well as handling of changes
- Geo-location of responses
- Option to fully outsource the customer's DNS service using the Secure DNS infrastructure.

9.10 Stop Phishing

Co to jest: Blocking traffic network coming from a phishing website created by a cyber-criminal.

What it's about: Minimization of the consequences of phishing attacks, especially blocking network traffic to identified phishing websites, aimed at the customer's web service users (e.g. home-banking).

How it works: An active blockade of network traffic between Orange Polska network users, and servers or domains identified as elements of a phishing campaign. By using the SOC and CERT Orange Polska team, we can guarantee a swift blockade of the campaign, and notification of other rapid-response teams about the identified incident (CERT teams, alternative operators).

For whom: For customers providing online services (e-commerce).

Benefits:

- Minimization of the scale of attack by reducing the number of potential victims
- Lowering the costs of incident processing on the customer's side
- Significant reduction in the image risk connected with the customer's brand.

9.11 Web Application Firewall (WAF aaS)

What is it WAF?: Web Application Firewall platform is located in the backbone network of Orange Polska.

What it's about: Unavailability of services connected with the customer's application.

What it's about: Protection of the customer's resources form application attacks. The entire http/https traffic from the internet to the protected resources is being redirected to a service platform, and subjected to analysis according to the established security policy.

How it works: It allows protection from the most critical web application threats defined in OWASP Top 10, and allows increasing the security of web applications without the necessity of modifying their code.

For whom: For everyone using the World Wide Web, and possessing their own infrastructure.

Benefits:

- Ensuring the security of information and business processes
- Constant monitoring of traffic and identification of occurrence of potential threats
- Competences of the Security Operation Center experts available 24/7/3655
- Immediate defence against attacks at the customer's infrastructure
- No need to invest in adequate infrastructure and flexible accounting model, thanks to cloud computing

10. Dictionary

AaS (ang. as a service) – an abbreviation that refers to services provided to the customer via the Internet.

Abuse – misuse of some capabilities of the Internet, i.e. inconsistent with the purpose or the law. Internet abuses include: network attacks, spam, viruses, illegal content, phishing, etc. An Abuse Team is a unit responsible for receiving and handling reported cases of abuse.

ACK "acknowledge" - one of the TCP flags set to confirm the network connection.

Adres IP (ang. IP address) – IP address (Internet Protocol address) a unique number for each device (e.g. computer) on the Internet, allowing its unambiguous identification in the network.

DNS Adress – used for naming devices on the Internet. It consists of domain names separated by periods. It is convenient for users and uses DNS hierarchical structure to translate it into IP address that is understandable for devices on the network.

Backdoor – "back door"; a vulnerability of the computer system created purposely in order to obtain later access to the system. A backdoor can be created by breaking into the system either by some vulnerability in the software or running a Trojan unknowingly by the user.

Blackholingfrom "black hole" – an action of redirecting network traffic to such IP addresses on the Internet where it can be neutralized without informing the sender that the data did not reach its destination.

Bot from "robot" – an infected computer that is taken over and performs the attacker's commands.

Botnet – "network of bots" – infected computers remotely controlled by an attacker. Botnets are typically used to run massive DDoS attacks or send spam.

C&C (*ang. Command and Control*) servers – an infrastructure of servers that is operated by cybercriminals, used to remotely send commands and control botnets.

CERT/CSIRT (*Computer Emergency Response Team, Computer Security Incident Response Team*) – a computer incident response team. The main task of CERT is quick response to reported cases of threats and violations of network security. The right to use the name CERT have only teams that meet very high requirements.

CISSP (*ang. Certified Information Systems Security Professional*) – an internationally recognized certificate confirming the knowledge, skills and competences in the field of network security.

Datagram - a block of data sent between computers on the Internet.

DDoS (*ang. Distributed Denial of Service*) – a network attack that involves sending to a target system such amount of data which the system is not able to handle. The aim of the attack is to block the availability of network resources. A DDoS attack uses multiple computers and multiple network connections, which distinguishes it from a DoS attack that uses a single computer and a single Internet connection.

DNS (*ang. Domain Name System*) - a protocol for assigning domain names to IP addresses. This system has been created for the convenience of Internet users. The Internet is based on IP addresses, not domain names, therefore, it requires DNS to map domain names into IP addresses.

DNS address – used for naming devices on the Internet. It consists of domain names separated by periods. It is convenient for users and uses DNS hierarchical structure to translate it into IP address that is understandable for devices on the network.

DNS sinkhole – DNS server that sends false information, making impossible to connect the target website(s). It can be used to detect and block malicious network traffic.

Domain name – a name of a domain; used in the URL to identify the addresses of websites. Examples of domains are .gov, .org, com.pl.

Exploit – a program that allows an attacker to take control over the computer system by exploiting vulnerabilities in operating systems and software.

Exploit 0-day– 0-day exploit - an exploit that appears immediately after the information about the vulnerability is published and for which a patch is not yet prepared.

Exploit kit – software that is run on servers, whose purpose is to detect vulnerabilities.

Firewall – software (device) whose main function is to monitor and filter traffic between a computer (or a local area network) and the Internet. Firewall can prevent from many attacks, allowing early detection of intrusion attempts and blocking unwanted traffic.

Honeypot – "honey pot"; a trap system, that aims at detecting attempts of unauthorized access to a computer system or data acquisition. It often consists of a computer and a separate local area network, which together pretend to be a real network but in fact are isolated and properly secured. From the outside, a honeypot gives an impression as if it contained data or resources attractive from the point of view of a potential intruder.

HTTP (Hypertext Transfer Protocol) – a communication protocol used by the World Wide Web. It performs as a so-called request-response protocol, e.g. when a user types an URL in the browser, then the HTTP request is sent to the server. The server provides resources such as HTML and other files and returns them as a response.

HTTPS (*Hypertext Transfer Protocol Secure*) – a secure communication protocol, which is an extension of the HTTP protocol and enables the secure exchange of information by encrypting data using SSL. When using a secure HTTPS, a web address begins with "https: //".

ICMP (*Internet Control Message Protocol*) – a protocol for transmitting messages about the irregularities in the functioning of the IP network, and other control information. One of the programs that uses this protocol is ping that let a user check whether there is a connection to another computer on the network.

IDS (Intrusion Detection System) – a device or software that monitors network traffic, detects and notifies about the identified threats or intrusions.

Incydent – an event that threaten or violate the security of the Internet. Incidents include: intrusion or an attempt of intrusion into computer systems, DDoS attacks, spam, distributing malware, and other violations of the rules that apply to the Internet.

IoT (*Internet of Things*) - concept of a system for collecting, processing and exchanging data between "intelligent" devices, via a computer network. The IoT includes: household appliances, buildings, vehicles, etc.

IP (*Internet Protocol*) – a unique number for each device (e.g. computer) on the Internet, allowing its unambiguous identification in the network. IPS (Intrusion Prevention System) - a system that detects threats and prevents attacks in real time.

IPS (*Intrusion Prevention System*) – a system that detects threats and prevents attacks in real time.

Keylogger – a program that operates in secret and logs the information entered via the keyboard. It is used to track activities and capture sensitive user data (i.e. passwords, credit card numbers).

Malware (*malicious sofware*) – software aimed at malicious activity directed at a computer user. Malware include: computer viruses, worms, Trojan horses, spyware.

MSISDN (*ang. Mobile Station International Subscriber Directory Number*) – phone number; a subscriber number in mobile network stored on the SIM card and in the registry of subscribers.

OWASP (*ang. Open Web Application Security Project*) – the global association whose main idea is to improve the security of Web applications.

Phishing – a type of Internet scam whose goal is to steal the user's identity, i.e. such sensitive data that allows cybercriminals to impersonate the victim (e.g. passwords, personal data). Phishing occurs as the result of actions performed by the unconscious user: opening malicious attachments or clicking on a fake link.

Port scanning - action of sending data (TCP or UDP) to a specific computer system on the network. It enables to get information about the operation of certain services and opening of certain ports. Scanning is typically performed in order to check the security or it precedes an intrusion.

Ransomware – a type of malware, which when installed on a victim's system encrypts files making them inaccessible. Decryption requires paying a ransom to cybercriminals.

Rootkit – a program whose task is to hide the presence and activity of the malware from system security tools. A rootkit removes hidden programs from the list of processes and faciliate an attacker to gain unauthorized access to a computer.

RST (*reset*) – one of the TCP flags that resets the connection

SIEM (*Security Information and Event Management*) – a system for collecting, filtering and correlation of events from many different sources and converting them into valuable data from the security point of view.

Sinkholing (*hole*) – a redirection of unwanted network traffic generated by malware or botnets. Redirection can be done into the IP addresses where the network traffic can be analyzed, as well as into non-existent IP addresses.

Port scanning – action of sending data (TCP or UDP) to a specific computer system on the network. It enables to get information about the operation of certain services and opening of certain ports. Scanning is typically performed in order to check the security or it precedes an intrusion.

SLA (*Service Level Agreement*) – an agreement to provide services at the guaranteed level. SLA is agreed between the client and the service provider.

Sniffing – an action of eavesdropping and analysis of network traffic. Sniffing can be used for managing and troubleshooting the network administrators but also by cyber criminals to wire-tapping and interception of confidential information of users (e.g. passwords).

SOC (*ang. Security Operations Center*) – a security center that combines both technical and organizational functions, in which systems such as SIEM, anti-virus programs, IDS/IPS systems, firewalls, provide meaningful information to the central incident management system.

Spam – unsolicited and unwanted messages sent in bulk, usually using email. Messages of this type are usually sent anonymously using botnets. Most often spam messages advertise products or services.

Spyware (*spy software*) – spy software that is used to monitor actions of a computer user. The monitoring activity is carried out without consent and knowledge. The information collected includes: addresses of visited websites, email addresses, passwords or credit card numbers. Among spyware programs are adware, trojans and keyloggers.

SSL (*Secure Socket Layer*) – the security protocol to ensure the confidentiality and integrity of data and their authentication. Currently, the most commonly used version is SSLv3 that is considered as a standard for secure data exchange and developed under the name of TLS (Transport Layer Security).

SYN (*ang. synchronization*) – one of the TCP flags sent by the client to the server in order to initiate the connection.

SYN Flood - a popular network attack, whose main purpose is to block the services of the server. It uses TCP.

TCP (*Transmission Control Protocol*) – the connection protocol; one of the basic network protocols for controlling data transmission over the Internet. It requires connection between devices in the network and enables to obtain confirmation that data reached the destination.

Trojan – Trojan horse; a malicious program that enables cybercriminals to remotely take control of the computer system. An installation of a trojan on a user computer is usually done by running malicious applications download from untrusted websites or mailing attachments. Besides a remote command execution, a trojan can allow eavesdropping and intercepts user passwords.

UDP (*ang. User Datagram Protocol*) – a connectionless protocol, one of the basic network protocols. Unlike TCP, it does not require setting up the connection, observing sessions between devices and a confirmation that the data reached the destination. It is mostly used for transmission in real time.

URL (*Universal Resource Locator*) – the web address used to identify the servers and their resources. It is essential in many Internet protocols (e.g. HTTP).

VoIP (*Voice Over Internet Protocol*) – "Internet telephony"; a technique for transmitting speech via the Internet. Audio data is sent using the IP protocol.

Vulnerability – an error; feature of computer hardware or software that exposes a security risk. It can be exploited by an attacker if an appropriate fix (patch) is not installed.

Worm – a self-replicating malicious computer program. It spreads across networks, which is connected to the infected computer, using either vulnerabilities in the operating system or simply user's naivety. Worms are able to destroy files, send spam, or acting as a backdoor or a Trojan horse.

Więcej informacji znajdziesz na:

www.cert.orange.pl