Security

CERT Orange Polska Report 2016

We will guide you into a secure future

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

IS

INTEGRATED
SOLUTIONS

Table of Contents

1 **Introduction**....4

2 **Summary.**....7

3 **Trends for year 2017**....10

4 **Tips for social media users** 13

5 **Incidents handled by CERT Orange Polska.**....16

5.1 Incidents divided by category....16
5.2 DDoS Attacks....28

6 **Cyberspace security level in Poland**....36

6.1 Malware in Poland 36
6.2 Mobile Malware....44
6.3 CERT Orange Polska honeypot system data....45
6.4 Phishing campaigns on Polish Internet users....49
6.5 Attacks on e-banking services....50
6.6 Case studies....52

7 **Main threats, vulnerabilities and events of 2016**....56

8 **Orange Polska security services**....64

8.1 Protection from DDoS attacks....64
8.2 Web Application Protection (WAF as a Service)....65
8.3 SIEM as a Service....65
8.4 SOC as a Service....65
8.5 Feed as a Service....65
8.6 IP Reputation Service....67
8.7 Code Audit....67
8.8 Security tests....67
8.9 Protection from malicious software (Malware Protection InLine)....68
8.10 Secure DNS....69

9 **CERT Orange Polska - team presentation** 70

9.1 Organizational structure....71
9.2 Team history....72
9.3 Domestic and international cooperation....72
9.4 Achievements and projects....74
9.5 Computer incident response procedure....80

10 **Methodology**....84

10.1 The telemetric base of CERT Orange Polska....84
10.2 Incident classification....86

11 **According to our partners**....90

11.1 Sekurak....90
11.2 The Cybersecurity Foundation....91
11.3 Niebezpiecznik....92
11.4 Zaufana Trzecia Strona....93

12 **Dictionary**....94

13 **Attachments**....98

1. Introduction

Year 1997… 13-year-old Mark Zuckerberg doesn't think about Facebook yet, social media do not exist, Wirtualna Polska (eng. Virtual Poland) one of the pioneers of Polish Internet is only two years old and the number of Polish Internet users reaches the „astronomical" million. We are eager for knowledge. We are looking for information not only in the press or TV - Internet is becoming our window to the world and hardly anyone realizes at the time what risks virtual world carries. In that year, still as Telekomunikacja Polska, we bring a special IT security unit to life, which competences and constituency we have been developing for 20 years now.

The cyberspace became our natural environment, where threats eventually moved from the „real" world. That is why one of our priorities is maintaining high security standards of our network and enhancing operational capabilities of CERT Orange Polska. We work very efficiently - only in the previous year we have analysed billions of events, from which eventually over 17 thousand actual security incidents got into hands of analysts, operators and experts.

Modern incident prevention in the web must take place on various levels. Detecting incidents and eliminating their consequences is one thing, but an educated user can, thanks to his awareness, prevent the threat proactively, before it even occurs. Times when we had viruses installed are becoming a thing of the past, now we are doing that… by ourselves. The cybercriminal does not even have to understand malicious software – he can buy it. So we have assumed that to success is social engineering, that is why we regularly inform through CERT Orange Polska website and company blog about up to date threats.

The CyberShield, for which year 2016 was the first year of functioning, educated and helped almost 250 thousand Neostrada users to eliminate serious threats. Threat prevention is not possible without cooperation, and as much as competition is a natural thing in business, it is obvious that when security is in question everyone is better off working together. Our collaboration with the National Cybersecurity Centre, and effective protection of events including such important ones as – the NATO Summit and World Youth Day is a proof of that. Being the first in Poland and 16th in Europe to earn the „Certified by Trusted Introducer" status is not just words, it's hard work of CERT Orange Polska. Requirements that must be met to advance to the elite are exorbitant, but thanks to that, when seeing the distinctive stamp the customer can be sure he puts his safety into the hands of first-rate experts.

> **> Threat prevention is not possible without cooperation, and as much as competition is a natural thing in business, it is obvious that when security is in question everyone is better off working together.**

What can we expect in the future? In the opinion of the partners of our report, the key words for the year 2017 will be DDoS and social engineering. In that first field we have been developing for years now and have achieved a unique competence level on a domestic scale. We also dedicate 2017 for enhancing our efforts in identification and analysis of malware and blocking cybercriminals' infrastructure. It's all to ensure that also in the field of IT security, Orange Polska can continuously and deservedly hold the Network #1.

This is our pleasure to present the third edition of the CERT Orange Polska Report. Have a good read.

Piotr Jaworski
Executive Director-Network
Orange Polska

Orange

2. Summary

Since the Orange Polska network covers around 40% of Polish Internet, it can be safely assumed that conclusions from the annual CERT Orange Polska report can apply to the Polish network as a whole. Of course, we leave the matter of reaching the conclusions to the reader, but basing upon the whole of the report summarized here, one thing is for sure – criminals do not intend to stop their activity in the Internet when money is constantly within their reach.

17199 incidents happened throughout a year, which gives almost 47 for each day – this is the operational work of CERT Orange Polska. Among the incidents handled, the ones from the “abusive content” are still the most common (41%). Almost 20 percent are intrusion attempts, 6,7% - malware, and almost 17 incidents out of 100 are DDoS attacks.

In that last aspect, there is no difference between Poland and rest of the world – the attacks last shorter (the number of the ones lasting 15-30’ increased almost six-fold), and their targets are being picked with much more care. As compared with the year 2015, the number of attacks classified as weak (below 200 Mbps) has significantly increased (from below 29,4 to 40,1 percent!). The last year was also marked by two biggest DDoS attacks in history – 620 Gbps on the security blogger Brian Krebs’s website and almost 1 Tbps on the OVH hosting company.

In that second case, the attack was possible because of the newly created Mirai botnet, composed of Internet of Things devices. In this aspect, problems are probably just beginning, since the boom on IoT devices is on the increase, and the level of their security remains very low. According to the data of CERT Orange Polska, as much as 50 percent of network endpoints (from the sample tested) had sample tested had contact with malicious software! We mostly have our devices infected during the pre-Christmas shopping frenzy. And we act more and more carelessly with phones running Android or do not replace legacy devices with unsupported software.

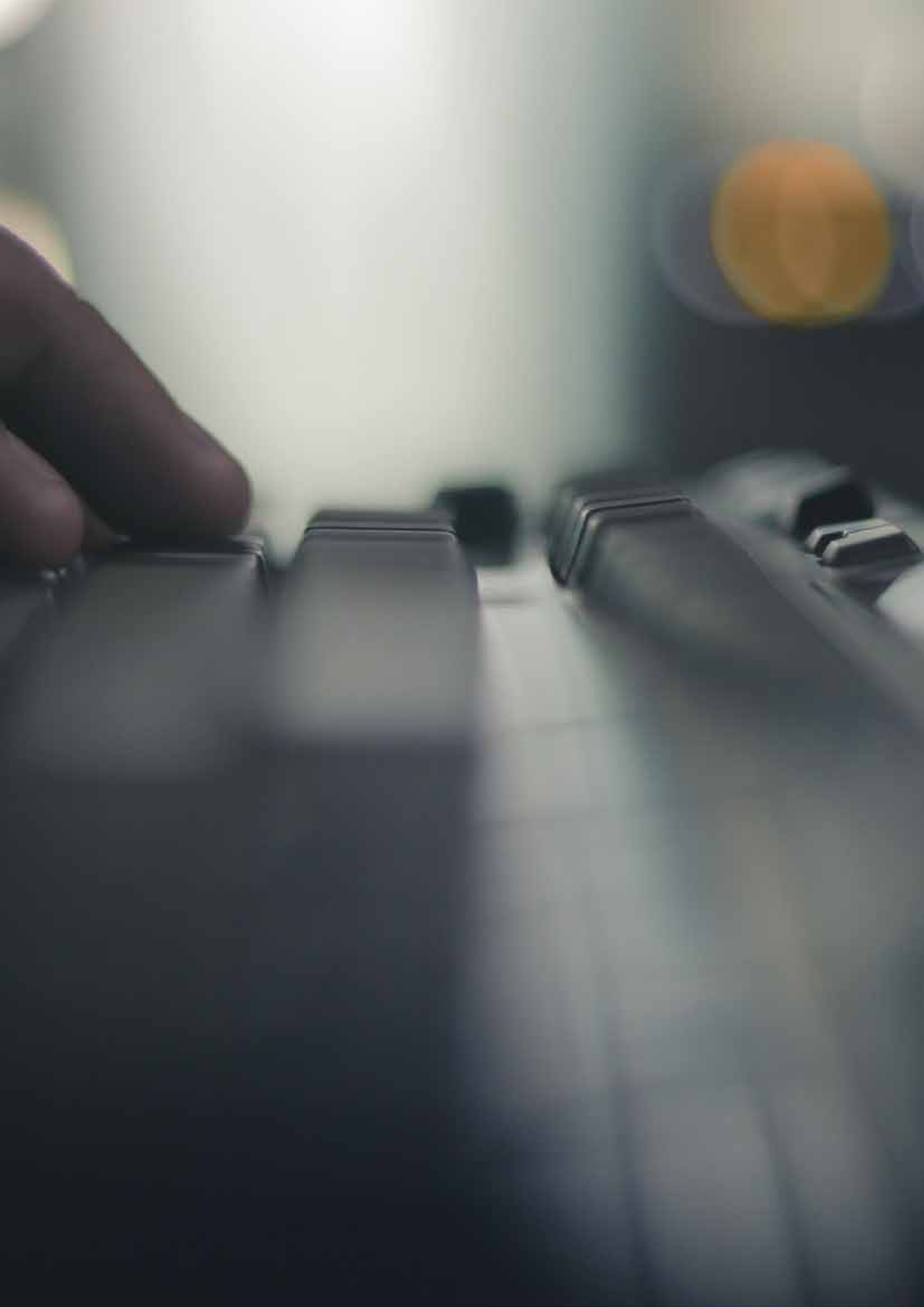
Speaking of carelessness, it is worth mentioning that the most popular login/password combination is... root/password. This is the conclusion from password attacks registered on CERT Orange Polska's honeypot device „farm". So it may be assumed with almost 100 percent certainty that this is true, as cybercriminals know the best what passwords to try when searching for vulnerable devices.

> **17199 incidents happened throughout a year, which gives almost 47 for every day – this is the operational work of CERT Orange Polska. Among the incidents handled, the ones from the "offensive or illegal content" are still the most common (41%). Almost 20 percent are hacking attempts, 6.7% - malware, and almost 17 incidents out of 100 are DDoS attacks**

CERT Orange Polska tries to counteract this in various ways – starting from technological measures, through combination of technology, knowledge and raising awareness (thanks to the CyberShield we have managed to protect almost one quarter million users from threats), and ending with education alone, using the website: https://cert.orange.pl/ and the company's official blog http://blog.orange.pl/. The analysis of events of the year 2016 indicates that most attacks relied heavily on more or less social engineering used by the cybercriminals. This which means that consequent education has the capacity to considerably improve the security of internet users.

In 2017, 20 years has passed since the establishment of the first unit responsible exclusively for ensuring IT security within the structure of Telekomunikacja Polska.

In the previous year, CERT Orange Polska joined the elite group of 16 European CERTs awarded the *Certified* status under the Trusted Introducer initiative. The team also made a very good score during the pan-European CyberEurope 2016 exercises, earning the 6th place out of 114 participating teams. This is why in this year's report we would like to invite the readers to take a look behind the "securitish stage". We want to show where does the content published in the CERT Orange Polska report come from, to explain how and why – are security incidents classified. Because as much as competition is natural in business, when bearing cybercriminals' determination in mind, it becomes clear that in regard to security it is better to work together for increased effectiveness. Everyone will benefit from this.



3. Trends for year 2017

It is certain that reduction in malware, ransomware and phishing campaigns is not an option – these things will continue happening for a long time. Despite large-scale efforts (also by Orange Polska) to raise internet danger awareness, many internet users still allow themselves to be deceived and open suspicious-looking attachments, or click on links in e-mails impersonating well-known brands.

Attackers are emboldened by low effectiveness of culprit detection and low number of reports to law enforcement agencies. Also their lives are made easier by the fact that today it is no longer necessary to write malicious software from scratch and to plan malicious campaigns. Malware and tools for its distribution can simply be purchased and configured to fit individual needs.

In the previous year we have also predicted a dynamic increase in number of attacks using Internet of Things (IoT), which means devices connected to network that are not computers/smartphones. We hit the bulls-eye. It was mostly previously infected webcams and video recorders that were used for the biggest DDoS attack in history (almost one terabit per second), reported in 2016. This kind of attack could block access to electronic banking services of over a thousand large banks at the same time! In the year 2017 we foresee further increase in significance of attacks using IoT. Manufacturers of an increasing number of devices implement features allowing remote control of their products, and too often do they release them to the market without security tests. As result, such solutions are becoming results becoming easy targets for attackers, especially when combined with lack of recommendations to change the default passwords, which are secret to no one.

Also, it doesn’t look like criminals are about to give up their most popular method of propagation of malicious software, which is social media. There, social engineering rules and will rule – for a long time there will be no shortage of situations, when we receive strange-looking note via Messenger, or see that a friend liked some strange-looking status. Therefore, if we act carelessly - the next moment our account is no longer ours.

In recent months fanpages with fake contests started to appear on Facebook with increased frequency. Using identity of well-known brands or people, they turn out to be very effective. How does it work? A fake profile with a contest is created, that is name-sponsored by a popular brand or person. The alleged prize can be free shopping vouchers or even a luxurious car. One only has to like a post, share it on one’s profile and post a comment of a specified content. This allows the criminals to get to more users, namely friends of their first victims. Finally, information appears on the profile, saying that in order to check the list of winners, a form provided must be. And additionally, the identity of the “winner” needs to be verified with a PIN received via SMS to confirm the “winner’s” phone number. As you may have guessed, it is not identity that is being confirmed, but a subscription of an expensive Premium SMS service. The cost of unwanted messages can reach even 30 PLN for each! Ironically, the criminals acted in accordance with the law, as below the form there is a link to the terms of service in fine print, describing the service as well as the fees, but who reads terms of service anyway? As a result, the victims only find out about the high charges from their phone bills.

> In the year 2017 we foresee further increase in significance of attacks using IoT.

It is also good to remember to be careful about sharing personal information on various social network sites, especially concerning our professional career. There are many indications that year 2017 will be marked by phishing specially designed for certain professional groups, which can significantly affect its effectiveness. There is a greater probability that an accountant will open an adequately named Excel file, and if the criminal trying to attack our company previously find the right candidates on Facebook or LinkedIn, his chances of success will significantly increase.

Krzysztof Białek

SOC & CERT Manager
Orange Polska

4. Tips for social media users

In times when the key resource in short supply is time, we have moved a substantial part of our people-to-people activities to the Internet, with the use of social media. Naturally, criminals interested in our data followed.

In social media we can fall victim to privacy threats as well as IT related ones. Facebook remains the unquestionable leader when it comes to social media. One of the most popular methods of attack using Facebook is cross-site scripting (XSS) – embedding malicious code in contents of a website – but especially one of its variations, Self-XSS, when the user is persuaded using socio-technical methods to copy a piece of text (script) and to run it in their browser's address bar. Self-XSS attacks may also activate a hidden code on user's computer and lead to installation of malicious software.

Criminals use social engineering to persuade the user to perform a specific task – clicking on a post or entering seemingly unimportant data, such as mother's name. Users on the other hand forget that this sort of information often form part or whole of their passwords, and from there it is only one step from complete identity takeover.

"Clickjacking" is also a common phenomenon that can be encountered on Facebook. A criminal tries to attract user's attention and force him to interact, generally by fabricating a "catchy" message. Clicking on it causes execution of malicious code without user's knowledge. Its first effect is usually the user's status update (e.g. a "like" of a post) and in the result of that, propagation of the code to his contacts. In the next step, the cybercriminal can already perform actual malicious activities.

Despite the development of technology and social engineering, one of the greatest threats to user's privacy remains his "friends", who by default have access to most of the data residing on the account. A popular method used by criminals is mirroring data from a profile of a certain user (information, photos) creating a new account and sending a friend request. As a result, by automatically accepting the "renewed" request, we grant the cybercriminal access to our profile.

Twitter is the most valuable service of all social media when it comes to communication of current information and event coverage. It is natural then, that it becomes a major area of activity not only for criminals acting on a monetary incentive (e.g. fundraising scams), but also for sophisticated disinformation hubs, when taking ease of creation and distribution of information, as well as the option of preparing it precisely for a certain group of users/influencers into account.

On Twitter, special attention should be paid to shortened hyperlinks. Since Twitter allows only 140 signs per post, it somewhat enforces using additional URL shortening services. The user is not able to deduce where the link leads to just by analysing its characters. Once the link with malicious content had been clicked on, it is usually too late to back out.

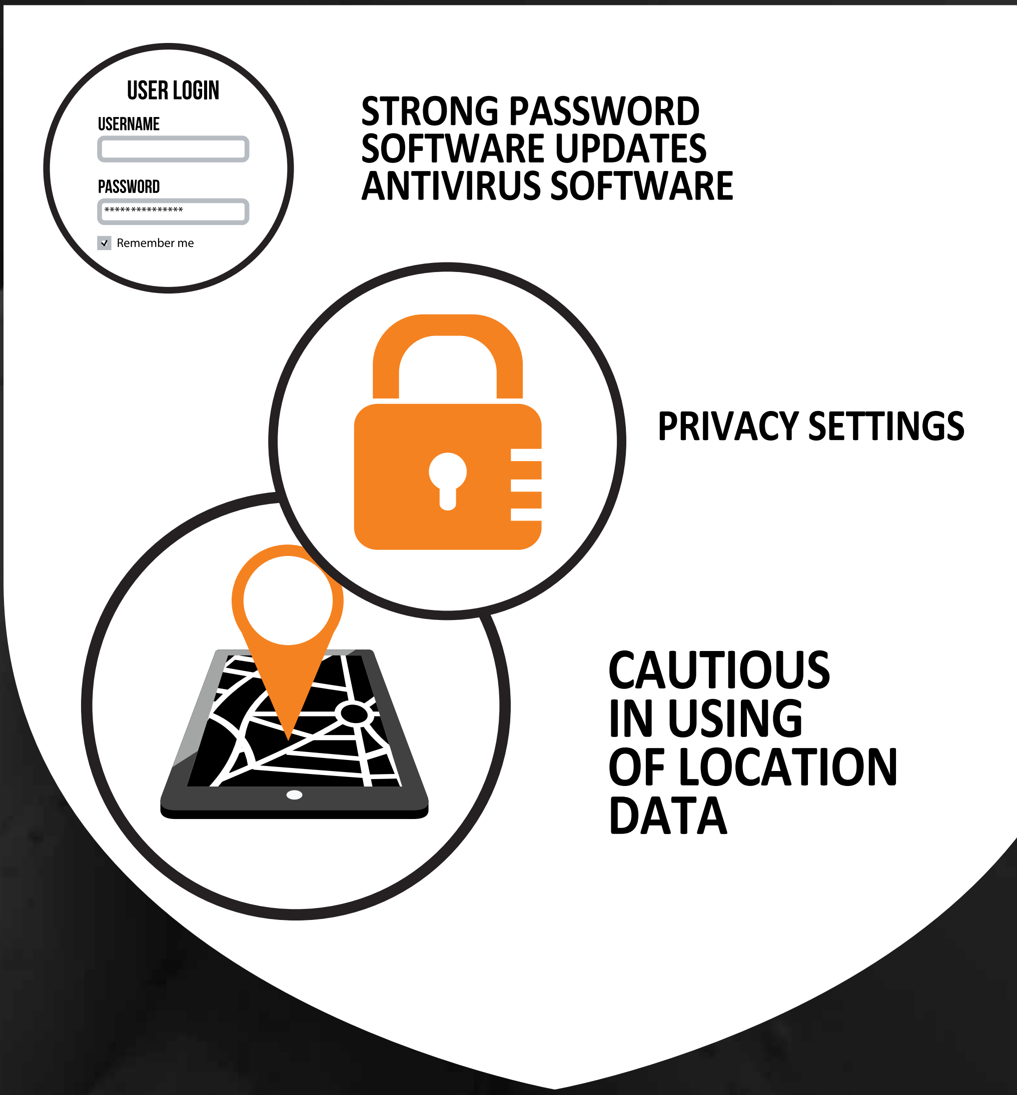
> **A criminal tries to attract user's attention and force him to interact, generally by fabricating a "catchy" message. Clicking on it causes execution of malicious code without user's knowledge.**

Lots of information about users that criminals may find valuable can be found on LinkedIn, a service often referred to as "Facebook for business". Due to the high possibility of associating a potential victim with an employer, it is a perfect starting point for spear-phishing campaigns, which means social engineering actions targeting a narrow group of recipients.

There is no doubt that the social media threats are closely related to technological attacks, being an area of special interest and monitoring by CERT Orange Polska.

What to do to feel safer in social networks?

1. Each service offers an option to modify privacy settings – use them to to increase level of security for the data residing on the profiles.
2. Carefully choosing “friends” and our affiliation with various social groups
3. Maintaining caution when using location data, preferably not using them at all
4. Avoiding to publish personal information (date of birth, vacation plans, daily schedule, credit card number etc.)
5. Not clicking on suspicious-looking links and posts (scan the link before opening it).
6. And of course, as always:
   a. Setting a strong password (12+ characters, capital and lower-case letters, special signs, numbers)
   b. Ensuring regular software updates
   c. Using antivirus software



STRONG PASSWORD
SOFTWARE UPDATES
ANTIVIRUS SOFTWARE

PRIVACY SETTINGS

CAUTIOUS
IN USING
OF LOCATION
DATA

5. Incidents handled by CERT Orange Polska

Effectiveness in detecting and handling incidents is the most common indicator for evaluating response teams. To ensure the ability of as fast and effective reaction as possible, CERT should constantly monitor events within the network which is its operating area through its telemetric base.

In 2016 the CERT Orange Polska team registered almost 9 billion system events[1] per month, which is one third more events per month than in 2015. Thanks to this highly developed, automated environment, CERT Orange Polska was able to detect security events[2], which deviated from accepted norms (anomalies) and expected actions by systems and users. There were over one hundred and seventy thousands of them each month. 1433 of them were classified as incidents and required management by CERT Orange Polska specialists. In total, CERT Orange Polska handled 17 199 incidents in 2016.

The methodology, a description of the incident classification and the telemetric base of CERT Orange Polska are presented in detail in chapter 10.

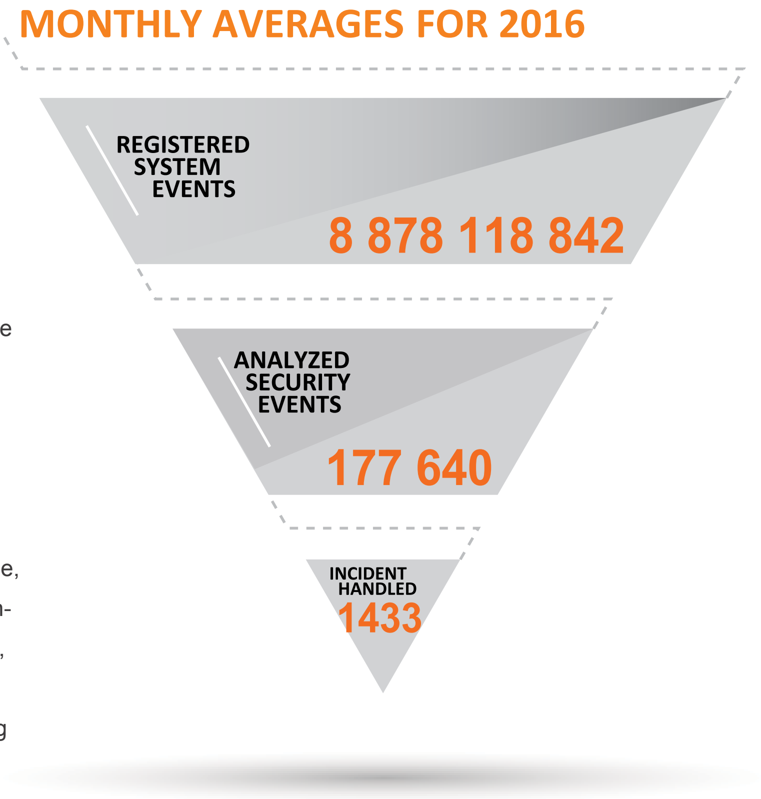
5.1 Incidents divided by category

In this section, we present security incidents related to Internet network services that were handled by CERT Orange Polska in 2016, divided into categories.

Among the incidents reported by CERT Orange Polska, the majority of them were the ones from the abusive content class, which made up over 40% of all cases. The other large groups were intrusion attempts – 20.3%, denial of service attacks –16.76% and violations related to information gathering – 11.7%. The group of the least frequently occurred incidents were those that were classified as malicious software – 6.73%, network frauds – 1.71%, network intrusions and unauthorized access to information – less than 1%. Other incidents that were not classified into these categories made up 1.17% of all incidents.

[1] *System event should be understood as an event describing the operation of the system that may contain information about the state of the IT security of the system.*

[2] *Security events should be understood as those among all the events that describe the state of IT security of the system.*



Looking at different categories of incidents might give an impression that some of commonly occurring phenomena, such as malware, appear to be underestimated. However, it is worth to analyze what exactly is behind the individual categories. Some of them include such types of incidents that may explain some doubts. For example, the most numerous category "offensive or illegal content" includes cases of spam. In turn, for a long time, spam has been the main carrier of malware. Thus, only a synthetic look and understanding the meaning of all categories, allows for a proper evaluation of existing network phenomena related to cyber threats.

> In total, CERT Orange Polska handled 17 199 incidents in 2016.

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

Percentage distribution of incidents handled by CERT Orange Polska in 2016

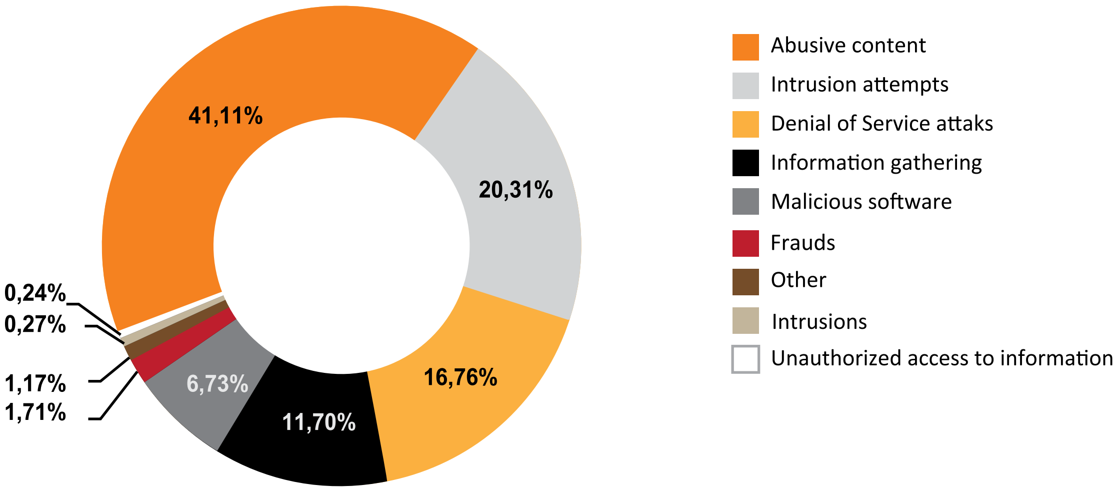


Figure 2 *Percentage distribution of incidents handled by CERT Orange Polska in 2016*

41%

REPORTED INCIDENTS OF „ABUSIVE CONTENT” CLASS

x2

NEARLY **DOUBLE INCREASE** OF INCIDENTS IN APRIL **DUE TO INCREASED NUMBER OF PHISHING AND SPAM CAMPAIGNS RELATED TO THE LAUNCH OF „500+” PROGRAM**

The e-mail system has became one of the most popular worldwide method of a communication, thus malicious use of this system made it very effective in terms of malware distribution. Thanks to cheap and massive distribution, attachments with malicious software, links embeddedin emails' content, are one of the most successful cyberattacks' vectors.

As shown in the chart below, the dispersion of incidents over time is quite regular. Nearly double increase in incidents in April was due to the increased number of phishing and spam campaigns, related to the “500+” program. The commencement of benefit payments resulted in the increased activity of cybercriminal groups.

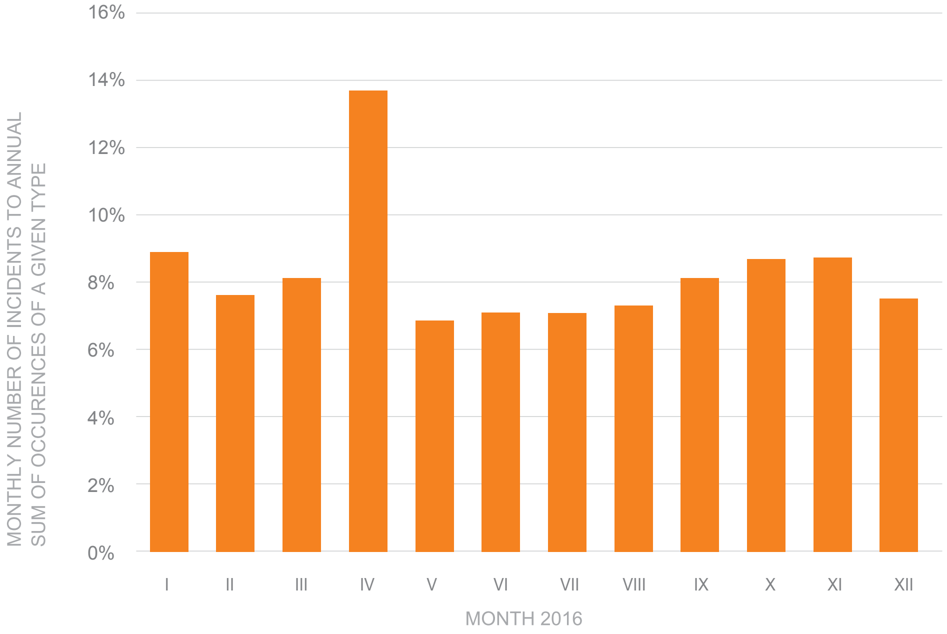


Figure 3 *Monthly distribution of incidents in 2016.*

In the next sections, we present the various types of incidents, along with the time distribution of their occurrences in 2016.

5.1.1 Malicious software

The „malicious software” class includes infections, distribution of malware and hosting C&C servers, remotely controlling a network of infected computers. Incidents of this characteristics makes 6,7% of the whole. This also includes ransomware infections.

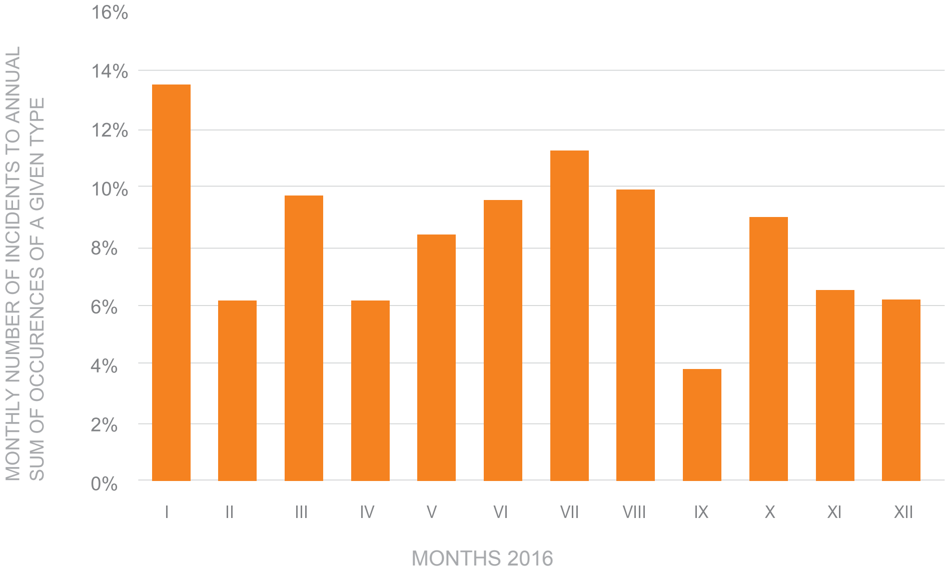


Figure 4 *Monthly distribution of malicious software incidents in 2016*

In practice, in most of the analyzed incidents cybercriminals achieved their objective by using malicious software, that is why we dedicated a separate part of the report to this threat (see sections 6.1. and 6.2.).

5.1.2 Denial of Service

The „Denial of Service" class of incidents consists mostly of various kinds of Distributed Denial of Service attacks (DDoS). All the incidents of this type represented 16.7% of total. Just as malicious software, this kind of incidents can pose a serious threat and cause significant losses. For this reason, we dedicated a separate section of the report exclusively to them (see section 5.2).

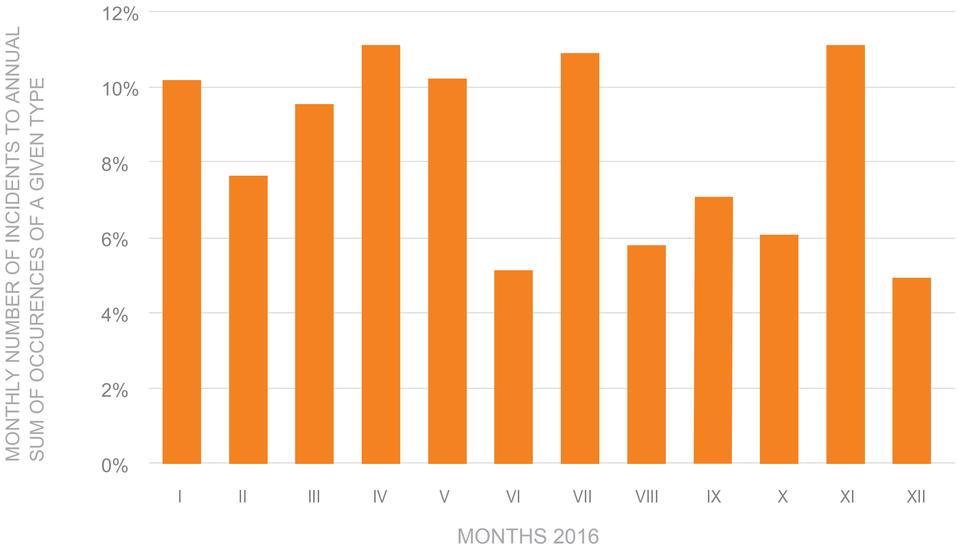


Figure 5 *Monthly distribution of denial of service incidents in 2016*

5.1.3 Data gathering

The class described as data gathering includes cases of scanning, sniffing, and phishing. In most cases, these kinds of threats are important elements of more advanced attacks, e.g.: ones described as APT (Advanced Persistent Threat). Incidents of this type made up 11.7% of total.

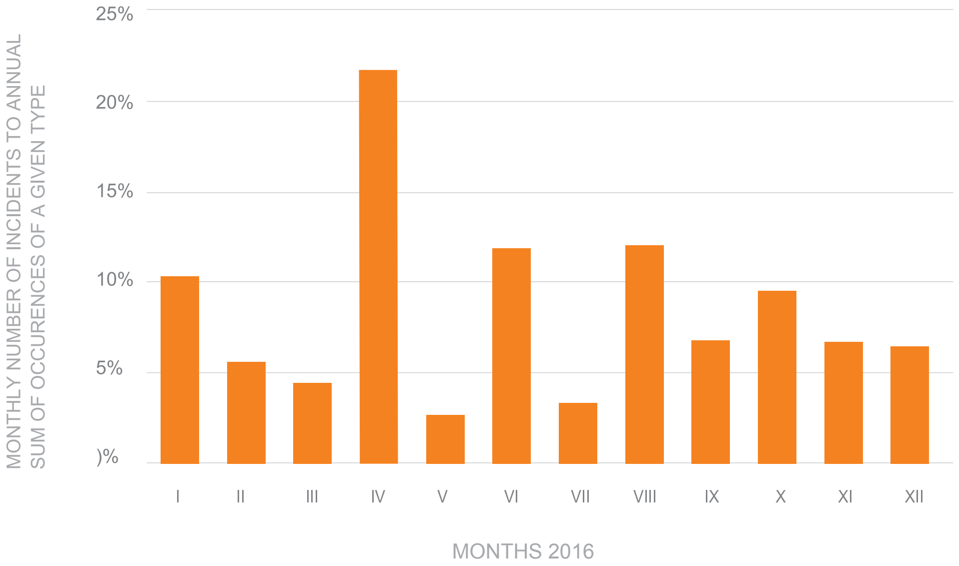


Figure 6 *Monthly distribution of data gathering incidents in 2016.*

5.1.4 Intrusion attempts

The intrusion attempts incident class includes security breaching attempts through exploiting system, component or network vulnerabilities, as well as logging attempts into services or control systems. Cases of this type made up 20.3% of all incidents. It is worth noticing that there was a significant increase in this type of incidents in the second half of the year. This may indicate the intensification of more advanced attacks that are going further than typical passive scanning techniques.

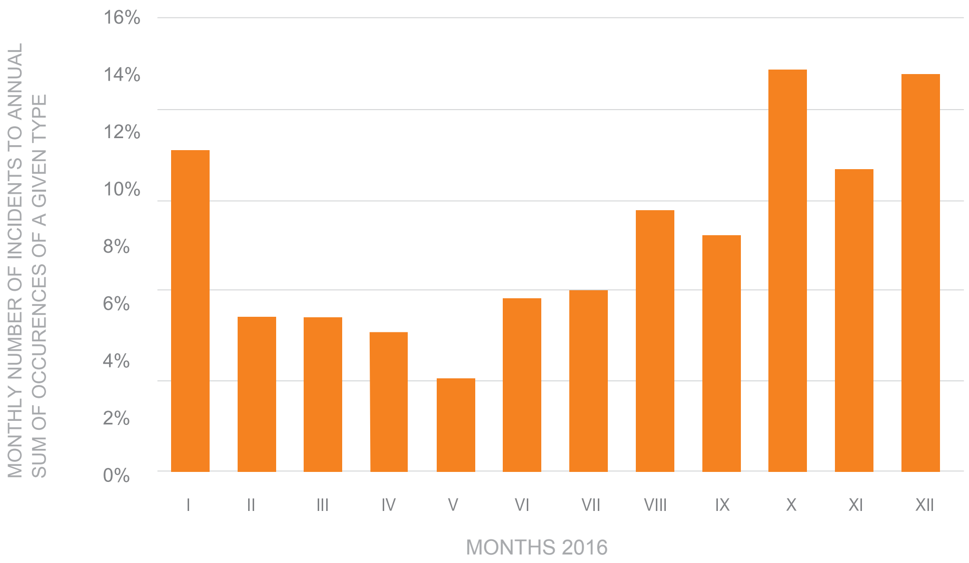


Figure 7 *Monthly distribution of intrusion attempts incidents in 2016*

5.1.5 Intrusions

This class of incidents consists of the types of incidents like "intrusion attempts" but which ended with a positive effect from the point of view of the attacker. As can be seen when comparing the temporal distribution of the data for this category and the category of the intrusion attempts – the two situations do not have to be in a close correlation.

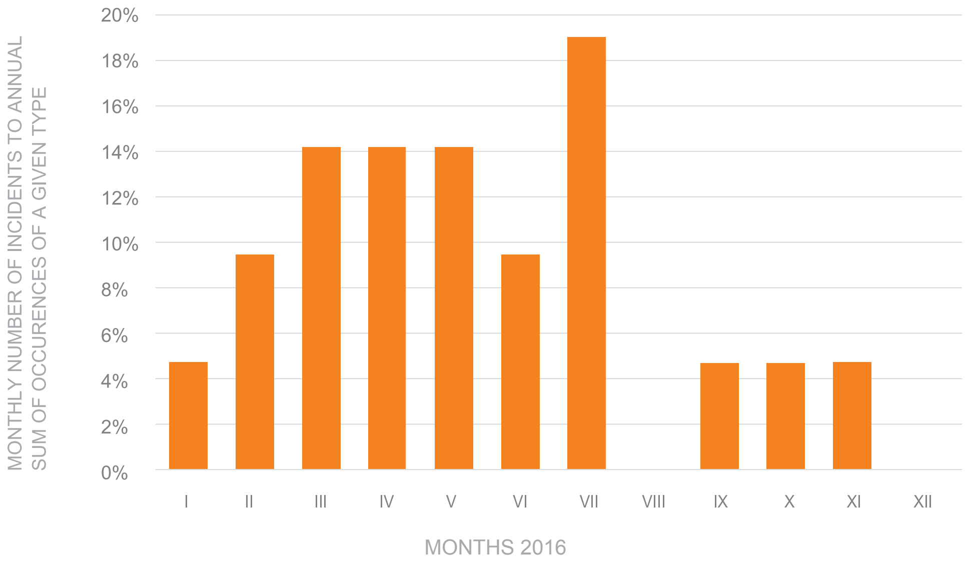
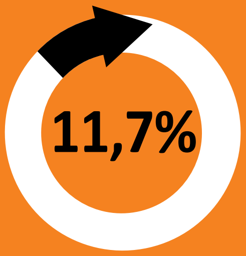


Figure 8 *Monthly distribution of intrusion incidents in 2016*



11.7% OF ATTACKS RELATED TO GATHERING OF INFORMATION THAT CAN BE USED IN ADVANCED PERSISTENT THREAT ATTACKS
INCREASE FROM 4.3% IN 2015

Looking at different categories of incidents might give an impression that some of commonly occurring phenomena, such as malware, appear to be underestimated. However, it is worth to analyze what exactly is behind the individual categories. Some of them include such types of incidents that may explain some doubts. For example, the most numerous category "offensive or illegal content" includes cases of spam. In turn, for a long time, spam has been the main carrier of malware. Thus, only a synthetic look and understanding the meaning of all categories allows for a proper evaluation of existing network phenomena related to cyber threats.

5.1.6 Unauthorized access to information

This class consists of cases of an unauthorized access to an information and change or deletion of information sets. In 2016, 0.24% of such cases were reported. However, such incidents have a high specific gravity. In practice, they represent serious problems of information leakage or other consequences of an unauthorized access to data. A relatively small number of such incidents cause temporary fluctuations, which can be seen in the graph, like in the case of data for January – nearly 60% of all cases.

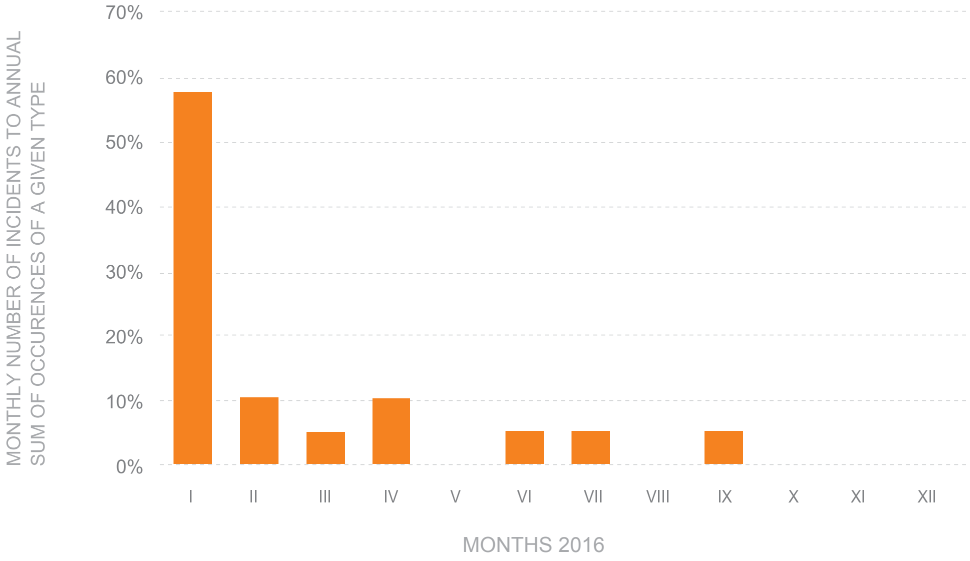


Figure 9 *Monthly distribution violation of unauthorized access to information incidents in 2016*

5.1.7 Fraud

Cases of an unauthorized use of resources and an illegal impersonation. These cases accounted for 1.7% of all incidents, close to half of them took place in April. The reason for this was the increased number of attacks spoofing well-known brands and institutions, including, among others, under the Orange brand and the institutions associated with the 500+ program. Important social and political events very often were used to carry out large-scale IT attacks.

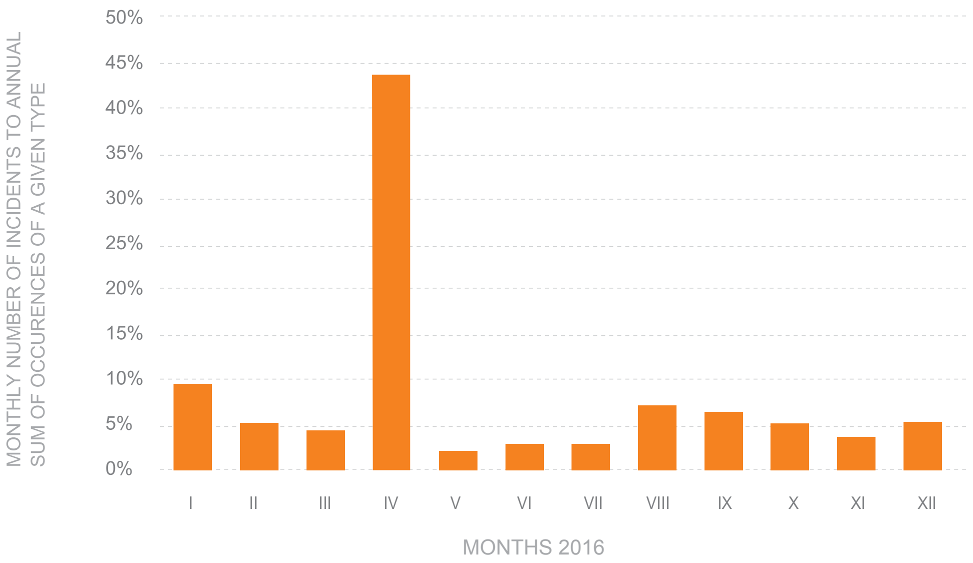
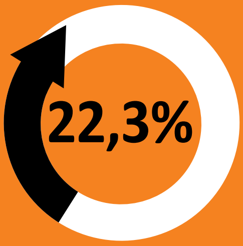


Figure 10 *Monthly distribution of fraud incidents in 2016*

5.1.8 Abusive content

Types of incident for this category are especially a spam distribution, copyright violation and illegal content distribution (child pornography, racist, xenophobic or affirmation of the violence). This is 41% of all incidents and they are undoubtedly most common incidents.

Incidents in this category should be considered not only as very negative from the social perspective, but also as the important technological threat. The electronic mail system has became one of the most popular worldwide method of a communication, thus malicious use of this system made it very effective in terms of malware distribution. Thanks to cheap and massive distribution, attachments which contain malicious software, links embaded in emails' content, are one of the most successful cyberattacks' vectors.



NEARLY EVERY 4th DDoS ATTACK HAS THE HIGHEST LEVEL OF CRITICALITY – 22.3%
(INCREASE FROM 15.7% IN 2015)

SHORTER DURATION OF DDoS ATTACK, AVERAGE DURATION WAS:
16 min.
(23 MINUTES IN 2015)

Incidents in this category should be considered not only as very negative from the social perspective, but also as the important technological threat.
The electronic mail system has became one of the most popular worldwide method of a communication, thus malicious use of this system made it very effective in terms of malware distribution. Thanks to cheap and massive distribution, attachments which contain malicious software, links embaded in emails' content, are one of the most successful cyberattacks' vectors.

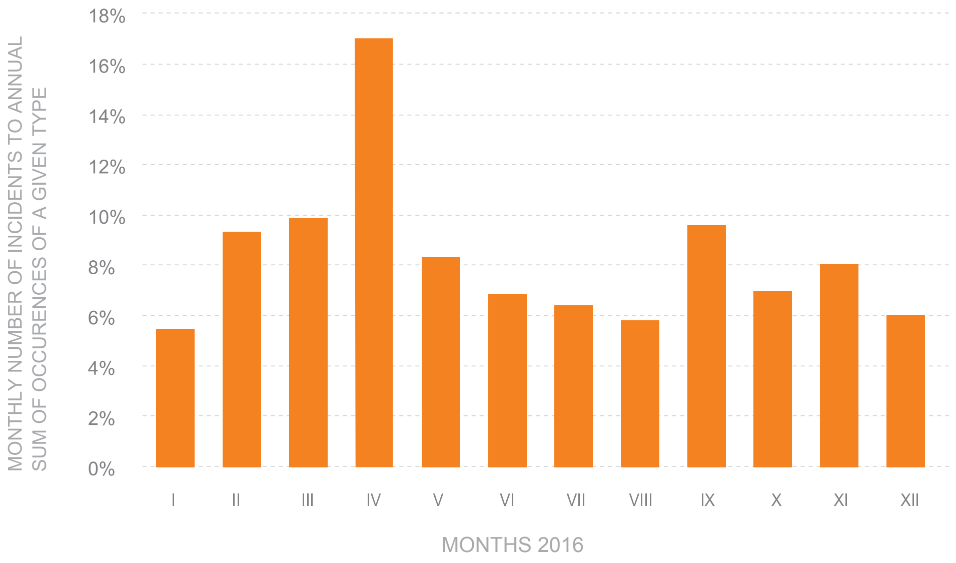


Figure 11 *Monthly distribution of abusive content incidents in 2016*

5.1.9 Other incidents

All other incidents that were not classified in the categories above accounted for 1.1% of all cases. There is no dominant type of incident within this set.

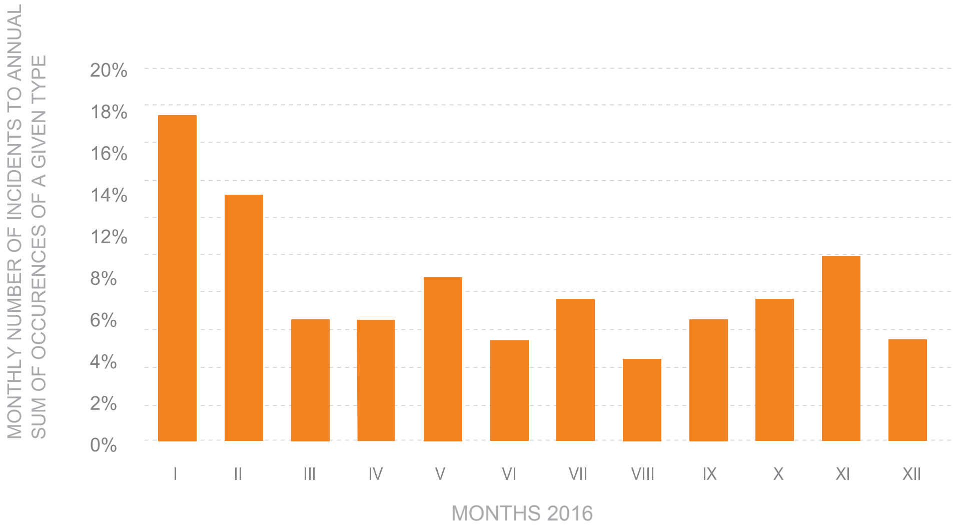


Figure 12 *Monthly distribution of other incidents in 2016*

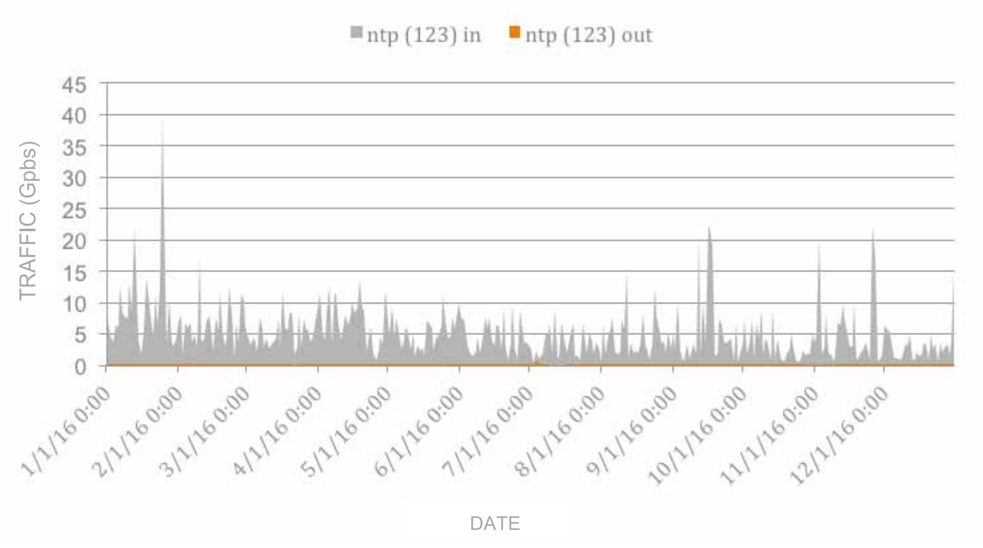
5.2 DDoS Attacks

DDoS (Distributed Denial of Service) attacks are a significant threat to the availability of networks and computer systems. The attacker, in order to strengthen the "power" of the attack, uses system and protocols vulnerabilities. The network traffic activity on specified, popular ports, is presented below.

5.2.1 DDoS Attacks – traffic characteristics

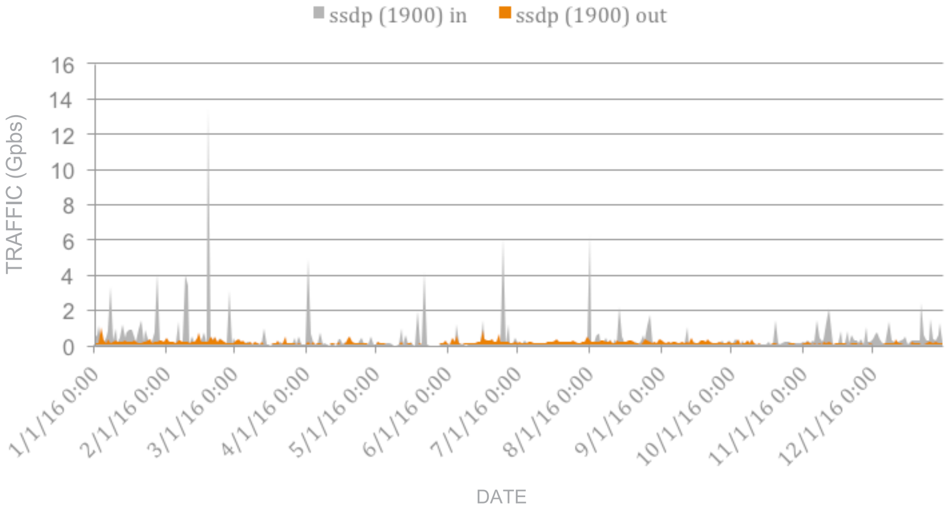
Traffic on port 123 in the Orange Polska network

Port 123 is used by the NTP (Network Time Protocol). This service is used for clock synchronization between computer systems by using the official time source from the time servers.



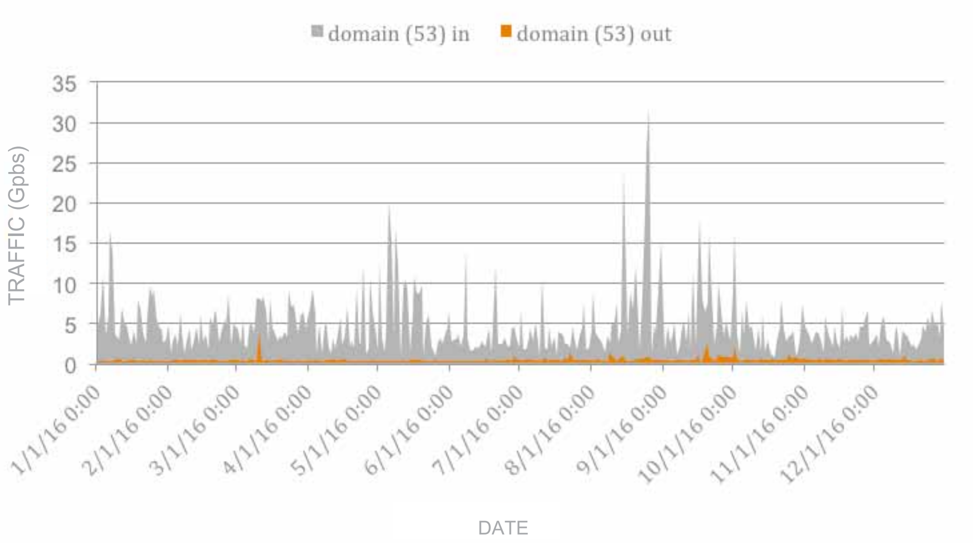
Traffic on port 1900 in the Orange Polska network

The port 1900 is used for the SSDP (Simple Service Discovery Protocol) for the detection of UPnP (Universal Plug-and-Play)



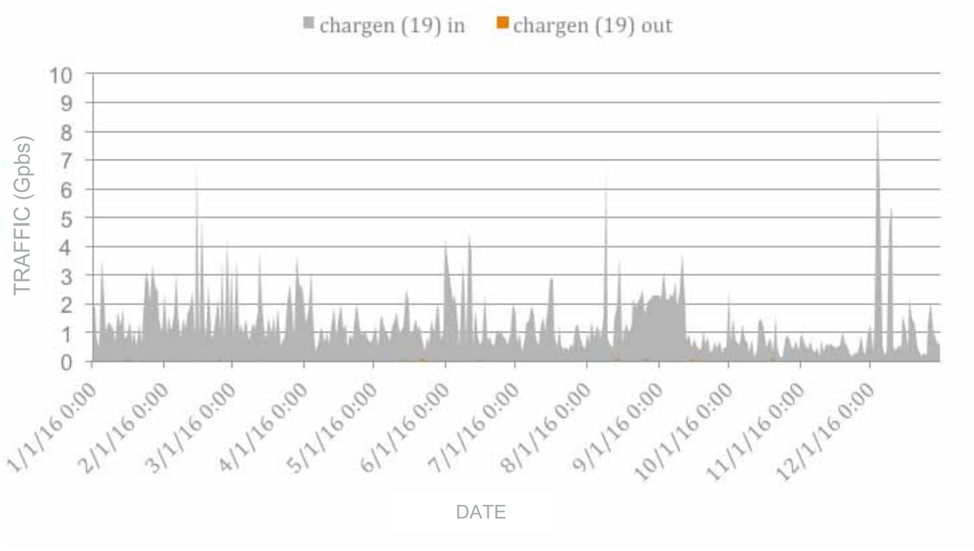
Traffic on port 53 in the Orange Polska network

The port 53 is used for the DNS (Domain Name System), which is responsible for the mutual translation of domain names and IP addresses.



Traffic on port 19 in the Orange Polska network

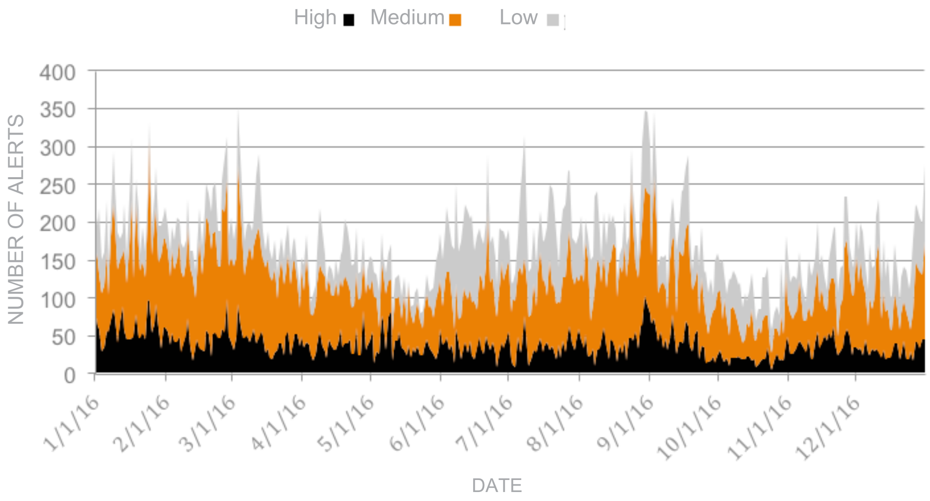
The 19 port for CHARGEN (Character Generator Protocol) protocol, which is used for testing, debugging, and measurement purposes.



5.2.2 DDoS attacks – types of attacks

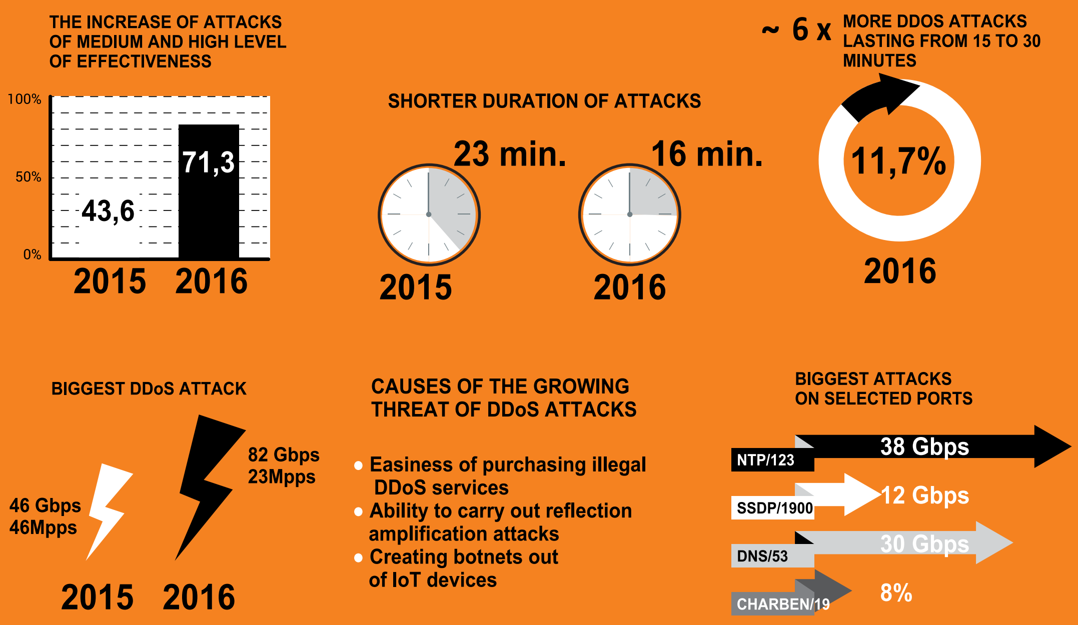
The classification used by CERT Orange Polska assigns DDoS attacks into one of three categories. The high alert is usually an attack which has a significant impact on the services availability. The attacks classified as medium and low can be dangerous only under special conditions.

DDoS alerts distribution in time presented in the three categories.



The higher speed of the general internet network connectivity is not the only reason the attacks increase. The additional important causes are: a low price of the attacks on the underground illegal market. The popularity of the amplification attacks and last but not least - attacks based on the Internet of Things botnets, what we observed especially in the last quarter of the year 2016.

DDoS ATTACKS of 2016



THE INCREASE OF ATTACKS OF MEDIUM AND HIGH LEVEL OF EFFECTIVENESS

SHORTER DURATION OF ATTACKS

~ 6 x MORE DDOS ATTACKS LASTING FROM 15 TO 30 MINUTES

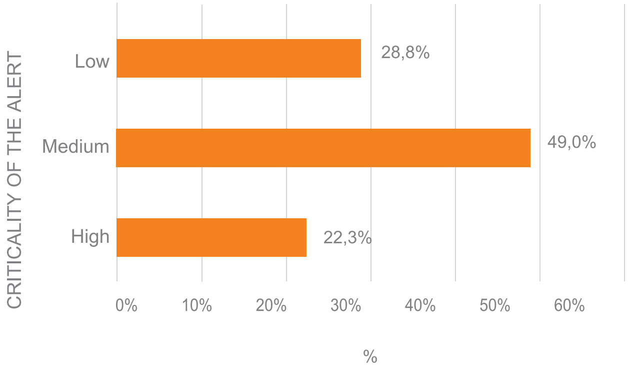
BIGGEST DDoS ATTACK

CAUSES OF THE GROWING THREAT OF DDoS ATTACKS

- Easiness of purchasing illegal DDoS services
- Ability to carry out reflection amplification attacks
- Creating botnets out of IoT devices

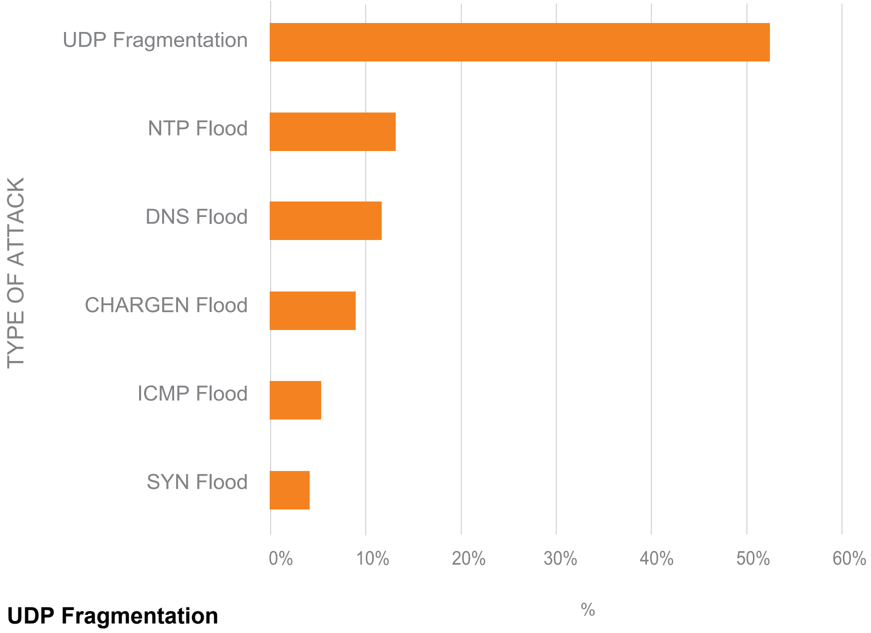
BIGGEST ATTACKS ON SELECTED PORTS

The percentage of the criticality categories of DDoS alerts



It is a significant change in the criticality alerts distribution for 2016 comparing to 2015. Regarding high criticality alerts - there are 6.6 percentage points more of them. Regarding medium alerts – there are 21.1 percentage points more of them.

The most common types of DDoS attacks



UDP Fragmentation

If a UDP packet which you send is too large (more than 1500 MTU) then it must be split into datagrams (MTU) of the maximum possible size, and then merged again on the destination device. This process consumes significant level of the victim's computer processing power.

Reflected DDoS

This attack is about using protocols vulnerability which is sending back feedback much larger than the size of the original request. The attacker spoofs the victim's IP computer, and as a result this computer receives a very large feedback which cause the malfunction of a device or a service. The most common protocols used for this attacks are UDP protocols, including DNS, SNMP, CHARGEN, NTP or SSDP. In case of such attacks we call it the DRDoS attack (Distributed Reflection DoS).

ICMP Flood

This attack is performed by sending a flood of ICMP packets. They are sent from many sources of compromised hosts (bots). An attacker sends packets as often as possible. A sources system does not expect the positive feedback for a destination system and this conducts the attacked system to stop.

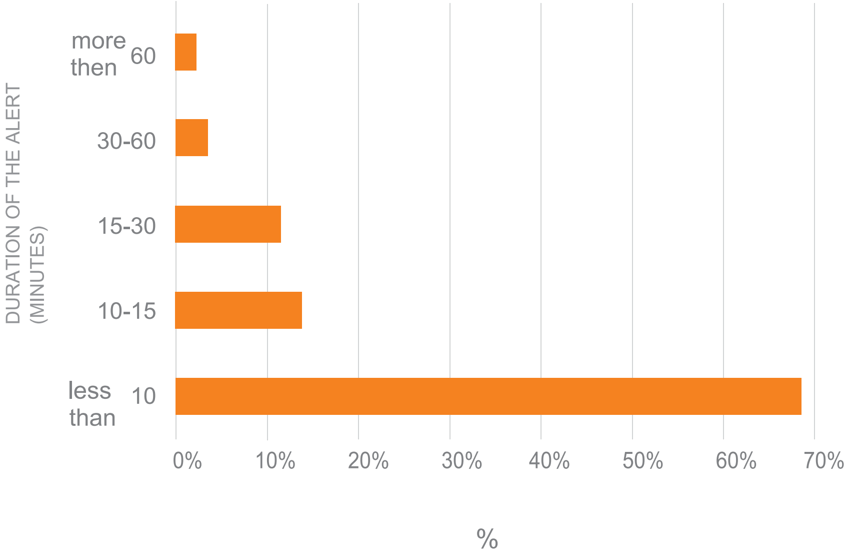
SYN Flood / TCP RST / NULL

This attack methodology is to exploit the vulnerability of the TCP (Transmission Control Protocol), particularly its mechanism of the connection establishment called three-way handshake. An attcker sends to TCP port a packet with the SYN flag, which is used to initiate a connection between a source and a destination hosts. In the next step a system reacts with the SYN-ACK feedback. After sending it a system expects the final signal with the ACK flag. This signal is not sent by an attacker. The consequences of it a consumption of the victim's power resources.

In 2016, the same as in the years 2014 and 2015, the most common types of DDoS attacks were UDP fragmentation attacks and DDoS reflected attacks, especially those based on DNS, NTP, SSDP, CHARGEN and SNMP protocols. In 2015 the most often exploited where NTP based attacks – 11%, then SSDP based attacks – 10% and DNS based attacks – 7%. In 2016 most attacks were again NTP ones – 13.2%, DNS – 11.8% and CHARGEN – 8.9%. It is worth to notice less ICMP based attack, which we observed only about a half of the 2015 number.

5.2.3 DDoS attacks - volume and duration of the attack

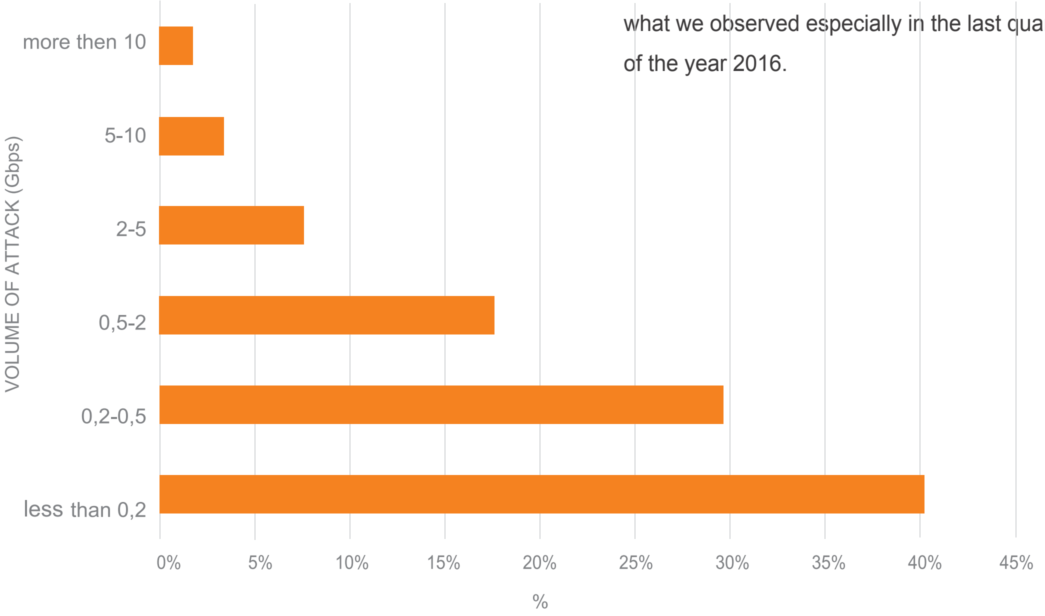
The duration of DDoS attacks observed in Orange Polska



In 2016 we still observe, as we saw in 2015, a further diversification of attacks' destination together with a further decline of the average attack duration. The average attack duration in 2016 was about 16 minutes (23 minutes in 2015). There were only about 50% of the attacks which last longer than 1 hour, but there are almost six times more attacks longer than 15 minutes but not longer than 30 minutes. Only 0.8 percentage point less attacks between 30 and 60 minutes. Finally 68.5% of all attacks (55.8 % in 2015) were attacks shorter than 10 minutes.

More information about the DDoS attacks causes are presented in the chapter 6.6.1.

The volume of DDoS attacks observed in Orange Polska



Attacks with the characteristic of the volume between 2 and 5 Gbps, 5-10 Gbps and more 10 Gbps, increased only 0.5 percentage point comparing to the year 2015. The most significant change was related to the attacks between 0.5 and 2 Gbps. In 2015 36.3% of all attacks were in this category. In 2016 only 17.6%. In contrary more attacks were in the category of attacks between 0.2 and 0.5 Gbps (22% in 2015). The same was for attacks weaker than 0.2 Gbps - 40.1% in 2016 and 29.4% in 2015.

In 2016 the average of the maximum volume of the attacks observed in the Orange Polska network was slightly higher than in 2015 and it reached a value of 1.1 Gbs. The maximum observed attack volume was 82 Gbps and 23 Mpps (in 2015 – 46 Gbps and 16 Mpps). The higher speed of the general internet network connectivity is not the only one the attacks increase. The additional important causes are: a low price of the attacks on the underground illegal market, the popularity of the amplification attacks and last but not least - attacks based on the Internet of Things botnets, what we observed especially in the last quarter of the year 2016.

6 Cyberspace security level in Poland

Due to dynamics of of changes in cyberspace, malware development and altering motivations of cybercriminals the assessment of threats level and forecasting them is a challenge. Last year was a perfect example of rapid change of attack vectors and infection patterns. Data below come from CERT Orange Polska systems that analyse network traffic for malware. Sample covers approx. 1% of users with broadband Internet access.

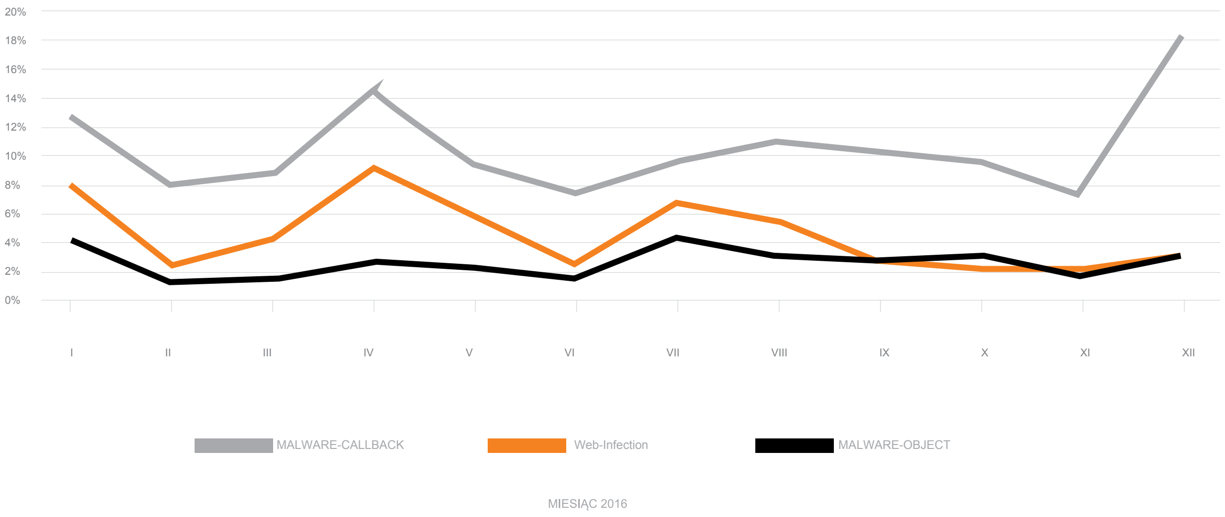
6.1 Malware in Poland

Identified attacks were divided into three unique types:

- **Malware object:** malware delivery to the end station
- **Web infection**: real-time infection and malware installation on victim's device
- **Malware callback**: confirmation of successful start-up of malicious code by connecting with remote command & control server (to download further instructions or transfer stolen information)

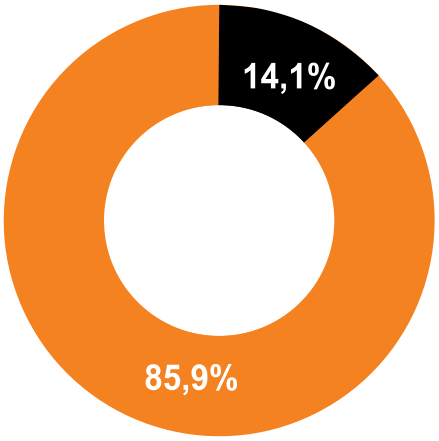
There are many ways to deliver malware to workstations. More and more of malware avoid detection at the network layer by using encryption mechanisms in TCP communication.

Percentage of detected type of events related to identified malware

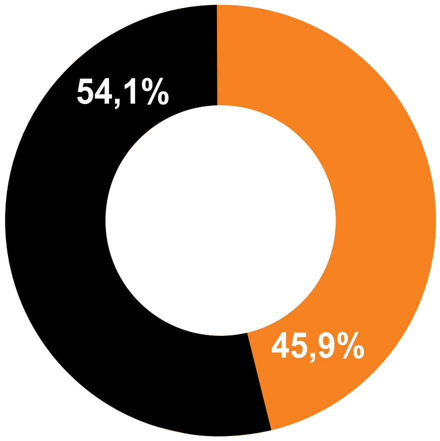


Type	Description
Malware Callback	Communication with C&C server established by an infected computer.
Malware Object	Files in the network identified as malicious.
Web Infection	Infections delivered through a web browser. Usually using exploit kits.

Distinct majority of events are callbacks to the control center, which are a result of the mechanisms of action of nowadays infections and also emphasize the low level of security of Internet users. Large majority of malware after launching on a user's workstation, in the second phase of the operation will infect processes, libraries or system applications thereby preventing itself from detection by antivirus systems and from effective removing of infection. In this way, without the user's awareness, many workstations become part of a botnets and are used among others to send spam or to conduct DDoS attacks.



Ratio of users infected by malicious software to users without infection (monthly average %)



Ratio of users infected by malicious software to users without infection (yerly average %)

■ Infected

🟧 Without infection

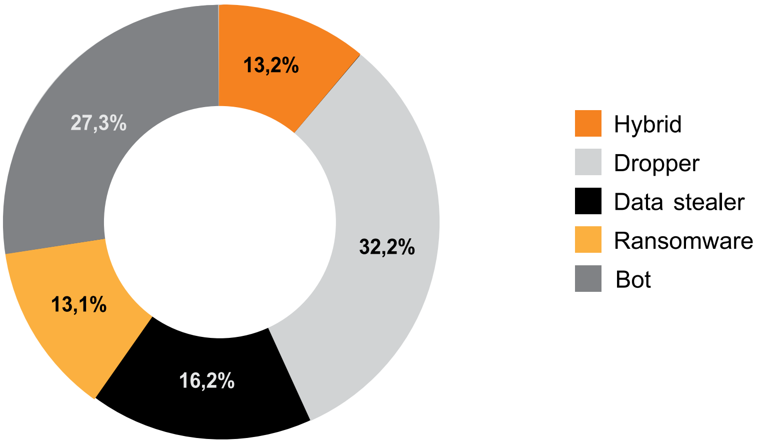
In the tested sample, approximately every tenth computer showed signs of malware infection, while almost 50% of users had to deal with malicious software – as a victim of the infection, part of a botnet or unaware recipient of the infected files.

The graphics below shows five categories of malicious software, divided by function that malware performs on victim's workstation:

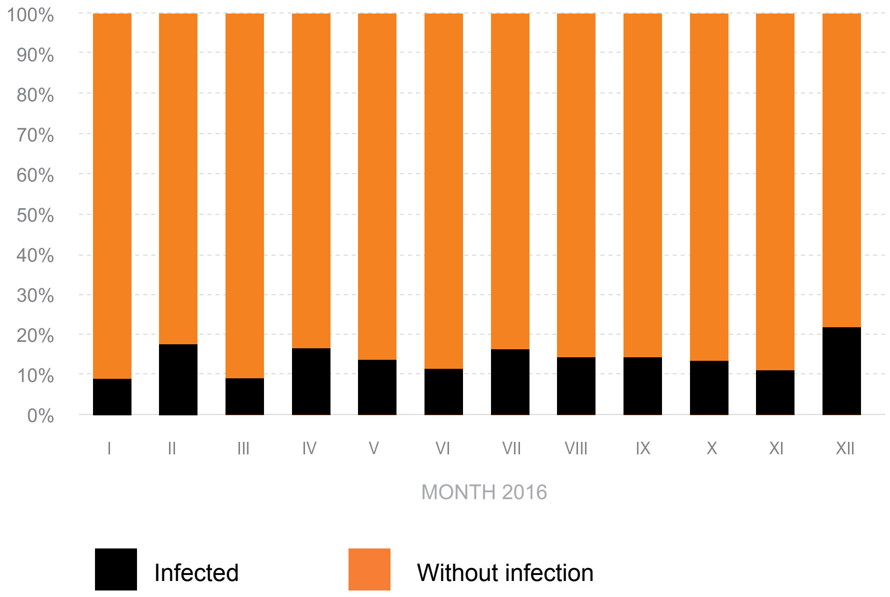
- **Dropper**. After setting up communication with the control center, downloads additional malicious content.
- **Bot**. Enables cybercriminals to take control over device to perform DDoS attacks, lower security level or launch "man in the middle" attacks by redirecting user's traffic to compromised domains.
- **Data stealer**. Software aimed at stealing access credentials to transactional systems, credit card numbers or mail accounts.
- **Ransomware**. By encrypting user's data forces victims to pay ransom in exchange for the restoration of access to the files. In 2016, number of infections in this group, identified by CERT Orange Polska, grew by 240% compared to the previous year.
- **Hybrid.** The combination of several functions merged and delivered in one malware.

Malware types

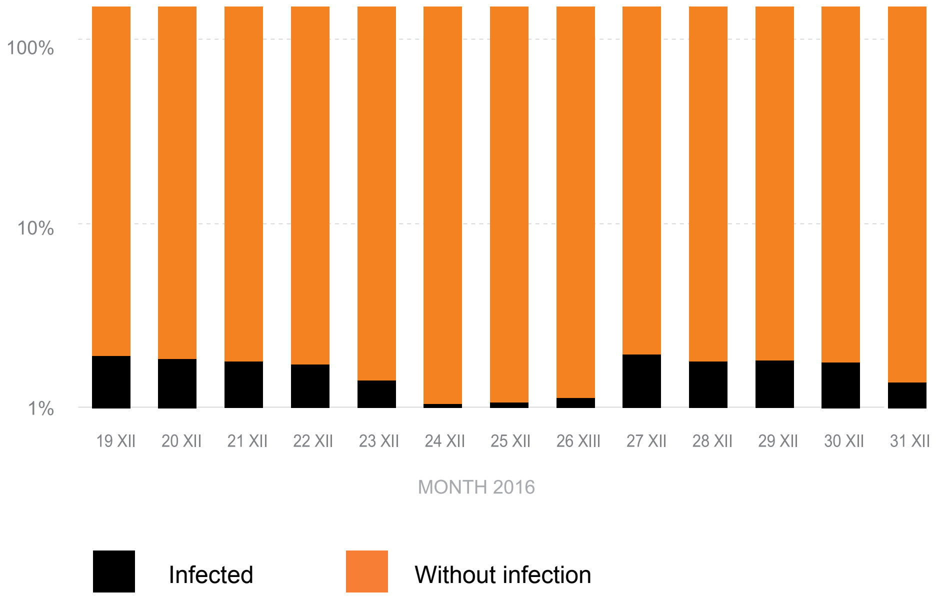
Next charts show the amplitude of changes in the number of detected infections over months or days. Changes are a result of major phishing campaign scarried out over the year and of reasons not related to cybersecurity such as Christmas and holidays.



USERS INFECTED BY MALWARE (STATS FOR EACH MONTH OF 2016)



RATIO OF USERS INFECTED BY MALICIOUS SOFTWARE
TO USERS WITHOUT INFECTION (DAILY AVERAGE)



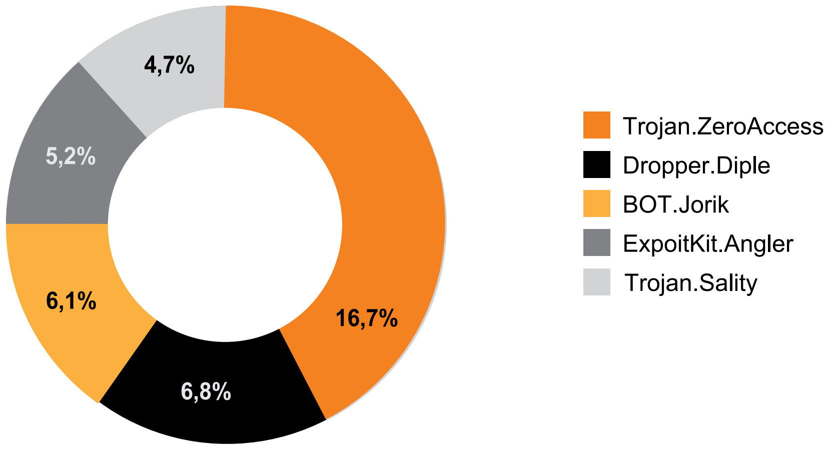
The first quarter of 2016 year was quiet for users because of the smallest number of threats compared to the rest of the year. The main contribution in the events had **Trojan.ZeroAccess**, dropper downloading, among others, applications, consuming computing resources of victim's workstation or used for Bitcoin mining as well as for forcing users to click on the pay-per-click ads. Similar functions performs the second of the droppers, **Diple,** downloading ZeroAccess malware and malicious code that steals sensitive data from the victim's workstation. In the first quarter, especially in February, we also identified increased activity of **Jorik** bot also used for Bitcoin mining by consuming resources of compromised devices.

At the turn of 2015 and 2016, CERT Orange Polska observed an intensive campaign of spreading ransomware **Cryptowall** through **ExploitKit.Angler**. It infects - by injecting malicious HTML / JavaScript – websites and then using vulnerability in the victim's system, downloads and installs malicious code on the computer.

The “first five” of the first quarter closes hybrid **Trojan.Sality** that steals sensitive data from workstations and uses compromised devices for targeted attacks or spam campaigns.

During the second quarter, a further development of the

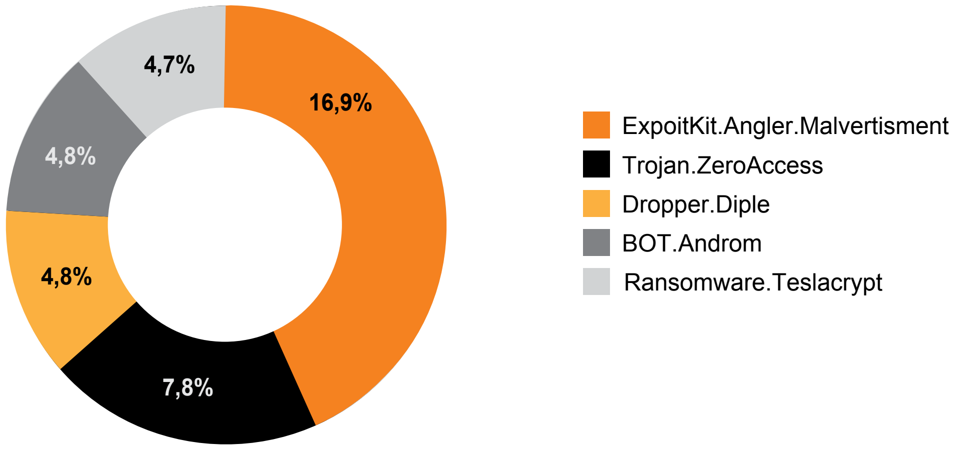
TOP 5 malware detected in 1Q 2016



infections based on exploit kits that use vulnerabilities in network applications and antivirus protection was noticed. **Malvertisment** - as the name implies - is a malicious advertising, found mostly on sites offering pirated versions of software or enabling free watch of latest movies and TV series, in exchange for running in the background several little bothersome ads.

Users had to constantly fight with the ransomware due to **Bot.Androm**. What deserves attention, objectives of downloaded to workstations ransomware **Teslacrypt** were not only to encrypt photos and documents, but also the files from games, preventing them from running and successful reinstallation. The third quarter contained the least anomalies,

TOP 5 malware detected in 2Q 2016

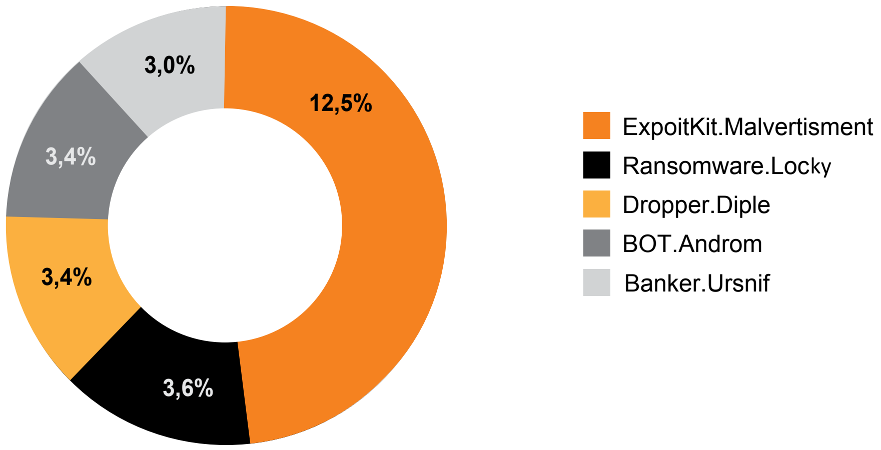


maintaining the trend from the first half of the year. E-mail boxes were regularly filled by phishing campaigns and that was the way in which **Ransomware.Locky** was usually distributed (script that hides in macros of MS Excel or MS Word). In the third quarter, intensified infections of banking Trojans were noticed, including Ursnif, whose next versions learned to recognize whether a file containing ready to execute code is opened by the user or by processes characteristic for security solutions. Malware runs only in the first case.

browsers, allowing to conduct "man-in-the-browser" attack - modification of the data at bank transfers when performing electronic payments.

However, the last months of 2016 were dominated by the backdoor at Internet of Things devices, running under Linux - **Bot.Mirai**. September 20th, botnet consisting of infected devices by this malware, was used for the first time. The result was one of the largest DDoS attacks in the history (up to 620 Gbps).

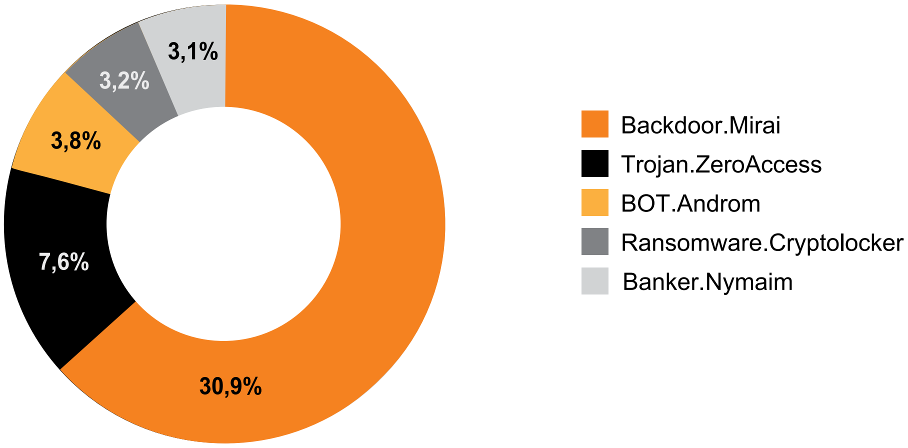
TOP 5 malware detected in 3Q 2016



The most common malicious software in the fourth quarter was an effect of new vulnerabilities and new malware families (Mirai) as well as the beginning of the academic year and the shopping season before holidays. In "invoices" campaigns, cybercriminals placed **Ransomware.TorrentLocker** - a new modification of known Cryptolocker that communicates with C&C to exchange keys via encrypted channel.
Nymaim activity on the other hand was aimed to infect

Due to relatively low level of Internet of Things devices security (default passwords, outdated software) and their increasing popularity, Mirai spread also in Poland, dominating among the biggest botnets identified in the tested sample by CERT Orange Polska.

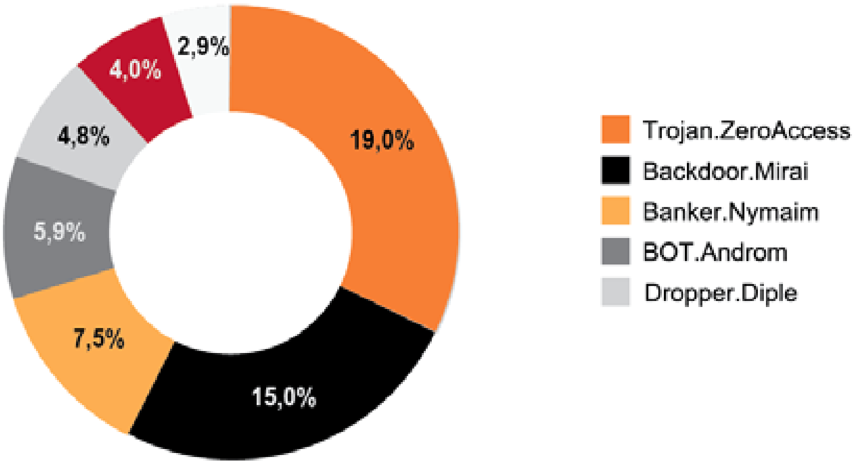
TOP 5 malware detected in 4Q 2016



In 2016 we identified more than 3.5 million events, more than 400 varieties of malware and about 5,000 unique samples. We have witnessed an intensified ransomware campaings and the birth of a new botnet - **Mirai**, which in 2017 may be one of the largest sources of DDOS attacks, also at the Polish service providers market.

6.2 Mobile Malware

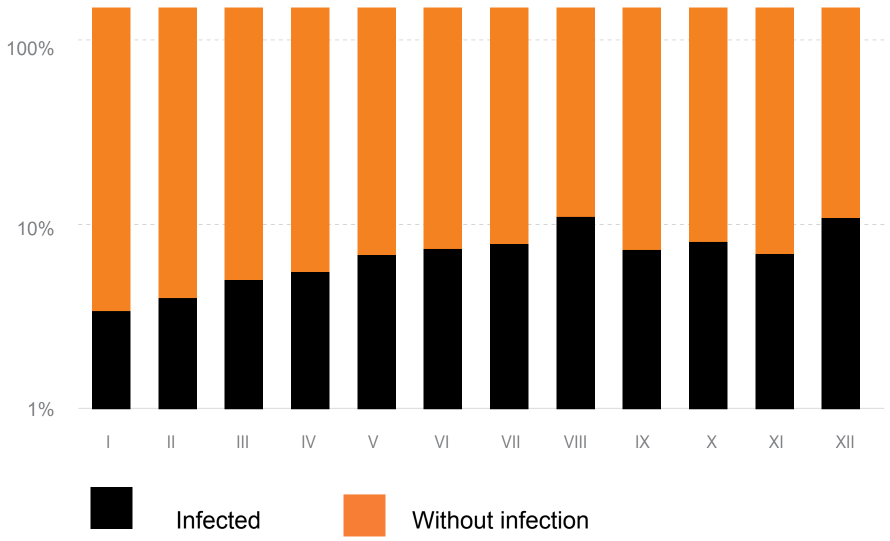
Biggest botnets - %of all connections to botnets during the year



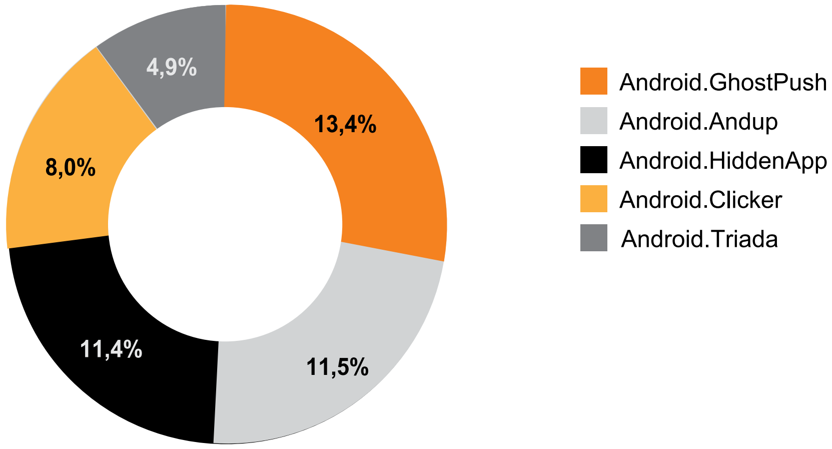
Although threats to mobile devices in 2016 were a little over 7% (almost 250 000 events per year), the number of detected infections increased by 290% compared to 2015. The upward trend, as seen in the graph below, gradually slows down, stabilizes however at a relatively high level of about 8-9% of the number of users infected with mobile malware. Should be pointed out, that in most cases, users with infected mobile devices were also related with malicious software on personal computers.

The main causes of this are: spreading payment

USERS INFECTED BY MOBILE MALWARE (MONTHLY AVERAGE)



TOP 5 threats for mobile devices in 2016



services realized by smartphones and tablets, a large variety of mobile malware (including ransomware) and growing number of well-known vulnerabilities to non-updated versions of operating systems, especially the old versions of Android.

Most popular mobile threats are entirely malware families for Android devices

The leader is **GhostPush** that uses vulnerabilities to obtain root privileges, effectively masks its presence in the system and therefore is resistant to attempts of detection. **Andup** and **HiddenApp** are mobile droppers that masquerade as legitimate applications. On the other hand, **Clicker** uses a browser to visit in the background, without the user's awareness, advertisements of pornographic sites. Last on the list of malware, **Triada**, can modify the messages from social media and install downloaded by itself other applications. But first it infects the master process of Android, responsible for running each application, which means adding functionality of Triada to any program that runs on the device.

6.3 CERT Orange Polska honeypot system data

Since 2015 CERT Orange Polska uses a system of honeypots, it allows to gather additional information about the attacks. Honeypots are specially configured vulnerable services ("bait"), deliberately exposed to attack, while prepared to gather as much information such as:

- sources of attacks: IP addresses and autonomous system (AS),
- IP addresses that contain malicious content,
- lists of passwords used by the attackers, including automatic tools that scan devices available on the network,
- characteristics of botnet communication,
- unknown vulnerabilities (0-day) of network devices and methods of their use,
- new methods of use of open services in terms of DDoS attacks.

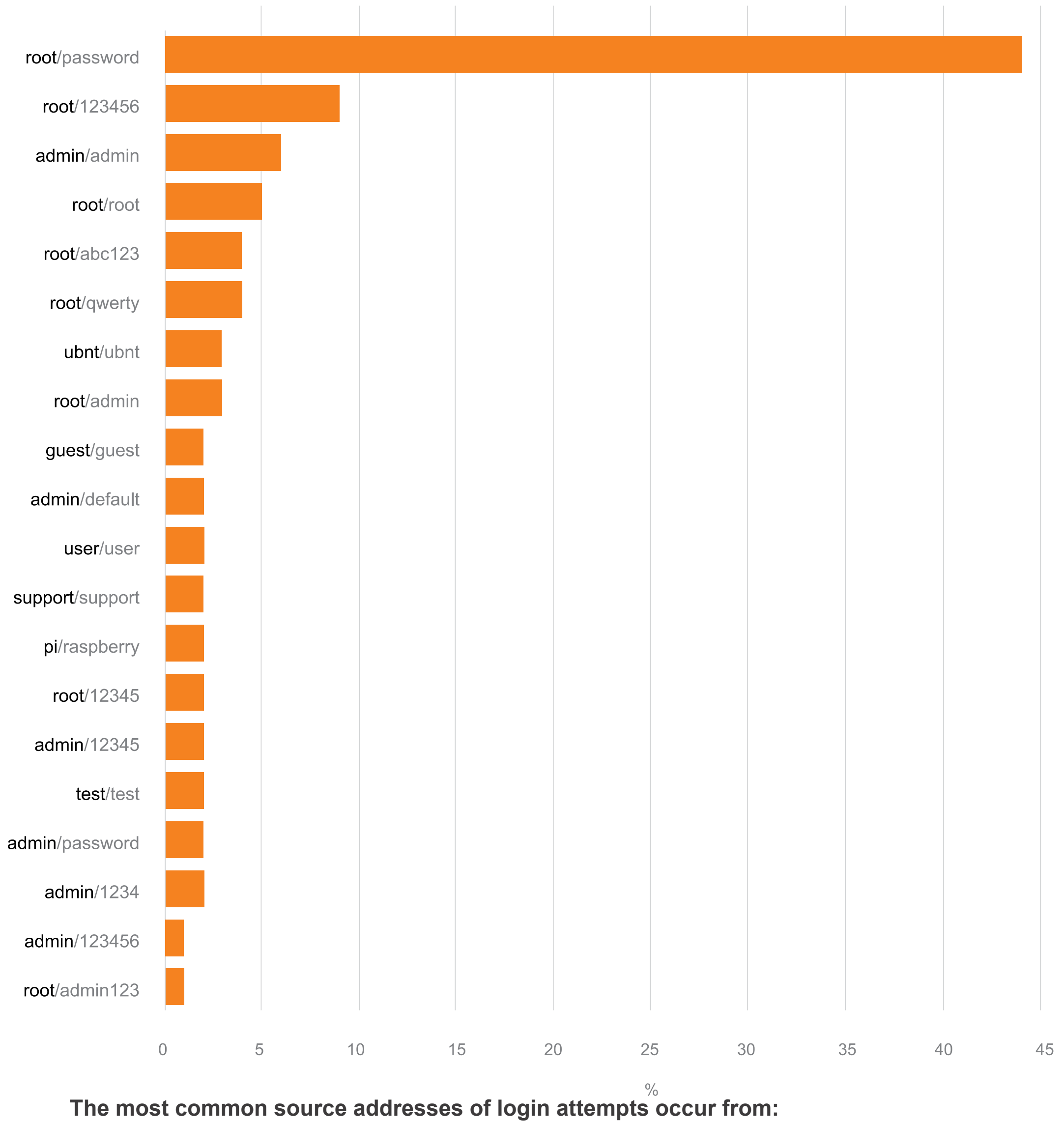
> **> Threat prevention is not possible without cooperation, and as much as competition is a natural thing in business, it is obvious that when security is in question everyone is better off working together.**

Collected information is used, among others, to implement additional security measures, identify new threats, optimize protection systems against DDoS, identify botnets C&C servers. It is an important source of threat data for CyberShield.

6.3.1 Login attempts

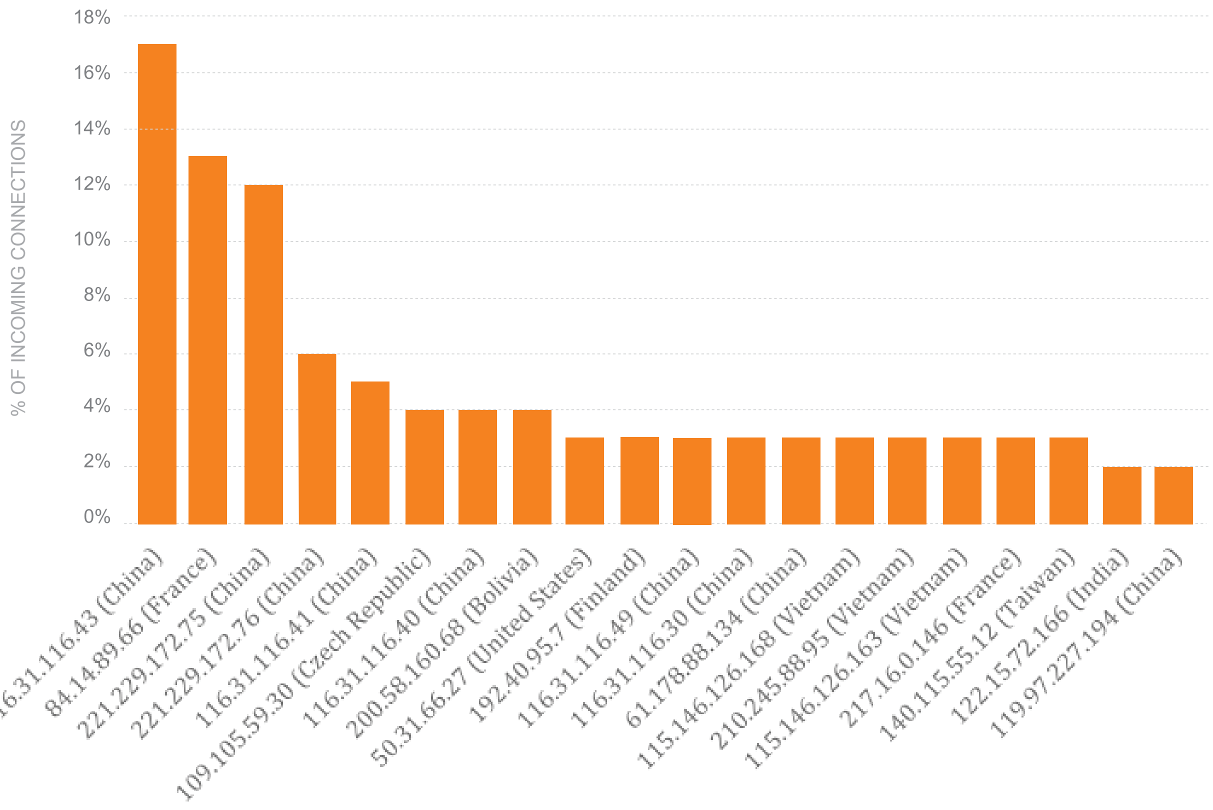
One of the easiest ways to take control over of the service or gain access to the system is to takeover data needed in authorization process: username and password. Because attacks on passwords tend to be time-consuming and resource-consuming, criminals first of all will try to log into the services and devices using default or common usernames and passwords, as shown in the graph below.

TOP 20 USERNAME / PASSWORD COMBINATION USED
IN LOGIN ATTEMPTS TO SERVICE

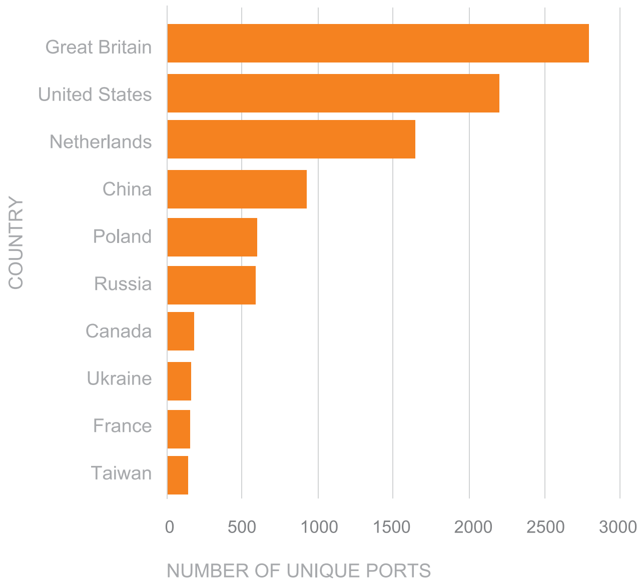


The most common source addresses of login attempts occur from:

TOP 20 source IPs



TOP 10 countries that scanned the largest number of unique ports:



6.3.2 Port scanning

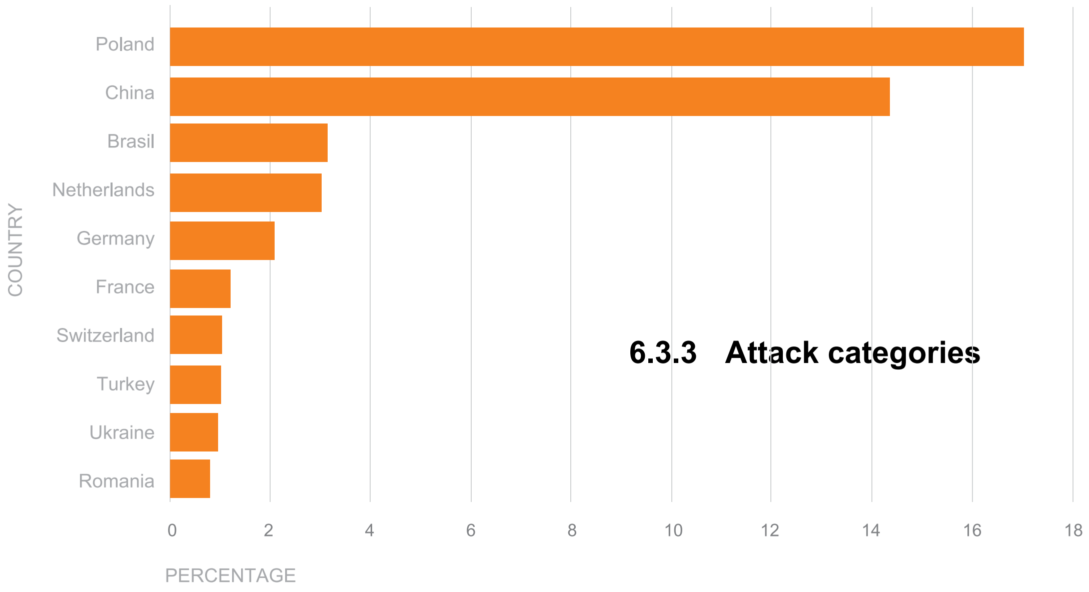
Cybercriminal attempting to break into a targeted machine begins with reconnaissance of victim's network environment, for example by scanning system to find out active services (open to certain ports). This allows the attacker to determine types and versions of services running on the potential targeted system. If it turns out that one of them has an unpatched vulnerability it can be used to attack or even execute arbitrary code with the privileges of the administrator. That would allow easier access to the system for attacker and to better hide his presence by rootkits installation.

The tables below show statistics for port and services scanning, based on the IP addresses of scanning sources analysis carried out by CERT Orange Polska. The largest numbers of scans are from source addresses located in the UK, USA and the Netherlands.

List of countries from which came most of scans looks different. In this case, the biggest scanning sources are Poland, China and Brazil. The largest number of scans from Poland detected in the Orange Polska network may be caused by "proximity" of network sources of such scans. In case of foreign scans, they may be partially filtered by the other operators.

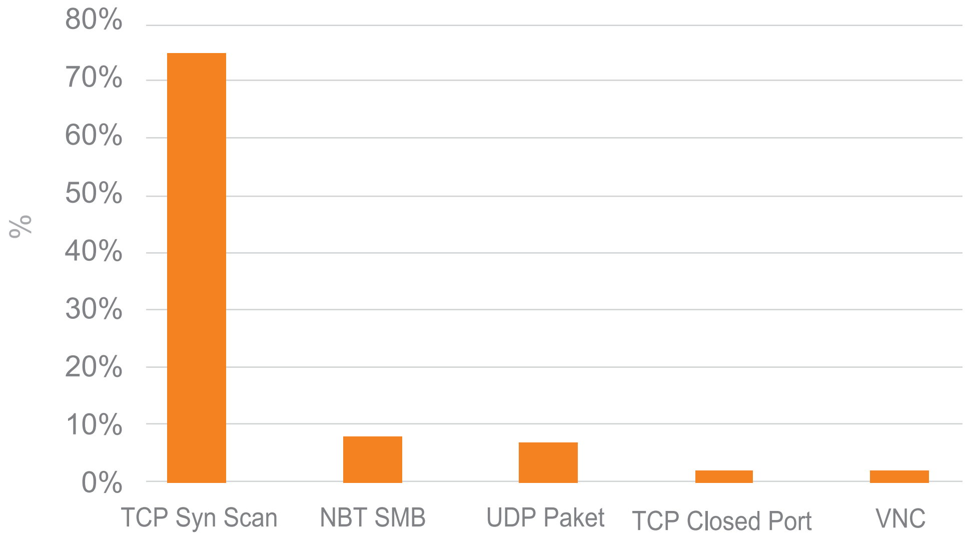
If we know what is being scanned, we can conclude what vulnerabilities and attacks are most commonly used. Therefore, here is a list of TOP 10 ports scanned in terms of the number of scans.

TOP 10 countries, from which came most of scans:

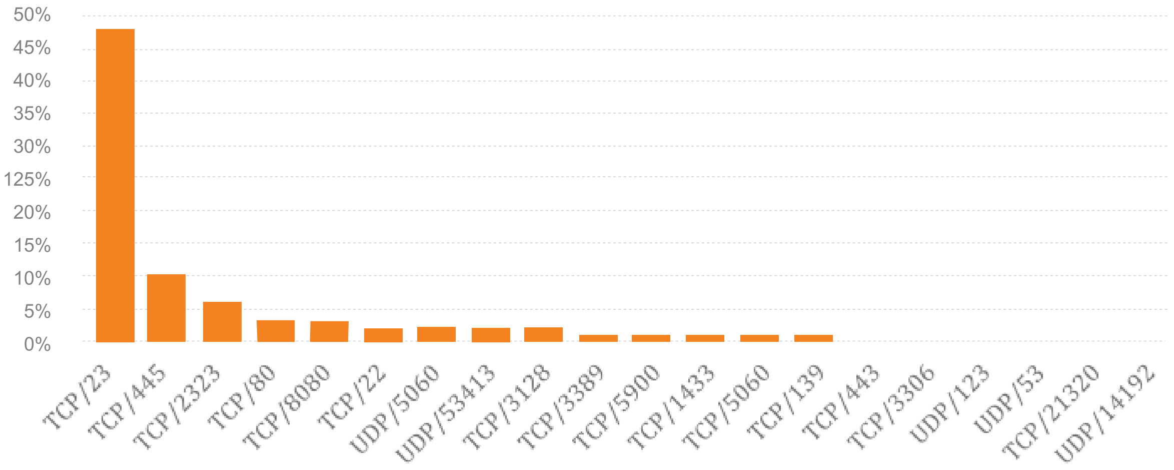


6.3.3 Attack categories

No.	Port	Description
1	5060	Default Session Initiation Protocol port; Commonly used signaling protocol for VoIP.
2	1433	Standard port for Microsoft SQL Server; Frequently scanned by bots looking for vulnerable or protected by weak passwords databases.
3	5900	VNC port; VNC is a system enabling remote access to the desktop of another computer.
4	110	Default POP3 port used by e-mail clients to receive messages; can be used for example in brute force attack in order to compromise e-mail account password
5	3389	Remote Desktop Protocol port; can be used to gain control over system or as destination port in DDoS attack.
6	3306	MySQL port – most common Relational Database Management System.
7	1900	SSDP port that is used to detect UPnP (Universal Plug-and-Play) devices; frequently used in DDoS attacks.
8	161	Simple Network Management Protocol port; family of protocols used in network devices management; allows to gain detailed information about network.
9	995	port POP3S (Secure Post Office Protocol)
10	8080	Port used by many web proxy servers and applications as: Syncthing GUI, M2MLogger or Apache Tomcat server.



TOP 20 destination ports for entire honeypot enviroment



6.4 Phishing campaigns on Polish Internet users

As expected, phishing attacks and malware campaigns occurred very often in 2016. Below we present some cases of attacks against which users of our network were protected by CERT Orange Polska:

Phishing attacks related to „500+ Family Program"

- Mailing campaigns, impersonating Internet portals for the submission of applications
- Premium SMS subscription services

Phishing attacks on e-banking users

- Mailing campaigns, impersonating e-banking portals
- Aimed at stealing of account login information and payment card data

Phishing attacks on clients of the Poczta Polska

- Malware campaigns
- False mail messages, impersonating notifications from the Poczta Polska and containing links to the Cryptolocker software (type of ransomware)
- Ransom for decrypting data - 1299 zlotys (only for a short period), and later - 2399 zlotys

Phishing attacks on the clients of PZU Group (Polish insurance company), under the guise of sending an invoice

- Malware campaigns

Phishing attacks on the clients of Play (Polish mobile provider)

- Malware campaigns

The actions taken to protect the users of the Orange Polska network included:

- Identification of samples (malicious e-mails, web pages, domains/IP, samples of software)
- Blocking of users' traffic to malicious domains/IP/phishing websites

Examples:

- In case of phishing attacks on clients of the Polish Post, about 10 thousand connections was blocked what prevented malicious data encryption on victim's computers
- About 10 phishing sites related to 500+ Program were blocked
- warnings and advices published on pages CERT.Orange.pl and blog.orange.pl
- cooperation with the web hosting companies - removal of malicious content inserted by attackers
- direct communication to users that visited fake webpages (see example pages below)

6.5 Attacks on e-banking services

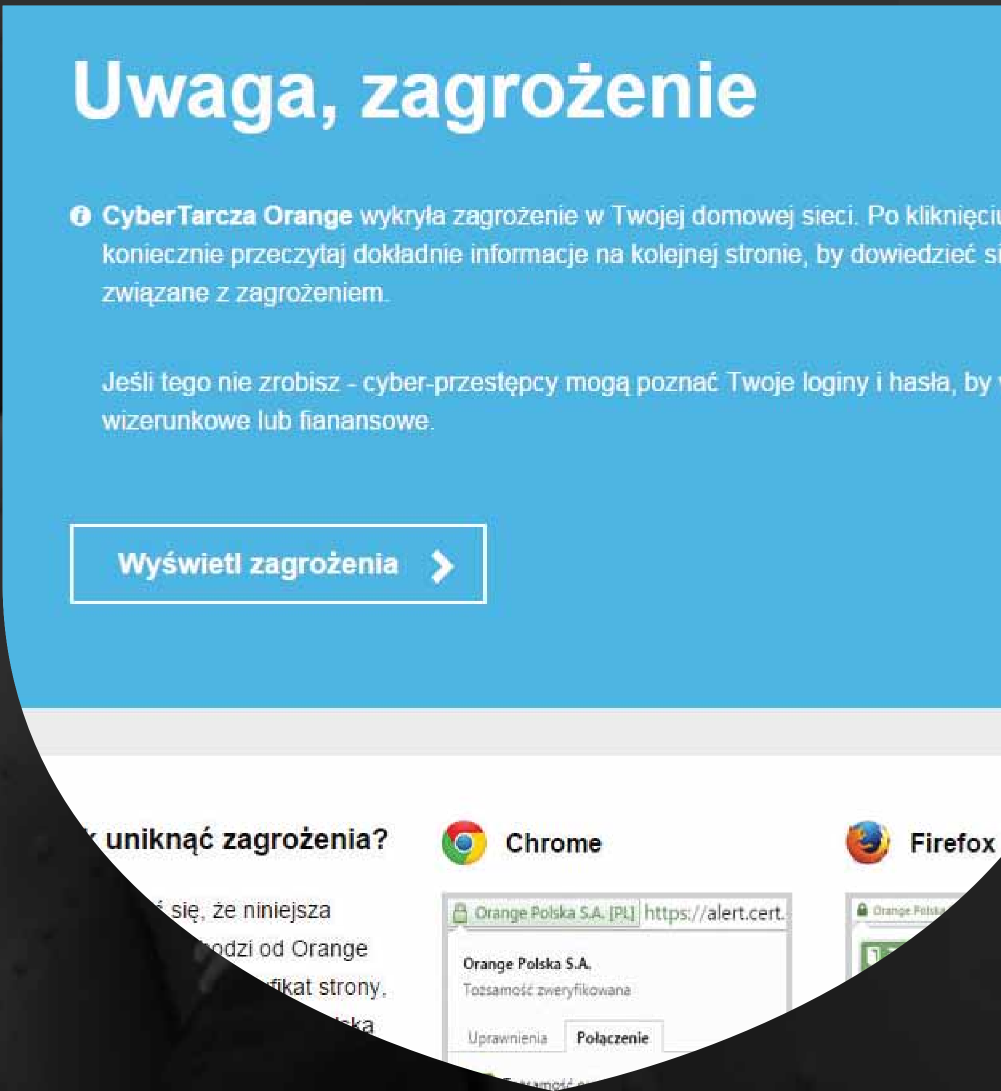
For years, the finance sector has been the focus of cybercriminals and also the year 2016 brought a wave of attacks on Internet banking systems. They were aimed both at the technical infrastructure and directly at banks' customers.

They have proven that the channel used for bank-client communication, more and more often is an e-mail or SMS – a form very vulnerable to threats, and because of this, effectively exploited. In particular, among the dominating methods are phishing attacks during which customers are at risk of stealing of their login information and payment card data. Even worse, the content of fake e-mails is better adapted for particular banks and customers, and false bank services imitate better the real ones. One of the key issues that still remains is the improvement of security measures and monitoring of services that are used in the bank's communication with customers.

In the last year, institutions of the banking sector were not spared the DDoS attacks, during which monetary demands were made. Banks proved to be quite well prepared and even DDoS attacks with a capacity of 50 Gbps did not block their services, and the clients barely noticed any difference in functioning of the transaction services.

The scale and diversity of threats on online banking continue to grow. Recent years have shown that improving security remains for the financial sector the highest priority issue. Huge outlays on security mean that this is still one of the most protected sectors of critical services. This fact was used in connection with the start of the " 500+ program " when banks enabled registration program on their own platforms.
It improved the process of registration of beneficiaries, but most of all it reduced stealing of their confidential data, during extreme intensity of phishing attacks when the program started.

The financial sector has been for a long time in the focus of cybercriminals and also the year 2016 brought a flood of attacks on Internet banking systems. They were aimed both at the technical infrastructure and directly at banks' customers. They have proven that the line of the “bank-customer” contact – more often an e-mail or SMS – is very vulnerable and thus effectively exploited by attackers.



Uwaga, zagrożenie

CyberTarcza Orange wykryła zagrożenie w Twojej domowej sieci. Po kliknięciu
koniecznie przeczytaj dokładnie informacje na kolejnej stronie, by dowiedzieć si
związane z zagrożeniem.

Jeśli tego nie zrobisz - cyber-przestępcy mogą poznać Twoje loginy i hasła, by
wizerunkowe lub fianansowe.

6.6 Case studies

6.6.1 DDoS attack on the Neostrada customer

The incident concerned a specific DDoS attack (Distributed Denial of Service) as it was aimed at resources of one of the Neostrada clients. While it can be assumed that the goal of the attack was to limit the availability of Internet service of one client, its size alerted the operators. There was a real risk of disruption of Internet access for others, by using the attacked network node. Due to the need to maintain a high quality of services, network nodes of Orange Polska are proactively monitored 24/7 for network traffic that might indicate an attack attempt.

The characteristics of the attack:

Size: average 50 Gbps (gigabits per second), at peak nearly 70 Gbps.
Duration: about 1.5 hours.
Attack Type: mostly DNS Amplification (reinforced reflection using open DNS servers) and IP Fragmentation

The attack was neutralized in this case, by setting a black-hole trap - to prevent any communication to/from the attacked IP address. In such case, the attacked IP address is excluded from the pool of available addresses, which clears the communication with other users connected to the same network devices. A user whose IP address was attacked, is given a new IP address (within the Neostrada service, addresses are dynamic), which allows uninterrupted connection to the Internet.
The DDoS attacks against the clients of broadband Internet are relatively common, due to the ease and low cost of carrying them out. Some of the DDoS tools are available for free, while on the black market, DDoS "service" costs a few/several dollars. Its duration usually does not exceed several minutes. However, in most cases, even a few minutes is enough (available as free tests) to prevent the execution of transactions in a given time, block access to the service at a critical moment, or what is more frequent, for instance log out a gamer from e-sport competitions.

> **> Due to the need to maintain a high quality of services, network nodes of Orange Polska are proactively monitored 24/7 for network traffic that might indicate an attack attempt.**

6.6.2 Phishing attack on users of MMS Orange Polska and frauds related to Premium SMS services

The incident concerned sending of e-mails that pretended to be messages from Orange Polska. Phishing mails informed about the availability of a missed MMS from Orange Polska and urged using premium rate services.

Fake e-mail messages were sent out from an e-mail address MMS ORANGE <mms@mms.orange.pl>. The purpose of such e-mail was to persuade a user to visit a phishing site that allegedly referred to Orange Polska. Clicking on the reference link http://mms.orange.pl, provided in the message, actually led a user to one of fake sites, i.a.: http://mms-orange.8634.su/, http://mms-orange.ivi.pl, http://mms-orange.pl. Then the victim was asked to

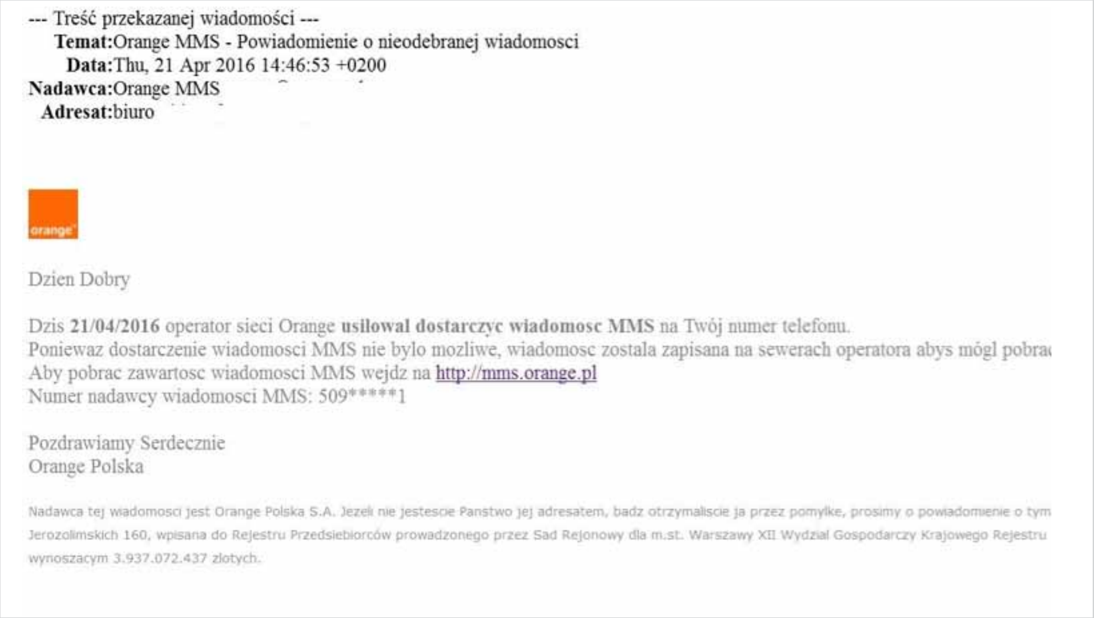
send an SMS – from a phone number, on which allegedly an MMS failed to be delivered – to a premium rate number, specified on the phishing page.
The attacker objective was the extortion of money from victims. Sending an SMS resulted in the victim's charge on more than 30 zloty for each SMS.

The scale of this incident was about tens of SMS sent by users. Such a little impact was the result of measures taken by the CERT Orange Polska and other security units:

- Blocking connections to phishing websites for Orange Polska users
- Intervention for blocking dissemination of phishing website
- Posting a warning message about the threat on the website orange.pl (cert.orange.pl; blog.orange.pl)
- Providing guidance and recommendations to the Hotline Orange Polska consultants
- Blocking, at the request of Orange Polska, the Premium SMS service and refund to subscribers for sending SMS using a phishing website.

6.6.3 Phishing attack under the guise of an invoice from Orange Polska

The incident concerned dissemination of e-mails claiming to be from the Orange Polska, under the guise of an invoice delivery. Fake e-mails looked almost identical to the original ones.



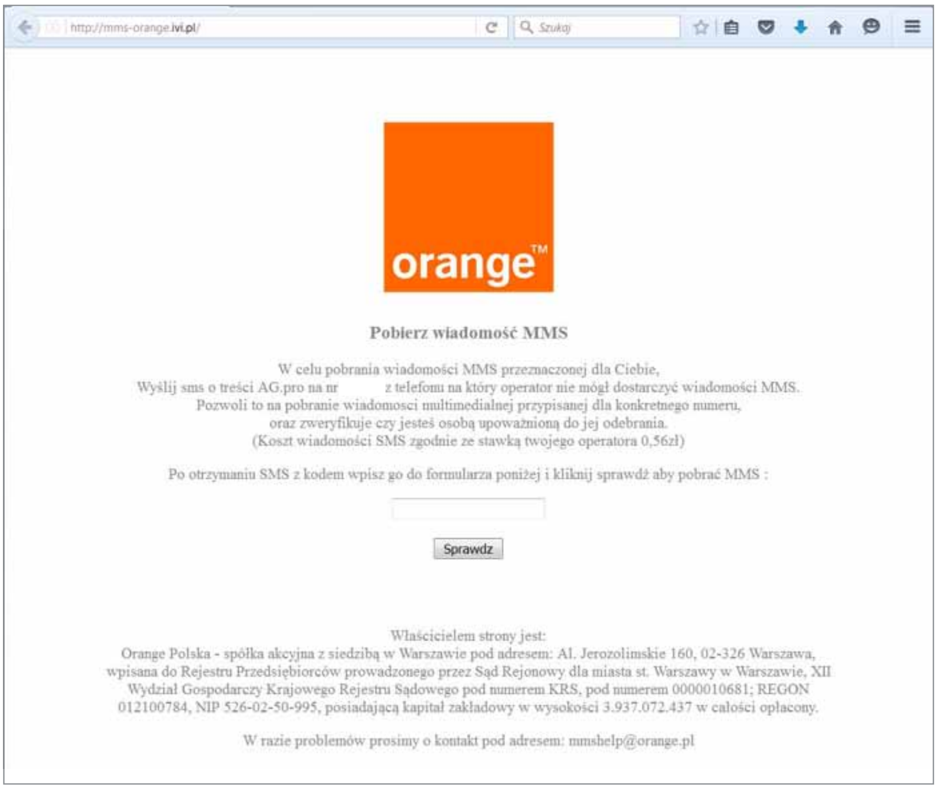
--- Treść przekazanej wiadomości ---
Temat: Orange MMS - Powiadomienie o nieodebranej wiadomosci
Data: Thu, 21 Apr 2016 14:46:53 +0200
Nadawca: Orange MMS
Adresat:biuro

Dzien Dobry

Dzis **21/04/2016** operator sieci Orange **usilowal dostarczyc wiadomosc MMS** na Twój numer telefonu.
Poniewaz dostarczenie wiadomosci MMS nie bylo mozliwe, wiadomosc zostala zapisana na sewerach operatora abys mógl pobra
Aby pobrac zawartosc wiadomosci MMS wejdz na http://mms.orange.pl
Numer nadawcy wiadomosci MMS: 509*****1

Pozdrawiamy Serdecznie
Orange Polska

Nadawca tej wiadomosci jest Orange Polska S.A. Jezeli nie jestescie Panstwo jej adresatem, badz otrzymaliscie ja przez pomylke, prosimy o powiadomienie o tym
Jerozolimskich 160, wpisana do Rejestru Przedsiebiorców prowadzonego przez Sad Rejonowy dla m.st. Warszawy XII Wydzial Gospodarczy Krajowego Rejestru
wynoszacym 3.937.072.437 zlotych.



http://mms-orange.ivi.pl/

Pobierz wiadomość MMS

W celu pobrania wiadomości MMS przeznaczonej dla Ciebie,
Wyślij sms o treści AG.pro na nr z telefonu na który operator nie mógł dostarczyć wiadomości MMS.
Pozwoli to na pobranie wiadomosci multimedialnej przypisanej dla konkretnego numeru,
oraz zweryfikuje czy jesteś osobą upoważnioną do jej odebrania.
(Koszt wiadomości SMS zgodnie ze stawką twojego operatora 0,56zł)

Po otrzymaniu SMS z kodem wpisz go do formularza poniżej i kliknij sprawdź aby pobrać MMS :

Właścicielem strony jest:
Orange Polska - spółka akcyjna z siedzibą w Warszawie pod adresem: Al. Jerozolimskie 160, 02-326 Warszawa, wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla miasta st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS, pod numerem 0000010681; REGON 012100784, NIP 526-02-50-995, posiadającą kapitał zakładowy w wysokości 3.937.072.437 w całości opłacony.

W razie problemów prosimy o kontakt pod adresem: mmshelp@orange.pl

Characteristics of fake messages:

- the message sender address: e-faktura@pl.orange.com
- the subject of a message: E-Invoice Orange account 1.18733482 / 1.17703897
- a message body contained a fake hyperlink in the form of PDF icon and recommendation to click on it in order to download the invoice

However, the link (http: //miliciousURL/ddl7.data.hu/get/0/9618321/FAKTURA_P_14841360_16030804998006.pdf.zip) led to a malicious site from which malicious file may be downloaded. The user's computer becomes infected upon a malicious file opening. The result of the malicious code analysis identified i.a. malicious domains and controlling IP addresses. The virus allowed taking complete control of an infected machine, which in turn made made sensitive data theft possible to steal sensitive data.

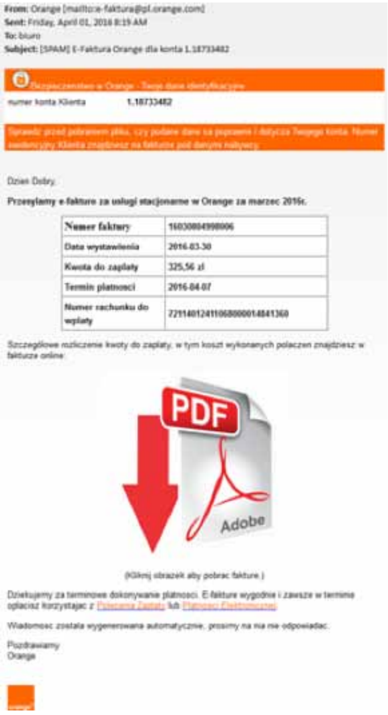
> On many occasions, malware analyses are a foundation for advanced analytical work of reaction team specialists. CERT Orange Polska regularly conducts such analysis. Selected results are presented in the annexes to this report.

Although the scale of the attack on the basis of reported incidents (a few hundred) was large, quick actions, inhibiting the attack, helped effectively to protect users of the Orange Polska network.

The measures taken to minimize the threat were as follows:

- Blocking the access to malicious domains/IP addresses (malicious/phishing websites, C&C) for Orange Polska users
- Intervention aimed at providers (owing malicious domains/IP addresses) concerning blocking malware distribution
- Posting a warning message about the threat on the pages of orange.pl (cert.orange.pl; blog.orange.pl)
- Providing guidance and recommendations for Orange Polska Hotline consultants
- Reporting the case to law enforcement agencies.

It is worth noting that the mail domain from which Orange Polska sends the original invoice delivery notification, has a number of safeguards. On the one hand, they discourage criminals to carry out the attacks, but on the other hand limit their consequences - many users will not receive such a spam mail. The server pl.orange.com uses i.a.DKIM (Domain Keys Identified Mail) technology. If this technology is supported by the server of the user email provider, then message from the above address, substituted by a cybercriminal, will be automatically rejected.



From: Orange [mailto:e-faktura@pl.orange.com]
Sent: Friday, April 01, 2016 8:15 AM
To: biuro
Subject: [SPAM] E-Faktura Orange dla konta 1.18733482

Bezpieczenstwo w Orange - Twoje dane identyfikacyjne

numer konta Klienta	1.18733482

Sprawdz przed pobraniem pliku, czy podane dane sa poprawne i dotycza Twojego konta. Numer ewidencyjny Klienta znajdziesz na fakturze pod danymi nabywcy.

Dzien Dobry,

Przesylamy e-fakture za uslugi stacjonarne w Orange za marzec 2016r.

Numer faktury	1603080498006
Data wystawienia	2016-03-30
Kwota do zaplaty	325,56 zl
Termin platnosci	2016-04-07
Numer rachunku do wplaty	72114012411068000014841360

Szczegółowe rozliczenie kwoty do zaplaty, w tym koszt wykonanych polaczen znajdziesz w fakturze online.

(Kliknij obrazek aby pobrac fakture.)

Dziekujemy za terminowe dokonywanie platnosci. E-fakture wygodnie i zawsze w terminie oplacisz korzystajac z Polecenia Zaplaty lub Platnosci Elektronicznej.

Wiadomosc zostala wygenerowana automatycznie, prosimy na nia nie odpowiadac.

Pozdrawiamy
Orange

6.6.4 Malware

In many cases, the malware analysis is the basis of advanced analytical work of response team specialists. CERT Orange Polska regularly conducts such analysis. Selected results of the analysis are presented in the annexes to this report.

7 Main threats, vulnerabilities and events of 2016

As expected in the year 2016, cyberspace was a frequently used field of criminal activity. Increasingly believable phishing campaigns and data leaks from numerous databases were frequent events. Also, there was no shortage of critical vulnerabilities being revealed in popular systems. All the more it pleases to see the increasing involvement of governments and international organization into developing countermeasures against ICT attacks. Approval of the NIS Directive by the Member Countries, or the outcome of the NATO Summit Warsaw 2016 should be classified as such initiatives.

CERT OPL carries out constant monitoring of events connected with cyber-security. In case of appearance of information about a threat, CERT OPL conducts an analysis, and if needed, takes necessary actions connected with the protection of Orange Polska clients through i.a. restricting communication with the criminals' servers, running information campaigns or launching the CyberShield campaign.

Overview of the main events of the year 2016

12.01

Bug on OLX.pl allowing user account interception

Due to a bug in the mobile application OLX for Android, the users of OLX.pl were giving others opportunity to intercept their accounts by posting links to their ad's on Facebook. This was possible due to an automatic login code embedded into the links. By clicking on a link to such ad, other users automatically gained access to someone else's account, thus allowing the possibility of viewing and modifying data. Several dozen OLX users were affected. The bug was fixed on January 12.

14.01

Mailing campaign impersonating InPost under the guise of acknowledgement of parcel receipt .

Internet users were receiving phishing messages impersonating the InPost Company and faking acknowledgement of receipt. The fake acknowledgements included a request for review of the shipping along with information about an attachment containing delivery details. In truth, the e-mails contained malicious attachment which installed a Trojan upon opening.

19.01

Vulnerability in Linux allowing raising privileges to the root level.

At the beginning of the year, a serious vulnerability was detected in the keyring mechanism, which has been present in the system's kernel for about three years. The published exploit allowed regular users to gain root privileges. Due to Linux system's popularity, the threat applied to various devices, including smartphones running Android system. In case of Android, this dangerous bug allowed gaining access to data of other applications. A swift patch development was announced, however especially in case of Android, due to usually short support by the manufacturer, a considerable amount of devices may never get updated.

26.01

Bug on the website viasms.pl allowing downloading private data of any chosen clients

Lack of appropriate identification system created a threat of a private data leak in an online loan company viasms.pl. Any client of this company could download the contents of loan agreements concluded by other clients. This was possible due to a trivial agreement identification system. All that was needed was to enter an agreement identifier (which was incremented by 1) in the particular place of the web address bar. The problem of data leak could apply to over 2 million agreements. The agreements included i.a. Personal Identity number, series and the number of the identity card, personal address, e-mail address and phone number.

01.02

Bug in a mobile application from T-Mobile granting access to other clients' private data

T-mobile subscribers using iboa.pl service or MiBOA application for managing their account experienced a problem of automatic login to other users' accounts. Automatic login resulted in gaining unauthorised access to contact information of other subscribers. They could review payments information, call history and change many settings. T-Mobile solved the problem after a few hours, by disabling the automatic login option and setting a requirement to enter phone number and one-use password to login.

03.02

Mailing campaign impersonating Orange Polska under the guise of sending an invoice

Internet users were receiving phishing messages impersonating the Orange Polska company. This time, the fake messages were supposed to convince the victims to open a file that resembled the operator's invoice. The aim was to steal the subscriber's private data. The malicious software worked as a keylogger, taking snapshots of active applications, copying "cookies" and logging information from browsers. Orange Polska blocked addresses of the services connecting with malware for its clients, ensuring them that their data is secure, even if they had carelessly opened the malicious file.

2016

27.02

Break-in into the 2be.pl server room resulting in, i.a. services ceasing to function

The break-in was serious enough to block functioning of all hosting services provided by the company. During the next few days after the failure, the anxiety of the clients who had been deprived of access to the services and also begun worrying about the safety of their data and domains was increasing. Unavailability of services continued for 2 months.
As a result, over 2 thousand clients lost their data. The direct result was termination of the Adweb's contract by NASK (as National Domain Registry). NASK addressed the subscribers affected by the crash to request an authinfo code directly from it, which would allow transferring the service. In response to that, the owner of the Adweb Company announced that after 14 years, he terminates his operation.

29.02

Phishig attacks on mBank's electronic banking users

mBank clients became a target of a phishing campaign aimed at bank account login information, and payment card data breaches. The message to the bank's clients contained false information that their account has been blocked for security reasons, due to an alleged unauthorised access attempt. In the e-mail, clients were asked to click on the link provided, which was to verify the account owner's data and unblock the account. The campaign used several fake domains which were not detected as phishing by browsers. A careless client could fail to notice that the link doesn't lead to the secure site of the bank (the https:// part was lacking) and that the message was sent from a random e-mail address. Clicking on the provided link resulted in being redirected to a fake mBank website and filling a fake form with private personal data.

01.03

DROWN – a new kind of attack on TLS protocol

Information about a new attack targeting TLS protocol was posted on the Internet. The attack can be carried out if the server with whom communication is being made supports the SSLv2 protocol and uses the same private key. The attack is also possible if the server doesn't support SSLv2, but shares the private key with a different server which does support it. Since the attack belongs into the MITM type, an additional condition for carrying out such attack, would be that the attacker should be positioned between the client and the server in communication.

09.03

Publication of the CERT Orange Polska report for year 2015

This was the second edition of this report and the only document of this kind released by the Polish Telecom. The report addresses current security issues and is aimed at a wide demoaudience interested in the topic of security.

14.03

Certification of CERT Orange Polska as Trusted Introducer

CERT Orange Polska was granted the Certified status by the Trusted Introducer organisation, operating alongside TF-CSIRT. TF-CSIRT is the largest European organisation bringing together reaction teams, and certification is the highest level of award granted by this group. Thus, CERT Orange Polska became the first and only one such team in Poland to date.
At the same time, it joined the most exclusive group of only sixteen certified teams in entire Europe.

23.03

Mailing campaign impersonating the Polish Post

Internet users were receiving phishing messages impersonating the Polish Post. The messages contained information that their parcel cannot be delivered.
The e-mails could raise suspicion due to a strange title and sender address.
A careless message recipient however, who clicked on the link provided in the e-mail to check parcel details, was redirected to a website impersonating the official one of Polish Post's. There, he downloaded an extremely malicious Cryptolocker software file, which encrypted files on his computer's hard drive. Decryption was possible after paying a ransom.

30.03

Phishing campaigns connected with the 500+ programme

In connection with launching the 500+ programme, threats of data breaches and monetary extortion from the programme beneficiaries appeared almost immediately. The cybercriminals copied the official rodzina500plus.gov.pl website, creating an almost identical one in the domain rodzina500plus.info.pl (hosted in Poland). Blocking the fake website resulted in creation of its clone in rodzina500plus.net.pl (this time hosted in Russia). The fake website offered an option submit an application online, requiring the beneficiary's phone number in the first step. Then the victim received a text message to this number, containing a code the entering of which activated a subscription of a pay SMS service. It is worth mentioning that the phishing websites were successfully blocked by the Orange CyberShield, and the clients of Orange were informed about the threat.

01.04

Phishing campaign impersonating Orange Polska under the guise of sending an invoice

Once again, CERT Orange Polska noted increasing number of fake Orange Polska invoices containing malware-infected attachment. The fake invoices were distributed among Internet users. The clients of Orange Polska were protected from downloading the malicious attachment.

2016

04.04

Hacked KOD's websites

At the beginning of February first unconfirmed reports from several Internet users appeared, presenting screenshots of replaced Committee for the Defence of Democracy (KOD, Kijowski's private blog) websites. At that time there were no reliable sources that would allow verifying the authenticity of these reports. Also, in the beginning there was no sufficient evidence allowing confirming that the websites were hacked. Eventually, the attack victim himself announced that his wp.pl e-mail account was compromised, and that the KOD websites were replaced. At the same time he noted that the functionality of the KOD's website was immediately restored. The e-mail account, on the other hand hasn't been used for a long time, and it was disconnected from any services related with the KOD's activity.

07.04

Hacking of the Zbiornik.com service and data leak

Software vulnerability caused a user data leak on the sex dating site zbiornik.com. As a result of vulnerability of one of the older scripts, the hacker managed to copy part of the database. The threat of releasing the data to the public was then used to blackmail both owners of the site and its users, in order to extort a ransom. In response to blackmail, the websites administrators made the issue public and offered a reward for determining the hacker's identity. Also, they made efforts to secure the servers and patch potential system vulnerabilities. Users were advised to change their passwords, which were additionally secured. Due to strong competition among such services, this kind of incidents may occur more often.

13.04

Hacking into the "Horyzont " hosting service

The Horyzont Technologie Internetowe hosting company from Poznan fell victim to hacking, which resulted in both company's and clients' websites becoming unavailable (including Lech Poznan's site). According to the company's announcement, the attack used vulnerabilities of in the old version of PHP. The company assured that the infrastructure and the client's data were not threatened, and the service would be restored within several hours.

15.04

Dismantling Lublin-based criminal group robbing bank accounts

The Polish Police and public prosecutor's office managed to dismantle an international criminal group assembled in Lublin Voivodship, which stole 94 million PLN from banks.
The criminals used the Timba virus to intercept data from bank accounts. The total outcome is 800 break-ins into bank accounts in Poland, Europe, USA and Canada. Among the affected parties businesses, universities, county and regional offices were in majority, but alongside them, there were also private individuals. The group has been functioning since at least 2012. 148 people were detained, coming mostly from Poland and Latvia. It was possible to return 57 million PLN to the victims.

22.04

Mailing campaign impersonating Orange Polska under the guise of unread MMS messages

CERT Orange Polska noted an increase in number of e-mail notifications distributed among Internet users, concerning allegedly unreceived MMS messages from Orange Polska. In the contents of the e-mails the recipient was being convinced to click on a fake link, which in reality led to a phishing site. Upon entering the site in order to download the MMS message the user was advised to send a SMS message from the phone which supposedly failed to receive the MMS message. The phone number on the website was premium-rate, and additionally it activated a subscription of pay incoming SMS messages. CERT Orange Polska took appropriate measures, blocking the access to the phishing websites for its clients. Aside from that, it undertook several interventions connected with blocking spam and not spreading of phishing websites (at e-mail and hosting service providers) and intervened at the Premium Rate service provider.

04.05

Arresting PollyPocket, suspected of breaking in to Plusbank

The police arrested the second hacker standing behind the break-in into Plusbank. The hacker nicknamed PollyPocket along with previously detained Polsilver, redirected several dozen bank transfers to their accounts (totalling 3,5 million PLN). Then they located the money on bitcoin stock exchange.
The cybercriminal has been caught thanks to cooperation of the Central Bureau of Investigation of the National Police and IT security specialists from the National Police Headquarters. During the apprehension, computers, data storage devices, cell phones, and SIM cards were secured. The charges included computer fraud attempt concerning property of substantial value and money laundering, which combined carries a sentence of 10 years in jail. PollyPocket was already known from previous incidents connected with i.a. disclosure of personal data of an Internal Security Agency captain and theft of a film script along with contact information of many Polish actors.

06.05

Private data leak of over million users of the BeautifulPeople.com dating service

Due to insufficient database protection, data of over a million users of dating website BeautifulPeople.com has leaked. The data included surname, phone number, full address, and sexual preferences. The data intercepted by the criminals was put up for sale on the darknet. The break-in resulted also in the leak of 15 million private messages exchanged between the portal's users. The portal officially announced that the database security has been increased, and affected users were informed about the leak. This is yet another incident which shows how important it is to protect one's privacy in the web and to reduce the amount of personal data shared to a bare minimum.

2016

09.05

DDoS attacks on Polish banks and blackmail attempt

The DDoS attack on at least two large Polish banks continued over a course of several days. The attackers were making threats monetary demands. During the first attack, the bandwidth achieved by the attackers was reaching a dozen Gbps, whereas during next ones, over 50 Gbps. The banks repelled the attacks successfully, and the clients barely noticed any difference in functioning of the transaction services. The analysis of the attack indicates that the traffic could come from many different sources, including services like „DDoS as a service", which means services allowing ordering a pay DDoS attack on a chosen target.

18.05

Data leak from the LinkedIn service

In the darknet TheRealDeal service an offer appeared concerning selling a database from the LinkedIn website containing 167 million records, 117 million of which included e-mail address and password hash. It turned out that the offer was a result of a data leak from 2012, when a list of 6,5 million SHA1hashes originating from LinkedIn was published on a Russian forum. Back then, after a certain delay, LinkedIn admitted to the leak, but did not reveal its scale. Only now it came to light that it was a complete database of over 150 million users. Since it was anticipated that in a short time 90% of the passwords will be broken, users were advised to change their passwords as soon as possible, especially those who had a LinkedIn account in the year 2012 and were using the same e-mail address and password for logging into other websites.

28.05

Data leak from the MySpace.com website

Another user database sales offer which appeared in the TheRealDeal service revealed one of the biggest data leaks in history to date connected with MySpace service. The database put on sale contained over 400 million passwords stored as SHA1 # shortcuts (including that of over a million Polish Internet users). Similarly as with the one from LinkedIn, the leak must have happened much earlier, but hasn't been made public. The size of the MySpace database increased to around one billion users during this time.

01.06

Malware campaign using fake PGE invoices

Internet users were receiving phishing messages impersonating the Polish Energy Group (PGE). The fake e-mails got to their mailboxes on the 1st of June, which could cause some of the PGE's clients to let down their guard. Clicking on the provided link redirected to a fake website. Dynamically changing addresses of the phishing sites were an impediment to spam filters. On the sites, upon entering CAPTCHA, a download of a fake invoice in a .zip format would start, the extraction of which resulted in installation of a Cryptolocker-type malware, encrypting the data from the hard drive. Ultimately, the ransomware attack was aimed at extorting a ransom.

13.06

Data leak from the iMesh.com service

Putting data on sale in the darknet revealed another user data leak, this time from iMesh.com - a P2P service used for data exchange. The iMesh service was attacked in the year w 2013 and in the result over 50 million accounts were stolen, including 2,5 million from Polish users. The data contained i.a. IP and e-mail addresses, logins and passwords stored as MD5 hash function with salt. For safety purposes it should be assumed that the users' passwords were disclosed.

15.06

Putting intercepted servers on sale (xDedic)

A wide range of offers concerning access to intercepted business and private servers functions under the name of xDedic. It consists of over 175 thousand IP addresses leading to over 70 thousand servers worldwide. The scope of possibilities of using such servers is obviously enormous, and the price of access reflects that. Using an address of a trusted company is one of them. CERT Orange Polska (in collaboration with Kaspersky's team), came to the rescue of xDedic's victims by providing the website https://cert.orange.pl/xdedic/index.php, on which it can be checked if one of our IP addresses does not appear in the xDedic's database. In case of finding our IP address in the database we should follow the instructions provided by Orange Polska.

26.06

Malware attack on Facebook users

The Facebook service was hit by a virus which caused sending notifications to friends about including them in the comments. Upon clicking on the notification the user was redirected to an external domain, from which a malicious JavaScript file would be downloaded. The virus was not just sending notifications, but could publish posts containing malicious links on the user's timeline, send messages via chat, and also encrypt the victim's data.

2016

04.07

The establishment of the National Cybersecurity Centre (NC Cyber)

The National Cybersecurity Centre (NC Cyber) was established within NASK's structure. As an early warning and response centre, as well as data collaboration between key cybersecurity-related entities and data exchange centre, NC Cyber is to ensure the cybersecurity of the Republic of Poland. The centre functions on a 24/7/365 basis.

06.07

The NIS directive approved by the European Parliament

The European Parliament approved the NIS directive (Network and Information Security), which is to ensure a high level of cyber-security in EU. The directive imposes obligations on key service providers in every EU country, with regard to security services and reporting incidents national authorities. It also stresses the need to establish Computer Emergency Response Teams (CSIRT), whose co-operation would be coordinated by the European Union Agency for Network and Information Security (ENISA). The directive came into force after 20 days since its legislation. The member countries will have 21 months for its implementation.

08.07

Break-in to Netia and user data leak

There was a break-in into one of Neita's websites and web servers. Over 18 GB of the operator's data was stolen. Links to the stolen data were published on Twitter. The Netia's website was shut down, and its visitors would see a message that it was under maintenance. The stolen data included clients' first and second names, full addresses, Personal Identity numbers, identity card numbers and series, phone numbers, bank account numbers, e-mail addresses, and also contents of messages sent through contact forms. In response to the incident, Netia informed its clients about the break-in and the leak by sending SMS messages.

14.07

Phishing attacks on Onet E-mail users

Cybercriminals tried to steal passwords to mailboxes from Onet.pl e-mail users. As reported by the Zaufana Trzecia Strona website, one of the Onet E-mail users reported receiving a fake message about a successful login attempt through an unrecognized device in Estonia. The user was being convinced to update password recovery information if that attempt was not made by him. The link provided redirected to a fake website being very similar to the real Onet E-mail website, where the user was asked to enter the old password and set a new one. After changing the password, a separate message informed about a secure log-out from all devices and suggested the need to re-log using the new password. This time, the link led to the original Onet sign-in website.

20.07

Malware campaign impersonating PZU

Fake messages, impersonating PZU (Polish Insurance Company) and informing about unpaid invoices, were distributed to Internet users' e-mailboxes. The recipient could gain information on debts after clicking the provided link. Clicking on the link resulted in downloading a malware-containing file. At that time, the malicious file could only be detected by three little-known antivirus software programs. The attacker chose a trusted and well-known company and the end of the week as the time of the attack to increase its effectiveness.

21.07

Raising BRAVO-CRP emergency level in cyberspace during the WYD

At the time of World Youth Day, the emergency level in Poland's cyberspace was raised to the BRAVO-CRP level. BRAVO-CRP means an increased risk of an attack on IT systems. This imposes an obligation on public administration to ensure availability of personnel responsible for security of those systems in emergency mode. At the same time, it obliges to an increased monitoring of the cyber-security situation in Poland. Also, the general emergency level was raised to the ALFA level, which means a general warning that there is a risk of a terrorist attack.
The emergency levels were in force between 21 of July to 1st of August.

22.07

E-mail leak from the Democratic National Committee

WikiLeaks published several thousand e-mails which leaked from the server of the Democratic National Committee (DNC). Their contents suggested that Hilary Clinton was favoured by the party's authorities over Bernie Sanders. The messages came from the accounts of the most important members of the Committee, such as: director of communications, chief financial officers, and advisors.

2016

25.08

Data leak from the PESEL system

The Ministry of Digital Affairs uncovered a huge data leak from the PESEL (Polish Electronic System for Registration of the Population) system, the trace of which led back to several bailiff offices. One of the offices was in possession of as much as 800 thousand personal data records of Polish citizens. Apart from citizens' basic personal data, the PESEL system contains: first and second parents' names, date and place of birth, marital status, birth certificate number, registered address as well as series, number, and expiration date of ID cards and passports. It is quite astonishing that it was a year before the issue was detected, even though the number of requests to the PESEL system reached 2 million, and they were also being sent at night. The data can be put on the darknet, and access to detailed personal data of citizens gives criminals opportunities for colossal frauds, e.g. identity theft or forging ID cards.

Vulnerability in iPhone and iPad systems allowing i.a. stealing data

A serious vulnerability was revealed in iPhone and iPad systems, which was being exploited by the advanced Pegasus spyware. Researchers from Citizen Lab and Lookout determined that the malware uses three previously unknown vulnerabilities in Apple devices, and that it bypasses the iOS system security up to version 9.3.4. They called this exploit chain Trident. Malicious software could steal a number of data, including contents of messages, addresses of websites viewed and application data of Facebook, Skype, Gmail, etc. An update to the newest version of iOS (which contained adequate patches) was recommended as soon as possible.

01.09

Data leak from the music website Last.fm

Another data leak was revealed, this time from the music website Last.fm. The scale was 43 million user accounts, including at least a million belonging to Polish users. In this case, the leak also took place much earlier, which means in 2012. The data included username, e-mail address, password hash, and registration date. The passwords were stored as MD5 hash function, so it should be assumed that most of them were eventually broken. To protect ourselves from similar leaks we can use password management programs, avoid using the same password on different websites, and when possible, enable two-factor authentication.

14.09

A vulnerability in the ZUS's electronic platform, allowing viewing other peoples' private data

A vulnerability in the Electronic platform of Social Insurance Institution was patched in September, which allowed any person in possession of other tax-payer's basic personal information (first and second name Personal Identity Number) to create an account in his or her name. The system then would automatically fill in further information, such as employment history, contributions paid etc.

20.09

Record-breaking DDoS attack on OVH

The hosting company OVH became the target of the biggest DDoS attack in history, with bandwidth reaching even 990 Gbps. The source of the attack were IoT (Internet of Things) devices, and within these, mostly CCTV cameras and in-home IP devices. Countering DDoS attacks is quite challenging, as it requires huge financial outlays for hardware and link, as well as for specialists that react to new threats in swift and efficient way.

21.09

DdoS attack on Brian Krebs's website

Briana Krebs's (one of the most popular bloggers writing about IT security) website was attacked using traffic with bandwidth of 620 Gbps. It was one of the biggest DDoS attacks in history.

22.09

Yahoo user data leak being revealed

A huge personal data leak which happened in 2014 and affected at least 500 million users was revealed. The data included i.a. first and second names, phone numbers, e-mail addresses and password hashes (bcrypt). It remains unknown what vulnerabilities were exploited and who was behind this.

12.10

Fake SMS messages and frauds connected with SMS Premium service

Fake SMS enabling a pay Premium service were received by the clients of Orange. The contents of such fake message included information about an option to disable the service by sending SMS to the provided number, which actually resulted in money extortion. CERT Orange Polska warned its clients about the threat and informed that Orange never enables pay services without client's consent, and that most of services have a free trial period.

2016

13-14.10

Participation of CERT Orange Polska in Cyber Europe 2016

The CERT Orange Polska team took part in the operational phase of the fourth edition of the Cyber Europe 2016 exercises, organised by the ENISA agency. In Poland, the exercises were coordinated by the Ministry of Digital Affairs. The purpose of the exercises was checking procedural readiness for advanced threats from cyberspace and the effectiveness of cooperation of relevant actors, both on domestic and European level.

13.10

Malware campaign impersonating Play

The infected Play invoices were sent to public, mostly company e-mail addresses. In many cases the believability was enhanced by the fact that the recipient was addressed with a first, middle and last name. It is suspected that the cybercriminals might have obtained the data from the National Court Register. Malicious files included in the fake invoice could be detected by only 6 antivirus software programs. Opening the fake file resulted in a ransomware infection and encryption of the hard drive.

20.11

Malware attack on Facebook users

Facebook users could become victims of the attack by clicking on fake pictures in the chat window, only seemingly sent by a friend. In reality, the picture was a malicious .svg file sent by a worm. Downloading and running the file in the victim's browser resulted in being redirected to fake site impersonating YouTube and inducing the user into installing a malicious browser extension. There were also reports over the Internet that the attack was used for distribution of the Locky ransomware.

28.11

Attack on routers of the Deutsche Telekom users

One of the attacks from 2016 was targeted at Internet of Things devices. This time, the attack was exploiting vulnerability in some of the DSL modems. Among its victims were i.a. 900 thousand devices in the Deutsche Telekom network.

07.12

ISFB and an attack on Gmail users

In November/early December 2016, Gmail users infected with malicious ISFB software in one of previous campaigns might have fallen victim to a new form of attack. While using the Gmail web application, the ISFB injected a malicious HTML script inducing the user into providing his phone number. Giving the number resulted in receiving a SMS message containing a link which led to a malicious APK application.

15.12

Record-breaking user data leak from Yahoo

The biggest user private data leak in history was revealed. The leak again concerned the Yahoo website, but this time the data theft included a billion e-mail accounts. The data included e-mail addresses, usernames, and passwords. The break-in occurred in the year 2013. Yahoo advised its users to change their passwords.

Faktury Play

Phishing campaign under the guise of invoices sent by an IT operator was using a customized Trojan. The interesting thing is that the malware was also able to spread through USB sticks.

8 Orange Polska security services

8.1 Protection from DDoS attacks

The service offers protection of the client's online resources from volumetric denial of service attacks. The network traffic to the protected resources is monitored for anomalies that could result in bandwidth saturation and thus in loss of business process continuity on a 24/7/365 basis.

In case of an actual attack the suspicious packages are filtered, and only clean network traffic reaches the client. DDoS attacks are understood by:

- Attacks on bandwidth necessary for providing a service, e.g. by datagram flood ICMP/UDP,
- Attacks aiming to exhaust resources of the service-providing system, e.g. flooding with TCP SYN-flagged packages,
- Attacks on a specific application used for providing the service, e.g. attacks with the use of HTTP protocol (a large number of sessions imitating the session in the user's browser), DNS or protocols of VoIP applications.

The service functions thanks to combination of environments of the Arbor Networks platform, SOC and CERT Orange Polska teams as well as the application of other operative mechanisms in domestic and international traffic (dnssinkholing, blackholing etc.). The requirement necessary for using this service is having an Internet connection from Orange Polska in the MetroEthernet technology.

8.2 Web Application Protection (WAF as a Service)

The purpose of this service is protection of the client's web resources shared in the Internet (servers and applications) based on the Web Application Firewall platform located in the backbone network of Orange Polska. The entire http/https traffic from the Internet to the protected resources is redirected through the service platform and analyzed according to the approved security policy.

This service provides protection from the ten most critical web application threats defined in OWASP Top 10 and allows increasing web application security without the necessity to modify the code.

8.3 SIEM as a Service

The SIEM system (Security Information and Event Management) is a key element of IT security in the organization. When properly configured, the system gathers events from systems and applications crucial for conducting business, and conducts correlation in search of undesirable activities, which may be security incidents and pose a threat to the continuity of business processes.

The service offers made-to-measure implementation of the SIEM system for the client's critical structure: installation of the solution, availability and monitoring on 24/7/365 basis, integration of log sources, formulation and implementation of event correlation scenarios.

The immediate availability of the platform along with the knowledge and experience of Orange Polska experts allows quick coverage of key systems with monitoring to an extent desired by the client.

8.4 SOC as a Service

The service allows the client to use the help of the Security Operations Centre (SOC) team of Orange Polska - operators, analysts and experts are available on a time basis determined in the SLA – monitoring the SIEM system, which collects events from the client's computer. The SOC team, working 24/7/365, identifies events bearing the mark of security incidents (according to the security scenarios determined with the client) and reacts to each recognized incident in accordance with the defined procedures.

The service includes: integration of the client's SIEM system with an incident reaction team defined in the SLA, access to the portal and incident handling procedures, access to the human resources guaranteed by the contract, reports, administration and system maintenance.

The basis necessary for efficiently functioning SIC team is the possession of an implemented and properly functioning SIEM system by the client; for this reason, the SOC aaS service is often combined with the SIEM aaS service.

8.5 Feed as a Service

A subscription service consisting in delivery of information about malicious network activity detected in Orange Polska's infrastructure to the clients. The information is delivered in form of files in specific formats, including data on C&C

Orange Polska security services

1. Protection from DDoS attacks
2. Web Application Protection (WAF as a Service)
3. SIEM as a Service
4. SOC as a Service
5. Feed as a Service
6. IP Reputation Service
7. Code Audit
8. Security tests
    a. Penetration tests
    b. Performance tests (DDoS as a Service)
9. Protection from malicious software (Malware Protection InLine)
10. Malicious software analysis
11. Secure DNS

servers, domains and OP addresses of websites infecting browsers with malicious software, IP addresses exhibiting malicious network activity towards the Orange network (port scanning, attack attempts etc.).

The data-containing file may be downloaded automatically (API) or via web browser, and they allow the client to enhance the systems possessed with additional data. This allows filtration of the traffic between the client's localization and malicious websites in the Internet translating directly into improved security of the client's resources.

8.6 IP Reputation Service

This service offers an additional level of protection for the organization's IT resources that are published in the Internet for business purposes (electronic banking, e-commerce systems, intranet portals etc.).

The service consists in polling the Orange reputation base (online, real-time) for status of a computer/device, which tries to gain access to websites published by the organization – before this kind of access will be granted (e.g. before a user will have the chance to view the site or log into the company's web portal) Status is understood as information whether a device attempting to access the client's systems and identifying with a certain IP address may be infected with malicious software.

The service is offered in a form of a website (with a documented API interface), which accepts https requests containing the IP address in question from authorized subjects and responds with its status. The service only provides information about infections for the IP addresses from the Orange pool.

8.7 Code Audit

The service offers source code audit of the developed software in order to eliminate errors, which might result in critical security vulnerabilities during the application use in the production environment. The use of such vulnerability by unauthorized persons might lead, among others, to data leak, which usually means difficult to evaluate financial and reputation losses as well as legal consequences. Scanning of the source code is executed on the basis of a professional tool dedicated to both automatic and static code testing.

Supporting more than 20 programming languages, the service covers wide spectrum of applications, starting from compiled binary apps (C, C++ etc.) for operating systems, to web applications (PHP/Java/JS etc.). Results of the automatic scan are later verified by an Orange expert, who verifies and classifies the found vulnerabilities and finally reports them to the Client. The report contains the detailed vulnerability lists, the assessment of their impact on app's security and guidelines on how to effectively eradicate these vulnerabilities.

8.8 Security tests

8.8.1 Penetration tests

This service consists in an attempt to gain unauthorized access to the client's given IT system in order to practically assess the current state of security, especially in terms of presence of known vulnerabilities and resistance to hacking attempts.

This kind of test makes it possible for the client to become familiar with thresholds at which the elements tested cease working properly, and the procedure ends with a report of the actions taken and recommendations the CERT Orange Polska team concerning changes in infrastructure and suggested security measures.

The analysis is conducted from the viewpoint of a potential hacker, so it can include active exploitation of vulnerabilities (e.g. by using exploits). As opposed to security audit services, penetration tests don't have to be conducted according to formalized methodology, the formulation of which would be difficult due to dynamically changing state of knowledge (e.g. new exploits). The methodology of the test is based upon the experience of Orange Polska. Our evaluators possess certificates confirming their competence and ethics: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker). The penetration tests conducted by Orange Polska provide the client with objective and independent evaluation of the factual state of security of his systems. The offer includes blackbox infrasctrucure and web application tests.

8.8.2 Performance tests (DDoS as a Service)

This service consists in launching a controlled volumetric attack (D)DoS on IT systems designated by the client (connection, servers, websites, network interface controller) in order to practically assess the current state of security, especially in terms of bandwidth saturation attempts.

The analysis conducted from the viewpoint of potential hacker uses the infrastructure of and traffic generators from Spirent Communications Company. It is possible to choose between a couple dozen test scenarios of volumetric attacks of different levels and vectors of the attack. This kind of test makes it possible for the client to become familiar with thresholds at which the elements tested cease working properly, and the procedure ends with a report of the actions taken and recommendations the CERT Orange Polska team concerning changes in infrastructure and suggested security measures.

8.9 Protection from malicious software (Malware Protection InLine)

This service offers protection of the client's network resources through prevention and detection malware infections that could spread from the Internet. The client's traffic at his Internet interface is monitored and analysed for the presence of malicious code in files transferred (not just executable ones) and scripts.

The oncoming malware is detected with use of various detection techniques connected with a detailed attack analysis. The suspicious flow is reconstructed in virtual machines conducting detailed analyses of the malware's activity in an environment simulating real working stations. The process is based on the analysis of code activity in a non-signature manner, which allows including malware that was not classified before and as well as code using complex mechanisms for concealing their activity. Due to the nature of such attacks, there is no information on them available beforehand that could be used in processes like correlation and determining reputation.

The outgoing traffic is analysed for unauthorized connections of malicious software with C&C servers. This allows confirming the presence of an infection in the client's network before the implementation of a service which makes it possible to detect infections spread with the use of non-network attack vectors (e.g. infection through USB port by pen drive read-out). The requirement necessary for using this service is having an Internet connection from Orange Polska in the MetroEthernet technology.

8.9.1 Malicious software analysis

The analysis of the malware sent from a client to CERT Orange Polska. If the suspected file might act as a threat to the client's IT security, the team runs it in virtual sandbox environment. The suspected file is then being analysed alongside with gathering information on all of its actions, including the determination of the IP addresses of Command&Control botnet servers, analysing the malware malicious activity in the system as well as analysing propagation tactics. On the basis of the conducted research, the team creates a report which is useful for blocking malicious activity coming out from the client's network.

8.10 Secure DNS

Geographical dispersion of client's servers responding to DNS questions. Such questions are usually directed to the nearest (in the network sense) server. Orange Polska uses the "anycast" technology, well know solution that has been in use in the Internet for years now.
World-known networks operate within this technology, and they serve domains such as .com or .pl.

SecureDNS contains more than 40 nodes located in the Orange network as well as in other networks in Polska and worldwide.

The main benefit of SecureDNS is pulling away attacks on DNS from our own infrastructure.
Each of the DDoS attacks is being dispersed throughout the world, which means that there won't appear spots with a high traffic concentration. A potential weak spot in the Client's network is then being eradicated. It ensures the high level of reliability and efficiency. Failure of one of the DNS nodes does not affect the operation of the other. The requests are directed to the other nods automatically and the infrastructure will address them if either one nod (from over 50) is still operational.
The answers from the nearest nod will come out as soon as is possible, through the shortest route, without the delays.

We offer also a full outsourcing of the Client's DNS service which bases on our SecureDNS infrastructure.

9 CERT Orange Polska - team presentation

CERT Orange Polska (Computer Emergency Response Team Orange Polska) is a special unit within Orange Polska, responsible for the safety of Internet users receiving servicers from this network operator.

CERT Orange Polska monitors security threats within systems connected with the Orange Polska network, ie. in the range of autonomous systems[3]: AS5617, AS29535, AS33900, AS43447, AS12743 - RIPE NCC). This addressing is a constituency of CERT Orange Polska, within which it reacts to the detected threats, especially to the incidents reported by the network's users.

The main tasks of this team include:

- Taking the necessary measures in situations involving cyber-security threats.
- Aiding the Internet Society of Orange Polska in introducing proactive means of reducing the risk of the of IT security threats, especially through informing and warning the users of the possibility of emergence of threats that can directly affect them (e.g. about the detected vulnerabilities, IT threats) and available means of averting them,
- Aiding the Internet Society of Orange Polska, as well as all the Internet users in Poland, in responding to incidents that has already occurred (or are ongoing). Especially through informing and warning the users of the possibility of emergence of threats that can directly affect them, e.g. an ongoing attack originating from the user's computer or available means containing this threat and reducing the damage that could result from it.

CERT Orange Polska is the main helpdesk for the users of Orange Polska network when it comes to reacting to incidents that could pose a threat to their IT systems, while simultaneously being the only trusted point of contact for other net users involved in dealing with the incidents that are being addressed.

[3] https://en.wikipedia.org/wiki/Autonomous_system

9.1 Organizational structure

Structurally, CERT Orange Polska is located within the Orange Polska, in the area of Technology (IT Infrastructure and Cybersecurity).

In the Orange Group, in addition to the autonomous action of individual CERT-type security teams in different countries, there is also the Orange-CERT-CC, which, if necessary, can coordinate the work of all security units of the entire Orange Group.

The organizational structure of the team is layered and consists of three main lines of support. This sort of multi-level approach to organizing the reaction team allows optimal utilization of competencies and technological resources.

The first line of support are operators of CERT Orange Polska who work 24/7/365, monitoring the level of user security in our network, accepting reports, analyzing events and reacting to identified security incidents and taking up measures to minimize threats.

The second and third lines of support are the teams of analysts and experts. They support the daily work of the operative line in case of occurrence of more complex events, not included in procedures of reacting to standard incidents. They are also responsible for conducting threat analyses, optimizing the process of dealing with standard security incidents as well as the development of tools of detection and minimization of threats.

Operating and processing model of CERT Orange Polska

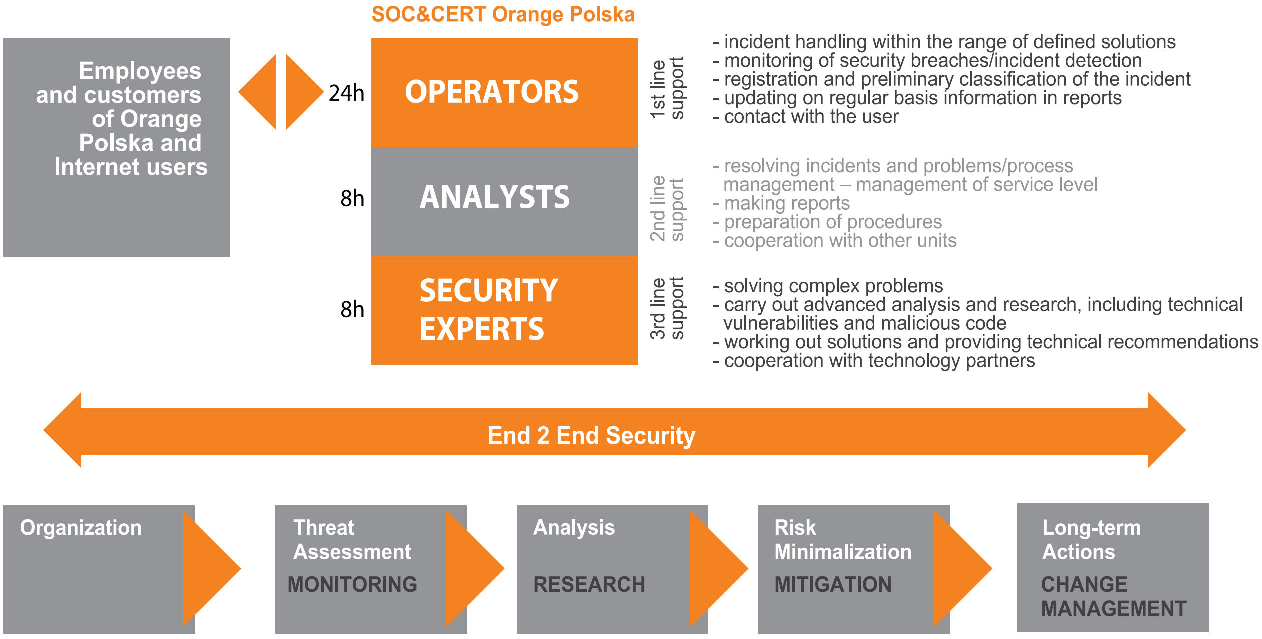

SOC&CERT Orange Polska
Employees and customers of Orange Polska and Internet users
24h
OPERATORS
1st line support
- incident handling within the range of defined solutions
- monitoring of security breaches/incident detection
- registration and preliminary classification of the incident
- updating on regular basis information in reports
- contact with the user
8h
ANALYSTS
2nd line support
- resolving incidents and problems/process management – management of service level
- making reports
- preparation of procedures
- cooperation with other units
8h
SECURITY EXPERTS
3rd line support
- solving complex problems
- carry out advanced analysis and research, including technical vulnerabilities and malicious code
- working out solutions and providing technical recommendations
- cooperation with technology partners
End 2 End Security
Organization
Threat Assessment
MONITORING
Analysis
RESEARCH
Risk Minimalization
MITIGATION
Long-term Actions
CHANGE MANAGEMENT

Figure 13 *Operating and processing model of CERT Orange Polska*

9.2 Team history

The first specialized unit, responsible solely for IT security incident management was created within the company structure as early as 1997. In the year 2006 – we became the third unit in Poland and currently the only telecommunications operator to hold the right to use the CERT (Computer Emergency Response Team) name.

The name is awarded by the Carnegie Mellon University (the operator of CERT Coordination Center), exclusively to the teams meeting high standards for management of IT security incidents. Currently, we are also the only CERT-type unit in Poland certified by the Trusted Introducer (www.trusted-introducer.org) organization.

9.3 Domestic and international cooperation

9.3.1 Trusted Introducer

In terms of domestic and international cooperation the last year was marked by the promotion of CERT Orange Polska as a part of the European Trusted Introducer initiative. Trusted Introducer is an initiative working alongside the biggest organization associating IT threat reaction teams in Europe, GEANT TF-CSIRT.

With 16 of March CERT Orange Polska became the first unit with the „Trusted Introducer Certified Team" status in the country and one of the merely sixteen such units across Europe. It is the result of a several-months process of certification confirming, among others the fact of meeting the standards of Mature Model of Security Incident Management and achieving the required high level in every of several dozen parameters being verified.

The chart above shows the evaluation of each parameters in four categories: Organization (O), Human (H), Tools (T), Processes (P).

- 0 – not available/undefined/unaware,
- 1 – implicit (known/considered but not written down),
- 2 – explicit, internal (written down but not formalized),
- 3 – explicit, formalized on authority of CSIRT head,
- 4 – explicit, audited on authority of governance levels above the CSIRT head.

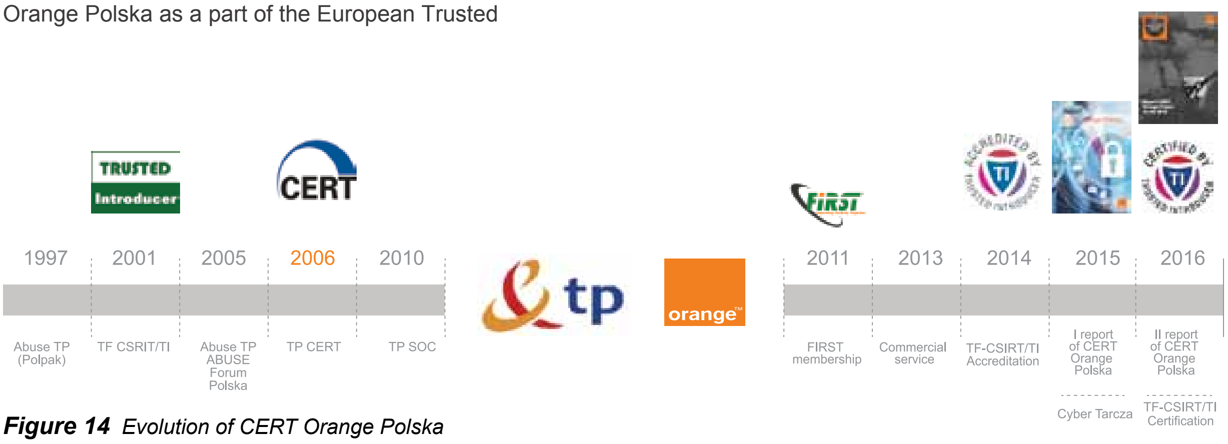


Figure 14 *Evolution of CERT Orange Polska*

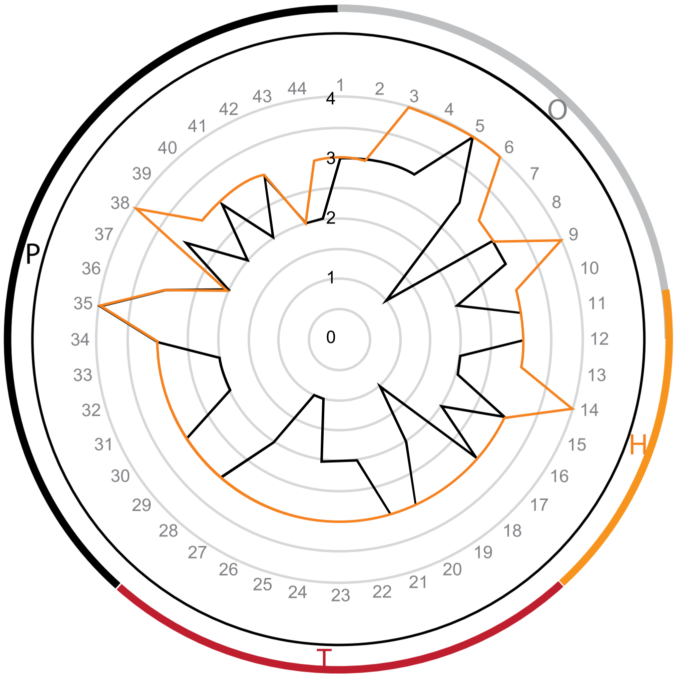


***Figure 15** Evaluation of quality parameters of CERT Orange Polska within certification of Trusted Introducer*

All parameters relate to the basic principles of operation, owned resources, technical preparation and organization of the team and implementation of key processes. The parameters represent a responsive team level of maturity in the area of incident management. This model is treated by the international environment of CSIRTs as a reference model for development. It is used in the certification process of Trusted Introducer.

9.3.2 FIRST

CERT Orange Polska takes part in operations of the biggest organization associating IT threat reaction teams like CERT – FIRST worldwide (Forum of Incident Response and Security). Membership in this kind of organizations is, above all the organizational and operative support for providing high quality services. It directly affects the efficiency of threat minimization, the security of the Orange Polska network, affecting the continuity of the services being delivered and functioning of the business as well as improves the effectiveness of delivering commercial services. It does not only mean prestige, but above all, access to knowledge and good practices.

9.3.3 National Cybersecurity Centre

In 2016 a cooperation of domestic cyber-security units has begun units (from both private and public sector) has begun as a part of the National Cybersecurity Centre (NC Cyber). It is one of the effects of introducing the NIS directive - the directve of the Parliament and European Council concerning resources for high level of common security of networks and IT systems on the UE territory). The NIS directive assumes the extension in cooperation of the member countries concerning cyber-security, and defines responsibilities of key services operators as well as digital services providers in the same field. Every EU country is obliged to appoint bodies for overseeing IT security and for working out appropriate strategy.

9.3.4 The NATO Summit and the World Youth Day

The agreement established in July of the year 2016 between The Ministry of Digital Affairs, NASK and Orange Polska allowed to enhance the cooperation with organs of public administration, consisting in informing one another and securing Poland's cyberspace from large-scale attacks, such as phishing attacks, malware attacks or the threat of DDoS attacks aiming to paralyze IT networks in Poland.

The CERT Orange Polska protected against, among others: DDoS attacks aimed at infrastructure supporting the NATO Summit as well as the one supporting PAP and KAI, during the World Youth Day.

9.3.5 Abuse Forum

As a part of domestic cooperation CERT Orange Polska also takes part in Abuse Forum operations – an unofficial organization, bringing together representatives of the largest Polish IT operators, internet providers, social media, banks and other organizations working towards better cyber-security, as well as public administration organs, including ministries and central offices. Recurring meetings and mailing list serve to improve communication and enhancing cooperation, so that we can be even more efficient in preventing and reacting to threats emerging in the web. Apart from working on an ongoing basis, we also cooperate with similar units from different subjects, especially in case of detecting a threat that can affect them (i. a. malware infected invoices received by the customers of Orange Polska).

9.4 Achievements and projects

9.4.1 Cyber Europe 2016

CERT Orange Polska took part and earned the sixth place (out of 114 teams) in Cyber Europe 2016 exercises conducted by ENISA (The European Union Agency for Network and Information Security). The Polish section of the exercises was coordinated by the Ministry of Digital Affairs.

The CyberEurope exercises are organized every two years and that are the biggest civilian cyber-security exercises organized in Europe. This year, it was the fourth edition that took place. The organizers launched i.a. the exercise platform on which tasks aiming to assess the introduced procedures and team were published since April 2016. Over the course of six months of exercises, 114 teams completed 12 tasks. It was the first time for CERT Orange Polska to take part in an international enterprise of such scale. It was an opportunity to test the technical and organizational capabilities as well as the cooperation with teams from other countries and the relations with other entities in Poland.

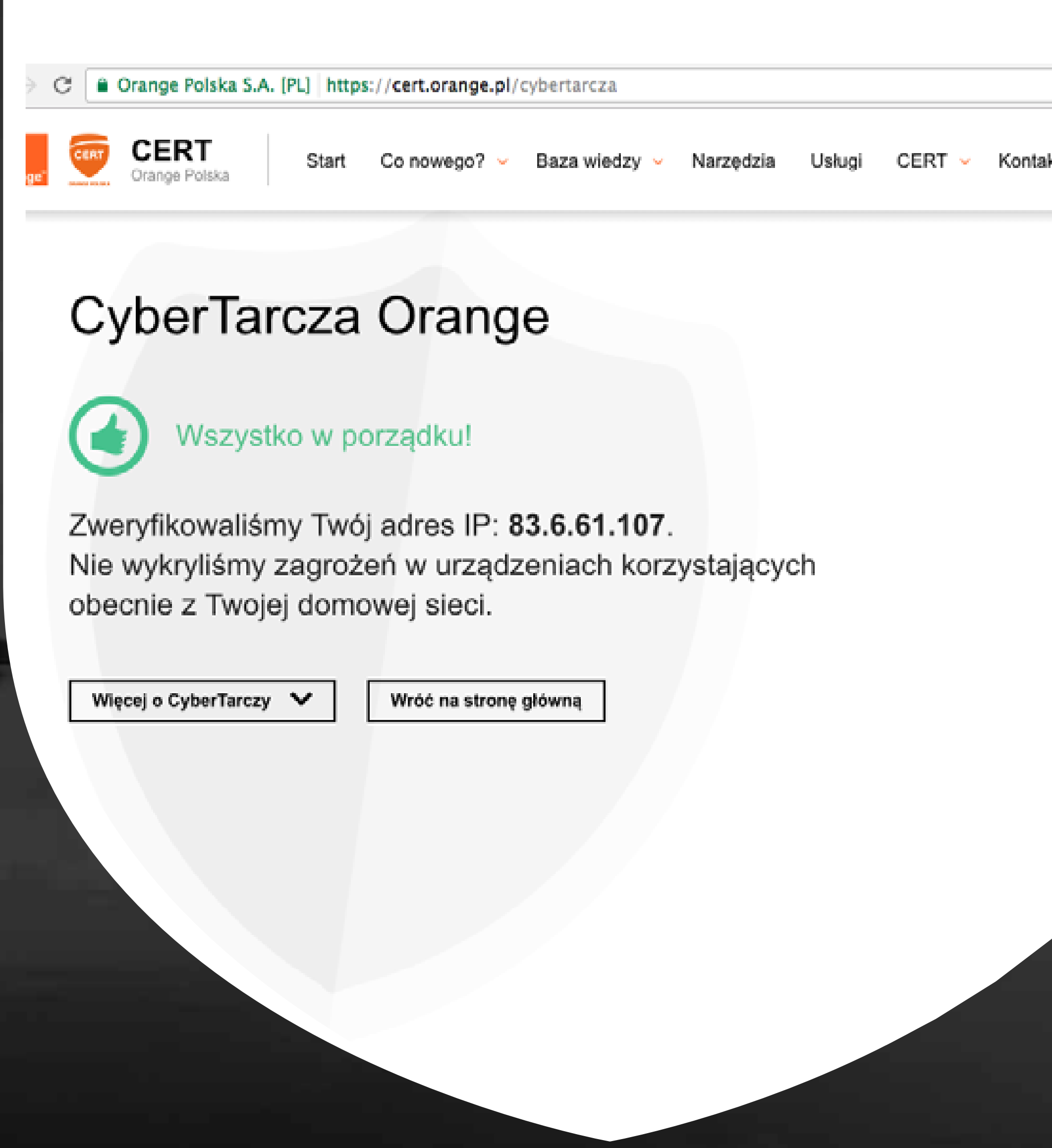
9.4.2 CyberShield

Novelties, especially the most innovative ones, and above all in the field of IT security, are usually welcomed with a great deal of scepticism. It was likewise throughout the first few months of introducing the CyberShield, for which year 2016 was the first full year of functioning.

For the clients of Neostrada, CyberShield is a webpage which pops up automatically in the event of infection with exceptionally malicious software, or in other situations – like information about the status of home network security. However, there is much more behind what we see on the screen.

The first step is identification of the malware. Not just every kind of malware, as this still falls upon the antivirus software – the CyberShield takes care of new strains of malware causing a great deal of trouble for most antivirus programs or ones impossible to detect by them at all. In its essence, the CyberShield is not meant to replace other security measures, but to compliment them and due to that minimize the risk of a successful attack on our home network. This is why the CyberShield – as the only solution of this kind – can also inform the users about systemic or software-related vulnerabilities in their home network.

After identifying the activity of a malicious code or vulnerability is thoroughly analysed, not only to acquire information on the threats connected with the infection, but also to block the communication between the infected device and the cybercriminal commanding it remotely. Thanks to that the user of Orange Polska network, stays relatively safe despite the infection.

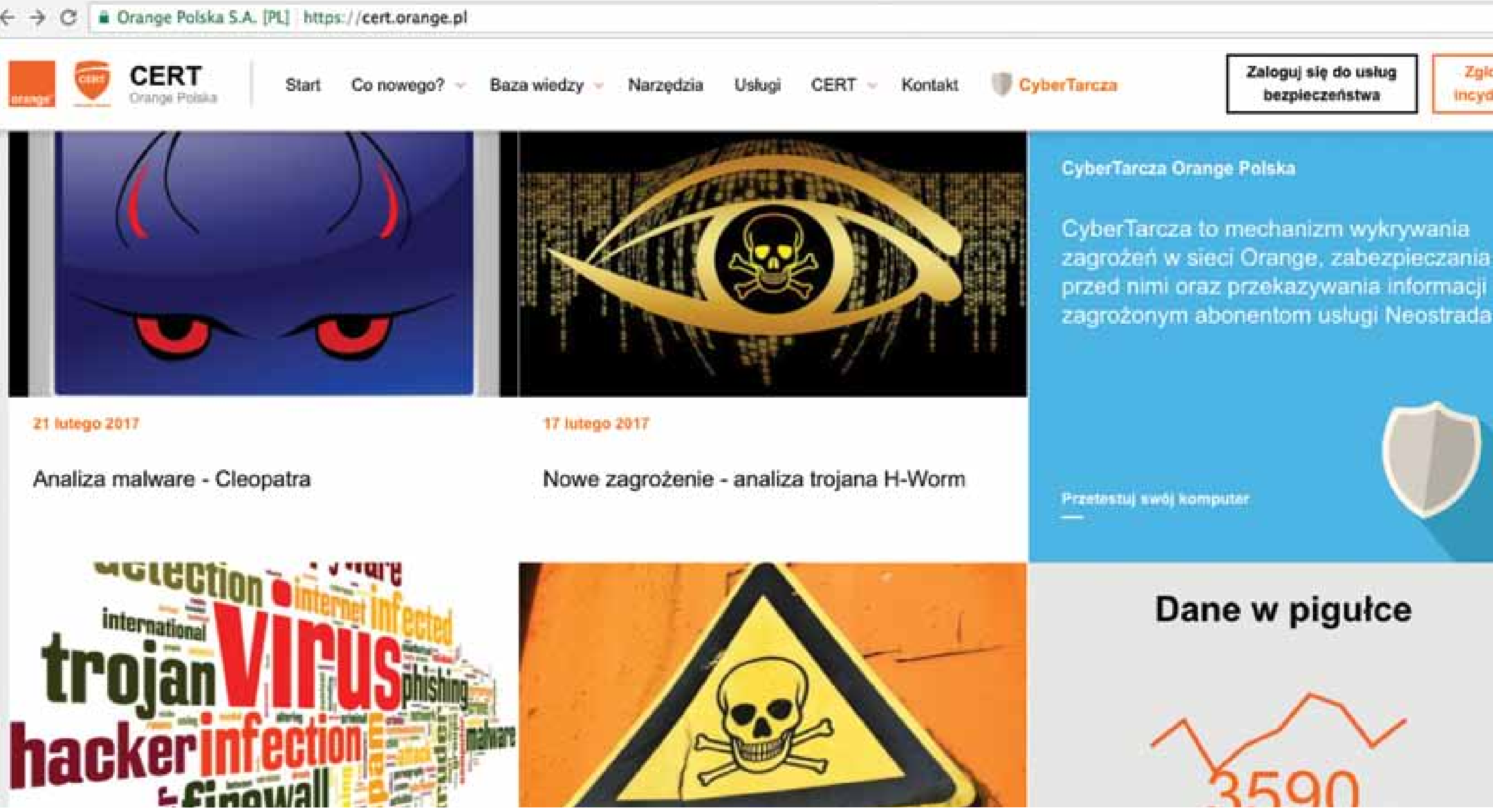


CyberTarcza Orange

Wszystko w porządku!

Zweryfikowaliśmy Twój adres IP: **83.6.61.107**.
Nie wykryliśmy zagrożeń w urządzeniach korzystających obecnie z Twojej domowej sieci.

Next, the information about the activity of the code analysed, along with a detailed instruction is passed to the CyberShield, and the system, after finding the movement pattern characteristic for the given malware passes the information directly to the victim's web browser or allows them to become familiar with the threats by accessing this site: https://cert.orange.pl/CyberShield Currently, CyberShield services over 2 million clients using the Neostrada service, as well as – in the reactive version, which requires accessing the website – Internet DSL and Business Package services. As much as in the first months one of the most popular Google searches concerning the CyberShield was: „CyberShield – how to disable?", in the year 2016 out of almost half million users noticed about the threats only 0,05% decided to resign from the protection. The several dozen of threats from which the CyberShield is meant to protect seems to be a drop in the ocean as compared to the diversity of viruses; but on the other hand, – this kind of protection includes the kind of malware that is not yet detectable by common antivirus software. The effect turns out to be an actual increase in security and a "cleaner" Orange Polska network. It works this way because the CyberShield allows removal of threats that could possibly spread on a large scale and create a threat for multiple network users. CERT Orange Polska is aware that the mobile network becomes an enormous source of threats nowadays, and because of this works are underway to extend the CyberShield to the users of mobile network users. Of course, in both cases we are discussing a completely free service. We are convinced that it is an ideal project when it comes to receiving mutual benefits by both the users and the IT operator.



21 lutego 2017

Analiza malware - Cleopatra

17 lutego 2017

Nowe zagrożenie - analiza trojana H-Worm

CyberTarcza Orange Polska

CyberTarcza to mechanizm wykrywania zagrożeń w sieci Orange, zabezpieczania przed nimi oraz przekazywania informacji zagrożonym abonentom usługi Neostrada

Przetestuj swój komputer

Dane w pigułce

> CERT Orange Polska is aware that the mobile network becomes an enormous source of threats nowadays, and because of this works are underway to extend the CyberShield to the users of mobile network users.

9.4.3 Parental control - „Secure Starter" and „Protect Children in the Web"

The Internet is not just a vast fount of knowledge and interesting information – it's also dangerous content which an adult can handle, but a child or a teenager may not. This is where the necessity to develop the field in cybersecurity that for a long time had remained unacknowledged – the parental control services.

Introduced in September 2014 „Secure Starter" was an innovative service on a European scale, allowing the activation of basic parental control by simply installing a dedicated SIM card and conducting the entire network filtering process exclusively on the operator network's level. No necessity to configure turned out to be a blessing not only for the parents, who may not be familiar with new technologies, but also for those who do not like spending time on complex configuration. The media, which received the new service very positively, highlighted the lack of the necessity for configuration. That last part, alongside automatic blockage of websites containing pornography, children pornography or graphic – does not present any problem. The interesting part is that the service created as parental control turned out to be quite effective as... an antivirus solution. Most of the sites blocked since the beginning of the existence of the „Secure Starter" are websites classified as „malware". Distribution of illegal content is very often accompanied by distribution of malicious software.

In September 2016 a paid service „Protect Children in the Web" has been activated, this time based exclusively on an application. The next step will be merging the features of both services, creating a hybrid parental control, combining advantages of both methods of filtering, also available for free in its basic version. Installation of any application will not be necessary for it to function, which will allow launching a fully functional service on mobile phones not functioning under control of the most popular operating systems (Android, iOS, Windows Mobile), or resignation in case of devices with lower efficiency. Configuration of the service will be possible through a website, and the fact of using parental control will be recognized with the use of the SIM card's MSISDN number. Thanks to that it will not be possible to uninstall the service by uninstalling the application, so that bypassing the filters by the child will become much more difficult.

9.4.4 CERT Orange Polska Blog

Terms like phishing, malware, ransomware, spam, botnet, or DDoS – are daily bread for cyber-security experts, but in the sum of people most frequently exposed to such threats we will not find many of them. The question is, does a regular Internet user understand what are we writing to him about, when we want to tell him about the threats of using the Internet?

Basing upon the analysis of e-mails which Internet users write to CERT Orange Polska as well as upon a brief analysis of a number of internet comments it is possible to quite accurately conclude that a regular Internet user does not even read the content of e-mails he receives. The result is endless list of cybercrime victims, ending up e.g. with their bank accounts cleared.

> **The IT incident reaction team of Orange Polska protected against, among others: DDoS attacks aimed at infrastructure supporting the NATO Summit as well as the one supporting PAP and KAI during the World Youth Day.**

This is why CERT Orange Polska tries to get to the users with substantial and messages, we do believe, has a chance to breach its way into their consciousness and protect them against various threats. The main source of education is CERT Orange Polska website (https://cert.orange.pl/) and the operator's blog (https://blog.orange.pl/). The first site gathers basic topics concerning security - i.a. how to secure a computer, how to deal with malicious software, how to create a strong password. It also recommends free security utilities. The second website focuses on describing threats in the context of real events which took place in Poland and worldwide.

Videos from the (un)Safe Web can be found on Orange Polska's YouTube account, presenting issues concerning security (such as strong passwords, phishing, social engineering) as well as ways of dealing with threats.

9.4.5 Conferences attended by the CERT Orange Polska

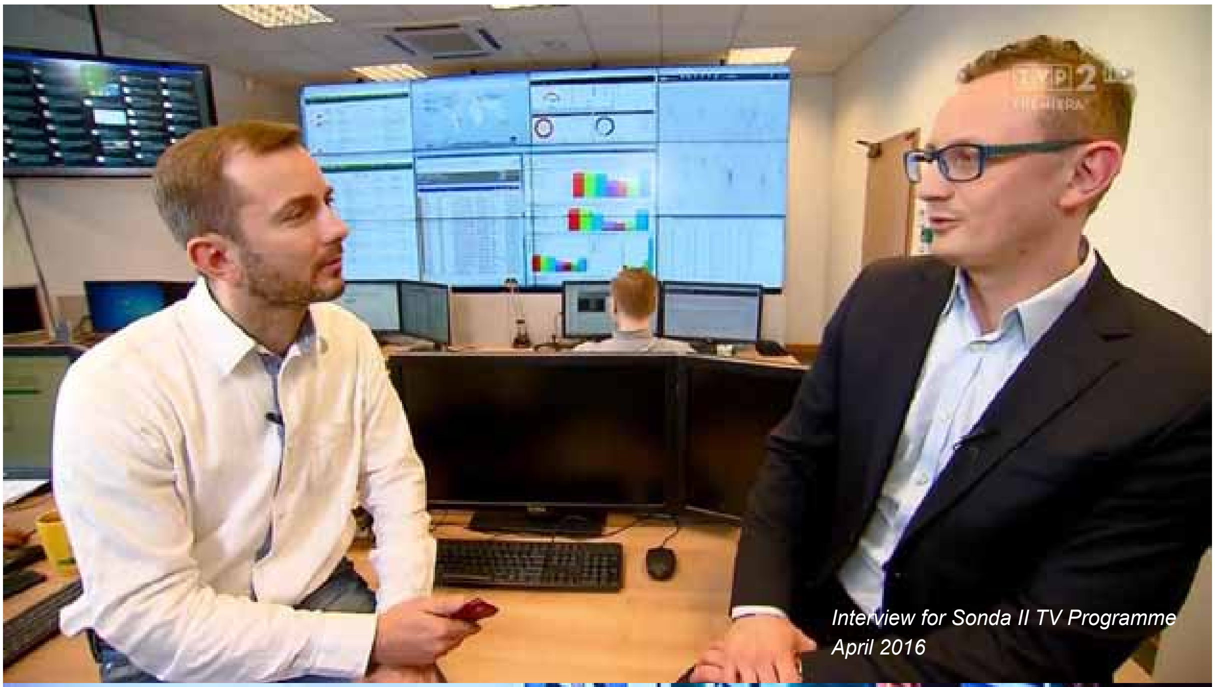
- *Polish Network Operators Group Meeting*
- *Mobile Security Center Seminar*
- *Open Source Day*
- *Federated Conference on Computer Science and Information Systems*

- 10th International Conference „Security of children and youth in the Internet”
- Security Case Study – IT Securty Conference
- Polish Network Operators Group jesień
- Advanced Threat Summit
- Interview for Sonda II TV Programme – April 2016 http://blog.orange.pl/korporacyjny/entry/o-sieci-telekomunikacyjnej-i-bezpieczenstwie-w-programie-sonda-2/
- Presentation of the „CyberShield” project at TF-CSIRT/TI meetings – Zurich, 20th-21st September 2016 https://tf-csirt.org/tf-csirt/meetings/49th-meeting-zurich-switzerland/
- Co-organization and and attendence at Telecom Security Forum – November 2016

TelSec (Telecom Security Forum), November 2016

Polish Network Operators Group Meeting March 2016

Security Case Study Conference September 2016



Interview for Sonda II TV Programme
April 2016

Polish Network Operators Group Meeting
March 2016

9.5 Computer incident response procedure

Computer security incident response relies on strictly defined processes and procedures. Here we present the basic scheme describing the most important steps.

Process of the incident management consists of:

1. Reporting and verifying the incident;
2. Initial assessment of the outcomes (triage);
3. Assigning the incident to the expert;
4. Handling the incident;
5. Closing the incident.

Reported incident has two main sources: the user (abnormally functioning hardware, service, application, etc.) or the real-time analysis systems (IPS, IDS, SIEM) alerts on abnormal traffic in the network.

The team verifies the computer incident in the three aspects:

- Whether the reported incident can be actually classified as a computer security incident;
- Whether the reported incident concerns the area of CERT Orange Polska team expertise (if it is related to its constituency);
- Whether the reported incident doesn't concern already registered computer security incident;

The next stage is initial classifying of the incident and assessment of its impact on the computer system. Then, the appropriate priority is assigned to the incident.

Given priority depends on several variables:

- Type of the incident (see section XX of this report);
- Its impact on Client's business processes;
- Type of data, which security is threatened by the incident;
- Possibilities of computer system recovery;

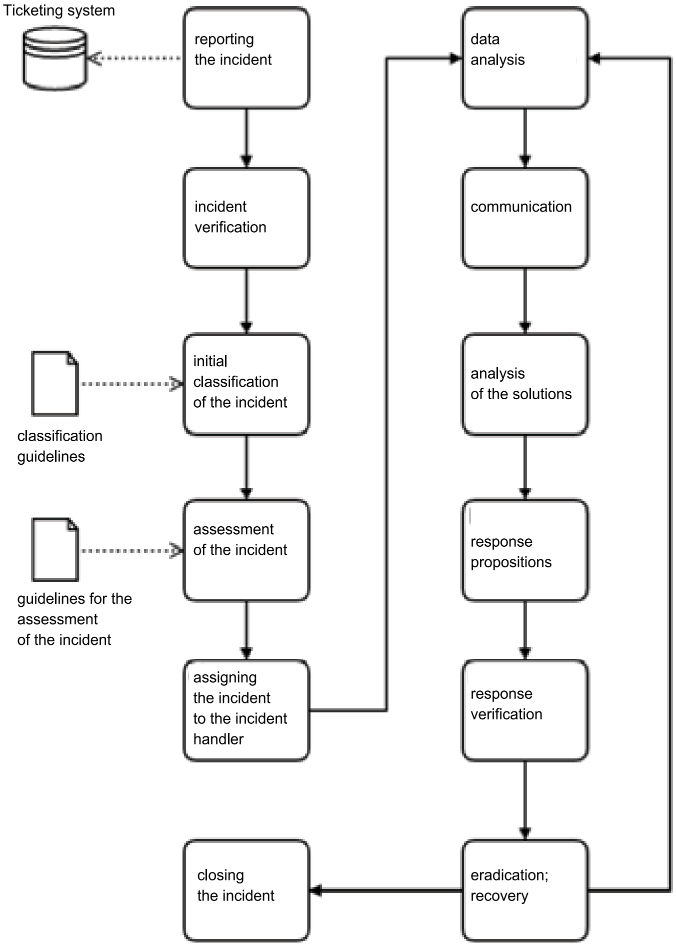

Ticketing system
reporting the incident
incident verification
classification guidelines
initial classification of the incident
guidelines for the assessment of the incident
assessment of the incident
assigning the incident to the incident handler
closing the incident
data analysis
communication
analysis of the solutions
response propositions
response verification
eradication; recovery

Figure 16 *Basic activities in the computer incident response process handled by CERT Orange Polska*

- Type of the Client (resulting from the SLA agreement);
- Type of the entity that reports the incident (individual user, media news, commercial client, government administration etc.)

Assigning the appropriate priority is very important, especially when massive and sophisticated attacks are occurring. It is a key to choose the best response strategy

Each of the incidents should be assigned to the incident handler, who operates according to the process shown below:

All of the steps have to be executed in several cycles, in which successive goals should be:

1. Reducing the impact of the incident (isolation of the network segments and working stations, redirecting the traffic, securing the evidence);
2. Mitigation of the impact (eradication the source, system recovering);
3. Restoration of the production services (and verification correctness of their operations).

The last stage, often underestimated, is a proper closing of the incident, which stands for carrying out a post-incident review and updating an information on the incident, in particular: when and by whom the incident has been noticed, what was the scope of the incident, what measures have been taken to reduce the impact of the incident, which strategy has been chosen and what was done to restore the production services.

The procedure presented above remains general for all of the incidents. Types of the incidents vary in measures taken to handle them, so that a good practice should be creating guidelines for each one.

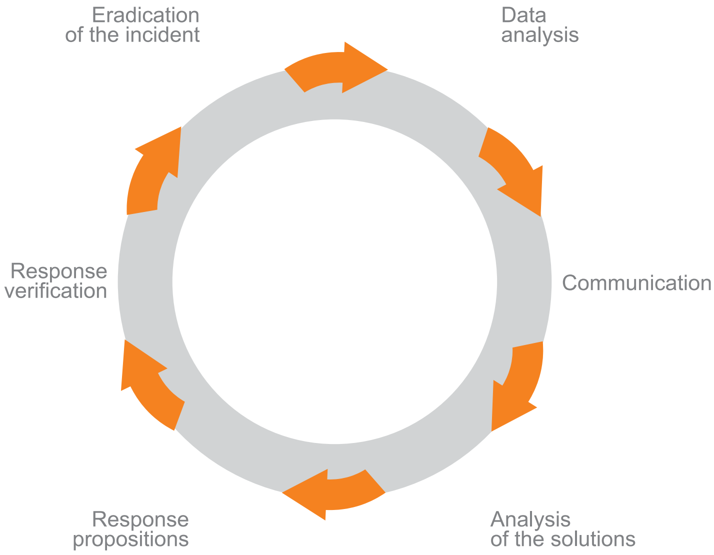


Figure 17 *Process of the basic computer incident response in CERT Orange team*

9.5.1 Incident Handling Guide – DDoS[4] example

DDoS (Distributed Denial of Service) is often executed by flooding the computer system with superfluous requests in an attempt to overload the system.
Without a special equipment or support from an Internet service provider (ISP) preventing the DDoS attack is very difficult. The crucial step is to understand the equipment being used. Typically, admins either underestimate or overvalue capabilities of their resources.
It is best to assume that our resources will eventually be attacked, so that a part of the tasks has to be done in an advance. Actions worth undertaking are:

[4] *proposed set can be used to organize response strategy for DDoS attack, also in cooperation with CERT Orange Polska*

DDoS (Distributed Denial of Service) is often executed by flooding the computer system with superfluous requests in an attempt to overload the system. Without a special equipment or support from an Internet service provider (ISP) preventing the DDoS attack is very difficult. The crucial step is to understand the equipment being used. Typically, admins either underestimate or overvalue capabilities of their resources.

1. Contact the Internet service provider in order to learn about the DDoS attack support, and the procedure of applying for such a support;
2. Develop a “white list” of IP addresses and protocols, which under the circumstance of an attack should be taken care of in the first place (important clients, crucial stakeholders);
3. Check the time-to-live (TTL) parameter for DNS settings in regard to systems which might be attacked. Lower the TTL, if necessary, in order to redirect the DNS;
4. Contact the ISP, law enforcement agencies and administration teams responsible for intrusion detection, firewalls etc.
5. Check the documentation of the IT infrastructure: business owners, IP addressing; create the network topology mapper and the list of resources;
6. Estimate potential losses in the event of a DDoS attack;
7. Prepare continuity plans and emergency plans;
8. Check the network configuration, operating systems and applications which might be the targets;
9. Elaborating the IT infrastructure performance under the normal mode (eases detection of anomalies); Prepare the operation characteristics of the IT infrastructure in a normal mode (this facilitates anomalies discoveries).

If an attack occurs, the first phase contains actions which concentrate on the analysis:

1. Understand the data flow;
2. Identify the targeted infrastructure;
3. Analyse the following event logs: servers, routers, firewalls, applications and other IT resources which might be targets;
4. Determine which aspects differentiate traffic tied with the attack and normal traffic (IP addresses, ports, TCP flags);
5. Initiate the traffic analysing software (tcpdump, ntop, NetFlow, etc.).

After analysing the attack and determining its nature it is necessary to mitigate its impact on the system by:

1. Reducing the traffic tied to the attack as close as possible to the the external network border points (routers, firewalls, load balancers, etc.);
2. Closing the unwanted processes on the servers and routers and TCP/IP protocols configuration;
3. Switching to the alternative networks and blackholing the traffic;
4. Increasing the capacity of the network;
5. Passing the traffic through the service or device that protects from DDoS attacks;
6. Configuring the filters, so that they can block the packets generated by the requests responding system.

10 Methodology

10.1 The telemetric base of CERT Orange Polska

10.1.1 Basic kinds of data

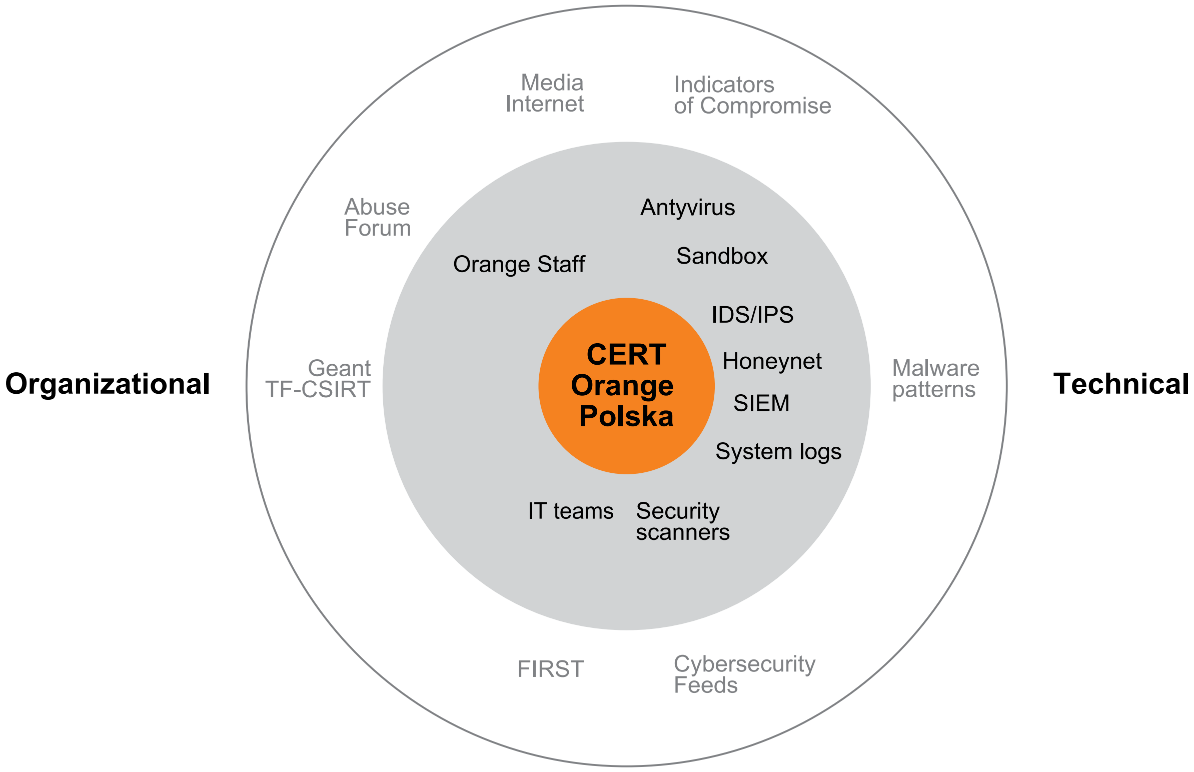
Below, the basic terms connected with the data presented in this report are described. They introduce the two fundamental ideas – event and incident.

Event – an activity in the system resulting from actions taken by user, application, service, etc. An event causes a signal to be generated in the security monitoring system, which should undergo automatic or manual analysis. An event may become an incident.

Incidents – are all the emerging events compromising IT security, which means all actions that violate the established security rules and which result in a treat. Examples of such security-breaching actions are presented in the incident classification section.

The relation between an event and an incident is meant to be understood in a way that an event may transform into an incident, which thus requires to be handled. A reverse situation should not take place, with a reservation that in case of doubts whether we are dealing with an event or an incident, the case should be resolved in favor of incident.

Sources of information about cybersecurity threats



10.1.2 Telemetric architecture

In this report, cases are described that were concern of, and were handled by Orange CERT Polska. The cases included in the report regarded both situations in which an attack was launched on resources connected with the Orange Polska network, and in which IT attacks were launched with the use of this network. They included all kinds of networks from the viewpoint of the end user, which here means both private users and corporate subjects.
The sources of data concerning the incidents originated from both internal and external systems. The following sources have fallen under the „external" category:

- The media
- Organizations dealing with IT security
- Users and administrators
- Manufacturers, hardware and software dealers
- Service and network content providers (ISP/ICP)
- other CERTs

The sources listed below, on the other hand are the internal ones, used in completing this report and simultaneously they make up an extensive telemetric base belonging to CERT Orange Polska . Along with the external sources they sum into a vast database, allowing creating the most detailed picture of IT security of the Orange Polska network.

The telemetric base of CERT Orange Polska consists of the following elements:

- Honeypots – systems imitating actual IT systems while in fact being a trap allowing analysing cybercriminal activity.
- SIEM (Security Information and Event Management) – a tool of processing events and detecting incidents
- Monitored systems and networks
- Logs, flows (information on the network packages sent), registries – source information from IT hardware in the Orange Polska network
- Systems of the Intrusion Detection System class
- Systems of the Intrusion Prevention System calss
- Systems of the firewall class
- AWntiviurs software
- Anti-spam systems
- Systems of the Sandbox class

10.2 Incident classification

In this report, a new incident classification has been used. Partially, it concurs with the one used in previous reports. The change is a result of an endeavour of international CERT-type reaction teams as well as organizations collaborating with them (e.g. ENISA or Europol) to come up with a common classification. The most advanced result of these works is the classification presented in the publication „Common Taxonomy for the National Network of CSIRTs[5]" .

In the previous reports CERT Orange Polska used the classification based on eCSIRT.net project (http://www.ecsirt.net/cec/service/documents/wp4-pub-userguide-v10.html) including the changes applied by Europol (https://www.europol.europa.eu/publications-documents/common-taxonomy-for-national-network-of-csirts) as classification for the domestic CSIRTs. The classification does not differ much from the one proposed in the current report, which allows continuation of the analyses of the trends observed.

The classification used includes all types of events reported

[5] *https://www.europol.europa.eu/publications-documents/common-taxonomy-for-national-network-of-csirts*

Incident class	Incident type	Incident description
Malware	Infection	Infecting one or various systems with a specific type of malware.
	Distribution	
	C&C hosting	
	Undetermined	
Availability	DoS/DDoS	Disruption of the processing and response capacity of systems and networks in order to render them inoperative.
	Sabotage	Premeditated action to damage a system, interrupt a process, change or delete information, etc.
Gathering of information	Scanning	Active and passive gathering of information on systems or networks.
	Sniffing	Unauthorised monitoring and reading of network traffic.
	Phishing	Attempt to gather information on a user or a system through phishing methods.
Intrusion attempt	Exploitation of vulnerability	Attempt to intrude by exploiting a vulnerability in a system, component or network.
	Login attempt	Actual intrusion by exploiting a vulnerability in the system, component or network.
Intrusion	Exploitation of vulnerability	Actual intrusion by exploiting a vulnerability in the system, component or network.
	Compromising an account	Actual intrusion in a system, component or network by compromising a user or administrator account.
Information Security	Unauthorised access	Unauthorised access to a particular set of information
	Unauthorised modification/deletion	Unauthorised change or elimination of a particular set of information
Fraud	Misuse or unauthorised use of resources	Use of institutional resources for purposes other than those intended.
	Illegitimate use of the name of a third party	Use of the name of an institution without permission to do so.
Abusive content	SPAM	Sending SPAM messages.
	Copyright	Distribution and sharing of copyright protected content.
	Child pornography, racism and apology of violence	Dissemination of content forbidden by law.
Other	Other	Other

Table 1 Incident classification used by CERT Orange Polska

and handled by the CSIRT/CERT-type teams. The categories are based upon the type and effect of the activities violating IT security, connected with the process of an attack on an IT system and its use. This kind of division is useful mainly in terms of operational activities and the goal achieved through them. In practice, many methods and techniques leading to achieving a certain goal were used in the incidents analysed, mostly related to the use of malicious software.

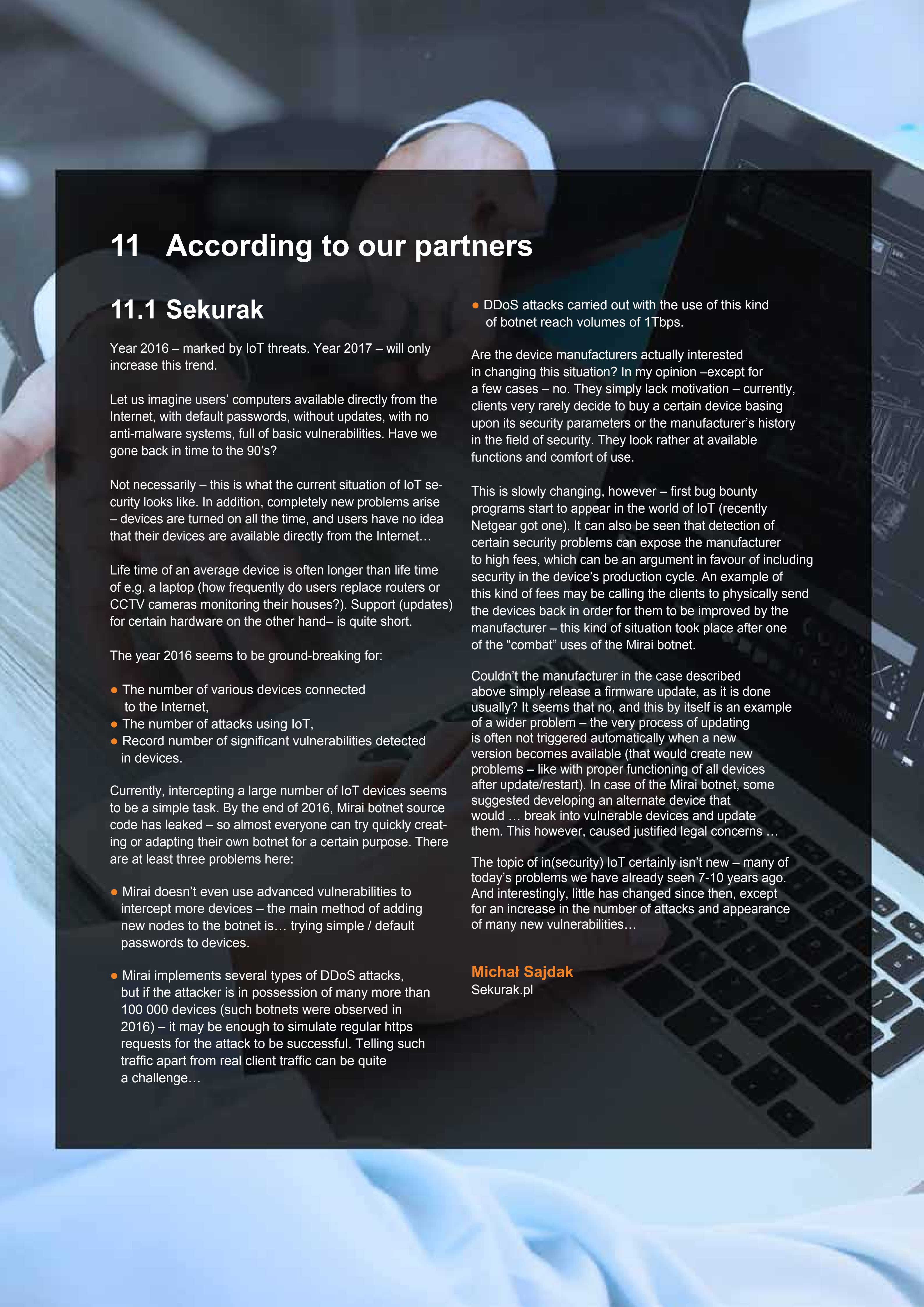
Below, the classification used is presented in detail. It may be used for two purposes:

- Familiarizing oneself with the classification approved by the CERT Orange Polska, in order to better understand what kind of incidents happen in the network protected by the team
- Understanding the classification to use it for one's own goals, (which may be particularly useful for other reaction teams) and aim for unification, understanding and classification of incidents by Polish reaction teams.

The CERT Orange Polska team, operating actively in favour of cyber-security in Poland, is deeply interested in promoting the classification described, and it declares

Incident type	Event type	Event description
Infection	Malware infection	The presence of any of the types of malware was detected in a system.
Distribution	Malware dissemination	Malware attached to a message or email message containing link to malicious URL.
C&C hosting	C&C hosting	System used as a command-and-control point by a botnet. Also included in this field are systems serving as a point for gathering information stolen by botnets.
Undetermined	Connection to suspicious system or port (specific malware)	System attempting to gain access to an IP address or URL normally linked to a specific type of malware, e.g. C&C or a distribution page for components linked to a specific botnet.
DoS/DDoS	Exploit or tool aimed at exhausting resources	One single source using specially designed software to affect the normal functioning of a specific service, by exploiting a vulnerability.
	Flood of requests	Mass mailing of requests (network packets, emails, etc...) from one single source to a specific service, aimed at affecting its normal functioning.
Sabotage	Vandalism	Logical and physical activities which – although they are not aimed at causing damage to information or at preventing its transmission among systems – have this effect.
	Intentional disruption of data transmission and processing mechanisms	Logical and physical activities aimed at causing damage to information or at preventing its transmission among systems.
Scanning	System probe	Single system scan searching for open ports or services using t hese ports for responding.
Sniffing	Network scanning	Scanning a network aimed at identifying systems which are active in the same network.
	DNS zone transfer	Transfer of a specific DNS zone.
	Wiretapping	Logical or physical interception of communications
Phishing	Dissemination of phishing emails	Mass emailing aimed at collecting data for phishing purposes with regard to the victims.
	Hosting of phishing sites	Hosting web sites for phishing purposes.
	Aggregation of information gathered through phishing schemes	Collecting data obtained through phishing attacks on web pages, email accounts, etc.

Incident type	Event type	Event description
	Aggregation of information gathered through phishing schemes	Collecting data obtained through phishing attacks on web pages, email accounts, etc.
Exploitation of vulnerability	Exploit attempt	Unsuccessful use of a tool exploiting a specific vulnerability of the system
	SQL injection attempt	Unsuccessful attempt to manipulate or read the information of a database by using the SQL injection technique.
	XSS attempt	Unsuccessful attempts to perform attacks by using cross-site scripting techniques.
	File inclusion attempt	Unsuccessful attempt to include files in the system under attack by using file inclusion techniques.
Login attempt	Brute force attempt	Unsuccessful login attempt by using sequential credentials for gaining access to the system.
	Password cracking attempt	Attempt to acquire access credentials by breaking the protective cryptographic keys.
	Dictionary attack attempt	Unsuccessful login attempt by using system access credentials previously loaded into a dictionary.
Exploitation of vulnerability	Use of local or remote exploit	Successful use of a tool exploiting a specific vulnerability of the system.
	Atak SQL injection	Manipulation or reading of information contained in a database by using the SQL injection technique.
	Atak XSS	Attacks performed with the use of cross-site scripting techniques.
	Atak File inclusion	Inclusion of files into a system under attack with the use of file inclusion techniques.
	Control system bypass	Unauthorised access to a system or component by bypassing an access control system in place.
Compromising an account	Theft of access credentials	Unauthorised access to a system or component by using stolen access credentials.
Unauthorised access	Unauthorised access to a system	Unauthorised access to a system or component.
	Unauthorised access to information	Unauthorised access to a set of information.
	Data exfiltration	Unauthorised access to and sharing of a specific set of information.
Unauthorised modification/deletion	Modification of information	Unauthorised changes to a specific set of information.
	Deleting of information	Unauthorised deleting of a specific set of information.
Misuse or unauthorised use of resources	Misuse or unauthorised use of resources	Use of institutional resources for purposes other than those intended.
Illegitimate use of the name of a third party	Illegitimate use of the name of a third party	Using the name of an institution without permission to do so.
SPAM	Email flooding	Sending an unusually large quantity of email messages.
	Sending an unsolicited message	Sending an email message that was unsolicited or unwanted by the recipient.
Copyright	Distribution and sharing of copyright protected content	Distribution or sharing of content protected by copyright and related rights.
Child pornography, racism and apology of violence	Dissamination of content forbidden by law	Distribution or sharing of illegal content such as child pornography, racism, xenophobia, etc.
Other	Other	Other



11 According to our partners

11.1 Sekurak

Year 2016 – marked by IoT threats. Year 2017 – will only increase this trend.

Let us imagine users' computers available directly from the Internet, with default passwords, without updates, with no anti-malware systems, full of basic vulnerabilities. Have we gone back in time to the 90's?

Not necessarily – this is what the current situation of IoT security looks like. In addition, completely new problems arise – devices are turned on all the time, and users have no idea that their devices are available directly from the Internet…

Life time of an average device is often longer than life time of e.g. a laptop (how frequently do users replace routers or CCTV cameras monitoring their houses?). Support (updates) for certain hardware on the other hand– is quite short.

The year 2016 seems to be ground-breaking for:

- The number of various devices connected to the Internet,
- The number of attacks using IoT,
- Record number of significant vulnerabilities detected in devices.

Currently, intercepting a large number of IoT devices seems to be a simple task. By the end of 2016, Mirai botnet source code has leaked – so almost everyone can try quickly creating or adapting their own botnet for a certain purpose. There are at least three problems here:

- Mirai doesn't even use advanced vulnerabilities to intercept more devices – the main method of adding new nodes to the botnet is… trying simple / default passwords to devices.

- Mirai implements several types of DDoS attacks, but if the attacker is in possession of many more than 100 000 devices (such botnets were observed in 2016) – it may be enough to simulate regular https requests for the attack to be successful. Telling such traffic apart from real client traffic can be quite a challenge…

- DDoS attacks carried out with the use of this kind of botnet reach volumes of 1Tbps.

Are the device manufacturers actually interested in changing this situation? In my opinion –except for a few cases – no. They simply lack motivation – currently, clients very rarely decide to buy a certain device basing upon its security parameters or the manufacturer's history in the field of security. They look rather at available functions and comfort of use.

This is slowly changing, however – first bug bounty programs start to appear in the world of IoT (recently Netgear got one). It can also be seen that detection of certain security problems can expose the manufacturer to high fees, which can be an argument in favour of including security in the device's production cycle. An example of this kind of fees may be calling the clients to physically send the devices back in order for them to be improved by the manufacturer – this kind of situation took place after one of the "combat" uses of the Mirai botnet.

Couldn't the manufacturer in the case described above simply release a firmware update, as it is done usually? It seems that no, and this by itself is an example of a wider problem – the very process of updating is often not triggered automatically when a new version becomes available (that would create new problems – like with proper functioning of all devices after update/restart). In case of the Mirai botnet, some suggested developing an alternate device that would … break into vulnerable devices and update them. This however, caused justified legal concerns …

The topic of in(security) IoT certainly isn't new – many of today's problems we have already seen 7-10 years ago. And interestingly, little has changed since then, except for an increase in the number of attacks and appearance of many new vulnerabilities…

Michał Sajdak
Sekurak.pl

11.2 Cybersecurity Foundation

20 years have passed since the first incident response teams appeared in Polish cyberspace. The landscape of the battlefield changed beyond recognition over this time. In the beginning, computer scanning was a challenge and a call to real action. Today such cases are treated as a kind of „network noise", an opportunity to learn about cybercriminals' activities or gain input for educational activities considerations.

The real challenge became conducting technical analyses of e.g. malicious software, but also the way of organising work of large response teams. For maximum efficiency, teams must be developed with the inclusion consist of experts in many IT security areas. Their activities should be organized into processes and supported with adequate technical tools.

It seems that thankfully, decision makers are becoming aware of that. In 2016, new Polish teams joined the European organisation associating CSIRTs (Geant TF-CSIRT, Trusted Introducer) and the ones already there shown high activity. CERT Orange Polska was the first team to be awarded the Certified status. What is more it did so in good style, which can be learnt about from this report. Aside from this team, nine more Polish teams can be found on the list. They deserve a commendation for operating proactively and with accordance with the procedures, but then a great responsibility rests with them for systematic actions for the sake of protecting not only their own resources, but the entire Polish cyberspace. And what better example of such responsibility there is, than the CyberShield programme launched by CERT Orange Polska.

Also, the activity over the country is worth noting, aiming to structure the field of cyber-security on a domestic scale. The Ministry of Digital Affairs is working on the final version of the strategy and promises a bill on cyber-security. The Ministry of Development announces the creation of the Cyberpark Enigma, and the Ministry if National Defence announces serious expenses for IT defensive capability, but above all for coordination. This is necessary to eliminate the mistakes of the past. It was the lack of coordination that was highlighted in the famous NIK report from 2015, which was referred to numerous times during discussions about the state of cyber-security in Poland.

Such actions are a necessity. We see over and over again that effects of cyber-attacks can be severe. New threats arise with regard to e.g. the Internet of Things. Entire waves of criminal actions take a heavy toll, which could clearly be seen in 2016 in regard to ransomware. Finally, threats from the cyberspace are increasingly beginning to affect the world of politics and international relations.

That last phenomenon has especially intensified in the year 2016. The most famous examples were of course the accounts and reports concerning the influence of cyber-attacks on the elective process in the United States. On that occasion, various tools have been used. Altogether, they can be described as general phenomenon of hybrid of technical and disinformation-related threats. The one and the other started to live in close symbiosis. Information gained in result of attacks created source material for trolls spreading disinformation. These two phenomena should be taken into account collectively. This opens a new area of cooperation of technical specialists with experts dealing with research and reaction to informational operations. This is the key reason for us to launch the new INFO OPS project in the Cybersecurity Foundation.

Mirosław Maj,
The Cybersecurity Foundation

11.3 Niebezpiecznik

It is not cyber-weapons or APT attacks that Polish companies should be concerned about in the first place. Such was the conclusion – probably surprising to many – which we reached after analysing the results of penetration tests conducted in the last few years. This is because in situations where we had permission to “attack” employees (and not only servers and web applications) we attained hundred percent success rate, without using malware, inducing users into opening attachments, or infecting their devices.

This may be surprising to individuals who have never been creating phishing campaigns, but the employees just gave us all that we needed – specific documents or access data to the company’s systems. In each attack, all that was needed was sending a few e-mails with adequately prepared contents to skillfully chosen victim-employees.

It is worth noting that while preparing the fake e-mails and choosing victims we took results of a week’s reconnaissance into account. Our analysts gathered everything that could be found out about the victim-company from public sources (department structure, personnel data, contractor network). Only on the basis of this information have we established whom would we impersonate (victim’s colleagues, superiors or clients). This laborious and costly work always paid off, bringing tens of thousands percent returns.

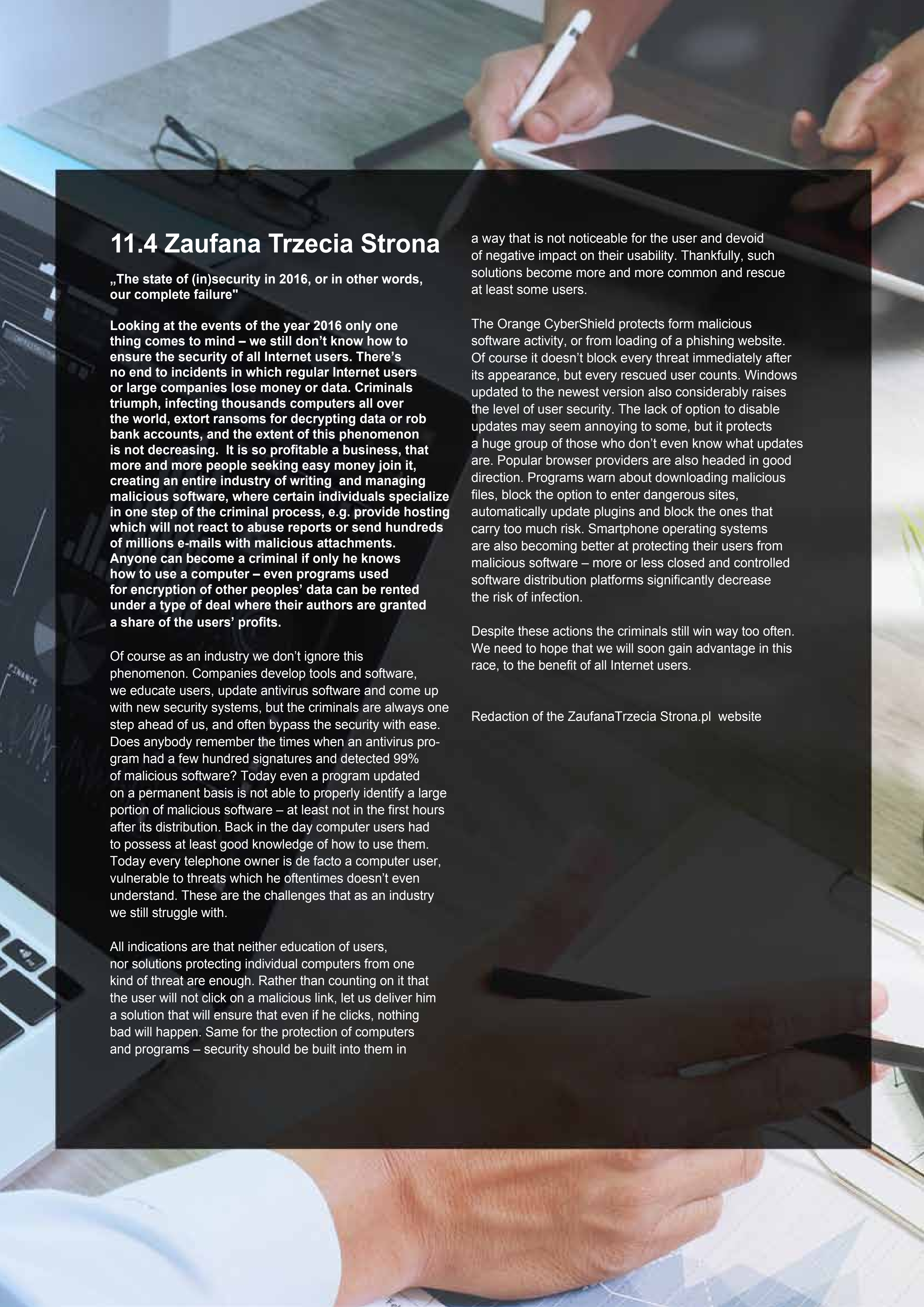
To our amazement, technical workers also fell for the fake e-mails, and oftentimes the key to success lain in choosing the right time to send them. It is a myth that only “Mrs Bradys” end up as victims.

Apart from surprisingly high percentage of victims (usually around 40% of the company’s employees), it was quite saddening to see that the IT departments of all the companies who managed to detect our attacks were not able to handle incidents of that type. They either failed to completely remove us from the company’s systems, or they couldn’t inform the personnel about the attack in a way that would prevent more people from falling for it.

In addition, our observations seem to be confirmed by the recent events in Poland. There is less mailing campaigns in which malware-infected e-mails are sent to everyone indiscriminately. Criminals now segregate their victims and send messages with specific contents to certain target groups e.g. attorneys to legal offices, projects faking AutoCAD files to architects (https://niebezpiecznik.pl/post/uwaga-prawnicy-e-mail-pelnomocnictwo-dla-kancelarii-zawieral-wirusa/), fake class enrol lists to students, (https://niebezpiecznik.pl/post/uwaga-studenci-ten-e-mail-to-scam/) or fake notifications from e-commerce websites to people actually selling on them (https://niebezpiecznik.pl/post/scam-zablokowalismy-ci-sprzedaz-na-allegro/).

Such segmentation of victims is an example of minimal reconnaissance and effort, but basing on our own experience, we are convinced that this kind of actions bring bigger profits, let alone the fact that narrow target groups make it harder for security researchers to detect and reveal such incidents. It seems like the time has come to focus our honeypots toward specific industries.

Piotr Konieczny
Niebezpiecznik.pl



11.4 Zaufana Trzecia Strona

„The state of (in)security in 2016, or in other words, our complete failure"

Looking at the events of the year 2016 only one thing comes to mind – we still don't know how to ensure the security of all Internet users. There's no end to incidents in which regular Internet users or large companies lose money or data. Criminals triumph, infecting thousands computers all over the world, extort ransoms for decrypting data or rob bank accounts, and the extent of this phenomenon is not decreasing. It is so profitable a business, that more and more people seeking easy money join it, creating an entire industry of writing and managing malicious software, where certain individuals specialize in one step of the criminal process, e.g. provide hosting which will not react to abuse reports or send hundreds of millions e-mails with malicious attachments. Anyone can become a criminal if only he knows how to use a computer – even programs used for encryption of other peoples' data can be rented under a type of deal where their authors are granted a share of the users' profits.

Of course as an industry we don't ignore this phenomenon. Companies develop tools and software, we educate users, update antivirus software and come up with new security systems, but the criminals are always one step ahead of us, and often bypass the security with ease. Does anybody remember the times when an antivirus program had a few hundred signatures and detected 99% of malicious software? Today even a program updated on a permanent basis is not able to properly identify a large portion of malicious software – at least not in the first hours after its distribution. Back in the day computer users had to possess at least good knowledge of how to use them. Today every telephone owner is de facto a computer user, vulnerable to threats which he oftentimes doesn't even understand. These are the challenges that as an industry we still struggle with.

All indications are that neither education of users, nor solutions protecting individual computers from one kind of threat are enough. Rather than counting on it that the user will not click on a malicious link, let us deliver him a solution that will ensure that even if he clicks, nothing bad will happen. Same for the protection of computers and programs – security should be built into them in a way that is not noticeable for the user and devoid of negative impact on their usability. Thankfully, such solutions become more and more common and rescue at least some users.

The Orange CyberShield protects form malicious software activity, or from loading of a phishing website. Of course it doesn't block every threat immediately after its appearance, but every rescued user counts. Windows updated to the newest version also considerably raises the level of user security. The lack of option to disable updates may seem annoying to some, but it protects a huge group of those who don't even know what updates are. Popular browser providers are also headed in good direction. Programs warn about downloading malicious files, block the option to enter dangerous sites, automatically update plugins and block the ones that carry too much risk. Smartphone operating systems are also becoming better at protecting their users from malicious software – more or less closed and controlled software distribution platforms significantly decrease the risk of infection.

Despite these actions the criminals still win way too often. We need to hope that we will soon gain advantage in this race, to the benefit of all Internet users.

Redaction of the ZaufanaTrzecia Strona.pl website

12 Dictionary

AaS – "as a service"; an abbreviation that refers to services provided to a customer via the Internet.

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

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

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

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

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

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

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

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

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

CSIRT – (Computer Security Incident Response Team) – an incident response team. The concept synonymous with CERT.

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

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

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

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

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

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

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

HTTP – (Hypertext Transfer Protocol) – a communication protocol used by the World Wide Web. It performs as a so-called request-response protocol, e.g. when a user types an URL in the browser, 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 a secure exchange of information by encrypting data using SSL. When using a secure HTTPS, a web address begins with "https://".

ICMP – (Internet Control Message Protocol) – a protocol for transmitting messages about the irregularities in the functioning of the IP network, and other control information. One of the programs that uses this protocol is ping that lets a user to 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 threatens or violates the security of the Internet. Incidents include: intrusion or an attempt of intrusion into a 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 to transmit data over the Internet. The main function of this protocol is to provide information needed to route and deliver data to the destination.

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

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

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

OWASP – (ang. Open Web Application Security Project) – globalne stowarzyszenie, które główną ideą jest poprawa bezpieczeństwa aplikacji webowych.

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 a result of actions performed by the unconscious user: opening malicious attachments or clicking on a fake link.

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

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

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

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

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

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

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

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

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

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

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

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

SYN – (synchronization) – one of the TCP flags sent by the client to the server in order to initiate the connection. SYN Flood – a popular network attack, whose main purpose is to block the services of the server. It uses TCP.

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

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

UDP – (User Datagram Protocol) – a connectionless protocol, one of the basic network protocols. Unlike TCP, it does not require setting up the connection, observing sessions between devices and a confirmation that the data has 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).

Virus – a malicious program or a piece of code hidden within another program, that replicates itself in the user's operating system. Depending on the type of virus, it can have various destructive features such as deleting files or even hard disk formatting.

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

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

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

13 Attachments:

1. Malware analysis – „E-Faktura” Orange

njRAT

https://cert.orange.pl/analizy/Analiza_njrat.pdf

2. Malware analysis – „E-Faktura” Orange

Win32.PWSZbot.fc

https://cert.orange.pl/analizy/Analiza_Win32.PWSZbot.pdf

3. Malware analysis

Keylogger iSPY

https://cert.orange.pl/analizy/iSpy-FINAL.pdf

For more information please visit:

www.cert.orange.pl