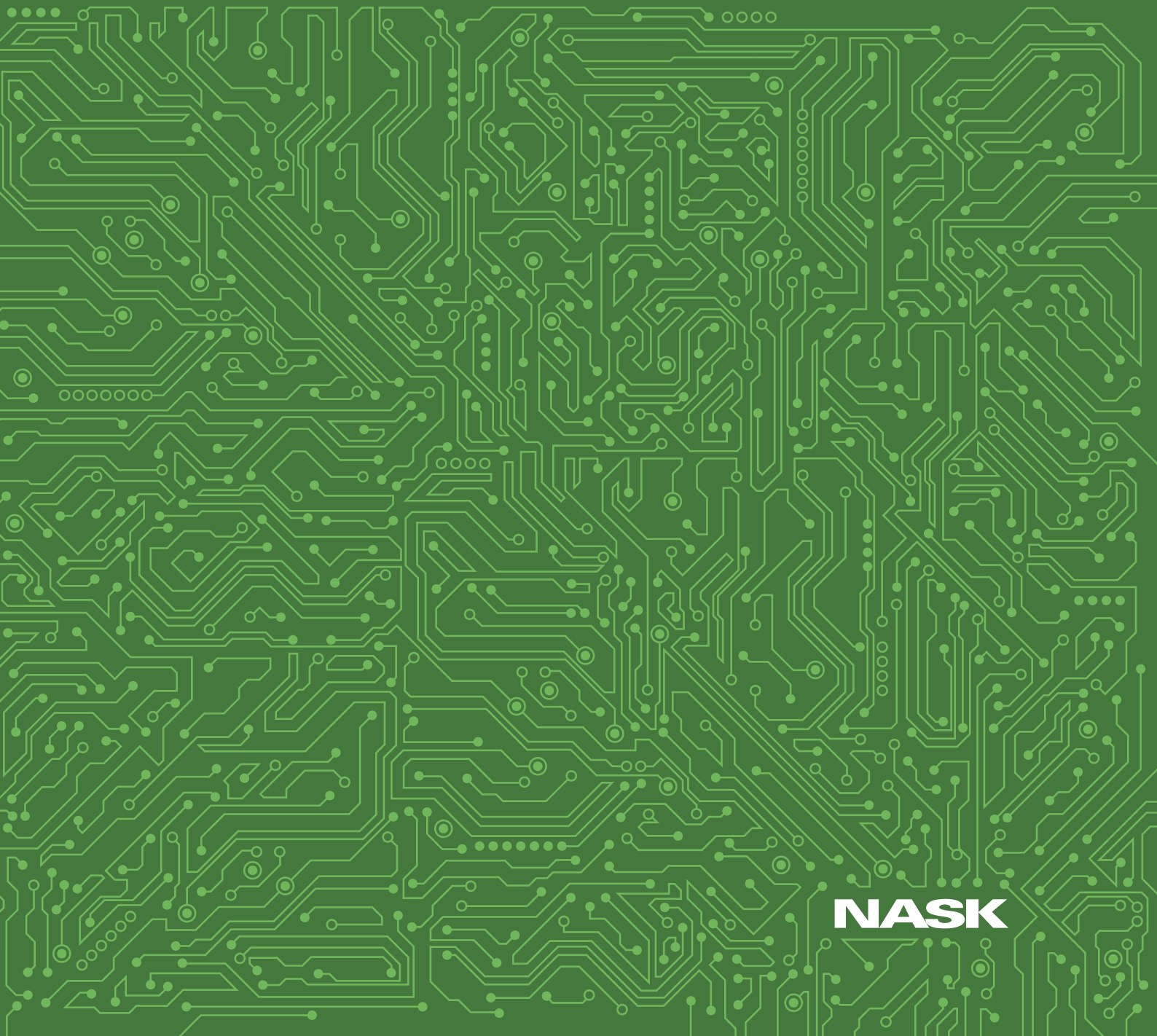
CERT POLSKA

REPORT 2014

CERT.PL



NASK

CERT Polska Report 2014

Publisher:
NASK
ul. Wąwozowa 18, 02-796 Warszawa
tel. (22) 38 08 200, e-mail: cert@cert.pl

Text and editing:
CERT Polska / NASK

Graphic design, typesetting, composition:
Anna Nykiel

ISSN 2084-9079

CERT POLSKA

REPORT 2014

CERT.PL

NASK

Contents

Introduction

This report presents the most important trends and observations that we think shaped Polish cybersecurity in 2014. This includes new, upcoming threats, their evolution and our responses to them.

In 2014 CERT Polska continued its effort to better the security of Internet users in Poland and worldwide. Last year our efforts focused on botnet mitigation, especially when these botnets used .pl domain for command and control services. Our actions made the cybercriminals limit the use of the .pl TLD and we observed the misuse of .pl domain much more rarely. However, there are cases in which the Domain Name Tasting service (short lived domain registration) is used for Exploit Kit deployment.

The most severe threat to Polish cyberspace users were (and still are) banking trojans. In 2014, we observed the rise of Tinba, VMZeuS, Kronos and IFSB families. All of the mentioned malware uses so called “webinjects” little snippets of (usually JavaScript) code that are injected in the online bank website to perform specific tasks, like using social engineering to steal one time passwords. Webinjects also played another role: they were served when a home router was hacked and had its DNS servers changed. Due to this change, an affected user connected to the online bank website using a cybercrimals’ proxy, which in turn injected a Java-Script code to the website.

Last year we also observed an increase in APT attacks, some of which were targeting Poland: examples include APT 28, Dragon Fly and Black Energy 2. However, these operations are much broader than just being directed at Poland which remained one of many targets, rather than a primary one.

An interesting new category of malware threats made their debut: malware that changed the bank account number either in the Windows clipboard (VBKlip) or in the browser’s memory (Banatrix). There is some evidence that the authors of this malware are able to freely use Polish language and as such, we decided to analyze this malware further.

Security vulnerabilities in the basic network protocols, their implementations or other popular tools composed another piece of the cybersecurity landscape in 2014. Cybercriminals still use the misconfigured network services like DNS or NTP to launch DDoS attacks. Data from our n6 platform provides a good estimate on the rate at which these vulnerabilities and misconfigurations are fixed by the Polish network operators.

Statistical analysis presented in this report are largely based on the data contained in the n6 platform. There are over 50 different sources of information coming from over 30 different companies and groups from all over the world. This data, combined with our own sources, enables us to present this unique analysis of the state of security of Polish networks in 2014.

We encourage you to cooperate with us and be a part of our projects and initiatives. Security starts with each and every one – if we do not work together, the Internet will never be free from the malicious activities.

Executive summary

- According to our data, there are 280 000 computers in Poland that have a bot during an average 24-hour window.
- We observed a surge in the misuse of the Domain Name Tasting services – short lived domains that can be "tested" before being bought.
- Polish companies and organization were targeted during APT campaigns like Pawn Storm, Black Energy or Energetic Bear. However, Poland was not a primary target for these campaigns.
- An increase cybercriminal activity directed at the Polish Internet users is the most important and the most disturbing trend in 2014. Cybercriminals, in at least several cases, were able to steal upwards of several hundred thousand dollars.
- The most popular banking trojans in 2014 were ISFB, Tinba, Kronos and VMZeuS.
- The biggest botnets in Polish networks in 2014 were Conficker, ZeroAccess and Zeus (including all its subsequent modifications and variants). However, only ZeroAccess and Zeus infection percentages have risen. Virut encountered a significant drop in the number of infections.
- There was a small increase in the number of attacks on Polish corporations and local administration.
- There were at least 7 different social engineering scenarios used in webinject malware campaigns.
- We see more and more attacks coming from within Poland. Sometimes, attackers haved even developed and used their own malware, like VBKlip or Banatrix.
- The most popular method of infection of users in Polish networks are malicious email attachments.
- A lot of security vulnerabilities in network protocols and tools were being reported by the international mainstream media. However, there is a visible significant lack of communication and understanding between experts, journalists and readers.
- Despite the severity of Shellshock or Heartbleed we did not observe or get any information about any crippling attacks that were using this vulnerabilities. However, attacks using them are still observed and probably are here to stay.

- Traditional phishing targets many different online sites. Apart from more traditional targets, like banks and financial services, popular targets include online gaming sites and IRS or its counterparts.

- Although DDoS attacks can provide significant inconvenience, especially in the ecommerce segment, the average user is not affected economically by it. In 2014 DDoS attacks on Polish President and Polish Stock Exchange websites were reported by many media outlets, however they were performed only to make a statement rather than a serious threat.

- In 2014 there were several dataleaks concerning Polish users, but the one concerning Polish Stock Exchange was the most significant.

- Android malware is present in Poland, but is not a significant issue.

- Number of open DNS server dropped in 2014 and this was largely attributed to the actions of Orange.

- Most malicious URLs in the .pl domain were hosted in the Interia.pl sp. z o.o. autonomous system.

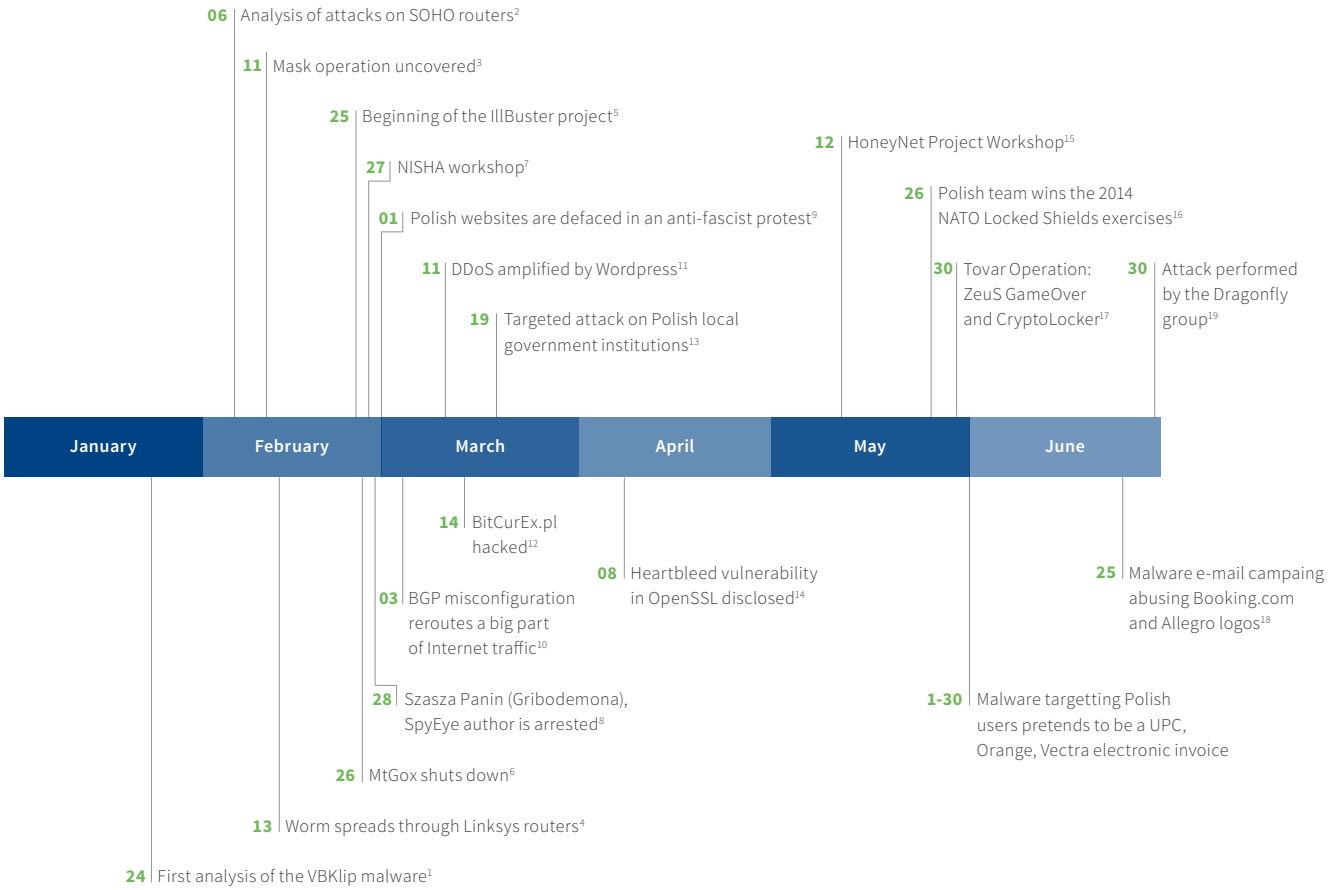
- The most popular misconfigured network protocol in Poland is SSDP.

- Most popular TLDs in which the malicious URLs are hosted (including targeting Polish users) are: .com, .org and .ru.

- Percentage of the malicious URLs hosted in .pl registrars reflects the sizes of these registrars rather than their capability in handling malicious registrations.

- C&C statistics are almost the same as last year's. However, there is a new country on the list Uruguay in which all of the C&C servers are located in one autonomous system.

Key Events in 2014



[1] http://www.cert.pl/news/7955

[2] http://www.cert.pl/news/8019

[3] http://niebezpiecznik.pl/post/operacja-maska-7-lat-w-ukryciu-prawie-400-ofiar-z-31-krajow-kolejny-rzadowy-malware/

[4] http://zaufanatrzeciastrona.pl/post/internetowy-robak-infekuje-nieza-bezpieczone-rutery-linksysa/

[5] http://www.cert.pl/news/8171

[6] http://zaufanatrzeciastrona.pl/post/tajemnicze-wlamanie-do-mtgox-czyli-jak-wartosc-bitcoinow-spadla-do-zera/

[7] http://nisha.cert.pl/node/224

[8] http://krebsonsecurity.com/2014/01/feds-to-charge-alleged-spyeye-trojan-author/

[9] http://niebezpiecznik.pl/post/ukranscy-anonimowi-podmienili-kilkanascie-polskich-stron-www/

[10] http://zaufanatrzeciastrona.pl/post/czemu-indonezyjski-operator-probowal-wczoraj-przejac-wieksza-czesc-internetu/

[11] http://niebezpiecznik.pl/post/trwaja-ataki-ddos-wykorzystujace-wordpressa-sprawdz-czy-twoj-blog-zostal-uzyty-w-ataku/

[12] http://niebezpiecznik.pl/post/bitcurex-polska-gielda-btc-zhackowana/

[13] http://zaufanatrzeciastrona.pl/post/ukierunkowany-atak-na-pracownikow-polskich-samorzadow/

[14] http://niebezpiecznik.pl/post/krytyczna-dziura-w-openssl-ponad-65-serwerow-w-internecie-podatnych-na-podsluch-i-to-od-2-lat/

[15] http://www.cert.pl/news/8196

[16] http://www.cert.pl/news/8647

[17] http://blog.shadowserver.org/2014/06/08/gameover-zeus-cryptolocker/

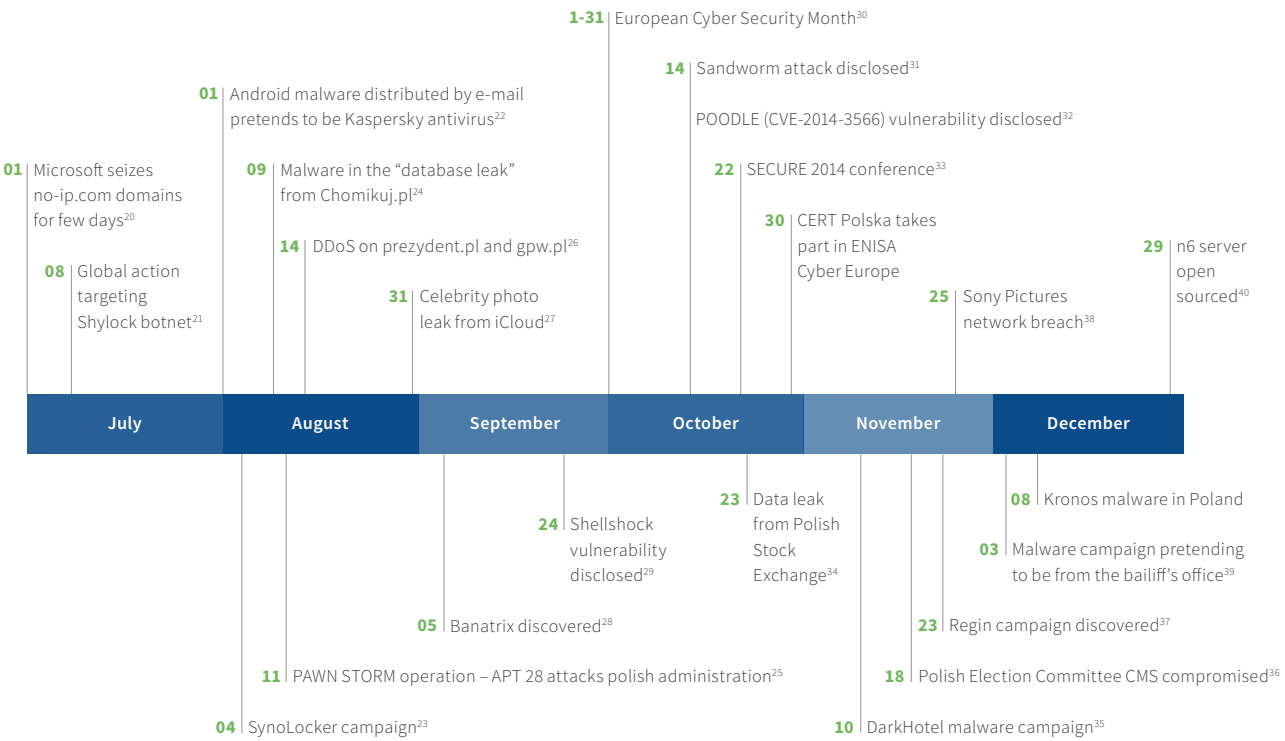
[18] http://www.cert.pl/news/8706, http://www.cert.pl/news/8798

[19] http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

[20] http://niebezpiecznik.pl/post/nie-dziala-ci-domena-od-no-ip-com-microsoft-ja-przejal/

[21] https://www.europol.europa.eu/content/global-action-targeting-shylock-malware

This chronological review contains key events related to the activities of CERT Polska and other important events we felt were relevant to our work, both in Poland and worldwide.



[22] http://niebezpiecznik.pl/post/wreszcie-ktos-zrobil-calkiem-dobry-fake-mail-czyli-twoj-bank-i-kaspersky/

[23] http://niebezpiecznik.pl/post/jesli-masz-nas-a-marki-synology-lepiej-zrob-kopie-bezpieczenstwa-czyli-synolocker-w-akcji/

[24] http://zaufanatrzeciastrona.pl/post/falszywy-wyciek-prawdziwych-danych-uzytkownikow-chomikuj-pl/

[25] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf

[26] http://niebezpiecznik.pl/post/cyber-berkut-atakuje-polskie-serwisy-internetowe-prezydent-plpadl-gwp-tez/

[27] http://en.wikipedia.org/wiki/2014_celebrity_photo_hack

[28] http://www.cert.pl/news/8999

[29] http://www.cert.pl/news/9083

[30] http://bezpiecznymiesiac.pl/

[31] http://niebezpiecznik.pl/post/4-nowe-i-krytyczne-dziury-w-windows-jedna-uzyta-przez-rosjan-atakujacych-polskie-firmy/

[32] https://www.openssl.org/~bodo/ssl-poodle.pdf

[33] http://secure.edu.pl

[34] http://niebezpiecznik.pl/post/gielda-papierow-wartosciowych-zhackowana/

[35] http://securelist.com/blog/research/66779/the-darkhotel-apt/

[36] http://niebezpiecznik.pl/post/wlamanie-na-serwery-panstwowej-komisji-wyborczej-wykradziono-hashe-hasel-i-klucze-urzednikow/

[37] http://niebezpiecznik.pl/post/zhackowal-komputery-komisji-europejskiej-nadajniki-sieci-gsm-oraz-komputer-prezydenta/

[38] http://niebezpiecznik.pl/post/sony-totalnie-zhackowane-wykradziono-olbrzymia-ilosc-danych-i-zablokowano-komputery-pracownikom-ponoc-takze-tym-w-polsce-siedziby-zamkniete-pracownicy-zwolnieni-do-domow/

[39] http://www.cert.pl/news/9484

[40] http://www.cert.pl/news/9635

Malware in the world

2014 was unique in the sheer amount of events that had a significant impact on both big business and big politics, like the credit card data leak at Target, MtGox downfall and politically motivated Syrian Electronic Army attacks. There were also some more advanced malware campaigns like APT28, Regin, Careto, Sandworm or Uroburos.

However, the average Pole was more affected by banking trojans, like Zeus family malware, VBKlip or Banatrix. We also observed several RAT or keylogger campaigns against Polish users, including e.g. Ardamax Keylogger.

One APT campaign, called APT28, was particularly interesting. This operation was performed by a group called “Pawn Storm”. In August 2014 this group targeted Polish public administration and in July they were able to put exploit kits on bip.gov.pl and OBRUM research institute webistes. The exploit kits dropped the Sednit malware. In September, the Warsaw Commodity Clearing House website was hacked in a similar manner. Apart from this campaign, several others APTs were directed against Polish users. Among them were Black Energy and Energetic Bear, as well as the (more random) DarkHotel.

It was the first time that Poland was targeted for intelligence gains on a larger scale. There were also some hacktivist attacks: a DDoS on prezydent.pl (Polish President website) or gpw.pl (Polish Stock Exchange website) and a DDoS attack on Polish equivalent of Securities Exchange Comission as a part of #OpRemember Anonumous campaign.

Despite all of this, Poland is still not the main target of APT operations and we hope that it will remain the case for the following years.

Most important threats in .pl

2014 brought a lot of threats to regular Internet users. When you are presented with such a threat, you assess not only the technical excellence of the exploit, but also the level of financial losses that it could produce for these regular users. And, although all DDoS attacks are burdensome for content providers, ecommerce brands or local and federal governments, the regular user usually is not affected financially by those actions. Another type of attack, more economically motivated, is malicious software created to maximize financial gains for cybercriminals. This malware can realize its goal in a twofold manner. Infected machines can be utilized to perform new attacks (such as DDoS, sending spam, ad frauds, hosting of malicious content, proxying targeted attacks) or to provide direct financial benefit to the attacker (such is the case with ransomware, data extraction, social engineering attacks on online banking users). Both of these scenarios were observed in Poland. Both of these malware attack scenarios are serious threats, but we decided to focus on the latter.

Malicious DNS servers

In the first half of 2014 a lot of different media reported massive attacks on the owners of, easily exploitable, SOHO routers. After the device was broken into, cybercriminals changed the DNS server IPs and redirected the queries to the servers controlled by them. This enabled them to serve fake, often malicious, websites and persuade them to e.g. install malware that supposedly was just a “plugin update” or “popular software”. It also made it easier for them to perform phishing attacks targeting online banking services. Then, preying on the fact that user does not notice that his connection is not encrypted, attackers extract login data and try to present him with a social engineering attack.

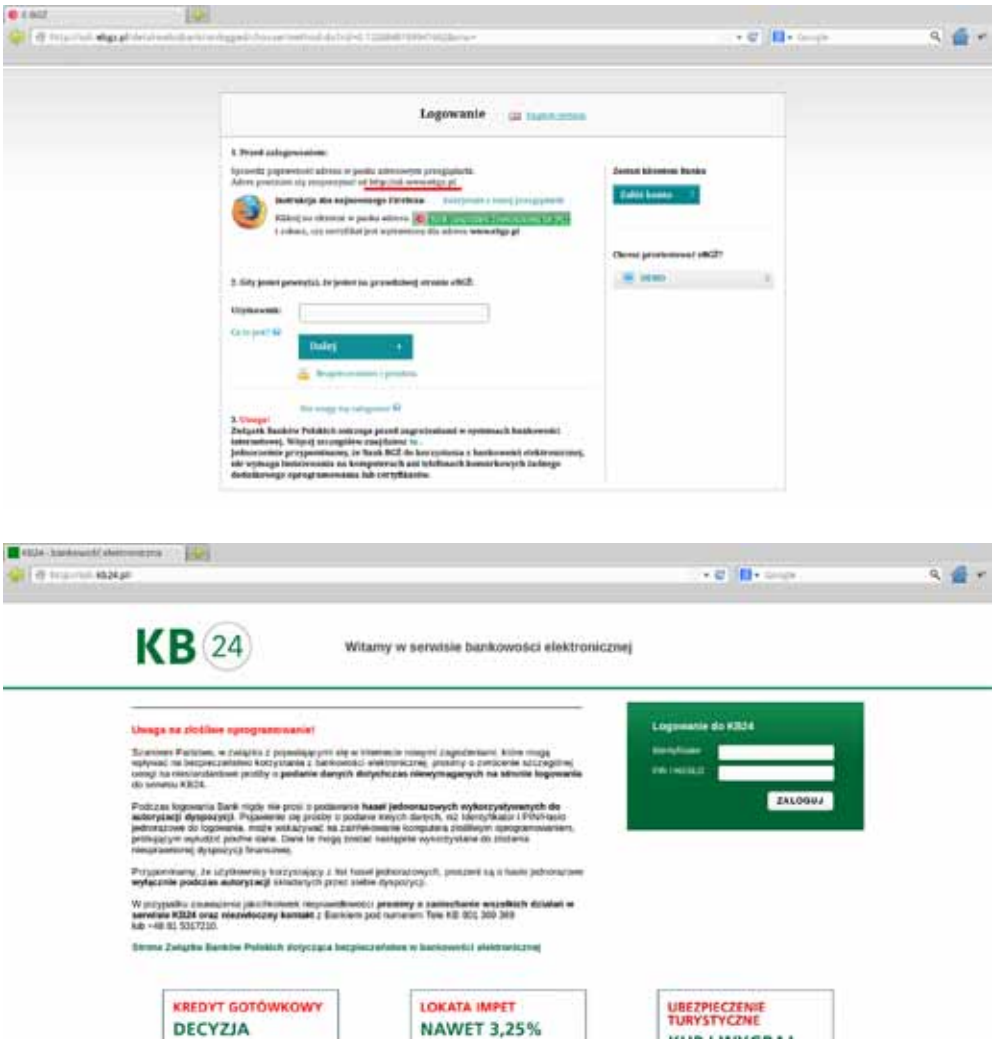


Chart 1. Fake login screens.

Malware campaigns

In 2014, not unlike in the previous years, there were many attacks that used e-mail to impersonate known Polish and international companies, like Allegro.pl, Orange, Play, T-Mobile, mBank, DHL, Netia, UPC, Poczta Polska, UPS, Booking.com or Vodafone. There also were e-mails which were supposedly sent because a user bought an item on Polish online action website Allegro.pl and was instructed to pay for it.

Chart 2. E-mail pretending to be information about an item bought via Allegro.

All of these scenarios had a common factor in them – e-mails included a malicious attachment or a link to a malicious executable. These messages are also more carefully prepared then the campaigns we observed in the last years. They looked almost exactly like the original messages, so it was relatively easy to convince the user to click on a link or open executable posing as a PDF file. Companies, which identities were abused by the attackers, reacted very quickly. The reaction varied widely and included: messages sent or presented to the users outlining the current campaign, changing the email themes, stopping the practice of including PDF files in emails, sending mails from a correct domain owned by a company, instead of using the marketing agency domain. Most of the companies tend to use SPF[1], however not all mail servers enforce it. In previous years the market was dominated by different versions of Zeus, SpyEye, Citadel, or even Zeus Gameover/P2P (up until the December of 2012). Last year however proved that cybercriminals are very flexible when it comes to the malware family they use and we observed several new strains, not present on the Polish market previously: VmZeus, KINS, Tinba, IFSB/Gozi2, Kronos, SmokeLoader (as a dropper). However, there is still a common point in all of these attacks: ATS *(Automatic Transfer Script)* used to host the webinjects and provide an easy platform for attackers to manage the money transfers. These ATS were described in detail in our 2013 report. The same ATS were used also with conjuction with the SOHO attacks.

[1] Sender Policy Framework http://www.openspf.org/

Heartbleed – CVE-2014-0160

April the 7th of 2014 was the day when the world heard about Heartbleed – a vulnerability in the OpenSSL library. This vulnerability was affecting versions 1.0.1a-f of the library and allowed not too skillful attackers to read a portion of client or server memory. OpenSSL is used both by server applications (like web or e-mail servers) and by client applications (however the most popular browsers do not use this functionality). This vulnerability was easily exploited and left no traces on the affected machine. It was discovered independently by Neel Meht from the Google Security Team and the Finnish company Codenomicon[2].

[2] http://www.smh.com.au/it-pro/security-it/heartbleed-disclosure-timeline-who-knew-what-and-when-20140415-zqurk.html

Were Polish systems affected?

Scanning the TCP/443 port (default HTTPS port) in Polish IP space shortly after the vulnerability disclosure yielded the following results:

- 15,737 IPs were running a vulnerable service, which is 1.8% of all of the IPv4 addresses which had TCP/443 open.,
- 675,478 IPs were running HTTPS service, but were not vulnerable. This is 76.8% of all of the IPv4 addresses which had TCP/443 open.

The rest of the IPs either were unresponsive or reported some kind of error. The vulnerability was mainly present on edu.pl domains. From 13,490 most popular (according to Alexa.com) addresses in .pl domain, 765 (5.7%) were vulnerable, including several large internet ecommerce sites. ARAKIS – our early warning honeypot based system – observed a surge in TCP traffic on ports connected with the use of SSL protocol: 443 (HTTPS), 465 (SMTPS), 993 (IMAP), 995 (POP3).

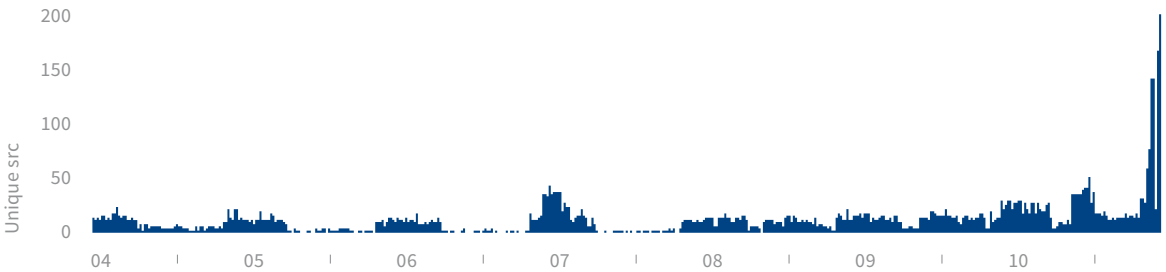


Figure 3. Destination port 443/TCP. From 04.04.2014 10:10:06 To 11.04.2014 10:10:06.

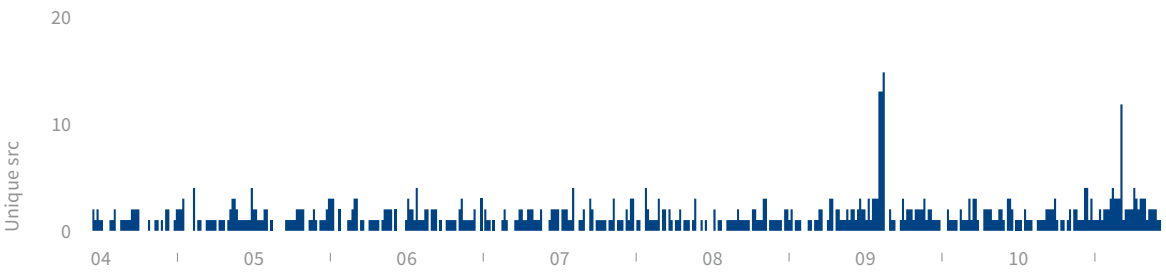


Figure 4. Destination port 465/TCP. From 04.04.2014 10:06:43 To 11.04.2014 10:16:43.

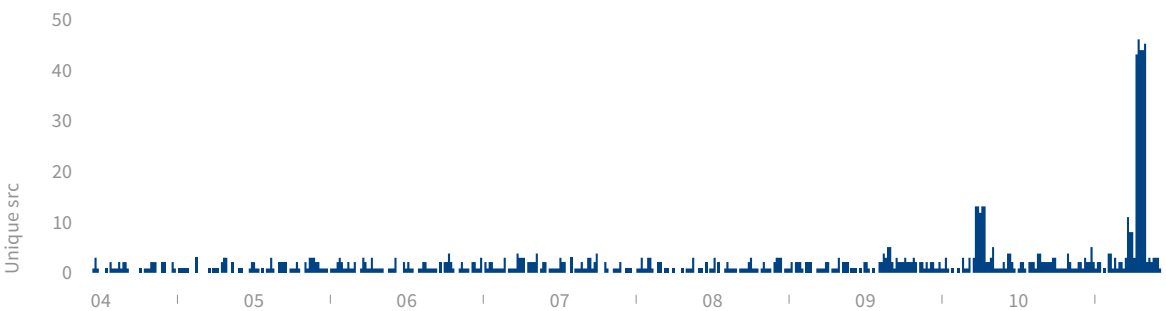


Figure 5. Destination port 993/TCP. From 04.04.2014 10:10:56 To 11.04.2014 10:10:56.

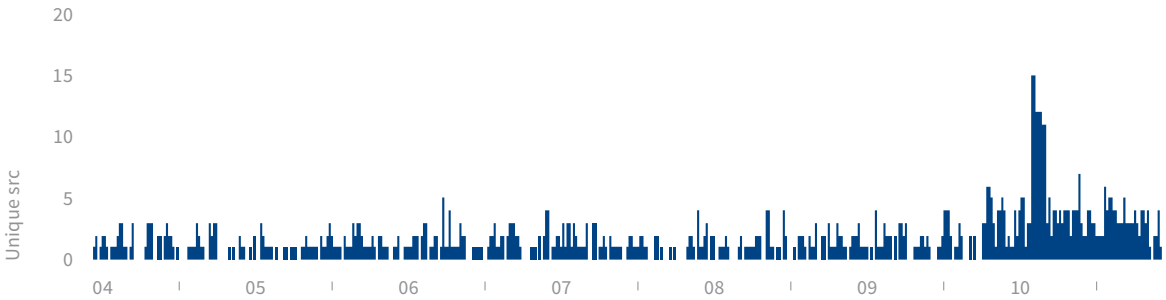


Figure 6. Destination port 995/TCP. From 04.04.2014 10:11:23 To 11.04.2014 10:11:23.

We have also monitored the rate at which the vulnerability was mitigated in the .gov.pl and .mil.pl websites (governmental and miliatry services). Two days after the vulnerability was made public, 57 out of 698 services (8.1%) was using the affected version of the library. This number dropped significantly and at the end of 10th of April (three days after publication) only 18 services were left with the vulnerability (2.6%). This decline is presented on the chart below.

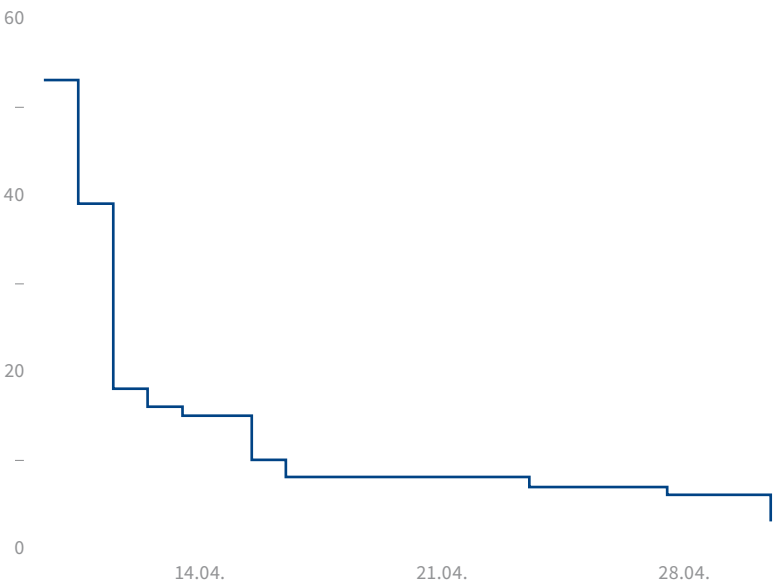


Figure 7. Affetcted services in .gov.pl and .mil.pl domains.

The aftermath

CVE-2014-0160 was also the first vulnerability to gain international recognition by the mainstream media. It also has a logo and domain[3]. It also provided a ground for discussion about the responsible disclosure.

[3] http://heartbleed.com/

Shellshock[4]

2014 saw another big vulnerability, discovered by Stéphane Chazelas, which affected bash shell and allowed attackers to remotely execute code, even with root permissions, with some special prerequisites like having the CGI module to Apache or having an SSH account on server (via OpenSSH "ForceCommand" option) or having one of many other applications using the same mechanism to process the shell environmental variables. First official patch mitigated only one exploit and did not remove the vulnerability. Suddenly there was an influx on a similar vulnerabilities reported, among others, by Michał Zalewski. Finally on the 1st of October he proclaimed that all of them were fixed. Of course, Shellshock is still used for attacks on unpatched webservers and to distribute malware[5, 6, 7].

As we have mentioned, in 2014 mainstream media started reporting vulnerabilities to the average users. This was probably in part due to the movement to create logos and catchy names for every discovered vulnerability and in part due to the fact that regular users could be affected by some of them (e.g. Heartbleed). However, this could lead to misunderstandings and sometimes even factual errors in the reports, which come from the lack of technical background of some of the journalists. Most famous example of that kind was a statement made by one of the Polish media, which can be translated to "IT security experts are still trying to cover the hole left by the Heartbleed virus, which is an error in OpenSSL protocol"[8].

[4] CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187

[5] http://blog.malwaremustdie.org/2014/09/mmd-0028-2014-fuzzy-reversing-new-china.html

[6] http://blog.malwaremustdie.org/2014/10/mmd-0029-2015-warning-of-mayhem.html

[7] http://blog.malwaremustdie.org/2015/01/mmd-0030-2015-new-elf-malware-on.html

[8] http://tvn24bis.pl/wiadomosci-gospodarcze,71/czeka-nas-powtorka-z-heartbleed-wykryto-nowa-luke-w-kodzie,437143.html, accessed on 25 February 2015

Case studies

APT in Poland

To quote the SANS paper about the APT[9]:
In 2006, the United States Air Force (USAF) analysts coined the term advanced persistent threat (APT) to facilitate discussion of intrusion activities with their uncleared civilian counterparts. Thus, the military teams could discuss the attack characteristics yet without revealing classified identities. Bejtlich explains the components of the terminology.

- *Advanced* means the adversary is conversant with computer intrusion tools and techniques and is capable of developing custom exploits.
- *Persistent* means the adversary intends to accomplish a mission. They receive directives and work towards specific goals.
- *Threat* means the adversary is organized, funded and motivated.

The use of the term APT became very prevalent and infashion recently. It became a kind of umbrella term for several, highly subjective, threats:

- "advanced" malware
- malware that attacks "important" institutions
- malware that targets selected, not usually welldefined, targets.

The advantage gained in the APT can be monetized or used for other purposes. Every year sees an increase in APT attacks, partly because they are becoming more and more popular and partly due to the popularity of the term.

Below is the brief summary of several APTs (in any of the abovementioned meaning) in which Poles were victims.

[9] SANS Technology Institute, *Assessing Outbound Traffic to Uncover Advanced Persistent Threat*, http://www.sans.edu/student-files/ projects/ JWP-Binde-McRee-OConnor.pdf, accessed on 27.02.2015

SandWorm group and BlackEnergy malware

In October 2014 several portals reported news about the SandWorm group, supposedly coming from Russia, that used BlackEnergy to attack several institutions. Among them were governmental and NATO facilities, academic institutions, companies from the energy, telecommunications or defense sectors. The attacked person was carefully selected and had a spear phishing e-mail sent to them, including details like the names of the conferences that she was about to attend. According to researchers from iSIGHT partners, the main goal of the campaign was to exfiltrate confidential data. Spearphishing attacks were done using a specially crafted Microsoft Office documents that exploited either CVE-2014-4114 or CVE-2013-3906 vulnerabilities in Word or PowerPoint document processing to perform Remote Code Execution. This file, when opened, lead to the execution and installation of the BlackEnergy malware, which provided a complete control of the infected machine.

Most of the targets were based in Ukraine and Poland. According to the information published by iSIGHT partners in Poland energy sector was the primary target. We were informed by researchers from ESET about 28 unique IP addresses in Poland and 43 unique IP addresses in Ukraine that were infected with BlackEnergy.

APT28 group, PawnStorm operation and SEDNIT malware

One of the more popular events of 2014 was a report by FireEye[10] concerning a group called APT28. According to this report, this group may have been supported by the Russian government and was aiming at providing information valuable to that government. Authors of the distributed malware were also most probably Russian, according to FireEye.

The infection procedure was rather complex. First step was a spearphishing attack – a specially crafted and targeted e-mail message with a Microsoft Office file. When a user opened the file, one of the vulnerabilities was used to gain control, e.g. CVE-2012-0158 – vulnerability in ActiveX, which is used by MS Office. The next step was the dropper called "Sourface", which downloaded and installed a backdoor called "Eviltoss". The primary goal of this backdoor was to gather and steal information stored on the victim's computer. All this malware zoo was called "Sednit" and contained many specialized modules, like the ones used to steal saved logins and passwords, access network drives and devices, performing changes in the Windows registry, starting new processes or simply logging the user activity.

APT28 group targeted organizations from the defense sector (like NATO), governmental institutions of the Georgian or East European governments (like the Ministry of Defence). Some of the targets were located in Poland and Hungary.

Similar attacks took place between July and September 2014. This campaign was called "Pawn Storm" by Trend Micro. The attackers were able to compromise several governmental website and Warsaw Commodity Clearing House service. In August the group sent multiple malicious .mht files, which also used an ActiveX CVE-2012-0158 vulnerabilities. They were targeting several Polish governmental employees. Similarly to the APT28 activities, this campaign also started with a spearphishing email messages.

[10] APT28: A Window into Russia's Cyber Espionage Operations?: https://www.fireeye.com/content/dam/legacy/resources/pdfs/apt28.pdf, accessed on 02.03.2015

Dragonfly/Energetic Bear

In June and July 2014 Symantec and Kaspersky published a detailed report about the Dragonfly/Energetic Bear group. This group was operating since at least 2011 and was targeting defense and avionics industries in the United States and Canada.
In 2013 the group started targeting energy sector, pipeline operators and power plants localized in the United States and in Europe.
Drangonfly group used three different methods to infect the victim's computer. Firstly, they used a malicious PDF attachment, which used an Adobe Flash vulnerability (CVE-2011-0611). Then, in June 2013 Dragonfly started to attack and compromise energy related websites injecting a malicious code to iframes, which redirected users to the exploit kit hosting websites. They used LightsOut exploit kit or its newer version called "Hello". Machine compromised by the exploit kit was infected with Oldrea backdoor (also called Havex or Energetic Bear RAT) or Karagany trojan.

Third, most advanced infection method was infecting the ICS software packages available on the vendor websites. Software packages were bundled with a Trojan horse and put back up on the vendor website. This created an illusion that they were safe to use and install. According to the Symantec report, compromised ICS packages were available for download for at least 10 days in April 2014. Once infected, attackers were able to steal data, upload and execute other files, steal the password and login credentials as well as make screenshots.

Based on the data that was shared with us, we were able to identify 350 unique infected IP addresses in Poland.

Darkhotel group

In November 2014 report about the Darkhotel (or Tapaoux) group was published. According to the analyst from Kaspersky, attackers were infecting luxurious hotels WiFi networks in Japan. This hotels were targeted because they were a usually chosen by the upper management and R&D personnel working in the electronics, pharmaceutical and automotive industries. Compromised WiFi network required hotel guests to enter room number and last name in order to get access. This could potentially lead to a very specific targeting. Group used a social engineering attack to lead a victim to install malware. They presented a website with a fake update to a popular software and asked user to install it on her computer. In reality, this update was infected with a trojan horse. This update was also signed using a compromised CA, so that user was fairly certain that this was a legitimate update. In total, Darkhotel was able to obtain 10 different private CA keys, all of them only 512 bit. Infected user had his login and password data stolen. What was interesting is that the first C&C contact was performed 180 days after the infection, and machines with Korean locale were not infected. Darkhotel was using following tools: Tapaoux, Pioneer, Karba and Nemim. Our aggregated n6 data shows that 36 different Polish IP addresses were infected, 16 of which belong to the mobile operators.

Misconfigured servers and services in Poland

In 2013 we started to publish information about misconfigured DNS and NTP servers used for DDoS attacks. In 2014 attackers started to use exotic, 30 year old protocols, such as CHARGEN (Character Generator Protocol, RFC864) or QOTD (Quote Of The Day, RFC865). Reflected DDoS was also performed using DNS, NTP, SSDP (Simple Service Discovery Protocol), SNMP (Simple Network Management Protocol) and NetBIOS (Network Basic Input/Output System) protocols. On December 2014 North Korea was targeted in a DNS/NTP reflected DDoS attack[11].

All of these protocols share a common factor – they are based on the spoofingprone UDP protocol. Reflected attacks are based on the ability to change (spoof) the source IP address. The server usually sends a response to the declared source IP, not to the actual sender of the message. Using a – TCP protocol for this attack would be less effective TCP has to establish a connection before any data is sent.

[11] http://www.arbornetworks.com/asert/2014/12/north-korea-goes-offline/, accessed on 03 March 2015.

What are the misconfigured services?

DNS is one of the key Internet protocols. It provides users with a translation between domain name (e.g. *www.cert.pl*) and the IP address (e.g. *162.159.246.20*). This allows users to remember a much more natural domain name, instead of the IP address.

NTP is a widely used service and protocol used to synchronize clock between different machines.

SNMP is a protocol used to manage network devices (e.g. routers, switches) using IP network. SNMP is supported by the majority of network devices.

SSDP is a protocol created by Microsoft and Hewlett-Packard used to detect UPnP (Universal Plug and Play) devices.

NetBIOS is a protocol created in the 80s. Its purpose was to allow applications created using NetBIOS API to communicate over TCP/IP network.

QOTD and **CHARGEN** are both protocols created in the 70s and used to test the network connectivity. Both accept a onebyte UDP packet request and respond with Quote Of The Day (QOTD) or random 72 ASCII characters (CHARGEN). The latter one was implemented in quite a few network printers.

The reflected attack is based on the fact that some services generate response packet, which is significantly larger than a request packet. For example, sending a 20-30 byte request to the DNS server may result in a response that is 20 times bigger. Sending 1 byte packet to CHARGEN service can lead to a response that has 74 bytes, while QOTD will generate even 100 bytes in response. Current record holder for the biggest response to request ratio is NTP, which can generate a response that is several hundred times larger than the request.

Generating a large response is the expected behavior for CHARGEN and QOTD and that is why these protocols should be made obsolete or restricted to the local network. Large NTP response is just a misconfiguration and should be resolved by applying appropriate measures. However, making SSDP and SNMP protocol accessible from the Internet poses a significant risk of being used by an attacker – these protocols, albeit very useful, should only be accessed from a specific set of networks.

Vulnerable and misconfigured services in Poland

In 2014 CERT Polska received information about misconfigured CHARGEN, Netbios, NTP, SNMP, SSDP, QOTD services on Polish IP space.

	Service	Unique IP addresses in a year	Daily average of unique IP addresses
1	SSDP	2,562,309	144,189
2	SNMP	2,325,483	67,176
3	DNS	2,226,699	101,020
4	NTP	278,484	33,112
5	Netbios	186,101	13,070
6	QOTD	21,993	442
7	CharGen	18,997	839

Table 1. Most popular misconfigured services in Poland.

Table 1 presents the most popular misconfigured services in Poland used in DDoS attack. According to this data, most commonly misconfigured protocol is SSDP. According to our expectations, QOTD and CHARGEN are at the bottom of the table.

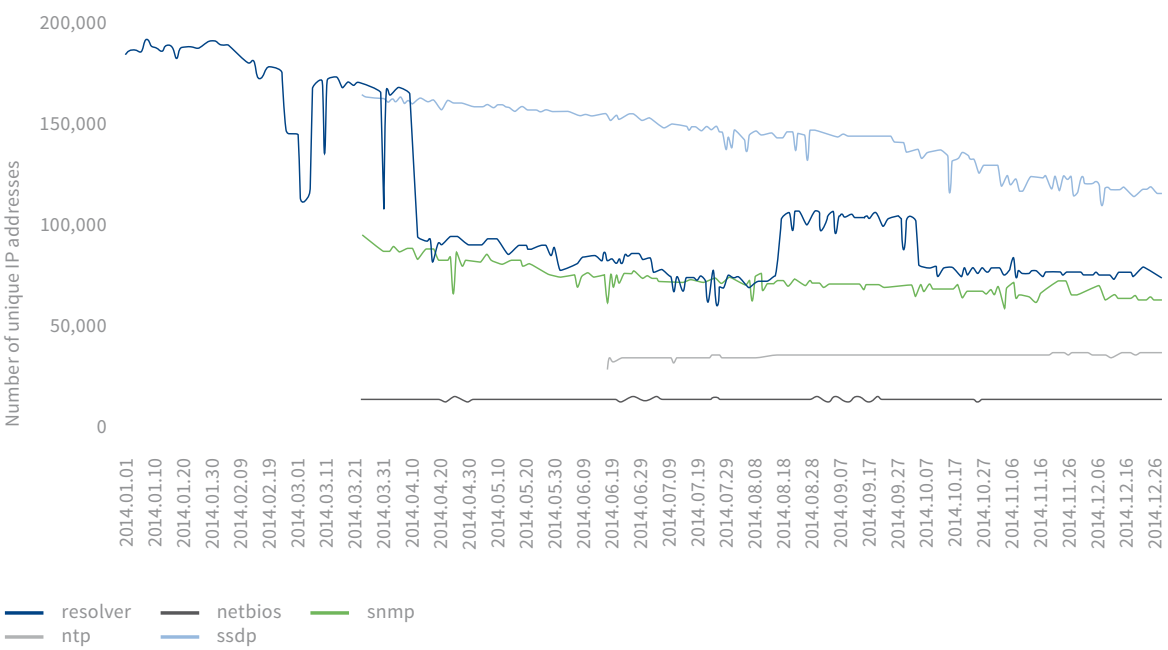


Figure 8. Number of the unique IP addresses with misconfigured services (dns, ntp, netbios, ssdp, snmp) in 2014. [dane: 150.csv].

Chart 1 present a number of unique IP addresses with misconfigured services per day. Most of our data were available since the second quarter of 2014.

The biggest fall in the misconfigured services was observed regarding the DNS service. At the end of 2014 almost half of DNS servers administrators solved a problem with DNS configuration. This can be attributed due to the fact that media outlets were reporting DDoS attacks performed using misconfigured DNS. Shadowserver's "Open Resolver Scanning Project" could be also a contributing factor, as well as actions performed by Orange Polska. SSDP and SNMP protocols registered a smaller fall, with NTP and NetBIOS almost staying at the same level. This is especially troubling when you consider that DDoS attacks using NTP protocol are becoming more and more frequent. Both CHARGEN and QOTD noted a slight increase in the unique IP address count, but they are still a very small part of the overall problem.

Open DNS servers in Polish autonomous systems

Charts 9-14 present a daily distribution of unique IP address with open DNS servers in Polish autonomous systems. This is only limited to the biggest contributors to the open DNS problem in Poland. As you can see on these charts, some ISPs did take actions against the open DNS problem and tried to resolve it. Orange network reduced number of the open DNS server by two thirds. Analyzing the data from our n6 platform, it seems that this fall is due to actions taken by Orange against a DSL service provided for businesses. In Netia, GTS and UPC there is also a noticeable decline in the number of open DNS servers. However, Multimedia Polska and Vectra had a constant number of open DNS server, while T-Mobile registered a slight increase.

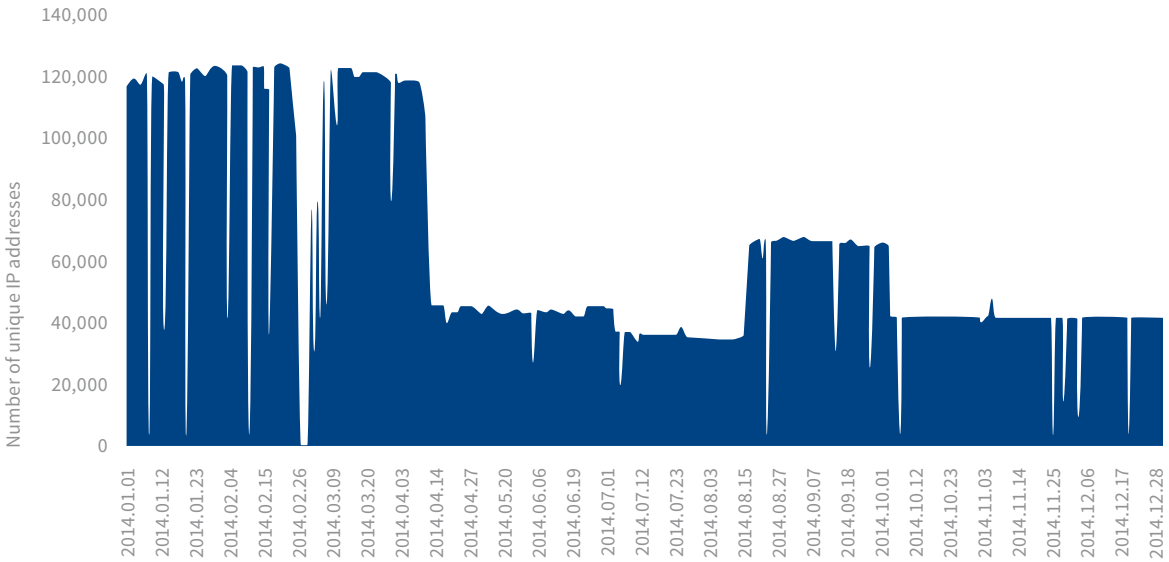


Chart 9. AS5617 – Orange.

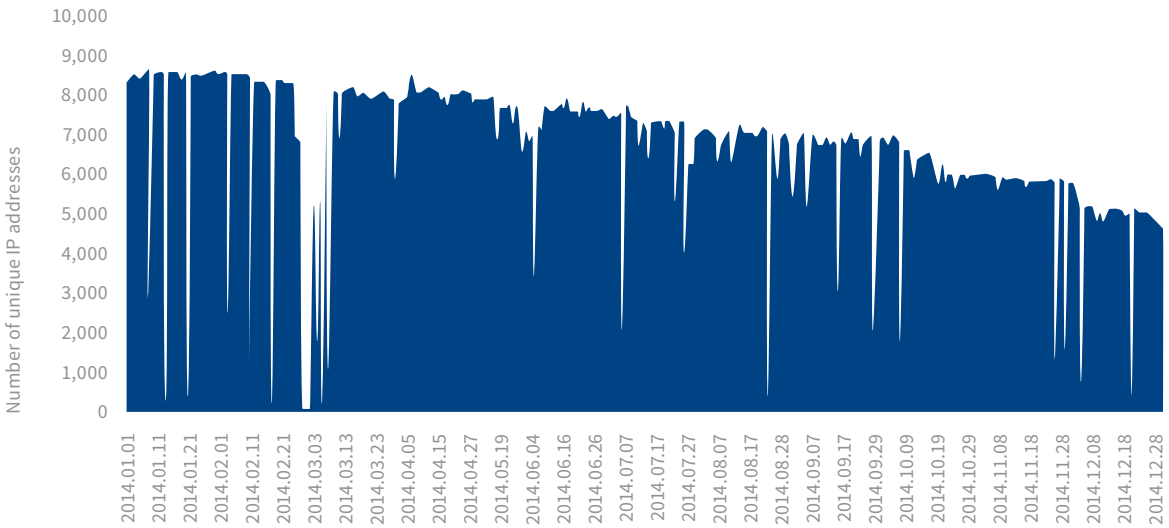


Chart 10. AS12741 – Netia.

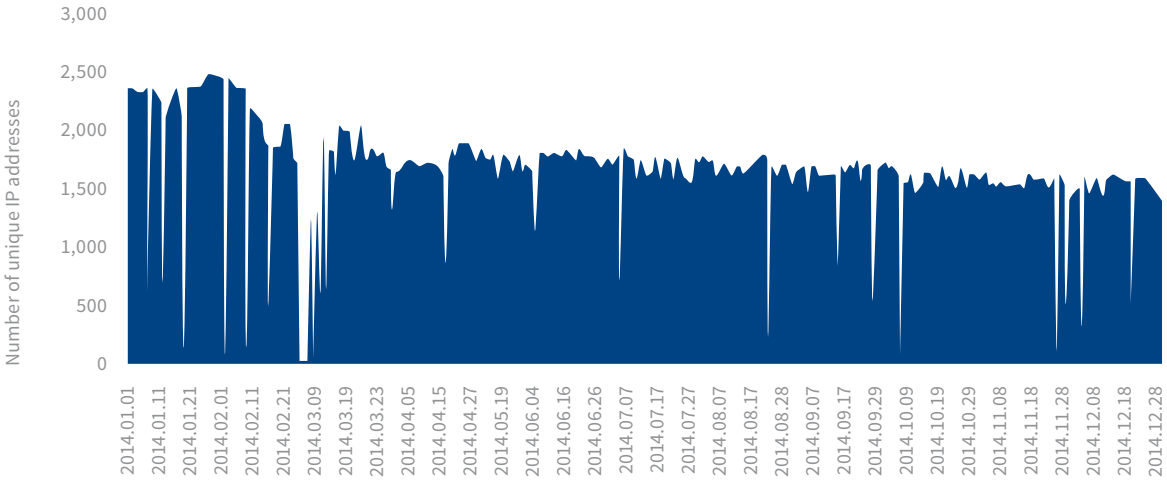


Chart 11. AS6714 – GTS.

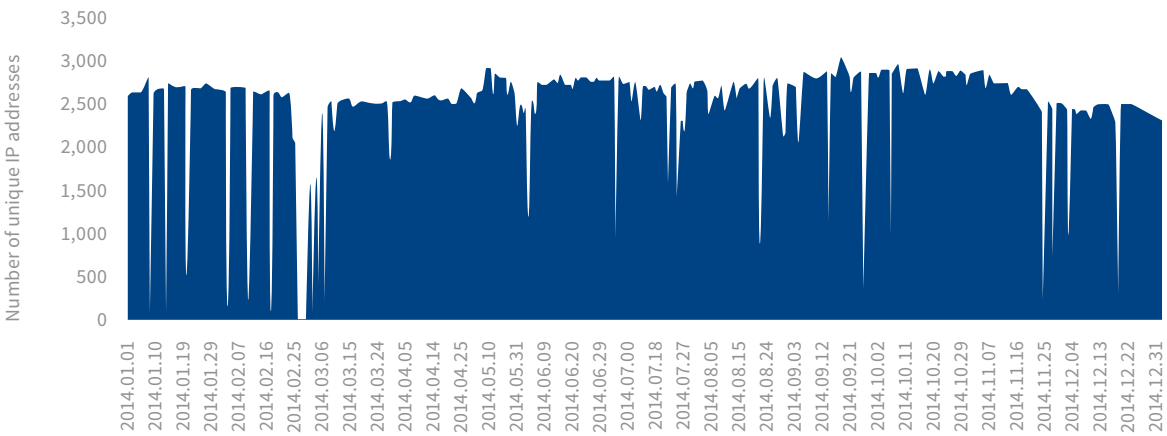


Chart 12. AS21021 – Multimedia.

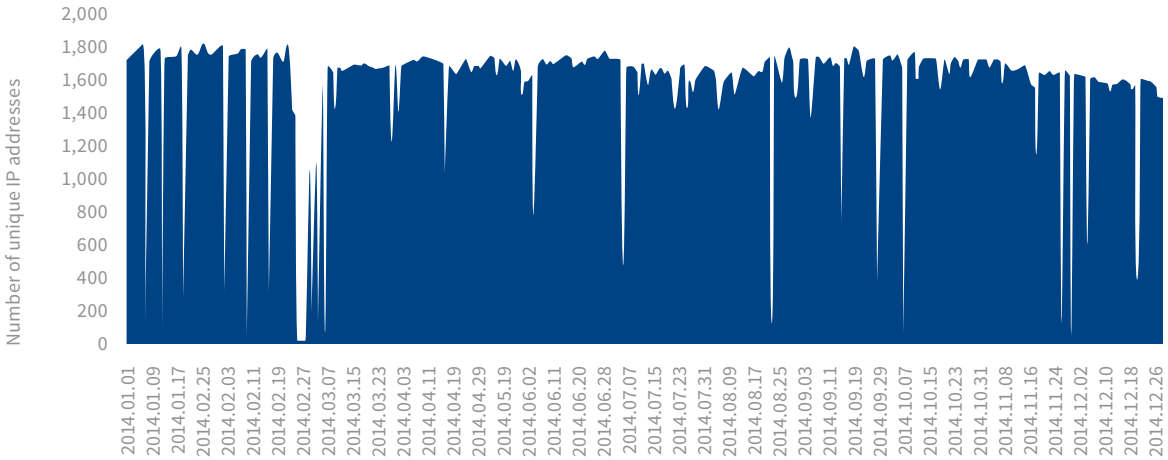


Chart 13. AS29314 – Vectra.

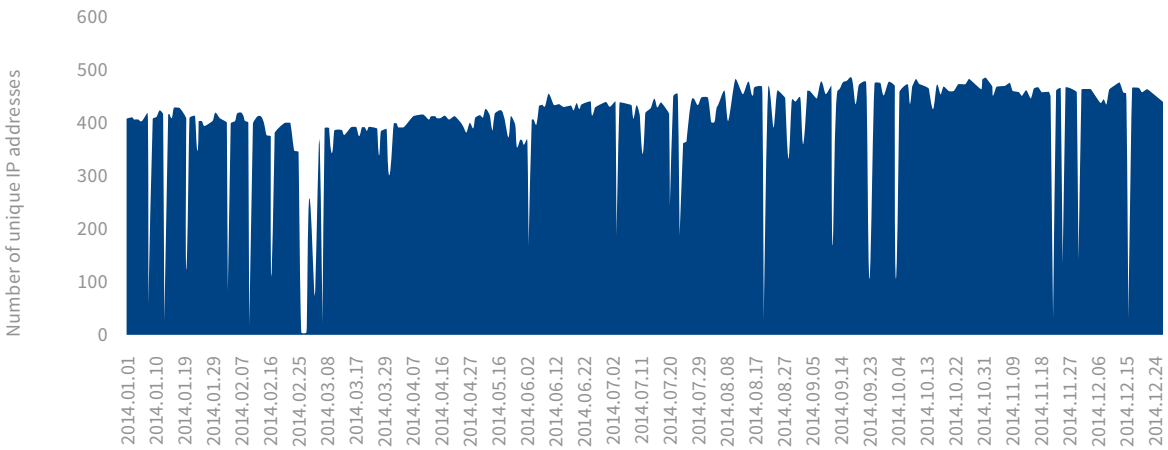


Chart 14. AS12912 – T-Mobile.

Devices with open SNMP service

Most of the devices with open SNMP service are SOHO routers. This was expected, as SNMP is a protocol used to manage network devices and SOHO router are abundant these days. Most of these routers have an SNMP agent enabled by default and their "administrators" – regular Internet users – usually lack knowledge to disable that feature. This increases a DDoS risk for other Internet users.

In 2014 we have received 17,398,675 records about 2,325,483 unique IP addresses, which contained 110,409 unique responses to *sysName* and *sysDescr* queries. In the table 2 we present most common responses to that queries.

	Unique IPs	SNMP response	Vendor
1	1,540,995	TD-W8901G	TP-LINK
2	1,172,505	System Description	–
3	667,374	ADSL Modem	–
4	502,459	Wireless ADSL Gateway	Netgear
5	243,576	AirLive WT-2000A	AirLive
6	177,942	TD-8961ND	TP-LINK
7	76,564	TD-8840T 2.0	TP-LINK
8	70,151	Residental ADSL Gateway	Thomson
9	69,595	802.11n Wireless ADSL 2/2+ Router	Planet
10	58,341	RTL867x System Description	–

Table 2. Most popular responses to SNMP queries.

Most popular SOHO vendor with open SNMP was TP-LINK, although most of the routers were older devices. It seems that newer devices have SNMP disabled by default, which seems to have eliminated the problem. What is more interesting, some of the SNMP responses were coming from the network printers.

The good news is that there is a steady decline in a number of devices with misconfigured SNMP. Breaking data to specific vendors, the decline is also clearly visible. The only vendor that noted an increase in the number of misconfigured SNMP devices is Zhone.

Malware made in Poland

Last quarter of 2013 and whole 2014 saw an emergence of banking malware made by Polish actors. Leading the way was VBKlip, also known as Banapter or ClipBanker. It was based on a really simple idea. VBKlip monitored Windows clipboard and when it found a valid bank account number – 26 numbers with or without spaces – this number was replaced with another one, either hardcoded or downloaded from a C&C server.

Frequently, in order to pay an invoice, users copy the account number from that invoice to clipboard and then paste it to the online banking website. This switch usually goes unnoticed as people rarely compare the two numbers after pasting.

This simple idea was then copied by a numerous number of different malware strains, which we decided to divide into four main families, as shown on the diagram. This diagram also shows connections between different families and actors behind them.

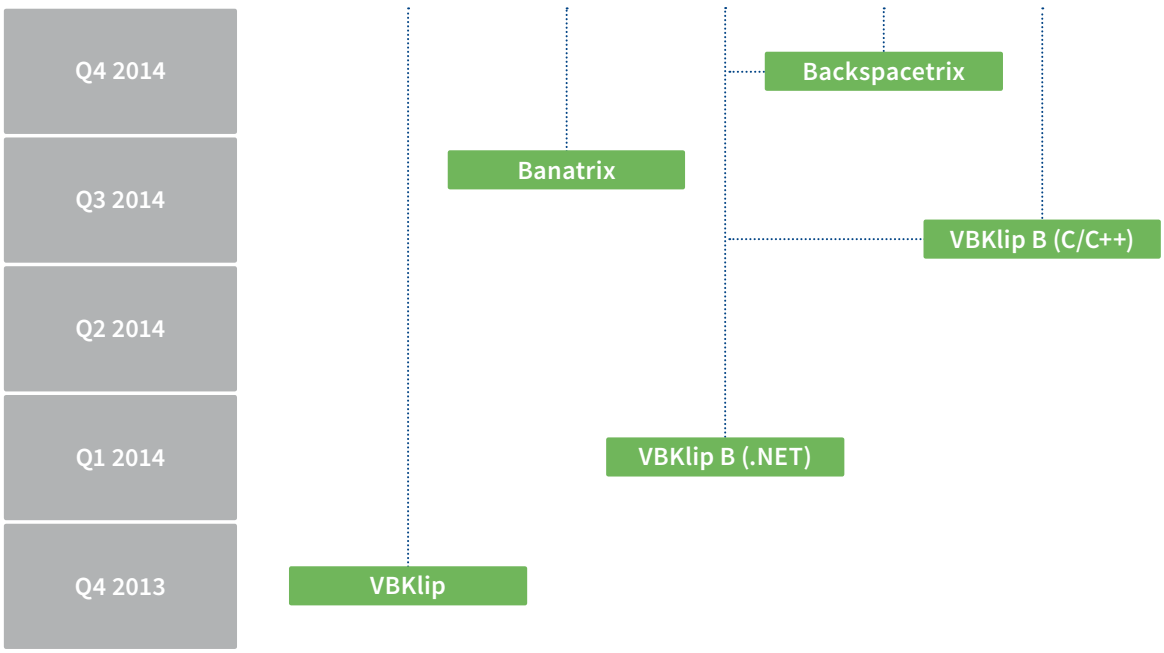


Figure 15. Polish malware development in individual quarters.

VBKlip

This malware is written in Visual Basic 6.0. Both the dropped (part responsible for installing the malware) and the actual malware are written in this language. Whole package is composed of several important components (different processes and programs):

- Component responsible for reporting. It gathers and sends (via SMTP) reports containing, among others, following elements:
  - victim's bank name as seen in the online banking website title,
  - browser name,
  - local time,
  - malware version,
  - money mule account ID.
- Component responsible for the actual bank account number replacement.
- Component, which is responsible for encryption and communication with a C&C server. It also makes sure that all other components are up and running. If one of them stops, this component will restart it.
- Keylogger, which encrypts the keystrokes and saves them into a file. They are then sent with an aforementioned report.

In the few months that this threat was active, it constantly evolved – for example the keylogger functionality was added in later releases. Similarly, the content of reports grew. Newer versions sent e.g. process list to the attackers.

One of the most interesting cases of these types of attacks was a case with two friends, were one wanted to make a loan repayment to the other one. However, lender did not notice that the malware switched his own bank account number when he tried to copy it to e-mail. Hence, the payment was made to the money mule account, despite the fact that the person who made the wire transfer was not infected.

VBKlip.B

This simple idea was quickly copied by another malware author. However, this one lacked the programming skills of the original and wrote a very simple .NET program, which had a hardcoded bank account number and did not communicate with the C&C server. Whole code was several lines long, but we know of some cases in which it succeeded in stealing the money from users. This malware later evolved to C/C++ programming languages, however it was not enriched with any new features.

Banatrix

Of all of the Polish malware families that we have seen in 2014 Banatrix seems to be the most technologically advanced one. This malware was used to replace the bank account number in the browser memory, however its implementation allowed an attacker to execute any arbitrary code on the victim's machine. This was used to extract passwords saved in the Mozilla Firefox browser.

This malware iterates over all active processes and searches for the Internet Explorer, Firefox, Opera or Chrome process by comparing the process names. If it finds such process it then scans its memory searching for 26 digit string (with or without spaces). If it finds such string, it overwrites the string with the one obtained from the C&C server.

However, malware architecture allows for a lot more. The general concept behind this malware is presented in the diagram.

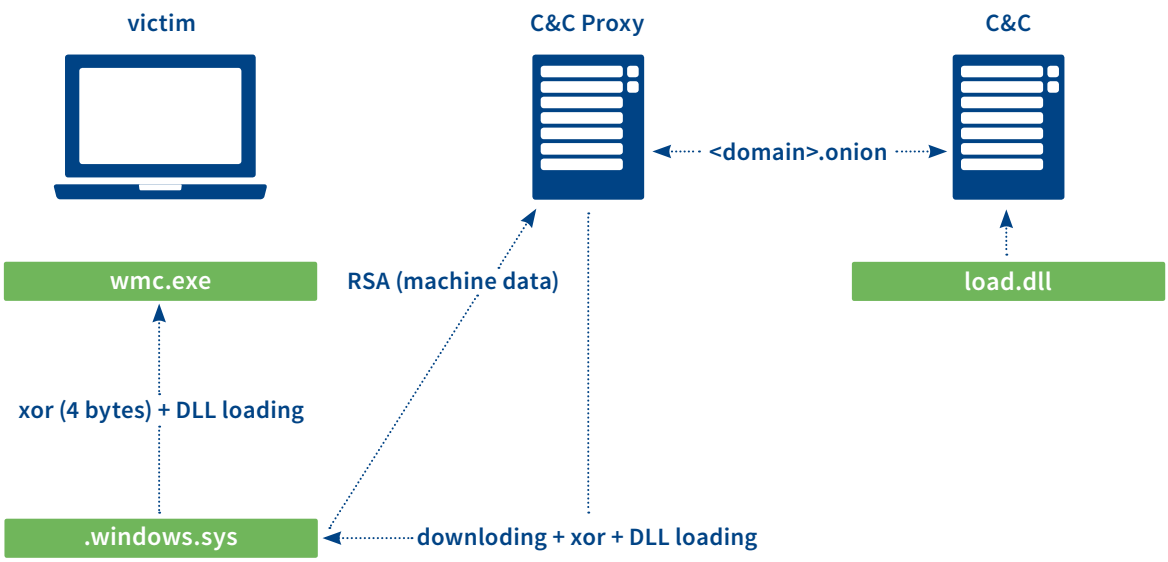


Figure 16. Operating diagram malware Banatrix.

Upon the first run the malware drops two files: xor encrypted DLL and an exe file. The library file is decrypted and loaded into the process memory. It is then encrypted again, using a different, random key and saved with that key to the same file. This results in a different file every time the malware runs. The loaded library then performs 4 steps.

1. It connects to the C&C proxy server, sending some machine info (e.g. OS version or username) and .onion domain, where the real C&C is.
2. C&C proxy connects (using a TOR network) to hidden service and passes the request.
3. C&C proxy get a response from a real C&C and sends it back to the malware. This response contains a xor-encrypted DLL file, which should be executed on user's machine.
4. DLL file is then executed on the victim's machine, but it is never saved. This is probably a forensic countermeasure.

The most recent version of the malware uses a Domain Generation Algorithm to make both the analysis and the sinkholing harder.

Backspacetrix

At the end of 2014 a new kind of threat emerged. VBKlip.B author stole Banatrix idea and created his own malware. Due to the lack of programming skills, he wrote a very simple .NET program, which registered when user entered 26 digits, then emulated shift+backspace presses. This removed the number that user have just entered. Then, this malware emulated pressing 26 digits, which resulted in the same visual effect bank account number just switched right before a user eyes. Again, no C&C communication took place.

Our activities

NATO Locked Shields 2014

In 2014 r. the Polish team which included two members of CERT Polska won a realtime network defence NATO exercise called Locked Shields. The exercise lasted for 5 days, between May 20 and May 24, with participation of 12 teams from 17 nations. Each team had 50 virtual machines in its network that had to be protected against attacks from the Red Team. The machines included IP cameras, pfSense firewall, VoIP systems and Android, all of which are not typically elements of such exercises. The goal of the exercise was not only to defend the resources at the network level (IPv4 and IPv6), but also to detect preinstalled malicious code and compromised systems. Apart from CERT Polska, the Polish team consisted of members of MIL-CERT, Military Counterintelligence, CERT.GOV.PL and Military University of Technology. Locked Shields are organized annually by the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn.

n6

The n6 (Network Security Incident eXchange) Platform is an automated system created by CERT Polska for collection, processing and distribution of data related to computer security. Its goal is to effectively, reliably and timely deliver large volumes of data to relevant parties, such as network owners, administrators and operators. Every day n6 processes millions of events from Poland and the rest of the world and delivers them to more than 200 recipients. More information is available at n6.cert.pl.

In 2014 we started a test implementation of a new version of the system, with new capabilities. From the user's point of view, the most important change is a consistent API available for all types of data offered by the platform. It simplifies access to the system, particularly with external security monitoring systems such as IDS and SIEM.

In December 2014 a significant part of n6 code was made available publicly with GPL licence to lower technical barriers in information sharing across different organizations. The open component is a Python library – n6sdk – that allows to easily connect data sources (eg. SQL databases) and share data to authenticated users through an n6-compliant RESTful API.

› More information and Git repository of the code is available at GitHub: https://github.com/CERT-Polska/n6sdk

NECOMA Project

We continued our efforts in the European-Japanese joint project NECOMA (Nippon-European Cyberdefense-Oriented Multilayer threat Analysis). NECOMA is a research project started in 2013, aimed at strengthening IT security through increasing resilience to existing and new threats.

Foundations of NECOMA were laid out in our previous Annual Report. In 2014, NASK employees published a number of articles related to results of research done within the project[12]. We have also further developed the n6 Platform to exchange data between partner organizations, leading to publishing of n6SDK (see above).

The project is financed by the Japanese Ministry of Internal Affairs and Communications and European Union, as a part of the Seventh Framework Programme (FP7/20072013), Grant No. 608533.

› Detailed information about NECOMA, news and publications are available at: www.necoma-project.eu

[12] "Comparative study of supervised learning methods for malware analysis", http://www.itl.waw.pl/czasopisma/JTIT/2014/4/24.pdf

OUCH!

"What is Malware?", "Securing Your Home Network", "I'm Hacked. Now What?" – these are just some of the subjects covered by SANS "OUCH!" in 2014. "OUCH!" is a free monthly bulletin for computer users with practical advice on IT security. Each edition covers a single accessibly presented topic along with a list of hints and tips on how to protect oneself, friends and family, as well as organizations.The bulletin is available in 23 languages.

Thanks to the cooperation between CERT Polska and the SANS Institute, Polish edition of the bulletin is available since April 2011. Each bulletin is created and reviewed by the SANS "Securing The Human" team, recognised providers of on-line security related content. Authors are experts in IT security, auditors and administrators. CERT Polska makes a localized version of each bulletin, not only translating its content, but adjusting it to Polish environments.

The bulletin's intended audience are users without broad knowledge about computer security, and all topics are described in a manner accessible to an average user. CERT Polska encourages distribution of "OUCH!" in enterprises, educational institutions and homes, in particular among users who lack advanced knowledge about IT security. The more the users become aware of threats, the harder it will be for the criminals to act.

› All Polish editions of "OUCH!" can be found at: http://www.cert.pl/ouch. For English edition and other languages visit: www.securingthehuman.org/resources/newsletters/ouch/

NISHA Project

NISHA *(Network for Information Sharing and Alerting)* Project, the goal of which was dissemination of information about online safety and creation of pilot network of information portals, ended in March 2014. The consortium members were CERT Polska (NASK), national CSIRT teams of Hungary and Portugal, and German Institute for Internet Security (Westfälische Hochschule). The news portals set up during the project continue to exchange information about computer security and share them locally in their local languages. The Polish portal is available at http://nisha.cert.pl.

Additionally, each partner's goal was to reach home users as well small and medium enterprises with NISHA content. The reasoning behind such a focus group was that is has a key role in Internet security due to its sheer size along with insufficient knowledge about threats, which makes it an easy target of cybercriminals. For this task, each of the partners has organized meetings to present the project and possibilities to get involved in content sharing. A meeting hosted by CERT Polska took place on February 27 at NASK's premises. The main topic was effective information flow from news producers to consumers in IT security world.

NISHA: Łukasz Siewierski presents "Underground Economy".

Workshop participants discussed ways of reaching average users with IT security related information. A crucial element in this process is the involvement of intermediaries in information distribution – media, educational institutions, companies and enterprises – which at the same time are also prone to being attacked. The workshop focused on possibilities, needs and existing problems between different actors in the process of making expert information and intermediaries in reaching the end user.

The meeting helped in identifying fundamental problems in delivering information about current threats. The main reason of lack of interest among average users is inadequateness of language used to convey the message – often too technical, full of terms that only experts would understand. Furthermore, there is still no coherent basic knowledge base on computer security available for end users. Such base would be very beneficial in creation of educational materials and understandable articles describing current threats.

In Poland, there are many competent institutions capable of producing valuable educational material on IT security. However, they usually have problems in reaching end users. On the other hands, the users usually have no incentives to seek information and educate themselves. Hence, there is a great potential in cooperation between experts delivering reliable, professional information and entities able to reach a wider audience with technical information provided in accessible form.

The NISHA Project was cofinanced by the European Commission as part of "The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks" (CIPS) Programme

European Cyber Security Month

In October 2014, for the third time in Europe and for the second time in Poland, the European Cyber Security Month was organized – a European campaign to disseminate knowledge about IT security. As part of the ECSM, European Commission supported several initiatives of EU countries towards education of cybercitizens. NASK and CERT Polska joined the campaign, creating bezpiecznymiesiac.pl (*secure month* in Polish) a webpage presenting events initiated by NASK during the campaign.

One of the events was a knowledge quiz "Security in the Internet" for all Internet users, with a goal to test their familiarity with the topic of IT security. The quiz is still available at the Polish NISHA portal (http://nisha.cert.pl/quiz). The questions cover security issues discussed by "OUCH!", published monthly by SANS Institute and CERT Polska. The quiz is not just a test, but also an educational tool, because each question is commented by an expert and has references to source material, explaining the respective topic in accessible form.

Another initiative was targeting university students and involved a HackMe challenge. The task required participants to extract encrypted files from a traffic dump in PCAP format. The difficulty level turned out not to be too high and we have received answers before the deadline. The fastest correct solutions were awarded with book prizes.

› The challenge (and solution) is available at: http://www.cert.pl/news/9120.

SECURE 2014

SECURE 2014 took place on October 22-23 at Copernicus Science Centre in Warsaw with over 350 participants who could select from 39 talks by 47 authors. As usual, the conference was preceded by SECURE Handson workshops, delivered by trainers from CERT Polska.

The opening keynote was "The Arms Race" by Mikko Hypponen – a renowned security specialist from F-Secure. It wasn't the first time when Mikko was speaking at SECURE, this time giving an excellent introduction into current security landscape. He was followed by Stephen Brannon from Verizon and Ilkka Sovanto from NCSC-FI. Brannon presented Verizon Breach Report – a unique approach to global threat analysis with involvement of dozens of researchers and companies from around the world (including CERT Polska). Ilkka Sovanto discussed the process of vulnerability analysis and disclosure, using a very visible example of Heartbleed, which Sovanto was personally involved in. In parallel sessions there was no lack of deeply technical presentations, including Mateusz "j00ru" Jurczyk on risks assosciated with malware analysis and Maciej Kotowicz on malicious email attachments purporting financial documents. Softer topics included an interesting analysis of spectacular TOR users' failures by Adam Haertle. One of the tracks was dedicated to security of little known or explored systems, eg. unmanned aerial vehicles (LogicalTrust), VLC networks (Grzegorz Blinowski, Warsaw University of Technology) and embedded systems (firmware.re).

On the second day, plenary talks included Bill Hagestad's (Red Dragon Rising) coverage of activities of Chinese and Russian criminals as well as Jart Armin's (Cyberdefcon) attempt to describe impact of cybercrime on economies with concrete metrics. Armin also discussed CyberROAD – the project where CERT Polska teams up with Cyberdefcon and many other researchers to create cybercrime and cyberterrorism research roadmaps (see page 36). Parallel sessions included, among others, Nikolay Koval from Ukrainian government CERT, Michał Sajdak (sekurak.pl) and Jurriaan Bremer (co-author of Cuckoo Sandbox).

The conference concluded with prize draws in many contests and challenges prepared by the organizers and conference partners, including Capture The Flag by DragonSector team.

› Conference slides are available at http://www.secure.edu.pl/historia/2014/program.php and video recordings at http://goo.gl/y6kaSC

ENISA Report "Actionable Information for Security Incident Response"

In 2014 experts from CERT Polska were contracted by ENISA to write a report on "Actionable Information for Security Incident Response". The publication is dedicated for members of incident response teams, as well as everyone who collects, analysis or shares information on IT security and threats.

The "actionable information" covers a wide range of information which can be used to trigger concrete actions towards mitigation or elimination of threats. CERT Polska has been involved in exchange of such information for years, mainly through its n6 platform (see XXXX). However, in our opinion, existing publications did not sufficiently describe and discuss associated problems. Hence, our main goal during writing of the report was to create a comprehensive overall presentation of processing of different types of information by incident response teams.

The report defines "actionable information" in the context of computer security, identifies its key properties and proposes a generalized model of processing of data by incident response teams. We have included three detailed case studies in the areas of: application of indicators of compromise to repulse a targeted attack, botnet monitoring for increased situational awareness, and efficient data sharing on national level.

The report is complemented with a practical exercise to illustrate application of available free opensource tools to process information and repulse attacks, and a reference document describing 53 technical standards essential in information exchange and 16 publicly available systems for processing and managing security related information.

› The documents are available at ENISA website[13]:

- Actionable information for security incident response
- Standards and tools for exchange and processing of actionable information
- Exercise: Using indicators to enhance defence capabilities [PDF]

[13] ENISA: www.enisa.europa.eu

The CyberROAD Project

CyberROAD is a research project funded by European Commision within FP7, with the objective to identify current and future problems in tackling cybercrime and cyberterrorism, as well as development of roadmap for future research. The first steps in the project are to a picture of the current situation of technological, social, economic, political, and legal environments, which contribute to the development of cybercrime and cyberterrorism. The collected scenarios describing this situation will then be addressed in order to identify gaps, future possible developments and research priorities. As part of the research on cybercrime it was decided to focus on Poland as an example country for which a comparative analysis of this phenomenon with the other countries of Europe and the world will be made. Publicly visible activity of the project was the publication of a survey on cybercrime. CyberROAD project started in May 2014 and will last 24 months. It brings together 20 institutions from 11 countries, with Poland represented by NASK, and CERT Polska in particular.

› More information can be found on the project website: http://www.cyberroad-project.eu/

Verizon DBIR Report

In 2014 CERT Polska participated in a project run by Verizon (a large American Internet service provider) to create a worldwide *Data Breach Investigations Report*. The report covers analysis of data and statistics gathered from 50 different organisations from around the globe, about confirmed security incidents. More than 63 000 incidents were combined, affecting 95 countries. 92% of the incidents could be reduced to 9 basic attack scenarios. Among the most important scenarios, notable examples were dynamically growing numbers of successful POS (Point of Sale) compromises with malicious software, web application attacks, cyberintelligence attacks and credit card skimmers. CERT Polska's contribution to the report included also a paragraph on banking trojan and financial scams in Poland.

› The Verizon DBIR Report is available at http://www.verizonenterprise.com/DBIR/2014/

ILLBuster Project

The goal of ILLbuster, a project which started in 2014, is to create a system for automated discovery and analysis of malicious and illegal websites. Detection will be based on DNS traffic analysis, and the system should be able to discover sites with malicious code, child pornography, phishing and counterfeit product offers. NASK is the leader of the technical part – ILLBuster uses the n6 platform as a data source, and the scanner is based on Honey Spider Network 2 developed in CERT Polska.

The project is funded by the European Commission (DGHOME) within the programme „Prevention of and Fight against Crime" (ISEC HOME/2012/ISEC/AG/4000), and is realized by the consortium of Italian universities – Università de Cagliari and Università degli Studi di Milano-Bicocca, American University of Georgia, Italian Police Forces – Guardia di Finanza and Polizia Postale, a Swedish enterprise Netclean, an Italian NGO – Tech and Law Center, and CERT Polska.

› More information about the project: http://pralab.diee.unica.it/en/ILLBuster

The Honeynet Project Security Workshop in Warsaw

12-14 May were the days of the 2014 edition of The Honeynet Project Security Workshop. This worldwide known conference attracts IT security experts for many years. Last year edition was held in Warsaw, Poland, and was attended by over 160 participants from around the world. CERT Polska members and The Polish Chapter of The Honeynet Project actively participated in preparations, contributing to making the agenda, promotion, finding sponsors, and local logistics.

The conference agenda included talks on current trends in development of malicious software and countermeasures, as well as demos of tools for data analysis and detection of attacks on infrastructure. The last day of the event was devoted to workshops on reverse engineering in Windows and Android systems, securing infrastructure based on virtualization, and botnet mitigation with tools developed by members of The Honeynet Project Foundation.

Public appearances

In 2014 CERT Polska members conducted 5 workshops and 4 trainings, gave 29 talks and presentations on various conferences and seminars, and participated in panel discussions.

CERT Polska organized two major events – the annual conference SECURE 2014 and a workshop on the NISHA project, and supported The Honeynet Project Security Workshop 2014.

Apart from local conferences and events, CERT Polska members presented – among other places – at FIRST Symposium in Zurich (CH), APWG eCrime 2014 in Birmingham, AL (US), FIRST Annual Conference in Boston, MA (US) and Botconf in Nancy (FR).

ARAKIS 2.0 – The next generation EWS

ARAKIS is a modular early warning system against network threats. Its main task is automated discovery of attack patterns by heuristical analysis of network traffic. The first version of ARAKIS was developed in 2007, and in 2014 – based on experience from ARAKIS 2 – work on the second version was concluded. The main goal is unaltered, but the ways it is now realised have substantially changed the system was designed and developed from scratch.

ARAKIS 2.0 is based on cuttingedge algorithms for detection of repeating threat patterns. Network traffic is collected by a distributed network of sensors and parallely subjected to a number of analysis in the central computing cluster. While the main source of data remains nonproduction traffic from honeypots, the traps have been replaced with newer, more interactive ones, able to deal with modern attacks, eg. on web applications, SSH or SCADA systems. The honeypots were placed in a cloud (honeyfarm), making them less prone to failures, easier to manage and update. In addition, the system was extended with capabilities to optionally analyse production traffic inside corporate networks and logs from production web servers. To provide maximum privacy and not interact with confidential information sent over protected networks, the analysis is based on network protocol headers up to level 4, without actual content. ARAKIS 2.0 is fed with knowledge from the n6 platform, as well as indicators of compromise provided by CERT Polska analytics. Thus, the system always uses current information on C&C servers, malicious IP addresses, phishing etc. to detect threats inside networks it protects.

Apart from the advanced analysis, it is equally important to present their findings to the user in a friendly way. Consumers of ARAKIS 2.0 are mainly IT security specialists, so a priority has been given on versatility and flexibility of querying and displaying of information, correlation of findings and presentation. AQL (ARAKIS Query Language) can be used to run queries on any data in the system, provides several statistical functions, and allows to present results as tables, maps, or one of eight different types of charts. With AQL the user can create periodic reports with varying levels of complexity from a simple statistical summary to a detailed investigation report.

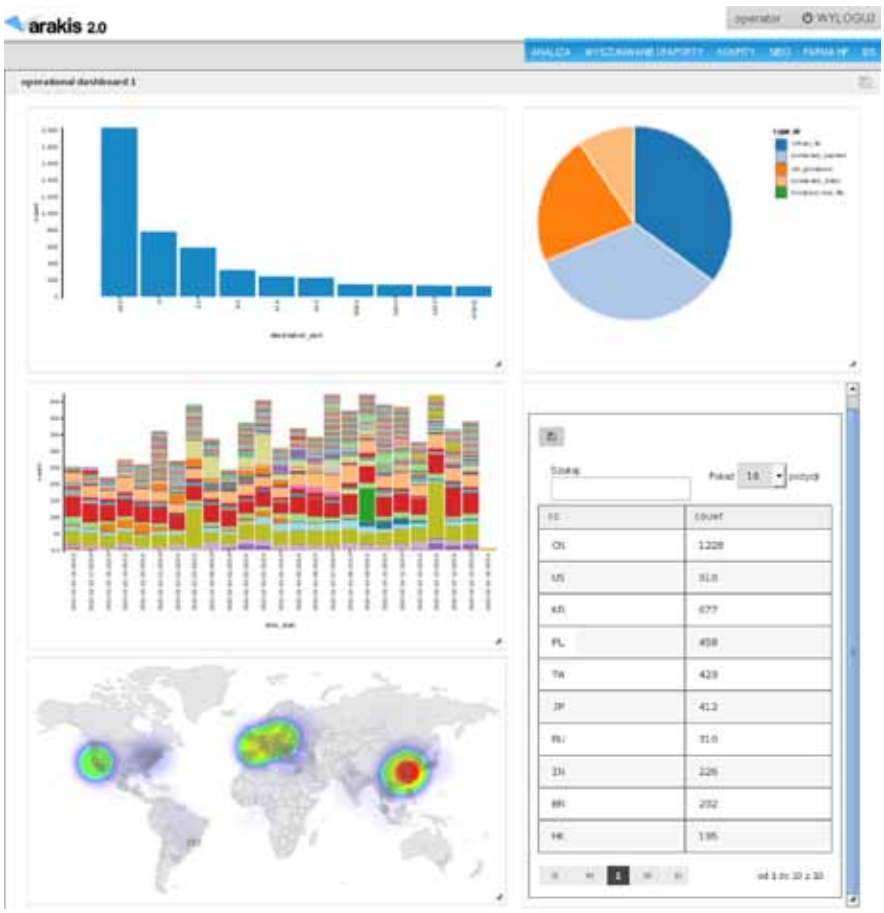


Figure 17. ARAKIS 2.0 – AQL query results.

Development of ARAKIS 2.0 took 2 years, based on an agreement between NASK and the Ministry of Science and Higher Education of Poland. At NASK, staff involved in the project included members of Software Development Department, CERT Polska and the Laboratory of Methods of Security of Networks and Information in the Scientific Department.

Statistics

Botnets in Poland

This section describes data from the n6 platform about botnets active in Poland. Raw numbers are presented in the tables below.

Based on the data we have about 280,000 machines in Poland are infected with some kind of malware on an average day. The actual numbers are probably higher by some 10-20 percent.

	Percentage of infected IP addresses	Maximum daily number of unique infected IP addresses	AS Number	Operator
1	4.02%	27,354	12912	TMobile Polska
2	2.44%	15,607	39603	P4 (Play)
3	2.31%	13,693	21021	Multimedia Polska
4	2.09%	30,520	12741	Netia
5	1.71%	9,051	29314	Vectra
6	1.68%	92,340	5617	Orange Polska
7	1.54%	3,837	20960	TK Telekom
8	1.44%	19,099	8374	Plus
9	0.95%	14,544	6830	UPC Polska
10	0.78%	2,528	43939	Internetia

Table 1. Infections in Polish networks.

Table 1 shows percentage of IP addresses from a given operator in pool of data about infections. The first four positions did not change in comparison to 2013, but T-Mobile's advantage has significantly dropped. The absolute number of unique IP addresses seen as infected has risen for all operators. It must be noted that some operators, in particular mobile ones, use very short lease times for IP addresses (much shorter than a day). As a consequence, their daily numbers are likely overstated in comparison to numbers of infected machines.

	Botnet	Number of IP addresses	Percentage
1	Conficker	62,221	22.19%
2	ZeroAccess	32,460	11.57%
3	Zeus (w tym Citadel i pochodne)	25,311	9.03%
4	Sality	14,003	4.99%
5	Zeus GameOver	12,513	4.46%
6	Ircbot	10,768	3.84%
7	Bankpatch	6,086	2.17%
8	Banatrix	5,385	1.92%
9	Virut	4,014	1.43%
10	Kelihos	3,922	1.40%
	other:	103,750	37.00%

Table 2. The largest botnets in Poland.

The biggest botnet in Poland remains Conficker, although its "market share" has dropped by 4.6 percentage points. The second one is ZeroAccess, which came third in 2013. The third largest botnet is Zeus which we counted together with Citadel and their variants. Its share has increased by almost 2 percentage points. It should be noted that Sality has plummeted from the second place (14%) in 2013 to only fourth (5%) last year.

Conficker and Virut are two botnets, over which criminals have no control. Hence, they are not active anymore. Conficker has been sinkholed since 2009, and Virut since 2013 (mostly by CERT Polska). Their presence in the table is the evidence to the fact that many computers remain infected years after the compromise, often for the lifetime of its hardware. In addition, Conficker is a worm that spreads not only through vulnerabilities in the operating system, but also using removable drives. Virut on the other hand is a virus that attaches to executable files and documents. While it is more difficult for Virut spread than for Conficker, there are still new infections from files that can be downloaded from old web sites.

Out of ten largest botnets in Poland, four are built with banking trojans.

	Botnet	Number of IP addresses	Percentage
1	Zeus	25,311	45.80%
2	Zeus Gameover	12,513	22.64%
3	Bankpatch	6,086	11.01%
4	Banatrix	5,385	9.74%
5	Gozi	2,752	4.98%
	other:	3,218	5.82%

Table 3. Banking trojans.

Table 3 shows number for botnets threatening users of internet banking services. Most banking trojans use a mechanism of "webinjects" to modify contents of banking transaction system website before it is displayed to the user by the browser. Banatrix, first seen by CERT Polska in 2013, employs other method, swapping account number in the browser process's memory.

Statistics of incidents handled

This part of the report presents statistics on incident reports that were handled manually by our team. They are mostly serious incidents, or ones where our team can take direct actions, rather than just forward information to appropriate network administrators. The incidents are reported by internal systems, as well as external parties.

Type of incident	Number of incidents	Percentage
Abusive Content	370	28.86
Spam	365	28.47
Harassment	0	0
Child/Sexual/Violence	2	0.16
Other	3	1
Malicious Code	98	7.64
Virus	0	0
Worm	0	0
Trojan	8	0.62
Spyware	0	0
Dialer	0	0
Other	90	7.02
Information Gathering	98	7.64
Scanning	13	1.01
Sniffing	0	0
Social Engineering	0	0
Other	5	0.39
Intrusion attempts	36	2.81
Exploiting of Known Vulnerabilities	4	0.31
Unauthorized Login Attempts	5	0.39
New Attack Signature	1	0.08
Other	26	2.03
Intrusions	13	1.01
Privileged Account Compromise	1	0.08
Unprivileged Account Compromise	7	0.55
Application Compromise	0	0
Other	5	0.39
Availability	69	5.38
DoS	6	0.47
DDoS	63	4.91
Sabotage	0	0
Other	0	0
Information Security	25	1.95
Unauthorized Acces to Information	8	0.62
Unauthorized Modification of Information	0	0
Other	17	1.95
Fraud	613	47.82
Unauthorized Use of Resources	5	0.39
Copyrights	0	0
Masquerade (Identity Theft, Phishing)	383	29.88
Other	225	17.55
Other	40	3.12

Table 4. Incidents handled manually.

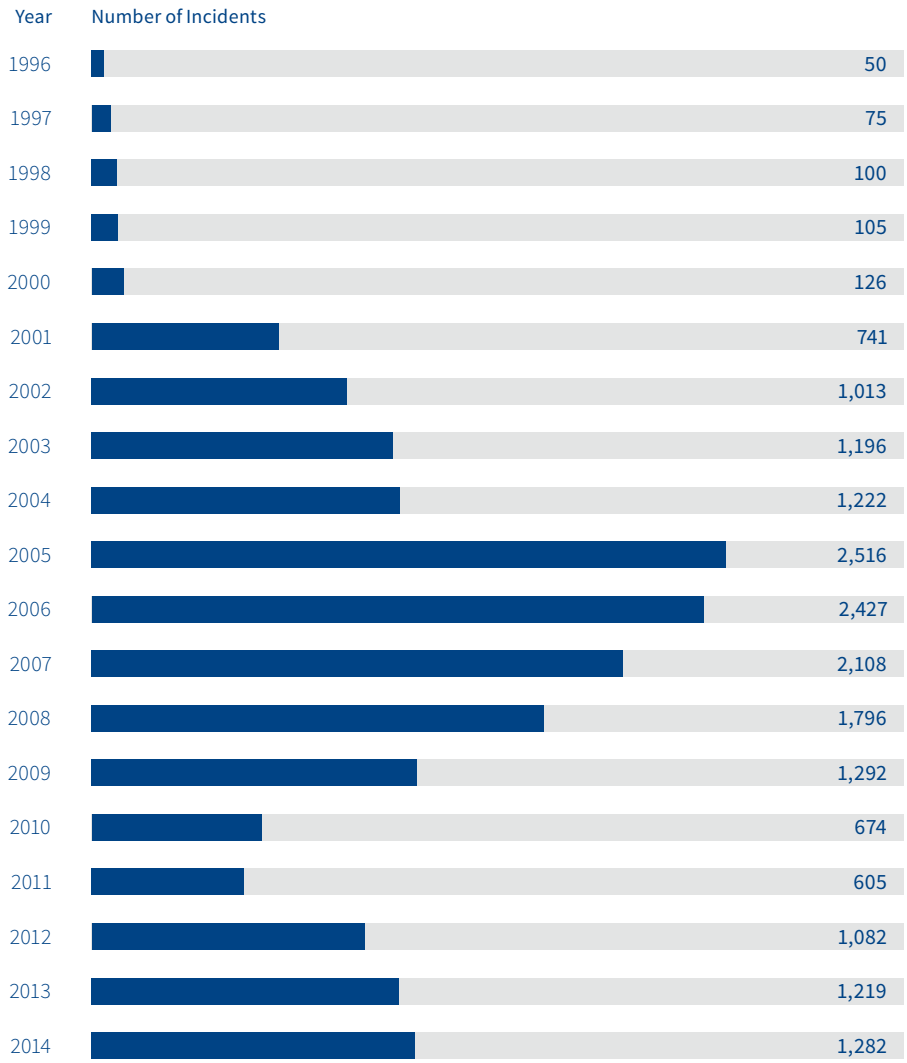


Figure 18. Incidents handled manually.

In 2014 CERT Polska manually handled 1,282 incidents. Most of them involved either some kind of a computer fraud (47.28%) or illegal content (28.86%).

Reporters as well as victims of incidents were usually commercial companies (59.44% and 47.11% respectively), with significant majority of reporters from abroad (66.69%) and victims usually from Poland (31.59%).

In 2014 we handled a large of number incidents involving phishing (29.88%) – it should be noted that they were mostly fake web pages on Polish servers, or phishing sites purporting Polish companies. Over the year we have noted several large campaigns against Polish users of online banking systems. In just a single campaign criminals distributed about 20 different URLs, all hosting the same phishy content. As in previous years, the global scale of the phenomenon was much bigger than what we observed at CERT Polska.

There was a significant drop in percentage of incidents concerning malicious code from 26.26% in 2013 to 7.64% last year. As it happened before, the ways malicious software evolve have forced us to review the ways we handle and classify incidents. Most of the incidents concerned malicious software that targeted Polish users in some way. Consequently, we used one incident to handle a whole campaign, distinguished by its target (in most cases a specific group of online banking users) and infrastructure (eg. C&Cs, ATSs). Within the campaign there can be between a few and a few dozens of reports about the same instance of malware.

A new phenomenon in 2014 is a large number of computer fraud incidents marked as "Other" (17.55%). They're incidents connected to campaigns targeting online banking users, and they concern mule accounts used by criminals. They are used in connection with different types of malicious software – from fake invoices to VBKlip.

It should be stressed that increased activities against online banking customers are the most important and at the same time most threatening trend in 2014. We've observed criminals apply all known and some previously unknown scenarios to steal money, and the amounts transferred fraudulently were often six-digit numbers.

C&C Servers

In 2014 we received (on average) 147 reports per day about new IP addresses and domain names used as C&C servers. Over the year we have received information about 8,304 unique IP addresses and 7,646 unique domain names used for managing botnets.

Below we describe the statistics from the point of view of location of IP addresses, as well as the TLDs of C&C domains.

IP Addresses

We received reports about IP addresses from 104 countries. Similarly to previous years, most of them were located in the United States (almost 29%). Over 70% of C&C servers were hosted in just 10 countries, as shown in the table below.

	Country	Number of IP addresses	Percentage
1	United States	2,397	28.7%
2	Ukraine	706	8.5%
3	Germany	629	7.6%
4	Russia	603	7.3%
5	The Netherlands	319	3.8%
6	France	296	3.6%
7	United Kingdom	249	3.0%
8	Uruguay	242	2.9%
9	Canada	236	2.8%
10	Greece	204	2.5%
...	...	...	...
16	Poland	76	0.9%

Table 5. Countries hosting the highest number of C&C servers.

We have observed C&Cs in 1,626 different autonomous systems. Almost one in five malicious servers was located in one of top ten autonomous systems.

	AS number	Operator	Number of IP addresses	Percent age (globally)
1	16276	OVH Systems	332	4.0%
2	6057	Administracion Nacional de Telecomunicaciones	242	2.9%
3	3320	Deutsche Telekom AG	168	2.0%
4	24940	Hetzner Online AG	167	2.0%
5	6799	Ote SA (Hellenic Telecommunications Organisation)	160	1.9%
6	13335	CloudFlare, Inc.	137	1.6%
7	36351	SoftLayer Technologies Inc.	124	1.5%
8	26496	GoDaddy.com, LLC	102	1.2%
9	15895	„Kyivstar" PJSC	100	1.2%
10	47583	Hostinger International Limited	98	1.2%

Table 6. Autonomous systems hosting the highest number of C&Cs.

C&C servers in Poland were hosted on 76 different IP addresses (0.9% globally) in 36 autonomous systems. The table 7 shows 14 autonomous systems in Poland with the highest number of C&Cs.

	AS number	Operator	Number of IP addresses	Percentage (in PL)
1	59491	Livenet Sp. z o.o.	10	13.2%
1	51290	HOSTEAM S.C.	10	13.2%
3	12824	home.pl sp.z.o.o. 5 6,6%	5	6.6%
3	198540	Przedsiebiorstwo Uslug Specjalistycznych ELAN mgr inz. Andrzej Niechcial	5	6.6%
5	15967	nazwa.pl S.A.	4	5.3%
6	49792	IONICPLAS	2	2.6%
6	15694	ATM S.A.	2	2.6%
6	43939	Internetia Sp.z o.o.	2	2.6%
6	12618	PLBYDMANCOM	2	2.6%
6	42154	„EuroNet" s.c. Jacek Majak, Aleksandra Kuc	2	2.6%
6	6714	GTS Poland Sp. z o.o.	2	2.6%
6	198414	BiznesHost.pl sp. z o.o.	2	2.6%
6	5617	Orange Polska Spolka Akcyjna	2	2.6%
6	197226	„SPRINT"	2	2.6%

Table 7. Polish autonomous systems hosting highest number of C&Cs.

Domain names

We have received reports about 7,647 fully qualified domain names that were used for botnet management. They were registered in 137 top-level domains, with almost 30% in .com.

	TLD	Number of domain names	Percentage
1	.com	2,241	29.3%
2	.net	1,058	13.8%
3	.org	590	7.7%
4	.info	532	7.0%
5	.ru	357	4.7%
6	.de	249	3.3%
7	.biz	237	3.1%
8	.su	198	2.6%
9	.in	186	2.4%
10	.br	152	2.0%

Table 8. Top-level domains where C&C domain names were registered.

Malicious websites

In 2014 CERT Polska received 21,231,896 reports about unique malicious URLs, 593,136 of them concerning unique URLs in .pl domain.

Malicious websites in .pl

On average, we received 1,625 unique URLs in .pl per day.

	Unique URL addresses	Domain name
1	46,942	mattfoll.eu.interiowo.pl
2	12,832	premiumfilmy.pl
3	7,707	interiowo.pl
4	5,639	bialydom.pl
5	5,325	static.sd.softonic.pl
6	5,105	aanna74.eu.interiowo.pl
7	4,904	prywatneznajomosci.cba.pl
8	4,630	polityczni.pl
9	4,521	gim8.pl
10	4,053	meczyk.pl

Table 9. Fully qualified domain names with most unique malicious URLs.

Table 9 shows fully-qualified domain names in pl where, according to our data feeds, most malicious URLs were located.

	Number of unique URLs	IP address	ASN	Operator
1	57,393	217.74.66.183	AS16138	INTERIA.PL Sp z.o.o.
2	44,722	217.74.65.161	AS16138	INTERIA.PL Sp z.o.o.
3	21,799	217.74.65.163	AS16138	INTERIA.PL Sp z.o.o.
4	11,950	193.203.99.113	AS47303	Redefine Sp. z o.o.
5	8,973	46.41.144.24	AS12824	home.pl sp. z o.o.
6	8,737	193.203.99.114	AS47303	Redefine Sp. z o.o.
7	8,438	95.211.144.89	AS16265	LeaseWeb B.V.
8	7,378	217.74.65.162	AS16138	INTERIA.PL Sp z.o.o.
9	6,101	85.17.73.180	AS16265	LeaseWeb B.V.
10	5,569	37.59.49.187	AS16276	OVH SAS

Table 10. IP addresses hosting most malicious URLs.

Table 10 shows IP addresses, where most malicious URLs were located. Similarly to 2013, top of the table is dominated by Interia – a large hosting and content provider. Table 11 presents autonomous systems hosting most malicious URLs, featuring home.pl, OVH, Onet and Interia.

	Number of unique URLs	ASN	Operator
1	132,170	16138	INTERIA.PL Sp z.o.o.
2	89,178	12824	home.pl sp. z o.o.
3	31,244	16276	OVH SAS
4	27,061	47303	Redefine Sp. z o.o.
5	23,510	16265	LeaseWeb B.V.
6	23,497	15967	Netia SA
7	18,499	24940	Hetzner Online AG
8	9,694	29522	Krakowskie e-Centrum Informatyczne JUMP
9	8,869	12741	Netia SA
10	7,098	12990	Grupa Onet.pl S.A.

Table 11. Autonomous systems hosting most malicious URLs in .pl.

Table 11 shows countries, in which servers with malicious .pl URLs were located. As expected, overwhelming majority of them was in Poland. The rest of the table does not significantly differ from 2013.

	Number of unique URLs	Country
1	404,364	Poland
2	27,484	Germany
3	21,459	The Netherlands
4	19,242	France
5	7,169	United States
6	5,395	Spain
7	1,683	United Kingdom
8	786	Canada
9	353	Czech Republic
10	289	Russia

Table 12. Countries, in which malicious .pl URLs were hosted.

Global data

On average we received 58,169 malicious URLs per day.

Table 13 shows domain names in which, according to our data feeds, most malicious URLs were located.

	Unique URLs	Domain name
1	223,473	hao.ie768.com
2	172,607	download.goobzo.com
3	163,088	www.horizoncardservices.com
4	152,444	down.llrx.org
5	146,734	dde.de.drivefilesb.com
6	110,637	s1.upgrade.mkjogo.com
7	107,273	www.iblowjob.com
8	100,320	dc589.2shared.com
9	98,524	esd.nzs.com.br
10	86,000	kyle.mxp4037.com

Table 13. Fully-qualified domain names, where most malicious URLs were located.

	Unique URLs	IP address	ASN	Operator	Country
1	294,226	222.186.60.12	23650	CHINANET jiangsu province backbone	China
2	290,889	222.186.60.2	23650	CHINANET jiangsu province backbone	China
3	237,944	222.186.60.44	23650	CHINANET jiangsu province backbone	China
4	202,698	123.150.206.130	17638	ASN for TIANJIN Provincial Net of CT	China
5	200,426	118.121.252.162	4134	Chinanet	China
6	190,026	5.135.246.48	16276	OVH Systems	France
7	172,763	107.20.238.80	14618	Amazon.com, Inc.	United States
8	163,088	67.192.100.25	33070	Rackspace Hosting	United States
9	143,243	115.29.226.120	37963	Alibaba (China) Technology Co., Ltd.	China
10	141,740	103.249.72.30	132827	GATEWAY-AS-AP GATEWAY INC,JP	Japan

Table 14. IP addresses, where most malicious URLs were located.

Table 14 shows IP addresses, where most malicious URLs were located. Top 5 addresses are in China. Table 15 shows autonomous systems with most malicious URLs, dominated by two world's largest hosting providers: Amazon and OVH, followed by China Telecom Backbone.

	Number of unique URLs	ASN	Operator
1	1,504,917	AS16509	Amazon.com, Inc.
2	1,412,769	AS16276	OVH SAS
3	1,125,198	AS4134	China Telecom Backbone
4	1,022,558	AS23650	CHINANET jiangsu province backbone
5	876,696	AS14618	Amazon.com, Inc.
6	736,794	AS20940	Akamai International B.V.
7	580,083	AS37963	Hangzhou Alibaba Advertising Co..Ltd.
8	511,871	AS26496	GoDaddy.com, LLC
9	486,203	AS15169	Google Inc.
10	430,375	AS46606	Unified Layer

Table 15. Autonomous systems where most malicious URLs were located.

	Number of unique URLs	Country
1	8,493,123	United States
2	3,503,922	China
3	1,332,016	France
4	1,023,746	Germany
5	747,611	The Netherlands
6	719,451	Europe
7	620,753	Russia
8	528,220	Poland
9	417,986	Hong Kong
10	383,700	United Kingdom

Table 16. Countries in which most malicious URLs were located.

Table 16 shows countries where most malicious URLs were hosted.The top positions are occupied by countries with largest hosting infrastructure. “Europe” in 6th place represents European autonomous systems, for which a specific country cannot be determined.

	Number of unique URLs	TLD
1	11,390,264	.com
2	1,763,566	.net
3	1,100,521	.org
4	1,011,063	.ru
5	593,136	.pl
6	570,705	.info
7	368,501	.br
8	361,077	.biz
9	324,013	.de
10	314,480	.cn

Table 17. Top level domains, where most malicious URLs were located.

Table 17 shows 10 most popular top level domains where malicious URLs were located. .pl’s high position is obviously determined by data feeds, focused mostly on delivery of information about .pl and Polish networks.

Phishing

This section covers only statistics about phishing in original meaning of this term – creation of fake impressions of well known businesses (usually with use of email messages and web pages) in order to steal sensitive data and/or money. Hence, we do not cover here the campaign of fake invoices, distributed in order to infect unsuspecting victims with malware, which was widespread in summer 2014.

The statistic include only phishing pages hosted in Poland, so they do not cover phishing campaigns of Polish banks where the fake pages were hosted abroad.

In 2014 CERT Polska processed 85,893 reports of phishing in Polish networks, with 18,775 unique URLs in 4,862 domains, hosted on 1,989 IP addresses. This means a slight growth of the phenomenon in comparison to 2013.

Because of a change in how we collect information about phishing sites (large parts of data are pulled from external sources at fixed intervals), we do not give a raw number of reports for each autonomous system – contrary to last year, those numbers would bear no meaning and could not be easily compared against each other. Instead, we introduce "addresdays" – number of IP addresses multiplied by the number of days they were actively reported as hosting phishing sites – as an estimation of how quickly an operator responds to phishing reports.

	ASN	Operator	Number of IP addresses	Number of URLs	Addressdays
1	12824	home.pl sp. z o.o.	700	8,928	13,906
2	15967	nazwa.pl S.A. (d.NetArt)	295	2,828	1,891
3	59491	Livenet Sp. z o.o.	82	1,103	412
4	43333	CIS NEPHAX	61	386	985
5	29522	Krakowskie eCentrum Informatyczne JUMP	58	174	974
6	198414	BiznesHost.pl	50	235	358
7	16276	OVH	45	355	955
8	15694	ATM S.A.	45	136	619
9	41079	SuperHost.pl sp. z o.o.	38	740	1,796
10	5617	Orange Polska S.A.	35	110	239

Table 18. Polish autonomous systems where most phishing sites were hosted.

The list of networks hosting phishing sites did not significantly change since the previous year. The leaders are still the biggest Polish hosting operators – home. pl and nazwa. pl (formerly NetArt).

	Phishing target	Number of cases
1	PayPal	1,456
2	Steam	111
3	AOL	48
4	Apple	43
5	Itau	42
6	eBay	36
7	Capitec Bank	36
8	Internal Revenue Service	20
9	Allegro	16
10	Bradesco	15
11	NatWest Bank	12
12	Visa	11
13	Poste Italiane	11
14	Cielo	10
15	Wells Fargo	9
	other banks	50

Tabela 19. Brands used for phishing attacks.

There are, however, some peculiarities on the list of most common targets of phishing hosted in Poland. Although PayPal is still the primary goal amongst phishers, Steam has its debut at second place, and banks appearances are to be noted. Allegro (the largest Polish ecommerce platform) made it to top 10 with 16 phishing cases. Other Polish brand – PKO BP is beyond the table with 2 phishing sites hosted in Poland. Interestingly,Google and Amazon also did not make it to top 15 of 2014 with 8 and 6 cases respectively. An interesting trend is marked with appearances of tax offices of several countries, including American IRS (20 cases), South African and British HMRC (2 cases each, not shown in the table).

Misconfigured servers and services in Poland

In 2014 CERT Polska received reports about 3,440,981 unique IP addresses of misconfigured servers in Poland. For each problematic service we present top 10 autonomous systems where vulnerable servers were located. The tables include ratio of unique IP addresses from the AS that were reported over a year and the size of this AS, as well as percentage of IP addresses from the AS in the pool of all reported addresses.

CHARGEN

18,997 unique IP addresses were reported with misconfigured chargen.

	Number of Unique IP Addresses	ASN	Operator	Ratio	Percentage in all reports
1	12,727	5617	Orange Polska Spolka Akcyjna	0.23%	66.99%
2	1,536	12741	Netia SA	0.10%	8.09%
3	1,432	8374	Polkomtel Sp. z o.o.	0.11%	7.54%
4	1,045	12912	T-MOBILE POLSKA S.A.	0.15%	5.50%
5	653	29314	VECTRA S.A.	0.12%	3.44%
6	308	6830	Liberty Global Operations B.V.	0.01%	1.62%
7	72	39375	Telekomunikacja Podlasie Sp. z o.o.	0.26%	0.38%
8	62	8477	ZTS Echostar Studio Poznan Poland	0.09%	0.33%
9	41	30838	Jerzy Krempa „Telpol” PPMUE	0.16%	0.22%
9	41	41809	Enterpol	0.33%	0.22%

Table 20. Polish autonomous systems with most misconfigured Chargen servers.

DNS

2,226,699 IP addresses were reported as running misconfigured DNS service. Notably, within one operator – Spółdzielnia Telekomunikacyjna OST – two-third of all IP addresses was reported at some point.

	Number of Unique IP Addresses	ASN	Operator	Ratio	Percentage in all reports
1	1,752,713	5617	Orange Polska Spolka Akcyjna	31.80%	77.32%
2	230,243	12741	Netia SA	15.73%	10.16%
3	77,559	21021	Multimedia Polska S.A.	13.08%	3.42%
4	25,139	12912	T-MOBILE POLSKA S.A.	3.70%	1.11%
5	18,256	29314	VECTRA S.A.	3.46%	0.81%
6	13,632	6714	GTS Poland Sp. z o.o.	3.77%	0.60%
7	10,659	6830	Liberty Global Operations B.V.	0.11%	0.47%
8	7,099	38987	Spółdzielnia Telekomunikacyjna OST	63.02%	0.31 %
9	6,770	20960	TK Telekom sp. z o.o.	2.72%	0.30%
10	5,324	13000	Leon sp. z o.o.	10.83%	0.23%

Table 21. Polish autonomous systems with most misconfigured DNS servers.

Netbios

186,101 unique IP addresses were reported for this service. Orange dropped to number 3, thanks to its policy of blocking port 137/UDP in traffic toward end customers.

	Number of Unique IP Addresses	ASN	Operator	Ratio	Percentage in all reports
1	69,492	12741	Netia SA	4.75%	37.34%
2	41,095	21021	Multimedia Polska S.A.	6.93%	22.08%
3	20,937	5617	Orange Polska Spolka Akcyjna	0.38%	11.25%
4	5,021	12912	T-MOBILE POLSKA S.A.	0.74%	2.70%
5	4,253	13110	INEA S.A.	2.61%	2.29%
6	2,631	5550	Technical University of Gdansk, Academic Computer Center TASK	4.01%	1.41%
7	2,215	8970	WROCMAN-EDU	3.38%	1.19%
8	2,071	6714	GTS Poland Sp. z o.o.	0.57%	1.11%
9	1,825	8374	Polkomtel Sp. z o.o.	0.14%	0.98%
10	1,719	198414	Biznes-Host.pl sp. z o.o.	20.35%	0.92%

Table 22. Polish autonomous systems with most misconfigured Netbios servers.

NTP

278,484 unique IP addresses were reported for this service.

	Number of Unique IP Addresses	ASN	Operator	Ratio	Percentage in all reports
1	219,430	5617	Orange Polska Spolka Akcyjna	3.98%	78.79%
2	21,143	12741	Netia SA	1.44%	7.59%
3	4,147	6714	GTS Poland Sp. z o.o.	1.15%	1.49%
4	3,158	21021	Multimedia Polska S.A.	0.53%	1.13%
5	1,932	12912	T-MOBILE POLSKA S.A.	0.28%	0.69%
6	1,656	13110	INEA S.A.	1.02%	0.59%
7	1,334	20804	Exatel S.A.	0.71%	0.48%
8	1,143	15997	ITSA	3.49%	0.41%
9	1,106	8374	Polkomtel Sp. z o.o	0.08%	0.40%
10	874	31229	E24 sp. z o.o.	3.45%	0.31%

Table 23. Polish autonomous systems with most misconfigured NTP servers.

QOTD

21,993 unique IP addresses were reported for this service.

	Number of Unique IP Addresses	ASN	Operator	Ratio	Percentage in all reports
1	14,193	5617	Orange Polska Spolka Akcyjna	0.26%	64.53%
2	2,296	12741	Netia SA	0.16%	10.44%
3	1,484	8374	Polkomtel Sp. z o.o.	0.11%	6.75%
4	1,126	29314	VECTRA S.A.	0.21%	5.12%
5	1,045	12912	T-MOBILE POLSKA S.A.	0.15%	4.75%
6	450	6830	Liberty Global Operations B.V.	0.01%	2.05%
7	119	41809	Enterpol	0.97%	0.54%
8	79	39375	Telekomunikacja Podlasie Sp. z o.o.	0.28%	0.36%
9	68	56575	TepsaNet Stanislaw Nowacki	3.32%	0.31%
10	55	13110	INEA S.A.	0.03%	0.25%

Table 24. Polish autonomous systems with most misconfigured QOTD servers.

SNMP

2,325,483 unique IP addresses were reported for this service. Similarly to DNS, two thirds of IP addresses of Spółdzielnia Telekomunikacyjna OST were reported as having misconfigured SNMPv2.

	Number of Unique IP Addresses	ASN	Operator	Ratio	Percentage in all reports
1	1,718,526	5617	Orange Polska Spolka Akcyjna	31.18%	73.90%
2	498,100	12741	Netia SA	34.03%	21.42%
3	33,046	12912	T-MOBILE POLSKA S.A.	4.86%	1.42%
4	23,401	6714	GTS Poland Sp. z o.o.	6.46%	1.01%
5	7,587	38987	Spółdzielnia Telekomunikacyjna OST	67.36%	0.33%
6	6,609	29007	Petrotel Sp. z o.o.	40.34%	0.28%
7	3,371	6830	Liberty Global Operations B.V.	0.04%	0.14%
8	3,352	20960	TK Telekom sp. z o.o.	1.35%	0.14%
9	2,826	29314	VECTRA S.A.	0.53%	0.12%
10	1,630	24709	MNI Telecom S.A. IP Backbone	3.64%	0.07%

Table 25. Polish autonomous systems with most misconfigured SNMP servers.

SSDP

2,562,309 unique IP addresses were reported for this service making SSDP the protocol with most reported misconfigured servers in 2014. The autonomous systems with the largest number of open SSDP servers in relation to its size is owned by Spółdzielnia Telekomunikacyjna OST.

	Number of Unique IP Addresses	ASN	Operator	Ratio	Percentage in all reports
1	1,751,912	5617	Orange Polska Spolka Akcyjna	31.79%	68.37%
2	371,063	12741	Netia SA	25.35%	14.48%
3	195,854	21021	Multimedia Polska S.A.	33.02%	7.64%
4	68,820	29314	VECTRA S.A.	13.02%	2.69%
5	30,596	12912	T-MOBILE POLSKA S.A.	4.50%	1.19%
6	20,302	6830	Liberty Global Operations B.V.	0.21%	0.79%
7	16,060	6714	GTS Poland Sp. z o.o.	4.44%	0.63%
8	8,209	38987	Spółdzielnia Telekomunikacyjna OST	72.88%	0.32%
9	7,393	29007	Petrotel Sp. z o.o.	45.12%	0.29%
10	5,129	31304	Espol Sp. z o.o.	23.85%	0.20%

Table 26. Polish autonomous systems with most misconfigured SSDP servers.

Scanning

This category covers identified cases of unauthorised connections that may indicate either a compromise of the source machine or intentional malicious activity of its user. All numbers in the statistics below are based on automated reports from partners and CERT Polska own monitoring systems, which are handled by the n6 platform.

In 2014 CERT Polska received reports about 876,970 unique IP addresses (about 45.5 thousand more than in 2013) where scans originated. Those addresses were located in 2017 countries. Polish networks accounted for 107,141 unique addresses.

Due to the nature of source data – some of it is generated by our monitoring systems where target hosts are in Poland, while for external sources the source hosts are in Poland), we decided to split statistics in three sections – scanned services (without regard for origin and destination), scans targeting Polish hosts, and scans targeting foreign networks.

Scanned services

In 2013 the target port of most reported scans was 23/TCP, typically used by telnet. The growth in comparison to 2013 is significant – from less than 65 thousand to almost 200 thousand scans. A serious rise in activity (but without a change of the position in ranking) was observed on port 80/TCP used mostly by web servers, often running web applications – number of unique scanning source IP addresses has increased by 60% since 2013. The biggest drop – almost by a half – was related to port 445/TCP (Windows RPC), and – by over a half – related to 1433/TCP (MS SQL). Table 27 and figure 19 both present the top 10 most scanned services.

	Destination port	Number of IP addresses	Percentage	Service
1	23/TCP	198,509	18.2 %	telnet
2	3389/TCP	139,898	12.9 %	RDP (remote desktop)
3	445/TCP	134,524	12.4 %	Windows RPC
4	80/TCP	114,646	10.5 %	web servers, web applications
5	4899/TCP	111,938	10.3 %	Radmin
6	5000/TCP	69,603	6.4 %	various
7	22/TCP	38,058	3.5 %	SSH
8	1433/TCP	23,184	2.1 %	MS SQL
9	8080/TCP	20,811	1.9 %	web cache and proxy
10	139/TCP	11,941	1.1 %	NetBIOS, file sharing
	other:	224,933	20.7 %	

Table 27. Most commonly scanned ports.

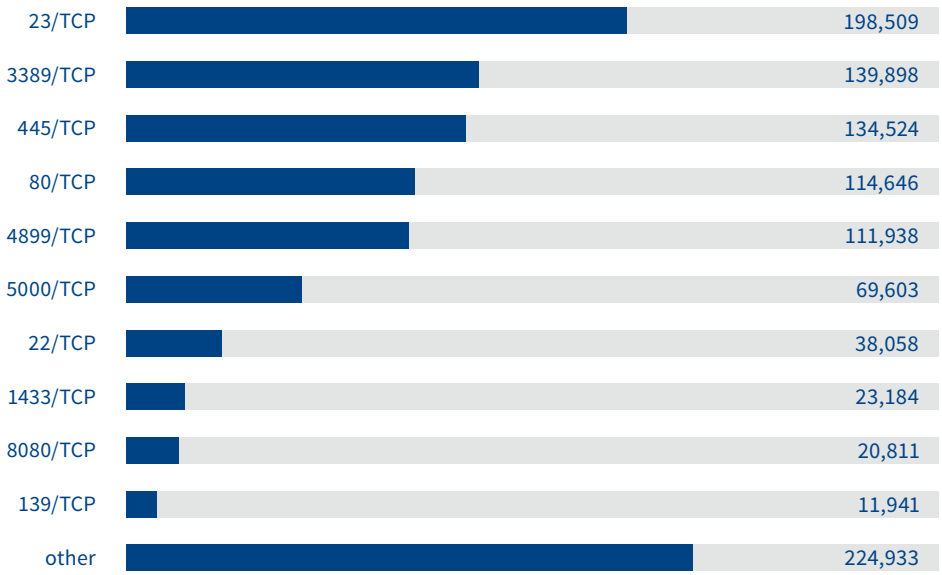


Figure 19. Most commonly scanned ports.

Snort rules

Snort rules are used for detection of attacks in systems based on open-source Snort IDS. Table 28 presents 10 rules most commonly matched by ARAKIS.

	Snort rule	Number of IP addreses	Percentage	Destinantion port
1	RDP connection request	131,256	21.21 %	3389/TCP
2	MS Terminal server request	130,943	21.16 %	3389/TCP
3	Radmin Remote Control Session Setup Initiate	110,297	17.82 %	Mostly 4899/TCP
4	WEB-IIS view source via translate header	70,034	11.32 %	80/TCP
5	Potential SSH Scan	23,232	3.75 %	22/TCP
6	Suspicious inbound to MSSQL port 1433	23,032	3.72 %	1433/TCP
7	RDP disconnect request	16,097	2.60 %	3389/TCP
8	LibSSH Based SSH Connection – Often used as a BruteForce Tool	15,541	2.51 %	22/TCP
9	Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection	10,403	1.68 %	3389/TCP
10	Suspicious inbound to mySQL port 3306	6,317	1.02 %	3306/TCP
	other:	81,739	13.21 %	—

Table 28. Snort rules most commonly matched by ARAKIS.

Foreign networks

One in three scans from foreign IP addresses originated in China. Other countries had significantly lower shares, and the first three positions in the table below remain unchanged. Ten countries where most scans towards Polish networks originated are presented in Table 29 and Figure 20.

	Country	Number of IP addresses	Percentage
1	China	272,672	35.5%
2	United States	56,910	7.4%
3	Russia	35,977	4.7%
4	India	34,755	4.5%
5	Brasil	30,792	4.0%
6	Taiwan	24,299	3.2%
7	Turkey	23,481	3.1%
8	Mexico	19,701	2.6%
9	Thailand	19,441	2.5%
10	South Korea	15,695	2.0%
	other:	234,690	30.5%

Table 29. Countries where most scans originated (Poland excluded).

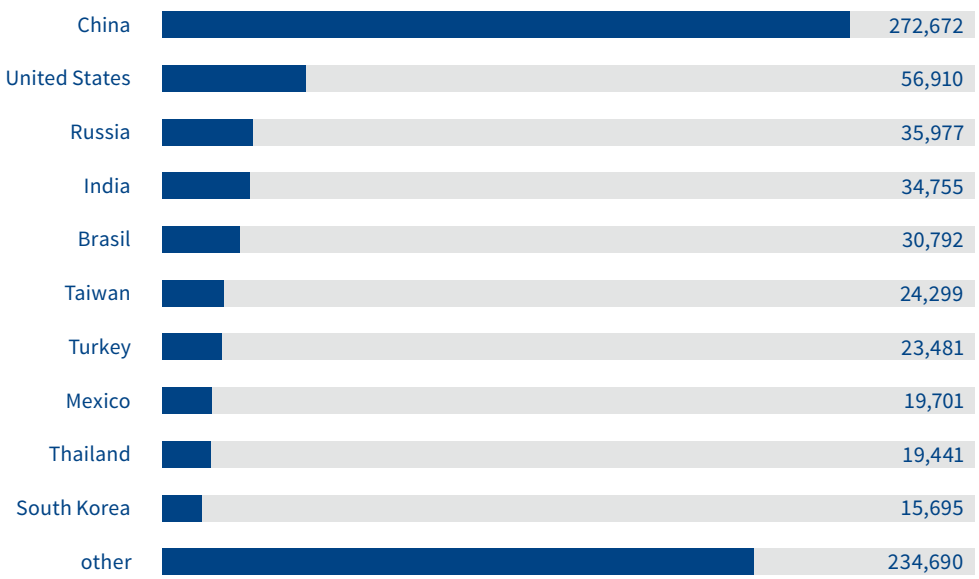


Figure 20. Countries where most scans originated (Poland excluded).

Table 30 presents the autonomous systems where most scans originated. Scans from the first one – China Telecom Backbone – were four times as frequent as from the second one (also Chinese). Interestingly, there is no American AS in the top 10, although United States came second in numbers of scanning IP addresses per country. Most plausible explanation is that it's due to the fact that many American ISPs manage their own, relatively small, autonomous systems. In China, on the other hand, most networks are managed by large government entities.

	ASN	Operator	Country	Number of IP addresses	Percentage
1	4134	China Telecom Backbone	China	184,592	23.32%
2	4837	China Unicom Backbone	China	43,534	5.50%
3	9121	Turk Telekomunikasyon Anonim Sirketi	Turcja	18,698	2.36%
4	3462	Data Communication Business Group	Tajwan	18,696	2.36%
5	8151	Uninet S.A. de C.V.	Mexico	15,823	2.00%
6	9829	BSNL (Bharat Sanchar Nigam Ltd)	India	15,759	1.99%
7	18881	Global Village Telecom	Brasil	7,952	1.00%
8	4766	Korea Telecom	Korea	7,082	0.89%
9	4812	Shanghai Telecom	China	6,992	0.88%
10	17552	True Internet Co.,Ltd.	Tailand	6,716	0.85%
	other:			465,791	58.84%

Table 30. Foreign autonomous systems where most scans originated.

Polish networks

In 2013 we witnessed a change at the "leader" position, held by Netia for several previous years. Most IP addresses reported as scanning originated from AS5617 (Orange Polska), with Netia slightly behind. The complete list of top 10 Polish autonomous systems where scans originated is presented in the Table 31 and Figure 21.

	ASN	Operator	Number of IP addresses	Percentage
1	5617	Orange	28,304	26.40%
2	12741	Netia SA	28,222	26.33%
3	8374	Polkomtel Sp. z o.o.	17,759	16.57%
4	21021	Multimedia Polska S.A.	13,237	12.35%
5	12912	T-Mobile Polska SA	1,639	1.53%
6	29007	Petrotel Sp. z o.o.	1,533	1.43%
7	6714	GTS Poland Sp. z o.o.	1,099	1.03%
8	21243	Polkomtel Sp. z o.o.	1,063	0.99%
9	6830	Liberty Global Operations B.V. (UPC)	1,008	0.94%
10	49185	Protonet	994	0.93%
	other:		12,342	11.5 %

Table 31. Polish autonomous systems with highest numbers of originating scans.

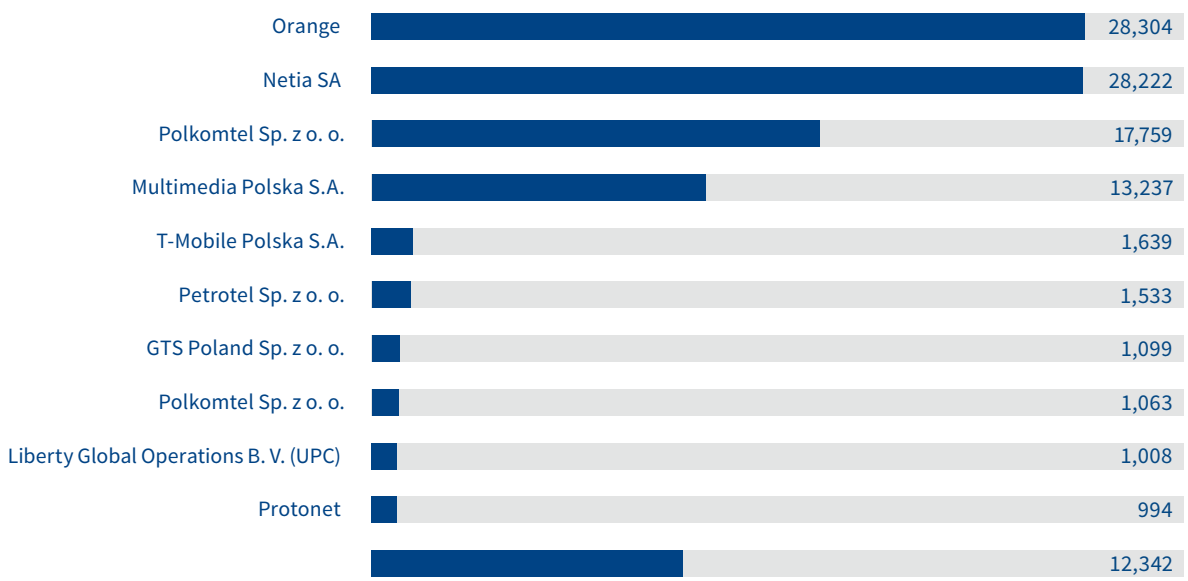


Figure 21. Polish autonomous systems with highest numbers of originating scans.

About CERT Polska

The CERT Polska team operates within the structures of NASK (Research and Academic Computer Network) – a research institute which conducts scientific studies, operates the national .pl domain registry and provides advanced IT services. CERT Polska is the first Polish computer emergency response team. Active since 1996 in the response teams community, it has become a recognized and experienced entity in the field of computer security. Since its launch, the core of the team's activity has been handling security incidents and cooperation with similar units worldwide. CERT Polska also conducts extensive securityrelated R&D. In 1998, CERT Polska became a member of the international forum of response teams (FIRST), and since 2000 it has been a member of the working group of the European response teams: TERENA TFCSIRT, accredited by Trusted Introducer. In 2005 by the initiative of CERT Polska, a forum of Polish abuse teams, Abuse FORUM, was created. In 2010 CERT Polska joined the AntiPhishing Working Group, an association of companies and institutions which actively fight online crime.

Main responsibilities of CERT Polska include:

- registration and handling of network security incidents;
- active response in case of direct threats to users;
- cooperation with other CERT teams in Poland and worldwide;
- participation in national and international projects related to the IT security;
- research into methods of detecting security incidents, analysis of malware, systems for exchanging information on threats;
- development of proprietary and open source tools for detection, monitoring, analysis, and correlation of threat;
- regular publication of the annual CERT Polska Report on security of Polish cyberspace; informational and educational activities, aimed at raising awareness in relation to IT security, including:
  – maintaining a blog at http://www.cert.pl as well as Facebook and Twitter accounts;
  – organization of the annual SECURE conference analysis and testing of IT security solutions.

CONTACT

Incident reports: cert@cert.pl

Spam reports: spam@cert.pl

Information: info@cert.pl

PGP Key: www.cert.pl/pub/0x553FEB09.asc

Website: www.cert.pl

Facebook: fb.com/CERT.Polska

RSS: www.cert.pl/rss

Twitter: @CERT_Polska, @CERT_Polska_en

NASK/CERT Polska

Wąwozowa 18, 02-796 Warszawa

Phone: +48 22 38 08 274

Fax: +48 22 38 08 399