POLISH INTERNET

SECURITY LANDSCAPE

2015

ISSN 2084-9079

CERT Polska
Report 2015

CERT.PL>_

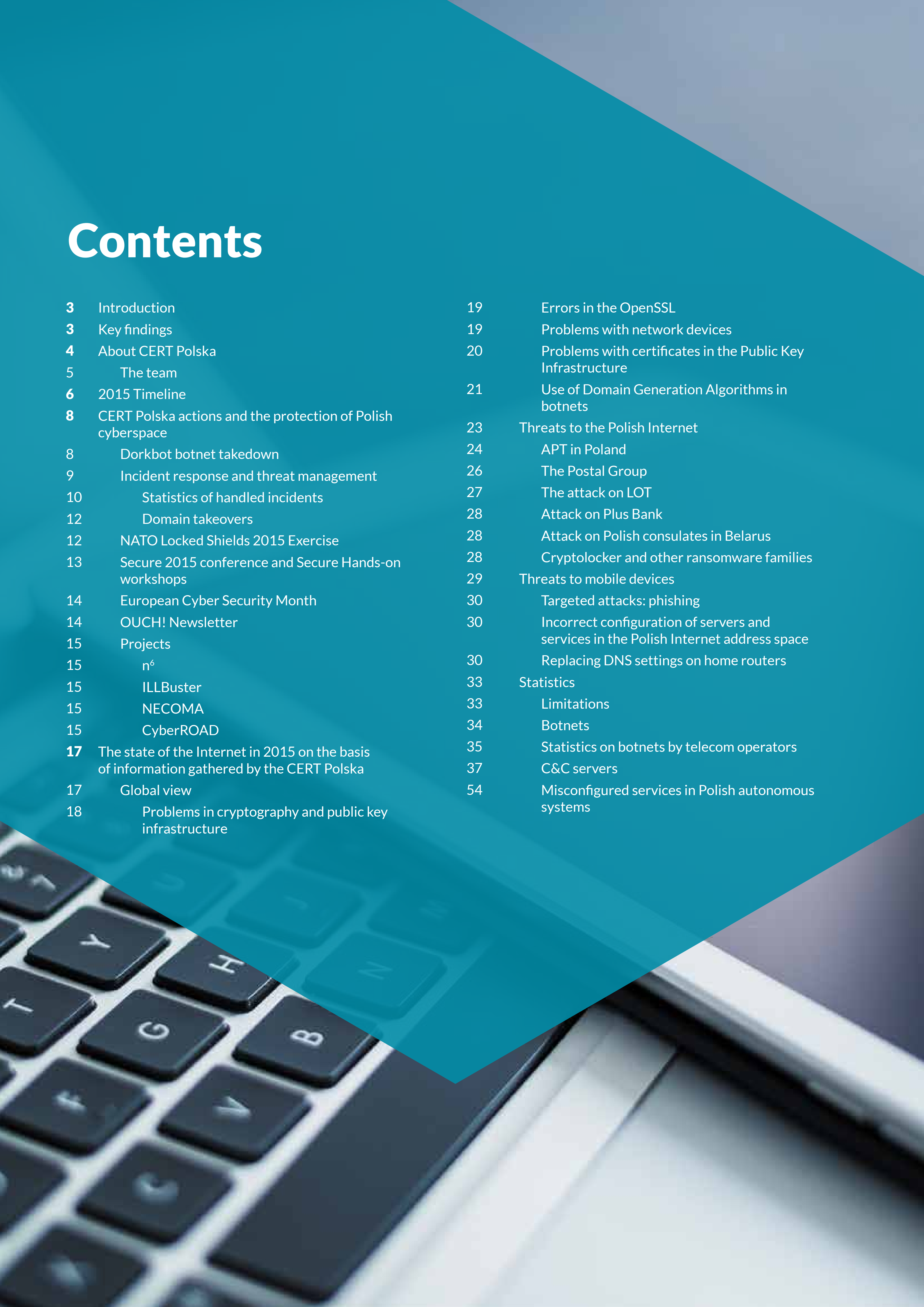
POLISH INTERNET

SECURITY LANDSCAPE

2015

NASK

CERT Polska
Report 2015



Contents

Introduction

With great pleasure, we hereby present you the yearly report on the activities of CERT Polska for the year 2015. In some ways it was a year of great change for the Polish Internet – targeted attacks against Poland's key companies and organizations intensified, and Polish authorities, well aware of the dangers, commissioned NASK to create a report containing proposals, based on our expertise, for the organization of the defense system of the cyberspace of the Republic of Poland. Earlier, the European Union Agency for Network and Information Security (ENISA) published a couple of guidebooks about processing actionable information on incidents, vulnerabilities and threats, developed by CERT Polska. In addition to participation in these projects, our team worked hard fighting cybercrime, especially targeting the financial sector. The work is an invaluable aid to the Polish law enforcement agencies.

In the upcoming years we expect an increase in network threats, in terms of both their number and impact. With information technology encroaching all areas of human activity, network security is becoming an issue of safety for us all. This will be a challenge in the years to come.

The CERT Polska Team

Key **findings**

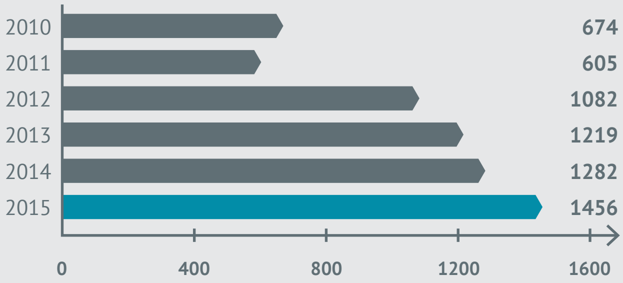
- In 2015, targeted attacks against Polish entities intensified. They affected large institutions and companies, as well as whole industries, groups of companies and organizations.
- Most of Polish Internet Service Providers have similar percentages of infected customers. The notorious exception is Netia, where the ratio is significantly higher.
- New banking malware (Dyre / Dyreza families), previously used only against customers of western banks, started targeting customers of Polish banks.
- Ransomware attacks were successful against Windows, as well as Android and Linux systems.
- There was an increase in the number of phishing sites hosted on Polish servers. Paypal remains the most common phishing target.
- There was no significant change in observed numbers of botnets' C&C servers per country. An interesting new entry in the ranking is Uruguay with the third biggest number of known C&C servers.
- Domain Generation Algorithms (DGA) are a popular technique for increasing the resilience of botnets against takeovers and takedowns. The largest DGA botnets in Poland observed throughout 2015 were TinBa DGA, ISFB / Gozi2 and Conficker.
- The public disclosure of government-sponsored internet espionage and sabotage in 2015 seems to justify classifying the internet as the fifth domain of military warfare (cyber-warfare).
- Security researchers discovered numerous vulnerabilities in commonly used cryptographic libraries caused by software bugs and incorrect usage, due to failed assumptions of computational security.
- Due to the insufficient level of security provided by SHA-1 algorithm, most browsers will discontinue support for it.

- The number of misconfigured, publicly accessible DNS, SNMP and SSDP servers allowing for DDoS amplification decreased, while the number of misconfigured NTP and NetBIOS servers increased.
- In Poland, the most commonly misconfigured Internet services are DNS servers.

About **CERT** Polska

CERT Polska is a part of NASK (Research and Academic Computer Network) - a research institute that also operates the .pl TLD registry and offers a range of advanced telecom services. CERT Polska is the first CSIRT established in Poland. Since its inception in 1996, thanks to a dynamic activity in the CERT/CSIRT community, the team has become a recognized and experienced player in the field of computer security. The core activities provided by CERT Polska include incident handling and cooperation with similar units around the world, both in operational fields and research and development. CERT Polska is a member of various international forums and working groups, including FIRST (since 1998), TF-CSIRT (since 2000) and APWG (since 2010). In 2005, CERT Polska started a forum for the Polish abuse incident handling teams - Abuse Forum.

Number of incidents manually handled by CERT Polska



The main activities of CERT Polska are:

- Incident registration and handling;
- detection and analysis of threats targeting Polish internet users and systems and networks in .pl TLD;
- active response against direct threats to Polish internet users;
- cooperation with other CSIRTs in Poland and worldwide as well as with law enforcement authorities;
- participation in national and international projects related to IT security;
- research activities in the field of methods of detection of security incidents, malware analysis and exchange of threat intelligence;
- development of own tools for detection, monitoring, analysis and correlation of threats;
- creating the CERT Polska yearly report that describes the state of safety and security of the Polish internet;
- information dissemination and educational activities, aimed at increasing the awareness of ICT security, including:
  - » cert.pl blog and social media presence with a strong message of IT security issues;
  - » organization of annual conference SECURE;
  - » specialized trainings and workshops.

The team

Our team is one of leading organizations in Polish information security scene. We are often in the front line of the trenches, researching new threats – malware samples, exploits and attacks. Due to increase of importance of information security, our team is growing rapidly.

We have some bragging rights: we routinely take down botnets, and our research is widely cited by such names as Microsoft, Kaspersky Labs, F-Secure, Websense, and Arbor Networks. Our specialists take part in competitions such as NATO Locked Shields, and in their free time our team members are also known for their CTF skills.

We lead and take part in international research project for the European Union or NATO, and results of the projects are deployed in the real world. We also have trained security professionals all over the world: Mexico, Dubai, Hong-Kong, you name it.

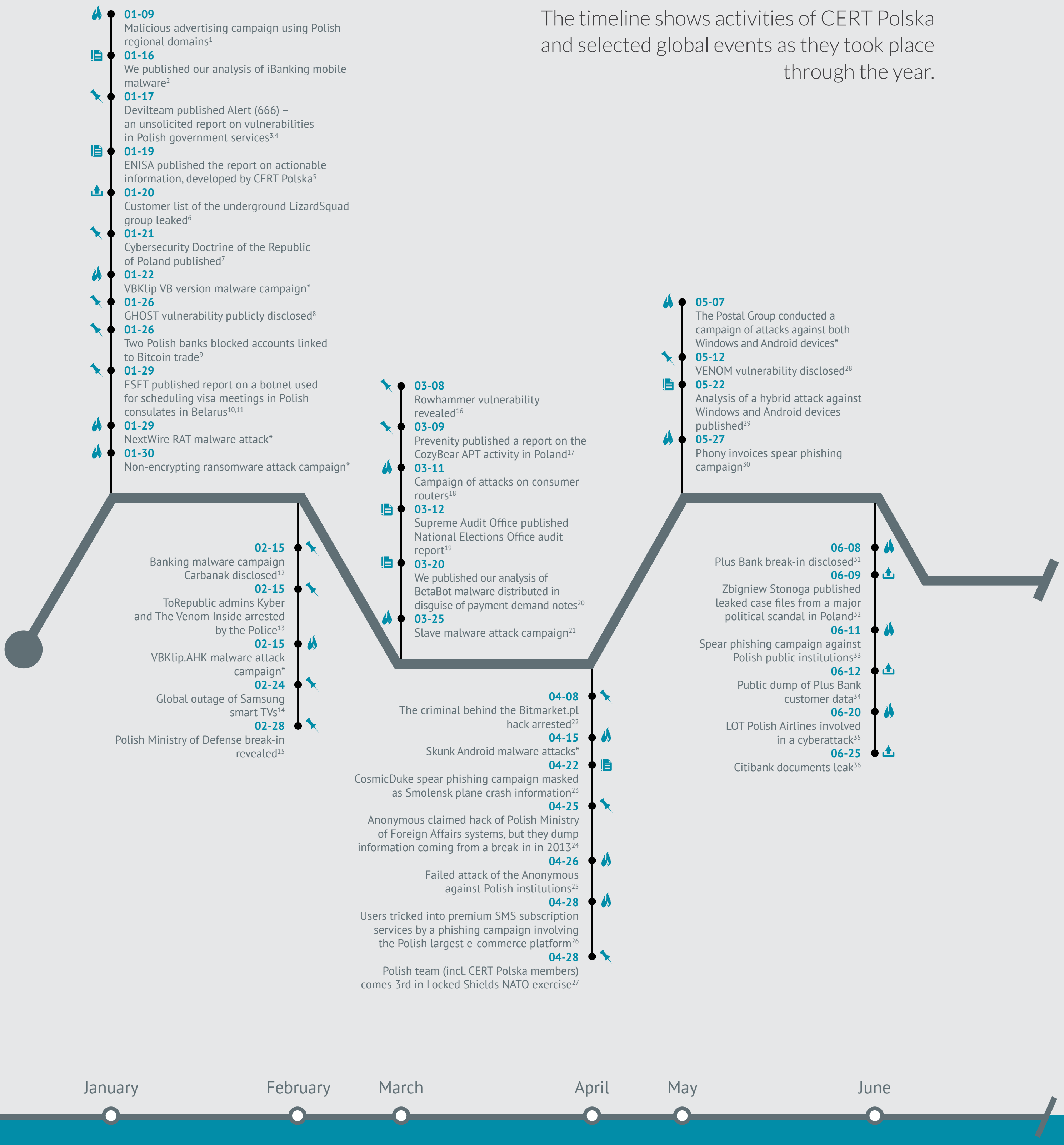
In 2015, members of CERT Polska gave talks at 27 conferences in 9 countries, were frequently interviewed in Polish media, and conducted 11 training courses.

“We employ top class experts, who win professional competitions and combat threats as a part of international cooperation. We’re looking for people passionate about computer security to join us and perfect their skills.”

– Piotr Kijewski, the Head of CERT Polska

2015 **Timeline**

The timeline shows activities of CERT Polska and selected global events as they took place through the year.



01-09
Malicious advertising campaign using Polish regional domains[1]

01-16
We published our analysis of iBanking mobile malware[2]

01-17
Devilteam published Alert (666) – an unsolicited report on vulnerabilities in Polish government services[3,4]

01-19
ENISA published the report on actionable information, developed by CERT Polska[5]

01-20
Customer list of the underground LizardSquad group leaked[6]

01-21
Cybersecurity Doctrine of the Republic of Poland published[7]

01-22
VBKlip VB version malware campaign*

01-26
GHOST vulnerability publicly disclosed[8]

01-26
Two Polish banks blocked accounts linked to Bitcoin trade[9]

01-29
ESET published report on a botnet used for scheduling visa meetings in Polish consulates in Belarus[10,11]

01-29
NextWire RAT malware attack*

01-30
Non-encrypting ransomware attack campaign*

02-15
Banking malware campaign Carbanak disclosed[12]

02-15
ToRepublic admins Kyber and The Venom Inside arrested by the Police[13]

02-15
VBKlip.AHK malware attack campaign*

02-24
Global outage of Samsung smart TVs[14]

02-28
Polish Ministry of Defense break-in revealed[15]

03-08
Rowhammer vulnerability revealed[16]

03-09
Prevenity published a report on the CozyBear APT activity in Poland[17]

03-11
Campaign of attacks on consumer routers[18]

03-12
Supreme Audit Office published National Elections Office audit report[19]

03-20
We published our analysis of BetaBot malware distributed in disguise of payment demand notes[20]

03-25
Slave malware attack campaign[21]

04-08
The criminal behind the Bitmarket.pl hack arrested[22]

04-15
Skunk Android malware attacks*

04-22
CosmicDuke spear phishing campaign masked as Smolensk plane crash information[23]

04-25
Anonymous claimed hack of Polish Ministry of Foreign Affairs systems, but they dump information coming from a break-in in 2013[24]

04-26
Failed attack of the Anonymous against Polish institutions[25]

04-28
Users tricked into premium SMS subscription services by a phishing campaign involving the Polish largest e-commerce platform[26]

04-28
Polish team (incl. CERT Polska members) comes 3rd in Locked Shields NATO exercise[27]

05-07
The Postal Group conducted a campaign of attacks against both Windows and Android devices*

05-12
VENOM vulnerability disclosed[28]

05-22
Analysis of a hybrid attack against Windows and Android devices published[29]

05-27
Phony invoices spear phishing campaign[30]

06-08
Plus Bank break-in disclosed[31]

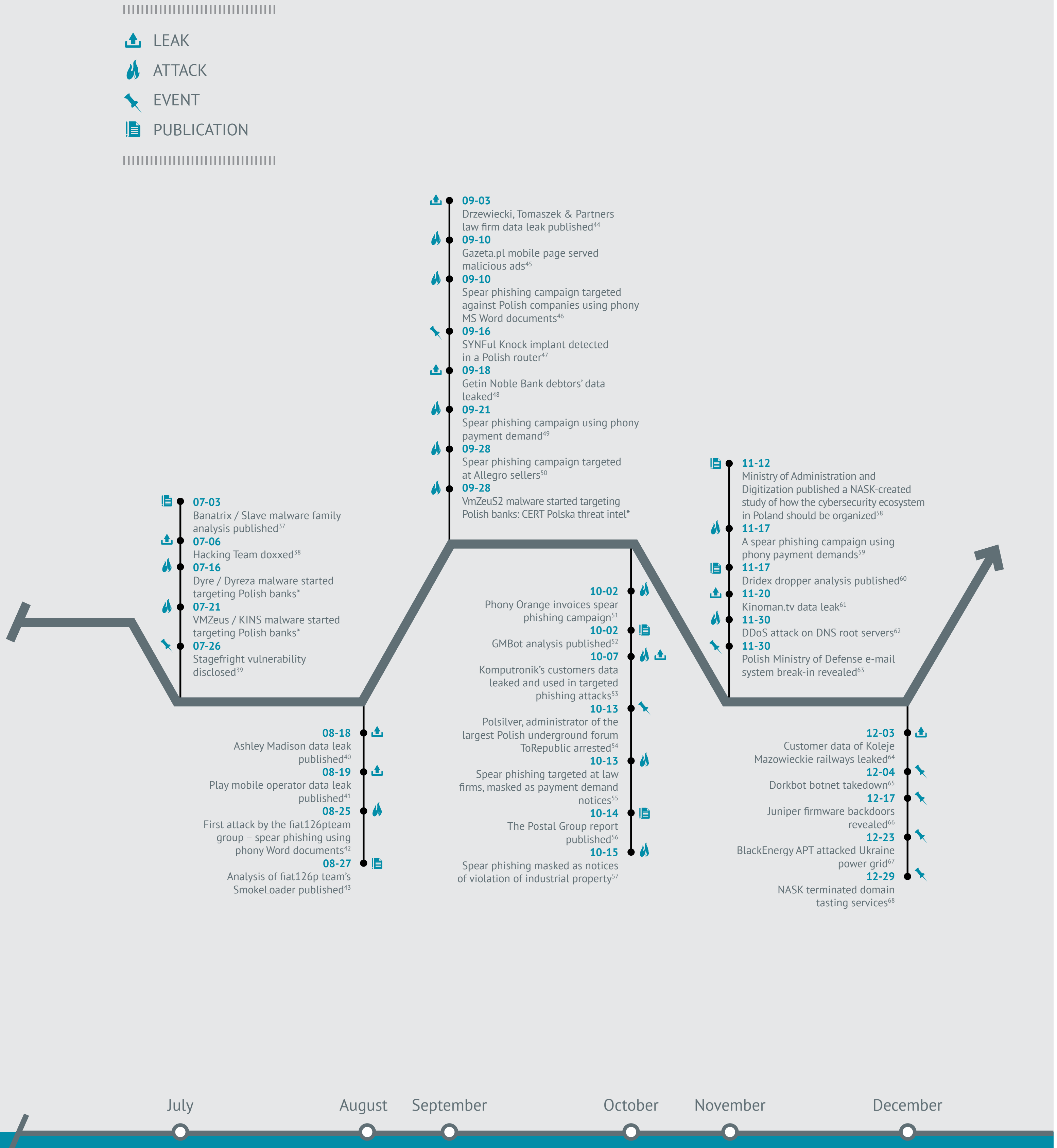
06-09
Zbigniew Stonoga published leaked case files from a major political scandal in Poland[32]

06-11
Spear phishing campaign against Polish public institutions[33]

06-12
Public dump of Plus Bank customer data[34]

06-20
LOT Polish Airlines involved in a cyberattack[35]

06-25
Citibank documents leak[36]



LEAK
ATTACK
EVENT
PUBLICATION

07-03
Banatrix / Slave malware family analysis published[37]

07-06
Hacking Team doxxed[38]

07-16
Dyre / Dyreza malware started targeting Polish banks*

07-21
VMZeus / KINS malware started targeting Polish banks*

07-26
Stagefright vulnerability disclosed[39]

08-18
Ashley Madison data leak published[40]

08-19
Play mobile operator data leak published[41]

08-25
First attack by the fiat126pteam group – spear phishing using phony Word documents[42]

08-27
Analysis of fiat126p team's SmokeLoader published[43]

09-03
Drzewiecki, Tomaszek & Partners law firm data leak published[44]

09-10
Gazeta.pl mobile page served malicious ads[45]

09-10
Spear phishing campaign targeted against Polish companies using phony MS Word documents[46]

09-16
SYNFul Knock implant detected in a Polish router[47]

09-18
Getin Noble Bank debtors' data leaked[48]

09-21
Spear phishing campaign using phony payment demand[49]

09-28
Spear phishing campaign targeted at Allegro sellers[50]

09-28
VmZeuS2 malware started targeting Polish banks: CERT Polska threat intel*

10-02
Phony Orange invoices spear phishing campaign[51]

10-02
GMBot analysis published[52]

10-07
Komputronik's customers data leaked and used in targeted phishing attacks[53]

10-13
Polsilver, administrator of the largest Polish underground forum ToRepublic arrested[54]

10-13
Spear phishing targeted at law firms, masked as payment demand notices[55]

10-14
The Postal Group report published[56]

10-15
Spear phishing masked as notices of violation of industrial property[57]

11-12
Ministry of Administration and Digitization published a NASK-created study of how the cybersecurity ecosystem in Poland should be organized[58]

11-17
A spear phishing campaign using phony payment demands[59]

11-17
Dridex dropper analysis published[60]

11-20
Kinoman.tv data leak[61]

11-30
DDoS attack on DNS root servers[62]

11-30
Polish Ministry of Defense e-mail system break-in revealed[63]

12-03
Customer data of Koleje Mazowieckie railways leaked[64]

12-04
Dorkbot botnet takedown[65]

12-17
Juniper firmware backdoors revealed[66]

12-23
BlackEnergy APT attacked Ukraine power grid[67]

12-29
NASK terminated domain tasting services[68]

1 https://zaufanatrzeciastrona.pl/post/zlosliwe-reklamy-atakuja-z-uzyciem-polskich-domen-regionalnych/

2 http://www.cert.pl/news/9699

3 https://niebezpiecznik.pl/post/duzo-dziur-w-polskich-serwisach-rzadowych-gov-pl/

4 https://zaufanatrzeciastrona.pl/post/kilkadziesiat-powaznych-i-kilkaset-mniejszych-bledow-w-serwerach-w-domenie-gov-pl/

5 http://www.cert.pl/news/9684

6 https://zaufanatrzeciastrona.pl/post/polskie-ofiary-i-uzytkownicy-serwisu-ddos-od-lizard-squad/

7 http://niebezpiecznik.pl/post/doktryna-cyberbezpieczenstwa-rzeczypospolitej-polskiej-zostala-opublikowana/

8 http://niebezpiecznik.pl/post/ghost-powazna-dziura-w-popularnej-bibliotece-linuksa/

9 http://niebezpiecznik.pl/post/akcja-bankow-wymierzona-w-polskich-posiadaczy-bitcoinow/

10 https://zaufanatrzeciastrona.pl/post/polskie-konsulaty-na-bialorusi-celem-nowego-botnetu/

11 http://www.welivesecurity.com/2015/01/29/msilagent-pyo-have-botnet-will-travel/

12 http://niebezpiecznik.pl/post/jak-zniknelo-300-milionow-dolarow-czyli-najwieksze-w-historii-bankowosci-wlamanie-operacja-carbanak/

13 https://zaufanatrzeciastrona.pl/post/ogromny-sukces-polskiej-policji-administratorzy-torepublic-zatrzymani/

14 http://niebezpiecznik.pl/post/globalna-awaria-telewizorow-samsunga/

15 http://niebezpiecznik.pl/post/kto-wlamal-sie-do-prywatnych-skrzynek-pocztowych-pracownikow-mon-i-sztabu-generalnego-wojska-polskiego/

16 http://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html

17 http://malware.prevenity.com/2015/03/euroapt.html

18 http://www.cert.pl/news/9751

19 http://niebezpiecznik.pl/post/nik-opublikowalo-raport-dotyczacy-kontroli-w-pkw/

20 http://www.cert.pl/news/9768

21 http://securityblog.s21sec.com/2015/03/new-banker-slave-hitting-polish-banks.html

22 http://niebezpiecznik.pl/post/policja-aresztowala-rafala-ktory-okradl-bitmarket-pl-na-85000-pln/

23 http://malware.prevenity.com/2015/04/malware-w-5-rocznice-katastrofy-samolotu.html

24 http://niebezpiecznik.pl/post/msz-zhackowane-przez-anonimowych/

25 https://zaufanatrzeciastrona.pl/post/podsumowanie-zapowiadanych-na-dzisiaj-atakow-anonymous-na-polskie-instytucje/

26 http://niebezpiecznik.pl/post/doszlo-do-wlamania-na-twoje-konto-w-serwisie-allegro/

27 http://www.cert.pl/news/10081

28 http://niebezpiecznik.pl/post/venom-dziura-w-serwerowniach-i-chmurach-czyli-zemsta-dyskietki/

29 http://www.cert.pl/news/10180

30 http://niebezpiecznik.pl/post/alert-powiadomienie-o-wystawionych-fakturach/

31 https://zaufanatrzeciastrona.pl/post/powazne-wlamanie-do-polskiego-banku-skradzione-dane-i-hasla-klientow/

32 http://wiadomosci.gazeta.pl/wiadomosci/1,114871,18083437.html

33 http://malware.prevenity.com/2015/08/wykradanie-danych-z-instytucji.html

34 https://zaufanatrzeciastrona.pl/post/wlamywacz-spelnil-grozbe-i-publikuje-dane-klientow-plus-banku/

35 http://niebezpiecznik.pl/post/komputery-lot-u-zaatakowane-samoloty-uziemione/

36 http://niebezpiecznik.pl/post/poufne-dokumenty-polskiego-odzialu-centrum-operacyjnego-citi-wyciekly-do-internetu/

37 http://www.cert.pl/news/10358

38 https://zaufanatrzeciastrona.pl/post/producent-rzadowych-trojanow-zhakowany-ogromny-wyciek-jest-takze-polski-slad/

39 http://niebezpiecznik.pl/post/950-milionow-telefonow-z-androidem-mozna-zhackowac-jednym-mms-em/

40 http://niebezpiecznik.pl/post/37-milionow-milosnikow-skokow-w-bok-moze-dzis-spac-na-kanapie/

41 http://niebezpiecznik.pl/post/wyciek-danych-osobowych-klientow-playa/

42 https://zaufanatrzeciastrona.pl/post/uwaga-na-nowy-sprytny-atak-na-polskich-internautow/

43 http://www.cert.pl/news/10484

44 http://www.wykop.pl/link/2734243/

45 http://niebezpiecznik.pl/post/uwaga-na-mobilna-strone-gazeta-pl/

46 https://zaufanatrzeciastrona.pl/post/uwaga-na-nowy-atak-fiat126pteam-celem-polskie-firmy/

47 https://zaufanatrzeciastrona.pl/post/polski-ruter-na-liscie-zainfekowanych-unikatowym-zlosliwym-oprogramowaniem/

48 http://niebezpiecznik.pl/post/dane-dluznikow-getina-i-noble-banku-na-sprzedaz/

49 https://zaufanatrzeciastrona.pl/post/uwaga-na-trzy-nowe-kampanie-zlosliwego-oprogramowania-atakujace-polakow/

50 https://zaufanatrzeciastrona.pl/post/uwaga-na-nowa-fale-atakow-celem-sprzedawcy-allegro/

51 https://zaufanatrzeciastrona.pl/post/uwaga-na-nowy-nietypowy-atak-udajacy-faktury-orange/

52 http://www.cert.pl/news/10648

53 http://niebezpiecznik.pl/post/wyciek-adresow-e-mail-klientow-komputronika-uwaga-na-falszywe-wiadomosci-z-wezwaniem-do-zaplaty/

54 http://niebezpiecznik.pl/post/policja-zlapala-polsilvera-administratora-torepublic-zamieszanego-we-wlamanie-do-plusbanku/

55 https://zaufanatrzeciastrona.pl/post/uwaga-na-nowy-atak-na-kancelarie-prawnicze-wezwanie-do-zaplaty/

56 http://www.cert.pl/news/10746

57 https://zaufanatrzeciastrona.pl/post/nowy-atak-zawiadomienie-o-naruszeniu-wlasnosci-przemyslowej/

58 http://www.cert.pl/news/10803

59 https://zaufanatrzeciastrona.pl/post/ciekawa-i-bardzo-roznorodna-kampania-zlosliwego-oprogramowania/

60 http://www.cert.pl/news/10832

61 http://niebezpiecznik.pl/post/wyciek-danych-z-serwisu-kinoman-tv-przez-6-godzin-mozna-bylo-pobierac-dane-uzytkownikow/

62 https://zaufanatrzeciastrona.pl/post/silne-ataki-na-kluczowe-elementy-infrastruktury-internetu/

63 http://www.rp.pl/Sluzby-mundurowe/311309859-Cyberszpiedzy-grasuja-w-MON.html

64 http://niebezpiecznik.pl/post/adminadmin-oto-dane-logowania-broniace-dostepu-do-bazy-4000-wlascicieli-kart-mazowieckich-kolei/

65 http://www.cert.pl/news/10926

66 http://forums.juniper.net/t5/Security-Incident-Response/Important-Announcement-about-ScreenOS/ba-p/285554

67 https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered

68 http://www.dns.pl/news/press.html – Informacja dotycząca zaprzestania świadczenia usługi testów nazw domeny .pl (DNT) z dn. 2015-12-30.

* CERT Polska threat intelligence

The main activities of CERT Polska are:

- incident registration and handling
- detection and analysis of threats targeting Polish internet users and systems and networks in .pl TLD
- active response against direct threats to Polish internet users
- cooperation with other CSIRTs in Poland and worldwide as well as with law enforcement authorities
- participation in national and international projects related to IT security
- research activities in the field of methods of detection of security incidents, malware analysis and exchange of threat intelligence
- development of own tools for detection, monitoring, analysis and correlation of threats
- creating the CERT Polska yearly report that describes the state of safety and security of the Polish internet
- independent tests and analyses of internet security solutions
- information dissemination and educational activities, aimed at increasing the awareness of ICT security, including:
  - cert.pl blog and social media presence with a strong message of IT security issues;
  - organization of annual conference SECURE;
  - specialized trainings and workshops

CERT Polska actions and the **protection** of Polish cyberspace

From our standpoint, two events of 2015 were of immense significance to our activities as well as to the security of the Polish cyberspace.

In June 2015 the Supreme Audit Office (NIK) published the results of a wide audit carried out in a number of state institutions. The focus of the audit was the protection of the state's cyberspace at the national level[1]. The audit started in mid-2014 and NASK was one of its subjects, with special focus on the activities of our team. Although the gist of the report is that the state lacks a coherent and system-wide approach to fighting cyberspace threats, the activities of NASK and CERT Polska were approved as fulfilling the required roles.

In November 2015, the Ministry of Administration and Digitization published a study document titled "The Republic of Poland cyberspace defense system". The Ministry delegated creation of the document to NASK, and CERT Polska participated in creation of the study[2]. The 200-page document is a comprehensive analysis looking at the issue on many levels and it provides a description of the situation in Poland as of September 2015. The document proposes three alternatives for the organization of the future security system in both the strategic and operational aspects. The proposals feature a detailed discussion of the actors and stakeholders with their roles in each of the variants, as well as necessary legislative changes and an estimation of associated costs. The proposed solutions are also assessed using the SWOT methodology. The document includes key recommendations from the authors. As far as we know, it is the first document of its kind in Poland that goes in such depth and breadth on this issue. We hope that the report - based on years of our experience - will contribute to improving cybersecurity of Poland.

Direct link to the document (in Polish): https://mac.gov.pl/files/nask_rekomendacja.pdf

Dorkbot botnet takedown

CERT Polska has partnered with Microsoft, ESET and law enforcement agencies including US-CERT/DHS, FBI, Interpol and Europol in disruption of the Dorkbot[3] malware family botnet. This takedown – which included sinkholing of the botnet's infrastructure – took place on 3rd of December 2015. Dorkbot is a well-known family of malware, operating under the radar since 2011. Its main objective is to steal data (including credentials), disable security applications (such as antivirus programs), and to distribute other types of malware. According to early estimates, Dorkbot has infected at least one million PCs running Windows worldwide last year, with an average monthly infection size of about 100,000 machines. Polish users were among the targets.

In the past, part of the infrastructure used to manage Dorkbot was located in Poland. Our main role in the disruption of the Dorkbot malware family was to provide analytics related to the way the botnet functioned and data on existing botnets as well as consultations on the proper way of proceeding. As a result of our activities in the international consortium, infrastructure used to botnet's management has been disposed of and the botnet traffic was forwarded to the sinkhole.

Our first encounter with Dorkbot on a larger scale took place in the autumn of 2012, when the malware began to propagate via Skype[4] among Polish users. In addition to instant messaging, Dorkbot also propagated through social networking and USB media. We performed a thorough analysis of this threat and disrupted the botnet through sinkholing, which included taking over some .pl domains used to manage it. Dorkbot domains were linked to the Domain Silver rogue registrar whose domains we took over in mid-2013[5].

[1] https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-w-cyberprzestrzeni.html
[2] https://mac.gov.pl/aktualnosci/system-bezpieczenstwa-cyberprzestrzeni-rp-ekspertyza-nask
[3] http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Win32/Dorkbot
[4] http://www.cert.pl/news/6434
[5] http://www.cert.pl/news/7539

The botnet's simple structure is based on the IRC protocol and from today's point of view is not complicated. Dorkbot has been lurking under the radar of the incident response community since its first appearance. The main danger lies in the possibility of acting as an installer *(dropper)* for other malware (similar business model was deployed by other botnet that we neutralized – a Polish botnet called Virut[6]).

According to our estimates, the present scale of Dorkbot infections in Poland is negligable. Regardless of the situation in Poland, our participation in such projects contributes to improving the security of all Internet users, and helps to prevent future attacks against Polish internet users. Estimating the true scale of the infection will be possible only after collecting data from sinkholes.

For more technical details on the Dorkbot takedown, Microsoft MMPC[7] has an extensive writeup including statistical data and a list of software installed by Dorkbot.

Incident response and threat management

In 2015, CERT Polska manually handled 1,456 incidents. Most of them were related to computer fraud (41.96%) and information gathering (18.54%).

The source of most reports was categorized as "Other Security-related Organization" (39.9%) and other CSIRTs (35.9%). The victims were mostly commercial organizations (60.2%). Both the reporter and the victim were mostly from abroad (65.2% and 47.9%).

In 2015, we recorded an increased share of phishing incidents (34%, compared to 29.88% in 2014). It should be emphasized that these were mainly incidents of phishing placed on Polish servers, or phishing impersonating Polish institutions, located on servers abroad.

Throughout the whole year we noted several major phishing campaigns attacking Polish users of electronic banking.

The most interesting were attacks where the criminals do not limit themselves to stealing the login credentials but attempt to collect (m)TAN-s as well in order to subvert two-factor authentication. As in previous years, the global scale of the problem was much greater than what was observed by CERT Polska.

As in 2014, the percentage of malware incidents remained at a fairly low level of 8.52 percent.

[6] http://www.cert.pl/news/6744

[7] https://blogs.technet.microsoft.com/mmpc/2015/12/02/microsoft-assists-law-enforcement-to-help-disrupt-dorkbot-botnets/

Over the course of 2015, criminals have used virtually every type of banking trojan available on the black market:

- Bublik
- dridex
- Dyre
- emotet
- isfb
- kronos
- slave
- tinba
- tinba DGA
- vawtrak
- Zeus

Almost all the malware was used to carry out Man-in-the-Browser attacks, intercepting online banking transactions using the so-called webinject technology. In the next step, the victims were usually directed to Automatic Transfer Systems (ATS) used by the criminals to manage fraudulent payments. At this stage we also observed that criminals utilize most of the tools available on the underground markets.

This seems to prove that the Polish market is very interesting for criminal groups, and the ROI rate for them is high enough to sustainably profit from their operations, with ability to invest in the latest malicious software and tools available on the underground markets. This applies both to natively Polish groups, as well as those coming and acting from abroad.

Statistics of handled incidents

The reported incidents received by CERT Polska are summarized in the statistics below. The numbers are based on reports from both external and our internal sources.

Incident type	Number of incidents	%
Abusive content	**146**	**10.03**
Spam	143	9.82
Harassment	0	0
Child / Sexual / Violence	0	0
Malicious software	**142**	**9.75**
Virus	1	0.07
Worm	0	0
Trojan	16	1.1
Spyware	0	0
Dialer	1	0.07
Information gathering	**270**	**18.54**
Scanning	224	15.38

Sniffing	0	0
Social Engineering	1	0.07
Intrusion attempts	**76**	**5.22**
Exploiting known vulnerabilities	45	3.09
Login attempts	9	0.62
New attack signatures	0	0
Intrusions	**10**	**0.69**
Privileged account compromise	2	0.14
Unprivileged account compromise	2	0.14
Application compromise	1	0.07
Attacks on resource availability	**35**	**2.4**
Denial of Service	2	0.14
Distributed denial of service	33	2.27
Sabotage	0	0
Attack on information security	**89**	**6.11**
Unauthorized access to information	63	4.33
Unauthorized modification of information	1	0.07
Fraud	**611**	**41.96**
Unauthorized use of resources	6	0.41
Copyright infringement	0	0
Identity theft	495	34
Other	**77**	**5.29**

Table 1. Incidents handled by CERT Polska by type

Year	Number of incidents
1996	50
1997	75
1998	100
1999	105
2000	126
2001	741
2002	1013
2003	1196
2004	1222
2005	2516
2006	2427
2007	2108
2008	1796
2009	1292
2010	674
2011	605
2012	1082
2013	1219
2104	1282
2015	1456

Table 2. Incidents handled manually by CERT Polska by year

Domain takeovers

As a part of the effort to improve the safety and security of Internet users, CERT Polska takes over or suspends domains used in malware C&C infrastructure or distribution campaigns or ones used in phishing.

NATO Locked Shields 2015 Exercise

The Polish team, with participation of CERT Polska representatives, won the third place in the NATO Locked Shields 2015 exercise. The winning team came from NATO CIRC (NATO Computer Incident Response Capability) and the second place went to the team from Estonia. Locked Shields 2015 was attended by 14 teams.

The exercise is organized by the Centre of Excellence for Cyber-Defence of NATO and involves defending a simulated network of a small country. This year the network was comprised of two Internet service providers, a power plant, telephone service, military, research, office and private networks and a reconnaissance drone control center.

The defenders were to protect the entire infrastructure from attacks, to ensure the operation of services to civilian users and to collaborate with teams from neighboring countries in combating threats. Attacks included a wide range of threats - saturating links (DDoS), taking control over the flow of data on the network (BGP hijacking) and malware and backdoors placed in defended computers by attackers before the simulated war.

The score was not only based on the technical expertise, but also on the cooperation between the teams, the quality of services provided to end users and ensuring the operation of critical infrastructure - the simulated power plant. In 2015, the tasks included for the first time defending a drone (unmanned patrol aircraft) against the (cyber) hijacking. Another new aspect was the extensive use of IPv6.

Secure 2015 conference and Secure Hands-on workshops

XIX Conference on ICT security SECURE took place on 14-15 October 2015 in Copernicus Science Centre in Warsaw. The conference was attended by over 400 participants who could choose among as many as 45 presentations and sessions, lined in up in four parallel tracks.

The strategic partner of the event was the National Centre for Research and Development, and the honorary patronages were granted by the Ministry of Administration and Digitization, Ministry of Science and Higher Education and the European Union Agency for Network and Information Security ENISA.

Lighting talks were again part of the conference agenda, and were presented by the conference participants (by earlier arrangement). This formula receives a warm reception from the audience, due to variety of topics presented and dynamical form of the five minute presentations.

The Supreme Audit Office presented the conclusion of the audit carried out in 2014 on the subject of cyberspace protection activities and legal obligations compliance by the government sector in Poland. Right after the presentation, a panel discussion between representatives of concerned organizations, including NASK and Internal Security Agency debated on the presented state of affairs.

The conference was not devoid of technical talks. Top-ranked among them was introduction to malware analysis by Lenny Zeltser from the SANS Institute, Jeremy Brown presented his approach to “Hacking Virtual Appliances” and Maciej Kotowicz from CERT Polska has shown his research under the title “Unpacking: from art to tradecraft”. Many talks focused on specific attacks and criminal groups operations: Łukasz Siewierski of CERT Polska talked about The Postal Group and F-SECURE’s Artturi Lehtiö has shown his research on “The Dukes” APT campaign.

Presentations from Polish security bloggers were also well received by the participants: Piotr Konieczny from niebezpiecznik.pl talked about financial attacks (“How we stole 9,000,000 PLN from Polish companies”), and Adam Haertle from zaufanatrzeciastrona.pl focused on metadata (“It’s just metadata”). The conference keynote was “Programming and hacking” by Gynvael Coldwind, the leader of the Dragon Sector CTF team.

Less technical, but enthusiastically welcomed was the presentation on craft beers by Michał “Doc” Marańda, which was the last one for the first day of the conference as it was the prelude to the evening party.

Traditionally, on the day before the conference, members of CERT Polska led the SECURE Hands-on training workshops.

Slides from the conference are available on the conference website http://www.secure.edu.pl/historia/2015/program.php and the videos from talks are on YouTube: https://goo.gl/QteuyE

European Cyber Security Month

EUROPEJSKI
MIESIĄC
BEZPIECZEŃSTWA
CYBERNETYCZNEGO

In October 2015 the European campaign to popularize computer security awareness took place. This was the fourth time in Europe and the third time in Poland that the campaigns was carried out.

During the European Cyber Security Month, the European Commission and the European Union Agency for Network and Information Security (ENISA) supported various initiatives across the European Union, aimed at the users of the internet. NASK and CERT Polska joined this noble initiative by creating a website bezpiecznymiesiac.pl, which featured events carried out by NASK as part of the campaign.

One of the activities was the quiz "Safety on the Internet", that allowed the broad range of internet users to check their knowledge of computer and data communication security. The questions verify the knowledge of the topics covered in the Polish edition of the monthly "OUCH!" bulletin, published by the SANS Institute and CERT Polska. The quiz is also of educational value, because each question is accompanied by an expert commentary and references to further sources of information on given topic.

Another, more technical HackMe-style challenge was published on the CERT Polska blog. The contestants' task was to find a password hidden in a dump of network traffic recorded in a PCAP file. The challenge proved to be difficult and the deadline had to be extended. The first participants to come up with correct answers were awarded with books on reverse engineering of software.

The challenge is still available (with solution) at: http://www.cert.pl/news/10766.

OUCH! Newsletter

OUCH is an online, monthly bulletin for Internet users. It presents security tips on topics like "Safe online gaming", "Generational cyber-gap", "Social Media", "Backup and Data Recovery" - these are just a sample from 2015 issues. Each issue includes a brief, accessible presentation on a selected topic with a list of tips on how you can protect yourself, your loved ones and your organization. The newsletter is published each month in 26 languages.

The Polish version of the newsletter is being published since 2011 and is a result of cooperation between CERT Polska and the SANS Institute. The content of each issue of OUCH! is created and consulted with the SANS 'Securing The Human" team. The authors of the newsletter are working directly in the area of IT security as auditors and administrators. CERT Polska creates a Polish version of the bulletin translating its contents from English, as well as adapting the discussed details of the issues to the Polish realities.

The target audience of the newsletter are users who do not have extensive knowledge of computer security, thus the topics of the newsletter are presented in a simple and accessible way. CERT Polska encourages the public to distribute OUCH! at homes, businesses and educational institutions. Raising awareness about risks among businesses and households helps protecting the general public in all social contexts.

OUCH! is available under the Creative Commons license (BY-NC-ND 3.0), which means that the newsletter can be distributed within freely, provided that it is not used for commercial purposes. All Polish editions of OUCH! can also be found at: http://www.cert.pl/ouch.

Over **25 000** people took the online cybersecurity quiz.

Hackme challenge was downloaded **910** times.

Projects

n6

The n6 platform is an automated system for collecting, managing and sharing threat intelligence. In 2015 it handled a record number of more than 200 million notifications of threats in Polish address space. Accurate figures, broken down by types of threats and autonomous systems can be found in the "Statistics" section of this report.

The platform shares the data through an application programming interface (API) based on HTTP and REST architecture. We supplemented it with a test interface that is based on STOMP streaming protocol[9], which allows users to receive information about threats as a stream, minimizing the delays that often occur when other methods of data exchange are employed. Additionally, we have provided the users with ability of receiving periodic notifications when new information about their networks is available. Notifications are especially useful for people managing smaller networks, for which we may not have daily data about new threats.

Access to the n6 is free, more information is available on the project website: http://n6.cert.pl/. To take advantage of the new features, please contact us at n6@cert.pl.

ILLBuster

The ILLBuster project began in 2014 with the purpose of creating an engine for automated detection and analysis of harmful websites. The detection is done by analyzing the DNS traffic, and then the system scans the website looking for malicious code, child sexual abuse imagery, phishing sites, and offers of sale of counterfeit goods.

The technical aspect of the project ended in 2015 as its goal was to create and deploy software for detecting and analyzing of the discovered websites. NASK was the leader of this task and the ILLBuster is based on Honey Spider Network 2, a software developed earlier at NASK.

In late 2015 the intended users of the system (Italian law enforcement authorities) began testing of the system in their daily operations, and the project will be formally completed in February 2016.

The project is funded by the European Commission under the grant program ISEC HOME / 2012 / ISEC / AG / 4000 "Prevention of and Fight against Crime", and is realized by the consortium consisting of two Italian universities - Università de Cagliari and Università degli Studi di Milano-Bicocca, American University of Georgia, the Italian police - Guardia di Finanza and the Polizia Postale, a Swedish company Netclean, the Italian NGO Tech and Law Center together with NASK / CERT Polska.

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

NECOMA

CERT Polska participates in a Euro-Japanese research project NECOMA (Nippon-European Cyberdefense-Oriented Multilayer Threat Analysis). The consortium consists of ten organizations from Europe and Japan.

One of the significant achievements of the project was the integration of the Japan-developed centralized network threats data storage, with a similar system, called n6 and used by CERT Polska. From the technical standpoint integration was achieved using our actively developed n6 SDK library[10]. The library is licensed under the conditions of GNU General Public License. Also, in October 2015 the development of modules designed to detect and address network threats was finished. After that the consortium activities focused on delivering the technology demonstrator.

NECOMA is funded by the Ministry of Internal Affairs and Communications of Japan and the European Union, as part of the 7. Framework Programme (FP7 / 2007-2013), the grant agreement number 608533. More information, including publications are available on the official website: http://www.necoma-project.eu/

CyberROAD

CyberROAD is a research project funded by the European Commission under the FP7 program, which aims to identify current and future problems in the fight against cybercrime and cyber terrorism and develop research roadmap to cover the identified problems. The project started in May 2014 and lasts 24 months. It brings together 20 enti-

[9] Simple Text Oriented Messaging Protocol, https://stomp.github.io/

[10] The library is available on GitHub account CERT Poland at https://github.com/CERT-Polska/n6sdk

ties from 11 countries. Poland is represented in the form of NASK / CERT Polska.

In 2015, the project refined the second and third series of surveys aimed identifying the current challenges for the technological, social, economic, political and legal framework for the fight against cybercrime and cyber terrorism. The research focused on Poland as an example country for the comparative analysis of cybercrime in relation to other European countries and the whole world. Preliminary results of the research survey were presented during the SECURE 2015 conference.

In 2015 the project consortium also worked on the development of taxonomy on cybercrime and cyber-terrorism and the first scenarios of future research on these issues. In August 2015 the ARES conference, held in Toulouse, organized the first public workshop of the project.

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

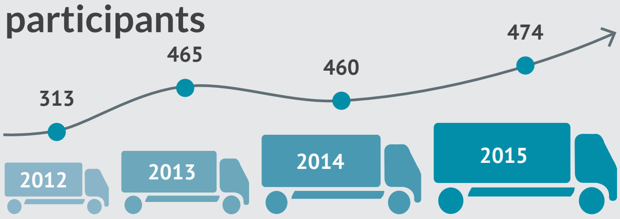
SECURE 2015 Conference

45 talks

2 days

SECURE is an unique opportunity to get to know the work of leading security researchers from around the world.

Number of SECURE conference participants



SECURE 2016 Conference

2016

25-26 October

AIRPORT Okęcie Hotel, Warsaw, Poland

The state of the Internet in 2015 on the basis of information gathered by the CERT Polska

Global view

As 2015 progressed, Internet security was mostly present in the media in the form of reports on personal data leaks. The sensational attack on Ashley Madison website was widely discussed[11] and had a considerable impact on the lives of users whose data have been disclosed. This included media attributing suicides to the consequences of the leak[12]. It was one of the biggest and most dangerous data leaks in history, comparable only in our opinion to the July 2015 leak of four million personal records maintained by the US government Office of Personnel Management for the purpose of security vetting. Unlike Ashley Madison, the data were not disclosed on the Internet, but passed to the instigators of the attack, assumed by US government to be China[13].

In 2015, security researchers also revealed the scale of Internet espionage conducted as what security researchers label Advanced Persistent Threat (APT) campaigns. Some of the APT campaigns were attributed to state-sponsored actors, eg. The Equation Group was allegedly a US National Security Agency[14] operation, Animal Farm purported as French[15] and the APTs called The Dukes / CozyBear[16], Sofacy / APT28[17] and Turla / Uroburos / APT29 are assumed to come from Russia. The techniques used by the actors behind these campaigns are characterized by cleverness and ingenuity. Operators of Turla used redirection of traffic through satellite links to make their botnet communicate with its C&C server[18] and Equation Group implanted Trojan horses in the firmware of the targeted computers' hard drives. Unfortunately, backdoors found in Cisco routers around the world could not be attributed to any known APT (more on the attack in the SYNFul Knock section below). Also, the perpetrators of the DDoS attack on the global DNS system were not identified, even if this was a highly coordinated attack on the worldwide core internet infrastructure.

At the end of the year backdoors in Juniper networking equipment were found. Somebody purposely introduced an incorrect implementation of the random number generator to the firmware, which allows an attacker, who knows the cryptographic characteristics of the device, to decrypt traffic going through the virtual private network (VPN) established on the device. The second Juniper backdoor was an universal password implanted in the firewall software that allowed to log in to the machine's administrator account.

At least two events – namely, the compromises of Gamma Group and Hacking Team – combined the trends of data breaches and APTs in a peculiar, synergistic way. The two companies were developing and selling lawful spying software to law enforcement authorities in various countries. In both cases the companies' networks were penetrated and internal documents were published. In case of Hacking Team the documents included all company products' source code, exploits, certificates and copies of internal and external correspondence.

The year ended with a case of offensive use of the Internet as a battlefield. On December 23, the operators of Black Energy APT attacked computers controlling the power grid of Ukraine, and the attack caused a few hours of electrical blackout in hundreds of thousands of households in the region of Ivano-Frankivsk.

Commercial computer crime also evolved. An example of a disruptive approach in criminal malware operations was Carbanak. Cybercriminals used the malware to attack corporate networks of banks, gain access and control of internal systems and eventually steal money using various techniques – from alteration of data in transactional systems

[11] http://krebsonsecurity.com/2015/08/was-the-ashley-madison-database-leaked/
[12] http://www.bbc.com/news/technology-34044506
[13] http://arstechnica.com/security/2015/06/encryption-would-not-have-helped-at-opm-says-dhs-official/
[14] http://www.kaspersky.com/about/news/virus/2015/equation-group-the-crown-creator-of-cyber-espionage
[15] https://securelist.com/blog/research/69114/animals-in-the-apt-farm/
[16] https://labsblog.f-secure.com/2015/09/17/the-dukes-7-years-of-russian-cyber-espionage/
[17] https://securelist.com/blog/research/72924/sofacy-apt-hits-high-profile-targets-with-updated-toolset/
[18] https://securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sky/

and databases to controlling ATMs to directly dispense cash[19].

In summary, in 2015 the Internet has become openly a platform for professional attacks motivated by political or financial gains. This was reflected by the language used to describe information security issues in 2015: any event where the Internet was used as a tool of espionage, political leverage and warfare was labelled *cyber*. As a prefix or a standalone word it appeared in 2015 in numerous statements from politicians, business leaders, military and marketing materials. Approaching the issue in a more formal way, the military understands *cyber* as the fifth domain of warfare, after land, water, air, and space (according to the US military doctrine).

Yet another area where new threats arise is the Internet of Things. Both industrial control systems and consumer equipment can be found accessible from the Internet with full administrative access enabled by default. Examples of Internet of Things threats are attack on Ukraine power grid, and global outage of Samsung Smart TVs due to unavailability of cloud API provided by Samsung.

Security researchers managed to break the software-hardware barrier which was considered impenetrable until now – modern RAM chips density makes the memory prone to changing stored bits with intensive, repeated operations on a single row of memory cells. This vulnerability was demonstrably used to break out from a sandbox environment and it can be implemented even in JavaScript – making it possible to embed an exploit in a web page.

As banking botnets mitigation methods evolved, the criminals adapted too, shifting their focus from internet banking to ransomware. With ransomware, they do not need to face a strong adversary like a bank, capable of deploying system-wide mitigations on many levels, and the victim is only protected by a personal or organizational data backup routine, not very common among individual home PC users.

Besides botnet mitigations, 2015 saw rapid growth in exchange of incident data and indicators of compromise. CERT Polska led the way with the guides on utilizing and exchanging actionable information that we wrote, commissioned by ENISA[20]. Our own contribution to the field is the research and development that we do as development of the n6 platform.

The problems in cryptography and public key infrastructure

The year 2015 brought many discoveries of vulnerabilities in the cryptographic libraries and tools, as well as many news about problems and bugs concerning network security mechanisms. We consider the following issues as the most important ones.

Logjam

The Logjam attack is based on enforced downgrade of cryptographic keys to a weak set of keys in TLS connections. This makes the connection vulnerable to *man-in-the-middle attacks* (MitM) and eavesdropping of the transmitted content[21]. The Logjam targets Diffie-Hellman scheme, in which sufficiently large prime numbers are exchanged. Due to difficulty of calculation of the discrete logarithm, which could reveal what numbers were sent, utilization of the Diffie-Hellman scheme ensures the secrecy of data transmission. By forcing usage of the DHE_EXPORT grade keys, length of prime numbers is limited to 512 bits, which comes from US export restriction laws established in the 1990s. Most of the hosts supporting DHE_EXPORT set use one of the three primes, which are statically stored in the application code. Knowing this, the researchers performed calculations for earlier steps of the discrete logarithm algorithm for this set of numbers. During a real data exchange, the last step of computations could be performed in 70 seconds, thus allowing to perform a MitM attack on the connection and decryption of exchanged data. According to the discoverers at the moment of disclosure more than 8% of the first million of most popular domains could be vulnerable as well as the majority of the web browsers.

FREAK

The Factoring Attack on RSA-EXPORT Keys (FREAK) is similar to Logjam as it is also based on enforcing the use of the export grade keys in TLS, however in this case the RSA mechanism is attacked[22]. The FREAK allows a *Man in the Middle attack* and sniffing the contents of sent messages. In many implementations (e.g. in Apache's mod_ssl) cracking a single key allowed to eavesdrop all sessions, because once an export grade temporary key was selected, the keys would not change until the server was restarted.

[19] https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/

[20] https://www.enisa.europa.eu/media/press-releases/new-guide-by-enisa-actionable-information-for-security-incident-response

[21] https://weakdh.org/

[22] https://FREAKattack.com/

The attack consists of a number of separate steps. During the establishment phase of an encrypted connection, the attacker downgrades the RSA keys in the client's request with export level (RSA_EXPORT) keys, which are at most 512 bits long. The server responds with a corresponding key, and the client, due to a bug in the cryptographic library, accepts this answer, even though it does not match the requested grade. The attacker can now perform factorization of exchanged keys, that due to their small length is not difficult, and therefore learn the private keys, what allows him for decryption of exchanged data. The researchers who found this vulnerability utilize the EC2 infrastructure to perform a real attack. It was achieved in 7.5 hours, at a cost of around 100 USD. The main conditions for performing the FREAK attack is a bug in the cryptographic libraries, the relative ease of keys' factorizations, the servers' support for export grade RSA keys and the infrequent change of the temporary key. According to the authors at the time of disclosure approximately 26.3% of all HTTPS servers were vulnerable to the FREAK attack.

Data collected by the Shadowserver Foundation shows that in Poland 5,205 servers support RSA_EXPORT keys (as of 10 December 2015).

Freestart Collision in SHA-1 algorithm

In November 2015, Marc Stevens, Pierre Thomas and Karpman Peyrin published a paper in which they presented a special case of a collision in SHA-1 hash function[23]. This is not a complete collision, since the attacker can choose the initialization vector. However, it is a big step towards the full breaking of SHA-1, as in the case of the MD-5 function. The attack was performed by scientists in 10 days with a 64 GPUs cluster.

According to the authors the collision of SHA-1 in autumn 2015 costs from 75 to 120 thousand USD using the infrastructure of Amazon EC2. It is an important estimation, because earlier it was expected to cost approximately 170 thousand USD in 2018[24]. In such perspective, the attack is within the financial capabilities of criminal groups.

The most important conclusion is the need for faster withdrawal of SHA-1 from common usage. For example, the latest versions of Google Chrome will display a warning on the websites if the site's certificate public key is signed using SHA-1, and the certificate is valid after 1 January 2016[25].

Errors in the OpenSSL

One of the major vulnerabilities in the OpenSSL library in the last year was a bug which allows issuing certificates, that do not have to be signed by any valid certification authority (CA). The error was dubbed as the "Alternative chains certificate forgery" and assigned a CVE number CVE-2015-1793[26].

During the certificate verification process, the OpenSSL library checked if a correct chain of signatures could be created up to the CA. If it failed, an alternative chain of certifications was searched. An error in the implementation caused that during this search in some situations the CA flag (indicating the certification authority) of the top certificates was not checked. This allowed to perform a *Man in the Middle attack* by utilizing a specially crafted certificate issued by the attacker, which was signed with a malformed certificate chain.

Problems with network devices

At the end of December 2015, Juniper Networks announced two independent vulnerabilities in certain versions of ScreenOS operating system, which controls firewall devices. According to the official information, these changes have been introduced in an unauthorized way.

The vulnerabilities were given numbers CVE-2015-7755 and CVE-2015-7756. The first one referred to the existence of a backdoor in SSH and Telnet services. It enabled gaining remote administrative access to a vulnerable device by using a hardcoded password.

The second CVE referred to the possibility of decrypting VPN traffic. Vulnerable operating systems were equipped with a random number generator based on Dual_EC_DRBG algorithm, which potentially may have a built-in backdoor. The generator was used to generate keys to encrypt the VPN traffic. The attacker responsible for changing the source code replaced some of the parameters of the RNG algorithms, what allowed them to reveal generated numbers. Finally, it gave the possibility of passive decryption of the VPN traffic.

[23] https://sites.google.com/site/itstheshappening/

[24] https://www.schneier.com/blog/archives/2012/10/when_will_we_se.html

[25] http://blog.chromium.org/2014/09/gradually-sunsetting-sha-1.html

[26] https://www.openssl.org/news/secadv/20150709.txt

Problems with certificates in the Public Key Infrastructure

Public key certificates, which are part of the Public Key Infrastructure, are a very important element of encrypted connections utilizing the SSL and TLS protocols. They provide means for verification of identity of data exchange parties, for example a bank's webserver, and prevent from Man in the Middle attacks. For this reason any reports of abuses or manipulations in the processing of these certificates instantly appear in news headlines.

In 2015 the most famous cases were problems with certificates that were installed by the computer manufacturers.

Chronologically the first were Lenovo's problems. On some of their devices, the company installed an application and a root certificate belonging to Superfish, Inc.[27] The application was adding advertisements to web pages visited by the user, and the root certificate allowed it to interfere with the content secured with the SSL / TLS protocols. Probably all machines equipped with this software had a single shared private key associated with the root certificate. Unfortunately, the certificate was eventually broken and made public, thus exposing users to Man in the Middle attacks[28].

A similar situation occurred with devices manufactured by Dell company, where an additional root certificate called eDellRoot was installed[29]. Unfortunately, the private key was also available on the machines, and ultimately it was also publicly disclosed. After closer investigation of certificate stores it was found that Dell installed on its computers also a second certificate, DSDTestProvider, which had a similar potential for abuse.

The manufacturers published information about those problems on their websites along with instructions how to protect the vulnerable equipment.

Other type of abuse of the Public Key Infrastructure occurred as a result of issuance of EV type (Extended Validation) precertificates by Symantec for the domains google.com and www.google.com[30]. The certificates were not issued at the request of the Google, and were used for internal testing. After the audit in Symantec it was found that more crafted certificates were issued for various domains[31].

This event is quite important due to the higher level of trust for EV certificates in the PKI. Usually the DV *(Domain-Validated)* certificates are issued to a person who confirms the control of the domain name for which the signature is generated. Whereas Extended Validation certificates are issued by the CA after additional verification of the applicant, e.g., checking the actual representation of the legal entity[32]. Web browsers indicate different levels of trust by using different user interface elements depending on the type of certificate, for example some versions of the Mozilla Firefox display a gray padlock for sites with DV certificates, and green for the ones signed with EV certificates[33].

Cases of abuse were detected by Google through the mechanisms introduced by the Certificate Transparency project[34], which aims to remove some of the problems in the current architecture of the PKI, e.g., usage of incorrectly issued certificates or certificates issued by malicious CA.

Another case of manipulation of certificates related to Google was performed by the Mideast Communication Systems (MCS). The certificates were issued without owner's knowledge and were signed by a Chinese CA China Internet Network Information Center (CNNIC)[35]. Probably none of these certificates was used to conduct attack. The official statement by the MCS blamed human error in handling a separated test environment, which allegedly caused a certificate leak noticed by Google[36]. Eventually the root certificate of CNNIC was withdrawn from the trusted list in Chrome, Firefox and IE.

[27] https://support.lenovo.com/pl/pl/product_security/superfish

[28] http://arstechnica.com/security/2015/02/lenovo-pcs-ship-with-man-in-the-middle-adware-that-breaks-https-connections/

[29] http://www.dell.com/support/article/us/en/19/SLN300321

[30] https://googleonlinesecurity.blogspot.com/2015/09/improved-digital-certificate-security.html

[31] https://googleonlinesecurity.blogspot.com/2015/10/sustaining-digital-certificate-security.html

[32] https://www.eff.org/deeplinks/2015/09/symantec-issues-rogue-ev-certificate-googlecom

[33] https://support.mozilla.org/en-US/kb/how-do-i-tell-if-my-connection-is-secure

[34] http://www.certificate-transparency.org/

[35] https://googleonlinesecurity.blogspot.com/2015/03/maintaining-digital-certificate-security.html

[36] http://www.mcsholding.com/MCSResponse.aspx

Use of Domain Generation Algorithms in botnets

Botnets use Domain Generation Algorithms (DGAs) to provide means for communication between bots and the Command and Control server. The list of generated domains is usually long (there may be even tens of thousands) and changes over time. Algorithmically generated domain names most often take the form of pseudo-random strings of characters, such as gdvf5yt.pl. It is often quite hard to register the domains before the criminals do, especially in a number of different top level domains. On the other hand, without the information which of the generated domains will actually become registered, it is inefficient to blacklist them all. In order to obtain the list of generated domain names, the particular algorithm has to be reverse engineered. The pseudo randomness of domain names makes it impossible to predict them, and ensures their availability for registration (there are usually very few collisions with already registered domains). It also considerably increases the number of domains possible to create and use as C&C infrastructure.

Simplified diagram of DNS requests for a C&C server's IP address in DGA botnet is presented below.

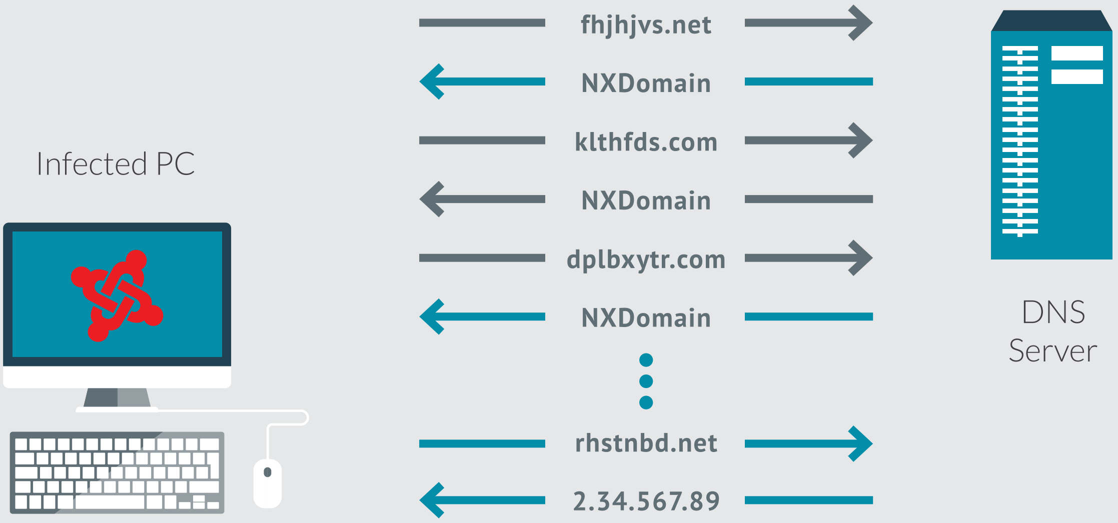


Figure 1. DGA botnet queyring for C&C server address

The infected computer queries for domains from the generated list. Due to the fact that most of them have not been registered, the bot gets numerous NXDOMAIN responses, what indicates nonexistence of the queried domains. The search usually continues until the IP address of C&C server is found.

Domain generation algorithms are fed with a seed, which is shared between the owner of the botnet - the botmaster - and bots. This ensures that the set of generated domains is the same in the entire botnet. So far, some algorithms use the current date as the seed, other ones use strings in the internal configuration of malware, or data from external sites, for example from Twitter. The length and the distribution of characters in created domain names is different between families of botnets. In addition, they are registered in different top level domains, e.g., .com, .org, or .info.

DGA botnets in Poland

The most important families of DGA botnets attacking users in Poland are:

- Tinba DGA,
- ISFB / Gozi2,
- Bamital,
- Conficker,
- Virut,
- Nymaim,
- Dyre / Dyreza.

Example: Tinba DGA

Tinba, or TinyBanker, is used to steal login credentials for internet banking. One of the versions uses DGA to generate domain names for the C&C servers. The generated domains are registered in various TLD-s, for example .ru, .su, .net, .com, .org, .pk, .in. The seed for the domain generator is a set of two keys: the first is a selected domain name and the second is a string without a specific meaning.

Example domains for sample 4e943eb5a205b08e8fc3f23a856e8dd8554800c4bb037c096b1340f806ff261e (source: malwr.com) are provided in the table below.

i28h63gdb67uehdi.cc			
epxylvumlrfe.com	edmjknrfpqsh.com	uutdiihloccx.com	fgxlkkfiptid.com
epxylvumlrfe.net	edmjknrfpqsh.net	uutdiihloccx.net	fgxlkkfiptid.net
epxylvumlrfe.in	edmjknrfpqsh.in	uutdiihloccx.in	fgxlkkfiptid.in
epxylvumlrfe.ru	edmjknrfpqsh.ru	uutdiihloccx.ru	fgxlkkfiptid.ru

Table 3. Example domains generated by Tinba DGA sample

The first domain in the list above is in the .cc TLD, and as already mentioned, it is a fragment of the seed for the domain generator. Each of the created pseudo-random strings is joined with the selected set of top-level domains (here: .com, .net, .in, .ru). Domain names constructed in this manner are subsequently queried by bots until a response with the IP address of the C&C server is received.

Trends in the development of DGA methods

The utilization of DGAs in botnets forced researchers to create new detection methods. In response, malware authors continuously refine mechanisms they create. The following are the probable directions of development of the DGAs. Some of the described methods (e.g. use of anonymizing networks or natural language words) have been already applied in practice.

Trends in the development of DGA methods:

1. New domain namespaces:
    1. domains that contain non-ASCII characters *(Internationalized Domain Names);*
    2. alternative networks of DNS root servers, for example OpenNIC, Namecoin;
    3. anonymizing networks, for example Tor (to some extent).

2. Generation algorithms improvement:
    1. improvement of the algorithms' quality, including avoiding obvious errors in implementation;
    2. reduction of the probability of collisions with other DGA botnets or legitimate domains.

3. Reduction of introduced anomalies:
    1. generation of domains which resemble those created by humans, eg., by the use of natural language words;
    2. manipulation of time between consecutive queries for the generated domains;
    3. reduction of the number of queried domains.

4. Obfuscation of malware's DNS network traffic:
    1. in case of detection of malware analysis tools querying for a different set of domains or not using the DGA mechanism to conceal such capability;
    2. utilization of several sets of generated domains to obfuscate the actual one, for example by using local seed.

5. Changing schemes of generator seeds' distribution:
    1. changing the generator seed during operation;
    2. publishing seeds on popular websites (with plain text or by using obfuscation or steganography);
    3. segmentation of bots in a botnet by using different seeds.

Threats to the Polish Internet

Global Internet threats tend to materialize in Polish network later or on a much smaller scale.

The biggest threat to an average internet user in Poland were banking trojans. The banking malware usually arrives on Polish market with some delay in comparison to western countries, examples being Dyre and Dridex. The infections with those malware families did happen in Poland, but the main targets of its operators were not Polish banks and Polish users. First Dyre infections in Poland started in mid-2014, and were targeted against foreign institutions. Attacks against Polish users started at the beginning of 2015.

Poland has its own small malware market, with the most known example of local product being VBKlip/Banatrix, which is a Polish malware that replaces the recipient's account number during the copy-paste operation. Such attacks are still the local specialty. The Polish malware family was in 2015 joined by Slave, a malware utilizing classical web-inject technology to perform Man In The Browser attacks. Compared to the situation further east, the Polish malware market seems tiny.

Similarly to the global tendencies, the Polish criminal underground has its own underground forums, with the most famous being ToRepublic. As it was the case with Silk Road, in 2015 Polish Police arrested some of the ToRepublic administrators, suspected of stealing money from local governments' accounts. Increased success rate of police operations is a big step in securing the Polish internet.

Targeted attacks were a novelty in 2015. It was mostly *spear-phishing*, used against persons, organizations and businesses to steal data (including financial data), sometimes to request ransom for not publishing (dumping) the data online.

We are aware of some Cryptolocker infections in 2015, but the infection campaigns seem less intensive as compared to western countries. Also in 2015 Polish institutions weren't targeted by groups such as DD4BTC or Armada Collective, that perform DDoS attacks to request ransom. We expect this situation to change. Also the number of Polish data leaks was small, and the scale of the leaks was incomparable to, for example, Ashley Madison leak.

Another difference between local and global threat landscapes was the lack of PoS malware.

In 2015 we have observed espionage–related activity of APT groups that are usually assumed to have ties with Russia (see below).

APT in Poland

Advanced Persistent Threat (APT) is the name given to high-tech attacks on political, economic, industrial and military targets. The main purpose of such attacks is information stealing. According to Richard Bejtlich[37] APT should be defined as:

- **Advanced** - as attackers use a variety of techniques and methods to effectively break the defenses of the target, utilizing known vulnerabilities, but also discovering new ones, used specifically to conduct the attack.

- **Persistent** - due to the formal objective of carrying out a successful attack. The operation is performed clandestinely to draw no attention. After acquiring access to victim's single system, lateral movement in the network is conducted to expand control to other machines, so that long-term and persistent presence in the network is established.

- **Threat** - because the attacker is an organized group with an sufficient technical knowledge, resources and budget. The threat is persistent, as long as the attacker is motivated (politically, economically) to steal the victim's information. The software used in attack is not dangerous as it is, but the people behind the operation are.

[37] What Is Apart and What Does It Want?, http://taosecurity.blogspot.com/2010/01/what-is-apt-and-what-does-it-want.html

Below we discuss the main APT actors targeting Poland. The descriptions are based on publicly available sources, which contain detailed specification of campaigns and tools used in the attacks.

It should be emphasized that in the description of the APTs we do not indicate the source of the attacks, due to the high uncertainty of the process of attribution. Evidence used in this process are often clues that can be easily planted by attackers to deceive researchers and raise false flags. Nevertheless, the authors of the cited reports try to give the approximate source of the attacks, as well as a set of information supporting their assumptions.

Duqu 2.0

Duqu 2.0 is known for successful penetration of the internal systems of Kaspersky Lab, a Russian developer of security solutions. The company published a comprehensive report[38] after the discovery of the presence of the intruders. The APT targeted, among others, events related to meetings of the P5 + 1 group, engaged in negotiations on the Iranian nuclear program, and commemoration of 70th anniversary of the liberation of Auschwitz death camp in Poland.

The original infection at Kaspersky had likely occurred through the use of a 0-day exploit. Then a reconnaissance phase on the local network was carried out and other local machines were compromised, also using 0-day vulnerabilities. A special MSI file was transferred between machines which contained malicious software. The file is built of several layers of data that are compressed and encrypted. More than 100 Duqu 2.0 modules are known, providing various functions, e.g., collection of information about the system, user, network environment, the domain and databases. One feature distinguishing Duqu 2.0 from common malware is its lack of any persistence mechanism to ensure a permanent presence in the infected systems. The malware is only stored in RAM, which allows it to remain undetected for a long time. The stealthiness is achieved by using kernel-level code, implanted through 0-day vulnerabilities, which according to the authors of the Kaspersky's report, is an evidence of technical advancement of Duqu 2.0. However, some of the compromised machines do have installed malicious hardware drivers to provide a foothold in the network in the event of loss of control. The drivers are implanted on hosts with high uptime, which serve as the point of contact between the machines on the local network and the C&C servers. Additionally, Duqu 2.0 uses a wide range of protocols and communication methods depending on the location of the compromised machine. These can be HTTP / HTTPS protocols, SMB / RDP, system pipes, as well as image steganography.

CozyDuke

CozyDuke, also called CozyBear or EuroAPT, belongs to the family of APT tools called the Dukes[39]. According to information published by Prevenity, Cozy Duke has been used to attack Polish institutions[40], and it was also used against targets in other European countries. The infection scenario was usually the same: the user received an e-mail with a forged sender address, masquerading as an institution of the European Union. The message included a link to a pdf file located on a server of the organization associated with the EU. In reality, the downloaded file was a zip archive containing self-extracting RAR archive, which in turn included two other files. Eventually an insignificant pdf file was presented to the victim, but in the background the main malware was dropped on the victim's system. Another type of decoy used was a video of monkeys in an office (hence the other name of this threat - "Office monkeys"). The CozyDuke can download additional tools, but also modules from other sets of the Dukes family, e.g. from the Onion-Duke, the SeaDuke or the HammerDuke. The capabilities of the CozyDuke include stealing passwords and their hashes, creating screenshots, and executing remote commands via the system command line. Acquired information is sent to the attackers through HTTP / HTTPS, and in case of any problems with the above, the communication fails over to Twitter.

Uroburos

The Uroburos APT, also called Turla or Snake, was probably developed in association with the worm Agent.BTZ, which was used in the attack on the local network infrastructure of the US Army in 2008[41]. The Uroburos is used to attack similar targets - ministries, embassies, military, education or pharmaceutical companies. According to Kaspersky Lab, the group behind this APT has been active for over 8 years and has attacked 45 countries, including Poland[42,43]. Symantec,

[38] The Duqu 2.0.Technical Details. Version: 2.1, https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf

[39] The Dukes 7 Years Of Russian Cyber-Espionage, https://labsblog.f-secure.com/2015/09/17/the-dukes-7-years-of-russian-cyber-espionage/

[40] EuroAPT, http://malware.prevenity.com/2015/03/euroapt.html

[41] Agent.btz: a Source of Inspiration ?, https://securelist.com/blog/virus-watch/58551/agent-btz-a-source-of-inspiration/

[42] Satellite Turla: APT Command and Control in the Sky, https://securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sky/

[43] The Epic Turla Operation, https://securelist.com/analysis/publications/65545/the-epic-turla-operation/

which uses the name Turla for Uroburos, associates it with another tool, the EpicTurla, and attributes the attacks of the Waterbug group[44]. According to Symantec, Uroburos/Turla is responsible for attacks on more than 100 countries and more than 4500 computers.

The scenario of Uroburos attack is quite complex[45]. At the beginning a single machine is infected with EpicTurla, which is less advanced than Uroburos/Turla. The machine is analyzed and a backdoor is installed. After that a reconnaissance of the surrounding network is performed. Eventually the Uroburos/Turla is delivered to conduct an actual APT attack. The attackers may quit at each of the above steps if the compromised host is not suitable for their purposes or it is out of their scope of interest. According to Symantec, the initial infections are performed by targeted phishing or by watering hole attacks. In the latter variant, websites visited by targets of the attack are infected with malware. The first time a user visits such a compromised website an individual profile is created, and if it fits interest profile, on the next visit a suitable exploit is used.

The code of Uroburos/Turla is executed from the driver level in the kernel by exploiting a vulnerability in virtualization software VirtualBox[46,47]. It should be noted that the authors are constantly changing their software, using new techniques to hide their presence in the system. The architecture of this malware allows adding new modules without the need of recompiling the rootkit. Interestingly, machines running either Windows or Linux can be infected[48].

The Uroburos capabilities include stealing passwords and their hashes used for authentication, collecting information about the machines and networks, and stealing documents. It uses different protocols for communication: HTTP, SMTP[49], system pipes, but also covert channels in HTTP and SMTP protocols. As in the case of the Duqu 2.0, the Uroburos/Turla sends information outside the local network by using compromised machines operating as a sort of a proxy.

SYNful Knock

The SYNful Knock is a name given to a number of special modifications in Cisco routers' software, which implanted a backdoor to these devices. The modification was performed secretly and allowed unauthorized access to networks from affected routers. Furthermore, an attacker could download additional modules extending basic capabilities. Information about this threat was originally published by FireEye[50].

The modification was implanted permanently in the device's firmware, but any additional module was kept in the volatile memory and was erased when the device was rebooted.

The SYNful Knock is especially dangerous, because routers are not typically searched for backdoors and are often not monitored for backdoor communications. Hence they provide a good place for gaining a foothold while infiltrating internal networks.

The modified equipment could be contacted for two purposes: to load additional modules via the HTTP protocol or to obtain remote access through the use of a serial console port or telnet. In the first case it was necessary to send a set of specially crafted TCP segments on port 80, for example the first segment of the opening combination must have appropriate values in the sequence and acknowledge number fields. In the second case the remote access was possible via telnet and serial console port (but not through SSH), by simply providing only the user name. The SYNful Knock was identified in Cisco Series 1841, 2811 and 3825.

According to the Shadowserver Foundation on 20 September 2015 in Poland there were 9 routers with SYNful Knock implant (out of 163 globally)[51]. On 21 January 2016 Shadowserver scanner did not detect vulnerable routers in our country.

[44] The Waterbug attack group, Version 1.02, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf

[45] The Epic Turla Operation, https://securelist.com/analysis/publications/65545/the-epic-turla-operation/

[46] Dissecting Turla Rootkit Malware Using Dynamic Analysis, http://labs.lastline.com/dissecting-turla-rootkit-malware-using-dynamic-analysis

[47] Turla: APT Group Gives Their Kernel Exploit a Makeover, http://labs.lastline.com/turla-apt-group-gives-their-kernel-exploit-a-makeover

[48] The 'Penquin' Turla, https://securelist.com/blog/research/67962/the-penquin-turla-2/

[49] Uroburos: the snake rootkit, Andrzej Dereszowski, Tecamac, http://artemonsecurity.com/uroburos.pdf

[50] SYNful Knock - A Cisco router implant - Part I, https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html

[51] http://blog.shadowserver.org/2015/09/21/synful-knock/

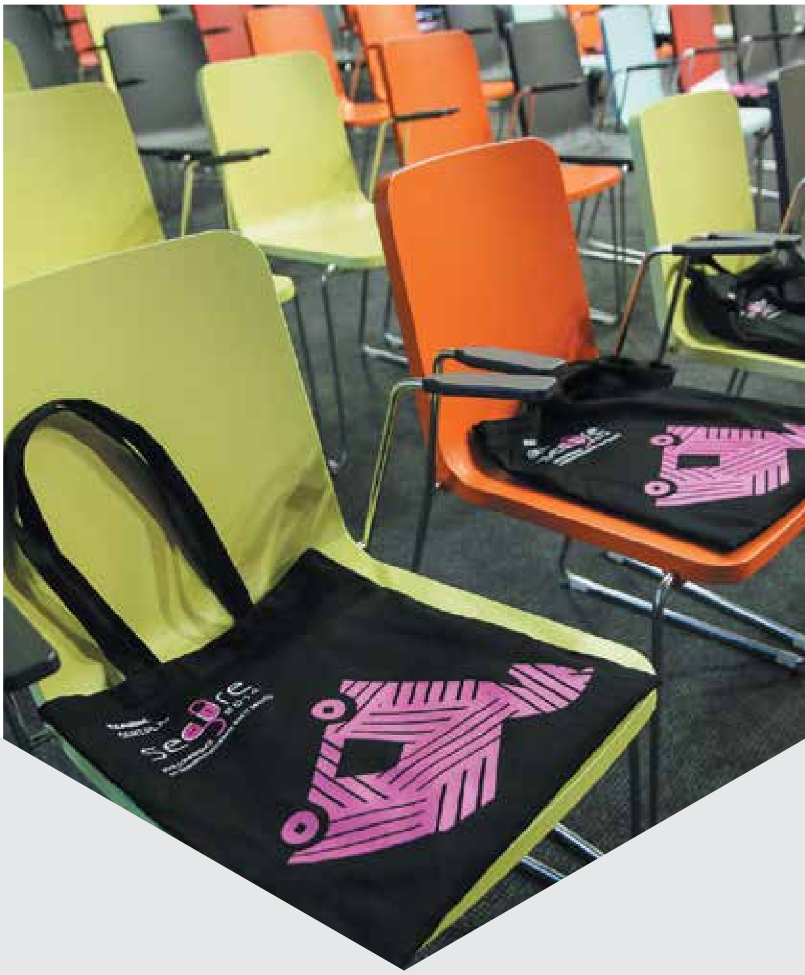
The Postal Group

On the 16th of October 2015, during the Secure conference, we presented a report outlining actions performed by a group of criminals, which we have called "The Postal Group". This name is derived from the fact that they masquerade their phishing attacks as messages from a post office. In our report we presented our own analysis as well as information shared by ZaufanaTrzeciaStrona.pl and Logical Trust.

The Postal Group has operated since 2013. CERT Polska began analysis of Postal Group malware in May 2015, after a series of phishing attacks, during which criminals impersonated the notifications sent to users by the Polish Post Office. The e-mails supposedly informed about an undelivered package – however, they also included a link which, after several redirects, lead to the download of a malicious file for Android or Windows operating systems. Polish users were not the sole target of such campaigns, as similar attacks were also seen in Australia. In that case the phishing messages used the logo of Australian Federal Police and pretended to be traffic ticket fine notifications. A British version of those e-mails also tried to impersonate a well-known and trusted brand - Royal Mail. In most cases cybercriminals used a document with a macro or a password-protected zip file with malware itself. Password was always given in the e-mail body.

The aim of the criminals was to encourage users to install malicious software: Andromeda or TorrentLocker for Windows or OpFake for Android. Criminals also earned money through the affiliate program of online casinos advertised in spam messages.

TorrentLocker installed by criminals wasn't anything new. It was a popular malware which encrypts user data (ransomware). It also has means to steal user mail account settings. The second bot, Andromeda, was used only as a dropper to distribute and install another malware - Slave. It is a simple bot targeting online banking users, employing typical techniques to modify the content of web pages in the user's browser. Slave also steals bitcoins by changing data in the system clipboard whenever an unsuspecting user copies a bitcoin wallet address.



The phishing websites were not only targeting Windows users, but, based on the User-Agent header, they were also trying to infect Android users. In this case, mobile phones would get infected with OpFake - a program combining functions of stealing information from mobile user (application data, information about phone, account status, address book) with trojan horse backdoor functions (sending/reading/editing SMS, taking control of the device, stealing banking data). The latter feature was implemented by using the technique of overlaying UI elements of banking or e-mail applications (so called application overlay). To make the login / password form believable, OpFake was enhancing the form with the logo of the appropriate bank.

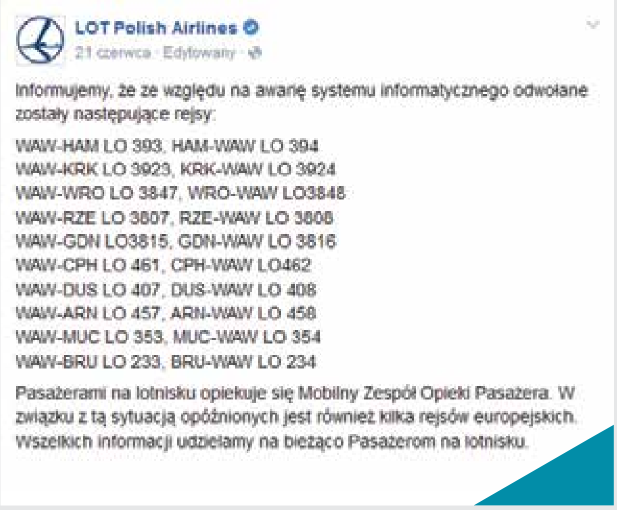
According to data shared by Logical Trust, malware distributed via the Postal Group campaign in August 2015 was downloaded by Polish users 6,388 times. More details can be found in the report published on our website.

The attack on LOT

On June 21, 2015 LOT Polish Airlines flights originating from Warsaw Frederic Chopin Airport were grounded for about 4 hours.

The first announced reason for the delay was a failure of one of the airline systems. Later, on its official Facebook profile, the airline stated that its ground systems were "affected by an IT attack". Based on information shared by LOT with the general public within the hours following the incident, it can be supposed that the airline was a victim of a DDoS attack which affected the communication with Eurocontrol. As a result, it was impossible to submit flight plans, required to enter the controlled European airspace. LOT assured, however, that systems affecting passenger security, especially those installed onboard of the aircrafts, were not affected by the incident in any way.

The incident was investigated by the Polish government CSIRT CERT.GOV.PL. At LOT's request the prosecutor's office launched an investigation. In September 2015 media revealed conclusions of an internal report prepared by independent investigators, which LOT submitted to the prosecutor's office. The report suggested that lack of communication could be a result of an reflected DNS amplification attack, using a server inside the airline's network to generate massive volume of outgoing traffic.



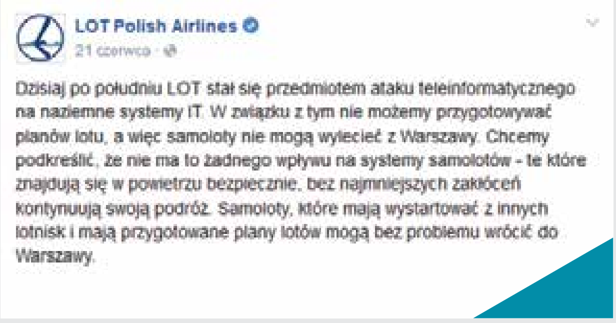
LOT Polish Airlines
21 czerwca · Edytowany

Informujemy, że ze względu na awarię systemu informatycznego odwołane zostały następujące rejsy:

WAW-HAM LO 393, HAM-WAW LO 394
WAW-KRK LO 3923, KRK-WAW LO 3924
WAW-WRO LO 3847, WRO-WAW LO3848
WAW-RZE LO 3807, RZE-WAW LO 3808
WAW-GDN LO3815, GDN-WAW LO 3816
WAW-CPH LO 461, CPH-WAW LO462
WAW-DUS LO 407, DUS-WAW LO 408
WAW-ARN LO 457, ARN-WAW LO 458
WAW-MUC LO 353, MUC-WAW LO 354
WAW-BRU LO 233, BRU-WAW LO 234

Pasażerami na lotnisku opiekuje się Mobilny Zespół Opieki Pasażera. W związku z tą sytuacją opóźnionych jest również kilka rejsów europejskich. Wszelkich informacji udzielamy na bieżąco Pasażerom na lotnisku.

Notification of flights cancelled due to attack;
PLL LOT Facebook page



LOT Polish Airlines
21 czerwca

Dzisiaj po południu LOT stał się przedmiotem ataku teleinformatycznego na naziemne systemy IT. W związku z tym nie możemy przygotowywać planów lotu, a więc samoloty nie mogą wylecieć z Warszawy. Chcemy podkreślić, że nie ma to żadnego wpływu na systemy samolotów - te które znajdują się w powietrzu bezpiecznie, bez najmniejszych zakłóceń kontynuują swoją podróż. Samoloty, które mają wystartować z innych lotnisk i mają przygotowane plany lotów mogą bez problemu wrócić do Warszawy.

Notification of an internet attack on PLL LOT network;
PLL LOT Facebook page

> "During the second half of August 2015, over forty percent of people who received phishing emails posing as Polish Post Office notifications opened it and downloaded malware to their PC-s."
>
> **TVN24 bis**

The attack on Plus Bank

In the spring of 2015, rumors appeared that an infrastructure of a Polish bank was compromised and infiltrated by the criminals. There were two sources of this information:

- the "underground" forum ToRepublic, where attackers claimed they hacked a system in a bank and published parts of stolen data as a proof, and
- a security news portal Zaufana Trzecia Strona, which was used by the attackers as a mediator in their negotiations with the bank.

More complete information was revealed after the attackers tried to blackmail the bank, demanding 200 thousand Polish zlotys (about 50 thousand euros) for silence and for refraining from publishing the stolen customer data. A ToRepublic administrator nicknamed "Polsilver" confessed he had attacked Plus Bank and published parts of stolen data. He also described the events which allegedly followed. According to his story, he had tried to get in touch with the Management Board of the bank and other individuals inside the bank since March 26. Discouraged by their lack of response he had sent notices to the Polish Financial Supervision Authority, Polish Banks Association, MasterCard, CERT and Office of Competition and Consumer Protection. As a proof of his presence in the bank's systems, Polsilver published parts of transaction history as well as account balances of Tobias Solorz - the CEO of Polkomtel which owns Plus Bank.

The attacker also claimed that he was able to steal about 1 million zlotys (about 250 thousand euros) from customers' accounts. The bank confirmed that they had a security incident, but refused to comment or reveal any details. According to the media, Polsilver was arrested in October 2015.

The attack on Polish consulates in Belarus

In January 2015 ESET discovered and researched the internal workings of a very interesting botnet. MSIL/Agent.PYO, as ESET called it, uses infected machines to register visa applications in Polish consulates in Belarus. The target of the attack is a system called e-konsulat[52], which was designed with intention to shorten waiting times and cut physical queues for visa applicants. However, after the implementation it turned out that all available timeslots are instantly reserved, and in Belarussian towns a number of companies popped up, offering registration services for a fee of 150 to 300 US dollars. For Belarussian citizens, with average wages of about 400 US dollars after devaluation of Belarussian ruble, the price was quite steep.

The situation attracted media interest. The Polish Ministry of Foreign Affairs attempted to make automatic reservation of meeting times more difficult by implementing CAPTCHA, but it did not bring the expected results. ESET's discovery of MSIL/Agent.PYO turned out to be a breakthrough in addressing the issue. The main functionality of the botnet was making automatic reservations of meetings in Polish consulates. The malware had been distributed through December 2014 by Nuclear Exploit Kit, and only installed on computers located in Belarus. Starting from December 20, 2014, bots were receiving commands from the botnet's C&C. The machines were tasked with filling up the registration forms at e-konsulat.gov.pl. Within 9 days at least 4 versions of the botnet were created, and after 5 weeks of monitoring 925 infected hosts were identified[53].

Cryptolocker and other ransomware families

In 2015, we saw a significant growth in the number of attacks using software which encrypts user data (ransomware). Nowadays, this type of attacks is not only a threat to the users of Windows systems, but also to Linux and Android users. In Poland, the most effective way to distribute this type of malicious software (in this case Cryptolocker) was an e-mail campaign pretending to be from the Polish Post Office.

In this campaign criminals sent e-mails supposedly notifying about an undelivered package – however, they also included a link which, after several redirects, led to the download of a malicious file (.exe or .apk depending on the operating system). After running a program, all files with certain extensions were encrypted. The program also displayed a message on the screen, describing actions to be taken in order to recover the encrypted data. For this campaign, the ransom was set to 1.47546 BTC. If the ransom was paid, user's data were decrypted.

Another ransomware example from the last year - LockerPIN, which operated mostly in the US, was a malicious

[52] registration service for visa applications operated by Ministry of Foreign Affairs of the Republic of Poland www.by.e-konsulat.gov.pl

[53] http://www.welivesecurity.com/2015/01/29/msilagent-pyo-have-botnet-will-travel/

software directed to users of mobile devices. This ransomware changes PIN of the user's device, effectively blocking access to it. In this case, the telephone owner wouldn't be able to regain control over the phone, even after paying the ransom.

In 2015, the most unusual ransomware sample that we encountered was the first ransomware aimed at administrators of Linux servers. With the 128-bit AES working in CBC mode, the program was encrypting all files in users' home directories, directories associated with web services, logs and backups. After performing the encryption, the program created a file with the instructions on how to get the decryption tool. Despite strong encryption algorithm used in this case, the malware creator made many mistakes at the implementation, making it possible to recover files without having to pay a ransom. This time, the campaign didn't affect Polish users but we expect that it can return in an improved form.

Currently one of the most interesting , sophisticated and rapidly disseminating malware families of ransomware is Cryptowall. The latest version made its debut in the end of 2015 using a different vector of attack compared to the earlier versions (phishing and spam). In this variation, Cryptowall is distributed through utility called Nuclear Exploit Kit (a tool attacking applications such as Adobe Flash, Java, Silverlight, redirecting the user to a malicious web page). After successful exploitation of the user's browser, the malware is downloaded and user resources are encrypted.

Many ransomware authors make mistakes, so that the data can be decrypted without paying any money. However, experienced criminals create unique keys for each user, and recovery of files without paying the ransom is not possible. It should also be noted that the present-day ransomware can encrypt not only local, but also network resources. This may occur if the process of a malicious program has write access to network drives. Therefore, when performing a backup we should remember to completely separate it from the system in use. Backup stored on a shared public network or on drives mounted to the user's system won't protect the user against ransomware attack as it will encrypt files on all reachable volumes.

Threats to mobile devices

In 2015 we have observed several different malicious programs targeting users of mobile devices based on Android. Still, the number of infections, as well as the popularity of such malware is quite low. The main threat, especially active in the second half of 2015 was GMBot – an application for Android, which uses the application overlay technique.

Application overlay is often used in malicious Android applications in order to impersonate another app. When a malicious app checks that the user opened an online banking app, it displays a window on top of that app (e.g. banking application) with a message, usually asking for credentials. The user assumes that this message comes from the banking app and provides login, password and other sensitive data, that he would never leave on a phishing website.

Due to changes to the Android API, introduced by Google from version 5.0, this kind of attack is no longer possible. This means that more than one third (at the moment of writing) of all Android users will not see the windows injected by the malicious application. At the first half of 2015, we also noticed a similar campaign, aimed at users with Windows and Android operation systems. Cybercriminals impersonated the Polish Post Office, sending e-mails supposedly informing about an undelivered package. Then, they display the notification to download an .exe or .apk file (depending on the user's operating system). In this case, apk file was malicious software known as OpFake. Like GMBot, it used application overlay technique.

Targeted attacks: phishing

Over the past few years we have seen numerous variations of messages impersonating different companies and institutions such as express mail services, telecommunication companies, bailiff's offices, internet stores etc. All of them were distributed with an intent to install malware on users' computers. The content, as well as the alleged sender, were designed to intrigue recipient and thus induce him to take some specific action, such as opening an attachment or visit a malicious website. We have thus observed a wide range of malicious software used for these purposes, including Tinba, isfb, Andromeda, BetaBot, Dyre/Dyreza, Dridex and VBKlip. The messages were distributed by different actors, often the only factor connecting them was the technique they used - sending spam to random recipients with malicious attachments or links. Unfortunately, such attacks are still present, likely because they are still sufficiently successful from the criminals' point of view, despite of many warnings and alerts issued by security companies and authorities.

Attacks on law firms

Last year we have seen more sophisticated, precisely targeted attacks on a larger scale. Particularly interesting, for a number of reasons, was a wave of attacks on law firms. The attackers impersonated a company allegedly pursuing a contract for legal services. The criminals have even set up a webpage of the fake company, and sent a request to answer several simple questions to the law firm's address. In case a response was received, further communication followed (often from a different email account), with attempts to infect the recipients with malware - either with a malicious attachment, or with a file served from a link[54]. The malware would pretend to be an update for Microsoft Office, while in reality it would enable the attackers to download and run arbitrary code without user's knowledge or consent. An example of malware used in cases we analyzed was Smoke Loader[55].

Other targeted attacks

During last year CERT Polska has received signals about other types of targeted attacks. Examples include attacks on businesses, with attackers impersonating their contractors. Quite often they are preceded by attackers gaining access to internal systems and ability to read through internal and external emails. While initial infection is by random chance, criminals make use of information they collect to build a credible scenario for a targeted attack. Once they know the profile of the company, they send fake invoices or make orders for goods on behalf of known contractors. At times, they attempt to steal sensitive information for ransom. Such attacks are performed by both Polish and foreign individuals.

Incorrect configuration of servers and services in the Polish Internet address space

We distribute information about the vulnerable services and servers in Poland using the n6 platform. Compared to previous years, when we delivered data on misconfigured servers and services such as DNS, NTP, SNMP, SSDP, NetBIOS, QOTD and Chargen, we increased the scope of information provided with new vulnerable services: SSL 3.0 (POODLE vulnerability) and TLS (FREAK vulnerability), IPMI, UNIX port mapper and the database services (Elasticsearch, MSSQL, Redis, MongoDB).

Replacing DNS settings on home routers

Incidents reported to us are often reappearances of campaigns that we observed in previous years. Usually, reused campaigns have improved their Polish spelling in messages or present more credible story concerning "premium accounts", "technical work" or "incorrect money transfers". These changes usually do not have significant impact on the attackers' tactics. Sometimes however, we observe much improved campaigns in which the changes - seemingly very subtle - have significant impact on the effectiveness of the attack. One such example is the campaign substituting the DNS settings on home routers.

Malicious DNS servers

A large scale malicious DNS servers campaign was observed in Poland by CERT Polska at the beginning of 2014. The campaign was carried out by performing a great number of hacking attempts directed on home routers and – whenever the attempts were successful - replacing their DNS settings with external DNS servers controlled by the attackers. These actions allowed criminals to take control over the webpages displayed by browsers inside victims' networks, and more specifically allowed redirecting

[54] https://zaufanatrzeciastrona.pl/post/uwaga-na-nowy-atak-na-kancelarie-prawnicze-wezwanie-do-zaplaty/

[55] http://www.cert.pl/news/10484

the users to fake websites. In this case, a user whose network infrastructure was attacked, was directed by criminals to a fake shopping website or fake internet banking service. This allowed criminals to obtain access to user credentials or perform Man in The Middle attack on the connection of the customer and the bank - the customer, in fact, connected only to the proxy server set up by criminals, while the actual connection to the bank happened from other machines belonging to them.

The campaign was relatively quickly detected, mainly due to the fact that criminals connected to the banking systems from a single IP address (two addresses in the later stage of the campaign). This enabled financial institutions to detect the anomaly of establishing a large number of user sessions from a single IP address.

In 2015 this scenario has undergone a significant update. In the new version of the campaign criminals began to tunnel connections to internet banking services through other compromised routers, the list of which was changed every few sessions. This procedure significantly delayed the detection of anomalies.

This kind of attack introduces another threat – the possibility of ISP's router takeover. Local ISPs often do not put proper emphasis on security, leaving the default password set on routers, or use the same password for all devices on their network. In such cases it is sufficient to takeover a single vulnerable device allowing to read the password, which in return gives possibility to access all other home user routers and main network ones. By performing such actions criminals are able to take control over the Internet traffic of all customers of a given ISP.

Vulnerabilities in consumer routers were also quickly used as an extremely cheap and fast way to anonymize connections. Majority of home routers used by the end users are based on Linux. In many cases, only basic functions of such devices are used, such as routing, port forwarding, and sometimes prioritizing connections. Most of users are not aware of the fact that the device, which is plugged all the time to their network, can be subverted by a third party or malicious software.

Very often, while we investigate a security incident, we deal with cases of port scanning or intrusion attempts to IT systems. In 2015 we began to receive large number of reports in which compromised home routers played a key role. They were used to set up a tunnel, thus allowing criminals to carry out attacks using the IP address of the router. In some cases, they were also used as proxy servers for malware. An example of such malware is Dyre, which through the use of compromised routers to set up its communication network makes it difficult to find the C&C server.

An important advantage of using home routers to tunnel connections is the fact that in most cases, due to the characteristics of the devices (usually a small amount of available disk space or lack thereof), all information about connections is stored only in memory. Hence, when the device is disconnected from the power supply (in order to secure evidence in the proceedings) all connection information is lost, including the information about the tunnels.

At the time of obtaining access to the router, criminals, in order to secure continued access to the device, made changes to device settings, including administrative passwords. Next, they updated the software in order to patch the vulnerability. This made them sure that the device that has been taken over, will not fall prey to other attackers. Another type of attacks on routers were cases of replacing firmware. It is a technique similar to that used by the attackers implanting SYNFul Knock, described in the section about APT.

SSL Vulnerabilities: FREAK and POODLE

The SSL POODLE vulnerability was discovered in 2014 and is currently the most common vulnerability reported to the n6 platform. Interestingly, the number of vulnerable servers is still growing. In 2015 the number of vulnerable web servers grew more than twofold and reached the level of approximately 420 thousand. The probable cause of this continuous growth are servers with default configuration, allowing for the use of SSLv3.

The SSL FREAK was observed in significantly lesser numbers (slightly more than 5,000 notifications of unique IP addresses a day) and the number of vulnerable servers remained stable during the year.

Both these vulnerabilities, in contrast to other misconfigured services described in this chapter, are vulnerabilities that cannot be used to reflected and amplify DDoS attacks.

DDoS attacks

Some misconfigured services (e.g. DNS, NTP, SNMP, SSDP) can be used to conduct reflected DDoS attacks. The reflected attacks use the technique of sending an IP packet with a spoofed source address. After reaching the target server, the response is sent to the spoofed address rather than

to the actual sender of the packet. A limitation of attacks leveraging spoofed source addresses is the inability to establish a full TCP session, but this does not apply to connectionless UDP.

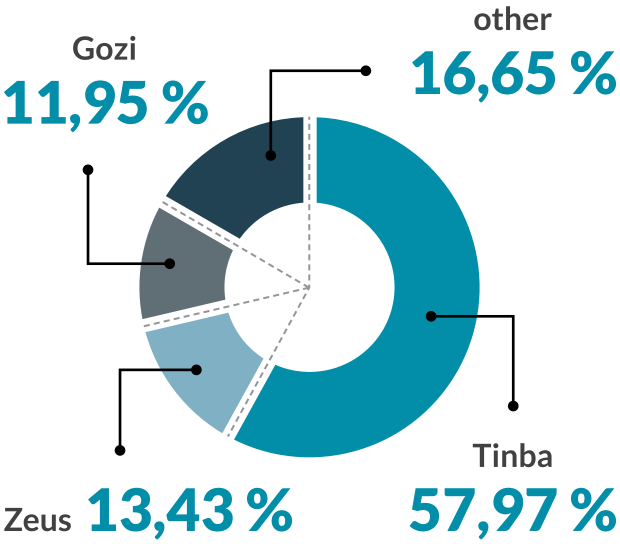
An amplified reflected attack takes advantage of the fact that some network services generate significantly greater response when compared to the query. For example, sending approximately 20 bytes to a vulnerable DNS server may cause the server to send a response up to 20 times larger.

Data exfiltration

Running database services on publicly accessible servers, in particular without enabled user authentication or with default user credentials poses a serious risk of unauthorized access and data exfiltration. Incorrect configuration of databases or other services is often a result of using by the administrator the default, commonly known configuration.

Biggest banking trojans in Poland

Most banking trojans use webinject technology to modify e-banking pages and give criminals full access to a victim's bank account with opportunity to transfer money.



Statistics

Statistics presented in this section are based on data collected by the n6 platform. Information about threats come from many sources, including CERT Polska operations, automated monitoring systems (sinkhole, ARAKIS), but also from external organizations - non-profits, independent researchers, national CERTs and commercial entities. Among 200 million incident reports for the Polish address space, which were automatically processed in 2015, 98% came from external sources.

It is worth noting how diverse are the methods of obtaining information about incidents. Below are some of the most common ones:

- Data on infected computers (bots) is obtained primarily through takeover of botnet infrastructure (C&C servers' domains) and redirecting the traffic to a sinkhole.
- Detection of attacks on computers that provide services on the Internet (e.g. SSH, WWW) is performed by using special trap systems that are disguised as real servers (honeypots).
- In a similar way - using client honeypot systems, pretending to be web browsers - malicious web pages that infect users visiting them can be detected.
- Detection of vulnerable services (e.g. misconfigured NTP servers that can be used to perform DDoS attacks) is done by scanning the IPv4 address space on a large scale. This method has long been used by criminals, while in 2015 there was a significant increase in the number of scans carried out by entities acting towards improvement of the level of security of the Internet.

"Of 200 millions automatically processed reports of incidents concerning Polish address space that we received, 98 percent came from external sources."

Limitations

We have made every effort to make the large scale incidents statistics represent the threat landscape as close as possible. Please note that these statistics have some limitations, mainly resulting from the nature of the available data sources. First of all, it is not possible to gather all possible information about all types of threats, the best example being targeted attacks at specific entities or groups of users (as opposed to mass attacks), which usually will not be recorded by our monitoring systems, and will not be reported to our team.

The problem with getting the actual representation of the threat landscape is also due to the fact that any given threat may be active for a long time before it is discovered and its regular observation starts. For example - the number of infected computers in a given botnet can be difficult to determine before the takeover of the infrastructure (botnet's C&C servers).

An important issue is defining the scale of the threat, which is usually determined by counting IP addresses associated with it and observed during a single day. We make the assumption that the number of IP addresses is close to the number of devices and users affected. Of course, this is an imperfect measure because of the widespread use of two mechanisms, which affect the number of observed public IP addresses:

- NAT (Network Address Translation), resulting in an underestimation, because one external IP address is often used by a lot of computers.
- DHCP (dynamic addressing), causing an overestimation, because, for example, the same infected computer may be detected several times during the same day.

We suspect that the impact of both of these mechanisms on the aggregated results cancels itself in the large part, but careful examination of the effects of NAT and DHCP in this context would require a separate analysis to be carried out.

The last remark concerns the version of Internet Protocol: all of the statistics relate to the fourth version of this protocol. This is due to a small level of deployment of IPv6 in Polish networks, and associated with it, a small number of incident reports we receive for this type addresses.

Botnets

Botnets in Poland

The following tables present data on the size of botnets in Poland. Data on botnets in Polish networks come from the n6 project. From the available data we can conclude that in 2015 there were almost 150,000 infected computers in Poland. We estimate that the actual number is probably higher by a small percentage.

tinba	22899	15.52%
Conficker	17007	11.53%
foreign	13155	8.92%
Sality	10804	7.32%
bamital	6045	4.10%
Zeus	5305	3.60%
Gozi	4720	3.20%
zeroaccess	4092	2.77%
Kelihos	3776	2.56%
Virut	3132	2.12%
Total:	**147533**	

Table 4. The largest botnets in Poland

In the above table we present the largest observed botnets in Poland. The size of the botnet was calculated as the maximum daily number of infected PCs during the year. The biggest botnet in Poland last year was Tinba, a very dangerous banking trojan. Tinba increased its activity significantly in the middle of the year, with the highest infection level kept only for a few days during the year. The average number of computers infected with Tinba was around 4,300 a day. It should be noted that Tinba is a type of malware managed by different, usually unrelated people. Its popularity is not surprising, because the source code of the bot leaked in mid-2014 and since then we observe a growing number of its instances, both operated by "professional" and "amateur" criminals, the latter just beginning their work with the malware.

The second place was taken by the Conficker, a giant botnet, which was first sinkholed in 2009 and since that time we observe a slow decline in the number of reported infections. However, the percentage of total infection rates remained at a similar level compared to the previous year.

ZeroAccess, which two years ago was the third on the list and last year the second, in this year's ranking was only the ninth.

Again, it should be emphasized that three out ten largest botnets in Poland are related to banking trojans.

In conclusion, it is worth noticing that there is a gradual decline in numbers of most of the old botnets (Conficker, Zeroaccess, GameOver, and another in the Zeus family).

Banking trojans

tinba	22899	57.97%
Zeus	5305	13.43%
Gozi	4720	11.95%
Dyre	2526	6.39%
rovnix	1889	4.78%
Other		5.48%

Table 5. Data on banking trojans

Table 5 gives data on botnets, which are a threat to customers of internet banking. Most banking trojans modify the bank's web page displayed on the infected computer, which allows criminals to steal the credentials and to have full access to the victim's account and allows them to transfer funds out of the accounts. In 2014 and in 2015 we observed a progressive use of newer malware, not previously found in Poland, performing attacks on users of internet banking. An example of this trend is the Dyre/Dyreza, which caused problems for users of western banks, but wasn't really used in attacks against Polish users. In early 2015 this situation, unfortunately, changed.

Botnet activity

According to our observations the activity of old, long sinkholed botnets is steadily declining. Primarily this is due to the lack of new infections and the withdrawal of the old, infected machines. For newer threats the situation is slightly different. For example, the Gozi trojan that infected several hundred computers during the year, dramatically increased its activity in November, and in result took seventh place in our ranking in Table 4. A similar observation, albeit without such large difference in the daily number of infected machines, can be made in case of the infamous winner of our ranking - Tinba. In the record day we received more than 5 times the number of reports about computers infected with Tinba than on average throughout the year.

Statistics on botnets by telecom operators

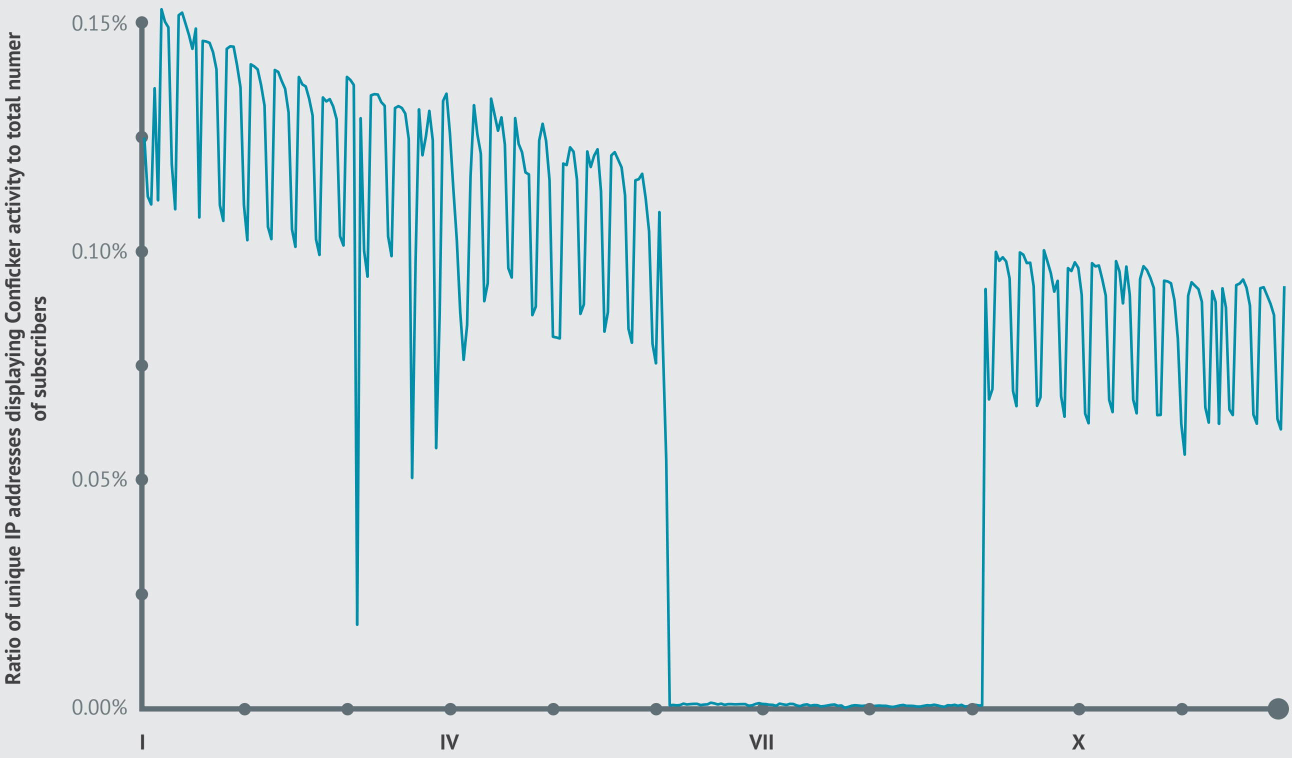
Data related to the activity of botnets in 2015 were also analyzed for infection rates of the largest Polish telecom operators' networks.

One of the most interesting facts observed by us, was the decline of the number of bots in the Aero2 network (AS15855). Until mid-March every day we received reports of more than 900 infected machines calling from the Aero2 network, and after March 16 there was a sharp decrease to an average of only 3 reports a day. We believe that this situation is a consequence of changes in the infrastructure of Aero2 network and using another autonomous system for users' outbound traffic.

Another interesting phenomenon we noticed was variation in the number of infections with different trojan families among ISPs. For example Internetia (AS43939) and Multimedia Polska (AS21021) had lower levels of infection with Slenfbot compared to other operators. In addition, in the Internetia's network there was a much lower number of Cutwail reports. And Tinba, a dangerous banking trojan was largely infecting users of mobile operators (P4 Plus, T-Mobile), especially in the fourth quarter.

Another interesting observation was the decline in the activity of the Conficker worm to virtually zero in the period from early May to late August in the Orange Polska network (AS5617). The activity level or the number of infected machines is often determined by the number of connections to sinkholes. We suspect that the decline in activity of the Conficker worm in the Orange Polska network was associated with the launch of the CyberTarcza (CyberShield) service, which Orange Polska announced in mid-April. CyberTarcza could block connections to the C&C servers of Conficker, including sinkholes from which we get the statistics. Graph showing Conficker activity in Orange Polska network is presented in Figure 2.

Figure 2. **Chart of activity of the Conficker worm in Orange Polska network**



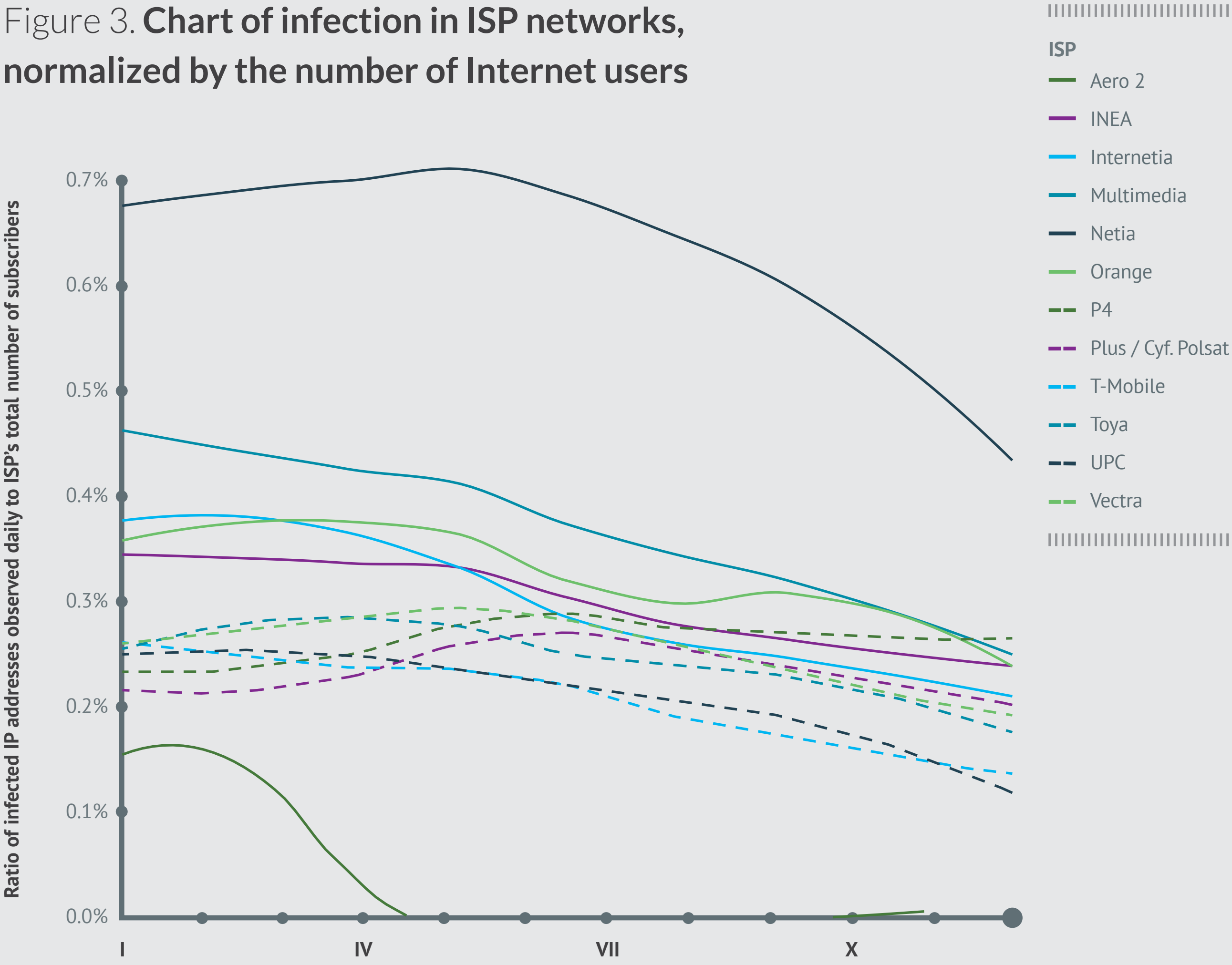
In Figure 3 we present a chart of infection rates by ISPs, normalized by the number of Internet users (based on the report of the Office of Electronic Communications [UKE] for 2014). Our most important observations are:

- In nearly every provider's network, the number of infections decreased during the year
- Netia's level of infections is twice higher comparing to other ISPs
- Multimedia Polska is second in the terms of the level of infection, and the third is Orange Polska.

"Number of cyberattacks affecting Poland is scary. A number of people equivalent to population of Katowice is attacked every day."

Spider's Web

Figure 3. **Chart of infection in ISP networks, normalized by the number of Internet users**



C&C servers

In 2015 we have received information about 4,612 unique IP addresses, and 6,227 unique Fully Qualified Domain Names (FQDN) used as C&C servers for managing and controlling the botnets.

Due to the nature of the threat we decided to describe it with regard to the location of an IP address, or top-level domain name (TLD). In the statistics we have omitted data from sinkhole servers of CERT Poland.

IP addresses

We received incident reports concerning IP addresses from 80 countries. As in previous years, most of the malicious servers were located in the United States (almost 26%). 75% of all C&C servers are hosted in 10 countries presented in Table 6.

Rank	Country	Number of IP addresses	Percentage
1.	United States	1,182	25.6%
2.	Germany	500	10.8%
3	Uruguay	423	9.2%
4	Greece	310	6.7%
5	United Kingdom	215	4.7%
6	France	210	4.6%
7	Netherlands	176	3.8%
8	Russia	166	3.6%
9	Italy	138	3.0%
10	Indonesia	136	2.9%
...	...	...	...
17	Poland	43	0.9%

Table 6. Countries with biggest number of botnet C&C servers known to CERT Polska

We observed 790 different autonomous systems hosting the C&C servers. More than 40% of all malicious servers were located within 10 ASes.

Rank	AS number	AS name	Number of IP addresses	Percentage
1	6057	Administracion Nacional de Telecomunicaciones	428	9.3%
2	6799	Ote SA (Hellenic Telecommunications Organisation)	309	6.7%
3	3320	Deutsche Telekom AG	293	6.4%
4	16276	OVH Systems	264	5.7%
5	1267	Wind Telecomunicaztioni SpA	129	2.8%
6	17974	PT Telekomunikasi Indonesia	126	2.7%
7	26496	GoDaddy.com, LLC	119	2.6%
8	47583	Hostinger International Limited	110	2.4%
9	18403	The Corporation for Financing & Promoting Technology	100	2.2%
10	9299	Philippine Long Distance Telephone Company	85	1.8%

Table 7. Autonomous systems which hosted the most of C&C servers

In Poland, the C&C servers were located on 43 different IP addresses (17th place in the world with a share of 0.9%) belonging to 20 autonomous systems. In the table we present the list of 10 Polish autonomous systems which hosted most of C&C servers (almost 80% of all malicious servers in Poland).

Rank	AS number	AS name	Number of IP addresses	Percentage
1	31621	Grupa Allegro Sp. z o.o.	6	14.0%
2	13119	Zachodniopomorski Uniwersytet Technologiczny w Szczecinie	4	11.6%
2	42656	Grupa Allegro Sp. z o.o.	4	9.3%
2	49792	IONIC Sp. z o.o. Sp. k.	4	9.3%
5	59491	Livenet Sp. z o.o.	3	7.0%
5	197226	“SPRINT” S.A.	3	7.0%
5	16276	OVH SAS	3	7.0%
5	51290	HOSTEAM S.C. Tomasz Groszewski Bartosz Waszak Łukasz Groszewski	3	7.0%
9	9112	Institute of Bioorganic Chemistry Polish Academy of Science, Poznan Supercomputing and Networking Center	2	4.7%
9	43939	Internetia Sp. z o.o.	2	4.7%

Table 8. Autonomous systems which hosted the most of C&C servers in Poland

Domain names

We have also received reports of 6227 fully qualified domain names (FQDN), which were assigned to servers managing botnets. They were registered within 139 top-level domains, with over 30% in the .info TLD.

Rank	TLD	Number of domains	Percentage
1	.info	1,983	31.8%
2	.com	1,257	20.2%
3	.net	786	12.6%
4	.org	464	7.5%
5	.de	316	5.1%
6	.ru	139	2.2%
7	.biz	126	2.0%
8	.in	103	1.7%
9	.su	99	1.6%
10	.eu	68	1.1%

Table 9. Top-level domains in which the servers C&C servers were registered

Phishing

In this section we present only statistics on phishing in the traditional sense of the word, meaning spoofing (mainly via e-mail and web pages) of well-known brands with the aim to obtain sensitive data. Thus we do not refer either to phishing with malware or to, for example, impersonating supplier invoices in order to distribute malware. Statistics refer to pages hosted in Poland, therefore do not include phishing of Polish institutions with websites hosted abroad.

In 2015 we handled 881,504 phishing reports concerning Polish networks with regard to about 29,762 URLs in 4,535 domains located at 1,822 IP addresses. This is a slight decrease compared to the previous year (bigger number of unique URLs is due to the generation of many pseudo-random subdomains or subdirectories on compromised servers, which makes it difficult to report phishing sites to anti-phishing services).

The vast majority of phishing sites was hosted as a result of hacking a legal web site (as opposed to those for which a dedicated domain and / or hosting was obtained). About 6% of all phishing attacks was related to compromised web sites based on WordPress.

No.	AS number	AS name	IP addresses	URL-s
1	12824	home.pl sp. z o.o.	543	5,653
2	15967	nazwa.pl S.A.	284	3,002
3	198414	BiznesHost.pl	80	1,318
4	29522	Krakowskie Centrum Informatyczne JUMP	62	207
5	16276	OVH	53	555
6	43333	CIS NEPHAX	53	392
7	15694	ATM S.A.	38	270
8	59491	Livenet sp. z o.o.	33	162
9	8308	NASK	32	132
10	41406	ATM S.A.	32	5

Table 10. Polish Autonomous Systems with the biggest numbers of phishing pages

A minor reshuffle of the list took place as compared to the previous year. The first two positions remain unchanged, and as one would expect, are represented mainly by the largest hosting centers.

Among the targets of phishing hosted in Poland the leader for years has been Paypal. In 2015, however, its lead over other brands significantly decreased. In comparison with 2014, the share of phishing directed at banking sites significantly increased - the second place was taken by phishing targeting the Wells Fargo bank (in 2014 it ranked 15th with 9 reported cases), and the third - Bank of America (in 2014 it was outside the top fifteen in the ranking). In total, we recorded 682 cases of phishing attacks on banks - over three times more than a year ago (185). Google and Amazon returned to the top fifteen ranking, with Steam disappearing. The new one in the ranking is Netflix, for which we registered 35 phishing cases in Polish networks. This is not directly related to the service start on the Polish market, as phishing attacks were not dedicated to Polish users. But perhaps due to the significant increase of coverage in the world, obtaining the login data from users via phishing has become more profitable. Among other noteworthy new services are Dropbox and Alibaba - also growing in popularity. In addition to Alibaba also other e-commerce platforms were targets of phishing, but on a smaller scale. We noted 4 cases of phishing for Allegro and 15 cases concerning the Swiss site Ricardo.

Phishing target	Number of phishing pages
Paypal	286
Wells Fargo	147
Bank of America	132
Google	116
Apple	115
Yahoo	113
Dropbox	77
Alibaba	50
AOL	35
Netflix	35
Chase	34
Amazon	23
Westpac	22
American Express	21
Bradesco	20
NatWest Bank	20
Other banks	233

Table 11. Most popular phishing targets ranked by number of phishing pages

DDoS attacks

In 2015 we received reports of about 2,484 incidents concerning DoS / DDoS attacks coming from the Polish networks. These incidents were initiated from 1,161 unique IP addresses. The targets of the attacks were 419 unique IP addresses, with 363 belonging to Polish networks.

In comparison, year 2014 brought 64 incidents concerning 22 unique IP addresses belonging to the Polish address space, which represents only a small percentage of DoS / DDoS attacks in 2015.

Table 12 shows the 10 Polish autonomous systems from which usually DoS / DDoS attacks originated.

No.	AS number	AS name	Number of incidents
1	5617	Orange Poland SA	428
2	16276	OVH SAS	186
3	13119	Zachodniopomorski Uniwersytet Technologiczny w Szczecinie	148
4	12741	Netia S.A.	132
5	6830	Liberty Global Operations B.V.	104
6	59491	Livenet Sp. z o.o.	99
7	50188	KOLNET s.c.	85
8	29314	VECTRA S.A.	69
9	12912	T-Mobile Polska S.A.	46
10	56945	NEANET	41

Table 12. Autonomous systems in Poland as sources of DoS / DDoS attacks

Table 13 shows the 10 Polish autonomous systems with most IP addresses acting as DoS / DDoS attacks initiators.

No.	AS number	AS name	The number of IP addresses
1	5617	Orange Polska S.A.	265
2	16276	OVH SAS	82
3	6830	Liberty Global Operations B.V.	79
4	12741	Netia S.A.	70
5	29314	VECTRA S.A.	48
6	21021	Multimedia Polska S.A.	30
7	8374	Polkomtel sp. z o.o.	30
8	59491	Livenet Sp. z o.o.	29
9	12912	T-Mobile Polska S.A.	29
10	16342	Toya sp. z o.o.	19

Table 13. Autonomous systems in Poland with the most IP addresses initiating DoS / DDoS attacks

Table 14 shows 10 Polish autonomous systems with the biggest number of targets of DoS / DDoS attacks.

No.	AS number	AS name	The number of IP addresses
1	5617	Orange Polska S.A.	93
2	6830	Liberty Global Operations B.V.	72
3	21021	Multimedia Polska S.A.	38
4	12741	Netia S.A.	20
5	198073	Telewizja Kablowa "Słupsk" Sp. z o.o.	11
6	51290	HOSTEAM S.C. Tomasz Groszewski Bartosz Waszak Łukasz Groszewski	10
7	8374	Polkomtel Sp. z o.o.	6
8	29314	VECTRA S.A.	6
9	15694	ATM S.A.	4
10	59491	Livenet Sp. z o.o.	4

Table 14. Autonomous systems in Poland with the biggest number of targets of DoS/DDoS attacks

Misconfigured services

In 2015 we received reports of 3.07 million unique Polish IP addresses which were hosting incorrectly configured servers and services. For each protocol we chose 10 autonomous systems in which, during the year, we observed the biggest number of unique IP addresses associated with the vulnerable misconfigured services. The tables present a summary of the number of unique IP addresses with misconfigured services seen during the year in relation to the number of IP addresses in the autonomous system, and the share of the number of unique IP addresses in the autonomous system in the global sum of all received misconfiguration reports.

”

> “In the second week of march 2015 CERT Polska warned about a new campaign of attacks on home routers. […] Taking over a router allows the criminals to invade the victim’s privacy by seeing what pages are visited. It also allows to change the home network’s DNS servers settings, and to install malware on the attacked devices.”
>
> **Dziennik Internautów**

Chargen

We received 166,514 reports for 23,578 unique IP addresses. Daily average: 833 unique IP addresses.

No.	The number of unique IP addresses	AS number	AS name	Share in the network	Total share
1	17,612	5617	Orange Polska Spółka Akcyjna	0.32%	74.70%
2	2,517	8374	Polkomtel Sp. z o.o.	0.19%	10.68%
3	1,239	12741	Netia SA	0.08%	5.25%
4	1,134	12912	T-MOBILE POLSKA SPÓŁKA AKCYJNA	0.17%	4.81%
5	367	29314	VECTRA S.A.	0.07%	1.56%
6	33	30838	Jerzy Krempa “Telpol” PPMUE	0.11%	0.14%
7	28	39375	Telekomunikacja Podlasie Sp. z o.o.	0.10%	0.12%
8	25	13110	INEA S.A.	0.02%	0.11%
9	23	43939	Internetia Sp. z o.o.	0.01%	0.10%
10	22	34937	Stowarzyszenie Oławska Telewizja Kablowa	0.33%	0.09%

Table 15. Number of misconfigured chargen services

DNS

We received 14 985 555 reports of 1 529 738 unique IP addresses. The daily average was 58 114 unique IP addresses.

No.	The number of unique IP addresses	AS number	AS name	Share in the network	Total share
1	1,262,542	5617	Orange Polska Spółka Akcyjna	22.90%	82.53%
2	131,864	12741	Netia SA	9.00%	8.62%
3	27,990	21021	Multimedia Polska S.A.	4.72%	1.83%
4	15,973	12912	T-MOBILE POLSKA SPÓŁKA AKCYJNA	2.35%	1.04%
5	8,126	6714	T-Mobile Polska S.A.	2.30%	0.53%
6	7,530	29314	VECTRA S.A.	1.43%	0.49%
7	5,390	6830	Liberty Global Operations B.V.	0.31%	0.35%
8	4,233	20960	TK Telekom sp. z o.o.	1.70%	0.28%
9	2,996	31304	Espol Sp. z o.o.	13.93%	0.20%
10	2,994	35007	Miconet Sp. z o.o.	53.16%	0.20%

Table 16. Number of misconfigured DNS servers

NetBIOS

We received 4,339,076 reports of 169,339 unique IP addresses. The daily average was 17,471 unique IP addresses.

No.	The number of unique IP addresses	AS number	AS name	Share in the network	Total share
1	55,719	12741	Netia SA	3.80%	32.90%
2	35,719	5617	Orange Polska Spółka Akcyjna	0.65%	21.09%
3	23,260	21021	Multimedia Polska S.A.	3.92%	13.74%
4	4,174	12912	T-MOBILE POLSKA SPÓŁKA AKCYJNA	0.61%	2.46%
5	3,362	49185	PROTONET Adrian Ludyga	14.43%	1.99%
6	2,942	8374	Polkomtel Sp. z o.o.	0.22%	1.74%
7	2,771	13110	INEA S.A.	1.70%	1.64%
8	2,453	5550	Technical University of Gdansk, Academic Computer Center TASK	3.74%	1.45%
9	2,319	8970	WROCMAN-EDU educational part of WASK network	3.54%	1.37%
10	2,253	198414	Biznes-Host.pl sp. z o.o.	18.73%	1.33%

Table 17. Number of misconfigured NetBIOS servers

NTP

We received 9,246,970 reports of 477,647 unique IP addresses. The daily average was 37,153 unique IP addresses.

No.	The number of unique IP addresses	AS number	AS name	Share in the network	Total share
1	396,442	5617	Orange Polska Spółka Akcyjna	7.19%	83.00%
2	32,200	12741	Netia SA	2.20%	6.74%
3	7,227	6714	T-Mobile Polska S.A.	2.04%	1.51%
4	4,026	12912	T-MOBILE POLSKA SPÓŁKA AKCYJNA	0.59%	0.84%
5	2,676	21021	Multimedia Polska S.A.	0.45%	0.56%
6	2,221	8374	Polkomtel Sp. z o.o.	0.17%	0.46%
7	1,972	13110	INEA S.A.	1.21%	0.41%
8	1,951	20804	Exatel S.A.	1.06%	0.41%
9	1,441	15997	Intelligent Technologies S.A.	4.40%	0.30%
10	1,151	20960	TK Telekom sp. z o.o.	0.46%	0.24%

Table 18. Number of misconfigured NTP servers

QOTD

We received 140,878 reports for 28,106 unique IP addresses. The daily average was 545 unique IP addresses.

No.	The number of unique IP addresses	AS number	AS name	Share in the network	Total share
1	21,000	5617	Orange Polska Spółka Akcyjna	0,38%	74,72%
2	2,575	8374	Polkomtel Sp. z o.o.	0,19%	9,16%
3	1,730	12741	Netia SA	0,12%	6,16%
4	1,148	12912	T-MOBILE POLSKA SPÓŁKA AKCYJNA	0,17%	4,08%
5	513	29314	VECTRA S.A.	0,10%	1,83%
6.	289	6830	Liberty Global Operations B.V.	0,02%	103%
7	94	56575	TepsaNet Stanisław Nowacki	4,59%	0,33%
8	66	41809	Enterpol K. Król P. Latosiewicz B. Wojciechowski	0,54%	0,23%
9	41	39375	Telekomunikacja Podlasie Sp. z o.o.	0,15%	0,15%
10	31	30923	Młodzieżowa Spółdzielnia Mieszkaniowa	0,25%	0,11%

Table 19. Number of misconfigured QOTD services

SNMP

We received 12 110 828 reports for the 2 130 085 unique IP addresses. The daily average was 46 028 unique IP addresses.

No.	The number of unique IP addresses	AS number	AS name	Share in the network	Total share
1	1,662,970	5617	Orange Polska Spółka Akcyjna	30.17%	78.07%
2	392,914	12741	Netia SA	26.83%	18.45%
3	26,825	12912	T-MOBILE POLSKA SPÓŁKA AKCYJNA	3.95%	1.26%
4	15,999	6714	T-Mobile Polska S.A.	4.52%	0.75%
5	2,453	20960	TK Telekom sp. z o.o.	0.99%	0.12%
6	2,271	29007	Petrotel Sp. z o.o.	13.86%	0.11%
7	1,625	6830	Liberty Global Operations B.V.	0.09%	0.08%
8	1,596	21021	Multimedia Polska S.A.	0.27%	0.07%
9	1,591	35007	Miconet Sp. z o.o.	28.25%	0.07%
10	1,469	29314	VECTRA S.A.	0.28%	0.07%

Table 20. Number of misconfigured SNMP services

SSDP

We received 14,692,104 reports for 2,058,941 unique IP addresses. The daily average was 57,990 unique IP addresses.

No.	The number of unique IP addresses	AS number	AS name	Share in the network	Total share
1	1,501,965	5617	Orange Polska Spółka Akcyjna	27.25%	72.95%
2	274,860	12741	Netia SA	18.77%	13.35%
3	118,119	21021	Multimedia Polska S.A.	19.91%	5.74%
4	40,538	29314	VECTRA S.A.	7.70%	1.97%
5	24,705	12912	T-MOBILE POLSKA SPÓŁKA AKCYJNA	3.63%	1.20%
6	11,210	6714	T-Mobile Polska S.A.	3.17%	0.54%
7	8,328	38987	Spółdzielnia Telekomunikacyjna OST	73.93%	0.40%
8	5,641	29007	Petrotel Sp. z o.o.	34.43%	0.27%
9	4,711	31304	Espol Sp. z o.o.	21.91%	0.23%
10	3,429	35007	Miconet Sp. z o.o.	60.88%	0.17%

Table 21. Number of misconfigured SSDP servers

Malicious website

We received reports on 20,769,308 unique malicious URLs and the URLs' domain names resolved to 777,294 IP addresses. Of this numbers, 579,948 unique URLs were associated with 15,045 IP addresses registered in the .pl domain.

The table 22 presents full domain names which, according to our data, host the biggest number of malicious URLs in the .pl domain.

No.	The number of unique IP addresses	Domain name
1	12,484	radson_master.fm.interiowo.pl
2	7,465	forumrowerowe.pl
3	6,716	prywatne-znajomosci.cba.pl
4	5,853	mattfoll.eu.interiowo.pl
5	5,418	bialy-dom.pl
6	4,954	taniewycieczkisharm.pl
7	3,869	static.sd.softonic.pl
8	3,825	rybnik1.pl
9	3,772	polityczni.pl
10	3,652	liniamedia.com.pl

Table 22. Full domain names hosting the biggest number of unique malicious URLs

No.	The number of unique URLs	IP address	ASN	AS name
1	71,176	37.59.49.187	16276	OVH SAS
2	64,507	176.31.124.7	16276	OVH SAS
3	24,245	217.74.65.161	16138	INTERIA.PL sp. z o.o.
4	15,770	95.211.144.65	60781	LeaseWeb Netherlands B.V.
5	12,678	193.203.99.113	47303	Redefine Sp z o.o.
6	11,811	193.203.99.114	47303	Redefine Sp z o.o.
7	11,414	188.116.19.98	43333	NEPHAX Spółka jawna Arkadiusz Kawalec Michał Podsiadły
8	10,076	85.17.73.180	60781	LeaseWeb Netherlands B.V.
9	8,927	217.74.66.167	16138	INTERIA.PL
10	8,568	94.23.95.141	16276	OVH SAS

Table 23. IP addresses which host the biggest number of malicious URLs in .pl domain

Table 23 presents IP addresses which were related to the biggest number of malicious URLs. Compared to 2014, there were changes in the top ranking of AS that the addressed belong to, that is Interia lost to OVH. Table 24 presents autonomous systems with the biggest number of malicious URLs. In this ranking Interia gave way to OVH too (compared with 2014). The Top 10 ASes in 2015 were: nazwa.pl (AS15967), NEPHAX (AS43333), E24 (AS31229) and Biznes-Host.pl (AS198414), replacing autonomous systems: Netia (AS15967 and AS12741), Hetzner (AS24940) and Grupa Onet.pl (AS12990).

No.	The number of unique URLs	ASN	AS name
1	160,944	16276	OVH SAS
2	87,595	12824	home.pl S.A.
3	39,801	16138	INTERIA.PL sp. z o.o.
4	37,801	15967	nazwa.pl
5	37,032	47303	Redefine Sp z o.o.
6	27,603	16265	LeaseWeb Network B.V.
7	24,072	43333	NEPHAX Spółka jawna Arkadiusz Kawalec Michał Podsiadły
8	19,955	31229	E24 sp. z o.o.
9	11,780	198414	Biznes-Host.pl sp. z o.o.
10	10,967	29522	Krakowskie e-Centrum Informatyczne JUMP Dziedzic, Pasek, Przybyla s. j.

Table 24. Autonomous systems with the biggest number of malicious URLs in .pl domain

No.	The number of unique URLs	Country
1	375,344	Poland
2	143,955	France
3	28,385	The Netherlands
4	13,896	United States
5	10,496	Germany
6	3,998	Spain
7	1,471	United Kingdom
8	360	Czech Republic
9	282	Russia
10	206	Canada

Table 25. Countries which hosted the biggest number of malicious URLs in .pl domain

Table 25 lists the countries hosting the biggest number of malicious URLs in the .pl domain. Poland at the first place in this ranking should not be a surprise. This was followed by countries which house the largest hosting companies in the world. Somewhat surprising is more than 7-fold increase in the number of malicious URLs in France.

In 2015 CERT Polska...

... received information on 2484 DOS/DDOS incidents coming from Polish networks.

... received reports on over 3.070.000 misconfigured internet services in Polish networks.

... handled 881.504 reports of phishing sites hosted in Polish networks. 29.762 phishing URL-s belonged to 4.535 domains and were hosted on 1.822 IP addresses.

... received notofications of 20.769.308 malicious URL-s.

Scanning

The scanning category describes cases of detected unauthorized connection attempts. These can be indicators of a misconfiguration, an infection of the computer which has initiated the connection or that the computer has been taken over by criminals, or it was an action initiated by the user. Statistics of incident reports presented in the tables below were received automatically. The statistics include data received from our partners and from our own monitoring systems.

In 2015, we received reports of 594,503 unique IP addresses, which performed scans of network services. These addresses came from 217 countries. We recorded 4,029 unique IP addresses from the Polish networks.

Due to the nature of the data received we decided to divide statistics into three parts: the scanning of services where the country of the source of attack does not matter, scanning from the Polish networks and scanning from abroad.

Some data come from our own sources (the target IP address of the scan is located in Poland), while other come from external sources (when scanning was performed from a computer within a Polish network).

Scanned services

Last year the most frequently scanned port was TCP 23 on which the telnet service is running. We have seen a major change in comparison to 2013: scanning for telnet services accounted for more than half of all scans, compared to 18% in 2013. The increase in activity and a change from the 7th place to 2nd was also recorded for port TCP 22 used by the SSH service. In case of scanning for RDP service (remote desktop) running on port TCP 3389, there was almost 7-fold decrease in the number of unique source IP addresses.

Table 26 presents the 10 most scanned ports.

No.	Destination port	The number of IP addresses	Percentage	Service
1	23/TCP	387,934	51.83%	telnet
2	22/TCP	44,159	5.90%	SSH
3	445/TCP	33,231	4.44%	Windows RPC
4	80/TCP	32,483	4.34%	Web servers, web applications
5	53413/UDP	22,521	3.01%	
6	3389/TCP	20,780	2.78%	RDP (Remote Desktop)
7	8080/TCP	12,896	1.72%	Proxy and web cache
8	1433/TCP	12,165	1.63%	MS SQL
9	137/UDP	8,359	1.12%	NetBIOS
10	3306/TCP	7,308	0.98%	MySQL
–	**other**	**166,585**	**22.26%**	**–**

Table 26. The most frequently scanned ports

Snort rules

Snort rules are used to identify attacks by automated tools. Table 27 presents the 10 rules most often reported by the ARAKIS early warning system.

No.	Snort rule	The number of IP addresses	Percentage	Destination port
1	MS Terminal server request	117,301	16.47%	3389/TCP
2	RDP connection request	117,282	16.47%	3389/TCP
3	LibSSH Based SSH Connection – Often used as a BruteForce Tool	98,148	13.78%	22/TCP
4	Radmin Remote Control Session Setup Initiate	79,028	11.10%	4899/TCP
5	ET POLICY Suspicious inbound to MSSQL port 1433	64,887	9.11%	1433/TCP
6	ET POLICY Suspicious inbound to mySQL port 3306	43,978	6.18%	3306/TCP
7	WEB-IIS view source via translate header	41,142	5.78%	80/TCP
8	ET SCAN Potential SSH Scan	41,010	5.76%	22/TCP
9	ET POLICY Suspicious inbound to PostgreSQL port 5432	22,002	3.09%	5432/TCP
10	ET POLICY RDP disconnect request	13,065	1.83%	3389/TCP
–	**other**	**74,298**	**10.43%**	**–**

Table 27. The Snort rules most reported by the ARAKIS system

Foreign networks

Like in previous years, more than one third of IP addresses performing scans came from China. Russia dropped from the top 3 ranking and the place was taken over by Turkey. The top 10 ranking for countries is presented in table 28.

No.	Country	The number of IP addresses	Percentage
1	China	223,621	37.61%
2	USA	37,921	6.38%
3	Turkey	36,318	6.11%
4	Taiwan	25,880	4.35%
5	Russia	24,675	4.15%
6	India	23,659	3.98%
7	Brasil	21,767	3.66%
8	South Korea	18,173	3.06%
9	Spain	17,524	2.95%
10	Thailand	12,161	2.05%
–	**other**	**152,804**	**25.70%**

Table 28. Countries with IP addresses performing the biggest number of scans (excluding Poland)

Table 29 presents foreign autonomous systems with the biggest number of IP addresses that performed scans. The first two places in the ranking were occupied by Chinese networks with the percentage of 31%. The top 10 does not include any of the USA autonomous systems, despite the fact that the country was on the 2nd place in the ranking of countries. The reason for such results is probably related to the fact that in China there are only few but large state-owned networks, and in the USA there are many more networks with their own AS numbers.

No.	ASN	AS name	Country	Number of IP addresses	Percentage
1	4134	China Telecom Backbone	China	92,693	15.81%
2	4837	China Unicom Backbone	China	89,643	15.29%
3	9121	Turk Telekomunikasyon Anonim Sirketi	Turkey	30,360	5.18%
4	3462	Data Communication Business Griup	Taiwan	19,640	3.35%
5	12715	Jazz Telecom	Spain	14,769	2.52%
6	9829	BSNL (Bharat Sanchar Nigam Ltd)	India	11,300	1.93%
7	4766	Korea Telecom	South Korea	10,548	1.80%
8	4788	™ NET	Malaysia	6,535	1.11%
9	28573	CLARO S.A.	Brazil	4,636	0.79%
10	4808	CNCGROUP	China	4,030	0.69%
–	**–**	**other**	**–**	**302,266**	**51.54%**

Table 29. Foreign autonomous systems with most IP addresses that were sources of scans

Polish networks

For scans coming from the Polish networks the first place was taken by Orange Polska S.A. with the share of a third of all Polish addresses that were sources of scans. The top 10 also includes networks that weren't as high in the ranking in previous years: Livenet, Sprint and TK Telekom. Full ranking is presented in the table 30.

No.	ASN	AS name	The number of IP addresses	Percentage
1	5617	Orange Polska S.A.	1,400	35.71%
2	12741	Netia S.A.	395	10.08%
3	21021	Multimedia Polska S.A.	182	4.64%
4	59491	Livenet sp. z o.o.	97	2.47%
5	49185	Protonet	80	2.04%
6	197226	Sprint S.A.	78	1.99%
7	20960	TK Telekom sp. z o.o.	70	1.79%
8	6714	T-Mobile Polska S.A.	63	1.61%
9	29314	Vectra S.A.	62	1.58%
10	12912	T-Mobile Polska S.A.	55	1.40%
–	**–**	**other**	**2,482**	**63.32%**

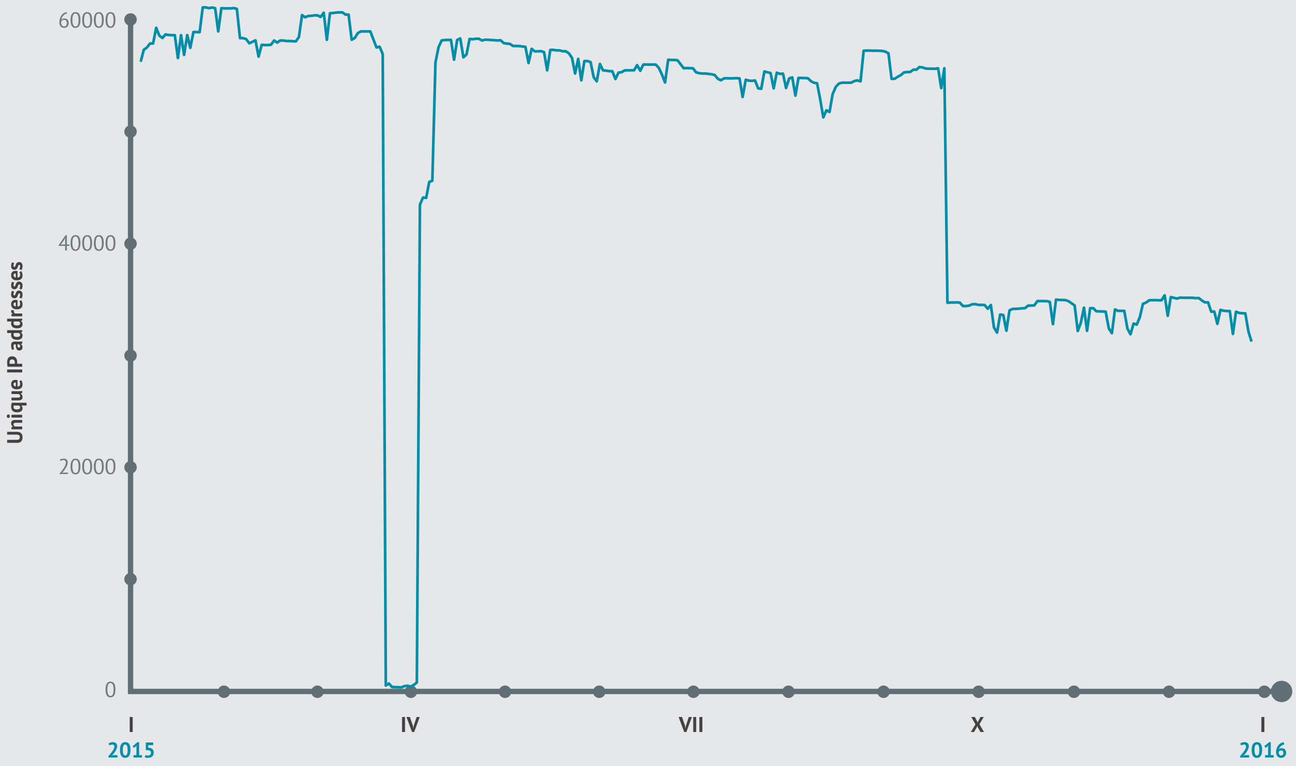
Table 30. Polish autonomous systems with the biggest numbers IP addresses that were sources of scans

“In the last year the most reported misconfigured services were SSDP and open DNS and SMTP servers.”

Misconfigured services in Polish autonomous systems

Similarly to 2014, most of reports of misconfigured services in the past year concerned services like SSDP, open DNS servers and SNMP. A positive development, concerning those three protocols, was a decline of the total number of IP addresses which these services were running on over the year. In the terms of the average number of daily reports the NetBIOS and NTP are following them in the ranking. In this case, however, we've seen an increase in the number of misconfigured servers. Further in the ranking are the services with the number of reports being less than a thousand a day: Chargen and QOTD. Due to the relatively small number of reports for Chargen and QOTD their analysis is omitted. In examining the situation in each autonomous systems we chose only those that have at least 10,000 IPv4 addresses.

Figure 4. **The number of unique IP addresses of incorrectly configured DNS servers**

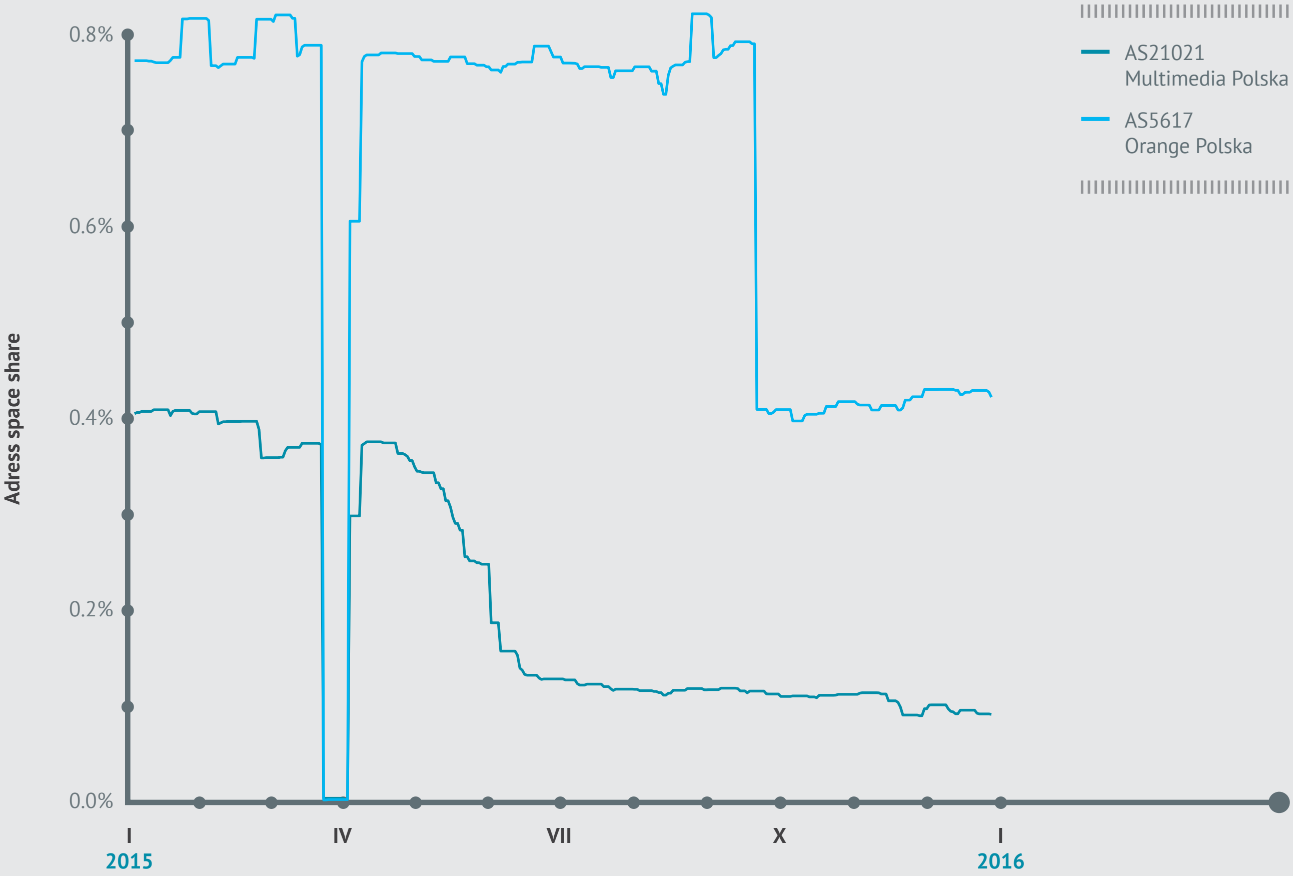


DNS

The Multimedia Polska network scored the largest (more than 4x) decrease of IP addresses with open DNS servers in relation to the size of the autonomous system. Daily number of reports for open DNS servers in the Multimedia Polska network fell in mid-2015 from over 2,000 to just over 500 and remained like that until the end of the year. It is less than 0.1% of IP addresses belonging to the autonomous system 210210 belonging to the Multimedia Polska. From early 2015 until mid-September, the highest rate of daily reported IP addresses of open servers accounted for nearly 0.8% of all IP addresses reported to the system. However, in the second half of September we have seen a sharp decline of nearly half, i.e. to 0.4% of the number of IP addresses of Orange Polska network (AS5617). This number remained at a similar level until the end of 2015.

We did not see a large, significant autonomous system with the number of open DNS servers increasing during 2015.

Figure 5. **Address space of Multimedia Polska and Orange Polska with incorrectly configured DNS servers**



SNMP

Similarly to DNS, we have not observed an increase in the number of misconfigured SNMP servers in any AS. The largest decrease of 2.5x was observed in T-Mobile Polska networks (AS12912 and AS6714), but the overall scale was minuscule: 0.29% of all T-Mobile's IP addresses at the beginning of the year and 0.12% of all IP addresses in the available address pool of T-Mobile were reported daily as addresses that host incorrectly configured SNMP services.

Autonomous system with the highest percentage of the address pool has been reported to the n6 platform as hosting incorrectly configured SNMP services was Netia (AS12741) with a score of more than 1.4% at beginning of the year and nearly 0.8% at the end of 2015.

Figure 6. **The number of unique IP addresses with incorrectly configured SNMP servers**

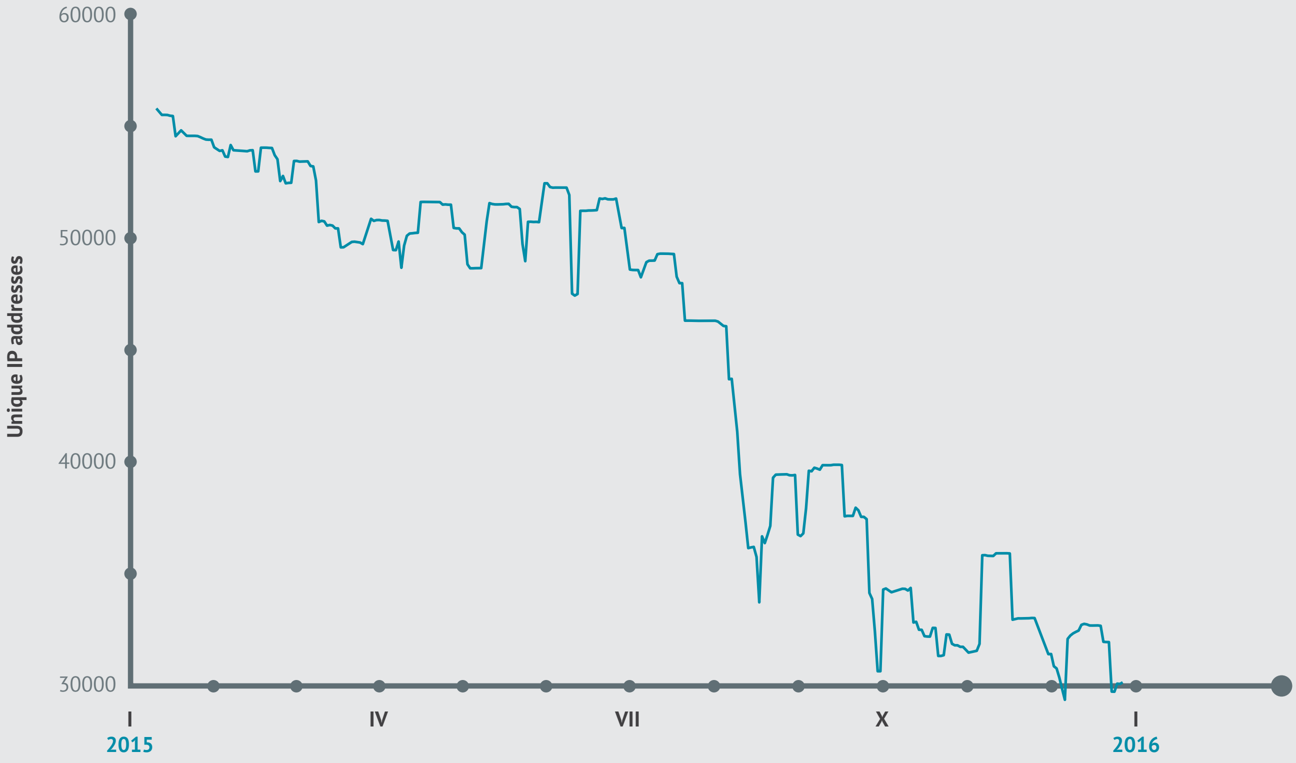
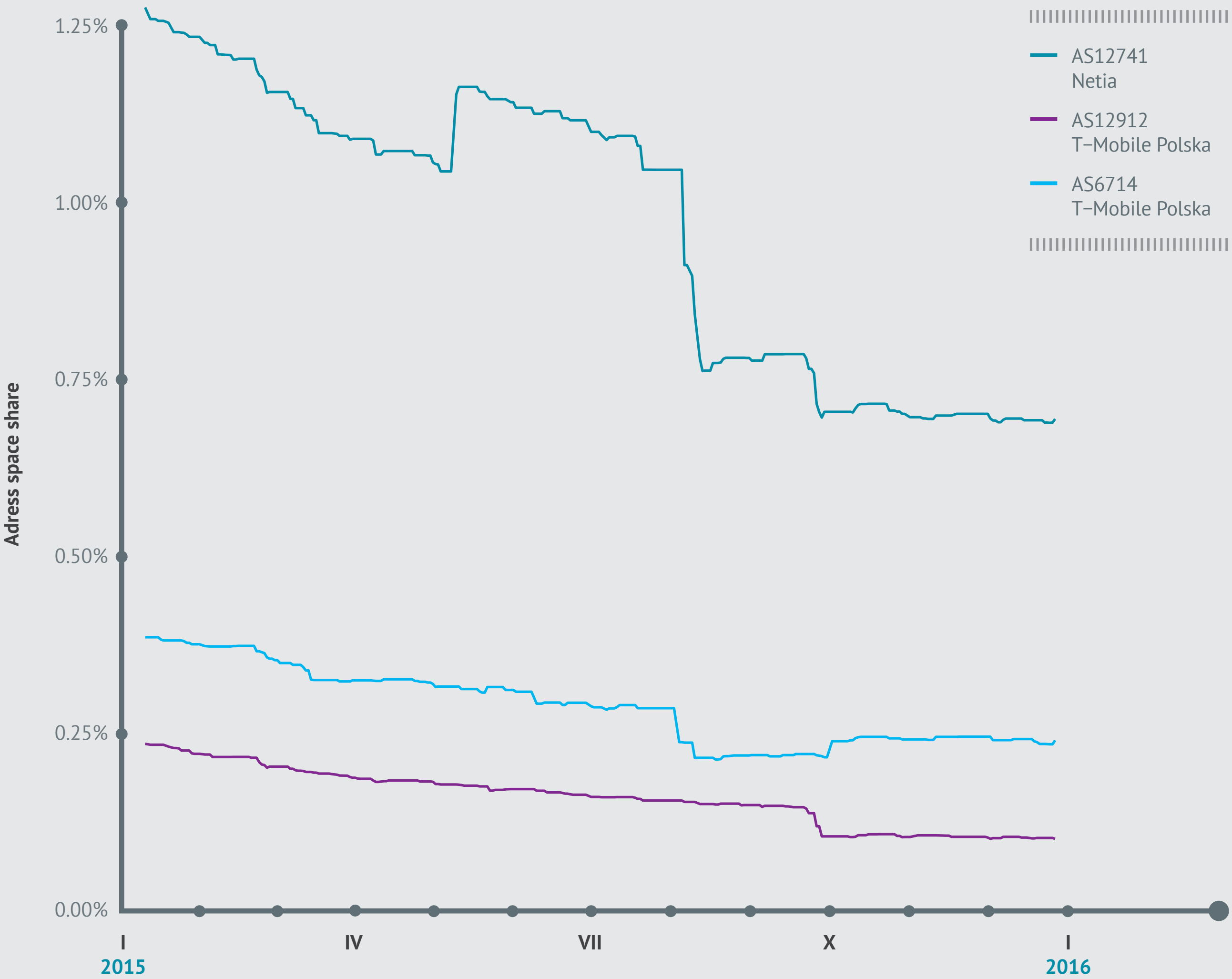


Figure 7. **Address space of Netia and T-Mobile networks with incorrectly configured SNMP servers**



SSDP

SSDP is the second protocol in terms of daily number of reports of open servers available on public IP address space. It is worth noting that in the case of SSDP there were autonomous systems reported, with more than 1% of all IP addresses reported as SSDP servers running on public address space. The record belongs to Servcom autonomous system (AS41256), where the maximum daily number of reported IP addresses of open SSDP services was 2,149, which is 5.6% of all addresses belonging to the provider. It is interesting that this number has doubled during the year. Among the networks witha size of more than 10,000 IP addresses a positive surprise was Multimedia Polska (AS21021), which successfully reduced number of reported IP addresses 9x (a decrease from 1.35% to 0.15%).

Figure 5. **The number of unique IP addresses from incorrectly configured SSDP servers**

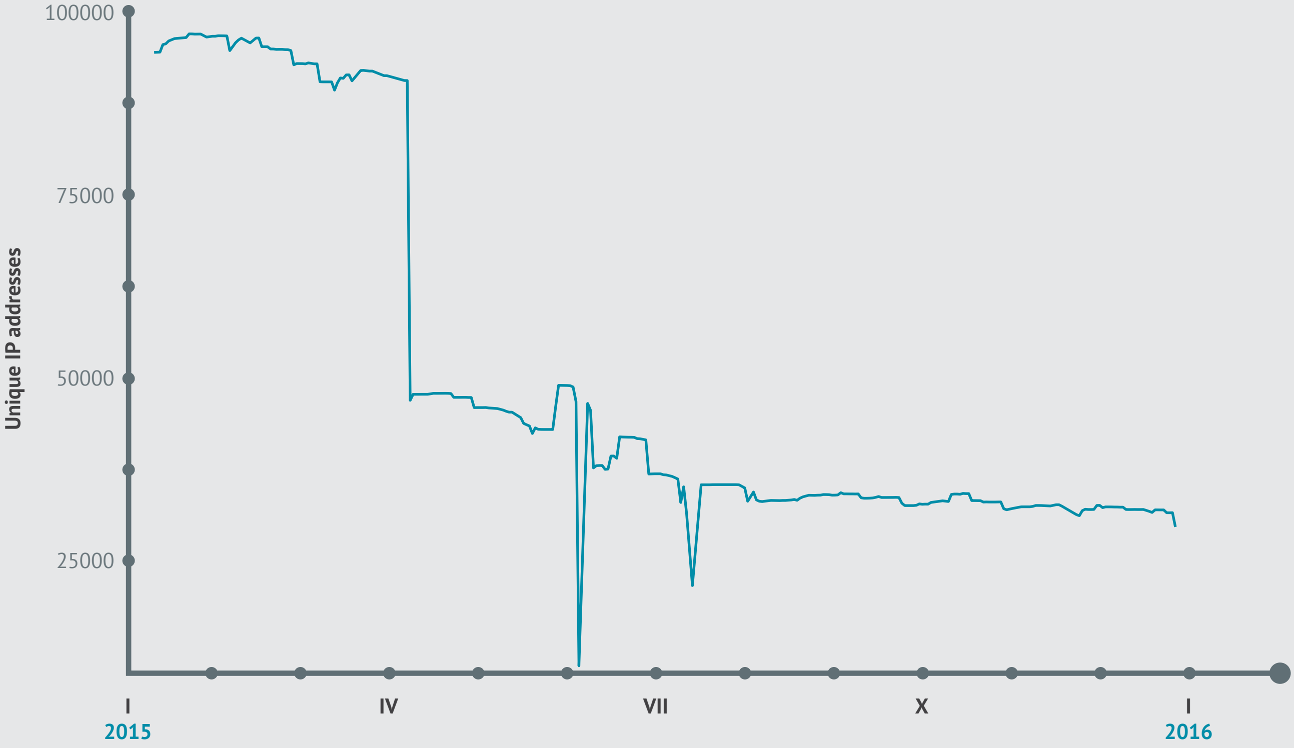
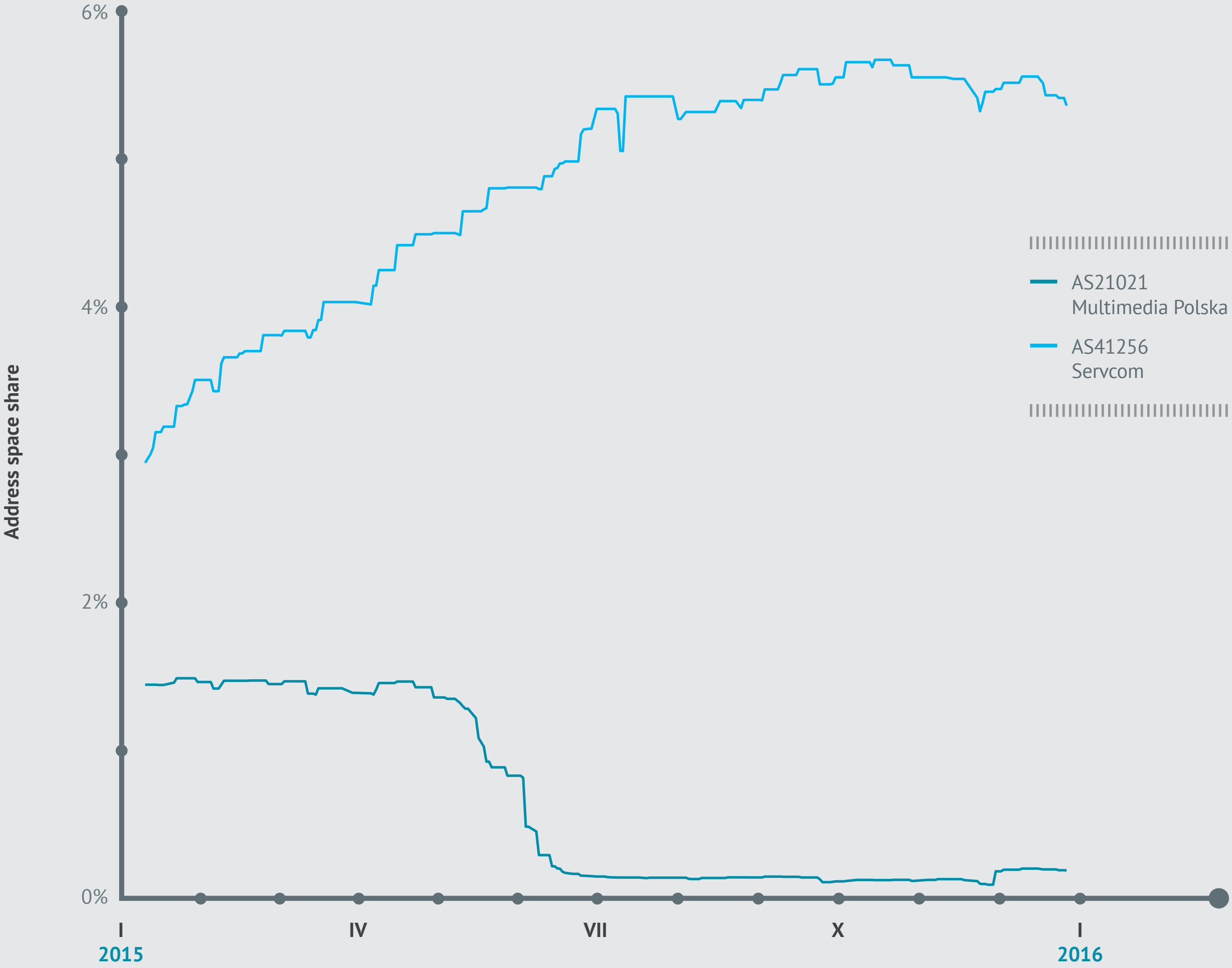


Figure 9. **Address space of Multimedia Polska and Servcom with incorrectly configured SSDP servers in 2015**



NTP

Number of servers that provide NTP service, commonly used to synchronize system time with standard time sources, and in the case of a misconfiguration - giving possibility of DDoS attacks, increased during the year by 25 percent. Apart from networks of Multimedia Polska (AS21021), Cyfronet AGH (AS8267) and Internetia (AS43939) we didn't register any other autonomous systems with decreasing number of incorrectly configured NTP servers. T-Mobile stands out quite negatively with one of its autonomous systems (AS6714), where the number of incorrectly configured NTP servers increased during the year 3x and is still growing.

Figure 10. **The number of unique IP addresses of incorrectly configured NTP servers in 2015**

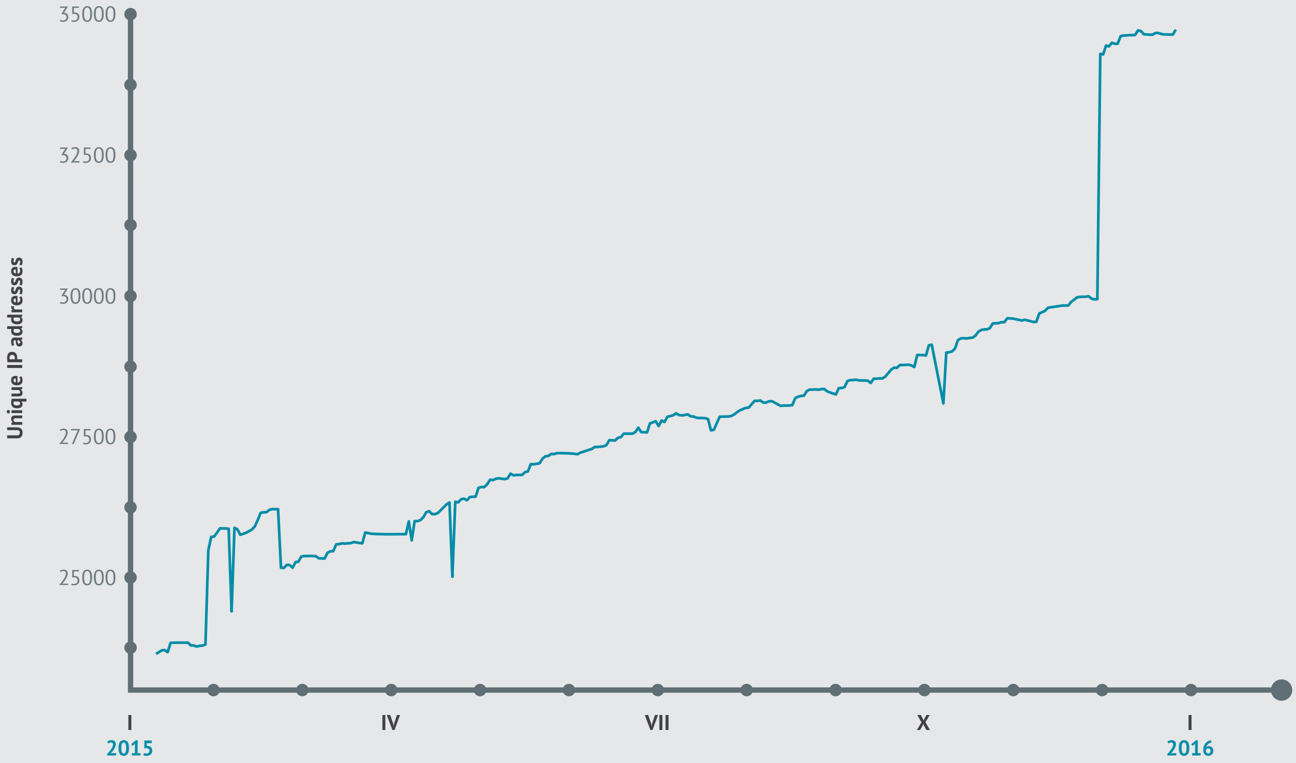
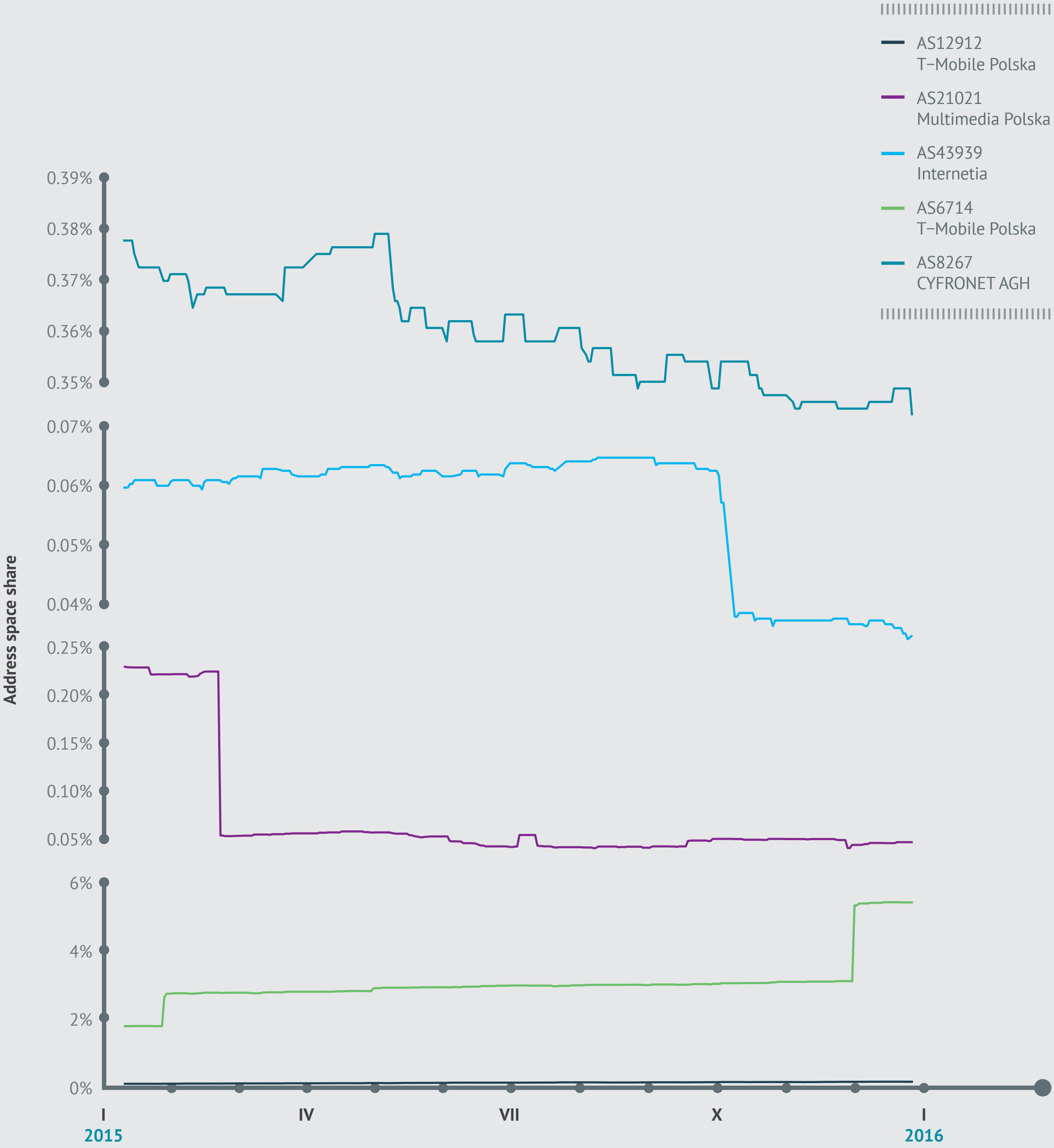


Figure 11. **Address space of networks of Cyfronet AGH, Internetia, Multimedia Polska and T-Mobile Polska with incorrectly configured NTP servers in 2015**



NetBIOS

Incorrectly configured NetBIOS servers were also used to perform DDoS attacks and their number has increased in the past year by as much as 75 percent. With an average number of reports at just over 17,000 IP addresses per day, a big impact on the increase in the overall number of misconfigured servers had Orange Polska (AS5617), where we recorded 600% growth, and the network of Biznes-Host.pl (AS198414), which turned out to be the infamous leader in terms of the number of misconfigured servers in relation to the size of its network. More than 13% of IP addresses that belong to Biznes-Host.pl were reported in December 2015 to the n6 system as incorrectly configured NetBIOS services (for comparison, the problem of misconfigured NetBIOS service in the network of Orange Polska affected less than 0.14% of the address pool). In the other autonomous systems, the level of misconfigured NetBIOS servers remained unchanged or decreased, particularly in the networks of INEA (AS13110) and Multimedia Polska (AS21021).

Figure 12. **The number of unique IP addresses with incorrectly configured NetBIOS servers in 2015**

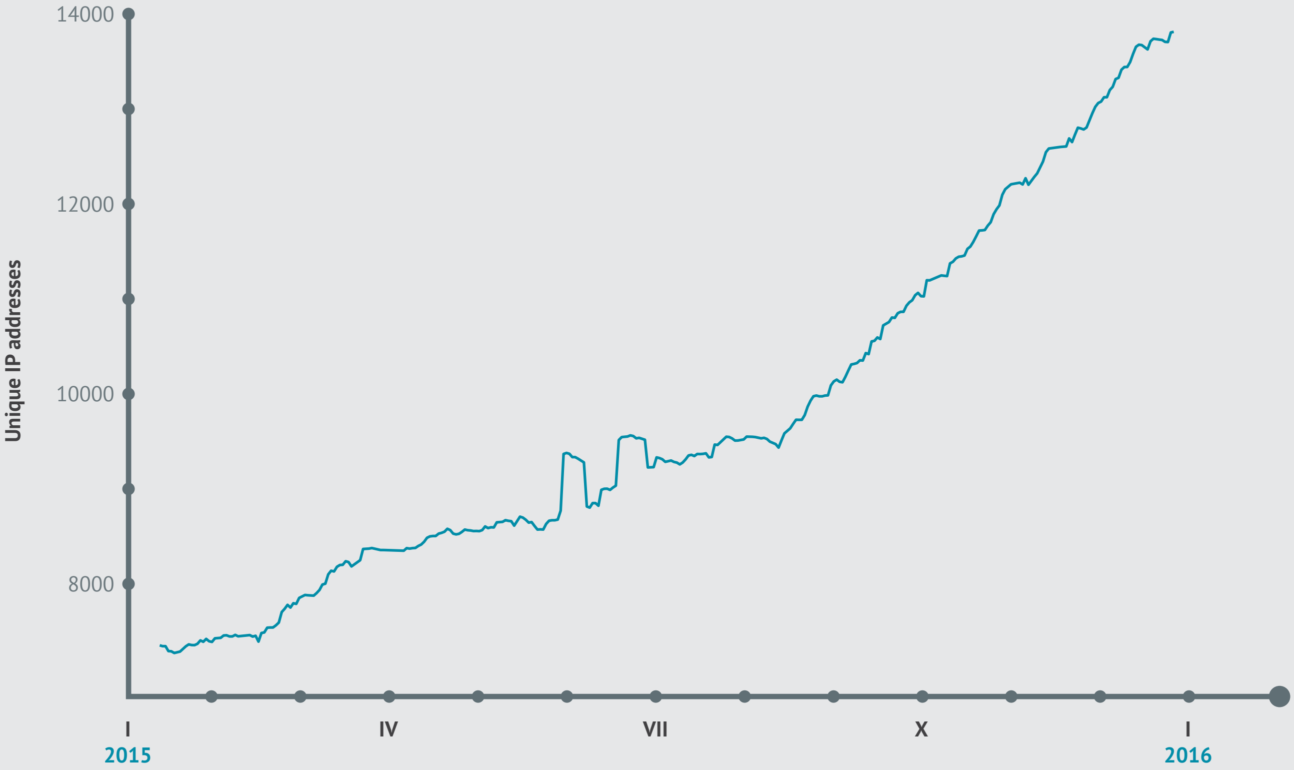


Figure 13. **Network address space of INEA, Multimedia Polska and Orange Polska with incorrectly configured NetBIOS servers in 2015**

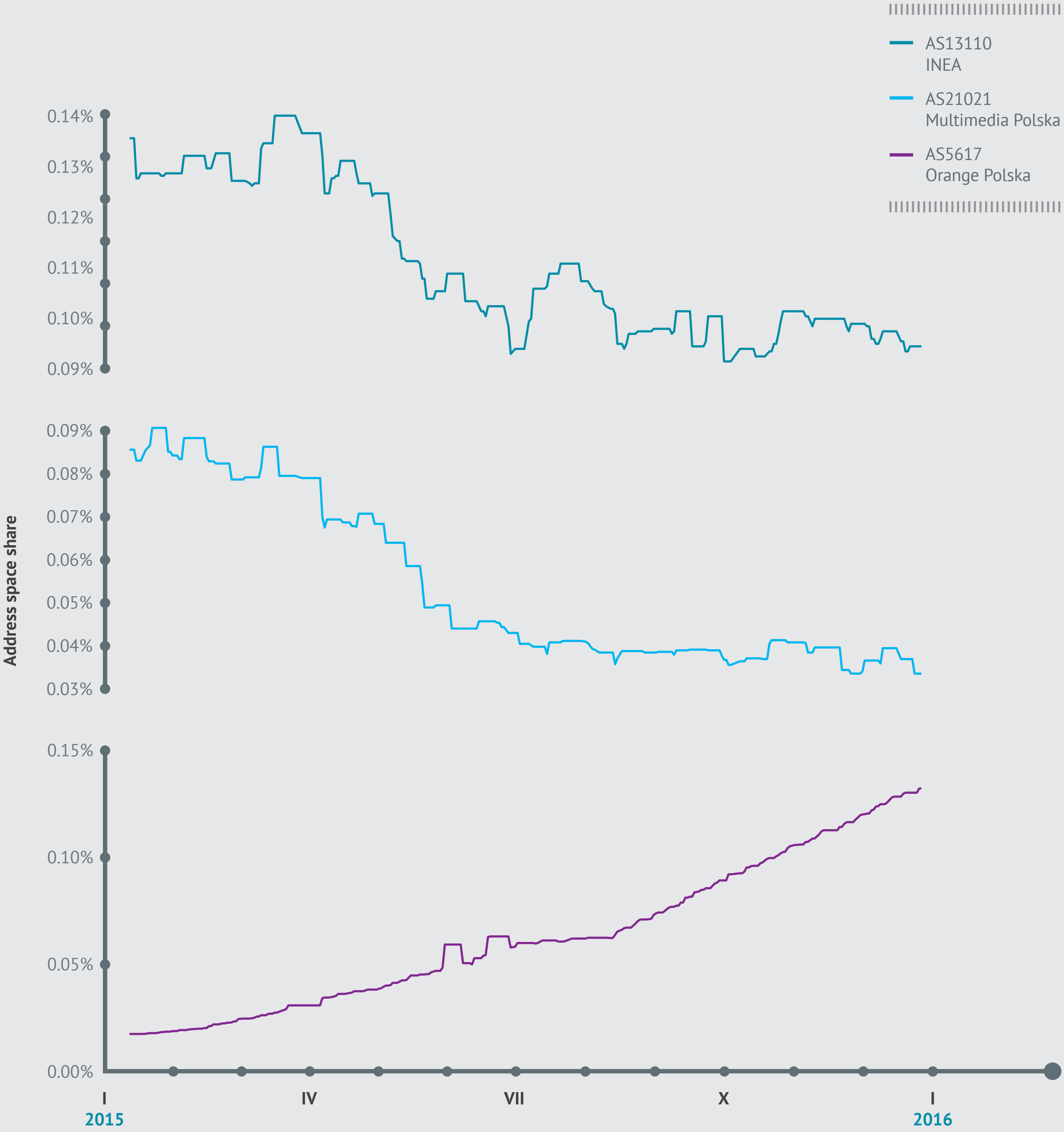
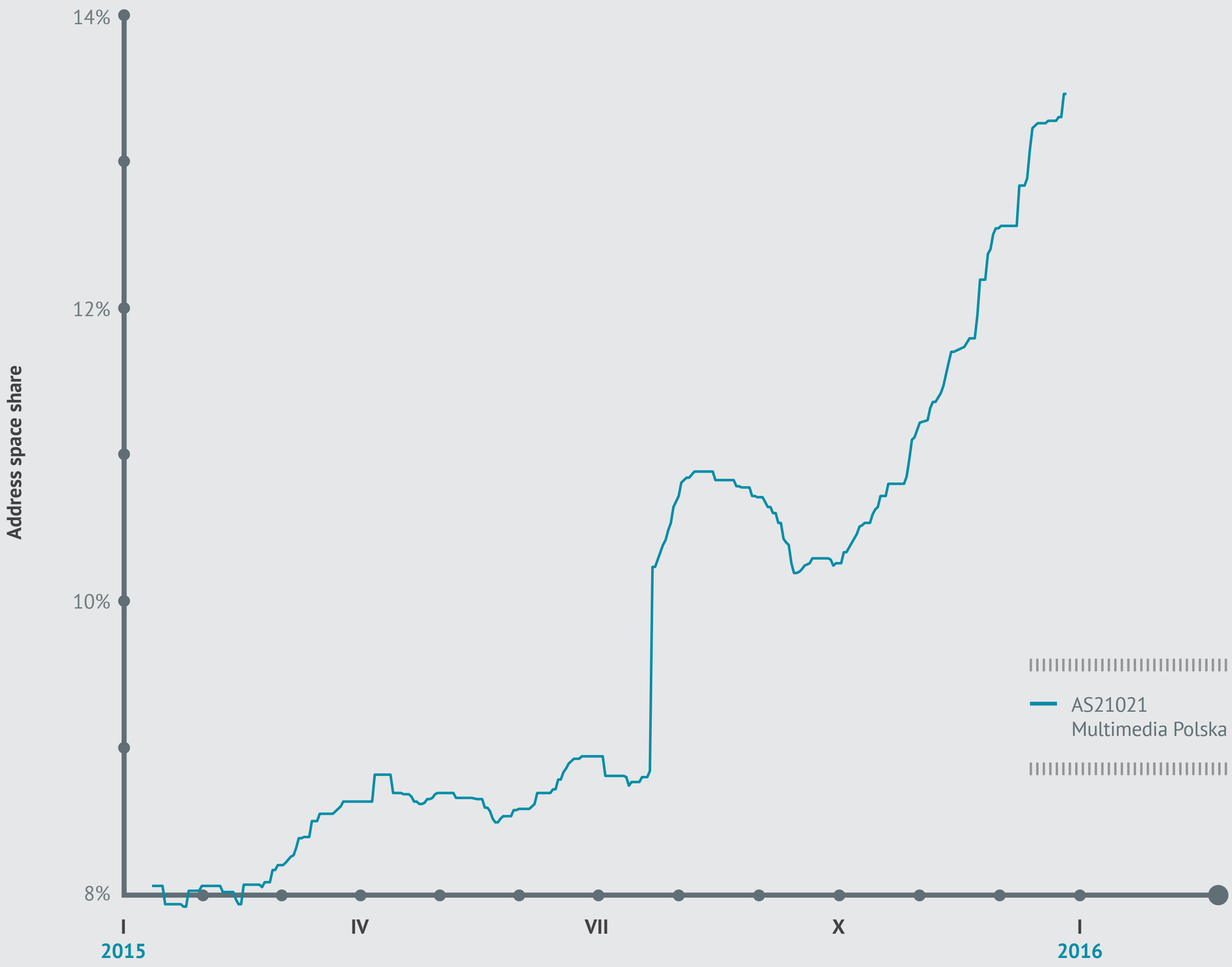


Figure 14. **Przestrzeń adresowa sieci Biznes-Host.pl z błędnie skonfigurowanymi serwerami NetBIOS w 2015 roku**



Contact

Incident reports: cert@cert.pl
Spam reports: span@cert.pl
General contact: info@cert.pl
PGP key: www.cert.pl/pub/0x553FEB09.asc

Web: www.cert.pl
Facebook: fb.com/CERT.Polska
RSS: www.cert.pl/rss
Twitter: @CERT_Polska, @CERT_Polska_en

CERT.PL>_

NASK/CERT Polska
ul. Kolska 12, 01-045 Warszawa
Phone: +48 22 38 08 274
Fax: +48 22 38 08 399

Graphical design and layout:
DUSZEK STUDIO Agata Duszek

Scan this QR-Code
with your smartphone
to visit our web page.