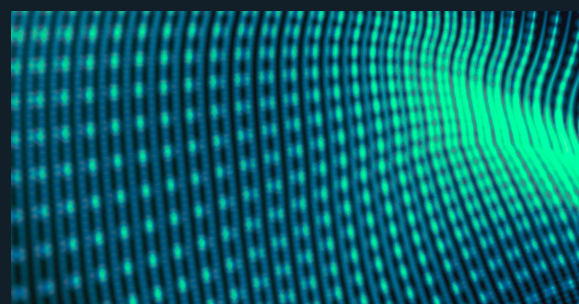




ANNUAL REPORT

FROM THE ACTIONS
OF CERT POLSKA



2021

The Polish Internet
security landscape

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/en

**ANNUAL
REPORT**
FROM THE ACTIONS
OF CERT POLSKA

2021

The Polish Internet
security landscape

Introduction	7
About CERT Polska	9
Highlights from 2021	11
Calendar of key incidents	14
Protection of Polish cyberspace and actions taken by CERT Polska	19
Annual summary of reported incidents	20
Warning List	25
#BezpiecznyPrzemysł (Safe Industry)	28
SECURE conference	30
Exercises and competitions	31
Locked Shields	31
European Cyber Security Challenge	32
CTF scene	33
Projects	35
MWDB and Karton	35
MWDB Core project development	35
Automatic classification of malware samples based on ApiVectors	36
mwdb.cert.pl statistics	38
DRAKVUF Sandbox	39
DRAKVUF project development in 2021	39
Google Summer of Code	39
CERT Polska participates in GSoC	40
Linux Injector for automated malware analysis	40
HID simulation for DRAKVUF	40
n6 3.0 – new release	41
MeliCERTes	42
CyberExchange	43

Incidents and threats	44
Ransomware	45
Major threats	46
Observed trends	46
Ransomware as a Service model development	46
Multiple extortions	46
Increase in damage resulting from attacks	47
Law enforcement effort mounting	47
Relevant ransomware families	47
REvil/Sodinokibi	47
Conti	47
Hive	47
Ransomware guidebook	48
Major vulnerabilities in 2021	48
Log4Shell	49
VMware vCenter	49
Microsoft Exchange	50
ProxyLogon	50
ProxyShell	51
Evolution of known phishing campaigns	51
Facebook account takeovers	51
Fake payment gateways	54
Phishing from sellers on advertising websites	55
Text message campaigns in Poland	57
Malware targeting mobile devices	57
Overview of new trojans detected	58
Flubot	58
BlackRock	58
ERMAC	58
Malware campaigns for Android devices observed in 2021	58

Inpost parcel pick-up	59
Terms and conditions update and anti-spam policy	60
STOP COVID	62
Parcel delivery	63
Voicemail	64
mObywatel	65
Adobe Flash update, received photos	66
Incorrect DPD Pickup order address	67
Parcel delivery, voicemail and Adobe Flash update	68
How can you avoid infections?	68
Scams and fake investment schemes	70
Data leaks	75
How is data leaked?	75
Cybercriminal activities	76
How can you assure your safety?	76
Provide just the minimum amount of personal data required	76
Use the identity separation method	76
Use unique, strong passwords	76
Respond to incident alerts	77
How can you respond to a data leak?	77
Attack on Trusted Profile	78
Incident analysis	79
Perpetrator apprehended	79
Impersonation, threats and false bomb scare alerts	80
Formbook/XLoader malware campaigns	80

Statistics	84
Statistical accuracy and limitations	85
Botnets	85
Botnets in Poland	85
Botnet activity broken down by telecoms operators	86
C&C servers	88
Phishing	90
Malicious pages	91
Services facilitating DRDoS attacks	93
Open DNS servers	96
SNMP	97
Portmapper	98
SSDP	99
NTP	100
NetBIOS	101
Vulnerable services	102
CWMP	106
SSL-POODLE	107
RDP	108
TELNET	108
TFTP	109
BadWPAD	110



INTRODUCTION

A new report and well-known techniques – this is how the key facts observed in 2021 can be summarised. Criminals have perfected well-known methods of committing fraud and have more often turned to methods infrequently used before. We have observed numerous attempts at spoofing by means of not only fake institutional websites, but also such techniques as phone number spoofing or identity theft. To carry out attacks, cybercriminals use tools designed to remotely manage the users' devices and to attempt to use sophisticated social-engineering tricks. All this has translated into a record number of reports in the computer fraud category, whose share in the total number of incidents handled by us was almost 90%. Therefore, in 2021, we still did our utmost to popularise such initiatives as the CERT Polska Warning List. While publishing useful tips in social media, we also provided support to the users themselves, instructing them how to recognise and prevent social-engineering attacks.

In 2021, numerous attack attempts targeting various Internet users' habits and vulnerabilities were also reported. The first example consists in using a single password to several different sites, which enables criminals to gain access to several different accounts. It significantly enhances their

capability to perform planned hostile actions. Another vulnerability enabling fraudsters to achieve their goals is people's naive belief in methods ensuring quick and easy earnings. This year abounded in campaigns promoting rapid profits resulting from fake investments in crypto-currencies or Polish State Treasury company assets. Such scenarios were non-linear, but the result for a victim was always the same - loss of money saved or even borrowed.

As far as more technical aspects of cybersecurity are concerned, two important vulnerabilities must be highlighted: Attempts to exploit Log4Shell and Microsoft Exchange-related vulnerabilities in Poland. They made us realise how important it is to handle the vulnerability management process correctly in modern organisations, and how vital it is to cooperate with the right security team.

The report also includes descriptions of our ongoing research and development projects, including open-source tools. Statistics regarding incidents and threats reported in Polish operator networks, collected via data available from the n6 platform, are also worth noting.

Welcome to our report!

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

def calculate_points(challenge, solves):
    return int(round(challenge.min_points + (challenge.max_points - challenge.min_points) /
                    (1 + (max(0, solves - 1) / 11.92201) ** 1.206969)))

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()

    solver = current_session.get_solver()
    solver.solve(challenge_id=challenge.id, contest_id=contest.id)

    solver.add_solution(challenge, 'flag': flag)

    solver.submit(challenge, 'flag': flag)

    raise ChallengesService.AlreadySolved()
```

ABOUT CERT POLSKA

The CERT Polska team operates within the structures of NASK (Research and Academic Computer Network) - a national research institute which conducts scientific studies, operates the national .pl domain registry and provides advanced IT services. CERT Polska is the first Polish computer emergency response team. Active since 1996 in the response team community, it has become a recognised and experienced entity in the field of computer security.

Since its launch, the team's core activity has consisted in security-incident handling as well as co-operation with similar units worldwide, in terms of operating and research as well as implementation activities. In 1998, CERT Polska became a member of the international forum of response teams (FIRST), and since 2000 it has been a member of the working group of the European response teams: TERENA TF-CSIRT, with the "Certified by Trusted Introducer" status. In 2005 CERT Polska's initiative resulted in establishing a forum for Polish abuse teams, i.e. the Abuse FORUM, and, in 2010, CERT Polska joined the Anti-Phishing Working Group, an association of companies and institutions which actively combat on-line crime. Since the Polish Act on the National Cybersecurity System of 5 July 2018 was enforced, our team has been involved in numerous **CSIRT NASK** tasks, as per Art. 26 of this Act.

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

- monitoring cybersecurity-related threats and incidents at the national level;
- providing information on incidents and risks to entities involved in 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 critical incident handling process;
- cooperating with sector cybersecurity teams in the scope of coordination of major incident handling, including those involving two or more European Union Member States, and critical incidents, and in the scope of exchanging information that allows countering cybersecurity threats;
- performing advanced analyses of malicious software and vulnerabilities;
- monitoring cybersecurity threat indicators;
- developing tools and methods to detect and combat cybersecurity threats;
- conducting awareness-raising activities in the cybersecurity area;
- creating and sharing tools for voluntary cooperation and exchange of information on cybersecurity threats and incidents;
- participating in the CSIRT Network;
- coordinating the process of handling incidents reported by:
 - units from the public finance sector indicated in Art. 9, section 2–6, 11 and 12 of the Act of 27 August 2009 on public finances;
 - units subordinate to or supervised by government administration authorities, excluding units referred to in section 7, item 2 of the Polish Act on the National Cybersecurity System;
 - research institutes;
 - Office of Technical Inspection;
 - Polish Centre for Accreditation;
 - National Fund for Environmental Protection and Water Management and voivodeship-based funds for environmental protection and water management;
 - commercial law companies performing public service tasks within the meaning of Art. 1, section 2 of the Polish Act of 20 December 1996 on municipal management;
 - digital service providers, except for those listed in section 7, item 5 of the Polish Act on the National Cybersecurity System;
 - key service providers, except for those listed in section 5 and 7 of the Polish Act on the National Cybersecurity System;
 - entities other than those listed in items a to j and sections 5 and 7 of the Polish Act on the National Cybersecurity System;
 - natural persons.



HIGHLIGHTS FROM 2021

1. In 2021, CERT Polska registered 29,483 unique cybersecurity-related incidents. It constitutes an increase by as much as 182% compared to 2020. The most widespread type of incident was phishing, i.e. 76.57% of all incidents handled. The number of such notifications increased by 196%, on a year-on-year basis. The economy sectors where such incidents were detected most often included: media, wholesale, mail and courier services.
2. In 2021, our Warning List was supplemented with 33,000 domains. The most commonly observed phishing campaign schemes consisted of illegally obtaining Facebook login credentials. The number of such incidents increased threefold in comparison with 2020.
3. Within the framework of the #BezpiecznyPrzemysł (Safe Industry) activity, we propagate the enhancement of the cybersecurity level of the Polish industrial infrastructure. As a result of searching for new vulnerabilities inherent in the hardware widely used in Poland, five of them were assigned with a CVE number, including two with a high CVSS 10.0 threat level.
4. We observed a 13% increase in the number of ransomware-related incidents. The most intense activity was noted among digital infrastructure entities, natural persons and public administration entities. Most frequently deployed ransomware families included: REvil/Sodinokibi and Phobos, and next Lockbit 2.0, STOP/DJVU, Makop, QLocker and Avaddon.
5. In fact, Ransomware as a Service model became an actual standard. Cybercriminals seek to maximise their profit from a single attack by demanding a ransom not only for encrypted data recovery, but also for refraining from disclosing or reporting an attack.
6. Critical security gaps were detected in such popular software as: VMware vCenter, Microsoft Exchange and the Apache Log4j library. In each case, we strived to determine a number of vulnerable devices in Poland and contact affected entities to inform about problems and provide them with methods of mitigation.
7. Cybercriminals focused on perfecting well-known phishing scenarios: taking over Facebook accounts, providing fake payment gateways and extorting money from sellers on classifieds sites.
8. We observed the advent of three new trojans for the Android platform, i.e. Flubot, BlackRock and ERMAC. They were most frequently distributed via fake text messages and emails containing links to adequately crafted websites.
9. Due to the increase in the number of acts using such text messages as a means for distributing malicious links, we launched a special line at: +48 799 448 084, where an incident can be reported by forwarding a text message containing a suspicious link.
10. Cybercriminals began to exploit a new fraud scheme involving fake cryptocurrency investment opportunities. Two scenarios were most widely used. Firstly, phone calls were made concerning supposedly previously invested funds. Secondly, sites offering fake investment opportunities were promoted on social media.
11. On 21 July 2021, the CERT Polska team observed an inflow of notifications and media publications on alarming emails received by Profil Zaufany (Trusted Profile) users. We established that it was a "credential stuffing" type of attack, consisting in mass attempts to log into ePUAP platform user accounts

by means of passwords obtained as a result of previous data leaks. At the beginning of August 2021, Warsaw Metropolitan Police officers apprehended a suspect in the town of Wola Krzywiecka.

12. In total, we collected information on 439,077 zombie IP addresses, which shows decrease by 31% in relation to 2020. As during the previous year, the most common ones include Andromeda, Avalanche and Conficker. Next there is the Flubot attacking the Android system, followed by QSnatch responsible for QNAP device infections.
13. Over the whole year, we noted a gradual decrease in the number of devices facilitating DRDoS attack deployment, using such services as DNS open resolvers, SNMP, portmapper and SSDP. As for NTP, Netbios and mDNS services, the number of IP addresses remains at a similar level throughout the year.
14. As before, the most vulnerable services included: CWMP, SSL-POODLE, RDP, Telnet and TFTP. Over the last year, we observed a positive trend consisting in the gradual decrease in numbers of devices related to the Poodle vulnerability, as well as RDP and Telnet services. This trend began in 2020. Significant decrease in the number of vulnerable devices was also noted in relation to the CWMP service.



CALENDAR OF KEY INCIDENTS

JANUARY

28.01

Critical vulnerability of CVE-2021-3156 in Sudo.

<https://cert.pl/posts/2021/01/krytyczna-podatnosc-cve-2021-3156-w-sudo/>

28.01

Ransomware attack on the chain of American Heart of Poland cardiology clinics.

<https://zaufanatrzeciastrona.pl/post/atak-ransoware-na-najwieksza-siec-klinik-kardiologicznych-w-polsce/>

FEBRUARY

4.02

Police liquidated a criminal group responsible for setting up fake on-line stores.

<https://zaufanatrzeciastrona.pl/post/nastepna-banda-internetowych-oszustow-w-rekach-policji/>

9.02

CD Projekt informs about a ransomware attack on the company's network.

<https://niebezpiecznik.pl/post/cd-projekt-informuje-o-ataku-ransomware-na-swoja-siec/>

18.02

Personal Data Protection Office (UODO) imposed a fine of PLN 100,000 on the National School of Judiciary and Public Prosecution (KSSIP) in relation to a data leak in 2020.

<https://niebezpiecznik.pl/post/100-tys-zi-kary-za-wyciek-danych-sedziow-i-prokuratorow/>

MARCH

2.03

Critical vulnerabilities within the Microsoft Exchange email server.

<https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901>

10.03

Unavailability of numerous sites in Europe caused by an OVH server room fire.

<https://niebezpiecznik.pl/post/splonela-serwerownia-ovh/>

17.03

Break-ins at the National Atomic Energy Agency site and zdrowie.gov.pl portal.

<https://niebezpiecznik.pl/post/panstwowa-agencja-atomistyki-zhackowana-wrzuciono-falszywy-komunikat-o-wzroscie-promieniowania/>

APRIL

3.04

Disclosing a package of 533 million Facebook users' data.

<https://niebezpiecznik.pl/post/facebook-wyciek-dane-533-milionow-uzytownikow/>

20.04

Leak of personal data related to over 20,000 police officers, fire-fighters, customs officers and border control officers.

<https://niebezpiecznik.pl/post/wyciek-20000-danych-policjantow-funkcjonariuszy/>

MAY

18.05

Distributing spoof emails "conscription to the cyber-army" misrepresenting an affiliation with Brigadier-General Karol Molenda.

<https://niebezpiecznik.pl/post/nie-nie-zostales-powolany-do-cyberwojska/>

JUNE

1.06

Uniqi published the email addresses of several thousand clients by sending emails without using the "blind carbon copy" (BCC) option

<https://niebezpiecznik.pl/post/wpadka-uniqa/>

8.06

Break-in at Minister Michał Dworczyk's email box.

<https://niebezpiecznik.pl/post/michal-dworczyk-wyciek-telegram/>

JULY

18.07

Amnesty International published a report on Pegasus spyware operation analysis.

<https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/>

31.07

Leak of Tauron clients' data.

<https://niebezpiecznik.pl/post/wykradziono-dane-osobowe-klientow-aurona-w-tym-nagrania-rozmow/>

AUGUST

13.08

Police apprehended the person responsible for the credential stuffing attack carried out in relation to the Profil Zaufany (Trusted Profile) functionality.

<https://niebezpiecznik.pl/post/wlamywal-sie-na-profile-zaufane-zostal-aresztowany-na-2-miesiace-ale-grozi-mu-8-lat/>

15.08

Critical errors in Realtek Wi-Fi modules.

https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2021-35392_35395.pdf

16.08

Leak of a2mobile, Premium Mobile and NAU Mobile clients' data.

<https://niebezpiecznik.pl/post/dane-klientow-a2mobile-premium-mobile-i-nau-mobile-byly-dostepne-dla-wlamywaczy/>

SEPTEMBER

11.09

Leak of Centrum Medyczne Luxmed Lublin sp. z o.o. client data.

<https://niebezpiecznik.pl/post/luxmed-informuje-o-incydencie-otwarty-dostep-do-danych-osobowych-pacjentow/>

30.09

Ransomware attack on Totolotek.

<https://niebezpiecznik.pl/post/totolotek-zhackowany-dane-uzytownikow-mogly-wyciec/>

OCTOBER

4.10

Malfunction resulting in a Meta company server unavailability lasting for several hours.

<https://niebezpiecznik.pl/post/facebook-whatsapp-i-instagram-nie-dzialaja/>

8.10

Fake COVID vaccination certificates.

<https://niebezpiecznik.pl/post/falszowanie-certyfikat-covid-paszport/>

NOVEMBER

4.11

Some REvil ransomware group members apprehended.

<https://www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged>

8.11

Open letter from CERT Polska personnel.

<https://cert.pl/posts/2021/11/list-otwarty/>

8.11

Ransomware attack on European Media Markt branches.

<https://www.bleepingcomputer.com/news/security/mediamarkt-hit-by-hive-ransomware-initial-240-million-ransom/>

16.11

Mandiant company published a report related to UNC1151 activity.

<https://www.mandiant.com/resources/unc1151-linked-to-belarus-government>

DECEMBER

10.12

Critical vulnerability in the Apache Log4j library.

<https://cert.pl/posts/2021/12/krytyczna-podatnosc-w-bibliotece-apache-log4j/>

A man with short brown hair, wearing a light blue button-down shirt and a lanyard, is focused on his silver laptop. He is standing in a futuristic, teal-lit environment with blurred background lights and structural elements. The overall mood is professional and technological.

**PROTECTION
OF POLISH
CYBERSPACE AND
ACTIONS TAKEN
BY CERT POLSKA**

Annual summary of reported incidents

Each year, CERT Polska successively records a growing number of notifications and incidents related to cybersecurity. In 2021, CERT Polska recorded 116,071 notifications. Among them, our specialists defined 65,586 notifications, on the basis of which **29,483 (in total) unique cybersecurity-related incidents were recorded.**

Incident-related notifications can be submitted to us in the following ways:

- to our email address: cert@cert.pl;
- via a form available at incydent.cert.pl;
- via a form available at incydent.cert.pl/domena;
- by telephone: +48 22 380 82 74;
- by post using the form available at bip.nask.pl.

CERT Polska recorded an **increase in the number of incidents handled by as much as 182% compared to the previous year.** One must also remember that, in 2020, CERT Polska handled 10,420 unique cybersecurity-related incidents.

The most widespread type of incidents in 2021 was phishing, i.e. 76.57% of all incidents handled. **In comparison with the previous year, the number of incidents classified increased by 196%,** to a new level of 22,575 incidents. Similarly to the previous year, the March 2020 launch of the Warning List against hazardous sites exerted fundamental impact on the increase in the number of phishing-related incidents recorded. In 2021, the most widespread phishing attacks consisted in Facebook spoofing, i.e. 4852 incidents.

The other most widespread incident type recorded and handled by CERT Polska was malware. In 2021, 2847 incidents of this type were recorded, i.e. 9.66% of all incidents handled. In relation to the previous year, this number increased by 281%.

The third place in the ranking of the number of incidents recorded last year goes to the category of offensive and illegal content, including spam. In total this amounted to 1.05%. Such low percentage results from the fact that the CERT Polska team often ascribes numerous notifications to a single

incident. It is particularly noticeable in this incident category, because as many as 21,522 notifications were related to 311 incidents. Additionally, incidents related to the offensive and illegal content are handled by the dedicated Dyżurnet.pl team, also operating within NASK structures. Frequently handled incidents of this type were the sextortion scam attacks consisting in the mass distribution of emails informing about the alleged takeover of the victim's equipment and the possession of materials presenting the victim in an erotic context. In exchange for paying the requested ransom, the attacker offers to delete the compromising material.

While recording incidents, CERT Polska classifies them and ascribes them to corresponding sectors. In 2021, CERT Polska specialists recorded 8339 (in total) incidents related to the media sector. This is approximately 28.28% of all incidents recorded. This sector includes, but is not limited to, incidents occurring on social media, in the press or on television. Among all incidents classified to the media sector, 91.73% of incidents were phishing-related.

The next sector in terms of the number of recorded incidents was the wholesale and retail commerce sector. In this sector, 17.38% (in total) of all incidents were recorded, i.e. 5125 incidents. It includes, among other things, incidents on auction sites and on-line shops. Similarly to the media sector, phishing incidents also account for a significant proportion of all incidents, i.e. 89.17%.

The third sector (4338 incidents) was the mail and courier service sector. There, 4338 cybersecurity-related incidents were recorded, 84.14% of which were related to phishing. This sector included incidents involving freight-forwarding companies or email operators.

In 2021, within the framework of the Act on the National Cybersecurity System, CSIRT NASK handled **36 incidents classified as serious**, i.e. incidents whose occurrence caused considerable interference in key service provision. They included 31 serious incidents in the banking sector, 3 in the power generation sector and 2 in the healthcare sector. CERT Polska recorded 4 more serious incidents than in 2020.

In 2021, CSIRT NASK handled 512 incidents related to public entities. It constituted an 11% increase in comparison with the previous year. Incidents classified as public entity-related incidents were most frequently recorded in the public administration sector, i.e. 288 cases. Other sectors included: education and upbringing – 81 incidents, and digital infrastructure – 43 incidents.

See Table 1 and 2 for detailed incident statistics, divided into economic sectors and incident types.

In the middle of April 2021, the presence of Flubot malware was initially detected in Poland. Due to the fact that it spreads via text messages, we launched a special telephone line to handle it. Since 24 April, users can report an incident to CERT Polska by forwarding a received text message containing suspicious links to the telephone number +48 799 448 084.

By the end of last year, **we had received 23,308 notifications to this dedicated number**, whose content included URLs. 11,852 of them (50.8%) were located within a domain included in the Warning List. **Thanks to such text message notifications, 3,588 malicious domains were blocked. This was 10.6% of all domains blocked in 2021.** This number is quite surprising, given that most of them were placed on the list in November and December.

Launching the text message notification channel also enabled us to gain an insight into the types of fraud most often spread using this method. Conclusively, as many as 10,693 malicious links were related to Flubot distribution, which was the key reason for launching this notification channel. The second most numerous incidents were related to phishing using the PGE and InPost company image. The number of notifications related to this campaign reached 863. The third place in this infamous ranking goes to scams aimed at auction portal sellers, i.e. 403 incidents. All these campaigns are described in detail in the individual chapters below.

Economy sector	Number of incidents	%
Power engineering	4,084	13.85%
Transport	220	0.75%
Banking	947	3.21%
Financial market infrastructure	563	1.91%
Healthcare	150	0.51%
Water supply systems	18	0.06%
Digital infrastructure	1,606	5.45%
Other	68	0.23%
None	0	0.00%
Public administration	429	1.46%
Construction and real estate management	89	0.30%
Culture and heritage conservation	11	0.04%
Physical culture	2	0.01%
Education and upbringing	142	0.48%
Agriculture	2	0.01%
Fishery	0	0.00%
Religions and national minorities	6	0.02%
Insurance	3	0.01%
Chambers of economy and commerce	4	0.01%
Wholesale and retail	5,125	17.38%
Production	421	1.43%
Logistics and distribution	18	0.06%
Mail and courier services	4,338	14.71%
Tourism	15	0.05%
Waste management	6	0.02%
Hotels, restaurants, catering	295	1.00%
Media	8,339	28.28%
Other services	118	0.40%
Natural persons	2,464	8.36%
Total	29,483	100.00%

Table 1. Incidents handled by CERT 2021, broken down into economic sectors.

Incident types	Number of incidents	%
I. Offensive and illegal content	311	1.05%
Spam	262	0.89%
Discrediting, offending	9	0.03%
Child pornography, violence	4	0.01%
Unclassified	36	0.12%
II. Malware	2,847	9.66%
Virus	1	0.00%
Network worm	0	0.00%
Trojan horse	9	0.03%
Spyware	0	0.00%
Dialer	0	0.00%
Rootkit	1	0.00%
Unclassified	2,836	9.62%
III. Information gathering	27	0.09%
Scanning	19	0.06%
Sniffing	0	0.00%
Social engineering	3	0.01%
Unclassified	5	0.02%
IV. Break-in attempts	127	0.43%
Exploiting known vulnerabilities	2	0.01%
Unauthorised login attempts	15	0.05%
New attack signature	0	0.00%
Unclassified	110	0.37%
V. Break-ins	247	0.84%
Privileged account compromise	6	0.02%

Unprivileged account compromise	118	0.40%
Application compromise	6	0.02%
Bot	2	0.01%
Unclassified	115	0.39%
VI. Resource availability	148	0.50%
Denial of Service (DoS)	6	0.02%
Distributed Denial of Service (DDoS)	74	0.25%
Computer sabotage	1	0.00%
Outage (no malice)	53	0.18%
Unclassified	14	0.05%
VII. Attack on information safety	55	0.19%
Unauthorised access to information	33	0.11%
Unauthorised modification of information	3	0.01%
Unclassified	19	0.06%
VIII. Computer fraud	25,472	86.40%
Unauthorised use of resources	3	0.01%
Copyright breach	1	0.00%
Masquerade (identity theft, spoofing)	12	0.04%
Phishing	22,575	76.57%
Unclassified	2,881	9.77%
IX. Vulnerable services	216	0.73%
Open sites vulnerable to abuse	53	0.18%
Unclassified	163	0.55%
X. Other	33	0.11%
Total	29,483	100.00%

Table 2 .Incidents handled by CERT 2021, broken down into categories according to the eCSIRT.net mkVI taxonomy¹.

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

Warning List

In March 2021, the CERT Polska Warning List including reported hazardous sites that had been operating for one year. This list of domains is free-

of-charge and is used by telecom operators, administrators and individual users alike to improve network security by blocking known domains used for phishing and financial theft.



Uwaga! Ta strona stanowi zagrożenie

Może ona wyciągnąć dane osobowe, dane uwierzytelniające do kont bankowych lub serwisów społecznościowych. W trosce o Twoje bezpieczeństwo dostawca internetu powstrzymał próbę ataku poprzez tę stronę.

Przypominamy:



Dokładnie sprawdzaj adres i wygląd strony, na której podajesz dane logowania, dane osobowe czy karty płatniczej.



Nie działaj pod presją czasu, uważaj na wszelkie wiadomości, które skłaniają do działania natychmiast.



Weryfikuj źródło informacji zanim podejmiesz działania na jej podstawie lub ją powielisz.



Nie jesteś pewien czy dana wiadomość jest prawdziwa? **Skontaktuj się** z rzekomym nadawcą innym znanym kanałem i/lub poszukaj potwierdzenia informacji w innych źródłach.



Zgłaszaj do CERT Polska każdą podejrzaną stronę, a także wiadomości email i SMSy, które mogą wyciągnąć dane. Formularz znajdziesz na stronie <https://incydent.cert.pl>.

Oficjalne informacje i komunikaty na temat koronawirusa znajdziesz na stronie: <https://gov.pl/koronawirus>.

Lista ostrzeżeń zawierająca wykaz witryn stanowiących zagrożenie znajduje się na stronie https://cert.pl/ostrzezenia_phishing.

Fig. 1. Message indicating that a site has been blocked by the Warning List. The site appearance may differ depending on a given telecoms operator.

The easiest way to start using the List is to add it, in the adblock format,² to the uBlock Origin extension, in the browser installed. For more information on such integration, see the subpage devoted to the List³.

In response to ever-intensifying Flubot malware campaigns, in April, we deployed a new method of reporting suspicious domains, i.e. via text mes-

sages⁴. Thus, if a user receives a text message containing a malicious URL address, they can report it immediately by forwarding the entire message to a dedicated telephone number, i.e. **+48 799 448 084**. We analyse such messages, and the domains attached are entered in the Warning List, provided they are actually used for fraudulent operations.

2. https://hole.cert.pl/domains/domains_adblock.txt

3. https://cert.pl/en/posts/2020/03/malicious_domains/

4. https://twitter.com/CERT_Polska/status/1385588498883874817



Dziś udostępniliśmy nowy sposób zgłaszania nam wiadomości SMS wyłudzających pieniądze. Wystarczy przekazać nam treść otrzymanej wiadomości na numer 799-448-084. Nasi analitycy zdecydują o dopisaniu podejrzanej domeny do naszej listy ostrzeżeń.

[Translate Tweet](#)

3:36 pm · 23 Apr 2021 · TweetDeck

107 Retweets 13 Quote Tweets 220 Likes



Fig. 2. Indications informing about the deployment of a service facilitating suspicious content reporting via text messages.

By the end of the year, almost **42,000 malicious domains were entered in the list, 33,000 already in 2021**. Each blocked domain was thoroughly verified by our staff before being considered malicious, thus creating one of the most reliable sources of this type of data that can be processed automatically.

As a result of the increasing list deployment degree in various content filtering systems, **only in 2021, we prevented around 4 million attempts to enter sites designated as phishing sites.**

Phishing campaigns aimed at obtaining Facebook login data were most common (7785 domains). It was the most widespread form of phishing in 2020; however, what we observed is over three-fold increase in 2021. The most common scheme used was to trick people into disclosing their login details in order to supposedly verify their age for watching a video depicting a drastic or shocking event. We presented selected examples of such attacks in warnings published on 10 May⁵ and 11 October 2021⁶.

5. https://twitter.com/CERT_Polska/status/1391757158551805955

6. https://twitter.com/CERT_Polska/status/1447547559245930497



Fig. 3. Site featuring fake information related to vaccinations. In order to view the video attached, users must first enter their account login details to verify their age. Cybercriminals use the data obtained in this way to perform further phishing-related activities.

We are glad that more companies and individual users make use of our Warning List related to hazardous sites. We have already observed a steady, upward trend. Thus we hope that, next year, we will be able to extend the list coverage even further and, as a result, protect more Polish users.

Please report incidents at: <https://incydent.cert.pl/> and forward malicious text messages to **+48 799 448 084**, as our effective operation hinges mostly on users' notifications.

#BezpiecznyPrzemysł (Safe Industry)

In 2021, we continued our #BezpiecznyPrzemysł (Safe Industry) campaign, within the framework of which we propagate enhancement of the cybersecurity level of the Polish industrial infrastructure. For this purpose, we look for devices accessible from the Internet, such as PLC controllers or control panels (HMI). Next we contact their owners and advise on how to secure them. This year, we focused mainly on developing internal automation tools and looking for new vulnerabilities in hardware commonly used in Poland.

During the year, we acted on numerous cases in which it was possible to remotely take complete control of an industrial process. The most interesting ones include:

- 6 water purification plants;
- 4 water treatment stations (see Fig. 4);
- 1 intermediate sewage pumping station;
- 1 small hydroelectric power plant;
- central heating systems in a flight control tower;
- numerous building automation systems in shopping centres;
- 1 HVAC system in a church (Fig. 5).

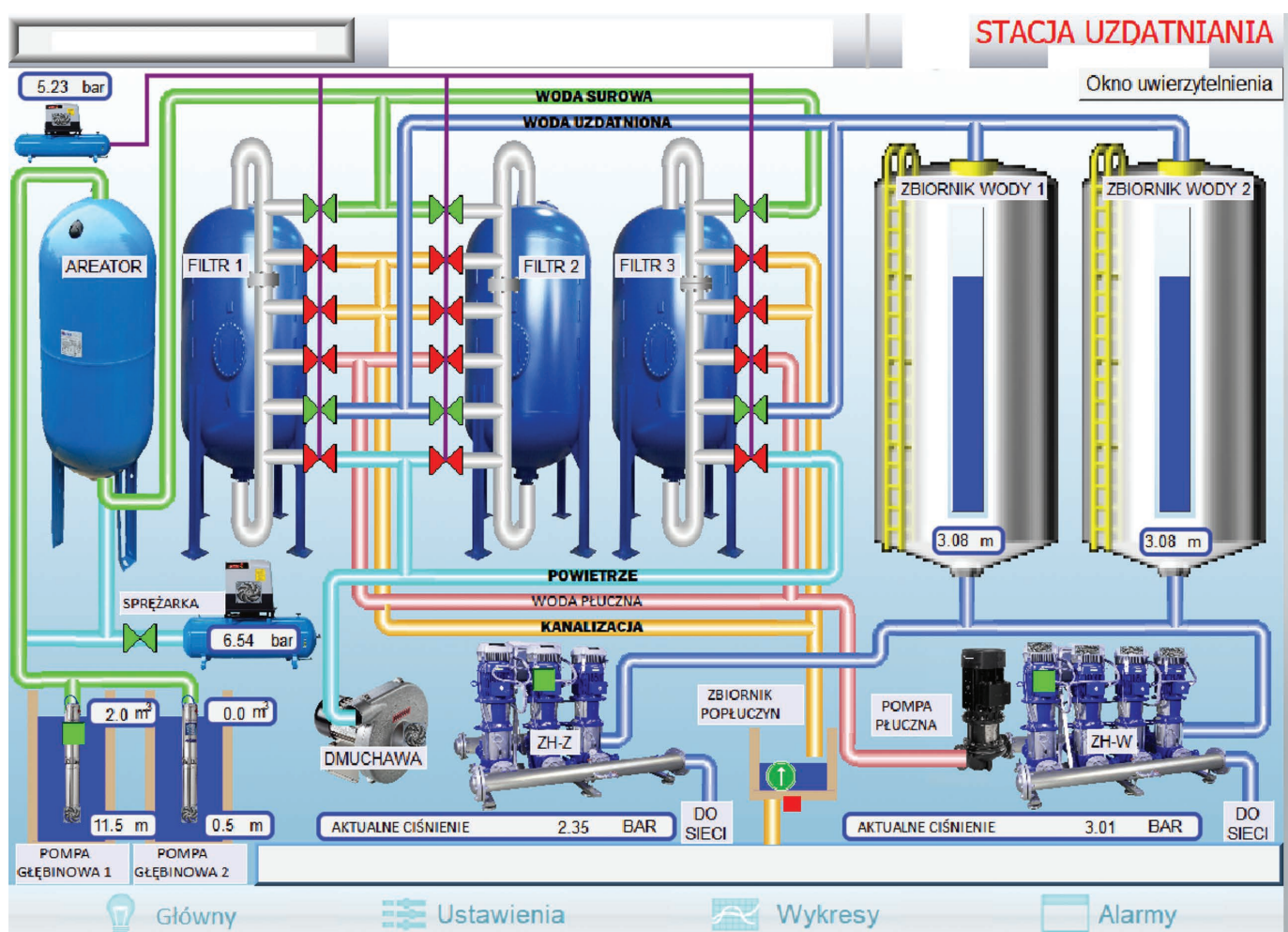


Fig. 4. Water treatment station operator's panel available on-line.

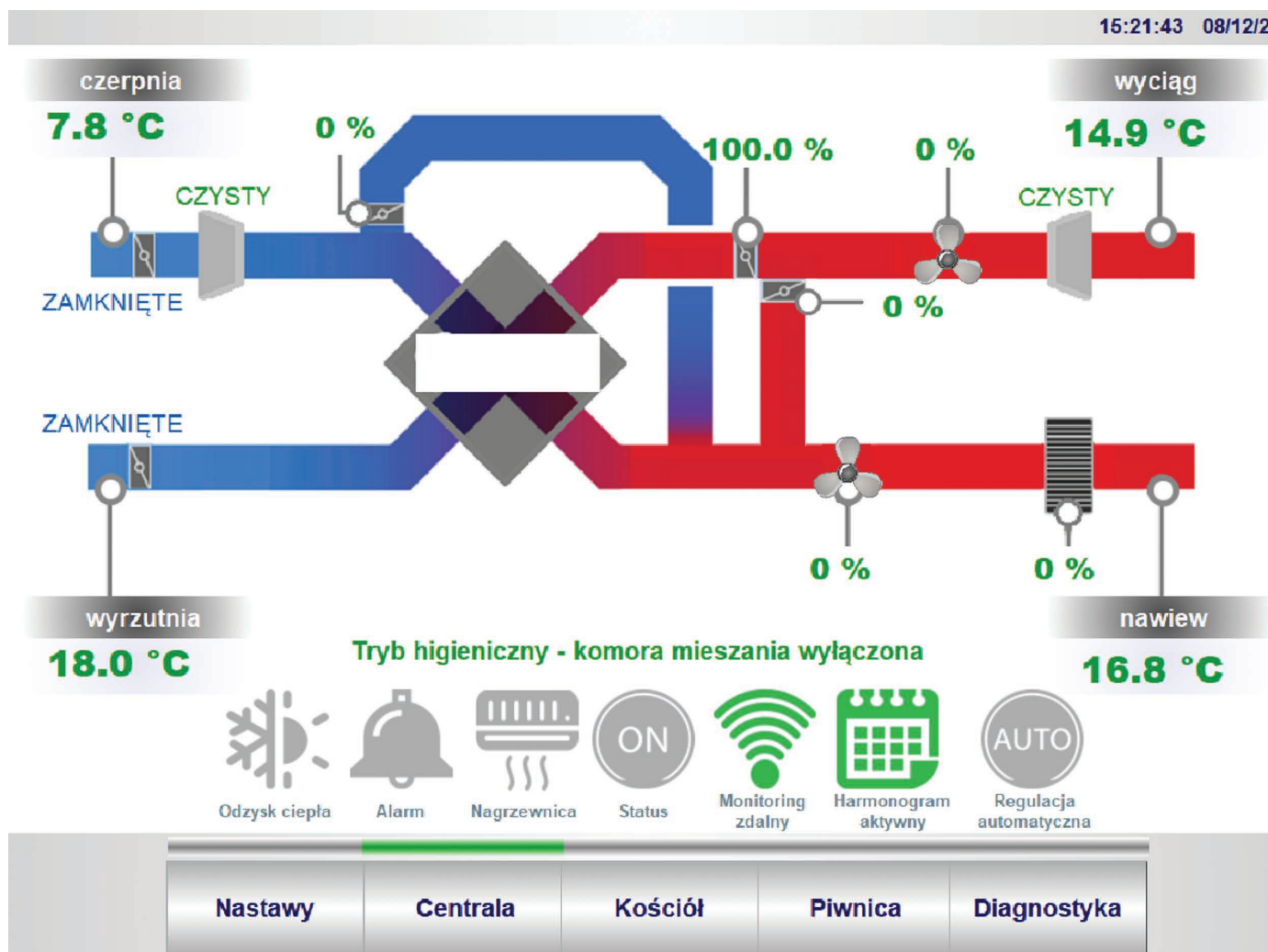


Fig. 5. HVAC system control panel available on-line.

As a result of searching for new vulnerabilities, we obtained the ability to remotely execute code on as many as two devices acting as a central HMI in small plants.

- 3 CVE (CVE-2021-27446, CVE-2021-27444, CVE-2021-27442) in the **Weintek EasyWeb cMT** software, including a critical vulnerability (CVSS 10.0) facilitating remote code execution without any authorisation⁷;
- 2 CVE (CVE-2021-43931, CVE-2021-43936) in the **Distributed Data Systems WebHMI** software, including a critical vulnerability (CVSS 10.0) facilitating remote code execution without any authorisation⁸.

All vulnerabilities were reported through a responsible bug disclosure process, in cooperation with manufacturers. In each case, we also provided warnings and recommendations through the cybersecurity authorities competent for the sectors concerned, as soon as the problem was detected. See Fig. 6 for an example of such a warning.

7. <https://www.cisa.gov/uscert/ics/advisories/icsa-21-082-01>

8. <https://www.cisa.gov/uscert/ics/advisories/icsa-21-336-03>

Ostrzeżenie o podatności w panelach operatorskich (HMI) firmy Weintek

Szanowni Państwo,

wypełniając obowiązki CSIRT NASK, a także działając w porozumieniu z organem właściwym ds. cyberbezpieczeństwa, informujemy o problemach dotyczących bezpieczeństwa **paneli operatorskich HMI firmy Weintek**. Przygotowaliśmy rekomendacje, mające podnieść poziom bezpieczeństwa tych urządzeń.

Co zostało wykryte

CSIRT NASK w ramach własnych badań wykrył krytyczną podatność w panelach HMI **Weintek z serii cMT**. Wg. naszych informacji podatne są wszystkie modele z tej serii we wszystkich dostępnych wersjach firmware'u. Na podatność nie istnieje jeszcze łatka producenta. Jednocześnie natrafiliśmy na liczne przypadki dostępu tego systemu bezpośrednio z Internetu, w szczególności w sektorze wodno-kanalizacyjnym.

Zagrożenia

Wykryta podatność pozwala na zdalne wykonanie kodu na poziomie systemu operacyjnego, bez

Fig. 6. Fragment of a warning sent to individual sectors following detection of a new vulnerability in Weintek panels.

SECURE conference

In 2021, we celebrated two important jubilees. We celebrated the 25th anniversary of establishing the CERT Polska team and the 25th edition of the SECURE conference. For the last 25 years, we have been building a community working towards ICT security, and the SECURE conferences present a unique opportunity to share our expertise and experience in this area.

On 15 June, the fourth edition of the SECURE Early Bird conference took place. Stewart Garrick from the Shadowserver foundation was our special guest, and he told us about cooperation with CERT Polska aimed at enhancing users' security on a national level. On the other hand, CERT Polska specialists presented issues they deal with on a daily basis. The topics discussed included the list of malicious domains published by us (Mateusz Szymaniec), problems encountered in reporting bugs in industrial systems (Marcin Dudek) and the use of seized websites and social media accounts for disinformation purposes (Marcin Dudek).

The main SECURE conference took place on 19–20 October. As in the previous year, the conference 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 started with a panel discussion summarising the 25 years of our team's operation. Apart from Przemek Jaroszewski, former CERT Polska managers, i.e. Krzysztof Silicki, Mirosław Maj and Piotr Kijewski, also participated in this discussion.

As usual, the content-related level of presentations left nothing to be desired. The speakers included: Adam Haertle giving a presentation on cybercriminals' slip-ups, Alexandre Dulaunoy and Jean-Louis Huynen from CIRCL presenting a method of tracking cryptocurrency-mining botnets, and the Minister Janusz Cieszyński, who discussed the amendment to the Act on the National Cybersecurity System. We also hosted Piotr Borkowski,

who described the method of Red Team building and operation, Kamil Dudek giving a presentation on methods for bypassing the Secure Boot mechanism, and Grzegorz Tworek speaking about methods for cheating digital signature functionalities in Windows.

For clips featuring the conference events, visit YouTube⁹. News can be followed on the SECURE conference website, as well as on Twitter¹¹, Facebook¹² and LinkedIn¹³ accounts.

Exercises and competitions

CERT Polska regularly participates in national and international exercises testing both technical threat analysis skills and incident response procedures. International exercises organised by the global cybersecurity industry in 2021 served as an attempt to find its feet in a totally new reality. Following a year-long break caused by the Covid pandemic, Locked Shields and European Cyber Security Challenge series were organised. Towards the end of the year, we could also see the return of some regular international cybersecurity conferences, which in turn enables Capture The Flag competition organisers to start organising final competitions.

Locked Shields

Locked Shields is the most extensive and advanced cyber defence exercise in the world. For the last 11 years (except for 2020), it has been organised in spring by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) based in Estonia. Governments of countries financing the centre's operation, commercial entities and scientific institutions all participate in the exercises. National teams (and security teams from invited international organisations) take on the role of the "blue" teams. They act as computer incident rapid response teams which, over the course of two days of the exercise, at the request of a fictional country (Berylia, incorporated in the NATO structures), must protect a simulated IT infrastructure from attacks initiated by the "red" team. In 2021, over 2000 professionals from 30 countries participated in the exercises.

As part of a simulated military base, each "blue" team was tasked with defending 150 IT systems: from standard systems such as workstations, servers, network equipment and cloud solutions, to specialised systems such as an air defence system, LTE network and ICS systems, i.e. a power plant with a power distribution system, water treatment plant, and, for the first time, an observation satellite's ground control system. Systems defended by 22 "blue" teams were subjected to over 4,000 attacks.

The exercise structure requires each team to coordinate multiple aspects of cyber security management when faced with a hybrid conflict. Apart from securing systems and repelling attacks as part of incident response operations, the blue teams are also expected to share information through international cooperation, and participate in intertwined parallel exercise paths consisting of:

- IT forensics analysis, in which teams, during a dedicated "Capture The Flag" competition, must analyse system images received and reconstruct the course of an incident;
- mass media analysis, where the effectiveness of responding to disinformation activities in a simulated traditional and social media environment is tested;
- legal analysis, during which teams must prepare a number of legal analyses in the field of international law;
- strategic activities, in which selected crisis management processes are tested.

In 2021, the Polish team, led by the military National Cyberspace Security Center and consisting of military and civilian experts, i.e. CSIRT teams, public institutions, critical infrastructure entities and companies operating, e.g. in the banking and telecommunication sectors, took the fourth place, which was quite a feat. The first three places went to: Sweden, Finland and the Czech Republic.

In 2021, CERT Polska and NASK experts managed the operations of as many as four sub-teams within the Polish national teams:

- special systems (including ICS systems);
- web applications;
- network infrastructure;
- legal matters.

9. <https://www.youtube.com/user/CERTPolska>

10. <https://secure.edu.pl>

11. <https://twitter.com/securepl>

12. <https://www.facebook.com/Konferencja.SECURE>

13. <https://www.linkedin.com/showcase/10852603/>



Fig. 7. Certain ICS systems used in the exercise, photo: NATO CCDCOE.

European Cyber Security Challenge

After a year-long break caused by the Covid pandemic, the European Cyber Security Challenge competition, i.e. the youth European cybersecurity championship, was organised once again. Organised annually, the competition launched by the European Commission in 2013 aims to popularise cybersecurity-related issues and encourage young people to pursue a career in this area. Since 2016, the event has been organised by ENISA. A Polish team participated in it for the first time in 2018.

Before the finals, each country must select a 10-member team consisting of 5 people aged between 14 and 20 and 5 people aged between 21 and 25. During this edition of the competition, due to the fact that the event was cancelled a year ago, it was decided to exceptionally raise the age limit by one year.

Similarly to other countries, Poland organises qualifications for the national team. From the very beginning, the CERT Polska team is responsible for organisation, care for the Polish team and its participation in the European finals.

The individual CTF qualifying competition conducted between 2–4 July on the hack.cert.pl platform attracted 108 participants, 59 of whom completed at least one task. Participants strived to handle tasks in the following categories: web application security, software reverse engineering, exploiting security vulnerabilities, cryptography, computer forensics and electronics.

The Polish team comprised:

- Jakub Kądziołka (captain);
- Kacper Kluk;
- Kajetan Grzybowski;
- Jakub Wasilewski;
- Szymon Borecki;
- Krzysztof Haładyn;
- Jakub Nowak;
- Patryk Balicki;
- Grzegorz Uriasz;
- Karol Baryła.

Everybody may pit their wits against the actual contest tasks from the last-year's and current qualifications available at <https://hack.cert.pl>.

The finals were organised 28 September – 1 October in Prague. Despite the Covid pandemic, 19 national teams took part in the competition.

In the final competition, the Polish team stood on the podium for the first time, taking second place. The first and third places went to, respectively: Germany and Italy. The 2022 finals will be held in Vienna.



Fig. 8. ECSC 2021 finals in Prague, photo: NASK.

CTF scene

Capture The Flag (CTF) events are team cybersecurity competitions. They are organised by scientific institutions, governments, non-governmental organisations and CTF teams.

They can be divided as per their forms and locations. “Jeopardy” is the most popular formula for the competition, in which teams take on from a dozen to several dozen tasks of varying difficulty in several categories, i.e. web application security, reverse engineering and exploitation of detected vulnerabilities, cryptography or IT forensics

analysis. Solving a task ends with acquiring a hidden “flag”, i.e. a piece of text, which the teams exchange for points on the competition platform. The team with the most points wins. This formula is employed for European Cyber Security Challenge finals and qualifications to the Polish national team.

An “attack/defence” exercise is another formula employed for CTF competitions, in which each team receives an identical copy of an IT infrastructure on which the tasks-applications prepared by the organisers are run. The competition comprises

rounds lasting several minutes, during which each team tries to steal flags from the other teams' systems. The winner is the team which loses as few flags as possible (i.e. is able to quickly identify vulnerabilities and secure its services) and steals as many flags as possible (i.e. manages to exploit the vulnerabilities found and bypasses security measures implemented by other teams).

Before the Covid pandemic, the most prestigious competitions combined both formulas, i.e. qualifiers conducted on-line using the "jeopardy" formula and on-line finals employing the "attack/defence" formula. The latter usually took place during international cybersecurity conferences. As a result of the pandemic, most regular conferences were suspended or held on-line, which negatively affected the global CTF scene. Simultaneously, the younger teams benefited from it. As with the previous year, they took most places on the podium of the worldwide CTFTIME ranking. The American "perfect blue" took the first place, for the second year in a row. The second place was taken by the new "organizers" team consisting of members of university teams from Switzerland, Germany and Great Britain. The South Korean Super Guesser

team took the third place. Three Polish teams were present in the Top 20, i.e.: Dragon Sector, justCatTheFish and p4. Dragon Sector and p4 also organised new editions of their contests. The "Dragon CTF" competition was won by the Balsn team from Taiwan, and the pan-European team hxp won the competition organised by p4.

2021 also saw the second edition of the "Hack-a-Sat", an IT security in the space industry competition organised by the American armed forces. The "Poland Can Into Space" team consisting of p4 and Dragon Sector members participated in this competition for the second time. The Polish team won the qualification round which, similarly to the previous year, was held in the "jeopardy" formula, thus improving its result from last year (second place). This allowed them to participate in the finals, i.e. an "attack/defense" formula competition, meaning that teams must not only control their satellite, but also defend it against other teams' attacks and steal flags from systems installed on the simulated satellites of other teams. Similarly to the previous year, the "Poland Can Into Space" team came second in the final ranking.



Fig. 9. "Poland Can Into Space" team members (Dragon Sector / p4), second best team during the Hack-A-Sat 2 competition, photo: p4.

Projects

MWDB and Karton

The MWDB project is one of the CERT Polska's initiatives aimed at providing a repository for efficient exchange of information on malware. It has been continuously developed since 2018, i.e. since the public deployment of the `mwdb.cert.pl` site. Current components available to malware analysts include:

- **MWDB Core**¹⁴, i.e. open-source software constituting the core of the `mwdb.cert.pl` site. It facilitates commissioning a similar malware repository within its own infrastructure.
- **Karton**¹⁵ – a project constituting an open-source framework for building and integrating microservices that make up an automated malware analysis environment.
- Other ancillary projects, e.g. **mquery**¹⁶ (sample search accelerator based on Yara rules), **malduck**¹⁷ (library used to build modules for extraction of static configurations from samples) or **DRAKVUF Sandbox**¹⁸ described in detail in a separate article at 39.

MWDB Core project development

In 2021, intensive work was performed to supplement the MWDB Core project with additional functions. One of the activities consisting in the experimental introduction of a capability facilitating external MWDB Core site integration with `mwdb.cert.pl`. This integration makes it possible to search the repository and download objects from the remote `mwdb.cert.pl` site, from the level of the MWDB Core instance interface.

In subsequent releases, built-in MWDB Core integration with the Karton project was introduced, so that additional extension installation is not necessary to automatically spawn analyses for added samples. In addition, the administration of own instances has been made significantly easier, and it is now possible to delete any objects from the interface. For a complete list of MWDB Core modifications broken down into individual releases, visit the “Releases” tab, on the MWDB Core project Github page: <https://github.com/CERT-Polska/mwdb-core/releases>. Numerous improvements were introduced thanks to suggestions and corrections from external contributors.

27 Aug 2021

psrok1

v2.5.0

907fd10

Compare

v2.5.0

Release focused on Karton integration bugfixes and small improvements

New features and improvements:

- Added support for AWS IAM authentication for Minio (#443, thanks @alex-ilgayev!)
- Built-in Karton integration allows to bind Karton analyses that doesn't origin from MWDB (#430, #436)

Bugfixes:

- Fixed handling of escape characters contained in config field and referenced by search query (#437)
- Fixed scrollbar issues in react-ace component (#441)
- Fixed `requests` package dependency conflict (#440)

Contributors



alex-ilgayev

► Assets 2



2 people reacted

Fig. 10. Description of MWDB Core software, release v2.5.0.

14. <https://github.com/CERT-Polska/mwdb-core>

15. <https://github.com/CERT-Polska/karton>

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

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

18. <https://github.com/CERT-Polska/drakvuf-sandbox>

In order to support analysts in effective utilisation of the MWDB, we organised a series of presentations and workshops in 2021. One of them, “Build Your Own Malware Analysis Pipeline Using New Open Source Tools”, was held on 15 April as part of the FIRST Workshop Series¹⁹, and is available on the FIRST organisation’s YouTube channel, at: https://www.youtube.com/watch?v=dPwzF_hsCow. For this type of workshops we created the **kar-ton-playground** environment where you can easily set up basic projects making up MWDB and attempt to add your own integrations to it.

The MWDB platform has been developed within the framework of the AMCE and JTAN projects created within the EU Connecting Europe Facility.

Automatic classification of malware samples based on ApiVectors

In the 2020 report, (page 65²⁰), we described our experimental project related to classifying malware samples on the basis of the system APIs used by them.

The sample analysis process step consists in running it in our DRAKVUF Sandbox²¹ tool, from which we obtain several to several hundred (and even several thousand, in extreme cases) memory dumps. Next, these dumps are subjected to static detection of Windows API function calls in the binary code of the application tested, which is contained in them. To this end, we use the ApiScout²² tool designed by Daniel Plohmann.

One of the more compact outputs provided by ApiScout consists of binary vectors with a length of 1024, in which each bit corresponds to one or more “interesting” (particularly from the point of view of reverse engineering) functions ensuring similar operation. As a result, we have obtained an ApiVector whose example visualisation is presented in Fig. 11.

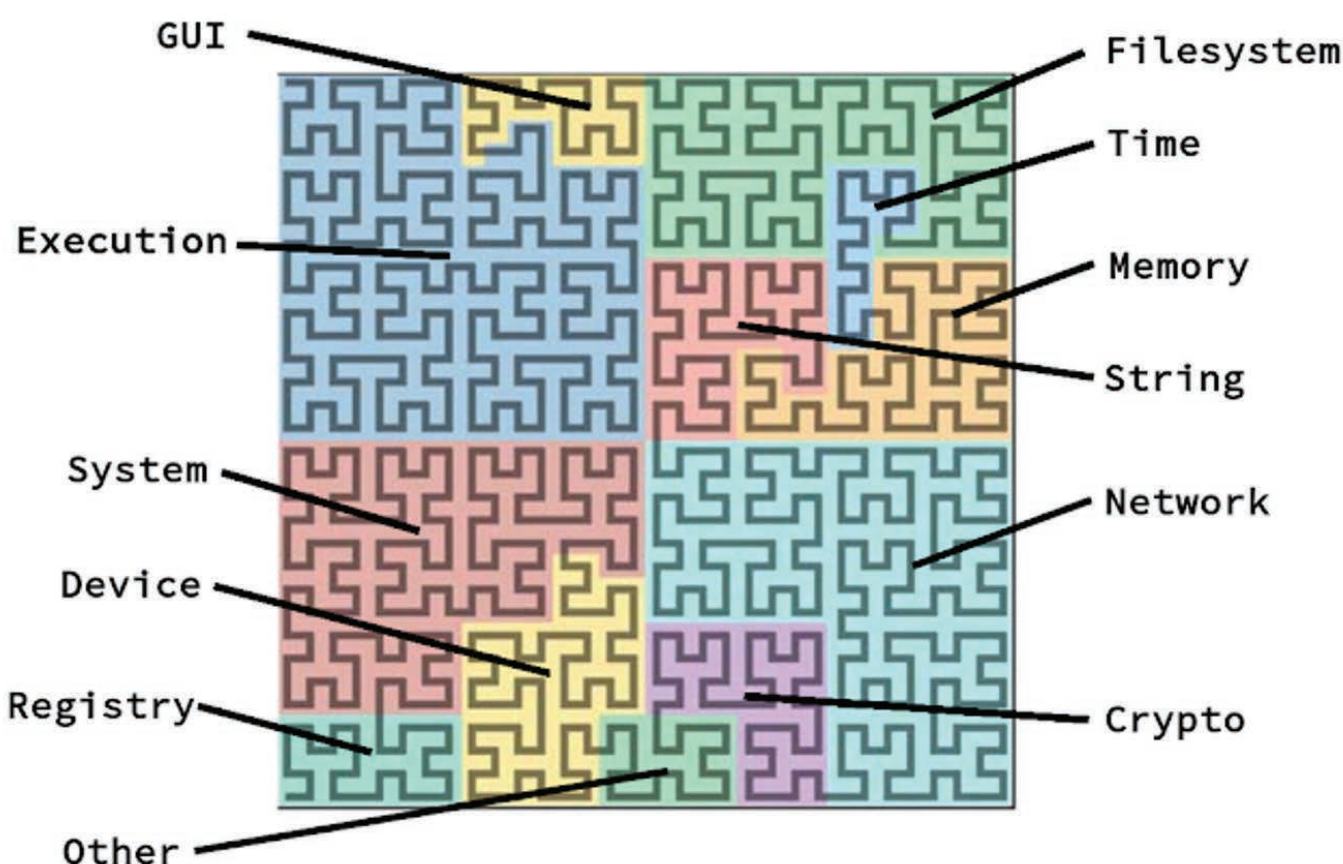


Fig. 11. Graphic representation of ApiVector (ApiQR) using a Hilbert curve, as divided into semantic bits²³.

19. <https://www.first.org/events/training/ws-mar-apr2021/>
20. https://cert.pl/en/uploads/docs/Report_CP_2020.pdf#page=65
21. <https://github.com/CERT-Polska/drakvuf-sandbox>
22. <https://github.com/danielplohmann/apiscout>
23. <http://byte-atlas.blogspot.com/2018/04/apivectors.html>

The resulting ApiVectors are then used to assign samples to known malware families.

In 2021, the project was developed further. The starting point was the conclusion, from the previous year, regarding the superiority of the classification method at the level of individual memory dumps (i.e. omitting the aggregation of ApiVectors) over classification at the level of samples.

The classification method was changed accordingly. Previously, each ApiVector obtained from a memory dump was compared to that in the ApiVector included in the supervised model, which have malware family names assigned to them, and matched to all those above a certain fixed similarity threshold (degree of similarity is calculated from the Jaccard index²⁴). Following the change introduced, only the single most similar ApiVector from the model is selected (or possibly several ApiVectors if there is a tie). The structure and the model creation method remain unchanged. Moreover, the corresponding similarity value is also stored along with the dump classification. At this point, the similarity threshold is no longer necessary, so we decided to dispense with it altogether, in order to retain as much information as possible, since the process of selecting the most relevant ones and choosing the appropriate threshold can be run by an analyst at a later stage.

The inclusion of an additional manually created model was also implemented in the automatic classification mechanism. This makes it easier to manage model elements added automatically.

In order for the ApiScout to operate flawlessly, a database of function offsets exported by libraries from the Windows API is necessary, which also applies to memory addresses where the libraries

themselves are loaded. We generate such a database only once for a given guest VM image. We call it a static profile. Since such a profile is generated on a running system, it takes into account the ASLR mechanism impact, but unfortunately not to the full extent, as some libraries may be loaded to different addresses for each running process. Due to this, certain ASLR offsets in the static profile become invalid, which makes it impossible for ApiScout to determine the real addresses of functions from libraries corresponding to these offsets, and consequently to detect calls of such functions in memory dumps. Therefore, it was necessary to collect the library loading addresses for each process separately, while still running the sample in DRAKVUF Sandbox. These addresses would then be combined with the static profile to create profiles dedicated to individual processes. We call them dynamic profiles. In 2021, they were implemented in our classifier, making it possible to detect Windows API function calls that previously could have not been detected.

In relation to the above-mentioned improvement, we also automated the process of the static profile collection from the guest VM, as previously the profile was generated manually using an additional tool provided together with ApiScout²⁵. The implementation based on this tool has been built into DRAKVUF Sandbox. The way of handling the new method of providing static profiles was not completed on the classifier side, as that is planned for 2022.

A new, more advanced user interface was also created to present classification results. It was designed as an MWDB plug-in to be implemented for production in 2022.

24. https://pl.wikipedia.org/wiki/Indeks_Jaccarda

25. https://github.com/danielplohmann/apiscout/tree/master/apiscout/db_builder

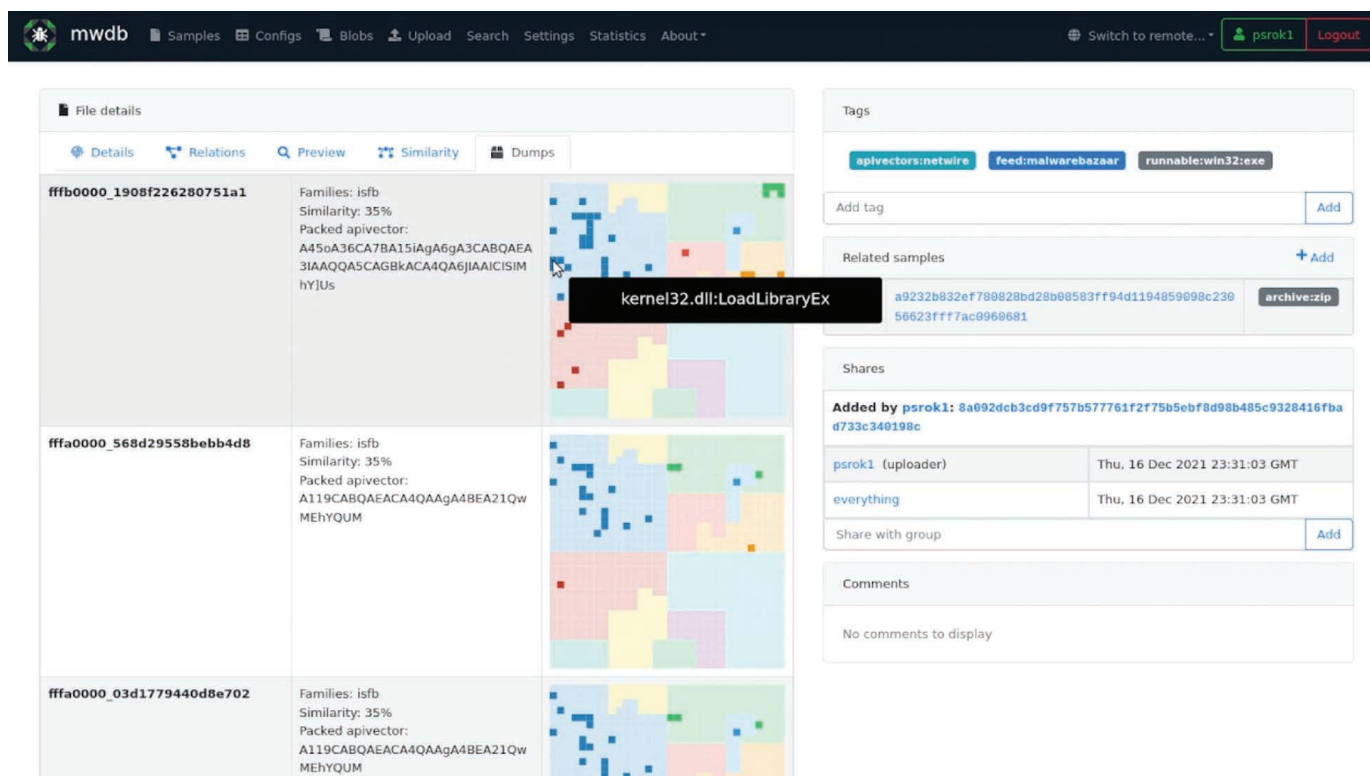


Fig. 12. Example view of the new user interface.

The classification system is based on open-source components designed by CERT Polska, including: task management system (**Karton**), MWDB client library (**mwdblib**)²⁶, and a library supporting the malware analysis process (**Malduck**). The system is developed as part of the SPARTA project, i.e. the T-SHARK sub-programme, for large-scale malware analysis purposes.

mwdb.cert.pl statistics

In 2021, mwdb.cert.pl enabled us to:

- analyse a total of 368,000 malware samples;
- obtain 19,000 static configurations;
- register 188 accounts for malware analysts community. In total, the mwdb.cert.pl platform already has 842 users.

Family name	Number of executable files	Number of unique configurations
Mirai	14,315	3,087
Agent Tesla	11,540	4,311
Formbook (XLoader)	9,191	1,380
Lokibot	3,409	1,227
Sodinokibi	2,763	1,947
Raccoon	2,314	352
QBot	2,212	70
Cobalt Strike	1,656	531
Emotet	1,627	27
Alien RAT	1,502	894

Table 3. Ten most popular malware families according to the number of samples recognised by the mwdb.cert.pl site in 2021.

26. <https://github.com/CERT-Polska/mwdblib>

CERT.PL MWDB

Top detections by CERT.PL MWDB for malware samples on MalwareBazaar.

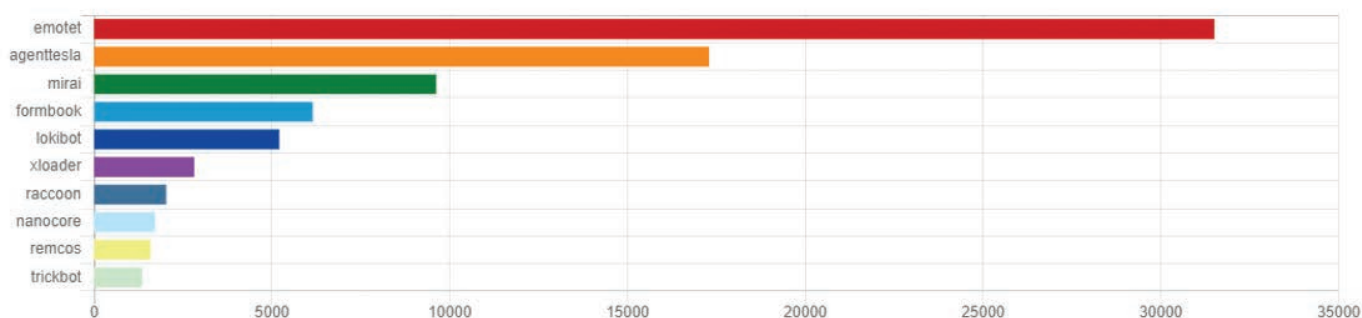


Fig. 13. Total statistics of malware families detected by mwdb.cert.pl, on the basis of samples added to the MalwareBazaar site²⁷.

The above results were achieved thanks to the significant participation of the community of malware analysts, both those who provide samples for the mwdb.cert.pl site and users of the MWDB Core platform who share valuable suggestions and improvements.

DRAKVUF Sandbox

The DRAKVUF Sandbox²⁸ project was made public at the beginning of 2020. Its goal is to create a system for malware analysis, based on the DRAKVUF²⁹ system. For more information on the project and its development in 2020, see page 71 of our 2020 report³⁰.

In 2021, the sandbox was further developed. This consisted of 197 pull requests included in the repository, the vast majority of which were enhancements to existing sandbox capabilities and documentation. New features include:

- pulling TLS keys from a guest VM to be loaded to Wireshark for network traffic decryption³¹;
- *drakplayground*³² – an environment facilitating quick setting up and interacting with a test VM, also useful for modifying the target snapshot³³;

- generating a Windows API profile for the ApiScout tool³⁴ (for more information, see page 36);
- implementation of an infrastructure for testing, including regression testing to allow translation into greater stability for subsequent releases³⁵.

DRAKVUF project development in 2021

As in previous years, as part of the sandbox development process, our team also supported development of the base project itself, i.e. DRAKVUF. We fixed numerous bugs and made improvements³⁶, e.g. implemented protection against the malware use of the API-Hammering technique³⁷.

However, the most extensive DRAKVUF modifications were introduced, with participation of CERT Polska specialists, in relation to the participation in the Google Summer of Code programme.

Google Summer of Code

Google Summer of Code (GSoC)³⁸ is a programme focused on attracting new contributors to the open-source community. Participants are expected to work on a project for several months under the guidance of mentors from a selected open-source organisation.

Potential participants contact the mentoring organisations they wish to work with. Then they draw up a project draft based on an idea published

27. <https://bazaar.abuse.ch/statistics/>

28. <https://github.com/CERT-Polska/drakvuf-sandbox>

29. <https://github.com/tklengyel/drakvuf>

30. https://cert.pl/en/uploads/docs/Report_CP_2020.pdf

31. <https://github.com/CERT-Polska/drakvuf-sandbox/pull/392>

32. <https://github.com/CERT-Polska/drakvuf-sandbox/pull/435>

33. https://drakvuf-sandbox.readthedocs.io/en/latest/usage/managing_snapshots.html#snapshot-modification

34. <https://github.com/danielplohmann/apiscout>

35. https://drakvuf-sandbox.readthedocs.io/en/v0.18.1/regression_testing.html

36. <https://github.com/CERT-Polska/drakvuf-sandbox/releases/tag/v0.15.0-p2>

37. <https://github.com/tklengyel/drakvuf/pull/1114>

38. <https://summerofcode.withgoogle.com>

by the organisation. Once approved, they spend several weeks getting to know the community and existing code, and defining milestones in collaboration with the mentors. As a follow-up, they spend the next 12 weeks writing code for the project.

Since 2005, the Google Summer of Code programme has brought together over 18,000 new open software contributors from 112 countries and over 17,000 mentors from 118 countries. As a result, over 40 million lines of code has been written for 746 open-source organisations.

CERT Polska participates in GSoC

In 2021, the CERT Polska team participated in a programme run by the HoneyNet Project^{39 40} organisation, which resulted in the start of cooperation with two students.

The outcome was the implementation of two DRAKVUF project improvements described in articles published by guest authors on our website.

Linux Injector for automated malware analysis⁴¹

Contributor: Manorit Chawdhry

The objective of the project was to create a Linux injector for DRAKVUF, i.e. a tool that can inject shellcode and write and read Linux files from a guest VM. Such capabilities make it possible to inject a malware sample into a guest machine, run that sample, and retrieve all the files that were written to disk as a result of such a run.

DRAKVUF had already had a stable injector implemented for Windows. Its Linux equivalent also existed, but it was unstable and relied on fixed offsets within the glibc library, which actually vary across releases. In the new approach, the author decided to use the Linux system call interface directly, which was possible because this interface is stable across Linux kernel versions.

For the duration of GSoC, three methods were implemented in the Linux injector:

1. *shellcode* – injects the specified machine code into a selected process and runs it;
2. *writefile* – copies a file from the host to the guest VM. From an automated malware analysis perspective, it is mainly used to inject a sample;

3. *readfile* – copies a file from the guest VM to the host. This is particularly useful when malware operates in multiple stages – with this method we can obtain a file that it has written to disk.

After GSoC was over, the Linux injector was supplemented with the *execproc* method that runs a program on the guest VM using *vfork* and *execve* system calls. From that point on, the injector was ready to be used for automatic analysis of Linux malware

The whole Linux injector code is available in the DRAKVUF repository, at GitHub⁴².

HID simulation for DRAKVUF⁴³

Contributor: Jan Gruber

The objective of the project was to create in DRAKVUF a mechanism for simulating human interaction with a system, the artificiality of which would be undetectable. This is intended to deceive malware and induce it to reveal its true behaviour.

It was implemented as a DRAKVUF plug-in called *hidsim* (i.e. Human Interface Device simulator, i.e. HID simulator).

This plug-in provides three functionalities:

1. playback of previously recorded HID events;
2. performing random, human-like mouse movements;
3. autonomous clicking of buttons in windows appearing on the screen (only in Windows 7).

An additional tool called *hiddump* was implemented to record event sequence templates. It is used to capture HID events in Linux, and saving relative and normalised versions of such events in a binary file.

During the project, the DRAKVUF repository was supplemented with approximately 3200 lines of code and 700 lines of comments in ten pull requests.

Apart from the above-mentioned contributions to DRAKVUF project development, two auxiliary projects were created:

- *ansible-drakvuf*⁴⁴ – automation in Ansible to implement DRAKVUF in a selected host;
- *vmi-reconstruct-gui*⁴⁵ – a tool used to reconstruct the Windows 7 system GUI run on

39. <https://www.honeynet.org/gsoc/gsoc-2021/>

40. https://twitter.com/CERT_Polska_en/status/1369593756643647491

41. <https://cert.pl/en/posts/2021/08/gsoc-linux-injector/>

42. <https://github.com/tklengyel/drakvuf/tree/master/src/libinjector/linux>

43. <https://cert.pl/en/posts/2021/08/hid-simulation-for-drakvuf/>

44. <https://github.com/jgru/ansible-drakvuf>

45. <https://github.com/jgru/vmi-gui-reconstruction>

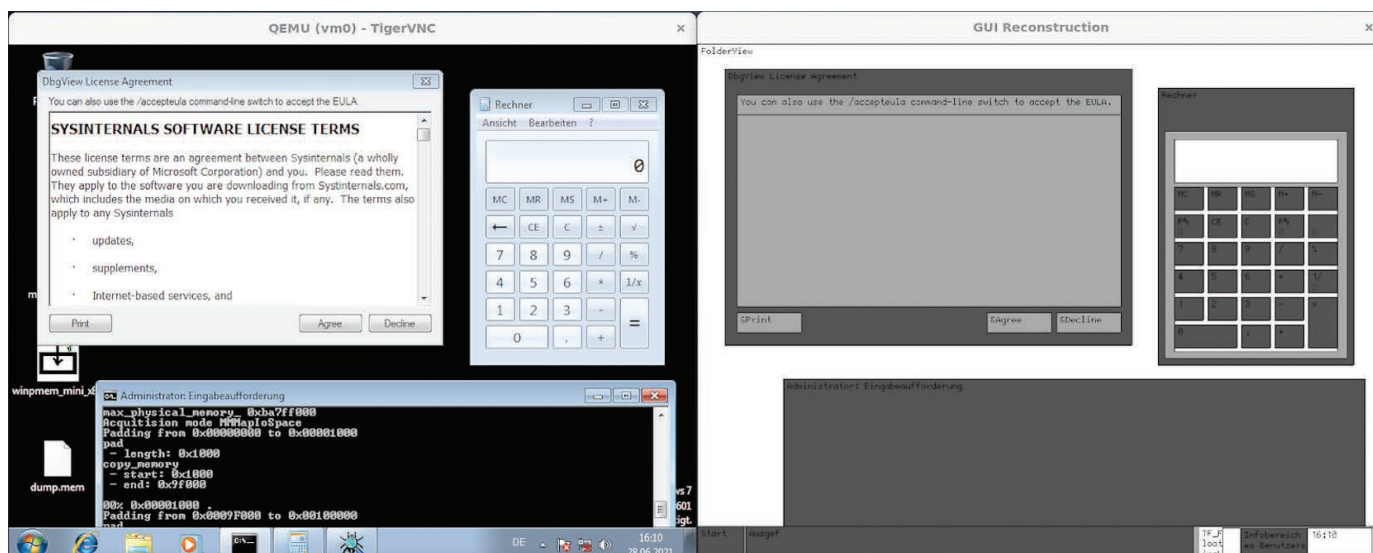


Fig. 14. Example of Windows 7 system GUI reconstruction using the vmi-reconstruct-gui⁴⁶ tool.

n6 3.0 – new release

In 2021, we released an extensive n6 system update published on open-source licence. The biggest change consisted in migrating the existing code to the latest Python 3 version. The process required numerous minor fixes and code organisation as

per the latest standards. Along with the programming language version upgrade, the main branch of the code was supplemented with a new component related to integration of a tool similar to n6, i.e. IntelMQ. From now on, it is possible to combine elements of both systems in a flexible, tailor-made manner.

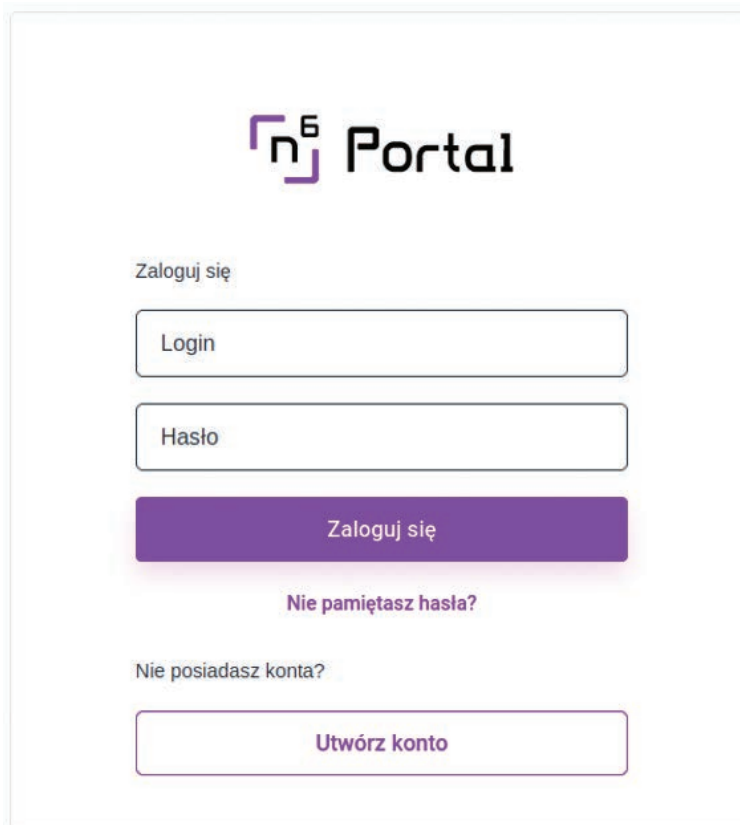


Fig. 15. Login screen for a new user interface.

46. <https://cert.pl/uploads/2021/08/hid-simulation-for-drakvuf/vmi-gui-reconstruction.png>

A completely new graphical user interface (n6 Portal) constitutes another major modification. We added another authentication layer (after entering a password) along with a second component, an interactive notification form and full support for notifications. The Portal was also provided with its own dashboard, where information related to incidents occurring in an organisation's network is automatically presented.

From now on, Portal settings can be modified via a form used to alter the organisation's configuration, as well as via user's personal settings. On the Portal, users can reset their API keys or change the second login component. Currently, the new n6 version supports TOTP with QR codes. New n6 REST API functionalities include API key authentication and minor performance-related optimisations. For the source code with related documentation, visit <https://github.com/CERT-Polska/n6>.

The development work related to n6 was co-financed under the EU Connecting Europe Facility.

MeliCERTes

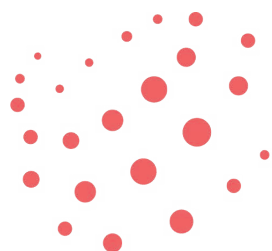
In 2020, we launched a three-year project called MeliCERTes (SMART 2018/1024) and have been continuing it with the view to developing a plat-

form for effective exchange of operational information between CSIRT teams, which facilitates detection and prevention of incidents and coordination of responses at the European level. The platform is created in response to the needs of CSIRTs Network comprising national CSIRTs of all EU Member States, as well as CERT-EU.

The project was undertaken to the order of the European Commission, and is created by a consortium controlled by NASK. Apart from CERT Polska, other project participants include CERT.at, CERT-EE, CIRCL, SK-CERT and Deloitte.

MeliCERTes is based on three main pillars:

- central services provided for the CSIRTs Network with a key role played by ENISA responsible for their maintenance;
- open-source tools to be used locally by CSIRTs and other security-related entities (for more information, see: <https://github.com/melicertes/docs>);
- services made voluntarily available by CSIRTs to the community to combat threats (e.g. MWDB maintained by our team).



melicertes

In December 2021, we completed the Advanced Threat Monitoring and Cooperation on the European and National Levels (AMCE) project implemented using the 2018-PL-IA-0168 grant obtained under the EU Connecting Europe Facility. Within the framework of the programme we developed numerous systems used for operational purposes, e.g.:

- the n6 platform;
- MWDB platform for exchange of malware-related information;
- mtracker, i.e. a botnet tracking system;
- tools supporting the maintenance of a list of warnings against malicious sites;
- in cooperation with the Shadowserver foundation: a network of honeypots developed within the framework of the SISSDEN project (<https://sisssden.eu/>).

A large amount of code resulting from the above-mentioned activities is available under open licence on our GitHub account, at: <https://github.com/CERT-Polska/>.

AMCE also included other activities, e.g. organising the European Cybersecurity Month (<https://bezpiecznymiesiac.pl/>) in Poland, or qualifications to and participation in the European Cyber Security Challenge (for more information, see page 32).

We also managed to secure another grant under the Connecting Europe Facility, and launch the Joint Threat Analysis Network project (JTAN, grant no. 2020-EU-IA-0260), during the second half of the year. In contrast to AMCE implemented individually by our team, in this case we operate a leader of a consortium associating European CSIRTs.

The main objective of JTAN is to develop tools for information retrieval (Cyber Threat Intelligence) and create mechanisms facilitating more efficient data exchange between systems used by CSIRTs. Most of the necessary work is planned for 2022–2023, and we will inform about the results on our website (<http://cert.pl/>) as well as in next annual reports.

CyberExchange

In 2021, we were able to resume our operations under the CyberExchange project, which supports exchange of expertise and experience among European CERT teams. Apart from CERT Polska, teams participating in this initiative came from Austria, Croatia, the Czech Republic, Greece, Latvia, Luxembourg, Malta, Romania and Slovakia. CZ.NIC, the Czech association CSIRT.CZ operates within, is the consortium leader.

The project is based on short internships abroad which allow specialists from national, governmental and academic response teams to learn about the characteristics of work performed by analogous institutions in other countries. Its another objective consists in establishing direct contacts being a key element of efficient international co-operation.

The COVID-19 pandemic and related restrictions made travel impossible from the first quarter of 2020. During the second half of 2021 we were able to host CERT.LV and CERT.hr representatives taking advantage of the improvement in the situation. The focus of the joint work was directed on tools supporting CSIRT operational activities and malware analysis.



Cyber Exchange



INCIDENTS AND THREATS

Ransomware

One of the most significant threats to cybersecurity in 2021 was ransomware, i.e. malware used to encrypt data in order to extort a ransom for its recovery. CERT Polska registered **124 ransomware-related incidents**. This was almost **13% more in comparison with 2020, when we handled 110 such incidents**. Considering individual sectors, the **highest activity was observed in relation to digital infrastructure entities and natural**

persons (27 incidents each) and in the **public administration** domain (18 incidents). Across all sectors, **32 incidents involving public entities were recorded**. These included **local government entities and healthcare system institutions**. In the private sector, for example, **CDProjekt fell prey** to HelloKitty malware, at the beginning of the year. The company issued a statement saying that the **encrypted data was successfully restored thanks to maintained backups**.

Number of incidents recorder, broken down into sectors

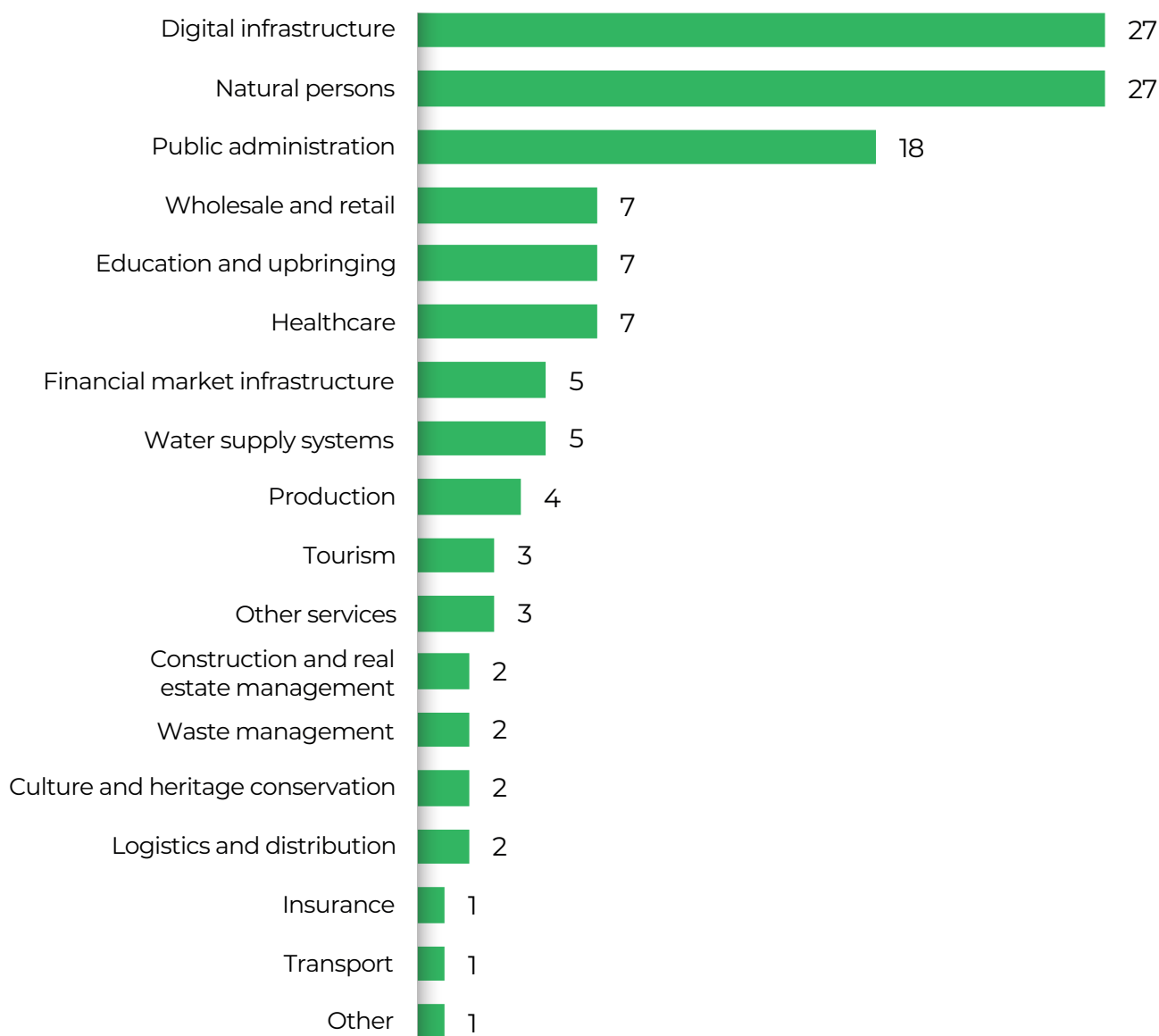


Chart 1. Number of incidents recorded, broken down into sectors.

Major threats

Two malware families are responsible for the vast majority of ransomware incidents we observed: **REvil/Sodinokibi** and **Phobos** (36 and 25 recorded

incidents respectively). Other typically present families included: **Lockbit 2.0**, **STOP/DJVU**, **Makop**, **QLocker** and **Avaddon**.

Number of incidents recorded, broken down into ransomware families

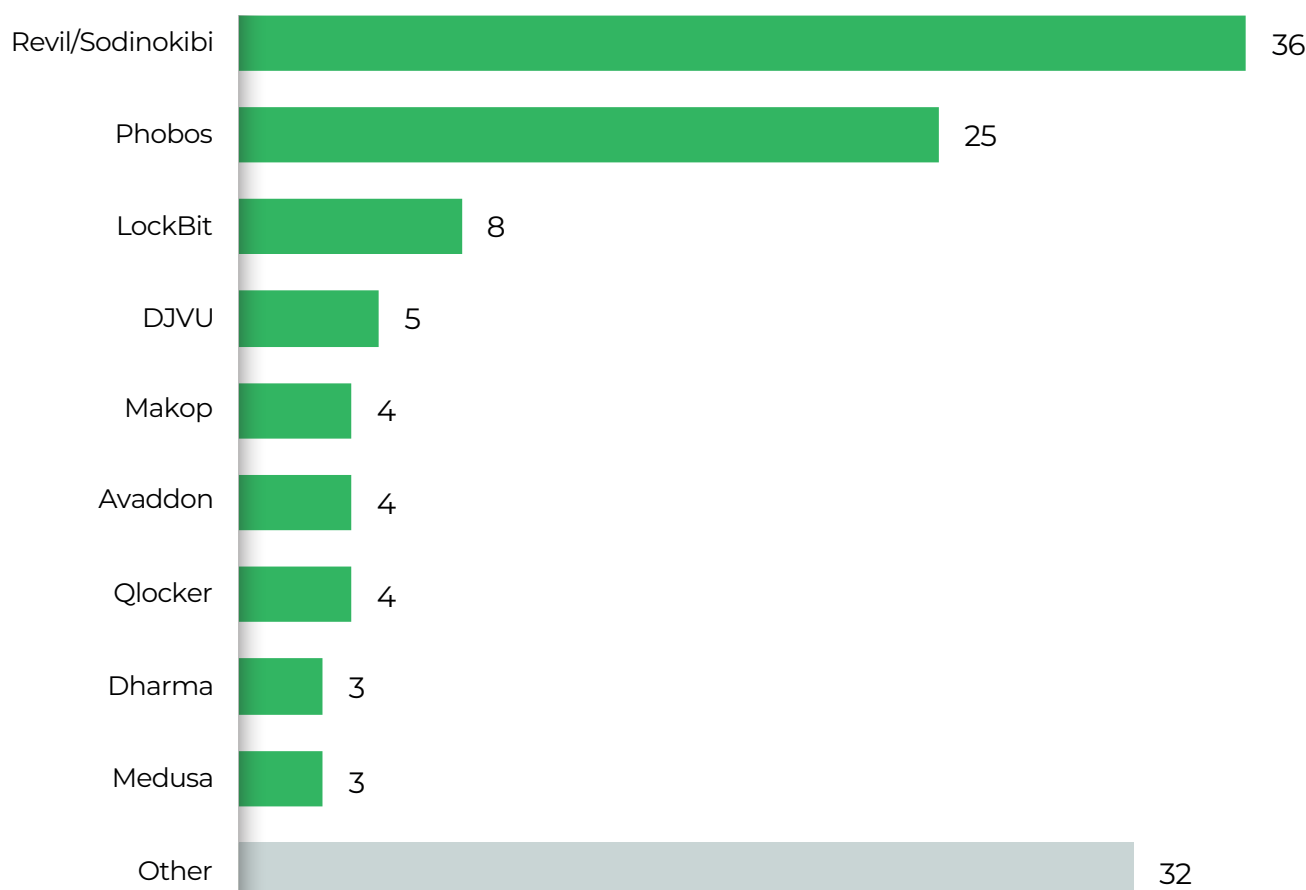


Chart 2. Number of incidents recorded, broken down into ransomware families.

Observed trends

Ransomware as a Service model development

The RaaS model became a *de facto* standard, and it is expected to continue to dominate the ransomware market in the years to come⁴⁷. It enables encryption malware authors to devote more attention to its development, delegating the execution of attacks to customers. This allows more advanced solutions and services to be deployed, such as sites that allow ransom to be negotiated, stolen data to be made public or 24/7 support for attackers.

Multiple extortions

Cybercriminals seek to maximise their profit from a single attack by demanding a ransom not only for encrypted data recovery^{48 49}. The threat of data disclosure or informing other entities, e.g. partners, shareholders, regulators or the public, about an attack is also subject to negotiation. Moreover, if the attackers manage to obtain sensitive data belonging to the organisation's customers or partners, they too may be blackmailed, and the information obtained may be used to design an attack on their equipment.

47. Sophos 2022 Threat Report <https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2022-threat-report.pdf>

48. 2021 Trends Show Increased Globalized Threat of Ransomware <https://www.cisa.gov/uscert/ncas/alerts/aa22-040a>

49. ENISA Threat Landscape 2021 <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>

Increase in damage resulting from attacks

A survey conducted at the beginning of the year by Sophos⁵⁰ showed that the average amount of losses caused by a ransomware attack nearly doubled (from less than USD 800,000 in 2020, to just over USD 1.8 million in 2021). Moreover, two-thirds of the companies that fell prey to ransomware reported a significant drop in revenues⁵¹. Thus it is also not unreasonable to see a reduction in cybersecurity insurance services, particularly those related to ransomware⁵².

Law enforcement effort mounting

Such factors as increase in damage, information theft and targeting large corporations led to intensification of law enforcement agencies' activity aimed at combating cybercrime groups employing ransomware. In some cases, international investigation teams were formed to identify and apprehend the perpetrators. This led to a number of arrests, decisions to cease operations by some groups⁵³ and partial retreat by others from attention-grabbing attacks⁵⁴.

Relevant ransomware families

REvil/Sodinokibi

The REvil software, also dubbed Sodinokibi, was one of the main threats, both in Poland and internationally⁵⁵. It was developed by the group responsible for another ransomware family - GandCrab. REvil was made available as part of the RaaS model, along with all the infrastructure used to prepare attacks, negotiate with victims and publish stolen data. Before encryption, data identified as valuable was stolen and used for double blackmail. Companies like Acer⁵⁶, Quanta Computer and Apple⁵⁷ fell prey to such attacks.

One incident exerting the most adverse effect was the attack targeted at Kaseya, whose Kaseya VSA software was used to infect almost 1500 clients⁵⁸. It was achieved using a supply-chain type attack in which malicious code was distributed along with a software update. The close cooperation of 17 countries, Europol, Eurojust and INTERPOL resulted in arresting seven people tied to the group responsible for Revil⁵⁹ ransomware attacks. Moreover, universal decryptors were successfully created, allowing recovery of data belonging to over 50,000 REvil/Sodinokibi and GandCrab attack victims. This tool is available on the No More Ransom⁶⁰ project website.

Conti

Conti is distributed using the spear-phishing technique, stolen/weak RDP credentials or vulnerable services. Tools such as TrickBot or Cobalt Strike are used first, and the ransomware itself is used once access to more machines have been obtained and information identified as sensitive has been transferred⁶¹. Data collected on the Ransomwhere⁶² project website shows that, of all ransomware families, Conti brought cybercriminals the highest profit. Back in 2021, it amounted to a dozen or so million USD. In 2022, we have witnessed a considerable information leak of information regarding the group responsible for Conti, including correspondence spanning several years and other sensitive data⁶³.

Hive

Hive ransomware extorted one of the highest ransom amounts in the history of cybercrime. In November 2021, it was used to attack the international Media Markt store network, with demands amounting to USD 240 million. The Hive model

50. The State of Ransomware 2021 <https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf>
51. Ransomware: the true cost to business, https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf
52. Insurers run from ransomware cover as losses mount <https://www.reuters.com/markets/europe/insurers-run-ransomware-cover-losses-mount-2021-11-19/>
53. ENISA Threat Landscape 2021 <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>
54. 2021 Trends Show Increased Globalized Threat of Ransomware <https://www.cisa.gov/uscert/ncas/alerts/aa22-040a>
55. IBM X-Force Threat Intelligence Index 2022 <https://www.ibm.com/security/data-breach/threat-intelligence/>
56. Computer giant Acer hit by \$50 million ransomware attack <https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/>
57. REvil gang tries to extort Apple, threatens to sell stolen blueprints <https://www.bleepingcomputer.com/news/security/revil-gang-tries-to-extort-apple-threatens-to-sell-stolen-blueprints/>
58. Kaseya: Roughly 1,500 businesses hit by REvil ransomware attack <https://www.bleepingcomputer.com/news/security/kaseya-roughly-1-500-businesses-hit-by-revil-ransomware-attack/>
59. Five affiliates to Sodinokibi/REvil unplugged <https://www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged>
60. The No More Ransom Project <https://www.nomoreransom.org>
61. Conti Ransomware <https://www.cisa.gov/uscert/ncas/alerts/aa21-265a>
62. Ransomwhere Project <https://ransomwhere.re/>
63. Conti Ransomware Group Diaries, Part I: Evasion <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/>

of operation is RaaS, stolen data is published on a site prepared by the creators, where dozens of companies are already present. Group-IB researchers managed to gain access to an administration panel used by the criminals, making public a wealth of information on the group's activities⁶⁴. Despite the fact that Hive only became active in the second half of the year, at least 355 organisations fell victim to it by mid-October.

Ransomware guidebook

We encourage you to consult the ransomware guidebook drawn up by our team. We describe steps that can be taken to prepare for this type of threat, as well as the steps you should take once an infection has been identified. The guidebook is available on the CERT Polska website, at: https://www.cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf.

Major vulnerabilities in 2021

2021 was abundant in serious vulnerabilities that were very quickly adapted and exploited by cybercriminals, particularly ransomware groups. There is a clear trend consisting in an increase in exploitation of vulnerabilities in software used by companies, e.g. Microsoft Exchange or VMware vCenter, relative to those in software used by end users, such as MS Office or a browser.

In 2021, the NVD database managed by NIST published 21,957 vulnerabilities. It constitutes a slight increase in comparison with 2020 (3,500 more). It should be noted, however, that despite this large number of reported vulnerabilities, as of the date of writing this report, only 326 were actively exploited, according to CISA⁶⁵.

The activity of criminal groups is not limited to vulnerabilities disclosed in a given year. Fig. 16 shows the vulnerabilities most commonly exploited by ransomware groups (as of October 2021). We also recommend analysing the list of vulnerabilities currently used during attacks, continuously updated by CISA: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

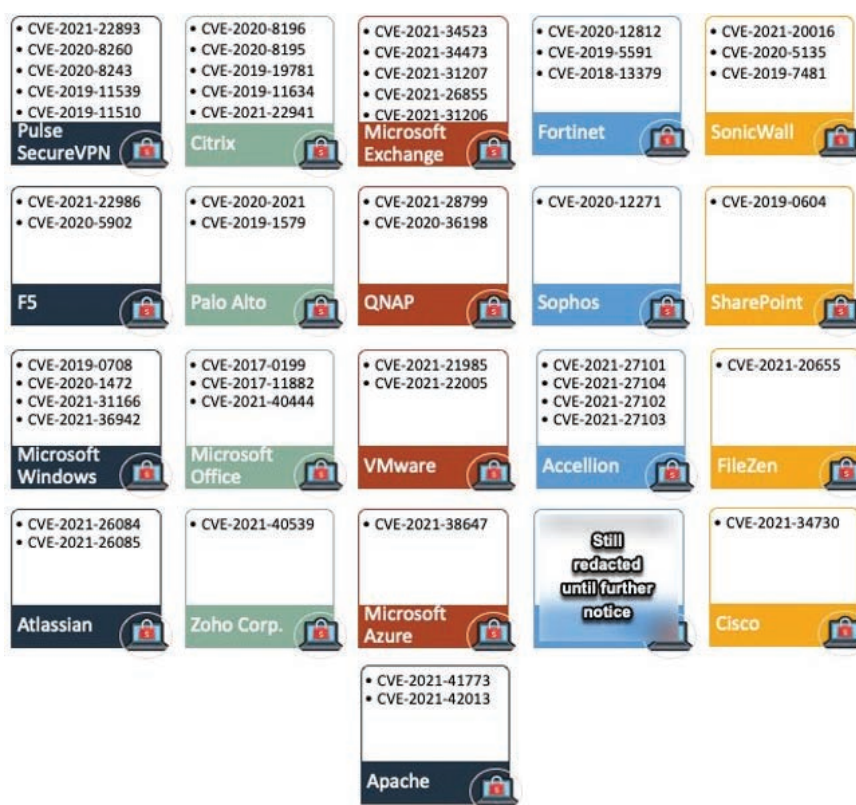


Fig. 16. Vulnerabilities most commonly exploited by ransomware in 2021⁶⁶.

64. Inside the Hive <https://blog.group-ib.com/hive>

65. Known exploited vulnerabilities catalog <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

66. <https://twitter.com/pancak3lullz/status/1447644282614161412/photo/1>

By far the most talked about vulnerability of 2021 was the Log4j library vulnerability, known as Log4Shell. Nevertheless, our observations show that the most successful attacks were caused by vulnerabilities in Microsoft Exchange, also known as ProxyLogon and ProxyShell, whose effects can still be observed. Detection of such attacks is often delayed. This is due to the fact that criminal groups resell the access they have gained, and the incident is noticed and reported only when this access is obtained by a group that monetises it, e.g. by installing ransomware.

Log4Shell

At the end of 2021, a critical vulnerability was reported worldwide concerning one of the most commonly used event logging libraries used by Java applications, i.e. Apache Log4j. Shortly after a suitable patch was released, information about further problems emerged, which eventually led to the publication of four CVEs – see Table 4.

CVE	Vulnerable Log4j versions	Description
CVE-2021-44228	2.0-beta9 do 2.14.1. Excluding 2.12.2-2.12.*	First vulnerability known as “Log4shell” Facilitates remote code execution.
CVE-2021-45046	2.0-beta9 do 2.15.0. Excluding 2.12.2-2.12.*	Vulnerability constituting a bypass of the patch deployed in version 2.15.0. Facilitates remote code execution.
CVE-2021-45105	2.0-alpha1 do 2.16.0 Excluding 2.3.1 i 2.12.3-2.12.*	Vulnerability facilitating a denial-of-service attack.
CVE-2021-44832	2.0-beta7 do 2.17.0 Excluding 2.3.2 i 2.12.4-2.12.*	Vulnerability facilitates remote code execution if the login configuration can be edited. Such a threat is very rare in itself.

Table 4. Log4j library vulnerabilities disclosed in 2021.

The main threat related with Log4Shell is the remote code execution ability, the exploitation of which (depending on the configuration) can be very simple. This is definitely the vulnerability which, in 2021, received most publicity and resulted in system patches being developed on an unprecedented scale.

As part of the measures to prevent detrimental impact of this vulnerability:

- See the website for daily updated recommended actions to be taken to address the vulnerability. They are available at the following address. <https://cert.pl/posts/2021/12/krytyczna-podatnosc-w-bibliotece-apache-log4j/>
- We sent warnings to relevant sectors via competent authorities, national-level CSIRTs, KRPM and RCB, requesting their further distribution.

- Using the list of contact persons provided in the Polish Act on the National Cybersecurity System, we delivered warnings to **2976** entities. In total, individual notifications were sent.
- We also published a warning in the S46 system.

VMware vCenter

The VMware vCenter software facilitates centralised management of the vSphere virtualisation platform. This product is very often used by larger organisations with their own server rooms. Therefore gaining access to them often means taking over most of the company’s infrastructure.

In 2021, as many as three patches for critical VMware vCenter vulnerabilities (CVE-2021-21972, CVE-2021-21985, CVE-2021-22005) were released, and later used to carry out massive attacks. Each of them allowed remote code execution without authentication.

This is a good example of how quickly such patches are analysed by attackers. In the case of two vulnerabilities (CVE-2021-21985, CVE-2021-22005), only a few days passed between the warning publication by VMware and their exploitation. Also very quickly, ready-to-use exploits were publicly available.

Although the vCenter access should be restricted to the administrative network only, a significant number of publicly available instances can be found on the Internet. **Over 300 cases in Poland.** Regarding both vulnerabilities, we informed the owners of such servers to update them immediately and recommended that they should not be accessible from the Internet.

Microsoft Exchange

Microsoft Exchange is the most popular corporate email server, used by the biggest companies in the world. By taking control of it, an attacker not only gains access to the email messages of the entire organisation, but also often has the ability to take over the domain controller.

As many as two groups of critical vulnerabilities allowing remote code execution were published in 2021: ProxyLogon and ProxyShell.

ProxyLogon

CVE-2021-26855 is the major vulnerability dubbed ProxyLogon. It allows you to bypass authentication and execute commands as an administrator in MS Exchange. Together with it, three vulnerabilities facilitating remote code execution at the operating system level using previously gained administrative access were detected (CVE-2021-26857, CVE-2021-26858, CVE-2021-27065).

Interestingly enough, the DEVCORE team which discovered this vulnerability claim that Microsoft was informed as early as in January 2021, but it took 3 more months to patch them⁶⁷. In the meantime, it appeared that the vulnerabilities had been exploited by one of the groups, i.e. APT – HAFNIUM, before the necessary patch was deployed. From then, things accelerated rapidly. Microsoft issued patches with immediate effect, and within days, examples of how to exploit the vulnerability for attacks became publicly available. Even such a short time between a patch release and appearance of public exploits for such an important component of many companies' mail servers resulted in a flurry of attacks by both APT and ransomware groups. Fig. 17 presents how the above-mentioned vulnerabilities were combined and exploited to carry out attacks.

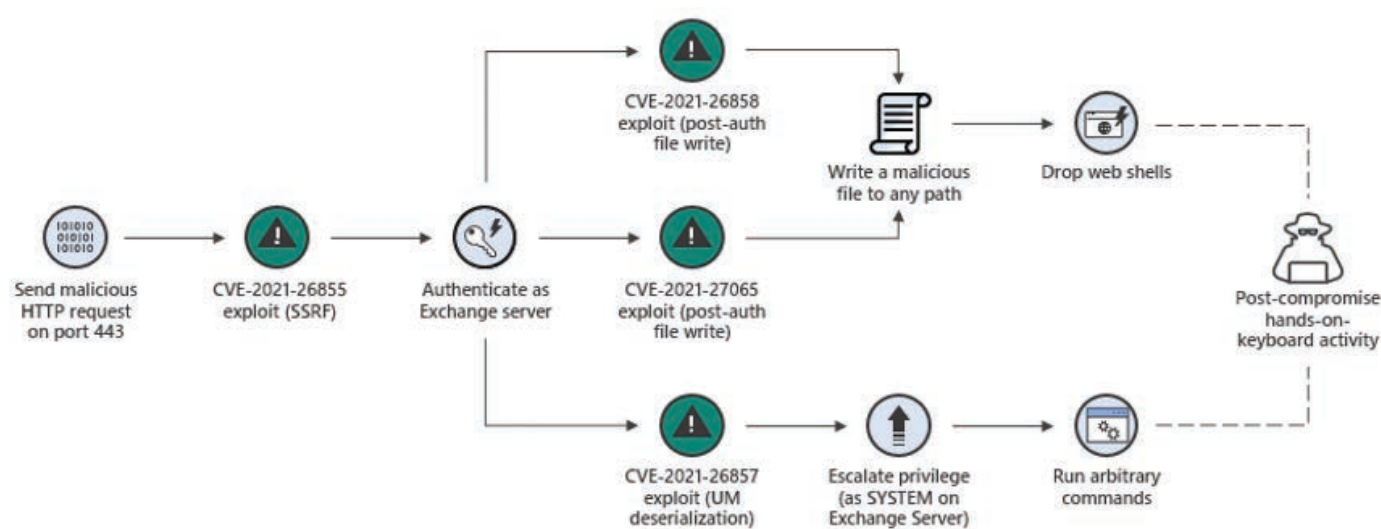


Fig. 17. Method of exploiting the ProxyLogon vulnerabilities to execute attacks⁶⁸

67. <https://proxylogon.com/>

68. Source: <https://www.microsoft.com/security/blog/2021/03/25/analyzing-attacks-taking-advantage-of-the-exchange-server-vulnerabilities/>

According to good practice, direct access to an MS Exchange login panel from the Internet should not be possible, but unfortunately this is a common bad practice. As part of our activities, seeing the seriousness of the problem, from the moment the vulnerability was disclosed, we scanned Polish IP addresses daily for possible vulnerable servers. In the following days, we also searched for web shells left by attackers within known paths. See below for some statistics from this period:

- Number of MS Exchange instances in Polish IP addresses at least once confirmed as vulnerable: **1784**.
- Number of MS Exchange instances in Polish IP addresses that were still vulnerable during the period when the vulnerability was exploited on a mass scale: **453** – very likely break-ins.
- Number of MS Exchange instances with a backdoor (web shell) installed: **159** – confirmed break-ins. The number is significantly underestimated, as only known web shell paths were scanned.
- Number of notifications sent to organisations: **975** (some organisations owned several servers).
- Direct escalation (including establishing responsible administrators by phone): approx. **100**.

ProxyShell

In August 2021, Orange Tsai, a security researcher associated with the DEVCORE team, published another set of MS Exchange vulnerabilities⁶⁹. The major one, i.e. CVE-2021-34473, made it possible to bypass authentication, and other vulnerabilities (CVE-2021-34523 and CVE-2021-31207) allowed to obtain higher-level access rights to upload a web shell. Fortunately, this time Microsoft patched the vulnerability 3 months in advance of publication, giving numerous organisations the time they needed to fix it. The adverse impact was also lessened by the fact that, capitalising on the *ProxyLogon* experience, numerous companies restricted access to email only when logged into a VPN. We also detected much fewer vulnerable servers in Polish IP addresses:

- Number of MS Exchange instances in Polish IP addresses at least once confirmed as vulnerable: **240**.
- Number of notifications sent to organisations: **83** (some organisations owned several servers).

We are still dealing with the consequences of these vulnerabilities and the number of servers attacked at that time. It is often the case that, after receiving a notification of ransomware encryption, several months earlier the organisation had been notified of a vulnerable MS Exchange instance, or even of our detection of a web shell, but it had taken insufficient action to remove all the backdoors left by an attacker.

Evolution of known phishing campaigns

As far as phishing cybercriminals are concerned, last year was marked by the refinement of well-functioning schemes. A significant number of recorded incidents involved variants of campaigns used in previous years.

Facebook account takeovers

In 2021, we recorded mostly two variants of phishing attacks affecting Facebook users. The most popular one spread through posts within theme groups. The most common targets included open groups with a large number of members, i.e. usually local (city, commune level) or trading groups, i.e. “sell/exchange/give away”.

An ad used to carry out an attack has a simple structure. It consists of a short phrase describing a certain emotion (fear, outrage, request for help) and a link to a fake page. The Open Graph tag mechanism plays a vital role in the entire process, thanks to which a post is supplemented with a given thumbnail, domain and page title. Authors of certain phishing campaign versions noticed an inconsistency in OGTags⁷⁰ mechanism interpretation by Facebook, which enabled them to counterfeit the domain name displayed. See Fig. 18 for the effect of this error.

69. <https://www.zerodayinitiative.com/blog/2021/8/17/from-pwn2own-2021-a-new-attack-surface-on-microsoft-exchange-proxyshell>

70. The Open Graph Protocol <https://ogp.me/>



Fig. 18. The phishing post suggesting that the link leads to the wiadomosci.wp.pl site.

The subject of the post was linked to a news story with gripping content. Most often it would be a kidnapping, murder, mugging or rape. Correct alignment of the displayed page title with the name of the local group is also worth noting. For example, in the (fictional) “Raszyn Community” group, a title displayed in a thumbnail would be

“Missing 3-year-old from Raszyn. Parents beg for help”. In addition to the above-mentioned information categories, we noticed rapid adjustment to the current social situation, e.g. information about 500+ programme alterations or alleged complications after receiving a Johnson&Johnson vaccine.



Fig. 19. Fake post adjusted to a group name.

Fake pages consist of 2 elements: an informational part usually containing a shocking video clip that can be viewed following age confirmation, and a fake Facebook login panel acting as a fake verification method. Initially, the appearance of the first stage of the phishing attack was aimed at imitating a well-known news website, but over

the course of a year, it evolved, taking the appearance of an unspecified social network, to the final form resembling the view of a single Facebook post. The whole process is based on imitating the mechanism for logging into the application by linking an account to a Facebook account.

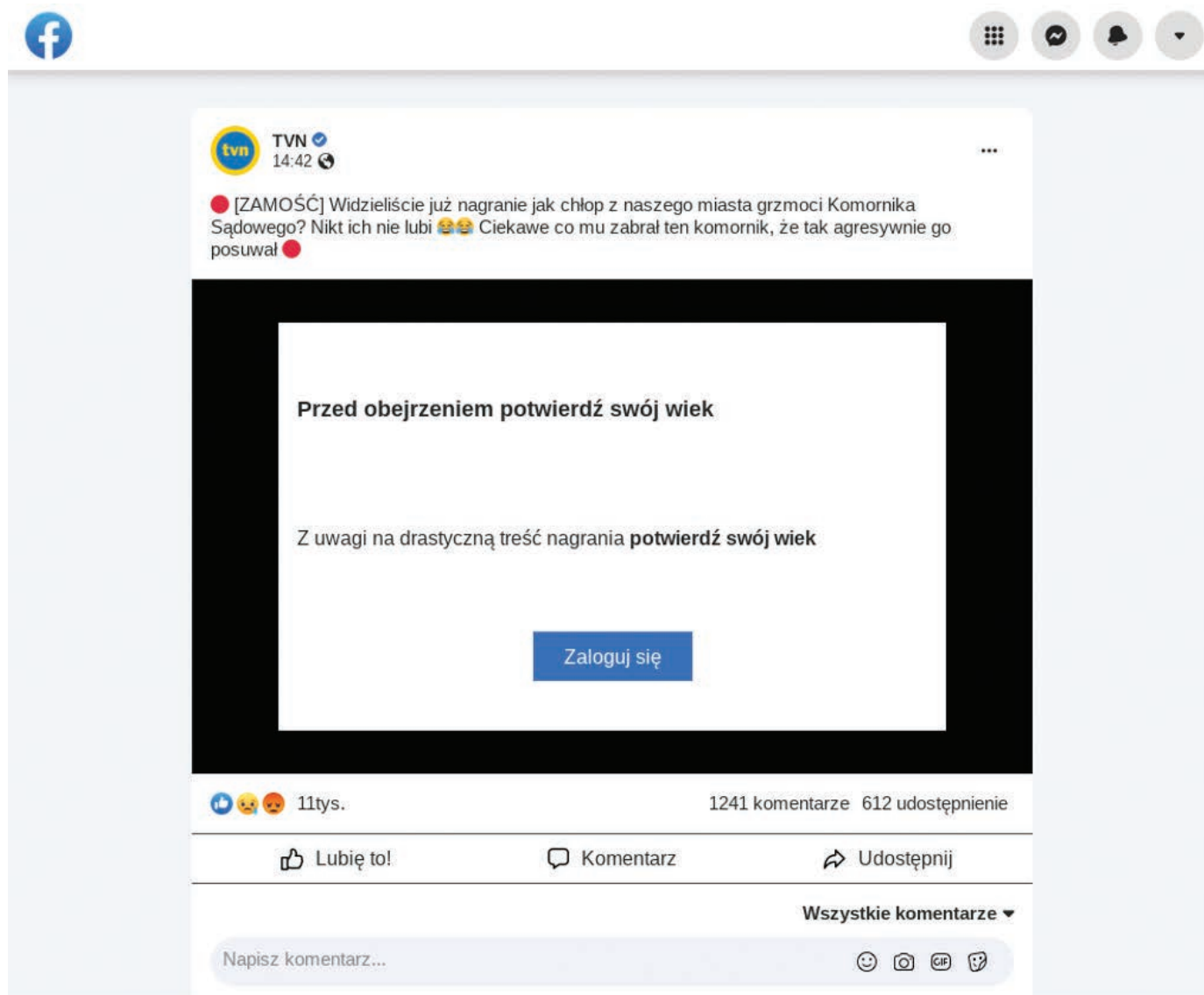


Fig. 20. Fake page with a shocking video clip resembling a Facebook post.

The second noticeable group of phishing attacks aimed at taking over Facebook platform accounts included fake voting and competitions. Here, the scheme is simpler than the one described above. It consists in sending a message to friends from an already taken over account asking them to par-

ticipate in a lottery by following a link attached. Obviously, the URL sent leads users to a fake login panel. An interesting aspect of this campaign is that this phishing instance can only be viewed on mobile devices.

Although we have been observing an increasing number of phishing campaigns collecting Facebook account data, there is no clear theme of financial gains resulting from the campaigns. This constitutes a change in relation to previous years, when phishing for BLIK codes from friends of the owner of a taken over account was very popular. Some of the variants of the described scheme appear to be linked to investment frauds described in the section “Fraud and fake investment schemes”. Profiles obtained in this way are also used to further spread phishing messages.

Fake payment gateways

In 2021, the number of phishing attacks using the fake payment gateway scheme increased, although the percentage of this scenario among all scams decreased. Our team recorded the highest

number of incidents following the pattern observed at the end of 2020, and consisted of a text message, a panel informing about the need for a surcharge and a fake payment gateway using the eCard company image. The phishing message asks for an extra payment for a designated service and contains a link where this payment can be made. Over the course of the year, cybercriminals moved from directly sending the target domain to using characteristic URL shorteners in the .sv and .co domains. Within this campaign, we noticed three distinct schemes: surcharges to parcels sent via InPost, electricity bills from PGE and gas bills from PGNiG. Initially, the counterfeit eCard panel phished only for bank account data; however, it was extended with the BLIK code “payment” functionality in April.

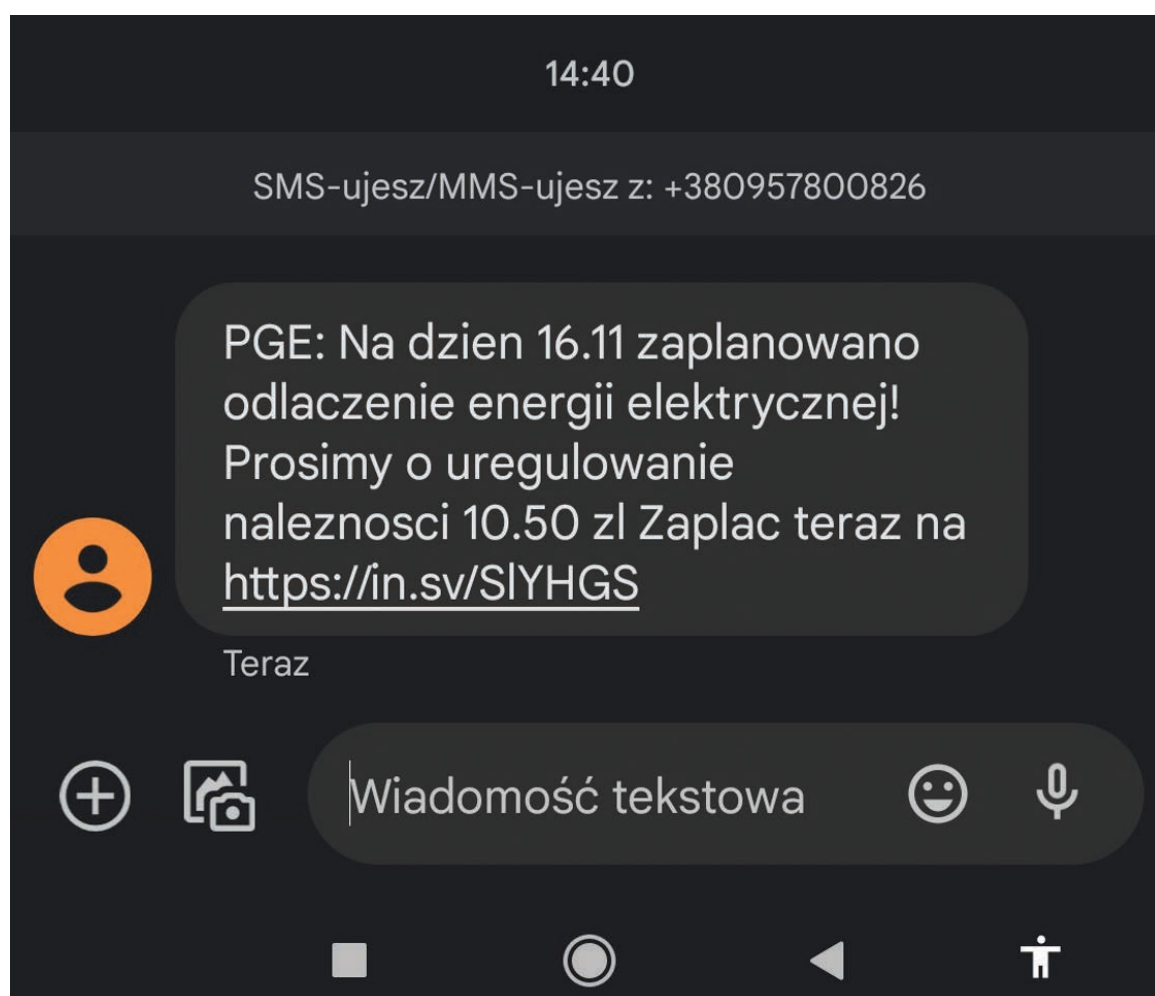


Fig. 21. Fake text message requesting an electricity bill surcharge payment.



Płatności online

Na dzień **18-03-2022** zaplanowano odłączenie energii elektrycznej!
Prosimy o uregulowanie należności.

Umowa numer: **GKETRNG785362**

Kwota należności: **4.27 zł**

Ureguluj należność szybko i wygodnie za
pomocą przelewu szybkiego bądź BLIK.

[Przejdź do płatności →](#)



Fig. 22. Fake page displaying a message requesting for electricity bill surcharge payment leading to a payment gateway.

Apart from this scheme dominating throughout the year, smaller campaigns using the PayU payment gateway image were also noticeable. The scenario is the same as it has been for several years now, i.e. a link to a fake site is sent via text messages. It is accompanied by content that uses various elements making the whole design more credible. This year, the most common themes for these messages were:

- payment of a fine;
- surcharge resulting from an incorrect tax return settlement;
- vaccination lottery.

Unlike the one described above, this campaign was not run throughout the year, but was based on short 2–3 day periods, during which text messages were sent en masse.

Phishing from sellers on advertising websites

The leading pattern related to phishing scams consists in the fact that they target sellers, rather than buyers. This type of attack first appeared in late 2020, and has been growing rapidly ever since. Probably its biggest success factor is the fact that it looks for victims among sellers, which adds credibility to the whole endeavour. A person under attack is actually willing to sell an item and expects contact from strangers. In addition, such factors as the Covid pandemic reality and promotion of remote purchasing options by portals targeting local trade with self-pick-up of parcels have also had an impact on the development of this scheme.

Initially, potential victims included people selling items through the OLX portal. They were sent a link to a fake page containing an item purchase related message and button to collect the trans-

ferred money. The button, however, directed them to a page that phished for credit card data. Over time, additional elements of the scam began to appear, such as fake on-line banking login panels (some banks require customers to log in to confirm card transactions) or a chat with an employee guiding the user through the scam.

In the first months of 2021, in addition to exploitation of the OLX company's image, fake pages "impersonating" InPost courier pages or Poczta Polska pages appeared to display information about the delivery method selected by the supposed buyer. Next, advertisers operating on different platforms were targeted:

- Vinted – second-hand clothes trading platform;
- Blablacar – paid transfers of people during private trips;
- Booking – short-term rental.

In all such cases, the method employed was the same. Cybercriminals informed that someone had paid for the service/item offered and encouraged advertisers to click a link to collect the money.

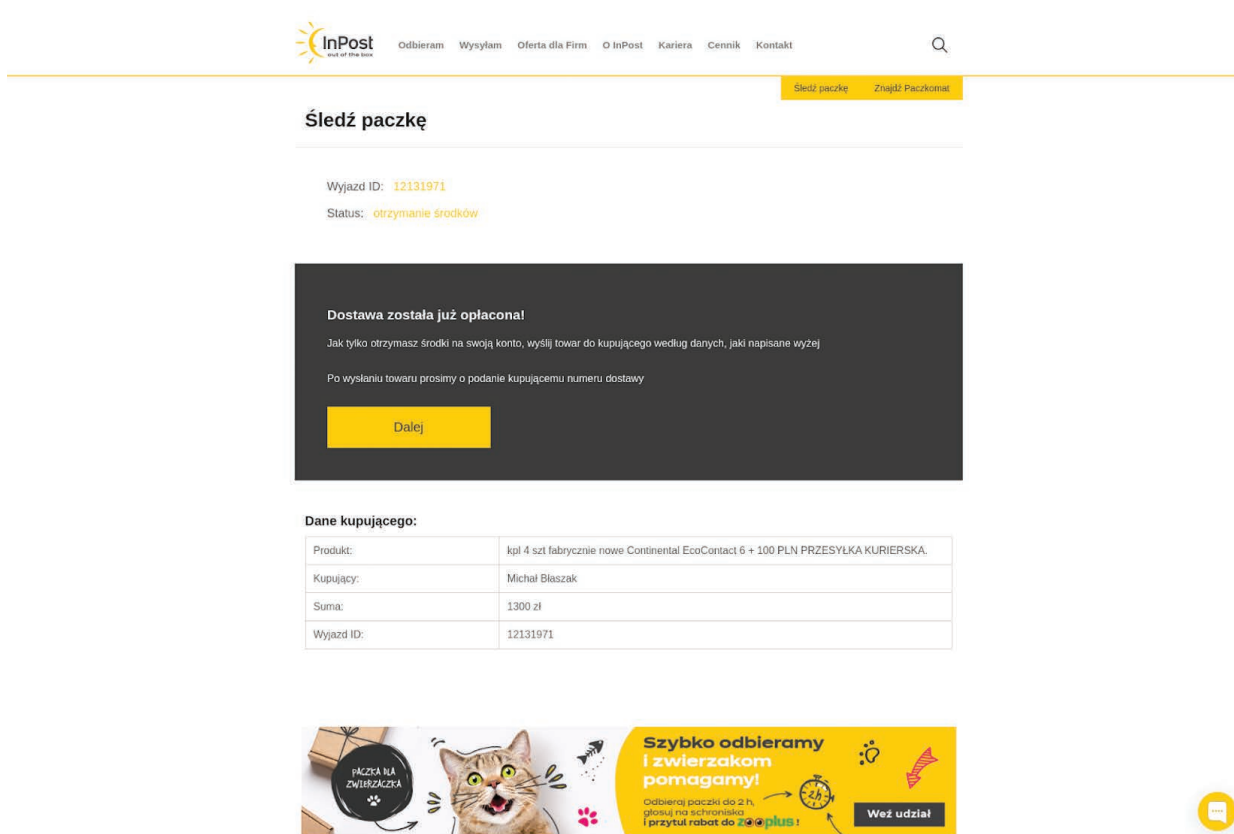


Fig. 23. Example of a fake page using the InPost image.

Initially, WhatsApp was used to distribute malicious links. First, a contacting person would send a link to a genuine offer asking if it was still valid. After engaging the victim in a conversation simulating interest in the item, the fraudster would send a link to a phishing page. Over time, other

methods were exploited, e.g. email notifications or simple text messages. The majority of fake pages were related to offers that might have suggested that the seller was keen to sell the item quickly. The most popular categories included clothing, children's accessories, electronics and jewellery.

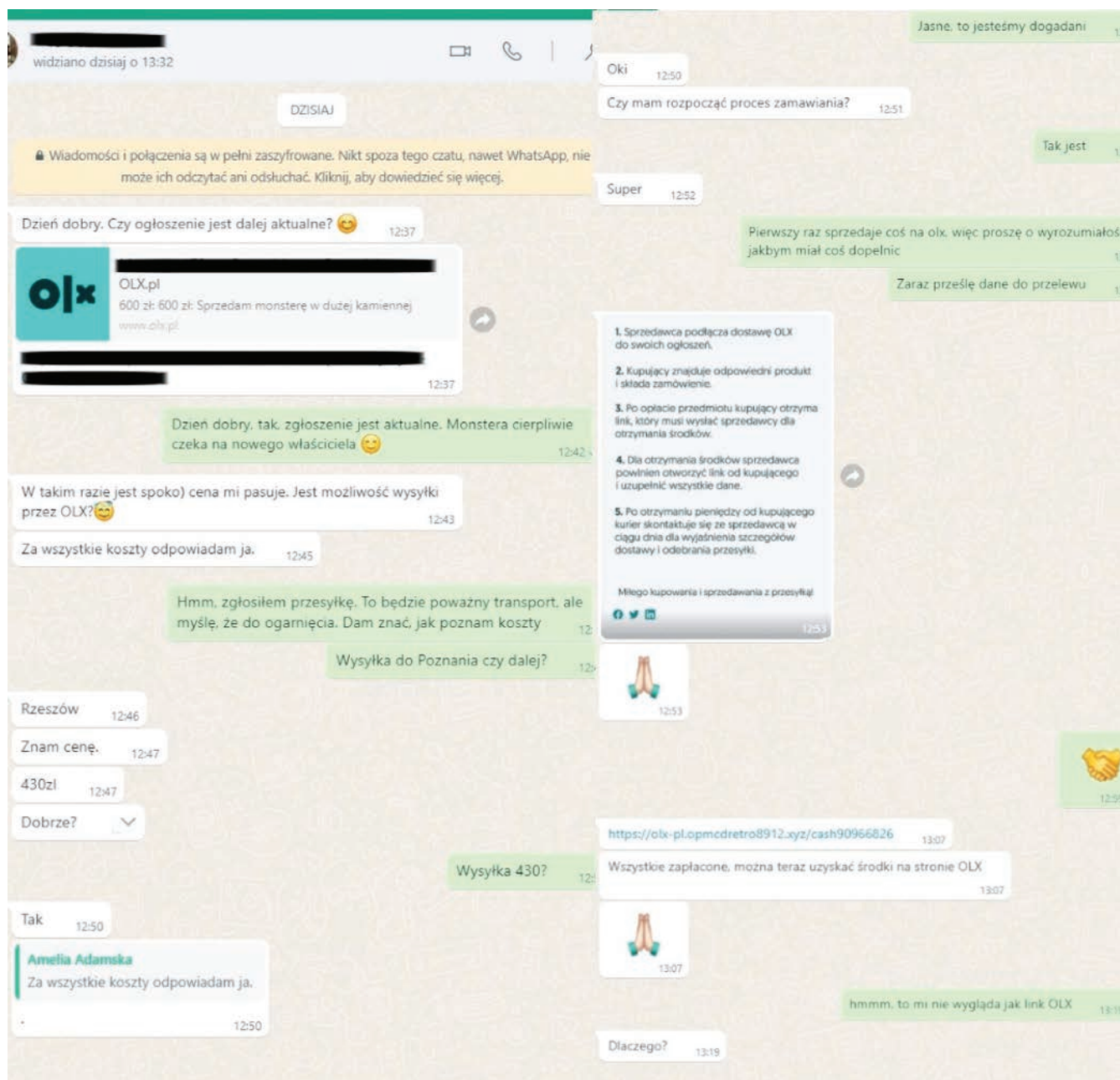


Fig. 24. Conversation with a person faking interest in purchasing an item.

Text message campaigns in Poland

Malware targeting mobile devices

The mobile device market has been growing steadily over the years, and we could also observe this trend in 2021. According to the Digital 2021⁷¹ report, during the period from January 2020 and January 2021, the global number of mobile device users increased by 93 million, i.e. by 1.8%. The report shows that the mobile device market is

dominated by two operating systems: Android at 72.5% of devices in December 2020, and iOS used in 26.9% of smartphones.

According to a survey commissioned by UKE (Office of Electronic Communications), in 2021⁷², 96.9% of the surveyed used a mobile phone, 80.4% of which used a smartphone. One must also note that almost 74% of users encountered automatic text message services. By far the largest number of respondents (over 90%) received automatic notifications regarding RCB (Government Centre for Security) alerts, while just over 50% received

71. Digital 2021 <https://datareportal.com/reports/digital-2021-global-overview-report>

72. https://www.uke.gov.pl/download/gfx/uke/pl/defaultaktualnosci/36/410/1/2021_raport_uke_klienci_indywidualni.pdf

system messages from their operators (service activation or payments). 49.3% of respondents mentioned notifications from courier companies and the post office.

The popularity of smartphones and automatic text message services did not escape the cybercriminals' notice. Increasingly often, they design phishing campaigns targeting their users and create malware attacking mobile platforms.

In 2021, we observed significant increase in the number of reports related to this threat. In that period, the CERT Polska team received over 17,500 reports on malware designed for Android devices.

Overview of new trojans detected

Flubot

Flubot (or Cabassous) was first observed at the end of 2020, in Finland and Spain^{73 74}, where phishing campaigns making use of FedEx and DHL and Correos logos were run. Flubot campaigns were run in several dozen countries, including Poland. While analysing the Flubot, 4.9⁷⁵ version sample, CERT Orange Polska determined 28 countries to which text messages were sent.

The basic Flubot functionality consists in injecting substituted login pages to specific applications. Credentials entered in such panels are then sent to a C&C server.

The name Flubot derives from the way this malware is propagated (like standard flu), and describes its method of operation. Flubot uses an infected phone to further spread phishing messages. This means that, with each instance of infection, the number of bots sending phishing messages to random phone numbers increases.

One must note that the database of phone numbers to which messages are sent is supplied partly by contact lists from infected phones.

With subsequent campaigns carried out in numerous countries, we observed development of Flubot's features. These included interception of communication between the bot and C&C server was made more difficult by introducing DNS over HTTPS traffic tunnelling mechanisms.

BlackRock

In the second quarter of 2020 new malware appeared, i.e. BlackRock⁷⁶, which was largely based on code and functions "borrowed" from the Xerxes and LokiBot malware family. Apart from the incident below, in 2020 the CERT Polska team did not observe any campaigns related to this malware family. In 2021, the campaign was active for a very short period of time.

The BlackRock capabilities include:

- logging of entered data;
- listing, forwarding and sending of text messages;
- locking screens;
- collecting device information and notifications;
- hiding application icons;
- enabling deletion of applications;
- injecting fake login panels into specific applications.

ERMAC

In September 2021, the CERT Polska team observed a new variant of the Cerberus trojan described in 2020, namely ERMAC. As compared to previous variants, the encryption algorithm used so far was altered. A reporting function for the list of accounts added to the system was also implemented. As with the first version of Cerberus, it was put up for sale a few months earlier. ERMAC was probably used by the same actor responsible for the BlackRock campaign.

Malware campaigns for Android devices observed in 2021

Similarly to previous years, in 2021 mobile device malware was most commonly distributed via fake text messages and emails containing links to counterfeit websites. Although these sites presented various content, their goal was the same – to encourage a potential victim to download a malicious file from an indicated resource.

Below, in chronological order, we present an overview of the most interesting campaigns observed by CERT Polska in 2021.

73. *INCIBE-CERT Flubot Analysis Study 2021* https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/incibe-cert_flubot_analisis_study_2021_v1.pdf

74. *New Massive Mobile Malware Ring Targeting Europe* <https://www.prodaft.com/resource/detail/flubot-new-massive-mobile-malware-ring-targeting-europe>

75. *Flubot 4.9 - szybka analiza* <https://cert.orange.pl/aktualnosci/flubot-4-9-szybka-analiza>

76. *BlackRock - The trojan that wanted to get them all* https://www.threatfabric.com/blogs/blackrock_the_trojan_that_wanted_to_get_them_all.html

Inpost parcel pick-up

In the first half of January, the CERT Polska team observed a continuation of the Alien malware distribution campaign, using the InPost company's logos. The distribution method did not change in 2021, as it still sent text messages to random numbers, which contained a link to a page resembling the InPost portal. The messages

were designed to encourage users to download applications from the indicated resource. For this purpose, the cybercriminals highlighted the need to take action in relation to the situation.

It is believed that the campaign was completed in the second half of January. In 2021, our team did not observe any more reports related to Alien.

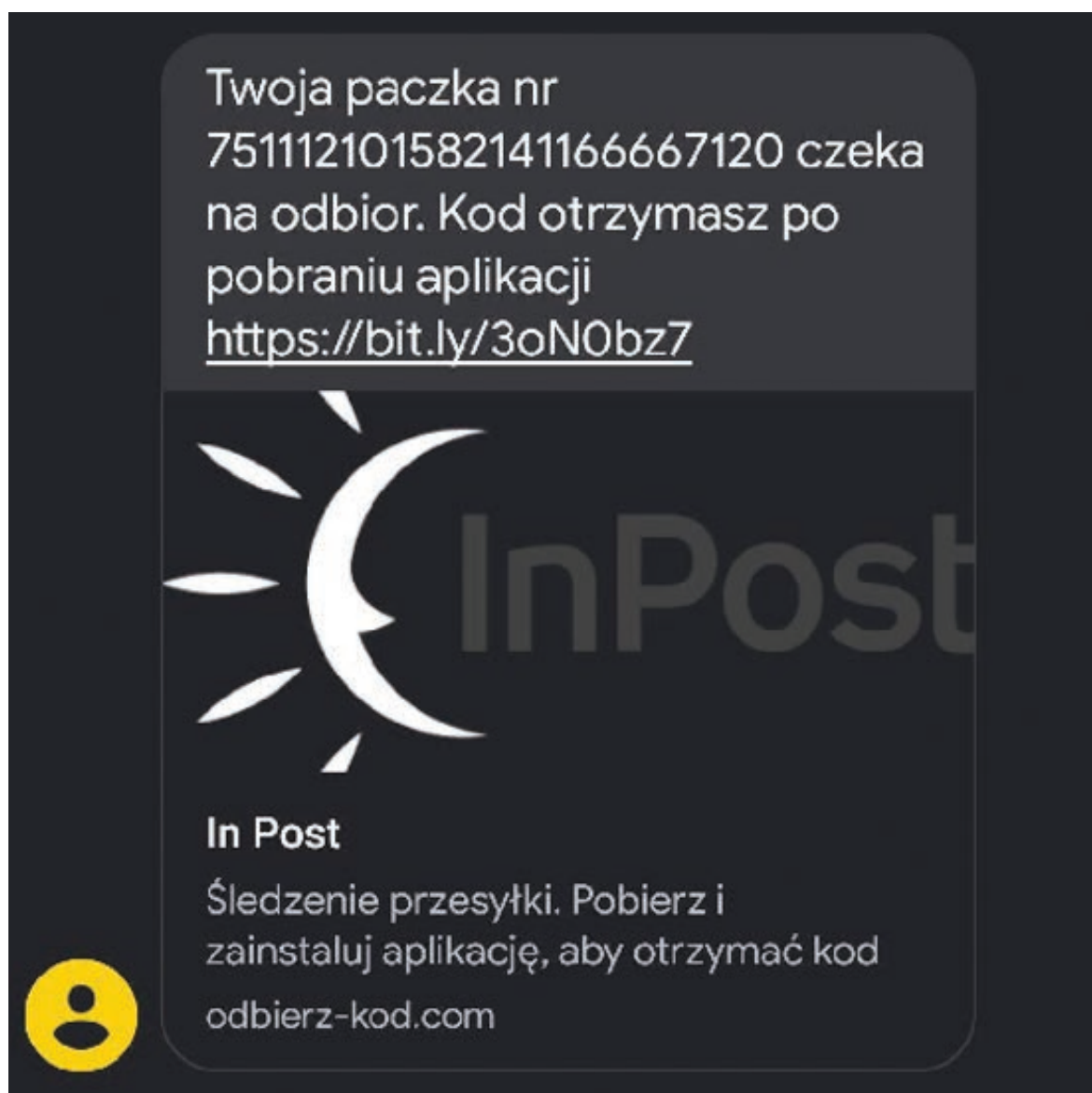


Fig. 25. Example of a message impelling to download and install malware.

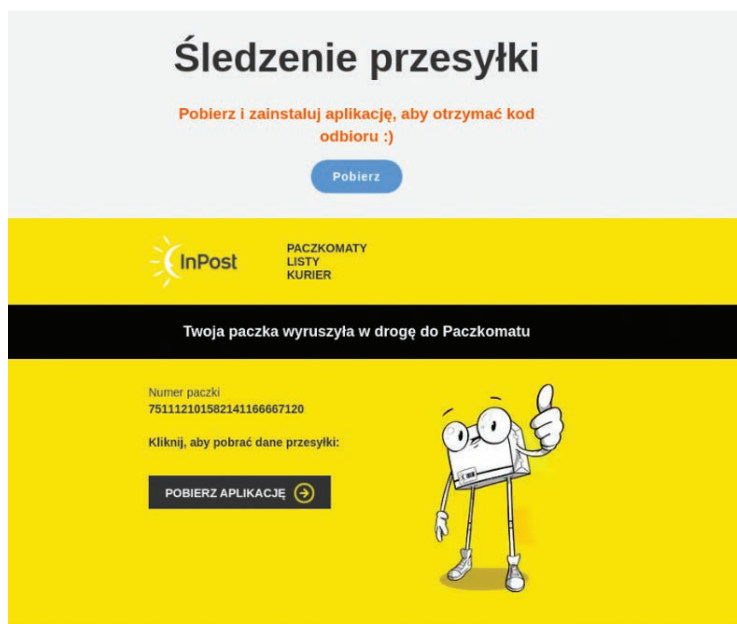


Fig. 26. Fake page encouraging to install malware.

Terms and conditions update and anti-spam policy

In the first half of 2021, CERT Polska observed a continuation of the Hydra malware distribution campaign using email service provider logos, e.g. WP, o2, Onet or Interia. Random recipients received messages in their mailboxes from an alleged mailbox administrator. Depending on the

scam variant, the body of the email contained information about having to approve updated terms and conditions, or a fake notification informing that the account had been blocked due to alleged spam distributed from the mailbox. Regardless of the scheme, the fraudsters' objective remained the same – to encourage the victim to download and install malware. The last time this scheme was used was in May 2021.



Fig. 27. Fake email informing about an alleged update to terms and conditions and necessity to take certain actions to avoid blocking the account.



Fig. 28. Site impersonating the Onet Poczta site, encouraging users to download malware

Loans

In February 2021, the CERT Polska team observed the development of campaigns distributing malware belonging to the Hydra family. In this case, the logo of a non-existent financial entity was created and used. Fraudsters sent emails informing that a loan application, allegedly sub-

mitted by the addressee, had been approved. The message content contained a link to a portal making it possible to transfer the loaned money to a bank account. Upon accessing the page, the visitor was informed again that the loan had been granted. After clicking any button on the page, the visitor was informed that an application must be downloaded for this purpose.

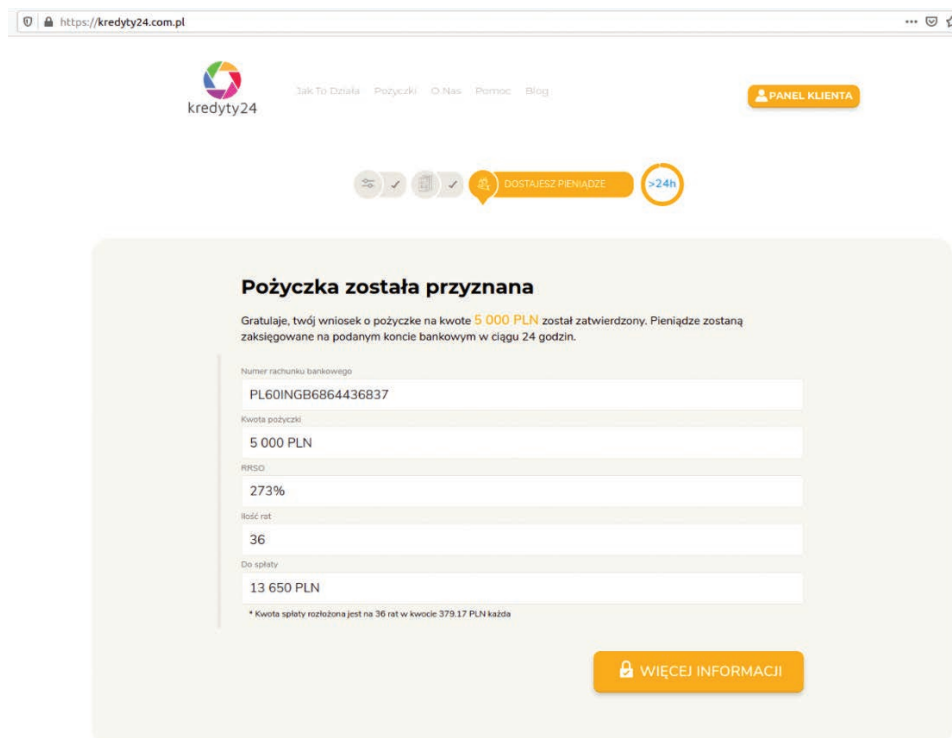


Fig. 29. Fake page informing about an alleged loan.

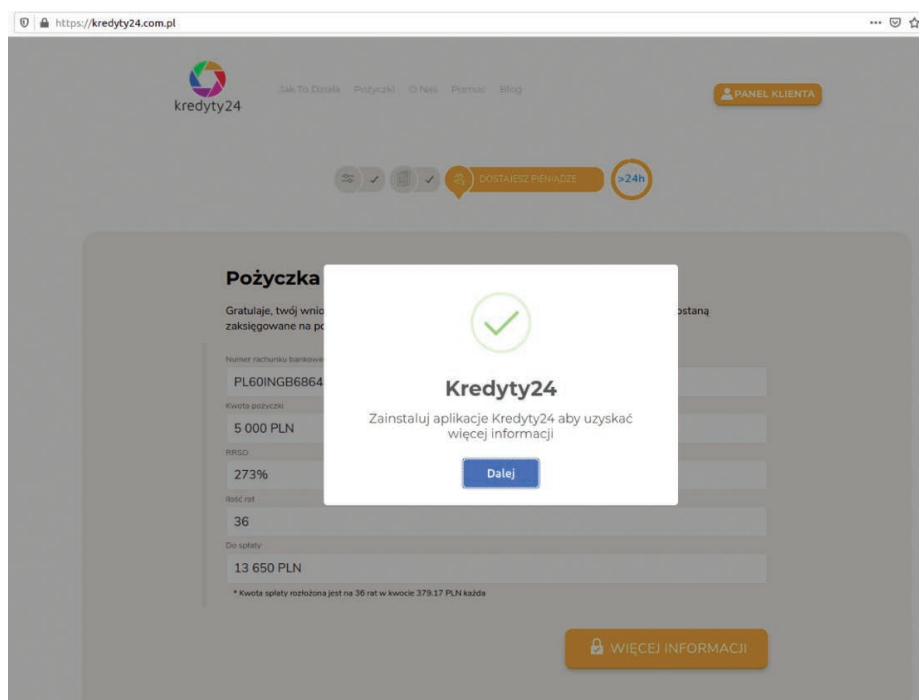


Fig. 30. Prompt encouraging to download malware

STOP COVID

In January 2021, the first and only BlackRock malware distribution campaign took place. It exploited the then popular theme of applications informing about contact with a person suffering from COVID-19. Fraudsters sent text messages to random phone numbers encouraging them to

install the software. After clicking an attached link, a portal appeared to encourage users to download the application from the indicated resource. After the victims downloaded the malware, they were urged to proceed in line with installation instructions that actually informed them how to bypass system security measures restricting the installation of applications from unknown sources.



Fig. 31. Page featuring a fake app for COVID-19 infection tracing.



Fig. 32. Instructions informing how to bypass the security measures restricting the installation of applications from unknown sources.

Parcel delivery

In mid-April 2021, the first of three phases of the new campaign was deployed, which dominated other schemes in terms of its scale of distribution. Mobile phone users received massive numbers of messages informing them of alleged parcel detention by customs or other problems with its delivery. Such messages also included a link to a page with the DHL logo and encouraged users to install an application to manage and track the alleged shipment. In reality, it was a banking trojan from the Flubot family.

The scale of this scam must not be underestimated. The scheme exploited domains that had most likely been hijacked beforehand. This is evidenced by the use of a large number of unique names (more than 400), which in no way coincided with the courier service theme exploited. Moreover, during the first wave of infections lasting from 15 to 27 April 2021, our team received over 3500 Flubot-related reports. It was approximately 50% of all notifications handled during that period.

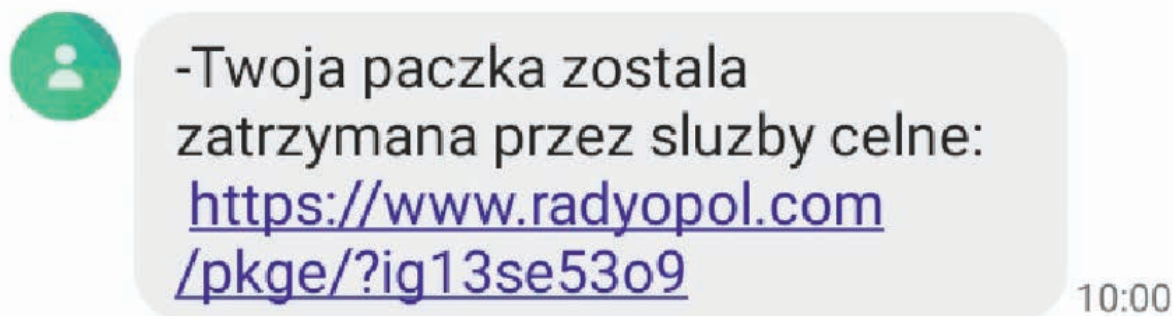


Fig. 33. Fake text message informing about allegedly retained parcel.



Fig. 34. Page with the DHL logo encouraging users to install an application to manage and track the alleged shipment.

Voicemail

After almost 4 months of no activity from Flubot operators, a new campaign appeared on 12 August. This time, the scam consisted in using telecoms operator trademarks and informing about an alleged message left on the recipient's voicemail. Similarly to the previous case, the message contained a link that redirected users to a page where the app could be downloaded. The distinctive feature of the page was its minimalist design, simply presenting data regarding the alleged voicemail message.

The key feature of this campaign was a similar formula for designing subsequent message patterns. As the campaign developed, more mechanisms were added to limit the ability of Android operating system spam filters to detect potential spam. For this purpose, random strings of characters were added at the beginning of the message.

During 16 days of this wave activity (12–28 August 2021) our team handled over 2,000 reports.

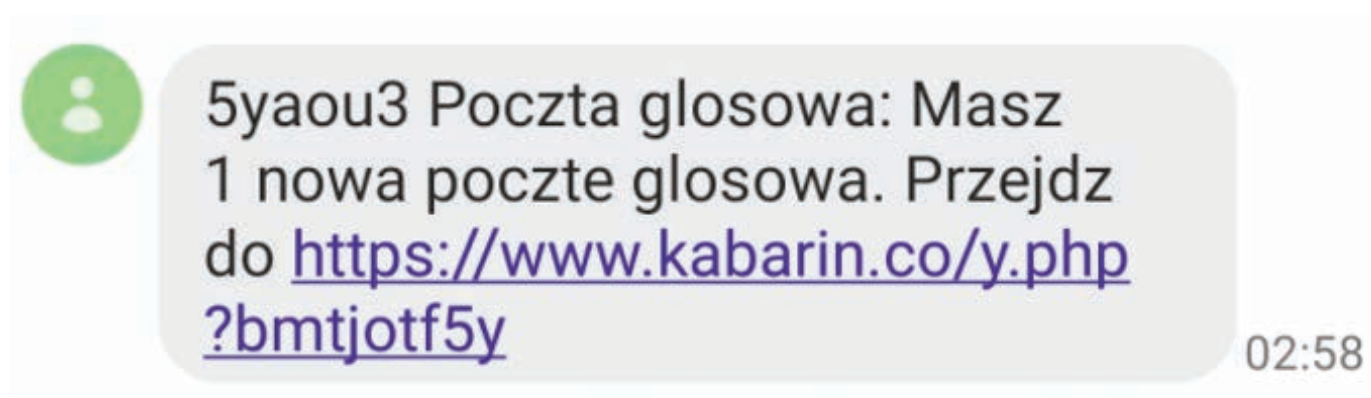


Fig. 35. Text message informing about an alleged voicemail message.

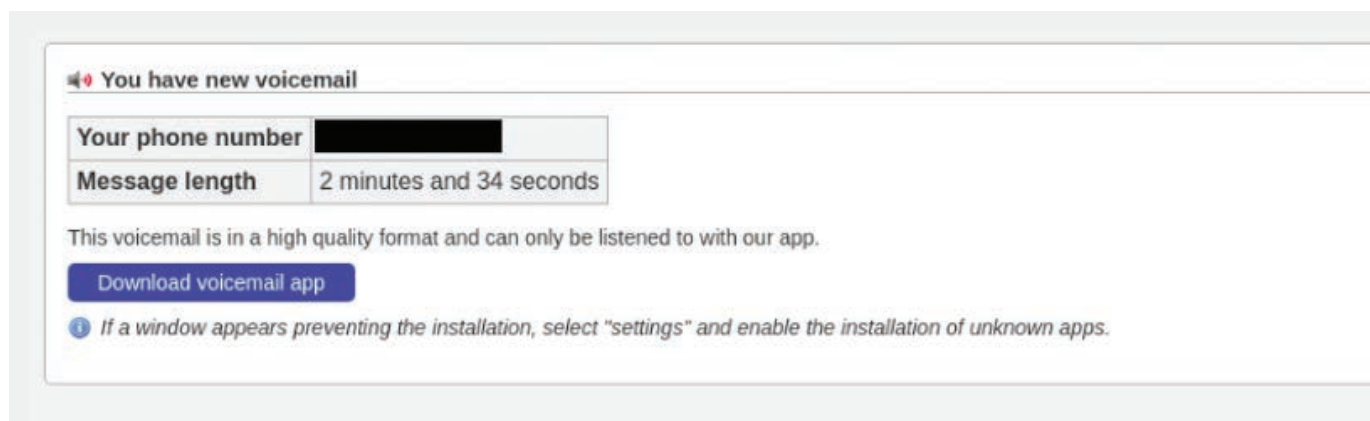


Fig. 36. Fake page encouraging to download an application making it possible to play back the message.

mObywatel

In mid-August 2021, a campaign related to ERMAC, a new banking trojan family derived from Cerberus, was detected. This time cybercriminals used the mObywatel application image. Random recipients were sent text messages from the sender identified as “MOBYWATEL” to inform them of an alleged appointment for their next vaccination dose or of winning the “national lottery”. The message also contained a link to an application that would provide the recipient with more information. After entering the page, they were

directed to a fake Google Play application view, where they were supposedly able to download the mObywatel app.

Fraudsters are increasingly keen to use the image of the Google Play shop to authenticate the source of an application to be downloaded. Users may simply not notice that the page only resembles the genuine Google Play store. Thus it is so important to download all apps from within the store’s application level (rather than via the website), and to pay attention to the messages displayed during installation.



Fig. 37. Fake text message informing of winning the „national lottery”.



Fig. 38. Counterfeit Google Play store view allegedly making it possible to download the mObywatel app.

Adobe Flash update, received photos

The campaign exploiting the mObywatel app image was not the only scheme distributed by the ERMAC-related actor. In the same period, random phone numbers received text messages informing them that a wallet containing the address-

ee's documents had allegedly been found. The content featured a link to a page using the Adobe company logo and encouraged to download the required Adobe Flash Player update. Similarly to the mObywatel app scam, an APK file being malware from the ERMAC was made available from the resource indicated.

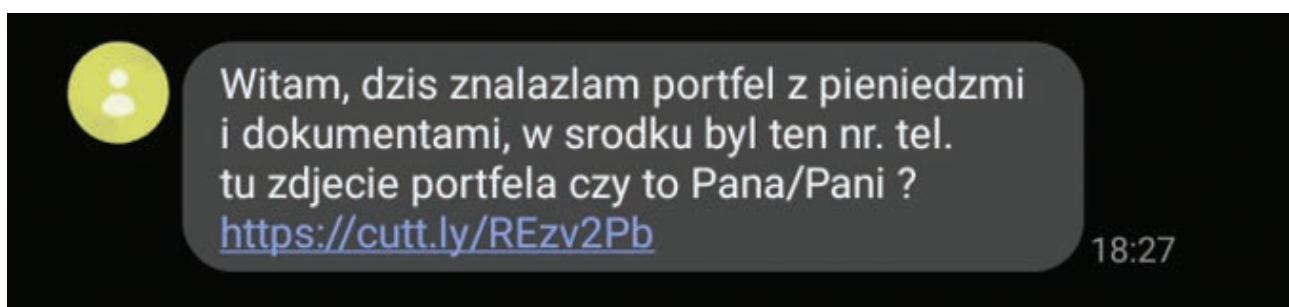


Fig. 39. Text message informing about finding a wallet containing documents.

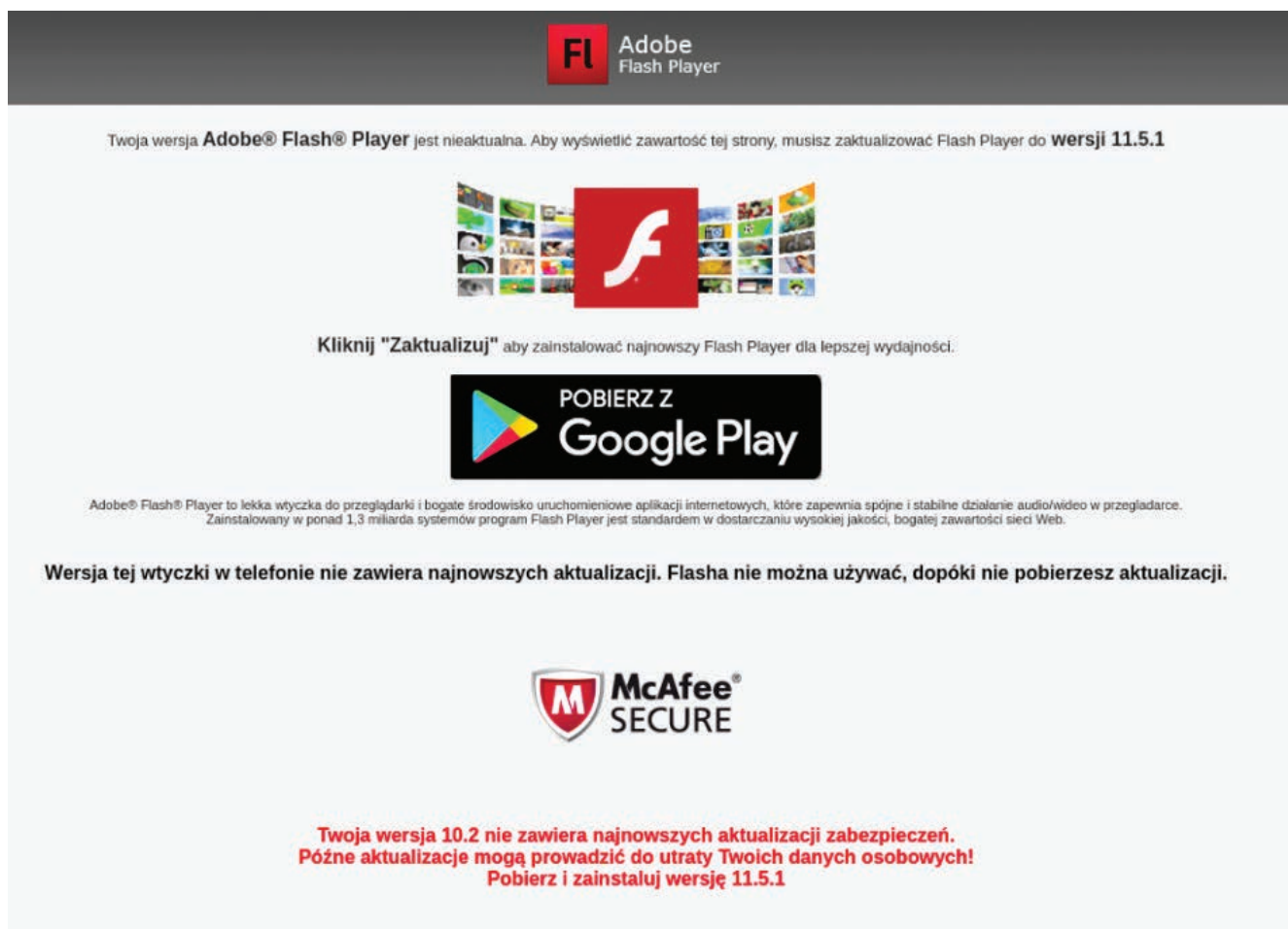


Fig. 40. Page with an alleged Adobe Flash Player update.

Incorrect DPD Pickup order address

The last campaign carried out by the actor responsible for ERMAC also consisted of sending large numbers of text messages. This time they informed about an alleged error in an order address provided to the DPD courier company. It

was also implied that the addressee could obtain more information by using a system whose link was included in the message. As in previous campaigns organised by this actor, the page using a specific entity's image, encouraged to download and install malware.

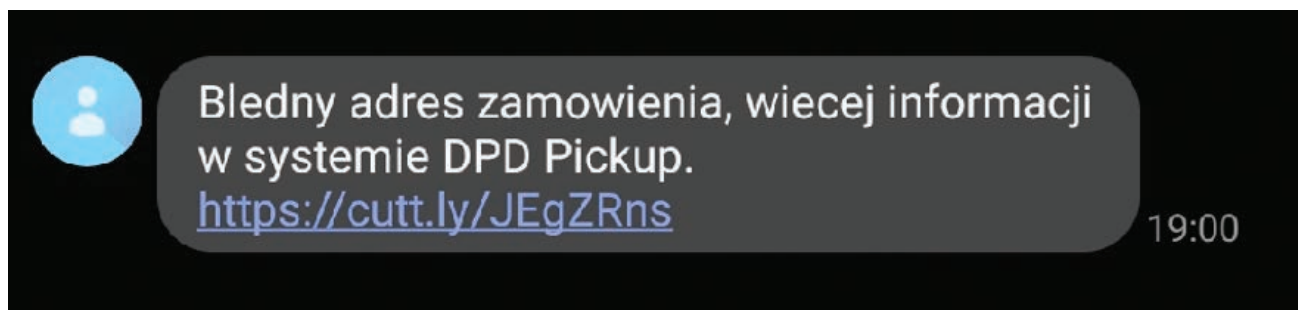


Fig. 41. Fake message regarding an alleged incorrect order address.

Parcel delivery, voicemail and Adobe Flash update

Starting from mid-November 2021 till the end of the year, the CERT Polska team noted an increasing number of reports related to a mass Flubot family malware distribution campaign. During this campaign, our team handled over **11,500** related reports. During this campaign, both schemes used in the previous campaigns were used interchangeably.

How can you avoid infections?

First of all, you should avoid installing applications from unknown sources. When in doubt, verify whether the message you received inviting you to install the application is real. At the same time, remember that simply clicking a link sent in a text or email message and entering a dangerous site does not automatically result in installing malware.

Before installing applications from sources other than the application store pre-installed on the device, a system generates a message asking whether to allow installation of applications from a given source⁷⁷.

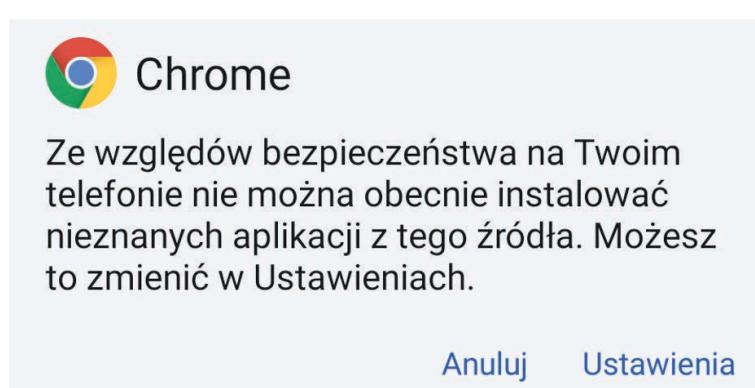


Fig. 42. Example of a message requesting permission to install an app via Google Chrome.

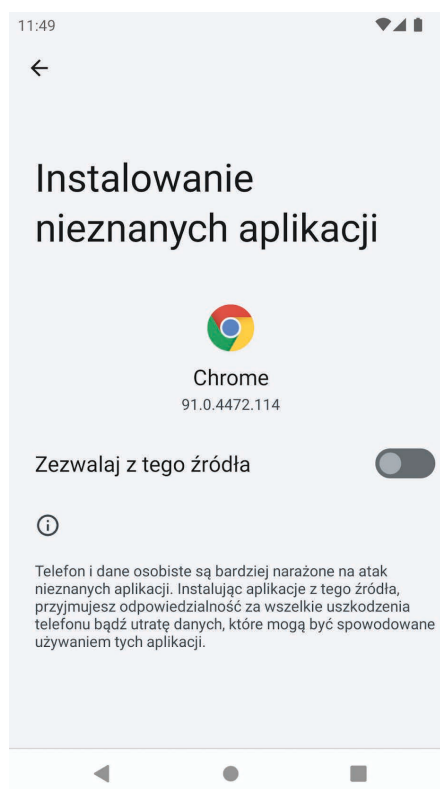


Fig. 43. Page in settings where users may allow installation of an app from a particular source.

77. Functionality available since Android 8 Oreo: <https://developer.android.com/studio/publish#publishing-unknown>

Even after you have allowed an app to be installed from a particular source, a message appears before it is installed asking if you want to allow this app to be installed.



Fig. 44. Example of a message before installing a fake Flash Player application.

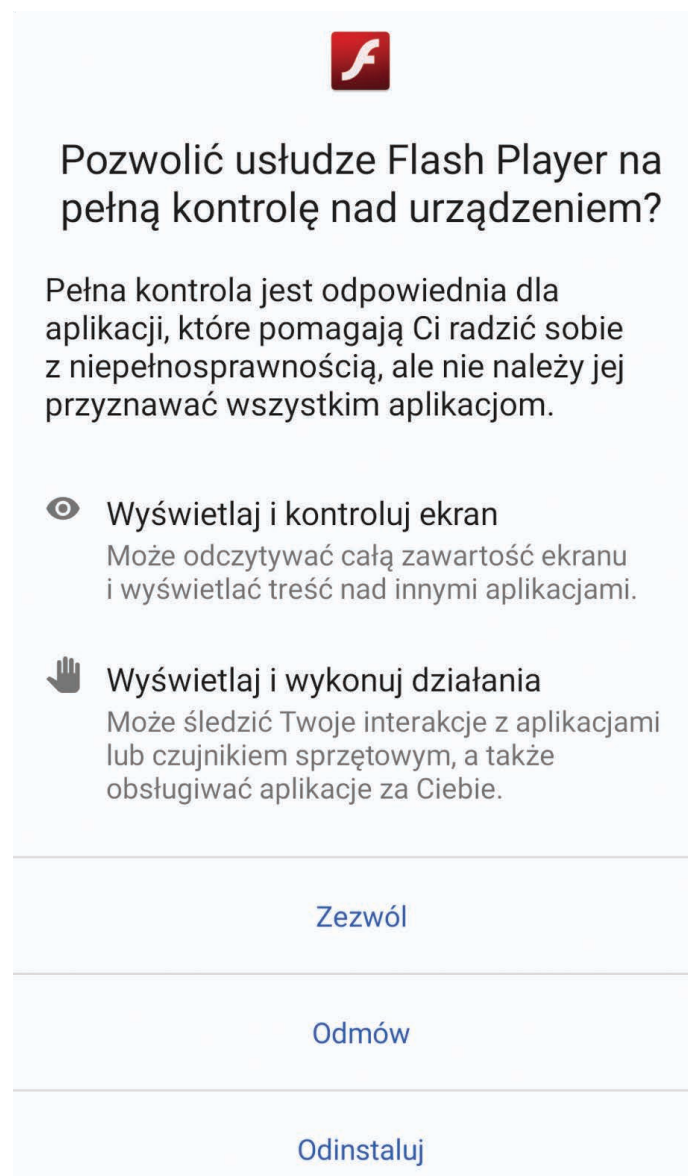


Fig. 45. Example of a message where a fake Flash Player application asks for permission to control a device.

After installing an app, it can be very difficult to remove it - the families described in this document come with sophisticated protection mechanisms. However, if you realise that a device has been infected, it is always advisable to seek help from a specialist, e.g. by reporting the incident via the contact form on the CERT Polska website.

We encourage you to follow our social media profiles, where we continuously post warnings of similar campaigns and recommendations for action to be taken to neutralise a given threat. Taking into account the "third wave" of Flubot

infections, we have published a concise guide defining actions to be taken in case a suspicious message is received⁷⁸.

Scams and fake investment schemes

During the first months of 2021, we witnessed an increase in cryptocurrency popularity, i.e. Bitcoin in particular. It was confirmed also by the growing number of "bitcoin" keyword searches in Google. At that time, the value of Bitcoin sky-rocketed, as illustrated in the chart below.



Chart 3. Bitcoin prices in the analysed period⁷⁹.

This trend did not go unnoticed by criminals who exploited it in new scams. Virtually all the cases of fake investment schemes analysed involved cryptocurrencies. Bitcoin was most commonly mentioned, probably because it is the most recognised cryptocurrency. Victims were encouraged to "invest" using several mechanisms, two of which were employed most frequently.

The largest number of reported cases involved a phone call concerning supposedly previously invested funds. The caller offered assistance in withdrawing these funds. For this purpose, installation

of a remote access (remote desktop) program such as AnyDesk was required. Although the program itself is perfectly legal and widely used, in this case it allowed fraudsters to gain access to the device.

The other scam massively employed by cyber-criminals was much more complex. It consisted in promoting sites offering fake cryptocurrency investment schemes using a specially devised algorithm that was supposed to indicate particularly profitable asset purchase and sales opportunities.

78. <https://www.facebook.com/CERT.Polska/posts/4774454839241535>

79. <https://www.google.com/finance/quote/BTC-PLN>

RAPORT SPECJALNY: Eksperci są pełni podziwu dla Tomasz Biernacki jego ostatniej inwestycji, co wywołało przerażenie wśród dużych banków."

Korzystając z tej „luki fortuny”, polscy obywatele zgarniają już miliony złotych bez wychodzenia z domu – ale czy to jest legalne?

Jak widać w



Tomasz Biernacki ujawnia nową, tajną inwestycję, która sprawia, że setki Polaków stają się bardzo bogaci.

(Puls Biznesu) - polski przedsiębiorca, menedżer, założyciel i współwłaściciel sieci handlowej Dino Polska Tomasz Biernacki, zdobył sławę jako zuchwała osoba mówiąca wprost, która nie ma oporów, by mówić szczerze o tym, jak zarabia pieniądze.

W zeszłym tygodniu Tomasz był gościem programu „Kuba Wojewódzki Show”, w którym ujawnił nową „lukę fortuny”. Taka „luka”, wg jego słów, może zamienić każdą osobę w **milionera w ciągu 3-4 miesięcy**. Biernacki przekonywał wszystkich ludzi w Polsce, by skorzystali z tej świetnej okazji, zanim wielkie banki ostatecznie tego zabronią.

WYNIKI CZYTELNIKÓW

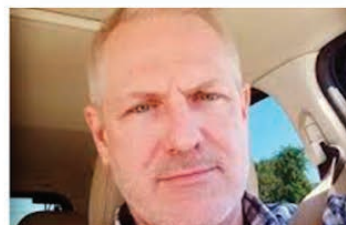
Wygrana: 7 521 zł



"Korzystałem z **Bitcoin Up** dopiero od 2 tygodni a już wykupiłam dzięki niemu urlop w Europie."

Anna Tomaszewska
z Gdańska

Wygrana: 5 552 zł



"Korzystam z **Bitcoin Up** od ponad dwóch tygodni a mój początkowy wkład 1100 zł wzrósł do 5 802 złotych. To o wiele więcej niż mogę zarobić w pracy."

Marik Majewski
Łódź

Wygrana: 9 200 zł



Fig. 46. Example of a site using celebrities' images to promote fake investment schemes.

Fake investment platforms were often advertised on Facebook via hijacked accounts in order to make messages more credible among friends. Clicking the link would usually transfer the user to a site that looked like a well-known news portal. It would contain an article, often featuring celebrities, describing a new, highly effective site enabling users to invest without having any expertise. Following registration, the victim was often encouraged to initially invest a relatively small amount, usually the equivalent of around 200 euros. The platform could then be used to observe an alleged increase in the investment portfolio value. However, the presented growth

had nothing to do with reality. As victims became more trustful, the cybercriminals could convince them to increase the invested funds.

Another scam involved sending notices requesting the need to pay a tax or additional fees. To this end, the fraudsters impersonated various institutions. The final stage of the scam consisted in tricking the victim into installing a remote computer access program. Similarly to the previously described mechanism, the apparent aim was to facilitate the withdrawal of funds. Allowing remote access to a computer and bank account opened in the browser also often enabled fraudsters to take out loans on behalf of unwary users.

In the second half of 2021, the CERT Polska team started receiving reports concerning another scam. In that case, instead of investing in cryptocurrencies, the criminals advertised sites facilitating the alleged purchase of shares in various blue-chip companies. Initially, the scam mainly concerned energy sector companies. The operation pattern shifts coincide temporarily with large price drops in most cryptocurrencies. Information available in the media regarding the uncertainty of the cryptocurrency market may have scared

off potential victims from this type of investment. Similarly to the previous scheme, advertisements were published on various social networking sites, e.g. Facebook or YouTube, which made unauthorised use of well-known companies' logos, images of celebrities or even politicians holding the most important state positions. It is worth noting that criminals also used external advertising mechanisms to display content promoting malicious sites on renowned news portals.

Cel jest blisko
Sponsored

PGE

**W ciągu 2 tygodni
możesz kupić
nowy samochód.**

PGE-KING.WEB.APP
Dowiedz się więcej

[Learn more](#)

Polski rynek akcji
Sponsored

ORLEN

Zainwestuj w akcje PKN ORLEN
Zyskaj do 20 000 zł co miesiąc
Pierwsze 20 osób może zacząć już od 900 zł
Wspierany przez polski rząd

IMPOUNDDEMONETIZATIONS.XYZ
Kliknij na link, wyślij swoją aplikację i zacznij zarabiać!
Czym są akcje? Ten artykuł jest poświęcony następującym
kwestiom: pochodzenie akcji, w jaki sposób akcje mogą...

[Learn more](#)

Fig. 47. Ads using the PGE and Orlen companies' images to promote fake investment schemes.

After a while, the criminals even started creating videos tampering with images from TV programmes. Images were accompanied by recordings to make investments on promoted

sites. What is more, towards the end of the year, the fraudsters exploited images of other entities. These included CD Projekt RED and Volkswagen.

Wiadomości
Sponsored


Po śmierci męża zaczęła żyć lepiej...👍
Marzena mówi, że spełniła swoje marzenie, kupiła dom i może samodzielnie utrzymać dzieci, mimo braku pracy. Wszystko dzięki programowi, który samodzielnie handluje na giełdzie i przynosi stabilny zysk👍
Każdy może zrozumieć, w tym celu musisz zarejestrować się na oficjalnej stronie internetowej👉👈



INVEST12.XYZ
Więcej szczegółów

Learn more

Życie szczęśliwych ludzi
Sponsored



INVESTS-DC.WEB.APP
Dowiedz się więcej

Learn more

Fig. 48. Advertisements using fake video materials to promote fraudulent investment schemes.

Such advertisements usually included a link to a contact form page, through which a person interested in investing could submit their contact

details. In almost every case, such pages looked the same and the criminals only replaced the logos or photos.

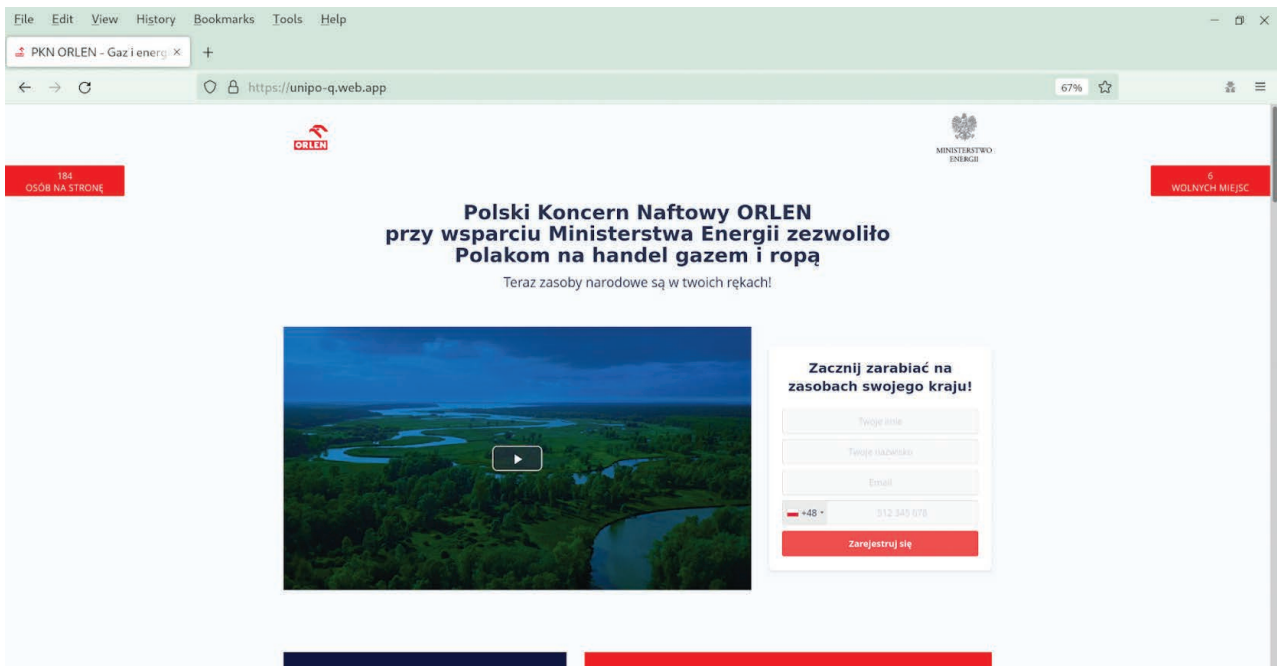


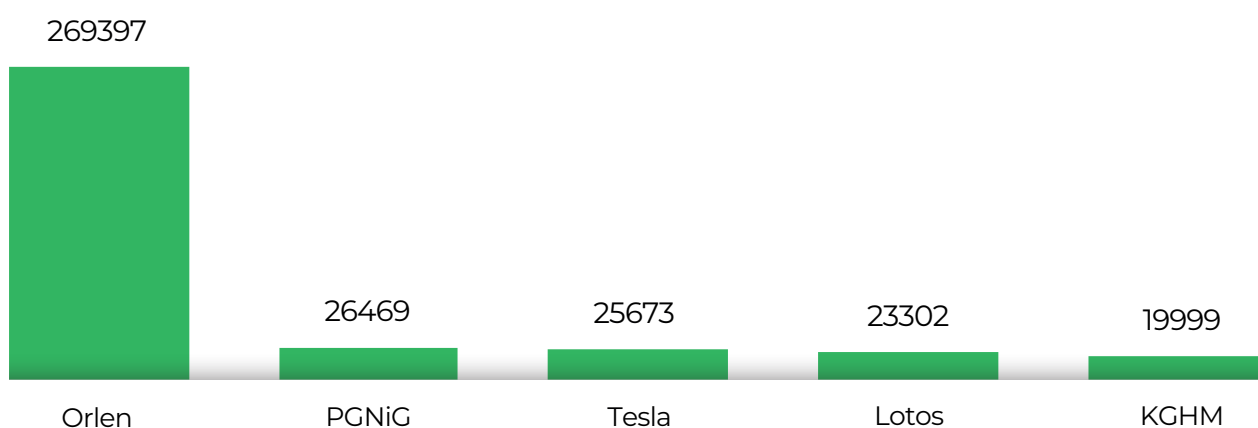
Fig. 49. Malicious use of the Orlen company's image to promote fake investment schemes.

After providing the required contact details, a company representative offering allegedly safe and very lucrative investment schemes, contacted the interested party by phone and urged them to transfer funds. As in the case of scams exploiting people's interest in cryptocurrencies, the amount invested was initially relatively small, but increased over the course of the conversation. Sometimes, to boost victims' trust, they were given information related to possible profits. The next stage was for the fraudsters to gain access to the bank account of people interested in making a quick profit. To this end, as in the previously described scams, a representative would urge people to install a remote desktop application.

In some cases, a fake investment company's representative asked the investor to undergo a similarly fake verification process. In order to do this, the investor was sent a link to a page where they had to upload a scan of their ID or provide exact personal details.

All domains used in these two scams were entered in the Warning List related to hazardous sites. Over the course of 2021, our team analysed 5719 such domains, and 378,000 entry attempts were noted.

Number of domains included in the list hosting sites impersonating the given entity



Number of recorded attempts to visit websites impersonating the given entity

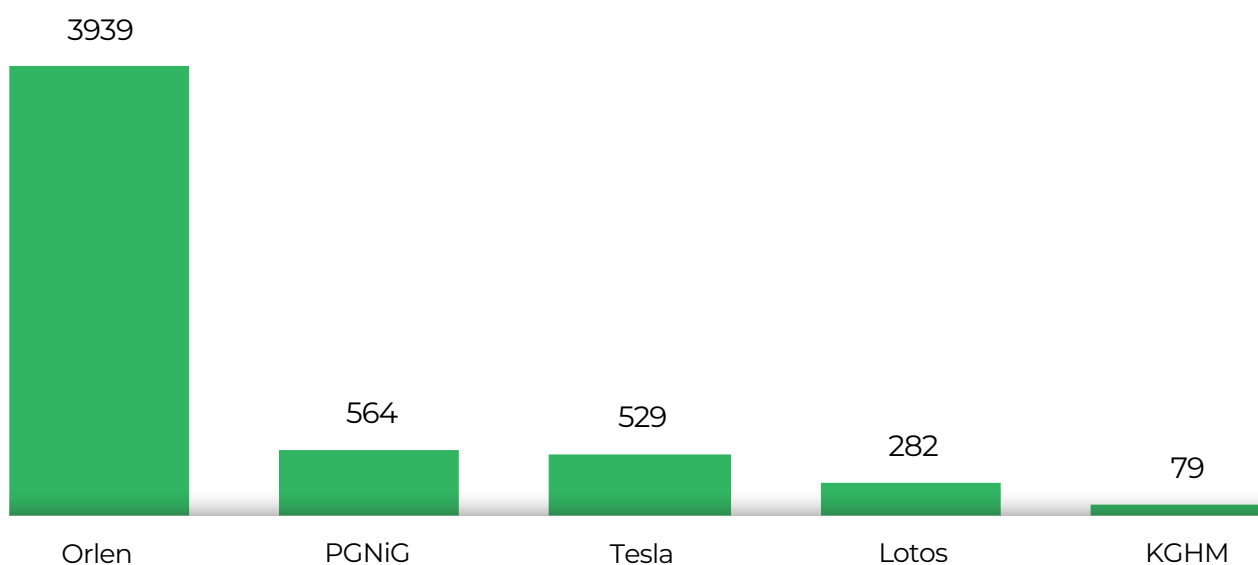


Chart 5. Charts presenting five entities with the largest numbers of entry attempts to domains included in the Warning List.

Data leaks

As the amount of data processed in IT systems continues to increase, we witness increasing numbers of data leak incidents. This applies equally to large corporations, small businesses and individuals. Data security is the responsibility of all individuals, who must strictly adhere to security procedures at every data flow level. ICT systems themselves constitute an equally important aspect, as they require deploying security measures at the stage of design, configuration and maintenance.

How is data leaked?

Not every data leak is caused by a hacker attack. Unintentional leaks caused by data processors also happen. The simplest example is sending mass communication by email using the carbon copy (CC)⁸⁰ feature. In such cases, one email sent may disclose the data of hundreds of people.

Another common issue is the incorrect configuration of systems, e.g. allowing access to databases without protecting them with passwords. Such was the case for Comparitech's analysts who, in March 2021, publicly informed⁸¹ about an on-line database containing the personal data of 35 million US residents that was available without any restrictions.

A data leak also happens when an unencrypted data carrier (laptop, hard drive, memory stick) is lost or stolen. A similar situation occurs in the event of theft, loss or disposal of unencrypted documents. In July, internet users from the town of Piła discovered⁸² a container full of intact documents left in a publicly accessible location. This incident was most likely related to the closing down of a nearby bank branch.



Fig. 50. Container with intact, not shredded documents⁸³.

80. (CC – carbon copy) – a copy of an email is sent to additional recipients. In such cases, the BCC (blind carbon copy) feature is a safe alternative.

81. Source: <https://www.comparitech.com/blog/information-security/35-million-us-residents-exposed/>

82. Source: <https://www.rmf.fm/magazyn/news,40086,bank-wyrzucil-dokumenty-klientow-na-smietnik-tysiace-danych-osobowych-znalazlo-sie-na-ulicy.html>

83. Source: <https://www.wykop.pl/wpis/59209573/aktualizacja-sytuacji-pod-santanderem-w-pile-dawni/>

Fortunately, not every case of free data access results in a leak. Numerous unsecured databases or abandoned documents never fall into the wrong hands. However, this may lead to underestimating the problem. In every case, extreme caution should be exercised.

Cybercriminal activities

Obviously, criminal activity also poses a serious threat to data security. Stolen data can be resold or used as a starting point for further scams. Such data constitutes a popular commodity on the black market, and is readily stolen.

Cybercriminals often target websites with user registration features. Here the aim is to intercept a login data database, i.e. usually email addresses and (secured) passwords. A common mistake by Internet users involves using a single password (or its variations) to log into numerous sites, criminals can gain access to their other resources in this way. For example, by stealing a person's password from a fishing fans' forum, they then attempt to log into that person's mailbox. Once they have access to the mailbox, they can then reset the password for other sites, e.g. Facebook, and use this to perform further fraudulent activity, e.g. steal money by extorting BLIK codes.

It is standard practice to store passwords in a covert form (cryptographic hash function) in a database. However, there are effective methods for obtaining the explicit form of a password stored in this way. Their effectiveness depends on the hash function used and also given password complexity. Nevertheless, even a set of personal data without passwords is also a valuable commodity, making it possible, among other things, to carry out targeted attacks. Sometimes PESEL (personal registration) numbers are also used in authentication processes. One must remember that PESEL numbers are subject to special protection under Art. 87 of the GDPR and must be processed in line with the principle of data minimisation (Art. 5, section 1c, GDPR); however, they must not be treated as secret information.

Ransomware is a very serious threat that has been in full bloom in recent years. This is a type of malware that encrypts files on infected computers. The victim is presented with a ransom demand, in which the criminals demand money

in exchange for a key to decrypt the files. Recently, it has become increasingly common for data to be sent to the perpetrators' servers, in addition to its encryption. Criminal groups involved in such attacks usually target large corporations. However, the data leaked as a result of their operations also concerns entities outside these organisations, e.g. contractors or service users. See the NNN site for detailed information on ransomware.

How can you assure your safety?

Unfortunately, as direct or indirect users of various IT systems, we have no way to realistically assess the actual leak risk. In addition, even the best-secured IT systems are always susceptible to human error, the likelihood of which can never be fully eliminated. One should therefore assume that our data has already been made public or that it will soon be. With this in mind, it is worth following a few rules, not only to reduce the risk of our data leaking, but also to minimise the detrimental impact of such incidents in advance.

Provide just the minimum amount of personal data required

The less information that is processed, the less attractive it becomes to cybercriminals, or the more difficult it will be to exploit it to carry out an attack or commit identity theft. In numerous cases, providing true or complete personal data is not necessary, such as on sites featuring free entertainment content.

Use the identity separation method

It is common good practice to separate business and private computer environments. We can enhance the effectiveness of this principle by dividing these environments into further constituent spaces, such as by setting up separate email boxes for "official business", on-line shopping, entertainment services, etc. This will automatically increase our privacy and, in the event of a leak, reduce the amount of necessary work (e.g. changing phone numbers, email addresses).

Use unique, strong passwords

Strong passwords make brute-force/dictionary attacks very difficult, and using different passwords for different sites mitigates the risks described in the section “Cybercriminal activity”. Passwords do not need to be memorised – it is good practice to use password managers. See the CERT Polska publication on the safe creation and use of passwords available on our website⁸⁴.

Respond to incident alerts

The provisions of the personal data protection act impose an obligation on personal data administrators to inform users about data leak detection. Such a notification must, first of all, contain the scope of data leaked. If password hashes are also leaked then, most frequently, user account passwords have to be reset. Such warnings must not be ignored, and they always require a proportional response. Read them carefully and, after making sure that they apply to your account, follow the administrator’s instructions. Assessing message veracity is key - if you suspect a message may be fraudulent, contact the site administrator in question. This results from the fact that the CERT Polska team have observed phishing messages whose scenario is based on alleged administrator’s request for changing a password or perform another operation requiring logging into a site.

How can you respond to a data leak?

Actions to be taken depend on the context of the leak and type of data that has been disclosed. In a large number of cases, this collection will include our password, which must be changed immediately. In addition, if we use the same password in any other system, that must also be changed.

If the leaked data concerns not only our virtual identity, but also our legal personality (PESEL number, ID card number), it is worth considering taking steps to reduce the risk of falling prey to identity theft. A popular way for criminals to monetise such data is to attempt to take out a loan or credit using someone else’s personal data. Unfortunately, so far Poland has not implemented any government-level, unified method of protection against such criminal activity. However, certain

commercial solutions are available, both paid and free-of-charge, to protect banks and lenders from providing benefits to people using stolen identities. They also protect consumers. Such solutions include:

- BIK (Credit Information Office) – providing notifications on loan applications submitted using stolen data and reports summarising our credit obligations.
- BIG (Register of Debtors) – collecting and making available information on people with unliquidated financial obligations.
- bezpiecznyPESEL.pl portal – making it possible to report a PESEL number as stolen to prevent taking out any loans using victim’s personal data.

In addition to the above, if your ID card details have been made public, you should consider replacing it. Apart from replacing the ID card itself, its new data should be updated in all relevant institutions, especially in banks. Criminals are able to quickly forge an ID card, which can have many serious and unpleasant consequences.

Furthermore, one must realise that data leaks are perfect opportunities for criminals, allowing them to constantly develop their capabilities for both mass and more personalised attacks. The more up-to-date data criminals obtain, the more credible frauds they can perpetrate. While caution and cyber-hygiene should be an everyday routine for Internet users, we should be even more on our guard when a data leak is revealed. If cybercriminals are able to use our data to launch an attack, they will certainly not pass up such an opportunity.

The “Have I been pwned?” site (<https://haveibeen-pwned.com/>) enables us to check whether our email address has been made available during known data-leak incidents. It also allows us to add our address to the facility continuously monitoring new leaks, then we will be informed if there is an incident involving our digital identity.

Follow us on our Facebook (<https://fb.com/CERT.Polska>) and Twitter (@CERT_Polska) profiles, where we can keep you informed about currently observed scam scenarios and other threats to which Polish Internet users are exposed.

84. <https://cert.pl/posts/2022/01/kompleksowo-o-haslach/>

Attack on Trusted Profile

On 21 July 2021, the CERT Polska team observed a stream of notifications and media publications on alarming emails received by Trusted Profile functionality users. The emails informed users of failed login attempts. People reporting such incidents claimed that they had not (at that time) attempted to log into their Trusted Profiles, and, in particular, could not recall any failed attempts

to log into their profiles. Janusz Cieszyński, the Secretary of State for Digitalisation in the Chancellery of the Prime Minister, swiftly responded to such incidents. As a result of conversations with Cieszyński, the CERT Polska team, being the national IT security response team (CSIRT NASK), started coordinating and assisting in establishing the origins of such alarming messages, in cooperation with the ePUAP platform provider, i.e. the Center for Information Technology (COI).



Niebezpiecznik ✓

@niebezpiecznik

⚠️ Uwaga! Otrzymujemy sporo zgłoszeń, że dostajecie maile z Profilu Zaufanego o nieudanej próbie logowania.

Albo ktoś masowo próbuje się logować na PZ testując hasła z wycieków (zmieńcie na unikatowe) albo PZ znowu nie działa jak należy



Z jednym i z drugim nic nie zrobicie...

[Translate Tweet](#)

15:26 · 21 Jul 21 · [Tweetbot for iOS](#)

52 Retweets 3 Quote Tweets 161 Likes



Janusz Cieszyński ✓ @jciesz · 21 Jul 21

Replying to [@niebezpiecznik](#)

To nowa funkcjonalność - informacja o nieudanym logowaniu. Analizujemy wzmożony ruch „testujący” który pojawił się w ostatnich dniach.

11

3

33



Fig. 51. Message informing about failed attempts to log into the Trusted Profile⁸⁵.

85. Source: <https://twitter.com/niebezpiecznik>

Incident analysis

Information published on Twitter by the “Niebezpiecznik” industry site described a mass login attempt made by an unknown actor or a failure of the government system. However, a failure was ruled out. While handling the incident, the CERT Polska team determined that an attack took place involving mass login attempts to ePUAP platform user accounts using the Trusted Profile. This type of attack exploits the users’ tendency to reuse the same passwords on several sites. Login credentials are usually obtained from data leaks made public, and used to log into accounts on other sites. Such operation schemes are defined as “credential stuffing”.

While handling the incident, the CERT Polska team collected relevant information to be passed onto the relevant authorities for further investigation and possible legal action.

Perpetrator apprehended

At the beginning of August 2021, officers of the Warsaw Metropolitan Police apprehended a suspect in the town of Wola Krzywiecka. During the arrest, computer equipment and various data carriers were also secured. During the analysis of the material collected, it was revealed that the man used stolen credentials to gain unauthorised access to the accounts of at least 239 people. The investigation also revealed the fact that data obtained in this way was made available to third parties. The 27-year-old suspect admitted to carrying out an attack on Trusted Profile users. In connection with the above, he was remanded in pre-trial detention for 2 months. The sentence for the crimes committed may be as high as 8 years in prison.

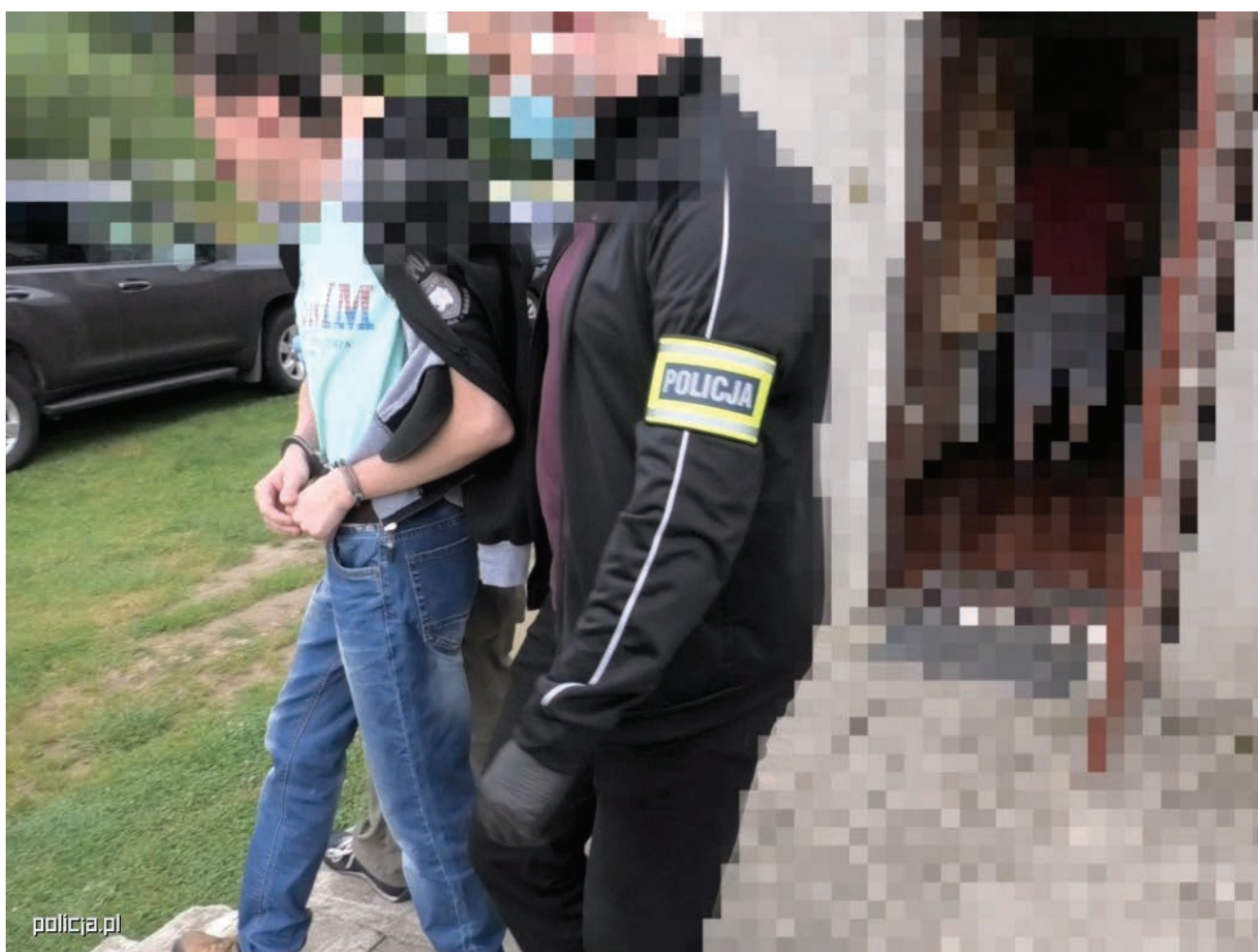


Fig. 52. Apprehension of a suspect allegedly responsible for attacks Source: policja.pl.

Impersonation, threats and false bomb scare alerts

In 2021, we had to deal with numerous incidents involving false bomb scare alerts and threats targeting various institutions and public figures. Such attacks had also occurred in previous years in the usual form of anonymous emails sent to mailboxes, forcing employees of institutions to evacuate. False bomb scare alarms are often referred to as “cascade” attacks, as one perpetrator sends out threats to several institutions at the same time, increasing the chance of a response and placing a significant burden on the emergency services.

Such messages are usually sent out from mailboxes registered just for the purposes of an attack. In addition, the cybercriminals register with a given email site and send out threats using the Tor anonymising network, making it difficult to trace them. Due to the media publicity generated by such actions, this method is constantly exploited by new copycats.

Additionally in 2021, criminals started to impersonate recognised public figures, politicians, journalists, as well as employees of cybersecurity institutions. They set up mailboxes to send out threats, with a given person’s name in the login. Personal data was also included in the message content. The nature of the mailbox use and message content followed the previous patterns, but the use of personal data generated additional publicity and provoked recipients to try to contact the impersonator, e.g. to verify the origin of the message.

At the end of the year, the campaign was extended with phone calls with threats in which the Caller ID Spoofing method was employed. It is made possible by special VoIP Internet gateways from which calls can be made using any phone number. More importantly, this technique does not require hijacking the victim’s phone. Such gateways exploit vulnerabilities of protocols used in mobile networks. As a result, mobile network operators are often unable to verify whether a call presenting a given number actually comes from the SIM card registered to the number. It must be noted that Caller ID Spoofing is not a new technique and is also commonly used in phishing attacks, where criminals impersonate a bank or

local police station. A similar spoofing technique can also be used for text messages to substitute any number or name in the sender field.

To further lend credibility to the threats, phone campaigns used information gathered from publicly available sources such as social media profiles or leaked databases from on-line shops. Such sources were used to obtain phone numbers (both of impersonation victims and threat recipients) and other personal information. The calls were made using a voice synthesiser that read the text of a message.

If you are not sure if a phone call you have received actually comes from the phone number displayed, it is best to hang up and call back. It is worth noting that spoofing is also used to pull classic scams. If you receive a call from your bank and are unsure of the caller’s identity, banks often provide the option of authentication performed by a bank employee using a separate channel, e.g. by displaying a notification in an app installed on the phone or within a website.

Formbook/XLoader malware campaigns

In 2021, we noticed an upward trend related to using the Formbook/Xloader family malware. The MWDB system data shows that, in 2021, 6205 samples belonging to this malware family was added, from which 1342 unique configurations of this trojan were obtained.

Formbook is a multi-function trojan operating in Windows systems and facilitating the stealing of login data from forms, both in browsers and email software. Its features also include monitoring the key strokes and the clipboard, as well as remotely taken screenshots from an infected device.

It was initially observed at the beginning of 2016⁸⁶, and was available for purchase in the “malware-as-a-service” (MaaS) form allowing access to the compiled software and C&C panel running on its author’s server. Additionally, the source code of the panel itself was put up for sale to run it on one’s own server. After the first year of operation, the author abruptly stopped selling this malware, citing the use of the program in malicious campaigns as the reason. However, this did not stop criminals with access to the C&C panel source code from continuing to use the purchased tool, and Formbook itself became one of the most popular malware families⁸⁷.

86. <https://www.virusbulletin.com/uploads/pdf/magazine/2018/VB2018-Nicolao.pdf>

87. <https://any.run/malware-trends/>



The image is a promotional graphic for FormBook 0.3. At the top, there is a dark blue background with a network of yellow and red lines. In the center, a grey book-like icon with a face and the letters 'FB' is shown, with the version number '0.3' in pink to its right. Below this is a dark blue section with the word 'ABOUT' in white. The text describes FormBook as advanced internet activity logging software coded in low-level language (ASM/C), designed for extensive and powerful internet monitoring. Below this is a pink horizontal bar with the word 'FEATURES' in white. A list of features follows, including being coded in ASM/C, hidden startup, PE-injection, Ring3 kit, balloon executable, no suspicious windows API, thread-safe hooks, encrypted communication, install manager, file browsing, full Unicode support, and supported browsers (HTTP, HTTPS, SPDY, HTTP/2, keystroke, clipboard, and password recovery).

ABOUT

FormBook is advance internet activity logging software coded in low level language ASM/C which means it does not require any dependency to work perfectly on all versions of windows. FormBook is designed with aim to give you extensive and powerful internet monitoring experience with its ultimate stability alongside flexibility that is above the edge of all existing monitoring/spy tools.

FEATURES

- Coded in ASM/C (x86_x64)
- Startup (Hidden)
- Full PE-Injection (No dll/ No drop/ both x86 and x64)
- Ring3 kit
- Bin is Balloon Executable (MPIE + MEE)
- Doesn't use suspicious windows API
- No blind hook, all hooks are thread safe including the x64, so crash is unlikely
- All communication with panel are encrypted
- Install Manager
- File Browsing (FB-Connect)
- Full Unicode-Support
- Supported Browsers:
HTTP, HTTPS, SPDY, HTTP/2, KEYSTROKE, CLIPBOARD & PASSWORD RECOVERY (both 32bits and 64bits browser)

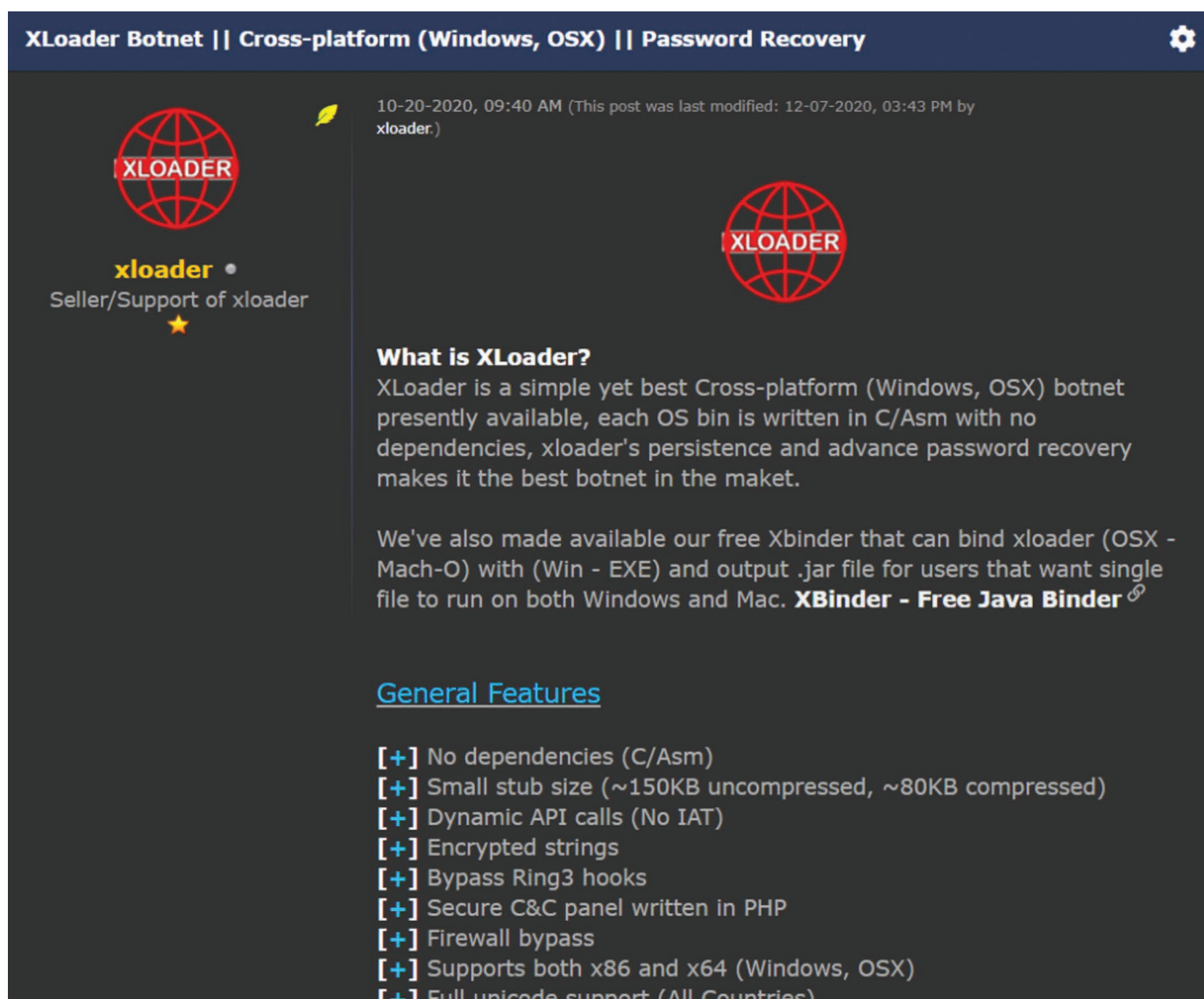
Fig. 53. Formbook sales offer⁸⁸.

After four years, i.e. in 2020⁸⁹, the forum featured an ad for a new trojan called Xloader, which, when analysed, showed numerous similarities to the previously sold Formbook. Unlike in the previous case, the trojan was published in two versions -

for Windows and MacOS devices. In addition, the seller renounced the sale of the panel source code and allowed only time-limited access to the tool. Since that time, the Formbook and Xloader names have been used interchangeably.

88. <https://www.mandiant.com/resources/formbook-malware-distribution-campaigns>

89. <https://blog.checkpoint.com/2021/09/10/august-2021s-most-wanted-malware-formbook-climbs-into-first-place/>



XLoader Botnet || Cross-platform (Windows, OSX) || Password Recovery

10-20-2020, 09:40 AM (This post was last modified: 12-07-2020, 03:43 PM by xloader.)

xloader •
Seller/Support of xloader

What is XLoader?
XLoader is a simple yet best Cross-platform (Windows, OSX) botnet presently available, each OS bin is written in C/Asm with no dependencies, xloader's persistence and advance password recovery makes it the best botnet in the market.

We've also made available our free Xbinder that can bind xloader (OSX - Mach-O) with (Win - EXE) and output .jar file for users that want single file to run on both Windows and Mac. **XBinder - Free Java Binder**

General Features

- [+] No dependencies (C/Asm)
- [+] Small stub size (~150KB uncompressed, ~80KB compressed)
- [+] Dynamic API calls (No IAT)
- [+] Encrypted strings
- [+] Bypass Ring3 hooks
- [+] Secure C&C panel written in PHP
- [+] Firewall bypass
- [+] Supports both x86 and x64 (Windows, OSX)
- [+] Full unicode support (All Countries)

Fig. 54 XLoader sales offer⁹⁰.

The infection vector most common for this malware family comprises attachments in phishing emails, often impersonating existing businesses. These messages request users to pay outstanding invoices or shipping fees for ordered goods. Increasingly, hyperlinks directing to a malicious file download site are added, instead of an

attachment. Fig. 56 shows a message taken from a campaign impersonating the BPS bank, in which, after clicking the image (being also a hyperlink), an ISO format archive was downloaded. After unzipping it and running the embedded executable file, a device was infected with Formbook/Xloader family malware.

90. <https://research.checkpoint.com/2021/top-prevalent-malware-with-a-thousand-campaigns-migrates-to-macos/>

From Bank Polskiej Spółdzielczości S.A. <sales@cobra-europa.eu> ☆
 Subject: Bank Polskiej Spółdzielczości S.A. Alert Powiadomienia o Płatności Faktury

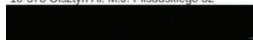
Witam,

Wysyłamy potwierdzenie wysłania przelewu za pośrednictwem bankowości elektronicznej Banku Polskiej Spółdzielczości S.A. na kwotę: 70 543,13 zł, tytuł: Zapłata faktury;
 nadawcą przelewu jest: Broekman Logistics Sp. ogród zoologiczny.

Załączone informacje o płatności są wydawane na życzenie naszego klienta.



Oddział w Olsztynie
 10-578 Olsztyn Al. M.J. Piłsudskiego 32



Bank Polskiej Spółdzielczości S.A.
 KRS 0000069229, Kapitał zakładowy i wpłacony 438 025 241,00 zł
 NIP 896-00-01-959, REGON 930603359
 Pomyśl o środowisku zanim wydrukujesz ten e-mail.

Uwaga: niniejsza wiadomość przeznaczona jest wyłącznie dla jej adresata i może być poufna. Jeśli nie jest Pani/Pan adresatem, prosimy o poinformowanie nadawcy i skasowanie wiadomości. Rozpowszechnianie, kopiowanie lub inne działanie o podobnym charakterze jest zabronione.



Fig. 55 Example of a message exploiting the BPS image⁹¹.

91. https://twitter.com/CERT_Polska/status/1433359784569364483/photo/1



STATISTICS

In this section of our report, we present statistics related to incidents that are automatically processed, mostly using the n6 platform⁹². They concern vulnerable systems, probable infections or successful attacks in Polish networks, which were detected by automatic scanners and then reported to CERT Polska. The data is aggregated, standardised and made available to selected network administrators or relevant CSIRT teams, via the n6 platform.

Statistical accuracy and limitations

We have made every effort to ensure that the image resulting from the statistics presented accurately describes all large-scale threats. One must not forget, however, that there are certain limitations, mainly due to the nature of the available source data. First of all, it is not possible to collect full information on all types of threats, which is best exemplified by attacks targeting specific entities or user groups. Unlike mass attacks, these exploits are usually not registered by our monitoring systems or reported to our team. The problem with accurate presentation of the current state of affairs also results from the fact that a threat can be active – even for a long time – before it is investigated and regular monitoring is initiated. For example, the number of infected computers encompassed by a botnet may be difficult to determine before it is neutralised by taking over the command and control infrastructure (C&C). Another important issue is to be able to determine the scale of a given threat, which is most often achieved by counting the associated IP addresses observed throughout the day. Thus it is assumed that the number of addresses is close to

the number of affected devices or users. Obviously, this measure is imperfect due to the widespread use of two mechanisms affecting visible public addresses, i.e.:

- NAT (address translation) causing underestimation, because there are often multiple computers behind a single external IP address;
- DHCP (dynamic addressing) causing overestimation, because the same infected computer can be detected several times in one day with different addresses.

One might suspect that the influence of both mechanisms on the aggregated results is largely cancelled, but a thorough examination of the NAT and DHCP impact in this context would require a separate analysis. The final remark concerns the IP protocol version, i.e. all the statistics given refer to the fourth version of this protocol. This is due to the still minor degree of IPv6 implementation in Poland and, what follows, due to the negligibly small number of reports we receive regarding this type of addresses.

Botnets

In this section, statistical data related to botnet activity is presented. It must be unambiguously stated that the data presented includes only recognised and monitored botnets, for which relevant data is available.

Botnets in Poland

Table 5 presents the number of infected computers in Polish networks. In 2021, we collected information concerning 439,077 (in total) zombie IP addresses. It constitutes a drop by approximately 200,000 in relation to 2020.

92. n6.cert.pl/en/

	Family	Daily maximum value	Daily average value	Standard deviation
1	Andromeda	3 139	1 927	498
2	Avalanche	2 028	867	296
3	Conficker	1 962	832	360
4	Flubot	1 638	122	218
5	QSnatch	1 192	939	170
6	Nymaim	1 044	90	178
7	Hummer	833	391	177
8	ISFB	816	438	180
9	Mirai	752	334	144
10	Necurs	558	309	103

Table 5. Largest botnets in Poland.

For many years now, we have been observing the activity of botnets that are already sinkholed within Polish networks. The Andromeda botnet is a perfect example, which is once again at the top of the above-mentioned list, with an average daily number of infected devices reaching almost 2,000. Here, similarly to 2020, we observed steady further decreases during the year. At the beginning of the year, average values reaching 2500 IP addresses were reported; however, at the end of the year, the value decreased to the level of 1500 IP addresses. The downward trend was also recorded as far as QNAP Systems infections with the Qsnatch botnet are concerned. The decrease amounted to 500 IP addresses, in comparison to values recorded in January and December 2021. As regards Avalanche and Conficker, a downward trend was also visible. Once again, the list contains the IoT Mirai botnet.

Monthly, on average 334 IoT devices with IP addresses were infected with this botnet family. It constitutes an improvement by approximately 200 devices in relation to 2020.

Botnet activity broken down by telecoms operators

Chart 6 presents the degree of infection of users in largest telecommunications operator networks. It has been estimated based on the daily number of infected IP addresses. The degree of infection is determined by dividing the number of bots by the number of customers using Internet access services provided by a given operator. We also used data presented in the “Report on Polish telecommunications market in 2020” published by the Office of Electronic Communications⁹³.

93. https://www.uke.gov.pl/download/gfx/uke/pl/defaultaktualnosci/36/391/10/raport_o_stanie_rynku_telekomunikacyjnego_w_polsce_w_2020_roku_.pdf

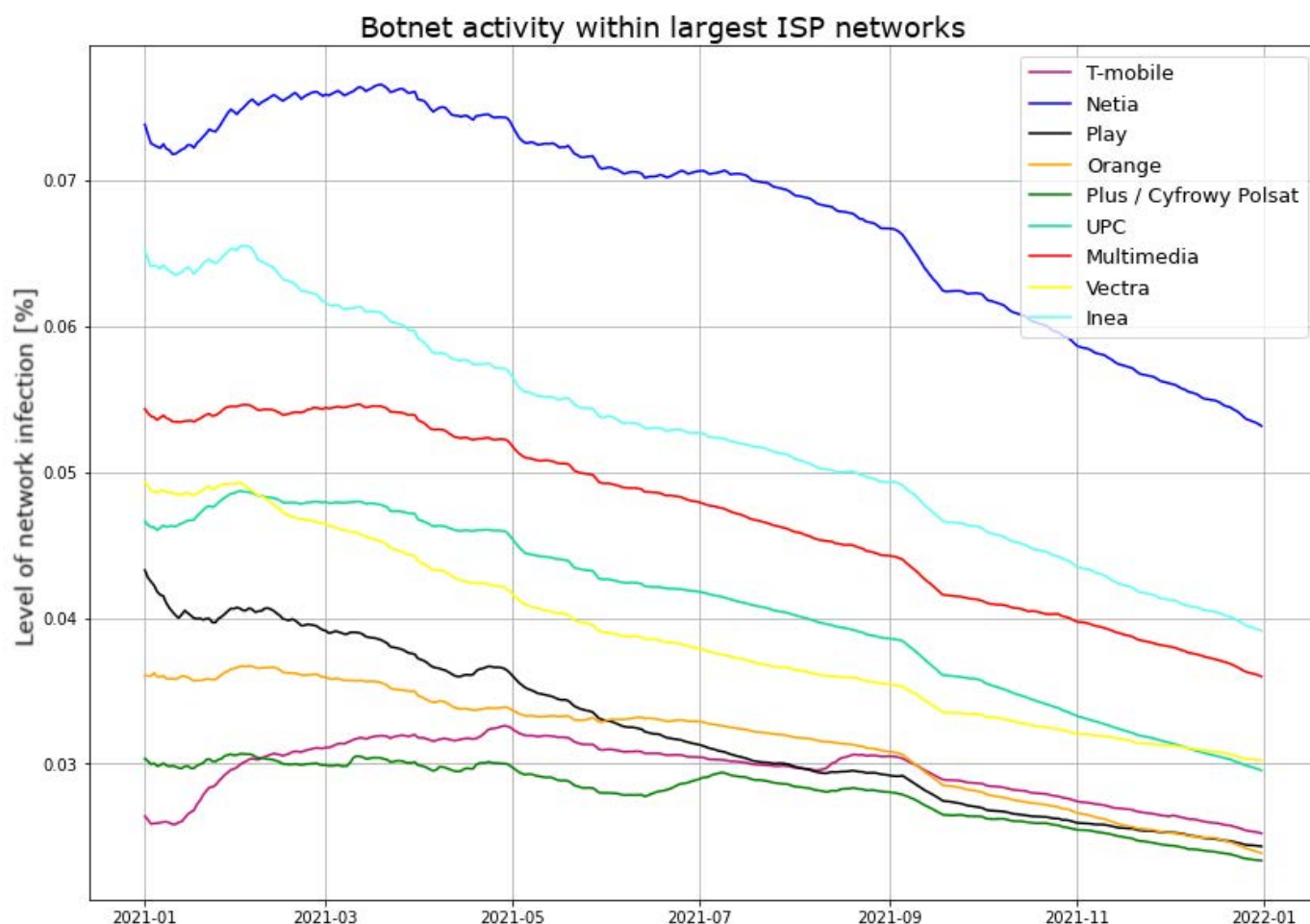


Chart 6. Botnet activity within largest ISP networks in 2021.

In 2021, the average daily number of infected devices within the Polish Internet amounted to 6621. During the year, a steady downward trend could be observed. In January 2021, the degree of infections in Polish networks was approximately 9,000 devices. In the middle of the year, the number of infected devices reached a level of approximately 7,000, to subsequently fall to a level of 4,000 by the end of the year.

Similarly to previous years, the largest estimated percentage of infected users were present in the Netia networks. As for this ISP, a decreasing trend was retained. The significant decrease in the degree of network infection over the year also applied to the remaining Polish providers, which constitutes a favourable change, because the downward trend last year was not so pronounced. For each of the operators, the infection rate did not exceed one per thousand.

As for the Andromeda botnet, the highest number of infected devices was observed in Orange, Plus and Cyfrowy Polsat networks. The daily number of IP addresses remains steady at a level of above 300 addresses. The largest number of infected NAS devices is present in the Orange (250 devices on average) and UPC (150 devices on average) networks. Conficker botnet infections are most widespread in Orange and Netia (100 devices on average in both cases). Similarly to the previous year, Mirai botnet infections were observed mostly in the Orange networks. In other networks, the share of Miraiem infections was negligible.

C&C servers

In 2021, we collected information regarding 9410 IP addresses likely used as botnet management (Command & Control) servers. Due to the nature of the threat, we decided to describe the problem in relation to IP address locations and the top-level domain (TLD) of the C&C domain name. The sta-

tistics exclude reports on CERT Polska sinkhole servers that we use to disable botnets and detect infected machines. As in previous years, most malicious servers were located in the United States (33%). 68% of all C&C servers were maintained in 10 countries – see Table 6. We observed such servers in 136 countries all over the world.

Item	Country	Number of IP addresses	Share
1	USA	3 089	32,83%
2	The Netherlands	694	7,38%
3	Germany	566	6,01%
4	Russia	465	4,94%
5	Thailand	412	4,38%
6	China	326	3,46%
7	Great Britain	225	2,39%
8	France	212	2,25%
9	India	183	1,94%
10	Hong Kong	182	1,93%
...
30	Poland	59	0,63%

Table 6. Countries with largest numbers of C&C servers.

We observed 1580 various autonomous systems (AS) where C&C servers were embedded. Ten autonomous systems contained more than 28% of all

malicious servers. The table below indicates that cybercriminals choose large hosting companies to maintain their infrastructure.

Item	AS number	Name	Number of IP addresses	Share
1	13,335	Cloudflare	727	7.73%
2	14,061	DigitalOcean	353	3.75%
3	45,629	JasTel	314	3.34%
4	16,509	Amazon	271	2.88%
5	36,352	ColoCrossing	203	2.16%
6	15,169	Google	181	1.92%
7	16,276	OVH	172	1.83%
8	9009	M247	158	1.68%
9	213,035	Des Capital	154	1.64%
10	46,606	Unified Layer	143	1.52%

Table 7. Autonomous systems with largest numbers of C&C servers.

In Poland, C&C servers were active at 59 different IP addresses (30th place in the world, with a share of 0.63%) in 34 autonomous systems. Table 8 summarises autonomous systems where the biggest

numbers of malicious botnet management servers were located. In total, they amounted to almost 60% of all C&C servers in Poland.

Item	AS number	Name	Number of IP addresses	Share
1	204,957	Green Floid	7	11.86%
2	20,940	Akamai	7	11.86%
3	51,290	Hosteam	3	5.08%
4	16,625	Akamai	3	5.08%
5	21,021	Multimedia	3	5.08%
6	57,509	L&L	2	3.39%
7	12,824	home.pl	2	3.39%
8	197,226	Sprint	2	3.39%
9	12,912	T-Mobile	2	3.39%
10	35,787	Internet Cafe	2	3.39%
11	201,814	Meverywhere	2	3.39%

Table 8. Autonomous systems in which the largest number of C&C servers are hosted in Poland.

We were also notified of 6,291 Fully Qualified Domain Names (FQDN) operating as botnet management servers. They were registered within 222 top-level domains (TLD), 58% of which within .com.

See Table 9 for a list of most common TLD. 6 .pl domains were used as C&C servers.

Item	TLD	Number of domains	Share
1	.com	3,645	57.94%
2	.net	321	5.10%
3	.xyz	313	4.98%
4	.org	277	4.40%
5	.ru	169	2.68%
6	.id	140	2.22%
7	.info	58	0.92%
8	.club	54	0.86%
9	.on-line	52	0.83%
10	.top	44	0.70%
...
54	.pl	6	0.10%

Table 9. Top-level domain in which C&C servers are registered.

Phishing

This sub-section only includes statistics on phishing in the traditional sense of the word, i.e. impersonation of well-known brands, using email and websites to phish for sensitive data. We do not address either phishing with malware or impersonation of invoice providers, e.g. for malware distribution purposes.

In 2021, we obtained 18,852 (in total) reports on phishing activity in Polish networks. They concerned 7508 URL addresses with 4076 domains which were divided into 1002 IP addresses. This means that the number of systems located under Polish addresses and constituting the phishing infrastructure is lower in comparison with the previous year. While analysing results for individual autonomous systems, the significant number concerning home.pl is noticeable, probably due to its commercial offer also being attractive for cybercriminals.

Item	AS number	AS name	Number of IP addresses	Number of domains
1	12,824	home.pl	293	902
2	15,967	Nazwa.pl	164	346
3	20,940	Akamai Technologies	73	34
4	16,625	Akamai Technologies	57	115
5	41,079	H88	39	795
6	16,276	OVH	26	54
7	203,417	LH.pl	25	196
8	29,522	KEI.PL	24	45
9	57,367	Atman	21	36
10	43,641	Sollutium	21	31

Table 10. Polish autonomous systems with largest numbers of phishing sites.

Malicious pages

Last year, we collected information on 2,915,585 URL addresses related to malware activity, 47,742 of which were within the .pl domain, and 43,125 were distributed to Polish IP addresses.

As far as URL addresses are concerned, the most popular second-tier domain within the .pl domain was home.pl (5328 occurrences).

Similarly, we collected information on 266,748 domain names, 3754 of which were within the .pl domain, and 3154 were distributed to Polish IP addresses. See Table 11 for the most popular IP addresses at which these domains were located.

As far as domain names are concerned, the most commonly present second-tier domains within the .pl domain included *com.pl* (237 occurrences), *home.pl* (177 occurrences) and *neostrada.pl* (131 occurrences).

Item	Number of .pl domains	IP address	ASN	Name
1	141	217.97.216.17	5,617	Orange
2	103	3.121.154.182	16,509	Amazon
3	89	91.212.150.245	43,350	nForce
4	71	172.67.169.11	13,335	Cloudflare
5	71	104.21.27.72	13,335	Cloudflare
6	57	37.59.49.187	16,276	OVH
7	56	176.31.124.7	16,276	OVH
8	21	212.180.187.186	9,085	Supermedia
9	18	195.78.67.35	41,079	Cyber Folks
10	17	5.252.231.39	203,417	LH.pl

Table 11. IP addresses hosting the largest number of malware-related .pl domains.

Item	Number of IPs	ASN	Name	Percentage of all addresses in AS	Share
1	211,824	4837	China Unicom	0.36%	36.78%
2	67,017	9829	National Internet Backbone	1.24%	11.64%
3	43,327	4134	Chinanet	0.04%	7.52%
4	29,681	17,816	China Unicom	0.76%	5.15%
5	28,262	8661	Telekomi i Kosoves	67.32%	4.91%
6	24,406	13,335	Cloudflare	1.53%	4.24%
7	18,708	17,622	China Unicom	2.66%	3.25%
8	15,241	17,488	Hathway	1.52%	2.65%
9	7,518	17623	China Unicom	1.15%	1.31%
10	6,836	46,606	Unified Layer	0.53%	1.19%

Table 12. Autonomous systems in which the largest numbers of malware-related IP addresses were located.

Services facilitating DRDoS attacks

In 2021, we were informed of 614,404 IP addresses located in Poland where services facilitating Distributed Reflection Denial of Service (DRDoS) attacks operated. See below for the list of services that could have been used for attacks and were the most represented in the Polish Internet. They are discussed further in the report.

We took into account IP addresses at which misconfigured services are actually available, as well as services that are available intentionally (e.g. public open resolvers) and honeypot systems, as it is difficult to distinguish between them on the basis of Internet scanning data and their total number is small.

A size of an autonomous system (AS) was established on the basis of RIPE data valid as of 1 July 2021.

Item	Name of vulnerability / open service	Average daily number of IP addresses	Daily maximum number of IP addresses	Standard deviation	Observation time
1	resolver	31,920	43,039	4862	97.80%
2	SNMP	26,291	31,352	2619	97.53%
3	portmapper	17,453	23,045	1428	95.34%
4	SSDP	15,659	18,817	1,422	96.43%
5	NTP	15,646	17,787	618	97.26%
6	NetBIOS	11,613	13,437	763	96.43%
7	mDNS	4,127	5,117	398	95.34%
8	mssql	2,512	3,311	515	95.89%
9	chargen	181	292	54	97.26%
10	qotd	40	61	9	95.06%
11	xdmcp	11	33	7	97.26%

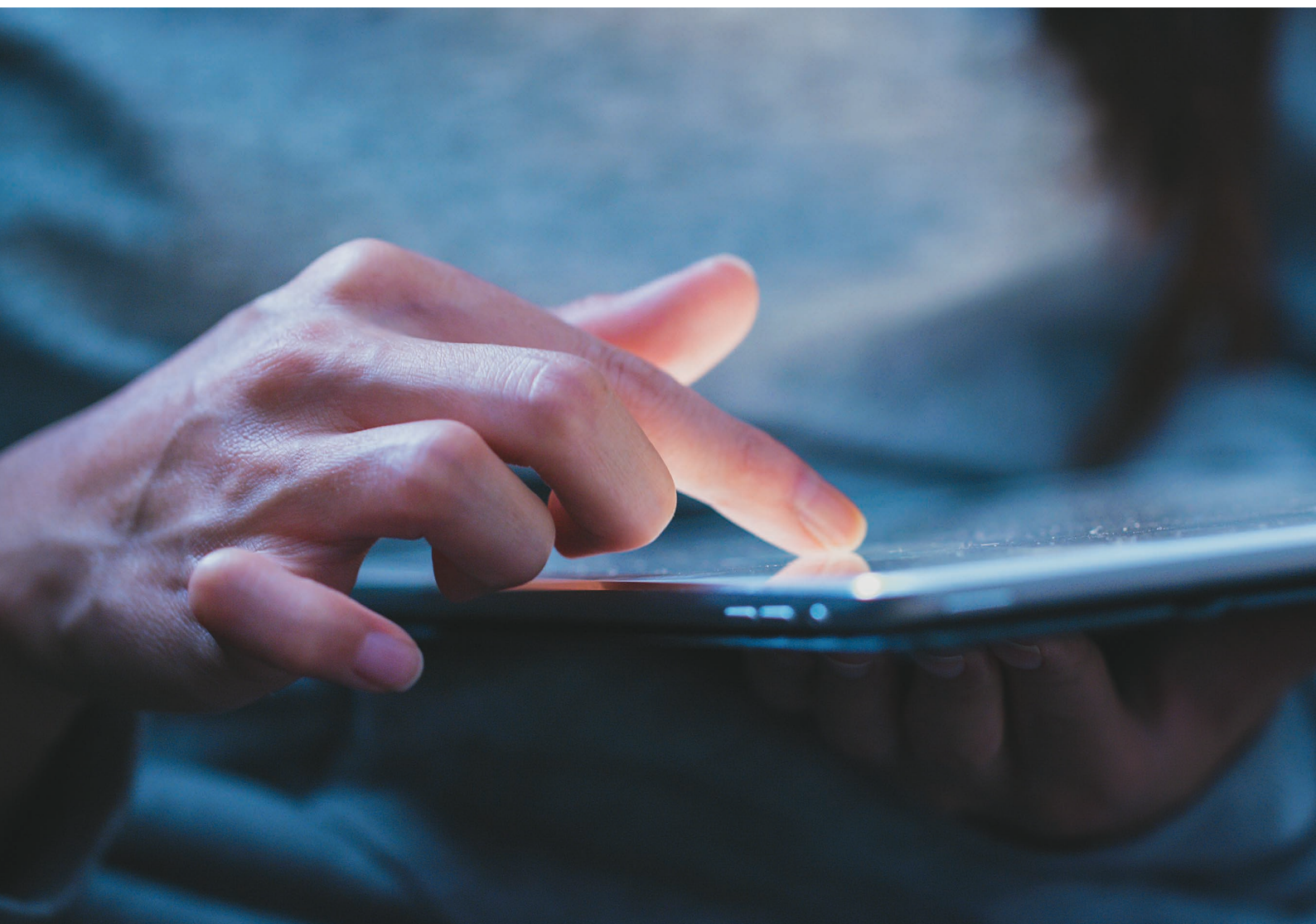
Table 13. List of most common misconfigured services that can be used for DRDoS attacks. The standard deviation value refers to the variation in the daily number of IP addresses observed over the year, and the total observation time corresponds to the part of the year for which we had information regarding a particular service.

When analysing data on services facilitating DRDoS attacks and services with known vulnerabilities in 2021, we used a methodology similar to that first introduced in the 2020 report. Also in 2021, we had incomplete data from some autonomous systems at certain periods of time. The problem concerned mainly of the autonomous systems belonging to Orange (AS5617). We have noted extensive daily variations in the number of IP addresses, alternating periods of this number decreasing and increasing and related lack of stability. According to our analysis, the most probable reason for this situation is that Orange blocked some queries generated by large-scale Internet scans performed by the Shadowserver foundation, which is the main provider of data on incorrectly configured and compromised network services (more details on Shadowserver's activities are available on the organisation's website⁹⁴). The problem affects all the services analysed and, as

in many cases the share of AS5617 in the total number of IP addresses for a given service is large, it significantly affects the aggregate statistics. We decided to correct the data using the method described in detail in the 2020 report. If you are interested, we encourage you to read the 2020 report for details. Next, tables and charts provided in the report were developed on the basis of the corrected data.

Chart 7. presents the forecast trend for the number of observed devices that can be used to run DRDoS attacks during a year. The charts refer to seven most frequently reported services.

The positive trend consists in the gradual decrease of the number of devices related to the resolver, SNMP, portmapper and SSDP services over the entire year. As for NTP, Netbios and mDNS services, the number of IP addresses remains at a similar level throughout the year.



94. <https://www.shadowserver.org/what-we-do/>



Chart 7. Most widespread misconfigured services that can be exploited in DRDoS attacks. The chart shows variations in the numbers of vulnerable IP addresses in Poland in 2021.

Open DNS servers

Similarly to previous years, in 2021 open DNS servers (open resolvers) were the most popular services facilitating DRDoS attacks. Despite their key role in the entire Internet operation, a 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 2021, we received 11,250,637 reports concerning 164,009 IP addresses with activated open resolvers, which constitutes a decrease (i.e. a slight improvement) by less than 10% of addresses in comparison with 2020. Currently, the daily average number of addresses is 31,920. Throughout 2021, we noted a gradual decrease in the daily number of IP addresses featuring this service. Similarly to previous years, the list of autonomous systems with the highest number of addresses was topped

by AS5617, i.e. the Orange network. For this autonomous system, a positive trend can be noticed in the decrease in the daily average number of IP addresses. This autonomous system had the main impact on the decrease in the daily average number of addresses with open resolvers calculated for all systems. As far as the other autonomous systems presented are concerned, the daily number of IP addresses remains constant during a year or the changes are insignificant. As for AS15969, the high percentage of addresses (10%) that can be exploited to carry out a DRDoS attack is alarming. The situation is even worse in the case of AS200889, in which over 50% of IP addresses are vulnerable. In comparison with 2020, the decrease in the number open resolvers in the Netia (AS12741) network can be observed again, i.e. the average daily number fell by 124 year-on-year.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	5617	Orange	19,241	28,949	0.35%
2	12,741	Netia	1,215	1,480	0.07%
3	6,830	UPC	461	518	0.01%
4	13,110	Inea	409	470	0.24%
5	29,314	Vectra	321	387	0.06%
6	15,969	SYSTEMIA	301	347	9.80%
7	5,588	T-Mobile	283	339	0.02%
8	12,912	T-Mobile	283	372	0.04%
9	8,374	Plus / Cyfrowy Polsat	280	317	0.02%
10	200,889	MARIANWITEK	276	320	53.91%

Table 14. Daily number of IP addresses at which an open DNS server was detected, broken down into autonomous systems.

SNMP

The Simple Network Management Protocol (SNMP) has been created for remote management of network devices. Its use is recommended only in isolated networks that are to be managed. An SNMP-based service visible on the Internet poses a threat of unauthorised access to a device or can be exploited for DDoS attacks.

In 2021, we received 9,094,972 reports concerning 155,046 addresses with activated SNMP, i.e. the number of addresses decreased by approximately 23% in relation to 2020. The key indicator, i.e. the daily average number of occurrences, was 26,291 addresses, i.e. the number increased by about

12% each year. Netia's AS12741 is at the top of the list, again. While analysing data collected only in 2021, a downward trend was visible, particularly at the end the year. It resulted mostly from the rapid decrease related to Netia's AS12741 that might have been caused by alterations in device configurations within its autonomous system. In 2021, Digicom (AS57978) appeared on the list for the very first time, featuring a high percentage of addresses in AS. A slight increase over the year was visible only in the case of this provider. The high percentage of addresses in the Net Center autonomous system (AS60920) is again a cause for alarm, as over 22% of IP addresses broadcast by this system came with an SNMP instance open to Internet access.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	12,741	Netia	8,630	10,955	0.52%
2	5,617	Orange	2,857	3,476	0.02%
3	20,804	TELENERGO	875	960	0.36%
4	60,920	NETCENTER	691	763	22.49%
5	56,515	OXYNET	505	659	3.79%
6	202,281	C3	422	888	8.24%
7	199,390	ALFAKS	400	998	13.02%
8	4	ISI	358	419	0.55%
9	8,374	Plus / Cyfrowy Polsat	329	381	0.02%
10	57,978	DIGICOM	324	452	15.82%

Table 15. Daily number of IP addresses at which an active SNMP service was detected in a publicly available interface, broken down into autonomous systems.

Portmapper

Portmapper is a low-level service typical for Unix operating systems. It is utilised by higher-layer protocols, including NFS (Network File System). A publicly available portmapper can be exploited for DDoS attacks.

In 2021, we received 5,954,751 reports concerning 64,713 IP addresses with the portmapper service available at a public interface. The daily average amounted to 17,453 addresses, i.e. decreased by almost 7% in comparison with 2020. In mid-February 2021, a drop from the level of approximately 21,000 addresses to 18,000 addresses could be observed. This number remained almost unchanged

in the later part of the year, with a slight downward trend, finally reaching a level approximately 16,000 IP addresses in December. The rapid decrease was caused by the AS61317 system placed at the top of our list. Such situations may result, for example, from updating the configurations of machines at these service providers or introducing required traffic filtering rules. As far as the remaining autonomous systems are concerned, the situation was quite stable, with a slight downward trend. Similarly to 2020, ATMAN (AS57367) and OVH (AS16276) are high on the list with an average number of IP addresses similar to the one recorded in the previous year. Data Space (AS57367) with a high percentage of infected IP addresses (almost 7%) is a new entry on the list.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	61,317	ASDETUK	2,559	5864	0.24%
2	57,367	ATMAN	1,330	1400	8.12%
3	50,599	Data Space	841	1049	6.70%
4	16,276	OVH	825	1,085	0.02%
5	5,617	Orange	712	1,147	0.01%
6	20,804	TELENERGO	604	885	0.25%
7	59,491	LIVENET	414	689	5.78%
8	47,329	WDM	406	422	4.17%
9	12,741	Netia	391	453	0.02%
10	197,155	ARTNET	339	418	3.01%

Table 16. Daily number of addresses at which an active Portmapper service detected at a publicly available interface, broken down into autonomous systems.

SSDP

The Simple Service Discovery Protocol is a protocol used to detect devices, and it operates as part of the Universal Plug and Play (UPnP) standard. As a standard, SSDP is used in small local networks and should not be accessible from the Internet.

In 2021, we received 5,311,285 reports concerning 170,969 IP addresses related to the SSDP service. We noted a drop in the number of IP addresses by almost 7% in comparison with 2020. However, this decrease is not as significant as in 2020 and 2019, when it amounted to over 50%. The daily average number of occurrences amounted to 15,659 ad-

resses, constituting a decrease by over 20% in relation to the previous year. However, a gradual decrease in the number of IP addresses was noted throughout the year. The AS5617 system belonging to Orange was on the top of the list for another year in a row. As far as this autonomous system is concerned, we noted an irregular decrease in the number of IP addresses in mid-November 2021, i.e. from the level of 2,000 addresses to 500 addresses. Moreover, a high percentage of addresses in the autonomous system belonging to DERKOM (AS197697) must be noted again, as it amounted to 20% in 2021. It constitutes a significant year-on-year increase (about 12% during the previous year).

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	5,617	Orange	1,912	3,016	0.03%
2	197,697	DERKOM	1,732	2,051	21.14%
3	29,314	Vectra	1,119	1,638	0.21%
4	12,741	Netia	762	941	0.05%
5	8,374	Plus / Cyfrowy Polsat	529	615	0.04%
6	41,023	ARREKS	458	497	12.78%
7	50,231	SYRION	221	325	0.88%
8	31,242	TKPSA	213	370	0.19%
9	199,201	SPI-NET	213	291	6.93%
10	12,912	T-Mobile	206	239	0.03%

Table 17. Daily number of addresses at which an active SSDP service was detected in a publicly available interface, broken down into autonomous systems.

NTP

The Network Time Protocol (NTP) is a common time synchronisation protocol used in computer networks. However, publicly accessible NTP servers making the monlist command available can be exploited for DDoS attack purposes.

In 2021, we received 5,385,816 reports concerning 30,730 IP addresses, i.e. the number decreased by almost 8% year-over-year. One must remember that previously such decrease was much more

significant, i.e. amounting to approximately 85% of addresses. The daily average number of occurrences was 15,646 addresses. For this service, the daily number of IP addresses averaged around the same level throughout the year. Compared to the previous year, the number of addresses operating this protocol in the Orange autonomous system (AS5617) decreased by about 700 addresses. As far as Netia and T-Mobile companies are concerned (second and third position on the list), this number remained steady at a similar level.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	5,617	Orange	1,434	2,595	0.03%
2	12,741	Netia	1,430	1,651	0.09%
3	5,588	T-Mobile	1,056	1,203	0.08%
4	48,956	HYPERNET	358	505	7.77%
5	199,715	MSITELEKOM	350	394	2.24%
6	20,960	TKTELEKOM	320	352	0.13%
7	20,804	TELENERGO	257	379	0.11%
8	8,798	PAGI	253	394	2.82%
9	9,085	SUPERMEDIA	243	274	0.57%
10	31,242	TKPSA	242	312	0.21%

Table 18. Daily number of addresses at which an active NTP service was detected in a publicly available interface, broken down into autonomous systems.

NetBIOS

NetBIOS is a low-level protocol used mostly by Microsoft systems. It should only be used in local networks, and it poses a threat if it is accessible from a public network, and not just because the service can be exploited for DDoS purposes.

In 2021, we received 3,934,411 reports concerning 44,254 IP addresses, i.e. the number decreased by 10% in comparison with 2020. The daily average

number of occurrences was 11,613 addresses, i.e. the value decreased by over 8% in relation to the previous year. Throughout the year, we observed a steady number of IP addresses with the NetBIOS service activated. All the autonomous systems presented in the table below showed a similar pattern in relation to the overall chart. Similarly to 2020, the two top places are taken by autonomous systems belonging to Orange and Netia, with an average number of IP addresses comparable to the previous year.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	5,617	Orange	7,162	9,007	0.13%
2	12,741	Netia	612	722	0.04%
3	13,110	Inea	127	151	0.08%
4	12,824	home.pl	122	141	0.06%
5	8,267	CYFRONET	105	136	0.14%
6	8,374	Plus / Cyfrowy Polsat	94	124	0.01%
7	5,588	T-Mobile	77	95	0.01%
8	8,970	WASK WROCMAN	76	152	0.12%
9	31,242	TKPSA	76	91	0.07%
10	197,226	SPRINT	66	84	0.46%

Table 19. Daily number of addresses at which an active NetBIOS service was detected in a publicly available interface, broken down into autonomous systems.

Vulnerable services

This section presents statistics on services exposed to attacks and vulnerabilities in services that may result in information leaks. It includes services with known vulnerabilities as well as services that have not been configured correctly, allowing, for example, unrestricted access from the internet despite good security practices or access to applications without authentication. In 2021, we observed 45,199,753 such cases regarding 1,250,311 Polish IP addresses.

Further in the report, we present detailed information on threats that most frequently occur in Polish networks. The presented statistics are calculated in a manner analogous to the method discussed in the sub-section on services making DRDoS attacks possible. As regards vulnerable services, the same problem concerning low reliability of data obtained from AS5617 (Orange) occurred. For this reason, we employed the same estimation method.

The most common vulnerable services with the highest positions on the list include: RDP, Telnet and TFTP. Such services are most often protected by restricting access to them from external addresses; therefore, the public availability of a service may indicate a configuration error and a potential vulnerability. However, just the fact that a service is publicly available does not always mean that it is vulnerable. For example, accessibility of an RDP service from the Internet, provided its software is up-to-date and correct security mechanisms are enabled, does not constitute a vulnerability. However, this method of access should only be used when no other option is available. We recommend that VPN mechanisms providing additional protection of remote access services such as RDP or VNC should be deployed.

The above idea is more difficult to implement in the case of databases and similar applications (Memcached, MongoDB, Elasticsearch, Redis). In their case, public access almost certainly results from misconfiguration and should be treated as a vulnerability.



Item	Name of vulnerability / open service	Average daily number of IP addresses	Daily maximum number of IP addresses	Standard deviation	Observation time
1	CWMP	35,829	167,047	50,592	96.71%
2	SSL-POODLE	26,167	37,277	3,634	96.71%
3	RDP	14,178	22,656	2,205	96.98%
4	Telnet	13,269	20,344	2,236	96.34%
5	TFTP	11,599	17,958	2,593	95.06%
6	BadWPAD	9,109	13,030	1,465	99.17%
7	ISAKMP	5,698	7,563	560	95.89%
8	VNC	3,993	7,857	976	96.43%
9	SSL-FREAK	3,518	5,750	911	97.26%
10	SMB	3,162	4,532	472	97.26%
11	NAT-PMP	1,861	2,520	370	95.34%
12	IPMI	712	974	168	96.43%
13	MongoDB	563	607	26	96.16%
14	Memcached	173	198	19	96.71%
15	LDAP	83	110	10	96.43%
16	Elasticsearch	56	70	7	96.98%
17	Redis	38	61	8	96.43%

Table 20. List of most numerous services exposed to attacks, present in Poland. The standard deviation refers to the variation in the daily number of IP addresses observed over the year. The total observation time corresponds to the number of days during the year for which we had information concerning a given service.



In comparing 2021 with 2020, one may notice no changes regarding the first seven places on the list. The CWMP protocol still comes in first. However, one should note a significant change in the average daily number of IP addresses in this case. We observed a decrease of approximately 60,000.

Chart 8 shows the observed pattern of the number of devices hosting vulnerable services per year, created using the IP address count approximation method discussed above. The charts refer to seven most frequently reported services.

While analysing the chart, one may observe a positive trend consisting in gradual decrease in numbers of devices related to the Poodle vulnerability, as well as RDP and Telnet services, over the year. This continues the previous-year's downward trend. The CWMP service chart particularly draws attention. Here, by mid-February 2021, the number of IP addresses remained stable (at a level similar to the second half of 2020). From that time, a large decrease from around 160,000 to 15,000 could be observed. This resulted from the impact exerted by AS6830, belonging to UPC. In 2020, we observed a reverse situation in which rapid increase in the daily number of IP addresses occurred in the middle of the year, and it also resulted from data obtained from the above-mentioned autonomous system.

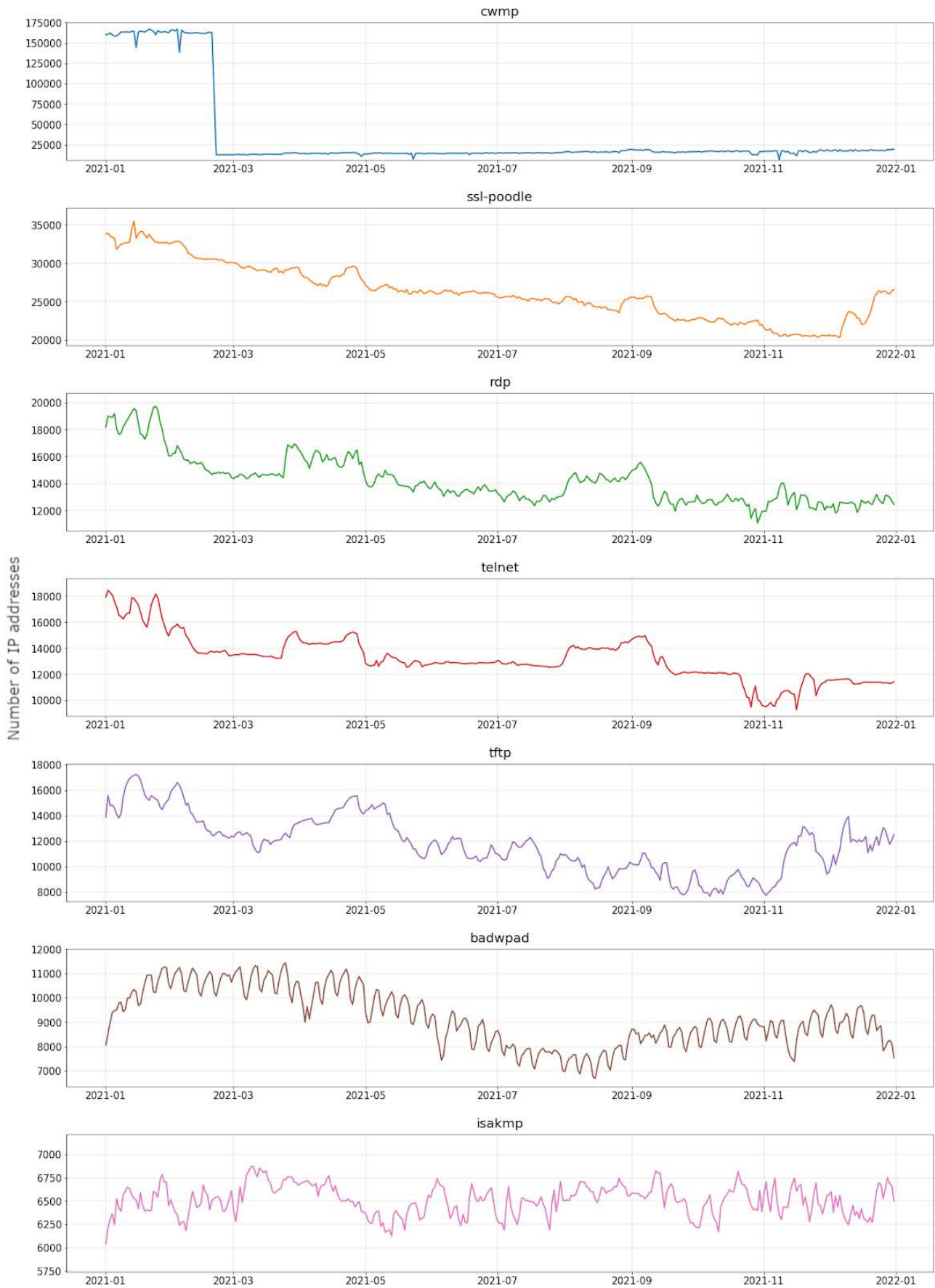


Chart 8. Most common services under threat. The chart shows variations in the numbers of vulnerable IP addresses in Poland in 2021.

CWMP

CWMP is a service based on the TR-069 specification, which is most often implemented in home DSL routers. It facilitates remote management of the device by operators, e.g. firmware updates. Incorrect implementation of this service allows an attacker to take complete control over a device. This vulnerability is exploited by, e.g. IoT botnets to infect consecutive devices.

In 2021, we received 12,238,412 reports concerning 597,642 IP addresses related to the publicly available CWMP service. It constitutes a drop by approximately 45% of addresses in comparison with 2020, and decreased by over 60% in comparison with 2019. The daily average number of addresses was 35,829, i.e. almost three times lower than in the previous year. The UPC's autonomous system (AS6830) had the most significant impact on such a decrease. In 2021, its daily average number of

addresses was over 20,000, down from the previous year when it amounted to about 58,000. This change was visible in mid-February when the number of addresses started falling from 160,000 down to approximately 15,000, and was retained to the end of the year. The significant share of AS6830 in the total number of IP addresses for the CWMP service determines the pattern for the general chart. The majority of the other autonomous systems in the table display an upward trend over the year. One should also note the T-Mobile's AS5588 system for which the number of IP addresses remained steady in 2021, after a rapid fall at the beginning of December 2020 to the level of a few hundred, which could reflect alterations in device configuration in this operator's autonomous system. The high percentage of vulnerable addresses in the INTERTOR (AS200125) network is quite alarming, as over 10% of all addresses in this autonomous system are vulnerable.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	6,830	UPC	20,217	151,247	0.51%
2	12,741	Netia	5,256	5,895	0.32%
3	5,617	Orange	3,192	4,826	0.02%
4	21,021	Multimedia	1,109	1,238	0.18%
5	5,588	T-Mobile	525	713	0.04%
6	44,124	RYBNET	521	1,066	3.63%
7	50,231	SYRION	452	970	1.80%
8	51,337	DEBACOM	420	641	6.84%
9	29,314	Vectra	386	527	0.07%
10	200,125	INTERTOR	326	442	10.61%

Table 21. Daily numbers of addresses at which a CWMP service was detected in a publicly available interface, broken down into autonomous systems.

SSL-POODLE

Known SSL/TLS protocol vulnerabilities are still quite common among users of the Polish Internet. POODLE is definitely the most popular one, and it facilitates attacks resulting in the disclosure of transmitted encrypted information.

We received 9,081,181 reports concerning 215,368 IP addresses. This value shows a drop by almost 19% addresses in comparison with 2020. The daily average number of addresses was 26,167, i.e. It

decreased by over 16% in comparison with the previous year. In the case of the majority of autonomous systems, we observed a gradual decrease in 2021, except for a slight increase in December. AS59958 (P.H.U MMJ) is an exception, as similarly to 2020, the number of addresses increased steadily in its case. As far as UPC (AS6830) is concerned, we noted an abrupt drop in early August, which may indicate changes in the device configuration in this operator's autonomous system. In 2020, this autonomous system experienced an abrupt increase during the year.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	12,741	Netia	4,940	6,534	0.30%
2	5,617	Orange	3,712	5,442	0.01%
3	6,830	UPC	1,517	2,540	0.04%
4	59,958	P.H.U MMJ	863	1,239	4.38%
5	43,939	INTERNETIA	678	890	0.26%
6	31,242	TKPSA	459	588	0.40%
7	5,588	T-Mobile	446	658	0.04%
8	13,110	Inea	354	479	0.21%
9	29,314	Vectra	352	501	0.07%
10	29,007	PETROTEL	338	450	2.06%

Table 22. Daily number of addresses at which an active SSL service with the POODLE vulnerability was detected, broken down into autonomous systems.

RDP

RDP (Remote Desktop Protocol) is a Microsoft ownership protocol facilitating remote access to graphic environments in the Windows systems. Although this protocol ensures convenient access to systems, we recommend that access to port 3389 on external interfaces should be closed.

In 2021, we received 4,978,071 reports concerning 96,335 IP addresses (decrease by almost 24% in comparison with 2020) at which the RDP service

available in a public interface was detected. The daily average number of addresses was 14,178 (decrease by about 40% in comparison with 2020). In most autonomous systems presented in the table, one may notice a slight downward trend analogous to the one shown in the general chart. The situation is reverse only in the case of OVH (AS16276), i.e. a slight increase in the number of addresses was noticed throughout the year.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	5,617	Orange	5,042	7,826	0.02%
2	12,741	Netia	1,090	1,382	0.07%
3	6,830	UPC	711	860	0.02%
4	12,912	T-Mobile	339	401	0.05%
5	8,970	WASK WROCMAN	329	402	0.50%
6	13,110	Inea	328	404	0.20%
7	8,374	Plus / Cyfrowy Polsat	324	395	0.02%
8	16,276	OVH	278	356	0.01%
9	204,957	GREENFLOID	261	442	2.08%
10	21,021	Multimedia	260	355	0.04%

Table 23. Daily number of addresses in which a RDP service was detected in a publicly available interface, broken down into autonomous systems.

TELNET

Telnet is an outdated communication protocol for remote terminal operation, i.e. a predecessor of the current SSH. Its complete lack of encryption is its biggest weakness, so it should not be deployed, particularly on public networks.

In 2021, we collected 4,640,545 reports concerning 115,656 IP addresses. It constitutes a drop by approximately 31,000 in comparison with the previous year. The average daily number of addresses was 13,269. It constitutes a drop by approximately

37,000 addresses in comparison with the previous year. For this protocol, the average daily number of addresses decreased or remained the same for most autonomous systems. AS35191 is the only exception, as there was slight increase in the first half of the year, after which the number of IP addresses remained relatively stable. Among the autonomous systems shown in Table 24, the C3 NET (AS202281) autonomous system can be negatively singled out again, in which approximately 13% of all broadcast addresses come with the available Telnet service.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	5,617	Orange	4,919	6,795	0.02%
2	12,741	Netia	2,662	3,331	0.16%
3	202,281	C3-NET	688	797	13.44%
4	35,191	ASTA-NET	406	612	0.70%
5	8,374	Plus / Cyfrowy Polsat	370	435	0.03%
6	12,912	T-Mobile	370	418	0.05%
7	21,021	Multimedia	310	402	0.05%
8	6,830	UPC	269	315	0.01%
9	13,110	Inea	238	261	0.14%
10	5,588	T-Mobile	222	270	0.02%

Table 24. Daily number of addresses at which a Telnet service was detected in a publicly available interface, 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 over the internet, as this may lead to information leaks.

We received 3,909,428 reports concerning 85,977 IP addresses with available TFTP. It constitutes a drop by approximately 19% in comparison with 2020, and decrease by over 60% in comparison with 2019. The daily average number of addresses

was 11,599, i.e. a drop by approximately 26%. The general chart does not show any upward or downward trend for the year as a whole. The number of IP addresses remains at a similar, stable level. It refers to all autonomous systems presented in the table. Similarly to the previous year, Orange's AS5617 is at the top of the list. High percentages of addresses within the autonomous systems belonging to the "Północ" Housing Cooperative in Częstochowa (AS198000) and WIFIMAX (AS199510) are particularly visible. The situation is similar to the one reported for the previous year.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	5,617	Orange	6,178	9,300	0.08%
2	198,000	SMPOLNOC	1,685	1,970	18.28%
3	12,741	Netia	520	618	0.03%
4	196,927	RTK	400	790	4.88%
5	21,021	Multimedia	300	336	0.05%
6	199,201	SPI-NET	285	617	9.28%
7	39,507	IPIVISION	194	243	0.52%
8	199,510	WIFIMAX	138	161	17.97%
9	42,673	SKYWARE	137	263	0.96%
10	200,125	INTERTOR	130	159	4.23%

Table 25. Daily number of addresses at which a TFTP service was detected in a publicly available interface, broken down into autonomous systems.

BadWPAD

BadWPAD is an attack exploiting the incorrect configuration of DNS suffixes in vulnerable machines. Potentially, it may allow the redirection of any HTTP requests by substituting fabricated proxy maintenance rules in a form of a PAC file downloaded automatically by the Web Proxy Auto-Discovery Protocol mechanism.

In 2021, we received 3,296,647 reports concerning 358,400 IP addresses where devices vulnerable to this attack were available. It constitutes a drop by approximately 30% in comparison with 2020. The daily average number of IP addresses was 9109, i.e. a drop by approximately 23%. Looking at the overall graph, we can observe a slight downward trend throughout the year, which is also evident for all autonomous systems presented in Table 26.

Item	AS number	AS name	Average	Maximum	Percentage of all addresses in AS
1	21,021	Multimedia	4,417	6,101	0.72%
2	35,191	ASTA-NET	468	676	0.80%
3	35,378	SATFILM	411	577	1.38%
4	12,741	Netia	349	507	0.02%
5	5,617	Orange	293	539	0.01%
6	44,061	SMSNET	239	350	1.11%
7	43,118	EAW	203	275	0.27%
8	29,314	Vectra	199	4,454	0.04%
9	30,975	TKK	174	243	0.71%
10	6,830	UPC	174	289	0.01%

Table 26. Daily number of addresses of devices vulnerable to the BadWPAD attack, broken down into autonomous systems.



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

