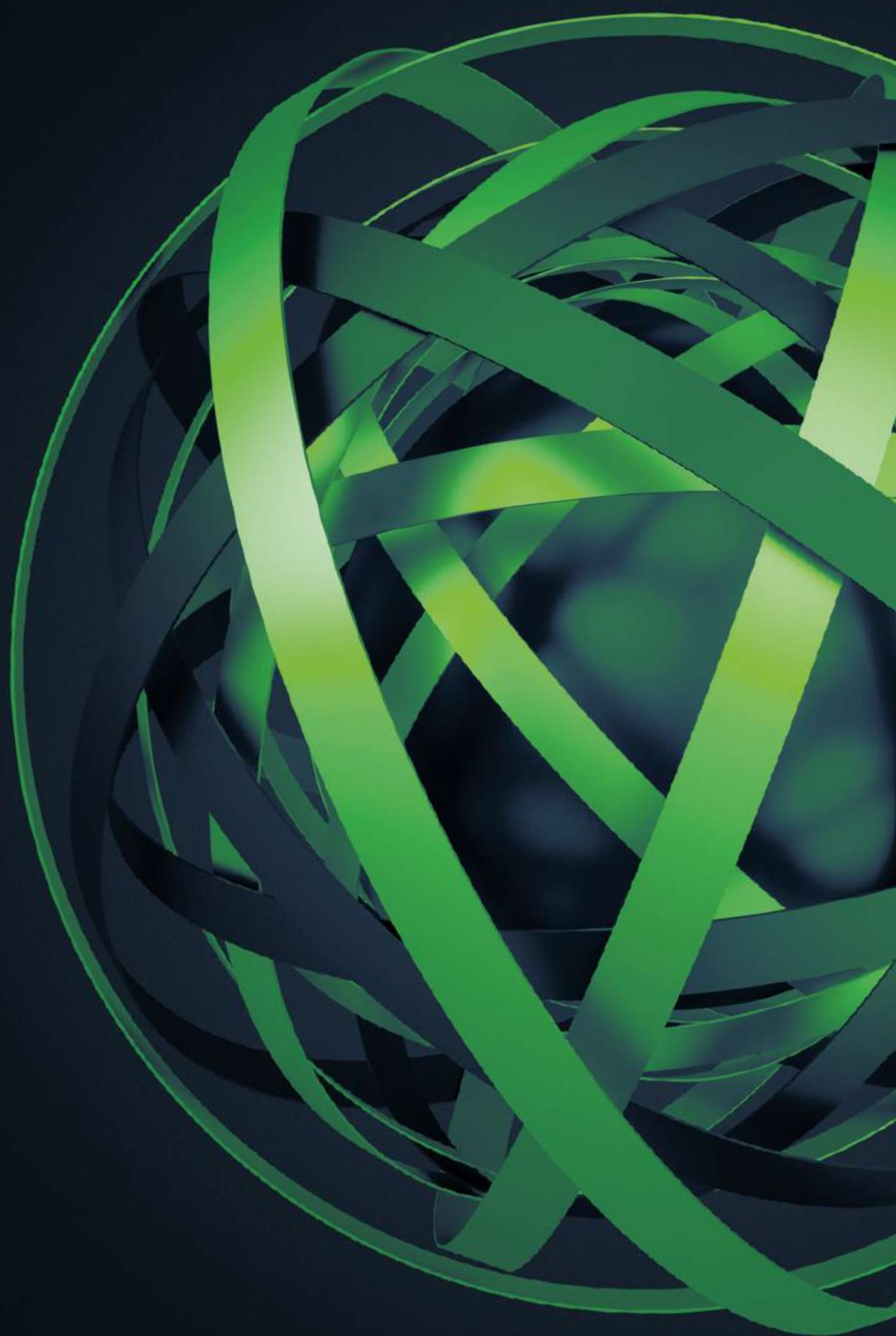


ANNUAL REPORT 2024

from the actions of CERT Polska

The Polish security landscape



TITLE: Annual report from the actions of CERT Polska 2024.
The Polish security landscape.

AUTHORS: CERT Polska team

©NASK National Research Institute

Warsaw 2025

ISBN: 978-83-68356-09-0

This publication is distributed under the terms of the Creative Commons
Attribution – (CC BY) 4.0 International Licence

National Research Institute NASK
12 Kolska Street
01-045 Warsaw

Table of contents

Introduction	4
About CERT Polska	5
Calendar	7
Incidents and threats	13
Overview of new campaigns	14
Ransomware	17
Major vulnerabilities in 2024	22
Data leaks	28
Observed activities of APT groups	31
Fraudulent advertising on major online platforms	37
Mobile malware	41
Activities of CERT Polska	43
The Act on Combating Abuse in Electronic Communications	44
CERT Polska in the mObywatel application	46
The Warning List	48
CERT Polska as a CVE Numbering Authority	49
Education and promotion – we continue our efforts to build cybersecurity awareness among Poles	52
SECURE	55
#BezpiecznyPrzemysł (Safe Industry)	56
Web application audits	59
Locked Shields 2024	62
ECSC 2024	63

- Projects 66**
 - Artemis 67
 - moje.cert.pl 68
 - MWDB 69
 - Snitch 69
 - DNS4EU 73
 - JTAN 75
 - FETTA 81

- Statistics 83**
 - Incidents and incident reports 84
 - n6 88
 - Artemis 103

- List of figures 106
- List of tables 108
- List of charts 109

Introduction

Another year of CERT Polska's activities is behind us. An absolutely record-breaking year, if we take into account practically all the statistics cited in our previous reports. Behind these numbers is the daily work of experts who care for the safety of Poles online every day. This year's report is about this work, the key challenges we face and the threats we analyse.

We describe, for example, our tools such as Artemis and Snitch, which allow us to respond effectively to threats and work for cybersecurity. Most of them are available as open-source projects. We believe that this way we can build a foundation for the development of security beyond our constituency.

In order to develop tools, we need to know in which areas they are still needed. That is why a large part of our everyday work is analysing the activities of cybercriminals. A summary of these observations can be found in the section on incidents and threats.

We want the report to have its permanent elements – those that allow us to follow trends and tendencies, and at the same time, to always include references to current events and changes. In this year's edition, we devote a lot of space to fraud that originates on social media platforms, but we also describe changes that increase user security. Blocking of text messages from cybercriminals based on patterns created by CERT Polska is undoubtedly one of them.

In the report we also talk about our partnerships, including international ones, with cybersecurity teams that have resulted in projects, exercises and workshops. We talk about educational and awareness-raising activities, including the launch of a new reporting channel through the mObywatel app. Information on this and other topics can be found in the chapter summarising the activities of CERT Polska. Knowledge of cybersecurity, awareness of threats and methods of combating them are the most effective weapons in the fight against cybercriminals. With this in mind we present you with the latest CERT Polska report.

Have a good read!

About CERT Polska

We care about Polish Internet security. It is a slogan that reflects the meaning and purpose of our work very well.

CERT Polska is the first Polish computer emergency response team. Through our effective operations, since 1996 we have become a reliable and renowned partner among experts and in the public sector. Today we build a similar position among citizens, through reliable report handling and educational operations.

The CERT Polska team acts within the structures of NASK – National Research Institute and executes some of the tasks of CSIRT NASK team in accordance with the Act on National Cybersecurity System. We are a team responsible for security-incident handling as well as working with similar units worldwide, in terms of operations, research and implementation activities.

Since the entry into force of the Act of 5 July 2018 on the National Cybersecurity System (Ustawa o Krajowym Systemie Cyberbezpieczeństwa), the team has been carrying out many of the tasks of CSIRT NASK, in accordance with Article 26 of this Act.

According to Article 26 of the Act, we are responsible for:

- monitoring cybersecurity-related threats and incidents at the national level,
- responding to the incidents reported,
- coordinating the process of handling incidents,
- performing advanced analyses of malware and vulnerabilities,
- developing tools and methods to detect and combat cybersecurity threats,
- conducting awareness-raising activities in the cybersecurity area.

We also coordinate 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 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 province-based funds for environmental protection and water management;
- commercial 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 Act on the National Cybersecurity System;
- key service providers, except for those listed in section 5 and 7 of the Act on the National Cybersecurity System;
- entities other than those listed in sections 5 and 7 of the Act on the National Cybersecurity System;
- natural persons.

A vital aspect of our work is also to build cybersecurity awareness and proactive seeking of solutions to the challenges faced by the above institutions. We take an individual approach to each report. We provide support and content-related assistance. We monitor trends in cyberspace and maintain statistics. We effectively warn and inform. For more details about our daily work, see the text below. Welcome to our report!

Calendar



JANUARY

- 16.01** We have warned domain owners about scammers impersonating the National Domain Registry and phishing for email login details
<https://www.facebook.com/share/p/18kmpJ6kVw>
- 31.01** CERT Polska's participation in the FETTA project – partnership and knowledge sharing in the field of CTI in the European Union
<https://cert.pl/posts/2024/01/fetta>
- 100,000 text messages reported via the 8080 number in January 2024
<https://www.facebook.com/share/p/1TbSzYZNDU>

FEBRUARY

- 02.02** We published information about the Balada Injector campaign infecting WordPress websites using popular plugins.
<https://cert.pl/posts/2024/02/balada-injector>
- 09.02** We reported on critical vulnerabilities in VPN gateways from Fortinet and Ivanti
<https://www.facebook.com/share/p/1B1RPq5u57>
- 15.02** We coordinated the disclosure of critical vulnerabilities in Comarch ERP XL software
<https://cert.pl/posts/2024/02/CVE-2023-4537>

MARCH

- 18.03** We warned about a cyber fraud campaign using the subject of tax refunds
<https://www.facebook.com/share/p/18dtSc3kyH>
- 29.03** Recommendation of the Government Plenipotentiary for Cybersecurity regarding Fortinet products
<https://www.gov.pl/web/baza-wiedzy/rekomendacja-pelnomocnika-rzadu-ds-cyberbezpieczenstwa>

APRIL

- 08.04** Start of the educational series #WiedzaInformacje (Knowledge Information) dedicated to AI
<https://cert.pl/posts/2024/04/wstep-do-deepfake>
- 16.04** Publication of the 'CERT Polska Annual Report for 2023'
<https://cert.pl/posts/2024/04/raport-roczny-2023>
- 16–17.04** The 27th edition of the Secure conference
<https://cert.pl/posts/2024/04/secure-2024>
- 26.04** Polish-Finnish team with experts from CERT Polska among the top three teams at Locked Shields 2024
<https://www.facebook.com/share/p/18qFBc9BRj>

MAY

- 08.05** We warned about the APT28 campaign targeting Polish government institutions
<https://cert.pl/posts/2024/05/apt28-kampania>
- 17.05** Recommendations of CERT Polska for strengthening the protection of OT systems
<https://cert.pl/posts/2024/05/rekomendacje-ot>
- 21.05** Article 'DNS4EU project – partnership at the European level'
<https://cert.pl/posts/2024/05/dns4eu>

JUNE

- 06.06** We scanned 25,000 domains with the Secure Mail tool
https://x.com/NASK_pl/status/1798661003653034413
- 10.06** We coordinated the disclosure of vulnerabilities in medical centre software
<https://cert.pl/posts/2024/06/CVE-2024-1228>

- 12.06** Critical vulnerabilities in MegaBIP software detected by CERT Polska as part of its own tests, recommendation of the Government Plenipotentiary for Cybersecurity regarding Public Information Bulletins
<https://cert.pl/posts/2024/06/CVE-2024-1576>
- 21.06** Start of the 2nd edition of the #CyberParawan (Cyber Screen) educational series
<https://cert.pl/posts/2024/06/cyberparawan>

JULY

- 11.07** We informed about the data leak detected by us from the website megamodels.pl and about the possibility for users to use the website bezpiecznedane.gov.pl
<https://www.facebook.com/share/p/1LtnCMYfgM>
- 16.07** We warned about the sale of fake tickets on social media
<https://cert.pl/posts/2024/07/oszustwa-biletowe>
- 22.07** We warned about a campaign impersonating the Ministry of Interior and Administration
<https://www.facebook.com/share/p/1Ao96bpWAt/>

AUGUST

- 01.08** CVE programme – first year behind us!
<https://cert.pl/posts/2024/08/rok-cna>
- 08.08** We presented the Artemis tool at the Black Hat conference in Las Vegas
<https://nask.pl/aktualnosci/polski-artemis-w-las-vegas>
- 14.08** Launch of the Network Safety service in the mObywatel app
<https://info.mobywatel.gov.pl/aktualnosci/usluga-bezpiecznie-w-sieci>

SEPTEMBER

- 03.09** The first notification about the active cyber-fraud campaign was sent to those who had activated the Secure Online service in the mObywatel app
<https://www.facebook.com/share/p/15tU2eN5wW>
- 16–26.09** We warned against fraudsters exploiting the subject of flooding
<https://www.facebook.com/share/p/19sqpdodz9>
<https://www.facebook.com/share/p/17zbQMHAWr>
<https://www.facebook.com/share/p/1YjMguUe9C>

OCTOBER

- 01.10** The article „The Dark Knight Returns: Analysis of the Joker malware”
<https://cert.pl/posts/2024/10/analiza-joker>
- 11.10** Team from Poland takes 3rd place at the European Cybersecurity Challenge championships
<https://nask.pl/aktualnosci/wielki-sukces-polacy-na-podium-europejskich-mistrzostw-w-cyberbezpieczenstwie>
- 18.10** Data leak at AIUT, recommendations from the Government Plenipotentiary for Cybersecurity
<https://www.gov.pl/web/baza-wiedzy/wzrost-liczby-incydentow-zwiazanych-z-wyciekiem-danych—zalecenia-pelnomocnik-rzadu-do-spraw-cyberbezpieczenstwa>

NOVEMBER

- 15.11** First million scam messages blocked thanks to text message patterns
<https://nask.pl/aktualnosci/mamy-pierwszy-milion-jak-cert-polska-walczy-z-oszustwami-komputerowymi>

- 20.11** Article 'Warning, fake CAPTCHA, or how not to get infected'
<https://cert.pl/posts/2024/11/Uwaga-falszywa-CAPTCHA-czy-li-nie-daj-sie-zainfekowac>
- 25.11** Article 'Advertising fraud on large online platforms'
<https://cert.pl/posts/2024/11/Oszustwa-reklamowe-na-duzych-platformach>

DECEMBER

- 01.12** Marcin Dudek is the new head of CERT Polska
<https://cert.pl/posts/2024/11/marcin-dudek-kierownikiem>
- 04.12** Article: 'CERT Polska's expectations regarding Meta's solution to the problems with fraud on its social media platforms'
<https://cert.pl/posts/2024/12/oczekiwania-wobec-meta>
- 10.12** The State Treasury has transferred the rights to the plot of land to NASK-PIB, on which the NASK Cybersecurity Centre building is to be constructed
<https://nask.pl/aktualnosci/przelom-w-projekcie-centrum-cyberbezpieczenstwa-nask>
- 13.12** Start of educational series #12CyberPorad (12 Cyber Tips)
<https://www.facebook.com/share/p/182beGVMaT>

Incidents and threats



Overview of new campaigns

The threat landscape in Polish cyberspace continues to evolve. On the one hand, we see the well-known phishing campaigns from recent years intended to obtain logins and passwords for popular e-mail services or social media sites, or fake ad websites mimicking services such as OLX or Allegro. On the other hand, novel campaigns are emerging that are interesting from a cybersecurity point of view.

CERT Polska's efforts to combat cyber threats can be categorised in various ways, which is what the front-line operators specialise in – in the following article, you can find the recollections of two of them, focused on the large-scale scam campaigns from which we try to protect Polish Internet users.

KAROL: The year 2024 was definitely intense in terms of criminal activity online. Is there anything in particular that stands out in your memory?

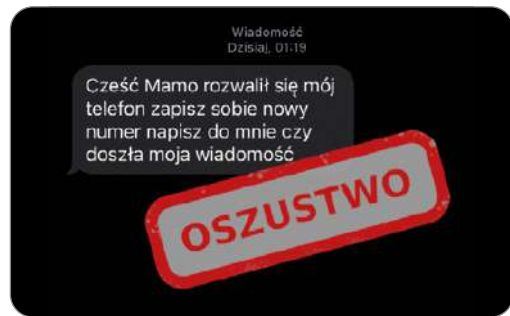
BARTOSZ: There are campaigns that we have known about for many years, but they can still surprise us with new developments. Last year, I would single out two in particular:

WhatsApp – child scam

- B.:** In 2024, we saw a return of the campaign targeting parents, which involves extorting money for the alleged purchase of a new phone for the child. The fraudster usually contacted the victim by a text message.
- K.:** It is worth mentioning here that thanks to the introduction of patterns provided by CERT Polska, such text messages were often blocked by telephone operators before they reached the recipient!
- B.:** Yes, and at the same time, it encouraged criminals to modify the content of these messages, often by deliberately making spelling mistakes, swapping letters and using other typographical tricks. This allowed them to bypass the safeguards, but at the same time made it easier for potential victims to realise that something is wrong.
- K.:** What happened next? The scammer introduced themselves in a way that clearly suggested that they were the recipient's child and informed them that their phone had been damaged, which was the reason for writing from a new number. In some cases, the victim was asked to continue the conversation via WhatsApp. The aim of the campaign was to extort money from unaware parents.

B.: And it works, because although for many people spending a few thousand zlotys on a phone is not easy, the scammers were open to negotiation – they offered to buy a cheaper phone, allowed for other forms of payment, and even guided the victim step by step through the alleged purchase process, often phishing for payment card details at the same time.

FIGURE 1. Example of a message sent by criminals



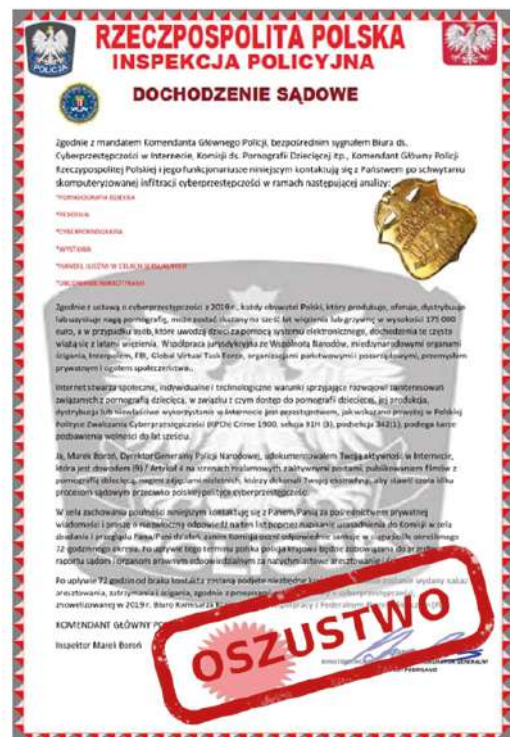
Police summons

K.: The second recurring campaign is the notorious impersonation of Polish and foreign law enforcement agencies. The criminals are particularly ‘fond’ of the Chief of Police.

B.: We saw letters with that person’s last name at least several times a day. The message contained accusations of, for example, paedophilia and the possession and distribution of videos showing the sexual abuse of children. It instructed us to contact the sender immediately to resolve the situation, threatening to take the matter to court if we did not respond.

FIGURE 2. Attachment sent in a message pretending to be from the Police

K.: The criminals were also very understanding and offered to settle the matter amicably – for an appropriate fee, of course.



Copyright breach

B.: But among these ‘old chestnuts’ there was also something new – a scam campaign based on alleged copyright violations.

K.: I knew you would mention it, you were very interested when we first saw reports related to it in the fourth quarter of 2024.

B.: Because the formula itself was interesting – the fraudsters, posing as legal representatives of various entities, reported alleged violations of their customers’ copyrights. The message demanded the immediate removal of the protected materials, threatening consequences if no action was taken. Detailed information on the subject of the violation was allegedly to be found in the attached PDF file.

- K.:** So far it sounds like a prelude to a fake police officer scam. Only the scammers responsible for this campaign wrote even worse Polish?
- B.:** That's right – it distracted from the fact that clicking on the icon, pretending to be a PDF attachment or a link with alleged evidence, downloaded an archive containing a file that, when opened, led to a malware infection, e.g. Lumma stealer. The entity which rights were allegedly infringed, and the arguments of the 'principal' varied depending on the iteration of the campaign, but the general scheme of action of the fraudsters was the same in each case. As we increasingly use AI-generated content, the accidental violation of someone's intellectual property seems likely enough for fraudsters to exploit it.

FIGURE 3. Fake message informing about copyright violation



QR codes

- K.:** Speaking of technological developments and malware, it is impossible not to mention the scammers impersonating parking meter operators and the National Tax Administration...
- B.:** Indeed, one of the most interesting campaigns was the one in which the first stage did not take place on the Internet at all – it took place on the streets, among parked cars.
- K.:** The scammers put cards imitating parking fines on the windscreen wipers, with QR codes leading to a website where the fine could allegedly be paid. Another variant were stickers on parking metres that led to a fake payment

gateway. It's worth knowing who actually manages the paid parking zones in your city so that you don't fall victim to such a simple scam.

False CAPTCHA

- B.:** B.: And did you have your 'favourite' campaign of the past year?
- K.:** To know the answer to this question, you must confirm that you are not a robot.
- B.:** Preferably by selecting the text and pressing certain keyboard shortcuts?
- K.:** In that order: Ctrl+C, Windows+R, Ctrl+V and Enter, please.
- B.:** What script will I run this way?
- K.:** Probably one that downloads something more from the prepared server. Maybe a stealer, maybe ransomware, maybe you'll just activate a premium subscription.
- B.:** And if you want to have access to premium materials about other scam campaigns...
- K.:** ...as well as a free subscription to the latest information in the field of cyber...
- B.:** ...we too invite you to a specially prepared server: cert.pl.
- K.:** And to our social media!

Ransomware

As in previous years, incidents involving ransomware attacks were the most destructive and had the most serious impact on organisations in 2024. The malicious code prevents access to data by encrypting it, with the objective of extorting a ransom in exchange for the key to regain access to the data. In addition, during attacks, malware operators usually try to destroy backups. Many groups also use the

FIGURE 4. Fake request for payment

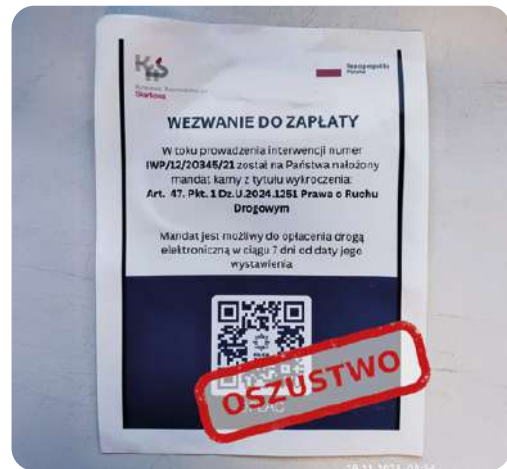
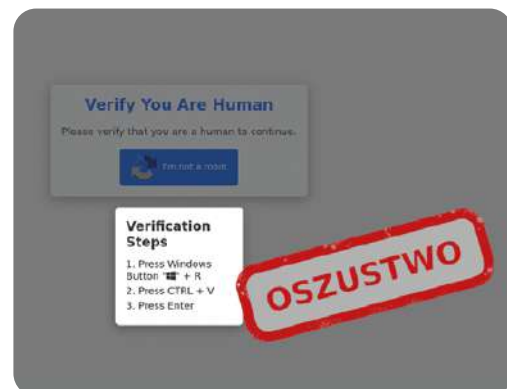


FIGURE 5. Example of false verification using Captcha



double extortion technique, i.e. before encrypting the data, the criminals transfer it from the attacked infrastructure to servers they control, so that they can later blackmail the attacked organisations with the threat of publishing the stolen information.

In 2024, the CERT Polska team registered a total of 147 incidents related to ransomware attacks. This is a decrease of approx. 8% compared to the record year 2023. However, as in 2023, the vast majority of incidents were reported by business entities (87), followed by individuals (35) and public entities (25). Incidents in public entities mostly concerned institutions from the public administration sector (14 incidents) and education and higher education (9 incidents). In 2024, significant data sets were published that had been stolen as a result of ransomware attacks on Atende Software and AIUT. The data leaks included technical documentation of systems implemented for third parties and authentication data. Due to the potential threats associated with unauthorised access to industrial automation systems by third parties, the CERT Polska team took action with the objective of identifying and warning AIUT’s customers in parallel to the communication carried out by the company.

Major threats

In 2024, as in the previous year, the majority of recorded ransomware incidents were related to infections with malware from the Phobos family – we recorded 17 such incidents. The number of incidents caused by the next most common variants was very similar. The second most common ransomware family was Magniber software. In this case, the number of incidents we recorded was 12. The targets of the attacks were primarily private individuals. The third most common threat we observed was the ransomware STOP(Djvu), which was identified in 10 incidents. Almost as many, 9 incidents, were caused by LockBit malware. We also recorded attacks aimed at Polish entities, carried out by the Akira, Ransom-Hub and INC groups. In 30 incidents, the information obtained during the report process did not allow for the identification of the ransomware used in the attack.

TABLE 1. Number of incidents recorded, broken down into ransomware families

Ransomware families	Number of incidents recorded
Phobos	17
Magniber	12
STOP (Djvu)	10
LockBit	9
MedusaLocker	7
Nigra	6

Ransomware families	Number of incidents recorded
Akira	6
Other	50
Not classified	30

Families identified by CERT Polska in 2024

LockBit

LockBit malware is used in the Ransomware-as-a-Service (RaaS) model. It means that the group responsible for developing the malicious code makes it available to criminals carrying out ransomware attacks in exchange for a share of the ransom paid by the victims. The large number of independent malware operators translates into a significant variety of techniques and tools used in attacks, but many of them have in common the exfiltration of data from the attacked entity before encryption begins. Information about the attacks and the stolen data is then published on the group's websites available on the TOR network. On 20 February 2024, law enforcement agencies seized LockBit's infrastructure as part of the international operation Cronos, which made it possible to recover some of the encryption keys (the decryptor was published on the website nomoreransom.org). Unfortunately, the group soon became active again. In 2024 it posted a total of 546 entries on its website reporting intrusions into various entities, and in December it announced the planning of LockBit version 4.0 for 2025.

Magniber

The second most common ransomware family was Magniber, with 11 out of 12 incidents involving individuals whose devices were attacked during a campaign that took place over the summer holidays. This family was first recorded in 2017. The group responsible for Magniber ransomware often exploits known vulnerabilities and the software uses direct system calls (syscall) to avoid detection by antivirus engines. The campaign using this malware family started at the end of July/beginning of August 2024 and ended around 19 September. The distribution channels used by Magniber include websites with free sports broadcasts and websites illegally distributing copies of commercial software. The reports received also coincide with published analyses of this malware, which indicate that Magniber ransomware targets users still using Windows 7, a system that has not received security patches since 2020. It should be emphasised that the leading web browsers have ended support for this version of the system, and vulnerabilities in non-updated versions may be one of the attack vectors of this ransomware.

INC/Lynx Ransomware

The group responsible for the INC ransomware appeared in July 2023, and we recorded its first attacks on Polish entities in the last quarter of 2024. In most of the cases we analysed, the attack vector turned out to be vulnerable software that had not been updated to the version recommended by the manufacturer. In addition, the group installed remote access tools such as ScreenConnect, Atera and AnyDesk on the infected machine with the objective of gaining access to it. In two cases, several days passed between the initial access to the infrastructure and the start of encryption, and information about the attack or the allegedly stolen data (according to the note left) was never published on the group's blog. In March 2024, the INC group put the code of its ransomware up for sale, and since July, the Lynx group has been active, also running a number of websites where it publishes data stolen from the attacked entities (some sources suggest that this is a rebranding or the result of a conflict between INC members). In December 2024, the CERT Polska team analysed an incident in which notes were left in an encrypted environment indicating both the Lynx and INC groups.

Akira

Another relatively new ransomware group is Akira. Its first activity was observed in March 2023. On its leak site, the group uses a characteristic theme referring to the first computers from the 1980s. What also distinguishes the group is that the notes it leaves after the attack do not contain a specific ransom amount, but only a link to the site, the victim's unique ID and an invitation to negotiate. The group gains access to the infrastructure of the attacked entity mainly by exploiting the lack of two-factor authentication (in the incidents we analysed, brute force attacks were used) or vulnerabilities in VPN edge devices, especially Cisco. In March 2024, the Cisco Talos Incident Response team published information about a new variant of the Akira_v2 encryptor used to attack Linux systems and Megazord for Windows systems. According to Talos IR, the group reverted to its original encryptor at the end of 2024.

FIGURE 6. Leak site of the Akira Group

The image shows a terminal window with a green title bar containing the text "[AKIRA]". The main content of the terminal is as follows:

```
AKIRA

Well, you are here. It means that you're suffering from cyber incident right now. Think of our action as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that there is a fair price to make it all go away.

Do not rush to assess what is happening - we did it to you. The best thing you can do is to follow our instructions to get back to your daily routine, by cooperating with us you will minimize the damage that might be done.

Those who choose different path will be shamed here publicly. The functionality of this blog is extremely simple - enter the desired command in the input line and enjoy the juiciest information that corporations around the world wanted to stay confidential.

Remember, You are unable to recover without our help. Your data is already gone and cannot be traced to the place of final storage nor deleted by anyone besides us.

quest@akira:~$ help

List of all commands:

leaks      - hacked companies
news       - news about upcoming data releases
contact    - send us a message and we will contact you
help       - available commands
clear      - clear screen

quest@akira:~$
```

Observations on ransomware

Difficulties in identifying the attacker

One of the basic pieces of information we want to obtain after a ransomware attack is to identify which family we are dealing with. Quickly identifying the group responsible for the attack and the techniques they use makes it much easier to identify the potential attack vector, assess the risk of data exfiltration and the credibility of the threats made in the ransom note. However, attackers are increasingly only providing contact details in the ransom note left by the encryption software and omitting signatures that would clearly link the attack to a particular group. In addition, the leaking of the source code of some ransomware variants (e.g. Conti in 2022 or LockBit at the end of 2023) or its resale (INC in early 2024) result in the emergence of new hybrids that share features from different ransomware families. This trend may also be caused by pressure from law enforcement agencies, making it more important for many ransomware groups to avoid the attention of cybersecurity entities and institutions than to build their image.

False double extortion

The technique of double extortion is standard in the ransomware threat landscape, as has also been pointed out in CERT Polska reports for recent years. The vast majority of notes left by encryption software contain a threat to publish the stolen data, even if no exfiltration has taken place. Sometimes, ransomware operators will post a fake announcement of the supposedly leaked data on their website (which they later remove) to increase the pressure on the affected entities. In such cases, the attackers usually do not publish any samples of the data. Last year, we also saw a case where information about a hack that did not actually take place was published, and the 'evidence' provided by the ransomware operators came from an attack on another organisation. During the analysis of one of the incidents related to the ransomware infection carried out by RansomHub operators, we also observed that attackers do not publish all the files they have or restrict access to previously published data. It should also be taken into account that it can take several months from the attack to the disclosure of the incident by the intruders.

Prolonged attacks

Unfortunately, as was the case last year, the typical attack vector identified in the incidents we analysed was the use of credentials for remote access systems not protected by multi-factor authentication. Attackers obtain this data in various ways, for example, by buying it from malware operators (who steal it from infected systems) or by obtaining it from leaks on third-party websites (if the user does not use unique passwords). The second common vector was the exploitation of

known vulnerabilities in edge devices that had not been updated for many months despite the manufacturer releasing relevant security patches. An example of such a vulnerability, the exploitation of which we observed in several incidents, is CVE-2023-48788, described in more detail in the chapter on the [most important vulnerabilities](#) (p. 24) in 2024. In many of the analysed cases, the attackers had access to the victim's infrastructure many months before the encryption process began. This made it significantly more difficult both to determine the attack vector (due to insufficient log retention and obfuscation of other traces) and to restore the entity to operation (complicating the determination of backups that do not contain elements left by the adversary). It should also be emphasised that attackers often do not even try to hide their presence, using foreign IP addresses (often from outside the European Union) for connections, as well as generating numerous anti-virus system warnings when they try to install the malware of their choice on a computer that is a bridgehead in an attack on an organisation.

Ransomware guidebook

As mentioned at the beginning, ransomware attacks are a serious threat to public organisations, companies and individuals. We encourage you to read the guide prepared by our team. The guide describes the measures that can be taken to prepare for this type of threat, as well as the steps that should be taken once an infection has been detected. The guide is available on the CERT Polska website: https://www.cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf.

Major vulnerabilities in 2024

CERT Polska conducts permanent activities aimed at reducing the number of vulnerable product instances active on the Polish Internet. In the event of publication of information about a new vulnerability, an assessment is made of the risk posed to Polish entities. If the vulnerable product is widely used in Poland or the exploitation of the vulnerability it contains may pose a significant threat to entities, the CERT Polska team carries out activities aimed at identifying the owners of instances available on the Internet.

In 2024, the CERT Polska team decided to intensify its activities aimed at effectively reaching out to entities. Unlike the n6 system, which automatically sends notifications about threats to previously reported network scopes, the team tries to identify some of the entities when it considers that they fall within its competence and the potential use of the vulnerability would threaten serious consequences. For this purpose, CERT Polska uses many available sources, but due to the fact that often the only available information is the IP address of the vulnerable device, many threatened entities cannot be identified. In this case, notifications are sent according to the data in the RIPE database.

For each instance of software found, the CERT Polska team tries to determine whether it is affected by the vulnerability in question – it would not be useful to send information about the threat to administrators who have already updated their devices. The most common method is to determine the software version. If this is not possible, in some cases we use low-invasive methods of detecting security vulnerabilities that do not affect the work of the tested software. If this is not possible either, and the new vulnerability carries a high risk of attack, then e-mails are sent to all entities using the software.

In 2024, the actions described above resulted in 11,913 e-mails being sent to various recipients. These usually concerned separate vulnerabilities, of which there were 119 in total, although there were also cases of reminders about older vulnerabilities when, for example, an exploit allowing for their exploitation was publicly released – this significantly increases the risk of attacks.

This is also the place to note the difficulties the team faced in trying to convince a given entity to update or take other mitigating action. In addition to the aforementioned problems of identifying the entities, sending notifications to publicly available addresses had varying degrees of effectiveness. Notifications were often not forwarded to the persons responsible for IT security and no action was taken. In rare cases, the team contacted the entities by telephone after sending e-mails and informed them of the need to respond. This approach proved to be the most effective, but it is resource intensive.

TABLE 2. Notifications sent by CERT Polska regarding vulnerabilities in individual products

Product	Number of notifications
FortiOS	3,070
Really Simple Security	1,693
Zimbra	778
Cisco ASA	647
PAN-OS	610
QNAP	561
Microsoft Exchange	395
Zabbix	365
Webmin/Virtualmin	340
Ivanti	339

Fortinet FortiClientEMS (CVE-2023-48788)

A vulnerability in FortiClientEMS, discovered in March 2024, allows unauthenticated attackers to inject any SQL query directly into Microsoft SQL Server's internal database. As a result, in combination with the use of *the xp_cmdshell* function in MSSQL, the attacker could execute any command on the vulnerable device with the highest system privileges. Exploiting this vulnerability meant taking full control of the device and gaining access to any data on it. In this case the attacker could, for example, take over the Active Directory administrator account by dumping the password hash, thus taking over the entire organisation domain.

Shortly after the vulnerability was published online, publicly available code was released that allowed the vulnerability to be exploited, significantly increasing the risk of vulnerable devices being compromised. As recently as March, some security companies detected cases of the vulnerability being exploited on customers' devices that were accessible from the Internet¹. After taking over vulnerable devices, attackers installed remote management tools such as Atera, AnyDesk and ScreenConnect on them as a way to ensure constant access to the compromised infrastructure.

In August, the CERT Polska team identified 24 publicly available FortiClientEMS devices in Poland and took action to warn their owners of the threat. Although the number of these devices may not seem particularly alarming compared to other vulnerabilities observed, the use of CVE-2023-48788 has been observed in attacks on several organisations, which usually resulted in the takeover of the entire infrastructure. The objective of the attacks was often to launch ransomware, but the CERT Polska team also registered cases of this vulnerability being exploited by APT groups. In such situations, the attack remained undetected for up to several months.

Fortinet FortiManager (CVE-2024-47575)

The critical vulnerability discovered in FortiManager software was caused by inadequate user input data sanitisation, which allowed the injection of any command that was then directly executed on the device². Information about the vulnerability was published by Fortinet in October 2024.

Exploiting this vulnerability allows attackers to gain administrative control over the FortiManager instance. Once the device is compromised, attackers can retrieve its configuration or password hashes, deploy malicious configurations,

1 <https://darktrace.com/blog/forticlient-ems-exploited-inside-the-attack-chain-and-post-exploitation-tactics>, <https://redcanary.com/blog/threat-intelligence/cve-2023-48788/>, <https://www.esentire.com/security-advisories/widespread-exploitation-of-fortinet-vulnerability-cve-2023-48788>

2 <https://labs.watchtower.com/hop-skip-fortijump-fortijumphigher-cve-2024-23113-cve-2024-47575/>

install backdoors and potentially gain access to other devices managed by FortiManager, which can lead to the compromise of the entire network. Two weeks after the vulnerability was published, a publicly available exploit had already appeared on the Internet.

According to an analysis by Mandiant³, the vulnerability CVE-2024-47575 in FortiManager was actively exploited by the UNC5820 group. The attackers gained access to configuration data from multiple compromised FortiManager devices, including user password hashes and configuration details of managed FortiGate devices. Although no evidence of further exploitation of this data was found, this event shows the risk that such a vulnerability poses to the security of the entire infrastructure.

Even before the official vulnerability announcement, the CERT Polska team informed the administrators of 27 publicly accessible FortiManager instances about the threat. Based on the IoCs provided with the warning, some entities identified the use of this vulnerability in their infrastructure.

Fortinet FortiOS/FortiProxy (CVE-2024-21762)

FortiOS is an operating system that is mainly used on FortiGate devices (firewalls). In February 2024, a critical vulnerability was published in FortiOS and FortiProxy systems, which allows an unauthenticated attacker to execute arbitrary code or commands via a specially crafted HTTP request. The vulnerability is caused by improper handling of data transferred using *chunked transfer encoding*, resulting in overwriting of an unauthorised memory area.

A few days after the vulnerability was published by Fortinet, CISA announced that it was being actively used to carry out attacks. Soon after, an exploit was published, which further increased the risk of attacks.

Since the disclosure of the vulnerability, CERT Polska has been working to identify the devices at risk and inform their owners of the threat. The day after the vulnerability was published, the administrators of all FortiGate devices identified in Poland were notified of the threat. Since March, the CERT Polska team has been conducting periodic, active scans of all FortiGate devices for the possibility of exploiting the CVE-2024-21762 vulnerability. For this purpose, the Artemis tool is used, the module of which responsible for the implementation of this task has been published in an open repository⁴ on our GitHub.

3 <https://cloud.google.com/blog/topics/threat-intelligence/fortimanager-zero-day-exploitation-cve-2024-47575>

4 https://github.com/CERT-Polska/Artemis-modules-extra/tree/main/forti_vuln

A scan conducted in March showed that 2,462 vulnerable instances were available in Poland at that time. Thanks to the continuous efforts of the CERT Polska team, whose objective is to reach the administrators of these devices, and the inclusion of FortiOS and FortiProxy in the recommendation of the Government Plenipotentiary for Cybersecurity regarding the immediate update of Fortinet products⁵, the number of vulnerable devices has been reduced by almost a half.

Despite the high prevalence of the CVE-2024-21762 vulnerability, CERT Polska has not recorded any incidents in which the use of this vulnerability has been confirmed.

Palo Alto Networks PAN-OS – GlobalProtect (CVE-2024-3400)

GlobalProtect is a feature of the Palo Alto Networks PAN-OS operating system that allows remote access to an organisation's network. In April 2024, a critical vulnerability was discovered in this component, allowing the creation of arbitrary files with administrator privileges. This vulnerability can be exploited by modifying the SESSID cookie, which does not undergo proper sanitisation. After creating a file with a suitably crafted name, it is possible to inject a command into the system, which in the practical terms allows unauthenticated attackers to remotely execute arbitrary code on the device and thus take control of it.

Initial reports suggested that the vulnerability only affects devices with telemetry enabled, but Palo Alto Networks later clarified that devices in any configuration are affected.

The CVE-2024-3400 vulnerability was used to carry out attacks even before its public disclosure. Attackers used the vulnerability to retrieve the device configuration, which they then used to transfer activities to subsequent devices in the victim's environment. In many cases, the devices were tested for vulnerabilities by creating an empty file, without further activity on the part of the attackers⁶.

The CERT Polska team received 2 reports regarding the exploitation of the CVE-2024-3400 vulnerability. In both cases, the attackers' objective was to obtain the device configurations.

5 <https://www.gov.pl/web/baza-wiedzy/rekomendacja-pelnomocnika-rzadu-ds-cyberbezpieczenstwa>

6 <https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/>

One week after the vulnerability was published, CERT Polska actively scanned devices using GlobalProtect available in Poland and identified 25 affected devices. The administrators of these devices were notified of the risk and the need to update the software. Such scans were periodically repeated and by the end of the year the number of vulnerable devices was limited to 8 cases in Poland.

Ivanti Connect Secure (multiple vulnerabilities)

Ivanti Connect Secure is a service that allows you to establish SSL VPN connections to access your organisation's internal resources. It is troublesome to limit access to this service because for employees working remotely, it acts as a point of contact with the organisation's network. This results in a high level of interest from criminals in vulnerabilities found in this class of solutions.

In 2024, many critical vulnerabilities affecting the Ivanti Connect Secure service were found and published. Some of them were found by security researchers and reported to the manufacturer accordingly, but others, such as CVE-2024-21887 or CVE-2023-46805, were discovered during ongoing attacks using them⁷. Below are brief descriptions of what we consider to be the most important vulnerabilities that have been identified by the US CISA as being actively exploited:

- CVE-2023-46805 – bypassing authentication to use unavailable features,
- CVE-2024-21887 – possibility of command injection,
- CVE-2024-21888 – escalation of normal privileges to administrator privileges,
- CVE-2024-21893 – SSRF vulnerability that allows an attacker to send unauthorised HTTP requests from a server,
- CVE-2024-21894 – launching DoS attacks and, under certain conditions, remote code execution.

Although the CERT Polska team has not observed any successful attacks on Polish entities using these vulnerabilities, it is possible that this is only a matter of time. According to the incident response team in Luxembourg, which we are working with, there have been many successful attacks in their country⁸.

In 2024, the CERT Polska team sent out a total of 7 notifications to entities with Ivanti devices in their networks. These notifications were sent after the publication of a vulnerability that the team considered to be at high risk of being exploited by criminals. Around 120–150 devices are being monitored, but it is not known how many of them are updated regularly.

7 <https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/>

8 <https://www.circl.lu/pub/tr-78/>

Synacor Zimbra (CVE-2024-45519)

Zimbra Collaboration Suite is a software for teamwork. Its server component responsible for handling e-mails had the CVE-2024-45519 vulnerability that allowed unauthenticated users to execute commands.

The corresponding patch was released on 4 September, and information about the vulnerability was published a month later. Although the manufacturer of Zimbra Collaboration Suite did not provide any technical details on how to exploit the vulnerability, on 3 October CISA, based on reports from researchers, added the vulnerability to the list of actively exploited vulnerabilities.

Since then, scripts have appeared on the Internet that allow users to verify whether a given server is vulnerable, articles analysing the technical aspects of the vulnerability in detail are also available⁹, meaning that it is now much easier to carry out attacks and attracting the interest of more criminal groups. For the attack to be successful, the *postjournal* service must be running on the server, which is disabled by default.

So far, the CERT Polska team has not recorded any successful attacks on Polish entities using CVE-2024-45519. Attempts to identify vulnerable instances of this software have verified that there were 551 in Poland on 30 September and that their number was decreasing – on 12 December there were already 351.

Due to the high probability of this vulnerability being exploited (including by APT groups), the team took action with the objective of sending notifications to the entities responsible for the individual Zimbra software instances. The notifications included recommendations to perform an immediate update and to verify that there were no traces of vulnerability exploitation in the application logs.

Data leaks

Searching for leaks

One of the areas of activity of CERT Polska, apart from responding to reported incidents, is proactive search for emerging threats. One of the elements of these activities is tracking data leaks from Polish companies and institutions, carried out both by direct monitoring of the websites used by criminals (e.g. known as leak sites of ransomware groups on which they publish information and data of their victims), as well as using tools provided by external entities. If we become

9 <https://projectdiscovery.io/blog/zimbra-remote-code-execution>

aware of a leak, our objective is to identify the source and send a warning to the affected entity. Most often, we record website intrusions that lead to the theft of associated databases. We also monitor information about compromised accounts posted on forums in the TOR network. If we notice that a file containing the credentials of users from Poland has been posted on the Internet, we forward this information to the administrators of the respective services so that they can take measures to secure these accounts. In 2024, we managed to inform about the leak of medical data from the software of Medily sp. z o.o., to name one.

Service bezpiecznedane.gov.pl

In 2024, our team continued to use the Secure Data website with the objective of informing Polish Internet users whether their data had been leaked. During the year, we recorded 3 such incidents, and we decided to publish them on the website.

FIGURE 7. Homepage of the bezpiecznedane.gov.pl website



megamodels.pl

In July 2024, we received a report with a link to a public data set described as 'users of the website megamodels.pl'. During our analysis of the material, we confirmed that the data had indeed been stolen from this website. Although the leak included information about more than 182,000 accounts, a significant portion of them were created by bots and the data did not belong to real people, so the actual scale of the incident was smaller. We estimate that the number of accounts created with real data was less than 40,000.

The leaked data included the first name, last name, email address, password hashes, age, telephone number, province and town/city of residence, date of birth, physical parameters and nationality of the account owner.

After the data in the leak was confirmed as genuine, the database was published on the bezpiecznedane.gov.pl website to allow potential victims to verify their data.

sklepbaterye.pl

At the beginning of 2025, data from the online shop sklepbaterye.pl was published online. An analysis of the collected material showed that the data was downloaded by criminals around August 2024 and affected over 200,000 customers. The leaked data included first name, last name, e-mail address, telephone number, password hash and delivery address.

Following confirmation of the veracity of the leak, the database was uploaded to the bezpiecznedane.gov.pl website.

superpharm.pl

In October 2024, customer data of the Superpharm chain was leaked. Based on the collected material and our partnership with the company, we concluded that the data of 1.6 million customers of the online shop superpharm.pl had been leaked. At the time of writing this article, our team has not observed the data becoming publicly available.

The leaked data included: first name, last name, e-mail and password hash. Data on gender and date of birth was also partially leaked.

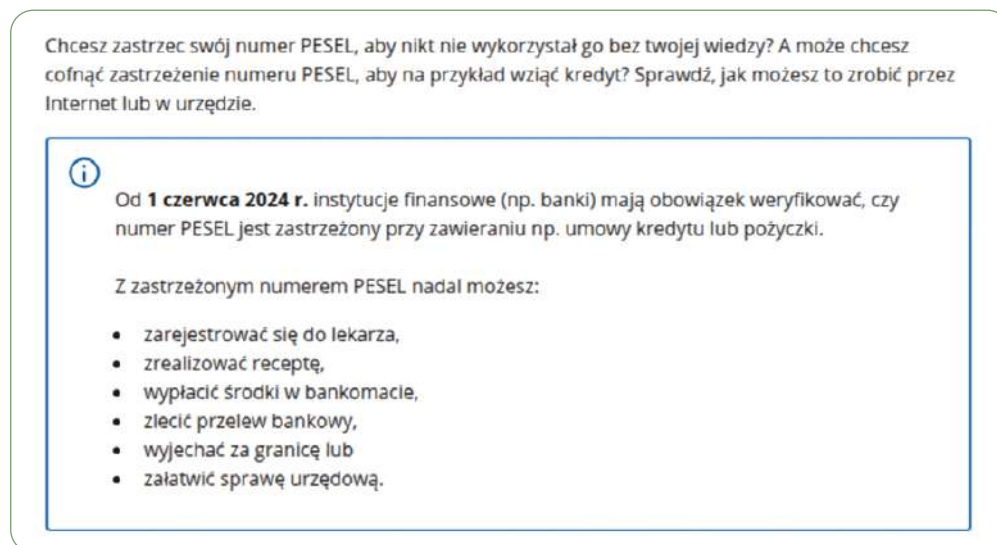
Personal Identification Number (PESEL) registration

From 17 November 2023, it has been possible to restrict usage of your Personal Identification Number (PESEL) number, and from 1 June 2024, financial institutions (e.g. banks) are required to verify that the PESEL number has not been restricted, e.g. when entering into a loan agreement. This is a measure that, in the event of a personal data leak, is intended to prevent any financial obligations from being incurred in our name. PESEL restriction can be cancelled in the mObywatel application or during a visit to a bank, post office or municipality office. The app can also be used to check the status of your Personal Identification Number (PESEL) and the history of queries from various institutions. This allows you to check whether anyone has tried to use your data without authorisation.

More information is available at:

<https://www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie>.

FIGURE 8. Information on usage restriction of the Personal Identification Number (PESEL) from the gov.pl website



Data leaks on moje.cert.pl

In 2024, we started developing a new website – moje.cert.pl – to support administrators. One of the main features we implemented is a module for tracking password leaks related to company domains and effectively informing administrators if they are registered. More information about moje.cert.pl can be found in [the project report section](#) (pp. 67–70).

Observed activities of APT groups

In 2024, we again observed a high level of activity among APT groups linked to foreign countries. The groups conducted their activities for both intelligence and propaganda purposes. Most of the observed attacker activity was related to phishing for email credentials, malware distribution, and attacks on industrial systems. By 2024, it is no longer only the largest companies or public institutions that are targeted, but also smaller companies with a role in supply chains and even people close to those attacked (their family members or friends).

The cases described in the report represent only a part of the activity of APT groups, monitored by CERT Polska/CSIRT NASK, and do not fully reflect the scale of known attacks by these groups on Polish institutions.

The APT group activity we observed in 2024 is presented in the table below. Most of the attacks observed involved groups linked to the Russian Federation and the Republic of Belarus.

TABLE 3. APT group activity observed by CERT Polska/CSIRT NASK in 2024 has been marked with ⊗

	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII
UNC1151/Ghostwriter (Russia/Belarus)		⊗	⊗	⊗		⊗		⊗	⊗	⊗	⊗	⊗
APT28/Fancy Bear/ Forest Blizzard (Russia)	⊗	⊗	⊗	⊗	⊗	⊗	⊗		⊗	⊗		
APT29/Cozy Bear/ Midnight Blizzard (Russia)										⊗		
Sandworm/Voodoo Bear/ Seashell Blizzard (Russia)				⊗						⊗		
Turla/Venomous Bear/ Secret Blizzard (Russia)	⊗	⊗			⊗							
APT-UNK3	⊗											
APT-UNK4							⊗					

Selected campaigns

UNC1151/Ghostwriter

In 2024, the UNC1151 group continued its intensive activities, which had already been noted in previous years, and was once again considered the most active organisation among the groups monitored by the CSIRT NASK. According to publications by Mandiant¹⁰ and Google¹¹, the UNC1151 group is most likely linked to the Belarusian government, but according to other sources, it also has connections to the Russian secret service¹². In the past year, this group has demonstrated an extremely diverse range of attack methods, including both phishing attacks on email service customers and malware infections. The group was also involved in propaganda activities that targeted Polish Olympians, the armed conflict in Ukraine and military exercises taking place in Poland. Such a wide spectrum of activity indicates that the group aims not only to achieve intelligence objectives, but also to influence public opinion on key socio-political issues.

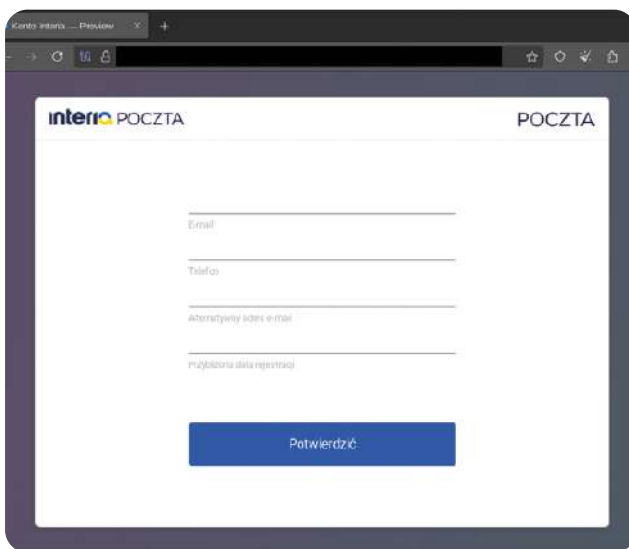
10 <https://www.mandiant.com/resources/unc1151-linked-to-belarus-government>

11 <https://blog.google/threat-analysis-group/update-threat-landscape-ukraine>

12 <https://www.gov.pl/web/sluzby-specjalne/ustalenia-abw-i-skw-dot-atakow-hakerskich>

For most of the year, UNC1151 group ran an intensive email campaign in which, under the pretext of account suspension and the need to change passwords, they persuaded users to provide their login details for email websites. Based on the information we have, and the number of reports received from citizens, we can conclude that these activities were carried out on a large scale, with the objective of targeting people performing various tasks or social functions.

FIGURE 9. Fake login panel for the Interia webmail service used by the UNC1151 group



In the malware attacks, the group used the motive of invitations to industry meetings and conferences to encourage users to download the attached archive file from an e-mail. The archives contained files in CHM (Compiled HTML Help) format which, when opened, displayed an invitation to a real event to the unsuspecting user, at the same time activating malicious code. In a further step, the infected systems downloaded Cobalt Strike, a tool that can be used to take control of a system remotely and perform a variety of actions, such as stealing data, spreading through the network, or installing additional attacker tools.

In June 2024, the CERT Polska team communicated with the Polish Anti-Doping Agency (POLADA) about a possible malware infection and then undertook a full analysis of the incident. The analysis determined that the attack was probably carried out by an actor who exploited a vulnerability in one of the systems at a Polish institution and then resold access to the infrastructure, known as an access broker. Based on the artefacts found, it was concluded that as a result of this activity, the UNC1115 group gained access to the organisation's systems and subsequently stole data relating to Polish athletes. At the end of the Olympic Games in Paris, the POLADA website was hacked, and the stolen data was published on a Telegram channel associated with the UNC1151 group. The group used the event to distribute disinformation content regarding the use of doping substances by Polish athletes.

FIGURE 10. Propaganda content posted by the UNC1151 group on the website of the Polish Anti-Doping Agency

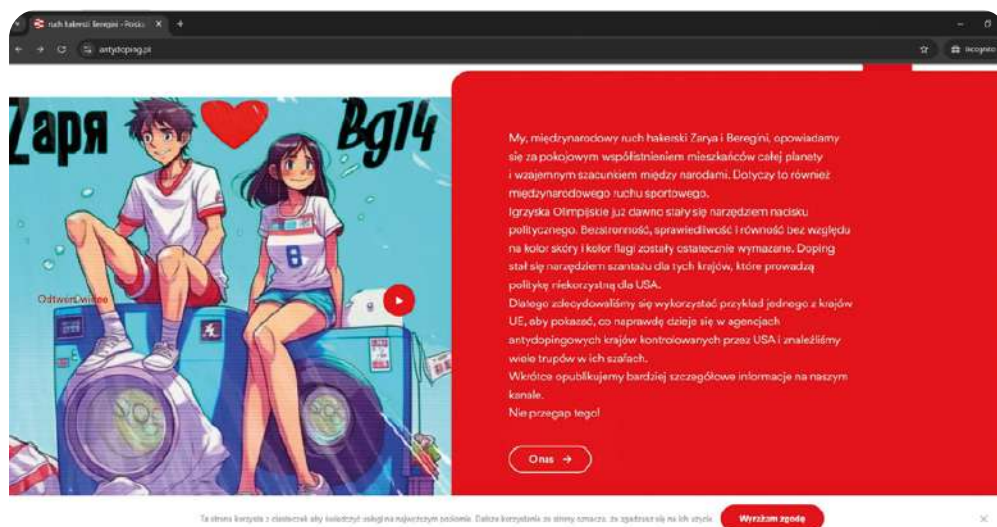
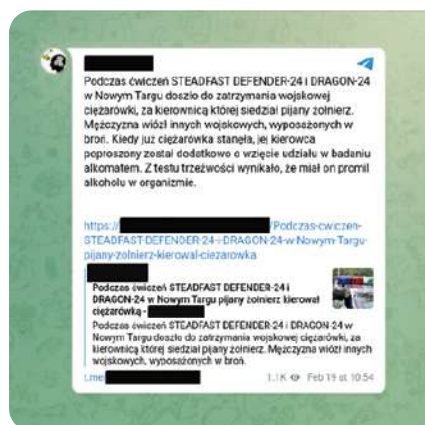


FIGURE 11. Example of disinformation content on Telegram



Last year, the group was repeatedly linked to the distribution of disinformation content; for example, regarding the situation in Ukraine, the military exercises Steadfast Defender 2024 and Dragon-24, and many other socio-political events.

APT28/Fancy Bear/Forest Blizzard

In 2024, CERT Polska observed a significant increase in the activity of the APT28 group, which is linked to the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). The group's activities mainly focused on the distribution of malware and attempts to steal access data to Microsoft Outlook email systems.

In May 2024, CSIRT NASK, in partnership with CSIRT MON and CSIRT GOV, observed another example of the many attempts to infect users in Polish institutions and public entities with malware. The content of the e-mails sent was designed to arouse the interest of potential victims and get them to click on the link provided in the body of the message.

FIGURE 12. Example of a message used by the APT28 group to distribute malware



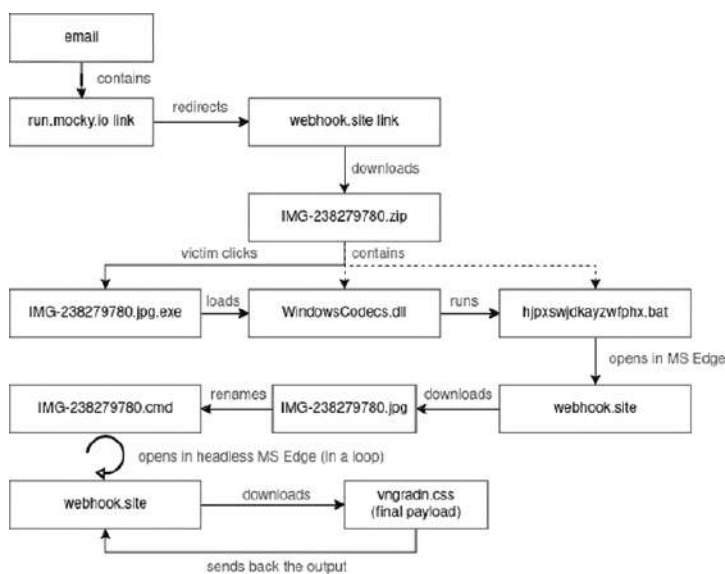
After clicking on the link, the user was first redirected to the run.mocky.io website and then to webhook[.]io, which provided the ZIP archive. These services are free and popular with IT professionals. It should be emphasised that using free, commonly used services instead of their own domains allows adversaries to significantly reduce the detection of malicious links and at the same time reduces the cost of their operation. This is a trend we observe in many APT groups.

The ZIP archive contained 3 files:

- a Windows calculator with a changed name, e.g. IMG-238279780.jpg.exe, which pretends to be a photo and encourages the victim to click,
- .bat script (hidden file),
- a fake Windows library Codecs.dll (hidden file).

If the victim launched IMG-238279780.jpg.exe (which is a harmless calculator), during start-up it would try to load the WindowsCodecs.dll library, planted by the attackers. This technique is known as DLL Side-Loading. The main purpose of the DLL library was to run the attached BAT script. After going through the successive stages of infection, the user was infected with the HEADLACE malware. A full analysis of the campaign is described on our website¹³.

FIGURE 13. Diagram showing the different stages of infection



13 <https://cert.pl/posts/2024/05/apt28-kampania>

In addition to malware-related activities, the APT28 group conducted intensive phishing campaigns targeting Polish government institutions. The objective of these activities was to phish for Microsoft Outlook account credentials, which could allow attackers to access sensitive information. Gaining such access would allow the theft of business correspondence, which would pose a serious threat to the security of information in these institutions. Access to the account could also enable the APT28 group to obtain data about employees from the address book, a valuable database for further activities. This scenario could also enable the group to distribute malware by exploiting trust in the senders of the messages.

FIGURE 14. Example of a fake Microsoft Outlook login panel from the APT28 group



National and international partnership and participation in the FETTA project

In 2024, as part of its activities related to monitoring the activity of APT groups, CSIRT NASK continued its close partnership with national CSIRTs (CSIRT MON and CSIRT GOV) and teams from Polish secret services, with which it regularly exchanged information about threats and carried out campaign analyses.

Thanks to international partnerships within the CSIRTs Network and with commercial partners, information on attacks taking place simultaneously in other European countries was exchanged, which contributed to the effective protection of citizens and institutions from threats.

In 2024, the CERT Polska team also became involved in the FETTA¹⁴ project (Federated European Team for Threat Analysis), the main task of which is to facilitate partnerships and knowledge exchange in the CTI area, including information on threats related to APT groups, vulnerabilities exploited, and new methodologies used by attackers.

14 <https://cert.pl/posts/2024/01/fetta>

Fraudulent advertising on major online platforms

Large online platforms offer a wide range of marketing services, such as high-ranking sponsored links in search engines or sponsored posts on social media. The potential of these tools has been recognised by fraudsters, who more and more often use them to distribute content that encourages users to, for example, share their contact details and express interest in participating in a fraudulent investment scheme.

Advertisements are designed to look like an article from a well-known news website or TV news channel, or an official announcement on a government website. The large number of advertisements and content that legitimises the scam means that criminals are successfully convincing some users to take part in a fraudulent investment.

In 2024, we have seen a significant increase in such incidents. In just one week in March 2024, CERT Polska blocked as many as 300 new websites using the image of Wojciech Cejrowski, and in the first quarter, it identified nearly 14,000 domains offering fraudulent investments¹⁵. The variety of content has also increased and has also started to include the sale of supplements, the promotion of fake law firms and fake fundraisers.

Criminals are very keen to use the images and status of famous people or brands to lend credibility to the scam they promote. In the course of our research, we noticed the use of the image of **more than 139 public figures**, including politicians, journalists, athletes, doctors and influencers. The advertisements contained doctored graphics or videos spreading false information about an alleged death, a compromising situation or a revealed conspiracy in order to arouse the user's interest and then get them to visit the website. This mechanism not only causes image damage to people whose image has been used without their consent but is also extremely dangerous to society. The trust that followers place in famous people is abused and used to steal from unsuspecting users, who then blame the victims of the scam for their financial losses.

The scale of this problem does not only affect Polish users, as it is a global issue¹⁶ – similar campaigns are observed virtually everywhere in the world. However, the fight against this practice is hampered by the insufficient reaction of online platforms to fraudulent content. This is especially true for those with the largest reach, belonging to tech giants such as Meta (Facebook, Instagram) or Google.

15 <https://archiwum.nask.pl/pl/aktualnosci/5368,CERT-Polska-Liczba-oszustw-finansowych-w-inter-necie-alarmujaco-rosnie-Na-co-uwaz.html>

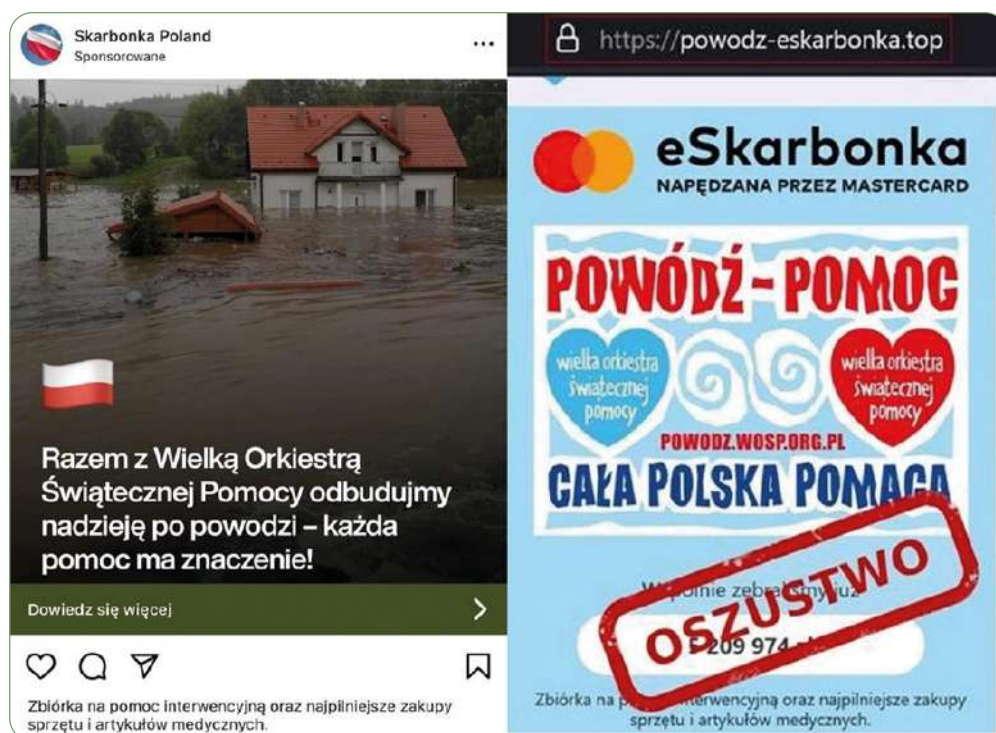
16 <https://www.debunk.org/the-largest-disinformation-and-scam-attack-ever-recorded-in-lithuania-part-i>

Campaigns observed using advertising on large online platforms

The problem of fraudulent advertising is not narrowed down to false investments. In 2024, we noticed the emergence of advertisements for medical products that are promoted using similar techniques to those used in investment frauds. The advertisements most often used the image of doctors as medical experts vouching for the effectiveness of a given drug, as well as journalists allegedly conducting a news report. The websites to which the advertisements led most often imitated popular news websites, such as TVP Info, or impersonated government news websites, such as the Ministry of Health. Pornographic material has also been used to advertise medication used to treat erectile dysfunction.

The criminals also exploit current events that the public is concerned about. The floods that took place in September 2024 quickly became the subject of their campaigns. The disaster caused significant damage in the Dolnośląskie Province, for example, resulting in many fundraising and aid campaigns. One of the campaigns, using sponsored posts, promoted a fake fundraiser supposedly organized by the Great Orchestra of Christmas Charity.

FIGURE 15. Example of a scam using the subject of the flood. On the left: an advertisement for a fake fundraiser; on the right: a website that was deceptively similar to the real eSkarbonka website run by the Great Orchestra of Christmas Charity



Problems with moderation by online platforms

Online platforms have the option of reporting malicious advertisements. Those belonging to Meta allow you to select the 'Report Advertisement' option, which makes it possible to report fraudulent content. At the same time, users have told us that their reports to Meta are often not accepted and are closed after 7 days with the status 'We have not removed the ad'.

To verify these reports, we tested reporting ads that we considered fraudulent from a standard Facebook user account from January to November 2024. Only 10 of the 122 notifications of malicious ads were removed. In 106 cases (87% of all cases), the reports were closed with the status 'Ad not removed' and in 6 cases, no response was received.

One of the challenges faced by platform moderators and analysts is known as cloaking, a set of methods used by fraudsters to display a different page or advertisement to verification mechanisms than to actual users. Before redirecting the user to a fraudulent website the criminals check, for example, what browser and via what website the user entered the advertising website. If it was not done directly by clicking on the advertisement, the user is often redirected to a website that looks like a normal, harmless website. Such practices can make moderation significantly more difficult.

Restriction of the visibility of the CERT Polska article on fraud by the Meta company

On 25 November 2024, an analysis¹⁷ was published on the CERT Polska website, which comprehensively shows how fraudsters use social media platforms to steal from Poles. A link to the article was also posted on Facebook. However, the article was removed from Facebook shortly after publication. Articles written by the media that decided to cover the CERT Polska publication suffered a similar fate.

Due to the problems that occurred, CERT Polska presented a statement on its website¹⁸ regarding Meta's limitation of the visibility of the article about fraud on the Facebook platform. After the deleted posts were republished, Meta representatives were presented with expectations¹⁹ regarding problems related to fraud on their platforms. The expectations were also published on the CERT Polska website.

17 <https://cert.pl/posts/2024/11/Oszustwa-reklamowe-na-duzych-platformach/>

18 <https://cert.pl/posts/2024/11/blokada-na-meta-stanowisko/>

19 <https://cert.pl/posts/2024/12/oczekiwania-wobec-meta/>

After a few days, Meta restored the posts related to the article. Talks then began on, for example, integrating the Warning List with Meta's platforms to better protect Polish users from scams.

Presentations on scams on social media platforms at the Oh My Hack 2024 conference

The problem of advertisements on social media platforms was the topic of two presentations at the Oh My Hack conference, which took place on 26 November 2024. One of them was the presentation entitled 'ScamBook', in which Paweł Srokosz from CERT Polska and Piotr Zarzycki from CERT Orange Polska talked about scams that occur on the Facebook platform. The recording of the presentation is available on YouTube²⁰. The observed weaknesses of moderation processes on social media platforms were also the topic of Jakub Mrugalski's presentation 'Fraud, malware and pseudo-moderation – the other side of social media', which also took place during the conference.

Summary

In 2024, CERT Polska observed an increasing use of online platforms for the distribution of fraudulent content. It has also been observed that fraudsters commonly exploit technical weaknesses in the verification methods used by platforms to circumvent the built-in moderation mechanisms.

One solution that can help to identify malicious websites in Poland is the Warning List, which has been used by telecommunications network operators since 2020 to block access to malicious websites. Every click on an advert often involves a tracking link before the user is forwarded to the final page. If the tracking link prevented forwarding to links with domains on the Warning List and automatically blocked adverts that link to these domains, it would significantly reduce the effectiveness of scammers' campaigns.

In 2024, we added 52,131 domains to the Warning List that were associated with fraudulent investments, accounting for 55% of all domains added to the List. This compares to around 32,000 domains and 40% of all domains added in 2023.

For more information on the threat, see our analysis 'Advertising scams on large online platforms' (<https://cert.pl/posts/2024/11/Oszustwa-reklamowe-na-duzych-platformach>) published on the CERT Polska website.

20 <https://www.youtube.com/watch?v=AastpuFMHEU>

Mobile malware

In this chapter, we present statistics on malware for Android mobile devices observed and detected by the CERT Polska team in 2024. The data comes from threat hunting, user reports and the MWDB platform.

TABLE 4. Malware statistics for Android mobile platforms in 2024

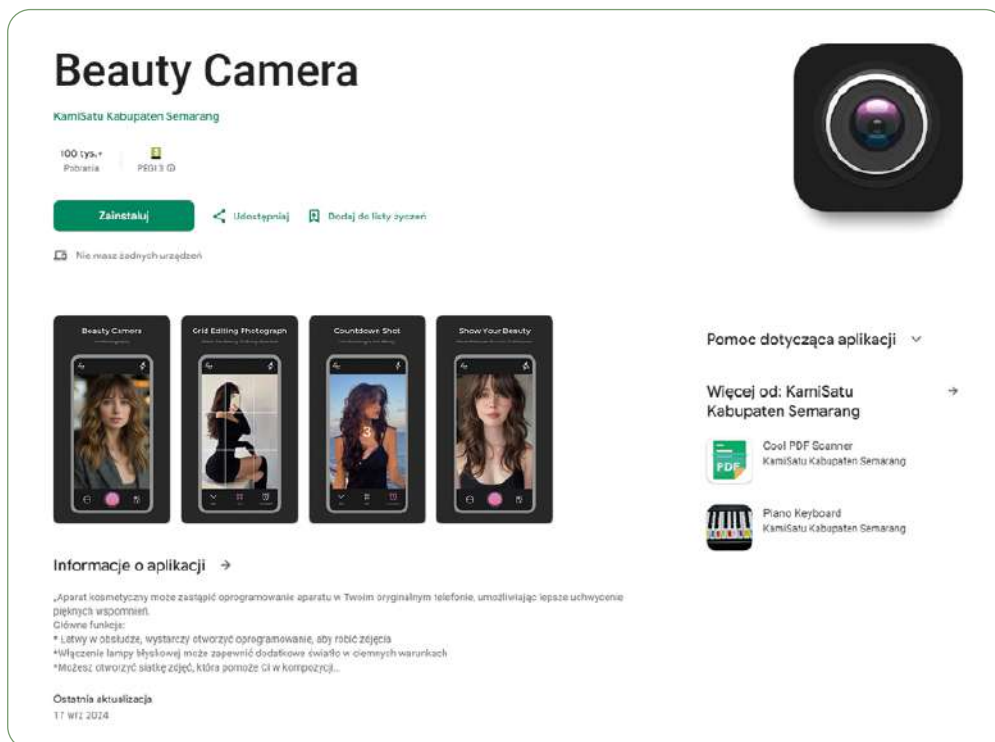
Family name	Number of samples
Coper	2,827
Hook	539
Cerberus	211
SpyNote (Spymax)	177
Ermac	154
Joker	97
Hydra	81
Alien	75
GodFather	41

In 2024, we identified a total of 4,202 malware samples for Android mobile devices. The rest of the samples we observed could not be clearly categorised into one family. The vast majority of the samples were not targeted at Polish users and were also observed in previous years. It should be noted that the Joker malware was the only campaign distributed through the official Google Play app store. The other samples were hosted on external websites.

The Joker campaign

The first samples of Joker were observed as early as 2019. It has evolved over the past years and in 2024, according to the data we had, it became the largest campaign distributed on the Google Play platform. Joker is aimed at a larger group of end users, including Polish recipients. The average time that malware is available in the Play Store is between a few days and a few weeks. During this time, the malware is downloaded by thousands or even hundreds of thousands of users. All samples detected by CERT Polska in 2024 were reported directly to Google and removed from the Google Play Store.

FIGURE 16. Example of Joker malware in the Google Play store



Joker always disguises itself as a seemingly harmless application, e.g. a photo editor, emoji, messenger, flashlight modifiers and many more. After the user downloads and activates the app, the interface looks harmless and is as described on Google Play, as in the example above: 'The beauty camera can replace the camera software on your original phone, allowing you to capture beautiful memories better'. A comprehensive analysis of the malware's behaviour revealed a sophisticated and malicious mechanism designed with the objective of subscribing users to premium services without their knowledge or consent. It is a multi-stage process that utilises encrypted communication, obfuscated code and unauthorised access to sensitive user data. After analysing each component and flow of operations, we can conclude that the application poses a serious threat to the security, privacy and finances of its users. For more information on the campaign and a detailed technical analysis, see the article 'The Dark Knight Returns: Analysis of the Joker Malware' (<https://cert.pl/posts/2024/10/analiza-joker>).

Activities of CERT Polska



The Act on Combating Abuse in Electronic Communications

The Act on Combating Abuse in Electronic Communications came into force in September 2023, but most of the provisions on specific solutions came into force throughout 2024.

Malicious text message templates

The biggest new statutory task we have been given is to maintain a list of malicious text message patterns. In partnership with telecommunications operators, we have created a process and tools to improve record keeping.

Based on the analysis of the reports received, we publish regular expressions that describe specific messages or entire text message campaigns. The register is updated via a system to which text message operators have access. Within 5 minutes of publication, the pattern is automatically downloaded, and the operator is obliged to block any message that matches the pattern. As part of the fight against smishing, we also keep a list of text message sender id reserved for public entities. An institution that reports such a sender id obtains full rights to it, thus blocking any attempt to send a message with a given sender id by another sender.

In 2024, we created 746 templates, which resulted in 1,475,366 undelivered text messages. After the implementation period, the number of blocked text messages increased significantly. In the second half of the year, we registered 1,363,706 messages, which accounted for 92% of all blocked text messages. The sender id list included 271 ids registered by 254 institutions.

Text message report statistics

In 2024, we recorded more reports (354,566) than in the previous year (221,880). This represents a year-to-year increase of 60%. The number of messages considered to be malicious also increased compared to the previous year (119,752) (140,659). When interpreting this figure, it is important to note that starting in 2024 we also consider messages that do not contain a link but follow known fraud patterns to be malicious. The change in the way the statistics are kept was due to the legal definition of smishing, which does not require a link in the message.

It should be noted that in 2024, the highest number of reports was recorded in January (as many as 102,602). The mechanism for blocking text message patterns came into effect in April 2024, so for the purpose of analysing the effects of the act, the corresponding periods of April to December 2023 and 2024 should be compared. Furthermore, due to the advertising campaign for the 8080 number, we received more than 1/3 of the reports for the entire period of April to December in December 2023, so this month should also be considered unreliable.

From the beginning of the second quarter to the end of November, we recorded 96,704 (2023) and 155,543 (2024) reports. This corresponded to the identification of 49,646 and 53,681 malicious messages respectively. Considering the fact that the second number also includes messages without a link, we have recorded a decrease in the share of smishing in reports from 51% to 36%. For the first time since we started monitoring this attack vector, we can say that the increase has stopped, and maybe even that the number of malicious text messages in Poland has decreased.

If we consider the effects of the blockages alone from the beginning of April 2024 to the end of December 2024, each malicious message reported to us resulted in 24 messages not reaching their potential victim. Based on the analysis of the results from the second half of the year, one reported message resulted in 31 malicious messages not being delivered. November was a record-breaker in this respect, when this ratio stood at 49. That is why we still encourage you to send messages to **8080**. This is not only a way to get an answer to the question 'Is the message malicious?', but also to share information with us so that we can react as quickly as possible, because when it comes to this process, the reaction time is what counts.

The statistics above allow us to draw the conclusion that the message blocking mechanism has visible effects. However, this is not enough to declare victory in the fight against smishing. It should also be remembered that there are other ways in which fraud is distributed – the fact that fewer fraudulent text messages are reaching users most likely means that fraud is taking place on other communication platforms.

Secure mail

The Act on Combating Abuse in Electronic Communications has imposed an obligation on public entities to use SPF, DMARC and DKIM mail protection mechanisms. Together, they prevent e-mail spoofing, especially if both the sender and recipient of the e-mail use them. The statutory obligation only applies to public entities, but since these entities work with private sector companies, we felt it was important to support both sectors in configuring SPF, DMARC and DKIM. Therefore, in 2023, we created the website bezpiecznapoczta.cert.pl, to allow organisations to check the configuration correctness of mechanisms that increase the security of e-mail. The system is similar to the available English-language solutions, but its advantage is the accurate Polish translations of errors.

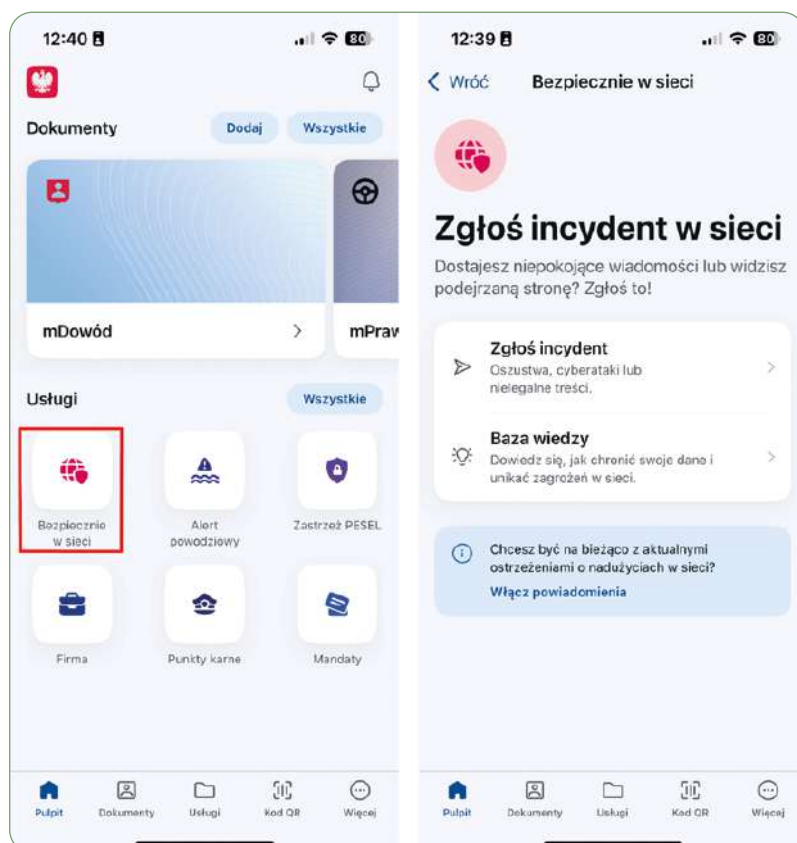
The website is constantly used by a large number of entities, both public and private. In 2024, users checked the correctness of the configuration of approx. 24,000 domains using bezpiecznapoczta.cert.pl, including approx. 10,000 domains more than once.

Since the system is an open-source tool available in our GitHub repository (<https://github.com/CERT-Polska/mailgoose>), it can also be used by other CSIRT teams. Its structure allows for convenient translation into other languages and a change of the interface colour scheme in accordance with the corporate identity of a given institution. For example, the National Cyber Security Centre of Lithuania has launched a similar system at <https://sauguspastas.nksc.lt/>, and other European CSIRT teams are interested in launching similar solutions.

CERT Polska in the mObywatel application

On 13 August 2024, in partnership with the Centralny Ośrodek Informatyki (Central Computing Centre), we launched **the Network Safety** service. As part of our joint efforts, we have created a product that allows users to receive notifications about threats and provides access to a database of knowledge about various aspects of cybersecurity. An additional reporting channel has been created, better suited to the needs of mobile device users.

FIGURE 17. On the left: the Network Safety Service icon on the main screen, on the right: the Network Safety Service in the mObywatel application



Reporting to CERT Polska

In the mObywatel application, the user can:

- report a link leading to a fraud (**Malicious website**),
- provide a description of a potential fraud (**Fraud**),
- send information about another incident (**Another**), e.g. about the incorrect configuration of the public service used by the user.

The user can also obtain information about the correct way to report text messages and e-mails via other channels provided by us, namely **8080** number and using the form on the website **incydent.cert.pl**.

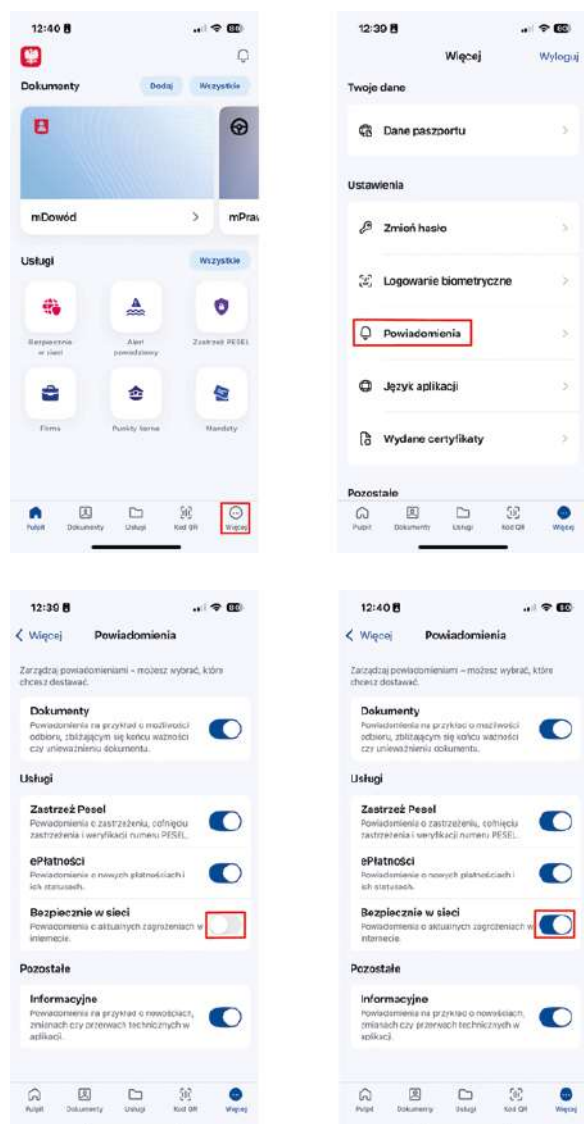
Threat notifications

The notification service was created to reach the largest possible group of recipients with a message about a currently observed fraud pattern. This may concern a specific campaign or an increase in recurring scams, e.g. in the pre-Christmas period these are scams related to messages about problems with parcel delivery.

Each notification from CERT Polska is titled '**Network Safety Alert**' and consists of two parts: a short introduction located in the notification bar, and a description that elaborates on the subject of the warning. For this reason, it is worth clicking on the notification to see its full content. Archived notifications are available for re-reading for several days in a list that appears when you press **the bell** icon in the upper right corner of the main view of the mObywatel app.

Notifications are optional, so each interested user must **enable them themselves**. This can be done by pressing the **More** button in the lower right corner of the main screen, then selecting **Notifications** in the **Settings** section and checking the appropriate field in the **Services** → **Network Safety section**. More than 160,000 users are already using the optional notifications.

FIGURE 18. Instructions on how to enable notifications in the Network Safety Service.



Knowledge database

The objective of the knowledge database is to provide a wide range of users with the necessary information on the subject of cybersecurity. The articles included in this collection can cover a variety of topics, including advice on cyber hygiene, descriptions of common scams, and an introduction to the work of CERT Polska and other institutions. At the end of 2024, the Knowledge database contained articles describing, for example, the rules for properly securing an account and creating a secure password, as well as the most common fraud schemes. In the last quarter of 2024, the Knowledge database was used by almost 48,000 users.

The Warning List

We have been maintaining a dangerous websites Warning List since March 2020. One of the important developments in this regard was the launch of the free phone number 8080 at the end of 2023 for reporting suspicious text messages, including messages with links. Our team verifies the links. If they lead to a harmful website used by fraudsters to mislead users and phish for data, the website is added to the Warning List. In total, our team analysed more than 300,000 reports of suspicious websites in 2024 based on text messages received in combination with domains submitted via the form available at incydent.cert.pl, as well as domains reported by partners. In 2024, 92,600 malicious domains were added to the Warning List, compared to 79,300 the year before. In 2024, these were mainly websites offering fake investments and domains posing as popular websites in order to phish login details from potential victims.

There has also been a noticeable increase in the number of users of the second version of the Warning List, in which changes have been made to make it easier to use by keeping harmful domains for 6 months. If a domain still contains dangerous content after six months, it is added as a new entry. This limits the size and content of the List to current threats. The total number of downloads of all formats of the Warning List in 2024 was 345 million, an increase of 80% compared to 2023.

The Warning List fulfils its function. We can also see this thanks to the statistics collected by some entities, including one of the largest telecommunications operators in Poland, clearly showing how many fraud attempts we have been able to block and thus protect users from harmful content. Based on our own data and the data provided by our partners, we can estimate the number of visits to undesirable websites blocked by the Warning List in 2024 at 71.8 million. Compared to 2023, this is an increase of 33%.

As every year, we encourage you to report any questionable links or domains using the form available at <https://incydent.cert.pl> and to forward suspicious text messages to 8080 number. We would also like to thank all reporting persons – every piece of information contributes to increasing the security of network users.

CERT Polska as a CVE Numbering Authority

In 2024, the CERT Polska team continued its activities as CNA (CVE Numbering Authority), thus strengthening its involvement in the global vulnerability management system.

Changes to CVE in 2024

Since 1 August 2023 CERT Polska has had CNA status, which allows it to assign identifiers and publish information about vulnerabilities in the international CVE (Common Vulnerabilities and Exposures) programme, supporting the disclosure of security vulnerabilities in software or computer hardware. Since 1999, the programme has been cataloguing vulnerabilities and assigning them unique identifiers. In its 25th year, the programme has undergone a number of changes. MITRE, the organisation responsible for managing it, has published updated guidelines for CNA. According to these guidelines, if a vulnerability is harmful and there is a risk that it may be publicly disclosed, it is possible to assign CVE identifiers regardless of whether or not customers need to update their software. Moreover, the new edition of the CWE (Common Weakness Enumeration) guidelines 'Root Cause Mapping' has been developed to identify the cause of a problem even more precisely. In accordance with MITRE's suggestions, we have carried out a remapping of CWEs in the CVE entries we have published to date. The new version of CVSS (Common Vulnerability Scoring System) 4.0, which replaced the previous 3.1 model, extended the risk assessment to include additional factors, such as detailing the impact of the vulnerability on external systems. We quickly adapted the changes to our processes, allowing us to publish information in accordance with the latest standards.

The specialists from the CERT Polska team shared their experiences in coordinated vulnerability disclosure with representatives of the public and private sectors during industry meetings: Partnership for Cybersecurity, Winter School of Cybersecurity, Hackbreakers' Meetup or the scientific conference 'Security online. Cyber resilience'.

Coordinated vulnerability disclosure in the European Union

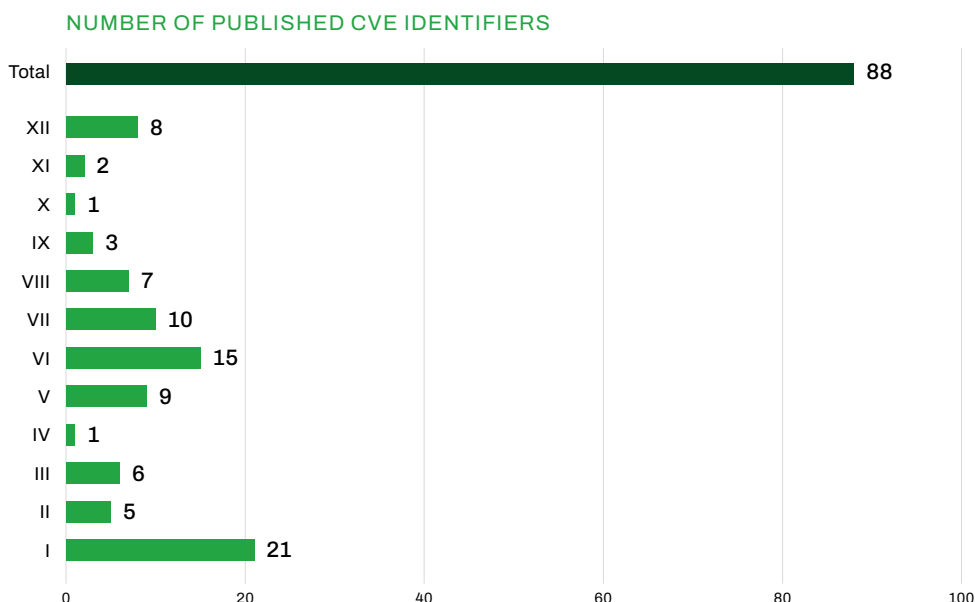
The process of coordinated vulnerability disclosure was introduced into the European legal system through the provisions of the NIS 2 Directive. According to the Article 12, each Member State should designate one of its CSIRTs to act as a coordinator. Under the Polish law implementing the NIS 2 Directive, our team has been appointed to this role.

In 2024, the European Union introduced new regulations on the obligation to report actively exploited vulnerabilities and serious incidents in products with digital elements under the Cyber Resilience Act (CRA). This act also provides for the voluntary reporting of any vulnerabilities and cyber threats to the CSIRT designated as the coordinator, what imposes additional tasks in this area on the designated CSIRT. The CERT Polska team is preparing to implement its new responsibilities by, for example, monitoring ENISA's launch of the European Vulnerability Database (EUVD) and actively participating in consultations on the design of the Single Reporting Platform (SRP). The goal is to create a central point for reporting vulnerabilities in the European Union with the objective of standardising data and the flow of information at the EU level.

Important vulnerabilities disclosed

CERT Polska disclosed 88 vulnerabilities in various systems and applications in 2024. Before disclosure, the team coordinated contact between the parties involved, supporting researchers and software manufacturers in responding to threats quickly and responsibly.

TABLE 5. Number of vulnerabilities disclosed in each month of 2024



The coordinated disclosure of serious vulnerabilities in the Comarch ERP XL software was carried out in a CVD (Coordinated Vulnerability Disclosure) process in partnership with one of the largest software manufacturers in Poland. The vulnerabilities were reported, confirmed, fixed and published. They included:

- [CVE-2023-4537](#) – downgrading the MS SQL protocol to an unencrypted form, which made it possible to spy on and modify communications,

- [CVE-2023-4538](#) – encryption of authentication data using the same shared key in all vulnerable versions of the software facilitated the retrieval of passwords in unencrypted form,
- [CVE-2023-4539](#) – using the same hard-coded password for a special database account allowed access to stored information.

The most complex CVD process in 2024 was the coordination of a report concerning data protection errors in medical clinic software, as this process involved the need for independent verification of the vulnerabilities with the manufacturers of the 6 programs listed in the report we received. In the case of Eurosoft Przychodnia ([CVE-2024-1228](#)), drEryk Gabinet ([CVE-2024-3699](#)) and SimpleCare by Estomed Sp. z o.o. ([CVE-2024-3700](#)) the vulnerability consisted in using a permanently encoded password for the database, which was the same in all systems. However, in Asseco's mMedica software, a similar vulnerability was discovered internally and fixed in previous years, which is why we did not assign a CVE identifier. The Kamsoft KS-AOW and Kamsoft KS-PPS software did not use hard-coded passwords, only predefined ones, and no changes were required during installation. The manufacturer has announced that it intends to introduce solutions to discourage the use of default passwords. Our analysis has also shown that it is a bad practice for administrators of many medical facilities to allow access to the medical database from the public Internet network. This allows attackers to carry out brute force attacks on credentials or to exploit vulnerabilities of this type to obtain sensitive data stored in the database.

CERT Polska, as part of its own research, found a number of critical vulnerabilities ([CVE-2024-1576](#), [CVE-2024-1577](#), [CVE-2024-1659](#), [CVE-2024-6160](#), [CVE-2024-6527](#)) in the MegaBIP software used to publish the Public Information Bulletin. Due to the fact that new and serious vulnerabilities are still being found and the unsatisfactory partnership with the software author, we have requested relevant recommendations. On 12 June 2024, the Government Plenipotentiary for Cybersecurity imposed an obligation on entities of the national cyber security system, including public entities, not to use SmodBIP and MegaBIP systems to provide public information. We disclosed vulnerabilities in the SmodBIP software ([CVE-2023-4837](#), [CVE-2023-5378](#)), which had not been supported for many years, at the end of 2023.

Articles containing information about all vulnerabilities disclosed by the CERT Polska team are published at cert.pl/cve. For more information about how our team handles vulnerability reports, please visit cert.pl/cvd.

Education and promotion – we continue our efforts to build cybersecurity awareness among Poles

Another record-breaking year is behind us. This refers to both reports and incidents, the number of which exceeded 100,000 in 2024. The average monthly number of reports processed by the CERT Polska team is around 50,000. Of course, many factors contributed to this situation. Cybercriminals are as active as ever, but awareness of cyber threats is also growing, thanks in part to the various activities undertaken by the CERT Polska team. This includes educational and promotional campaigns, as well as the presence of experts in national and local media and at industry events. Another example of this is the participation of the CERT Polska team in coordinating the vulnerability disclosure process.

Communicating about threats

Our activity on social media is not without significance in building knowledge about threats in the area of cybersecurity. Regular warnings are one of the things that deserve attention. They concern the biggest scammer campaigns and are published simultaneously on the CERT Polska profiles on Facebook, X, and LinkedIn. A new feature introduced last year was push notifications sent via the mObywatel app, informing about current cyber threats. They are part of the new Network Safety service, which also allows you to report an incident and update your knowledge with easy-to-understand articles on how to stay safe on the Internet. We have written more about the new service in [the article 'CERT Polska in the mObywatel application'](#) (p. 46). It is worth noting that submitting reports using the application was one of the topics of a media campaign carried out by the Central Computing Centre in partnership with the Ministry of Digital Affairs.

Educational cycles

In addition to warnings about scams in social media channels, regular educational cycles are also published. In April we launched our

FIGURE 19. Network Safety service in the mObywatel app



#WiedzaInformacje (Knowledge Information) series, dedicated to AI and in particular to the phenomenon of deepfake. In the posts, we described topics such as the origin and history of deepfakes, examples of their use, and misconceptions about them. We also suggested what to look out for in order to recognise manipulated material. In June, ahead of the European Parliament elections, we published an article entitled 'Deepfake and the elections' on the cert.pl website, together with posts. It drew attention to, for example, the possibilities of deepfake technology, such as the generation of fake statements by politicians.

During the summer holidays, as in 2023, we presented the #CyberParawan (Cyber Screen) series, in which we described the scenarios used by fraudsters and gave tips on how to deal with cyber threats. We started with the 'booking fraud' for people who were still planning their trips. In this scam, fraudsters take over the accounts of venues on booking websites (not only on the website from which the scam takes its name). In the second part of the series, we recalled a scam targeting parents of children away from home. It starts with a WhatsApp message saying, 'Dear parent, my phone has broken.' The aim of this scam is to extort money. We have prepared the third post with holiday entertainment enthusiasts in mind and described what is known as a ticket scam. We also discussed the topic of telephone fraud, in which the caller pretends to be a foreign police or customs officer, and warned against sensational headlines on social media.

In December, we published the #12CyberPorad (12 Cyber Tips) series, in which we reminded users of the rules for creating strong passwords and recommendations on enabling two-factor authentication.

Industry conferences

We supplemented the educational activities mentioned above with our presence at key industry conferences such as Black Hat in Las Vegas, hack.lu in Luxembourg and Oh My Hack in Warsaw. In Las Vegas, Krzysztof Zając presented the capabilities of the Artemis system, and during Oh My Hack we talked about a model way of reporting incidents, fighting smishing and fraud on large platforms. Krystian Szeffler, who took part in the Security Case Study, used examples to explain why it is worth taking care of industrial security and emphasised that the Snitch tool developed by the CERT Polska team is a solution to the challenges in this area. We also attended TF-CSIRT meetings and job fairs, took part in international competitions and exercises (which are also described in this report), and provided expert support to hackathon participants.

FIGURE 20. Illustration used to promote the #12CyberPorad (12 Cyber Tips) series on social media



FIGURE 21. Krzysztof Zając at the Black Hat conference in Las Vegas

In the past year, we have also written articles on current threats, including the Joker malware, the fake Captcha problem and fraud on large online platforms, to which we also devote a separate [article in this report](#) (p. 37–40).

Coordinated vulnerability disclosure

CERT Polska also complements its expert image as a CNA (CVE Numbering Authority), a role it has held since August 2023. This allows our team to contribute to the vulnerability database by assigning identifiers and publishing vulnerability information in the CVE programme. Over the past year, we have assigned 88 such identifiers to vulnerabilities, including those discovered as part of our research activities. It should be stressed that we are the only institution in the country to perform this function and the seventh CERT in Europe.

CVE (Common Vulnerabilities and Exposures) is an international programme supporting the disclosure of security vulnerabilities in software or hardware. Anyone who finds a vulnerability can report it to the organisation that is the CNA, i.e. the CVE Numbering Authority. Coordinated disclosure of vulnerabilities is usually a complex and lengthy process, involving establishing secure contact with the appropriate recipient, removing the vulnerability and distributing the corrected software to customers. Sometimes, it takes several months from the report to the publication of the information. This makes us all the more pleased with the result achieved last year – it is a confirmation of the high standards of service for this type of report provided by CERT Polska. The software bugs we have disclosed are described in the article [‘CERT Polska as CVE Numbering Authority’](#) (pp. 49–51).

The activities discussed above build the recognition of the CERT Polska brand and trust in it. They also result in an increase in the number of reports, and a larger

pool of reports provides a more complete picture of what is happening in cyberspace and the opportunity to act and react more effectively. Therefore, campaigns promoting the value of reports and educating about cyber threats are set to continue in 2025.

SECURE

The 27th edition of the Secure conference is behind us. Two days in April, filled with knowledge and important discussions, brought together over 500 participants in Warsaw. The slogan of the 2024 edition was 'Horizon of cyber challenges'. However, we did not focus exclusively on the future – many presentations concerned current issues and showed that in the third decade of the 21st century it is about time to realise that cybersecurity is simply security.

This belief resonated very strongly in the speeches and discussions that took place as part of the plenary programme. Earlier, during the opening of the conference, NASK-PIB director Radosław Nielek spoke about it. Cybersecurity in this broad context was also presented by the Deputy Prime Minister and Minister of Digital Affairs Krzysztof Gawkowski, and the Trend Map presented by Natalia Hatałska clearly showed that we are moving towards a world in which technology is even more integrated into everyday life. The first block of presentations was closed by Sebastian Kondraszuk, the then manager of CERT Polska, who presented our annual report for 2023 and, like the previous speakers, emphasised that cybersecurity concerns every citizen. He also pointed out the still prevailing trend of social engineering scams.

After the plenary session, the lectures were divided into two paths: technical and local government/policy. The technical path was dominated by our specialists. Bartosz Trybus, Krzysztof Szafarski, Jarosław Jedynek, Krzysztof Zajac and Filip Marczewski shared conclusions from their daily work and presented the tools they develop at CERT Polska. They talked about [Artemis](#) (p. 67), we also got acquainted with the analysis of incidents related to ransomware and we had the opportunity to learn about the rules of cyber hygiene in an organisation.

Although the second path focused mainly on legal solutions, our representative was also present there. Szymon Sidoruk took part in a debate on the Act on Combating Abuse in Electronic Communications, during which he presented the perspective of people receiving reports of abuse.

The second day of the conference began with a lecture by INHOPE Executive Director Denton Howard on international standards for combating CSAM. Next, Deputy Minister of Justice Krzysztof Śmiszek took the stage to talk about AI in the context of human rights, followed by Professor Przemysław Biecek, whose presentation served as an introduction to the AI cybersecurity track.

Subsequent speeches concerned ways of navigating in a world in which artificial intelligence is a fact and an important component of reality. This topic was also addressed by Dr Agnieszka Gryszczyńska from the National Public Prosecutor's Office and Agata Ślusarek from the Polish Financial Supervision Authority, who talked about how LLM is already being used by cybercriminals.

An important part of the conference were the accompanying workshops for a wide range of specialists. Participants could learn the secrets of mobile malware analysis, get to know the MISIP system in an introductory or advanced training course, and learn crisis communication in case of incidents. After the conference, participants could also take part in a two-day training course on Cybersecurity Resilience in Critical Infrastructure organised by the SANS Institute, CISO4U and CISO Poland. The instructor was Tim Conway, director of the SANS Institute.

Secure is the oldest Polish conference on cybersecurity. In 2024, for the 27th time, we managed to gather experts willing to share their knowledge in one place. In 2025, the conference is going to be one of the flagship events of the Polish Presidency of the Council of the European Union and is scheduled to take place in Bydgoszcz.

#BezpiecznyPrzemysł (Safe Industry)

In 2024, we continued the #BezpiecznyPrzemysł (Safe Industry) initiative, which aims to increase the level of cybersecurity of Polish industrial infrastructure. We focus on identifying industrial devices accessible from the public Internet, such as PLC controllers and operator panels (HMIs), and informing owners about the threats arising from their improper configuration. Thanks to the CERT Polska made system [Snitch](#) (p. 69) (details later in the report), and its subsequent improvements, the visibility of scanned devices has increased, as well as the efficiency of the monitoring, decision-making and incident response processes.

Events

Four treatment plants and further discoveries

In January 2024, there was an intrusion into the control systems of municipal wastewater treatment plants. In March we obtained a recording from the Telegram messenger, in which a hacktivist group bragged about their activities on one of the Russian-language channels. They presented the possibility of modifying the parameters of the technological process – changing the mode of work from automatic to manual and showing the possibility of controlling the equipment, i.e. pumps, mixers or blowers.

FIGURE 22. Main menu of the control panel of the wastewater treatment plant



FIGURE 23. Settings of the technological process of the treatment plant, with the possibility to change the operating modes



The main menu of the panel displayed the name of the treatment plant and the direct contact details of the website for the automation system. This is a common practice that facilitates efficient contact. During conversations with engineers, they shared their version of events from that time:

Some time ago we received information from these facilities that the technological parameters had changed for unknown reasons. We reacted immediately to restore the normal work agreement. It happened only once. It did not occur to us that it could be an attack by external hackers because such an incident had never happened before.

In the end, it turned out that the HMI panels from Weintek were accessible from the Internet via SIM routers with a VNC remote desktop. A simple login password was probably used, which led to unauthorised access. Fortunately, the attack had limited consequences, and the remote access was disconnected. Passwords on VNC servers are limited to only 8 characters, and the service does not have any

limits on the number of unsuccessful login attempts, making it possible to perform a brute force password attack.

Later, as part of routine searches for public unsecured systems, we found two more instances based on the same Weintek system. We recognised them by the design of the panels and the contact details they contained. After contacting engineers in charge of the systems, the remote access was secured.

FIGURE 24. Start screen of the control panel of a sewage treatment plant with visible contact details.



Remote desktop

For many years, we have been monitoring poorly secured remote desktops. Despite the notifications we send out, we regularly learn about systems that have been compromised, most often due to the use of a simple password. One of the most frequently observed reports used to connect to industrial systems via remote desktop is VNC. For this reason, we decided to scan VNC server instances with easy-to-guess passwords within Polish address space. Five passwords were selected that are frequently used in industrial devices and were used to verify the collateral of 7,806 VNC servers available in Poland. As a result, 299 instances with insufficient security were identified. Many of them provided access to control panels of facilities such as water treatment stations, industrial furnaces or small hydropower plants. On this basis, actions were taken to identify the owners of these facilities and inform them of the threat.

FIGURE 25. Screenshots of some of the found panels



Web application audits

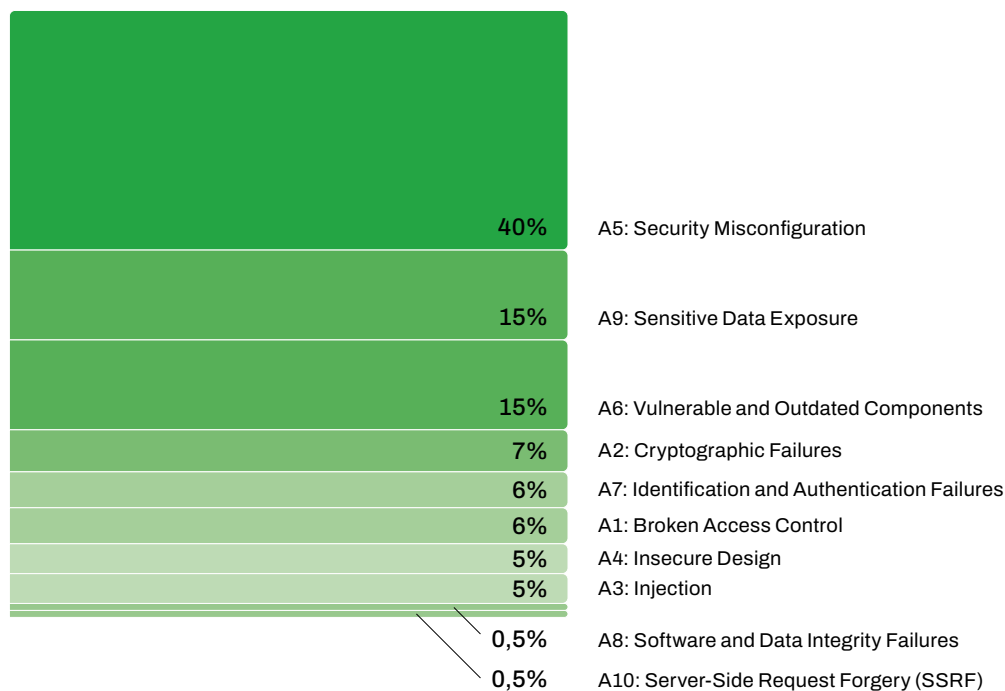
The Security Testing Team operating within CERT Polska carried out a series of security audits in 2024, 82% of which involved penetration testing of web applications. The aim of the tests was to identify vulnerabilities in many systems. These vulnerabilities could pose a threat in the event of possible attacks on individual application components.

We conduct various types of research and apply selected strategies and techniques to each of them. The work scenarios that we use for specific tests are the result of our proprietary approach to ICT system audits. They are based on the experience of specialists and methods based, for example, on sources and standards such as OWASP (Open Web Application Security Project).

The most important elements of our methodology are: system analysis and threat identification, manual tests supported by automatic tests, reporting, i.e. presentation of the results of the audit carried out, taking into account the level of criticality of security vulnerabilities, together with recommendations adapted to the specificity of each system.

We used OWASP Top Ten 2021 to classify vulnerabilities. Due to the frequent lack of access to application logs, we replaced category A9: Security Logging and Monitoring Failures with category A9: Sensitive Data Exposure, which includes vulnerabilities resulting from incorrect implementation of mechanisms for the protection of sensitive data.

CHART 1. Chart showing vulnerabilities by category



The results of the audits carried out indicate which areas require improvement. A significant percentage of vulnerabilities were recorded in four categories:

- A5 – implementation of incorrect system safeguards (40%),
- A6 – obsolete versions of components (15%),

- A9 – incorrect implementation of mechanisms protecting sensitive data (15%),
- A2 – incorrect implementation of cryptographic solutions (7%).

Incorrect configuration of security solutions (A5, A2) and systems with known security vulnerabilities (A6) make the system an easy target, even for less advanced attackers. If the vulnerabilities are exploited by an attacker, there is a likelihood that they may gain control over critical infrastructure components, gain access to confidential data, including internal URL/IP addressing information, employee e-mail addresses, and configuration files available on the server, and, in the worst case, completely take over the infrastructure.

A high percentage of vulnerabilities related to the implementation of basic protection mechanisms and sensitive data left on the server (A9) indicate the need for audits, updates of system configurations and components, and the application of current security practices. If these measures are carried out regularly, threats can be eliminated at an early stage, thus significantly reducing the risk of successful attacks on systems and applications.

The lower vulnerability rates were in the following categories:

- A7 – incorrect implementation of authentication/identification mechanisms (6%),
- A1 – incorrect implementation of authorisation mechanisms (6%),
- A3 – incorrect implementation of data input control/validation mechanisms (5%).

Incorrect access control to resources or even a lack of access control (A7, A1) leads to critical security violations. Authentication is a key process aimed at ensuring that only units with specific privileges gain access to use specific resources. Confirmation of the requester's identity is necessary for effective access control. Without proper authentication and authorisation, an attacker can try to access API resources, for example, which can lead to potential violations of data confidentiality and integrity. Depending on the nature of the errors in the implementation of the authorisation mechanisms, unauthorised access can lead, for example, to the user performing operations within the application that should not be possible due to a lack of authorisation.

In the case of incorrect implementation of data input control/validation mechanisms (A3), remote code execution, i.e. complete takeover of the system, may occur. Input data provided by the user should always be considered as potentially threatening the security of the application and therefore properly controlled.

The audit results confirmed the need for regular penetration tests, which – when supplemented by the systematic implementation of recommendations – minimise the risk of potential attacks and enable more effective system protection.

Locked Shields 2024

Locked Shields is the world's largest defence exercise simulating an attack on ICT infrastructure, organised since 2010 by the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE). With each edition, the exercise becomes more and more complex, which affects not only the technologies used and the systems defended, but also the scenario, non-technical and strategic components, and the number of participants. In 2024, more than 4,000 specialists from 40 countries took part in the exercise.

The aim of the Locked Shields exercise is to test the defence capabilities of NATO members and invited guests in a simulated cyberattack on national infrastructure. Since 2022, all teams have been made up of representatives from two countries (or a country and a NATO entity), thus strengthening partnerships and comparing crisis management procedures. For 48 hours, each team, acting as the fictitious island nation of Berylia, defends its copy of critical infrastructure against attacks by the organisers, who take on the role of the hostile country Crimsonia.

In recent years, exercise organisers have placed increasing emphasis on non-technical aspects and issues related to effective partnerships. Media, legal or strategic decision-making teams must analyse and respond to current events to the same extent as technical teams respond to ongoing attacks. During the exercises, a complex scenario was implemented in which technical knowledge and situational awareness were intertwined with strategic decisions and legal analyses. The technical part challenged the participants from all countries to repel more than 8,000 attacks on 6,000 virtual systems.

The Polish-Finnish team and the Austrian-Swiss team were recognised for their cross-team exchange of information about threats, which had a positive impact on the results of all participants in the exercise. Finally, the Polish-Finnish team was one of the top 3 teams, along with the Estonian-French and Latvian-NATO teams. The organisers surprised the participants because they did not give the exact final score and place classification.

Specialists from many sectors contributed to the success of the Polish team. As every year, the exercise was commanded by a military unit of the Cyber Defence

FIGURE 26. A representative of the Locked Shields 2024 exercise organiser discusses the situation in Berylia, defended by team BT17.



Component Command (DKWOC). The entire team consisted of selected specialists from the military sector, special services, private and public entities, including representatives of CERT Polska. Such a selected representation is crucial for the preparation and verification of the national response capability and the partnership of many independent entities, institutions and specialists on a daily basis. In the event of a serious ICT incident, it is the efficient cooperation between many entities that can be a significant challenge and a decisive factor in the speed of dealing with the threat.

Specialists from CERT Polska took over the management of the special systems, network, external user support and legal teams. In addition, they shared their knowledge and experience as members of these teams and the web application team.

ECSC 2024

The European Cybersecurity Challenge (ECSC) is an international cybersecurity competition organised by ENISA, in which national teams from the European Union and teams from other invited countries compete against each other. Each team consists of 5 people aged between 14 and 20 and 5 people aged between 21 and 25.

National qualifiers

As every year, we were responsible for organising the national qualifiers. In 2024, 77 participants competed in 22 tasks, and 55 of them submitted at least one 'flag' – proof that they had solved the task. The task categories included web application security, computer forensics, reverse engineering, cryptography and steganography.

Finals in Turin

The final competition took place from 8 to 11 October. It was organised by the Italian institutions: Agenzia per la Cybersicurezza Nazionale (Italian government agency for cybersecurity) and CINI Cybersecurity National Lab (national research laboratory for cybersecurity in Italy). In addition to the competitors, specialists from CERT Polska and NASK-PIB were present at the place of the competition in the roles of member of the steering committee, member of the jury, watchdog (person taking care of the fair course of the competition) and team supervisors. A total of 40 teams participated in the entire event, including 6 guest teams and 3 teams as observers.

On the first day, the participants prepared for the competition by familiarising themselves with the infrastructure and platforms. The competition took place on the second and third days and consisted of 2 formats:

- CTF Jeopardy – teams solved tasks of varying difficulty levels inspired by real cybersecurity problems. The competitors had to demonstrate analytical and technical skills as well as creativity.
- CTF Attack & Defence – each team had a set of vulnerable services at their disposal, and the task was to both attack the services of other teams and defend their own.

FIGURE 27. Polish team at the ECSC 2024 competition



After a fierce competition, the Polish team won the bronze medal, which was the second highest result in the history of the Polish team's participation in this competition. The second place went to the hosts (Italy), and the winners were the German team. The final result of our team was made up of the results from two days of competition, in which it took 3rd and 7th place respectively.

FIGURE 28. Polish team at the closing ceremony

ECSC 2025 in Poland

During the closing ceremony, the ECSC flag was ceremoniously handed over to Polish delegation. NASK is set to host the ECSC 2025 finals from 6 to 10 October 2025 in Warsaw.

We encourage you to take part in the national qualifications planned for June 2025 and to follow and support the competitors!

FIGURE 29. The Polish team receives the competition flag

Projects



Artemis

Artemis tests websites and other systems, such as email, for security vulnerabilities and misconfigurations. The CERT Polska team is responsible for the development of this tool. Regular scanning of systems allows for monitoring and improving their security level. The results are not made public. They are forwarded to the administrators, who gain valuable information that can be used to improve the security of the systems they manage and thus prevent attackers from exploiting the detected problems. Primarily, entities from CSIRT NASK constituency, are subject to scanning. Entities not included in the scan can independently request a check of their domains on the moje.cert.pl website.

In 2024, the system found over 331,000 vulnerabilities and misconfigurations, including almost 20,000 with a high risk. The total number of problems detected since the project began, i.e. since January 2023, has exceeded half a million. More detailed statistics on the identified problems can be found [later in the report](#) (pp. 103–105).

It is worth noting that we have continuously developed the system during the reporting period. The most important changes we have made in 2024 include a significant increase in scanning speed, numerous improvements to the system interface and increased stability, as well as new modules, e.g. a module that detects outdated WordPress plugins, a module that checks if the Drupal system version is up to date, and another module that detects SQL Injection vulnerabilities. We have also increased the number of databases used as a source of information about the websites of public institutions, which has enabled us to scan a larger number of entities.

Artemis is an open-source tool and its code is available on GitHub (<https://github.com/CERT-Polska/Artemis>). This means that the system can also be used and developed by specialists from outside CERT Polska. Among the most important people contributing to the development of the Artemis system are Kshitij Kapoor, who has been pursuing this goal as part of the Google Summer of Code programme, and Matúš Mikuláš, who is doing so as part of the Erasmus student programme.

Other CSIRT teams, both Polish and foreign, are also users of the system, which proves that CERT Polska has a significant impact on improving the security of systems outside its constituency.

In 2024, we presented the Artemis project at the hack.lu conference in Luxembourg, Black Hat in the USA and TF-CSIRT in Copenhagen. In addition, CERT Polska conducted training sessions in which other CSIRT teams could configure the tool themselves and start scanning their domains.

moje.cert.pl

In order to make CERT Polska tools available to a wider group of recipients, we launched a test version of the moje.cert.pl website in 2024. This system can be used by private individuals, small companies and large institutions – all you need to do is create an account.

On the moje.cert.pl website, you can request a security scan of your domains and receive information about leaked user passwords within these domains. Network administrators can also receive information about malware infections and other threats in their networks. New improvements are added on an ongoing basis, and there are plans to integrate with other CERT Polska systems in the future.

Security scans are carried out on a regular basis – depending on the organisation's demand, one, two or four months after the previous scan. During the tests, CERT Polska uses the [Artemis](#) (p. 67), system, which detects a large number of vulnerabilities and misconfigurations affecting security. Network events are retrieved from the [n6 system](#) (p. 88).

To prevent unauthorised persons from viewing the results of scans or network events, entities must prove that they are the owners of the domain before the scan starts. To achieve that, they need to add a TXT record to the domain configuration or to place a file in a specified location on the server. The organisation's ownership of the network is verified by the CERT Polska operators.

By the end of December 2024, during the test phase, 467 users had registered on the website and added 936 domains in which the system detected 12,538 vulnerabilities and misconfigurations, including 852 high-risk ones. In the added domains, 552 account password leaks were detected.

By adding their domains to the website, organisations provide the CERT Polska team with contact details, which will later be used for communication in case vulnerabilities or threats are identified.

We presented the system in 2024 during industry events. We invited institutions to use it, for example, at a meeting of the Interuniversity Computerisation Centre, during the e-Health Outlook conference organised by the e-Health Centre and as part of the Sekurak Cyberstarter event. An invitation to join the system, along with information about the possibility of scanning more domains, is also included in the e-mails with scan results sent as part of the Artemis project.

Thanks to the moje.cert.pl website:

- entities have access to numerous cybersecurity tools in one place.

- users can conveniently add and remove the domains and networks they administer – they can therefore scan all their domains (not only the main domain, but also, for example, domains related to promotional campaigns or additional projects),
- users can share the scan results with colleagues,
- CERT Polska has the possibility of informing recipients about new tools.

MWDB

The MWDB platform is our solution for storing and processing malware samples, gathering information about them and for partnerships with external analysts. In 2024, 471 external cybersecurity professionals were given access to the platform. At the end of 2024, the total number of organisations we work with was 1,910. The platform code is available free of charge under an open-source licence (<https://github.com/CERT-Polska/mwdb-core>).

Among the implementation activities that we carried out in 2024, it is worth highlighting the performance improvements related to the development of the website and the use of the OpenID Connect protocol for external integration, in particular with the CSIRTs Network and Trusted Introducer networks. In addition, in 2024, we developed the integration of external data sets, which allowed us to significantly increase the amount of processed information – 20.7 million malware samples were added to the repository, compared to 312.5 thousand samples in 2023. As a result, we identified more than 46,000 new unique configurations of programmes used by criminals, compared to 13,000 in 2023. The results of this approach are satisfactory, but the solution is somewhat of a compromise: although we obtained more than 3 times as many configurations, only 0.23% of the analyses provided significant new information compared to 4.3% in the previous year, based on the number of processed files.

As part of our international partnerships and to promote the website, we presented it at numerous training sessions and workshops at conferences for CSIRTs and industry specialists in 2024. This allows us to strengthen relationships with system users, exchange experiences and build an international contact network.

Snitch

The availability of OT/IoT devices on the Internet can have serious consequences for the cyber security of the institutions concerned. Snitch allows you to

automatically monitor this exposure using Shodan, Zoomeye, FOFA, and n6 services. In 2024, Snitch was expanded with new functions to facilitate the analysis or reporting of vulnerable systems, and even a module to check for vulnerabilities in systems, e.g. default passwords.

More information in notifications

In order to increase reliability and make it easier to identify the devices mentioned in our messages, we have added additional information about the reported systems, such as the serial number or model of the device.

This is made possible by expanding Snitch to include the ability to search through collected service data. This data is selected by a specialist using regular expressions. This makes work and analysis on case data much easier compared to the time-consuming process of clicking through each service individually.

Default passwords

Another important extension of Snitch was the integration of the new data source Nuclei. Nuclei is a vulnerability scanner that determines whether a service is vulnerable based on a defined template. The template defines the process and conditions that will determine whether the service is vulnerable. Nuclei enables the operator to build scripts in a standardised way that check the vulnerabilities of a given service. As a pilot project, we started to implement checking of default passwords in web panels of OT systems for several rules in August. The Nucleus database²¹ does not have many templates dedicated to OT systems. After a transition period, we want to expand the Nucleus database by making the templates we have created public. This should also be a time for patching vulnerabilities.

21 <https://github.com/projectdiscovery/nuclei-templates>

FIGURE 30. Content of a sample notification sent from Snitch

Szanowni Państwo,

jesteśmy zespołem reagowania na incydenty bezpieczeństwa informatycznego CERT Polska.

Wiadomość ta przeznaczona jest dla osoby odpowiedzialnej za bezpieczeństwo informatyczne. Jeśli nie są Państwo odpowiednimi adresatami, prosimy o poinformowanie nas o tym oraz przekazanie niniejszej wiadomości do odpowiednich osób.

W ciągu ostatnich 4 dni zaobserwowaliśmy następujące publicznie dostępne usługi XYZ HMI:

- 77.x.x.x:443 [tcp] (host: YUI, użytkownik "admin" używa domyślnego hasła)
- 77.x.x.x:443 [tcp] (host: SW-POZNAN, użytkownik "admin" używa domyślnego hasła)
- 77.x.x.x:443 [tcp] (host: xMT-AC26, użytkownik "admin" używa domyślnego hasła)
- 78.x.x.x:443 [tcp] (host: xMT-123B)
- 77.x.x.x:443 [tcp] (host: xMT-ABB1, użytkownik "admin" używa domyślnego hasła)
- 77.x.x.x:443 [tcp] (host: xMT-SUC-ZG)

Ich publiczna dostępność może stanowić niebezpieczeństwo dla Państwa systemów. Jeśli konieczny jest dostęp zdalny, zalecamy wykorzystanie VPN z wieloskładnikowym uwierzytelnianiem.

Obserwujemy działania licznych grup, najczęściej prorosyjskich, wymierzone w systemy automatyki przemysłowej. Tego typu systemy nigdy nie powinny być dostępne bezpośrednio z internetu, nawet jeśli są chronione hasłem.

Zwracamy się z uprzejmą prośbą o weryfikację usług pod wskazanymi adresami i podjęcie działań w celu ich zabezpieczenia. Więcej o zagrożeniu i rekomendacjach można przeczytać pod adresem: <https://cert.pl/posts/2024/05/rekomendacje-ot/>

Będziemy wdzięczni za wszelką pomoc, jakiej mogą Państwo udzielić na tym etapie, oraz przekazanie informacji o podjętych przez Państwa działaniach w celu rozwiązania problemu.

Z poważaniem

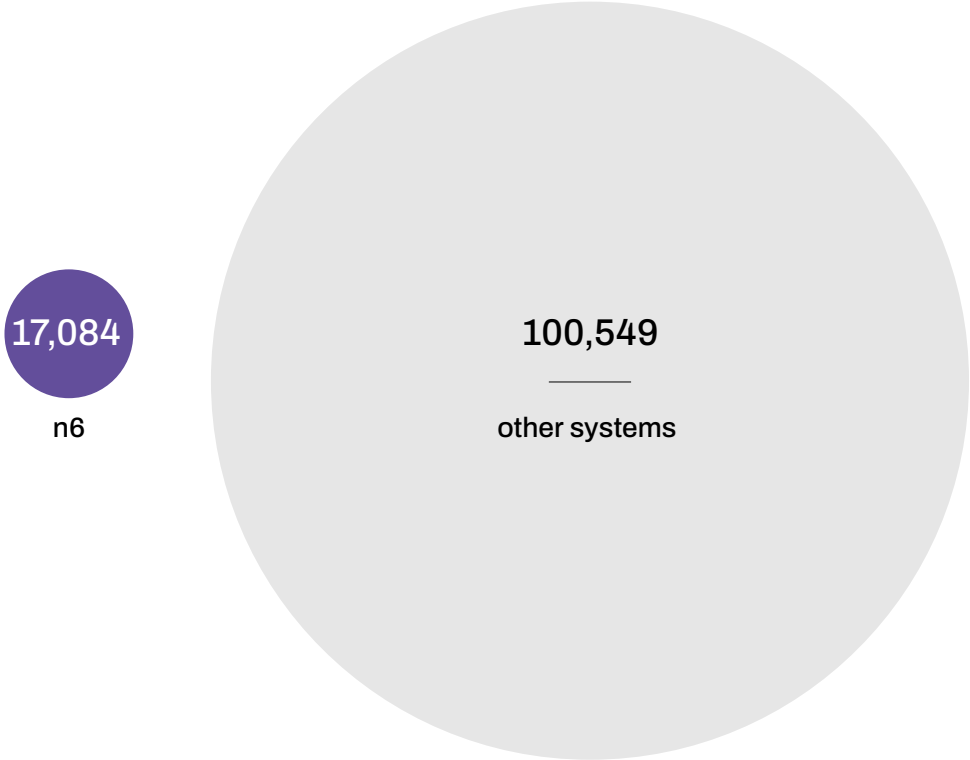
Zespół CSIRT NASK/CERT Polska

www.cert.pl

New data sources

For information about events in OT environments, the n6 system is mainly fed with data from Snitch, as well as data obtained thanks to the partnership with the Shadowserver Foundation. According to plans from the beginning of 2024, in addition to incident reporting to the n6 system, Snitch allows to define search phrases for retrieving data from n6. Thanks to the data from n6, we were able to add new dorks to 10 rules and create 3 completely new rules. In 2024, n6 provided 6.8% of hosts that were not visible through other sources. Additionally, this year we started using the FOFA search engine.

FIGURE 31. Comparison of the number of hosts obtained through n6 only



Reporting statistics

In 2024, the Snitch system began to be used by the newly formed Vulnerability Handling and Threat Hunting Team at CERT Polska to monitor IT systems such as VPN servers, file servers, content management systems and mail servers. For this reason, the data is provided separately for OT and IT systems.

TABLE 6. Snitch statistics broken down into OT and IT systems

Number	OT	IT	Sum
Rules	61	73	134
Unique hosts	4,488	27,520	32,008
Unique services	6,896	28,329	35,225
Notifications sent	11,588	4,163	15,751

Last year, Snitch sent reports over a period of 7 months and only to OT systems. Comparing the monthly average, the number of reports sent for OT systems in 2024 was 4.8 times higher than in 2023.

DNS4EU

The goal of the DNS4EU project is to create a public DNS resolver that is an alternative to the services currently used on the market. It will be a completely European solution, focused on user protection, compliant with privacy rules and resistant to attacks, thus contributing to strengthening the European Union’s digital independence and the security of its citizens.



The service will be available to individual users, public institutions, ministries, local government units, medical and educational institutions, and customers of telecommunications service providers. These entities often do not have the resources to ensure the quality of DNS services at an appropriate level, in particular in terms of end-user security and compliance with personal data protection regulations.

The project is being carried out by an international consortium consisting of Whalebone (Czech Republic, leader), CZ.NIC (Czech Republic), CVUT (Czech Republic), Time.lex (Belgium), deSEC (Germany), HUN-REN Sztaki (Hungary), ABILAB (Italy), DNSC (Romania) and NASK-PIB.

NASK-PIB is responsible for creating solutions in DNS4EU that detect domains used for phishing, which is intended to increase the security of resolver users. On the NASK-PIB side, the project is being implemented by CERT Polska together with the Research and Development Centre. Our work focuses on detecting phishing domains based on data from the domain registry and through the analysis of DNS queries. It should be noted that the research and development work on these solutions is still ongoing and the first of them has entered the production testing stage while this report was being prepared.

Detection of phishing domains based on domain registry data

In our first solution, we have created an early detection system for phishing domain registrations. The system uses data from the .pl domain registry on recently registered domains to predict which of them may be used for phishing. The purpose is to shorten the response time of CERT Polska before they are used by criminals on a large scale. The domain register contains data on domains (e.g. their names, registration time), registrars and the contact details of domain owners. A set of features is extracted from this data and fed into the machine learning model. In addition, the data is enriched with information from additional services, such as information from address databases and the geolocation of IP addresses. We also used our operational experience in handling phishing incidents and added additional features depending on the current situation, e.g. keywords related to the brands being attacked, whose image is used in phishing campaigns.

The prototype of the detector was launched at the end of 2024 and incorporated into the phishing detection process that we use to add domains to our Warning List. Work on this solution is still ongoing and includes expanding detection to include new features and a wider range of domains, as well as ways of using top-level domains (TLDs) other than .pl.

Analysis of DNS queries

The second way of detecting phishing domains is through DNS query analysis. We try to extract as much information as possible from the queries while maintaining the privacy of end users, e.g. by anonymising their IP addresses. We analyse the queried domain names and the relationships between the queries, both in terms of time and, for example, their source addresses. The analysis of all aspects serves to identify domains that are actively used for phishing attacks.

The analysis of queried domains focuses on the textual form of domain names. We test and compare various NLP (Natural Language Processing) techniques with the aim of best representing domain names in a form that is understandable to machine learning algorithms. This is called embedding, and a range of different methods are used here, such as fastText and BERT. We also test various machine learning algorithms for domain classification – both traditional ones, such as decision forests and gradient boosting, as well as those using neural networks.

The analysis of query dependencies focuses on discovering characteristics that can distinguish phishing queries from other queries. Time and address dependencies are tested (while maintaining anonymisation), and links between queried domains are checked for different periods of time and for different query sources. Signal processing techniques help with this, as DNS queries can be treated as time series to a certain extent.

In addition to research problems, we also solve technical problems such as the processing of large amounts of data and its storage, as well as the development of data flow architecture for machine learning models and its implementation.

The above-described part of our work in the DNS4EU project is at an earlier stage than the detection of phishing domains based on data from the domain registry due to its dependence on other architectural elements of the entire resolver. However, the solution that is being developed will be more universal because it is being adapted to detect phishing across all top-level domains (TLDs) using resolver data, regardless of access to domain registry data.

For more information, please visit the official project website www.joindns4.eu.

The project is co-financed by the European Union. Grant number: 101095329 21-EU-DIG-EU-DNS, the full name of the project is DNS4EU and European DNS Shield.



Funded by
the European Union

JTAN

Last year, we completed the three-year Joint Threat Analysis Network (JTAN) project. Our team coordinated the work of an international consortium consisting of 7 European national CSIRTs: from Luxembourg (CIRCL), Latvia (CERT.LV), Austria (CERT.at), Slovakia (SK-CERT), Estonia (CERT-EE), Romania (DNSC) and a private company from France: Corexalys.

JTAN's main goal was to improve the tools used by European CSIRTs and to strengthen partnerships between the teams, in particular through more intensive information exchange. The work focused on tools for collecting, analysing and exchanging information on Cyber Threat Intelligence (CTI).

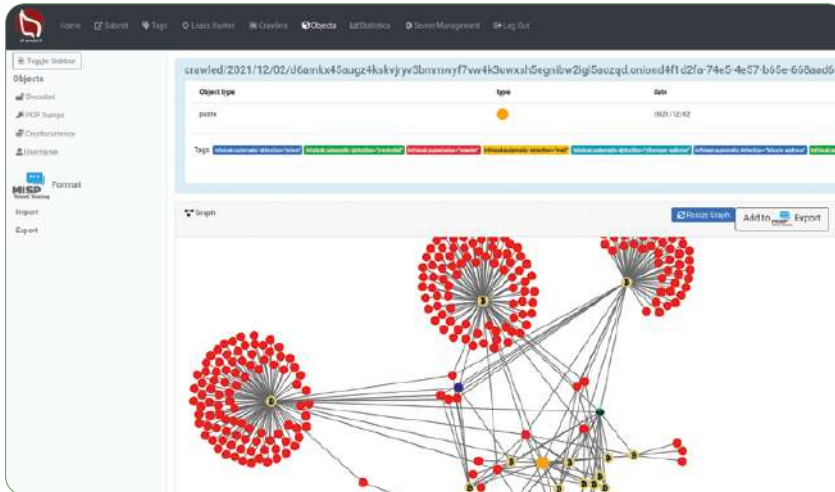
Open-source tools

During the project, the consortium developed features of many open-source tools. This allows the JTAN results to be used by other entities responsible for cybersecurity, including national CSIRTs and SOC teams in companies and institutions. Below we present a brief description of these tools and the scope of work carried out as part of the project.

AIL is a comprehensive system for collecting, indexing and analysing unstructured security-related data. It is used, for example, to detect information leaks and to analyse content shared on the TOR network. The automatic semantic analysis of collected content has been added to AIL, thanks to which analysts can effectively identify information that requires more thorough checking. In addition,

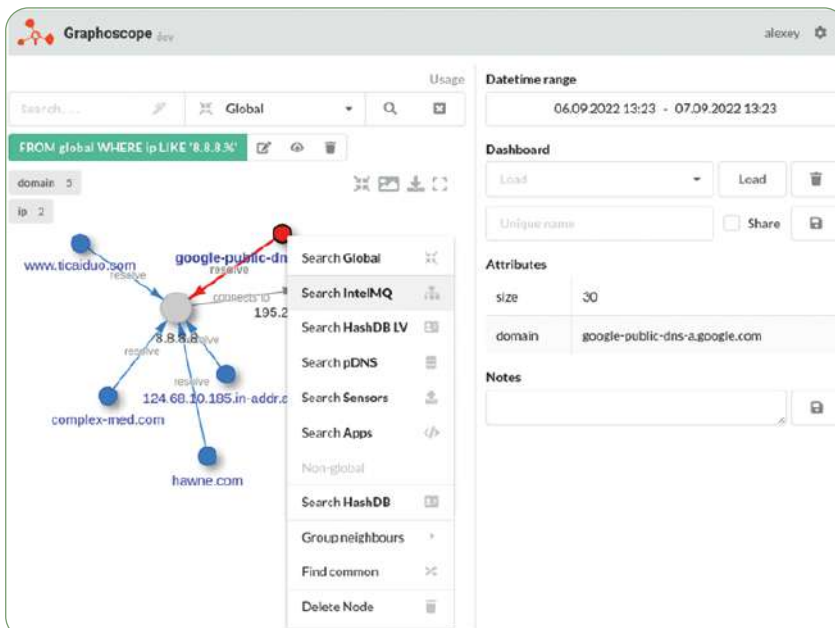
version 4.0 adds optional automatic synchronisation between AIL instances. Project website: <https://www.ail-project.org>.

FIGURE 32. Screenshot of the AIL tool interface



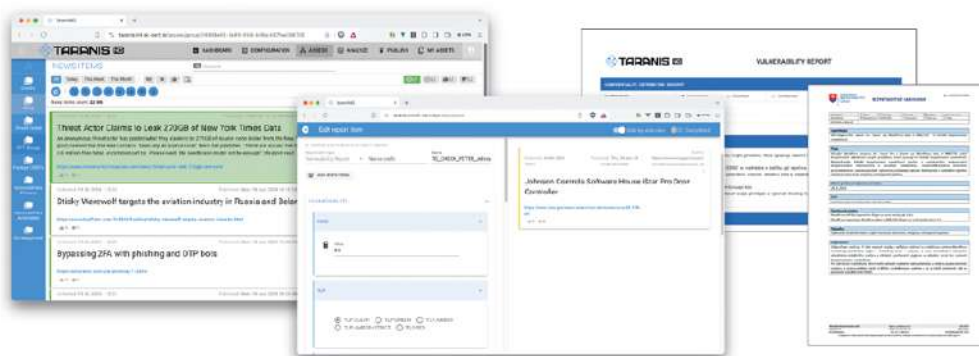
Graphoscope is a tool for analysts offering functions that improve data mining and graph-based threat analysis. Analysts can correlate and filter information from many different data sources, as well as use SQL-style queries for advanced searching. The work on JTAN included preparing the first public release of the tool, updating the documentation, improving the web interface, and adding new plugins and updating existing ones. Project repository: <https://github.com/cert-iv/graphoscope>.

FIGURE 33. Screenshot of the Graphoscope interface



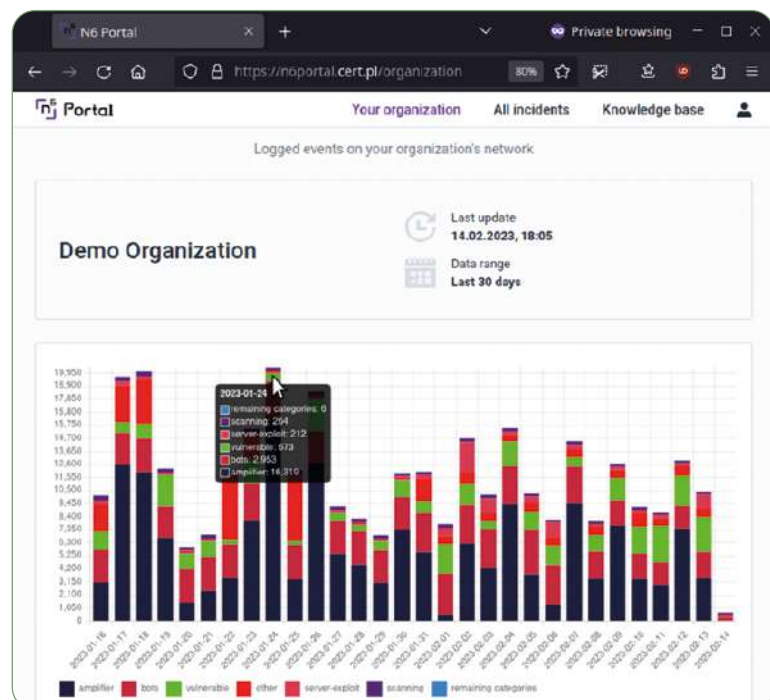
Taranis NG is a system for continuous collection and analysis of open-source information (OSINT). The system enables automatic data collection from such sources as websites, RSS, social media platforms, and e-mails. It also supports the work of analysts in evaluating and selecting relevant elements on the basis of which reports are prepared. Analysts can configure reports or create new ones. During the project, the handling of group work on reports was improved, as well as the system's performance has increased. New predefined report templates have also been added, multiple bugs fixed, and the tool's overall implementation has been simplified. Project repository: <https://github.com/SK-CERT/Taranis-NG>.

FIGURE 34. Screenshot of the Taranis NG tool interface



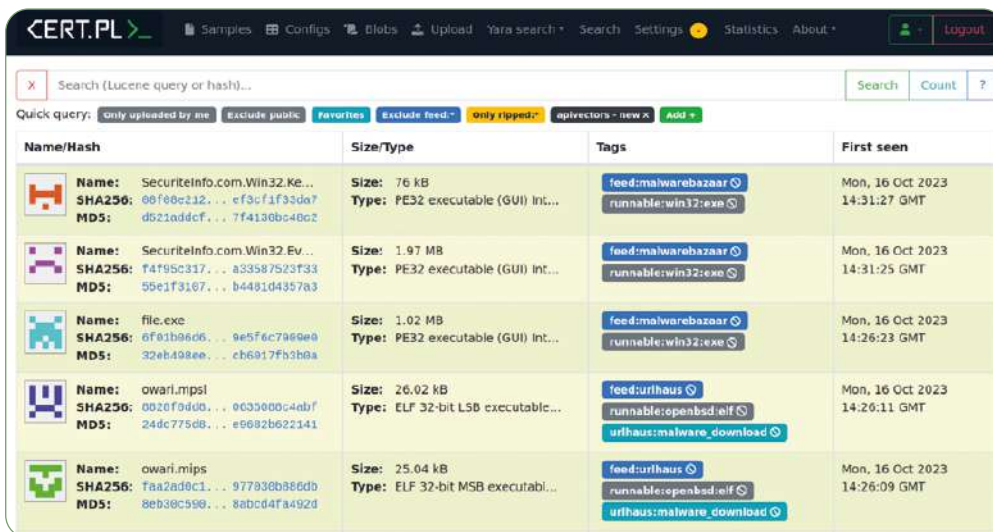
The n6 platform, created and developed by CERT Polska, is used to aggregate data from multiple automated sources and to send notifications about detected threats to IT infrastructure operators for organisations registered in the system. During the work on the project, support for authentication using the OpenID Connect was added, over 40 new data sources were integrated. Moreover, the work completed during JTAN included performance optimisations and improved data visualisations on the web portal. In addition, many bugs were fixed, and changes were made to facilitate long-term maintenance and development of the platform. Information for entities from Poland: <https://cert.pl/n6>, source code: <https://github.com/CERT-Polska/n6>.

FIGURE 35. Screenshot of the n6 platform interface



The MWDB platform, developed by CERT Polska, is an advanced malware data repository. It allows for the storage of files and all other related information and provides an effective search mechanism. During JTAN visualisations were improved and the ability to easily store complex analysis results was added to the tool. Integration with the MISP information exchange platform was also implemented, making it easier to share analysis results with a wider group of recipients. Project repository: <https://github.com/CERT-Polska/mwdb-core>.

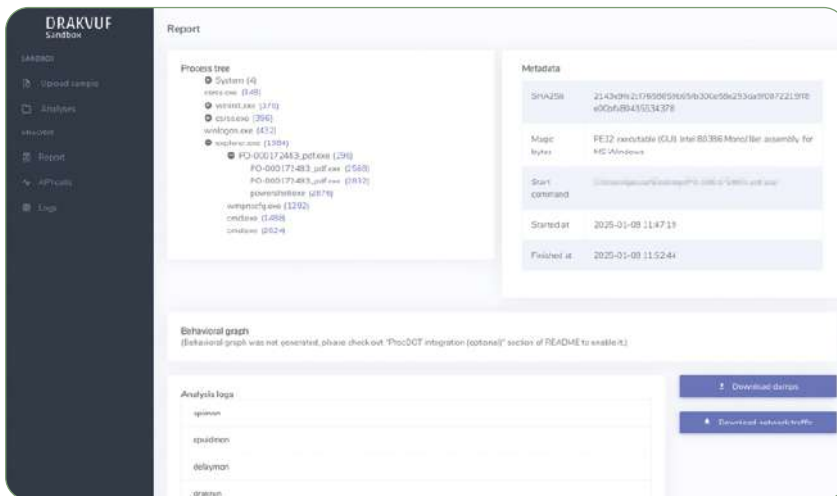
FIGURE 36. Screenshot of the MWDB platform interface



Name/Hash	Size/Type	Tags	First seen
Name: SecuriteInfo.Win32.Ke... SHA256: 00f80e212...ef3cf1f33da7 MDS: d521addcf...7f4130bc48c2	Size: 76 kB Type: PE32 executable (GUI) Int...	feed:malwarebazaar runnable:win32:exe	Mon, 16 Oct 2023 14:31:27 GMT
Name: SecuriteInfo.Win32.Ev... SHA256: f4f95c317...a33587523f33 MDS: 59e1f3167...b4481d4357a3	Size: 1.97 MB Type: PE32 executable (GUI) Int...	feed:malwarebazaar runnable:win32:exe	Mon, 16 Oct 2023 14:31:25 GMT
Name: file.exe SHA256: 6f01b96d6...9e5f6c7969e0 MDS: 32eb498ee...cb6917f52b0a	Size: 1.02 MB Type: PE32 executable (GUI) Int...	feed:malwarebazaar runnable:win32:exe	Mon, 16 Oct 2023 14:26:23 GMT
Name: owari.mpsl SHA256: 0026f9dd0...0c3500c4abf MDS: 244c77508...e9892b62141	Size: 26.02 kB Type: ELF 32-bit LSB executabl...	feed:urhaus runnable:openbsd:elf urhaus:malware_download	Mon, 16 Oct 2023 14:26:11 GMT
Name: owari.mips SHA256: faa2ad0c1...977930b366db MDS: 8eb30c590...8abc04fa492d	Size: 25.04 kB Type: ELF 32-bit MSB executabl...	feed:urhaus runnable:openbsd:elf urhaus:malware_download	Mon, 16 Oct 2023 14:26:09 GMT

DRAKVUF Sandbox is an advanced malware analysis system that is the primary engine used by CERT Polska for automated malware detonation. It uses Virtual Machine Introspection (VMI) technology, which makes it possible to monitor processes running in virtual machines without having to modify their systems (agentless monitoring), making it difficult for malware to detect the tool. DRAKVUF Sandbox offers an analysis engine, a web-based user interface for viewing results and modules for processing low-level raw logs to high-level, human-readable form. In addition to many improvements related to the system installation and maintenance, JTAN added support for accurate tracing of the malware execution based on the hardware feature offered by the modern Intel processors (Intel Processor Tracing). Project repository: <https://github.com/CERT-Polska/drakvuf-sandbox>.

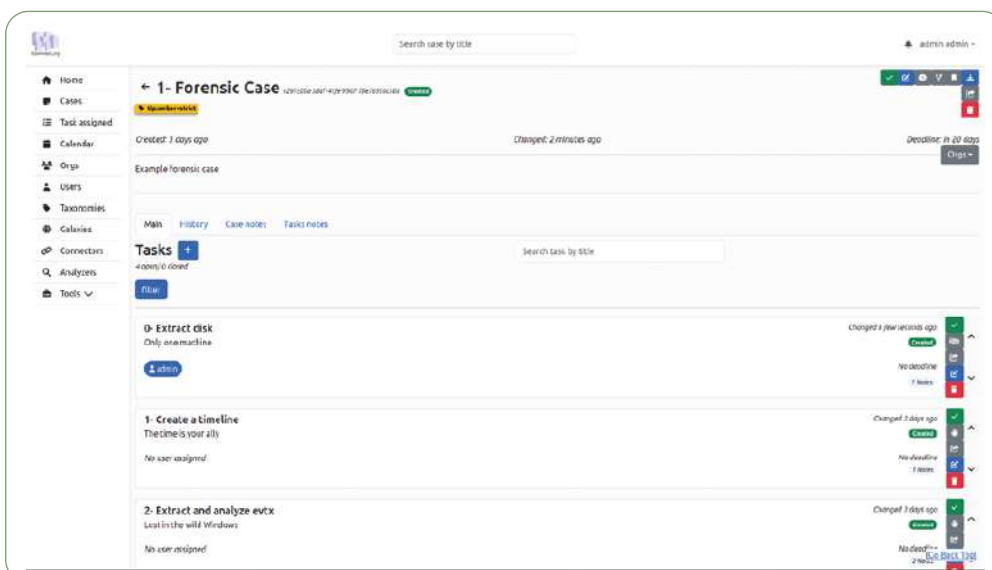
FIGURE 37. Screenshot of the DRAKVUF Sandbox interface



New tools were also developed as part of the JTAN project, which are discussed below.

FlowIntel is a system supporting analysts in managing CTI-related tasks and responding to incidents. The tool supports the coordination of work on incident handling, information analysis, and report creation through management and assignment of tasks within a team and also facilitates communication between analysts working on a given case. The configurable process templates, the system's integration with the MISP information exchange platform and the integrated calendar also increase the efficiency of group work. In addition, users can export data to other platforms, use external services to enrich data and automate activities using the API. Project repository: <https://github.com/flowintel/flowintel>.

FIGURE 38. Screenshot of the FlowIntel interface



Private Search Set is a data format based on Bloom filters that enables private data sets to be shared with a high level of confidentiality. It offers fast lookup of values (e.g. Indicators of Compromise, hashes or strings) without revealing their content, easy distribution of private sets to groups of users or organisations, and the possibility of private offline searches. The uses of Private Search Set include reducing the risk of data leaks, protecting sensitive information such as personal data or sensitive materials, and secure information exchange in situations where full content sharing is not possible (e.g. due to confidentiality or legal restrictions). Project repository: <https://github.com/hashlookup/private-search-set>.

CocktailParty is a tool for sharing and managing data streams based on the WebSocket protocol. Users can easily view and enable available data sources using a web interface. In JTAN, CocktailParty is used to share real-time data from CIRCL's monitoring systems, including Passive DNS. Project repository: <https://github.com/flowintel/cocktailparty>.

Internal tools

In addition to the open-source software, the CSIRTs involved in the project have developed new and expanded existing threat monitoring systems addressing their own operational needs.

CERT.at developed a framework for assessing the risk associated with Internet domains at the level of the entire .at zone. It then created a system that uses machine learning to calculate the risk associated with individual domains with the goal of early detection of domains that may pose a threat to users.

DNSC created hardware sensors aimed at small and medium-sized enterprises to protect them against network-level attacks. The devices are based on the Raspberry Pi platform and can be easily deployed in the target network. Administrators have access to all events detected in the monitored infrastructure, and thanks to the centralised logging, DNSC has access to information on attacks on a national level. The sensors are made available to interested entities without any fees, and during the project they were deployed by over 100 entities in Romania.

CERT Polska developed a new version of the sinkhole system, which is used to collect data from network traffic to seized malicious internet domains (e.g. WPAD domains: <https://cert.pl/posts/2019/06/przejecie-domen-pl-zwiazanych-z-atakiem-badwpad>). The new version makes the maintenance and development of the system significantly easier.

Thanks to the JTAN project, the infrastructure for malware analysis at CERT-EE and CERT Polska were expanded as well. CERT-EE maintains the Cuckoo sandbox, which is publicly available for security analysts and other users who want to check the behaviour of suspicious files. Cuckoo version 2 is available at <https://cuckoo.cert.ee>, and a test version of Cuckoo 3 is reachable

at <https://cuckoo-hatch.cert.ee>. In the case of CERT Polska, the hardware resources used by the MWDB service have been expanded.

Other activities

The tools developed within the framework of JTAN were actively promoted, especially among cybersecurity teams. Twelve technical workshops and training sessions were held, and 4 hackathons were organised, which provided an opportunity for technical discussions and joint work on the implementation of new features. In addition, the partners in the consortium shared their experiences on an ongoing basis.

The key element of the project was to improve the exchange of threat intelligence, which was achieved by creating a data exchange network suitable for interconnection of automatic monitoring systems. The network was based on MISP, a platform for exchanging threat information commonly used by CSIRTs in Europe. A separate instance was launched for JTAN, which allows for easier management of large amounts of automatically generated data. The second element of the network is a set of real time data streams managed through the Cocktail-Party broker. The tools developed in the project have been integrated with both solutions, ensuring their interoperability.

The technical foundations created in JTAN enable better partnerships between cybersecurity teams, both among European national CSIRTs and in other CSIRT/SOC communities.

The project was co-financed by the European Union under the Connecting Europe Facility, action number: 2020-EU-IA-026.



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

FETTA

In 2024, we started a three-year project called Federated European Team for Threat Analysis together with our counterpart team in Luxembourg, CIRCL (Computer Incident Response Center Luxembourg). The main objective of the project is to provide more accurate Cyber Threat Intelligence (CTI) to entities in Poland, Luxembourg and, through the CSIRT Network, in other European Union countries. The project includes the development of new situation reports and the improvement of existing ones, as well as the development of tools for collecting and analysing cybersecurity data.



The basic premise of FETTA is analytical partnership – sharing knowledge will allow for a more accurate description of threats and reduce duplication of analysts' work. Ultimately, we want to create a virtual CTI team that can include many national CSIRTs.

The project is based on open-source solutions developed by CERT Polska and CIRCL, such as MISP, MWDB, Cerebrate, AIL and n6. This means that the results of FETTA – in the form of tool improvements – will also be available to all potential users.

In 2024, we focused on the analysis of requirements for CTI products, the acquisition of new data sources and, together with the Research and Development Centre of NASK, using honeypots to develop methods for detecting new threats to services and devices available on the Internet. In the next stage, we are going to focus on tightening the cooperation between the teams.

The project is co-financed by the European Cybersecurity Competence Centre (ECCC), the Digital Europe programme, grant number: 101128030. CERT Polska is leading the consortium.



**Funded by
the European Union**



ECCC 
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Statistics



Incidents and incident reports

In 2024, the CERT Polska team recorded 600,990 incident reports that were analysed. Based on these, 103,449 security incidents were recorded that had or could have had an adverse impact on cybersecurity (see Table 7).

TABLE 7. Number of incident reports and incidents registered in 2024



The number of incident reports in 2024 increased by 62% compared to 2023, while the number of recorded cybersecurity incidents in 2024 increased by 29% compared to 2023. Even though the increase in the number of incidents is lower than in previous years, the upward trend is still visible. Since the implementation of the Act on National Cybersecurity System, the largest increase in the number of incidents was recorded in 2023, when the number more than doubled compared to 2022, and in 2021, when the number of incidents almost tripled compared to 2020.

The increase in the number of reports and recorded cybersecurity incidents is due, among other things, to the growing public awareness of the threats and the role of the CERT Polska team in monitoring, analysing and responding to cybersecurity incidents, as well as in conducting information activities on the threats that occur. Table 9 shows the number of incidents in 2018–2024.

Reports are sent to us via:

- the form available at <https://incydent.cert.pl> – incident report,
- the form available at <https://incydent.cert.pl/domena> –report a phishing domain,
- text message to 8080 number – report a suspicious text message,
- the mObywatel app – report a malicious website, fraud or other incident (Network Safety service),
- e-mail: cert@cert.pl,
- traditional mail to NASK-PIB.

Most common incident types in 2024

Computer fraud

The most common category of incidents registered in 2024 was computer fraud. A total 97,995 incidents of this type were registered, accounting for 95% of all incidents handled. Compared to 2023, the number of computer frauds increased by 29%. The frauds include fake online shops and the ever-popular investment scams, in which fraudsters impersonate various oil and energy companies, firms and institutions. The fraudsters reach out to potential victims through advertisements on, for example, social media. In the advertisements, they encouraged investing on investment platforms and promised high profits, but their real goal was to extort money.

The most common type of computer fraud was phishing, i.e. attempts to obtain confidential data such as logins and passwords for email, bank websites, social networking sites or other online services. In 2024, there were 40,120 such incidents, accounting for 39% of all registered incidents. Among the most common phishing campaigns were cases of unauthorised use of the image of the sales services OLX – 9,865 cases, Allegro – 4,053 cases, and the social media service Facebook – 3,871 cases.

Malware

The second most common type of threat was malware. In 2024, 1,891 incidents of this type were registered.

Vulnerable services

The third most common type of threat were vulnerable services. In 2024, 1,634 incidents of this type were registered.

Act on the National Cybersecurity System

In 2024, under the Act on the National Cybersecurity System, CSIRT NASK handled 57 incidents classified as significant. These are incidents that have caused or could have caused a serious reduction in the quality or interruption of the continuity of a key service. Among the 57 significant incidents recorded in 2024, 44 events took place in the banking and financial market infrastructure sector, 11 concerned the healthcare sector and 2 were related to the transport sector. The number of significant incidents in 2024 increased by 43% compared to 2023. No DSP incidents were registered in 2024.

In 2024, CSIRT NASK handled 3,450 incidents in public entities. This is an increase of 58% compared to the previous year. The highest number of incidents was recorded in public administration – 1,911 cases, followed by the education sector – 579 cases, and the healthcare sector – 440 cases. Data on the number of incidents reported to CSIRT NASK by law are also presented in Table 8.

TABLE 8. Incidents reported by law to CSIRT NASK from 1 January to 31 December 2024

57 Significant incidents	0 DSP incidents	3,450 Incidents in public entities
------------------------------------	---------------------------	--

Statistics broken down by sector of the economy and type of incident are presented in tables 10 and 11.

TABLE 9. Number of incidents handled by CERT Polska in 2018–2024

Year	Number of incidents
2024	103,449
2023	80,267
2022	39,683
2021	29,483
2020	10,420
2019	6,484
2018	3,739

TABLE 10. Incidents handled by CERT 2024, broken down by economic sectors. Designation of sectors according to the internal classification of CSIRT NASK

Sector	Number of incidents	Percent
Financial market infrastructure	44,020	42,6%
Wholesale and retail	18,324	17,7%
Media	13,322	12,9%

Sector	Number of incidents	Percent
Mail and courier services	5,216	5,0%
Power engineering	4,632	4,5%
Digital infrastructure	4,055	3,9%
Natural persons	2,735	2,6%
Banking	2,544	2,5%
Public Administration	2,337	2,3%
Hotels, restaurants, catering	1,108	1,1%
Production	956	0,9%
Other	837	0,8%
Other Services	737	0,7%
Education and upbringing	733	0,7%
Healthcare	604	0,6%
Transport	565	0,5%
Culture and heritage conservation	292	0,3%
Logistics and distribution	184	0,2%
Construction and real estate management	68	0,1%
Water supply systems	59	0,1%
Agriculture	32	0,0%
Waste management	27	0,0%
Tourism	19	0,0%
Chambers of economy and commerce	15	0,0%
Insurance	14	0,0%
Physical culture	8	0,0%
Religions and national minorities	5	0,0%
Fishery	1	0,0%
Total	103,449	100,0%

TABLE 11. Incidents handled by CERT Polska in 2024, broken down by category. Category designation according to ENISA taxonomy.

Threat type	Number of incidents	Percent
Computer fraud	97,995	94,7%
Malware	1,891	1,8%
Vulnerable services	1,634	1,6%
Abusive and illegal content	775	0,7%
Break-ins	447	0,4%
Resource availability	426	0,4%
Break-in attempts	179	0,2%
Attack on information safety	62	0,1%
Information gathering	26	0,0%
Other	14	0,0%
Total	103,449	100,0%

n6

In this part of the report, we present statistics based on events processed automatically using the n6 platform. The events cover vulnerable systems, possible infections or successful attacks on Polish networks. The information was obtained from CERT Polska’s proprietary systems and external sources. The data is aggregated, normalised and shared free of charge to network owners and relevant CSIRT teams.

Methodology

We made much effort to ensure that the image of the situation resulting from the presented statistics accurately defines all large-scale threats. One must not forget, however, that there are certain limitations, mainly due to the nature of the available data sources.

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 the presentation of the current threat landscape is also caused by the fact that a threat may be active – even for a longer time – until it is analysed, and its regular observation starts. For example, the number of infected computers grouped in a botnet may be difficult to determine before it is neutralised by taking over the C&C infrastructure.

It is also important to determine the scale of the threat. This is usually done by looking at the number of related IP addresses observed during the day. Thus, it is assumed that the number of addresses is close to the number of affected equipment or users. Obviously, this is an imperfect measure due to the widespread use of two mechanisms that affect the visible public addresses:

- 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 assume that the influence of both mechanisms on the aggregated results cancels itself, but a thorough examination of the NAT and DHCP impact in this context would require a separate analysis.

The next remark concerns the IP protocol version, i.e. all the given statistics refer to the fourth version of this protocol. This is due to the still low degree of IPv6 implementation in our country and, consequently, to the negligible number of reports we receive in relation to this type of addresses.

The last remark refers to the size of autonomous systems (AS). We determined them based on data from RIPE from 1 July 2024.

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.

Bots in Poland

In 2024, we collected information about 281,218 IP addresses showing bot activity. Compared to 2023, this is a slight increase of over 3,000. The average daily number of infected devices on the Polish Internet was 4,749. Over the year, we observed a steady downward trend from over 6,000 at the beginning of the year to around 4,000 at the end of the year. Table 12 shows the number of infected computers in Polish networks in 2024.

TABLE 12. Largest botnets in Poland

Family	Daily maximum value	Daily average value	Standard deviation	Observation time
Socks5Systemz	2,611	1,537	443	98,63%
Andromeda	1,455	665	177	100%
Ngioweb	796	170	240	21,03%
Avalanche	754	176	200	99,72%
Android Vo1d	587	416	81	29,78%
Android Triada	548	327	77	87,43%
AdLoad	463	237	73	98,90%
Nymaim	428	91	55	100%
PseudoManuscript	424	257	68	98,63%
Hummer	387	70	30	97,81%

Particular attention should be paid to Socks5Systemz, which once again took first place in the table – with an average number of infected devices exceeding 1,500. It is a malicious resident proxy software that has been active on the Internet for over 5 years. For many years, we have been observing the activity of already sink-holed botnets within Polish networks. One example of such a botnet is Andromeda, which is once again at the top of the above table with a daily average number of infected devices of almost 700. In the case of the Andromeda, Avalanche, Android Triada, Nymaim and Hummer botnets, we observe a persistent number of infected devices on an annual basis. However, we recorded a downward trend in the case of the Socks5Systemz, AdLoad and PseudoManuscript botnets. We only started to observe some of the threats at the end of the year. Among those listed in the table is Android Vo1d.

C&C servers in Poland

C&C servers were active in Poland under 70 different IP addresses in 30 autonomous systems. This is more than in 2023, when we collected information on 26 IP addresses in 16 autonomous systems. The autonomous systems with the most Polish IP addresses were AS210558 and AS20940. In the first one, we observed 12, and in the second one, 11 addresses. In 2024, we received 5 reports about a fully qualified domain name (FQDN) that functioned as a C&C server, using the .pl domain.

Phishing

This part of the report only includes statistics on phishing in the traditional sense of the word, i.e. ‘impersonation’ of well-known brands, using e-mail and websites to phish for sensitive data. For example, we do not include in this category the cases of impersonation of invoice providers distributing malware.

Phishing hosted in Polish networks

In 2024, we received a total of 235,618 reports about phishing in Polish networks. They concerned 64,844 URL addresses with 62,952 domains which were divided into 3,169 IP addresses. In Table 13, we have listed 10 providers who hosted phishing and whose infrastructure was located in our country. As in previous years, home.pl has a significant share compared to other autonomous systems.

TABLE 13. Providers with the highest number of phishing websites in Polish autonomous systems

Provider name	AS numbers	Number of IP addresses	Number of domains	Number of domains on the Warning List
home.pl	12824	757	3,391	640
Akamai Technologies	20940, 16625	633	424	0
Cyber Folks	41079, 29522, 43758	228	5,215	133
Nazwa.pl	15967	177	2,869	6
OVH	16276	139	1,802	10
Orion Network	41564	104	216	3
LH.pl	203417	97	1,465	14
Atman	57367, 15694, 24723	80	2,342	66
Artnet	200088, 197155	76	323	22
IQ PL	47544	56	397	0

Phishing inserted on the CERT Polska's the Warning List

In 2024, 92,647 domains were inserted on the Warning List of CERT Polska, resolving to 29,780 IP addresses. As in 2023, criminals attacking users used Cloudflare services to hide the real location of the server – as many as 25,276 IP addresses belonged to this provider.

In Table 14, we have included the most common top-level domains that appeared on the Warning List. The most popular TLDs were .com, .top, and .pl. The popularity of the Polish TLD and .com is due to the increased effectiveness of impersonating the original domain.

Table 15 shows the most common targets that criminals impersonated. In 2024, the most common target of phishing was investment fraud. In this case and in the case of fraud on OLX, InPost, Netflix, Gazeta.pl, Meta and Booking, we have seen an increase in the number of domains. In the case of scams related to Allegro, Facebook and Baltic Pipe, a decrease is visible.

TABLE 14. Most common top-level domains (TLD) included in the Warning List

TLD	Number of domains
.com	38,321
.top	7,378
.pl	7,231
.xyz	5,395
.site	2,338
.shop	2,233
.cfd	1,936
.click	1,926
.lat	1,922
.net	1,799

TABLE 15. The most common phishing impersonation targets that are included in the Warning List

Phishing target	Number of domains in 2024	Number of domains in 2023
Investment frauds	42,172	20,609
OLX	9,714	4,564
Allegro	4,074	11,015
Facebook	3,862	6,638
InPost	2,908	2,770
Baltic Pipe	2,795	6,971
Netflix	2,470	1,495
Gazeta.pl	2,057	658
Meta	1,142	660
Booking	1,064	94

Services enabling to conduct DRDoS attacks

In 2024, we received 27,202,309 reports about 585,325 IP addresses in Poland that hosted services that could have been used to conduct Distributed Reflection Denial of Service (DRDoS) attacks. We took into account IP addresses at which misconfigured services are actually available, as well as those 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.

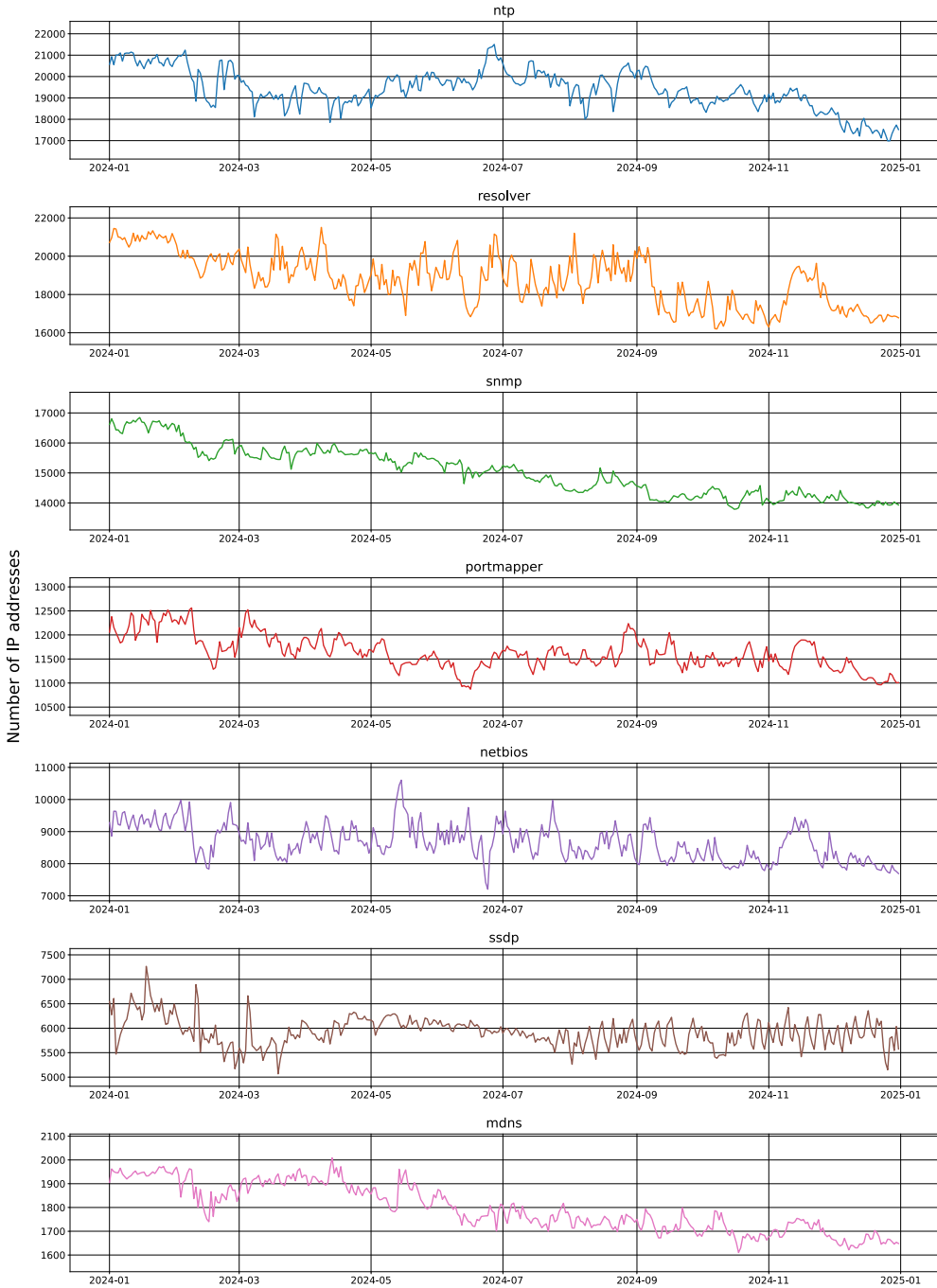
Table 16 presents a list of services that could have been used for attacks and were the most represented in the Polish Internet. The standard deviation refers to the variation in the daily number of IP addresses observed over the year. The observation time means the percentage of the year for which we had information about a given service. The selected services are discussed later in this subchapter.

TABLE 16. List of the most common misconfigured services that can be used for DRDoS attacks.

Name of vulnerability/ open service	Average daily number of IP addresses	Daily maximum number of IP addresses	Standard deviation	Observation time
NTP	19,310	21,573	779	100%
Open resolver	18,795	21,877	1,077	99,45%
SNMP	14,966	16,984	857	99,45%
Portmapper	11,597	12,572	444	99,72%
NetBIOS	8,670	10,792	705	99,45%
SSDP	5,892	7,466	487	100%
mDNS	1,785	2,012	139	99,72%
mssql	1,143	2,046	217	99,45%
Ubiquiti	1,001	1,386	157	99,72%
DVR DHCPDiscover	545	2,757	404	99,72%
CHARGEN	107	142	13	99,45%
CoAP	38	49	5	99,18%
QOTD	16	34	4	99,72%
XDMCP	15	21	1	99,72%
ARD	8	13	1	99,72%
RDPEUDP	4	121	8	95,62%

Chart 2 shows the trend in the number of devices we have observed that can be used to carry out DRDoS attacks. The charts refer to the seven most frequently reported services.

CHART 2. Most common misconfigured services that can be used in DRDoS attacks. The chart shows variations in the numbers of vulnerable IP addresses in Poland in 2024



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 used for DDoS attacks.

Number of reports per year

7,306,131

Number of unique IP addresses to which the reports related

147,559

TABLE 17. Daily number of addresses where an active NTP service on a publicly available interface was detected, broken down by autonomous systems.

AS number	AS name	Average	Maximum	Percentage of all addresses in AS
5617	Orange	10,131	13,601	0,06%
57608	DGNET	1,432	2,055	16,95%
12741	Netia	1,310	1,492	0,08%
6830	UPC	841	1,099	0,03%
12912	T-Mobile	810	877	0,07%
48956	HYPERNET	604	862	12,42%
199715	MSITELEKOM	383	441	2,45%
9085	SUPERMEDIA	275	293	0,65%
39869	LIVENET	270	321	1,01%
29314	Vectra	266	334	0,05%

Open DNS servers

Open DNS servers (open resolver) can be used to carry out 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.

Number of reports per year

5,024,018

Number of unique IP addresses to which the reports related

259,309

TABLE 18. Daily number of IP addresses at which an open DNS server was detected, broken down by autonomous systems

AS number	AS name	Average	Maximum	Percentage of all addresses in AS
5617	Orange	12,243	15,723	0,06%
12741	Netia	1,445	3,439	0,09%
12912	T-Mobile	566	650	0,05%
198023	YESNET	514	648	10,04%
50599	Dataspace	428	1,069	3,56%
6830	UPC	412	474	0,01%
13110	INEA	356	397	0,22%
29314	Vectra	332	384	0,06%
8374	Plus/ Cyfrowy Polsat	280	319	0,07%
31242	TKPSA	197	219	0,17%

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.

Number of reports per year

5,478,083

Number of unique IP addresses to which the reports related

72,970

TABLE 19. Daily number of IP addresses at which an active SNMP service was detected in a publicly available interface, broken down by autonomous systems

AS number	AS name	Average	Maximum	Percentage of all addresses in AS
12741	Netia	1,761	1,891	0,11%
5617	Orange	1,667	1,702	0,01%
20804	TELENERGO	757	833	0,31%

AS number	AS name	Average	Maximum	Percentage of all addresses in AS
199390	ALFAKS	502	507	16,34%
8374	Plus/Cyfrowy Polsat	485	568	0,11%
12912	T-Mobile	410	505	0,04%
57978	Digicom	346	376	16,89%
57608	DG-Net	340	644	4,02%
6830	UPC	237	256	0,01%
41809	Netia	209	245	1,70%

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.

Number of reports per year

4,309,706

Number of unique IP addresses to which the reports related

46,761

TABLE 20. Daily number of addresses at which an active portmapper service detected at a publicly available interface, broken down into autonomous systems

AS number	AS name	Average	Maximum	Percentage of all addresses in AS
16276	OVH	2,952	4,141	0,06%
50599	Dataspace	467	984	3,88%
57367	ECO-ATMAN	319	360	2,31%
12741	Netia	251	270	0,02%
201814	MEVSPACE	247	359	1,46%
6830	UPC	223	414	0,01%
31242	TKPSA	209	231	0,19%
197155	ARTNET	209	226	1,74%
59491	LIVENET	192	279	2,68%
50840	HITME	179	189	3,88%

NetBIOS

NetBIOS is a low-level protocol used mostly by Microsoft systems. It should be used only in local networks. If it is available from a public network, it constitutes a threat – for example in connection with the possibility of using it for DDoS attacks.

Number of reports per year

1,689,197

Number of unique IP addresses to which the reports related

33,438

TABLE 21. Daily number of addresses at which an active NetBIOS service was detected in a publicly available interface, broken down into autonomous systems

AS number	AS name	Average	Maximum	Percentage of all addresses in AS
5617	Orange	4,599	5,462	0,03%
12741	Netia	325	449	0,02%
13110	INEA	125	141	0,08%
12912	T-Mobile	112	140	0,01%
16276	OVH	102	166	0,00%
12824	home.pl	87	103	0,04%
8374	Plus/Cyfrowy Polsat	78	90	0,02%
8970	WASK	64	236	0,10%
197226	SPRINT	54	60	0,38%
29314	Vectra	48	64	0,01%

Vulnerable services

In this section, we present statistics on services that are vulnerable to attacks and vulnerabilities in services that can lead to information leaks. These include services with known vulnerabilities as well as services that have not been configured correctly, for example, allowing unrestricted access to the Internet contrary to good security practices or access to applications without authentication. In 2024, we recorded 53,010,669 such observations concerning 882,826 IP addresses from Poland.

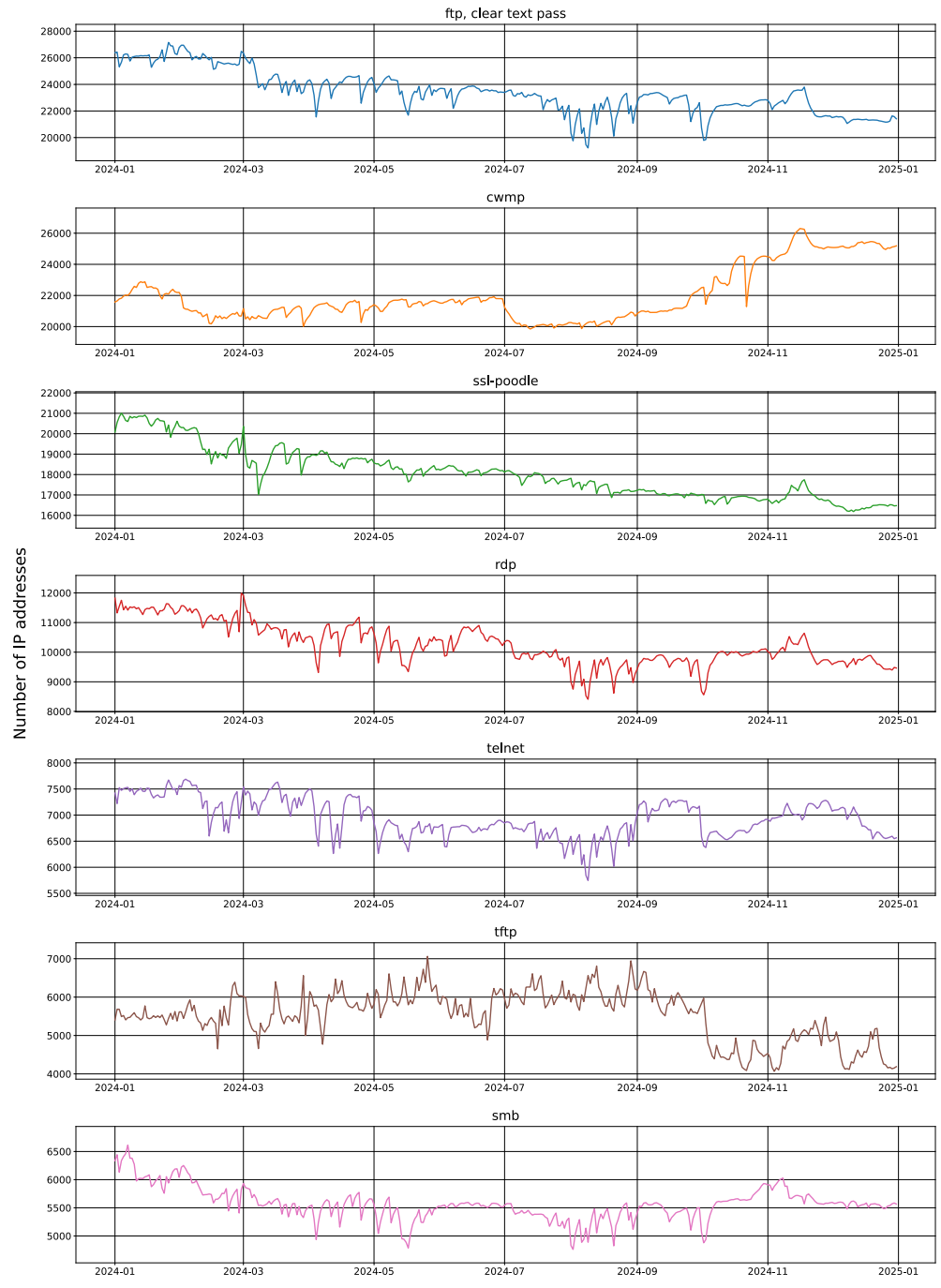
Table 22 presents a list of services that could have been attacked and were the most numerous in the Polish Internet. The standard deviation refers to the variation in the daily number of IP addresses observed over the year. The observation time means the percentage of the year for which we had information about a given service.

TABLE 22. List of the most numerous services exposed to attacks in Poland

Name of vulnerability/ open service	Average daily number of IP addresses	Daily maximum number of IP addresses	Standard deviation	Observation time
FTP (clear text credentials)	23,049	27,269	1,853	99,45%
CWMP	21,855	26,304	1,803	98,90%
SSL-POODLE	17,884	21,008	1,465	99,67%
RDP	10,115	12,045	886	99,45%
Telnet	6,867	7,815	647	99,72%
TFTP	5,507	7,055	470	99,72%
SMB	5,499	6,531	425	100%
VNC	3,409	5,712	637	100%
RSYNC	1,934	2,551	256	99,72%
SSL-FREAK	1,933	2,962	286	99,72%
MQTT	1,028	1,305	117	100%
MongoDB	746	886	77	100%
AMQP	718	850	80	100%
AFP	668	1,084	121	100%
NAT-PMP	643	890	121	99,45%
IPMI	467	613	91	99,72%
Redis	440	2,863	832	99,72%
IPP	428	675	71	100%
ISAKMP	376	462	28	89,72%
LDAP	277	334	17	100%
Memcached	193	214	18	100%

Chart 3 shows the annual trend in the number of devices with vulnerable services that we have observed. The charts refer to 7 most frequently reported services

CHART 3. Most common vulnerable services. The chart shows variations in the numbers of vulnerable IP addresses in Poland in 2024



We have divided the discussion of vulnerable services into sections on Exchange servers, HTTP services, and industrial systems (ICS/OT). The information is presented in separate tables below.

Exchange

This table provides information concerning the vulnerable Microsoft Exchange servers. All the vulnerabilities listed are Remote Code Execution vulnerabilities. The standard deviation refers to the variation in the daily number of IP addresses observed over the year. The observation time means the percentage of the year for which we had information about a given service.

TABLE 23. List of the most numerous exchange servers exposed to attacks in Poland

Vulnerability name	Average daily number of IP addresses	Daily maximum number of IP addresses	Standard deviation	Observation time
CVE-2024-21410	337	435	61	42,34%
CVE-2024-26198	174	384	58	79,50%
CVE-2023-21529	44	98	13	99,18%
CVE-2023-36439	38	118	21	99,18%
CVE-2022-41082	31	71	9	99,18%
CVE-2023-36745	30	77	13	99,18%
CVE-2024-21410	19	70	6	86,33%
CVE-2021-27065	9	19	2	99,18%
CVE-2020-0688	9	19	2	99,18%
CVE-2021-26855	5	10	1	99,18%

HTTP

The following provides information on systems using the HTTP protocol that may be vulnerable to attacks. The meaning of the vulnerabilities given in the table is as follows:

- **Basic auth** – the server allows credentials to be sent in plaintext, without encryption.
- **Basic auth (IoT)** – as above. It applies to IoT devices.
- **.git folder** – a publicly available .git folder.

The standard deviation refers to the variation in the daily number of IP addresses observed over the year. The observation time means the percentage of the year for which we had information about a given service.

TABLE 24. List of the most numerous HTTP servers exposed to attacks in Poland

Name	Average daily number of IP addresses	Daily maximum number of IP addresses	Standard deviation	Observation time
Basic auth	8,039	11,334	965	99,18%
Basic auth (IoT)	4,969	8,632	880	99,18%
Folder .git	440	562	46	99,18%
Fortinet CVE-2024-21762	270	648	92	82,51%
Fortinet CVE-2023-27997	269	528	128	99,72%
Roundcube CVE-2023-43770	264	329	20	88,25%
Tinyproxy CVE-2023-49606	249	415	76	65,02%
Roundcube CVE-2023-5631	196	621	129	99,72%
Zimbra CVE-2024-45519	187	391	46	24,31%
Zimbra CVE-2022-37042	152	207	22	99,72%
Palo Alto VPN CVE-2024-3400	32	253	16	70,21%
GeoServer CVE-2024-36401	8	53	6	74,04%
Ivanti VPN CVE-2024-21894	6	10	1	44,26%

Industrial control systems

This table provides information concerning the publicly available ICS/OT systems. No specific vulnerabilities were checked during scanning. Such devices, however, should not be available from the Internet. Industrial protocols often do not support authentication at all. The list provides IP addresses the services listed below are actually available, as well as services that are available intentionally, including honeypot systems, as it is difficult to distinguish between them on the basis of Internet scanning data, and their total number is small. The standard deviation refers to the variation in the daily number of IP addresses observed over the year. The observation time means the percentage of the year for which we had information about a given service.

TABLE 25. List of the most numerous ICS/OT systems exposed to attacks in Poland

Name of vulnerability/ open service	Average daily number of IP addresses	Daily maximum number of IP addresses	Standard deviation	Observation time
S7	179	279	31	100%
Codesys	147	236	28	100%
BACnet	116	161	17	100%
Modbus	92	135	14	100%
EtherNet/IP	62	81	7	100%
OPC UA Binary	28	47	4	100%
Fox	24	34	3	100%
Unitronics	17	40	7	99,72%
DNP3	10	19	2	99,45%
IEC 60870-5-104	6	12	2	99,72%
Omron FINS	6	15	1	99,72%
GE SRTP	6	12	2	100%
PC Worx	5	8	1	84,69%
MELSEC-Q	3	7	0	99,45%
ICCP	2	6	1	97,54%

Artemis

In 2024, a total of 249,806 domains and IP addresses and 795,547 subdomains were scanned, which was more than three times as many as in 2023. This increase is due both to the inclusion of new categories of websites (e.g. cultural institutions) in the scan and to improvements in the techniques for finding domains and subdomains.

The institutions scanned included those listed in the table below.

TABLE 26. Number of scanned domains, subdomains and IP addresses in 2024, broken down by category

Category	Number of domains and IP addresses scanned	Number of subdomains scanned
Universities , e.g. university and faculty websites, but also domains related to conferences or research projects	142,630	110,185
Schools and educational institutions , including websites of primary and secondary schools and post-secondary schools, youth community centres, kindergartens and psychological and pedagogical counselling centres	67,509	281,478
Local government units , municipal and district websites, but also, for example, the websites of waste disposal companies, archive domains or mail handling systems	20,501	230,448
Cultural institutions , e.g. the websites of theatres, galleries or libraries	6,878	16,272
Submitted domains : domains of companies and entities that have voluntarily submitted them for scanning	6,189	101,617
Health sector , e.g. the websites of hospitals, but also of public institutions related to health	3,178	18,422
Banks	1,839	15,926
.gov.pl domains	1,596	17,520
Politicians and parties , websites of candidates, members of parliament, senators, mayors and political parties in the context of parliamentary, local or European elections	1,202	1,496
National newspapers and websites	792	80,090
Key service providers	439	23,407
Professional organisations , e.g. websites of chambers of physicians or lawyers	375	2,813
Local newspapers and websites	214	865
Industrial automation manufacturers	87	1,812

A total of 331,632 vulnerabilities or misconfigurations were reported, including 19,965 with high, 220,429 with medium and 91,238 with low threat. This represents an almost twofold increase in the number of vulnerabilities and misconfigurations detected in comparison to 2023. This increase is due to both the creation of new modules in the Artemis system and the addition of new categories of scanned websites. At least one vulnerability/misconfiguration was detected in 104,137 scanned domains/subdomains.

The types of vulnerabilities or misconfigurations found are summarised in the table below. The scan is automatic, which is why the figures may include duplicates or refer to situations where there is no vulnerability in reality, e.g. incorrectly configured SSL/TLS was detected on a domain that is not actually used.

TABLE 27. Number of vulnerabilities or misconfigurations found in 2024 and a description of the associated risks

Number of occurrences	Type of vulnerability/misconfiguration	Risk associated with vulnerability/misconfiguration
193 864	Use of outdated software	Attack using known vulnerabilities – some of the vulnerabilities can result in the possibility of downloading data from the website, others allow changing the content of the website or, for example, obtaining the administrator rights
45 667	Problems with the configuration of SSL/TLS or similar mechanisms	Interception of user communication with the website – if the data is intercepted and the criminal acquires the login and password, they can log in to the website as an authorised user
31 532	Instances in which a resource such as an administration panel or login panel (e.g. for a database or remote desktop service) was publicly accessible	An attack is possible, for example, if one of the accounts has a weak password or if there are vulnerabilities in the service.
26 527	Incorrectly configured mechanisms for verifying the e-mail sender	Sending fake e-mails from a given domain
19 894	Instances in which server configuration information, a list of subdomains or lists of files in server folders were publicly available	This can make it easier for an attacker to conduct reconnaissance, learn the software used or file names that should not be publicly available, and consequently also make it possible to download them
6040	Specific critical or serious vulnerabilities	For example, taking over a page or downloading data from a database
4792	Instances in which sensitive data such as backups, source code, database dumps or the server event log were publicly available	Download of sensitive data
170	Instances in which a domain was about to expire	Unavailability of the service or takeover of the domain by an attacker

System administrators receive regular updates on the vulnerabilities detected. More information on the Artemis project is available in [other part of the report](#) (p. 67).

List of figures

FIGURE 1.	Example of a message sent by criminals	15
FIGURE 2.	Attachment sent in a message pretending to be from the Police	15
FIGURE 3.	Fake message informing about copyright violation	16
FIGURE 4.	Fake request for payment	17
FIGURE 5.	Example of false verification using Captcha	17
FIGURE 6.	Leak site of the Akira Group	20
FIGURE 7.	Homepage of the bezpiecznedane.gov.pl website	29
FIGURE 8.	Information on usage restriction of the Personal Identification Number (PESEL) from the gov.pl website	31
FIGURE 9.	Fake login panel for the Interia webmail service used by the UNC1151 group	33
FIGURE 10.	Propaganda content posted by the UNC1151 group on the website of the Polish Anti-Doping Agency	34
FIGURE 11.	Example of disinformation content on Telegram	34
FIGURE 12.	Example of a message used by the APT28 group to distribute malware	35
FIGURE 13.	Diagram showing the different stages of infection	35
FIGURE 14.	Example of a fake Microsoft Outlook login panel from the APT28 group	36
FIGURE 15.	Example of a scam using the subject of the flood. On the left: an advertisement for a fake fundraiser; on the right: a website that was deceptively similar to the real eSkarbonka website run by the Great Orchestra of Christmas Charity	38
FIGURE 16.	Example of Joker malware in the Google Play store	42
FIGURE 17.	On the left: the Network Safety Service icon on the main screen, on the right: the Network Safety Service in the mObywatel application	46
FIGURE 18.	Instructions on how to enable notifications in the Network Safety Service	47
FIGURE 19.	Network Safety service in the mObywatel app	52

FIGURE 20.	Illustration used to promote the #12CyberPorad (12 Cyber Tips) series on social media	53
FIGURE 21.	Krzysztof Zając at the Black Hat conference in Las Vegas	54
FIGURE 22.	Main menu of the control panel of the wastewater treatment plant	57
FIGURE 23.	Settings of the technological process of the treatment plant, with the possibility to change the operating modes	57
FIGURE 24.	Start screen of the control panel of a sewage treatment plant with visible contact details	58
FIGURE 25.	Screenshots of some of the found panels	59
FIGURE 26.	A representative of the Locked Shields 2024 exercise organiser discusses the situation in Berylia, defended by team BT17	62
FIGURE 27.	Polish team at the ECSC 2024 competition	64
FIGURE 28.	Polish team at the closing ceremony	65
FIGURE 29.	The Polish team receives the competition flag	65
FIGURE 30.	Content of a sample notification sent from Snitch	71
FIGURE 31.	Comparison of the number of hosts obtained through n6 only	72
FIGURE 32.	Screenshot of the AIL tool interface	76
FIGURE 33.	Screenshot of the Graphoscope interface	76
FIGURE 34.	Screenshot of the Taranis NG tool interface	77
FIGURE 35.	Screenshot of the n6 platform interface	77
FIGURE 36.	Screenshot of the MWDB platform interface	78
FIGURE 37.	Screenshot of the DRAKVUF Sandbox interface	79
FIGURE 38.	Screenshot of the FlowIntel interface	79

List of tables

TABLE 1.	Number of incidents recorded, broken down into ransomware families	18
TABLE 2.	Notifications sent by CERT Polska regarding vulnerabilities in individual products	23
TABLE 3.	APT group activity observed by CERT Polska/CSIRT NASK in 2024 has been marked with x	32
TABLE 4.	Malware statistics for Android mobile platforms in 2024	41
TABLE 5.	Number of vulnerabilities disclosed in each month of 2024	50
TABLE 6.	Snitch statistics broken down into OT and IT systems	73
TABLE 7.	Number of incident reports and incidents registered in 2024	84
TABLE 8.	Incidents reported by law to CSIRT NASK from 1 January to 31 December 2024	86
TABLE 9.	Number of incidents handled by CERT Polska in 2018–2024	86
TABLE 10.	Incidents handled by CERT 2024, broken down by economic sectors. Designation of sectors according to the internal classification of CSIRT NASK	86
TABLE 11.	Incidents handled by CERT Polska in 2024, broken down by category. Category designation according to ENISA taxonomy	88
TABLE 12.	Largest botnets in Poland	90
TABLE 13.	Providers with the highest number of phishing websites in Polish autonomous systems	91
TABLE 14.	Most common top-level domains (TLD) included in the Warning List	92
TABLE 15.	The most common phishing impersonation targets that are included in the Warning List	92
TABLE 16.	List of the most common misconfigured services that can be used for DRDoS attacks	93
TABLE 17.	Daily number of addresses where an active NTP service on a publicly available interface was detected, broken down by autonomous systems	95

TABLE 18.	Daily number of IP addresses at which an open DNS server was detected, broken down by autonomous systems	96
TABLE 19.	Daily number of IP addresses at which an active SNMP service was detected in a publicly available interface, broken down by autonomous systems	96
TABLE 20.	Daily number of addresses at which an active portmapper service detected at a publicly available interface, broken down into autonomous systems	97
TABLE 21.	Daily number of addresses at which an active NetBIOS service was detected in a publicly available interface, broken down into autonomous systems	98
TABLE 22.	List of the most numerous services exposed to attacks in Poland	99
TABLE 23.	List of the most numerous exchange servers exposed to attacks in Poland	101
TABLE 24.	List of the most numerous HTTP servers exposed to attacks in Poland	102
TABLE 25.	List of the most numerous ICS/OT systems exposed to attacks in Poland	103
TABLE 26.	Number of scanned domains, subdomains and IP addresses in 2024, broken down by category	104
TABLE 27.	Number of vulnerabilities or misconfigurations found in 2024 and a description of the associated risks	105

List of charts

CHART 1.	Chart showing vulnerabilities by category	60
CHART 2.	Most common misconfigured services that can be used in DRDoS attacks. The chart shows variations in the numbers of vulnerable IP addresses in Poland in 2024	94
CHART 3.	Most common vulnerable services. The chart shows variations in the numbers of vulnerable IP addresses in Poland in 2024	100



NASK-PIB/CERT Polska

Kolska 12 Street
01-045 Warsaw

Reception

+48 22 380 82 00
+48 22 380 82 01

Secretary

+48 22 380 82 04
+48 22 380 82 01

info@cert.pl
www.cert.pl