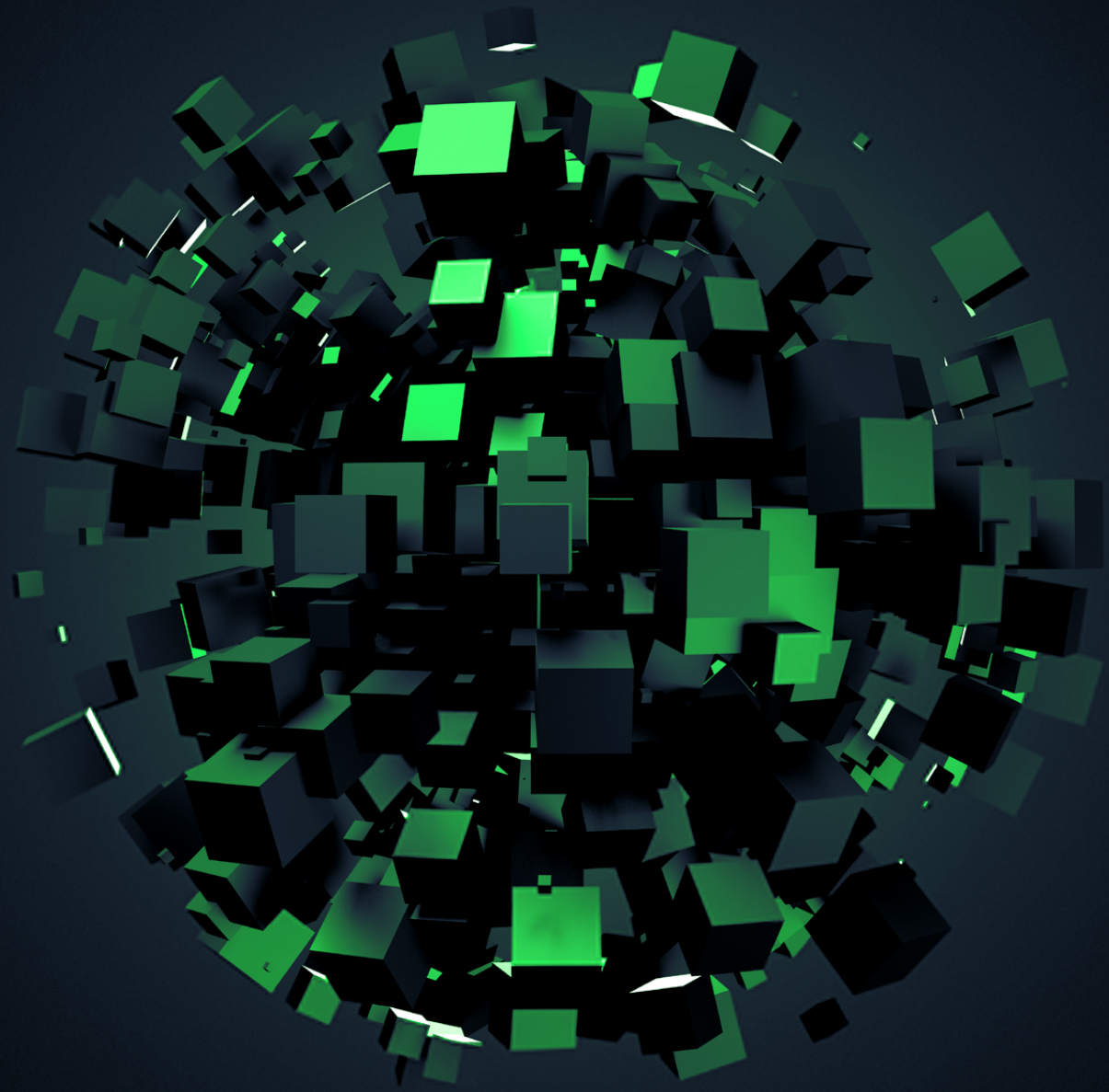
ANNUAL REPORT 2025

from the actions of CERT Polska

The Polish security landscape



30 LAT | CERT.PL NASK

ANNUAL REPORT 2025

from the actions of CERT Polska

The Polish security landscape

CERT.PL NASK | NASK | Ministry of Digital Affairs Republic of Poland

THIS PROJECT IS FUNDED BY THE MINISTRY OF DIGITAL AFFAIRS

TITLE: Annual report from the actions of CERT Polska 2025.
The Polish security landscape.

AUTHORS: CERT Polska team

Warsaw 2026

ISBN: 978-83-68356-52-6

National Research Institute NASK
12 Kolska Street
01–045 Warszawa

Table of contents

Introduction

Another year of CERT Polska's activities is behind us. It was a special one, as it marked the end of the third decade of our operations – we are celebrating our 30th anniversary! The year 2025 was a time full of challenges, growth, and a comprehensive approach to shaping cybersecurity – from proactive threat detection, through handling reports and responding to incidents, to sharing knowledge and building public awareness.

Here, you will find stories about widespread fraud campaigns, insights from monitoring APT groups, and first-hand information on breakthroughs in threat detection. We will talk about security testing, vulnerability disclosure, malware, and ransomware attacks.

As always, we will also cover national and international cooperation, exercises and competitions, projects involving teams from around the world, Poland's presidency of the Council of the European Union, and new initiatives connecting cybersecurity professionals from various institutions and sectors of the economy.

There will also be plenty of topics for fans of solid technical solutions. In the report, we will discuss services and software that we co-create or develop ourselves – AIPITCH, DNS4EU, FETTA, PERUN, Artemis, the Warning List, MWDB, n6, and our flagship initiative – moje.cert.pl.

The above list shows just how complex and diverse the tasks our team faces daily are. However, at the core of all these activities lies the need to strengthen and improve the system that makes Poland's cyberspace safer. The second pillar is knowledge – awareness of threats and understanding how to prevent them are the most effective weapons in the fight against cybercriminals.

CERT Polska is made up of people, and we want our report to feel human too. Substantive, rich in reliable knowledge, data, and charts, yet at the same time engaging and compelling. Today, you will read about many important and challenging topics, but they are also matters we can simply be proud of – both as CERT and as Poles.

Enjoy your reading!

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,
- coordination of incident handling,
- 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:

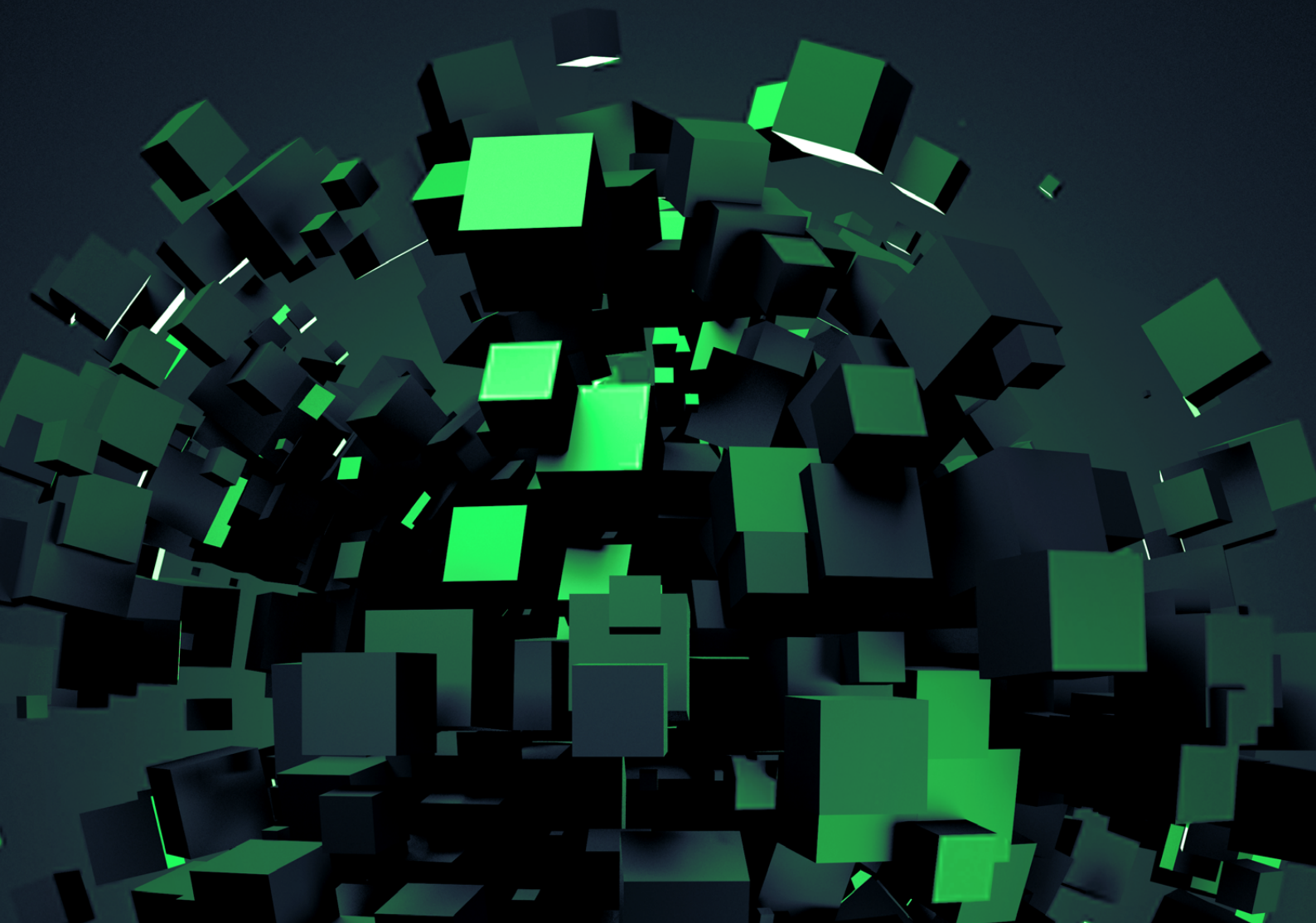
- units from the public finance sector indicated in Article 9, section 2–6, 11 and 12 of the Act of 27 August 2009 on public finances,
- units subordinate to or supervised by government administration authorities, excluding units referred to in section 7, item 2 of the Act on the National Cybersecurity 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 building cybersecurity awareness and proactively seeking 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

01.01–**30**.06 Period of Poland's Presidency of the Council of the European Union

https://www.gov.pl/web/cyfryzacja/polska-prezydencja-w-radzie-ue-bezpieczna-i-cyfrowa-europa-dzieki-dzialaniom-ministerstwa-cyfryzacji2

02.01 Announcement of the planned phase-out of the first version of the Warning List

https://cert.pl/en/posts/2025/01/hole-v1-deprecation-notice/

09.01 Artemis detected over 500,000 bugs and vulnerabilities

https://x.com/CERT_Polska/status/1877314450845262010

13.01 We reported a data breach involving the website sklepbaterie.pl

https://x.com/CERT_Polska/status/1878786709510390037

17.01 We warned about a phishing campaign targeting Onet e-mail users

https://x.com/CERT_Polska/status/1880315748419268641

FEBRUARY

05.02 We warned about websites impersonating gov.pl, falsely claiming to provide information about financial support

https://x.com/CERT_Polska/status/1887121450823188910

11.02 We reported a campaign in which fraudsters sent messages about a supposed tax refund

https://x.com/CERT_Polska/status/1889269064234914191

12.02 Launch of the moje.cert.pl service

https://cert.pl/posts/2025/02/moje.cert.pl/

MARCH

07.03 Data from Genesis Market was made available on moje.cert.pl

https://x.com/CERT_Polska/status/1898002700203147307

18.03 Scans carried out through moje.cert.pl allowed us to detect over 100,000 vulnerabilities and misconfigurations

https://x.com/CERT_Polska/status/1901918495685988657

24.03 We warned about a phishing campaign in which fraudsters impersonated the e-TOLL system

https://x.com/CERT_Polska/status/1904131427324555692

25.03 We published the article “Critical vulnerabilities in the Ingress-Nginx controller in Kubernetes”

https://cert.pl/posts/2025/03/krytyczne-podatnosci-w-kontrolerze-ingress-nginx-kubernetes/

28.03 Service moje.cert.pl has over 10,000 users

https://x.com/NASK_pl/status/1905514627188097523

28.03 We warned about a campaign using the image of the Patent Office

https://x.com/CERT_Polska/status/1905612569374503160

31.03 We published the article “Meta fails to sufficiently address CERT Polska’s recommendations”

https://cert.pl/en/posts/2025/03/evaluation-of-expectations-towards-meta/

APRIL

03–04.04 SECURE International Summit 2025 in Bydgoszcz

https://polish-presidency.consilium.europa.eu/en/news/europe-unites-in-the-face-of-cyber-attacks-end-of-the-secure-international-summit-2025/

03.04 Launch of the “2024 Annual Report on CERT Polska’s Activities”
https://cert.pl/en/posts/2025/04/annual-report-2024/

18.04 CERT Polska training for employees of the Warsaw Waterworks
https://x.com/CERT_Polska/status/1913176503711379599

18.04 New leak sources added to moje.cert.pl
https://x.com/CERT_Polska/status/1913212995783532622

23.04 We warned about a campaign in which fraudsters impersonated the BLIK service
https://x.com/CERT_Polska/status/1914993630323855666

24.04 We published an article on deobfuscation techniques in Lumma Stealer
https://cert.pl/en/posts/2025/04/peephole-deobfuscation/

30.04 The portal bezpiecznedane.gov.pl was enriched with additional datasets
https://x.com/CERT_Polska/status/1917602656853299642

MAY

09.05 In the NATO Locked Shields 2025 exercise, the Polish-French team took 2nd place
https://x.com/CERT_Polska/status/1920832659820892167

12–16.05 CyberWeek in Kraków – a week of expert meetings and work on the future of cybersecurity in Europe
https://x.com/CYFRA_GOV_PL/status/1923389157931397380

19.05 We warned about a campaign in which fraudsters impersonated Tauron Polska Energia
https://x.com/CERT_Polska/status/1924464876774105293

22.05 Launch of threat notifications in moje.cert.pl
https://cert.pl/posts/2025/05/moje.cert.pl-powiadomienia/

JUNE

01.06 The phase-out of the first version of the Warning List

https://cert.pl/en/posts/2025/01/hole-v1-deprecation-notice/

04.06 We warned about a campaign in which fraudsters impersonated InPost and distributed malware

https://x.com/CERT_Polska/status/1930233080767291609

05.06 We published the article “UNC1151 campaign exploiting a vulnerability in Roundcube software to steal credentials”

https://cert.pl/en/posts/2025/01/hole-v1-deprecation-notice/

06.06 EU Cyber Blueprint adopted during the formal meeting of the Transport, Telecommunications, and Energy Council

https://x.com/CERT_Polska/status/1930988050647286042

11.06 We warned about a campaign in which fraudsters impersonated the Statistical Office in Warsaw

https://x.com/CERT_Polska/status/1932757483920990329

16.06 We warned about another wave of fake ads claiming the possibility of winning a public transport season ticket

https://x.com/CERT_Polska/status/1934612683996696683

23.06 Recommendation from the Government Plenipotentiary for Cybersecurity regarding Roundcube software updates

https://x.com/CERT_Polska/status/1937193939146068304

JULY

04–06.07 National qualifications for the European Cybersecurity Challenge 2025

https://x.com/CERT_Polska/status/1941134908388233589

09.07 In 2025, we added 100,000 domains to the Warning List

https://x.com/CERT_Polska/status/1942961943574384785

17.07 We reported a campaign of fake SMS messages claiming users' computer data had been compromised

https://x.com/CERT_Polska/status/1945785553296732293

21.07 Announcement of the Polish representatives for the European Cybersecurity Challenge 2025

https://x.com/CERT_Polska/status/1947250200629698847

24.07 We reported the publication of a decryptor for the Phobos/8Base ransomware group

https://moje.cert.pl/komunikaty/2025/19/publikacja-dekryptora-phobos/

AUGUST

01.08 We reported an e-mail campaign claiming the recipient had compromising recordings

https://x.com/CERT_Polska/status/1951236500508516363

06.08 We released the DRAKVUF Sandbox v0.19.0 tool

https://x.com/CERT_Polska/status/1953106389481509309

07.08 We published "CERT Polska team recommendations for establishing CSIRT teams"

https://cert.pl/posts/2025/08/rekomendacje-csirt/

12.08 After six months of operation, moje.cert.pl has over 12,500 users

https://x.com/NASK_pl/status/1955167359955529868

20.08 We warned about an SMS campaign claiming a "government energy coupon"

https://x.com/CERT_Polska/status/1958159593718026362

SEPTEMBER

03.09 We warned about a new "refund" scam in which fraudsters impersonated the NFZ (National Health Fund)

https://x.com/CERT_Polska/status/1963225473900519803

05.09 We published the guide “The security of your pocket: how to protect your phone”

https://cert.pl/bezpieczny-telefon/

16.09 Through scans conducted via moje.cert.pl, we detected one million vulnerabilities and misconfigurations

https://x.com/CERT_Polska/status/1967978056104206662

17.09 We published the article “How to recognize fake websites and avoid phishing”

https://cert.pl/posts/2025/09/analiza-adresow-stron/

19.09 We warned about remote job offers with suspiciously high salaries

https://x.com/CERT_Polska/status/1968948175756214636

22.09 We reported that 1.8 million records containing login credentials were added to the bezpiecznedane.gov.pl service

https://x.com/CERT_Polska/status/1970090473533456432

OCTOBER

06–09.10 Final competitions of the European Cybersecurity Challenge 2025 in Warsaw

https://www.nask.pl/aktualnosci/cyberbitwa-rozstrzygnieta-wlosi-gora-polska-w-pierwszej-dziesiatce

15.10 We published the first issue of the monthly report on the state of cybersecurity in Poland

https://cert.pl/posts/2025/10/raport-miesieczny-09/

24.10 A campaign of fake SMS messages in which fraudsters impersonated the e-Tax Office

https://x.com/CERT_Polska/status/1981707250596237406

NOVEMBER

03.11 We published the article “Analysis of the NGate (NFC relay) malware campaign”

https://cert.pl/posts/2025/11/analiza-ngate/

04.11 We warned about a fake message campaign targeting PKO BP bank customers

https://x.com/CERT_Polska/status/1985738816670588973

14.11 We reported on an actively exploited vulnerability CVE-2025-64446 in FortiWeb software

https://moje.cert.pl/komunikaty/2025/57/aktywnie-wykorzystywana-krytyczna-podatnosc-w-urzadzeniach-fortinet-forti web-manager/

DECEMBER

02.12 Four CERT Polska experts spoke at the Oh My Hack 2025 conference

https://x.com/CERT_Polska/status/1995504567157481857

04.12 We reported a critical vulnerability CVE-2025-55182 (React2Shell)

https://moje.cert.pl/komunikaty/2025/61/krytyczna-podatnosc-w-react-server-components-oraz-innych-aplikacjach-z-tym-rozwiazaniem/

09.12 We warned about a phishing campaign in which fraudsters impersonated Spotify

https://x.com/CERT_Polska/status/1998361990641648061

13.12 We published the article “Public Wi-Fi networks – is there anything to worry about?”

https://cert.pl/posts/2025/12/publiczne-sieci-wifi/

13.12–**24**.12 We shared posts as part of the holiday #CyberPrezent (#CyberGift) series

https://x.com/CERT_Polska/status/2003858209610850480

19.12 We reported that moje.cert.pl has 15,000 registered users

https://x.com/CERT_Polska/status/2002000973766484051

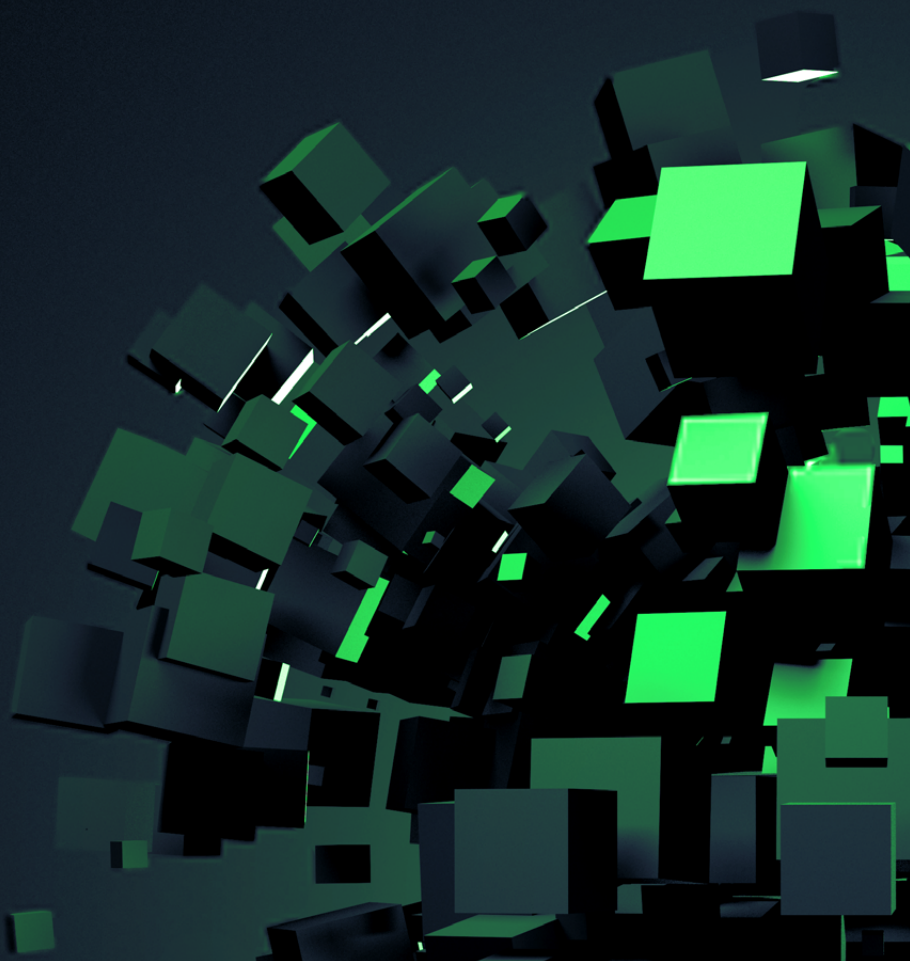
29.12 Coordinated attacks targeting multiple entities in the energy sector

https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/

31.12 We posted that the number of malicious domains added by us to the Warning List since its inception has exceeded 500,000.

https://x.com/CERT_Polska/status/2006379829466177890

30 Years of CERT Polska – perspectives from the team leaders



Marcin Dudek

HEAD OF CERT POLSKA SINCE 2025

This year, we are celebrating the 30th anniversary of CERT Polska. It is the result of tremendous work by many people over the years. The team has grown, the environment and challenges have changed, but certain elements have always remained foundational. What amazed me when I joined CERT Polska six years ago was the level of commitment of the people working here and their sense of mission.

When we analyse an incident, it is not just about making the statistics match, but about actually understanding what happened. When we detect a new type of phishing site, simply blocking it is not enough – curiosity drives us to discover another hundred and create rules to catch new ones. Many ideas for development and initiatives arise from the bottom up. For example, the moje.cert.pl portal was not imposed by anyone – a group of people realized that such a place was missing and created it within a few months.

This is also thanks to successive generations of team leaders, each coming from within the organization, who understood the team's specificity and knew that sometimes it is enough to lightly guide directions rather than impose them. Krzysiek, Mirek, Piotrek, Przemek, Sebastian – thank you. The contribution of each of you has been invaluable to what CERT Polska is today.

I am curious about your perspective over the years: how did "cyber" look in your time? What were the challenges back then? Which decisions were crucial? And most importantly – what should we continue to prepare for?

Krzysztof Silicki

HEAD OF CERT POLSKA FROM 1996 TO 2001

How did the cybersecurity landscape in Poland look when you assumed the position of Head of CERT Polska? What types of threats were dominant?

The beginning of CERT's history dates back to 1996. This was only a few years after NASK connected Poland to the global Internet. There was a dynamic increase in the number of hosts connected to the network, and even then, many threats and incidents could already be observed. For example, we were dealing with mass scanning and probing within the national IP address space, looking for vulnerabilities in the configuration of computers connected to the Internet – and finding system weaknesses or weak passwords was not difficult, because few connected entities were aware of the need to use firewalls, and users often used weak passwords. A common type of incident was so-called website defacements, in which various hackers broke into victims' computer systems and replaced their websites with their own content. The affected entity suffered reputational loss, while the attacker gained recognition among peers. Methods for installing "Trojan horses," replacing system files, and penetrating additional computers in the attacked local network were already known. Mass spam was also already a problem at that time. Interestingly, the first attempts at credit card-related fraud also occurred, with instructions on how to carry it out published online. Incidentally, since 1996, we have been publishing annual CERT Polska reports, which allow these issues to be traced over time.

What were the greatest challenges during your tenure as team leader?

First of all, reaching out to users to inform them that CERT exists, explaining its purpose, and raising awareness that the Internet is not only a fun medium for global communication, but also carries threats, so it is important to take care of one's security. We received a lot of information from CERTs abroad about attempts to attack hosts in the .pl domain, and we contacted anyone who could potentially be a target of an attack. Even at the beginning of our operations, there were events in which tens of thousands of computers in Poland were scanned and attacked by automated scripts. At that time, many organizations and users learned that we existed and offered knowledge and assistance.

Second, probably at that time, the lack of tools was a challenge. We had to create, adapt, and develop tools ourselves in order to at least partially automate our activities, because the scale of incidents was growing, while CERT consisted of only a few, then a dozen people.

Third, there was a lack of awareness among institutional and individual users that Internet security was not a niche topic and that everyone has a share of responsibility for overall security.

From your perspective, which decisions, changes, or achievements were crucial?

Of course, first of all, the decision by the leadership at the time to establish CERT within NASK. The management at the time positively received a bottom-up initiative to address security issues – this was crucial. Second, the focus on collaboration. Very quickly, we became a member of FIRST, the global organization of CERTs. We worked domestically to promote the CERT concept and support the creation of security teams, for example at large operators (Telbank, TP SA), and to cooperate with them. We also established a network for collaboration among security teams – the Abuse Forum – which a few people in the community probably still remember. Third, we almost immediately launched the SECURE conference. This is the first conference in Poland dedicated to IT security, which continues to this day, and it provides us and our constituency with an opportunity to review each year the state of cybersecurity, current threats, attacks, challenges, and strategies for defence.

However, I consider the greatest achievement to be the consistent building and upholding of a system of values that fostered a sense of mission, a real impact on reality, responsibility, high ethical standards, and the willingness to share knowledge and results.

These values attracted successive, highly competent individuals with excellent ideas for further development of CERT.

What do you consider to be the greatest cybersecurity challenges over the next 5 years? Particularly in the context of the role CERT Polska may play.

CERT Polska has gone through several phases of development along its journey. By taking on, on its own initiative, the mission of acting for the security of the Internet, through building top-level expertise, conducting innovative national and international research projects, cooperating with others who needed assistance or worked for the country's cybersecurity, to assuming the statutory role of one of the three national-level CSIRTs. I am convinced that CERT Polska will face further stages of development due to factors such as the advancement of artificial intelligence and other breakthrough technologies, the evolution of the national cybersecurity system in response to new challenges and legislation including EU law, geopolitical, hybrid, or military threats, and simply the increasing pace and scale of threats. I believe that in the coming years, a key focus will be supporting CERT Polska in the development of the National Cybersecurity System (KSC) through the creation and assistance in establishing sectoral CERTs/CSIRTs. The national response system must be properly scaled by expanding the hierarchy of additional response teams that will operate in cooperation with each other.

Of course, a major challenge is for CERT Polska to simultaneously fulfil analytical, operational, and research roles at the highest level, but such activities are precisely the fuel for a team of this calibre. Therefore, I wish our CERT continued success in the years to come.

Mirosław Maj

HEAD OF CERT POLSKA FROM 2001 TO 2010

How did the cybersecurity landscape in Poland look when you assumed the position of Head of CERT Polska? What types of threats were dominant?

When I assumed the position of Head of CERT Polska in May 2001, the cybersecurity landscape in Poland looked completely different from today. Threats were already becoming increasingly common, but at the same time, the level of e-services was at a completely different stage – the scale of digitization and dependence on online services was incomparably smaller.

As for dominant threats, there were not yet APT-class threats in the sense we understand today. Instead, daily challenges included mass scanning – broad, "wholesale" attempts to detect vulnerable services and systems.

At the same time, we had long been convinced that large-scale threats could affect the entire network, not just individual computers or institutions. And the year 2001 provided the clearest evidence: worms such as Nimda and Code Red demonstrated how quickly and widely incidents of "Internet-scale" could spread.

What were the greatest challenges during your tenure as team leader?

The greatest challenges during my tenure were primarily due to the very rapid growth in the number of incidents, while the team remained very small. The scale of work was growing faster than our operational capacity.

In addition, we set ourselves an ambitious goal: a sense of responsibility for the entire .pl domain, which was also the reason for changing the team's name from CERT NASK to CERT Polska. This was immensely satisfying, but it also meant a tremendous amount of work – both domestically and internationally. During this period, we also began actively participating in international structures, which opened new opportunities but added additional responsibilities.

Another significant challenge was building a network of contacts: developing the Polish community of response teams through the Abuse Forum and creating real collaboration between entities that had previously often operated in isolation or did not exist at all, while we worked to demonstrate that they should be established.

If I had to identify the single most difficult task, it would probably be convincing authorities in the country that the role of cybersecurity was growing rapidly and that concrete actions were needed.

From your perspective, which decisions, changes, or achievements were crucial?

I believe that the aforementioned change of the team's name – although it may seem symbolic – was important. It sent a clear signal: we declare

our support, both domestically and internationally, that we will assist in handling every incident related to the .pl constituency. Equally crucial was engaging in international projects. We built consortia, participated in projects for certain communities, such as the emerging CSIRT structures in Eastern Europe, and became a bridge for international cooperation.

What do you consider to be the greatest cybersecurity challenges over the next 5 years? Particularly in the context of the role CERT Polska may play.

From my perspective, the greatest cybersecurity challenges over the next five years will be directly related to the role of a national-level CSIRT. The collective NASK constituency CSIRT is becoming enormous, particularly in the context of implementing NIS 2, which significantly expands the scope of entities subject to its requirements.

CERT Polska already has vast experience in handling very demanding, advanced cases. However, the key task in the coming years will be developing mechanisms for scaling: knowledge, operational activities, tools, communication, and collaboration models, so that effective approaches can be practically applied across individual sectors. The problem is simple – specialists alone are not enough, so this cannot be solved merely by increasing the size of the team. It will also be crucial to develop collaboration models with sectoral CSIRTs, especially since I expect that they will operate in very different ways.

Effective, repeatable mechanisms will therefore be needed for both prevention and response – mechanisms that allow entities to achieve the required level of resilience more quickly and handle incidents more efficiently, without being fully dependent on the resources of the national CSIRT.

To give an example: a moment is approaching when it will no longer be sufficient to “simply” offer a service such as moje.cert.pl (which, by the way, is a very good solution). It will also be necessary to teach how to use this service effectively – and perhaps even to enforce specific actions on the part of regulated entities, so that the support translates into tangible improvements in security, rather than ending with mere availability of the tool.

Piotr Kijewski

HEAD OF CERT POLSKA FROM 2010 TO 2016

How did the cybersecurity landscape in Poland look when you assumed the position of Head of CERT Polska? What types of threats were dominant?

Botnets composed of infected Windows personal computers dominated, with a scale that was usually measured in hundreds of thousands or even millions of machines worldwide. Of course, there were systems from Poland among them.

Banking Trojans were at the forefront. They underwent rapid development, both in terms of methods for stealing money or gaining access to bank accounts (including via infections of mobile devices) and in terms of the botnets that enabled these attacks (mechanisms such as P2P or DGA for management). For the first time, we began to counteract this process in an organized way – both through the development of methods for detecting and blocking so-called webinjects (which are malicious code injected by malware that mimics bank websites) and through the active disruption of botnets in the framework of international cooperation.

At that time, a significant portion of botnet command-and-control infrastructure, including the famous Virut (one of the largest botnets in the world at that time), was located in the .pl domain, which became an increasingly serious problem.

Spam and DDoS attacks were also a greater challenge than today, also driven by large botnets. There were also the first observations of APT attacks, attributed to nation-states, which was a novelty. These attacks were naturally more targeted, in contrast to mass attacks driven by botnets, and observing them at that time represented a greater challenge than it does today.

Ransomware was in its infancy and usually consisted of displaying messages about encryption (or data leaks), intended to intimidate rather than actually encrypt victims' systems.

Due to banking Trojan attacks and early ransomware, ordinary users in Poland began to feel the effects of attacks on their own wallets for the first time, which was also a novelty.

What were the greatest challenges during your tenure as team leader?

Cybersecurity was not yet treated as seriously as it is today, both within NASK itself and in the country or at the governmental level. At that time, CERT Polska was, in fact, a de facto national CERT, recognized both domestically and internationally, but without an official mandate from the state. This implied, among other things, the necessity to secure funding from NASK's own resources or from European grants, and to a lesser

extent from national grants. We could not afford larger investments, but we managed to invest in what was most important – in people.

A key aspect during this period was making decisions regarding the direction of the team's development, which was by no means obvious at that time.

From your perspective, which decisions, changes, or achievements were crucial?

Above all, it involved making decisions regarding specialization, independence, and the development of our own tools. Realizing that with just over a dozen people in CERT we could not be equally proficient in all aspects of national-scale incident response, we focused on areas where we could achieve the greatest impact. These included the development and distribution of threat intelligence feeds within the country, enhancing situational awareness of national-level events, developing independent malware analysis and threat detection systems, and actively disrupting and counteracting botnets (including through sinkholing).

A key initiative that significantly changed the cybersecurity landscape in Poland was the establishment of a process for suspending and taking over .pl domains (so-called sinkholing) that were used to manage botnets or distribute malware – including the then well-known Virut botnet. Thanks to this, we quickly "cleaned" the .pl domain of such threats, earning recognition internationally as well. This, in turn, led to numerous further collaborations in this area on an international scale, and publications in English helped enhance the team's positive reputation.

We succeeded in creating a positive atmosphere within the team, which has endured for years and attracted people who wanted to make a difference for the greater good. An incentive for many was the freedom to choose the areas they wanted to focus on, personal development through participation in CTF competitions (with numerous successes), and international conferences, which also provided opportunities to establish contacts with specialists from other countries.

The result of our various initiatives are systems that continue to operate to this day, such as ARAKIS, n6, BotSense, and MWDB, and the team remains known worldwide for its own (innovative) solutions.

What do you consider to be the greatest cybersecurity challenges over the next 5 years? Particularly in the context of the role CERT Polska may play.

There are a number of challenges, but I will focus on the one most closely related to effective national-scale incident response, in situations where the emergence of a new vulnerability enabling remote code execution in a popular product automatically leads to attacks.

Today it is said that "cybersecurity is national security." Every device connected to a network can become a target not only of cybercriminals but also of attacks backed by other states. And this is already happening. Every newly discovered vulnerability that allows remote code execution on a susceptible device – whether it is a corporate

or home router, a firewall, VPN, PLC, or a file-sharing system, etc. – is immediately exploited by both cybercriminals and hostile states.

In order to protect the state, it is crucial to understand the current attack surface of Poland's network infrastructure, which can change from day to day, or even hour to hour. It is also necessary to develop an efficient system to react as quickly as possible to new vulnerabilities and attacks, in cooperation with partners across the country, largely leveraging automation (and, to some extent, AI where feasible).

There is still much to be done in this area in Poland (as recent attacks on the energy sector have shown). CERT Polska is well positioned to play a leading role in this field.

Przemysław Jaroszewski

HEAD OF CERT POLSKA FROM 2016 TO 2021

How did the cybersecurity landscape in Poland look when you assumed the position of Head of CERT Polska? What types of threats were dominant?

For all internet users, the defining moment was undoubtedly the beginning of the COVID-19 pandemic. It forced a rapid acceleration of digitalization of services, both in the public and private sectors. Unfortunately, this trend was immediately exploited by criminals, who multiplied fraud scenarios – from fake online stores to websites impersonating government institutions or social organizations.

This period also marked the beginning of intensive discussions on the threat of information warfare and combating disinformation online.

What were the greatest challenges during your tenure as team leader?

This period coincided with the implementation of the National Cybersecurity System Act. It was the first regulation of such comprehensive scope concerning the duties and responsibilities of entities critical to the state and its citizens. The greatest challenge was building the trust of the companies and institutions covered by the Act toward the national CSIRTs, which collect a wide range of sensitive information about infrastructure while at the same time supporting their constituency in incident response and resilience building.

From your perspective, which decisions, changes, or achievements were crucial?

Certainly, the entry into force of the aforementioned National Cybersecurity System Act was crucial, as it triggered a number of organizational changes within NASK and also redefined the role of the CERT

Polska team. From that moment on, the team gained legally defined responsibilities and tools to combat cyber threats for the first time.

What do you consider to be the greatest cybersecurity challenges over the next 5 years? Particularly in the context of the role CERT Polska may play.
I believe that the greatest challenge will remain building and maintaining trust in state institutions and in public-private partnerships. The role of entities such as sectoral CSIRTs is particularly important here, as they should operate by directly involving the regulated organizations within their structures.

Sebastian Kondraszuk

HEAD OF CERT POLSKA FROM 2021 TO 2024

How did the cybersecurity landscape in Poland look when you assumed the position of Head of CERT Polska? What types of threats were dominant?
The years 2021–2024 were a period of very rapid growth in reports of online fraud. I consider it extremely important that we did not remain passive observers of these events. During this time, many methods for detecting threats were tested, supporting the very early identification of infrastructure involved in fraudulent activities. Some of these ideas were successfully translated into internal projects aimed at improving the quality of domain registration in the .pl domain managed by NASK – PIB. The Warning List, which we launched in 2020, has become a key link in the chain of protecting internet users from online fraud. It is worth remembering this when nearly 700 domains are added to the List every day!

What were the greatest challenges during your tenure as team leader?
The strength of CERT Polska has always been the people who make up the team. However, operating within a constantly expanding scope of activities, combined with the rapid growth in incoming reports, we faced the challenge of ensuring both the inflow and retention of the human resources we needed. Due to the limited ability to compete with the commercial market, we placed even greater emphasis on developing internal capabilities. It will come as no surprise that, for the people working at CERT Polska, the opportunity to carry out projects that contribute to Poland's development has always been, and remains, just as important as remuneration. I believe that as long as we maintain these two pillars, we will continue to attract the best experts in the country.

The second area I saw as a challenge was the constantly increasing volume of incoming reports and their uneven distribution, especially given the need to maintain priorities that went far beyond online fraud.

A good test of our capabilities was an advertisement encouraging submissions to CERT Polska broadcast during the World Cup football match Poland – Argentina. That day, we recorded a record daily number of reports. Today, thanks largely to advanced automation, sudden and significant surges in reports are a situation we manage very well.

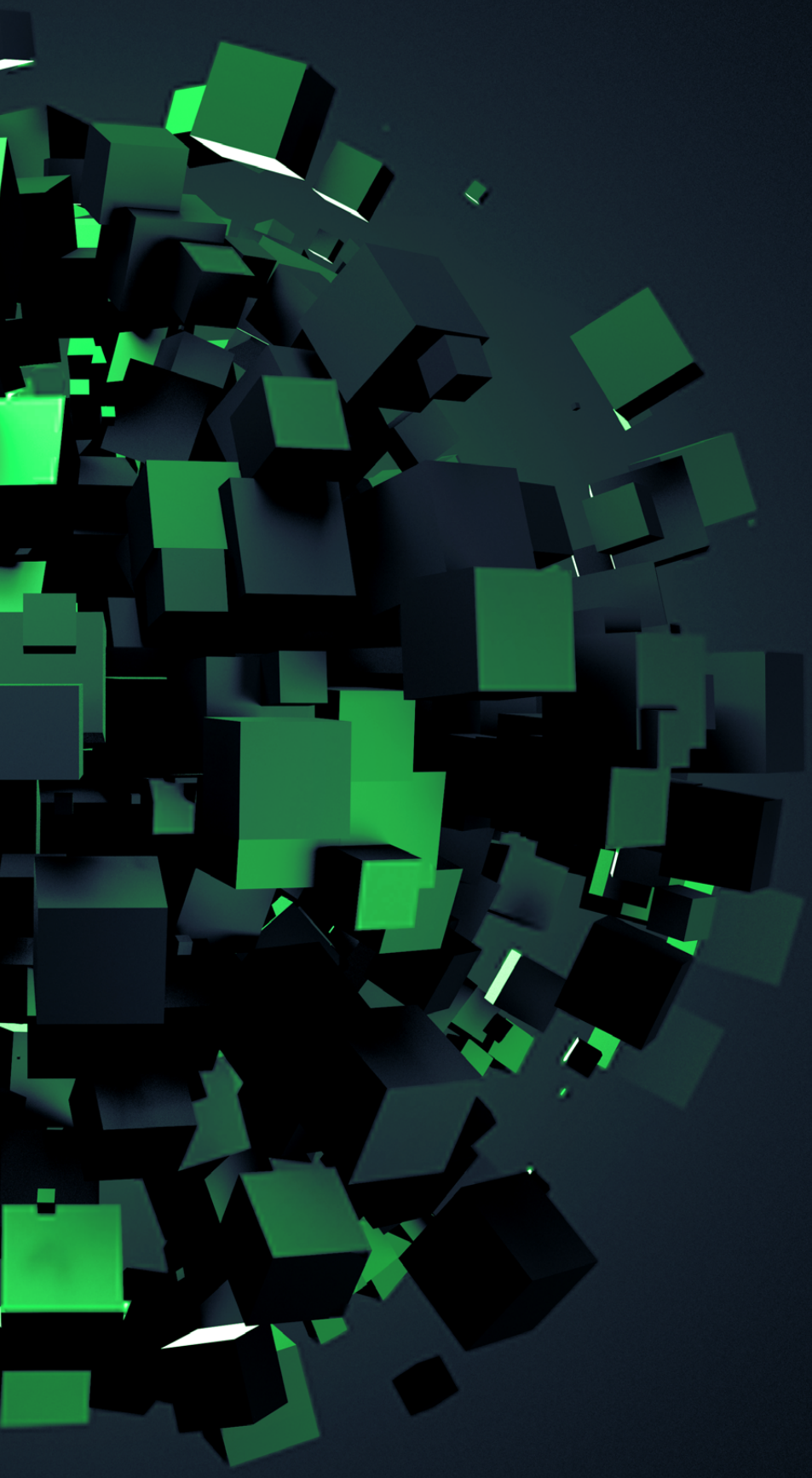
From your perspective, which decisions, changes, or achievements were crucial?

In the field of combating online fraud, a major success has been the development of solutions that are both effective and acceptable to the parties involved, and their subsequent practical implementation. The Act on Combating Abuse in Electronic Communications is a perfect example of how coordinated information exchange between market participants can raise the level of security. I extend my recognition to all former and current CERT Polska operators for their contributions to making critical decisions that protected users' data and money. I also wish to equally acknowledge the professionalisation of the field of digital forensics. Insights drawn from the analysis of the most serious incidents in the country have contributed to the development of competencies and tools that often allow us to fully understand the course of an attack. Moreover, we successfully use this experience to support national law enforcement authorities.

What do you consider to be the greatest cybersecurity challenges over the next 5 years? Particularly in the context of the role CERT Polska may play.

In my opinion, we will continue to observe a shortening of the lifecycle of schemes used by criminals. CERT Polska has played, and will continue to play, a significant role in identifying and documenting them. A key challenge will certainly be reaching internet users as quickly as possible with information that will help them make informed decisions. As a second very important objective, I see the continued growth in awareness among participants of the cybersecurity system, as well as a greater recognition of the benefits of active participation in it. These entities will, to a large extent, fall within the responsibility of CSIRT NASK. I believe that we will continue to be one of the leading players on the map of cybersecurity in Poland, with a broad and, above all, practical offering.

Incidents and threats



Overview of new campaigns

The threat landscape in Polish cyberspace is constantly evolving. Criminals systematically refine their methods, and their campaigns are becoming increasingly difficult to distinguish from legitimate communication. Among established attack patterns, phishing campaigns aimed at stealing passwords to e-mail accounts and social media services remain dominant. Fake websites impersonating government services and courier service providers also continue to show high levels of activity, particularly those posing as Poczta Polska and InPost.

In the following section, we present an overview of the most common campaigns observed in 2025, along with a description of the techniques used by fraudsters and the potential consequences for users.

Tax refund – e-Tax Office and KAS

One of the most common phishing scenarios remains the promise of a tax refund. Criminals exploit the image of the Ministry of Finance, sending emails about a supposed refund awaiting approval. These messages are characterized by a professional appearance that mimics official correspondence from government institutions, which increases their credibility. The messages contain a link to a fake website imitating a government portal. Under the pretext of finalizing the refund procedure, the site attempts to obtain online banking login credentials and payment card details. The intercepted data enables perpetrators to take over victims' bank accounts and carry out transactions on their behalf.

FIGURE 1. Fake message informing about a tax refund

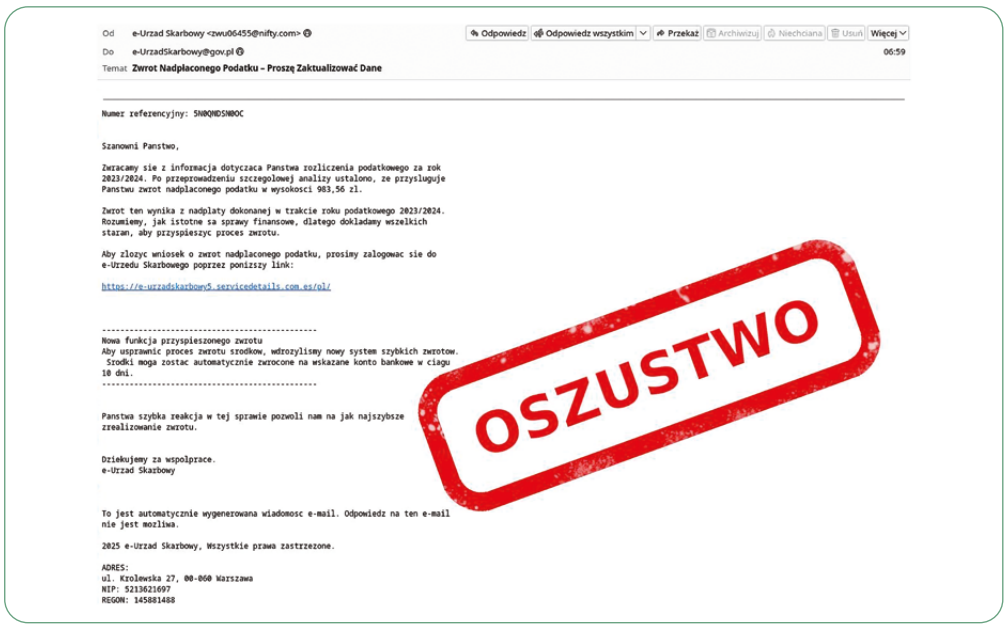


FIGURE 2. Example of a tax refund scam

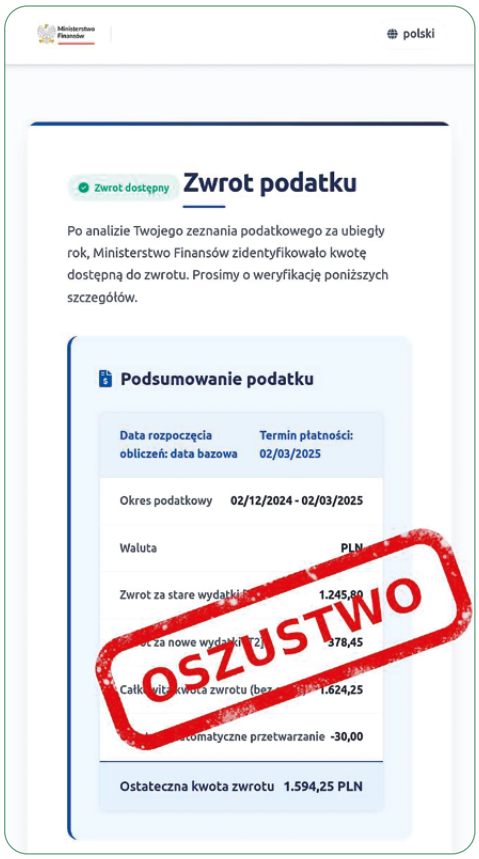
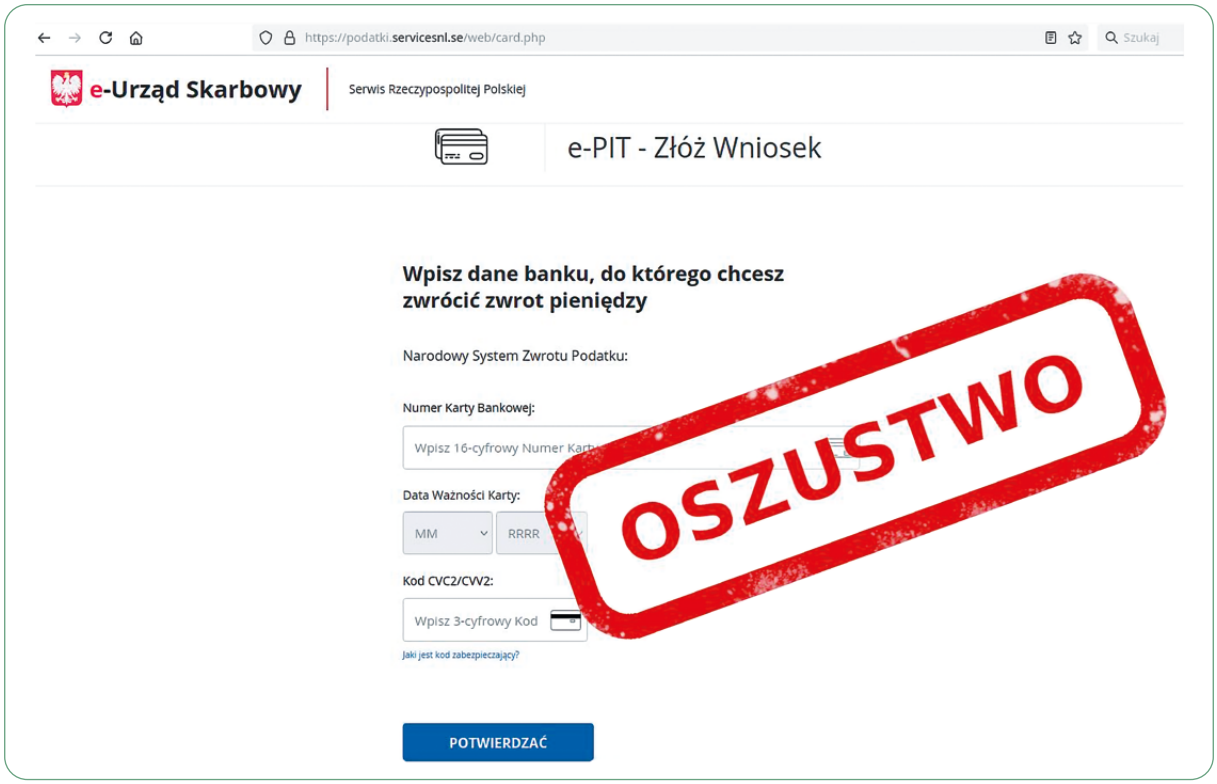


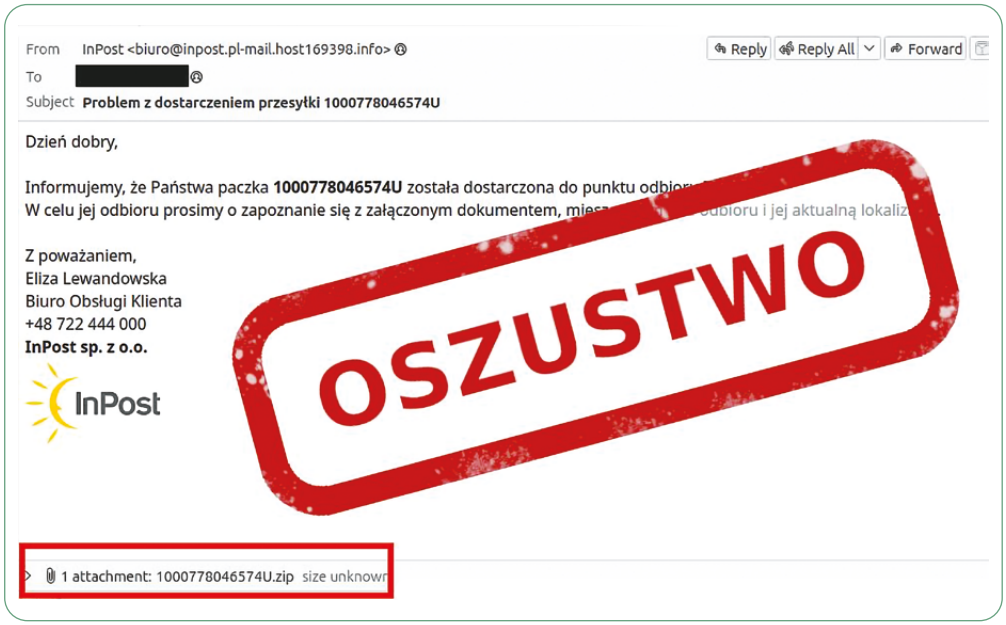
FIGURE 3. Fake website used to steal payment card details



Undelivered parcels – InPost, Poczta Polska, e-Delivery

The popularity of online shopping makes messages related to courier shipments an effective lure used by cybercriminals. They particularly often impersonate InPost. In fraudulent e-mails, they claim there are issues with the delivery of a parcel and encourage the recipient to download and open an attachment. The attachment contains a malicious script which, once executed, installs malware on the victim's device. This malware enables the theft of e-mail account passwords and additionally uses the computing power of the infected device to mine cryptocurrencies (so-called cryptojacking).

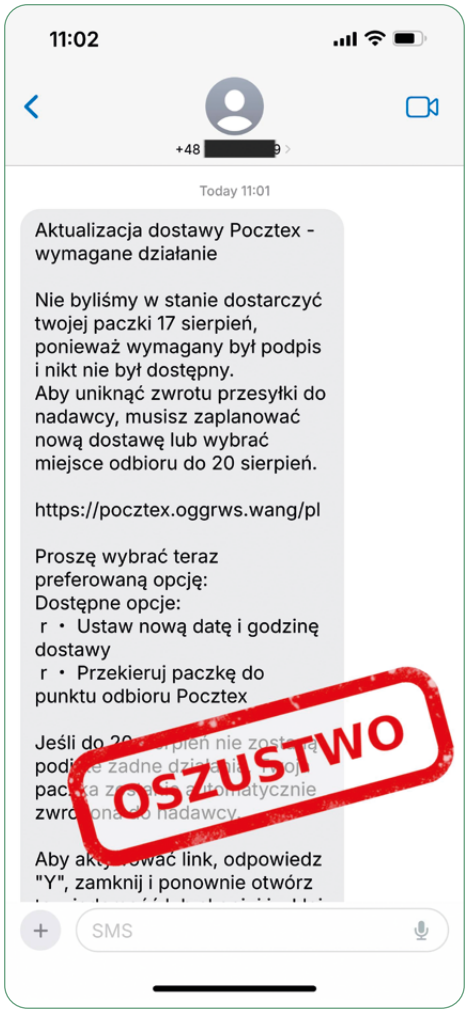
FIGURE 4. Fake message informing the recipient about a delivery issue



In addition to e-mail, criminals also use SMS. Fraudulent text messages inform recipients about fictitious delivery problems and redirect them to phishing websites imitating popular courier companies to steal personal data and payment card information.

A particularly interesting variant of this campaign bypasses built-in mobile phone protections against opening links from unknown senders. Encouraging the recipient to reply to the message activates the embedded link and facilitates access to the phishing site. This demonstrates how criminals adapt their methods in response to newly introduced security mechanisms.

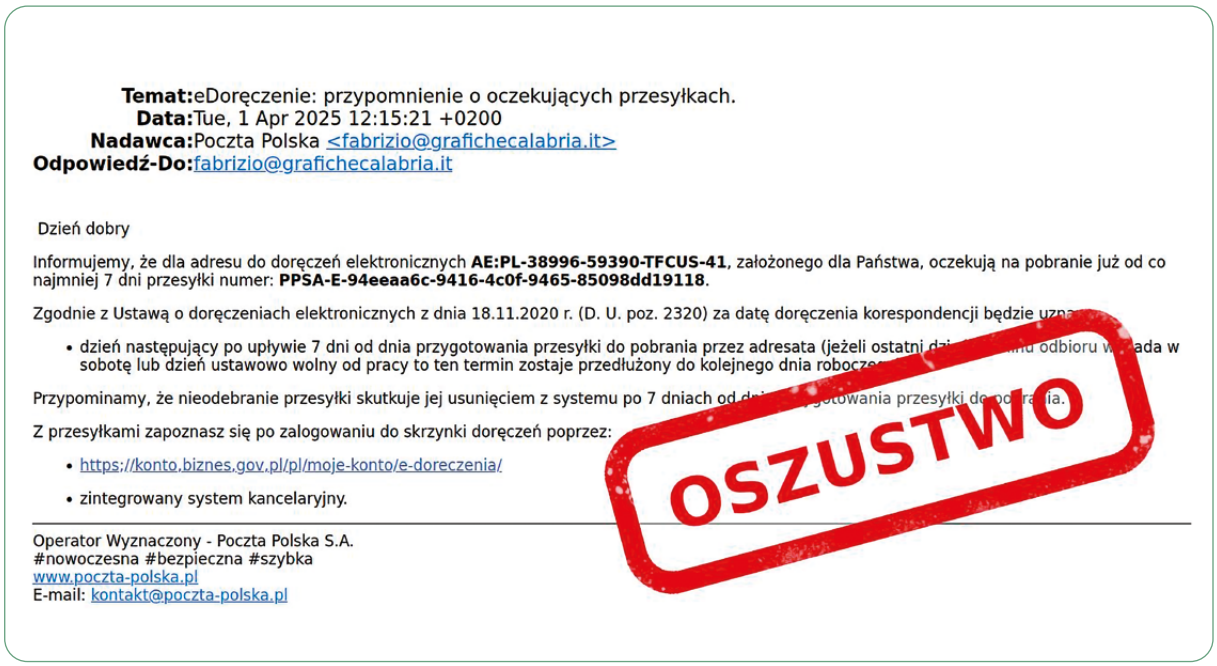
FIGURE 5. Example of a fake SMS message in which fraudsters encourage the user to reply



With the growing popularity of digital public administration services, campaigns impersonating the e-Doręczenia (e-Delivery) system have also emerged. Fraudulent e-mails inform recipients about an undelivered official correspondence and include a warning that it will be deleted if no action is taken within a specified time.

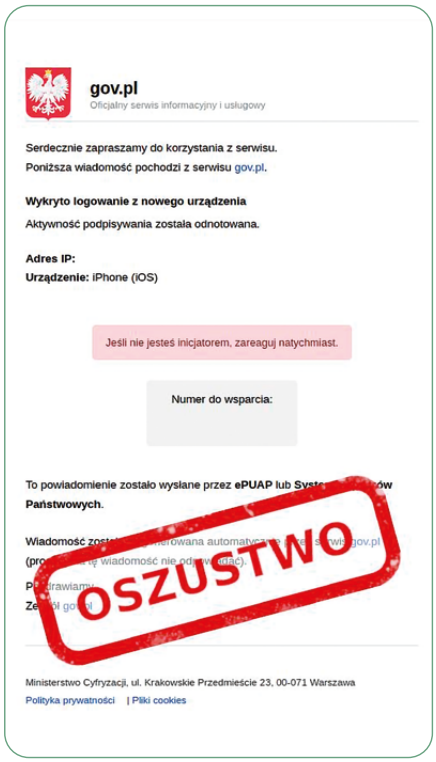
These messages contain a link to a website imitating the biznes.gov.pl portal, where e-mail login credentials are harvested. The campaign exploits a sense of urgency – the threat of document deletion is intended to prompt immediate action without verifying whether the message is legitimate.

FIGURE 6. Fake message with a link to a website used to steal e-mail login credentials



Official matters – services in the gov.pl domain

Government services in the gov.pl domain enjoy a high level of public trust, which is why criminals often exploit their image in phishing campaigns. The distributed messages appear in several variants: notifications about pending official correspondence, detected activity on a user account, or a session registered on an unknown mobile device.



A common element across all variants is an attempt to persuade the recipient to make a phone call to a specified number. During the call, the perpetrators use various manipulation techniques to convince the victim to install software that enables remote access to their computer.

Taking control of the device allows attackers to perform bank transfers from the victim's account, leading to the loss of funds.

FIGURE 7. Fake message informing about a new session on an unknown mobile device

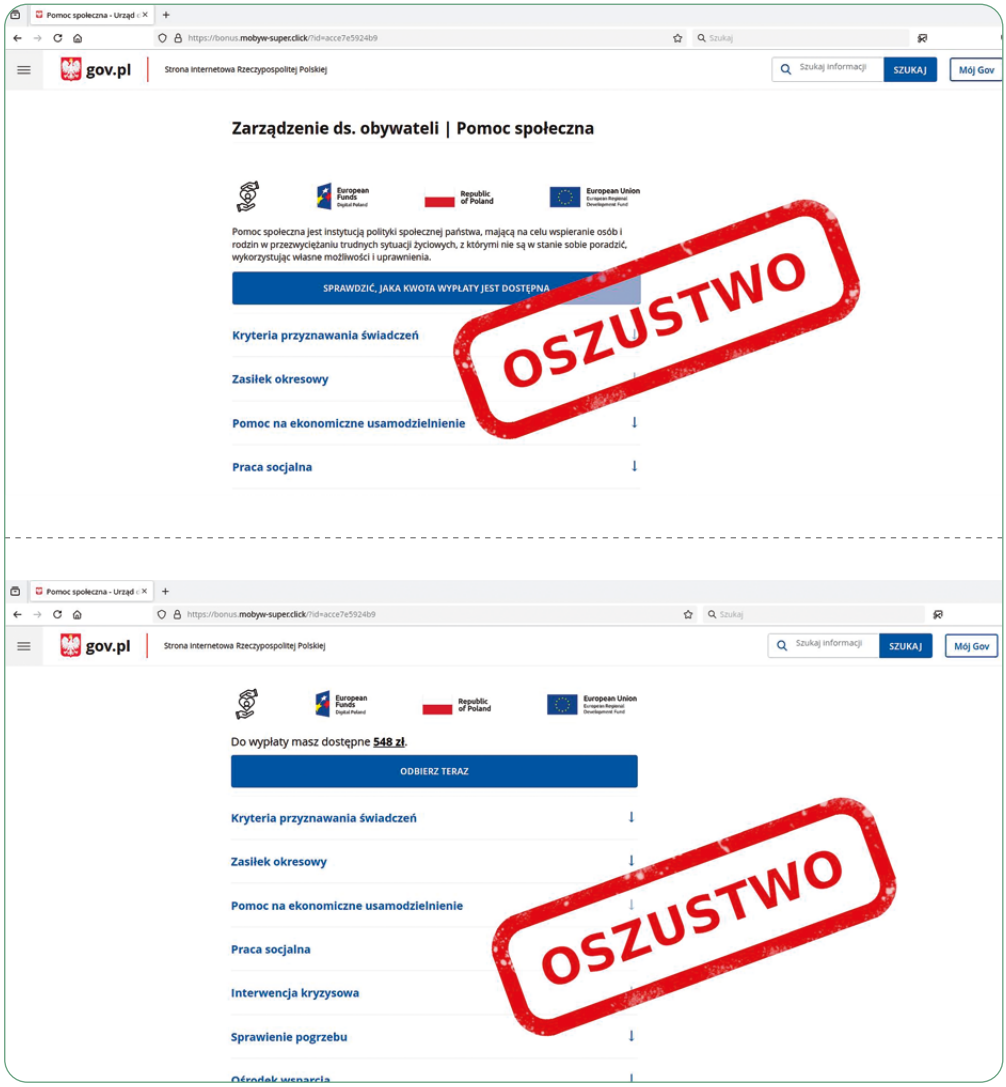
FIGURE 8. Fake message in which fraudsters encourage the user to synchronize their e-mail inbox

Verification of eligibility for social benefits

The promise of easy access to social benefits is another effective fraud scenario. Fraudulent advertisements are spread on social media, offering users the possibility to check their eligibility for additional payments. These ads redirect users to websites imitating the gov.pl portal, where the only required step is entering a PESEL number.

After entering the PESEL number, the user is redirected to a page impersonating the payment operator Przelewy24, which contains fake online banking login forms. The intercepted credentials allow attackers to access victims' bank accounts and steal funds.

FIGURE 9. Fake website impersonating the gov.pl portal, allegedly allowing users to check their eligibility for social benefits



e-TOLL fee

Fraudulent messages related to the e-TOLL system find a receptive audience among drivers. The messages inform recipients about an alleged unpaid road toll and include a link to a website imitating the official service.

The website uses a two-step data harvesting mechanism. The first form is used to collect the victim's personal data, including their ID card number. The second captures payment card details, including the CVV/CVC code. The obtained information enables perpetrators to steal money from the victim's account.

FIGURE 10. Fake notification about an unpaid road toll

Statistical Office

Criminals also exploit the name of the Statistical Office in Warsaw. The distributed e-mails inform recipients about a fictitious obligation to complete documentation and include a malicious attachment.

The credibility of these messages is reinforced by their professional structure, including a detailed footer that resembles official correspondence from a public institution. The attachment contains RAT (Remote Access Trojan – trojan enabling remote access), which, once executed, allows perpetrators to take control of the victim's computer. The malicious software steals saved passwords and other sensitive data stored on the infected device.

FIGURE 11. E-mail containing a malicious attachment – an example of impersonation of the Statistical Office in Warsaw

Fake investments – social media advertisements

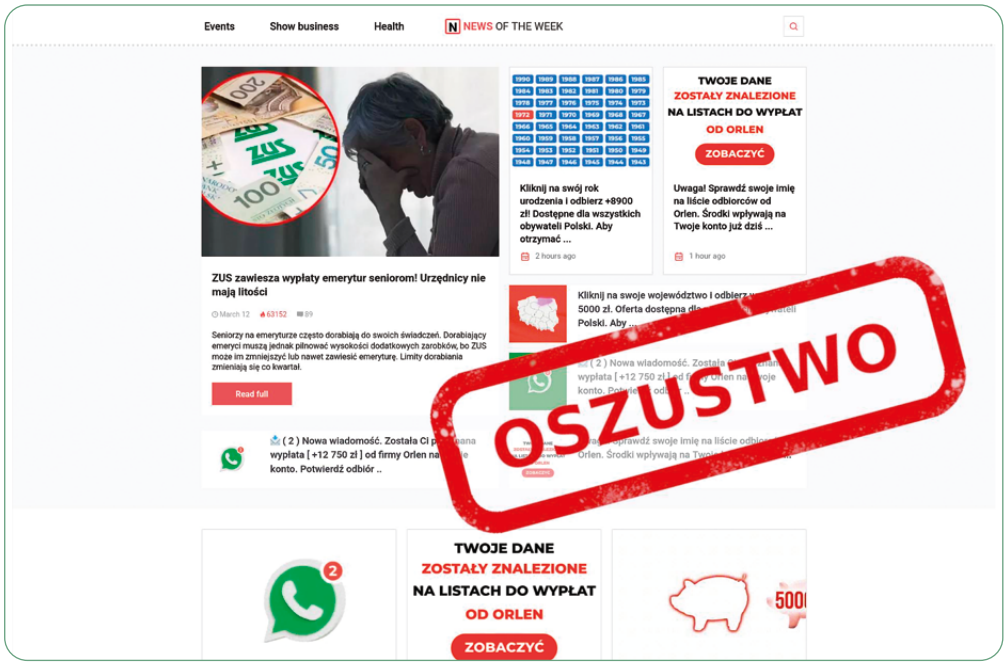
Investment scams are among the most financially harmful threats in the Polish cyberspace. Perpetrators mass-register websites offering fictitious investment programs and trading platforms, often using the likeness of public figures as fake endorsements.

The scam mechanism relies on psychological manipulation. After making a payment, the victim is shown falsified charts indicating a supposed increase in the value of the invested funds. The simulation of profits aims to build trust and encourage the user to make further payments. Attempting to withdraw funds reveals the true nature of the scheme – the accumulated money is taken by the perpetrators.

A typical element of such campaigns is creating a sense of urgency and presenting the prospect of above-average returns with minimal risk.

FIGURE 12. Fake investment platform impersonating Baltic Pipe

FIGURE 13. Fake investment platform impersonating Orlen



NFZ – reimbursement for the purchase of medicines

The healthcare sector is not immune to cybercriminal activity. Messages impersonating the National Health Fund (NFZ) inform recipients about the possibility of obtaining reimbursement for purchased medications and direct them to a fraudulent website designed to steal personal data and passwords.

Perpetrators also use a sense of urgency – the messages indicate a short deadline to claim the funds, limiting the time for verifying the authenticity of the message and prompting users to react without careful consideration.

FIGURE 14. Fraud exploiting reimbursement for medication purchases

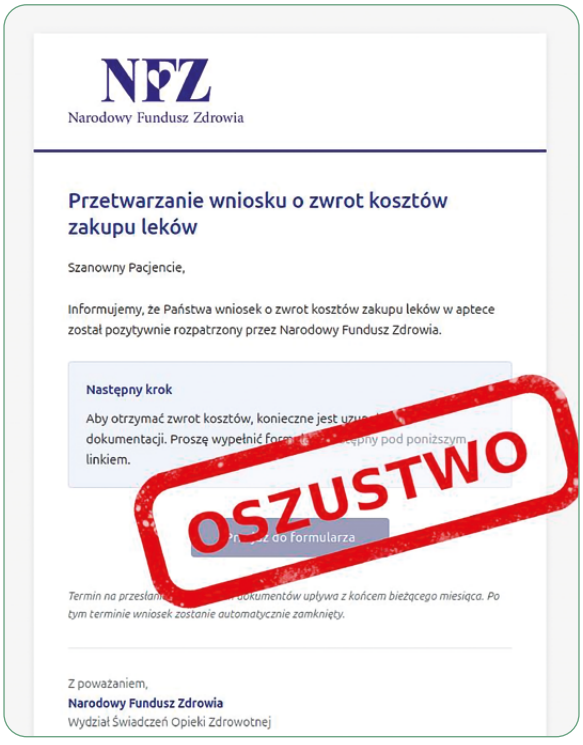
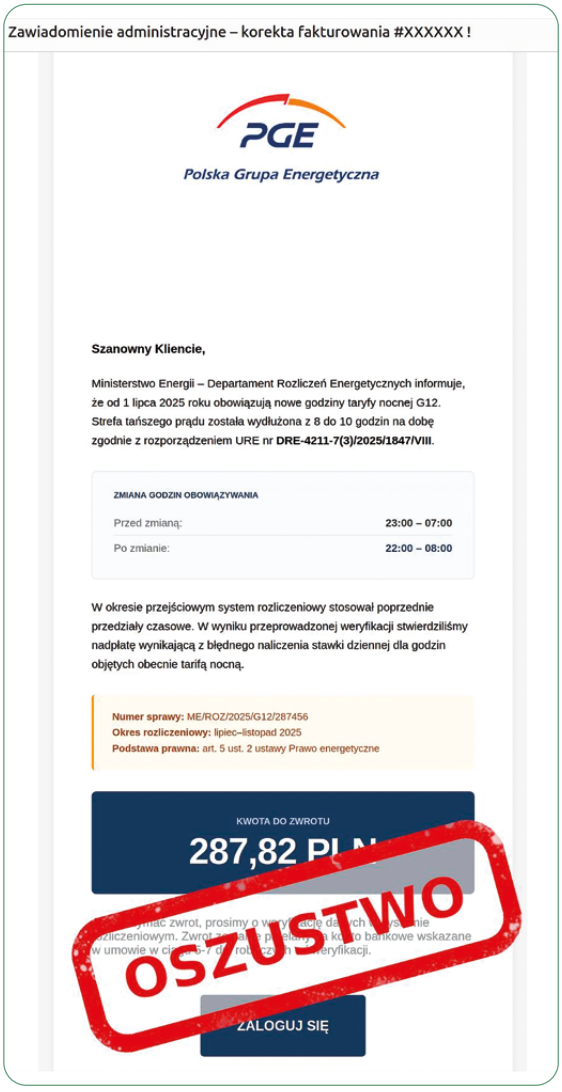


FIGURE 15. Fake notification of funds granted by NFZ

FIGURE 16. Fake e-mail informing about a supposed electricity overpayment and reimbursement



Electricity overpayment reimbursement

In the context of rising energy prices, campaigns promising reimbursement of electricity overpayments prove particularly effective. Cybercriminals impersonate electricity providers and cite fictitious changes in legal regulations. The messages direct recipients to fake websites designed to steal payment card information.

The campaigns are highly professional. Messages are written in correct Polish with a formal correspondence style, and phishing websites closely replicate the visual design of official energy provider sites. The careful execution of materials makes it difficult to recognize the threat. The most important clue remains the website address, which may resemble the original but differs in at least a small detail.

Summary

The analysis of the presented phishing campaigns allows for the identification of common characteristics of contemporary threats in the Polish cyberspace, the vast majority of which are phishing attacks. Cybercriminals consistently impersonate trusted institutions – both governmental and private – professionally

imitating their official correspondence. The employed psychological manipulation techniques, especially creating a sense of urgency, as well as promises of financial gain, effectively prompt victims to act without proper verification.

The observed trend indicates a systematic increase in the sophistication of attacks. Phishing materials are characterized by increasingly high quality – correct language, faithful copies of original interfaces, and carefully structured messages. Perpetrators flexibly adapt their fraud scenarios to current events, seasonal trends, and legislative changes, which further enhances the effectiveness of the campaigns.

Mobile malware

In this chapter, we present statistics on malware for Android mobile devices observed and detected by the CERT Polska team in 2025. The analysed samples originate from threat-hunting activities, user reports, and the MWDB platform.

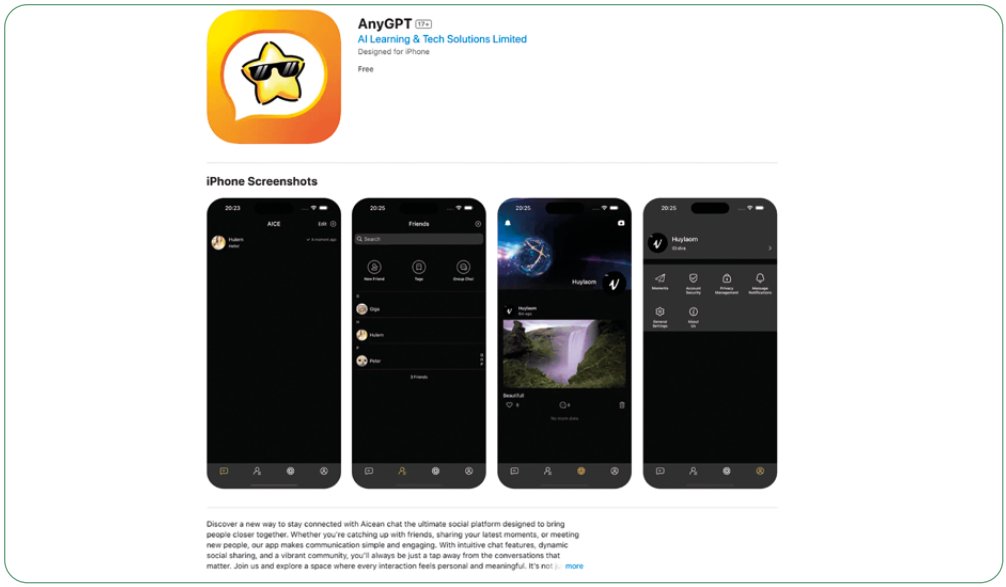
In 2025, we reported a total of 393 samples of malicious software targeting mobile devices to Google, as well as 119 applications impersonating well-known Polish companies. These applications were distributed through the Google Play Store and were removed from the store following our reports. Other malicious applications were hosted on external websites, and the number of unique samples targeting Polish users that we observed amounted to 181.

Overview of selected mobile malware campaigns in 2025

Spark cat

Cybercriminals used malicious code leveraging a special framework based on OCR (Optical Character Recognition) technology. This allowed the applications to analyse images stored on the victim's device and extract sensitive information from them, such as passwords or cryptocurrency wallet recovery phrases. The cybercriminals focused primarily on stealing cryptocurrencies, like Bitcoin, although the malware could also capture other confidential data. The applications were distributed through both the App Store and Google Play Store.

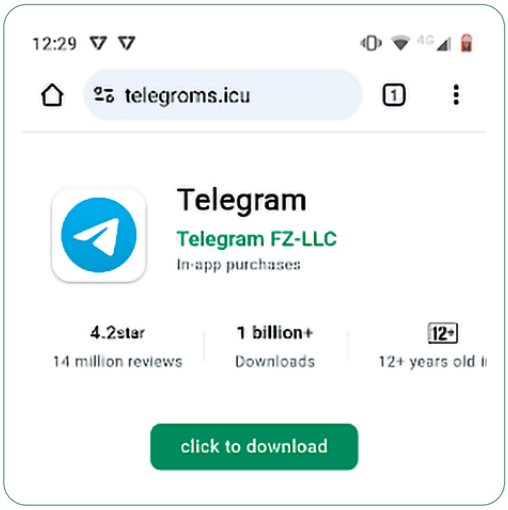
FIGURE 17. Screenshot from the App Store of a malicious application from the Spark Cat family



SpyMax

The SpyMax malware campaign we observed targeted users of the Telegram application. Malicious applications were distributed via a website impersonating the Google Play Store. Once executed, the malware installs itself on the device as a legitimate-looking Telegram app. SpyMax includes typical RAT functionalities, including a keylogger and the exfiltration of sensitive information from infected devices.

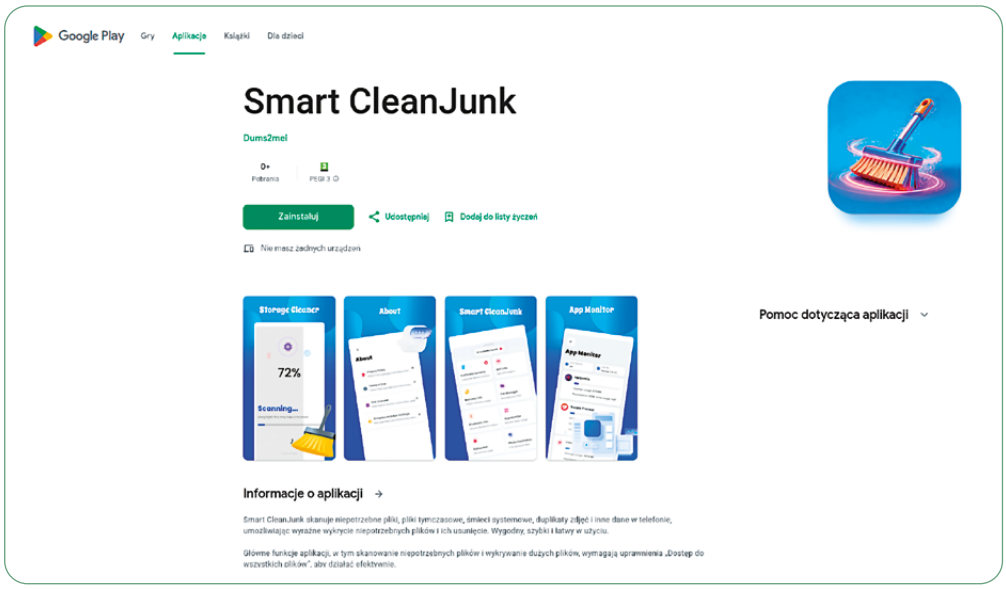
FIGURE 18. Screenshot from Google Play Store of a SpyMax malicious application



Joker

We covered the Joker malware campaign in more detail in 2024 in the article “The Dark Knight Returns: Analysis of the Joker Malware” (https://cert.pl/en/posts/2024/10/analiza-joker/). In 2025, we detected an additional 352 samples, which were analysed by our team and reported directly to Google. All samples were subsequently removed from the Google Play Store.

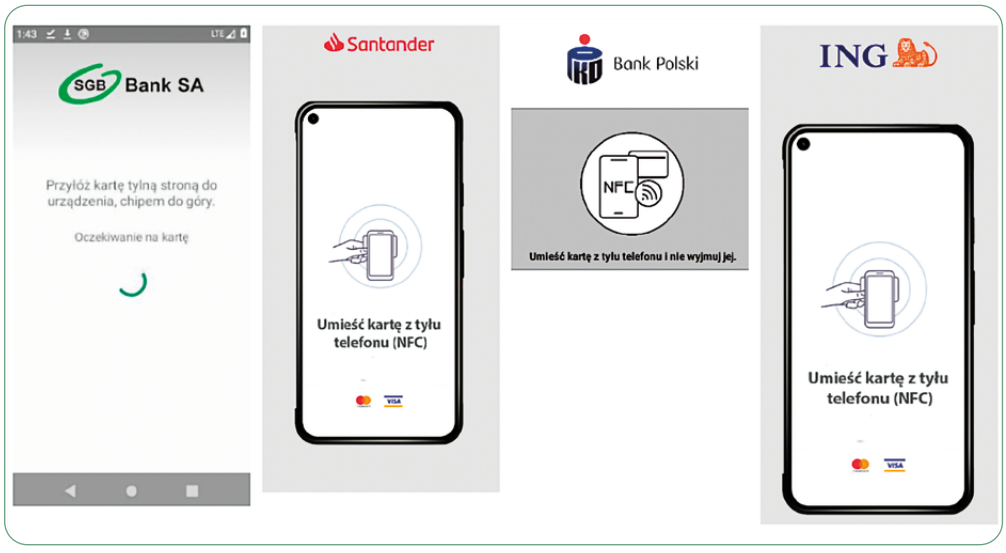
FIGURE 19. Screenshot from Google Play Store of a Joker malicious application



NGate

The most dangerous mobile malware campaign we observed in 2025 targeting Polish users was the NGate campaign. The attack aims to enable unauthorized cash withdrawals from ATMs using victims' payment cards. Criminals do not physically steal the card. Instead, they relay the card's NFC traffic from the victim's phone to a device controlled by the attacker at the ATM. More information about this threat is available in our article "Analysis of the NGate (NFC relay) malware campaign" (https://cert.pl/en/posts/2025/11/analiza-ngate/).

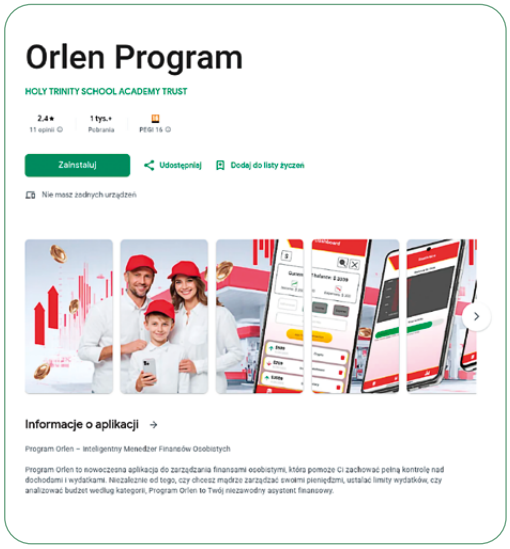
FIGURE 20. Screenshots from NGate app



Apps impersonating well-known Polish companies on Google Play Store

In 2025, we observed an increase in the number of applications on Google Play Store impersonating well-known Polish energy and fuel companies, corporations, and institutions. We reported 119 such applications, with Orlen being the most frequently targeted brand. These applications are primarily designed to attempt financial fraud through fake investment schemes. In the current modus operandi, these apps are usually advertised via other applications already installed on the potential victim's device, containing a link to Google Play Store. Both the advertisement and the application itself leverage the branding of another well-known and recognizable company.

FIGURE 21. Screenshot from Google Play Store of an application impersonating Orlen

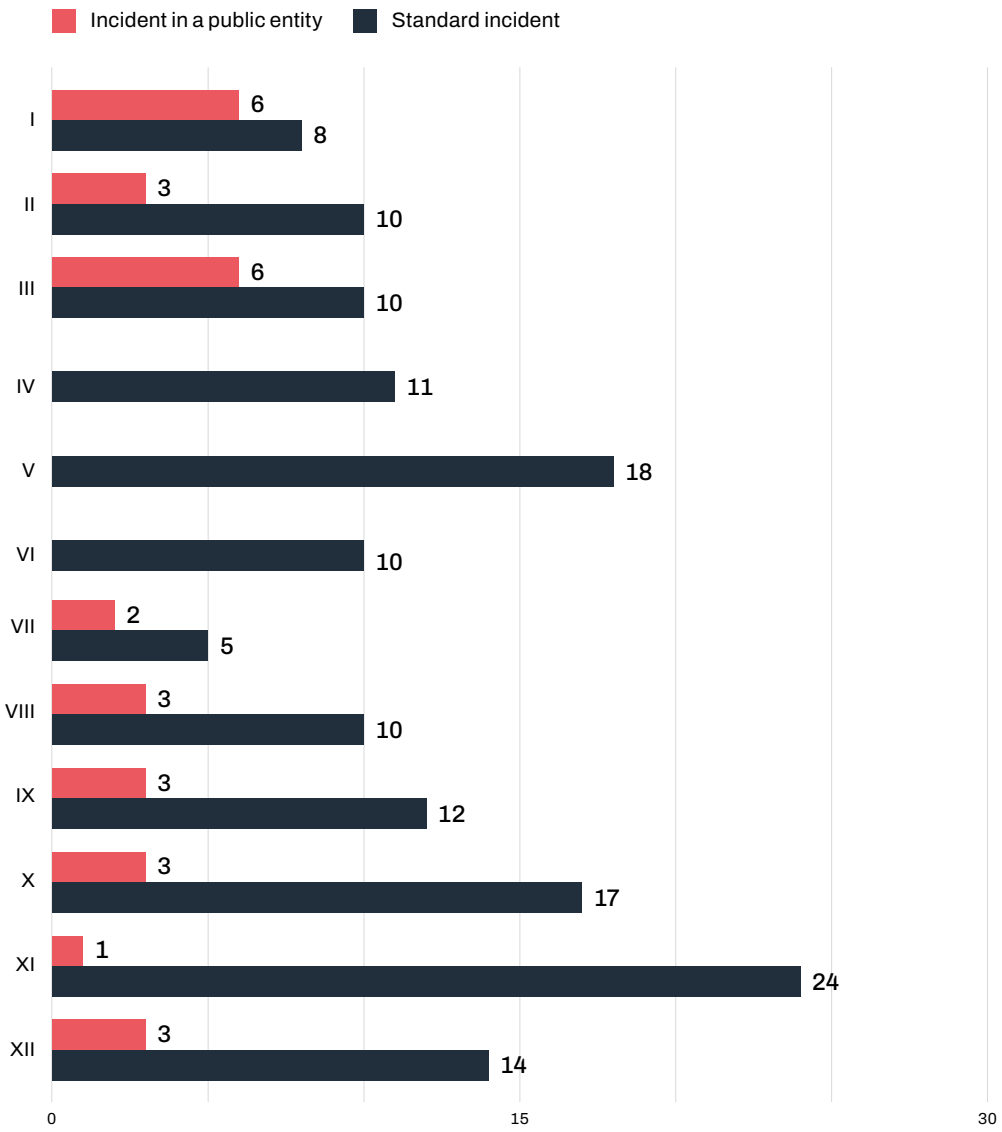


Ransomware

The year 2025 brought another record in the number of incidents related to ransomware attacks. These incidents continue to pose a threat with the most destructive and severe impact on organizational operations. Ransomware attacks observed by our team are most often targeted at commercial entities and public institutions. The attackers are financially motivated criminal groups aiming to encrypt as many IT systems of the targeted organization as possible, primarily focusing on data critical for business continuity. Customarily, during these attacks, ransomware operators also attempt to destroy backup copies, then demand a ransom from the victims in exchange for a decryption key that would allow recovery of the data affected by the attack. Many groups also use the double extortion technique – 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 or selling it on the dark web.

In 2025, CERT Polska recorded 179 ransomware attacks, a significant increase compared to 2024 (147 incidents), surpassing even the previous record from 2023 (161 incidents). In 2025, most reports came from private entities (129), 30 incidents were reported by public institutions, and 20 reports came from individuals. Among incidents reported by public entities, half (15 incidents) involved local government administration. The second most frequently affected sector was education (including higher education institutions). None of the registered incidents met the thresholds to be classified as a major incident under the National Cybersecurity System Act.

CHART 1. Number of ransomware attacks by month and entity type



Major threats

Despite the high diversity of threats related to ransomware, similar to previous years, a few families were observed particularly frequently.

TABLE 1. Number of incidents recorded, broken down into the most frequently observed ransomware families

Ransomware families	Number of incidents recorded
Qilin	13
Proxima	8

Ransomware families	Number of incidents recorded
Makop	8
LockBit	8
Beast	7
RansomHub	6
Unknown	46*

* In 33 cases, we had no information allowing us to attempt identification of the ransomware used.

Qilin

Ransomware from the Qilin family is distributed as Ransomware-as-a-Service (RaaS) – attacks are carried out by affiliates who use the malicious code and infrastructure provided by the ransomware creators in exchange for a share of the ransom obtained from the victim. The Qilin group filled a gap in the RaaS market left by effective law enforcement actions against the largest ransomware groups (operations Cronos[1] and Endgame[2]), which led to the dismantling or disbanding of major criminal groups operating in this area. In 2025, we recorded 13 attacks involving ransomware from this family. These attacks were mainly targeted at medium and large enterprises. In nearly half of the cases, the suspected attack vector was compromised VPN credentials allowing remote access to the victim's infrastructure. The Qilin group operates a so-called leak site, a blog where it publishes information about attacked entities and stolen materials. However, information about most incidents reported to us was not posted on the group's blog. It should also be noted that not every published report of an attack results in the disclosure of stolen materials. At the same time, the group sometimes does not publish sample files, even though post-incident analysis confirmed that data had been transferred out of the victim's infrastructure.

LockBit

In 2025, the CERT Polska team recorded 8 attacks involving ransomware from the LockBit family, which, like Qilin, operates under the RaaS model. In recent years, the LockBit group has remained a leader in terms of activity and the number of targeted entities; however, thanks to law enforcement actions in 2024, the scale of its operations was significantly reduced.

1 https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

2 https://www.europol.europa.eu/operations-services-and-innovation/operations/operation-endgame

In May 2025, the group's website was attacked and altered. At that time, a database was published containing, among other things, cryptocurrency wallets used by the group's clients and records of conversations with victims. The group, however, remains active – in September 2025, it announced the release of a new ransomware version labelled LockBit 5.0. It should be noted that due to the leak of some tools used to build executable files for LockBit 3.0, not all attacks using this ransomware family are carried out by operators affiliated with its original creators. In 2025, the LockBit group published on its blog only one attack affecting a Polish entity.

Beast

Beast is another ransomware family operating under the RaaS model. In 2025, the CERT Polska team recorded 7 incidents involving attacks using this malware. In 3 confirmed cases, the attack vector was the Remote Desktop Protocol (RDP) service, while in one case the vector could not be confirmed; however, the targeted entity did provide such a service. The group maintains a so-called leak site, but in 2025 it did not publish any information regarding attacks on Polish entities.

Makop i Proxima

Makop is a ransomware variant derived from the Phobos malware, operating under the RaaS model and active since 2020. In 2025, 8 incidents were attributed to this family. Proxima ransomware (also known as BlackShadow) was active in the first quarter of 2025, during which all 8 incidents were recorded, with 5 occurring in February. In most reported incidents related to these ransomware families, no information was available to determine the attack vector (nor was it identified by the reporting entity). In the case of Proxima, we observed that in 5 cases the targeted entity provided remote access to the affected computers via the RDP service.

Observations on ransomware threats

Unsafe remote access services

In the vast majority of incidents – cases where the targeted entities maintained logs sufficient to determine the attack vector – unauthorized access occurred via remote access services that were not protected with two-factor authentication. Attackers can obtain credentials in various ways, including phishing, leaks from external services, or activity of stealer-type malware. They may also guess passwords through brute-force attacks. Unfortunately, for many incidents reported to our team, determining the attack vector was impossible. It is particularly noteworthy that in 46 ransomware

incidents reported to CERT Polska, the targeted entity had a publicly accessible Remote Desktop Protocol (RDP) service. This number is likely underestimated, as many reports did not include information about the infrastructure and remote access methods of the attacked entity. In two incidents reported to our team, password compromise and ransomware infection occurred within less than two weeks of exposing the RDP service to the Internet. This underscores how critical it is to implement two-factor authentication on all services enabling remote access to infrastructure.

Attacks

A major challenge in analysing ransomware incidents remains insufficient log retention, especially from edge devices and the Active Directory domain controller. Many reports came from entities without a central log collector, meaning logs cover only a few days retrospectively. In many cases, logs from incidents analysed by our team clearly indicated that the infiltration of the attacked entity's infrastructure was carried out by the ransomware operator rather than fully automatically. Such attacks were often spread over time (even several weeks) with priorities including not only obtaining the highest possible privileges but also locating backup servers and hypervisors. For backups stored on NAS servers, attackers typically did not encrypt files; instead, they reinitialized the storage space, aiming to erase the data. For compromised hypervisors, attackers usually encrypted virtual machine files, deleted snapshots, and sometimes changed administrative account passwords. Ransomware operators very often used legitimate tools and programs built into the operating system ("living off the land"), and malicious software was deployed only after disabling security mechanisms.

Difficulties in identifying the attacker

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. Meanwhile, in 2025, as in 2024, in many cases identifying the ransomware family used proved to be a major challenge. Due to pressure from law enforcement, some criminal groups refrain from publicizing their activities in order to avoid drawing attention from cybersecurity entities and institutions. These attackers do not include characteristic elements in the ransom notes they leave, do not sign them, and often do not maintain publicly accessible blogs where they would publish information about new victims. The situation is further complicated by leaks of the source code of certain ransomware families and the use of fragments or entire ransom notes originating from other malware families. We have also observed situations where multiple ransomware families were used during a single attack. All these factors create difficulties not only for incident responders and post-incident analysts but also

for the attacked entity – particularly if it does not have a backup of the data affected by the attack and is forced to wait for a publicly available decryptor.

False double extortion

The double extortion technique and the transfer of data outside the organization prior to encryption remain standard practices in the ransomware threat landscape. Some ransomware groups even declare that they will not perform encryption at all, limiting themselves solely to data theft (this was the official reason for the suspension of operations and rebranding of the RansomHub group in the first quarter of 2025). The vast majority of notes left by encryption software contain a threat to publish the stolen data, even if no exfiltration has actually taken place. To exert additional pressure, attackers may provide false information suggesting that the alleged infiltration of the infrastructure had lasted for months. In 2025, CERT Polska received a few incidents in which the note left by the attackers was not based on a generic template but was specifically prepared for the individual victim, using information obtained during the intrusion. However, the generic content of a note does not mean that data exfiltration did not take place. It should also be noted that many months can elapse between the attack and the public disclosure of the incident by the attackers. There is no consistent rule regarding the information published by attackers – for example, listing files supposedly in their possession does not necessarily mean they were actually exfiltrated.

Observed activities of APT groups

In 2025, CERT Polska observed an intensification of activities by APT groups linked to foreign states. The attacks targeted Polish public entities, private companies, and individuals in public or political roles, including former officials, politicians, and researchers. There was also a noticeable increase in the use of political motives by attackers to achieve their objectives, such as information exfiltration or societal polarization. For the first time in CERT Polska's history, coordinated attacks against Poland's energy sector were observed, aimed at causing destructive impact.

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

All incidents described in this chapter are attributed by CERT Polska to APT group activity; however, in some cases, detailed or definitive attribution has not been provided due to limitations in available data or internal policy decisions.

Selected campaigns and incidents

Activity of the UNC1151/Ghostwriter group

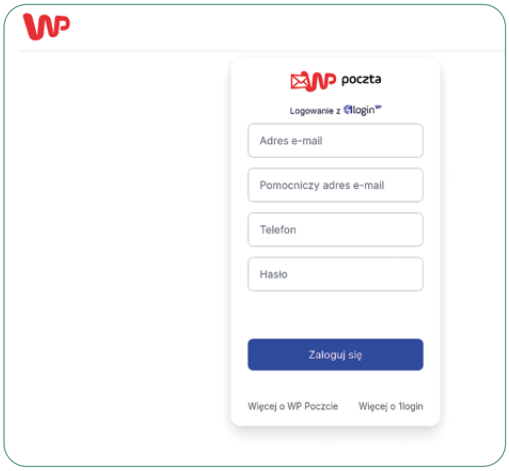
In 2025, the UNC1151 group, as in previous years, remained one of the most active among the activity clusters attributed by CERT Polska to APT groups. According to publications by Google[3], UNC1151 is highly likely linked to the Belarusian government, although other sources also indicate connections to Russian intelligence services[4]. The group's activities were highly diverse. It sought to dynamically change the techniques it used, both in phishing attacks, attacks involving malware, and when exploiting software vulnerabilities[5], as well as when engaging in disinformation activities aimed at polarizing Polish society, including during the election campaign preceding the presidential elections. Due to the diversity of the campaigns conducted by the UNC1151 group, they are described below in sections A–D.

A. PHISHING CAMPAIGNS TARGETING E-MAIL SERVICES

For several years, the UNC1151 group has focused on gaining access to the e-mail accounts of Polish citizens[6], in order to subsequently exfiltrate messages that may contain valuable information or that can be used for propaganda purposes. These attacks are characterized by high diversity as well as frequent changes in the techniques employed. The campaigns we observed were conducted regularly over many weeks, from Monday to Friday, and targeted hundreds of individuals whose e-mail accounts were hosted on services such as Interia, Onet, and Wirtualna Polska.

It is also worth highlighting the issue of domains used in phishing campaigns. At the beginning of the year, the group used domains it had registered itself to host phishing panels imitating login pages of e-mail services. In subsequent quarters, the actor began using compromised websites, typically belonging to Polish entities, for this purpose.

FIGURE 22. Example of a phishing panel used by the UNC1151 group



3 https://blog.google/threat-analysis-group/update-threat-landscape-ukraine

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

5 https://cert.pl/en/posts/2025/06/unc1151-campaign-roundcube/

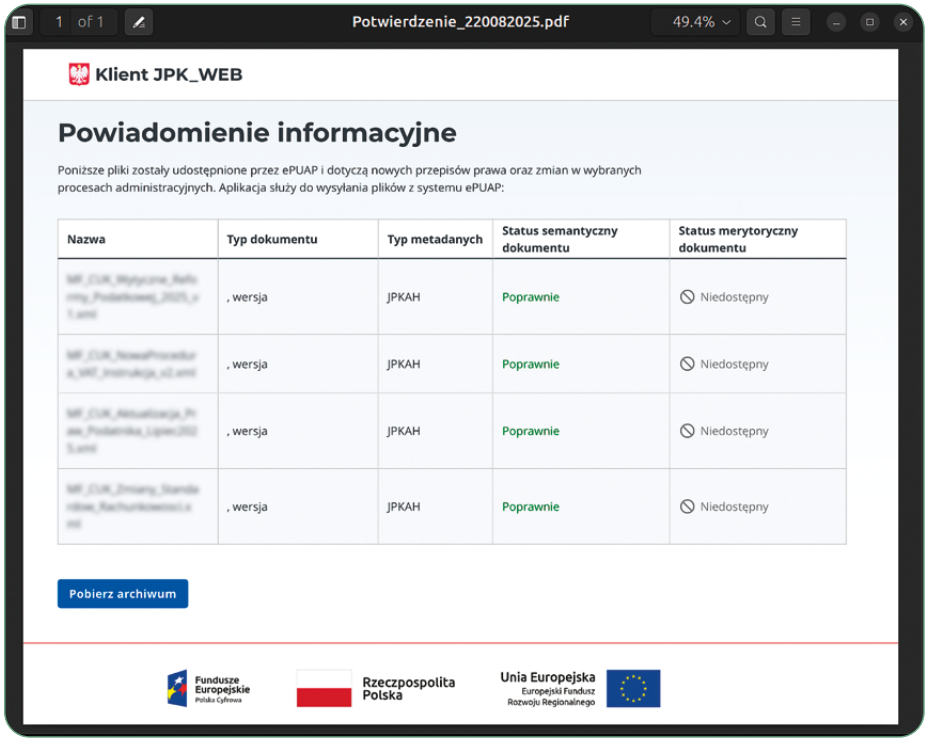
6 https://cert.pl/posts/2022/07/techniki-unc1151/

B. MALWARE DISTRIBUTION

In addition to conducting phishing campaigns targeting e-mail services, in 2025 the UNC1151 group also made intensive efforts to distribute malware, aiming to gain remote access to victims' computers and to steal authentication data for various external services and internal resources.

The attackers regularly change both the techniques and the types of files used to conceal malicious software. In the past year, the most commonly used initial infection vectors were CHM files, such as Microsoft Compiled HTML Help files, as well as XLS files with macros and PPT presentation files. As social engineering lures, the group used themes such as university resolutions, debt collection, payment of political party membership fees, as well as topics related to agriculture and rural areas.

FIGURE 23. Example of a lure used by the UNC1151 group to distribute malware



In addition to using agriculture-related themes, the group also conducted a campaign during the year directly targeting the agricultural sector. For this purpose, a fake CAPTCHA mechanism (so-called ClickFix) was used, placed on popular agriculture-related websites to which the group had previously gained access. An unsuspecting user, after visiting an infected website, was prompted to paste the contents of the clipboard into the "Run" dialogue box in Windows, allegedly to verify that they were not a robot. In reality, this action resulted in malware being downloaded onto the user's computer, with the purpose of data exfiltration.

FIGURE 24. Fake user verification

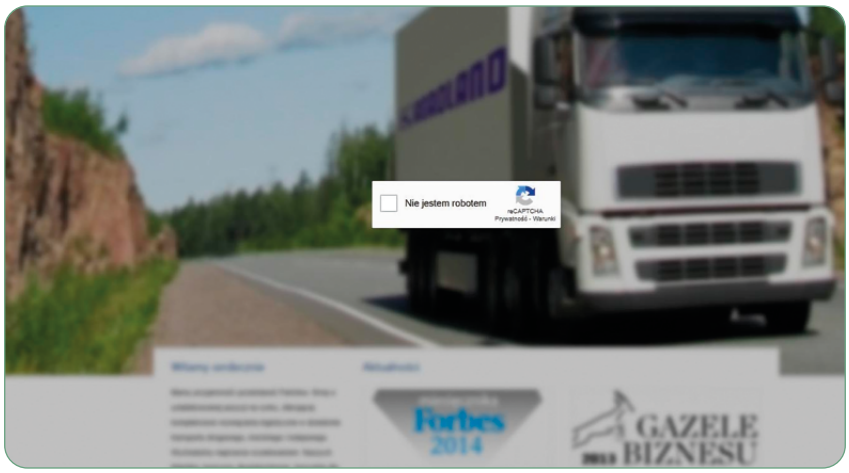
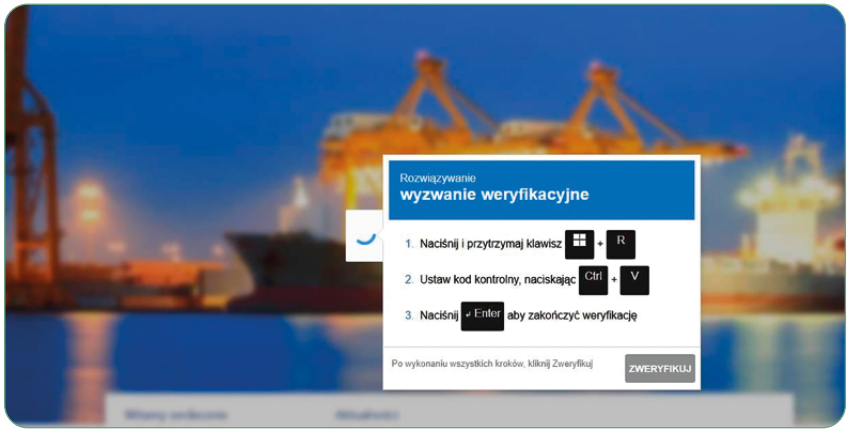


FIGURE 25. Fake CAPTCHA used by the UNC1151 group



C. EXPLOITATION OF VULNERABILITIES IN ROUNDCUBE SOFTWARE

In the past year, the UNC1151 group repeatedly conducted campaigns exploiting the CVE-2024-42009 vulnerability in order to steal credentials. This vulnerability allows the execution of JavaScript code when a specially crafted e-mail is opened. Attackers sent e-mails with subject lines designed to encourage recipients to read the message and take immediate action.

FIGURE 26. Example of a message exploiting CVE-2024-42009, distributed by the UNC1151 group

When an unsuspecting victim opened the e-mail, on a system not updated by the administrator, the vulnerability was exploited, resulting in the installation of a so-called Service Worker in the user's browser. Subsequently, the user was redirected to an e-mail login page, while the Service Worker intercepted all login attempts to the Roundcube application and sent copies of the credentials to the attacker's server. More technical details of the attack are described in the article "UNC1151 campaign exploiting a vulnerability in Roundcube software to steal credentials."[7]

The UNC1151 group used the obtained access to e-mail accounts in two ways. If the contents of a mailbox were deemed valuable by the attackers due to the messages and information contained within, they used it for further data exfiltration. Otherwise, the group used the account to distribute additional messages to other institutions and companies that might be using a vulnerable version of Roundcube software. Attackers frequently reused legitimate messages found in compromised e-mail accounts, to which they attached the exploit, and then distributed them to new targets. This technique was intended to make the communication appear more credible.

It is worth noting that in 2025, the CVE-2024-42009 vulnerability was also exploited in campaigns targeting Polish entities by the APT28 group.

D. ELECTION-RELATED DISINFORMATION

In March 2025, CSIRT NASK observed activity by the UNC1151 group in connection with the upcoming presidential elections at that time. These campaigns used, among other things, the image of the Ukrainian House foundation as well as candidates participating in the elections. The attacks aimed, among other objectives, to deepen the polarization of Polish society, but also to incite hostility toward the Ukrainian minority in Poland.

Materials created by the group were promoted, among others, through advertising campaigns on YouTube and TikTok, but were also posted in auction descriptions on the OLX platform, where the group conducted fake sales of gadgets containing vulgar content.

CSIRT NASK cooperated with the Information Protection Division of Cyberspace at NASK – PIB in monitoring these campaigns.

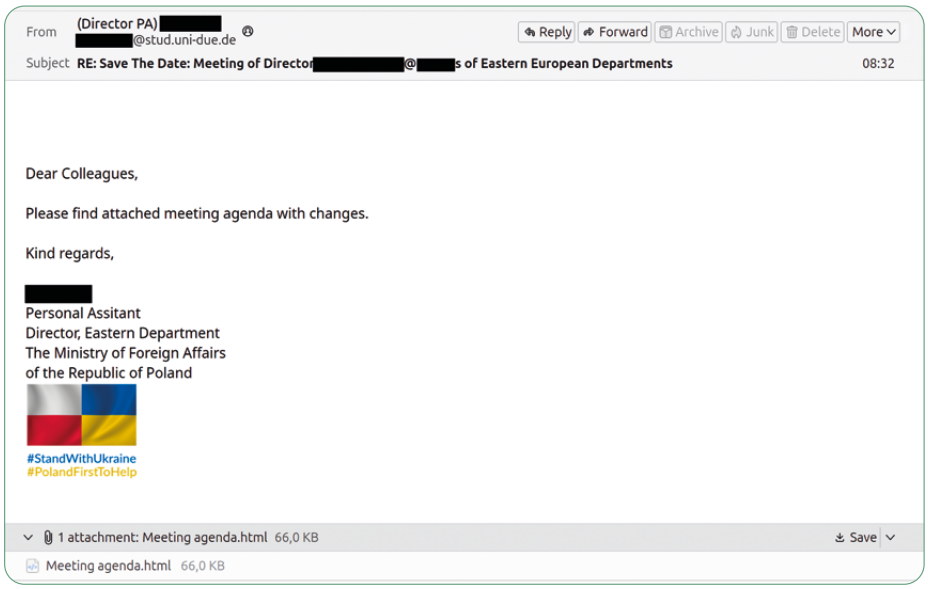
Device Code Phishing

In February of the previous year, CSIRT NASK received information through the European CSIRT Network about a campaign in which attackers impersonated an employee of the Polish Ministry of Foreign Affairs. The attackers

7 https://cert.pl/en/posts/2025/06/unc1151-campaign-roundcube/

distributed a malicious attachment via e-mail, lending it credibility by using a legitimate message containing an invitation related to the Polish presidency of the Council of the European Union. This message was most likely obtained by the attackers from a compromised e-mail account of one of its recipients. The objective was to gain access to Microsoft 365 resources belonging to employees of European embassies.

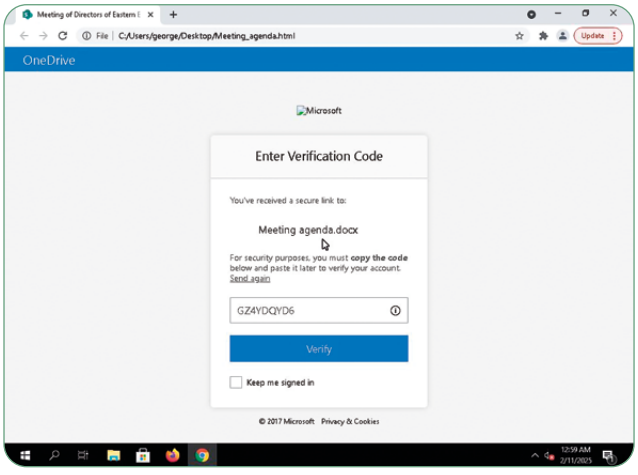
FIGURE 27. Content of the e-mail message distributed to employees of European embassies



The attackers attempted to exploit an alternative Microsoft authentication mechanism via an HTML file that retrieved a Device Code generated by the attackers from their server. Subsequently, the user was prompted to copy the code and paste it while logged into their Microsoft account, which would grant the attackers access to the victim's account, their data, and all resources and services within the organization's tenant.

In the following weeks of February, CSIRT NASK tracked further iterations of the campaign, in which attackers used different themes – an invitation from a Polish ambassador to a video call, a joint statement by individuals supporting Alexei Navalny, and videoconferences involving representatives of foreign government agencies and think tanks.

Figure 28. HTML file used in the Device Code Phishing attack



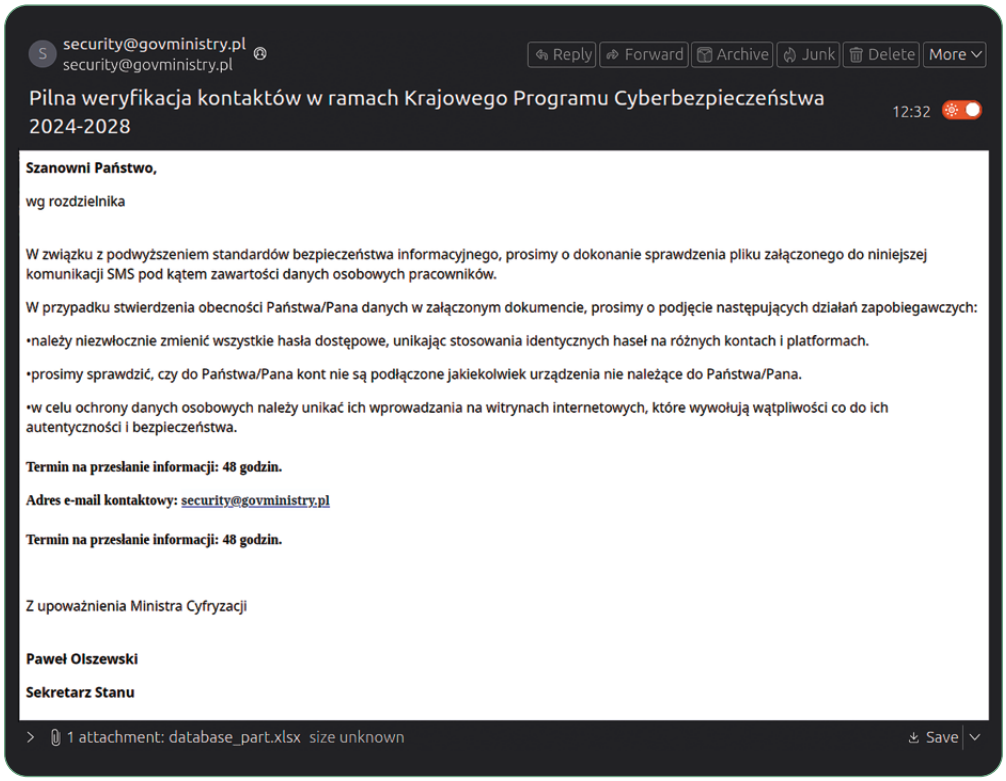
Polish Space Agency

At the end of February 2025, CERT Polska obtained information about suspicious activity within the infrastructure of the Polish Space Agency. During the analysis, the presence of an attacker was confirmed and persistence mechanisms left behind were identified. The attacker registered their own applications within a Microsoft Azure tenant and communicated with them via the Graph API in order to exfiltrate data. The incident analysis and response activities were conducted jointly with the CSIRT MON team.

Harvesting of information on employees of the national cybersecurity system

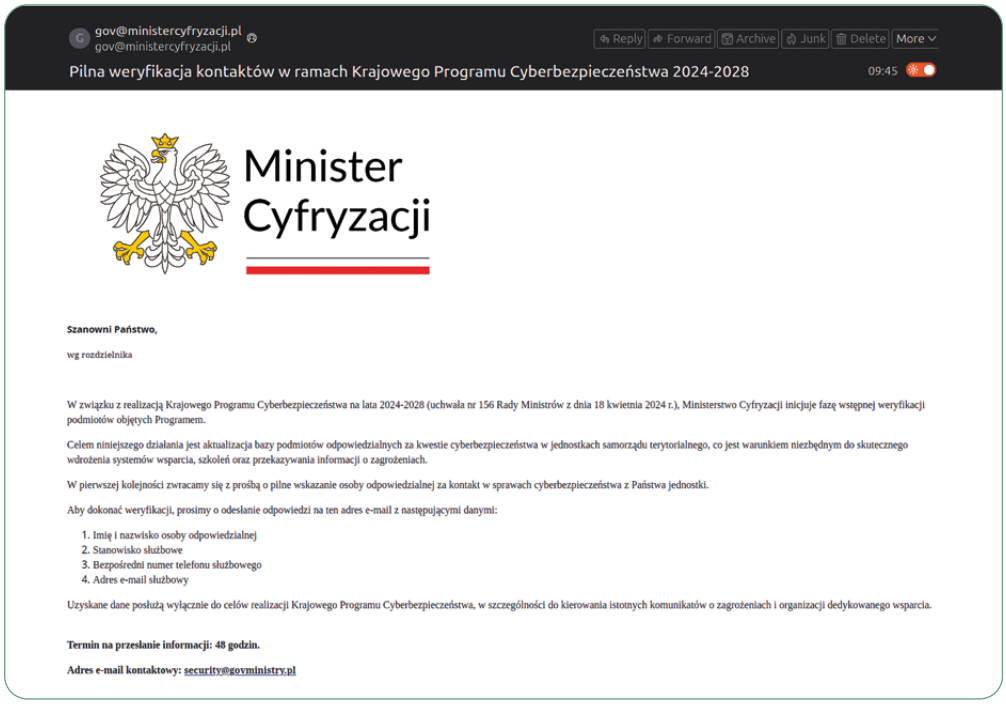
At the end of October 2025, CSIRT NASK observed for the first time a campaign in which attackers impersonated the Ministry of Digital Affairs and Deputy Minister Paweł Olszewski. The targets of this campaign were local government units. The attackers prepared two variants of the campaign distributed via e-mail messages sent from the domain govministry[.]pl. In the first variant, an XLSX spreadsheet file was attached to the message, linking to a website where a second document allegedly containing the complete set of information was hosted. In reality, it was a heavily obfuscated executable file containing malware.

FIGURE 29. Content of the message in which attackers impersonated Deputy Minister of Digital Affairs Paweł Olszewski



In the second variant of the campaign, the attackers, using social engineering techniques, attempted to persuade recipients to provide detailed information about individuals responsible for IT security within the respective local government units, including names, surnames, phone numbers, and e-mail addresses. If successful in obtaining this data, the attackers would most likely attempt to carry out targeted attacks against these specific individuals. CSIRT NASK took action to warn all Polish municipalities about the ongoing campaign.

FIGURE 30. Content of the message used to harvest information about local government employees



Coordinated attacks on the energy sector

At the end of December 2025, for the first time in Poland's history, coordinated, targeted attacks of a sabotage nature were carried out against entities in the energy sector. The conducted analysis showed that they were attributed to an activity cluster publicly known as "Static Tundra" (Cisco), "Berserk Bear" (CrowdStrike), "Ghost Blizzard" (Microsoft), and "Dragonfly" (Symantec). The activities targeted at least 30 wind and photovoltaic farms, a private company from the manufacturing sector, and a large combined heat and power plant supplying heat to nearly half a million customers in Poland.

These incidents affected both IT systems and physical industrial devices, which is relatively rare among previously documented attacks. It is worth emphasizing that this occurred during a period when Poland was facing low temperatures and snowstorms. At the same time, it should be noted that the attacks did not affect the ongoing production of electricity or the supply of heat.

CERT Polska participated in the handling of the incidents from the moment they were detected and supported the affected entities in the forensic analysis, which resulted in the publication of a report to share knowledge about the course of the incident and the techniques used by the attackers. The report is available on the cert.pl website.[8]

Key vulnerabilities

In 2024, we intensified our efforts to effectively reach entities using software containing vulnerabilities that, in our assessment, posed a high risk. As these efforts yielded tangible results, we continued them in 2025.

We continuously monitored new information to identify vulnerabilities whose exploitation by attackers could pose a significant risk to Polish entities. Subsequently, we carried out activities aimed at identifying the owners of internet-exposed instances. The results of scans related to the vulnerabilities we considered most critical in 2025 are presented in Table 2. Not all scans were performed by our team – in some cases, the information was obtained from partners.

However, the team's approach to sending notifications underwent certain changes. A new source of information about device owners is the free service moje.cert.pl, where administrators can provide the domains and network ranges they manage. By sharing their contact details, they enable the CERT Polska team to reach them much faster and more effectively with critical information regarding security vulnerabilities.

Another new element is the publication of warnings within the moje.cert.pl service. In the case of high-risk vulnerabilities, in parallel with e-mail notifications sent to specific entities, we also publish warnings in this service. We also took this step in cases where identifying vulnerable instances and their owners proved difficult. More information on how to follow issued notifications can be found in the chapter „Moje.cert.pl" (→ pp. 104–105).

TABLE 2. Number of software instances vulnerable or exposed to the internet at the time notifications were sent by the CERT Polska team

Product	Status	Number of instances
React Server Components	vulnerable	1943
PAD CMS	vulnerable	961

8 https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/

Product	Status	Number of instances
Cisco Secure Firewall ASA/FTD	vulnerable	427
FortiOS / FortiProxy (CVE-2024-55591, CVE-2025-24472)	vulnerable	240
Ivanti Connect Secure	vulnerable	120
NetBird VPN	vulnerable	40
Citrix NetScaler ADC/Gateway	vulnerable	17
Omnissa Workspace ONE UEM	vulnerable	15
Ivanti EPMM	vulnerable	4
SonicWall SonicOS	publicly exposed	440
FortiOS z włączonym SSO (CVE-2025-59718, CVE-2025-59719)	publicly exposed	326
Microsoft SharePoint Server	publicly exposed	50
Ingress-NGINX	publicly exposed	11
Cisco Secure Email Gateway	publicly exposed	4
Fortinet FortiWeb Manager	publicly exposed	2

Roundcube (CVE-2024-42009, CVE-2025-49113)

DATE OF VULNERABILITY DISCLOSURE: 05.08.2024, 02.06.2025

Roundcube is a popular web-based e-mail client widely used by many Polish organizations, including the largest hosting providers. The CERT Polska team observed the exploitation of a critical XSS vulnerability (CVE-2024-42009) in attacks enabling the takeover of mailbox credentials.

The CVE-2024-42009 vulnerability consists of an HTML sanitization flaw allowing the execution of JavaScript code in the context of a user reading a specially crafted e-mail message. Attackers could modify the e-mail client interface, mislead users, or take over authentication data, which led to full account compromise. CVE-2025-49113 is a PHP deserialisation vulnerability in the upload.php file, allowing an authenticated user to achieve remote code execution on the Roundcube server via an insecure _from parameter. The combination of this vulnerability with credentials obtained as a result of XSS attacks could allow remote attackers to take over mail servers.

CERT Polska detected an UNC1151 campaign targeting Polish entities, in which compromised mailboxes were used for further distribution of XSS exploits. Attackers installed Service Workers as a persistence mechanism

to intercept credentials. The scale of the attacks was high, as Roundcube is used not only by individual organizations but also by the largest Polish hosting providers, meaning that all of their customers were potentially exposed. More information about these vulnerabilities is available in the article titled “UNC1151 campaign exploiting a vulnerability in Roundcube software to steal credentials”.[9]

A precise determination of the number of vulnerable instances proved impossible due to backporting (updates applied without changing the version number) and Roundcube being hidden behind VPNs, which in turn made both scanning and contacting administrators impossible. CERT Polska published warnings for users, including via the moje.cert.pl service,[10] and supported entities affected by the attacks.

Ivanti Connect Secure / Policy Secure / ZTA Gateway (CVE-2025-0282, CVE-2025-0283, CVE-2025-22457)

DATE OF VULNERABILITY DISCLOSURE: 08.01.2025, 03.04.2025

Ivanti Connect Secure, Policy Secure, and ZTA Gateway are VPN and access control solutions used in corporate networks.

We observed the exploitation of vulnerabilities CVE-2025-0282 and CVE-2025-0283, which enabled unauthenticated remote code execution as well as privilege escalation after initial access was obtained. These vulnerabilities were actively exploited as zero-days for several weeks before Ivanti published information about them. Mandiant[11] confirmed that the Chinese threat group UNC5221 had been using them since mid-December 2024, and that on compromised devices it disabled SELinux and syslog, and left scripts (web shells) to maintain persistent access and enable credential theft. CERT Polska received information about the exploitation of these vulnerabilities in several Polish organizations.

A critical vulnerability, CVE-2025-22457, was also identified in these devices, consisting of a stack buffer overflow that allowed remote unauthenticated attackers to execute arbitrary code and fully compromise the device. Mandiant[12] again confirmed active exploitation of this vulnerability by a group suspected to have links to China. The vulnerability was exploited before its public disclosure, which also classifies it as a zero-day.

9 https://cert.pl/en/posts/2025/06/unc1151-campaign-roundcube/

10 https://moje.cert.pl/komunikaty/2025/4/krytyczna-podatnosc-w-oprogramowaniu-roundcube

11 https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day

12 https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-exploiting-critical-ivanti-vulnerability

CERT Polska scanned the Polish internet, identified 120 vulnerable Ivanti Connect Secure devices, and promptly notified their administrators about the need to apply updates and inspect devices for signs of compromise.

SonicWall SonicOS (CVE-2024-53704)

DATE OF VULNERABILITY DISCLOSURE: 09.01.2025

SonicOS is the operating system of SonicWall network devices. A vulnerability was identified in the SSL VPN authentication mechanism, which allows attackers to bypass authentication and hijack the session of the most recently logged-in user.

Exploitation of this vulnerability enables access to private user networks, reading Virtual Office bookmarks, downloading NetExtender configurations, and establishing a VPN tunnel with the victim's privileges.[13] After the vulnerability was publicly disclosed, an exploit script also appeared, and the vulnerability was actively exploited in attacks.

Following the publication of information about the vulnerability, CERT Polska identified more than 440 SonicWall devices on the Polish internet. Administrators were promptly notified of the threat.

FortiOS / FortiProxy (CVE-2024-55591, CVE-2025-24472)

DATE OF VULNERABILITY DISCLOSURE: 14.01.2025, 11.02.2025

Critical vulnerabilities were identified in FortiOS and FortiProxy that allow authentication bypass. This enables a remote attacker to obtain administrator privileges by sending a specially crafted request to the Node.js WebSocket module or the CSF proxy.

The vulnerabilities were actively exploited weeks before information about them was disclosed. Arctic Wolf[14] linked an ongoing attack campaign to these vulnerabilities, in which attackers created administrative accounts and modified VPN configurations. The CERT Polska team also observed exploitation of these vulnerabilities in Poland.

13 https://bishopfox.com/blog/sonicwall-cve-2024-53704-ssl-vpn-session-hijacking

14 https://arcticwolf.com/resources/blog/cve-2024-55591

In January 2025, 240 vulnerable devices were identified and their administrators were notified. Since then, the situation has been continuously monitored, and information about not updated instances has been provided. At the end of December 2025, 35 vulnerable devices remained.

Ingress NGINX Controller for Kubernetes (CVE-2025-1097, CVE-2025-1098, CVE-2025-24513, CVE-2025-24514, CVE-2025-1974)

DATE OF VULNERABILITY DISCLOSURE: 24.03.2025

Ingress NGINX Controller for Kubernetes (short name: Ingress-NGINX) is the default traffic controller in Kubernetes clusters, providing reverse-proxy and load balancing functionality. In versions up to and including 1.12.0 and 1.11.4, critical vulnerabilities were identified that allow unauthenticated remote code execution by exploiting a webhook exposed by default by this service.

The webhook service is exposed on TCP port 8443 and is typically reachable by all pods in the cluster, which allows an attacker with network access to execute arbitrary code via a specially crafted HTTP request. Exploitation of the vulnerability may result in unauthorized access to data stored across all namespaces in a Kubernetes cluster, leading to full compromise of the environment.

The CERT Polska team identified 11 publicly available instances of Ingress-NGINX in Polish IP space. Administrators of these systems were notified about the threat and recommendations to update the controller to versions that eliminate the vulnerabilities, and an article titled “Critical vulnerabilities in the Ingress-NGINX controller in Kubernetes”[15] was published on the CERT Polska website, in which the described threat was explained in detail.

Ivanti Endpoint Manager Mobile (CVE-2025-4427, CVE-2025-4428)

DATE OF VULNERABILITY DISCLOSURE: 13.05.2025

Ivanti Endpoint Manager Mobile (EPMM) is a system for managing devices in corporate environments. The CVE-2025-4427 vulnerability enables authentication bypass in the API component, allowing an attacker to access

15 https://cert.pl/posts/2025/03/krytyczne-podatnosci-w-kontrolerze-ingress-nginx-kubernetes

protected resources. CVE-2025-4428 is a vulnerability allowing remote code execution in the same API component, enabling an authenticated attacker to execute arbitrary code via specially crafted requests.

Exploitation of both vulnerabilities allows unauthenticated remote code execution and access to data about employees and devices managed by EPMM, including retrieval of sensitive configuration information and potential escalation of attacks within the network. Ivanti confirmed detection of real-world attacks exploiting this chain before the official disclosure of the vulnerabilities, meaning the flaws were operating as zero-days in production environments of some customers.[16]

CERT Polska identified 4 vulnerable EPMM instances exposed to the internet in May, and since then their administrators were periodically notified about the issue. By December 2025, the number of vulnerable Ivanti EPMM devices had dropped to zero.

Citrix NetScaler ADC/Gateway (CVE-2025-6543)

DATE OF VULNERABILITY DISCLOSURE: 25.06.2025

NetScaler ADC and NetScaler Gateway are network devices used for load balancing and providing VPN-based remote access. The CVE-2025-6543 vulnerability was officially described by the manufacturer as a denial-of-service issue related to a memory overflow in instances configured as remote access gateways. In practice, however, the same mechanism could be exploited for remote code execution and full compromise of vulnerable devices.[17]

Even before patches were released, cases of device compromise were observed globally, in which attackers deployed malicious scripts (web shells) or other persistence mechanisms. The impact of these intrusions was difficult to reliably detect without targeted threat-hunting activities. CERT Polska received information from partners about exploitation of CVE-2025-6543 to compromise devices, confirming that in practice the vulnerability could be used for remote code execution.

After the publication of vulnerability information, we identified several publicly exposed and vulnerable NetScaler ADC/Gateway instances. We contacted their administrators as quickly as possible to recommend applying security updates and reviewing logs for potential compromise. This communication was carried out via e-mail, and we also published a notice in the moje.cert.pl

16 https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM

17 https://www.rapid7.com/blog/post/etr-zero-day-exploitation-of-netscaler-adc-and-netscaler-gateway

service.[18] In parallel, we conducted active scanning of Citrix instances to search for known web shells and other indicators of compromise. However, no successful infections were confirmed in Polish organizations.

Sudo (CVE-2025-32463)

DATE OF VULNERABILITY DISCLOSURE: 30.06.2025

Sudo is a tool for privilege management in Unix/Linux systems that allows execution of selected commands with administrator privileges. The CVE-2025-32463 vulnerability identified in it allows local privilege escalation and is related to the handling of the chroot option. The vulnerability enables execution of arbitrary commands as the root user, even if the user is not defined in the sudoers file. As a result, an attacker who has access to the system as a regular user can gain full control over the operating system.

The vulnerability stems from improper handling of the nsswitch.conf configuration file from a user-controlled directory when sudo is executed with the chroot option, which allows loading malicious libraries and escalating privileges. It is particularly important that the vulnerability can also be exploited in the default sudo configuration, without additional modifications on the administrator's side, which significantly increases the risk of attack. The vulnerability affected the latest versions at the time of popular Linux distributions such as Ubuntu, Fedora, and Red Hat Enterprise Linux.

Due to the nature of the vulnerability, we decided to publish a warning for administrators via the moje.cert.pl service[19] as the most effective communication channel in situations where it is not possible to directly associate the vulnerability with specific publicly accessible services.

Microsoft SharePoint Server (CVE-2025-53770)

DATE OF VULNERABILITY DISCLOSURE: 19.07.2025

Microsoft SharePoint Server is a content management system that can be deployed on-premises within an organization's infrastructure. The CVE-2025-53770 vulnerability applies exclusively to on-premise installations and results from deserialisation of untrusted data, which allows unauthenticated attackers to achieve remote code execution via specially crafted HTTP requests. The mechanism involves, among other things,

18 https://moje.cert.pl/komunikaty/2025/17/aktywnie-wykorzystywane-krytyczne-podatnosci-narzedzia-citrix-netscaler

19 https://moje.cert.pl/komunikaty/2025/11/krytyczna-podatnosc-narzedzia-sudo-w-wersji-do-1917-wacznie

manipulation of ViewState and the ASP.NET MachineKey, enabling full system compromise, including access to organizational data and resources.

Information about the vulnerability was published in July 2025, and Microsoft initially did not release a patch, which significantly hindered rapid mitigation and increased the risk of successful attacks. Activity by state-sponsored actors, including Chinese groups, was observed, highlighting the level of risk associated with this vulnerability.[20]

The CERT Polska team observed attempts to exploit this vulnerability in organizations located in Poland. Conducted scans identified 50 publicly accessible SharePoint Server instances in the Polish internet. Their administrators were notified of the threat.

Omnissa Workspace ONE UEM (CVE-2025-25231)

DATE OF VULNERABILITY DISCLOSURE: 11.08.2025

Omnissa Workspace ONE UEM (formerly VMware AirWatch) is an MDM system used for managing mobile devices in corporate environments. A path traversal vulnerability was discovered in the on-premise version, which allows an attacker to read arbitrary files from the server disk without authentication.

The vulnerability was actively exploited in attacks targeting Polish entities to steal sensitive information, including employee data. At the beginning of September, we received information about 15 vulnerable internet-exposed instances and promptly notified administrators about the threat and the need to update the software. We also published a notice for administrators in the moje.cert.pl service.[21]

Cisco Secure Firewall ASA/FTD (CVE-2025-20333, CVE-2025-20362, CVE-2025-20363)

DATE OF VULNERABILITY DISCLOSURE: 25.09.2025

Cisco Secure Firewall ASA (Adaptive Security Appliance) and FTD (Firewall Threat Defense) are network firewall devices. Three vulnerabilities affecting these products were published, two of which were classified

20 https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities

21 https://moje.cert.pl/komunikaty/2025/29/aktywnie-wykorzystywana-krytyczna-podatnosc-w-narzedziu-omnissa-workspace-one-uem-airwatch-mdm

as critical (CVE-2025-20333 and CVE-2025-20362), resulting from improper handling of HTTP requests to the WebVPN component.

The vulnerabilities allow an unauthenticated attacker to access network resources without authentication and achieve remote code execution with root privileges, leading to full device compromise. We observed active exploitation of these vulnerabilities in attacks targeting Polish entities.

We identified 427 vulnerable devices, directly notified their administrators, and published a warning in the moje.cert.pl service.[22] Due to the high risk and the presence of instances running unsupported versions of the product, the Government Plenipotentiary for Cybersecurity issued a recommendation for immediate updates of Cisco ASA/ Cisco Firepower products or their decommissioning.[23]

PAD CMS (CVE-2025-7063, CVE-2025-7065, CVE-2025-8117, CVE-2025-8120, CVE-2025-8121, CVE-2025-8122)

DATE OF VULNERABILITY DISCLOSURE: 30.09.2025

PAD CMS is content management software used mainly in public sector entities for managing Public Information Bulletin websites. CERT Polska coordinated the disclosure process of a series of critical vulnerabilities, including several identified through internal research.[24]

The most severe vulnerabilities allowed an unauthenticated attacker to inject a custom script into a website, which could lead to remote code execution and full server compromise. We identified 961 vulnerable PAD CMS instances on the Polish internet, mainly in municipal offices, libraries, and schools.

Due to its widespread use in the public sector and the lack of prospects for a manufacturer-issued update because the product is end-of-life, CERT Polska notified all administrators about the need to replace the software, and the Government Plenipotentiary for Cybersecurity issued a recommendation to immediately decommission PAD CMS.[25]

22 https://moje.cert.pl/komunikaty/2025/36/aktywnie-wykorzystywane-krytyczne-podatnosci-w-urzadzeniach-cisco-asa-i-cisco-firepower

23 https://www.gov.pl/web/cyfryzacja/rekomendacja-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-dotyczaca-aktualizacji-produktow-cisco

24 https://cert.pl/posts/2025/09/CVE-2025-7063

25 https://www.gov.pl/web/cyfryzacja/rekomendacja-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-zaprzestanie-korzystania-z-oprogramowania-pad-cms

Oracle E-Business Suite (CVE-2025-61882)

DATE OF VULNERABILITY DISCLOSURE: 05.10.2025

Oracle E-Business Suite is an integrated ERP system used for enterprise management. The critical CVE-2025-61882 vulnerability in the BI Publisher Integration component allows unauthenticated remote code execution by an attacker with network access.

The vulnerability was exploited as a zero-day for weeks before Oracle released a security patch. CrowdStrike and Google confirmed exploitation of the vulnerability by the CL0P group to exfiltrate data from organizations. The first signs of attacks were dated to August 2025.[26]

Despite the low level of Oracle EBS deployment in Poland, CERT Polska received a report of an incident in which this vulnerability was exploited. The ease of exploitation and high impact on organizations, including the potential leakage of sensitive business data, place this vulnerability high in the risk classification.

NetBird VPN (CVE-2025-10678)

DATE OF VULNERABILITY DISCLOSURE: 20.10.2025

NetBird is a VPN platform based on the WireGuard protocol. CERT Polska received a report of a vulnerability related to default credentials of an administrator account created by ZITADEL – the default identity provider in the NetBird solution. The manufacturer's installation script did not remove or change the default password, which allowed remote administrative access to the VPN management panel.

As a result, many instances could be accessed using widely known default credentials, giving full control over the network infrastructure. CERT Polska assigned a CVE identifier to this vulnerability and coordinated the responsible disclosure process with the manufacturer.[27]

The CERT Polska team identified more than 40 NetBird instances in the Polish internet with active default administrator accounts. All administrators were notified about the threat one month before the vulnerability disclosure.

26 https://www.crowdstrike.com/en-us/blog/crowdstrike-identifies-campaign-targeting-oracle-e-business-suite-zero-day-CVE-2025-61882

27 https://cert.pl/en/posts/2025/10/CVE-2025-10678/

Fortinet FortiWeb Manager (CVE-2025-64446)

DATE OF VULNERABILITY DISCLOSURE: 14.11.2025

FortiWeb Manager is a component of the FortiWeb system, a web application firewall used to protect web applications against attacks. It enables centralized management of configuration and security policies for FortiWeb instances.

The vulnerability identified in it, CVE-2025-64446, results from a path traversal vulnerability that allows an unauthenticated attacker to execute administrative commands via specially crafted HTTP or HTTPS requests sent to the GUI panel. The attack involves sending a POST request with a payload creating a new administrator account to a specific path, which grants attackers full control over the device. The vulnerability was actively exploited before Fortinet officially disclosed information about it in November 2025, with the first exploitation attempts observed in October 2025.[28]

In Poland, scans conducted by the CERT Polska team identified only a few publicly accessible FortiWeb Manager instances. Despite the small scale, such a vulnerability poses a serious risk, especially for devices located in internal networks with flat topology, where untrusted users may have access to the management panel. Administrators of the identified instances were notified about the risk and recommendations to disable HTTP/HTTPS access to the management interface until updates are applied, and a warning was published in the moje.cert.pl service regarding this threat.[29]

React Server Components (CVE-2025-55182)

DATE OF VULNERABILITY DISCLOSURE: 03.12.2025

The detected CVE-2025-55182 vulnerability enables remote code execution in React Server Components (RSC) and other applications using RSC, such as Next.js.

Exploitation involves sending a specially crafted HTTP request that results in arbitrary code execution on the server before any authentication checks are performed. Publicly available descriptions and PoC code significantly increased the risk of mass attacks against RSC applications. Mandiant[30] reported exploitation of this vulnerability by multiple groups, mainly linked to China, which deployed persistence mechanisms on compromised servers.

28 https://arcticwolf.com/resources/blog/cve-2025-64446

29 https://moje.cert.pl/komunikaty/2025/57/aktywnie-wykorzystywana-krytyczna-podatnosc-w-urzadzeniach-fortinet-fortiweb-manager

30 https://cloud.google.com/blog/topics/threat-intelligence/threat-actors-exploit-react2shell-cve-2025-55182

From the first day after disclosure, we scanned the Polish internet for vulnerable websites. We identified nearly 2,000 instances enabling remote code execution and notified their administrators. Despite no reported incidents of exploitation of this vulnerability in Poland, the popularity of this technology indicates a high level of risk; therefore, we also issued a warning via the moje.cert.pl service.[31]

FortiOS / FortiProxy / FortiWeb / FortiSwitchManager (CVE-2025-59718, CVE-2025-59719)

DATE OF VULNERABILITY DISCLOSURE: 09.12.2025

FortiOS, FortiProxy, FortiWeb, and FortiSwitchManager are Fortinet products used for network security and device management. Vulnerabilities were identified in these products related to incorrect verification of cryptographic signatures. These vulnerabilities allow an unauthenticated attacker to bypass FortiCloud SSO authentication via a specially crafted SAML message.

The vulnerabilities affect devices with FortiCloud SSO enabled, which is activated automatically after registration in FortiCare via the GUI, unless the administrator disables the relevant option. Exploitation of the vulnerability leads to unauthorized administrative access. Arctic Wolf shortly after disclosure observed attacks exploiting these vulnerabilities.[32]

We scanned the Polish internet for Fortinet FortiOS products with SSO authentication enabled. We identified 326 such devices, and their administrators were informed about the risk and recommendations to disable the feature or apply updates, both via email and through a notice published in the moje.cert.pl service.[33]

31 https://moje.cert.pl/komunikaty/2025/61/krytyczna-podatnosc-w-react-server-components-oraz-innych-aplikacjach-z-tym-rozwiazaniem

32 https://arcticwolf.com/resources/blog/arctic-wolf-observes-malicious-sso-logins-following-disclosure-cve-2025-59718-cve-2025-59719

33 https://moje.cert.pl/komunikaty/2025/64/podatnosci-w-oprogramowaniu-fortios-fortiproxy-fortiweb-i-fortiswitchmanager

Cisco Secure Email Gateway oraz Secure Email and Web Manager (CVE-2025-20393)

DATE OF VULNERABILITY DISCLOSURE: 17.12.2025

Cisco offers Secure Email Gateway (formerly IronPort) and Secure Email and Web Manager solutions used to protect e-mail communication against threats. They are based on the AsyncOS system, in which a critical vulnerability was identified that allows an unauthenticated attacker to remotely execute arbitrary code with root privileges. The vulnerability is related to improper input validation in the Spam Quarantine service. Although the service is disabled by default and, according to best practices, should not be exposed to the internet, incorrect configuration can enable full device compromise without requiring any credentials.

This vulnerability was actively exploited in cyberattacks long before official security patches were released. According to Cisco Talos analysis,[34] the campaign is attributed to a Chinese espionage group tracked as UAT-9686 (with links to APT41 and UNC5174). After compromising devices, attackers deployed malware, including the AquaShell backdoor providing persistent access, as well as tools such as AquaTunnel and Chisel for traffic tunneling and further network exploitation.

We identified several devices in the Polish internet with the Spam Quarantine service incorrectly exposed to the internet. The owners of these instances were immediately notified about the critical risk. However, due to the nature of the Spam Quarantine service, which often operates only within internal organizational networks, external scanning does not allow identification of all affected entities. For this reason, we published a notice for administrators via the moje.cert.pl platform[35] to warn about the risk of exploitation of this vulnerability for privilege escalation within corporate networks.

Data leaks

In 2025, CERT Polska continued operational activities and cooperation with state authorities to disclose information about data leaks containing records related to Polish citizens. A key activity aimed at effectively mitigating the impact of such incidents is proactive monitoring of cyberspace.

34 https://blog.talosintelligence.com/uat-9686

35 https://moje.cert.pl/komunikaty/2025/65/krytyczna-podatnosc-cve-2025-20393-w-oprogramowaniu-cisco-asyncos-software

We monitor websites where criminals publish data obtained from victims of attacks, forums on the TOR network, communication channels used by criminals, as well as collect and analyse information obtained using tools from external providers. Whenever a potential data leak is detected, we contact the affected entity to determine the source and scope of the leak and to help mitigate its impact.

Bezpiecznedane.gov.pl

Since 2023, CERT Polska has consistently been feeding the service bezpiecznedane.gov.pl with data from disclosed leaks, enabling Polish internet users to verify whether and to what extent their data may have been compromised.

Due to its national scope, the service often contains data exceeding what is available on similar international platforms. In some cases, thanks to cooperation with companies and institutions affected by leaks, CERT Polska is able to include not only data published by criminals but also complete sets of stolen data. This allows potentially affected citizens to obtain relevant information regardless of whether their data appeared in the sample published by attackers.

A unique feature of the service is the ability for users, in selected cases, to check using their PESEL number whether their data may have been exposed. In 2025, we added information on 10 data leaks to the service. Below we present those leaks that occurred in 2025.

Data set of login credentials published on a criminal forum

At the beginning of February 2025, a list containing 11 million pairs of e-mail addresses and passwords was published on a criminal forum. CERT Polska analysis showed that a significant portion of the records were historical entries, already appearing in previous leaks and in some cases dating back up to 10 years.

Babyhit.pl

In March 2025, a data leak from the babyhit.pl online store was published on a criminal forum, containing data of approximately 600,000 individuals. The analysis showed that the leak included data such as first name, last name, delivery address, e-mail address, and phone number.

Data set of login credentials published in Telegram app

In September 2025, a list containing more than 1.8 million records appeared on a public Telegram channel. Although CERT Polska analysis showed that most of the data originated from previous leaks, some records appeared to potentially originate from 2025.

SuperGrosz.pl

In October 2025, an offer to sell a database of customers of SuperGrosz.pl appeared online, and the company confirmed a data security breach. The sample shared by criminals included the following data: first name and surname, residential or correspondence address, e-mail address, phone number, PESEL number, identity document information, and login data with password hashes. We contacted the company, which confirmed the breach and provided the bezpiecznedane.gov.pl service with the complete dataset of affected customers.

Itaka.pl

Also in October 2025, an offer to sell a database of customers of the travel agency Itaka was published online. The description of the offer indicated 2.2 million entries, with approximately 10,000 records shared as a sample. Itaka confirmed that a data breach affecting part of its “Customer Zone” system had occurred. The leak contained first names and surnames, e-mail addresses, and phone numbers. The company stated that no financial data or PESEL numbers were exposed. According to Itaka’s communications, the leak affected at least 10,000 individuals, although the company noted that the actual scale may be larger. Unlike the SuperGrosz.pl leak, in this case the bezpiecznedane.gov.pl service contains only the data published by criminals.

Wkdzik.pl

In December 2025, a breach of systems supporting the wkdzik.pl online store occurred, resulting in access to several databases maintained by the company. Based on analysis of the material and internal findings, it was confirmed that customer and contractor databases were exfiltrated. They contained first name, last name, e-mail address, phone number, and delivery address. The database was subsequently put up for sale by a person claiming to be the attacker, increasing the risk of further dissemination and potentially future use in attempts to harvest sensitive information. The company provided the data from the stolen databases to the bezpiecznedane.gov.pl service to enable users to verify whether they were affected by the incident.

Abfoto.pl

In December 2025, a breach occurred in the systems supporting the abfoto.pl online store, resulting in unauthorized access to a customer database. The database contained data such as first name and surname, e-mail address, phone number, residential or shipping address, order value and number of orders, and in some cases company data. According to findings, the incident affected over 100,000 customers. Although the database has not been publicly released, the company provided the data to the bezpiecznedane.gov.pl service.

Data set of Facebook login credentials

Officers from the Central Cybercrime Bureau in Białystok, during investigation RSD.27/25, dismantled an organized criminal group that first used phishing to obtain Facebook login credentials and then used a messaging application on the platform to extort BLIK codes from other Facebook users. From May 2022 to May 2024, more than 100,000 stolen login and password pairs for the Facebook platform were secured. The victim database was provided for publication in the bezpiecznedane.gov.pl service. It should be noted that this is the first such cooperation between institutions, enabling citizens – if they verify that their login credentials were compromised due to the group's activity – to contact the authority conducting the investigation, as stated in the CBZC notice published in the service.

Notifications about data leaks in moje.cert.pl

One of the core functions of the moje.cert.pl system is monitoring information about password leaks affecting users within corporate and institutional domains. When such a leak is identified, registered administrators are notified without delay. More information about moje.cert.pl can be found in the section of the report dedicated to our projects (→ pp. 104–105).

Recommendations after a data leak

Regardless of the source and scope of a leak, all data obtained by criminals may be used to make future social engineering attacks more credible. After a leak, users may also experience an increase in unwanted e-mails, spam phone calls, or scam attempts. Criminals may also use the obtained data to gain access to various services, which is why it is important to carefully read security notifications received in applications, e.g. regarding login confirmations or transaction authorizations.

The mitigation approach depends on how and what data was leaked.

In the case of infostealer malware, it is recommended to:

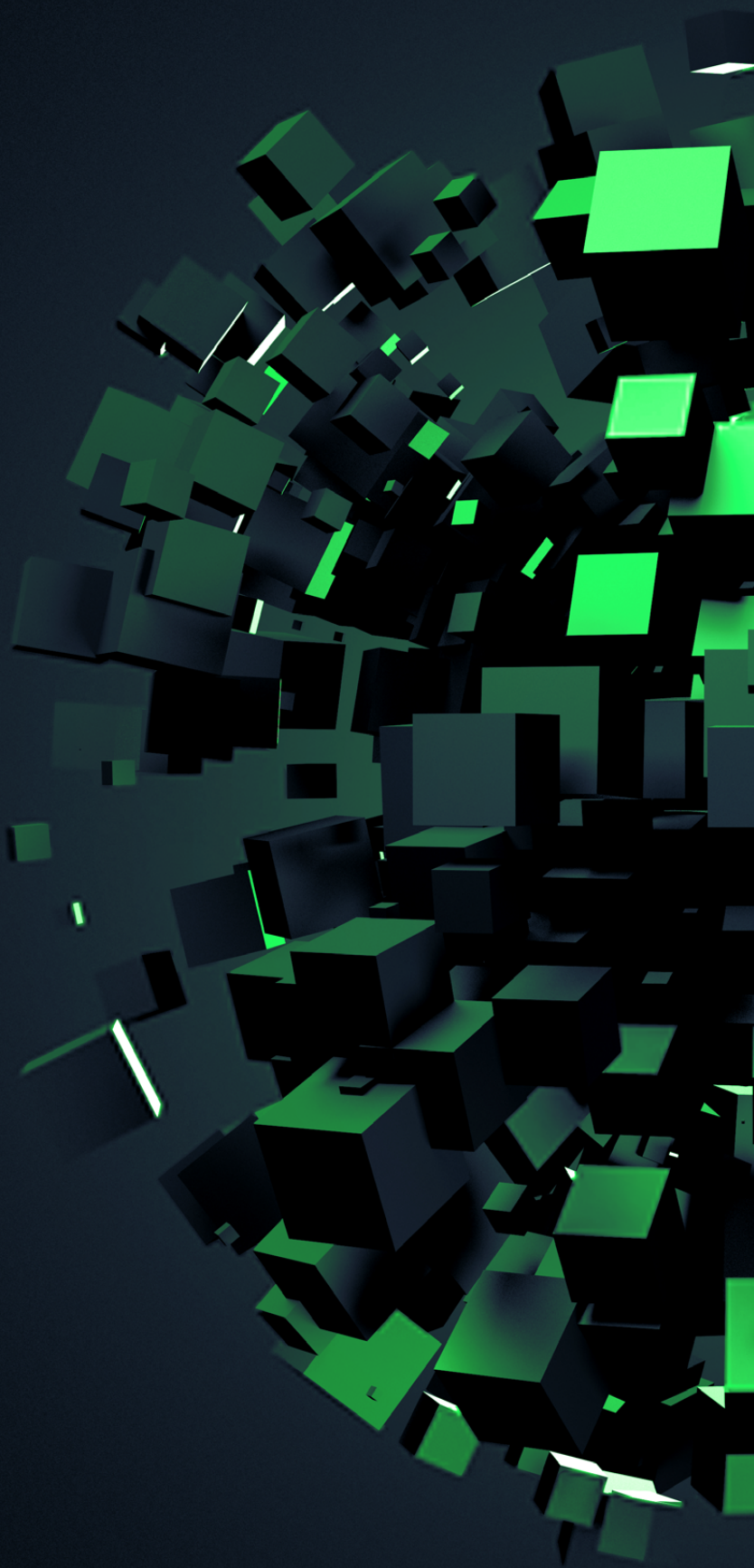
- mmediately change passwords for all services accessed from a potentially infected machine – these changes must be performed from a different, trusted system,
- change passwords everywhere the same credentials were reused,
- perform a full reinstallation of the operating system on the potentially infected machine.

In the case of phishing or a data leak from a third-party entity:

- if a password was leaked – immediately change it in the service and everywhere it was reused,
- if the PESEL number was leaked – register the PESEL number, which may help reduce the risk of misuse (https://www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie),
- if debit/credit card data (card number and CVV/CVC) was leaked – immediately block the card and contact the bank,
- if identity document information or a scan of an identity document was leaked – immediately block the document and obtain a replacement.

In addition – regardless of whether the data has already appeared in a leak or not – we recommend following proper password hygiene and using multi-factor authentication wherever possible. More information is available in our cybersecurity hygiene guide at: https://cert.pl/bezpieczne-hasla.

Activities of CERT Polska



The Warning List

In 2025, the Warning List set a new record. Hundreds of thousands of malicious domains blocked by CERT Polska demonstrate how important this tool is.

Currently, the second version of the Warning List is maintained. Domains are placed on the list for a period of 6 months from the moment of analysis, and if malicious content is still present, the domain is re-added to the list. Compared to the first version, in which domains were listed permanently, this approach helps reduce the size of the file and focuses on current threats and campaigns observed by our team. We observe that domains are used for a short time but at large scale. A proper implementation of the Warning List allows blocking such threats within 5 minutes of domains being added by our team.

Information about malicious domains is collected through several channels, one of the most frequently used still being number 8080. The ease of reporting by forwarding a suspicious SMS to this number makes it a frequently chosen method for submitting sites for analysis, especially those received via SMS. Reports of suspicious websites or e-mails are also submitted via the form available at incydent.cert.pl or through the mObywatel (mCitizen) application within the “Safe online” service. Based on data from these sources, our own data, and information provided by partners, and after our analysis, nearly 245,000 domains were added to the Warning List in 2025.

Ease of use combined with high effectiveness has made the Warning List widely adopted by users. We observe this in download numbers, which in 2025 reached nearly 1.3 billion, resulting in the blocking of approximately 141.1 million visits to malicious websites. This represents an increase compared to 2024 of 273% and 96.5% respectively.

We thank all reporters and continue to encourage the submission of suspicious links, domains, and SMS messages also in 2026.

SMS fraud

For years, one of the most popular ways of reaching potential fraud victims has been SMS messages. Each of us has a phone almost always with us, and we immediately react to most notifications, especially those from messaging apps. Most visits to phishing websites occur within 15 minutes of receiving a message. In such situations, we usually do not pay attention to who wrote to us, but instead start by checking “what was sent.” At the same time, the cost of sending a phishing message is negligible – about a few dozen groszy. It can therefore be easily calculated that a “return on investment” in the form of sending 10,000 SMS

messages requires deceiving just one person for PLN 1,000–2,000. Reports published by the NBP[36] show that the scale of financial losses is much greater.

SMS message reports

We have been closely examining the use of SMS messages for the distribution of fraud since the turn of 2020 and 2021. One of the tools used to monitor this phenomenon are the statistics we collect and present in annual reports. In April 2021, we began accepting reports of suspicious messages via a reporting channel. To simplify the reporting process, in November 2023 we launched a free short number 8080. This was made possible thanks to cooperation with the telecommunications market and the entry into force of the Act on Combating Abuse in Electronic Communications.[37]

So far, we have recorded record numbers of SMS reports every year, however 2025 brought a reversal of the upward trend. We received 295,169 reports of suspicious SMS messages, which represents a decrease of 16.8% compared to the previous year (354,566). An even more interesting situation concerns messages classified as malicious. In 2024 there were 140,659, while in 2025 this value (81,395) fell to a level comparable with 2022 (82,319). The comparison of the last quarters of recent years is also interesting. Until now, the number of frauds related to the "undelivered parcel" motif increased during the holiday shopping period. In 2022–2024, malicious messages accounted on average for 35.4% of all Q4 reports, while in 2025 this share was only 10.3%. This results from the occurrence of factors described below.

Blocking malicious SMS messages

The Act on Combating Abuse in Electronic Communications was adopted, among other reasons, to provide public institutions with tools to combat this type of threat. One such tool is the mechanism for blocking SMS messages.

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. 2025 was the first year in which

36 https://nbp.pl/system-platniczy/dane-i-analizy/transakcje-oszukancze

37 https://orka.sejm.gov.pl/proc9.nsf/ustawy/3069_u.htm

telecommunications operators blocked messages throughout the period from January to December. Based on the previously presented statistics regarding the number of reports alone, we can conclude that the blocking system may influence the use of SMS messages for fraud distribution.

In 2024, we created 746 templates, which resulted in 1,475,678 blocks.[38] In 2025, 790 templates led to the blocking of 1,883,610 malicious SMS messages. This statistic shows the growing effectiveness of the system – in its first year of operation, it resulted in an average of 1,978 blocked fraud attempts per template, while in the past year this increased to 2,384 thwarted attempts.

A key factor in counteracting fraud is response time. Requests to send several or a dozen thousand messages usually take up to 30–40 minutes. For this reason, 10 templates may result in fewer blocks than a single one created after receiving only a few reports. Therefore, we are continuously developing our analytical system: in 2024, each reported malicious message resulted on average in 24 blocks. In 2025, we managed to maintain this ratio at the level of 23 undelivered messages. Once again, the record month was November – 84 blocks per smishing report.

SMS campaigns

In 2025, we observed a progressive shift in scam scenarios using SMS messages. The statistics cited earlier already suggested that the popularity of parcel-related narratives had decreased. This applies to the entire group of messages containing a link to a phishing website. At the same time, we are recording an increasing proportion of scams in which SMS is merely an encouragement or bait to establish contact. Such a motif appears, for example, in alleged messages from a child about a damaged phone or SIM card and the need to contact them via another messenger, in fake SMS messages containing information about profits on our currency/investment account, or a notification of a login attempt on our cryptocurrency account.

Some of these changes can be attributed to the mechanism for blocking suspicious SMS messages – it is significantly easier for us to recognise smishing containing a link thanks to analysis based on whether a website address is included on the Warning List. As a result, blocking templates for messages containing links are created somewhat faster. Another reason is that fraudsters adapt very quickly to current trends. An example is the exploitation of the investment boom in recent years. Criminals select appropriate scenarios to increase the likelihood that the recipient will have

38 Data on blocked SMS messages are estimated based on reports submitted by telecommunications operators, taking into account the proportional share of these operators in the mobile telephony market..

a familiar reference point for the message they receive. In the vast majority of cases, these are not personalised scams; instead, criminals benefit from the scale effect. Therefore, it is always worth asking yourself whether the parcel we are waiting for is really being delivered by the courier company that is contacting us, why an advisor or exchange is sending an SMS instead of a notification in an app, or why our child did not ask a teacher to inform us about an incident – or whether we even have a child at all.

We continue to encourage support in the fight against smishing by sending messages to number 8080. This is not only a way to obtain an answer to the question "Is the message malicious?," but also a way to protect other users. In this process, response time is of greatest importance, therefore we ask that suspicious content be reported without hesitation.

Coordinated vulnerability disclosure

In 2025, CERT Polska achieved significant results in the area of coordinated vulnerability disclosure. We published 165 CVE identifiers, of which 8 vulnerabilities were discovered through in-house research. Activity in this area is an important operational pillar of the team in the context of implementing the requirements of European legislation, in particular the NIS 2 Directive and the CRA Regulation, which define new obligations for entities participating in the vulnerability management ecosystem.

CNA activities

Since August 2023, CERT Polska has held CNA (CVE Numbering Authority) status and remains the only entity in Poland authorised to assign identifiers within the CVE (Common Vulnerabilities and Exposures) programme, which is the global standard for numbering and cataloguing software vulnerabilities. In the first operational year (August 2023 – July 2024), CERT Polska published 73 CVE identifiers. We are systematically increasing our experience, gaining the trust of security researchers, and strengthening contacts with software manufacturers, which enables more effective handling of subsequent vulnerabilities submitted to us for coordinated disclosure.

The year 2025 brought a significant increase in activity: a total of 165 CVE identifiers published by CERT Polska represents a doubling of previous output and reflects the growing number of vulnerability reports coming both from external researchers and from the team's own research findings.

TABLE 3. Published CVE identifiers from January to December 2025

Month of 2025	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII	Total
Number of published CVE identifiers	4	9	11	15	22	3	6	36	16	12	21	10	165
Based on own research by CERT Polska	0	0	0	0	0	0	0	0	7	1	0	0	8

The number of vulnerability disclosures published in a given month varies, as reported cases may concern a single or multiple flaws within the same product. In 2025, our record in terms of volume was a set of 17 vulnerabilities in CGM CLININET, published on 27 August 2025. As a result, this month became the most active in terms of disclosed vulnerabilities.

The most significant vulnerabilities disclosed with our assistance included:

- CVE-2025-7063 and 8 other CVEs in PAD CMS software enabling, among other things, password changes for any user. In response to the identified threats and the lack of further support for the product, the Government Plenipotentiary for Cybersecurity issued a recommendation to discontinue the use of this software.
- CVE-2025-9313 in Asseco Poland S.A. mMedica software enabling unauthorized access to the database,
- CVE-2024-8773 and CVE-2024-8774 in SIMPLE.ERP software enabling privilege escalation to database administrator,
- CVE-2025-10910 in Govee network-enabled products enabling takeover of the device.

The process of our team's research on CMS software for Public Information Bulletins has been described in a separate article (→ p. 92).

An example of a vulnerability disclosure coordinated by us that was widely discussed in the industry is CVE-2025-4049 in SIGNUM-NET's FARA software. The controversy arose from the manufacturer's questioning of the existence and detection method of the reported vulnerabilities. Our subsequent investigation confirmed the reported flaws, which prompted the manufacturer to take remedial action.

However, the most difficult cases from our perspective remain those where, despite multiple attempts to contact the software manufacturer, we receive no response and the vulnerabilities remain unpatched. In the past year, this issue affected many reported vulnerabilities:

- CVE-2025-22270 and 4 other CVEs in CyberArk Endpoint Privilege Manager software,

- CVE-2024-13892 and 2 other CVEs in Smartwares CIP-37210AT and C724IP cameras,
- CVE-2025-2098 in Fast CAD Reader software by Beijing Honghu Yuntu Technology,
- CVE-2025-3758 and 1 other CVE in Netis Systems WF2220 software,
- CVE-2025-53811 in Mosh-Pro application for macOS operating systems,
- CVE-2025-7761 in Akcess-Net Lepszy BIP software,
- CVE-2025-54172 and 14 other CVEs in OpenSolution software: Quick.CMS, Quick.CMS.Ext, Quick.Cart,
- CVE-2025-9983 in GALAYOU G2 cameras,
- CVE-2025-53701 and 1 other CVE in Vilar VS-IPC1002 cameras,
- CVE-2025-9977 in Times Software E-Payroll software,
- CVE-2025-65007 and 4 other CVEs in WODESYS WD-R608U router software.

CERT Polska's operation as a CNA involves strict adherence to the guidelines of the international CVE programme. This means, among other things, that we may handle reports or document our own findings only for products that do not fall within the scope of responsibility of other CNAs – in such cases, we are obliged to redirect the reporter to the appropriate organization. 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.

CVE programme crisis

In April 2025, the CVE programme was affected by a serious funding-related crisis. The existing contract for the maintenance and development of CVE, carried out by MITRE on behalf of the U.S. government agency CISA, expired on 16 April 2025. This created a real risk that the database, developed over 25 years, would stop being updated, which could have led to chaos in the global vulnerability management ecosystem. At the last moment, CISA announced an extension of the CVE programme maintenance contract to avoid a break in service continuity.

Such disruptions would have affected national vulnerability databases, software development tools, and incident response systems. In the short term, this would have prevented the reservation and publication of CVE entries, leading to chaos in vulnerability communication. In the longer term, decentralised and competing databases would have emerged, and trust in the global registry would have been undermined.

The crisis highlighted a structural weakness in the programme's dependence on a single source of funding. In response, several initiatives emerged aimed at supporting the long-term stability of the vulnerability management ecosystem. Examples include the establishment of the CVE Foundation to increase the independence of the CVE programme, ENISA's acceleration of the publication of the European Vulnerability Database (EUVD), and the decentralised Global CVE (GCVE) identification system proposed and developed by the CIRCL (Computer Incident Response Center Luxembourg) team.

Expected legal changes

A key element for the area of coordinated vulnerability disclosure is the legal framework, which originates from the NIS 2 Directive (Network and Information Security Directive 2), adopted by the Council of the EU on 28 November 2022. The implementation of the Polish transposition has been delayed, and the deadline for transposition into national law passed on 17 October 2024. According to the amendment to the Act on the National Cybersecurity System, our team is designated as the coordinator of the vulnerability disclosure process.

The year 2025 was a period of preparation for the implementation of the European Union's Cyber Resilience Act (CRA), primarily concerning manufacturers of products with digital elements. Provisions in Chapter IV of the CRA (Articles 35–51) will apply from 11 June 2026, while those in Article 14 (defining manufacturers' obligations regarding vulnerability and incident reporting) will apply from 11 September 2026. The remaining provisions of the CRA will apply from 11 December 2027. Manufacturers will be required, among other things, to ensure that their products do not contain actively exploited vulnerabilities, to document software components used in a product through a Software Bill of Materials (SBOM), to maintain a coordinated vulnerability disclosure policy, and to promptly report incidents and actively exploited vulnerabilities to the designated CSIRT team.

Reporting and information exchange will take place via a newly established single reporting platform (SRP), which is expected to be made available by ENISA by 11 September 2026. The CERT Polska team actively participates in all phases of the design and consultation of the new platform. We also took part in consultations on the delegated regulation published by the European Commission on 11 December 2025. It supplements the CRA with conditions allowing the delay of information sharing between authorised CSIRTs. Among the reasons justifying such a delay are situations where the information enables easy re-exploitation of a vulnerability, the reported vulnerability is still under a CVD process, or one of the other CSIRTs is affected by an incident compromising the confidentiality of the shared information.

Role of CERT Polska in the CVD ecosystem

CERT Polska actively participates in international initiatives related to coordinated vulnerability disclosure. We are engaged in the work of the CSIRTs Network – we participate as co-leaders in the activities of the Working Group on Coordinated Vulnerability Disclosure (WG CVD). The group's work focuses on harmonising CVD procedures and policies within the European Union.

In addition, in 2025 we were invited to join the Global Community of Practice on CVD (CoP CVD), a forum established by CISA. This initiative aims to promote cooperation between governmental entities involved in the vulnerability disclosure process, as well as to enable the exchange of experience and the development of best practices.

In 2025, we also shared our experience in coordinated vulnerability disclosure, among others during workshops for software manufacturers in the healthcare sector in Poland, as well as for representatives of government organisations and critical infrastructure entities in Kosovo.

#BezpiecznyPrzemysł (#SafeIndustry)

In 2025, we continued the #BezpiecznyPrzemysł (#SafeIndustry), aimed at raising the level of cyber security of Poland's industrial infrastructure. We focus on identifying industrial devices accessible from the public internet, such as PLC controllers and HMI operator panels, and on informing owners about risks arising from improper configuration of these devices. Thanks to our proprietary Snitch system (details on p. 107), which we continuously improve, the visibility of scanned devices increased, as did the efficiency of the monitoring and decision-making process, thereby reducing incident response time.

Events

Water treatment plant

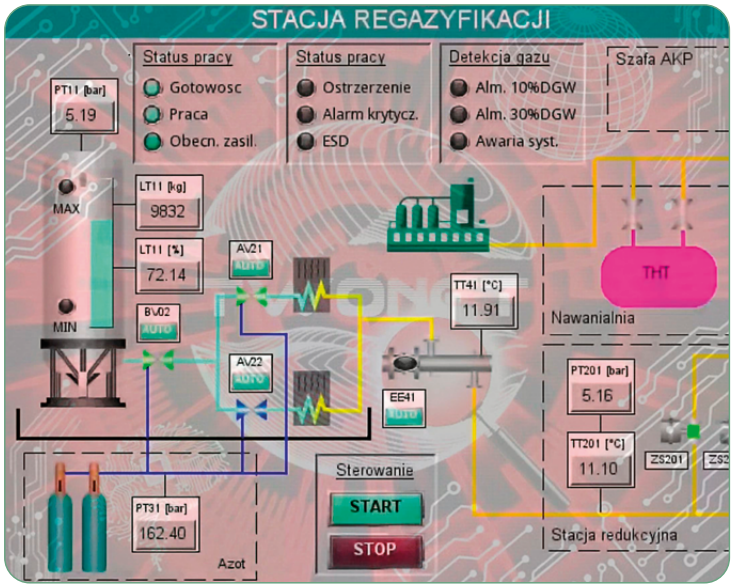
As a result of logging into the water treatment plant's devices, hackers changed pump settings, which led to depletion of the tank's resources and, consequently, caused a disruption in water supply. After regaining access to the control panels, the values were restored to their proper state, and once the tanks were refilled, water supply was restored.

The incident caused a water supply outage lasting approximately 6 hours for around 2,500 residents of the municipality.

Regasification plant

A regasification plant is a medium-sized installation that converts liquefied natural gas (LNG) back into gaseous form, enabling its further use in gas networks and industrial installations. A hacktivist group published a recording on the Telegram messaging platform showing how it changed operating parameter settings.

FIGURE 31. Screenshot from a recording in which a hacktivist group changes operating parameter settings of a regasification plant



Remote desktop

In 2025, we continued the initiative of checking default passwords for the VNC remote desktop. The VNC protocol is an easy attack vector due to its archaic authentication mechanism or its complete absence. This is further compounded by the common practice of setting very simple passwords such as: 111111, 12345678. Attacks on HMI panels are highly public and visually striking due to the ability to document successful logins to management panels. Among attackers exploiting weaknesses in the VNC protocol, we observed hacktivist groups.

In 2025, we expanded our login attempts to panels with new passwords, and in cases of systems attacked by hacktivists, we supplemented our test database with passwords used after obtaining them from administrators. Our observations show that the VNC protocol is most commonly used by:

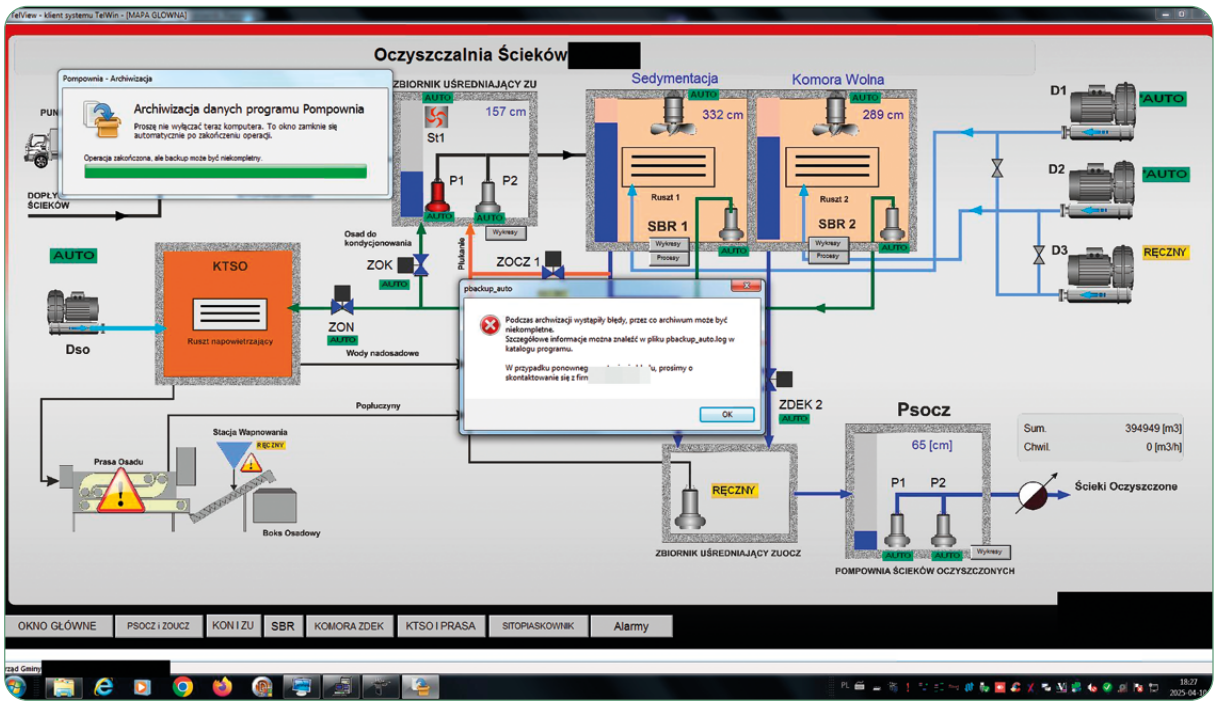
- small hydropower plants,
- wastewater treatment/pumping stations,
- Building Management Systems (BMS), e.g. in hospitals or private homes,

- HVAC (heating, ventilation, air conditioning), e.g. in shopping malls, discount stores, large-scale facilities,
- management panels of swimming pool installations (e.g. hotel pools, public swimming pools).

When information about system's presence is obtained, the team contacts the responsible entity, sends notifications, and forwards the information to the appropriate CSIRT.

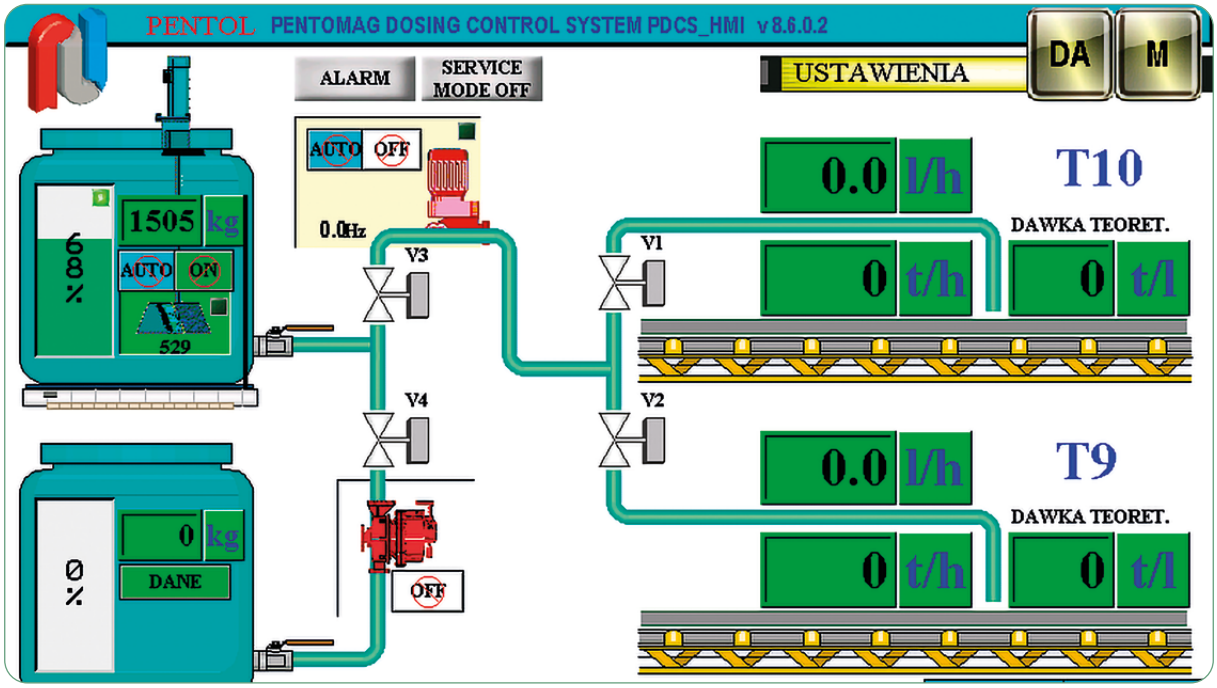
FIGURE 32. Panel of one of the water treatment plants in which operating parameter settings were changed

FIGURE 33. Panel of a municipal wastewater treatment plant to which we gained access using a simple password



Among non-standard cases, we observed a control system for dosing the PentoMag agent, which is a special fuel additive used to prevent corrosion and ash deposition in boilers, engines, or turbines.

FIGURE 34. Control system for fuel additive dosing



Web application audits

The Security Testing Team operating within CERT Polska carried out a series of security audits in 2025, 72% of which involved penetration testing of web applications. The aim of the conducted research was to identify vulnerabilities which, if exploited, could pose a threat to individual components or entire information systems.

All penetration tests were carried out using our proprietary audit methodology. Depending on the scope and nature of the assessment, we applied appropriate strategies and testing techniques, and test scenarios were developed based on the team's audit experience as well as established industry patterns and standards, such as the Open Web Application Security Project (OWASP) guidelines.

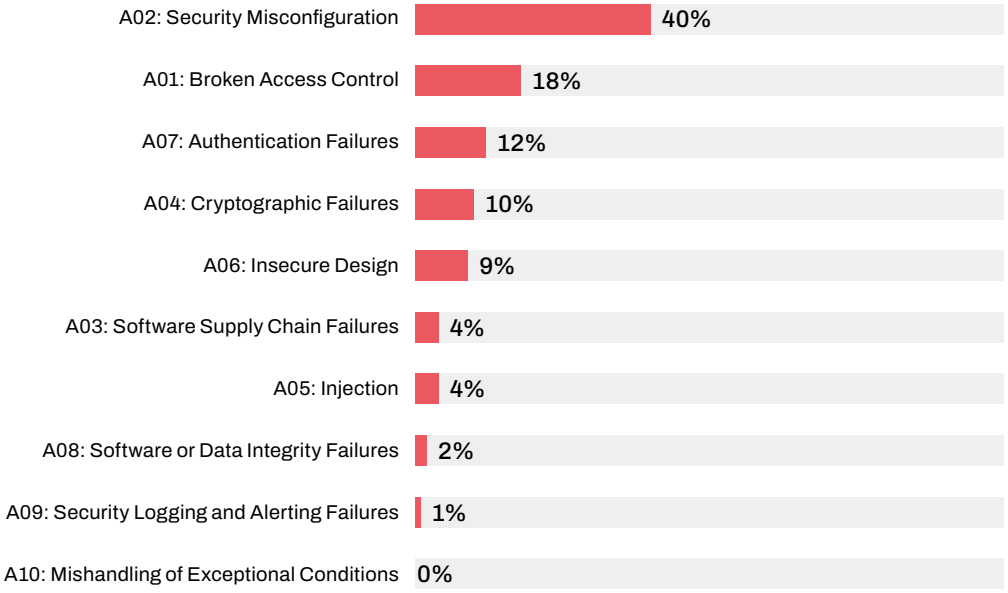
The key elements of the adopted methodology included:

- analysis of system architecture and identification of potential threats,
- manual testing supported by automated tools,

- preparation of audit reports presenting results with consideration of the severity level of identified vulnerabilities,
- formulation of recommendations tailored to the specific characteristics of the tested system.

For vulnerability classification, we used the OWASP Top Ten 2025 standard.

CHART 2. Chart showing vulnerabilities by category



The results of the conducted audits made it possible to identify areas requiring particular attention and remediation measures. The vast majority of detected vulnerabilities were identified in four categories, described below.

- A02 – Security Misconfiguration (incorrect configuration of systems and services): approx. 40%. These vulnerabilities most often resulted from incorrect configuration of system components and could lead to unauthorised access to resources or privilege escalation.

- A01 – Broken Access Control (improper access control): approx. 18%. These vulnerabilities indicated flaws related to improper management of access to data, increasing the risk of unauthorised disclosure or modification.

- A07 – Authentication Failures (improper implementation of authentication mechanisms): approx. 12%. This category included errors in the area of authentication, including improper session management, insufficient user identity verification, and weak password policies.

- A04 – Cryptographic Failures (incorrect implementation of cryptographic solutions): approx. 10%. These vulnerabilities concerned, among others, the use of outdated cryptographic algorithms, improper key generation, and inadequate storage of cryptographic materials.

Collectively, the above categories accounted for approx. 80% of all detected vulnerabilities, clearly indicating areas requiring priority remediation actions.

The analysis also showed that a smaller proportion of vulnerabilities fell into the following categories:

- A06 – Insecure Design (security-related design flaws): approx. 9%,
- A05 – Injection: approx. 4%.

This means that in the tested systems, issues related to security design flaws and classic injection-based attacks (e.g. SQL Injection) occurred relatively rarely. However, it should be emphasised that these vulnerabilities may lead to severe consequences such as bypassing security mechanisms, privilege escalation, or unauthorised access to data. In particular, injection attacks enable code injection, allowing manipulation of data, execution of unauthorised operations, and, in extreme cases, takeover of the application server.

Despite their relatively low frequency, these vulnerabilities require continuous monitoring and remediation, as their potential impact on system security can be critical in nature.

The audit results confirm the validity of conducting regular penetration tests, which, combined with systematic implementation of recommendations, significantly reduce the risk of security incidents.

Security analysis of public sector mobile applications

The growing number of mobile applications used in the public sector creates significant challenges in ensuring their security. These applications are widely available to citizens and often process information identifying users and administrative personnel, which increases the requirements for confidentiality and data integrity protection. At the same time, limited organisational resources make it difficult to conduct full-scale manual security testing for each application.

The response to these needs is the developed tool Deckard, whose purpose is to streamline the mobile application security analysis process by automating selected tests and standardising the collection and presentation of results.

Scope of the analysed material

As part of the project, we conducted an analysis of 283 Android mobile applications included in the "Register of mobile applications of public entities" published on the dane.gov.pl portal[39], based on the state of the register as of July 2025.

The analysed applications represent various areas of public sector activity, including public administration, healthcare, education, transport, culture, waste management, media, and agriculture. The collected dataset constitutes a representative sample of mobile applications provided by public entities.

Analysis method and assumptions of the Deckard project

The Deckard project is based on the guidelines of the OWASP Mobile Application Security Testing Guide (MASTG) and the OWASP Mobile Application Security Verification Standard (MASVS). For the purposes of automation, we extracted a set of checks identified as a baseline security level, common to all types of mobile applications, regardless of their functionality or business model.

The list includes security issues that are commonly found in mobile applications and can be detected automatically with a high level of confidence. They constitute the fundamental security requirements for mobile applications.

The baseline set of vulnerabilities includes, among others:

- presence of debug mode in production builds,
- trust in user-added certificates,
- support for outdated operating system versions (minSdkVersion < 23),
- insufficient security when using WebView,
- storage of cryptographic keys in the code,
- use of outdated certificates (expired validity period),
- lack of APK integrity verification,
- use of unencrypted network communication.

Deckard performs analysis as a modular process in which individual stages use microservices running in a containerised environment. The tools used (including MobSF, JADX, and custom scripts) return results in a unified format, enabling further automated aggregation and report generation.

39 https://dane.gov.pl/pl/dataset/1875,wykaz-adresow-stron-internetowych-i-wykaz-aplikacji--mobilnych-podmiotow-publicznych/resource/65295

Security vulnerability classification

The identified issues were grouped into thematic classes of findings, allowing for a more general and readable presentation of the analysis results for reporting purposes. Below we describe the types of errors identified during the analysis.

- Runtime environment configuration issues – these result from incorrect configuration of the application in the production environment, in particular leaving debugging mechanisms enabled or the absence of basic platform security controls.

- Unsecured network communication – issues related to improper handling of network protocols and TLS. These include, among others, acceptance of user-added certificates, faulty SSL error handling, or the absence of a defined list of certificates that the application may trust. As a result, data transmitted between the application and the server may be intercepted or modified.

- Cryptographic and key management issues – these concern improper use of cryptographic mechanisms, such as weak algorithms, insufficient key lengths, or storing cryptographic keys directly in the application code. These issues affect the confidentiality and integrity of processed data.

- Application integrity and resistance to manipulation – these are issues related to the lack of mechanisms protecting the application against modification, code substitution, or analysis. They include, among others, the Janus vulnerability (CVE-2017-13156), lack of modern APK signing schemes (v2/v3/v4), and absence of mechanisms hindering reverse engineering.

- Attack surface exposure and inter-component communication – these relate to excessive exposure of application components, lack of input validation, and insecure inter-process communication (IPC) mechanisms. These issues increase the attack surface and may lead to unauthorised access to application functions or user data.

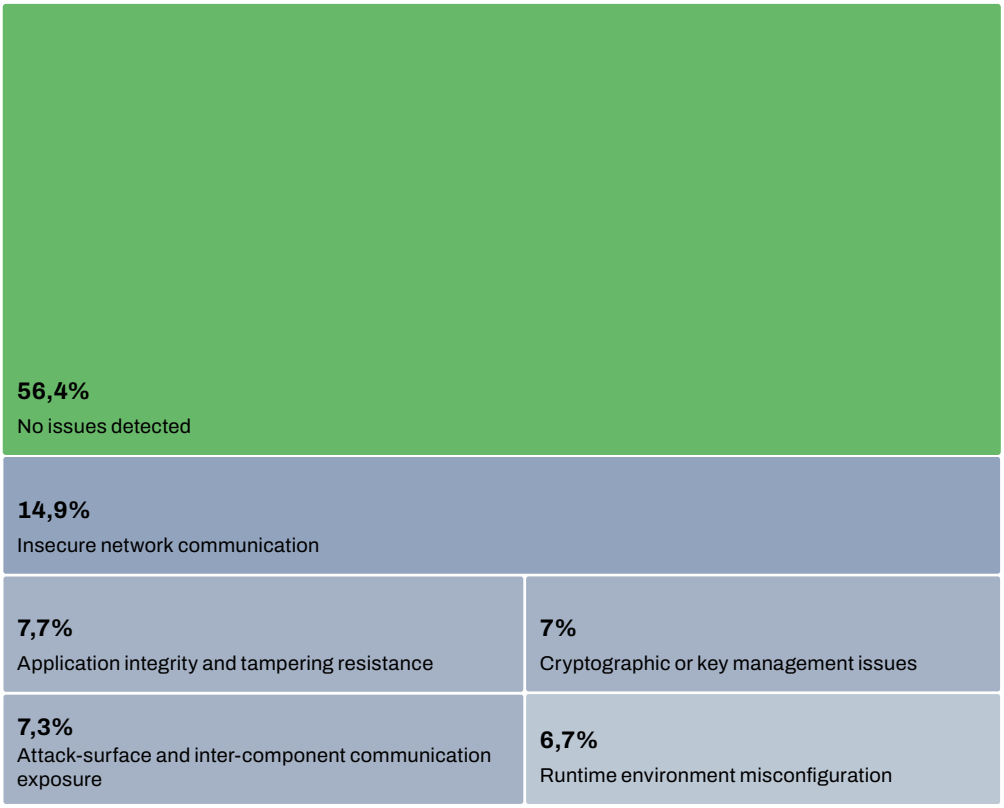
Statistics of detected security vulnerabilities

As part of the quantitative analysis, we determined the frequency of occurrence of individual classes of security findings in the analysed set of mobile applications. The results of the statistical analysis were presented in two complementary charts showing:

- the structure of all test results,
- the frequency of occurrence of vulnerabilities in applications.

The first chart presents the distribution of all executed test results, regardless of whether a given check resulted in a detected issue or not.

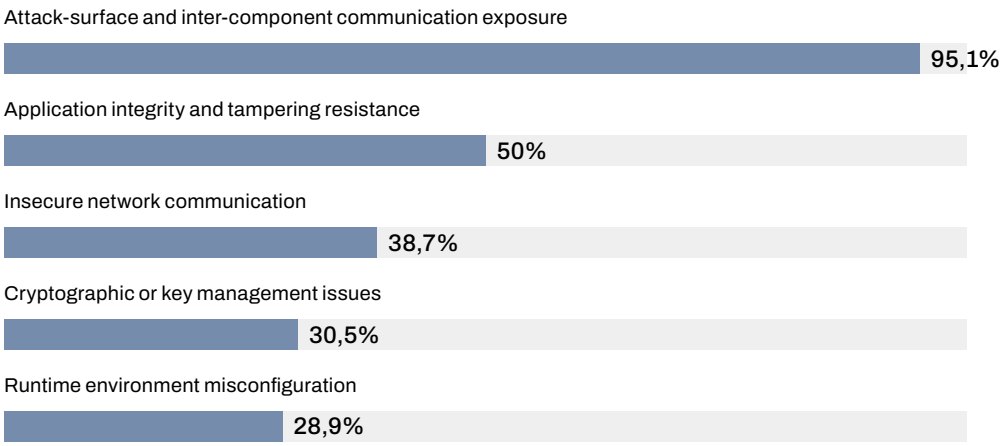
CHART 3. Structure of all test results



Each test result was assigned to a vulnerability category or marked as a negative result, not classified as a security vulnerability. From this perspective, approx. 56.4% of all executed checks resulted in a negative outcome. The largest share among detected issues was represented by findings in the area of insecure network communication (14.9%), while the remaining categories reached values of approx. 6–7%.

The second chart presents the percentage of applications in which at least one finding from a given category of issues was detected.

CHART 4. Frequency of vulnerabilities in applications



The results indicate that the highest proportion of applications contained findings related to attack surface exposure and inter-component communication (95.1%) and integrity and resistance to manipulation (50%). The remaining categories were also present in a significant share of the analysed applications (insecure network communication – 38.7%, runtime environment configuration issues – 28.9%).

The presented statistics include only those classes of vulnerabilities that have been implemented in the Deckard system at its current stage of development. With further expansion of the tool's functionality, an increase in the number of detected findings and a more complete picture of the security level of the analysed applications is expected.

Conclusions and directions for further development

The work carried out to date on the Deckard project confirms the validity of using automation in the initial security analysis process for mobile applications in the public sector. The applied approach enables rapid detection of repetitive, baseline security flaws and organizes results in a consistent and scalable manner.

In the next stages, we plan further development of the tool by expanding the scope of supported OWASP MASTG tests, increasing coverage for both static and dynamic analysis, and integrating results with vulnerability management systems. Deckard constitutes a foundation for building a standardized process for assessing the security of mobile applications in the public sector, enabling effective risk management across the entire digital services ecosystem.

Locked Shields 2025

From 6 to 9 May 2025, the 15th edition of Locked Shields took place – the world's largest cyber defence exercise, organised by NATO's Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE). It brought together 41 countries divided into 17 teams. The task of more than 4,000 specialists in incident response, law, and communications was to defend the fictional state of Berylia against attacks from the adversary "Crimsonia", created for the purposes of the exercise.

The scale of the four-day exercise required close cooperation from participants, which closely reflects the conditions of a real attack. In addition, each team consisted of representatives from at least two NATO member states, which also allowed for comparison of procedures and response scenarios to threats.

In the Locked Shields 2025 edition, the Polish team, led by an officer from the Cyber Defence Forces Command (DKWOC), joined forces with representatives of France from the Commandement de la cyberdéfense (COMCYBER). With a significant contribution from CERT Polska experts, we once again reached the podium – this time taking second place. We ranked between the winning team of Germany and Singapore and the joint operation of Italy, Slovenia, and the United States.

Protecting the infrastructure prepared for the exercise was not easy – each team had to secure more than 8,000 systems under its responsibility. The scenario involved near-continuous escalation – from disinformation activities, through data leaks and malware propagation, to direct attacks on energy grids, communications infrastructure, and air defence systems. Incident mitigation was only one aspect of defence – equally important were strategic communications directed at the population of Berylia and continuous analysis of the legal aspects of undertaken actions.

Year by year, the complexity of challenges prepared for Locked Shields increases in line with the most current trends in cyberspace. In 2025, we observed a significant rise in the role of artificial intelligence in both offensive and defensive processes, an increasing importance of cloud infrastructure, and the first consideration of quantum computing issues. All of this took place under constant time pressure, stress, and competition. To reflect reality as closely as possible, political pressure elements were also introduced, and the exercise scenario included geopolitical tensions and violations of state sovereignty.

The purpose of exercises such as Locked Shields is to test states' readiness to deal with the challenges of a changing world and cyberspace, but also – and perhaps above all – to build mechanisms of mutual trust, support, and information sharing, which in the face of real threats will be crucial for the NATO community to effectively repel hostile actions. Polish cyberspace

is protected by hundreds of specialists who are willing and able to cooperate. This was the case during Locked Shields under the leadership of DKWOC, when CERT Polska experts were responsible, among others, for protecting special systems, networks, web applications, and legal matters, and it is also the case on a daily basis, when Polish institutions share responsibilities within their constituencies, exchange information and experience, and provide operational support to one another.

Research on CMS software for Public Information Bulletins

Content Management Systems (CMS) enable convenient operation of websites; however, the presence of vulnerabilities in such software means that many websites may become targets of attacks. Some of these systems are used to operate Public Information Bulletins (BIP). We receive a significant number of vulnerability reports in CMS systems; therefore, in 2025 we additionally tested some of these solutions as part of our own activities.

Public sector entities are required to maintain Public Information Bulletins, and many of them choose ready-made solutions dedicated to this purpose. As our observations show, there are products whose developers do not ensure the security of their systems, particularly in terms of implementing patches addressing reported vulnerabilities.

We contacted the vendors of selected solutions and received software for testing. We were able to verify security on isolated instances not used in production; in some cases, we also had access to the source code. This allowed us to test the products for the presence of the most common threats. However, it should be noted that the tests we conducted do not guarantee detection of all vulnerabilities. In addition, updates released by developers may introduce new vulnerabilities in the future.

In 2025, CERT Polska assigned 43 CVE identifiers for vulnerabilities in CMS-class programs used to maintain Public Information Bulletins. Among the identified issues were, among others, authentication-related flaws (e.g. passwords stored in plaintext – CWE-256), lack of restrictions on file uploads (CWE-434), and improper neutralisation of input data (CWE-79). In the case of receiving information about critical vulnerabilities, the team identifies potentially affected instances and informs administrators about the risks associated with these security flaws.

Due to the high level of risk posed by vulnerabilities in PAD CMS software, the Government Plenipotentiary for Cybersecurity recommended discontinuing

the use of this product.[40] This is already the second recommendation concerning a BIP system, following the 2024 recommendation issued by the Government Plenipotentiary for Cybersecurity regarding Public Information Bulletins.[41]

Co-creation of sectoral CSIRT teams

In the past year, NASK – PIB established a partnership with the Polish Financial Supervision Authority[42] and the Ministry of Infrastructure[43] to support the development of sectoral cybersecurity teams. The initiative is funded by the Recovery and Resilience Facility and the European Union.

Development of CSIRT KNF

The CSIRT KNF team, established under the ordinance of the Chair of the Polish Financial Supervision Authority, has been operating since 1 July 2020 and performs tasks related to cybersecurity for entities in the financial sector. It is an important element in combating fraud targeting domestic users of financial systems. The key services of the team include monitoring vulnerabilities identified in the sector and mitigating their impact, as well as educational activities. The substantive role of CSIRT NASK in the project is to improve processes (review and assessment) and systems (security testing) of the partner. The aim is to achieve an advanced level of maturity for CSIRT KNF in accordance with the "ENISA CSIRT Maturity Framework".[44] Project work also focuses on the development of functionalities of the moje.cert.pl service, which is described in more detail in a separate article (→ pp. 104–105). Through the access interface, coordinated information flow regarding incidents requiring response will be possible. In addition, aggregated statistics on incidents affecting sector entities will be compiled, which will streamline and accelerate the process of assessing the overall risk level.

40 https://www.gov.pl/web/cyfryzacja/rekomendacja-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-zaprzestanie-korzystania-z-oprogramowania-pad-cms

41 https://www.gov.pl/web/cyfryzacja/rekomendacja-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-dotyczaca-biuletynow-informacji-publicznej

42 https://www.nask.pl/projekty/csirt-knf-budowa-i-rozwoj-sektorowego-zespolu-cyberbezpieczenstwa-dla-sektora-bankowego-i-infrastruktur

43 https://www.nask.pl/projekty/utworzenie-csirt-sektorowego-o-nazwie-roboczej-csirt-infrastruktura

44 https://www.enisa.europa.eu/topics/incident-response/csirt-capabilities/csirt-maturity

Establishment of CSIRT Infrastruktura

CSIRT Infrastruktura (Infrastructure) is a newly emerging unit whose formal establishment is planned for 2026. Its scope of activity will cover the transport sector as well as the supply and distribution of drinking water. The aim of the support provided by CSIRT NASK is to establish fully operational structures of the sectoral cybersecurity team and to achieve readiness to perform tasks arising from the Act on the National Cybersecurity System (KSC). The creation of a new unit of this type was also announced by the Ministry of Digital Affairs.[45] CSIRT Cyfra will be responsible for the digital infrastructure sector.

CERT Polska team recommendations for establishing CSIRT teams

In 2025, alongside the CSIRT KNF mentioned above, CSIRT CeZ was also operating in Poland for entities in the healthcare sector. It was established in January 2023. The amendment to the Act on the National Cybersecurity System (KSC) provides for a significant expansion of the list of sectors, as well as the mandatory establishment of sectoral CSIRTs by the competent supervisory authority. In response to current and future challenges faced by organizations responsible for establishing such units, the CERT Polska team published guidance recommendations[46] in August 2025. The document is intended to help decision-makers define the resources necessary to organize response teams in line with applicable industry standards, while also ensuring their smooth integration into the existing national system. A previous, non-public version of the recommendations had already been prepared with the development of sectoral CSIRTs in mind. The August 2025 publication can also be applied to other types of cybersecurity teams, including commercial ones such as CERTs, SOCs, or ISACs. We encourage stakeholders to take these guidelines into account when creating or developing cybersecurity teams.

ECSC 2025

The European Cybersecurity Challenge (ECSC) is an international cybersecurity competition organized by the European Union Agency for Cybersecurity (ENISA). Participants include national teams from European

45 https://www.gov.pl/web/cyfryzacja/ministerstwo-cyfryzacji-tworzy-csirt-cyfra--oto-wszystko-co-warto-na-ten-temat-wiedziec

46 „Rekomendacje zespołu CERT Polska dla ustanawiania zespołów CSIRT", https://cert.pl/posts/2025/08/rekomendacje-csirt

countries as well as invited teams from other states. Each team consists of 5 people aged between 14 and 20 and 5 people aged between 21 and 25.

National qualifiers

As in previous years, CERT Polska conducted national qualifications to select participants for the team representing Poland in the final competition. 2025 was a record-breaking year in terms of interest in the competition – 186 participants took part in the qualifiers, which is 30 more than the previous record. During the competition, participants had the opportunity to solve 22 tasks (including 4 designed for beginners starting their journey with CTF-style competitions). At least one "flag" confirming task completion was submitted by 177 participants, which was also a record result in the history of the qualifiers conducted by us.

Finals in Warsaw

The finals of the 2025 edition were exceptional – for the first time in ECSC history, Poland served as the host country. The event, organized by the National Research Institute NASK (together with CERT Polska) and the Ministry of Digital Affairs, took place on 6–9 October at the Torwar arena. Teams from 39 countries took part in the competition (including 5 guest teams).

On the first day, participants were able to familiarize themselves with the platforms used during the competition and test the correctness of the infrastructure. After this technical phase, the official opening ceremony took place, hosted by Gynvael Coldwind – one of the most recognizable figures in the Polish CTF community.

As in previous editions, the main competition consisted of two parts held on two consecutive days. It included the following formats:

- CTF Jeopardy – tasks of varying difficulty levels inspired by real cybersecurity problems,
- CTF Attack & Defence – a set of vulnerable services administered by each team, where the goal was to defend one's own services while attacking opponents' systems.

On the final day, the closing ceremony took place. The audience had the opportunity to listen to a "CTF Stories" presentation by Michał "Redford" Kowalczyk and a "Fun Facts" presentation covering interesting statistics and events from the competition, delivered by Louis Burda from Attacking-Lab (the group responsible for preparing tasks and technical support on the second day).

The final ranking was based on combined results from both competition days using a normalization formula. After the points were tallied, Italy

stood on the top step of the podium (also winning on each of the two days), followed by Denmark in second place and Germany in third. The Polish team finished the competition in 7th place, based on 10th place in the Jeopardy category and 5th place in the Attack & Defence category. In the ranking of guest teams, the United States team achieved the best result.

FIGURE 35. Polish team at the ECSC 2025 competition

FIGURE 36. Winners of ECSC 2025 – the Italian team

Polish Presidency of the Council of the European Union

From 1 January to 30 June 2025, Poland held the presidency of the Council of the European Union. The slogan of the Polish presidency, "Security, Europe!", was also reflected in cybersecurity matters, which were treated as a priority. The CERT Polska team actively participated in initiatives supporting the exchange of experience between EU Member States and strengthening the Union's resilience to cyber threats.

Increased engagement in European affairs

The Polish presidency was associated with intensified involvement of national institutions in decision-making and expert processes at the EU level. Particular attention should be given to co-creating and implementing solutions that enhance digital security, participation in legislative work, and active representation of Polish interests. The CERT Polska team participated in consultations, working groups, and initiatives aimed at building a common European resilience against cyber threats.

SECURE International Summit

One of the most important events of the Polish Presidency was the SECURE International Summit 2025 conference, held on 3–4 April in Bydgoszcz. CERT Polska played a central role in organizing and substantively preparing the event. The programme included panels on building EU cyber resilience, implementing the Cyber Resilience Act, challenges related to the development of AI and disinformation, and civil-military cooperation in incident response. More about this event is presented in a separate chapter (→ pp. 98–100).

Chairmanship of the CSIRT Network

In January 2025, a representative of CERT Polska assumed the role of Chair of the CSIRT Network. This responsibility includes representing the Network in external forums and coordinating activities related to its work, such as establishing response procedures, engaging in incident information sharing, and increasing the Network's activity. The chairmanship lasts one and a half years and involves cooperation within the so-called Trio, consisting of the three consecutive EU Council Presidency countries: Poland, Denmark and Cyprus.

CSIRT Network meeting in Kraków

In May 2025, Kraków hosted a regular meeting as part of the so-called CyberWeek, which brought together representatives of the CSIRT Network, CyCLONe, and other EU groups responsible for cooperation in the field of cybersecurity. The event provided an opportunity to exchange experience and discuss challenges arising from the implementation of new regulations, including NIS 2 and the Cyber Resilience Act. Participants also discussed the assumptions of the Cyber Blueprint document, which sets out a plan for coordinated response to large-scale cybersecurity incidents. The CERT Polska team, in cooperation with the AGH University of Krakow and the Ministry of Digital Affairs, was responsible for organizing the meeting.

Cyber Blueprint

During the presidency, the CERT Polska team worked closely with the Permanent Representation of the Republic of Poland to the European Union to effectively represent Poland's interests in legislative negotiations, expert knowledge exchange, and the promotion of Polish cybersecurity solutions at EU level.

We also participated in work on the Cyber Blueprint, a document defining a new framework for managing digital crises, adopted in June 2025. This document establishes common procedures for responding to major digital incidents in the European Union and serves as an important reference point in building the Union's digital resilience. The new version of the Cyber Blueprint is the first comprehensive update of the document since 2017. It includes practical and operational aspects, as well as changes resulting from the NIS 2 Directive and many other legislative acts. The full text of the document is available at: https://eur-lex.europa.eu/eli/C/2025/3445/oj/pol.

Supporting events

CERT Polska was actively involved in the exchange of experience between national and European institutions during workshops, panels, and expert sessions, as well as during key events of the Polish Presidency, such as the healthcare sector conference "Health Security – Challenges, Innovation, Future", held on 8 April in Kraków.

SECURE International Summit

On 3–4 April 2025, the SECURE International Summit took place in Bydgoszcz – a special edition of CERT Polska's flagship conference, organized in response to the need to strengthen international cooperation in cybersecurity.

Over 700 guests, more than 30 panels and presentations, and a wide range of experts made it the largest cybersecurity conference held within the Polish Presidency of the Council of the European Union. Participants engaged in discussions with national and international experts on initiatives, projects, best practices, and trends in cyberspace. Workshops were also an integral part of the event, allowing participants to develop practical technical skills.

European dimension of the meeting

The conference programme reflected the main cybersecurity priorities of Poland and the European Union. Among the speakers were international guests representing both European institutions and national authorities responsible for cybersecurity in Member States. Speakers included, among others: Christiane Kirketerp de Viron (European Commission), Hans de Vries (ENISA), Catherine Godin (Embassy of Canada in Poland), and Stefania Ducci (Italian National Cybersecurity Agency – ACN). The Polish government was represented by Deputy Prime Minister and Minister of Digital Affairs Krzysztof Gawkowski.

Discussions also addressed a future joint strategy for responding to cyber threats in the European Union. Such a strategy is necessary, as incidents pose a real and potentially large-scale threat. It is worth noting that the discussions held during SECURE influenced the final shape of regulations in this area. A few weeks later, a new version of the Cyber Blueprint was adopted – a response plan for major Europe-wide incidents. This is the first comprehensive update of the document since 2017.

More on this topic is covered in the chapter on the Polish Presidency of the Council of the European Union (→ pp. 96–98).

CERT Polska's annual report – a long-awaited premiere

Attacks, trends, tools. The premiere of the CERT Polska annual report has become a permanent part of the SECURE agenda. Marcin Dudek, head of our team, informed conference participants about the conclusions presented in the report, as well as the threat landscape in the Polish cyberspace over the past year. On the same day the report was distributed to conference participants, it was also published on the cert.pl website.

Diverse topics – one goal

The programme also included discussions on cybersecurity challenges related to the development of artificial intelligence, new legal regulations in this area, and issues concerning disinformation. The diversity of the agenda was intentional. We aimed to present content relevant to cybersecurity specialists in managerial, technical, and legal domains, as well as other stakeholders responsible for this area in public institutions and private companies.

The SECURE International Summit builds on a long-standing tradition – the SECURE conferences have brought together cybersecurity experts for over a quarter of a century. In the next edition of the event, planned for April 2026, we intend to return to the roots – the discussion will take place in Warsaw, and its focus will be primarily on technical topics.

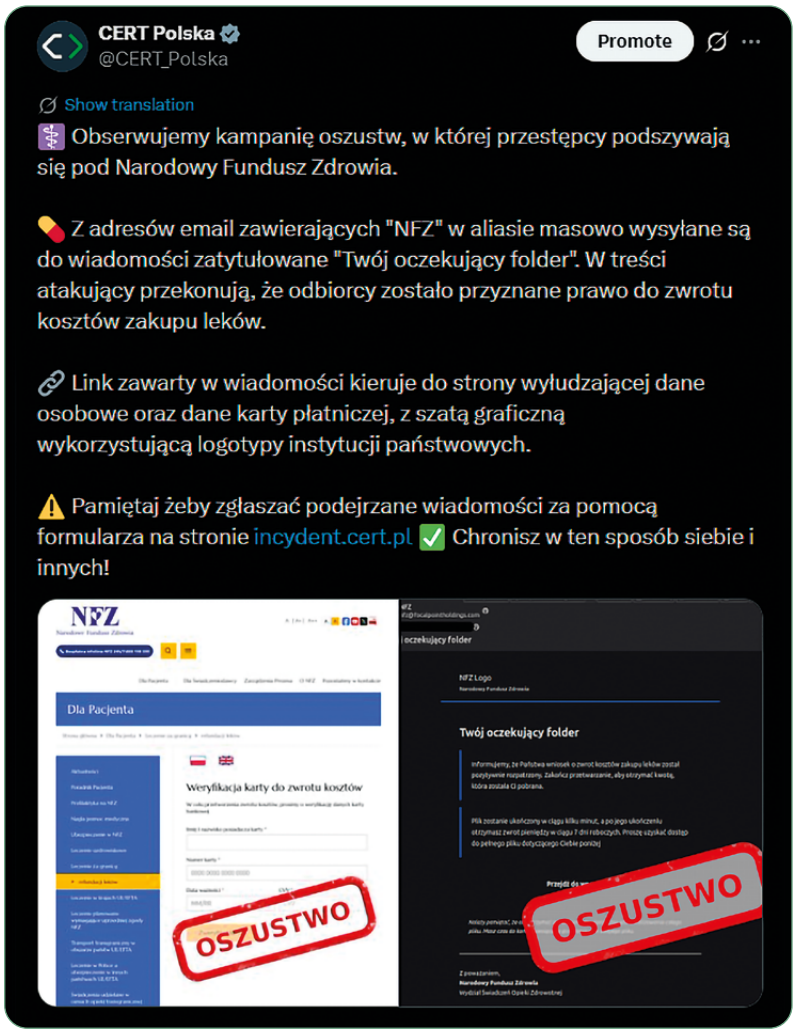
Cybersecurity education and promotion build awareness among Poles

Articles on educational activities in recent annual reports have traditionally begun by noting another record in the number of reported incidents and notifications. In 2025, it was no different – 658.3 thousand reports and 260.8 thousand incidents reflect the scale of the team's daily work. These figures show that the average monthly number of reports processed by CERT Polska in 2025 was nearly 55 thousand. This significant increase in awareness and willingness to report threats is also the result of educational and outreach activities. This includes both media campaigns and the presence of experts at industry events.

Social media – reaching audiences at scale

Our activity on social media has become essential, as we aim to bring cybersecurity content as close to users as possible. Key to building awareness of threats and the importance of reporting them are systematically published alerts. They cover the largest fraud campaigns and are published simultaneously on CERT Polska's profiles on Facebook, X, and LinkedIn. They are complemented by push notifications sent via the mObywatel application. These are part of the "Safe Online" service, which enables users to report incidents, receive notifications about current cyber threats, and, through articles on safe internet usage, continuously update their knowledge.

FIGURE 37. Warning published on X



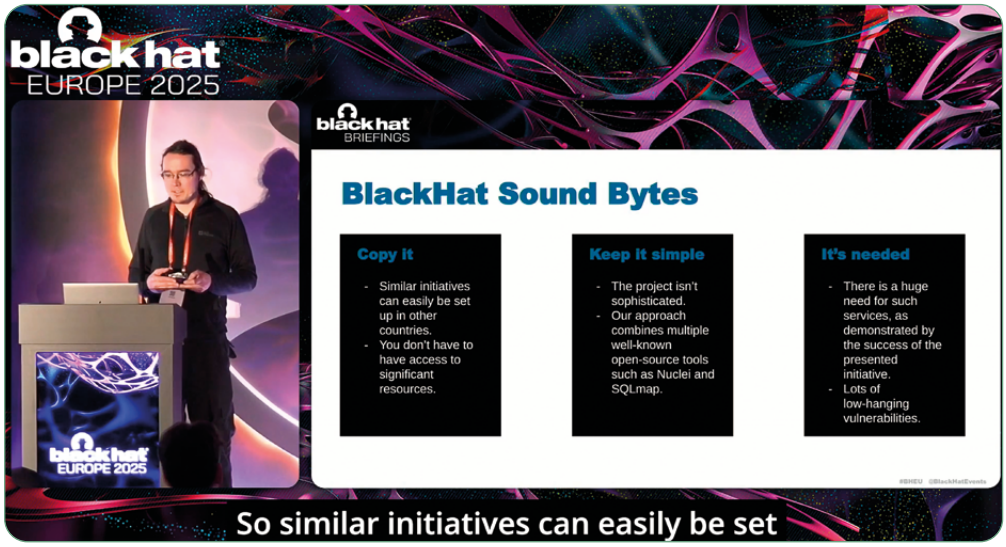
In addition to on-demand warnings, educational content is also published across social media channels. Once again, we offered users a series of holiday-themed posts. The #CyberPrezent (#CyberGift) consisted of 12 short texts covering security systems, current threats, and ways to prevent them. By addressing challenges such as data leaks and phishing, we provided readers with practical advice on how to deal with them.

Figure 38. Illustration used to promote the #CyberPrezent (#CyberGift) series on social media

Participation in conferences – building an expert reputation

We supplemented the educational activities mentioned above with our presence at key industry conferences such as Black Hat Europe in London and Oh My Hack in Warsaw. In London, Krzysztof Zając presented the moje.cert.pl service, while at OMH we discussed malware detection, the use of AI for vulnerability discovery, and fuzzing techniques. We also covered incident communication and large-scale website scanning. 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 39. Slide excerpt from Black Hat Europe conference presentation



In the context of competitions, the European Cybersecurity Challenge (ECSC) is particularly worth mentioning. Nearly 400 young people from around the world competed in Warsaw over two days for the title of best team. This prestigious event aimed primarily to strengthen international cybersecurity cooperation and promote the field among young people at the start of their career paths. The competition also aimed to increase defensive, educational, and innovation potential in this critical area. Through ECSC-related outreach activities, we sought to reach a broader audience, including youth, students, and professionals from other fields, emphasizing the importance of secure use of technology. More on ECSC 2025 is covered in the article on pp. 94–96.

Articles and media campaigns – a full spectrum of activities!

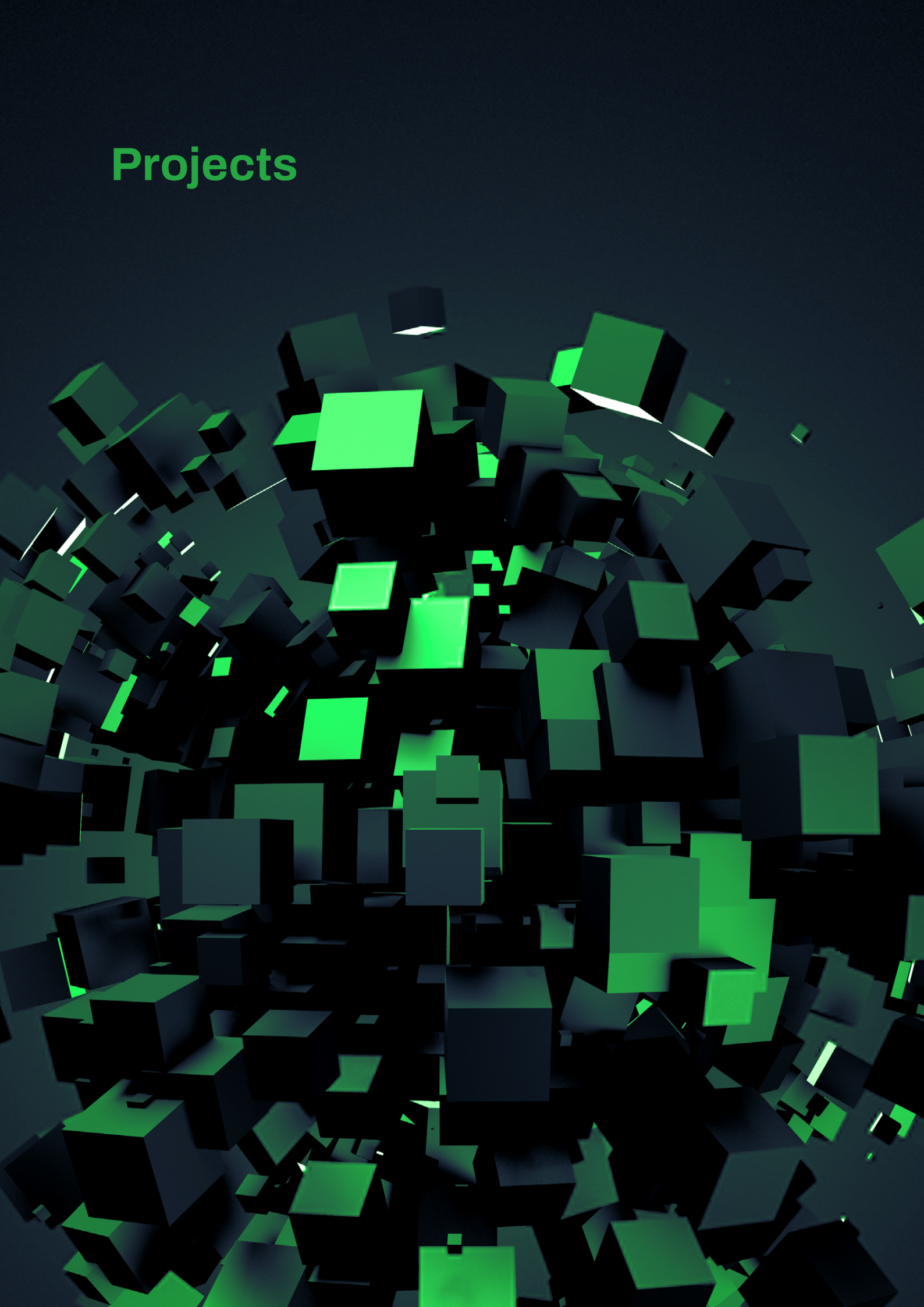
In the past year, we also published articles addressing current threats, including malware such as NGate, myths related to public Wi-Fi, and activities of APT groups such as UNC1151, which used a vulnerability in Roundcube to steal credentials.

We also highlighted CERT Polska's role and the importance of incident reporting during the nationwide media campaign "Safe Day". The TV campaign aired on major Polish broadcasters – TVP, TVN, and Polsat – starting on 8 May. The informational spot featuring Marek, who reports dangerous content to protect others, reached millions of viewers.

FIGURE 40. Excerpt from the "Safe Day" campaign advertisement

Emphasizing the importance of incident reporting is a key part of our overall outreach strategy. A higher volume of reports provides a more complete picture of what is happening in cyberspace and enables more effective action on our side. Such themes will continue in 2026, which is a special year for us. The CERT Polska team will celebrate its 30th anniversary, and we intend to highlight our achievements, present our tools and their impact. We therefore encourage readers to follow next year's report and our activities throughout 2026.

Projects



Moje.cert.pl

On 12 February 2025, CERT Polska made moje.cert.pl, available to the public. In this portal, any registered user – from the owner of a niche blog to the administrator of many websites and systems in a large institution – can easily increase the cybersecurity of their domains and networks.

After the user has entered information about their domains and networks, and it has been verified that the user owns them, the user is presented with information about vulnerabilities, ranging from the low-risk ones, such as misconfiguration of SSL/TLS, to the very serious ones, such as the possibility of remote code execution. In addition, the moje.cert.pl portal automatically notifies of password leaks, including those caused by malware stealing passwords from a user's computer, and provides the ability to download information about various network incidents, for example, when a server becomes part of a botnet or shares malicious content.

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 system (for more information, see pp. 105–107), which detects a large number of vulnerabilities and misconfigurations affecting security. Network incidents are retrieved from the n6 system (for more information, see pp. 124–140). Further, data on password leaks posted in the moje.cert.pl system comes from commercial sources, and is enriched with collections from CERT Polska's own operational activities and those of other CSIRT teams, such as CSIRT KNF.

The portal provides up-to-date warnings addressed to Internet administrators and users about threats in the Polish cyberspace. The communications include, among other things, descriptions of ongoing campaigns run by criminals and vulnerability alerts. This content can be accessed by all interested parties, not just those registered with the service. Moreover, everyone can also receive these communications via e-mail.

The moje.cert.pl service is developed in an agile manner. The version that was made available to users in February 2025 was not the final one. The service was made public shortly after the launch of the test version, so we were able to verify quite quickly whether it was responding to users' needs and also to find out what changes should be introduced. This ensured that further development of the project took into account the needs reported by users for both improvements and new features of moje.cert.pl.

In 2025, as part of the project development, we added (among other things):

- the publication of security advisories and their delivery via e-mail, as well as the possibility to read them via a web interface or RSS;

- API to integrate other systems into the portal;
- features that enable .pl domain registrars to scan the security of their customers' domains as part of the Twoja Bezpieczna Strona (Your Secure Site) project;
- features that, with the consent of the entities, enable sectoral CSIRT teams to access information on the infrastructure and vulnerabilities of entities in their sector. These features are currently used by the CSIRT KNF team. In future, they will also be made available to the other sectoral cybersecurity teams.

The portal is very popular among users, indicating that they appreciate its functionalities. By the end of 2025, more than 15,000 users registered with the service and added more than 18,000 domains. Detailed statistics are presented in the following part of the report (→ p. 120).

The moje.cert.pl service has been presented at numerous conferences, both national ones: SECURE International Summit in Bydgoszcz, Security Case Study and Oh My Hack in Warsaw, and those abroad: TF-CSIRT in Oslo, NatCSIRT in Copenhagen and Black Hat Europe in London. We hope that the promotion of our solution internationally will encourage CSIRT teams in other countries to build similar solutions.

Artemis

Artemis has tested websites and other systems, such as e-mail, for security vulnerabilities and misconfigurations since 2023. 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. Since 2024, entities not included in the scan have been able to independently request a check of their domains and networks on moje.cert.pl.

The Artemis system is under constant development, with the changes made in 2025 including:

- a feature to identify resources, i.e. subdomains, IP addresses, technologies, and technology versions associated with the scanned site, making it possible, among other things, to present this information in the moje.cert.pl portal;

- a possibility to modify the configuration of a specific scan, for example, by increasing the number of tests or by including additional modules – more thorough and longer tests can be carried out for domains of greater importance, such as gov.pl subdomains;
- further modules to detect vulnerabilities such as Local File Inclusion, Server-Side Request Forgery, Server-Side Template Injection, Remote Code Execution, etc.;
- a module to detect the possibility of bypassing 403 Forbidden response;
- a module to check whether a simple password can be used to log into the system;
- a module to check whether a domain directs to an unused IP address, which may result in that IP address being purchased by another user and, consequently, in the domain hosting content controlled by another person;
- numerous changes to increase scanning speed and stability.

The development of the Artemis system was largely driven by making moje.cert.pl available to the public by CERT Polska as on this portal, all those willing can take advantage of free scanning of their domains and networks with the Artemis system. As a result, the system had to be brought up to speed and adapted to the requirements of the service as the number of detected vulnerabilities more than doubled.

In 2025, CERT Polska, on a regular basis, conducted scans of public institutions, such as schools, hospitals, and universities, so an important area of our activities was system administration, problem solving, and answering questions from the scanned institutions. Detailed statistics on the scans are presented in the following following part of the report (→ pp. 121–123).

The Artemis system is open source software, available on GitHub at https://github.com/CERT-Polska/Artemis. As a result, it is used by other CSIRT teams, both domestic and foreign, and can be developed by external contributors. The most important of these in 2025 was Abhinav Karn, who developed the system as part of the Google Summer of Code programme and is the author of some of the above-mentioned modules.

In 2025, we presented the Artemis system at numerous conferences, both nationally and abroad, including Black Hat Europe in London, FIRST in Copenhagen, and Oh My Hack in Warsaw.

Snitch

The availability of OT/IoT devices on the Internet can have serious consequences for the cybersecurity of the institutions where they are used. This also applies to IT systems, which are regularly affected by new vulnerabilities. Snitch allows automatic monitoring of the exposure using Shodan, Zoomeye, FOFA, and n6 services. Then it sends a report via e-mail and makes relevant entries in the n6 database, notifying people responsible for these systems.

New contact data

In 2025, the Snitch system started using new sources of contacts. In addition to the RIPE database, the CERT Polska contacts database and data from moje.cert.pl are used. This makes it possible to contact the administrators responsible for the detected vulnerable systems, particularly those who wish to be informed.

If you would like to receive notifications from the Snitch system, we recommend that you verify your subnet at moje.cert.pl. You will then be notified directly from Snitch via e-mail and notifications will also be visible in the "Network Incidents" view at moje.cert.pl.

Reporting statistics

In 2025, our team produced many new rules detecting the most popular IT/OT solutions and those that contained critical vulnerabilities published during the year. For OT systems, the number of rules increased by 50% and for IT systems – by 170% in comparison to the end of 2024. If we compare the number of notifications sent, the result was 90% higher for OT and it increased by 420% for IT. As the number of rules for IT systems increased, many more vulnerable services were identified. This was not included in the statistics on notifications sent by Snitch because IT-related notifications were partially sent by other CERT Polska systems.

TABLE 4. Snitch statistics broken down into OT and IT systems

Number of	OT	Increase*	IT	Increase*	Unique total*
Rules	**90**	1,5	**194**	2,7	284
Unique hosts	**8367**	1,9	**42,856**	1,6	50,997
Unique services	**10,135**	1,5	**47,146**	1,7	57,280
Notifications sent	**22,045**	1,9	**21,739**	5,2	43,784

* Difference relative to 2024. There are hosts in the statistics that simultaneously belong to the IT and OT categories, hence the additional column with a unique total.

The arithmetic mean of the increments in 2025 is 2.2 compared to the previous year.

AIPITCH

The AIPITCH (AI-Powered Innovative Toolkit for Cybersecurity Hubs) project, in which CERT Polska participates on behalf of NASK – PIB, aims to develop tools using artificial intelligence to better protect the Polish cyberspace. This is a three-year project and the works started in 2025.

Apart from NASK – PIB, the consortium includes: The National Centre for Nuclear Research (NCBJ), CIRCL (Computer Incident Response Center Luxembourg), which is our Luxembourgish counterpart, Italy's ABI Lab, and the Shadowserver Foundation. The consortium conducts research that is expected to enhance the activities of cybersecurity operational teams by integrating new AI-provided functions into key tools and processes.

AIPITCH focuses on creating tools to support key operational tasks, in particular early threat detection and improved analytical processes. The project covers, among other things, developing early warning systems against new attacks on online services or against phishing, conducting automated analysis of large volumes of data from various sources reporting cybersecurity threats, and working on an AI chatbot to facilitate users with reporting incidents. An important part of the project is the integration of AI-based tools with internal network monitoring systems and incident response support platforms.

The first tools developed under the project will enter service in 2026.

The project is co-financed by the European Cybersecurity Competence Centre (ECCC), Digital Europe Programme, grant number: 101190545.

Co-funded by the European Union

PERUN

The PERUN (Protecting Sensitive Cyber Ecosystems from Upcoming Next Generation and AI-generated Malware Threats) project was launched in October 2025. The project is

focused on detecting and combating malware, including AI-generated malware that bypasses traditional signature-based detection mechanisms. The project will develop methods and tools at a high level of technological maturity for practical implementation in SOCs, CSIRTs, research and education networks, and others. Solutions will be piloted in entities from key sectors, such as energy.

The international consortium comprises research bodies and companies from Germany, Poland, Romania, France, Italy, Spain, Belgium, and Switzerland. The main tasks of our team include developing the DRAKVUF Sandbox, as well as testing and integrating solutions produced by our partners to support malware analysis. The project works are scheduled for three years (2025–2028) and the outcomes will be used in the operational activities of CERT Polska.

The project is co-financed by the European Cybersecurity Competence Centre (ECCC), Horizon Europe, grant number: 101225653. The views and opinions expressed are solely those of the authors and do not reflect the official position of the EU or ECCC. Neither the European Union nor the grant-giving institution shall be liable for these.

Co-funded by the European Union

FETTA

The CERT Polska continued its work in 2025 as part of the Federated European Team for Threat Analysis (FETTA) project. We are implementing it together with our counterpart in Luxembourg, CIRCL (Computer Incident Response Centre 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 EU Member States. 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.

Development of the n6 platform

An important part of the project is the development of n6, which is our platform for the distribution of cybersecurity threat and incident data, with the code made available under an open-source licence. The main n6 instance, maintained by CERT Polska, has more than a thousand registered entities that receive information on their networks free of charge. In addition to this, data is also made available via moje.cert.pl.

The most important outcome of the work carried out in 2025 was the enrichment of the portal with contextual information, so that users can interpret and respond to their infrastructure-related incidents more quickly, without having to manually search external sources. For incidents containing CVE identifiers, integration with the European Union Vulnerability Database (EUVD) was added to present a reliable description of the vulnerability, and in cases where CERT Polska recommendations are available, a quick link to the relevant technical messages on moje.cert.pl was provided. In parallel, a knowledge base covering hundreds of the most common types of threats, including vulnerabilities, malware, misconfigurations, attacks on network services, was launched on the portal.

Other works comprised the expansion and maintenance of data sources, portal usability enhancements (filtering, search, export), and the Single-Sign-On (SSO) function improvements, allowing integration with systems used by the European CSIRT Network (MeliCERTes tool platform), documentation updates, as well as the optimisation of performance and the strengthening of reliability.

The statistics on incidents processed by the n6 platform are presented in the last part of this report (→ pp. 124–140). Public releases of n6 are available on GitHub: https://github.com/CERT-Polska/n6.

Other activities

In 2025, we continued to develop CTI products, in particular cyclical reports on current threats (APTs, ransomware, hactivists). Together with CIRCL, we prepared the first joint CTI report on the most relevant vulnerabilities in 2024, the methodology for their assessment, and the way to identify exposed instances, and we shared this report with the CSIRT Network. Meanwhile, in collaboration with the NASK – PIB Research and Development Centre, we conducted an analysis of the IoT/Linux botnet landscape.

We also held a series of expert workshops for analysts from both teams, resulting in an exchange of know-how and operational information, as well as outlining common directions for research and tool development.

The project is co-financed by the European Cybersecurity Competence Centre (ECCC), Digital Europe Programme, grant number: 101128030. CERT Polska is the leader of the consortium. The views and opinions expressed are solely those of the authors and do not reflect the official position of the EU or ECCC. Neither the European Union nor the grant-giving institution shall be liable for these.

Co-funded by the European Union

DNS4EU

In December 2025, we completed our works in the DNS4EU project, which aimed to launch a secure European DNS server. The project was co-financed by the European Commission and reflected its desire to ensure the digital sovereignty of the European Union.

The project was performed by an international consortium consisting of Whalebone (Czechia, leader), CZ.NIC (Czechia), CVUT (Czechia), Time.lex (Belgium), deSEC (Germany), HUN-REN Sztaki (Hungary), ABILAB (Italy), DNSC (Romania), and NASK – PIB.

The main outcome of the project was the launch of a public DNS service in June 2025. It is freely accessible and free of charge. The service provides five different security configurations, which are as follows:

- protection against malicious domains,
- protection against malicious domains + child protection,
- protection against malicious domains + ad blocking,
- protection against malicious domains + child protection + ad blocking,
- DNS without filtering.

As part of the project, NASK – PIB developed solutions to detect phishing domains in order to provide a higher security level for the service users. This task was implemented by CERT Polska together with the Research and Development Centre. Our work focused on two concepts for detecting phishing domains: by using data from the .pl registry and by analysing DNS queries from users. We described both concepts in the 2024 annual report, and the summary of the results is described below.

Detection of phishing domains based on domain registry data

In November 2024, we launched an early detection system for .pl phishing domains based on machine learning. The system became part of our phishing detection environment, which is responsible for identifying domains included in the Warning List. Our system uses data from the .pl domain registry to identify suspicious domains moments after registration in order to reduce our team's response time.

Thanks to monitoring new domain registrations, in almost 80% of the cases, our system was able to identify phishing domains faster than other sources of

information we used. In addition, around 14% of the phishing domains found by the system were not repeated by other sources, indicating that the system can obtain unique operational information. We also observed that the system helped to discover domains that had been overlooked when using other methods, for example, due to the lacking evidence of phishing content. In these cases, identification by our system selected the domains for a second, in-depth analysis.

The early detection system identifies phishing domains which, once verified, are included the Warning List. As such, it protects Internet users in Poland through the integration of the List by major Polish Internet providers and it protects users anywhere in the world who use DNS4EU servers.

Analysis of DNS queries

The Analysis of anonymised DNS queries to DNS4EU servers resulted in the development of two phishing domain detection systems. The first system analyses domain names linguistically, while the second one examines the temporal dependencies of queries. The domain name-based detection system uses different language models to create embeddings, which are representations of words in a form that can be understood by machine learning algorithms: FastText[47] and Llama[48]. The first model is used for fast domain filtering, while the second one provides high quality detection.

The second detection system analyses temporal relationships between DNS queries to discover co-occurrences between known phishing domains and other domains. The identification of strong dependencies enables the detection of previously unknown phishing domains. Tests confirmed the effectiveness of this approach in finding unknown phishing.

The main challenge for both systems is that for many of the identified domains, it is difficult to find evidence that they are used for phishing. Unfortunately, singling out a domain alone is often not enough to clearly determine whether it provides malicious content. For example, without the full URL – which cannot be observed at DNS level – it is usually impossible to find the phishing content and thus fully confirm whether the domain has been correctly classified by our systems.

More about the project

News and details about DNS4EU, including instructions on how to set up the service, can be found on the official project website: www.joindns4.eu.

47 https://fasttext.cc/

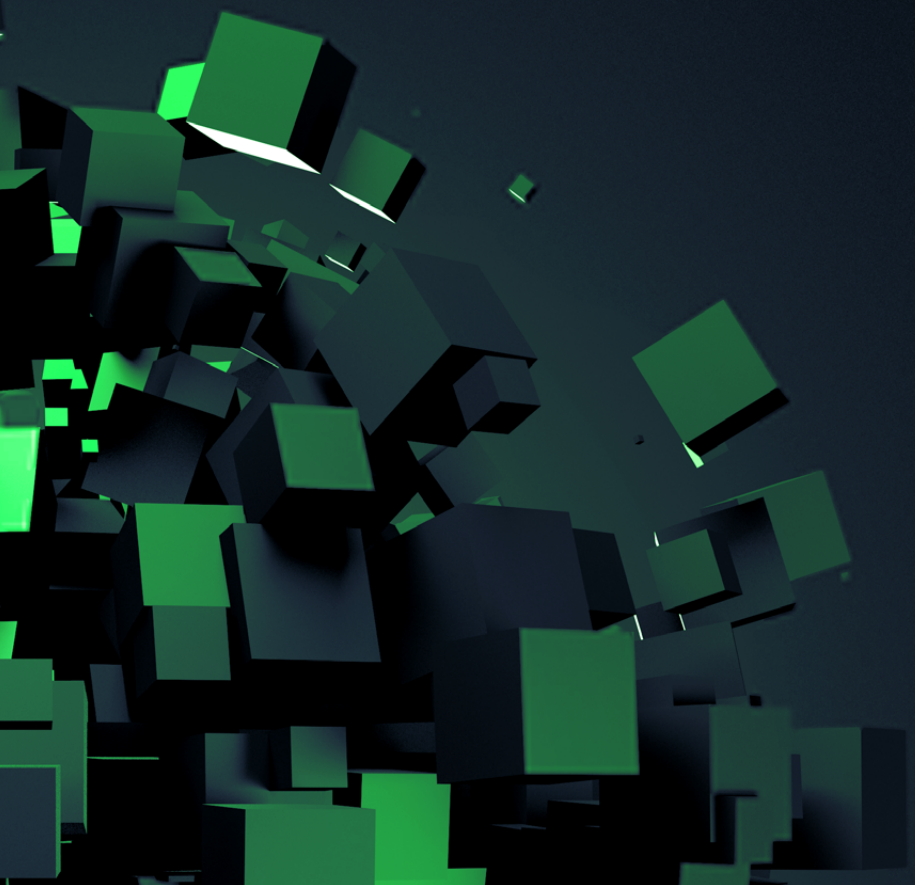
48 https://www.llama.com/

Although main part of the project is completed, we continue to cooperate within DNS4EU, analysing DNS query data and providing information on malicious domains as detected.

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

Co-funded by the European Union

Statistics



Incidents and incident reports

In 2025, the CERT Polska team received 658,320 incident reports that were analysed in detailed. 260,783 unique security incidents were recorded based on these reports. These are incidents that had or could have had a negative impact on the cybersecurity level.

The number of incident reports in 2025 increased by 10% compared to 2024, while the number of cybersecurity incidents recorded in 2025 increased by 152% compared to 2024. For many years, there has been a continuing upward trend in the number of incidents recorded per year. The increase in the number of reports and recorded cybersecurity incidents stems, among other things, from the growing public awareness of the threats, as well as from the role of CERT Polska in monitoring, analysing, and responding to cybersecurity incidents. Outreach work on the existing threats is an important factor contributing to the public awareness. Table 5 shows the number of incidents in 2018–2025.

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 – reporting a phishing domain,
- a text message to 8080 – reporting a suspicious text message,
- the mObywatel app – reporting 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 2025

Computer fraud

The largest category of incidents registered in 2025 was computer fraud. There were 253,238 such incidents, representing 97% of all incidents handled. Compared to the previous year, the number of computer frauds increased by 158%.

The most frequent type of computer fraud was phishing, i.e. attempts to obtain confidential data such as logins and passwords for e-mail, bank websites, social networking sites or other online services. In 2025, there were 78,391 incidents of this type, accounting for 30% of all recorded incidents. Computer frauds included fake online shops and investment

scams, in which fraudsters impersonated oil and energy companies, other enterprises and institutions, and also used images of well-known people. The most frequently used phishing campaigns included unauthorised use of images of sales sites (OLX – 28,462 incidents, Allegro – 22,513 incidents) and attempts to obtain credentials for e-mail accounts (2519 incidents).

Malware

The second most common category of threat in 2025 was malware. 3438 incidents of this type were recorded, including infections of IT systems and unauthorised access attempts using malicious code. Among these incidents, there were 179 cases of crypto ransomware, which could lead to the loss of data or system availability and generate a significant risk to the business continuity of affected entities. Malware incidents continue to pose a significant threat to ICT security, requiring ongoing monitoring and rapid response.

Vulnerable services

Vulnerable services were the third significant type of threat. In 2025, 1732 incidents of this type were recorded and they were related to security vulnerabilities in publicly available ICT services and systems. These incidents may have allowed unauthorised access to resources, escalation of privileges or disruption of services. Vulnerable service incidents highlight the importance of regular software updates, proper system configuration, and ongoing monitoring of the security status of the ICT infrastructure.

Table 7 shows the statistics by incident category.

Act on the National Cybersecurity System

In 2025, CSIRT NASK handled 27 incidents classified as serious under the Act on National Cyber Security System. These were incidents that caused or could have caused a significant reduction in the quality or interruption of the continuity of a key service. Of the 27 serious incidents, 14 involved the banking sector and financial markets infrastructure, eight occurred in the health sector, and five affected the transport sector. Compared to 2024, the number of serious incidents in 2025 decreased by 53%, and the number of serious incidents in the banking sector and financial markets infrastructure decreased by 68%. This decrease is linked to the implementation of the DORA regulation, requiring financial entities to report serious incidents to CSIRT KNF. No significant incident was recorded in 2025.

Further, CSIRT NASK handled 5111 incidents in public entities in 2025, an increase of 48% compared to the previous year.

TABLE 5. Number of incidents handled by CERT Polska in 2018–2025

Year	Number of incidents
2025	260,783
2024	103,449
2023	80,267
2022	39,683
2021	29,483
2020	10,420
2019	6484
2018	3739

TABLE 6. Incidents handled by CERT Polska in 2025 by economic sector. Sector designation according to the internal classification of CSIRT NASK

Sector	Number of incidents	Percentage
Natural persons	250,595	96.1%
Public administration	2801	1.1%
Wholesale and retail	2231	0.9%
Other	1291	0.5%
Education and upbringing	1258	0.5%
Healthcare	724	0.3%
Digital infrastructure	495	0.2%
Other services	255	0.1%
Culture and heritage conservation	218	0.1%
Banking	179	0.1%
Transport	140	0.1%
Water supply systems	95	0.0%
Production	93	0.0%
Construction and real estate management	78	0.0%
Media	60	0.0%
Power engineering	52	0.0%
Logistics and distribution	36	0.0%

Sector	Number of incidents	Percentage
Financial market infrastructure	35	0.0%
Waste management	31	0.0%
Agriculture	29	0.0%
Hotels, restaurants, catering	23	0.0%
Physical culture	18	0.0%
Mail and courier services	13	0.0%
Tourism	10	0.0%
Insurance	9	0.0%
Religions and national minorities	5	0.0%
Chambers of economy and commerce	5	0.0%
Fishery	4	0.0%
Total	**260,783**	**100.0%**

TABLE 7. Incidents handled by CERT Polska in 2025 by category

Threat category	Number of incidents	Percentage
Computer fraud	253,238	97.1%
Malware	3438	1.3%
Vulnerable services	1732	0.7%
Abusive and illegal content	950	0.4%
Break-ins	750	0.3%
Resource availability	427	0.2%
Break-in attempts	139	0.1%
Attack on information security	76	0.0%
Other	18	0.0%
Collection of information	15	0.0%
Total	**260,783**	**100.0%**

MWDB

MWDB is an advanced analytics platform developed by CERT Polska to collect, analyse, and share information on malware. The system, which we are continuously developing, supports the work of cybersecurity analysts in Poland and around the world, enabling the exchange of knowledge and effective tracking of malware trends. The platform code is available free of charge under an open-source licence (https://github.com/CERT-Polska/mwdb-core).

Development of the MWDB platform

We analysed more than 4.1 million unique malware samples within the MWDB platform in 2025. As a result of these analyses, more than 20,900 new unique malware configurations were identified (for example, command-and-control server addresses or encryption keys).

In parallel with the database development, we worked intensively on the platform software itself. In 2025, we published four new versions of MWDB[49] with significant performance improvements. Some of the changes we implemented were the result of collaboration with external contributors, demonstrating the community's active engagement in the development of the project.

Dynamic malware analysis – DRAKVUF Sandbox

One of the key components of the MWDB ecosystem is the DRAKVUF Sandbox project, used for dynamic malware analysis. This mechanism enables suspicious files to be run securely in an isolated and closely monitored virtual environment. Thus, analysts can track the actual behaviour of the samples, including the consequences of their detonation, such as downloading the final malware, attempting to connect to known Command & Control servers or trying to steal data from the victim's system. To this end, the project uses the open-source DRAKVUF monitor by Tamas Lengyel (https://github.com/tklengyel/drakvuf), which observes the execution of the samples from the hypervisor level via virtual machine introspection (VMI). This allows analysis to be performed in an agentless manner, that is without the need to install additional software on the "guest" side of the system (such software could be detected by the suspect malware that is analysed).

Like MWDB, the DRAKVUF Sandbox project is an open-source tool and its code is publicly available (https://github.com/CERT-Polska/drakvuf-sandbox).

49 https://github.com/CERT-Polska/mwdb-core/releases

The project underwent a major upgrade in 2025, resulting in the release of v0.19.0 and v0.20.0[50]. The changes enabled the samples to be analysed using the latest version of the DRAKVUF engine, and consequently, a newer version of the Microsoft Windows operating system (Windows 10 22H2). We also significantly improved the stability of the analyses and the quality of the analytical reports that are generated. As part of our work on the DRAKVUF Sandbox, we also made significant improvements to the DRAKVUF engine.

Users of the MWDB platform

The MWDB platform is of growing interest to the cybersecurity community. In 2025, 696 external users were granted access to the platform and the total number of registered external accounts on the platform was 2533.

Moje.cert.pl

By the end of 2025, 15,156 users registered on moje.cert.pl and added 18,315 domains. The service has a real impact on the security of the Polish cyberspace: in 2025, we detected 531,206 vulnerabilities in domains added to the service, of which 21,258 were high-risk vulnerabilities. We also informed users of 3,914,212 password leaks and 191,342 network incidents, such as servers running scans or hosting phishing. In addition, 70 communications were published on the site; they are available without logging into the portal but users can also request to receive them by e-mail. By the end of 2025, 5127 people took advantage of this opportunity.

For more information on the portal, see „Moje.cert.pl” (pp. 104–105).

Artemis

From the beginning of January to the end of December 2025, Artemis scanned a total of 92,183 domains and IP addresses, and 808,331 subdomains.

The institutions scanned included those listed in the table below.

50 https://github.com/CERT-Polska/drakvuf-sandbox/releases

TABLE 8. Number of domains, subdomains, and IP addresses scanned in 2025 by category

Category	Number of domains and IP addresses scanned	Number of subdomains scanned
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	46,018	400,994
Local government units: municipal and district websites, but also, for example, the websites of waste disposal companies, archive domains and mail handling systems	20,612	157,765
Universities, for example, university and faculty websites, but also domains related to conferences or research projects	7412	85,890
Cultural institutions, for example, the websites of theatres, galleries or libraries	6893	36,023
Submitted domains: domains of companies and entities that have voluntarily submitted them for scanning before the launch of moje.cert.pl	6409	40,180
Health sector, including the websites of hospitals, but also of health-related public institutions	2829	17,422
Newspapers and news portals	2310	84,688
.gov.pl domains	1789	28,390
Banks	1125	1625
Key service providers	601	17,123
Politicians and parties: websites of candidates, members of parliament, senators, political parties and others in the context of local or presidential elections	591	16,998
Professional organisations, for example, websites of chambers of physicians or lawyers	411	3971
Domains submitted by the Ministry of Infrastructure	338	477
Industrial automation manufacturers	172	5576
Other	316	12,663

In some cases, a domain may belong to several categories.

Domains with the www prefix are excluded from the above list. This means that if a page is available at both www.strona.pl and strona.pl, it will be included once.

A total of 374,068 vulnerabilities or misconfigurations were reported in 2025, including 13,629 with high, 248,195 with medium, and 112,244 with low severity. This represents an increase of about 20% in the number of vulnerabilities and misconfigurations detected in comparison to 2024.

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 actual vulnerability, for example, misconfigured SSL/TLS was detected on a domain that is not actually used.

TABLE 9. Number of vulnerabilities or misconfigurations found in 2025 and a description of the associated risks

Number of occurrences	Type of vulnerability/ misconfiguration	Risk associated with vulnerability/ misconfiguration
183,700	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.
58,170	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 into the website as an authorised user.
51,554	Misconfigured mechanisms for verifying the e-mail sender	Sending fake e-mails – a criminal can impersonate a sender from a particular domain.
36,264	Instances where a resource such as an administration panel or login panel (for example, 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.
25,684	Instances where 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 about the software used or file names that should not be publicly available, and consequently download them.
9116	Specific critical or serious vulnerabilities	For example, taking over a page or downloading data from a database.

Number of occurrences	Type of vulnerability/ misconfiguration	Risk associated with vulnerability/ misconfiguration
7468	Instances where sensitive data such as backups, source code, database dumps or the server event log were publicly available.	Download of sensitive data
1677	Other medium-risk vulnerabilities	For example, Open Redirect: an attacker can craft a link in the entity's domain that redirects to any other site, including, for example, one containing malware.
357	Servers still hosting domains that no longer exist	The attacker can communicate directly with the server and interact with the webpage, even though it is considered deleted.
78	Instances where a domain was about to expire.	Unavailability of the service or takeover of the domain by an attacker

More information on the Artemis project is provided in other part of the report (→ pp. 105–107).

Secure mail

Sending fake e-mails is a technique regularly used by cybercriminals. That is why, in 2023, we created a service called bezpiecznapoczta.cert.pl. It allows organisations to check the correct configuration of mechanisms such as SPF, DMARC and DKIM, which make it difficult to impersonate a sender from a given domain. In addition, the Act on Combating Abuse in Electronic Communications made it mandatory for public entities to use these mechanisms.

In 2025, the configuration of almost 33,000 domains was checked using this service. This represents an increase of almost 40% from 2024, showing that this type of tool is responding to the entities' needs.

n6

In this part of the report, we present statistics based on incidents processed automatically using the n6 platform. The incidents 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. Above 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.

Malware (from MWDB)

As in previous years, the predominant type of malware was the so-called stealers, that is malware that steals sensitive information, such as passwords, from the victim's system. Among the 3438 unique malware samples provided to CERT Polska as part of incident reports, our MWDB platform automatically classified the family in 449 cases (some samples involved infection with more than one family). The results are shown below in Table 10.

TABLE 10. Number of incidents where specific malware families were identified

Family	Number of incidents reported
remcos	131
agenttesla	127
formbook	57
xworm	43
PurelogsStealer	23
reverseloader	17
404keylogger	13
lokibot	10
asyncrat	8
expiro	7
quasar	7
mirai	3
SnakeKeylogger	6
Cobalt Strike	2
LockBit	1
Lumma Stealer	1
redline	1

Phishing

This part of the report only includes statistics on phishing in the traditional sense of the word, that is "impersonation" of well-known brands, using e-mail and websites to phish for sensitive data. For example, the cases of impersonation of invoice providers to distribute malware are not included in this category.

Phishing hosted in Polish networks

In 2025, we received a total of 144,320 reports about phishing in Polish networks only. They concerned 3203 URL addresses with 4430 domains which were divided into 1875 unique IP addresses located in Poland. The decrease in the total number of phishing domains compared to the previous year analysis was caused by a methodology change: we did not include low-confidence data sources when calculating the 2025 statistics. Table 11 lists 10 providers

who hosted the most phishing sites and whose infrastructure was located in Poland. As in previous years, there is a significant share of home.pl among the providers chosen by criminals. This Polish provider had the highest number of domains added to the Warning List. This means that phishing campaigns using this provider's domains chose Polish users as their main target and were therefore the most frequently reported and observed by our team.

TABLE 11. Providers with the highest number of phishing websites in Polish autonomous systems in 2025

Provider name	AS numbers	Number of IP addresses	Number of domains	Number of domains on the Warning List
home.pl	12824	324	449	297
Cyber Folks	41079, 43758 29522	140	437	55
Atman	57367 15694	87	290	25
OPS PL	48707	6	254	0
Nazwa.pl	15967	89	221	48
dhosting.pl	48896	29	175	8
DATASPACE	50599	34	175	4
Akamai	20940	348	168	1
LH.pl	203417	61	158	76
OVH SAS	16276	72	148	3

Phishing inserted on the CERT Polska's the Warning List

In 2025, 244,341 domains were inserted on the Warning List of CERT Polska, resolving to 53,544 unique IP addresses. As in 2024, criminals used mainly Cloudflare services to hide the real location of the server, with as many as 43,843 IP addresses having prefixes in AS13335.

Table 12 shows the most common targets that criminals impersonated. In 2025, the most common target of phishing was investment fraud. The biggest increase was recorded for sites impersonating the TVN television station.

TABLE 12. The most common phishing impersonation targets that are included in the Warning List

Target of phishing	Number of domains in 2025	Number of domains in 2024
Fake investments	98,663	42,172
OLX	28,562	9714
Allegro	22,613	4074
Orlen	16,977	972
TVN	11,644	7
Gazeta.pl	11,367	2057
Polsat News	7632	80
Telegram	5415	20
Onet	3390	866
Wprost	3189	7

Table 13 includes the most common top-level domains that were added to the Warning List in 2025. The most popular TLDs were .com, .pro, and .icu. In 2025, criminals were less likely to register .pl domains. There were 2887 .pl domains on the Warning List.

TABLE 13. Most common top-level domains (TLDs) included in the Warning List in 2025

TLD	Number of domains
.com	77,483
.pro	28,918
.icu	18,946
.cfd	14,741
.net	10,884
.sbs	10,875
.top	8602
.shop	8386
.info	6257
.online	5039

Services enabling to conduct DRDoS attacks

In 2025, we recorded more than 23,289,818 reports of 424,947 Polish IP addresses associated with publicly visible services that enabled Distributed Reflection Denial of Service (DRDoS) amplification attacks. The statistics of reports primarily consist of misconfigured services, which realistically affect the security of ICT systems. A small proportion of the reports concerned honeypot systems and other services made available on purpose, but it is difficult to distinguish them based on the results of the overall scan. Their impact on statistics was minimal.

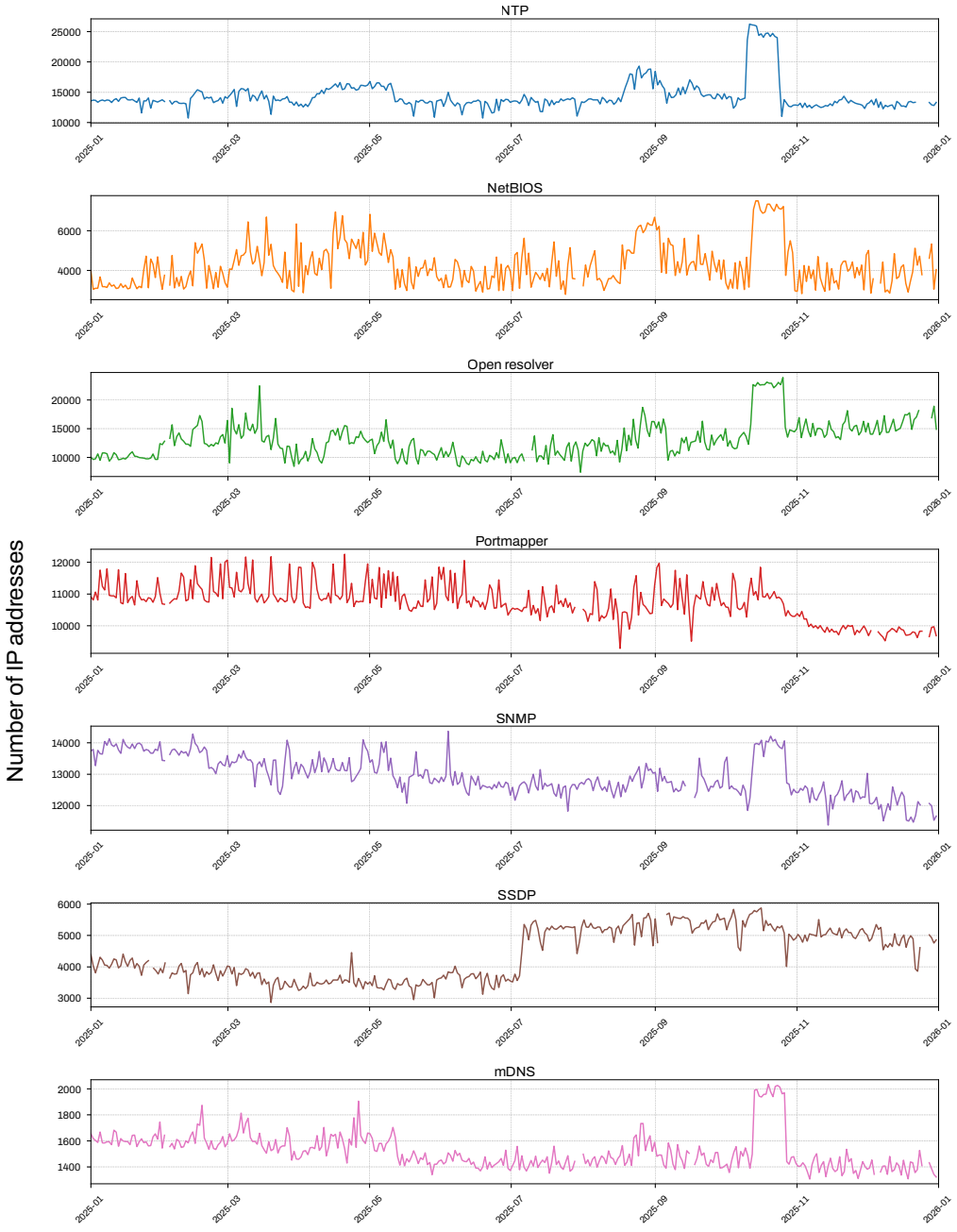
It is to be noted that the number of reports noticeably decreased in relation to 2024 (27,202,309 reports), indicating a decrease in available services that could be used in a DRDoS attack. The type of services noted remains largely unchanged.

Table 14 presents a summary of the most frequently noted services that could have been used for DRDoS attacks in the context of Polish IP addresses. The reports are grouped into daily statistics, from which annual statistics were calculated. Values are rounded to the nearest whole number. Observation time is a percentage representation of the number of days in a year on which at least one service report was noted. The standard deviation refers to the variation in the daily number of IP addresses observed over the year.

TABLE 14. List of the most common misconfigured services that can be used for DRDoS attacks.

Item	Name of vulnerability/ open service	Average daily number of IP addresses	Daily maximum number of IP addresses	Standard deviation	Observation time
1.	NTP	14,482	26,317	2494	99.18%
2.	Open resolver	13,013	23,960	3138	98.90%
3.	SNMP	12,944	14,383	639	99.18%
4.	Portmapper	10,731	12,258	667	98.90%
5.	SSDP	4394	5886	843	98.90%
6.	NetBIOS	4231	7532	1086	98.90%
7.	mDNS	1516	2034	155	98.90%
8.	mssql	1020	1594	132	98.90%
9.	DVR DHCPDiscover	872	2238	445	98.36%
10.	Ubiquiti	744	962	90	99.18%
11.	CHARGEN	111	162	22	98.90%
12.	CoAP	34	41	3	98.90%
13.	QOTD	17	29	3	98.90%
14.	XDMCP	11	14	2	99.18%
15.	ARD	6	9	1	98.90%
16.	RDPEUDP	4	14	2	95.89%

FIGURE 41. Charts showing changes in the number of vulnerable IP addresses in Poland in 2025 in the context of the most common misconfigured services that can be used in DRDoS attacks



The five most frequently observed services are described in more detail below. The statistics of reports for these services are also grouped into daily data from 2025, with an additional breakdown by autonomous systems.

NTP

The Network Time Protocol (NTP) is a common time synchronisation protocol used in computer networks. However, publicly available NTP servers supporting the monlist command can be used for DDoS attacks. As in 2024, it was the most common service in this category.

Number of reports during the year: **5,254,569**

Number of unique IP addresses covered by the reports: **101,857**

TABLE 15. Daily number of addresses where an active NTP service on a publicly available interface was detected, broken down by autonomous systems.

Item	AS number	AS name	Average daily number of IP addresses	Daily maximum number of IP addresses	Percentage of all IP addresses in AS
1.	5617	Orange	2851	14,226	0.26%
2.	12741	Netia	775	840	0.07%
3.	12912	T-Mobile	655	784	0.07%
4.	48956	HyperNET	429	629	12.93%
5.	43372	Telnap Telecom	287	366	5.11%
6.	199715	MSI Telekom	219	442	2.83%
7.	9085	Supermedia	216	294	0.69%
8.	59491	LiveNet	172	179	2.50%
9.	15694	Atman	170	187	0.27%
10.	8267	ACK Cyfronet AGH	164	210	0.27%

Open DNS servers

Open DNS servers (open resolver) can be used to carry out DRDoS attacks. Despite their key role in the 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 during the year: **4,769,640**

Number of unique IP addresses covered by the reports: **171,196**

TABLE 16. Daily number of IP addresses at which an open DNS server was detected, broken down by autonomous systems

Item	AS number	AS name	Average daily number of IP addresses	Daily maximum number of IP addresses	Percentage of all IP addresses in AS
1.	5617	Orange	2218	10,440	0.19%
2.	9141	P4 (Play)	1781	6841	0.42%
3.	12741	Netia	740	1496	0.12%
4.	12912	T-Mobile	562	621	0.06%
5.	201814	Mevspace	365	2659	13.32%
6.	13110	INEA	346	368	0.21%
7.	8374	Polkomtel	317	356	0.08%
8.	29314	Vectra	312	341	0.06%
9.	50599	Dataspace	279	1205	9.81%
10.	6830	Liberty Global Europe Holding BV	225	419	0.04%

SNMP

SNMP (Simple Network Management Protocol) 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 not only poses a threat of unauthorised access to a device but also can be exploited for DDoS attacks.

Number of reports during the year: **4,688,089**

Number of unique IP addresses covered by the reports: **49,712**

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

Item	AS number	AS name	Average daily number of IP addresses	Daily maximum number of IP addresses	Percentage of all IP addresses in AS
1.	12741	Netia	1375	1699	0.14%

Item	AS number	AS name	Average daily number of IP addresses	Daily maximum number of IP addresses	Percentage of all IP addresses in AS
2.	20804	EXATEL	670	1189	0.49%
3.	8374	Polkomtel	599	697	0.16%
4.	199390	Alfa Komputer System	476	507	16.50%
5.	12912	T-Mobile	423	495	0.04%
6.	57978	Digicom	338	352	17.19%
7.	5617	Orange	305	1862	0.03%
8.	200594	SOFT PARTNER	223	307	14.99%
9.	9141	P4 (Play)	218	306	0.02%
10.	13110	INEA	188	206	0.12%

Portmapper

Portmapper is a low-level service typical of 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 during the year: **3,874,126**

Number of unique IP addresses covered by the reports: **39,764**

TABLE 18. Daily number of addresses at which an active portmapper service detected at a publicly available interface, broken down into autonomous systems

Item	AS number	AS name	Average daily number of IP addresses	Daily maximum number of IP addresses	Percentage of all IP addresses in AS
1.	16276	OVH	2250	2510	0.06%
2.	12876	Scaleway	631	1042	0.21%
3.	50599	Dataspace	417	1315	10.70%
4.	57367	Atman	255	298	2.16%
5.	25369	Hydra Communications	251	252	0.23%
6.	12741	Netia	217	261	0.02%

Item	AS number	AS name	Average daily number of IP addresses	Daily maximum number of IP addresses	Percentage of all IP addresses in AS
7.	201814	Mevspace	195	304	1.52%
8.	50840	HitMe	190	204	4.43%
9.	197155	Artnet	180	237	1.93%
10.	31242	P4 (Play)	163	197	0.17%

SSDP

SSDP Simple Service Discovery Protocol) is a protocol used to detect and advertise selected devices and services on a given network. Usually, it primarily identifies devices operating under the UPnP (Universal Plug and Play) protocol, but if available to the public, it is – like the above-mentioned services – a threat and can be used for DDoS attacks.

Number of reports during the year: **1,608,242**

Number of unique IP addresses covered by the reports: **44,414**

TABLE 19. Daily number of addresses where an active SSDP service on a publicly available interface was detected, broken down by autonomous systems.

Item	AS number	AS name	Average daily number of IP addresses	Daily maximum number of IP addresses	Percentage of all IP addresses in AS
1.	197697	DERKOM	1498	1698	20.73%
2.	29314	Vectra	561	790	0.13%
3.	21021	Multimedia Polska	341	734	0.12%
4.	41023	ARREKS	340	378	10.55%
5.	8374	Polkomtel	153	204	0.05%
6.	12741	Netia	145	280	0.02%
7.	12912	T-Mobile	124	147	0.01%
8.	57101	WadowiceNET	98	114	2.12%
9.	43118	East&West	90	146	0.20%
10.	5617	Orange	89	389	0.01%

Vulnerable services

In 2025, we noted 55,605,774 incidents related to the observation of vulnerable services. These incidents concerned 810,173 Polish IP addresses. The statistics include both services with actively exploited vulnerabilities and services that are misconfigured, allowing, among other things, unauthorised access to information or management of a given service. The number of registered incidents remained at a similar level to the previous year (53,010,669 observations).

Table 20 presents a list of services that could have been attacked and were the most represented in the Polish Internet. The calculation method we adopted is analogous to that described in the section on DRDoS attacks.

Figure 42 shows the year-on-year changes in the number of registered IP addresses associated with vulnerable services. The charts refer to seven most frequently reported services.

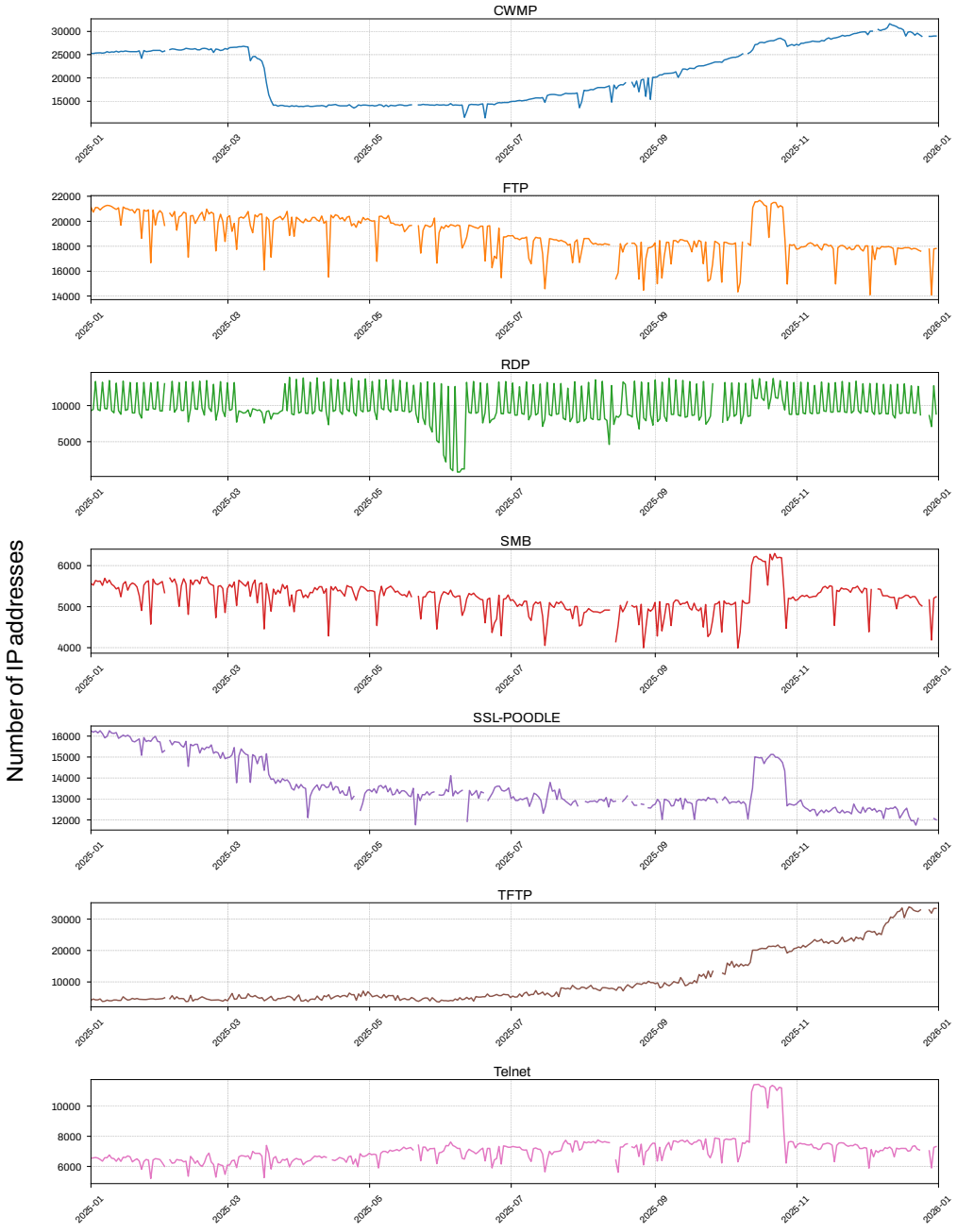
The charts for CWMP and TFTP (in Figure 42) show significant changes in the number of reports over the year. An analysis of the quarterly statistics shows that for these services, the number of noted IP addresses for most Autonomous Systems (ASs) remained at a similar level, with increases or decreases in the statistics driven by significant changes in individual ASs. In the case of CWMP, the number of reports for ASN 12741 (Netia) remained very high in the first quarter, with an average of more than 12,000 reports per day. This number has decreased significantly and remained relatively low since the second half of the second quarter. Over the course of the year, ASN 29314 (Vectra) stood out, with an average of 300 IP addresses registered per day in the first two quarters, 2000 IP addresses per day in the third quarter, and more than 9600 IP addresses per day in the fourth quarter. It was mainly this change that caused a steady increase at the end of the year. The situation is similar in the context of TFTP. Most of the registrations held steady for the AS data. The exception to the rule was ASN 9141 (P4/Play), for which the number of registrations increased significantly, from an average of a few dozen IP addresses per day in the first half of the year to an average of 2000 addresses per day in the third quarter, and averaged over 12,000 addresses in the last quarter of 2025.

The sudden drop in the number of IP addresses associated with CWMP is most likely linked to the deployment of an update to a particular manufacturer's device group that disables support for the service at default settings. On the other hand, the gradual increase in CWMP and TFTP registrations in the second half of the year can be linked to the introduction of new devices using these protocols by default.

TABLE 20. List of the most numerous services exposed to attacks in Poland

Item	Name of vulnerability/ open service	Average daily number of IP addresses	Daily maximum number of IP addresses	Standard deviation	Observation time
1.	CWMP	21,078	31,677	6031	98.63%
2.	FTP (clear-text credentials)	18,817	21,676	1983	98.90%
3.	SSL-POODLE	13,506	16260	1272	98.90%
4.	TFTP	10,337	33,662	8250	98.90%
5.	RDP	10,045	13,941	2516	98.90%
6.	Telnet	7042	11,446	1088	99.18%
7.	SMB	5190	6283	523	98.90%
8.	VNC	2801	5006	452	99.18%
9.	RSYNC	1602	1993	295	99.18%
10.	SSL-FREAK	1187	1769	224	99.18%
11.	MQTT	1064	1364	104	99.18%
12.	MongoDB	815	919	145	99.18%
13.	AMQP	725	797	65	98.90%
14.	Redis	568	2521	665	98.90%
15.	AFP	496	746	105	98.90%
16.	NAT-PMP	435	523	45	99.18%
17.	ISAKMP	428	1117	164	78.08%
18.	IPP	335	521	47	98.63%
19.	IPMI	281	316	19	98.90%
20.	LDAP	238	273	23	99.18%
21.	Memcached	159	226	30	99.18%

FIGURE 42. Charts showing changes in the number of vulnerable IP addresses in Poland in 2025 in the context of the most commonly used services exposed to attacks



As in last year's report, as part of the discussion on vulnerable services, we decided to additionally separate information on Exchange servers, the HTTP service, and industrial systems (ICS/OT). The information is presented in separate tables below. The calculation methods and designations we adopted are analogous to those described in the section on DRDoS attacks.

Exchange

This section provides information concerning the vulnerable Microsoft Exchange servers. Most of the vulnerabilities listed in the table allow remote code execution on an affected system. The most recent vulnerability recorded, CVE-2025-53786, relates to privilege escalation and is not as critical as previously observed vulnerabilities. The team sent notifications regarding this vulnerability to server owners, causing most instances to be updated. Out of almost 70 servers, on average only seven servers remain flagged as exposed to this vulnerability. The overall number of registered instances of vulnerable Exchange servers has dropped significantly since 2024, suggesting that the messages sent to administrators and the following updates have had a positive effect.

TABLE 21. List of the most frequently recorded vulnerabilities of Exchange servers exposed to attacks in Poland

Item	Name of vulnerability/ open service	Average daily number of IP addresses	Daily maximum number of IP addresses	Standard deviation	Observation time
1.	CVE-2024-26198	7	92	14	98.63%
2.	CVE-2025-53786	7	67	10	39.18%
3.	CVE-2023-36745	3	13	3	96.71%
4.	CVE-2023-36439	3	13	3	97.81%
5.	CVE-2024-21410	3	11	2	98.63%
6.	CVE-2023-21529	3	11	2	98.63%
7.	CVE-2022-41082	3	11	2	98.63%
8.	CVE-2020-0688	2	8	2	98.08%
9.	CVE-2021-27065	2	8	2	98.08%
10.	CVE-2021-26855	2	6	1	98.63%

HTTP

The following provides selected 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** – HTTP servers that use Basic Authentication. The server allows credentials to be sent in plaintext, without encryption.

- **Basic auth (IoT)** – as above. It applies to IoT devices.
- **Folder .git** – a publicly available .git folder.

The remaining vulnerabilities refer to the standard CVE designation system.

TABLE 22. List of the most numerous servers exposed to attacks in Poland. Items were selected on the basis of both the average daily number of addresses and significant observation time

Item	Name of vulnerability/ open service	Average daily number of IP addresses	Daily maximum number of IP addresses	Standard deviation	Observation time
1.	Basic auth	6836	7779	616	98.90%
2.	Basic auth (IoT)	3654	5002	548	98.90%
3.	Folder .git	367	439	26	98.63%
4.	Cisco CVE-2025-20333, CVE-2025-20362, CVE-2025-20363	141	286	83	24.93%
5.	React Server CVE-2025-55182	122	398	106	6.85%
6.	Fortinet CVE-2024-21762	84	501	108	98.90%
7.	Fortinet CVE-2024-55591	79	281	48	94.52%
8.	Roundcube CVE-2023-43770	75	129	51	46.30%
9.	Fortinet CVE-2023-27997	74	501	118	98.90%
10.	Fortinet CVE-2024-23113	70	501	103	98.90%
11.	Plex Media Server CVE-2025-34158	69	239	57	35.34%
12.	Tinyproxy CVE-2023-49606	66	238	59	98.90%
13.	Roundcube CVE-2023-5631	62	129	51	46.30%
14.	Roundcube CVE-2025-49113	45	318	58	4.11%
15.	Zimbra CVE-2024-45519	31	107	33	98.90%
16.	Zimbra CVE-2025-62763	16	30	12	18.36%
17.	VMare CVE-2025-22224	15	58	13	82.19%

Item	Name of vulnerability/ open service	Average daily number of IP addresses	Daily maximum number of IP addresses	Standard deviation	Observation time
18.	GLPI CVE-2025-24801	12	34	11	77.81%
19.	FreePBX CVE-2025-57819	11	27	6	29.59%
20.	VMware CVE-2025-41236	9	49	10	44.66%

Industrial control systems

The following section provides information on ICS/OT systems that are publicly visible on the web. Specific vulnerabilities were not checked during the scanning process but these types of devices should never be visible or accessible from the internet. Industrial protocols often do not support authentication, leaving them vulnerable to unauthorised modification and access to significant information by unauthorised persons.

The following list, as with the previous statistics, provides IP addresses where the services concerned are actually available, as well as those that are available intentionally (for example, honeypot systems) as it is difficult to distinguish the latter on the basis of scanning data and their total number is small.

Compared to the previous year, the overall average daily number of IP addresses remained at a similar level but there were changes in the popularity of the services to which these addresses relate. The largest increases occurred for the BACnet protocol (about 40 more addresses per day on average), while the largest decreases were for S7 and Codesys (about 20 fewer addresses per day on average). The other protocols remained at very similar levels.

TABLE 23. List of the most numerous ICS/OT systems exposed to attacks in Poland

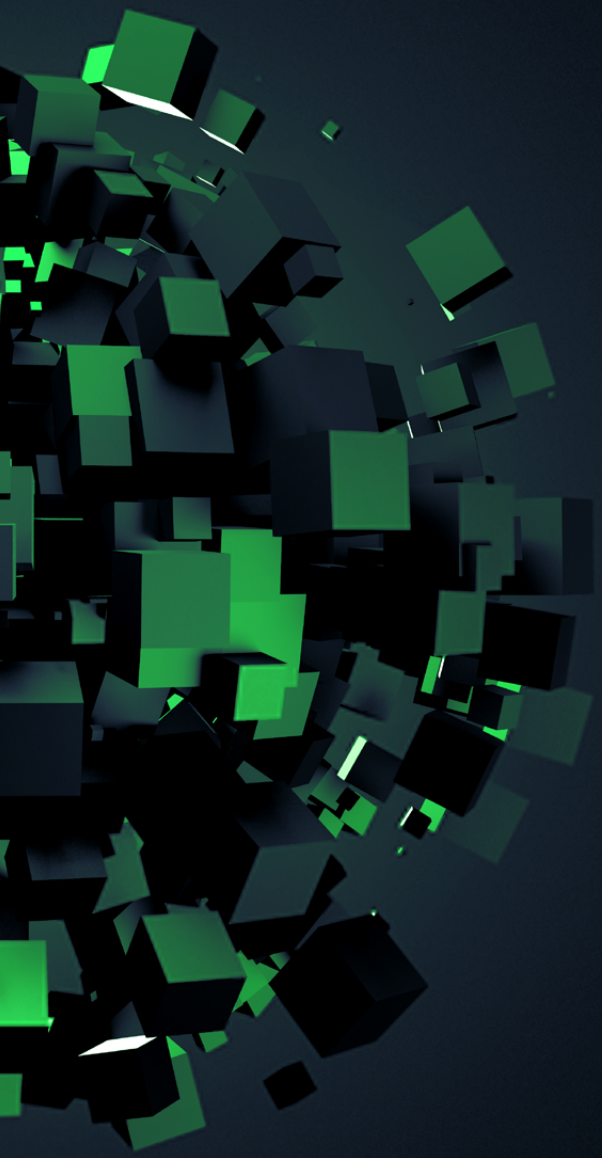
Item	Name of vulnerability/ open service	Average daily number of IP addresses	Daily maximum number of IP addresses	Standard deviation	Observation time
1.	S7	157	225	19	98.63%
2.	BACnet	157	208	21	98.36%
3.	Codesys	124	181	18	98.63%
4.	Modbus	102	141	14	98.63%
5.	EtherNet/IP	60	75	6	98.36%

Item	Name of vulnerability/ open service	Average daily number of IP addresses	Daily maximum number of IP addresses	Standard deviation	Observation time
6.	OPC UA Binary	27	41	5	98.63%
7.	Fox	18	22	3	98.63%
8.	Unitronics	14	22	2	98.63%
9.	DNP3	9	23	3	98.36%
10.	IEC 60870-5-104	8	22	4	98.63%
11.	Omron FINS	7	14	2	98.63%
12.	PC Worx	6	9	1	97.26%
13.	GE SRTP	5	8	1	97.81%
14.	ICCP	3	6	2	95.07%
15.	MELSEC-Q	2	4	1	93.42%

List of figures

List of tables

List of charts



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
cert.pl