ANNUAL REPORT
ON CYBERSECURITY
2025

POLISH FINANCIAL MARKET IN THE FACE OF THREATS

TABLE OF CONTENTS

01. Introduction (pp. 2-4)

02. Clients' financial security (pp. 5-46)

- 2.1 Fake investment as the dominating fraud (pp. 6-24)
- 2.2 Fake stores: a growing threat (pp. 25-30)
- 2.3 Scams targeting bank customers (pp. 31-37)
- 2.4 Malware (pp. 38-46)

03. Security of financial market entities (pp. 47-99)

- 3.1 Cyber Threat Intelligence (CTI): from responding to predicting (pp. 48-54)
- 3.2 DDoS attacks against the banking sector (pp. 55-61)
- 3.3 Current trends in cyber threats (pp. 62-74)
- 3.4 DORA as foundation for the cyber resilience of the financial market (pp. 75-79)
- 3.5 moje cert.pl – a sectoral module of CSIRT KNF for the financial market (pp. 80-83)
- 3.6 Cooperation with CSIRTs at the national level (pp. 84-89)
- 3.7 Educational activities of CSIRT KNF (pp. 90-99)

The year 2025 has proved that the Polish financial market is characterised by the highest degree of digitalisation in the European Union and that clients' activity in mobile and online channels in Poland reaches exceptional levels as compared to our entire continent. This digital maturity enhances the sector's competitiveness, increases the availability of services and creates ease for users, but also naturally expands the attack surface. In consequence, cybersecurity becomes not only a technical area, but also one of the pillars of stability of and confidence in the financial system. External studies published at the end of November 2025 show that Poland ranks first in the European Union in terms of the number of mobile and online transactions [1].

In such a context, CSIRT KNF focused in 2025 on the recognition, monitoring and mitigation of major threats affecting the safety of clients and the business continuity of financial institutions. We saw further professionalisation of cybercrime and a growing scale of operations involving the use of automation, multi-stage attack scenarios and precise victim profiling. Social engineering scams played a crucial role in the cyber threat landscape, including campaigns conducted by attackers impersonating financial institutions and public-trust entities. SMS phishing (smishing) and e-mail phishing remained one of the mostly used initial attack vectors, with its effectiveness being enhanced by a combination of psychological techniques with elements of technical impersonation and a dynamic domain infrastructure.

At the same time, criminal pressure linked to fake investments remained high. This type of fraud still causes particularly severe social and financial harm, as it often leads to major losses for retail clients.

[1] https://www.deloitte.com/pl/pl/about/press-room/polskie-centrum-finansowe-europejskim-liderem-w-liczbie-transakcji-mobilnych-i-internetowych.html

In 2025, we saw further evolution of such offers in terms of their narrative and the ways used to make them look more credible: from the use of image of public persons and symbols of trust to increasingly efficient methods of mimicking interfaces of legitimate entities and building multi-channel paths of contact with the victim.

Threats stemming from technological and business interdependence gained relevance. Supply chain attacks – understood as the compromise targeting software and IT service providers as well as operators supporting business processes – were a clear sign that the sector's resilience must be looked at from an 'ecosystem' perspective. An incident in one link of the chain may translate into operational risk in many institutions at the same time, which requires mature management of third-party risk, consistent security requirements, and verifiable monitoring practices.

Another important phenomenon in 2025 was the activity of malware targeting end users' devices. This manifested as both classical campaigns aimed at taking over authentication data in a PC environment and a growing scale of threats in the mobile environment. In this area, we pay special attention to scenarios of fraud linked to contactless payments and communication interception techniques, including various types of relay attacks. These phenomena highlight the need to further enhance multi-factor authentication mechanisms, client education, and protection of end devices based on current risk models.

DDoS attacks targeting the financial market infrastructure remained a permanetn element of the threat landscape. The level and cyclical nature of such attacks confirm that they are used both as a way to disrupt service availability and as a smokescreen for malicious activities carried out simultaneously. CSIRT KNF believes, though, that for the vast majority of cases the consequences of such incidents were mitigated swiftly and effectively. This is a sign of a growing organisational and technological maturity of supervised institutions and of how valuable the cooperation within the national cybersecurity system is.

This report includes a summary of key developments in 2025, main insights into the changing tactics and techniques used by attackers, and brief conclusions in favour of enhancing the digital resilience of the financial sector. CSIRT KNF remains focused on protecting market participants, reducing the scale and effects of cybercrime and building safe conditions for the development of innovative financial services in Poland.

02. CLIENT'S FINANCIAL SECURITY

2.1 FAKE INVESTMENT AS THE DOMINATING FRAUD

A fake investment has been the most common and harmful attack scenario of money theft. Through social engineering and manipulation, scammers induce their victims into investing in fake investments promoted with the use of advertisements in social media, web search engines and popular news services. The fraudulent scheme is based on promises of very high profits and minimum – or even zero – investment risk.

Manipulated victims, believing that the investment is safe, often times give their life savings to criminals. In order to finance the alleged investment, victims are also often ready to contract new loans. This type of fraud has for years been the most common and harmful threat leading to huge financial losses for the victims.

Phishing domains

CSIRT KNF uses various tools to monitor, on an ongoing basis, the content posted by criminals and to request a website blocking order for such content. Website blocking orders are issued for websites and advertisements used for stealing data through contact forms.

The underlying scheme consists in obtaining contact details from an unaware user. Scammers usually steal forename, surname and phone number. Information so obtained can be used by scammers to carry out a social engineering attack: during a phone call, they get their victims to invest capital in fake financial instruments, which actually have never existed.

In 2025, CSIRT KNF identified and requested a website blocking order for 41 751 dangerous domains. As many as 40 225 of those domains were linked to fake investments, which accounts for more than 96.34% of all domains reported. This figure leaves no doubt that the scale of this threat has remained enormous for years.

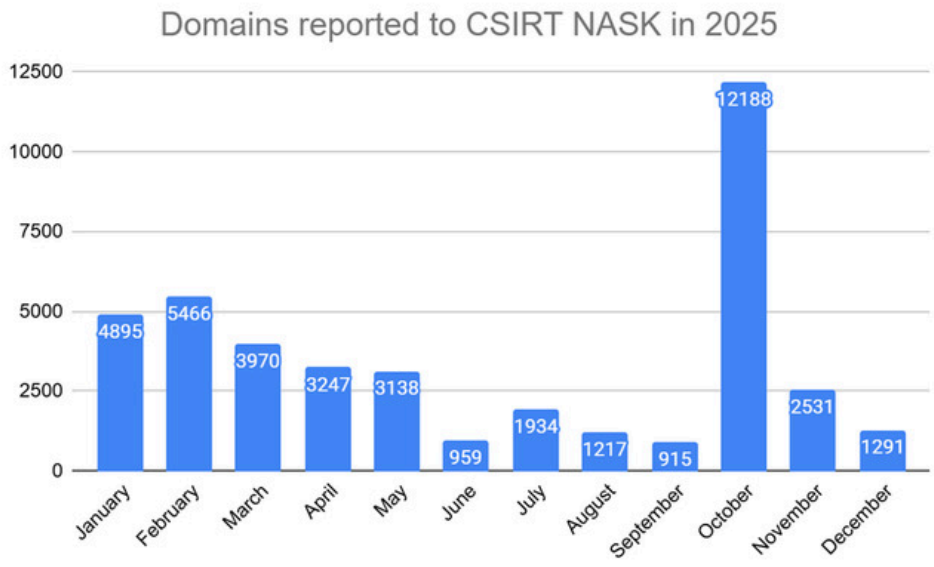


Chart 1. Domains reported by CSIRT KNF to CSIRT NASK in 2025 by month

In 2025, an evolution was noticed in campaigns promoting fake investments. Very often, attackers would use forms embedded directly in Lead Ads, without redirecting to external sites. This model allowed scammers to close the entire scam process within just one platform, eliminating costs such as domain purchase or hosting costs. In terms of security, this technique makes threat mitigation much more difficult: the lack of an external URL address impedes traditional redirection site blocking and limits defensive actions to reporting only the advertisement creation and the advertisement publisher's profile. As a result, we have recorded an annual decrease in the number of reported websites by 9 490 and an increase in the number of reported profiles by 1 288. The mitigation measures must then include not only website blocking but also quick blocking of advertisement creations as well as advertisers' profiles and accounts.

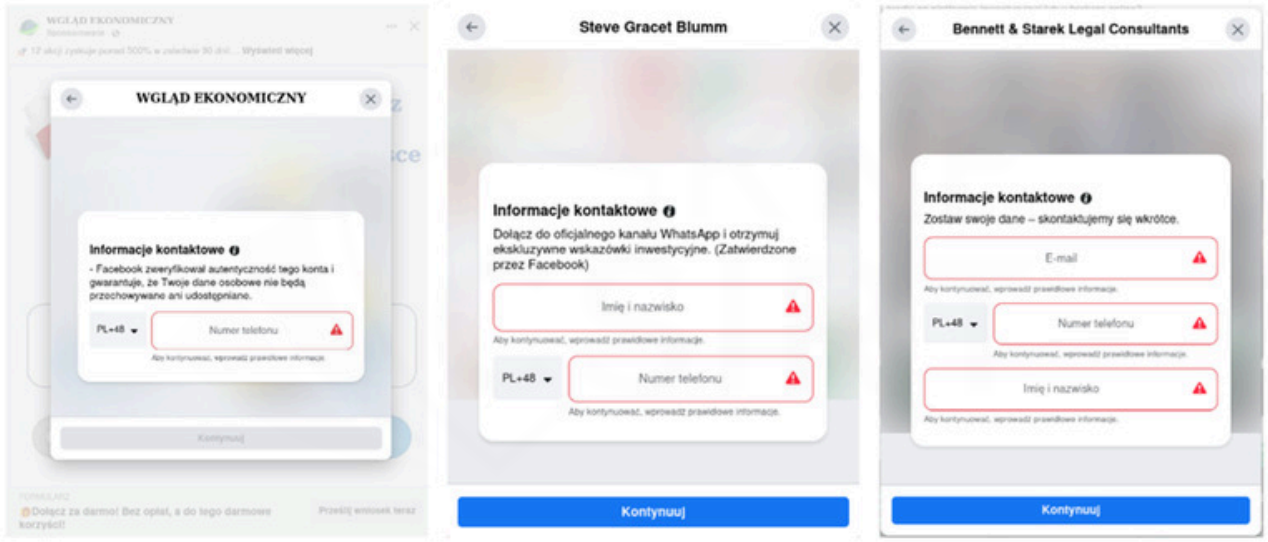


Image 1. Contact forms in advertisements used by criminals

Advertisements on social media

Partnership with national and international entities constitutes the foundation of the activity of CSIRT KNF. In combating cybercrime, CSIRT KNF maintains dedicated channels for report escalation. Continuous exchange of information about threats allows faster response and more effective blocking of harmful online content.

In response to the persisting high number of fake advertisements on Facebook, CSIRT KNF maintains a special fast-response path to report and block harmful content on that platform. In 2025, these measures resulted in 9 751 fraudulent advertisements being blocked.

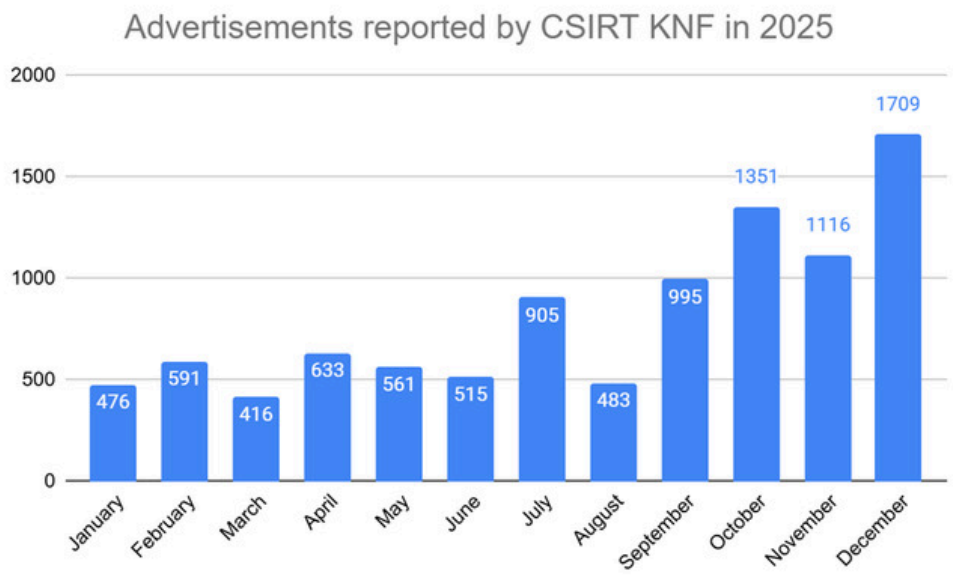


Chart 2. Advertisements reported by CSIRT KNF in 2025 by month

We also reported 4 358 profiles of fake advertisement publishers. This represents a 41.95% increase compared to last year. In consequence, the accounts were blocked, which prevented publication of new malicious content.

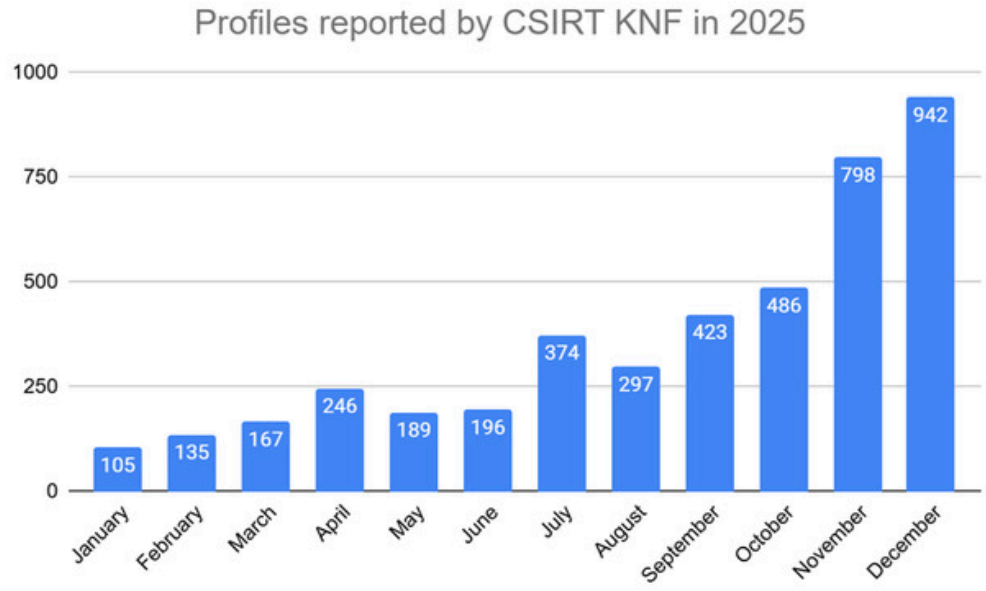


Chart 3. Profiles reported by CSIRT KNF in 2025 by month

Image exploitation

To make their scam look authentic and to create a sense of trust in their victims, criminals often used the image of famous people and company logos. A common practice in fake advertisements consisted in using pictures of politicians, celebrities or business people. Other types of exploited image included faces of recognised role models from the world of finance as well as logos of lawful companies, which was supposed to suggest connections with the real business.

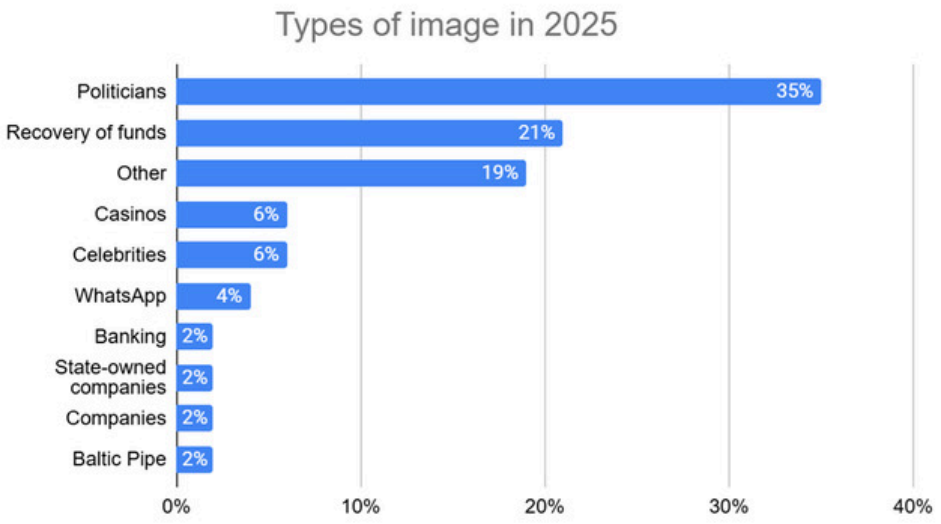


Chart 4. Types of image used in fraudulent advertisements in 2025

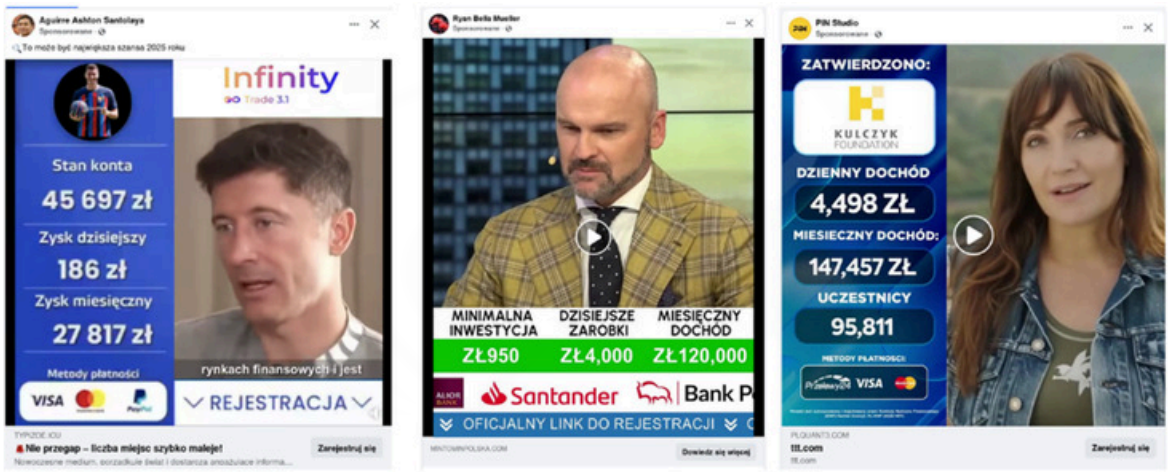


Image 2. Examples of image used in fake investment ads

The scammers would prey on the trust that Poles have in public institutions. Fake campaigns would constantly make references to Polish companies or institutions such as Orlen, Social Insurance Institution (ZUS) or Warsaw Stock Exchange (GPW). Major infrastructure projects, such as Baltic Pipe or Baltica, also served as an alluring decoy.

Cybercriminals created a false narrative suggesting that every citizen can become a shareholder in those projects and earn money on Poland's energy security. The names are used to lull potential victims into a false sense of security.

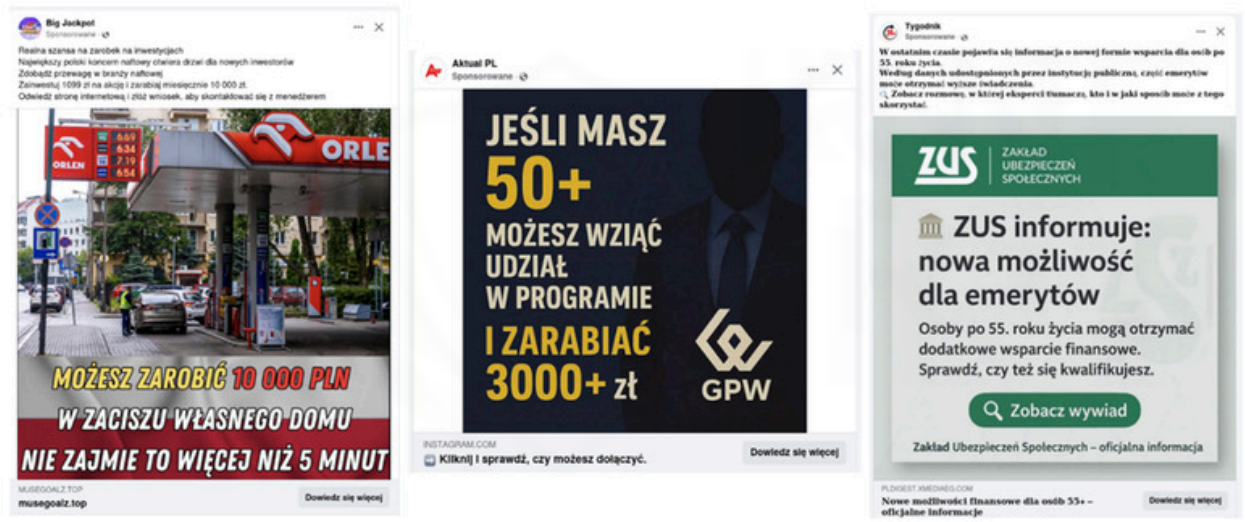


Image 3. Examples of firms and institutions exploited in fake investment ads

Image 4. Advertisement of a fake investment in 'Baltica 2' infrastructure project

Image 5. An article on a fake site announcing a breakthrough energy project

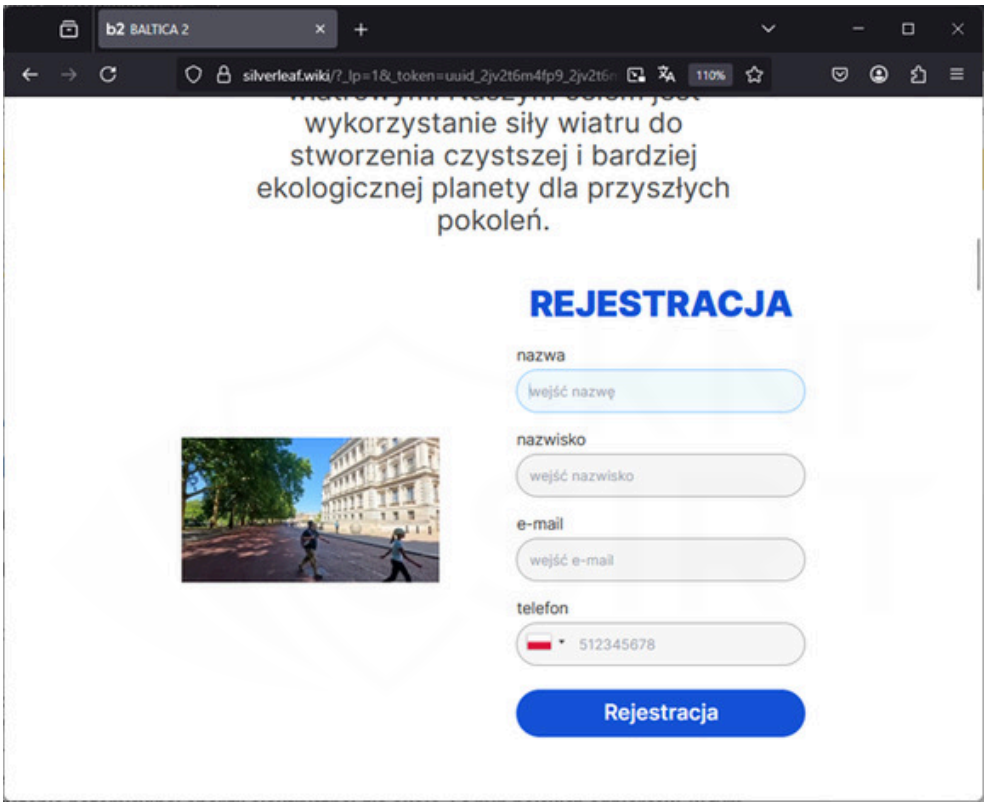


Image 6. A contact form used to collect contact details

The scammers did not limit themselves to state-owned companies but exploited the reputation of the entire financial sector. To render their fictitious offers more credible, they misused logos of banks and renowned brokerage offices. Gaffed advertisements and articles often suggested the existence of clandestine partnerships or exclusive investment schemes allegedly available only to clients of those specific institutions, thus putting even more pressure on the victim to make a quick payment.

Image 7. Examples of advertisements exploiting logos of financial firms

The criminals would try to use visual elements of leading media and industry-specific websites by creating entire websites imitating real news services. On multiple occasions, CSIRT KNF would record cases of using trademarks of entities such as Onet, Money.pl or TVN 24. The fraudsters would cook up fake articles and interviews to add attractiveness to their offers and they would pose as professional online finance sites. The victim would get the impression that the 'best-ever investment' is something professional journalists and experts wrote about.

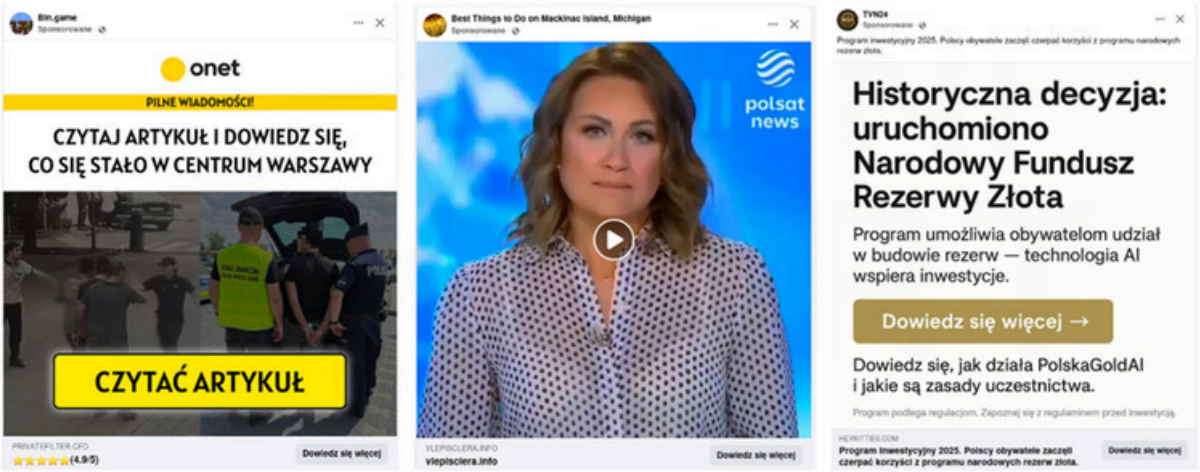


Image 8. Examples of advertisements impersonating news services

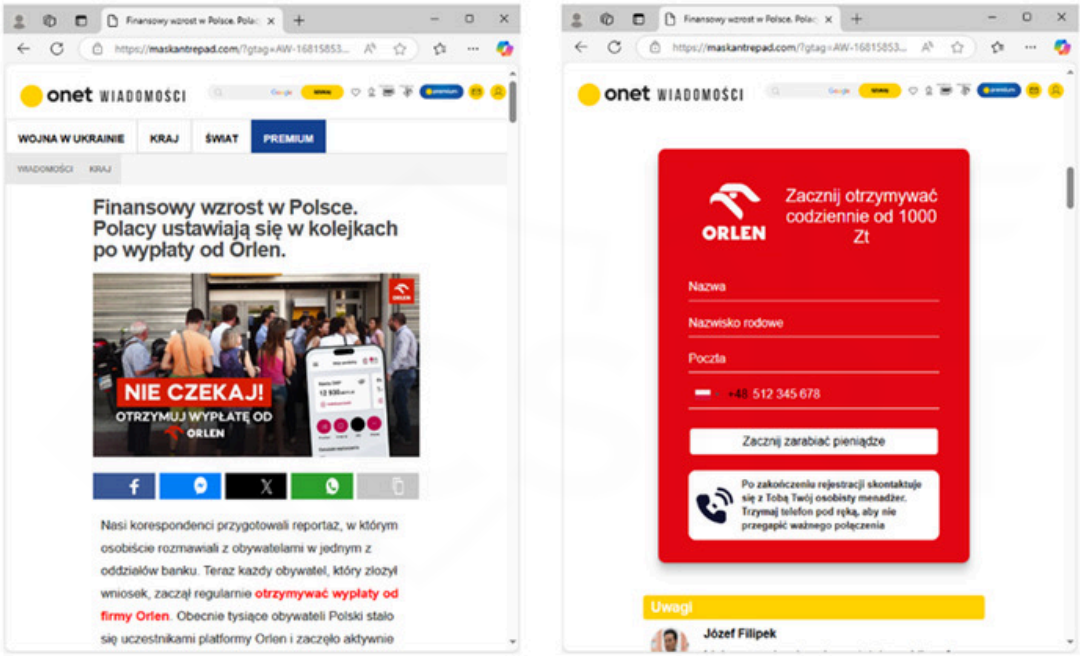


Image 9. An article on a fake site inducing users to transfer money into fake investment schemes

A credible-looking graphic design was completed with descriptions of a tempting vision of instant and effortless enrichment. Perpetrators would use manipulative slogans to make victims believe that the success of the investment is secured by high-tech cryptographic algorithms or artificial intelligence. The advertising content would contain mostly phrases suggesting zero risk and a vision of passive income achieved without any knowledge of economics. Slogans such as: ‘receive 500 euro a day’ or ‘guaranteed income’ were supposed to convince the user that technology would do all the work for them.

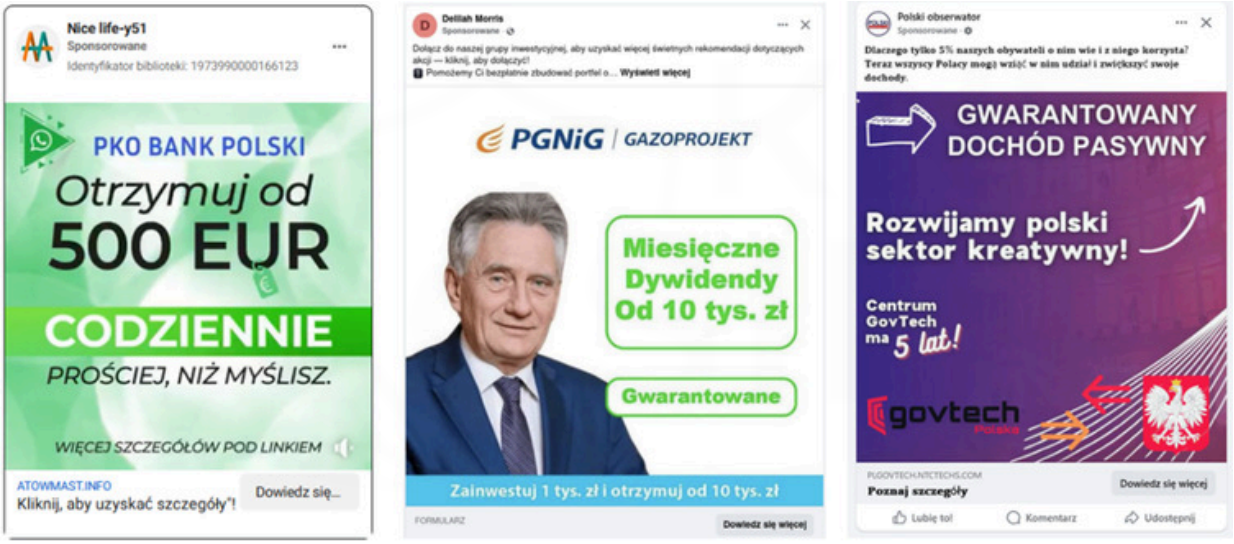


Image 10. Examples of catchy slogans in fake investment ads

Image 11. Examples of fake investment ads using the AI theme

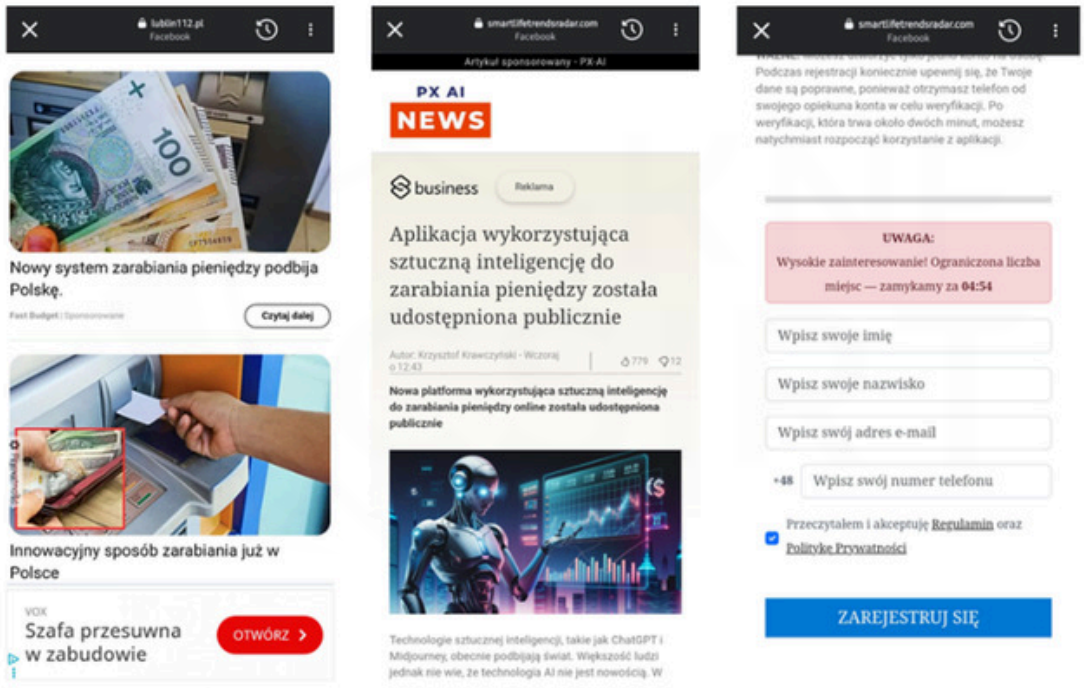


Image 12. A fake investment ad and redirection site

An analysis of news, trends and public mood enabled them to quickly adapt their methods. As a result, threads referring to high-profile events were almost instantly implemented in the content of fake advertisements on fraudulent sites.

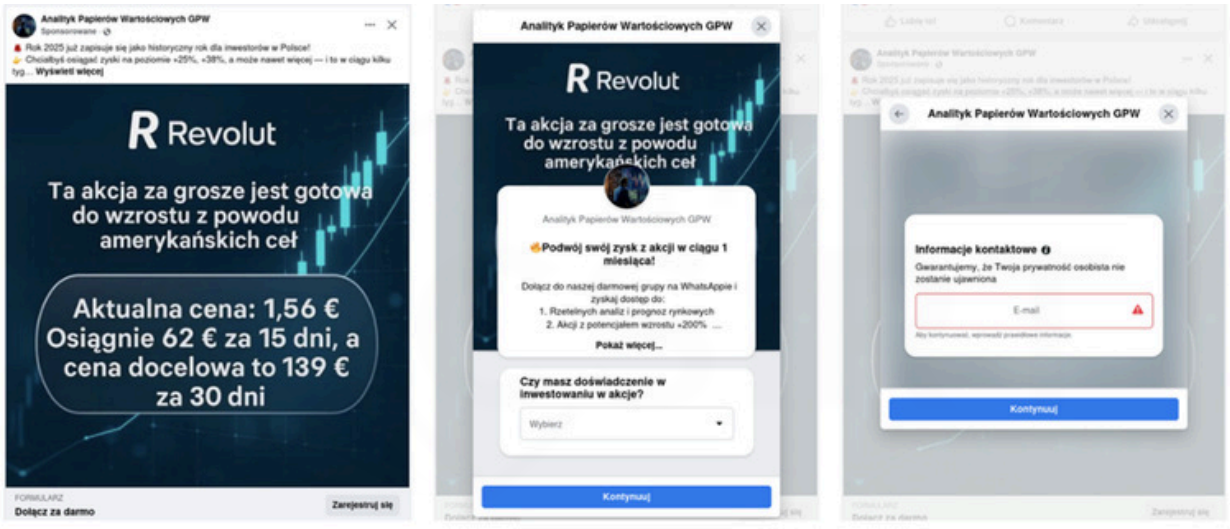


Image 13. A fake investment ad referring to the imposition of U.S. tariffs

Fake investment ads were also spotted on Youtube, Bing, Google, TikTok and X, but on a much smaller scale. This could be caused by the fact that Facebook offers fraudsters access to a larger group of potential victims, which translates into higher efficacy of fraudulent actions taken on that platform.

Image 14. Fake investment ads on YouTube.com and X.com

Advice for internet users

Don’t be misled by any online promise of quick high earnings. It’s usually an attempt at fraud. Prior to any investment, consult a licensed adviser and check the firm, including against the KNF’s List of Public Warnings. Always follow the rule of limited trust in online interactions: if the offer seems too perfect to be true, it’s probably fake.

Deepfake

In their materials, fraudsters sometimes use deepfake technology. It enables them to steal identity of well-known people, politicians and journalists and use it to endorse, among others, fake investments. The technique enables creation of seemingly authentic videos in which faces are replaced and voices are cloned so that the viewer has the impression they are watching a real speech or appearance.

Everything seems very realistic and, at first glance, quite indistinguishable from the truth. Lip movements may be synchronised with the words spoken, and the tone of voice may be strikingly similar to the real one. Fraudsters generate fake interviews and appearances to render the scam more credible in the eyes of victims.

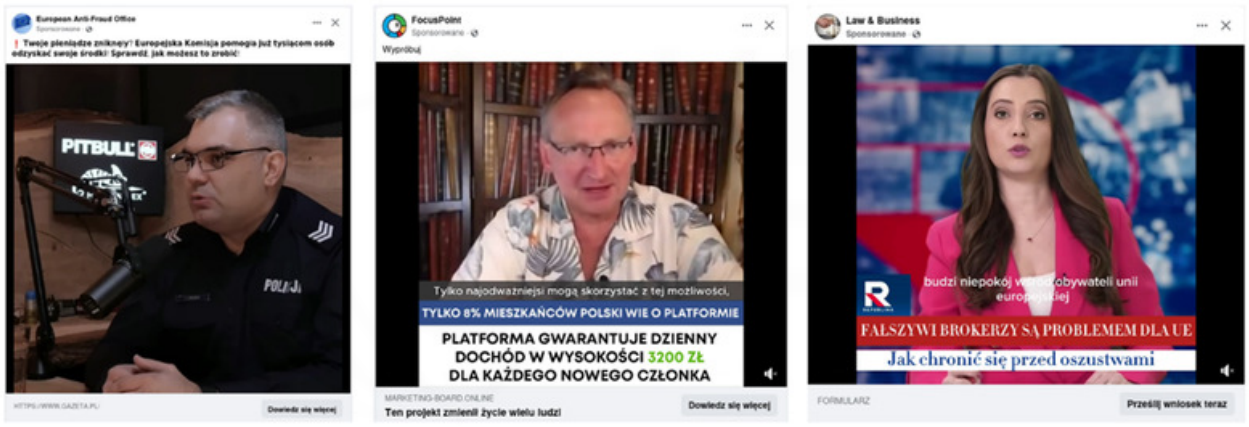


Image 15. Examples of image used in deepfakes

Examples of recordings made using this technology to promote fake investments can be found on the website of the Education Centre for Financial Market Security at: https://cebrf.knf.gov.pl/deepfake

Recovery scam

In relation to 2024, we can see a significant increase in the occurrence of advertisements promising the recovery of stolen funds (recovery scam). With this type of scam criminals impersonate firms or organisations engaged in the recovery of lost funds.

This is actually a next step following an investment scam: recovery scam aims to deceive people who have already fallen victim to a fake investment. Criminals often approach victims and introduce themselves as law firms, lawyers or debt collectors claiming they can recover lost funds.

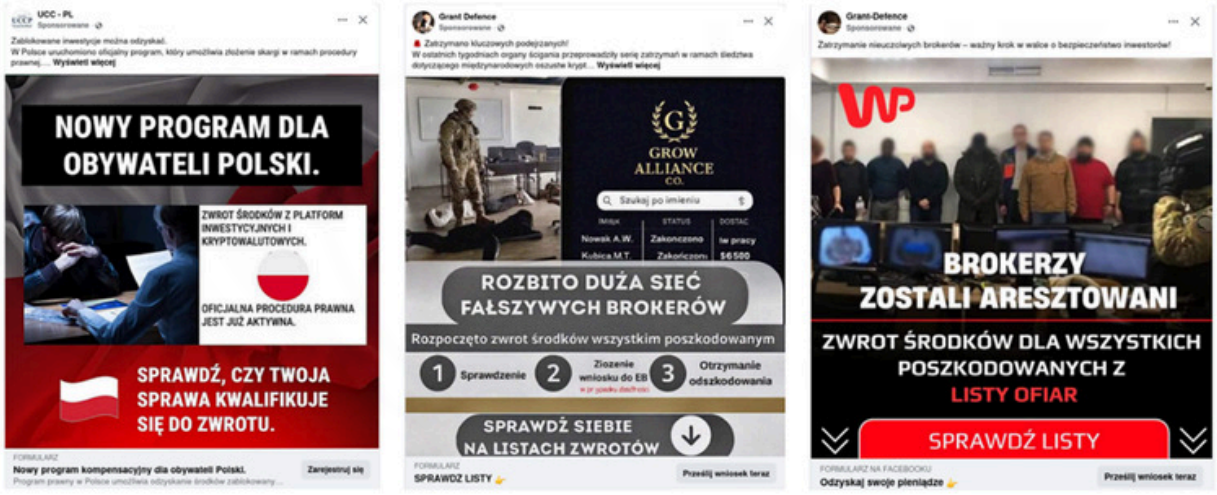


Image 16. Fake advertisements offering recovery of stolen funds

The modus operandi here is exceptionally cynical and compatible with the original investment scam. The advertisement redirects a potential victim to a site or form to steal contact details. The phone number or e-mail address so obtained allows perpetrators to contact the victim and manipulate them into making the payment by claiming that the payment is allegedly necessary to recover stolen funds.

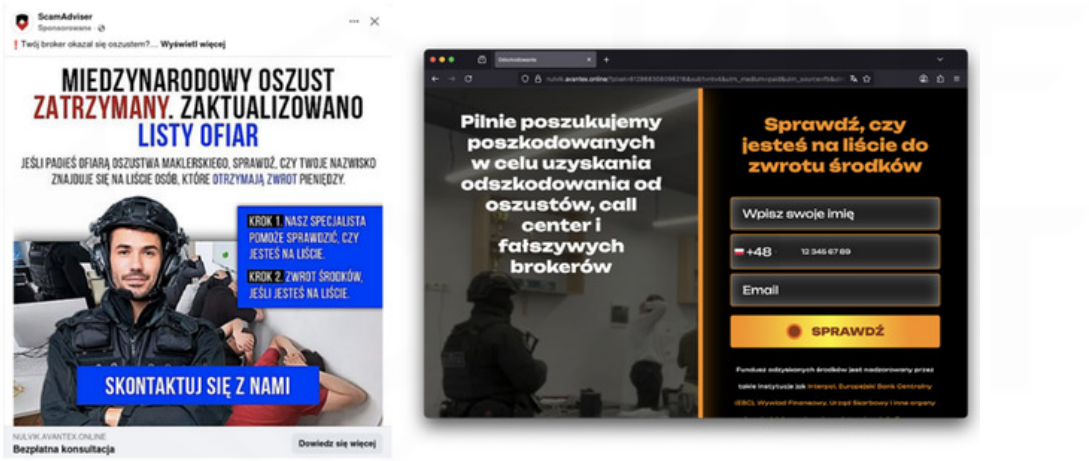


Image 17. Fake advertisement offering recovery of lost funds and the redirection site

The money swindling process may last months. After the initial payment, new requests will follow: for new legal fees, administrative fees, taxes or commissions. Each payment is described as 'the last' step towards money recovery. This way some victims lose even more tens of thousands of Polish zloties, believing the recovery of lost funds is getting closer and closer.

Advice for internet users

Check all assistance offers. Before you decide to transfer your money to anyone, contact real institutions or organisations. Do not pay for promises. Avoid firms and individuals who request advance payment for money recovery. Report scams: every scam should be reported to competent law enforcement authorities to help stop the criminals. Seek legal assistance.

Advertisement masking

A decrease in the number of reported advertisements does not reflect the real decrease in the scale of the threat occurring on a platform. In order to avoid instant blocking, criminals are becoming increasingly creative and effective in masking their actions; this is why their campaigns are more difficult to track and they can have more time to reach users before the campaign is banned.

The use of versioning

Cybercriminals use Facebook's ads functionality, which allows them to create many variants of the same advertisement. The functionality is used by criminals for camouflage: one malicious version is hidden among many neutral ones. The result is that the preliminary view or check of an ad banner do not raise any concern. Attack detection is also hindered by the Ad Library itself. Although the system detects multiple versions of an ad, the library can restrict the view to a single image and it might not show the image that is currently displayed to users.

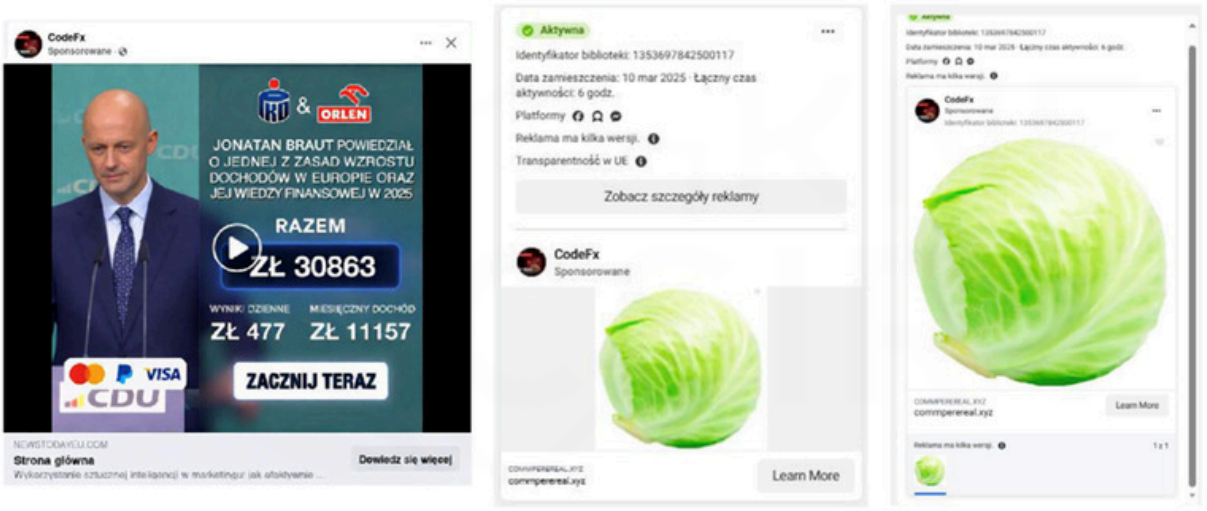


Image 18. How criminals use versioning

The use of letters from a different alphabet

Criminals use text obfuscation, a technique of replacing letters with characters from other alphabets which at first glance look very similar. The text is readable to the user but constitutes a totally different string of characters for search algorithms. In consequence, a phrase entered in the search box and visible on the screen gives no result because the system would require insertion of exact non-standard characters that were used by the fraudsters. Even a slight change in one letter makes the advertisement 'invisible' to a person searching for the phrase using key words. This often makes the manual identification of the source of the attack impossible without the direct link to the advertisement.

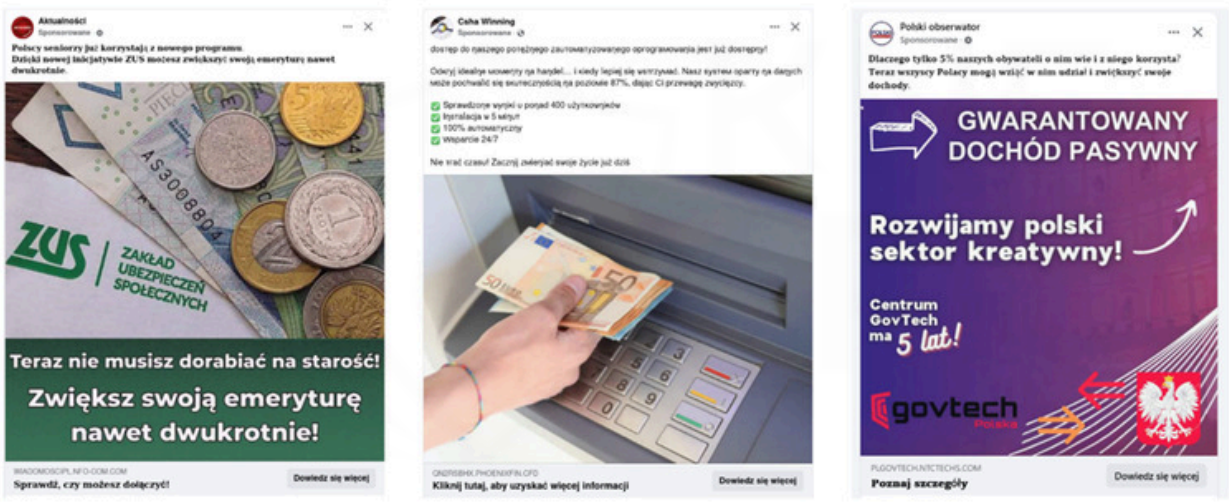


Image 19. Examples of letters from other alphabets

Artificial extension of video length

Fraudsters sometimes replace static images with videos. While doing so, they use video length extension: the fraudsters' proper message lasts only 1–2 minutes, while the full video is artificially extended multiple times using black background or a static image. Such an action probably exploits performance gaps of verification algorithms, which fail to carefully analyse the whole material.

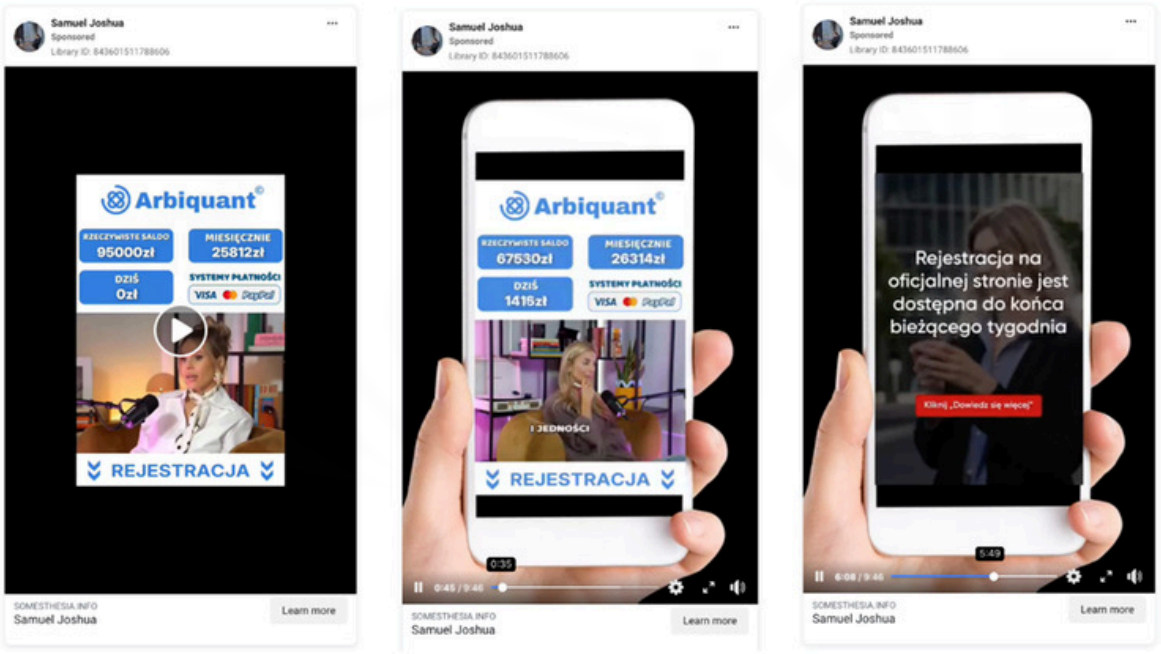


Image 20. Artificial extension of video length

Plugs

A relatively frequent strategy is to use completely neutral images (thumbnails), which do not suggest any scam visually. This is a deliberate strategy targeting analysts and automatic verification systems based on image analysis. Since the image does not raise any concern, the algorithm approves the advertisement for publication, and the analyst might overlook it. The malicious nature of the campaign will reveal itself only at a deeper level: in the content of a post or after clicking on the redirecting link, which makes the superficial screening ineffective.

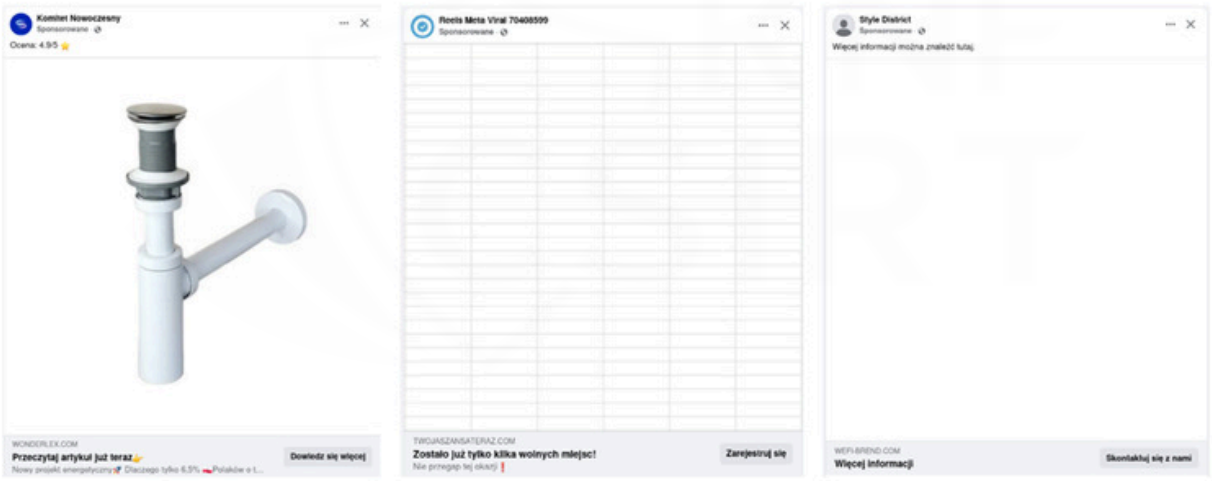


Image 21. Examples of plugs used in fraudulent advertisements

Masking malicious content (versioning, obfuscation, plugs, video length extension) does not occur as single incidents any more but as part of a ‘regular’ strategy of avoiding moderation and keeping the advertisement active as long as possible.

2.2 FAKE STORES: A GROWING THREAT

Introduction

Today, online shopping is one of most common methods of buying products. Availability and convenience of online shopping are the reasons why users eagerly choose online stores. However, the growing popularity of online shopping creates space for criminal actions. In recent years, we have seen a high number of sites impersonating legitimate online stores. Their main purpose is to steal money and personal data of users who mistakenly treat such sites as a trusted store for their purchases.

Scale

In 2025, CSIRT KNF requested the blocking of 404 domains of fake online stores. Criminals impersonated mainly high-profile brands from industries such as fashion, sports and home design. By exploiting the image of e-commerce leaders, the fraudsters would create confusingly similar sites in oSites of fake online stores show multiple items at very low prices. The key characteristic is the availability of all items despite heavily discounted prices. The site design is inspired by the layout and styles of famous brands to create a sense of trust among potential victims. To deepen the trust, fraudsters add alerts about allegedly completed transactions which are displayed when the user views items.

The fraudsters often use time pressure by adding high-urgency phrases (e.g. ‘the clock’s ticking!’) regarding the time left until the end of a special offer or a limited number of available items. These techniques are based on psychological mechanisms which induce users to be less vigilant and thus make purchasing decisions faster.

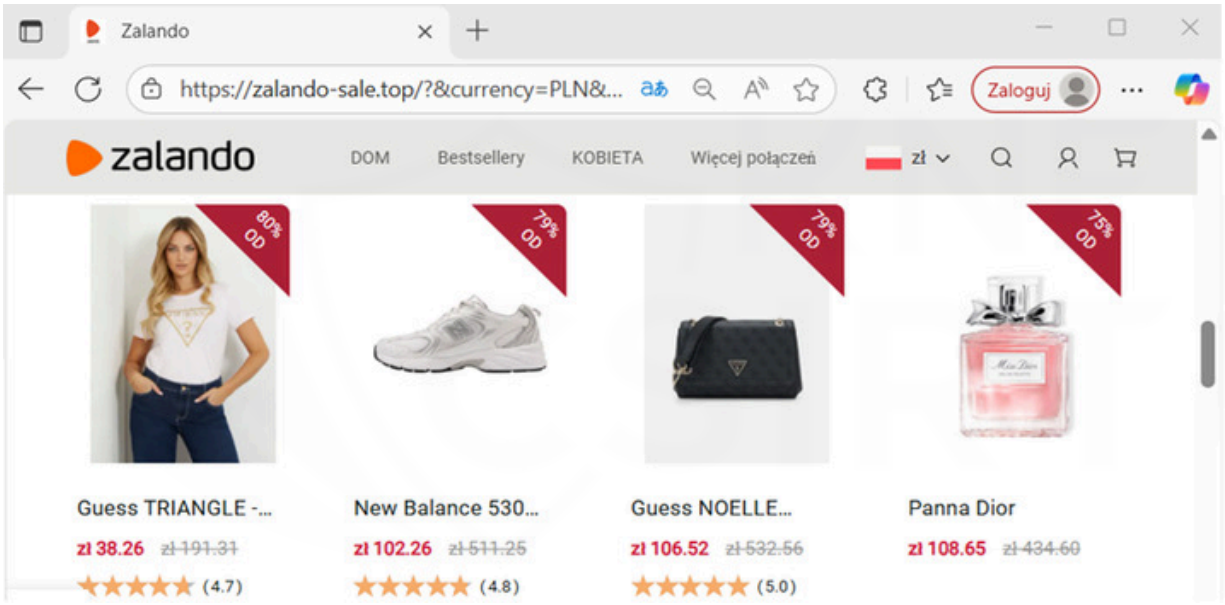


Image 22. Fake Zalando site with discounted products

Scam process

Stage 1: catching attention

A scam usually starts with an ad displayed on social media. The ad uses a logo of a famous brand or catches attention with a price reduction. The ad is supposed to redirect a user to a fake webshop page.

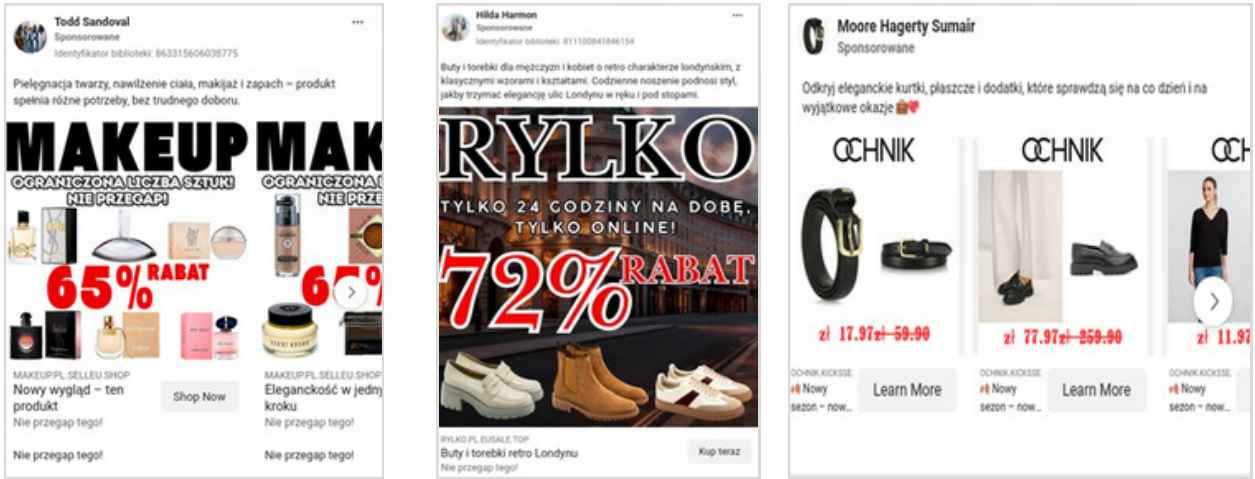


Image 23. Fake advertisements on Facebook in which cybercriminals impersonated famous stores

Stage 2: fake website

After being redirected to the site, the user comes across a website imitating the layout of a real store. Domains of such websites are created so as to impede their identification. The site offers many products at good prices, often using further promotional mechanisms to encourage quick purchase. Users can see ‘customers recently bought items’ messages, which are to suggest that many customers use the site to buy many items, and the clearly visible counter showing the time left until the end of the special offer urges the user to make a quick decision.

Image 24. Counter showing the time left until the end of special offer

Fake stores are often visually indistinguishable from their original version. The only element which allows users to distinguish a fake store from the real one is the domain name, which – although very close to the original – remains the only detectable difference. Criminals often used domains confusingly similar to the real domains of well-known brands, hoping that the user wouldn’t spot the subtle difference in the URL syntax.

Comparison between a fake site of the Reverb store and the original (official) site:

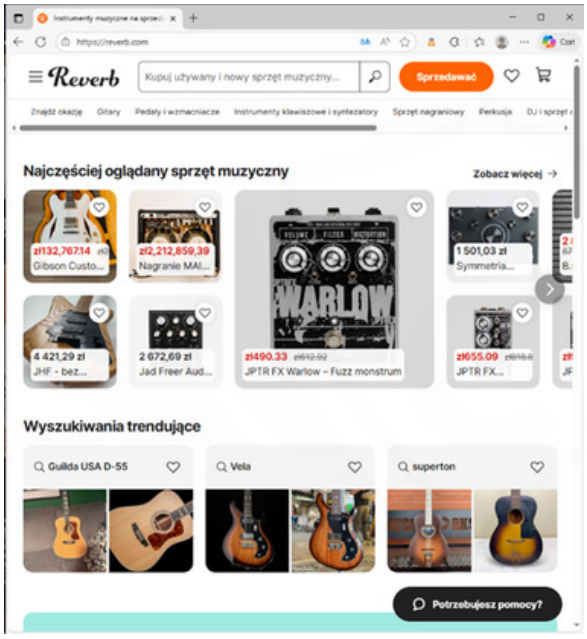


Image 25. Real site of the Reverb store

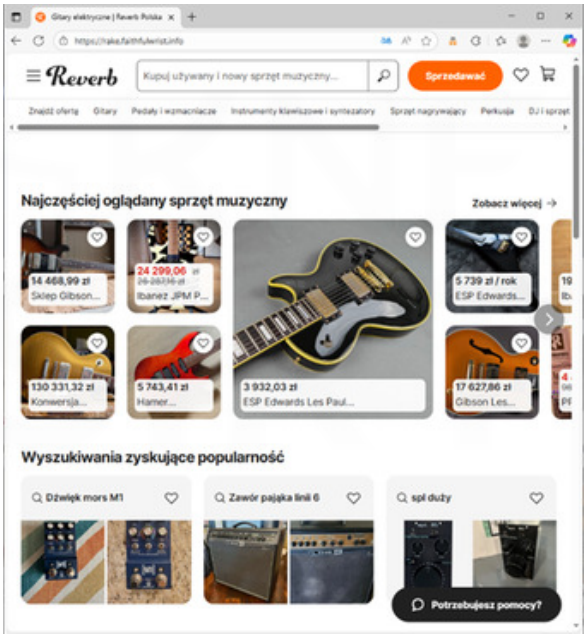


Image 26. Fake site of the Reverb store

Stage 3: stealing personal and payment card details

After selecting items, the user is redirected to a form and asked to enter their personal details, such as forename, surname, address, and phone number. Next, the site requests payment card details. After the details are entered, there is a risk of attempted unauthorised transaction and the risk of capturing information which then can be used for further crimes.

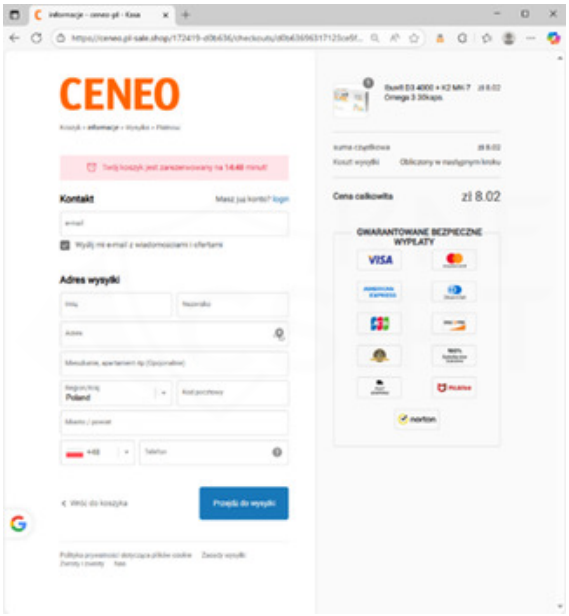


Image 27. A fake delivery site impersonating ceneo.pl

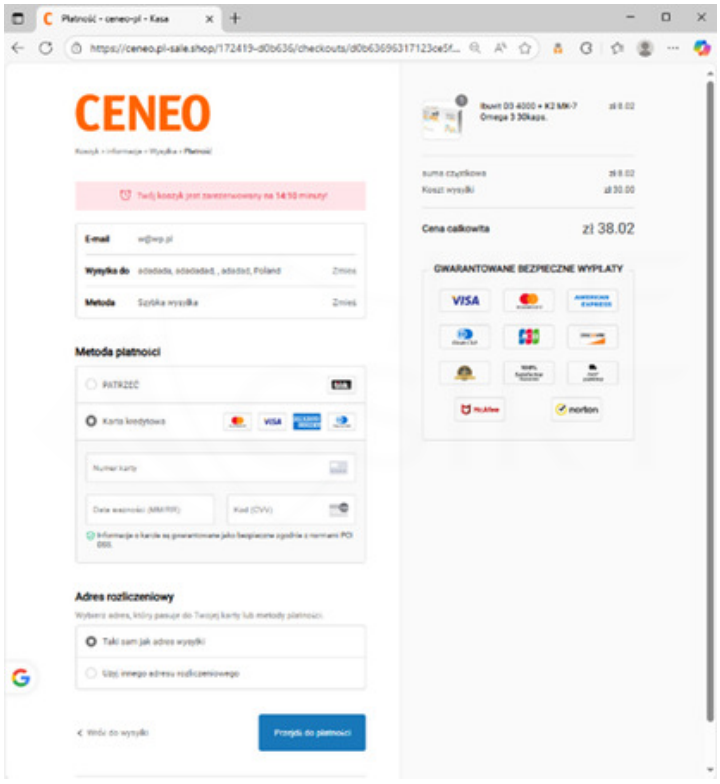


Image 28. A fake payment site impersonating ceneo.pl

Recommendations for internet users

- Check the source of the ad on social media and make sure it has been posted by the official, trustworthy profile.
- Search for the company name in the CEIDG or KRS database and make sure that the firm actually exists.
- Check the terms and conditions and the privacy policy for any inconsistency or error; these documents are often copied by fraudsters indiscriminately and contain many obvious errors.
- Check site addresses and make sure they do not raise any concern. Insert the store name in a new browser window and compare site addresses. Search for the domain name in the whois.com database and check the domain's creation date.
- Stay vigilant about tempting offers; always be extra careful when an online offer seems too good to be true, especially for limited-time offers.

2.3 SCAMS TARGETING BANK CUSTOMERS

In some of the identified phishing campaigns, cybercriminals impersonated financial market entities directly. They would create sites confusingly similar to the official banking sites to get the users to let their guard down. The goal was usually to steal online banking login details.

Scale

In 2025, CSIRT KNF requested a website blocking order for 256 sites linked to banking scams. This accounts for only 0.61% of all domains reported, but such sites are a very serious threat to online banking customers. Those sites are used to steal login credentials directly and serve as a link in a more complex chain of social engineering attacks, causing direct financial losses to affected customers.

Characteristics

Criminals would use multiple methods to distribute malicious sites. The methods included fake advertisements, SMS messages. and e-mails. The strategy involved sending messages with false information, for example about an allegedly rejected transfer and the urgent need to update details so that the transfer could be effected. The message contained a link which, if clicked on, would take the victim directly to a phishing site used to steal confidential information, such as online banking logins and passwords or payment card details.

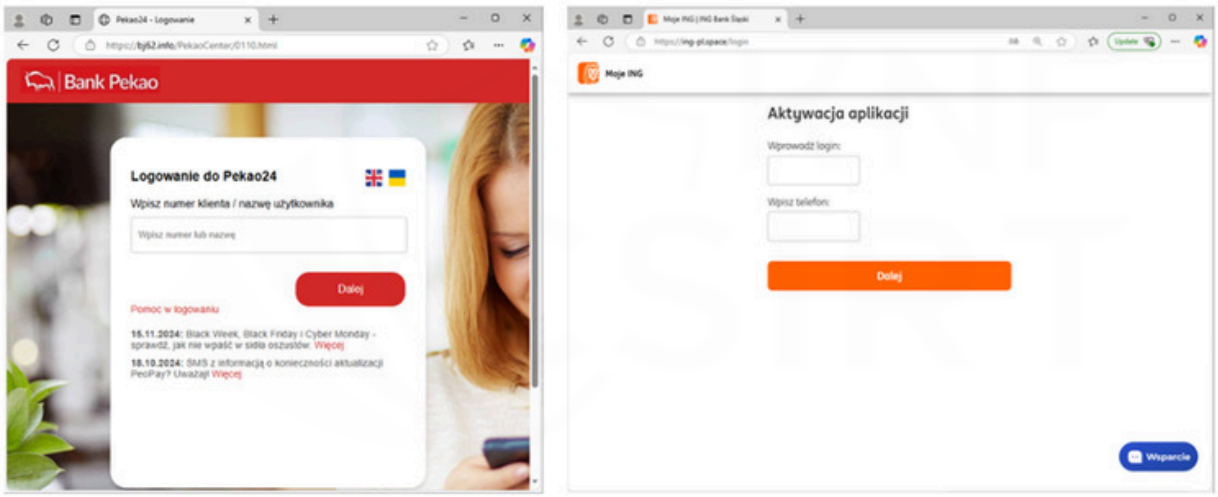


Image 29. Examples of fake online banking login sites

Fake e-mails

Cybercriminals would send e-mails saying, for example, it was necessary to update online banking details. The message contained a link which, if clicked on, would redirect a victim to a phishing site imitating the real online banking login site.

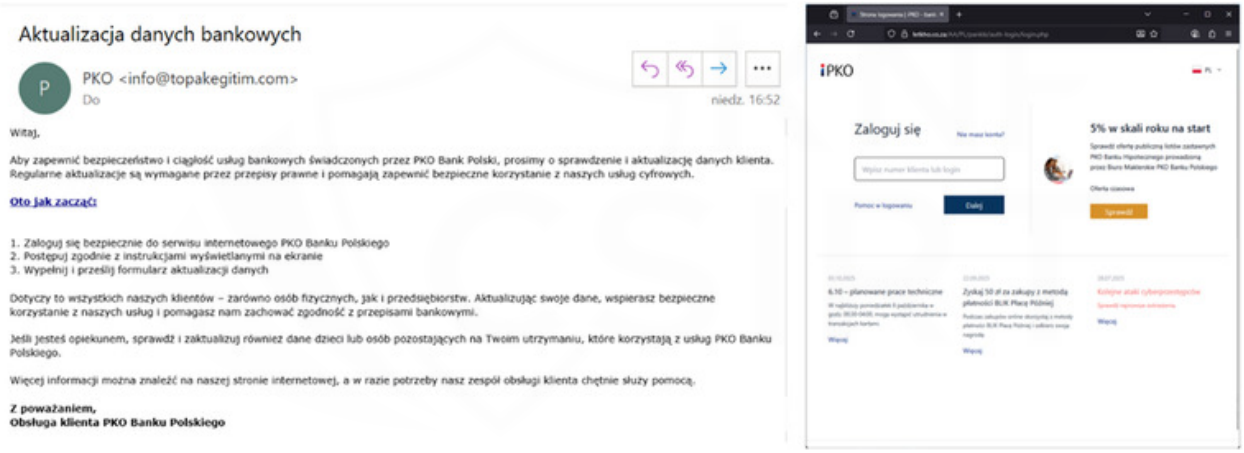


Image 30. A fake e-mail impersonating PKO Bank Polski and a rogue site stealing login credentials from users

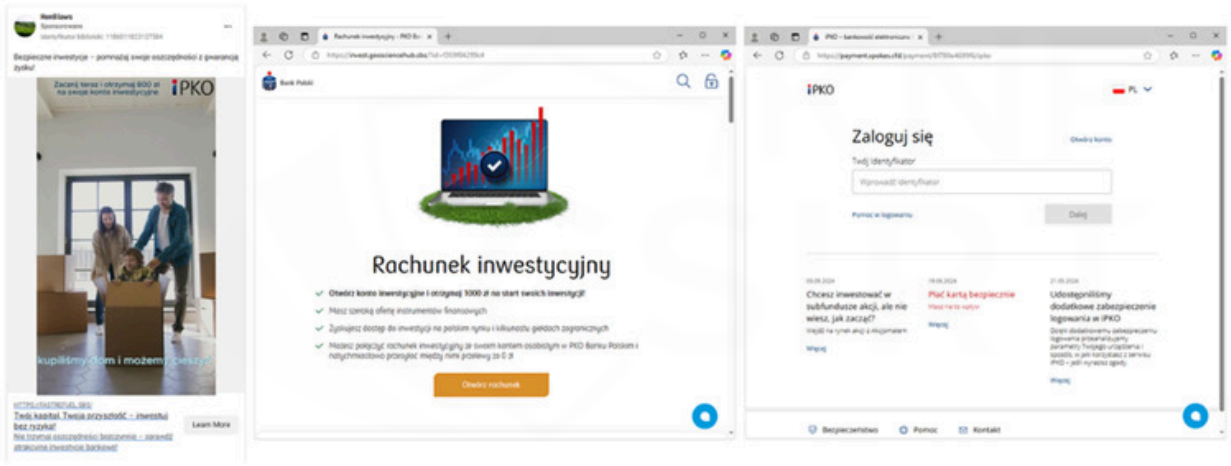


Image 31. A fake advertisement and a site impersonating PKO Bank Polski

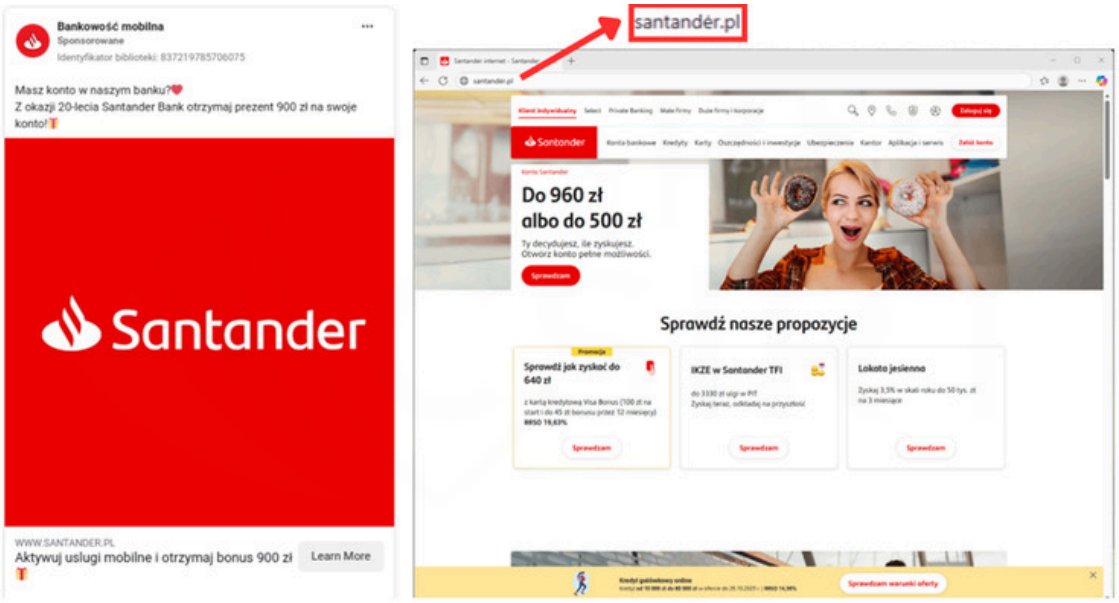


Image 32. A fake advertisement and a site impersonating Santander Bank Polska

To decrease users' vigilance, fraudsters would deliberately include a real bank's domain in their ads. Despite that, what actually happened was that the victim was redirected to a fake online banking site. In that case, scammers would also use Punycode. The system allows them to use, in a domain name, characters from other alphabets (e.g. the Cyrillic script), which visually are very difficult to distinguish from standard characters, making the fake address in the web browser's address bar look almost identical to the real one. On the malicious site, cybercriminals would steal not only login credentials but also a series of confidential personal data, including Personal Identification Number (PESEL) and mother's maiden name. The data so obtained could be used for further crimes, for example an unlawful attempt at taking out a loan.

Search engines

In addition to social media marketing, criminals would also actively use web search engines to distribute fake online banking sites.

This fraud pattern is based on the assumption that some online banking customers do not enter the URL directly in the web browser's address bar. Cybercriminals would use website positioning, so that their malicious site was displayed high in the search results.

Consequently, by clicking on such a link, the user was convinced that they are entering the real website of their bank. In reality, however, they were redirected to a rogue site being a visual copy of the original website. The details entered on the fake site would go straight to cybercriminals.

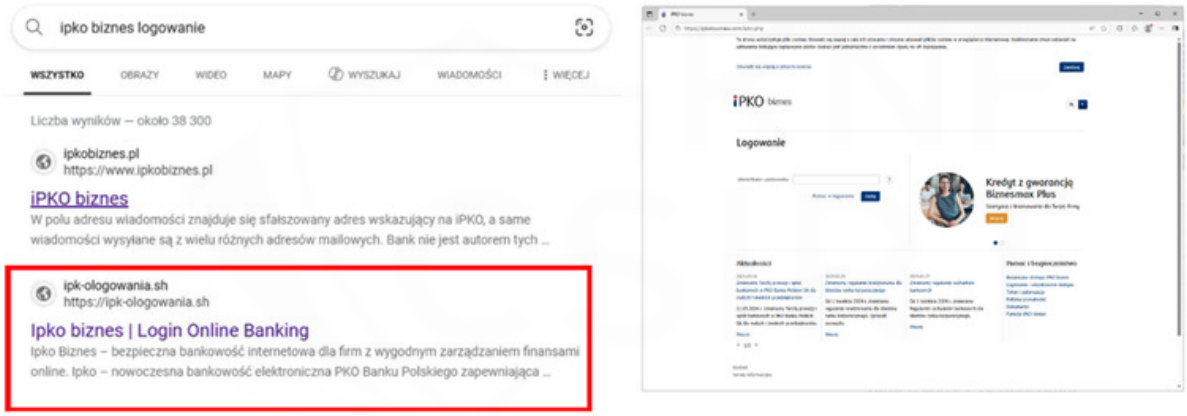


Image 33. Fake PKO BP login site in search results

Fake SMS messages

Identified phishing strategies also included smishing – the use of fake SMS messages.

Fraudsters would pretend to be credible institutions, such as banks or courier service operators, and informed victims about alleged issues, for example the need to pay more money for the shipment or problems with the online banking account.

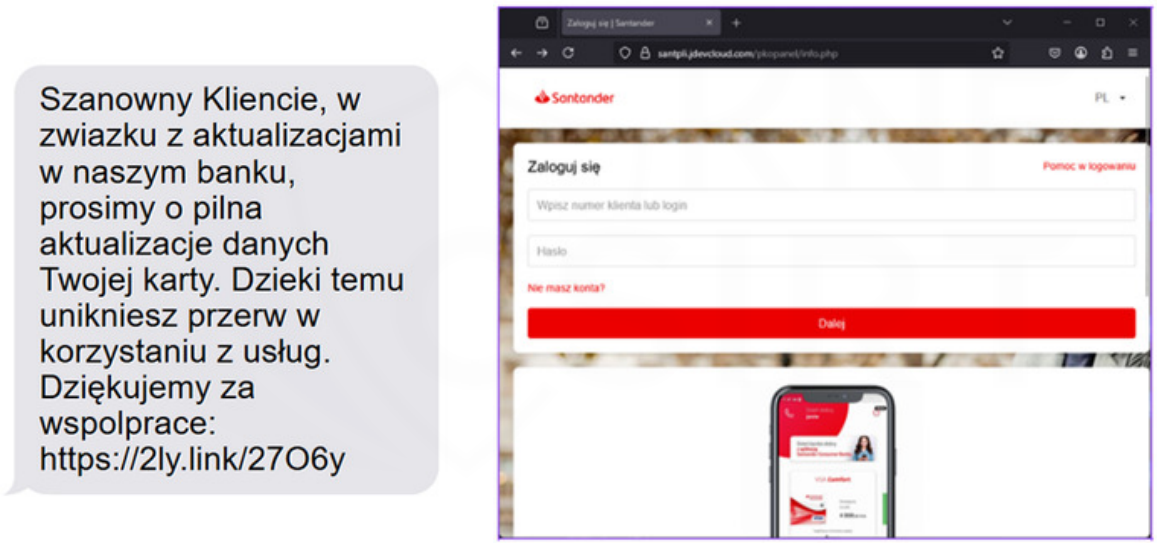


Image 34. An SMS message and a site impersonating Santander Bank Polska

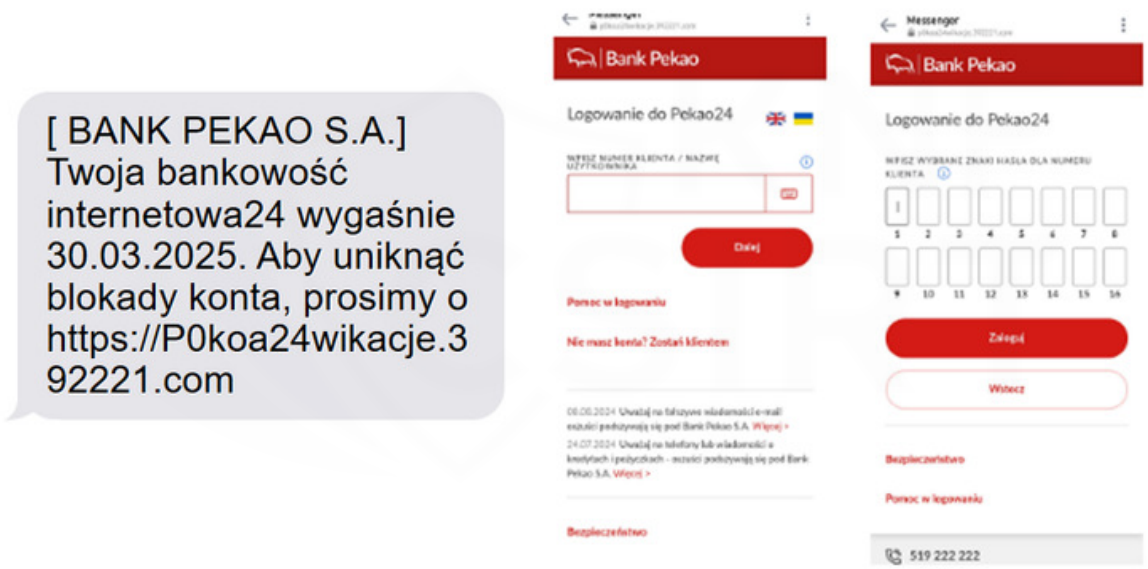


Image 35. A fake SMS message impersonating Bank Pekao S.A.

Apart from the attacks targeted directly at the banking sector, a significant percentage of incidents were campaigns exploiting the image of postal and courier service operators. The attack scenario was based on a social engineering technique of suggesting the need to pay an alleged outstanding fee to unblock the delivery. The low amount of claim (usually a few Polish zloties) was to decrease the victim's vigilance and induce them to use a dummy payment gate, designed for stealing full payment card details. The consequence of providing card payment details was the execution of unauthorised online transactions for sums which largely exceeded the fee declared.

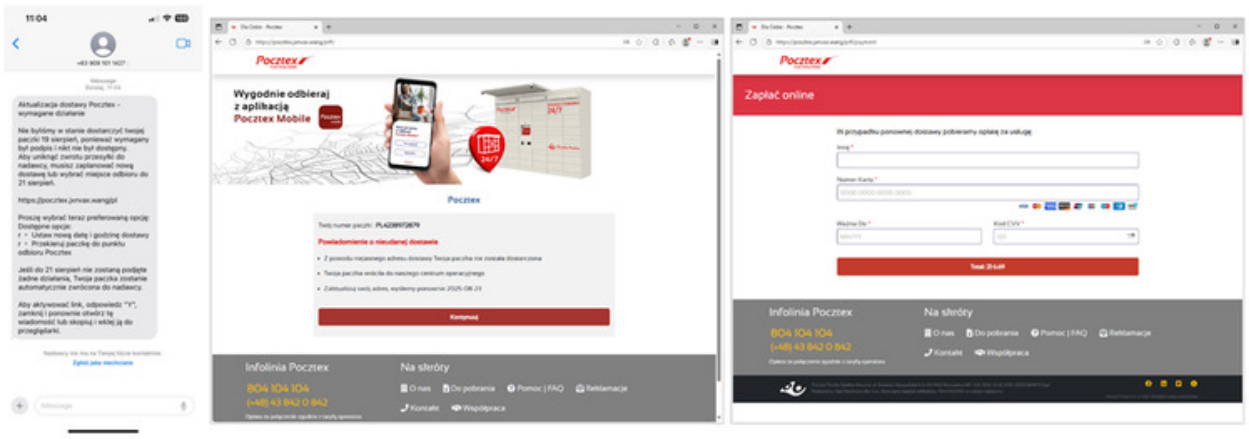


Image 36. An SMS message and a site impersonating Pocztex

These campaigns would exploit the image of leading Polish logistics service providers: InPost, Poczta Polska, DHL, DPD, etc. In order to lend credibility to their attack, the criminals would often use SMS Spoofing (sender ID spoofing). Thus, malicious messages were automatically grouped by victims' devices in one thread with authentic messages from carriers. Such action could decrease the recipients' vigilance.

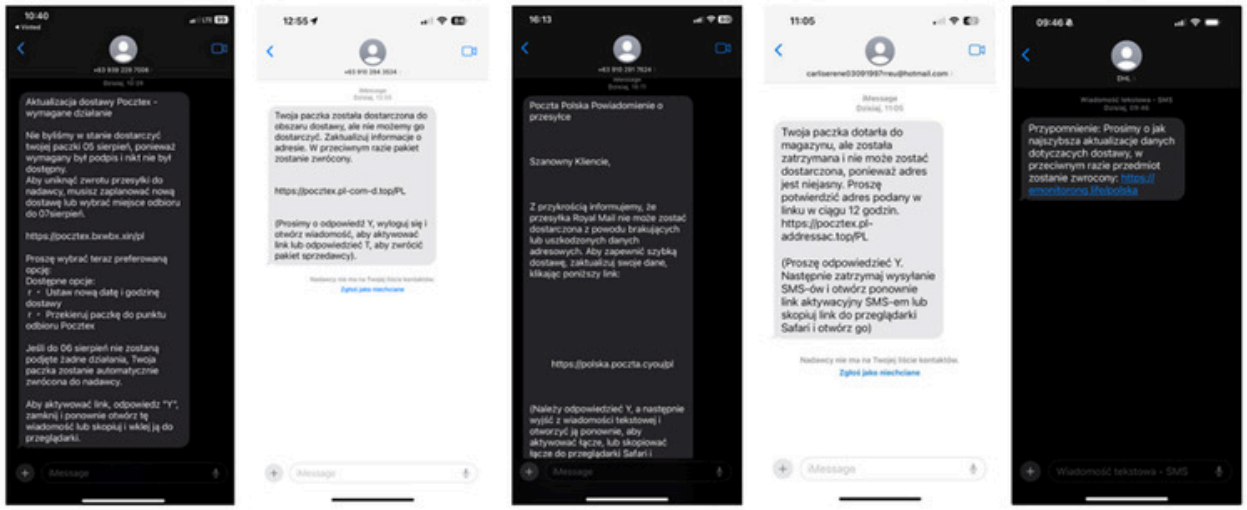


Image 37. Examples of SMS messages impersonating courier and postal services

2.4 MALWARE

One of the categories of threat to financial market participants is malware. CSIRT KNF engages in, among others, monitoring, analysing and exchanging information about malware samples and malware campaigns. Although last year's scale of malware-related attacks was not as high as the occurrence of phishing or scams involving fake investments, the threat from malware certainly should not be ignored.

In 2025, we could see malware targeting both users of devices running on Windows and holders of Android-based mobile devices. The malware we warned against was found in scams exploiting the image of entities and products from fields such as: banking, event industry, tourism or e-commerce. Here is an overview of the threats we informed you about on the CSIRT KNF social media channels.

- E-mail campaign impersonating Booking.com, where attackers would send out a fake message requesting payment for a seemingly attached invoice. The e-mail actually contained a HTML file which, if opened, would trigger a message saying the document cannot be displayed and what next steps the recipient should take. The execution of the instruction could result in the victim's device infection with malware [2].

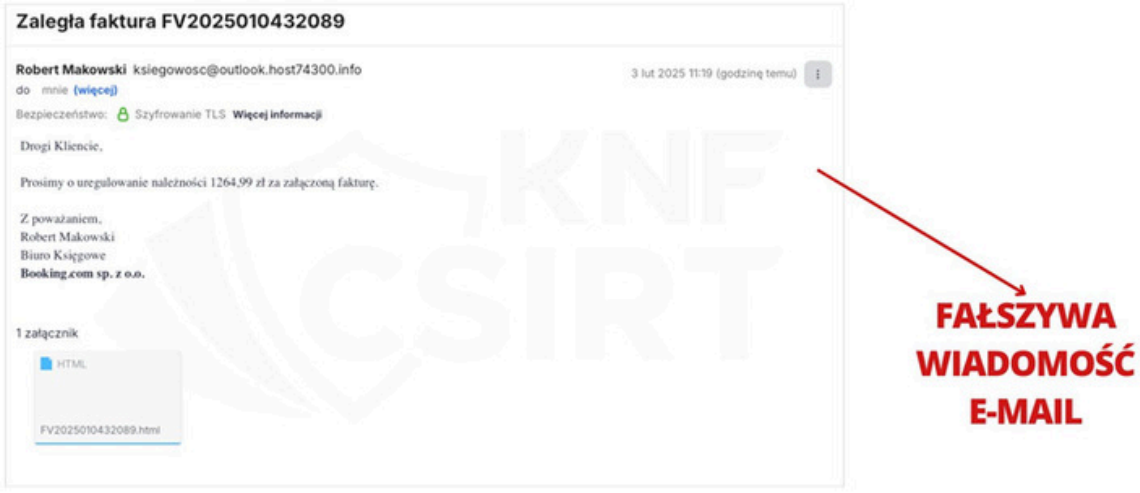


Image 38. An e-mail impersonating Booking.com

[2] https://x.com/CSIRT_KNF/status/1886417315983470664

- A campaign impersonating InPost where fraudsters would send an e-mail to inform the recipient about the parcel 'awaiting' status. To collect the parcel, the recipient would have to open the document with parcel location and collection code. The attached archive contained malware which could take over login details and other sensitive information[3].

Image 39. An e-mail impersonating InPost

- A campaign where attackers would pose as mBank by sending a message about a fictitious transaction related to the settlement of an invoice. More information about the payment details were in the attachment (a malicious TAR archive), which due to its double extension could be misinterpreted as a PDF document[4].

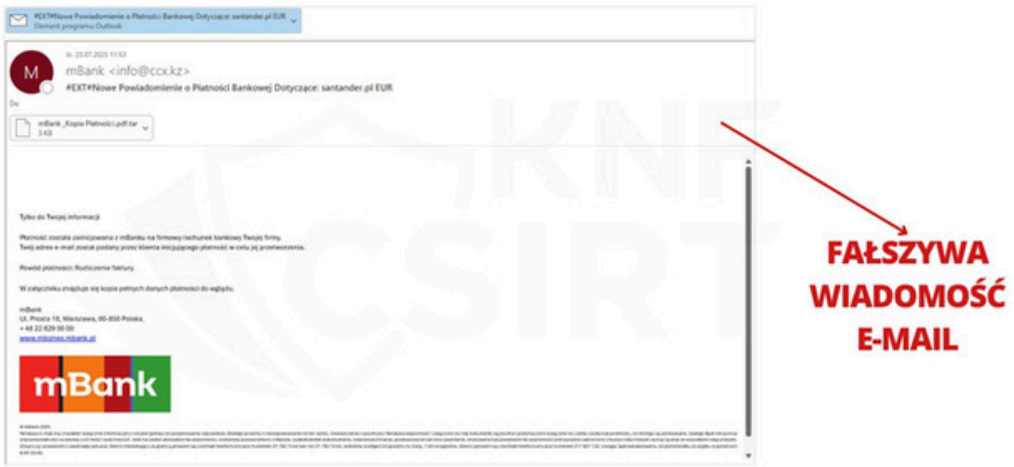


Image 40. An e-mail impersonating mBank

[3] https://x.com/CSIRT_KNF/status/1942524257222774804
[4] https://x.com/CSIRT_KNF/status/1950502256303919508

A separate sub-category of observable threats was mobile malware, where attackers would evidently focus on users of the Android system. The malware we analysed in this area occurred in the following cases:

- In January 2025, we issued a warning against a fake application posing as OLX Payments. The infection process took place in stages. As soon as the user launched the malware, it displayed a message requesting the user to update Google Services in order to continue to use the application. If the user installed and launched the package from the next infection phase, they would receive instructions on granting authorisations related to the Accessibility Services function, which in turn could result in the take-over of control over the device. In further steps, the fraudulent application impersonated the InPost brand and displayed fake forms for logging into online banking[5].

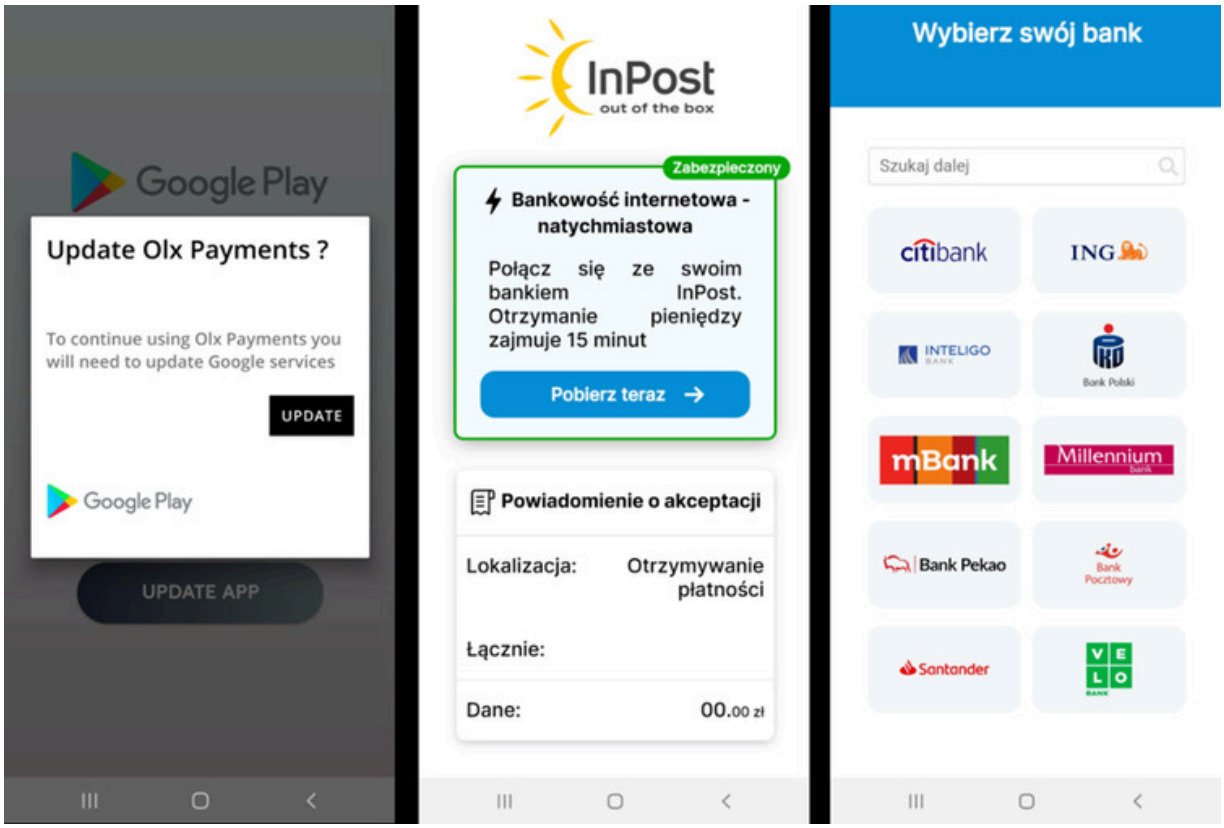
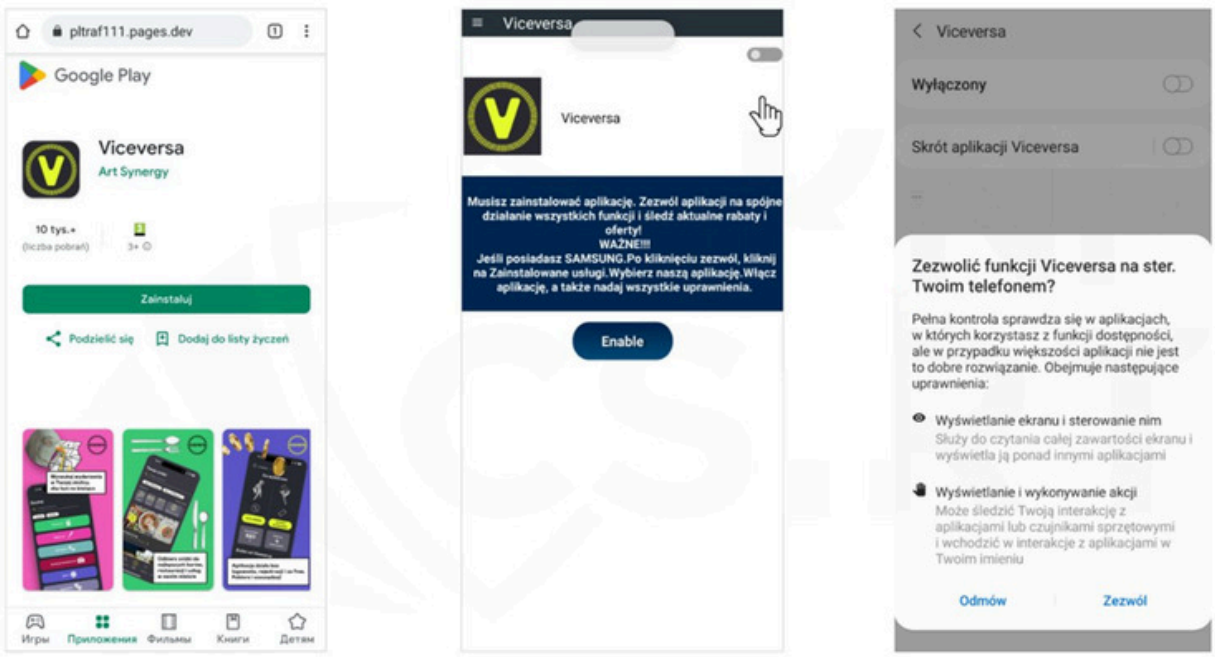


Image 41. The screen of the fake OLX Payments app

[5] https://x.com/CSIRT_KNF/status/1882074515229807056

- In late March, we noticed impersonation of the Viceversa app. In that case, we were dealing with a fake site imitating Google Play to distribute malware. A visit on the site would allow the user to download an untrusted APK file onto the user's device. Having launched the fraudulent app and gone through next steps, the victim could activate the Accessibility Services system function and potentially pass the control over the device to the malware[6].



Grafika 42. Strona dystrybuująca i ekrany fałszywej aplikacji Viceversa

- The end of May 2025 was the time when we issued a communication about malware impersonating a non-existing IKO Lokata app. The malware sample based on which we performed our study had been collected through one of our analytical services. Roughly at the same time, we spotted malicious ads on Facebook whose style was similar to the application we analysed. During the analysis, however, the addresses that the fraudulent ads would lead to did not provide us with the malware sample in question. Visually, the malware's style was inspired by the IKO mobile app.

[6] https://x.com/CSIRT_KNF/status/1906691444984717615

Functionally, after being launched, the malware displayed a window with information that a new version of the app was available, asking the user to proceed with the update. The update was supposed to ensure that the software would run smoothly. Going through next steps – installation of an additional module and activation of the Accessibility function – could expose the victim to the next stage of the infection process, in a way typical of an Android-type malware. The artefacts we analysed indicated we might be dealing with a malware family named Crocodilus [7], [8]. More details on the malicious sample can be found in our article titled Analiza złośliwej aplikacji mobilnej IKO Lokata [Analysis of the malicious IKO Lokata mobile app] [9].

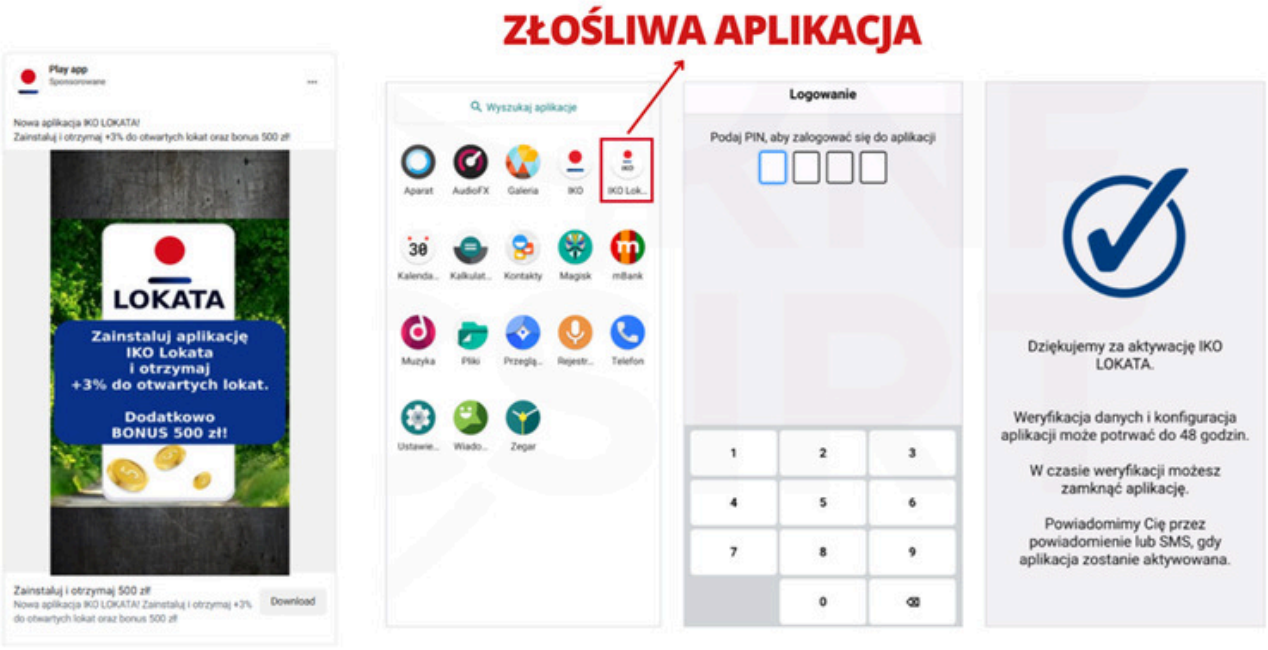


Image 43. Social media ad and screens of the fake IKO Lokata app

In the space of mobile malware, directed towards holders of Android devices, we identified a new attack model – the NFC Relay attack. A malicious use of the Near Field Communication (NFC) technology was already mentioned in 2024 by our neighbours south of Poland and presented by researchers from ESET. The use of malware was to enable the NFC data saved on the victim's card to be relayed through an infected phone to an attacking device

[7] https://www.threatfabric.com/blogs/exposing-crocodilus-new-device-takeover-malware-targeting-android-devices
[8] https://x.com/naumovax/status/1906727042353107402
[9] https://cebrf.knf.gov.pl/images/IKO%20Lokata%20Malware%20-%20Analiza.pdf

Fraudsters could attempt to use the data so obtained, for example to make a contactless withdrawal of funds from an ATM (while attempting to also steal the PIN code to the victim's card) or to effect contactless payment using a payment terminal. It should be noted that the NFC Relay technique described by ESET is based on a legal NFCGate research solution[10], whose functionality was abused by attackers[11].

In 2025, NFC Relay scams were the subject of our warnings multiple times. The common denominator of the cases in question were fake applications imitating banking solutions (we have seen cases of impersonation of PKO BP, Santander, ING, and SGB Bank S.A.). After being opened, the applications would request placing a card (implicitly, a payment card) on the back of the device. At least in one case we saw an outgoing communication after a test RFID card was placed on the device (we were not able to verify whether the operation would success in the case of a payment card and whether the data being transmitted would be sufficient to withdraw funds), and in some other cases, following the fulfilment of appropriate conditions, a window imitating a 'PIN pad' appeared.

The distribution of malware would each time take place without Google Play and involve installation of the application from an untrusted source (we have seen, for example, distribution of packages using the files.fm hosting service)[12],[13],[14],[15],[16]. With the growing popularity of this scam model, we included it in the cybercrime trends in 2025 and provided its description in: Krajobraz cyberzagrożeń w polskim sektorze finansowym 2025 (GTL) [Cyber threats in the Polish financial sector 2025 (GTL)][17].

[10] https://github.com/nfcgate/nfcgate
[11] https://www.welivesecurity.com/en/eset-research/ngate-android-malware-relays-nfc-traffic-to-steal-cash/
[12] https://x.com/CSIRT_KNF/status/1887474108323037617
[13] https://x.com/CSIRT_KNF/status/1952325687584448969
[14] https://x.com/CSIRT_KNF/status/1953381743714529560
[15] https://x.com/CSIRT_KNF/status/1969040488402673831
[16] https://x.com/CSIRT_KNF/status/1983536938880581770
[17] https://cebrf.knf.gov.pl/images/GTL_2025_FINAL.pdf

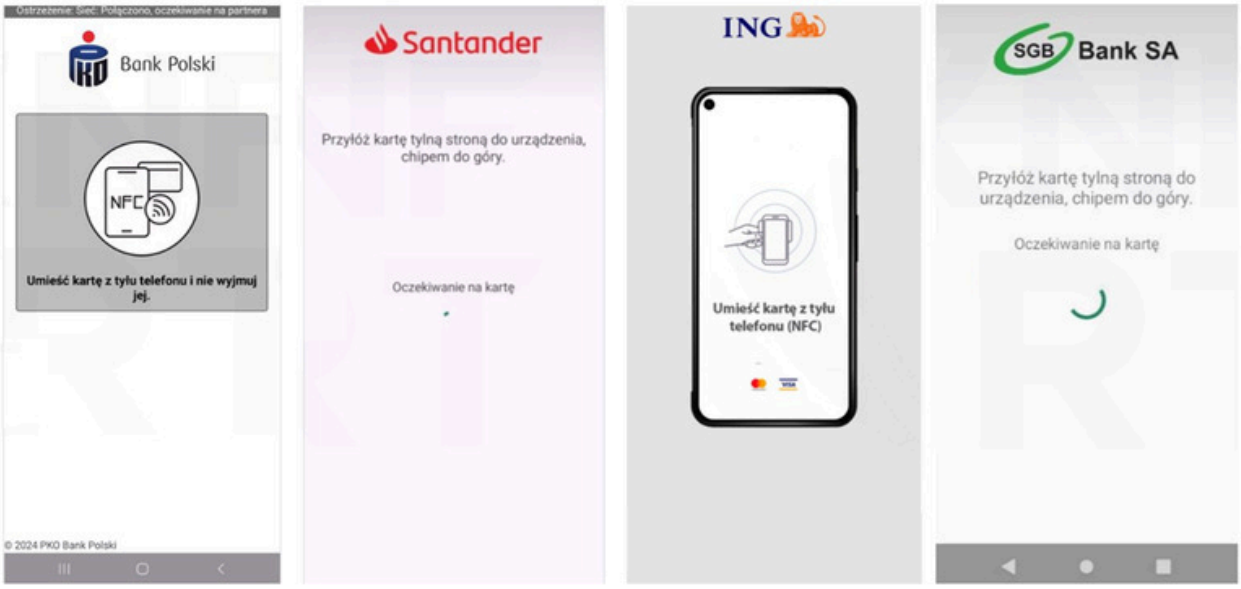


Image 44. The use of banks' logos in fake NFC applications

```
import de.tu_darmstadt.seemoo.nfcgate.db.pcapng.ISO14443Stream;
import de.tu_darmstadt.seemoo.nfcgate.db.worker.LogInserter;
import de.tu_darmstadt.seemoo.nfcgate.gui.fragment.CaptureFragment;
import de.tu_darmstadt.seemoo.nfcgate.gui.fragment.RelayFragment;
import de.tu_darmstadt.seemoo.nfcgate.network.UserTrustManager;
import de.tu_darmstadt.seemoo.nfcgate.nfc.NfcManager;
import de.tu_darmstadt.seemoo.nfcgate.util.NfcComm;
import java.io.IOException;
import java.util.Iterator;
import java.util.List;

/* loaded from: classes.dex */
public class MainActivity extends AppCompatActivity {
    NfcManager mNfc;

    public NfcManager getNfc() {
        return this.mNfc;
    }

    @Override // androidx.fragment.app.FragmentActivity, androidx.activity.ComponentActivity, androidx.core.app.ComponentActivity, android.app.Activity
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        SharedPreferences.Editor editorEdit = PreferenceManager.getDefaultSharedPreferences(this).edit();
        editorEdit.putString("host", "[redacted]");
        editorEdit.putString("port", "[redacted]");
        editorEdit.putString("session", "[redacted]");
        editorEdit.apply();
        setContentView(R.layout.activity_main);
        setSupportActionBar((Toolbar) findViewById(R.id.toolbar));
        getSupportFragmentManager().beginTransaction().replace(R.id.main_content, new RelayFragment()).commit();
        NfcManager nfcManager = new NfcManager(this);
        this.mNfc = nfcManager;
        if (!nfcManager.hasNfc() || !this.mNfc.isEnabled()) {
            showWarning(getString(R.string.error_NFCCAP));
        }
        UserTrustManager.init(this);
    }
```

Image 45. A decompiled portion of one of the samples, showing how a code from the NFCGate research project was used in a fake application[18]

[18] https://github.com/nfcgate/nfcgate

- In the first half of December, we covered a fake mobile app named ‘Klucz bezpieczeństwa Pekao’ [Pekao security key]. When launched, the app displayed a screen requesting a ‘Play component’, which was supposed to ensure a safe and stable operational environment of the app. In reality, installation of the component triggered another screen, which on the pretense of requesting configuration encouraged the user to assign the app authorisations to the ‘Accessibility Services’ function. This in turn could lead to someone else’s taking over control of the device [19]. Our analysis of the downloaded ‘Play Component’ package has identified a certificate fingerprint identical to the certificate used in the payload of the FvncBot trojan, described in the first half of December by Intel471 [20].

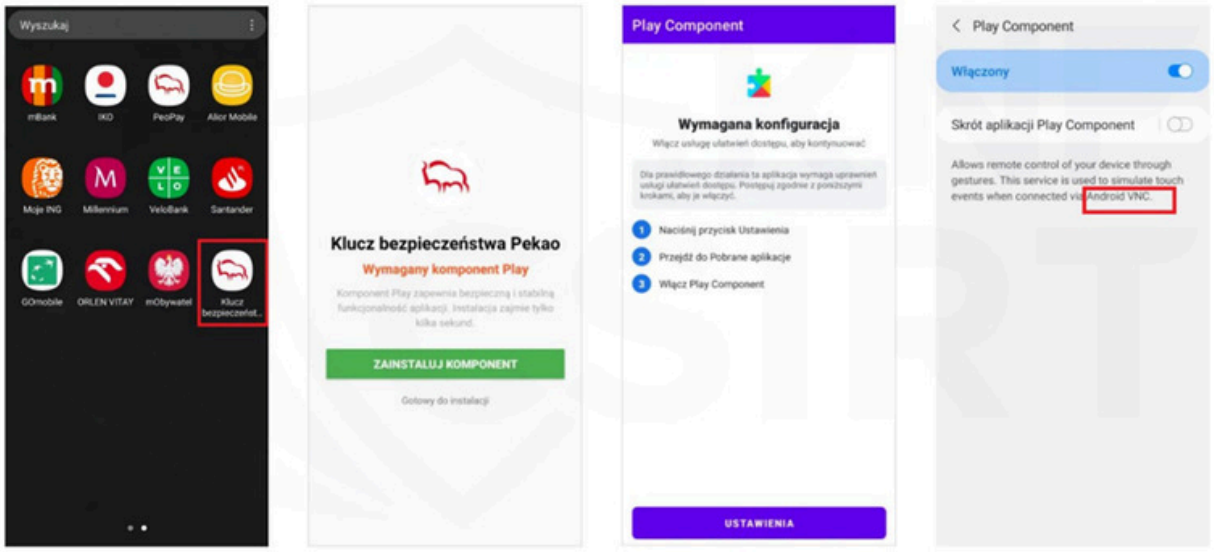
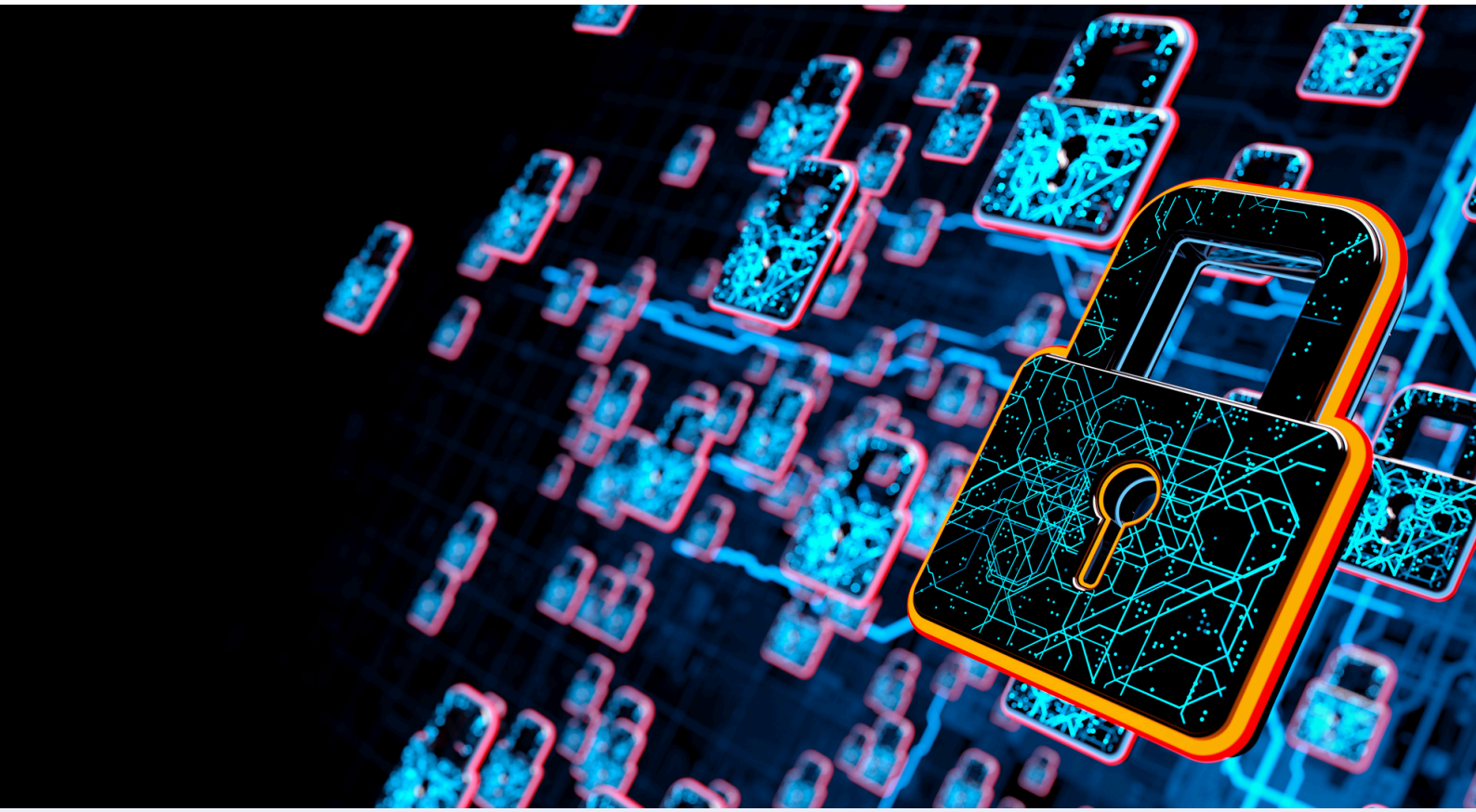


Image 46. Fake app named ‘Pekao security key’

[19] https://x.com/CSIRT_KNF/status/1999100373508710628
[20] https://www.intel471.com/blog/new-fvncbot-android-banking-trojan-targets-poland

03. SECURITY OF FINANCIAL MARKET ENTITIES

3.1 CYBER THREAT INTELLIGENCE (CTI): FROM RESPONDING TO PREDICTING



Evolution of approach to threats

CSIRT KNF acts based on an approach which focuses on predicting new threats, not only responding to the existing ones. We focus on capturing early signals which might indicate campaigns in the preparatory stage and we analyse them for any potential impact on the financial sector in Poland. By doing so, we can issue early warnings about upcoming criminal actions and support institutions in their preparations before real incidents occur.

CSIRT KNF is constantly monitoring various OSINT sources, both those which are publicly available and those which are hard to access. We gather data from websites that release information about data leaks, from domain registration platforms, social media, criminals' forums, and communication channels announcing new campaigns or techniques to be used by cybercriminals. We use those sources to extract data which are relevant for the banking sector in Poland and we regularly share them with institutions in order to support them in risk assessment, detection of early attack signals and implementation of appropriate security measures.

Monitoring of ransomware groups and analysis of data leaks

As part of the CTI, CSIRT KNF is monitoring the activity of ransomware groups globally. We pay special attention to the analysis of information about data leaks published by those groups. We check every case for potential impact on the supply chain in the Polish banking sector.

We analyse:

- published data on ransomware attacks at global level
- victims' potential links with the financial market in Poland
- risk to supply chains of supervised entities
- vulnerabilities and attack vectors used by criminal groups.

In 2025, we also looked at attacks directed at online stores and other websites, as some of those attacks might have affected the users of financial services. In this area, we worked closely with CERT Poland by sharing our information with them and analysing the nature of the incidents. The information we gathered were forwarded and ultimately published at bezpiecznedane.gov.pl. Thus, the information can be used by both institutions and individuals who want to check whether their data may have appeared in the materials disclosed during such attacks.

The monitoring of hactivist groups

2025 was also a year of increased activity of hactivist groups, largely linked to the geopolitical situation in our region. CSIRT KNF engages in ongoing monitoring of such groups by analysing their declared goals, operating methods and potential threats to the financial sector in Poland. We are monitoring communication in forums, on Telegram channels and at other places where such groups publish information about their plans.

It should be noted that the declarations made by hactivist groups often do not reflect the real scale of their actions. Some announcements about the ‘successes’ are actually information about access to publicly available resources, such as open transmissions from urban video surveillance or public streaming services. The groups present such actions as serious hacking operations, but the truth is no actual cyberintrusion or system compromise has taken place. A major part of the CTI is the ability to distinguish a real threat from a propagandist hype.

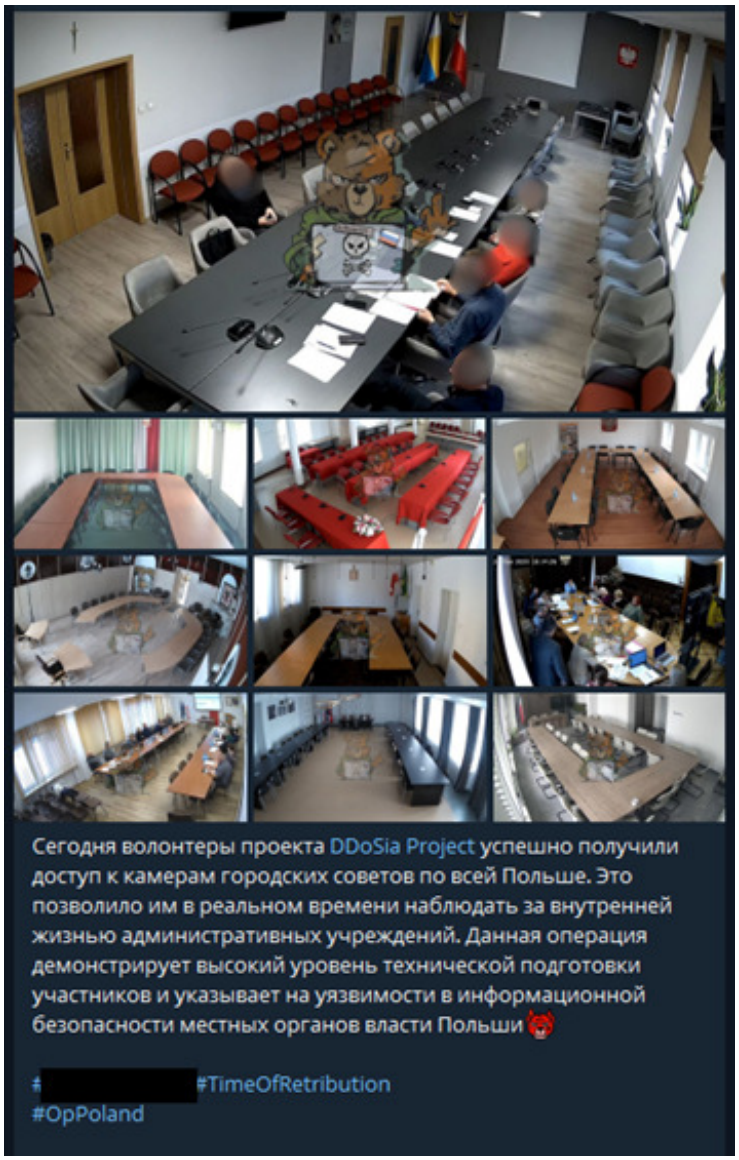


Image 47. Information published by a cybercriminal group on Telegram

In case of detection of a threat targeting the financial market in Poland, we inform entities about a potential attack before the attack is initiated. Such early warnings allow institutions to enhance their security measures and prepare themselves for defence.

In addition to the monitoring and early warning, CSIRT KNF runs a platform which allows financial market entities to exchange Indicators of Compromise (IOCs). This way, institutions can exchange information about detectable threats in real time, which allows the entire sector to respond to new campaigns faster. We also provide a channel for the exchange of experiences among entities to enable the exchange of knowledge about effective defence methods and lessons learned from incidents.

Resilience of the Polish financial sector

Importantly, in 2025 we did not record any successful ransomware attack targeted directly at a Polish entity from the financial sector. It is a remarkable success and a proof of high maturity of cybersecurity in the sector. Polish banks, brokerage houses and other financial institutions effectively protect their infrastructure against such threats.

Threats in the supply chain

Although attacks targeting the financial sector directly are rare, we have seen a rise in incidents concerning supply chains. Criminals tend to carry out more and more attacks targeting providers of technologies, IT services or software used by financial institutions. Such an indirect attack vector may cause serious consequences for the security of final users of financial services.

In 2025, we were monitoring cases of attacks against:

- providers of software used in the financial sector
- firms providing IT services to banks and other financial institutions
- entities responsible for services supporting the functioning of financial institutions.

In each such a case, we analysed the risk to the Polish market and, where necessary, we communicated potential threats to the entities concerned.

Proactive cooperation with the market

With our proactive approach, we can warn financial entities about threats before real attacks take place. Instead of responding to incidents that have already occurred, we focus on predicting the actions of criminals and on supporting institutions in their efforts to prevent issues. Early warning is of utmost importance to the entire sector. Communicating information in advance can allow for quicker adjustments, blocking orders being issued for new domains used in campaigns or simply for increasing vigilance where risk may occur. This is what often stops a threat at its early stages.
When we detect new fraud patterns or attack methods that may affect the financial sector, we inform entities, even if we have not recorded any such incident in Poland yet. We regularly issue recommendations and warnings concerning new threats, before they can even reach Polish institutions.

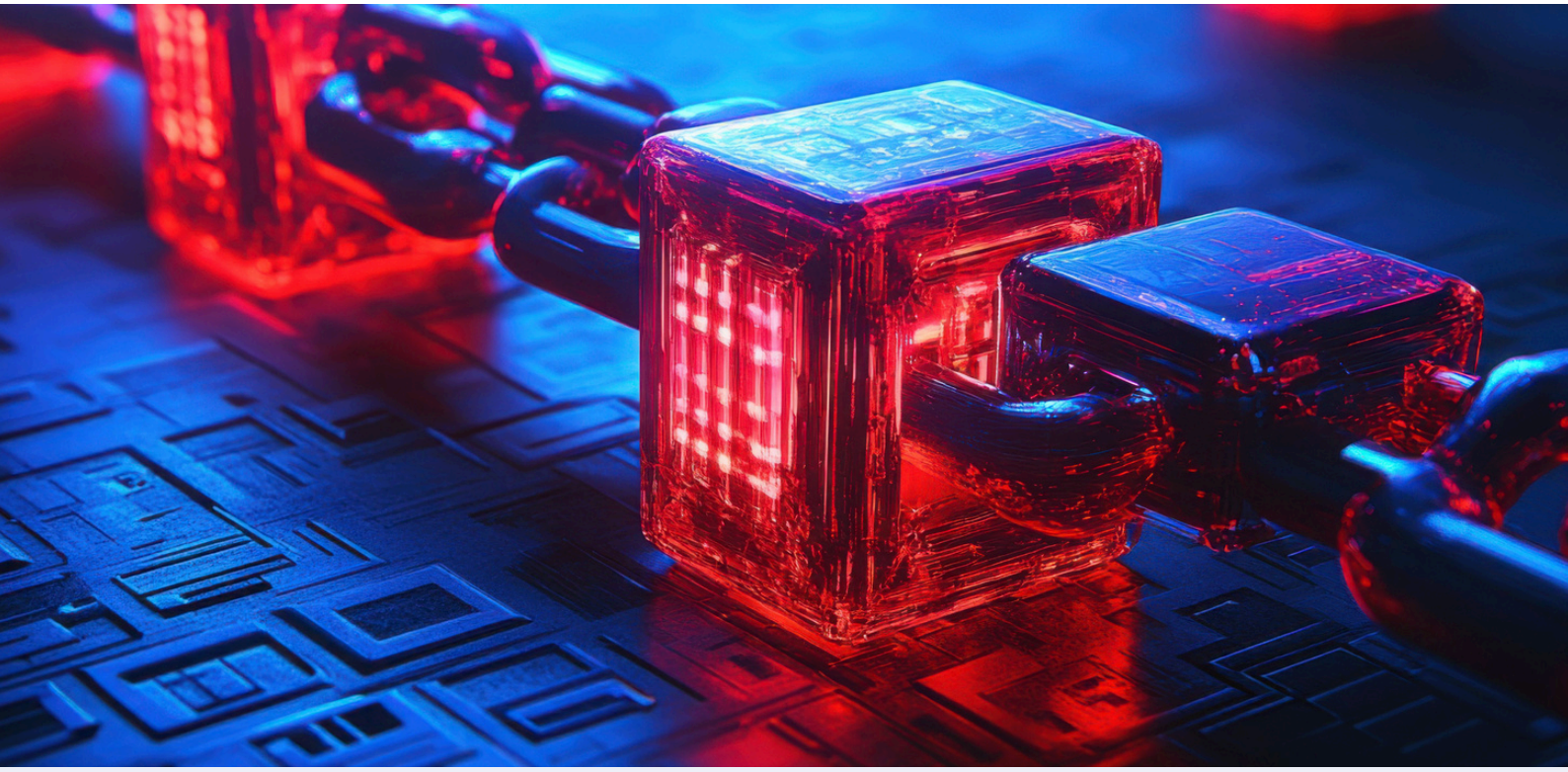
One of the examples of such proactive approach in 2025 was a warning about a campaign of APT groups linked to North Korea, targeting IT and HR departments of financial institutions. Attackers steal the identity of real individuals and use it to apply for technical positions by sending fake CVs. The goal is to get hired or at least gain access to internal systems at the recruitment stage. We did not record any case of a successful attack of this kind against the Polish financial sector, but we warned institutions about the threat and issued recommendations to draw the attention of HR departments to this type of fraud and provided guidance on the verification of candidates' identity.

This is one of many cases where we act in advance: we analyse global trends and incidents, we assess their potential effect on the Polish financial market and we provide institutions with specific information before they have to face a real threat.

Another important aspect here is the exchange of information with other CERTs, both the sector-specific and national ones. This helps us better understand the links between incidents in various parts of the economy and assess more quickly whether a given signal may affect financial institutions. Such cooperation works both ways: we share our observations but also use the expertise of other teams, which altogether increases the resilience of the entire 'ecosystem'.

This approach requires continuous analysis of many sources, tracking criminal activity in underground forums, and quick response to unusual signals. This work is intense but its effects are very concrete: more security in the financial sector.

3.2 DDOS ATTACKS AGAINST THE BANKING SECTOR



Nature of threat

DDoS (Distributed Denial-of-Service) attacks have been one of the most frequent threats to the financial sector all over the world for years. Their purpose is to overload the victim's infrastructure with a large volume of network traffic, which may lead to unavailability of services for clients. For banks, brokerage houses or payment systems, even a short interruption of operationality means not only financial losses but also a loss of clients' trust.

The financial sector is an attractive target for several reasons. Firstly, financial institutions must ensure business continuity: clients expect to have access to their funds and services 24/7. Secondly, attacks against banks attract media attention, which is particularly important to hacktivist groups that seek publicity. Thirdly, with the current geopolitical situation, the Polish financial sector, being part of the infrastructure of a country that supports Ukraine, has become a target for groups linked to Russia.

It is worth remembering that DDoS attacks have become goods widely available as part of Cybercrime-as-a-Service model. Services that allow a DDoS attack to be performed may be found not only in the darknet but also in the clear web, and this lowers the entry barrier for potential attackers. At the same time, the scale of attacks is increasing along with the development of network infrastructure: larger broadbands on the side of end users, development of 5G, and the growing number of IoT equipment mean more sources of potential attacks.

For this reason, resilience to DDoS attacks is not an option but a necessity. Polish financial institutions have been building defence capabilities in this regard for years and CSIRT KNF supports them in preparing for attacks and in coordinating activities when attacks are being waged.

Scale of threats in 2025

In 2025, CSIRT KNF identified 787 DDoS attacks targeted at the Polish financial sector. This is a clear increase in comparison to previous years, which fits into a broader picture of threats observed in the entire region of Central and Eastern Europe.

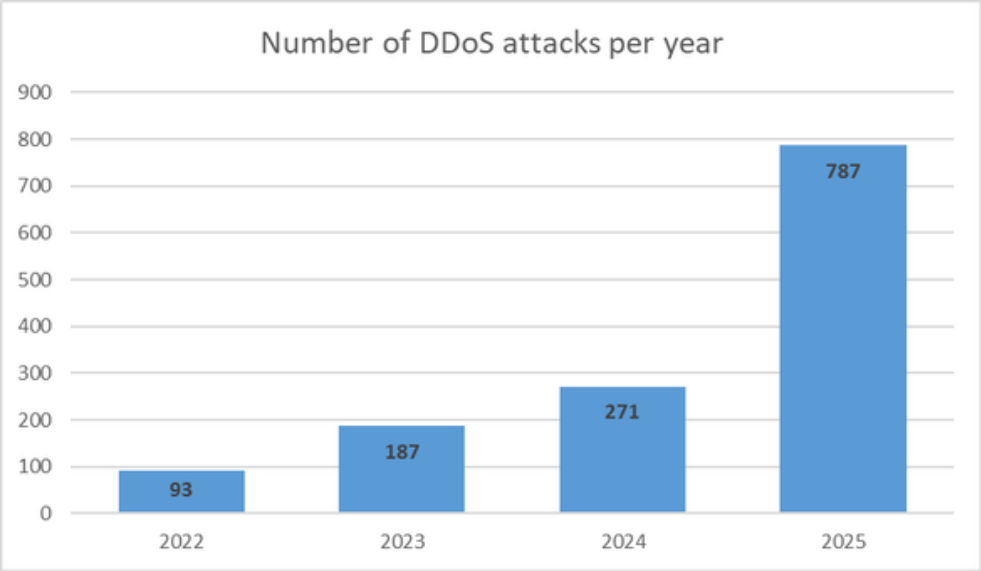


Chart 5. Number of DDoS attacks per year

The largest attack reported, which happened in May, reached a volume of 1.3 Tbps at its peak. This was one of the most powerful attacks ever experienced by Polish financial institutions. In total, we identified 19 attacks with volumes exceeding 500 Gbps and 48 attacks falling in the 100–500 Gbps range; those were attacks requiring advanced defence mechanisms and well-prepared infrastructure.

The vast majority of attacks (78%) were volumetric attacks, namely those consisting in overloading the bandwidth with enormous traffic. Application attacks, targeted at specific services and applications, accounted for 12% of cases, while 10% were mixed attacks combining the two techniques.

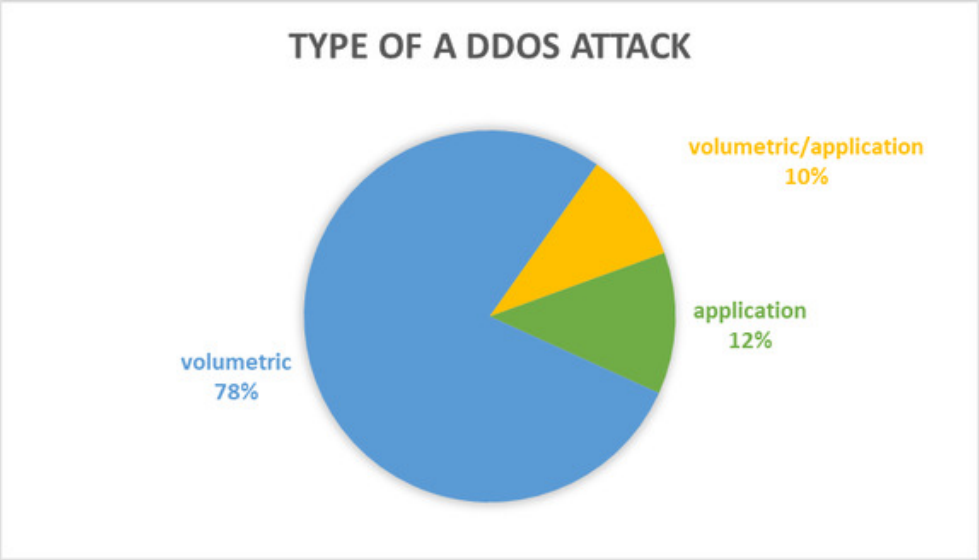


Chart 6. Type of a DDOS attack

The intensity of attacks was uneven throughout the year. May proved to be the most intensive month, with 172 registered attacks, including the already mentioned record attack with the volume of 1.3 Tbps. September, November, and December also saw increased activity of attackers.

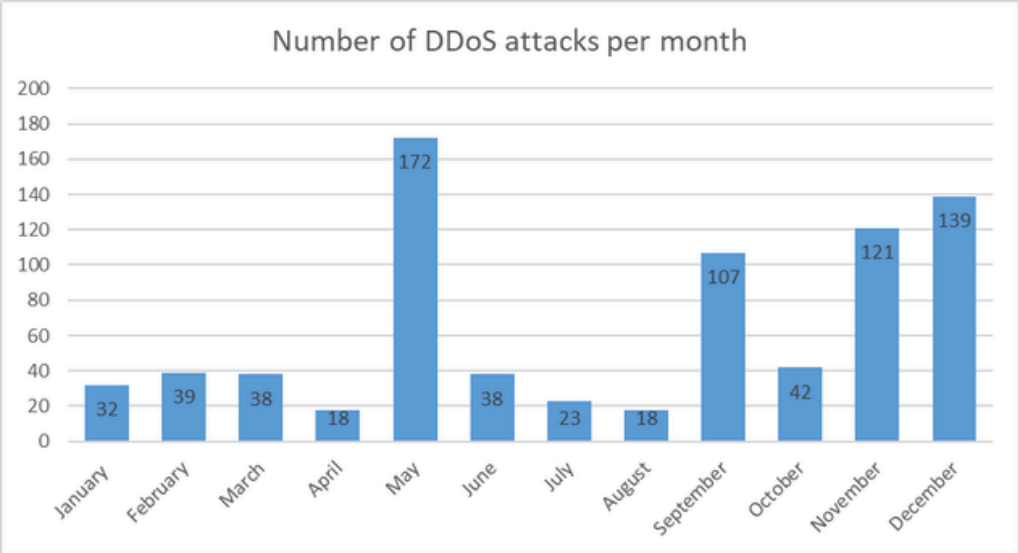


Chart 7. Number of DDoS attacks per month

Resilience of the sector

Despite the significant number of attacks and record volumes, the vast majority of attacks did not affect the continuity of financial services. Clients of banks and other financial institutions in the majority of cases have not experienced any impact of those attacks on the availability of services that they use on a daily basis.

This resilience did not come from nowhere. This is a result of consistent work of the entire sector: investing in security, building competence of teams, and developing cooperation among institutions. The Polish financial sector treats cybersecurity not only as a cost or regulatory requirement but as a priority and shared responsibility.

An important element of the resilience is willingness to share knowledge and experience. Financial institutions compete with each other on a daily basis, but when it comes to security, they can act together. Information about attacks, effective defence methods and observed threats are being exchanged among entities, which allows the entire sector to learn from the experiences of single institutions.

Organisational preparedness is of no lesser importance. Technical solutions themselves will not be enough if they are not accompanied by tested protocols, clearly specified division of roles, and seamless communication in a crisis. Financial institutions regularly test their readiness and improve their incident response processes.

CSIRT KNF supports such activities by acting as a coordinator for exchange of information and a point of contact for the entire sector. Together, we build an ‘ecosystem’ in which a threat for one institution becomes a lesson for all the others.

Monitoring and exchange of information

CSIRT KNF actively monitors threats related to DDoS attacks and engages in ongoing exchange of information with financial market entities. As part of this cooperation, we exchange IP addresses used to launch attacks and we share effective mitigation methods. This allows institutions to respond to new campaigns faster, set network traffic filtering rules, and draw conclusions from the experience of other entities that faced similar threats in the past.

We also look for early signals of planned attacks – by monitoring the activity of hactivist groups and their declarations revealing targets in the financial sector. The groups often announce their intentions in communication channels in advance, which gives us a chance to warn potential targets and support them in preparing their defence.

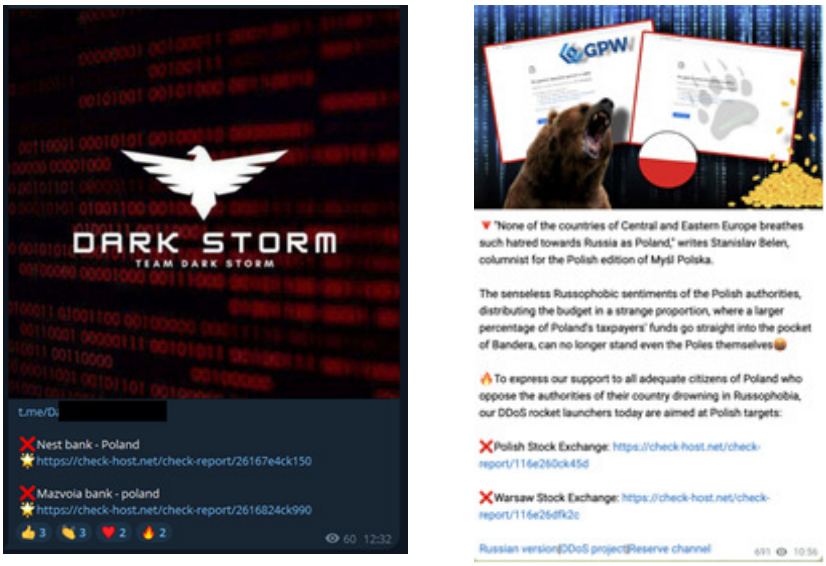


Image 48. Information on planned attacks published by a hacktivist group

It is worth remembering that DDoS attacks are sometimes used as a smoke screen for other criminal activities. While security teams are being focused on countering volumetric attacks, attackers may attempt to achieve other goals. For this reason, during any DDoS attack, the monitoring of security should be maintained at a level not lower than the level applicable to regular traffic, and institutions should stay vigilant for other potential threats.

Summary

Year 2025 witnessed a high number of DDoS attacks against the Polish financial sector: 787 registered incidents, including the attack with the record volume of 1.3 Tbps. Despite this scale of threats, the sector showed high resilience. This is an outcome of years of investments in the infrastructure, relations built with telecommunications operators and security service providers, as well as regular improvements of response protocols.

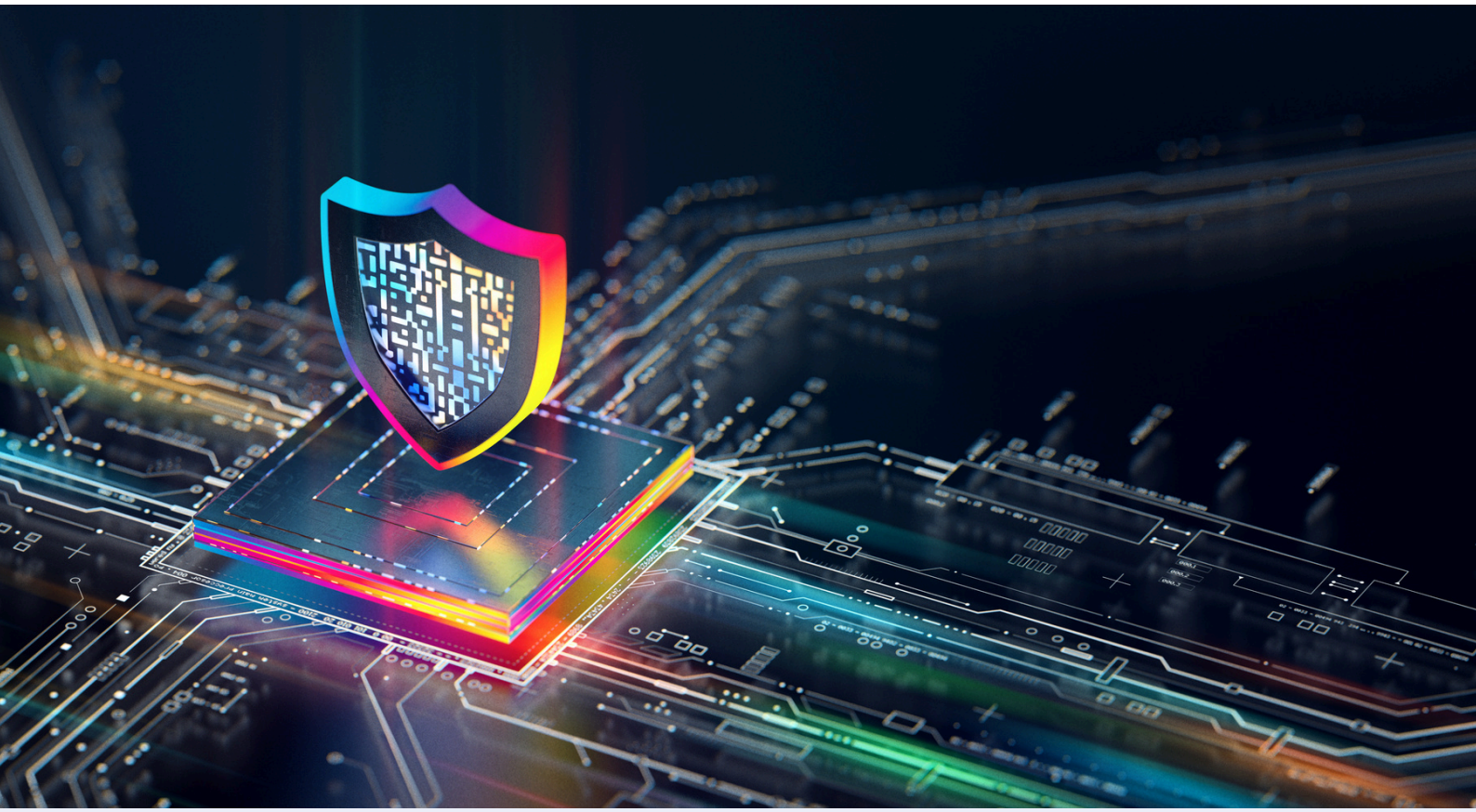
It is worth mentioning that in 2022 CSIRT KNF published a document titled Good practices in DDoS countermeasures[21], which remains valid and serves as a reference point for financial institutions. The figures of 2025 confirm that the recommendations included in that document were incorporated into the sector's practice: even attacks with a volume exceeding 1 Tbps are not able to distort the operations of Polish financial institutions.

Image 49.Good practices in DDoS countermeasures, a document published by CSIRT KNF.

CSIRT KNF will continue its activities for monitoring DDoS threats, exchanging information with the market and providing early warnings on planned attacks. Together with financial institutions we work to make sure that DDoS attacks are just a nuisance for the sector, not a real threat to business continuity.

[21] https://cebrf.knf.gov.pl/images/Raporty/Dobre_praktyki_w_zakresie_przeciwdziaania_atakom_DDoS_77247.pdf

3.3 CURRENT TRENDS IN CYBER THREATS



2025 witnessed further changes in terms of cyber threats identified, understood both globally and in the context of financial sector entities.

The changes are clearly reflected by the updated proposal for the list of ten most often identified threats, published periodically as part of the OWASP Top 10. The draft update of the list of 2021 was published on 6 November 2025.

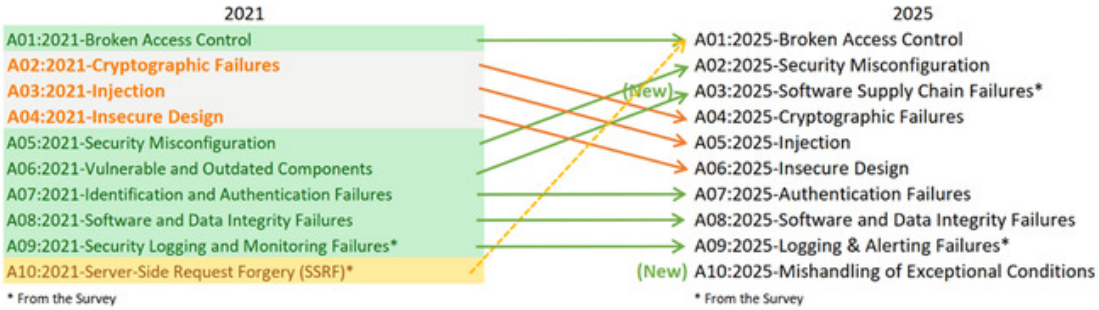


Image 50. The most common identified threats – OWASP Top 10 [22]

The second and third positions on the list changed considerably, with the following categories of vulnerabilities being ranked in these positions:

- A02: Security Misconfiguration – a vulnerability which went up from the 5th position (Top10 2021) to the 2nd position. According to OWASP, the number of configuration errors is growing steadily – 3% of applications analysed displayed at least one of 16 weaknesses under CWE (Common Weakness Enumeration) weaknesses belonging to this category. The underlying cause is a growing dependence of applications on correct configuration.
- A03: Software Supply Chain Failures – a category which is an extended version of former A06:2021 (Vulnerable and Outdated Components), covering the entire 'ecosystem' of dependences, building systems and distribution infrastructure. According to specialists in IT security incident response, the category has been indicated in the surveys as one of the most critical issues. The data show rare detectability of this type of threats, mainly due to difficulties in testing them. At the same time, the vulnerability in question achieves the highest average rates in exploitability and impact categories within the CVE.

[22] https://owasp.org/Top10/2025/0x00_2025-Introduction/

Vulnerabilities identified by CSIRT KNF in the years 2023–2025 also confirm the tendency for threats to increase, as described by OWASP.

As for the exploitation and identification of new CVEs (Common Vulnerabilities and Exposures), year 2025 since its beginning witnessed signs of intensification of this trend. The publicly available VulnCheck report on the number of new CVEs identified in the first half of 2025 shows that 432 new vulnerabilities have been registered by the end of June. 32% of them were actively exploited in attacks even before being officially registered in the CVE database [23].

The chart published by VulnCheck is also worth noting as it illustrates the mean time between the publication of information about a new security gap and the identification of examples of actively exploiting it in attacks, which in 2025 was less than one day.

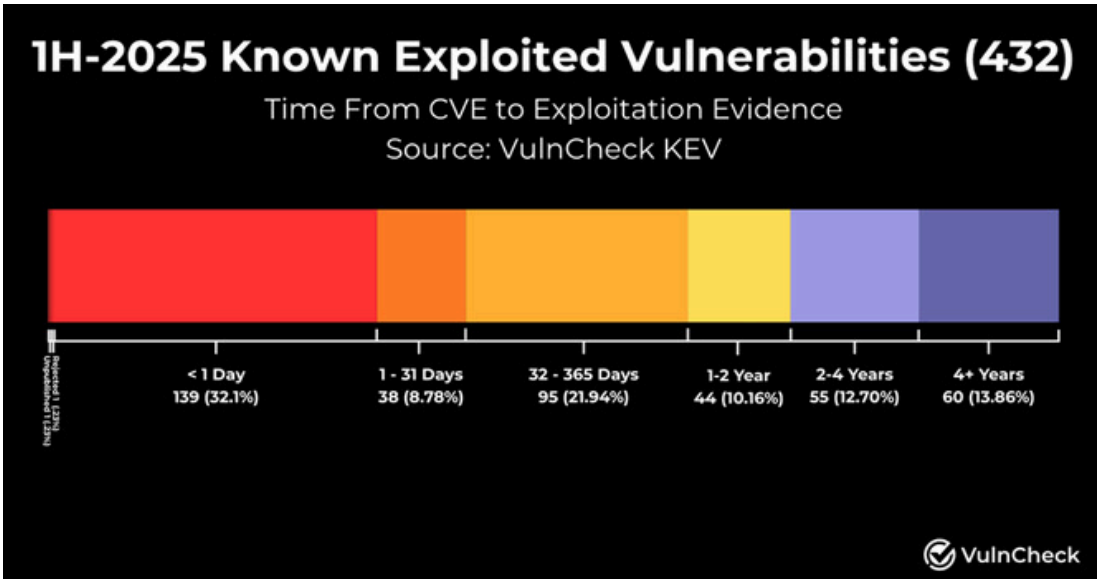


Image 51. Information on the number of new CVEs disclosed in the first half of 2025

The figure defines a time frame in which teams responsible for maintenance of systems and applications may respond to the disclosure of a new known vulnerability and launch a remediation process to be able to effectively mitigate, in all likelihood, a threat related to the possibility of that vulnerability being potentially used in an attack.

[23] https://www.vulncheck.com/blog/state-of-exploitation-1h-2025

A threat caused by Supply Chain attacks is, to a large extent, a result of limited possibility of monitoring cybersecurity at external providers of tools and services. Moreover, in the vast majority of cases, organisations do not have information about the components provided by broadly defined third-party technology providers.

The results of the BitSight survey were published in an article at helpnetsecurity.com entitled Hidden risks in the financial sector's supply chain[24] in November 2025, in which researchers analysed more than 41 000 financial organisations and their relations with over 50 000 technology providers by identifying links between uneven monitoring and gaps in risk management in the financial sector's digital supply chain. The findings confirm a gap in the possibilities of actively monitoring Supply Chain threats. The research identified the total of 99 major technology providers for the financial sector, including both well-known large companies, such as Microsoft or Google, but also those less visible in the IT market, such as General Dynamics and NICE Group, which also play key roles in the supply chain, even though they are less often the centre of attention prior to identification of security gaps in their products or infrastructure safeguards. In comparison to financial organisations, external providers showed worse results in 16 out of 22 risk categories distinguished in the research. The area related to managing vulnerabilities and the so-called OPSEC (Operations Security) exposure was particularly neglected. The research also debunked the myth that larger providers are in possession of stronger cyber safeguards. Providers with larger market share achieve worse security results, which suggests that larger infrastructure and number of customers may expand the attack surface. Non-monitored service providers in the financial sector had 2.9 times more critical CVE vulnerabilities in their own infrastructure than monitored providers had.

[24] https://www.helpnetsecurity.com/2025/11/11/hidden-financial-sector-cyber-risk/

Moreover, 2.8 times more of such vulnerabilities were exploited in attacks in comparison to providers that were subject to monitoring. The findings suggest that active monitoring not only increases the visibility of threats but also motivates providers to improve safeguards in their own environment and for services provided, ultimately with a positive effect on the security of the entire financial sector.

The increase in the level of risk related to threats in the form of a supply chain attack is widely noticeable and this sort of attacks increasingly often have serious consequences, as also pointed out by Gartner analytics and research company.

The number of breaches related to supply chains in 2025 increased by 68% and those breaches currently account for 15% of all attacks resulting in data breaches. In 2024, 35.5% of data breaches were related to third parties, which shows an increase by 29% in comparison to 2023[25]. Gartner predicts that 45% of organisations will experience supply chain breaches by the end of 2025, which means a triple increase since 2021[26].

It should be noted that one of major incidents of supply chain attack in recent years have been attacks on NPM packages, a very popular and widely used package manager for the Node.js (JavaScript) environment. An example of a successful supply chain attack is an attack to which Jaguar Land Rover (JLR) fell a victim. The perpetrators managed to compromise the account of one of JLR's providers and, thus, they accessed the project management system. The consequences of that incident went far beyond the brand itself. The financial loss related to the attack was estimated at 1.9 billion Sterling pounds in the United Kingdom alone[27].

[25] https://deepstrike.io/blog/data-breach-statistics-2025
[26] https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends
[27] https://cybermonitoringcentre.com/2025/10/22/cyber-monitoring-centre-statement-on-the-jaguar-land-rovercyber-incident-october-2025/

Activities of CSIRT KNF to support the financial sector in terms of warning against cyber threats

In 2025, CSIRT KNF continued its intense activity in the area of identifying vulnerabilities and supporting financial market entities. During the year it published 625 warnings and 19 sectoral recommendations, dozens of targeted security screenings were conducted, and in 51 cases threats identified resulted in addressing individual recommendations to specific financial sector entities.

Statistics:

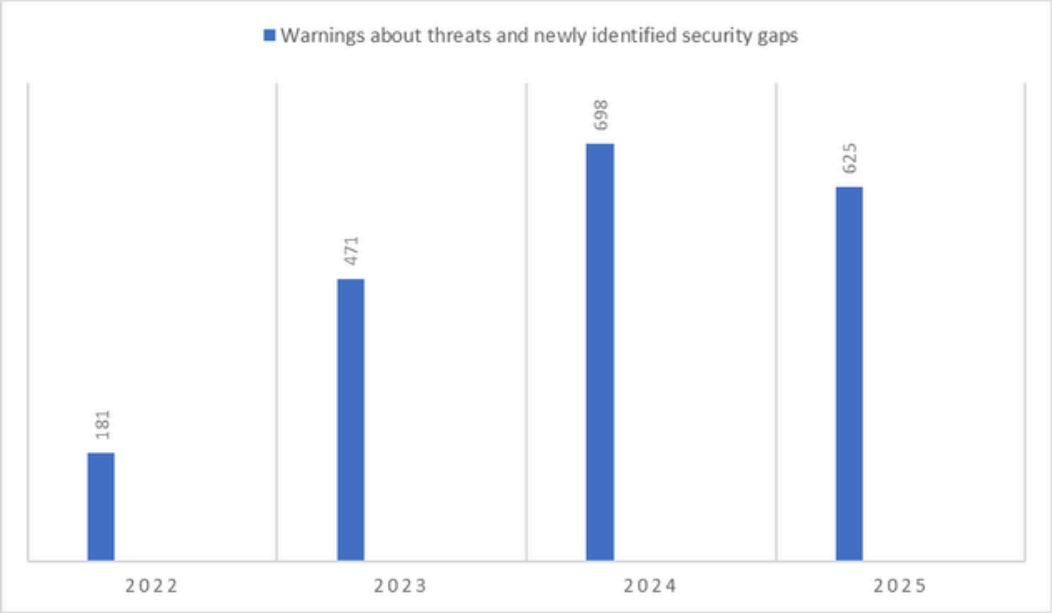


Chart 8. Activities of CSIRT KNF in the area of identifying vulnerabilities and supporting financial market entities

Warnings about threats and newly identified security gaps disclosed by manufacturers and security experts are a key instrument to immediately inform users of the financial sector about cybercrime campaigns, identified vulnerabilities and identified methods of waging attacks.

In 2025, more than ever, sectoral recommendations were focused on vulnerabilities and campaigns with a potential to affect all entities or a significant part of the financial market. The aim was to enable a single security recommendation to be used by a number of financial market institutions.

At the same time, in line with the practice of recent years, CSIRT KNF continued activities of scanning the security of publicly available infrastructure of financial entities that form associations. The screenings remained precisely targeted and dedicated to individual entities, taking into account their specific systems, applications and services exposed online. Detected threats were communicated each time in the form of a tailored set of recommendations addressed to the specific entity that uses a given product, infrastructure or tool.

As a result, in 2025, CSIRT KNF integrated two complementary levels of impact: a broad, horizontal reach – through recommendations addressed to the entire financial sector, and an entity-specific dimension – by initiating activities aimed at identifying and analysing vulnerabilities and threats in the publicly available layer of IT infrastructure of specific market participants.

Statistics:

Chart 9 . Activities of CSIRT KNF in the area of identifying vulnerabilities and supporting financial market entities

This model strengthens the sector's maturity in the area of vulnerability management and translates into the actual increase in the level of security of financial market entities.

The most material vulnerabilities in IT systems, which vulnerabilities were actively exploited in the campaigns disclosed in 2025 were security gaps identified in the following products:

1. React/Next.js – a critical vulnerability, described in CVE-2025-55182, later named React2Shell, published at the end of 2025. The gap that enabled an attacker to execute a code remotely, carrying out an RCE attack, was followed by a wave of active exploitation. The screening for vulnerable systems began shortly after information on the gap was published. The first wave of attempts of actively using it was observed on 3 to 5 December.

React2Shell vulnerability uses the non-standard logic of React Flight Protocol (RFP) used by React Server Components. The gap allows attackers to overwrite the properties of variables on the server side and take over the control of a JavaScript object by manipulating RFP chunks. In contrast to standard vulnerabilities, RFP uses non-standard protocol based on chunks, which gives attackers significant opportunities in terms of evading detection and carrying out post-exploitation activities.

Vulnerable components:

- Next.js (main attack vector – majority of public PoC)
- React Router (experimental RSC functionality, not enabled by default)
- Expo (a framework with experimental support for RSC)
- React RSC (calling a function directly)
- Waku (a framework using randomly generated endpoints)

The following exploit variants were identified during the campaign:

- Initial execution-based exploits – the most basic, direct calling of 'NodeJS' process and 'require' modules
- Droppers – saving the secondary payload onto a drive
- In-memory exploits – activities carried out in memory entirely, without any records on a drive
- Unicode escaping – fingerprint masking by escaping Unicode (\uXXXX)
- In-memory web shells – modification of HTTP NodeJS server prototype that enables creation of a fully in-memory web shell, active on paths controlled by an attacker

Apart from threat actors' activities strictly related to activities aimed at identifying potential attack targets in the public web and further exploiting React2Shell vulnerabilities, one could also observe successful attempts of using publicity around the vulnerability to distribute malware that impersonates React2Shell vulnerability scanners or is implemented in them, appearing in a PoC form in various sources.

2. MongoDB – a vulnerability within the MongoDB Server which enables remote, unauthenticated attackers to read uninitialised heap memory as a result of incorrect processing of data length in Zlib compressed protocol headers. Vulnerable products and versions:

- MongoDB 8.2.0 – 8.2.3
- MongoDB 8.0.0 – 8.0.16
- MongoDB 7.0.0 – 7.0.26
- MongoDB 6.0.0 – 6.0.26
- MongoDB 5.0.0 – 5.0.31
- MongoDB 4.4.0 – 4.4.29
- All versions of MongoDB Server 4.2, 4.0 and 3.6

The vulnerability was described in CVE-2025-14847 with CVSSv3.1: 8.7 - improper handling of length parameter inconsistency in the implementation of zlib compression, enabling the read of uninitialised heap memory by an unauthenticated client.

The effective use of the gap may result in disclosing sensitive data stored in the server process memory, such as internal status information or memory indicators. The gap was addressed by a patch in the following versions of MongoDB Server: 8.2.3, 8.0.17, 7.0.28, 6.0.27, 5.0.32, 4.4.30. The vulnerability was widely searched for and actively used, which was caused mainly by the ease with which it could be exploited, and by quick publication of the vulnerability's PoC.

3. Citrix – products of NetScaler ADC and NetScaler Gateway, in which vulnerabilities were identified as described in CVE-2025-7775 CVSS v4.0 9.2 – Memory overflow vulnerability leading to Remote Code Execution and/or Denial of Service, CVE-2025-7776 CVSS v4.0 8.8 – Memory overflow vulnerability leading to unpredictable or erroneous behaviour and Denial of Service, CVE-2025-8424 CVSS v4.0: 8.7 – Improper access control on the NetScaler Management Interface. Among the above, it was the CVE-2025-7775 gap that was actively used in attacks even before it was identified by the manufacturer as a 0-Day gap. The campaigns of threat actors were targeted at infrastructure with the vulnerable configuration.

- Gateway: VPN virtual server, ICA Proxy, CVPN, RDP Proxy or AAA virtual server
- LB virtual servers (HTTP, SSL, HTTP_QUIC) in versions 13.1, 14.1, 13.1-FIPS, NDcPP related to: IPv6 services, IPv6 DBS services, CR virtual server of HDX type

4. Citrix – NetScaler ADC/Gateway product, in which CVE-2025-12101 CVSS 5.9 vulnerability, Cross-Site Scripting (XSS) type, was identified. The vulnerability occurs exclusively in appliances configured as Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA virtual server. The mechanism of XSS attack makes it possible to inject a malware script into the context of user session.

5. Fortinet – a gap in FortiWeb safeguards, which was described in CVE-2025-52970 CVSS 7.7, may enable an unauthenticated remote attacker who has non-public information pertaining to the device and targeted user account to log in as any existing user on a vulnerable-version device via a specially crafted request. The vulnerability was addressed by patches in FortiWeb versions 7.6.4, 7.4.8, 7.2.11 and 7.0.11.

6. Fortinet – a vulnerability described in CVE-2025-64446 CVSSv3: 9.1, 0-day path traversal type, which allows an unauthenticated attacker to execute administrative commands on the system via crafted http requests. This was addressed by a patch in versions 8.0.2, 7.6.5, 7.4.10, 7.2.12, 7.0.12.

7. Fortinet – a vulnerability disclosed in the FortiWeb product, described in CVE-2025-58034 with CVSSv3 6.7, allows an authenticated attacker to execute a command in the system via crafted HTTP requests or a CLI command. This may result in a complete takeover of the system and impact the integrity, confidentiality or availability of data processed by the system. The gap was eliminated by security patches in versions 8.0.2, 7.6.6, 7.4.11, 7.2.12, 7.0.12.

8. Spring – vulnerabilities described in CVE-2025-41248 CVSSv3.1 7.5 – authorisation bypass, concerning the use of @PreAuthorize annotation and other method security annotations, which may result in bypassing authorisation, as well as CVE-2025-41249 CVSSv3.1: 7.5, being a gap related to applications that use Spring Security's @EnableMethodSecurity in combination with security annotations in generic superclasses or interfaces. The gaps were identified in the following versions of Spring Security and Spring Framework applications:

- Spring Security in versions lower than: 6.4.10, 6.5.4
- Spring Framework: 6.2.0 – 6.2.10, 6.1.0 – 6.1.22, 5.3.0 – 5.3.44 lower than 6.2.11, 6.1.23, 5.3.45. 6.0.x versions are not supported by the manufacturer and patches will not be published.

9. Cisco – vulnerabilities disclosed in Cisco Adaptive Security Appliance (ASA), described in CVE-2025-20333 CVSS 9.9 – VPN Web Server Remote Code Execution, where a Buffer Overflow gap in VPN allows an attacker to execute a code remotely. It is combined to create a chain with the vulnerability described in CVE-2025-20362 CVSS 6.5 – VPN Web Server Unauthorised Access, which allows for unauthorised access to VPN web server, resulting in a so-called exploitation chain. This enables a complete takeover of a vulnerable system. Yet another gap identified in Cisco ASA was CVE-2025-20363 CVSS 9.0 – an error in HTTP processing, enabling the execution of any code. The gaps described in CVE-2025-20333 and CVE-2025-20362 were actively used in attacks. The patches were published in versions 7.0.8.1, 7.2.10.2, 7.4.2.4, 7.6.2.1, and 7.7.10.1.

10. IBM – a vulnerability disclosed in SIEM QRadar system, described in CVE-2025-36007 CVSS 7.8, resulting from improper assignment of privileges to an update script in IBM QRadar SIEM. An attacker with a limited local access to the system could use an erroneous configuration of script privileges to execute operations with advanced privileges of account administrator. The exploitation mechanism is based on the manipulation of software update process. The gap was addressed by the security patch in IBM QRadar SIEM 7.5.0 UP14.

11. MikroTik – a vulnerability identified in WebFig component of MikroTik RouterOS in version 7.14.2 and SwOS in version 2.18. It was described in CVE-2025-61481 CVSS: 10.0 – it enables an attacker without credentials to execute any code on a vulnerable device, thanks to a crafted http package.

12. Oracle – a gap in identity and access manager in Oracle Identity Manager, described in CVE-2025-61757 CVSSv3 9.8 – an error in the REST WebServices component, which enables an unauthenticated attacker to take over Identity Manager, using a crafted HTTP request. The vulnerability relates to IM versions 12.2.1.4.0 and 14.1.2.1.0.

13. Oracle – vulnerabilities identified in the Marketing Administration component of Oracle E-Business Suite and in Oracle Financial Services Applications, described in CVE-2025-61884 CVSS 7.5 – for Oracle E-Business Suite, a Server-Side Request Forgery type gap, which enables a remote attacker to send http requests from the target's server to internal or external resources, which may result in disclosing data or executing a code remotely. CVE-2025-53037 CVSS: 9.8 – Oracle Financial Services Analytical Applications Infrastructure in versions 8.0.7.9, 8.0.8.7 and 8.1.2.5; this vulnerability enables an attacker to have full access to the system by executing a code remotely through a http request. CVE-2025-53072 CVSS 9.8 – Oracle FLEXCUBE / E-Business Suite Marketing, a gap in the Marketing Administration module of Oracle E-Business Suite in versions 12.2.3 – 12.2.14, which enables an unauthenticated attacker to execute a code remotely through crafted http requests. CVE-2025-62481 CVSS 9.8 – Oracle FLEXCUBE / E-Business Suite Marketing; a gap in the Marketing Administration module enables an unauthenticated attacker to execute a code remotely by sending crafted http requests. The vulnerability enables an attacker to access and modify clients' data and to upload and propagate a malicious code. CVE-2025-53036 CVSS 8.6 – Oracle Financial Service Analytical Applications Infrastructure, a high-risk gap which enables an attacker to get unauthorised access to application data and escalating privileges in the financial application.

14. Fortra – a vulnerability leading to the injection of an object and the execution of any code, disclosed in GoAnywhere Managed File Transfer (MFT) product in its versions lower than 7.8.4 and Sustain Release 7.6.3, described in CVE-2025-10035 with CVSS 10.0 – Deserialization vulnerability in License Servlet.

15. Omnissa – a gap disclosed in Omnissa Workspace ONE UEM in (On-Premises) versions, described in CVE-2025-25231 with CVSSv3.1: 7.5 – Secondary Context Path Traversal Vulnerability, enabling an attacker to gain unauthorised access to confidential data (read-only) using the Path Traversal technique. The security patch was released in versions 24.10.0.11, 24.6.0.35, 24.2.0.30, 23.10.0.50.

3.4 DORA AS FOUNDATION FOR THE CYBER RESILIENCE OF THE FINANCIAL MARKET

2025 was the first year in which Regulation of the European Parliament and of the Council (EU) 2022/2554 on digital operational resilience for the financial sector was effective. The new regulations established uniform requirements on the management of ICT risk and security incident reporting by financial market entities across the European Union, while their implementation has had significant results in improving operational security standards.

Prior to the entry into force of the regulations, 2024 witnessed a series of organisational and technical activities, including the key action of launching the SOID system, available at https://csirt.knf.gov.pl. The platform is currently a central solution for reporting ICT incidents. It allowed the standardisation of reporting and improved completeness and quality of data reported, which translated into a more efficient analysis of incidents and more effective coordination of reports on CSIRT KNF side.

One of the most visible effects of DORA's entry into force was the significant extension of the scope of entities subject to the reporting obligation. In comparison to the previous obligation based on the Act on National Cybersecurity System, the number of obliged institutions has increased substantially. This resulted directly in a larger number of reports addressed to CSIRT KNF in 2025. The change in scale and diversification of entities required the adaptation of incident handling processes and the expansion of operational capabilities.

In 2025, after DORA officially entered into force on 17 January, entities subject to new reporting obligations submitted to CSIRT KNF a total of 274 reports on serious ICT incidents. The structure of those incidents reflected the nature of operational challenges faced by the sector: the dominating category were failures, accounting for approximately 96% of all reports. 41% of them concerned failures within the institution's own environment (113 reports), while 55% were failures at ICT third-party service providers (151 reports). The remaining 4% of reports (10 incidents) covered other categories of events.

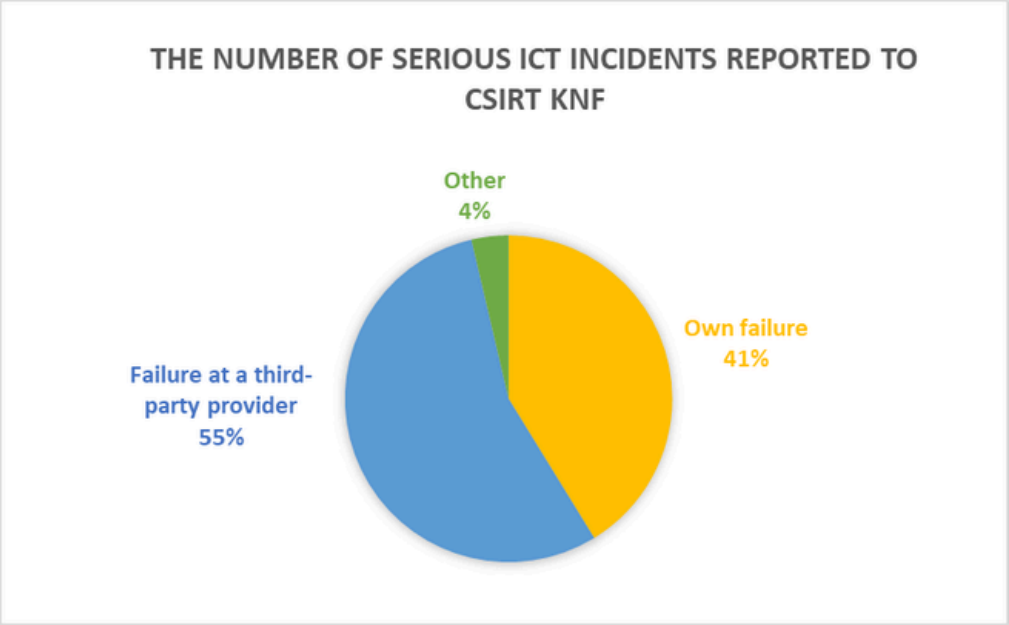


Chart 10. The number of serious ICT incidents reported to CSIRT KNF by category

The high share of incidents related to failures confirms how important for the stable functioning of the financial market is the resilience of technological infrastructure and of the supply chain of ICT services, including proper supervision of critical services provided by third parties. At the same time, first months of DORA application showed a growing awareness among institutions in terms of necessity to report immediately and comprehensively, which translated into better data quality and a more reliable picture of the sector's operational situation.

A novelty introduced by DORA is an obligation to send information about significant cyber threats, understood as data about potential cybercrime activities that may affect the functioning of the financial sector. The mechanism streamlined the flow of information among market institutions, allowed new trends and adversaries' tactics to be identified faster, and improved the ability to take preventive actions. The exchange of information, both at the national level and the European level, has been significantly enhanced.

DORA also introduced uniform standards of classifying and reporting ICT incidents. The uniform model of reporting improved data consistency and their analytical usability, supporting the process of identifying patterns of threats and responding to incidents faster. The standardisation of information has allowed more precise situational reconnaissance at the sector level and better threat profiling.

The first year in which the regulations were effective was also marked by the intensification of international cooperation. The obligation to exchange information about incidents and trends resulted in intensified cooperation between competent authorities of EU Member States, which enabled more coordinated preventive actions and faster flow of information about threats. CSIRT KNF participated in those processes actively by supporting the creation of a more integrated and resilient cybersecurity environment at the European level.

One of the key challenges in the first year of application of DORA was the varying level of organisational maturity among financial market entities. In order to support institutions in adapting to new requirements, CSIRT KNF carried out educational activities, including, among others, CEDUR webinars, as well as publication of information materials. The support contributed to improving the quality of incident reports and the quality of the incident handling process.

In 2025, the Team provided the following CEDUR webinars addressed to the financial market entities supervised by Komisja Nadzoru Finansowego which apply DORA:

- DORA – first reporting obligations and presentation of reporting systems (creating accounts, submitting reports based on the example of selected reporting forms) – 3 deadlines;
- DORA reporting – performing reporting obligations, discussing the most common errors – 4 deadlines;
- Requirements of DORA, preceded by the implementation of Recommendation D and IT guidelines issued by the KNF – 4 deadlines;

- DORA – practical examples of filling out the register of information (SPR-PF-18 form) – 2 deadlines;
- DORA – practical examples of submitting KRI questionnaires (SPR-PF-26 and SPR-PF-27 forms) – 2 deadlines;
- Managing incidents and cyber threats in line with DORA – 3 deadlines
- TLPT – comprehensive approach to security tests – 3 deadlines;
- Implementation of DORA from the perspective of the financial supervision authority – 2 deadlines;
- DORA – practical examples of submitting a report on ICT risk and ICT risk management framework (SPR-PF-01 form);
- DORA – submission of a report, examples with form SPR-PF-00, as well as answers to questions about form SPR-PF-01.

Image. 52 Information published by the UKNF in social media concerning the registration for CEDUR webinars focused on DORA

Thanks to preparation in 2024, in particular the implementation of the SOID system and improvement of incident handling processes, in 2025 CSIRT KNF was able to receive and coordinate reports in an efficient manner, despite a visible growth in their number. The increase in the quality and consistency of reported data was supported by the risk analysis process and preventive actions at the level of the whole financial sector.

3.5 MOJE CERT.PL – A SECTORAL MODULE OF CSIRT KNF FOR THE FINANCIAL MARKET

In 2025, one of key directions in strengthening cyber resilience of the financial sector was the development of consistent mechanisms for sharing information about threats and incidents. In this context, the expansion of the moje.cert.pl platform and launching it within a CSIRT KNF's sectoral module for the financial market was of paramount importance. The development of this solution is financed under the National Recovery and Resilience Plan (KPO).

The significance of the moje.cert.pl platform results from a simple fact: in an environment of quick, automated and multi-channel attacks, the defensive advantage is created not only by the quality of safeguards in a single institution but, first and foremost, by the response time and flow of information across the entire sector. Even the best prepared entity may be weakened if it receives a warning about a new campaign, vulnerability or fraud scheme too late. The sectoral module is to shorten this distance by providing possibly early, structured and practical information, which may be quickly translated into technical and operational actions.

The expanded platform will support security processes at several levels. Firstly, it will enable safe and standardised reporting of incidents and quicker communication of warnings about active campaigns targeted at the sector. Secondly, it is supposed to improve the effectiveness of analysis thanks to better correlation of data and organising information within a single model of reporting. Thirdly, it will improve the coordination of interinstitutional activities, which is particularly important in the case of incidents of distributed nature, mass campaigns, and where operational risk is higher.

In practice, this means better preparedness of the sector for the most common categories of threats: multi-channel phishing, investment scams, malware that targets clients' end devices, as well as incidents resulting from technological and business dependencies. The common, sectoral 'nexus' for the exchange of information allows the risk of domino effect to be reduced and the resilience of the whole 'ecosystem' to be reinforced, in particular in situations where attackers test the vulnerabilities of many institutions at the same time, hoping to find the weakest link.

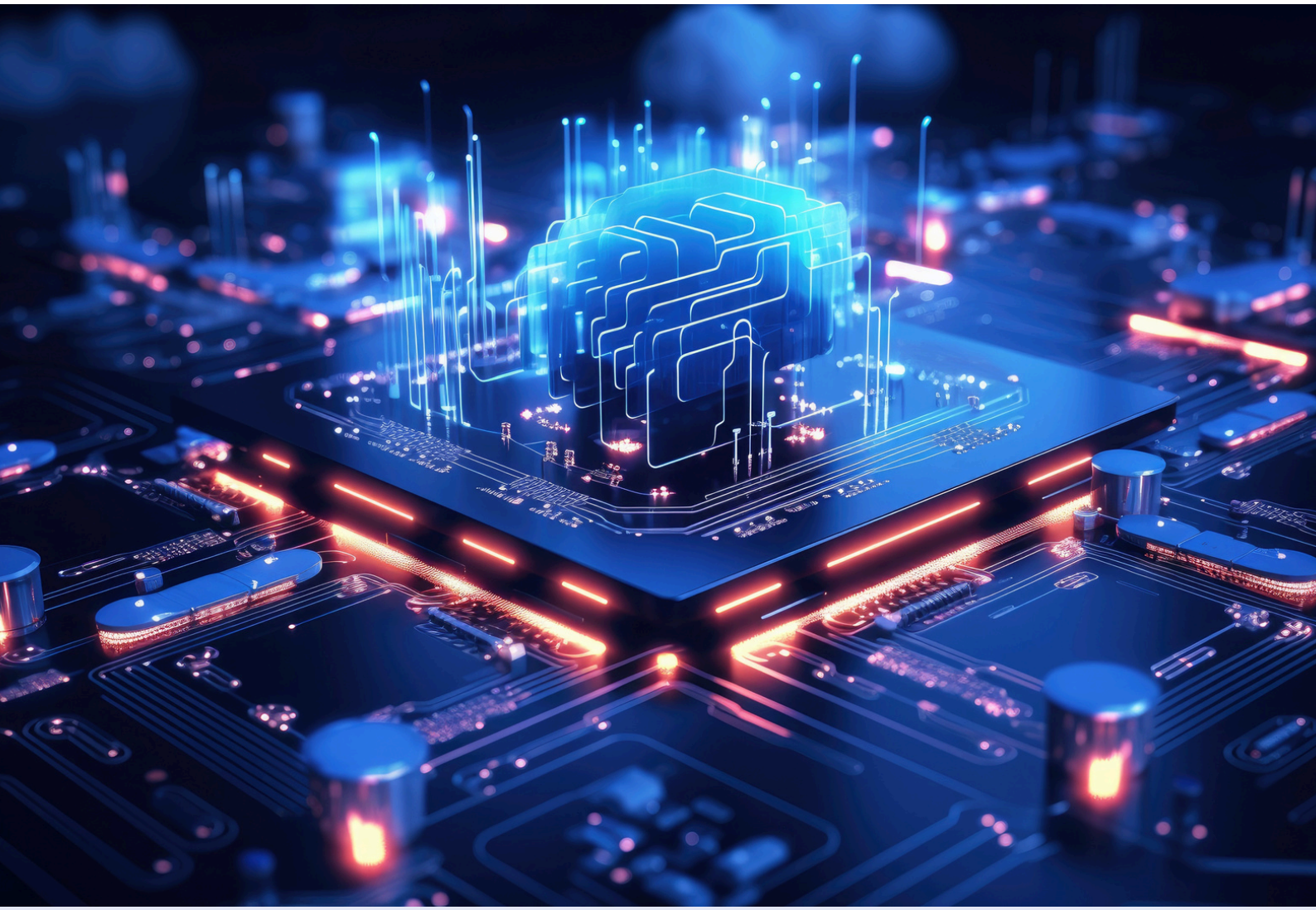
From the perspective of CSIRT KNF, the sectoral module in moje.cert.pl is a step towards a model in which the defence of the financial market is based on the stable, practical sharing of knowledge and not solely on the post factum response. The platform is to facilitate a quick distribution of recommendations, support prioritisation of risks, and raise awareness of threats among the sector's institutions. The final beneficiary of such actions are clients as the shorter time of detection and better coordination of response translate directly into the mitigation of incidents' consequences and the stability of financial services.

The development of the moje.cert.pl platform in a sectoral format, therefore, not only enhances the technical detection and response capacities but also builds confidence in digital financial services. In the context of growing scale of remote transactions and high criminal activity, this is a solution that actually improves the security of the market's functioning by enabling quicker, more consistent and more effective defence activities.

Image 53. Information about the moje.cert.pl project.

More details about the project can be found here:

3.6 COOPERATION WITH CSIRTS AT THE NATIONAL LEVEL



The effective ensuring of cybersecurity is based on cooperation and efficient flow of information among national-level CSIRTs and sectoral teams. This is exactly the regular exchange of knowledge, observations and experience that makes it possible to identify threats faster, assess their importance more accurately, and coordinate mitigation measures more effectively. Year 2025 confirmed, again, that well-organised cooperation among teams has a direct impact on the security and stability of the Polish financial sector. Below is a short summary prepared by national-level CSIRT teams, covering their perspective on actions taken together with CSIRT KNF and examples of what particularly supported the effectiveness of our cooperation in the past year.

CSIRT MON

In 2025, cooperation between CSIRT MON and CSIRT KNF was mainly of practical and operational nature. It focused on the efficient exchange of information, verification of observations, and quick forwarding of signals of threats potentially important also for the financial market. In cybersecurity, these are often details that matter, which is why direct communication among named contact points in both teams was the foundation of cooperation.

On a daily basis we used a communication channel to exchange short observations, questions, arrangements and indicators of compromise (IoC), requiring quick confirmation or additional information. Such a model allowed us to efficiently decide whether a specific signal requires that an incident should be registered or monitored further and enabled the exchange of information in a pace appropriate to the dynamics of threats.

In 2025, CSIRT MON registered four incidents related to the remit of CSIRT KNF and five exchanges of information with CSIRT KNF were carried out without officially registering incidents.

The exchanged information concerned both ongoing threats, such as ‘commodity’ threats, and threats related to the activity of APT groups. The common area of interest was also communication of IoCs related to phishing campaigns.

The continuity of cooperation is also essential. In 2023–2024, CSIRT KNF and competent units on the MON side would actively cooperate in the area of gathering intelligence on infrastructure related to one of hacktivist groups involved in DDoS attacks. Information collected as part of that cooperation are still used in mechanisms of informing entities belonging to the national cybersecurity system about the activity of the group by supporting quicker intelligence and preparing defence measures.

To sum up, in 2025, the cooperation between CSIRT MON and CSIRT KNF was smooth and of clearly operational nature, supporting the swift exchange of information about risks relevant also for the financial market. We are planning to develop it further in the years to come through cyclical working meetings and gradual automation of the process of exchanging information about threats based on modern standards. In order to maintain high-quality cooperation, the standardisation of operational rules (such as escalation, minimum scope of data, IoC distribution), while staying compliant with legislation and industry standards, is also being considered.

CSIRT GOV

In 2025, CSIRT GOV witnessed a stable, high number of incidents related to social engineering attacks that were targeted attacks or used the attributes (image, similar website – typosquatting) of banking sector entities. Advertisements of fake investments in projects of banking sector, government or private entities have remained a constant theme over the recent years. It is not rare that in order to make the alleged investments look legitimate, the image of persons holding public functions was used.

Another persistent threat for the Polish financial sector are attempts of exploiting– often critical – vulnerabilities present in widely used components and ICT systems. Increasingly often one may observe mass attempts of exploiting new vulnerabilities, including 0-day ones, in popular services, and the timeframe between first reports about a vulnerability and attempts to exploit it becomes increasingly shorter.

One of the growing threats for the Polish financial sector can be APT (Advanced Persistent Threat) groups, whose main goal is to achieve financial profit. Currently, a limited activity of such groups is being noted, but they are likely to intensify their actions in the nearest future.

Therefore, as always, it is key to cooperate closely and exchange information about threats in the cyberspace of the Republic of Poland among entities subject to the Act on the National Cybersecurity System.

In view of both the aforementioned challenges for the financial sector of the Republic of Poland witnessed so far and the growing threats, quick time of response is of the essence. On-going cooperation and exchange of information among CSIRT GOV, CSIRT KNF and other entities subject to the Act on the National Cybersecurity System in all situations remains invaluable.

Cooperation between CSIRT KNF and CSIRT NASK in counteracting cyber threats

One of the main drivers of effective cooperation between CSIRT KNF and CSIRT NASK is a high level of communication, both in terms of pace of exchange of information and mutual trust. This allows for quicker sound decisions and accurate measures.

Due to the sectoral nature of CSIRT KNF, the team plays an important role as a single contact point between the national CSIRT and financial market entities. This actually facilities coordination and speeds up incident response.

Examples of benefits from the cooperation

- Reporting suspected bank accounts – information acquired by CERT Polska are received, via CSIRT KNF, quicker by the banking sector for verification.

- Distribution of information about vulnerabilities – if a high-risk vulnerability is detected, CSIRT KNF makes it possible to reach precisely relevant entities in the financial sector. Reversely, based on the diligent actions of CSIRT KNF, CSIRT NASK receives information about new campaigns and detected vulnerable or effectively attacked instances outside the remit of CSIRT KNF. Based on the data, a coordinated incident handling process is launched.

- Response to large-scale incidents – DDoS attacks from the last year targeted at the sector's participants and the Poland-wide issue with card payments confirmed that quick circulation of information is essential and actually helps CSIRT NASK get the full picture of the situation at the national level.

Joint actions in the area of counteracting cyber threats

For the second year running, CSIRT KNF reported a record number of materials used by criminals to swindle funds from Polish nationals. All those cases were handled through the CERT Polska Warning List[28]. Cooperation in this regard is not limited, however, to reporting websites; thanks to the continuous exchange of information about criminals' tactics and mutual exchange of techniques and indicators, teams are more effective in identifying new domains and eliminating them before potential victims are reached.

[28] https://cert.pl/lista-ostrzezen/

3.7 EDUCATIONAL ACTIVITIES OF CSIRT KNF

Education is one of the key ways to build the resilience of internet users to current cyber threats. In view of the rising number of attacks, improving skills and knowledge of financial market participants becomes particularly important.

CSIRT KNF actively participates in the activities which aim to promote knowledge about cyber threats and to enhance cybersecurity. As part of the Education Centre for Market Participants (CEDUR) in 2025, representatives of CSIRT KNF served as speakers during training seminars (webinars) addressed to various groups, among others:
1) primary and secondary school students and teachers
2) seniors and their caretakers
3) representatives of institutions competent for protection of rights of non-professional financial market participants, including municipality and district-level consumer ombudsmen
4) staff of commercial banks and cooperative banks
5) financial institutions' staff providing services to online banking customers, and individuals interested in cybersecurity
6) individual financial market participants, including investors

The webinars included, among others:

a) CEDUR webinars organised as part of the 13th edition of Global Money Week (GMW)[29], addressed to primary and secondary school students and teachers:

- 'Cybercriminals in the world of finance', a webinar aimed at raising awareness of the methods used by online fraudsters and presenting good practices for protection against money theft;
- 'Mobile phone safety: how to protect oneself from cybercriminals', a webinar on cybersecurity threats to the funds of mobile device users;

[29] The UKNF is the national coordinator of Global Money Week (GMW) and World Inwestor Week (WIW) in Poland.

b) CEDUR webinars organised as part of World Investor Week (WIW)[30], addressed to primary and secondary school students and teachers, and individual financial market participants:

- 'Cybersecurity from the perspective of a user of financial services: practical aspects', a webinar aimed at raising awareness of the methods used by online fraudsters and presenting good practices for protection against money theft

- 'Cybersecurity: traps for the young and how to stay safe', a webinar on the practical aspects of cybersecurity in the financial sector, including identified cyber threats targeting the young

- Presentation 'How to improve one's online safety' during the Financial Education Day as part of World Investor Week, with an overview of the most common fraud methods used by cybercriminals and the ways to improve one's online safety

c) CEDUR webinars for seniors and their caretakers:

- 'Safety of seniors: how not to get scammed online', a webinar aimed at raising awareness among seniors and sensitising this social group as a group which is particularly vulnerable to cybercriminals

- 'Secure online payments for seniors' (three dates), a webinar aimed at raising awareness among seniors and their caretakers in regard to the current threats caused by cybercriminals.

[30] The UKNF is the national coordinator of Global Money Week (GMW) and World Inwestor Week (WIW) in Poland.

The training courses focused on the overview of the most common methods of attacks on the funds of internet and mobile device users, and good practices on how to improve online safety, illustrated by relevant examples for each group of users. The webinars for, among others, seniors and their caretakers were organised by the UKNF in cooperation with the National Police Headquarters and the Minister for Senioral Policy.

Participation in the training initiatives, including CEDUR webinars, was free.

More information about CEDUR webinars can be found at:

In 2025, representatives of CSIRT KNF also participated in conferences and events dedicated to cybersecurity, including:

- Conference ‘Safe school in the digital world: challenges and solutions’. On 26 March 2025, the Teacher Training Centre (CEN) in Białystok hosted a province-level conference ‘Safe school in the digital world: challenges and solutions’. The event was attended by teachers, school principals, school counsellors, psychologists and experts on education and safety of the youth. The meeting aimed to draw attention to new threats related to the students’ functioning in the digital world and to present specific tools and measures that can help support their online safety. During the conference, representatives of CSIRT KNF presented practical methods of prevention against data theft and all kinds of cyberattacks. The conference also served as a vital forum for the exchange of views and experiences, allowing the participants to reflect on how school can effectively prepare young people to use technology with awareness and responsibility.

- Training course ‘Innovations and cybersecurity in the financial market’. A series of training courses for secondary school students was held as part of the Education Centre for Financial Market Security (CEBRF). The goal was to explain the key principles of safe use of the internet and financial services. The participants could learn more about most common online shopping fraud methods and phishing attempts using fake online banking sites. Moreover, explanation was provided on the tactics used by cybercriminals and on how to spot potential threats.

- Cybersecure finance classes for the youth. On 20 March, The Kornel Makuszyński Primary School No 2 in Pruszków held a training course dedicated to financial innovations, cybersecurity, and disinformation. The event gathered students from Pruszków and local high schools. One part of the workshop focused on digital safety in the area of finance. Katarzyna Bartnik, a representative of CSIRT KNF, discussed the most common online threats, tactics used by cybercriminals, and practical ways to protect oneself against various scams.

- Participation in the meeting of the Senioral Policy Council. Karol Paciorek, Manager of CSIRT KNF, together with a representative of the UKNF’s Commercial Banking Department took part in the meeting of the Senioral Policy Council. The meeting provided an overview of the most common methods of cyberattacks encountered by older persons. Threats such as fake investment ads were highlighted and good practices for improving online safety were presented.

- In a material published on CyberDefence24, ‘How cybercriminals clean out our accounts’, Karol Paciorek, Manager of CSIRT KNF, talked about most common methods and techniques used by cybercriminals and presented good practices to improve online safety.

- Cyber24 Day. During another edition of the ‘Cyber24 Day’ conference, Karol Paciorek, Manager of CSIRT KNF, joined a panel dedicated to the challenges and trends regarding digital finance safety. He shared experiences in protecting the financial market against cyberthreats and explained the role of CSIRT KNF in building institutional resilience and in protecting users of cashless services.
  During the panel, the experts discussed:
  a) new forms of scams and cyberattacks,
  b) solutions to enhance the security of online payments,
  c) the role of institutional cooperation in protecting the savings of Polish citizens.

- Conference ‘Cybersecure Lubelskie Province’. On 16 October, Michał Strzelczyk, representative of CSIRT KNF, joined a conference held by the Marshal’s Office of Lubelskie Province in Lublin, the Central Bureau for Combating Cybercrime, the Innovation and Technology Centre in Lublin, and the LCK Lubelskie conference centre. In his presentation, Michał Strzelczyk described the facets of financial crime and the possible ways of detecting it.

- European Cybersecurity Month. As part of the educational campaign, CSIRT KNF focused on the protection of finances and personal data of online users. This involved posting on social media, throughout the month, practical tips and infographics to warn the public against most common cyberthreats. The prepared content advised on how to effectively protect bank accounts and how to recognise suspicious phishing attempts, while minimising the risk of data or money theft.

- Partnership for Cybersecurity. CSIRT KNF cooperates with and provides support to the entities and organisations which develop cybersecurity competences. As part of the 'Partnership for Cybersecurity' programme – initiated by NASK – PIB Polish Research Institute) and the Ministry of Digital Affairs and serving as a platform for the exchange of information about cyber threats – representatives of CSIRT discussed aspects of business continuity in the financial market, outlined the cyberthreat landscape and indicated the most common fraud methods used by cybercriminals.

- A training session for Sister Bursars at convents. As more and more attacks target cyberspace users, a training session was conducted for Sister Bursars at convents to provide information about cyber threats and possible protection measures.

- CyberDay. Representatives of CSIRT KNF also participated in an event dedicated to raising cybersecurity awareness, organised by Bank Gospodarstwa Krajowego. The presentation showed the landscape of threats in the financial sector as well as the methods and tactics used by cybercriminals.

- An interview for CyberDefence24. In an episode of CyberDefence24 from the 'Cybersecure as a bank' series, Karol Paciorek, Manager of CSIRT KNF, talked about the most common scam methods used by cybercriminals during Black Week as well as good practices on secure online shopping.

- KSC-EXE 2025. Representatives of the UKNF acting as the competent authority and CSIRT KNF (the sectoral team for cybersecurity for the financial sector) took part in the KSC-EXE 2025 national cybersecurity exercise. The exercise verified, among others:
  a) the effectiveness of incident response procedures;
  b) the speed and quality of inter-institutional communication;
  c) the coordination of work during a crisis.

Education Centre for Financial Market Security (CEBRF)

The Education Centre for Financial Market Security (CEBRF) was launched by the UKNF and its Computer Security Incident Response Team for incidents in the Polish financial sector (CSIRT KNF). The core mission of the Centre is to carry out information and education activities and to promote knowledge about financial security. Cybercriminals constantly come up with new tactics to carry out online scams. It is essential to understand that – apart from blocking fake domains or reporting unsafe ads – what we need is educational activities to raise awareness among cyberspace users. The CEBRF website contains publications on current cyber threats and scam methods.

CEBRF publications

CSIRT KNF is monitoring and identifying current cyber threats. As part of the educational activities in 2025, the following were published:

- Krajobraz zagrożeń w polskim sektorze finansowym 2025 (GTL) [The landscape of threats in the Polish financial sector 2025]. The document gives a comprehensive overview of the key threats to the financial sector. Each section describes attack methods, examples of incidents, and motivations of cybercriminals. The purpose is to provide exhaustive information that can help readers defend themselves against threats.

The full document can be found at:

- Analiza złośliwej aplikacji mobilnej IKO Lokata [Analysis of the malicious IKO Lokata mobile app]. The document analyses a campaign spotted by CSIRT KNF on Facebook, in which cybercriminals would publish fake ads urging users to download malware impersonating a non-existent 'IKO Lokata' app. The campaign was targeted at users of the Android system.

The analysis of the campaign and potential consequences of downloading the malicious app on a device can be found here:

- Przegląd wybranych oszustw internetowych [Overview of selected online scams]. A monthly series of articles about the newest threats and attack methods used by cybercriminals as identified by CSIRT KNF

CSIRT KNF monthly overviews of selected online scams can be found here:

- Overview of online scams, January 2025
- Overview of online scams, February 2025
- Overview of online scams, March 2025
- Overview of online scams, April 2025
- Overview of online scams, May 2025
- Overview of online scams, June 2025
- Overview of online scams, July 2025
- Overview of online scams, August 2025

- Overview of online scams, September 2025
- Overview of online scams, October 2025
- Overview of online scams, November 2025
- Overview of online scams, December 2025

The activity of CSIRT KNF on social media

One of the key activities of CSIRT KNF is the divulgation of knowledge about current cyber threats. For this purpose, the Team mainly uses social media, which allow it to respond quickly to the emerging threats and to reach the users effectively. Its public communications become part of information circulating in the media and are then used by numerous general and specialised news services. In 2025, this translated into 1 995 press articles based on information provided by CSIRT KNF.

The Team's online activity was focused on a regular publication of warnings and educational materials regarding cybercrime. In the same year, 177 posts appeared, aiming to raise cybersecurity awareness among users and to reduce the risk of financial losses.

The warnings about threats usually concerned attempts to impersonate financial institutions, the use of malware to take over money, fake investment ads to steal personal data, and fake shopping sites designed to obtain payment card details.

We invite everyone to follow the CSIRT KNF accounts on Twitter/X, LinkedIn and Facebook, where we are posting news and updates about new tactics of cybercriminals.

CONTACT

Polish Financial Supervision Authority

Cybersecurity Department – CSIRT KNF

ul. Piękna 20,
00-549 Warszawa

knf@knf.gov.pl
csirt@knf.gov.pl