KNF CSIRT

RAPORT ROCZNY
CYBERBEZPIECZEŃSTWA
2025

POLSKI RYNEK FINANSOWY W OBLICZU ZAGROŻEŃ

SPIS TREŚCI

01. Wstęp (str. 2-4)

02. Bezpieczeństwo klienta rynku finansowego (str. 5-46)

- 2.1 Fałszywe inwestycje jako oszustwo o dominującej skali (str. 6-24)
- 2.2 Fałszywe sklepy – rosnące zagrożenie (str. 25-30)
- 2.3 Oszustwa na klientów bankowości (str. 31-37)
- 2.4 Złośliwe oprogramowanie (str. 38-46)

03. Bezpieczeństwo podmiotów rynku finansowego (str. 47-100)

- 3.1 Cyber Threat Intelligence – od reagowania do przewidywania (str. 48-54)
- 3.2 Ataki DDoS na rynek finansowy (str. 55-61)
- 3.3 Aktualne trendy cyberzagrożeń (str. 62-74)
- 3.4 DORA jako fundament cyberodporności rynku finansowego (str. 75-79)
- 3.5 moje.cert.pl – sektorowy moduł CSIRT KNF dla rynku finansowego (str. 80-83)
- 3.6 Współpraca z CSIRT-ami poziomu krajowego (str. 84-89)
- 3.7 Działania edukacyjne CSIRT KNF (str. 90-100)

Rok 2025 potwierdził, że polski rynek finansowy należy do najbardziej zdigitalizowanych w Unii Europejskiej, a aktywność klientów w kanałach mobilnych i internetowych osiąga poziomy wyjątkowe w skali naszego kontynentu. Ta dojrzałość cyfrowa wzmacnia konkurencyjność sektora, zwiększa dostępność usług i buduje wygodę po stronie użytkowników, ale równocześnie naturalnie poszerza pole ataku. W konsekwencji cyberbezpieczeństwo staje się nie tylko obszarem technicznym, lecz jednym z filarów stabilności i zaufania do systemu finansowego. Zewnętrzne analizy opublikowane pod koniec listopada 2025 roku wskazują, że Polska zajmuje pierwsze miejsce w Unii Europejskiej pod względem liczby transakcji mobilnych i internetowych[1].

W takim kontekście CSIRT KNF w 2025 roku koncentrował się na rozpoznawaniu, monitorowaniu i ograniczaniu skutków zagrożeń, które w największym stopniu oddziałują na bezpieczeństwo klientów oraz ciągłość działania instytucji finansowych. Obserwowaliśmy dalszą profesjonalizację cyberprzestępczości i rosnącą skalę działań wykorzystujących automatyzację, wieloetapowe scenariusze ataku oraz precyzyjne profilowanie ofiar. Szczególnie istotne miejsce w krajobrazie zagrożeń nadal zajmowały oszustwa oparte o socjotechnikę, w tym kampanie podszywające się pod instytucje finansowe i podmioty zaufania publicznego. Phishing w kanałach SMS i e-mail pozostawał jednym z najczęściej wykorzystywanych wektorów inicjujących incydenty, a jego skuteczność była wzmacniana przez łączenie technik psychologicznych z elementami podszycia technicznego oraz dynamiczną infrastrukturą domenową.

Równolegle utrzymywała się wysoka presja przestępcza związana z fałszywymi inwestycjami. Ten typ oszustw pozostaje szczególnie dotkliwy społecznie i finansowo, gdyż często prowadzi do znacznych strat po stronie klientów indywidualnych.

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

W 2025 roku widzieliśmy dalszą ewolucję narracji oraz sposobów uwiarygadniania takich ofert – od wykorzystania wizerunków osób publicznych i symboli zaufania, po coraz sprawniejsze naśladowanie interfejsów legalnych podmiotów oraz budowanie wielokanałowych ścieżek kontaktu z ofiarą.

Wzrosło znaczenie zagrożeń wynikających z zależności technologicznych i biznesowych. Ataki na łańcuch dostaw – rozumiane zarówno jako kompromitacja dostawców oprogramowania, usług IT, jak i podmiotów wspierających procesy biznesowe – stanowiły wyraźny sygnał, że odporność sektora musi być rozpatrywana w sposób ekosystemowy. Incydent w jednym ogniwie może przełożyć się na ryzyko operacyjne w wielu instytucjach równocześnie, co wymaga dojrzałego zarządzania ryzykiem stron trzecich, konsekwentnych wymagań bezpieczeństwa oraz weryfikowalnych praktyk monitorowania.

Istotnym elementem w 2025 roku była także aktywność złośliwego oprogramowania wymierzonego w urządzenia użytkowników końcowych. Dotyczy to zarówno klasycznych kampanii nastawionych na przejęcie danych uwierzytelniających w środowisku PC, jak i rosnącej skali zagrożeń w ekosystemie mobilnym. W tym obszarze szczególną uwagę zwracamy na scenariusze nadużyć powiązanych z płatnościami zbliżeniowymi oraz technikami pośredniczenia w komunikacji, w tym odmiany ataków typu relay. Zjawiska te podkreślają konieczność dalszego wzmacniania mechanizmów uwierzytelniania wieloskładnikowego, edukacji klientów oraz ochrony urządzeń końcowych w oparciu o aktualne modele ryzyka.

Stałym elementem krajobrazu zagrożeń pozostawały ataki DDoS wymierzone w infrastrukturę podmiotów rynku finansowego. Ich poziom i cykliczność potwierdzają, że jest to narzędzie wykorzystywane zarówno do zakłócania dostępności usług, jak i jako element presji lub zasłona dymna dla działań prowadzonych równolegle. Z perspektywy CSIRT KNF ważne jest jednak to, że w zdecydowanej większości przypadków skutki takich incydentów były ograniczane w sposób szybki i skuteczny. Wskazuje to na rosnącą dojrzałość organizacyjną i technologiczną instytucji nadzorowanych, a także na wartość współdziałania w ramach krajowego systemu cyberbezpieczeństwa.

Raport ten przedstawia podsumowanie kluczowych zjawisk z 2025 roku, najważniejsze obserwacje dotyczące zmieniających się taktyk i technik atakujących oraz syntetyczne wnioski wspierające dalsze wzmacnianie odporności cyfrowej sektora finansowego. CSIRT KNF pozostaje skoncentrowany na ochronie uczestników rynku, ograniczaniu skali i skutków cyberprzestępczości oraz budowaniu bezpiecznych warunków dla rozwoju innowacyjnych usług finansowych w Polsce.

02. BEZPIECZEŃSTWO KLIENTA RYNKU FINANSOWEGO

2.1 FAŁSZYWE INWESTYCJE JAKO OSZUSTWO O DOMINUJĄCEJ SKALI

Fałszywe inwestycje to od lat najbardziej rozpowszechniony i szkodliwy scenariusz ataku, który ma na celu kradzież środków finansowych. Przestępcy posługując się socjotechniką i manipulacją nakłaniają ofiary do inwestowania w fałszywe inwestycje, które promowane są z wykorzystaniem nośników reklamowych w mediach społecznościowych, wyszukiwarkach internetowych oraz popularnych serwisach informacyjnych. Schemat oszustwa opiera się na obietnicach bardzo wysokich zysków przy minimalnym bądź nawet zerowym ryzyku inwestycyjnym.

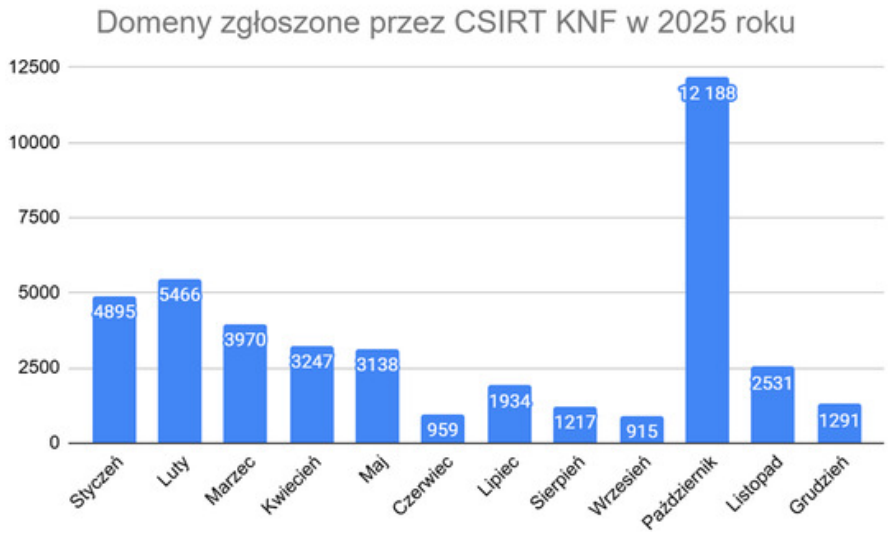
Zmanipulowane ofiary, wierząc w bezpieczną inwestycję, niejednokrotnie przekazują przestępcom oszczędności. Aby sfinansować rzekomą inwestycję, często są również skłonni do zaciągnięcia kredytów lub pożyczek. Ten rodzaj oszustw to od lat najbardziej powszechne i szkodliwe zagrożenie skutkujące ogromnymi stratami finansowymi poszkodowanych osób.

Domeny phishingowe

CSIRT KNF, korzystając z różnych narzędzi, na bieżąco monitoruje i zgłasza do blokady treści publikowane przez przestępców. Głównym celem blokad są witryny oraz reklamy wyłudzające dane poprzez formularze kontaktowe.

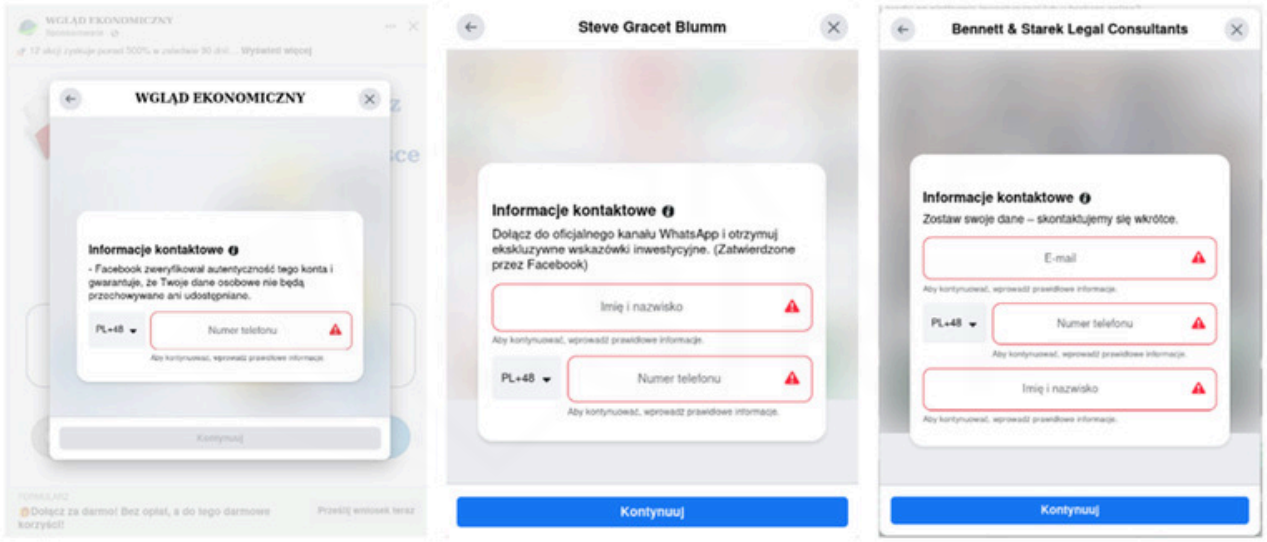
Mechanizm oszustwa opiera się na pozyskaniu danych kontaktowych nieświadomego użytkownika. Zazwyczaj wyłudzane jest imię, nazwisko oraz numer telefonu. Zdobyte w ten sposób informacje służą przestępcom do przeprowadzenia ataku socjotechnicznego – podczas rozmowy telefonicznej nakłaniają oni ofiary do ulokowania kapitału w fikcyjne instrumenty finansowe, które w rzeczywistości nigdy nie istniały.

W 2025 roku CSIRT KNF zidentyfikował i zgłosił do blokady 41 751 niebezpiecznych domen. Aż 40 225 z nich było związanych z fałszywymi inwestycjami, co stanowi ponad 96,34% wszystkich zgłoszonych domen. Ta liczba nie pozostawia wątpliwości co do utrzymującej się od lat ogromnej skali tego zagrożenia.



Wykres 1. Domeny zgłoszone do CSIRT NASK przez CSIRT KNF w poszczególnych miesiącach 2025 roku

W 2025 roku zaobserwowano ewolucję w kampaniach promujących fałszywe inwestycje. Atakujący bardzo często wykorzystywali formularze wbudowane bezpośrednio w ekosystem reklamowy (tzw. Lead Ads), rezygnując z przekierowań na zewnętrzne witryny. Model ten pozwolił na zamknięcie całego procesu oszustwa w obrębie jednej platformy, eliminując koszty takie, jak zakup domen czy hosting. Z perspektywy bezpieczeństwa technika ta znacząco utrudniła mitygację zagrożenia – brak zewnętrznego adresu URL uniemożliwił tradycyjne blokowanie stron docelowych, ograniczając działania defensywne jedynie do zgłaszania samej kreacji reklamowej oraz profilu publikującego reklamę. W rezultacie odnotowaliśmy spadek zgłoszonych stron o 9490 w ujęciu rocznym, przy jednoczesnym wzroście liczby zgłoszonych profili o 1288. Działania mitygacyjne muszą więc obejmować nie tylko blokowanie witryn, ale też szybkie blokowanie kreacji reklamowych, profili i kont reklamodawców.

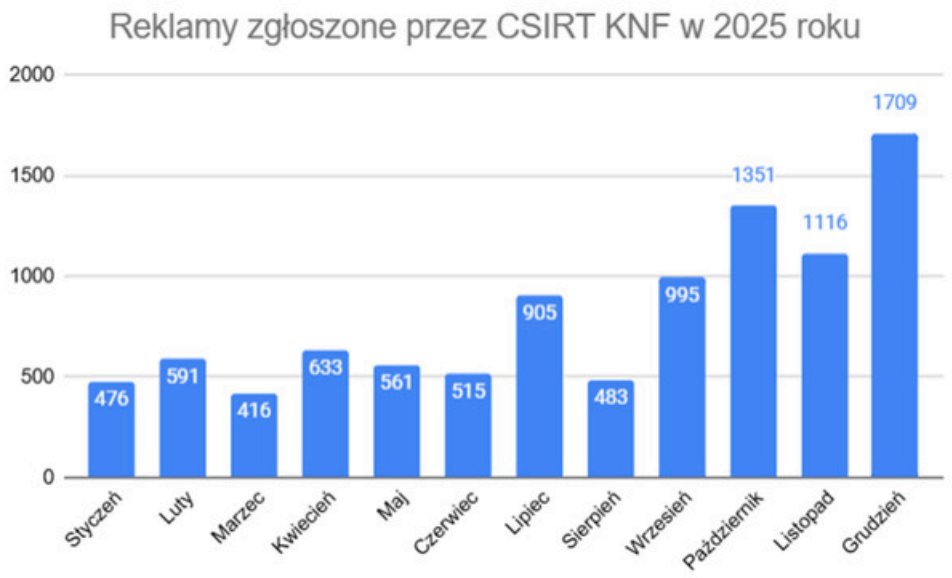


Grafika 1. Formularze kontaktowe w reklamach wykorzystywane przez przestępców

Reklamy w mediach społecznościowych

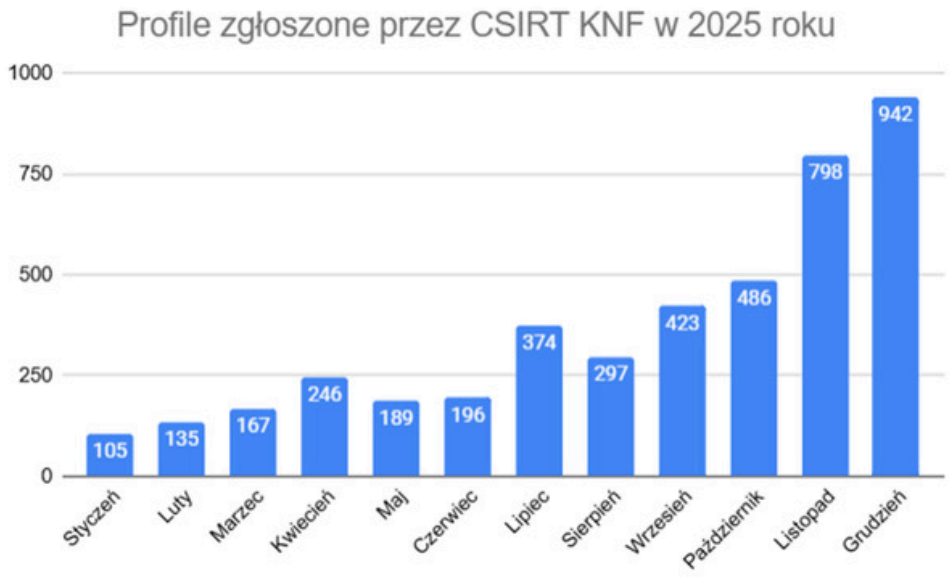
Fundamentem działalności CSIRT KNF jest partnerstwo z podmiotami krajowymi i zagranicznymi. W ramach walki z cyberprzestępczością CSIRT KNF utrzymuje kanały przeznaczone do eskalacji zgłoszeń. Ciągła wymiana informacji o zagrożeniach pozwala na znacznie szybszą reakcję i skuteczniejsze blokowanie szkodliwych treści w Internecie.

W odpowiedzi na utrzymującą się dużą liczbę fałszywych reklam na platformie Facebook, zespół CSIRT KNF utrzymuje specjalną ścieżkę szybkiego reagowania, służącą do zgłaszania i blokowania szkodliwych treści na tej platformie. Skutkiem tych działań w 2025 roku było zablokowanie 9751 oszukańczych reklam.



Wykres 2. Reklamy zgłoszone przez CSIRT KNF w 2025 roku w poszczególnych miesiącach

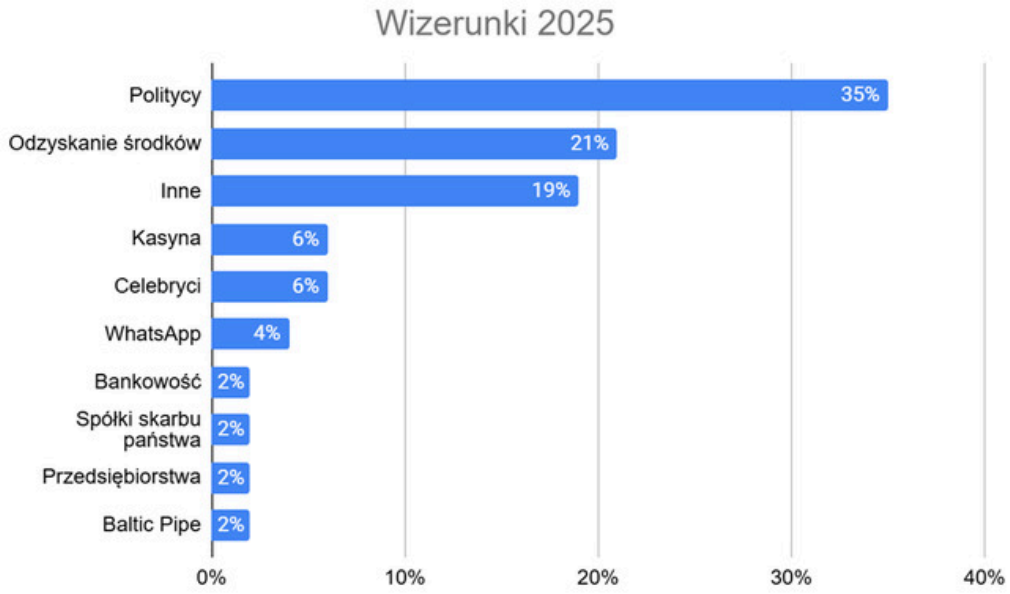
Zgłosiliśmy również 4358 profili publikujących fałszywe reklamy. Jest to wzrost o 41,95% w porównaniu do roku ubiegłego. W rezultacie konta te zostały zablokowane, co uniemożliwiło im zamieszczanie kolejnych złośliwych treści.



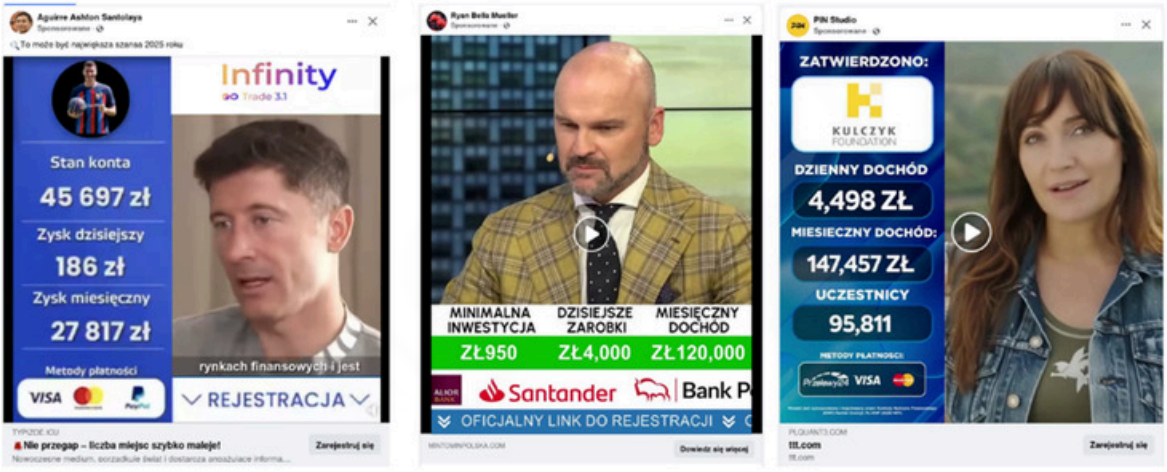
Wykres 3. Profile zgłoszone przez CSIRT KNF w 2025 roku w poszczególnych miesiącach

Wykorzystywane wizerunki

Przestępcy, aby nadać oszustwu pozory autentyczności i wzbudzić zaufanie ofiar, często posługiwali się wizerunkami znanych osób i logotypami firm. W fałszywych reklamach standardem stało się wykorzystywanie zdjęć polityków, celebrytów czy przedsiębiorców. Wykorzystywano również wizerunki autorytetów z branży finansowej oraz logotypy działających firm, co miało na celu sugerować powiązanie z „prawdziwym" biznesem.



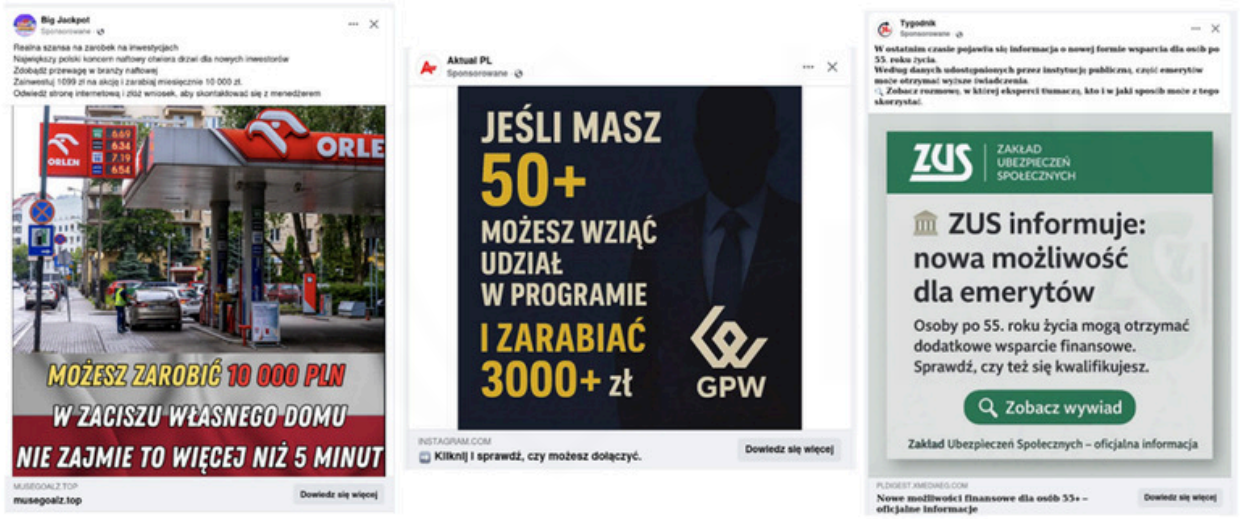
Wykres 4. Wykorzystywane wizerunki obserwowane w oszukańczych reklamach w 2025 roku



Grafika 2. Przykładowe wizerunki wykorzystywane w reklamach fałszywych inwestycji

Oszuści chętnie żerowali na zaufaniu, jakim Polacy darzą instytucje państwowe. W fałszywych kampaniach nagminnie pojawiały się nawiązania do instytucji i spółek takich, jak Orlen, ZUS czy Giełda Papierów Wartościowych. Równie atrakcyjnym „wabikiem" były wielkie projekty infrastrukturalne, takie jak Baltic Pipe oraz Baltica.

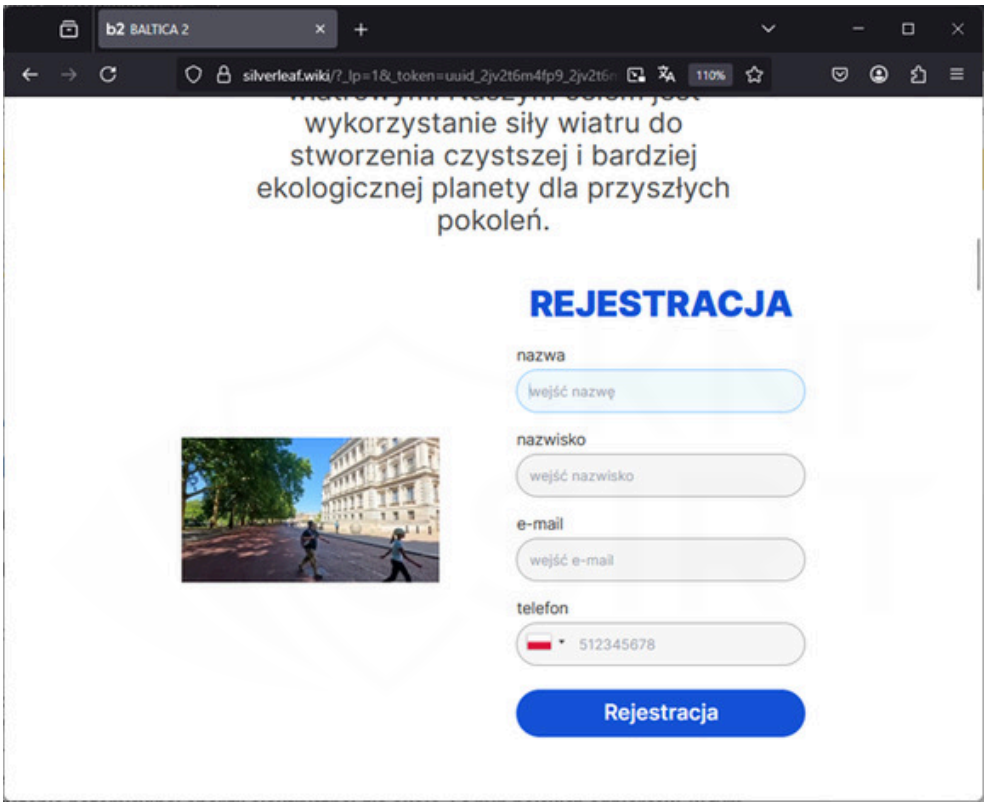
Cyberprzestępcy tworzyli fałszywą narrację sugerując, że każdy obywatel może stać się udziałowcem tych przedsięwzięć i zarabiać na bezpieczeństwie energetycznym kraju. Wykorzystywanie tych nazw ma na celu uśpienie czujności potencjalnych ofiar.



Grafika 3. Przykłady firm i instytucji wykorzystywanych w reklamach fałszywych inwestycji

Grafika 4. Reklama fałszywej inwestycji w projekt infrastrukturalny Baltica 2

Grafika 5. Artykuł na fałszywej stronie informujący o przełomowym projekcie energetycznym

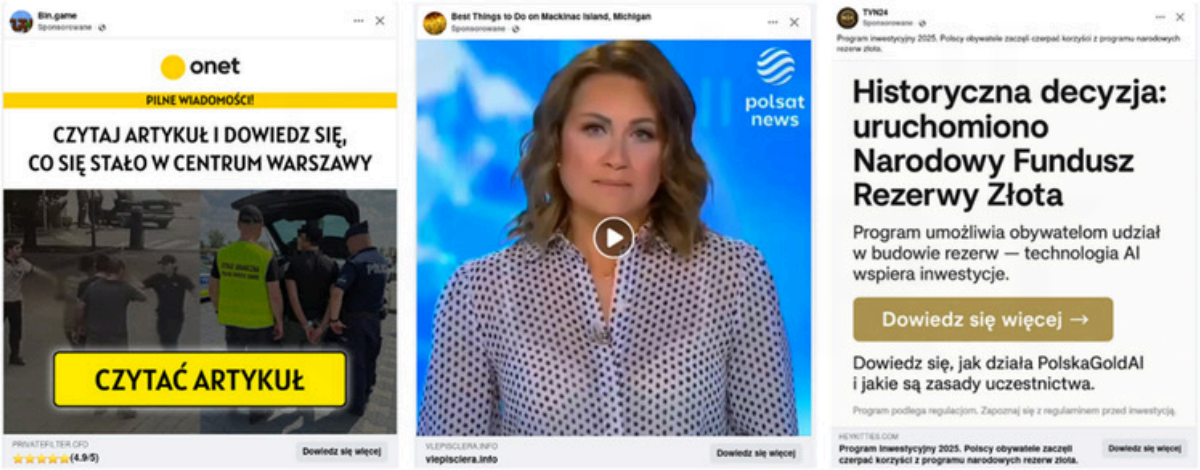


Grafika 6. Formularz kontaktowy wykorzystywany do zbierania danych kontaktowych

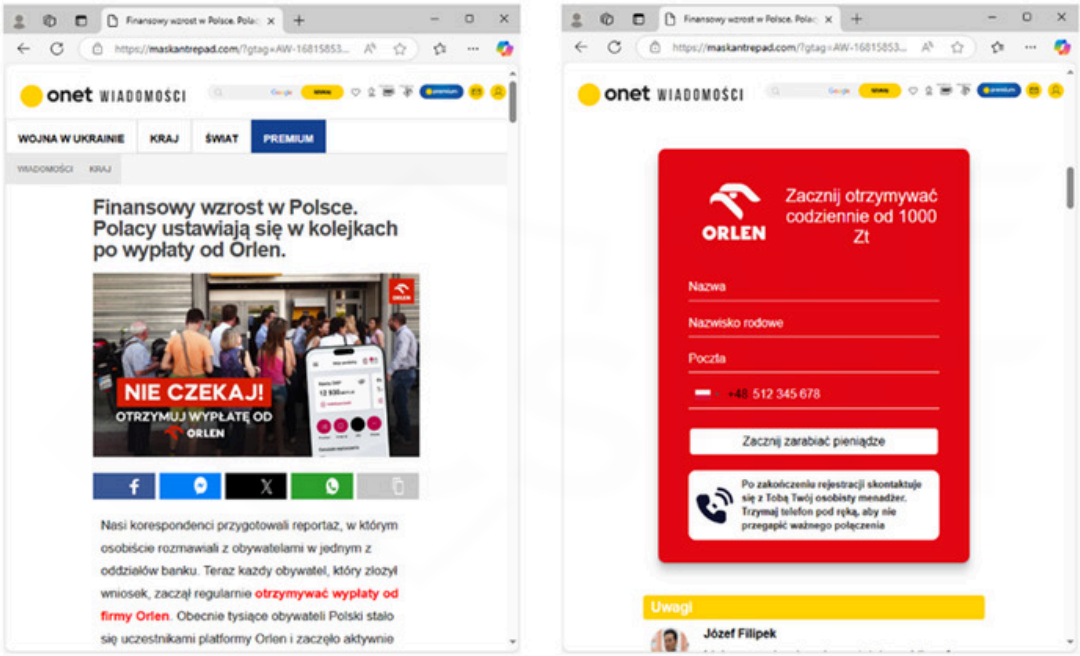
Oszuści nie ograniczali się jedynie do spółek państwowych wykorzystując autorytet całego sektora finansowego. Aby uwiarygodnić fikcyjne oferty w swoich kampaniach bezprawnie posługiwali się znakami firmowymi banków oraz renomowanych biur maklerskich. W spreparowanych reklamach i artykułach często sugerowano istnienie tajnych partnerstw lub ekskluzywnych programów inwestycyjnych dostępnych rzekomo tylko dla klientów tych konkretnych instytucji, co dodatkowo potęgowało presję na ofierze do szybkiej wpłaty środków.

Grafika 7. Przykłady reklam wykorzystujących logotypy firm z sektora finansowego

Przestępcy często sięgali po elementy wizualne czołowych mediów oraz portali branżowych, tworząc całe witryny imitujące prawdziwe serwisy informacyjne. CSIRT KNF wielokrotnie odnotowywał przypadki wykorzystania znaków towarowych serwisów informacyjnych takich, jak Onet, Money.pl czy TVN24. Oszuści preparowali fałszywe artykuły i wywiady, a w celu dodania ofercie atrakcyjności podszywali się również pod specjalistyczne portale finansowe. Dzięki temu ofiara miała wrażenie, że o „inwestycji życia" napisali rzetelni dziennikarze i eksperci.

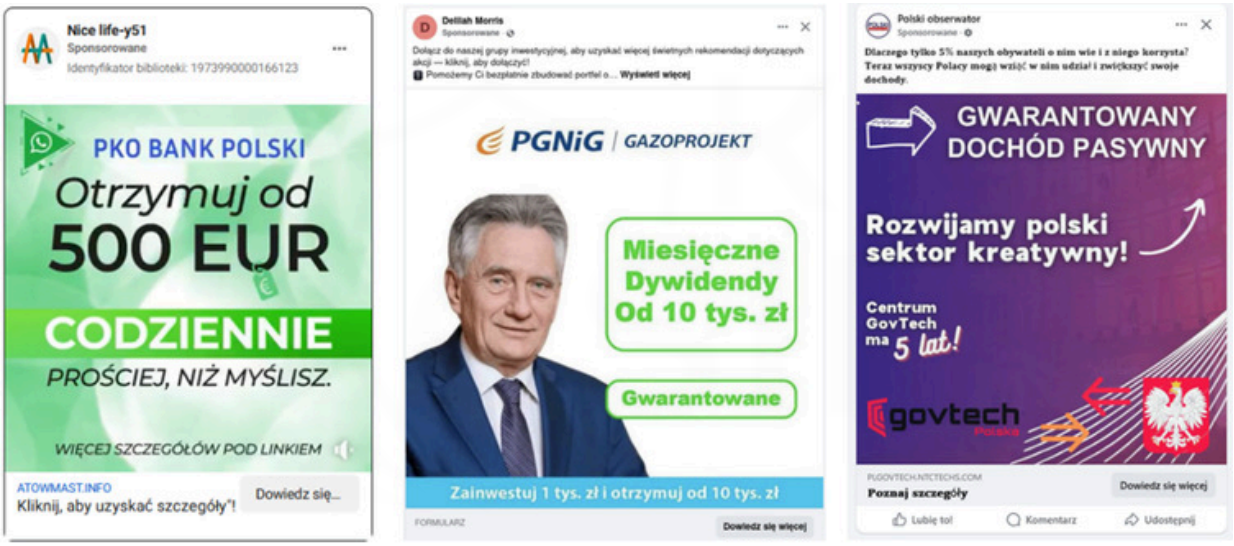


Grafika 8. Przykłady reklam podszywających się pod serwisy informacyjne



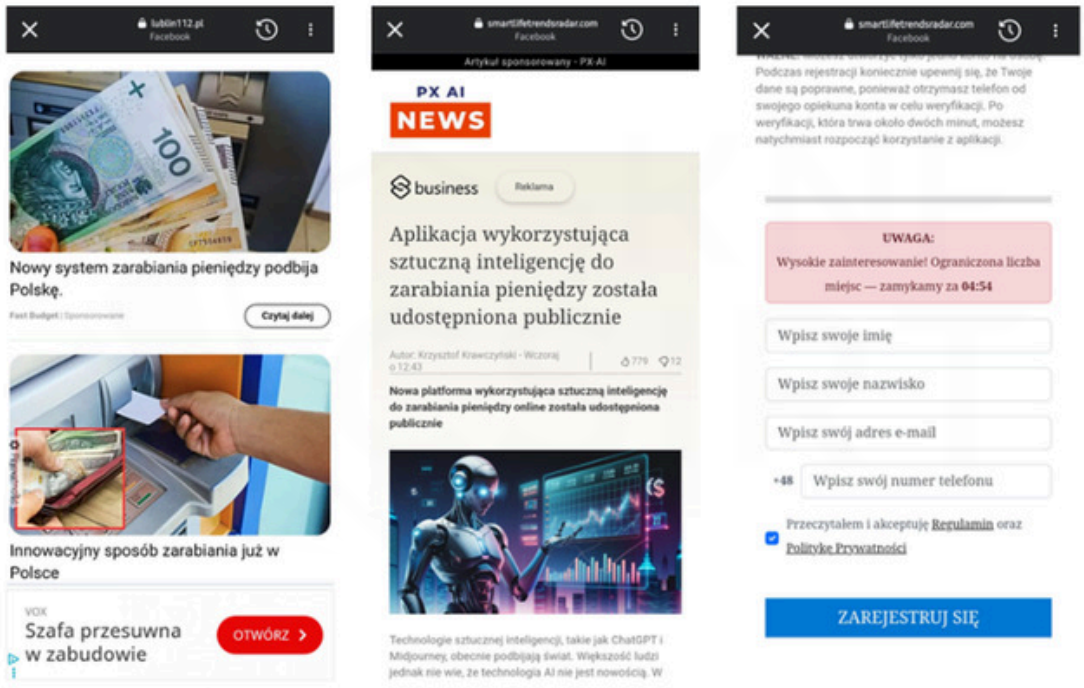
Grafika 9. Artykuł na fałszywej stronie nakłaniający do zainwestowania w fałszywe inwestycje

Uzupełnieniem wiarygodnej warstwy graficznej były opisy kuszące wizją błyskawicznego i bezwysiłkowego wzbogacenia się. Sprawcy stosowali manipulacyjne slogany wmawiając ofiarom, że za sukces odpowiadają nowoczesne, tajne algorytmy lub sztuczna inteligencja. W treściach reklamowych dominowały frazy sugerujące brak ryzyka oraz wizja pasywnego dochodu, osiąganego bez konieczności posiadania wiedzy ekonomicznej. Hasła takie, jak: „otrzymuj 500 euro dziennie” czy „gwarantowany dochód” miały przekonać odbiorcę, że technologia wykona całą pracę za niego.



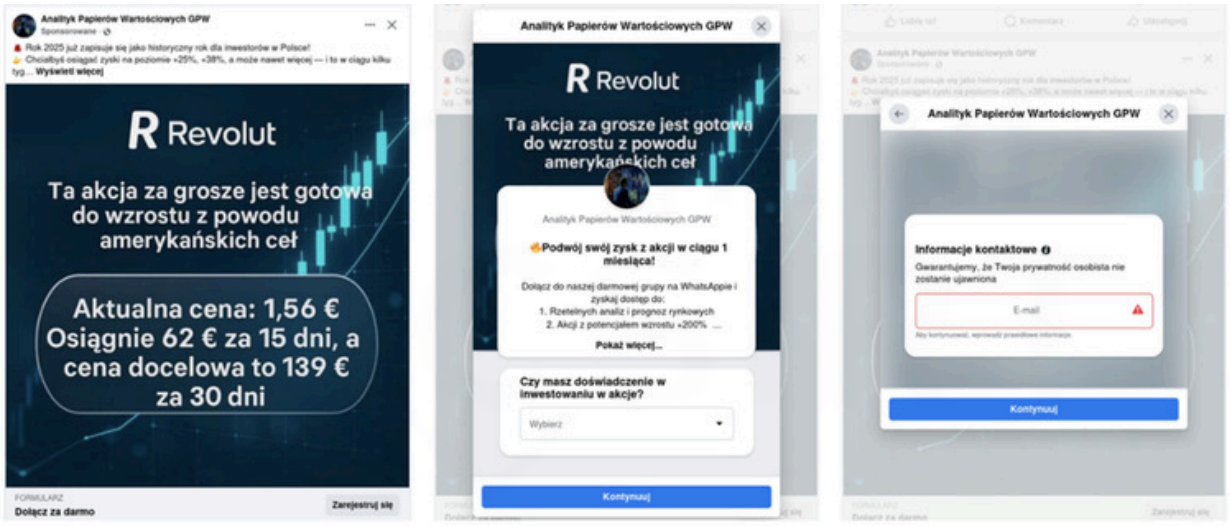
Grafika 10. Przykłady chwytliwych haseł w reklamach fałszywych inwestycji

Grafika 11. Przykładowe reklamy fałszywych inwestycji z wykorzystaniem motywu sztucznej inteligencji



Grafika 12. Reklama fałszywej inwestycji oraz strona docelowa

Analiza newsów, trendów i nastrojów społecznych służyła im do błyskawicznego dopasowywania swoich działań. W rezultacie wątki nawiązujące do głośnych wydarzeń były niemal natychmiast implementowane w treściach fałszywych reklam oraz na oszukańczych stronach.



Grafika 13. Reklama fałszywej inwestycji nawiązująca do wprowadzenia amerykańskich ceł

Reklamy fałszywych inwestycji odnotowano również w serwisach YouTube, Bing, Google, TikTok oraz na platformie X, jednak w znacznie mniejszej skali. Może to być spowodowane tym, że Facebook oferuje oszustom dostęp do szerszego grona potencjalnych ofiar, co przekłada się na wyższą skuteczność ich działań na tej platformie.

Grafika 14. Reklamy fałszywych inwestycji na platformach YouTube.com oraz X.com

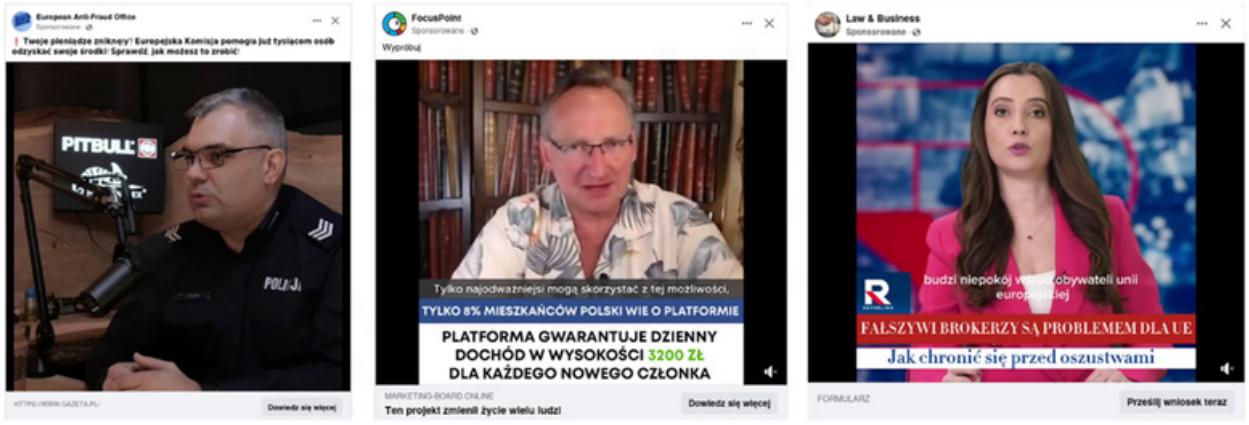
Rada dla internautów

Nie daj się zwieść internetowym obietnicom szybkiego i wysokiego zarobku, gdyż zazwyczaj są one próbą oszustwa. Przed każdą inwestycją skonsultuj się z licencjonowanym doradcą i koniecznie zweryfikuj firmę, zaglądając między innymi na Listę ostrzeżeń publicznych KNF. Pamiętaj, że w sieci obowiązuje zasada ograniczonego zaufania – jeśli oferta wydaje się zbyt idealna, by była prawdziwa, najpewniej jest fałszywa.

Deepfake

Oszuści w swoich materiałach czasami korzystają z technologii deepfake. Służy im ona do kradzieży tożsamości znanych osób, polityków i dziennikarzy, by ich wizerunkiem firmować m.in. fałszywe inwestycje. Technika ta umożliwia tworzenie wiarygodnych filmów, w których twarze są podmieniane, a głosy klonowane w taki sposób, że odbiorca ma wrażenie, że ogląda autentyczną przemowę lub prawdziwe wystąpienie.

Całość często wygląda bardzo realistycznie i na „pierwszy rzut oka" może być bardzo trudna do odróżnienia od prawdy. Ruch warg może być zsynchronizowany z wypowiadanymi słowami, a barwa głosu łudząco przypominać tą prawdziwą. Przestępcy generują fałszywe wywiady i wystąpienia, które mają na celu uwiarygodnienie oszustwa w oczach ofiar.



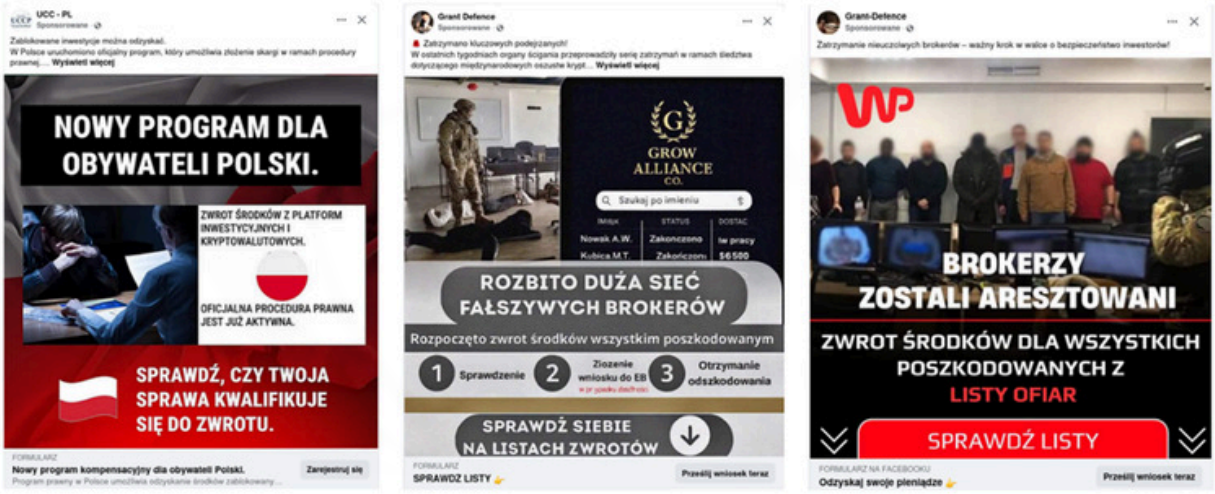
Grafika 15. Przykłady wizerunków wykorzystanych w deepfake'ach

Z przykładowymi nagraniami wykorzystującymi tę technologię do promocji fałszywych inwestycji można zapoznać się na stronie Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego, dostępnej pod adresem: https://cebrf.knf.gov.pl/deepfake

Oszustwo na odzyskiwanie skradzionych środków

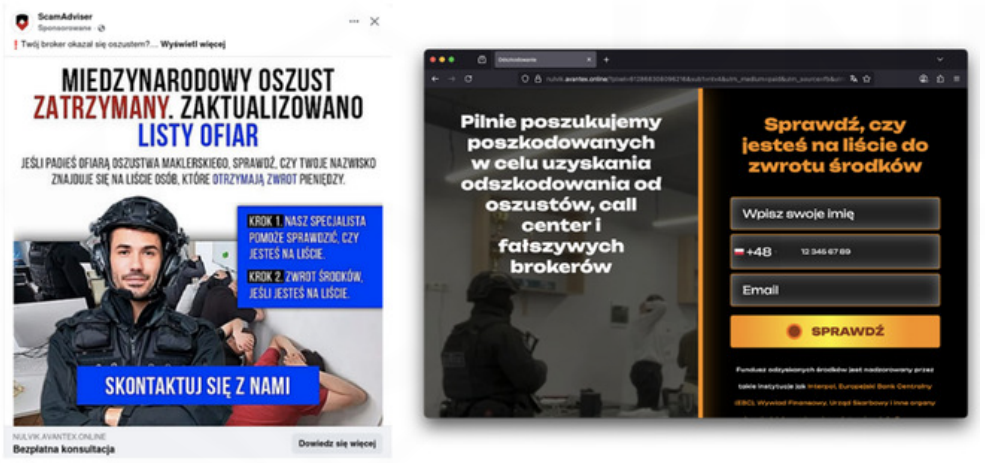
W stosunku do 2024 roku odnotowujemy znaczący wzrost reklam oferujących możliwość odzyskania wcześniej skradzionych środków finansowych (ang. recovery scam). To rodzaj oszustwa, w którym przestępcy podszywają się pod firmy lub organizacje zajmujące się odzyskiwaniem utraconych środków finansowych.

W rzeczywistości jest to kontynuacja schematu oszustwa na fałszywe inwestycje, które ma na celu ponowne oszukanie osób, które już wcześniej padły ofiarą fałszywych inwestycji. Przestępcy kontaktują się z ofiarami przedstawiając się jako kancelarie, prawnicy lub specjaliści od windykacji, twierdząc, że mają możliwość odzyskania utraconych środków.



Grafika 16. Fałszywe reklamy oferujące możliwość zwrotu skradzionych środków

Mechanizm działania jest wyjątkowo cyniczny i pozostaje zbieżny z pierwotnym oszustwem inwestycyjnym. Reklama przekierowuje na witrynę bądź formularz służący do wyłudzenia danych kontaktowych. Pozyskany numer telefonu lub adres e-mail pozwala sprawcom na nawiązanie kontaktu i manipulację ofiarą, by ta wpłaciła środki pod pretekstem konieczności wniesienia opłat rzekomo koniecznych do odzyskania wcześniej utraconych środków.



Grafika 17. Fałszywa reklama oferująca możliwość odzyskania utraconych środków oraz docelowa strona

Proces wyłudzania może trwać miesiącami. Po początkowej opłacie pojawiają się kolejne żądania – dodatkowe koszty prawne, opłaty administracyjne, podatki czy prowizje. Każda płatność jest przedstawiana jako „ostatnia" przed odzyskaniem pieniędzy. Niektóre ofiary tracą w ten sposób kolejne dziesiątki tysięcy złotych, wierząc, że są coraz bliżej odzyskania pierwotnie utraconych środków.

Rada dla internautów

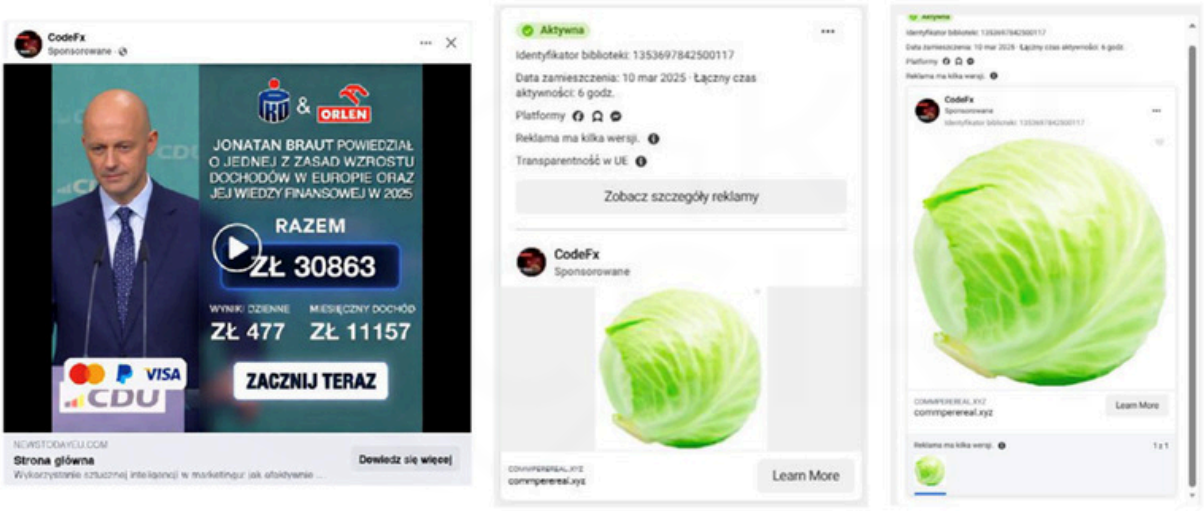
Weryfikuj oferty pomocy. Zanim przekażesz komukolwiek jakiekolwiek pieniądze, skontaktuj się z prawdziwymi instytucjami lub organizacjami. Nie płać za obietnice. Unikaj firm i osób, które żądają opłat „z góry" za odzyskanie pieniędzy. Każde oszustwo zgłaszaj odpowiednim organom ścigania, aby pomóc w zatrzymaniu przestępców. Poszukaj pomocy prawnej.

Maskowanie reklam

Spadek liczby zgłoszonych reklam nie odzwierciedla realnego spadku skali zagrożenia na platformie. Aby uniknąć natychmiastowych blokad, przestępcy coraz kreatywniej i skuteczniej maskują swoje działania, dzięki czemu ich kampanie są trudniejsze do namierzenia i mogą dłużej docierać do użytkowników, zanim zostaną one usunięte.

Wykorzystanie mechanizmu wersjonowania

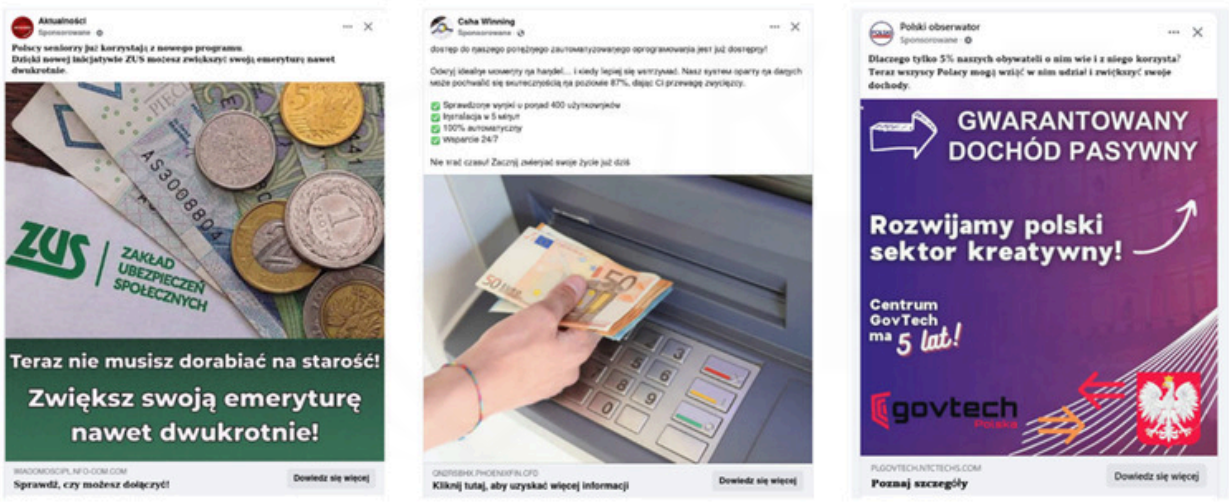
Cyberprzestępcy wykorzystują funkcjonalność systemu reklamowego Facebooka, która pozwala na tworzenie wielu wariantów tej samej reklamy. Ta funkcjonalność jest wykorzystywana przez przestępców do kamuflażu: jedna złośliwa wersja jest ukrywana pośród wielu neutralnych. W rezultacie wstępny podgląd czy weryfikacja plakatu reklamy nie budzą podejrzeń. Wykrycie ataku utrudnia też sama biblioteka reklam. Mimo że system wykrywa wiele wersji reklamy, biblioteka potrafi ograniczyć podgląd do pojedynczego obrazu i nie pokazywać tego, który jest aktualnie wyświetlany użytkownikom.



Grafika 18. Wykorzystanie mechanizmu wersjonowania przez przestępców

Wykorzystanie liter innego alfabetu

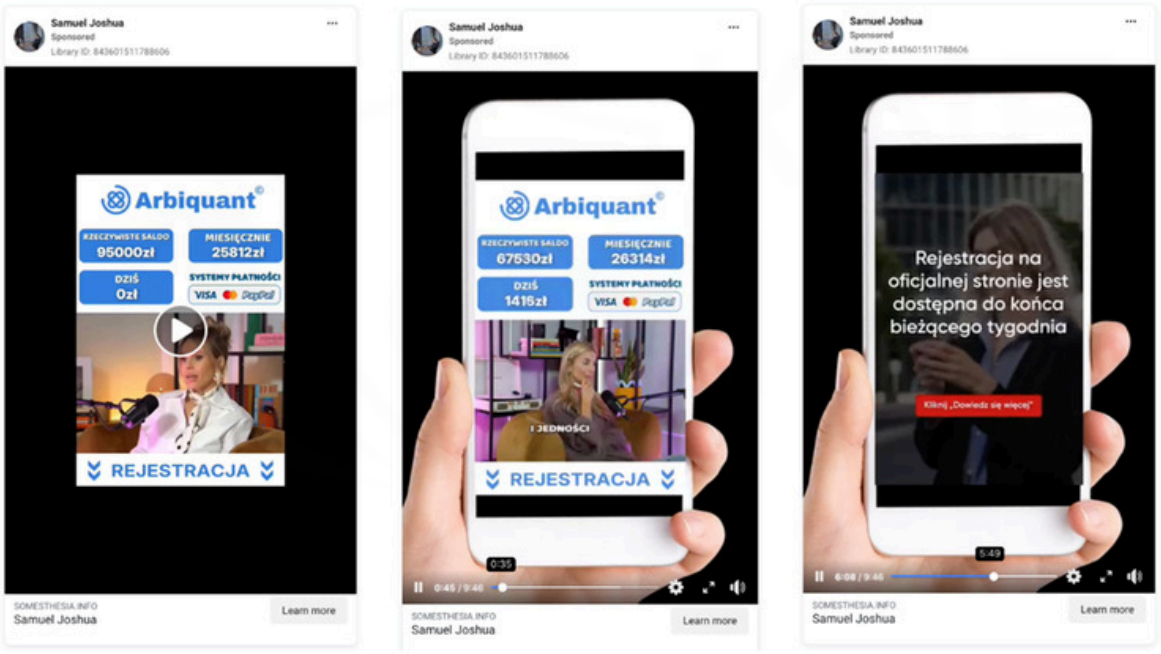
Przestępcy stosują technikę obfuskacji tekstu, polegającą na zastępowaniu liter znakami z innych alfabetów, które wizualnie wyglądają do siebie bardzo podobnie. Dla użytkownika tekst jest czytelny, ale dla algorytmów wyszukiwania stanowi zupełnie inny ciąg znaków. W rezultacie wpisanie w wyszukiwarkę frazy widocznej na ekranie nie zwraca żadnych wyników, ponieważ system wymagałby podania dokładnych, niestandardowych znaków użytych przez oszustów. Nawet drobna podmiana litery sprawia, że reklama staje się „niewidzialna” dla osoby szukającej jej po słowach kluczowych. To sprawia, że ręczne namierzenie źródła ataku jest często niemożliwe bez posiadania bezpośredniego linku do reklamy.



Grafika 19. Przykłady wykorzystania liter z innych alfabetów

Sztuczne wydłużanie długości filmu

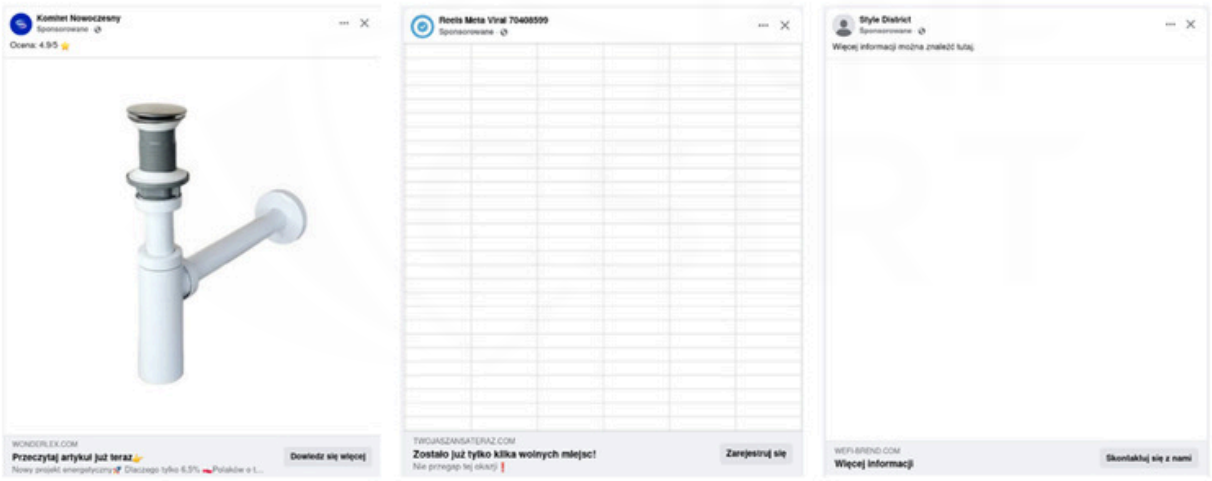
Oszuści czasami zastępują statyczne grafiki materiałami wideo. Stosują przy tym technikę wydłużania treści: właściwy przekaz oszustwa trwa zaledwie 1-2 minuty, podczas gdy cały film jest sztucznie wielokrotnie wydłużany za pomocą czarnego tła lub statycznego obrazu. Takie działanie prawdopodobnie wykorzystuje luki w wydajności algorytmów weryfikacyjnych, które nie analizują dokładnie całego materiału.



Grafika 20. Sztuczne wydłużanie długości filmu

Zaślepki

Stosunkowo częstą taktyką jest stosowanie całkowicie neutralnych grafik (miniatur), które wizualnie nie sugerują żadnego oszustwa. Jest to celowe działanie wymierzone w analityków oraz automatyczne systemy weryfikacji oparte na analizie obrazu. Skoro grafika nie wzbudza podejrzeń, algorytm akceptuje reklamę do publikacji, a analityk może taką reklamę przeoczyć. Złośliwy charakter kampanii ujawnia się dopiero na głębszym poziomie – w treści posta lub po kliknięciu w link przekierowujący, co czyni powierzchowną analizę nieskuteczną.



Grafika 21. Przykładowe zaślepki używane w przestępczych reklamach

Maskowanie złośliwych treści (wersjonowanie, obfuskacja, zaślepki, wydłużanie wideo) to już nie pojedyncze incydenty, tylko element „normalnej” taktyki kampanii nastawionej na omijanie moderacji i utrzymanie aktywnej reklamy jak najdłużej.

2.2 FAŁSZYWE SKLEPY – ROSNĄCE ZAGROŻENIE

Wstęp

Zakupy internetowe są dziś jedną z dominujących form nabywania produktów. Dostępność i wygoda, jaką dają zakupy online sprawiają, że sklepy internetowe są chętnie wybierane przez użytkowników. Jednocześnie rosnąca popularność zakupów online tworzy sprzyjające warunki dla działań przestępczych. W ostatnich latach obserwuje się dużą liczbę stron podszywających się pod legalne sklepy internetowe. Ich głównym celem jest kradzież środków finansowych oraz danych osobowych użytkowników, którzy błędnie uznają je za zaufane źródło zakupów.

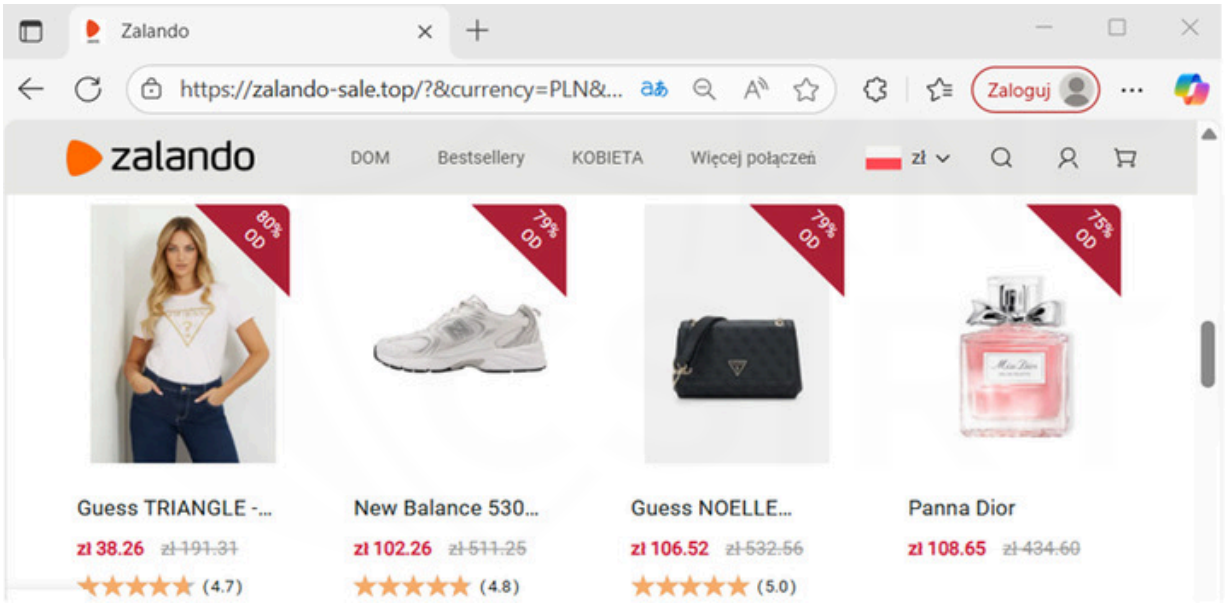
Skala zjawiska

CSIRT KNF w 2025 roku zgłosił do zablokowania 404 domeny fałszywych sklepów internetowych. Przestępcy podszywali się głównie pod rozpoznawalne marki z branży odzieżowej, sportowej oraz wyposażenia wnętrz. Wykorzystując wizerunek liderów rynku e-commerce oszuści tworzyli łudząco podobne witryny, aby pod pretekstem atrakcyjnych wyprzedaży okradać użytkowników.

Charakterystyka ataków

Witryny fałszywych sklepów internetowych prezentują wiele produktów w znacznie obniżonych cenach. Kluczową cechą jest dostępność wszystkich produktów mimo bardzo dużych przecen. Witryny wzorowane są na układzie i stylistyce znanych marek, aby wzbudzić wiarygodność wśród potencjalnych ofiar. By pogłębić to wrażenie oszuści dodają powiadomienia o rzekomo zrealizowanych transakcjach, które są wyświetlane podczas przeglądania produktów.

Techniką często wykorzystywaną przez oszustów jest presja – odliczanie czasu do końca promocji lub informacja o ograniczonej liczbie dostępnych produktów. Techniki te bazują na mechanizmach psychologicznych, które skłaniają użytkowników do szybszego podjęcia decyzji zakupowych, ograniczając ich czujność.

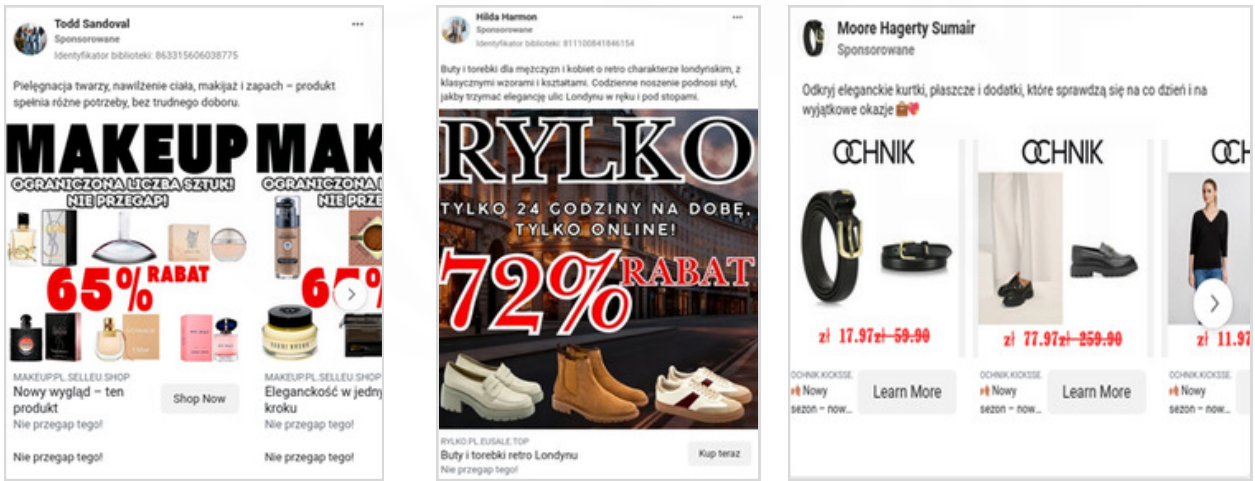


Grafika 22. Fałszywa strona Zalando z przecenionymi produktami

Proces oszustwa

Etap 1: wzbudzenie zainteresowania

Oszustwo zwykle rozpoczyna się od reklamy wyświetlanej w mediach społecznościowych. Reklama wykorzystuje logo znanej marki lub przyciągającą uwagę promocję cenową. Jej zadaniem jest przekierowanie użytkownika na fałszywą stronę sklepu internetowego.



Grafika 23. Fałszywe reklamy na platformie Facebook, w których cyberprzestępcy podszywali się pod znane sklepy

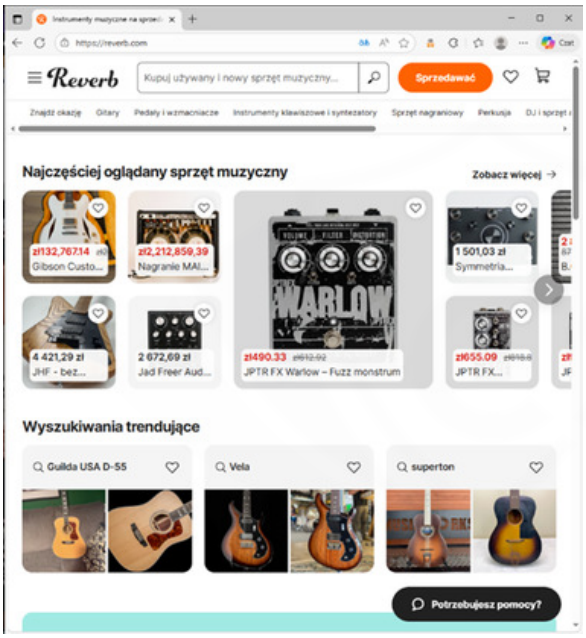
Etap 2: fałszywa strona internetowa

Po przejściu do witryny użytkownik trafia na stronę imitującą wygląd prawdziwego sklepu. Domeny takich stron są tworzone w sposób mający utrudnić ich identyfikację. W ofercie znajdują się liczne, atrakcyjne cenowo produkty, często wzbogacone o dodatkowe mechanizmy promocyjne zachęcające do szybkiego zakupu. Użytkownikom wyświetlane są komunikaty o „ostatnich zakupach innych klientów", które mają sugerować, że na stronie dokonywane są liczne zakupy, a wyeksponowany licznik czasu trwania promocji wywołuje presję na użytkowniku do podjęcia szybkiej decyzji.

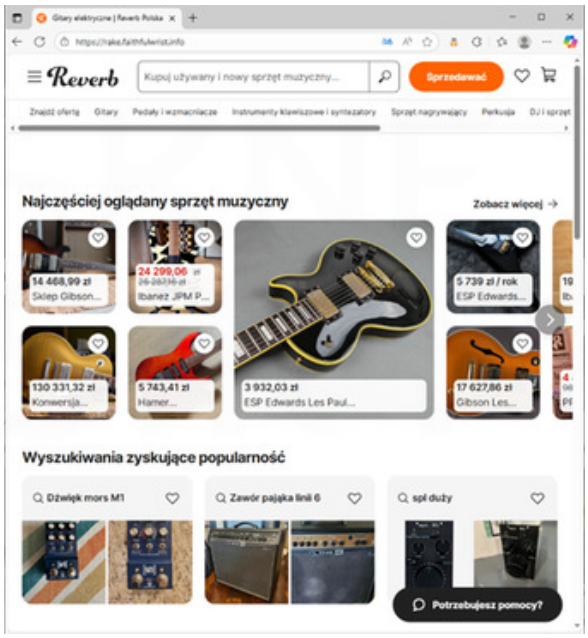
Grafika 24. Licznik czasu promocji

Fałszywe sklepy często bywają wizualnie nie do odróżnienia od ich pierwowzoru. Jedynym elementem pozwalającym odróżnić fałszywy sklep od prawdziwego jest adres domeny, który – choć często zbliżony do oryginału – pozostaje jedyną różnicą możliwą do dostrzeżenia. Przestępcy często wykorzystywali domeny łudząco podobne do prawdziwych domen popularnych marek, licząc na to, że użytkownik nie zauważy subtelnych różnic w składni adresu URL.

Porównanie fałszywej strony sklepu Reverb do jej oryginału:



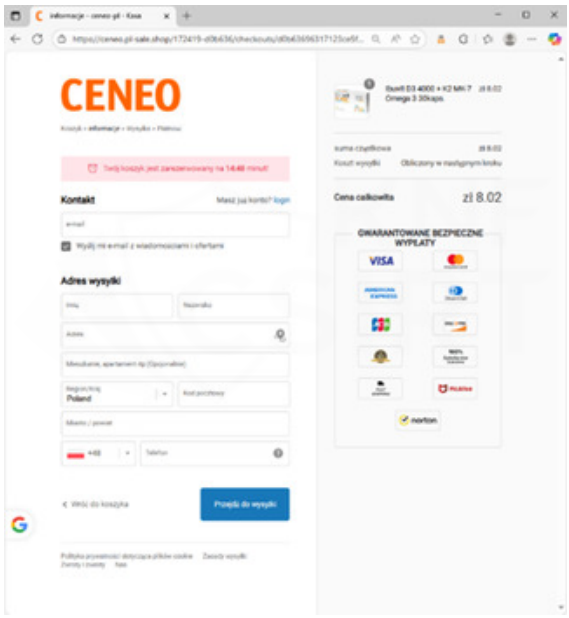
Grafika 25. Prawdziwa strona sklepu Reverb



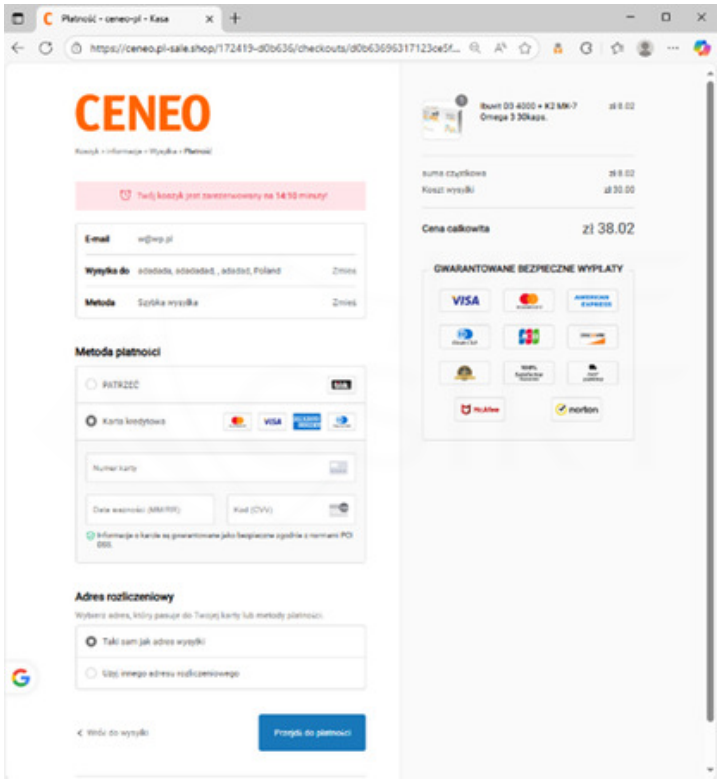
Grafika 26. Fałszywa strona sklepu Reverb

Etap 3: wyłudzanie danych osobowych i kart płatniczych

Po wyborze produktów użytkownik kierowany jest do formularza, w którym proszony jest o podanie danych osobowych, takich jak imię i nazwisko, adres oraz numer telefonu. Następnie strona wymaga wprowadzenia danych karty płatniczej. Po ich wpisaniu może dojść do próby nieautoryzowanej transakcji oraz przechwycenia informacji, które następnie mogą zostać wykorzystane do dalszych przestępstw.



Grafika 27. Fałszywa strona wysyłkowa podszywająca się pod ceneo.pl



Grafika 28. Falszywa strona płatnicza podszywająca się pod ceneo.pl

Rekomendacje dla użytkowników Internetu

- Weryfikuj źródło reklamy w mediach społecznościowych, upewnij się, czy udostępnił ją oficjalny, godny zaufania profil.
- Wyszukaj nazwę firmy w bazie CEIDG lub KRS i upewnij się, że firma w rzeczywistości istnieje.
- Sprawdź regulamin i politykę prywatności pod względem sprzeczności lub błędów, często te dokumenty są bezmyślnie kopiowane przez oszustów i zawierają wiele oczywistych błędów.
- Weryfikuj adresy stron internetowych, czy nie wzbudzają podejrzeń. Wpisz nazwę sklepu w nową kartę przeglądarki i porównaj adresy stron. Wyszukaj adres domeny w bazie whois.com i sprawdź datę utworzenia domeny.
- Zachowaj czujność przy kuszących ofertach, zawsze zwracaj szczególną ostrożność, gdy oferta w Internecie wydaje się zbyt dobra, zwłaszcza jeśli jest ograniczona czasowo.

2.3 OSZUSTWA NA KLIENTÓW BANKOWOŚCI ELEKTRONICZNEJ

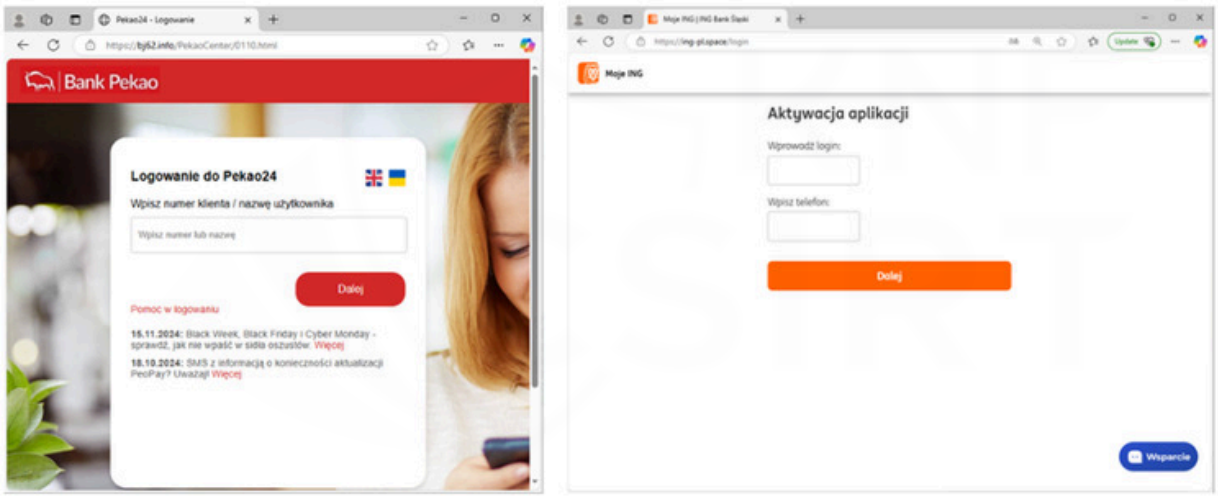
Wśród zidentyfikowanych kampanii phishingowych obecne były również te, w których cyberprzestępcy podszywali się bezpośrednio pod podmioty z rynku finansowego. Tworzyli oni witryny łudząco przypominające oficjalne serwisy bankowe, aby uśpić czujność użytkowników. Celem zazwyczaj była kradzież danych logowania do bankowości elektronicznej.

Skala zjawiska

W 2025 roku CSIRT KNF zgłosił do zablokowania 256 stron powiązanych z oszustwami bankowymi. Choć jest to zaledwie 0,61% wszystkich zgłoszonych domen, stanowią one bardzo poważne zagrożenie dla klientów bankowości elektronicznej. To właśnie one służą do bezpośredniej kradzieży poświadczeń logowania i są ogniwem złożonych ataków socjotechnicznych, prowadząc do bezpośrednich strat finansowych poszkodowanych klientów.

Charakterystyka

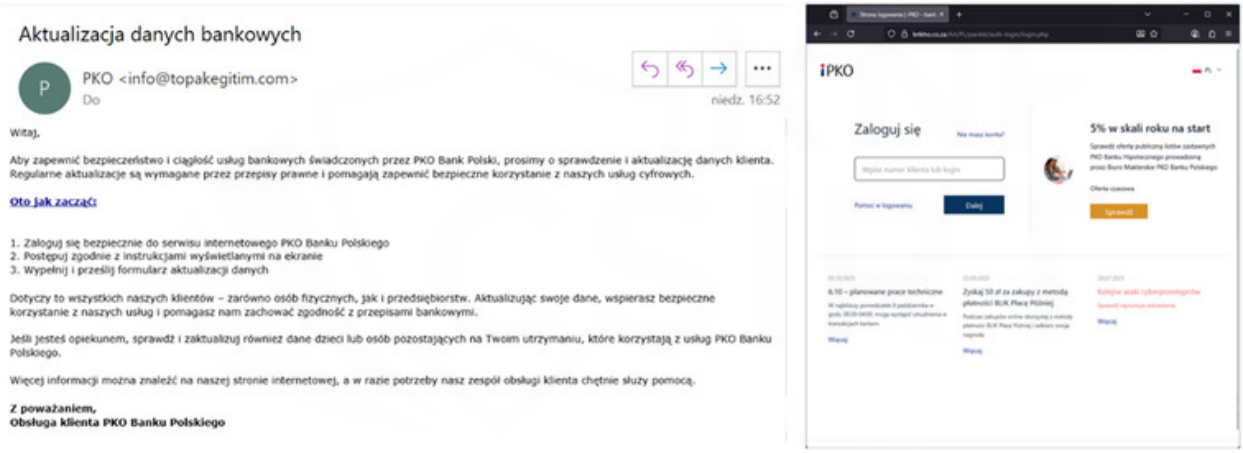
Przestępcy korzystali z wielu metod dystrybucji złośliwych stron. Były to zarówno fałszywe reklamy, jak i wiadomości SMS oraz e-mail. Mechanizm działania polegał na rozsyłaniu komunikatów, które zawierały fałszywą informację, na przykład o rzekomo odrzuconym przelewie z koniecznością pilnej aktualizacji danych, aby ten mógł zostać zrealizowany. W treści wiadomości znajdował się odnośnik, którego kliknięcie prowadziło ofiarę bezpośrednio na stronę phishingową służącą do wyłudzenia poufnych informacji takich, jak loginy i hasła do bankowości elektronicznej lub dane kart płatniczych.



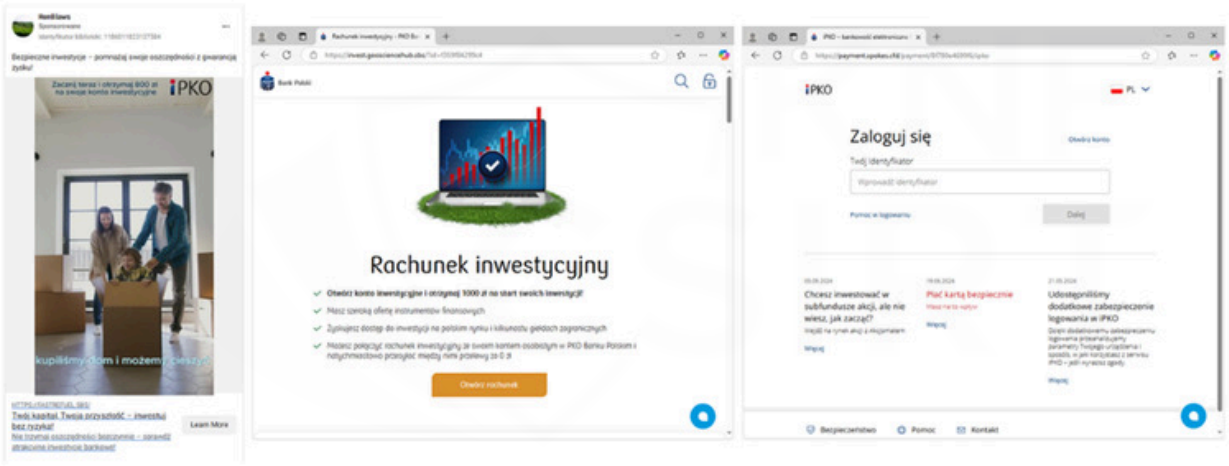
Grafika 29. Przykładowe fałszywe strony logowania do bankowości elektronicznej

Fałszywe wiadomości e-mail

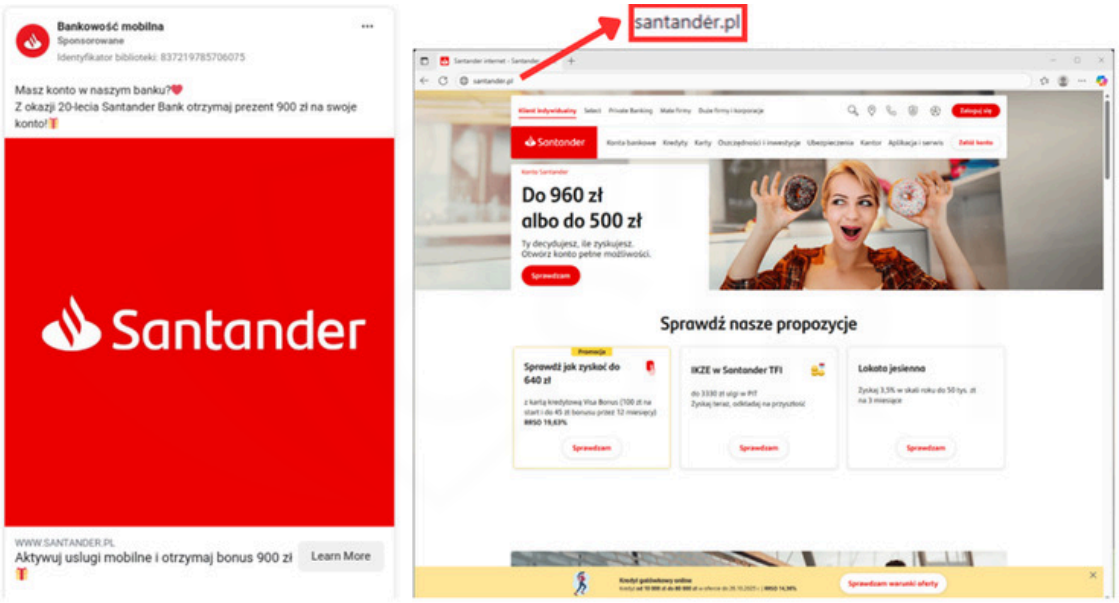
Cyberprzestępcy przesyłali wiadomości e-mail np. informujące o konieczności aktualizacji danych w bankowości elektronicznej. W wiadomości znajdował się link, po kliknięciu w niego ofiara trafiała na stronę phishingową imitującą prawdziwą stronę logowania do bankowości elektronicznej.



Grafika 30. Fałszywa wiadomość e-mail podszywająca się pod PKO Bank Polski oraz niebezpieczna strona wyłudzająca poświadczenia logowania użytkowników



Grafika 31. Fałszywa reklama oraz strona internetowa podszywająca się pod PKO Bank Polski



Grafika 32. Fałszywa reklama oraz strona internetowa podszywająca się pod Santander Bank Polska

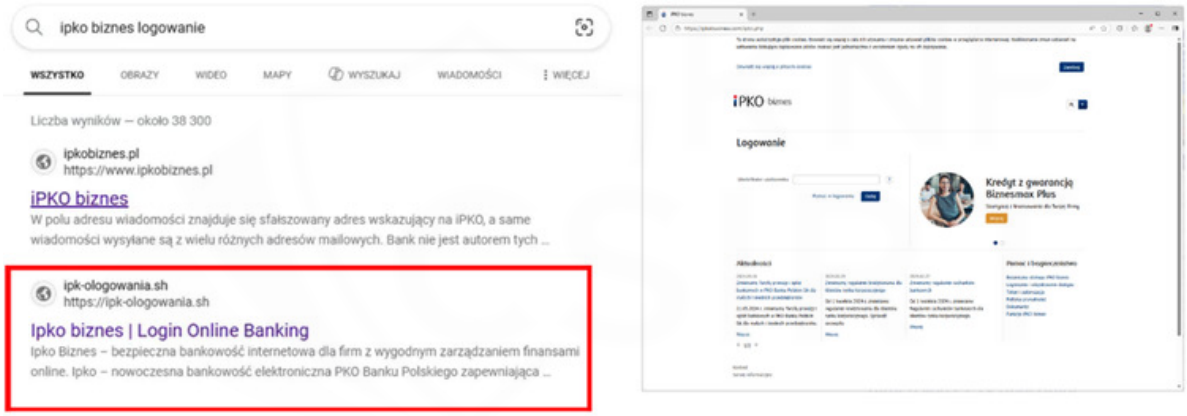
W celu uśpienia czujności użytkowników oszuści w publikowanych reklamach celowo umieszczali prawdziwą domenę banku. Pomimo tego, w rzeczywistości kliknięcie w reklamę przekierowywało ofiarę na fałszywą stronę bankowości elektronicznej. Dodatkowo w tym przypadku przestępcy wykorzystali mechanizm Punycode. Pozwala on na użycie w nazwie domeny znaków z innych alfabetów (np. cyrylicy), które wizualnie są bardzo trudne do odróżnienienia od standardowych liter, sprawiając, że fałszywy adres w pasku przeglądarki wygląda niemal identycznie jak prawdziwy. Na złośliwej witrynie cyberprzestępcy wyłudzali nie tylko poświadczenia logowania, ale także szereg poufnych danych osobowych, w tym między innymi numer PESEL oraz nazwisko panieńskie matki. Dane pozyskane w ten sposób mogły posłużyć im do dalszych przestępstw, na przykład bezprawnej próby wzięcia pożyczki.

Wyszukiwarki

Oprócz wykorzystania reklam w mediach społecznościowych, przestępcy aktywnie posługiwali się również wyszukiwarkami internetowymi do dystrybucji fałszywych stron bankowości elektronicznej.

Mechanizm oszustwa bazuje na założeniu, że część klientów bankowości elektronicznej nie wprowadza adresu URL bezpośrednio w pasek przeglądarki. Cyberprzestępcy wykorzystywali mechanizm pozycjonowania, dzięki czemu ich złośliwa strona wyświetlała się wysoko w wynikach wyszukiwania.

W rezultacie użytkownik klikając w taki link był przekonany, że wchodzi na prawdziwą stronę swojego banku. W rzeczywistości jednak następowało przekierowanie do niebezpiecznej witryny, która stanowiła wizualną kopię oryginalnej strony. Dane wprowadzone na tej fałszywej stronie trafiały bezpośrednio w ręce cyberprzestępców.

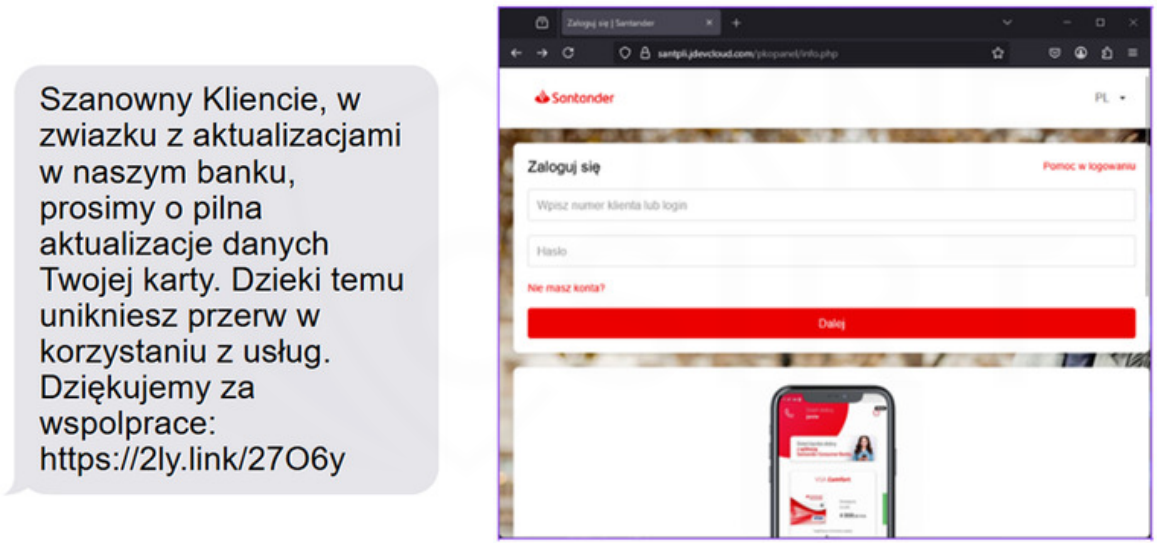


Grafika 33. Fałszywa strona logowania PKO BP w wynikach wyszukiwania

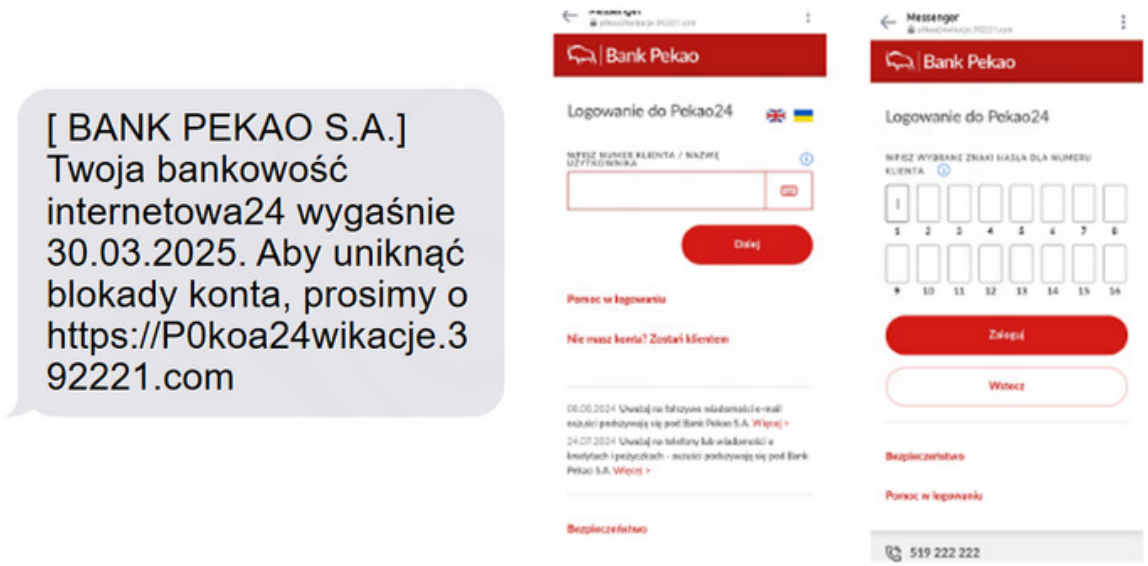
Fałszywe wiadomości SMS

Wśród zidentyfikowanych metod wyłudzeń obecne były również kampanie typu smishing, wykorzystujące fałszywe wiadomości SMS.

Oszuści podszywali się pod wiarygodne instytucje takie, jak banki czy operatorzy usług kurierskich i informowali ofiary o rzekomych nieprawidłowościach, na przykład o konieczności dopłaty do przesyłki lub problemach z kontem w bankowości elektronicznej.

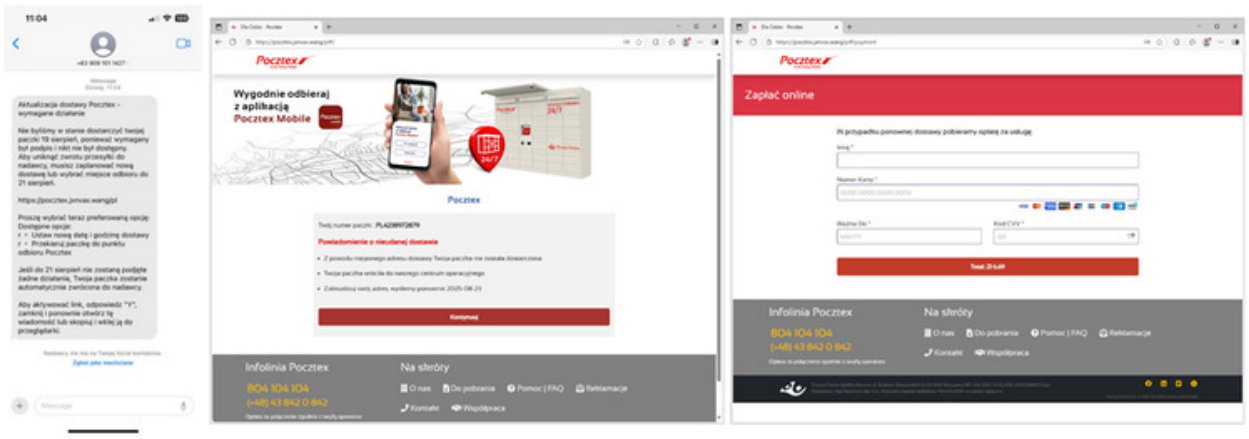


Grafika 34. Wiadomość SMS oraz strona internetowa podszywająca się pod Santander Bank Polska



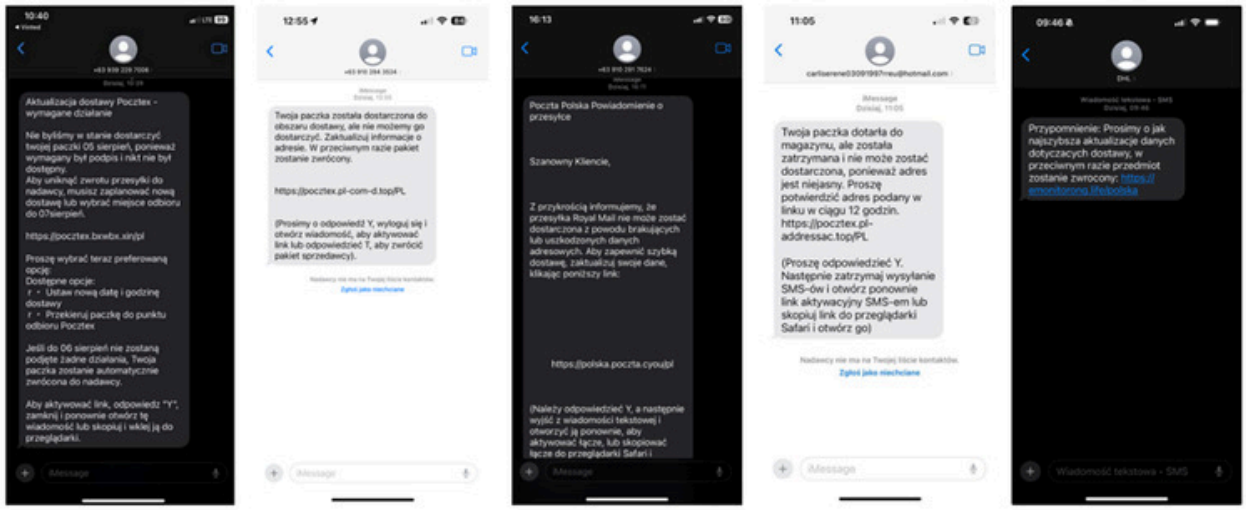
Grafika 35. Fałszywa wiadomość SMS podszywająca się pod Bank Pekao SA

Poza atakami wycelowanymi bezpośrednio w sektor bankowy, istotny odsetek incydentów stanowiły kampanie wykorzystujące wizerunek operatorów usług pocztowych i kurierskich. Scenariusz ataku opierał się na socjotechnice sugerującej konieczność uregulowania rzekomej niedopłaty w celu odblokowania dostawy. Niska kwota roszczenia (zazwyczaj rzędu kilku złotych) miała na celu obniżenie czujności ofiary i skłonienie jej do skorzystania z podstawionej bramki płatności, służącej do wyłudzenia pełnych danych karty płatniczej. Konsekwencją wprowadzenia danych kart płatniczych była realizacja nieautoryzowanych transakcji internetowych na kwoty znacznie przewyższające deklarowaną opłatę.



Grafika 36. Wiadomość SMS wraz ze stroną internetową podszywającą się pod Pocztex

W kampaniach tych wykorzystywano wizerunek wiodących na polskim rynku operatorów logistycznych, m.in. InPost, Poczty Polskiej, DHL czy DPD. W celu uwiarygodnienia ataku przestępcy wykorzystywali często mechanizm SMS Spoofing (fałszowanie identyfikatora nadawcy). Dzięki temu złośliwe wiadomości były automatycznie grupowane przez urządzenia ofiar w jednym wątku z autentycznymi komunikatami od firm przewozowych. Takie działanie mogło zmniejszyć czujność odbiorców.



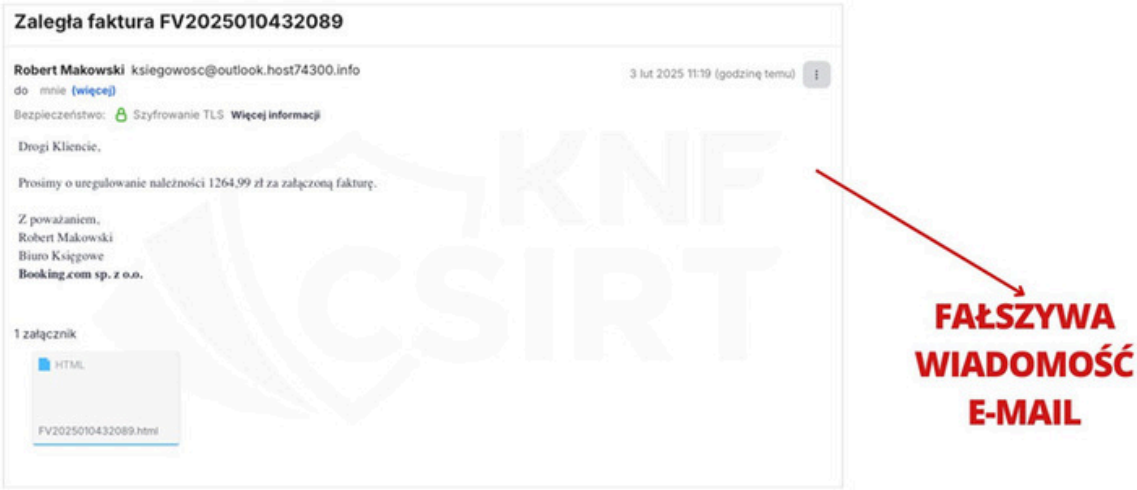
Grafika 37. Przykładowe wiadomości SMS podszywające się pod usługi kurierskie oraz pocztowe

2.4 ZŁOŚLIWE OPROGRAMOWANIE

Jedną z kategorii zagrożeń, na którą narażeni są uczestnicy rynku finansowego, jest złośliwe oprogramowanie. Zespół CSIRT KNF w ramach swojej aktywności prowadzi działania obejmujące m.in. monitorowanie, analizę i wymianę informacji o próbkach i kampaniach malware. Choć w minionym roku skala zjawiska nie była tak wysoka, jak w przypadku phishingu czy oszustw związanych z wykorzystaniem fałszywych inwestycji, zagrożenia z pewnością nie należy lekceważyć.

Rok 2025 pozwolił zaobserwować złośliwe oprogramowanie wymierzone zarówno w użytkowników urządzeń działających pod kontrolą systemu Windows, jak również posiadaczy urządzeń mobilnych funkcjonujących w oparciu o system Android. Malware obecny był w oszustwach podszywających się pod wizerunki podmiotów i produktów z takich obszarów, jak: bankowość, eventy, turystyka czy e-commerce. Poniżej prezentujemy przegląd zagrożeń, o których informowaliśmy w ramach prowadzonych przez CSIRT KNF kanałów w mediach społecznościowych.

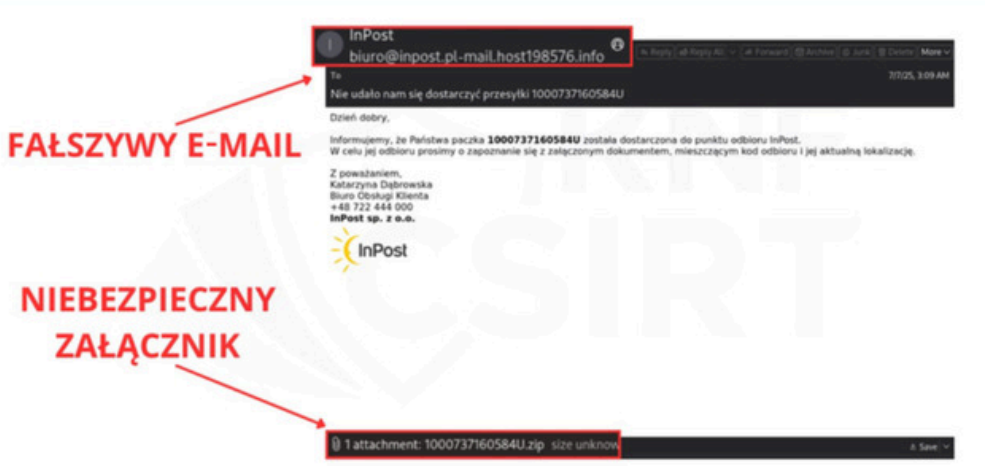
- Kampania e-mail podszywająca się pod Booking, w której atakujący rozsyłali fałszywą wiadomość, informując o konieczności uregulowania płatności za rzekomo załączoną fakturę. W rzeczywistości e-mail zawierał plik w formacie HTML, którego otwarcie skutkowało komunikatem o niemożności wyświetlenia dokumentu oraz kolejnych krokach, jakie powinien podjąć odbiorca wiadomości. Realizacja instrukcji mogła skutkować zainfekowaniem urządzenia ofiary szkodliwym oprogramowaniem[2].



Grafika 38. Wiadomość e-mail podszywająca się pod Booking

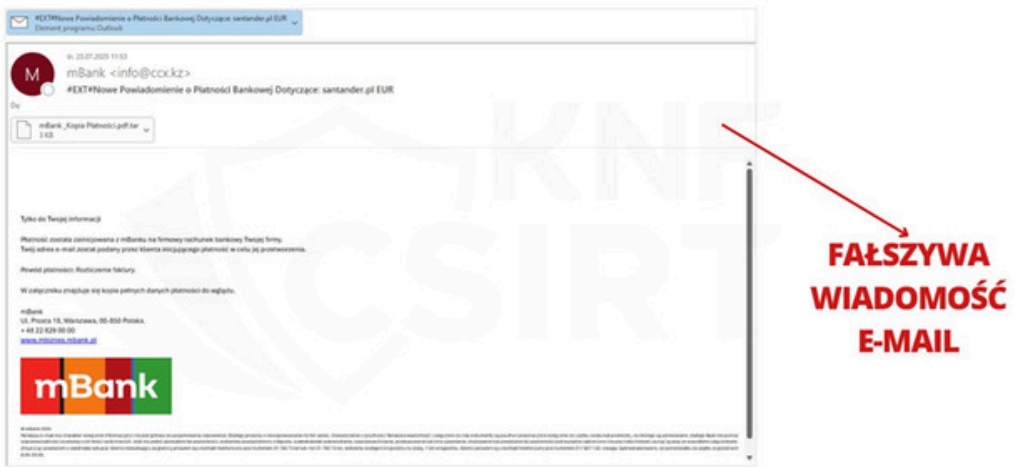
[2] https://x.com/CSIRT_KNF/status/1886417315983470664

- Kampania podszywająca się pod InPost, w której oszuści wykorzystując wiadomość e-mail informowali odbiorcę o oczekującej przesyłce. Odbiór paczki miał wiązać się z koniecznością otwarcia dokumentu zawierającego jej lokalizację oraz kod odbioru. Załączone archiwum zawierało złośliwe oprogramowanie mogące przejąć dane logowania i inne wrażliwe informacje[3].



Grafika 39. Wiadomość e-mail podszywająca się pod firmę InPost

- Kampania, w której atakujący podszywali się pod mBank przesyłając wiadomość o pozorowanej transakcji związanej z rozliczeniem faktury. Szczegółowe informacje na temat danych płatności miały znajdować się w załączniku – złośliwym archiwum TAR, które ze względu na podwójne rozszerzenie mogło być mylnie interpretowane jako dokument PDF[4].

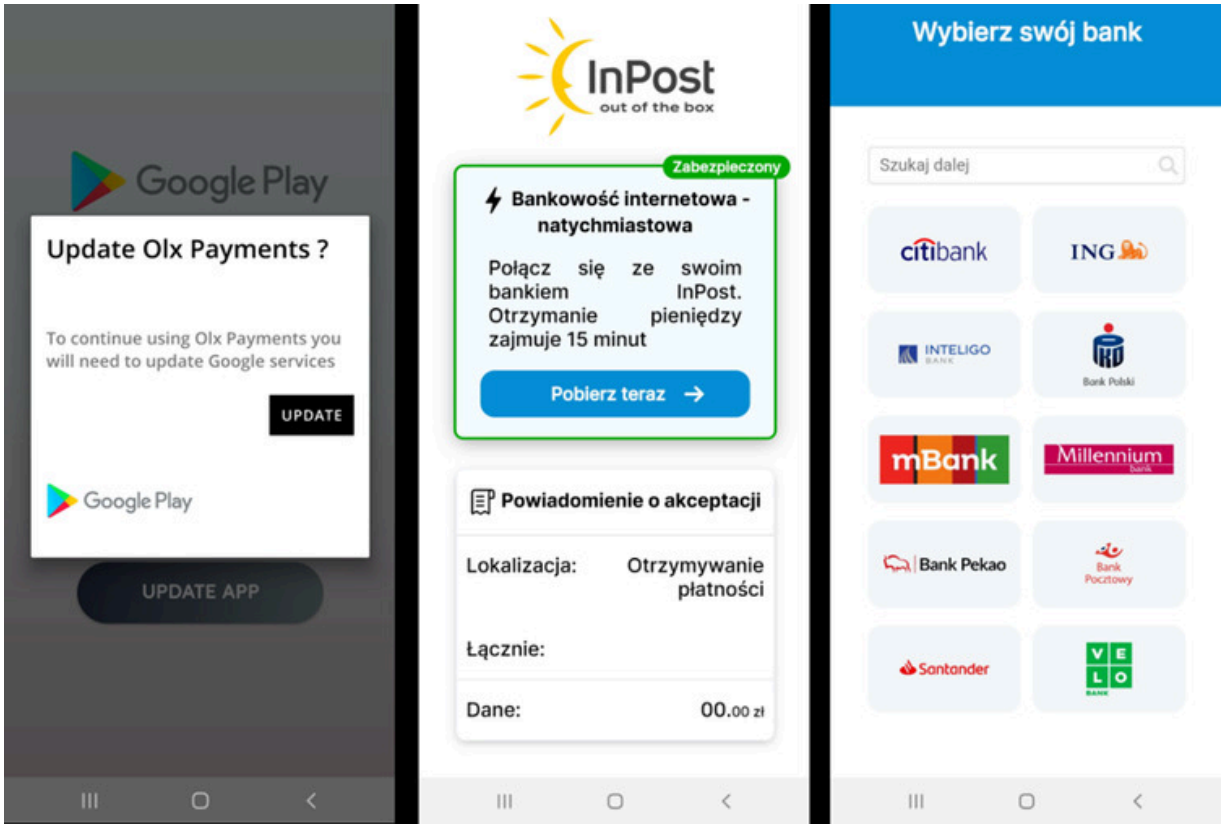


Grafika 40. Wiadomość e-mail podszywająca się pod mBank

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

Osobną podkategorię obserwowanych zagrożeń stanowił malware mobilny, gdzie atakujący w zauważalnym stopniu koncentrowali się na użytkownikach systemu Android. Analizowane przez nas złośliwe oprogramowanie z tego obszaru obejmowało następujące przypadki:

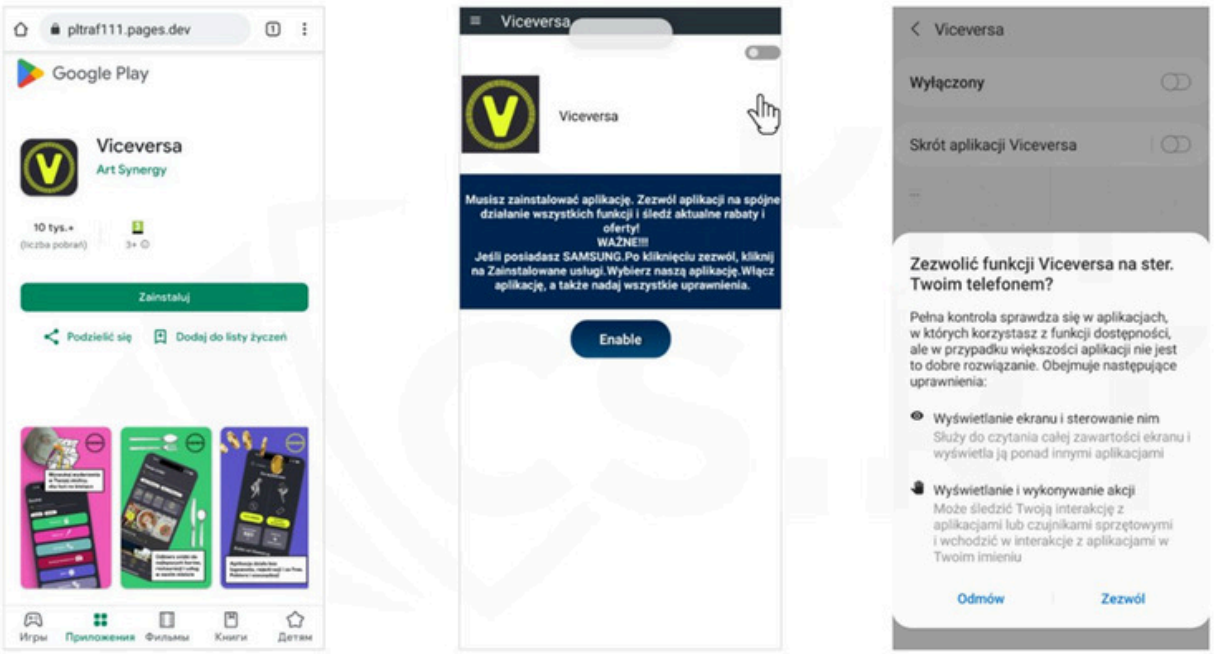
- W styczniu 2025 roku ostrzegaliśmy przed fałszywą aplikacją o nazwie OLX Payments. Proces infekcji przebiegał tu etapowo. Uruchomienie malware skutkowało wyświetleniem komunikatu o rzekomej potrzebie aktualizacji Google Services mającej umożliwić dalsze korzystanie z aplikacji. W przypadku instalacji i uruchomienia pakietu z kolejnej fazy infekcji, ofiara była instruowana odnośnie przydzielenia uprawnień związanych z funkcją Ułatwień Dostępu (ang. Accessibility Services), to z kolei mogło skutkować przejęciem kontroli nad urządzeniem. W kolejnych krokach oszukańcza aplikacja podszywała się pod markę InPost i prowadziła do wyświetlenia fałszywych formularzy logowania do bankowości elektronicznej[5].



Grafika 41. Ekran fałszywej aplikacji OLX Payments

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

- Pod koniec marca obserwowaliśmy podszycie pod aplikację Viceversa. W opisywanym przypadku mieliśmy do czynienia z imitującą Google Play fałszywą stroną internetową, za pomocą której odbywała się dystrybucja malware. Wizyta na stronie umożliwiała pobranie na urządzenie niezaufanego pliku APK. W wyniku uruchomienia oszukańczej aplikacji i przejścia przez kolejne kroki, ofiara mogła aktywować systemową funkcję Ułatwień Dostępu i potencjalnie przekazać kontrolę nad urządzeniem złośliwemu oprogramowaniu[6].

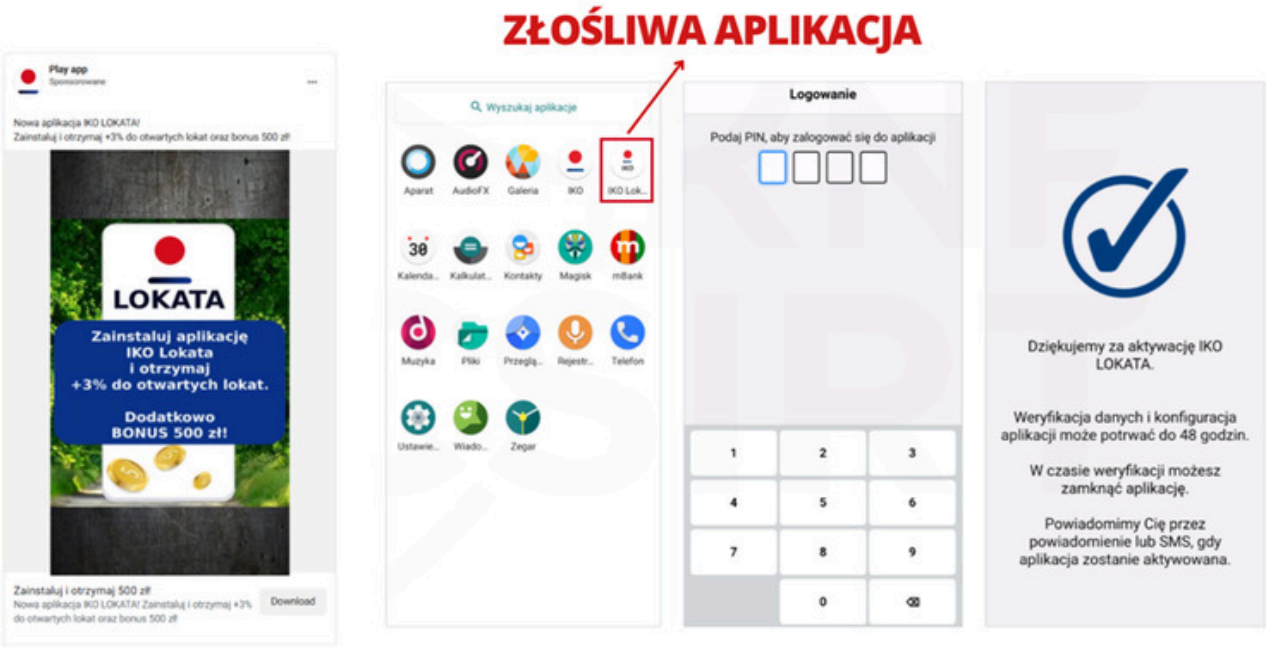


Grafika 42. Strona dystrybuująca i ekrany fałszywej aplikacji Viceversa

- Końcówka maja 2025 to czas w którym informowaliśmy o złośliwym oprogramowaniu podszywającym się pod nieistniejącą aplikację IKO Lokata. Próbka malware, na podstawie której przeprowadziliśmy badanie, została przez nas pobrana w ramach jednego z serwisów analitycznych. W podobnym czasie obserwowaliśmy na platformie Facebook złośliwe reklamy, które swoją stylistyką przypominały analizowaną aplikację. W trakcie badania adresy, pod które prowadziły oszukańcze reklamy, nie zaserwowały nam jednak analizowanej próbki malware. W warstwie wizualnej malware nawiązywał nieco stylistyką do aplikacji mobilnej IKO.

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

Od strony funkcjonalnej, po uruchomieniu, wyświetlane było okno informujące o dostępności nowej wersji aplikacji z zachętą do aktualizacji. Miała ona wpłynąć na płynne działanie programu. Przejście ofiary przez kolejne kroki – instalację dodatkowego modułu oraz aktywację funkcji Dostępności, mogło w sposób popularny dla androidowego malware narazić ją na dalszy proces infekcji. Analizowane artefakty wskazywały, że mogliśmy mieć do czynienia ze złośliwym oprogramowaniem z rodziny Crocodilus[7],[8]. Więcej szczegółów dotyczących złośliwej próbki opublikowaliśmy w artykule „Analiza złośliwej aplikacji mobilnej IKO Lokata”[9].



Grafika 43. Reklama w mediach społecznościowych i ekrany fałszywej aplikacji IKO Lokata

W przestrzeni mobilnego malware, ukierunkowanego na posiadaczy urządzeń z Androidem, obserwowaliśmy nowy model ataku wykorzystujący tzw. NFC Relay. Wzmianki o złośliwym zastosowaniu tego podejścia mogliśmy zauważyć już w 2024 roku u naszych południowych sąsiadów, gdzie w jednej ze swoich analiz przedstawili ją badacze z firmy ESET. Użycie złośliwego oprogramowania miało tam umożliwić przekazanie danych NFC zapisanych na karcie ofiary, za pośrednictwem zainfekowanego telefonu do urządzenia atakującego.

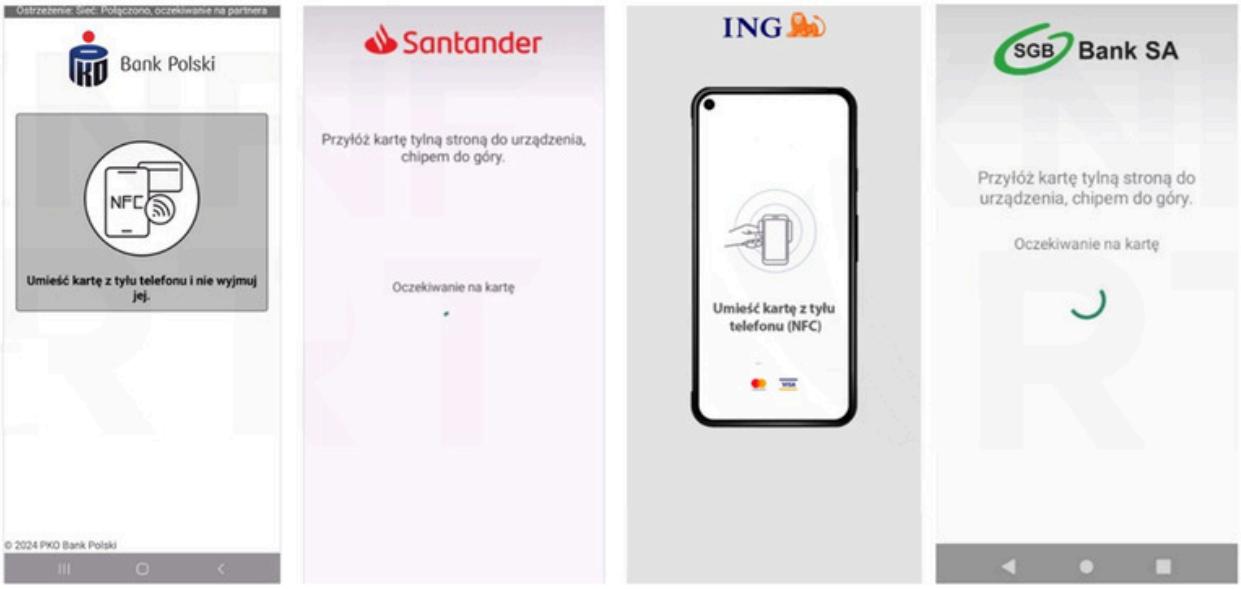
[7] https://www.threatfabric.com/blogs/exposing-crocodilus-new-device-takeover-malware-targeting-android-devices
[8] https://x.com/naumovax/status/1906727042353107402
[9] https://cebrf.knf.gov.pl/images/IKO%20Lokata%20Malware%20-%20Analiza.pdf

Tak pozyskane dane oszuści mogli próbować wykorzystać np. do zbliżeniowej wypłaty środków z bankomatu (równolegle próbując wyłudzić kod PIN do karty ofiary) lub realizacji płatności bezstykowej przy terminalu płatniczym. Warto zauważyć, że opisywana przez ESET technika NFC Relay opiera się o legalne rozwiązanie badawcze NFCGate[10], którego funkcjonalność została nadużyta przez atakujących[11].

W 2025 roku o oszustwach z motywem NFC Relay w tle informowaliśmy kilkukrotnie. Wspólnym mianownikiem opisywanych przypadków były fałszywe aplikacje imitujące rozwiązania bankowe (obserwowaliśmy podszycia pod PKO BP, Santander, ING oraz SGB Bank SA). Uruchomione aplikacje wnioskowały o umiejscowienie karty (w domyśle karty płatniczej) w tylnej części urządzenia. Przynajmniej w jednym przypadku zaobserwowaliśmy komunikację wychodzącą po przyłożeniu testowej karty RFID (nie udało nam się potwierdzić, czy operacja powiodłaby się w przypadku karty płatniczej oraz czy przesyłane dane okazałyby się wystarczające do wypłaty środków), a w części przypadków, po spełnieniu odpowiednich warunków, okno imitujące tzw. „PIN pad".

Rozpowszechnianie złośliwego oprogramowania każdorazowo odbywało się z pominięciem Google Play i zakładało instalację aplikacji z tzw. niezaufanego źródła (obserwowaliśmy np. dystrybucję pakietów przy użyciu serwisu hostingowego files.fm)[12],[13],[14],[15],[16]. Z uwagi na rosnącą popularność tego modelu oszustwa, uwzględniliśmy go w trendach cyberprzestępczości 2025 roku opisując dodatkowo w dokumencie „Krajobraz cyberzagrożeń w polskim sektorze finansowym 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



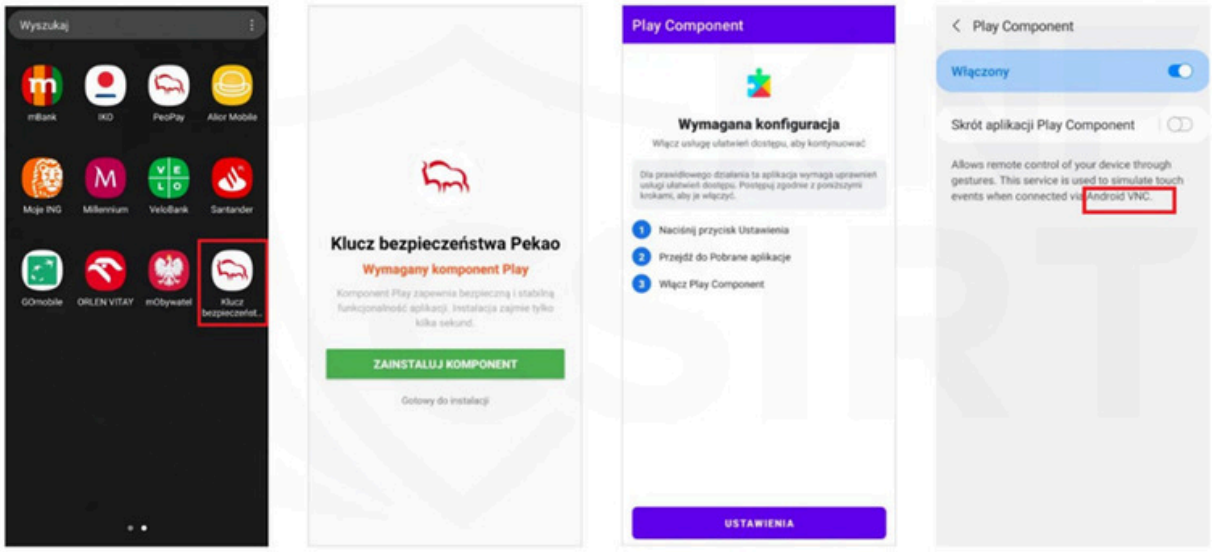
Grafika 44. Użycie logotypów banków w fałszywych aplikacjach wykorzystujących NFC

```
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);
    }
```

Grafika 45. Zdekompilowany fragment jednej z próbek – widoczne zastosowanie w fałszywej aplikacji – wykorzystanie kodu pochodzącego z projektu badawczego NFCGate [18]

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

- W pierwszej połowie grudnia pisaliśmy o fałszywej aplikacji mobilnej pod nazwą „Klucz bezpieczeństwa Pekao". Jej uruchomienie skutkowało wyświetleniem ekranu informującego o wymaganym „komponencie Play", mającym rzekomo zapewnić stabilną i bezpieczną funkcjonalność aplikacji. W rzeczywistości instalacja komponentu prowadziła do wyświetlenia kolejnego ekranu, który pod pozorem wymaganej konfiguracji zachęcał do przydzielenia zainstalowanej aplikacji uprawnień do funkcji „ułatwień dostępu". To z kolei mogło prowadzić do przejęcia kontroli nad urządzeniem[19]. Przeprowadzona przez nas analiza instalowanego pakietu „Play Component" wykazała tożsamy „certificate fingerprint", względem certyfikatu zastosowanego w payloadzie trojana FvncBot opisanego w pierwszej połowie grudnia przez Intel471[20].

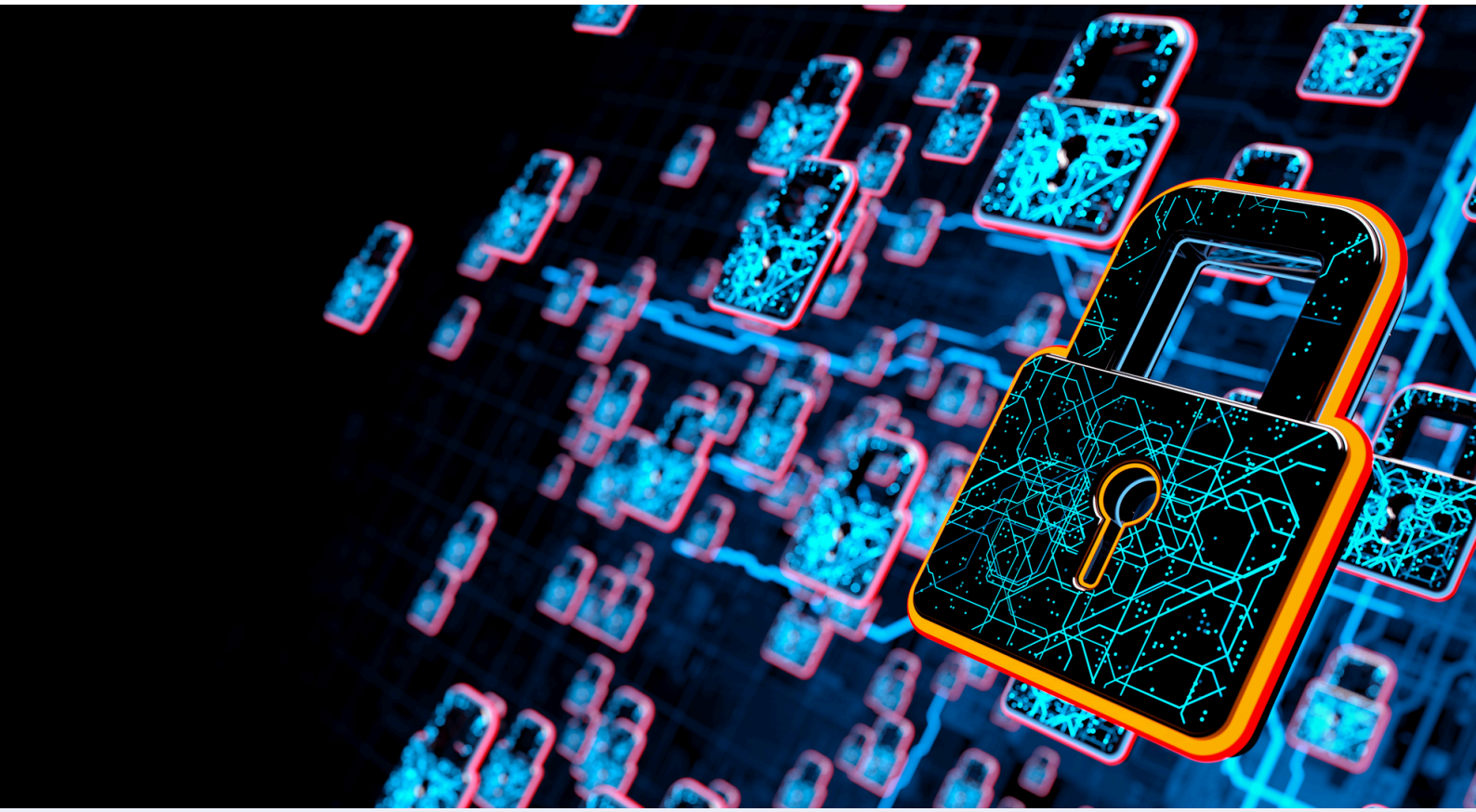


Grafika 46. Fałszywa aplikacja mobilna Klucz bezpieczeństwa Pekao

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

03. BEZPIECZEŃSTWO PODMIOTÓW RYNKU FINANSOWEGO

3.1 CYBER THREAT INTELLIGENCE (CTI) – OD REAGOWANIA DO PRZEWIDYWANIA



Ewolucja podejścia do zagrożeń

CSIRT KNF działa w oparciu o podejście, które stawia na przewidywanie zagrożeń, a nie tylko reagowanie na te już widoczne. Skupiamy się na wychwytywaniu wczesnych sygnałów mogących świadczyć o przygotowywanych kampaniach i analizujemy je pod kątem możliwego wpływu na polski rynek finansowy. Dzięki temu możemy wcześniej ostrzegać instytucje o nadchodzących działaniach przestępczych i wspierać je w przygotowaniu się zanim dojdzie do realnych incydentów.

CSIRT KNF stale obserwuje różnorodne źródła OSINT, zarówno te jawne, jak i trudno dostępne. Zbieramy informacje z serwisów publikujących dane o wyciekach, z monitoringu rejestracji nowych domen, z mediów społecznościowych, forów przestępczych, a także z kanałów komunikacyjnych, w których pojawiają się zapowiedzi kampanii lub technik wykorzystywanych przez cyberprzestępców. Wyciągamy z tego dane, które są istotne z punktu widzenia polskiego rynku finansowego i regularnie przekazujemy je instytucjom, aby wspierać je w ocenie ryzyka, wykrywaniu wczesnych sygnałów ataków i wdrażaniu odpowiednich zabezpieczeń.

Monitoring grup ransomware i analiza wycieków

W ramach działań CTI zespół CSIRT KNF prowadzi ciągły monitoring aktywności grup ransomware na poziomie globalnym. Szczególną uwagę poświęcamy analizie danych z wycieków publikowanych przez te grupy. Sprawdzamy każdy przypadek pod kątem potencjalnego wpływu na łańcuch dostaw polskiego rynku finansowego.

Analizujemy:

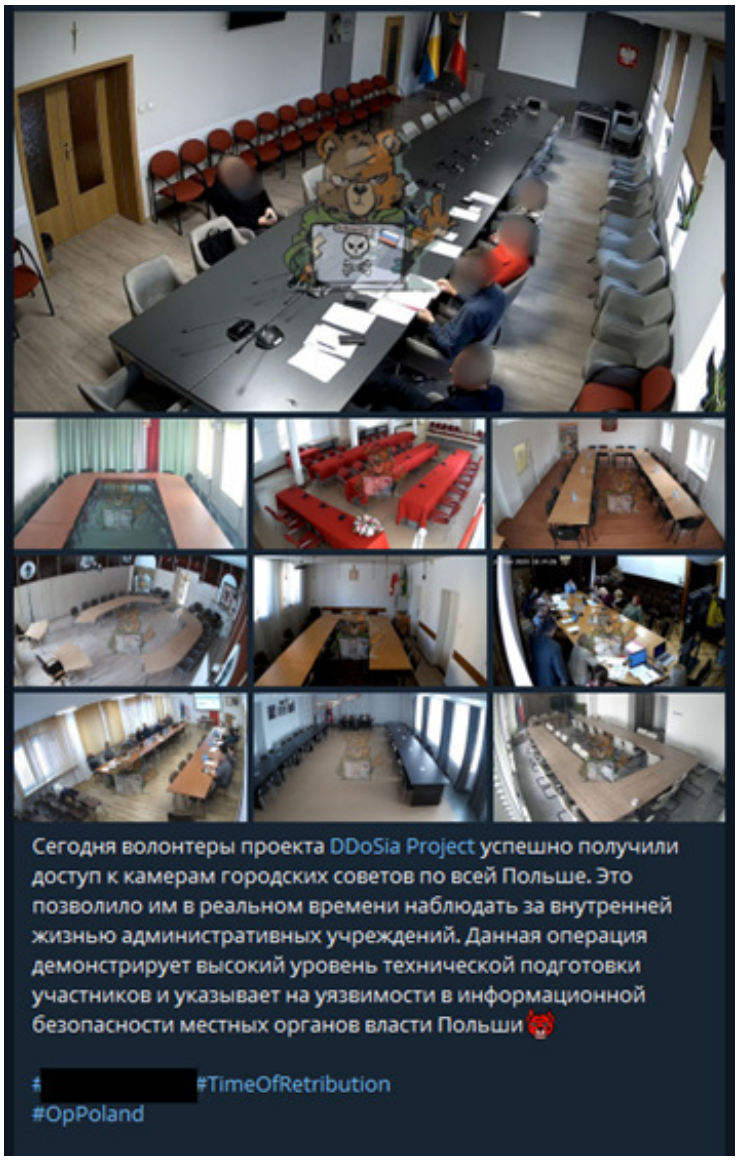
- publikowane dane z ataków ransomware na poziomie światowym
- potencjalne powiązania ofiar z polskim rynkiem finansowym
- ryzyko dla łańcuchów dostaw podmiotów nadzorowanych
- podatności i wektory ataków wykorzystywane przez grupy przestępcze

Dodatkowo w 2025 roku zwracaliśmy uwagę na ataki wymierzone w sklepy online oraz inne serwisy internetowe, bo część z nich mogła pośrednio wpływać także na klientów usług finansowych. W tych sprawach współpracowaliśmy z CERT Polska, przekazując zebrane informacje i analizując charakter incydentów. Zebrane informacje przekazaliśmy dalej i ostatecznie zostały udostępnione w serwisie bezpiecznedane.gov.pl. Dzięki temu mogą z nich korzystać zarówno instytucje, jak i osoby, które chcą sprawdzić, czy ich dane mogły pojawić się wśród materiałów ujawnionych podczas takich ataków.

Monitoring grup haktywistycznych

Rok 2025 to również czas wzmożonej aktywności grup haktywistycznych, w dużej mierze powiązanej z sytuacją geopolityczną w regionie. CSIRT KNF prowadzi bieżący monitoring tych grup, analizując ich deklarowane cele, metody działania i potencjalne zagrożenia dla polskiego sektora finansowego. Obserwujemy komunikację na forach, w kanałach Telegram i innych miejscach, gdzie grupy te publikują informacje o planowanych działaniach.

Warto przy tym zauważyć, że deklaracje grup haktywistycznych często nie odpowiadają rzeczywistej skali ich działań. Część publikowanych „sukcesów" to w rzeczywistości informacje i dane pochodzące z publicznie dostępnych zasobów, takich jak otwarte transmisje z kamer miejskich czy publiczne serwisy streamingowe. Grupy te prezentują takie działania jako poważne operacje hakerskie, podczas gdy w praktyce nie doszło do żadnego włamania ani kompromitacji systemów. Umiejętność odróżnienia rzeczywistego zagrożenia od propagandowego szumu jest istotną częścią pracy analitycznej CTI.



Grafika 47. Informacja opublikowana przez grupę cyberprzestępczą w serwisie Telegram

W przypadku wykrycia zagrożenia wymierzonego w polski rynek finansowy, informujemy podmioty o potencjalnym ataku jeszcze przed jego rozpoczęciem. Takie wczesne ostrzeżenia pozwalają instytucjom na wzmocnienie zabezpieczeń i przygotowanie się do obrony.

Oprócz samego monitoringu i ostrzegania, CSIRT KNF prowadzi platformę umożliwiającą podmiotom rynku finansowego wspólną wymianę wskaźników kompromitacji (IOC). Dzięki niej instytucje mogą w czasie rzeczywistym dzielić się informacjami o zaobserwowanych zagrożeniach, co pozwala całemu sektorowi szybciej reagować na nowe kampanie. Zapewniamy również kanał wymiany doświadczeń między podmiotami, który umożliwia dzielenie się wiedzą o skutecznych metodach obrony i lessons learned z incydentów.

Odporność polskiego rynku finansowego

Warto podkreślić istotny fakt: w 2025 roku nie odnotowaliśmy przypadku udanego ataku ransomware bezpośrednio na polski podmiot z rynku finansowego. To znaczący sukces, który świadczy o wysokim poziomie dojrzałości cyberbezpieczeństwa w tym sektorze. Polskie banki, domy maklerskie i inne instytucje finansowe skutecznie zabezpieczają swoją infrastrukturę przed tego typu zagrożeniami.

Zagrożenia w łańcuchu dostaw

Choć bezpośrednie ataki na rynek finansowy są rzadkie, zaobserwowaliśmy wzrost liczby incydentów dotyczących łańcuchów dostaw. Przestępcy coraz częściej atakują dostawców technologii, usług IT czy oprogramowania wykorzystywanego przez instytucje finansowe. Taki pośredni wektor ataku może prowadzić do poważnych konsekwencji dla bezpieczeństwa końcowych użytkowników usług finansowych.

W 2025 roku monitorowaliśmy przypadki ataków na:

- dostawców oprogramowania wykorzystywanego w sektorze finansowym
- firmy świadczące usługi IT dla banków i innych instytucji finansowych
- podmioty odpowiedzialne za usługi wspierające funkcjonowanie instytucji finansowych

W każdym takim przypadku przeprowadzaliśmy analizę ryzyka dla polskiego rynku i gdy było to konieczne, informowaliśmy odpowiednie podmioty o potencjalnych zagrożeniach.

Proaktywna współpraca z rynkiem

Dzięki proaktywnemu podejściu możemy ostrzegać podmioty rynku finansowego o zagrożeniach jeszcze zanim dojdzie do realnych ataków. Zamiast reagować na incydenty po fakcie, skupiamy się na przewidywaniu działań przestępców i wspieraniu instytucji w zapobieganiu problemom. Wczesne ostrzeganie ma duże znaczenie dla całego sektora. Informacje przekazane z wyprzedzeniem pozwalają szybciej wdrożyć poprawki, zablokować nowe domeny wykorzystywane w kampaniach albo po prostu zwiększyć czujność w miejscach, w których może pojawić się ryzyko. Często właśnie to zatrzymuje zagrożenie na etapie przygotowań.

Gdy wykrywamy nowe schematy oszustw lub metody ataków, które mogą mieć wpływ na sektor finansowy, informujemy o nich podmioty, nawet jeśli nie odnotowaliśmy jeszcze takich incydentów w Polsce. Regularnie wydajemy rekomendacje i ostrzeżenia dotyczące nowych zagrożeń, zanim te zdążą dotrzeć do polskich instytucji.

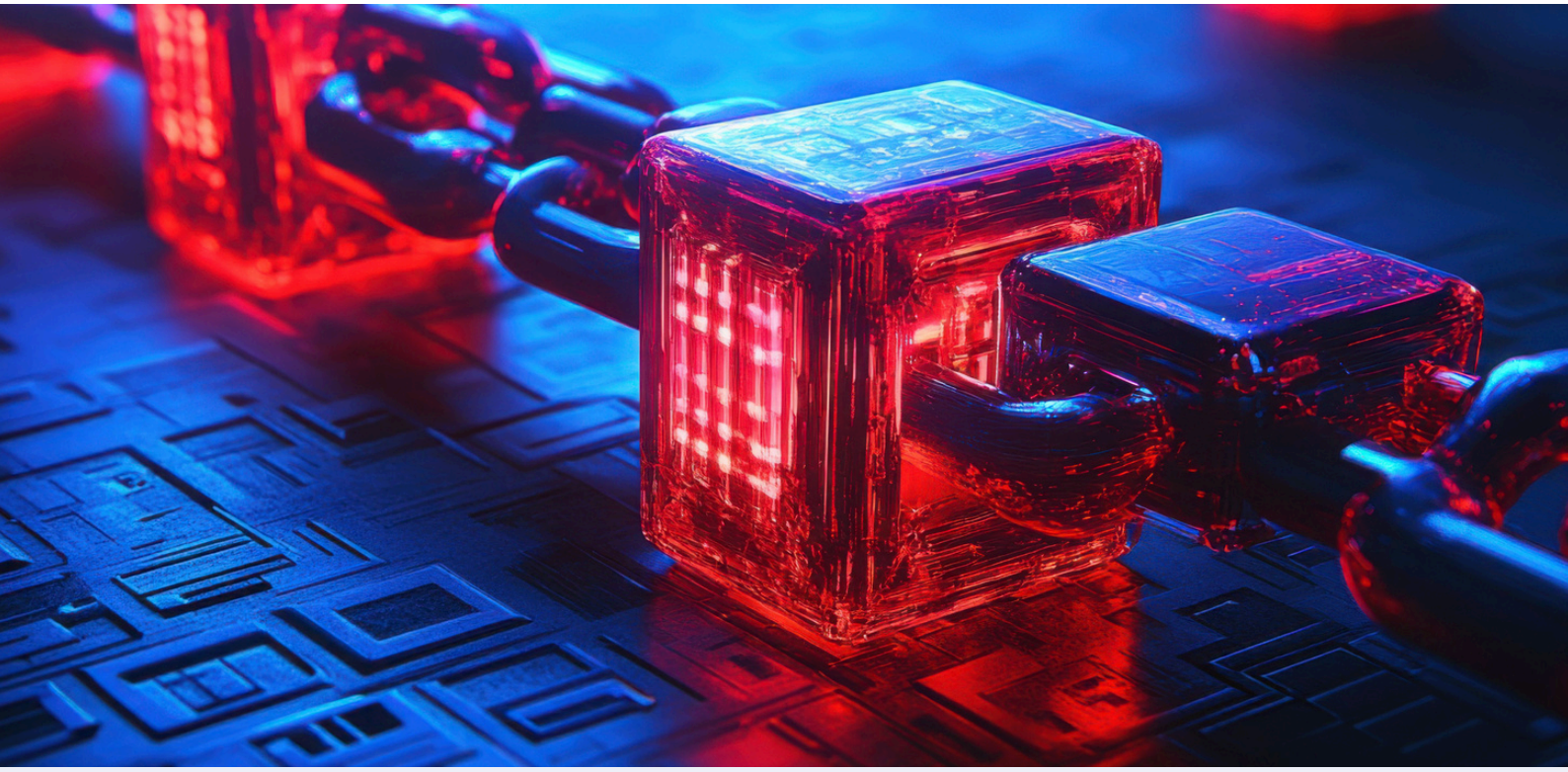
Jednym z przykładów takiej proaktywnej działalności w 2025 roku było ostrzeżenie o kampanii grup APT powiązanych z Koreą Północną, wymierzonej w działy IT i HR instytucji finansowych. Atakujący kradną tożsamość realnych osób i wykorzystują ją do aplikowania na stanowiska techniczne, wysyłając fałszywe CV. Celem jest uzyskanie zatrudnienia lub przynajmniej dostępu do wewnętrznych systemów na etapie rekrutacji. Choć nie odnotowaliśmy przypadku udanego ataku tego typu na polski sektor finansowy, prewencyjnie ostrzegliśmy instytucje o zagrożeniu i wydaliśmy rekomendacje mające na celu zwrócenie uwagi działów HR na ten schemat oszustwa oraz wskazówki dotyczące weryfikacji tożsamości kandydatów.

To jeden z wielu przypadków, w których działamy wyprzedzająco – analizujemy globalne trendy i incydenty, oceniamy ich potencjalny wpływ na polski rynek finansowy i przekazujemy instytucjom konkretne informacje zanim zagrożenie stanie się dla nich realne.

Ważną rolę odgrywa tu także wymiana informacji z innymi zespołami CERT, zarówno sektorowymi, jak i krajowymi. Pozwala to lepiej rozumieć powiązania między incydentami w różnych częściach gospodarki i szybciej ocenić, czy dany sygnał może wpływać na instytucje finansowe. Taka współpraca działa w obie strony – przekazujemy swoje obserwacje, ale też korzystamy z wiedzy innych zespołów, co wzmacnia odporność całego ekosystemu.

To podejście wymaga ciągłej analizy wielu źródeł, śledzenia aktywności przestępczej na forach undergroundowych i szybkiego reagowania na nietypowe sygnały. To intensywna praca, ale jej efekty są bardzo konkretne – bezpieczniejszy rynek finansowy.

3.2 ATAKI DDOS NA RYNEK FINANSOWY



Charakter zagrożenia

Ataki DDoS (Distributed Denial of Service) od lat stanowią jedno z najczęstszych zagrożeń dla sektora finansowego na całym świecie. Ich celem jest przeciążenie infrastruktury ofiary ogromną ilością ruchu sieciowego, co może prowadzić do niedostępności usług dla klientów. Dla banków, domów maklerskich czy systemów płatności nawet krótkotrwała przerwa w działaniu oznacza nie tylko straty finansowe, ale też utratę zaufania klientów.

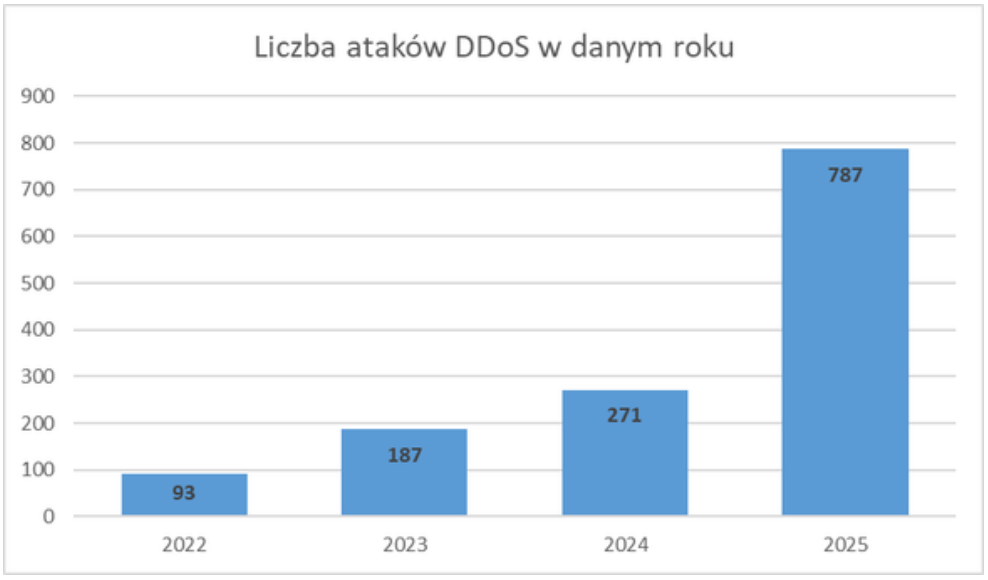
Rynek finansowy jest atrakcyjnym celem z kilku powodów. Po pierwsze, instytucje finansowe muszą zapewniać ciągłość działania – klienci oczekują dostępu do swoich środków i usług bez przerwy. Po drugie, ataki na banki przyciągają uwagę mediów, co jest szczególnie istotne dla grup haktywistycznych szukających rozgłosu. Po trzecie, w kontekście obecnej sytuacji geopolitycznej polski sektor finansowy, jako część infrastruktury kraju wspierającego Ukrainę, stał się celem dla grup powiązanych z Rosją.

Warto też pamiętać, że ataki DDoS stały się towarem powszechnie dostępnym w modelu Cybercrime as a Service. Usługi umożliwiające przeprowadzenie ataku można znaleźć nie tylko w darknecie, ale też w otwartym Internecie, co obniża barierę wejścia dla potencjalnych atakujących. Jednocześnie skala ataków rośnie wraz z rozwojem infrastruktury sieciowej – większe pasma u użytkowników końcowych, rozwój sieci 5G i rosnąca liczba urządzeń IoT oznaczają więcej potencjalnych źródeł ataków.

Dlatego odporność na ataki DDoS to nie opcja, ale konieczność. Polskie instytucje finansowe od lat budują zdolności obronne w tym zakresie, a CSIRT KNF wspiera je zarówno w przygotowaniu do ataków, jak i w koordynacji działań podczas ich trwania.

Skala zagrożenia w 2025 roku

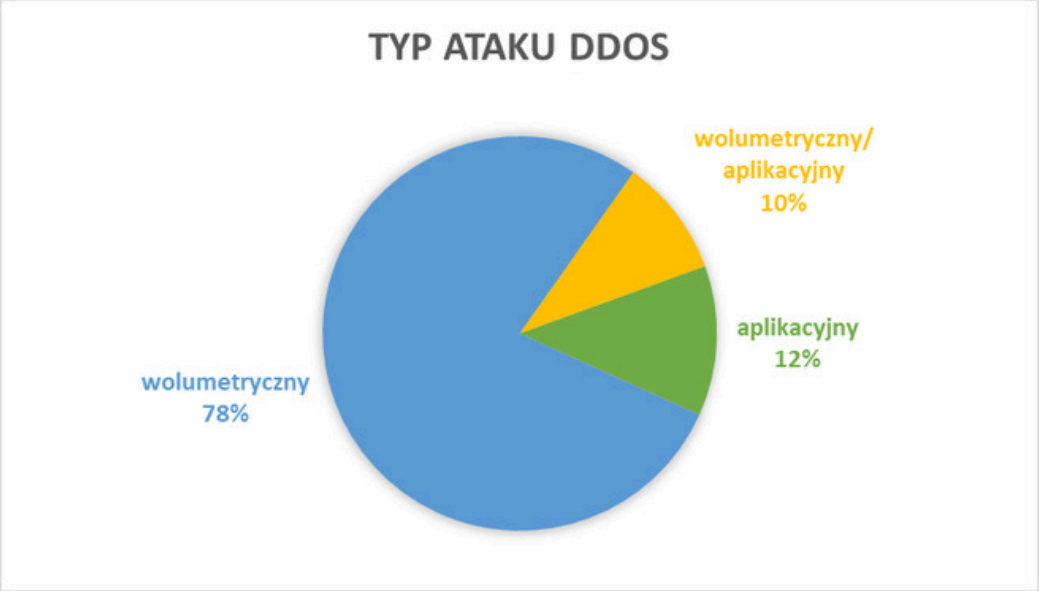
W 2025 roku CSIRT KNF zarejestrował 787 ataków DDoS wymierzonych w polski sektor finansowy. To wyraźny wzrost w porównaniu z poprzednimi latami, który wpisuje się w szerszy obraz zagrożeń obserwowany w całym regionie Europy Środkowo-Wschodniej.



Wykres 5. Liczba ataków DDoS w danym roku

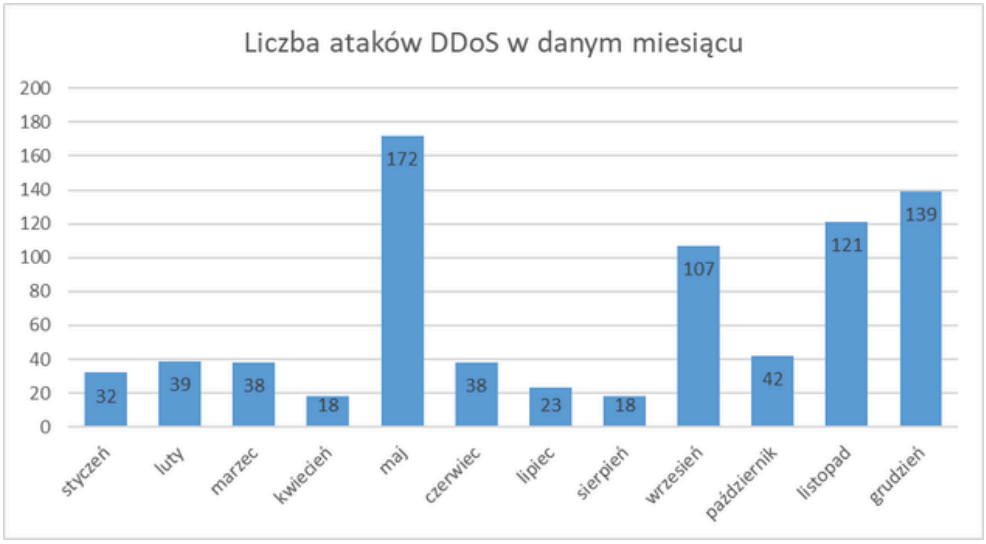
Największy odnotowany atak osiągnął w szczycie wolumen 1,3 Tbps i miał miejsce w maju. Był to jeden z najpotężniejszych ataków, z jakimi kiedykolwiek mierzyły się polskie instytucje finansowe. W sumie odnotowaliśmy 19 ataków przekraczających 500 Gbps oraz 48 ataków w przedziale 100-500 Gbps – to ataki wymagające zaawansowanych mechanizmów obrony i dobrze przygotowanej infrastruktury.

Zdecydowana większość ataków (78%) miała charakter wolumetryczny, czyli polegający na przeciążeniu łącza dużą ilością ruchu. Ataki aplikacyjne, celujące w konkretne usługi i aplikacje, stanowiły 12% przypadków, a pozostałe 10% to ataki mieszane łączące obie techniki.



Wykres 6. Typ ataku DDoS

Intensywność ataków była nierównomierna w ciągu roku. Maj okazał się najbardziej intensywnym miesiącem ze 172 zarejestrowanymi atakami, w tym wspomnianym rekordzistą o wolumenie 1,3 Tbps. Wrzesień, listopad oraz grudzień również przyniosły zwiększoną aktywność atakujących.



Wykres 7. Liczba ataków DDoS w danym miesiącu

Odporność rynku

Pomimo znacznej liczby ataków i rekordowych wolumenów, zdecydowana większość z nich nie przyniosła skutków dla ciągłości działania usług finansowych. Klienci banków i innych instytucji finansowych, w większości przypadków, nie odczuli wpływu tych ataków na dostępność usług, z których korzystają na co dzień.

Ta odporność nie wzięła się znikąd. To efekt lat systematycznej pracy całego sektora – inwestycji w bezpieczeństwo, budowania kompetencji zespołów oraz rozwijania współpracy między instytucjami. Polski sektor finansowy traktuje cyberbezpieczeństwo jako priorytet i wspólną odpowiedzialność, a nie tylko koszt czy wymóg regulacyjny.

Ważnym elementem tej odporności jest gotowość do dzielenia się wiedzą i doświadczeniami. Instytucje finansowe, mimo że konkurują ze sobą na co dzień, w obszarze bezpieczeństwa potrafią działać wspólnie. Informacje o atakach, skutecznych metodach obrony i zaobserwowanych zagrożeniach „przepływają" między podmiotami, co pozwala całemu sektorowi uczyć się na doświadczeniach pojedynczych instytucji.

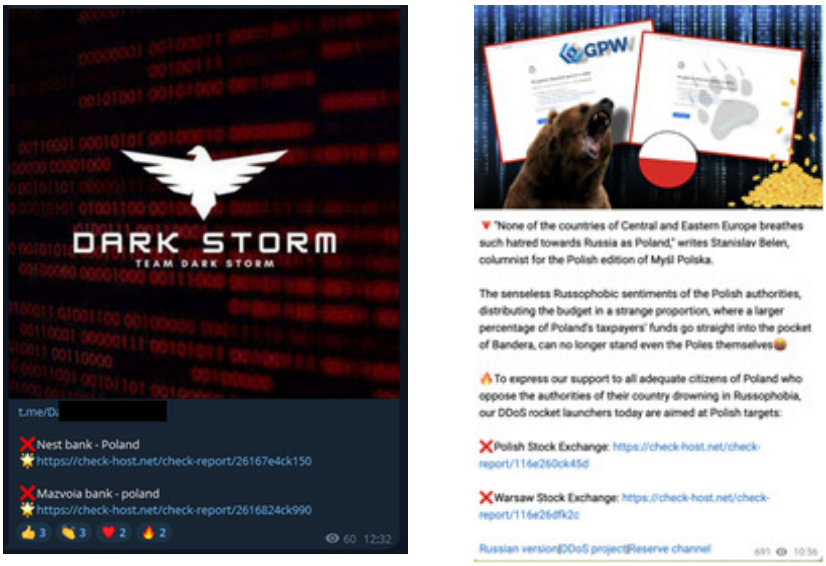
Nie mniej ważne jest przygotowanie organizacyjne. Same rozwiązania techniczne nie wystarczą, jeśli nie towarzyszą im przećwiczone procedury, jasno określone role i sprawna komunikacja w sytuacji kryzysowej. Instytucje finansowe regularnie testują swoją gotowość i doskonalą procesy reagowania na incydenty.

CSIRT KNF wspiera te działania pełniąc rolę koordynatora wymiany informacji i punktu kontaktowego dla całego sektora. Wspólnie budujemy ekosystem, w którym zagrożenie dla jednej instytucji staje się lekcją dla wszystkich pozostałych.

Monitorowanie i wymiana informacji

CSIRT KNF aktywnie monitoruje zagrożenia związane z atakami DDoS i prowadzi bieżącą wymianę informacji z podmiotami rynku finansowego. W ramach tej współpracy wymieniamy się adresami IP źródeł ataków oraz skutecznymi metodami mitygacji. Dzięki temu instytucje mogą szybciej reagować na nowe kampanie, konfigurować reguły filtrowania ruchu i uczyć się na doświadczeniach innych podmiotów, które wcześniej zmierzyły się z podobnymi zagrożeniami.

Poszukujemy również sygnałów zapowiadających planowane ataki – monitorując aktywność grup haktywistycznych i ich deklaracje dotyczące celów w sektorze finansowym. Grupy te często z wyprzedzeniem ogłaszają swoje zamiary w kanałach komunikacyjnych, co daje nam możliwość ostrzeżenia potencjalnych celów i wsparcia ich w przygotowaniu do obrony.



Grafika 48. Informacja o planowanych atakach opublikowana przez grupę haktywistyczną

Warto też pamiętać, że ataki DDoS bywają wykorzystywane jako zasłona dymna dla innych działań przestępczych. Podczas gdy zespoły bezpieczeństwa koncentrują się na odpieraniu ataku wolumetrycznego, atakujący mogą próbować realizować inne cele. Dlatego w trakcie ataku DDoS monitoring bezpieczeństwa powinien być utrzymany na poziomie nie niższym niż przy normalnym ruchu, a instytucje powinny zachować czujność wobec innych potencjalnych zagrożeń.

Podsumowanie

Rok 2025 przyniósł dużą liczbę ataków DDoS na polski sektor finansowy – 787 zarejestrowanych incydentów, w tym atak o bezprecedensowym wolumenie 1,3 Tbps. Pomimo tej skali zagrożeń sektor wykazał wysoką odporność. To efekt lat inwestycji w infrastrukturę, budowania relacji z operatorami telekomunikacyjnymi i dostawcami usług bezpieczeństwa oraz systematycznego doskonalenia procedur reagowania.

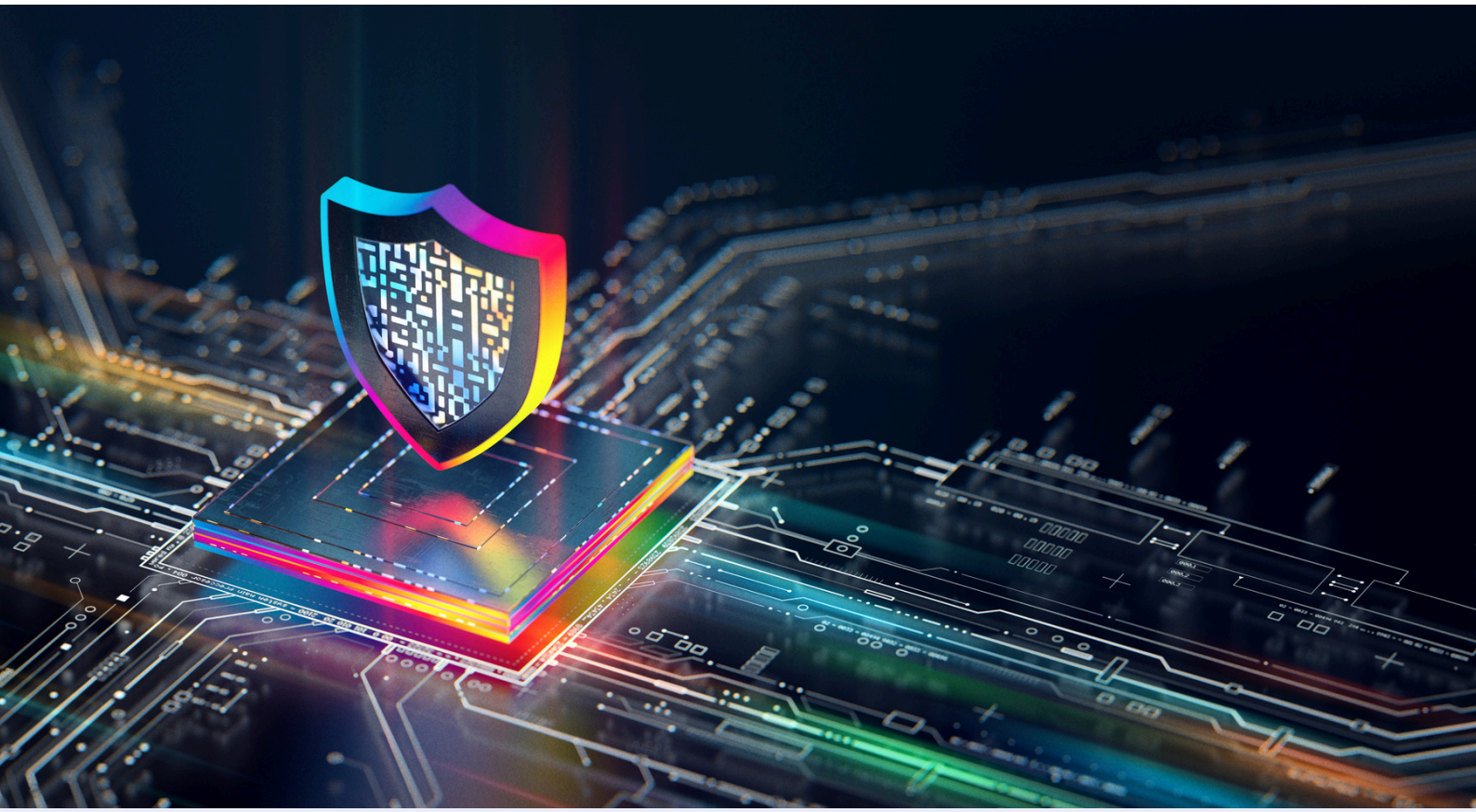
Warto przypomnieć, że w 2022 roku CSIRT KNF opublikował dokument „Dobre praktyki w zakresie przeciwdziałania atakom DDoS”[21], który w dalszym ciągu pozostaje aktualny i stanowi punkt odniesienia dla instytucji finansowych. Wyniki roku 2025 potwierdzają, że rekomendacje zawarte w tym dokumencie zostały przez sektor wdrożone w praktyce – nawet ataki przekraczające 1 Tbps nie są w stanie zakłócić działania polskich instytucji finansowych.

Grafika 49. Opublikowany przez CSIRT KNF dokument „Dobre praktyki w zakresie przeciwdziałania atakom DDoS”

CSIRT KNF będzie kontynuował działania w zakresie monitorowania zagrożeń DDoS, wymiany informacji z rynkiem oraz wczesnego ostrzegania o planowanych atakach. Wspólnie z instytucjami finansowymi pracujemy nad tym, żeby ataki DDoS pozostały dla sektora uciążliwością, a nie realnym zagrożeniem dla ciągłości działania.

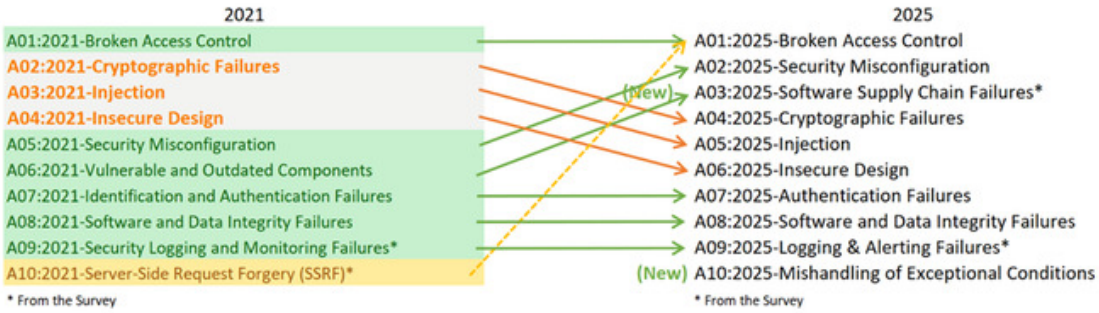
[21] https://cebrf.knf.gov.pl/images/Raporty/Dobre_praktyki_w_zakresie_przeciwdziaania_atakom_DDoS_77247.pdf

3.3 AKTUALNE TRENDY CYBERZAGROŻEŃ



Rok 2025 przyniósł kolejne zmiany w zakresie identyfikowanych cyberzagrożeń, zarówno w ujęciu globalnym, jak i w kontekście podmiotów sektora finansowego.

Zmiany te wyraźnie odzwierciedla zaktualizowana propozycja zestawienia dziesięciu najczęściej identyfikowanych zagrożeń, publikowanego cyklicznie w ramach OWASP Top 10. Projekt aktualizacji zestawienia z 2021 roku opublikowano 6 listopada 2025 roku.



Grafika 50. Najczęściej identyfikowane zagrożenia – OWASP Top 10[22]

Znaczące zmiany odnotowano na pozycjach drugiej i trzeciej rankingu, które zajęły następujące kategorie podatności:

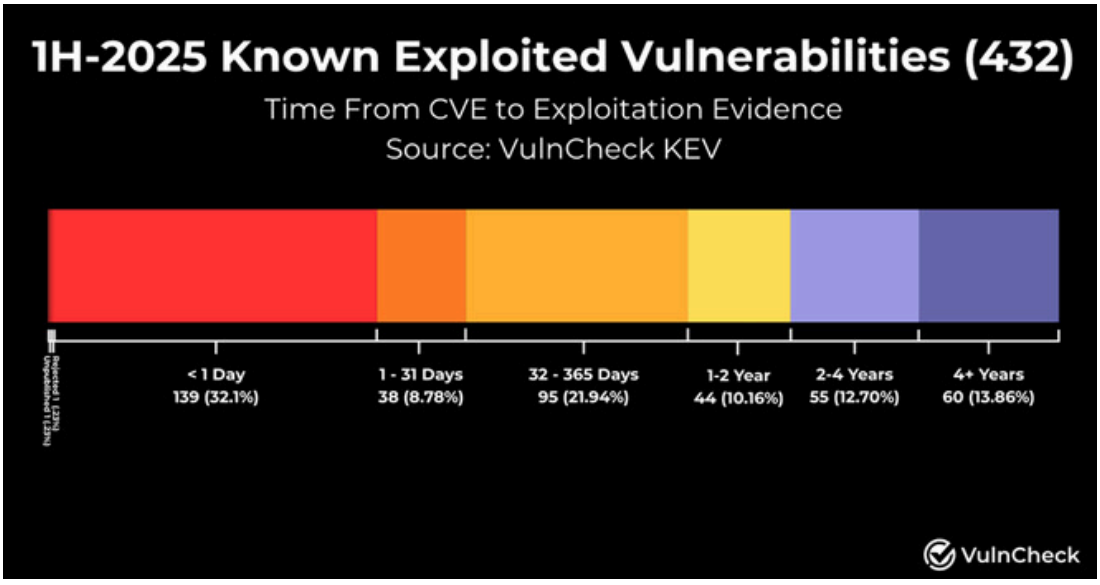
- A02: Security Misconfiguration – podatność, która awansowała z 5. miejsca (Top 10 2021) na pozycję 2. Według OWASP liczba błędów konfiguracyjnych systematycznie rośnie – 3% analizowanych aplikacji wykazywało co najmniej jedną z 16 słabości CWE (Common Weakness Enumeration) z tej kategorii. Przyczyna tkwi w rosnącej zależności aplikacji od właściwej konfiguracji.
- A03: Software Supply Chain Failures – kategoria stanowiąca rozszerzoną wersję poprzedniego A06:2021 (Vulnerable and Outdated Components), obejmującą cały ekosystem zależności, systemy budowania oraz infrastrukturę dystrybucyjną. Według środowiska specjalistów ds. reagowania na incydenty bezpieczeństwa IT, kategoria ta została w przeprowadzonych ankietach wskazana jako jeden z najbardziej krytycznych problemów. Dane wskazują na rzadką wykrywalność tego typu zagrożeń, głównie ze względu na trudności w ich testowaniu. Jednocześnie podatność ta osiąga najwyższe średnie wskaźniki w kategoriach exploitability oraz impact w ramach CVE.

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

Podatności identyfikowane przez CSIRT KNF w latach 2023-2025 również potwierdzają opisywaną przez OWASP tendencję rozwoju zagrożeń.

W zakresie eksploatacji i identyfikowania nowych podatności CVE (Common Vulnerabilities and Exposures) rok 2025 od początku sygnalizował nasilenie tego trendu. Z publicznie dostępnego raportu VulnCheck, dotyczącego liczby nowych CVE ujawnionych w pierwszej połowie 2025 roku, wynika, że do końca czerwca zarejestrowano 432 nowe podatności. 32% z nich było aktywnie eksploatowanych w atakach jeszcze przed formalnym zarejestrowaniem w bazie CVE[23].

Na uwagę zasługuje również opublikowany przez VulnCheck wykres ilustrujący średni przedział czasu między publikacją informacji o nowej luce w zabezpieczeniach, a identyfikacją przypadków jej aktywnej eksploatacji w atakach, który w 2025 roku wyniósł poniżej jednego dnia.



Grafika 51. Informacja dotycząca liczby nowych CVE ujawnionych w pierwszej połowie 2025 roku

Wartość ta definiuje dostępne okno czasowe, w którym zespoły odpowiedzialne za utrzymanie systemów i aplikacji mogą zareagować na ujawnienie nowej, znanej podatności oraz uruchomić proces remediacji, aby z wysokim prawdopodobieństwem móc skutecznie zmitygować zagrożenie związane z możliwością jej potencjalnego wykorzystania w ataku.

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

Zagrożenie ze strony ataków typu Supply Chain wynika w znacznej mierze z ograniczonych możliwości monitorowania aspektów cyberbezpieczeństwa u dostawców zewnętrznych narzędzi oraz usług. Ponadto w przeważającej liczbie przypadków organizacje nie dysponują informacją o komponentach dostarczanych przez szeroko rozumianych dostawców technologii zewnętrznych (third-party technology providers).

Wyniki badań BitSight zostały opublikowane w artykule zamieszczonym przez serwis helpnetsecurity.com pt.: „Hidden risks in the financial sector's supply chain"[24] z listopada 2025 roku, w którym badacze przeanalizowali ponad 41 000 organizacji finansowych oraz ich relacje z ponad 50 000 dostawcami technologii, identyfikując zależności pomiędzy nierównomiernym monitoringiem oraz lukami w zarządzaniu ryzykiem w cyfrowym łańcuchu dostaw sektora finansowego. Wyniki badań potwierdzają istnienie luki w możliwościach aktywnego monitorowania zagrożeń typu Supply Chain. W badaniu zidentyfikowano łącznie 99 najważniejszych dostawców technologii dla sektora finansowego, w tym zarówno znane, duże firmy, jak Microsoft czy Google, ale również mniej widoczne na rynku IT, takie jak General Dynamics i NICE Group, które również pełnią kluczowe role w łańcuchu dostaw, choć rzadziej znajdują się w centrum uwagi przed ujawnieniem luk bezpieczeństwa w ich produktach lub zabezpieczeniach infrastruktury. W porównaniu z organizacjami finansowymi, zewnętrzni dostawcy wykazali gorsze wyniki w 16 z 22 przyjętych w badaniu kategorii ryzyka. Szczególnie zaniedbano obszar związany z zarządzaniem podatnościami oraz ekspozycję tzw. OPSEC (Operations Security). Badania te obaliły również mit o tym, że więksi dostawcy dysponują mocniejszymi zabezpieczeniami cybernetycznymi. Dostawcy z większym udziałem rynkowym mają gorsze oceny bezpieczeństwa, co sugeruje, że większa infrastruktura i liczba klientów mogą zwiększać powierzchnię ataku. Niemonitorowani dostawcy usług sektora finansowego posiadali 2,9 razy więcej krytycznych podatności, opisanych w CVE w infrastrukturze własnej niż dostawcy monitorowani.

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

Ponadto 2,8 razy więcej z tych podatności było eksploitowanych w atakach w porównaniu z dostawcami objętymi procesem monitorowania. Wnioski te sugerują, że aktywne monitorowanie nie tylko zwiększa widoczność zagrożeń, ale też motywuje dostawców do poprawy zabezpieczeń własnego środowiska i świadczonych usług, co w konsekwencji pozytywnie wpływa na bezpieczeństwo całego sektora finansowego.

Wzrost poziomu ryzyka związanego z zagrożeniem w postaci ataku na łańcuch dostaw jest powszechnie zauważalny. Ataki tego typu mają coraz częściej poważne konsekwencje, na co wskazuje również przedsiębiorstwo badawczo-analityczne Gartner.

Liczba naruszeń związanych z łańcuchem dostaw w 2025 roku wzrosła o 68%, stanowiąc obecnie 15% wszystkich ataków, których skutkiem jest naruszenie danych. W 2024 roku 35,5% naruszeń danych było związanych z podmiotami trzecimi, co oznacza wzrost o 29% w stosunku do 2023 roku[25]. Gartner przewiduje, że 45% organizacji doświadczy naruszeń łańcucha dostaw do końca 2025 roku, co oznacza trzykrotny wzrost od 2021 roku[26].

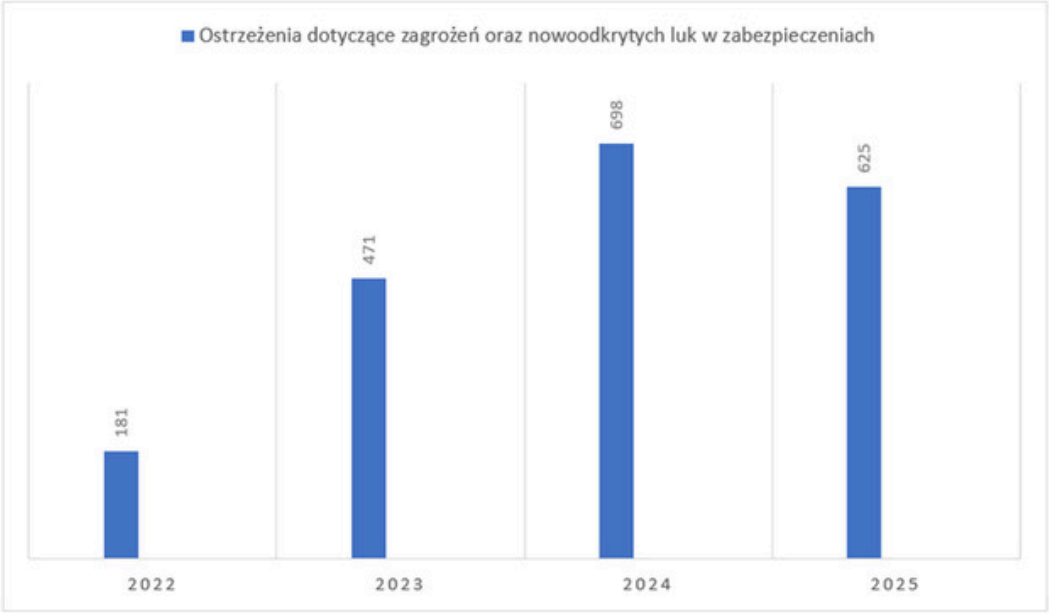
Warto wskazać, że jednym z największych incydentów typu Supply Chain Attack w ostatnich latach były ataki na paczki NPM – bardzo popularnego oraz szeroko wykorzystywanego menadżera pakietów środowiska Node.js (JavaScript). Przykładem skutecznie przeprowadzonego ataku na łańcuch dostaw może być atak, którego ofiarą padła firma Jaguar Land Rover. Sprawcom ataku udało się skompromitować konto jednego z dostawców tej firmy i w ten sposób uzyskali oni dostęp do systemu zarządzania projektami. Konsekwencje tego incydentu wykraczają daleko poza samą markę. Szacuje się, że straty finansowe związane z atakiem tylko w Wielkiej Brytanii[27] wyniosły 1,9 miliarda funtów.

[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/

Działanie CSIRT wspomagające sektor finansowy w zakresie ostrzegania przed cyberzagrożeniami

W 2025 roku CSIRT KNF utrzymał wysoką aktywność w obszarze identyfikacji podatności i wspierania podmiotów rynku finansowego. W ciągu roku opublikowano 625 ostrzeżeń, 19 rekomendacji sektorowych oraz zrealizowano dziesiątki celowanych skanów bezpieczeństwa, z których w 51 przypadkach zidentyfikowane zagrożenia skutkowały przekazaniem indywidualnych rekomendacji do konkretnych podmiotów sektora finansowego.

Statystyki:



Wykres 8. Ostrzeżenia CSIRT KNF dotyczące zagrożeń oraz nowoodkrytych luk w zabezpieczeniach

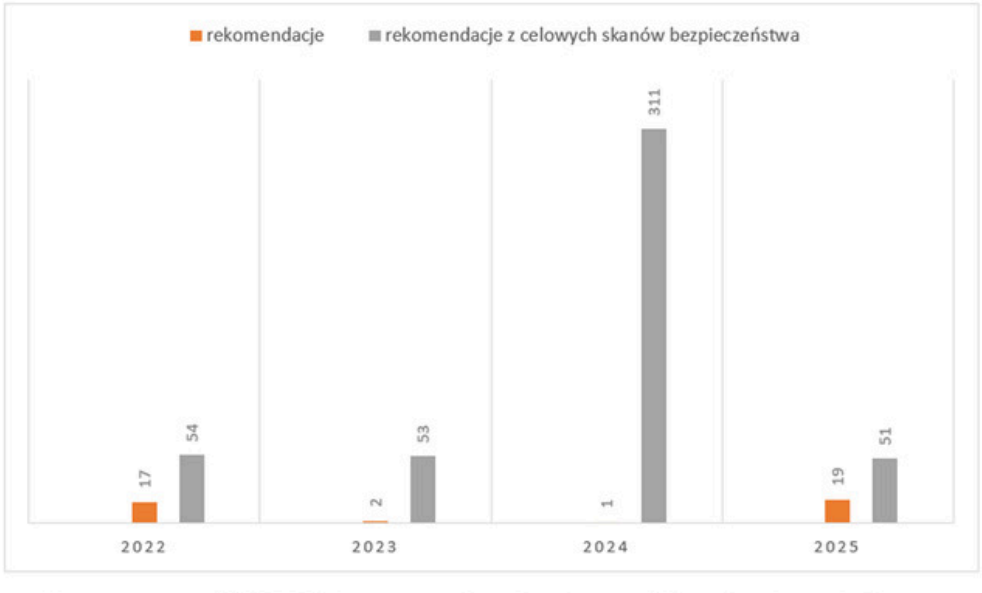
Ostrzeżenia dotyczące zagrożeń oraz nowo odkrytych luk w zabezpieczeniach ujawnianych przez producentów oraz ekspertów ds. bezpieczeństwa, stanowią kluczowy instrument natychmiastowego informowania uczestników sektora finansowego o prowadzonych kampaniach cyberprzestępczych, wykrytych podatnościach oraz rozpoznanych metodach przeprowadzania ataków.

W 2025 roku w większym stopniu niż dotychczas rekomendacje sektorowe ukierunkowano na podatności oraz kampanie, które mogły mieć potencjał oddziaływania na wszystkie podmioty lub znaczną część rynku finansowego. Miało to na celu umożliwienie wykorzystania pojedynczej rekomendacji bezpieczeństwa przez wiele instytucji rynku finansowego.

Jednocześnie, zgodnie z praktyką lat poprzednich, zespół CSIRT KNF kontynuował działania z zakresu skanowania bezpieczeństwa publicznie dostępnej infrastruktury podmiotów finansowych należących do zrzeszeń. Skany te zachowały charakter działań precyzyjnie ukierunkowanych – przeznaczonych indywidualnym podmiotom, z uwzględnieniem specyficznych systemów, aplikacji oraz usług eksponowanych w sieci Internet. Wykryte zagrożenia przekazywano każdorazowo w formie spersonalizowanego zestawienia rekomendacji adresowanych do danego podmiotu wykorzystującego wskazany produkt, infrastrukturę lub narzędzie.

W konsekwencji w 2025 roku CSIRT KNF zintegrował dwa wzajemnie uzupełniające się poziomy oddziaływania: w wymiarze szerokiego, horyzontalnego zasięgu – poprzez rekomendacje kierowane do całości sektora finansowego, oraz w wymiarze celowanym – poprzez inicjowanie działań nastawionych na identyfikację i analizę podatności oraz zagrożeń w publicznie dostępnej warstwie infrastruktury informatycznej poszczególnych uczestników rynku.

Statystyki:



Wykres 9. Aktywność CSIRT KNF w obszarze identyfikacji podatności i wspierania podmiotów rynku finansowego

Ten model wzmacnia dojrzałość sektora w obszarze zarządzania podatnościami i przekłada się na rzeczywisty wzrost poziomu bezpieczeństwa podmiotów rynku finansowego.

Do najistotniejszych podatności w systemach informatycznych, które były aktywnie wykorzystywane w kampaniach ujawnionych w 2025 roku, można zaliczyć luki bezpieczeństwa zidentyfikowane w następujących produktach:

1. React/Next.js – krytyczna podatność, opisana w CVE-2025-55182, którą z czasem nazwano React2Shell, została opublikowana pod koniec roku 2025. Luka, która pozwalała atakującemu na zdalne wykonanie kodu, atak typu RCE, pociągnęła za sobą falę aktywnej eksploatacji. Skanowanie za podatnymi systemami rozpoczęło się zaraz po opublikowaniu informacji na temat luki. Pierwsza fala prób jej aktywnego wykorzystania była obserwowana w okresie 3-5 grudnia.

Podatność React2Shell wykorzystuje niestandardową logikę protokołu React Flight Protocol (RFP) używanego przez React Server Components. Luka umożliwia atakującym nadpisanie właściwości zmiennych po stronie serwera i przejęcie kontroli nad obiektem JavaScript poprzez manipulację chunkami RFP. W przeciwieństwie do standardowych podatności, RFP wykorzystuje niestandardowy protokół oparty na chunkach, co daje atakującym znaczące możliwości w zakresie unikania detekcji i działań post-eksploatacyjnych.

Podatne komponenty:

- Next.js (główny wektor ataku – większość publicznych PoC)
- React Router (eksperymentalna funkcjonalność RSC, niewłączona domyślnie)
- Expo (framework z eksperymentalnym wsparciem dla RSC)
- React RSC (bezpośrednie wywołania funkcji)
- Waku (framework wykorzystujący losowo generowane endpointy)

W trakcie kampanii zidentyfikowano następujące warianty eksploitów:

- Initial execution-based exploits – najprostsze, bezpośrednie wywołanie NodeJS process i require modules
- Droppers – zapisanie drugiego etapu payloadu na dysku
- In-memory exploits – działania całkowicie w pamięci, bez zapisu na dysku
- Unicode escaping – maskowanie fingerprints poprzez escape'owanie Unicode (\uXXXX)
- In-memory webshells – modyfikacja prototypu serwera HTTP NodeJS, umożliwiająca utworzenie webshell całkowicie w pamięci, działającego na ścieżkach kontrolowanych przez atakującego

Poza działaniami Threat Aktorów ściśle powiązanymi z aktywnością, której celem było identyfikowanie w sieci publicznej potencjalnych celów ataku oraz dalszego eksploitowania podatności React2Shell, odnotowano również udane próby wykorzystania rozgłosu wokół podatności do dystrybucji złośliwego oprogramowania podszywającego się lub zaimplementowanego w „skanery" podatności React2Shell, które pojawiały się w formach PoC w różnych źródłach.

2. MongoDB – podatność w MongoDB Server, która umożliwia zdalnym, nieuwierzytelnionym atakującym odczyt niezainicjalizowanej pamięci heap w wyniku nieprawidłowej obsługi długości danych w nagłówkach protokołu skompresowanego zlib. Podatne produkty i wersje:

- 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
- wszystkie wersje MongoDB Server 4.2, 4.0 oraz 3.6

Podatność opisano w CVE-2025-14847 z CVSSv3.1 8.7 – typu improper handling of length parameter inconsistency w implementacji kompresji zlib, umożliwiająca read of uninitialized heap memory przez nieuwierzytelnionego klienta.

Skuteczne wykorzystanie luki może prowadzić do ujawnienia wrażliwych danych znajdujących się w pamięci procesu serwera, takich jak informacje o stanie wewnętrznym lub wskaźniki pamięci. Lukę zaadresowano poprawką w następujących wersjach MongoDB Server: 8.2.3, 8.0.17, 7.0.28, 6.0.27, 5.0.32, 4.4.30. Podatność była szeroko wyszukiwana oraz aktywnie wykorzystywana, na co wpłynęła głównie łatwość jej eksploitacji oraz szybkie opublikowanie PoC podatności.

3. Citrix – produkty NetScaler ADC oraz NetScaler Gateway, w których zidentyfikowano podatności opisane w 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 behavior and Denial of Service, CVE-2025-8424 CVSS v4.0 8.7 – Improper access control on the NetScaler Management Interface. Pośród wymienionych, luka opisana w CVE-2025-7775 była aktywnie wykorzystywana w atakach jeszcze przed jej zidentyfikowaniem przez producenta, jako 0-Day.

Kampanie threat aktorów były ukierunkowane na infrastrukturę w podatnej konfiguracji:

- Gateway: VPN virtual server, ICA Proxy, CVPN, RDP Proxy lub AAA virtual server
- LB virtual servers (HTTP, SSL, HTTP_QUIC) w wersjach 13.1, 14.1, 13.1-FIPS, NDcPP powiązane z usługami: IPv6, IPv6 DBS, CR virtual server typu HDX

4. Citrix – produkt NetScaler ADC/Gateway, w którym zidentyfikowano podatność CVE-2025-12101 CVSS 5.9 – typu Cross-Site Scripting (XSS). Podatność występuje wyłącznie w appliance'ach skonfigurowanych jako Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) lub AAA virtual server. Mechanizm ataku XSS pozwala na wstrzyknięcie złośliwego skryptu do kontekstu sesji użytkownika.

5. Fortinet – luka w zabezpieczeniach FortiWeb, która została opisana w CVE-2025-52970 CVSS 7.7, może umożliwić nieuwierzytelnionemu zdalnemu atakującemu, dysponującemu niepublicznymi informacjami o urządzeniu oraz koncie atakowanego użytkownika, zalogowanie się jako dowolny istniejący użytkownik na podatnej wersji urządzenia za pomocą specjalnie przygotowanego żądania. Podatność została zaadresowana poprawkami w wersjach FortiWeb 7.6.4, 7.4.8, 7.2.11 oraz 7.0.11.

6. Fortinet – podatność opisana w CVE-2025-64446 CVSSv3 9.1, 0-day typu path traversal, który pozwala nieuwierzytelnionemu atakującemu na wykonywanie poleceń z uprawnieniami administratora w systemie za pośrednictwem spreparowanych zapytań http. Została ona zaadresowana poprawką bezpieczeństwa w wersjach 8.0.2, 7.6.5, 7.4.10, 7.2.12, 7.0.12.

7. Fortinet – podatność ujawniona w produkcie FortiWeb, która została opisana w CVE-2025-58034 z CVSSv3 6.7 – pozwala uwierzytelnionemu atakującemu na wykonanie polecenia w systemie za pośrednictwem spreparowanego pakietu HTTP lub polecenia w CLI. Może to skutkować pełnym przejęciem systemu oraz wpłynąć na integralność, poufność lub dostępność przetwarzanych przez system danych. Luka została załatana poprawką bezpieczeństwa w wersjach 8.0.2, 7.6.6, 7.4.11, 7.2.12, 7.0.12.

8. Spring – podatności, które zostały opisane w CVE-2025-41248 CVSSv3.1 7.5 – Authorization bypass, dotyczący użycia adnotacji @PreAuthorize i innych adnotacji method security, co może skutkować ominięciem autoryzacji oraz CVE-2025-41249 CVSSv3.1 7.5 – luka odnosząca się do aplikacji korzystających ze Spring Security @EnableMethodSecurity w połączeniu z adnotacjami bezpieczeństwa umieszczonymi w generycznych nadklasach lub interfejsach. Zostały zidentyfikowane w aplikacjach Spring Security oraz Spring Framework w wersjach:

- Spring Security w wersjach niższych niż: 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 niższych niż: 6.2.11, 6.1.23, 5.3.45. Wersje 6.0.x są pozbawione wsparcia producenta, poprawki nie będą publikowane.

9. Cisco – podatności ujawnione w Cisco Adaptive Security Appliance (ASA), opisane w CVE-2025-20333 CVSS 9.9 – VPN Web Server Remote Code Execution, w której luka typu Buffer Overflow w VPN web server umożliwia zdalne wykonanie kodu. Jest ona łączona w łańcuch z podatnością opisaną w CVE-2025-20362 CVSS 6.5 – VPN Web Server Unauthorized Access, która pozwala na unauthorized access do VPN web server w tak zwany łańcuch eksploitacji pozwalający na całkowite przejęcie podatnego systemu. Kolejną z luk zidentyfikowanych w Cisco ASA była CVE-2025-20363 CVSS 9.0 – błąd w HTTP processing, umożliwiający wykonanie dowolnego kodu. Luki opisane w CVE-2025-20333 oraz CVE-2025-20362 były aktywnie wykorzystywane w atakach. Poprawki zostały opublikowane w wersjach 7.0.8.1, 7.2.10.2, 7.4.2.4, 7.6.2.1, 7.7.10.1.

10. IBM – podatność ujawniona w systemie SIEM QRadar, którą opisano w CVE-2025-36007 CVSS 7.8 – wynikająca z nieprawidłowego przypisania uprawnień do skryptu aktualizacji w IBM QRadar SIEM. Atakujący posiadający ograniczony dostęp lokalny do systemu mógł wykorzystać błędną konfigurację uprawnień skryptu, by wykonać operacje z podwyższonymi uprawnieniami konta administratora. Mechanizm wykorzystania bazuje na manipulacji procesem aktualizacji oprogramowania. Luka została zaadresowana poprawką bezpieczeństwa w IBM QRadar SIEM 7.5.0 UP14.

11. MikroTik – podatność zidentyfikowana w komponencie WebFig w MikroTik RouterOS w wersji 7.14.2 oraz SwOS w wersji 2.18. Została opisana w CVE-2025-61481 CVSS: 10.0 – umożliwia ona atakującemu wykonanie dowolnego kodu na podatnym urządzeniu bez konieczności posiadania poświadczeń, za pośrednictwem spreparowanego pakietu http.

12. Oracle – luka w menadżerze zarządzania tożsamością oraz dostępem w produkcie Oracle Identity Manager, która została opisana w CVE-2025-61757 CVSSv3 9.8 – błąd w komponencie REST WebServices, umożliwia przejęcie systemu Identity Manager przez atakującego nie wymagając uwierzytelnienia, za pośrednictwem spreparowanego żądania HTTP. Podatność odnosi się do wersji IM 12.2.1.4.0 oraz 14.1.2.1.0.

13. Oracle – podatności zidentyfikowane w produktach Oracle E-Business Suite w komponencie Marketing Administration, a także Oracle Financial Services Applications, które opisano w CVE-2025-61884 CVSS 7.5 – dot. Oracle E-Business Suite, typu Server-Side Request Forgery luka umożliwiająca zdalne wysyłanie żądań http z serwera ofiary do zasobów wewnętrznych lub zewnętrznych, co może prowadzić do ujawnienia danych lub zdalnego wykonania kodu. CVE-2025-53037 CVSS: 9.8 – Oracle Financial Services Analytical Applications Infrastructure w wersjach 8.0.7.9, 8.0.8.7 oraz 8.1.2.5, podatność ta umożliwia atakującemu pełny dostęp do systemu poprzez zdalne wykonanie kodu za pośrednictwem zapytania http. CVE-2025-53072 CVSS 9.8 – Oracle FLEXCUBE/E-Business Suite Marketing, luka w module Marketing Admin pakietu Oracle E-Business Suite w wersjach 12.2.3-12.2.14 pozwala na zdalne wykonanie dowolnego kodu, bez uwierzytelnienia za pomocą spreparowanych zapytań http. CVE-2025-62481 CVSS 9.8 – Oracle FLEXCUBE/E-Business Suite Marketing – luka w module Marketing Admin pozwala atakującemu na zdalne wykonanie kodu bez uwierzytelnienia poprzez wysłanie spreparowanych zapytań http. Podatność ta pozwala atakującemu na uzyskanie dostępu do danych klientów, modyfikowanie treści, a także upload i propagowanie złośliwego kodu. CVE-2025-53036 CVSS 8.6 – Oracle Financial Service Analytical Applications Infrastructure, luka o wysokim poziomie ryzyka, umożliwiająca atakującemu na nieautoryzowany dostęp do danych aplikacji oraz eksalowanie uprawnień w aplikacji finansowej.

14. Fortra – podatność prowadząca do wstrzyknięcia obiektu i wykonania dowolnego kodu, ujawniona w produkcie GoAnywhere Managed File Transfer (MFT) w wersjach niższych niż 7.8.4 oraz Sustain Release 7.6.3, została opisana w CVE-2025-10035 z CVSS 10.0 – Deserialization vulnerability w License Servlet.

15. Omnissa – luka ujawniona w produkcie Omnissa Workspace ONE UEM w wersjach (On-Premises), która została opisana w CVE-2025-25231 z CVSSv3.1 7.5 – Secondary Context Path Traversal Vulnerability, pozwalająca atakującemu na uzyskanie nieuprawnionego dostępu do danych poufnych (read-only) z wykorzystaniem techniki Path Traversal. Poprawka bezpieczeństwa została wydana w wersjach 24.10.0.11, 24.6.0.35, 24.2.0.30, 23.10.0.50.

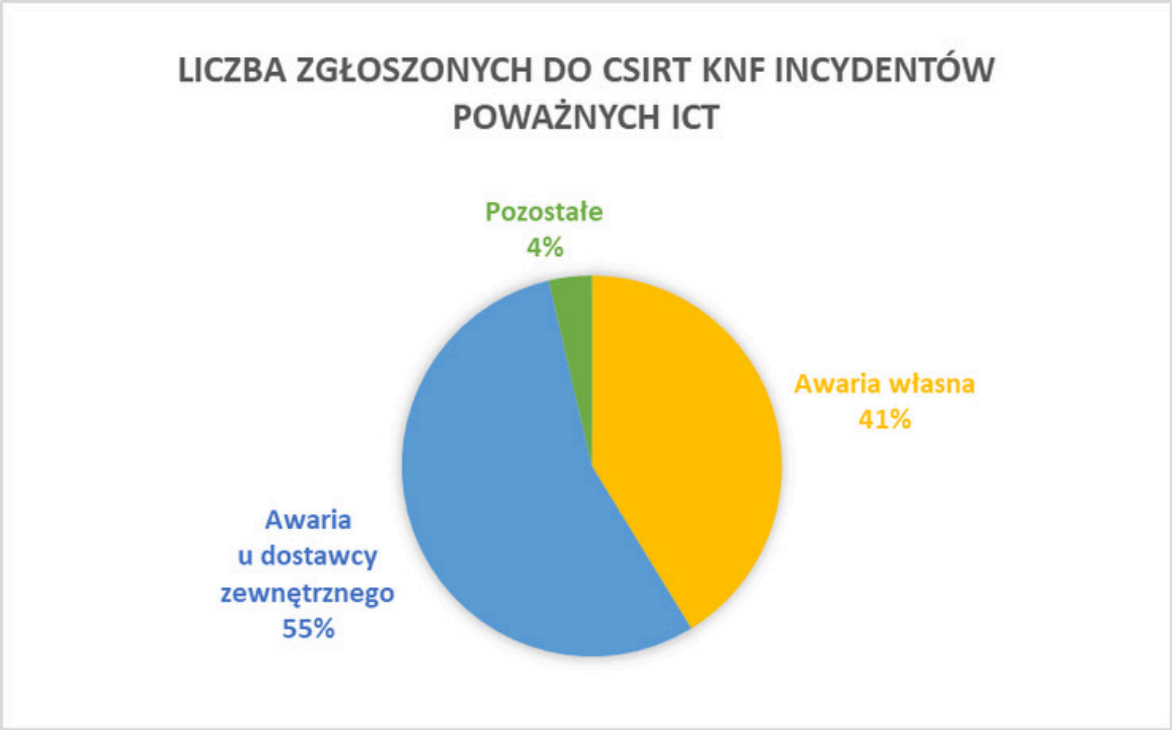
3.4 DORA JAKO FUNDAMENT CYBERODPORNOŚCI RYNKU FINANSOWEGO

Rok 2025 zapoczątkował obowiązywanie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Nowe przepisy ustanowiły jednolite wymagania dotyczące zarządzania ryzykiem ICT oraz raportowania incydentów bezpieczeństwa przez podmioty rynku finansowego w całej Unii Europejskiej, a ich wdrożenie wpłynęło na istotne podniesienie standardów bezpieczeństwa operacyjnego.

W przygotowaniu do wejścia w życie regulacji, w 2024 roku przeprowadzono szereg działań organizacyjnych i technicznych, z których kluczowym było uruchomienie systemu SOID, dostępnego pod adresem https://csirt.knf.gov.pl. Platforma stanowi obecnie centralne rozwiązanie dla zgłaszania incydentów ICT. Umożliwiła standaryzację sposobu raportowania oraz poprawiła kompletność i jakość zgłaszanych danych, co przełożyło się na sprawniejszą analizę incydentów i efektywniejszą koordynację obsługi zgłoszeń po stronie CSIRT KNF.

Jednym z najbardziej zauważalnych efektów wejścia w życie DORA było istotne rozszerzenie zakresu podmiotów objętych obowiązkiem raportowania. W porównaniu do dotychczas funkcjonującego obowiązku opartego na ustawie o Krajowym Systemie Cyberbezpieczeństwa (KSC), liczba instytucji zobowiązanych wzrosła znacząco. Przełożyło się to wprost na zwiększoną liczbę zgłoszeń kierowanych do CSIRT KNF w 2025 roku. Zmiana skali i zróżnicowanie podmiotów wymagały dostosowania procesów obsługi oraz zwiększenia zdolności operacyjnych.

W 2025 roku, już po formalnym wejściu w życie DORA 17 stycznia, podmioty objęte nowymi obowiązkami raportowania przekazały do CSIRT KNF łącznie 274 zgłoszenia incydentów poważnych ICT. Struktura tych incydentów odzwierciedlała charakter wyzwań operacyjnych stojących przed sektorem – dominującą kategorię stanowiły awarie, które odpowiadały za około 96% wszystkich zgłoszeń. Wśród nich 41% dotyczyło awarii zachodzących w środowisku własnym instytucji (113 zgłoszeń), natomiast 55% stanowiły awarie u zewnętrznych dostawców usług ICT (151 zgłoszeń). Pozostałe 4% zgłoszeń (10 incydentów) obejmowało inne kategorie zdarzeń.



Wykres 10. Liczba zgłoszonych do CSIRT KNF incydentów poważnych ICT z podziałem na kategorie

Wysoki udział incydentów związanych z awariami potwierdził, jak istotne znaczenie dla stabilnego funkcjonowania rynku finansowego ma odporność infrastruktury technologicznej oraz łańcucha dostaw usług ICT, w tym właściwe nadzorowanie usług krytycznych świadczonych przez podmioty trzecie. Jednocześnie pierwsze miesiące stosowania DORA uwidoczniły rosnącą świadomość instytucji w zakresie konieczności niezwłocznego i kompletnego raportowania, co przełożyło się na poprawę jakości danych oraz bardziej miarodajny obraz sytuacji operacyjnej sektora.

Nowością wprowadzoną przez DORA jest obowiązek przekazywania informacji o znaczących cyberzagrożeniach, rozumianych jako dane o potencjalnych aktywnościach cyberprzestępczych mogących mieć wpływ na funkcjonowanie sektora finansowego. Mechanizm ten usprawnił przepływ informacji pomiędzy instytucjami rynku, umożliwił szybszą identyfikację nowych trendów i technik działania adwersarzy oraz zwiększył zdolność do podejmowania działań prewencyjnych. Wymiana informacji, zarówno na poziomie krajowym, jak i europejskim, uległa znaczącemu wzmocnieniu.

DORA wprowadziła również jednolite standardy klasyfikacji oraz raportowania incydentów ICT. Ujednolicony model raportowania zwiększył spójność danych i ich użyteczność analityczną, wspierając proces identyfikacji wzorców zagrożeń i szybszego reagowania na incydenty. Standaryzacja informacji pozwoliła na bardziej precyzyjne rozpoznanie sytuacji w skali sektora oraz lepsze profilowanie zagrożeń.

Pierwszy rok obowiązywania regulacji charakteryzował się również intensyfikacją współpracy międzynarodowej. Obowiązek wymiany informacji o incydentach i trendach wpłynął na zwiększenie współdziałania pomiędzy organami właściwymi państw członkowskich UE, co umożliwiło bardziej skoordynowane działania zapobiegawcze oraz szybszy przepływ informacji dotyczących zagrożeń. CSIRT KNF aktywnie uczestniczył w tych procesach, wspierając budowę bardziej zintegrowanego i odpornego środowiska cyberbezpieczeństwa na poziomie europejskim.

Zróżnicowany poziom dojrzałości organizacyjnej podmiotów rynku finansowego stanowił jedno z kluczowych wyzwań w pierwszym roku obowiązywania DORA. W celu wsparcia instytucji w dostosowaniu się do nowych wymogów, CSIRT KNF prowadził działania edukacyjne obejmujące m.in. szkolenia oraz webinaria CEDUR, a także publikację materiałów informacyjnych. Wsparcie to przyczyniło się do podniesienia jakości zgłaszanych incydentów oraz poprawy procesu obsługi.

W 2025 przeprowadzono następujące webinaria CEDUR skierowane do podmiotów rynku finansowego nadzorowanych przez Komisję Nadzoru Finansowego stosujących Rozporządzenie DORA:

- Rozporządzenie DORA – pierwsze obowiązki sprawozdawcze oraz prezentacja systemów do sprawozdawczości (zakładanie kont, przekazywanie sprawozdań na przykładzie wybranych formularzy sprawozdawczych) – 3 terminy;
- Sprawozdawczość DORA – realizacja obowiązków sprawozdawczych, omówienie najczęstszych błędów – 4 terminy;
- Wymogi Rozporządzenia DORA, a wcześniejsze wdrożenie Rekomendacji D i wytycznych IT KNF – 4 terminy;

- Rozporządzenie DORA – praktyczne przykłady wypełniania rejestru informacji (formularz SPR-PF-18) – 2 terminy;
- Rozporządzenie DORA – praktyczne przykłady przekazywania Ankiet KRI (formularz SPR-PF-26 i SPR-PF-27);
- Zarządzanie incydentami i cyberzagrożeniami zgodnie z Rozporządzeniem DORA – 3 terminy;
- Testy TLPT – kompleksowe podejście do testów bezpieczeństwa;
- Wdrożenie Rozporządzenia DORA z perspektywy organu nadzoru finansowego – 2 terminy;
- Rozporządzenie DORA – praktyczne przykłady przekazywania sprawozdania dotyczącego informacji na temat ryzyka ICT oraz ram zarządzania ryzykiem ICT (formularz SPR-PF-01);
- Rozporządzenie DORA – przekazanie sprawozdania, przykłady zawierające formularz SPR-PF-00 oraz odpowiedzi na pytania dotyczące formularza SPR-PF-01.

Grafika 52. Informacja opublikowana przez UKNF w mediach społecznościowych dotycząca rejestracji na webinaria CEDUR poświęcone Rozporządzeniu DORA

Dzięki przygotowaniom realizowanym w 2024 roku – w szczególności wdrożeniu systemu SOID oraz doskonaleniu procesów obsługi incydentów – CSIRT KNF był w stanie w 2025 roku przyjmować i koordynować zgłoszenia w sposób sprawny, mimo wyraźnego wzrostu ich liczby. Wzrost jakości raportowanych danych oraz ich spójności wspierał proces analizy ryzyka i podejmowania działań prewencyjnych w skali całego sektora finansowego.

3.5 MOJE.CERT.PL – SEKTOROWY MODUŁ CSIRT KNF DLA RYNKU FINANSOWEGO

W 2025 roku jednym z kluczowych kierunków wzmacniania odporności cybernetycznej sektora finansowego było rozwijanie spójnych mechanizmów współdzielenia informacji o zagrożeniach i incydentach. W tym kontekście szczególne znaczenie ma rozbudowa platformy moje.cert.pl oraz uruchomienie w jej ramach modułu sektorowego CSIRT KNF dla rynku finansowego. Rozwój tego rozwiązania jest finansowany ze środków Krajowego Planu Odbudowy i Zwiększania Odporności (KPO).

Znaczenie platformy moje.cert.pl wynika z prostego faktu: w środowisku, w którym ataki są szybkie, zautomatyzowane i wielokanałowe, przewagę obronną buduje nie tylko jakość zabezpieczeń w pojedynczej instytucji, ale przede wszystkim czas reakcji i przepływ informacji w skali całego sektora. Nawet najlepiej przygotowany podmiot może zostać osłabiony, jeśli ostrzeżenie o nowej kampanii, podatności lub schemacie oszustwa dotrze do niego zbyt późno. Moduł sektorowy ma ten dystans skracać dostarczając możliwie wczesne, uporządkowane i praktyczne informacje, które można szybko przełożyć na działania techniczne i operacyjne.

Rozbudowana platforma będzie wspierać procesy bezpieczeństwa na kilku poziomach. Po pierwsze, umożliwi bezpieczne i ustandaryzowane zgłaszanie incydentów oraz szybsze przekazywanie ostrzeżeń o aktywnych kampaniach wymierzonych w sektor. Po drugie, ma zwiększyć skuteczność analiz dzięki lepszej korelacji danych i uporządkowaniu informacji w jednolitym modelu raportowania. Po trzecie, poprawi koordynację działań międzyinstytucjonalnych, co jest szczególnie istotne przy incydentach o charakterze rozproszonym, kampaniach masowych oraz sytuacjach o podwyższonym ryzyku operacyjnym.

W praktyce oznacza to lepsze przygotowanie sektora na najczęściej obserwowane kategorie zagrożeń: phishing wielokanałowy, oszustwa inwestycyjne, malware uderzający w urządzenia końcowe klientów, a także incydenty wynikające z zależności technologicznych i biznesowych. Wspólny, sektorowy „punkt ciężkości” dla wymiany informacji pozwala ograniczać ryzyko efektu domina i wzmacniać odporność ekosystemu jako całości – zwłaszcza w przypadkach, w których atakujący testują podatność wielu instytucji równolegle, licząc na najsłabsze ogniwo.

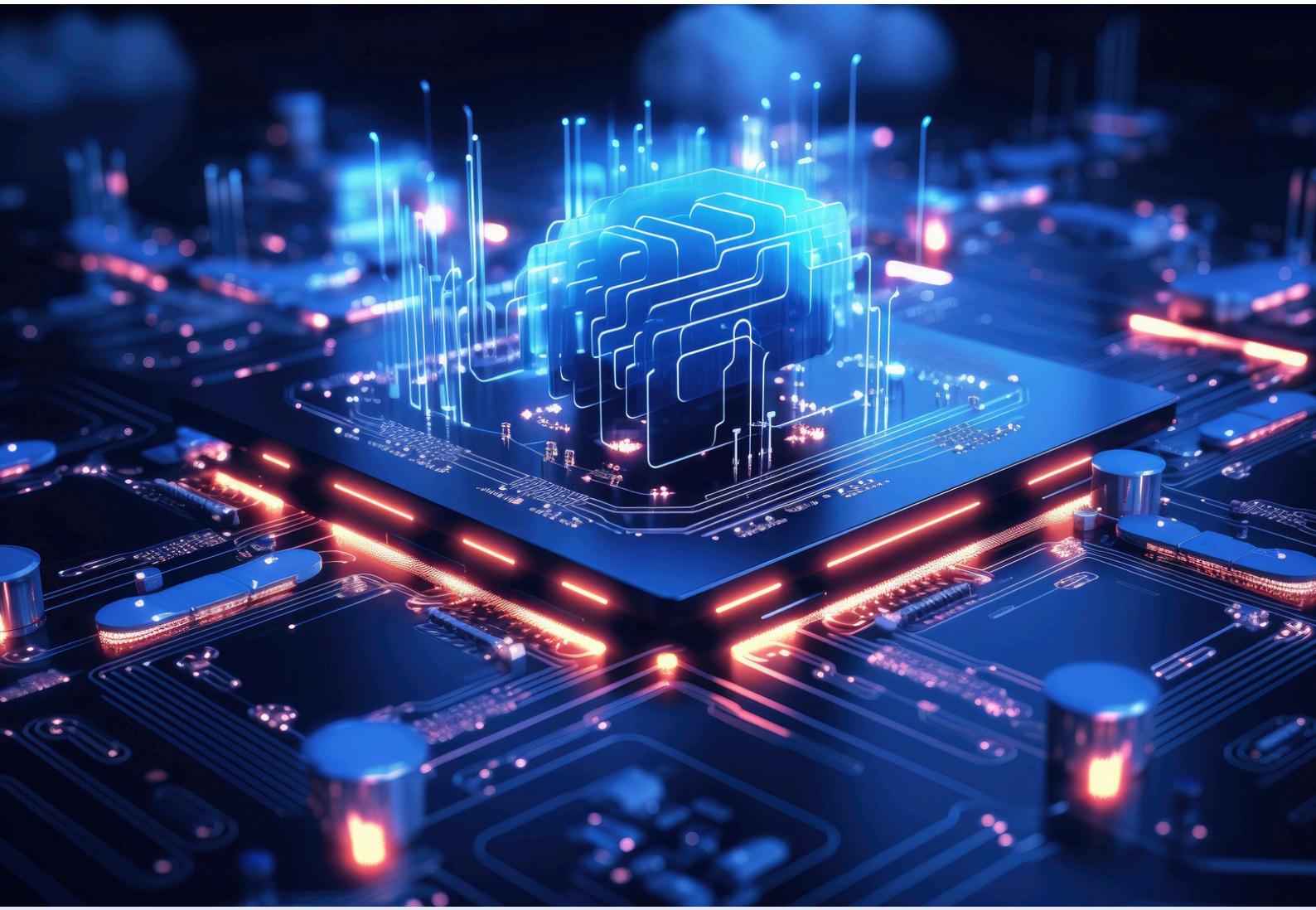
Z perspektywy CSIRT KNF, moduł sektorowy w moje.cert.pl to krok w stronę modelu, w którym obrona rynku finansowego opiera się na stałym, praktycznym współdzieleniu wiedzy, a nie wyłącznie na reakcji po fakcie. Platforma ma ułatwiać szybką dystrybucję rekomendacji, wspierać priorytetyzację ryzyka, a także wzmacniać świadomość zagrożeń wśród instytucji sektora. Ostatecznym beneficjentem tych działań są klienci – ponieważ krótszy czas detekcji i lepsza koordynacja reagowania bezpośrednio przekładają się na ograniczanie skutków incydentów i stabilność usług finansowych.

Rozwój moje.cert.pl w formule sektorowej wzmacnia więc nie tylko techniczne zdolności wykrywania i reagowania, ale także zaufanie do cyfrowych usług finansowych. W warunkach rosnącej skali transakcji zdalnych i wysokiej aktywności przestępczej jest to rozwiązanie, które realnie zwiększa bezpieczeństwo funkcjonowania rynku, umożliwiając szybsze, bardziej spójne i skuteczniejsze działania ochronne.

Grafika 53. Informacja o projekcie moje.cert.pl

Więcej informacji o projekcie dostępnych jest pod linkiem

3.6 WSPÓŁPRACA Z CSIRT-AMI POZIOMU KRAJOWEGO



Skuteczne zapewnienie cyberbezpieczeństwa opiera się na współpracy i sprawnym przepływie informacji pomiędzy CSIRT-ami poziomu krajowego a zespołami sektorowymi. To właśnie regularna wymiana wiedzy, obserwacji i doświadczeń pozwala szybciej identyfikować zagrożenia, trafniej oceniać ich znaczenie oraz skuteczniej koordynować działania ograniczające ryzyko. Rok 2025 po raz kolejny potwierdził, że dobrze zorganizowana współpraca międzyzespołowa ma bezpośredni wpływ na bezpieczeństwo i stabilność polskiego sektora finansowego. Poniżej przedstawiamy krótkie podsumowania przygotowane przez zespoły CSIRT poziomu krajowego – ich perspektywę na wspólne działania z CSIRT KNF oraz przykłady tego, co w minionym roku szczególnie wspierało efektywność naszej kooperacji.

C:[SIRT/MON

CSIRT MON

W 2025 roku współpraca CSIRT MON i CSIRT KNF miała przede wszystkim charakter praktyczny i operacyjny. Skupiała się na sprawnej wymianie informacji, weryfikacji obserwacji oraz szybkim przekazywaniu sygnałów o zagrożeniach, które mogą mieć znaczenie również dla rynku finansowego. W cyberbezpieczeństwie często decydują szczegóły, dlatego podstawą współdziałania była bezpośrednia komunikacja między wyznaczonymi punktami kontaktowymi w obu zespołach.

Na co dzień korzystaliśmy z kanału komunikacji, który umożliwiał przekazywanie krótkich obserwacji, pytań, uzgodnień oraz wskaźników kompromitacji (IoC) wymagających szybkiego potwierdzenia lub uzupełnienia. Taki model pozwalał sprawnie rozstrzygać, czy dany sygnał wymaga rejestracji incydentu, czy dalszego monitorowania, oraz ułatwiał wymianę informacji w tempie adekwatnym do dynamiki zagrożeń.

W 2025 roku w CSIRT MON zarejestrowano cztery incydenty związane z obszarem odpowiedzialności CSIRT KNF oraz przeprowadzono pięć wymian informacji z CSIRT KNF bez formalnego rejestrowania incydentu.

Wymieniane informacje dotyczyły zarówno bieżących zagrożeń typu „commodity", jak i zagrożeń powiązanych z działalnością grup APT. Wspólnym obszarem zainteresowania było również przekazywanie IoC związanych z kampaniami phishingowymi.

Istotnym elementem jest także ciągłość współpracy. W latach 2023-2024 CSIRT KNF oraz właściwe jednostki po stronie MON aktywnie współpracowały w zakresie rozpoznawania infrastruktury powiązanej z jedną z grup haktywistycznych prowadzących ataki typu DDoS. Pozyskane w ramach tej współpracy informacje są nadal wykorzystywane w mechanizmach informowania podmiotów KSC o aktywności tej grupy, wspierając szybsze rozpoznanie i przygotowanie do działań ochronnych.

Podsumowując w 2025 roku współpraca CSIRT MON i CSIRT KNF przebiegała sprawnie i miała wyraźny wymiar operacyjny, wspierając szybką wymianę informacji o zagrożeniach istotnych także dla rynku finansowego. W kolejnych latach planujemy ją dalej rozwijać poprzez cykliczne spotkania robocze oraz stopniowe zwiększanie automatyzacji wymiany informacji o zagrożeniach w oparciu o nowoczesne standardy. Dla utrzymania wysokiej jakości współdziałania rozważane jest także ujednolicenie zasad operacyjnych (m.in. eskalacja, minimalny zakres danych, dystrybucja IoC), przy zachowaniu zgodności z przepisami i standardami branżowymi.

CSIRT GOV

Zespół CSIRT GOV obserwował na przestrzeni 2025 roku stałą, wysoką ilość incydentów związanych z atakami socjotechnicznymi ukierunkowanymi bądź wykorzystującymi atrybuty (wizerunek, podobna domena – typosquatting) podmiotów sektora bankowego. Niezmiennymi motywami wykorzystywanymi na przestrzeni ostatnich lat pozostają reklamy dotyczące fałszywych inwestycji w przedsięwzięcia sektora bankowego, rządowe, czy podmiotów prywatnych. Nierzadko do legitymizacji rzekomych inwestycji wykorzystywany był wizerunek osób pełniących funkcje publiczne.

Dodatkowym, stałym zagrożeniem dla polskiego sektora finansowego są próby wykorzystywania – często krytycznych – podatności w powszechnie stosowanych komponentach oraz systemach teleinformatycznych. Coraz częściej można zauważyć masowe próby wykorzystania nowych podatności, w tym typu 0-day na popularne usługi, gdzie stale skraca się czas między pierwszymi doniesieniami o występowaniu podatności, a próbami jej wykorzystania.

Jednym z rosnących zagrożeń dla polskiego sektora finansowego mogą być grupy APT (Advanced Persistent Threat), których głównym celem jest zysk finansowy. Obecnie notuje się ich niewielką aktywność, natomiast prawdopodobnym jest jej zwiększenie w najbliższej przyszłości.

W związku z tym, jak zawsze, kluczowa pozostaje bliska współpraca oraz wymiana informacji o zagrożeniach w cyberprzestrzeni RP między podmiotami ustawy o krajowym systemie cyberbezpieczeństwa (KSC).

Zarówno przy wspomnianych, obserwowanych dotychczas wyzwaniach dla sektora finansowego RP, jak i rosnących zagrożeniach kluczowy jest niezmiennie szybki czas reakcji. Nieoceniona we wskazanych sytuacjach pozostaje bieżąca współpraca i wymiana informacji między zespołami CSIRT GOV, CSIRT KNF oraz pozostałymi podmiotami ustawy o KSC.

Współpraca CSIRT KNF i CSIRT NASK w zwalczaniu cyberzagrożeń

Jednym z najważniejszych czynników skutecznej współpracy pomiędzy zespołami CSIRT KNF i CSIRT NASK jest wysoki poziom komunikacji – zarówno w zakresie tempa wymiany informacji, jak i wzajemnego zaufania. Dzięki temu możliwe jest szybsze podejmowanie trafnych decyzji oraz realizacja celnych działań.

Z uwagi na sektorowy charakter CSIRT KNF, zespół ten pełni istotną rolę pojedynczego punktu kontaktowego pomiędzy CSIRT-em krajowym a podmiotami rynku finansowego. Realnie usprawnia to koordynację i przyspiesza reakcję na incydenty.

Przykłady korzyści z tej współpracy

- Zgłaszanie podejrzanych kont bankowych – informacje pozyskane przez CERT Polska trafiają za pośrednictwem CSIRT KNF szybciej do sektora bankowego w celu weryfikacji.

- Dystrybucja informacji o podatnościach – w przypadku wykrycia podatności o wysokim stopniu zagrożenia, CSIRT KNF umożliwia precyzyjne dotarcie do właściwych podmiotów w sektorze finansowym. W drugą stronę, w oparciu o rzetelne działania partnera, CSIRT NASK otrzymuje informacje o nowych kampaniach oraz wykrytych podatnych lub skutecznie zaatakowanych instancjach spoza właściwości CSIRT KNF. W oparciu o te dane uruchamiany jest skoordynowany proces obsługi.

Reakcja na incydenty o dużej skali – ubiegłoroczne ataki DDoS na uczestników sektora, a także ogólnopolski problem z płatnościami kartą potwierdziły, że szybki obieg informacji jest kluczowy i realnie służy CSIRT NASK dla potrzeb budowania pełnego obrazu sytuacyjnego na poziomie krajowym.

Wspólne działania w obszarze przeciwdziałania cyberzagrożeniom

Kolejny rok zespół CSIRT KNF zgłosił rekordową liczbę materiałów wykorzystywanych przez przestępców do wyłudzeń środków finansowych od obywateli Polski. Wszystkie te przypadki zostały odnotowane na Liście Ostrzeżeń CERT Polska[28]. Współpraca w tym zakresie nie ogranicza się jednak do zgłaszania domen. Dzięki ciągłej wymianie informacji o sposobach działania sprawców oraz wzajemnemu udostępnianiu technik i wskaźników, zespoły skuteczniej identyfikują nowe domeny i eliminują je, zanim dotrą do potencjalnych ofiar.

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

3.7 DZIAŁANIA EDUKACYJNE CSIRT KNF

Edukacja stanowi jeden z najważniejszych sposobów budowania odporności użytkowników Internetu na współczesne zagrożenia cybernetyczne. W obliczu stale rosnącej liczby ataków szczególnego znaczenia nabiera podnoszenie wiedzy i umiejętności uczestników rynku finansowego.

Zespół CSIRT KNF aktywnie uczestniczy w działaniach, których celem jest popularyzowanie wiedzy o cyberzagrożniach oraz wzmacnianie poziomu cyberbezpieczeństwa. W ramach projektu edukacyjnego Centrum Edukacji dla Uczestników Rynku – CEDUR w 2025 roku przedstawiciele CSIRT KNF wzięli udział w charakterze prelegentów w seminariach szkoleniowych (webinariach) skierowanych do różnych grup odbiorców m.in.:
1) uczniów szkół podstawowych i ponadpodstawowych oraz nauczycieli
2) seniorów oraz ich opiekunów
3) przedstawicieli instytucji ochrony praw nieprofesjonalnych uczestników rynku finansowego, w tym miejskich i powiatowych rzeczników konsumentów
4) pracowników banków komercyjnych i banków spółdzielczych
5) pracowników instytucji finansowych obsługujących klientów bankowości internetowej oraz osób zainteresowanych tematyką cyberbezpieczeństwa
6) indywidualnych uczestników rynku finansowego, w tym inwestorów

Wśród spotkań wymienić można m.in.:

a) webinaria CEDUR zorganizowane w ramach 13. edycji kampanii Global Money Week (GMW) – Światowy Tydzień Pieniądza[29], skierowane do uczniów szkół podstawowych i ponadpodstawowych oraz nauczycieli:

- „Cyberprzestępcy w świecie finansów", którego celem było zwiększenie poziomu świadomości odnośnie do działań cyberoszustów w Internecie, a także zaprezentowanie dobrych praktyk mogących uchronić przed kradzieżą środków finansowych
- „Bezpieczny telefon – jak chronić się przed cyberprzestępcami", podczas którego przedstawiono problematykę zagrożeń cyberbezpieczeństwa dla środków finansowych użytkowników urządzeń mobilnych

[29] UKNF jest krajowym koordynatorem międzynarodowych kampanii Global Money Week (GMW) i World Inwestor Week (WIW).

b) webinaria CEDUR zorganizowane w ramach kampanii World Inwestor Week (WIW) – Światowy Tydzień Inwestora[30], skierowane do uczniów szkół ponadpodstawowych i nauczycieli oraz do indywidualnych uczestników rynku finansowego:

- „Cyberbezpieczeństwo z perspektywy klienta usług finansowych – aspekty praktyczne", którego celem było zwiększenie poziomu świadomości odnośnie do działań cyberoszustów w Internecie, a także zaprezentowanie dobrych praktyk mogących uchronić przed kradzieżą środków finansowych

- „Cyberbezpieczeństwo – pułapki czyhające na młodzież i jak się przed nimi chronić", podczas webinarium przedstawiono praktyczną problematykę cyberbezpieczeństwa w sektorze finansowym z uwzględnieniem obserwowanych cyberzagrożeń nakierowanych na młodzież

- Prezentacja „Jak poprawić swoje bezpieczeństwo w sieci" podczas Dnia Edukacji Finansowej w ramach kampanii World Investor Weeek, gdzie przybliżono najpopularniejsze metody oszustw stosowanych przez cyberprzestępców oraz wskazano sposoby służące poprawie swojego bezpieczeństwa w sieci

c) webinaria CEDUR dla seniorów i ich opiekunów:

- „Bezpieczny senior – jak nie dać się oszukać w Internecie", webinarium miało na celu zwiększenie świadomości i uwrażliwienie tej grupy społecznej jako szczególnie narażonej na działania cyberprzestępców
- „Bezpieczne płatności w Internecie dla seniorów" (w 3 terminach), którego celem było zwiększenie świadomości seniorów i ich opiekunów w zakresie aktualnych zagrożeń spowodowanych działalnością cyberprzestępców.

[30] UKNF jest krajowym koordynatorem międzynarodowych kampanii Global Money Week (GMW) i World Inwestor Week (WIW).

Podczas szkoleń omówiono najpopularniejsze metody ataków na środki finansowe użytkowników Internetu i urządzeń mobilnych oraz dobre praktyki służące poprawie bezpieczeństwa w sieci na przykładach dopasowanych do perspektywy poszczególnych grup odbiorców. Przy organizacji webinariów skierowanych m.in. do seniorów i ich opiekunów UKNF współpracował z Komendą Główną Policji oraz Ministrem do spraw Polityki Senioralnej.

Udział w inicjatywach szkoleniowych, w tym webinariach CEDUR, był bezpłatny.

Informacje o webinariach CEDUR są dostępne pod adresem

Przedstawiciele zespołu CSIRT KNF w 2025 roku uczestniczyli również w konferencjach i wydarzeniach poświęconych tematyce cyberbezpieczeństwa m.in.:

- Konferencja „Bezpieczna szkoła w cyfrowym świecie – wyzwania i rozwiązania” – 26 marca 2025 roku w Centrum Edukacji Nauczycieli w Białymstoku zorganizowano wojewódzką konferencję „Bezpieczna szkoła w cyfrowym świecie – wyzwania i rozwiązania”. W wydarzeniu uczestniczyli nauczyciele, dyrektorzy szkół, pedagodzy, psycholodzy oraz specjaliści zajmujący się edukacją i bezpieczeństwem młodych osób. Spotkanie miało na celu zwrócenie uwagi na nowe zagrożenia związane z funkcjonowaniem uczniów w świecie cyfrowym oraz przedstawienie konkretnych narzędzi i działań, które mogą wspierać ich bezpieczeństwo w sieci. Podczas konferencji przedstawiciele CSIRT KNF zaprezentowali praktyczne metody ochrony przed kradzieżą danych i różnego rodzaju cyberatakami. Konferencja była również ważnym forum wymiany poglądów i doświadczeń, pozwalając uczestnikom zastanowić się nad tym, jak szkoła może skutecznie przygotowywać młodzież do odpowiedzialnego i świadomego korzystania z technologii.

- Szkolenie pt. „Innowacje i cyberbezpieczeństwo na rynku finansowym" – w ramach projektu Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego (CEBRF) zorganizowano serię szkoleń dla uczniów szkół ponadpodstawowych. Ich głównym celem było przybliżenie kluczowych zasad bezpiecznego korzystania z Internetu oraz usług finansowych. Uczestnikom przedstawiono najczęściej spotykane metody oszustw zakupowych oraz prób wyłudzeń przy wykorzystaniu fałszywych witryn bankowości elektronicznej. Wyjaśniono również, w jaki sposób działają cyberprzestępcy oraz jak rozpoznawać potencjalne zagrożenia.

- Cyberbezpieczne lekcje o finansach dla młodzieży – 20 marca w Szkole Podstawowej nr 2 im. Kornela Makuszyńskiego w Pruszkowie odbyło się szkolenie, które poświęcone było innowacjom finansowym, cyberbezpieczeństwu oraz zagadnieniom związanym z dezinformacją. Wydarzenie zgromadziło uczniów z Pruszkowa oraz pobliskich liceów. Jedna z części warsztatowych skupiała się na bezpieczeństwie cyfrowym w obszarze finansów. Katarzyna Bartnik, przedstawicielka CSIRT KNF, omówiła najczęściej występujące zagrożenia internetowe, schematy działania cyberprzestępców oraz praktyczne metody ochrony przed różnymi formami oszustw.

- Udział w posiedzeniu Rady ds. Polityki Senioralnej – Karol Paciorek, kierownik CSIRT KNF, wraz z przedstawicielem Departamentu Bankowości Komercyjnej w UKNF uczestniczyli w posiedzeniu Rady ds. Polityki Senioralnej. Podczas spotkania przybliżone zostały najpopularniejsze metody cyberataków, z którymi mierzą się seniorzy. Zaakcentowano także zagrożenie jakim są oferty fałszywych inwestycji i wskazano na dobre praktyki służące poprawie bezpieczeństwa w Internecie.

- W materiale opublikowanym przez CyberDefence24 „Jak cyberprzestępcy czyszczą nasze konta" Karol Paciorek, kierownik CSIRT KNF, opowiedział o najpopularniejszych metodach i technikach stosowanych przez cyberprzestępców, a także wskazał na dobre praktyki służące poprawie bezpieczeństwa podczas korzystania z Internetu.

- Cyber24 Day – podczas kolejnej edycji konferencji Cyber24 Day Karol Paciorek, kierownik zespołu CSIRT KNF, wziął udział w panelu poświęconym wyzwaniom i trendom związanym z bezpieczeństwem w cyfrowych finansach. Podzielił się doświadczeniami z obszaru ochrony rynku finansowego przed cyberzagrożeniami oraz przedstawił rolę CSIRT KNF w budowaniu odporności instytucji i ochronie odbiorców usług bezgotówkowych.
  Podczas panelu eksperci rozmawiali o:
  a) nowych metodach oszustw i cyberataków,
  b) rozwiązaniach zwiększających bezpieczeństwo płatności elektronicznych,
  c) roli współpracy między instytucjami w ochronie oszczędności Polaków.

- Konferencja „Lubelskie Cyberbezpieczne" – 16 października Michał Strzelczyk, przedstawiciel CSIRT KNF, uczestniczył w konferencji organizowanej przez Urząd Marszałkowski Województwa Lubelskiego w Lublinie, Centralne Biuro Zwalczania Cyberprzestępczości, Lubelskie Centrum Innowacji i Technologii oraz LCK Lubelskie. Podczas prezentacji przybliżył oblicza przestępczości finansowej, a także wskazał na możliwe sposoby ich wykrywania.

- Europejski Miesiąc Cyberbezpieczeństwa – w ramach kampanii edukacyjnej CSIRT KNF skupił się na ochronie finansów i danych osobowych użytkowników w Internecie. Podczas całego miesiąca publikowane były w mediach społecznościowych praktyczne porady oraz infografiki, które miały na celu ostrzeżenie przed najczęstszymi zagrożeniami w cyberprzestrzeni. Opracowane materiały dotyczyły tego, jak skutecznie chronić konta bankowe oraz rozpoznawać podejrzane próby wyłudzenia informacji, minimalizując ryzyko kradzieży danych czy środków finansowych.

- Partnerstwo dla Cyberbezpieczeństwa – zespół CSIRT KNF współpracuje z podmiotami i organizacjami rozwijającymi kompetencje w dziedzinie cyberbezpieczeństwa oraz udziela im wsparcia. W ramach programu Partnerstwo dla Cyberbezpieczeństwa (PdC) – stworzonego z inicjatywy NASK – Państwowego Instytutu Badawczego oraz Ministerstwa Cyfryzacji i służącego jako platforma do wymiany informacji o zagrożeniach cybernetycznych – przedstawiciele CSIRT omówili zagadnienia związane z ciągłością działania na rynku finansowym, a także przybliżyli krajobraz cyberzagrożeń oraz wskazali na najpopularniejsze metody oszustw stosowane przez cyberprzestępców.

- Sesja szkoleniowa dla Sióstr ekonomek żeńskich zgromadzeń zakonnych – w związku z coraz powszechniejszymi atakami wymierzonymi w użytkowników cyberprzestrzeni przeprowadzona została sesja szkoleniowa dla Sióstr ekonomek żeńskich zgromadzeń zakonnych, podczas której wskazano na problematykę zagrożeń cyberbezpieczeństwa i możliwe sposoby ochrony.

- CyberDay – przedstawiciele CSIRT KNF uczestniczyli także w wydarzeniu poświęconym budowaniu świadomości w zakresie cyberbezpieczeństwa, organizowanym przez Bank Gospodarstwa Krajowego. Podczas prezentacji przybliżony został krajobraz zagrożeń w sektorze finansowym, a także omówiono metody i sposoby działań stosowanych przez cyberprzestępców.

- Wywiad dla CyberDefence24 – w odcinku CyberDefence24 z cyklu „Cyberbezpiecznie jak w banku" Karol Paciorek, kierownik CSIRT KNF, przybliżył najpopularniejsze metody oszustw stosowane przez cyberprzestępców podczas Black Week oraz dobre praktyki pozwalające na bezpieczne zakupy w sieci.

- KSC-EXE 2025 – przedstawiciele Urzędu Komisji Nadzoru Finansowego, pełniącego rolę organu właściwego, oraz CSIRT KNF – sektorowy zespół cyberbezpieczeństwa sektora finansowego – uczestniczyli w ćwiczeniach krajowego systemu cyberbezpieczeństwa KSC-EXE 2025. Podczas ćwiczeń sprawdzano m.in.:
  a) skuteczność procedur reagowania na incydenty,
  b) szybkość i jakość komunikacji pomiędzy instytucjami,
  c) koordynację działań w sytuacjach kryzysowych.

Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego (CEBRF)

Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego (CEBRF) powołane zostało przez Urząd Komisji Nadzoru Finansowego i działający w jego strukturach Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego w polskim sektorze finansowym (CSIRT KNF). Główną misją Centrum Edukacji jest realizacja działań informacyjno-edukacyjnych oraz popularyzowanie wiedzy z zakresu bezpieczeństwa finansowego. Cyberprzestępcy nieustannie wymyślają nowe sposoby oszustw internetowych. Bardzo ważnym jest, aby poza blokowaniem fałszywych domen czy zgłaszaniem niebezpiecznych reklam, prowadzić także działania edukacyjne mające na celu poprawę świadomości wśród użytkowników cyberprzestrzeni. Na stronie internetowej zamieszczane są publikacje dotyczące bieżących zagrożeń w cyberprzestrzeni oraz stosowanych przez oszustów metod działania.

Publikacje CEBRF

Zespół CSIRT KNF na bieżąco monitoruje i identyfiikuje występujące zagrożenia w cyberprzestrzeni. W ramach działalności edukacyjnej w 2025 roku opublikowane zostały następujące materiały:

- „Krajobraz zagrożeń w polskim sektorze finansowym 2025 (GTL)" – w dokumencie przeprowadzono kompleksowy przegląd kluczowych zagrożeń dla sektora finansowego. Każda sekcja zawiera metody ataków, przykłady incydentów oraz motywacje cyberprzestępców. Celem jest dostarczenie wszechstronnych informacji, które pozwolą na przygotowanie się do obrony przed zagrożeniami.

Z dokumentem można zapoznać się pod tym linkiem

- „Analiza złośliwej aplikacji mobilnej IKO Lokata” – w materiale przeprowadzno analizę kampanii zaobserwowanej przez zespół CSIRT KNF na portalu Facebook, w której cyberprzestępcy publikowali fałszywe reklamy zachęcające do pobrania złośliwego oprogramowania podszywającego się pod nieistniejącą aplikację „IKO Lokata”. Kampania wycelowana była w użytkowników urządzeń mobilnych z systemem Android.

Z analizą kampanii oraz z potencjalnymi konsekwencjami zainstalowania złośliwej aplikacji na urządzeniu można zapoznać się tutaj:

- „Przegląd wybranych oszustw internetowych” – comiesięczny cykl artykułów opisujących najnowsze zagrożenia i metody ataków stosowane przez cyberprzestępców, zidentyfikowane przez CSIRT KNF.

Z comiesięcznymi przeglądami wybranych oszustw internetowych opracowanymi przez CSIRT KNF można zapoznać się tutaj:

- Przegląd oszustw internetowych styczeń 2025
- Przegląd oszustw internetowych luty 2025
- Przegląd oszustw internetowych marzec 2025

- Przegląd oszustw internetowych kwiecień 2025
- Przegląd oszustw internetowych maj 2025
- Przegląd oszustw internetowych czerwiec 2025
- Przegląd oszustw internetowych lipiec 2025
- Przegląd oszustw internetowych sierpień 2025
- Przegląd oszustw internetowych wrzesień 2025
- Przegląd oszustw internetowych październik 2025
- Przegląd oszustw internetowych listopad 2025
- Przegląd oszustw internetowych grudzień 2025

Aktywność CSIRT KNF w mediach społecznościowych

Jednym z kluczowych obszarów działalności zespołu CSIRT KNF jest upowszechnianie wiedzy na temat aktualnych zagrożeń cybernetycznych. W tym celu wykorzystywane są przede wszystkim media społecznościowe, które umożliwiają szybkie reagowanie na pojawiające się zagrożenia oraz skuteczne docieranie do odbiorców. Publikowane komunikaty trafiają następnie do obiegu medialnego i są wykorzystywane przez liczne portale informacyjne oraz branżowe. W 2025 roku przełożyło się to na 1995 publikacji prasowych opartych na informacjach przekazywanych przez CSIRT KNF.

Aktywność zespołu w przestrzeni internetowej koncentrowała się na regularnym udostępnianiu ostrzeżeń oraz materiałów edukacyjnych dotyczących działalności cyberprzestępców. W analizowanym roku opublikowano 177 wpisów, których celem było zwiększenie świadomości użytkowników w zakresie bezpieczeństwa cyfrowego oraz ograniczenie ryzyka strat finansowych.

Najczęściej sygnalizowane zagrożenia obejmowały próby podszywania się pod instytucje finansowe, wykorzystanie złośliwego oprogramowania do przejmowania środków pieniężnych, fałszywe oferty inwestycyjne służące wyłudzaniu danych osobowych, a także spreparowane serwisy sprzedażowe mające na celu pozyskanie informacji o kartach płatniczych.

Zachęcamy do obserowania kont CSIRT KNF w serwisach Twitter/X, LinkedIn oraz Facebook, gdzie na bieżąco informujemy o nowych sposobach działania cyberprzestępców.

KONTAKT

Urząd Komisji Nadzoru Finansowego

Departament Cyberbezpieczeństwa – CSIRT KNF

ul. Piękna 20,
00-549 Warszawa

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