KNF CSIRT

RAPORT ROCZNY CSIRT KNF

2024

Spis treści

SPIS TREŚCI

01.
Wstęp (str. 3-6)

02.
Statystyki z działalności CSIRT KNF (str. 7-13)

03.
Fałszywe inwestycje – dominujące zagrożenie 2024 (str. 14-24)

04.
Fałszywe ankiety – rosnące zagrożenie (str. 25-30)

05.
Oszustwa kurierskie i pocztowe (str. 31-36)

06.
Oszustwa bankowe – podszywanie się pod instytucje finansowe (str. 37-43)

SPIS TREŚCI

07.
Złośliwe oprogramowanie
(str. 44-50)

08.
Publikacje: analizy, opracowania, raporty
(str. 51-56)

09.
Wybrane podatności w systemach informatycznych w 2024 roku
(str. 57-61)

10.
Działalność edukacyjna CSIRT KNF
(str. 62-65)

11.
Rok 2024 pod hasłem „DORA”
(str. 66-67)

01.
WSTĘP

WSTĘP

Zespół CSIRT KNF, jako sektorowy zespół cyberbezpieczeństwa dla rynku finansowego, działa w strukturach Urzędu Komisji Nadzoru Finansowego, w ramach ustawy o Krajowym Systemie Cyberbezpieczeństwa.

W ramach naszych działań koordynujemy obsługę zagrożeń i incydentów poważnych w podmiotach z sektora finansowego. Do głównych zadań zespołu należy monitorowanie i analiza działań cyberprzestępców wyłudzających środki finansowe. W ramach pracy operacyjnej wykrywamy i blokujemy strony o charakterze oszukańczym. Analizujemy także złośliwe oprogramowanie w kontekście bezpieczeństwa środków finansowych. Poprawa poziomu świadomości użytkowników odnośnie do zagrożeń w cyberprzestrzeni jest istotnym elementem działalności CSIRT KNF.

W Raporcie Rocznym CSIRT KNF 2024, poświęconym analizie zagrożeń cyberbezpieczeństwa w sektorze finansowym, opracowanym z perspektywy sektorowego zespołu CSIRT KNF, omawiamy różne aspekty zagrożeń, z którymi mierzyli się zarówno profesjonalni, jak i nieprofesjonalni uczestnicy rynku finansowego. Mamy nadzieję, że raport okaże się wartościowym źródłem informacji dla wszystkich zainteresowanych zagadnieniami związanymi z zagrożeniami i cyberbezpieczeństwem w obszarze finansów.

W 2024 roku obserwowaliśmy liczne kampanie, których celem była kradzież środków finansowych uczestników rynku finansowego. Metody i techniki socjotechniczne stosowane przez grupy przestępcze z roku na rok stają się coraz bardziej wyrafinowane, co pozwala na skuteczne wpływanie na działania użytkowników.

W 2024 roku dominujące zagrożenie stanowiły oferty fałszywych inwestycji dystrybuowane za pośrednictwem nośników reklamowych w popularnych serwisach społecznościowych, wyszukiwarkach czy serwisach internetowych. W raporcie prezentujemy najczęstsze metody ataków i cyberoszustw stosowanych przez cyberprzestępców w 2024 roku.

Działania edukacyjne, mające na celu wzrost świadomości odnośnie do zagrożeń w cyberprzestrzeni, są istotnym elementem działalności CSIRT KNF. W raporcie omawiamy liczne działania edukacyjne zrealizowane w 2024 roku. Raport zawiera także analizy techniczne, które publikowane były na przestrzeni całego roku.

W 2024 roku CSIRT KNF odnotował rekordową liczbę wykrytych niebezpiecznych domen (**51 241**) i zgłosił je do CERT Polska w celu zablokowania. Za pośrednictwem złośliwych domen wykradano m.in.:

- dane do logowania do bankowości elektronicznej,
- informacje o kartach płatniczych,
- dane osobowe.

🔍 **Kluczowe liczby:**

- Na listę ostrzeżeń CERT Polska w 2024 roku wpisanych zostało **92 279** niebezpiecznych domen.
- CSIRT KNF zgłosił o **70,9%** więcej domen niż w 2023 roku (wzrost z **30 140** do **51 241**). Takie strony zidentyfikowane przez CSIRT KNF zgłaszane są do CSIRT NASK, w celu ich zablokowania poprzez wpisanie na listę ostrzeżeń[1].

📈 **Analiza trendów 2021-2024:**

- 2021: 11 468 domen
- 2022: 17 200 domen
- 2023: 30 140 domen
- 2024: 51 241 domen

Ten czterokrotny wzrost w ciągu ostatnich lat jasno pokazuje intensyfikację działań cyberprzestępców (wykres 4).

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

🎯 **Główne kategorie ataków w 2024 roku:**

- Fałszywe inwestycje: 45 985 domen (89,4%)
- Fałszywe ankiety: 4030 domen
- Usługi kurierskie/pocztowe: 521 domen
- Portale społecznościowe: 166 domen
- Fałszywe bramki płatności: 125 domen

👥 **Analiza socjotechniczna – wykorzystywane wizerunki:**

- Politycy: 26%
- Inne: 19%
- Celebryci: 14%
- Odzyskanie środków: 11%
- Spółki Skarbu Państwa: 11%
- Baltic Pipe: 7%
- Przedsiębiorcy: 6%
- Influencerzy: 4%
- Bankowe: 1%
- Tesla: 1%

🛡️ **Kluczowe wyzwania:**

- Znaczny wzrost liczby fałszywych domen inwestycyjnych.
- Profesjonalizacja działań przestępczych.
- Szybka adaptacja przestępców do wdrażanych zabezpieczeń.
- Umiejętność wykorzystania przez przestępców metod socjotechnicznych.
- Umiejętność dostosowania się przez cyberprzestępców do panującej sytuacji w kraju i na świecie.

⚡ **Wnioski:**

- Rok 2024 pokazał bezprecedensowy wzrost ataków phishingowych.
- Jednymi z najczęściej występujących oszustw były fałszywe inwestycje.
- Wykorzystywanie wizerunku znanych osób i marek pozostaje główną taktyką socjotechniczną.
- Konieczne jest dalsze wzmacnianie mechanizmów ochrony i edukacji użytkowników.

02. STATYSTYKI Z DZIAŁALNOŚCI CSIRT KNF

STATYSTYKI Z DZIAŁALNOŚCI CSIRT KNF

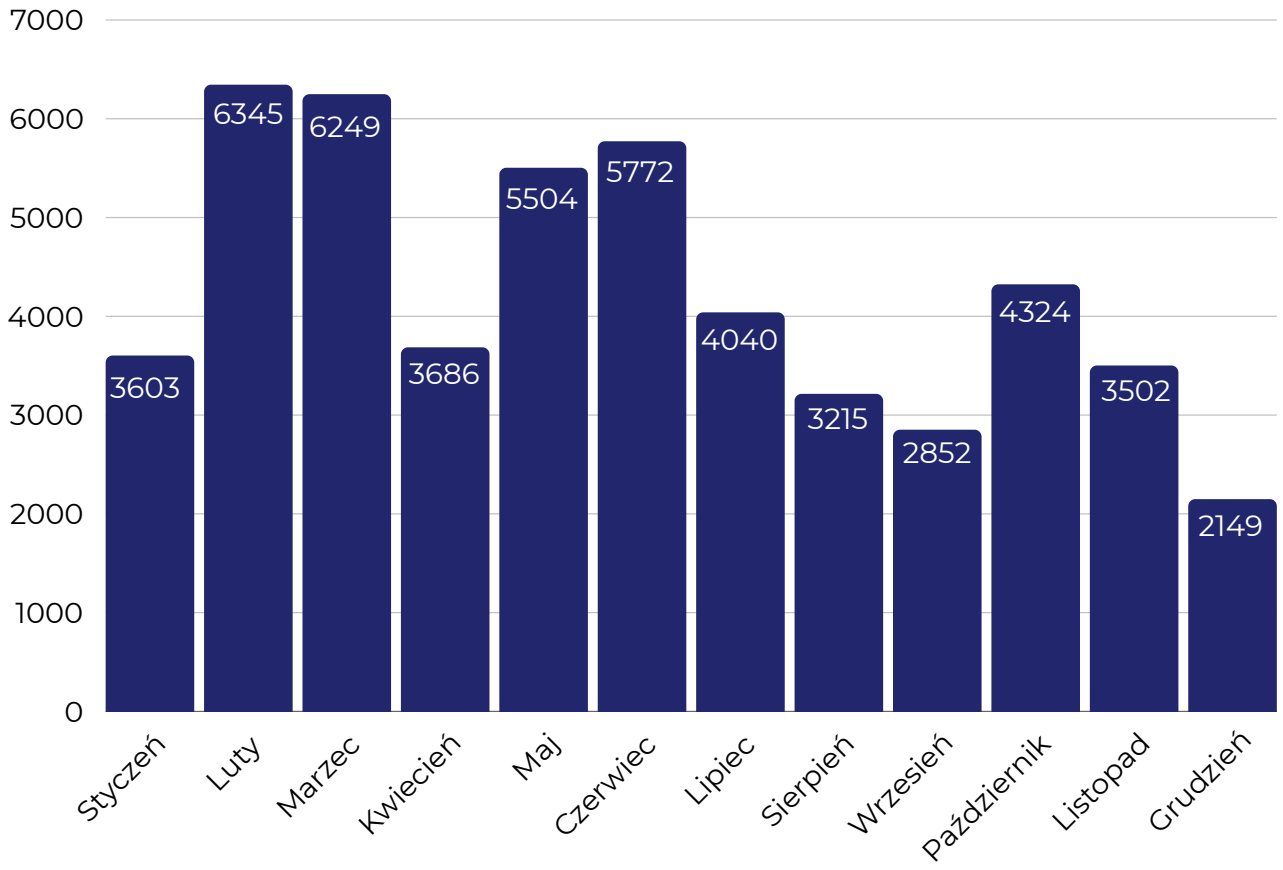
Jednym z głównych zadań zespołu CSIRT KNF jest bieżąca analiza i monitorowanie pojawiających się zagrożeń w obszarze cyberbezpieczeństwa, w szczególności tych dotyczących klientów rynku finansowego. Uzyskane w ten sposób informacje wykorzystywane są do działań zapobiegających incydentom w podmiotach rynku finansowego oraz działań edukacyjnych podnoszących świadomość klientów bankowości elektronicznej w zakresie cyberbezpieczeństwa.

Działania te obejmują przede wszystkim szybką identyfikację oraz ograniczanie dostępu do fałszywych stron internetowych. Niebezpieczne strony wykrywane przez CSIRT KNF zgłaszane są do CSIRT NASK, gdzie dokonywana jest ich blokada za pośrednictwem wpisania na listę ostrzeżeń.

Domeny phishingowe

Coraz większą skalę niebezpieczeństw, z którymi mierzą się użytkownicy cyberprzestrzeni, ukazuje rosnąca liczba wykrywanych przez CSIRT KNF domen phishingowych. Liczba zidentyfikowanych, oszukańczych domen wzrosła z **17 200** w 2022 roku do **30 140** w 2023 roku oraz do **51 241** w 2024 roku.

Domeny zgłoszone do CSIRT NASK przez CSIRT KNF w 2024 roku w poszczególnych miesiącach



Wykres 1. Domeny zgłoszone do CSIRT NASK przez CSIRT KNF w 2024 roku w poszczególnych miesiącach

Zespół CSIRT KNF w 2024 roku zgłosił do zablokowania **51 241** domen phishingowych (wykres 2).

Wykres 2. Liczba zgłoszonych domen phishingowych w latach 2021 - 2024 przez CSIRT KNF

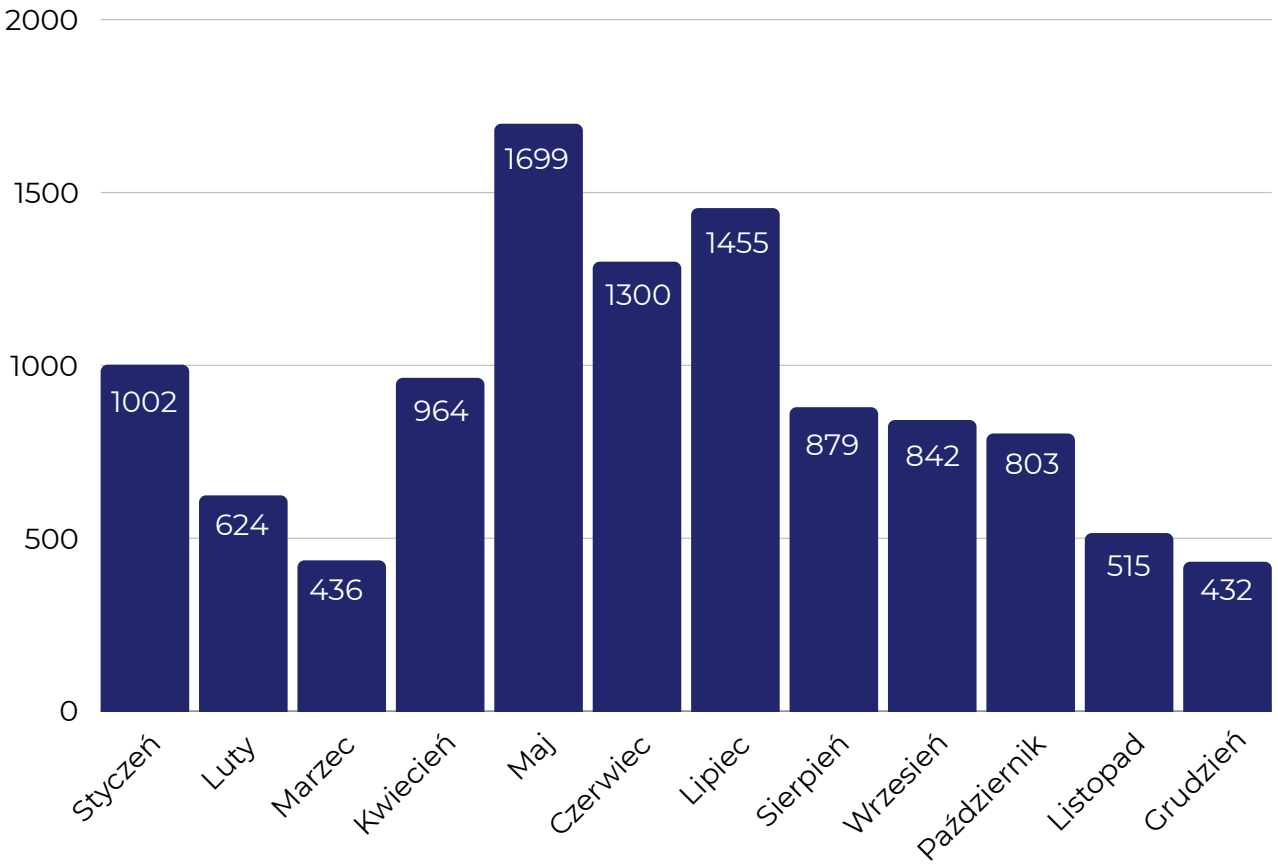
Reklamy w mediach społecznościowych

CSIRT KNF współpracuje z wieloma instytucjami i organizacjami na arenie krajowej i międzynarodowej, wymieniając informacje i koordynując działania przeciwdziałające oszustwom. W związku ze znaczącą liczbą fałszywych reklam publikowanych na portalu Facebook, CSIRT KNF wypracował mechanizmy wykrywające takie działania przestępcze oraz procesy przekazywania fałszywych reklam do blokady.

Wykorzystując udostępnioną przez portal Facebook bibliotekę reklam oraz inne narzędzia i zasoby poszczególnych portali mediów społecznościowych, CSIRT KNF wyszukuje i analizuje tego typu akcje reklamowe.

W 2024 roku CSIRT KNF zgłosił do zablokowania **10 951** oszukańczych reklam w mediach społecznościowych. Zgromadzone dane miesięczne pokazują zmienność w liczbie wyświetlanych fałszywych reklam na portalu Facebook. Najwięcej reklam tego typu odnotowano w maju i w lipcu, z kolei najmniej było ich w marcu i w grudniu.

Reklamy zgłoszone do zablokowania w 2024 roku

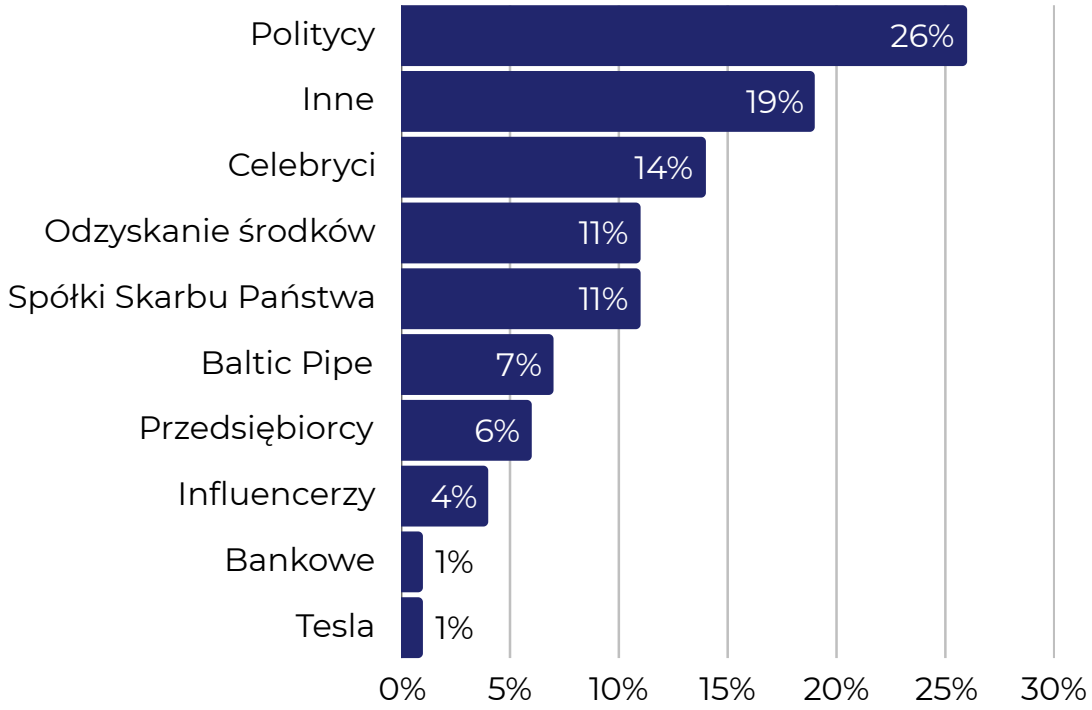


Wykres 3. Reklamy zgłoszone do zablokowania w 2024 roku

Wykorzystywane wizerunki

Zespół CSIRT KNF zgłosił do CSIRT NASK w 2024 roku aż **45 985** niebezpiecznych domen, które związane były z **fałszywymi inwestycjami**. Domeny te wpisane zostały na listę ostrzeżeń prowadzoną przez CSIRT NASK.

Reklamy fałszywych inwestycji identyfikowane przez CSIRT KNF stanowią jedno z głównych zagrożeń wymierzonych w użytkowników rynku finansowego w Polsce. Ten rodzaj ataku polega na zachęceniu ofiary do zainwestowania swoich oszczędności w projekty lub produkty inwestycyjne, które w rzeczywistości nie istnieją. O tym, jak przebiega oszustwo „na fałszywą inwestycję" opisujemy w rozdziale „Fałszywe inwestycje – dominujące zagrożenie 2024".



Wykres 4. Wykorzystywane wizerunki w reklamach fałszywych inwestycji w 2024 roku

Najwięcej przypadków oszustw inwestycyjnych wiązało się z wykorzystywaniem wizerunku polityków. Przestępcy bardzo często podszywali się również pod celebrytów. Dużą część reklam fałszywych inwestycji stanowiły także oszustwa związane z wykorzystaniem motywu odzyskania utraconych środków. Spora część reklam dotyczyła wykorzystania wizerunków spółek Skarbu Państwa. Najmniejszy odsetek stanowiły zaś przestępstwa, w których cyberprzestępcy wykorzystywali wizerunek influencerów, instytucji bankowych czy przedsiębiorstwa Tesla (wykres 4).

03. FAŁSZYWE INWESTYCJE - DOMINUJĄCE ZAGROŻENIE 2024

FAŁSZYWE INWESTYCJE - DOMINUJĄCE ZAGROŻENIE 2024

Skala zjawiska

W 2024 roku CSIRT KNF zidentyfikował i zgłosił do blokady **45 985** domen związanych z fałszywymi inwestycjami, co stanowi **89,4%** wszystkich zgłoszonych domen. Liczby te nie tylko obrazują skalę problemu, ale również wskazują na znaczące nasilenie tego rodzaju oszustwa w porównaniu z latami poprzednimi. Fałszywe inwestycje stały się najbardziej powszechnym i szkodliwym typem oszustw w Polsce, skutkując ogromnymi stratami finansowymi i społecznymi. Oszuści stale doskonalą swoje metody, co wymaga ciągłej adaptacji i rozwoju mechanizmów obronnych.

Charakterystyka ataków

Przestępcy w atakach wykorzystywali zaawansowane techniki socjotechniczne, budując fałszywe platformy inwestycyjne, które charakteryzowały się:

- profesjonalnym wyglądem stron internetowych, imitującym oficjalne serwisy inwestycyjne,
- sfałszowanymi historiami transakcji i wykresami,
- systemami referencyjnymi zachęcającymi do polecania platformy znajomym,
- fałszywymi opiniami i rekomendacjami,
- złożonymi systemami uwierzytelniania imitującymi prawdziwe platformy.

Wykorzystywane wizerunki

Analiza kampanii tworzonych przez cyberoszustów wykazała zróżnicowane strategie ich działania. Przestępcy celowo wykorzystują wizerunki osób i instytucji budzących zaufanie w społeczeństwie. Najczęściej wykorzystywane wizerunki to:

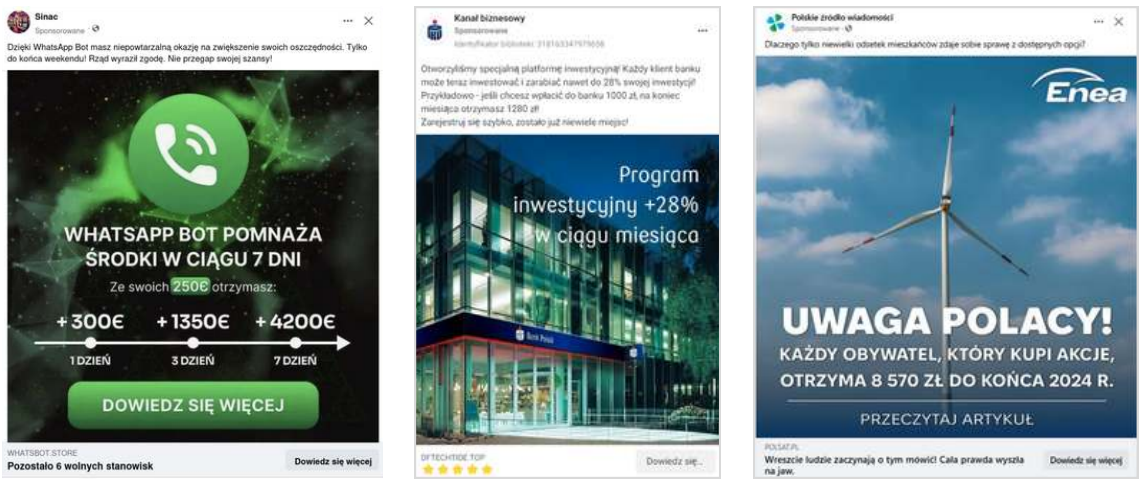
- **politycy** (26%) – najczęściej wykorzystywany wizerunek ze względu na rozpoznawalność i zaufanie społeczne,
- **celebryci** (w tym influencerzy) (14%) – wykorzystywani do oszukiwania młodszych użytkowników,
- **spółki Skarbu Państwa** (11%) – uwiarygodnienie poprzez powiązanie z instytucjami państwowymi,
- **Baltic Pipe** (7%) – wykorzystanie znaczącego projektu infrastrukturalnego,
- **przedsiębiorcy** (6%) – bazowanie na autorytecie biznesowym.

Mechanizmy oszustwa
Przestępcy stosują wieloetapowe schematy działania:

1. Etap wstępny:

- Targetowane reklamy w mediach społecznościowych, które wykorzystywały algorytmy do precyzyjnego docierania do potencjalnych ofiar ataku. Cyberprzestępcy w tworzonych reklamach podszywali się pod znane osoby, instytucje, spółki Skarbu Państwa czy podmioty z sektora finansowego (grafika 1-2).

Grafika 1. Przykłady reklam fałszywych inwestycji, które publikowali cyberprzestępcy



Grafika 2. Przykłady reklam fałszywych inwestycji, które publikowali cyberprzestępcy

Przestępcy w 2024 roku chętnie wykorzystywali technologię deepfake do tworzenia materiałów oszukańczych. Podszywali się pod znane osoby, generując nagrania video, na których przedstawiona była treść zachęcająca do rzekomych inwestycji. W pierwszej połowie 2024 roku zespół CSIRT KNF zaobserwował, że przestępcy nakładali na nagrania modyfikacje graficzne (grafika 3-4). Działania te mogły wynikać z chęci ukrycia nagrań przed detektorami implementowanymi na portalach społecznościowych. Fałszywe oferty (zarówno w postaci nagrań video, jak i statycznych reklam) dystrybuowane były m.in. poprzez reklamy na portalu Facebook.

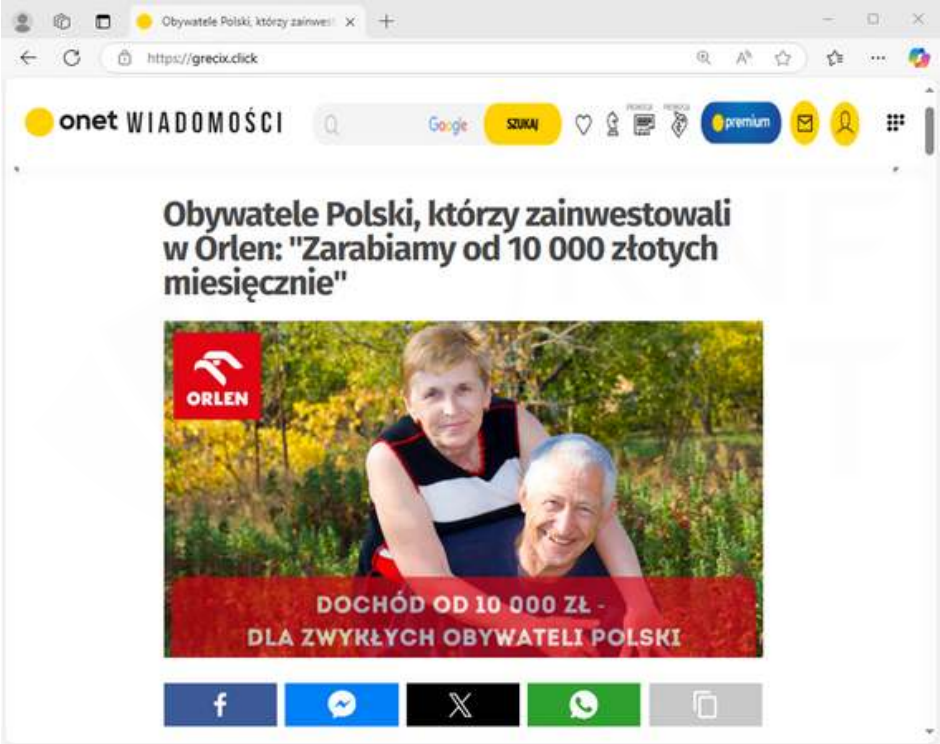
Grafika 3. Przykład wykorzystywania technologii deepfake do manipulacji - zastosowanie modyfikacji graficznych

Grafika 4. Przykład wykorzystywania technologii deepfake do manipulacji - zastosowanie modyfikacji graficznych

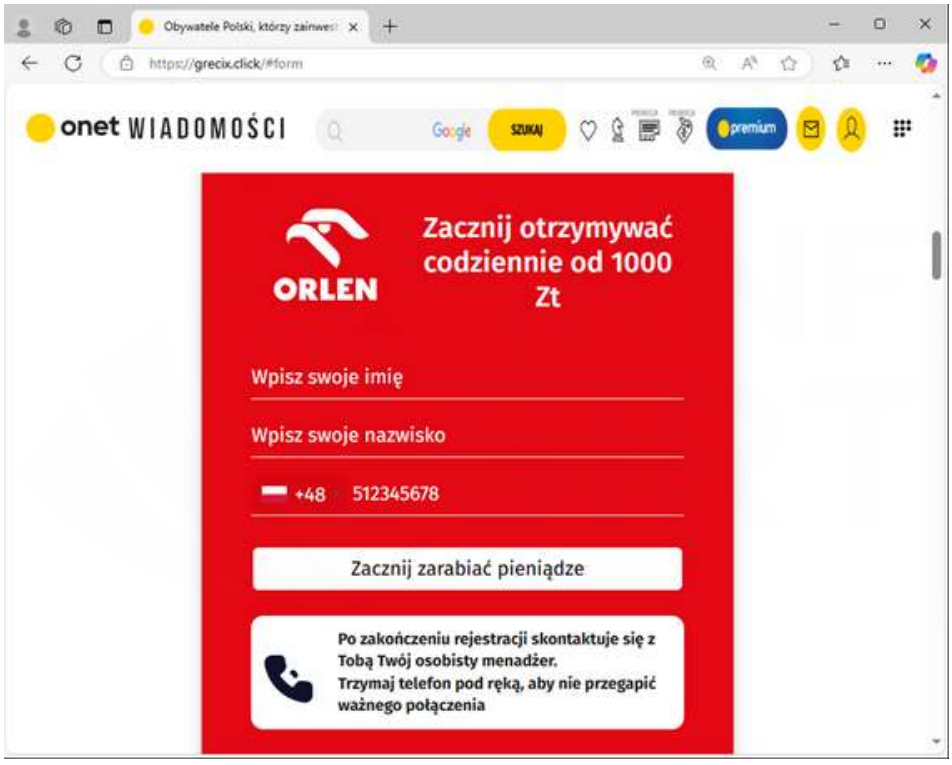
Zachęcamy także do obejrzenia przykładowych filmów, w których cyberprzestępcy wykorzystywali technologię deepfake: https://cebrf.knf.gov.pl/deepfake

Oszustwa na portalach i w wyszukiwarkach

- Oszuści publikowali artykuły dotyczące inwestycji na portalach stworzonych przez nich, które wyglądem przypominały znane serwisy. Miało to na celu uwiarygodnienie oszustwa i przekonanie użytkownika, że oferowana inwestycja jest prawdziwa (grafika 5-6).



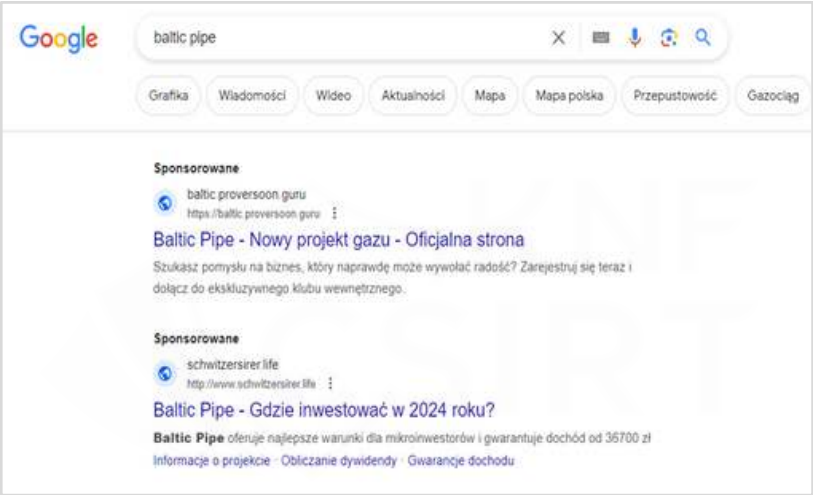
Grafika 5. Artykuł na fałszywej stronie informacyjnej nakłaniający do zainwestowania w fałszywe inwestycje



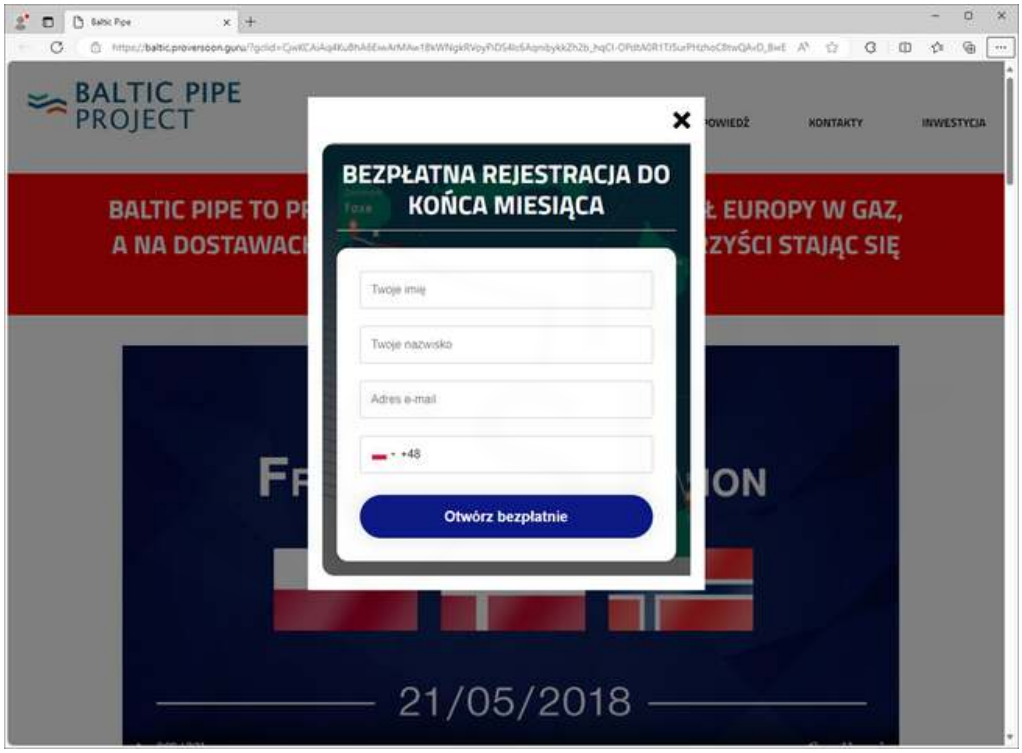
Grafika 6. Fałszywa strona, na której oszuści zachęcali do dokonania rejestracji

Kampanie spamowe i phishingowe kierujące użytkowników na fałszywe strony

- Użytkownikowi wpisującemu w wyszukiwarkę frazę związaną z inwestowaniem wyświetlała się na pierwszym miejscu w wynikach wyszukiwania oszukańcza reklama (grafika 7-8).



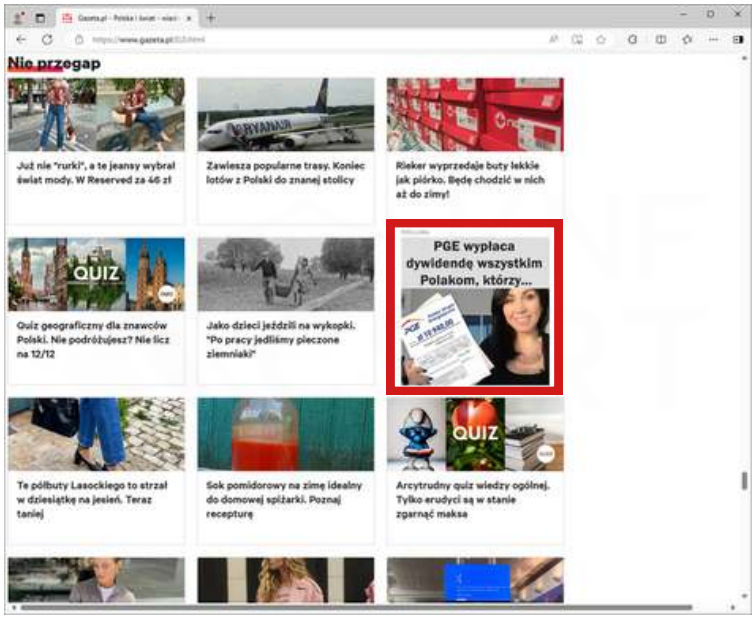
Grafika 7. Wyniki w wyszukiwarce internetowej prowadzące do fałszywych serwisów inwestycyjnych



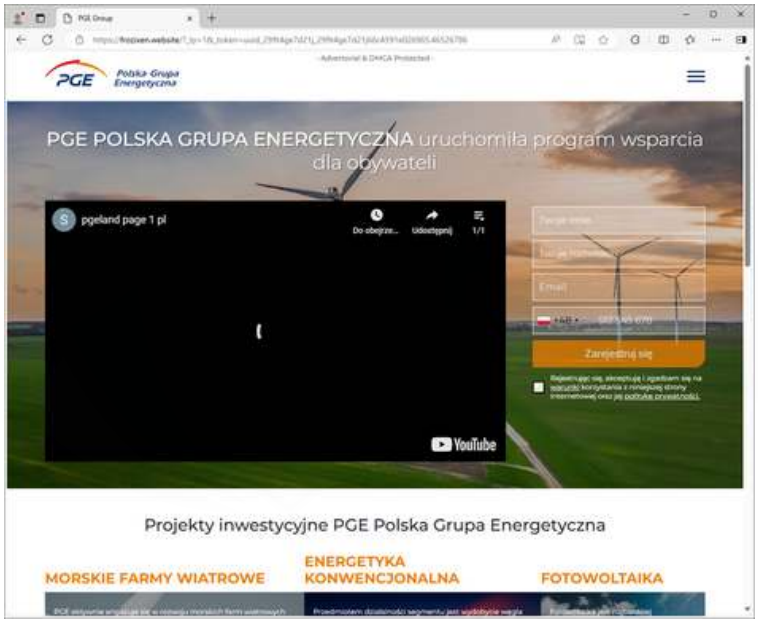
Grafika 8. Fałszywa strona podszywająca się pod projekt Baltic Pipe, do której prowadziła niebezpieczna reklama w wyszukiwarce Google

Reklamy fałszywych inwestycji w ogólnopolskich serwisach informacyjnych

- Oszuści w zamieszczanych reklamach wykorzystywali wizerunki znanych osób czy instytucji, oferując szybkie zyski w krótkim czasie (grafika 9-10).



Grafika 9. Reklama fałszywej inwestycji pojawiająca się na stronie portalu informacyjnego Gazeta.pl



Grafika 10. Fałszywa strona podszywająca się pod PGE, do której prowadziła reklama

2. Etap przekonywania:

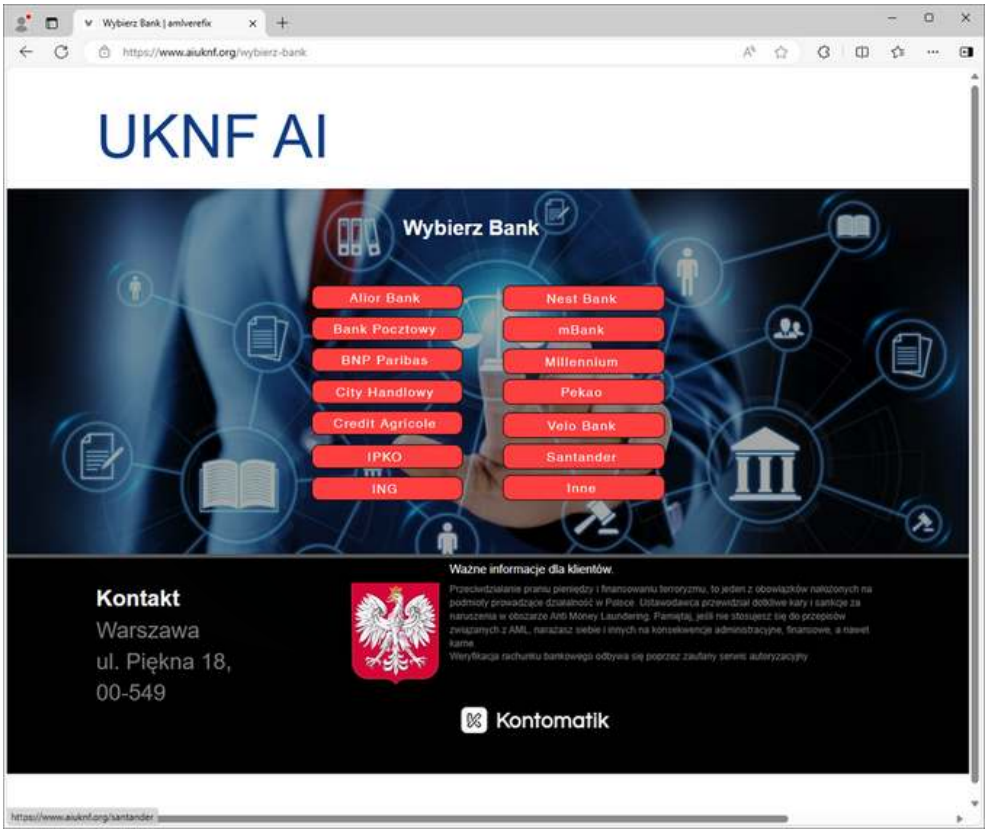
- Prezentowanie wymyślonych historii sukcesu inwestycyjnego, często z udziałem rzekomych „ekspertów".
- Symulowanie zysków, które zachęcają użytkowników do większych wpłat.
- Stosowanie presji, np. ograniczonych ofert promocyjnych, by zmusić ofiarę do szybkiego działania.
- Korzystanie z fałszywych doradców inwestycyjnych, którzy kontaktują się bezpośrednio z ofiarami.

3. Etap wyłudzenia:

- Wymaganie wpłaty minimalnej, jako warunku uczestnictwa w platformie inwestycyjnej.
- Zachęcanie do kolejnych wpłat, rzekomo zwiększających potencjalne zyski.
- Blokowanie wypłat i wymuszanie dodatkowych opłat, np. za „weryfikację konta" lub „zwrot środków".

Metody stosowane przez cyberprzestępców miały na celu wzmocnienie prowadzonej gry psychologicznej. Przykładowo oszuści na fałszywych stronach wykorzystujących wizerunek Urzędu Komisji Nadzoru Finansowego informowali o rzekomej konieczności przejścia procesu „przeciwdziałania praniu pieniędzy". W tym celu wysyłali link do strony „UKNF AI", gdzie ofiara zachęcana była do wpisania danych osobowych, wybrania banku oraz przekazania danych uwierzytelniających do bankowości elektronicznej (grafika 11-12).

Grafika 11. Fałszywa strona podszywająca się pod Urząd Komisji Nadzoru Finansowego, wyłudzająca dane osobowe

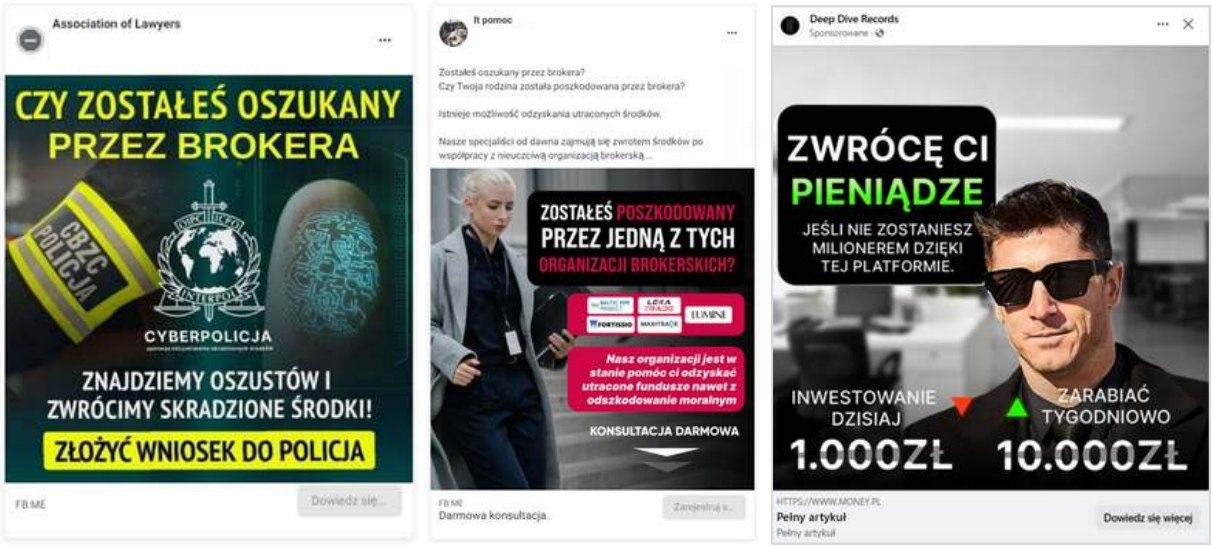


Grafika 12. Fałszywa strona podszywająca się pod Urząd Komisji Nadzoru Finansowego zachęcająca do wybrania banku i przekazania danych uwierzytelniających do bankowości elektronicznej

- Oferowanie możliwości rzekomego odzyskania utraconych środków.

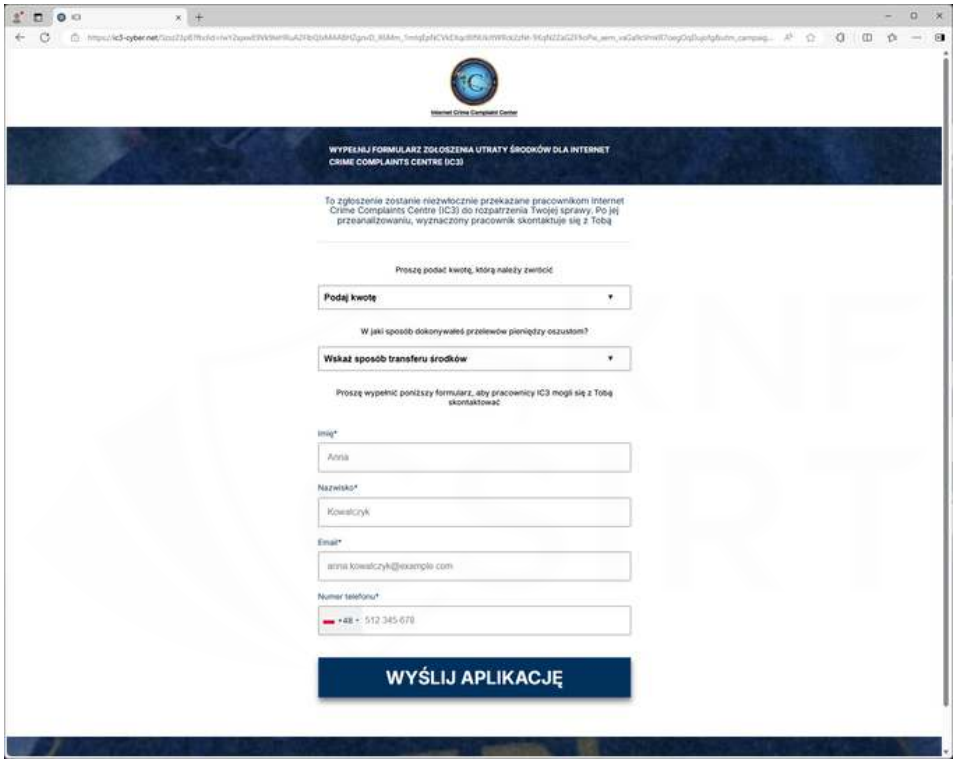
Powtarzającym się schematem było publikowanie przez cyberprzestępców informacji o rzekomej możliwości odzyskania utraconych wcześniej pieniędzy. W rzeczywistości była to ponowna próba oszukania osób, które już wcześniej padły ofiarą tego oszustwa. Oszuści publikując tego rodzaju reklamy liczyli, że wiele osób zdecyduje się na ponowne pozostawienie swoich danych kontaktowych, a oni będą mogli dalej prowadzić grę psychologiczną i nakłaniać ofiary do zainwestowania kolejnych środków. Socjotechnika stosowana przez przestępców w tym schemacie oszustwa pokazuje, jak dobrze są oni przygotowani.

Przykłady reklam zamieszczanych przez cyberprzestępców, oferujących rzekomą możliwość odzyskania utraconych środków (grafika 13):



Grafika 13. Reklamy zamieszczane przez cyberprzestępców w mediach społecznościowych

Po kliknięciu w reklamę użytkownik trafiał na niebezpieczną stronę, gdzie oszuści wymagali wypełnienia formularza i pozostawienia swoich danych kontaktowych (grafika 14).



Grafika 14. Fałszywa strona z formularzem wyłudzającym dane osobowe użytkowników

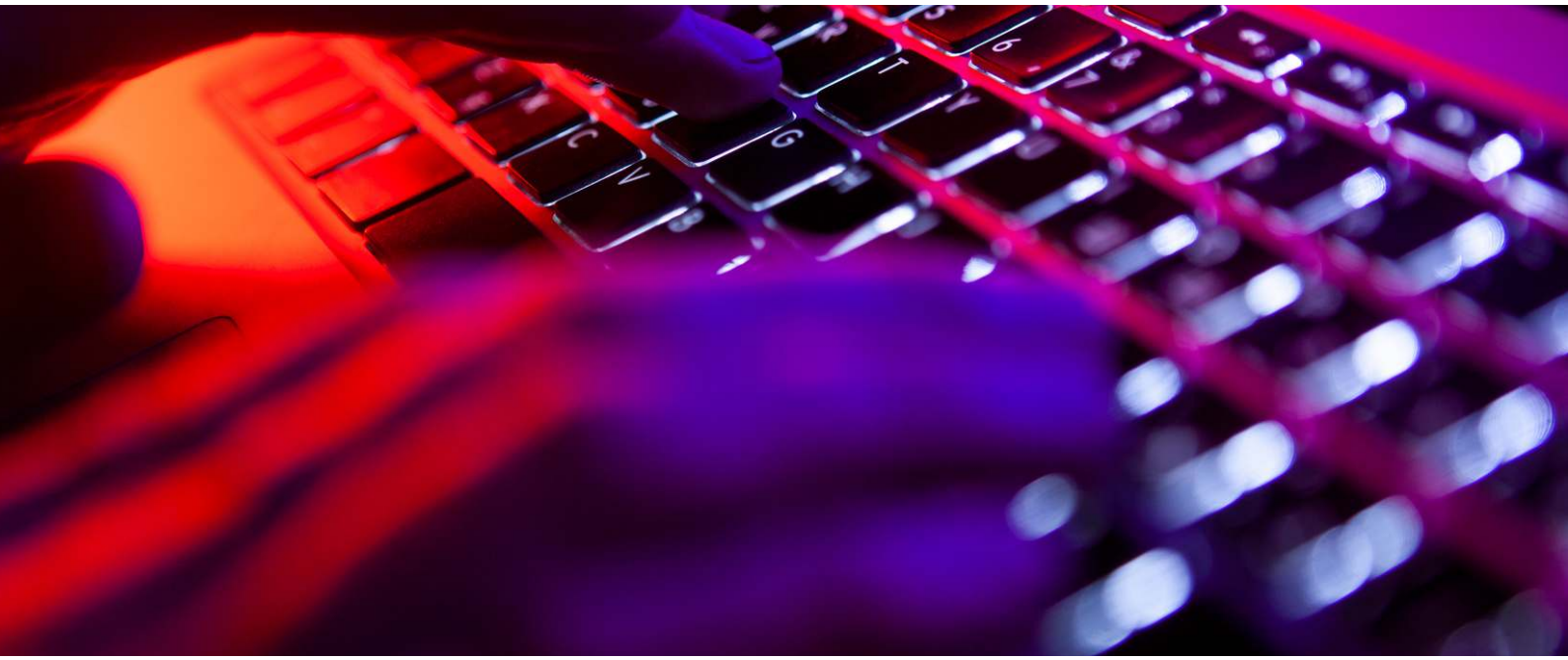
Trendy i ewolucja

W 2024 roku zaobserwowano:

- Wzrost wykorzystania sztucznej inteligencji do tworzenia przekonujących materiałów reklamowych na potrzeby oszustwa.
- Automatyzację procesów oszustwa.
- Szybką zmianę domen w reakcji na blokady.
- Wykorzystywanie aktualnych wydarzeń, np. gospodarczych.
- Personalizację ataków pod konkretne grupy odbiorców.

Rekomendacje dla użytkowników Internetu

- Bądź ostrożny wobec ofert, w których obiecywane są szybkie i wysokie zyski – bardzo często świadczy to o próbie oszustwa.
- Skonsultuj się z doradcą inwestycyjnym – zanim podejmiesz decyzję o inwestycji, zapytaj licencjonowanego doradcę o opinię. Pomoże on zweryfikować wiarygodność oferty.
- Zastosuj zasadę ograniczonego zaufania – jeśli oferta wydaje się zbyt atrakcyjna, aby mogła być prawdziwa, istnieje duże prawdopodobieństwo, że jest to oszustwo. Dokładnie sprawdź wiarygodność firmy zamiast polegać na samych obietnicach.
- Śledź Listę ostrzeżeń publicznych KNF[2]. Brak podmiotu na Liście ostrzeżeń publicznych KNF nie zwalnia z powinności sprawdzenia go w wiarygodnych źródłach informacji. Warto również zweryfikować np. czy dany podmiot znajduje się w jednym z rejestrów prowadzonych przez UKNF lub w wyszukiwarce podmiotów.



[2] https://www.knf.gov.pl/dla_konsumenta/ostrzezenia_publiczne

04. FAŁSZYWE ANKIETY - ROSNĄCE ZAGROŻENIE

FAŁSZYWE ANKIETY - ROSNĄCE ZAGROŻENIE

Skala zjawiska
W 2024 roku CSIRT KNF zidentyfikował **4030** domen związanych z fałszywymi ankietami, co stanowi drugi najczęstszy typ oszustw w polskim sektorze finansowym. Jest to znaczący wzrost w porównaniu do lat poprzednich.

Charakterystyka ataków
Oszustwa ankietowe charakteryzują się następującymi elementami:

Mechanizm działania
- Podszywanie się pod znane marki i instytucje.
- Obietnica wysokich nagród za wypełnienie krótkiej ankiety.
- Fałszywe konkursy konsumenckie.
- Presja („tylko dziś", „ostatnie 50 nagród").
- Imitacja badań rynkowych.

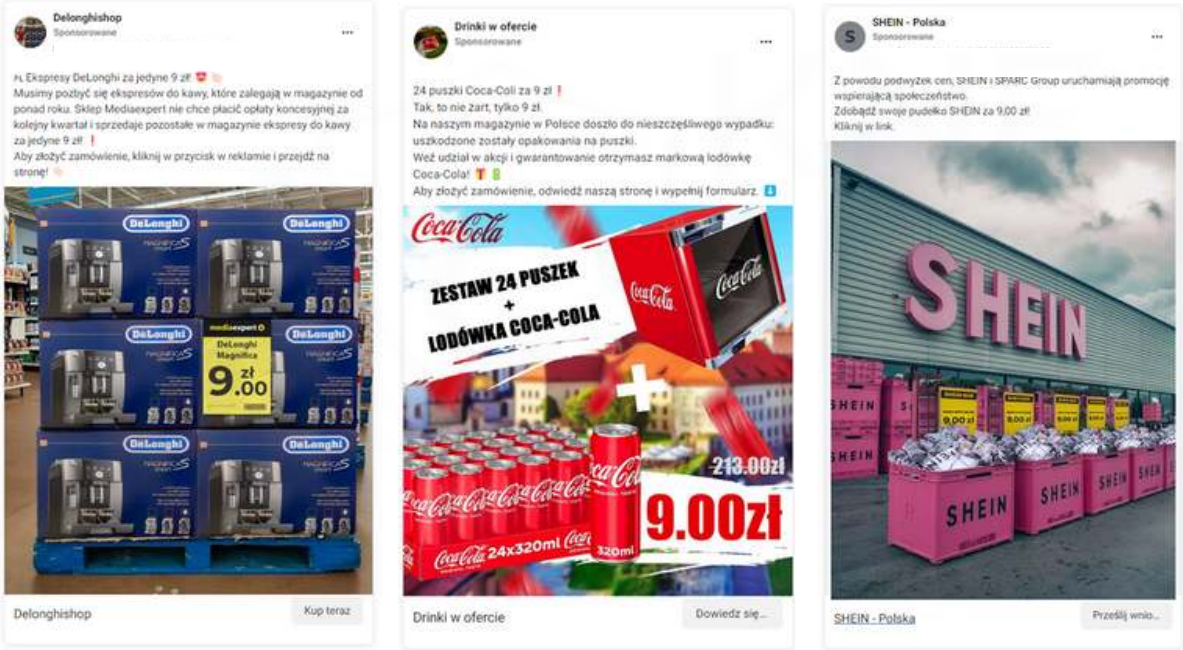
Wykorzystywane techniki
1. Uwiarygodnienie:
- Profesjonalny wygląd strony internetowej.
- Wykorzystanie prawdziwych logotypów firm.
- Fałszywe komentarze „szczęśliwych zwycięzców".
- Liczniki sugerujące zbliżanie się do uzyskania nagrody.
- Podrobione certyfikaty i pieczęcie jakości.

2. Psychologiczne:
- FOMO (Fear of Missing Out), czyli obawa przed utratą okazji do zdobycia nagrody skłania użytkowników do podjęcia szybkich działań.
- Ograniczona dostępność nagród.
- Społeczny dowód słuszności, czyli podejmowanie decyzji na podstawie obserwacji zachowania innych osób.
- Manipulacja emocjami.

Proces oszustwa

Etap 1. Wzbudzanie zainteresowania u potencjalnej ofiary

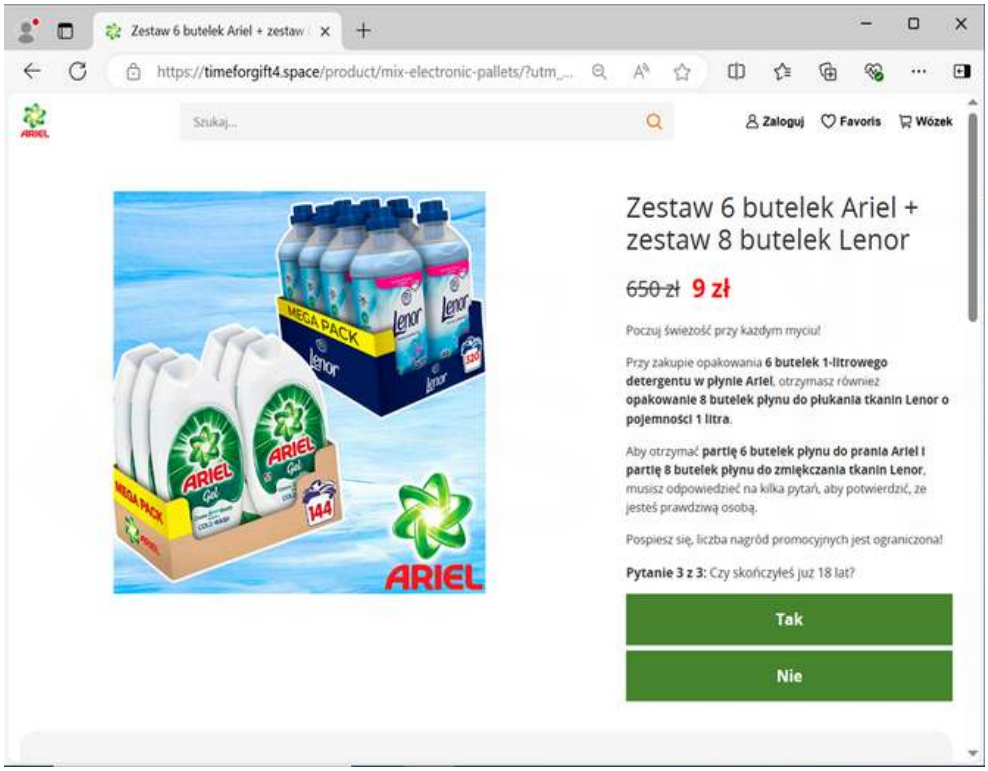
- Wykorzystywanie logotypów znanych marek w reklamach w mediach społecznościowych, by zachęcić do udziału w konkursach lub badaniach, (np. opinii).
- Wiadomości SMS oraz e-mail zawierające linki do fałszywych stron internetowych.



Grafika 15. Reklamy zamieszczane przez cyberprzestępców w mediach społecznościowych, wykorzystujące logotypy znanych marek

Etap 2. Ankieta

- Ankiety były skonstruowane tak, aby wydawały się być krótkie i łatwe do wypełnienia, co zachęcało użytkowników do ich ukończenia.
- Pozornie profesjonalny wygląd wykorzystujący elementy graficzne i strukturę strony internetowej charakterystyczną dla renomowanych firm (grafika 16).
- Pytania początkowo neutralne stopniowo przechodzące do prośby o dane osobowe oraz dane kart płatniczych.
- Wyświetlane wskaźniki sugerowały, że użytkownik zbliża się do uzyskania obiecanej nagrody, co motywowało go do kontynuowania wypełniania ankiety.

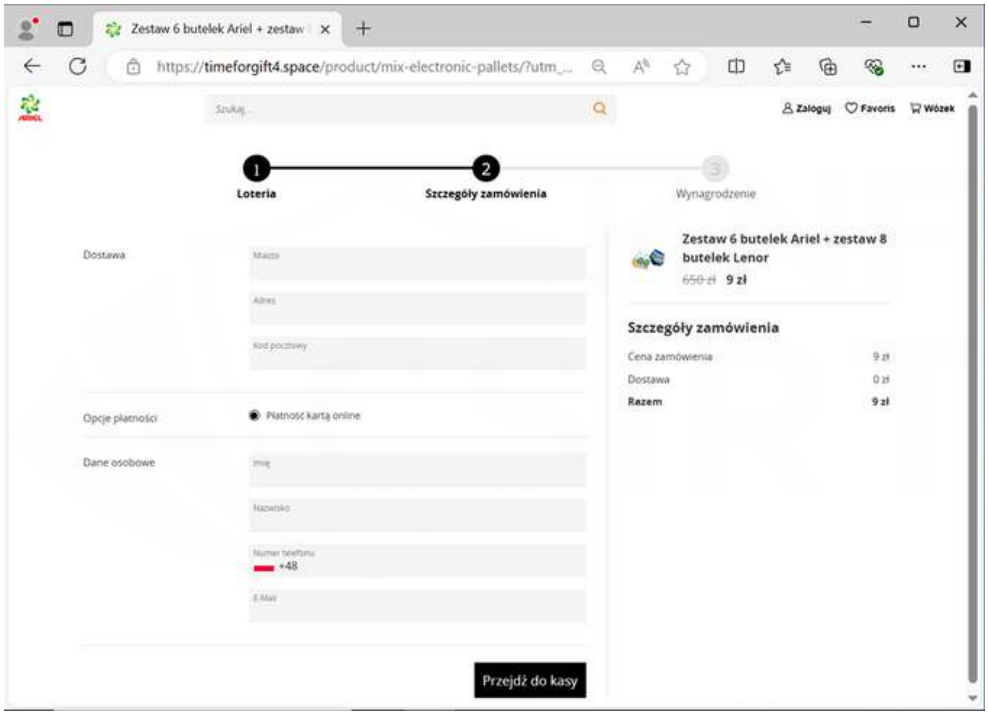


Grafika 16. Fałszywa strona, na której wymagane jest odpowiedzenie na pytania

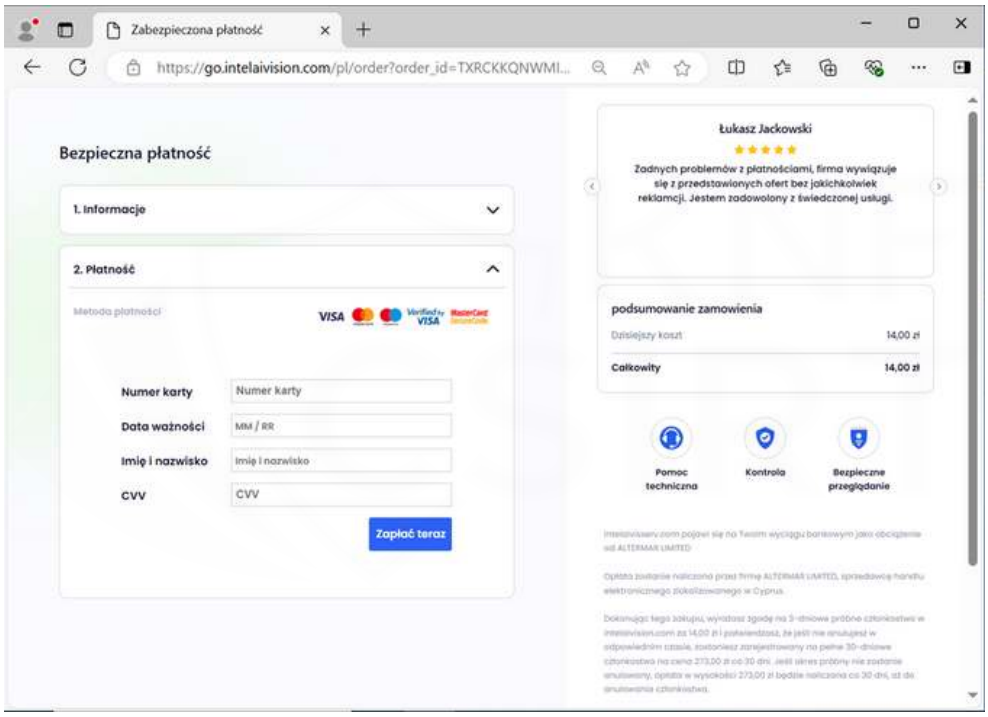
Etap 3. Wyłudzenie

- Użytkownik zachęcony ofertą, trafiał na stronę internetową, na której proszony był o udzielenie odpowiedzi na kilka pytań.
- Następnie trafiał na stronę z formularzem do wpisania danych osobowych oraz informacji o karcie płatniczej (grafika 17-18).
- W kolejnym etapie, przestępcy starali się wyprowadzić środki z rachunków użytkowników, wykorzystując do tego „model subskrypcyjny".

Wygląd fałszywych stron wyłudzających dane osobowe oraz informacji o kartach płatniczych:



Grafika 17. Fałszywa strona wyłudzająca dane osobowe użytkowników



Grafika 18. Fałszywa strona wyłudzająca informacje o kartach płatniczych użytkowników

Rekomendacje dla użytkowników Internetu

- Weryfikuj źródło ankiety – zawsze upewnij się, że pochodzi ona z wiarygodnego źródła, np. oficjalnej firmy lub instytucji.
- Sprawdzaj adres e-mail nadawcy i domenę strony internetowej – zwróć szczególną uwagę, czy nie wzbudzają podejrzeń.
- Chroń swoje dane osobowe i finansowe – unikaj podawania numeru PESEL, serii i numeru dowodu osobistego, danych karty kredytowej i płatniczej oraz haseł na stronach, których autentyczność jest wątpliwa. Pamiętaj, że celem fałszywych ankiet może być wyłudzenie pieniędzy lub kradzież tożsamości.

05. OSZUSTWA KURIERSKIE I POCZTOWE

OSZUSTWA KURIERSKIE I POCZTOWE

Skala zjawiska

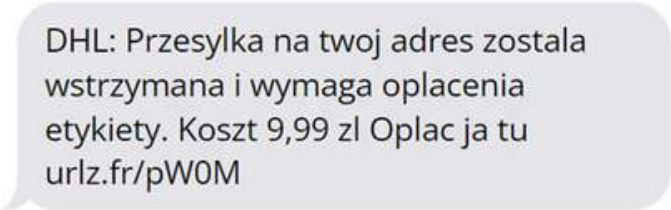
W 2024 roku CSIRT KNF zidentyfikował **521** domen związanych z oszustwami kurierskimi i pocztowymi. Ten typ ataków, choć mniej liczny niż oszustwa inwestycyjne czy ankietowe, charakteryzuje się wysoką skutecznością ze względu na powszechność usług kurierskich.

Charakterystyka mechanizmów oszustwa

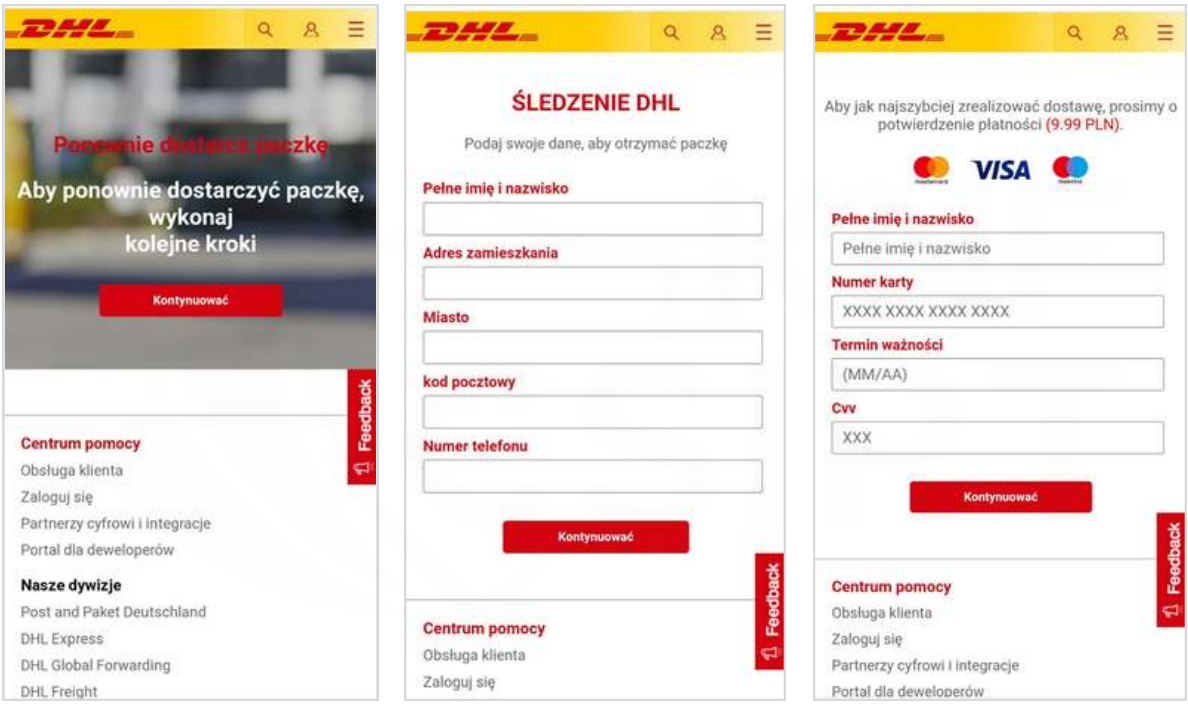
Typowe scenariusze

1. Dopłaty do przesyłek:

- Ofiara otrzymywała SMS lub e-mail z informacją o konieczności dopłaty niewielkiej kwoty (grafika 19).
- Wiadomość zawierała link prowadzący do fałszywej strony internetowej do dokonania płatności (grafika 20).
- Przestępcy wywierali presję, twierdząc, że paczka zostanie zwrócona do nadawcy, jeśli użytkownik nie dokona opłaty.
- Podszywanie się pod znanych operatorów, takich jak InPost, DHL czy Poczta Polska, w celu zwiększenia wiarygodności.

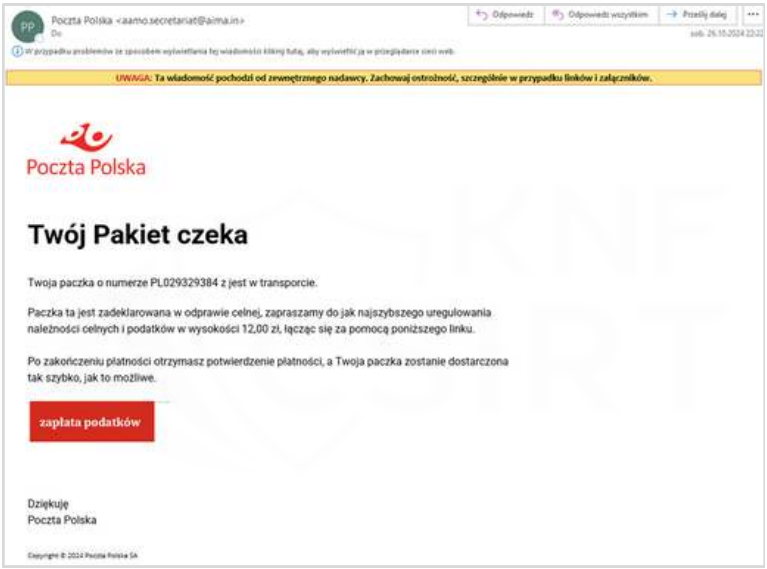


Grafika 19. Fałszywa wiadomość SMS podszywająca się pod firmę kurierską DHL

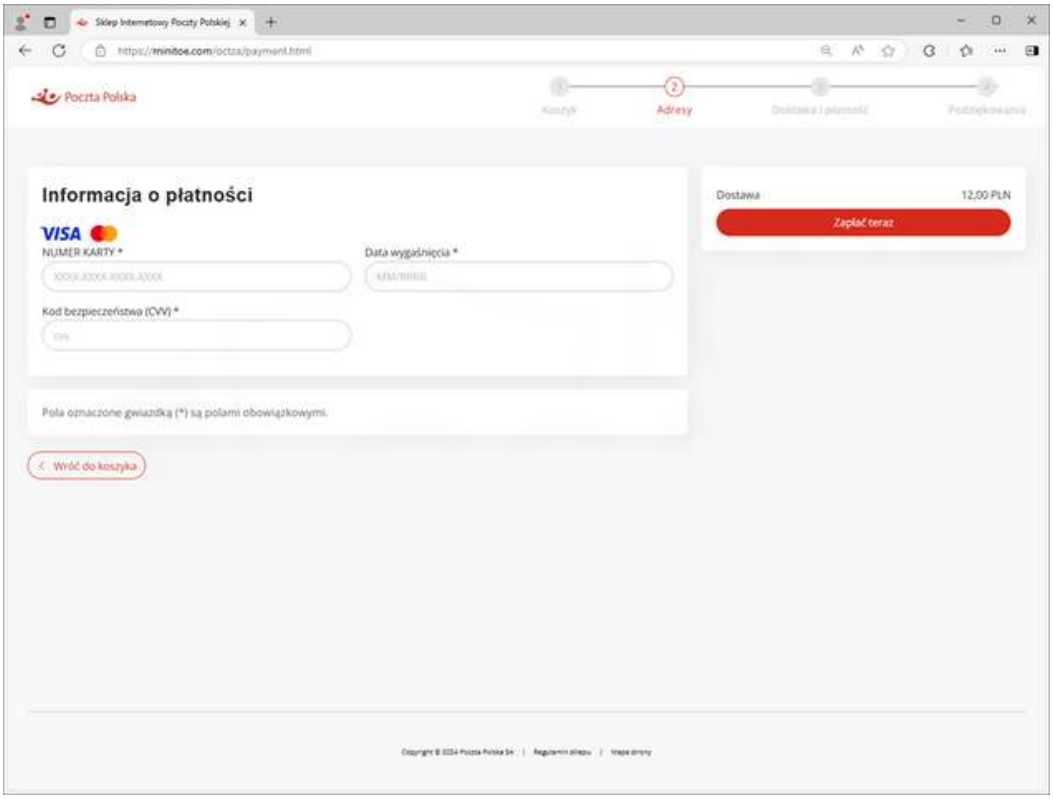


Grafika 20. Przykłady niebezpiecznych stron, na których oszuści wyłudzali dane osobowe użytkowników oraz informacje o kartach płatniczych

Cyberprzestępcy przesyłając fałszywe wiadomości e-mail, podszywali się pod Pocztę Polską, informowali o rzekomej opłacie celnej i konieczności uregulowania należności (grafika 21). Po kliknięciu w link, który znajdował się w wiadomości, użytkownik trafiał na niebezpieczną stronę wyłudzającą dane karty płatniczej (grafika 22).



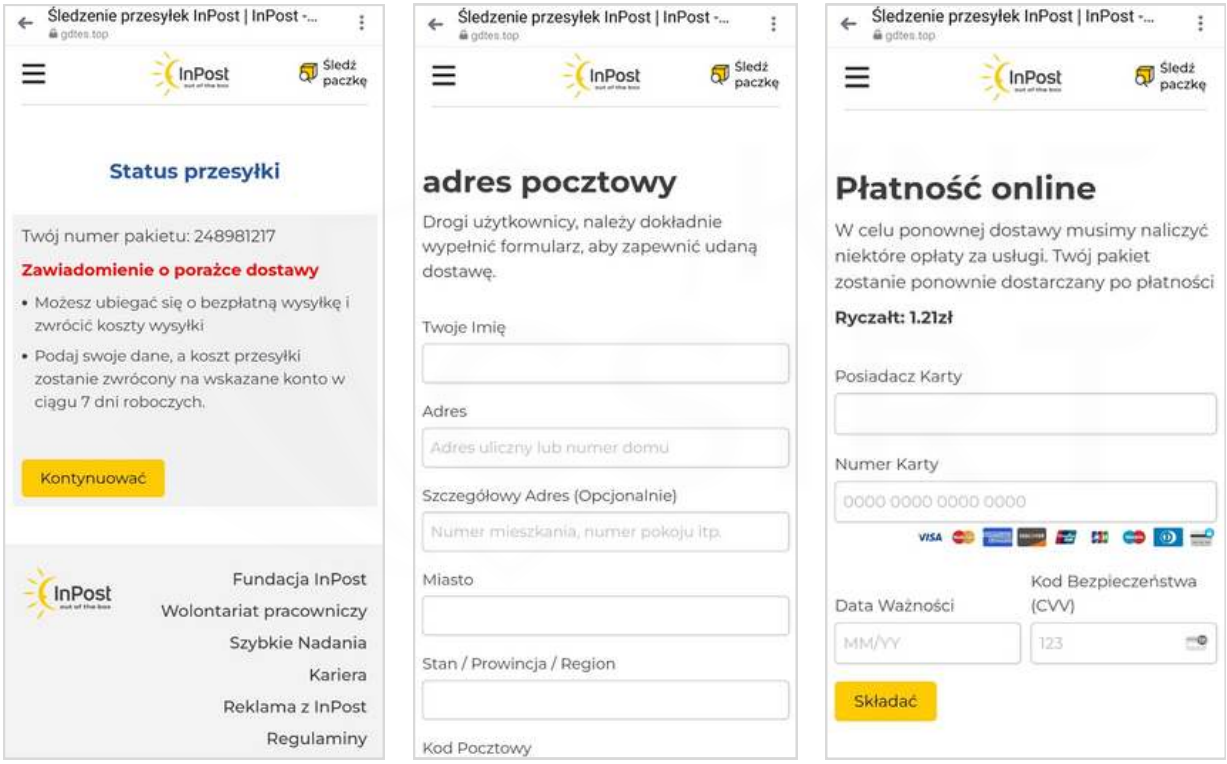
Grafika 21. Fałszywa wiadomość e-mail z informacją o konieczności uregulowania należności



Grafika 22. Fałszywa strona, na której oszuści wymagali wprowadzenia danych karty płatniczej

2. Niedoręczone paczki:
   - Ofiara otrzymywała powiadomienie o nieudanej próbie doręczenia przesyłki (grafika 23).
   - Przestępcy prosili o podanie danych osobowych w celu ponownego dostarczenia paczki.
   - Kliknięcie w link prowadziło do fałszywej strony służącej do wyłudzenia danych kart płatniczych (grafika 24).

Grafika 23. Fałszywa wiadomość SMS podszywająca się pod firmę kurierską InPost



Grafika 24. Przykłady niebezpiecznych stron, na których oszuści wyłudzali dane osobowe użytkowników

Metody działania przestępców

Techniki uwiarygodnienia

- Strony internetowe były zaprojektowane tak, by wyglądem przypominały prawdziwe witryny internetowe firm kurierskich.
- Wykorzystanie prawdziwych logotypów firm.
- Komunikacja w e-mailach i SMS-ach miała profesjonalny charakter.
- Podawane numery przesyłek były realistyczne, co sprawiało, że ofiary rzadziej podejrzewały oszustwo.

Wykorzystywane kanały:

- SMS,
- wiadomości e-mail,
- komunikatory internetowe.

Sezonowość ataków

- Okresy zakupowe: znaczny wzrost aktywności w czasie intensywnych zakupów online, takich jak Black Friday, Cyber Monday oraz przed świętami.
- Wydarzenia specjalne: ataki były dostosowywane do bieżących wydarzeń, takich jak promocje czy wyprzedaże, by zwiększyć ich skuteczność.

Rekomendacje dla użytkowników

- Zachowaj ostrożność po otrzymaniu wiadomości (SMS lub e-mail) o rzekomej dopłacie do przesyłki. Zanim klikniesz w jakikolwiek link, upewnij się, że pochodzi on od zaufanego przewoźnika. Fałszywe wiadomości często wywierają presję, by skłonić cię do natychmiastowej reakcji.
- Skontaktuj się bezpośrednio z przewoźnikiem – jeśli masz wątpliwości, użyj oficjalnych danych kontaktowych (ze strony internetowej firmy kurierskiej). Nie odpowiadaj na podejrzane wiadomości i nie korzystaj z przesłanych w nich linków czy numerów telefonów.
- Pobieraj aplikacje tylko z zaufanych źródeł – korzystaj z oficjalnych aplikacji mobilnych firm kurierskich, dostępnych w Google Play lub App Store. Unikaj instalowania aplikacji z nieznanych źródeł, ponieważ mogą zawierać złośliwe oprogramowanie.
- Zgłaszaj podejrzane wiadomości SMS – jeśli otrzymasz SMS, który wydaje się próbą oszustwa, prześlij go na numer 8080. Pomagasz w ten sposób w szybszej identyfikacji zagrożeń i ograniczeniu skali ryzyka.

06. OSZUSTWA BANKOWE -PODSZYWANIE SIĘ POD INSTYTUCJE FINANSOWE

OSZUSTWA BANKOWE - PODSZYWANIE SIĘ POD INSTYTUCJE FINANSOWE

Skala zjawiska

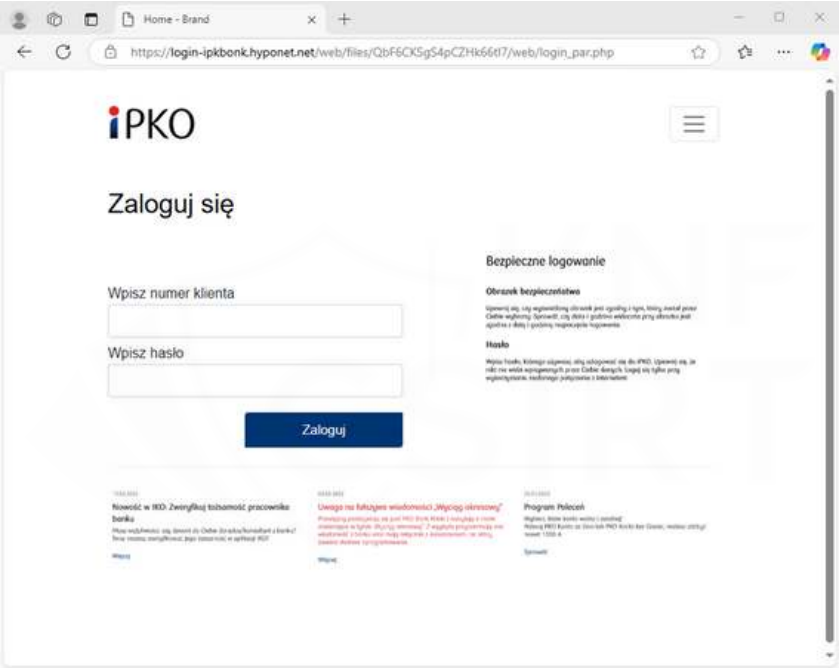
W 2024 roku CSIRT KNF zidentyfikował **175** domen związanych z oszustwami bankowymi. Cyberprzestępcy na tworzonych przez siebie stronach internetowych podszywali się pod podmioty rynku finansowego i wykorzystywali je do kradzieży danych do logowania do bankowości elektronicznej.

Charakterystyka ataków

Główne metody podszywania się

1. Fałszywe strony logowania:

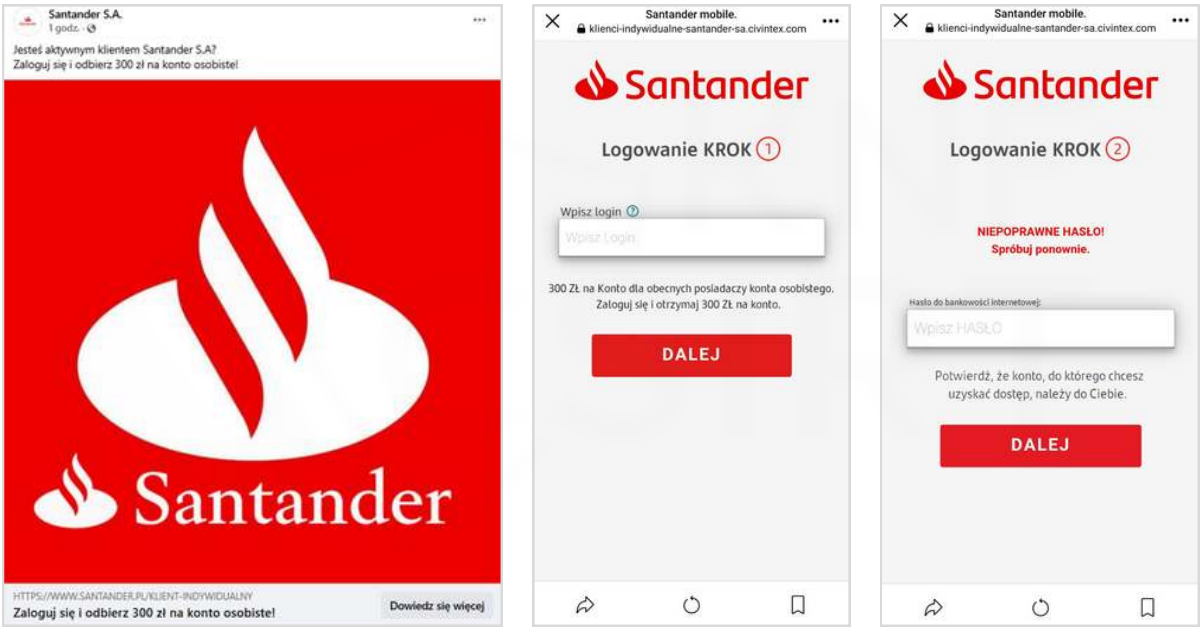
- Oszuści tworzyli precyzyjne kopie stron internetowych banków, które były niemal nie do odróżnienia od ich oryginałów (grafika 25).



Grafika 25. Niebezpieczna strona wyłudzająca dane do logowania użytkowników, podszywająca się pod PKO BP

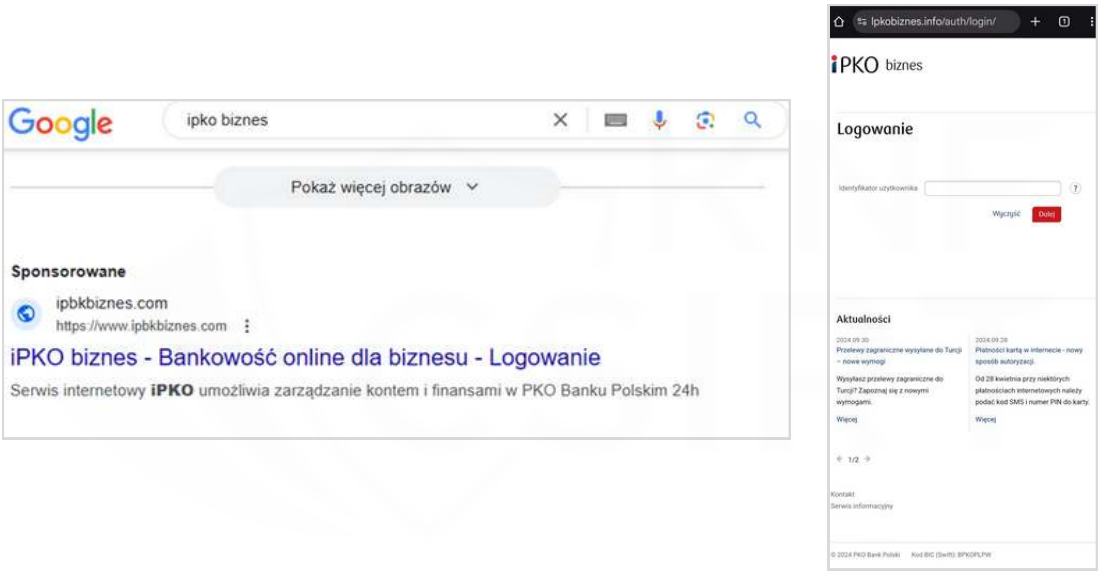
- Przekierowania z fałszywych reklam

Przestępcy podszywając się pod polskie banki publikowali reklamy na portalu Facebook. Pod pretekstem rzekomej możliwości odebrania nagrody wyłudzali dane uwierzytelniające do bankowości elektronicznej oraz dane kart płatniczych (grafika 26).



Grafika 26. Reklama w mediach społecznościowych oraz przykłady fałszywych stron wyłudzających dane do logowania, podszywających się pod Santander Bank Polska

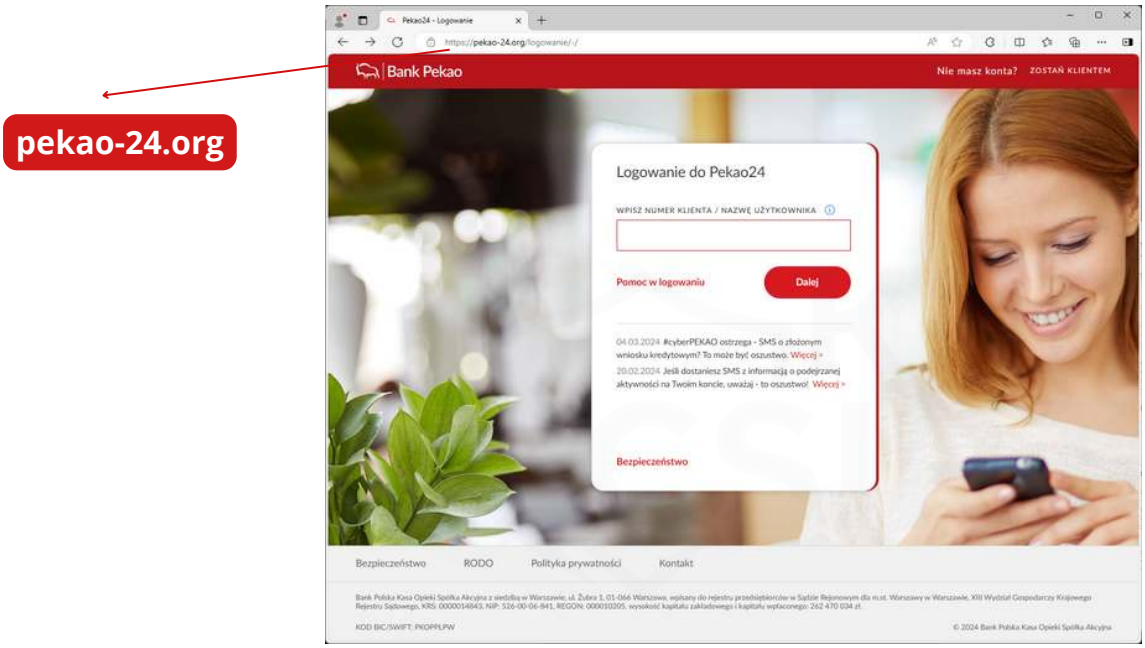
Przestępcy podszywając się pod PKO Bank Polski wykupili reklamy w wyszukiwarce Google. Reklamy te prowadziły do fałszywych stron internetowych, łudząco podobnych do stron do logowania do bankowości elektronicznej dla klientów biznesowych banku. W ten sposób atakujący wykorzystali pozycjonowanie wyników wyszukiwania w wyszukiwarce. Po wpisaniu „w Google" frazy mającej na celu znalezienie opisywanej strony bankowości, pierwszymi pojawiającymi się wynikami były te wykupione jako reklamy. Oszuści na niebezpiecznych stronach wyłudzali dane do logowania do bankowości elektronicznej (grafika 27).



Grafika 27. Reklama w wyszukiwarce Google, w której cyberprzestępcy podszywali się pod PKO Bank Polski

- Phishingowe domeny podobne do oryginalnych (grafika 28)

Przestępcy, aby zwiększyć wiarygodność kampanii phishingowych wykorzystywali wizerunek polskich banków. Oszuści tworzyli strony zbliżone do tych oryginalnych, gdzie adres domeny różnił się tylko jedną literą, znakiem interpunkcyjnym bądź zmianą w jednym ze słów.



Grafika 28. Niebezpieczna strona wyłudzająca dane do logowania użytkowników, podszywająca się pod Bank Pekao

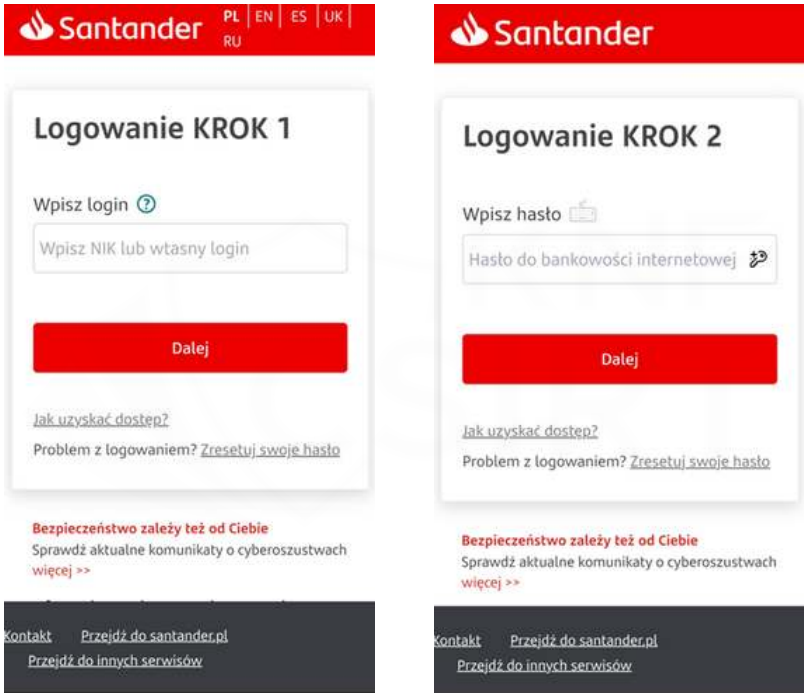
2. Oszustwa komunikacyjne:

- SMS-y o zablokowaniu konta (grafika 29)

Przestępcy podszywając się pod Santander Bank Polska przesyłali wiadomości SMS informując m.in. o rzekomym wygaśnięciu dostępu do aplikacji. Celem uniknięcia niedogodności zachęcali do kliknięcia w link zawarty w wiadomości.

Grafika 29. Fałszywa wiadomość SMS podszywająca się pod Santander Bank Polska

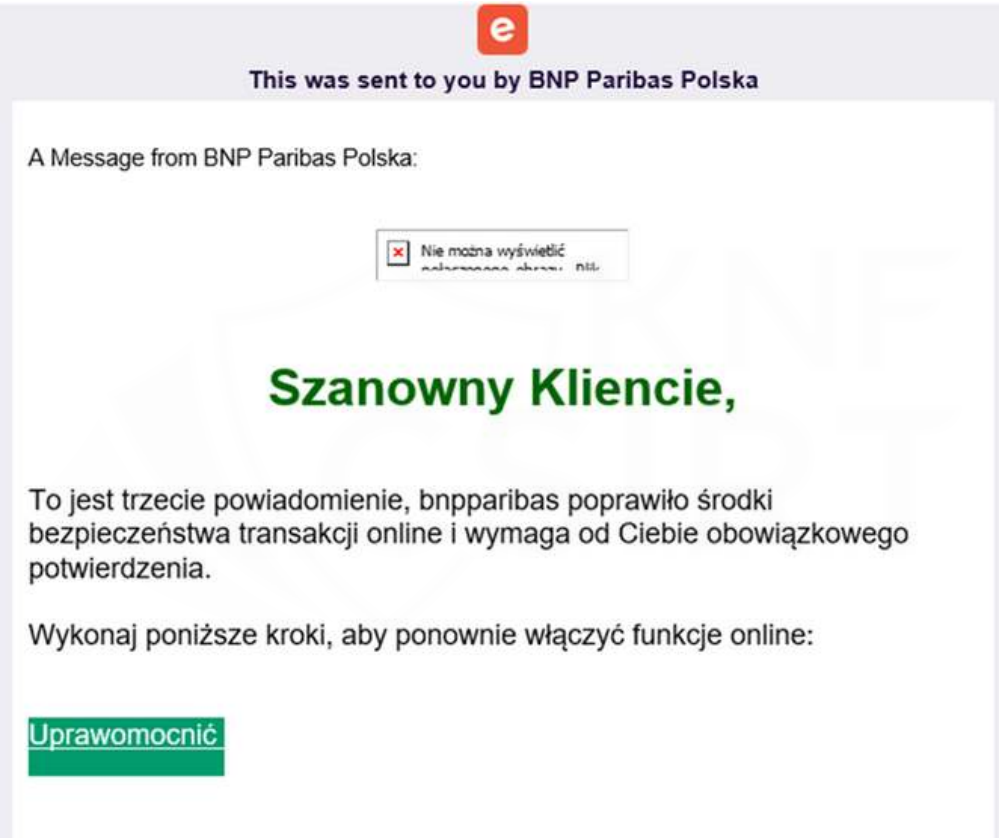
Link znajdujący się w wiadomości prowadził do fałszywej strony bankowości elektronicznej, na której cyberprzestępcy wyłudzali dane do logowania.



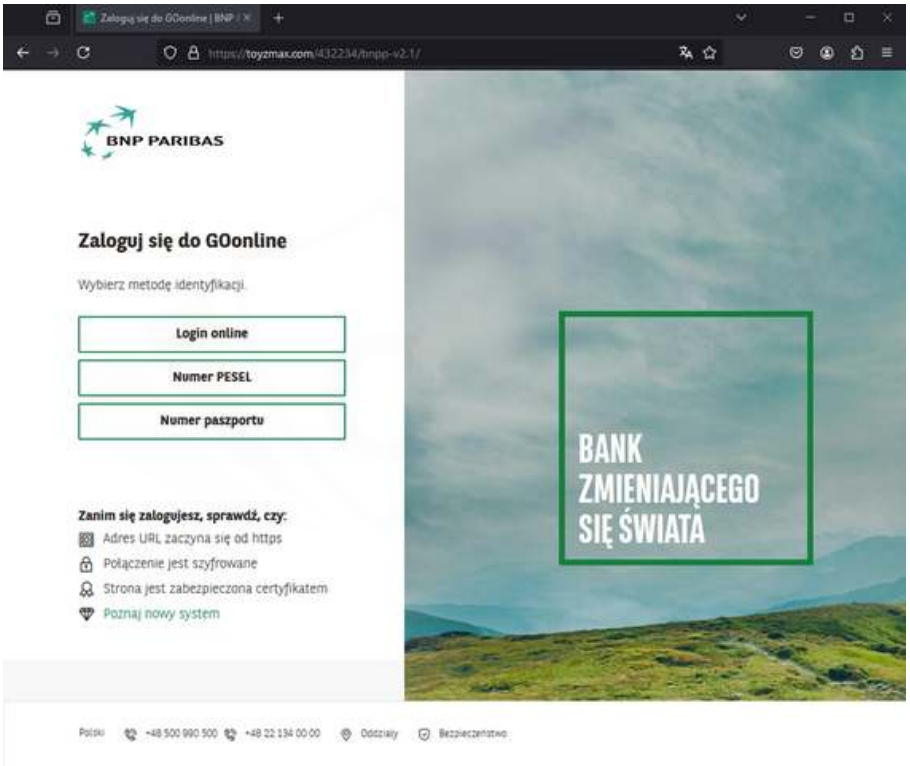
Grafika 30. Niebezpieczne strony podszywające się pod Santander Bank Polska

- E-maile o konieczności weryfikacji danych (grafika 31)

Przestępcy podszywając się pod Bank BNP Paribas wysyłali wiadomości e-mail i informowali o rzekomej konieczności „aktualizacji systemu, celem poprawienia bezpieczeństwa". W rzeczywistości link ukryty pod przyciskiem „Uprawomocnić" prowadził na stronę phishingową, podszywającą się pod stronę logowania do bankowości elektronicznej BNP Paribas. W ten sposób atakujący wyłudzali dane do logowania do bankowości elektronicznej.



Grafika 31. Treść fałszywej wiadomości e-mail, podszywającej się pod Bank BNP Paribas



Grafika 32. Fałszywa strona podszywająca się pod Bank BNP Paribas

Rekomendacje dla klientów banków

- Dokładnie weryfikuj adres www – zawsze sprawdzaj, czy odwiedzasz oficjalną stronę swojego banku. Upewnij się, że adres jest poprawny i nie zawiera podejrzanych znaków ani literówek.
- Korzystaj z oficjalnych aplikacji – do logowania i wykonywania operacji bankowych używaj wyłącznie zaufanych aplikacji pobranych z oficjalnych źródeł (Google Play, App Store).
- Weryfikuj autentyczność komunikacji bankowej – jeśli dostaniesz od banku wiadomość wzbudzającą wątpliwości lub przypominającą opisane oszustwa, możesz:
  - Skontaktować się z pracownikiem banku – aby potwierdzić, czy rzeczywiście występują jakiekolwiek problemy z twoim kontem.
  - Zadzwonić na infolinię banku – numer znajdziesz m.in. na oficjalnej stronie internetowej banku.
  - Odwiedzić najbliższą placówkę banku – pracownicy pomogą ci zweryfikować wszelkie niepokojące informacje.
  - Zachować ostrożność podczas udostępniania danych – nigdy nie podawaj osobom trzecim loginu, ani kodów autoryzacyjnych do bankowości internetowej. Banki nigdy nie proszą o takie dane.
  - Korzystać z dwustopniowej weryfikacji (2FA) – włącz w banku dodatkowe zabezpieczenie logowania. Nawet jeśli ktoś pozna twoje hasło, nie uzyska dostępu do konta bez potwierdzenia tożsamości w drugim kroku.

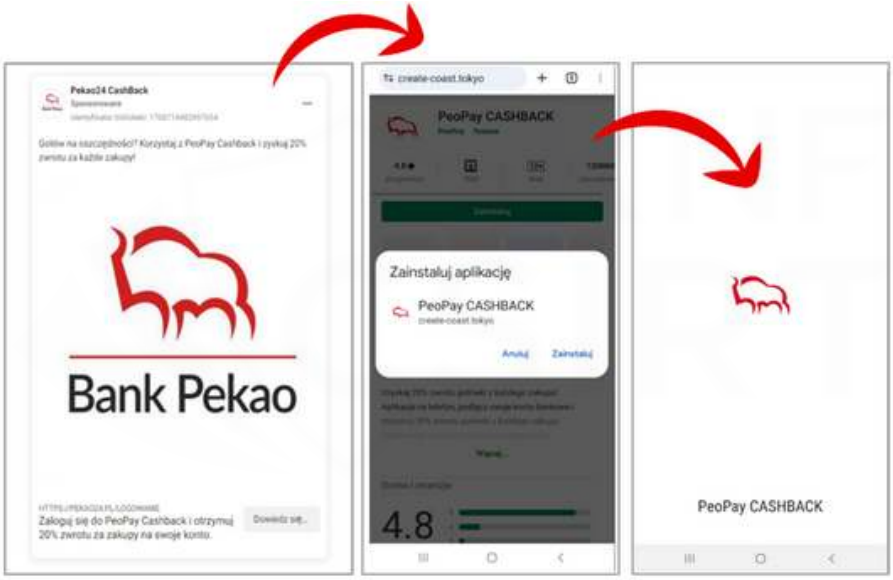
07. ZŁOŚLIWE OPROGRAMOWANIE

ZŁOŚLIWE OPROGRAMOWANIE

Ataki z wykorzystaniem technologii PWA/WebAPK

Oszustwa z użyciem PWA/WebAPK opisane zostały w raporcie z 2023 roku, w którym szczegółowo przedstawiono schemat działania przestępców, wykorzystujących te technologie do przeprowadzania ataków phishingowych. W scenariuszu główne zagrożenie stanowiła możliwość instalacji na urządzeniu złośliwej aplikacji, z pominięciem typowych ostrzeżeń dotyczących niezaufanych źródeł. Szkodliwa aplikacja mogła imitować np. interfejs bankowości elektronicznej w celu wyłudzenia od użytkowników wrażliwych danych[3].

Niektóre z obserwowanych w 2024 roku złośliwych aplikacji również korzystały ze wspomnianych technologii. Jednym z przykładów był scenariusz, gdzie w pierwszej fazie ataku zastosowano szkodliwą reklamę na portalu Facebook. Po kliknięciu w nią, użytkownik trafiał na złośliwą stronę internetową, umożliwiającą instalację fałszywej aplikacji **PeoPay CASHBACK** (grafika 33).



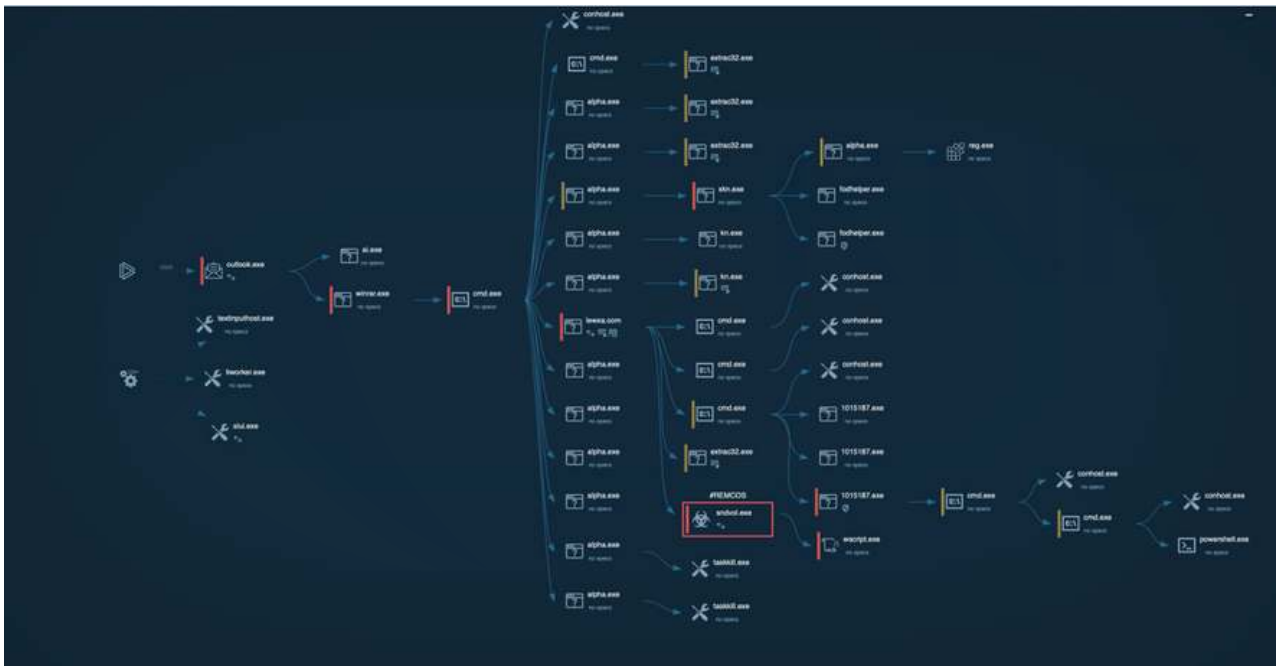
Grafika 33. Przykład fałszywej reklamy na portalu Facebook kierującej na złośliwą stronę, umożliwiającą instalację fałszywej aplikacji PeoPay CASHBACK

[3] https://cebrf.knf.gov.pl/komunikaty/artykuly-csirt-knf/362-ostrzezenia/874-wykorzystanie-tehnologii-webapk-do-ataku-phishingowego

W roku 2024 w sektorze finansowym zaobserwowano wiele kampanii złośliwego oprogramowania należącego do różnorodnych rodzin malware. Zwiększyło się również wykorzystywanie oprogramowania typu stealer. Obserwowano zarówno mniejsze incydentalne wystąpienia, jak i kampanie na masową skalę.

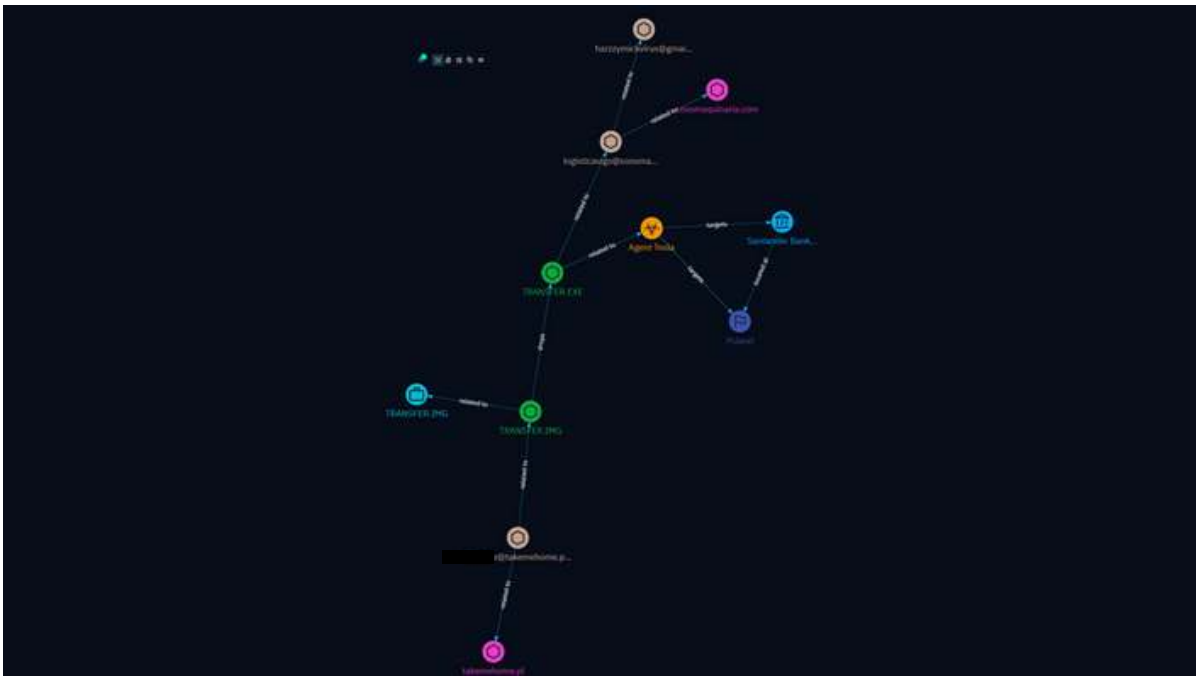
Przegląd rodzin złośliwego oprogramowania, których kampanie obserwowano w sektorze finansowym:

- **Lumma Stealer** – złośliwe oprogramowanie typu infostealer, które potrafi wykradać szeroki wachlarz informacji. Obserwowano wiele kampanii z jego wykorzystaniem. W jednej z kampanii adwersarze podszywali się pod Służbę Podatkową Ukrainy, o czym raportowało kilka podmiotów z sektora finansowego. Kampanie obserwowane były również przez CERT-UA, który dokonał atrybucji do grupy UAC-0050.
- **RuRat** – oprogramowanie to potrafi po infekcji kontrolować przejęty system, posiada również wiele mechanizmów, które posiada oprogramowanie typu stealer.
- **RemcosRAT** – w roku 2024 obserwowano powracające kampanie z wykorzystaniem tego oprogramowania również w wariancie z AceCryptor, który miał dodatkowo zamaskować złośliwy kod (grafika 34).

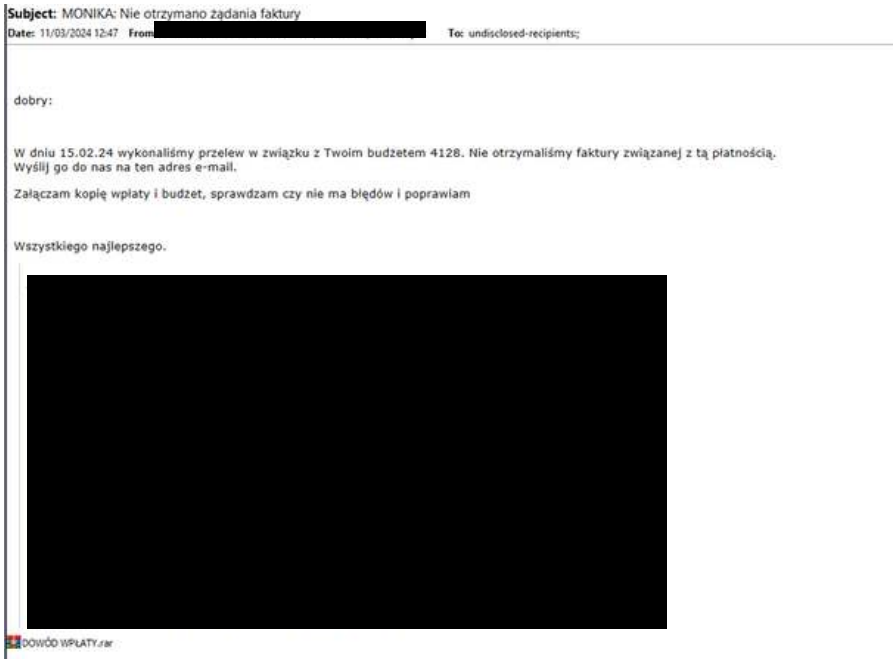


Grafika 34. Schemat uruchamiania procesów podczas infekcji RemcosRAT

- **AgentTesla** – jedno z najczęściej występujących zagrożeń raportowanych przez uczestników rynku finansowego, obserwowano wystąpienia AgentTesla niemal we wszystkich możliwych konfiguracjach i wariantach, które były raportowane w obszarze cyberbezpieczeństwa (grafika 35-36).



Grafika 35. Schemat kampanii AgentTesla



Subject: MONIKA: Nie otrzymano żądania faktury
Date: 11/03/2024 12:47 **From:** [redacted] **To:** undisclosed-recipients;

dobry:

W dniu 15.02.24 wykonaliśmy przelew w związku z Twoim budżetem 4128. Nie otrzymaliśmy faktury związanej z tą płatnością.
Wyślij go do nas na ten adres e-mail.

Załączam kopię wpłaty i budżet, sprawdzam czy nie ma błędów i poprawiam

Wszystkiego najlepszego.

[redacted]

DOWÓD WPŁATY.rar

Grafika 36. Przykład wiadomości z kampanii AgentTesla

- **GuLoader** – obserwowano również kampanie tzw. loaderów, czyli oprogramowania, które miało możliwości pobrania innego złośliwego oprogramowania, jak GuLoader – jednego z najczęściej wykorzystywanych. Inne obserwowane loadery to: XLoader, ModiLoader oraz DelphiLoader (grafika 37).

Grafika 37. Przykład wiadomości z GuLoaderem

- **STRRAT** – kolejne oprogramowanie typu RAT (ang. Remote Access Trojan), które posiada także moduły charakterystyczne dla stealera. Co ciekawe, podszywa się ono pod ransomware – zmienia rozszerzenia plików na .crimson i zostawia notatkę z żądaniem okupu, jednak w rzeczywistości nie dochodzi do szyfrowania danych (grafika 38).

Grafika 38. Wiadomość z STRRAT, dystrybuowana z polskich adresów e-mail

- **Xworm** – kolejny przedstawiciel złośliwego oprogramowania typu RAT, którego wykorzystanie jest obserwowane również w sektorach finansowych innych państw (grafika 39).

Subject: Zapytanie ofertowe 908121
Date: 29/05/2024 13:03 **From:** [redacted] **To:** undisclosed-recipients;;

Cześć,

Szukamy zakupu Twojego produktu dla naszego klienta.

Proszę znaleźć dołączone zapytanie dla pierwszego etapu tego zakupu.

Załączony arkusz zawiera docelowe ceny dla większości produktów.
Podkreśliłem 10 elementów do skupienia się na cenach – pozostałe elementy są opcjonalne do ceny (zastosujemy podobny poziom cen w oparciu o inne ceny).

Proszę wrócić do mnie na lub przed 04/06/2024

Jeśli potrzebujesz więcej czasu, daj mi znać, dopóki nie będziesz potrzebował.

Jeśli masz jakiekolwiek pytania, proszę również dać mi znać.

Z poważaniem / Best regards

[redacted]

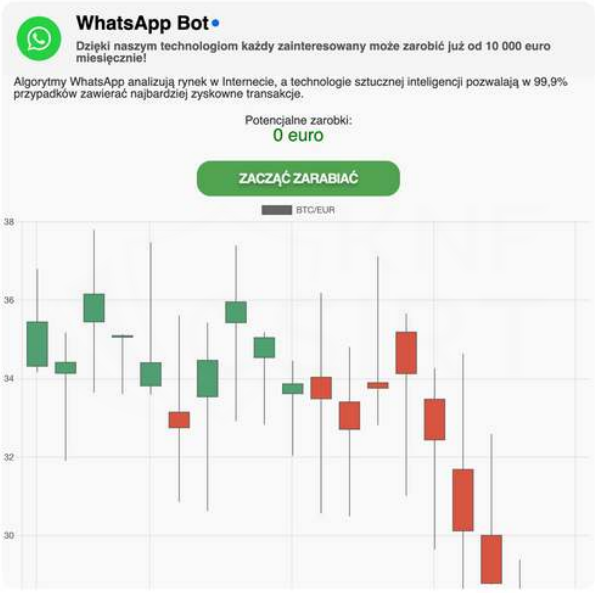
RFQ_908121777210000056560 01.tgz

Grafika 39. Przykład wiadomości dystrybuującej Xworm

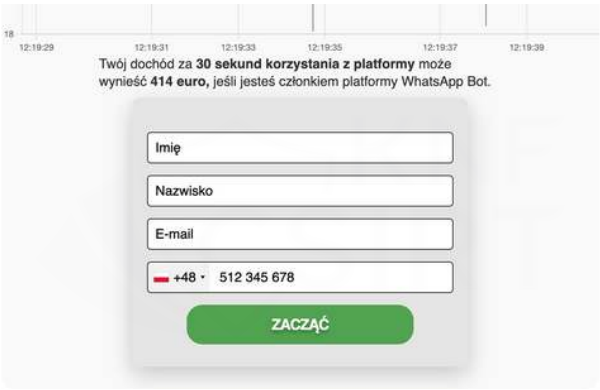
- **Malware mobilny:**

Nieprzerwanie od wybuchu wojny ukraińsko-rosyjskiej i rozpadu wielu grup przestępczych specjalizujących się w wytwarzaniu złośliwego oprogramowania na urządzenia mobilne, obserwowano malejący trend w liczbie kampanii – zwłaszcza trojanów bankowych – wymierzonych w uczestników polskiego sektora finansowego.

Oprogramowanie wykorzystywane przede wszystkim w oszustwach inwestycyjnych. Aplikacje dystrybuowane poprzez reklamy na portalach społecznościowych miały za zadanie przede wszystkim zbierać dane kontaktowe potencjalnych ofiar lub uwiarygodniać oszustwo w dalszych etapach. W tego typu kampaniach stosowano zarówno „zwykłe" aplikacje, jak i te korzystające z mechanizmów WebAPK/PWA (grafika 40–41).

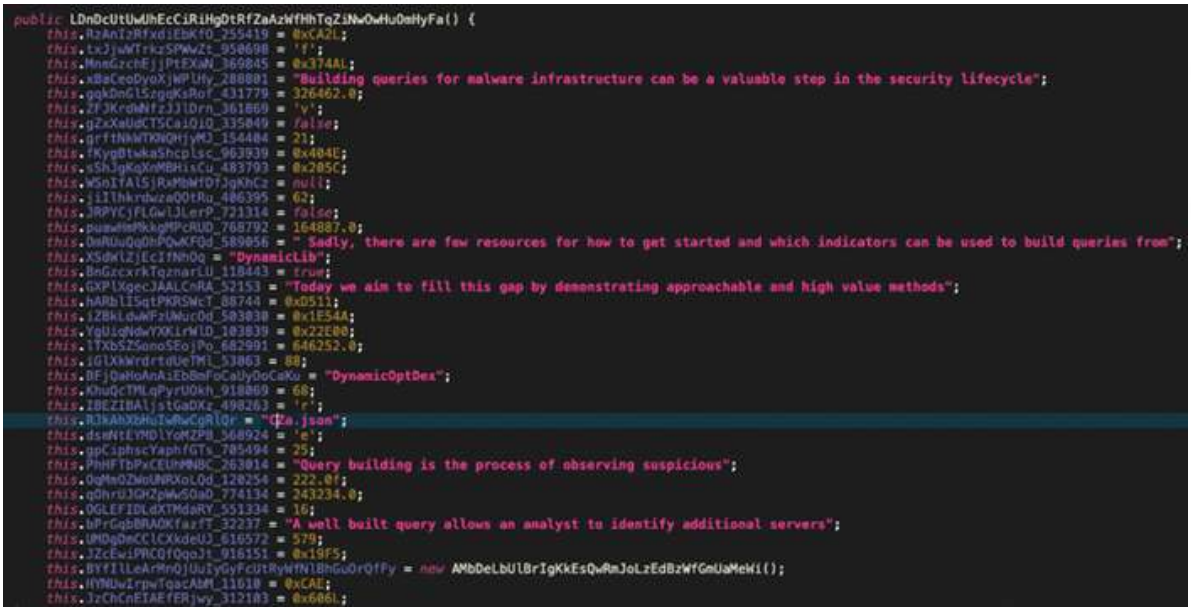


Grafika 40. Ekran aplikacji mobilnej podtrzymującej oszustwo inwestycyjne



Grafika 41. Ekran aplikacji mobilnej zbierający dane do oszustwa inwestycyjnego

- PeoPay Smart – kampania złośliwego oprogramowania, która wykorzystując komponent WebView, otwierała fałszywą stronę imitującą panel logowania do aplikacji bankowości elektronicznej. Atakujący w kodzie źródłowym umieścili ciągi znaków z jednego z artykułów o śledzeniu infrastruktury cyberprzestępców. Aplikacja mogła także wykradać wiadomości SMS, co pozwalało na przechwytywanie kodów autoryzacyjnych z banku (grafika 42).



Grafika 42. Konfiguracja złośliwej aplikacji

08.
RAPORTY I ANALIZY

PUBLIKACJE: ANALIZY, OPRACOWANIA, RAPORTY

Zespół CSIRT KNF prowadzi monitoring oraz analizę metod stosowanych przez cyberprzestępców i na podstawie zebranych informacji na bieżąco publikuje raporty. Opracowania te skupiają uwagę na dynamicznie rozwijających się zagrożeniach w cyberprzestrzeni i mają na celu zwiększenie świadomości użytkowników oraz ich skuteczną reakcję.

Wybrane opracowania opublikowane przez CSIRT KNF w 2024 roku:

1. „Booking.com – rezerwacja malware”

- Opracowanie: Link do raportu
- Opis: Raport opisujący oszustwa wymierzone zarówno we właścicieli hoteli, jak i gości hotelowych. W opracowaniu wskazano na techniki stosowane przez cyberprzestępców do kradzieży poufnych informacji i pieniędzy.
- Miesiąc publikacji: **Styczeń 2024**

2. „Kryptowaluty za darmo – przejęcia kont na portalu Twitter/X"

- Opracowanie: Link do raportu
- Opis: W opracowaniu wskazano do jakich celów cyberprzestępcy wykorzystują przejęte konta na portalu Twitter/X, czym jest „airdrop" i jak można przeciwdziałać fałszywym promocjom. Przybliżono także, co kryje się pod pojęciem „drainer" i dlaczego stanowi zagrożenie dla kryptowalut.
- Miesiąc publikacji: **Styczeń 2024**

3. „Analiza kampanii mobilnego malware dystrybuowanego poprzez reklamy Facebook"

- Opracowanie: Link do raportu
- Opis: Analiza techniczna przedstawia kampanię phishingową podszywającą się pod #PeoPay, dystrybuowaną za pośrednictwem reklam na portalu Facebook. Cyberprzestępcy w publikowanych reklamach oferowali użytkownikom możliwość otrzymania rzekomych środków w zamian za zainstalowanie aplikacji.
- Miesiąc publikacji: **Luty 2024**

4. „HookBuilder - stwórzmy Hookbota”

- Opracowanie PL: Link do raportu PL
- Opracowanie EN: Link do raportu EN
- Opis: Raport przybliża analizę infrastruktury malware na Androida - HookBot oraz HookBuilder.
- Miesiąc publikacji: **Luty 2024**

5. „Twoje konto na Facebooku może stać się narzędziem oszustów”

- Opracowanie PL: Link do raportu PL
- Opracowanie EN: Link do raportu EN
- Opis: W raporcie został ukazany rosnący problem kampanii phishingowych celujących w konta reklamowe. Przybliżono również metody i sposoby ochrony konta reklamowego użytkownika.
- Miesiąc publikacji: **Luty 2024**

6. „Phishing jako usługa – demaskowanie ekosystemu kampanii phishingowych”

- Opracowanie: Link do raportu
- Opis: W opracowaniu przeanalizowano międzynarodową kampanię phishingową. Raport ujawnia narzędzia i infrastrukturę wykorzystywaną przez cyberprzestępców oraz ich metody szybkiego rozpowszechniania fałszywych stron.
- Miesiąc publikacji: **Marzec 2024**

7. „Schematy i metody oszustw inwestycyjnych”

- Opracowanie: Link do raportu
- Opis: W opracowaniu przeanalizowano międzynarodową kampanię phishingową. Raport ujawnia narzędzia i infrastrukturę wykorzystywaną przez cyberprzestępców oraz ich metody szybkiego rozpowszechniania fałszywych stron internetowych.
- Miesiąc publikacji: **Sierpień 2024**

8. „Dobre praktyki w zakresie zapobiegania i reagowania na ataki ransomware"

- Opracowanie: Link do raportu
- Opis: Opracowanie zostało przygotowane przez zespół CSIRT KNF we współpracy z podmiotami rynku finansowego oraz ekspertami z obszaru cyberbezpieczeństwa. Dokument zawiera podpowiedzi i wytyczne, które pozwalają zwiększyć odporność systemów informatycznych organizacji na ataki ransomware, a w przypadku ich wystąpienia, podpowiada jak podjąć odpowiednie działania, aby zmitygować skutki takiego incydentu. Ataki ransomware stanowią aktualnie jedno z najpoważniejszych zagrożeń dla bezpieczeństwa organizacji. Każda organizacja powinna przeprowadzić analizę ryzyka w obszarze ataków ransomware na swoją infrastrukturę teleinformatyczną i na podstawie jej wyników przygotować odpowiednie procesy, procedury oraz dobrać odpowiednie narzędzia i rozwiązania techniczne, w taki sposób, aby zminimalizować ryzyko wystąpienia incydentu ransomware.
- Miesiąc publikacji: **Maj 2024**

Zapraszamy do zapoznania się z naszymi publikacjami, opracowaniami i analizami, które dostępne są tutaj[4].

[4] https://cebrf.knf.gov.pl/komunikaty/raporty

09. WYBRANE PODATNOŚCI W SYSTEMACH INFORMATYCZNYCH W 2024 ROKU

WYBRANE PODATNOŚCI W SYSTEMACH INFORMATYCZNYCH W 2024 ROKU

Do najistotniejszych podatności w systemach informatycznych, które były aktywnie wykorzystywane w kampaniach prowadzonych przez threat aktorów w 2024 roku, można zaliczyć luki bezpieczeństwa zidentyfikowane w produktach firm: Ivanti, Fortinet oraz Zimbra. Wśród podatności ujawnionych w produktach Ivanti w 2024 roku, do najistotniejszych można zaliczyć luki bezpieczeństwa, które zostały opisane w:

- **CVE-2023-46805 CVSS 8.2** – Ivanti Connect Secure and Ivanti Policy Secure Authentication Bypass Vulnerability. Opublikowana 10 stycznia 2024 roku[5].
- **CVE-2024-21887 CVSS 9.1** – Ivanti Connect Secure and Ivanti Policy Secure Command Injection Vulnerability. Opublikowana 10 stycznia 2024 roku[6].
- **CVE-2024-21888 CVSS 8.8** – Ivanti Connect Secure and Ivanti Policy Secure Privilege Escalation Vulnerability. Opublikowana 31 stycznia 2024 roku[7].
- **CVE-2024-21893 CVSS 8.2** – Ivanti Connect Secure, Ivanti Policy Secure and Ivanti Neurons for ZTA Server-Side Request Forgery (SSRF) Vulnerability. Opublikowana 31 stycznia 2024 roku[8].
- **CVE-2024-22024 CVSS 8.3** – Ivanti Connect Secure, Ivanti Policy Secure and ZTA Gateways XML External Entity (XXE) Vulnerability. Opublikowana 8 lutego 2024 roku[9].

[5] https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US
[6] https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US
[7] https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US
[8] https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US
[9] https://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?language=en_US

Trzy ze wskazanych podatności były aktywnie wykorzystywane przez threat aktorów w kampaniach, które zidentyfikowano na początku 2024 roku. Podatności CVE-2023-46805 oraz CVE-2024-21887 były w styczniu 2024 roku, aktywnie wykorzystywane w kampaniach do instalacji Webshella na podatnych urządzeniach firmy Ivanti. Eksploitowanie obu luk pozwalało threat aktorom na ominięcie mechanizmu uwierzytelnienia oraz uzyskanie możliwości zdalnego wykonania kodu w podatnym środowisku.

Podatność CVE-2024-21893, typu server-side request forgery, była aktywnie wyszukiwana i wykorzystywana od lutego 2024 roku, krótko po opublikowaniu PoC tej podatności. Jej skuteczne wykorzystanie zapewniało atakującym ograniczony dostęp do zasobów.

Opisane podatności były na tyle aktywnie wykorzystywane, a ich remediacja, ze strony producenta, na tyle długotrwała i nieskuteczna, że Agencja rządowa CISA, po dodaniu luk do katalogu znanych, ekslpoitowanych podatności, rekomendowała aby agencje rządowe w USA wycofały z produkcyjnego użytkowania wskazane, podatne produkty Ivanti: Ivanti Connect Secure and Ivanti Policy Secure. Nawet jeśli została na nich zainstalowana poprawka bezpieczeństwa lub zastosowano inne środki remediacyjne.

Lista źródeł:

- https://socradar.io/attackers-exploit-ivanti-connect-secure-zero-day-vulnerabilities-to-deploy-webshells-cve-2023-46805-cve-2024-21887
- https://www.tenable.com/cve/CVE-2024-21893
- https://www.tenable.com/blog/cve-2023-46805-cve-2024-21887-cve-2024-21888-and-cve-2024-21893-frequently-asked-questions
- https://socradar.io/cybersecurity-in-2025-2024s-biggest-cyber-attacks-lessons-for-future/

Pośród podatności, zidentyfikowanych w 2024 roku w produktach firmy Fortinet, dwie krytyczne luki były szczególnie aktywnie wykorzystywane przez threat aktorów:

- **CVE-2024-21762 CVSS 9.8** – Forti OS - SSL VPN, N-day vulnerability, allows a remote unauthenticated actor to execute arbitrary commands by specially crafted HTTP requests. Opublikowana 9 lutego 2024 roku.

- **CVE-2024-47575 CVSS 9.8** – missing authentication for critical function in FortiManager and FortiManager Cloud. Opublikowana 23 października 2024 roku.

Podatność CVE-2024-21762 umożliwiała nieautoryzowanemu zdalnemu aktorowi wykonanie dowolnych poleceń za pomocą specjalnie spreparowanych żądań HTTP. Podatnością dotknięte były komponenty Secure Socket Layer Virtual Private Network (SSL VPN) w systemie operacyjnym **FortiOS**. Zgodnie z informacją opublikowaną przez producenta, podatność ta była wykorzystywana w atakach ukierunkowanych na:

- infrastrukturę krytyczną,
- sektor produkcyjny,
- dostawców usług rządowych.

Podatność CVE-2024-47575, zidentyfikowana w platformie zarządzania oprogramowaniem Fortinet, **FortiManager**, była aktywnie wykorzystywana przez threat aktorów umożliwiając atakującym wykonanie dowolnego kodu lub poleceń za pomocą specjalnie spreparowanych żądań. Luka była wykorzystywana m.in. przez grupę monitorowaną przez Mandiant, jako UNC5820. Aktorzy za jej pomocą eksfiltrowali pliki konfiguracyjne urządzeń FortiGate, zarządzane za pomocą podatnego produktu FortiManager.

Lista źródeł:

- https://cloud.google.com/blog/topics/threat-intelligence/fortimanager-zero-day-exploitation-cve-2024-47575
- https://www.csoonline.com/article/3586092/critical-fortinet-vulnerability-finds-zero-day-rce-exploits.html
- https://www.csoonline.com/article/1306816/fortinet-urges-patching-n-day-bug-amid-ongoing-nation-state-exploitation.html

Podatność, pozwalająca na zdalne wykonanie kodu, która została w 2024 roku ujawniona w produkcie firmy Zimbra Collaboration Suite (ZCS), opisana w **CVE-2024-45519 z CVSS 9.8**, z uwagi na krytyczność, niski poziom skomplikowania eksploitacji oraz aktywne wykorzystywanie w kampaniach, została uwzględniona w Rekomendacji Pełnomocnika Rządu ds. Cyberbezpieczeństwa dotyczącej oprogramowania **Zimbra Collaboration**, w której stwierdza się, że stosowanie oprogramowania z tą podatnością ma negatywny wpływ na bezpieczeństwo publiczne i istotny interes bezpieczeństwa państwa.

Lista źródeł:

- https://www.gov.pl/web/baza-wiedzy/rekomendacja-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-dotyczaca-oprogramowania-zimbra-collaboration
- https://cybersecuritynews.com/zimbra-rce-vulnerability
- https://socradar.io/rce-vulnerability-in-zimbra-cve-2024-45519/

08. DZIAŁALNOŚĆ EDUKACYJNA

Działania edukacyjne są istotnym elementem budowania świadomości zagrożeń dla wzmacniania poziomu cyberbezpieczeństwa użytkowników Internetu. W związku z rosnącą z roku na rok liczbą zagrożeń, koniecznym staje się ciągłe podnoszenie świadomości nieprofesjonalnych uczestników rynku finansowego.

Zespół CSIRT KNF przeprowadził działania edukacyjne m.in. w ramach projektu edukacyjnego **Centrum Edukacji dla Uczestników Rynku – CEDUR**. W ramach projektu CEDUR, realizowanego przez Urząd Komisji Nadzoru Finansowego, zorganizowano webinaria dla różnych grup odbiorców, m.in. dla uczniów i nauczycieli oraz rodziców i opiekunów, seniorów i ich opiekunów, a także indywidualnych uczestników rynku finansowego.

Wśród inicjatyw propagujących wiedzę z zakresu cyberbezpieczeństwa wśród nieprofesjonalnych uczestników rynku finansowego z udziałem przedstawicieli zespołu CSIRT KNF w charakterze prelegentów, wymienić można m.in.:

- webinaria **CEDUR** zorganizowane w ramach 12. edycji kampanii **Global Money Week (GMW)** – Światowy Tydzień Pieniądza, skierowane do uczniów i nauczycieli szkół podstawowych i ponadpodstawowych oraz do rodziców i opiekunów:
  - „Cyberoszuści atakują – jak nie dać się okraść w Internecie" (2 edycje);
  - „Bezpieczny telefon – jak chronić się przed cyberprzestępcami";
  - „Dziecko w sieci – cyberbezpieczeństwo z perspektywy rodzica".
- webinaria CEDUR zorganizowane w ramach kampanii **World Inwestor Week (WIW)** – Światowy Tydzień Inwestora, skierowane do uczniów szkół ponadpodstawowych i nauczycieli oraz do indywidualnych uczestników rynku finansowego:
  - „Cyberoszustwa inwestycyjne – jak się przed nimi chronić";
  - „Najnowsze sposoby działania cyberoszustów – czyli jak nie dać się okraść w Internecie".
- prezentację „Jak nie dać się oszukać w Internecie" podczas **Ring the Bell for Financial Literacy** – uroczystości inaugurującej krajową edycję **WIW 2024**;
- webinaria CEDUR dla seniorów i ich opiekunów:
  - „Bezpieczny senior – jak nie dać się oszukać w Internecie";
  - „Na co uważać i jak nie dać się okraść w Internecie – bankowość elektroniczna dla seniorów" (3 edycje).

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 do indywidulanych uczestników rynku, w tym seniorów i ich opiekunów, UKNF współpracował z Komendą Główną Policji, Ministerstwem Rodziny, Pracy i Polityki Społecznej oraz Ministrem do spraw Polityki Senioralnej.
Udział w inicjatywach szkoleniowych, w tym webinariach CEDUR, był bezpłatny. Informacje o webinariach CEDUR są dostępne pod adresem www.knf.gov.pl na podstronie „Edukacja finansowa/Seminaria CEDUR".

Przedstawiciele zespołu CSIRT KNF w 2024 roku uczestniczyli również w konferencjach i wydarzeniach poświęconych tematyce cyberbezpieczeństwa m.in.:

- Secure 2024,
- Confidence 2024,
- BSides Warsaw,
- OhMyHack 2024,
- Cyber24Day,
- Europejski Miesiąc Cyberbezpieczeństwa,
- Partnerstwo dla Cyberbezpieczeństwa.

Aktywność w mediach społecznościowych

Zespół CSIRT KNF prowadzi profile w mediach społecznościowych, tj. na portalach X, Facebook i LinkedIn, gdzie publikuje informacje i ostrzeżenia dotyczące najnowszych sposobów działania cyberprzestępców oraz oszustw internetowych. Aby dotrzeć do jak najszerszego grona odbiorców w 2024 roku przygotowano **254** publikacje w mediach społecznościowych, które dotyczyły najnowszych metod i sposobów działania cyberprzestępców. Na podstawie wiadomości pochodzących z publikacji CSIRT KNF w 2024 roku powstało ponad dwa tysiące artykułów w portalach branżowych oraz informacyjnych o zasięgu ogólnopolskim.

W 2024 roku ostrzeżenia publikowane w mediach społecznościowych dotyczyły głównie:

- fałszywych stron bankowości elektronicznej,
- złośliwego oprogramowania specjalizującego się w kradzieży środków finansowych,
- fałszywych produktów inwestycyjnych wyłudzających dane od użytkownika,
- fałszywych stron portali sprzedażowych wyłudzających dane kart płatniczych,
- fałszywych stron firm kurierskich wyłudzających dane kart płatniczych.

Grafika 42. Ostrzeżenie CSIRT KNF w mediach społecznościowych dotyczące weryfikacji domeny

09. ROK 2024 POD HASŁEM "DORA"

ROK 2024 POD HASŁEM „DORA”

W 2024 roku trwały przygotowania w związku z wdrożeniem 17 stycznia 2025 roku Rozporządzenia DORA.

Zacznijmy od tego, czym jest DORA

DORA (ang. Digital Operational Resilience Act), a w zasadzie Rozporządzenie DORA, to unijne przepisy mające na celu ujednolicenie i wzmocnienie odporności operacyjnej instytucji sektorów finansowych krajów Unii Europejskiej, w tym także Polski. To swoista odpowiedź regulatora europejskiego na rozszerzający się krajobraz cyberzagrożeń i nieustannie rosnącą potrzebę wykorzystywania technologii informacyjno-komunikacyjnych przez wspominane wcześniej organizacje. Aby osiągnąć zamierzone cele, DORA nakłada obowiązek skutecznego i uregulowanego zarządzania ryzykiem związanym z technologiami informatycznymi. Rozporządzenie zostało podzielone na 5 obszarów. Są nimi:

- zarządzanie ryzykiem ICT,
- testowanie operacyjnej odporności cyfrowej, czyli testy TLPT,
- zarządzanie ryzykiem dostawców usług ICT,
- stworzenie ram kontroli i nadzoru krajowych oraz unijnych organów nadzoru, w tym nad kluczowymi dostawcami usług ICT i łańcuchem dostaw,
- ujednolicenie, rozbudowanie i scentralizowanie zgłaszania incydentów poważnych ICT przez podmioty finansowe na poziomie krajowym i unijnym.

CSIRT KNF a DORA

Jako sektorowy zespół cyberbezpieczeństwa odpowiedzialni jesteśmy za część dotyczącą raportowania incydentów poważnych ICT, czyli zgodnie z omawianym rozporządzeniem, zdarzeń *„(...) o dużym negatywnym wpływie na sieci i systemy informatyczne, które wspierają krytyczne lub istotne funkcje podmiotu finansowego (...)”*. Więcej na ten temat w artykule „Definicje i przegląd obowiązków w obszarze zarządzania incydentami związanymi z ICT”.

Aby dane zdarzenie mogło być uznane za incydent poważny ICT, musi ono spełnić określone kryteria klasyfikacji i progi istotności. Obejmują one m.in.: liczbę klientów, kwotę lub liczbę transakcji, których dotknęło zdarzenie, krytyczność usług, czas trwania zdarzenia, ewentualną utratę danych, skutki reputacyjne i gospodarcze, zasięg geograficzny.

Zdarzenie zakwalifikowane jako incydent poważny ICT należy zaraportować do Urzędu Komisji Nadzoru Finansowego, a docelowo do zespołu CSIRT KNF za pośrednictwem Systemu Obsługi Incydentów DORA (SOID), dostępnego na stronie: https://csirt.knf.gov.pl. Formularz jest podzielony na 3 etapy:

- wstępne powiadomienie;
- sprawozdanie śródokresowe;
- sprawozdanie końcowe.

Ważne jest także, aby pamiętać, że Rozporządzenie DORA wprowadziło również ramy czasowe:

1. Wstępne powiadomienie składane jest:

a. do 4 godzin od zaklasyfikowania zdarzenia jako incydent,

b. ale nie później niż 24 godziny od wykrycia incydentu.

2. Sprawozdanie śródokresowe składane jest do 72 godzin od zgłoszenia wstępnego powiadomienia.

3. Sprawozdanie końcowe składane jest do 30 dni od daty złożenia ostatniego sprawozdania śródokresowego.

Testy TLPT – druga domena CSIRT KNF

Drugim ważnym obszarem działań dla sektorowego zespołu cyberbezpieczeństwa, jakim jest CSIRT KNF, są testy TLPT (Threat-Led Penetration Testing), czyli testy penetracyjne ukierunkowane na analizę zagrożeń. Mają one na celu nie tylko identyfikację potencjalnych zagrożeń, ale również dogłębną ocenę poziomu zabezpieczeń organizacji – zarówno pod kątem technicznym, jak i organizacyjnym. Testy TLPT są zaprojektowane tak, aby imitować rzeczywiste cyberataki, umożliwiając organizacjom weryfikację poziomu odporności na zagrożenia oraz podjęcie odpowiednich działań naprawczych. Wdrożenie ich jest kluczowe dla skutecznego zarządzania ryzykiem w coraz bardziej złożonym środowisku cyfrowym.