RAPORT ROCZNY CSIRT KNF

2023

SPIS TREŚCI

01. Wstęp (str. 2)

02. Wybrane statystyki z działalności CSIRT KNF (str. 4)

03. TOP 5 Najistotniejszych cyberoszustw i zagrożeń dla klientów rynku finansowego w 2023 roku w ocenie CSIRT KNF (str. 10)

04. Raporty i analizy (str. 50)

05. Działalność edukacyjna CSIRT KNF w 2023 roku (str. 56)

06. Wpływ rozwoju sztucznej inteligencji na działania cyberprzestępców - podsumowanie 2023 roku (str. 62)

01.
WSTĘP

WSTĘP

Mamy zaszczyt przedstawić Państwu Raport Roczny 2023, stanowiący analizę zagrożeń dotyczących cyberbezpieczeństwa w obszarze rynku finansowego, opracowany z perspektywy sektorowego zespołu CSIRT KNF. W raporcie tym prezentujemy różnorodne aspekty zagrożeń, z którymi mierzyli się zarówno profesjonalni jak i nieprofesjonalni uczestnicy rynku finansowego. Wierzymy, że raport będzie stanowił cenne źródło wiedzy dla wszystkich zainteresowanych zagadnieniami związanymi z zagrożeniami i cyberbezpieczeństwem w obszarze finansów.

W minionym, 2023 roku obserwowaliśmy liczne ataki, których celem były środki finansowe uczestników rynku finansowego. Grupy przestępcze rok do roku doskonalą wykorzystywane przez siebie mechanizmy socjotechniki i manipulacji, przez co mogą skutecznie wpływać na zachowania użytkowników. Bardzo poważny problem w 2023 roku stanowiły różnego rodzaju oszustwa dystrybuowane za pośrednictwem nośników reklamowych w popularnych serwisach społecznościowych, wyszukiwarkach internetowych czy też serwisach informacyjnych. Warto również wskazać na znaczący wzrost zainteresowania cyberprzestępców technologią wykorzystującą mechanizmy sztucznej inteligencji w tym narzędzia i techniki pozwalające na generowanie treści deepfake [1] np. w różnego rodzaju oszustwach inwestycyjnych.

W poszczególnych częściach raportu przedstawiamy opisy najistotniejszych zagrożeń, z którymi mieliśmy do czynienia w 2023 roku, informacje nt. działań edukacyjnych podejmowanych przez CSIRT KNF, a także analizy techniczne publikowane na przestrzeni całego roku.

[1] https://cyberpolicy.nask.pl/wpcontent/uploads/2023/09/Cyberbezpieczenstwo-AI.-AI-w-cyberbezpieczenstwie.pdf

02. WYBRANE STATYSTYKI Z DZIAŁALNOŚCI CSIRT KNF

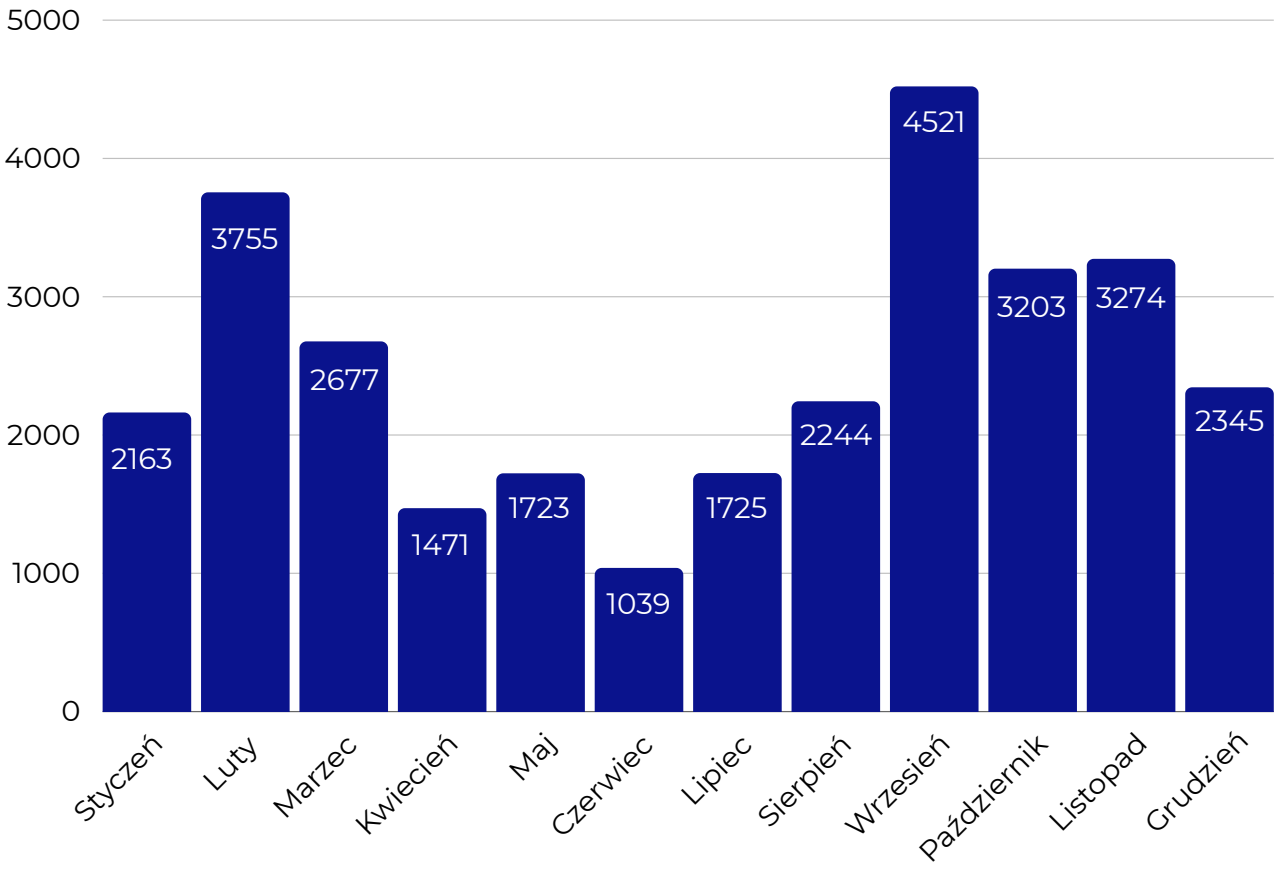
WYBRANE STATYSTYKI Z DZIAŁALNOŚCI CSIRT KNF

Jednym z zadań zespołu CSIRT KNF jest analiza aktualnych trendów oraz zagrożeń w obszarze cyberbezpieczeństwa, w tym ukierunkowanych na ataki na klientów rynku finansowego. Zebrane informacje wykorzystywane są zarówno do działań ograniczających ryzyka wystąpienia incydentu w podmiotach rynku finansowego czy ryzyko strat finansowych klientów, ale również do działań edukacyjnych. Powyższe działania obejmują m.in. wczesne wykrywanie oraz ograniczanie dostępu (w tym blokowanie) do stron internetowych o charakterze oszukańczym. Takie strony internetowe zidentyfikowane przez CSIRT KNF zgłaszane są do CSIRT NASK, w celu ich zablokowania poprzez wpisanie na listę ostrzeżeń[2]. Realizowane jest to w ścisłej współpracy z podmiotami rynku finansowego jak i podmiotami szeroko rozumianego obszaru technologicznego, co pozwala na efektywną i sprawną reakcję w przypadku wykrycia potencjalnych zagrożeń.

Zespół CSIRT KNF w 2023r. zgłosił do zablokowania 30 140 domen phishingowych.

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

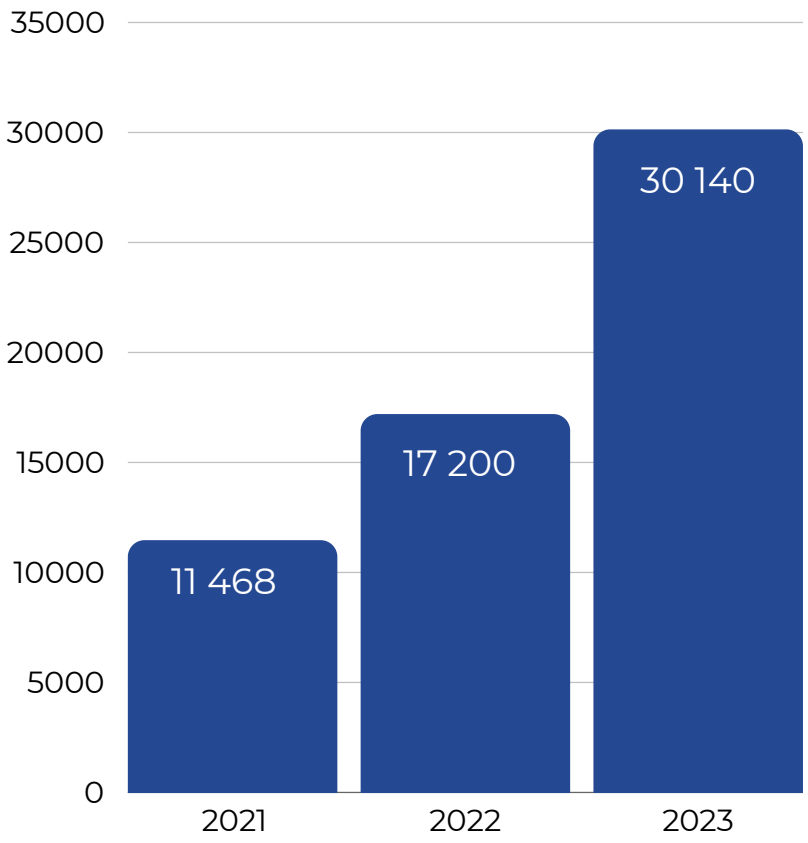
Domeny zgłoszone do CSIRT NASK przez CSIRT KNF w 2023 roku w poszczególnych miesiącach



Wykres 1. Domeny zgłoszone do CSIRT NASK przez CSIRT KNF w 2023 roku w poszczególnych miesiącach

Rosnącą skalę zagrożeń czyhających na użytkowników Internetu obrazuje wzrost liczby wykrywanych przez nas domen phishingowych. Liczba domen phishingowych zidentyfikowanych przez CSIRT KNF wzrosła z **11468** w roku 2021 do **17200** w 2022 roku oraz do **30 140** w 2023 roku.

Liczba zgłoszonych domen phishingowych w latach 2022 i 2023 przez CSIRT KNF



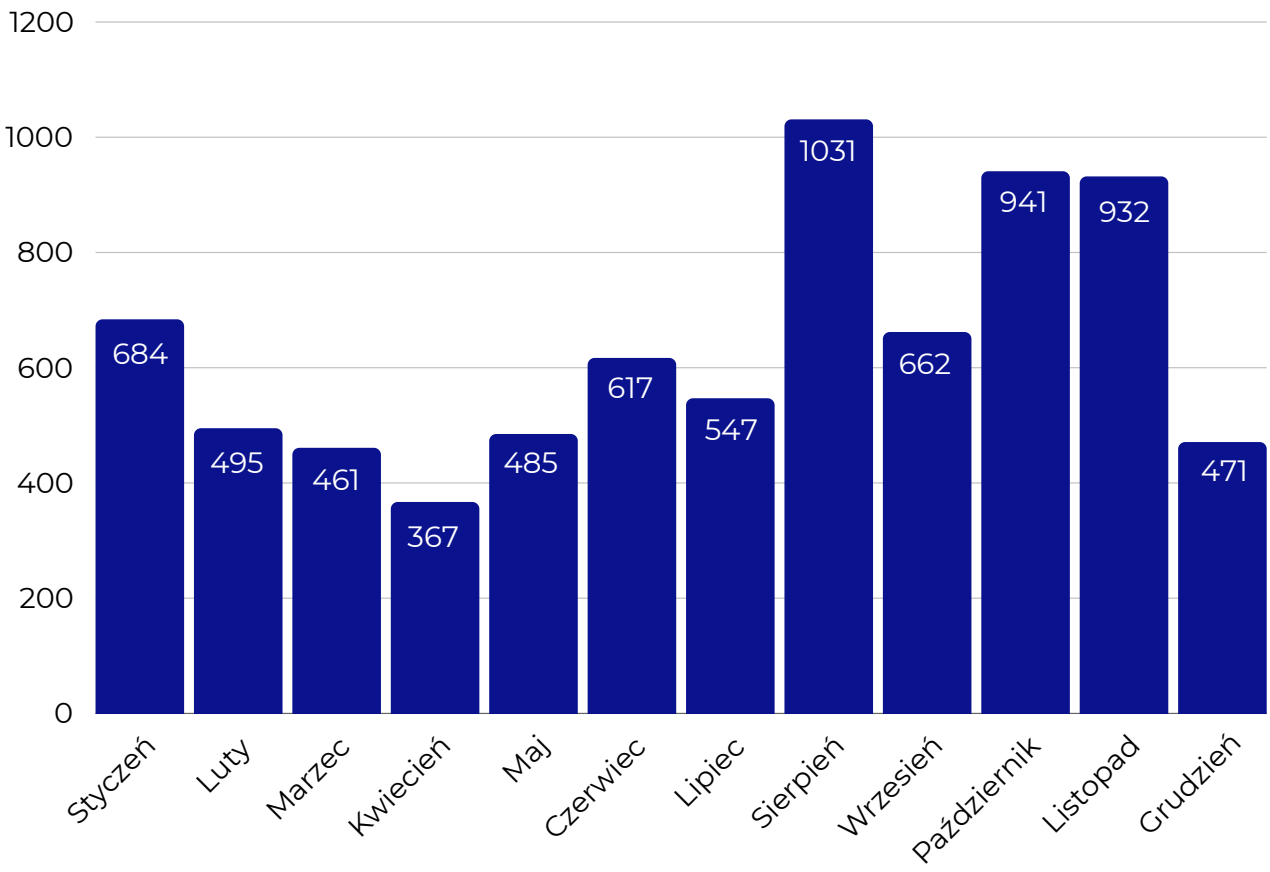
Wykres 2. Liczba zgłoszonych domen phishingowych w latach 2022 i 2023 przez CSIRT KNF

Aż **26 781** zgłoszonych domen, zgłoszonych przez CSIRT KNF na listę ostrzeżeń prowadzoną przez CSIRT NASK w 2023, było związanych z **fałszywymi inwestycjami**.

Wykrywane przez CSIRT KNF reklamy fałszywych inwestycji są jednymi z najczęstszych ataków na użytkowników rynku finansowego w Polsce. Oszustwo „na fałszywą inwestycję" polega na nakłonieniu ofiary do „zainwestowania" środków finansowych w nieistniejące projekty lub produkty inwestycyjne. O szczegółach związanych z tym oszustwem piszemy na stronie **10**.

W 2023 CSIRT KNF zgłosił do zablokowania 7963 oszukańcze reklamy w mediach społecznościowych.

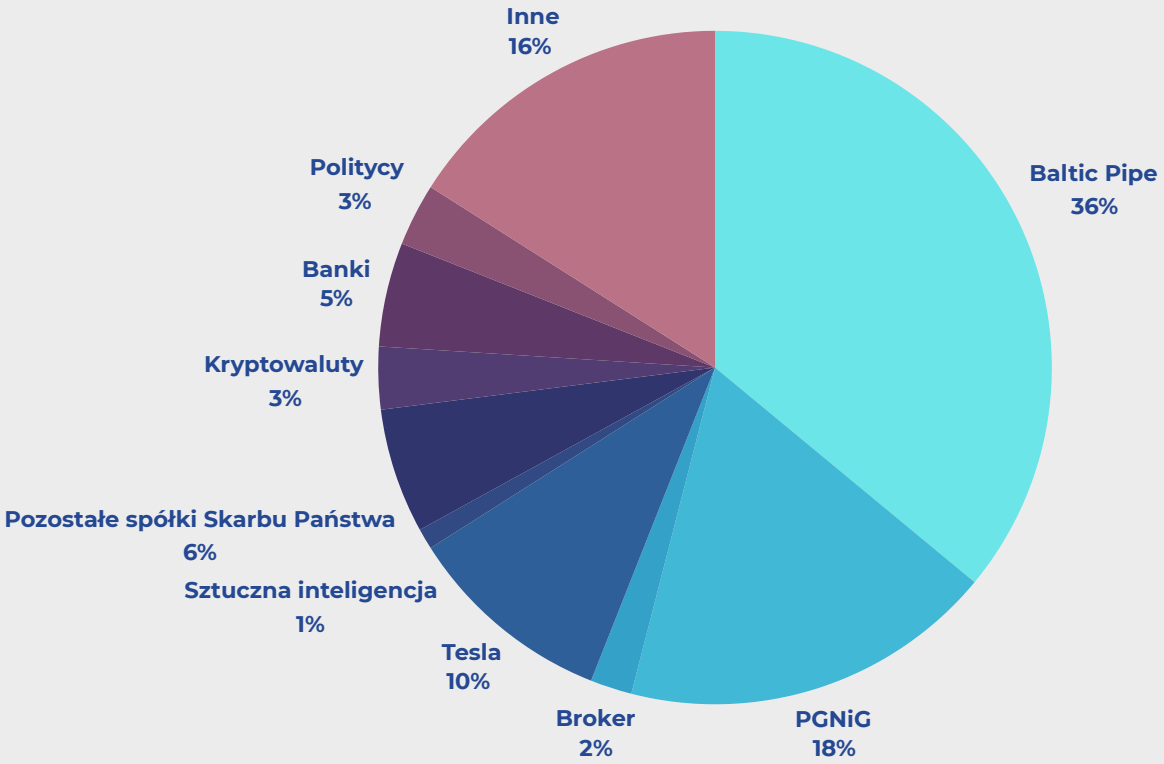
Reklamy zgłoszone do zablokowania w 2023 roku



Wykres 2. Reklamy zgłoszone do zablokowania w 2023 roku

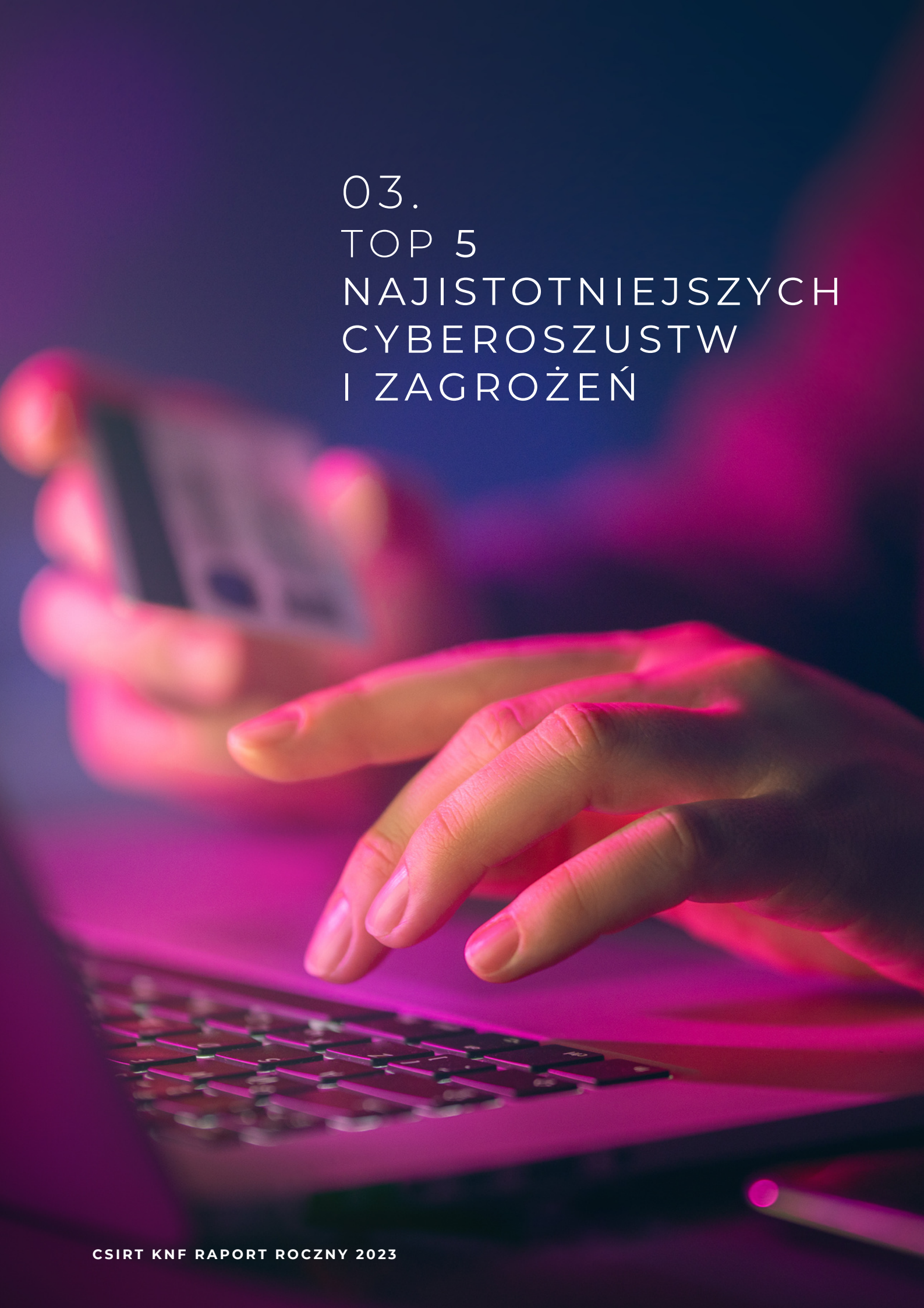
Najwięcej przypadków oszustw wiązało się z wykorzystywaniem wizerunku projektu Baltic Pipe, natomiast drugą najczęściej wykorzystywaną nazwą własną było PGNiG. Dużą część reklam fałszywych inwestycji stanowiły także oszustwa związane z wykorzystaniem marki Tesla. Na wykresie nr. 4 zaprezentowano statystyki oszustw, w których wykorzystywano wizerunki instytucji bankowych, polityków, kryptowalut, brokerów oraz sztucznej inteligencji.

Wykorzystywane wizerunki w oszukańczych reklamach w 2023 roku



Wykres 3. Wykorzystywane wizerunki w oszukańczych reklamach w 2023 roku

Warto tutaj także wskazać, że cyberprzestępcy w 2023 roku coraz częściej wykorzystywali złośliwe strony internetowe nie tylko do wyłudzeń loginów i haseł do bankowości elektronicznej, ale także do różnego rodzaju manipulacji zachęcającej użytkowników do realizacji przelewów na podstawione przez nich konta. Działania mające na celu identyfikację i ograniczenie dostępu złośliwych stron są istotnym elementem działalności zespołu CSIRT KNF. Dzięki temu możliwe jest ograniczenie potencjalnych strat użytkowników wynikających z oszustw internetowych.



03.
TOP 5 NAJISTOTNIEJSZYCH CYBEROSZUSTW I ZAGROŻEŃ

TOP 5 NAJISTOTNIEJSZYCH CYBEROSZUSTW I ZAGROŻEŃ DLA KLIENTÓW RYNKU FINANSOWEGO W 2023 ROKU W OCENIE CSIRT KNF

W tej części raportu prezentujemy najistotniejsze z perspektywy CSIRT KNF zagrożenia, które dotykały użytkowników polskiej cyberprzestrzeni w 2023 roku.

Cyberprzestępcy poza nowymi scenariuszami cyberprzestępstw, udoskonalali również te, które skutecznie od lat wykorzystują w celu kradzieży środków finansowych. Od ponad dwóch lat obserwujemy odejście od zaawansowanych technologiczne ataków np. z wykorzystaniem złośliwego oprogramowania na rzecz socjotechniki i manipulacji ofiarą jako głównego wektora ataków. Wiodącym trendem obserwowanym przez nas w 2023 roku było nakłanianie potencjalnych ofiar do realizacji wpłat na nieistniejące, fałszywe okazje inwestycyjne, których reklamy dystrybuowane były z wykorzystaniem nośników reklamowych w mediach społecznościowych, wyszukiwarkach internetowych lub też popularnych serwisach informacyjnych. Cyberprzestępcy jak co roku dystrybuowali też swoje złośliwe treści przy wykorzystaniu wiadomości SMS lub email.

Fałszywe okazje inwestycyjne

W 2023 roku oszustwa inwestycyjne stanowiły jedno z najistotniejszych zagrożeń dla środków finansowych użytkowników. Mechanizm tych oszustw opiera się na manipulacji i fałszywych obietnicach wysokich zysków przy minimalnym ryzyku. Cyberprzestępcy zamieszczając reklamy fałszywych inwestycji zachęcali użytkowników możliwością szybkiego wzbogacenia się. Ofiary często przyciągane były atrakcyjnymi wizualnie ofertami inwestycji w produkty lub usługi, które w rzeczywistości nie istniały.

Publikowane przez cyberprzestępców reklamy zawierały chwytliwe hasła tj. „zarabiaj z największym bankiem w Polsce" czy „inwestuj bez ryzyka". Oszuści dla uwiarygodnienia swoich działań i wzbudzenia w odbiorcy zaufania, posługiwali się wizerunkami znanych osób, instytucji z sektora energetycznego czy technologicznego, spółek Skarbu Państwa, a także podmiotów z rynku finansowego.

O ile w przypadku np. cyberprzestępstwa polegającego na włamaniu na konto bankowe i kradzieży środków finansowych klienta, straty finansowe ofiary obejmowały środki finansowe zebrane na koncie[3], o tyle oszustwo na fałszywe inwestycje wiązało się zazwyczaj z bardzo wysokimi stratami finansowymi. Ofiara zmanipulowana przez oszustów, wierząc w wysokie zyski bez ryzyka niejednokrotnie przekazywała przestępcom oszczędności całego życia, a nierzadko także dodatkowe środki finansowe uzyskane w ramach zaciągniętego kredytu lub pożyczone od rodziny lub znajomych.

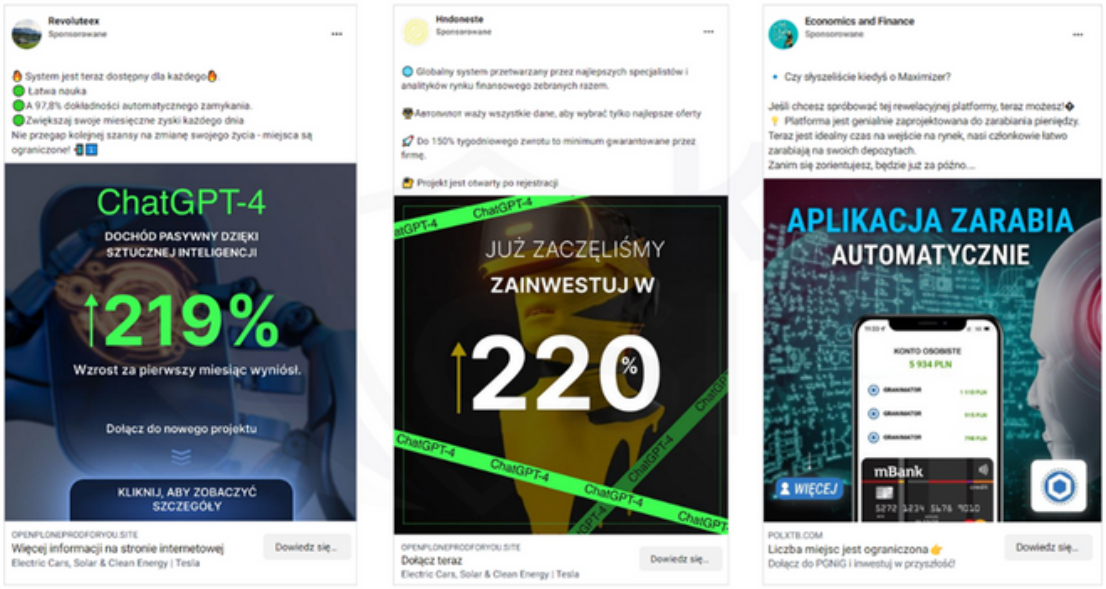
Pamiętaj! Nie istnieją inwestycje finansowe bez ryzyka! O tym w jaki sposób bezpiecznie i świadomie inwestować dowiesz się z kampanii informacyjnych Urzędu Komisji Nadzoru Finansowego pt. „Cyberoszustwa inwestycyjne" oraz „Inwestuj świadomie"[4].

Cyberprzestępcy do dystrybucji reklam fałszywych inwestycji najczęściej wykorzystywali popularne portale społecznościowe, wyszukiwarki internetowe bądź reklamy w ogólnopolskich serwisach informacyjnych.

Grafika 1. Przykłady reklam fałszywych inwestycji, które publikowali cyberprzestępcy

[3] z wyjątkami kiedy przestępcy mając pełny dostęp do internetowego konta bankowego ofiary dodatkowo zaciągali w jego imieniu kredyt, a następnie po przyznaniu tego kredytu również te pieniądze wyprowadzali z konta
[4] https://www.knf.gov.pl/dla_konsumenta/kampanie_informacyjne/cyberoszustwa_inwestycyjne
https://www.knf.gov.pl/dla_konsumenta/kampanie_informacyjne/inwestuj_swiadomie

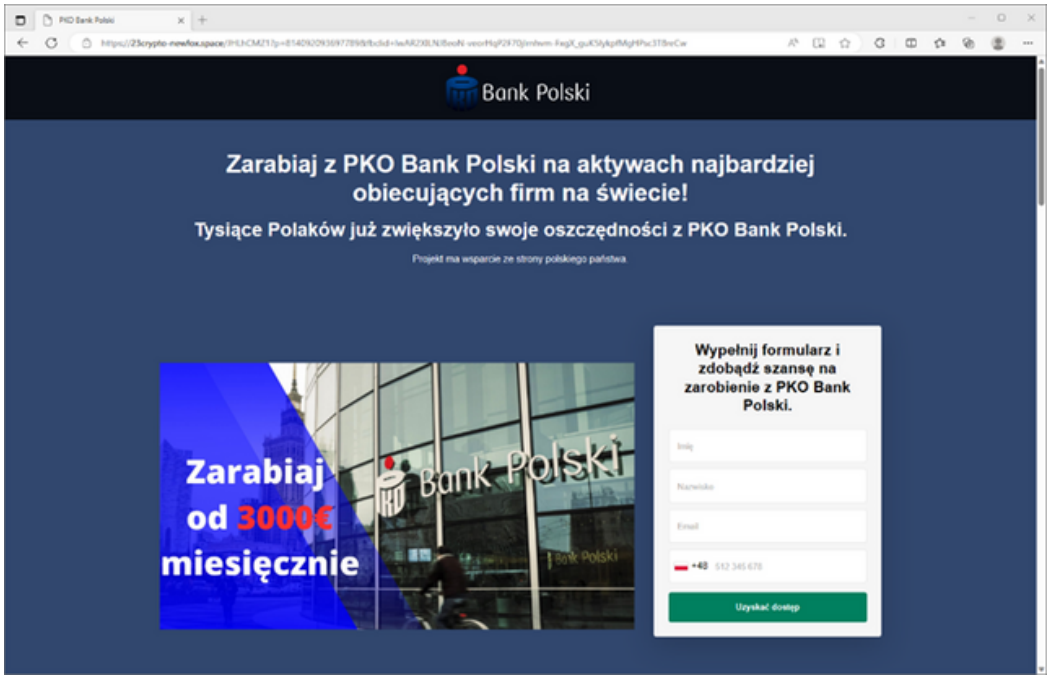
Oszuści uważnie śledzą zmieniające się nastroje społeczne, zainteresowania internautów, otoczenie i trendy technologiczne. Popularność sztucznej inteligencji wpłynęła również na działania cyberprzestępców, którzy dostrzegli potencjał do tworzenia nowych wariantów swoich oszustw. W publikowanych reklamach wykorzystywali oni ten motyw, zachęcając użytkowników do inwestycji i przyciągając obietnicami ogromnych zysków.



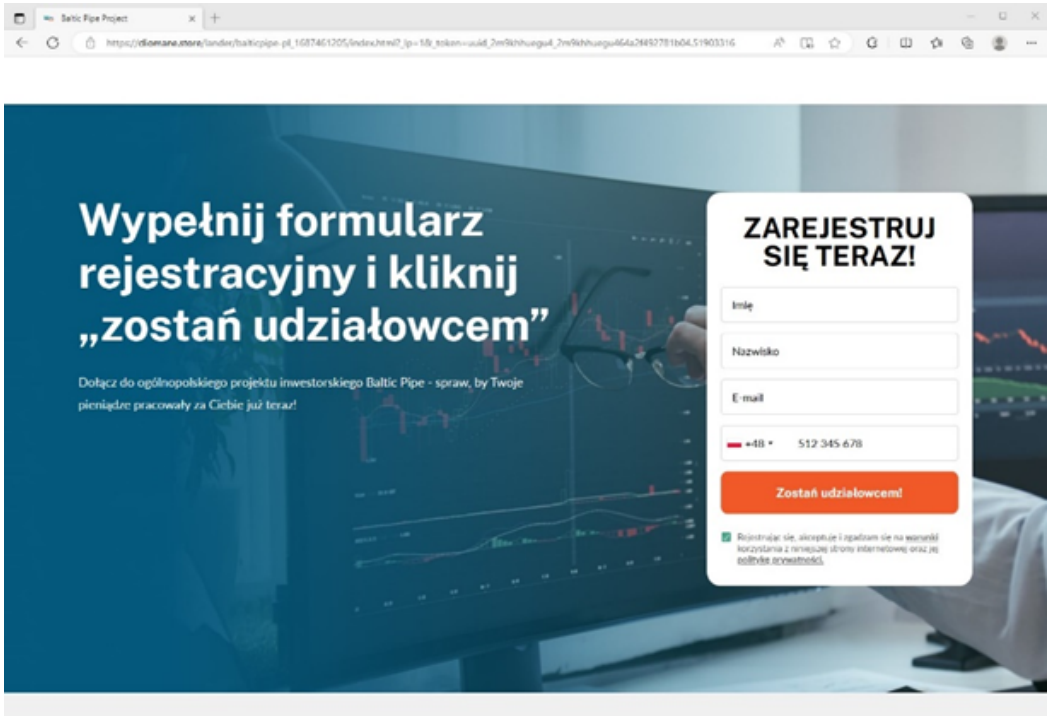
Grafika 2. Przykłady reklam fałszywych inwestycji z wykorzystaniem motywu sztucznej inteligencji

Dystrybucja reklam fałszywych inwestycji przez media społecznościowe

Jednym z głównych narzędzi wykorzystywanych przez oszustów w 2023 roku były fałszywe strony internetowe i oszukańcze reklamy umieszczane w mediach społecznościowych. Reklamy fałszywych inwestycji publikowane w Internecie kierowały użytkowników do niebezpiecznych stron, na których znajdował się formularz rejestracyjny, który nieświadoma ofiara wypełniała. W ten sposób cyberprzestępcy pozyskiwali dane kontaktowe, a w kolejnym kroku nawiązywali kontakt telefoniczny z ofiarami i zachęcali do tego, aby zainwestowały swoje oszczędności.

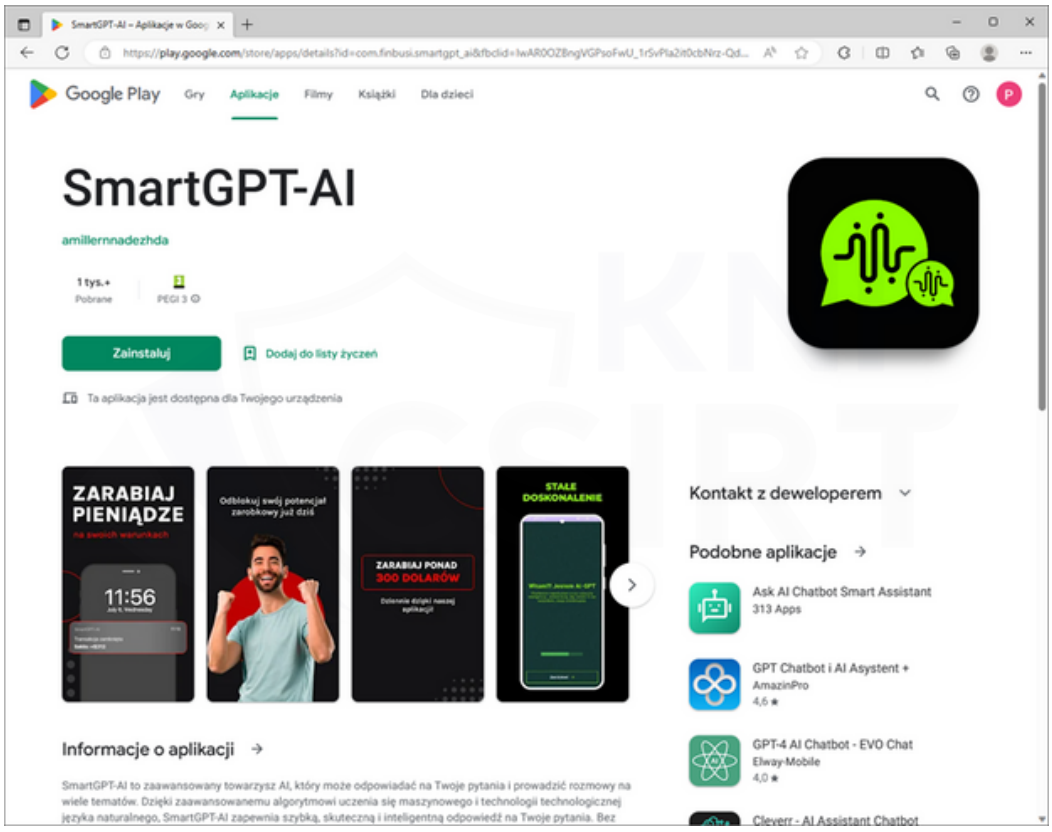


Grafika 3. Przykład fałszywej strony z formularzem do pozostawienia danych kontaktowych



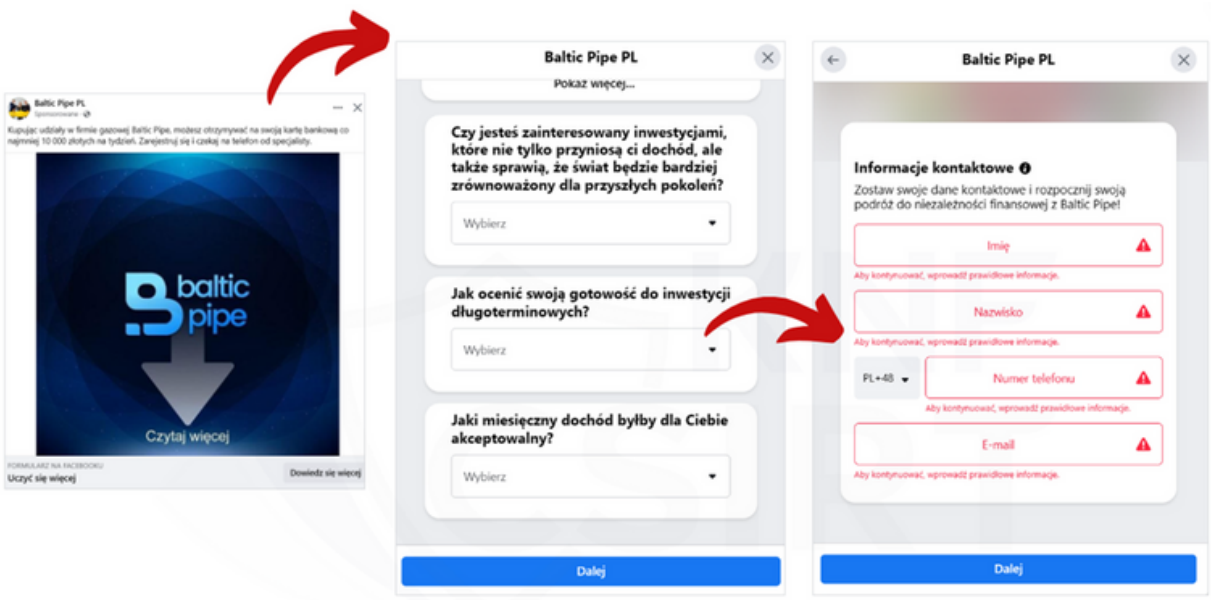
Grafika 4. Przykład fałszywej strony z formularzem do pozostawienia danych kontaktowych

W niektórych scenariuszach ataków z wykorzystaniem fałszywych inwestycji oszuści przekierowywali ofiary sklepu z aplikacjami mobilnymi Google Play, gdzie umieszczone były aplikacje, które po zainstalowaniu i uruchomieniu, wyłudzały dane kontaktowe użytkowników. Aplikacje tego typu często także wykorzystywały wizerunek znanych i rozpoznawalnych podmiotów czy organizacji. Takie działania były celowo zaprojektowane, aby nadać fałszywym inwestycjom pozory autentyczności.



Grafika 5. Przykład niebezpiecznej strony zachęcającej do pobrania fałszywej aplikacji

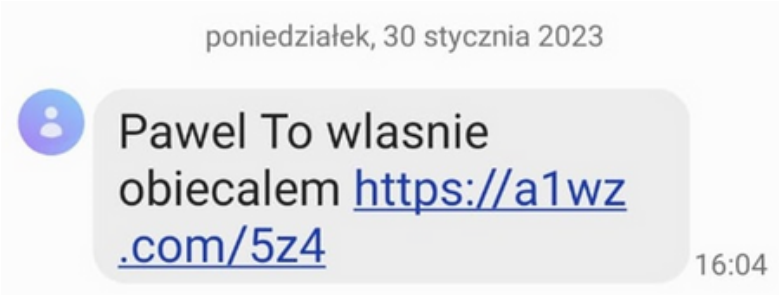
W niektórych przypadkach dane kontaktowe ofiary były wyłudzane z wykorzystaniem wbudowanych w media społecznościowe ankiet i formularzy.



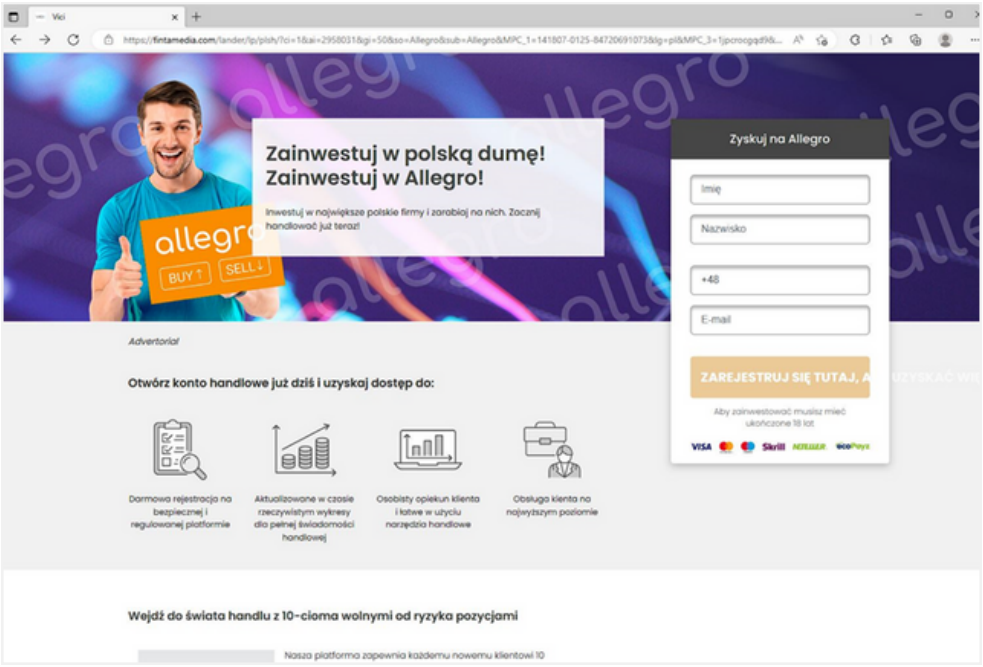
Grafika 6. Jeden z wariantów wykorzystywany przez cyberprzestępców w oszustwach inwestycyjnych

Inne techniki dystrybucji reklam fałszywych inwestycji

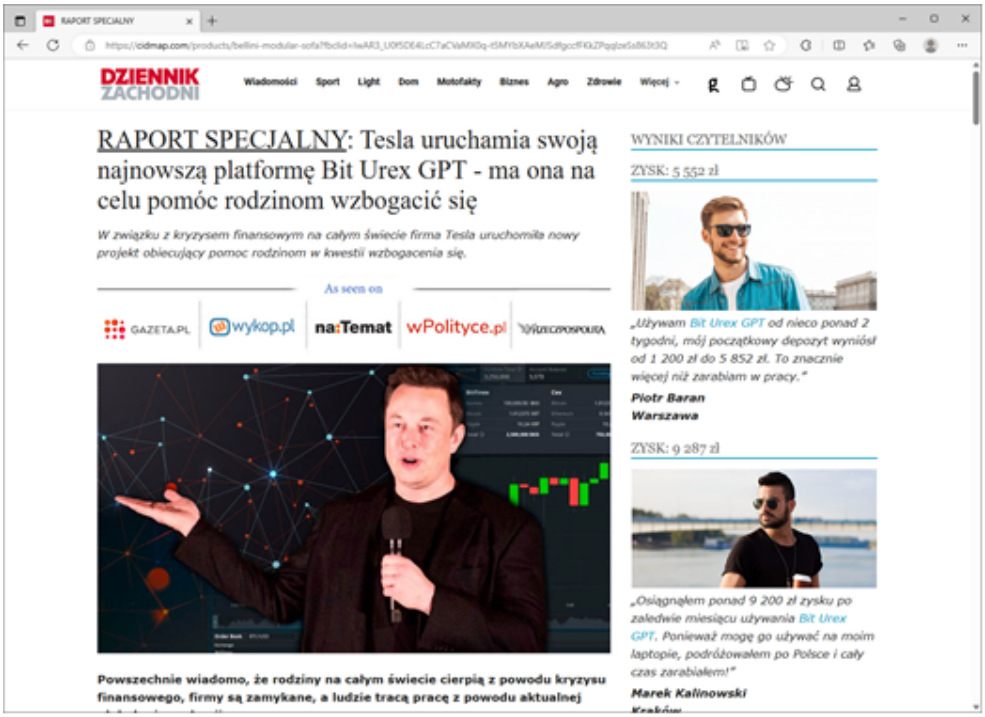
Oprócz mediów społecznościowych, cyberprzestępcy do dystrybucji swoich fałszywych ofert wykorzystywali również e-maile i wiadomości SMS. Podobnie jak reklamy fałszywych inwestycji w mediach społecznościowych, zawierały one linki prowadzące do niebezpiecznych stron internetowych, które zaprojektowane były w taki sposób, aby wyglądały jak te oryginalne, często podszywając się pod znane firmy lub instytucje, co dodatkowo zwiększało ich pozorną wiarygodność.



Grafika 7. Przykładowa wiadomość SMS wykorzystywana w oszustwie na fałszywą inwestycje

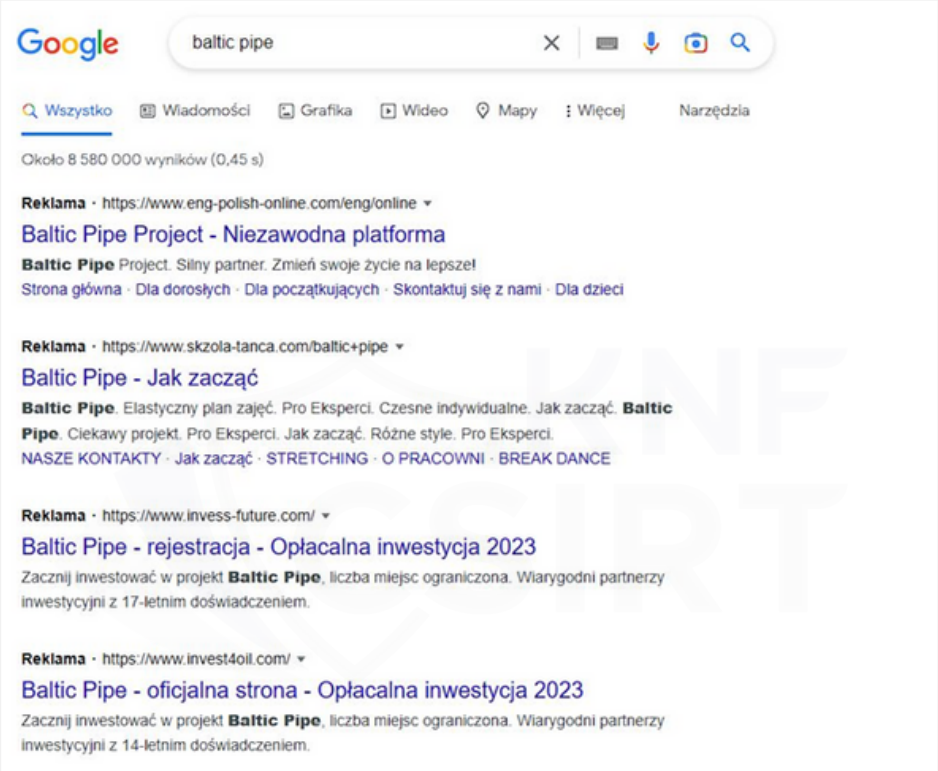


Grafika 8. Przykład fałszywej strony inwestycyjnej z wiadomości SMS



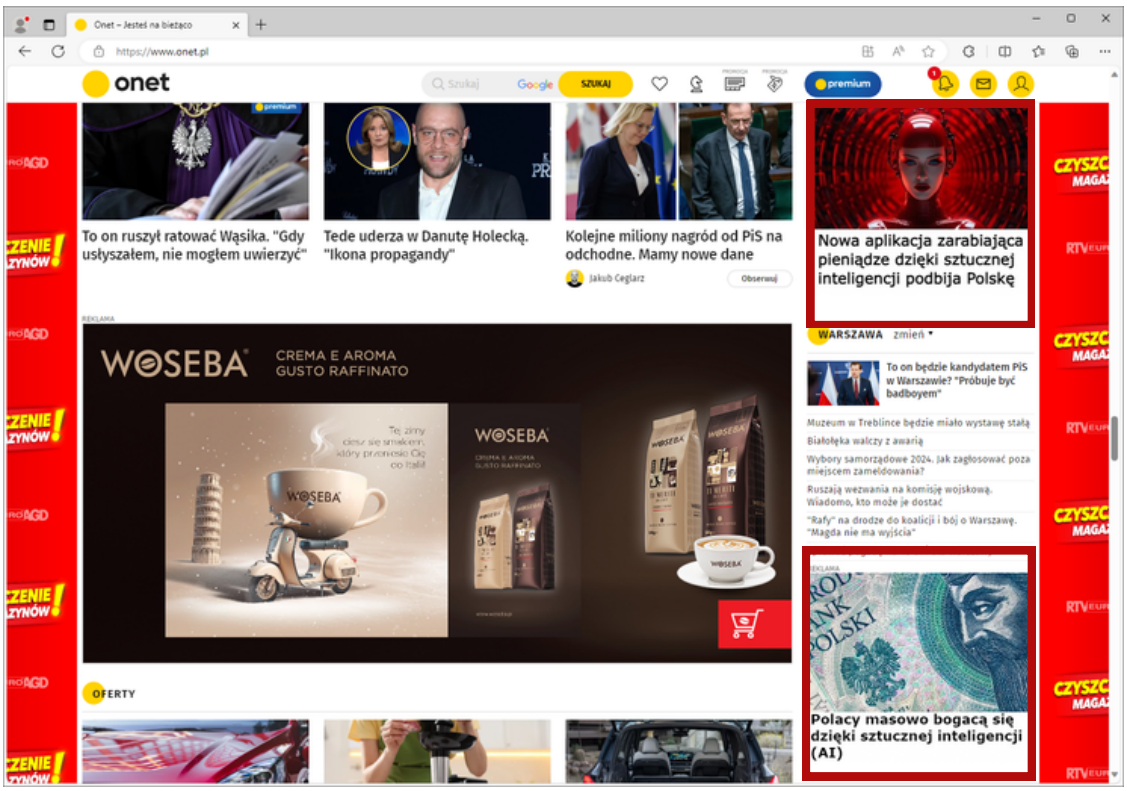
Grafika 9. Artykuł na fałszywej stronie informacyjnej nakłaniający do zainwestowania w fałszywe inwestycje

Kolejnym kanałem dystrybucji reklam fałszywych inwestycji były wyszukiwarki internetowe. Użytkownik poszukający informacji na temat inwestowania lub też pasywnych źródeł dochodu, w wyszukiwarce internetowej mógł natrafić na wyniki prowadzące go do fałszywych serwisów wyłudzających dane, które były reklamami wykupionymi przez oszustów w tych właśnie wyszukiwarkach i tak spozycjonowane, aby wyświetlać się użytkownikom Internetu jako pierwsze wyniki wyszukań.

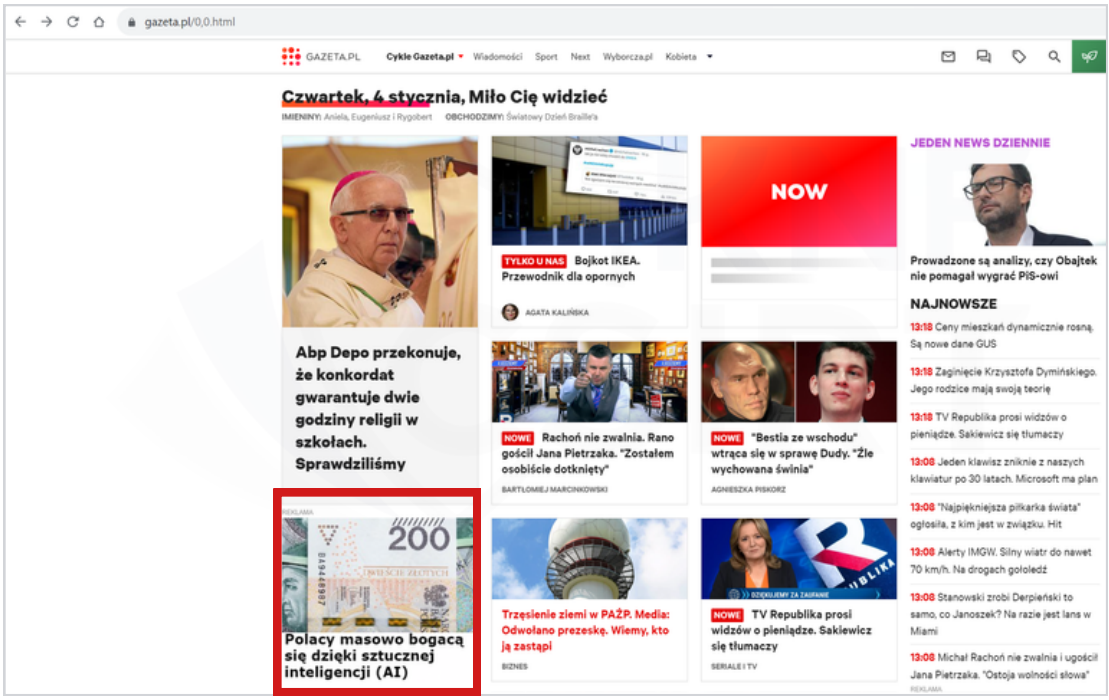


Grafika 10.Wyniki w wyszukiwarce internetowej prowadzące do fałszywych serwisów inwestycyjnych.

Reklamy fałszywych inwestycji pojawiały się również na stronach ogólnopolskich portali informacyjnych. Oszuści w publikowanych reklamach wykorzystywali motyw sztucznej inteligencji i oferowali możliwość szybkiego wzbogacenia się.



Grafika 11. Reklamy fałszywych inwestycji pojawiające się na stronie portalu informacyjnego Onet



Grafika 12. Reklama fałszywej inwestycji pojawiająca się na stronie portalu informacyjnego Gazeta.pl

Proces manipulacji użytkownikiem przez telefon

Po pozyskaniu danych kontaktowych, oszuści inicjowali kontakt do ofiary. Najczęściej odbywało się to poprzez bezpośredni kontakt telefoniczny od rzekomego konsultanta, ale także przez wiadomość e-mail lub w formie odpowiedzi na zapytanie złożone przez ofiarę na fałszywej stronie internetowej. W tej fazie oszustwa przestępcy skupiali się na budowaniu relacji zaufania z ofiarą, odpowiadając na pytania, oferując pomoc i doradztwo, a także używając terminologii finansowej, aby wejść w rolę wiarygodnego eksperta.

Następnym etapem oszustwa było przekierowanie ofiary na fałszywą platformę inwestycyjną, która często zaprojektowana była w zbliżony sposób do prawdziwych stron inwestycyjnych, uwzględniając funkcje pozwalające na rzekome inwestowanie i śledzenie zysków.

W rzeczywistości, pieniądze wpłacone przez ofiarę nigdy nie były inwestowane, lecz trafiały bezpośrednio do oszustów.

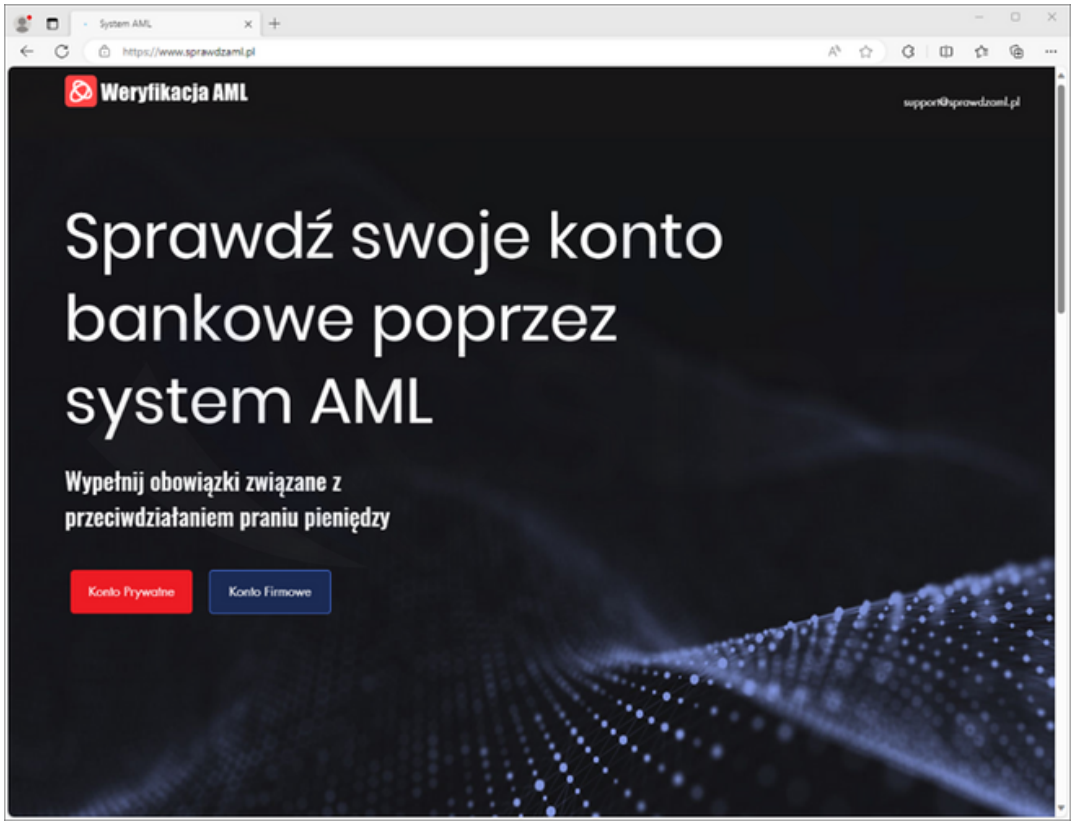
Cyberprzestępcy często stosowali socjotechnikę, aby przekonać ofiary lub wręcz wymusić kolejne wpłaty poprzez np. :

- **Straszenie karami za zbyt wysoki zysk** - oszuści informowali ofiary o rzekomych karach czy opłatach związanych z nadmiernymi zyskami;
- **Wymóg dopłaty podatku przy próbie wypłaty środków** - gdy ofiara próbowała wypłacić środki, oszuści mogli twierdzić, że konieczna jest opłata podatku lub innych fikcyjnych opłat.

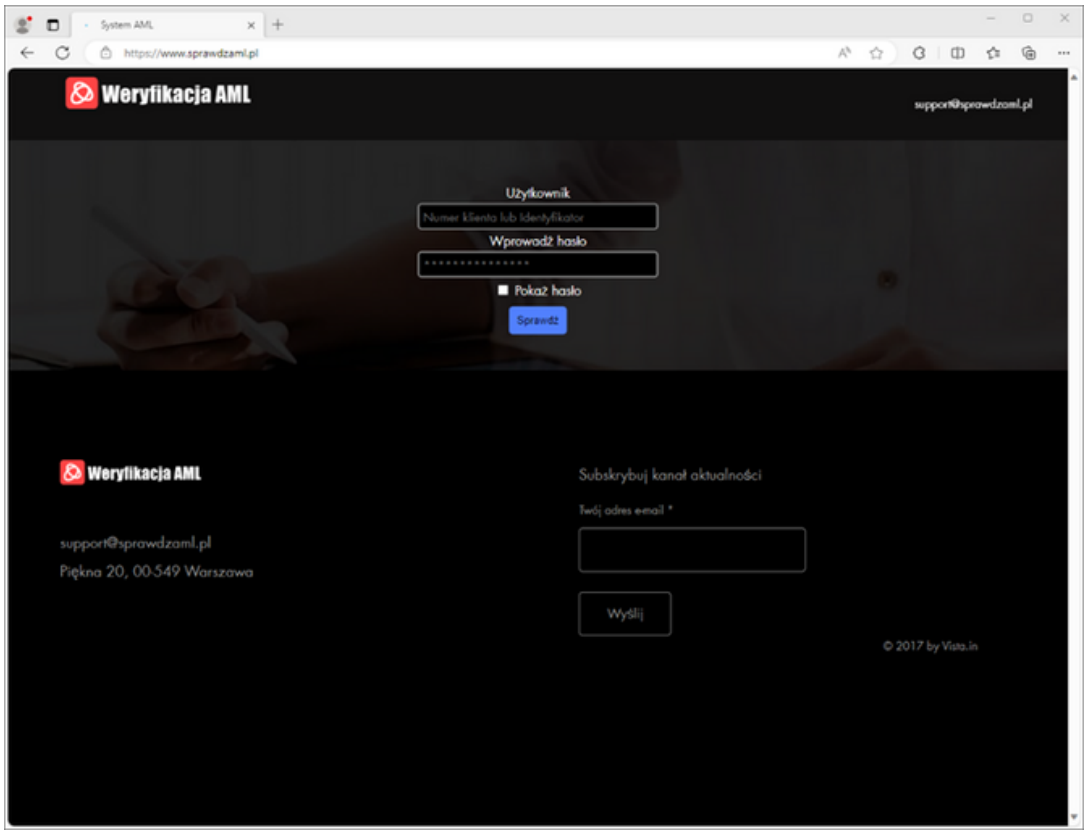
Oprócz opisanego wyżej nakłonienia ofiary do bezpośredniego przelania pieniędzy w ramach fałszywej inwestycji (które trafiały bezpośrednio do oszustów) przestępcy wykorzystywali w tym scenariuszu także inne sposoby kradzieży środków finansowych:

- **Wyłudzanie danych logowania do bankowości elektronicznej** - przez fałszywe strony, które imitują oficjalne procedury AML (przeciwdziałanie praniu pieniędzy), oszuści starali się uzyskać dostęp do danych logowania ofiary;
- **Instalację aplikacji do pomocy zdalnej** - w niektórych przypadkach, oszuści prosili o instalację oprogramowania do zdalnej pomocy, co pozwalało im na przejęcie kontroli nad urządzeniem ofiary i pełny dostęp przestępców do danych wykorzystywanych do logowania do bankowości elektronicznej.

Wszystkie te działania były dostosowane do indywidualnej podatności ofiary na manipulację, co zwiększało skuteczność oszustwa.



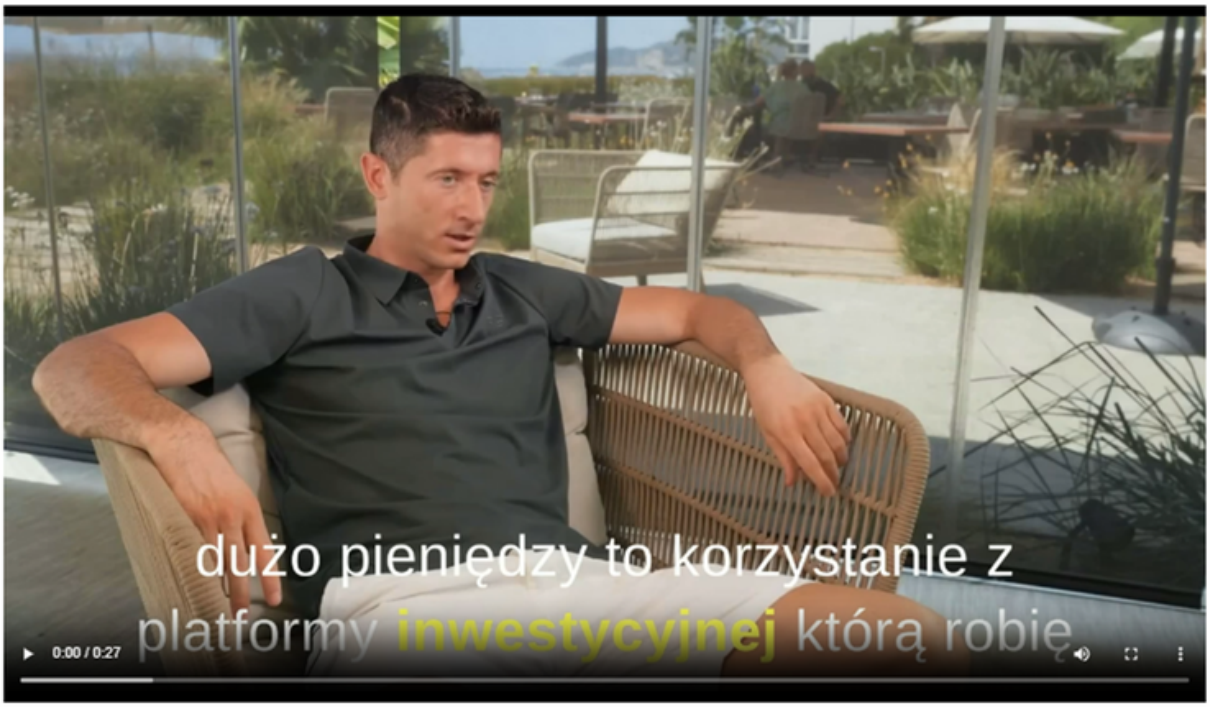
Grafika 11. Przykład fałszywej strony do weryfikacji AML



Grafika 12. Przykład fałszywej strony do weryfikacji AML

Deepfake w oszustwie na fałszywą inwestycję

W 2023 roku obserwowaliśmy nasilenie wykorzystania technologii deepfake w oszustwach na fałszywe inwestycje. Technika ta pozwala na tworzenie „obrazów lub nagrań, które zostały przekonująco zmienione i zmanipulowane w celu fałszywego przedstawienia kogoś jako robiącego lub mówiącego coś, co w rzeczywistości nie zostało zrobione lub powiedziane”[5]. W ten sposób oszuści podszywali się pod osoby znane medialnie i nielegalnie wykorzystując ich wizerunek namawiali do fałszywych inwestycji. Wykorzystanie technologii deepfake do tego typu manipulacji jest wysoko skuteczne. Nagrania wideo tego typu są bardzo realistyczne i przekonujące, wywołując u ofiary tym większe przekonanie o legalności tej inwestycji skoro przekonuje do niej osoba znana z pierwszych storn gazet.



Grafika 13. Przykład wykorzystywania technologii deepfake do manipulacji i wykorzystania głosu znanej osoby

[5]. Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/deepfake, dostęp: 27.03.2023

Zwalczanie reklam fałszywych inwestycji przez CSIRT KNF

W odpowiedzi na rosnącą liczbę oszustw inwestycyjnych, zespół CSIRT KNF podejmuje aktywne działania w celu wyszukiwania i identyfikacji oszukańczych reklam i domen internetowych. 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. Pozwala to na szybką identyfikację i reagowanie na nowe schematy oszustw, co jest kluczowe w prewencyjnym ograniczaniu ich skutków. Oprócz wyszukiwania fałszywych reklam, CSIRT KNF wyszukuje i identyfikuje oszukańcze domeny internetowych, które są wykorzystywane do przeprowadzania oszustw inwestycyjnych. Dzięki ciągłej analizie i śledzeniu nowych domen, jesteśmy w stanie szybko identyfikować potencjalne zagrożenia i ostrzegać o nich.

CSIRT KNF współpracuje z wieloma instytucjami i organizacjami na arenie krajowej i międzynarodowej, wymieniając informacje i koordynując działania przeciwdziałające oszustwom inwestycyjnym. Prowadzi także akcje informacyjne, publikując ostrzeżenia na swoich profilach w mediach społecznościowych takich jak X, Facebook, LinkedIn. Te działania mają na celu edukację użytkowników i zapobieganie potencjalnym stratom finansowym.

W 2023 roku CSIRT KNF zgłosił do zablokowania 26 781 domen internetowych oraz 7963 oszukańcze reklamy w mediach społecznościowych, które dotyczyły fałszywych okazji inwestycyjnych.

Jak unikać oszustw inwestycyjnych

Przed podjęciem jakiejkolwiek decyzji inwestycyjnej, ważne jest, aby dokładnie zweryfikować oferenta i samą ofertę. Należy sprawdzić wiarygodność firmy lub platformy inwestycyjnej, poszukując niezależnych opinii i recenzji. Dobrą praktyką jest także śledzenie listy ostrzeżeń publicznych KNF, która dostępna jest na stronie internetowej Komisji Nadzoru Finansowego[6], a także rejestrów czy wyszukiwarek podmiotów w zakresie weryfikacji zakresu ich działalności .

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

Unikanie inwestycji w produkty, które są reklamowane jako "bez ryzyka" czy "gwarantujące wysokie zyski", jest kluczowe, ponieważ takie obietnice są często znakiem ostrzegawczym. Należy zachować ostrożność przy udostępnianiu swoich danych osobowych i finansowych gdyż oszuści często wykorzystują zebrane informacje do dalszych prób wyłudzeń w innych scenariuszach przestępczych. Nie należy nigdy nikomu udostępniać danych logowania do kont bankowych ani instalować nieznanych aplikacji, na żądanie czy prośbę pochodzącą od niezweryfikowanych źródeł. Zrozumienie podstawowych zasad inwestowania i ryzyka związanego z różnymi rodzajami inwestycji może pomóc również w rozpoznawaniu podejrzanych ofert a podnoszenie poziomu własnej świadomości finansowej jest jednym ze sposobów na uniknięcie oszustwa. Ważne jest, aby nie podejmować decyzji pod wpływem emocji czy presji. Oszuści często stosują taktykę wywoływania w ofierze poczucia potrzeby natychmiastowego działania czy pilności, aby zmusić ją do szybkich i nieprzemyślanych decyzji. Zawsze warto poświęcić czas na analizę i konsultację planowanych działań z zaufanymi osobami lub doradcami finansowymi.

Schemat oszustwa inwestycyjnego opisany został w naszym cyklu najpopularniejszych oszustw internetowych. Opracowanie dostępne jest tutaj[7]

Phishing z wykorzystaniem wiadomości e-mail i SMS

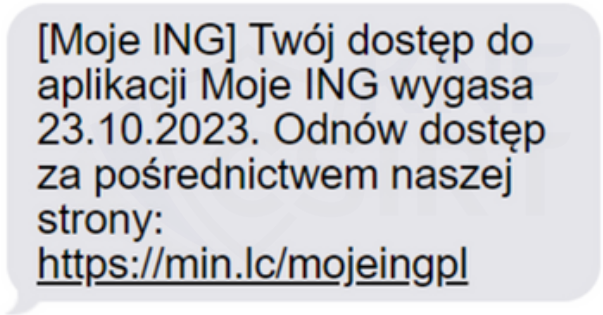
Tak jak w latach poprzednich tak i w 2023 roku jednym z początkowych wektorów ataków prowadzących do kradzieży środków finansowych użytkowników był phishing. Cyberoszuści w sposób masowy rozsyłali fałszywe wiadomości e-mail i SMS, w których podszywali się pod banki, firmy kurierskie, dostawców energii elektrycznej, znane sklepy bądź instytucje administracji publicznej. Znajdujące się w wiadomościach SMS linki prowadziły do fałszywych stron bankowości elektronicznej czy też pośredników płatności, gdzie cyberprzestępcy wyłudzali loginy i hasła użytkowników lub też dane kart płatniczych. Cyberprzestępcy zmieniają w tym oszustwie głównie wizerunki instytucji, pod które się podszywają co wynika np. ze wzrostu popularności danych usług na rynku. W 2023 roku odnotowaliśmy zwiększenie liczby kampanii oszukańczych z wykorzystaniem wizerunków platform streamingowych.

[7] https://cebrf.knf.gov.pl/encyklopedia-cyberbezpieczenstwa/schematy-oszustw/falszywe-inwestycje

Identyfikowane przez CSIRT KNF kampanie phishingowe można podzielić na następujące kategorie:

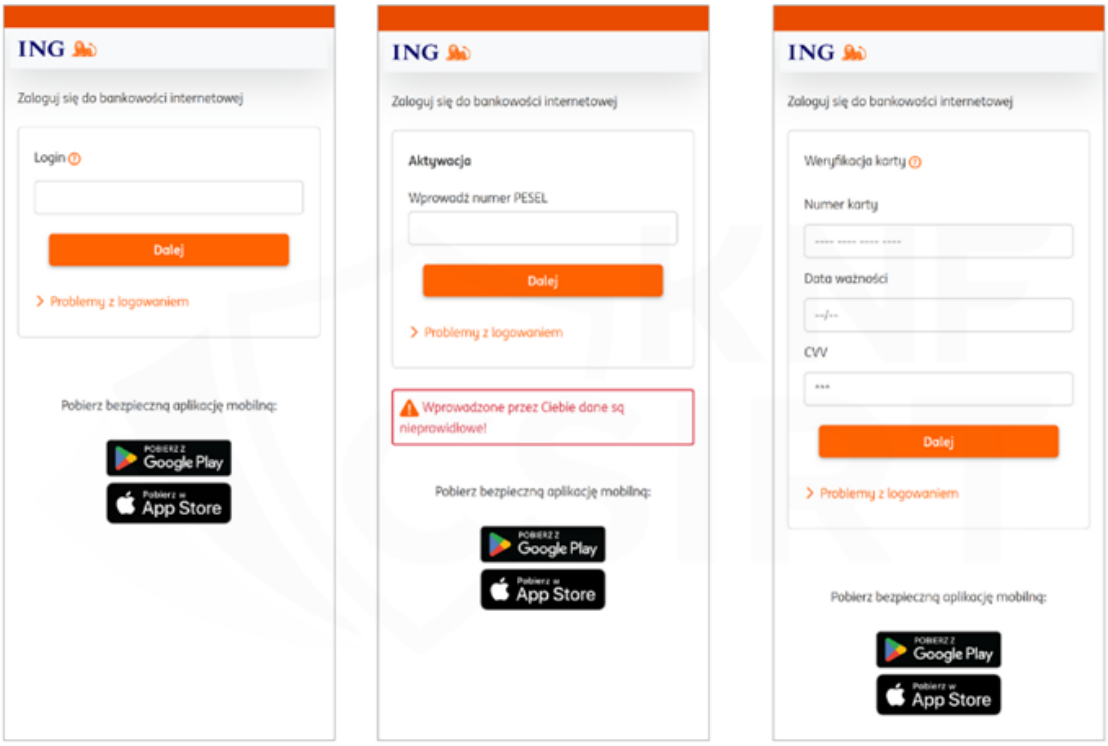
- **podszywanie pod usługi kurierskie i pocztowe** - oszuści tworzyli fałszywe strony internetowe przypominające te należące do znanych firm kurierskich lub pocztowych. Celem tych działań było wyłudzenie danych osobowych lub środków finansowych pod pretekstem monitorowania przesyłki czy opłaty za dodatkowe usługi;
- **podszywanie pod portale ogłoszeniowe** - na fałszywych stronach internetowych oferowane były nieistniejące produkty lub usługi. Po dokonaniu płatności, kontakt z oszustem był niemożliwy, a towar nigdy nie był dostarczony;
- **podszywanie pod bankowość elektroniczną** - cyberprzestępcy tworzyli strony internetowe, które podszywały się pod strony banków i innych podmiotów rynku finansowego. Oszuści wykorzystywali je do kradzieży danych logowania do bankowości elektronicznej i innych serwisów, co umożliwiało im dostęp do kont i środków finansowych;
- **fałszywe bramki płatności** - to strony internetowe, które imitowały bramki płatności online. Używane były przez cyberprzestępców do przechwycenia danych kart kredytowych i innych danych płatniczych;
- **fałszywe sklepy internetowe** - oszuści tworzyli strony imitujące legalne sklepy online. Cyberprzestępcy oferowali produkty po atrakcyjnych cenach, aby zachęcić klientów do zakupu. Po dokonaniu płatności, zamówione produkty nie były dostarczane;
- **portale społecznościowe** - na fałszywych stronach oszuści podszywali się pod platformy społecznościowe i wykorzystywali je do przeprowadzania różnych oszustw, od wyłudzenia danych dostępowych, wykradania danych osobowych aż do wyłudzania środków finansowych.

Przykład kampanii wymierzonej w klientów Banku ING. Oszuści przesyłali wiadomości SMS z informacją o wygaśnięciu dostępu do aplikacji:



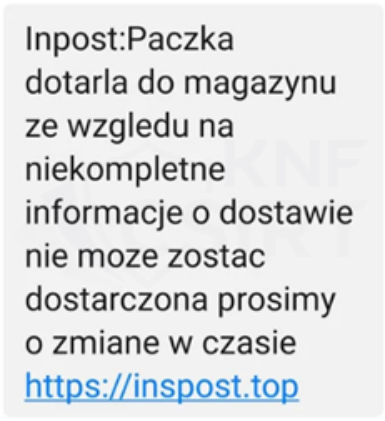
Grafika 14. Fałszywa wiadomość podszywająca się pod Bank ING

Link znajdujący się w wiadomości prowadził do fałszywej strony bankowości elektronicznej. Cyberprzestępcy poza danymi logowania wyłudzali także dane kart płatniczych płatniczych.



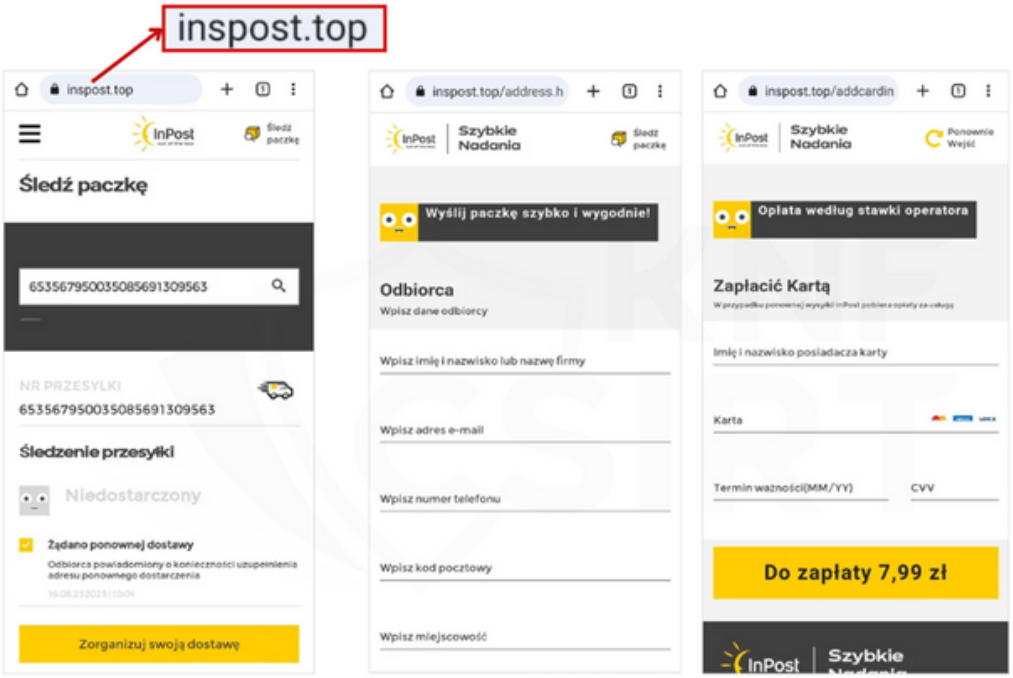
Grafika 15. Przykłady niebezpiecznych stron wykorzystywanych w opisywanej kampanii phishnignowej

Działania cyberprzestępców wymierzone były także w klientów firm kurierskich takich jak m.in. InPost, DPD, DHL, UPS. W treści wiadomości SMS przekazywana była informacja o pojawieniu się problemów z dostarczeniem przesyłki czy potrzebą zaktualizowania adresu dostawy. Tego typu kampanie od lat nasilają się głównie w okresie poprzedzającym święta Bożego Narodzenia, w którym co do zasady realizujemy więcej zakupów w Internecie przygotowując prezenty dla najbliższych.



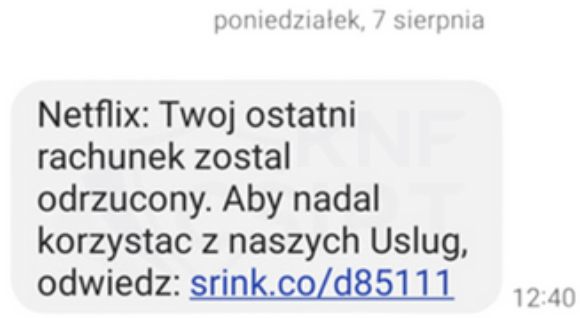
Grafika 16. Fałszywa wiadomość SMS podszywająca się pod firmę kurierską InPost

Link znajdujący się w wiadomości SMS kierował do niebezpiecznej strony wyłudzającej dane osobowe oraz dane kart płatniczych.

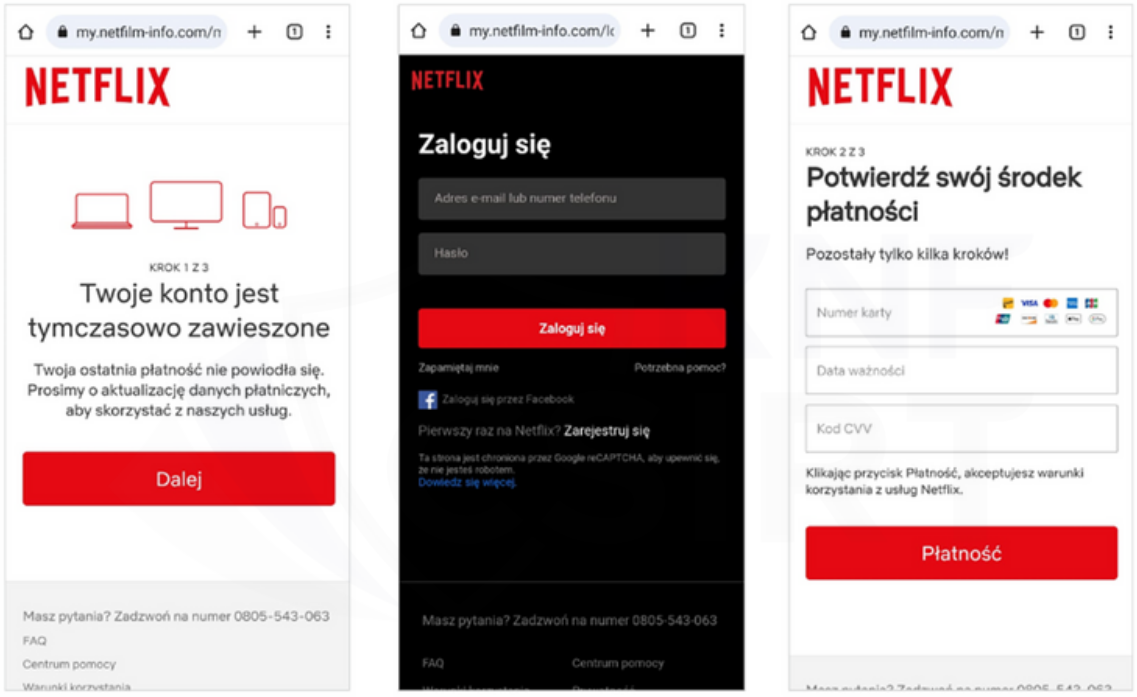


Grafika 17. Przykłady niebezpiecznych stron, na których oszuści wyłudzali dane osobowe użytkowników

W 2023 r. oszuści przesyłali również fałszywe wiadomości SMS podszywające się pod znane platformy streamingowe. W treści wiadomości użytkownicy informowani byli o rzekomych problemach z kontem. Po wejściu w link użytkownik trafiał na fałszywą stronę, na której wyłudzane były dane kart płatniczych.



Grafika 18. Fałszywa wiadomość SMS podszywająca się pod serwis Netflix



Grafika 19. Niebezpieczne strony podszywające się pod serwis Netflix

Więcej o fałszywych wiadomościach SMS przeczytać można w naszym artykule opisującym ten schemat oszustwa, który dostępny jest tutaj [8].

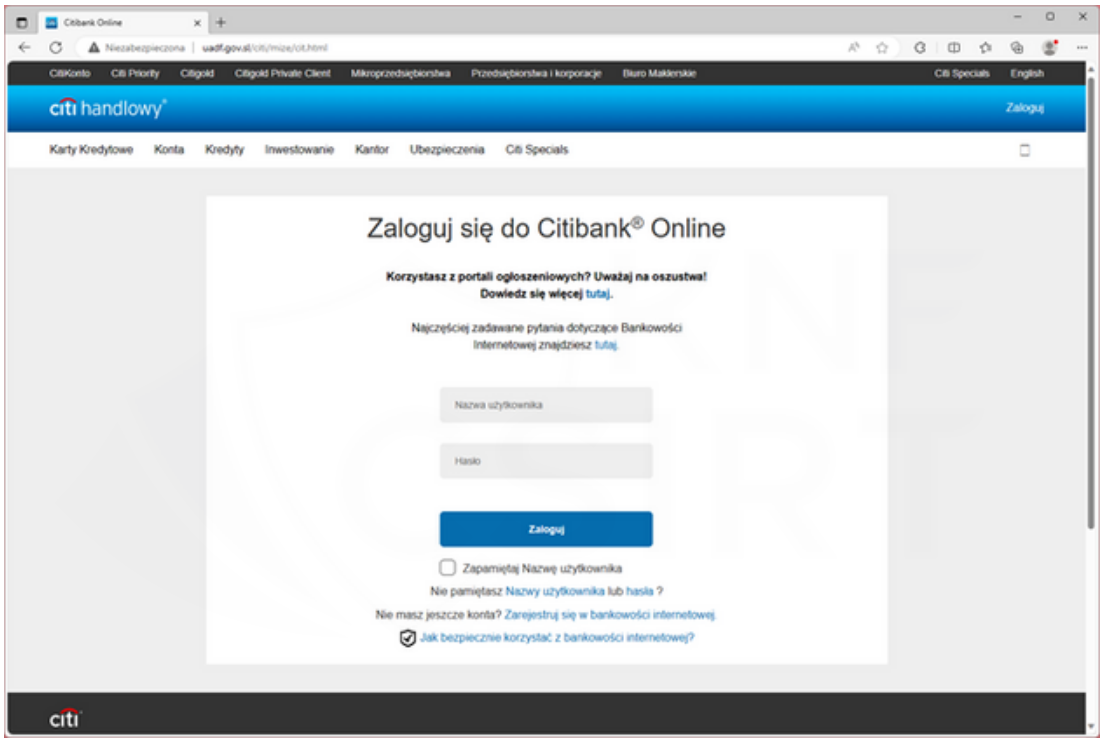
Do dystrybucji swoich kampanii phishingowych przestępcy wykorzystywali także pocztę elektroniczną. Przesyłany w wiadomości mailowej link prowadził do fałszywych stron, gdzie wyłudzane były dane logowania do bankowości elektronicznej bądź dane kart płatniczych użytkowników.

Wśród zidentyfikowanych kampanii phishingowych wymienić należy podszycia pod podmioty z rynku finansowego. Cyberprzestępcy przesyłali wiadomości e-mail np. informujące o rzekomo odrzuconym przelewie przychodzącym ze względu na brak aktualnych danych. W wiadomości znajdował się link, po jego kliknięciu ofiara trafiała na stronę phishingową.

[8] https://cebrf.knf.gov.pl/encyklopedia-cyberbezpieczenstwa/schematy-oszustw/falszywe-wiadomosci-sms

Grafika 20. Treść fałszywej wiadomości e-mail, którą otrzymywała ofiara

Jeżeli ofiara dała się zmanipulować i podała tam dane logowania, to trafiały one bezpośrednio do przestępców.

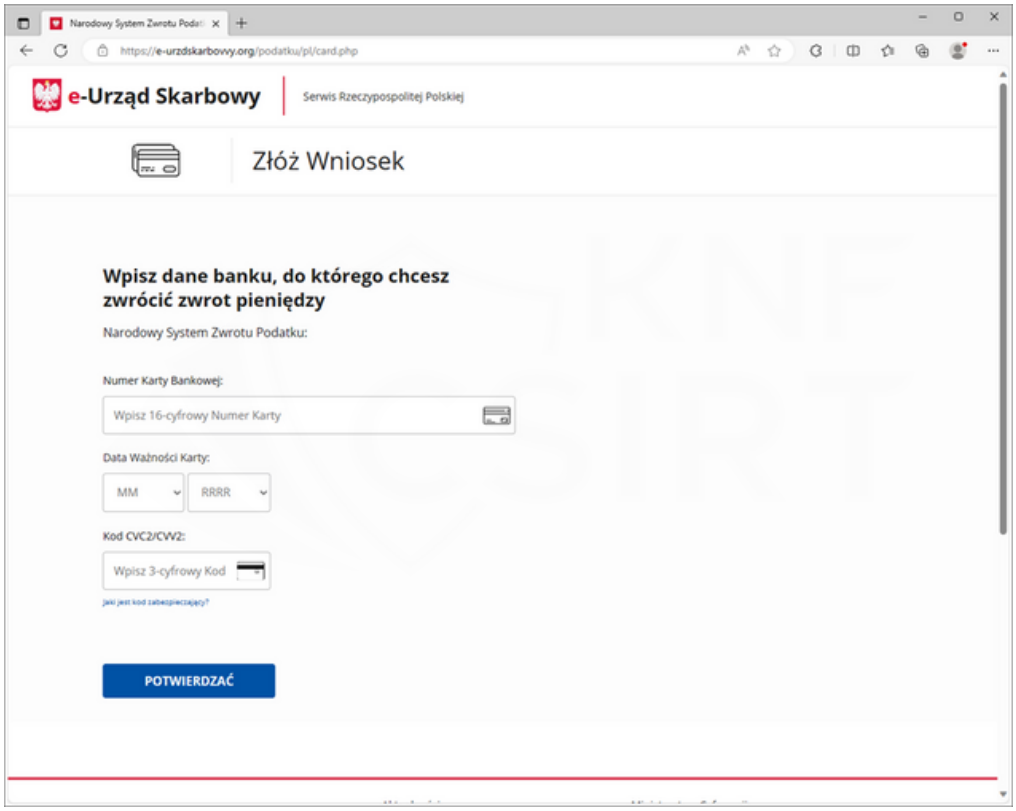


Grafika 21. Przykład fałszywej strony wyłudzającej dane logowania

Jak co roku w okresie rozliczeń podatkowych, cyberprzestępcy przygotowali kampanie oszukańczą powołując się na rzekomą możliwość odebrania zwrotu nadpłaconego podatku. W phishingowej wiadomości mailowej zachęcali do kliknięcia w link który przekierowywał użytkownika na fałszywą stronę podszywającą się pod stronę urzędu skarbowego na której wymagane było wprowadzenie danych karty płatniczej.

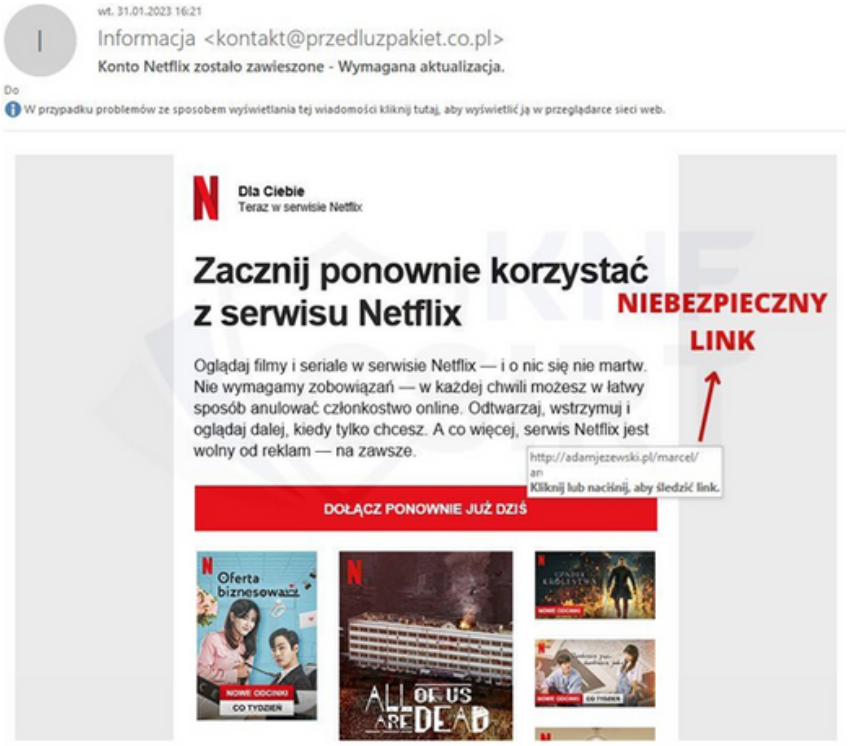
Grafika 22. Treść fałszywej wiadomości e-mail, podszywającej się pod serwis Urzędu Skarbowego

Strona phishingowa, na której oszuści informowali o rzekomej możliwości otrzymania zwrotu podatku:

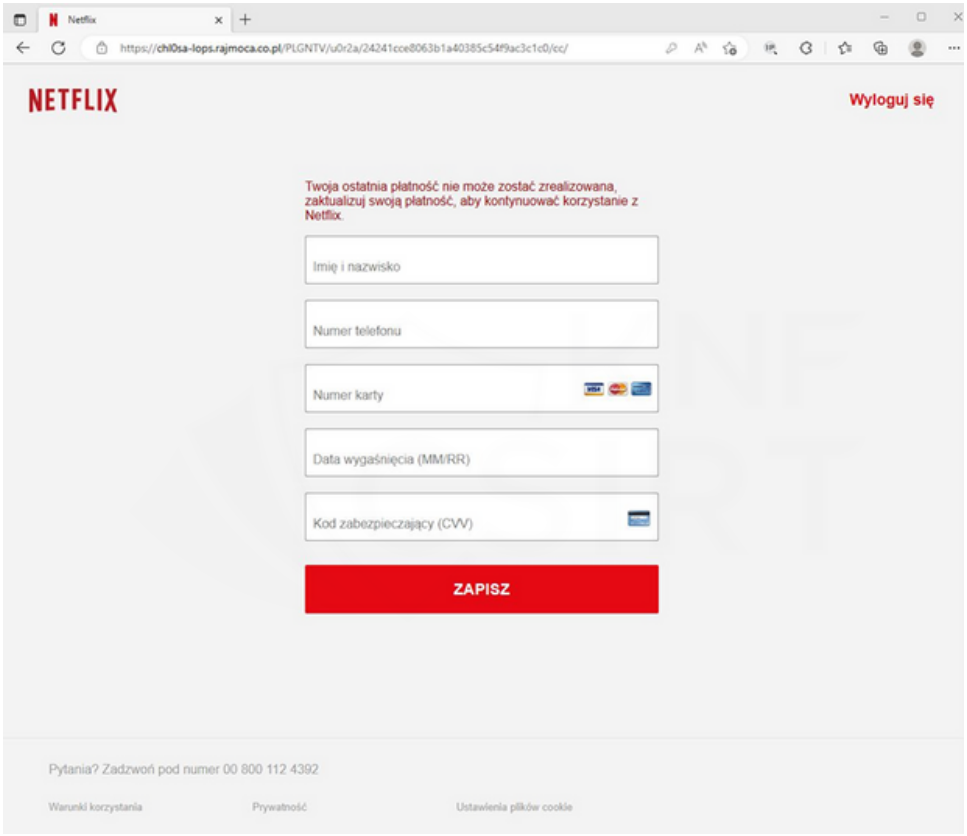


Grafika 23. Fałszywa strona podszywająca się pod GOV

Wspomniane już kampanie oszukańcze dot. serwisów streamingowych dystrybuowane były również poprzez wiadomości email. Podobnie jak w scenariuszu fałszywych wiadomości SMS, w przypadku maili oszuści podszywając się pod serwis Netflix informowali o problemach z kontem. Po wejściu w link, który znajdował się w wiadomości użytkownik trafiał na niebezpieczną stronę wyłudzającą dane karty płatniczej.



Grafika 24. Fałszywa wiadomość e-mail z informacją o zawieszeniu konta



Grafika 25. Fałszywa strona, na której oszuści wymagali wprowadzenia danych osobowych oraz danych karty płatniczej

W 2023 roku CSIRT KNF zidentyfikował 955 domen internetowych podszywających się pod popularne firmy kurierskie. Tego typu domeny dystrybuowane są najczęściej za pośrednictwem wiadomości SMS lub e-mail. Największe natężenie kampanii związanych z przesyłkami odnotowaliśmy w okresach świątecznych.

Ze schematem oszustwa "Fałszywe wiadomości e-mail" zapoznać się można tutaj[9].

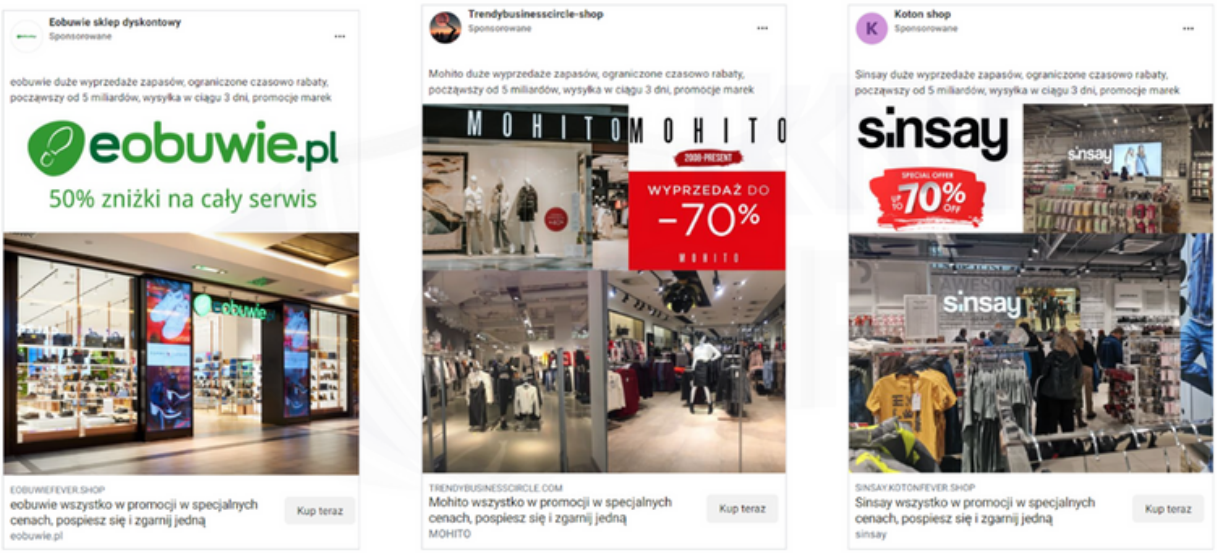
Oszustwa z wykorzystaniem nośników reklamowych - czyli reklama dźwignią oszustwa

Problem wykorzystywania przez cyberprzestępców internetowych nośników reklamowych do dystrybucji stron phishingowych opisany został w części raportu poświęconej fałszywym inwestycjom, ale reklamy były wykorzystywane również do propagowania fałszywych stron bankowości, fałszywych sklepów wyłudzających od użytkowników przelewy lub też numery kart płatniczych oraz innych obszarów, które pozwalały na monetyzację działań przestępczych. Tutaj również, tak jak przy fałszywych inwestycjach przestępcy wykorzystują bezprawnie wizerunki znanych marek w celu zwiększenia wiarygodności swoich oszustw. Prezentujemy wykorzystywane przez cyberprzestępców nośniki reklamowe w 2023 roku w obszarze finansowym oraz e-commerce.

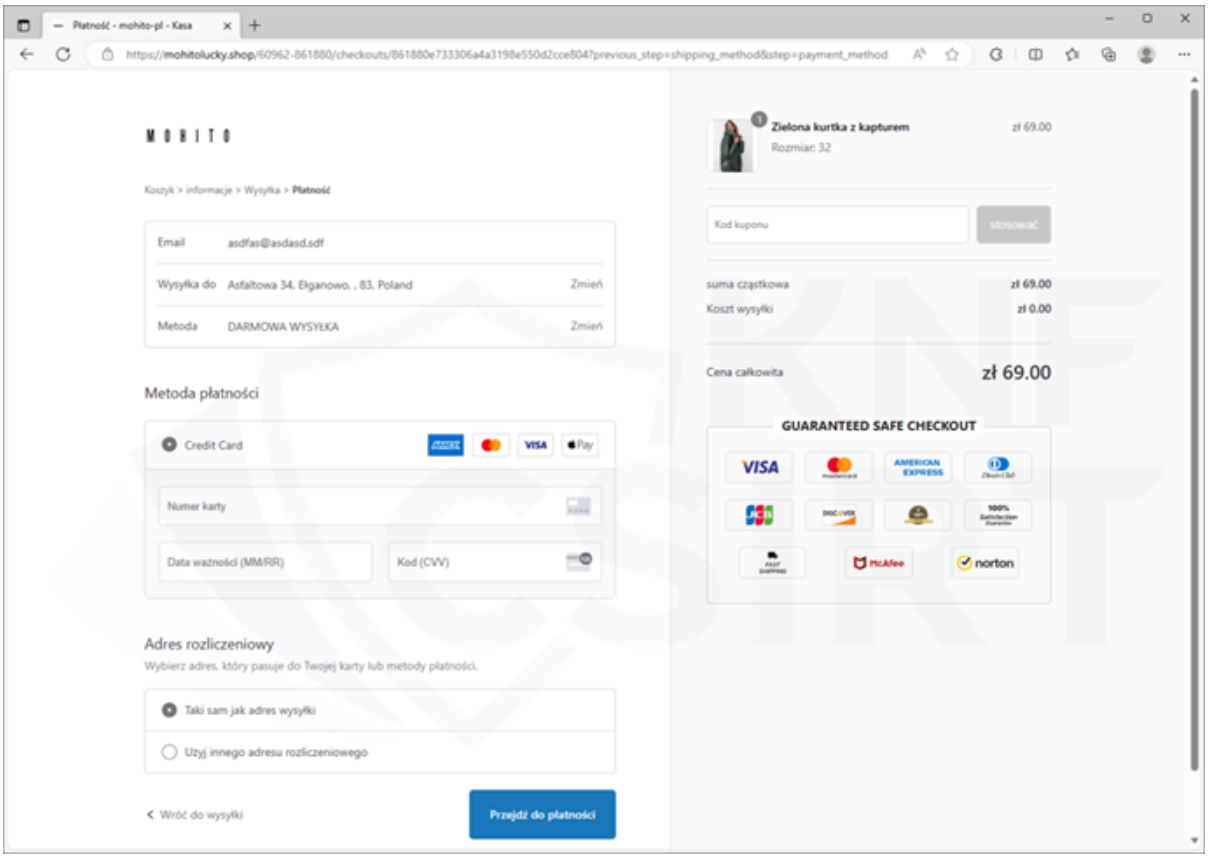
Fałszywe sklepy z promocjami

W reklamach publikowanych w mediach społecznościowych cyberprzestępcy podszywali się pod internetowe sklepy znanych marek oferując fałszywe kupony rabatowe i zniżki na zakupy. Po kliknięciu w reklamę ofiara przekierowywana była na stronę internetową, na której wypełniała formularz z danymi osobowymi, a następnie zachęcana była do podania danych karty płatniczej, które docelowo trafiały do oszustów. Nasilenie tego typu kampanii zespół CSIRT KNF zaobserwował w okresie wyprzedaży i promocji związanych z „Black Friday".

[9] https://cebrf.knf.gov.pl/encyklopedia-cyberbezpieczenstwa/schematy-oszustw/falszywe-wiadomosci-e-mail



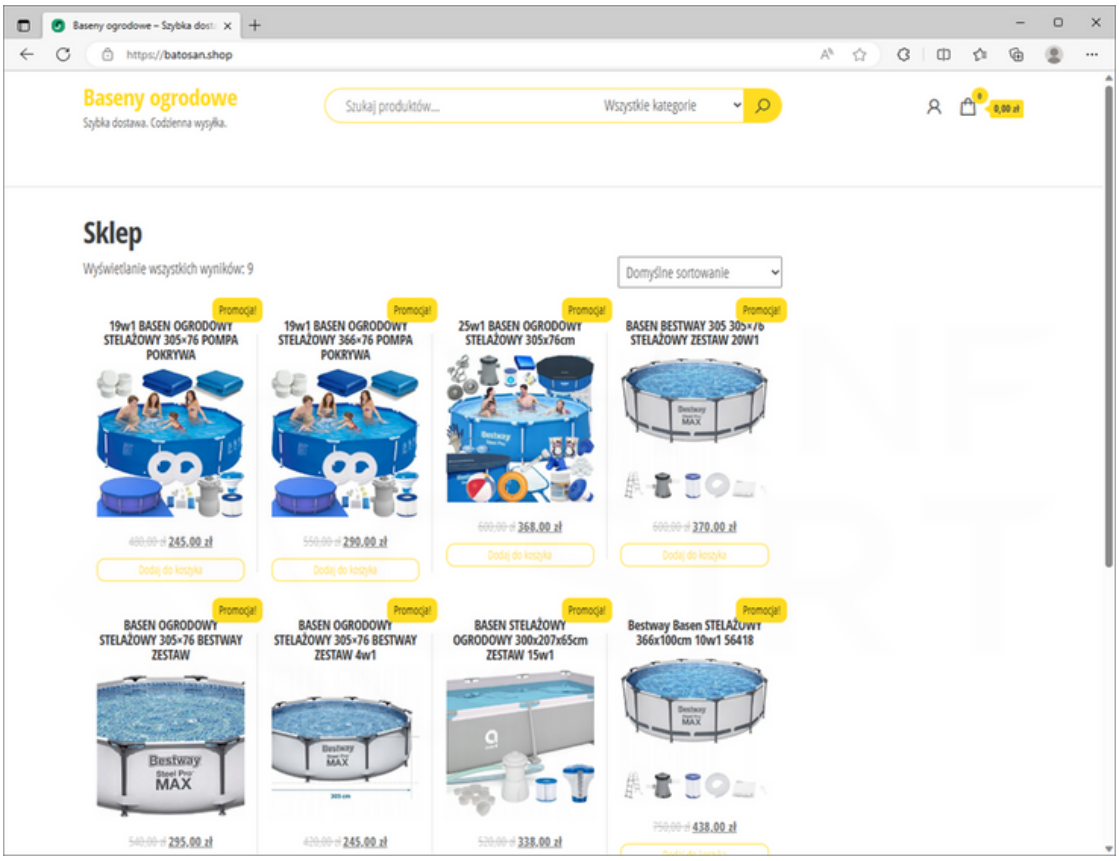
Grafika 26. Reklamy zamieszczane przez cyberprzestępców w mediach społecznościowych, podszywające się pod znane marki sklepów



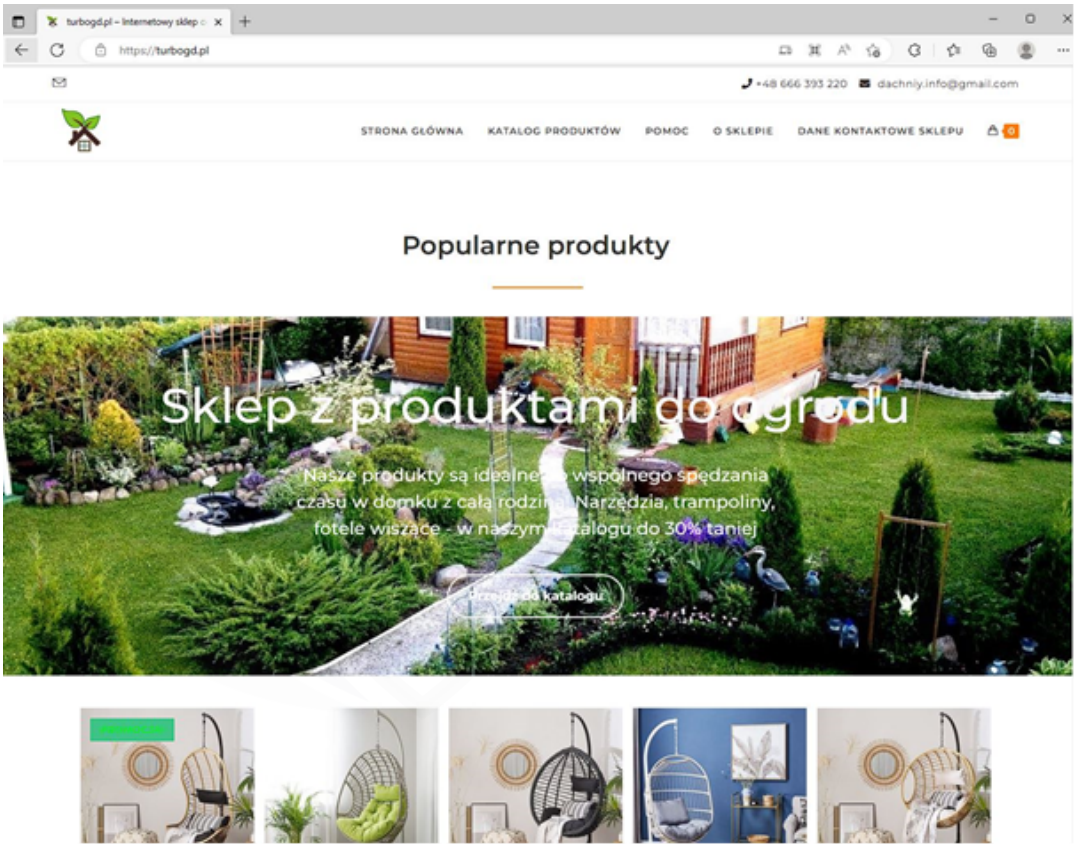
Grafika 27. Niebezpieczna strona wyłudzająca dane użytkowników

Fałszywe sklepy, a pory roku?

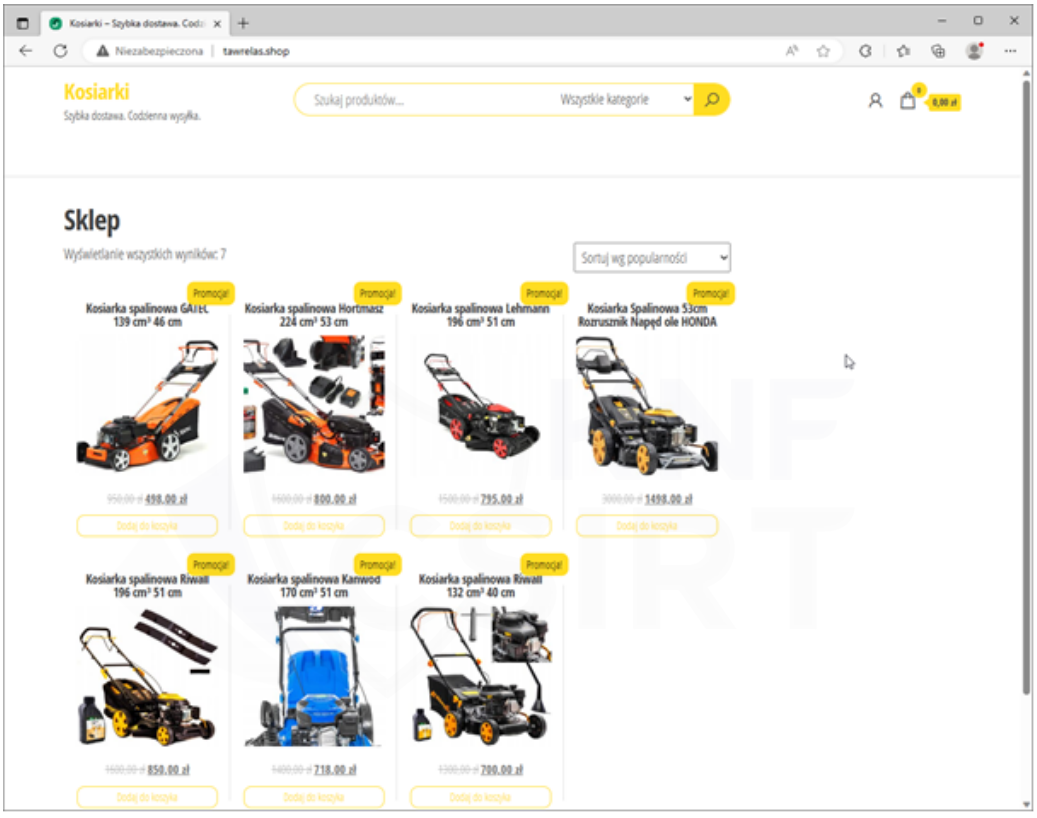
Poza reklamami w mediach społecznościowych cyberprzestępcy tworzyli także fałszywe strony internetowe sklepów, gdzie oferowali produkty po bardzo atrakcyjnych cenach. Zaobserwowaliśmy sezonowość tego typu sklepów. W okresie letnim były to fałszywe sklepy z trampolinami, rowerami i basenami ogrodowym, a w sezonie wiosennym najczęściej występowały sklepy z fałszywymi ofertami sprzętów ogrodniczych takich jak kosiarki czy tunele foliowe. W okresach jesiennym i zimowym cyberprzestępcy przygotowywali fałszywe sklepy oferujące węgiel w bardzo okazyjnych cenach. W praktyce po dokonaniu wpłaty na fałszywej stronie sklepu użytkownicy nigdy nie otrzymywali zamówionego towaru, a sklep po pewnym czasie przestawał istnieć.



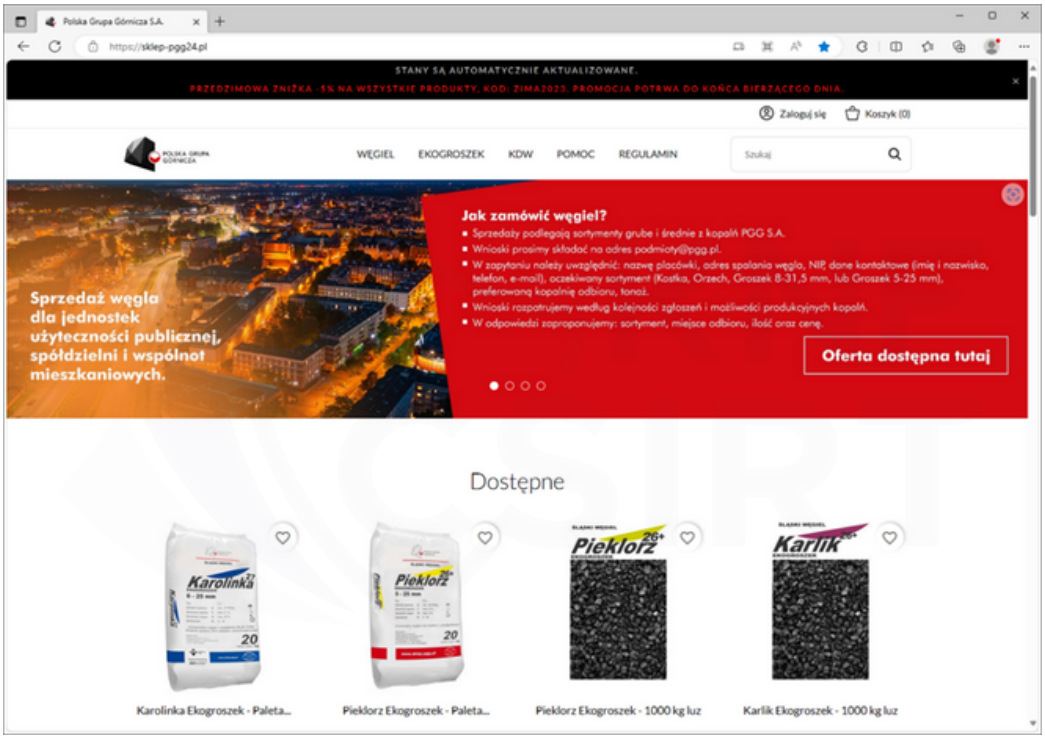
Grafika 28. Fałszywa strona sklepu z basenami – przygotowana przez cyberprzestępców w okresie letnim



Grafika 29. Fałszywa strona sklepu ze sprzętem ogrodniczym – przygotowana przez cyberprzestępców w sezonie wiosennym



Grafika 30. Fałszywa strona sklepu z sprzętem ogrodniczym – przygotowana przez cyberprzestępców w sezonie wiosennym



Grafika 31. Niebezpieczna strona podszywająca się pod Polską Grupę Górniczą – przygotowana przez cyberprzestępców w sezonach jesiennym i zimowym

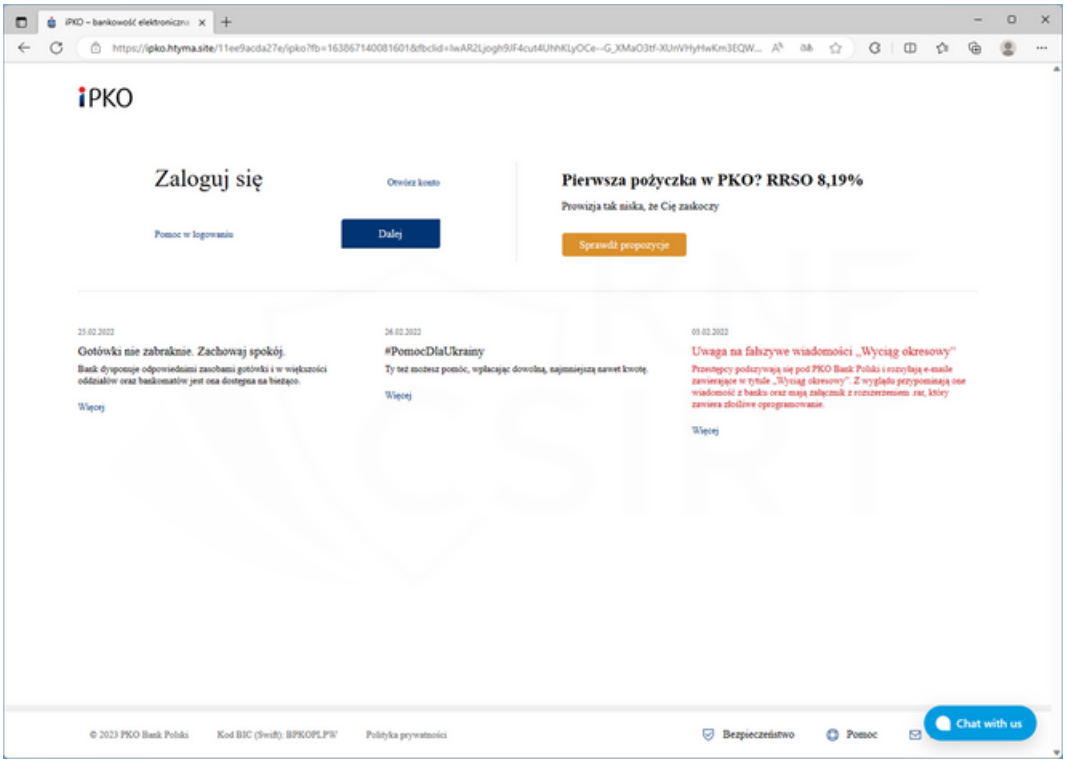
Przypominamy, że przed podaniem jakichkolwiek danych i podjęciem decyzji o zakupie należy zweryfikować sklep z wyjątkowo niską cenowo ofertą. Więcej o fałszywych sklepach przeczytać można w naszym artykule opisującym ten schemat oszustwa, który dostępny jest tutaj [10].

Super okazja czy fałszywa strona bankowości?

Cyberprzestępcy zamieszczając reklamy w mediach społecznościowych podszywali się również pod podmioty rynku finansowego. W treści publikowanych reklam zachęcali użytkowników atrakcyjnymi ofertami handlowymi np. możliwością otrzymania dodatkowych środków finansowych czy pożyczki z niską stopą procentową. Treść zamieszczanych reklam miała zachęcić ofiarę do wprowadzenia swoich danych na niebezpiecznej stronie.

[10] https://cebrf.knf.gov.pl/encyklopedia-cyberbezpieczenstwa/schematy-oszustw/falszywe-sklepy

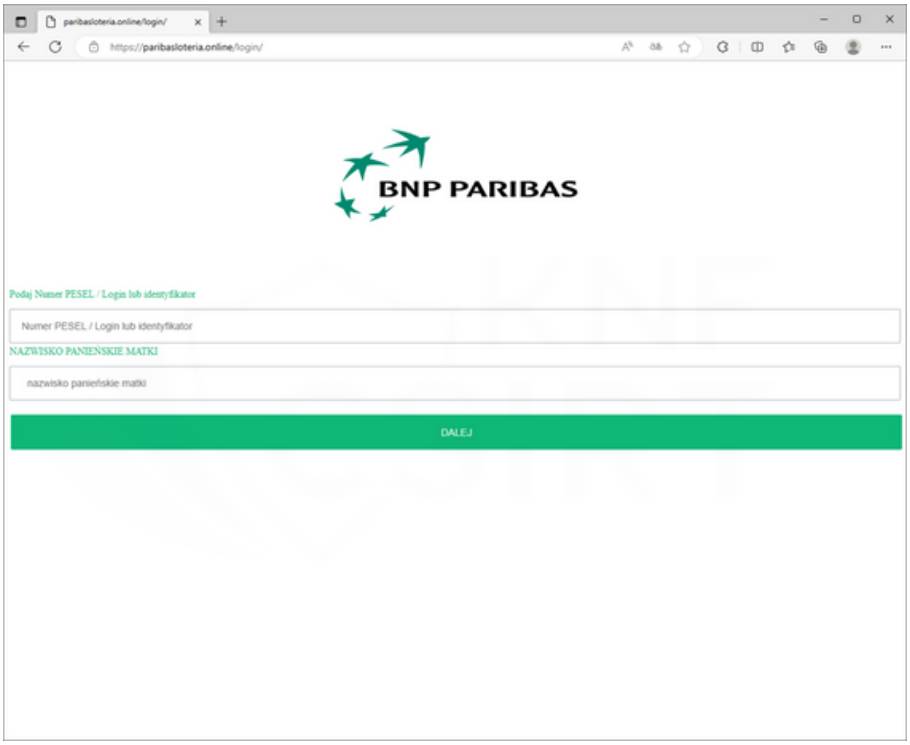
Grafika 32. Reklama zamieszczona przez cyberprzestępców, zachęcająca pożyczką z niską stopą procentową



Grafika 33. Niebezpieczna strona wyłudzająca dane logowania użytkowników

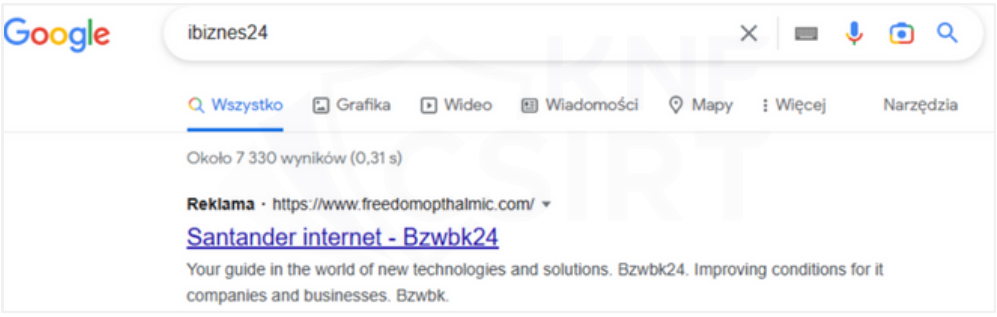
Oprócz atrakcyjnych warunków kredytowania przestępcy zachęcali ofiary do podawania danych obiecując różnego typu nagrody. Np. podszywając się pod Bank BNP Paribas oszuści aby uśpić czujność użytkowników, w reklamie wyświetlali prawdziwą domenę banku, jednak w rzeczywistości reklama kierowała ofiarę do fałszywej strony bankowości elektronicznej. Cyberprzestępcy poza poświadczeniami logowania wyłudzali na niej także dane osobowe m. in. numer PESEL czy nazwisko panieńskie matki.

Grafika 34. Reklama w mediach społecznościowych, w której cyberprzestępcy podszywali się pod Bank BNP Paribas

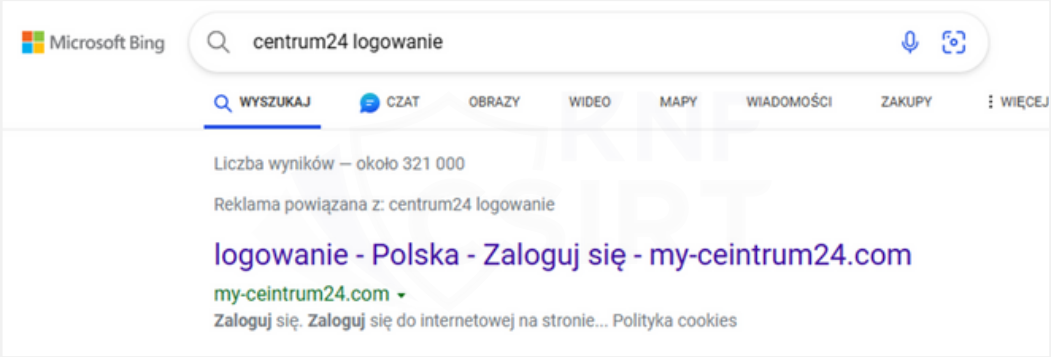


Grafika 35. Niebezpieczna strona wyłudzająca dane logowania użytkowników

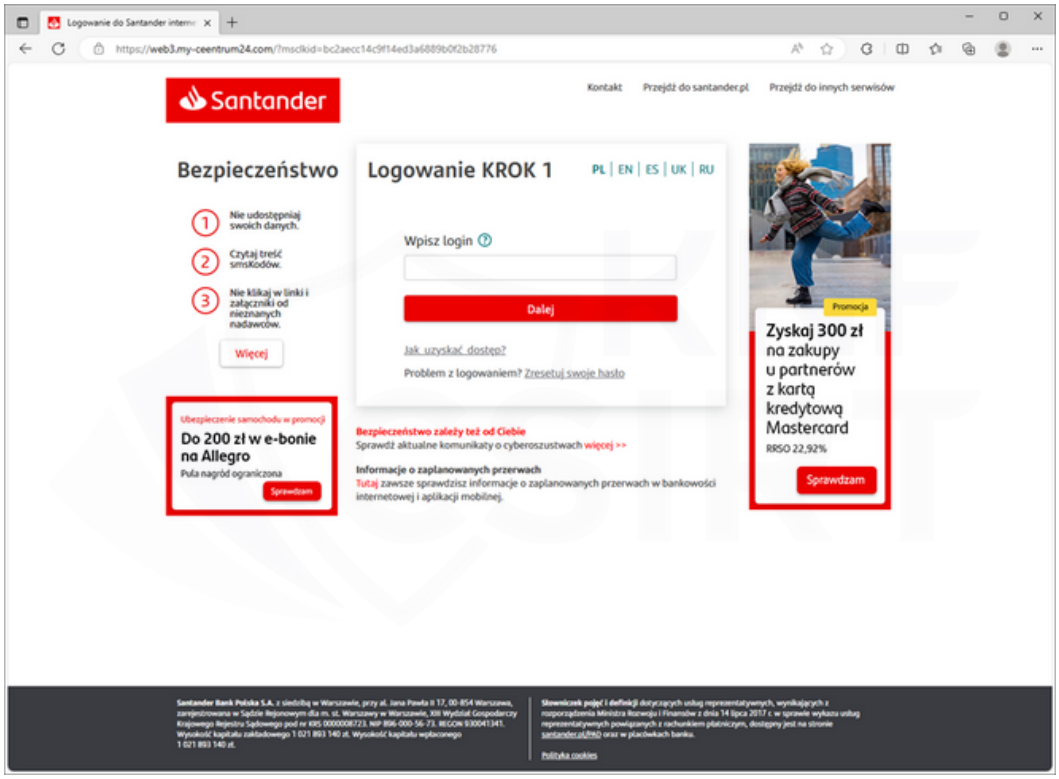
Oprócz wykorzystania reklam w mediach społecznościowych do dystrybucji fałszywych stron bankowości elektronicznej przestępcy wykorzystywali w 2023 roku wyszukiwarki internetowe. Wynika to z prostej zasady, że użytkownicy chcąc zalogować się do swojego banku nie pamiętając pełnego adresu strony logowania wpisują nazwę banku w wyszukiwarce. Cyberprzestępcy wykupując reklamę w wyszukiwarce internetowej wykorzystywali mechanizm pozycjonowania, dzięki czemu ich reklama wyświetlała się na pierwszym miejscu w wynikach wyszukiwania. Użytkownik wchodząc w taką reklamę, był przekonany, że wchodzi na stronę swojego banku, a faktycznie przekierowany był do niebezpiecznej strony przypominającej oryginalną stronę. Wprowadzone tam dane trafiały bezpośrednio w ręce cyberprzestępców.



Grafika 36. Reklama w wyszukiwarce Google, w której cyberprzestępcy podszywali się pod Santander Bank Polska



Grafika 37. Reklama podszywająca się pod Santander Bank Polska



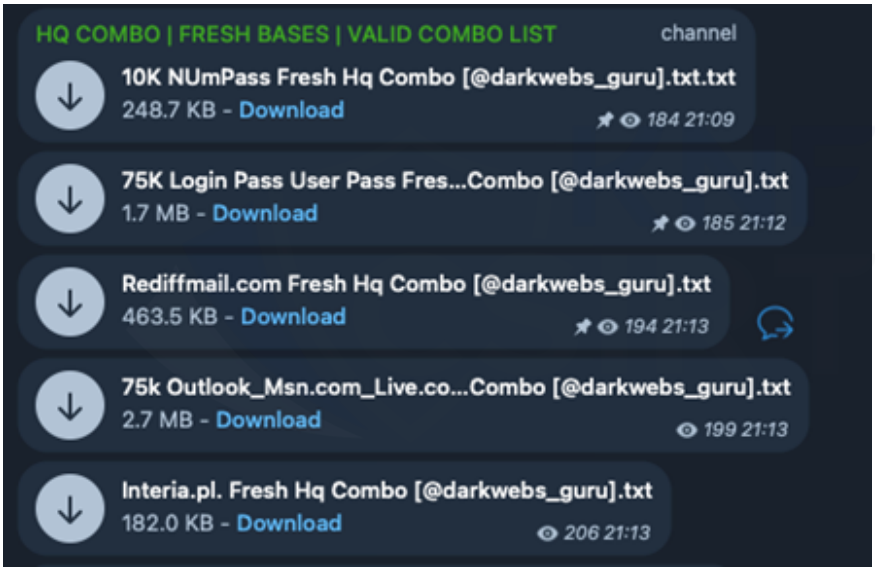
Grafika 38. Fałszywa strona bankowości elektronicznej, którą wykorzystywali cyberprzestępcy

Więcej o wykorzystaniu reklam w wyszukiwarkach internetowych do dystrybucji fałszywych stron bankowości elektronicznej przeczytać można w naszym schemacie, który dostępny jest tutaj [11] .

[11] https://cebrf.knf.gov.pl/encyklopedia-cyberbezpieczenstwa/schematy-oszustw/falszywe-reklamy-w-wyszukiwarce-google

Złośliwe oprogramowanie typu Stealer - czyli skąd przestępcy mają hasła użytkowników?

Oprócz typowych działań phishingowych w których zmanipulowana ofiara wprowadzała dane dostępowe na fałszywej stronie internetowej podstawionej przez przestępców istnieją inne metody kradzieży tego typu danych. Dzieje się to bardzo często za sprawą złośliwego oprogramowania określanego jako tzw. „Stealery". Są to niebezpieczne programy zaprojektowane do kradzieży poufnych danych z zainfekowanego komputera.



Grafika 39. Darmowe logi ze Stealerów, udostępnione przez przestępców

Czym są Stelaery?

Stealery to zaawansowane formy złośliwego oprogramowania, które mają na celu kradzież cennych danych z zainfekowanych urządzeń. Zakres danych wykradanych przez stealery to głównie dane osobowe i finansowe użytkowników, loginy i hasła, dane kart kredytowych, informacje o kontach bankowych oraz inne sensytywne informacje. Stealery działają zazwyczaj w ukryciu, bez wiedzy użytkownika, i mogą być zdalnie sterowane przez cyberprzestępców.
Stealery mogą przybrać różne formy, od prostych keyloggerów [12], które rejestrują naciśnięcia klawiszy, po bardziej zaawansowane oprogramowanie, które może przechwytywać zrzuty ekranu, dane z formularzy internetowych, a także dane przechowywane w przeglądarkach.

Grafika 40. Logi udostępnione przez przestępców zawierające dane użytkowników serwisu interia.pl

Jak dochodzi do infekcji Stealerem?

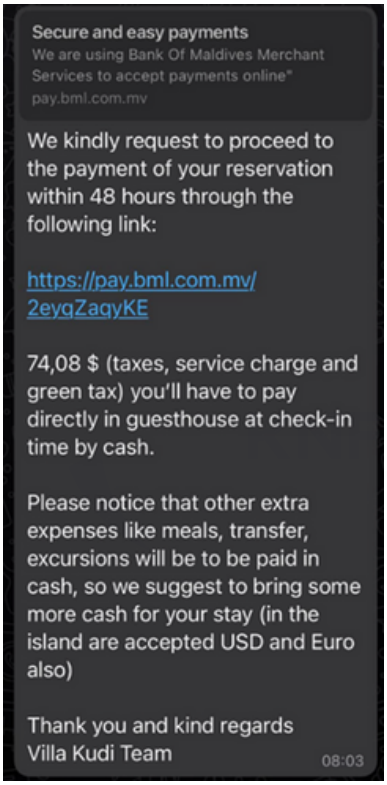
Rozpowszechnianie Stealera często odbywa się poprzez wyrafinowane techniki inżynierii społecznej. Phishing jest jedną z najpopularniejszych metod, gdzie przestępcy wysyłają do ofiar fałszywe e-maile lub wiadomości, które wydają się być wiarygodne i zachęcają ofiary do kliknięcia w zainfekowany link lub otwarcie załącznika. Cyberprzestępcy, w celu dystrybucji złośliwego oprogramowania, wykorzystują także fałszywe profile i wiadomości w mediach społecznościowych.

[12] Oprogramowanie szpiegujące, rejestrujące naciśnięcia klawiszy na klawiaturze.

Co mają wspólnego Stealery i hotele?

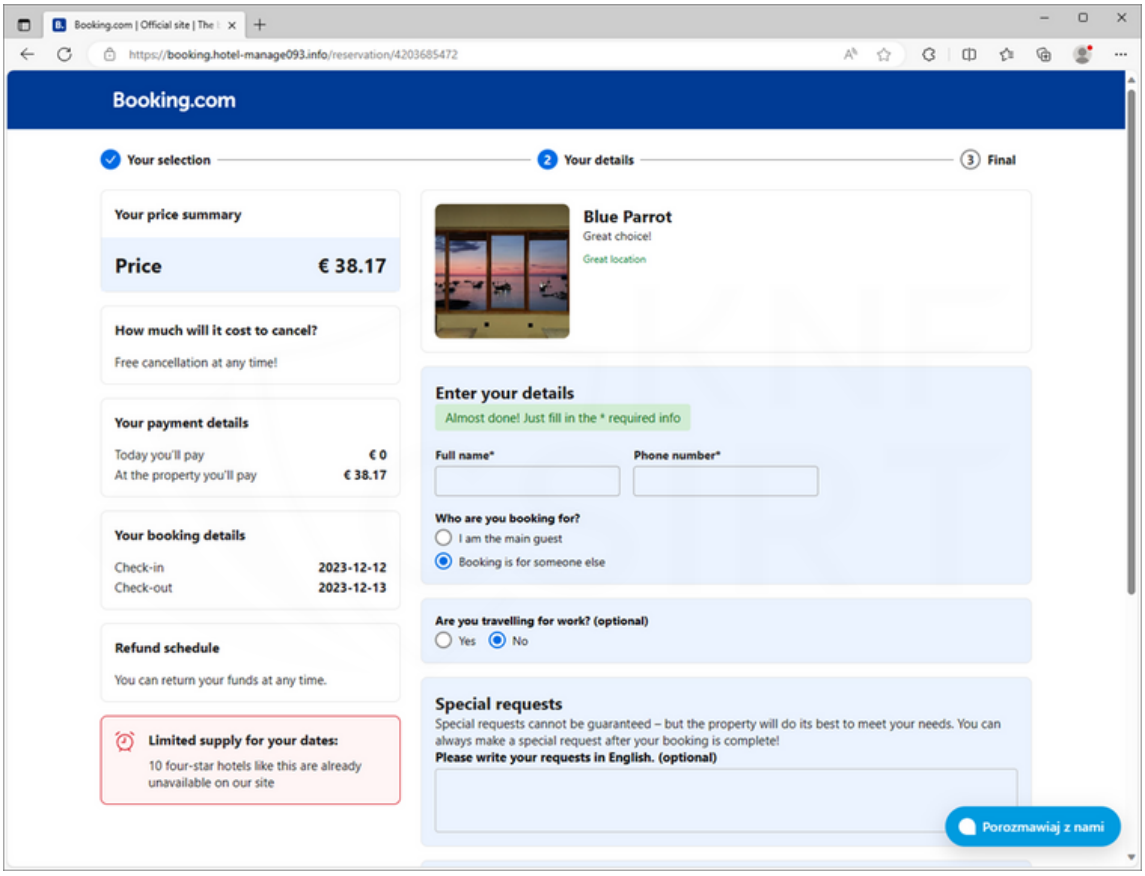
W 2023 odnotowaliśmy przypadki, w których Stealer został rozpowszechniony poprzez fałszywe wiadomości e-mailowe kierowane do właścicieli hoteli lub też osoby korzystające z usług hotelowych, które wysyłane były rzekomo z popularnych platform rezerwacyjnych z którymi te hotele współpracują jak np. booking.com.
Cyberprzestępcy wykorzystując phishing, wysyłali do odbiorcy email załącznik zawierający złośliwe oprogramowanie (Stealer), aby pozyskać dane logowania do portalu Booking, a następnie z przejętych kont klientów serwisu Booking właściciele hoteli otrzymywali fałszywe zapytania rezerwacyjne w formie wiadomości e-mail ze złośliwym załącznikiem zawierającym stealer. Po zainfekowaniu urządzenia po stronie hotelu, przestępcy wykradali dane logowania do portalu Booking, a następnie uzyskiwali dostęp do szerokiego zakresu informacji. W następnych etapach oszustwa tworzyli fałszywe oferty i strony phishignowe i dystrybuowali je do potencjalnych klientów.

Treść przesyłanej przez cyberprzestępców wiadomości przez aplikację Booking.com. Oszuści, podszywając się pod właściciela hotelu przesyłali ofierze link do strony phishingowej, mającej na celu kradzież danych karty płatniczej.



Grafika 41. Przykładowa treść wiadomości wysyłanej przez oszustów poprzez system Booking.com. zawierająca link do strony phishingowej

Po wejściu w link, który znajdował się w wiadomości, ofiara przekierowywana była na fałszywą stronę przypominającą oryginalną stronę hotelu, na której oszuści wymagali podania danych karty płatniczej w celu rzekomego potwierdzenia rezerwacji bądź dokonania płatności za pobyt w hotelu.



Grafika 42. Fałszywa strona podszywająca się pod Booking.com

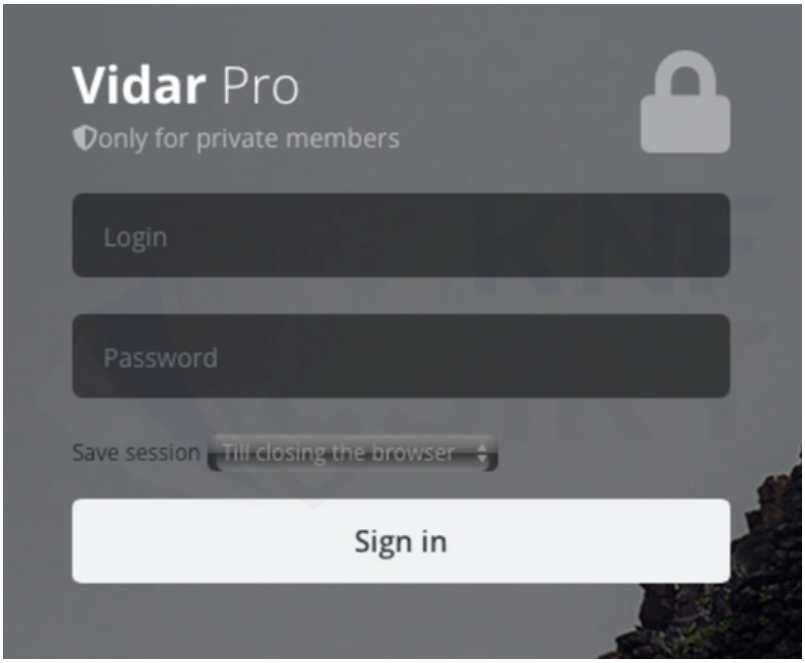
Ze szczegółowym raportem opisującym tę metodę wykorzystywaną przez cyberprzestępców można zapoznać się tutaj[13] .

Rodzaje Stealerów

Vidar Stealer to rodzaj złośliwego oprogramowania typu info-stealer, które skupia się na kradzieży rozległego wachlarza prywatnych danych z zainfekowanych komputerów. Jest to szczególnie niebezpieczne narzędzie, zdolne do wykradania danych logowania, historii przeglądania, danych kart kredytowych, danych z portfeli kryptowalutowych oraz innych wartościowych danych osobowych i finansowych. Charakteryzuje się dużą wszechstronnością, pozwalającą atakującym na dostosowywanie go do konkretnych celów i zbieranie specyficznych typów danych.

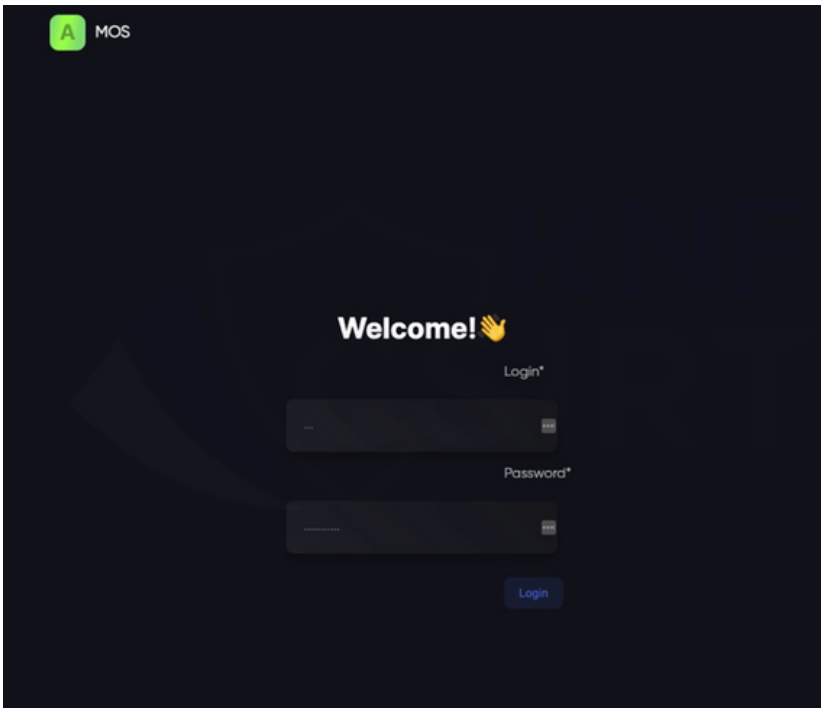
[13] https://cebrf.knf.gov.pl/images/Raporty/Booking_-_rezerwacja_malware_1.pdf

Po zainfekowaniu systemu, Vidar Stealer działa automatycznie, skanując komputer w poszukiwaniu informacji, które są następnie przesyłane do serwera kontrolowanego przez atakującego. Jego zdolność do szybkiego przetwarzania i eksfiltracji danych czyni go wyjątkowo groźnym, ponieważ użytkownicy mogą nie zdawać sobie sprawy z infekcji, zanim nie dojdzie do poważnego naruszenia ich prywatności i bezpieczeństwa.



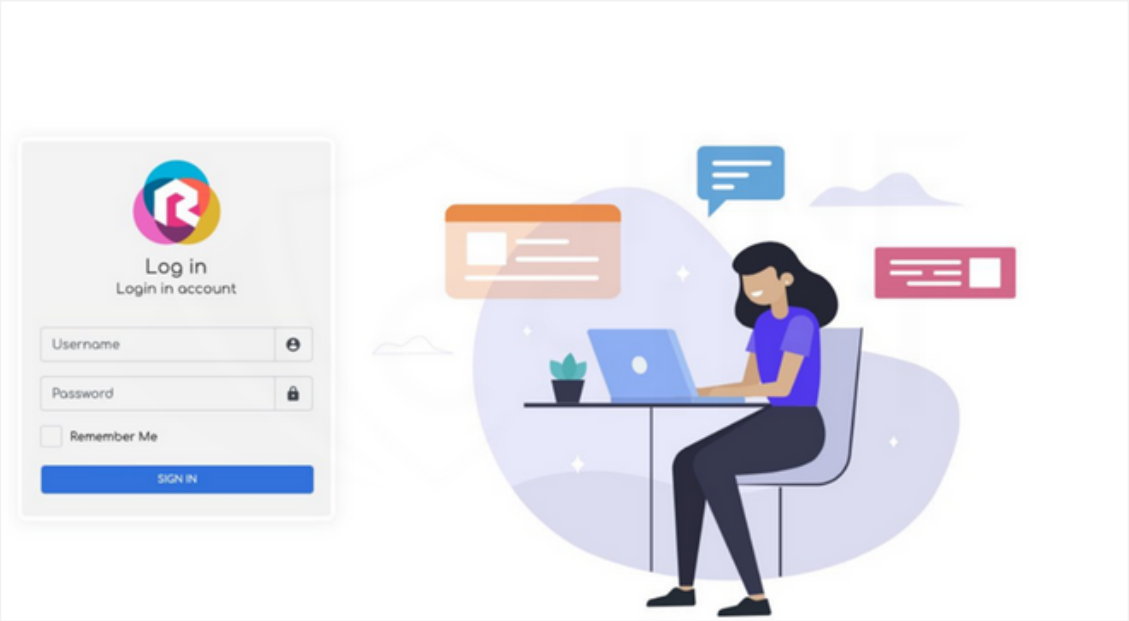
Grafika 43. Panel logowania do Vidar Stealer

AMOS Stealer to specyficzny rodzaj złośliwego oprogramowania, które ukierunkowane jest na użytkowników komputerów Apple Macbook. Jest to szczególnie ciekawy przypadek złośliwego oprogramowania, które zmienia perspektywę postrzegania systemów MacOS od wielu lat uważanych za względnie odporne na złośliwe oprogramowanie. AMOS Stealer demonstruje, że żaden system nie jest całkowicie odporny na zagrożenia. Przestępcy stosują wyrafinowane metody dystrybucji tego złośliwego oprogramowania np. z wykorzystaniem nośników reklamowych w wyszukiwarce Google, docierając do szerokiego grona odbiorców nieświadomych ryzyka, co bezpośrednio przekłada się na skalę i zasięg działania tego Stealera.



Grafika 44. Panel logowania do AMOS Stealer

RisePro – kolejny rodzaj stealera który wyróżnia się metodą dystrybucji poprzez PrivateLoader, platformę dystrybucji malware działającą na zasadzie płatności za instalację (PPI). Ta metoda jest znana z udostępniania fałszywego, łamiącego zabezpieczenia oprogramowania oraz nielegalnych treści, co umożliwia szerokie rozprzestrzenianie się RisePro. Analiza wykazała, że RisePro potrafi kraść dane karty kredytowej, hasła i dane z portfeli kryptowalutowych ofiar. Co istotne, to złośliwe oprogramowanie jest w stanie przesyłać skradzione dane na serwer kontrolowany przez atakującego, co zwiększa ryzyko wykorzystania tych informacji w nielegalnych działaniach. Napisany w języku C++, RisePro jest dostępny do zakupu poprzez komunikator Telegram, co umożliwia łatwy dostęp i wykorzystanie przez potencjalnych cyberprzestępców. Zwraca uwagę fakt, że RisePro wykorzystuje podobny system wbudowanych zależności DLL, co znane złośliwe oprogramowanie Vidar, przeznaczone do kradzieży haseł. W działaniu, RisePro przeprowadza skanowanie kluczy rejestru zainfekowanego systemu, zapisuje skradzione dane do pliku tekstowego, wykonuje zrzut ekranu i kompresuje te informacje do archiwum ZIP, które następnie jest wysyłane do atakującego. RisePro jest również zdolny do skanowania folderów systemu plików w poszukiwaniu danych takich jak dokumenty zawierające dane karty kredytowej, co obrazuje jego wysoką skuteczność w lokalizowaniu i ekstrakcji wartościowych danych.



Grafika 45. Panel logowania do RisePro Stealer

Strategie ochrony i reakcji

Ochrona przed Stealerami wymaga kompleksowego podejścia. Najważniejsze jest stosowanie dobrych praktyk cyberhigieny, takich jak regularne aktualizacje oprogramowania, używanie silnych i unikalnych haseł oraz włączenie dwuetapowej weryfikacji. Ważne jest również korzystanie z zaufanych źródeł oprogramowania.

Więcej o dobrych praktykach dowiedzieć się można z materiału opublikowanego przez CERT Polska, który dostępny jest tutaj[14].

[14] https://cert.pl/posts/2022/01/kompleksowo-o-haslach/

Oszustwa telefoniczne

Za jedno z najistotniejszych zagrożeń wymierzonych w użytkowników cyberprzestrzeni w 2023 uznać należy również vishing czyli rodzaj phishingu wykorzystujący rozmowy telefoniczne. Cyberprzestępcy podszywając się pod numer telefonu różnych instytucji czy organizacji takich jak banki, policja, instytucje publiczne czy firmy pożyczkowe, kontaktowali się z ofiarami i przy wykorzystaniu metod socjotechnicznych wyłudzali różnego rodzaju informacje. Oszuści, aby wpłynąć na zachowania użytkowników informowali o rzekomych próbach włamania na konto bankowe, konieczności zweryfikowania przelewu czy innych problemach, które służyły manipulacji ofiarą, wywołanie w niej poczucia niepewności i strachu. Finalnie zmanipulowana ofiara pod presją czasu i w stresie przekazywała przestępcom informacje które wykorzystywali oni do kradzieży środków finansowych. Prowadzenie tego typu oszustw ułatwiały szczegółowe dane o ofierze które przestępcy wykorzystywali do uwiarygodniania i potwierdzania prawdziwości wymyślonych historii.

Po raz kolejny potwierdziły się przypadki, w których cyberprzestępcy aktywnie reagowali na sytuacje na rynku finansowym i bardzo szybko dostosowywali do nich scenariusze przestępcze. Zaobserwowaliśmy atak vishingowy, oparty o motyw niedostępnych w danym momencie usług bankowych. Oszuści wykorzystując komunikaty publikowane przez banki (np. informacje o czasowej niedostępności lub awarii systemu bankowości elektronicznej czy braku możliwości zapłaty kartą, trudności z korzystaniem z bankomatów i wpłatomatów itp.) kontaktowali się z ofiarami i próbowali wyłudzić od nich poufne informacje, np. dane uwierzytelniające do bankowości elektronicznej, numer PESEL lub dane karty płatniczej.

W kolejnych etapach oszuści wymagali od użytkowników zainstalowania programu do zdalnego pulpitu i zalogowania się do swojej bankowości elektronicznej co pozwalało im na obserwację działań użytkowników i wprowadzanych przez nich treści w tym danych dostępowych do systemów bankowych, poczty elektronicznej czy mediów społecznościowych.

04.RAPORTY I ANALIZY

RAPORTY I ANALIZY

Zespół CSIRT KNF prowadzi stały monitoring i analizę sposobów i działań cyberprzestępców, czego wynikiem są także publikowane w 2023 roku opracowania i raporty. Publikacje te, będące wynikiem naszego zaangażowania i specjalistycznej wiedzy, koncentrują się na aktualnych wyzwaniach w dziedzinie cyberbezpieczeństwa i dynamicznie zmieniających się zagrożeniach w cyberprzestrzeni. Obejmują one tematy takie jak międzynarodowe kampanie phishingowe, analizy złośliwego oprogramowania oraz identyfikację i analizy nowych schematów ataków. Nasze publikacje mają na celu informowanie, edukowanie i reagowanie na nowe zagrożenia w cyberprzestrzeni, ze szczególnym uwzględnieniem bezpieczeństwa klientów i podmiotów polskiego rynku finansowego.

Wybrane opracowania, opublikowane przez CSIRT KNF w 2023:

1. **"HOOKBOT - nowa rodzina złośliwego oprogramowania mobilnego"**
   - Wersja PL: Link do raportu PL
   - Wersja EN: Link do raportu EN
   - Opis: Raport przedstawia techniczną analizę funkcjonowania złośliwego oprogramowania HOOKBOT. Treść raportu zawiera szczegóły funkcjonowania poszczególnych komponentów malware oraz listę formularzy podszywających się pod legalne aplikacje.
   - Miesiąc publikacji: **Luty 2023**

2. "Wykorzystanie technologii WebAPK do ataku phishingowego"

- Wersja PL: Link do raportu PL
- Wersja EN: Link do raportu EN
- Opis: Raport zawiera analizę phishingowej strony internetowej, wykorzystującej mobilną technologię WebAPK do instalacji złośliwej aplikacji na urządzeniach z systemem Android.
- Miesiąc publikacji: **Lipiec 2023**

3. "Międzynarodowa Kampania Phishingowa Podszywająca się pod Instytucje Pocztowe: Analiza"

- Wersja PL: Link do raportu PL
- Wersja EN: Link do raportu EN
- Opis: Raport szczegółowo analizuje międzynarodową kampanię phishingową, która wykorzystuje fałszywe strony internetowe podszywające się pod znane instytucje pocztowe. Zawiera analizę wykorzystywanych technik i środków zapobiegawczych.
- Miesiąc publikacji: **Lipiec 2023**

4. "Analiza złośliwego oprogramowania z serwisu YouTube"

- Wersja PL: Link do raportu PL
- Wersja EN: Link do raportu EN
- Opis: dokument omawia szczegółowo rozprzestrzenianie się złośliwego oprogramowania poprzez serwis YouTube, prezentując metody jego dystrybucji i wpływ na użytkowników.
- Miesiąc publikacji: **Lipiec 2023**

5. "RANSOMED[.]VC – forum, ransomware czy haktywiści?"

- Wersja PL: Link do raportu PL
- Wersja EN: Link do raportu EN
- Opis: Analiza koncentruje się na RANSOMED[.]VC, badając jego charakter jako forum, oprogramowanie ransomware, oraz potencjalną aktywność haktywistyczną. Raport zawiera kluczowe wnioski dotyczące zagrożeń z nim związanych.
- Miesiąc publikacji: **Wrzesień 2023**

6. "AMOS/ATOMIC Stealer – malware na MAC OS"

- Wersja PL: Link do raportu PL
- Wersja EN: Link do raportu EN
- Opis: Publikacja skupia się na analizie AMOS/ATOMIC Stealer, specyficznego rodzaju złośliwego oprogramowania atakującego systemy MAC OS, przedstawiając metody działania i sposoby ochrony.
- Miesiąc publikacji: **Październik 2023**

7. "Globalna kampania podszywająca się pod usługi pocztowe"

- Wersja PL: Link do raportu PL
- Wersja EN: Link do raportu EN
- Opis: Raport omawia szczegóły globalnej kampanii phishingowej, która wykorzystuje fałszywe strony internetowe imitujące usługi pocztowe, zwracając uwagę na techniki stosowane przez przestępców i środki zaradcze.
- Miesiąc publikacji: **Listopad 2023**

8. "MADCAT RANSOMWARE – wielowymiarowe przestępstwo"

- Wersja PL: Link do raportu PL
- Wersja EN: Link do raportu EN
- Opis: dokument analizuje MADCAT Ransomware, przedstawiając wielowymiarowy charakter grupy jako przestępców i oszustów.
- Miesiąc publikacji: **Listopad 2023**

Zapraszamy do zapoznania się z naszymi publikacjami, opracowaniami i analizami które dostępne są tutaj [15].

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

04. DZIAŁALNOŚĆ EDUKACYJNA

DZIAŁALNOŚĆ EDUKACYJNA CSIRT KNF W 2023 ROKU

Wzmacnianie świadomości użytkowników w zakresie zagrożeń występujących w cyberprzestrzeni stanowi istotny element działalności CSIRT KNF. To świadomość zagrożeń jest podstawowym elementem ochrony i bezpieczeństwa. Pojawiające się nowe zagrożenia czy coraz bardziej wyrafinowane techniki i sposoby działania cyberprzestępców wymagają od użytkowników Internetu stałego aktualizowania wiedzy w tym zakresie.

W 2023 roku zespół CSIRT KNF przeprowadził szereg szkoleń m.in. w ramach projektu edukacyjnego Centrum Edukacji dla Uczestników Rynku – CEDUR, realizowanego przez Urząd Komisji Nadzoru Finansowego. Tematyka szkoleń obejmowała prezentację aktualnych zagrożeń wymierzonych w użytkowników cyberprzestrzeni. Podczas webinariów, w których udział był bezpłatny, uczestnikom przybliżone zostały najpopularniejsze metody ataków, sposoby działania złośliwego oprogramowania, a także dobre praktyki pozwalające na uchronienie się przed oszustwami internetowymi. Szkolenia skierowane były głównie do uczniów szkół ponadpodstawowych i nauczycieli oraz seniorów i ich opiekunów.
Wśród inicjatyw (realizowanych w ramach międzynarodowych kampanii) propagujących wiedzę z zakresu cyberbezpieczeństwa rynku finansowego, w których uczestniczyli przedstawiciele CSIRT KNF wyróżnić można realizowane w ramach kampanii międzynarodowych:

- Global Money Week (GMW) – Światowy Tydzień Pieniądza[16] 2023, przeprowadzone zostały webinaria CEDUR o tematyce cyberbezpieczeństwa, dla uczniów szkół ponadpodstawowych i nauczycieli:

[16] Global Money Week (GMW) - Światowy Tydzień Pieniądza - coroczna międzynarodowa kampania z zakresu edukacji finansowej na rzecz dbania o to, by dzieci i młodzież od najmłodszych lat zyskiwały świadomość finansową i stopniowo rozwijały wiedzę, umiejętności, a także kształtowały postawy i zachowania niezbędne do podejmowania racjonalnych decyzji finansowych i docelowo uzyskały finansowy dobrostan i finansową odporność. Organizatorem kampanii GMW jest Międzynarodowa Sieć ds. Edukacji Finansowej działająca przy Organizacji Współpracy Gospodarczej i Rozwoju - OECD/INFE. UKNF jest koordynatorem krajowym GMW.

- „Bezpieczny telefon – jak chronić się przed cyberprzestępcami?”. Podczas szkolenia przedstawiona została problematyka zagrożeń cyberbezpieczeństwa dla środków finansowych użytkowników urządzeń mobilnych. Przybliżono najczęściej występujące metody i techniki stosowane przez cyberprzestępców, a także możliwe sposoby pozwalające na uchronienie się przed oszustwami;
- „Cyberoszuści atakują – jak nie dać się okraść w Internecie”, w ramach którego przedstawiona została problematyka zagrożeń cyberbezpieczeństwa dla środków finansowych użytkowników Internetu. W trakcie webinarium omówione zostały m.in. zagadnienia ataków phishingowych, zagrożenia czyhające w mediach społecznościowych, oszustwa na portalach sprzedażowych oraz oszustwa inwestycyjne.

W ramach kampanii World Inwestor Week 2023 – Światowy Tydzień Inwestora[17] – przeprowadzone zostały webinaria CEDUR o tematyce cyberbezpieczeństwa, dla uczniów szkół ponadpodstawowych i nauczycieli:

- „Cyberbezpieczeństwo z perspektywy klienta usług finansowych – aspekty praktyczne”, w ramach szkolenia omówione zostały zagadnienia związane z atakami phishingowymi, zagrożeniami w mediach społecznościowych, na portalach sprzedażowych czy oszustwa inwestycyjne.
- „Jak zadbać o bezpieczeństwo swojego telefonu i nie dać się okraść”, w ramach którego wskazano na najpopularniejsze zagrożenia wymierzone w użytkowników urządzeń mobilnych. W trakcie webinarium omówione zostały m.in. zagadnienia popularnych metod ataków, sposobu działania złośliwego oprogramowania, najczęściej popełnianych błędów wpływających na bezpieczeństwo, jak również dobrych praktyk służących jego poprawie.

[17] World Investor Week (WIW) - Światowy Tydzień Inwestora - kampania o zasięgu globalnym powołana do życia przez Międzynarodową Organizację Komisji Papierów Wartościowych (IOSCO) w 2017 r. na rzecz zwiększenia świadomości społecznej na temat roli edukacji oraz ochrony inwestorów na rynku finansowym. Kampania ma na celu promowanie inicjatyw podejmowanych w tym obszarze przez krajowe instytucje nadzorujące i regulujące rynki papierów wartościowych. UKNF jest koordynatorem krajowym WIW.

W celu zwiększenia świadomości i uwrażliwienia seniorów na zagrożenia występujące w Internecie tematyka webinariów CEDUR dla seniorów i ich opiekunów obejmowała następujące zagadnienia z obszaru cyberbezpieczeństwa:

- „Cyberbezpieczeństwo w kontekście zagrożeń występujących w Internecie, w szczególności oszustw na urządzeniach mobilnych” [18],
- „Cyberbezpieczeństwo podczas zawierania transakcji elektronicznych z podmiotami rynku finansowego, ochrona konsumentów na rynku finansowym, w szczególności przed działalnością cyberprzestępców, uwzględniając takie metody oszustw, jak vishing i spoofing” [19].

Supervision Hack

Zespół CSIRT KNF uczestniczył w drugiej edycji maratonu programowania Supervision Hack organizowanego przez Urząd Komisji Nadzoru Finansowego. Zadaniem uczestników było zmierzenie się z przygotowanymi przez UKNF zadaniami programistycznymi. Jednym z wyzwań było „Ads Detect” opracowane przez CSIRT KNF, w ramach którego należało rozbudować narzędzie pozwalające na skuteczniejsze wykrywanie fałszywych reklam.

Konferencja PLNOG

Zespół CSIRT KNF w 2023 roku aktywnie uczestniczył w konferencjach poświęconych zagadnieniom cyberbezpieczeństwa. Podczas 32. edycji konferencji PLNOG, Kierownik zespołu CSIRT KNF – Paweł Piekutowski zaprezentował temat „Był sobie DDoS, czyli o tym kto je robi, komu, jak, za ile i czy to w ogóle ma sens.” Podczas wystąpienia przybliżył m. in czynniki mające wpływ na zwiększenie grup haktywistycznych, odpowiedzialnych za przeprowadzanie ataków typu DDoS na terenie kraju, kosztach zrealizowania takich ataków czy sposobów pozwalających na ochronę przed nimi.

[18]Webinarium zorganizowane we współpracy z Komendą Główną Policji.
[19] Webinarium zorganizowane we współpracy z Komendą Główną Policji oraz Ministerstwem Rodziny i Polityki Społecznej.

Confidence 2023

Podczas 23 edycji konferencji „Confidence 2023" przedstawiciele zespołu CSIRT KNF przybliżyli tematykę Cyber Threat Intelligence i Threat Huntingu w dwóch wystąpieniach tj. „Nurkowanie głębinowe z rekinami, czyli kampanie przestępcze od środka..." oraz „Historia threat actora: mobilny malware na pęczki".

Security Case Study

Podczas konferencji „Security Case Study 2023" skupiającej środowisko IT security, zaprezentowane zostało wystąpienie „Od zera do hakera w ataku na łańcuch dostaw". Podczas wystąpienia omówione zostały ryzyka związane z Supply Chain Attack, a w ramach studium przypadku zaprezentowane zostało narzędzie napisane przy pomocy AI, służące do wyszukiwania podatności stron internetowych. Drugim wystąpieniem była tożsama z konferencją „Confidence 2023" prezentacja „Nurkowanie głębinowe z rekinami, czyli kampanie przestępcze od środka..." zaktualizowana o dane i informacje pozyskane od czerwca 2023 roku.

Advanced Threat Summit

Podczas 10 edycji konferencji Advanced Threat Summit przedstawicielki CSIRT KNF zaprezentowały temat „Jak cyberprzestępcy oszukują ludzi i dlaczego tak bardzo lubią sektor finansowy, czyli krajobraz cyberzagrożeń z punktu widzenia CSIRT KNF". Podczas wystąpienia wskazane zostały najciekawsze schematy oszustw oraz scenariusze stosowane przez cyberprzestępców. Przybliżona została także analiza grup przestępczych z kategorii cybercrime.

Partnerstwo dla Cyberbezpieczeństwa

Zespół CSIRT KNF będący elementem krajowego systemu cyberbezpieczeństwa współpracuje i wspiera podmioty i organizacje budujące kompetencje w zakresie cyberbezpieczeństwa. W ramach programu Partnerstwo dla Cyberbezpieczeństwa (PdC), powstałego z inicjatywy NASK – Państwowy Instytut Badawczy i Ministerstwa Cyfryzacji, stanowiącego przestrzeń do wymiany informacji o cyberzagrożeniach, przedstawiciele zespołu CSIRT KNF przybliżyli tematykę związaną z atakami DDoS i zagrożeniami dotyczącymi wykorzystania sztucznej inteligencji przez cyberprzestępców.

Aktywność w mediach społecznościowych

Zespół CSIRT KNF prowadzi profile w mediach społecznościowych tj. w portalach X, Facebook i LinkedIn, gdzie publikuje informacje i ostrzeżenia dotyczące najnowszych sposobów działania cyberprzestępców oraz oszustw internetowych. Aby dotrzeć do jak najszerszego grona odbiorów w 2023 roku przygotowano 256 publikacji w mediach społecznościowych, które dotyczyły najnowszych metod i sposobów działania cyberprzestępców. Na podstawie wiadomości pochodzących z publikacji CSIRT KNF w 2023 roku powstało ponad tysiąc artykułów w portalach branżowych oraz informacyjnych o ogólnopolskim zasięgu.

W 2023 roku ostrzeżenia publikowane w mediach społecznościowych dotyczyły głównie:

- fałszywych stron bankowości elektronicznej,
- fałszywych ofert inwestycyjnych wyłudzających dane od użytkownika,
- fałszywych stron podszywających się pod usługi kurierskie czy pocztowe, gdzie wyłudzane były dane kart kredytowych.

Grafika 46. Ostrzeżenie CSIRT KNF w mediach społecznościowych dotyczące wykorzystania nowej funkcji aplikacji WhatsApp, w atakach na użytkowników cyberprzestrzeni

05. WPŁYW ROZWOJU SZTUCZNEJ INTELIGENCJI

WPŁYW ROZWOJU SZTUCZNEJ INTELIGENCJI NA DZIAŁANIA CYBERPRZESTĘPCÓW - PODSUMOWANIE 2023

Miniony rok, przez wielu, uznany został jako rok sztucznej inteligencji. Gdy pod koniec roku 2022 do publicznego stosowania oddany został ChatGPT-3.5, w ciągu zaledwie 5 dni zyskał ponad milion użytkowników (dla porównania Netflixowi zajęło to 41 miesięcy, Facebookowi 10 miesięcy, a Instagramowi 2,5 miesiąca). Zdobycie 100 milionów użytkowników zajęło ChatGPT dwa miesiące (TikTok na taką skalę czekał dziewięć miesięcy). W marcu 2023 roku, kiedy to OpenAI udostępnił ChatGPT-4 który dał użytkownikom nowe możliwości a przede wszystkim nieznaną do tej pory jakość interakcji z tego typu technologią. Kolejne aktualizacje eliminujące m.in. halucynację odpowiedzi modelu językowego, udostępnienie połączenia webowego (pozwalającego na wyszukiwania treści online), czy dodanie modułu głosowego pociągnęło za sobą fale tworzenia nowych narzędzi AI.

Aby przybliżyć podstawy tematyki AI, zachęcamy do zapoznania się z naszymi artykułami, które przedstawiają definicyjne wprowadzenie do świata AI:

- https://cebrf.knf.gov.pl/komunikaty/artykuly-csirt-knf/362-ostrzezenia/887-wprowadzenie-do-sztucznej-inteligencji

- https://cebrf.knf.gov.pl/komunikaty/artykuly-csirt-knf/362-ostrzezenia/892-jak-sztuczna-inteligencja-przetwarza-dane

Niestety dostęp do technologii AI wyprzedził ogólną wiedzę o sposobie jej działania, w konsekwencji wielu użytkowników wykorzystujących narzędzia AI, nie jest świadomych tego z czym mają do czynienia, a tym bardziej jakie rodzi to zagrożenia. Obawa, która spędza sen z powiek osób zajmujących się ochroną informacji, to nierozsądne udostępnianie materiałów służbowych w tego typu narzędziach, mogące prowadzić do ujawnień informacji i wycieków danych.

Cyberoszuści szukają, obserwują, testują i również wspierają swoje działania wykorzystując nowoczesne technologie – w tym AI - do tworzenia treści i uwiarygodniania scenariuszy oszustw. Tym wykorzystaniem, z którym w 2023 roku mieliśmy najczęściej w analizach do czynienia to nagrania video przygotowane dzięki wykorzystaniu technologii deepfake.

Deepfake to technika oparta na sztucznej inteligencji, wykorzystująca metody głębokiego uczenia się do tworzenia lub modyfikowania obrazów i nagrań wideo, tak aby wydawały się realistyczne, ale są fałszywe.

Scenariuszem, w którym przestępcy najczęściej wykorzystywali fałszywe nagrania jest opisywane w tym raporcie oszustwo na „fałszywe okazje inwestycyjne". Metoda przestępcza, w której atakujący obiecując rzekome pewne zyski z inwestycji, przy wykorzystaniu licznych zabiegów socjotechnicznych, zachęcają ludzi do przekazywania im wysokich kwot.

Oszuści, aby jeszcze bardziej uwiarygodnić swoje manipulacje, zaczęli publikować w mediach społecznościowych fałszywe nagrania video, w których znane osoby (m.in. sportowcy, politycy, aktorzy) zachęcają potencjalne ofiary do zainwestowania pieniędzy. Z biegiem czasu, cyberprzestępcy zaczęli robić coraz to bardziej wiarygodnie wyglądające nagrania deepfake, utrudniając tym samym możliwość rozpoznania oszustwa. Nie jest to jednak jedyne miejsce, w którym przestępcy dopuszczali się użycia omawianej technologii. Zarówno w Polsce, jak i na świecie w 2023 roku znane były przypadki użycia sfałszowanych nagrań głosu w przestępstwach znanych pod nazwą „na legendę" lub bardziej powszechnie jako „metoda na wnuczka/policjanta". W takich przypadkach do ofiary oszustwa dzwonił np. rzekomy policjant, po czym przekazywał telefon członkowi rodziny, a w rzeczywistości rozmowa prowadzona była głosem imitującym członka rodziny.

Na świecie występowały również przypadki wykorzystania technologii deepfake do oszustw typu BEC (ang. business email compromise). Dla przykładu, brytyjska firma energetyczna straciła 243 tys. dolarów z powodu oszustwa głosowego typu deepfake [20]. Jak podają statystyki przygotowane przez ekspertów z Contentdetector AI, w 2023 r. w mediach społecznościowych może się pojawić około 500 000 filmów i fałszywych treści głosowych, co jest zgodne z prognozami DeepMedia (firmy specjalizującej się w wykrywaniu i analizie deepfake'ów). To duży wzrost w porównaniu z poprzednimi latami. W 2021 roku w Internecie zidentyfikowano 14 678 fałszywych filmów, a było to dwukrotnie więcej niż w 2018 roku.

[20] https://cyberpolicy.nask.pl/wp-content/uploads/2023/09/Cyberbezpieczenstwo-AI.-AI-w-cyberbezpieczenstwie.pdf

W Stanach Zjednoczonych liczba przypadków deepfake wykorzystywanych do oszustw wzrosła z 0,2% do 2,6% między 2022 rokiem, a I kwartałem 2023 roku. W Kanadzie odsetek ten wzrósł z 0,1% do 4,6% [21].

Deepfake nie są jedynymi zastosowaniami sztucznej inteligencji w rękach przestępców. Dostosowali oni modele AI do swoich potrzeb tak, aby pomagały im w prowadzeniu wybranych scenariuszy przestępczych. Na koniec 2023 roku na forach przestępczych można było zobaczyć reklamy kilkudziesięciu tego typu narzędzi, z czego w przestrzeni medialnej największy rozgłos zyskały dwa – WormGPT oraz FraudGPT.

Według deklaracji narzędzia te potrafią m.in.:

- tworzyć poprawne treści wiadomości phishingowych w dowolnym języku (warto zaznaczyć, że dokładnie to samo można osiągnąć legalnymi narzędziami, przy odpowiednio zbudowanym zapytaniu),
- proponować scenariusze oszustwa w zależności od kraju, języka i innych czynników wpływających na kampanie phishingowe,
- generować złośliwe oprogramowanie,
- nauczyć prowadzenia ataków, w tym budowania i publikowania stron phishingowych,
- pomóc w zarządzaniu stronami phishingowymi.

W naszej ocenie rozwój narzędzi AI może przyczynić się do znacznego obniżenia progu wejścia w świat cyberprzestępczości.

Rok 2023 pozostawił po sobie wiele pytań. Czy przestępcy będą rozwijać narzędzia przestępcze oparte na AI? Czy wykorzystanie deepfake stanie się tak powszechne? Czy metody wykrywania zmanipulowanych treści będą rozwijać się w co najmniej takim samym tempie, co narzędzia do ich generowania? Jak bardzo zmieni się krajobraz zagrożeń w najbliższych miesiącach? Te i wiele innych pytań pozostaje obecnie bez odpowiedzi i my także takimi je tu pozostawiamy.

[21] https://contentdetector.ai/articles/deepfake-statistics