KNF CSIRT

FAŁSZYWE INWESTYCJE

WPROWADZENIE

Fałszywe inwestycje są jednymi z najczęściej występujących ataków wymierzonych w osoby korzystające z usług oferowanych na rynku finansowym. Oszustwo polega na nakłonieniu ofiary za pomocą technik manipulacji do inwestycji, która jest fałszywa. Na przestrzeni ostatniego roku ten rodzaj oszustwa stał się jednym z najpopularniejszych sposobów wyłudzenia pieniędzy.

W większości przypadków schemat działania jest bardzo podobny. Przestępcy dystrybuują fałszywe strony przy pomocy reklam umieszczonych w mediach społecznościowych. Przyciągają one uwagę użytkowników, zarówno oprawą graficzną, która coraz częściej wygląda bardzo profesjonalnie, jak też ofertą bardzo wysokich zysków bez ryzyka utraty środków finansowych przy minimalnym nakładzie pracy i zaangażowaniu. Oszuści wykorzystują wizerunki znanych osób, firm oraz instytucji państwowych, w celu uwiarygodnienia swojej reklamy. Po podaniu danych w formularzu na stronie, z użytkownikiem kontaktuje się konsultant oferujący pomoc w przejściu całego procesu.

Oszuści są bardzo dobrze przygotowani do rozmowy z ofiarą. Aby wzbudzić zaufanie użytkowników odpowiadają na zadawane pytania, używając m.in. technicznych zwrotów. Następnie ofiara otrzymuje dostęp do fałszywej platformy inwestycyjnej, na którą może wpłacić środki. Po ich zdeponowaniu oszuści wykorzystują socjotechnikę, nakłaniając poszkodowanego do kolejnych wpłat, przeważnie pod pretekstem atrakcyjnej koniunktury na rynkach finansowym i szybkim pomnożeniu zysków z kolejnej inwestycji. Starają się w ten sposób wymusić na ofierze maksymalizację kwoty kolejnej wpłaty.

CSIRT KNF podejmuje szereg działań, aby przeciwdziałać oszustwom inwestycyjnym. Zespół aktywnie prowadzi akcję informacyjną w mediach społecznościowych, gdzie publikuje ostrzeżenia odnośnie najnowszych metod ataków. Ostrzeżenia mają na celu dotarcie do jak największej liczby użytkowników i ich ochronę przed nieświadomym zainwestowaniem środków finansowych w fałszywe inwestycje. Od początku tego roku wystosowano 22 ostrzeżenia, które zostały opublikowane na Platformach Twitter, Facebook oraz LinkedIn.

WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

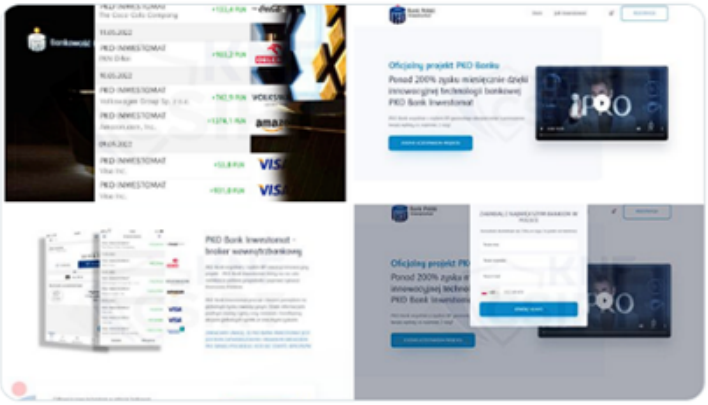
PRZYKŁADY OSTRZEŻEŃ NA PLATFORMIE TWITTER

CSIRT KNF
@CSIRT_KNF

Uwaga na fałszywe reklamy inwestycyjne, w których cyberprzestępcy podszywają się pod @PKOBP. W rzeczywistości prowadzą one do niebezpiecznych stron wyłudzających dane, a docelowo kradzieży środków pieniężnych.

Nie dajcie się nabrać i ostrzeżcie znajomych!

Translate Tweet



1:10 PM · Jun 9, 2022 · Twitter Web App

CSIRT KNF
@CSIRT_KNF

Uwaga na kolejne oszustwo inwestycyjne, w którym cyberprzestępcy podszywają się pod @MF_GOV_PL i zachęcają do inwestycji w nową (nieistniejącą) walutę państwową. W rzeczywistości dokonanie rejestracji na fałszywej stronie i zainwestowanie środków grozi ich utratą. Bądźcie czujni!

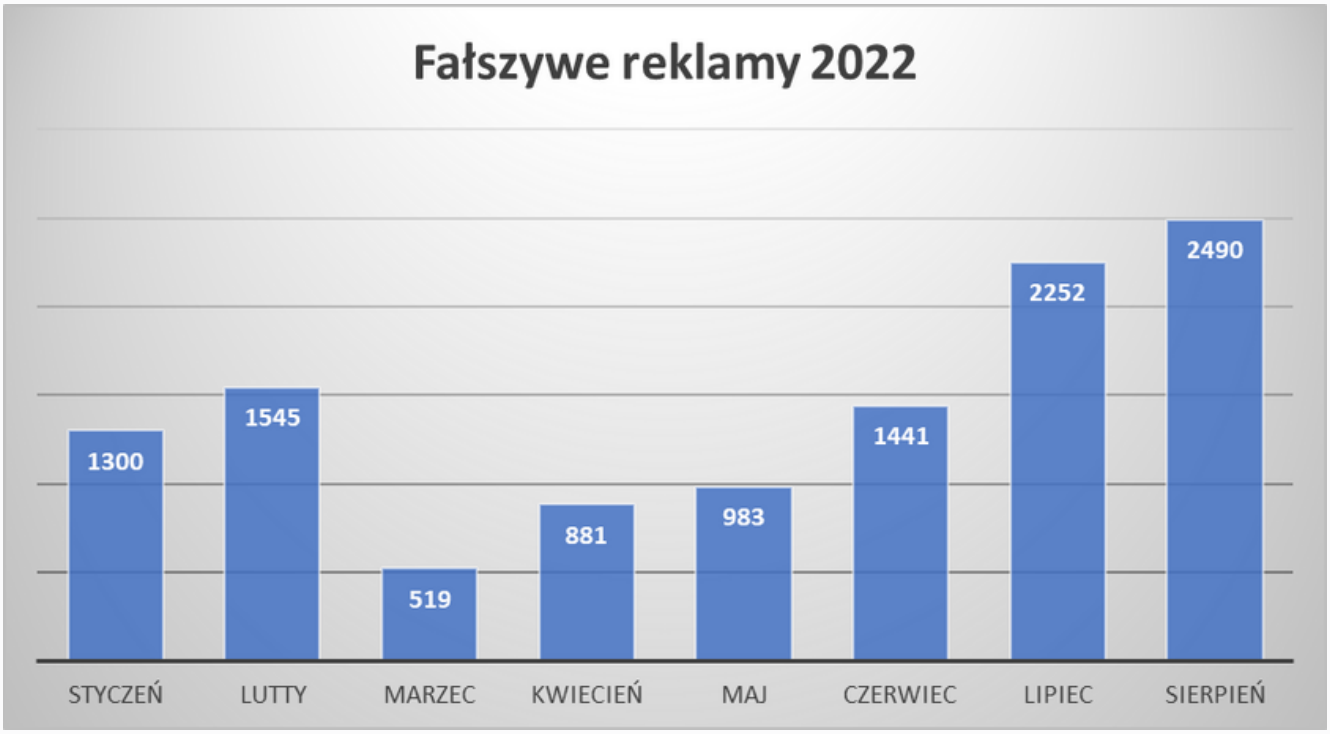
Translate Tweet

3:07 PM · Jun 7, 2022 · Twitter Web App

WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

FAŁSZYWE INWESTYCJE 01.01.2022-31.08.2022

CSIRT KNF przeciwdziała oszustwom inwestycyjnym również poprzez aktywne zgłaszanie fałszywych reklam. Reklamy wyszukiwane są przy pomocy narzędzia Facebook Library Ads, następnie ich identyfikatory są przesyłane do przedstawicieli platformy Facebook. W okresie 01.01.2022 - 31.08.2022 zgłoszono 11 411 fałszywych reklam.



Ogólna liczba fałszywych reklam zgłoszonych do zablokowania w poszczególnych miesiącach.

FAŁSZYWE INWESTYCJE 01.01.2022-31.08.2022

We wskazanym okresie, największą liczbą oszustw inwestycyjnych, jaką odnotował zespół CSIRT KNF, było wykorzystanie wizerunku spółki Orlen. Przestępcy dosyć często podszywali się również pod przedsiębiorstwo Tesla. Spora część dotyczyła także pozostałych spółek skarbu państwa oraz banków. Najmniejszy odsetek stanowiły zaś przestępstwa, w których cyberprzestępcy posługiwali się znakiem towarowym innych firm takich jak CD Projekt, Nvidia, Avast czy też kryptowalut.

Wykorzystywane wizerunki w raportowanym okresie.

METODY DZIAŁANIA OSZUSTÓW

Oszuści stosują różnego rodzaju techniki socjotechniczne, które mają na celu zmanipulowanie ofiary. Poza obietnicą dużych zysków, w krótkim czasie i bez ryzyka utraty pieniędzy, w reklamie umieszczone są filmy, na których osoba opowiada jak wzbogaciła się i polepszyła swoje życie korzystając z danej inwestycji.

W filmach wykorzystywane są urywki programów telewizyjnych, informacyjnych lub rozrywkowych. Podstawiany jest głos lektora, który opowiada o danym „programie" oraz możliwości szybkiego zarobku. Stosowana jest również technika podstawiania narracji w języku polskim pod wypowiedź osób anglojęzycznych, tak, aby pasowały do danego oszustwa. Aby zwiększyć wiarygodność, w reklamach umieszczane są wizerunki znanych osób takich jak celebryci, politycy, inwestorzy, sportowcy oraz inne osoby znane medialnie.

Przykładowe reklamy wykorzystujące wizerunek znanych osób

WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

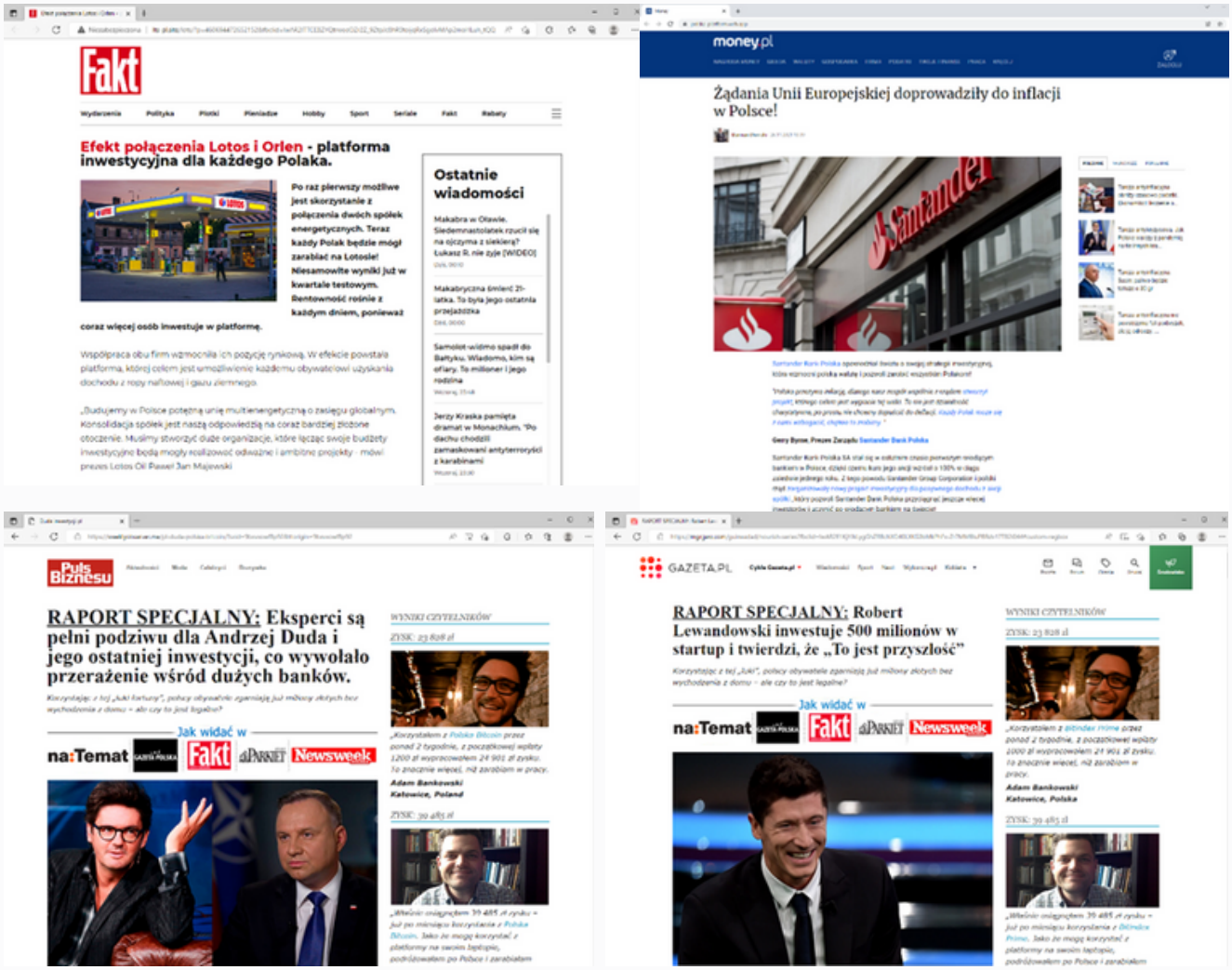
METODY DZIAŁANIA OSZUSTÓW

Sposoby manipulacji użytkowników podlegają ciągłej ewolucji i modyfikacji. Przestępcy śledzą globalne trendy i dostosowują swoje działania tak, aby były jak najbardziej wiarygodne. Reklamy często są spersonalizowane i dopasowane do konkretnej grupy odbiorców np. emerytów lub młodzieży. Treść reklam bardzo często nawiązuje do aktualnego stanu politycznego lub danego okresu np. świątecznego.

Reklamy ukierunkowane kolejno; na emerytów; w okresie świątecznym; w Black Friday.

Następną techniką stosowaną przez cyberprzestępców jest uwiarygodnienie danej inwestycji. Cyberprzestępcy przygotowują fałszywe strony, na których zamieszczają informacje odnośnie możliwości, jakie oferuje „platforma". Użytkownik klikając w reklamę, jest przenoszony na witrynę, która do złudzenia przypomina portal informacyjny. Na podstawionych stronach umieszczony jest zmyślony opis programów inwestycyjnych, które zapewniają szybki zysk. Po kliknięciu odpowiedniego przycisku, następuje przeniesienie do strony z formularzem, gdzie ofiara proszona jest o podanie swoich danych. Taki zabieg ma na celu uwiarygodnienie inwestycji w oczach ofiary.

METODY DZIAŁANIA OSZUSTÓW



Przykłady fałszywych stron podszywających się pod portale informacyjne.

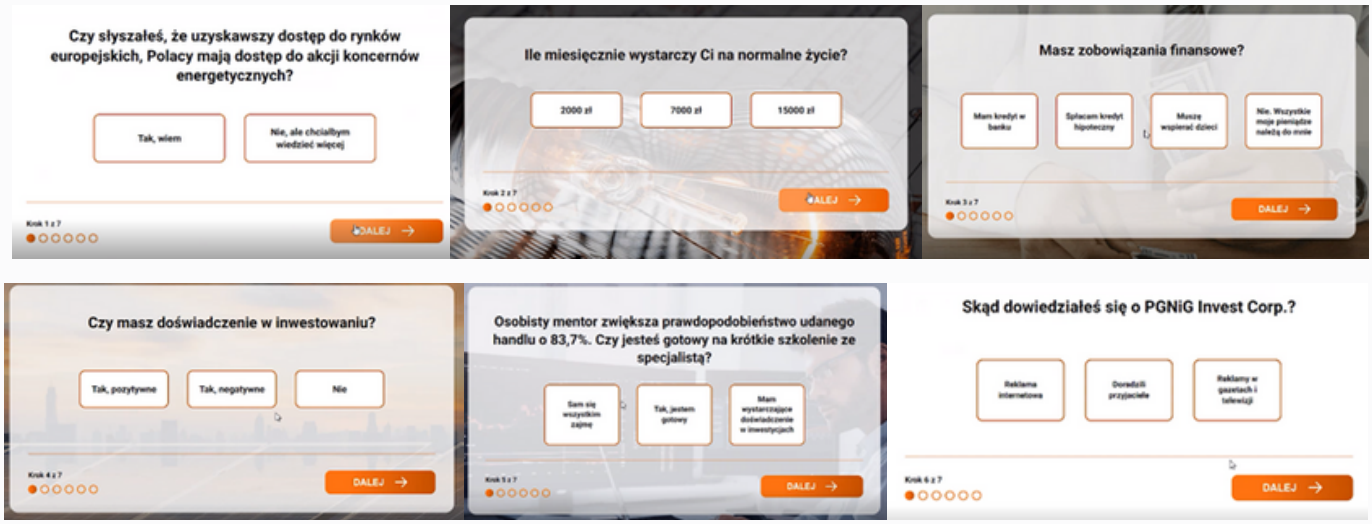
Fałszywe artykuły przekierowują do stron, na których ofiara proszona jest o podanie imienia, nazwiska, numeru telefonu i adresu email.

Przykładowy formularz w oszustwie wykorzystującym wizerunek PGNiG

WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

METODY DZIAŁANIA OSZUSTÓW

W niektórych przypadkach przestępcy zastosowali ankietę, która zbiera dane na temat ofiary. Często pojawiają się pytania o wiek, ogólną wiedzę o inwestowaniu, oczekiwany dochód, możliwości inwestycyjne oraz pytania mające na celu utwierdzenie ofiary w przekonaniu, że bierze udział w prawdziwej inwestycji. Zebrane w ten sposób informacje mogą posłużyć oszustom do obrania odpowiedniego scenariusza, dzięki któremu będą mogli w łatwiejszy sposób nakłonić osobę poszkodowaną do większej „inwestycji".



Przykładowa ankieta w oszustwie wykorzystującym wizerunek PGNiG

Po wprowadzeniu danych w formularzu następuje kontakt telefoniczny z osobą, która przedstawia się, jako opiekun projektu. Osoba ta jest bardzo dobrze przygotowana i często odpowiada na wszystkie zadawane pytania. Potrafi bardzo długo opowiadać o danym programie, oferuje swoją pomoc oraz dostosowuje dialog do wcześniej uzyskanych informacji. Dopóki nie zainwestujemy większej kwoty pieniędzy kontakt ze strony oszustów jest bardzo częsty. W późniejszej fazie preferują jednak kontakt przez komunikatory np. WhatsApp.

WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

PRZYKŁADOWY SCENARIUSZ ATAKU

1 Ofiara została nakłoniona do inwestycji w wysokości 500 zł.

2 W ciągu dwóch tygodni, na podstawionej stronie uzyskała ‚zysk" 800 zł.

3 Przestępcy pozwalają na wypłatę 300 zł z konta – na koncie ‚zostaje" 1000 zł.

4 W ciągu następnych tygodni występują wahania na koncie – w niektórych momentach ofiara widzi ‚stratę".

5 Kontakt ze strony opiekuna oraz informacja, że po wpłaceniu kolejnej kwoty 1000 zł uruchomi się specjalny program.

6 Wpłata spowodowała zysk do 6000 zł w ciągu 2 tygodni.

WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

PRZYKŁADOWY SCENARIUSZ ATAKU

7 Kolejny kontakt ze strony opiekuna – oferta specjalnej promocji i próba nakłonienia do większej inwestycji.

8 Kolejne tygodnie przynoszą wyświetlony na koncie ofiary ‚zysk" 90 000 zł.

9 Zgłoszenie chęci wypłaty pieniędzy. Pieniądze znikają z konta na fałszywej platformie inwestycyjnej, a ofiara informowana jest o wypłacie.

10 Kontakt ze strony opiekuna i informacja o konieczności opłacenia podatku oraz prowizji w wysokości 20 000zł, które są wymagane do wypłaty pieniędzy.

11 Próby wyłudzenia pieniędzy poprzez informacje o kolejnych dopłatach, karach lub podatkach.

12 Po kategorycznej odmowie wpłaty kolejnych pieniędzy przez ofiarę następuje urwanie kontaktu przez oszustów.

WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

SCHEMAT OSZUSTWA

W czasie trwania całego procesu oszukańczego, „opiekun", poprzez częste kontakty zyskuje zaufanie poszkodowanego. W przypadku wystąpienia problemu z wpłatą pieniędzy, proponuje swoją pomoc poprzez aplikację zdalnego kontrolowania pulpitu np. AnyDesk. Kiedy uzyska zgodę, informacje wyświetlane na monitorze wykorzystuje do udoskonalenia swoich technik. Dzięki temu może np. zobaczyć kwotę na koncie ofiary i zna jej możliwości „inwestowania". Informacje uzyskane w ten sposób wykorzystuje przy kolejnych kontaktach, gdzie informuje o „promocjach" lub „karach".

Przedstawiony schemat ataku jest przykładowy, każdy może wyglądać w odmienny sposób. Zależy to przede wszystkim od chęci potencjalnej ofiary do inwestycji oraz jej naiwności. Oszuści dostosowują swoje techniki działania do profilu zainteresowanego. Może to być długie i mozolne nakłanianie ofiary do wpłaty małej ilości środków, a następnie próba uzależnienia jej od danej inwestycji przy pomocy platformy lub kilkukrotne duże wpłaty, a następnie urwanie kontaktu.

W przypadku uzyskania przez oszusta dużego zaufania ofiary, zachęca on do instalacji aplikacji „pomocy", czyli aplikacji do zdalnego zarządzania pulpitem jak Anydesk lub TeamViewer. Następnie przy ich pomocy następuje namówienie ofiary do zalogowania na swoje konto bankowe, a następnie bezpośrednia próba wypłacenia wszystkich pieniędzy i pozostawienie poszkodowanego bez środków finansowych.

BEZPIECZEŃSTWO

Statystyki pokazują, że oszustwa inwestycyjne stanowią jeden z poważniejszych problemów, z jakimi mierzą się osoby korzystające z usług oferowanych na rynku finansowym.
Działania cyberprzestępców przybierają coraz to nowe, zmodyfikowane formy, aby skutecznie wpłynąć na zachowania użytkowników.

Jak nie dać się oszukać?

1

Ostrożność przede wszystkim!

Wszelkiego typu reklamy oferujące szybki zysk w krótkim czasie powinny wzbudzić niepokój.

2

Oprogramowanie tylko z zaufanych źródeł.

Należy pamiętać o tym, aby nigdy nie instalować aplikacji z niezaufanych źródeł tj. spoza oficjalnych sklepów sugerowanych przez producenta.

3

Śledzenie listy ostrzeżeń.

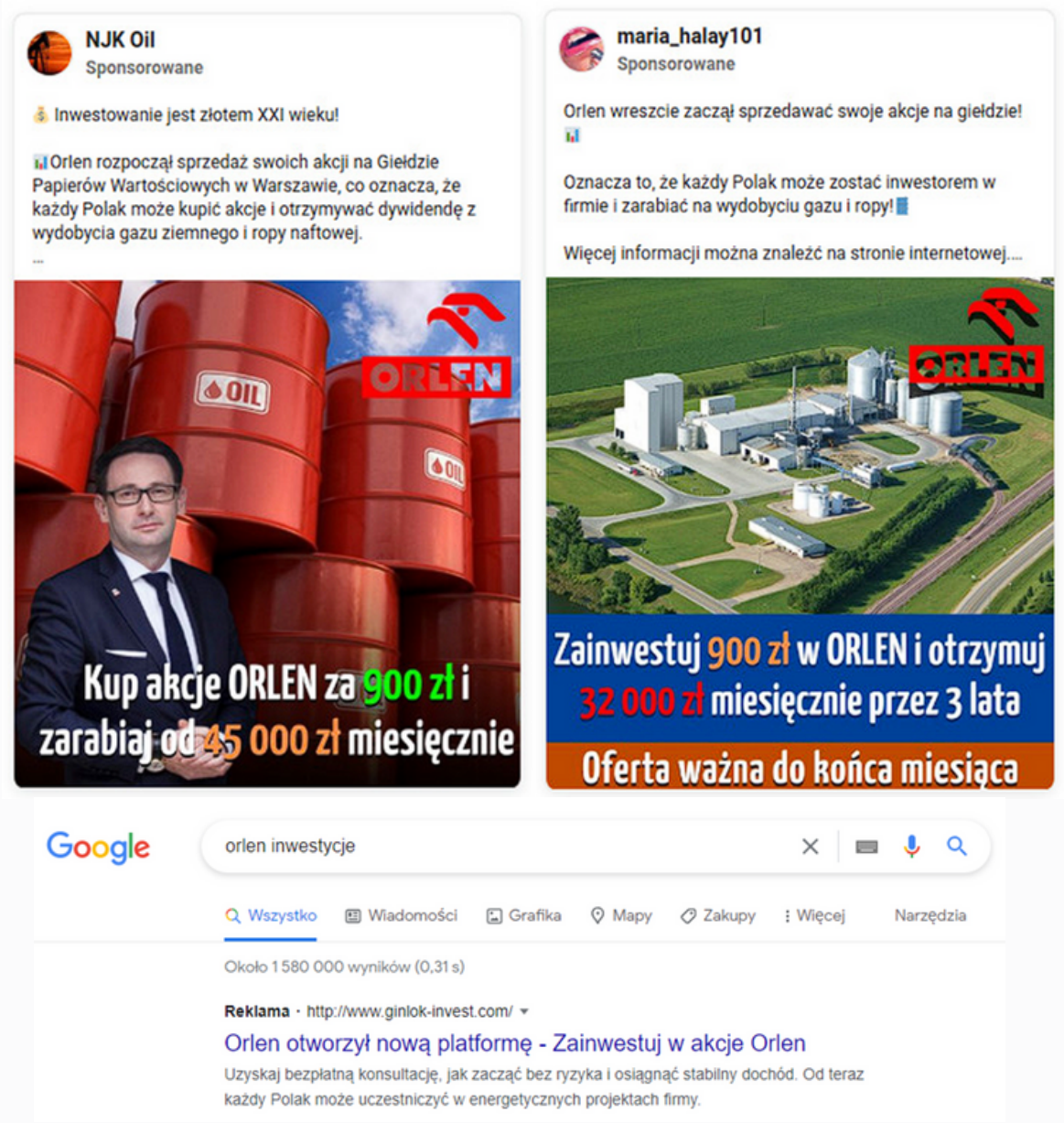
Dobrą praktyką jest sprawdzanie listy ostrzeżeń, dostępnej na stronie internetowej Komisji Nadzoru Finansowego. Weryfikacja podmiotów, które się na niej znajdują może uchronić przed tego typu oszustwami.

LISTA OSTRZEŻEŃ PUBLICZNYCH KNF:
HTTPS://WWW.KNF.GOV.PL/DLA_KONSUMENTA/OSTRZEZENIA_PUBLICZNE

WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

ORLEN

Ponad 72% reklam posługuje się wizerunkiem firmy Orlen. W reklamach bardzo często wykorzystywany jest wizerunek pracowników, prezesa spółki, często w połączeniu z politykami oraz celebrytami. Reklamy umieszczane są najczęściej na platformie Facebook, oraz sporadycznie w wyszukiwarce Google.

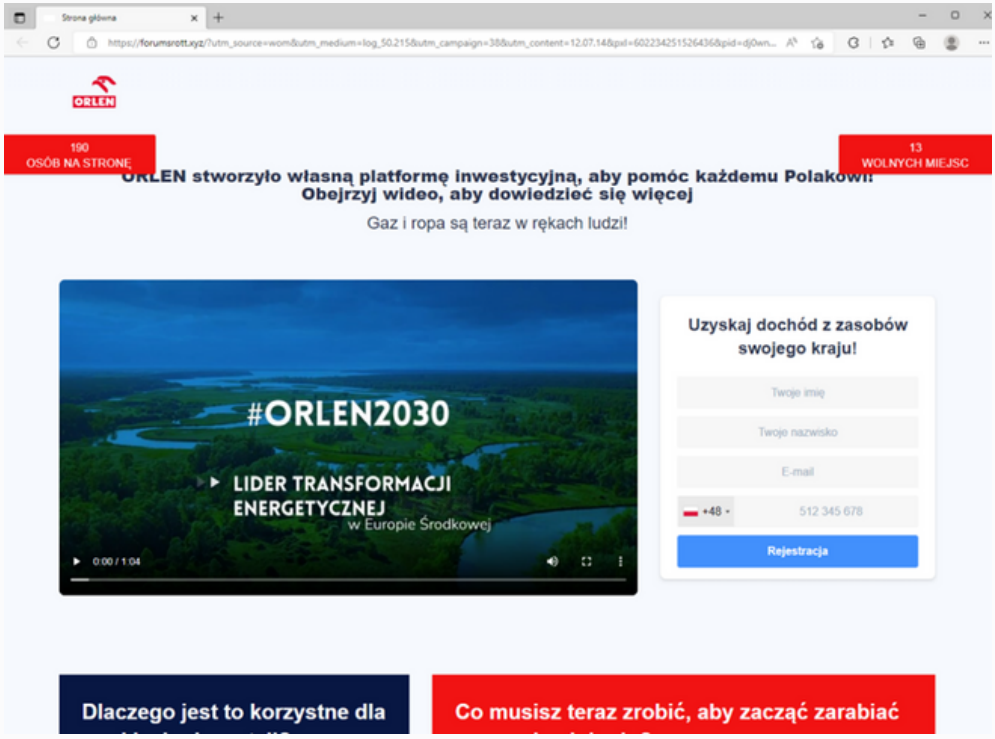


Przykładowe reklamy umieszczone w Google oraz na platformie Facebook.

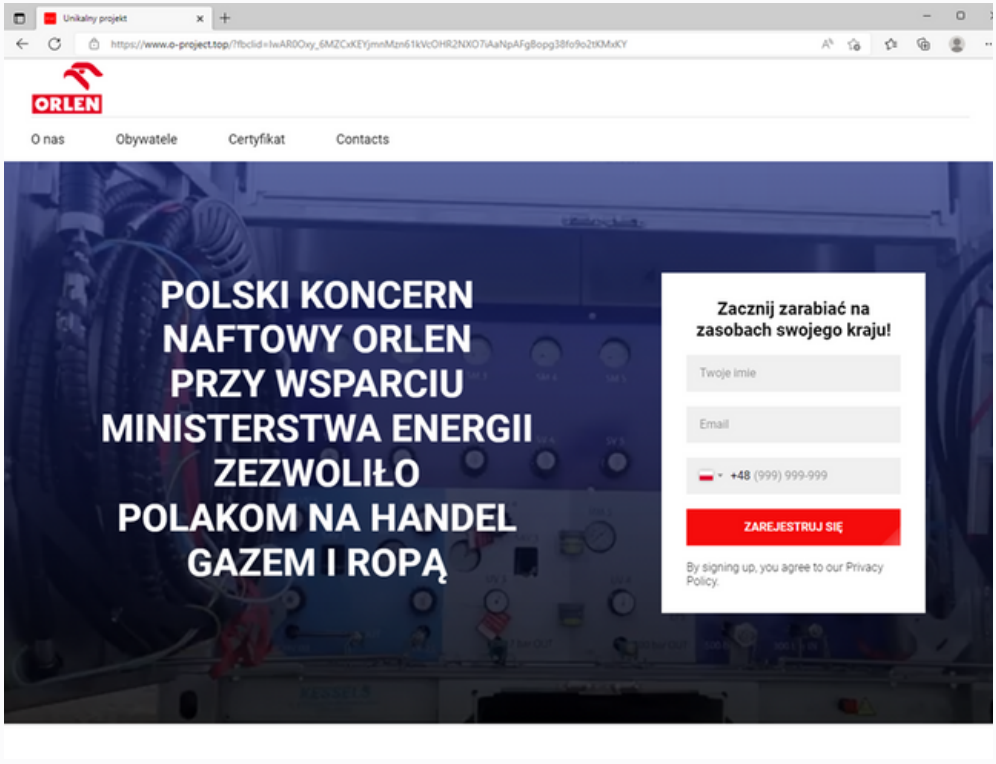
WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

ORLEN

Wygląd fałszywej strony:



Strony od czasu do czasu są modyfikowane, poniżej wyświetlony jest inny wariant witryny.



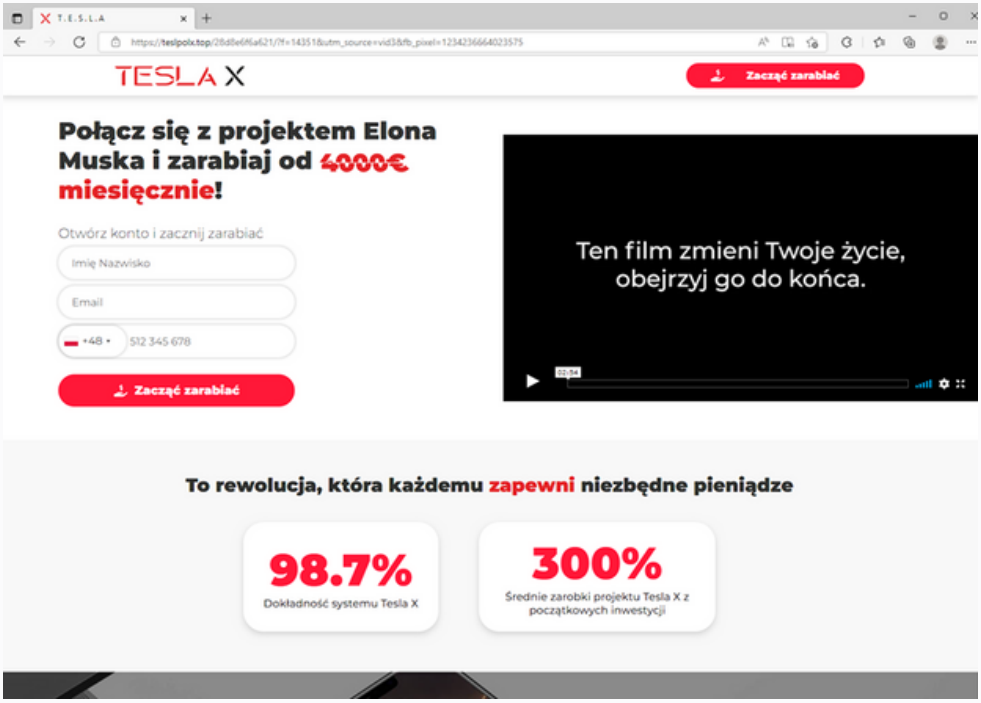
WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

TESLA

Tesla, Inc. – Amerykańskie przedsiębiorstwo zajmujące się produkcją samochodów elektrycznych. Wizerunek firmy Tesla oraz Elona Muska był wykorzystywany w około 15% reklam. Bardzo często zawierają one filmy, w których podstawione osoby opowiadają o tym jak wzbogaciły się przy pomocy specjalnego programu otwartego przez daną firmę.

Przykłady Reklam:

Przykład strony:



WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

POZOSTAŁE SPÓŁKI SKARBU PAŃSTWA

Oszuści wykorzystują również logo i nazwy firm, których udziałowcem jest Skarb Państwa. Oferują one możliwości szybkiego zysku poprzez inwestycję w złoto, paliwo lub akcje spółek państwowych. Poniżej lista wykorzystanych wizerunków oraz przykładowe reklamy.

1. KGHM

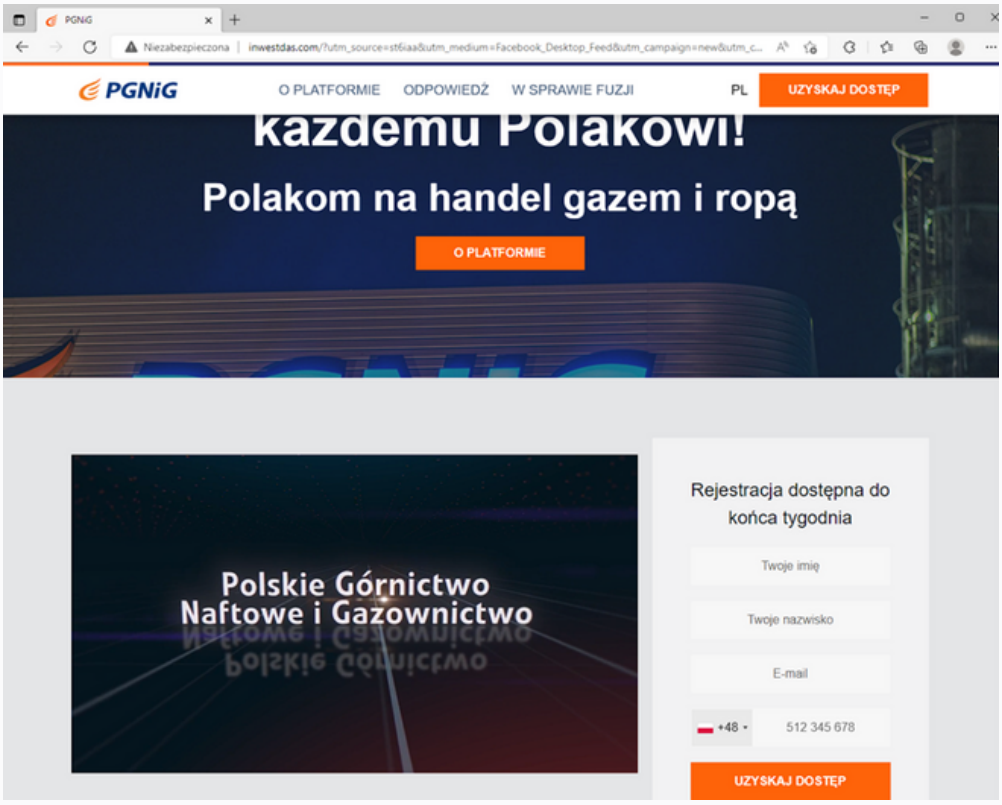
Przykład strony:

WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

POZOSTAŁE SPÓŁKI SKARBU PAŃSTWA

2. PGNiG

Przykładowa strona:



WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

POZOSTAŁE SPÓŁKI SKARBU PAŃSTWA

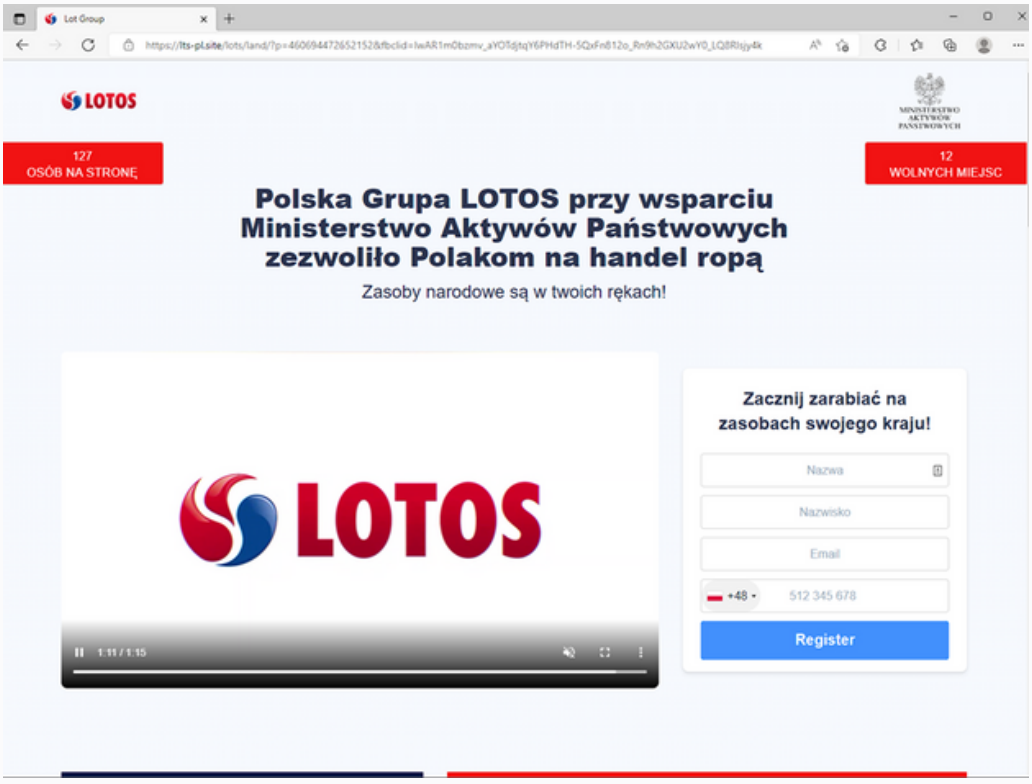
3. PGE

Przykładowa strona:

POZOSTAŁE SPÓŁKI SKARBU PAŃSTWA

4. Lotos

Przykładowa strona:

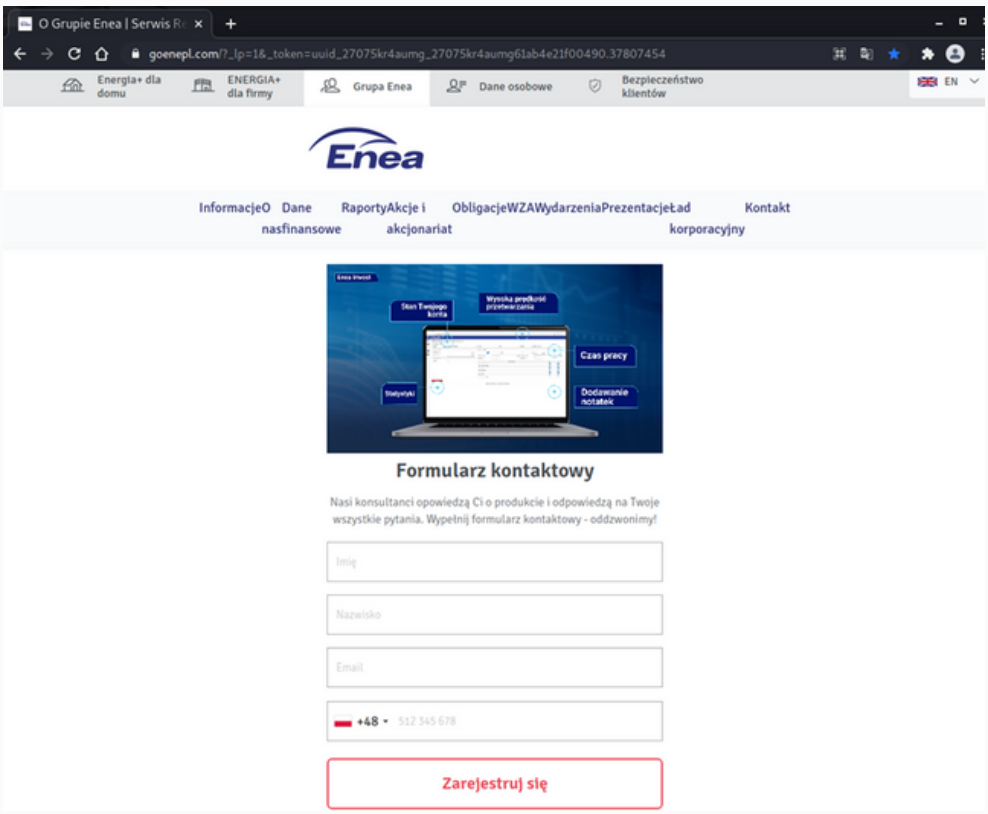


WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

POZOSTAŁE SPÓŁKI SKARBU PAŃSTWA

5. Enea

Przykładowa strona:



POZOSTAŁE SPÓŁKI SKARBU PAŃSTWA

6. Powszechny Zakład Ubezpieczeń

Przykładowa strona:

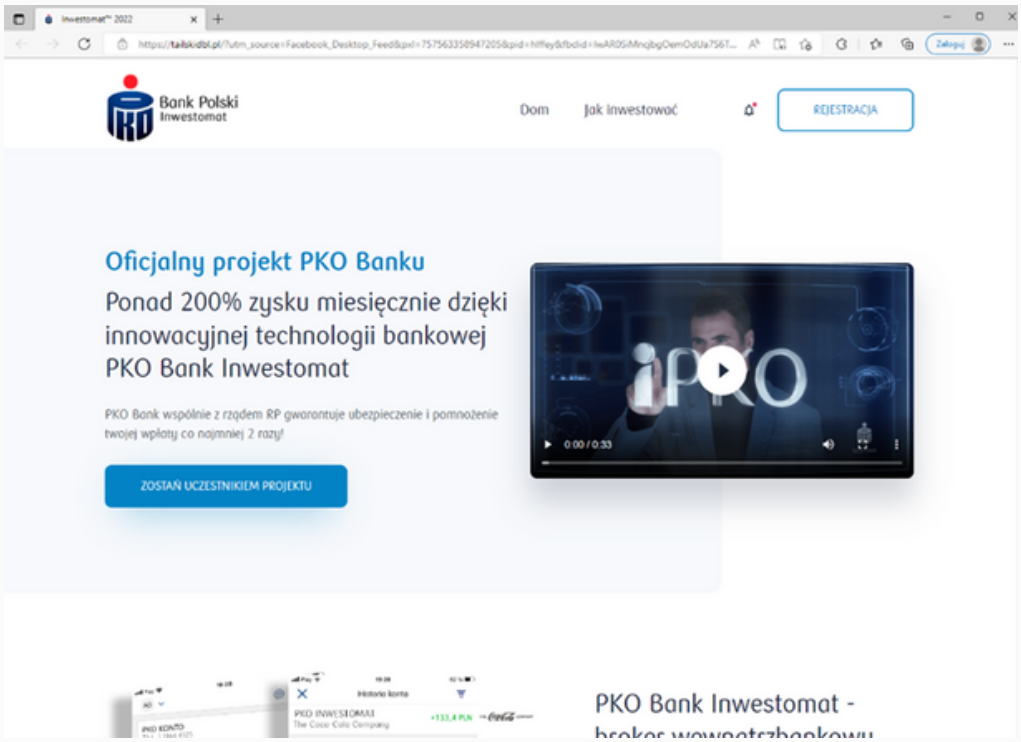
WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

BANKOWE

Wizerunki banków są coraz częściej wykorzystywane do promowania fałszywych inwestycji. Oszuści często promują swoje strony poprzez zamieszczanie informacji, iż dany bank uruchomił platformę inwestycyjną, która zapewnia zyski w krótkim czasie. Poniżej prezentujemy zidentyfikowane przez nas kampanie.

1. PKO BP / Inwestomat

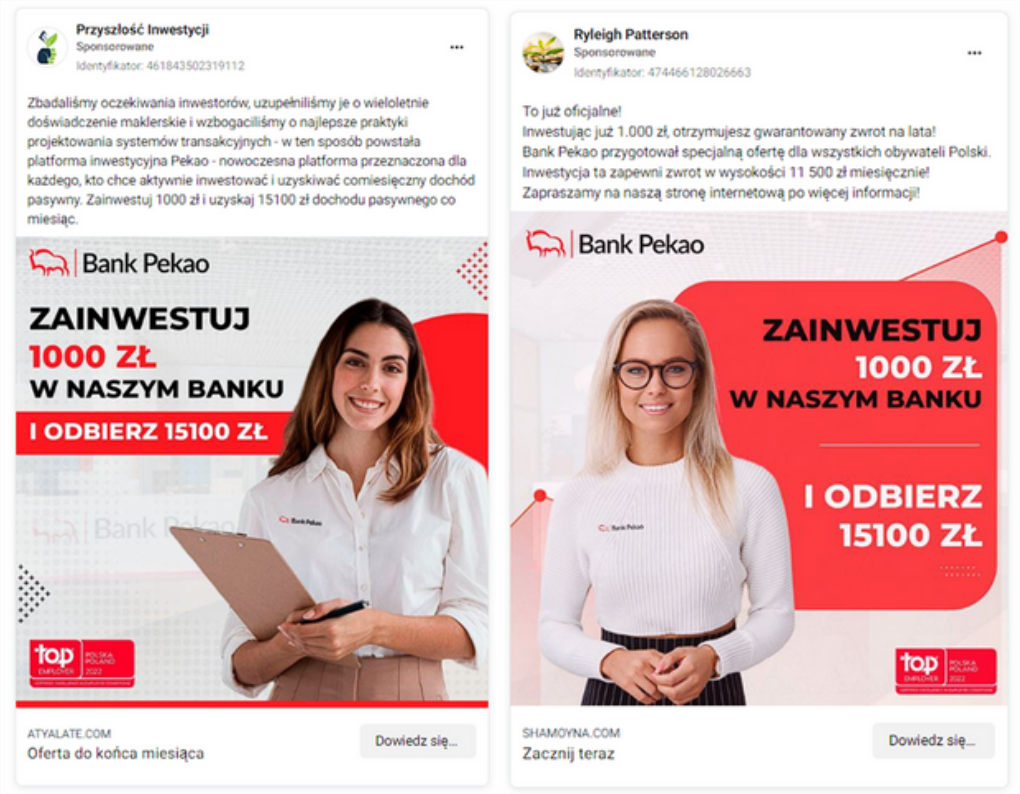
Przykładowa strona:



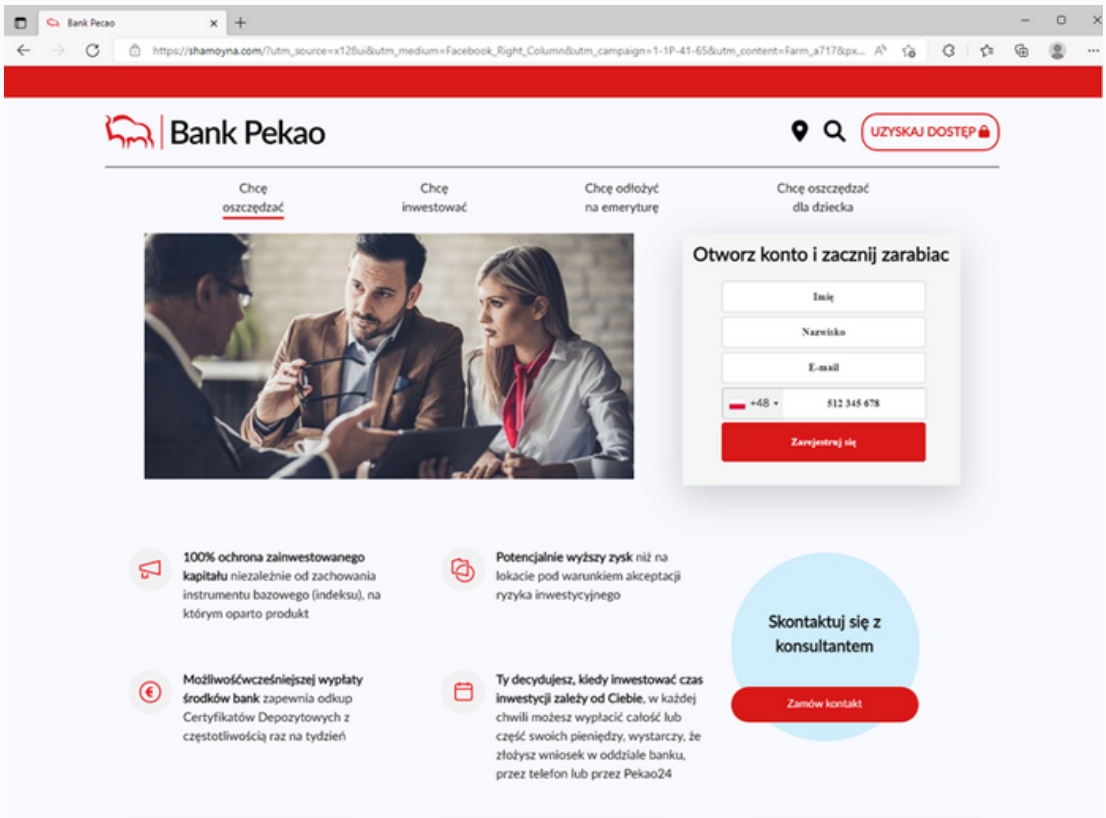
WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

BANKOWE

2. Pekao



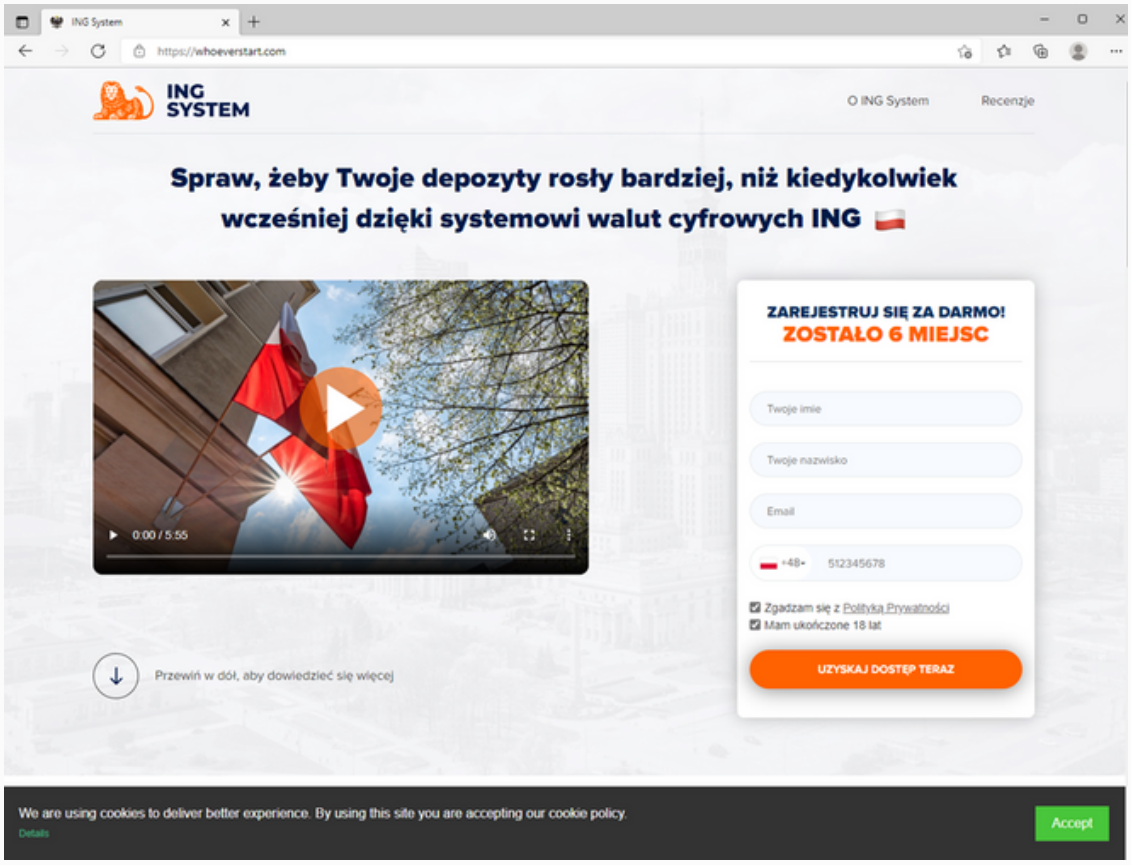
Przykładowa strona:



BANKOWE

3. ING

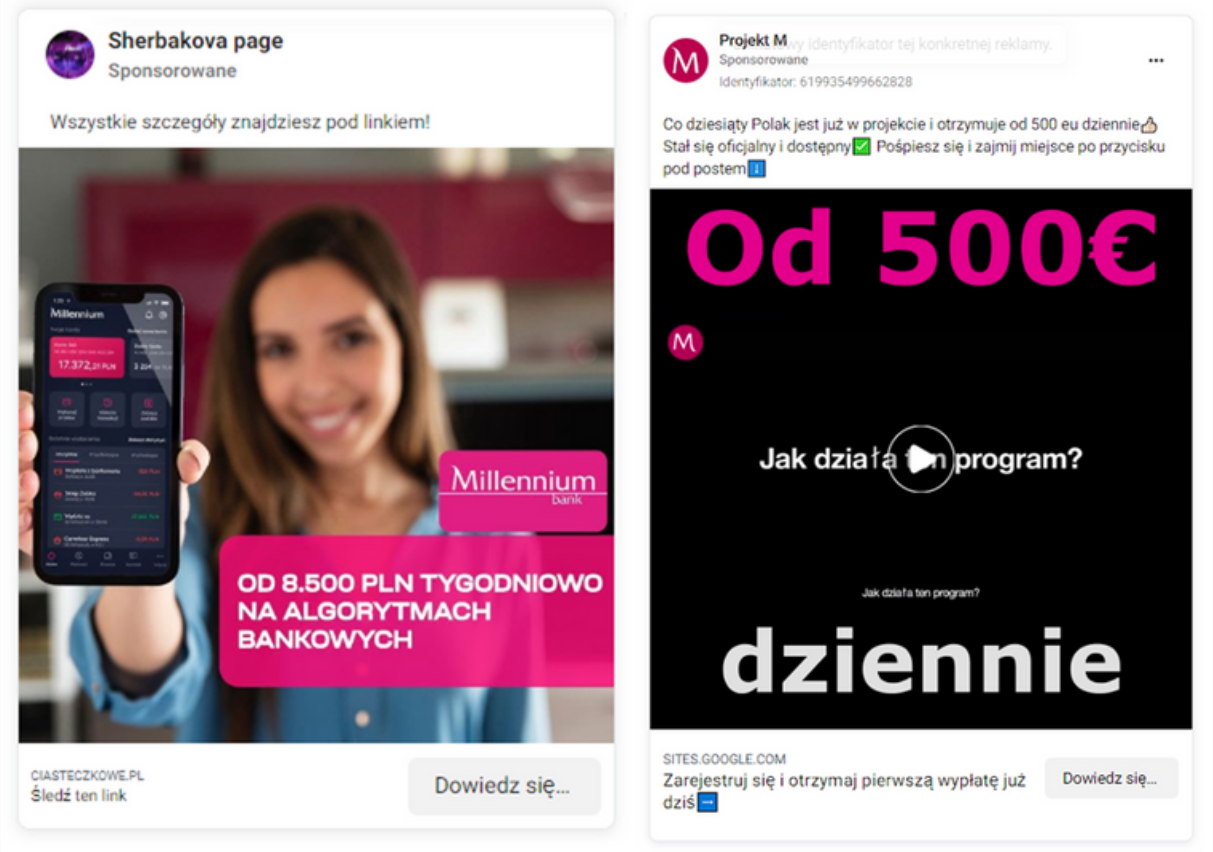
Przykładowa strona:



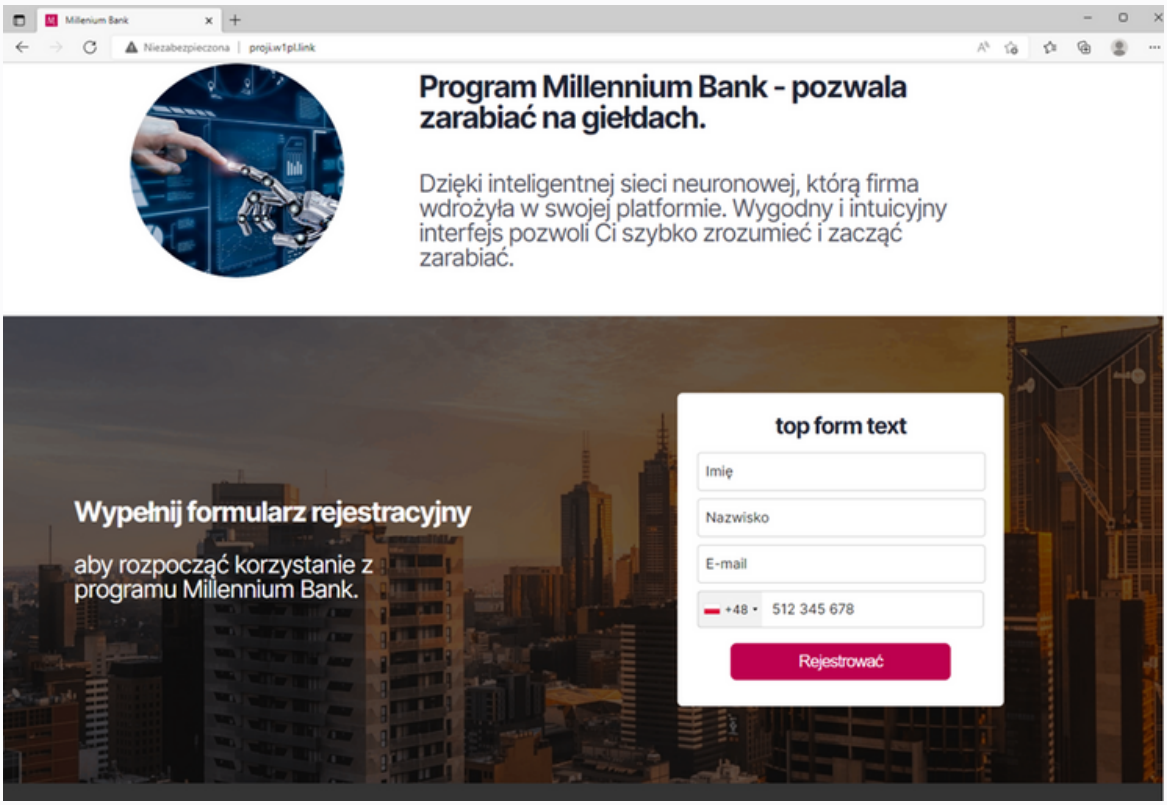
WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

BANKOWE

4. Millennium



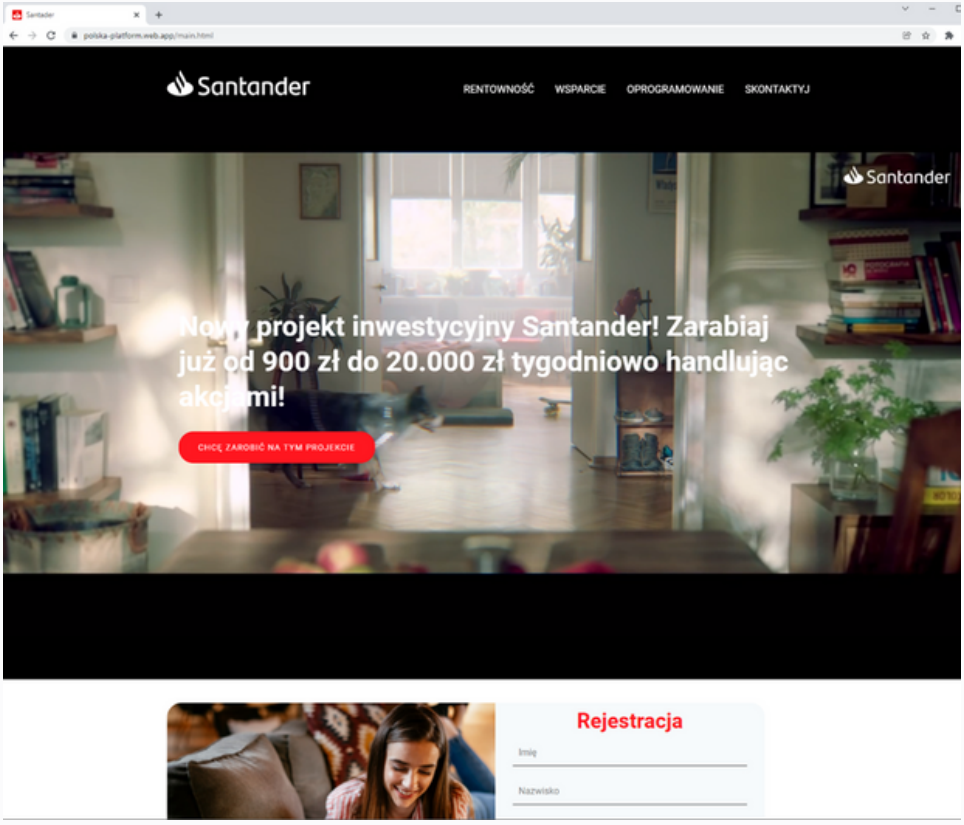
Przykładowa strona:



BANKOWE

5. Santander

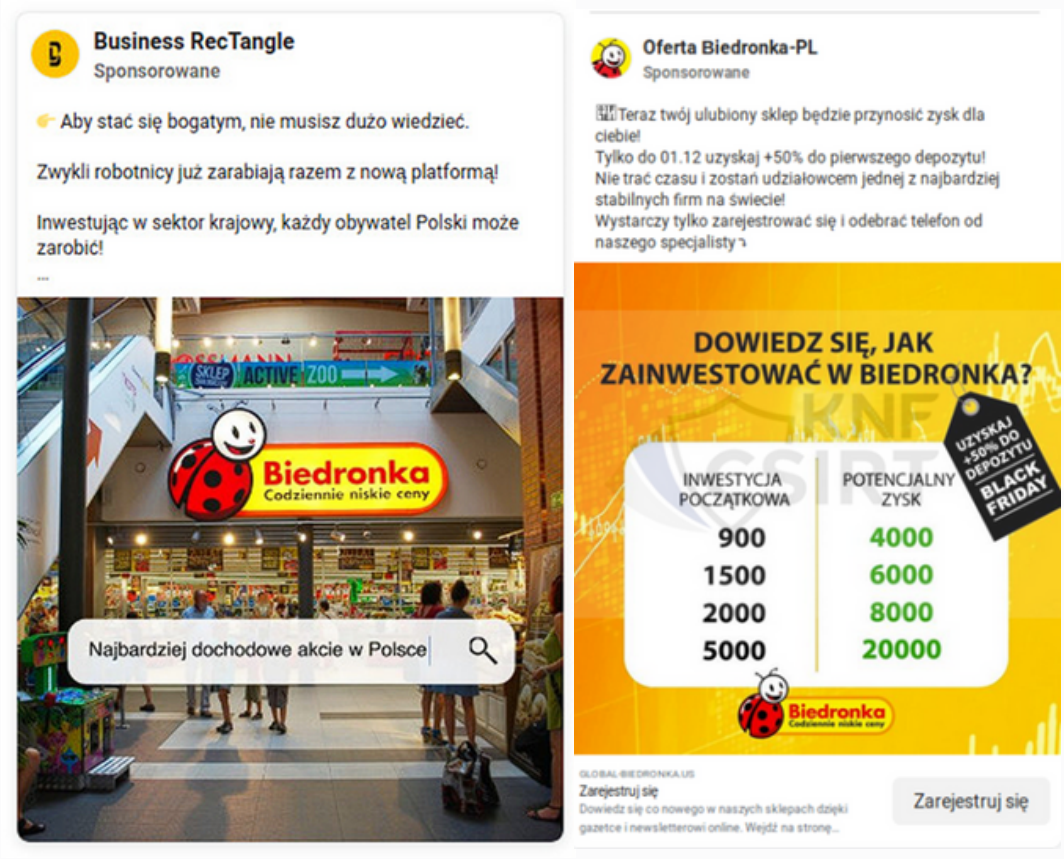
Przykładowa strona:



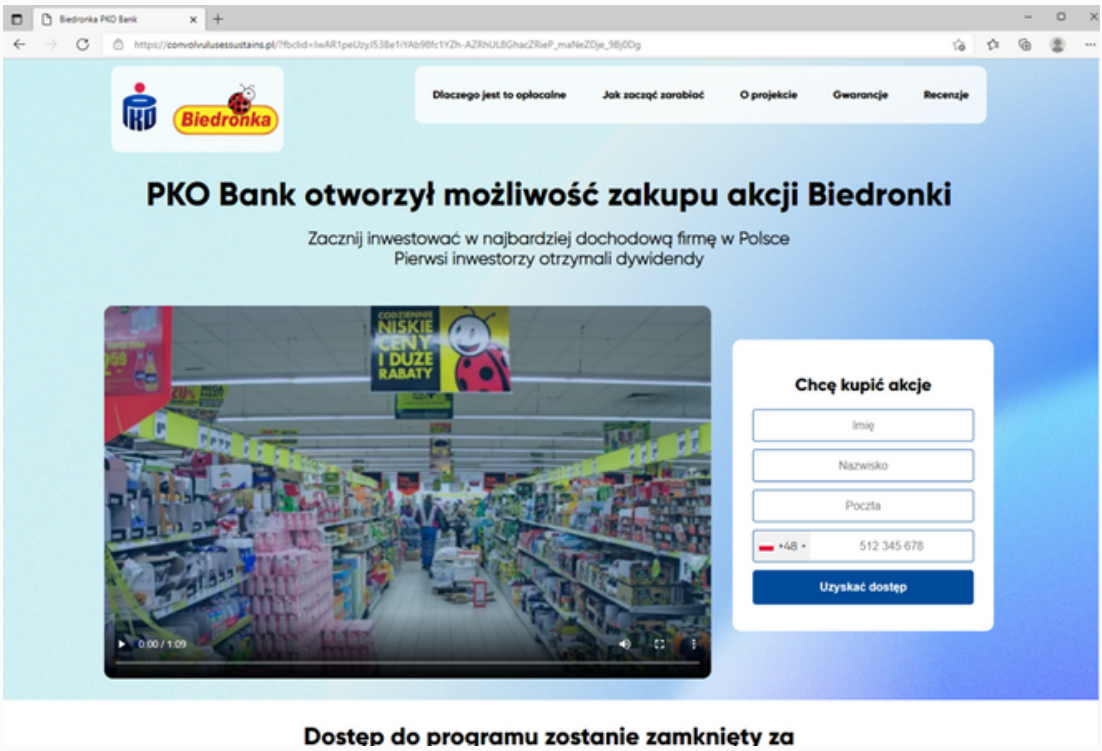
WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

BANKOWE

6. PKO BP/ Biedronka

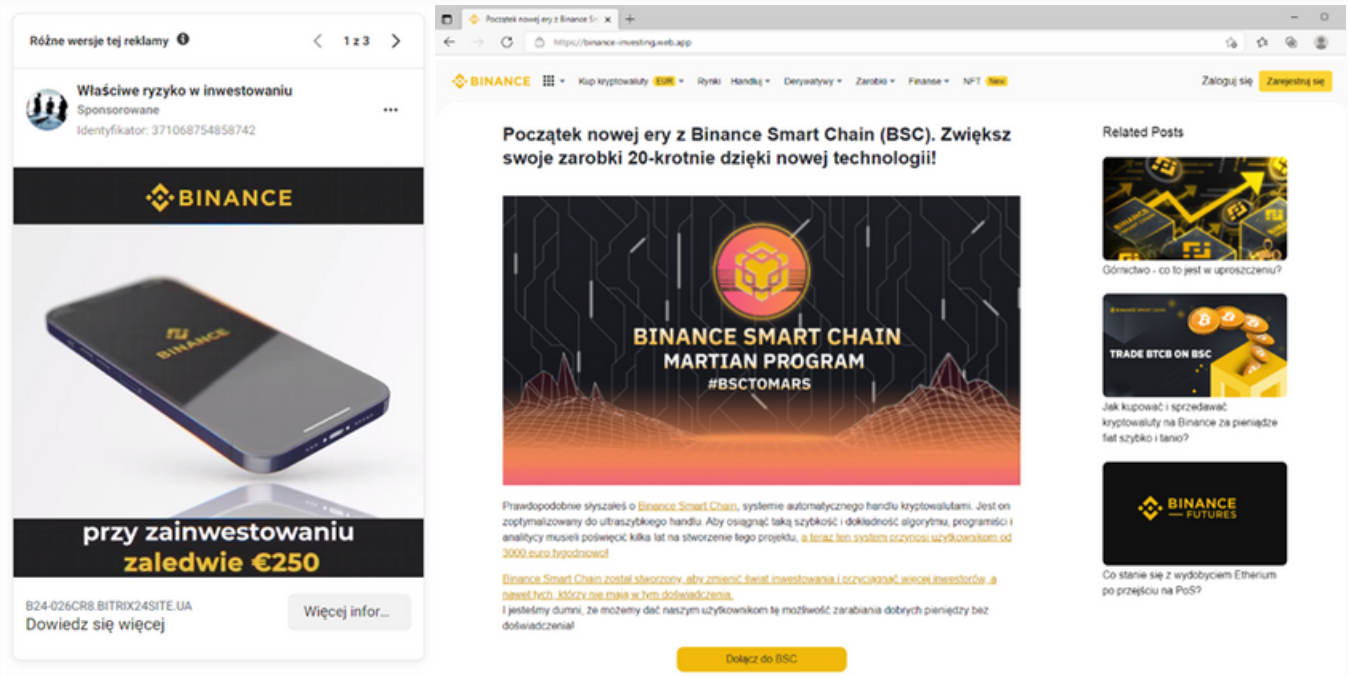


Przykładowa strona:

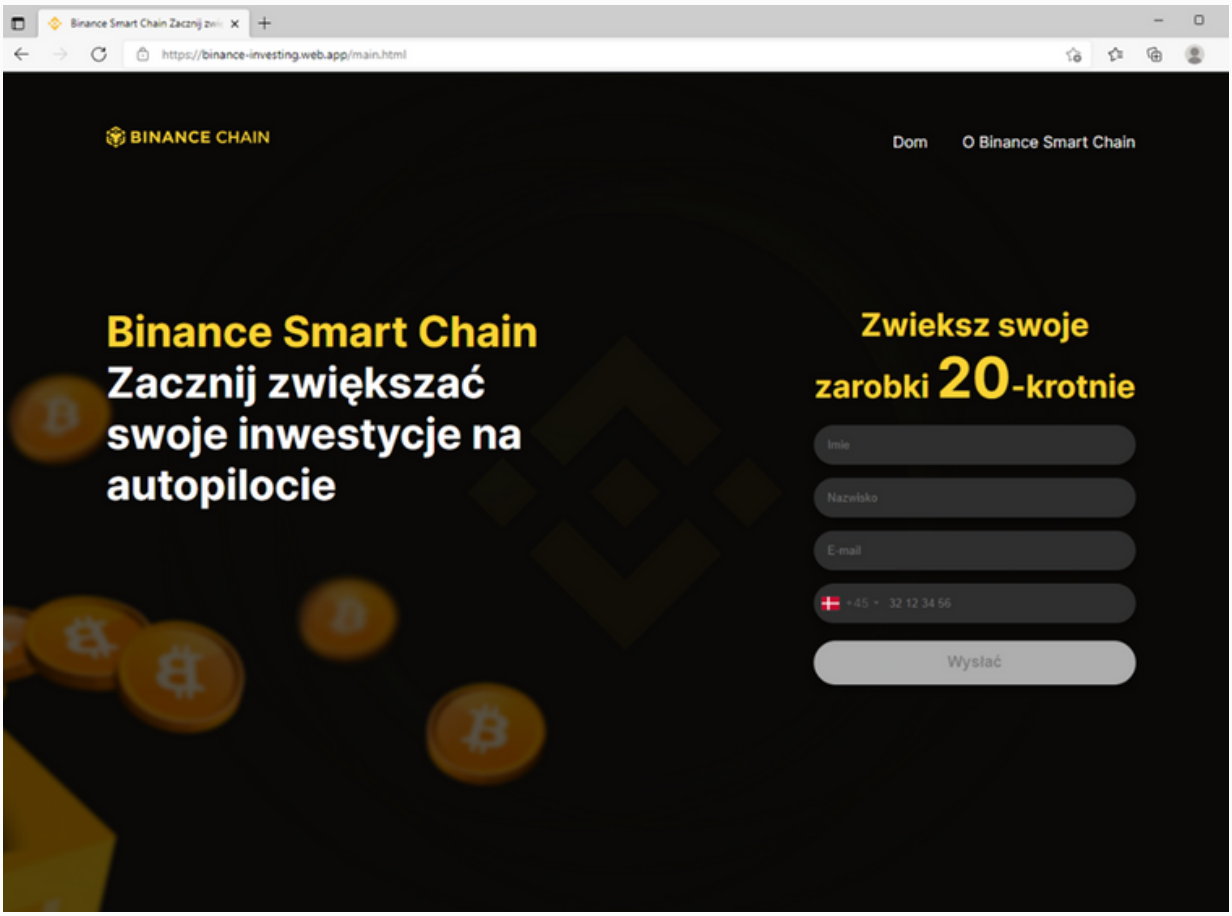


KRYPTOWALUTY

1. Biance



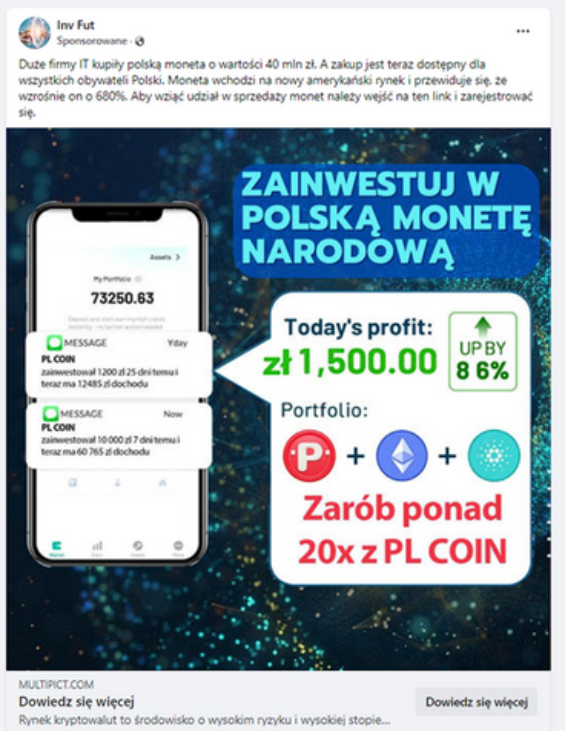
Przykładowa strona:



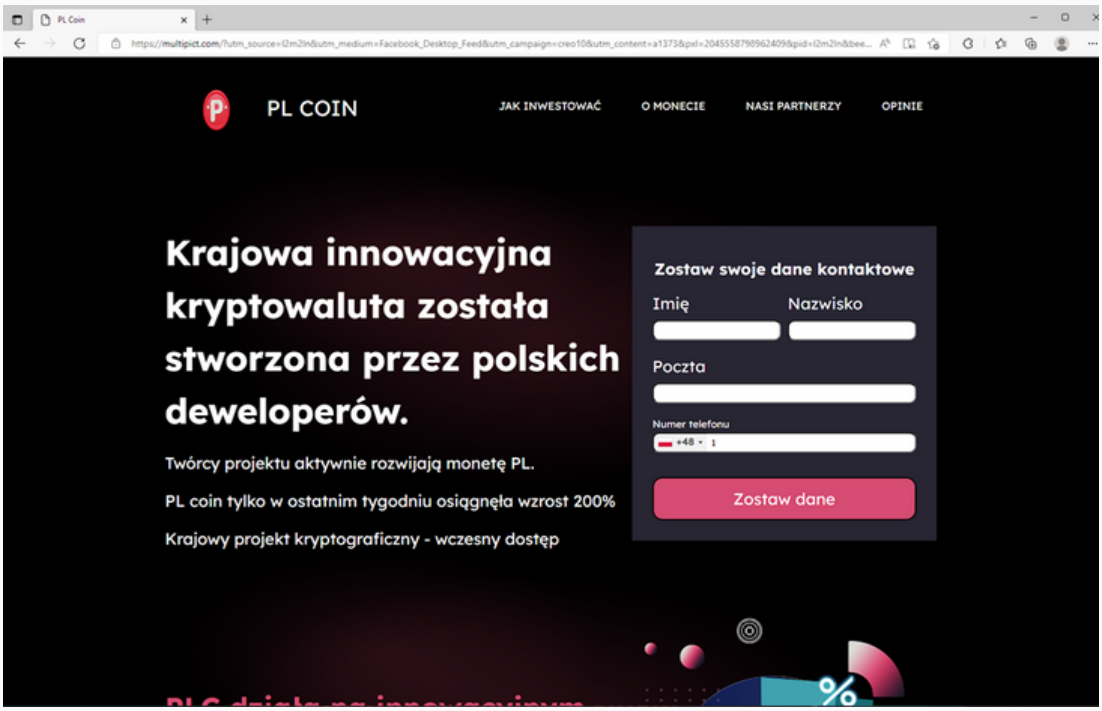
WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

KRYPTOWALUTY

2. PlnCoin



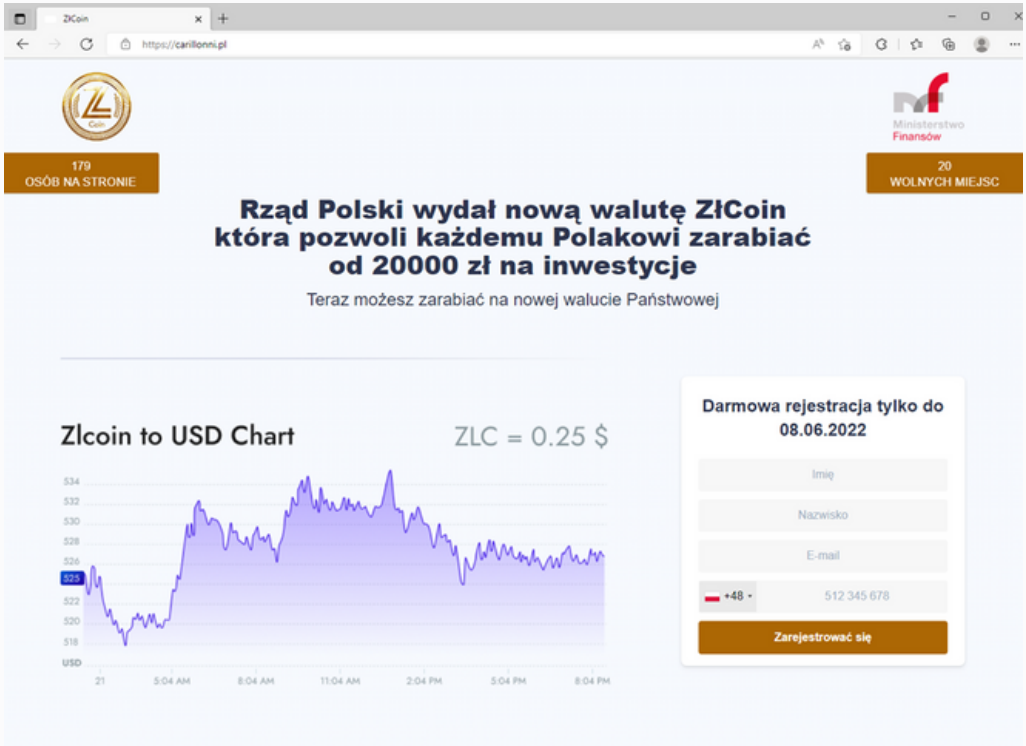
Przykładowa strona:



KRYPTOWALUTY

3. ZłCoin

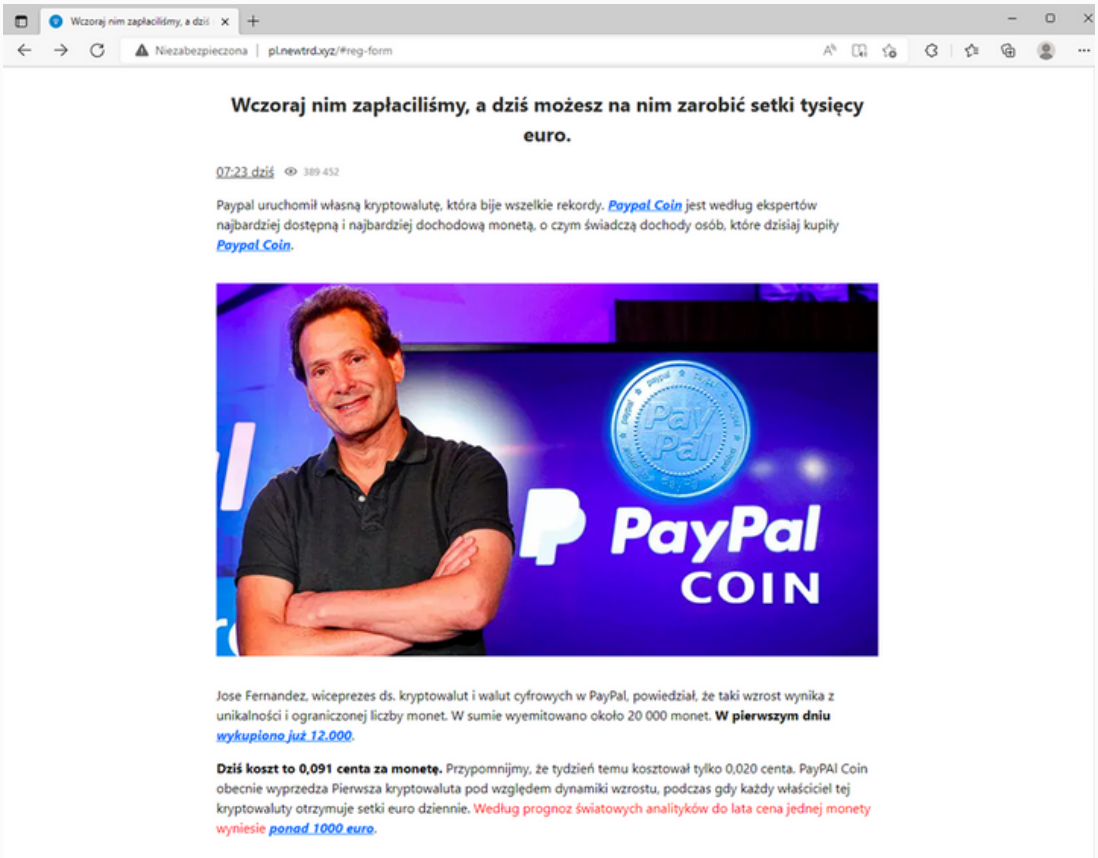
Przykładowa strona:



KRYPTOWALUTY

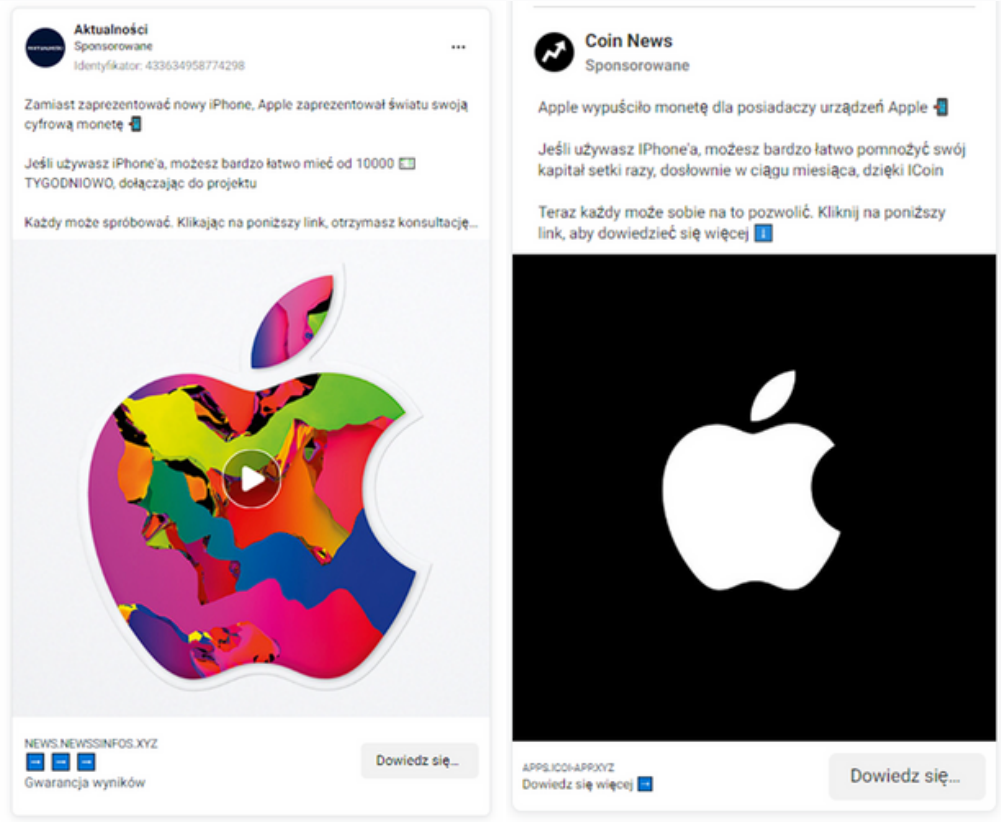
4. PayPal Coin

Przykładowa strona:

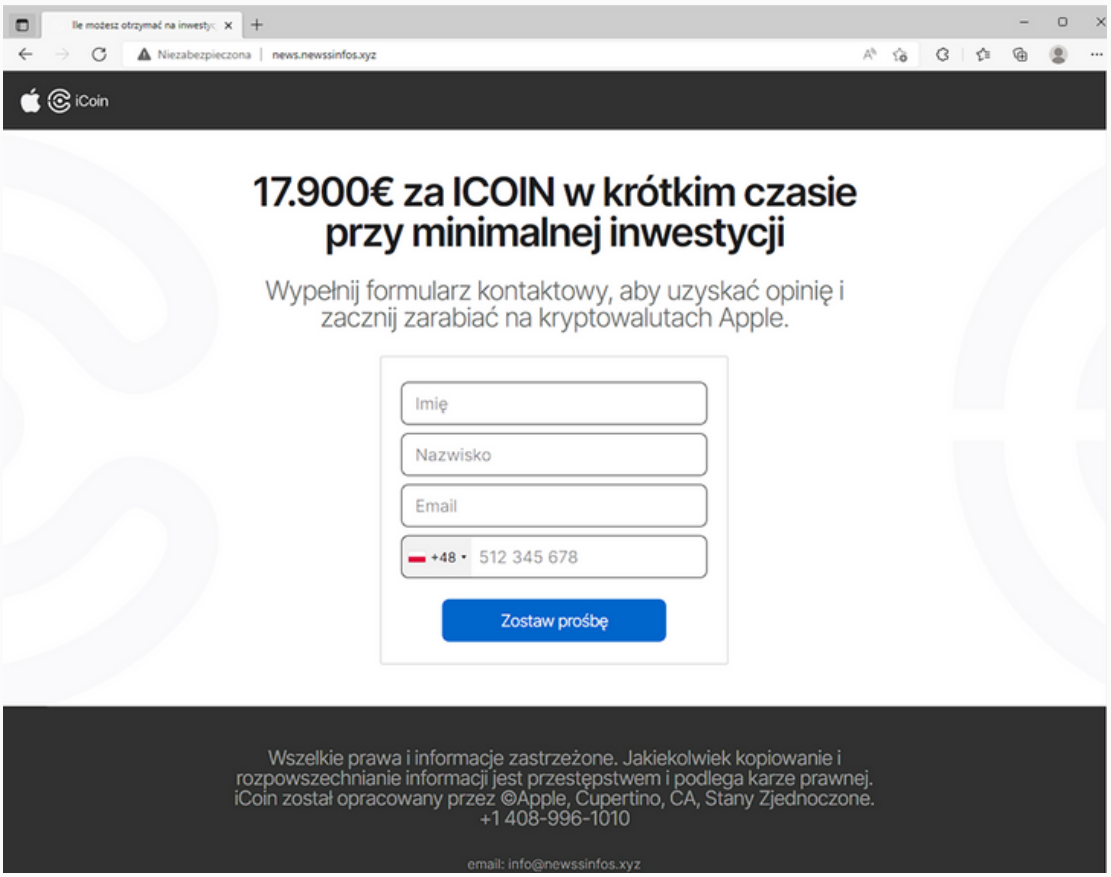


KRYPTOWALUTY

5. Apple Coin



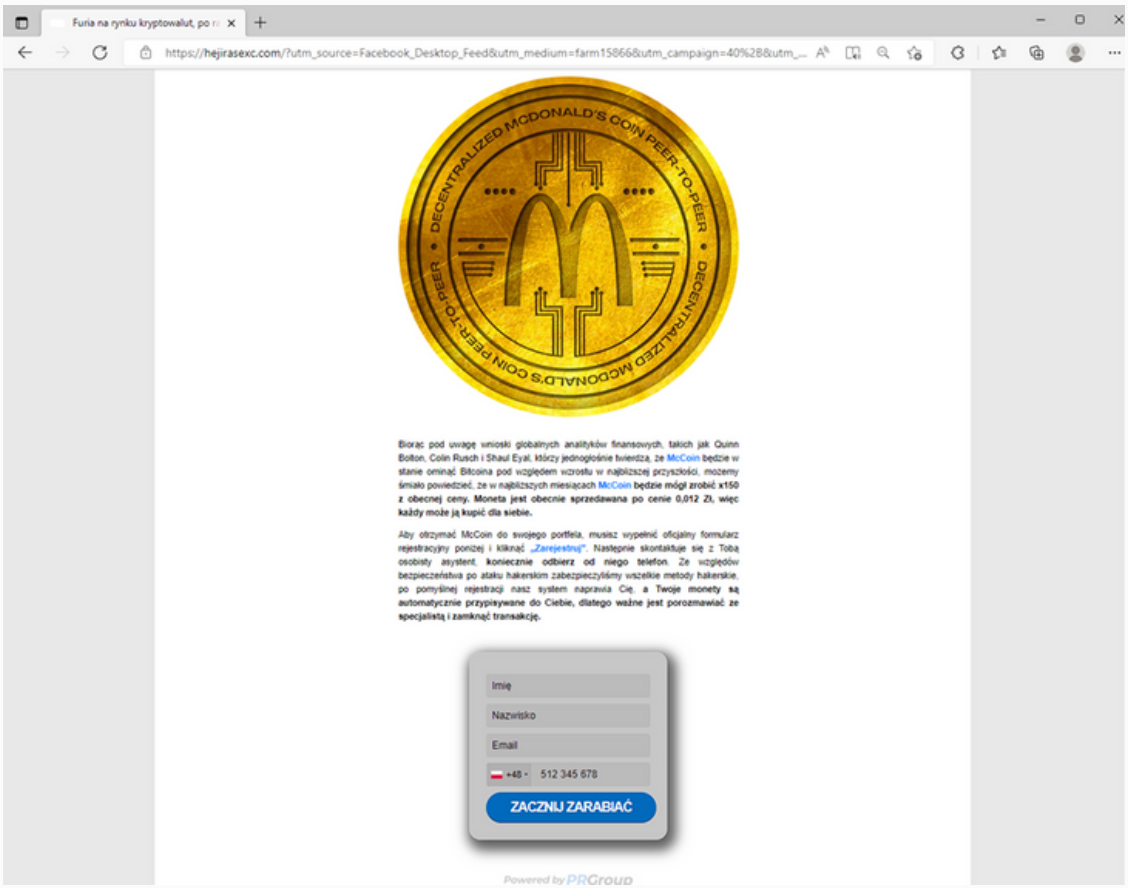
Przykładowa strona:



KRYPTOWALUTY

6. McDonald Coin

Przykładowa strona:



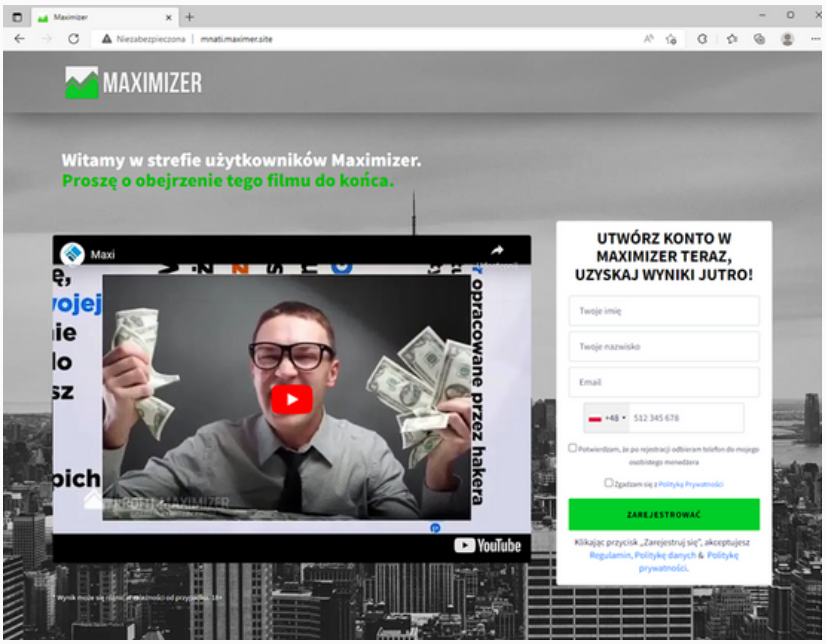
WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

INNE

Poniżej prezentujemy kilka wybranych firm, których wizerunki były wykorzystane do oszustwa na fałszywe inwestycje. Zaobserwowano trend wskazujący, że przestępcy często tworzą własne „marki", które mogą przyciągać uwagę potencjalnej ofiary. Spowodowane jest to próbą uniknięcia blokady za podszycie się pod istniejący podmiot. Cyberprzestępcy wykorzystują również wizerunki firm z różnych dziedzin technologicznych.

1.Maxmizer

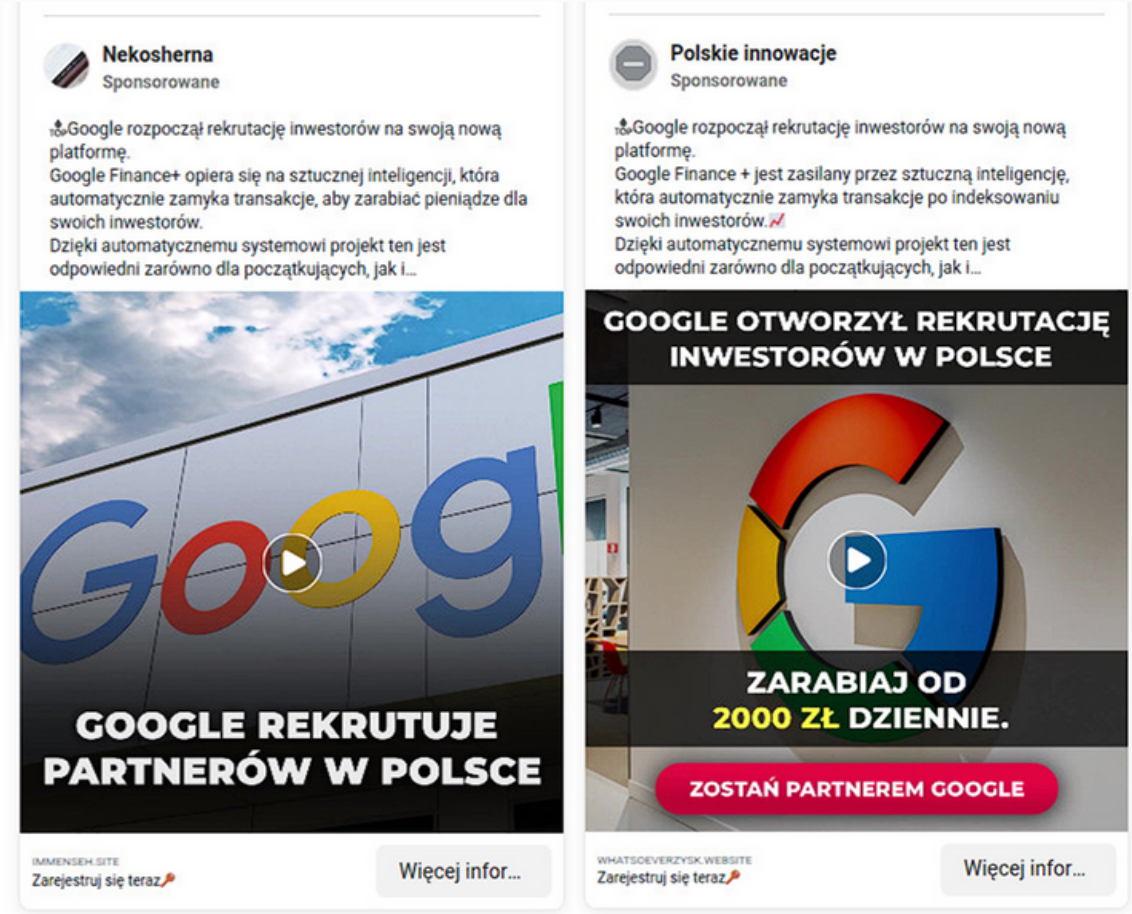
Przykładowa strona:



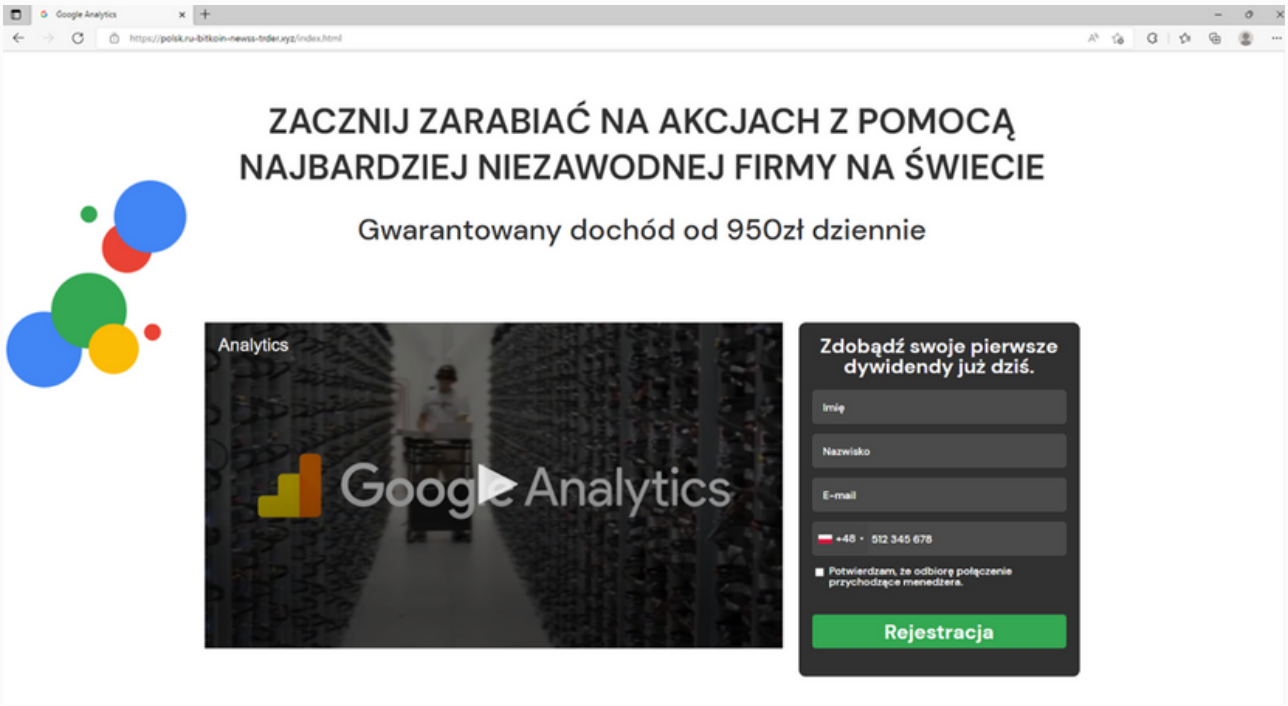
WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

INNE

2. Google



Przykładowa strona:

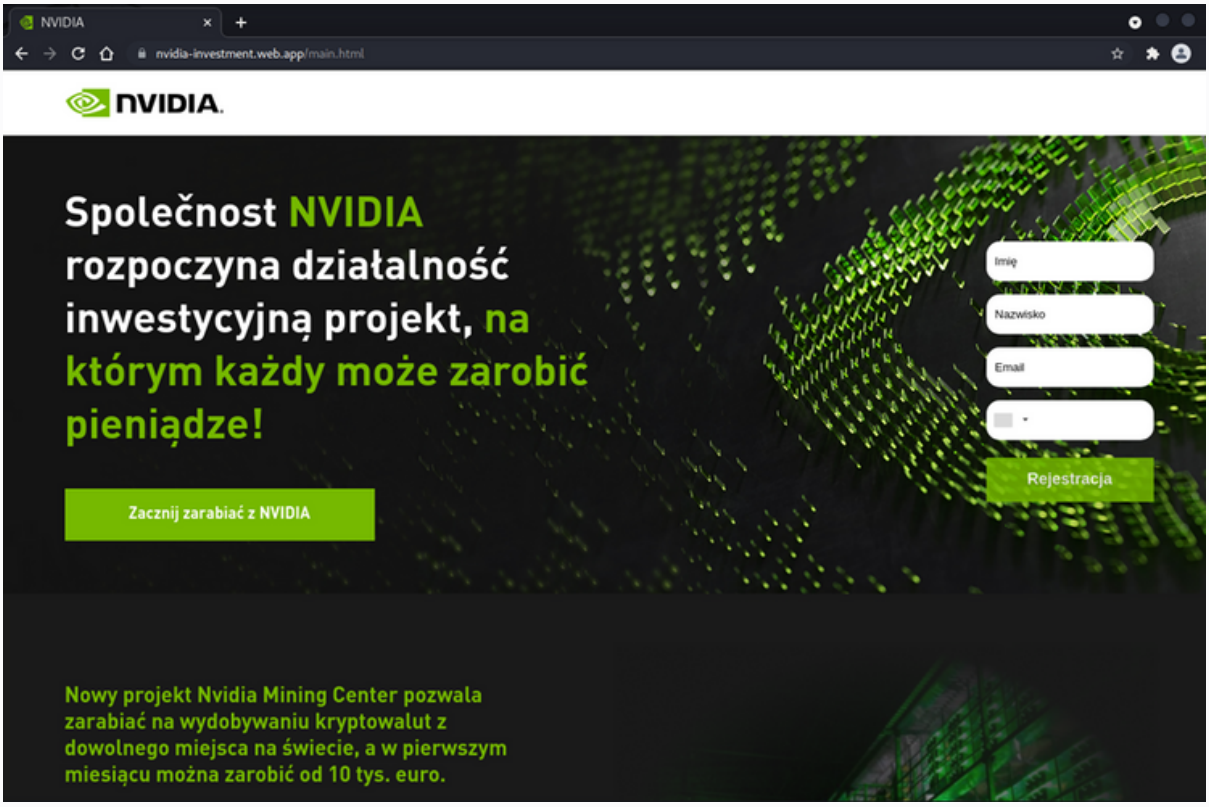


WIĘCEJ OSTRZEŻEŃ: HTTPS://TWITTER.COM/CSIRT_KNF

INNE

3. Nivida

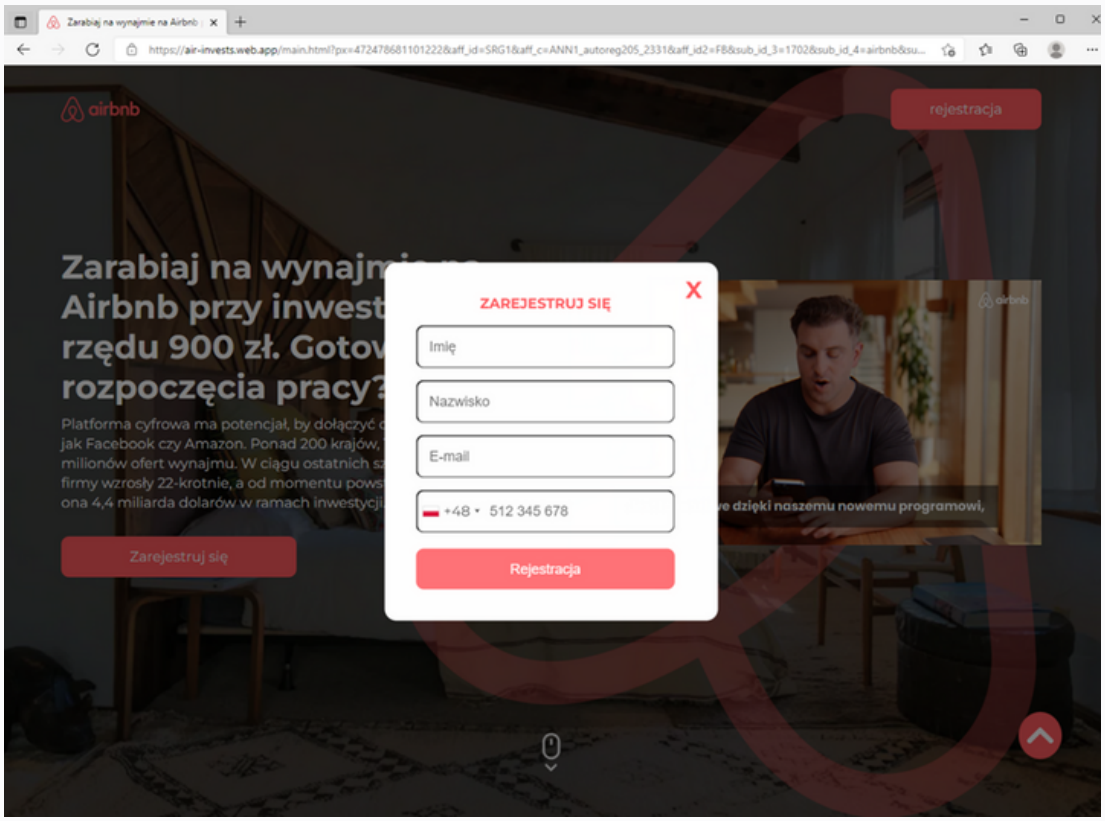
Przykładowa strona:



INNE

4. Airbnb

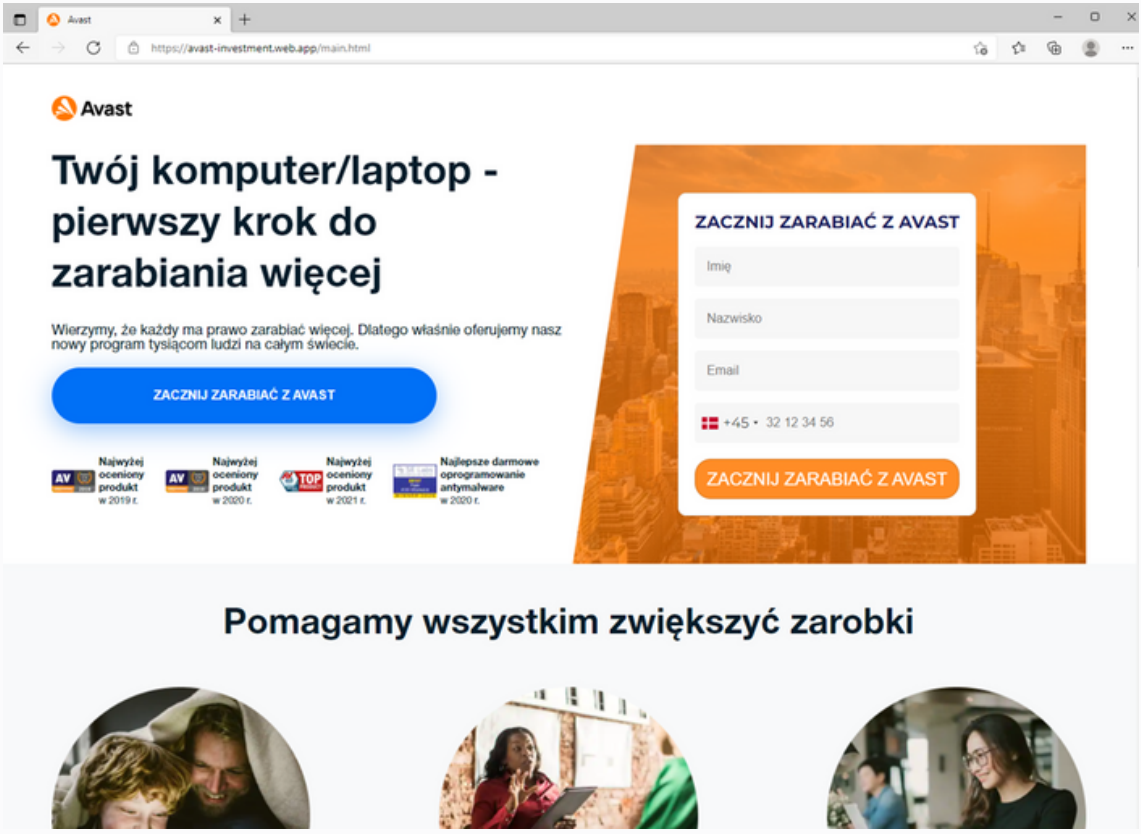
Przykładowa strona:



INNE

5. Avast

Przykładowa strona:



PODSUMOWANIE

Lista prezentowanych podmiotów jest wybiórcza, w każdym kolejnym miesiącu przestępcy wykorzystują wizerunek kolejnych instytucji bankowych, spółek państwowych lub firm. O nowych sposobach działania oszustów inwestycyjnych i nie tylko, informujemy za pośrednictwem mediów społecznościowych, zachęcamy do obserwowania naszego konta Twitter, LinkedIn oraz Facebooka.