KNF CSIRT

CYBERZAGROŻENIA W SEKTORZE FINANSOWYM

2022

Spis treści

TREŚCI

01.

Wstęp (str. 3)

02.

Statystyki z działalności CSIRT KNF (str. 4-8)

03.

Wybrane kampanie oszustów w 2022 roku (str. 9-29)

04.

Złośliwe oprogramowanie (str. 30- 47)

05.

Zagrożenia i rekomendacje odnośnie do ataków DDoS oraz działania haktywistów pod kątem wojny w Ukrainie (str. 48- 57)

Spis treści

TREŚCI

06.

Działania edukacyjne
CSIRT KNF w 2022 roku
(str. 58-67)

07.

Najważniejsze podatności
w 2022 roku
(str. 68-70)

08.

Cyberbezpieczeństwo 2022
z różnych perspektyw
(str. 71 - 77)

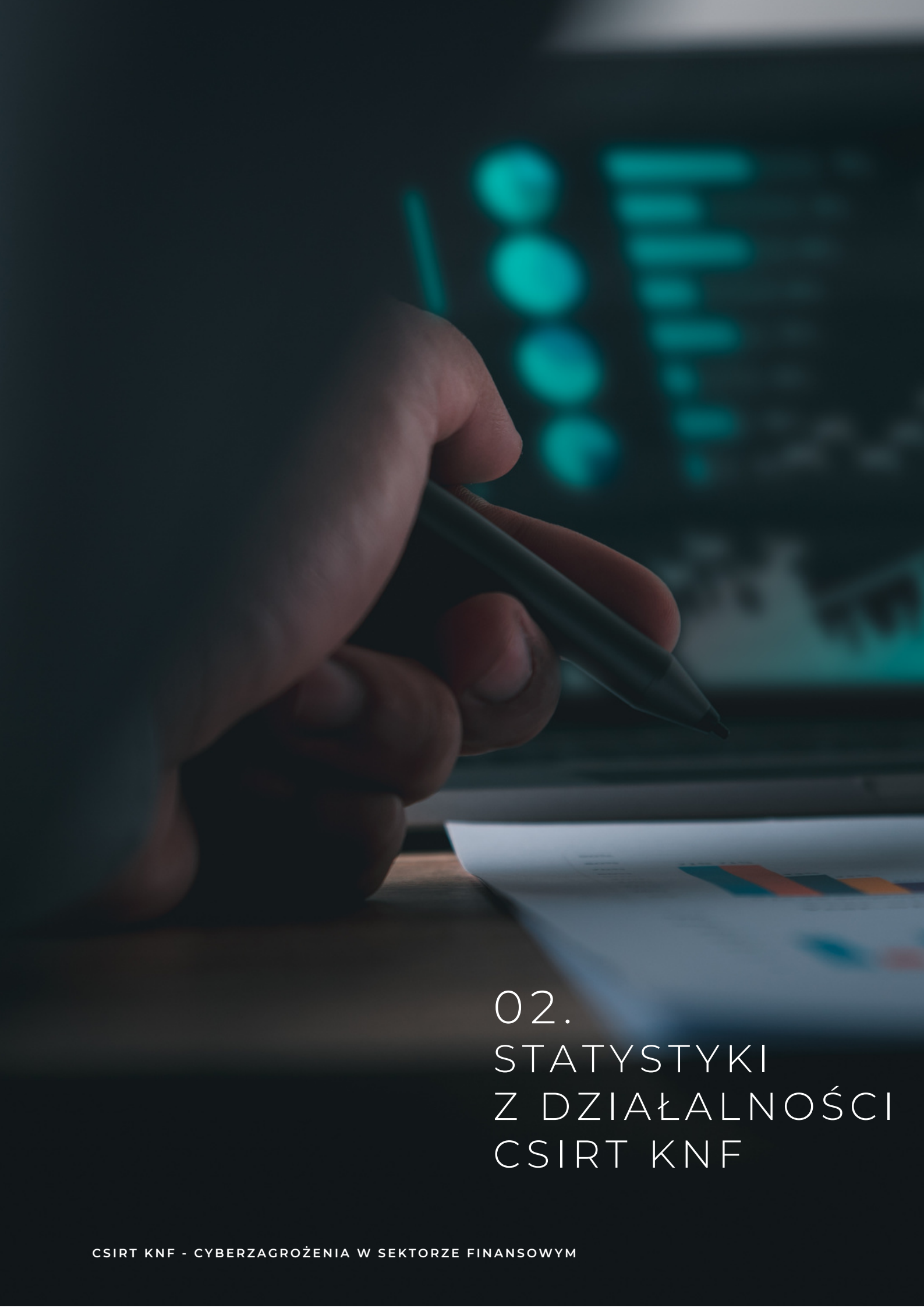
WPROWADZENIE

Szanowni Państwo,

Z przyjemnością przedstawiamy Państwu Raport Roczny, poświęcony analizie zagrożeń dla cyberbezpieczeństwa rynku finansowego z perspektywy sektorowego zespołu CSIRT KNF. W obliczu dynamicznie rozwijającego się świata technologii, a także z coraz większą cyfryzacją usług finansowych, ochrona przed cyberatakami staje się kluczowym wyzwaniem dla instytucji finansowych na całym świecie.

W minionym roku obserwowaliśmy liczne ataki zarówno na infrastrukturę podmiotów finansowych, jak i na samych klientów oraz ich środki finansowe. Grupy przestępcze w atakach na użytkowników skupiały się na różnego rodzaju manipulacjach i socjotechnikach. W raporcie zebraliśmy i prezentujemy najczęstsze metody ataków i cyberoszustw stosowanych w 2022 roku. Nie można pominąć także innego istotnego zagrożenia, które nabierało szczególnego znaczenia w związku z wybuchem konfliktu w Ukrainie. Grupy haktywistyczne przeprowadzały ataki typu DDoS, mające na celu ograniczenie dostępności świadczonych usług finansowych. W naszym raporcie opisujemy ataki i sposoby działania tych grup. Poprawa poziomu świadomości odnośnie do zagrożeń w cyberprzestrzeni jest istotnym elementem działalności CSIRT KNF. W 2022 roku przeprowadziliśmy liczne działania edukacyjne, które również opisujemy w ramach raportu.

Zapraszamy Państwa do zapoznania się z przygotowanym przez nas materiałem opisującym zidentyfikowane przez CISRT KNF zagrożenia dla cyberbezpieczeństwa na rynku finansowym. Wierzymy, że będzie on wartościowym źródłem informacji dla każdej osoby zainteresowanej zagadnieniami dotyczącymi cyberbezpieczeństwa.

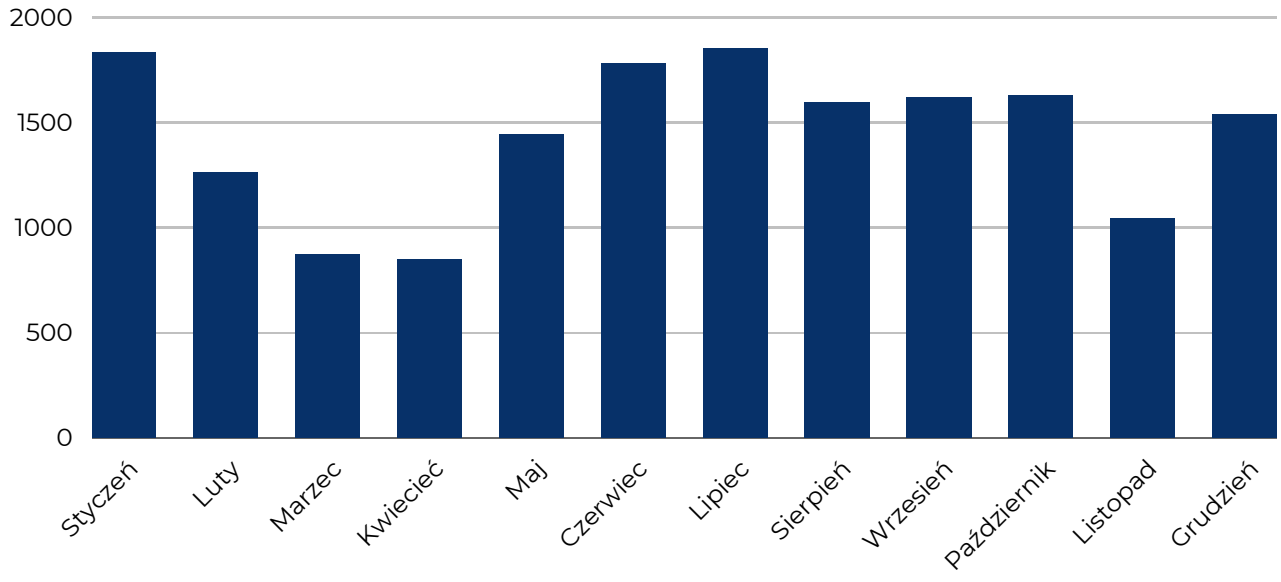


02.
STATYSTYKI Z DZIAŁALNOŚCI CSIRT KNF

Statystyki z działalności CSIRT KNF

Zespół CSIRT KNF na bieżąco monitoruje i analizuje nowe trendy oraz zagrożenia z obszaru cyberbezpieczeństwa ukierunkowane na klientów rynku finansowego. Zgromadzona w ten sposób wiedza wykorzystywana jest do działań mających na celu mitygację ryzyk oraz działań edukacyjnych podnoszących świadomość klientów bankowości elektronicznej w zakresie cyberbezpieczeństwa.
Prowadzimy działania analityczne mające na celu wcześniejsze wykrywanie i ograniczenie dostępu do stron o charakterze oszukańczym. Na bieżąco monitorowane są nowo powstające domeny internetowe. W przypadku identyfikacji podszywania się pod podmiot z sektora finansowego, we współpracy z zespołem CSIRT NASK prowadzone są działania zmierzające do usunięcia fałszywej strony lub ograniczenie dostępu do niej. Ograniczenie dostępu do zidentyfikowanych stron o charakterze oszukańczym realizowane jest na mocy porozumienia pomiędzy KPRM, UKE, NASK PIB, a polskimi operatorami telekomunikacyjnymi.

Domeny zgłoszone przez CSIRT KNF do CERT POLSKA w 2022 roku



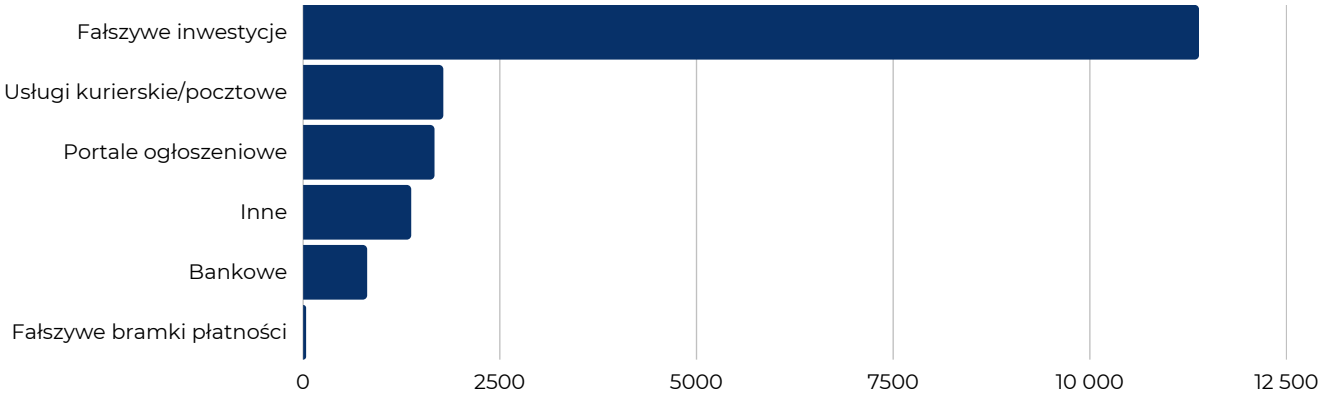
Wykres 1. Liczba domen zgłoszonych przez CSIRT KNF do CERT POLSKA w 2022 roku.

W 2022 r. zespół CSIRT KNF zidentyfikował i zgłosił do zablokowania 17 200 fałszywych domen.

Statystyki z działalności CSIRT KNF

Z analiz prowadzonych przez zespół CSIRT KNF wynika, że problem oszustw internetowych znacząco wzrósł w związku z pandemią COVID-19 oraz częstszym dokonywaniem zakupów internetowych. Natomiast w 2022 roku można zauważyć spadek liczby powstawania niebezpiecznych domen po wybuchu konfliktu w Ukrainie. Domeny wykorzystywane były do kradzieży numerów kart płatniczych, kradzieży poświadczeń klientów do bankowości elektronicznej, kradzieży poświadczeń do portali społecznościowych oraz oszustw na fałszywe inwestycje. Złośliwe strony zostały zgłoszone do CERT Polska w celu ich zablokowania, a tym samym ochrony klientów przed przypadkowym lub omyłkowym ich użyciem.

Kategorie zgłoszonych domen



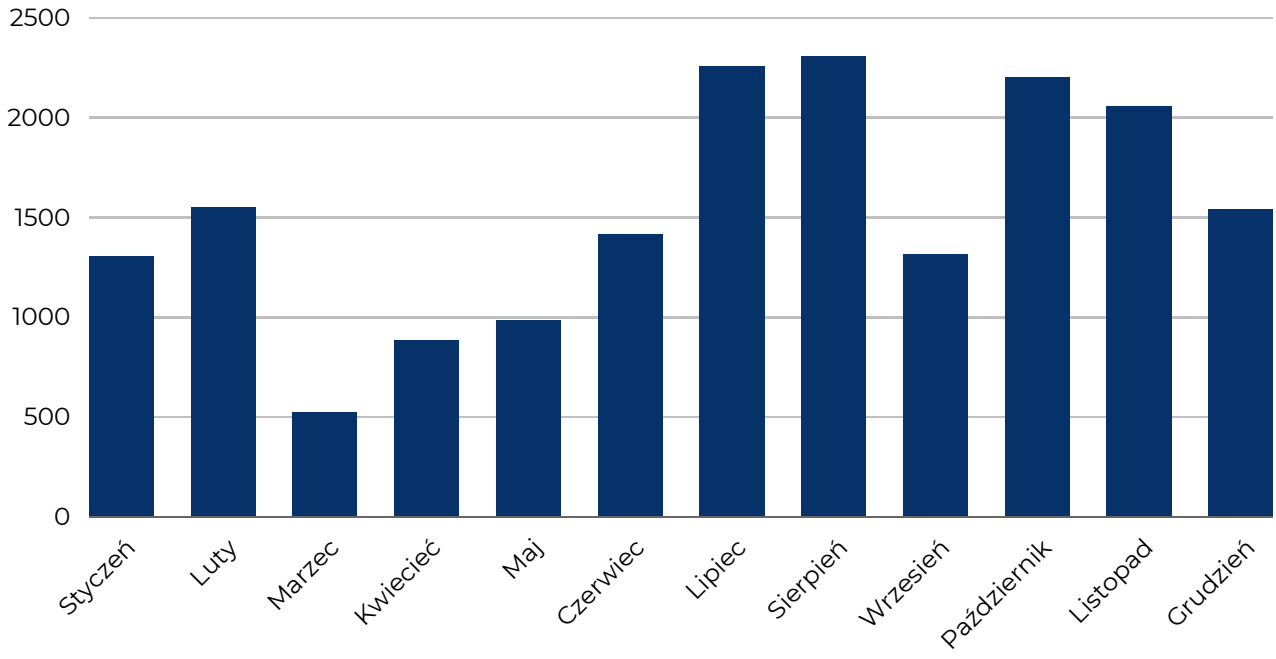
Wykres 2. Kategorie zgłoszonych domen przez CSIRT KNF w 2022 roku.

W 2022 r. najwięcej zidentyfikowanych przez CSIRT KNF oszukańczych domen było wykorzystywanych przez cyberprzestępców do tzw. fałszywych inwestycji, którzy przy pomocy spreparowanych reklam w mediach społecznościowych, oferują duże zyski w krótkim czasie. Do uwiarygodnienia często wykorzystywane są wizerunki znanych osób lub instytucji, w tym spółek skarbu państwa takich jak PKP, Orlen, KGHM, PGE, Lotos oraz wizerunki banków.

Statystyki z działalności CSIRT KNF

Zespół CSIRT KNF aktywnie wyszukuje oszukańcze reklamy przy pomocy udostępnionej przez portal Facebook biblioteki reklam. W 2022 r. zespół CSIRT KNF zidentyfikował i zgłosił do usunięcia 17 899 fałszywych reklam umieszczonych na portalu Facebook.

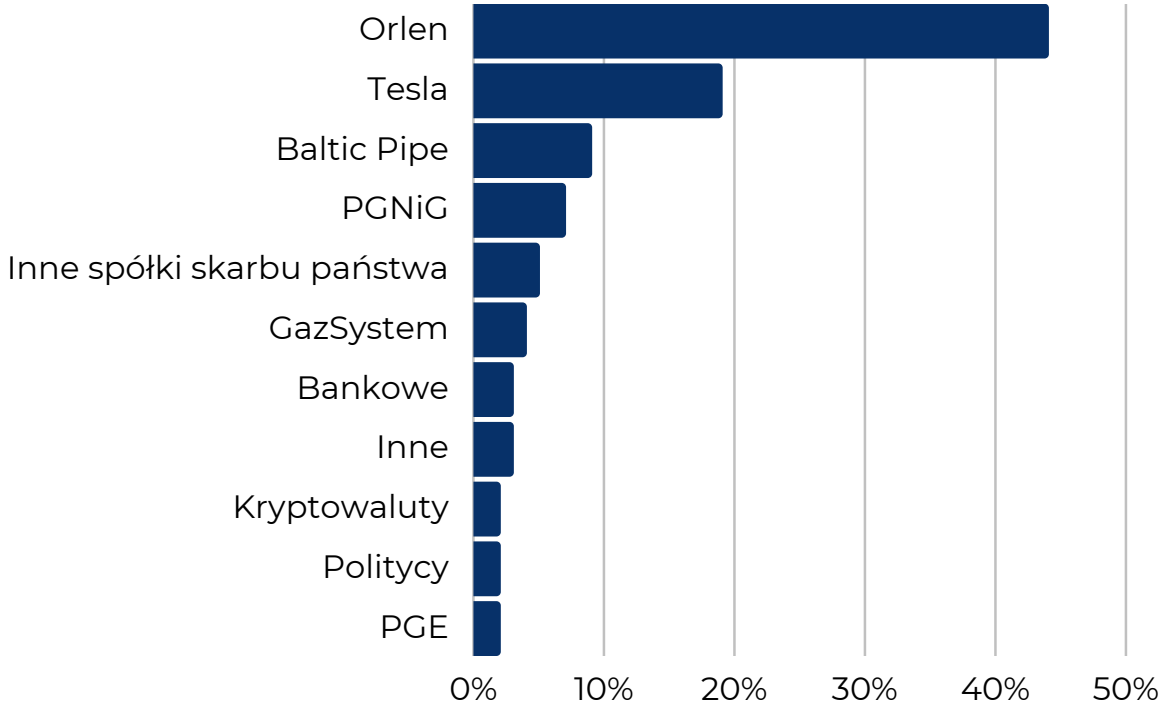
Fałszywe Reklamy Inwestycyjne zgłoszone w 2022 roku



Wykres 3. Fałszywe reklamy inwestycyjne zgłoszone w 2022 roku.

Zgromadzone dane miesięczne pokazują zmienność w liczbie wyświetlanych fałszywych reklam na platformie. Najwięcej reklam odnotowano w okresie letnim, oraz w październiku i listopadzie, z kolei najmniej było ich w marcu. Spadek ten może być związany z inwazją Rosji na Ukrainę, która miała miejsce w lutym. Lato było najbardziej intensywnym okresem działań cyberprzestępców, co wpłynęło na znaczny wzrost liczby reklam. We wrześniu odnotowano spadek zamieszczanych reklam, co mogło być efektem tego, iż przestępcy zmienili wykorzystywany przez nich wcześniej wizerunek spółki skarbu państwa z sektora paliwowego. W kolejnych miesiącach natomiast odnotowano znaczny wzrost oszukańczych reklam, w których wykorzystywano wizerunki spółek skarbu państwa z sektora energetycznego oraz gazowego.

Wykorzystywane wizerunki w fałszywych reklamach w 2022 roku



Wykres 4. Wykorzystywane wizerunki w fałszywych reklamach w 2022 roku.

Cyberprzestępcy w celu uwiarygodnienia potencjalnej inwestycji, wykorzystują wizerunek podmiotów, które są postrzegane jako wiarygodne. W takich przypadkach, przestępcy nie tylko oszukują potencjalne ofiary, ale także niszczą dobre imię firmy, której logo wykorzystują. Zebrane przez nas dane wskazują, że najczęściej wykorzystywany był wizerunek marki Orlen **(7918 reklam)**, a następnie Tesla **(3337 reklam)**. Duże zainteresowanie budzą również pozostałe spółki skarbu państwa takie jak GazSystem, PGNiG, BalticPipe oraz PGE. Fałszywe reklamy inwestycyjne stanowią poważny problem oraz zagrożenie dla nieprofesjonalnych uczestników rynku finansowego w Polsce. Ulokowanie środków w taką inwestycję może spowodować całkowitą ich utratę, a nawet doprowadzić do zadłużenia się potencjalnego inwestora.

03. WYBRANE KAMPANIE OSZUSTÓW W 2022 ROKU

Wybrane kampanie oszustów w 2022 roku

Kierunek działań cyberprzestępców w 2022 roku nie uległ zmianie. Ich głównym celem była nadal kradzież środków finansowych. Oszuści w większości przypadków wykorzystywali znane i sprawdzone metody kradzieży środków finansowych użytkowników, rozszerzając niektóre o nowe elementy i dostosowując do panującej sytuacji. Poniżej prezentujemy najciekawsze z naszej perspektywy kampanie oszustów wymierzone w użytkowników cyberprzestrzeni w ubiegłym roku.

Fałszywe inwestycje

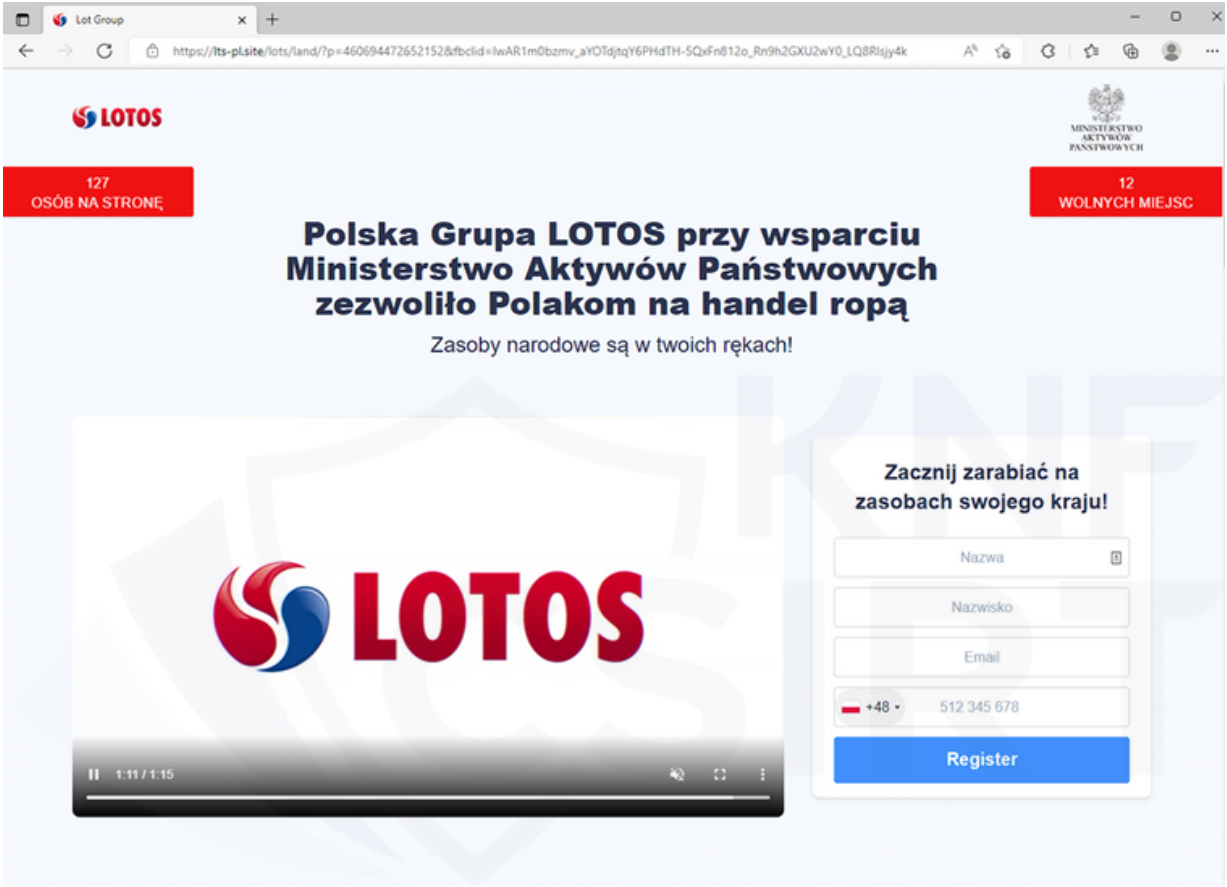
W 2022 roku cyberprzestępcy nakłaniali użytkowników do inwestowania pieniędzy oferując im szybki zysk bez ryzyka utraty środków, mowa tu o oszustwie na fałszywe inwestycje. Oszuści publikowali fałszywe reklamy na specjalnie przygotowanych stronach internetowych bądź portalach społecznościowych. Z reklam dowiadywaliśmy się o możliwości szybkiego zarobku, a wykorzystywany w nich wizerunek znanych osób ze świata sportu, kultury czy polityki lub oferty firmowane logotypem największych polskich firm i banków miały uwiarygodnić proponowane inwestycje oraz uśpić naszą czujność.

Poniżej przykład fałszywej reklamy inwestycyjnej wykorzystującej wizerunek banku PKO BP:

Grafika 1. Fałszywa reklama inwestycyjna wykorzystująca wizerunek banku PKO BP.

Wybrane kampanie oszustów w 2022 roku

Sposób działania oszustów jest niezmienny, w pierwszej kolejności chodziło im o pozyskanie danych swoich ofiar, aby nawiązać z nimi kontakt telefoniczny lub e-mailowy. Następnie przy wykorzystaniu technik manipulacji nakłaniali ofiary do przekazania zdjęcia dowodu osobistego pod pozorem zarejestrowania ich na platformie inwestycyjnej lub prosili o dokonanie przelewu w niewielkiej kwocie na wskazany przez nich rachunek. Przestępcy szli o krok dalej i namawiali zmanipulowane osoby do zainstalowania na swoim urządzeniu programu do dostępu do zdalnego pulpitu. Wykorzystując to narzędzie, oszuści pod pozorem pomocy w poruszaniu się po specjalnie przez nich spreparowanej platformie inwestycyjnej, wyłudzają od swoich ofiar dane logowania do bankowości internetowej, dane karty oraz nierzadko zaciągają na nie kredyty. Nieświadoma zagrożenia osoba, udostępniając swój rachunek, nie tylko traci środki, ale też często uczestniczy w procederze przestępczym prania brudnych pieniędzy.



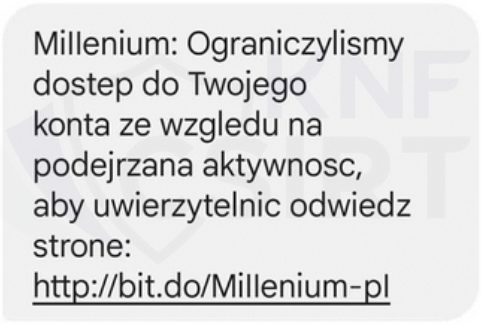
Grafika 2. Fałszywa strona podszywająca się pod Grupę Lotos.

Wybrane kampanie oszustów w 2022 roku

Fałszywe wiadomości SMS

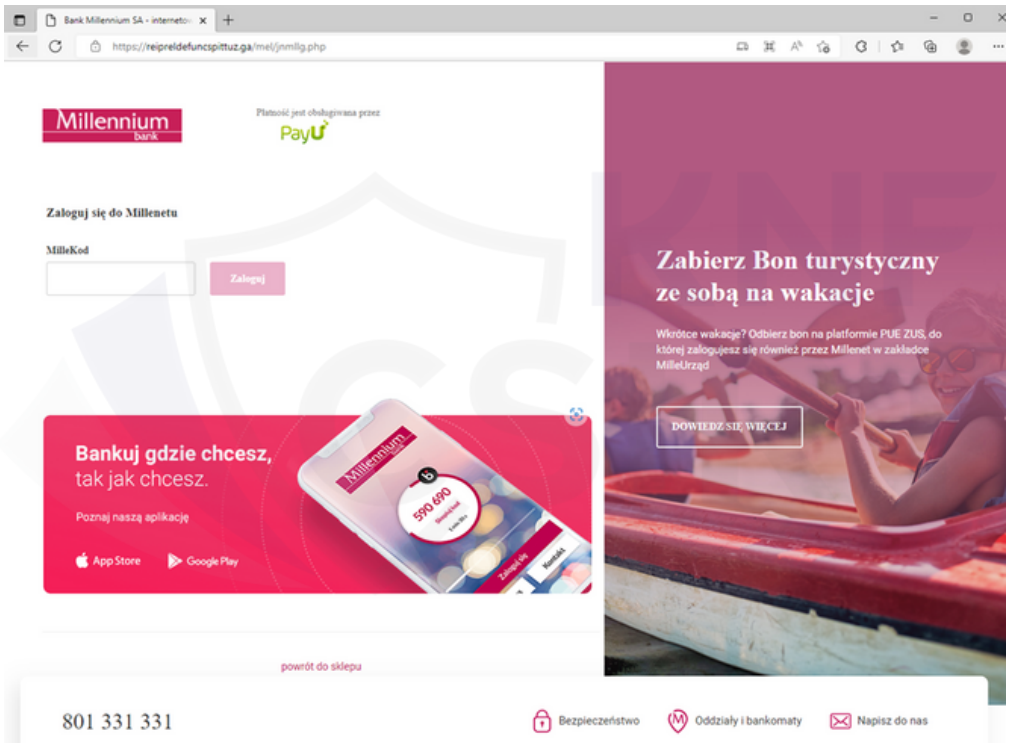
W 2022 roku najczęściej stosowaną metodą kradzieży środków finansowych użytkowników był phishing. Cyberoszuści przesyłali fałszywe wiadomości SMS, w których podszywali się pod znane banki, firmy kurierskie, dostawców energii elektrycznej, portale sprzedażowe bądź instytucje administracji publicznej. Znajdujący się w wiadomości link prowadził na niebezpieczne strony bankowości elektronicznej, gdzie cyberprzestępcy wyłudzali loginy i hasła użytkowników.

Treść fałszywej wiadomości SMS podszywającej się pod bank Millennium. Oszuści informują o rzekomym ograniczeniu dostępu do konta:



Grafika 3. Fałszywa wiadomość SMS.

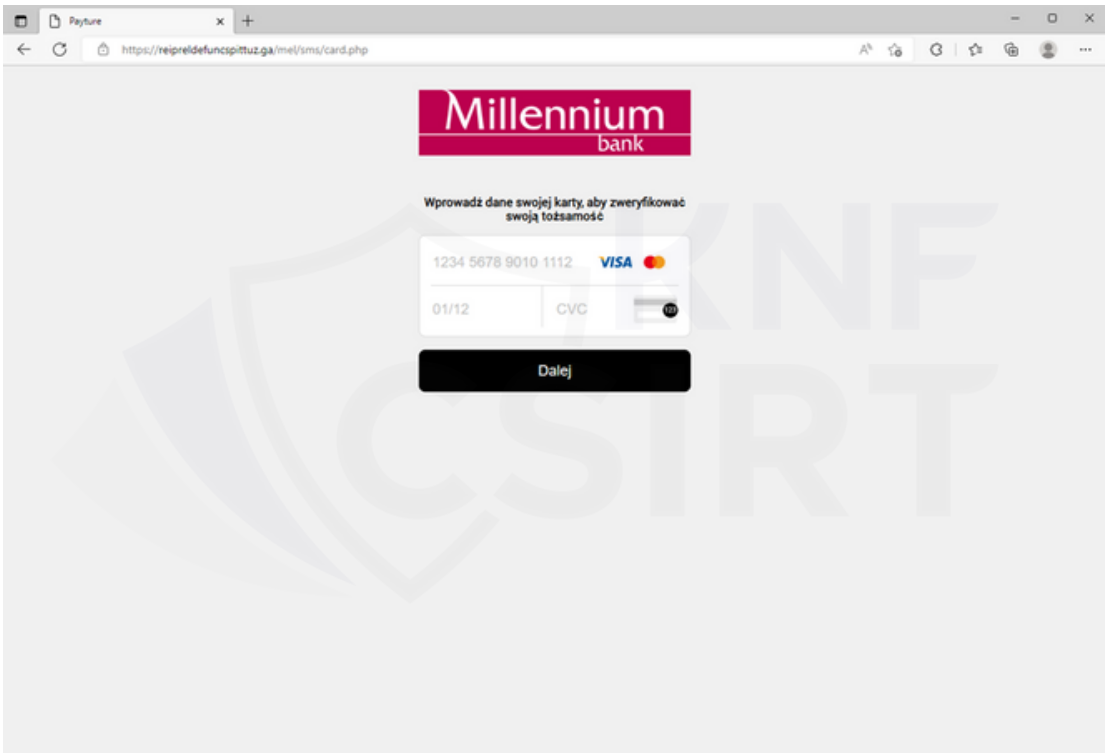
Link prowadził do fałszywej strony bankowości elektronicznej:



Grafika 4. Fałszywa strona podszywająca się pod Bank Millennium.

Wybrane kampanie oszustów w 2022 roku

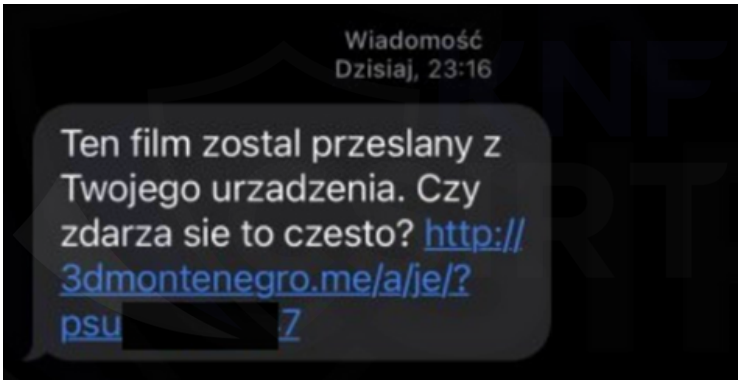
Cyberprzestępcy poza loginami i hasłami wyłudzali również dane do kart płatniczych użytkowników:



Grafika 5. Fałszywa strona podszywająca się pod Bank Millennium, wyłudzająca dane do kart płatniczych użytkowników.

Popularnym schematem działań w 2022 roku było wykorzystanie wiadomości SMS w celu zainfekowania urządzeń mobilnych złośliwym oprogramowaniem FluBot. Oszuści przesyłali do użytkowników fałszywe SMS-y, gdzie zachęcali do kliknięcia w link z rzekomo ciekawym filmem. Zawarty w wiadomości link prowadził do spreparowanej strony, na której rozprzestrzeniana była złośliwa aplikacja przejmująca kontrolę nad urządzeniem i wykradająca środki finansowe użytkowników.

Przykład fałszywej wiadomości SMS przesyłanej przez cyberprzestępców:



Grafika 6. Fałszywa wiadomość SMS.

Wybrane kampanie oszustów w 2022 roku

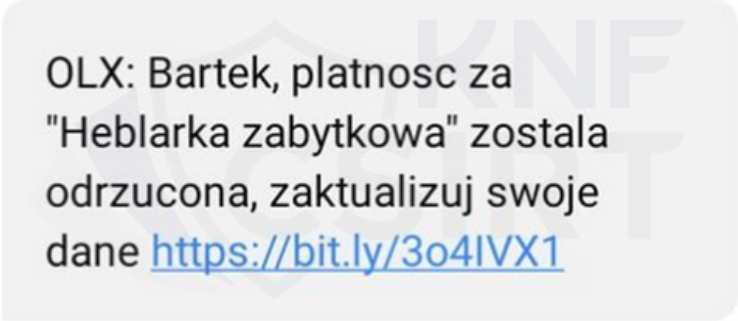
Fałszywa aplikacja po zainstalowaniu usiłowała uzyskać uprawnienia do korzystania z tzw. ułatwień dostępu:

Grafika 7. Fałszywa aplikacja usiłująca uzyskać uprawnienia do funkcji Dostępność.

Działania cyberprzestępców wymierzone były również w użytkowników portali sprzedażowych. Cyberprzestępcy rozbudowali swój schemat oszustwa „na kupującego" – poza jednym z dobrze znanych komunikatorów zaczęli wykorzystywać nowy kanał komunikacji. Mowa tutaj o spersonalizowanych wiadomościach SMS z linkiem prowadzącym na niebezpieczne strony, na których możliwe było rzekome odebranie środków za sprzedawany przedmiot. W rzeczywistości użytkownicy byli okradani ze znajdujących się środków na ich rachunku bankowym .

Wybrane kampanie oszustów w 2022 roku

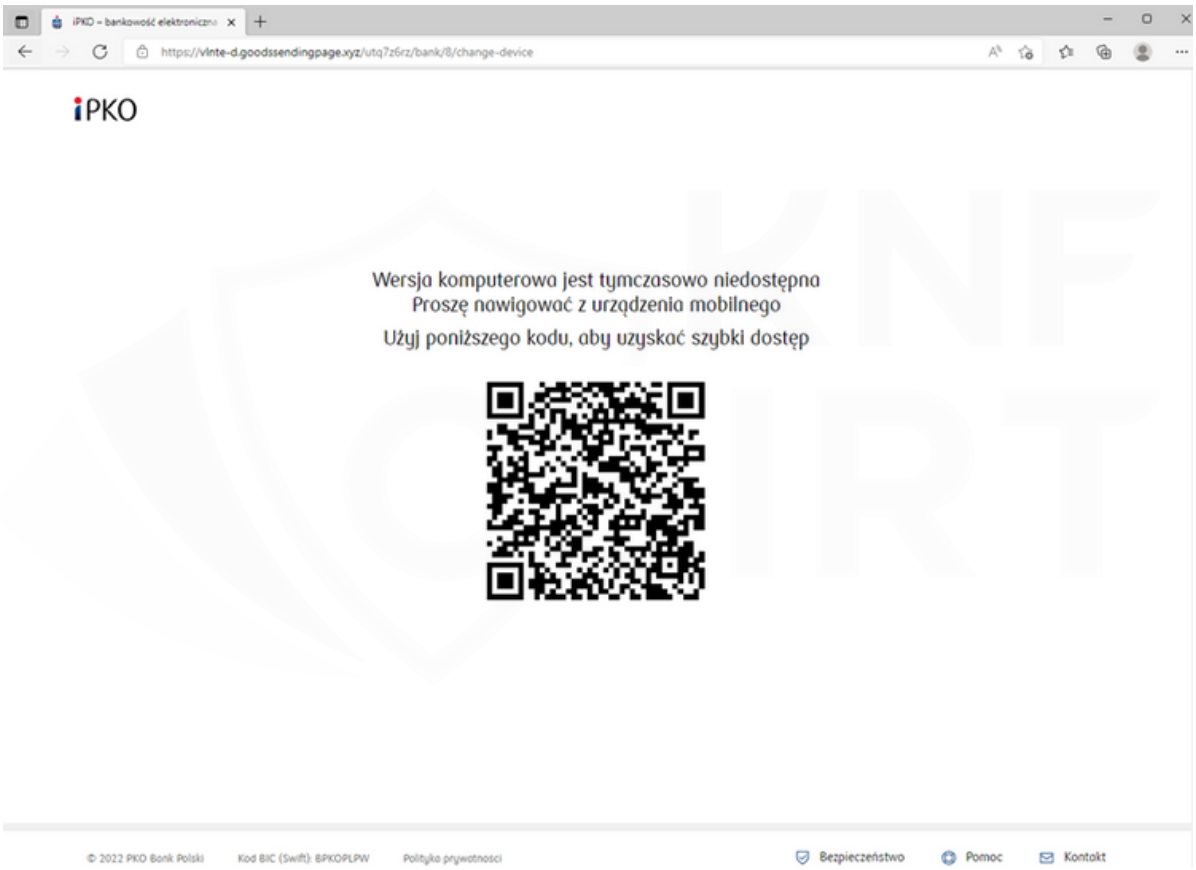
Przykład spersonalizowanej wiadomości SMS, którą otrzymywała ofiara:



Grafika 8. Fałszywa wiadomość SMS, podszywająca się pod portal sprzedażowy.

Cyberprzestępcy przygotowali nowy schemat oszustwa na kupującego. Aby dokonać płatności wymagali użycia kodu QR. W dalszym etapie użytkownicy byli przekierowywani do fałszywej strony banku. Wykorzystując tę technikę oszuści w łatwy sposób mogli zamaskować niebezpieczne linki. W omawianym przypadku podszywali się pod popularny portal sprzedażowy.

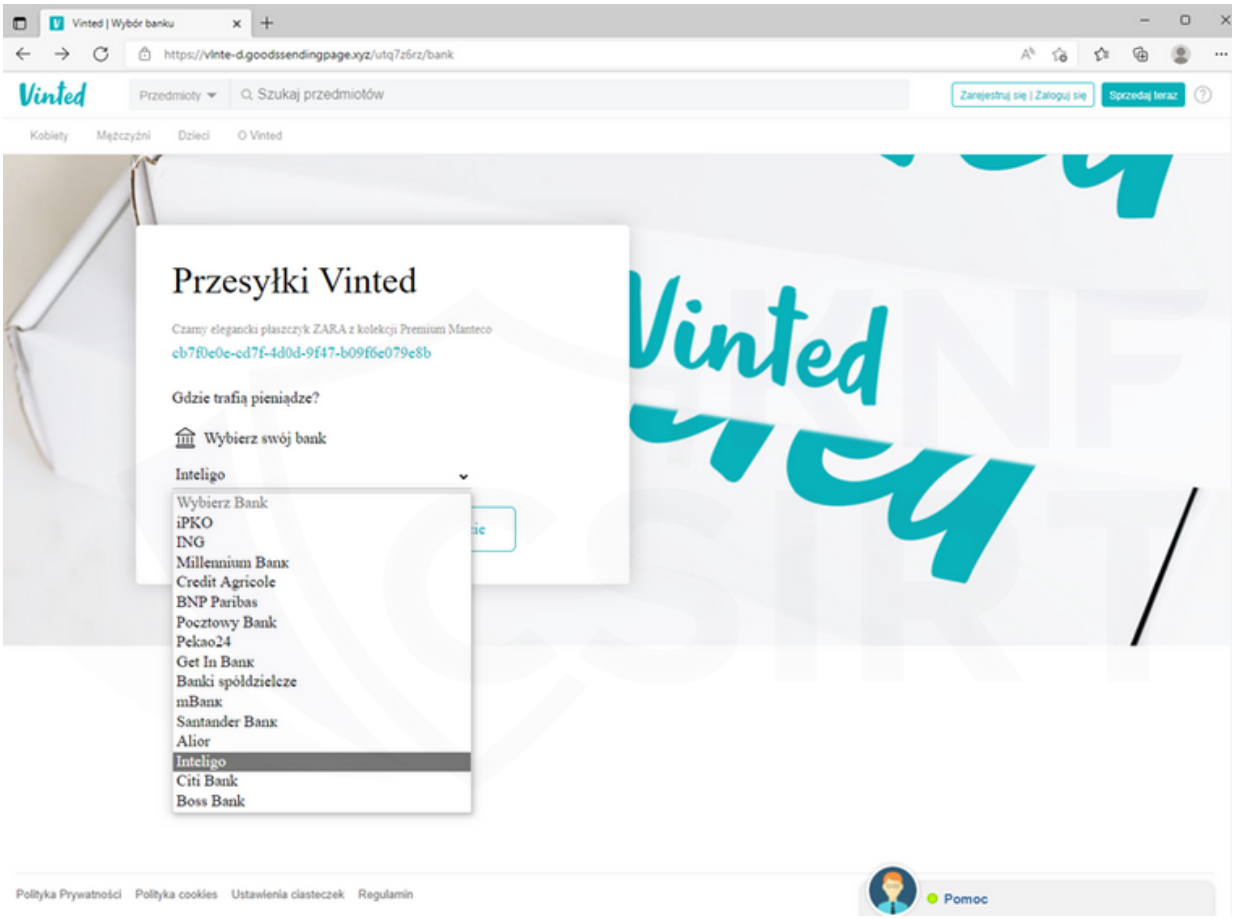
Fałszywa strona, na której oszuści informowali o konieczności zeskanowania kodu QR:



Grafika 9. Fałszywa strona zachęcająca do zeskanowania kodu QR.

Wybrane kampanie oszustów w 2022 roku

Po zeskanowaniu kodu QR użytkownik przenoszony był na niebezpieczną stronę, gdzie spośród dostępnych na liście banków należało wybrać swój:



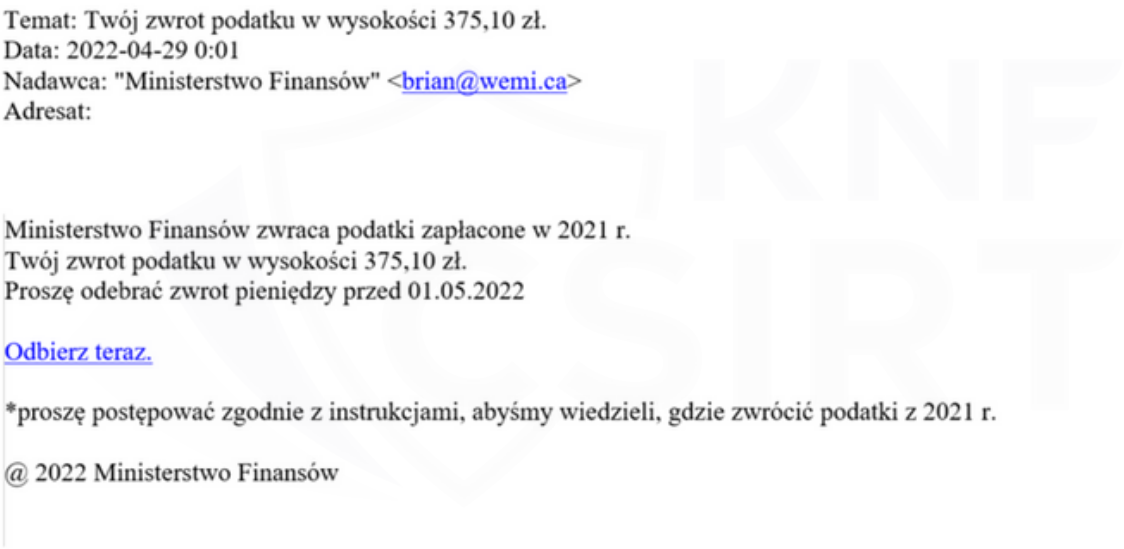
Grafika 10. Fałszywa strona podszywająca się pod znany portal sprzedażowy.

Wybrane kampanie oszustów w 2022 roku

Podszywanie się pod instytucje rządowe

Oszuści szukają coraz nowszych sposobów na kradzież środków finansowych użytkowników. W celu uwiarygodnienia swoich działań podszywali się pod polskie instytucje rządowe. W okresie dokonywania rozliczeń użytkownicy otrzymywali fałszywe wiadomości e-mail z rzekomego Ministerstwa Finansów, informujące o możliwości zwrotu podatku. Przesłany w wiadomości link prowadził do fałszywej strony wyłudzającej dane karty płatniczej.

Treść fałszywej wiadomości e-mail, którą otrzymywała ofiara:



Temat: Twój zwrot podatku w wysokości 375,10 zł.
Data: 2022-04-29 0:01
Nadawca: "Ministerstwo Finansów" <brian@wemi.ca>
Adresat:

Ministerstwo Finansów zwraca podatki zapłacone w 2021 r.
Twój zwrot podatku w wysokości 375,10 zł.
Proszę odebrać zwrot pieniędzy przed 01.05.2022

Odbierz teraz.

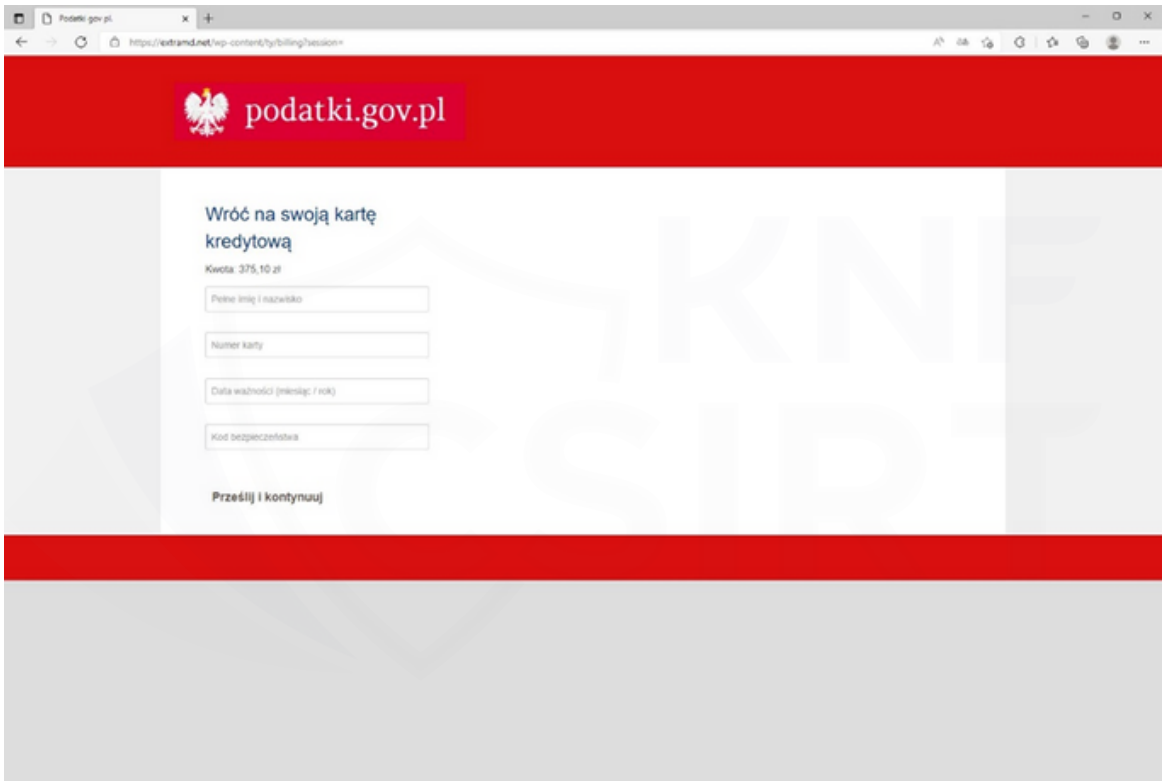
*proszę postępować zgodnie z instrukcjami, abyśmy wiedzieli, gdzie zwrócić podatki z 2021 r.

@ 2022 Ministerstwo Finansów

Grafika 11. Treść fałszywej wiadomości e-mail podszywającej się pod Ministerstwo Finansów.

Wybrane kampanie oszustów w 2022 roku

Fałszywa strona wyłudzająca dane kart płatniczych:



Grafika 12. Niebezpieczna strona wymagająca wprowadzenia danych karty płatniczej.

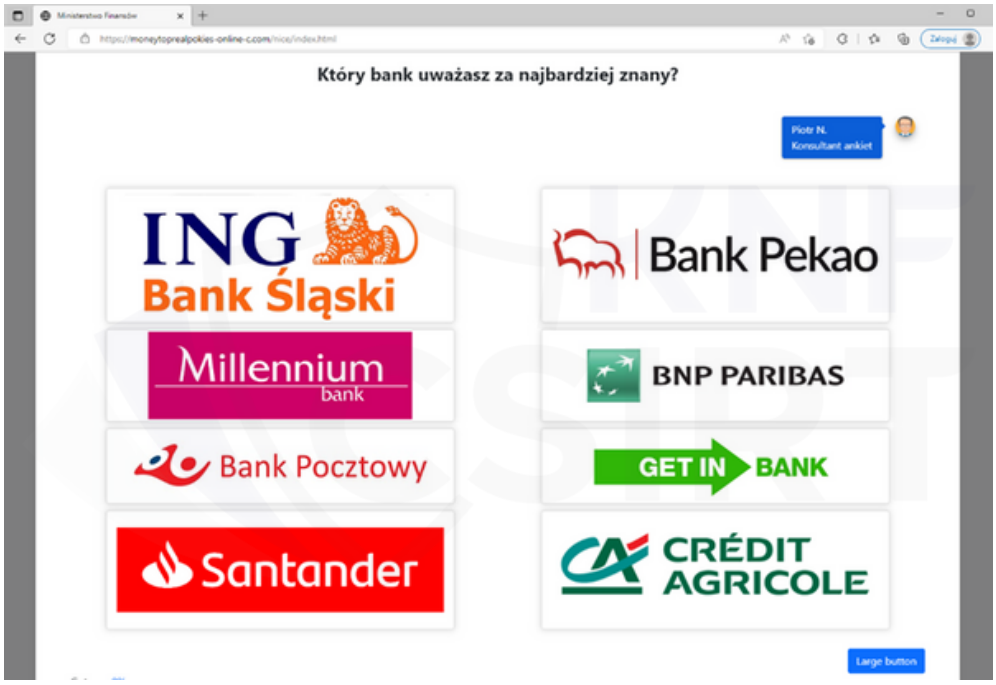
Innym występującym scenariuszem, w którym oszuści wykorzystywali wizerunek Ministerstwa Finansów były fałszywe reklamy w mediach społecznościowych informujące o specjalnej akcji. Użytkownicy zachęcani byli do wypełnienia krótkiej ankiety, za którą rzekomo mieli otrzymać środki na swoje konto. Linki znajdujące się w wiadomościach prowadziły do niebezpiecznych stron wyłudzających loginy i hasła do bankowości internetowej.

Wybrane kampanie oszustów w 2022 roku

Tak wyglądała fałszywa reklama zachęcająca do wzięcia udziału w ankiecie:

Grafika 13. Treść fałszywej reklamy publikowanej przez cyberprzestępców w mediach społecznościowych.

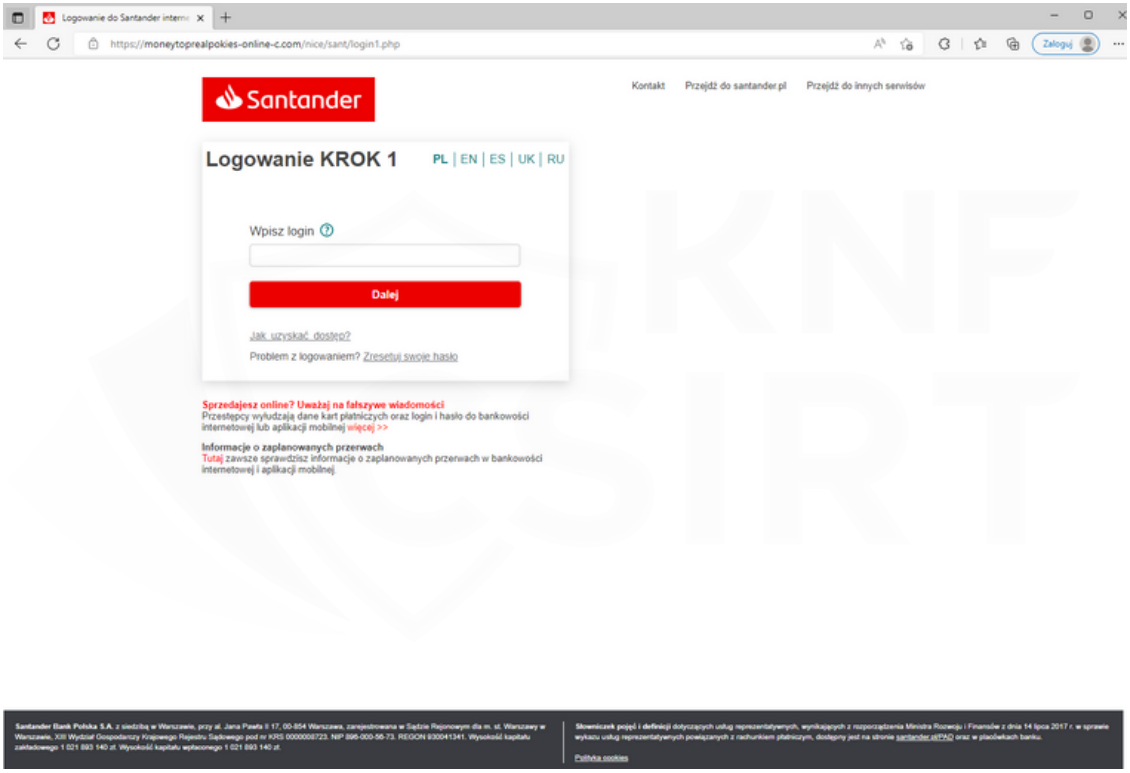
Po kliknięciu w reklamę, użytkownik był przekierowywany na fałszywą stronę z ankietą:



Grafika 14. Niebezpieczna strona z ankietą.

Wybrane kampanie oszustów w 2022 roku

Aby otrzymać rzekome środki na swoje konto, po wypełnieniu ankiety od użytkownika wymagane było wprowadzenie poświadczeń logowania na stronie podszywającej się pod bankowość elektroniczną:



Grafika 15. Niebezpieczna strona podszywająca się pod Santander Bank Polska, wyłudzająca poświadczenia logowania.

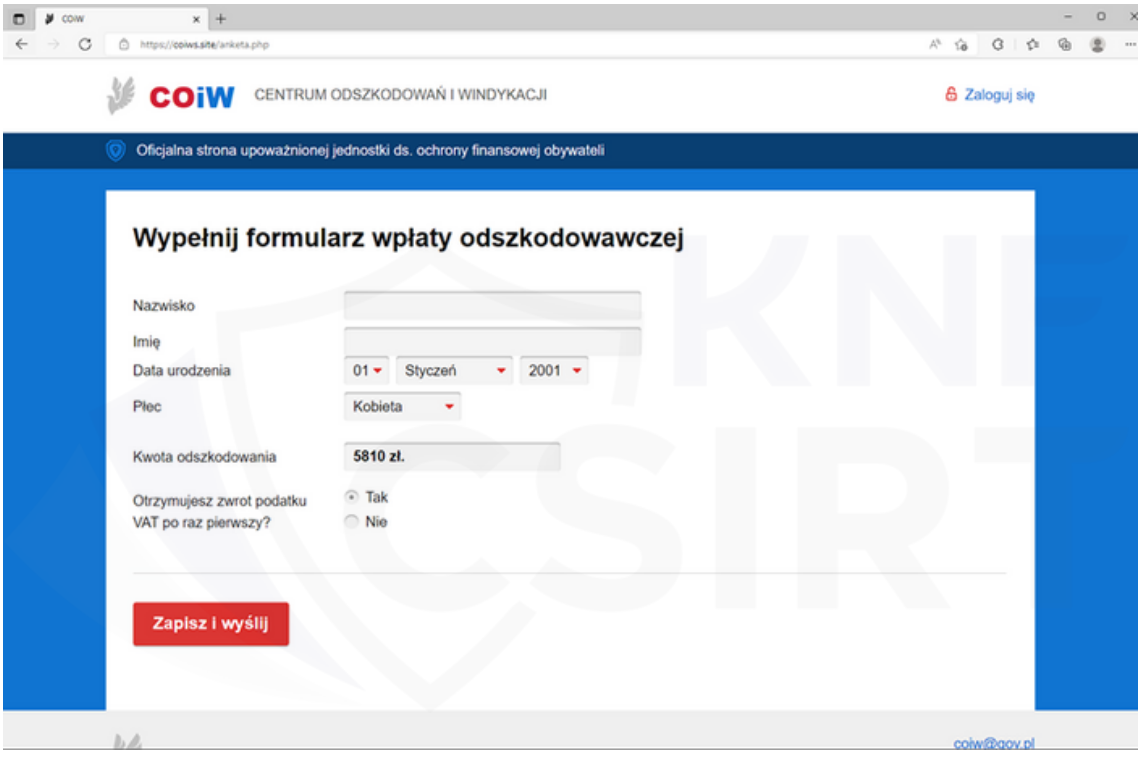
Cyberprzestępcy wykorzystując fałszywe reklamy w mediach społecznościowych podszywali się także pod Urząd Skarbowy, informując o rzekomych odszkodowaniach. Na spreparowanych stronach zachęcali użytkowników do wypełnienia formularza w celu otrzymania środków finansowych. W rzeczywistości oszuści wyłudzali dane osobowe oraz poświadczenia logowania do bankowości elektronicznej.

Wybrane kampanie oszustów w 2022 roku

Tak wyglądała fałszywa reklama:

Grafika 16. Fałszywa reklama podszywająca się pod Urząd Skarbowy.

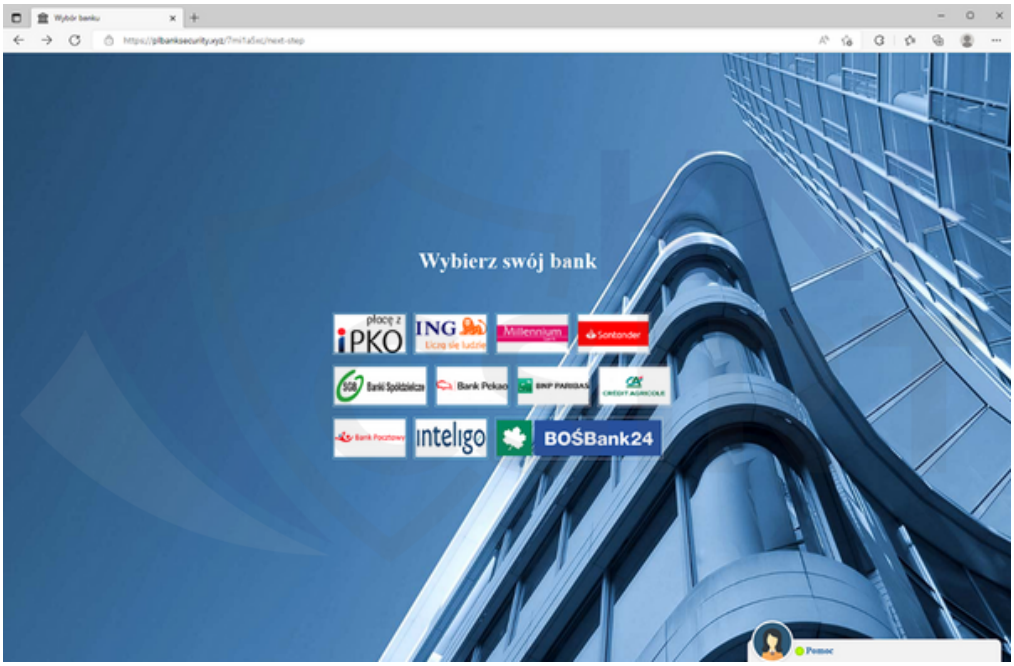
Wygląd niebezpiecznej strony, na której wymagane było wypełnienie formularza w celu otrzymania wypłaty odszkodowawczej:



Grafika 17. Fałszywa strona z formularzem.

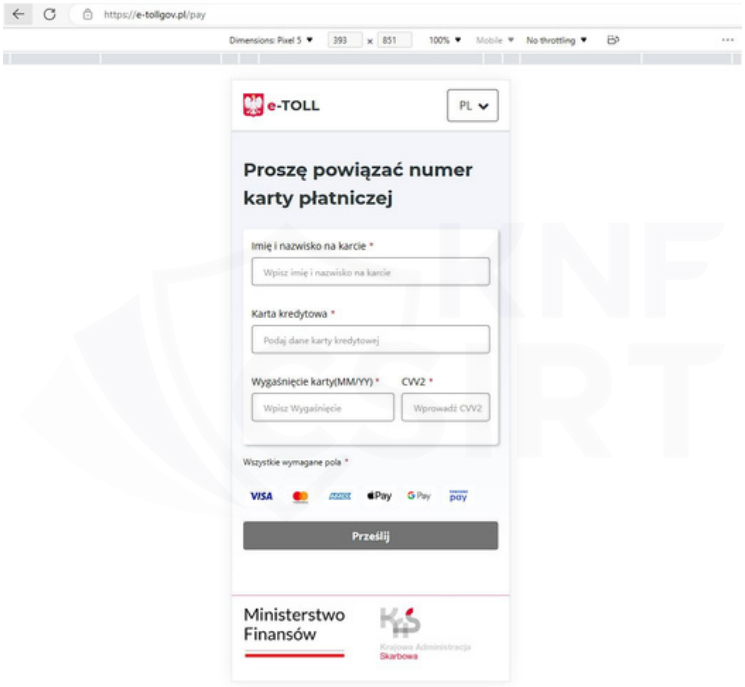
Wybrane kampanie oszustów w 2022 roku

W kolejnym kroku użytkownik przenoszony był na stronę, gdzie należało wybrać swój bank. Po wybraniu ikony banku użytkownik przekierowywany był na fałszywą stronę bankowości elektronicznej, gdzie oszuści wyłudzali poświadczenia logowania.



Grafika 18. Fałszywa strona zachęcająca do wybrania swojego banku.

Cyberprzestępcy za cel obrali sobie również rządowe systemy tj. e-TOOL. Na niebezpiecznych stronach nakłaniali użytkowników do dokonania płatności za przejazd, a w kolejnym kroku wyłudzali dane do karty płatniczych. Poniżej wygląd fałszywego formularza użytego przez atakujących:

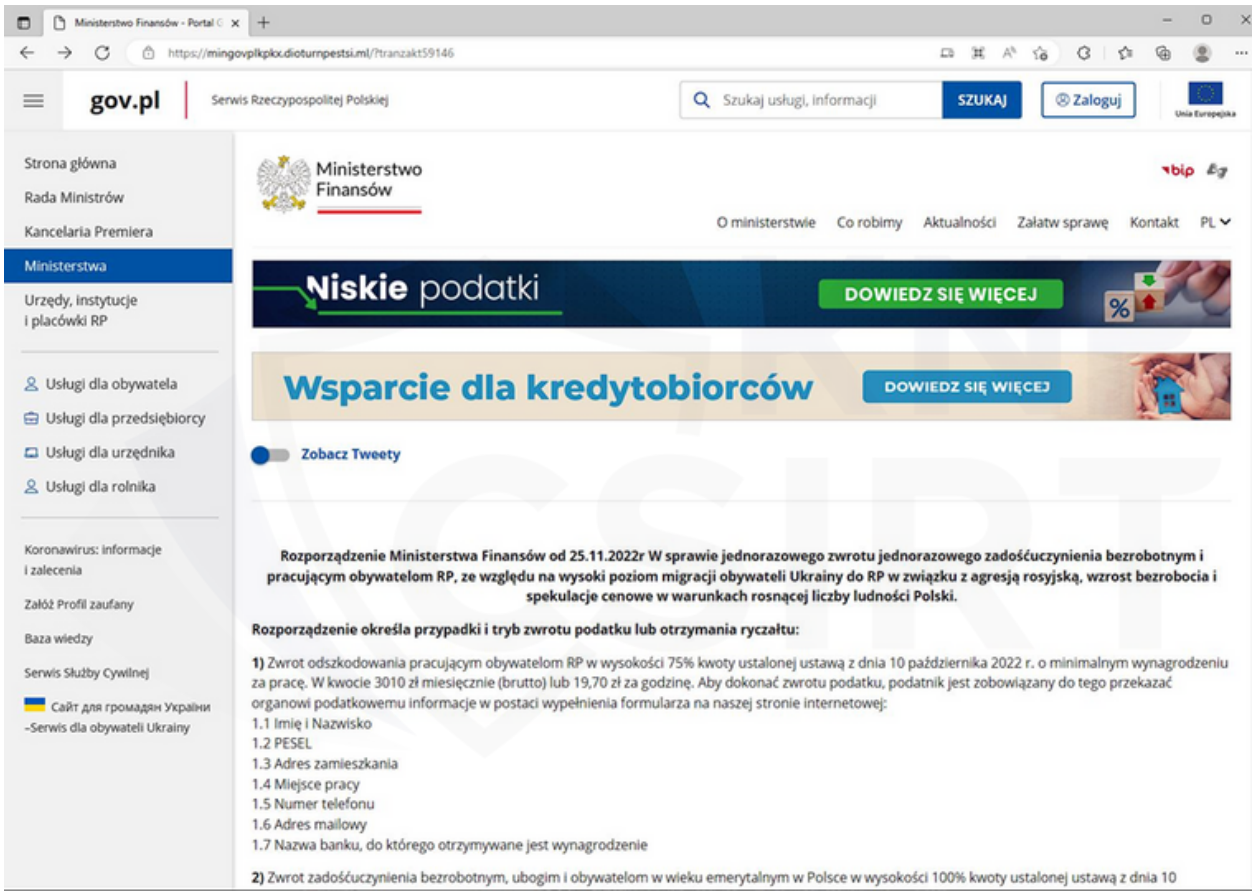


Grafika 19. Fałszywa strona wyłudzająca dane do karty płatniczej.

Wybrane kampanie oszustów w 2022 roku

Innym scenariuszem ataku, gdzie oszuści ponownie wykorzystywali wizerunek Ministerstwa Finansów było zachęcanie użytkowników do odbioru jednorazowego świadczenia. Na spreparowanych stronach próbowali wyłudzać hasła do bankowości internetowej i dane osobowe. Po wypełnieniu formularza użytkownik otrzymywał wiadomość SMS z informacją o zatwierdzeniu wniosku. Przesłany w niej link prowadził do fałszywej strony bankowości elektronicznej, gdzie wyłudzano loginy i hasła.

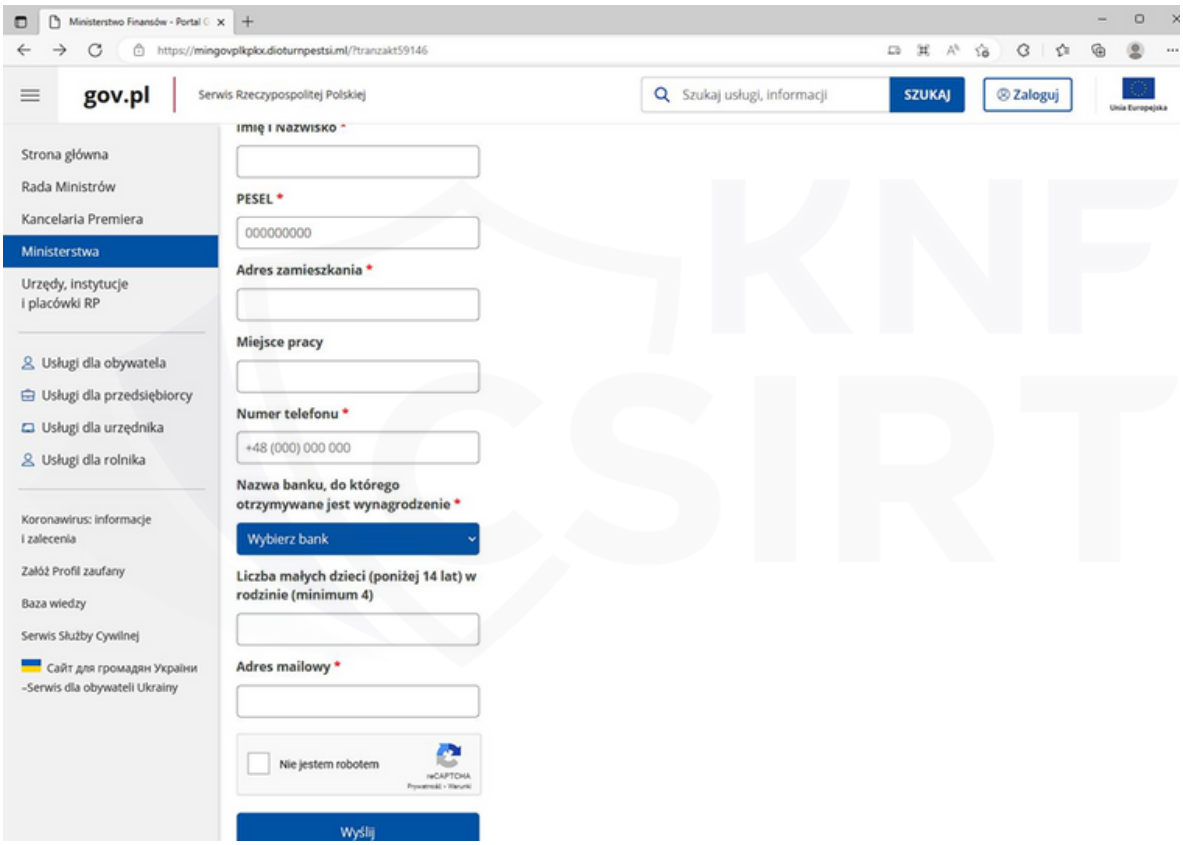
Wygląd fałszywej strony, na której informowano o wsparciu dla kredytobiorców:



Grafika 20. Fałszywa strona podszywająca się pod Ministerstwo Finansów, informująca o możliwości otrzymania wsparcia.

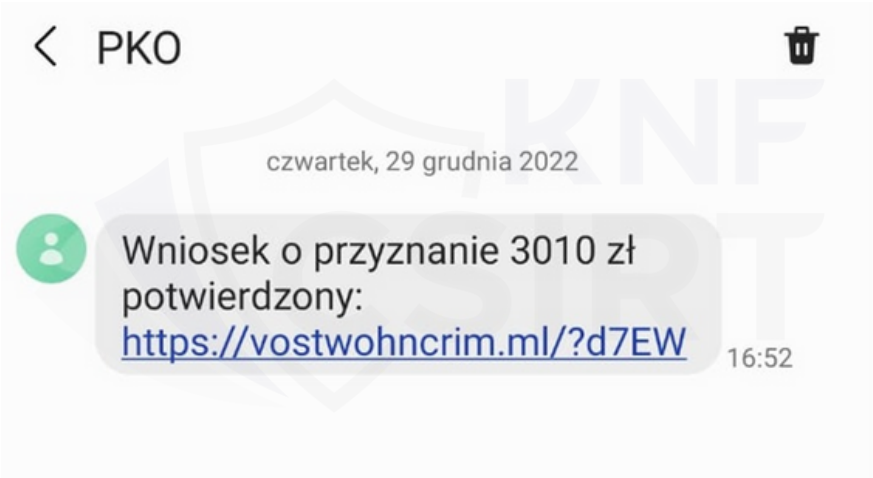
Wybrane kampanie oszustów w 2022 roku

Na fałszywym formularzu wymagane było wprowadzenie swoich danych osobowych:



Grafika 21. Fałszywa strona podszywająca się pod Ministerstwo Finansów, na której wymagane było wprowadzenie swoich danych.

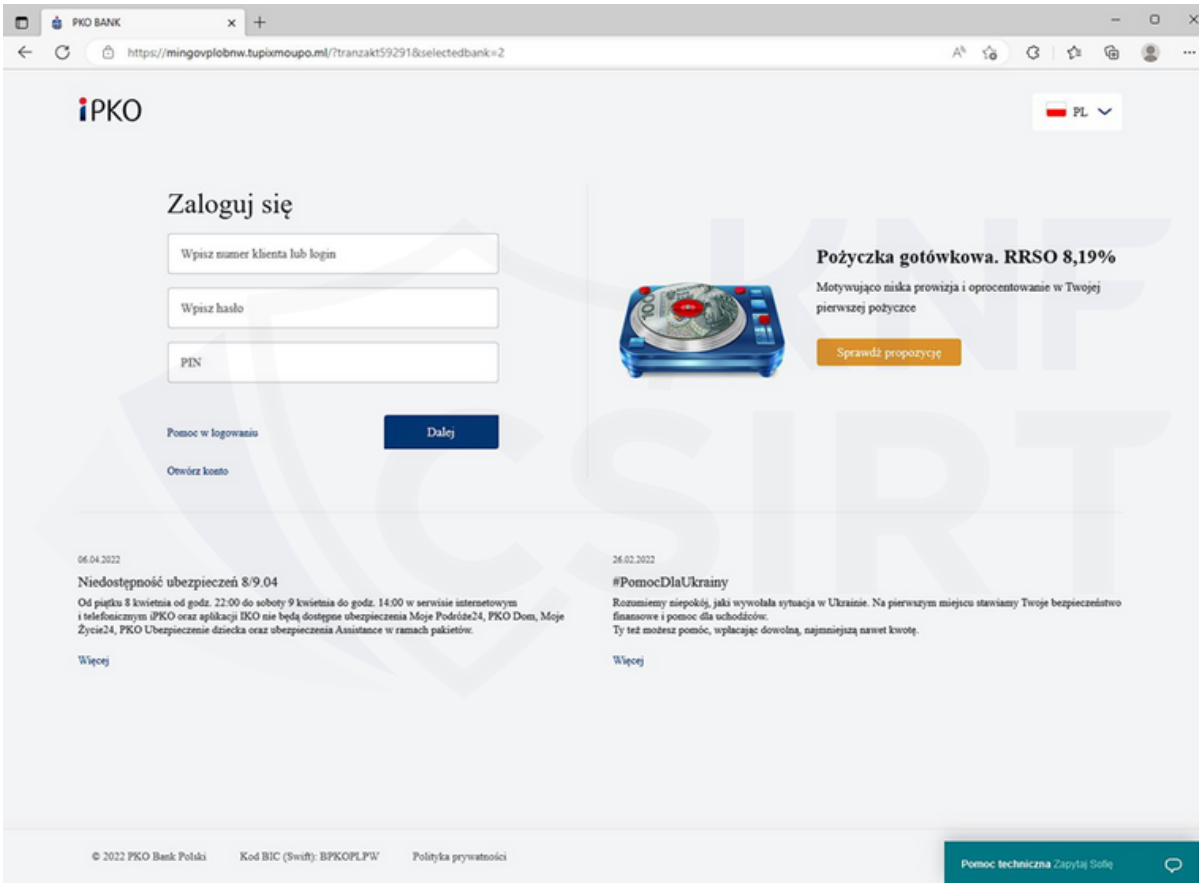
Fałszywy SMS z informacją o zatwierdzonym wniosku:



Grafika 22. Fałszywa wiadomość SMS, którą otrzymywała ofiara.

Wybrane kampanie oszustów w 2022 roku

Link prowadził na fałszywą stronę bankowości elektronicznej:



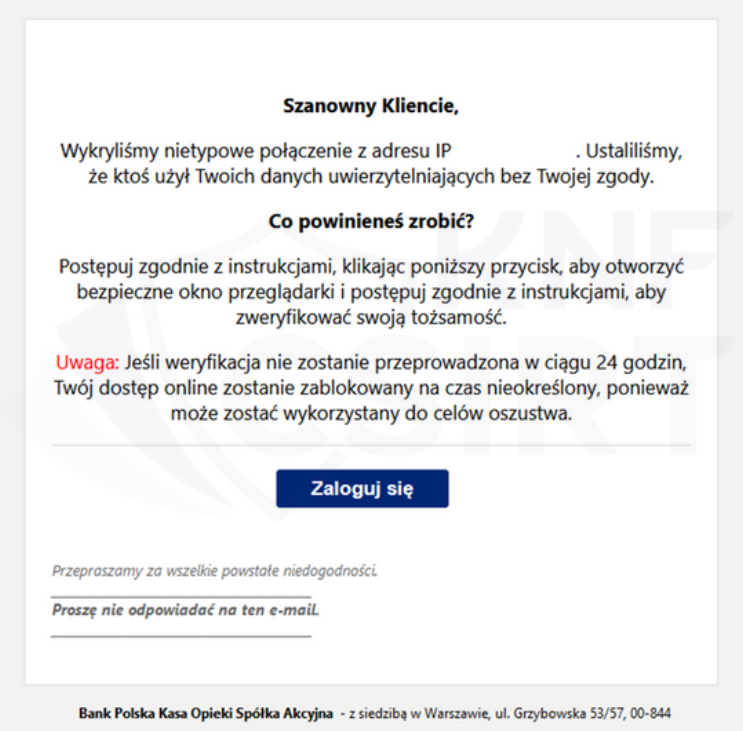
Grafika 23. Fałszywa strona podszywająca się pod bank PKO BP, wyłudzająca poświadczenia logowania użytkowników.

Wybrane kampanie oszustów w 2022 roku

Fałszywe wiadomości e-mail

Jednym z często występujących w 2022 roku zagrożeń były fałszywe kampanie dystrybuowane za pośrednictwem wiadomości e-mail. Oszuści najczęściej podszywali się pod znane banki, gdzie w treści wiadomości informowali użytkowników o obciążeniu konta, konieczności potwierdzenia płatności czy zaktualizowania danych. Przesyłany w wiadomości mailowej link prowadził do fałszywych stron bankowości elektronicznej, na których wymagane było wprowadzenie swojego loginu i hasła.

Przykładowa treść wiadomości e-mail przesyłanej do ofiar. W tym przypadku oszuści podszywali się pod bank Pekao:



Szanowny Kliencie,

Wykryliśmy nietypowe połączenie z adresu IP . Ustaliliśmy, że ktoś użył Twoich danych uwierzytelniających bez Twojej zgody.

Co powinieneś zrobić?

Postępuj zgodnie z instrukcjami, klikając poniższy przycisk, aby otworzyć bezpieczne okno przeglądarki i postępuj zgodnie z instrukcjami, aby zweryfikować swoją tożsamość.

Uwaga: Jeśli weryfikacja nie zostanie przeprowadzona w ciągu 24 godzin, Twój dostęp online zostanie zablokowany na czas nieokreślony, ponieważ może zostać wykorzystany do celów oszustwa.

Zaloguj się

Przepraszamy za wszelkie powstałe niedogodności.

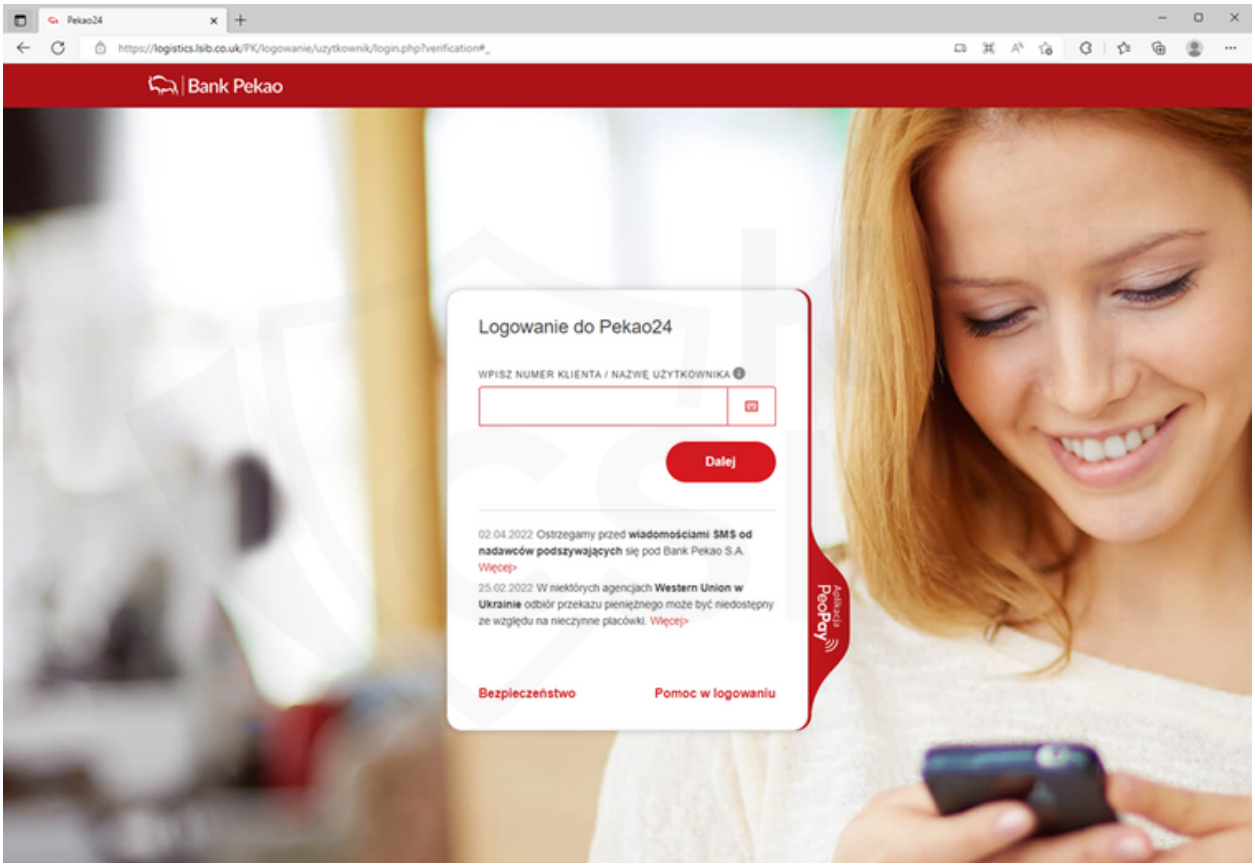
Proszę nie odpowiadać na ten e-mail.

Bank Polska Kasa Opieki Spółka Akcyjna - z siedzibą w Warszawie, ul. Grzybowska 53/57, 00-844

Grafika 24. Fałszywa wiadomość e-mail.

Wybrane kampanie oszustów w 2022 roku

Fałszywa strona bankowości elektronicznej wyłudzająca poświadczenia logowania użytkowników:



Grafika 25. Fałszywa strona podszywająca się pod bank Pekao.

Wybrane kampanie oszustów w 2022 roku

Przybliżając wybrane zagrożenia występujące w roku ubiegłym należy wspomnieć także o oszustwach telefonicznych. Cyberprzestępcy podszywając się pod dowolny numer telefonu podawali się za konsultantów banku, pracowników Komisji Nadzoru Finansowego czy też innych instytucji zaufania publicznego. Pod pretekstem konieczności zweryfikowania przelewu, włamania na konto, odblokowania rachunku jak również wystąpienia innych problemów próbowali nakłonić ofiarę do ujawnienia swoich poufnych informacji tj. poświadczenia logowania czy danych karty płatniczej. W kolejnym etapie oszuści nakłaniali ofiarę do zainstalowania programu do zdalnego zarządzania pulpitem, a następnie zalogowania się do swojego konta w bankowości internetowej.

Cyberprzestępcy wykorzystywali legalne programy umożliwiające obserwację wprowadzanych przez użytkownika treści, a także przejęcie kontroli nad jego urządzeniem. W rezultacie, niczego nieświadome ofiary oddawały dostęp do swoich oszczędności. Oszuści, aby stworzyć wrażenie jak najbardziej wiarygodnych, podczas rozmowy dysponują informacjami o ofierze. Ponadto stosują techniki manipulacji, pozwalające wywołać u rozmówcy poczucie presji oraz szybkiej reakcji.

Wybrane kampanie oszustów w 2022 roku

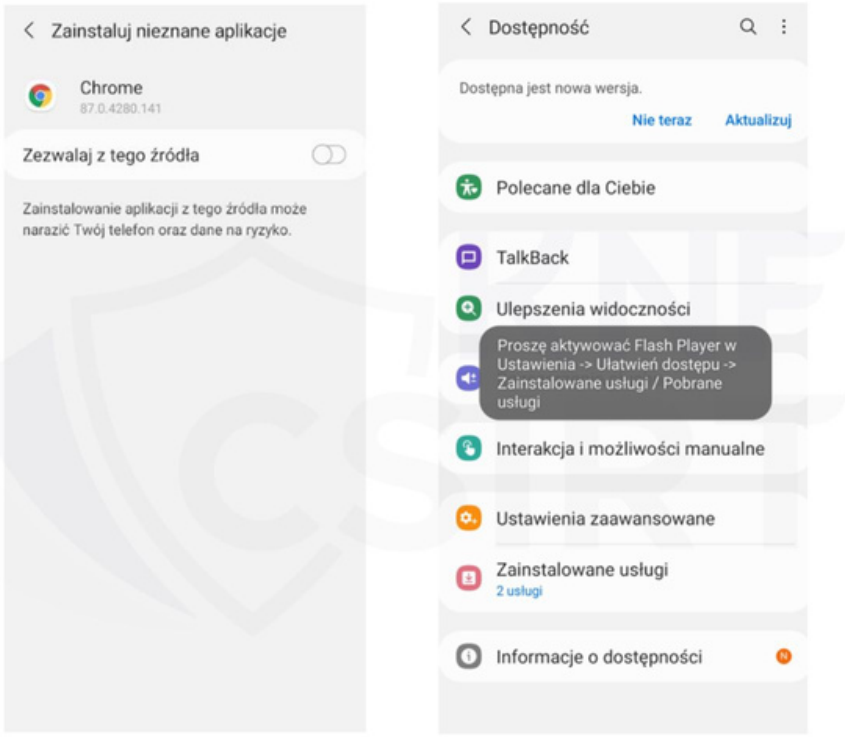
Grafika 26. Przykład rozmowy oszusta z ofiarą .

04. ZŁOŚLIWE OPROGRAMOWANIE

Złośliwe oprogramowanie

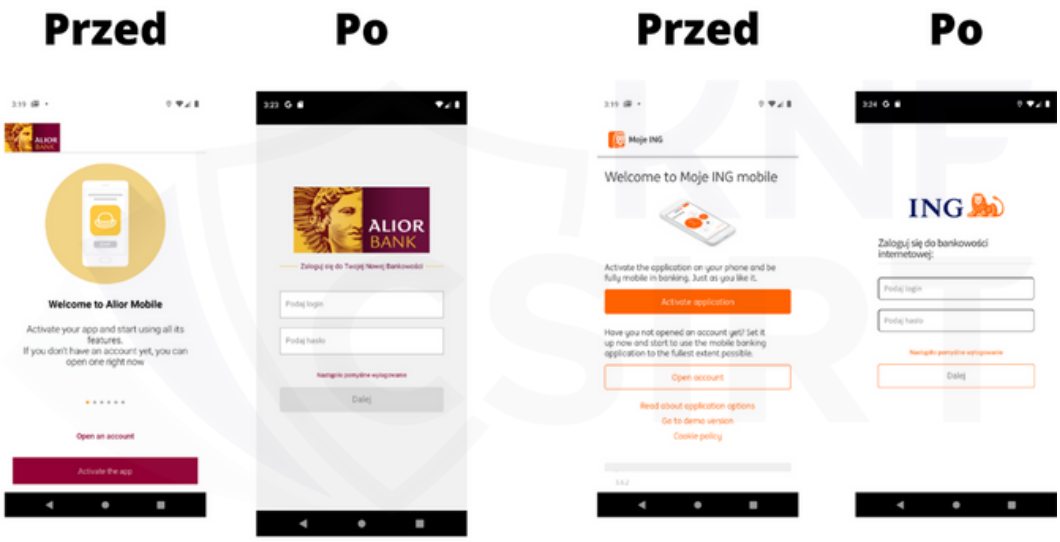
Popularność urządzeń mobilnych, fakt wykorzystywania ich do kluczowych operacji z perspektywy prywatności i bezpieczeństwa, obejmujących dostęp do poczty e-mail, wiadomości SMS, płatności internetowych, czy kontaktów sprawia, że stanowią one atrakcyjny cel dla złośliwego oprogramowania.

W 2022 roku, obserwowane z punktu widzenia zespołu CSIRT KNF kampanie mobilnego malware obejmowały w głównej mierze dystrybucję szkodliwego oprogramowania ukierunkowanego na użytkowników systemu Android. Popularną drogą infekcji były wiadomości SMS, e-mail oraz fałszywe reklamy prowadzące do oszukańczych stron internetowych, skąd następowało pobranie złośliwej aplikacji. W przeważającej części przypadków uruchomienie malware wymagało od użytkownika zgody na instalację aplikacji pochodzących z tzw. niezaufanych źródeł. W przypadku uruchomienia, popularną praktyką niebezpiecznej aplikacji była próba uzyskania uprawnień do funkcji Dostępność. W sytuacji wyrażenia zgody, złośliwe oprogramowanie mogło samodzielnie uzyskiwać kolejne uprawnienia, takie jak dostęp do połączeń, kontaktów czy wiadomości SMS. Inną praktyką było wyłudzanie danych logowania, wprowadzanych na zainfekowanych urządzeniach do atakowanych aplikacji (np. bankowości elektronicznej). W pojedynczych przypadkach obserwowaliśmy dystrybucję fałszywych produktów w oficjalnych sklepach z aplikacjami. W tym podejściu celem oszukańczych aplikacji było wyłudzenie danych od użytkowników lub wykorzystanie ich w oszustwie typu fałszywe inwestycje.



Grafika 27. Domyślna konfiguracja systemu Android, chroniąca przed instalacją aplikacji z tzw. „niezaufanych źródeł" oraz próba wyłudzenia od ofiary zgody na dostęp do funkcji Dostępność przez złośliwe oprogramowanie podszywające się pod Flash Player.

Złośliwe oprogramowanie



Grafika 28. Przykłady fałszywych nakładek wyłudzających dane logowania, przysłaniających uruchamiane aplikacje.

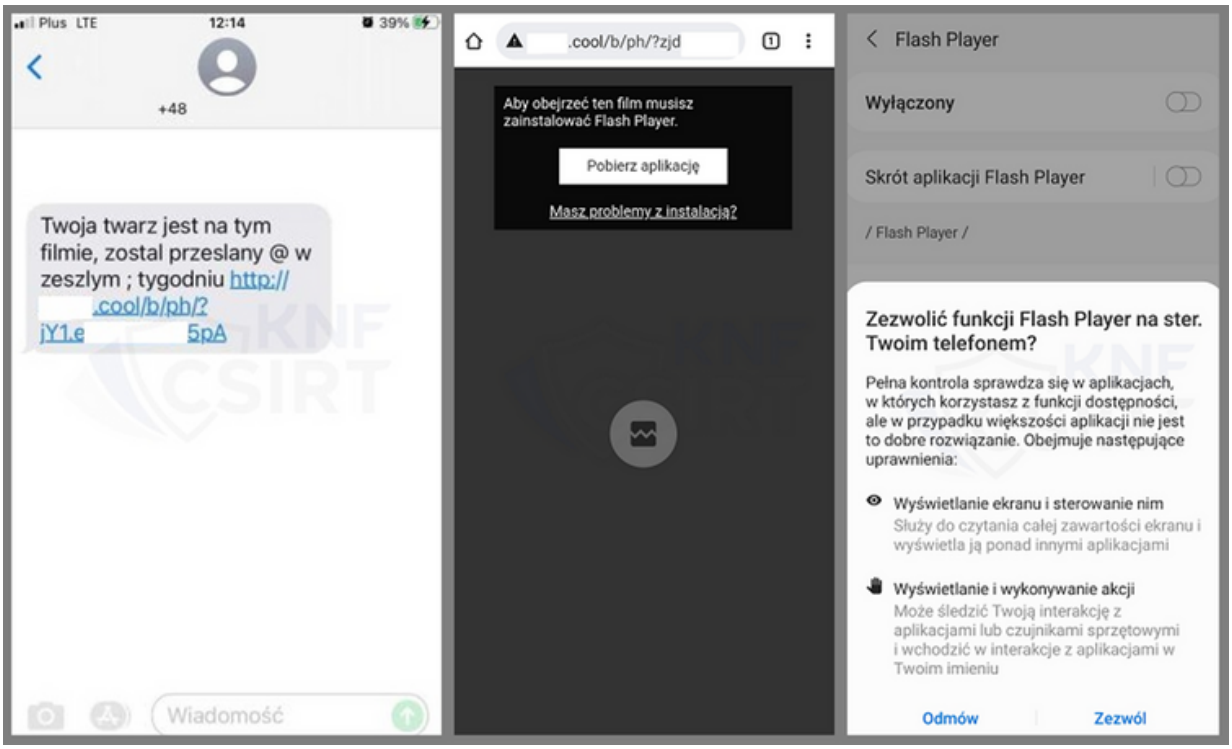
FluBot

FluBot to odmiana złośliwego oprogramowania, o którym pisaliśmy już w grudniu 2021 roku, przeprowadzając analizę sposobu jego działania i dystrybucji [1]. Aktywność tej rodziny malware, atakującej użytkowników systemu Android, w 2022 roku przypadała na jego pierwszą połowę.

W tym czasie czterokrotnie informowaliśmy o kampaniach malware dystrybuujących FluBota [2], [3], [4], [5]. Oszukańcze SMS'y informowały np. o nowej wiadomości głosowej, otrzymanej w zależności od wariantu SMSa od szefa, lekarza, naszego banku, etc. W kampaniach pojawiały się również warianty wiadomości informujące o rzekomym przesłaniu filmu z urządzenia osoby atakowanej lub z jej udziałem. Wraz z początkiem czerwca, na stronie EUROPOLu pojawił się komunikat prasowy, informujący o zakończonej powodzeniem operacji przejęcia i zatrzymania przestępczej instrastruktury Flubota. W międzynarodową operację zaangażowane było 11 krajów Europy i Australii [6].

1. https://www.knf.gov.pl/dla_rynku/CSIRT_KNF/Aktualnosci?articleId=76193&p_id=18
2. https://twitter.com/CSIRT_KNF/status/1478008084673011714
3. https://twitter.com/CSIRT_KNF/status/1485965628498497538
4. https://twitter.com/CSIRT_KNF/status/1522500190279720960
5. https://twitter.com/CSIRT_KNF/status/1526126668523442177
6. https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones

Złośliwe oprogramowanie



Grafika 29. Przykład wiadomości SMS prowadzącej do pobrania złośliwej aplkacji.

Bian Lian aka Hydra

Rodziną złośliwego oprogramowania, której aktywność opisywaliśmy zarówno w początkowym, jak i końcowym okresie minionego roku był BianLian aka Hydra. Jedną z podstawowych funkcjonalności Hydry było przesłanianie ekranów logowania do aplikacji przy użyciu wyświetlanych nakładek (ang. overlays). W przebiegu ataku nakładki mogą służyć potencjalnemu przejmowaniu wprowadzanych do nich informacji (np. danych logowania). Nieco bardziej szczegółową analizę Hydry przedstawiliśmy w jednym z naszych artykułów, gdzie została opisana dystrybucja tej rodziny malware z wykorzystaniem kampanii mailowej posługującej się wizerunkiem ING [7]. Dodatkowo, w pierwszym kwartale 2022 na naszych kanałach społecznościowych zamieściliśmy krótki film informacyjny, demonstrujący sposób działania złośliwej próbki na zainfekowanym urządzeniu [8].

7. https://cebrf.knf.gov.pl/images/Raporty/ZoliweOprogramowanieHydra.pdf
8. https://www.youtube.com/watch?v=_JqohC3jaaY

Złośliwe oprogramowanie

Treść fałszywego e-maila:

Drogi Kliencie,

Nasz system wykrył, że nie masz zainstalowanej naszej aplikacji zabezpieczającej na swoim urządzeniu mobilnym. Z tego powodu Twoje konto zostało zablokowane. Wykonaj zalecane kroki, aby usunąć blokadę. Wszystkie blokady zostaną ponownie zniesione po ich wykonaniu.

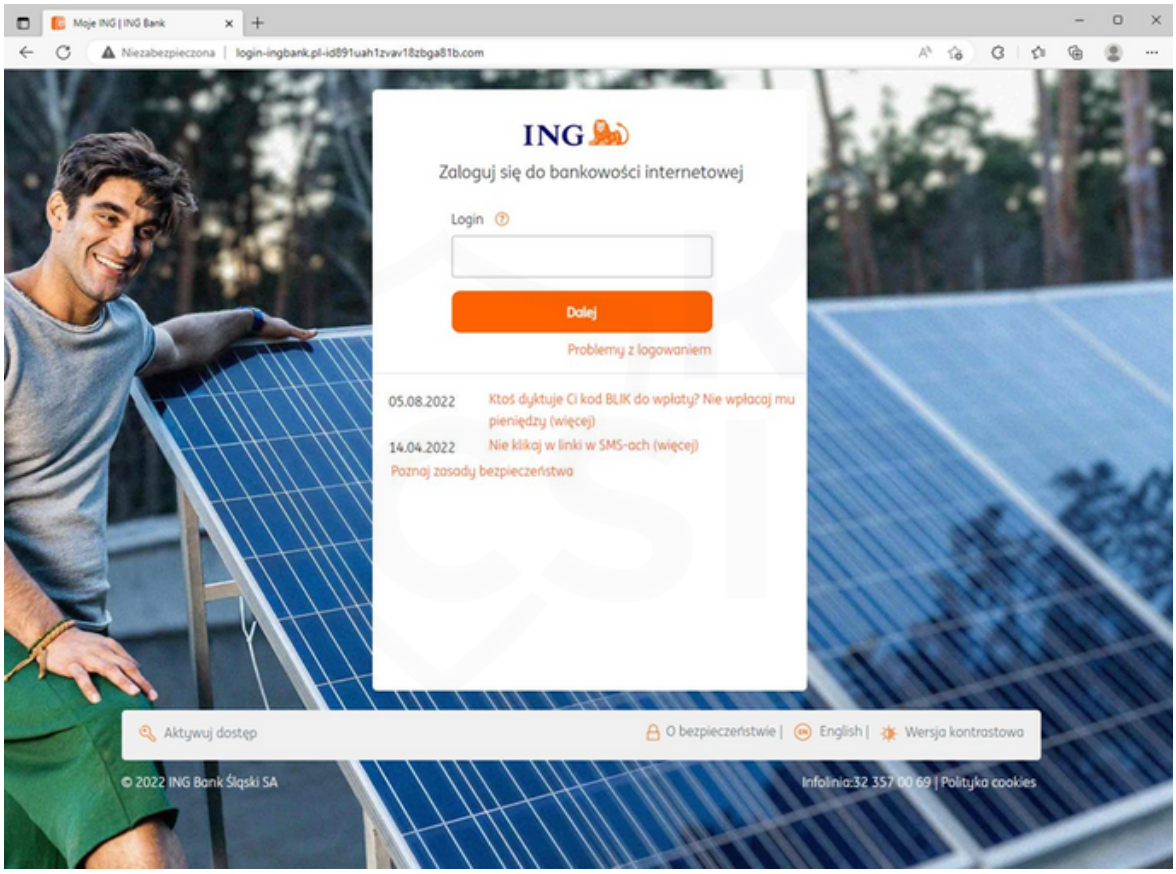
Rozpocznij proces

Dziękujemy za zrozumienie i prosimy o wybaczenie niedogodności.

Z poważaniem
ING Powiadomienie informacyjne

Grafika 30. Fałszywa wiadomość e-mail, w której cyberprzestępcy podszywali się pod ING Bank Śląski.

Po kliknięciu w „Rozpocznij proces" użytkownik przenoszony był na fałszywą stronę podszywającą się pod bank ING, gdzie wymagane było wprowadzenie loginu i hasła:

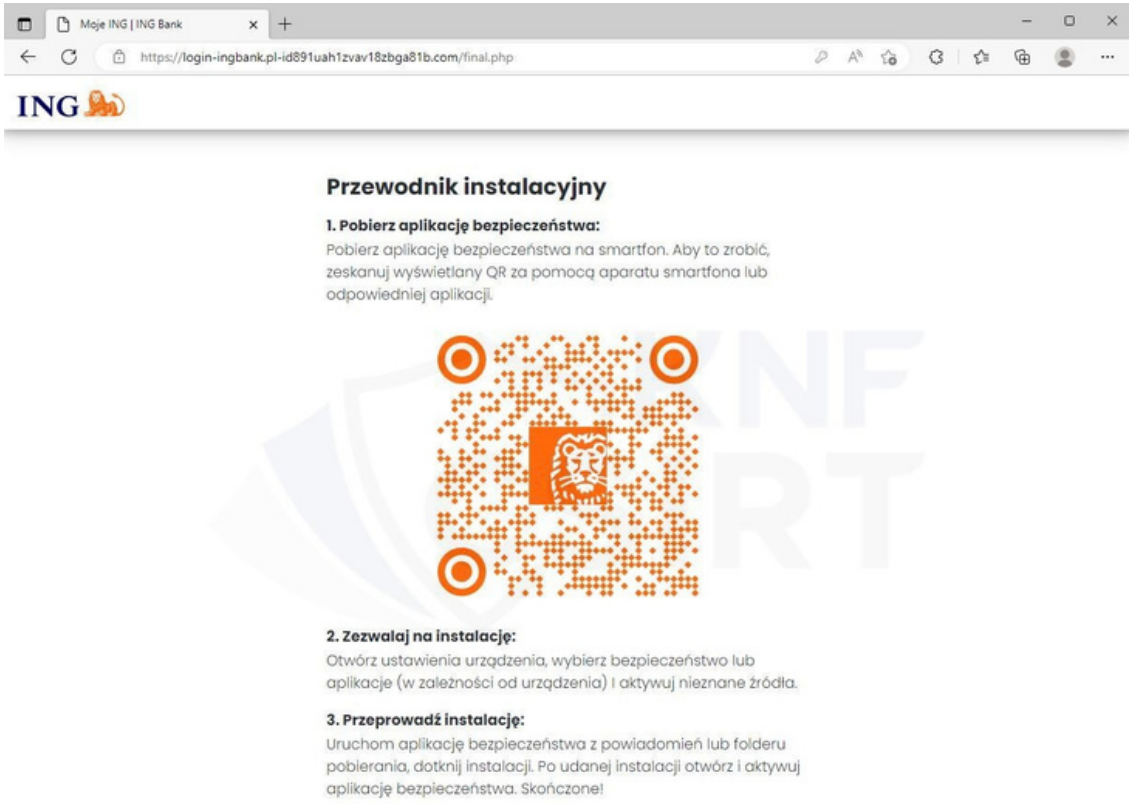


Grafika 31. Niebezpieczna strona wykradająca poświadczenia logowania użytkowników.

Złośliwe oprogramowanie

W ostatnim kroku ofiara zachęcana była do pobrania złośliwej aplikacji przejmującej kontrolę nad urządzeniem. Pobranie aplikacji skutkowało zainfekowaniem telefonu złośliwym oprogramowaniem BianLian aka Hydra, przeznaczonym na urządzenia mobilne z systemem Android.

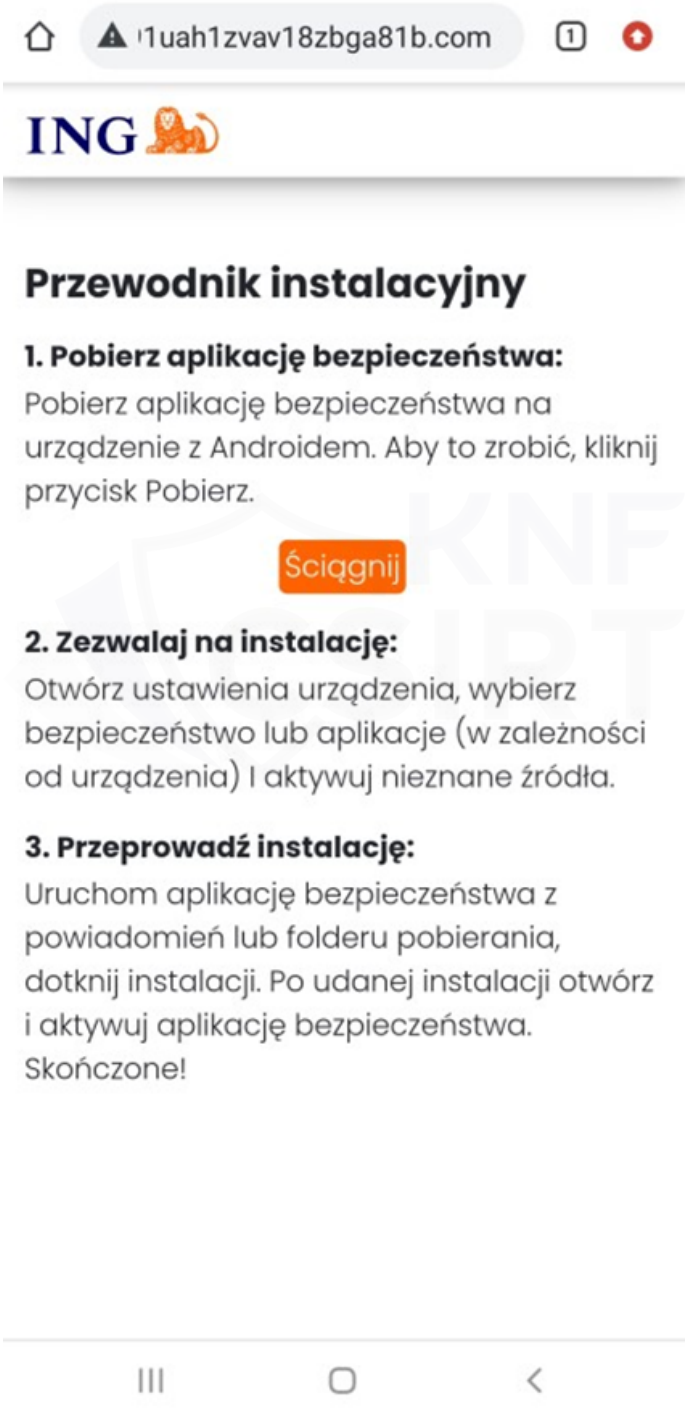
Strona wyświetlana podczas korzystania z komputera. Oszuści wykorzystują kod QR, który prowadzi do pobrania złośliwej aplikacji:



Grafika 32. Fałszywa witryna, posługująca się logotypem ING, prowadząca do pobrania niebezpiecznej aplikacji.

Złośliwe oprogramowanie

Fałszywa strona wyświetlana w przypadku urządzeń mobilnych:

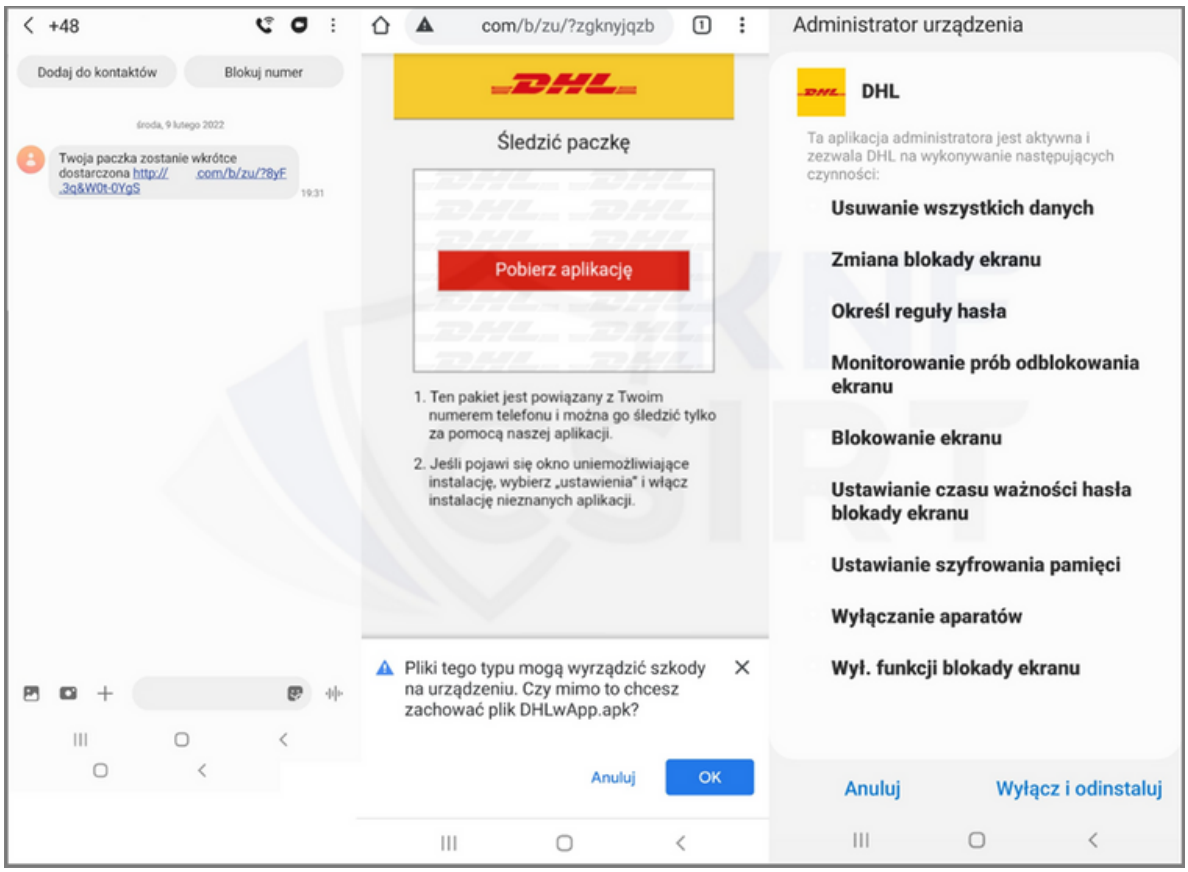


Grafika 33. Niebezpieczna strona wyświetlana na urządzeniu mobilnym.

Złośliwe oprogramowanie

Fałszywa aplikacja wykorzystująca wizerunek DHL

W pierwszej połowie lutego informowaliśmy o dystrybucji kolejnego wariantu złośliwego oprogramowania wymierzonego w urządzenia z Androidem [9]. Sam sposób dostarczenia był powszechnie znany. Potencjalna ofiara otrzymywała wiadomość SMS informującą o zbliżającym się doręczeniu przesyłki. Na końcu wiadomości znajdował się link, kierujący odbiorcę na fałszywą stronę internetową. Złośliwa strona posługiwała się logotypem firmy kurierskiej DHL, informując odwiedzającego o możliwości śledzenia przesyłki (wyłącznie za pomocą dedykowanej aplikacji). Instalacja i uruchomienie fałszywej aplikacji pochodzącej z tzw. niezaufanego źródła (spoza oficjalnego sklepu Google Play) skutkowały zainfekowaniem urządzenia. Złośliwa aplikacja po uruchomieniu wnioskowała o przydzielenie uprawnień do systemowej funkcji "Dostępność" (ang. Accessibility Services), po uzyskaniu której samodzielnie wyrażała zgodę na dostęp do kolejnych kluczowych uprawnień. Wśród uzyskanych przywilejów wymienić możemy m.in. dostęp mikrofonu, kontaktów, SMS-ów, zarządzania połączeniami telefonicznymi czy systemowej funkcji administratora urządzenia.



Grafika 34. Ilustracja złośliwej kampanii i uzyskane przez aplikację uprawnienie administratora urządzenia.

9. https://twitter.com/CSIRT_KNF/status/1491753589886406664

Złośliwe oprogramowanie

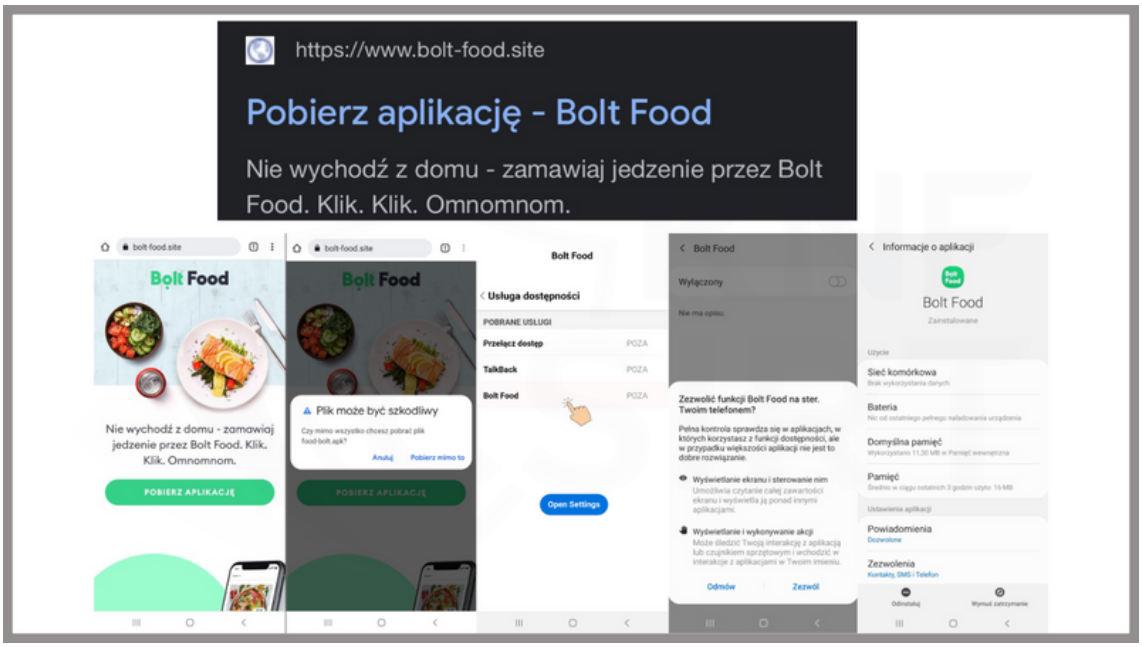
ERMAC v2

Trojan ERMAC v2 jest złośliwym oprogramowaniem atakującym urządzenia mobilne działające pod kontrolą systemu Android. Popularnym sposobem dystrybucji ERMACa v2 było podszywanie się pod aktualizacje oprogramowania oraz popularne aplikacje mobilne. Wspólnym mianownikiem technik używanych przez atakujących, było w tym wypadku nakłonienie ofiary do pobrania i instalacji aplikacji spoza oficjalnego sklepu Google Play. Złośliwe oprogramowanie po uruchomieniu usiłowało wymusić na użytkowniku przyznanie uprawnień do systemowej funkcji "Dostępność". Jeżeli ofiara dała się wprowadzić w błąd, udzielając fałszywej aplikacji wymaganej zgody, następowało przejęcie kontroli nad zainfekowanym urządzeniem. Złośliwe oprogramowanie zyskując możliwość wchodzenia w interakcje z oknami wyświetlanymi na ekranie urządzenia, samodzielnie wyrażało zgodę na przyznanie kolejnych, krytycznych uprawnień. W konsekwencji ERMAC mógł uzyskać dostęp do kontaktów, SMS-ów czy danych uwierzytelniających ofiary.

Jedną z funkcji pozwalających na potencjalne przejęcie danych, było wyświetlanie fałszywych formularzy logowania. Wspomniane formularze potrafiły przykrywać prawdziwe aplikacje uruchamiane przez użytkownika, np. rozwiązania do obsługi bankowości elektronicznej. Malware skutecznie utrudniał przywrócenie urządzenia do ustawień fabrycznych. W minionym roku trzykrotnie informowaliśmy o kampaniach z użyciem ERMACa. Dwukrotnie trojan podszywał się pod aplikację BoltFood [10], [11], wykorzystując do tego fałszywą stronę internetową, na którą ofiara trafiała np. za pośrednictwem oszukańczej reklamy wyświetlanej w wynikach wyszukiwarki Google. W przypadku jednej z kampanii, w której ERMAC podszywał się pod przeglądarkę Google Chrome, opublikowaliśmy krótki film edukacyjny, ilustrujący działanie złośliwego oprogramowania [12].

10. https://twitter.com/CSIRT_KNF/status/1527201315331383297
11. https://twitter.com/CSIRT_KNF/status/1528990782153183232
12. https://www.youtube.com/watch?v=P1BSuCexaW0

Złośliwe oprogramowanie



Grafika 35. Ilustracja złośliwej kampanii i uzyskane przez aplikację niebezpieczne uprawnienia.

Fałszywa aplikacja w Google Play

W drugiej połowie września 2022 ostrzegaliśmy przed fałszywą aplikacją mobilną, wykorzystującą wizerunek firmy Smartney [13]. Aplikacja została opublikowana w sklepie Google Play. Oszuści wykorzystywali aplikację w celu wyłudzenia danych od użytkowników.

Grafika 36. Ilustracja złośliwej kampanii podszywającej się pod firmę Smartney.

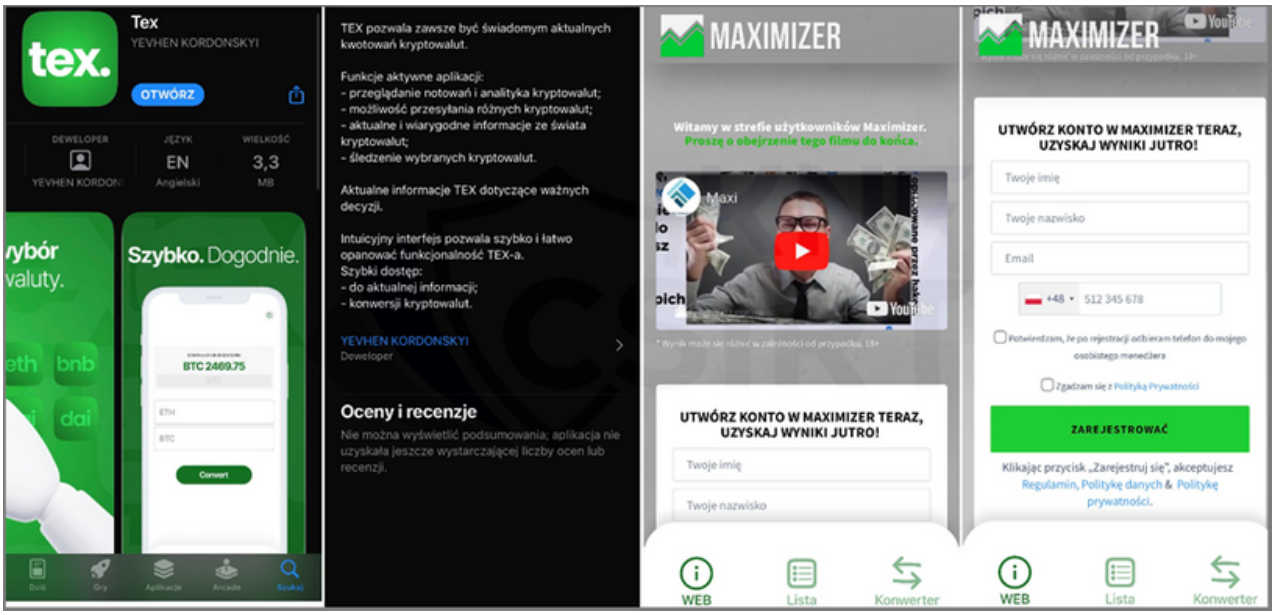
13. https://twitter.com/CSIRT_KNF/status/1570703511343734790

Złośliwe oprogramowanie

Fałszywa aplikacja w App Store

Trzeci kwartał roku to także fałszywa aplikacja w sklepie AppStore [14]. Była to pierwsza, zidentyfikowana przez nas aplikacja na iOS, wykorzystywana w oszustwie na tzw. fałszywe inwestycje.

Poniżej publikujemy zrzuty ekranu z oszukańczego produktu.



Grafika 37. Zidentyfikowana przez nas fałszywa aplikacja na iOS.

14. https://twitter.com/CSIRT_KNF/status/1570788436432551938

Złośliwe oprogramowanie

Częstym celem ataków złośliwego oprogramowania są także komputery użytkowników. Najczęściej dystrybuowane są one za pośrednictwem różnego rodzaju wiadomości zawierających załączniki lub też pliki prowadzące do złośliwych plików. W 2022 roku obserwowaliśmy liczne kampanie złośliwego oprogramowania dystrybuowanego za pośrednictwem wiadomości e-mail. Wśród najpopoularniejszych odmian wyróżnić można oprogramowanie QakBot, AgentTesla czy Redline Stealer, który specjalizuje się w wykradaniu haseł zapisanych przez użytkownika.

Rok 2022 to także intensywny rozwój złośliwego oprogramowania typu wipper, które w intensywny sposób było wykorzystywane do ataków na podmioty z sektora energetycznego i finansowego na terenie Ukrainy. Jednym z popularniejszych „wiperów" był CaddyWiper, którego najważniejsze fragmenty kodu i funkcjonalność została opisana w raporcie CSIRT KNF:

https://www.knf.gov.pl/dla_rynku/CSIRT_KNF/Aktualnosci?articleId=77763&p_id=18

Grafika 38. Zrzut ekranu przedstawiający stronę knf.gov.pl, na której opublikowany został raport CSIRT KNF.

Kampania Qbot wykorzystująca technikę reply-chain

W marcu 2022 miała miejsce masowa kampania złośliwego oprogramowania dystrybuowanego za pośrednictwem wiadomości e-mail. To, co jest charakterystyczne dla tej kampanii to wykorzystanie techniki reply-chain. Technika ta polega na wykorzystaniu treści wiadomości wykradzionych z innych systemów do uwiarygodnienia wiadomości phishingowej. Mail ze złośliwym linkiem przesyłany jest w taki sposób, że wygląda jak kontynuacją wcześniejszej korespondencji. W ten sposób atakującym prościej jest przekonać użytkownika do uruchomienia złośliwego załącznika.

Przesyłana w ramach tej kampanii wiadomość zawierała link prowadzący do złośliwego oprogramowania Qbot, w samej zaś treści znajdowało się hasło do jego uruchomienia.

From:
Sent: Friday, March 11, 2022 11:17 AM
To:
Subject: Re:

[EXTERNAL EMAIL]

Dobry dzieÅ„!
SprawdÅ° pilne oÅ›wiadczenie, proszÄ™:

https://onedrive.live.com/download?cid=B254C53B6D2CFBAA&resid=B254C53B6D2C
21120&authkey=AARC3PTeoXvr5AM

HasÅ‚o pliku.: DH5566

Grafika 39. Treść wiadomości e-mail, którą otrzymywała ofiara.

Złośliwe oprogramowanie

Fałszywe wiadomości e-mail z wykorzystaniem wizerunku banku

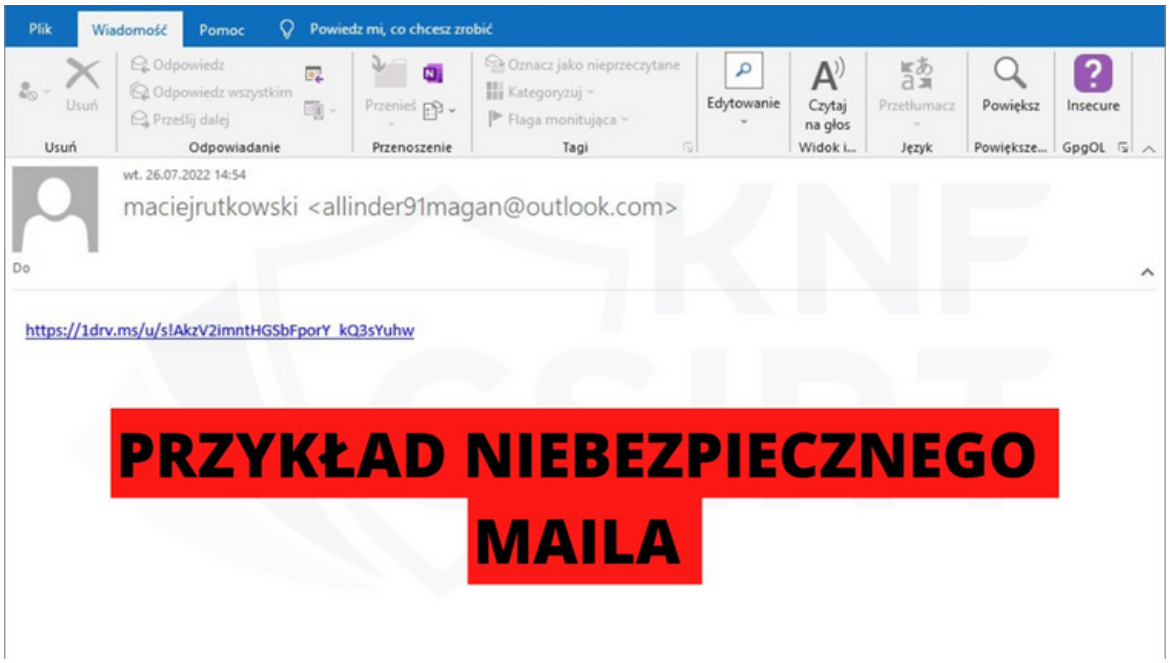
Cyberoszuści wykorzystywali również pocztę elektroniczną do dystrybucji szkodliwego oprogramowania na urządzenia mobilne. Przesyłane w wiadomościach niebezpieczne załączniki lub linki kierowały do pobrania złośliwego oprogramowania. Wśród pojawiających się należy wskazać na fałszywe oprogramowanie Agent Tesla, QakBot czy Formbook.

Na poniższym zrzucie ekranu znajduje jest treść fałszywej wiadomości e-mail, podszywającej się pod bank Pekao. Użytkownicy informowani byli o rzekomo załączonej kopii polecenia wypłaty. W rzeczywistości pod ikoną pliku XLSX krył się link, który zawierał złośliwe oprogramowanie Agent Telsa, przejmujące kontrolę nad urządzeniem i przechwytujące hasła do bankowości elektronicznej.

Grafika 40. Fałszywa wiadomość e-mail, w której cyberprzestępcy podszywali się pod bank Pekao.

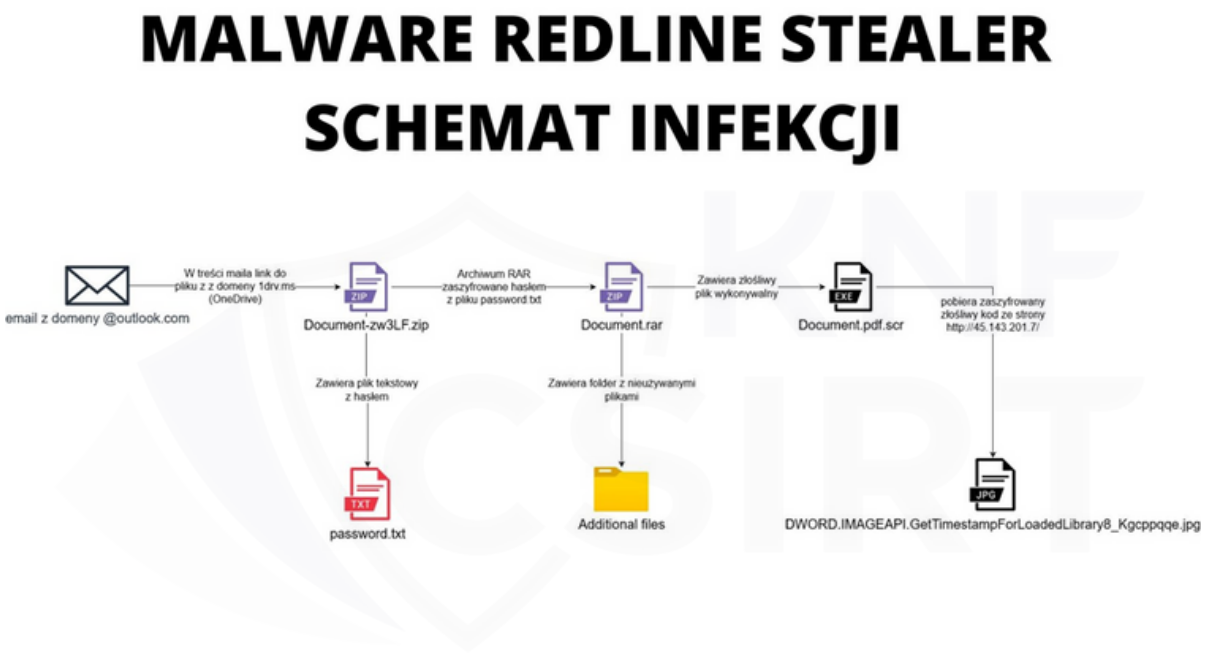
Redline Stealer - złośliwe oprogramowanie wykradające hasła

Stealery to rodzaj złośliwego oprogramowania specjalizującego się w wykradaniu haseł z komputera ofiary. Tego typu oprogramowanie cieszyło się dużą popularnością w 2022 roku. W lipcu rozsyłane były wiadomości bez tytułu, w treści zawierające tylko hiperłącze. Po kliknięciu pobierane było archiwum ZIP, zawierające plik tekstowy z hasłem do znajdującego się w tym samym miejscu zaszyfrowanego archiwum ZIP. Dopiero tam zaszyty był plik wykonywalny Document.pdf.scr będący złośliwym oprogramowaniem Redline Stealer.



Grafika 41. Przykład wiadomości wykorzystywanej do dystrybucji złośliwego oprogramowania Redline Stealer.

Złośliwe oprogramowanie

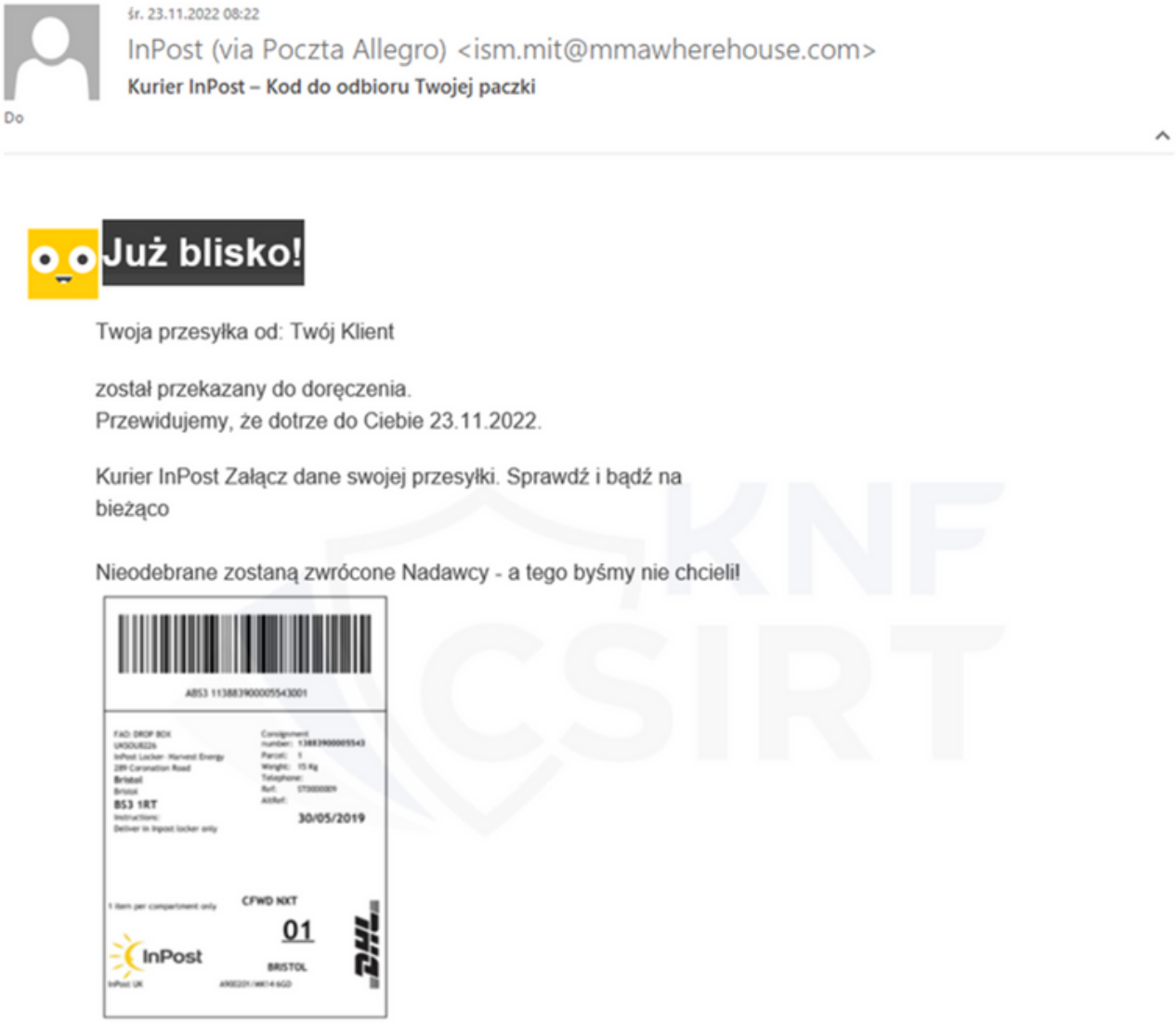


Grafika 42. Schemat infekcji - malware Redline Stealer.

Wykorzystanie wizerunku firm kurierskich do dystrybucji złośliwego oprogramowania

Cyberprzestępcy bardzo często wykorzystują także wizerunki firm kurierskich. W listopadzie informowaliśmy o kampanii wykorzystującej wizerunek firmy kurierskiej InPost. W treści znajdował się obrazek udający etykietę, po kliknięciu którego pobierane było złośliwe oprogramowanie FormBook.

Złośliwe oprogramowanie



Grafika 43. Treść fałszywej wiadomości e-mail podszywającej się pod firmę kurierską InPost.

Jak się chronić przed złośliwym oprogramowaniem?

Zachęcamy do stosowania dobrych praktyk w zakresie ochrony przed szkodliwym oprogramowaniem. Poniższe wskazania nie eliminują wszelkich potencjalnych wariantów stosowanych przez adwersarzy, pomagają natomiast niwelować wiele z nich, a tym samym podnosić bezpieczeństwo użytkownika.

01. Weryfikuj adresy odwiedzanych stron internetowych (szczególną uwagę zwracaj na nazwę domeny)

02. Nie klikaj w linki i załączniki, które wzbudzają Twoją wątpliwość i takie, których się nie spodziewałeś

03. Korzystaj z programu antywirusowego i dbaj o jego aktualizację

04. Zrezygnuj z wprowadzania zmian, obniżających bezpieczeństwo Twojego urządzenia (np. wyrażania zgody na instalację aplikacji pochodzących z tzw. niezaufanych źródeł)

05. Uważaj jakie uprawnienia przydzielasz instalowanym aplikacjom (w przypadku urządzeń mobilnych jednym z czynników zwiększających ryzyko infekcji jest udzielanie zgody na dostęp do uprawnień określanych jako Dostępność / Ułatwienia Dostępu / Accessibility Services)

06. Zadbaj o prawidłowo wykonane i bezpiecznie przechowywane kopie zapasowe

07. Pamiętaj o aktualizacjach systemu i oprogramowania

05. ZAGROŻENIA I REKOMENDACJE ODNOŚNIE DO ATAKÓW DDOS ORAZ DZIAŁANIA HAKTYWISTÓW POD KĄTEM WOJNY W UKRAINIE

Zagrożenia i rekomendacje odnośnie do ataków DDoS oraz działania haktywistów pod kątem wojny w Ukrainie

Ataki DDoS/DoS...

Przedsiębiorstwa prywatne, podmioty administracji publicznej, rynku finansowego i wiele innych podmiotów przetwarza ogromne ilości informacji, dodatkowo obecne czasy i rosnąca potrzeba bycia konkurencyjnym, ale i zapewnienia rzetelnych informacji u źródła sprawiają, że tzw. „obecność organizacji w Internecie" staje się nieodłącznym elementem prowadzenia działalności. Dlatego tak ważnym jest, aby zadbać o zachowanie trzech elementarnych zasad bezpieczeństwa informacji: poufności, integralności i dostępności. Na potrzeby tego artykułu skupimy się tylko na trzecim elemencie, czyli potrzebie zapewnienia dostępności. Jak mówi definicja „dostępność, to właściwość wskazująca na to, że określone dane mogą być wykorzystywane przez osoby w określonym czasie i w określony sposób". Oznacza to umożliwienie dostępu do danych i dokonywanie na nich operacji. Co do zasady jest to prawda, należy jednak mieć na uwadze, że wiele podmiotów musi zapewnić stałą (tj. 24h/7/365) dostępność swoich zasobów dla klientów. Potrzeba ta rodzi oczywiście możliwości do prowadzenia ataków cybernetycznych, która chętnie jest wykorzystywana, jak pokazał nam rok 2022. Mowa o popularnym rodzajów działań cyberprzestępców, czyli atakach odmowy dostępu Denial of Service (DoS) oraz Distributed Denial of Service (DDoS). W uproszczeniu, ataki DDoS/DoS można scharakteryzować jako działanie przestępcze mające na celu spowodowanie czasowej niedostępności systemów teleinformatycznych i usług organizacji świadczonych drogą elektroniczną.

Niedostępność usługi sieciowej można wykonać na klika sposobów. Biorąc pod uwagę warstwę modeli OSI rozróżnia się ataki:

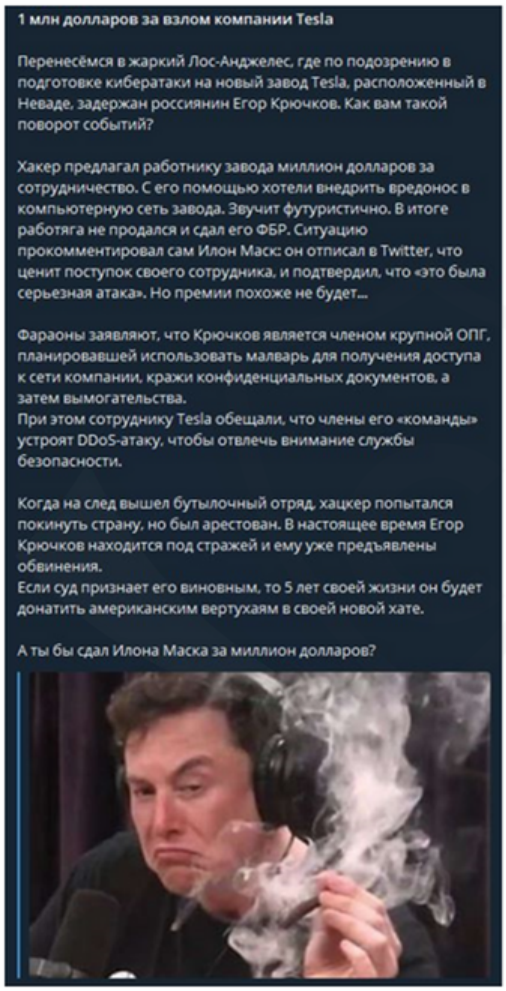
- Wolumetryczne – są to ataki ilościowe, wykonywane najczęściej w warstwie sieciowej L3 lub transportowej L4,
- Aplikacyjne – są to ataki jakościowe, wykonywane w warstwie aplikacji L7.

Wysoko wykwalifikowani atakujący zwykle łączą ataki wolumetryczne i aplikacyjne. W istocie skupiają się jednak na atakach na poziomie aplikacji, które wyrządzają rzeczywiste szkody.

W zasadzie po co te ataki DDoS/DoS...

Jak można przeczytać na forach przestępczych (po tłumaczeniu): „Motywem ataku DDoS może być wszystko, od cyber-chuligaństwa po wymuszenie." Jednym z nich jest chęć odwrócenia uwagi ofiary. Książkowym wręcz przykładem jest próba ataku hakerskiego na Teslę, z 2020 roku. Zaplanowany atak DDoS miał na celu zaabsorbowanie działu bezpieczeństwa Tesli do tego stopnia, aby ten nie zauważył wyprowadzania dużej ilości dokumentów poufnych (grafika 44).

Zagrożenia i rekomendacje odnośnie do ataków DDoS oraz działania haktywistów pod kątem wojny w Ukrainie



TŁUMACZENIE:

„(...) obywatel Rosji Egor Kryuchkov został zatrzymany pod zarzutem przygotowywania cyberataku na nową fabrykę Tesli w Nevadzie. Co sądzicie o takim obrocie spraw?

Haker oferował pracownikowi fabryki milion dolarów za współpracę. Zamierzali wykorzystać go do zainfekowania sieci komputerowej fabryki złośliwym oprogramowaniem. (...)

(...) Kruchkov jest członkiem dużej zorganizowanej grupy przestępczej, która planowała wykorzystać złośliwe oprogramowanie do uzyskania dostępu do sieci firmy, wykraść poufne dokumenty, a następnie wyłudzić pieniądze.

W tym samym czasie pracownikowi (...) członkowie jego "zespołu" przeprowadzali atak DDoS, aby odwrócić uwagę. (...)"

Grafika 44. Odwrócenie uwagi w celu przeprowadzenia ataku.

Kolejnym motywem ataku jest chęć zastraszenia ofiary oraz wymuszenie zapłaty za nieprzeprowadzenie lub przerwanie działania. Nie można zapomnieć również o motywacjach politycznych, te z kolei mają najczęściej na celu pokazanie siły przeciwnika i/lub wprowadzenie chaosu w organizacji ofiary. Motywów działania można wymieniać jeszcze wiele, ale warto skupić się na powodzie wyboru tego typu działalności przestępczej.

Zagrożenia i rekomendacje odnośnie do ataków DDoS oraz działania haktywistów pod kątem wojny w Ukrainie

Ataki DDoS/DoS są stosunkowo najtańszymi z dostępnych metod przestępczych, jak i najprostszymi do zorganizowania, przy jednoczesnym zachowaniu tego, co dla atakującego jest najważniejsze, czyli skuteczność i osiągnięcie celu. Obecnie nie jest już nadużyciem powiedzieć, że atak DDoS na wybraną organizację może przeprowadzić każdy. Jeżeli nie ma umiejętności technicznych i wiedzy, może wynająć usługę (grafika 45). Jeżeli nie stać go na wynajęcie usługi, może się sam douczyć i przy zmniejszonych kosztach wykonać atak samodzielnie. Oczywiście, od tego w dużej mierze uzależniona jest skuteczność działania przestępczego.

Grafika 45. Przykładowe oferty przeprowadzenia ataków DDoS.

Jak walczyć z atakami typu DDoS, czyli „Dobre praktyki w zakresie przeciwdziałania atakom DDoS" przygotowywane przez CSIRT KNF, we współpracy z ekspertami telekomunikacyjnymi...

W związku z pojawiająca się potrzebą, w lutym 2022 roku, CSIRT KNF we współpracy ze specjalistami ds. telekomunikacji przygotował i przekazał do użytku publicznego dokument opisujący koncepcje, narzędzia i techniki chroniące przed atakami DDoS. Zawarte została w nim lista wskazówek jakie komponenty warto wziąć pod uwagę wzmacniając odporność infrastruktury organizacji na ataki, czy wykonując analizę ryzyka, aby ocenić przygotowanie organizacji w poszczególnych obszarach.

Zagrożenia i rekomendacje odnośnie do ataków DDoS oraz działania haktywistów pod kątem wojny w Ukrainie

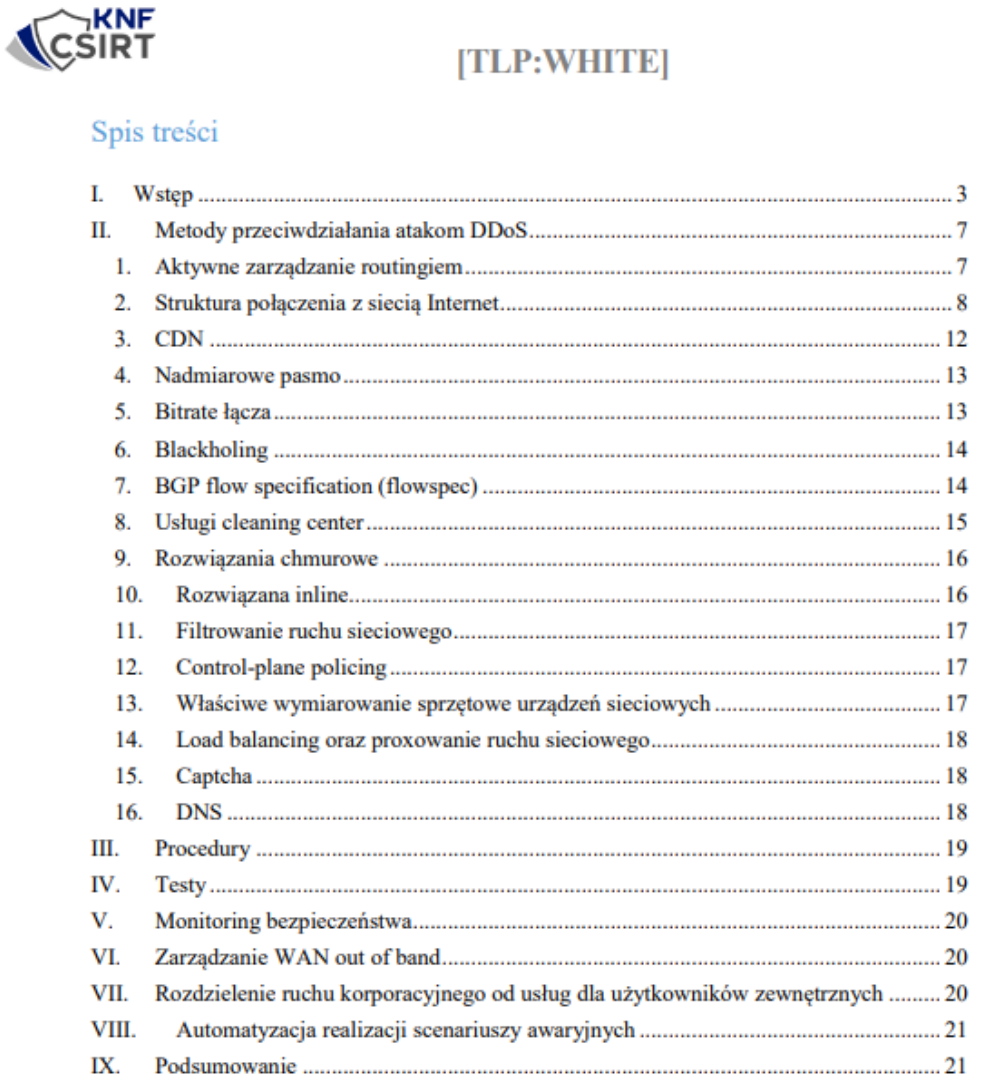
Znalazły się tam m.in.:

- aktywne zarządzanie routingiem
- struktura połączenia z siecią Internet
- mechanizmy CDN (Content Delivery Network)
- nadmiarowe pasmo w odniesieniu do konkretnego łączą telekomunikacyjnego
- bitrate łącza (rozumiany jako ilość bitów jaką można przesłać w jednostce czasu)
- blackholing
- BGP flow specification (flowspec)
- usługi cleaning center
- rozwiązania chmurowe
- rozwiązana inline
- filtrowanie ruchu sieciowego
- control-plane policing
- właściwe wymiarowanie sprzętowe urządzeń sieciowych
- load balancing oraz proxowanie ruchu sieciowego
- zastosowanie zabezpieczenia captcha
- wdrożenie architektury rozproszonej serwisu DNS

W materiale uwzględniono również potrzebę odpowiedniego przygotowania i stosowania procedur na wypadek wystąpienia ataku, zwracając uwagę na to, że w trakcie trwania takiego ataku ważnym jest zapewnienie monitorowania bezpieczeństwa infrastruktury i usług w stopniu nie gorszym niż przy standardowym ruchu użytkowników i bezawaryjnym świadczeniu usług, celem wykrycia ewentualnych innych działań przestępczych. Zaznaczono również ważność określenia i realizowania harmonogramu regularnych i cyklicznych testów. Uwzględniono potrzebę zapewnienia możliwości zarządzania infrastrukturą teleinformatyczną (np. zarządzanie siecią WAN) w przypadku ataku DDoS, poprzez zapewnienie alternatywnych (zapasowych, nadmiarowych) łącz wykorzystywanych dla celów administracyjnych, które powinny być odrębne od pasma wykorzystywanego do świadczenia usług organizacji. Podobnie jak rozdzielenie ruchu korporacyjnego od usług dla użytkowników zewnętrznych.
Należy mieć jednak na uwadze, że nie istnieją gotowe, kompleksowe rozwiązania ani jedna uniwersalna metoda ochrony przed atakami typu DDoS. Budowanie infrastruktury odpornej na ataki nie może być sprowadzone wyłącznie do kupienia gotowego produktu czy usługi, lecz powinno być systemowym podejściem do zaprojektowania całego łańcucha technologicznego odpowiedzialnego za dostarczenie ostatecznej usługi, tworząc wielowarstwową ochronę organizacji zgodnie z zasadą defence in depth.

Zagrożenia i rekomendacje odnośnie do ataków DDoS oraz działania haktywistów pod kątem wojny w Ukrainie

Zachęcamy do zapoznania się z całością dokumentu (przygotowanego w dwóch wersjach językowych) pod adresem:
https://www.knf.gov.pl/dla_rynku/CSIRT_KNF/AktualnosciarticleId=77245&p_id=18



KNF CSIRT

[TLP:WHITE]

Spis treści

I. Wstęp ... 3
II. Metody przeciwdziałania atakom DDoS ... 7
1. Aktywne zarządzanie routingiem ... 7
2. Struktura połączenia z siecią Internet ... 8
3. CDN ... 12
4. Nadmiarowe pasmo ... 13
5. Bitrate łącza ... 13
6. Blackholing ... 14
7. BGP flow specification (flowspec) ... 14
8. Usługi cleaning center ... 15
9. Rozwiązania chmurowe ... 16
10. Rozwiązana inline ... 16
11. Filtrowanie ruchu sieciowego ... 17
12. Control-plane policing ... 17
13. Właściwe wymiarowanie sprzętowe urządzeń sieciowych ... 17
14. Load balancing oraz proxowanie ruchu sieciowego ... 18
15. Captcha ... 18
16. DNS ... 18
III. Procedury ... 19
IV. Testy ... 19
V. Monitoring bezpieczeństwa ... 20
VI. Zarządzanie WAN out of band ... 20
VII. Rozdzielenie ruchu korporacyjnego od usług dla użytkowników zewnętrznych ... 20
VIII. Automatyzacja realizacji scenariuszy awaryjnych ... 21
IX. Podsumowanie ... 21

Grafika 46. Raport CSIRT KNF dotyczący dobrych praktyk w zakresie przeciwdziałania atakom DDoS.

Zagrożenia i rekomendacje odnośnie do ataków DDoS oraz działania haktywistów pod kątem wojny w Ukrainie

Wojna w Ukrainie

W lutym 2022 roku większość świata zwróciła swoje oczy w stronę Ukrainy, gdzie Rosja rozpoczęła fizyczną inwazję. Jednak już na kilka dni wcześniej wojna ta rozpoczęła się w cyberbprzestrzeni. I o ile większość współczuła naszym sąsiadom za wschodniej granicy, starając się wesprzeć ich w walce, o tyle kraje jak Polska musiały również zadbać o swoje bezpieczeństwo, zarówno fizyczne jak i cyber. Tak rozpoczęto wprowadzanie kolejnych progów alarmowych [15], a zespoły takie jak CSIRT KNF rozpoczęły prace analityczne mające na celu wykrywanie zagrożenia dla sektora finansowego.

Haktywiści do broni...

W wojnie w cyberprzestrzeni szybko do głosu doszli haktywiści [16]. Początkowo pojedyncze zespoły przerodziły się w dziesiątki grup opowiadające się zarówno za stroną ukraińską, jak i rosyjską. Grupy prorosyjskie początkowo prowadziły narracje obrony swojego kraju, informując, że będą atakować tylko te kraje, które zaatakowały Rosję, narracja ta jednak z czasem się zmieniła i z teoretycznego obrońcy, stali się agresorami, którzy podejmowali swoje działania jako pierwsi. Często wybór kraju jakie obierają haktywiści wynika z działań politycznych np. wypowiedź, którą uznają za wrogą, przekazanie pomocy Ukrainie. Głównymi zadaniami jakie wyznaczyli sobie członkowie grup prorosyjskich była dezinformacja, hakowanie oraz ataki DDoS. Działania dezinformacyjne dotyczą głównie obszarów wojskowych oraz próby nakłonienia społeczeństwa do uwierzenia w nieczyste zamiary Polski. O ile w Ukrainie ta dezinformacja była mocno krzewiona, o tyle w Polsce nie pojawiały się takie sytuacje, tym bardziej wpływające na sektor finansowy. W zakresie hakowania pierwsza, i najdłużej aktywna grupa haktywistów jaka podejmowała działania i o nich informowała, była grupa XakNet. Jednak w zakresie działań w Polsce, tym bardziej dotykających obszaru cyberbezpieczeństwa, nie stwierdzono żadnych naruszeń. Dlatego na potrzeby tego raportu skupimy się na atakach typu DDoS, w związku z tym, że tych było zdecydowanie najwięcej i miały pewien, chociaż nie krytyczny, wpływ na podmioty sektora finansowego w Polsce.

15. Premier Mateusz Morawiecki podpisał zarządzenie wprowadzające trzeci stopień alarmowy CRP (CHARLIE–CRP) na terytorium całego kraju, które obowiązuje do momentu pisania artykułu. Stopnie alarmowe CRP dotyczą zagrożenia w cyberprzestrzeni. Stopień CHARLIE–CRP jest trzecim z czterech stopni alarmowych określonych w ustawie o działaniach antyterrorystycznych. Stopień ten jest wprowadzany w przypadku wystąpienia zdarzenia potwierdzającego prawdopodobny cel ataku o charakterze terrorystycznym w cyberprzestrzeni albo uzyskania wiarygodnych informacji o planowanym zdarzeniu. [gov.pl]

16. Haktywizm to połączenie aktywizmu społeczno-politycznego z hakerstwem, co powoduje problemy w zdefiniowaniu tego zjawiska. Z jednej strony bowiem jest on określany jako przejaw internetowej mobilizacji, a z drugiej termin ten opisuje działania przestępcze w przestrzeni wirtualnej. Haktywiści stosują bowiem metody wywodzące się z hakerstwa, ale wyróżnia ich polityczna motywacja. [Piotrowska, M.: Haktywizm – społeczna korzyść czy zagrożenie?, Studia Humanistyczne AGH 2017]

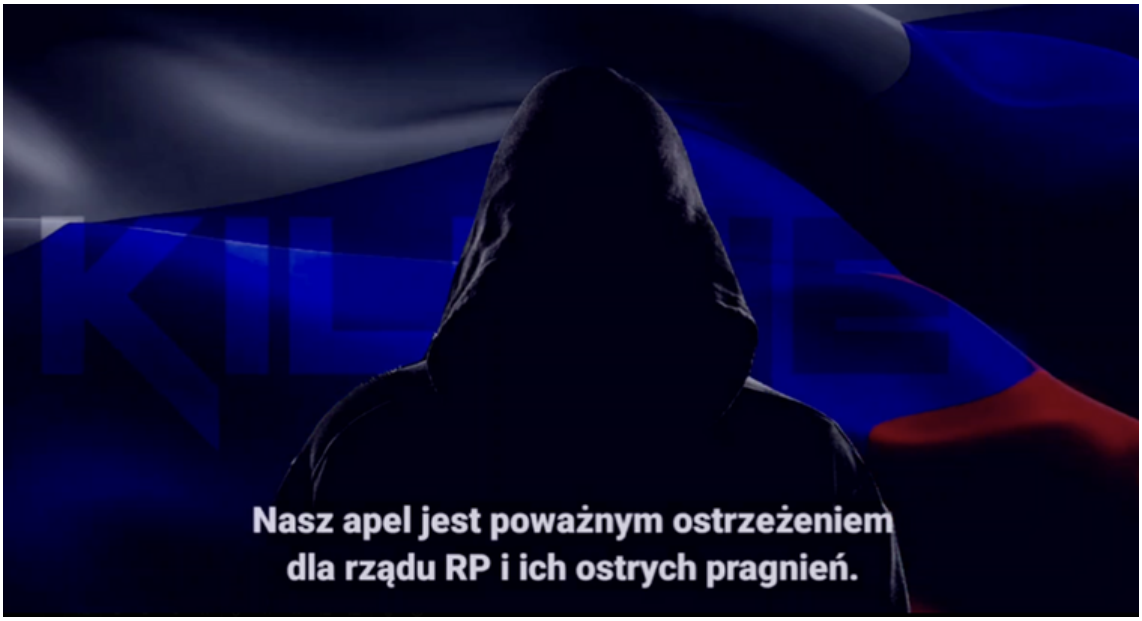
Zagrożenia i rekomendacje odnośnie do ataków DDoS oraz działania haktywistów pod kątem wojny w Ukrainie

Dlaczego DDoSy....

Jak już wspomnieliśmy, w bardzo krótkim czasie powstało wiele grup haktywistow. Następnie grupy te zaczęły tworzyć sojusze, porozumienia, łączyć się, współpracować, dzielić zadania. Zdecydowana większość grup zajęła się przeprowadzaniem ataków typu DDoS. Wynika to ze stosunkowej prostoty tego typu działania. Osoby, które uczestniczą w grupach często nie maja wiedzy technicznej w zakresie przeprowadzania cyberataków, a odpowiednio przygotowane narzędzie do działań typu ataki DDoS, pozwala im na podejmowanie kroków, bez wiedzy jakie procesy dokładnie zachodzą na ich urządzeniach.

DDoSy w Polsce i w sektorze finansowym...

Początek wojny to również czas kiedy ataki w cyberprzestrzeni skupione były stricte przeciwko Ukrainie, z czasem jednak haktywiści zaczęli wychodzić poza ten obszar i atakować również sojuszników naszych wschodnich sąsiadów. Właśnie dlatego w krótkim czasie polskie strony także pojawiły się w zakresie zainteresowania prorosyjskich haktywistów. Pierwszy apel rosyjski skierowany do Polski, z szantażem którego wynikiem miało być nasze wycofanie się w pomocy Ukrainie opublikowała jednak z pierwszych i najbardziej znanych grup – Killnet. Filmik został udostępniony w dniu 23.03.2022, na ich kanale, w aplikacji Telegram (grafika 47).



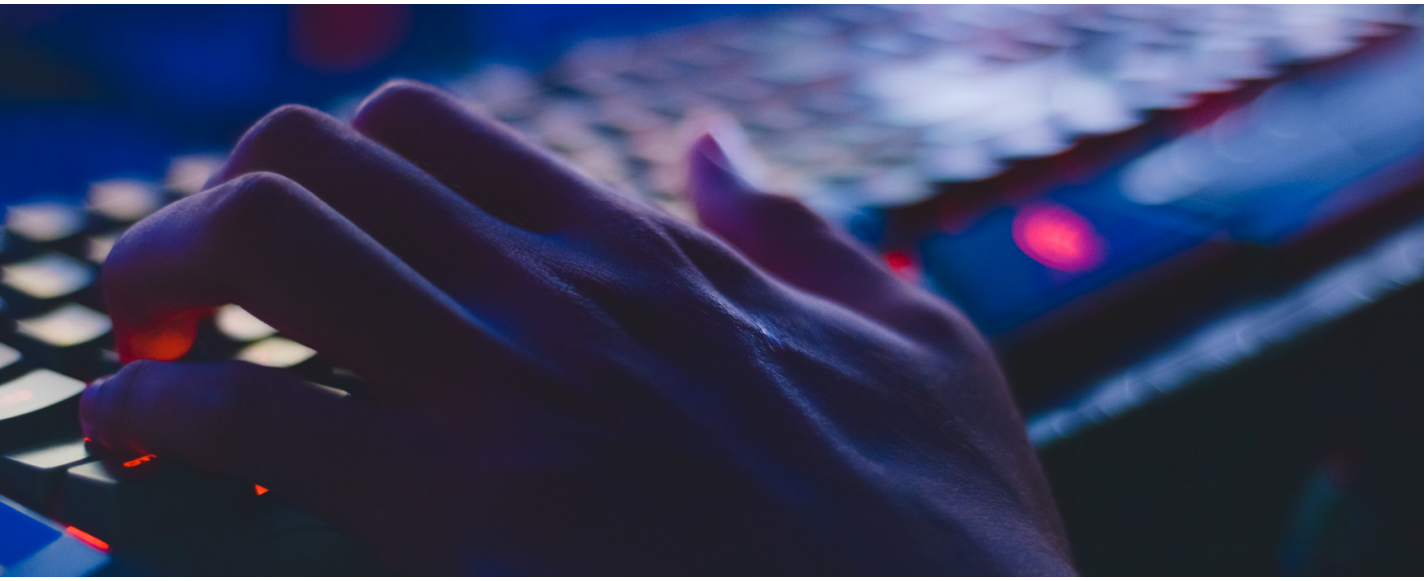
Grafika 47. Filmik grupy Killnet wzywający Polskę do wycofania się z pomocy Ukrainie.

Zagrożenia i rekomendacje odnośnie do ataków DDoS oraz działania haktywistów pod kątem wojny w Ukrainie

Na kanałach telegramowych zarówno grupy Killnet, jak i innych, domeny polskie jako cel ataku, zaczęły pojawiać się coraz częściej. To na czym zależy tym atakującym to rozgłos, dlatego też wyniki swoich działań opisują w nierzetelny sposób, m.in. w kwietniu 2022 na profilach prorosyjskich haktywistów można było przeczytać o rzekomym paraliżu sektora transportowego w Polsce. W rzeczywistości mowa była o ataku DDoS, który faktycznie się odbył, ale tylko na strony informacyjne wybranych lotnisk polskich, nie mając żadnego wpływu na logistykę lotów, a już tym bardziej na bezpieczeństwo transportu. Podobnie dzieje się w przypadku innych celów. Oczywiście ataki skierowane były również w strony należące do podmiotów z sektora finansowego. Jedną z pierwszych stron, która została zaatakowana po opublikowaniu wspomnianego filmu z szantażem, była strona Narodowego Banku Polskiego. Jednak, co ważne, podobnie jak w przypadku ataku na strony informacyjne lotnisk, również w sektorze finansowym, jeżeli nawet atak przeprowadzony był skutecznie i obrany cel był niedostępny, to nie miało to krytycznego znaczenia dla funkcjonowanie banków, systemów rozliczeń w Polsce, czy innych procesów. Mogło to stanowić najwyżej chwilową niedogodność dla osób odwiedzających w tym czasie te strony. Ataki jednak, co do zasady, nie trwały długo, dlatego wnioskujemy, że co do niektórych działań haktywstów nikt (bądź liczba osób bliska zeru) nie odczuł konkretnej niedostępności.

Nie karmmy potwora

Od inwazji fizycznej, a jednocześnie wojny w cyberprzestrzeni minęło kilka miesięcy. Od tego czasu haktywiści nie podjęli żadnych działań, które miałyby jakiekolwiek wpływ na funkcjonowanie kraju, czy atakowanych organizacji. Jednak to, co jest ich celem, to osiąganie medialnego rozgłosu, z ich perspektywy najlepiej z przekazem, który sami kreują o swoich możliwościach i mocy.



Zagrożenia i rekomendacje odnośnie do ataków DDoS oraz działania haktywistów pod kątem wojny w Ukrainie

Nie karmmy potwora

Jedna ze złotych zasad cyberbezpieczeństwa mówi, że nie wolno lekceważyć żadnego wroga – my w pełni się z nią zgadzamy i nawet haktywistów, którzy od kilku miesięcy nie wykazali się istotnymi działaniami, nie lekceważymy, na bieżąco śledzimy i podejmujemy odpowiednie kroki. Apelujemy jednak do mediów, organizacji które stały się lub mogą stać atakiem tych grup przestępczych, jak i wszystkich, którzy mają zasięgi w Internecie o rzetelne i nieprzebarwione przedstawianie podejmowanych przez haktywistów działań.

06. DZIAŁANIA EDUKACYJNE CSIRT KNF W 2022 ROKU

Działania edukacyjne CSIRT KNF w 2022 roku

Działania edukacyjne są jednym z istotnych elementów budowania cyberbezpieczeństwa. Wraz z rosnącą liczbą zagrożeń z roku na rok, koniecznym staje się ciągłe podnoszenie świadomości użytkowników cyberprzestrzeni. Zespół CSIRT KNF prowadzi szereg działań mających na celu edukowanie i informowanie w zakresie cyberzagrożeń w sektorze finansowym.

Zespół CSIRT KNF przeprowadził w 2022 roku szereg działań szkoleniowych mających na celu poprawę świadomości odnośnie do zagrożeń cyberbezpieczeństwa dla przyszłych i obecnych klientów instytucji finansowych. W ramach projektu edukacyjnego Centrum Edukacji dla Uczestników Rynku - CEDUR, realizowanego przez Urząd Komisji Nadzoru Finansowego przeprowadzono szkolenia online, w trakcie których przedstawione zostały zagadnienia z zakresu cyberbezpieczeństwa, ochrony środków finansowych klientów i działania złośliwego oprogramowania. Seminaria skierowane były w szczególności do uczniów szkół ponadpodstawowych oraz nauczycieli, seniorów, a także instytucji ochrony praw nieprofesjonalnych uczestników rynku finansowego.

Przedstawiciele CSIRT KNF w ramach działań edukacyjnych uczestniczyli w wielu inicjatywach o zasięgu krajowym i zagranicznym, których celem było rozpowszechnianie wiedzy z zakresu cyberbezpieczeństwa rynku finansowego, z których wymienić można m.in.:

Magazyn Kryminalny

W ramach serii wystąpień przedstawiciele zespołu CSIRT KNF omówili najpopularniejsze oszustwa wymierzone w nieprofesjonalnych uczestników rynku finansowego. W poszczególnych odcinkach zostały poruszone następujące zagadnienia:

- oszustwa SMS – wskazano jakie działania należy podjąć aby nie paść ofiarą cyberprzestępców,
- oszustwa na portalach sprzedażowych – przedstawiono najczęściej występujące scenariusze ataków,
- oszustwa telefoniczne – wskazano na metody pozwalające na rozpoznanie fałszywego konsultanta,
- fałszywe inwestycje – przedstawiono możliwe metody ochrony przed cyberprzestępcami.

Światowy Dzień Konsumenta

W ramach Światowego Dnia Konsumenta przeprowadzony został wykład pt. „Sposoby kradzieży środków finansowych w cyberprzestrzeni – Jak nie dać się okraść w Internecie”, w trakcie którego przybliżone zostały najważniejsze zasady pozwalające konsumentom na bezpieczne funkcjonowanie na rynku usług finansowych. Wskazano również na najpopularniejsze metody stosowane przez cyberprzestępców.

Działania edukacyjne CSIRT KNF w 2022 roku

Global Money Week 2022

Przedstawiciele Zespołu CSIRT KNF uczestniczyli w 10. edycji międzynarodowej kampanii poświęconej budowaniu świadomości finansowej [17]. W ramach GMW 2022 przeprowadzone zostały webinaria:

- „Cyberoszuści atakują – jak nie dać się okraść w Internecie" skierowane do uczniów szkół ponadpodstawowych i nauczycieli. Omówione zostały najczęściej występujące oszustwa w Internecie, a także wskazano na dobre praktyki w obszarze bezpieczeństwa środków finansowych.
- „Bezpieczny telefon – jak chronić się przed cyberprzestępcami" skierowane do młodzieży mające na celu poszerzenie świadomości w zakresie oszustw wymierzonych w użytkowników urządzeń mobilnych. Podczas szkolenia omówione zostały najczęściej występujące zagrożenia cyberbezpieczeństwa dla środków finansowych użytkowników. Wskazano na dobre praktyki pozwalające na uchronienie się przed złośliwym oprogramowaniem.

Locked Shields

Polska na drugim miejscu na świecie! Olbrzymi sukces polskich specjalistów od cyberbezpieczeństwa, którzy zajęli drugie miejsce w największych organizowanych przez NATO, międzynarodowych ćwiczeniach obszaru cyberbezpieczeństwa „Locked Shields 2022". W dniach 19-22 kwietnia przedstawiciele Departamentu Cyberbezpieczeństwa UKNF wzięli udział w największych na świecie ćwiczeniach z obszaru cyberbezpieczeństwa. Nasi reprezentanci to: Krzysztof Zieliński, Karol Paciorek, Wiktor Szymanik.

Połączone polsko-litewskie siły wojskowych i cywilnych specjalistów z obszaru cyberbezpieczeństwa, pod dowództwem oficera NCBC – DKWOC przez dwa dni broniły systemów IT wirtualnego państwa Berylia przed przeprowadzonymi w czasie rzeczywistym cyberatakami. W ćwiczeniu, którego celem jest utrzymanie pełnej dostępności usług świadczonych obywatelom wirtualnego państwa Berylia oraz szybkie i skuteczne reagowanie na pojawiające się zagrożenia, brały udział zespoły ze wszystkich państw NATO. Locked Shkields jest największym i najbardziej złożonym ćwiczeniem cyberobrony na świecie, które pozwala na stałe zacieśnianie współpracy obszaru wojskowego z obszarem cywilnym, wypracowanie ścieżek komunikacji, wymianę doświadczeń i stałe podnoszenie kompetencji.

17. 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. Webinaria UKNF podczas GMW organizowane były w ramach projektu edukacyjnego Centrum Edukacji dla Uczestników Rynku - CEDUR. UKNF jest koordynatorem krajowym GMW.

Działania edukacyjne CSIRT KNF w 2022 roku

Szkolenie pt. "Innowacje i cyberbezpieczeństwo na rynku finansowym"

W ramach projektu Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego - CEBRF przeprowadzono cykl szkoleń skierowanych do uczniów szkół ponadpodstawowych, których celem było przedstawienie najważniejszych zasad bezpieczeństwa w korzystaniu z Internetu oraz z usług finansowych. Zaprezentowane zostały najpopularniejsze schematy oszustw zakupowych oraz wyłudzeń z wykorzystaniem fałszywych stron bankowości elektronicznej. Wskazano na schematy działań oszustów i sposoby wykrywania zagrożeń.

Grafika 48. Szkolenie przeprowadzone zostało na GPW w Warszawie, fot. UKNF.

Konferencja naukowa pt. ”Bezpieczny DZIECIAK w cyber”

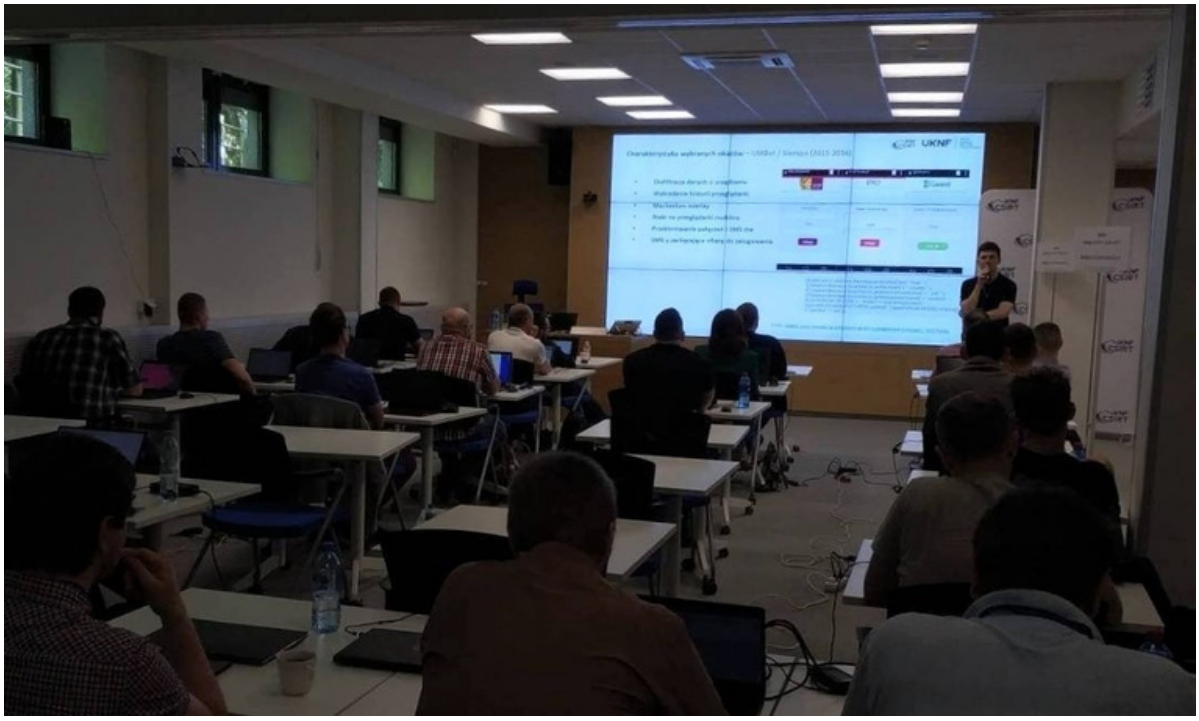
Podczas konferencji poświęconej bezpieczeństwu dzieci w sieci zorganizowanej przez Wydział Nauk Politycznych i Stosunków Międzynarodowych Uniwersytetu Warszawskiego oraz Centrum Badań nad Terroryzmem Collegium Civitas, przedstawiciele UKNF przybliżyli najważniejsze statystyki dotyczące występujących zagrożeń w internecie.

Działania edukacyjne CSIRT KNF w 2022 roku

Wskazano również na najpopularniejsze metody stosowane przez cyberprzestępców w celu wyłudzenia środków finansowych użytkowników. Ponadto przybliżone zostały możliwe sposoby ochrony przed cyberprzestępcami.

Szkolenie „Wprowadzenie do analizy malware mobilnego (Android)”

W ramach działań edukacyjnych CSIRT KNF zorganizował trzydniowy cykl całodniowych warsztatów wprowadzających do analizy malware dla systemu Android. Szkolenie skierowane było do przedstawicieli sektora finansowego – pracowników zespołów reagowania na incydenty, administratorów sieci, programistów i osób zainteresowanych tematyką cyberbezpieczeństwa. Szkolenie składało się z dwóch części – wykładowej, gdzie omówione zostały kwestie dotyczące zyskiwania na popularności przez malware mobilny. Omówiono architekturę platformy i budowę aplikacji mobilnych. Wskazano na najważniejsze trendy w rozwoju złośliwego oprogramowania, a także na kwestię pozyskiwania próbek, przygotowania laboratorium analitycznego, analizy statycznej czy dynamicznej. Druga część szkolenia obejmowała warsztaty praktyczne, podczas których uczestnicy szkolenia samodzielnie przeanalizowali próbki złośliwego oprogramowania.



Grafika 49. Przedstawiciele sektora finansowego podczas szkolenia, fot. CSIRT KNF.

Działania edukacyjne CSIRT KNF w 2022 roku

XXXI Forum Ekonomiczne

Podczas dyskusji panelowej pt. „(De)Centralizacja rozwoju cyberbezpieczeństwa w różnych sektorach gospodarki" wskazano na znaczenie współpracy sektorowej i wymiany informacji o zagrożeniach jako ważnego aspektu przyczyniającego się do rozwoju cyberbezpieczeństwa. Przybliżono również zadania CSIRT KNF odpowiedzialnego za obsługę incydentów w podmiotach rynku finansowego.

Europejski Miesiąc Cyberbezpieczeństwa 2022

Zespół CSIRT KNF uczestniczył w ogólnoeuropejskiej akcji mającej na celu poszerzenie wiedzy z zakresu cyberbezpieczeństwa. W ramach kampanii opracowano serię infografik dotyczących bezpieczeństwa w Internecie. Ponadto we współpracy z NASK przeprowadzony został webinar „Bezpieczeństwo urządzeń mobilnych – jak chronić się przed oszustwami w Internecie?", podczas którego omówione zostały najpopularniejsze sposoby ataków wymierzone w użytkowników korzystających z urządzeń z systemem Android.

World Investor Week - Światowy Tydzień Inwestora 2022

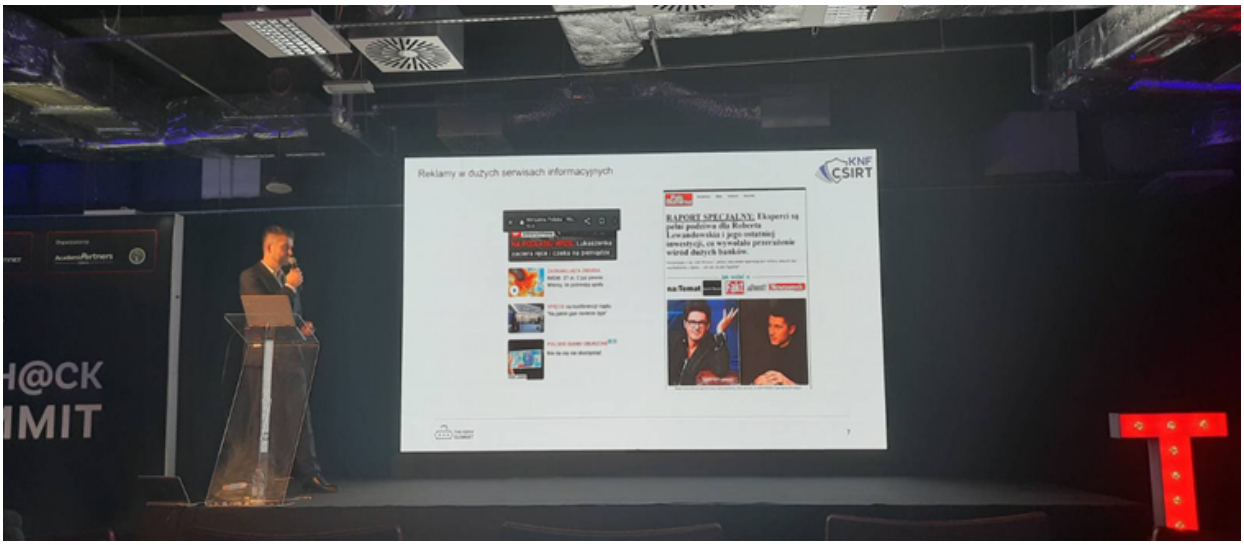
W ramach Światowego Tygodnia Inwestora [18] przedstawiciele CSIRT KNF przeprowadzili webinaria CEDUR pt. „Cyberbezpieczeństwo z perspektywy klienta usług finansowych – aspekty praktyczne" oraz „Jak zadbać o bezpieczeństwo swojego telefonu i nie dać się okraść". Wskazano na najczęściej występujące zagrożenia wymierzone w klientów bankowości internetowej oraz przybliżono podstawowe zasady pozwalające na bezpieczne funkcjonowanie w sieci.

Konferencja „The Hack Summit"

Kierownik zespołu CSIRT KNF – Paweł Piekutowski podczas konferencji zaprezentował temat „Cyberoszuści i fałszywe inwestycje w mediach społecznościowych". Podczas wystąpienia przedstawił raport zespołu dotyczący fałszywych inwestycji opisujący najczęściej pojawiające się schematy oszustw inwestycyjnych wykorzystywane przez cyberprzestępców w 2022 roku.

18. 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 powyższym obszarze przez krajowe instytucje nadzorujące i regulujące rynki papierów wartościowych. UKNF jest koordynatorem krajowym WIW.

Działania edukacyjne CSIRT KNF w 2022 roku



Grafika 50. Kierownik zespołu CSIRT KNF - Paweł Piekutowski podczas wystąpienia, fot. CSIRT KNF.

Supervision Hack

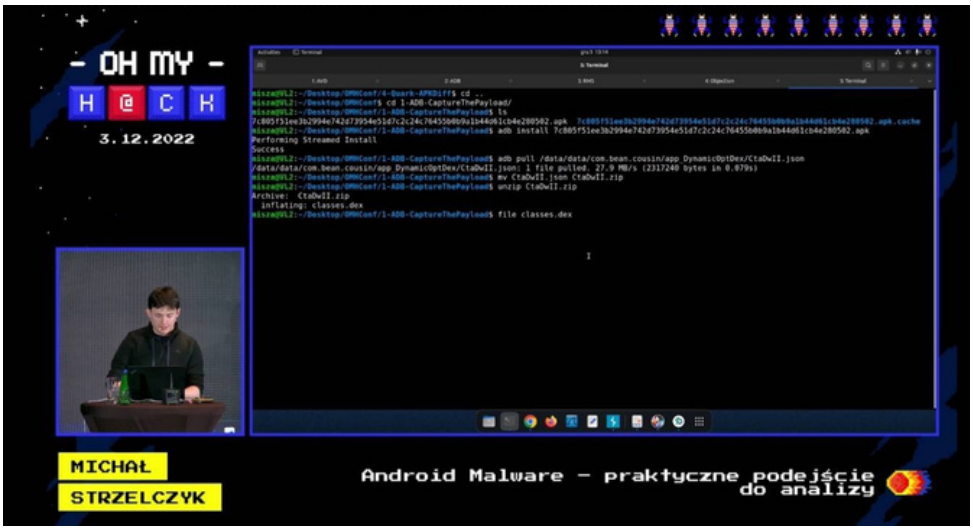
Zespół CSIRT KNF uczestniczył w pierwszym maratonie programowania organizowanym przez Urząd Komisji Nadzoru Finansowego. Zadaniem uczestników było stworzenie innowacyjnych rozwiązań dla rynku finansowego i podniesienie poziomu cyberbezpieczeństwa. Jednym z wyzwań było „Catch'em all, czyli mechanizm detekcji stron Phishngowych", które przygotowane zostało przez zespół CSIRT KNF, aby zautomatyzować i ulepszyć proces oceny stron oraz zwiększyć prędkość ich weryfikacji.

Grafika 51. Pierwszy maraton programowania organizowany przez UKNF, fot. UKNF.

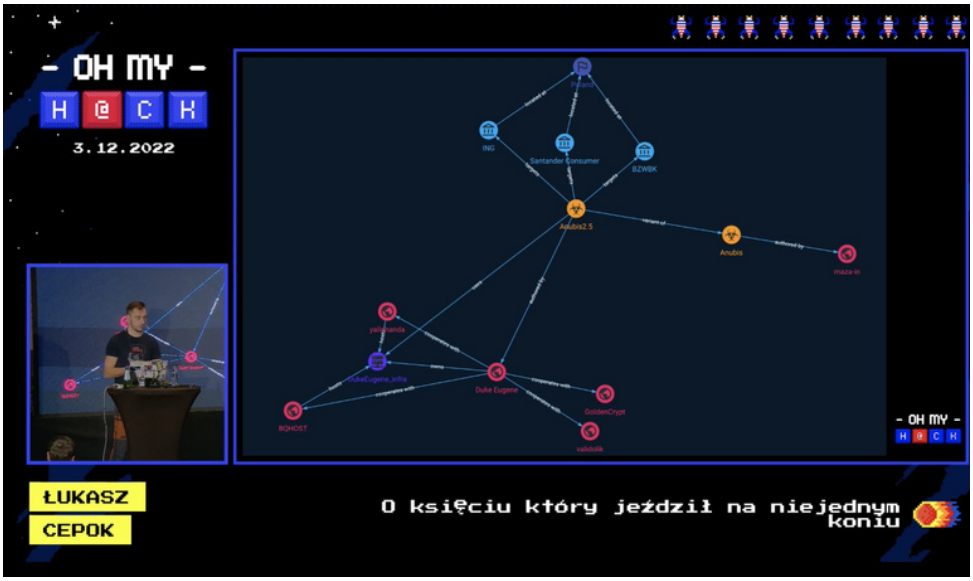
Działania edukacyjne CSIRT KNF w 2022 roku

Konferencja Oh my H@ck

Zespół CSIRT KNF aktywnie uczestniczy w największych wydarzeniach skupiających praktyków z obszaru bezpieczeństwa. Podczas kolejnej edycji konferencji „Och my H@ack" przedstawiciele zespołu CSIRT KNF przybliżyli tematykę Threat Huntingu i Analizy Malware Mobilnego. Zespół CSIRT KNF reprezentował Michał Strzelczyk, który przedstawił temat "Android Malware - praktyczne podejście do analizy". Łukasz Cepok przybliżył tematykę Threat Huntingu. Temat, który zaprezentował to "O księciu, który jeździł na niejednym koniu".



Grafika 52. Przedstawiciel CSIRT KNF przybliżający temat Android Malware, fot. Proidea.



Grafika 53. Przedstawiciel CSIRT KNF przybliżający temat Threat Huntingu, fot. Proidea.

Działania edukacyjne CSIRT KNF w 2022 roku

Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego - CEBRF

Projekt edukacyjny Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego (CEBRF) to inicjatywa Urzędu Komisji Nadzoru Finansowego (UKNF) i działającego w jego strukturach Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego w polskim sektorze finansowym (CSIRT KNF). Głównym założeniem Centrum Edukacji dla Bezpieczeństwa Rynku Finansowego jest aktywne edukowanie społeczeństwa i popularyzacja wiedzy w zakresie bezpieczeństwa finansowego. Wraz z rosnącą skalą zagrożeń występujących w cyberprzestrzeni koniecznym staje się edukowanie społeczeństwa i budowanie świadomości w tym zakresie. Na potrzeby zespołu przygotowana została strona www, na której publikowane są artykuły opisujące najnowsze trendy w cyberprzestępczości oraz sposoby działania oszustów.

Działalność akademicka

Urząd Komisji Nadzoru Finansowego we współpracy z Wyższą Szkołą Policji w Szczytnie i Biurem do Walki z Cyberprzestępczością Komendy Głównej Policji opracował program studiów podyplomowych z zakresu cyberbezpieczeństwa. Przedstawiciele CSIRT KNF uczestniczyli w inauguracyjnym posiedzeniu Naukowo - Eksperckiej Rady ds. Cyberbezpieczeństwa przy Wyższej Szkole Policji w Szczytnie. Głównym celem powołania Rady jest wypracowanie mechanizmów pozwalających na efektywniejsze kształcenie kadr w obszarze cyberbezpieczeństwa, a także współpraca środowiska akademickiego z podmiotami, których zadaniem jest zapewnienie bezpieczeństwa polskiej cyberprzestrzeni. Działania Rady skupiają się na prowadzeniu badań, szkoleń, wydawaniu wytycznych, a także wspieraniu działań mających na celu budowanie świadomości w zakresie bezpiecznego funkcjonowania w cyfrowym świecie.

Pracownicy zespołu CSIRT KNF prowadzą wybrane zajęcia dydaktyczne na studiach podyplomowych, dzieląc się swoim doświadczeniem w obszarze ataków na środki finansowe klientów w cyberprzestrzeni oraz cyberryzyka i cyberbezpieczeństwa wewnętrznego organizacji.

Działania edukacyjne CSIRT KNF w 2022 roku

Social media - zasięg

W prowadzonych w mediach społecznościowych (Twitter, LinkedIn, Facebook) profilach zespołu CSIRT KNF publikowane są informacje i ostrzeżenia odnośnie do najnowszych metod ataków oraz oszustw internetowych. Informacje o zagrożeniach publikowane przez CSIRT KNF są następnie dystrybuowane przez media internetowe o szerokim zasięgu społecznym. Na podstawie wiadomości pochodzących z publikacji CSIRT KNF w 2022 powstały 2054 artykuły w portalach branżowych oraz informacyjnych.

W celu dotarcia do jak najszerszego grona odbiorców zespół CSIRT KNF aktywnie działa w mediach społecznościowych takich jak Twitter, Facebook, LinkedIn. W 2022 roku przygotowano 199 publikacji w mediach zawierających ostrzeżenia odnośnie do najnowszych ataków lub artykuły opisujące metody działania cyberprzestępców.

Ostrzeżenia dotyczyły głównie:

- fałszywych stron bankowości elektronicznej
- złośliwego oprogramowania specjalizującego się w kradzieży środków finansowych
- fałszywych produktów inwestycyjnych wyłudzających dane od użytkownika
- fałszywych stron portali sprzedażowych – wyłudzających numery kart kredytowych

Grafika 54. Ostrzeżenie CSIRT KNF w mediach społecznościowych dotyczące fałszywych zbiórek na rzecz Ukrainy.

07. NAJWAŻNIEJSZE PODATNOŚCI W 2022 ROKU

Najważniejsze podatności w 2022 roku

Potencjalne podatności bezpieczeństwa w infrastrukturze informatycznej są jednym z największych zagrożeń dla cyberbezpieczeństwa każdej instytucji. Aby zadbać o bezpieczeństwo systemów każda z organizacji powinna na bieżąco monitorować i analizować pojawiające się zagrożenia w cyberprzestrzeni. Zespół CSIRT KNF wspiera podmioty z sektora finansowego w monitorowaniu infrastruktury oraz wspólnie z zespołami CSIRT poziomu krajowego dystrybuuje zalecenia techniczne odnośnie do sposobów postępowania z zagrożeniami. W 2022 roku Zespół CSIRT KNF przygotował i przesłał do podmiotów rynku finansowego 181 ostrzeżeń zawierających szczegółowe opisy zagrożeń oraz proponowane działania mitygujące, zwiększające poziom bezpieczeństwa. Poniżej przedstawiamy, w naszej ocenie, najważniejsze podatności i zagrożenia dla cyberbezpieczeństwa infrastruktury.

TOP 5 Podatności w 2022 z perspektywy CSIRT KNF

1. Log4Shell (CVE-2021-44228)

Podatność opublikowana pod koniec 2021 roku, opisana w CVE-2021-44228, pozwala na zdalne wykonanie kodu po stronie systemu wykorzystującego w aplikacji wskazaną podatną bibliotekę Java. Podatność ta, określana również nazwą Log4shell, była w 2022 roku jedną z najczęściej wyszukiwanych i wykorzystywanych podatności. Krytyczność zagrożenia wynikała z szerokiego zastosowania wskazanej biblioteki oraz faktu, że ustalenie czy dany system lub aplikacja są podatne, wymagało podjęcia dodatkowych działań analitycznych ze strony administratora danej usługi. Sytuacja ta skutkowała długim czasem dostępności w Internecie, dużej ilości hostów nie posiadających poprawki bezpieczeństwa.

2. ProxyNotShell (CVE-2022-41040)

Kolejną istotną podatnością odnotowaną w 2022 roku, jest podatność identyfikowana pod nazwą ProxyNotShell, dot. serwerów Microsoft Exchange Server 2013, MS Exchange Server 2016, oraz MS Exchange Server 2019. Ataki powiązane z tym zagrożeniem, wynikały z możliwości wykorzystania dwóch podatności serwerów Exchange. Pierwszą z nich była podatność opisana w CVE-2022-41040 podatność typu server-side request forgery (SSRF), pozwalająca na eskalację uprawnień. Kolejną opisaną w CVE-2022-41082 była podatność pozwalająca na zdalne wykonanie kodu po stronie serwera. Obie podatności, skutecznie wykorzystane, pozwalały na uzyskanie zdalnego dostępu do serwera Exchange. Podatność ProxyNotShell była w 2022 roku dynamicznie wyszukiwana, a sama metoda ataku ewoluowała z czasem, skutkując możliwością dalszego wykorzystania wskazanych podatności pomimo wdrożenia przez administratora systemu zaleceń bezpieczeństwa opisanych przez producenta.

Najważniejsze podatności w 2022 roku

3. FortiOS SSL-VPN (CVE-2022-42475)

Podatnością zidentyfikowaną w komponencie „FortiOS SSL-VPN", która jest istotna ze względu na liczbę podatnych wersji oprogramowania oraz krytyczności elementów infrastruktury, w której podatne urządzenia mogą być wykorzystywane. Opisane w CVE-2022-42475 zagrożenie umożliwia zdalne wykonanie polecenie lub kodu na urządzeniu działającym pod kontrolą FortiOS lub FortiProxy. Jej wykorzystanie nie wymaga od atakującego posiadania poświadczeń użytkownika jak również może być wykonana zdalnie.

4. Follina (CVE-2022-30190)

Podatność opisana w CVE-2022-30190, ujawniona w maju 2022 roku. Zagrożenie zidentyfikowane w pakiecie MS Office, pozwalające na zdalne wykonanie kodu. Ujawniony problem dotyczył protokołu ms-mdst (Microsoft Support Diagnostic Tool), który pozwalał na wykonanie dowolnego kodu PowerShell. Poprawka bezpieczeństwa dot. Folina, została opublikowana dla pakietów MS Office 365 oraz 2021. Podatność ta była wykorzystana w trwającym konflikcie zbrojnym pomiędzy Rosją, a Ukrainą jako element wojny hybrydowej.

5. F5 BIG-IP (CVE-2022-1388)

Podatność krytyczna zidentyfikowana w 2022 roku, która była intensywnie wyszukiwana przez cyberprzestępców. Zagrożenie dotyczące F5 BIG-IP iControl Rest zostało opisane w CVE-2022-1388. Podatność opublikowana została w maju 2022 roku i może być wykorzystana przez atakującego, który posiada dostęp sieciowy do urządzenia BIG-IP na porcie do zarządzania. Pozwala ona na zdalne wykonanie kodu, dodawania lub usuwanie plików, jak również zatrzymywanie usług. Aby podatność została skutecznie wykorzystana, wystarczy, że do Internetu będzie wystawione API REST, BIG-IP.

08. CYBERBEZPIECZEŃSTWO 2022 Z RÓŻNYCH PERSPEKTYW

Cyberbezpieczeństwo 2022 z różnych perspketyw

W cyberbezpieczeństwie niezwykle istotną rolę pełni efektywna komunikacja, wymiana informacji i dzielenie się wiedzą pomiędzy poszczególnymi zespołami CSIRT/CERT. Rok 2022 był kolejnym rokiem, który udowodnił, że wzajemna współpraca międzyzespołowa przyczynia się do budowania stabilności finansowej sektora finansowego. Ten rozdział ukazuje spojrzenie na miniony rok z perspektywy innych zespołów, z którymi mamy przyjemność współpracować na co dzień.

CERT POLSKA

To prawdziwa przyjemność kolejny rok obserwować rezultaty pracy CSIRT KNF na rzecz cyberbezpieczeństwa sektora finansowego. Sektora, którego klienci są nieustannie w polu zainteresowania przestępców. Jak duża praca została już wykonana, ale także jak dużo pracy ciągle przed nami, najlepiej świadczy statystyka oraz artykuły zawarte w tym raporcie, które z jednej strony pokazują aktualnie panujące trendy, a z drugiej - omawiają działania oszustów z ostatnich miesięcy. Lektura pokazuje, że za nami rok obfitujący w burzliwe wydarzenia. W tym kontekście należy docenić wkład, pomysły i zaangażowanie zespołu CSIRT KNF w rozwój i zasilanie systemów CERT Polska. To między innymi dzięki nieprzerwanej wymianie informacji udało się uratować pieniądze bardzo wielu internautów.

Nadchodzący rok na pewno będzie kontynuacją działań które już znamy i rozumiemy. Przestępcy nie zatrzymają się w próbach dostarczania swoich kampanii poprzez miejsca lub systemy, które ciągle dają taką możliwość. Ich identyfikacja oraz próba ulepszenia to nieustająca praca, niemniej jak pokazały doświadczenia - dająca wymierne rezultaty. CERT Polska niezmiennie będzie udzielać poparcia inicjatywom na rzecz podnoszenia odporności biznesu, jakości legislacji, a także świadomości obywateli operujących w ramach rynku finansowego.

CERT Polska to historycznie pierwszy w Polsce zespół reagowania na incydenty. Dzięki skutecznej działalności od 1996 r. staliśmy się wiarygodnym i rozpoznawalnym partnerem w środowisku eksperckim i sektorze publicznym. Dziś poprzez rzetelną obsługą zgłoszeń oraz działalność edukacyjną podobną pozycję budujemy wśród obywateli. Zespół CERT Polska działa w strukturach NASK – Państwowego Instytutu Badawczego i realizuje część zadań zespołu CSIRT NASK zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa.

Cyberbezpieczeństwo 2022 z różnych perspektyw

CERT POLSKA

W obszarze naszego działania ostatni rok także przyniósł znaczące zmiany. W 2022 r. zaobserwowaliśmy ponad 34 proc. wzrost zarejestrowanych incydentów cyberbezpieczeństwa, w porównaniu do roku poprzedniego. Ilość wszystkich zgłoszeń wzrosła o blisko 178 proc., a tych powiązanych z incydentami o ponad 75 proc.
W całym 2022 r. otrzymaliśmy ponad 322 tysiące zgłoszeń, co przełożyło się na ponad 39 tysięcy obsłużonych incydentów, w tym ponad 35 tysięcy w kategorii oszustw komputerowych, gdzie prowadzimy wspólne i skoordynowane działanie z zespołem CSIRT KNF. 25 625 incydentów zaklasyfikowaliśmy jako phishing. Imponująca jest również liczba zgłoszeń w tym obszarze - ponad 82 tysiące. W tle wspomnianych ataków phishigowych były oczywiście wyłudzane dane logowania do bankowości elektronicznej.

Wciąż obserwowaliśmy także wzrost wykorzystania motywu “fałszywych inwestycji”. Wspierane reklamami w przeglądarkach oraz mediach społecznościowych oraz bardzo dobrze przygotowane strony zachęcały do rzekomo bezpiecznego wykorzystania oszczędności. Pewnym novum były fałszywe inwestycje z wojennym motywem w tle - skierowana do Polaków kampania reklam opisujących platformy inwestycyjne, za pomocą których można szybko wzbogacić się na inwestycjach w kryptowaluty lub akcje firm. Artykuł, który miał zachęcić do inwestowania, sugerował, że rosyjscy imigranci wykorzystują darmowe narzędzie w celu ominięcia sankcji i szybkiego zarobku.

Nie jest to jedyny przykład, który pokazuje, że sytuacja za naszą wschodnią granicą wpływała na cyberbezpieczeństwo. Zdarzenia, które bezpośrednio łączymy z wojną w Ukrainie, to też np. zmasowane ataki typu DDoS na portale krajowych podmiotów gospodarczych czy pojawienie się fałszywych sklepów z opałem.

Jednoznacznie pokazuje to jak bardzo cyberprzestrzeń zależna jest od wydarzeń w świecie rzeczywistym. Jak intensywnie geopolityka wpływa dziś na to, z czym mierzymy się w sieci. I jak cenna w tym świecie jest współpraca, zwłaszcza na poziomie operacyjnym. Na taką współpracę liczymy z zespołem CSIRT KNF!

Cyberbezpieczeństwo 2022 z różnych perspektyw

CERT ORANGE

CERT Orange Polska to specjalistyczna jednostka w strukturach operatora, odpowiedzialna za bezpieczeństwo użytkowników internetu, korzystających z sieci Orange Polska. Mamy za sobą przeszło ćwierć wieku historii (w 1997 roku powstał Abuse Polpak), w 2006 roku uzyskaliśmy prawo do używania nazwy CERT, w 2011 dołączyliśmy do organizacji FIRST, zaś w 2016, jako pierwszy polski CERT uzyskaliśmy certyfikację w ramach inicjatywy Trusted Introducer.
Oficjalnie wygląda to tak, a operacyjnie – to po prostu mozolna praca z miliardami eventów, której efektem jest bezpieczniejsza sieć. Nie tylko dla klientów usług Orange Polska. Jesteśmy bowiem odpowiedzialni za tak istotną część polskiego internetu, że to, co się dzieje w naszej sieci, mniej lub bardziej wpływa też na innych.

Jak wyglądał z naszego punktu widzenia 2022 rok?
Wśród obsłużonych incydentów niezmiennie lideruje kategoria „Gromadzenie informacji" (przeszło 40 proc. przypadków). Wydaje się być dość szeroka, tymczasem obejmuje przede wszystkim przypadki phishingu oraz skanowania portów. Warto jednak pamiętać, że takie aktywności to bardzo często element bardziej zaawansowanych ataków, mających na celu kradzież informacji czy oszustwa finansowe. Dalsze miejsca na niechlubnym podium to dostępność zasobów (czyli de facto ataki DDoS) – których liczba, podobnie jak pierwszej kategorii, nieco wzrosła, w porównaniu z 2021 – oraz złośliwe oprogramowanie (w tym przypadku minimalny spadek).
W drugiej połowie roku zaobserwowaliśmy lawinowy wzrost socjotechniki z fałszywymi inwestycjami w tle. Fałszywe reklamy na Facebooku, podszywające się pod znane marki, czy też „wspierające przekaz" twarzami znanych polityków lub celebrytów.

Kontakt:
https://cert.orange.pl
https://twitter.com/cert_opl

Cyberbezpieczeństwo 2022 z różnych perspektyw

CERT BIK

O BIK CERT

Rolą zespołów i działów ds. bezpieczeństwa jest bieżące analizowanie, wykrywanie, stałe przewidywanie i zgłaszanie rozwiązań oraz skuteczne reagowanie w przypadku ich wystąpienia. Na tych fundamentach powołany został wewnętrzny zespół CERT Grupy BIK (Computer Emergency Response Team BIK Group).

Zespół ten działa wielotorowo, współpracuje z komórkami bezpieczeństwa oraz z ekspertami i zarządami firm – instytucji finansowych, z bankami komercyjnymi, bankami spółdzielczymi, firmami telekomunikacyjnymi, czy niezależnymi specjalistami cyberbepieczeństwa.

Zadaniem Zespołu CERT jest identyfikacja zagrożeń oraz sprawne zarządzanie zdarzeniami i incydentami bezpieczeństwa teleinformatycznego w sieciach i systemach obsługiwanych przez spółki z Grupy BIK.

Najważniejsze zagrożenie z perspektywy CERT Grupy BIK w 2022 r.:

- Socjotechniki z wykorzystaniem phishingu, spoofingu, telefony z prefixami innych krajów (głuche telefony), smishingu, podszywanie się pod instytucje (vishing i phishing).
- Wzrost liczby ataków, w tym DDoS.

Największe wyzwania według CERT Grupy BIK w 2023 r.:

- Rozwój pasywnej biometrii jako rozwiązania dla sektora finansowego.
- Wsparcie BIK w zakresie rozwoju o wdrożenia na rynku mechanizmu zastrzeżenia kredytowego.
- Przygotowanie i implementacja dyrektywy NIST2 w sektorze finansowym i budowa współpracy w ramach Krajowego Systemu Cyberbezpieczeństwa (KSC).

Cyberbezpieczeństwo 2022 z różnych perspektyw

CERT BIK

Raport Antyfraudowy BIK 2022 diagnozuje skalę wyłudzeń z perspektywy klientów indywidualnych, małych i średnich firm oraz dużych firm i korporacji. Prezentuje on wyniki badań zrealizowanych w tych trzech segmentach, koncentrując uwagę zarówno na obszarze ochrony danych, jak również na tematyce poziomu bezpieczeństwa osób i biznesu.

Klienci indywidualni

- 32% osób indywidualnych osobiście doświadczyło próby wyłudzenia. Najczęściej mieli styczność z podejrzanymi mailami, na których zwykle opiera się phishing.
- 13% wskazało na zagrożenie phishingiem, z którym mieli do czynienia sami badani lub także osoby im bliskie. Wciąż powszechną wśród złodziei praktyką jest np. wysyłanie linków do fałszywych stron banku i skłanianie ofiar do wpisania danych do logowania.

MŚP

- Około 300 tys. małych i średnich firm w Polsce padło ofiarą zdarzeń fraudowych w ciągu ostatnich 12 miesięcy. Zjawisko dotknęło więc około 17 proc. firm z sektora MŚP w Polsce.
- Wśród ankietowanych podmiotów (MŚP) odsetek firm, które korzystają z narzędzi antyfraudowych, wynosi tylko 14,6%.

Cyberbezpieczeństwo 2022 z różnych perspektyw

CERT BIK

Andrzej Karpiński, dyrektor ds. Bezpieczeństwa Grupy BIK:

> Raport Antyfraudowy wyraźnie pokazuje różnicę w podejściu do tematu zagrożeń pomiędzy dużymi firmami, a podmiotami z sektora małych i średnich przedsiębiorstw. W tej drugiej grupie dominuje przekonanie, że samodzielnie poradzą sobie z problemem fraudów.
> Tymczasem przedsiębiorcy powinni zdać sobie sprawę, że spoczywa na nich odpowiedzialność nie tylko za majątek firmy, ale również za dane klientów. Ponoszą ryzyko związane nie tylko z możliwym wyłudzeniem środków z firmowego konta, np. w wyniku podmiany numeru konta do wykonania przelewu, ale również dotyczące wykorzystania danych klientów."

Korporacje i duże podmioty, w tym także banki spółdzielcze, SKOK-i oraz instytucje ubezpieczeniowe, leasingowe, faktoringowe, telekomunikacyjne i firmy pożyczkowe.

- Ponad 10 mln zł rocznie traci 9% dużych firm z branży finansowej i telekomunikacyjnej w wyniku wyłudzeń.
- Wśród licznej grupy, jedna trzecia podmiotów z tej grupy dostrzega wzrost liczby zdarzeń fraudowych w 2022 r.
- 42% przedstawicieli ankietowanych korporacji deklaruje liczbę ponad 100 prób fraudów rocznie.

Ponad 3/4 ankietowanych przedstawicieli korporacji wskazuje, że w ochronie przed próbami oszustw stawiają przede wszystkim na rozwiązania IT.

DANE KONTAKTOWE

KONTAKT

Urząd Komisji
Nadzoru Finansowego

Departament
Cyberbezpieczeństwa
- CSIRT KNF

ul. Piękna 20,
00-549 Warszawa