TLP:CLEAR

RAPORT O ZAGROŻENIU / 29 PAŹDZIERNIKA 2026

Kampania phishingowa wymierzona w klientów PKO Banku Polskiego

Bankowość internetowa iPKO oraz iPKO biznes

Przestępcy wyłudzają dane logowania do bankowości internetowej i w czasie rzeczywistym nakłaniają klientów do przekazywania kodów oraz zatwierdzania operacji. Jednym z celów jest aktywacja aplikacji IKO na urządzeniu kontrolowanym przez przestępcę.

Najważniejsze ustalenia

115

unikalnych nazw domenowych

Zgłoszonych do CERT Polska do 29 października 2026 r.

Sterowanie sesją

Operator na bieżąco dobiera żądania danych i autoryzacji do przebiegu logowania w banku.

IKO

Aktywacja na urządzeniu przestępcy

Klient jest nakłaniany do wysłania SMS-a aktywacyjnego.

Zakres publikacji

Raport TLP:CLEAR zawiera opis kampanii, zanonimizowane ilustracje, rekomendacje oraz wskaźniki infrastruktury powiązanej z atakami. Adresy paneli operatorskich i wrażliwe dane operacyjne są zastrzeżone dla wersji TLP:RED. Dane ofiar nie są publikowane.

Autor: Zespół CSIRT KNF / Kontakt: csirt@knf.gov.pl

1. Dostarczenie i przebieg ataku

CSIRT KNF obserwuje kampanię co najmniej od 22 października 2026 r. Jej wyraźne nasilenie odnotowano 25 października. Ataki obejmują klientów detalicznych iPKO oraz użytkowników bankowości firmowej iPKO biznes. Wiadomości podszywają się m.in. pod Zespół Obsługi Klientów Instytucjonalnych PKO Banku Polskiego. Część tematów zawiera ciąg znaków przypominający numer sprawy.

Wiadomość wykorzystuje obowiązki przedsiębiorcy jako pretekst do otwarcia fałszywego formularza. Odwołania do AML, PSD2 i KNF mają uwiarygodnić prośbę o aktualizację danych.



iPKO

SPRAWA #6NFZ1ZKDZ8

Prosimy o aktualizację dokumentacji firmy

Szanowni Państwo,

Zgodnie z **Ustawą z dnia 1 marca 2018 r.** o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, **Dyrektywą PSD2** oraz zaleceniami **Komisji Nadzoru Finansowego**, jesteśmy zobowiązani do okresowej weryfikacji dokumentacji **Klientów Instytucjonalnych**.

Prosimy o niezwłoczne zalogowanie się do systemu bankowości elektronicznej i przejście do zakładki **Administracja › Dane Klienta**, aby potwierdzić lub zaktualizować **dane rejestrowe** oraz **dane reprezentantów**. **Brak odpowiedzi w ciągu 14 dni** będzie wymagał osobistej wizyty w oddziale banku z dokumentem tożsamości oraz aktualnym odpisem z **KRS** lub **CEIDG**.

Nigdy nie prosimy o hasła, kody autoryzacyjne ani dane karty. Weryfikacji dokonujemy wyłącznie **po zalogowaniu** do systemu bankowości elektronicznej. W razie wątpliwości prosimy o kontakt z **Konsultantem Biznes** pod numerem **801 36 36 36**.

Przejdź do iPKO biznes

Z poważaniem,
Zespół Obsługi Klientów Instytucjonalnych

Powszechna Kasa Oszczędności Bank Polski S.A. · ul. Puławska 15, 02-515 Warszawa
KRS 0000026438 · NIP 525-000-77-38 · REGON 016298263 · BIC/SWIFT: BPKOPLPW
Nadzór: Komisja Nadzoru Finansowego

Rysunek 1 Fragment wiadomości phishingowej podszywającej się pod PKO Bank Polski

Podszycie pod bank

Logo, numer sprawy i podpis zespołu obsługi klientów instytucjonalnych tworzą pozory oficjalnej korespondencji.

Presja obowiązku

Nadawca powołuje się na przepisy i żąda potwierdzenia danych rejestrowych firmy.

Termin 14 dni

Brak reakcji ma oznaczać konieczność wizyty w oddziale z dokumentami. Ma to skłonić odbiorcę do działania.

Wezwanie do logowania

Przycisk kieruje odbiorcę do dalszego etapu oszustwa. Wygląd wiadomości nie potwierdza autentyczności odsyłacza.

.

Tematy zaobserwowanych wiadomości

- *Odnowienie certyfikatu silnego uwierzytelniania (SCA) dla reprezentanta firmy. PKO*
- *PKO biznes · Odnowienie certyfikatu SCA*
- *iPKO biznes · Aktualizacja dokumentacji firmy*
- *Potwierdź swoje dane identyfikacyjne*
- *Nowe zasady logowania do iPKO biznes*
- *Komunikat iPKO biznes planowana synchronizacja danych profilu*

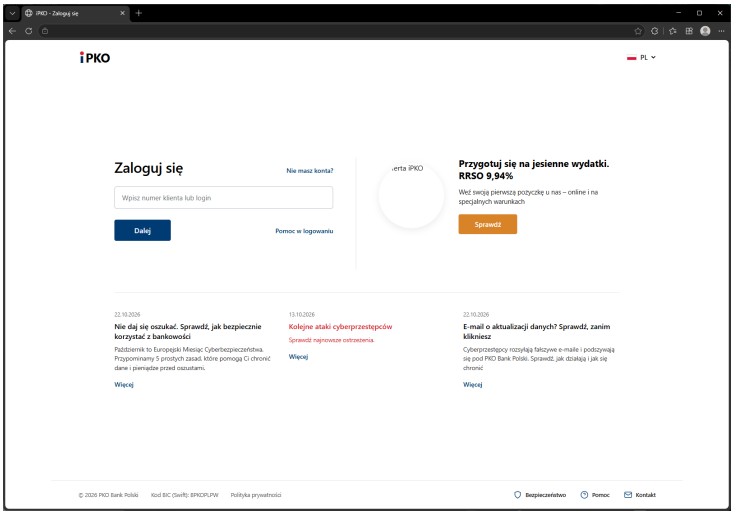
Przebieg sesji

Link prowadzi na stronę z formularzem logowania. Po wpisaniu danych klient widzi komunikat o trwającej weryfikacji, a operator wykorzystuje przejęte dane w prawdziwej bankowości. Kolejne ekrany są wybierane ręcznie.

Co widzi i robi klient	Co umożliwia to operatorowi
Wpisuje identyfikator lub numer klienta i hasło na fałszywej stronie.	Pozyskanie danych i próbę logowania w prawdziwym serwisie bankowym.
Ogląda komunikat o oczekiwaniu na weryfikację.	Czas na wykonanie czynności w bankowości i wybór kolejnego ekranu.
Otrzymuje prośbę o kod SMS, wskazanie tokena lub zatwierdzenie w IKO.	Uzyskanie autoryzacji potrzebnej w bieżącej próbie dostępu lub operacji.
Widzi błąd albo kolejne żądanie danych.	Ponowienie próby lub rozszerzenie wyłudzenia o kartę, dane osobowe i dokumenty.

Kolejność ekranów nie jest stała. Zależy od wariantu zestawu oraz decyzji operatora. Przekazane dane i zatwierdzenia mogą służyć do działania na rachunku lub aktywacji IKO na urządzeniu przestępcy.

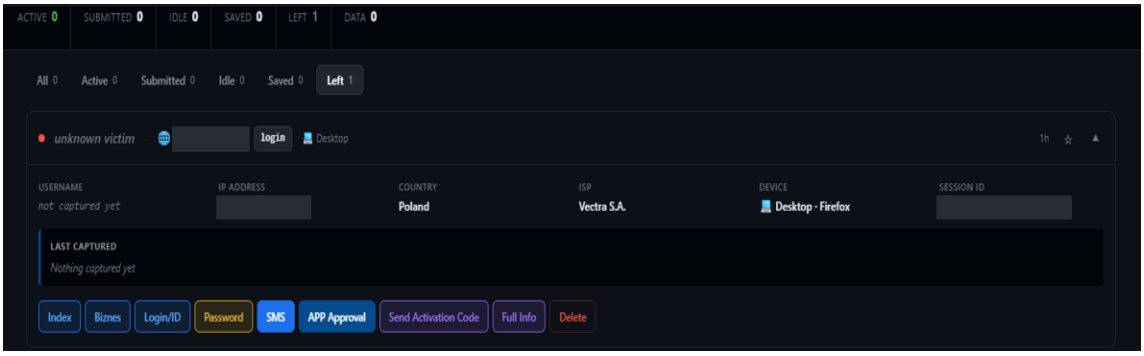
WIDOK KLIENTA



Rysunek 2 Fałszywa strona.

Fałszywa strona odtwarza układ serwisu bankowego i prosi o dane logowania.

WIDOK OPERATORA



Rysunek 3 Panel operatora.

Przyciski Login/ID, Password, SMS i APP Approval pozwalają wybrać żądanie widoczne dla klienta.

Na zrzucie widoczna jest również funkcja wysłania żądania kodu aktywacyjnego.

Ekrany żądania danych logowania i autoryzacji

Poniższe formularze zaobserwowano w analizowanym wariancie. Pokazują zakres dostępnych żądań, a nie obowiązkową sekwencję ani potwierdzenie skutecznego przejęcia rachunku.

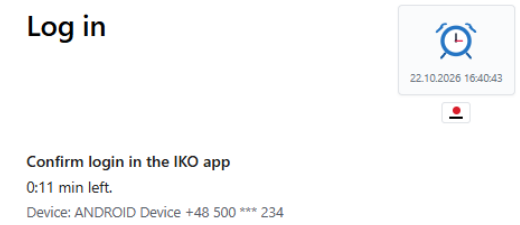


Rysunek 4. Fragment fałszywego formularza hasła.

HASŁO DO BANKOWOŚCI

Po identyfikatorze fałszywa strona żąda hasła. Pozyskana para danych może zostać użyta do próby logowania w prawdziwym serwisie bankowym.

Odtworzenie wyglądu formularza nie potwierdza, że klient znajduje się na stronie banku.

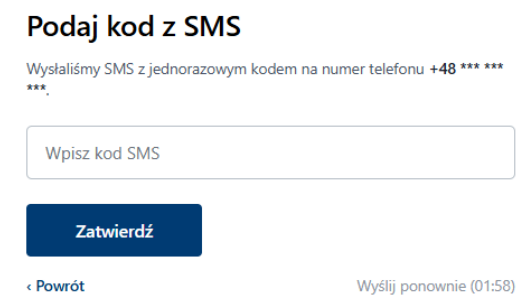


Rysunek 5. Żądanie zatwierdzenia logowania w aplikacji IKO.

ZATWIERDZENIE W APLIKACJI

Strona wyświetla prośbę o zatwierdzenie logowania w IKO. W opisanym mechanizmie przestępca wykorzystuje klienta do autoryzacji własnej próby logowania.

Znaczenie ma treść operacji w aplikacji, a nie wyjaśnienie podane na stronie phishingowej.



Rysunek 6. Fragment formularza wyłudzającego kod SMS.

KOD Z WIADOMOŚCI SMS

Kolejny formularz wyłudza jednorazowy kod. Operator może wywołać ten ekran wtedy, gdy potrzebuje autoryzacji w prawdziwym procesie bankowym.

Kod należy odczytywać wraz z opisem operacji w SMS-ie. Fałszywa strona może przedstawiać tę czynność jako zwykłą weryfikację.

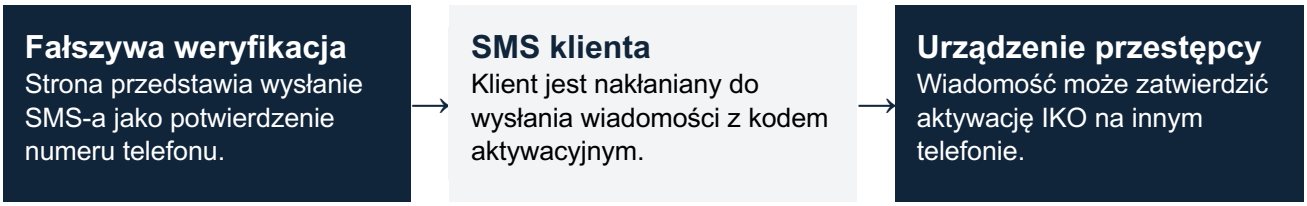
2. Zakres wyłudzeń

Zestawy phishingowe przewidują kilka rodzajów żądań. Ich kolejność i zakres zależą od wariantu strony oraz decyzji operatora.

- **Dane logowania.** Identyfikator lub numer klienta oraz hasło do bankowości internetowej.
- **Autoryzacja.** Kody z SMS-ów i e-maili, wskazania tokenów iPKO biznes i zatwierdzenia w aplikacji IKO.
- **Aktywacja IKO.** Wysłanie z telefonu klienta wiadomości SMS zawierającej kod aktywacyjny. Może to uruchomić IKO na urządzeniu kontrolowanym przez przestępcę.
- **Dane karty.** Numer karty, data ważności, CVV2 lub CVC2 oraz PIN.
- **Dane osobowe i dokumenty.** Imię i nazwisko, PESEL, data urodzenia, telefon, e-mail, adres i zdjęcia obu stron dowodu osobistego. Część paneli przewiduje też numer dokumentu i nazwisko panieńskie matki.

Aktywacja aplikacji IKO na urządzeniu przestępcy

W jednym z wariantów strona prosi klienta o wysłanie z własnego telefonu SMS-a z kodem oraz tekstem „IKO activation. Do not change the message”. Żądanie jest przedstawiane jako etap potwierdzania numeru telefonu lub weryfikacji. W rzeczywistości wysłanie takiej wiadomości może zatwierdzić aktywację IKO na telefonie kontrolowanym przez przestępcę i zapewnić mu dalszy dostęp do rachunku.

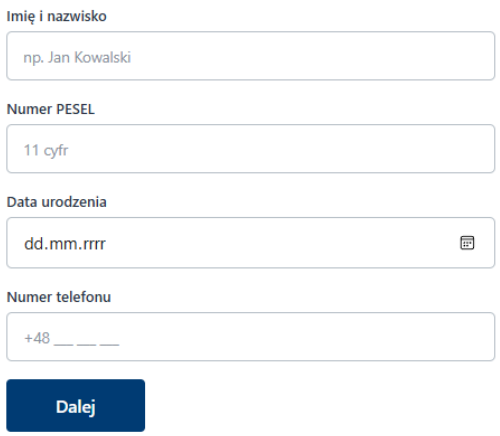


Ekran oczekiwania daje operatorowi czas na wykonanie czynności w prawdziwym systemie bankowym. Kolejna prośba o kod lub zatwierdzenie może więc pojawić się dopiero po przerwie. Sama zgodność wyglądu strony z bankowością oraz pozornie logiczna kolejność komunikatów nie potwierdzają autentyczności procesu.

Żądanie wysłania SMS-a aktywacyjnego należy odróżniać od prośby o podanie kodu z otrzymanej wiadomości. W pierwszym przypadku klient sam wysyła wiadomość wykorzystywaną w procesie aktywacji aplikacji.

Formularze rozszerzające zakres wyłudzenia

Oprócz danych dostępu zestaw zawiera formularze danych osobowych, karty i dokumentu tożsamości. Ich wyświetlenie może być kolejną decyzją operatora w trakcie tej samej interakcji.

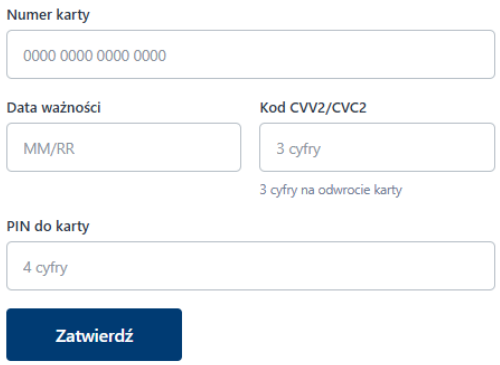


Rysunek 7. Fragment formularza danych osobowych.

DANE OSOBOWE

Formularz żąda imienia i nazwiska, numeru PESEL, daty urodzenia oraz numeru telefonu. Zakres żądania wykracza poza identyfikator i hasło do bankowości.

Komunikaty o bezpieczeństwie danych są częścią fałszywej strony.



Rysunek 8. Fragment formularza danych karty z polem PIN.

KARTA PŁATNICZA

Strona zbiera numer karty, datę ważności, CVV2 lub CVC2 i PIN. Umieszczenie tych pól w procesie rzekomej weryfikacji ma nadać żądaniu pozory uzasadnienia.

Żądanie PIN-u karty na stronie logowania jest sygnałem oszustwa.



Rysunek 9. Żądanie przesłania zdjęć dokumentu tożsamości.

DOKUMENT TOŻSAMOŚCI

Formularz prosi o zdjęcia obu stron dokumentu. Odwołanie do AML ma uzasadnić przekazanie kopii dowodu osobistego lub paszportu.

Pretekst regulacyjny powtarza argumentację z wiadomości e-mail i ma uwiarygodnić kolejne żądanie danych.

3. Infrastruktura i utrudnianie detekcji

Do 29 października 2026 r. do CERT Polska zgłoszono 115 unikalnych nazw domenowych powiązanych z kampanią.

Operatorzy równolegle korzystają z domen zarejestrowanych na potrzeby kampanii oraz z przejętych, legalnie działających witryn. Taka różnorodność utrudnia rozpoznanie ataku wyłącznie na podstawie nazwy strony lub miejsca jej hostowania.

Podszycie pod instytucje
pl-rzad[.]com
wladze-pl[.]com
pl-firma[.]net
Nazwy mają uwiarygodnić wiadomość o obowiązkach przedsiębiorcy.

Nazwy podobne do banku
ipkobiznes[.]net
ipkobp[.]com
ipkobformular-pl[.]online
Nazwa banku w adresie nie potwierdza autentyczności strony.

Przejęte witryny
Formularz w katalogu legalnie działającej strony
Atak może wykorzystywać także polskie witryny z końcówką .pl.

Na przejętych witrynach formularz może działać w wydzielonym katalogu, np. /-/pl-PL/ipkobiznes/logowanie. Nazwa znanego serwisu nie gwarantuje bezpieczeństwa konkretnej podstrony.

Rotacja subdomen

Konfiguracja wildcard DNS pozwala obsługiwać wiele nazw w obrębie jednej domeny bez osobnej rejestracji każdej z nich. Linki w wiadomościach mogą kierować do losowych subdomen, takich jak sesja-4w6n-pkobiznes.rzad-pl[.]net. Kolejne otwarcie linku może prowadzić pod inną nazwę. Blokada pojedynczej subdomeny nie musi obejmować następnego wariantu, co utrudnia utrzymywanie aktualnych reguł ochronnych.

Ukrywanie treści przed skanerami

Część stron stosuje cloaking, czyli ukrywa formularz przed ruchem rozpoznanym jako analityczny. Przed wyświetleniem treści sprawdzane są m.in. kraj połączenia, typ sieci i przeglądarka. Niektóre warianty wymagają dodatkowo rozwiązania CAPTCHA. Użytkownik przypominający potencjalną ofiarę z Polski otrzymuje formularz phishingowy, natomiast skaner może zobaczyć pustą stronę, błąd lub przekierowanie do zwykłej witryny.

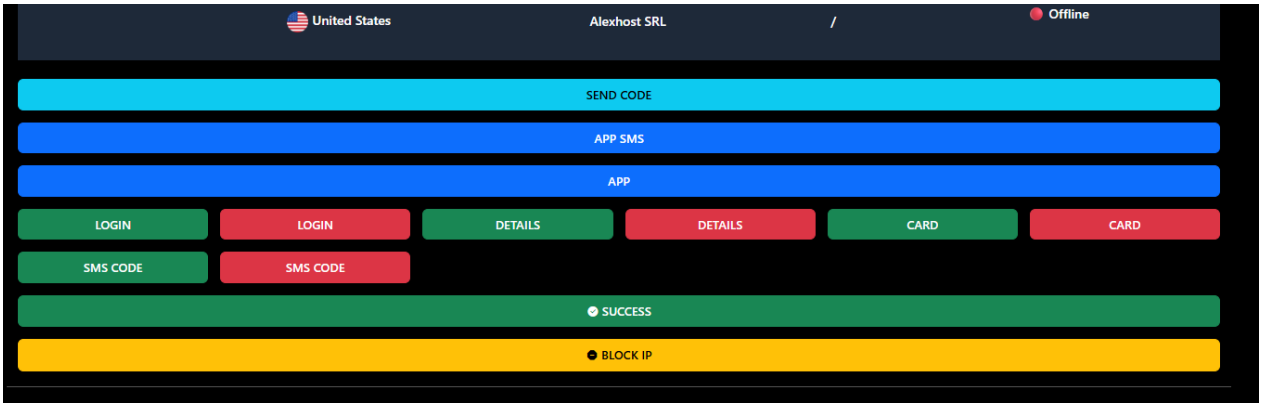
W efekcie automatyczna ocena może nie wykazać zagrożenia, mimo że formularz jest dostępny dla odbiorców kampanii. Weryfikacja takich zgłoszeń wymaga uwzględnienia warunków dostępu i ręcznej analizy. Nowe domeny oraz zmiany konfiguracji powodują, że lista znanych adresów szybko się dezaktualizuje.

4. Obsługa sesji przez operatora

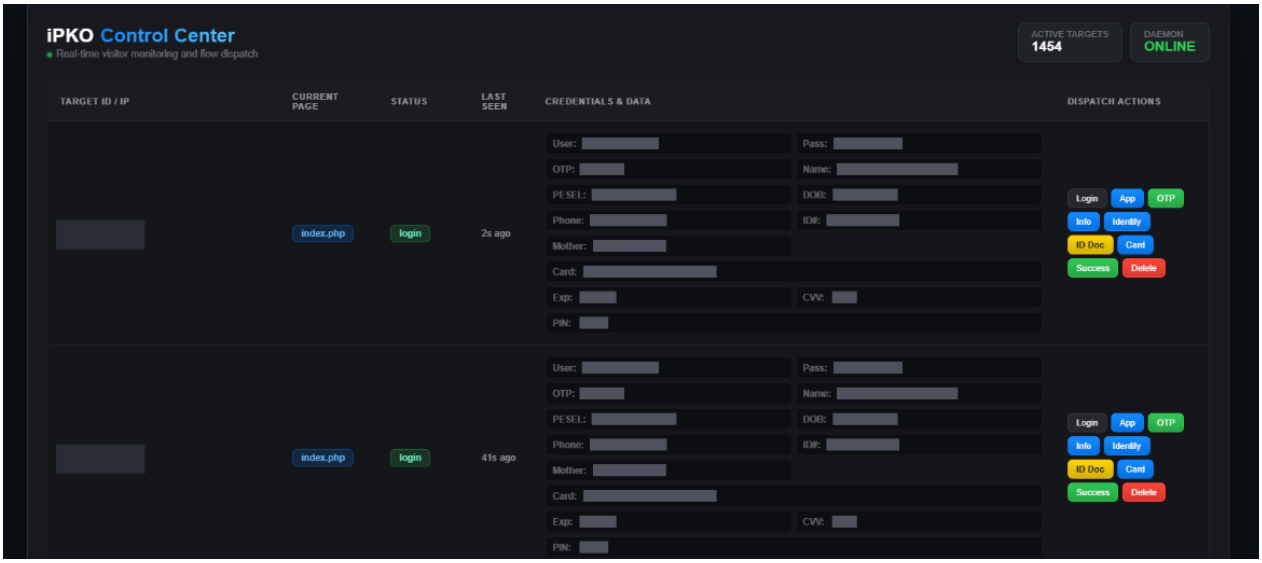
Analiza paneli potwierdziła ręczne sterowanie kolejnymi etapami wyłudzenia. Operator widzi stan sesji, ekran wyświetlany klientowi i dane wpisywane w formularzach. Dostępne informacje obejmują też adres IP, kraj, dostawcę połączenia i przeglądarkę. Część zestawów wysyła powiadomienia przez Telegram.

Przyciski w panelu pozwalają przełączać formularze, wyświetlać komunikat oczekiwania i ponawiać żądanie po błędzie. Operator może zaakceptować albo odrzucić dany etap. Odrzucenie wyświetla klientowi komunikat o błędzie i prośbę o ponowne wpisanie danych. Dostępne działania obejmują żądanie kodu SMS, zatwierdzenia w aplikacji, danych karty, danych osobowych lub zdjęć dokumentu.

Panel umożliwia także zakończenie sesji oraz blokadę adresu IP, np. gdy operator podejrzewa wizytę analityka lub skanera. Rozwiązania różnią się wyglądem i technologią, ale zachowują ten sam model ręcznego prowadzenia klienta przez kolejne formularze.



Rysunek 10. Panel sterowania sesją. Przyciski pozwalają wywołać żądanie kodu lub danych, zaakceptować albo odrzucić etap oraz zablokować adres IP.



Rysunek 11. Fragment panelu zbierającego dane z wielu sesji. Widoczne są stan formularza, pola przechwyconych danych i przyciski dalszych żądań. Adresy i dane identyfikujące zostały usunięte.

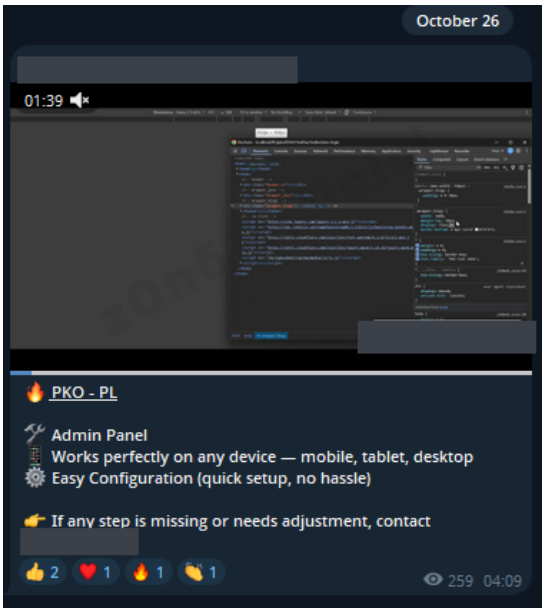
Zrzuty pokazują funkcje i sposób organizacji pracy operatora. Nie służą do ustalania liczby domen, unikalnych ofiar ani skutecznych przejęć rachunków.

Znaczenie dla ochrony klientów

Kolejne żądania nie muszą pojawiać się w stałej kolejności. Ofiara może uznać ekran oczekiwania lub komunikat o błędzie za element zwykłego procesu bankowego. Decydujące pozostają adres strony i treść operacji przedstawionej do zatwierdzenia.

5. Sprzedaż gotowych zestawów phishingowych

26 października 2026 r. w Telegramie opublikowano ofertę zestawu „PKO - PL”, obejmującego fałszywą stronę bankowości i panel administracyjny. Wkrótce po publikacji ten sam zestaw zaobserwowano na aktywnej stronie phishingowej.



Rysunek 12. Oferta zestawu phishingowego „PKO - PL” w Telegramie z 26 października 2026 r.

Co zawierała oferta

Do ogłoszenia dołączono nagranie pokazujące fałszywą stronę oraz obsługujący ją panel. Sprzedawca deklarował działanie na komputerach i urządzeniach mobilnych, łatwą konfigurację i pomoc przy uruchomieniu.

Deklaracje sprzedawcy opisują sposób reklamowania narzędzia. Nie stanowią niezależnego potwierdzenia wszystkich jego funkcji.

Związek z analizowaną kampanią

Zaobserwowanie tego samego zestawu na aktywnej stronie łączy ofertę sprzedaży z narzędziem wykorzystanym w ataku. Dostępność strony wraz z panelem zmniejsza zakres prac technicznych potrzebnych do uruchomienia wyłudzenia.

Równoległe warianty stron i paneli

W kampanii obserwowane są również inne warianty, różniące się technologią, hostingiem i zakresem zbieranych danych. Operatorzy modyfikują formularze i przenoszą je na kolejne serwery. Zmiana domeny lub wyglądu strony nie musi więc oznaczać zmiany mechanizmu wyłudzenia.

6. Rekomendacje

Do bankowości należy logować się przez zapisaną zakładkę lub samodzielnie wpisany adres. Prośbę o aktualizację danych najlepiej potwierdzić w banku, dzwoniąc na numer z jego oficjalnej strony.

Dla klientów banku

- **Sprawdzaj adres przed logowaniem.** Korzystaj z ipko.pl lub ipkobiznes.pl. Nie otwieraj strony logowania z linku w e-mailu ani SMS-ie.
- **Czytaj treść autoryzowanej operacji.** Sprawdź jej cel, a przy przelewie także kwotę i odbiorcę. Nie przekazuj kodu ani nie zatwierdzaj działania, którego sam nie zainicjowałeś.
- **Przerwij nietypowy proces weryfikacji.** Żądanie wysłania SMS-a aktywującego IKO, PIN-u karty lub zdjęcia dowodu na stronie logowania jest sygnałem oszustwa.
- **Po ujawnieniu danych natychmiast skontaktuj się z bankiem.** Poinformuj, jakie dane podałeś i jakie działania zatwierdziłeś. Poproś o sprawdzenie aktywnych urządzeń IKO i zabezpieczenie dostępu. Zmień hasło, a po ujawnieniu danych karty także ją zastrzeż.
- **Zgłaszaj podejrzane wiadomości.** Strony i e-maile można zgłaszać przez incydent.cert.pl. Podejrzane SMS-y można bezpłatnie przekazać na numer 8080.

Dla firm

- Przekaż ostrzeżenie działom finansów i księgowości oraz osobom uprawnionym do zatwierdzania przelewów.
- Nietypowe prośby o dane firmy, zmianę sposobu logowania lub dodatkową autoryzację weryfikuj bezpośrednio w banku.
- Uwzględnij w szkoleniach ataki prowadzone w czasie rzeczywistym i żądania aktywacji aplikacji na nowym urządzeniu.
- Regularnie przypominaj pracownikom, jak zgłaszać podejrzane wiadomości. Aktualizuj ostrzeżenia wraz ze zmianami treści e-maili i wyglądu stron.
- Śledź komunikaty CSIRT KNF, CERT Polska i banku oraz przekazuj istotne ostrzeżenia osobom obsługującym rachunki firmowe.

7. Podsumowanie

Kampania wymierzona w klientów PKO Banku Polskiego nadal trwa, a przestępcy na bieżąco uruchamiają kolejne domeny i warianty fałszywych stron. CSIRT KNF monitoruje jej przebieg i analizuje nową infrastrukturę. CERT PKO Banku Polskiego również identyfikuje nowe domeny i strony wykorzystywane do podszywania się pod bank. Wszystkie dane ofiar odzyskane w trakcie analizy są przekazywane do CERT PKO BP, aby bank mógł szybko zabezpieczyć zagrożone konta. Działania są koordynowane pomiędzy bankiem, CSIRT KNF i CERT Polska.

CERT Polska analizuje kampanię i dzieli się ustaleniami z podmiotami sektora finansowego, wspierając rozpoznawanie kolejnych wariantów ataku i przygotowanie działań ochronnych. Równolegle na bieżąco dodaje zidentyfikowane adresy do Listy Ostrzeżeń. Współpraca z CERT Polska obejmuje więc zarówno analizę zagrożenia i wymianę wiedzy, jak i ograniczanie dostępu do stron wykorzystywanych przez przestępców. Dziękujemy zespołowi CERT Polska za współpracę analityczną i przekazywanie informacji, które pomagają chronić klientów sektora finansowego.

Ważną rolę odgrywają również pozostałe podmioty sektora finansowego, które przekazują do CSIRT KNF informacje o kolejnych incydentach i próbki wiadomości. Zgłoszenia te pozwalają szybciej wykrywać nowe elementy kampanii i ostrzegać innych uczestników rynku.

Dziękujemy całemu sektorowi za tę współpracę.

Współpraca przy ograniczaniu skutków kampanii

CSIRT KNF	CERT PKO Bank Polski	CERT Polska
Monitorowanie kampanii i analiza nowej infrastruktury oraz zgłoszeń sektora.	Wykrywanie fałszywych stron i zabezpieczanie zagrożonych kont klientów.	Analiza kampanii, wymiana ustaleń z sektorem finansowym i bieżące dodawanie adresów do Listy Ostrzeżeń.

W przypadku pytań dotyczących tego zagrożenia prosimy o kontakt z naszym zespołem pod adresem: csirt@knf.gov.pl

Z poważaniem, Zespół

Znaczenie kolorów TLP dla odbiorców wiadomości

TLP: RED	Odbiorcy nie mogą dzielić się przekazanymi informacjami z nikim, z wyjątkiem innych odbiorców tych wiadomości.
TLP: AMBER	Odbiorcy mogą dzielić się informacjami jedynie w obrębie swojej organizacji (a także jej klientów i consituency) z osobami, które muszą poznać wiadomości oraz jedynie w zakresie niezbędnym do podjęcia stosownych działań. Dodatkowe ograniczenia mogą zostać wyspecyfikowane przez nadawcę w dowolnym zakresie i muszą być przestrzegane. Jednym ze standardowych ograniczeń jest oznaczenie **TLP:AMBER+STRICT** , które pozwala dzielić się informacjami wyłącznie w obrębie organizacji.
TLP: GREEN	Odbiorcy mogą dzielić się informacji ze swoimi współpracownikami, w ramach swojej i partnerskich organizacji oraz w swoim środowisku. Nie można jednak udostępniać tych informacji przez publiczne kanały informacyjne.
TLP: CLEAR	Dystrybucja informacji nie podlega żadnym ograniczeniom (z wyjątkiem praw autorskich).

8. Wskaźniki kompromitacji

Stan zestawienia: 29 października 2026 r.

Dostawca infrastruktury	Adres IP	Domeny i subdomeny
Akamai Connected Cloud	173[.]255[.]196[.]143	safpymecloud[.]com
AlexHost ALEXHOST S.R.L.	85[.]137[.]248[.]162	cycretalpha[.]org
AlexHost ALEXHOST S.R.L.	185[.]139[.]214[.]50	rwidamouadohtm[.]com
alwaysdata alwaysdata SARL	185[.]31[.]40[.]15	andrei[.]alwaysdata[.]net
Amazon.com, Inc. *	3[.]78[.]192[.]157 3[.]124[.]161[.]149 18[.]195[.]220[.]125 34[.]242[.]13[.]175 52[.]210[.]209[.]122 54[.]75[.]22[.]166	u117289154[.]ct[.]eu[.]sendgrid[.]net
Amazon.com, Inc. *	18[.]153[.]174[.]57 18[.]159[.]187[.]248 52[.]30[.]78[.]234 54[.]217[.]93[.]255 63[.]34[.]147[.]103 63[.]176[.]0[.]179 63[.]176[.]115[.]195	u2309924[.]ct[.]sendgrid[.]net u47785894[.]ct[.]sendgrid[.]net
Amazon.com, Inc. *	54[.]228[.]217[.]226	u47785894[.]ct[.]sendgrid[.]net
BisectHosting	216[.]201[.]76[.]201	euromaxdubai[.]com
CentrixNodes CentrixNodes LLC	104[.]223[.]81[.]26	wwwpko-biznes[.]hikkistikks[.]com
Cloudflare, Inc. *	104[.]18[.]37[.]79 172[.]64[.]150[.]177	bancper1792351096396[.]0840056[.]misitiohostgator[.]com
Cloudflare, Inc. *	104[.]21[.]33[.]123 172[.]67[.]162[.]138	jackielewis7216[.]dolceideaonline[.]it
Cloudflare, Inc. *	104[.]21[.]36[.]161 172[.]67[.]196[.]193	robertobarri[.]it
Cloudflare, Inc. *	104[.]21[.]39[.]52 172[.]67[.]143[.]102	lapaxe[.]com

Dostawca infrastruktury	Adres IP	Domeny i subdomeny
Cloudflare, Inc. *	104[.]21[.]51[.]221 172[.]67[.]188[.]253	servise-pko[.]com
Cloudflare, Inc. *	104[.]21[.]60[.]141 172[.]67[.]197[.]130	lawson87[.]fusiarovato[.]it
Cloudflare, Inc. *	104[.]21[.]83[.]212 172[.]67[.]181[.]245	ipkobiznes-pl[.]banco-ctt-2026[.]com
Cloudflare, Inc. *	172[.]67[.]68[.]20	ipko-pl[.]1wp[.]site
Cloudflare, Inc. *	172[.]67[.]136[.]191	ipkobiznes[.]multinfos[.]online
Cloudflare, Inc. *	172[.]67[.]146[.]9	pkonew[.]yeserviceklarone[.]com
Cloudflare, Inc. *	188[.]114[.]96[.]0 188[.]114[.]97[.]0	casagiardinelli[.]com credissarealty[.]com de[.]mouirca[.]info frirolioa[.]businesssyncrix[.]de homebanking[.]bansupparea[.]online hrema[.]brilourapew[.]com ipkonline[.]prospero-classical[.]com ipkosecure[.]prospero-classical[.]com rhosta[.]hurtonatonalasa[.]com support[.]itsme-digitalhub[.]click www[.]virginiadrudi[.]it zacharynelson1034[.]casinadelprincipe[.]it
Cloudflare, Inc. *	188[.]114[.]96[.]3	ipkobiznes[.]00075887[.]site mozesz[.]net
Cloudflare, Inc. *	188[.]114[.]97[.]3	ipko[.]infosipkobiznes[.]online ipko[.]polskiego[.]info pl-rzad[.]net supp[.]alphainfofineco[.]online wladze-pl[.]com
Cloudflare, Inc. *	2606:4700:7::a29f:872a	validacionappcom[.]kinsta[.]cloud
CLOUDFLARESPECTRUM Cloudflare London, LLC *	141[.]193[.]213[.]10 141[.]193[.]213[.]11	kundensrvlikpo[.]wpenginepowered[.]com
COMBELL-AS Combell NV	213[.]158[.]86[.]121	valenciafashioninstitute[.]com
DE-WEBGO webgo GmbH	185[.]30[.]35[.]27	www[.]web43[.]s321[.]goserver[.]host
DHOSTING-AS dhosting.pl Sp. z o.o.	109[.]95[.]157[.]137	ko****[.]dk***[.]pl (domena zanonimizowana)

Dostawca infrastruktury	Adres IP	Domeny i subdomeny
DigitalOcean, LLC	139[.]59[.]109[.]251	portal-all[.]lifesupport-ambulance[.]com
DigitalOcean, LLC	165[.]245[.]195[.]20	biznes-ipkoplinfo0x02910209109210[.]trainzinfo[.]com[.]ua
DigitalOcean, LLC	165[.]245[.]197[.]246	ww-ipkoplinfo[.]trainzinfo[.]com[.]ua
DigitalOcean, LLC	206[.]189[.]122[.]56	ww-ipkopl[.]aopeinture[.]fr ww-ipkoplinfo[.]earthly-essential-bracelets[.]com ww1-ipkopl[.]designlocalga[.]com ww1-ipkoplinfo[.]earthly-essential-bracelets[.]com
GODADDY-SXB Host Europe GmbH	37[.]148[.]200[.]5	ipkobiznes[.]app
GODADDY-SXB Host Europe GmbH	37[.]148[.]201[.]157	login[.]ipkopl[.]com pl[.]ipkobp[.]com www[.]ipkobp[.]com
GODADDY-SXB Host Europe GmbH	92[.]205[.]23[.]99	15c8d9e0f1a2[.]activegym[.]nl 37e0f1a2b3c49ab[.]art-lines[.]nl ipkobiznes[.]co
GODADDY-SXB Host Europe GmbH	92[.]205[.]59[.]244	59a2b3c4d5e6bcdef0129e[.]salonamiabel[.]nl 71c4d5e6f7a8def0123456789ab[.]artilleriemonument[.]nl ipkobiznes[.]net
GODADDY-SXB Host Europe GmbH	92[.]205[.]100[.]186	9nn[.]98a[.]mytemp[.]website
GODADDY-SXB Host Europe GmbH	92[.]205[.]170[.]8	9pn[.]c8e[.]mytemp[.]website
GODADDY-SXB Host Europe GmbH	92[.]205[.]172[.]200	gv4[.]37e[.]mytemp[.]website
Google LLC *	142[.]251[.]98[.]132	gs-ipkobiz[.]blogspot[.]com ipko-biznepl[.]blogspot[.]com ipko-biznverif[.]blogspot[.]com pl-bizip[.]blogspot[.]com
HIVELOCITY, Inc.	91[.]124[.]130[.]146	biorganicos[.]co
HIVELOCITY, Inc.	140[.]150[.]227[.]229	ngtel[.]co
HOMEPL-AS home.pl sp. z o.o.	79[.]96[.]1[.]…	z**[.]le****[.]pl (domena zanonimizowana)
HOMEPL-AS home.pl sp. z o.o.	79[.]96[.]142[.]…	mo******[.]pl (domena zanonimizowana)
HOMEPL-AS home.pl sp. z o.o.	89[.]161[.]254[.]…	st*********[.]pl (domena zanonimizowana)

Dostawca infrastruktury	Adres IP	Domeny i subdomeny
Infomaniak-AS Infomaniak Network SA	83[.]228[.]233[.]163	nextcloud[.]ginfo[.]org
Infomaniak-AS Infomaniak Network SA	128[.]65[.]195[.]93	cfamaj[.]marge-labo[.]com
Infomaniak-AS Infomaniak Network SA	2001:1600:0:aaaa::80:38	tip[.]rootcode[.]ch
InMotion Hosting, Inc.	23[.]235[.]204[.]196	dev[.]minepaneldashboard[.]com[.]br ghz[.]stjoansconventschool[.]com payment[.]deepaultech[.]com prod[.]deepaul[.]co re[.]luarpratas925[.]com[.]br
IONOS-AS IONOS SE	217[.]160[.]0[.]99	myblog-z4u5lhdbk9[.]live-website[.]com
IONOS-AS IONOS SE	217[.]160[.]0[.]192	myhostingforword-aw59mg2gh6[.]live-website[.]com
IONOS-AS IONOS SE	217[.]160[.]0[.]207	meinhostingfa14r-unzpdq4eqo[.]live-website[.]com
LHPL LH.pl Sp. z o.o.	5[.]252[.]229[.]…	la*********[.]pl (domena zanonimizowana)
Liquid Web, L.L.C	209[.]87[.]159[.]240	9ffc56b19e[.]nxcli[.]io
Liquid Web, L.L.C	209[.]87[.]159[.]245	0e03e3eb99[.]nxcli[.]io
Liteserver The Infrastructure Group B.V.	5[.]255[.]109[.]32	ilariafranchini[.]it
Locaweb Servicos de Internet S/A	186[.]202[.]153[.]206	portocaminhoes-am[.]com[.]br
Oracle Corporation	119[.]18[.]49[.]30	naaricarehospital[.]com
OrangeHost	173[.]252[.]167[.]10	zookingdoms[.]com
OVH OVH SAS	5[.]135[.]70[.]248	ecobiolanka[.]com
OVH OVH SAS	51[.]83[.]187[.]…	pa*****[.]wi******[.]pl (domena zanonimizowana)
OVH OVH SAS	142[.]44[.]161[.]81	promotunisia[.]com
PODAON Podaon SIA	188[.]137[.]176[.]16	ipkobizness-pl[.]infotelsrore[.]com
RaiolaNetworks Raiola Networks S.L.	178[.]211[.]133[.]18	vuestrasvoces[.]com
REGISTER-AS REGISTER S.P.A.	81[.]88[.]52[.]90	museogatto[.]it

Dostawca infrastruktury	Adres IP	Domeny i subdomeny
REGISTER-AS REGISTER S.P.A.	81[.]88[.]52[.]200	barent[.]it
RouterHosting LLC	45[.]59[.]113[.]110	directorio291445b8f0f7b61edd901158c8be6a53[.]diepo[.]online
RouterHosting LLC	172[.]86[.]91[.]13	logowanie[.]lpkobp[.]com logowanie[.]lpkobp[.]online
Serverhino Netversor GmbH	92[.]246[.]89[.]26	ipkobformular-pl[.]online
SWISSNET-AS SWISSNET LLC	31[.]56[.]209[.]36	pl-biznesipko[.]webinate[.]au poland-ipkobiznes[.]parmasinergiadonna[.]it
VNPT Corp	160[.]25[.]74[.]227	pl-firma[.]com pl-firma[.]net pl-rzad[.]com pl-wladze[.]com pl-wladze[.]net rzad-pl[.]com rzad-pl[.]net wabze[.]net wladze-pkobiznes[.]com wladze-pl[.]net
VNPT Corp	160[.]30[.]55[.]163	lapax[.]net
Zoho Canada Corporation *	199[.]67[.]84[.]80	ipkooooooooo[.]zohodesk[.]ca