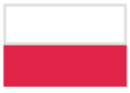
KWIECIEŃ 2026

Podsumowanie Miesiąca CERT POLSKA

Nr 4/2026

CERT.PL NASK
CSIRT NASK

PODSUMOWANIE MIESIĄCA CERT POLSKA



PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTERSTWA CYFRYZACJI

TLP: CLEAR

Publikacja wyraża jedynie poglądy autora/ów i nie może być utożsamiana z oficjalnym stanowiskiem Ministerstwa Cyfryzacji.

Autor: zespół CERT Polska

© Państwowy Instytut Badawczy NASK

Publikacja jest rozpowszechniana na zasadach licencji Creative Commons.

Uznanie autorstwa (CC BY) 4.0 Międzynarodowe.

SPIS TREŚCI

Statystyki zgłoszonych zagrożeń oraz zarejestrowanych incydentów

Zgłoszenia i incydenty cyberbezpieczeństwa

Statystyki przedstawione w tym rozdziale obejmują dane o liczbie zgłoszeń[1] oraz o liczbie incydentów obsłużonych przez CSIRT NASK w okresie od 1 do 30 kwietnia 2026 r. Wybrane dane ujęto również w szerszym horyzoncie czasowym, aby umożliwić obserwację zmian zachodzących w dłuższym okresie.

W dniu 3 kwietnia 2026 r. weszła w życie nowelizacja ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (UoKSC), która zmieniła definicje ustawowe, wprowadziła nowe kategorie podmiotów – podmioty kluczowe oraz podmioty ważne – a także rozszerzyła zakres raportowania o potencjalne zdarzenia dla cyberbezpieczeństwa (art. 2 pkt 11e), cyberzagrożenia (art. 2 pkt 4a) oraz poważne cyberzagrożenia (art. 2 pkt 11f). Nowelizacja zmodyfikowała również zasady klasyfikacji incydentów oraz poszerzyła katalog sektorów i podmiotów objętych ustawą. W konsekwencji dane publikowane od kwietnia 2026 r. mogą nie być w pełni porównywalne z danymi z okresów wcześniejszych.

Zgłoszenia zagrożeń oraz zarejestrowane incydenty – IV 2026

Tabela 1. Liczba zgłoszeń oraz zarejestrowanych incydentów od 1 do 30 kwietnia 2026 r.

Zgłoszone zagrożenia i zarejestrowane incydenty	Liczba
Zgłoszenia potencjalnych zdarzeń dla cyberbezpieczeństwa*	8,1 tys.
Zgłoszenia cyberzagrożeń*	38,7 tys.
Zgłoszenia incydentów	8,1 tys.
Zgłoszenia poważnych cyberzagrożeń*	2,0 tys.
Razem zgłoszenia	**56,9 tys.**
Zarejestrowane incydenty**	**23,7 tys.**

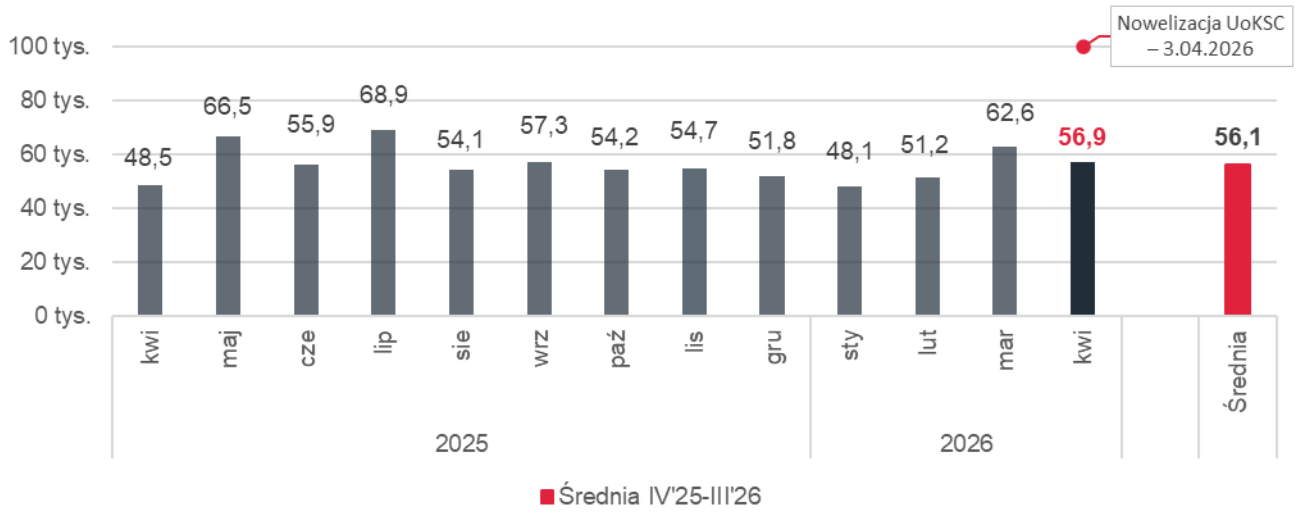
* Nowe kategorie zgłoszeń raportowane od kwietnia 2026 r.

** Incydenty zostały zarejestrowane na podstawie zgłoszeń incydentów, zgłoszeń cyberzagrożeń, zgłoszeń poważnych cyberzagrożeń oraz zgłoszeń potencjalnych zdarzeń dla cyberbezpieczeństwa.

[1] Zgłoszenia przesyłane są za pośrednictwem formularza dostępnego na stronie https://incydent.cert.pl lub są wysyłane na adres zgłoszeniowy cert@cert.pl, a także poprzez system S46. Otrzymane informacje o zagrożeniach stanowią podstawę rejestracji nowych incydentów.

W kwietniu 2026 r. zespół CERT Polska otrzymał **łącznie 56,9 tys. zgłoszeń**. Na ich podstawie **zarejestrowano 23,7 tys. incydentów** cyberbezpieczeństwa, które miały lub mogły mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych. Dotyczą one konkretnych kategorii zagrożeń, np. szkodliwych stron wyłudzających poufne informacje (ang. *phishing*), spamu czy ataku z użyciem szkodliwego oprogramowania. W wielu przypadkach jeden incydent był powiązany z kilkoma zgłoszeniami.

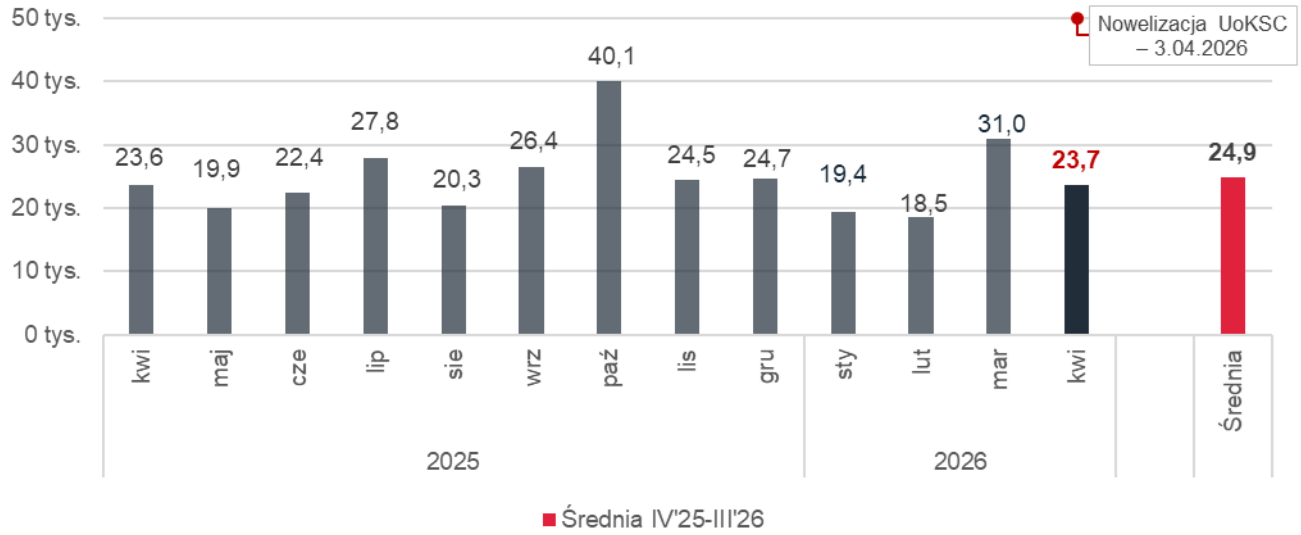
Zgłoszenia zagrożeń od IV 2025 do IV 2026



Wykres 1. Liczba wszystkich zgłoszeń od 01.04.2025 do 30.04.2026. Źródło: CERT Polska / CSIRT NASK.

Liczba wszystkich zgłoszeń odnotowanych w kwietniu 2026 r. była zbliżona do średniej liczonej z poprzednich 12 miesięcy. W porównaniu z analogicznym miesiącem 2025 r. liczba ta **zwiększyła się o 18%**. W stosunku do marca 2026 r. odnotowano **spadek o 9%**.

Zarejestrowane incydenty cyberbezpieczeństwa od IV 2025 do IV 2026



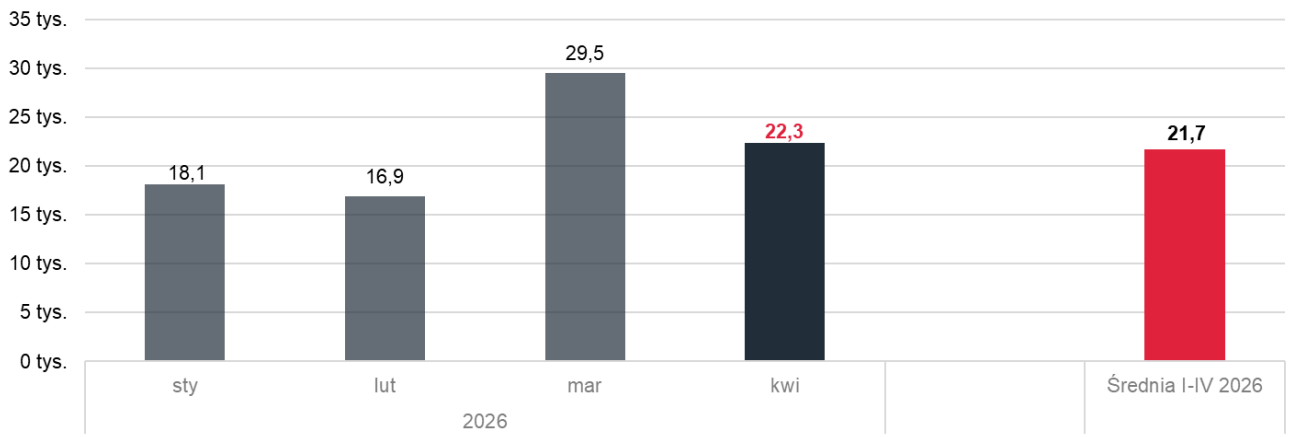
Wykres 2. Liczba zarejestrowanych incydentów od 01.04.2025 do 30.04.2026. Źródło: CERT Polska / CSIRT NASK.

Liczba incydentów zarejestrowanych w kwietniu 2026 r. wyniosła **23,7 tys.** W porównaniu z analogicznym miesiącem 2025 r. pozostawała ona na zbliżonym poziomie i nie przekroczyła średniej z poprzednich 12 miesięcy. W stosunku do marca 2026 r. odnotowano **spadek liczby incydentów o 24%**.

Liczba nazw szkodliwych domen wpisanych na Listę Ostrzeżeń CERT Polska I–IV 2026

Na Listę Ostrzeżeń wpisywane są domeny, które wprowadzają użytkowników w błąd i wyłudzają od nich dane. Takie domeny są blokowane na okres **6 miesięcy**. Po upływie tego czasu, jeśli nadal zawierają niebezpieczne treści, zostają **ponownie wpisane na listę** jako nowy wpis.

Lista Ostrzeżeń jest wykorzystywana przez operatorów telekomunikacyjnych, firmy, organizacje i samych użytkowników do **automatycznego blokowania dostępu do szkodliwych stron internetowych**, co pozwala ograniczać skutki ataków phishingowych i innych kampanii wymierzonych w obywateli Polski.



Wykres 3. Liczba nazw szkodliwych domen wpisanych na Listę Ostrzeżeń. Źródło: CERT Polska / CSIRT NASK.

Od 1 stycznia do 30 kwietnia 2026 r. na Listę Ostrzeżeń przed niebezpiecznymi stronami wpisano **86,9 tys.** szkodliwych domen, z czego w kwietniu 2026 r. dodano **22,3 tys.** nazw domen wykorzystywanych do wyłudzania danych osobowych, danych uwierzytelniających do kont bankowych i serwisów społecznościowych. Wartość ta w stosunku do marca 2026 r. **zmniejszyła się o 24%**.

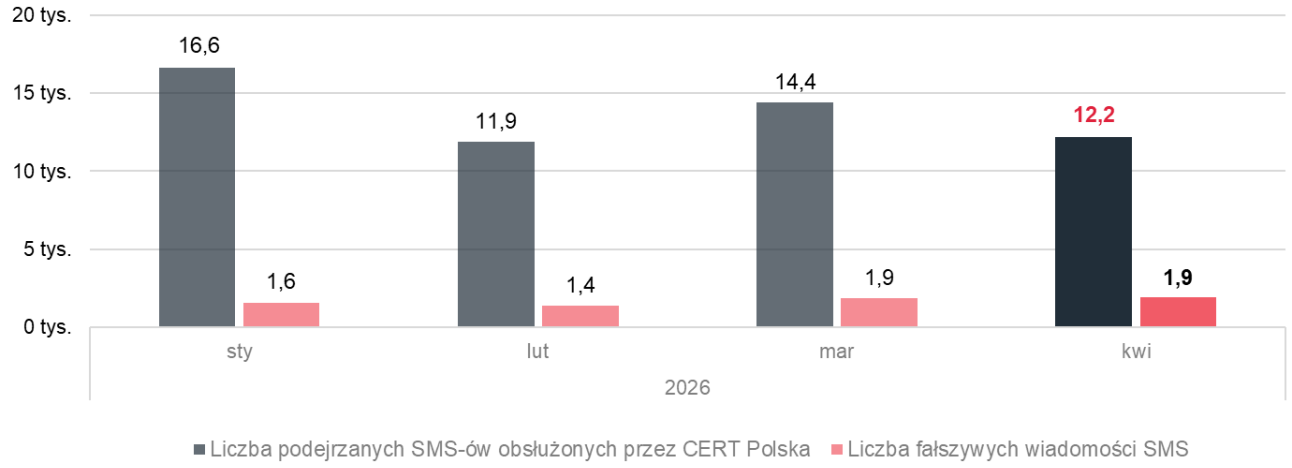
Lista Ostrzeżeń dostępna jest na stronie: CERT Polska/Lista Ostrzeżeń

Przykładowe nazwy fałszywych domen:

aldi-jonr.top; alebilet.336991.pl; allegro-lokalnie.ofei218129.sbs; be-eobuwie.shop; biedronka-pl.top; bnpparibas-auth.vercel.app; booking-guest-verlfy.com; ccc-pl.com; com-29381.sbs; disney-plus-center.com; doladujtelefon.click; dpd-pl.aberty.icu; energylandia-zator.eu; eobuwiekomfort-pl.shop; finance.portugal2026-news.com; i-santander.com; inwestycjapl9.info; lidl2026.shop; meblenataras24.shop; mennica-narodowa.info; mennicezlota.pl; mojogrod.store; myorlen-sp.com; ochnikrabat.top; oleksy-pl.sbs; olx.pl-aukcja4214.pl; onet.poczta.run; orln.live; pge.posta-online.info; pko-kredyt.pl; pl-ccc.top; rower-outlet.com; vinted.403773.pl; zoopolska.com

Liczba zgłoszeń wiadomości SMS przyjętych przez CERT Polska I–IV 2026

Od 1 stycznia do 30 kwietnia 2026 r. zespół CERT Polska zarejestrował **55,1 tys.** zgłoszeń podejrzanych SMS-ów. Liczba SMS-ów otrzymanych w kwietniu 2026 r. wyniosła **12,2 tys.** W porównaniu z marcem 2026 r. był to **spadek o 15%**. Wśród ogółu SMS-ów przyjętych w kwietniu 2026 r. **fałszywe wiadomości**, czyli takie, w których nadawca podszywa się pod inny podmiot, aby skłonić odbiorcę wiadomości do określonego działania – np. podania danych osobowych, przekazania pieniędzy, wejścia na stronę internetową lub instalacji oprogramowania, **stanowiły 16%**.



Wykres 4. Liczba SMS-ów zgłoszonych do CSIRT NASK w danym miesiącu.

Wzorce fałszywych wiadomości SMS I–IV 2026

Zgodnie z ustawą z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej CSIRT NASK **monitoruje występowanie smishingu** i **tworzy wzorce wiadomości**, które posiadają cechy pozwalające na uznanie ich za smishing. Działania te wykonuje na podstawie zgłoszeń podejrzanych wiadomości tekstowych (SMS) otrzymanych od odbiorców tych wiadomości oraz informacji otrzymanych od przedsiębiorców telekomunikacyjnych i innych podmiotów, np. banków, firm kurierskich, platform inwestycyjnych. CSIRT NASK zapewnia dostęp do informacji o występowaniu smishingu wraz ze wzorcami wiadomości Komendantowi Centralnego Biura Zwalczania Cyberprzestępczości, Prezesowi Urzędu Komunikacji Elektronicznej i przedsiębiorcom telekomunikacyjnym. Podejrzane SMS-y można zgłaszać do CSIRT NASK poprzez bezpłatny skrócony numer **8080**. W kwietniu 2026 r., na podstawie wytworzonych przez CERT Polska wzorców fałszywych wiadomości SMS, zablokowano łącznie **14,4 tys.** SMS-ów. Dane o zablokowanych wiadomościach SMS są szacowane na podstawie raportów przesyłanych przez operatorów telekomunikacyjnych z uwzględnieniem procentowego udziału tych operatorów w rynku telefonii mobilnej.

Tabela 2. Liczba wytworzonych wzorców fałszywych wiadomości SMS.

Wzorce fałszywych wiadomości SMS w 2026	sty	lut	mar	kwi	Razem
Liczba wytworzonych wzorców	118	97	85	**80**	**380**

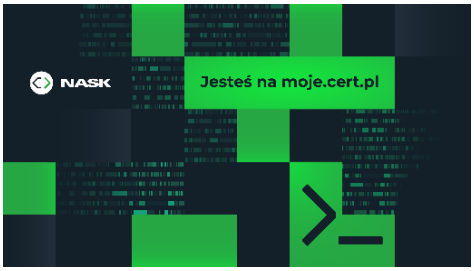
Wykaz wzorców wiadomości SMS znajduje się na stronie: telegraf.cert.pl

Moje.cert.pl

W 2025 r. zespół CERT Polska udostępnił bezpłatny serwis moje.cert.pl. Z serwisu mogą korzystać zarówno osoby prywatne posiadające stronę internetową, jak i małe firmy czy duże instytucje publiczne udostępniające wiele skomplikowanych systemów. Zarejestrowany użytkownik moje.cert.pl

może zamówić bezpłatne skanowanie bezpieczeństwa wszystkich swoich domen, uzyskać informacje na temat wycieków haseł użytkowników w swojej domenie, otrzymywać informacje o infekcjach szkodliwym oprogramowaniem i innych zagrożeniach w swoich sieciach (ta funkcja jest dostępna dla administratorów serwerów i sieci), a także sprawdzić, czy dana sieć jest chroniona przez Listę Ostrzeżeń przed niebezpiecznymi stronami. Ponadto w serwisie, w zakładce „Komunikaty" pojawiają się – i będą na bieżąco dodawane – ostrzeżenia dotyczące polskiej cyberprzestrzeni oraz alerty o podatnościach. Komunikaty te są dostępne na stronie także dla niezarejestrowanych użytkowników, a od sierpnia 2025 r. każdy może otrzymywać je również w wiadomości e-mail. Moje.cert.pl korzysta m.in. z systemów **Artemis** (skanowanie stron) i **n6** (informacje o zagrożeniach dla adresacji IP) – narzędzi pozwalających chronić dane i infrastrukturę.

W kwietniu 2026 r. w serwisie moje.cert.pl **zarejestrowało się 1,1 tys. nowych użytkowników**.



W okresie od 1 do 30 kwietnia 2026 r. CERT Polska wysłał **7,9 tys. powiadomień w ramach serwisu moje.cert.pl dotyczących wykrytych podatności lub błędnych konfiguracji**. Powiadomienia o wykrytych nieprawidłowościach zostały wysłane do osób, które zgłosiły daną stronę do skanowania w serwisie moje.cert.pl, a także do ich współpracowników dodanych w serwisie.

Więcej: moje.cert.pl

Podatności CVE

Zespół CERT Polska od sierpnia 2023 r. pełni funkcję CNA (ang. *CVE Numbering Authority*) – współtworzy bazę podatności poprzez nadawanie numerów CVE, które służą do identyfikacji i katalogowania publicznie ujawnionych podatności (więcej: CERT Polska/CNA). W kwietniu 2026 r. zespół CERT Polska nadał **21** numerów CVE. Wśród wykrytych podatności znalazły się podatności w oprogramowaniu m.in. GREENmod, Szafir, Hydrosystem Control System, Fudo Enterprise oraz LEX Baza Dokumentów.

Lista opublikowanych podatności dostępna jest na stronie: CERT Polska/CVE

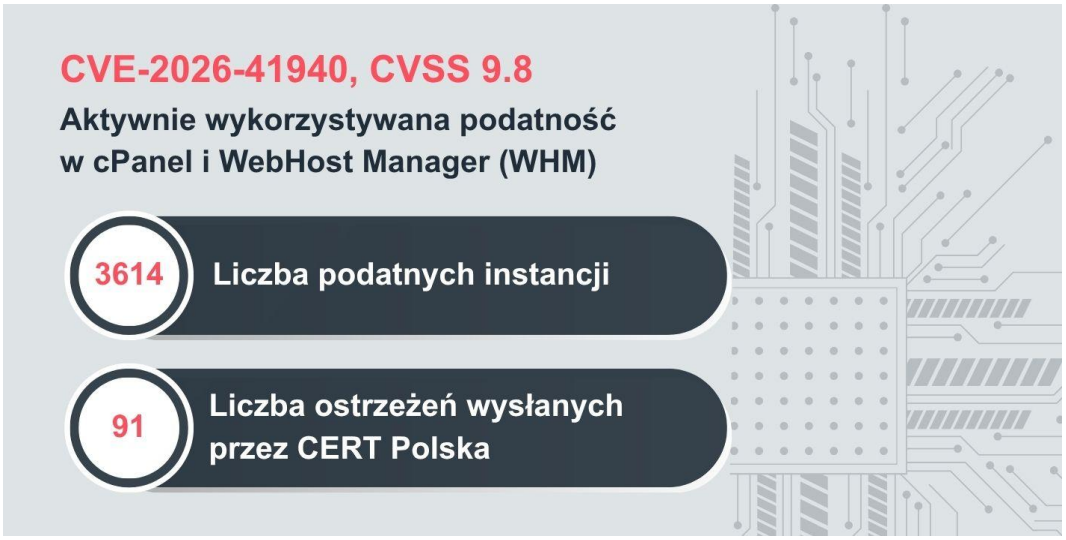
Tabela 3. Nadane numery CVE od 1 stycznia do 30 kwietnia 2026 r.

Numery CVE w 2026	sty	lut	mar	kwi	Razem
Liczba opublikowanych numerów CVE	16	12	32	**21**	**81**

Wybrane podatności i ich wpływ na krajobraz cyberbezpieczeństwa w Polsce – IV 2026

Podatność pozwala na obejście uwierzytelniania i zmianę haseł użytkowników (w tym administratora), co prowadzi do pełnego przejęcia systemu. W praktyce oznacza to możliwość uzyskania nieautoryzowanego dostępu do interfejsu zarządzania serwerem (BMC) i wykonania operacji administracyjnych bez znajomości danych logowania. Atakujący może zmodyfikować konfigurację sprzętową, uzyskać dostęp do konsoli KVM lub trwale przejąć kontrolę nad infrastrukturą na poziomie sprzętowym. Podatność otrzymała krytyczną ocenę CVSS (ang. *Common Vulnerability Scoring System*) 10.0.

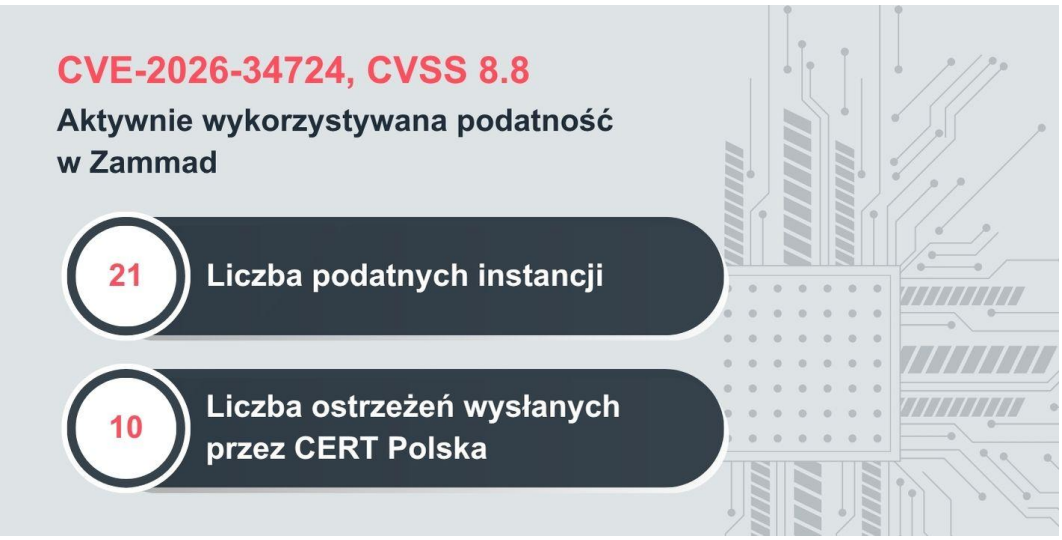
Więcej: https://socradar.io/blog/cve-2026-20093-cisco-imc-flaw



Krytyczna podatność umożliwia obejście logowania i uzyskanie dostępu administracyjnego bez uwierzytelnienia. Oznacza to możliwość uzyskania pełnych uprawnień administratora panelu

hostingowego bez poprawnych danych logowania, co skutkuje kompromitacją wszystkich zarządzanych usług i kont. Atakujący może m.in. modyfikować konfigurację serwera, uzyskać dostęp do danych klientów oraz wdrożyć trwałe mechanizmy dostępu.

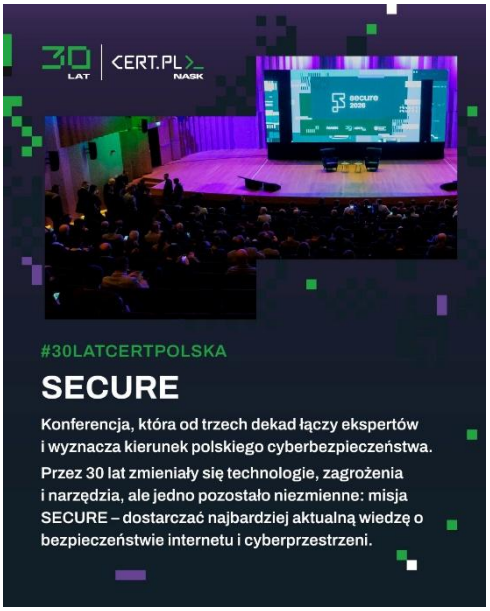
Więcej: https://www.catonetworks.com/blog/threat-brief-cve-2026-41940-critical-cpanel-whm-authentication-bypass-actively-exploited-in-the-wild



Luka typu Server-Side Template Injection (SSTI) w Zammad umożliwia zdalne wykonanie kodu (RCE), ale wymaga dostępu z wysokimi uprawnieniami. Podatność pozwala na wstrzyknięcie i wykonanie złośliwego kodu w aplikacji, jeśli atakujący ma wpływ na przetwarzane szablony (np. poprzez konfigurację lub dane wejściowe). W efekcie możliwe jest wykonywanie poleceń systemowych, eskalacja wpływu w środowisku oraz uzyskanie dostępu do danych przetwarzanych przez aplikację.

Więcej: https://www.sentinelone.com/vulnerability-database/cve-2026-34724

Wybrane informacje



8 kwietnia w Muzeum Historii Polski w Warszawie odbyła się **29. edycja konferencji SECURE** organizowanej przez NASK-PIB i działający w jego ramach zespół CERT Polska. Wydarzenie jak co roku było poświęcone przede wszystkim diagnozie aktualnych cyberzagrożeń, którymi są m.in. oszustwa inwestycyjne, incydenty ransomware, działania grup APT. Ważnym tematem była nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa.

Eksperci z CERT Polska wystąpili z prezentacjami: „Doświadczenia CERT Polska z realizacji projektu tworzenia CSIRT sektorowego", „Co nowego w moje.cert.pl?", „Jak informować o incydentach – wymiar prawny i praktyczny" oraz „Automatyzacja znajdowania błędów i podatności z wykorzystaniem fuzzingu i agentów opartych o LLM-y".

Tegoroczna edycja miała charakter jubileuszowy w związku z 30-leciem działalności zespołu CERT Polska. Była to okazja do przyjrzenia się, jak na przestrzeni lat zmieniały się cyberzagrożenia oraz narzędzia i metody służące do walki z nimi. O tym oraz o misji CERT Polska rozmawiali obecny kierownik zespołu oraz jego poprzednicy.

Więcej: nask.pl/SECURE 2026

8 kwietnia zespół CERT Polska opublikował **„Raport roczny 2025 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu"**. Najważniejsze wnioski wynikające z analiz zawartych w publikacji przedstawił kierownik zespołu CERT Polska podczas konferencji SECURE. W 2025 r. zespół zarejestrował 260 783 unikalnych incydentów bezpieczeństwa. To wzrost o 152% w stosunku do 2024 r. Wynika on m.in. z rosnącej świadomości użytkowników w zakresie zagrożeń oraz z rozwoju systemów CERT Polska stosowanych do monitorowania, analizowania i zwalczania incydentów bezpieczeństwa. Najpowszechniejszym rodzajem zagrożeń były oszustwa komputerowe, które stanowiły 97% wszystkich obsłużonych zdarzeń. W raporcie zostały szczegółowo opisane także pozostałe zagrożenia oraz narzędzia i systemy stworzone przez CERT Polska przyczyniające się do zapewnienia bezpieczeństwa w sieci, m.in. Lista Ostrzeżeń, moje.cert.pl, n6.

Więcej: cert.pl/Raport roczny CERT Polska 2025

3 kwietnia na stronie cert.pl ukazał się artykuł pt. **„Analiza cifrat: czy to ewolucja mobilnego RATa?”**. Zespół CERT Polska przeanalizował próbkę szkodliwego oprogramowania na Androida dystrybuowaną z wykorzystaniem infrastruktury podszywającej się pod Booking.com. Próbka była rozsyłana za pomocą wiadomości phishingowych, które prowadziły do fałszywej strony aktualizacji aplikacji Booking Pulse i w konsekwencji do pobrania złośliwego pliku APK. Aplikacja widoczna dla użytkownika była jedynie początkiem całej ścieżki infekcji. Analiza statyczna i dynamiczna wykazały, że pobrany plik APK jest wieloetapowym dropperem, który rozpakowuje drugi plik APK, następnie ukryty końcowy moduł, a ostatecznie uruchamia RAT wykorzystujący usługi ułatwień dostępu i komunikujący się przez WebSocket.

Więcej: cert.pl/Analiza cifrat: czy to ewolucja mobilnego RATa?

7 kwietnia w rozmowie opublikowanej na stronie nask.pl **kierownik zespołu CERT Polska** opowiedział m.in. o sztucznej inteligencji jako trendzie, który zmienił krajobraz cyberzagrożeń w 2025 r., o największych wyzwaniach, z jakimi mierzą się eksperci z CERT Polska, oraz podkreślił, że organizacje muszą zadbać o stałe rozwijanie kompetencji i podnoszenie świadomości, jak rozpoznawać zagrożenia i jak na nie reagować.

Więcej: nask.pl/AI w cyberbezpieczeństwie to miecz obosieczny

---

16 kwietnia zespół **CERT Polska poinformował**, że zasilił bazę serwisu bezpiecznedane.gov.pl informacjami dotyczącymi wycieków danych z dwóch sklepów online: vegehome.pl i polskiekoldry.pl. Po zalogowaniu do serwisu użytkownik może sprawdzić, czy jego adres e-mail lub numer telefonu znajdował się w którymś z wycieków.

Więcej: X/CERT Polska/Zasilenie bazy serwisu bezpiecznedane.gov.pl

Wystąpienia ekspertów CERT Polska

- 15 kwietnia – wystąpienie pt. „National CSIRT as a CVD Hub: Lessons from CERT.PL's Vulnerability Coordination Cases" na temat doświadczeń CERT Polska w obszarze skoordynowanego ujawniania podatności, konferencja VulnCon 2026, Scottsdale, Arizona.

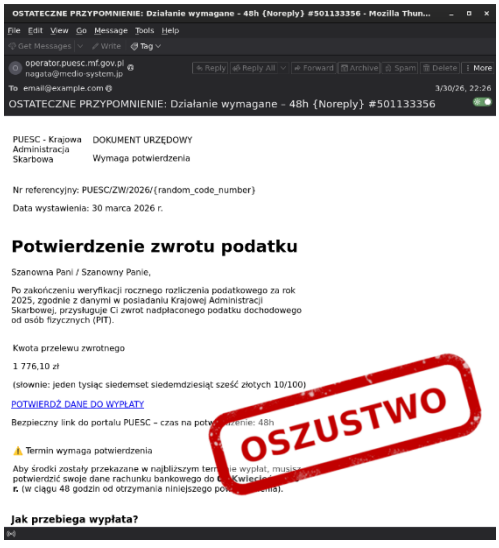
  Więcej: first.org/conference/program
- 17 kwietnia – udział w panelu dyskusyjnym „Bezpieczeństwo wodne w erze cyfrowej rewolucji" podczas Forum Wody w Białymstoku.

  Więcej: wobi.pl/Forum Wody – podsumowanie
- 21 kwietnia – prezentacja „Moje.cert.pl – darmowe narzędzia cyberbezpieczeństwa" na temat rozwoju jednego z kluczowych narzędzi wspierających administratorów i zespoły IT, konferencja online Admin Days.

  Więcej: Admin Days 2026 – informacje, agenda

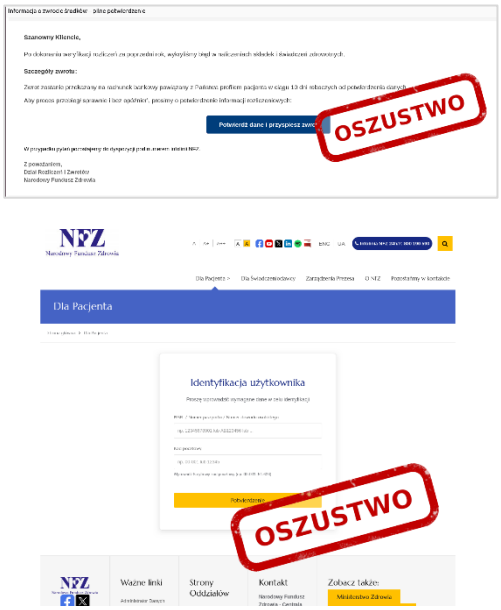
Komunikaty o zagrożeniach

Informacje o zaobserwowanych kampaniach publikowane przez zespół CERT Polska w serwisie moje.cert.pl oraz w serwisach społecznościowych.



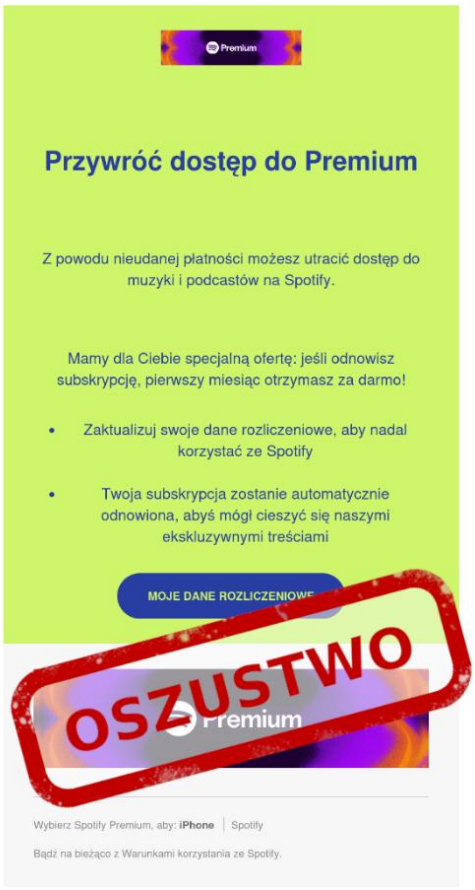
Zespół CERT Polska obserwował kolejną falę e-maili, w których oszuści podszywają się pod Krajową Administrację Skarbową. Wiadomości zawierają link do strony przypominającej Platformę Usług Elektronicznych Skarbowo-Celnych i informują o rzekomej możliwości odebrania zwrotu podatku. Po przejściu na stronę użytkownik jest proszony o podanie danych osobowych, m.in. numeru PESEL, a następnie danych karty płatniczej.

W przypadku otrzymania tego typu wiadomości przede wszystkim należy sprawdzić, czy adres strony, do której kieruje link przesłany w wiadomości, jest zgodny z oficjalną domeną instytucji. Warto też zalogować się do systemu i zweryfikować, czy tam również znajduje się komunikat podany w e-mailu.

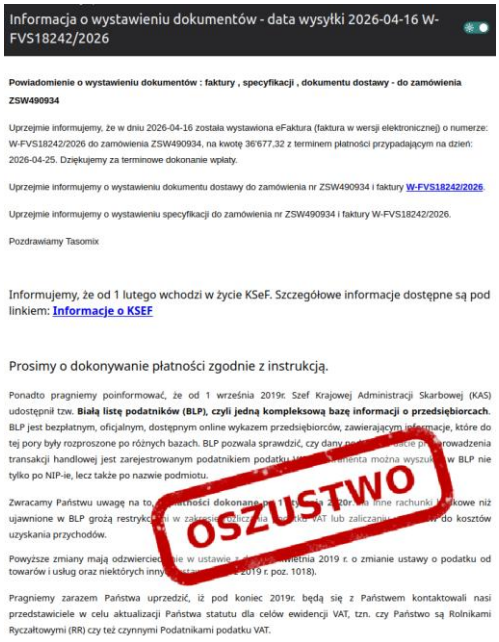


Zespół CERT Polska informował o kampanii wykorzystującej temat rozliczeń zdrowotnych. Do użytkowników trafiają wiadomości z informacją o rzekomych nieprawidłowościach w rozliczeniach składek NFZ. Wiadomości oprócz prośby o weryfikację danych zawierają link prowadzący do strony, która łudząco przypomina oficjalny serwis. Celem oszustów jest pozyskanie danych, takich jak loginy, dane osobowe czy informacje finansowe.

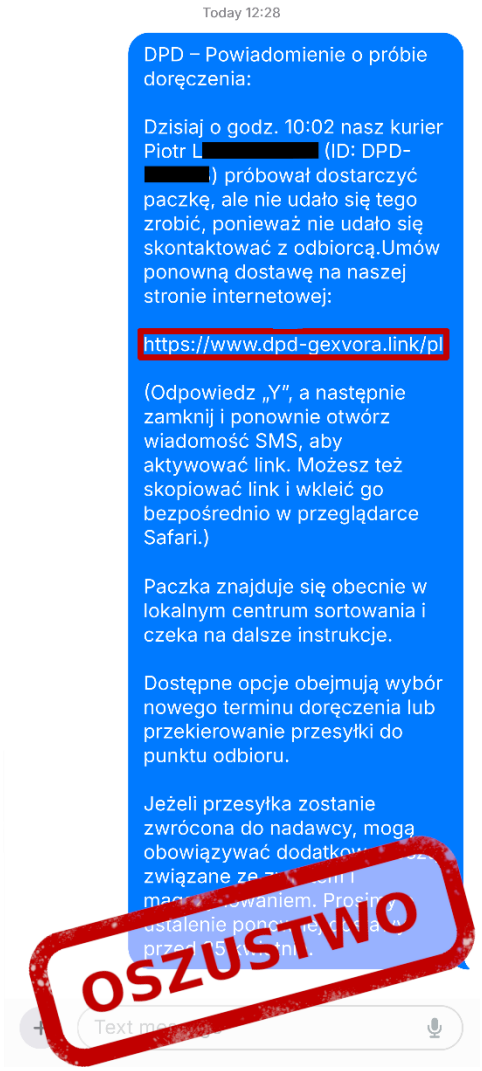
Zespół CERT Polska obserwował kampanię SMS-ową, która wykorzystuje motyw rzekomej aktualizacji karty SIM. Wiadomość zawiera informację o konieczności weryfikacji numeru telefonu, aby uniknąć blokady karty SIM. Dołączony link prowadzi do witryny podszywającej się pod stronę operatora, która zawiera panel logowania. Na stronie użytkownik proszony jest o podanie loginu, hasła oraz kodu, który przychodzi w wiadomości SMS. Celem oszustów jest przejęcie dostępu do konta.



Zespół CERT Polska ostrzegał przed kampanią phishingową, która wykorzystuje wizerunek platformy Spotify. Oszuści wysyłają wiadomości z informacją o rzekomo nieudanej płatności za subskrypcję usługi premium i grożą utratą dostępu do niej. Wiadomość zawiera odnośnik prowadzący do fałszywej strony przypominającej serwis Spotify. Odbiorca proszony jest o podanie danych logowania i szczegółów karty płatniczej, które w rzeczywistości trafiają do przestępców.



Zespół CERT Polska monitorował kampanię wymierzoną w użytkowników KSeF. Oszuści rozsyłają fałszywe powiadomienia o nowej fakturze. W wiadomości podany jest link, który rzekomo prowadzi do jej pobrania. Kliknięcie w link powoduje pobranie złośliwego oprogramowania ze strony stworzonej przez przestępców, a otwarcie pobranego pliku skutkuje zainfekowaniem komputera. Otrzymywanie powiadomień o fakturach to rutyna w większości firm, dlatego oszuści liczą na automatyczne kliknięcie – bez weryfikacji nadawcy czy adresu linku. Dokumenty należy pobierać wyłącznie po zalogowaniu bezpośrednio na platformę KSeF.

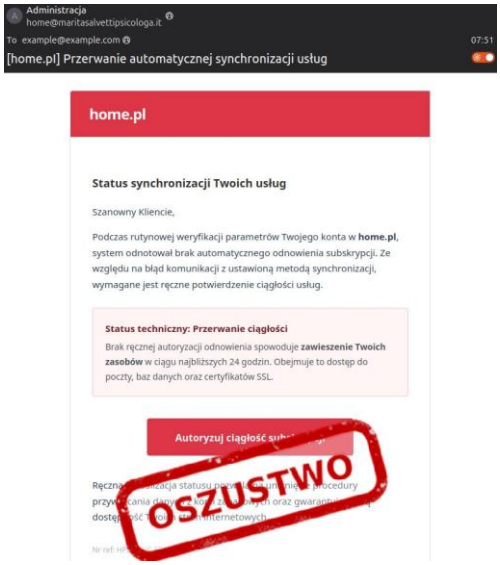


Zespół CERT Polska obserwował kampanię SMS-ową wykorzystującą wizerunek firmy DPD. Cyberprzestępcy piszą o nieudanej próbie dostarczenia paczki i konieczności umówienia nowego terminu. Wiadomości zawierają link przenoszący na fałszywą stronę, która imituje oficjalny serwis kurierski. Użytkownicy proszeni są o podanie danych kontaktowych oraz danych karty płatniczej – rzekomo w celu uiszczenia opłaty za zmianę terminu dostawy.

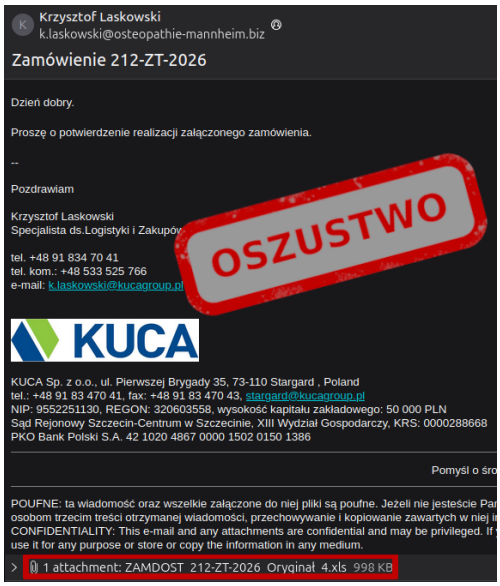
Aby chronić swoje dane, zawsze należy zwracać uwagę na adres domeny podanej w wiadomości, a status przesyłki sprawdzać bezpośrednio na oficjalnej stronie przewoźnika.

W serwisie moje.cert.pl opublikowano ostrzeżenie CSIRT KNF przed kampanią phishingową, w której oszuści podszywają się pod ZUS. W fałszywych wiadomościach SMS informują oni o rzekomym błędzie w stanie rozliczeń ubezpieczenia zdrowotnego. Dalej zachęcają do kliknięcia w znajdujący się w wiadomości link, a w kolejnym kroku wymagają podania numeru PESEL oraz informacji o karcie płatniczej.

Zespół CERT Polska obserwował kolejną falę kampanii phishingowej związanej z końcem okresu rozliczeń podatkowych, w której oszuści rozsyłają e-maile podszywające się pod Krajową Administrację Skarbową. Informują w nich o rzekomym zwrocie nadpłaconego podatku i zachęcają do podania danych potrzebnych do jego odebrania. Odnośnik zawarty w wiadomości prowadzi na fałszywą stronę Platformy Usług Elektronicznych Skarbowo-Celnych, gdzie przestępcy próbują wyłudzić numer PESEL, dane osobowe oraz dane karty płatniczej.



Zespół CERT Polska ostrzegał przed kampanią phishingową wykorzystującą wizerunek home.pl. Wiadomości zawierają link prowadzący do strony imitującej panel logowania serwisu hostingowego, na której użytkownik proszony jest o podanie loginu i hasła. Wprowadzone dane trafiają do przestępców.



Zespół CERT Polska informował o szeroko zakrojonej kampanii dystrybucji szkodliwego oprogramowania. Oszuści rozsyłają wiadomości e-mail, w których podszywają się pod prawdziwe firmy i nakłaniają do otwarcia rzekomej faktury lub opisu zamówienia. Do wiadomości dołączony jest dokument typu .xls, który z pozoru wygląda jak arkusz kalkulacyjny. Dokument ten jest jednak specjalnie przygotowany – wykorzystuje podatności występujące w wersjach pakietu Office wydanych przed 2017 rokiem i po otwarciu pobiera oprogramowanie wykradające dane użytkownika, tzw. stealer.

W przypadku otrzymania takiej wiadomości należy zweryfikować adres e-mail nadawcy, potwierdzić temat telefonicznie (samodzielnie znaleźć numer firmy, która rzekomo wysłała e-mail). Należy również dbać o to, żeby używane programy były aktualne i miały wsparcie producenta.

Zespół CERT Polska obserwował kampanię wykorzystującą motyw rzekomej nadpłaty za energię elektryczną. Oszuści rozsyłają nieprawdziwe wiadomości z informacją o zwrocie środków oraz linkiem prowadzącym do strony podszywającej się pod Orlen. Po przejściu do wskazanego formularza użytkownik proszony jest o podanie danych osobowych oraz danych karty płatniczej – informacje te trafiają do oszustów.

Zespół CERT Polska obserwował wzrost liczby fałszywych stron oferujących złoto, srebro, diamenty i produkty kolekcjonerskie. Schemat wyłudzeń polega na tworzeniu serwisów, które wizualnie przypominają ofertę znanych podmiotów, takich jak Mennica Polska. Na stronach są prezentowane atrakcyjne produkty o charakterze inwestycyjnym, a klienci są zachęcani do szybkiego zakupu.

W przypadku takich witryn warto: sprawdzić adres strony i porównać go z oficjalnymi domenami, zweryfikować opinie o sklepie oraz kontakt do sprzedawcy, zapoznać się z regulaminem i danymi rejestrowymi firmy, zachować ostrożność wobec wyjątkowo korzystnych okazji.

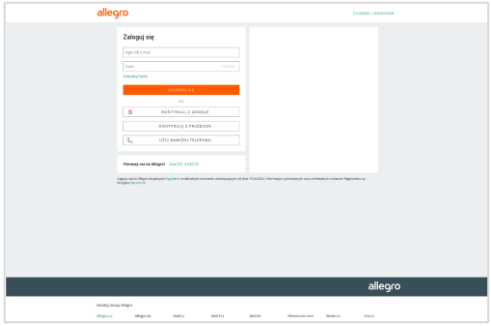
Więcej: Facebook/CERT Polska, X/CERT Polska oraz moje.cert.pl/komunikaty

Opis najczęściej występujących kampanii – IV 2026

Fałszywe strony oferujące wysokodochodowe inwestycje

Zespół CERT Polska w dalszym ciągu obserwował wzmożoną kampanię phishingową, w której oszuści podszywają się pod różnego rodzaju koncerny paliwowo-energetyczne, firmy i instytucje, m.in. Lotos, Tesla, PGNiG, PGE, Baltic Pipe. Oszuści reklamują w mediach społecznościowych oraz w wyszukiwarkach internetowych nieistniejące programy dla akcjonariuszy indywidualnych, a także rozsyłają wiadomości, w których informują o możliwości inwestowania środków z rzekomo wysokim zyskiem za pośrednictwem platform inwestycyjnych. Osoby zainteresowane dużymi zarobkami oraz inwestycjami w handel ropą, gazem czy akcje firmy są proszone o udostępnienie swoich danych osobowych i kontaktowych w formularzu, do którego prowadzi link umieszczony w reklamie lub wiadomości. Następnie z użytkownikiem kontaktuje się telefonicznie osoba podająca się za konsultanta i zachęca do zainwestowania środków w kryptowaluty, obligacje czy akcje firm na platformie, która – jak się później okazuje – uniemożliwia wypłaty zainwestowanych pieniędzy. Celem oszustów jest wyłudzenie środków finansowych.

Fałszywe strony Allegro

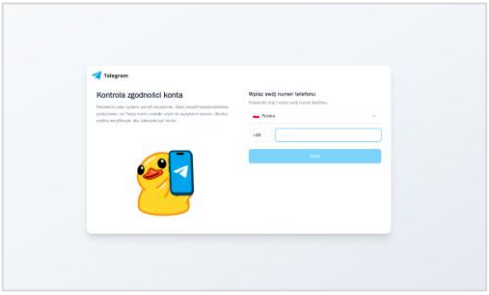


Zespół CERT Polska obserwował wzmożoną kampanię phishingową wykorzystującą wizerunek platformy Allegro. Na fałszywych stronach internetowych znajduje się panel logowania do tego serwisu służący do wyłudzania danych uwierzytelniających od użytkowników Allegro.

Fałszywe strony serwisu Gazeta.pl

Zespół CERT Polska rejestrował incydenty, w których atakujący za pośrednictwem stron internetowych podszywają się pod serwis Gazeta.pl. Na fałszywych stronach oszuści publikują artykuły, w których opisują rzekome inwestycje znanych osób w kryptowaluty, obligacje czy akcje na platformie inwestycyjnej. Platforma ta w rzeczywistości uniemożliwia wypłatę zainwestowanych pieniędzy, a celem oszustów jest wyłudzenie środków finansowych.

Fałszywe strony komunikatora Telegram



Zespół CERT Polska obserwował kampanię mającą na celu przejmowanie kont użytkowników komunikatora Telegram. Oszuści wysyłają wiadomości SMS z informacją, że konto użytkownika mogło brać udział w wysyłce spamu. Link zawarty w treści wiadomości prowadzi do strony internetowej, która wyłudza numer telefonu. Następnie użytkownik jest proszony o wpisanie kodu weryfikacyjnego wysłanego na jego numer – podanie go umożliwia atakującym przejęcie konta Telegram.

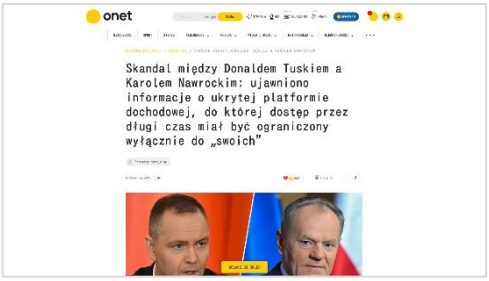
Fałszywe strony kanału Polsat News

Zespół CERT Polska rejestrował incydenty, w których oszuści wykorzystują wizerunek kanału telewizyjnego Polsat News. Na fałszywych stronach internetowych umieszczają artykuły na temat inwestycji, na których rzekomo można zarobić z dużym zyskiem, i zachęcają czytelników do rejestracji na platformie, która w rzeczywistości służy do wyłudzania środków finansowych.

Fałszywe strony OLX

Zespół CERT Polska zarejestrował incydenty, w których atakujący za pośrednictwem stron internetowych podszywają się pod serwis OLX. Strony te zawierają panel logowania do tego serwisu służący do wyłudzania od użytkowników danych uwierzytelniających.

Fałszywe strony serwisu Onet.pl

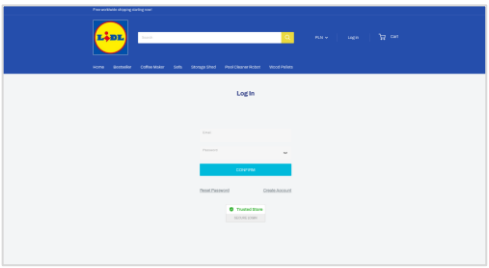


Zespół CERT Polska obserwował kampanię phishingową, w której oszuści podszywają się pod serwis Onet.pl i umieszczają na fałszywych stronach internetowych artykuły służące do reklamowania nieistniejących programów inwestycyjnych. Celem oszustów jest wyłudzenie środków finansowych.

Fałszywe strony firmy Orlen

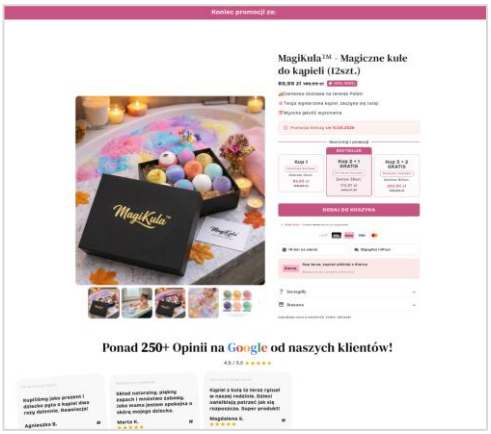
Zespół CERT Polska zarejestrował kampanię phishingową, w której wykorzystywany jest wizerunek Orlenu. Cel oszustów to wyłudzenie środków finansowych poprzez fałszywą platformę inwestycyjną.

Fałszywe panele logowania wykorzystujące markę Lidl



Zespół CERT Polska obserwował incydenty, w których oszuści wykorzystują wizerunek marki Lidl.
Na fałszywych stronach internetowych znajduje się panel logowania do sklepu internetowego. Celem oszustów jest pozyskanie od użytkowników danych uwierzytelniających.

Fałszywe strony sklepów internetowych



Zespół CERT Polska rejestrował incydenty, w których oszuści tworzą fałszywe sklepy internetowe zawierające towary w atrakcyjnych cenach. Na tych stronach zazwyczaj nie ma możliwości zapłaty za pobraniem, a na wielu z nich jedyną metodą płatności jest karta płatnicza.