LUTY 2026

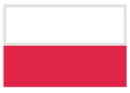
Podsumowanie Miesiąca CERT POLSKA

Nr 2/2026

CERT.PL NASK

CSIRT NASK

PODSUMOWANIE MIESIĄCA CERT POLSKA



PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTERSTWA CYFRYZACJI

TLP: CLEAR

Autor: zespół CERT Polska

SPIS TREŚCI

Statystyki zarejestrowanych zagrożeń 4

Moje.cert.pl 8

Podatności CVE 9

Wybrane podatności i ich wpływ na krajobraz cyberbezpieczeństwa w Polsce – II 2026 9

Wybrane informacje 10

Komunikaty o zagrożeniach 12

Opis najczęściej występujących kampanii – II 2026 17

Statystyki zarejestrowanych zagrożeń

Zgłoszenia i incydenty cyberbezpieczeństwa

Statystyki prezentowane poniżej obejmują dane o liczbie zarejestrowanych zgłoszeń[1] oraz o liczbie incydentów obsłużonych przez zespół CERT Polska w okresie od 1 do 28 lutego 2026 r.
Dla lepszego zobrazowania pojawiających się trendów niektóre z tych danych pokazywane są w dłuższej perspektywie czasu.

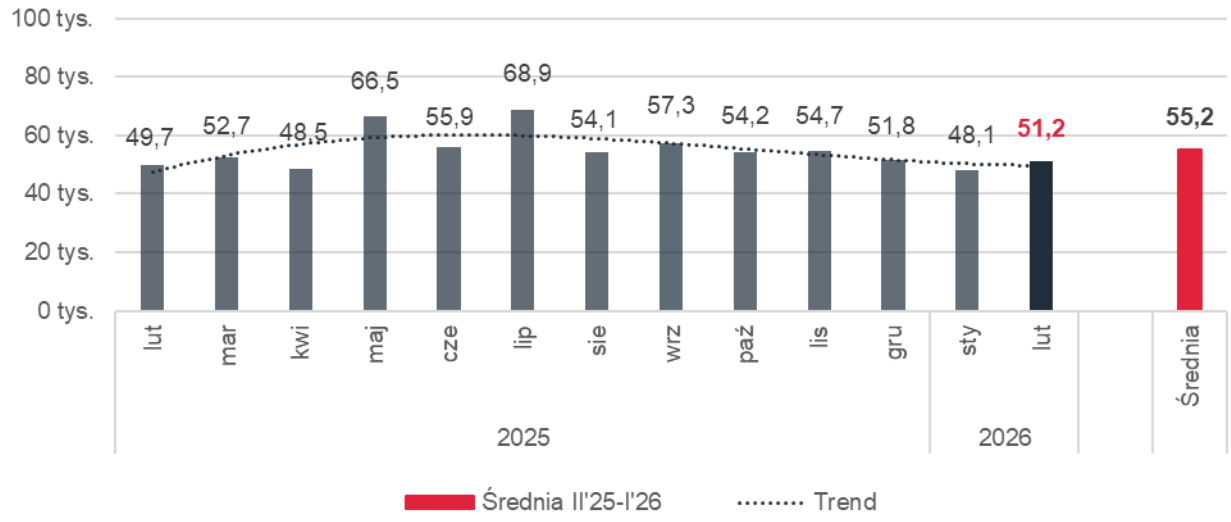
Zarejestrowane zgłoszenia i incydenty cyberbezpieczeństwa – II 2026

Tabela 1. Liczba zarejestrowanych zgłoszeń i incydentów od 1 do 28 lutego 2026 r.

Zagrożenia cyberbezpieczeństwa	Liczba
Zarejestrowane zgłoszenia	**51,2 tys.**
w tym zarejestrowane (obsłużone) incydenty	**18,5 tys.**

W lutym 2026 r. zespół CERT Polska otrzymał łącznie **51,2 tys.** zgłoszeń, które zostały przeanalizowane i pogrupowane. Na ich podstawie zarejestrowano **18,5 tys.** incydentów bezpieczeństwa, które miały lub mogły mieć niekorzystny wpływ na cyberbezpieczeństwo. 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.

Zarejestrowane zgłoszenia cyberbezpieczeństwa od II 2025 do II 2026

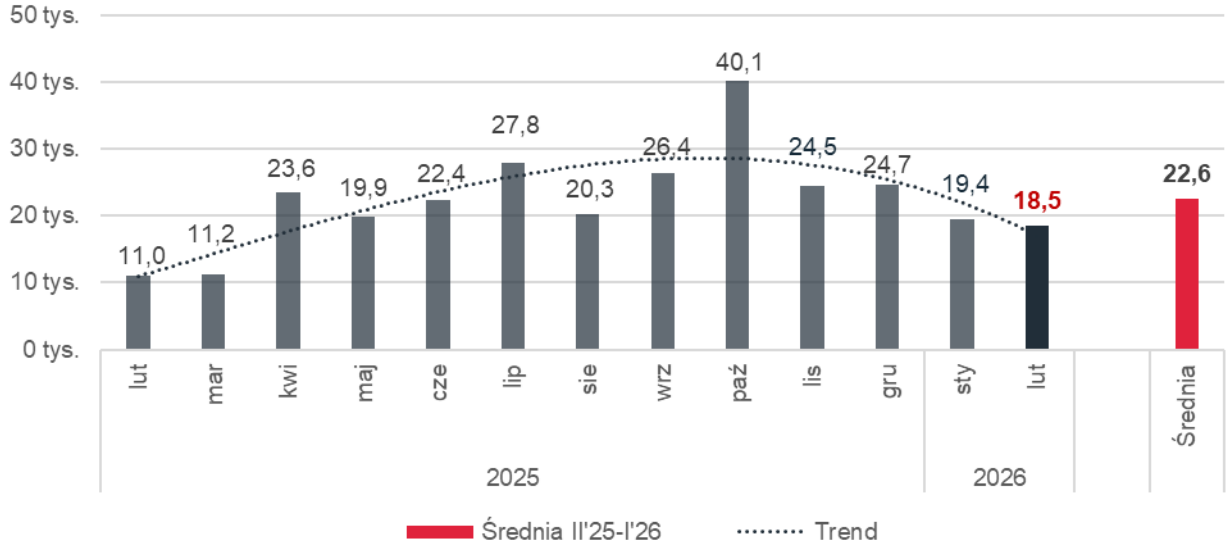


Wykres 1. Liczba zarejestrowanych zgłoszeń od 01.02.2025 do 28.02.2026. Źródło: CERT Polska / CSIRT NASK.

[1] Zgłoszenia przesyłane są za pośrednictwem formularza dostępnego na stronie https://incydent.cert.pl lub są wysyłane na adres zgłoszeniowy cert@cert.pl. Rejestrowane są także powiadomienia otrzymywane bezpośrednio od przedstawicieli sektora publicznego oraz prywatnego. Otrzymane informacje o zagrożeniach cyberbezpieczeństwa stanowią podstawę rejestracji nowych zgłoszeń, incydentów lub są rejestrowane wyłącznie do celów statystycznych, jako zgłoszenia niemające charakteru realnego zagrożenia.

Liczba zgłoszeń odnotowanych w lutym 2026 r. pozostawała poniżej średniej liczonej z poprzednich 12 miesięcy. W porównaniu z analogicznym miesiącem 2025 r. liczba ta **zwiększyła się o 3%**. W stosunku do stycznia 2026 r. był to **wzrost o 7%**.

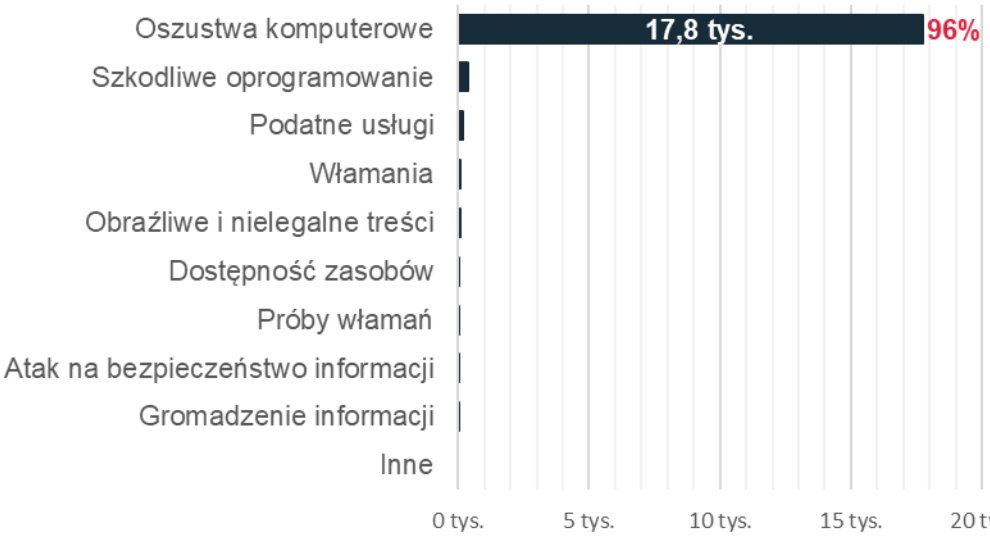
Zarejestrowane incydenty cyberbezpieczeństwa od II 2025 do II 2026



Wykres 2. Liczba zarejestrowanych incydentów od 01.02.2025 do 28.02.2026. Źródło: CERT Polska / CSIRT NASK.

Liczba incydentów zarejestrowanych w lutym 2026 r. wyniosła **18,5 tys.** W porównaniu z analogicznym miesiącem 2025 r. liczba incydentów w lutym 2026 r. **zwiększyła się o 68%** i pozostawała poniżej średniej liczonej z 12 poprzednich miesięcy. W stosunku do stycznia 2026 r. liczba zarejestrowanych incydentów **zmniejszyła się o 4%**.

Rodzaje zarejestrowanych zagrożeń – II 2026



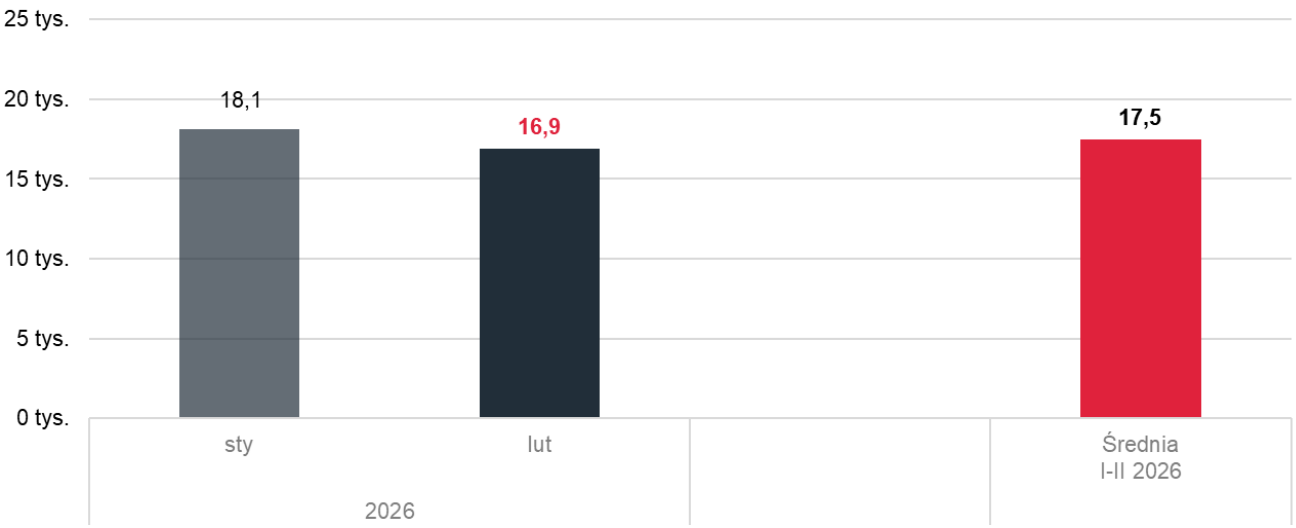
Wykres 3. Liczba zarejestrowanych incydentów według rodzaju od 1 do 28 lutego 2026 r. Źródło: CERT Polska / CSIRT NASK.

W analizowanym okresie zdecydowanie najczęściej występującą kategorią zagrożeń były oszustwa komputerowe. Wśród ogółu obsłużonych incydentów (**18,5 tys.**) stanowiły one **96%**. Najbardziej rozpowszechnionym rodzajem oszustw komputerowych były próby wyłudzania poufnych danych, np. loginu i hasła do poczty, strony banku, portalu społecznościowego czy innej usługi online (ang. *phishing*). W lutym 2026 r. łącznie odnotowano **5,6 tys.** tego typu incydentów.

Liczba nazw szkodliwych domen wpisanych na Listę Ostrzeżeń CERT Polska I–II 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 4. Liczba nazw szkodliwych domen wpisanych na Listę Ostrzeżeń. Źródło: CERT Polska / CSIRT NASK.

Od 1 stycznia do 28 lutego 2026 r. na Listę Ostrzeżeń przed niebezpiecznymi stronami wpisano **35 tys.** szkodliwych domen, z czego w lutym 2026 r. dodano **16,9 tys.** nazw domen wykorzystywanych do wyłudzania danych osobowych, danych uwierzytelniających do kont bankowych i serwisów społecznościowych. Wartość ta w stosunku do stycznia 2026 r. **zmniejszyła się o 7%**.

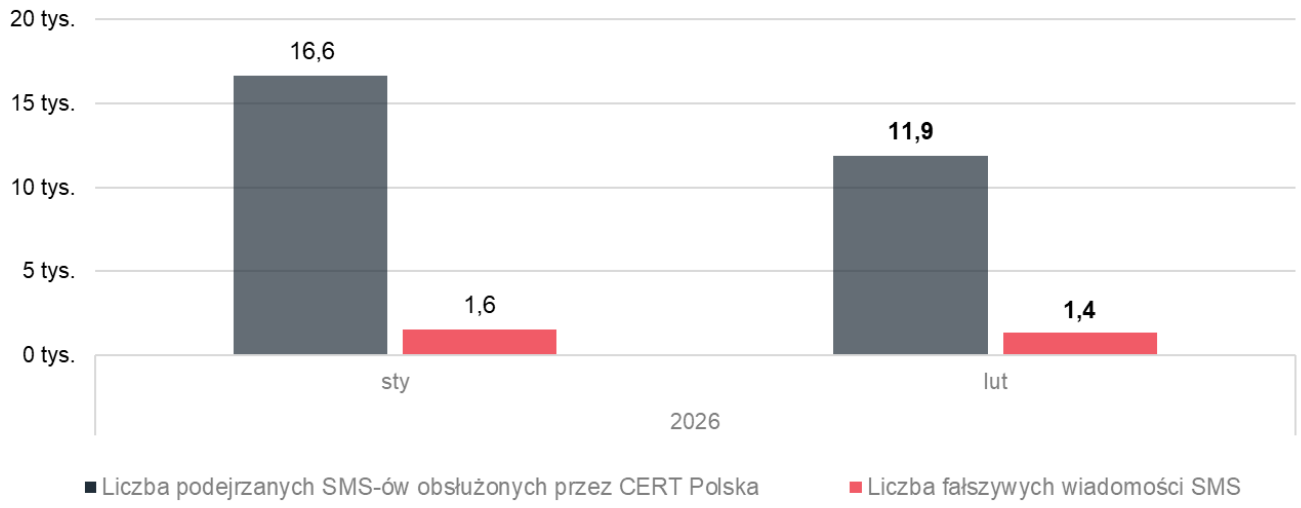
Lista Ostrzeżeń dostępna jest na stronie: CERT Polska/Lista Ostrzeżeń

Przykładowe nazwy fałszywych domen:

allegro.pl-01238.pl; booking.hotels-status.world; ccconline-pl.com; cyber-help.live; disney-dostepwstrzymany.com; diverse.onsale-pl.com; dpd-polska.net; dzieci-pl.com; dziecko-swiat.pl; eco-travelgarden.info; eobuwieoutlet.com; epic-games.info; gpt-gateway.com; in-post.help; inpost-przesylki-pl.com; ipkobizness.pl-switch.pro; jysk-de.shop; kontonetpocztasubskrypcje.netlify.app; lnpost.pac-zka-1323.bond; login.olx.pl.qu4dra.com; login-gov.pl; mebledomowe.shop; militaria-pl.com; nfz.gov-pl.com; ochnik1-pl.com; olx-dostawa715.cfd; online-psy.ch; orlenstrategy.com; pepco-sale.shop; pl-57276.cfd; poczta-onet.page.gd; smykpl.com; vinted.6eivfn.vip; vinted.pl-oferta9183154.sbs; vistulaai.com; webmail.165-154-235-200.cprapid.com

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

Od 1 stycznia do 28 lutego 2026 r. zespół CERT Polska zarejestrował **28,5 tys.** zgłoszeń podejrzanych SMS-ów. Liczba SMS-ów otrzymanych w lutym 2026 r. wyniosła **11,9 tys.**
W porównaniu ze styczniem 2026 r. był to **spadek o 29%**. Wśród ogółu SMS-ów przyjętych w lutym 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 12%**.



Wykres 5. Liczba SMS-ów zgłoszonych do CSIRT NASK w danym miesiącu.

Wzorce fałszywych wiadomości SMS I–II 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 lutym 2026 r., na podstawie wytworzonych przez CERT Polska wzorców fałszywych wiadomości SMS, zablokowano łącznie **38,2 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.

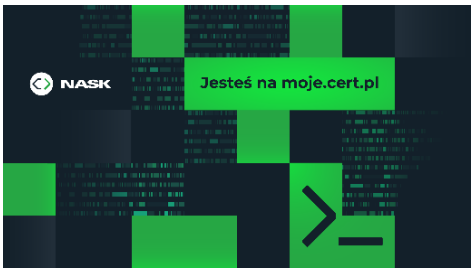
Wzorce fałszywych wiadomości SMS w 2026	sty	lut	Razem
Liczba wytworzonych wzorców	118	**97**	**215**

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 lutym 2026 r. w serwisie moje.cert.pl **zarejestrowało się 1,4 tys. nowych użytkowników**.



W okresie od 1 do 28 lutego 2026 r. CERT Polska wysłał **8,6 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

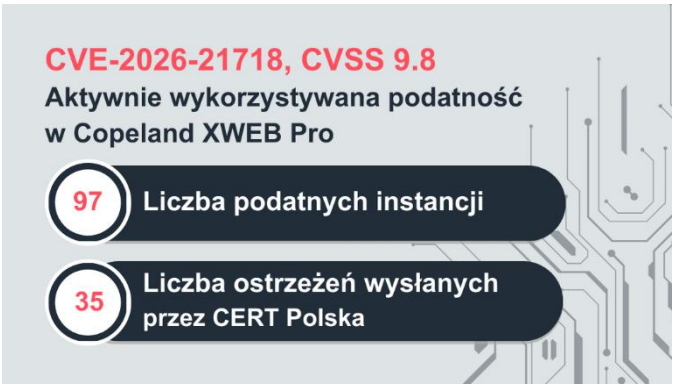
Zespół CERT Polska od sierpnia 2023 r. pełni funkcję CNA (ang. *CVE Numbering Authority*) – współtworzy bazę podatności poprzez nadawanie numerów CVE, które służą do identyfikacji i katalogowania publicznie ujawnionych podatności (więcej: CERT Polska/CNA). W lutym 2026 r. zespół CERT Polska nadał **12** numerów CVE. Wśród wykrytych podatności znalazły się podatności w oprogramowaniu m.in. Quick.Cart, Simple.ERP, Pro3W CMS oraz w aplikacji mObywatel na iOS.

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

Tabela 3. Nadane numery CVE od 1 stycznia do 28 lutego 2026 r.

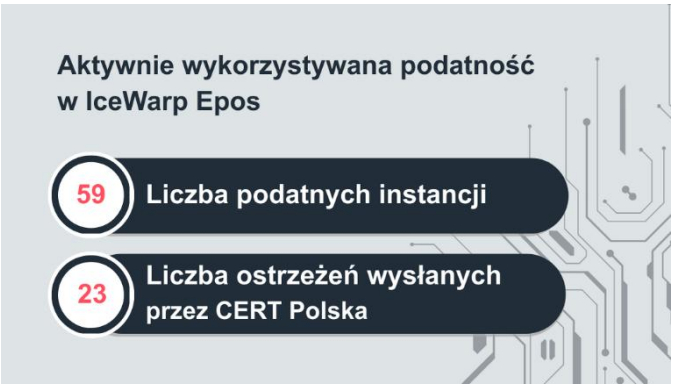
Numery CVE w 2026	sty	lut	Razem
Liczba opublikowanych numerów CVE	16	**12**	**28**

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



Podatność w oprogramowaniu Copeland XWEB Pro, w wersji 1.12.1 i starszych, polega na omijaniu mechanizmu uwierzytelniania, co umożliwia atakującemu uzyskanie – bez żadnych poświadczeń – uprawnień do wykonania kodu na urządzeniu. Luka ma niską złożoność ataku, może być wykorzystana z sieci zewnętrznej oraz powoduje poważne naruszenia poufności, integralności i dostępności systemu. Podatność otrzymała krytyczną ocenę CVSS (ang. *Common Vulnerability Scoring System*) 9.8.

Więcej: https://cvetodo.com/cve/CVE-2026-21718



Podatność w IceWarp Epos może umożliwić atakującemu uzyskanie nieautoryzowanego dostępu do serwera, na którym uruchomiony jest IceWarp. Problem dotyczy platform Windows oraz Linux, a skutecznie wykorzystana luka może prowadzić do przejęcia kontroli nad serwerem lub dalszej eskalacji ataku. Producent wskazuje, że podatność była krytyczna, jednak nie został jej nadany identyfikator podatności i CVSS.

Więcej: https://support.icewarp.com/hc/en-us/articles/39702252317713-IceWarp-Security-Update

Wybrane informacje

5 lutego w artykule „W ramach Centrum Cyberbezpieczeństwa NASK powstaje laboratorium fuzzingu” podano informację o powstającym w ramach **Centrum Cyberbezpieczeństwa NASK (CCN) Laboratorium Fuzzingu i Badania Złośliwego Oprogramowania – FUMAL**. Dzięki laboratorium Polska zyska realny wpływ na dobór projektów do testów fuzzingowych. CSIRT NASK wraz z partnerami krajowymi wskażą rozwiązania, np. biblioteki i aplikacje webowe czy systemy mobilne, które trafią do badań. Również zagrożenia będą wykrywane szybciej i na większą skalę, a wyniki analiz trafią bezpośrednio do zespołów reagujących na incydenty. FUMAL oprócz części zajmującej się testowaniem aplikacji rozwinie też istniejące już laboratorium CERT Polska do badania złośliwego oprogramowania i innych zagrożeń – Malware Lab CERT Polska. Projekt CCN jest realizowany przy wsparciu Programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027.

Więcej: nask.pl/W ramach Centrum Cyberbezpieczeństwa NASK powstaje laboratorium fuzzingu

12 lutego eksperci z CERT Polska poprowadzili śniadanie prasowe podsumowujące pierwszy rok działalności serwisu **moje.cert.pl**. Była to też okazja do zaprezentowania jego **nowej funkcjonalności o nazwie „Infrastruktura organizacji”**. Funkcjonalność ta, dostępna dla zarejestrowanych użytkowników, pozwala zobaczyć całość infrastruktury widocznej z internetu (z perspektywy potencjalnego atakującego), czyli np. subdomeny, wszystkie widoczne technologie, hosty, otwarte porty i powiązane z nimi podatności. Dzięki temu umożliwia zrozumienie faktycznej ekspozycji organizacji i ograniczenie liczby publicznie dostępnych punktów wejścia.

Zespół CERT Polska zachęca do przetestowania funkcjonalności z wykorzystaniem interaktywnego **demo dostępnego bez rejestracji** na stronie moje.cert.pl/organization/demo. Demo pozwala sprawdzić, jak funkcjonalność działa w praktyce – użytkownicy mogą swobodnie klikać, eksplorować i zobaczyć, jakie informacje platforma potrafi zidentyfikować.

Więcej: cert.pl/Rok moje.cert.pl i nowe narzędzie – infrastruktura organizacji

---

17 lutego na stronie cert.pl ukazał się artykuł **„ClickFix w akcji: jak fake captcha może zaszyfrować całą firmę”** na temat przeprowadzonej analizy incydentu typu Fake CAPTCHA, który miał miejsce w jednej z polskich organizacji. W artykule opisano m.in. przebieg infekcji krok po kroku, wskaźniki IoC, a także załączono szczegółową analizę wykorzystanych próbek złośliwego oprogramowania. Podczas obsługi incydentu CERT Polska wspierał zarówno organy ścigania, jak i zaatakowaną firmę w dochodzeniu i usuwaniu skutków ataku.

Więcej: cert.pl/ClickFix w akcji: jak fake captcha może zaszyfrować całą firmę

19 lutego prezydent RP Karol Nawrocki podpisał **ustawę z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw**. Ustawa wejdzie w życie **3 kwietnia 2026 r.**

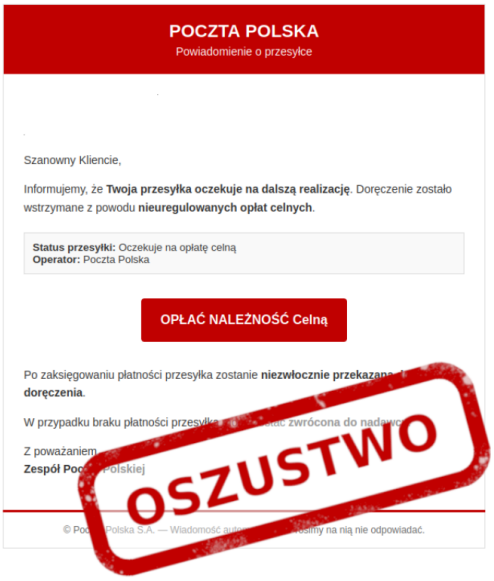
Więcej: isap.sejm.gov.pl/Dz.U. 2026 poz. 252

W dniach 25–26 lutego odbyła się jubileuszowa **10. edycja konferencji InfraSEC Forum**. Tematem przewodnim wydarzenia było cyberbezpieczeństwo elementów OT – ataki na nie są coraz częstsze i bardziej niebezpieczne. Kierownik CERT Polska wziął udział w rozmowie na temat „Incydenty w świecie OT: rzeczywistość bezpieczeństwa infrastruktury przemysłowej w Polsce i na świecie".

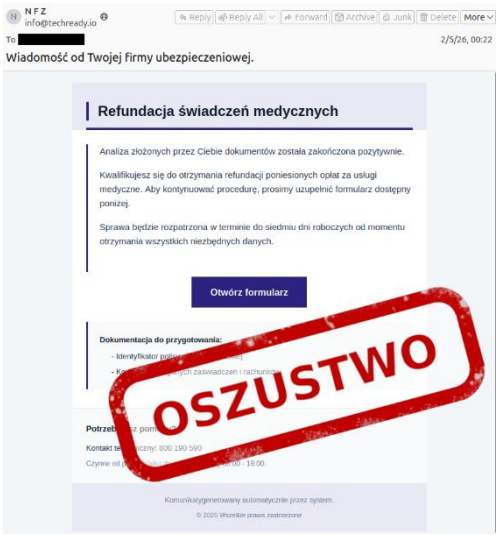
Więcej: infrasecforum.pl/relacja 2026

Komunikaty o zagrożeniach

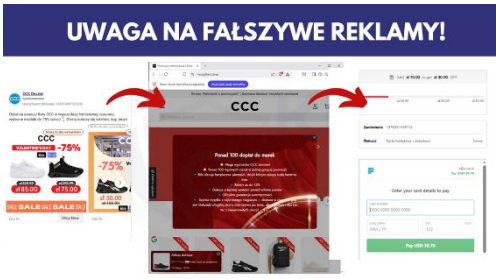
Informacje o zaobserwowanych kampaniach publikowane przez zespół CERT Polska w serwisie moje.cert.pl oraz w serwisach społecznościowych.



Zespół CERT Polska ostrzegał, że przestępcy podszywają się pod Pocztę Polską i wysyłają wiadomości e-mail, w których informują o nieopłaconych należnościach. Następnie przekonują odbiorcę do wejścia na przygotowaną stronę phishingową, do której link znajduje się w treści wiadomości. Strona internetowa ma szatę graficzną imitującą portal Poczty Polskiej, jednak wszelkie dane wprowadzone do znajdującego się tam formularza trafiają do oszustów. Przestępcy wyłudzają w ten sposób dane osobowe, adresowe i karty płatniczej.



Zespół CERT Polska obserwował kampanię oszustw, w których przestępcy podszywają się pod Narodowy Fundusz Zdrowia. W wiadomościach e-mail informują oni o rzekomej refundacji świadczeń. Link zawarty w treści wiadomości prowadzi do strony wyłudzającej dane osobowe i adresowe. Mogą one posłużyć przestępcom do prób nawiązywania dalszego kontaktu oraz w konsekwencji – do oszustwa.



Zespół CERT Polska udostępnił ostrzeżenie CSIRT KNF przed fałszywymi sklepami reklamowanymi na portalu Facebook. Oszuści promują fałszywe reklamy i „super rabaty", podszywając się pod znane marki. Linki prowadzą do stron wyłudzających dane osobowe i informacje o kartach płatniczych.

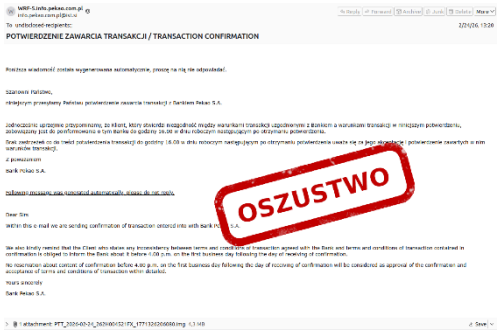
Zespół CERT Polska obserwował kampanię phishingową, w której oszuści podszywają się pod Krajową Administrację Skarbową. Wysyłają oni wiadomości na temat rzekomego wszczęcia kontroli podatkowej. W treści wiadomości znajduje się link, który prowadzi do fałszywej strony logowania do profilu zaufanego. Oszuści wykorzystują ten formularz do wyłudzania danych. CERT Polska przypomina, aby po otrzymaniu tego typu wiadomości: sprawdzić adres nadawcy wiadomości, samodzielnie wyszukać prawdziwy adres strony internetowej instytucji i zweryfikować, czy link z wiadomości na pewno prowadzi właśnie tam, a w przypadku jakichkolwiek wątpliwości skontaktować się z instytucją, która rzekomo wysłała wiadomość.

Zespół CERT Polska zaobserwował masową kampanię SMS-ową w związku z rozpoczęciem możliwości elektronicznego rozliczania PIT-11. Wiadomości zawierają informację o wysokości zwrotu oraz link do fałszywej witryny podszywającej się pod portal rządowy. Witryna ta służy przestępcom do wyłudzania danych podatników.

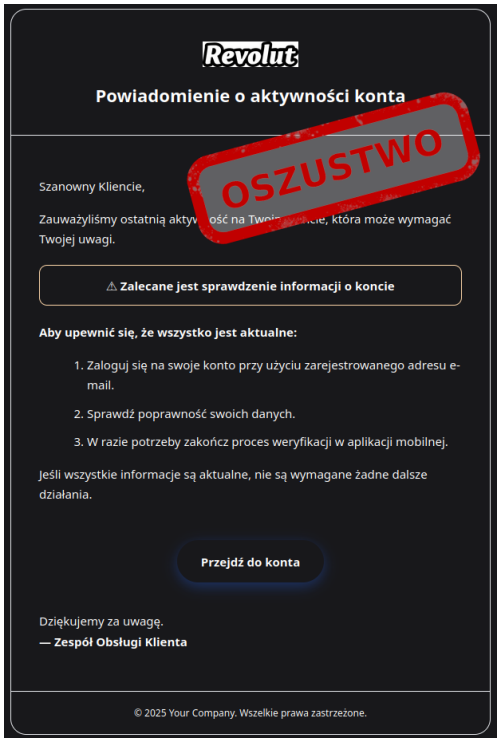
Zespół CERT Polska obserwował kampanię phishingową, w której oszuści wykorzystywali zimowe warunki pogodowe i podszywali się pod sklepy internetowe sprzedające np. węgiel. Oferowali atrakcyjne ceny i szybką dostawę, a ich celem było wyłudzenie pieniędzy – po tym, jak klient opłacił zamówienie, kontakt z fałszywym sklepem się urywał, a klient towaru nie otrzymywał. Aby zapobiec tego typu oszustwom, przed złożeniem zamówienia warto: sprawdzić, czy sklep widnieje w oficjalnych rejestrach przedsiębiorców, przejrzeć oceny sklepu (sprawdzić, czy zamieszczone opinie nie wydają się sztuczne, czy nie zostały dodane w podobnym czasie), zwrócić uwagę na dane kontaktowe, regulamin i politykę prywatności (czujność powinien wzbudzić np. brak adresu, numeru NIP czy działającego numeru telefonu do kontaktu), sprawdzić adres strony (czy domena zawiera błędy, literówki). Ponadto fałszywe sklepy często pozornie oferują wiele metod płatności, ale wymuszają uregulowanie rachunku szybkim lub tradycyjnym przelewem.

Zespół CERT Polska obserwował kampanię phishingową, w której cyberprzestępcy podszywają się pod serwis Amazon. W wiadomościach wysyłają rzekome podsumowanie subskrypcji Amazon Prime, którą – jak twierdzą – użytkownik może anulować i uzyskać zwrot kosztów. Po kliknięciu w załączony link otwiera się strona przygotowana przez oszustów. Witryna do złudzenia przypomina panel Amazon, jednak wszelkie dane wpisane w formularzu – w tym dane karty płatniczej oraz dane osobowe – trafiają bezpośrednio do cyberprzestępców.

Zespół CERT Polska informował, że oszuści podszywają się pod serwis e-TOLL. Wysyłają SMS-y, w których informują o rzekomym mandacie. Wiadomości w obrębie tej kampanii mogą się różnić, np. niektóre dotyczą rzekomego nowego wykroczenia, inne zachęcają do uregulowania grzywny przed jej podwyższeniem, ale cel jest wspólny dla wszystkich prób oszustwa. Treść wiadomości skłania do przejścia na stronę imitującą portal rządowy. Tam oszuści wyłudzają dane karty płatniczej – opłata do uiszczenia wydaje się niewielka, ale w rzeczywistości podanie danych umożliwia kradzież środków aż do wysokości limitów transakcyjnych. Przed podaniem swoich danych warto: sprawdzić adres nadawcy wiadomości, samodzielnie wyszukać prawdziwy adres strony internetowej instytucji i zweryfikować, czy link z wiadomości na pewno prowadzi właśnie tam, a w razie wątpliwości należy skontaktować się z instytucją, która rzekomo wysłała wiadomość.



Zespół CERT Polska zwracał uwagę na wiadomości, w których oszuści podszywają się pod Bank Pekao S.A. Cyberprzestępcy chętnie wykorzystują wizerunki banków do dystrybucji złośliwego oprogramowania. W przesyłanych wiadomościach informują o konieczności „weryfikacji dokumentu" i zachęcają odbiorców do pobrania załączonego pliku. W załączniku znajduje się plik w formacie .img, który w rzeczywistości zawiera złośliwe oprogramowanie typu infostealer. Po uruchomieniu może ono wykradać poufne informacje – m.in. dane logowania do kont, zapisane hasła czy informacje finansowe. W przypadku takich wiadomości warto zwracać uwagę na: poprawność adresu nadawcy wiadomości, treść wiadomości, która wywołuje presję czasu lub strach, prośby o pobieranie plików lub ich samodzielne uruchamianie. Ponadto podejrzane załączniki w nietypowych formatach – końcówki takie jak .tar, .exe, .js czy .7z mogą sugerować, że zawartość załącznika jest inna, niż obiecuje treść wiadomości.



Zespół CERT Polska obserwował kampanię phishingową, w której oszuści wykorzystują wizerunek Revoluta, aby wyłudzać dane logowania do kont użytkowników. Wiadomość to powiadomienie o rzekomej niepokojącej aktywności na koncie. Użytkownicy są zachęcani do sprawdzenia jej i kliknięcia w link, który prowadzi do strony wyłudzającej dane logowania. Dane przesłane za pomocą takiej złośliwej witryny trafiają bezpośrednio do przestępców. Dzięki temu mogą oni przejąć dostęp do konta, a w konsekwencji także zgromadzone na nim środki.

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

Opis najczęściej występujących kampanii – II 2026

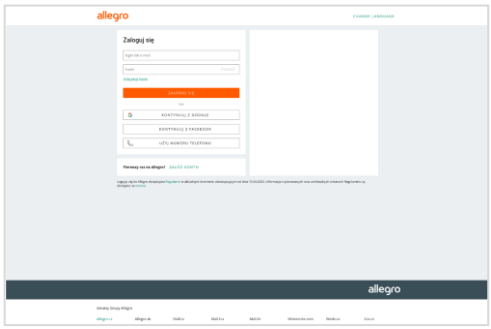
Fałszywe strony oferujące wysokodochodowe inwestycje

Zespół CERT Polska w dalszym ciągu obserwował wzmożoną kampanię phishingową, w której oszuści podszywają się pod różnego rodzaju koncerny paliwowo-energetyczne, firmy, instytucje, m.in. Lotos, Tesla, PGNiG. Oszuści reklamują w mediach społecznościowych czy w wyszukiwarkach internetowych nieistniejące programy dla akcjonariuszy indywidualnych, rozsyłają wiadomości. Informują w nich 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 okazuje, uniemożliwia wypłaty zainwestowanych pieniędzy. Celem oszustów jest wyłudzenie środków finansowych.

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.

Fałszywe strony Allegro

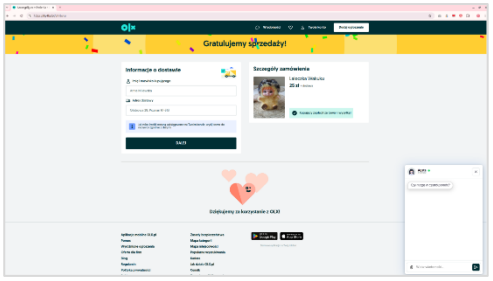


Zespół CERT Polska obserwował wzmożoną kampanię phishingową wykorzystującą wizerunek platformy Allegro. Na fałszywych stronach internetowych znajduje się panel logowania do tego serwisu służący do wyłudzania danych uwierzytelniających od użytkowników Allegro.

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 OLX

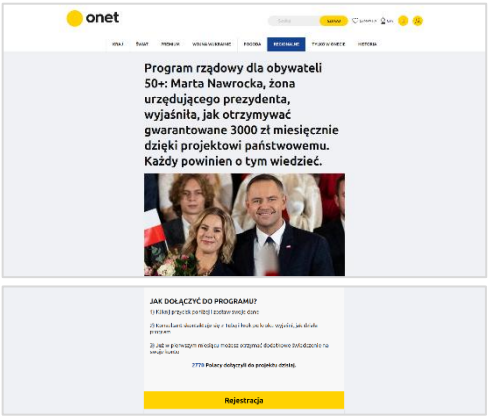


Zespół CERT Polska zarejestrował incydenty, w których atakujący za pośrednictwem stron internetowych podszywają się pod serwis OLX. Oszuści kontaktują się z potencjalną ofiarą przez komunikator WhatsApp. Wyrażają zainteresowanie przedmiotem z ogłoszenia, następnie informują, że zapłacili za zamówienie, a w kolejnym kroku wysyłają link do strony internetowej, poprzez którą rzekomo można wypłacić środki. Oprawa graficzna witryny przypomina stronę OLX, InPostu, DPD, DHL lub Poczty Polskiej. Znajduje się na niej fałszywy panel płatniczy. Podanie danych karty powoduje utratę środków finansowych przechowywanych na koncie bankowym.

Fałszywe strony firmy Orlen

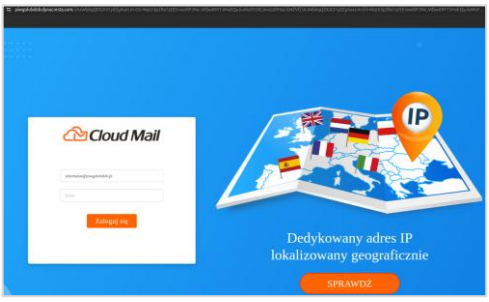
Zespół CERT Polska zarejestrował kampanię phishingową, w której wykorzystywany jest wizerunek Orlenu. Cel oszustów to wyłudzenie środków finansowych poprzez fałszywą platformę inwestycyjną.

Fałszywe strony serwisu Onet.pl



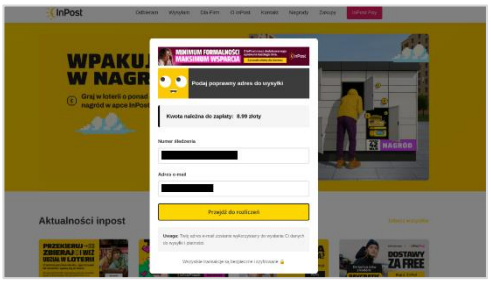
Zespół CERT Polska obserwował kampanię phishingową, w której oszuści wykorzystują wizerunek serwisu Onet.pl do reklamowania nieistniejących programów inwestycyjnych. Celem oszustów jest wyłudzenie środków finansowych.

Fałszywe panele logowania do aplikacji typu webmail



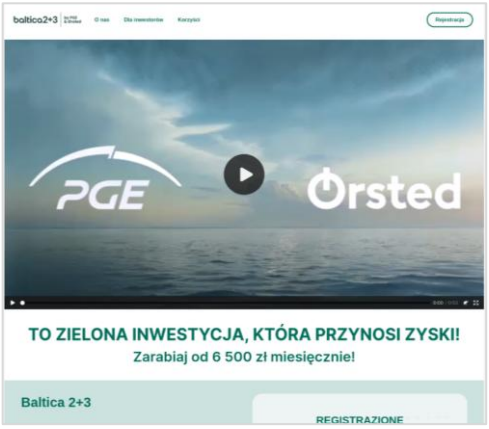
Zespół CERT Polska rejestrował incydenty, w których oszuści tworzyli fałszywe strony internetowe zawierające podrobiony panel logowania do aplikacji typu webmail, która umożliwia dostęp do poczty elektronicznej za pośrednictwem przeglądarki internetowej. Celem oszustów było pozyskanie danych logowania do poczty.

Fałszywe strony firmy InPost



Zespół CERT Polska rejestrował incydenty, w których oszuści podszywają się pod firmę InPost. Celem są użytkownicy serwisu OLX lub Vinted. Oszuści kontaktują się z potencjalną ofiarą. Wyrażają zainteresowanie przedmiotem z ogłoszenia, następnie informują, że opłacili produkt, i wysyłają link do strony internetowej, poprzez którą rzekomo można wypłacić środki. Witryna wykorzystuje wizerunek firmy InPost. Znajduje się na niej fałszywy panel płatniczy. Podanie danych karty powoduje utratę środków finansowych przechowywanych na koncie bankowym.

Fałszywe strony PGE



Zespół CERT Polska obserwował incydenty, w których oszuści wykorzystują wizerunek firmy PGE.
Na fałszywych stronach internetowych znajdują się artykuły na temat inwestycji, na których rzekomo można zarobić z dużym zyskiem.