GRUDZIEŃ 2025

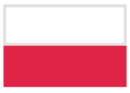
Podsumowanie Miesiąca CERT POLSKA CSIRT NASK

Nr 4/2025

CERT.PL NASK

CSIRT NASK

PODSUMOWANIE MIESIĄCA CERT POLSKA / CSIRT NASK





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 zarejestrowanych zagrożeń 4

Moje.cert.pl 9

Podatności CVE 10

Wybrane podatności i ich wpływ na krajobraz cyberbezpieczeństwa w Polsce – XII 2025 10

Wybrane informacje 12

Wystąpienia ekspertów CERT Polska 15

Komunikaty o zagrożeniach 15

Opis najczęściej występujących kampanii – XII 2025 18

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 31 grudnia 2025 r.
Dla lepszego zobrazowania pojawiających się trendów niektóre z tych danych pokazywane są w dłuższej perspektywie czasu.

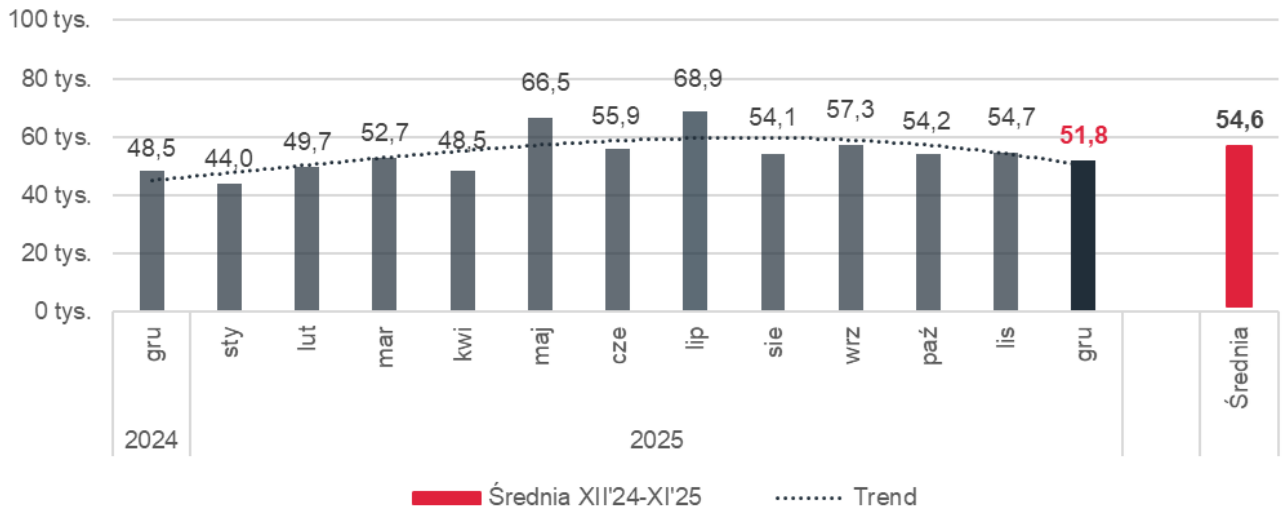
Zarejestrowane zgłoszenia i incydenty cyberbezpieczeństwa – XII 2025

Tabela 1. Liczba zarejestrowanych zgłoszeń i incydentów od 1 do 31 grudnia 2025 r.

Zagrożenia cyberbezpieczeństwa	Liczba
Zarejestrowane zgłoszenia	**51,8 tys.**
w tym zarejestrowane (obsłużone) incydenty	**24,7 tys.**

W grudniu 2025 r. zespół CERT Polska otrzymał łącznie **51,8 tys.** zgłoszeń, które zostały przeanalizowane i pogrupowane. Na ich podstawie zarejestrowano **24,7 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 XII 2024 do XII 2025

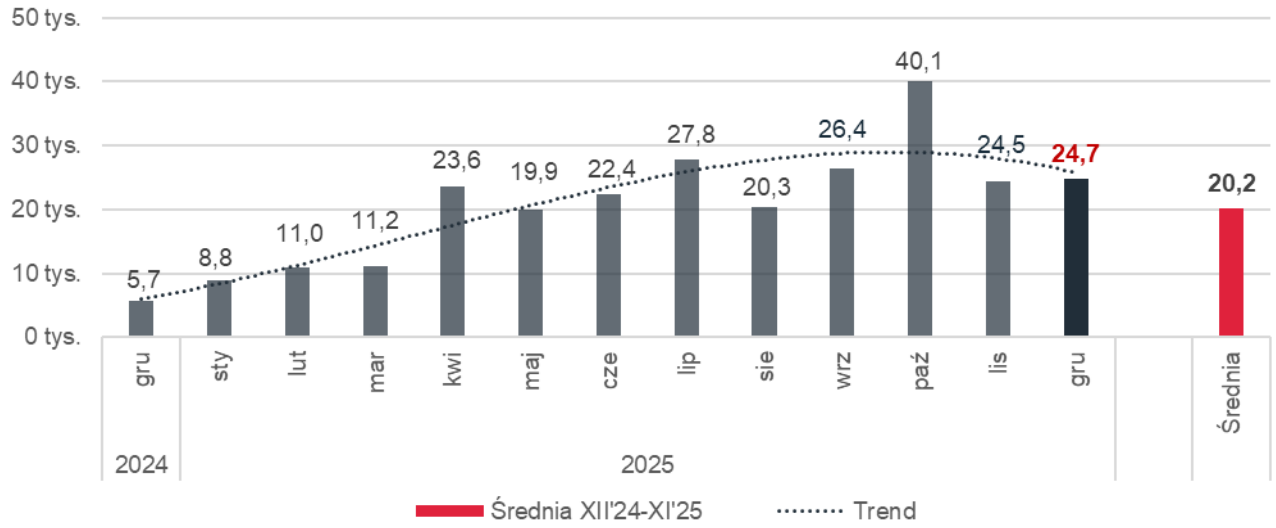


Wykres 1. Liczba zarejestrowanych zgłoszeń od 01.12.2024 do 31.12.2025. Źródło: CERT Polska / CSIRT NASK.

[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.

W całym 2025 r. liczba zgłoszeń zarejestrowanych przez zespół CERT Polska wyniosła **658,3 tys.**, co oznacza **wzrost o 10%** wobec 2024 r., kiedy takich przypadków było **601 tys.** W ujęciu miesięcznym liczba zgłoszeń odnotowanych w grudniu 2025 r. wyniosła **51,8 tys.** i nie przekroczyła średniej liczonej z poprzednich 12 miesięcy. W porównaniu z analogicznym miesiącem 2024 r. liczba ta **zwiększyła się o 7%**. W stosunku do listopada 2025 r. był to **spadek o 5%.**

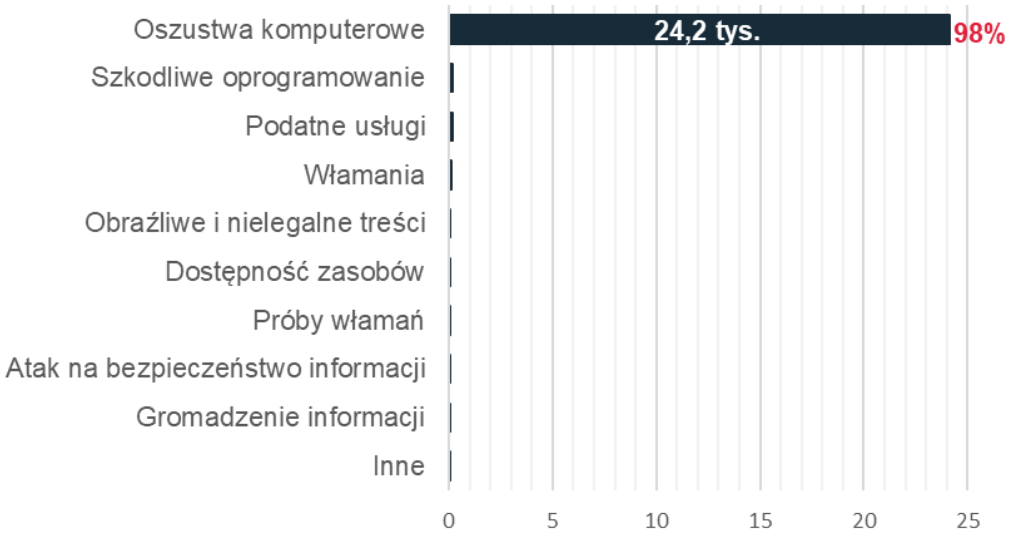
Zarejestrowane incydenty cyberbezpieczeństwa od XII 2024 do XII 2025



Wykres 2. Liczba zarejestrowanych incydentów od 01.12.2024 do 31.12.2025. Źródło: CERT Polska / CSIRT NASK.

W całym 2025 r. liczba incydentów zarejestrowanych przez zespół CERT Polska wyniosła **260,8 tys.**, podczas gdy w 2024 r. takich przypadków było **103,4 tys.**, co oznacza **wzrost o 152%**. W ujęciu miesięcznym liczba incydentów zarejestrowanych w grudniu 2025 r. wyniosła **24,7 tys.** i była wyższa od średniej liczonej z 12 poprzednich miesięcy. W porównaniu z grudniem 2024 r. liczba ta **zwiększyła się o 331%**.

Rodzaje zarejestrowanych zagrożeń – XII 2025



Wykres 3. Liczba zarejestrowanych incydentów według rodzaju od 1 do 31 grudnia 2025 r. Źródło: CERT Polska / CSIRT NASK.

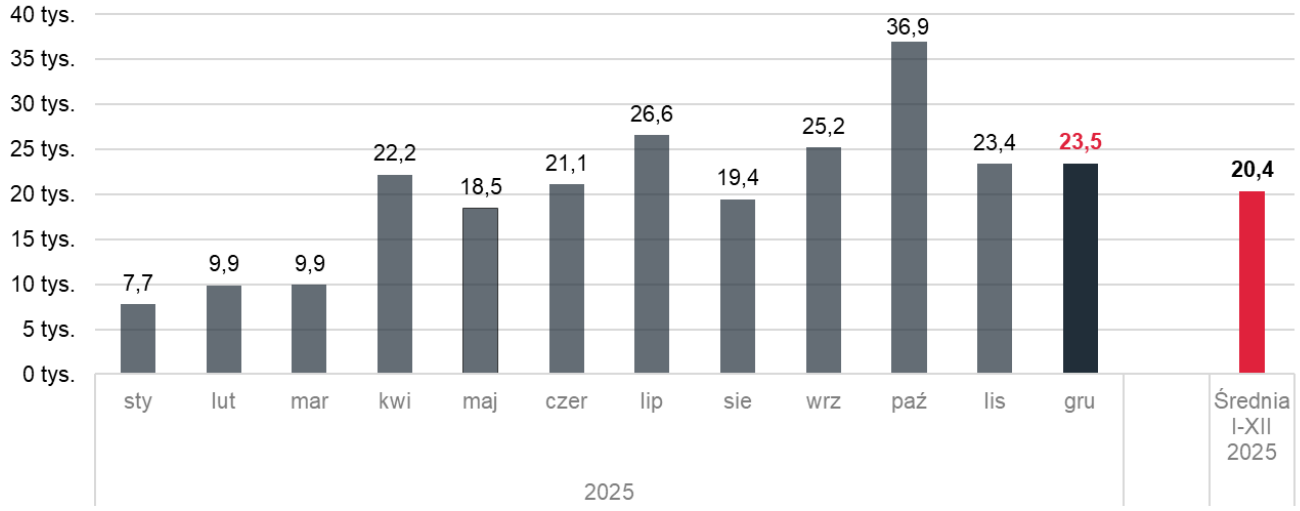
W analizowanym okresie zdecydowanie najczęściej występującą kategorią zagrożeń były oszustwa komputerowe. Wśród ogółu obsłużonych incydentów (**24,7 tys.**) stanowiły one **98%**. Najbardziej rozpowszechnionym rodzajem oszustw komputerowych były próby wyłudzania poufnych danych, np. loginu i hasła do poczty, strony banku, portalu społecznościowego czy innej usługi online (ang. *phishing*). W grudniu 2025 r. łącznie odnotowano **7,3 tys.** tego typu incydentów.

Liczba nazw szkodliwych domen wpisanych na Listę Ostrzeżeń CERT Polska I–XII 2025

CERT Polska prowadzi Listę Ostrzeżeń przed niebezpiecznymi stronami. Na listę 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.

Linki do takich stron rozpowszechniane są różnymi kanałami – poprzez **SMS-y, wiadomości e-mail oraz media społecznościowe**. Każdy może zgłosić do CERT Polska podejrzaną stronę za pomocą formularza dostępnego na stronie incydent.cert.pl/phishing. Podejrzane SMS-y można bezpłatnie przesyłać pod numer **8080**.



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

Od stycznia do grudnia 2025 r. na Listę Ostrzeżeń przed niebezpiecznymi stronami wpisano **244,3 tys.** szkodliwych domen, z czego w grudniu 2025 r. dodano **23,5 tys.** nazw domen wykorzystywanych do wyłudzania danych osobowych, danych uwierzytelniających do kont bankowych i serwisów społecznościowych.

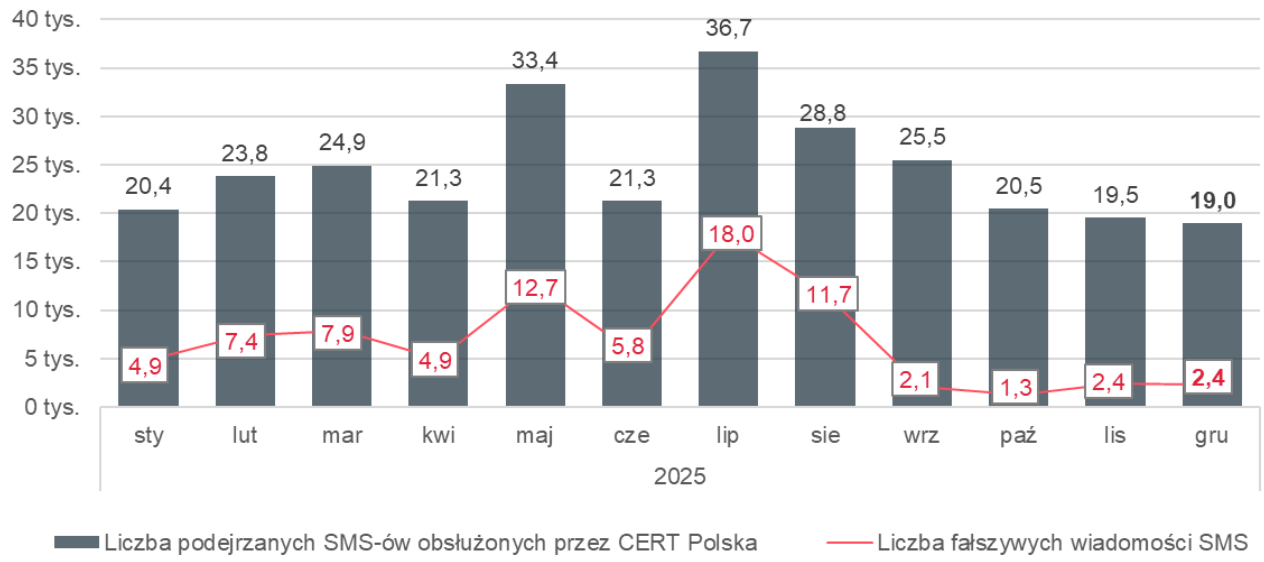
Lista Ostrzeżeń dostępna jest na stronie: CERT Polska/Lista Ostrzeżeń

Przykładowe nazwy fałszywych domen:

028731.lol; 1n8ost.y8mdhb.cyou; ai-invest-solution.com; alebilet.com-oferta.cfd; allegro.01648.click; allegro.pry-3082s.cfd; animalrescueinfo292d.info; app-lotto-online.org; booking.resevrbok.com; cash-banking.buzz; centrum-disney.com; click-money-app.com; disneyplus-center.com; dzieci-rodzina.store; edunetflix.com; eobuwies.wyprzedazonline.shop; fakturaklienta.com; faktyczarnowo.top; govpl.live; gpt-3v-app.net; inposts.app; inwestuj-od-rana.com; ipko.pl-dev-apps-auth-ai.pro; martessportplonline.com; moje-fakturaklientadisney.com; moje-spotify.com; nowajagazeta.info; olx.choinkimartyna-345679.xyz; pepco.wyprzedazonline.shop; serwis-mbank-bezpieczny.com; twojeinwestycje.com; usmiechrodzica.com

Liczba zgłoszeń wiadomości SMS przyjętych przez CSIRT NASK I–XII 2025

Od 1 stycznia do 31 grudnia 2025 r. zespół CERT Polska zarejestrował **295,2 tys.** zgłoszeń podejrzanych SMS-ów. Liczba SMS-ów otrzymanych w grudniu 2025 r. wyniosła **19 tys.**
W porównaniu z listopadem 2025 r. był to **spadek o 3%**. Wśród ogółu SMS-ów przyjętych w grudniu 2025 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–XII 2025

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**.

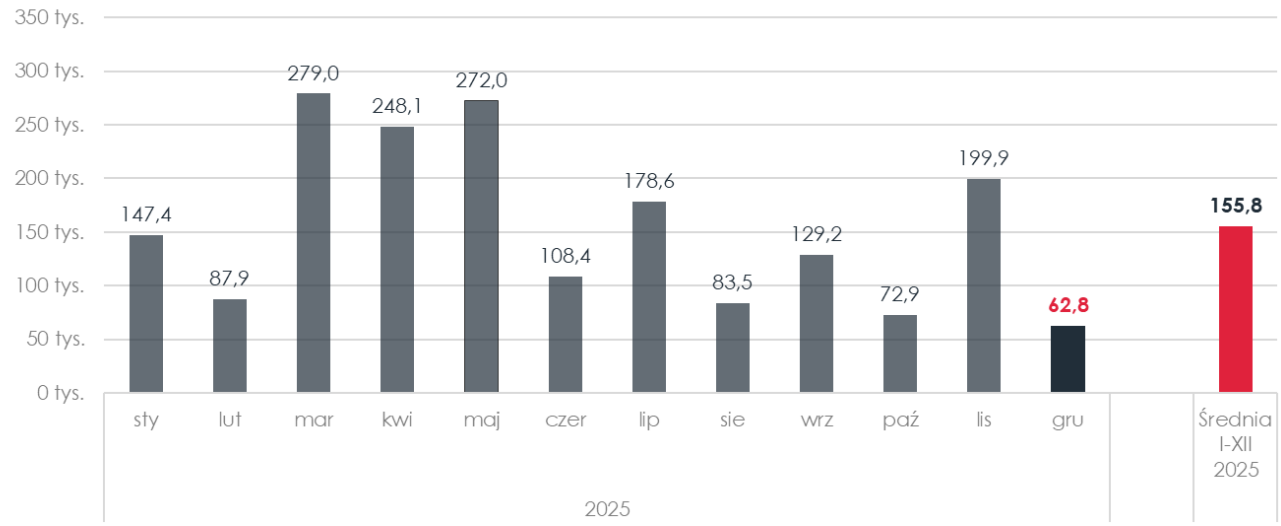
Tabela 2. Liczba wytworzonych wzorców fałszywych wiadomości SMS.

Wzorce fałszywych wiadomości SMS w 2025	sty	lut	mar	kwi	maj	cze	lip	sie	wrz	paź	lis	gru	Razem
Liczba wytworzonych wzorców	82	57	106	60	83	39	119	10	43	36	88	**67**	**790**

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

Liczba zablokowanych SMS-ów I–XII 2025

W okresie od 1 stycznia do 31 grudnia 2025 r., na podstawie wytworzonych przez CERT Polska wzorców fałszywych wiadomości SMS, zablokowano łącznie **1,9 mln** SMS-ów.

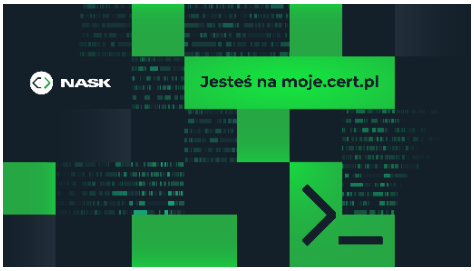


Wykres 6. Liczba SMS-ów zablokowanych na podstawie wzorców fałszywych wiadomości SMS w danym miesiącu. Źródło: CERT Polska / CSIRT NASK.

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 grudniu 2025 r. w serwisie moje.cert.pl **zarejestrowało się 578 nowych użytkowników**.



W okresie od 1 do 31 grudnia 2025 r. CSIRT NASK wysłał **4,3 tys. powiadomień w ramach serwisu moje.cert.pl dotyczących wykrytych podatności i 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 grudniu 2025 r. zespół CERT Polska nadał **10** numerów CVE. Wśród wykrytych podatności znalazły się podatności w oprogramowaniu m.in. urządzeń Govee z łącznością sieciową, WaveStore Server, routera WODESYS WD-R608U.

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

Tabela 3. Nadane numery CVE od 1 stycznia do 31 grudnia 2025 r.

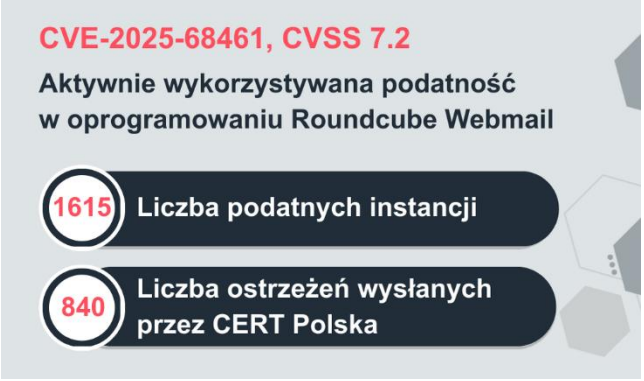
Numery CVE w 2025	sty	lut	mar	kwi	maj	cze	lip	sie	wrz	paź	lis	gru	Razem
Liczba opublikowanych numerów CVE	4	9	11	15	22	3	6	36	16	12	21	**10**	**165**

Wybrane podatności i ich wpływ na krajobraz cyberbezpieczeństwa w Polsce – XII 2025



Najpoważniejszą podatnością zidentyfikowaną w grudniu 2025 roku była luka występująca w komponencie react-server powszechnie wykorzystywanego przy tworzeniu stron internetowych frameworka React. W wyniku przesłania specjalnie spreparowanego żądania HTTP do aplikacji webowej atakujący mógł uzyskać nieautoryzowany dostęp umożliwiający wykonywanie poleceń na serwerze hostującym stronę. Jest to podatność, którą można łatwo wykorzystać m.in. ze względu na niski próg wejścia, a to znacząco zwiększa ryzyko ataków.

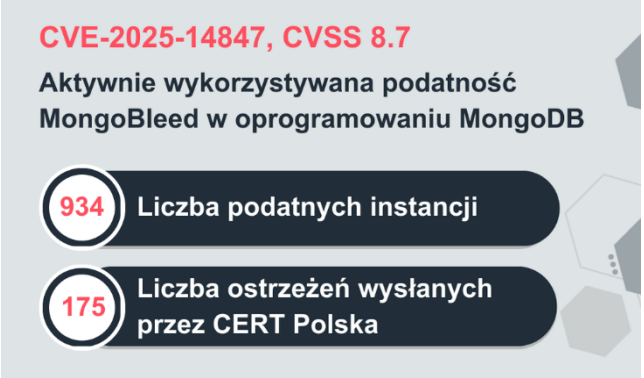
Więcej: https://moje.cert.pl/komunikaty/2025/61/krytyczna-podatnosc-w-react-server-components-oraz-innych-aplikacjach-z-tym-rozwiazaniem



Podatność występuje w wersjach wcześniejszych niż 1.5.12 oraz 1.6.12. Wynika ona z nieprawidłowego przetwarzania elementu animate w dokumentach SVG, co prowadzi do Cross-Site Scripting (XSS). Nieprawidłowa sanityzacja danych wejściowych umożliwia atakującym wykonanie złośliwego kodu JavaScript, co może prowadzić do przejęcia zawartości skrzynek pocztowych lub sesji użytkowników. Atakujący może dostarczyć

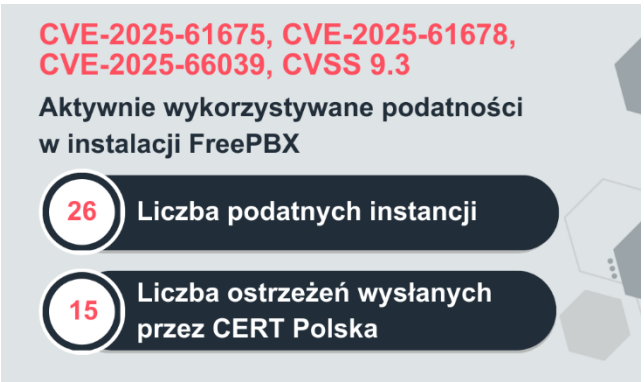
spreparowaną treść SVG np. poprzez załącznik lub odpowiednio skonstruowany URL, co skutkuje wykonaniem kodu JavaScript po stronie klienta.

Więcej: https://moje.cert.pl/komunikaty/2025/66/powazna-podatnosc-w-oprogramowaniu-roundcube-webmail



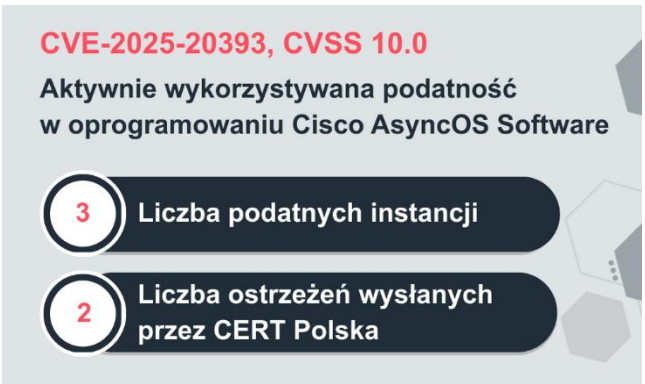
Podatne wersje oprogramowania MongoDB nieprawidłowo obsługiwały informację o długości danych przesyłaną przez użytkownika podczas korzystania z mechanizmu kompresji (zlib). W efekcie niezalogowany użytkownik mógł uzyskać dostęp do fragmentów pamięci, które nie zostały wcześniej zainicjalizowane. Problem ten może wydawać się mało groźny. W praktyce jednak, w związku z tym, że pamięć jest przydzielana dynamicznie, takie fragmenty mogły zawierać dane używane wcześniej przez system, np. klucze API, dane osobowe użytkowników lub inne wrażliwe informacje.

Więcej: https://moje.cert.pl/komunikaty/2025/69/podatnosc-cve-2025-14847-w-oprogramowaniu-mongodb



Podatności oznaczone jako CVE-2025-61675 oraz CVE-2025-61678 pozwalają na zdalne wykonanie kodu, ale wyłącznie przez użytkowników, którzy są już zalogowani do systemu. Z kolei podatność CVE-2025-66039 w określonej konfiguracji usługi umożliwia ominięcie mechanizmu logowania. W praktyce oznacza to, że połączenie tych podatności tworzy tzw. łańcuch ataku, który pozwala nawet niezalogowanemu użytkownikowi zdalne wykonanie kodu w systemie.

Więcej: https://thehackernews.com/2025/12/freepbx-authentication-bypass-exposed.html



Podatność ta pozwala nieuwierzytelnionemu atakującemu na zdalne wykonanie kodu w oprogramowaniu Cisco AsyncOS Software, które jest wykorzystywane w Cisco Secure Email Gateway oraz Cisco Secure Email and Web Manager. W konsekwencji możliwe jest przejęcie kontroli nad urządzeniem. Atakujący wykorzystuje usługę Spam Quarantine, która domyślnie jest wyłączona i przy prawidłowej konfiguracji nie powinna być dostępna z internetu.

Więcej: https://moje.cert.pl/komunikaty/2025/65/krytyczna-podatnosc-cve-2025-20393-w-oprogramowaniu-cisco-asyncos-software

Wybrane informacje



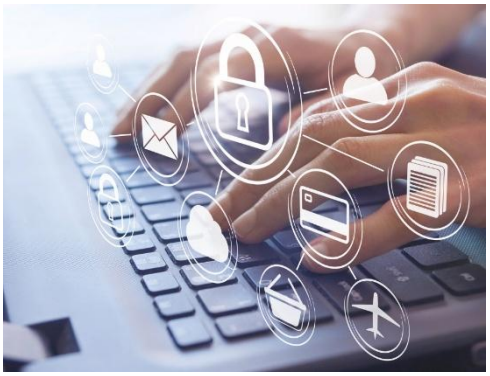
2 grudnia w Warszawie odbyła się konferencja poświęcona cyberbezpieczeństwu **Oh My Hack 2025**. Podczas tego wydarzenia eksperci z CSIRT NASK i CERT Polska zaprezentowali narzędzie do automatycznego wyszukiwania podatności za pomocą fuzzingu, przeanalizowali zagadnienie wykrywania złośliwych plików, podzielili się przemyśleniami dotyczącymi znajdowania podatności z pomocą agentów AI, opowiedzieli o serwisie moje.cert.pl (m.in. o tym, jakie narzędzia open source i źródła danych są wykorzystywane przez zespół CERT Polska oraz z jakimi wyzwaniami zespół musiał się zmierzyć), a także mówili o tym, jak ważny jest sposób komunikacji o incydentach w obszarze cyberbezpieczeństwa.

Więcej: omhconf.pl/Oh My Hack/agenda



Od 8 do11 grudnia w Londynie odbywała się konferencja **Black Hat Europe 2025** na temat cyberbezpieczeństwa. Podczas tego wydarzenia omawiano m.in. najnowsze trendy w tym obszarze, a także prezentowano narzędzia wspomagające ochronę w sieci. W tym kontekście ekspert z zespołu CERT Polska zaprezentował **Artemis** oraz **moje.cert.pl** – bezpłatne narzędzia, które ułatwiają rozwój cyberbezpieczeństwa podmiotów publicznych i prywatnych w Polsce.

Więcej: blackhat.com/Black Hat Europe 2025



11 grudnia w Warszawie zorganizowano prezentację nowej platformy Ministerstwa Cyfryzacji – **cyber.gov.pl**, która zapewnia dostęp do bezpłatnych usług i narzędzi, takich jak m.in. moje.cert.pl, Artemis, Bezpieczna Poczta, możliwość zgłaszania incydentów**.** Na platformie publikowane są także najważniejsze informacje, porady oraz aktualne ostrzeżenia z obszaru cyberbezpieczeństwa. Platforma cyber.gov.pl jest rozwijana we współpracy z NASK-PIB.

Więcej: gov.pl/Startuje cyber.gov.pl – centralne miejsce do ochrony przed cyberzagrożeniami



12 grudnia zespół CERT Polska przypominał użytkownikom internetu o możliwości sprawdzenia, czy ich dane mogły się znaleźć w jednym z ostatnich wycieków. Po zalogowaniu się w serwisie **bezpiecznedane.gov.pl** można przeszukać zarejestrowane wycieki z kilkudziesięciu źródeł pod kątem obecności swojego e-maila, numeru telefonu czy numeru PESEL. Baza serwisu jest aktualizowana na bieżąco o kolejne zbiory danych także dzięki pracy ekspertów z CERT Polska.

Więcej: facebook.com/CERT Polska



Od 13 grudnia zespół CERT Polska publikował **posty ze świątecznej serii #CyberPrezent** inspirowanej piosenką „12 days of Christmas". Przez 12 dni na cyberchoince pojawiały się symbole odnoszące się do ważnych z perspektywy cyberbezpieczeństwa zagadnień oraz związanej z nimi działalności CERT Polska. Każdy post zawierał informacje na dany temat oraz odnośnik do publikacji z szerszym omówieniem zagadnienia. Wśród tematów postów znalazły się: publiczne Wi-Fi, grupy APT, skanowanie zasobów sieciowych dostępnych w polskim internecie, bezpieczne hasła, zgłaszanie incydentów, wycieki danych, podatności, zgłoszenia podejrzanych SMS-ów, rozpoznawanie fałszywych wiadomości e-mail.

Więcej: facebook.com/#cyberprezent

---

17 grudnia **kierownik Działu CERT Polska udzielił wywiadu**, w którym podsumował działalność CERT Polska w obsłudze incydentów cyberbezpieczeństwa w 2025 r., omówił najczęstsze zagrożenia w tym obszarze i wskazał sektory najbardziej narażone na ataki. Podkreślił również, że wzrost liczby zarejestrowanych incydentów w 2025 r. jest związany m.in. z większą skutecznością ich wykrywania przez CERT Polska oraz z rozwojem systemów monitorujących podejrzaną aktywność w internecie. Działalność ta pozwala m.in. wykrywać domeny wykorzystywane w oszustwach inwestycyjnych, zanim zostaną one użyte w ataku. Kierownik CERT Polska wspomniał także o serwisie moje.cert.pl i planach rozwoju jego funkcjonalności oraz o innych projektach zwiększających ochronę przed cyberatakami, w tym o programach Cyberbezpieczne Wodociągi i Lokalne Centra Cyberbezpieczeństwa.

Więcej: pap.pl/Rozmowa z kierownikiem CERT Polska



19 grudnia zespół CERT Polska podzielił się statystykami na temat portalu **moje.cert.pl**, udostępnionego publicznie w lutym 2025 r. Od tego czasu w serwisie zarejestrowało się 15 tys. użytkowników, a w ramach usług przeskanowano ponad 3,3 mln domen, subdomen i adresów IP, w których znaleziono ponad pół miliona podatności lub błędnych konfiguracji. Ponadto zespół CERT Polska opublikował na stronie 65 komunikatów o zagrożeniach cyberbezpieczeństwa dla administratorów i użytkowników. Moje.cert.pl jest jedną z najbardziej rozbudowanych darmowych usług skanowania bezpieczeństwa na świecie.

Więcej: x.com/CERT Polska/Portal moje.cert.pl ma już 15 tysięcy użytkowników

---



23 grudnia zespół CERT Polska ogłosił datę **29. edycji SECURE**, najstarszej w Polsce konferencji poświęconej cyberbezpieczeństwu. Wydarzenie odbędzie się 8 kwietnia 2026 r. w Muzeum Historii Polski w Warszawie. Na stronie internetowej konferencji – **secure.edu.pl** – znajduje się zaproszenie do zgłaszania prezentacji, w którym podano także propozycje obszarów tematycznych wystąpień. Zainteresowane osoby mogą wysyłać zgłoszenia do 15 lutego 2026 r.

Więcej: x.com/CERT Polska/SECURE 2026



31 grudnia zespół CERT Polska opublikował post, w którym poinformował, że liczba szkodliwych domen dodanych **na Listę Ostrzeżeń przekroczyła 500 tys**. CERT Polska prowadzi Listę Ostrzeżeń od marca 2020 r. Wpisywane są na nią domeny, które wprowadzają użytkowników w błąd i wyłudzają od nich dane. CERT Polska z każdym rokiem coraz lepiej identyfikuje podejrzane witryny dzięki swoim systemom, ale nie mniej ważne pozostają zgłoszenia od użytkowników.

Więcej: x.com/CERT Polska/500 tys. domen dodanych na Listę Ostrzeżeń

Wystąpienia ekspertów CERT Polska

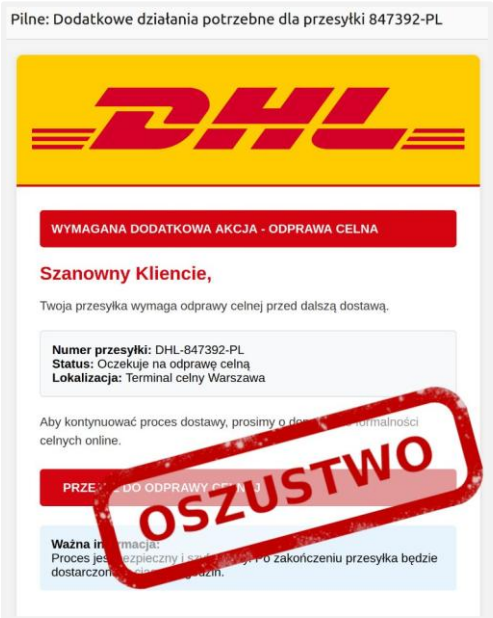
- 6 grudnia – udział w 9. Śląskim Festiwalu Nauki: prelekcja pt. „Człowiek – naj… ogniwo łańcucha (cyber)bezpieczeństwa”, a następnie rozmowa na tematy poruszone w tym wystąpieniu. Dodatkowo także aktywności na stanowisku NASK-PIB, który był partnerem wydarzenia.

  Więcej: śląskifestiwalnauki.pl/aktualności
- 10 grudnia – podczas sympozjum FIRST odbywającym się w Lublanie eksperci z CERT Polska przedstawili prezentację na temat działań podejmowanych w ramach projektu DNS4EU związanych m.in. z tworzeniem rozwiązań wykrywających domeny wykorzystywane do phishingu.

  Więcej: first.org/przedstawienie prezentacji
- 11 grudnia – prezentacja na temat CRA (Cyber Resilience Act) w sektorze zdrowia podczas warsztatów zorganizowanych przez Ośrodek Standaryzacji i Certyfikacji NASK-PIB. Wśród uczestników warsztatów byli m.in. producenci oprogramowania, przedstawiciele Ministerstwa Cyfryzacji, Ministerstwa Zdrowia, Centrum e-Zdrowia i Urzędu Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych.

Komunikaty o zagrożeniach

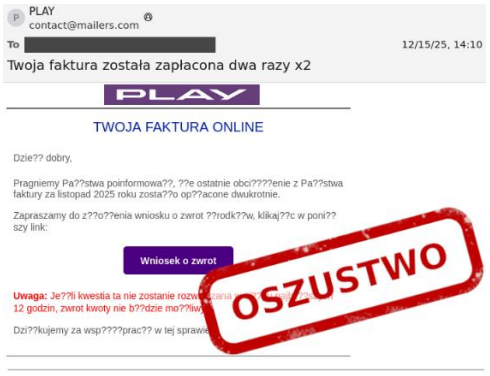
Informacje o zaobserwowanych kampaniach publikowane przez zespół CERT Polska w serwisie moje.cert.pl oraz w serwisach społecznościowych.



Zespół CERT Polska zwracał uwagę, że w okresie Black Friday oraz przedświątecznych zakupów wiele osób czeka na paczki i właśnie ten moment próbują wykorzystać cyberprzestępcy. CERT Polska obserwował kolejną kampanię phishingową, w której oszuści podszywają się pod firmę kurierską. W tym przypadku jest to firma DHL.
W wiadomościach e-mail przestępcy informują klienta, że przesyłka przed dalszą dostawą wymaga przejścia przez odprawę celną, a to jest związane z uiszczeniem niewielkiej opłaty. Po kliknięciu w link klient trafia na fałszywy formularz, który służy do wyłudzenia danych karty płatniczej. Przestępcy mogą następnie dokonywać nieautoryzowanych transakcji na rachunkach poszkodowanych osób.



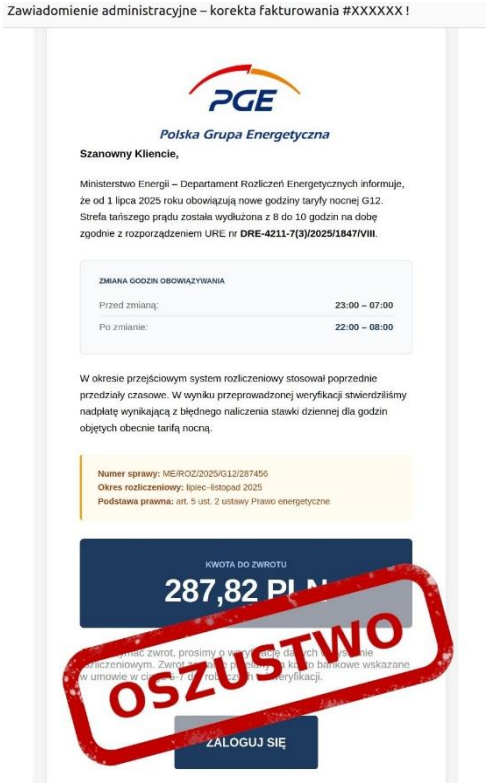
Zespół CERT Polska ostrzegał przed kampanią phishingową, w której przestępcy podszywają się pod jeden z popularnych serwisów do streamingu muzyki. Oszuści wysyłają wiadomości e-mail, w których informują o rzekomej konieczności aktualizacji metody płatności. Link zawarty w wiadomości prowadzi do fałszywej strony internetowej, która imituje panel logowania do serwisu. Pozyskane dane przestępcy mogą wykorzystać do przejęcia konta użytkownika. Zespół CERT Polska przypominał, żeby używać unikalnych haseł do różnych usług, a tam gdzie, to możliwe, ustawić także dwuetapową weryfikację.



Zespół CERT Polska zwracał uwagę, że przestępcy podszywają się pod operatorów komórkowych w wiadomościach e-mail zawierających informacje o rzekomym dwukrotnym opłaceniu ostatniej faktury przez odbiorcę wiadomości. Przekonują, że z tego tytułu należy mu się zwrot pieniędzy. Link w wiadomości kieruje na przygotowaną stronę phishingową, na której użytkownik jest proszony o podanie danych kontaktowych i karty płatniczej. Dane te są wykorzystywane do kolejnych oszustw i kradzieży pieniędzy z konta.



Zespół CERT Polska obserwował wzmożoną aktywność oszustów podszywających się pod firmy kurierskie. Pod pretekstem aktualizacji danych niezbędnych do dostarczenia przesyłki do odbiorcy przestępcy rozsyłają wiadomości SMS zawierające link do stron wyłudzających dane osobowe, adresowe i kart płatniczych. Często jako nadawca wiadomości figuruje nazwa firmy, tzw. nadpis. Taką wiadomość telefon może automatycznie umieścić w wątku z prawdziwą komunikacją od kuriera. W niektórych przypadkach oszuści podstawiają również fałszywe bramki płatnicze, które wizualnie niemal nie różnią się od prawdziwych – dlatego tak ważna jest weryfikacja adresu strony internetowej przed podaniem danych wrażliwych.

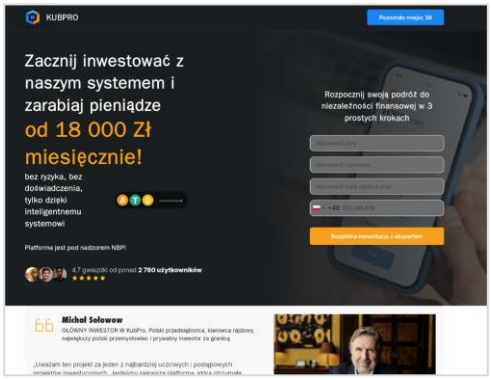


Zespół CERT Polska ostrzegał przed kolejną odsłoną kampanii oszustw opartych na rzekomym zwrocie pieniędzy. Przestępcy w wiadomościach e-mail podszywają się pod dostawców energii, powołują na rzekomą zmianę prawa i zachęcają do wejścia na przygotowaną przez nich stronę w celu weryfikacji danych w systemie rozliczeniowym. W ten sposób oszuści wyłudzają dane karty płatniczej.

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

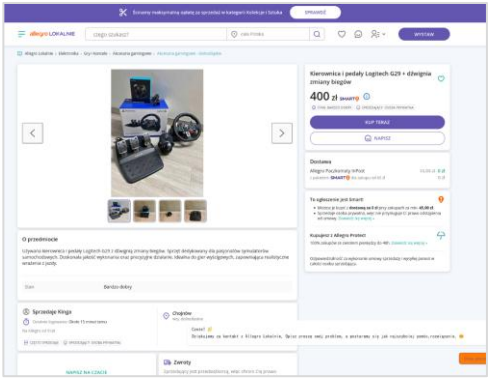
Opis najczęściej występujących kampanii – XII 2025

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 i PGE. 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 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 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 kanału TVN



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

Fałszywe strony Telewizji Polskiej (TVP)



Zespół CERT Polska obserwował kampanię phishingową, w której oszuści wykorzystują wizerunek strony internetowej Telewizji Polskiej. Na fałszywych witrynach znajdują się artykuły na temat inwestycji, na których rzekomo można zarobić z dużym zyskiem.

Fałszywe strony kanału Polsat News



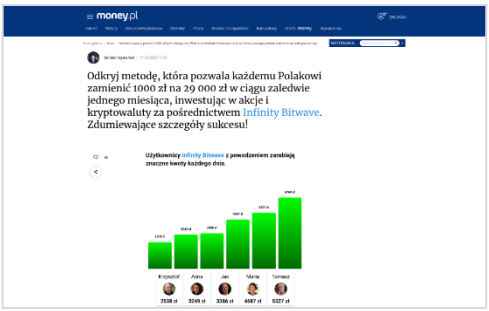
Zespół CERT Polska rejestrował incydenty, w których oszuści wykorzystują wizerunek kanału telewizyjnego Polsat News. Na fałszywych stronach internetowych umieszczają artykuły na temat inwestycji, na których rzekomo można zarobić z dużym zyskiem.

Fałszywe strony firmy Orlen



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

Fałszywe strony serwisu Money.pl



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

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 serwisu Fakt.pl



Zespół CERT Polska zarejestrował kampanię phishingową, w której wykorzystywany jest wizerunek serwisu Fakt.pl. Celem oszustów jest wyłudzenie środków finansowych poprzez fałszywą platformę inwestycyjną.