PAŹDZIERNIK 2025

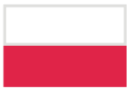
Podsumowanie Miesiąca CERT POLSKA CSIRT NASK

Nr 2/2025

CERT.PL NASK

CSIRT NASK

PODSUMOWANIE MIESIĄCA CERT POLSKA / CSIRT NASK



PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTERSTWA CYFRYZACJI

TLP: CLEAR

Autor: zespół CERT Polska

SPIS TREŚCI

Statystyki zarejestrowanych zagrożeń

Zgłoszenia i incydenty cyberbezpieczeństwa

Statystyki zawarte w niniejszym rozdziale obejmują dane o liczbie zarejestrowanych zgłoszeń[1] oraz o liczbie incydentów obsłużonych przez CSIRT NASK w okresie od 1 do 31 października 2025 r. Dla lepszego zobrazowania pojawiających się trendów niektóre z tych danych pokazywane są w dłuższej perspektywie czasu.

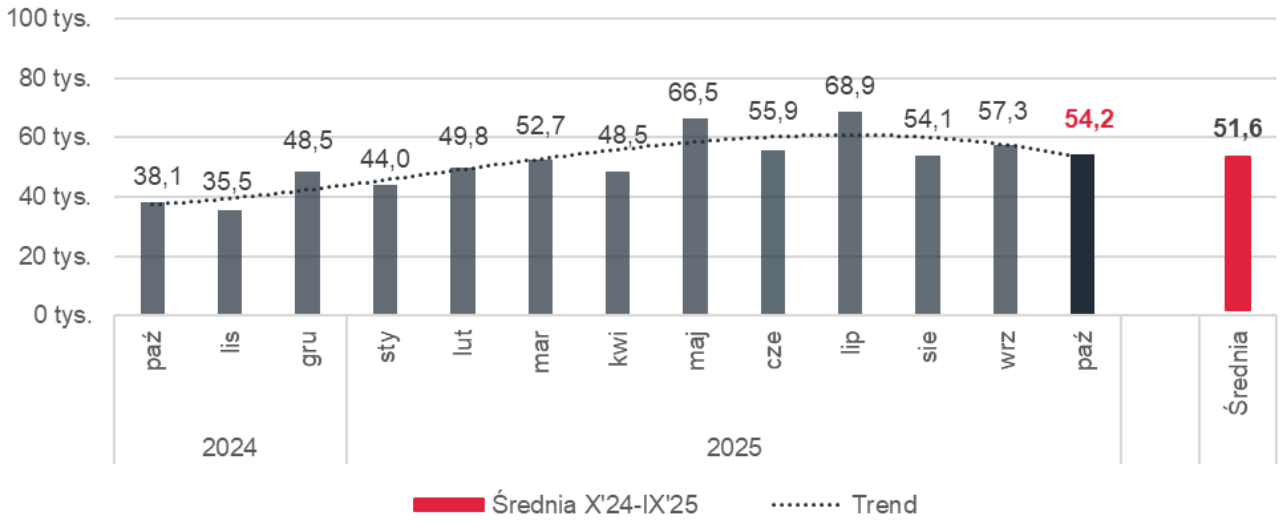
Zarejestrowane zgłoszenia i incydenty cyberbezpieczeństwa – X 2025

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

Zagrożenia cyberbezpieczeństwa	Liczba
Zarejestrowane zgłoszenia	**54,2 tys.**
w tym zarejestrowane (obsłużone) incydenty	**40,1 tys.**

W październiku 2025 r. CSIRT NASK otrzymał łącznie **54,2 tys.** zgłoszeń, które zostały przeanalizowane i pogrupowane. Na ich podstawie zarejestrowano **40,1 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 X 2024 do X 2025

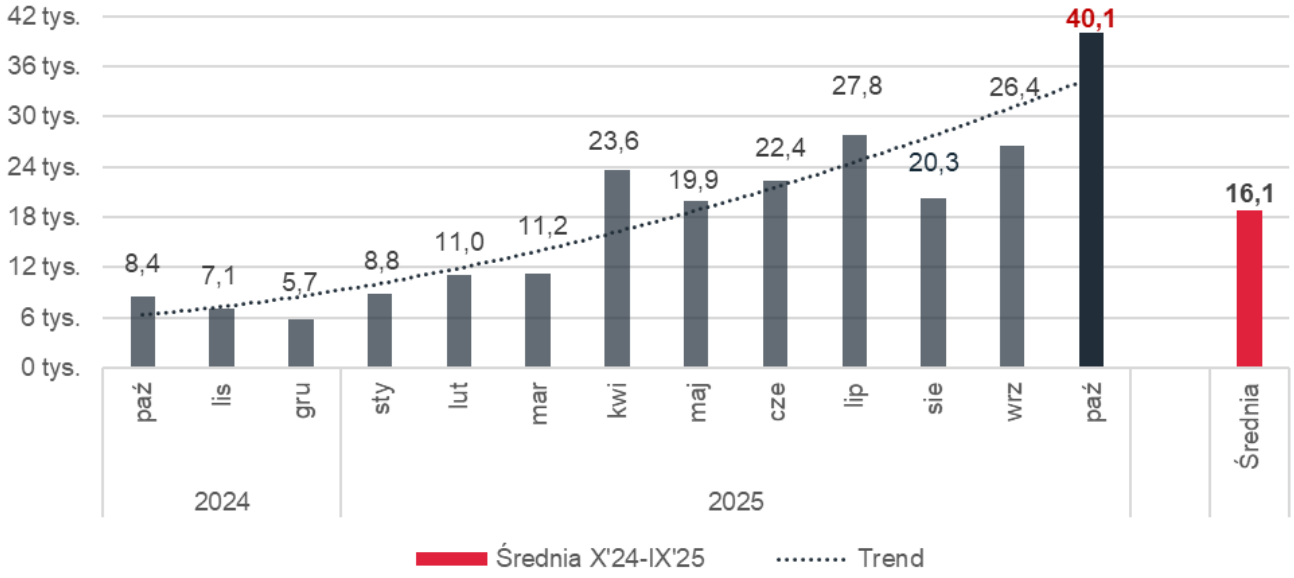


Wykres 1. Liczba zarejestrowanych zgłoszeń od 01.10.2024 do 31.10.2025. Źródło: CERT Polska / CSIRT NASK.

[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.

Liczba zgłoszeń odnotowanych w październiku 2025 r. przekroczyła średnią liczoną z poprzednich 12 miesięcy. W porównaniu z analogicznym miesiącem 2024 r. liczba ta **zwiększyła się o 42%**. W stosunku do września 2025 r. był to **spadek o 5%**.

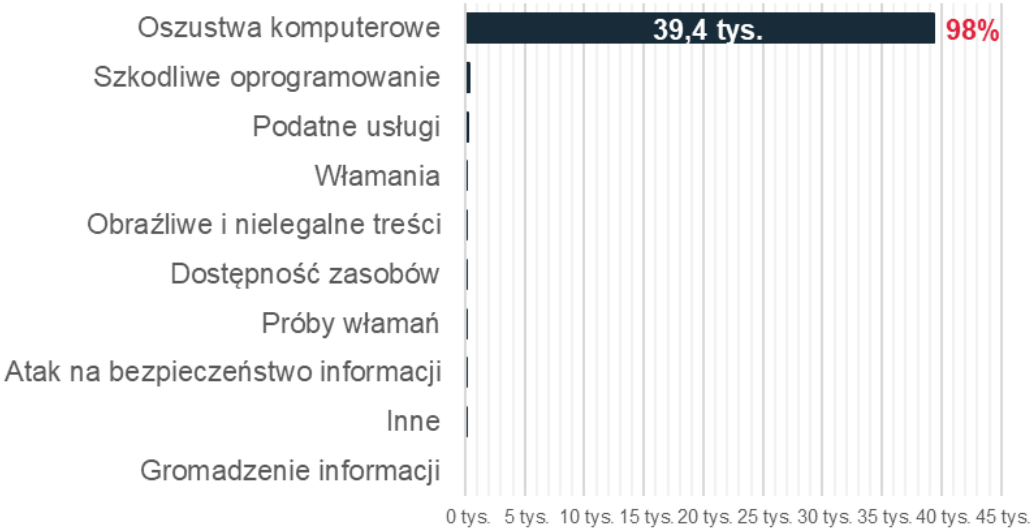
Zarejestrowane incydenty cyberbezpieczeństwa od X 2024 do X 2025



Wykres 2. Liczba zarejestrowanych incydentów od 01.10.2024 do 31.10.2025. Źródło: CERT Polska / CSIRT NASK.

Liczba incydentów zarejestrowanych w październiku 2025 r. wyniosła **40,1 tys.** W porównaniu z analogicznym miesiącem 2024 r. liczba incydentów w październiku 2025 r. **zwiększyła się o 375%** i pozostawała powyżej średniej liczonej z 12 poprzednich miesięcy. W stosunku do września 2025 r. liczba zarejestrowanych incydentów **zwiększyła się o 52%**.

Rodzaje zarejestrowanych zagrożeń – X 2025

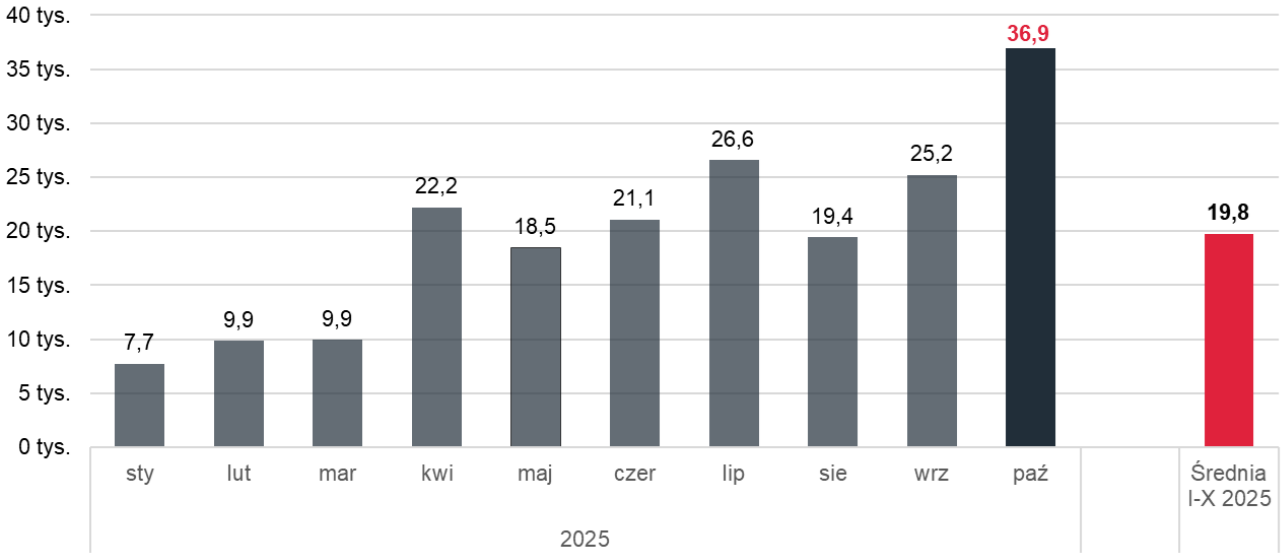


Wykres 3. Liczba zarejestrowanych incydentów według rodzaju od 1 do 31 października 2025 r. Źródło: CERT Polska / CSIRT NASK.

W analizowanym okresie zdecydowanie najczęściej występującą kategorią zagrożeń były oszustwa komputerowe. Wśród ogółu obsłużonych incydentów (**40,1 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 październiku 2025 r. łącznie odnotowano **11 tys.** tego typu incydentów.

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

CERT Polska prowadzi Listę Ostrzeżeń przed niebezpiecznymi stronami. Na listę wpisywane są domeny, które wprowadzają użytkowników w błąd oraz wyłudzają od nich dane. Szkodliwe domeny są blokowane na 6 miesięcy. Jeśli po upływie tego czasu nadal zawierają niebezpieczne treści, to zostają one dodane jako nowy wpis.



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

Od stycznia do października 2025 r. na Listę Ostrzeżeń przed niebezpiecznymi stronami wpisano **197,5 tys.** szkodliwych domen, z czego w październiku 2025 r. dodano **36,9 tys.** nazw domen wykorzystywanych do wyłudzania danych osobowych, danych uwierzytelniających do kont bankowych i serwisów społecznościowych. Wartość ta w stosunku do września 2025 r. **zwiększyła się o 46%**.

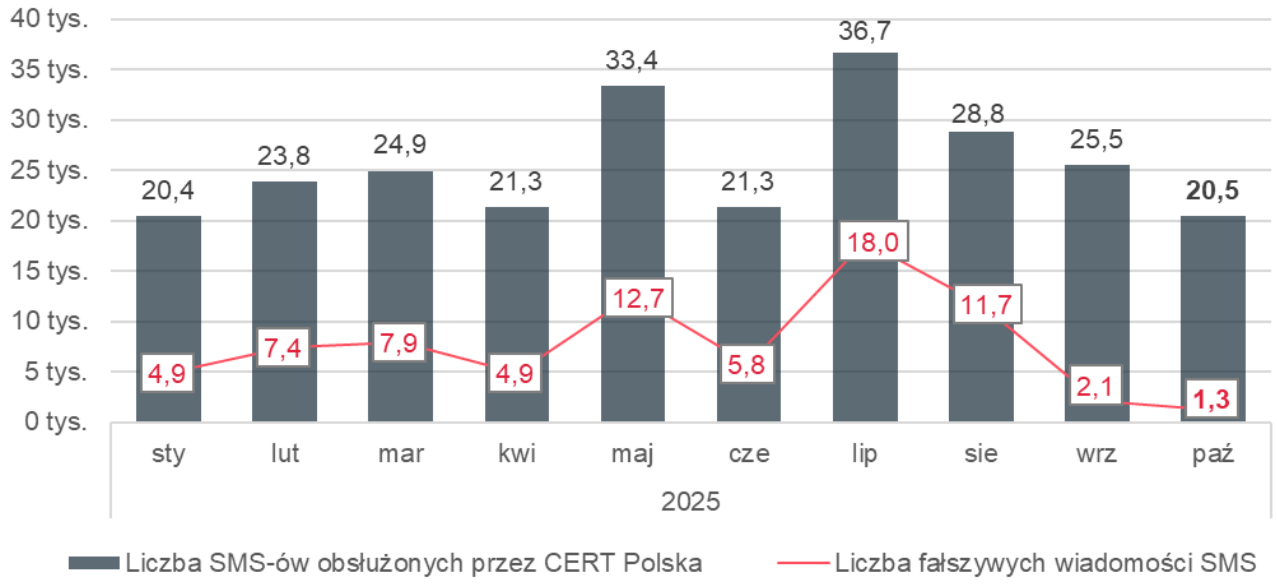
Lista Ostrzeżeń dostępna jest na stronie: CERT Polska/Lista Ostrzeżeń

Przykładowe nazwy fałszywych domen:

0lx.zam0wlenle73737.top; aiebilet.pl-smart5124.cfd; ai-investsoftware.com; allegro.bezpieczna-oferta92506972.cfd; biedronka-vip.shop; bitcoingoldmine-app.org; citibank.bfg.money; crypto-bankapp.com; drzewomadrosci.pl; eobuwie.pl-offr.shop; govministry.pl; inpost.lol; inpost-pakiet.com; klient-pkobppl-indywidualny.dream.press; morele-pl.com; my-disney-plus.com; netfilx-renwel.com; olx.pl-zakup-allegrosmart.cfd; pl-zakup-allegrosmart.cfd; pocztaonetpl.wixsite.com; polskagoldai-app.com; santader-lokaty.pl; sephora-promo.site; soc-telegram.org; tvn-energylandiazator.pl; tvn-pazdziernik.pl; vintedeu.com; vinted-profile.info; wiadomosci-gazeta24wyborcza.pl; zakupowcy.com; zalando-sale.top; zegarywinylowe.com; zwrot-podatku.dedyn.io

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

Od 1 stycznia do 31 października 2025 r. zespół CERT Polska zarejestrował **256,7 tys.** zgłoszeń SMS-ów. Liczba SMS-ów otrzymanych w październiku 2025 r. wyniosła **20,5 tys.** W porównaniu z wrześniem 2025 r. był to **spadek o 20%**. Wśród ogółu SMS-ów przyjętych w październiku 2025 r. **fałszywe wiadomości SMS stanowiły 6%**.



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

Wzorce fałszywych wiadomości SMS I–X 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. 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**.

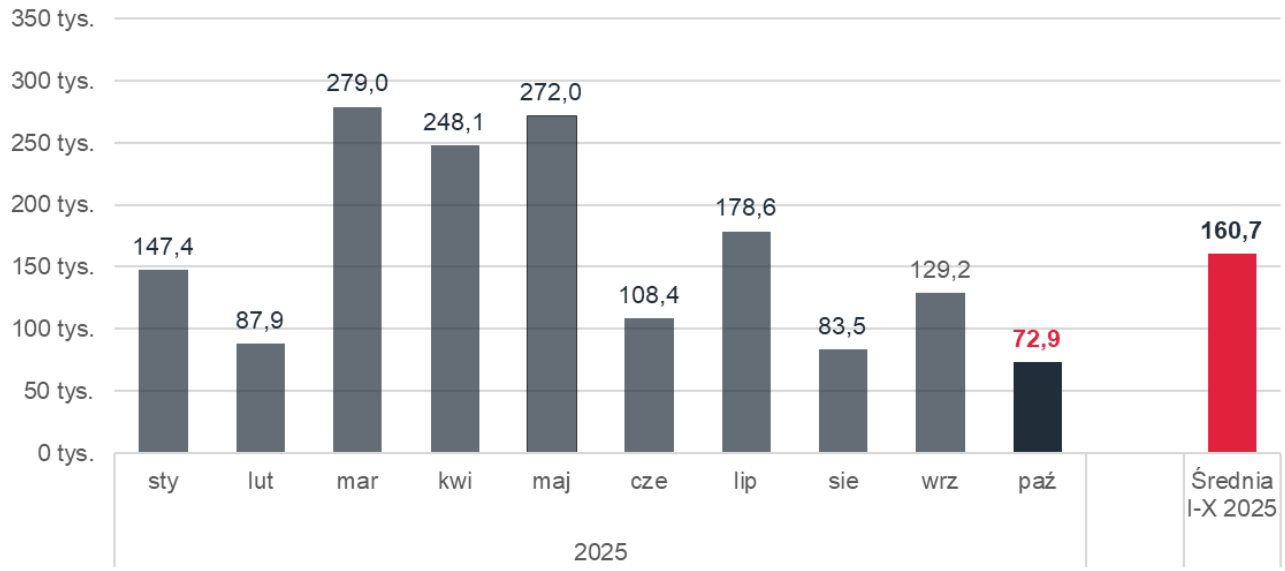
Tabela 2. Liczba wytworzonych wzorców fałszywych wiadomości SMS.

Wzorce fałszywych wiadomości SMS w 2025	sty	lut	mar	kwi	maj	cze	lip	sie	wrz	paź	Razem
Liczba wytworzonych wzorców	82	57	106	60	83	39	119	10	43	**36**	**635**

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

Liczba zablokowanych SMS-ów I–X 2025

W okresie od 1 stycznia do 31 października 2025 r., na podstawie wytworzonych przez CERT Polska wzorców fałszywych wiadomości SMS, zablokowano łącznie ponad **1,6 mln** SMS-ów.



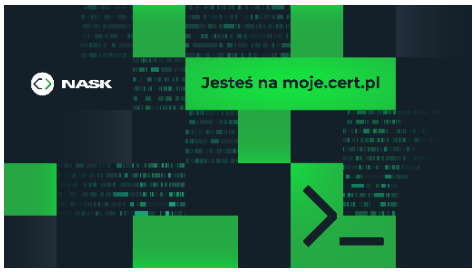
Wykres 6. Liczba SMS-ów zablokowanych na podstawie wzorców fałszywych wiadomości SMS w danym miesiącu. Źródło: CERT Polska / CSIRT NASK.

Moje.cert.pl

W 2025 r. zespół CERT Polska udostępnił szerokiemu gronu odbiorców 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 październiku 2025 r. w serwisie moje.cert.pl **zarejestrowało się 693 nowych użytkowników**.



W okresie od 1 do 31 października 2025 r. CSIRT NASK wysłał **3,8 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

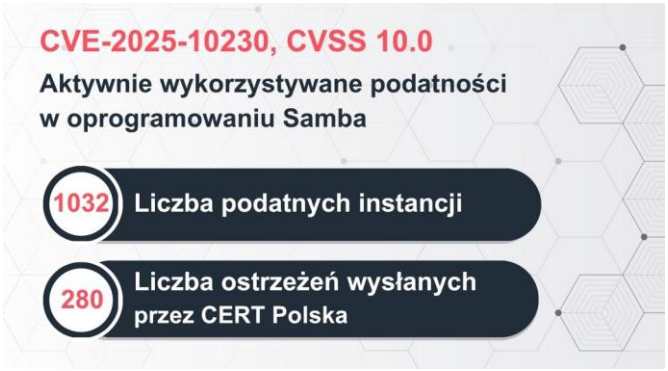
Zespół CERT Polska od sierpnia 2023 r. pełni funkcję CNA (ang. *CVE Numbering Authority*) – współtworzy bazę podatności poprzez nadawanie numerów CVE, które służą do identyfikacji i katalogowania publicznie ujawnionych podatności (więcej: CERT Polska/CNA). W październiku 2025 r. zespół CERT Polska nadał **12** numerów CVE. Wśród wykrytych podatności znalazły się podatności m.in. w oprogramowaniach SIMPLE.ERP, Studio Fabryka DobryCMS, Eveo URVE Smart Office, mMedica firmy Asseco Poland S.A. oraz w oprogramowaniu kamer Vilar VS-IPC1002. Przykładem podatności wykrytej przez CERT Polska w ramach badań własnych była podatność w oprogramowaniu Request Tracker.

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

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

Numery CVE w 2025	sty	lut	mar	kwi	maj	cze	lip	sie	wrz	paź	Razem
Liczba opublikowanych numerów CVE	4	9	11	15	22	3	6	36	16	**12**	**134**

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

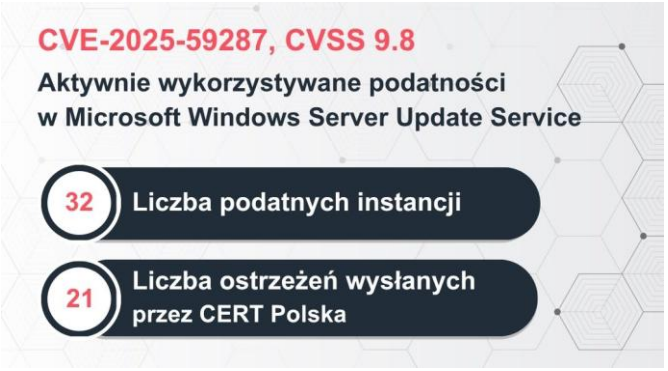


Podatność oznaczona jako CVE-2025-10230 umożliwia zdalne wykonanie kodu przez nieuwierzytelnionego atakującego poprzez wykorzystanie parametru wins hook, a w efekcie pozwala na przejęcie kontroli nad urządzeniem. Podatność występuje jedynie w środowiskach, w których oprogramowanie Samba jest wykorzystywane jako kontroler domeny i w których włączono protokół WINS. Według informacji pochodzących z niezależnej analizy, w chwili ujawnienia podatności zidentyfikowano około 266 tys. podatnych instancji.

Więcej: samba.org/CVE-2025-10230

W oprogramowaniu bazodanowym Redis wykryto podatność RediShell typu use-after-free, wynikającą z błędu ponownego wykorzystania zwolnionego miejsca w pamięci. Luka ta umożliwia uwierzytelnionemu atakującemu zdalne wykonanie kodu na systemie ofiary. Warto jednak zauważyć, że domyślna konfiguracja oprogramowania nie wymaga uwierzytelnienia, a wielu użytkowników pozostawia tę funkcję wyłączoną. Według badaczy, spośród około 330 tys. instancji wystawionych do internetu około 60 tys. działa bez uwierzytelnienia, co czyni je szczególnie podatnymi na atak. Podatność otrzymała maksymalną ocenę CVSS (ang. Common Vulnerability Scoring System), tj. 10.0.

Więcej: sekurak.pl/RediShell czyli krytyczna podatność w Redis



CVE-2025-59287 to podatność w usłudze Windows Server Update Service (WSUS) umożliwiająca zdalne wykonanie kodu przez nieuwierzytelnionego atakującego poprzez wykorzystanie błędu w odpakowywaniu (deserializacji) danych wejściowych. Podatność występuje jedynie w instancjach, dla których włączona jest funkcja WSUS Server Role, w domyślnej konfiguracji nie jest ona aktywna. W internecie dostępne są gotowe skrypty służące do eksploatacji tej podatności (gist.github.com/hawktrace/880b54fb9c07ddb028baaae401bd3951), dlatego kluczowa jest jej niezwłoczna mitygacja.

Więcej: msrc.microsoft.com/CVE-2025-59287

Wybrane informacje

1 października rozpoczęła się 13. edycja **Europejskiego Miesiąca Cyberbezpieczeństwa (ECSM – European Cybersecurity Month)**, kampanii zainicjowanej przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA). W ramach tej inicjatywy odbywają się konferencje, warsztaty, szkolenia i webinary, które mają zwiększać świadomość cyberzagrożeń oraz promować dobre praktyki. Oficjalna inauguracja 13. edycji ECSM odbyła się w Brukseli. Wśród wydarzeń towarzyszących były panele dyskusyjne poświęcone różnym aspektom cyberbezpieczeństwa. Ekspert zespołu CERT Polska uczestniczył w dyskusji na temat wzmacniania współpracy instytucji w zakresie zarządzania sytuacjami kryzysowymi w cyberbezpieczeństwie. W Polsce działania związane z kampanią ECSM koordynuje NASK-PIB.

Więcej: nask.pl/Ataki, dezinformacja, AI. Rusza Europejski Miesiąc Cyberbezpieczeństwa!

2 października w Warszawie odbyła się 6. edycja **konferencji Cyber24 Day**. Wśród poruszanych zagadnień była odporność Polski i Europy na cyberataki. Tej tematyce poświęcono panel pt. „Wyrafinowane, zdeterminowane, dofinansowane. Jak odpierać ataki grup APT?”, w którym uczestniczył kierownik CERT Polska. Eksperci dyskutowali o aktywności grup APT, budowaniu odporności na ich działania, o wyzwaniach w zakresie atrybucji ataków oraz na temat roli sztucznej inteligencji w cyberobronie.

Więcej: cyberdefence24.pl/Grupy APT jako długofalowe zagrożenie dla cyberbezpieczeństwa

---

W dniach 2–3 października w Józefowie odbyło się **XXXI Forum Teleinformatyki**. Temat przewodni tegorocznej edycji brzmiał: „System informacyjny państwa – czas na przełomowe idee, technologie, projekty”. Wśród uczestników byli eksperci z NASK-PIB, którzy wzięli udział m.in. w sesjach na temat cyberbezpieczeństwa procesów informacyjnych oraz cyberbezpieczeństwa w sektorze ochrony zdrowia.

Więcej: Forumti.pl

Od 6 do 9 października w Warszawie odbywały się **finały European Cybersecurity Challenge 2025 (ECSC)**, organizowane w tym roku przez **NASK-PIB i Ministerstwo Cyfryzacji**. ECSC to międzynarodowe prestiżowe zawody cyberbezpieczeństwa typu CTF (Capture The Flag) dla młodych talentów w wieku od 14 do 25 lat, rozgrywane pod patronatem ENISA. Zwycięzcami tegorocznej edycji, w której wzięło udział 40 narodowych drużyn, zostali reprezentanci Włoch, a drużyna z Polski zajęła 7. miejsce. W Polsce za kwalifikacje do zawodów odpowiadał **zespół CERT Polska**. Eksperci z tego zespołu byli obecni także podczas finałów: wystąpili w roli trenerów polskiej reprezentacji, prowadzili otwarty webinar z przełamywania zabezpieczeń aplikacji webowych, zajęcia praktyczne z kryptografii dla olimpijczyków, odpowiadali za część organizacyjną wydarzenia.

Więcej: nask.pl/Cyberbitwa rozstrzygnięta!

10 października na stronie nask.pl ukazał się artykuł pt. **„Nie daj cyberprzestępcom szans. Dzień Bezpiecznego Komputera”**. W tekście przedstawiono najważniejsze informacje na temat metod wykorzystywanych przez oszustów oraz porady ekspertów dla użytkowników sieci dotyczące podstawowych zasad bezpieczeństwa online.

Więcej: nask.pl/Nie daj cyberprzestępcom szans. Dzień Bezpiecznego Komputera

---

21 października zespół CERT Polska przypominał o tym, że weryfikacja adresu strony to pierwsza linia obrony przed phishingiem. Szczegółowe informacje na temat rozpoznawania stron przygotowanych przez oszustów znajdują się w artykule **„Jak rozpoznać fałszywe strony internetowe i uniknąć phishingu”** opublikowanym na stronie cert.pl.

Więcej: cert.pl/Jak rozpoznać fałszywe strony internetowe

28 października odbył się bezpłatny webinar dla przedsiębiorców pt. **„Wyciek i kradzież danych klientów – jak się zabezpieczyć?”**. Webinar otworzył serię szkoleń online realizowanych przez NASK-PIB oraz Ministerstwo Rozwoju i Technologii w ramach projektu „Cyfrowy Biznes”. Celem szkoleń jest wyposażenie przedsiębiorców w praktyczne umiejętności oraz narzędzia, które pozwalają skutecznie chronić dane i bezpiecznie rozwijać działalność w internecie.

Więcej: nask.pl/Cyberodporność w praktyce – bezpłatny webinar NASK i MRiT dla firm

Wystąpienia ekspertów CERT Polska

- 1 października – udział w panelu dyskusyjnym na temat geopolitycznych aspektów cyberbezpieczeństwa podczas ENISA CTI Conference 2025 w Brukseli.

  Więcej: enisa.europa.eu/CTI Conference 2025
- 7 października – udział w panelu poświęconym zarządzaniu incydentami i określaniu stopnia ich krytyczności, Bucharest Cybersecurity Conference 2025.

  Więcej: cybersecurity-centre.europa.eu/BCC2025
- 16 października – wystąpienie podczas konferencji „Lubelskie Cyberbezpieczne” na temat najlepszych praktyk z zakresu cyberbezpieczeństwa.

  Więcej: cbzc.policja.gov.pl/Konferencja Lubelskie Cyberbezpieczne
- 20 października – na konferencji Mega Sekurak Hacking Party odbywającej się w Krakowie kierownik CERT Polska zaprezentował, w jaki sposób serwis moje.cert.pl pomaga organizacjom monitorować bezpieczeństwo.

  Więcej: hackingparty.pl
- 21 października – prezentacja na temat wykrywania phishingu w ekosystemie DNS, konferencja hack.lu w Luksemburgu.

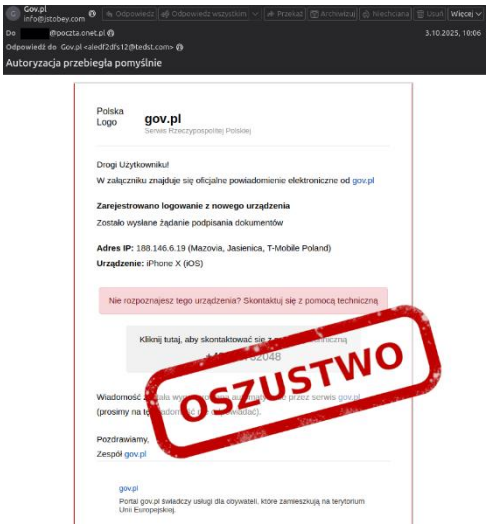
  Więcej: hack.lu/agenda
- 22 października – w ramach cyklu webinarów organizowanych przez ICANN i poświęconych walce z zagrożeniami cyfrowymi ekspert z zespołu CERT Polska wystąpił z prezentacją pt. „Jak polski zespół CSIRT radzi sobie z phishingiem, spamem i szkodliwymi SMS-ami”.

  Więcej: icann.org/ICANN Webinar Series for Europe: Fighting Digital Threats – How Poland's CSIRT Tackles Phishing, Spam and Malicious SMS
- 30 października – udział w spotkaniu w Ministerstwie Infrastruktury na temat cyberbezpieczeństwa sektora lotniczego – przedstawienie prezentacji na temat zagrożeń cyberbezpieczeństwa oraz roli serwisu moje.cert.pl we wzmacnianiu bezpieczeństwa instytucji.

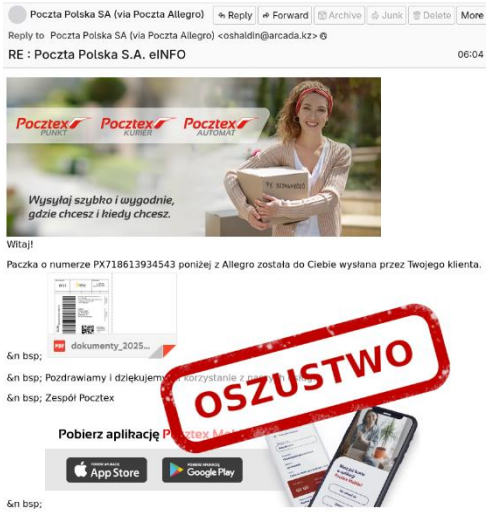
– 30 października – ekspert z zespołu CERT Polska prowadził warsztat poświęcony procesowi CVD (ang. *Coordinated Vulnerability Disclosure*, pol. koordynowane ujawnianie podatności) dla przedstawicieli organizacji rządowych oraz podmiotów infrastruktury krytycznej w Kosowie podczas spotkania grupy roboczej ds. cyberbezpieczeństwa infrastruktury krytycznej odbywającego się w Prisztinie.

Komunikaty o zagrożeniach

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

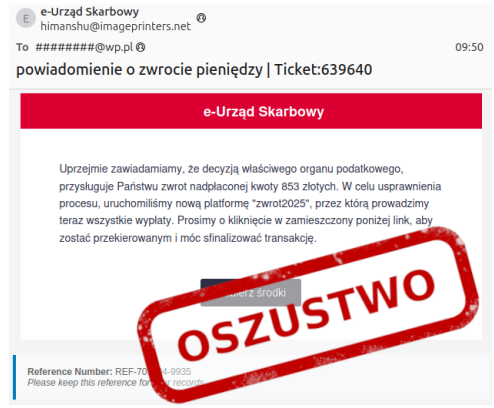


Zespół CERT Polska ostrzegał przed kampanią wykorzystującą wizerunek portalu gov.pl. W wiadomości e-mail imitującej typowe zabezpieczenie przed nieautoryzowanym dostępem oszuści informują, że na konto w portalu dokonano logowania z nowego nieznanego urządzenia. Sugestia zawarta w wiadomości, że logowanie nastąpiło w celu podpisania dokumentów, ma na celu wywołanie w użytkowniku niepokoju i skłonienie go do działania. W wiadomości znajduje się numer telefonu do rzekomej „pomocy technicznej". Nawiązanie kontaktu z przestępcami skutkuje próbą zmanipulowania i wyłudzenia środków finansowych. W takich przypadkach zawsze należy weryfikować domenę nadawcy wiadomości, czyli część adresu e-mail po znaku „@".



Zespół CERT Polska informował o kolejnej odsłonie kampanii phishingowych, w których oszuści podszywają się pod firmę kurierską. W wiadomości e-mail znajduje się informacja o nowej paczce wysłanej przez klienta, rzekomo za pośrednictwem usługi Pocztex. Zdjęcie załączone do wiadomości, które ma imitować etykietę przesyłki, zawiera odnośnik do strony pobierającej szkodliwe oprogramowanie.

Zespół CERT Polska opisywał najnowszą odsłonę kampanii oszustw na „niedostarczoną paczkę". Oszuści rozsyłają wiadomości e-mail, w których informują o paczce rzekomo gotowej do odbioru. Nadawcy wiadomości zachęcają do otwarcia załącznika, by zapoznać się ze szczegółami – kodem odbioru i aktualną lokalizacją paczki. W załączonym archiwum zip znajduje się plik ze szkodliwym oprogramowaniem, najczęściej w formacie .js.



Zespół CERT Polska obserwował dużą aktywność cyberprzestępców, którzy w wiadomościach e-mail podszywają się pod Urząd Skarbowy. W treści wiadomości, poza informacją o rzekomym zwrocie podatku, znajduje się link do strony internetowej. Witryna pozwala na wybór banku, a następnie prosi o podanie danych karty płatniczej i danych kontaktowych. Dane te trafiają bezpośrednio do przestępców, którzy mogą je wykorzystać do kradzieży pieniędzy z konta.

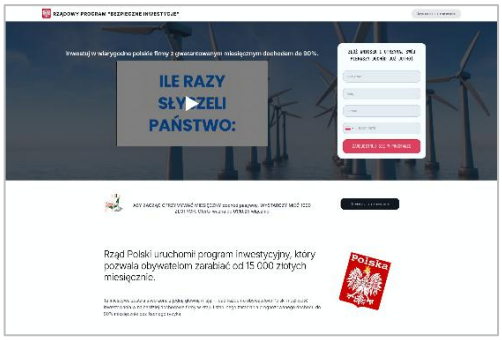
Zespół CERT Polska informował o bardzo podobnej kampanii do opisanej powyżej, w której przestępcy podszywają się pod Urząd Skarbowy. Oszuści stosują znany schemat – wysyłają informację o rzekomym zwrocie podatku oraz link do strony internetowej wyłudzającej dane karty płatniczej – jednak w tym przypadku dystrybucja phishingu odbywa się nie za pomocą e-maili, tylko wiadomości SMS.

Zespół CERT Polska ostrzegał przed kampanią phishingową, w której oszuści podszywają się pod Ministerstwo Cyfryzacji i wiceministra Pawła Olszewskiego. Atakujący wysyłają do jednostek samorządu terytorialnego spreparowane wiadomości imitujące oficjalną komunikację Ministerstwa Cyfryzacji. Pierwsza z wiadomości, wysłana 28.10.2025, zawierała szkodliwy plik wykonywalny arkusza kalkulacyjnego XLSX, który po uruchomieniu infekował hosta. Druga fałszywa wiadomość, wysłana 30.10.2025, bazowała na socjotechnice – jej celem było wyłudzenie danych osób odpowiedzialnych za bezpieczeństwo teleinformatyczne w danej organizacji. Przed kampanią ostrzegał także Pełnomocnik Rządu ds. Cyberbezpieczeństwa, który 30.10 wydał pilny komunikat.

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

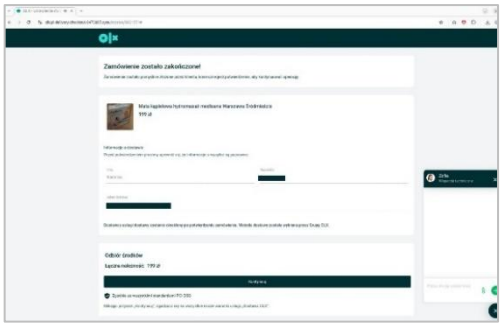
Opis najczęściej występujących kampanii – X 2025

Fałszywe strony oferujące wysokodochodowe inwestycje



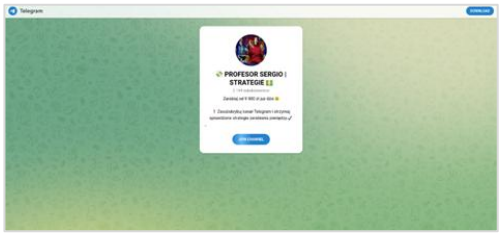
Zespół CERT Polska w dalszym ciągu obserwował wzmożoną kampanię phishingową, w której oszuści podszywają się pod różnego rodzaju koncerny paliwowo-energetyczne, firmy, instytucje, m.in. Lotos, Tesla, PGNiG i PGE. Oszuści reklamują w mediach społecznościowych czy w wyszukiwarkach internetowych nieistniejące 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 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.

OLX



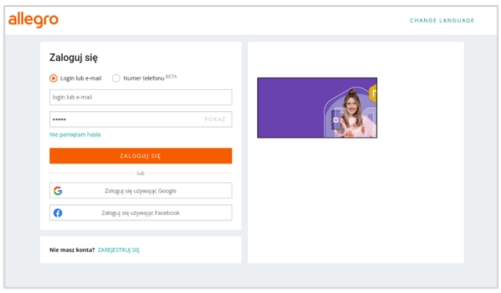
Zespół CERT Polska zarejestrował incydenty, w których atakujący za pośrednictwem stron internetowych podszywają się pod serwis OLX. Oszuści kontaktują się z potencjalną ofiarą przez komunikator WhatsApp. Wyrażają zainteresowanie przedmiotem z ogłoszenia, następnie informują, że zapłacili za zamówienie, 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.

Telegram Web



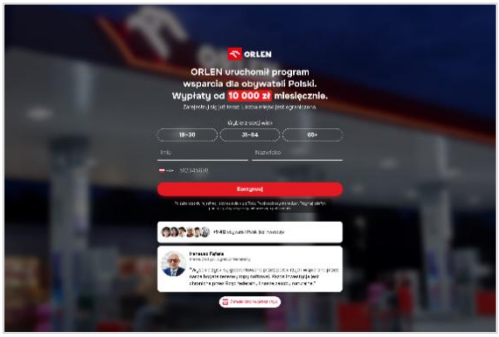
Zespół CERT Polska obserwował kampanię phishingową, w której wykorzystywany jest wizerunek komunikatora Telegram Web. Celem oszustów jest wyłudzenie środków finansowych poprzez fałszywą platformę inwestycyjną.

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.

Orlen



Zespół CERT Polska w dalszym ciągu rejestrował kampanię phishingową, w której wykorzystywany jest wizerunek Orlenu. Celem oszustów jest wyłudzenie środków finansowych poprzez fałszywą platformę inwestycyjną.

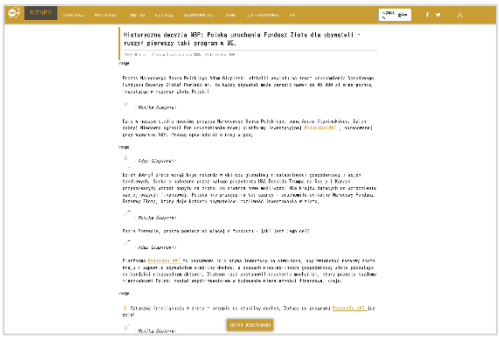
Polsat News

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.

Onet.pl

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

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.

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 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.