PAŹDZIERNIK 2026

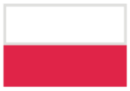
Podsumowanie Miesiąca CERT POLSKA

Nr 10/2026

CERT.PL NASK

CSIRT NASK

PODSUMOWANIE MIESIĄCA CERT POLSKA





PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTERSTWA CYFRYZACJI

TLP: CLEAR

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

Autor: zespół CERT Polska

© Państwowy Instytut Badawczy NASK

Publikacja jest rozpowszechniana na zasadach licencji Creative Commons.

Uznanie autorstwa (CC BY) 4.0 Międzynarodowe.

SPIS TREŚCI

Statystyki zgłoszonych zagrożeń oraz zarejestrowanych incydentów 4

Moje.cert.pl 9

Podatności CVE 10

Wybrane podatności i ich wpływ na krajobraz cyberbezpieczeństwa w Polsce – X 2026 10

Wybrane informacje 12

Wystąpienia ekspertów CERT Polska 14

Komunikaty o zagrożeniach 15

Opis najczęściej występujących kampanii – X 2026 19

Statystyki zgłoszonych zagrożeń oraz zarejestrowanych incydentów

Zgłoszenia i incydenty cyberbezpieczeństwa

Statystyki przedstawione w tym rozdziale obejmują dane o liczbie zgłoszeń[1] oraz o liczbie incydentów obsłużonych przez CSIRT NASK w okresie od 1 do 31 października 2026 r. Wybrane dane ujęto również w szerszym horyzoncie czasowym, aby umożliwić obserwację zmian zachodzących w dłuższym okresie.

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

Zgłoszone zagrożenia oraz zarejestrowane incydenty – X 2026

Tabela 1. Liczba zgłoszeń oraz zarejestrowanych incydentów od 1 do 31 października 2026 r.

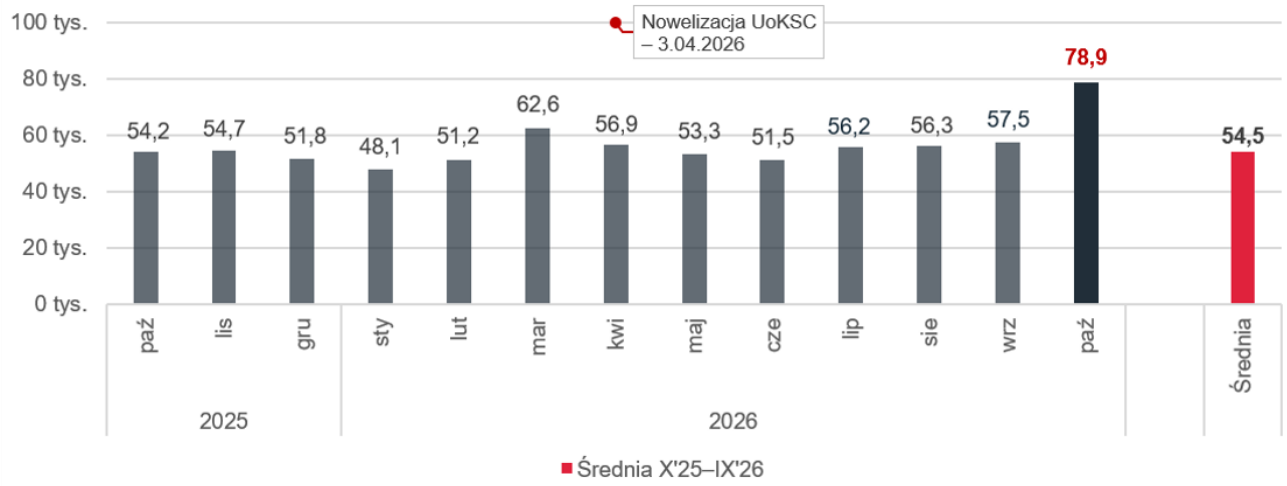
Zgłoszone zagrożenia i zarejestrowane incydenty	Liczba
Zgłoszenia potencjalnych zdarzeń dla cyberbezpieczeństwa*	7,6 tys.
Zgłoszenia cyberzagrożeń*	67,6 tys.
Zgłoszenia incydentów	3,6 tys.
Zgłoszenia poważnych cyberzagrożeń*	0,04 tys.
Razem zgłoszenia	**78,9 tys.**
Zarejestrowane incydenty**	**21,5 tys.**

* Nowe kategorie zgłoszeń raportowane od kwietnia 2026 r. ** Incydenty zostały zarejestrowane na podstawie zgłoszeń incydentów, zgłoszeń cyberzagrożeń, zgłoszeń poważnych cyberzagrożeń oraz zgłoszeń potencjalnych zdarzeń dla cyberbezpieczeństwa.

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

W październiku 2026 r. zespół CERT Polska otrzymał **łącznie 78,9 tys. zgłoszeń**. Na ich podstawie **zarejestrowano 21,5 tys. incydentów** cyberbezpieczeństwa, które miały lub mogły mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych. Dotyczą one konkretnych kategorii zagrożeń, np. szkodliwych stron wyłudzających poufne informacje (ang. *phishing*), spamu czy ataku z użyciem szkodliwego oprogramowania. W wielu przypadkach jeden incydent był powiązany z kilkoma zgłoszeniami.

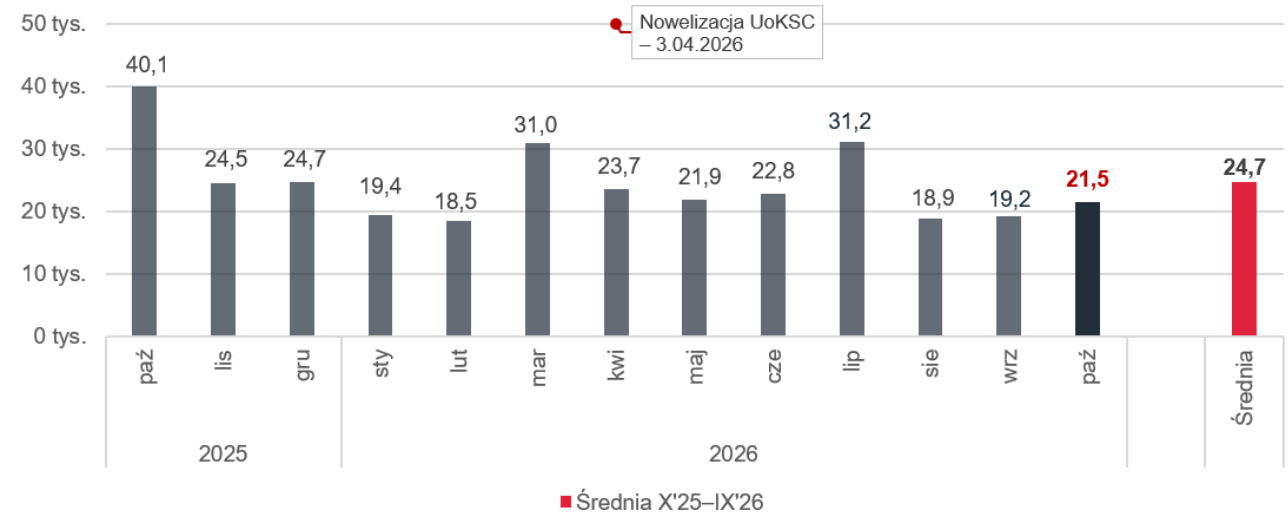
Zgłoszenia zagrożeń od X 2025 do X 2026



Wykres 1. Liczba wszystkich zgłoszeń od 01.10.2025 do 31.10.2026. Źródło: CERT Polska / CSIRT NASK.

Liczba wszystkich zgłoszeń odnotowanych w październiku 2026 r. utrzymywała się powyżej średniej z poprzednich 12 miesięcy. W porównaniu z analogicznym miesiącem 2025 r. liczba ta **zwiększyła się o 46%**, natomiast w stosunku do września 2026 r. **wzrosła o 37%**.

Zarejestrowane incydenty cyberbezpieczeństwa od X 2025 do X 2026



Wykres 2. Liczba zarejestrowanych incydentów od 01.10.2025 do 31.10.2026. Źródło: CERT Polska / CSIRT NASK.

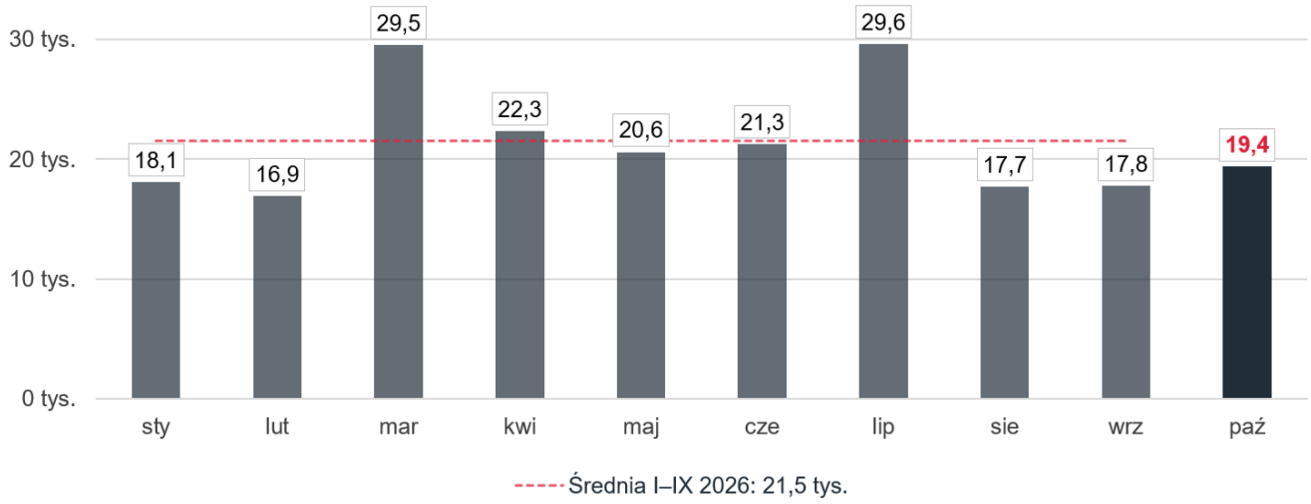
Liczba incydentów zarejestrowanych w październiku 2026 r. wyniosła **21,5 tys.** W porównaniu z analogicznym miesiącem 2025 r. **była niższa o 46%** i utrzymywała się poniżej średniej z poprzednich 12 miesięcy. Jednocześnie w stosunku do września 2026 r. liczba incydentów **wzrosła o 12%**.

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



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

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



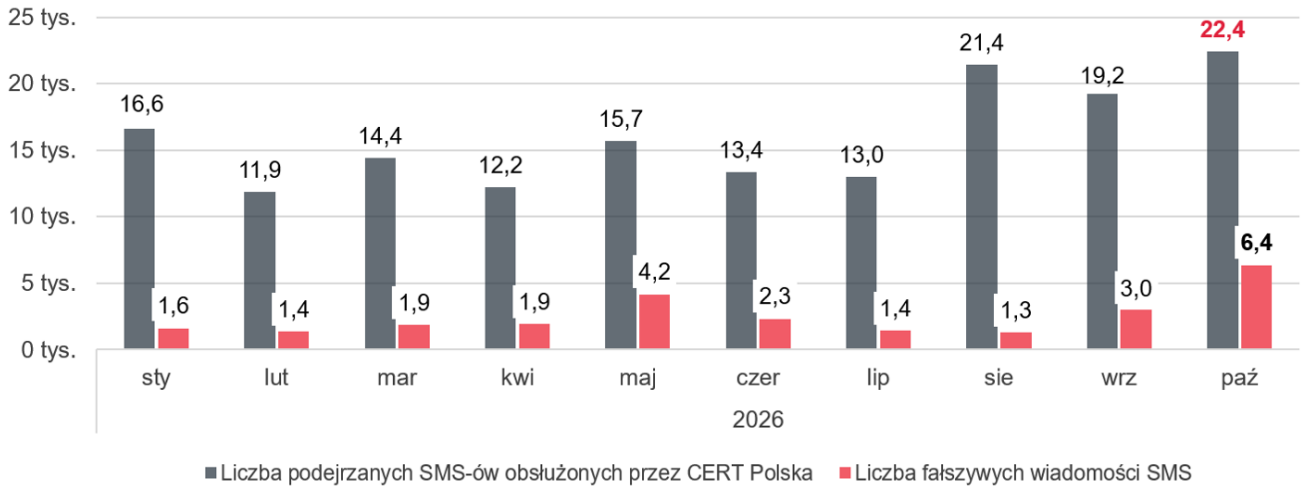
Wykres 3. Liczba nazw szkodliwych domen wpisanych na Listę Ostrzeżeń. Źródło: CERT Polska / CSIRT NASK.

Od 1 stycznia do 31 października 2026 r. na Listę Ostrzeżeń przed niebezpiecznymi stronami wpisano **213,1 tys.** szkodliwych domen, z czego w październiku 2026 r. dodano **19,4 tys.** nazw domen wykorzystywanych do wyłudzania danych osobowych, danych uwierzytelniających do kont bankowych i serwisów społecznościowych. Wartość ta w stosunku do września 2026 r. **wzrosła o 9%**.



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

Od 1 stycznia do 31 października 2026 r. zespół CERT Polska zarejestrował **160,2 tys.** zgłoszeń podejrzanych SMS-ów. Liczba SMS-ów otrzymanych w październiku 2026 r. wyniosła **22,4 tys.** W porównaniu z wrześniem 2026 r. był to **wzrost o 17%**. Wśród ogółu SMS-ów przyjętych w październiku 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 28%**.



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

Wzorce fałszywych wiadomości SMS I–X 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 październiku 2026 r., na podstawie wytworzonych przez CERT Polska wzorców fałszywych wiadomości SMS, zablokowano łącznie **31,7 tys.** SMS-ów. Dane o zablokowanych wiadomościach SMS są szacowane na podstawie raportów przesyłanych przez operatorów telekomunikacyjnych z uwzględnieniem procentowego udziału tych operatorów w rynku telefonii mobilnej.

Tabela 2. Liczba wytworzonych wzorców fałszywych wiadomości SMS.

Wzorce fałszywych wiadomości SMS w 2026	sty	lut	mar	kwi	maj	cze	lip	sie	wrz	paź	Razem
Liczba wytworzonych wzorców	118	97	85	80	105	36	57	94	67	**74**	**813**

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

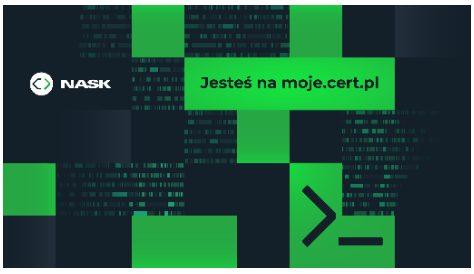
Moje.cert.pl

W 2025 r. zespół CERT Polska udostępnił bezpłatny serwis moje.cert.pl. Mogą z niego korzystać zarówno osoby prywatne posiadające stronę internetową, jak i firmy oraz instytucje publiczne. Zarejestrowany użytkownik moje.cert.pl może zamówić bezpłatne skanowanie bezpieczeństwa swoich domen, otrzymać informacje o wyciekach haseł użytkowników w swojej domenie, 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.

W serwisie dostępne są także moduły: **„Infrastruktura organizacji”** (pozwala zobaczyć całość infrastruktury widocznej z internetu, np. subdomeny, hosty, otwarte porty i powiązane z nimi podatności) oraz **„Podatności w używanych technologiach”** (podmioty wyrażają zgodę na wykorzystanie informacji o swojej infrastrukturze, dzięki czemu system może je zestawiać ze zbieranymi na bieżąco informacjami o nowych lukach bezpieczeństwa, np. w bramkach VPN).

Ponadto w serwisie, w zakładce „Komunikaty” zespół CERT Polska publikuje ostrzeżenia dotyczące polskiej cyberprzestrzeni oraz alerty o podatnościach. Komunikaty te są dostępne na stronie także dla niezarejestrowanych użytkowników, można również otrzymywać je 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 2026 r. w serwisie moje.cert.pl **zarejestrowało się 1,7 tys. nowych użytkowników**.



W okresie od 1 do 31 października 2026 r. CERT Polska wysłał **13,3 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

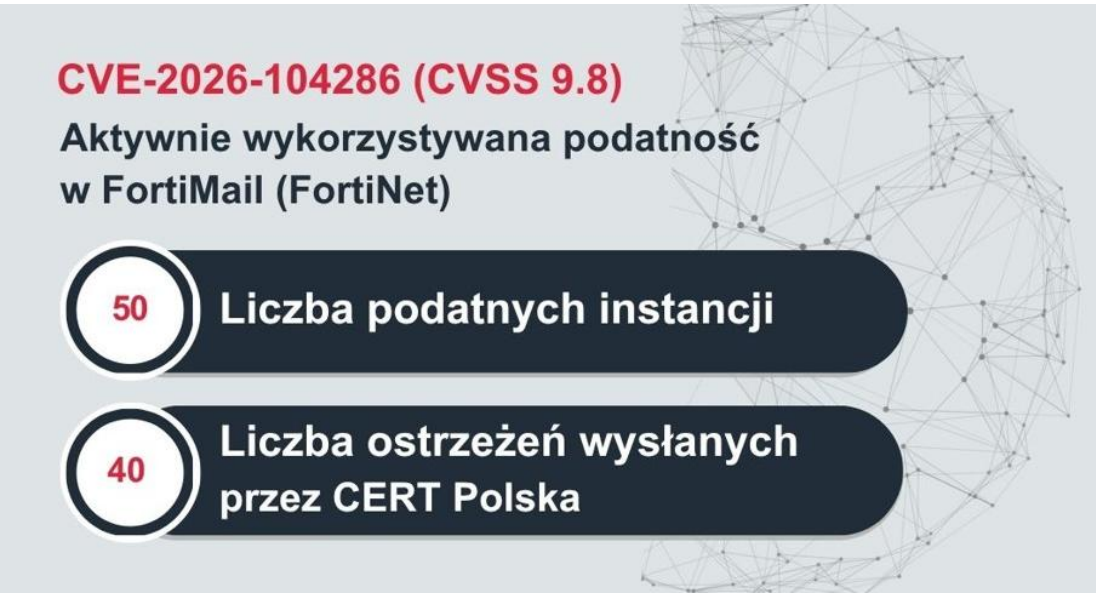
Zespół CERT Polska od sierpnia 2023 r. pełni funkcję CNA (ang. *CVE Numbering Authority*) – współtworzy bazę podatności poprzez nadawanie numerów CVE, które służą do identyfikacji i katalogowania publicznie ujawnionych podatności (więcej: CERT Polska/CNA). W październiku 2026 r. zespół CERT Polska **55** numerów CVE. Wśród wykrytych podatności znalazły się podatności w oprogramowaniu m.in. GNU Aspell, Sparx Systems Enterprise Architect, CGM CLININET, MTW CleanShot X, KGS Software tia Viewer, Wing FTP Server, Szafir, Płatnik. W ramach badań własnych CERT Polska znalazł **5** podatności: w oprogramowaniu Zimbra Collaboration (2 podatności) i Request Tracker oraz RT for Incident Response (3 podatności).

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

Tabela 3. Nadane numery CVE od 1 stycznia do 31 października 2026 r.

Numery CVE w 2026	sty	lut	mar	kwi	maj	cze	lip	sie	wrz	paź	Razem
Liczba opublikowanych numerów CVE	16	12	32	21	34	47	53	33	35	**55**	**338**

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

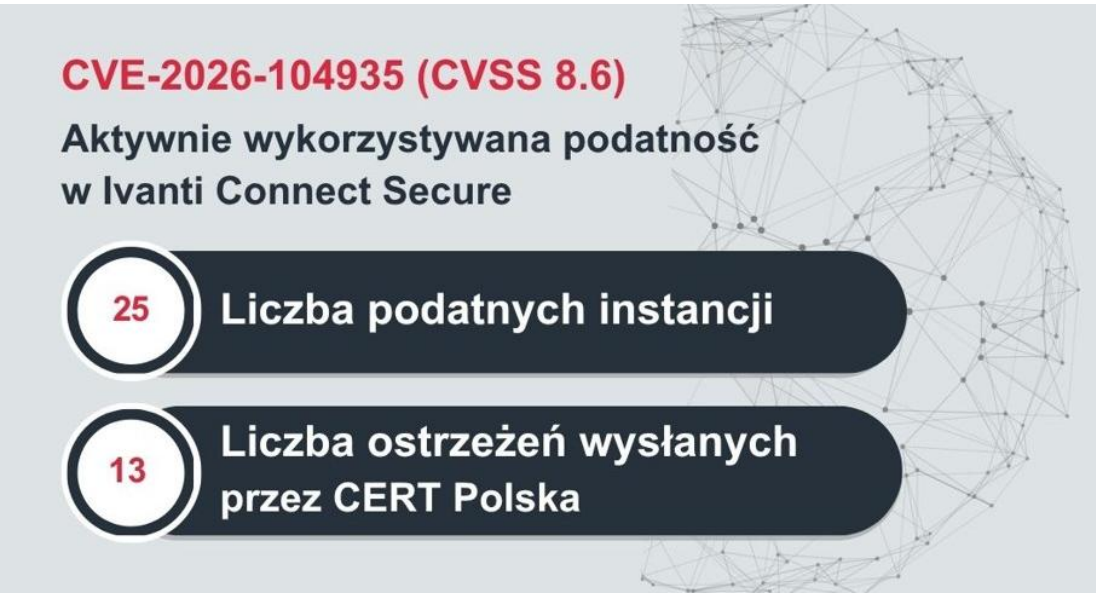


Krytyczna podatność w bramce pocztowej FortiMail, potwierdzona przez producenta jako aktywnie wykorzystywana w atakach. Podatność umożliwia nieuwierzytelnionemu atakującemu zapisywanie dowolnych plików w systemie, a w konsekwencji wykonanie dowolnego kodu poprzez specjalnie sformatowane żądania HTTP. Wykorzystanie podatności wymaga dostępu do interfejsu zarządzania

FortiMail. Skutki obejmują przejęcie bramki pocztowej i potencjalny dostęp do przetwarzanej korespondencji.

Rekomendujemy aktualizację do wersji FortiMail 8.0.2, 7.6.7 lub 7.4.9 albo nowszych. Dla gałęzi 7.2 zalecana jest migracja do gałęzi 7.4 lub nowszej, ponieważ poprawka (7.2.10) nie została jeszcze opublikowana. Instalacje na wersji 7.0 wymagają migracji do wersji poprawionej.

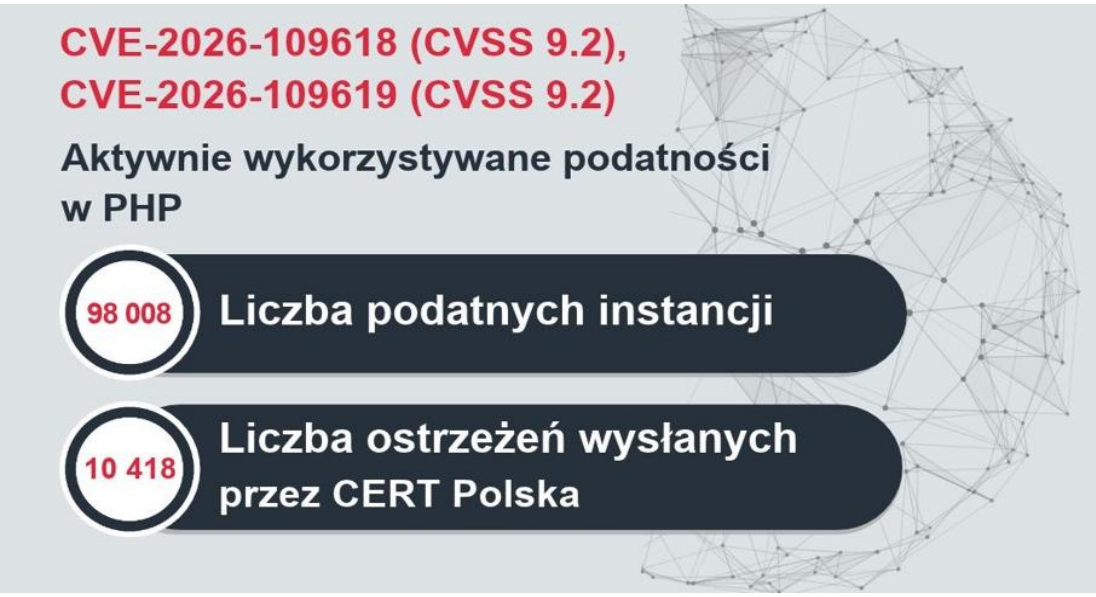
Więcej: https://nvd.nist.gov/vuln/detail/cve-2026-104286, https://fortiguard.fortinet.com/psirt/FG-IR-26-175



Podatność w bramie dostępu zdalnego Ivanti Connect Secure pozwala atakującemu na pominięcie uwierzytelniania poprzez przesłanie odpowiednio spreparowanego zapytania, które umożliwia zdalne wykonanie kodu na instancji. Skutki obejmują przejęcie bramy VPN, potencjalny dostęp do sieci wewnętrznej organizacji oraz kradzież poświadczeń użytkowników łączących się przez urządzenie. Producent informuje o aktywnym wykorzystaniu podatności przez atakujących.

Rekomendujemy: aktualizację do wersji 25.1.1.3, 25.1.3.0 lub 22.8R2.6 albo nowszych, ograniczenie dostępu do interfejsu zarządzania.

Więcej: https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-CVE-2026-104935?language=en_US, https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-104935



Dwie krytyczne podatności w PHP, nazwane php2shell. Luki pozwalają atakującemu na zdalne wykonanie dowolnych poleceń systemowych poprzez błędy w mechanizmie zarządzania pamięcią. Podatne są wszystkie wersje PHP, począwszy od wersji 5.4.

Rekomendujemy zgodnie z zaleceniem producenta aktualizację do wersji 8.5.12, 8.4.27, 8.3.36, 8.2.35.

Więcej: https://www.cve.org/CVERecord?id=CVE-2026-109618, https://www.cve.org/CVERecord?id=CVE-2026-109619, https://www.php.net/archive/2026.php#2026-10-21-5

Wybrane informacje



1 października rozpoczęła się 14. edycja **Europejskiego Miesiąca Cyberbezpieczeństwa** (ang. **European Cybersecurity Month, ECSM**), pod hasłem „Cyberbezpieczeństwo zaczyna się od Ciebie”. ECSM to ogólnoeuropejska kampania edukacyjna poświęcona bezpiecznemu korzystaniu z internetu, którą zainicjowała Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) z inicjatywy Komisji Europejskiej. W ramach kampanii odbywają się konferencje, warsztaty, szkolenia i webinary, które mają zwiększać świadomość cyberzagrożeń oraz promować dobre praktyki. W Polsce działania związane z kampanią ECSM koordynuje NASK – PIB.

Więcej: nask.pl/ECSM 2026: cyberbezpieczeństwo zaczyna się od Ciebie



7–8 października w Warszawie odbyła się 7. edycja konferencji **Cyber24 Days**, która zgromadziła ekspertów ds. cyberbezpieczeństwa oraz przedstawicieli administracji publicznej, biznesu, nauki i służb. NASK – PIB był jednym z partnerów wydarzenia. Uczestnicy konferencji rozmawiali m.in. o odporności Polski na cyberataki. Tej tematyce poświęcono panel „Eskalacja w cyberprzestrzeni. Na ile jesteśmy odporni?", w którym uczestniczył kierownik CERT Polska. W dyskusji na ten temat uwzględniono doświadczenia CERT Polska, w tym związane z incydentem w sektorze energii z grudnia 2025 r.

Więcej: cyberdefence24.pl/Informacje o Cyber24 Days



17 października na stronie cert.pl ukazało się opracowanie pt. **„Komunikacja kryzysowa w cyberbezpieczeństwie. Zasady skutecznej komunikacji podczas incydentu"**. Jest ono skierowane do osób odpowiedzialnych za komunikację, zarządzanie kryzysowe w organizacjach oraz do kadry kierowniczej. Podstawą opracowania są doświadczenia zespołu CERT Polska, zdobyte podczas obsługi tysięcy incydentów, a także aktualne wymogi prawne związane z nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa. W materiale zostały zebrane odpowiedzi na kluczowe pytania: kogo, jak i gdzie informować, co powinien zawierać komunikat, dlaczego komunikacja ma znaczenie i kiedy jest ona obowiązkowa. Są w nim także zawarte najważniejsze informacje na temat dobrych praktyk, ale też najczęstszych błędów w informowaniu o incydentach.

Więcej: cert.pl/Komunikacja kryzysowa w cyberbezpieczeństwie



W dniach 19–20 października w Bydgoszczy odbył się **Szczyt Cyfrowy IGF Polska 2026**, zorganizowany przez Ministerstwo Cyfryzacji we współpracy z NASK – PIB i Instytutem Łączności – Państwowym Instytutem Badawczym (IŁ – PIB). Przedstawiciele administracji publicznej, środowiska naukowego i technologicznego, biznesu oraz organizacji pozarządowych rozmawiali m.in. o przyszłości internetu, a także o tym, jak szybko zmienia się cyfrowy świat dzieci i nastolatków, o wpływie dezinformacji i sztucznej inteligencji na życie obywateli oraz o cyberbezpieczeństwie i cyfrowej suwerenności Europy. IGF Polska to wydarzenie cykliczne stanowiące część międzynarodowej inicjatywy ONZ.

Więcej: nask.pl/Bezpieczny internet zaczyna się od nas. NASK na IGF Polska



29 października w Warszawie odbyła się konferencja **Cyfrowy Samorząd**, która zamknęła ogólnopolski cykl spotkań przedstawicieli Ministerstwa Cyfryzacji, NASK – PIB, COI, CPPC i IŁ – PIB z samorządowcami ze wszystkich województw. Tematyka konferencji była zbieżna z zagadnieniami poruszanymi podczas tych spotkań. Prelegenci mówili o cyberbezpieczeństwie, telekomunikacji, kompetencjach AI w urzędach, o otwartych danych, a także o usługach cyfrowych, Architekturze Informacyjnej Państwa. NASK – PIB był reprezentowany przez ekspertów z CERT Polska, którzy omówili bieżące zagrożenia cyberbezpieczeństwa, zaprezentowali scenariusz ataku ransomware na podstawie technik obserwowanych w atakach m.in. na podmioty publiczne oraz przedstawili narzędzia rozwijane przez CERT Polska, służące do ochrony systemów organizacji przed cyberatakami.

Więcej: gov.pl/Konferencja Cyfrowy Samorząd



30 października podpisano porozumienie pomiędzy **NASK – PIB a Urzędem Komisji Nadzoru Finansowego**. Celem tej współpracy jest wzmocnienie możliwości zespołu **CSIRT KNF**, dbającego o cyberbezpieczeństwo sektora finansowego. Porozumienie pozwoli na wykorzystanie doświadczenia ekspertów z zespołu CERT Polska oraz narzędzi, które zespół tworzy i rozwija, do wspierania CSIRT KNF w monitorowaniu zagrożeń, analizie informacji i reagowaniu na incydenty. Szczególną rolę odegra w tym projekcie serwis moje.cert.pl – w ramach współpracy dostosowano funkcjonalności serwisu do specyfiki sektora finansowego tak, by ułatwić wsparcie poszczególnych instytucji oraz koordynację działań w całym sektorze. Dzięki współpracy zwiększy się bezpieczeństwo nie tylko instytucji finansowych, lecz także osób korzystających z oferowanych przez nie usług.

Więcej: nask.pl/NASK i KNF wzmacniają cyberochronę sektora finansowego

Wystąpienia ekspertów CERT Polska

- 6 października – przedstawienie dwóch prezentacji podczas konferencji SektorForum LIVE! zorganizowanej przez duński CERT: „How to approach looking for vulnerabilities in OT and how that differs from IT” i „Polish Energy Sector Incident – what can we learn?”.

  Więcej: sektorcert.dk/konferencja/informacje

- 6 października – wystąpienie pt. „Cyberodporność JST i ciągłość usług cyfrowych w reżimie NIS 2 i KSC” podczas Samorządowego Forum Kapitału i Finansów w Katowicach.

  Więcej: samorzadoweforum.pl/program
- 7 października – udział w panelu dyskusyjnym pt. „From Intel to Awareness: Building National Cyber Defence at Internet Scale” podczas konferencji zorganizowanej w Dublinie przez Krajowe Centrum Cyberbezpieczeństwa (NCSC) Irlandii.

  Więcej: ncsc-conference.ie/informacje
- 16 października – udział w panelu dyskusyjnym pt. „Czy wciąż boimy się DDoS-ów” oraz wystąpienie z prezentacją pt. „Co CERT łowi w Waszych sieciach” podczas konferencji PLNOG 2026 w Krakowie.

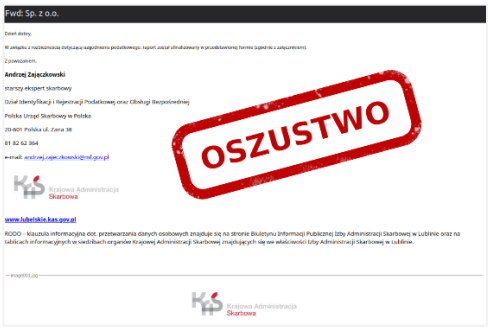
  Więcej: plnog.pl/agenda
- 20 października – prezentacja „moje.cert.pl – Twoje wsparcie w bezpieczeństwie” oraz udział w debacie pt. „SOC: Między algorytmem a literą prawa: Security Operations Center (SOC) na styku technologii, legislacji i suwerenności cyfrowej” podczas Kongresu Cyberbezpieczeństwa CyberTrust 2026 we Wrocławiu.

  Więcej: cybertrust.org.pl/agenda
- 28 października – prezentacja pt. „Cyberbezpieczeństwo przedsiębiorstw – od zagrożeń i regulacji do praktycznego wdrożenia” w ramach wydarzenia Konfederacji Lewiatan.

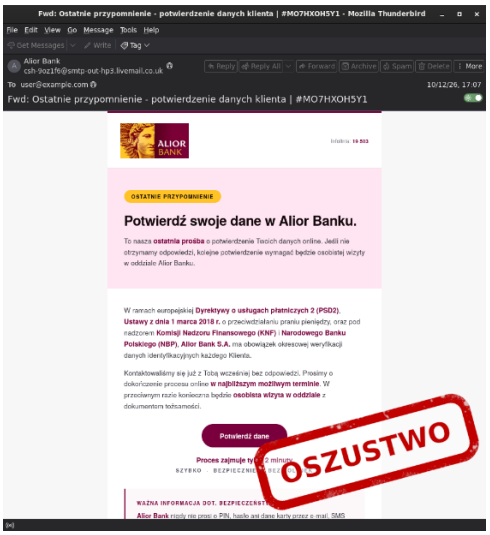
  Więcej: lewiatan.org/spotkanie/informacje

Komunikaty o zagrożeniach

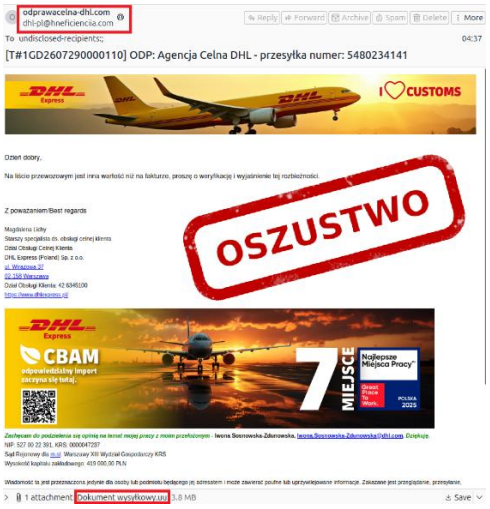
Informacje o zaobserwowanych kampaniach publikowane przez zespół CERT Polska w serwisie moje.cert.pl oraz w serwisach społecznościowych.



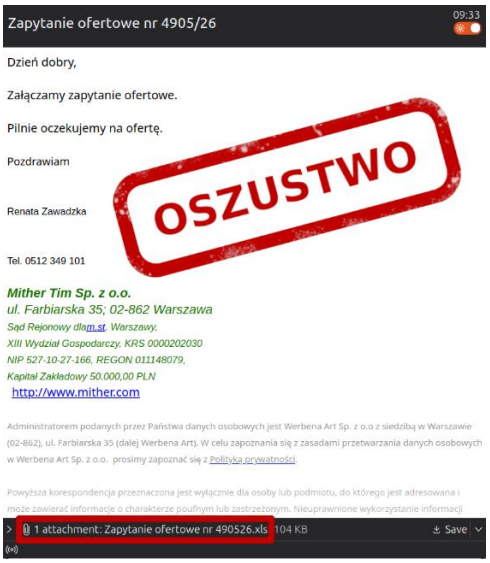
Zespół CERT Polska monitorował powrót kampanii phishingowej, w której oszuści podszywają się pod Krajową Administrację Skarbową. W wysyłanych e-mailach informują o rzekomych rozbieżnościach w rozliczeniu podatkowym. W wiadomości znajduje się załącznik, określany jako raport zawierający informacje o wykrytych rozbieżnościach. Otwarcie pliku przez użytkownika prowadzi do instalacji złośliwego oprogramowania z rodziny Remcos. Umożliwia ono atakującym zdobycie zdalnego dostępu do urządzenia i przejęcie przechowywanych na nim danych.



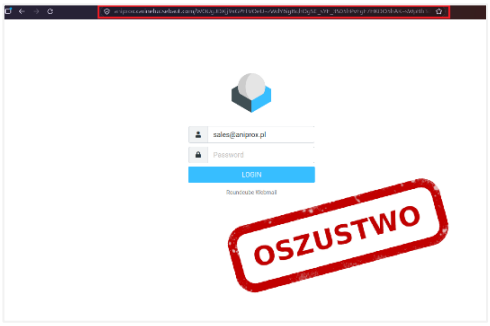
Zespół CERT Polska obserwował kampanię phishingową skierowaną do klientów Alior Banku. Oszuści wysyłają wiadomości e-mail, w których powołują się na regulacje prawne i proszą o pilne potwierdzenie danych identyfikacyjnych klienta. W wiadomości znajduje się przycisk z napisem „Potwierdź dane", który prowadzi do strony phishingowej służącej oszustom do wyłudzania danych logowania do bankowości elektronicznej.



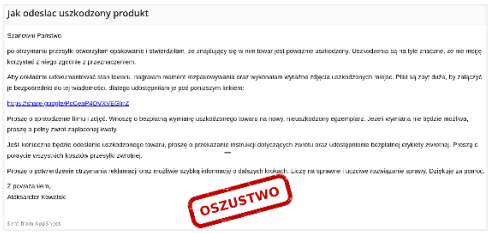
Zespół CERT Polska monitorował kampanię phishingową, którą przestępcy wykorzystują do dystrybucji szkodliwego oprogramowania. Oszuści podszywają się pod znane firmy kurierskie i wysyłają wiadomości e-mail, w których proszą o wyjaśnienie rzekomej niezgodności między listą przewozową a fakturą. Ich celem jest skłonienie odbiorcy do pobrania i otwarcia załącznika. W załączonym pliku znajduje się szkodliwe oprogramowanie MassLogger. Służy ono do kradzieży danych wprowadzanych na urządzeniu za pomocą klawiatury, np. loginów, haseł oraz innych informacji wykorzystywanych do uwierzytelniania.



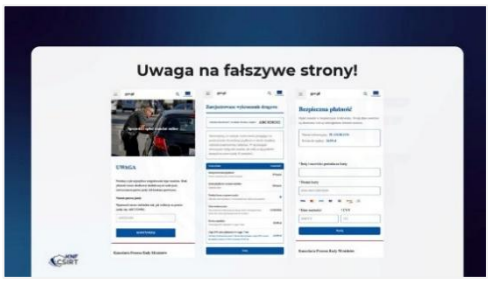
Zespół CERT Polska monitorował kampanię phishingową wymierzoną w przedsiębiorców. Oszuści wysyłają e-maile zawierające pilną prośbę o odpowiedź na zapytanie ofertowe dołączone do wiadomości. Otwarcie pliku z załącznika powoduje instalację szkodliwego oprogramowania z rodziny Remcos, które prowadzi do infekcji komputera i umożliwia atakującym zdalny dostęp do urządzenia. Mogą oni monitorować aktywność użytkownika (np. rejestrować wciskane przyciski, przejąć dostęp do kamery i mikrofonu), wykradać dane czy instalować kolejne rodzaje szkodliwego oprogramowania.



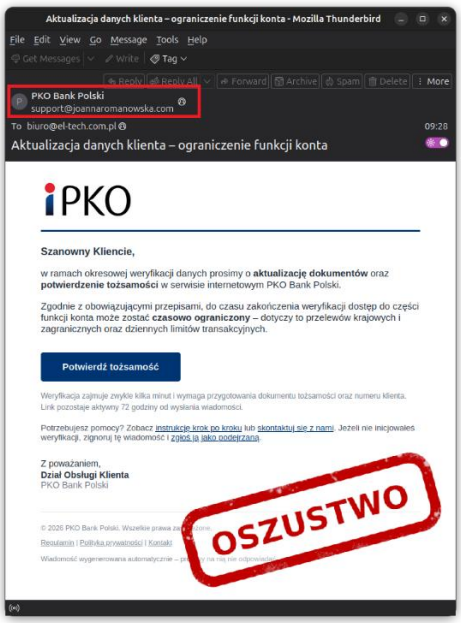
Zespół CERT Polska obserwował kolejną kampanię phishingową, w której oszuści podszywają się pod Krajową Administrację Skarbową. Cyberprzestępcy rozsyłają wiadomości e-mail z informacją o rzekomych rozbieżnościach w danych podatkowych, wykrytych podczas automatycznej weryfikacji pliku JPK_VAT. W treści e-maila znajduje się odnośnik z napisem „Zaloguj się za pomocą swojego e-maila, aby uzyskać dostęp do portalu podatkowego”, który prowadzi na stronę podszywającą się pod panel logowania do poczty elektronicznej.



Zespół CERT Polska obserwował kampanię dystrybucji złośliwego oprogramowania, w której cyberprzestępcy podszywają się pod klientów składających reklamację. Oszuści wysyłają e-maile, które przypominają zgłoszenie od klienta. Informują, że pod linkiem umieszczonym w wiadomości udostępniają plik z nagraniem dokumentującym otwieranie paczki z produktem oraz zdjęcia, na których są przedstawione widoczne na nim uszkodzenia. Z analizy przeprowadzonej przez zespół CERT Polska wynika, że link służy do dystrybucji oprogramowania należącego do rodziny malware Purerat. Tego rodzaju oprogramowanie może być wykorzystane m.in. do uzyskania zdalnego dostępu do zainfekowanego urządzenia i do kradzieży danych. Dane te mogą być wykorzystane przez cyberprzestępców do przeprowadzania kolejnych, bardziej precyzyjnych ataków.



W serwisie moje.cert.pl opublikowano ostrzeżenie CSIRT KNF przed fałszywymi wiadomościami SMS, w których oszuści podszywają się pod Główny Inspektorat Transportu Drogowego. Cyberprzestępcy wysyłają SMS-y z informacją o aktualizacji sprawy dotyczącej przekroczenia prędkości i podają link, pod którym można rzekomo zweryfikować szczegóły. Link prowadzi na fałszywą stronę internetową, na której oszuści nakłaniają do opłacenia rzekomego mandatu. Formularze zawarte na stronie służą do wyłudzenia numeru prawa jazdy oraz danych osobowych i danych karty płatniczej.



Zespół CERT Polska ostrzegał przed kampanią e-mail, w której cyberprzestępcy podszywają się pod bank PKO BP. W wysyłanych wiadomościach proszą klienta o aktualizację dokumentów i potwierdzenie tożsamości w serwisie internetowym banku. Jednocześnie informują, że do czasu zakończenia weryfikacji klient może mieć utrudniony dostęp do niektórych usług – dotyczy to przelewów krajowych i zagranicznych oraz dziennych limitów transakcyjnych. W wiadomości znajduje się przycisk z napisem „Potwierdź tożsamość", który prowadzi do strony podszywającej się pod serwis iPKO. Wyłudzone za jej pośrednictwem dane logowania mogą zostać wykorzystane do przejęcia dostępu do konta bankowego lub do kolejnych prób wyłudzenia danych. W innym wariancie tej kampanii oszuści wykorzystują tematy związane ze zmianami w obsłudze rachunków walutowych, z nowymi zasadami autoryzacji przelewów czy z aktualizacją dokumentacji firmy.

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



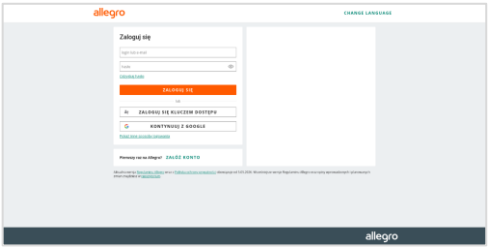
Opis najczęściej występujących kampanii – X 2026

Fałszywe strony oferujące wysokodochodowe inwestycje



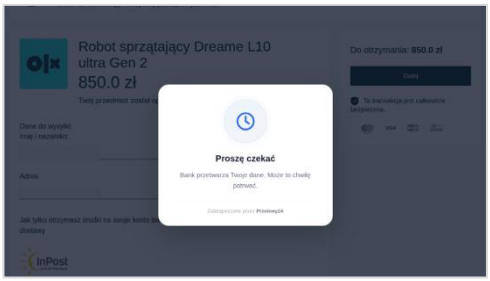
Zespół CERT Polska nadal obserwował wzmożoną kampanię phishingową, w której oszuści podszywają się pod różne koncerny paliwowo-energetyczne, firmy i instytucje, m.in. Lotos, Orlen, Tesla, PGNiG, PGE. Za pośrednictwem reklam w mediach społecznościowych i w serwisach internetowych, a także w rozsyłanych wiadomościach promują fikcyjne platformy inwestycyjne oraz rzekome programy dla akcjonariuszy i obiecują wysokie zyski. 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. Oszuści mogą uwiarygodniać swoje działania niewielkimi wypłatami (środki wykorzystywane w tym celu pochodzą od innych ofiar oszustw), jednak odzyskanie większych kwot jest zazwyczaj niemożliwe.

Fałszywe strony wykorzystujące wizerunek serwisu Allegro



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

Fałszywe strony podszywające się pod serwis OLX



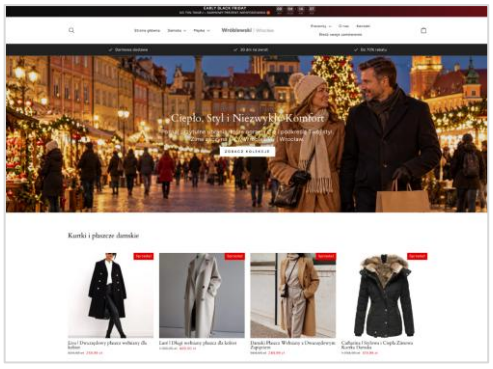
Zespół CERT Polska zarejestrował incydenty, w których atakujący za pośrednictwem stron internetowych podszywają się pod serwis OLX. Strony zawierają fałszywy panel logowania do serwisu lub fałszywy panel płatniczy. Celem oszustów jest wyłudzenie danych uwierzytelniających lub kradzież środków finansowych.

Fałszywe strony wykorzystujące wizerunek serwisu Gazeta.pl



Zespół CERT Polska rejestrował incydenty, w których atakujący za pośrednictwem stron internetowych podszywają się pod serwis Gazeta.pl.
Na spreparowanych stronach oszuści publikują artykuły, w których wykorzystują wizerunki znanych osób do promowania fałszywych platform inwestycyjnych.

Fałszywe sklepy internetowe



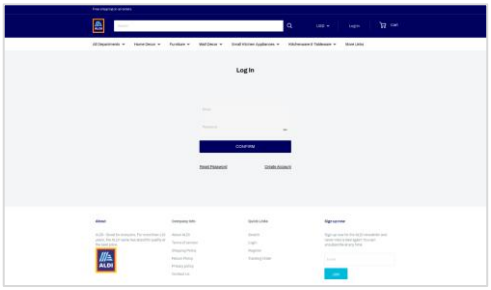
Zespół CERT Polska obserwował incydenty, w których oszuści tworzą fałszywe sklepy internetowe oferujące towary w atrakcyjnych cenach. Strony te służą do wyłudzania danych uwierzytelniających oraz do kradzieży środków finansowych.

Fałszywe strony podszywające się pod serwis Onet.pl



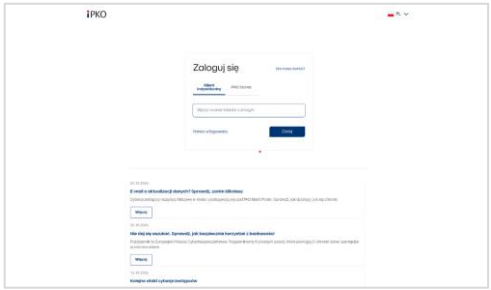
Zespół CERT Polska obserwował kampanię phishingową, w której oszuści podszywają się pod serwis Onet.pl i umieszczają na fałszywych stronach internetowych artykuły służące do reklamowania nieistniejących programów inwestycyjnych. Celem oszustów jest wyłudzenie środków finansowych.

Fałszywe strony wykorzystujące wizerunek marki ALDI



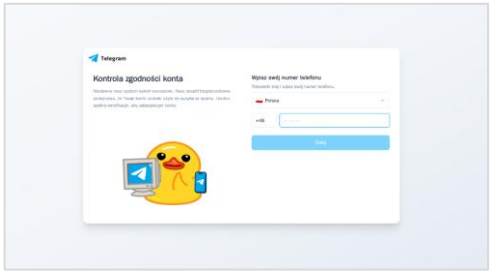
Zespół CERT Polska rejestrował incydenty, w których oszuści tworzą fałszywe sklepy internetowe z wykorzystaniem wizerunku sieci sklepów ALDI. Celem oszustów jest wyłudzenie od użytkowników danych uwierzytelniających oraz kradzież środków finansowych.

Fałszywe strony podszywające się pod PKO BP



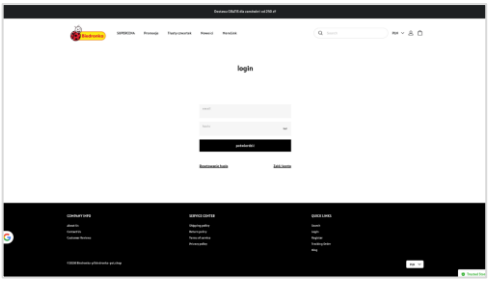
Zespół CERT Polska obserwował kampanię phishingową, w której oszuści wykorzystują wizerunek banku PKO BP. Celem oszustów jest pozyskanie danych uwierzytelniających do konta bankowego, a następnie kradzież środków finansowych.

Fałszywe strony podszywające się pod komunikator Telegram



Zespół CERT Polska obserwował kampanię mającą na celu przejmowanie kont użytkowników komunikatora Telegram. Oszuści wysyłają wiadomości SMS z informacją, że konto użytkownika mogło brać udział w wysyłce spamu i aby je zabezpieczyć, użytkownik ma przeprowadzić szybką weryfikację. Link zawarty w wiadomości prowadzi do strony internetowej, która służy do wyłudzenia numeru telefonu. Następnie użytkownik jest proszony o wpisanie kodu weryfikacyjnego wysłanego na jego numer telefonu. Podanie tego kodu umożliwia atakującym przejęcie konta Telegram poprzez sparowanie własnego urządzenia z kontem ofiary.

Fałszywe strony wykorzystujące wizerunek sieci sklepów Biedronka



Zespół CERT Polska obserwował strony internetowe wykorzystujące wizerunek sieci sklepów Biedronka. Na spreparowanych stronach znajduje się panel logowania do sklepu internetowego biedronka.pl. Celem oszustów jest pozyskanie od użytkowników danych uwierzytelniających.