MARZEC 2026

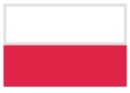
Podsumowanie Miesiąca CERT POLSKA

Nr 3/2026

30 LAT | 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

SPIS TREŚCI

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 marca 2026 r.
Dla lepszego zobrazowania pojawiających się trendów niektóre z tych danych pokazywane są w dłuższej perspektywie czasu.

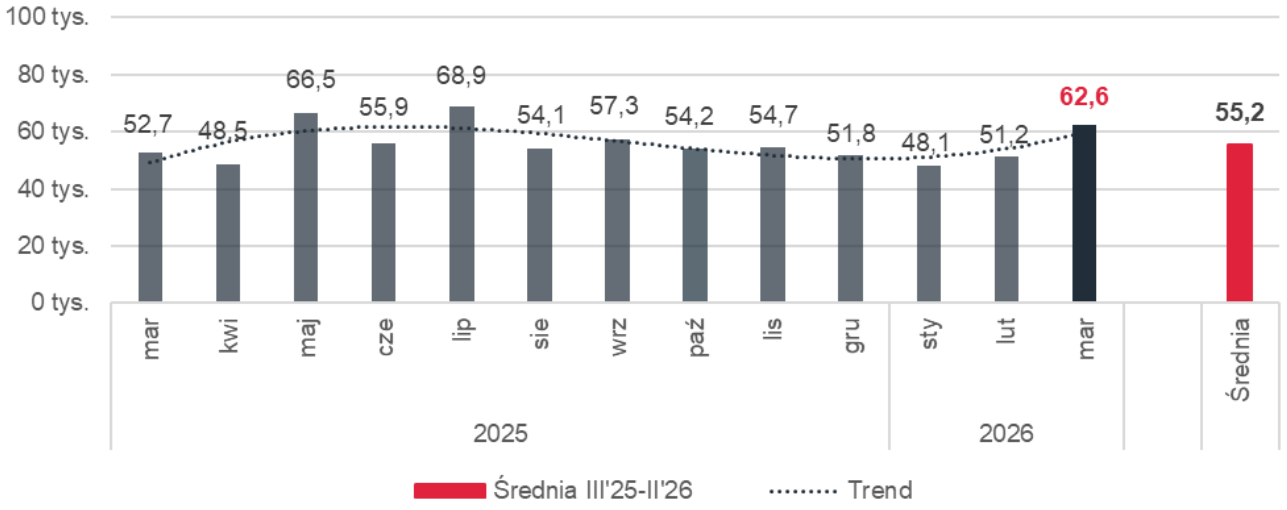
Zarejestrowane zgłoszenia i incydenty cyberbezpieczeństwa – III 2026

Tabela 1. Liczba zarejestrowanych zgłoszeń i incydentów od 1 do 31 marca 2026 r.

Zagrożenia cyberbezpieczeństwa	Liczba
Zarejestrowane zgłoszenia	**62,6 tys.**
w tym zarejestrowane (obsłużone) incydenty	**31,0 tys.**

W marcu 2026 r. zespół CERT Polska otrzymał łącznie **62,6 tys.** zgłoszeń, które zostały przeanalizowane i pogrupowane. Na ich podstawie zarejestrowano **31,0 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 III 2025 do III 2026

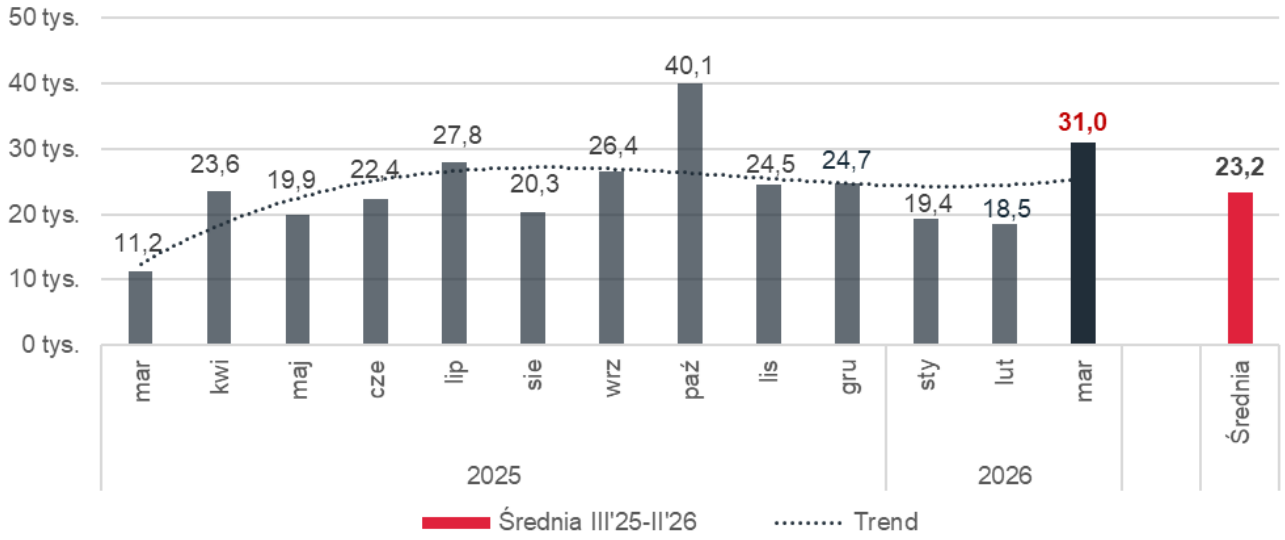


Wykres 1. Liczba zarejestrowanych zgłoszeń od 01.03.2025 do 31.03.2026. Źródło: CERT Polska / CSIRT NASK.

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

Liczba zgłoszeń odnotowanych w marcu 2026 r. przekroczyła średnią liczoną z poprzednich 12 miesięcy. W porównaniu z analogicznym miesiącem 2025 r. liczba ta **zwiększyła się o 19%**. W stosunku do lutego 2026 r. był to **wzrost o 22%**.

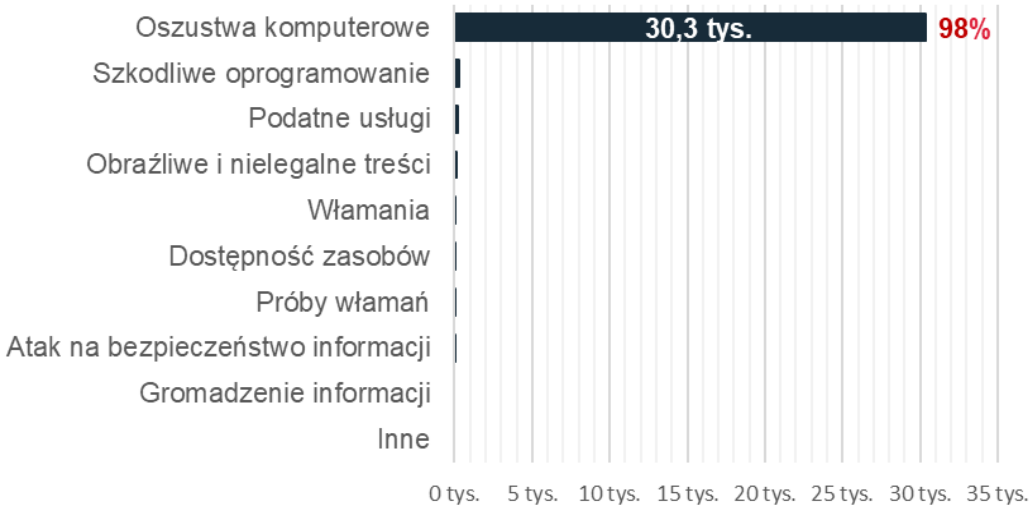
Zarejestrowane incydenty cyberbezpieczeństwa od III 2025 do III 2026



Wykres 2. Liczba zarejestrowanych incydentów od 01.03.2025 do 31.03.2026. Źródło: CERT Polska / CSIRT NASK.

Liczba incydentów zarejestrowanych w marcu 2026 r. wyniosła **31,0 tys.** W porównaniu z analogicznym miesiącem 2025 r. liczba incydentów w marcu 2026 r. **zwiększyła się o 178%** i przekroczyła średnią liczoną z 12 poprzednich miesięcy. W stosunku do lutego 2026 r. liczba zarejestrowanych incydentów **zwiększyła się o 68%**.

Rodzaje zarejestrowanych zagrożeń – III 2026



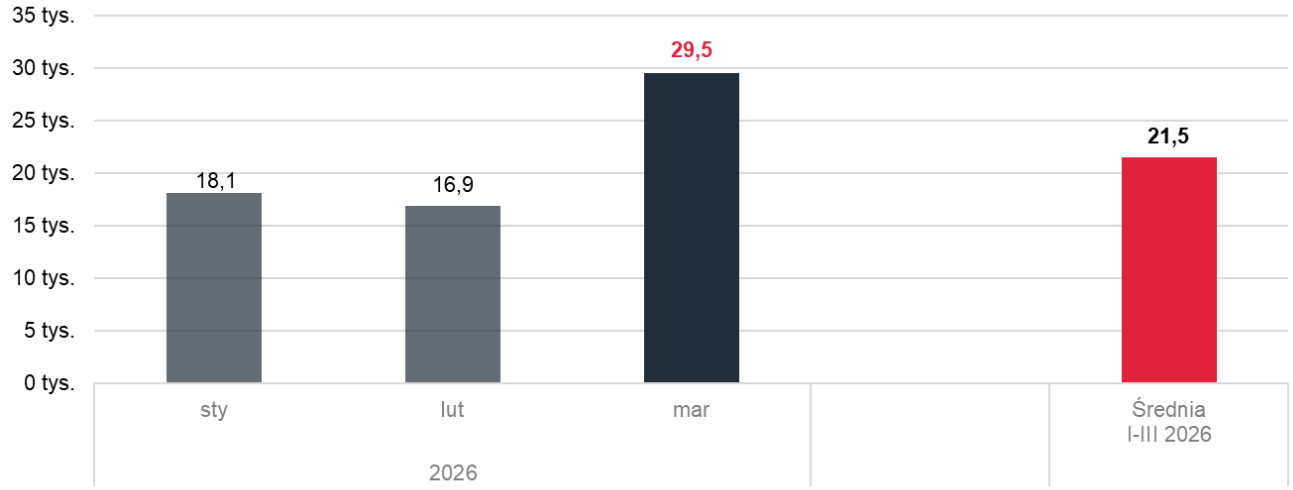
Wykres 3. Liczba zarejestrowanych incydentów według rodzaju od 1 do 31 marca 2026 r. Źródło: CERT Polska / CSIRT NASK.

W analizowanym okresie zdecydowanie najczęściej występującą kategorią zagrożeń były oszustwa komputerowe. Wśród ogółu obsłużonych incydentów (**31,0 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 marcu 2026 r. łącznie odnotowano **14,4 tys.** tego typu incydentów.

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

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

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

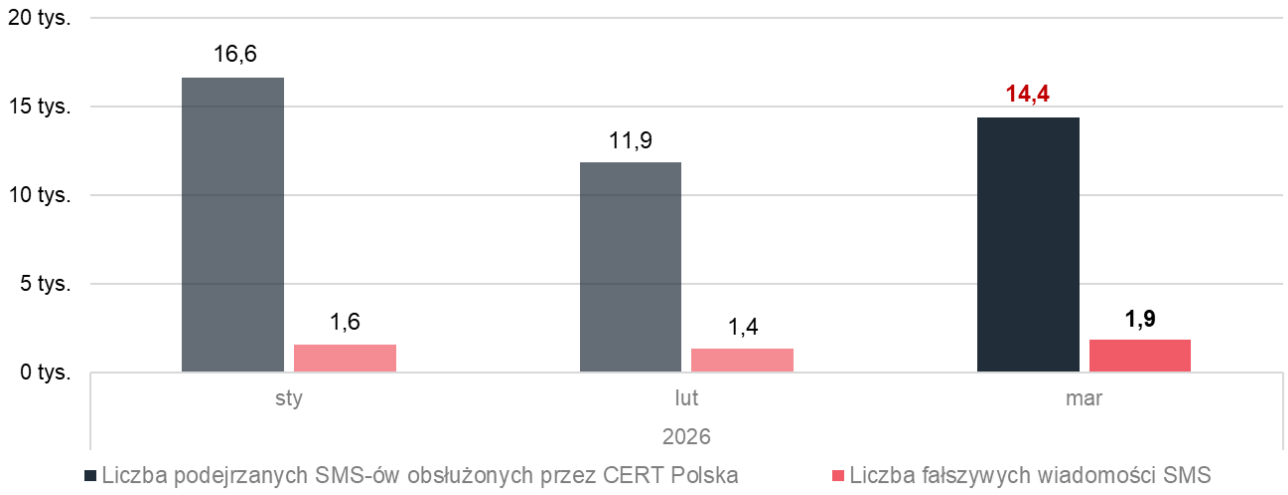


Wykres 4. Liczba nazw szkodliwych domen wpisanych na Listę Ostrzeżeń. Źródło: CERT Polska / CSIRT NASK.

Od 1 stycznia do 31 marca 2026 r. na Listę Ostrzeżeń przed niebezpiecznymi stronami wpisano **64,5 tys.** szkodliwych domen, z czego w marcu 2026 r. dodano **29,5 tys.** nazw domen wykorzystywanych do wyłudzania danych osobowych, danych uwierzytelniających do kont bankowych i serwisów społecznościowych. Wartość ta w stosunku do lutego 2026 r. **zwiększyła się o 75%**.

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

Od 1 stycznia do 31 marca 2026 r. zespół CERT Polska zarejestrował **42,9 tys.** zgłoszeń podejrzanych SMS-ów. Liczba SMS-ów otrzymanych w marcu 2026 r. wyniosła **14,4 tys.** W porównaniu z lutym 2026 r. był to **wzrost o 21%**. Wśród ogółu SMS-ów przyjętych w marcu 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 13%**.



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

Wzorce fałszywych wiadomości SMS I–III 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 marcu 2026 r., na podstawie wytworzonych przez CERT Polska wzorców fałszywych wiadomości SMS, zablokowano łącznie **75,9 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.

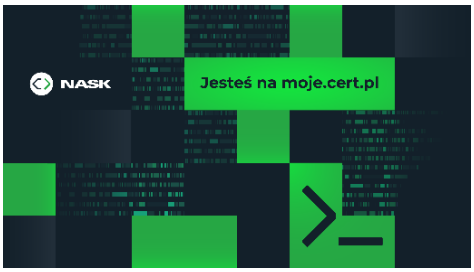
Wzorce fałszywych wiadomości SMS w 2026	sty	lut	mar	Razem
Liczba wytworzonych wzorców	118	97	**85**	**300**

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

Moje.cert.pl

W 2025 r. zespół CERT Polska udostępnił bezpłatny serwis moje.cert.pl. Z serwisu mogą korzystać zarówno osoby prywatne posiadające stronę internetową, jak i małe firmy czy duże instytucje publiczne udostępniające wiele skomplikowanych systemów. Zarejestrowany użytkownik moje.cert.pl może zamówić bezpłatne skanowanie bezpieczeństwa wszystkich swoich domen, uzyskać informacje na temat wycieków haseł użytkowników w swojej domenie, otrzymywać informacje o infekcjach szkodliwym oprogramowaniem i innych zagrożeniach w swoich sieciach (ta funkcja jest dostępna dla administratorów serwerów i sieci), a także sprawdzić, czy dana sieć jest chroniona przez Listę Ostrzeżeń przed niebezpiecznymi stronami. Ponadto w serwisie, w zakładce „Komunikaty" pojawiają się – i będą na bieżąco dodawane – ostrzeżenia dotyczące polskiej cyberprzestrzeni oraz alerty o podatnościach. Komunikaty te są dostępne na stronie także dla niezarejestrowanych użytkowników, a od sierpnia 2025 r. każdy może otrzymywać je również w wiadomości e-mail. Moje.cert.pl korzysta m.in. z systemów **Artemis** (skanowanie stron) i **n6** (informacje o zagrożeniach dla adresacji IP) – narzędzi pozwalających chronić dane i infrastrukturę.

W marcu 2026 r. w serwisie moje.cert.pl **zarejestrowało się 1,2 tys. nowych użytkowników**.



W okresie od 1 do 31 marca 2026 r. CERT Polska wysłał **4,5 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

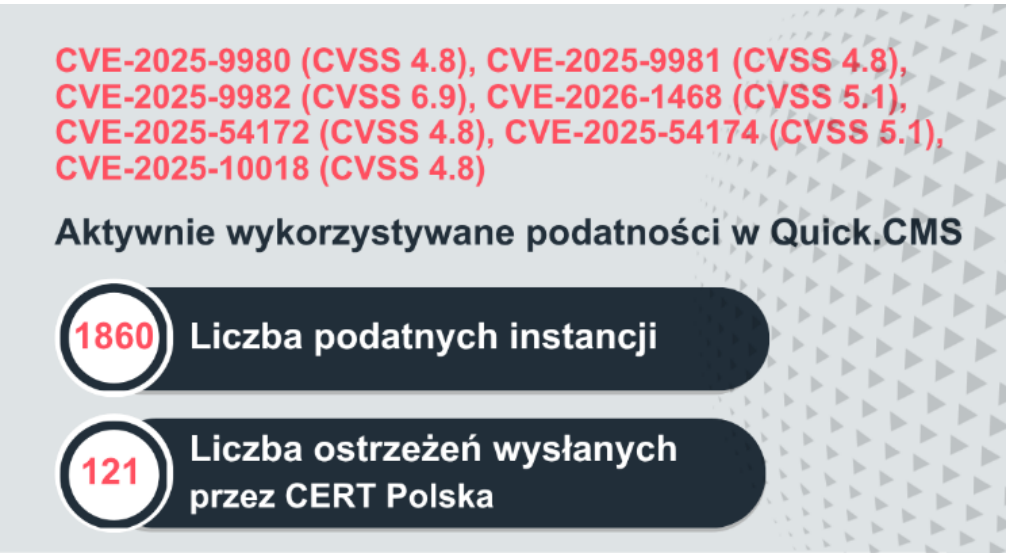
Zespół CERT Polska od sierpnia 2023 r. pełni funkcję CNA (ang. *CVE Numbering Authority*) – współtworzy bazę podatności poprzez nadawanie numerów CVE, które służą do identyfikacji i katalogowania publicznie ujawnionych podatności (więcej: CERT Polska/CNA). W marcu 2026 r. zespół CERT Polska nadał **32** numery CVE. Wśród wykrytych podatności znalazły się podatności w oprogramowaniu m.in. Bludit, CGM CLININET i CGM NETRAAD, DobryCMS oraz Raytha.

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

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

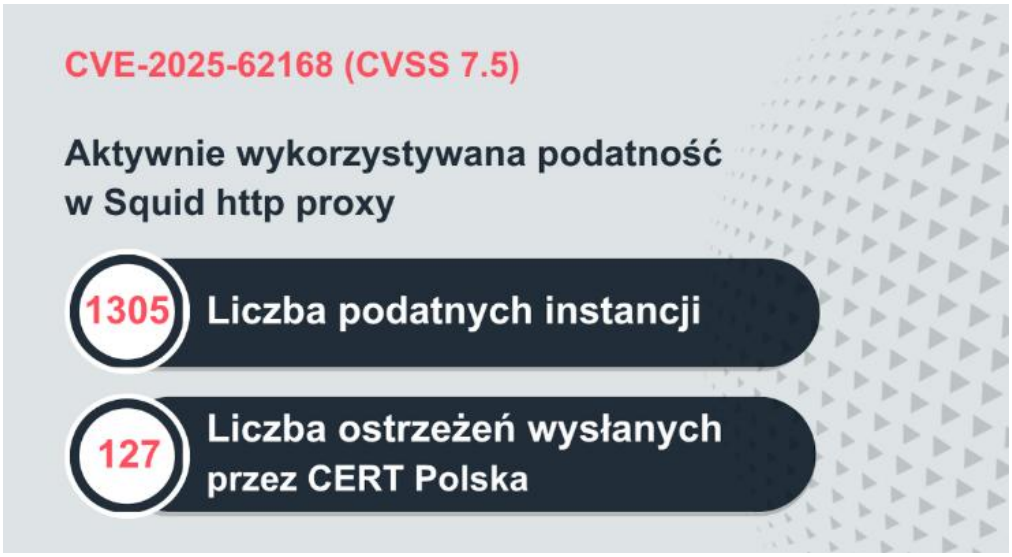
Numery CVE w 2026	sty	lut	mar	Razem
Liczba opublikowanych numerów CVE	16	12	**32**	**60**

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



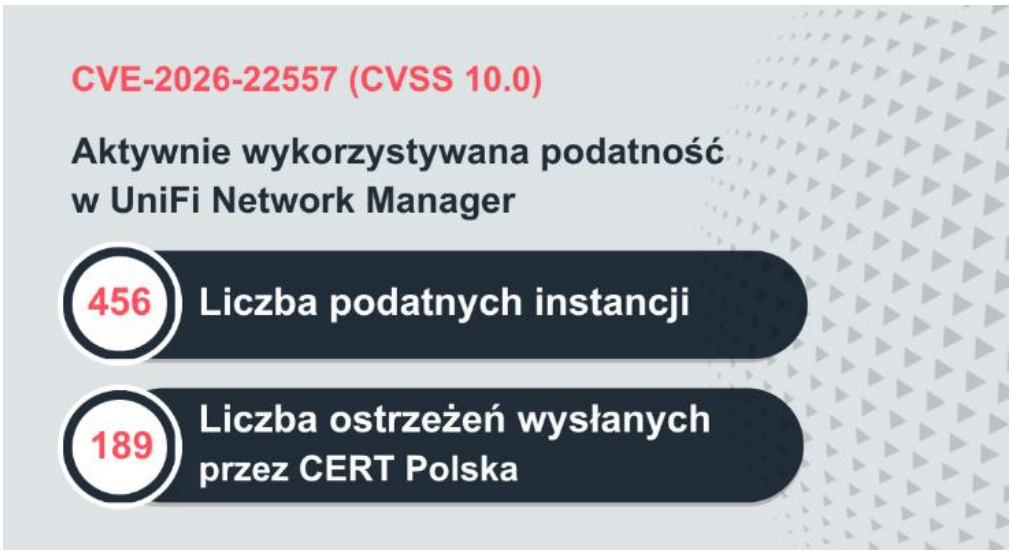
W oprogramowaniu Quick.CMS wykryto wiele podatności, które mogą ułatwiać nieautoryzowane modyfikacje treści, wstrzyknięcie złośliwego kodu lub przejęcie kontroli nad instancją, zwłaszcza jeśli zostaną połączone z innymi technikami ataku.

Więcej: https://access.redhat.com/security/cve/cve-2025-9980, https://access.redhat.com/security/cve/cve-2025-9981, https://access.redhat.com/security/cve/cve-2025-9982, https://access.redhat.com/security/cve/cve-2025-10018, https://access.redhat.com/security/cve/cve-2025-54172, https://www.cvedetails.com/cve/CVE-2025-54174, https://www.sentinelone.com/vulnerability-database/cve-2026-1468



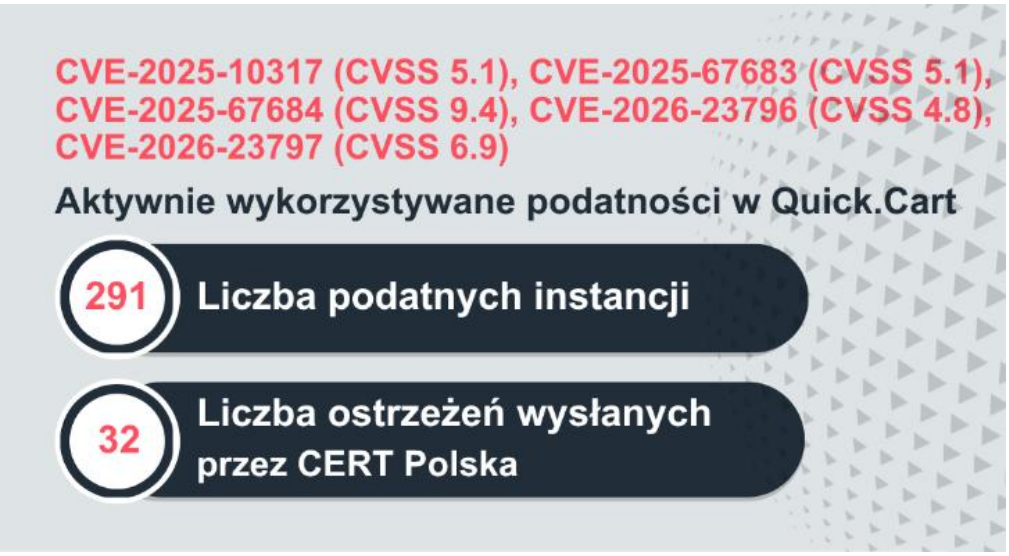
Podatność CVE-2025-62168 w Squid http proxy umożliwia wykorzystanie włączonej funkcjonalności email_err_data do przechwycenia danych wrażliwych, w tym tokenów autoryzacyjnych. Podatność może być wykorzystywana zdalnie.

Więcej: https://github.com/squid-cache/squid/security/advisories/GHSA-c8cc-phh7-xmxr



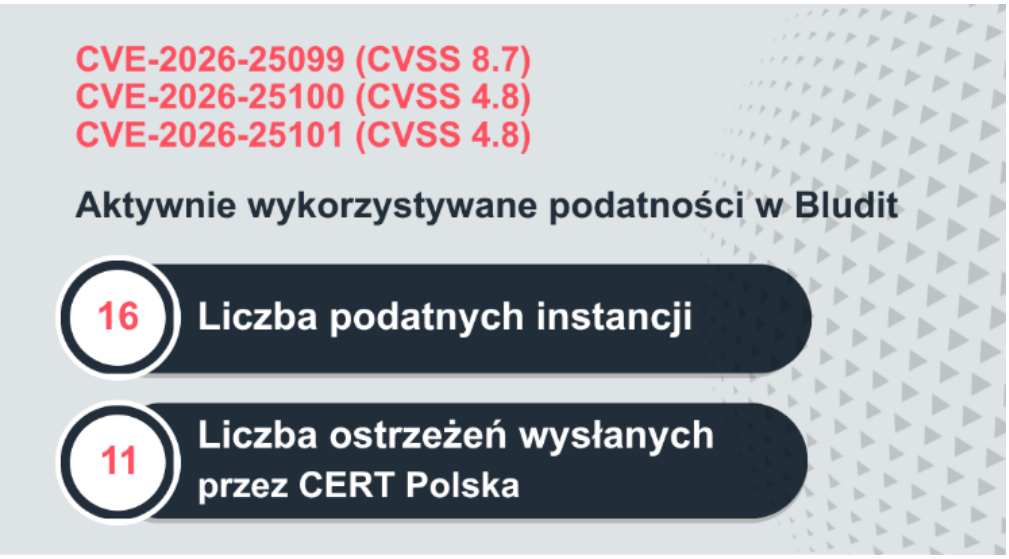
Podatność CVE-2026-22557 zidentyfikowana w aplikacji UniFi Network może umożliwiać zdalnemu atakującemu odczyt plików znajdujących się w systemie bez konieczności uwierzytelniania. Oznacza to, że atakujący może uzyskać dostęp do plików zawierających wrażliwe dane konfiguracyjne lub informacje umożliwiające dalsze ataki. Skuteczne wykorzystanie podatności może w konsekwencji prowadzić do pełnego przejęcia urządzenia.

Więcej: https://community.ui.com/releases/Security-Advisory-Bulletin-062-062/c29719c0-405e-4d4a-8f26-e343e99f931b



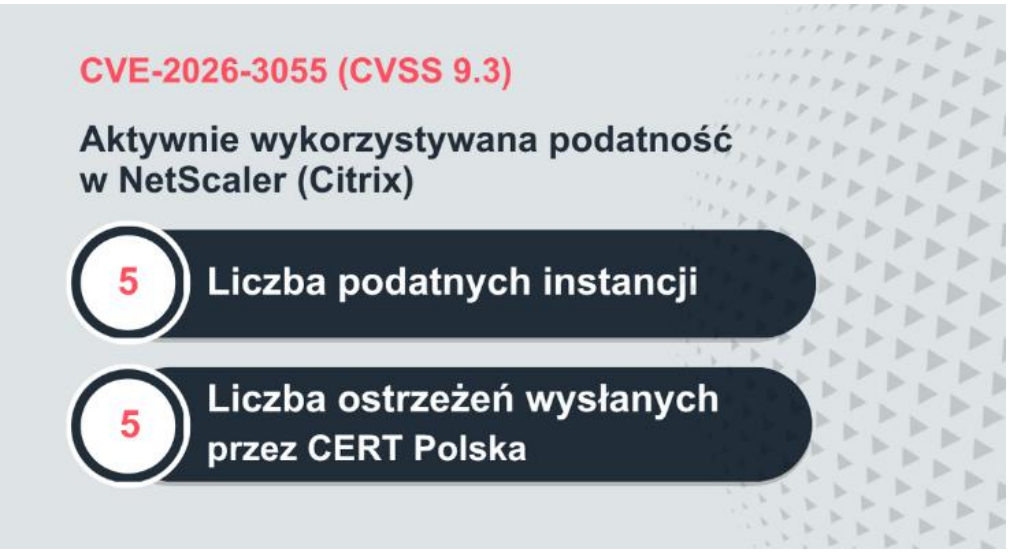
Zidentyfikowano wiele podatności w instancjach wykorzystujących framework Quick.Cart na stronach internetowych. Wykryte podatności, choć często wymagają uprawnień administratora, nadal stanowią realne zagrożenie, ponieważ mogą ułatwiać nieautoryzowane modyfikacje treści, wstrzyknięcie złośliwego kodu lub przejęcie kontroli nad instancją, zwłaszcza jeśli zostaną połączone z innymi technikami ataku.

Więcej: https://nvd.nist.gov/vuln/detail/CVE-2025-10317, https://access.redhat.com/security/cve/cve-2025-67683, https://www.sentinelone.com/vulnerability-database/cve-2025-67684, https://www.sentinelone.com/vulnerability-database/cve-2026-23796, https://www.sentinelone.com/vulnerability-database/cve-2026-23797



W oprogramowaniu Bludit zidentyfikowano wiele podatności, które są wykorzystywane na stronach internetowych. Umożliwiają one zdalne wykonywanie kodu przez uwierzytelnionego użytkownika, ustawienie identyfikatora sesji przed uwierzytelnieniem, co może prowadzić do przejęcia sesji oraz umieszczania szkodliwego kodu na serwerze.

Więcej: https://nvd.nist.gov/vuln/detail/CVE-2026-25099, https://nvd.nist.gov/vuln/detail/cve-2026-25100, https://nvd.nist.gov/vuln/detail/CVE-2026-25101



W oprogramowaniu NetScaler ADC (wcześniej Citrix ADC) oraz NetScaler Gateway (wcześniej Citrix Gateway) zidentyfikowano podatność oznaczoną jako CVE-2026-3055, która pozwala nieuwierzytelnionym atakującym na odczyt dowolnych obszarów pamięci. Może to prowadzić do ujawnienia informacji kluczowych dla bezpieczeństwa aplikacji i do przejęcia kontroli nad urządzeniem. Podatność dotyczy tylko urządzeń wykorzystujących uwierzytelnianie SAML IDP.

Więcej: https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696300

Wybrane informacje

11 marca **zespół CERT Polska, pierwszy w Polsce zespół reagowania na zagrożenia w sieci, rozpoczął świętowanie 30-lecia swojej działalności**. Z tej okazji zorganizowano w Ministerstwie Cyfryzacji konferencję prasową, podczas której o działaniach zespołu oraz o zmianach w krajobrazie cyberbezpieczeństwa w Polsce mówili wicepremier i minister cyfryzacji, dyrektor NASK-PIB oraz kierownik CERT Polska. Z okazji jubileuszu zespół CERT Polska publikował w mediach społecznościowych materiały, w których przypominał najważniejsze momenty swojej historii oraz prezentował projekty, narzędzia i inicjatywy realnie wpływające na bezpieczeństwo polskiego internetu. W postach znalazły się m.in. informacje na temat Listy Ostrzeżeń, projektów Artemis, moje.cert.pl, n6, MWBD oraz o roli CERT Polska w skoordynowanym ujawnianiu podatności.

Więcej: nask.pl/Cyberbezpiecznie od 30 lat. CERT Polska, facebook.com/#30latcertpolska

4 marca opublikowano informację o **międzynarodowej operacji koordynowanej przez Europol, wymierzonej w kampanię phishingową o nazwie „Tycoon 2FA”**. Eksperci z NASK-PIB i CERT Polska prowadzili działania we współpracy z funkcjonariuszami Zarządu w Rzeszowie Centralnego Biura Zwalczania Cyberprzestępczości. Na podstawie szczegółowych analiz zablokowano 120 polskich domen, które były powiązane z działalnością przestępczą realizowaną w ramach platformy Tycoon 2FA – narzędzia, które służyło cyberprzestępcom do przechwytywania informacji i danych wrażliwych podczas logowania użytkowników do kont pocztowych.

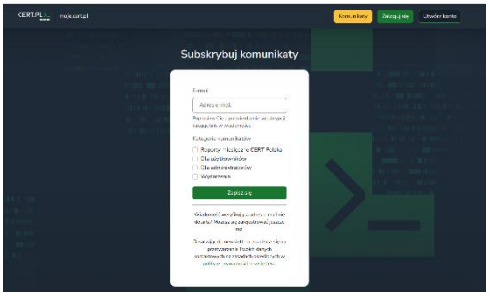
Więcej: cbzc.policja.gov.pl/120 polskich domen powiązanych z przestępczą platformą Tycoon 2FA zablokowanych

---

10 marca **zespół CERT Polska opublikował rekomendacje związane z atakami wymierzonymi w usługi chmurowe**. Atakujący uzyskują dostęp do kont administratorów między innymi za pomocą kampanii phishingowych i szkodliwego oprogramowania, a następnie wykorzystują wykupione licencje i usługi do swoich działań.

Więcej: moje.cert.pl/Rekomendacje związane z atakami wymierzonymi w usługi chmurowe

---



20 marca zespół CERT Polska poinformował o wprowadzeniu w serwisie **moje.cert.pl nowej kategorii komunikatu – „Wydarzenia”**. Ta część serwisu będzie zawierała rekomendacje zespołu CERT Polska dotyczące spotkań, szkoleń oraz konferencji związanych z cyberbezpieczeństwem. Aby zapisać się do subskrypcji komunikatów w kategorii „Wydarzenia”, należy skorzystać z ustawień konta w serwisie. Niezalogowani użytkownicy mogą użyć spersonalizowanego linku otrzymanego przy pierwszym zapisie do newslettera lub ponownie zgłosić się na stronie moje.cert.pl/komunikaty/subskrybuj.

Więcej: moje.cert.pl/Nowa funkcjonalność

23 marca **w Monitorze Polskim została opublikowana Uchwała nr 92 Rady Ministrów z dnia 10 marca 2026 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej**. Dokument wyznacza kierunki działań państwa do 2029 r. dotyczące wzmocnienia bezpieczeństwa systemów informatycznych, a także wskazuje obszary oraz działania służące rozwojowi krajowego systemu cyberbezpieczeństwa (KSC). Realizacja strategii ma zwiększyć odporność Polski na cyberzagrożenia oraz poprawić bezpieczeństwo obywateli, przedsiębiorstw i instytucji publicznych. Uchwała weszła w życie 24 marca 2026 r.

Więcej: gov.pl/Uchwała w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, monitorpolski.gov.pl/MP/2026/309

30 marca na stronie cert.pl ukazała się **„Analiza kampanii FvncBot”**. Zespół CERT Polska przeanalizował nowe próbki powiązane z kampanią FvncBot wymierzoną w polskich użytkowników internetu. W artykule opisano wariant kampanii wykorzystujący wizerunek Spółdzielczej Grupy Bankowej. Wieloetapowy łańcuch infekcji opiera się na socjotechnice – aplikacja najpierw wykorzystuje wizerunek znanego banku, a potem podszywa się pod prompty systemowe, aby zwiększyć wiarygodność i nakłonić użytkownika do instalacji. Kluczowym elementem ataku jest nadużycie uprawnień funkcji ułatwień dostępu umożliwiające przejęcie kontroli nad urządzeniem i wykonywanie operacji w imieniu użytkownika.

Więcej: cert.pl/Analiza kampanii FvncBot

30 marca ukazał się artykuł pt. **„CERT Polska i policja. Wspólny front przeciw cyberprzestępcom**”, w którym podsumowano cykl szkoleń prowadzonych przez ekspertów z zespołu CERT Polska w ramach projektu CROPT. Funkcjonariusze Centralnego Biura Zwalczania Cyberprzestępczości uczyli się, jak prowadzić proces analizy śledczej oraz jak zabezpieczać dane i sprzęt po ataku ransomware. Projekt CROPT koncentruje się na wzmacnianiu zdolności operacyjnych policji w zakresie zwalczania cyberprzestępczości m.in. poprzez szkolenia budujące praktyczne kompetencje techniczne.

Więcej: nask.pl/CERT Polska i policja. Wspólny front przeciw cyberprzestępcom

Wystąpienia ekspertów CERT Polska

- 11 marca – udział w panelu „Reagowanie na incydenty cybernetyczne” w Ambasadzie Kanady. Była to część spotkania „Cyberbezpieczny samorząd – jak się skutecznie obronić?” organizowanego przez Mazowiecką Wspólnotę Samorządową.

  Więcej: facebook.com/Mazowiecka Wspólnota Samorządowa
- 16 marca – prowadzenie prelekcji pt. „Krajobraz bezpieczeństwa polskiego internetu według CERT Polska” podczas konferencji SEMAFOR.

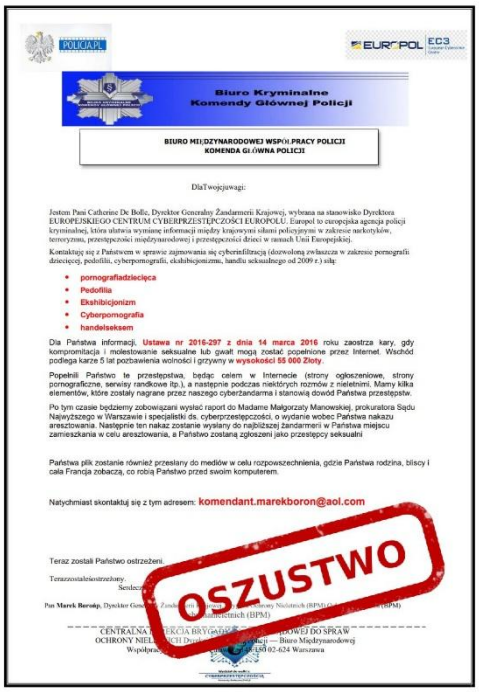
  Więcej: semaforkonferencja.pl/program
- 19 marca – wystąpienie pt. „Incydenty w cyberprzestrzeni. Krajobraz zagrożeń widziany z perspektywy CERT Polska” na konferencji CyberShield w Bydgoszczy.

  Więcej: bppt.pl/Konferencja CyberShield/agenda
- 25 marca – wystąpienie pt. „Reagowanie na incydenty cyberbezpieczeństwa w infrastrukturze krytycznej z perspektywy CSIRT-u” podczas Konferencji Informatyków Wodociągowych Polski Wschodniej w Lublinie.

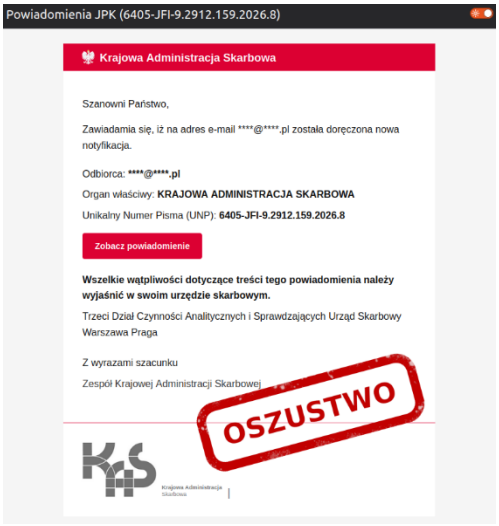
  Więcej: mpwik.lublin.pl/prezentacje z konferencji

Komunikaty o zagrożeniach

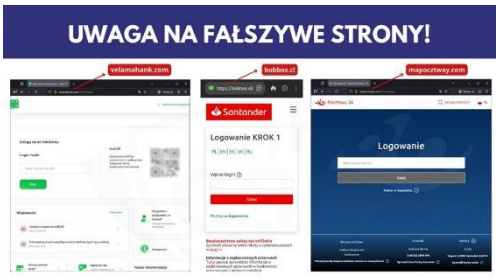
Informacje o zaobserwowanych kampaniach publikowane przez zespół CERT Polska w serwisie moje.cert.pl oraz w serwisach społecznościowych.



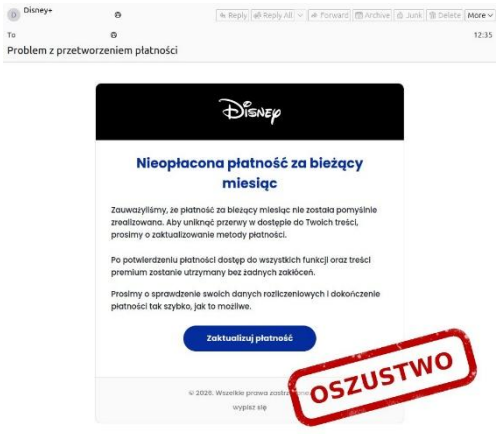
Zespół CERT Polska obserwował kampanię oszustw, w której cyberprzestępcy podszywają się pod organy ścigania (Policję oraz Europol) i grożą odpowiedzialnością karną za rzekome przestępstwa internetowe. Do wiadomości dołączany jest plik w formacie .pdf lub .jpg, który zawiera m.in. wezwanie do kontaktu pod wskazanym adresem mailowym. Celem jest wyłudzenie danych osobowych i pieniędzy. Oszuści wykorzystują autorytet instytucji, na które się powołują, żeby nakłonić potencjalną ofiarę np. do przesłania skanu dowodu osobistego. Często też namawiają do przekazania zdalnego dostępu do komputera, wykonania płatności czy spotkania w celu przekazania pieniędzy.



Zespół CERT Polska informował o kampanii phishingowej, w której oszuści podszywają się pod Krajową Administrację Skarbową (KAS). Wysyłają oni wiadomości, w których zawiadamiają odbiorcę o rzekomej nowej notyfikacji i umieszczają link prowadzący do strony zawierającej fałszywy formularz logowania do profilu zaufanego. Cyberprzestępcy próbują w ten sposób wyłudzić dane logowania do serwisu. Zespół CERT Polska przypomniał użytkownikom, że zanim podadzą swoje dane, powinni: sprawdzić adres nadawcy wiadomości, samodzielnie wyszukać prawdziwy adres strony internetowej tego podmiotu i zweryfikować, czy link z wiadomości na pewno prowadzi właśnie tam, a w przypadku jakichkolwiek wątpliwości skontaktować się z instytucją, która rzekomo wysłała wiadomość.

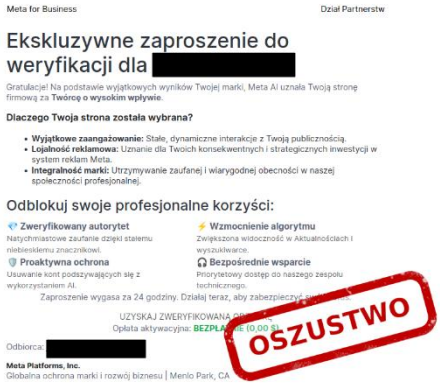


W serwisie moje.cert.pl opublikowano ostrzeżenie CSIRT KNF przed fałszywymi stronami bankowości elektronicznej. Oszuści przygotowali kampanie phishingowe, w których podszywają się pod VeloBank, Santander Bank Polska oraz Bank Pocztowy. Fałszywe strony służą do wyłudzania danych logowania do bankowości elektronicznej. Dane przesłane za pomocą takiej witryny trafiają bezpośrednio do przestępców. Dzięki temu mogą oni przejąć dostęp do konta, a w konsekwencji także zgromadzone na nim środki.

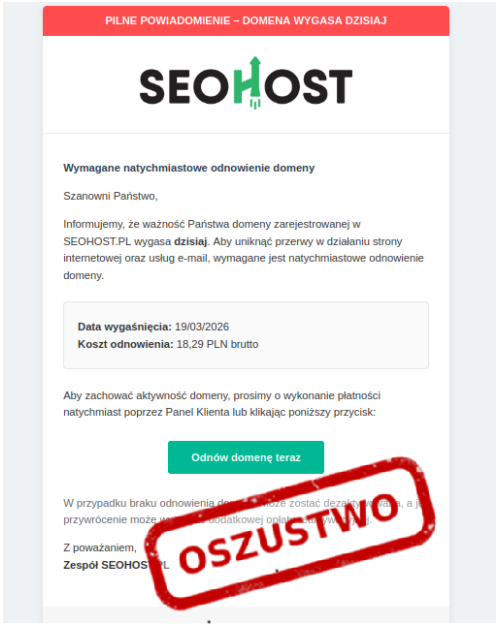


Zespół CERT Polska ostrzegał przed kampanią phishingową, w której oszuści podszywają się pod serwisy streamingowe, m.in. Disney+. Oszuści wykorzystują dwa scenariusze. W pierwszym wysyłają wiadomości, w których informują użytkownika o aktywacji abonamentu i naliczeniu opłaty oraz o możliwości anulowania usługi. Drugi scenariusz obejmuje informację o problemie z płatnością i prośbę o uaktualnienie danych oraz dokończenie płatności. Linki zawarte w wiadomościach prowadzą do stron podszywających się pod serwis streamingowy. Celem oszustów jest wyłudzenie danych logowania i danych płatności.

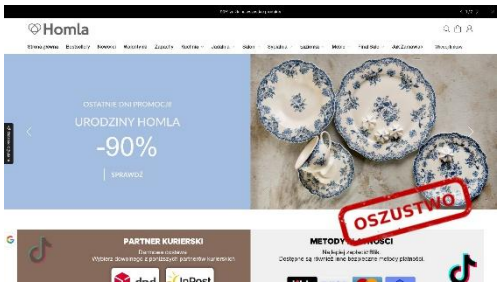
Zespół CERT Polska otrzymywał zgłoszenia dotyczące wiadomości e-mail informujących o rzekomym problemie z doręczeniem przesyłki przez Pocztę Polską. Aby możliwe było dokończenie dostawy, użytkownik jest proszony o uiszczenie opłaty celnej i aktualizację danych wysyłkowych. W treści wiadomości znajduje się odnośnik prowadzący do strony internetowej podszywającej się pod oficjalny serwis Poczty Polskiej. Tam znajduje się formularz, który służy oszustom do wyłudzania danych karty płatniczej użytkownika. Dobrym nawykiem przed podaniem swoich danych jest sprawdzanie adresu strony internetowej oraz weryfikacja informacji o przesyłce bezpośrednio w oficjalnym serwisie operatora lub aplikacji do śledzenia paczek.



Zespół CERT Polska monitorował kampanię phishingową, w której oszuści wykorzystują wizerunek firmy Meta. Komunikaty kierowane są głównie do osób prowadzących strony firmowe lub profile biznesowe w mediach społecznościowych. Wiadomość zawiera informację o rzekomej możliwości odblokowania nowych funkcji lub korzyści dla strony. Aby z nich skorzystać, użytkownik jest proszony o zalogowanie się na konto przez wskazany link. Link ten prowadzi na stronę phishingową, której celem jest przechwycenie danych logowania wpisanych w formularzu.



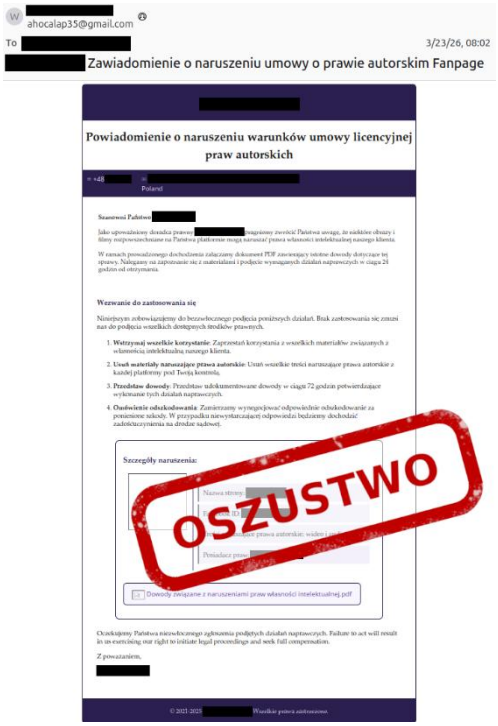
Zespół CERT Polska obserwuje wzmożoną aktywność oszustów wykorzystujących temat odnowienia domen. W wiadomościach e-mail pojawia się informacja o rzekomo zbliżającym się terminie wygaśnięcia domeny w serwisie Seohost. W treści wiadomości znajduje się odnośnik z napisem „Odnów domenę teraz”, który kieruje do strony zawierającej fałszywy panel logowania. Wprowadzone tam dane trafiają bezpośrednio do oszustów. Fałszywe witryny są często łudząco podobne do oryginału, dlatego warto sprawdzić adres nadawcy wiadomości oraz dokładny adres strony logowania. Warto także odszukać oficjalną stronę w wyszukiwarce zamiast korzystać z linku w wiadomości.



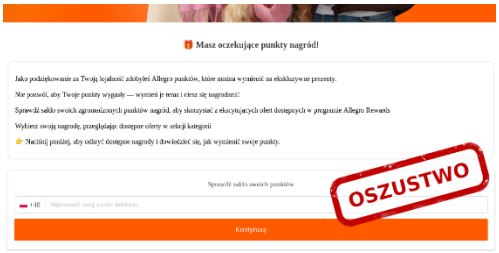
Zespół CERT Polska regularnie otrzymuje zgłoszenia dotyczące fałszywych sklepów internetowych oferujących produkty w wyjątkowo atrakcyjnych cenach. Strony te często pojawiają się jako posty sponsorowane w mediach społecznościowych – szczególnie w okresach wyprzedaży lub zmiany kolekcji – i do złudzenia przypominają oryginalne witryny z logotypami, zdjęciami i opisami produktów. W rzeczywistości są to fałszywe witryny przygotowane w celu wyłudzenia płatności. Przed zakupem warto sprawdzić adres strony, zweryfikować dane firmy, a także wyszukać stronę sklepu w wyszukiwarce zamiast wchodzić na nią poprzez reklamę.

Zespół CERT Polska obserwował kolejną odsłonę kampanii, w której oszuści podszywają się pod dostawcę energii. W wiadomościach informują oni o rzekomej nadpłacie wynikającej z podwójnego opłacenia faktury. Wiadomość zachęca do „odebrania zwrotu” poprzez kliknięcie w link. Strona, do której prowadzi ten link, przypomina panel klienta dostawcy energii. Wprowadzone tam dane logowania trafiają bezpośrednio do przestępców. CERT Polska przypominał użytkownikom, aby w podobnych sytuacjach weryfikowali należność, logując się samodzielnie do panelu klienta lub przez oficjalną aplikację, a także by zwracali uwagę na adres strony. Poza tym zawsze należy zachować ostrożność wobec komunikatów o „zwrotach”, zwłaszcza takich, które wywierają presję na szybkie działanie.

Zespół CERT Polska zwracał uwagę na kolejną kampanię dystrybucji złośliwego oprogramowania. Oszuści wysyłają e-maile zatytułowane „Faktura” zawierające lakoniczną zachętę do otwarcia załącznika. W pliku znajduje się złośliwe oprogramowanie typu RAT (Remote Access Trojan), umożliwiające zdalny dostęp do komputera odbiorcy. Uruchomienie załącznika może prowadzić do utraty kontroli nad urządzeniem, a w konsekwencji także do wycieków danych i strat finansowych. Warto zwracać uwagę na rozszerzenia plików w wiadomościach od nieznanych nadawców – formaty takie jak .zip, .tar, .exe, .js czy .7z mogą sugerować, że zawartość załącznika jest inna, niż obiecuje treść e-maila.



Zespół CERT Polska przestrzegał przed wiadomościami e-mail, w których oszuści podszywają się pod agencje marketingowe i informują o „naruszeniu praw autorskich”. W treści wiadomości znajduje się link prowadzący do rzekomych dowodów w sprawie. Po kliknięciu w link rozpoczyna się pobieranie pliku. Uruchomienie go powoduje instalację złośliwego oprogramowania typu stealer, które może przechwytywać dane zapisane w przeglądarce, w tym loginy, hasła i inne wrażliwe informacje. W przypadku otrzymania takiej wiadomości warto: sprawdzić adres nadawcy i domenę – literówki i błędy mogą oznaczać, że ktoś podszywa się pod prawdziwą firmę; skontaktować się z firmą za pomocą innego kanału kontaktu; zwrócić uwagę na presję czasu wywieraną przez nadawcę wiadomości (to popularna socjotechnika wykorzystywana przez cyberoszustów); sprawdzić rozszerzenie pliku – niektóre typy (na przykład .exe lub .js) mogą wskazywać na złośliwe oprogramowanie.



Zespół CERT Polska informował o nowym wariancie kampanii phishingowej, w którym oszuści wysyłają SMS-y z informacją o rzekomych punktach Allegro, które mają wkrótce wygasnąć. Wiadomości zawierają link oraz zachętę do szybkiego wykorzystania punktów i wyboru nagrody. Kliknięcie w link prowadzi do strony przypominającej oficjalny serwis sprzedażowy. Użytkownik proszony jest o podanie danych karty płatniczej pod pretekstem „aktywacji nagrody”. Jeśli link nie jest aktywny, oszuści proszą o odesłanie wiadomości o treści „Tak”, co pozwala im obejść zabezpieczenia telefonów przed linkami w niechcianej korespondencji.

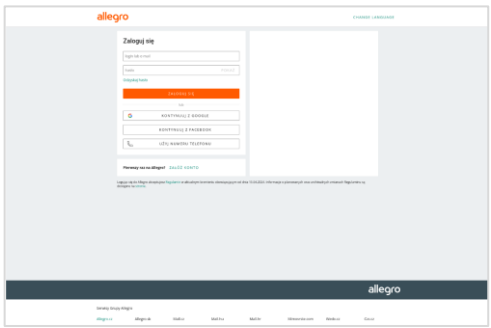
Więcej: Facebook/CERT Polska, X/CERT Polska oraz moje.cert.pl/komunikaty

Opis najczęściej występujących kampanii – III 2026

Fałszywe strony oferujące wysokodochodowe inwestycje

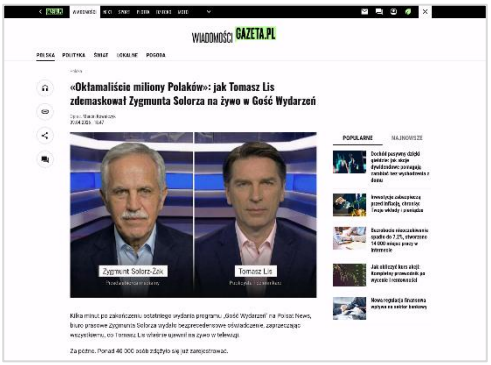
Zespół CERT Polska w dalszym ciągu obserwował wzmożoną kampanię phishingową, w której oszuści podszywają się pod różnego rodzaju koncerny paliwowo-energetyczne, firmy i instytucje, m.in. Lotos, Tesla, PGNiG, PGE, Baltic Pipe. Oszuści reklamują w mediach społecznościowych oraz w wyszukiwarkach internetowych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

Fałszywe strony Allegro



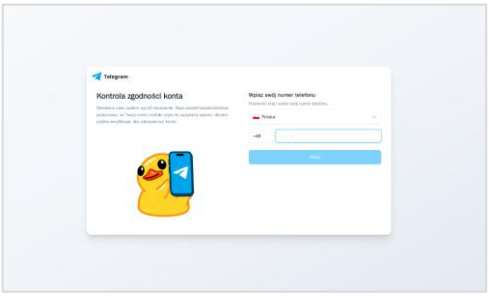
Zespół CERT Polska obserwował wzmożoną kampanię phishingową wykorzystującą wizerunek platformy Allegro. Na fałszywych stronach internetowych znajduje się panel logowania do tego serwisu służący do wyłudzania danych uwierzytelniających od użytkowników Allegro.

Fałszywe strony serwisu Gazeta.pl



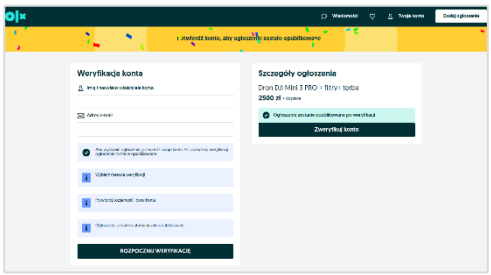
Zespół CERT Polska rejestrował incydenty, w których atakujący za pośrednictwem stron internetowych podszywają się pod serwis Gazeta.pl. Na fałszywych stronach oszuści publikują artykuły, w których opisują rzekome inwestycje znanych osób w kryptowaluty, obligacje czy akcje na platformie inwestycyjnej.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

Fałszywe strony komunikatora Telegram



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

Fałszywe strony OLX



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

Fałszywe strony firmy Orlen

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

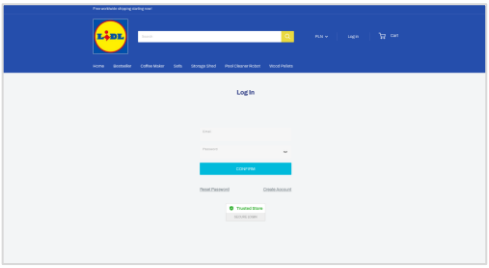
Fałszywe strony kanału Polsat News

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 serwisu Onet.pl

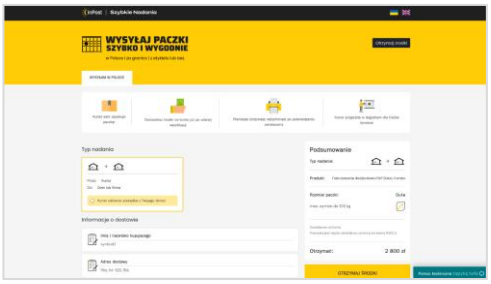
Zespół CERT Polska obserwował kampanię phishingową, w której oszuści podszywają się pod serwis Onet.pl i umieszczają na fałszywych stronach internetowych artykuły służące do reklamowania nieistniejących programów inwestycyjnych. Celem oszustów jest wyłudzenie środków finansowych.

Fałszywe panele logowania wykorzystujące markę Lidl



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

Fałszywe strony firmy InPost



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