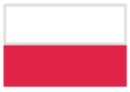
LIPIEC 2026

Podsumowanie Miesiąca CERT POLSKA

Nr 7/2026

CERT.PL NASK
CSIRT NASK

PODSUMOWANIE MIESIĄCA CERT POLSKA



PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTERSTWA CYFRYZACJI

TLP: CLEAR

Autor: zespół CERT Polska

SPIS TREŚCI

Statystyki 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 lipca 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 – VII 2026

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

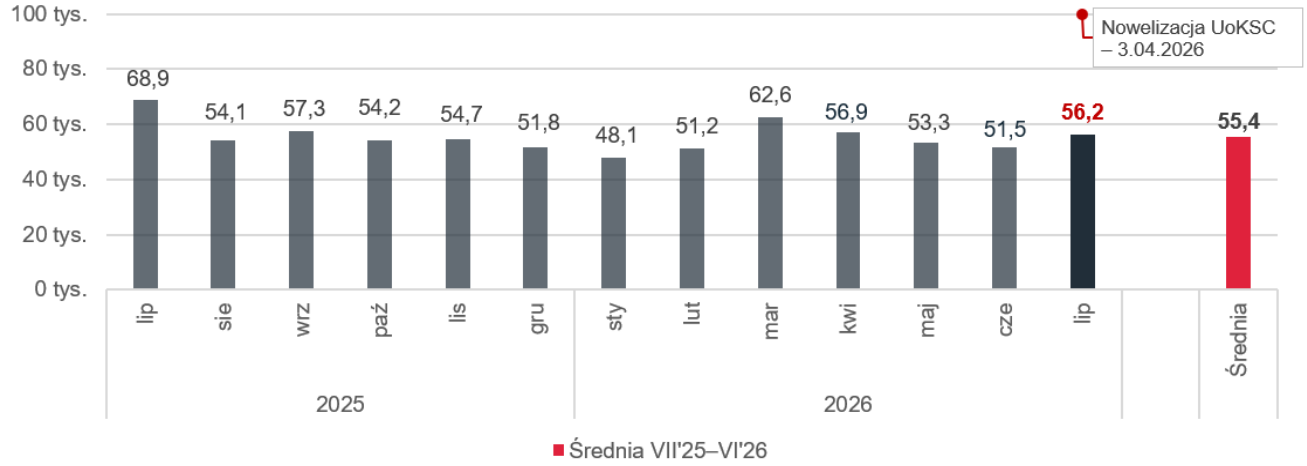
Zgłoszone zagrożenia i zarejestrowane incydenty	Liczba
Zgłoszenia potencjalnych zdarzeń dla cyberbezpieczeństwa*	6,3 tys.
Zgłoszenia cyberzagrożeń*	47,0 tys.
Zgłoszenia incydentów	2,8 tys.
Zgłoszenia poważnych cyberzagrożeń*	0,03 tys.
Razem zgłoszenia	**56,2 tys.**
Zarejestrowane incydenty**	**31,2 tys.**

* 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 lipcu 2026 r. zespół CERT Polska otrzymał **łącznie 56,2 tys. zgłoszeń**. Na ich podstawie **zarejestrowano 31,2 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.

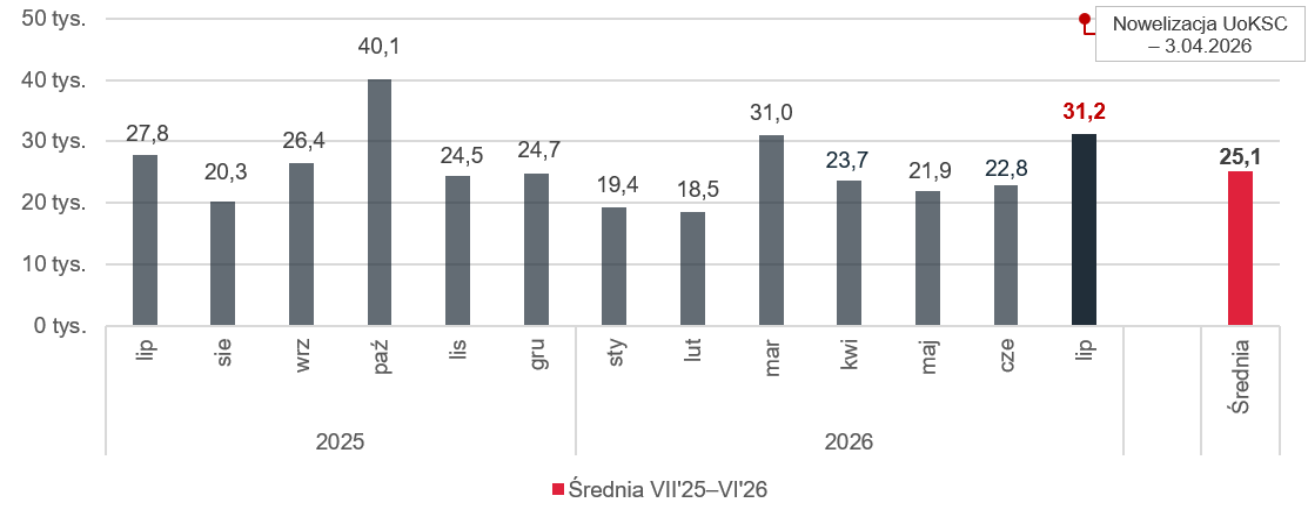
Zgłoszenia zagrożeń od VII 2025 do VII 2026



Wykres 1. Liczba wszystkich zgłoszeń od 01.07.2025 do 31.07.2026. Źródło: CERT Polska / CSIRT NASK.

Liczba wszystkich zgłoszeń odnotowanych w lipcu 2026 r. pozostawała powyżej średniej liczonej z poprzednich 12 miesięcy. W porównaniu z analogicznym miesiącem 2025 r. liczba ta **zmniejszyła się o 18%**. W stosunku do czerwca 2026 r. odnotowano **wzrost o 9%**.

Zarejestrowane incydenty cyberbezpieczeństwa od VII 2025 do VII 2026



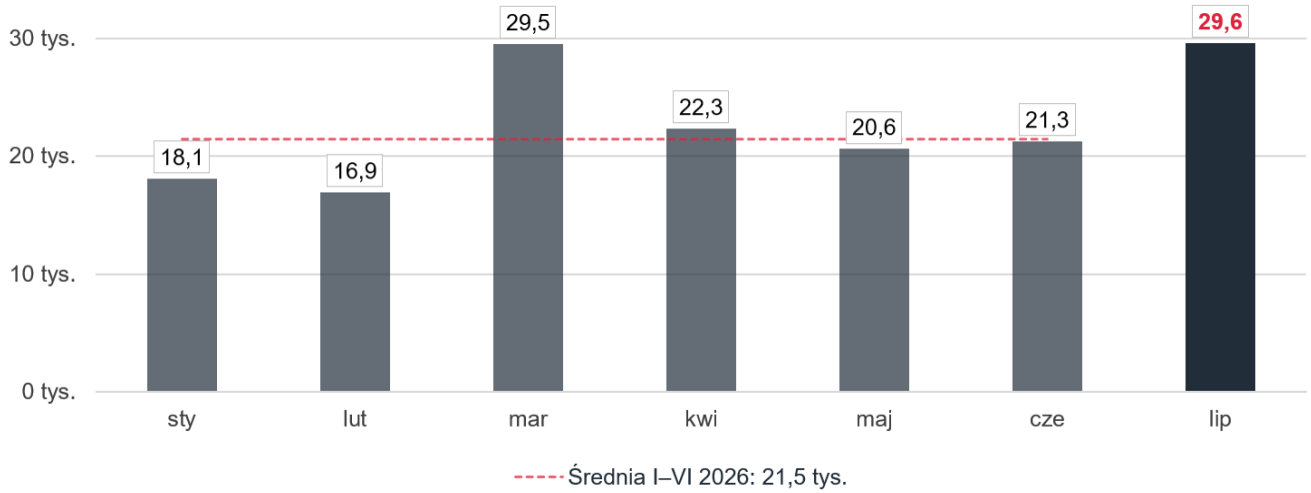
Wykres 2. Liczba zarejestrowanych incydentów od 01.07.2025 do 31.07.2026. Źródło: CERT Polska / CSIRT NASK.

Liczba incydentów zarejestrowanych w lipcu 2026 r. wyniosła **31,2 tys.** W porównaniu z analogicznym miesiącem 2025 r. liczba incydentów w lipcu 2026 r. **zwiększyła się o 12%** i pozostawała powyżej średniej liczonej z 12 poprzednich miesięcy. W stosunku do czerwca 2026 r. odnotowano **wzrost liczby incydentów o 37%**.

Liczba nazw szkodliwych domen wpisanych na Listę Ostrzeżeń CERT Polska I–VII 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.

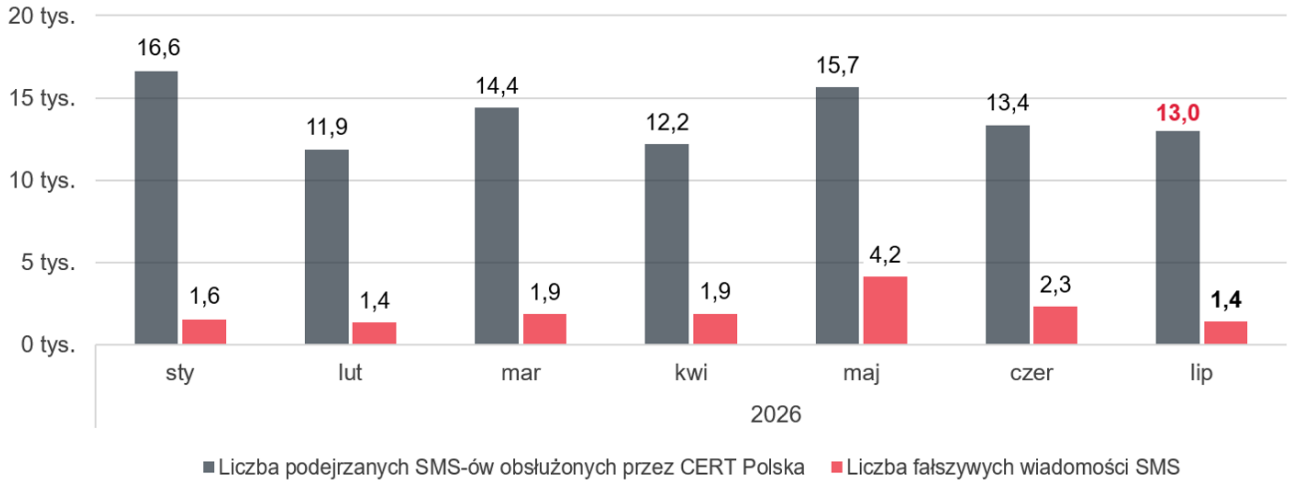


Wykres 3. Liczba nazw szkodliwych domen wpisanych na Listę Ostrzeżeń. Źródło: CERT Polska / CSIRT NASK.

Od 1 stycznia do 31 lipca 2026 r. na Listę Ostrzeżeń przed niebezpiecznymi stronami wpisano **158,3 tys.** szkodliwych domen, z czego w lipcu 2026 r. dodano **29,6 tys.** nazw domen wykorzystywanych do wyłudzania danych osobowych, danych uwierzytelniających do kont bankowych i serwisów społecznościowych. Wartość ta w stosunku do czerwca 2026 r. **zwiększyła się o 39%**.

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

Od 1 stycznia do 31 lipca 2026 r. zespół CERT Polska zarejestrował **97,1 tys.** zgłoszeń podejrzanych SMS-ów. Liczba SMS-ów otrzymanych w lipcu 2026 r. wyniosła **13 tys.** W porównaniu z czerwcem 2026 r. był to **spadek o 3%**. Wśród ogółu SMS-ów przyjętych w lipcu 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 11%**.



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

Wzorce fałszywych wiadomości SMS I–VII 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 lipcu 2026 r., na podstawie wytworzonych przez CERT Polska wzorców fałszywych wiadomości SMS, zablokowano łącznie **6,2 tys.** SMS-ów. Dane o zablokowanych wiadomościach SMS są szacowane na podstawie raportów przesyłanych przez operatorów telekomunikacyjnych z uwzględnieniem procentowego udziału tych operatorów w rynku telefonii mobilnej.

Tabela 2. Liczba wytworzonych wzorców fałszywych wiadomości SMS.

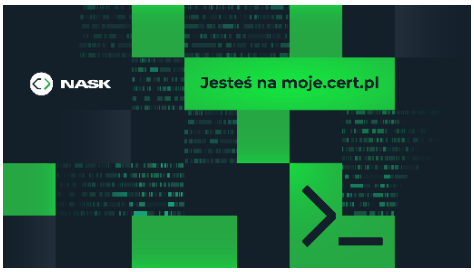
Wzorce fałszywych wiadomości SMS w 2026	sty	lut	mar	kwi	maj	cze	lip	Razem
Liczba wytworzonych wzorców	118	97	85	80	105	36	**57**	**578**

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" zespół CERT Polska publikuje 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 lipcu 2026 r. w serwisie moje.cert.pl **zarejestrowało się 619 nowych użytkowników**.



W okresie od 1 do 31 lipca 2026 r. CERT Polska wysłał **7,8 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 lipcu 2026 r. zespół CERT Polska nadał **53** numery CVE. Wśród wykrytych podatności znalazły się podatności w oprogramowaniu m.in. Windu CMS, GNU gawk, MyComplianceOffice MCO, SOPlanning. W ramach badań własnych CERT Polska znalazł 2 podatności w oprogramowaniu MWDB Core.

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

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

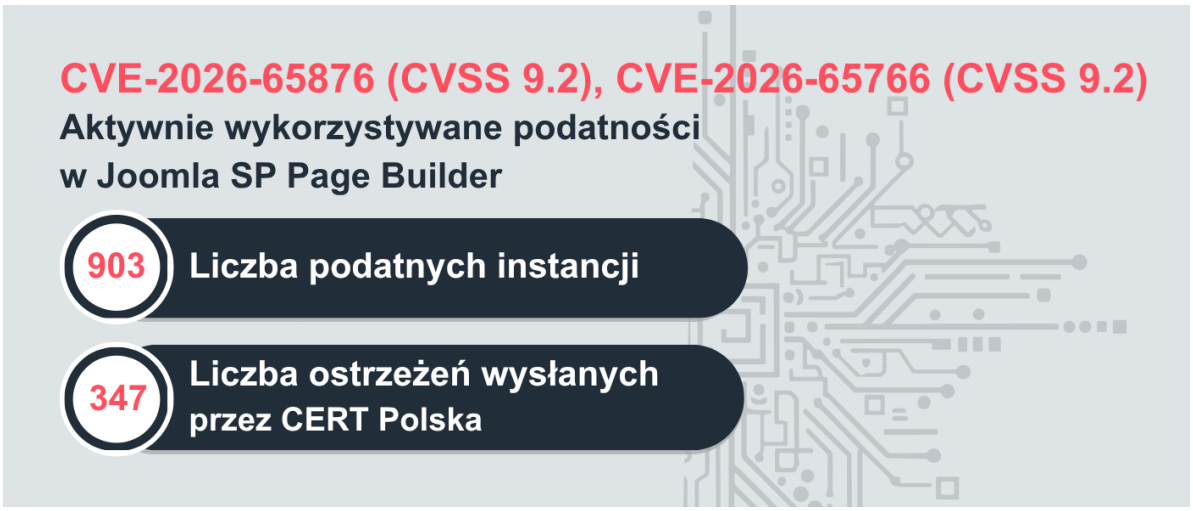
Numery CVE w 2026	sty	lut	mar	kwi	maj	cze	lip	Razem
Liczba opublikowanych numerów CVE	16	12	32	21	34	47	**53**	**215**

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

W systemie WordPress (wersje 6.8.x–7.0.x) wykryto dwie powiązane ze sobą podatności. Jedna z nich, oznaczona jako CVE-2026-63030, dotyczy błędnego przetwarzania zapytań w API i umożliwia obejście mechanizmów autoryzacji. Druga (CVE-2026-60137) wynika z braku zabezpieczeń przed wstrzyknięciem złośliwego kodu SQL do bazy danych. Połączenie tych luk pozwala atakującemu na zdalne wykonanie dowolnego kodu na serwerze (RCE) i przejęcie kontroli nad witryną.

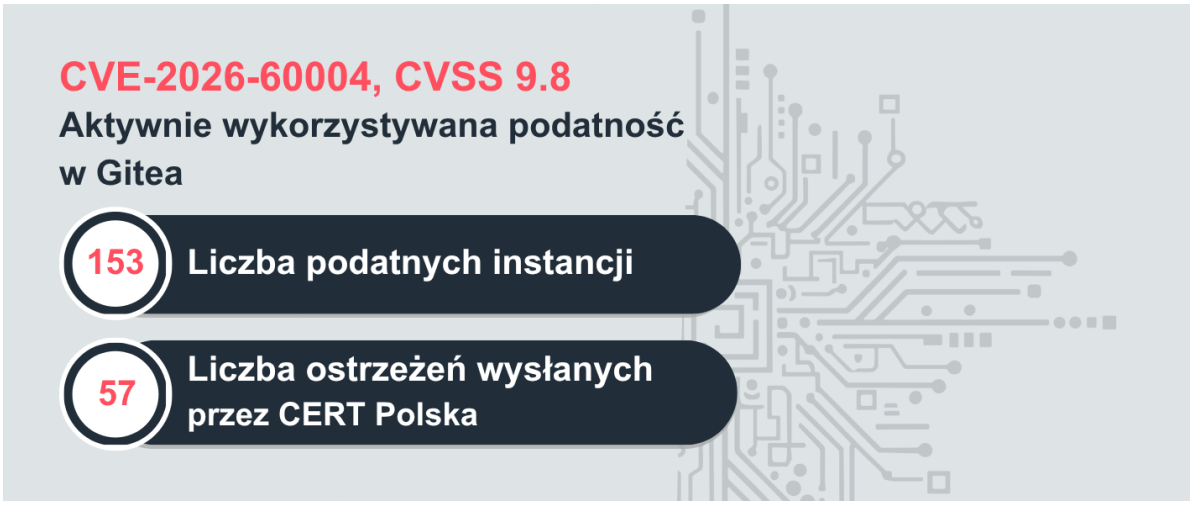
Obie podatności są aktywnie wykorzystywane w atakach, dlatego figurują w katalogu CISA KEV (Known Exploited Vulnerabilities). Rekomendujemy natychmiastową aktualizację do wersji 6.8.6 / 6.9.5 / 7.0.2 lub nowszej.

Więcej: https://ransomnews.com/wp2shell-wordpress-core-rce-2026



Wykryto dwie krytyczne podatności w popularnym rozszerzeniu SP Page Builder (w wersjach poniżej 6.7.1) służącym do budowania stron dla systemu Joomla. Błędy polegają na braku weryfikacji danych wprowadzanych przez użytkownika w dwóch różnych funkcjonalnościach (loadMoreArticles oraz Dynamic Content). Atakujący bez konieczności logowania może wstrzyknąć zapytania SQL i uzyskać dostęp do bazy danych, co w praktyce prowadzi do wycieku wrażliwych danych i przejęcia treści serwisu. Rekomendujemy aktualizację rozszerzenia do wersji 6.7.1 lub nowszej.

Więcej: https://www.sentinelone.com/vulnerability-database/cve-2026-65876



Wykryto krytyczną podatność w funkcji porównywania zmian (diffpatch) w Gitea, w wersjach 1.17–1.27.0. Atakujący poprzez złośliwą zawartość repozytorium może umieścić w nim własne skrypty, które uruchomią się automatycznie podczas operacji Git i wykonają dowolne komendy na serwerze z uprawnieniami usługi Gitea. W instalacjach z otwartą rejestracją atak jest możliwy bez logowania, co może doprowadzić do przejęcia kontroli nad serwerem, kradzieży poświadczeń i konfiguracji, modyfikacji wyników budowy oprogramowania. Rekomendujemy aktualizację do wersji 1.27.1 lub nowszej.

Więcej: https://www.cyberartspro.com/en/gitea-cve-2026-60004-rce-vulnerability

W urządzeniach Secure Mobile Access z rodziny SMA 1000 (wersje firmware 12.4.3 i 12.5.0) wykryto dwie podatności. Pierwsza (SSRF) pozwala atakującemu bez logowania nakłonić urządzenie do wykonywania żądań do dowolnych miejsc w sieci, co może służyć do ominięcia zabezpieczeń i rozpoznania infrastruktury wewnętrznej. Druga (Code Injection) umożliwia uwierzytelnionemu administratorowi wykonanie dowolnych komend systemowych. W połączeniu luki te prowadzą do pełnej kompromitacji urządzenia.

Obie podatności są aktywnie wykorzystywane i trafiły do katalogu CISA KEV. Rekomendujemy natychmiastową aktualizację zgodnie z komunikatem producenta (SNWLID-2026-0008).

Więcej: https://www.tenable.com/blog/cve-2026-15409-cve-2026-15410-sonicwall-sma-1000-zero-day-vulnerabilities-exploited-in-the

Wybrane informacje

NASK – PIB otrzymał dostęp do GPT-5.5 Cyber – innowacyjnego modelu sztucznej inteligencji stworzonego przez OpenAI do wykrywania i analizy cyberzagrożeń. Jest on przeznaczony do zaawansowanego wyszukiwania podatności, generowania poprawek i automatycznej naprawy, a także do analizy złośliwego oprogramowania czy wykonywania zadań z obszaru informatyki śledczej. Model jest udostępniany wyłącznie zaufanym partnerom. Polska i zespół CERT Polska działający w NASK – PIB dołączają do tego grona jako tzw. zweryfikowany obrońca. Eksperci zyskają zaawansowany dostęp za pośrednictwem programu Government Trusted Access for Cyber przeznaczonego dla jednostek rządowych.

Więcej: nask.pl/NASK z przełomowym narzędziem od OpenAI

Od 3 do 5 lipca odbywały się **kwalifikacje krajowe do European Cybersecurity Challenge – ECSC 2026, przeprowadzone przez zespół CERT Polska**.
ECSC to międzynarodowe zawody cyberbezpieczeństwa dla uczestników w wieku od 14 do 25 lat, organizowane co roku pod przewodnictwem Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA). Kwalifikacje miały formę indywidualnego konkursu Capture The Flag, podczas którego zawodnicy mierzyli się z zadaniami z obszarów takich jak kryptografia, inżynieria wsteczna, bezpieczeństwo aplikacji czy analiza podatności. W kwalifikacjach zostało wyłonionych 10 osób, które będą reprezentować Polskę podczas zawodów finałowych, które odbędą się w dniach 12–16 października br. w Niemczech.

Więcej: nask.pl/Sprawdź się w kwalifikacjach do ECSC 2026, linkedin.com/Kwalifikacje krajowe do ECSC 2026 oficjalnie dobiegły końca

---

Od 2 sierpnia 2026 r. zaczynają obowiązywać kolejne przepisy **AI Act**, w tym te dotyczące przejrzystości korzystania ze sztucznej inteligencji (art. 50), oraz rozpocznie się ich egzekwowanie. Nowe regulacje obejmują nie tylko dostawców systemów AI, lecz także media, wydawców, influencerów i organizacje wykorzystujące generatywną sztuczną inteligencję do tworzenia treści.
Na dostawcach systemów AI spoczywa obowiązek informowania użytkownika, że ma on do czynienia z systemem służącym do wchodzenia w interakcję z odbiorcą, chyba że wynika to z kontekstu. Dotyczy to np. chatbotów czy wirtualnych asystentów. Natomiast osoby i organizacje korzystające z generatywnej sztucznej inteligencji są zobowiązane do poinformowania odbiorcy o zastosowaniu AI, jeśli wygenerowała ona lub w istotny sposób zmodyfikowała obraz, materiał wideo, audio albo tekst publikowany w celu informowania społeczeństwa o sprawach leżących w interesie publicznym. Szczególne obowiązki dotyczą materiałów typu deepfake – treści te powinny być wyraźnie oznaczone jako wygenerowane lub zmanipulowane przez AI.

Więcej: nask.pl/Czas oznaczać treści AI. Nowe obowiązki dla firm, twórców i mediów, gov.pl/AI Act – co się zmieniło od 2 sierpnia 2026 roku?

W lipcu **zespół CERT Polska** opublikował w swoich mediach społecznościowych cykl postów na temat cyberzagrożeń związanych z wakacjami. Posty zawierały opis scenariuszy oszustw oraz porady, o czym trzeba pamiętać, aby nie dać się oszukać. Zwracano uwagę na oszustwa służące do wyłudzania danych, pieniędzy lub do przejęcia konta, w tym: wykorzystywanie wizerunków platform rezerwacyjnych i hoteli, fałszywe oferty (np. bilety w atrakcyjnych cenach), fałszywe wiadomości od znajomych z prośbą o pożyczkę (po przejęciu konta w mediach społecznościowych).

Więcej: Facebook/CERT Polska

Wystąpienia ekspertów CERT Polska

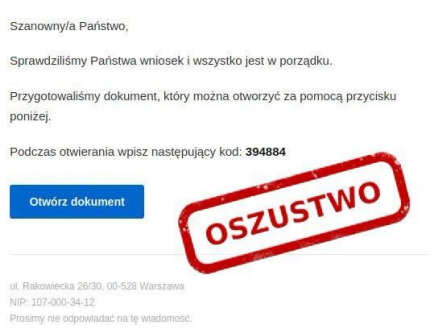
- 3 lipca – wygłoszenie wykładu pt. „Trzydzieści lat cyberbezpieczeństwa – obserwacje i prognozy CERT Polska” podczas uroczystości w Instytucie Podstawowych Problemów Techniki Polskiej Akademii Nauk, Warszawa.

  Więcej: ippt.pan.pl/relacja
- 20 lipca – wystąpienie na temat działalności CSIRT NASK, konferencja „Cyberbezpieczeństwo jednostek publicznych” w Szczecinie.

  Więcej: gov.pl/relacja

Komunikaty o zagrożeniach

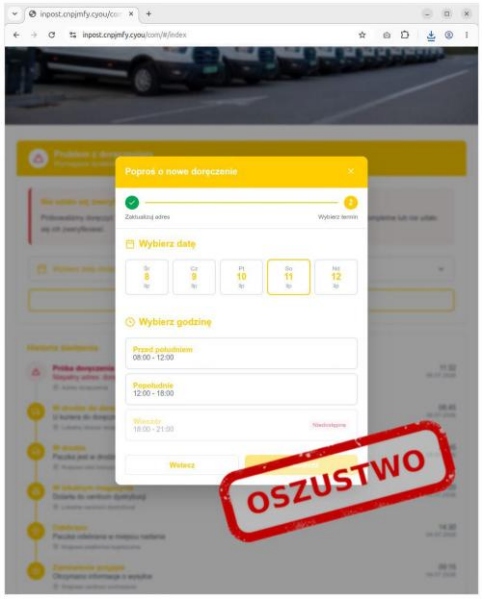
Informacje o zaobserwowanych kampaniach publikowane przez zespół CERT Polska w serwisie moje.cert.pl oraz w serwisach społecznościowych.



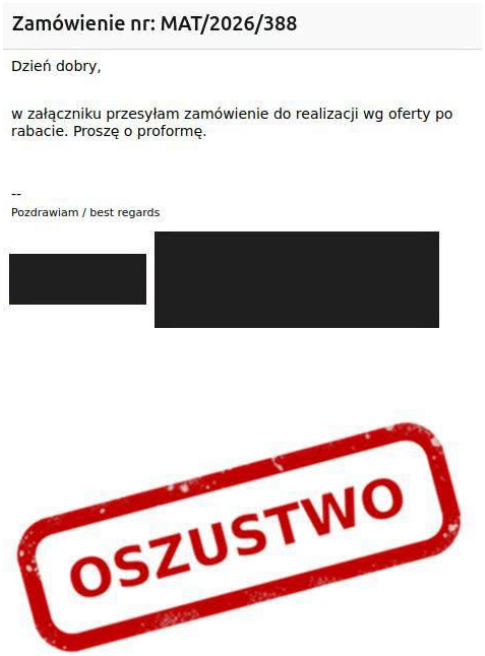
Zespół CERT Polska informował o kampanii phishingowej, w której oszuści podszywają się pod Narodowy Fundusz Zdrowia. Cyberprzestępcy rozsyłają wiadomości e-mail i informują o rzekomym zweryfikowaniu wniosku oraz o dokumencie, który można otworzyć po kliknięciu w link i podaniu kodu przesłanego w wiadomości. Link prowadzi do fałszywej strony internetowej przypominającej serwis NFZ, na której oszuści próbują wyłudzić dane osobowe i dane karty płatniczej pod pretekstem realizacji zwrotu należnych środków.

Zespół CERT Polska informował o kampanii phishingowej, w której oszuści podszywają się pod operatorów stref płatnego parkowania. Cyberprzestępcy informują odbiorcę wiadomości SMS o nieuregulowaniu przez niego opłaty za parkowanie. Link zawarty w wiadomości odsyła do strony internetowej imitującej oficjalny serwis płatności. Dane rejestracyjne pojazdu i dane karty płatniczej wpisane przez użytkownika mogą zostać później wykorzystane przez oszustów m.in. do kradzieży pieniędzy oraz do dalszych prób wyłudzeń.

Oszuści próbują także obchodzić zabezpieczenia telefonów przed linkami z nieznanych źródeł – w tym celu proszą o wysłanie odpowiedzi w konwersacji lub skopiowanie adresu fałszywej strony i wklejenie linku do przeglądarki.

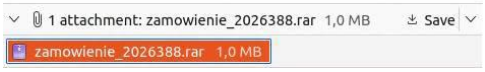


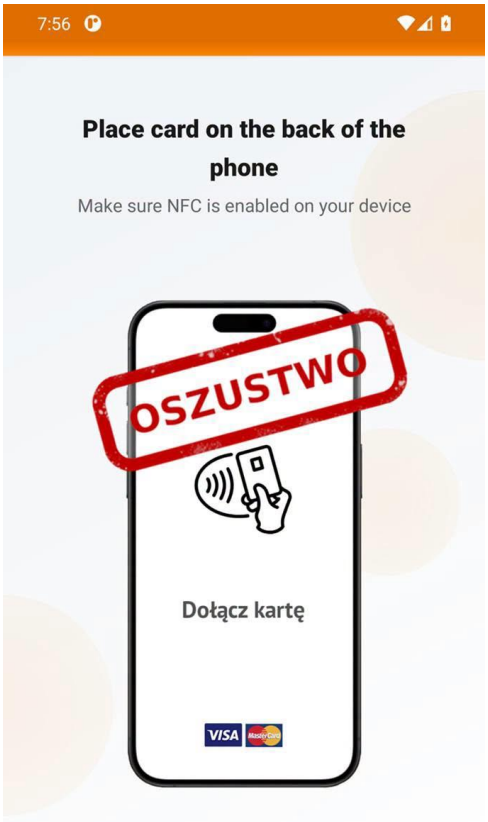
Zespół CERT Polska obserwował kolejną odsłonę kampanii phishingowej wymierzonej w klientów firmy InPost. W wiadomościach oszuści informują o rzekomej konieczności potwierdzenia danych adresowych z powodu nieudanej próby doręczenia przesyłki i podają link do strony internetowej przygotowanej w celu wyłudzenia danych osobowych oraz danych karty płatniczej.



Zespół CERT Polska obserwował kampanię wymierzoną w małych i średnich przedsiębiorców. Oszuści rozsyłają wiadomości e-mail z informacją o rzekomym zamówieniu lub zapytaniu ofertowym dołączonym do wiadomości. W załączniku zamiast dokumentu znajduje się szkodliwe oprogramowanie z rodziny Remcos. Jego uruchomienie prowadzi do infekcji komputera i pozwala atakującemu na zdalny dostęp do urządzenia.

Warto zwrócić uwagę na to, że adres nadawcy tych wiadomości często znajduje się w zagranicznej bądź nietypowej domenie.

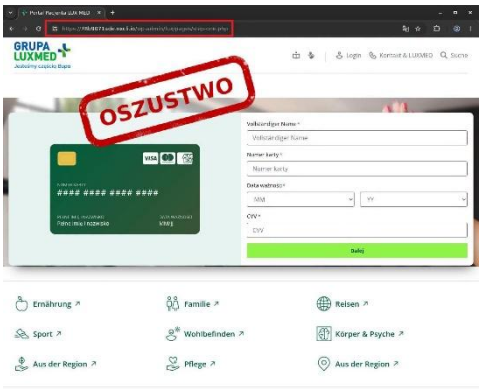




Zespół CERT Polska obserwował powrót kampanii złośliwego oprogramowania NGate. Mechanizm ataku opiera się na podszywaniu się pod pracowników banków. W następnym kroku cyberprzestępcy nakłaniają użytkowników do zainstalowania fałszywej aplikacji i przyłożenia karty płatniczej do telefonu z NFC. Więcej informacji na ten temat można znaleźć w artykule pt. Analiza kampanii złośliwego oprogramowania NGate (NFC relay) opublikowanym na stronie cert.pl.

Zespół CERT Polska obserwował kampanię phishingową, w której cyberprzestępcy podszywają się pod administrację poczty Onet. W wiadomościach e-mail znajduje się informacja o konieczności weryfikacji danych w celu rzekomego podniesienia poziomu bezpieczeństwa oraz jakości usługi. Oszuści próbują wyłudzić adres e-mail i hasło do skrzynki, a następnie informacje takie jak data urodzenia, adres zamieszkania, numer telefonu, a w kolejnym kroku także dane karty płatniczej.

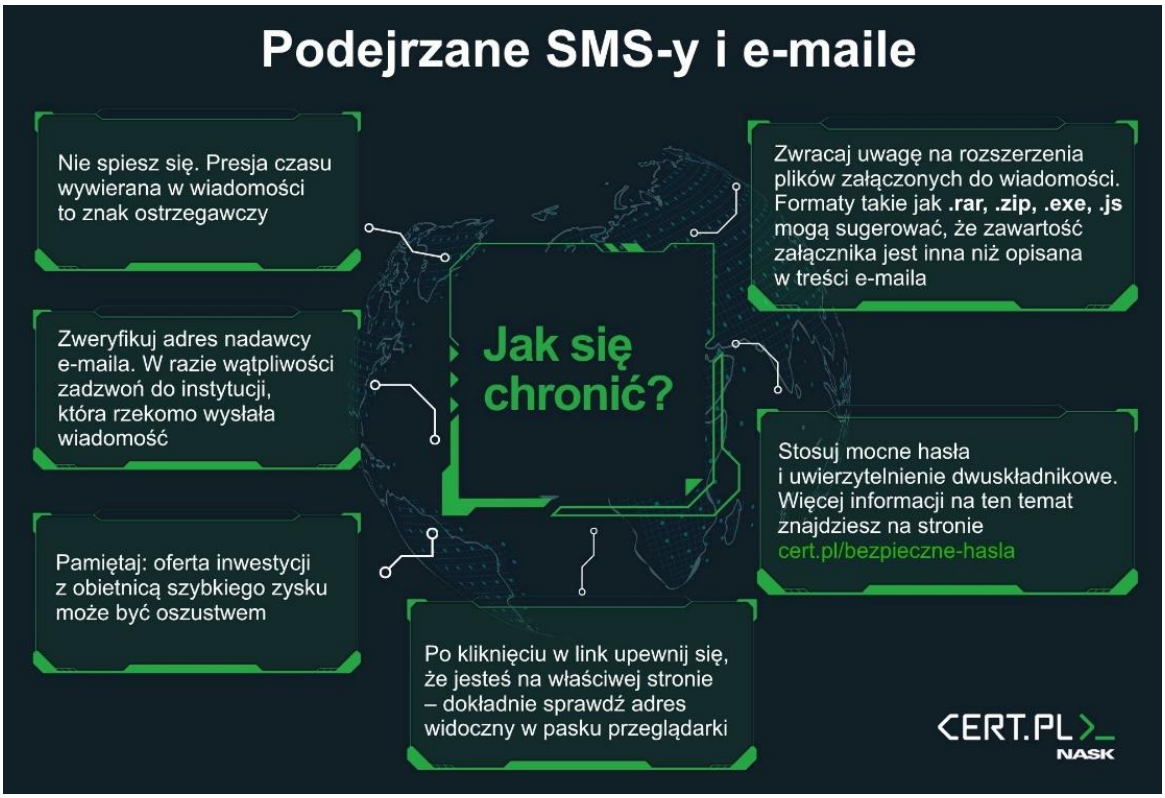
Zespół CERT Polska ostrzegał o wysyłanych przez cyberprzestępców wiadomościach e-mail, w których informują oni o rzekomym wygaśnięciu domeny i konieczności jej przedłużenia. W wiadomościach znajdują się linki prowadzące do fałszywych stron internetowych podszywających się pod popularnych rejestratorów domen. Oszuści próbują wyłudzić dane logowania do paneli administracyjnych związanych z obsługą domen i usług hostingowych.



Zespół CERT Polska ostrzegał przed oszustwem, w którym cyberprzestępcy podszywają się pod prywatnych dostawców usług medycznych, np. pod Grupę LUX MED. W wiadomościach e-mail oszuści informują o zaakceptowaniu wniosku o zwrot kosztów leczenia i podają link, który prowadzi do fałszywej strony internetowej wykorzystującej wizerunek placówki medycznej. Tam znajdują się formularze, które służą oszustom do wyłudzania danych osobowych oraz danych karty płatniczej pod pretekstem realizacji zwrotu należnych środków.

Zespół CERT Polska obserwował nowy scenariusz ataku – cyberprzestępcy podszywają się pod serwis gov.pl i wysyłają SMS-y, w których informują o rzekomej konieczności uzupełnienia danych we wniosku mieszkaniowym. W wiadomościach znajduje się link kierujący na fałszywą stronę, na której podana jest kwota dofinansowania przysługującego w ramach rządowych programów mieszkaniowych. Aby dokończyć weryfikację i otrzymać środki, użytkownik ma wpisać dane swojej karty płatniczej.

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

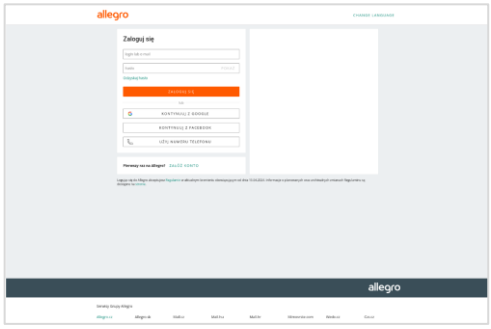


Opis najczęściej występujących kampanii – VII 2026

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, BBC. Oszuści reklamują w mediach społecznościowych oraz w serwisach 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.

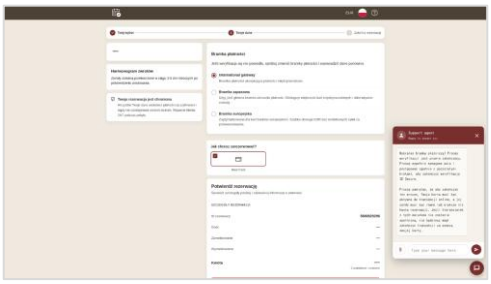
Fałszywe strony serwisu Gazeta.pl

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 wykorzystują wizerunki znanych osób do promowania inwestycji 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 firmy Orlen

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

Fałszywe strony dotyczące rezerwacji hotelowych

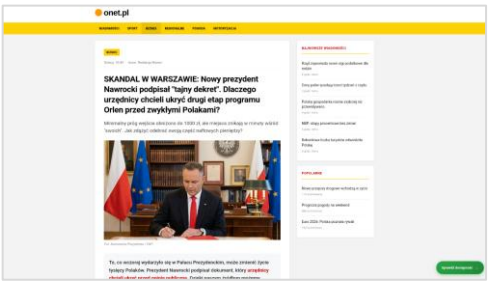


Zespół CERT obserwował kampanię phishingową wymierzoną w osoby mające rezerwacje hotelowe. Oszuści wysyłają wiadomości, w których informują o rzekomo nieudanej próbie kontaktu i proszą o pilne podjęcie działania. Wiadomości wydają się wiarygodne ze względu na wykorzystanie danych z prawdziwych rezerwacji. Odnośnik zawarty w wiadomości prowadzi do strony imitującej serwis hotelu lub platformę rezerwacyjną. Formularz, który się tam znajduje, służy oszustom do wyłudzania danych osobowych oraz danych karty płatniczej pod pozorem potwierdzenia rezerwacji lub realizacji płatności.

Fałszywe strony OLX

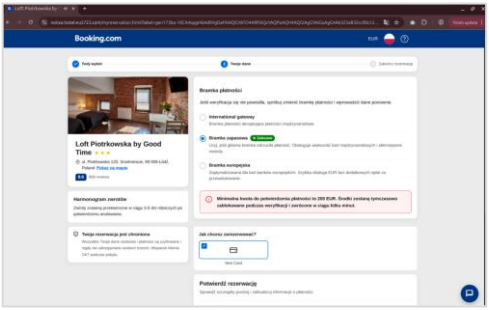
Zespół CERT Polska zarejestrował incydenty, w których atakujący za pośrednictwem stron internetowych podszywają się pod serwis OLX. Panel logowania do tego serwisu służy do wyłudzania od użytkowników danych uwierzytelniających.

Fałszywe strony serwisu Onet.pl



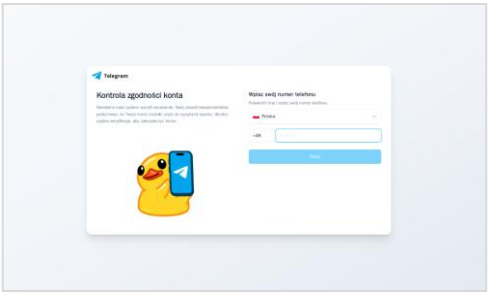
Zespół CERT Polska obserwował kampanię phishingową, w której oszuści podszywają się pod serwis Onet.pl i umieszczają na fałszywych stronach internetowych artykuły służące do reklamowania nieistniejących programów inwestycyjnych. Celem oszustów jest wyłudzenie środków finansowych.

Fałszywe rezerwacje serwisu Booking.com



Zespół CERT Polska rejestrował incydenty, w których cyberprzestępcy tworzą fałszywe strony internetowe przypominające witrynę serwisu rezerwacyjnego Booking.com. Panel logowania znajdujący się na tych stronach służy oszustom do wyłudzania od użytkowników ich danych uwierzytelniających lub danych karty płatniczej.

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 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 serwisu gov.pl

Zespół CERT Polska rejestrował incydenty, w których oszuści na spreparowanych stronach internetowych łudząco podobnych do stron serwisu gov.pl umieszczają artykuły, w których są opisywane nieistniejące programy inwestycyjne. Celem jest wyłudzenie środków finansowych.