LISTOPAD 2025

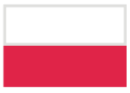
Podsumowanie Miesiąca CERT POLSKA CSIRT NASK

Nr 3/2025

CERT.PL NASK

CSIRT NASK

PODSUMOWANIE MIESIĄCA CERT POLSKA / CSIRT NASK




PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTERSTWA CYFRYZACJI

TLP: CLEAR

Autor: zespół CERT Polska

SPIS TREŚCI

Statystyki zarejestrowanych zagrożeń 4

Moje.cert.pl 9

Podatności CVE 9

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

Wybrane informacje 10

Komunikaty o zagrożeniach 12

Opis najczęściej występujących kampanii – XI 2025 15

Statystyki zarejestrowanych zagrożeń

Zgłoszenia i incydenty cyberbezpieczeństwa

Statystyki prezentowane poniżej obejmują dane o liczbie zarejestrowanych zgłoszeń[1] oraz o liczbie incydentów obsłużonych przez CSIRT NASK w okresie od 1 do 30 listopada 2025 r. Dla lepszego zobrazowania pojawiających się trendów niektóre z tych danych pokazywane są w dłuższej perspektywie czasu.

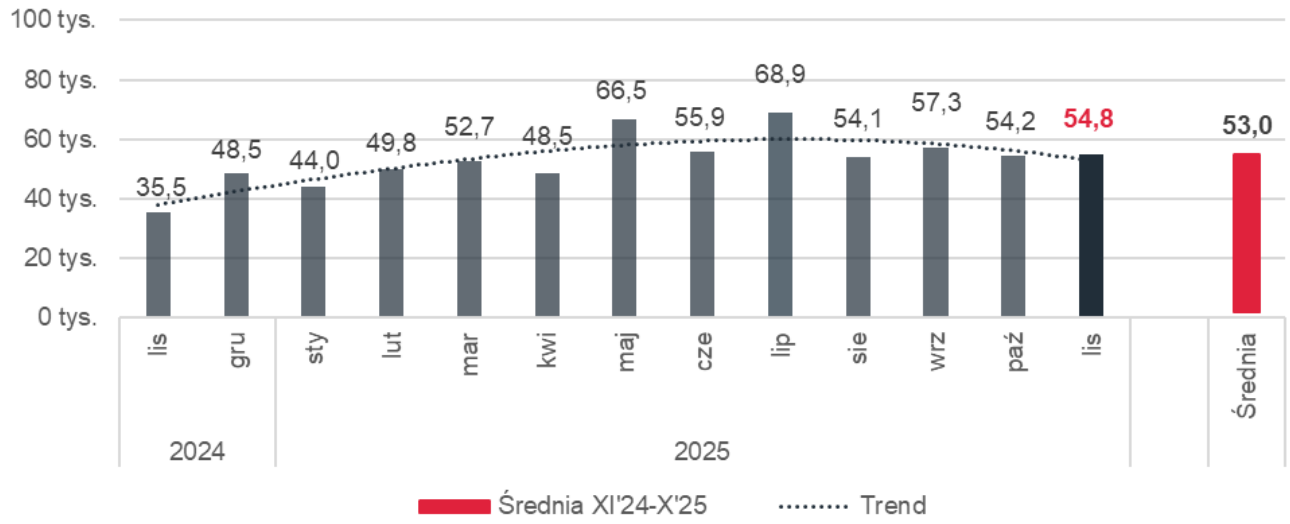
Zarejestrowane zgłoszenia i incydenty cyberbezpieczeństwa – XI 2025

Tabela 1. Liczba zarejestrowanych zgłoszeń i incydentów od 1 do 30 listopada 2025 r.

Zagrożenia cyberbezpieczeństwa	Liczba
Zarejestrowane zgłoszenia	**54,8 tys.**
w tym zarejestrowane (obsłużone) incydenty	**24,5 tys.**

W listopadzie 2025 r. CSIRT NASK otrzymał łącznie **54,8 tys.** zgłoszeń, które zostały przeanalizowane i pogrupowane. Na ich podstawie zarejestrowano **24,5 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 XI 2024 do XI 2025

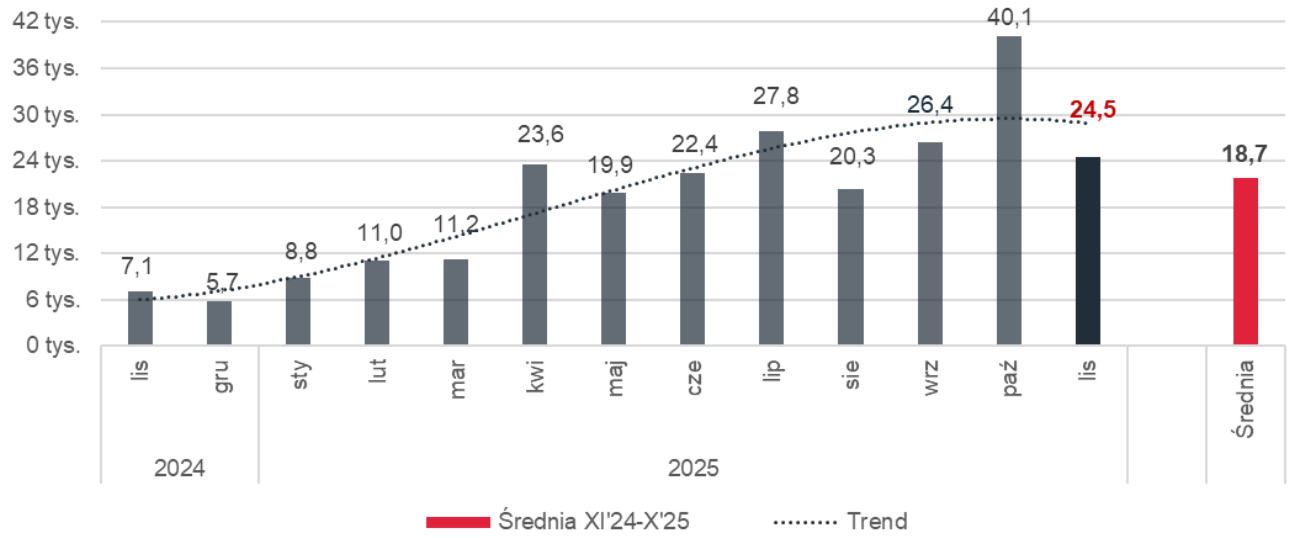


Wykres 1. Liczba zarejestrowanych zgłoszeń od 01.11.2024 do 30.11.2025. Źródło: CERT Polska / CSIRT NASK.

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

Liczba zgłoszeń odnotowanych w listopadzie 2025 r. przekroczyła średnią liczoną z poprzednich 12 miesięcy. W porównaniu z analogicznym miesiącem 2024 r. liczba ta **zwiększyła się o 54%**. W stosunku do października 2025 r. był to **wzrost o 1%**.

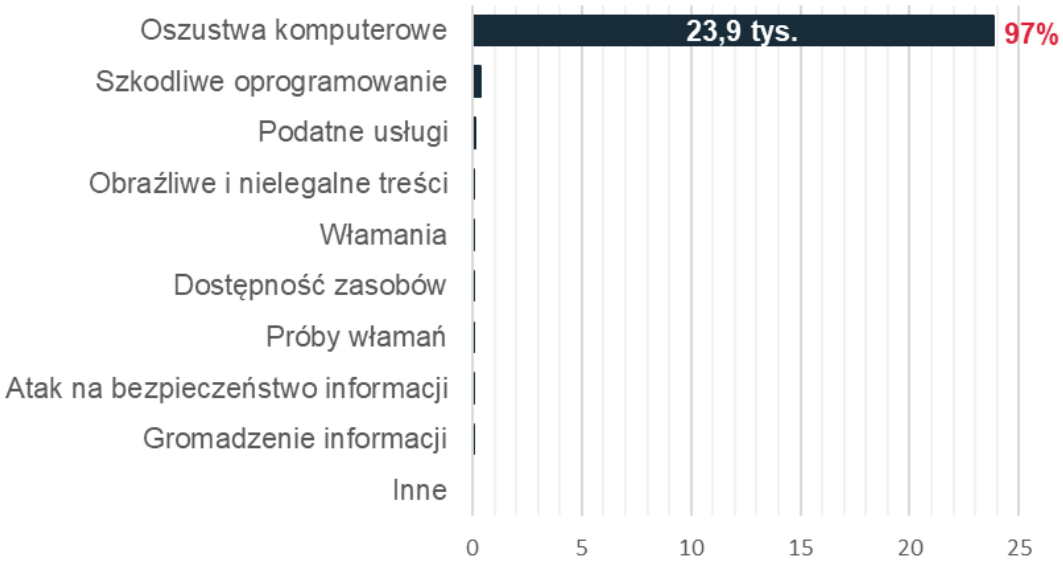
Zarejestrowane incydenty cyberbezpieczeństwa od XI 2024 do XI 2025



Wykres 2. Liczba zarejestrowanych incydentów od 01.11.2024 do 30.11.2025. Źródło: CERT Polska / CSIRT NASK.

Liczba incydentów zarejestrowanych w listopadzie 2025 r. wyniosła **24,5 tys.** W porównaniu z analogicznym miesiącem 2024 r. liczba incydentów w listopadzie 2025 r. **zwiększyła się o 245%** i pozostawała powyżej średniej liczonej z 12 poprzednich miesięcy. W stosunku do października 2025 r. liczba zarejestrowanych incydentów **zmniejszyła się o 39%**.

Rodzaje zarejestrowanych zagrożeń – XI 2025



Wykres 3. Liczba zarejestrowanych incydentów według rodzaju od 1 do 30 listopada 2025 r. Źródło: CERT Polska / CSIRT NASK.

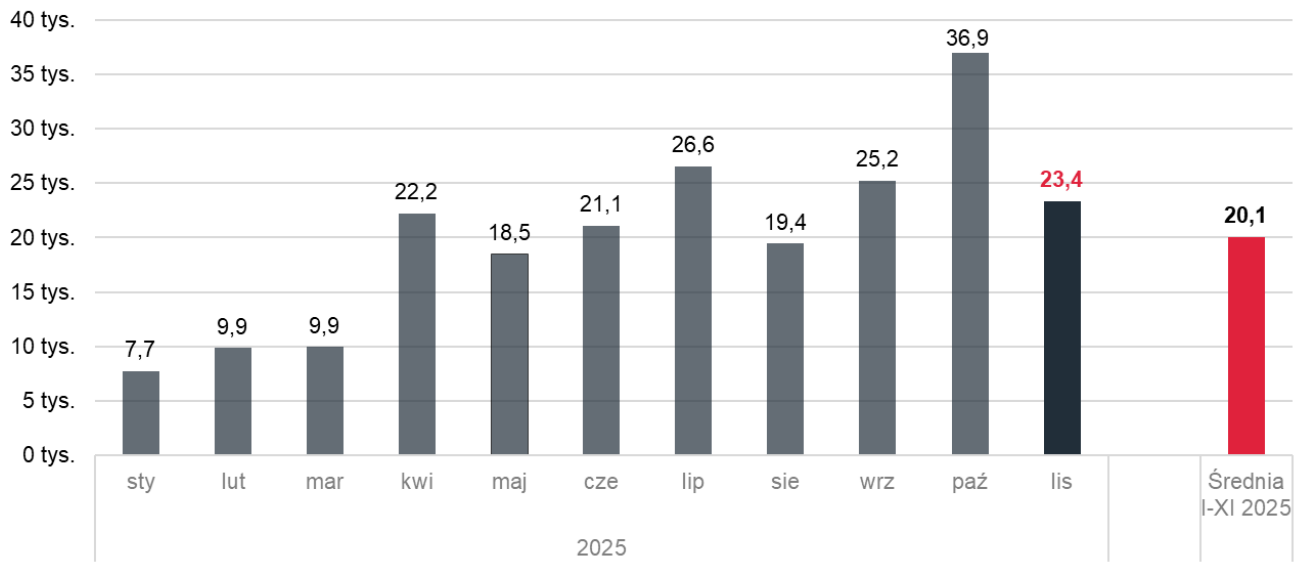
W analizowanym okresie zdecydowanie najczęściej występującą kategorią zagrożeń były oszustwa komputerowe. Wśród ogółu obsłużonych incydentów (**24,5 tys.**) stanowiły one **97%**. Najbardziej rozpowszechnionym rodzajem oszustw komputerowych były próby wyłudzania poufnych danych, np. loginu i hasła do poczty, strony banku, portalu społecznościowego czy innej usługi online (ang. *phishing*). W listopadzie 2025 r. łącznie odnotowano **7,5 tys.** tego typu incydentów.

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

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

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

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



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

Od stycznia do listopada 2025 r. na Listę Ostrzeżeń przed niebezpiecznymi stronami wpisano **220,9 tys.** szkodliwych domen, z czego w listopadzie 2025 r. dodano **23,4 tys.** nazw domen wykorzystywanych do wyłudzania danych osobowych, danych uwierzytelniających do kont

bankowych i serwisów społecznościowych. Wartość ta w stosunku do października 2025 r. **zmniejszyła się o 37%**.

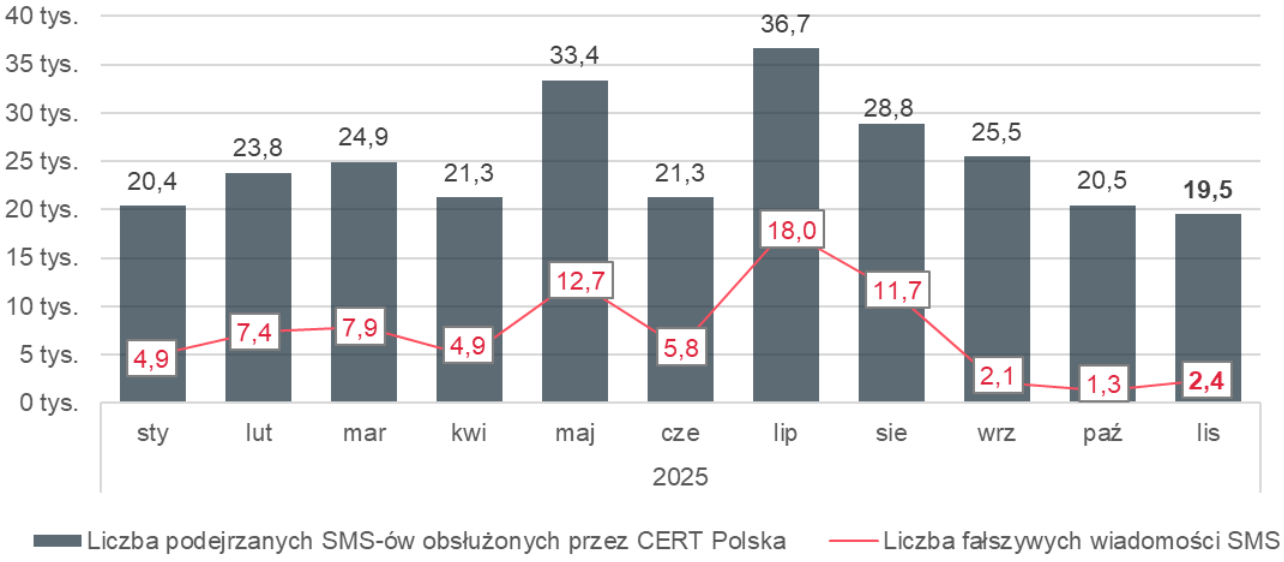
Lista Ostrzeżeń dostępna jest na stronie: CERT Polska/Lista Ostrzeżeń

Przykładowe nazwy fałszywych domen:

0lx.zam0wlenlef8445.top; 352710472.pl; aiebilet.allegrolokalnie.live; alertypolska.pro; allegro.pl-oferta122351-ps5-vr-2-z-gwarancja.sbs; biedronka.life; bitcoin-smarter.net; butysklep.shop; cryptosmartportal.com; dhl.pl-poczta.info; eobuwieonlinepl.com; govl.pl; inpost.fit; inpost.paczka-pl.com; inwestujai.site; inwestujpolskaonline.com; ipkobusiness.com; lidl-de.one; loginmojeing.ingbank.pl.adspire.top; mojnfz.leczenie-opieka.com; najlepsze-prezenty.shop; olx.oferta.asia; onetnewspl.com; orlen-invest.info; oswietlonydom.com; personal-ipko.cloud; pocztapolska.top; polska-gold-ai.pl; polskiwegiel24h.com; santander-lokaty.com.pl; sklepbiegacza.outletstore.sbs; sklep-xcom.shop; telegram-pl.com; twojeinwestycjes.com; vinted.pl-oferta2699247-laptop-gamingowy-i7-gtx-960m.sbs; zalando-vip.top; ziko-aptekaonline.sbs

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

Od 1 stycznia do 30 listopada 2025 r. zespół CERT Polska zarejestrował **276,2 tys.** zgłoszeń podejrzanych SMS-ów. Liczba SMS-ów otrzymanych w listopadzie 2025 r. wyniosła **19,5 tys.** W porównaniu z październikiem 2025 r. był to **spadek o 5%**. Wśród ogółu SMS-ów przyjętych w listopadzie 2025 r. **fałszywe wiadomości**, czyli takie, w których nadawca podszywa się pod inny podmiot, aby skłonić odbiorcę wiadomości do określonego działania – np. podania danych osobowych, przekazania pieniędzy, wejścia na stronę internetową lub instalacji oprogramowania, **stanowiły 12%**.



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

Wzorce fałszywych wiadomości SMS I–XI 2025

Zgodnie z ustawą z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej CSIRT NASK **monitoruje występowanie smishingu** i **tworzy wzorce wiadomości**, które posiadają cechy pozwalające na uznanie ich za smishing. Działania te wykonuje na podstawie zgłoszeń podejrzanych wiadomości tekstowych (SMS) otrzymanych od odbiorców tych wiadomości oraz informacji otrzymanych od przedsiębiorców telekomunikacyjnych i innych podmiotów, np. banków, firm kurierskich, platform inwestycyjnych. CSIRT NASK zapewnia dostęp do informacji o występowaniu smishingu wraz ze wzorcami wiadomości Komendantowi Centralnego Biura Zwalczania Cyberprzestępczości, Prezesowi Urzędu Komunikacji Elektronicznej i przedsiębiorcom telekomunikacyjnym. Podejrzane SMS-y można zgłaszać do CSIRT NASK poprzez bezpłatny skrócony numer **8080**.

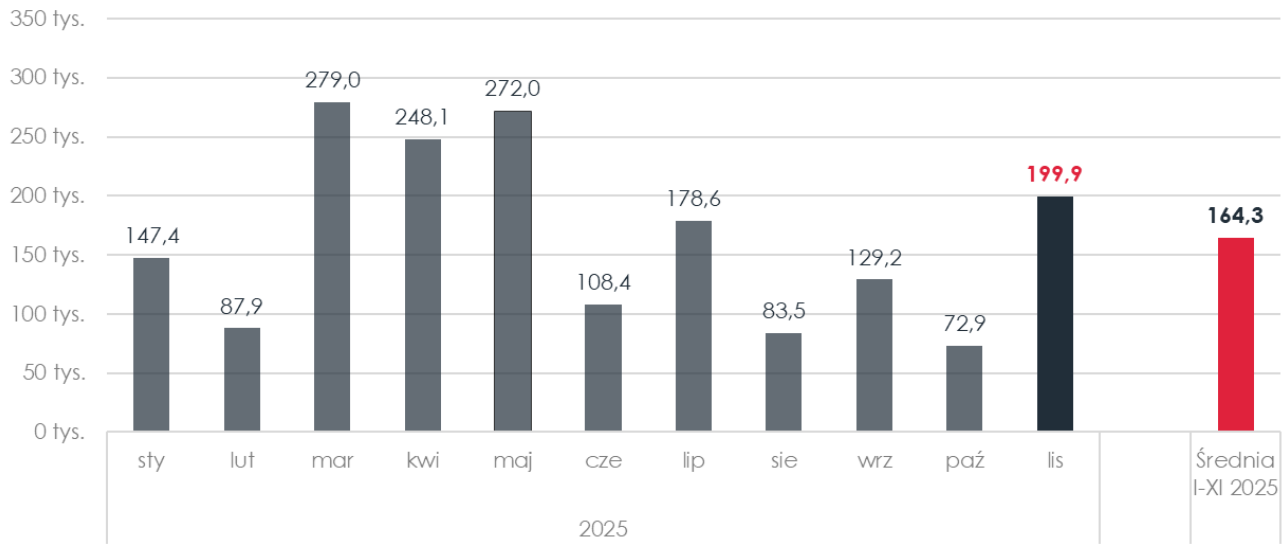
Tabela 2. Liczba wytworzonych wzorców fałszywych wiadomości SMS.

Wzorce fałszywych wiadomości SMS w 2025	sty	lut	mar	kwi	maj	cze	lip	sie	wrz	paź	lis	Razem
Liczba wytworzonych wzorców	82	57	106	60	83	39	119	10	43	36	**88**	**723**

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

Liczba zablokowanych SMS-ów I–XI 2025

W okresie od 1 stycznia do 30 listopada 2025 r., na podstawie wytworzonych przez CERT Polska wzorców fałszywych wiadomości SMS, zablokowano łącznie ponad **1,8 mln** SMS-ów.



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

Moje.cert.pl

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

W listopadzie 2025 r. w serwisie moje.cert.pl **zarejestrowało się 524 nowych użytkowników**.

W okresie od 1 do 30 listopada 2025 r. CSIRT NASK wysłał **5,9 tys. powiadomień w ramach serwisu moje.cert.pl dotyczących wykrytych podatności i błędnych konfiguracji**. Powiadomienia o wykrytych nieprawidłowościach zostały wysłane do osób, które zgłosiły daną stronę do skanowania w serwisie moje.cert.pl, a także do ich współpracowników dodanych w serwisie.

Więcej: moje.cert.pl

Podatności CVE

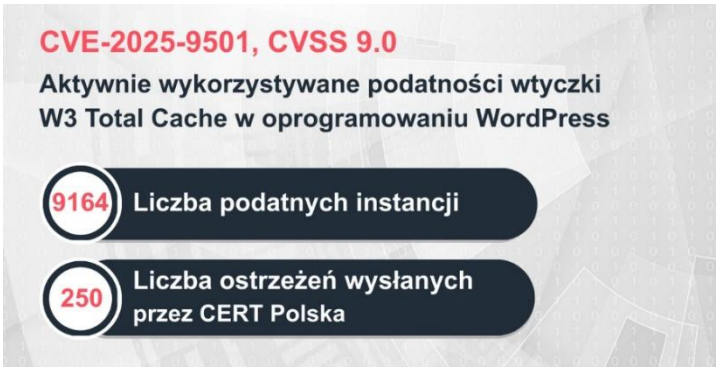
Zespół CERT Polska od sierpnia 2023 r. pełni funkcję CNA (ang. *CVE Numbering Authority*) – współtworzy bazę podatności poprzez nadawanie numerów CVE, które służą do identyfikacji i katalogowania publicznie ujawnionych podatności (więcej: CERT Polska/CNA). W listopadzie 2025 r. zespół CERT Polska nadał **21** numerów CVE. Wśród wykrytych podatności znalazły się podatności w oprogramowaniu m.in. JCD Windu CMS, SOPlanning i Times Software E-Payroll.

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

Tabela 3. Nadane numery CVE od 1 stycznia do 30 listopada 2025 r.

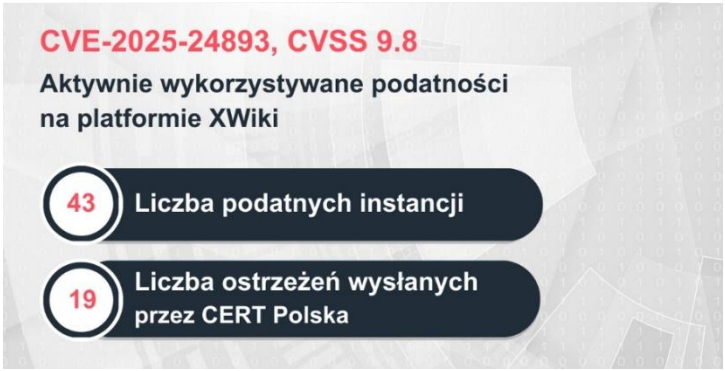
Numery CVE w 2025	sty	lut	mar	kwi	maj	cze	lip	sie	wrz	paź	lis	Razem
Liczba opublikowanych numerów CVE	4	9	11	15	22	3	6	36	16	12	**21**	**155**

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



Podatność polegająca na ataku typu command injection za pomocą funkcji _parse_dynamic_mfunc umożliwia niezautoryzowanym użytkownikom wykonywanie poleceń PHP poprzez przesłanie przygotowanego w specjalny sposób komentarza. Podatność została usunięta w wersji 2.8.13 przez producenta. Zalecana jest aktualizacja tej wtyczki do najnowszej wersji. Podatność otrzymała krytyczną ocenę CVSS (ang. Common Vulnerability Scoring System) 9.0.

Więcej: rcesecurity.com/Exploiting A Pre-Auth RCE in W3 Total Cache For WordPress (CVE-2025-9501)



Podatność umożliwia zdalne wykonanie kodu przez osobę niezalogowaną (anonimowego użytkownika). Atakujący może wykorzystać błąd w module wyszukiwania XWiki, co daje mu możliwość przejęcia kontroli nad serwerem. Oznacza to ryzyko dostępu do wrażliwych informacji, modyfikacji treści, instalacji złośliwego oprogramowania oraz trwałej kompromitacji systemu. Producent opublikował poprawki, które należy wdrożyć niezwłocznie. Podatność otrzymała krytyczną ocenę CVSS (ang. Common Vulnerability Scoring System) 9.8.

Więcej: securitybeztabu.pl/CISA dodaje luki XWiki (RCE) i VMware (LPE) do katalogu KEV

Wybrane informacje

3 listopada zespół CERT Polska opublikował **„Analizę kampanii złośliwego oprogramowania NGate (NFC relay)”**. Celem kampanii jest umożliwienie nieuprawnionych wypłat gotówki z bankomatów z wykorzystaniem kart płatniczych ofiar. Atak rozpoczyna się od wiadomości phishingowej, w której oszuści podszywają się pod bank i informują o rzekomym problemie technicznym lub incydencie bezpieczeństwa. W celu rzekomej aktywacji konta technicznego użytkownik jest nakłaniany do zainstalowania aplikacji na Androida z linku zawartego

w wiadomości. Następnie jest on proszony o zweryfikowanie swojej karty płatniczej w aplikacji. W tym celu musi przyłożyć fizyczną kartę do telefonu i wpisać PIN na klawiaturze ekranowej. Kiedy użytkownik zbliża kartę do modułu NFC, aplikacja przechwytuje jej dane (te same, które przepływają przez terminal w przypadku normalnej transakcji zbliżeniowej) i wysyła je przez internet do atakującego, który znajduje się przy bankomacie. Przestępca następnie odtwarza te dane w swoim telefonie, zbliża go do bankomatu i może w ten sposób wypłacić gotówkę.

Więcej: cert.pl/Analiza kampanii złośliwego oprogramowania NGate (NFC relay)

20 listopada ukazał się artykuł pt. **„Gra czy pułapka? Gdzie kończy się zabawa, a zaczyna cyberzagrożenie”**, poświęcony zagrożeniom, z którymi mogą się mierzyć gracze. W artykule specjaliści z CERT Polska scharakteryzowali najczęstsze schematy stosowane przez oszustów, podali sposoby na zmniejszenie ryzyka, takie jak regularne aktualizacje systemu, ostrożność przy pobieraniu nowych gier, korzystanie z dwuskładnikowego logowania, a także apelowali o to, by traktować bezpieczeństwo kont gamingowych tak samo poważnie jak ochronę danych finansowych.

Więcej: nask.pl/Gra czy pułapka? Gdzie kończy się zabawa, a zaczyna cyberzagrożenie

---

26 listopada w Warszawie odbyły się ćwiczenia **KSC-EXE 2025, podczas których sprawdzono działanie procedur oraz gotowość kluczowych podmiotów KSC do skutecznej współpracy w warunkach symulowanego kryzysu teleinformatycznego**. Ćwiczenia miały formułę Table Top Exercises (TTX), która pozwala uczestnikom na bezpieczne testowanie procedur, analizę scenariuszy i przegląd dostępnych zasobów bez ingerencji w rzeczywiste systemy IT. Udział w ćwiczeniach wzięło ponad 100 reprezentantów instytucji odpowiedzialnych za cyberbezpieczeństwo w Polsce, m.in. przedstawiciele organów właściwych, CSIRT-ów poziomu krajowego, w tym CSIRT NASK, sektorowych zespołów cyberbezpieczeństwa, RCB, UKE, CBZC. Ćwiczenia zostały zorganizowane przez Ministerstwo Cyfryzacji i Fundację Bezpieczna Cyberprzestrzeń.

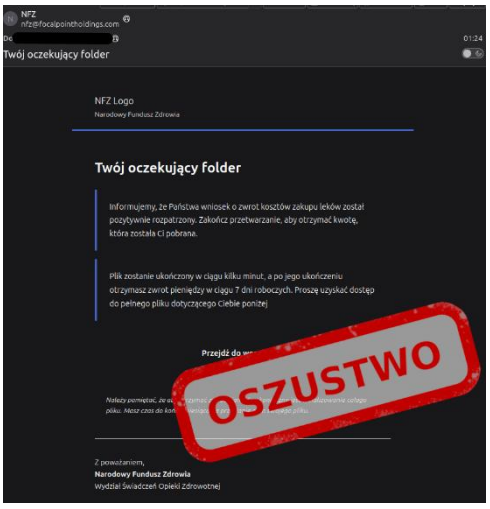
Więcej: gov.pl/KSC-EXE 2025: ćwiczenia krajowego systemu cyberbezpieczeństwa

27 listopada ENISA zorganizowała w Zagrzebiu 2. edycję **Cybersecurity Awareness Raising Conference**. Hasłem tegorocznej konferencji było wzmacnianie potencjału człowieka (ang. Empowering the Human Element) we wszelkich działaniach mających na celu ochronę przed cyberzagrożeniami. Uczestnicy wydarzenia dyskutowali m.in. na temat sposobów wykorzystania sztucznej inteligencji oraz strategii opartych na grywalizacji w tworzeniu kampanii zwiększających świadomość cyberbezpieczeństwa. Ekspert z CSIRT NASK wystąpił z prezentacją, w której podsumował kampanie edukacyjno-informacyjne przygotowane przez CERT Polska i NASK-PIB, oraz uczestniczył w panelu, podczas którego opowiedział o sukcesach w dziedzinie realnych działań podejmowanych przez obywateli pod wpływem tych kampanii.

Więcej: enisa.europa.eu/2nd Cybersecurity Awareness Raising Conference

Komunikaty o zagrożeniach

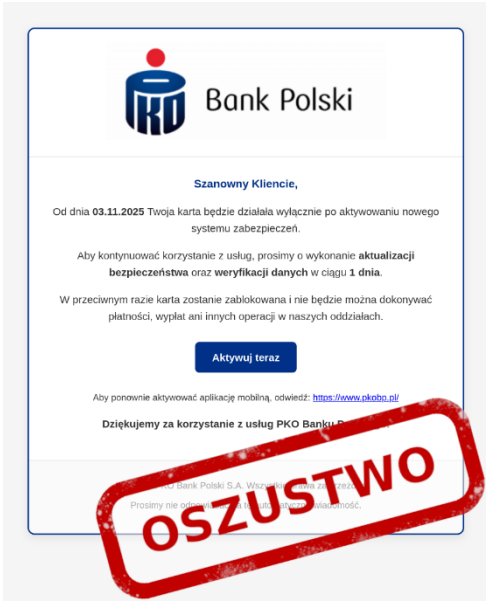
Informacje o zaobserwowanych kampaniach publikowane przez zespół CERT Polska w serwisie moje.cert.pl oraz w serwisach społecznościowych.



Zespół CERT Polska obserwował kampanię oszustw, w której przestępcy podszywają się pod Narodowy Fundusz Zdrowia. Z adresów e-mail zawierających w aliasie skrót „NFZ” masowo wysyłane są wiadomości zatytułowane „Twój oczekujący folder”. W treści wiadomości atakujący przekonują, że odbiorcy zostało przyznane prawo do zwrotu kosztów zakupu leków. Link zawarty w wiadomości kieruje do strony wyłudzającej dane osobowe oraz dane karty płatniczej.

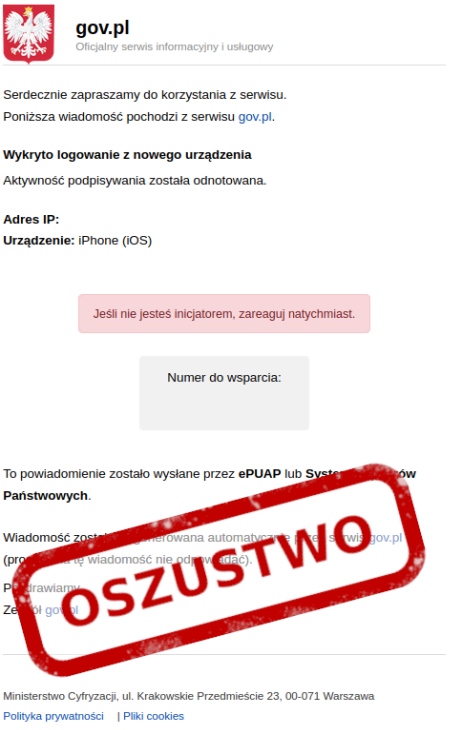
Zespół CERT Polska ostrzegał przed kampanią dystrybucji złośliwego oprogramowania NGate podszywającą się pod Spółdzielczą Grupę Bankową. Wiadomość wysłana przez oszustów zawiera informację o rzekomej aktywacji konta technicznego i nakłania do pobrania oraz zainstalowania złośliwej aplikacji z podanego linku. Szkodliwe oprogramowanie służy do ataku typu NFC relay, który polega na przechwyceniu komunikacji zbliżeniowej (np. danych karty płatniczej) i przekazaniu jej na odległość – np. do wspólnika przestępców czekającego przy bankomacie.

Więcej informacji o tej kampanii znajduje się w „Wybranych informacjach” na s. 10 i 11.



Zespół CERT Polska ostrzegał przed kolejną kampanią wymierzoną w klientów PKO BP. Odbiorca wiadomości e-mail jest informowany o rzekomej potrzebie wykonania aktualizacji bezpieczeństwa, bo w innym przypadku jego karta płatnicza przestanie działać. Link znajdujący się w wiadomości przekierowuje na fałszywy panel logowania do banku, który służy do wykradania loginów i haseł do bankowości elektronicznej.

Zespół CERT Polska obserwował kolejną kampanię, w której oszuści podszywają się pod NFZ. Adresaci wiadomości, pod pozorem odebrania zwrotu za zakupione leki, są zachęcani do odwiedzenia strony, która w rzeczywistości jest stroną phishingową wyłudzającą dane użytkowników. Ponadto oszuści informują o krótkim terminie odebrania wniosku, tak aby potencjalnie poszkodowane osoby miały mniej czasu, aby zorientować się, że podana wiadomość jest fałszywa.



Zespół CERT Polska informował o nowej odsłonie kampanii phishingowej, w której przestępcy podszywają się pod serwisy w domenie gov.pl. Oszuści rozsyłają różne warianty wiadomości, w których są podane informacje m.in.: o oficjalnym powiadomieniu elektronicznym od gov.pl, o nowej aktywności w serwisie gov.pl, o utworzeniu nowej sesji na urządzeniu mobilnym. W wiadomościach oszuści zachęcają do kontaktu telefonicznego pod wskazany numer. Po wykonaniu połączenia przez użytkownika przestępcy próbują nakłonić go do zainstalowania oprogramowania dającego im zdalny dostęp do komputera. W efekcie atakujący dokonują nieautoryzowanych przelewów na swoje konta.

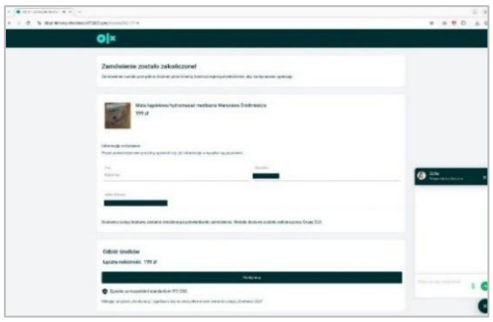
Więcej: Facebook/CERT Polska, X/CERT Polska oraz moje.cert.pl/komunikaty

Opis najczęściej występujących kampanii – XI 2025

Fałszywe strony oferujące wysokodochodowe inwestycje

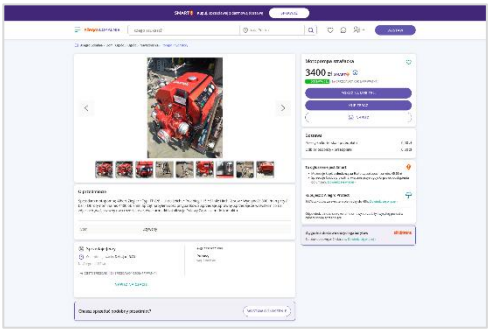
Zespół CERT Polska w dalszym ciągu obserwował wzmożoną kampanię phishingową, w której oszuści podszywają się pod różnego rodzaju koncerny paliwowo-energetyczne, firmy, instytucje, m.in. Lotos, Tesla, PGNiG i PGE. Oszuści reklamują w mediach społecznościowych czy w wyszukiwarkach internetowych nieistniejące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

Fałszywe strony OLX



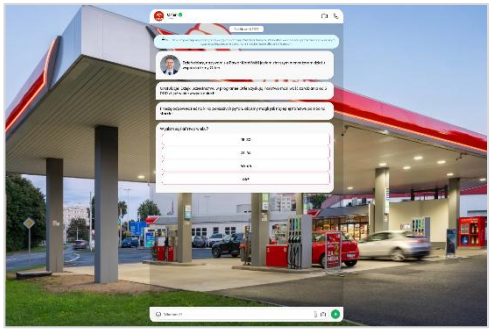
Zespół CERT Polska zarejestrował incydenty, w których atakujący za pośrednictwem stron internetowych podszywają się pod serwis OLX. Oszuści kontaktują się z potencjalną ofiarą przez komunikator WhatsApp. Wyrażają zainteresowanie przedmiotem z ogłoszenia, następnie informują, że zapłacili za zamówienie, a w kolejnym kroku wysyłają link do strony internetowej, poprzez którą rzekomo można wypłacić środki. Oprawa graficzna witryny przypomina stronę OLX, InPostu, DPD, DHL lub Poczty Polskiej. Znajduje się na niej fałszywy panel płatniczy. Podanie danych karty powoduje utratę środków finansowych przechowywanych na koncie bankowym.

Fałszywe strony Allegro



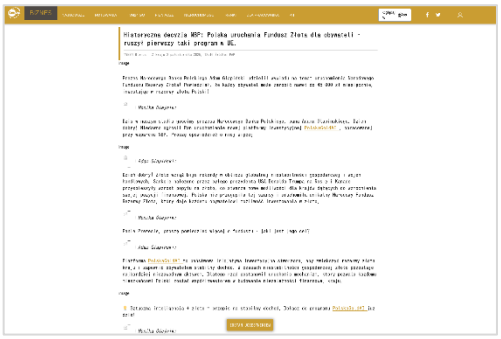
Zespół CERT Polska obserwował wzmożoną kampanię phishingową wykorzystującą wizerunek platformy Allegro. Na fałszywych stronach internetowych znajduje się panel logowania do tego serwisu służący do wyłudzania danych uwierzytelniających od użytkowników Allegro.

Fałszywe strony firmy Orlen



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

Fałszywe strony kanału TVN



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

Fałszywe strony 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.

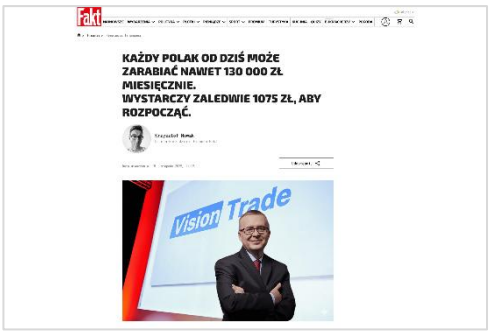
Fałszywe strony serwisu Gazeta.pl

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

Fałszywe strony serwisu Onet.pl

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

Fałszywe strony serwisu Fakt.pl



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

Fałszywe strony Telewizji Polskiej (TVP)

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