CZERWIEC 2026

# Podsumowanie Miesiąca CERT POLSKA

Nr 6/2026

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 30 czerwca 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 – VI 2026

**Tabela 1. Liczba zgłoszeń oraz zarejestrowanych incydentów od 1 do 30 czerwca 2026 r.**

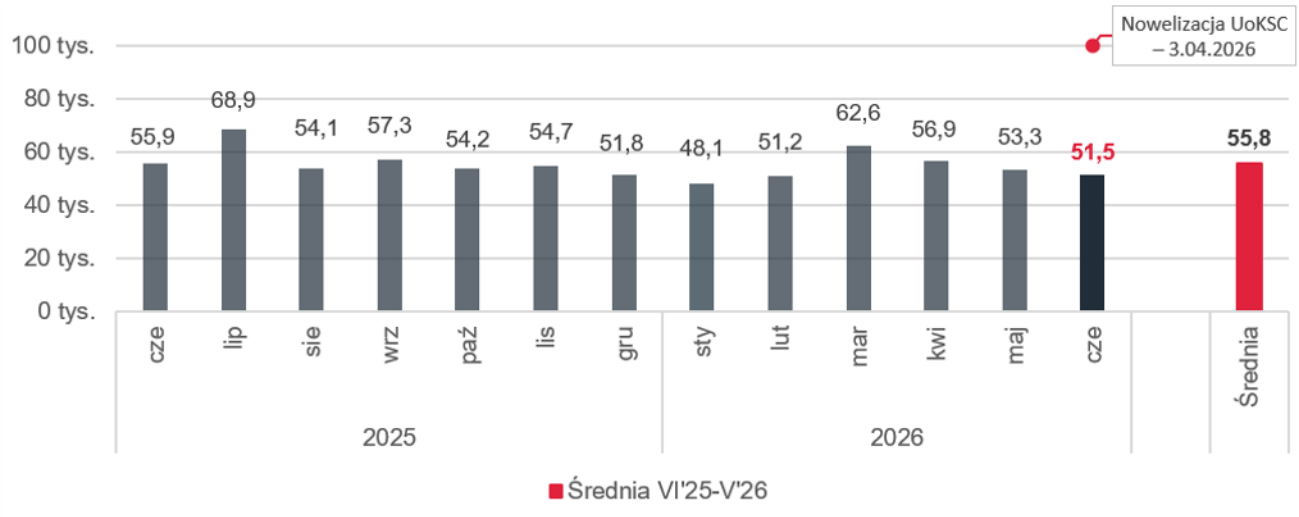
| Zgłoszone zagrożenia i zarejestrowane incydenty | Liczba |
|---|---|
| Zgłoszenia potencjalnych zdarzeń dla cyberbezpieczeństwa* | 6,2 tys. |
| Zgłoszenia cyberzagrożeń* | 41,7 tys. |
| Zgłoszenia incydentów | 3,4 tys. |
| Zgłoszenia poważnych cyberzagrożeń* | 0,16 tys. |
| **Razem zgłoszenia** | **51,5 tys.** |
| **Zarejestrowane incydenty**** | **22,8 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 czerwcu 2026 r. zespół CERT Polska otrzymał **łącznie 51,5 tys. zgłoszeń**. Na ich podstawie **zarejestrowano 22,8 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.

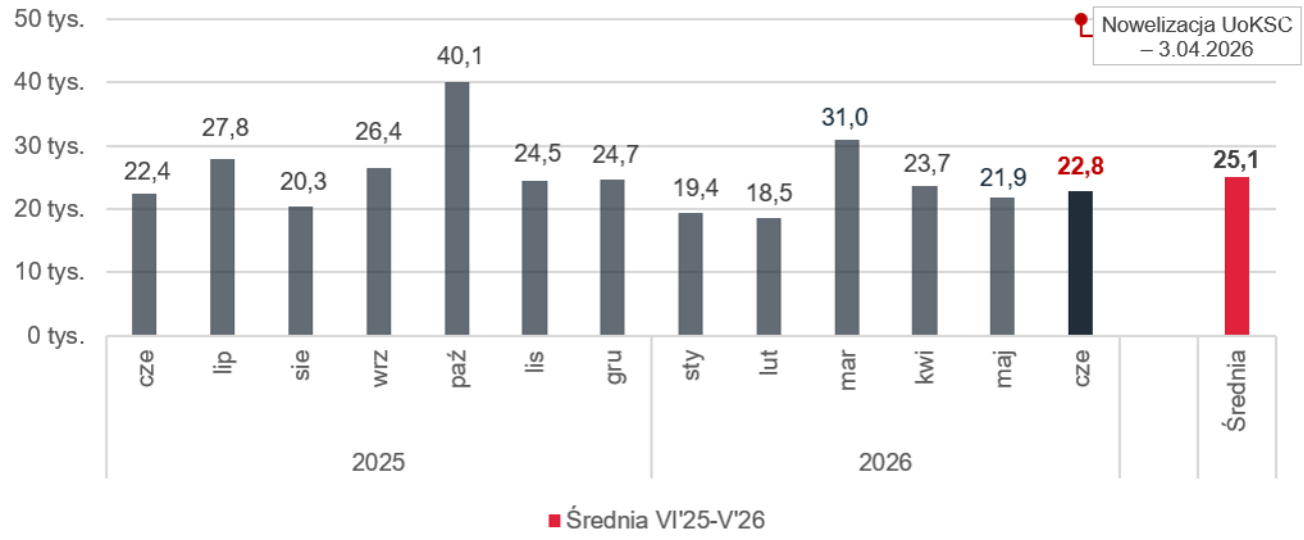
## Zgłoszenia zagrożeń od VI 2025 do VI 2026




**Wykres 1. Liczba wszystkich zgłoszeń od 01.06.2025 do 30.06.2026. Źródło: CERT Polska / CSIRT NASK.**

Liczba wszystkich zgłoszeń odnotowanych w czerwcu 2026 r. pozostawała poniżej średniej liczonej z poprzednich 12 miesięcy. W porównaniu z analogicznym miesiącem 2025 r. liczba ta **zmniejszyła się o 8%**. W stosunku do maja 2026 r. odnotowano **spadek o 3%**.

## Zarejestrowane incydenty cyberbezpieczeństwa od VI 2025 do VI 2026



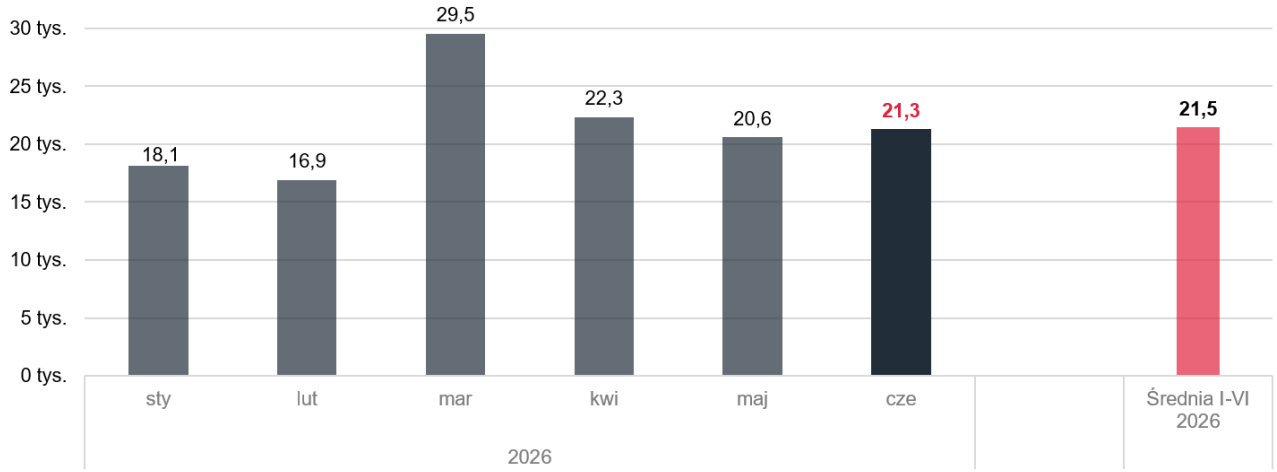

**Wykres 2. Liczba zarejestrowanych incydentów od 01.06.2025 do 30.06.2026. Źródło: CERT Polska / CSIRT NASK.**

Liczba incydentów zarejestrowanych w czerwcu 2026 r. wyniosła **22,8 tys.** W porównaniu z analogicznym miesiącem 2025 r. liczba incydentów w czerwcu 2026 r. **zwiększyła się o 2%** i pozostawała poniżej średniej liczonej z 12 poprzednich miesięcy. W stosunku do maja 2026 r. odnotowano **wzrost liczby incydentów o 4%**.

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

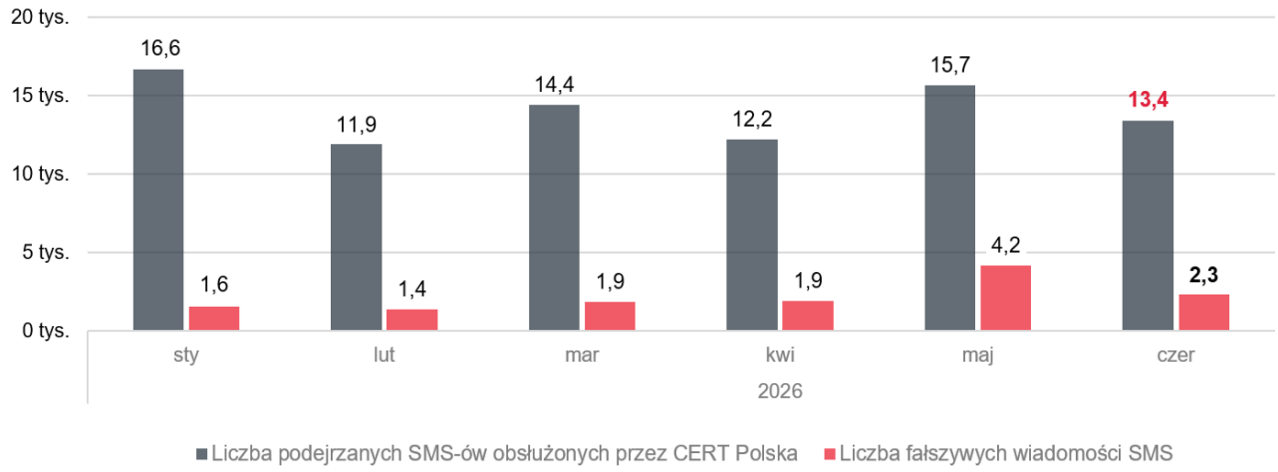



**Wykres 3. Liczba nazw szkodliwych domen wpisanych na Listę Ostrzeżeń. Źródło: CERT Polska / CSIRT NASK.**

Od 1 stycznia do 30 czerwca 2026 r. na Listę Ostrzeżeń przed niebezpiecznymi stronami wpisano **128,7 tys.** szkodliwych domen, z czego w czerwcu 2026 r. dodano **21,3 tys.** nazw domen wykorzystywanych do wyłudzania danych osobowych, danych uwierzytelniających do kont bankowych i serwisów społecznościowych. Wartość ta w stosunku do maja 2026 r. **zwiększyła się o 3%**.

## Liczba zgłoszeń wiadomości SMS przyjętych przez CERT Polska I–VI 2026

Od 1 stycznia do 30 czerwca 2026 r. zespół CERT Polska zarejestrował **84,1 tys.** zgłoszeń podejrzanych SMS-ów. Liczba SMS-ów otrzymanych w czerwcu 2026 r. wyniosła **13,4 tys.** W porównaniu z majem 2026 r. był to **spadek o 15%**. Wśród ogółu SMS-ów przyjętych w czerwcu 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 17%**.




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

## Wzorce fałszywych wiadomości SMS I–VI 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 czerwcu 2026 r., na podstawie wytworzonych przez CERT Polska wzorców fałszywych wiadomości SMS, zablokowano łącznie **23,6 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.

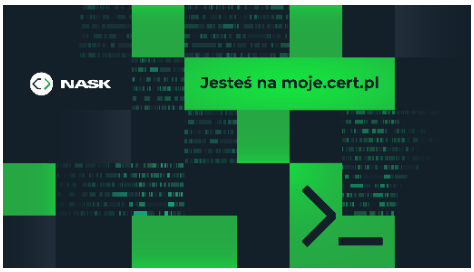
| Wzorce fałszywych wiadomości SMS w 2026 | sty | lut | mar | kwi | maj | cze | Razem |
|---|---|---|---|---|---|---|---|
| Liczba wytworzonych wzorców | 118 | 97 | 85 | 80 | 105 | **36** | **521** |

**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 czerwcu 2026 r. w serwisie moje.cert.pl **zarejestrowało się 707 nowych użytkowników**.




W okresie od 1 do 30 czerwca 2026 r. CERT Polska wysłał **10 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 czerwcu 2026 r. zespół CERT Polska nadał **47** numerów CVE. Wśród wykrytych podatności znalazły się podatności w oprogramowaniu m.in. Redeight CMS, SzafirHost, LMS, Logseq, Quick.CMS, Wirtualna Uczelnia.

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

**Tabela 3. Nadane numery CVE od 1 stycznia do 30 czerwca 2026 r.**

| Numery CVE w 2026 | sty | lut | mar | kwi | maj | cze | Razem |
|---|---|---|---|---|---|---|---|
| Liczba opublikowanych numerów CVE | 16 | 12 | 32 | 21 | 34 | **47** | **162** |

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


Podatność typu improper access control (CWE-284) we wbudowanym rejestrze obrazów Docker platformy Gitea umożliwia nieuwierzytelnionemu atakującemu pobieranie prywatnych obrazów Docker z instancji Gitea bez odpowiednich uprawnień.

Podatność wynika z braku odpowiedniej weryfikacji autoryzacji zapytań obsługi rejestru kontenerów, co pozwala na ominięcie mechanizmów kontroli dostępu i eksfiltrację prywatnych obrazów. Kod wykorzystujący podatność jest udostępniony w internecie, co dodatkowo zwiększa prawdopodobieństwo nieautoryzowanego dostępu.

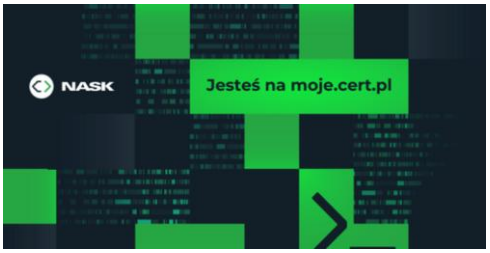
**Więcej:** https://labs.cloudsecurityalliance.org/research/csa-research-note-gitea-cve-2026-27771-container-exposure-20


Krytyczna podatność typu improper access control (CWE-284) w rozszerzeniu JCE (Joomla Content Editor) dla systemu CMS Joomla umożliwia nieuwierzytelnionemu atakującemu utworzenie nowych profili edytora, co może prowadzić do umieszczenia i wykonania na serwerze dowolnego kodu PHP.

Podatność dotyczy wersji JCE do 2.9.99.4 włącznie. Atakujący może przejąć pełną kontrolę nad serwerem webowym, uzyskać dostęp do bazy danych, modyfikować treść strony oraz wykorzystać skompromitowany serwer jako punkt startowy do dalszych ataków na infrastrukturę wewnętrzną. CVE w wyniku raportowanych przypadków aktywnego wykorzystania podatności trafiło do katalogu CISA KEV (Known Exploited Vulnerabilities).

**Więcej:** https://www.sonicwall.com/blog/joomla-content-editor-remote-code-execution

# Wybrane informacje




2 czerwca zespół CERT Polska opublikował artykuł pt. **„Zaufanie liczone w tysiącach – moje.cert.pl”**. Serwis moje.cert.pl od 2025 r. wspiera właścicieli domen i administratorów sieci w dbaniu o cyberbezpieczeństwo ich produktów. Na początku czerwca 2026 r. liczba zarejestrowanych użytkowników przekroczyła 20 tys. W ramach moje.cert.pl przeskanowano ponad 3,5 mln domen, subdomen i adresów IP oraz zidentyfikowano przeszło 750 tys. podatności i błędnych konfiguracji. Od lutego 2026 r. dostępna jest funkcjonalność „Infrastruktura organizacji”, która pozwala zobaczyć całość infrastruktury widocznej z internetu (a więc także z perspektywy potencjalnego atakującego), np. subdomeny, wszystkie widoczne technologie, hosty, otwarte porty i powiązane z nimi podatności.

**Więcej:** cert.pl/Zaufanie liczone w tysiącach – moje.cert.pl

10 i 11 czerwca odbyła się 8. edycja **Cyber Europe**, jednych z największych europejskich ćwiczeń z zakresu cyberbezpieczeństwa. Organizuje je co dwa lata ENISA, a ich celem jest testowanie procedur zarządzania kryzysowego. Każda edycja koncentruje się na wybranych sektorach gospodarki Unii Europejskiej – w tym roku scenariusz obejmował cyberzagrożenia skierowane na podsektory: transportu kolejowego i transportu morskiego. Tegoroczna edycja ćwiczeń była też okazją do przetestowania procedur zawartych w zaktualizowanym w 2025 r. dokumencie Cyber Blueprint określającym plan skoordynowanego reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę.
Po stronie polskiej w ćwiczeniach uczestniczyli m.in. przedstawiciele zespołu CERT Polska, Urzędu Morskiego w Szczecinie, Urzędu Transportu Kolejowego oraz innych podmiotów administracji publicznej, podsektorów transportu kolejowego i transportu morskiego.

**Więcej:** enisa.europa.eu/Cyber Europe 2026

---

12 czerwca na stronie cert.pl ukazał się artykuł pt. **„Kampania phishingowa grupy UNC1151/Ghostwriter na pocztę Gmail”** opisujący obserwowaną od kilku miesięcy przez zespół CERT Polska zmianę sposobu działania tej grupy APT. Atakujący dotychczas skupiali się na użytkownikach korzystających z usług polskich dostawców poczty elektronicznej (WP, Onet, Interia), natomiast od marca 2026 r. realizują również kampanie phishingowe wymierzone w użytkowników poczty Gmail. W kręgu zainteresowania grupy są osoby zaangażowane w życie polityczne, aktywne społecznie, zajmujące eksponowane stanowiska, naukowcy, dziennikarze, pracownicy administracji publicznej i służb mundurowych, a także inne osoby powiązane z nimi poprzez relacje rodzinne lub towarzyskie. Przejęte skrzynki poczty elektronicznej są przeszukiwane pod kątem listy kontaktów, wrażliwych dokumentów czy powiązanych kont. Istotnym rozwinięciem możliwości atakujących jest zdolność wyłudzania kodu dwuskładnikowego uwierzytelnienia.

**Więcej:** cert.pl/Kampania phishingowa grupy UNC1151/Ghostwriter na pocztę Gmail

15 czerwca w Warszawie odbyła się 3. edycja konferencji **Digital Skills Summit**. W wydarzeniu, zorganizowanym przez Ministerstwo Cyfryzacji i NASK – PIB we współpracy z Senatem RP, wzięli udział przedstawiciele administracji publicznej, instytucji odpowiedzialnych za bezpieczeństwo państwa, organizacji międzynarodowych, sektora technologicznego, środowiska naukowego oraz mediów. Tematem przewodnim konferencji było hasło „Kompetencje cyfrowe społeczeństwa a rozwój odporności informacyjnej państwa w obliczu zagrożeń hybrydowych". Rozmawiano także m.in. o kompetencjach cyfrowych kadr sektorów kluczowych w kontekście narodowej odporności cyfrowej – temu tematowi poświęcony był panel ekspercki, w którym uczestniczył dyrektor Pionu CSIRT NASK.

**Więcej:** nask.pl/Jak budować odporność cyfrową społeczeństwa? Digital Skills Summit 2026

---

15–16 czerwca w Katowicach odbyła się konferencja **CYBERSEC Expo & Forum**. Eksperci z zespołu CERT Polska wzięli udział w panelach: „Cyberportret polskiego biznesu 2026", „Ochrona infrastruktury krytycznej. Lekcje na przyszłość" i „CISO i CIO pod presją. Wyzwania menadżerów".

Podczas wydarzenia wręczono nagrody **CYBERSEC Awards**. NASK – PIB został wyróżniony w kategoriach Lider w Cyberedukacji oraz Innowacja Roku za Polski System Dystrybucji Klucza Kwantowego.

**Więcej:** cybersecforum.eu/program, nask.pl/Nagrody dla NASK. CYBERSEC 2026

---


19 czerwca zespół CERT Polska wydał **pilne rekomendacje dla wszystkich instytucji korzystających z oprogramowania FortiGate**. Była to odpowiedź na publikację informacji o wykryciu w sieci listy loginów i haseł do urządzeń FortiGate zawierającej kilkadziesiąt tysięcy wpisów z całego świata.

**Więcej:** moje.cert.pl/Pilne rekomendacje dla wszystkich instytucji korzystających z oprogramowania FortiGate

25 czerwca Pełnomocnik Rządu ds. Cyberbezpieczeństwa wydał **rekomendację dotyczącą ograniczenia ryzyk związanych z transportem poczty z wykorzystaniem nieszyfrowanych kanałów transmisji**. Wytyczne zawarte w dokumencie obejmują m.in. wyłączenie słabych algorytmów szyfrowania i protokołów kryptograficznych, konfigurację serwerów pocztowych w celu poprawnej weryfikacji certyfikatów TLS oraz ustawienie rekordów PTR w usłudze DNS. W rekomendacji podano także, że CSIRT NASK poszerzył zakres usług serwisu **bezpiecznapoczta.cert.pl** o moduł sprawdzający, czy serwery pocztowe obsługują szyfrowanie komunikacji. Ponadto w ramach projektu **Artemis** cykliczne skanowanie będzie obejmowało również sprawdzenie, czy serwery pocztowe umożliwiają zestawienie połączenia szyfrowanego.

**Więcej:** gov.pl/Rekomendacja Pełnomocnika Rządu ds. Cyberbezpieczeństwa

# Wystąpienia ekspertów CERT Polska

- 2 czerwca – udział w panelu dyskusyjnym poświęconym wspieraniu podmiotów sektora ochrony zdrowia we wdrażaniu nowych obowiązków w ramach nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, konferencja „Perspektywy e-Zdrowia. Nowy etap cyfryzacji i bezpiecznej transformacji”, Warszawa.

  **Więcej:** cez.gov.pl/informacje

- 11 czerwca – prowadzenie warsztatu pt. „Bezpieczna kancelaria komornicza – jak nie stracić danych i kontroli” podczas dorocznego Szkolenia Komorników i Asesorów w Karpaczu.

  **Więcej:** szkoleniekomornikow.pl/agenda

- 16 czerwca – wystąpienia ekspertów podczas spotkania FIRST w Denver. Pierwsza prezentacja pt. „How to Detect and Block over 200 Thousands of Investment Scam Domains” dotyczyła metod wykrywania oszustw inwestycyjnych oraz implementacji ich blokowania, np. z wykorzystaniem Listy Ostrzeżeń CERT Polska, druga – pt. „Analyzing Internet Background Radiation” – poświęcona była międzynarodowej współpracy w zakresie monitorowania ruchu sieciowego i technik wykrywania wartościowych informacji wśród „szumu”.

  **Więcej:** first.org/Conference 2026/agenda

- 19 czerwca – prezentacja pt. „Krajobraz bezpieczeństwa polskiego internetu według CERT Polska” podczas DEFCON Warsaw Meetup.

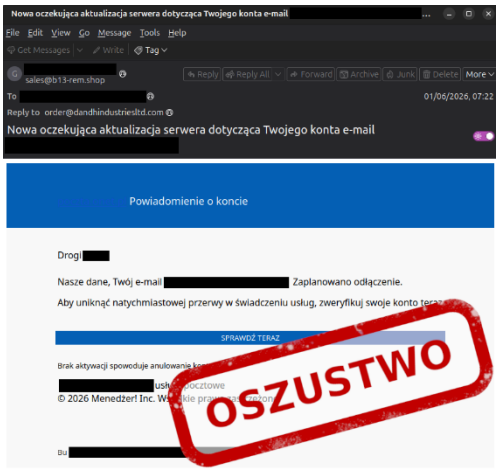
  **Więcej:** dc4822.org/DEFCON Warsaw Meetup/informacje, agenda

# Komunikaty o zagrożeniach

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

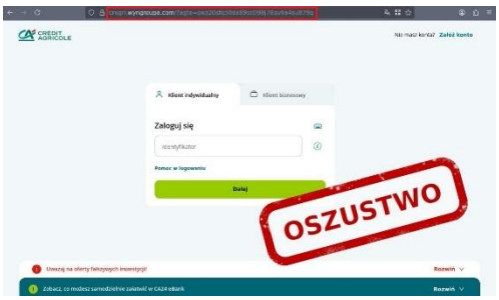

Zespół CERT Polska obserwował kampanię dystrybucji szkodliwego oprogramowania, w której oszuści wykorzystują wizerunek Alior Banku. Wysyłają e-maile, w których informują, że w załączniku znajduje się potwierdzenie wpłaty, rzekomo dokonanej przez klienta. Załącznik o rozszerzeniu .tar zawiera szkodliwe oprogramowanie, które wykrada dane z zainfekowanego urządzenia. Dane te mogą być wykorzystane przez cyberprzestępców do przeprowadzania kolejnych, bardziej precyzyjnych ataków.

---

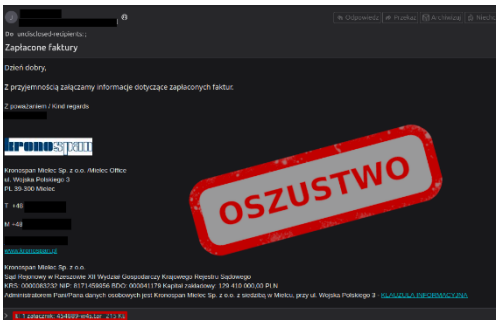



Zespół CERT Polska informował o kampanii phishingowej, w której oszuści podszywają się pod dostawcę usług pocztowych. Cyberprzestępcy informują odbiorcę wiadomości, że jego konto e-mail ma zostać wyłączone lub dezaktywowane i aby uniknąć natychmiastowej przerwy w świadczeniu usług, musi on je bezzwłocznie zweryfikować. Link zawarty w wiadomości odsyła do strony imitującej panel logowania poczty. Login i hasło wpisane przez użytkownika mogą zostać później wykorzystane przez oszustów m.in. do przejęcia skrzynki i innych powiązanych usług.

---

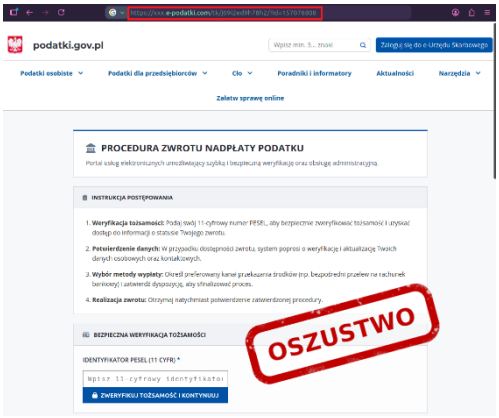



Zespół CERT Polska obserwował nasilające się kampanie phishingowe, w których cyberprzestępcy wykorzystują wizerunki znanych banków. W wiadomościach piszą o rzekomej pilnej konieczności weryfikacji danych klienta w związku ze zmianami w polityce bezpieczeństwa banku i podają link do strony internetowej podszywającej się pod prawdziwe serwisy bankowości elektronicznej. Dane uwierzytelniające trafiają do cyberprzestępców i mogą zostać przez nich wykorzystane do przejęcia konta lub dalszych nadużyć finansowych.



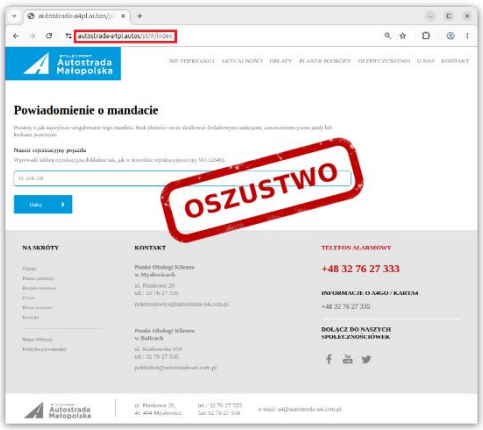

Zespół CERT Polska informował o kampanii phishingowej, w której oszuści podszywają się pod firmy z sektora produkcji. Cyberprzestępcy rozsyłają wiadomości e-mail przypominające standardową korespondencję biznesową związaną z rozliczeniami płatności. Do wiadomości dołączony jest plik, który zawiera szkodliwe oprogramowanie. Podejrzane załączniki najczęściej zdradza nietypowe rozszerzenie pliku, ujawniające plik wykonywalny albo archiwum, np.: .exe, .msi, .bat, .cmd, .scr, .zip, .rar czy .tar. Po uruchomieniu pliku przez użytkownika przestępcy uzyskują zdalny dostęp do urządzenia, co pozwala na kradzież danych lub zmianę konfiguracji komputera.

---

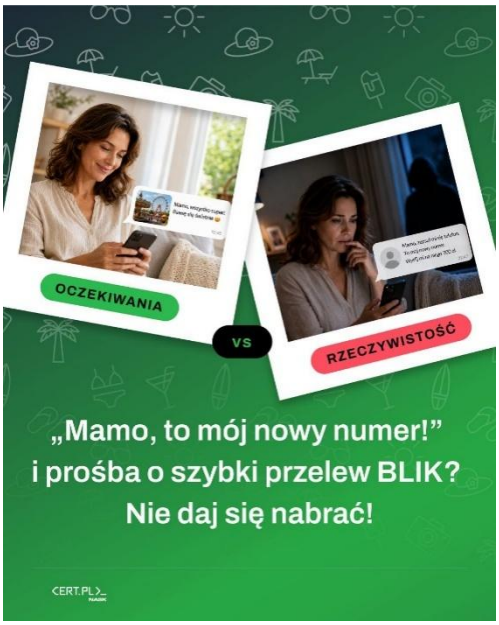



Zespół CERT Polska obserwował kampanię phishingową, w której oszuści rozsyłają e-maile imitujące korespondencję od Krajowej Administracji Skarbowej. W wiadomościach tych informują, że po zakończeniu weryfikacji rocznego rozliczenia podatkowego za 2025 r. użytkownikowi przysługuje zwrot nadpłaconego podatku dochodowego. Odnośnik zawarty w wiadomości prowadzi na stronę podszywającą się pod serwis podatki.gov.pl, gdzie przestępcy próbują wyłudzić numer PESEL, dane osobowe oraz dane karty płatniczej.

---



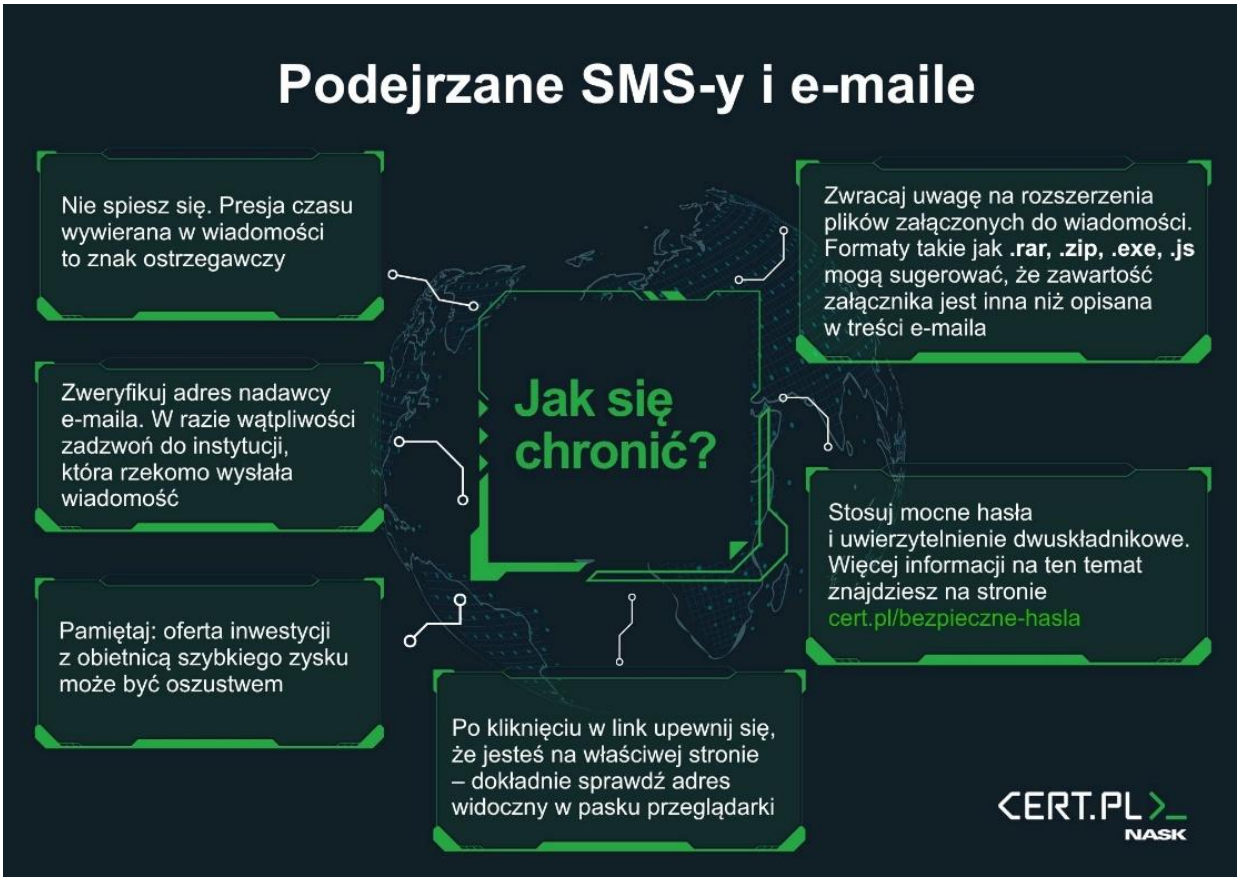

Zespół CERT Polska obserwował powrót kampanii SMS-owej, w której oszuści przesyłają powiadomienia o rzekomo nieuregulowanych opłatach za wykroczenia drogowe i informują, że brak płatności może skutkować dodatkowymi sankcjami, zawieszeniem prawa jazdy lub skierowaniem sprawy do sądu. Aby skłonić odbiorcę do szybkiego działania, oszuści podają krótki termin płatności oraz sugerują, że istnieją dowody wykroczenia (nagrania, zdjęcia). Link zawarty w wiadomości prowadzi do fałszywej strony, na której ma być dokonana płatność. Cyberprzestępcy wykorzystują wizerunek spółki zarządzającej autostradą A4. Użytkownik proszony jest o wpisanie numeru rejestracyjnego pojazdu, a następnie danych osobowych i karty płatniczej.




Zespół CERT Polska ostrzegał przed oszustwem wymierzonym w rodziców, których dzieci są na wakacyjnych wyjazdach. Dystrybucja oszustwa odbywa się za pomocą wiadomości SMS – cyberprzestępcy podszywają się w nich pod dzieci, które rzekomo mają uszkodzony telefon, więc piszą z nowego numeru i proszą o przesłanie pieniędzy. W SMS-ie zazwyczaj jest link do konwersacji na WhatsAppie i dalsza manipulacja odbywa się już za pośrednictwem tego komunikatora.

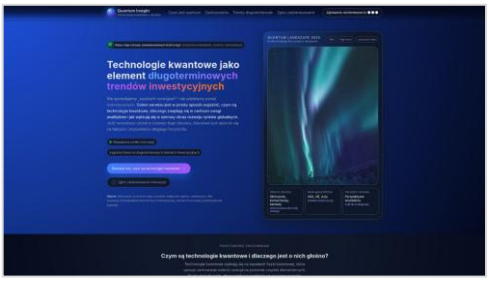
**Więcej:** x.com/CERT Polska/uwaga na wakacyjne oszustwo

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



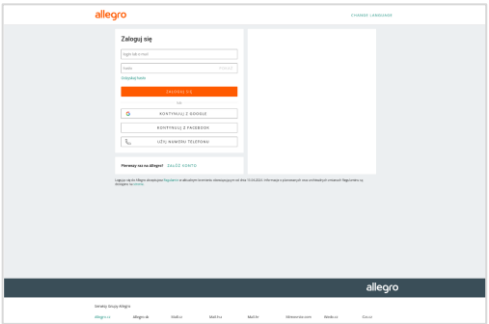
# Opis najczęściej występujących kampanii – VI 2026

## 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 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

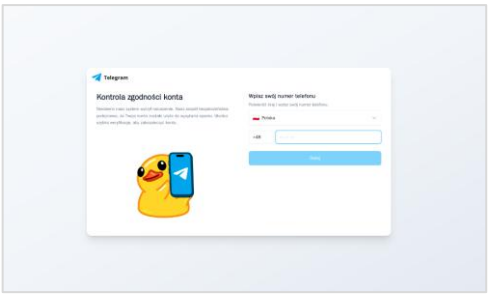



Zespół CERT Polska obserwował wzmożoną kampanię phishingową wykorzystującą wizerunek platformy Allegro. Na fałszywych stronach internetowych znajduje się panel logowania do tego serwisu służący do wyłudzania danych uwierzytelniających od użytkowników Allegro.

## 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 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 Onet.pl


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

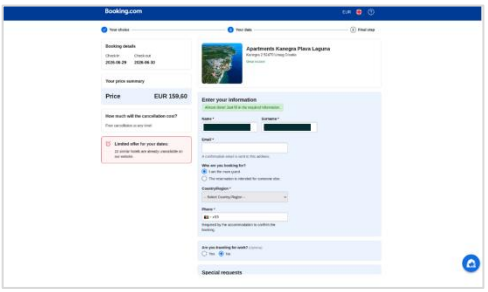
## Fałszywe strony serwisu gov.pl


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.

## Fałszywe strony OLX

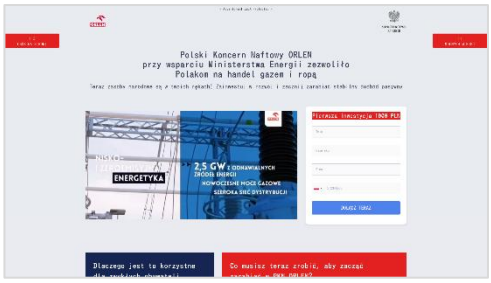
Zespół CERT Polska zarejestrował incydenty, w których atakujący za pośrednictwem stron internetowych podszywają się pod serwis OLX. Panel logowania do tego serwisu służy do wyłudzania od użytkowników danych uwierzytelniających.

## Fałszywe rezerwacje serwisu Booking.com



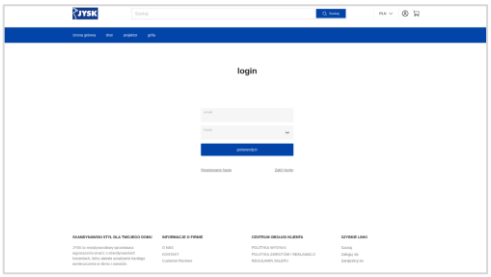

Zespół CERT Polska rejestrował incydenty, w których cyberprzestępcy tworzą fałszywe strony internetowe przypominające witrynę serwisu rezerwacyjnego Booking.com. Panel logowania znajdujący się na tych stronach służy oszustom do wyłudzania od użytkowników ich danych uwierzytelniających lub danych karty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

## Fałszywe strony 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 internetowe sieci handlowej JYSK




Zespół CERT Polska rejestrował incydenty, w których oszuści wykorzystują wizerunek marki JYSK.
Na fałszywych stronach internetowych znajduje się panel logowania służący do wyłudzania od klientów danych uwierzytelniających.